kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 AO Kaspersky Lab

目录

Kaspersky Security Center 15.1 帮助
新闻
关于 Kaspersky Security Center
  架构
  硬件和软件要求
    管理服务器要求
    Web Console 要求
    移动服务器要求
    管理控制台要求
    网络代理要求
  兼容的卡巴斯基应用程序和解决方案
  Kaspersky Security Center 15.1 的授权许可和功能
  关于 Kaspersky Security Center 组件的兼容性
  Kaspersky Security Center 的比较：基于 Windows 与基于 Linux
  关于 Kaspersky Security Center 云控制台
Kaspersky Security Center 15.1
  基本概念
    管理服务器
    管理服务器层级
    虚拟管理服务器
    移动设备服务器
    Web 服务器
    网络代理
    管理组
    受管理设备
    未分配的设备
    管理员工作站
    管理插件
    管理 Web 插件
    策略
    策略配置文件
    任务
    任务范围
    本地应用程序设置与策略的关系
    分发点
    连接网关
  主要安装方案
  Kaspersky Security Center 使用的端口
  用于 Kaspersky Security Center 的证书
    关于 Kaspersky Security Center 证书
    关于管理服务器证书
    对 Kaspersky Security Center 中使用的自定义证书的要求
    场景：指定自定义管理服务器证书

使用 klsetsrvcert 实用程序替换管理服务器证书
使用 klmover 实用程序将网络代理连接到管理服务器
重新颁发 Web 服务器证书
数据流量和端口使用的 schema
LAN 中的管理服务器和受管理设备
局域网中的主管理服务器和两个从属管理服务器
管理服务器位于 LAN、受管理设备位于互联网、反向代理使用中
管理服务器位于 LAN、受管理设备位于互联网、连接网关使用中
管理服务器位于 DMZ、受管理设备位于互联网
Kaspersky Security Center 组件和安全应用程序的交互：更多信息
交互模式中的惯例
管理服务器和 DBMS
管理服务器和管理控制台
管理服务器和客户端设备：管理安全应用程序
通过分发点在客户端设备上升级软件
管理服务器层级：主管理服务器和从属管理服务器
DMZ 中带有从属管理服务器的管理服务器层级
管理服务器、网段连接网关和客户端设备
管理服务器和 DMZ 中的两台设备：连接网关和客户端设备
管理服务器和 Kaspersky Security Center Web Console
激活和管理移动设备上的安全应用程序
部署最佳实践
强化指南
管理服务器部署
连接安全
账户和身份验证
管理服务器保护的管理
管理客户端设备保护
配置受管理应用程序的保护
管理服务器维护
事件传输到第三方系统
第三方信息系统安全建议
有关使用卡巴斯基安全应用程序的建议
部署准备
计划 Kaspersky Security Center 部署
部署保护系统的常规方案
关于在组织网络中规划 Kaspersky Security Center 的部署
选择企业保护结构
Kaspersky Security Center 的标准配置
标准配置：单一办公室
标准配置：由自己管理员运行的几个大规模办公室
标准配置：多个小远程办公室
为管理服务器选择 DBMS
配置与 Kaspersky Security Center 15.1 配合使用的 MariaDB x64 服务器
配置与 Kaspersky Security Center 15.1 配合使用的 MySQL x64 服务器
配置与 Kaspersky Security Center 15.1 配合使用的 PostgreSQL 或 Postgres Pro 服务器
使用 Kaspersky Endpoint Security for Android 管理移动设备

提供到管理服务器的互联网访问
互联网访问：本地网络上的管理服务器
互联网访问：DMZ 中的管理服务器
互联网访问：DMZ 中作为连接网关的网络代理
关于分发点
增加 klnagent 服务的文件描述符限制
计算分发点的数量和配置
管理服务器层级
虚拟管理服务器
Kaspersky Security Center 的限制信息
网络负载
反病毒保护的初始部署
反病毒数据库的原始更新
使客户端和管理服务器同步
反病毒数据库附加更新
利用管理服务器对客户端事件的处理
24小时流量
准备移动设备管理
iOS MDM 服务器
标准配置：DMZ 中的 Kaspersky Device Management for iOS
标准配置：组织本地网络中的 iOS MDM 服务器
使用 Kaspersky Endpoint Security for Android 管理移动设备
管理服务器性能相关信息
连接到管理服务器的限制
管理服务器性能测试报告
KSN 代理服务器性能测试结果
用于与外部服务交互的网络设置
部署网络代理和安全应用程序
初始化部署
配置安装程序
安装包
MSI 属性和转换文件
使用应用程序远程安装的第三方工具部署
关于 Kaspersky Security Center 中的远程安装任务
通过捕获和复制设备镜像来部署
硬盘驱动器镜像错误复制
使用 Microsoft Windows 组策略部署
通过 Kaspersky Security Center 远程安装任务的强制部署
运行 Kaspersky Security Center 创建的独立包
手动安装应用程序的选项
创建 MST 文件
在安装有网络代理的设备上远程安装应用程序
在远程安装任务中管理设备重启
安全应用程序安装包上的数据库更新
在 Kaspersky Security Center 中使用工具远程安装应用程序以便在受管理设备上运行相关可执行文件
监控部署

- 配置安装程序
  - 常规信息
  - 在静默模式下安装(带有响应文件)
  - 在静默模式下安装网络代理（没有响应文件）
  - 通过 setup.exe 的部分安装配置
  - 管理服务器安装参数
  - 网络代理安装参数
- 虚拟基础架构
  - 降低虚拟机负载的窍门
  - 对动态虚拟机的支持
  - 对虚拟机复制的支持
- 对网络代理设备文件系统回滚的支持
- 应用程序的本地安装
  - 网络代理的本地安装
  - 在静默模式下安装网络代理
  - 以静默模式安装 Linux 网络代理（使用应答文件）
  - 准备在封闭软件环境模式下运行 Astra Linux 的设备以安装网络代理
  - 以交互模式安装 Linux 网络代理
  - 应用程序管理插件的本地安装
  - 以静默模式安装应用程序
  - 使用独立包安装应用程序
  - 网络代理安装包设置
  - 查看隐私策略
- 部署移动设备管理系统
  - 使用 iOS MDM 协议部署管理系统
    - 安装 iOS MDM 服务器
    - 在静默模式安装 iOS MDM 服务器
    - iOS MDM 服务器部署方案
    - 简易部署方案
    - 涉及 Kerberos constrained delegation (KCD) 的部署方案
    - 接收 APNs 证书
    - 续费 APNs 证书
    - 配置备用 iOS MDM 服务器证书
    - 将 APNs 证书安装至 iOS MDM 服务器
    - 配置到苹果推送通知服务的访问
    - 在移动设备上发布和安装共享证书
  - 添加 KES 设备到受管理设备列表
  - 将 KES 设备连接至管理服务器
    - 直接连接设备到管理服务器
    - 连接 KES 设备到 Kerberos constrained delegation (KCD) 服务器的方案
    - 使用 Firebase Cloud Messaging
  - 与公共密钥基础架构整合
  - Kaspersky Security Center Web Server

Kaspersky Security Center 的安装
准备安装
使用 DBMS 的账户
配置 SQL Server 的使用账户（Windows 身份验证）
配置 SQL Server 的使用账户（SQL Server 身份验证）
配置 MySQL 和 MariaDB 的使用账户
在 MySQL 或 MariaDB DBMS 中将数据从共享表空间移动到每个表一个文件的表空间
配置 PostgreSQL 和 Postgres Pro 的使用账户
方案：对 Microsoft SQL Server 进行身份验证
场景：验证 MySQL 服务器
场景：验证 PostgreSQL 服务器
管理服务器安装建议
在失败转移集群上为管理服务器服务创建账户
定义共享文件夹
使用管理服务器工具通过活动目录组策略远程安装
通过传送 UNC 路径到独立包远程安装
从管理服务器共享文件夹更新
安装操作系统镜像
指定管理服务器地址
标准安装
步骤 1：查看授权许可协议和隐私策略
步骤 2：选择安装方法
步骤 3：安装 Kaspersky Security Center Web Console
步骤 4：选择网络规模
步骤 5：选择数据库
步骤 6：配置 SQL Server
步骤 7：选择身份验证模式
步骤 8：在硬盘驱动器上解压并安装文件
自定义安装
步骤 1：查看授权许可协议和隐私策略
步骤 2：选择安装方法
步骤 3：选择要安装的组件
步骤 4：安装 Kaspersky Security Center Web Console
步骤 5：选择网络规模
步骤 6：选择数据库
步骤 7：配置 SQL Server
步骤 8：选择身份验证模式
步骤 9：选择账户以启动管理服务器
步骤 10：选择账户以运行 Kaspersky Security Center 服务
步骤 11：选择共享文件夹
步骤 12：配置与管理服务器的连接
步骤 13：定义管理服务器地址
步骤 14：用于连接移动设备的管理服务器地址
步骤 15：选择应用程序管理插件
步骤 16：在硬盘驱动器上解压并安装文件

部署 Kaspersky Security Center 故障转移集群
方案：部署Kaspersky Security Center 故障转移集群
关于 Kaspersky Security Center 故障转移集群
为 Kaspersky Security Center 故障转移集群准备文件服务器
为 Kaspersky Security Center 故障转移集群准备节点
在 Kaspersky Security Center 故障转移集群节点上安装 Kaspersky Security Center
手动启动和停止集群节点
在 Windows 服务器故障转移集群上安装管理服务器
步骤 1：查看授权许可协议和隐私策略
步骤 2：选择集群上的安装类型
步骤 3：指定虚拟管理服务器的名称
步骤 4：指定虚拟管理服务器的网络详细信息
步骤 5：指定集群组
步骤 6：选择集群数据存储
步骤 7：指定用于远程安装的账户
步骤 8：选择要安装的组件
步骤 9：选择网络规模
步骤 10：选择数据库
步骤 11：配置 SQL Server
步骤 12：选择身份验证模式
步骤 13：选择账户以启动管理服务器
步骤 14：选择账户以运行 Kaspersky Security Center 服务
步骤 15：选择共享文件夹
步骤 16：配置与管理服务器的连接
步骤 17：定义管理服务器地址
步骤 18：用于连接移动设备的管理服务器地址
步骤 19：在硬盘驱动器上解压并安装文件
在静默模式下安装管理服务器
在管理员工作站安装管理控制台
安装 Kaspersky Security Center 后系统的变化
卸载程序
关于升级 Kaspersky Security Center
从先前版本升级 Kaspersky Security Center
在 Kaspersky Security Center 故障转移集群节点上升级 Kaspersky Security Center
在 Microsoft 故障转移集群节点上升级 Kaspersky Security Center
Kaspersky Security Center 的初始化配置
强化指南
管理服务器快速启动向导
关于快速启动向导
开始管理服务器快速启动向导
步骤 1：配置代理服务器
步骤 2：选择应用程序激活方法
步骤 3：选择保护范围和操作系统
步骤 4：选择受管理应用程序的插件
步骤 5：下载分发包并创建安装包
步骤 6：配置卡巴斯基安全网络使用
步骤 7：配置邮件通知

步骤 8：配置更新管理
步骤 9：创建初始保护配置
步骤 10：连接移动设备
步骤 11：下载更新
步骤 12：设备发现
步骤 13：关闭快速启动向导
配置管理控制台与管理服务器的连接
配置管理服务器的互联网连接设置
连接漫游设备
方案：通过连接网关连接漫游设备
方案：通过 DMZ 中的从属管理服务器连接漫游设备
关于连接漫游设备
将外部台式设备连接到管理服务器
关于漫游用户的连接配置文件
为漫游用户创建连接配置文件
关于将网络代理切换到其他管理服务器
根据网络位置创建网络代理切换规则
事件通知
配置事件通知
测试通知
通过运行可执行文件显示的事件通知
使用 TLS 的加密通信
配置界面
发现网络设备
情景：发现网络设备
未分配的设备
设备发现
Windows 网络轮询
活动目录轮询
IP 范围轮询
Zeroconf 轮询
使用 Windows 域查看和更改域设置
为未分配的设备配置保留规则
使用 IP 范围
创建 IP 范围
浏览和更改 IP 范围设置
使用活动目录组查看和修改组设置
创建将设备自动移至管理组的规则
在客户端设备上使用 VDI 动态模式
在网络代理安装包属性中启用 VDI 动态模式
搜索组成 VDI 的设备
将组成 VDI 的设备移至管理组
设备清单
添加有关新设备的信息
配置用于定义企业设备的标准
配置自定义字段

授权许可
超出了授权许可限制事件
关于授权许可
关于授权许可
关于最终用户授权许可协议
关于授权许可证书
关于授权许可密钥
关于密钥文件
关于订阅
关于激活码
撤销对最终用户授权许可协议的同意
关于数据提供
Kaspersky Security Center 授权许可选项
Kaspersky Security Center 和受管理应用程序的授权许可功能
Kaspersky 应用程序。集中部署
替换第三方安全应用程序
使用远程安装任务安装应用程序
安装应用程序到所选设备
在管理组中的客户端设备上安装应用程序
通过活动目录组策略安装应用程序
在 macOS 设备上远程安装应用程序
在从属管理服务器上安装应用程序
使用远程安装向导安装应用程序
使用管理插件
查看保护部署报告
应用程序的远程卸载
从管理组的客户端设备中远程卸载应用程序
从所选设备中远程卸载应用程序
使用安装包
创建安装包
创建独立安装包
创建自定义安装包
查看和编辑自定义安装包的属性
从 Kaspersky Security Center 分发包中获取网络代理安装包
将安装包分发至从属管理服务器
通过分发点分发安装包
将应用程序部署结果传输至 Kaspersky Security Center
为安装包定义 KSN 代理服务器地址
接收应用程序的最新版本
为远程安装准备 Windows 设备
准备 Linux 设备并在 Linux 设备上远程安装网络代理
准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理
准备 macOS 设备以远程安装网络代理
Kaspersky 应用程序：授权许可和激活
受管理应用程序的授权许可
查看使用中授权许可密钥的相关信息
添加授权许可密钥到管理服务器存储库

- 添加管理服务器授权许可密钥
- 部署授权许可密钥到客户端设备
- 自动分发授权许可密钥
- 创建和浏览授权许可密钥使用报告
- 查看有关应用程序授权许可密钥的信息
- 导出授权许可密钥文件

配置网络保护

- 方案：配置网络保护
- 策略设置和传播：以设备为中心的方法
- 关于以设备为中心和以用户为中心的安全管理方法
- Kaspersky Endpoint Security 策略的手动设置
  - 在高级威胁防护区域配置策略
  - 在关键威胁防护部分配置策略
  - 在常规设置部分配置策略
  - 在事件配置区域配置策略
- Kaspersky Endpoint Security 更新组任务的手动设置
- Kaspersky Endpoint Security 设备扫描组任务的手动设置
- 计划“查找漏洞和所需更新”任务
- 更新安装和漏洞修复组任务的手动设置
- 设置事件存储库中的最大事件数量
- 设置有关已修复漏洞的信息的最长保存期限
- 管理任务
  - 创建任务
  - 创建管理服务器任务
  - 为特定设备创建任务
  - 创建本地任务
  - 在嵌套组工作区中显示继承的组任务
  - 在任务启动前自动开启设备
  - 在任务结束后自动关闭设备
  - 限制任务运行时间
  - 导出任务
  - 导入任务
  - 转换任务
  - 手动启动和停止任务
  - 手动暂停和恢复任务
  - 监视任务执行
  - 浏览保存在管理服务器中的任务运行结果
  - 配置任务运行结果信息的过滤条件
  - 要修改任务回滚更改
  - 比较任务
  - 启动任务的账户
  - 导出任务执行的历史记录
  - 更改任务密码向导
    - 步骤 1：指定凭证
    - 步骤 2：选择要采取的操作
    - 步骤 3：查看结果
- 为属于虚拟管理服务器的管理组创建层级结构

- 策略和策略配置文件
  - 策略层级，使用策略配置文件
    - 策略层级
    - 策略配置文件
    - 策略设置继承
  - 管理策略
    - 创建策略
    - 在子组中显示继承的策略
    - 激活策略
    - 在出现病毒爆发事件时自动激活策略
    - 应用漫游策略
    - 修改策略回滚更改
    - 比较策略
    - 查看策略分发状态图
    - 删除策略
    - 复制策略
    - 导出策略
    - 导入策略
    - 转换策略
  - 管理策略配置文件
    - 创建策略配置文件
    - 修改策略配置文件
    - 删除策略配置文件
    - 创建策略配置文件激活规则
- 设备移动规则
- 克隆设备移动规则
- 软件分类
- 安装应用程序到客户端组织设备的先决条件
- 查看和编辑本地应用程序设置

更新 Kaspersky Security Center 和受管理应用程序

- 方案：定期更新 Kaspersky 数据库和应用程序
- 关于更新 Kaspersky 数据库、软件模块和应用程序
- 关于使用 diff 文件更新 Kaspersky 数据库和软件模块
- 启用下载 diff 文件功能
- 创建管理服务器的“将更新下载至存储库”任务
- 创建“将更新下载至分发点存储库”任务
- 配置管理服务器的“将更新下载至存储库”任务
- 验证已下载的更新
- 配置测试策略和辅助任务
- 浏览已下载的更新
- 在设备上自动安装 Kaspersky Endpoint Security 更新
- 离线模式更新下载
- 启用和禁用离线模式更新下载
- Kaspersky Security Center 组件的自动更新和补丁
- 启用和禁用 Kaspersky Security Center 组件的自动更新和补丁

自动分发更新
自动将更新分发至客户端设备
将更新自动分发至从属管理服务器
自动分配分发点
手动为设备指派分发点
从分发点列表删除设备
通过分发点下载更新
从存储库删除软件更新
集群模式下为 Kaspersky 应用程序安装补丁
在客户端设备上管理第三方应用程序
关于第三方应用程序
安装第三方软件更新
方案：更新第三方软件
查看有关第三方应用程序可用更新的信息
批准和拒绝软件更新
使用管理服务器从 Windows 更新同步更新
步骤 1：步骤 1：定义是否减少流量
步骤 2：应用程序
步骤 3：更新类别
步骤 4：更新语言
步骤 5：选择账户以移动任务
步骤 6：配置任务启动计划
步骤 7：定义任务名称
步骤 8：完成任务创建
手动在设备上安装更新
在网络代理策略中配置 Windows 更新
修复第三方软件漏洞
方案：查找和修复第三方软件中的漏洞
关于查找和修复软件漏洞
查看软件漏洞信息
查看受管理设备上的漏洞统计信息
扫描应用程序以查找漏洞
修复应用程序中的漏洞
修复隔离网络中的漏洞
方案：修复隔离网络中的第三方软件漏洞
关于修复隔离网络中的第三方软件漏洞
配置具有互联网访问权限的管理服务器以修复隔离网络中的漏洞
配置隔离的管理服务器以修复隔离网络中的漏洞
在隔离网络中传输补丁和安装更新
禁用在隔离网络中传输补丁和安装更新的选项
忽略软件漏洞
为第三方软件中的漏洞选择用户修补程序
更新安装规则
应用程序组
使用应用程序控制来管理可执行文件
获取并查看客户端设备上存储的可执行文件列表
为 Kaspersky Endpoint Security for Windows 策略创建应用程序类别

创建含有手动添加内容的应用程序类别
创建包括选定设备中的可执行文件的应用程序类别
创建包括特定文件夹中的可执行文件的应用程序类别
添加事件相关的可执行文件到应用程序类别
配置应用程序在客户端设备上的启动管理
查看应用到可执行文件的启动规则的统计分析的结果
查看应用程序注册表
更改软件清查开始时间
关于第三方应用程序的授权许可密钥管理
创建授权的应用程序组
管理已授权应用程序组的授权许可密钥
可执行文件存储库
查看可执行文件信息
监控和报告
方案：监控和报告
在管理控制台中监控信号灯和记录的事件
使用报告、统计和通知
使用报告
创建报告模板
查看和编辑报告模板属性
报告模板中的扩展过滤器格式
将过滤器转换为扩展格式
配置扩展过滤器
创建和浏览报告
保存报告
创建报告发送任务
步骤 1：选择任务类型
步骤 2：选择报告类型
步骤 3：报告操作
步骤 4：选择账户以移动任务
步骤 5：配置任务计划
步骤 6：定义任务名称
步骤 7：完成任务创建
管理统计信息
配置事件通知
为 SMTP 服务器创建证书
事件分类
查看事件分类
自定义事件分类
创建事件分类
将事件分类导出至文本文件
从分类中删除事件
根据用户请求添加应用程序到排除
设备分类
查看设备分类
配置设备分类
导出设备分类设置到文件

创建设备分类
根据导入的设置创建设备分类
在分类中从管理组中删除设备
监控应用程序安装和卸载
Kaspersky Security Center 组件事件
事件类型描述的数据结构
管理服务器事件
管理服务器严重事件
管理服务器功能失败事件
管理服务器警告事件
管理服务器信息事件
网络代理事件
网络代理功能失败事件
网络代理警告事件
网络代理信息事件
iOS MDM 服务器事件
iOS MDM 服务器功能失败事件
iOS MDM 服务器警告事件
iOS MDM 服务器信息事件
阻止频繁事件
关于阻止频繁事件
管理频繁事件阻止
移除对频繁事件的阻止
将频繁事件列表导出到文件
控制虚拟机状态的更改
使用系统注册表中的信息监控反病毒保护状态
当设备显示不活动时查看和配置操作
禁用 Kaspersky 公告
分发点和连接网关的调整
分发点的标准配置：单一办公室
分发点的标准配置：多个小远程办公室
分配受管理设备作为分发点
连接 Linux 设备作为隔离区域中的网关
通过连接网关将 Linux 设备连接到管理服务器
在 DMZ 中添加连接网关作为分发点
自动分配分发点
关于在选择用作分发点的设备上本地安装网络代理
关于使用分发点作为连接网关
将 IP 范围添加到分发点轮询的范围列表中
将分发点用作推送服务器
其他日常工作
管理管理服务器
创建管理服务器层级：添加从属管理服务器
连接至管理服务器以及在管理服务器之间切换
访问管理服务器及其对象的权限
通过互联网连接至管理服务器的条件

到管理服务器的加密连接
当设备连接时验证管理服务器
在管理控制台连接期间的管理服务器身份验证
配置允许连接到管理服务器的 IP 地址允许列表
使用 klscflag 实用程序关闭端口 13291
断开与管理服务器的连接
将管理服务器添加至控制台树
从控制台树中删除管理服务器
将虚拟管理服务器添加至控制台树
更改管理服务器服务账户实用工具 klsrvswch
更改 DBMS 凭据
更改管理服务器共享文件夹
使用管理服务器节点解决问题
查看和修改管理服务器的设置
调整管理服务器的常规设置
管理控制台界面设置
在管理服务器上的事件处理和存储
查看连接到管理服务器的日志
控制病毒爆发
限制流量
配置 web 服务器
使用内部用户
管理服务器设置的备份和恢复
使用文件系统快照降低备份时间
管理服务器设备不可操作
管理服务器设置或数据库被损坏
备份复制和管理服务器数据恢复
“备份管理服务器数据”任务
数据备份和恢复实用程序（klbackup）
交互模式下的数据备份和恢复
静默模式下的数据备份和恢复
使用 klbackup 实用程序切换受管理设备至另一台管理服务器的管理下
使用 MySQL 或 MariaDB 时备份和恢复管理服务器数据
优化管理服务器数据的备份和恢复
将管理服务器移动至其他设备
避免多个管理服务器之间的冲突
对管理组进行管理
创建管理组
移动管理组
删除管理组
自动创建管理组结构
将应用程序自动安装到管理组中的设备
管理客户端设备
将客户端设备连接至管理服务器
手动连接客户端设备至管理服务器。Klmover 工具
要建立客户端设备与管理服务器之间的通道连接

远程连接至客户端设备桌面
连接到 Windows 客户端设备
连接到 macOS 客户端设备
通过 Windows 桌面共享连接至客户端设备
配置重启客户端设备
审核在远程客户端设备上执行的操作
检查客户端设备与管理服务器之间的连接
自动检查客户端设备与管理服务器之间的连接
手动检查客户端设备与管理服务器之间的连接。Klnagchk 工具
关于检查设备和管理服务器之间的连接时间
在管理服务器上识别客户端设备
将设备移动至管理组
更改客户端设备的管理服务器
通过连接网关将连接到管理服务器的设备移动到另一台管理服务器
集群和服务器阵列
远程开启、关闭和重启客户端设备
关于在受管理设备和管理服务器之间使用持续连接
关于强制同步
关于连接计划
发送消息到设备用户
管理 Kaspersky Security for Virtualization
配置设备状态切换
标记设备和查看分配的标签
自动设备标记
查看和配置分配到设备的标签
客户端设备的远程诊断。Kaspersky Security Center 远程诊断工具
将远程诊断实用程序连接至客户端设备
为应用程序创建内存转储文件
启用和禁用跟踪，下载跟踪文件
下载应用程序设置
下载事件日志
下载多个诊断信息条目
开始诊断并下载诊断结果
开始、停止和重新启动应用程序
UEFI 保护设备
受管理设备设置
常规策略设置
网络代理策略设置
管理用户账户
使用用户账户
添加内部用户账户
编辑内部用户账户
更改允许的密码输入尝试次数
配置内部用户名称的唯一性检查
添加安全组
添加用户到组

- 配置对应用程序功能的访问权限。基于角色的访问控制
  - 应用程序功能的访问权限
  - 预定义用户角色
  - 添加用户角色
  - 为用户或安全组分配角色
  - 分配权限到用户和组
  - 传输用户角色到从属管理服务器
- 指派用户作为设备所有者
- 将消息传送给用户
- 查看用户的移动设备列表
- 为用户安装证书
- 查看发布给用户的证书列表
- 关于虚拟管理服务器的管理员

远程安装操作系统和应用程序

- 创建操作系统镜像
- 安装操作系统镜像
- 配置 KSN 代理服务器地址
- 添加 Windows Preinstallation Environment （WinPE） 的驱动程序
- 将驱动程序添加至带有操作系统镜像的安装包
- 配置 sysprep.exe 实用程序
- 在新联网的设备上部署操作系统
- 在客户端设备上部署操作系统
- 创建程序安装包
- 为应用程序安装包发布证书
- 安装应用程序到客户端设备

管理对象修订

- 关于对象修订
- 查看修订历史区域
- 比较对象修订
- 为对象修订和已删除对象信息设置存储期限
- 查看对象修订
- 保存对象修订到文件
- 回滚更改
- 添加修订描述

对象删除

- 删除对象
- 查看关于已删除对象的信息
- 从已删除对象列表永久删除对象

移动设备管理

- 方案：移动设备管理部署
- 有关管理 iOS MDM 设备的组策略
- 启用移动设备管理
- 修改移动设备管理设置
- 禁用移动设备管理
- 使用移动设备命令
  - 移动设备管理的命令
  - 使用 Firebase Cloud Messaging

发送命令
查看命令日志中的命令状态
使用移动设备证书
启动证书安装向导
步骤 1：选择证书类型
步骤 2：选择设备类型
步骤 3：选择用户
步骤 4：选择证书源
步骤 5：为证书分配标签
步骤 6：指定证书发布设置
步骤 7：选择用户通知方法
步骤 8：生成证书
配置证书发布规则
与公共密钥基础架构整合
启用支持 Kerberos Constrained Delegation
添加 iOS 移动设备到受管理设备列表
添加 Android 移动设备到受管理设备列表
管理 iOS MDM 设备
通过证书签署 iOS MDM 配置文件
添加配置文件
将配置文件安装至设备
从设备中删除配置文件
通过发布配置文件链接来添加新设备
通过由管理员安装配置文件来添加新设备
添加 provisioning 配置文件
将 provisioning 配置文件安装至设备
从设备中删除 provisioning 配置文件
添加受管理应用程序
在移动设备上安装应用
将应用从设备上卸载
在 iOS MDM 移动设备上配置漫游
查看有关 iOS MDM 设备的信息
将 iOS MDM 设备断开管理
发送命令到设备
检查所发送命令的执行状态
管理 KES 设备
创建 KES 设备移动应用程序包
启用基于证书的 KES 设备身份验证
查看有关 KES 设备的信息
将 KES 设备断开管理
数据加密和保护
查看已加密设备列表
查看加密事件列表
将加密事件列表导出到文本文件
创建和查看加密报告
在管理服务器之间传输加密密钥

- 数据存储库
  - 将存储库对象的列表导出到文本文件中
  - 安装包
  - 存储库中文件的主状态
  - 智能培训模式中的规则触发
    - 查看使用自适应异常控制规则执行的检测列表
    - 从自适应异常控制规则添加排除
      - 步骤 1：选择应用程序
      - 步骤 2：选择策略
      - 步骤 3：运行策略
  - 隔离区和备份区
    - 启用存储库文件远程管理
    - 查看存储库中的文件属性
    - 从存储库删除文件
    - 从存储库恢复文件
    - 将存储库中的文件保存到磁盘
    - 扫描隔离区中的文件
  - 活动威胁
    - 清除未处理文件
    - 将未处理的文件保存至磁盘
    - 从“活动威胁”文件夹中删除文件
- 卡巴斯基安全网络 (KSN)
  - 关于 KSN
  - 设置到卡巴斯基安全网络的访问
  - 启用和禁用 KSN
  - 查看已接受的 KSN 声明
  - 查看 KSN 代理服务器统计信息
  - 接受更新的 KSN 声明
  - 使用卡巴斯基安全网络获得增强保护
  - 检查分发点是否充当 KSN 代理服务器
- 切换在线帮助和离线帮助

导出事件到 SIEM 系统

- 配置导出事件到 SIEM 系统
- 在您开始之前
- 关于 Kaspersky Security Center 中的事件
- 关于事件导出
- 关于配置 SIEM 系统中的事件导出
- 标记要以 Syslog 格式导出到 SIEM 系统的事件
  - 标记要以 Syslog 格式导出的 Kaspersky 应用程序事件
  - 标记要以 Syslog 格式导出的常规事件
- 关于使用 Syslog 格式导出事件
- 关于使用 CEF 和 LEEF 格式导出事件
- 配置 Kaspersky Security Center 以导出事件到 SIEM 系统

直接从数据库导出事件
使用 klsql2 实用工具执行 SQL 查询
klsql2 实用工具中的 SQL 查询例子
查看 Kaspersky Security Center 数据库名称
查看导出结果
使用 SNMP 将统计信息发送到第三方应用程序
配置 SNMP 服务以与 Kaspersky Security Center 结合使用
SNMP代理和对象标识符
从对象标识符获取字符串计数器名称
SNMP 的对象标识符的值
故障排除
使用云环境
关于使用云环境
情景：在云环境中部署
在云环境中部署 Kaspersky Security Center 的先决条件
云环境中管理服务器的硬件要求
云环境中的授权许可选项
在云环境中工作的数据库选项
使用 Amazon Web Services 云环境
关于使用 Amazon Web Services 云环境
为 Amazon EC2 实例创建 IAM 角色和 IAM 用户账户
确保 Kaspersky Security Center 管理服务器具有使用 AWS 的权限
为管理服务器创建 IAM 角色
创建 IAM 用户账户以使用 Kaspersky Security Center
为安装应用程序到 Amazon EC2 实例创建 IAM 角色
使用 Amazon RDS
创建 Amazon RDS 实例
为 Amazon RDS 实例创建选项组
修改选项组
为 IAM 角色修改权限以使用 Amazon RDS 数据库实例
为数据库准备 Amazon S3 bucket
迁移数据库到 Amazon RDS
工作在 Microsoft Azure 云环境
关于使用 Microsoft Azure
创建订阅、应用程序 ID 和密码
分配角色到 Azure 应用程序 ID
在 Microsoft Azure 中部署管理服务器并选择数据库
使用 Azure SQL
创建 Azure 存储账户
创建 Azure SQL 数据库和 SQL Server
迁移数据库到 Azure SQL
在 Google Cloud 中工作
创建客户端电子邮件、项目 ID 和私钥
使用 Google Cloud SQL for MySQL 实例
在云环境中准备必要的客户端设备以使用 Kaspersky Security Center
创建配置云环境所需的安装包

- 配置云环境
  - 关于配置云环境向导
  - 步骤 1：选择应用程序激活方法
  - 步骤 2：选择云环境
  - 步骤 3：在云环境中授权
  - 步骤 4：配置与云的同步并选择后续操作
  - 步骤 5：在云环境中配置卡巴斯基安全网络
  - 步骤 6：在云环境中配置电子邮件通知
  - 步骤 7：创建云环境保护的初始配置
  - 步骤 8：步骤 8：选择在安装过程中操作系统必须重启时的操作（对于云环境）
  - 步骤 9：通过管理服务器接收更新
- 检查配置
- 云设备组
- 网段轮询
  - 为云段轮询添加连接
  - 为云段轮询删除连接
  - 配置轮询计划
- 安装应用程序到云环境中的设备
- 查看云设备属性
- 与云同步
- 在 Yandex.Cloud 中部署 Kaspersky Security Center

附录

- 高级功能
  - Kaspersky Security Center 操作自动化。klakaut 实用程序
  - 自定义工具
  - 网络代理磁盘克隆模式
  - 准备安装了网络代理的参考设备以创建操作系统映像
  - 配置从文件完整性监控接收消息
  - 管理服务器维护
  - 访问公共 DNS 服务器
  - 用户通知方法窗口
  - 设备分类窗口
  - 定义新对象名称窗口
- 使用管理界面的功能
  - 控制台树
  - 如何在工作区中更新数据
  - 如何浏览控制台树
  - 如何在工作区打开对象属性窗口
  - 如何在工作区中选择一组对象
  - 如何在工作区中更改表列集
- 参考信息
  - 上下文菜单命令
  - 受管理设备列表。列描述
  - 设备、任务和策略的状态
  - 管理控制台上的文件状态图标

搜索和导出数据
查找设备
设备搜索设置
在字符串变量中使用掩码
在搜索字段使用正则表达式
从对话框导出列表
任务设置
常规任务设置
“将更新下载至管理服务器存储库”任务设置
“将更新下载至分发点存储库”任务设置
“查找漏洞和所需更新”任务设置
“安装所需更新并修复漏洞”任务设置
子网全局列表
添加子网到子网全局列表
在子网全局列表中查看和修改子网属性
Windows、Linux 和 macOS 网络代理的使用：比较
Kaspersky Security Center Web Console
Kaspersky Security Center 管理服务器部署图表和 Kaspersky Security Center Web Console
Kaspersky Security Center Web Console 使用的端口
Kaspersky Security Center Web Console 界面
固定和取消固定主菜单的各部分
情景：Kaspersky Security Center Web Console 安装和初始化设置
安装
安装 Kaspersky Security Center (标准安装)
安装 Kaspersky Security Center Web Console
安装 Kaspersky Security Center Web Console，连接到安装在故障转移群集节点上的管理服务器
升级 Kaspersky Security Center Web Console
用于 Kaspersky Security Center Web Console 的证书
重新颁发 Kaspersky Security Center Web Console 的证书
替换 Kaspersky Security Center Web Console 证书
在 Kaspersky Security Center Web Console 中为受信任的管理服务器指定证书
将 PFX 证书转换为 PEM 格式
从 Kaspersky Security Center Windows 迁移
迁移到 Kaspersky Security Center 云控制台
迁移到 Kaspersky Next XDR Expert
迁移到 Kaspersky Security Center Linux
使用管理服务器数据备份迁移到 Kaspersky Security Center Linux
通过迁移向导迁移到 Kaspersky Security Center Linux
从 Kaspersky Security Center Windows 导出组对象
将导出文件导入到 Kaspersky Security Center Linux
将受管理设备切换为受 Kaspersky Security Center Linux 管理
登录到 Kaspersky Security Center Web Console 并登出
Kaspersky Security Center Web Console中的身份和访问管理器
关于身份和访问管理器
启用身份和访问管理器：方案
在 Kaspersky Security Center Web Console 中配置身份和访问管理器
在 Kaspersky Security Center Web Console 中注册 Kaspersky Industrial CyberSecurity for Networks 应用程序

- 身份和访问管理器的令牌生命周期和授权超时
- 下载和分发 IAM 证书
- 禁用身份和访问管理器

使用 NTLM 和 Kerberos 协议配置域身份验证

配置管理服务器

- 配置 Kaspersky Security Center Web Console 到管理服务器的连接
- 配置管理服务器连接事件记录
- 指定管理服务器的互联网连接设置
- 设置事件存储库中的最大事件数量
- UEFI 保护设备连接设置
- 创建管理服务器层级：添加从属管理服务器
- 查看从属管理服务器列表
- 删除管理服务器层级
- 管理服务器维护
- 配置界面
- 管理虚拟管理服务器
  - 创建虚拟管理服务器
  - 启用或禁用虚拟管理服务器
  - 为虚拟管理服务器分配管理员
  - 更改客户端设备的管理服务器
  - 删除虚拟管理服务器
- 启用账户保护以防止未经授权的修改
- 备份复制和管理服务器数据恢复
  - 创建数据备份任务
- 将管理服务器移动至其他设备
- 使用 klscmodchk 和 integrity_checker 实用程序检查模块的完整性

Kaspersky Security Center Web Console 的初始设置

- 快速启动向导（Kaspersky Security Center Web Console）
  - 步骤 1：指定互联网连接设置
  - 步骤 2：下载所需更新
  - 步骤 3：选择要保护的资产
  - 步骤 4：选择解决方案中的加密
  - 步骤 5：配置受管理应用程序的插件安装
  - 步骤 6：安装所选插件
  - 步骤 7：下载分发包并创建安装包
  - 步骤 8：配置卡巴斯基安全网络
  - 步骤 9：选择应用程序激活方法
  - 步骤 10：指定第三方更新管理设置
  - 步骤 11：创建基本的网络保护配置
  - 步骤 12：配置邮件通知
  - 步骤 13：执行网络轮询
  - 步骤 14：关闭快速启动向导
- 连接漫游设备
  - 方案：通过连接网关连接漫游设备
  - 方案：通过 DMZ 中的从属管理服务器连接漫游设备
  - 关于连接漫游设备
  - 将外部台式设备连接到管理服务器

关于漫游用户的连接配置文件
为漫游用户创建连接配置文件
关于将网络代理切换到其他管理服务器
根据网络位置创建网络代理切换规则
保护部署向导
步骤 1：开始保护部署向导
步骤 2：选择安装包
步骤 3：选择分发密钥文件或激活码的方法
步骤 4：选择网络代理版本
步骤 5：选择设备
步骤 6：指定远程安装任务设置
步骤 7：重启管理
步骤 8：安装前删除不兼容的应用程序
步骤 9：移动设备到受管理设备
步骤 10：选择访问设备的账户
步骤 11：开始安装
通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序
方案：通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序
获取 Kaspersky 应用程序插件
下载和创建卡巴斯基应用程序的安装包
更改自定义安装包数据大小的限制
下载 Kaspersky 应用程序的分发包
检查 Kaspersky Endpoint Security 是否已成功部署
创建独立安装包
查看独立安装包列表
创建自定义安装包
将安装包分发至从属管理服务器
使用远程安装任务安装应用程序
远程安装应用程序
通过活动目录组策略安装应用程序
在从属管理服务器上安装应用程序
指定 Unix 设备上的远程安装设置
启动和停止卡巴斯基应用程序
移动设备管理
替换第三方安全应用程序
发现网络设备
情景：发现网络设备
设备发现
Windows 网络轮询
IP 范围轮询
添加和修改 IP 范围
Zeroconf 轮询
域控制器轮询
身份验证和连接到域控制器
配置 Samba 域控制器
为未分配的设备配置保留规则

设备清单
添加有关新设备的信息
配置用于定义企业设备的标准
Kaspersky 应用程序：授权许可和激活
受管理应用程序的授权许可
添加授权许可密钥到管理服务器存储库
添加管理服务器授权许可密钥
部署授权许可密钥到客户端设备
自动分发授权许可密钥
查看使用中授权许可密钥的相关信息
从存储库删除授权许可密钥
撤销对最终用户授权许可协议的同意
续订卡巴斯基应用程序授权许可
使用 Kaspersky Marketplace 选择 Kaspersky 商业解决方案
配置网络保护
方案：配置网络保护
关于以设备为中心和以用户为中心的安全管理方法
策略设置和传播：以设备为中心的方法
策略设置和传播：以用户为中心的方法
网络代理策略设置
网络代理策略设置：按操作系统比较
启用和禁用网络代理的低资源消耗模式
Kaspersky Endpoint Security 策略的手动设置
配置卡巴斯基安全网络
检查受防火墙保护的网络列表
禁用网络驱动扫描
从管理服务器内存中排除软件详细信息
配置对工作站上的 Kaspersky Endpoint Security for Windows 界面的访问
在管理服务器数据库中保存重要的策略事件
Kaspersky Endpoint Security 更新组任务的手动设置
授予对"设备控制"阻止的外部设备的离线访问权限
远程删除应用程序或软件更新
任务
关于任务
关于任务范围
创建任务
手动启动任务
查看任务列表
常规任务设置
导出任务
导入任务
启动更改任务密码向导
步骤 1：指定凭证
步骤 2：选择要采取的操作
步骤 3：查看结果

- 创建“远程执行脚本”任务
  - 使用“远程执行脚本”任务在设备上远程安装应用程序
  - 配置“远程执行脚本”任务的通知和监控
  - 为“远程执行脚本”任务准备压缩文件
  - 根据清单文件创建安装包
- 管理客户端设备
  - 受管理设备设置
  - 创建管理组
  - 手动将设备添加到管理组
  - 手动将设备或者集群移动至管理组
  - 创建设备移动规则
  - 复制设备移动规则
  - 设备移动规则的条件
  - 关于集群和服务器阵列
  - 集群或服务器阵列的属性
  - 当设备显示不活动时查看和配置操作
  - 关于设备状态
  - 配置设备状态切换
  - 远程连接至客户端设备桌面
  - 通过 Windows 桌面共享连接至客户端设备
  - 设备分类
    - 从设备分类中查看设备列表
    - 创建设备分类
    - 配置设备分类
    - 从设备分类中导出设备列表
    - 在分类中从管理组中删除设备
  - 设备标签
    - 创建设备标签
    - 重命名设备标签
    - 删除设备标签
    - 查看分配了标签的设备
    - 查看分配到设备的标签
    - 手动标记设备
    - 从设备上删除分配的标签
    - 查看自动标记设备规则
    - 编辑自动标记设备规则
    - 创建自动标记设备规则
    - 为自动标记设备运行规则
    - 删除自动标记设备规则
    - 使用 klscflag 实用程序管理设备标签
- 策略和策略配置文件
  - 关于策略和策略配置文件
  - 关于“锁定”和锁定的设置
  - 策略继承和策略配置文件
    - 策略层级
    - 策略层级中的策略配置文件
    - 如何在受管理设备上实施设置

- 管理策略
  - 查看策略列表
  - 创建策略
  - 修改策略
  - 常规策略设置
  - 启用和禁用策略继承选项
  - 复制策略
  - 移动策略
  - 导出策略
  - 导入策略
  - 查看策略分发状态图
  - 删除策略
- 管理策略配置文件
  - 查看策略配置文件
  - 更改策略配置文件优先级
  - 创建策略配置文件
  - 修改策略配置文件
  - 复制策略配置文件
  - 创建策略配置文件激活规则
  - 删除策略配置文件

数据加密和保护

- 查看加密驱动器列表
- 查看加密事件列表
- 创建和查看加密报告
- 授予对处于离线模式的加密驱动器的访问权限

用户和用户角色

- 关于用于角色
- 查看用户账户和会话
- 配置对应用程序功能的访问权限。基于角色的访问控制
  - 应用程序功能的访问权限
  - 预定义用户角色
  - 分配对特定对象的访问权限
  - 向用户和安全组分配访问权限
- 添加内部用户账户
- 创建安全组
- 编辑内部用户账户
- 编辑安全组
- 为用户或安全组分配角色
- 添加用户账户到内部安全组
- 指派用户作为设备所有者
- 为所有用户配置两步验证
  - 关于两步验证
  - 为您自己的账户启用两步验证（Web Console）
  - 为您自己的账户启用两步验证（基于 MMC）
  - 对所有用户启用必需的两步验证（Web Console）
  - 为所有用户启用两步验证（基于 MMC）
  - 禁用用户账户的两步验证（Web Console）

禁用用户账户的两步验证（基于 MMC）
对所有用户禁用必需的两步验证（Web Console）
对所有用户禁用必需的两步验证（基于 MMC）
从两步验证中排除账户（云控制台）
从两步验证中排除账户（基于 MMC）
编辑安全代码颁发者的名称（Web Console）
编辑安全代码颁发者的名称（基于 MMC）
为您自己的账户配置两步验证 (Web Console)
为您自己的账户配置两步验证（基于 MMC）
生成新的 secret key
禁止新用户为自己设置两步验证
安装网络代理后将用户指定为 Linux 设备所有者
删除用户或安全组
更改用户账户的密码
创建用户角色
编辑用户角色
编辑用户角色范围
删除用户角色
关联策略配置文件到角色
传输用户角色到从属管理服务器
修改账户密码
撤销本地管理员权限
管理对象修订
回滚对象到先前修订
添加修订描述
查看并保存策略修订
对象删除
卡巴斯基安全网络 (KSN)
关于 KSN
设置对 KSN 的访问
启用和禁用 KSN 的使用
查看已接受的 KSN 声明
接受更新的 KSN 声明
检查分发点是否充当 KSN 代理服务器
情景：升级 Kaspersky Security Center 和受管理安全应用程序
更新 Kaspersky 数据库和应用程序
方案：定期更新 Kaspersky 数据库和应用程序
关于更新 Kaspersky 数据库、软件模块和应用程序
创建"将更新下载至管理服务器存储库"任务
验证已下载的更新
创建"将更新下载至分发点存储库"任务
启用和禁用 Kaspersky Security Center 组件的自动更新和补丁
自动安装 Kaspersky Endpoint Security for Windows 的更新
批准和拒绝软件更新
更新管理服务器
启用和禁用离线模式更新下载
更新离线设备上的 Kaspersky 数据库和软件模块

备份和恢复 Web 插件
分发点和连接网关的调整
分发点的标准配置：单一办公室
分发点的标准配置：多个小远程办公室
关于分配分发点
自动分配分发点
手动分配分发点
修改管理组的分发点列表
强制同步
启用推送服务器
在客户端设备上管理第三方应用程序
安装第三方软件更新
方案：更新第三方软件
安装第三方软件更新
创建“查找漏洞和所需更新”任务
“查找漏洞和所需更新”任务设置
创建“安装所需更新并修复漏洞”任务
添加更新安装规则
创建“安装 Windows Update 更新”任务
查看有关可用的第三方软件更新的信息
将可用软件更新列表导出到文件
批准和拒绝第三方软件更新
创建“执行 Windows Update 同步”任务
自动更新第三方应用程序
修复第三方软件漏洞
方案：查找和修复第三方软件中的漏洞
关于查找和修复软件漏洞
修复第三方软件漏洞
创建“修复漏洞”任务
创建“安装所需更新并修复漏洞”任务
添加更新安装规则
为第三方软件中的漏洞选择用户修补程序
查看有关在所有受管理设备上检测到的软件漏洞的信息
查看有关在选定受管理设备上检测到的软件漏洞的信息
查看受管理设备上的漏洞统计信息
将软件漏洞列表导出到文件
忽略软件漏洞
管理客户端设备上运行的应用程序
使用应用程序控制来管理可执行文件
应用程序控制模式和类别
获取并查看客户端设备上存储的可执行文件列表
创建含有手动添加内容的应用程序类别
创建包括选定设备中的可执行文件的应用程序类别
创建包括选定文件夹中的可执行文件的应用程序类别
查看应用程序类别列表

添加事件相关的可执行文件到应用程序类别
在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”
获取并查看客户端设备上安装的应用程序列表
从 Kaspersky 数据库创建第三方应用程序的安装包
从 Kaspersky 数据库查看和修改第三方应用程序安装包的设置
从 Kaspersky 数据库设置第三方应用程序的安装包
应用程序标签
创建应用程序标签
重命名应用程序标签
分配标签到应用程序
从应用程序上删除分配的标签
删除应用程序标签
监控和报告
方案：监控和报告
关于监控和报告的类型
仪表板和小部件
使用仪表板
添加小部件到仪表板
从仪表板隐藏小部件
移动小部件到仪表板
更改小部件尺寸或样子
更改小部件设置
关于仅仪表板模式
配置仅仪表板模式
报告
使用报告
创建报告模板
查看和编辑报告模板属性
导出报告到文件
生成和浏览报告
创建报告发送任务
删除报告模板
事件和事件分类
关于 Kaspersky Security Center 事件
使用事件分类
创建事件分类
编辑事件分类
查看事件分类列表
导出事件分类
导入事件分类
查看事件详情
导出事件到文件
从事件查看对象历史
删除事件
删除事件分类
设置事件存储期限

Kaspersky Security Center 组件事件
事件类型描述的数据结构
管理服务器事件
管理服务器严重事件
管理服务器功能失败事件
管理服务器警告事件
管理服务器信息事件
网络代理事件
网络代理功能失败事件
网络代理警告事件
网络代理信息事件
iOS MDM 服务器事件
iOS MDM 服务器功能失败事件
iOS MDM 服务器警告事件
iOS MDM 服务器信息事件
阻止频繁事件
关于阻止频繁事件
管理频繁事件阻止
移除对频繁事件的阻止
从 Kaspersky Security for Microsoft Exchange Server 接收事件
通知和设备状态
使用通知
查看屏幕通知
关于设备状态
配置设备状态切换
配置通知传送
通过运行可执行文件显示的事件通知
卡巴斯基公告
关于 Kaspersky 公告
指定 Kaspersky 公告设置
禁用 Kaspersky 公告
查看有关威胁检测的信息
Cloud Discovery
使用小部件启用 Cloud Discovery
将 Cloud Discovery 小部件添加到仪表板
查看有关云服务使用的信息
云服务的风险级别
阻止对不需要的云服务进行的访问
Kaspersky Security Center Web Console 活动日志
Kaspersky Security Center 与其他解决方案之间的集成
建立后台连接
导出事件到 SIEM 系统
配置导出事件到 SIEM 系统
在您开始之前
关于 Kaspersky Security Center 中的事件
关于事件导出
关于配置 SIEM 系统中的事件导出

标记要以 Syslog 格式导出到 SIEM 系统的事件
关于标记要以 Syslog 格式导出到 SIEM 系统的事件
标记要以 Syslog 格式导出的 Kaspersky 应用程序事件
标记要以 Syslog 格式导出的常规事件
关于使用 CEF 和 LEEF 格式导出事件
将事件转换为 CEF 或 LEEF 格式
关于使用 Syslog 格式导出事件
配置 Kaspersky Security Center 以导出事件到 SIEM 系统
直接从数据库导出事件
使用 klsql2 实用工具执行 SQL 查询
klsql2 实用工具中的 SQL 查询例子
查看 Kaspersky Security Center 数据库名称
查看导出结果
在云环境中使用 Kaspersky Security Center Web Console
Kaspersky Security Center Web Console 中的云环境配置
步骤 1：检查需要的插件和安装包
步骤 2：授权应用程序
步骤 3：选择云环境和授权
步骤 4：云段轮询，配置与云的同步并选择后续操作
步骤 5：选择一个应用程序来为其创建策略和任务
步骤 6：为 Kaspersky Security Center 配置卡巴斯基安全网络
步骤 7：创建保护的初始配置
通过 Kaspersky Security Center Web Console 进行云段轮询
为云段轮询添加连接
为云段轮询删除连接
通过 Kaspersky Security Center Web Console 配置轮询计划
通过 Kaspersky Security Center Web Console 查看云段轮询的结果
通过 Kaspersky Security Center Web Console 查看云设备的属性
与云同步：配置移动规则
将应用程序远程安装到 Azure 虚拟机
使用云 DBMS 创建管理服务器数据备份任务
客户端设备的远程诊断
打开远程诊断窗口
启用和禁用应用程序跟踪
下载应用程序的跟踪文件
删除跟踪文件
下载应用程序设置
下载事件日志
启动、停止和重新启动应用程序
运行 Kaspersky Security Center 网络代理的远程诊断并下载结果
在客户端设备上运行应用程序
为应用程序创建内存转储文件
在基于 Linux 的客户端设备上运行远程诊断
从隔离区和备份下载和删除文件
从隔离区和备份区中下载文件
更改 Kaspersky Security Center Web Console 界面的语言
API 参考指南

服务提供商最佳实践
计划 Kaspersky Security Center 部署
提供到管理服务器的互联网访问
Kaspersky Security Center 标准配置
关于分发点
管理服务器层级
虚拟管理服务器
使用 Kaspersky Endpoint Security for Android 管理移动设备
部署和初始化设置
管理服务器安装建议
在失败转移集群上为管理服务器服务创建账户
选择 DBMS
指定管理服务器地址
在客户端组织网络中配置保护
Kaspersky Endpoint Security 策略的手动设置
在高级威胁防护区域配置策略
在关键威胁防护部分配置策略
在常规设置部分配置策略
在事件配置区域配置策略
Kaspersky Endpoint Security 更新组任务的手动设置
Kaspersky Endpoint Security 设备扫描组任务的手动设置
计划“查找漏洞和所需更新”任务
更新安装和漏洞修复组任务的手动设置
建立管理组结构和分配分发点
标准 MSP 客户端配置：单一办公室
标准 MSP 客户端配置：多个小远程办公室
策略层级，使用策略配置文件
策略层级
策略配置文件
任务
设备移动规则
软件分类
关于多租户应用程序
管理服务器设置的备份和恢复
管理服务器设备不可操作
管理服务器设置或数据库被损坏
部署网络代理和安全应用程序
初始化部署
配置安装程序
安装包
MSI 属性和转换文件
使用应用程序远程安装的第三方工具部署
Kaspersky Security Center 中远程安装任务的常规信息
使用 Microsoft Windows 组策略部署
通过 Kaspersky Security Center 远程安装任务的强制部署
运行 Kaspersky Security Center 创建的独立包
手动安装应用程序的选项

- 在安装有网络代理的设备上远程安装应用程序
- 在远程安装任务中管理设备重启
- 反病毒应用程序安装包上的数据库更新
- 删除不兼容的第三方安全应用程序
- 使用命令提示符删除受密码保护的网络代理
- 在 Kaspersky Security Center 中使用工具远程安装应用程序以便在受管理设备上运行相关可执行文件
- 监控部署
- 配置安装程序
  - 常规信息
  - 在静默模式下安装(带有响应文件)
  - 在静默模式下安装网络代理（没有响应文件）
  - 通过 setup.exe 的部分安装配置
  - 管理服务器安装参数
  - 网络代理安装设置
- 虚拟基础架构
  - 降低虚拟机负载的窍门
  - 对动态虚拟机的支持
  - 对虚拟机复制的支持
- 对网络代理设备文件系统回滚的支持
- 关于漫游用户的连接配置文件
- 部署移动设备管理功能
  - 将 KES 设备连接至管理服务器
    - 直接连接设备到管理服务器
    - 连接 KES 设备到 Kerberos constrained delegation (KCD) 服务器的方案
    - 使用 Firebase Cloud Messaging
  - 与公共密钥基础架构整合
  - Kaspersky Security Center Web Server
- 其他日常工作
  - 在管理控制台中监控信号灯和记录的事件
  - 远程访问受管理设备
    - 使用"不要断开与管理服务器的连接"选项提供受管理设备和管理服务器之间的持续连接
    - 关于检查设备和管理服务器之间的连接时间
    - 关于强制同步
    - 关于隧道
- 层级指南
  - 关于本指南
  - Kaspersky Security Center 的限制信息
  - 管理服务器计算
    - 管理服务器的硬件资源计算
      - DBMS 和管理服务器的硬件需求
      - 数据库空间计算
      - 磁盘空间计算（使用或不使用漏洞和补丁管理功能）
    - 计算管理服务器的数量和配置
    - 有关将动态虚拟机连接到 Kaspersky Security Center 的建议

分发点和连接网关的计算
分发点需求
计算分发点的数量和配置
连接网关数量计算
任务和策略事件信息的记录
特别考虑和特定任务的优化设置
设备发现频率
管理服务器数据备份任务和管理服务器维护任务
更新 Kaspersky Endpoint Security 的组任务
清查任务
管理服务器和受保护设备间的网络负载详情
不同方案下的流量消耗
24 小时平均流量使用
联系技术支持
如果获得技术支持
通过 Kaspersky CompanyAccount 获得技术支持
获取管理服务器的转储文件
有关应用程序的信息来源
词汇表
Amazon EC2 实例
Amazon 系统映像 (AMI)
AWS Application Program Interface (AWS API)
AWS IAM 访问密钥
AWS 管理控制台
Cloud Discovery
HTTPS
IAM 用户
IAM 角色
iOS MDM 服务器
iOS MDM 设备
iOS MDM 配置文件
JavaScript
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center Web Server
Kaspersky Security Center 操作员
Kaspersky Security Center 的升级
Kaspersky Security Center 管理员
Kaspersky 更新服务器
KES 设备
MITM 攻击
Provisioning 配置文件
SSL
UEFI 保护设备
Windows Server 更新服务 （WSUS）
不兼容应用程序
事件严重级别
事件存储库

云环境
任务
任务设置
保护状态
共享证书
内部用户
分发点
卡巴斯基安全网络 （KSN）
卡巴斯基私有安全网络 (KPSN)
反病毒保护服务提供商
反病毒数据库
受管理设备
可用更新
备份文件夹
安装包
客户端管理员
密钥文件
广播域
应用程序商店
强制安装
强化指南
归属管理服务器
手动安装
授权的应用程序组
授权许可期限
更新
服务提供商管理员
本地任务
本地安装
活动授权许可
漏洞
特定设备的任务
病毒活动性阀值
病毒爆发
直接应用程序管理
移动设备服务器
程序设置
策略
管理员工作站
管理员权限
管理控制台
管理插件
管理服务器
管理服务器客户端（客户端设备）
管理服务器数据备份
管理服务器证书
管理组

组任务
网络代理
网络位置识别 (NLA)
网络保护状态
网络反病毒保护
虚拟管理服务器
补丁重要级别
设备所有者
身份和访问管理(IAM)
身份验证代理
轻量级 Nagent（LWNGT）
还原
还原管理服务器数据
远程安装
连接网关
配置文件
隔离区域 （DMZ）
集中式应用程序管理
额外（或备用）授权许可密钥
有关第三方代码的信息
商标声明
已知问题

Kaspersky Security Center 15.1 帮助

	新闻 了解最新应用程序版本中的新增内容。		**配置网络保护** 管理组织的安全。
	硬件和软件要求 检查支持什么操作系统和应用程序版本。		**Kaspersky 应用程序。更新数据库和软件模块** 维持保护系统的可靠性。
	部署和初始化设置 计划资源使用、安装管理服务器、安装网络代理和安全应用程序到客户端设备，以及整理设备到管理组。		**监控和报告** 查看您的基础架构、保护状态和统计信息。使用 Cloud Discovery 管理对云服务的访问。
	发现网络设备 发现您组织网络中的现有设备和新设备。		**替换第三方安全应用程序** 学习卸载不兼容应用程序的方法。
	Kaspersky 应用程序。集中部署 部署 Kaspersky 应用程序。		**分发点和连接网关的调整** 配置分发点。
	从先前版本升级 Kaspersky Security Center 从先前版本升级 Kaspersky Security Center 15.1。		**服务提供商的最佳实践（仅限在线帮助）** 学习如何部署、配置和使用应用程序的建议，以及解决应用程序操作中的典型问题的方法。
	Kaspersky 应用程序。授权许可和激活 几步激活 Kaspersky 应用程序。		**层级指南（仅限在线帮助）** 要在不同的条件下优化性能，需要考虑网络设备数量、网络拓扑和您需要的 Kaspersky Security Center 功能集。
	导出事件到 SIEM 系统 配置将事件导出到 SIEM 系统以进行分析。		**漏洞和补丁管理** 查找和修复第三方软件中的漏洞
	使用云环境 在云环境中部署 Kaspersky Security Center：Amazon Web Services™、Microsoft Azure™ 和 Google™ Cloud Platform。		**Frequently Asked Questions（仅限英语）** 查找有关如何解决常见问题的说明。
	Kaspersky Endpoint Security for Business 快速启动指南 开始使用 Kaspersky Endpoint Security for Business：安装和配置此解决方案。您还可以查看 Kaspersky Security Center 的功能比较，以选择最合适的网络安全管理方式。		

新闻

Kaspersky Security Center 15.1 更新 2

Kaspersky Security Center 15.1 更新 2 重点修复用户和测试团队报告的问题：

- 现在可以通过导入 TXT 文件指定基于 Linux 的受管理设备范围来正确执行任务。
- 现在，当使用在虚拟管理服务器上创建的远程安装任务安装卡巴斯基应用程序时，安装包仅通过该虚拟管理服务器管理的分发点使用操作系统工具传输到受管理设备。
- 解决了二级管理服务器在二级服务器的证书轮换后无法重新连接到主管理服务器的问题。
- 解决了影响 TLS 连接的问题。
- 解决了用户登录时导致多个“无效类型转换”错误的问题。
- Kaspersky Security Center 现在可以正确通过电子邮件发送事件通知。
- 修复了将*Kaspersky Security Center 从 14.2 版升级*到 15.1 版时将更新文件夹添加到备份副本的问题。
- 卡巴斯基应用程序授权许可的到期日期现在可以在 Kaspersky Security Center Web Console 中正确显示。
- **定位移动设备**和**获取设备位置历史记录**命令现在可以正常工作。
- 修复了包含移动证书的安装包在下载 1 小时后或 24 小时未使用后未被自动删除的问题。
- 现在，由特定标签激活的活动策略配置文件可以正确应用于描述中包含该标签的设备。
- 修复了导致 PostgreSQL 数据库错误消息出现在事件日志中的问题。
- 从两步验证中排除账户现在可正常工作。
- 修复了在启用Identity and Access Manager的情况下使用域身份验证时无法正常退出Kaspersky Security Center Web Console的问题。
- 现在，更新管理 Web 插件时，单击所需插件版本的链接即可开始下载。
- 修复了报告中的问题：
  - 当您为威胁和更新威胁报告创建传递任务，并将任务计划设置为**每月**时，报告中会正确填充数据。
  - 在*应用程序组件状态报告*模板中，按组件名称过滤已正确应用。
  - 现在可以过滤*保护部署报告*以仅显示未安装卡巴斯基应用程序的设备。这有助于直观地了解要安装应用程序的设备数量。
- 无论您是否在常规功能：基本功能**区域中拥有Cloud Discovery执行**权限，Cloud Discovery**小部件**都会正确显示。
- 提高了存储的过程和数据库操作的性能。
- 修复了与不存在的用户链接的过期证书导致所有用户的续费过程停止的问题。

- 解决了影响正确处理证书的问题。
- 将Kaspersky Security Center 从 14.2 版升级到 15.1 版后，现在可以正常从管理控制台中的从属虚拟管理服务器下载独立安装包。
- 修复了 Kaspersky Security Center Web Console 中的一个问题，即，当在卡巴斯基应用程序策略中启用卡巴斯基安全网络 (KSN)时，以下应用程序无法接受 KSN 声明： Kaspersky Endpoint Security for Linux 版本 12.2 或更早版本、Kaspersky Industrial CyberSecurity for Linux Nodes 版本 1.5 或更早版本、Kaspersky Security for Virtualization Light Agent版本 6.0 和 6.1、 Kaspersky Embedded Systems Security for Linux 版本 3.3 和 Kaspersky Security for Windows Server 版本 11.0.1.897。
- 修复了策略配置文件未应用于 Active Directory 域组中包含的基于 Linux 的设备的问题。
- 修复了从多个二级从属管理服务器尝试连接到主管理服务器时出现的问题。

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 具有多个新功能和改进。

- Cloud Discovery。这项新功能可让您监控尝试运行 Windows 的受管理设备上云服务的使用情况，并阻止对您认为不需要的云服务进行的访问。此功能仅在 Kaspersky Security Center Web Console 中提供。
- 域控制器轮询现在允许您通过基于 Linux 的分发点轮询 Samba 域控制器。进行了额外的改进来支持大型域的轮询。
- 增强了远程诊断基于 Linux 的受管理设备。
- 扩展的 macOS 设备硬件清单。macOS 设备上的网络代理会将 MAC 地址和设备序列号发送到管理服务器。
- 您现在可以检查与 SIEM 系统的连接。
- 内部用户的最长密码长度增加到 256 个字符。
- 当您从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux 时，您现在可以通过从备份副本恢复管理服务器的证书和私钥，将受管设备切换至 Kaspersky Security Center Linux 的管理之下。
- 当您运行清理工具或 klmover 实用程序来删除受密码保护的网络代理时，您会被提示输入卸载密码。
- 从 Kaspersky Security for Windows Server 升级到 Kaspersky Endpoint Security for Windows 不再需要重启目标设备。
- 在 Linux 客户端设备上安装网络代理期间或之后，可将用户指定为设备所有者。
- 现在，当您通过自定义脚本在受管理设备上安装软件时，可以收到有关远程安装的报告。
- 当您在受管理设备上执行多个自定义脚本时，可以为每个脚本设置优先级来定义执行顺序。这些脚本将按照优先级从高到低的顺序执行。
- 扩展的策略审计。现在可以查看策略修订的内容以及保存策略修订到文件。目前，这些功能仅适用于管理服务器策略和网络代理策略。

- 用户体验改进包括：
  - 通过固定 Kaspersky Security Center Web Console 的各个部分来实现主菜单个性化，以便从“**固定的**”部分快速访问。
  - 优化表格工作。现在，每个表格的默认视图会包含最常用的列。此外，您现在可以选择当前页面或整个表格中的所有项目，并对整个表格中的项目进行排序。
  - 改进的报告传送配置。您现在可以指定最多 20 个电子邮件地址用于接收报告，还可以指定报告传送时间表。
- 您可以从基于 Linux 的受管理设备上的账户撤销本地管理员权限。这为您提供了对用户账户的额外控制。例如，您可以在一次性分配完成后撤销本地管理员权限。
- 您可以更改基于 Linux 的受管理设备上的本地账户密码，例如当用户忘记本地账户密码或要执行计划的密码更改时。
- 在“**用户证书管理**”子部分中，您可以指定要安装的根证书。例如，这些证书可用于验证网站或网络服务器的真实性。
- 网络攻击报告现在包括实施攻击的设备的 MAC 地址和端口。
- 新增一个选项，强制内部用户在下次尝试登录 Kaspersky Security Center Web Console 时更改密码。
- 当您以 CEF 或 LEEF 格式将事件导出到 SIEM 系统时，不再检查商业授权许可。
- 当您从一个卡巴斯基安全应用程序迁移到另一个应用程序，且当前应用程序受到密码保护时，您现在可以在远程安装任务中指定卸载密码。
- Exchange ActiveSync 不再受支持。

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 具有多个新功能和改进。

- 新的强化指南已发布。我们强烈建议您仔细阅读指南并按照安全建议配置 Kaspersky Security Center 和您的网络基础设施。

  另外，请安装 Kaspersky Security Center 的最新更新。此更新包括用户账户两步验证和其他改进等基础设施保护功能。
- 现在自动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。
- 虚拟管理服务器上的用户权限可随时独立于主管理服务器进行配置。此外，您可以为主服务器用户分配管理虚拟服务器的权限。
- Kaspersky Security Center 现在支持使用以下 DBMS：
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x（所有版本）

  - Postgres Pro 14.x（所有版本）
  - MariaDB 10.1, 10.4, 10.5
- 您可以使用 Kaspersky Security Center Web Console 将策略和任务导出到一个文件，然后将策略和任务导入到 Kaspersky Security Center Windows 或 Kaspersky Security Center Linux。
- "**不使用代理服务器**"选项已从以下任务中删除：
  - *将更新下载至管理服务器存储库*
  - *将更新下载至分发点存储库*
- 要在云环境中保护客户端设备，您可以部署 Kaspersky Endpoint Security for Windows 而不是 Kaspersky Security for Windows Server。此功能现在 Kaspersky Endpoint Security 12.0 for Windows 版本发布后可用。
- 使用加密密钥现在受**常规功能**的访问权限限制：**加密密钥管理**功能区域。如果 Kaspersky Security Center 用户拥有**读取**权限，他们现在可以导出加密密钥；如果拥有**写入**权限，他们可以导入加密密钥。

Kaspersky Security Center 14

Kaspersky Security Center 14 具有多个新功能和改进。

- 您可以在隔离的网络中安装更新和修复第三方软件（不包括 Microsoft 软件）的漏洞。此类网络包括管理服务器和没有接入互联网的受管理设备。要修复此类网络中的漏洞，您需要使用具有互联网访问权限的管理服务器下载所需更新，然后将补丁传输到隔离的管理服务器。
- 对于 macOS 设备，已添加漫游用户的连接配置文件。使用连接配置文件，您可以为 macOS 设备上的网络代理配置规则，以连接到相同或不同的管理服务器，具体取决于设备位置。
- 网络代理现在可以安装在运行 Microsoft Windows 10 IoT Enterprise 的设备上。
- 在"**威胁报告**"中，现在可以筛选威胁列表，以便仅查看 Cloud Sandbox 检测到的威胁。
- Kaspersky Security Center 现在支持将 Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 作为受管理应用程序。

Kaspersky Security Center Web Console 具有多个新功能和改进。

- 您可以为不管理网络但希望在 Kaspersky Security Center 中查看网络保护统计信息的员工（例如高层管理人员）配置"仅仪表板模式"。当用户启用此模式后，只会显示带有一组预定义小部件的仪表板。因此，用户可以监视小部件中指定的统计信息，例如，所有受管理设备的保护状态、最近检测到的威胁数量或网络中最常见的威胁列表。
- Kaspersky Security Center Web Console 现在支持 Kaspersky Security for iOS 作为安全应用程序。
- 在任务属性中，您可以指定是否要将任务应用于子组和从属管理服务器（包括虚拟管理服务器）。
- Kaspersky Security Center 现在支持将 Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 作为受管理应用程序。

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 具有多个新功能和改进。

- 您现在可以在以下新操作系统上安装管理服务器、管理控制台、Kaspersky Security Center 13.2 Web Console 和网络代理（请参阅软件要求以了解详细信息）：
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2（2021 年 10 月更新）
  - Windows Server 2022
- 您可以使用 MySQL 8.0 作为数据库。
- 您可以将 Kaspersky Security Center 部署在 Kaspersky Security Center 故障转移集群上以提供 Kaspersky Security Center 的高可用性。
- Kaspersky Security Center 现在可以使用 IPv6 地址和 IPv4 地址。管理服务器可以轮询具有 IPv6 地址的设备的网络。

Kaspersky Security Center 13.2 Web Console 具有多个新功能和改进。

- 您现在可以通过 Kaspersky Security Center 13.2 Web Console 管理运行安卓的移动设备。
- Kaspersky Marketplace 以新菜单板块的形式提供：您可以通过 Kaspersky Security Center 13.2 Web Console 搜索卡巴斯基应用程序。
- Kaspersky Security Center 现在支持以下 Kaspersky 应用程序：
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 具有多个新功能和改进。

- 改进了与 SIEM 系统的集成。现在可以通过加密通道 (TLS) 将事件导出到 SIEM 系统。该功能可用于 Kaspersky Security Center Web Console 和基于 MMC 的管理控制台。
- 现在可以获取分发包形式的管理服务器补丁，分发包可用于将来更新到更高版本。
- Kaspersky Security Center 13.1 Web Console 增加了一个针对 Kaspersky Endpoint Detection and Response Optimum 的新区域**"警报"**。还增加了几个新的小组件，用于处理 Kaspersky Endpoint Detection and Response Optimum 检测到的威胁。
- 在 Kaspersky Security Center 13.1 Web Console 中，现在可以接收关于卡巴斯基应用程序授权许可到期的通知。
- 缩短了 Kaspersky Security Center 13.1 Web Console 的响应时间。

Kaspersky Security Center 13

Kaspersky Security Center 13 Web Console 增加了以下功能：

- 实施了两步验证。您可以启用两步验证，以降低 Kaspersky Security Center 13 Web Console 被未经授权访问的风险。
- 通过使用 NTLM 和 Kerberos 协议（单点登录）实施了域身份验证。单点登录功能允许 Windows 用户在 Kaspersky Security Center 13 Web Console 中启用安全身份验证，而无需在公司网络上重新输入密码。
- 您现在可以配置插件来使用 Kaspersky Managed Detection and Response。您可以使用此集成来查看事件和管理工作站。
- 您现在可以在管理服务器的安装向导中指定 Kaspersky Security Center 13 Web Console 的设置。
- 显示有关新版本更新和补丁的通知。您可以立即安装更新，也可以在以后随时安装。您现在可以通过 Kaspersky Security Center 13 Web Console 为管理服务器安装补丁。
- 处理表时，现在可以指定列的顺序和宽度，对数据进行排序和指定页面大小。
- 您现在可以通过单击报告名称来打开任何报告。
- Kaspersky Security Center 13 Web Console 现在提供韩语版本。
- “**监控和报告**”菜单新增了一个区域：Kaspersky 公告。该区域提供与您的 Kaspersky Security Center 版本和受管理设备上安装的受管理应用程序相关的信息，让您了解最新动态。Kaspersky Security Center 会定期删除过时的公告并添加新信息来更新该区域中的信息。但是，您可以根据需要禁用 Kaspersky 公告。
- 实施了用户账户设置更改后的附加身份验证。您可以启用对用户账户的保护，防止其遭未经授权的修改。如果启用此选项，修改用户账户设置需要具有修改权限的用户的授权。

Kaspersky Security Center 13 增加了以下功能：

- 实施了两步验证。您可以启用两步验证，以降低管理控制台被未经授权访问的风险。如果启用此选项，修改用户账户设置需要具有修改权限的用户的授权。现在可以为 KES 设备启用或禁用两步验证。
- 您可以通过 HTTP 将消息发送到管理服务器。现在已提供用于使用管理服务器 OpenAPI 的参考指南和 Python 库。
- 您可以颁发备用证书以在 iOS MDM 配置文件中使用，以确保在 iOS MDM 服务器证书到期后无缝切换受管理 iOS 设备。
- 多租户应用程序文件夹不再显示在管理控制台中。

关于 Kaspersky Security Center

本部分介绍 Kaspersky Security Center 的用途和主要功能和组件、以及如何购买 Kaspersky Security Center。

Online Help 中提供的信息可能与随应用程序一起出货的文档中的信息不同；此种情况下，Online Help 为是最新的。您可以通过点击应用程序界面的链接转到 Online Help，或者通过点击文档中 Online Help 的链接。Online Help 可以自动更新。如有必要，可以切换在线帮助和离线帮助。

Kaspersky Security Center 设计用于在组织网络中集中执行基本的管理和维护任务。该程序为管理员提供有关组织网络安全级别的详细信息，允许管理员使用 Kaspersky 程序配置保护系统所有的组件。

Kaspersky Security Center 是一款面向企业网络管理员和各种组织中负责设备保护的员工的应用程序。

使用 Kaspersky Security Center 您可以做以下事情：

- 创建一台管理服务器层级结构来管理组织网络以及远程办公室网络或客户组织网络。
  *客户端组织*是指由服务提供商确保反病毒保护的一种组机构。
- 创建一个管理组层级结构以整体的形式管理一组选定的客户端设备。
- 管理基于 Kaspersky 程序构建的反病毒保护系统。
- 创建操作系统镜像，并通过网络将其部署在客户端设备上，也可以执行远程安装 Kaspersky 和其他软件供应商的应用程序。
- 远程管理安装在客户端设备上的 Kaspersky 或其他厂商的程序。安装更新，查找和修复漏洞。
- 将 Kaspersky 应用程序的授权许可密钥集中部署到客户端设备、监控其使用情况，以及续订授权许可。
- 接收有关程序和设备运行的统计信息和报告。
- 接收有关 Kaspersky 程序操作中严重事件的通知。
- 管理移动设备。
- 管理保存在设备硬盘和可移动驱动器上的信息的加密处理，以及用户对加密数据的访问。
- 创建已连接至组织网络的硬件清查列表。
- 集中管理被安全应用程序移动到隔离区或备份区中的文件，以及安全应用程序已经推迟处理的文件。

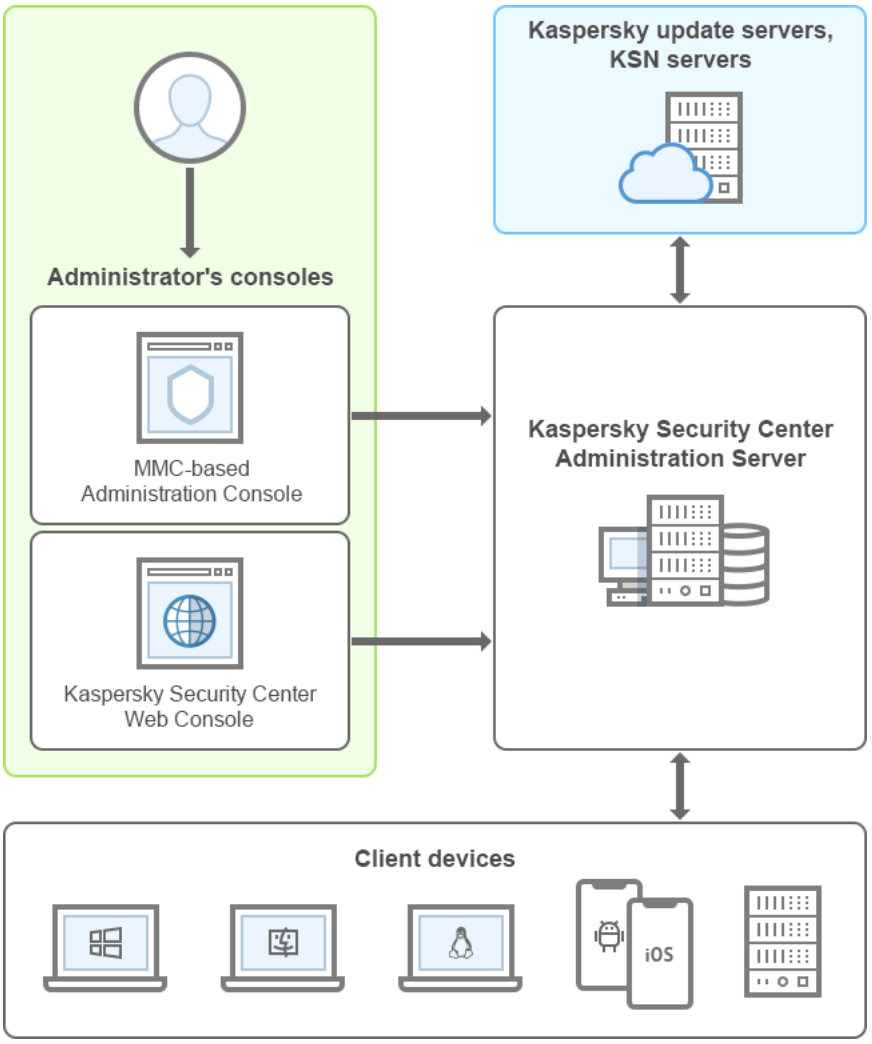
您可以通过 Kaspersky（例如，https://www.kaspersky.com.cn）或其合作伙伴公司购买 Kaspersky Security Center。

如果通过 Kaspersky 购买 Kaspersky Security Center，您可以从我们的网站复制应用程序。支付得到处理后，程序激活所需的信息会通过邮件发送给您。

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）以及 KSN 功能。

架构

该部分提供了对 Kaspersky Security Center 组件和其交互的描述。



Kaspersky Security Center 架构

Kaspersky Security Center 含有以下主要部件：

- *管理控制台*（简称*控制台*）。提供管理服务器和网络代理的管理服务用户界面。管理控制台作为 Microsoft Management Console (MMC) 的一个管理单元进行实施。使用管理控制台可以通过互联网远程连接到管理服务器。
- *Kaspersky Security Center Web Console*。提供 Web 界面以创建和维护由 Kaspersky Security Center 管理的客户端组织网络的保护系统。
- *Kaspersky Security Center 管理服务器*（也称为"*服务器*"）。集中管理组织网络中所安装应用程序的信息存储，并包含如何管理这些应用程序的信息。
- *Kaspersky 更新服务器*。Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

- *KSN 服务器*。包含 Kaspersky 数据库的服务器，该数据库中包含持续更新的文件、网络资源和软件信誉信息。卡巴斯基安全网络确保在遇到新型威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的性能并降低误报的可能性。

- *客户端设备*。受 Kaspersky Security Center 保护的客户公司设备。每台需要保护的设备都必须安装一个 Kaspersky 安全应用程序。

硬件和软件要求

- 管理服务器要求
- Web Console 要求
- 移动服务器要求
- 管理控制台要求
- 网络代理要求

管理服务器要求

最小硬件条件：

- CPU：运行频率为 1 GHz 或更高。64 位操作系统，CPU 最低频率 1.4 GHz。
- RAM：4 GB。
- 可用磁盘空间：10 GB。使用"漏洞和补丁管理"时，必须有至少 100 GB 的空闲磁盘空间。

对于云环境中的部署，管理服务器和数据库服务器的要求与物理管理服务器的要求相同（取决于要管理的设备数量）。

软件要求：

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

支持以下操作系统：

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 位
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (安装选项) (LTSB) 64 位
- Windows Server 2019 Standard/Datacenter/Core 64 位
- Windows Server 2022 Standard/Datacenter/Core 64 位

- Windows Server 2025 Standard/Datacenter/Core 64 位
- Windows Storage Server 2019 64 位

支持以下虚拟平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 64 位
- Microsoft Hyper-V Server 2022 64 位
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

支持以下数据库服务器（可以安装在其他设备上）：

- Microsoft SQL Server 2016（所有版本）64 位
- Microsoft SQL Server 2017 (所有版本) on Windows/Linux 64 位
- 适用于 Windows/Linux 64 位的 Microsoft SQL Server 2019（所有版本）（需要附加操作）
- Microsoft SQL Server 2022 (所有版本) on Windows/Linux 64 位
- MySQL 5.7 Community 32 位/64 位
- MySQL Standard Edition 8.0（版本 8.0.20 及更高版本）32 位/64 位
- MySQL Enterprise Edition 8.0（版本 8.0.20 及更高版本）32 位/64 位
- MariaDB 10.5（内部版本 10.5.27 及更高版本）32 位/64 位
- 搭载 InnoDB 存储引擎的 MariaDB Galera Cluster 10.3 32 位/64 位
- PostgreSQL 13.x 64 位
- PostgreSQL 14.x 64 bit
- PostgreSQL 15.x 64 位
- Postgres Pro 13.x Windows/Linux 64 位
- Postgres Pro 14.x Windows/Linux 64 位

有关详细信息和限制，请参阅以下主题：选择 DBMS。

SIEM 和其他信息管理系统：

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

Web Console 要求

Kaspersky Security Center Web Console 服务器

最小硬件条件：

- CPU：4 核，工作频率 2.5 GHz
- RAM：8 GB
- 可用磁盘空间：40 GB

管理服务器证书的最低要求：

- 证书签名算法 SHA-2
- 最小密钥长度 2048

如果需要重新颁发证书，请参阅Kaspersky Security Center 知识库。

Kaspersky Security Center Web Console 服务器支持的操作系统

操作系统。Microsoft Windows（仅 64 位版本）	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core (安装选项) (LTSB) Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019
虚拟化平台	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

客户端设备

对于客户端，Kaspersky Security Center Web Console 的使用仅需要一个浏览器。

最小屏幕分辨率为 1366x768 像素。

设备的硬件和软件需求和 Kaspersky Security Center Web Console 所使用的浏览器的需求是相同的。

浏览器：

- Google Chrome 128.0.6613.120 或更高版本
- Microsoft Edge 128.0.2739.67 或更高版本
- macOS 系统的 Safari 17.6
- “Yandex” 浏览器 24.7.3.1081 或更高版本
- Mozilla Firefox 扩展支持版本 115.14.0 或更高版本

移动服务器要求

iOS 移动设备管理 （iOS MDM）服务器

硬件要求：

- CPU：运行频率为 1 GHz 或更高。64 位操作系统，CPU 最低频率 1.4 GHz。
- RAM：2 GB。
- 可用磁盘空间：2 GB。

软件需求：Microsoft Windows（支持的 Windows 版本由管理服务器需求定义）。

管理控制台要求

硬件要求：

- CPU：运行频率为 1 GHz 或更高。64 位操作系统，CPU 最低频率 1.4 GHz。
- RAM：512 MB。
- 可用磁盘空间：1 GB。

软件要求：

- Microsoft Windows 操作系统（支持的操作系统版本由管理服务器的要求决定）：
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64 位
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) 64 位
  - Windows Server 2019 Standard/Datacenter 64 位
  - Windows Server 2022 Standard/Datacenter 64 位

    - Windows Server 2025 Standard/Datacenter/Core 64 位
    - Windows Storage Server 2019 64 位
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 运行于：
    - Microsoft Windows Server 2012 R2
    - Microsoft Windows Server 2016
    - Microsoft Windows Server 2019
    - Microsoft Windows Storage Server 2019
- 在 Microsoft Windows Server 2022 上运行的 Microsoft Edge

网络代理要求

最小硬件条件：

- CPU：运行频率为 1 GHz 或更高。64 位操作系统，CPU 最低频率 1.4 GHz。
- RAM：512 MB。
- 可用磁盘空间：1 GB。

基于 Linux 的设备的软件要求：必须安装 Perl 语言解释器 5.10 或更高版本。

操作系统。Microsoft Windows	Windows Embedded POSReady 2009 with latest Service Pack 32 位 Windows Embedded 7 Standard with Service Pack 1 32 位/64 位 Windows Embedded 8.1 工业专业版 32 位/64 位 Windows 10 Enterprise 2015 LTSB 32 位 / 64 位 Windows 10 Enterprise 2016 LTSB 32 位 / 64 位 Windows 10 IoT Enterprise 2015 LTSB 32 位 / 64 位 Windows 10 IoT Enterprise 2016 LTSB 32 位 / 64 位 Windows 10 Enterprise 2019 LTSC 32 位/64 位 Windows 10 IoT Enterprise 版 1703 32 位/64 位 Windows 10 IoT Enterprise 版 1709 32 位/64 位 Windows 10 IoT Enterprise 版 1803 32 位/64 位 Windows 10 IoT Enterprise 版 1809 32 位/64 位 Windows 10 20H2 IoT Enterprise 32 位/64 位 Windows 10 21H2 IoT Enterprise 32 位/64 位 Windows 10 IoT Enterprise 32 位/64 位 Windows 10 IoT Enterprise version 1909 32 位/64 位 Windows 10 IoT Enterprise LTSC 2021 32 位/64 位 Windows 10 IoT Enterprise 版 1607 32 位/64 位 Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 位/64 位 Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64 位 Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 位 Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 位 Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 位 Windows 8 Pro/Enterprise 32 位/64 位 Windows 8.1 Pro/Enterprise 32 位/64 位 Windows 7 Home/Pro/Enterprise/Ultimate with Service Pack 1 32 位/64 位 Microsoft Windows XP Professional Service Pack 2 32 位/64 位（仅受网络代理版本 10.5.1781 支持，可通过技术支持进行申请） Windows XP Professional Service Pack 3 及更高版本 32 位（受网络代理版本 14.0.0.20023 支持） 适用于嵌入式系统的 Windows XP Professional Service Pack 3 32 位（受网络代理版本 14.0.0.20023 支持） Windows MultiPoint Server 2011 Standard/Premium 64 位 Windows Server 2003 SP1 32 位/64 位（仅受网络代理版本 10.5.1781 支持） Windows Server 2003 SP2 标准版/企业版 32 位/64 位（仅受网络代理版本 10.5.1781 支持） Windows Server 2003 R2 标准版/企业版 SP2 32 位/64 位（仅受网络代理版本 10.5.1781 支持） Windows Server 2008 Standard/Enterprise/Datacenter/Foundation （Service Pack 2）32 位/64 位 Windows Server 2008 R2 Datacenter/Enterprise/Foundation/（含 Service Pack 1 及更高版本）64 位 Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64 位 Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 位 Windows Server 2016 Standard/Datacenter/Essentials/Server Core (安装选项) (LTSB) 64 位 Windows Server 2019 Standard/Datacenter/Core 64 位 Windows Server 2019 RS5 Standard/Essentials 64 位

	Windows Server 2022 Standard/Datacenter/Core 64 位 Windows Server 2022 21H2 Standard/Datacenter 64 位 Windows Server 2025 Standard/Datacenter/Core 64 位 Windows Storage Server 2019 64 位

操作系统。Linux	Debian GNU/Linux 10.x (Buster) 32 位/64 位 Debian GNU/Linux 11.x (Bullseye) 32 位/64 位 Debian GNU / Linux 12 (Bookworm) 32 位/64 位 Ubuntu Server 18.04 LTS (Bionic Beaver) 64 位 Ubuntu Server 20.04 LTS (Focal Fossa) 64 位 Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位 Ubuntu Server 22.04 LTS ARM 64 位 Ubuntu Server 24.04 LTS (Noble Numbat) 64 位 CentOS 6.7 及更高版本 32 位 CentOS 6.x（至 6.6）32 位/64 位 CentOS 7.x 64 位 CentOS Stream 8 64 位 CentOS Stream 9 64 位 CentOS Stream 9 ARM 64 位 Red Hat Enterprise Linux Server 6.x 32 位/64 位 Red Hat Enterprise Linux Server 7.x 64 位 Red Hat Enterprise Linux Server 8.x 64 位 Red Hat Enterprise Linux Server 9.x 64 位 SUSE Linux Enterprise Server 12 (所有服务包) 64 位 SUSE Linux Enterprise Server 15 (所有服务包) 64 位 SUSE Linux Enterprise Server 15（所有服务包）ARM 64 位 openSUSE 15 64 位 EulerOS 2.0 SP10 64 位 EulerOS 2.0 SP10 ARM 64 位 Astra Linux 特别版 RUSB.10015-01（操作更新 1.5）64 位 Astra Linux 特别版 RUSB.10015-01（操作更新 1.6）64 位 Astra Linux 特别版 RUSB.10015-16（发布版 1）（操作更新 1.6）64 位 Astra Linux 特别版 RUSB.10015-17（操作更新 1.7.3）64 位 Astra Linux 特别版 RUSB.10015-01（操作更新 1.7）64 位 Astra Linux 特别版 RUSB.10015-01（操作更新 1.8）64 位 Astra Linux 特别版 RUSB.10015-37 （操作更新 7.7）64 位 Astra Linux 特别版 RUSB.10152-02（操作更新 4.7）ARM 64 位 Astra Linux Common Edition（操作更新 2.12）64 位 ALT Workstation 10.1 64 位 ALT Server 10.1 64 位 ALT Education 10.1 64 位 ALT SP Server 10 32 位/64 位 ALT SP Server 10 ARM 64 位 ALT SP Workstation 10 32 位/64 位 ALT SP Workstation 10 ARM 64 位 ALT Server 10 64 位 ALT Server 10 ARM 64 位 ALT Workstation 10 32 位/64 位 ALT 8 SP Workstation (8.4) ARM 64 位 ALT 8 SP Server (8.4) ARM 64 位 ALT 8 SP Server (LKNV.11100-01) 32 位/64 位 ALT 8 SP Server (LKNV.11100-02) 32 位/64 位 ALT 8 SP Server (LKNV.11100-03) 32 位/64 位 ALT 8 SP Workstation (LKNV.11100-01) 32 位/64 位 ALT 8 SP Workstation (LKNV.11100-02) 32 位/64 位 ALT 8 SP Workstation (LKNV.11100-03) 32 位/64 位 Mageia 4 32 位 Oracle Linux 7 64 位 Oracle Linux 8 64 位 Oracle Linux 9 64 位 Linux Mint 20.x 64 位

	Linux Mint 21.1 及更高版本 64 位 AlterOS 7.5 及更高版本 64 位 GosLinux IC6/7.17 64 位 GosLinux IC6/7.2 64 位 SberOS 3.3.1 64 位 Platform V SberLinux OS Server (SLO) 8.8 64 位 Platform V SberLinux OS Server (SLO) 8.9.2 64 位 RED OS 7.3 ARM 64 位 RED OS 7.3 Server 64 位 RED OS 7.3 Certified Edition 64 位 RED OS 8 Certified Edition 64 位 ROSA Enterprise Linux Server 7.9 64 位 ROSA Enterprise Linux Desktop 7.9 64 位 ROSA COBALT 7.9 64 位 ROSA CHROME 12 64 位 AlmaLinux 8 及更高版本 64 位 AlmaLinux 9 及更高版本 64 位 Rocky Linux 8 及更高版本 64 位 Rocky Linux 9 及更高版本 64 位 Atlant，Alcyone 内部版本，版本 2022.02 64 位 MSVSPHERE 9.2 SERVER 64 位 MSVSPHERE 9.2 ARM 64 位 SynthesisM Server 8.6 64 位 SynthesisM Client 8.6 64 位 OSnova 2.10 64 位 Kylin 10 64 位 EMIAS 1.0 64 位 Amazon Linux 2 64 位 MosOS 15.4 Arbat 64 位 OS MES (Moscow Electronic School) 64 位
操作系统。macOS	有关受支持的操作系统列表，请参阅 Kaspersky Endpoint Security for Mac 帮助。

对于网络代理，还支持 Apple Silicon (M1) 架构以及 Intel。

支持以下虚拟平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM（基于内核的虚拟机）

在早于Microsoft Windows Server 2008 R2（服务器版本）和Microsoft Windows 7（桌面版本）的Windows版本上，网络代理程序不支持以下功能：

- 更新重译（分发点使用）
- KSN代理（分发点使用）
- 漏洞扫描任务

在运行 Microsoft Windows 10 RS4 或 RS5 版本的设备上，Kaspersky Security Center 可能无法在启用了大小写敏感的文件夹中检测到一些漏洞。

在运行 Windows 7、Windows Server 2008、Windows Server 2008 R2 的设备上安装网络代理之前，请确保已安装适用于操作系统 Windows 的安全更新 KB3063858（Windows 7 安全更新（KB3063858），适用于基于 x64 系统的 Windows 7 安全更新 (KB3063858)、Windows Server 2008 安全更新 (KB3063858)，Windows Server 2008 x64 版本安全更新 (KB3063858)，Windows Server 2008 R2 x64 版本安全更新 (KB3063858)。

在 Microsoft Windows XP，网络代理可能错误执行一些操作。

您只能在 Microsoft Windows XP 中安装或更新 Network Agent for Windows XP。受支持的 Microsoft Windows XP 版本及其相应的网络代理版本列在受支持操作系统列表中。您可以从此页面下载适用于 Microsoft Windows XP 的网络代理所需版本。

我们建议您安装与 Kaspersky Security Center 相同版本的网络代理。

Kaspersky Security Center 完全支持相同或更新版本网络代理。

适用于 macOS 的网络代理与适用于此操作系统的卡巴斯基安全应用程序一起提供。

兼容的卡巴斯基应用程序和解决方案

Kaspersky Security Center 支持集中部署和管理当前支持的所有卡巴斯基应用程序和解决方案。下表显示了基于 MMC 的管理控制台和 Kaspersky Security Center Web Console 支持了哪些卡巴斯基应用程序和解决方案。要了解应用程序和解决方案的版本，请参阅产品支持生命周期网页。

Kaspersky Security Center 支持的卡巴斯基应用程序和解决方案列表

卡巴斯基应用程序或解决方案的名称	受基于 MMC 的管理控制台支持	受 Kaspersky Security Center Web Console 支持
对于工作站		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓

卡巴斯基应用程序或解决方案的名称	受基于 MMC 的管理控制台支持	受 Kaspersky Security Center Web Console 支持
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	–	✓
对于工业解决方案		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (集中部署不被支持)	✓	✓
对于移动设备		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	–	✓
对于文件服务器		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
对于虚拟环境		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	–
对于邮件和协作服务器		
Kaspersky Security for Microsoft Exchange Servers	✓	–
对于目标攻击的检测		
Kaspersky Sandbox Server	–	✓
Kaspersky Endpoint Detection and Response Optimum	–	✓
Kaspersky Managed Detection and Response	–	✓
对于 KasperskyOS 设备		
Kaspersky IoT Secure Gateway	–	✓
Kaspersky Thin Client	–	✓
声誉数据库		
卡巴斯基私有安全网络	–	✓

Kaspersky Security Center 15.1 的授权许可和功能

Kaspersky Security Center 的某些功能需要授权许可。

下表显示了不同的授权许可所覆盖的 Kaspersky Security Center 功能。

要启用 Kaspersky Security Center 的功能，您必须通过添加管理服务器授权许可密钥来激活管理服务器。

> 您必须为每个管理服务器手动添加授权许可密钥。

授权许可和 Kaspersky Security Center 功能

Kaspersky Security Center 的功能	卡巴斯基漏洞和补丁管理	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	卡巴斯基网络安全解决方案完整版	卡巴斯基混合云安全标准版	卡巴斯基混合云安全企业版	Kaspersky EDR Optimum
漏洞评估	✓	✓	✓	✓	✓	✓	✓
补丁管理	✓	–	✓	✓	–	✓	✓
基于角色的访问控制	✓	✓	✓	✓	✓	✓	✓
安装操作系统和应用程序	✓	–	✓	✓	–	✓	✓
移动设备管理（即，管理用户的 iOS 和安卓设备）	✓	✓	✓	✓	–	–	✓
配置云环境，用于 AWS、Microsoft Azure 或 Google Cloud 等云环境中的工作	–	–	–	–	✓	✓	–
导出事件到 SIEM 系统：Syslog	✓	✓	✓	✓	✓	✓	✓
将事件导出到 SIEM 系统：IBM 的 QRadar 和 ArcSight 的 Micro Focus	✓	✓	✓	✓	✓	✓	✓

关于 Kaspersky Security Center 组件的兼容性

在下表中，您可以找到有关 Kaspersky Security Center 组件兼容性的信息。

Kaspersky Security Center 组件的兼容性

组件	兼容
Kaspersky Security Center 15.1 管理服务器	• Kaspersky Security Center 15.1 管理控制台。 • Kaspersky Security Center 15.1 Web Console。 • 以下版本的 Kaspersky Security Center 网络代理：16、15.4、15.1、15、14.2、14。
Kaspersky Security Center 15.1 Web Console	以下版本的 Kaspersky Security Center 管理服务器：15.1 和 14.2。
Kaspersky Security Center 15.1 主管理服务器	从属管理服务器： • Kaspersky Security Center 14 Windows。 • Kaspersky Security Center 14.2 Windows。 • Kaspersky Security Center 15.1 Windows。 • Kaspersky Security Center 14.2 Linux。 • Kaspersky Security Center 15 Linux。 • Kaspersky Security Center 15.1 Linux。
Kaspersky Security Center 15.1 从属管理服务器	主管理服务器： • Kaspersky Security Center 14 Windows。 • Kaspersky Security Center 14.2 Windows。 • Kaspersky Security Center 15.1 Windows。 • Kaspersky Security Center 14.2 Linux。 • Kaspersky Security Center 15 Linux。 • Kaspersky Security Center 15.1 Linux。

我们建议您使用最新版本的 Kaspersky Security Center 管理服务器和 Kaspersky Security Center Web Console。否则，Kaspersky Security Center 的功能可能会受到限制。您可以独立安装和升级 Kaspersky Security Center 管理服务器以及 Kaspersky Security Center Web Console。在这种情况下，您必须确保已安装的 Kaspersky Security Center Web Console 版本与您连接的管理服务器版本兼容。

如果您有最新版本的 Kaspersky Security Center Web Console 和先前版本的 Kaspersky Security Center，域身份验证期间会发生错误，错误文本将包含一条默认消息。

Kaspersky Security Center 的比较：基于 Windows 与基于 Linux

Kaspersky 提供 Kaspersky Security Center 作为 Windows 和 Linux 这两个平台的本地解决方案。在基于 Windows 的解决方案中，在 Windows 设备上安装管理服务器，而基于 Linux 的解决方案具有设计为安装在 Linux 设备上的管理服务器版本。此在线帮助包含有关 Kaspersky Security Center Windows 的信息。有关基于 Linux 的解决方案的详细信息，请参阅 Kaspersky Security Center Linux 在线帮助。

通过下表可以比较 Kaspersky Security Center 作为基于 Windows 的解决方案和基于 Linux 的解决方案的主要功能。

Kaspersky Security Center 作为基于 Windows 的解决方案和基于 Linux 的解决方案的功能比较

功能或属性	Kaspersky Security Center	
	基于 Windows 的解决方案	基于 Linux 的解决方案
管理服务器		
数据库管理系统 (DBMS) 位置	本地	本地 （不支持 Microsoft SQL）
在其中安装管理服务器的操作系统	Windows	Linux
管理服务器层级	✓	✓
支持虚拟管理服务器	✓	✓
使用 SNMP 将管理服务器统计信息发送到第三方应用程序	✓	计划于 2026 年实现
用于发布安装包和其他文件的 Web 服务器	✓	✓
在 Windows 服务器故障转移集群上安装管理服务器	✓	—
管理控制台		
管理控制台类型	基于 MMC 和基于 Web	基于 Web
在其中安装基于 Web 的管理控制台的操作系统	Windows 或 Linux	Linux
使用域身份验证登录控制台	✓	✓ 包含版本15.1-15.4不支持单点登录
管理客户端设备和从属管理组		
最大受管理设备数量（每台管理服务器）	100,000	50,000（使用 PostgreSQL 和 Postgres Pro）
网络轮询	✓	✓ 从版本16开始，支持FreeIPA和ALD Pro域控制器
保护 Windows、macOS 和 Linux 管理的设备	✓	✓
保护移动设备	✓ 移动设备的基本管理	✓ MDM 和使用 Kaspersky Secure Mobility Management 功能（需获得授权许可）。
虚拟机保护管理	✓	✓
保护公有云基础架构	✓	—
远程连接到客户端设备桌面	✓	✓ 从版本15.3开始

功能或属性	Kaspersky Security Center	
	基于 Windows 的解决方案	基于 Linux 的解决方案
数据加密和保护	✓	✓ 在安装了 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Mac 的 Windows 受管理设备上
部署 Kaspersky Security Center 故障转移集群	✓	✓
管理组中对集群和服务器阵列的支持	✓	✓
管理组层级	✓	✓
在 DMZ 中添加连接网关作为分发点	✓ （基于MMC的管理控制台）	计划于 2026 年实现
使用用户		
创建和管理用户账户	✓	✓
管理卡巴斯基应用程序		
应用程序策略	✓	✓
Kaspersky 应用程序的任务	✓	✓
卡巴斯基安全网络	✓	✓
KSN Proxy	✓	✓
卡巴斯基私有安全网络	✓	✓
为卡巴斯基应用程序集中部署授权许可密钥	✓	✓
客户端设备的远程诊断	✓	✓
自动更新卡巴斯基应用程序	✓	✓
自适应异常控制支持	✓	✓
以设备为中心的安全管理	✓	✓
以用户为中心的安全管理	✓	✓
系统管理		
在客户端设备上部署操作系统	✓	—
管理第三方授权许可	✓	—
将管理服务器用作 WSUS 服务器	✓	✓ （仅限 Windows Update 被动搜索模式）
在客户端设备上管理第三方应用程序		
安装第三方软件更新并修复第三方软件漏洞	✓	✓
监控、报告和审计		
管理对象修订	✓	✓
比较策略修订	✓	计划于 2026 年实现
查看和使用 Kaspersky Endpoint Detection and Response Optimum 检测到的警报	✓	✓
有关受管理设备上发生的事件的通知	✓	✓
监控策略状态和任务状态	✓	✓
集成		
与 Kaspersky Managed Detection and Response 整合	✓	✓
与 SIEM 系统集成	✓	✓ （仅使用 syslog）

功能或属性	Kaspersky Security Center	
	基于 Windows 的解决方案	基于 Linux 的解决方案
使用 CEF 和 LEEF 格式导出事件	✓	计划于 2026 年实现
通过 Active Directory、KASAP 和 Kaspersky TIP Sandbox 聚合警报和执行响应操作	—	✓ （从版本 15.4 开始） 您必须在 Kaspersky Next XDR Optimum 授权许可下激活管理服务器，然后将 Kaspersky Next XDR Optimum 授权许可密钥部署到您的受管理应用程序

关于 Kaspersky Security Center 云控制台

将 Kaspersky Security Center 用作本地应用程序意味着，您在本地设备上安装 Kaspersky Security Center（包括管理服务器），并通过基于 Microsoft 管理控制台的管理控制台（仅在 Kaspersky Security Center Windows 中可用）或 Kaspersky Security Center Web Console 来管理网络安全系统。

但是，您可以将 Kaspersky Security Center 用作云服务。在这种情况下，卡巴斯基专家将在云环境中安装和维护 Kaspersky Security Center，卡巴斯基将以服务的形式为您提供对管理服务器的访问。您可以通过基于云的管理控制台（名为 Kaspersky Security Center 云控制台）管理网络安全系统。该控制台的界面类似于 Kaspersky Security Center Web Console 的界面。

Kaspersky Security Center 云控制台的界面和文档以下列语言提供：

- 英语
- 法语
- 德语
- 意大利语
- 日语
- 葡萄牙语（巴西）
- 俄语
- 简体中文
- 西班牙语
- 西班牙语（拉丁美洲）
- 繁体中文

关于 Kaspersky Security Center 云控制台及其特征的更多信息请参见 Kaspersky Security Center 云控制台文档和 卡巴斯基网络安全解决方案文档。

Kaspersky Security Center 15.1

该部分提供了 Kaspersky Security Center 15.1 信息。

Online Help 中提供的信息可能与随应用程序一起出货的文档中的信息不同；此种情况下，Online Help 为是最新的。您可以通过点击应用程序界面的链接转到 Online Help，或者通过点击文档中 Online Help 的链接。Online Help 可以自动更新。如有必要，可以切换在线帮助和离线帮助。

基本概念

本部分解释与 Kaspersky Security Center 有关的基本概念。

管理服务器

使用 Kaspersky Security Center 组件可远程管理客户端设备上安装的 Kaspersky 应用程序。

安装了管理服务器组件的设备将被称作*管理服务器*（也称作*服务器*）。管理服务器必须被保护，包括物理保护，以防范非授权的访问。

管理服务器作为服务安装在设备上，且拥有以下属性集：

- 名称为“Kaspersky Security Center 管理服务器”
- 设置为在操作系统启动时自动启动
- 具有“**LocalSystem**”账户或在安装管理服务器过程中选择的用户账户

管理服务器执行以下功能：

- 存储管理组结构
- 存储有关客户端设备配置的信息
- 应用程序分发包的存储结构
- 将应用程序远程安装至客户端设备和远程卸载应用程序
- 更新卡巴斯基应用程序的应用程序数据库和软件模块
- 管理客户端设备上的策略和任务
- 存储有关客户端设备上已发生事件的信息
- 生成有关卡巴斯基应用程序操作的报告

- 向客户端设备部署授权许可密钥并存储授权许可密钥信息
- 转发有关任务进度的通知（例如在客户端设备上检测到病毒）

在应用程序界面中命名管理服务器

在基于 MMC 的管理控制台和 Kaspersky Security Center Web Console 的界面中，管理服务器可以具有以下名称：

- 管理服务器设备的名称，例如："*设备名称*"或"管理服务器：*设备名称*"。
- 管理服务器设备的 IP 地址，例如："*IP 地址*"或"管理服务器：*IP 地址*"。
- 从属管理服务器和虚拟管理服务器具有自定义名称，这些名称是您在将虚拟或从属管理服务器连接到主管理服务器时指定的。
- 如果您使用 Linux 设备上安装的 Kaspersky Security Center Web Console，则该应用程序将显示您在响应文件中指定的受信任管理服务器的名称。

您可以使用管理控制台或 Kaspersky Security Center Web Console 连接到管理服务器。

管理服务器层级

管理服务器可以排列在层级中。在该层次结构的不同嵌套级别上，每个管理服务器都可以拥有多个从属管理服务器（称为*从属服务器*）。从属服务器的嵌套级别不受限制。这样，主管理服务器的管理组将会包括所有从属管理服务器的客户端设备。因而，网络的隔离和独立区段可以通过不同的管理服务器进行管理，而后者又通过主服务器进行管理。

*虚拟管理服务器*是从属管理服务器的一个特例。

您可以使用管理服务器的层次结构执行以下操作：

- 降低管理服务器的负载（与整个网络中安装的单个管理服务器相比）。
- 减少 Intranet 流量并简化远程办公室的工作。您不必在主管理服务器和所有网络设备（例如，它们可能位于不同地区）之间建立连接。只需在每个网络节点中安装从属管理服务器，在从属服务器的各个管理组中分发设备，以及通过快速通信通道在从属服务器和主服务器之间建立连接。
- 在反病毒安全管理员之间分配责任。用于集中管理和监控企业网络中的反病毒安全状态的所有功能仍然可用。
- 服务提供商使用 Kaspersky Security Center。服务提供商只需安装 Kaspersky Security Center 和 Kaspersky Security Center Web Console。为了管理大量的多个组织的更多客户端设备，服务提供商可以向管理服务器层级中添加从属管理服务器（包括虚拟服务器）。

管理组层次结构中包括的每台设备都只能连接到一台管理服务器。您必须独立监控设备到管理服务器的连接。使用这些功能可以根据网络属性在不同服务器的管理组中搜索设备。

虚拟管理服务器

虚拟管理服务器（下文也称作*虚拟服务器*）是 Kaspersky Security Center 的一个组件，用于管理客户端组织网络的反病毒保护系统。

虚拟管理服务器是从属管理服务器的特例，与物理管理服务器相比，具有以下限制：

- 只能在主管理服务器上创建虚拟管理服务器。
- 虚拟管理服务器在其操作中使用主管理服务器数据库。虚拟管理服务器不支持数据备份和还原任务以及更新扫描和下载任务。
- 虚拟服务器不支持从属管理服务器（包括虚拟服务器）的创建。

此外，虚拟管理服务器具有以下限制：

- 在虚拟管理服务器属性窗口中，区域的数量是有限的。
- 要在虚拟管理服务器管理的客户端设备上远程安装卡巴斯基应用程序，您必须确保已在其中一台客户端设备上安装网络代理，以确保与虚拟管理服务器通信。在第一次连接到虚拟管理服务器时，该设备会被自动分配为分发点，并充当客户端设备与虚拟管理服务器的连接网关。
- 虚拟服务器只能通过分发点进行网络轮询。
- 若要重启发生故障的虚拟服务器，Kaspersky Security Center 需要重启主管理服务器和所有虚拟管理服务器。
- 在虚拟服务器上创建的用户无法在管理服务器上被分配角色。

虚拟管理服务器的管理员在该特定虚拟服务器上具有所有权限。

移动设备服务器

*移动设备服务器*是 Kaspersky Security Center 的一个组件，它可以提供对移动设备的访问，并且允许通过管理控制台来管理它们。移动设备服务器接收有关移动设备的信息并存储其配置文件。

Kaspersky Security Center 包含 iOS MDM 服务器作为移动设备服务器。此移动设备服务器用于管理支持 Apple® Push Notifications 服务（APNs）的移动设备。

Kaspersky Security Center 的移动设备服务器允许您管理以下对象：

- 单个移动设备。
- 多个移动设备。
- 同时连接至一个服务器集群的多个移动设备。在连接至一个服务器集群之后，此集群中安装的移动设备服务器将作为单个服务器显示在管理控制台中。

Web 服务器

Kaspersky Security Center *Web Server*（以下简称"*Web 服务器*"），是 Kaspersky Security Center 的一个组件，与管理服务器一同安装。Web 服务器用于通过网络传输独立安装包、iOS MDM 配置文件、以及共享文件夹的文件。

当您创建独立安装包时，它会自动发布在 Web 服务器上。已创建的独立安装包列表中会显示用于下载独立包的链接。必要时，您可以取消发布独立包或在 Web 服务器上重新发布。

当您为用户的移动设备创建 iOS MDM 配置文件时，它会自动发布在 web 服务器上。发布的配置文件在成功安装到用户移动设备后自动从 Web Server 删除。

共享文件夹专用于存储通过管理服务器所管理的所有设备用户的信息。如果用户无法直接访问共享文件夹，他/她可以通过 web 服务器的方式获取共享文件夹的信息。

要通过 web 服务器为用户提供共享文件夹的信息，管理员需要在共享文件夹中创建一个名为"public"的子文件夹并将相关信息复制至此。

信息传输链接的句法按以下格式：

`https://<Web 服务器名称>:<HTTPS 端口>/public/<对象>`

其中：

- `<Web Server name>`为 Kaspersky Security Center Web Server 的名称。
- `<HTTPS port>`为由管理员定义的 Web 服务器的 HTTPS 端口。HTTPS 端口可以在管理服务器属性窗口的"**Web 服务器**"区域设置。默认端口号是 8061。
- `<object>`是用户可以访问的子文件夹或文件。

管理员可以通过任意方式如电子邮件等将新链接发送给用户。

通过单击链接，用户可将所需信息下载至本地设备。

网络代理

管理服务器和设备之间的交互由 Kaspersky Security Center 的*网络代理*组件执行。网络代理必须安装在所有使用 Kaspersky Security Center 来管理 Kaspersky 应用程序的设备上。

网络代理作为服务安装在设备上，且具有以下属性集：

- 名称为"Kaspersky Security Center 网络代理"
- 设置为在操作系统启动时自动启动
- 使用 LocalSystem 账户

安装了网络代理的设备被称为*受管理设备*或*设备*。

您可以在 Windows、Linux 或 Mac 设备上安装网络代理。您可以通过以下方式获得组件：

- 管理服务器存储中的安装包（您必须安装了管理服务器）
- Kaspersky Web 服务器上的安装包

您不必在安装管理服务器的设备上安装网络代理，因为网络代理的服务器版本随管理服务器一同自动安装。

网络代理启动的进程名称叫 *klnagent.exe*。

网络代理同步管理服务器的受管理设备。我们建议您设置同步间隔（也叫*心跳*）为每 10,000 台受管理设备 15 分钟。

管理组

管理组（以下简称*组*）是受管理设备的逻辑集合，根据某一特征组合在一起以便作为 Kaspersky Security Center 的一个单元来统一管理。

管理组内的所有受管理设备都被配置以做如下事情：

- 使用共同的应用程序设置（您可以在组策略中指定）。
- 通过以指定设置创建组任务，对所有应用程序使用通用的操作模式。组任务的例子包括创建和安装公用安装包、更新应用程序数据库和模块、按需扫描设备和启用实时保护。

受管理设备只能属于一个管理组。

您可以创建管理服务器和组的层级。单个层次结构级别可以包括从属和虚拟管理服务器、组和受管理设备。您可以从一个组移动设备到其他组，而不做物理移动。例如，如果企业员工的职位从会计变更为开发者，您可以将该员工的设备从会计管理组移动到开发者管理组。然后，该设备将自动接收开发者的应用程序设置。

受管理设备

*受管理设备*是运行 Windows、Linux 或 macOS 且安装了网络代理的设备，或者是安装了 Kaspersky 安全应用程序的移动设备。您可以通过设备上安装的应用程序的任务和策略来管理此类设备。您也可以从受管理设备接收报告。

您可以让非移动受管理设备作为分发点和连接网关来运行。

设备仅可以被一个管理服务器管理。一个管理服务器可以管理最多 100,000 台设备，包括移动设备。

未分配的设备

*未分配的设备*是网络中未被包含在任何管理组中的设备。您可以在未分配设备上运行一些操作，例如，移动它们到管理组或在其上安装应用程序。

当在您的网络中发现新设备时，该设备转到"**未分配的设备**"管理组。您可以配置规则以便设备在被发现后被自动移动到其他管理组。

管理员工作站

*管理员工作站*是安装了管理控制台或用于打开 Kaspersky Security Center Web Console 的设备。管理员可以使用这些设备来远程集中管理客户端设备上安装的 Kaspersky 应用程序。

在设备上安装管理控制台后，系统会显示其图标，允许您启动管理控制台。在**开始 → 程序 → Kaspersky Security Center** 菜单中找到。

管理员工作站的数量不受限制。在任何管理员工作站中，都可以同时管理网络中多个管理服务器的管理组。您可以将管理员的工作站连接至层次结构任何级别的（物理或虚拟）管理服务器。

您可以将管理员的工作站作为客户端设备包括在管理组中。

在任何管理服务器的管理组中，同一台设备可以充当管理服务器客户端、管理服务器或管理员工作站。

管理插件

使用名为*管理插件*的专用组件通过管理控制台管理 Kaspersky 应用程序。每个可以通过 Kaspersky Security Center 管理的 Kaspersky 应用程序都包含一个管理插件。

使用应用程序管理插件，可以在管理控制台中执行以下操作：

- 创建和编辑应用程序策略和设置以及应用程序任务的设置。
- 获取有关应用程序任务和应用程序事件的信息，以及从客户端设备接收的应用程序操作统计信息。

您可以从卡巴斯基技术支持网页下载管理插件。

管理 Web 插件

特殊组件 — *管理 Web 插件* — 通过 Kaspersky Security Center Web Console 对 Kaspersky 软件进行远程管理。在下文中，管理 Web 插件也称为*管理插件*。管理插件是 Kaspersky Security Center Web Console 与特定 Kaspersky 应用程序之间的接口。使用管理插件，您可以配置应用程序任务和策略。

您可以从卡巴斯基网站下载管理 Web 插件。

管理插件提供以下：

- 创建和编辑应用程序任务和设置的界面
- 用于创建和编辑策略和策略配置文件以便远程集中配置卡巴斯基应用程序和设备的界面
- 应用程序事件传输
- Kaspersky Security Center Web Console 显示应用程序的操作数据和事件，以及从客户端设备转发的统计信息

策略

*策略*是应用于一个管理组和其子组的 Kaspersky 应用程序设置集。您可以在管理组的设备上安装多个 Kaspersky 应用程序。Kaspersky Security Center 为管理组中的每个 Kaspersky 应用程序提供一个策略。策略具有以下状态之一（请参见下表）：

策略的状态

状态	描述
活动	应用于设备的当前策略。对于每个管理组中的卡巴斯基应用程序，只能有一个策略处于活动状态。设备对卡巴斯基应用程序应用活动策略的设置值。
非活动	当前未应用于设备的策略。
漫游	如果选择该选项，策略将在设备离开企业网络时变为活动状态。

策略根据以下规则发挥作用：

- 您可以为单个应用程序配置拥有不同值的多个策略。
- 对于当前应用程序，只能有一个策略处于活动状态。
- 您可以在发生特定事件时激活处于非活动状态的策略。例如，您可以在病毒爆发时强制执行更严格的反病毒保护设置。
- 策略可以有子策略。

通常，您可以将策略用作对紧急情况（如病毒攻击）的准备。例如，如果存在通过闪存驱动器进行的攻击，您可以激活相应策略来阻止访问闪存驱动器。在这种情况下，当前的活动策略将自动变为非活动状态。

为了防止维护多个策略，例如，在不同的场合下只是更改几个设置时，可以使用策略配置文件。

*策略配置文件*是策略设置值的命名子集，用于替换策略的设置值。策略配置文件影响受管理设备上有效设置的形成。*有效设置*是当前应用于设备的一组策略设置、策略配置文件设置和本地应用程序设置。

策略配置文件根据以下规则发挥作用：

- 当出现特定的激活情况时，策略配置文件生效。
- 策略配置文件包含的设置值与策略设置不同。
- 激活策略配置文件会更改受管理设备的有效设置。
- 一个策略可以包含最多 100 个策略配置文件。

策略配置文件

有时候有必要为不同的管理组创建单一策略的若干实例；您也可能想要集中修改这些策略的设置。这些实例可能仅有一两处设置不同。例如，企业中所有的会计工作在相同策略下 — 但是高级会计被允许使用闪存驱动器，而初级会计不被允许。此种情况下，仅通过管理组层级应用策略到设备可能不方便。

要帮助您避免创建单一策略的多个实例，Kaspersky Security Center 允许您创建*策略配置文件*。策略配置文件用于在单一管理组中的设备在不同策略设置下运行时。

策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在受管理设备上活动。配置文件的激活将修改在设备上最初活动的"基本"策略的设置。修改的设置将使用已在配置文件中指定的值。

任务

Kaspersky Security Center 通过创建和运行*任务*来管理设备上安装的 Kaspersky 应用程序。安装、启用和停用程序、扫描文件、更新数据库和软件模块以及程序的其他操作均需要任务。

特定应用程序的任务仅在安装了该应用程序的管理插件时可以被创建。

任务可以在管理服务器和设备上执行。

以下任务在管理服务器上执行：

- 自动分发报告
- 将更新下载至管理服务器存储库
- 备份管理服务器数据
- 数据库维护
- Windows Update 同步
- 基于参考设备的操作系统镜像创建安装包

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

  本地任务可以被管理员通过管理控制台工具修改，或者被远程设备用户修改（例如，通过安全应用程序界面）。如果本地任务同时被管理员和受管理设备用户修改，管理员的修改将生效，因为其具有更高优先级。

- *组任务* — 在特定组的所有设备上执行的任务。

  除非在任务属性中指定了其他项，组任务也影响所选组的所有子组。组任务还影响（可选）已连接到部署在该组或其任意子组中的从属和虚拟管理服务器的设备。

- *全局任务* — 在一组设备上执行的任务，与设备是否包含在某个组中无关。

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务结果保存在 Microsoft Windows 事件日志和 Kaspersky Security Center 的事件日志中，既集中在管理服务器上，又位于每个设备上。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

- 对于*本地任务*，范围是设备本身。
- 对于*管理服务器任务*，范围是管理服务器。
- 对于*组任务*，范围是包含在组中的设备列表。

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

  您可以使用 IP 地址（或 IP 范围）、NetBIOS 名称或 DNS 名称作为设备地址。

- 从包含要添加的设备地址的 TXT 文件导入设备列表（每个地址必须单独一行）。

  如果通过文件导入设备列表或手动创建设备列表，且如果设备是以名称定义，则列表可以只包含其信息已被输入到管理服务器数据库中的设备。而且，信息必须在设备被连接或设备发现中输入。

- 指定设备分类。

  后续，任务范围随着包含在分类中的设备集的更改而更改。设备分类可以基于设备属性（包含安装在设备上的软件）创建，也可以基于分配到设备的标签来创建。设备分类是指定任务范围的最灵活的方法。

  设备分类的任务总是按管理服务器计划运行。这些任务无法运行在缺少管理服务器连接的设备上。使用其他方法指定范围的任务直接运行在设备上，且因此不取决于到管理服务器的设备连接。

  设备分类的任务不会按设备本地时间运行；相反，它们将按照管理服务器本地时间运行。使用其他方法指定范围的任务以设备本地时间运行。

本地应用程序设置与策略的关系

您可以使用策略为组中的所有设备设置完全相同的应用程序设置值。

使用本地应用程序设置可以为组中的各个设备重新定义策略指定的设置值。您只能设置策略允许修改的设置的值，即解锁设置的值。

应用程序在客户端设备上使用的设置的值由策略中该设置的锁定位置（🔒）确定：

- 如果设置修改被锁定，则在所有客户端设备中使用策略中定义的相同值。
- 如果设置修改被“解锁”，则应用程序使用每台客户端设备上的本地设置值，而不是策略中指定的值。然后，您可以在本地应用程序设置中更改设置。

这意味着在客户端设备上运行任务时，应用程序以两种不同的方式使用所定义的设置：

- 如果没有锁定设置以避免策略更改，则通过任务设置和本地应用程序设置使用。
- 如果锁定设置以避免更改，则通过组策略使用。

在首先根据策略设置应用策略之后，才会更改本地应用程序设置。

分发点

分发点（先前称为“更新代理”）是指安装了网络代理的设备，用于分发更新、远程安装应用程序和检索联网设备信息。分发点加速更新发布并释放管理服务器资源。

安装在作为分发点的设备上的网络代理的功能和用例因操作系统而异。

分发点可执行以下功能：

- 将从管理服务器接收到的文件分发到组中的客户端设备（包括使用 UDP 通过多播进行分发）。

  可被分发点传输的文件列表包括：

  - 卡巴斯基数据库和软件模块更新
  - 第三方软件更新
  - 安装包
  - 将管理服务器用作 WSUS 服务器时的 Windows 更新

  更新可以从管理服务器接收，或者从 Kaspersky 更新服务器获取。如果是后者，必须为分发点创建更新任务。运行 MacOS 的分发点设备无法从 Kaspersky 更新服务器下载更新。

  如果一个或多个运行 macOS 的设备在“*将更新下载至分发点存储库*”任务范围内，则该任务将以“*失败*”状态完成，即使该任务在所有 Windows 设备上均已成功完成。

- 使用 UDP 通过多点传送分发策略和组任务。
- 用作管理组中的设备与管理服务器的连接网关。

  如果组中的受管理设备与管理服务器之间的直接连接无法建立，则分发点可用作此组的管理服务器连接网关。在这种情况下，受管理设备将连接到连接网关，连接网关又连接到管理服务器。

  用作连接网关的分发点的可用性不会阻止受管理设备与管理服务器之间的直接连接。如果连接网关不可用，但在技术上可与管理服务器进行直接连接，则受管理设备将直接连接到管理服务器。

- 轮询网络以检测新设备并更新现有设备的信息。分发点应用与管理服务器相同的设备发现方法。
- 使用分发点操作系统的工具远程安装第三方软件和卡巴斯基应用程序。请注意，分发点可以在没有网络代理的客户端设备上执行安装。

  此功能允许将网络代理的安装包远程传输到位于管理服务器无直接访问权限的网络上的客户端设备。

- 作为代理服务器加入卡巴斯基安全网络 (KSN)。

  您可以在分发点端启用 KSN 代理服务器以使设备作为 KSN 代理服务器。此种情况下，KSN 代理服务 (ksnproxy) 在设备上运行。

文件通过 HTTP 或者 HTTPS 从管理服务器传输到分发点。使用 HTTP 或 HTTPS 促成更高性能，相比通过流量的 SOAP。

安装有网络代理的设备可以被手动（通过管理员）或自动（通过管理服务器）分配分发点。指定管理组的分发点的完整列表显示在关于分发点列表的报告中。

分发点的范围是管理员将其分配到其中的管理组，以及其所有嵌套级别的子组。如果已在管理组的层次结构中分配几个分发点，则受管理设备上的网络代理会连接到层次结构中最近的分发点。

网络位置也可以是分发点范围。网络位置用于手动创建设备集，分发点可在其上发布更新。网络位置可以被运行 Windows 操作系统的设备决定。

如果分发点被管理服务器自动分配，它通过广播域分配，而不是通过管理组。此情况发生在所有广播域已知时。网络代理在相同的子网与其它网络代理交换信息并发送给管理服务器它的其它网络代理的信息。管理服务器可以用此信息通过广播域分组网络代理。在管理组中超过 70% 的网络代理被轮询后，广播域对管理服务器已知。管理服务器每两小时轮询一次广播域。分发点通过广播域分配后，就无法通过管理组重新分配。

如果管理员手动分配分发点，则可以将它们分配给管理组或网络位置。

带有活动连接配置文件的网络代理不参与广播域检测。

Kaspersky Security Center 为每个网络代理分配不同于其他地址的单独的 IP 多点传送地址。这允许您避免由于 IP 重叠引起的网络过载。

当两个或更多分发点分配在单独的网络区域或单独的管理组，其中一个会变成活动分发点，其余的变成备用分发点。活动分发点直接从管理服务器下载更新和安装包，备用分发点只从活动分发点接收更新。此种情况下，文件从管理服务器下载一次，然后在分发点之间发布。如果因为任何原因活动分发点不可用，其中一个备用分发点将变成活动的。管理服务器自动分配分发点做为备用。

分发点状态（*活动*/*备用*）通过 klnagchk 报告中的复选框进行显示。

一个分发点需要至少 4 GB 的可用磁盘空间。如果分发点的磁盘剩余空间少于 2 GB，Kaspersky Security Center 将创建一个重要级别为“*警告*”的安全问题。安全问题将被发布在设备属性的“**安全问题**”部分中。

在分配为分发点的设备上运行远程安装任务需要另外的可用磁盘空间。剩余磁盘空间卷必须超过安装包的总大小。

在分配为分发点的设备上运行任何更新（补丁）任务和漏洞修复任务需要另外的可用磁盘空间。剩余磁盘空间卷必须是至少两倍的要安装补丁的总大小。

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

连接网关

*连接网关*是以特殊模式运行的网络代理。连接网关接受来自其他网络代理的连接，并通过其自身与服务器的连接将它们与管理服务器建立隧道连接。与普通的网络代理不同，连接网关等待来自管理服务器的连接，而不是建立与管理服务器的连接。

一个连接网关最多可以接收 10,000 台设备的连接。

使用连接网关有两种选择：

- 我们建议您在隔离区域 (DMZ) 中安装连接网关。对于漫游设备上安装的其他网络代理，您需要专门配置通过连接网关与管理服务器进行的连接。

  连接网关不以任何方式修改或处理从网络代理传输到管理服务器的数据。此外，它不会将此数据写入任何缓冲区，因此不能接受来自网络代理的数据并随后将其转发到管理服务器。如果网络代理尝试通过连接网关连接到管理服务器，但是连接网关无法连接到管理服务器，则网络代理会认为管理服务器无法访问。所有数据保留在网络代理上（不在连接网关上）。

  一个连接网关无法通过另一个连接网关连接到管理服务器。这意味着网络代理不能在作为连接网关的同时，使用另一个连接网关连接到管理服务器。

  所有连接网关都包含在管理服务器属性的分发点列表中。

- 您还可以在网络内使用连接网关。例如，自动分配的分发点也将成为各自范围内的连接网关。但是，在内部网络中，连接网关的效益不高。它们会减少管理服务器收到的网络连接数量，但不会减少传入数据量。即使没有连接网关，所有设备仍可以连接到管理服务器。

主要安装方案

该方案允许您部署管理服务器以及安装网络代理和安全应用程序到网络设备。您可以使用该方案更好的查看应用程序和安装应用程序。

Kaspersky Security Center 的安装包括以下步骤：

1. 准备工作
2. 在管理服务器设备上安装 Kaspersky Security Center 和 Kaspersky 安全应用程序
3. 在客户端设备上集中部署 Kaspersky 安全应用程序

在云环境中部署 Kaspersky Security Center 和为服务提供商部署 Kaspersky Security Center 在其他“帮助”部分中有介绍。

我们建议您分配至少一小时用于管理服务器安装和至少一个工作日用于完成方案。我们还建议您在将充当 Kaspersky Security Center 管理服务器的设备上安装安全应用程序，例如 Kaspersky Security for Windows Server 或 Kaspersky Endpoint Security。

该方案完成后，将通过以下方式在组织网络中部署保护功能：

- 将为管理服务器安装 DBMS。
- 将安装 Kaspersky Security Center 管理服务器。

- 将创建所有所需的策略和任务；将指定策略和任务的默认设置。
- 安全应用程序（例如，Kaspersky Endpoint Security for Windows）和网络代理将安装到受管理设备。
- 将创建管理组（可能组合成层级）。
- 如有必要，将部署移动设备保护功能。
- 如有必要，将分配分发点。

Kaspersky Security Center 安装分步骤进行：

准备工作

1 获取必要的文件

确保您拥有 Kaspersky Security Center 的授权许可密钥（激活码）或 Kaspersky 安全应用程序的授权许可密钥（激活码）。

解压缩从供应商处收到的存档。此压缩文件包含授权许可密钥（KEY 文件）、激活码和可由每个授权许可密钥激活的 Kaspersky 应用程序列表。

如果您想先试用 Kaspersky Security Center，则可以在卡巴斯基网站获得 30 天免费试用。

有关对 Kaspersky Security Center 未包含的 Kaspersky 安全应用程序进行授权的详细信息，可以参考这些应用程序的文档。

2 选择组织保护结构

找到更多 Kaspersky Security Center 组件。选择最适合您组织的保护结构和网络配置。基于网络配置和通信渠道的吞吐量，定义要使用的管理服务器数量以及如何在您的办公室间分发它们（如果您的组织运行分布式网络）。

要在不同的操作条件下获取和维持优化运行，请考虑网络设备数量、网络拓扑和您需要的 Kaspersky Security Center 功能集（更多详情，请参考 Kaspersky Security Center 层级指南）。

定义是否管理服务器层级将被用于您的组织。为此，您必须评估您的情况是否适合用单一管理服务器覆盖所有客户端设备，或者是否有必要创建一个管理服务器层级。您可能必须创建一个对应于您要保护的组织的组织结构的管理服务器层级。

如果您必须确保对移动设备的保护，请执行配置iOS MDM 服务器所需的所有先决操作。

确保您选为管理服务器以及安装管理控制台的设备满足所有的硬件和软件需求。

3 准备使用自定义证书

如果组织的公钥基础结构 (PKI) 要求您使用由特定证书颁发机构 (CA) 颁发的自定义证书，请准备这些证书并确保它们满足所有要求。

4 准备 Kaspersky Security Center 授权许可

如果您计划使用支持“移动设备管理”、“与 SIEM 系统集成”和/或“漏洞和补丁管理”的 Kaspersky Security Center 版本，确保您有应用程序授权许可密钥文件或激活码。

5 准备受管理安全应用程序的授权许可

在部署保护功能的过程中，您将必须向 Kaspersky 提供您要通过 Kaspersky Security Center 管理的应用程序的活动授权许可密钥（参见可管理安全应用程序列表）。有关任何安全应用程序的授权许可详情，可以参阅该应用程序的文档。

6 选择管理服务器和 DBMS 的硬件配置

计划 DBMS 和管理服务器硬件配置，需要考虑您网络设备的数量。

7 选择 DBMS

当选择 DBMS 时注意要由该管理服务器覆盖的受管理设备数量。如果您的网络包含少于 10,000 台设备且您不打算增加该数量，您可以选择免费 DBMS，例如 SQL Express 或 MySQL，并将其安装到管理服务器所在的同一设备。还可以选择 MariaDB DBMS，它允许管理多达 2 万台设备。如果您的网络包含多于 10,000 台设备（或如果您计划扩展您的网络到该数量的设备），我们建议您选择付费 SQL DBMS 并将其安装到专用设备。付费 DBMS 可以用于多个管理服务器，但免费 DBMS 仅可以用于一个。

如果您选择 SQL Server DBMS，请注意，您可以将数据库中存储的数据迁移到 MySQL、MariaDB 或 Azure SQL DBMS。要执行迁移，请备份数据并将其恢复到新的 DBMS。

8 安装 DBMS 并创建数据库

找到更多使用 DBMS 的账户详情并安装您的 DBMS。

安装之前选择受支持的 DBMS。例如，您可以选择 PostgreSQL、Postgres Pro、Microsoft SQL Server、MySQL 或 MariaDB。

对于如何安装所选 DBMS 的信息，请参考其文档。

如果您安装 MariaDB、MySQL、PostgreSQL 或 Postgres Pro，请使用建议的设置以确保 DBMS 正常运行。

写下并保存 DBMS 设置，因为您将在管理服务器安装时需要它们。这些设置包括 SQL Server 名称、连接 SQL Server 的端口号、访问 SQL Server 的账户名和密码。

> 如果您决定安装 PostgreSQL 或 Postgres Pro DBMS，请确保您为超级用户指定了密码。如果未指定密码，管理服务器可能无法连接到数据库。

默认下，Kaspersky Security Center 安装程序创建管理服务器信息存储数据库，但是您可以取消创建该数据库并使用其他数据库。此种情况下，确保数据库已被创建，您知道它的名称，管理服务器将再次访问该数据库的账户具有 db_owner 角色。

如果必要，联系您的 DBMS 管理员获取更多信息。

9 配置端口

确保所有必要的端口均已开放，以根据您选择的安全结构在组件之间进行交互。

如果您必须提供互联网访问给管理服务器，根据网络配置来配置端口并指定连接设置。

10 检查账户

确保您具有所有在设备上成功安装 Kaspersky Security Center 管理服务器和后续保护部署所需的本地管理员权限。在客户端设备上安装网络代理时，需要本地管理员权限。安装网络代理后，您可以使用它远程安装应用程序到设备，而不使用带有设备管理员权限的账户。

默认下，在用于安装管理服务器的设备上，Kaspersky Security Center 安装程序创建运行管理服务器和 Kaspersky Security Center 服务的本地账户：

- KL-AK-*：管理服务器服务账户
- NT Service/KSC*：管理服务器池中的其他服务的账户
- KlPxeUser：操作系统部署账户

您可以不必为管理服务器服务和其他服务创建账户。您使用您的现有账户，例如域账户，如果您计划安装管理服务器到故障转移集群，或者由于其他原因计划使用域账户而不是本地账户。在这种情况下，请确保已创建用于运行管理服务器和 Kaspersky Security Center 服务的账户，这些账户是非特权账户并且具有访问 DBMS 所需的所有权限。（如果您计划通过 Kaspersky Security Center 在设备上进一步部署操作系统，请不要选择退出创建账户。）

在管理服务器设备上安装 Kaspersky Security Center 和 Kaspersky 安全应用程序

1 为安全应用程序安装管理服务器、管理控制台、Kaspersky Security Center Web Console 和管理插件

从卡巴斯基网站下载 Kaspersky Security Center。您可以下载完整包，也可以仅下载 Web Console 或管理控制台。

安装管理服务器到所选设备（或多个设备，如果您计划使用多个管理服务器）。您可以选择管理服务器标准或自定义安装。管理控制台将同管理服务器一起安装。建议将管理服务器安装在专用服务器上，而不是域控制器上。

标准安装用在您要尝试 Kaspersky Security Center 并在网络中的小区域测试其操作的时候。在标准安装期间，您仅配置数据库。您还可以仅安装 Kaspersky 应用程序的管理插件的默认集合。如果您有过使用 Kaspersky Security Center 的经验，因此您可以在标准安装后指定所有相关设置，您也可以使用标准安装。

自定义安装允许您修改 Kaspersky Security Center 设置，例如共享文件夹路径、账户和连接管理服务器的端口，以及数据库设置。自定义安装允许您指定安装哪些 Kaspersky 管理插件。如果必要，您可以在静默模式启动自定义安装。

管理控制台和网络代理的服务器版本与管理服务器一起安装。您也可以在安装过程中选择安装 Kaspersky Security Center Web Console。

如果您想，安装管理控制台和/或 Kaspersky Security Center Web Console 到管理员的工作站以通过网络管理管理服务器。

2 初始化设置和授权许可

当管理服务器安装完成后，在第一次连接到管理服务器时，快速启动向导自动开始。根据现有需求指定管理服务器初始化配置。在初始化配置步骤，向导使用默认设置创建部署保护所需的策略和任务。然而，默认设置可能少于您组织需要的最优设置。如果必要，您可以编辑策略和任务设置（在客户端组织网络中配置保护、方案：配置网络保护）。

如果您计划使用基本功能意外的功能，请授权应用程序。您可以在快速启动向导的某步骤执行该操作。

3 检查管理服务器安装是否成功

当所有先前步骤完成后，管理服务器被安装并准备使用。

确保管理控制台正在运行且您可以通过管理控制台连接到管理服务器。此外，确保“将更新下载至管理服务器存储库”任务在管理服务器（在控制台树的“**任务**”文件夹）以及 Kaspersky Endpoint Security 策略（在控制台树的“**策略**”文件夹）中可用。

当检查完成时，继续以下步骤。

在客户端设备上集中部署 Kaspersky 安全应用程序

1 发现网络设备

该步骤是快速启动向导的一部分。您也可以手动启动设备发现。Kaspersky Security Center 接收网络中检测到的所有设备的地址和名称。然后您可以使用 Kaspersky Security Center 在检测到的设备上安装 Kaspersky 应用程序和其他供应商的软件。Kaspersky Security Center 定期启动设备发现，这意味着如果任何新实例出现在网络，它们将被自动检测。

2 安装网络代理和安全应用程序到网络设备

部署保护（在客户端组织网络中配置保护、方案：配置网络保护）到组织网络涉及到在设备发现中管理服务器检测到的设备上安装网络代理和安全应用程序（例如，Kaspersky Endpoint Security）。

安全应用程序用于保护设备，以防范病毒和/或其他威胁程序。网络代理确保设备和管理服务器之间的通信。网络代理设置默认被自动配置。

如果需要，可以以静默模式安装网络代理，其中包含响应文件或不包含响应文件。

在开始安装网络代理和安全应用程序到网络设备之前，请确保这些设备是可访问的（即，已开启）。您可以在虚拟机以及物理设备上安装网络代理。

安全应用程序和网络代理可以被远程或本地安装。

远程安装 – 使用保护部署向导，您可以将安全应用程序（例如 Kaspersky Endpoint Security for Windows）和网络代理远程安装在组织网络中由管理服务器发现的设备上。通常，远程安装任务成功部署保护到大多数网络设备。然而，它可能在一些设备上返回错误，如果，例如设备被关闭或由于其他原因无法访问。此种情况下，我们建议您手动连接到设备并使用本地安装。

本地安装用于不能使用远程安装任务部署保护的网络设备。要安装保护到此类设备，创建独立安装包以便在这些设备本地运行。

对于运行 Linux 和 macOS 操作系统的设备，请参阅 Kaspersky Endpoint Security for Linux 和 Kaspersky Endpoint Security for Mac 的相关文档了解网络代理安装描述。尽管运行 Linux 和 macOS 操作系统的设备被认为比运行 Windows 的设备漏洞少，我们建议您也在此类设备上安装安全应用程序。

安装后，确保安全应用程序被安装到了受管理设备。运行 Kaspersky 软件版本报告并查看结果。

3 部署授权许可密钥到客户端设备

部署授权许可密钥到客户端设备以在这些设备上激活受管理安全应用程序。

4 配置移动设备保护

该步骤是快速启动向导的一部分。

如果要管理企业移动设备，请执行必要的准备步骤并部署移动设备管理。

5 创建管理组结构

在某些情况下，要以最方便的方式在联网设备上部署保护，可能需要您在考虑到组织结构的情况下，将整个设备池划分为多个管理组。您可以创建移动规则以在组间分发设备，或者您可以手动分发设备。您可以为管理组分配组任务，定义策略范围并分配分发点。

确保所有受管理设备被正确分配到适当的管理组，且网络中不再有未分配的设备。

6 分配分发点

Kaspersky Security Center 会自动将分发点分配到管理组，但您可以在必要时手动分配它们。我们建议您在大规模网络中使用分发点以降低管理服务器负载，以及在具有分布式结构的网络中提供管理服务器通过窄通道访问到设备（或设备组）。您可以使用运行 Linux 的设备作为分发点，也可以使用运行 Windows 的设备。

Kaspersky Security Center 使用的端口

下表显示管理服务器和客户端设备使用的默认端口。如果需要，可以更改默认端口号。

如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server，端口 1433 用于 Microsoft SQL Server，端口 5432 用于 PostgreSQL 和 Postgres Pro）。请参阅 DBMS 文档以获取相关信息。

管理服务器使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
8060	klcsweb	TCP	传输发布的安装包到客户端设备	发布安装包。 您可以在管理控制台的管理服务器属性窗口的“**Web 服务器**”区域中或在 Kaspersky Security Center Web Console 中更改默认端口号。 该参数可选。出于安全原因，我们建议使用 8061 TCP 端口。

端口号	打开端口的进程名称	协议	端口目的	范围
8061	klcsweb	TCP (TLS)	传输发布的安装包到客户端设备	发布安装包。 您可以在管理控制台的管理服务器属性窗口的"**Web 服务器**"区域中或在 Kaspersky Security Center Web Console 中更改默认端口号。
13000	klserver	TCP (TLS)	从网络代理和从属管理服务器接收连接；也用于在从属管理服务器上从主管理服务器接收连接（例如，如果从属管理服务器在 DMZ 中）	管理客户端设备和从属管理服务器。 配置连接端口时，可以更改用于接收网络代理连接的默认端口号；您可以在管理控制台或在 Kaspersky Security Center Web Console 中创建管理服务器层级时，更改用于接收从属管理服务器连接的默认端口号。
13000	klserver	UDP	接收从网络代理关闭的设备的信息	管理客户端设备。 您可以在管理控制台的网络代理策略设置中或在 Kaspersky Security Center Web Console 中更改默认端口号。
13291	klserver	TCP (TLS)	接收从管理控制台到管理服务器的连接	管理管理服务器。 您可以在管理控制台的管理服务器属性窗口中更改默认端口号。
13299	klserver	TCP (TLS)	接收从 Kaspersky Security Center Web Console 到管理服务器的连接；接收通过 OpenAPI 到管理服务器的连接	Kaspersky Security Center Web Console，OpenAPI。 您可以在管理控制台的管理服务器属性窗口（**管理服务器连接设置**部分 → **连接端口**子部分）中更改默认端口号，或者在管理控制台中或在 Kaspersky Security Center Web Console 中创建管理服务器层级时进行更改。
14000	klserver	TCP	接收从网络代理的连接	管理客户端设备。 您可以在安装 Kaspersky Security Center 期间配置连接端口时更改默认端口号，或在手动连接客户端设备到管理服务器时进行更改。 该参数可选。出于安全原因，我们建议使用 13000 TCP 端口。
13111（仅当设备上运行 KSN 代理服务时）	ksnproxy	TCP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在管理服务器属性窗口中更改默认端口号。
15111（仅当设备上运行 KSN 代理服务时）	ksnproxy	UDP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在管理服务器属性窗口中更改默认端口号。
17000	klactprx	TCP (TLS)	接收从受管理设备的应用程序激活连接（除了从移动设备）	非移动设备用来通过激活码激活卡巴斯基应用程序的激活代理服务器。 您可以在管理服务器属性窗口中更改默认端口号。
17100（仅当管理移动设备时）	klactprx	TCP (TLS)	接收移动设备的应用程序激活连接	移动设备激活代理服务器。 您可以在管理服务器属性窗口中更改默认端口号。
19170	klserver	HTTPS (TLS)	使用 klsctunnel 实用程序建立与受管理设备的隧道连接	使用 Kaspersky Security Center Web Console 远程连接到受管理设备。 您只能在管理控制台的管理服务器属性窗口中更改默认端口号（**管理服务器连接设置**部分 →**连接端口**子部分 →**为 Kaspersky Security Center Web Console 打开远程桌面协议端口**选项）。
13292（仅当管理移动设备时）	klserver	TCP (TLS)	接收从移动设备的连接	移动设备管理。 您可以在管理控制台的管理服务器属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。
13294（仅当管理移动设备时）	klserver	TCP (TLS)	接收从 UEFI 保护设备的连接	管理 UEFI 保护客户端设备。 您可以在连接移动设备时更改默认端口号，或稍后在管理控制台的管理服务器属性窗口（**管理服务器连接设置**部分 → **连接端口**子部分）中或在 Kaspersky Security Center Web Console 中进行更改。

端口号	打开端口的进程名称	协议	端口目的	范围
13296	klserver	TCP (TLS)	发布 Prometheus 的 Kaspersky Security Center 指标	发布 Kaspersky Security Center 指标，Prometheus 将进一步获取这些指标。 您可以通过以下链接查看指标：https://<server_address>:13296/metrics。在 <server_address>，指定您的管理服务器的 IP 地址或域名。 您可以在管理控制台的管理服务器属性窗口中更改默认端口号。
30522， 30523（本地主机接口上的端口）	klnagent	TCP	使用 FileTransferBridge 组件从管理服务器接收卡巴斯基应用程序更新	接收卡巴斯基应用程序更新的管理服务器设备。

下表显示 iOS MDM 服务器使用的端口（仅当您管理移动设备时）。

iOS MDM 服务器使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
443	kliosmdmservicesrv	TCP (TLS)	接收来自 iOS 移动设备的连接	移动设备管理。 您可以在安装 iOS MDM 服务器时更改默认端口号。

下表显示 Kaspersky Security Center Web Console 服务器使用的端口。它可以是安装了管理服务器的同一设备，也可以是其他设备。

Kaspersky Security Center Web Console 服务器使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
8080	Node.js：服务器端 JavaScript	TCP (TLS)	接收从浏览器到 Kaspersky Security Center Web Console 的连接	Kaspersky Security Center Web Console。 您可以在运行 Windows 的设备或在 Linux 平台上安装 Kaspersky Security Center Web Console 时更改默认端口号。在 Linux ALT 操作系统上安装 Kaspersky Security Center Web Console 时，必须指定除 8080 以外的端口号，因为端口 8080 被操作系统使用。

下表显示安装网络代理的受管理设备使用的端口。

网络代理使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
15000	klnagent	UDP	从管理服务器或者分发点到网络代理的管理信号	管理客户端设备。 您可以在管理控制台的网络代理策略设置中或在 Kaspersky Security Center Web Console 中更改默认端口号。
15000	klnagent	UDP 广播	获取有关同一广播域内其他网络代理的数据（然后将数据发送到管理服务器）	传送更新和安装包。
15001	klnagent	UDP	接收来自分发点的多播请求（如果正在使用）	从分发点接收更新和安装包。 您可以在管理控制台的分发点属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。
30522， 30523（本地主机接口上的端口）	klnagent	TCP	使用 FileTransferBridge 组件从管理服务器接收卡巴斯基应用程序更新	从被指定为数据库更新源的管理服务器接收卡巴斯基应用程序更新的受管理设备。
161	klnagent	SNMP	监控和发现联网设备。	设备可发现性。

请注意，klnagent 进程也可以从端点操作系统的动态端口范围请求空闲端口。这些端口是由操作系统自动分配给 klnagent 进程的，所以 klnagent 进程可以使用一些已经被其他软件使用的端口。如果 klnagent 进程影响软件操作，请更改此软件中的端口设置，或更改操作系统中的默认动态端口范围以排除受影响的软件使用的端口。

另请注意，有关 Kaspersky Security Center 与第三方软件的兼容性的建议仅供参考，可能不适用于新版本的第三方软件。所描述的端口配置建议基于技术支持人员的经验和我们的最佳实践。

下表显示安装了网络代理用作分发点的受管理设备使用的端口。除了网络代理使用的端口，分发点设备也使用列出的端口（请参见上表）。

用作分发点的网络代理使用的端口

端口号	打开端口的进程名称	协议	端口目的	范围
13000	klnagent	TCP (TLS)	当分发点充当DMZ 中的连接网关时，从网络代理和 Kaspersky Security Center 接收连接。如果安装了管理服务器的设备被指定为分发点，则默认情况下使用端口 13001（而不是 13000）进行 SSL 连接。	管理客户端设备、传送更新和安装包。 详细信息请参见以下主题：管理服务器、网段中的连接网关和客户端设备。 您可以在管理控制台的分发点属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。
13111（仅当设备上运行 KSN 代理服务时）	ksnproxy	TCP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在管理控制台的分发点属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。
15111（仅当设备上运行 KSN 代理服务时）	ksnproxy	UDP	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在管理控制台的分发点属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。
17111（仅当设备上运行 KSN 代理服务时）	ksnproxy	HTTPS	接收从受管理设备到 KSN 代理服务器的请求	KSN 代理服务器。 您可以在管理控制台的分发点属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。
13295（仅当将分发点用作推送服务器时）	klnagent	TCP (TLS)	从客户端设备接收连接	推送服务器。 您可以在管理控制台的分发点属性窗口中或在 Kaspersky Security Center Web Console 中更改默认端口号。

下表显示域控制器设备使用的端口。

域控制器设备使用的端口

端口号	协议	端口目的	范围
389	TCP 或 UDP 上的 LDAP	连接到 LDAP 服务器	域控制器轮询
636	LDAP over TLS	连接到 LDAP 服务器	域控制器轮询

用于 Kaspersky Security Center 的证书

本节包含有关 Kaspersky Security Center 证书的信息，并介绍如何为管理服务器颁发自定义证书。

关于 Kaspersky Security Center 证书

Kaspersky Security Center 使用以下类型的证书来启用应用程序组件之间的安全交互：

- 管理服务器证书
- 移动证书
- iOS MDM 服务器证书
- Kaspersky Security Center Web Server 证书
- Kaspersky Security Center Web Console 证书

默认情况下，Kaspersky Security Center 使用自签名证书（即，由 Kaspersky Security Center 自身颁发），但是您可以将其替换为自定义证书，以更好地满足组织网络的要求并符合安全标准。在管理服务器验证自定义证书是否满足所有适用要求之后，该证书将承担与自签名证书相同的功能范围。唯一的区别是自定义证书不会在到期后自动重新颁发。您可以通过 klsetsrvcert 实用程序或通过管理控制台中的管理服务器属性区域将证书替换为自定义证书，具体取决于证书类型。使用 klsetsrvcert 实用程序时，需要使用以下值之一指定证书类型：

- C—端口 13000 和 13291 的通用证书。
- CR—端口 13000 和 13291 的通用备用证书。
- M—端口 13292 的移动证书。
- MR—端口 13292 的移动备用证书。
- MCA—自动生成的用户证书的移动证书颁发机构。

> 您无需下载 klsetsrvcert 实用程序。它包含在 Kaspersky Security Center 分发包中。该实用程序与以前的 Kaspersky Security Center 版本不兼容。

管理服务器证书的最长有效期不得超过 397 天。

管理服务器证书

管理服务器的身份验证以及管理服务器和受管理设备上的网络代理之间、或主管理服务器和从属管理服务器之间的安全交互都需要管理服务器证书。首次将管理控制台连接到管理服务器时，系统将提示您确认使用当前的管理服务器证书。每次更换管理服务器证书时，每次重新安装管理服务器后以及将从属管理服务器连接到主管理服务器时，都需要进行此类确认。此证书称为通用（“C”）证书。

安装管理服务器组件时会自动创建通用（“C”）证书。证书由两部分组成：

- klserver.cer 文件；默认情况下，它位于安装管理服务器组件的设备上的 C:\ProgramData\KasperskyLab\adminkit\1093\cert 文件夹中。
- 密钥位于 Windows 受保护的存储中。

此外，还存在一个通用备用（“CR”）证书。Kaspersky Security Center 会在通用证书到期前 90 天自动生成此证书。通用备用证书随后用于无缝替换管理服务器证书。当通用证书即将到期时，通用备用证书用于保持与受管理设备上安装的网络代理实例的连接。为此，通用备用证书会在旧的通用证书到期前 24 小时自动成为新的通用证书。

您还可以将管理服务器证书与其他管理服务器设置分开备份，以将管理服务器从一台设备移动到另一台设备而不丢失数据。

移动证书

在移动设备上对管理服务器进行身份验证需要移动证书（“M”）。您可以在快速启动向导的专门步骤配置移动证书的使用。

此外，还存在移动备用（“MR”）证书：它用于无缝替换移动证书。Kaspersky Security Center 会在通用证书到期前 60 天自动生成此证书。当移动证书即将到期时，移动备用证书用于保持与受管理移动设备上安装的网络代理实例的连接。为此，移动备用证书会在旧的移动证书到期前 24 小时自动成为新的移动证书。

如果连接方案要求在移动设备上使用客户端证书（涉及双向 SSL 身份验证的连接），您可以通过自动生成的用户证书（“MCA”）的证书颁发机构来生成那些证书。此外，通过快速启动向导可以开始使用由其他证书颁发机构颁发的自定义客户端证书，而与组织的域公钥基础结构 (PKI) 的集成允许您通过域证书颁发机构颁发客户端证书。

iOS MDM 服务器证书

在运行 iOS 操作系统的移动设备上对管理服务器进行身份验证时，需要 iOS MDM 服务器证书。与这些设备的交互通过不涉及任何网络代理的 Apple 移动设备管理 (MDM) 协议执行。反而在每台设备上都安装一个特殊的包含客户端证书的 iOS MDM 配置文件，以确保双向 SSL 身份验证。

此外，通过快速启动向导可以开始使用由其他证书颁发机构颁发的自定义客户端证书，而与组织的域公钥基础结构 (PKI) 的集成允许您通过域证书颁发机构颁发客户端证书。

当下载这些 iOS MDM 配置文件后，客户端证书会传输到 iOS 设备。每个受管理的 iOS 设备都有唯一的 iOS MDM 服务器客户端证书。通过自动生成的用户证书（“MCA”）的证书颁发机构生成所有 iOS MDM 服务器客户端证书。

Kaspersky Security Center Web Server 证书

Kaspersky Security Center Web Server（以下简称 Web 服务器）是 Kaspersky Security Center 管理服务器的一个组件，使用一种特殊类型的证书。发布后续下载到受管理设备的网络代理安装包以及发布 iOS MDM 配置文件、iOS 应用和 Kaspersky Security for Mobile 安装包都需要此证书。为此，Web 服务器可以使用各种证书。

如果禁用了移动设备支持，Web 服务器将按优先级顺序使用以下证书之一：

1. 通过管理控制台手动指定的自定义 Web 服务器证书
2. 通用管理服务器证书（“C”）

如果启用了移动设备支持，Web 服务器将按优先级顺序使用以下证书之一：

1. 通过管理控制台手动指定的自定义 Web 服务器证书
2. 自定义移动证书

3. 自签名移动证书（“M”）

4. 通用管理服务器证书（“C”）

Kaspersky Security Center Web Console 证书

Kaspersky Security Center Web Console 服务器（以下简称 Web Console）有自己的证书。当您打开网站时，浏览器会验证您的连接是否可信。Web Console 证书允许您对 Web Console 进行身份验证，并用于加密浏览器和 Web Console 之间的流量。

当您打开 Web Console 时，浏览器可能会通知您与 Web Console 的连接不是私有连接，并且 Web Console 证书无效。出现此警告是因为 Web Console 证书是自签名的，并且由 Kaspersky Security Center 自动生成。要移除此警告，可以执行以下操作之一：

- 将 Web Console 证书替换为自定义证书（推荐选项）。创建在您的基础架构中受信任且满足自定义证书要求的证书。
- 将 Web Console 证书添加到受信任浏览器证书列表中。我们建议您仅在无法创建自定义证书时才使用此选项。

关于管理服务器证书

两个操作基于管理控制台在连接期间进行的*管理服务器证书*：管理服务器身份验证以及与设备的数据交换。此证书还用于在主管理服务器连接到从属管理服务器时的身份验证。

由 Kaspersky 发布的证书

管理服务器证书是在安装管理服务器组件时自动生成的，并保存在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert 文件夹中。

如果管理服务器证书是由管理服务器版本 12.2 或更早版本生成的，则该证书的有效期为五年。否则，证书有效期限制为 397 天。在当前证书到期前 90 天，管理服务器会生成一个新证书作为备用证书。然后，新证书在过期日期一天前自动替换当前证书。客户端设备上的所有网络代理被自动配置以验证管理服务器新证书。

自定义证书

如果必要，您可以为管理服务器分配自定义证书。例如，为了更好的整合您企业的现有 PKI 或为了证书字段的自定义配置，这可能是必要的。

管理服务器证书的最长有效期不得超过 397 天。

当替换证书时，所有先前通过 SSL 连接到管理服务器的网络代理将丢失它们的连接，并将返回“管理服务器身份验证错误“。要消除该错误，您将必须在证书替换后恢复连接。

如果丢失了管理服务器证书，要想恢复该证书，必须重新安装管理服务器组件，然后还原数据。

如果您在不同的浏览器中打开 Kaspersky Security Center Web Console，并在管理服务器属性窗口中下载管理服务器证书文件，则下载的文件具有不同的名称。

对 Kaspersky Security Center 中使用的自定义证书的要求

下表显示了为不同的 Kaspersky Security Center 组件指定的自定义证书的要求。

Kaspersky Security Center 证书的要求

证书类别	要求	注释
通用证书，通用备用证书（“C”，“CR”）	最小密钥长度：2048 基本限制： • 路径长度限制：无 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法（可选）：服务器身份验证，客户端身份验证。	扩展密钥用法参数是可选的。 路径长度约束值可以是不同于“无”的整数，但不能小于 1。
移动证书，移动备用证书（“M”，“MR”）	最小密钥长度：2048 基本限制： • CA：true • 路径长度限制：无 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法（可选）：服务器身份验证。	扩展密钥用法参数是可选的。 如果通用证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。
自动生成的用户证书的证书 CA（“MCA”）	最小密钥长度：2048 基本限制： • CA：true • 路径长度限制：无 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法（可选）：服务器身份验证，客户端身份验证。	扩展密钥用法参数是可选的。 如果通用证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。
Web 服务器证书	扩展密钥用法：服务器身份验证。 从中指定证书的 PKCS #12/PEM 容器包括整个公钥链。 证书的使用者可选名称 (SAN) 存在；即，`subjectAltName` 字段的值有效。 证书符合浏览器对服务器证书施加的有效要求，以及 CA/浏览器论坛 的当前基线要求。	—
Kaspersky Security Center Web Console 证书	从中指定证书的 PEM 容器包括整个公钥链。 证书的使用者可选名称 (SAN) 存在；即，`subjectAltName` 字段的值有效。 证书符合浏览器对服务器证书的有效要求，以及 CA/浏览器论坛 的当前基线要求。	Kaspersky Security Center Web Console 不支持加密证书。

场景：指定自定义管理服务器证书

例如，您可以分配自定义管理服务器证书，以便更好地与贵司的现有公钥基础结构 (PKI) 集成，或自定义配置证书字段。最好在安装管理服务器后，快速启动向导完成之前立即替换证书。

管理服务器证书的最长有效期不得超过 397 天。

先决条件

以下条件必须得到满足：

- 新证书必须以 PKCS#12 格式创建（例如，通过组织的 PKI）。
- 对于新证书，必须满足下表中列出的要求。

  在下表中，请注意要求“CA: true”，这意味着新证书必须由受信任的证书颁发机构（CA）颁发。具有要求"CA: true"的新证书必须包含整个信任链和私钥，该私钥必须存储在扩展名为 pfx 或 p12 的文件中。

管理服务器证书的要求

证书类别	要求
普通证书，普通备用证书（“C”，“CR”）	最小密钥长度：2048 基本限制： • 路径长度限制：无 路径长度约束值可以是不同于“无”的整数，但不能小于 1。 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法 (EKU)：服务器身份验证，客户端身份验证。EKU 可选，但如果您的证书包含它，则必须在 EKU 中指定服务器和客户端身份验证数据。
移动证书，移动备用证书（“M”，“MR”）	最小密钥长度：2048 基本限制： • CA：true • 路径长度限制：无 如果通用证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法 (EKU)：服务器身份验证。EKU 可选，但如果您的证书包含它，则必须在 EKU 中指定服务器身份验证数据。

证书类别	要求
自动生成的用户证书的证书 CA（“MCA”）	最小密钥长度：2048 基本限制： • CA：true • 路径长度限制：无 如果普通证书的路径长度限制值不小于 1，则路径长度限制值可能是不同于“无”的整数。 密钥用法： • 数字签名 • 证书签名 • 密钥加密 • CRL 签名 扩展密钥用法 (EKU)：客户端身份验证。EKU 可选，但如果您的证书包含它，则必须在 EKU 中指定客户端身份验证数据。

公共 CA 颁发的证书没有证书签名权限。要使用此类证书，请确保您在网络中的分发点或连接网关上安装了网络代理版本 13 或更高版本。否则，您将无法在没有签名权限的情况下使用证书。

阶段

指定管理服务器证书分阶段进行：

1. **替换管理服务器证书**

   为此目的使用命令行 klsetsrvcert utility。

2. **指定新证书并恢复网络代理与管理服务器的连接**

   当证书被替换时，所有先前通过 SSL 连接到管理服务器的网络代理将丢失它们的连接，并返回“管理服务器身份验证错误。”要指定新证书和恢复连接，使用命令行 klmover utility。

3. **在 Kaspersky Security Center Web Console 的设置中指定新证书**

   更换证书后，在 Kaspersky Security Center Web Console 的设置中指定证书。否则，Kaspersky Security Center Web Console 将无法连接到管理服务器。

结果

当您结束场景时，管理服务器证书被替换，且服务器得到受管理设备上的网络代理验证。

使用 klsetsrvcert 实用程序替换管理服务器证书

要替换管理服务器证书：

从命令提示符运行以下实用程序：

```
klsetsrvcert [-t <证书类型> {-i <新证书路径> [-p <密码>] [-o <参数>] | -g <DNS 名称>}][-f <更换时间>][-r <根证书>][-l <日志文件路径>]
```

您无需下载 klsetsrvcert 实用程序。它包含在 Kaspersky Security Center 分发包中。它与以前的 Kaspersky Security Center 版本不兼容。

下表列出了 klsetsrvcert 实用程序参数的说明。

klsetsrvcert 实用工具参数值

参数	值
`-t <证书类型>`	要替换的证书类型。<证书类型>参数的可能值： • C—为端口 13000 和 13291 替换通用证书。 • CR—为端口 13000 和 13291 替换通用备用证书。 • M—在端口 13292 替换移动设备证书。 • MR—为端口 13292 替换移动备用证书。 • MCA—自动生成的用户证书的移动客户端 CA。
`-f <更换时间>`	更改证书的计划，使用格式“DD-MM-YYYY hh:mm”(对于端口 13000 和 13291)。 如果要在通用证书到期前用通用备用证书更换通用证书，请使用此参数。 指定受管理设备必须与新证书上的管理服务器同步的时间。
`-i <新证书路径>`	带有 PKCS#12 格式证书的容器（带有扩展名 .p12 或 .pfx 扩展名的文件）。
`-p <密码>`	用于保护 p12 容器的密码。 证书和私钥存储在容器中，因此需要密码才能解密带有容器的文件。
`-o <验证参数>`	证书验证参数（以分号分隔）。 要在没有签名权限的情况下使用自定义证书，请在 klsetsrvcert 实用程序中指定 `-o NoCA`。这对于公共 CA 颁发的证书很有用。 要更改证书类型 C 或 CR 的加密密钥长度，请在 klsetsrvcert 实用程序中指定 `-o RsaKeyLen:<密钥长度>`，其中 <密钥长度> 参数是所需的密钥长度值。否则，使用当前证书密钥长度。
`-g <DNS 名称>`	新证书将为指定 DNS 名称创建。
`-r <根证书>`	受信任的根证书颁发机构列表，格式 PEM。
`-l <日志文件路径>`	结果输出文件。默认下，输出被重定向到标准输出流。

例如，要指定“自定义管理服务器证书”，使用以下命令：

```
klsetsrvcert -t C -i <新证书路径> -p <密码> -o NoCA
```

证书替换后，所有通过 SSL 连接到管理服务器的网络代理都会失去连接。要恢复它，请使用命令行klmover utility。

为避免丢失网络代理连接，请使用以下命令：

1. 要安装新证书，请执行以下命令：

   ```
   klsetsrvcert.exe -t CR -i <新证书路径> -p <密码> -o NoCA
   ```

2. 要指定新证书的应用日期，请执行以下命令：

   ```
   klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
   ```

其中 "DD-MM-YYYY hh:mm" 是比当前日期晚 3-4 周的日期。将证书更改为新证书的时间偏移将允许将新证书被分发给所有网络代理。

使用 klmover 实用程序将网络代理连接到管理服务器

使用命令行 klsetsrvcert 实用程序替换管理服务器证书后，您需要在网络代理和管理服务器之间建立 SSL 连接，因为连接已断开。

要指定新的管理服务器证书并恢复连接：

从命令提示符运行以下实用程序：

```
klmover [-address <服务器地址>] [-pn <端口号>] [-ps <SSL端口号>] [-nossl] [-cert <证书文件路径>]
```

运行该实用程序需要管理员权限。

当网络代理安装在客户端设备上时，此实用程序会被自动复制到网络代理安装文件夹。

为了防止入侵者将设备移出管理服务器的控制，我们强烈建议为运行 klmover 实用程序启用密码保护。要启用密码保护，请在**网络代理策略设置使用卸载密码**使用卸载密码选项。

klmover 实用程序需要本地管理员权限。对于没有本地管理员权限操作的设备，可以忽略运行 klmover 实用程序的密码保护。

启用**使用卸载密码**选项还会为清理工具 (cleaner.exe) 启用密码保护。

对于通过连接网关连接到管理服务器的客户端设备，您不能使用 klmover 实用程序。对于这样的设备，您必须重新配置网络代理或重新安装网络代理并指定连接网关。

klmover 实用程序参数的描述如下表所示。

Klmover 实用程序参数值

参数	值
`-address <服务器地址>`	用于连接的管理服务器的地址。 您可以指定 IP 地址、NetBIOS 名称或 DNS 名称。
`-pn <端口号>`	用来建立与管理服务器的非加密连接的端口号。 默认端口号是 14000。
`-ps <SSL 端口号>`	使用 SSL 与管理服务器建立加密连接时使用的 SSL 端口号。 默认端口号是 13000。
`-nossl`	使用非加密连接管理服务器。 如果未使用该键值，网络代理将通过使用加密的 SSL 协议连接至管理服务器。
`-cert <证书文件的路径>`	访问管理服务器时使用指定的证书文件作为身份验证。
`-virtserv`	虚拟管理服务器的名称。

参数	值
`-cloningmode`	网络代理磁盘克隆模式。 使用以下参数之一配置磁盘克隆模式： • `-cloningmode`—请求磁盘克隆模式的状态。 • `-cloningmode 1`—启用磁盘克隆模式。 • `-cloningmode 0`—禁用磁盘克隆模式。
`-nauninstpwd <密码>`	使用此参数指定网络代理卸载密码。 该参数不是必需的。

例如，要将网络代理连接到管理服务器，则运行以下命令：

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

重新颁发 Web 服务器证书

发布后续下载到受管理设备的网络代理安装包以及发布 iOS MDM 配置文件、iOS 应用和 Kaspersky Endpoint Security for Mobile 安装包都需要 Kaspersky Security Center 中使用的 Web 服务器证书。根据当前的应用程序配置，可以使用不同的证书作为 Web 服务器证书（有关详细信息，请参阅“关于 Kaspersky Security Center 证书”）。

在开始升级应用程序之前，您可能需要重新颁发 Web 服务器证书以满足您组织的特定安全要求或保持受管理设备的持续连接。Kaspersky Security Center 提供了两种重新颁发 Web 服务器证书的方式；两种方法之间的选择取决于您是否通过移动协议（即，通过使用移动证书）连接和管理移动设备。

如果您从未在管理服务器属性窗口的“**Web 服务器**”区域中将您自己的自定义证书指定为 Web 服务器证书，则移动证书将用作 Web 服务器证书。在这种情况下，通过重新颁发移动协议本身来重新颁发 Web 服务器证书。

要在未通过移动协议管理移动设备的情况下重新颁发 Web 服务器证书：

1. 在控制台树中，右键单击相关管理服务器的名称，然后在上下文菜单中选择“**属性**”。
2. 在打开的管理服务器属性窗口的左侧窗格中，选择“**管理服务器连接设置**”区域。
3. 在子区域列表中，选择“**证书**”子区域。
4. 如果您计划继续使用 Kaspersky Security Center 颁发的证书，请执行以下操作：
   a. 在右侧窗格的“**管理服务器的移动设备身份验证**”设置组中，选择“**通过管理服务器发布的证书**”选项，然后单击“**重新发布**”按钮。
   b. 在打开的“**重新发布证书**”窗口的“**连接地址**”和“**激活条款**”设置组中，选择相关选项，然后单击“**确定**”。
   c. 在确认窗口中，单击“**是**”。

   或者，如果您计划使用自己的自定义证书，请执行以下操作：
   a. 检查您的自定义证书是否满足 Kaspersky Security Center 的要求和 Apple 可信证书的要求。如有必要，请修改证书。
   b. 选择“**其他证书**”选项，然后单击“**浏览**”按钮。

c. 在打开的“**证书**”窗口的“**证书类型**”字段中选择证书的类型，然后指定证书位置和设置：

- 如果选择了“**PKCS #12 容器**”，则单击“**证书文件**”字段旁边的“**浏览**”按钮，然后指定硬盘驱动器上的证书文件。如果证书文件受密码保护，请在“**密码(如果有)**”字段中输入密码。
- 如果选择了“**X.509 证书**”，则单击“**私钥(.prk, .pem)**”字段旁边的“**浏览**”按钮，然后指定硬盘驱动器上的私钥。如果私钥受密码保护，请在“**密码(如果有)**”字段中输入密码。然后单击“**公钥(.cer)**”字段旁边的“**浏览**”按钮，并指定硬盘驱动器上的私钥。

d. 在“**证书**”窗口中，单击“**确定**”。

e. 在确认窗口中，单击“**是**”。

移动证书已重新颁发以用作 Web 服务器证书。

要在已通过移动协议管理移动设备的情况下重新颁发 Web 服务器证书：

1. 生成自定义证书，并准备好在 Kaspersky Security Center 中使用。检查您的自定义证书是否满足 Kaspersky Security Center 的要求和 Apple 可信证书的要求。如有必要，请修改证书。
2. 在控制台树中，右键单击相关管理服务器的名称，然后在上下文菜单中选择“**属性**”。
3. 在打开的管理服务器属性窗口的左侧窗格中，选择“**Web 服务器**”区域。
4. 在“**通过 HTTPS**”菜单中，选择“**指定其他证书**”选项。
5. 在“**通过 HTTPS**”菜单中，单击“**更改**”按钮。
6. 在打开的“**证书**”窗口的“**证书类型**”字段中，选择您的证书类型：
   - 如果选择了“**PKCS #12 容器**”，则单击“**证书文件**”字段旁边的“**浏览**”按钮，然后指定硬盘驱动器上的证书文件。如果证书文件受密码保护，请在“**密码(如果有)**”字段中输入密码。
   - 如果选择了“**X.509 证书**”，则单击“**私钥(.prk, .pem)**”字段旁边的“**浏览**”按钮，然后指定硬盘驱动器上的私钥。如果私钥受密码保护，请在“**密码(如果有)**”字段中输入密码。然后单击“**公钥(.cer)**”字段旁边的“**浏览**”按钮，并指定硬盘驱动器上的私钥。
7. 在“**证书**”窗口中，单击“**确定**”。
8. 如有必要，在管理服务器属性窗口的“**Web 服务器 HTTPS 端口**”字段中，更改 Web 服务器的 HTTPS 端口号。单击“**确定**”。

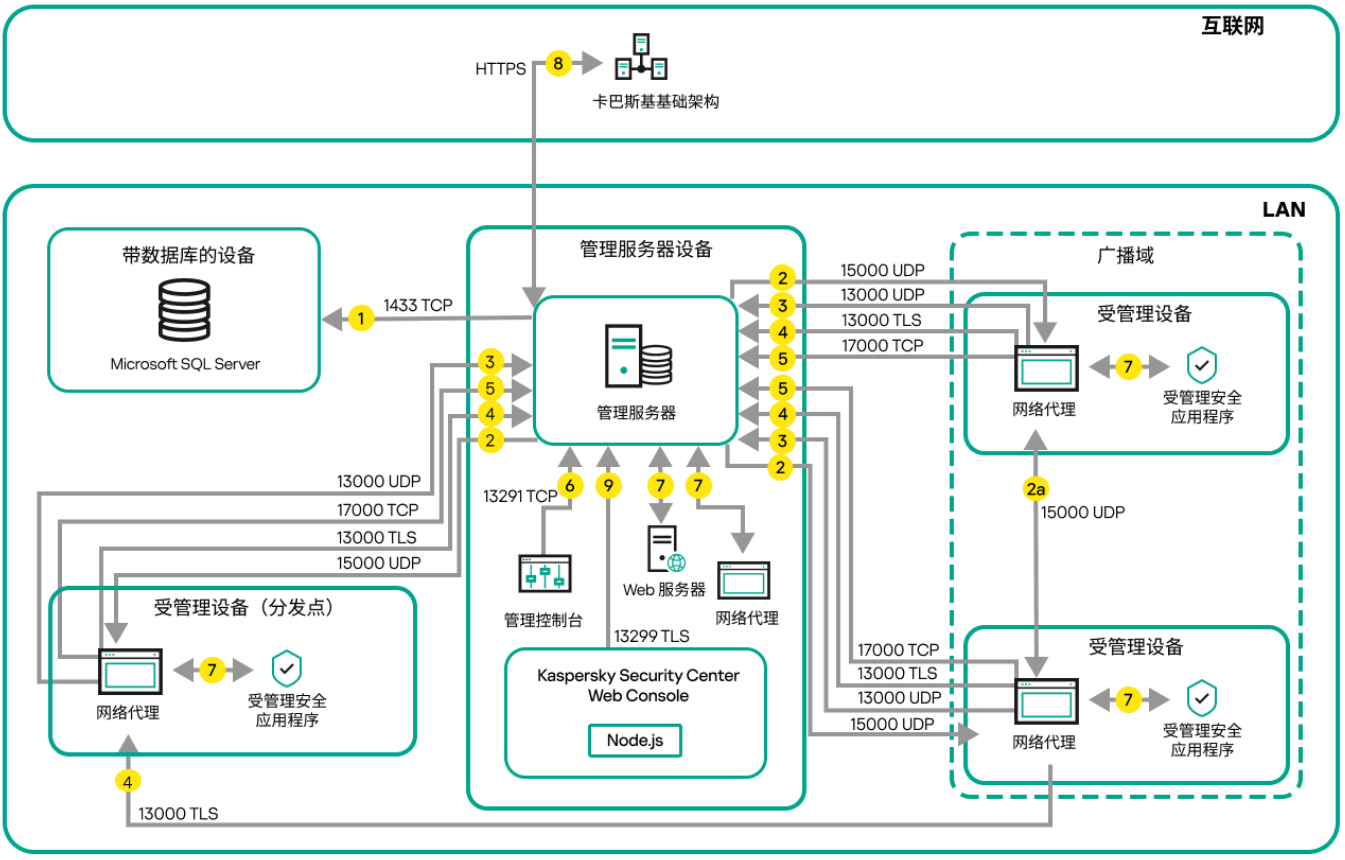
   Web 服务器证书已重新颁发。

数据流量和端口使用的 schema

该部分提供了 Kaspersky Security Center 组件、受管理安全应用程序和不同配置下的外部服务器之间的数据流量 schema。该 schema 使用在本地设备上必须可用的端口号提供。

LAN 中的管理服务器和受管理设备

下图显示 Kaspersky Security Center 仅在局域网 (LAN) 中被部署时的数据流量。



局域网 (LAN) 中的管理服务器和受管理设备

该图片显示了受管理设备连接到管理服务器的不同方式：直接或通过分发点。分发点降低发布更新时管理服务器的负载并优化网络流量。然而，分发点仅在受管理设备数量足够大时被需要。如果受管理设备数量较小，所有受管理设备可以从管理服务器直接接收更新。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server，端口 1433 用于 Microsoft SQL Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 TLS 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 TLS 端口 14000 从网络代理接收连接。Kaspersky Security Center 也支持通过端口 14000 连接网络代理，但推荐使用 TLS 端口 13000。

分发点在早期 Kaspersky Security Center 版本中被叫做更新代理。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. 来自基于 MMC 的管理控制台的数据通过端口 13291 传输到管理服务器（管理控制台可以安装在同一设备上，也可以安装在不同的设备上。）

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

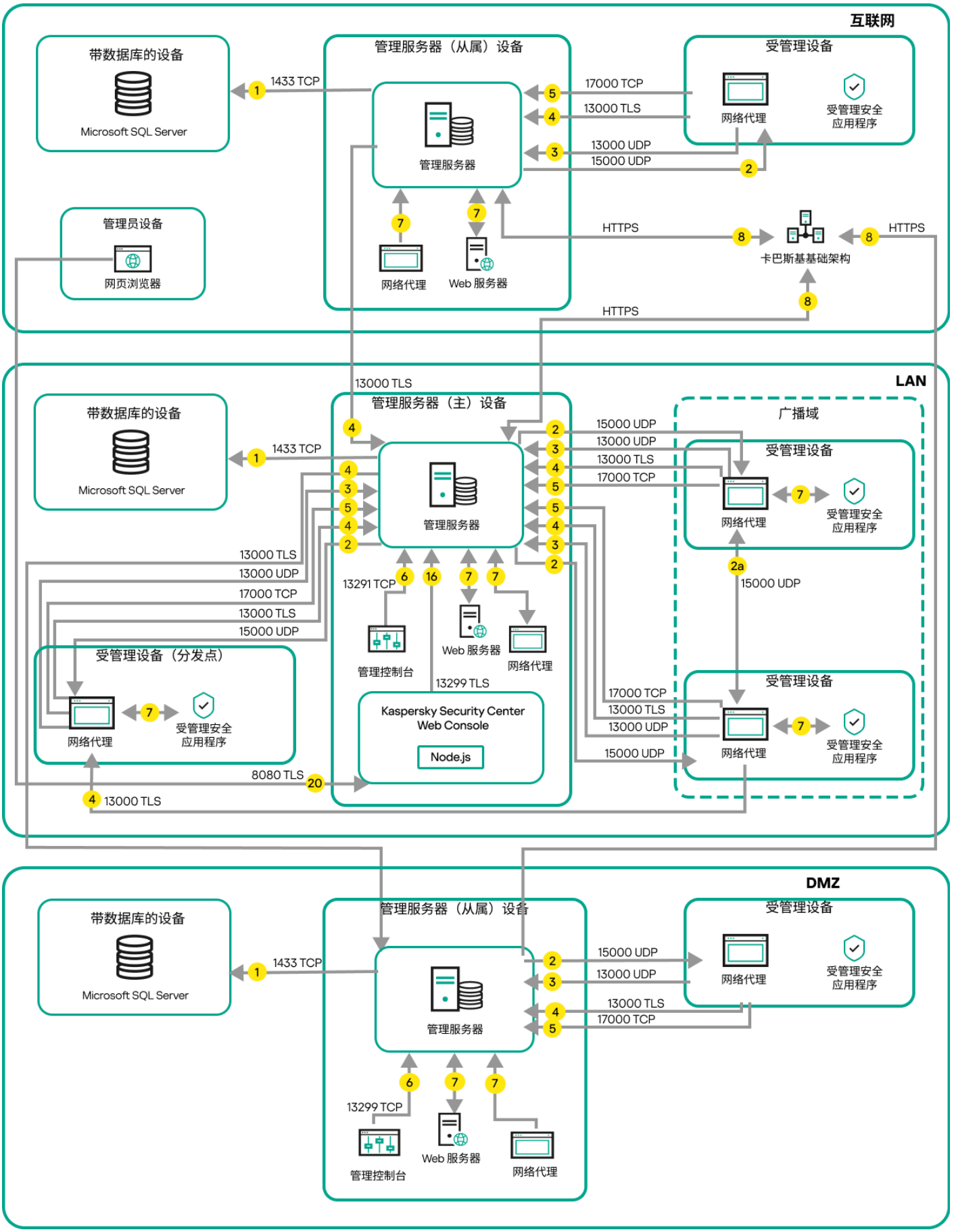
8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

局域网中的主管理服务器和两个从属管理服务器

下图显示管理服务器层级：主管理服务器位于局域网 (LAN)。一个从属管理服务器位于 DMZ；另一个从属管理服务器位于互联网。



管理服务器层级：主管理服务器和两个从属管理服务器

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server，端口 1433 用于 Microsoft SQL Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 TLS 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 TLS 端口 14000 从网络代理接收连接。Kaspersky Security Center 也支持通过端口 14000 连接网络代理，但推荐使用 TLS 端口 13000。

   > 分发点在早期 Kaspersky Security Center 版本中被叫做更新代理。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. 来自基于 MMC 的管理控制台的数据通过端口 13291 传输到管理服务器（管理控制台可以安装在同一设备上，也可以安装在不同的设备上。）

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

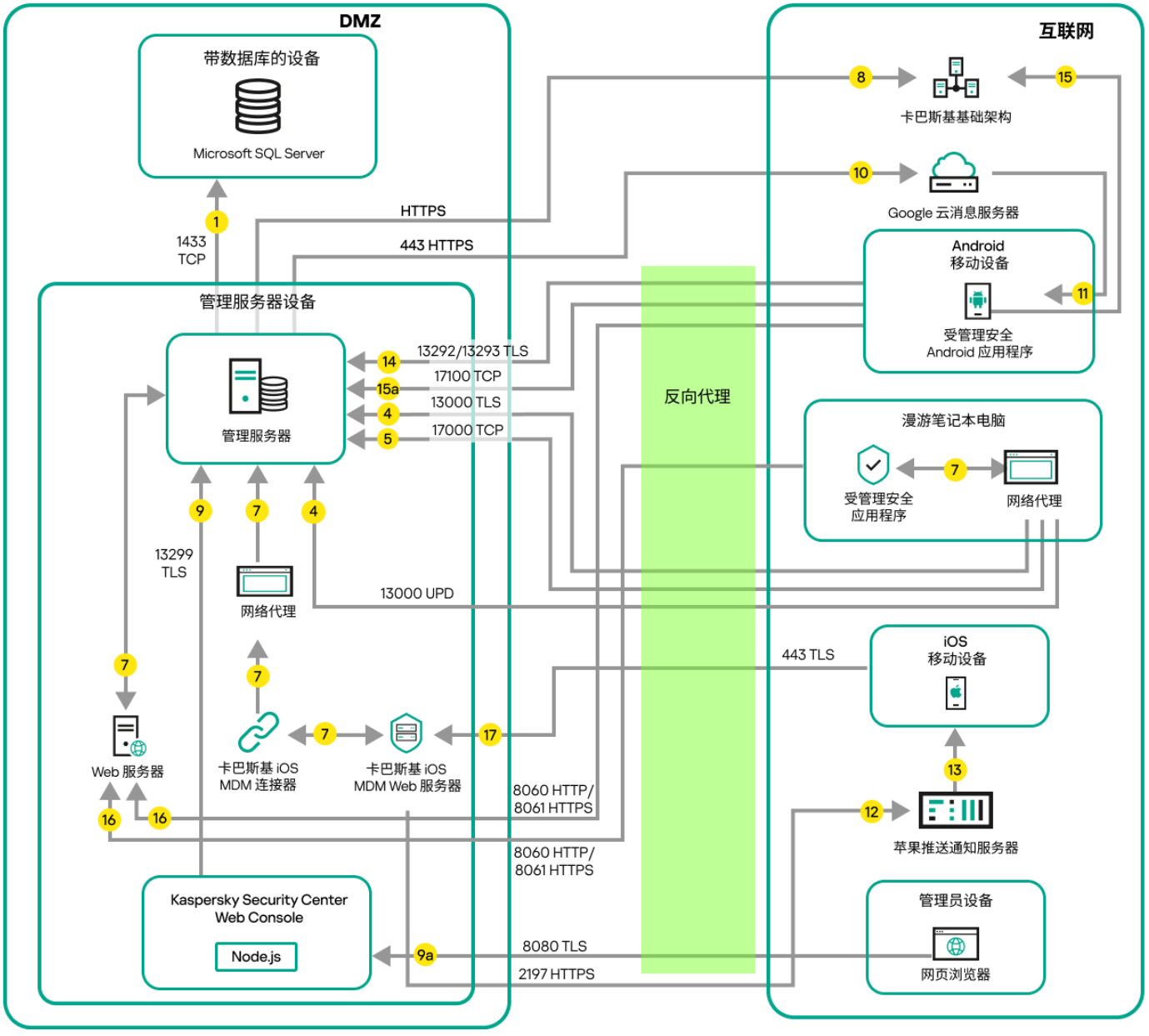
   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   9a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

管理服务器位于 LAN、受管理设备位于互联网、反向代理使用中

下图显示管理服务器处于局域网中且受管理设备，包括移动设备都在互联网中时的数据流量。在此图中，您选择的反向代理正在使用中。请参考应用程序的文档了解详情。



管理服务器位于局域网；受管理设备通过反向代理连接到管理服务器

如果您不想让移动设备直接连接到管理服务器，且不想在 DMZ 中分配连接网关，则该部署方案被推荐。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server，端口 1433 用于 Microsoft SQL Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 TLS 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 TLS 端口 14000 从网络代理接收连接。Kaspersky Security Center 也支持通过端口 14000 连接网络代理，但推荐使用 TLS 端口 13000。

   > 分发点在早期 Kaspersky Security Center 版本中被叫做更新代理。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. 来自基于 MMC 的管理控制台的数据通过端口 13291 传输到管理服务器（管理控制台可以安装在同一设备上，也可以安装在不同的设备上。）

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   9a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

10. 仅对 Android 移动设备：来自管理服务器的数据被传输到 Google 服务器。该连接用于通知 Android 移动设备他们需要连接到管理服务器。然后推送通知被发送到移动设备。

11. 仅对 Android 移动设备：来自 Google 服务器的推送通知被发送到移动设备。该连接用于通知移动设备他们需要连接到管理服务器。

12. 仅对 iOS 移动设备：来自 iOS MDM 服务器的数据被发送到 Apple 推送通知服务器。然后推送通知被发送到移动设备。

13. 仅对 iOS 移动设备：推送通知从 App 服务器被发送到移动设备。该连接用于通知 iOS 移动设备他们需要连接到管理服务器。

14. 仅对移动设备：来自受管理应用程序的数据通过 TLS 端口 13292 / 13293 被传输到管理服务器（或连接网关）— 直接或通过反向代理。

15. 仅对移动设备：来自移动设备的数据被传输到 Kaspersky 基础架构。

    > 如果移动设备没有互联网访问，数据通过端口 17100 发送到管理服务器，然后管理服务器将其发送到 Kaspersky 基础架构；然而，该方案很少被应用。

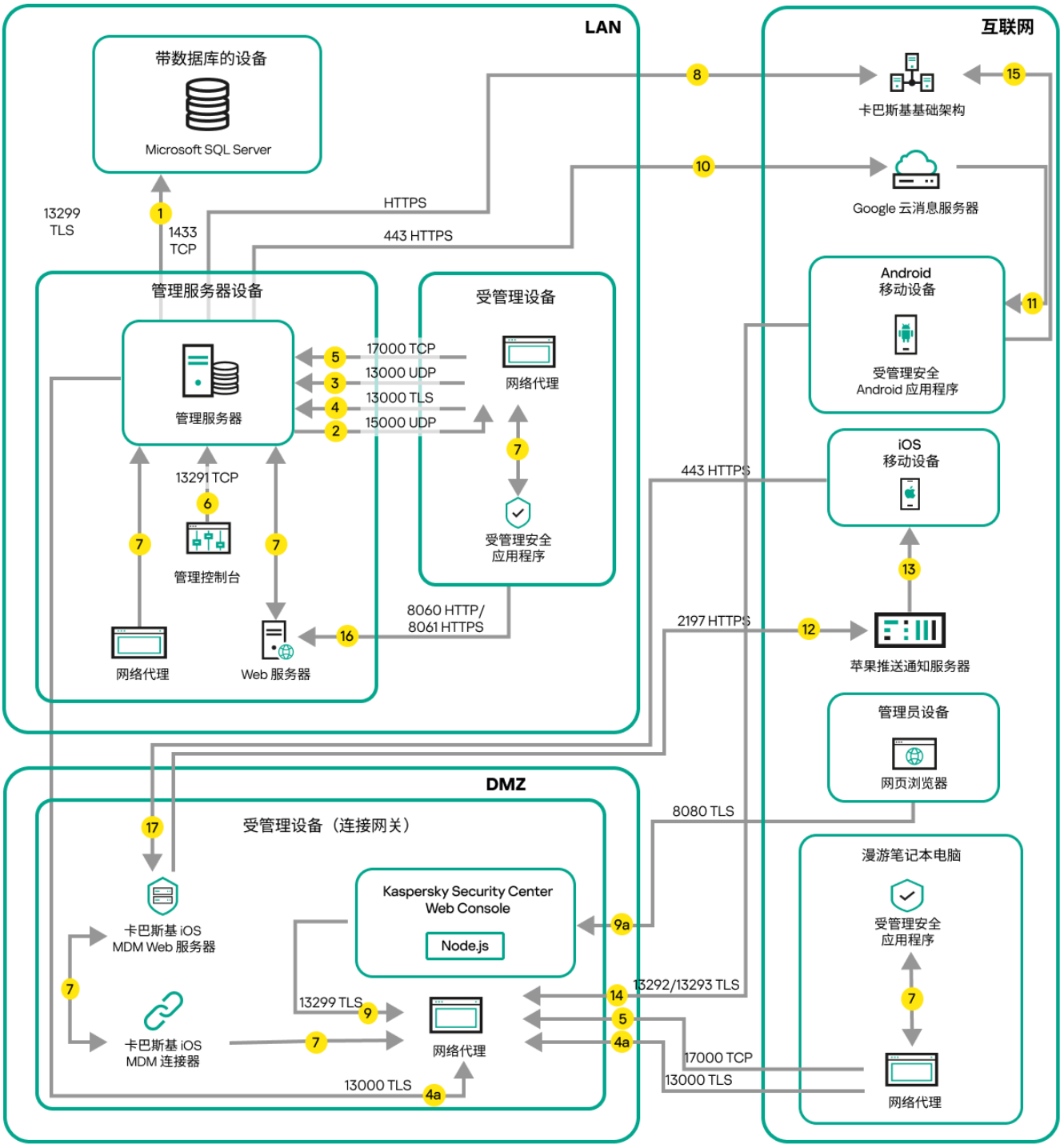
16. 来自受管理设备，包括移动设备的包请求被传输到 Web 服务器，该服务器位于管理服务器所在设备。

17. 仅针对 iOS 移动设备：来自移动设备的数据通过 TLS 端口 443 传输到 iOS MDM 服务器，该服务器与管理服务器位于同一设备上或位于连接网关上。

管理服务器位于 LAN、受管理设备位于互联网、连接网关使用中

下图显示管理服务器处于局域网中且受管理设备，包括移动设备都在互联网中时的数据流量。连接网关使用中。

如果您不想让移动设备直接连接到管理服务器，且不想使用反向代理或企业防火墙，则推荐采用该部署方案。



受管理移动设备通过连接网关连接到管理服务器

在该图中，受管理设备通过 DMZ 中的连接网关连接到管理服务器。未使用反向代理或企业防火墙。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server，端口 1433 用于 Microsoft SQL Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 TLS 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 TLS 端口 14000 从网络代理接收连接。Kaspersky Security Center 也支持通过端口 14000 连接网络代理，但推荐使用 TLS 端口 13000。

   > 分发点在早期 Kaspersky Security Center 版本中被叫做更新代理。

   4a.DMZ 中的连接网关还会通过 TLS 端口 13000 从管理服务器接收连接。由于 DMZ 中的连接网关无法访问管理服务器的端口，因此管理服务器会创建并维护与连接网关的永久信号连接。该信号连接不用于数据传输，仅用于发送网络交互邀请。当连接网关需要连接到服务器时，它将通过此信号连接通知服务器，然后服务器创建数据传输所需的连接。

   漫游设备也通过 TLS 端口 13000 连接到连接网关。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. 来自基于 MMC 的管理控制台的数据通过端口 13291 传输到管理服务器（管理控制台可以安装在同一设备上，也可以安装在不同的设备上。）

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   9a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

10. 仅对 Android 移动设备：来自管理服务器的数据被传输到 Google 服务器。该连接用于通知 Android 移动设备他们需要连接到管理服务器。然后推送通知被发送到移动设备。

11. 仅对 Android 移动设备：来自 Google 服务器的推送通知被发送到移动设备。该连接用于通知移动设备他们需要连接到管理服务器。

12. 仅对 iOS 移动设备：来自 iOS MDM 服务器的数据被发送到 Apple 推送通知服务器。然后推送通知被发送到移动设备。

13. 仅对 iOS 移动设备：推送通知从 App 服务器被发送到移动设备。该连接用于通知 iOS 移动设备他们需要连接到管理服务器。

14. 仅对移动设备：来自受管理应用程序的数据通过 TLS 端口 13292 / 13293 被传输到管理服务器（或连接网关）— 直接或通过反向代理。

15. 仅对移动设备：来自移动设备的数据被传输到 Kaspersky 基础架构。

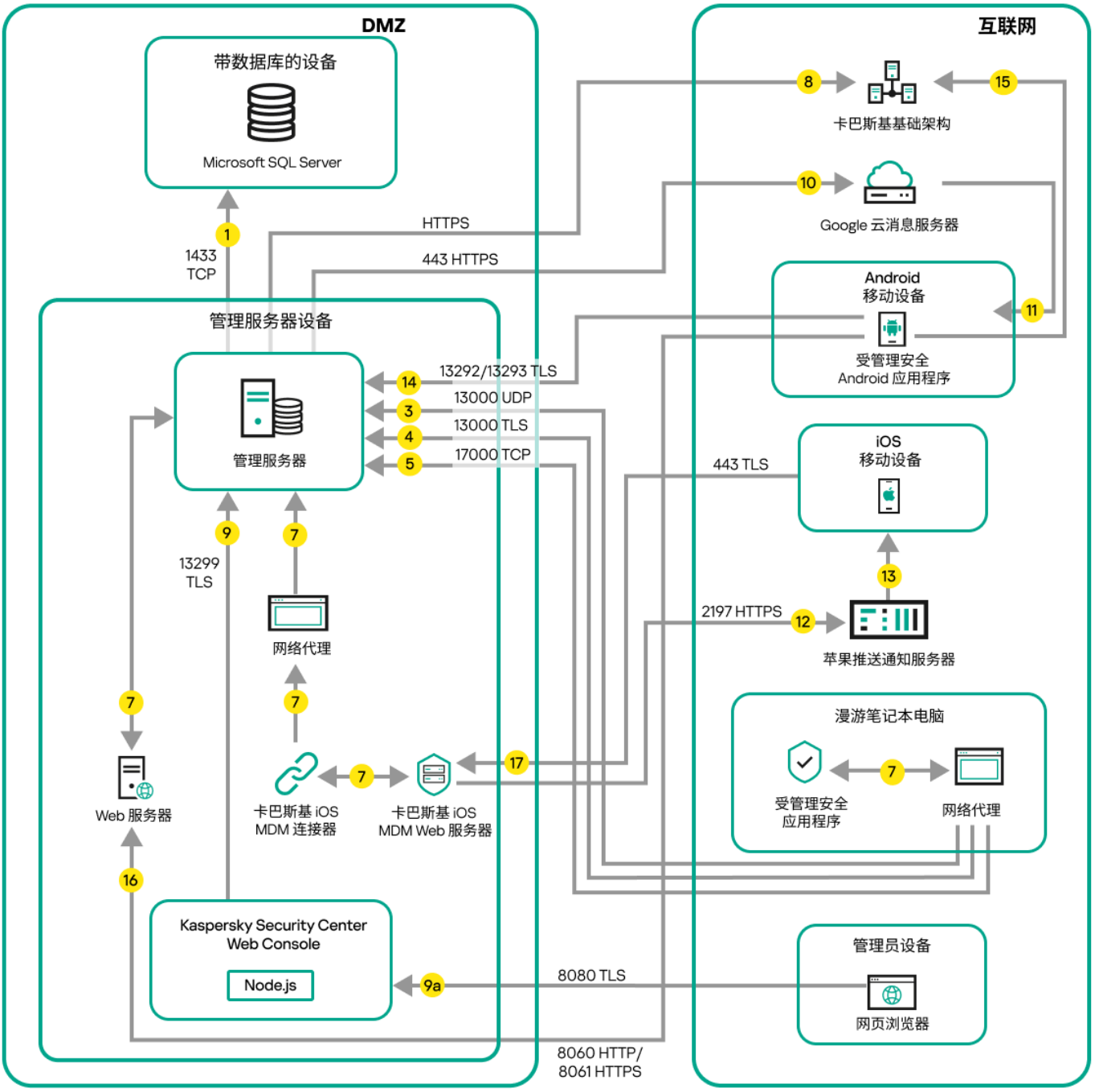
    如果移动设备没有互联网访问，数据通过端口 17100 发送到管理服务器，然后管理服务器将其发送到 Kaspersky 基础架构；然而，该方案很少被应用。

16. 来自受管理设备，包括移动设备的包请求被传输到 Web 服务器，该服务器位于管理服务器所在设备。

17. 仅针对 iOS 移动设备：来自移动设备的数据通过 TLS 端口 443 传输到 iOS MDM 服务器，该服务器与管理服务器位于同一设备上或位于连接网关上。

管理服务器位于 DMZ、受管理设备位于互联网

下图显示管理服务器处于 DMZ 中且受管理设备，包括移动设备，都在互联网中时的数据流量。



管理服务器位于 DMZ、受管理移动设备位于互联网

在该图像中，未使用连接网关：移动设备直接连接到管理服务器。

箭头表示流量的开始：每个箭头从发起连接的设备指向"回答"请求的设备。端口号和用于数据传输的协议名称被提供。每个箭头都有数字标签，对应的数据流量详情是：

1. 管理服务器发送数据到数据库。如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server，端口 1433 用于 Microsoft SQL Server）。请参阅 DBMS 文档以获取相关信息。

2. 来自管理服务器的通信请求被传输到所有非移动受管理设备，通过 UDP 端口 15000。

   网络代理在一个广播域内相互发送请求。然后将数据发送到管理服务器，并用于定义广播域的限制和分发点的自动分配（如果启用了此选项）。

   如果管理服务器无法直接访问受管理设备，则不会直接发送从管理服务器到这些设备的通信请求。

3. 受管理设备关闭的信息通过 UDP 端口 13000 被从网络代理传输到管理服务器。

4. 管理服务器通过 TLS 端口 13000 从网络代理和从属管理服务器接收连接。

   如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 TLS 端口 14000 从网络代理接收连接。Kaspersky Security Center 也支持通过端口 14000 连接网络代理，但推荐使用 TLS 端口 13000。

   > 分发点在早期 Kaspersky Security Center 版本中被叫做更新代理。

5. 受管理设备（除了移动设备）通过 TCP 端口 17000 请求激活。如果设备自己拥有互联网连接，则不必要；此种情况下，设备直接通过互联网发送数据到 Kaspersky 服务器。

6. 来自基于 MMC 的管理控制台的数据通过端口 13291 传输到管理服务器（管理控制台可以安装在同一设备上，也可以安装在不同的设备上。）

7. 单一设备上的应用程序交换本地流量（在管理服务器上或受管理设备上）。不需要打开任何外部端口。

8. 从管理服务器到 Kaspersky 服务器的数据（例如 KSN 数据或授权许可信息）和从 Kaspersky 服务器到管理服务器的数据（例如应用程序更新和反病毒数据库更新）使用 HTTPS 协议传输。

   如果您不想让您的管理服务器拥有互联网连接，您必须手动管理该数据。

9. Kaspersky Security Center Web Console 服务器通过 TLS 端口 13299 发送数据到管理服务器，该管理服务器可能被安装到相同或不同设备。

   9a.来自 Web 浏览器（安装在管理员的其他设备）的数据通过 TLS 端口 8080 传输到 Kaspersky Security Center Web Console 服务器。Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

10. 仅对 Android 移动设备：来自管理服务器的数据被传输到 Google 服务器。该连接用于通知 Android 移动设备他们需要连接到管理服务器。然后推送通知被发送到移动设备。

11. 仅对 Android 移动设备：来自 Google 服务器的推送通知被发送到移动设备。该连接用于通知移动设备他们需要连接到管理服务器。

12. 仅对 iOS 移动设备：来自 iOS MDM 服务器的数据被发送到 Apple 推送通知服务器。然后推送通知被发送到移动设备。

13. 仅对 iOS 移动设备：推送通知从 App 服务器被发送到移动设备。该连接用于通知 iOS 移动设备他们需要连接到管理服务器。

14. 仅对移动设备：来自受管理应用程序的数据通过 TLS 端口 13292 / 13293 被传输到管理服务器（或连接网关）— 直接或通过反向代理。

15. 仅对移动设备：来自移动设备的数据被传输到 Kaspersky 基础架构。

    如果移动设备没有互联网访问，数据通过端口 17100 发送到管理服务器，然后管理服务器将其发送到 Kaspersky 基础架构；然而，该方案很少被应用。

16. 来自受管理设备，包括移动设备的包请求被传输到 Web 服务器，该服务器位于管理服务器所在设备。

17. 仅针对 iOS 移动设备：来自移动设备的数据通过 TLS 端口 443 传输到 iOS MDM 服务器，该服务器与管理服务器位于同一设备上或位于连接网关上。

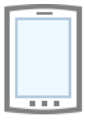
Kaspersky Security Center 组件和安全应用程序的交互：更多信息

该部分提供了与 Kaspersky Security Center 组件和受管理安全应用程序交互的方案。方案提供了必须可用的端口号和打开这些端口的进程名称。

交互模式中的惯例

下表提供了方案中使用的转换。

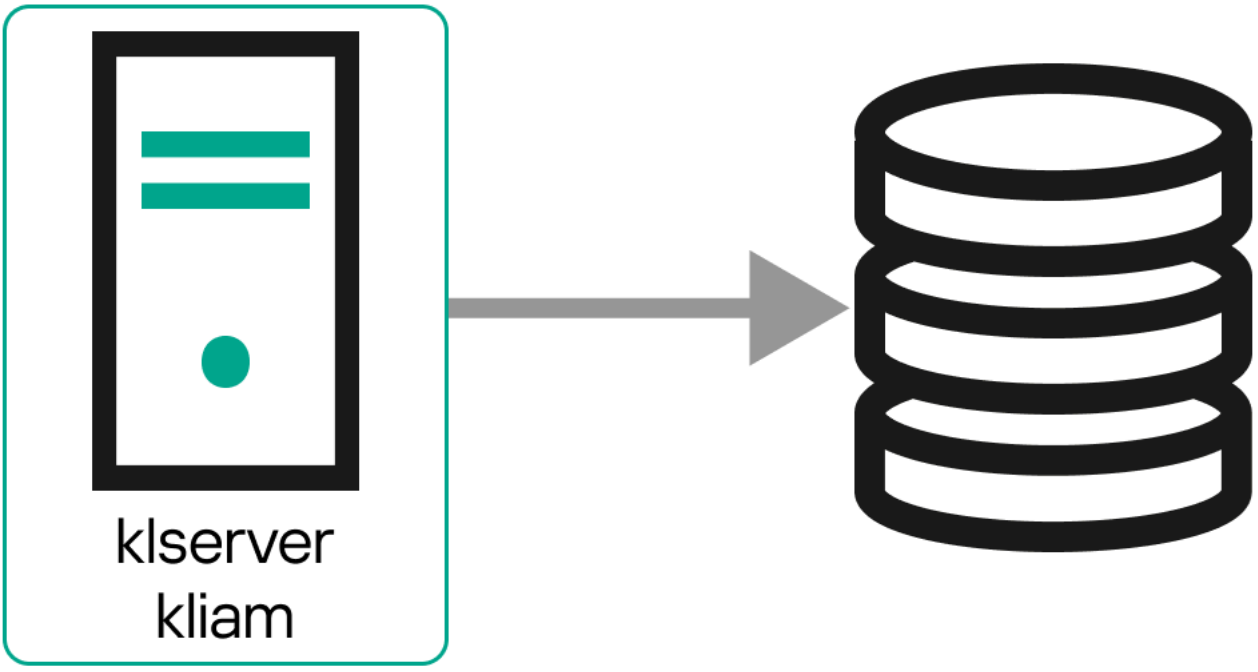
文档约定

图标	含义
	管理服务器
	从属管理服务器
	DBMS
	客户端设备(安装了网络代理和 Kaspersky Endpoint Security 系列应用程序，或 Kaspersky Security Center 可以管理的其他应用程序)
	连接网关
	分发点
	安装了 Kaspersky Security for Mobile 的移动客户端设备

	用户设备上的浏览器
	运行在设备和打开端口的进程
	端口和其号码
	TCP 流量（箭头方向显示流量方向）
	TCP 流量(箭头方向显示流量方向)
	COM 调用
	DBMS 传输
	DMZ 边界

管理服务器和 DBMS

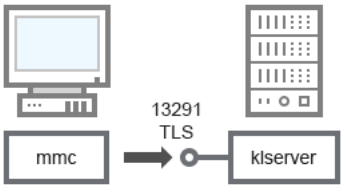
管理服务器数据输入到 SQL Server、MySQL 或 MariaDB 数据库。



管理服务器和 DBMS

如果您在不同设备上安装管理服务器和数据库，您必须使数据库所在设备的必要端口可用（例如，端口 3306 用于 MySQL Server，端口 1433 用于 Microsoft SQL Server）。请参阅 DBMS 文档以获取相关信息。

管理服务器和管理控制台



管理服务器和管理控制台

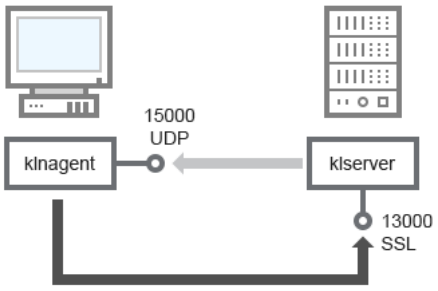
对于方法描述，参见下表。

管理服务器和管理控制台（流量）

设备	端口号	打开端口的进程名称	协议	TLS	端口目的
管理服务器	13291	klserver	TCP	是	从管理控制台接收连接

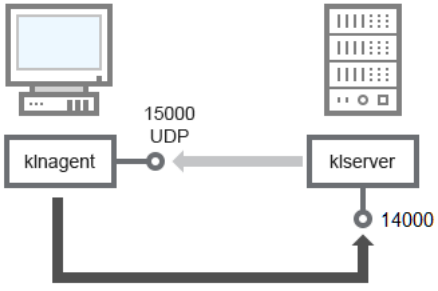
管理服务器和客户端设备：管理安全应用程序

管理服务器通过 SSL 端口 13000 从网络代理接收连接（参见下图）。



管理服务器和客户端设备：管理安全应用程序、通过端口 13000 连接（推荐）

如果您使用 Kaspersky Security Center 的早期版本，您网络中的管理服务器可以通过非 SSL 端口 14000 从网络代理接收连接（参见下图）。Kaspersky Security Center 15.1 也支持通过端口 14000 连接网络代理，尽管使用 SSL 端口 13000 是被推荐的。



管理服务器和客户端设备：管理安全应用程序、通过端口 14000 连接（低安全级）

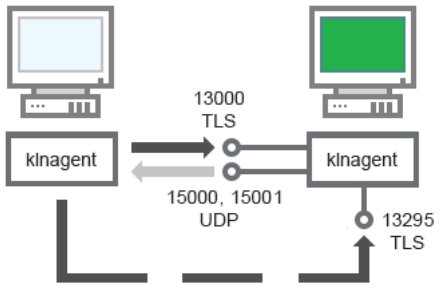
为了澄清方案，参见下图。

管理服务器和客户端设备：管理安全应用程序（流量）

设备	端口号	打开端口的进程名称	协议	TLS (仅对 TCP)	端口目的
网络代理	15000	klnagent	UDP	Null	网络代理多点传送
管理服务器	13000	klserver	TCP	是	接收从网络代理的连接
管理服务器	14000	klserver	TCP	否	接收从网络代理的连接

通过分发点在客户端设备上升级软件

客户端设备通过端口 13000 连接到分发点，如果您将分发点用作推送服务器，则还通过端口 13295 进行连接；分发点通过端口 15000 多播到网络代理（请参见下图）。更新和安装包通过端口 15001 从分发点接收。



通过分发点在客户端设备上升级软件

对于方法描述，参见下表。

通过分发点升级软件（流量）

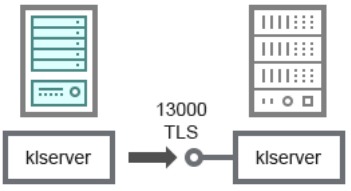
设备	端口号	打开端口的进程名称	协议	TLS (仅对 TCP)	端口目的
网络代理	15000	klnagent	UDP	Null	网络代理多点传送
网络代理	15001	klnagent	UDP	Null	从分发点接收更新和安装包
分发点	13000	klnagent	TCP	是	接收从网络代理的连接
分发点	13295	klnagent	TCP	是	（推送服务器）接收来自客户端设备的连接

管理服务器层级：主管理服务器和从属管理服务器

方案（参见下图）显示了如何使用端口 13000 确保层级中管理服务器之间的交互。

当组合两个管理服务器到一个层级，确保端口 13291 在两个管理服务器上都可以访问。通过端口 13291 连接管理控制台到管理服务器。

此后，当管理服务器组合到层级时，您将可以使用连接到主管理服务器的管理控制台管理两个管理服务器。因此，主管理服务器端口 13291 的可访问性是仅有的前提。



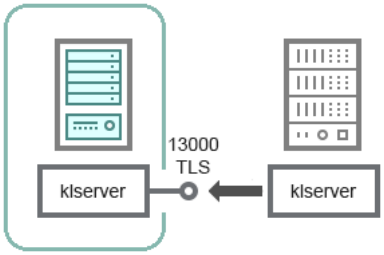
管理服务器层级：主管理服务器和从属管理服务器

对于方法描述，参见下表。

管理服务器层级（流量）

设备	端口号	打开端口的进程名称	协议	TLS	端口目的
主管理服务器	13000	klserver	TCP	是	从从属管理服务器接收连接

DMZ 中带有从属管理服务器的管理服务器层级



DMZ 中带有从属管理服务器的管理服务器层级

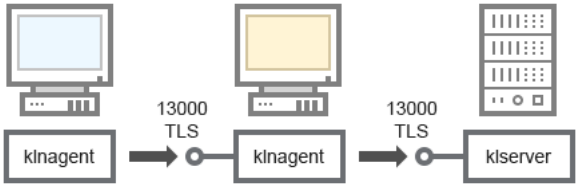
方案显示了管理服务器层级，其中 DMZ 中的从属管理服务器从主管理服务器接收连接（有关方案说明，请参见下表）。当组合两个管理服务器到一个层级，确保端口 13291 在两个管理服务器上都可以访问。通过端口 13291 连接管理控制台到管理服务器。

此后，当管理服务器组合到层级时，您将可以使用连接到主管理服务器的管理控制台管理两个管理服务器。因此，主管理服务器端口 13291 的可访问性是仅有的前提。

DMZ 中带有从属管理服务器的管理服务器层级（流量）

设备	端口号	打开端口的进程名称	协议	TLS	端口目的
从属管理服务器	13000	klserver	TCP	是	从主管理服务器接收连接

管理服务器、网段连接网关和客户端设备



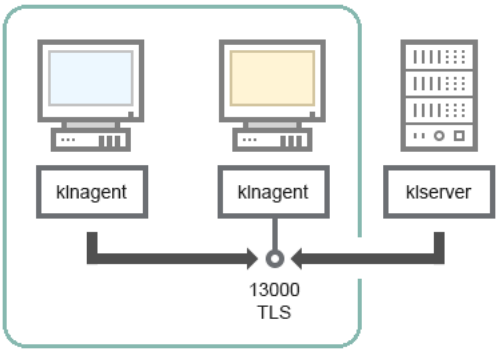
管理服务器、网段连接网关和客户端设备

对于方法描述，参见下表。

管理服务器、网段连接网关和客户端设备（流量）

设备	端口号	打开端口的进程名称	协议	TLS	端口目的
管理服务器	13000	klserver	TCP	是	接收从网络代理的连接
网络代理	13000	klnagent	TCP	是	接收从网络代理的连接

管理服务器和 DMZ 中的两台设备：连接网关和客户端设备



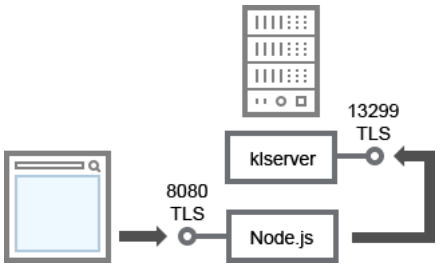
带有连接网关的管理服务器和 DMZ 中的客户端设备

对于方法描述，参见下表。

带有网段连接网关的管理服务器和客户端设备（流量）

设备	端口号	打开端口的进程名称	协议	TLS	端口目的
网络代理	13000	klnagent	TCP	是	接收从网络代理的连接

管理服务器和 Kaspersky Security Center Web Console



管理服务器和 Kaspersky Security Center Web Console

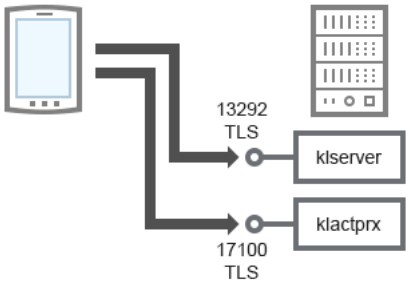
对于方法描述，参见下表。

管理服务器和 Kaspersky Security Center Web Console（流量）

设备	端口号	打开端口的进程名称	协议	TLS	端口目的
管理服务器	13299	klserver	TCP	是	接收通过 OpenAPI 从 Kaspersky Security Center Web Console 到管理服务器的连接
Kaspersky Security Center Web Console 服务器或管理服务器	8080	Node.js：服务器端 JavaScript	TCP	是	从 Kaspersky Security Center Web Console 接收连接

Kaspersky Security Center Web Console 可以安装到管理服务器或其他设备。

激活和管理移动设备上的安全应用程序



激活和管理移动设备上的安全应用程序

对于方法描述，参见下表。

激活和管理移动设备上的安全应用程序（流量）

设备	端口号	打开端口的进程名称	协议	TLS	端口目的
管理服务器	13292	klserver	TCP	是	接收从管理控制台到管理服务器的连接
管理服务器	17100	klactprx	TCP	是	接收移动设备的应用程序激活连接

部署最佳实践

Kaspersky Security Center 是一个分发的应用程序。Kaspersky Security Center 包含以下应用程序：

- 管理服务器 — 核心组件，设计用于管理组织设备和在 DBMS 中存储数据。
- 管理控制台 — 管理员基本工具。管理控制台与管理服务器一起出货，但是它也可以被单独安装在一个或几个由管理员运行的设备上。
- 网络代理 — 设计用于管理安装在设备上的安全应用程序，同时获取设备信息并传输该信息到管理服务器。网络代理安装在组织设备上。

Kaspersky Security Center 在组织网络上的部署运行如下：

- 管理服务器的安装
- 管理员设备上管理控制台的安装
- 网络代理和企业设备上安全应用程序的安装

强化指南

Kaspersky Security Center 设计用于在组织网络中集中执行基本的管理和维护任务。该应用程序使管理员可以访问有关组织网络安全级别的详细信息。Kaspersky Security Center 允许您配置使用卡巴斯基应用程序构建的所有保护组件。

Kaspersky Security Center 管理服务器拥有对客户端设备保护管理的完全访问权限，是组织安全系统中最重要的组件。因此，管理服务器需要增加保护方法。

配置之前，请使用管理服务器数据备份任务或 klbackup 实用程序创建 Kaspersky Security Center 管理服务器备份副本并将其保存在安全位置。

强化指南描述了配置 Kaspersky Security Center 及其组件的建议和功能，旨在降低其危害的风险。

强化指南包含以下信息：

- 选择管理服务器架构
- 配置与管理服务器的安全连接
- 配置访问管理服务器的账户
- 管理服务器保护的管理
- 管理客户端设备保护
- 配置受管理应用程序的保护
- 管理服务器维护
- 将信息传输到第三方应用程序
- 第三方信息系统安全建议

管理服务器部署

管理服务器架构

一般来说，集中式管理架构的选择取决于受保护设备的位置、相邻网络的访问、数据库更新的交付方案等。

在架构开发的初始阶段，我们建议熟悉 Kaspersky Security Center 组件以及他们之间的互动，以及数据流量和端口使用的模式。

基于此信息，您可以形成一个架构指定：

- 管理服务器位置和网络连接
- 管理员工作区的组织以及连接到管理服务器的方法
- 网络代理及防护软件的部署方法
- 使用分发点
- 使用虚拟管理服务器
- 使用管理服务器层级

- 反病毒数据库更新方案
- 其他信息流

选择用于安装管理服务器的设备

我们建议将管理服务器安装在组织基础架构的专用服务器上。如果服务器上没有安装其他第三方软件，您可以根据 Kaspersky Security Center 的要求配置安全设置而不依赖于第三方软件的要求。

您可以在物理服务器或虚拟服务器上部署管理服务器。请确保所选设备满足硬件和软件要求。

管理服务器位置

管理服务器管理的设备可以位于如下位置：

- 在局域网 (LAN) 上
- 在互联网上
- 在隔离区域 （DMZ）

同时，管理服务器也可以位于不同的网段：工业网段、企业网段和 DMZ 网段。

如果您使用 Kaspersky Security Center 管理隔离网段的保护，我们建议在隔离区域 (DMZ) 的一个分段部署管理服务器。这使您可以组织适当的网络分段并最大程度地减少流向受保护分段的流量，同时保持完整的管理功能和更新交付。

限制将管理服务器安装在域控制器、终端服务器或用户设备上

我们强烈不建议将管理服务器安装在域控制器、终端服务器或用户设备上。

我们建议您提供网络关键节点的功能分离。这种方法允许您在节点出现故障或受到损害时保持不同系统的可操作性。同时，您可以为每个节点创建不同的安全策略。

例如，通常应用于域控制器的安全限制会显著降低管理服务器的性能，并导致无法使用管理服务器的某些功能。如果入侵者获得了对域控制器的特权访问，Active Directory 域服务 (AD DS) 数据库可以被修改、损坏或销毁。此外，所有由 Active Directory 管理的系统和账户都可能受到损坏。

用于安装和运行管理服务器的账户

我们建议在本地管理员账户下运行管理服务器安装，以避免使用域账户访问管理服务器数据库。所需账户及其权利集取决于所选的 DBMS 类型、DBMS 位置和管理服务器数据库创建方法。

在 Kaspersky Security Center 安装期间，程序会自动创建 KLAdmins 和 KLOperators 组。这些组被授予连接至管理服务器和处理管理服务器对象的权限。

根据安装 Kaspersky Security Center 时使用的账户类型，系统会创建如下所示的 KLAdmins 和 KLOperators 组：

- 如果应用程序是在域内包含的用户账户下安装的，则系统会在管理服务器上和包含管理服务器的域内同时创建这些组。
- 如果应用程序是在系统账户下安装的，则系统仅会在管理服务器设备上创建这些组。

为了避免在域中创建 KLAdmins 和 KLOperators 组并因此**向管理服务器设备外的账户提供管理管理服务器的权限**，我们建议在本地账户下安装 Kaspersky Security Center。

在管理服务器安装期间，选择用于启动管理服务器作为服务的账户。默认情况下，应用程序会创建一个名为 KL-AK-* 的本地账户，管理服务器服务（klserver 服务）将在该账户下运行。

如有必要，管理服务器服务可以在所选账户下运行。此账户必须被授予访问 DBMS 所需的权限。出于安全原因，请使用非特权账户来运行管理服务器服务。

为了避免使用不正确的账户设置，我们建议自动生成账户。

从域中排除管理服务器

如果您使用管理服务器来保护重要系统的设备组，我们不建议将管理服务器设备包含在域中。这可让您区分 Kaspersky Security Center 管理权限并防止访问管理服务器以防域账户受到损害。

请考虑到，如果您在工作组中包含的设备上安装管理服务器，则以下使用管理服务器的场景将不可用：

- 使用Kaspersky Security Center 故障转移集群
- 使用Windows Server 故障转移群集
- 在单独的设备上使用 SQL Server for Windows

  仅当管理服务器和 SQL Server 在同一个域或者受信任域中时，您才可以在单独的设备上使用 SQL Server for Windows。如果管理服务器、SQL Server 和用于备份的 UNC 共享位于同一个工作组中，则您无法在 SQL Server 和共享之间安全地设置访问和读写权限。
- 使用管理服务器工具通过活动目录组策略远程安装

如果需要将管理服务器与 Active Directory 域断开连接，请遵循该主题中描述的步骤：如何更改 Kaspersky Security Center 的名称。

如果需要在工作组中包含的设备上安装管理服务器，您也可以使用 Kaspersky Security Center Linux 而不是 Kaspersky Security Center Windows。

连接安全

TLS 的使用

我们建议禁止与管理服务器的不安全连接。例如，您可以在管理服务器设置中禁止使用 HTTP 的连接。

请注意，默认情况下，管理服务器的几个 HTTP 端口是关闭的。其余端口用于管理服务器 Web 服务器 (8060)。此端口可受管理服务器设备的防火墙设置限制。

严格的 TLS 设置

建议使用 1.2 及以后版本的 TLS 协议，限制或禁止不安全的加密算法。

您可以配置管理服务器使用的加密协议 (TLS)。请注意，在发布管理服务器版本时，默认配置加密协议设置以确保安全的数据传输。

禁止使用 Windows 账户进行远程身份验证

您可以使用 LP_RestrictRemoteOsAuth 标志来禁止来自远程地址的 SSPI 连接。此标志允许您禁止使用本地或域 Windows 账户在管理服务器上进行远程身份验证。

将 LP_RestrictRemoteOsAuth 标志切换到禁止来自远程地址的连接模式：

1. 使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。
2. 在命令行中执行以下命令以指定 LP_RestrictRemoteOsAuth 标志的值：

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. 重启管理服务器服务。

如果通过安装在管理服务器设备上的 Kaspersky Security Center 网页控制台或管理控制台执行远程身份验证，则 LP_RestrictRemoteOsAuth 标志不起作用。

限制访问管理服务器数据库

我们建议限制访问管理服务器数据库。例如，只允许从管理服务器设备进行访问。这可降低管理服务器数据库因已知漏洞而受到损害的可能性。

您可以根据使用的数据库的操作说明配置参数，也可以在防火墙上提供关闭的端口。

对 Microsoft SQL Server 进行身份验证

如果 Kaspersky Security Center 使用 Microsoft SQL Server 充当 DBMS，则有必要保护 Kaspersky Security Center 传输到数据库或从数据库传输的数据以及存储在数据库中的数据免遭未经授权的访问。为此，您必须提供 Kaspersky Security Center 和 SQL Server 之间的安全通信。提供安全通信的最可靠方法是在同一设备上安装 Kaspersky Security Center 和 SQL Server，并对这两个应用程序使用共享内存机制。在所有其他情况下，建议使用 SSL/TLS 证书对 SQL Server 实例进行身份验证。

通常，管理服务器可以通过以下提供程序寻址 SQL Server：

- 使用 TCP/IP 或命名管道的 SQLOLEDB

  该提供程序被安装到 Windows 操作系统中并默认使用。

- 使用 TCP/IP、命名管道或共享内存的 MSOLEDBSQL

  如果想使用这个提供程序，您必须将其安装在具有管理服务器的设备上，然后将全局环境变量1的值设为 `KLDBADO_UseMSOLEDBSQL`。

- 使用 TCP/IP、Named Pipes或Shared memory的 MSOLEDBSQL19

  如果想使用此提供程序，您必须将其安装在带有管理服务器的设备上，然后将全局环境变量 `KLDBADO_UseMSOLEDBSQL` 的值设置为 `1`，并将全局环境变量 `KLDBADO_ProviderName` 的值设为 `MSOLEDBSQL19`。

此外，在使用 TCP/IP、命名管道或共享内存之前，请确保已启用所需的协议。

与外部 DBMS 的安全交互

如果在安装管理服务器期间将 DBMS 安装在单独的设备上（外部 DBMS），我们建议配置与该 DBMS 进行安全交互和身份验证的参数。有关配置 SSL 身份验证的更多信息，请参阅"身份验证 PostgreSQL 服务器"和"场景：身份验证 MySQL 服务器"。

配置允许连接到管理服务器的 IP 地址允许列表

默认情况下，Kaspersky Security Center 用户可以从安装了基于 MMC 的 Kaspersky Security Center 管理控制台、Kaspersky Security Center Web Console 或OpenAPI 应用程序的任何设备登录 Kaspersky Security Center。您可以配置管理服务器，使用户只能从具有允许 IP 地址的设备进行连接。例如，如果入侵者尝试通过安装在未包含在允许列表中的设备上的 Kaspersky Security Center Web Console 服务器连接到 Kaspersky Security Center，他或她将无法登录Kaspersky Security Center。

配置用于连接到 Kaspersky Security Center Web Console 的 IP 地址允许列表

默认情况下，Kaspersky Security Center 用户可以从任何设备连接到 Kaspersky Security Center Web Console。在安装了 Kaspersky Security Center Web Console 的设备上，您必须配置防火墙（内置于操作系统或第三方防火墙中），以便用户只能从允许的 IP 地址连接到 Kaspersky Security Center Web Console。

轮询期间与域控制器连接的安全性

管理服务器或 Linux 分发点通过 LDAPS 连接到域控制器以轮询域。默认情况下，连接时不需要证书验证。要强制执行证书验证，请将`KLNAG_LDAP_TLS_REQCERT`标志设置为 1。此外，您可以使用`KLNAG_LDAP_SSL_CACERT`标志指定证书颁发机构 (CA) 的自定义路径来访问证书链。

账户和身份验证

在执行以下步骤之前，请使用管理服务器数据备份任务或 klbackup 实用程序创建 Kaspersky Security Center 管理服务器备份副本并将其保存在安全位置。

通过管理服务器使用两步验证

Kaspersky Security Center 为 Kaspersky Security Center Web Console 和管理控制台的用户提供两步验证，基于 RFC 6238 标准（TOTP：基于时间的一次性密码算法）。

为您自己的账户启用两步验证后，每次登录 Kaspersky Security Center Web Console 或管理控制台时，都需要输入用户名、密码和附加的一次性安全代码。如果您对账户使用域身份验证，则只需输入附加的一次性安全代码。要接收一次性安全码，您的计算机或移动设备上必须安装认证应用。

有支持 RFC 6238 标准的软件和硬件验证器（令牌）。例如，软件验证器包括 Google Authenticator、Microsoft Authenticator、FreeOTP。

我们强烈建议不要在与管理服务器建立连接的同一台设备上安装认证应用。您可以在移动设备上安装认证应用。

限制新用户为自己设置两步验证

为了进一步提高 Kaspersky Security Center Web Console 访问安全性，您可以

禁止新用户为自己设置两步验证。

如果启用此选项，则被禁用两步验证的用户（例如新域管理员）无法为自己配置两步验证。因此，未经已启用两步验证的另一位 Kaspersky Security Center 管理员的批准，此类用户无法在管理服务器上进行身份验证，也无法登录 Kaspersky Security Center Web Console。

对操作系统使用双重身份验证

我们建议使用令牌、智能卡或其他方法（如果可能）在管理服务器设备上使用多重身份验证 (MFA) 进行身份验证。

限制保存管理员密码

如果您使用管理控制台，我们不建议在管理服务器连接对话框中保存管理员密码。

如果您使用 Kaspersky Security Center Web Console，我们不建议在用户设备上安装的浏览器中保存管理员密码。

内部用户账户的身份验证

默认情况下，管理服务器内部用户账户的密码必须遵守以下规则：

- 密码的字符长度必须是 8 到 256 位。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

默认下，允许的最大密码输入尝试次数是 10。您可以更改允许的密码输入尝试次数。

Kaspersky Security Center 用户可以输入无效的密码有限次数。达到限制后，用户账户被锁定一小时。

配置更改内部用户账户密码的选项

我们建议配置以下选项来更改内部用户账户的密码：

- 密码轮换期
- 需要更改密码的初次警告时间
- **用户必须在首次登录时更改密码**选项的值

用来防止未经授权修改的账户保护

我们建议启用附加选项来保护管理服务器的内部用户账户免遭未经授权的修改。必须为每个内部用户单独配置此保护。

管理服务器的专用管理组

我们建议为管理服务器创建一个专门的管理组。授予该组特殊访问权限并为其创建特殊安全策略。

为避免故意降低管理服务器的安全级别，我们建议限制可以管理专用管理组的账户列表。

KLAdmins 和 KLOperators 组

在 Kaspersky Security Center 安装期间，程序会自动创建 KLAdmins 和 KLOperators 组。KLAdmins 组被授予所有访问权限。KLOperators 组仅被授予读取和执行权限。授予 KLAdmins 组的权限被**锁定**。

您可以使用操作系统的标准管理工具查看 KLAdmins 和 KLOperators 组，并对这些组进行更改。

在制定使用管理服务器的规则时，有必要确定信息安全专家是否需要完全访问权限（并包含在 KLAdmins 组中）以执行标准任务。

大多数基本的管理任务可以在公司部门（或同一部门的不同员工）之间分发，并因此在不同账户之间分发。您还可以在 Kaspersky Security Center 中设置管理组访问差异。因此，可能会出现这样一种情况，KLAdmins 组账户下的授权将出现异常，并可能被视为事件。

如果 Kaspersky Security Center 安装在系统账户下，则仅在管理服务器设备上创建组。在这种情况下，我们建议确保只有在安装 Kaspersky Security Center 期间创建的条目才包含在该组中。我们不建议将任何组添加到在 Kaspersky Security Center 安装期间自动创建的 KLAdmins 组（本地和/或域）。您还应该限制更改该组的权利。KLAdmins 组必须仅包含一个非特权账户。

如果安装是在域用户账户下执行的，则会在管理服务器和包含管理服务器的域中创建组 KLAdmins 和 KLOperators。建议使用类似的方法，例如本地账户安装。

限制主管理员角色成员资格

我们建议限制主管理员角色成员资格。

默认情况下，在管理服务器安装之后，主管理员角色被分配给本地管理员组和创建的 KLAdmins 组。这对管理有用，但从安全的角度来看至关重要，因为主管理员角色具有广泛的权限，应该严格规范将此角色分配给用户。

本地管理员可以被从具有 Kaspersky Security Center 管理员权限的用户列表中排除。主管理员角色不能从 KLAdmins 组中删除。您可以在 KLAdmins 组中包括将用于管理管理服务器的账户。

如果您使用域身份验证，我们建议在 Kaspersky Security Center 中限制域管理员账户的权限。默认情况下，这些账户具有主管理员角色。此外，域管理员可以将其账户包括在 KLAdmins 组中以获得主管理员角色。为避免这种情况，您可以在 Kaspersky Security Center 安全设置中添加 Domain Admins 组，然后为其定义禁止规则。这些规则必须优先于允许的规则。

您还可以使用具有已配置的权限集的预定义用户角色。

配置对应用程序功能的访问权限

我们建议为每个用户或用户组灵活配置对 Kaspersky Security Center 功能的访问权限。

基于角色的访问控制允许通过使用一组预定义的权限创建标准用户角色并根据用户的职责范围将这些角色分配给用户。

基于角色的访问控制模型的主要优点：

- 易于管理
- 角色层级
- 最小特权方法
- 职责分离

您可以根据职位为某些员工分配内置角色，或创建全新的角色。

在配置角色时，注意与改变管理服务器设备保护状态和远程安装第三方软件相关的权限：

- 对管理组进行管理。
- 管理服务器操作。
- 远程安装。
- 更改用于存储事件和发送通知的参数。
  此权限允许您设置在事件发生时在管理服务器设备上运行脚本或可执行模块的通知。

使用单独的账户进行远程安装应用程序

除了访问权限的基本区分外，我们建议限制所有账户（主管理员或其他专用账户除外）进行应用程序远程安装。

我们建议使用单独的账户进行远程安装应用程序。您可以分配角色或者权限给单独账户。

保护 Windows 特权访问

我们建议考虑 Microsoft 关于提供特权访问安全性的建议。要查看这些建议，请前往保护特权访问文章。

建议的重点之一是特权访问工作站 (PAW) 的实施。

使用受管理服务账户 (MSA) 或组受管理服务账户 (gMSA) 运行管理服务器服务

Active Directory 有一种特殊类型的账户用于安全运行服务，称为组受管理服务账户 (MSA/gMSA)。Kaspersky Security Center 支持受管理服务账户 (MSA) 和受管理服务账户组 (gMSA)。如果这些账户类型在您的域中被使用，您可以选择它们之一作为管理服务器服务账户。

定期审核所有用户和用户的操作

我们建议对管理服务器设备上的所有用户进行定期审核。这使您能够应对与可能损害设备相关的某些类型的安全威胁。

另外，您还可以跟踪用户的操作，例如连接到管理服务器和断开连接、连接到管理服务器时出现错误以及对象修改（对于支持修订管理的对象）。

管理服务器保护的管理

选择管理服务器保护软件

根据管理服务器部署的类型和一般保护策略，选择应用程序来保护管理服务器设备。

如果您在专用设备上部署管理服务器，我们建议选择 Kaspersky Endpoint Security 应用程序来保护管理服务器设备。这可让您应用所有可用技术来保护管理服务器设备，包括行为分析模块。

如果管理服务器安装在基础设施中存在的设备上并且之前曾用于其他任务，我们建议考虑以下保护软件：

- Kaspersky Industrial CyberSecurity for Nodes。我们建议在包含在工业网络中的设备上安装此应用程序。Kaspersky Industrial CyberSecurity for Nodes 是一个应用程序，具有与各种工业软件制造商的兼容性证书。
- 推荐的安全解决方案。如果管理服务器安装在装有其他软件的设备上，我们建议考虑该软件供应商对安全解决方案兼容性的建议（可能已经有选择安全解决方案的建议，您可能需要配置信任区域）。

为保护应用程序创建单独的安全策略

我们建议为保护管理服务器设备的应用程序创建单独的安全策略。此策略必须不同于客户端设备的安全策略。这可让您为管理服务器指定最合适的安全设置，而不会影响其他设备的保护级别。

我们建议将设备分组，然后将管理服务器设备放入一个单独的组中，您可以为其创建特殊的安全策略。

保护模块

如果与管理服务器安装在同一设备上的第三方软件的供应商没有特别建议，我们建议激活并配置所有可用的保护模块（在检查这些保护模块的运行一段时间后）。

配置管理服务器设备的防火墙

在管理服务器设备上，我们建议配置防火墙以限制设备数量，管理员可以从这些设备通过管理控制台或 Kaspersky Security Center Web Console 连接到管理服务器。

默认情况下，管理服务器使用端口 13291 接收来自管理控制台的连接，使用端口 13299 接收来自 Kaspersky Security Center Web Console 的连接。我们建议限制可以使用这些端口管理管理服务器的设备数量。

管理客户端设备保护

限制将授权许可密钥添加到安装包

安装包存储在管理服务器共享文件夹的 Packages 子文件夹中。如果将授权许可密钥添加到安装包，则授权许可密钥可能会泄露，因为对安装包的存储库启用了共享读取访问权限。

为避免泄露授权许可密钥，我们不建议将授权许可密钥添加到安装包中。

我们推荐使用将授权许可密钥自动分发到受管理设备，通过受管理应用程序的“添加授权许可密钥”任务进行部署，并手动将激活码或密钥文件添加到设备。

在管理组之间移动设备的自动规则

我们建议限制使用自动规则在管理组之间移动设备。

如果您使用自动规则移动设备，这可能会导致策略的传播，这些策略为移动的设备提供比重新定位前的设备更多的权限。

此外，将客户端设备移动到另一个管理组可能会导致策略设置的传播。这些策略设置可能不适合分发给访客和不受信任的设备。

此建议不适用于将设备一次性初始分配给管理组。

分发点和连接网关的安全要求

安装了网络代理的设备可以充当分发点并执行以下功能：

- 将从管理服务器收到的更新和安装包分发到组内的客户端设备。
- 在客户端设备上执行第三方软件和卡巴斯基应用程序的远程安装。
- 轮询网络以检测新设备并更新现有设备的信息。分发点可以使用与管理服务器相同的设备检测方法。

在组织的网络上放置分发点用于：

- 降低管理服务器负载
- 流量优化
- 让管理服务器能够访问网络中难以到达的设备

考虑到可用功能，我们建议保护充当分发点的设备免受任何类型的未经授权的访问（包括物理访问）。

限制自动分配分发点

为了简化管理并保持网络的可操作性，我们建议使用分发点的自动分配。但是，对于工业网络和小型网络，我们建议您避免自动分配分发点，因为（例如）用于推送远程安装任务的账户的私人信息可以通过操作系统转移到分发点。

对于工业网络和小型网络，您可以手动分配设备作为分发点。

您还可以查看分发点活动报告。

Kaspersky Security Center 用户设备的安全要求

Kaspersky Security Center用户的设备必须满足特殊的安全要求。我们建议保护这些设备免受任何类型未经授权的访问（包括物理访问）：

Kaspersky Security Center 用户设备包括以下内容：

- 用户使用浏览器从其连接到 Kaspersky Security Center Web Console 的设备。
- 用户使用基于 MMC 的管理控制台从其连接到 Kaspersky Security Center 的设备。
- 通过 OpenAPI 与管理服务器交互的应用程序从其连接到 Kaspersky Security Center 的设备。

安装了 Kaspersky Security Center Web Console 的设备的安全要求

安装了 Kaspersky Security Center Web Console 的设备用于管理 Kaspersky Security Center，因此必须对这些设备的安全性应用特殊要求。我们建议保护这些设备免受任何类型未经授权的访问（包括物理访问）。

配置受管理应用程序的保护

受管理应用程序策略

我们建议为每种类型使用的应用程序和 Kaspersky Security Center 组件（网络代理、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Agent 等）创建一个策略。此组策略必须应用于所有受管理设备（根管理组）或根据配置的移动规则新的受管理设备将自动移动到其中的单独组。

指定用于禁用保护和卸载应用程序的密码

为防止入侵者禁用卡巴斯基安全应用程序，我们强烈建议为禁用保护和卸载卡巴斯基安全应用程序启用密码保护。您可以为（例如）Kaspersky Endpoint Security for Windows、Kaspersky Security for Windows Server、网络代理和其他卡巴斯基应用程序设置密码。启用密码保护后，我们建议通过关闭"锁"来锁定这些设置。

指定将客户端设备手动连接到管理服务器的密码（klmover 实用程序）

klmover 实用程序允许您手动将客户端设备连接到管理服务器。在客户端设备上安装网络代理时，自动将该实用程序复制到网络代理安装文件夹。

为了防止入侵者将设备移出管理服务器的控制，我们强烈建议为运行 klmover 实用程序启用密码保护。要启用密码保护，请在**网络代理策略设置使用卸载密码**使用卸载密码选项。

klmover 实用程序需要本地管理员权限。对于没有本地管理员权限操作的设备，可以忽略运行 klmover 实用程序的密码保护。

启用**使用卸载密码**选项还会为清理工具 (cleaner.exe) 启用密码保护。

使用卡巴斯基安全网络

在受管理应用程序的所有策略和管理服务器属性中，我们建议启用卡巴斯基安全网络 (KSN) 的使用并接受 KSN 声明。更新或升级管理服务器时，您可以接受更新后的 KSN 声明。在某些情况下，当法律或其他法规禁止使用云服务时，您可以禁用 KSN。

定期扫描受管理设备

对于所有设备组，我们建议创建一个定期运行完整设备扫描的任务。

发现新设备

我们建议正确配置设备发现设置：设置与 Active Directory 的集成，并指定用于发现新设备的 IP 地址范围。

出于安全目的，您可以使用包含所有新设备的默认管理组和影响该组的默认策略。

选择共享文件夹

如果您在运行 Windows 的设备上部署管理服务器并选择现有的共享文件夹（例如，用于放置安装包和存储更新的数据库的文件夹），我们建议确保向 Everyone 组授予读取权限，和向 KLAdmins 组授予写入权限。

管理服务器维护

备份管理服务器数据

数据备份允许您在不丢失数据的情况下恢复管理服务器数据。

默认情况下，数据备份任务在管理服务器安装后自动创建并定期执行，从而将备份保存在适当的目录中。

数据备份任务的设置可以更改如下：

- 备份频率增加
- 指定保存副本的特殊目录
- 更改备份副本的密码

如果您将备份副本存储在不同于默认目录的特殊目录中，我们建议限制该目录的访问控制列表 (ACL)。管理服务器账户和管理服务器数据库的账户必须具有此目录的写入权限。

管理服务器维护

管理服务器维护允许您降低数据库容量，提高应用程序的运行和操作可靠性。我们建议您至少每周维护一次管理服务器。

管理服务器通过专用任务进行维护。在维护管理服务器时，应用程序执行以下操作：

- 检查数据库错误
- 重组数据库索引
- 更新数据库统计信息
- 收缩数据库（如果必要）

安装操作系统更新和第三方软件更新

我们强烈建议您定期在管理服务器设备上为操作系统和第三方软件安装软件更新。

客户端设备不需要持续连接到管理服务器，因此在安装更新后重新启动管理服务器设备是安全的。管理服务器停机期间在客户端设备上注册的所有事件都会在连接恢复后发送给它。

事件传输到第三方系统

监控和报告

为了及时响应安全问题，我们建议配置监控和报告功能。

导出事件到 SIEM 系统

为了在重大损害发生之前快速检测安全问题，我们建议在 SIEM 系统中使用事件导出。

审计事件的电子邮件通知

Kaspersky Security Center 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。为了及时响应紧急情况，我们建议配置管理服务器以发送有关其发布的审计事件、关键事件、故障事件和警告的通知。

由于这些事件是系统内事件，因此可以预期它们的数量很少，这非常适用于邮件。

管理服务器功能的统计信息

为了及时响应安全问题，我们建议配置使用简单网络管理协议（SNMP）将管理服务器功能的统计信息发送到第三方应用程序。

第三方信息系统安全建议

CIS 基准的安全建议

当使用管理服务器和网络代理支持的操作系统、虚拟化平台或数据库服务器版本时，我们建议应用互联网安全中心 (CIS) 的最佳信息安全实践（如有）来微调这些信息系统。

互联网安全中心 (CIS) 是一家致力于提高信息技术领域安全性的非营利组织。特别是，CIS 负责开发和分发安全标准，例如 CIS 控制和 CIS 基准。这些标准是一组用于确保信息系统安全的建议和实践。

CIS 门户网站包含针对管理服务器和网络代理支持的以下信息系统版本提供的相关建议：

- 以下系列的操作系统：
  - 桌面版 Windows
  - 服务器版 Windows
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware 虚拟化平台
- 数据库服务器：
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Astra Linux 操作系统的安全建议

使用 Astra Linux 操作系统时，您应该遵循针对相应版本 Astra Linux 的红皮书中所述的安全建议。

RED OS 操作系统的安全建议

使用 RED OS 操作系统时，您应该使用 RED OS 官方文档中描述的管理员指南中的安全建议。

有关使用卡巴斯基安全应用程序的建议

在 Kaspersky Endpoint Security for Windows 中使用 KLAdmin 密码

具有不同计算机水平的多个用户可以共享一台安装了 Kaspersky Endpoint Security for Windows 的设备。如果用户可以不受限制地访问 Kaspersky Endpoint Security for Windows 及其设置，则设备的整体保护级别可能会降低。密码保护允许您根据授予用户的权限（例如，退出应用程序的权限）限制用户对 Kaspersky Endpoint Security for Windows 的访问。

限制访问 Kaspersky Endpoint Security for Windows 及其参数的方法之一是使用 KLAdmin 账户。KLAdmin 账户是可以不受限制地访问 Kaspersky Endpoint Security for Windows 的管理员账户。KLAdmin 账户有权在 Kaspersky Endpoint Security for Windows 中执行任何受密码保护的操作。KLAdmin 账户的权限无法撤销。您可以在 Kaspersky Endpoint Security for Windows 策略的属性中设置 KLAdmin 账户的密码。Kaspersky Endpoint Security for Windows 管理员对 KLAdmin 账户密码的安全使用负全部责任。如果您的组织有自己的密码策略，请遵循该策略的指示。

我们对保护组织免遭 KLAdmin 密码盗窃的建议如下：

- **一般要求**
  请勿使用账户名或部分账户名作为密码。
- **最小密码长度要求**
  创建一个长度至少为 10 个字符的密码。
- **使用多种字符类型的要求**
  设置一个包含不同类别字符的复杂密码：小写和大写字母、数字和特殊字符。
- **密码过期要求**
  将密码的最短有效期设置为 90 天。新密码不得与最近 24 个密码中的任何一个匹配。

部署准备

该部分描述了在部署 Kaspersky Security Center 之前必须采取的操作。

计划 Kaspersky Security Center 部署

该部分介绍了根据以下标准在组织网络中部署 Kaspersky Security Center 组件的最方便选项：

- 设备总数
- 在组织或地理上拆分的单元（本地办公室、分支）
- 由狭窄通道连接的网络拆分网络
- 需要到管理服务器的互联网访问

部署保护系统的常规方案

本部分描述了使用 Kaspersky Security Center 的企业网络保护系统的标准部署方案。

系统必须防止任何非授权的访问。我们建议您为您的操作系统安装所有可用更新，然后再安装应用程序到您的设备并物理保护管理服务器和分发点。

您可以使用 Kaspersky Security Center 部署保护系统到企业网络，通过以下部署方案：

- 使用下列方式之一通过 Kaspersky Security Center 部署保护系统：
  - 通过管理控制台
  - 通过 Kaspersky Security Center Web Console

  Kaspersky 应用程序自动安装在客户端设备上，并通过 Kaspersky Security Center 自动连接到管理服务器。

  基本部署方案是一种通过管理控制台部署保护系统的方案。使用 Kaspersky Security Center Web Console 允许从浏览器启动 Kaspersky 应用程序的安装。
- 使用在 Kaspersky Security Center 中生成的独立安装包手动部署保护系统。

  手动在客户端设备和管理员工作站中安装 Kaspersky 应用程序；在安装网络代理时指定客户端设备与管理服务器的连接设置。

  该部署方法建议在远程安装不可用时使用。

Kaspersky Security Center 可让您使用 Microsoft 活动目录组策略部署您的保护系统。

关于在组织网络中规划 Kaspersky Security Center 的部署

一个管理服务器可以支持最多 100,000 台设备。如果组织网络中的设备总数超过 100,000，必须在网络中部署多个管理服务器，并合并到一个方便集中管理的层级。

如果组织包含大规模有各自管理员的远程本地办公室（分支），则适合在这些办公室部署管理服务器。否则，此类办公室必须被视为通过低吞吐量通道连接的独立网络，请参见“标准配置：由自己管理员运行的多个大规模办公室”部分。

当使用由狭窄通道连接的拆分网络时，可以分配一个或几个网络代理作为分发点来节省流量（参见分发点数量计算表格）。这种情况下，一个拆分网络中的所有设备都从此本地更新中心上获取更新。实际分发点可以从管理服务器（默认情景）和互联网上的卡巴斯基服务器下载更新（参见“标准配置：多个小型远程办公室”）。

“Kaspersky Security Center 标准配置”部分提供了 Kaspersky Security Center 标准配置的详细描述。当计划部署时，根据组织架构选择最合适的标准配置。

在部署计划阶段，必须考虑到特别证书 X.509 到管理服务器的分配。X.509 证书到管理服务器的分配可能用在以下情况（部分列表）：

- 通过 SSL 终端代理或使用反向代理检查安全套接层 (SSL)
- 与组织公共密钥基础架构（PKI）的整合
- 在证书字段中指定所需值
- 提供所需的证书加密长度

选择企业保护结构

组织保护结构的选择根据以下因素进行定义：

- 组织的网络拓扑。
- 组织结构。
- 负责网络保护的员工的数量及其责任分配。
- 可用于分配以便保护管理组件的硬件资源。
- 可用于分配以便维护组织网络内部保护组件运行的通信通道的吞吐量。
- 在组织网络中执行关键管理操作的时间限制。关键管理操作，包括分发反病毒数据库和修改客户端设备的策略。

在选择保护结构时，建议您首先评估可用来操作集中式保护系统的网络和硬件资源。

要分析网络和硬件基础架构，建议您遵照以下过程：

1. 定义将部署保护的网络的以下设置：
   - 网段数量。
   - 各个网段之间的通信通道的速度。
   - 每个网段中的受管理设备的数量。
   - 可用于分配以便维护保护运行的每个通信通道的吞吐量。
2. 确定为所有受管理设备执行主要管理操作的最大允许时间。

3. 分析来自步骤 1 和步骤 2 的信息以及来自管理系统负载测试的数据。根据分析，回答以下问题：

   - 是否可以用单个管理服务器服务所有客户端，或者是否需要一台管理服务器层级？
   - 需要哪种管理服务器硬件配置以便用在项目 2 中指定的时间限制内处理所有客户端？
   - 是否需要使用分发点来减少通信通道的负载？

在获取上述问题的答案之后，您可以编辑组织保护所允许的一组结构。

在组织的网络中，您可以使用下列标准保护结构之一：

- 一台管理服务器。将所有客户端设备连接至单个管理服务器。管理服务器充当分发点。
- 一个包含分发点的管理服务器。将所有客户端设备连接至单个管理服务器。某些联网的客户端设备作为分发点运行。
- 管理服务器层级。每个网段都分配了单独的管理服务器，作为管理服务器常规层次结构的一部分。主管理服务器充当分发点。
- 包含分发点的管理服务器层级。每个网段都分配了单独的管理服务器，作为管理服务器常规层次结构的一部分。某些联网的客户端设备作为分发点运行。

Kaspersky Security Center 的标准配置

该部分描述了以下用于组织网络中的 Kaspersky Security Center 组件部署的标准配置：

- 单一办公室
- 几个大规模办公室，被地理拆分并由自己的管理员运行
- 多个小办公室，被地理拆分

标准配置：单一办公室

可以在组织网络中部署一个或多个管理服务器。管理服务器数量可以基于可用硬件或受管理设备总数来选择。

一个管理服务器可以支持最多 100,000 台设备。您必须考虑今后增加受管理设备的数量的可能性：最好连接较少设备到单一管理服务器。

管理服务器可以被部署在内部网络或 DMZ 中，具体取决于管理服务器是否需要互联网连接。

如果使用了多个服务器，建议您合并它们到一个层级。使用管理服务器层级时，允许您避免冗余策略和任务、处理整个受管理设备集合，使其如同被单一管理服务器管理一样：例如，搜索设备、创建设备分类和创建报告。

标准配置：由自己管理员运行的几个大规模办公室

如果组织有多个地理位置分散的大规模办公室，则必须考虑在每个办公室部署管理服务器的选项。每个办公室可以部署一台或多台管理服务器，具体取决于可用的客户端设备和硬件的数量。此种情况下，每个办公室可以被视为“标准配置：单一办公室”。为了简化管理，建议将所有管理服务器合并到一个层次结构（可能是多层）中。

如果一些员工带着他们的设备（笔记本电脑）在办公室之间移动，请在网络代理策略中创建网络代理连接配置文件。网络代理连接配置文件仅支持 Windows 和 macOS 服务。

标准配置：多个小远程办公室

该标准配置适用于总部办公室以及许多可通过互联网与总部办公室联系的远程小型办公室。每个远程办公室可能位于 Network Address Translation (NAT) 之外，例如，两个远程办公室之间无法建立连接，因为它们是隔离的。

总部办公室必须部署一台管理服务器，必须为所有其他办公室分配一个或多个分发点。如果办公室通过互联网连接，最好为分发点创建*将更新下载至分发点存储库*任务，这样它们将从卡巴斯基服务器、本地或网络文件夹直接下载更新，而不是从管理服务器下载。

如果远程办公室的一些设备不能直接访问管理服务器（例如，到管理服务器的访问是通过互联网提供但是一些设备没有互联网连接），分发点必须被切换到连接网关模式。此种情况下，远程办公室设备上的网络代理将被通过网关而不是直接连接到管理服务器，为了后期同步。

作为管理服务器，很可能无法轮询远程办公室网络，最好把该功能转给分发点。

管理服务器将无法发送通知到远程办公室 NAT 以外的受管理设备的端口 15000 UDP。要解决该问题，可以在作为分发点的设备的属性中启用持续连接到管理服务器模式（“**不断开与管理服务器的连接**”复选框）。如果分发点总数不超过 300 则该模式可用。使用推送服务器以确保受管理设备和管理服务器之间存在持续连接。有关详细信息，请参阅以下主题：使用分发点作为推送服务器。

为管理服务器选择 DBMS

当选择管理服务器使用的数据库管理系统（DBMS）时，您必须考虑到被管理服务器覆盖的设备数量。

下表列出了有效 DBMS 选项，以及它们的使用建议和限制。

对 DBMS 的建议和限制

DBMS	建议和限制
SQL Server Express Edition 2016 或后续版本	如果您打算为少于 10,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。 您可以限制事件存储库中事件的最大数量，以防止数据库溢出。 有关详细信息，请参阅以下主题：数据库空间的计算。 SQL Server Express Edition DBMS 被管理服务器和其他应用程序同时使用是被严格禁止的。 **执行 Windows 更新同步**任务不支持 Microsoft SQL Express 数据库。
本地 SQL Server 版本，而不是 Express 2016 或后续版本	没有限制。
远程 SQL Server 版本，而不是 Express 2016 或后续版本	仅在两台设备都在相同 Windows® 域中时可用；如果域不同，必须在它们之间建立双向信任关系。
本地或远程 MySQL 5.5、5.6 或 5.7（MySQL 版本 5.5.1、5.5.2、5.5.3、5.5.4 和 5.5.5 不再被支持）	如果您打算为少于 10,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。
本地或远程 MySQL 8.0.20 或更高版本	如果您打算为少于 50,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。
本地或远程 MariaDB（查看受支持的版本）	如果您打算为少于 20,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。
PostgreSQL、Postgres Pro（查看支持的版本）	如果您打算为少于 50,000 台设备运行单个管理服务器，请使用这些 DBMS 之一。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。

如果将 SQL Server 2019 用作 DBMS，并且未安装累积补丁 CU12 或更高版本，则在安装 Kaspersky Security Center 之后，必须执行以下操作：

1. 使用 SQL Management Studio 连接到 SQL Server。
2. 运行以下命令（如果为数据库选择了其他名称，请使用该名称而不是 KAV）：

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. 重新启动 SQL Server 2019 服务。

否则，使用 SQL Server 2019 可能导致错误，例如“资源池 'internal' 中没有足够的系统内存来运行此查询。”

配置与 Kaspersky Security Center 15.1 配合使用的 MariaDB x64 服务器

要成功配置 MariaDB x64 服务器以与 Kaspersky Security Center 配合使用，您必须使用除本文中指定的服务器参数之外的默认服务器参数。

Kaspersky Security Center 15.1 支持 MariaDB DBMS。有关支持的 MariaDB 版本的更多信息，请参阅“硬件和软件要求”部分。

如果将 MariaDB DBMS 用于 Kaspersky Security Center，请启用对 InnoDB 和 MEMORY 存储以及对 UTF-8 和 UCS-2 编码的支持。

my.ini 文件的推荐设置

要配置 my.ini 文件：

1. 在文本编辑器中打开 my.ini 文件。
2. 将以下行添加到 my.ini 文件的 [mysqld] 部分中：

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< 真实值不得少于期待 KAV 数据库大小的 80% >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

`innodb_buffer_pool_size` 的值不能小于预期 KAV 数据库大小的 80%。请注意，指定的内存是在服务器启动时分配的。如果数据库大小小于指定的缓冲区大小，则只分配所需的内存。如果您使用 MariaDB 10.4.3 或更早版本，所分配内存的实际大小大约比指定的缓冲区大小大 10%。

建议使用参数值 `innodb_flush_log_at_trx_commit=0`，因为值“1”或“2”会对 MariaDB 的运行速度产生负面影响。确保`innodb_file_per_table`参数设置为`1`。

对于 MariaDB 10.1，另外在 [mysqld] 部分输入以下行：

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

对于 MariaDB 10.6，另外在 [mysqld] 部分输入以下行：

```
optimizer_prune_level=0
optimizer_search_depth=8
```

默认情况下，优化器加载项 `join_cache_incremental`、`join_cache_hashed` 和 `join_cache_bka` 已启用。如果这些加载项未启用，必须启用它们。

要检查是否启用了优化器加载项：

1. 在 MariaDB 客户端控制台中，执行以下命令：

   ```
   SELECT @@optimizer_switch;
   ```

2. 检查其输出是否包含以下行：

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   如果这些行存在并且值为 `on`，则优化器加载项已启用。

   如果缺少这些行或值为 `off`，请执行以下操作：

   1. 在文本编辑器中打开 my.ini 文件。

   2. 将以下行添加到 my.ini 文件的 `[mysqld]` 部分中：

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

加载项 `join_cache_incremental`、`join_cache_hash` 和 `join_cache_bka` 已启用。

配置与 Kaspersky Security Center 15.1 配合使用的 MySQL x64 服务器

要成功配置 MySQL x64 服务器以与 Kaspersky Security Center 配合使用，您必须使用除本文中指定的服务器参数之外的默认服务器参数。

如果将 MySQL DBMS 用于 Kaspersky Security Center，请启用对 InnoDB 和 MEMORY 存储以及对 UTF-8 和 UCS-2 编码的支持。

my.ini 文件的推荐设置

要配置 my.ini 文件：

1. 在文本编辑器中打开 my.ini 文件。
2. 将以下行添加到 my.ini 文件的 `[mysqld]` 部分中：

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< 真实值不得少于期待 KAV 数据库大小的 80% >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (在大多数情况下，服务器使用小型事务处理)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

请注意，在 `innodb_buffer_pool_size` 值中指定的内存将在服务器启动时分配。如果数据库大小小于指定的缓冲区大小，则只分配所需的内存。已分配内存的实际大小大约比指定的缓冲区大小大 10%。有关详细信息，请参阅 MySQL 文档。

建议使用参数值 `innodb_flush_log_at_trx_commit = 0`，因为值“1”或“2”会对 MySQL 的运行速度产生负面影响。确保`innodb_file_per_table`参数设置为`1`。

配置与 Kaspersky Security Center 15.1 配合使用的 PostgreSQL 或 Postgres Pro 服务器

要成功配置 PostgreSQL 或 Postgres Pro 服务器以与 Kaspersky Security Center 配合使用，您必须使用除本文中指定的服务器参数之外的默认服务器参数。

Kaspersky Security Center 15.1 支持 PostgreSQL 和 Postgres Pro DBMS。如果您使用这些 DBMS 之一，请考虑配置 DBMS 服务器参数，使 DBMS 与 Kaspersky Security Center 达到最佳工作状态。

配置文件的默认路径是：`C:\Program Files\PostgreSQL\< 版本 >\data\postgresql.conf`

PostgreSQL 和 Postgres Pro 的推荐参数：

- `shared_buffers` = 安装 DBMS 的设备的 RAM 值的 25%

  如果 RAM 小于 1 GB，则保留默认值。
- `max_stack_depth = 2MB`
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`

- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

确保`standard_conforming_strings`参数设置为其默认值`on`。更新 postgresql.conf 文件后重新加载配置或重新启动服务器。有关详细信息，请参阅 PostgreSQL 文档。

如果您使用 Postgres Pro 15.7 或 Postgres Pro 15.7.1，请禁用`enable_compound_index_stats`参数：

```
enable_compound_index_stats = off
```

有关 PostgreSQL 和 Postgres Pro 服务器参数以及如何指定它们的详细信息，请参阅相应的 DBMS 文档。

有关如何为 PostgreSQL 和 Postgres Pro 创建和配置账户的详细信息，请参阅以下主题： 配置 PostgreSQL 和 Postgres Pro 的使用账户。

使用 Kaspersky Endpoint Security for Android 管理移动设备

安装了 Kaspersky Endpoint Security for Android™ 的移动设备(也叫 KES 设备)通过管理服务器管理。Kaspersky Security Center 支持以下管理 KES 设备的功能：

- 将移动设备处理为客户端设备：
  - 管理组中的成员关系
  - 监控，例如查看状态、事件和报告
  - 修改本地设置和为 Kaspersky Endpoint Security for Android 分配策略
- 以集中模式发送命令
- 远程安装移动应用包

管理服务器通过 TLS、TCP 端口 13292 管理 KES 设备。

提供到管理服务器的互联网访问

以下情况需要到管理服务器的互联网访问：

- 定期更新 Kaspersky 数据库、软件模块和应用程序
- 更新第三方软件

  默认情况下，管理服务器不需要互联网连接就可以在受管理设备上安装 Microsoft 软件更新。例如，受管理设备可以直接从 Microsoft 更新服务器下载 Microsoft 软件更新，也可以从组织的网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下载。在以下情况下，管理服务器必须连接到互联网：
  - 将管理服务器用作 WSUS 服务器时
  - 要安装除 Microsoft 软件以外的第三方软件的更新
- 修复第三方软件漏洞

管理服务器需要互联网连接才能执行以下任务：

- 针对 Microsoft 软件漏洞生成推荐的修复程序列表。该列表由 Kaspersky 专家创建并定期更新。
- 修复除 Microsoft 软件以外的第三方软件的漏洞。

- 管理漫游用户的设备（便携式电脑）
- 在远程办公室管理设备
- 与位于远程办公室的主管理服务器或从属管理服务器交互
- 管理移动设备

该部分描述了通过互联网提供到管理服务器的访问的典型方法。着眼于提供到管理服务器的互联网访问的每种情况都可能需要一个管理服务器专用证书。

互联网访问：本地网络上的管理服务器

如果管理服务器位于组织内部网络，则最好通过端口转发使管理服务器的 TCP 端口 13000 可从外部访问。如果需要移动设备管理，则最好使 TCP 端口 13292 可被访问。

互联网访问：DMZ 中的管理服务器

如果管理服务器位于组织网络的 DMZ 中，它不能访问组织内部网络。因此，以下限制被应用：

- 管理服务器无法检测新设备。
- 管理服务器无法通过在组织内部网络设备上强制安装来运行网络代理初始化部署。

这仅应用到网络代理初始化安装上。任何网络代理的后续升级或安全应用程序安装可以被管理服务器运行。同时，网络代理的初始化部署可以用其他方法运行，例如，通过 Microsoft 活动目录组策略。

- 管理服务器无法通过端口 15000 UDP 发送通知到受管理设备，该端口不是 Kaspersky Security Center 关键的运行端口。
- 管理服务器无法轮询活动目录。然而，活动目录轮询结果在大多数方案下不需要。

如果上述限制被视为严重限制，可以通过使用组织网络中的分发点删除这些限制：

- 要在没有网络代理的设备上运行初始化部署，您首先要在其中一台设备上安装网络代理，然后给它分配分发点状态。结果，在其他设备上的网络代理初始化安装将通过该分发点由管理服务器运行。
- 要在组织内部网络中检测新设备并轮询活动目录，您必须在其中一个分发点上启用相关的设备发现方法。

要确保将通知成功发送到组织内部网络中受管理设备的端口 15000 UDP，您必须使用分发点覆盖整个网络。在被分配的分发点的属性中，选择**不断开与管理服务器的连接**复选框。因此，管理服务器将建立一个到分发点的持续连接，同时这些分发点能够发送通知到组织内部网络（可以是 IPv4 或 IPv6 网络）中的设备的端口 15000 UDP。

互联网访问：DMZ 中作为连接网关的网络代理

管理服务器可以位于组织的内部网络，在该网络的 DMZ 中，可以有一个将网络代理作为反向连接网关运行的设备（管理服务器建立到网络代理的连接）。此种情况下，以下条件必须被满足以确保互联网访问：

- 网络代理必须安装在该 DMZ 中的设备上。当您安装网络代理时，在安装向导的“**连接网关**”窗口，选择“**使用网络代理作为 DMZ 连接网关**”。
- 必须将安装了连接网关的设备添加为分发点。添加连接网关时，在“**添加分发点**”窗口中选择“**选择**”→“**按地址在 DMZ 中添加连接网关**”选项。
- 要使用互联网连接将外部台式设备连接到管理服务器，必须更正网络代理的安装包。在创建的安装包的属性中，选择“**高级**”→“**通过使用连接网关连接到管理服务器**”选项，然后指定新创建的连接网关。

对于 DMZ 中的连接网关，管理服务器创建与管理服务器证书一同签署的证书。如果管理员决定分配自定义证书到管理服务器，它必须在连接网关在 DMZ 中被创建之前完成。

如果一些员工使用可以连接到管理服务器的便携式电脑，最好在网络代理策略中为网络代理创建交换规则。

关于分发点

安装了网络代理的设备可以用作分发点。在该模式中，网络代理可以运行以下功能：

- 分发更新（可以从管理服务器获取，或者从 Kaspersky 更新服务器获取）。在后一种情况下，必须为作为分发点的设备创建“*将更新下载至分发点存储库*”任务：
  - 安装软件（包括网络代理初始化部署）到其他设备。
  - 轮询网络以检测新设备并更新现有设备的信息。分发点应用与管理服务器相同的设备发现方法。

在组织网络中部署分发点可以带来以下好处：

- 降低管理服务器负载。
- 优化流量。
- 让管理服务器能够访问组织网络中难以到达的设备。NAT 以外分发点的可用性(与管理服务器有关)允许管理服务器运行以下操作：
  - 在 IPv4 或 IPv6 网络上通过 UDP 向设备发送通知
  - 轮询 IPv4 或 IPv6 网络
  - 执行初始部署
  - 用作推送服务器

为每个管理组分配分发点。此种情况下，分发点的范围包括管理组及其所有子组中的所有设备。然而，作为分发点的设备可能不包含在它被分配的管理组。

您可以让分发点作为连接网关工作。此种情况下，分发点范围内的设备将通过网关连接到管理服务器，而不是直接连接到管理服务器。该模式适合用在不允许管理服务器和受管理设备之间建立直接连接的场合中。

如果您使用基于 Linux 的设备作为分发点，我们强烈建议增加 klnagent 服务的文件描述符限制，因为如果分发点的范围包括许多设备，则默认的最大可打开文件数可能不够。

增加 klnagent 服务的文件描述符限制

如果基于 Linux 的分发点的范围包括许多设备，则可打开的文件（文件描述符）的默认限制可能不够。为了避免这种情况，您可以增加 klnagent 服务的文件描述符的限制。

要增加 klnagent 服务的文件描述符限制：

1. 在用作分发点的 Linux 设备上，执行以下命令：

   ```
   systemctl edit klnagent64.service
   ```

2. 在 `[Service]` 部分的 `LimitNOFILE` 参数中指定文件描述符的硬限制和软限制：

   `LimitNOFILE=<` 软资源限制 `>:<` 硬资源限制 `>`

   例如，`LimitNOFILE=32768:131072`。请注意，文件描述符的软限制必须小于或等于硬限制。

3. 运行以下命令以确保参数指定正确：

   ```
   systemd-analyze verify klnagent64.service
   ```

   如果参数指定不正确，此命令可能会输出以下错误之一：

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     如果出现此错误，则 `LimitNOFILE` 行中的符号指定不正确。您必须检查并更正输入的行。

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     如果出现此错误，则表示您输入的文件描述符的软限制超过了硬限制。您必须检查输入的行并确保文件描述符的软限制小于或等于硬限制。

4. 运行以下命令重新加载 systemd 进程：

   ```
   systemctl daemon-reload
   ```

5. 运行以下命令重新启动网络代理服务：

   ```
   systemctl restart klnagent
   ```

6. 运行以下命令以确保正确应用指定的参数：

   `less /proc/<` nagent 进程 ID `>/limits`

   其中 `<` nagent 进程 ID `>` 参数是网络代理进程的标识符。您可以运行以下命令来获取标识符：

   ```
   ps -ax | grep klnagent
   ```

对于基于 Linux 的分发点，可以打开的文件的限制增加了。

计算分发点的数量和配置

网络包含越多的客户端设备，就需要越多的分发点。我们建议您禁用分发点的自动分配。当分发点的自动分配被启用时，如果客户端设备数量很大，管理服务器就分配分发点并定义其配置。

使用单独分配的分发点

如果您计划使用特定设备作为分发点(就是，单独分配的服务器)，您可以不使用分发点的自动分配。此种情况下，确保您要分配为分发点的设备具有足够的剩余磁盘空间卷，不定期关闭，且禁用了睡眠模式。

网络中基于网络设备数量被专门分配的包含单一网段的分发点的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	可接受：(N/10,000 + 1)，建议：(N/5000 + 2)，N 是网络设备数量

网络中基于网络设备数量被专门分配的包含多个网段的分发点的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–100	1
大于 100	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

使用标准客户端设备（工作站）作为分发点

如果您计划使用标准客户端设备（就是，工作站）作为分发点，我们建议您按照所示分配分发点（参见下表），以便避免通信渠道和管理服务器过载。

网络中基于网络设备数量作为分发点工作的包含单一网段的工作站的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

网络中基于网络设备数量作为分发点工作的包含多个网段的工作站的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–30	1
31–300	2
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

如果分发点被关闭(或由于某些原因不可用)，其范围内的受管理设备可以访问管理服务器以更新。

管理服务器层级

一个 MSP 可能运行多个管理服务器。可能不方便管理几个不同的管理服务器，因此可以应用层次结构。两个管理服务器的“主/从”配置提供了以下选项：

- 一个从属管理服务器从主管理服务器继承策略和任务，这防止了重复设置。
- 主管理服务器上的设备分类可以包含从属管理服务器的设备。
- 主管理服务器的报告可以包含从属管理服务器的数据（包括详细信息）。

主管理服务器仅接收来自上面列出的选项范围内的非虚拟从属管理服务器的数据。此限制不适用于虚拟管理服务器，虚拟管理服务器与其主管理服务器共享数据库。

虚拟管理服务器

基于物理管理服务器，可以创建多个虚拟管理服务器，它们与从属管理服务器相似。相比于基于访问控制列表（ACLs）的任意访问模式，虚拟管理服务器模式功能更强大并且提供更高度隔离。除了具有策略和任务的已分配设备的专用管理组结构外，每个虚拟管理服务器还具有自己的未分配设备组、自己的报告集、选定的设备和事件、安装包、移动规则等。虚拟管理服务器的功能范围既可以被服务提供商 (xSP) 用来最大限度地隔离客户，也可以为具有复杂工作流和众多管理员的大型组织所用。

虚拟管理服务器与从属管理服务器非常相似，但是有以下不同点：

- 虚拟管理服务器缺少多数全局设置和自己的 TCP 端口。
- 虚拟管理服务器没有从属管理服务器。
- 虚拟管理服务器没有其他虚拟管理服务器。
- 物理管理服务器可以查看它所有虚拟管理服务器的设备、组、事件和受管理设备上的对象（隔离区条目、应用程序注册表等等）。
- 虚拟管理服务器仅可以扫描连接了分发点的网络。

Kaspersky Security Center 的限制信息

下表显示了 Kaspersky Security Center 当前版本的限制。

Kaspersky Security Center 的限制

限制类型	参数值
每个管理服务器的最大受管理设备数量	100,000
选中“**不断开与管理服务器的连接**”选项时的最大设备数	300
管理组最大数量	10,000
要存储的事件的最大数量	45,000,000
策略的最大数量	2000
任务的最大数量	2000
活动目录对象的最大总数（组织单元 (OU) 和用户账户、设备和安全组）	1,000,000
策略中配置文件的最大数量	100
单一主管理服务器的从属管理服务器的最大数量	500
虚拟管理服务器的最大数量	500
单一分发点可以覆盖的最大设备数量（分发点仅可以覆盖非移动设备）	10,000
可以使用单一连接网关的最大设备数量	10,000，包括移动设备
每个管理服务器的最大移动设备数量	100,000 减去固定的受管理设备数量

网络负载

本部分包含在关键管理操作期间客户端设备和管理服务器交换的网络流量。

网络的主要负载是由执行以下管理情景引起的：

- 反病毒保护的初始部署
- 反病毒数据库的原始更新
- 将客户端设备与管理服务器同步
- 反病毒数据库的定期更新
- 利用管理服务器对客户端设备上事件的处理

反病毒保护的初始部署

本部分提供在将 Network Agent 和 Kaspersky Endpoint Security for Windows 安装到客户端设备之后的流量值的相关信息（请参见下表）。

网络代理被强制安装，当安装所需文件被管理服务器拷贝到客户端设备上的共享文件夹时。安装后，网络代理使用到管理服务器的连接收回 Kaspersky Endpoint Security for Windows 的分发包。

流量

方案	单一客户端设备的网络代理安装包	在单一客户端设备上安装 Kaspersky Endpoint Security for Windows(数据库已更新)	网络代理和 Kaspersky Endpoint Security for Windows 同时安装
从客户端设备到管理服务器的流量，KB	1638.4	7843.84	9707.52
管理服务器至客户端设备的流量，KB	69,990.4	259,317.76	329,318.4
总流量（单个客户端设备），KB	71,628.8	267,161.6	339,025.92

网络代理被安装在客户端设备后，管理组中的一个设备可以被指派为分发点。它被用于分发安装包。在这个例子中，初始部署反病毒保护的流量随着是否使用 IP 多点传送而显著变化。

如果使用 IP 多点传送，安装包将一次发送到管理组中所有运行中的设备。因此，总流量将会较少 N 倍，N 代表管理组中所有运行中的设备总数。如果不使用 IP 多点传送，总流量等同于分发包从管理服务器下载的情况。然而，包源将会是分发点，而不是管理服务器。

反病毒数据库的原始更新

反病毒数据库初始更新期间（在客户端设备上首次启动数据库更新任务时）的流量速率如下：

- 从客户端设备到管理服务器的流量：1,8 MB。
- 管理服务器至客户端设备的流量：113 MB。
- 总流量（单个客户端设备），114 MB。

数据可能会根据当前反病毒数据库版本而有细微差别。

使客户端和管理服务器同步

此情景描述了当客户端设备和管理服务器之间发生大量数据同步时的管理系统的状态。客户端设备以管理员定义的间隔与管理服务器相连。管理服务器将比较客户端设备与管理服务器的数据、记录客户端设备最近一次连接数据库的信息以及同步数据。

这部分包含当连接客户端到管理服务器时基础管理期间的流量信息(参见下表)。表中数据可能会根据当前反病毒数据库版本而有细微差别。

流量

方案	从客户端设备到管理服务器的流量，KB	管理服务器至客户端设备的流量，KB	总流量（单个客户端设备），KB
在客户端设备上更新数据库之前初始同步	699.44	568.42	1267.86
在客户端设备上更新数据库之后初始同步	735.8	4474.88	5210.68
在客户端设备和管理服务器上未做改变的同步	11.99	6.73	18.72
改变组策略设定值后的同步	9.79	11.39	21.18
改变组任务设定值后的同步	11.27	11.72	22.99
强制客户端设备上未做改变的同步	77.59	99.45	177.04

在管理组中是否选用 IP 多点传送，其总体流量差异相当大。如果选用了 IP 多播，总流量将下降大约 N 倍，N 代表管理组中运行的设备数量。

按照如下情况指定在更新数据库之前和之后的初始同步的流量:

- 安装网络代理和安全应用程序到客户端设备
- 移动客户端设备到管理组
- 应用默认创建的组策略和任务到客户端设备

该表指明了在修改 Kaspersky Endpoint Security 策略设置中包括的保护设置时的流量速率。其他策略设置的数据可能与该表中显示的数据不同。

反病毒数据库附加更新

反病毒数据库上次更新后 20 小时增量更新时的流量比率如下：

- 从客户端设备到管理服务器的流量：169 KB。
- 管理服务器至客户端设备的流量：16 MB。
- 总流量（单个客户端设备），16.3 MB。

表中数据可能会根据当前反病毒数据库版本而有细微差别。

在管理组中是否选用 IP 多点传送，体流量差异相当大。如果选用了 IP 多播，总流量将下降大约 N 倍，N 代表管理组中运行的设备数量。

利用管理服务器对客户端事件的处理

本部分提供了当客户端设备遇到“检测到病毒”事件，并且随后将该事件发送到管理服务器并注册到数据库中时的流量值的相关信息（请参见下表）。

流量

方案	在“检测到病毒”事件发生时到管理服务器的数据传输	在“检测到病毒”事件发生 9 次时到管理服务器的数据传输
从客户端设备到管理服务器的流量，KB	49.66	64.05
管理服务器至客户端设备的流量，KB	28.64	31.97
总流量（单个客户端设备），KB	78.3	96.02

该表中的数据可能根据反病毒程序的当前版本和在其策略中定义的在管理服务器数据库中注册的事件而略有差异。

24小时流量

这部分包含管理系统在“安静”条件(客户端设备和管理服务器都没有数据变化)活动24小时的流量比率的信息(参见下表)。

表中数据描述了标准安装 Kaspersky Security Center 并完成快速启动向导后的网络条件。客户端设备和管理服务器同步的频率是20分钟一次，更新每一小时下载到管理服务器存储库一次。

空闲状态下每 24 小时的流量

流量	参数值
从客户端设备到管理服务器的流量，KB	3235.84
管理服务器至客户端设备的流量，KB	64,378.88
总流量（单个客户端设备），KB	67,614.72

准备移动设备管理

此部分提供下列信息：

- 关于用于通过在 iOS 设备上安装专用 iOS MDM 配置文件来管理它们的 iOS MDM 服务器
- 关于安装了 Kaspersky Endpoint Security for Android 的移动设备的管理

iOS MDM 服务器

iOS MDM 服务器允许您通过在 iOS 设备上安装专用 iOS MDM 配置文件来管理它们。它支持以下功能：

- 设备锁定
- 密码重置
- 数据擦除
- 安装和卸载应用
- 使用带有高级设置（例如 VPN 设置、电子邮件设置、Wi-Fi 设置、摄像头设置、证书设置等等）的 iOS MDM 配置文件

iOS MDM 服务器是一个 Web 服务，它通过 TLS 端口（默认下，端口 443）从移动设备接收传入连接，它被 Kaspersky Security Center 使用网络代理进行管理。网络代理安装在部署了 iOS MDM 服务器的设备本地。

当部署 iOS MDM 服务器时，管理员必须执行以下操作：

- 提供网络代理到管理服务器的访问
- 提供移动设备到 iOS MDM 服务器的 TCP 端口的访问

该部分涉及 iOS MDM 服务器的两个标准配置。

标准配置：DMZ 中的 Kaspersky Device Management for iOS

iOS MDM 服务器位于组织本地网络的 DMZ 中，并提供互联网访问。该方法的一个特殊功能就是当 iOS MDM Web 服务从互联网被设备访问时，将不会出现问题。

因为 iOS MDM 服务器的管理需要网络代理安装在本地，您必须确保网络代理与管理服务器的交互。您可以使用下列可用方法之一进行确保：

- 通过移动管理服务器到 DMZ。
- 通过使用连接网关：

  a. 在部署了 iOS MDM 服务器的设备上，通过连接网关连接网络代理到管理服务器。

  b. 在部署了 iOS MDM 服务器的设备上，分配网络代理作为连接网关。

标准配置：组织本地网络中的 iOS MDM 服务器

iOS MDM 服务器位于组织内部网络。必须启用端口 443（默认端口）以进行外部访问，例如，通过在支持 Kerberos 约束委派的反向代理上发布 iOS MDM Web 服务。

任何标准配置都需要 iOS MDM 服务器（范围 17.0.0.0/8）通过 TCP 端口 2197 访问 Apple Web 服务。该端口用于通过名为 APNs 的专用服务通知设备新命令。

使用 Kaspersky Endpoint Security for Android 管理移动设备

安装了 Kaspersky Endpoint Security for Android™ 的移动设备(也叫 KES 设备)通过管理服务器管理。Kaspersky Security Center 支持以下管理 KES 设备的功能：

- 将移动设备处理为客户端设备：
  - 管理组中的成员关系
  - 监控，例如查看状态、事件和报告
  - 修改本地设置和为 Kaspersky Endpoint Security for Android 分配策略
- 以集中模式发送命令
- 远程安装移动应用包

管理服务器通过 TLS、TCP 端口 13292 管理 KES 设备。

管理服务器性能相关信息

该部分显示了不同硬件配置的管理服务器性能测试的结果，以及连接受管理设备到管理服务器的限制。

连接到管理服务器的限制

管理服务器支持对 100,000 台设备的管理，而不降低性能。

不降低性能而连接到管理服务器的限制：

- 一个管理服务器可以支持最多 500 台虚拟管理服务器。
- 主管理服务器同时支持不多于 1000 个会话。
- 虚拟管理服务器同时支持不多于 1000 个会话。

管理服务器性能测试报告

管理服务器性能测试结果决定了在特定时间间隔内，管理服务器可以同步的最大客户端设备数量。您可以使用此信息选择在计算机网络中部署反病毒保护的最佳方案。

具有以下硬件配置的设备(参见下表)用于测试：

管理服务器硬件配置

参数	参数值
CPU	Intel Xeon CPU E5630，时钟速度 2.53 GHz，2 个套接字，8 核，16 个逻辑处理器
RAM	26 GB
硬盘驱动器	IBM ServeRAID M5014 SCSI 磁盘设备，487 GB
操作系统	Microsoft Windows Server 2019 Standard，版本 10.0.17763，内部版本 17763
网络	QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client)

SQL Server 设备硬件配置

参数	参数值
CPU	Intel Xeon CPU X5570，时钟速度 2.93 GHz，2 个插槽，8 核，16 个逻辑处理器
RAM	32 GB
硬盘驱动器	Adaptec Array SCSI Disk Device，2047 GB
操作系统	Microsoft Windows Server 2019 Standard，版本 10.0.17763，内部版本 17763
网络	Intel 82576 Gigabit

管理服务器支持创建 500 个虚拟管理服务器。

同步间隔是每 10000 台受管理设备 15 分钟（参见下表）。

管理服务器负载测试概要结果

同步间隔（分钟）	受管理设备数量
15	10,000
30	20,000
45	30,000
60	40,000
75	50,000
90	60,000
105	70,000
120	80,000

同步间隔（分钟）	受管理设备数量
135	90,000
150	100,000

如果将管理服务器连接至 MySQL 或 SQL Express 数据库服务器，不建议您使用该应用程序管理 10000 台以上的设备。对于 MariaDB 数据库管理系统，建议的受管理设备最大数量为 20000。

KSN 代理服务器性能测试结果

如果您的企业网络包含大量客户端设备且它们使用管理服务器作为 KSN 代理服务器，管理服务器硬件必须满足特定需求才可以处理来自客户端设备的请求。您可以使用以下测试结果评估您网络中的管理服务器负载，并分配硬件资源以提供 KSN 代理服务器的正常功能。

下表显示了管理服务器和 SQL Server 的硬件配置。此配置用于测试。

管理服务器硬件配置

参数	参数值
CPU	Intel Xeon CPU E5450，时钟速度 3.00 GHz，2 个套接字，8 核，16 个逻辑处理器
RAM	32 GB
操作系统	Microsoft Windows Server 2016 Standard

SQL 服务器硬件配置

参数	参数值
CPU	Intel Xeon CPU E5450，时钟速度 3.00 GHz，2 个套接字，8 核，16 个逻辑处理器
RAM	32 GB
操作系统	Microsoft Windows Server 2019 Standard

下表显示测试结果。

KSN 代理服务器性能测试结果

参数	参数值
每秒处理的最大请求数	4914
最大 CPU 使用	36%

用于与外部服务交互的网络设置

Kaspersky Security Center 使用以下网络设置与外部服务交互。

网络设置	地址	描述
端口：443 协议：HTTPS	activation-v2.kaspersky.com	应用程序激活。
端口：443 协议：HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	更新卡巴斯基数据库、软件模块和应用程序。
端口：443 协议：HTTPS	https://downloads.upd.kaspersky.com	• 更新卡巴斯基数据库、软件模块和应用程序。 • 检查卡巴斯基服务器是否可访问。 在下载卡巴斯基数据库和软件模块之前，Kaspersky Security Center 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。

网络设置	地址	描述
端口：80 协议：HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	更新卡巴斯基数据库、软件模块和应用程序。
端口：443 协议：HTTPS	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	使用卡巴斯基安全网络。
端口：443、1443 协议：HTTPS	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	使用卡巴斯基安全网络。
端口：443 协议：HTTPS	click.kaspersky.com redirect.kaspersky.com	打开界面中的链接。

网络设置	地址	描述
端口：80 协议：HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	这些服务器是公钥基础设施 (PKI) 的一部分，验证卡巴斯基数字签名证书的有效性状态所必需。CRL 是已撤销证书的列表。OCSP 允许您实时请求特定证书的状态。这些服务器有助于确保与数字证书交互的安全性并防止可能的攻击。
端口：443 协议：HTTPS	https://ipm-klca.kaspersky.com	营销公告。

为了让 Kaspersky Security Center 与外部服务正确交互，请考虑以下建议：
- 组织的网络设备和代理服务器上的端口 443 和 1443 必须允许未加密的网络流量。
- 当管理服务器与卡巴斯基更新服务器和卡巴斯基安全网络服务器交互时，必须避免用证书替换劫持网络流量（MITM 攻击）。

要使用 klscflag 实用程序通过 HTTP 或 HTTPS 协议下载更新：

1. 使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. 如果您想通过 HTTP 协议下载更新，请运行以下命令之一：

   - 在安装了管理服务器的设备上：

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - 在分发点上：

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   如果您想通过 HTTPS 协议下载更新，请运行以下命令之一：

   - 在安装了管理服务器的设备上：

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - 在分发点上：

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

部署网络代理和安全应用程序

要管理组织设备，您必须在其上安装网络代理。部署分发的 Kaspersky Security Center 到组织设备通常开始于在其上安装网络代理。

在 Microsoft Windows XP 中，网络代理可能错误执行以下操作：直接从卡巴斯基服务器（作为分发点）下载更新；作为 KSN 代理服务器（作为分发点）；检测第三方漏洞（如果漏洞和补丁管理被使用）。

初始化部署

要管理组织设备，您必须在每台设备上安装网络代理。

可以通过以下方式在运行 Windows 的受管理设备上安装网络代理：

- 使用应用程序远程安装的第三方工具。
- 通过克隆带有操作系统和网络代理的管理员硬盘驱动器镜像，通过使用 Kaspersky Security Center 提供的工具处理磁盘镜像或通过使用第三方工具。
- 对于 Windows 组策略，通过使用标准 Windows 组策略管理工具；或在自动模式下，通过 Kaspersky Security Center 远程安装任务的专用选项。
- 在强制模式下，通过 Kaspersky Security Center 的远程安装任务使用操作系统资源。
- 通过发送设备用户链接到 Kaspersky Security Center 生成的独立包。独立包是包含所选应用程序分发包的定义了设置的可执行模块集合。
- 在设备上手动运行应用程序安装程序。

可以通过以下方式在运行 Windows 的受管理设备上初始安装网络代理：

- 通过 SSH 连接到受管理设备并运行远程安装任务。
- 通过在受管理设备上运行包安装。

可以通过以下方式在运行 macOS 的受管理设备上初始安装网络代理：

- 通过 macOS 分发点运行远程安装任务。
- 通过发送设备用户链接到 Kaspersky Security Center 生成的独立包。独立包是包含所选应用程序分发包的具有预定义设置的可执行模块集合。

在设备上安装网络代理后，您可以通过该网络代理在该设备上执行卡巴斯基应用程序的远程安装。要安装的应用程序分发包通过网络代理和管理服务器之间的通信渠道，与管理员定义的安装设置一并传输。为了传递分发包，您可以使用中继分发节点，即分发点、组播传递等。

当选择部署应用程序到受管理网络的方法和策略时，您必须考虑很多因素（部分列表）：

- 组织网络的配置。
- 设备总数。
- 在组织网络的设备出席、不是任何活动目录域成员；在设备上具有管理员权限的统一账户的出席。
- 管理服务器和设备通道的容量。
- 管理服务器和远程子网之间的通信类型以及那些子网中的网络通道容量。
- 部署开始时在远程设备上应用的安全设置。这些参数允许建立与受管理设备的远程连接并开始安装。

配置安装程序

在开始部署 Kaspersky 应用程序到网络之前，您必须指定安装设置，就是在应用程序安装过程中定义的设置。当安装网络代理时，您应该指定最小值、连接管理服务器的地址，也可能需要一些高级设置。取决于您选择的安装方法，您可以用不同方法定义设置。最简单的方法(在所选设备上的手动交互式安装)，所有相关设置可以通过安装程序用户界面进行定义。

该定义设置的方法不适用于在设备组上的应用程序静默安装。通常情况下，管理员必须集中指定设置值；这些值可能用于在所选网络设备上的静默安装。

安装包

定义应用程序安装设置的第一个和主要的方法是通用的，因此适用于所有安装方法，用 Kaspersky Security Center 工具和多数第三方工具。该方法包括在 Kaspersky Security Center 中创建应用程序安装包。

安装包使用以下方法生成：

- 基于包含的*描述符*(带有 .kud 扩展名的包含了安装和结果分析规则以及其他信息的文件)从指定的分发包自动生成
- 来自安装程序的可执行文件或本地格式（.msi、.deb、.rpm）的安装程序，适用于标准或受支持的应用程序

生成的安装包以包含子文件夹和文件的文件夹形式分层级组织。除了原始分发包，安装包包含可编辑设置(包含安装程序设置和是否在安装结束时重启操作系统等处理规则)以及小的辅助模块。

单独支持的应用程序的安装设置值可以在创建安装包时在管理控制台的用户界面定义。当通过 Kaspersky Security Center 工具执行远程应用程序安装时，安装包被传送到设备，因此运行应用程序安装程序使得所有管理员定义的设置对该应用程序可用。当使用第三方工具安装 Kaspersky 应用程序时，您仅需要确保设备上整个安装包的可用性，即是分发包和其设置的可用性。安装包被 Kaspersky Security Center 创建并存储在共享文件夹下的专用子文件夹。

> 不在安装包参数中显示授权账户的任何细节。

关于在通过第三方工具部署之前对 Kaspersky 应用程序使用该配置方法的说明，参见“使用 Microsoft Windows 组策略部署”。

在 Kaspersky Security Center 安装之后，一些安装包被自动生成；它们可用于安装并包含网络代理和 Microsoft Windows 安全应用程序包。

> 尽管应用程序授权许可密钥可以在安装包属性中设置，但是建议您避免使用此授权许可分发方法，因为这样容易获取对安装包的读访问权限。您应该使用自动分发的授权许可密钥，或使用授权许可密钥安装任务。

MSI 属性和转换文件

另一个在 Windows 平台上配置安装的方法是定义 MSI 属性和转换文件。该方法可以被应用到以下情况：

- 当通过 Windows 组策略安装时，通过使用常规 Microsoft 工具或其他第三方工具处理 Windows 组策略。
- 当使用旨在处理 Microsoft Installer 格式的安装程序的第三方工具安装应用程序时。

使用应用程序远程安装的第三方工具部署

当任何应用程序远程安装工具(例如 Microsoft System Center) 都在组织中可用时，可以使用这些工具进行初始化部署。

必须执行以下操作：

- 选择能最好配合部署工具的配置应用程序的方法。
- 定义用于同步安装包设置修改(通过管理控制台界面)和所选的用于从安装包数据部署应用程序的第三方工具的操作的装置。
- 当从共享文件夹执行安装时，您必须确保该文件资源具有足够容量。

关于 Kaspersky Security Center 中的远程安装任务

Kaspersky Security Center 提供了远程安装应用程序的不同装置，它们作为远程安装任务实现(强制安装、复制硬盘驱动器镜像安装、通过 Microsoft Windows 组策略安装)。您可以为指定管理组和特定设备或设备分类创建远程安装任务（此类任务显示在管理控制台的“**任务**”文件夹中）。当创建任务时，您可以选择安装包(网络代理和/或其他应用程序的安装包)以用此任务安装，并指定定义远程安装方法的设置。此外，您可以使用远程安装向导，基于远程安装任务和结果监控。

管理组的任务影响指定组的设备和所有管理组子组的设备。如果任务中启用了相应设置，任务将覆盖组及其任何子组中包括的从属管理服务器的设备。

特定设备的任务在每一次运行时根据分类内容刷新客户端设备列表。如果分类包含连接到从属管理服务器的设备，任务也将在那些设备上运行。对于那些设置的详情和安装方法请参加以下。

要确保远程安装任务在连接到从属管理服务器的设备上成功操作，您必须使用转发任务提前转发您任务使用的安装包到对应的从属管理服务器。

通过捕获和复制设备镜像来部署

如果您需要安装网络代理到必须安装（或重新安装）操作系统和其他软件的设备，您可以使用捕获和复制设备镜像的机制。

要通过捕获和复制硬盘驱动器来执行部署：

1. 创建安装了操作系统和相关软件的“参考”设备，包含网络代理和安全应用程序。
2. 在设备上捕获参考镜像并通过 Kaspersky Security Center 专用任务分发该镜像到新设备。

   要捕获和安装磁盘镜像，您可以使用组织网可用第三方工具，或者 Kaspersky Security Center 提供的功能（在漏洞和补丁管理授权许可下）。

当从参考镜像部署设备时，如果您使用任何第三方工具处理磁盘镜像，您必须删除 Kaspersky Security Center 用以识别受管理设备的信息。否则，管理服务器将不能正确区分通过复制相同镜像创建的设备。

当使用 Kaspersky Security Center 工具捕获磁盘镜像时，该问题被自动解决。

使用第三方工具复制磁盘镜像

当应用第三方工具捕获安装了网络代理的设备镜像时，使用以下方法之一：

- 推荐方法。在参考设备上安装网络代理时，在网络代理服务第一次运行之前捕获设备映像（因为用于标识设备的唯一信息在网络代理第一次连接到管理服务器时创建）。此后，建议您在镜像捕获操作之前避免运行网络代理服务。ion.
- 在参考设备上，停止网络代理服务并使用 -dupfix 参数运行 klmover 实用工具。实用工具 klmover 包含在网络代理安装包中。在镜像捕获操作完成之前请避免任何网络代理服务的运行。
- 请确保 klmover 将使用 -dupfix 参数运行(强制需求)在目标设备网络代理服务第一次运行之前，在镜像部署后的操作系统第一次启动时。实用工具 klmover 包含在网络代理安装包中。
- 使用网络代理磁盘克隆模式。

> 如果硬盘驱动器映像被错误地复制，可以解决此问题。

您还可以捕获未安装网络代理的设备的镜像。为此，在目标设备上执行镜像部署，然后部署网络代理。如果使用此方法，请使用设备中的独立安装包提供对网络文件夹的访问权限。

硬盘驱动器镜像错误复制

如果网络代理硬盘驱动器镜像不遵照以下部署规则复制，一些设备可能以一个单独的图标在管理控制台一起显示并不断变换名称。

您可以使用下列可用方法之一解决该问题：

- 卸载网络代理

  该方法最可靠。您必须在错误复制镜像的设备上卸载网络代理，使用第三方工具，然后再次安装。网络代理无法通过 Kaspersky Security Center 工具卸载，因为管理服务器工具无法区分错误设备(它们都在管理控制台共享相同的图标)。

- 使用 "-dupfix" 参数运行 klmover 实用工具

  使用第三方工具运行 klmover 实用工具，在网络代理安装文件夹，使用 "-dupfix" 参数(klmover -dupfix)在错误(从镜像错误复制)设备上运行一次。您无法使用 Kaspersky Security Center 工具运行实用工具，因为管理服务器工具无法区分错误设备(它们都在管理控制台共享相同的图标)。

  然后在您运行实用工具之前删除显示错误设备的图标。

- 优化规则以检测错误复制的设备。

  > 该方法仅适用于版本 10 Service Pack 1 或更新的管理服务器和网络代理。

  必须优化检测错误复制的网络代理的规则，以便更改设备 NetBIOS 名称导致这些网络代理的自动“修复”(假设所有复制的设备拥有相同的 NetBIOS 名称)。

在管理服务器设备上，您必须导入以下显示的 reg 文件到注册表，然后重启管理服务器服务。

- 如果 32 位操作系统安装在管理服务器设备：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

- 如果 64 位操作系统安装在管理服务器设备：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

使用 Microsoft Windows 组策略部署

建议您通过 Microsoft Windows 组策略执行网络代理初始化部署，如果满足以下条件：

- 该设备是活动目录域中的成员。
- 部署方案允许您在开始部署网络代理到设备之前，等待下一次目标设备例行重启(或者您可以强制 Windows 组策略应用到这些设备)。

该部署方案包含以下：

- Microsoft Installer 格式的应用程序分发包(MSI 包)位于共享文件夹(目标设备的 LocalSystem 账户对该文件夹具有读权限)。
- 在活动目录组策略中，安装对象被创建用于分发包。
- 安装范围通过指定组织单元(OU)和 / 或安全组设置，包含目标设备。
- 目标设备下一次登录到域中时(设备用户登录到系统之前)，所有已安装的应用程序被检查。如果未找到应用程序，分发包从指定在策略中的资源中下载，然后被安装。

该部署方案的一个好处就是被分配的应用程序在目标设备的操作系统正在加载时被安装，甚至在用户登录到系统之前。即便有带有足够权限的用户卸载了该应用程序，它也将在操作系统下一次重启时被重新安装。该部署方案的劣势是管理员对组策略所做的更改在设备重启之前将不会生效(如果不涉及附加工具)。

您可以使用组策略安装网络代理和其他应用程序，如果它们的安装程序是 Windows Installer 格式。

当选择该部署方案后，您必须评估在应用 Windows 组策略后，从中复制文件到设备的文件资源负载。

通过 Kaspersky Security Center 远程安装任务处理 Microsoft Windows 策略

通过 Microsoft Windows 组策略安装应用程序的最简单方法就是在 Kaspersky Security Center 远程安装任务属性中选择"**在活动目录组策略中指定安装包的安装**"选项。此种情况下，您在运行任务时，管理服务器自动执行以下操作：

- 在 Microsoft Windows 组策略中创建所需对象。
- 创建专用安全组，包含目标设备到这些组，并为它们分配所选应用程序的安装。安全组集将在每一次任务运行时更新，与运行时的设备轮询一致。

要使该功能可操作，在任务属性中，指定对活动目录组策略有写权限的账户。

如果您要通过相同任务安装网络代理和其他应用程序，选择"**在活动目录组策略中指定安装包的安装**"选项将导致应用程序仅为网络代理在活动目录策略中创建安装对象。任务中所选的第二个应用程序将通过网络代理工具被安装，网络代理一旦安装在设备就开始安装。如果您要通过 Windows 组策略安装网络代理之外的应用程序，您必须仅为该安装包创建安装任务（没有网络代理包）。不是每个应用程序都可以使用 Microsoft Windows 组策略安装。要查找此能力，您可以参考安装应用程序的方法信息。

如果所需的对象通过 Kaspersky Security Center 工具被创建在组策略，Kaspersky Security Center 的共享文件夹将被用于安装包来源。当计划部署时，您必须将权衡该文件夹的读取速度和设备数量以及要安装的分发包大小。最好将 Kaspersky Security Center 的共享文件夹位于高性能专用文件存储库。

除了使用方便，通过 Kaspersky Security Center 自动创建 Windows 组策略还有如下好处：当计划网络代理安装时，您可以轻松指定安装完成后设备要被自动移动到的 Kaspersky Security Center 管理组。您可以在新任务向导或远程安装任务窗口设置中指定该组。

当通过 Kaspersky Security Center 处理 Windows 组策略时，您可以通过创建安全组为组策略对象指定设备。Kaspersky Security Center 同步安全组内容与任务中设备的当前集。当使用其他工具处理组策略时，您可以将组策略对象与所选的活动目录 OU 直接关联。

通过 Microsoft Windows 策略独立安装应用程序

管理员可以用自己名义在 Windows 组策略中创建安装所需的对象。此种情况下，他/她可以提供存储在 Kaspersky Security Center 共享文件夹中的包链接，或者上传这些包到专用文件服务器并提供相关链接。

可能有以下安装方案：

- 管理员创建安装包并在管理控制台设置其属性。组策略对象提供 Kaspersky Security Center 共享文件夹中的包的 MSI 文件的链接。
- 管理员创建安装包并在管理控制台设置其属性。然后管理员复制 Kaspersky Security Center 共享文件夹中整个 EXEC 子文件夹到组织专用文件资源的文件夹。组策略对象提供组织专用文件资源子文件夹中的包的 MSI 文件的链接。
- 管理员从互联网下载应用程序分发包(包括网络代理包)并将其上传到组织专用文件资源。组策略对象提供组织专用文件资源子文件夹中的包的 MSI 文件的链接。安装设置通过配置 MSI 属性或通过配置 MST 转换文件来定义。

通过 Kaspersky Security Center 远程安装任务的强制部署

要执行网络代理或其他应用程序的初始部署，您可以使用 Kaspersky Security Center 的远程安装任务强制安装选定的安装包，前提是每台设备都有具有本地管理员权限的用户账户。

强制安装也可以在设备无法被管理服务器直接访问时应用：例如，设备在隔离网络中，或者设备在本地网络但管理服务器在 DMZ。

初始部署时，不会安装网络代理。因此，在远程安装任务的设置中，无法选择使用网络代理安装应用程序所需的文件分发。您只能选择通过管理服务器或分发点使用操作系统资源来分发文件。

管理服务器服务必须使用在目标设备上具有管理权限的账户运行。或者，您可以在远程安装任务的设置中指定有权访问 admin$ share 的账户。

> 默认情况下，远程安装任务使用管理服务器运行所用账户的凭据应用到设备。需要澄清的是，这是用于访问 admin$ share 的账户，而不是运行远程安装任务的账户。安装在 LocalSystem 账户下进行。

您可以明确指定目标设备(使用列表)、通过选择它们所属的 Kaspersky Security Center 管理组或通过基于指定标准创建设备分类。安装开始时间定义在任务计划中。如果任务属性中启用了**运行错过的任务**设置，任务可以在设备开启时立即运行，或设备被移动到目标管理组时立即运行。

强制安装包括传送安装包到目标设备、随后复制文件到每个目标设备的 admin$ 资源，和在这些设备上远程注册支持服务。传送安装包到目标设备通过 Kaspersky Security Center 的网络交互功能运行。以下条件必须在此种情况下被满足：

- 目标设备可以从管理服务器端或分发点端访问。
- 目标设备的名称解析在网络中运行正常。
- 设备上的管理共享(admin$)保持启用。
- 以下系统服务正在目标设备上运行：
  - 服务器（LanmanServer）
    默认情况下，该服务正在运行。
  - DCOM 服务器进程启动器 (DcomLaunch)
  - RPC 端点映射器 (RpcEptMapper)
  - 远程过程调用 (RpcSs)
- TCP 445 端口在目标设备上打开，以便通过 Windows 管理工具实现远程访问。

  > TCP 139、UDP 137 和 UDP 138 由较旧的协议使用，对于当前应用程序来说不再是必需的。

  防火墙必须允许动态出站访问端口，以便从管理服务器和分发点连接到目标设备。
- 在网络代理部署期间，允许 Active Directory 域策略安全设置提供 NTLM 协议的操作。

- 在运行 Microsoft Windows XP 的目标设备上，简单文件共享模式被禁用。
- 在目标设备上，访问共享和安全模型被设置为*经典 - 本地用户以自身进行身份验证*。它绝不可以是*仅限访客 – 本地用户需要以访客身份进行身份验证*。
- 目标设备是域成员，或带有管理员权限的统一账户提前在目标设备上被创建。

要成功部署网络代理或其他应用程序到未加入 Windows Server 2003 或更高版本的 Active Directory 域的设备，您必须在该设备上禁用远程 UAC。远程 UAC 是阻止本地管理账户访问 admin$ 的原因之一，这对于强制部署网络代理或其他应用程序必不可少。禁用远程 UAC 不会影响本地 UAC。

在未分配到任何 Kaspersky Security Center 管理组的新设备上进行安装时，您可以打开远程安装任务属性并指定网络代理安装后设备要移动到的管理组。

当创建组任务时，记住每个组任务都影响所选组的潜逃组中的所有设备。因此，您必须避免在子组中的重复安装任务。

创建强制安装应用程序的任务的一个简化方法是自动安装。为此，您必须打开管理组属性，打开安装包列表，然后选择必须在该组中设备上安装的包。结果，所选安装包将被自动安装在该组和其所有子组中的所有设备上。包被安装的时间间隔取决于网络吞吐量和网络设备总数。

为了减轻管理服务器在向目标设备传送安装包时的负载，您可以在安装任务中选择通过分发点进行安装。注意，该安装方法给作为分发点的设备增加了大量负载。因此，建议您选择符合分布点要求的设备。如果您使用分发点，您必须确保它们存在于托管目标设备的每个隔离子网中。

使用分发点作为本地安装中心也可以用在与管理服务器具有窄通道通信的子网设备上的安装，此时子网中的通道带宽很高。

文件夹 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 所在分区的磁盘剩余空间必须超过所安装应用程序的分发包的总大小的好几倍。

运行 Kaspersky Security Center 创建的独立包

以上描述的网络代理和其他应用程序的初始化部署方法无法总被实现，因为不可能满足所有可应用条件。此种情况下，您可以通过 Kaspersky Security Center 创建通用可执行文件，叫做*独立安装包*，使用管理员准备的带有相关安装设置的安装包。独立安装包存储在 Kaspersky Security Center 共享文件夹。

您可以使用 Kaspersky Security Center 来给所选用户发送包含该共享文件夹文件链接的电子邮件，提示他们运行该文件(在交互模式或静默模式)。您可以附加独立安装包到电子邮件，然后发送它到对 Kaspersky Security Center 共享文件夹没有访问权限的设备用户。管理员也可以复制独立包到可移动驱动器，将其传送到相关设备然后稍后运行。

您可以从网络代理包或其他应用程序包创建独立包(例如，安全应用程序)。如果独立包从网络代理和其他应用程序创建，安装和网络代理一起启动。

当创建带有网络代理的独立包时，您可以指定当网络代理安装完成时，新设备(未分配到任何管理组的设备)将被自动移动到的管理组。

独立包可以在交互模式下运行(默认)，显示应用程序安装结果，或者可以运行在静默模式(以参数 "-s" 运行)。静默模式可以用在从脚本安装，例如操作系统镜像部署后要运行的脚本。静默模式安装的结果决定与进程返回代码。

单机版 Linux 网络代理具有来自 nmap 实用程序的可选依赖项。如果 nmap 实用程序缺失或早于版本 6.0，则 Broadcast DHCP Discover 功能不受支持。

手动安装应用程序的选项

管理员或资深用户可以在交互模式下手动安装应用程序。他们可以使用原始分发包或从其他生成并存储在 Kaspersky Security Center 共享文件夹的安装包。默认下，安装程序在交互模式下运行并提示用户所需的设置值。然而，当使用参数 "-s" 从安装包根目录运行 setup.exe 进程时，安装程序将运行在静默模式，使用配置安装包时定义的设置。

当从存储在 Kaspersky Security Center 共享文件夹的安装包的根目录运行 setup.exe 时，包先被复制到临时文件夹，然后应用程序安装程序将从本地文件夹运行。

创建 MST 文件

要转换 MSI 包的内容并将自定义设置应用到现有 MSI 文件，您必须创建 MST 格式的转换文件。为此，请使用包括在 Windows SDK 中的 Orca.exe 编辑器。

要创建 MST 文件：

1. 运行 Orca.exe 编辑器。
2. 转到**文件**选项卡，然后在菜单中单击**打开**。
3. 选择 Kaspersky Network Agent.msi 文件。
4. 转到**转换**选项卡，然后在菜单中选择**新建转换**。
5. 在**表格**列中，选择**属性**并写入以下值：
   - *EULA=1*
   - *SERVERADDRESS=<管理服务器地址>*

   单击“**保存**”按钮。
6. 转到**转换**选项卡，然后在菜单中选择**生成转换**。
7. 在打开的窗口中，指定您创建的转换文件的名称，然后单击**保存**按钮。

MST 文件已保存。

在安装有网络代理的设备上远程安装应用程序

如果连接到主管理服务器（或任何其从属管理服务器）的可操作网络代理被安装到设备，您可以升级该设备上的网络代理，以及通过网络代理安装、升级或卸载支持的应用程序。

您可以在远程安装任务的属性中启用“**使用网络代理**”选项。

如果选择此选项，带有管理员定义的安装设置的安装包将被通过网络代理和管理服务器之间的通信渠道传输到目标设备。

要优化管理服务器负载和最小化管理服务器和设备之间的流量，最好为每个远程网络或每个多播域分配分发点（请参见"关于分发点"部分和"创建管理组结构和分配分发点"部分）。此种情况下，安装包和安装设置通过分发点从管理服务器分发到目标设备。

而且，您可以使用分发点来多播传送安装包，这将允许您在部署应用程序时显著降低网络流量。

当通过网络代理和管理服务器之间的通信渠道传输安装包到目标设备时，所有准备传输的安装包都将被缓存在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer 文件夹。当使用多个不同类型的大安装包并涉及大量分发点时，该文件夹的尺寸将显著增长。

文件不能从 FTServer 文件夹手动删除。当原始安装包被删除时，对应数据将被自动从 FTServer 文件夹删除。

分发点接收的数据保存在文件夹 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp。

文件不能从 $FTCITmp 文件夹手动删除。使用该文件夹数据的任务完成后，该文件夹的内容将被永久删除。

因为安装包从中转存储库以优化传输的格式通过管理服务器与网络代理之间的通信渠道进行分发，原始文件夹里的安装包不允许更改。这些更改将不会被管理服务器自动注册。如果您需要手动修改安装包的文件(尽管建议您避免此方案)，您必须在管理控制台编辑安装包的任何设置。在管理控制台编辑安装包的设置导致管理服务器在目标设备传输缓存中更新安装包镜像。

在远程安装任务中管理设备重启

设备经常需要在完成应用程序远程安装时重启(尤其在 Windows)。

如果您使用 Kaspersky Security Center 远程安装任务，在新任务向导或所创建任务的属性窗口（**操作系统重启**区域）中，您可以选择 Windows 设备要求重启时执行的操作：

- **不重启设备**。此种情况下，自动重启不会运行。要完成安装，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息将被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的安装任务。
- **重启设备**。此种情况下，如果完成安装需要重启，设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的安装任务。
- **提示用户操作**。此种情况下，客户端设备上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。**提示用户操作**最适用于用户需要选择最合适重启时间的工作站。

安全应用程序安装包上的数据库更新

开始保护部署之前，您必须注意要随安全应用程序的分发包一起更新反病毒数据库(包块模块和自动补丁)。最好在开始部署之前更新应用程序安装包中的数据库(例如， 通过使用所选安装包上下文菜单中的相关命令)。这将减少目标设备在完成保护部署后所需的重启次数。

在 Kaspersky Security Center 中使用工具远程安装应用程序以便在受管理设备上运行相关可执行文件

使用新安装包向导，您可以选择任何可执行文件并为其定义命令行设置。为此，您可以添加所选文件或整个文件所在文件夹到安装包。然后，您必须创建远程安装任务并选择所创建的安装包。

当任务正在运行时，带有命令行所定义设置的指定可执行文件将在目标设备上运行。

如果您使用 Microsoft Windows Installer (MSI) 格式的安装程序，Kaspersky Security Center 使用标准工具分子安装结果。

如果有漏洞和补丁管理授权许可可用，Kaspersky Security Center (当为任何企业环境中支持的应用程序创建安装包时)也使用安装和安装结果分析规则。

否则，可执行文件的默认任务将等待运行中进程和所有子进程的完成。在所有运行中进程完成后，任务将被成功完成，不管初始进程的返回码是什么。要更改该任务的此类行为，在创建任务之前，您必须手动修改 Kaspersky Security Center 在新创建的安装包所在的文件夹及其子文件夹中生成的 .kpd 文件。

.kpd 文件使用 ASCII 编码。.kud 文件使用 Unicode 编码。

对于不需要等待运行中进程完成的任务，设置 [SetupProcessResult] 区域的等待设置的值为 0：

```
[SetupProcessResult]
Wait=0
```

对于仅需要等待 Windows 运行中进程，而不是所有子进程完成的任务，设置 [SetupProcessResult] 区域的 WaitJob 设置值为 0，例如：

```
[SetupProcessResult]
WaitJob=0
```

若要任务成功完成或者返回错误（具体取决于运行进程的返回码），创建一个将把错误代码保存到文件的可执行 .bat 文件，例如：

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

然后修改 Kaspersky Security Center 在新创建的安装包的文件夹中生成的 .kud 文件：

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0= 安装成功完成。
[SetupMainResult_ErrorCodes]
1=安装脚本错误
2=自定义错误
```

此种情况下，任何非列表中的返回码都会导致返回错误。

要在任务成功完成或任务结果错误中显示注释，在 [SetupProcessResult_SuccessCodes] 和 [SetupProcessResult_ErrorCodes] 区域根据进程返回码输入错误的简短描述，例如：

```
[SetupProcessResult_SuccessCodes]
0= 安装成功完成
3010=需要重启以完成安装
[SetupProcessResult_ErrorCodes]
1602=安装被用户取消
1603=安装过程中出现致命错误
```

要使用 Kaspersky Security Center 工具管理设备重启(如果需要重启以完成操作)，列出暗示重启的进程返回码，在 [SetupProcessResult_NeedReboot] 区域：

```
[SetupProcessResult_NeedReboot]
3010=
```

监控部署

要监控 Kaspersky Security Center 部署并确保在受管理设备上安装了安全应用程序和网络代理，您必须在“**部署**”区域检查信号灯。该信号灯位于管理控制台主窗口的管理服务器节点工作区。信号灯反映了当前部署状态。安装了网络代理和安全应用程序的设备数量显示在信号灯旁边。当任何安装任务正在运行时，您可以监控它们的进程。如果有任何安装错误发生，错误数量被显示。您可以通过点击链接查看错误详情。

您也可以在“**组**”选项卡上的“**受管理设备**”文件夹的工作区中使用部署方案。图表反映了部署进程，显示没有网络代理、带有网络代理或带有网络代理和安全应用程序的设备数量。

对于更多部署进程（或者特定安装任务的操作）的详情，请打开相关远程安装任务的结果窗口：右击任务并在上下文菜单中选择“**结果**”。窗口显示了两个列表：上面一个包含设备上的任务状态，下面一个包含从上面列表中选择的设备上的任务事件。

部署错误的信息被添加到管理服务器上的卡巴斯基事件日志。也可以通过“**事件**”选项卡上管理服务器节点中相应的事件分类来获得有关错误的信息。

配置安装程序

该部分提供了 Kaspersky Security Center 安装程序文件和安装设置的信息，以及如何在静默模式安装管理服务器和网络代理的建议。

常规信息

Kaspersky Security Center 15.1 组件(管理服务器、网络代理和管理控制台)的安装程序根据 Windows Installer 技术创建。MSI 包是安装程序的核心。该格式的包允许使用 Windows Installer 的所有好处：可量测性、补丁系统可用性、转换系统、通过第三方解决方案集中安装以及在操作系统中透明注册。

在静默模式下安装(带有响应文件)

管理服务器和网络代理安装程序可以使用响应文件工作(ss_install.xml)，其中整合了不需要用户参与的静默模式安装参数。ss_install.xml 文件位于与 MSI 包相同的文件夹；在静默模式安装时被自动使用。您可以通过命令行参数“/s”启用静默安装模式。

一个大概例子运行如下：

```
setup.exe /s
```

在以静默模式启动安装程序之前，请阅读最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。

ss_install.xml 文件 Kaspersky Security Center 安装程序参数的内部格式的实例。分发包包含带有默认参数的 ss_install.xml 文件。

请不要手动修改 ss_install.xml 文件。该文件可以通过 Kaspersky Security Center 工具修改，当在管理控制台编辑安装包参数时。

要修改管理服务器安装的响应文件：

1. 打开 Kaspersky Security Center 分发包。如果您使用完整的包 EXE 文件，请将其解压缩。
2. 从 Server 文件夹中，打开命令行，然后运行以下命令：

   ```
   setup.exe /r ss_install.xml
   ```

   Kaspersky Security Center 安装程序启动。
3. 按照向导的步骤配置 Kaspersky Security Center 安装。

   当您完成向导时，响应文件会根据您指定的新设置自动修改。

在静默模式下安装网络代理（没有响应文件）

您可以使用单独 .msi 包安装网络代理，以标准方法指定 MSI 属性的值。该方案允许网络代理使用组策略安装。

请勿将安装包重命名为 Kaspersky Network Agent.msi。重命名此包可能会导致将来更新网络代理时出现安装错误。

要避免通过 MSI 包属性定义的参数与响应文件中定义的参数冲突，您可以通过设置属性 `DONT_USE_ANSWER_FILE=1` 来禁用响应文件。MSI 文件位于 Kaspersky Security Center 分发包，在 Packages\NetAgent\exec 文件夹。一个带有 .msi 包的网络代理安装程序运行例子如下。

在静默模式下安装网络代理需要接受最终用户授权许可协议的条款。只有在您完全阅读、理解并接受最终用户授权许可协议的条款后，才使用 `EULA=1` 参数。

```
例如：
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

您也可以通过提前准备响应文件(带有 .mst 扩展名)来定义 msi 包的安装参数。该命令显示如下：

```
例如：
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

您可以在单一命令行中指定几个响应文件。

如果要使用 Windows 安装程序升级网络代理，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

通过 setup.exe 的部分安装配置

当通过 setup.exe 运行应用程序安装时，您可以添加 MSI 任何属性的值到 MSI 包。

该命令显示如下：

例如：
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

管理服务器安装参数

下表描述了安装管理服务器时您可以配置的 MSI 属性。所有参数都是可选的，除了 EULA 和隐私策略。

静默模式下安装管理服务器的参数

MSI 属性	描述	可用值
EULA	是否接受授权许可协议条款（必需）。	• 1 – 我已完全阅读、理解并接受最终用户授权许可协议的条款。 • 其它值或没有值 – 我不接受授权许可协议的条款（将不会执行安装）。
PRIVACYPOLICY	是否接受隐私策略条款（必需）	• 1 – 我了解并同意我的数据将按照《隐私策略》中的说明进行处理和传输（包括第三国家/地区）。我确认已完全阅读并理解《隐私策略》。 • 其它值或没有值 – 我不接受隐私策略的条款（将不会执行安装）。
INSTALLATIONMODETYPE	管理服务器安装类型	• 标准。 • 自定义。
INSTALLDIR	应用程序的安装文件夹	字符串值。
ADDLOCAL	要安装的组件列表(以逗号分隔)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 管理服务器安装正常运行的最小组件列表： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	网络大小	• NRT_1_100 - 从 1 到 100 个设备。 • NRT_100_1000 - 101 到 1000 台设备。 • NRT_GREATER_1000 - 多于 1,000 台设备。
SRV_ACCOUNT_TYPE	指定操作管理服务器服务的用户的方法	• SrvAccountDefault - 将自动创建用户账户。 • SrvAccountUser - 手动定义用户账户。
SERVERACCOUNTNAME	服务用户名	字符串值。
SERVERACCOUNTPWD	服务用户密码	字符串值。
DBTYPE	数据库类型	• MySQL – 将使用 MySQL 或 MariaDB 数据库。 • MSSQL – Microsoft SQL Server (SQL Express) 数据库将被使用。
MYSQLSERVERNAME	MySQL 或 MariaDB 服务器的完整名称	字符串值。
MYSQLSERVERPORT	连接到 MySQL 或 MariaDB 服务器的端口号	数字值。
MYSQLDBNAME	MySQL 或 MariaDB 服务器数据库名称	字符串值。
MYSQLACCOUNTNAME	连接到 MySQL 或 MariaDB 服务器数据库的用户名	字符串值。

MSI 属性	描述	可用值
MYSQLACCOUNTPWD	连接到 MySQL 或 MariaDB 服务器数据库的用户密码	字符串值。
MSSQLCONNECTIONTYPE	MSSQL 数据库使用类型	• InstallMSSEE — 从包安装。 • ChooseExisting – 使用已安装服务器。
MSSQLSERVERNAME	SQL Server 实例的完整名称	字符串值。
MSSQLDBNAME	SQL Server 数据库名称	字符串值。
MSSQLAUTHTYPE	连接到 SQL Server 的身份验证方法	• Windows。 • SQLServer。
MSSQLACCOUNTNAME	以 SQLServer 模式连接到 SQL Server 的用户名	字符串值。
MSSQLACCOUNTPWD	以 SQLServer 模式连接到 SQL Server 的用户密码	字符串值。

CREATE_SHARE_TYPE	指定共享文件夹的方法	• Create—创建新共享文件夹。此种情况下，必须定义以下属性：
		  • SHARELOCALPATH – 本地文件夹路径。
		  • SHAREFOLDERNAME — 文件夹的网络名称。
		• Null — EXISTSHAREFOLDERNAME 必须被正确指定。

EXISTSHAREFOLDERNAME	现有共享文件夹的完整路径	字符串值。
SERVERPORT	连接至管理服务器的端口号	数字值。
SERVERSSLPORT	建立到管理服务器的 SSL 连接的端口号	数字值。
SERVERADDRESS	管理服务器地址	字符串值。
SERVERCERT2048BITS	管理服务器证书密钥长度（位）	• 1 – 管理服务器证书的密钥长度为 2048 位。 • 0 – 管理服务器证书的密钥长度为 1024 位。 • 如果未指定值，管理服务器证书的密钥长度为 2048 位。
MOBILESERVERADDRESS	连接移动设备的管理服务器地址；如果未选择 MobileSupport 组件则忽略	字符串值。

网络代理安装参数

下表描述了安装网络代理时您可以配置的 MSI 属性。所有参数都是可选的，除了 EULA 和服务器地址。

静默模式下安装网络代理的参数

MSI 属性	描述	可用值
EULA	是否接受授权许可协议条款	• 1 – 本人确认已完全阅读、理解并接受本最终用户授权许可协议的条款和条件。 • 0 – 我不接受授权许可协议的条款（将不会执行安装）。 • 没有值 – 我不接受授权许可协议的条款（将不会执行安装）。
DONT_USE_ANSWER_FILE	从响应文件读取安装设置	• 1–不使用。 • 其它值或没有值 – 读取。
INSTALLDIR	网络代理安装文件夹路径	字符串值。
SERVERADDRESS	管理服务器地址(必需)	字符串值。
SERVERPORT	连接管理服务器的端口号	数字值。

MSI 属性	描述	可用值
SERVERSSLPORT	使用 SSL 协议加密连接到管理服务器的端口号	数字值。
USESSL	是否使用 SSL 连接	• 1 – 使用。 • 其它值或没有值 – 不使用。
OPENUDPPORT	是否打开 UDP 端口	• 1 – 打开。 • 其它值或没有值 – 不打开。
UDPPORT	UDP 端口号	数字值。
USEPROXY	是否使用代理服务器。 为了兼容性，不建议在网络代理安装包设置中指定代理连接设置。	• 1 – 使用。 • 其它值或没有值 – 不使用。
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	连接到代理服务器的代理地址和端口号	字符串值。
PROXYLOGIN	连接代理服务器的账户	字符串值。
PROXYPASSWORD	用于连接到代理服务器的账户密码（不要在安装包参数中指定授权账户的任何细节。）	字符串值。
GATEWAYMODE	连接网关使用模式	• 0 – 不使用连接网关。 • 1 – 使用该网络代理作为连接网关。 • 2 – 使用连接网关连接到管理服务器。
GATEWAYADDRESS	连接网关地址	字符串值。
CERTSELECTION	接收证书的方法	• GetOnFirstConnection – 从管理服务器接收证书。 • GetExistent – 如果选中此选项则选择现有证书，必须指定 CERTFILE 属性。
CERTFILE	证书文件路径	字符串值。
VMVDI	启用虚拟桌面基础架构（VDI）的动态模式	• 1 – 启用。 • 0 – 不启用。 • 没有值 – 不启用。
VMOPTIMIZE	网络代理设置是否对虚拟机监控程序优化	• 1 – 启用。 • 0 – 不启用。 • 没有值 – 不启用。
LAUNCHPROGRAM	安装后是否启动网络代理服务。如果 VMVDI=1，则忽略该参数	• 1 – 启动。 • 其它值或没有值 – 不启动。
NAGENTTAGS	网络代理标签（优先级高于响应文件中给定的标签）	字符串值。

虚拟基础架构

Kaspersky Security Center 支持虚拟机的使用。您可以在每台虚拟机上安装网络代理和安全应用程序，并可以在虚拟机监控程序级别保护虚拟机。在第一种情况下，您可以使用标准安全应用程序或 Kaspersky Security for Virtualization Light Agent 来保护您的虚拟机。在第二种情况下，您可以使用 Kaspersky Security for Virtualization Agentless。

Kaspersky Security Center 支持虚拟机回滚到先前状态。

降低虚拟机负载的窍门

当安装网络代理到虚拟机时，建议您禁用一些对虚拟机没有用的 Kaspersky Security Center 功能。

在虚拟机或用于生成虚拟机的模版上安装网络代理时，建议执行以下操作：

- 如果要运行远程安装，则在网络代理安装包的属性窗口的“**高级**”区域中，选择“**优化 VDI 设置**”选项。
- 如果要通过向导运行交互式安装，则在向导窗口中选择“**为虚拟基础架构优化网络代理设置**”选项。

选择这些选项将改变网络代理设置，因此以下功能在默认情况下保持禁用状态（在应用策略之前）：

- 获取已安装软件的信息
- 获取硬件信息
- 获取检测到的漏洞信息
- 获取需要更新的信息

通常，这些功能对于虚拟机不必要，因为它们使用统一软件和虚拟硬件。

禁用该功能是不可逆的。如果需要任何被禁用的功能，您可以通过网络代理策略启用它，或通过网络代理本地设置。网络代理本地设置通过管理控制台中相关设备的上下文菜单可用。

对动态虚拟机的支持

Kaspersky Security Center 支持动态虚拟机。如果虚拟架构部署在组织网络，动态（临时）虚拟机可以被用在特定情况。动态虚拟机基于管理员提供的模板以独立名称创建。用户使用了虚拟机一段时间，然后关闭虚拟机，则该虚拟机将从虚拟基础架构中删除。如果 Kaspersky Security Center 部署在组织网络，安装了网络代理的虚拟机将被添加到管理服务器数据库。在您关闭虚拟机后，对应的条目必须从管理服务器数据库中删除。

要运行自动删除虚拟机上的条目的功能，在动态虚拟机的模板上安装网络代理时，请选中“**启用 VDI 动态模式**”选项：

- 对于远程安装–在网络代理安装包的属性窗口（**高级**区域）
- 对于交互式安装 – 在“网络代理安装向导”中进行

> 当安装网络代理到物理设备时，不要选中“**启用 VDI 动态模式**”选项。

如果您要在删除虚拟机后将动态虚拟机的事件存储在管理服务器一段时间，那么，在管理服务器属性窗口，在“**事件存储库**”区域，选择“**设备被删除后存储事件**”选项并指定事件的最大存储期限（天）。

> 我们不建议在动态虚拟机上启用加密驱动器。

对虚拟机复制的支持

复制安装了网络代理的虚拟机或从安装了网络代理的模板创建虚拟机，和捕获和复制硬盘驱动器镜像的网络代理部署相同。因此，常规情况下，当复制虚拟机时，您需要执行与通过复制磁盘镜像部署网络代理时相同的操作。

然而，以下描述的两种情况展示了自动检测复制的网络代理。由于以上原因，您不必运行“通过捕获和复制设备磁盘镜像部署”中描述的复杂操作：

- “**启用 VDI 动态模式**”选项在网络代理被安装时选中：在操作系统每次重启后，该虚拟机将被认为是新设备，无论是否被复制。
- 以下 Hypervisor 之一被使用：VMware™、HyperV® 或 Xen®：网络代理通过更改的虚拟硬件 ID 检测虚拟机的复制。

虚拟硬件更改分析并不绝对可靠。在广泛应用该方法之前，您必须在小组虚拟机上测试您组织中使用的当前 hypervisor 版本。

对网络代理设备文件系统回滚的支持

Kaspersky Security Center 是一个分发的应用程序。在安装了网络代理的设备上回滚文件系统到先前状态将导致数据不同步和 Kaspersky Security Center 功能不正常。

文件系统(或一部分)可以在以下情况下回滚：

- 当复制硬件驱动器镜像时。
- 当通过虚拟架构恢复虚拟机状态时。
- 当从备份副本或恢复点恢复数据时。

安装了网络代理的设备上的第三方软件影响 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 文件夹的情景仅是 Kaspersky Security Center 的关键情景。因此，如果可能，您必须总是从恢复进程中排除该文件夹。

因此一些组织的工作规则提供了对设备文件系统的回滚，对安装了网络代理的设备的文件系统回滚的支持被添加到了 Kaspersky Security Center，从版本 10 Maintenance Release 1 开始(管理服务器和网络代理必须是版本 10 Maintenance Release 1 或更新)。当检测到时，这些设备被自动连接到管理服务器，带有完整数据清除和完整同步。

默认下，对文件系统回滚检测的支持在 Kaspersky Security Center 15.1 中被启用。

尽量不要回滚网络代理设备的 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 文件夹，因为完整数据的重新同步需要大量资源。

系统状态回滚在管理服务器设备上是不允许的。管理服务器使用的数据库的回滚也是不允许的。

您可以仅可以使用标准的 klbackup 实用工具从备份副本恢复管理服务器状态。

应用程序的本地安装

此部分介绍仅可在本地设备上安装的应用程序的安装过程。

要在所选客户端设备上执行应用程序本地安装，您必须具有此设备的管理员权限。

要在所选客户端设备上本地安装应用程序：

1. 在客户端设备上安装网络代理并配置客户端设备和管理服务器之间的连接。
2. 按照这些应用程序的指南说明，在设备上安装相关的应用程序。
3. 为每个在管理员工作站上安装的应用程序安装管理插件。

Kaspersky Security Center 还支持使用独立安装包进行应用程序本地安装。Kaspersky Security Center 不支持所有 Kaspersky 应用程序的安装。

网络代理的本地安装

要在设备上本地安装网络代理：

1. 在设备上，运行从互联网下载的分发包中的 setup.exe 文件。有关详细信息，请参阅以下主题：从 Kaspersky Security Center 分发工具包获取网络代理安装包。

   提示您选择要安装的 Kaspersky 程序的窗口将打开。

2. 在应用程序选择窗口中，单击“**仅安装 Kaspersky Security Center 网络代理**”链接以启动网络代理安装向导。遵照向导的说明操作。

   a. **管理服务器**

   端口

   指定管理服务器用于接收来自网络代理的连接的非 SSL 端口。

   默认情况下，此选项设置为 14000。

   SSL 端口

   指定管理服务器用于接收来自网络代理的连接的 SSL 端口。

   默认情况下，此选项设置为 13000。

   使用 SSL 连接到管理服务器

   如果启用此选项，则使用 SSL 协议通过安全端口连接管理服务器。

   默认情况下已启用该选项。

   允许网络代理打开 UDP 端口

   如果启用此选项，安装程序会自动打开管理服务器使用的端口来管理客户端设备并接收有关它的信息。

   默认情况下已启用该选项。

   UDP 端口

   可让您配置管理服务器用于管理客户端设备并接收有关它的信息的端口。

   默认情况下，此选项设置为 15000。

b. **代理服务器配置**

使用代理服务器

如果启用此选项，您可以指定代理服务器身份验证的凭据。

我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

默认情况下已禁用该选项。

地址

端口

账户

建立连接代理服务器的账户的用户名。

我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

密码

建立连接代理服务器的账户的密码。

我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

c. **连接网关**

不使用连接网关

使用网络代理作为 DMZ 连接网关

选择此选项使用网络代理作为非管制区域 (DMZ) 中的连接网关以连接到管理服务器，与之通信，以及在数据传输过程中保持网络代理上的数据安全。

通过使用连接网关连接到管理服务器

选择此选项，然后指定将充当连接网关的设备。

d. **管理服务器证书**

e. **代理标签**

f. **高级设置**

对未定义状态的组件自动安装可应用更新和补丁

我们建议保持此选项启用。您可以清除此选项以禁用 Kaspersky Security Center 组件的自动更新和修补。管理员可以使用策略重新启用自动更新和补丁。

默认情况下已禁用该选项。

启用网络代理服务保护

当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

默认情况下已禁用该选项。

启用 VDI 动态模式

如果启用此选项，将针对虚拟机上安装的网络代理启用虚拟桌面基础架构 (VDI) 的动态模式。

默认情况下已禁用该选项。

优化 VDI 的 Kaspersky Security Center 网络代理设置。禁用漏洞扫描以及应用程序和硬件清查。您可以通过网络代理策略编辑当前设置。

如果启用此选项，网络代理设置中将禁用以下功能：

- 获取已安装软件的信息
- 获取硬件信息
- 获取检测到的漏洞信息
- 获取需要更新的信息

默认情况下已禁用该选项。

g. **启动应用程序**

安装向导完成后，网络代理被安装在设备。

您可以查看 Kaspersky Security Center 网络代理服务的属性，还可以使用标准的 Microsoft Windows 工具（计算机管理\服务）来启动、停止或监控网络代理活动。

在静默模式下安装网络代理

网络代理可以在静默模式下安装，即，无需交互式输入安装参数。静默安装使用网络代理的 Windows Installer 数据包 (MSI)。MSI 文件位于 Kaspersky Security Center 分发包，在 Packages\NetAgent\exec 文件夹。

请勿将安装包重命名为 Kaspersky Network Agent.msi。重命名此包可能会导致将来更新网络代理时出现安装错误。

仅可在静默模式下从 MSI 包安装网络代理，不支持从 MSI 包进行交互式安装。

要在静默模式下将网络代理安装至本地设备：

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才使用下面的命令。
2. 运行命令

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

其中"setup_parameters"是一系列参数，其各自的值用空格隔开(PROP1=PROP1VAL PROP2=PROP2VAL)。

在参数列表中，您必须包含 EULA=1。否则网络代理不会被安装。

如果您正在使用 Kaspersky Security Center 的标准连接设置和远程设备上的网络代理，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

/l*vx 是写入日志的键。该日志在网络代理安装期间创建，保存在 C:\windows\temp\nag_inst.log。

除了 nag_inst.log，应用程序还会创建 $klssinstlib.log 文件，其中包含安装日志。此文件存储在 %windir%\temp 或 %temp% 文件夹中。为了进行故障排除，您或 Kaspersky 技术支持专家可能同时需要两个日志文件 - nag_inst.log 和 $klssinstlib.log。

如果您需要另外指定用于连接到管理服务器的端口，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

参数 SERVERPORT 对应于连接到管理服务器的端口号。

网络代理安装参数区域中列出了在静默模式下安装网络代理时可用到的参数名称和可能的值。

如果要使用 Windows 安装程序升级网络代理，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

以静默模式安装 Linux 网络代理（使用应答文件）

您可以使用应答文件（一个文本文件，其中包含一组自定义的安装参数：变量以及各自的值）安装 Linux 网络代理。使用此应答文件可以静默模式运行安装程序，即无需用户参与。

要以静默模式安装 Linux 网络代理：

1. 准备相关的 Linux 设备以进行远程安装。下载并创建远程安装包，这通过任意合适的软件包管理系统，使用网络代理的 .deb 或 .rpm 软件包来完成。

2. 如果您想在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，首先安装 insserv-compat 软件包以配置网络代理。

   如果要在使用操作系统 RED OS 7.3.4 或更高版本或 MSVSPHERE 9.2 或更高版本的设备上安装网络代理，请安装 libxcrypt-compat 包以确保网络代理正确运行。

3. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才执行下面的步骤。

4. 创建应答文件（TXT 格式）。将变量列表以 VARIABLE_NAME=variable_value 的格式添加到应答文件，每个变量一行。

   为了正确使用应答文件，必须在其中包含至少三个必需变量：

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

您还可以添加任意可选变量以使用更具体的远程安装参数。下表列出了可以包含在应答文件中的所有变量：

用作以静默模式安装 Linux 网络代理的参数的应答文件变量

用作以静默模式安装 Linux 网络代理的参数的应答文件变量

变量名称	是否必需	描述	可能值
KLNAGENT_SERVER	是	包含显示为完全限定域名 (FQDN) 或 IP 地址的管理服务器名称。	DNS 名称或 IP 地址。
KLNAGENT_AUTOINSTALL	是	定义是否启用静默安装模式。	1—启用静默模式；安装过程中不提示用户进行任何操作。 其他—禁用静默模式；安装过程中可能提示用户进行操作。
EULA_ACCEPTED	是	定义用户是否接受网络代理的最终用户授权许可协议 (EULA)；如果缺失，则可以解释为不接受 EULA。	1 – 本人确认已完全阅读、理解并接受本《最终用户授权许可协议》的条款和条件。 其它值或未指定 – 我不接受授权许可协议的条款（将不会执行安装）
KLNAGENT_PROXY_USE	否	定义与管理服务器的连接是否将使用代理设置。默认值是 0。	1—使用代理设置。 其他—不使用代理设置。
KLNAGENT_PROXY_ADDR	否	定义用于与管理服务器连接的代理服务器的地址。	DNS 名称或 IP 地址。
KLNAGENT_PROXY_LOGIN	否	定义用于登录代理服务器的用户名。	任何现有用户名。
KLNAGENT_PROXY_PASSWORD	否	定义用于登录代理服务器的用户密码。	操作系统中的密码格式允许的任何字母数字字符集。
KLNAGENT_VM_VDI	否	定义是否在用于创建动态虚拟机的映像上安装网络代理。	1—在以后用于创建动态虚拟机的映像上安装网络代理。 其他—安装期间不使用任何映像。
KLNAGENT_VM_OPTIMIZE	否	定义网络代理设置是否对虚拟机监控程序优化。	1—修改网络代理的默认本地设置，以便优化在虚拟机监控程序上的使用。
KLNAGENT_TAGS	否	列出分配给网络代理实例的标签。	一个或多个标签名称，以分号分隔。
KLNAGENT_UDP_PORT	否	定义网络代理使用的 UDP 端口。默认值是 15000。	任意现有端口号。
KLNAGENT_PORT	否	定义网络代理使用的非 TLS 端口。默认值是 14000。	任意现有端口号。
KLNAGENT_SSLPORT	否	定义网络代理使用的非 TLS 端口。默认值是 13000。	任意现有端口号。
KLNAGENT_USESSL	否	定义是否使用传输层安全性 (TLS) 进行连接。	1（默认）—使用 TLS。 其他—不使用 TLS。
KLNAGENT_GW_MODE	否	定义是否使用连接网关。	1（默认）—不修改当前设置（第一次呼叫时，不指定任何连接网关）。 2—不使用连接网关。 3—使用连接网关。需要 KLNAGENT_GW_ADDRESS。 4—网络代理实例用作非管制区域 (DMZ) 中的连接网关。需要服务器证书。

KLNAGENT_GW_ADDRESS	否	定义连接网关的地址。仅当 KLNAGENT_GW_MODE=3 时，该值才适用。	DNS 名称或 IP 地址。
KLNAGENT_DEVICEOWNER_REGISTRATION_START	否	允许在网络代理安装后作为设备所有者实用程序运行用户注册。如果关闭，则用户无法注册为设备所有者。	1 – 用户注册为设备所有者实用程序将在网络代理安装后运行。 其他–已关闭。

5. 运行网络代理安装程序。环境变量 KLAUTOANSWERS 指定应答文件的路径，该变量会被传递给安装命令。运行以下命令之一：

   - 要将网络代理从 RPM 包安装到 32 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件路径> yum install ./klnagent-<内部版本号>.i386.rpm`
   - 要将网络代理从 RPM 包安装到 64 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件路径> yum install ./klnagent64-<内部版本号>.x86_64.rpm`
   - 要在 Arm 架构的 64 位操作系统上从 RPM 包安装网络代理，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件路径> yum install ./klnagent64-<内部版本号>.aarch64.rpm`
   - 要将网络代理从 DEB 包安装到 32 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件路径> apt install ./klnagent_<内部版本号>_i386.deb`
   - 要将网络代理从 DEB 包安装到 64 位操作系统，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件路径> apt install ./klnagent64_<内部版本号>_amd64.deb`
   - 要在 Arm 架构的 64 位操作系统上从 DEB 包安装网络代理，请执行以下命令：
     `sudo KLAUTOANSWERS=<应答文件路径> apt install ./klnagent64_<内部版本号>_arm64.deb`

   根据操作系统配置，您还可以使用 rpm、dpkg 或 dnf 包管理器来安装网络代理。

Linux 网络代理的安装以静默模式开始；在此过程中不会提示用户进行任何操作。

准备在封闭软件环境模式下运行 Astra Linux 的设备以安装网络代理

在封闭软件环境模式下运行 Astra Linux 的设备上安装网络代理之前，您必须执行两个准备过程：下面说明中的一个和适用于任何 Linux 设备的常规准备步骤。

以拥有 root 权限的账户运行本说明中提供的命令。

要准备在封闭软件环境模式下运行 Astra Linux 的设备来安装网络代理：

1. 打开 `/etc/digsig/digsig_initramfs.conf` 文件，然后指定以下设置：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 在命令行中，运行以下命令来安装兼容包：

   ```
   apt install astra-digsig-oldkeys
   ```

3. 为应用程序密钥创建一个目录：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 将应用程序密钥/opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg放在上一步创建的目录中：

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

如果 Kaspersky Security Center 分发包不包含 kaspersky_astra_pub_key.gpg 应用程序密钥，您可以通过单击以下链接下载：https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. 更新 RAM 磁盘：

   ```
   update-initramfs -u -k all
   ```

   重新启动系统。

Linux 设备已准备好安装网络代理。您可以远程、在交互模式下或在静默模式下安装网络代理。

以交互模式安装 Linux 网络代理

本文介绍了如何通过逐步指定安装参数，以交互模式在 Linux 设备上安装网络代理。或者，您可以使用应答文件（一个文本文件，其中包含一组自定义的安装参数：变量以及各自的值）。使用此应答文件可以静默模式运行安装程序，即无需用户参与。

如果要在使用操作系统 RED OS 7.3.4 或更高版本或 MSVSPHERE 9.2 或更高版本的设备上安装网络代理，请安装 libxcrypt-compat 包以确保网络代理正确运行。

在交互模式下安装网络代理：

1. 运行网络代理安装程序。根据您的 Linux 发行版，运行以下命令之一：

   - 要将网络代理从 RPM 包安装到 32 位操作系统：

     ```
     # yum -i klnagent-< 内部版本号 >.i386.rpm
     ```

   - 要将网络代理从 RPM 包安装到 64 位操作系统：

     ```
     # yum -i klnagent64-< 内部版本号 >.x86_64.rpm
     ```

   - 要在 Arm 架构的 64 位操作系统上从 RPM 包安装网络代理：

     ```
     # yum -i klnagent64-< 内部版本号 >.aarch64.rpm
     ```

   - 要将网络代理从 DEB 包安装到 32 位操作系统：

     ```
     # apt install ./klnagent_< 内部版本号 >_i386.deb
     ```

   - 要将网络代理从 DEB 包安装到 64 位操作系统：

     ```
     # apt install ./klnagent64_< 内部版本号 >_amd64.deb
     ```

   - 要在 Arm 架构的 64 位操作系统上从 DEB 包安装网络代理：

     ```
     # apt install ./klnagent64_< 内部版本号 >_arm64.deb
     ```

2. 运行网络代理配置：

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. 阅读最终用户授权许可协议 (EULA)。文本显示在命令行窗口中。按空格键查看下一个文本段。然后，在出现提示时，输入以下值：

   - 如果您理解并接受 EULA 的条款，请输入“y”。
   - 如果您不接受 EULA 的条款，请输入“n”。要使用网络代理，您必须接受 EULA 的条款。
   - 输入 r 以再次显示 EULA。

4. 输入管理服务器的 DNS 名称或 IP 地址。
5. 输入管理服务器端口号。默认情况下使用端口 14000。
6. 输入管理服务器 SSL 端口号。默认情况下使用端口 13000。
7. 如果您想对网络代理和管理服务器之间的流量使用 SSL 加密，请输入 y。否则，输入 n。
8. 选择以下选项之一来配置网络代理：

   - [1] – 不配置连接网关。
     您的设备将不会充当连接网关，也不会通过连接网关连接到管理服务器。
   - [2] – 不使用连接网关。
     您的设备将不会通过连接网关连接到管理服务器。
   - [3] – 使用连接网关连接到服务器。
     您的设备将通过连接网关连接到管理服务器。
   - [4] – 用作连接网关。
     您的设备将充当连接网关。

网络代理安装在 Linux 设备上。

应用程序管理插件的本地安装

要安装应用程序管理插件：

在按照了管理控制台的设备上，运行可执行文件 klcfginst.exe。该文件包含于应用程序分发包中。

klcfginst.exe 包含在可通过 Kaspersky Security Center 管理的所有应用程序里。向导可方便进行安装，并且无需手动配置设置。

以静默模式安装应用程序

要以静默模式安装应用程序：

1. 打开 Kaspersky Security Center 的主应用程序窗口。
2. 在控制台树的“**远程安装**”文件夹中的“**安装包**”子文件夹中，选择相关应用程序的安装包，或者为该应用程序创建新安装包。

   安装包将存储于管理服务器的共享文件夹下的“安装包服务”文件夹中。每个安装包都对应一个独立的子文件夹。

3. 以下列方式之一打开所需安装包的存储文件夹：
   - 通过将相关安装包对应的文件夹从管理服务器复制到客户端设备。然后在客户端设备上打开复制的文件夹。
   - 通过从客户端设备打开对应于管理服务器预安装包的共享文件夹。

   如果共享文件位于安装了 Microsoft Windows Vista 的设备上，请为“**用户账户控制：以管理员批准模式运行所有管理员**”设置选择值“**已禁用**”（“**开始**”→“**控制面板**”→“**管理**”→“**本地安全策略**”→“**安全设置**”）。

4. 部署选择的程序，执行下面的操作：
   - 对于 Kaspersky Anti-Virus for Windows Workstations、Kaspersky Anti-Virus for Windows Servers 和 Kaspersky Security Center，打开 exec 子文件夹并用 /s 键值运行可执行文件（带 .exe 扩展名的文件）。
   - 对于其他 Kaspersky 应用程序，请在打开的文件夹中，以 /s 键值运行可执行文件（带 .exe 扩展名的文件）。

   以 `EULA=1` 和 `PRIVACYPOLICY=1` 参数运行可执行文件表示您已完全阅读、理解并接受最终用户授权许可协议和隐私策略的条款。您也知道并同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家）。授权许可协议和隐私策略的文本包含在 Kaspersky Security Center 分发包中。必须接受授权许可协议和隐私策略的条款才能安装程序或升级上一版本程序。

使用独立包安装应用程序

Kaspersky Security Center 允许您为应用程序创建独立安装包。独立安装包是一个位于 Web 服务器上的可执行文件。它可由电子邮件发送，也可以其他方式传送到客户端设备。收到的文件可以在本地客户端设备上运行，并且安装程序不涉及 Kaspersky Security Center。

单机版 Linux 网络代理具有来自 nmap 实用程序的可选依赖项。如果 nmap 实用程序缺失或早于版本 6.0，则 Broadcast DHCP Discover 功能不受支持。

要使用独立安装包安装应用程序：

1. 连接至必要的管理服务器。
2. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
3. 在工作区中，选择所需应用程序的安装包。
4. 使用下列方式之一，启动独立安装包的创建过程：
   - 在安装包的上下文菜单中，选择“**创建独立安装包**”。
   - 通过在安装包的工作区中单击“**创建独立安装包**”链接。

   独立安装包创建向导启动。遵照向导的说明操作。
   在向导的最后一步，选择一种方法将独立安装包传输至客户端设备。
5. 将独立安装包传输至客户端设备。
6. 在客户端设备上运行独立安装包。

这样，应用程序将以独立包所指定的设置，安装在客户端设备上。

当您创建独立安装包时，它会自动发布在 Web 服务器上。已创建的独立安装包列表中会显示用于下载独立包的链接。您可以取消发布选中的独立包，也可以重新在 Web 服务器上发布。默认情况下，使用端口 8060 下载独立安装包。

网络代理安装包设置

要配置网络代理安装包：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
   默认情况下，“**远程安装**”文件夹是“**高级**”文件夹的子文件夹。
2. 在网络代理安装包的上下文菜单中，选择“**属性**”。

“网络代理安装包属性”窗口将开启。

常规

“**常规**”区域显示有关安装包的常规信息：

- 安装包名称
- 为其创建该安装包的应用程序的名称和版本
- 安装包大小
- 安装包创建日期
- 安装包文件夹的路径

设置

本区域显示为确保网络代理在安装后就能正确工作所需的设置。该区域的设置仅在运行 Windows 的设备上可用。

在“**目标文件夹**”设置组，您可以选择要安装网络代理的客户端设备。

- **安装到默认文件夹**

  如果选择该选项，网络代理将安装在 <驱动器>:\Program Files\Kaspersky Lab\NetworkAgent 文件夹中。如果该文件夹不存在，系统会自动创建。

  默认情况下已选定该选项。

- **安装到指定文件夹**

  如果选择该选项，则网络代理将安装到输入字段中指定的文件夹中。

在以下设置组中，您可以设置网络代理远程卸载任务的密码：

- **使用卸载密码**

  如果启用此选项，通过单击“**修改**”按钮，可以输入卸载密码（仅适用于运行 Windows 操作系统的设备上的网络代理）。

  默认情况下已禁用该选项。

- **状态**

  密码状态：**密码已设置**或**密码未设置**。

  默认情况下，该密码未指定。

- **保护网络代理服务免遭非授权的卸载或终止，并防止设置更改**

  当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

  启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

  默认情况下已禁用该选项。

- **对未定义状态的组件自动安装可应用更新和补丁**

  如果启用此选项，将自动安装为管理服务器、网络代理、管理控制台、iOS MDM 服务器下载的所有更新和补丁。

  如果禁用此选项，所有已下载的更新和补丁只有在状态更改为“*已批准*”后才会更新。带有*未定义*状态的更新和补丁将不被安装。

  默认情况下已启用该选项。

连接

在该区域中，您可以配置网络代理至管理服务器的连接：要建立连接，您可以使用 SSL 或 UDP 协议。要配置连接，请指定以下设置：

- **管理服务器**

  安装了管理服务器的设备地址。

- **端口**

  用于连接的端口号。

- **SSL 端口**

  用于通过 SSL 协议的连接的端口号。

- **使用服务器证书**

  如果启用此选项，网络代理访问管理服务器时的身份验证将使用证书文件，您可以通过单击“**浏览**”按钮来指定该证书文件。

  如果禁用此选项，将在网络代理第一次连接到“**服务器地址**”字段指定的地址时从管理服务器接收证书文件。

  我们建议不禁用此选项，因为网络代理在连接到管理服务器时自动接收管理服务器证书被认为是不安全的。

  默认情况下已选中该选框。

- **使用 SSL**

  如果启用此选项，则使用 SSL 协议通过安全端口连接管理服务器。

  默认情况下已禁用该选项。我们建议您不要禁用此选项，以便您的连接保持安全。

- **使用 UDP 端口**

  如果启用此选项，网络代理将通过 UDP 端口连接至管理服务器。这允许管理客户端设备并接收有关它们的信息。

  UDP 端口必须在安装网络代理的受管理设备上开放。因此，我们建议您不要禁用此选项。

  默认情况下已启用该选项。

- **UDP 端口号**

  在该字段中，可以指定使用 UDP 协议连接管理服务器到网络代理的端口。

  默认 UDP 端口 15000。

- **在 Microsoft Windows 防火墙中打开网络代理端口**

  如果启用此选项，网络代理使用的端口将被添加到 Microsoft Windows 防火墙排除列表中。
  默认情况下已启用该选项。

- **使用代理服务器**

  如果此选项被启用，请指定代理服务器参数：
  - **代理服务器地址**
  - **代理服务器端口**

  如果您的代理服务器需要身份验证，请启用**代理服务器身份验证**选项并指定与代理服务器建立连接的账户的**用户名**和**密码**。我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

为了兼容性，不建议在网络代理安装包设置中指定代理连接设置。

高级

在“**高级**”区域，您可以配置如何使用连接网关。为此目的，您可以执行以下操作：

- 使用网络代理作为非管制区域 (DMZ) 中的连接网关以连接到管理服务器，与之通信，以及 在数据传输过程中保持网络代理上的数据安全。
- 使用连接网关连接到管理服务器以减少与管理服务器的连接数。在这种情况下，请在“**连接网关地址**”字段中输入将充当连接网关的设备的地址。
- 如果您的网络包含虚拟机，请配置虚拟桌面基础架构 (VDI) 的连接。为此目的，请执行以下操作：
  - **启用 VDI 动态模式**

    如果启用此选项，将针对虚拟机上安装的网络代理启用虚拟桌面基础架构 (VDI) 的动态模式。
    默认情况下已禁用该选项。

  - **优化 VDI 设置**

    如果启用此选项，网络代理设置中将禁用以下功能：
    - 获取已安装软件的信息
    - 获取硬件信息
    - 获取检测到的漏洞信息
    - 获取需要更新的信息

    默认情况下已禁用该选项。

- **允许在安装网络代理后运行用户注册实用工具**

  如果启用此选项，用户注册为设备所有者实用程序将在网络代理安装后运行。默认情况下已禁用该选项。

附加组件

在该区域,您可以为网络代理同时安装选择附加组件。

标签

“**标签**”区域显示网络代理安装后可以被添加到客户端设备的关键字列表。您可以在列表中添加和删除标签以及重命名它们。

如果标签旁的复选框被选中，该标签在网络代理安装过程中被自动添加到受管理设备。

如果标签旁的复选框被清空，该标签在网络代理安装过程中不被自动添加到受管理设备。您可以手动添加该标签到设备。

当从列表中删除标签时，它被自动从所有添加了该标签的设备上删除。

修订历史

在该区域，您可以查看安装包修订历史。您可以比较修订、查看修订、保存修订到文件和添加/编辑修订描述。

对特别操作系统可用的网络代理安装包设置在下表中给出。

网络代理安装包设置

属性区域	Windows	Mac	Linux
常规	✓	✓	✓
设置	✓	—	—
连接	✓	✓ (“**在 Microsoft Windows 防火墙中打开网络代理端口**”和“**仅使用代理服务器自动检测**”选项除外)	✓ (“**在 Microsoft Windows 防火墙中打开网络代理端口**”和“**仅使用代理服务器自动检测**”选项除外)
高级	✓	✓	✓
附加组件	✓	✓	✓
标签	✓	✓ (自动标记规则除外)	✓ (自动标记规则除外)
修订历史	✓	✓	✓

查看隐私策略。

隐私策略在 https://www.kaspersky.com.cn/products-and-services-privacy-policy 在线提供；也可以离线查看。例如，您可以在安装网络代理前阅读隐私策略。

要离线阅读隐私策略：

1. 启动 Kaspersky Security Center 安装程序。
2. 在安装程序窗口中，转到“**提取安装包**”链接。
3. 在打开的列表中，选择“Kaspersky Security Center 网络代理”，然后单击“**下一步**”。

   privacy_policy.txt 文件将出现在设备上的指定文件夹的 NetAgent 子文件夹中。

部署移动设备管理系统

该部分描述如何使用 iOS MDM, 以及 Kaspersky Endpoint Security 协议部署移动设备管理系统。

使用 iOS MDM 协议部署管理系统

Kaspersky Security Center 允许您管理运行 iOS 的移动设备。iOS MDM 移动设备即连接至 iOS MDM 服务器并由管理服务器管理的 iOS 移动设备。

移动设备通过以下步骤连接到 iOS MDM 服务器：

1. 管理员安装 iOS MDM 服务器。
2. 管理员获取 Apple 推送通知服务 (APNs) 证书（接收 APNs 证书，https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm）。

   APNs 证书允许管理服务器连接至 APNs 服务器以发送推送通知至 iOS MDM 移动设备。
3. 管理员安装 APNs 证书到 iOS MDM 服务器。
4. 管理员为 iOS 移动设备用户创建 iOS MDM 配置文件。

   iOS MDM 配置文件包含一系列将 iOS 移动设备连接至管理服务器的设置。

当 iOS MDM 配置文件安全完成，且 iOS MDM 设备与管理服务器同步后，设备就会显示在控制台树“**移动设备管理**”文件夹下的“**移动设备**”子文件夹中。

安装 iOS MDM 服务器

要在本地设备上安装 iOS MDM 服务器：

1. 运行 setup.exe 可执行文件。

   提示您选择要安装的 Kaspersky 程序的窗口将打开。

   在程序选择窗口，点击**安装 iOS MDM 服务器**链接运行 iOS MDM 服务器安装向导。
2. 选择目标文件夹。

   默认目标文件夹为<磁盘>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS。如果此文件夹不存在，则系统会在安装过程中自动创建。您可以使用“**浏览**”按钮更改目标文件夹。

3. 在向导的“**指定连接 iOS MDM 服务器的设置**”窗口的“**连接到 iOS MDM 服务的外部端口**”字段中，指定用于将移动设备连接至 iOS MDM 服务的外部端口。

   移动设备使用外部端口 5223 与 APNs 服务器进行通信。确保在防火墙中端口 5223 被打开，连接地址范围为 17.0.0.0/8。

   Port 443 默认用于连接到 iOS MDM 服务器。如果端口443已经由另一个服务或应用程序使用,它可以被其他端口取代,例如,端口9443。

   iOS MDM 服务器使用外部端口 2197 将通知发送到 APNs 服务器。

   APNs 服务器运行在负载均衡模式。移动设备不总是连接到相同的 IP 地址接收通知。地址范围 17.0.0.0/8 是为 Apple 留的，这就是为什么建议在防火墙设置中指定整个范围为允许范围。

4. 如果您想手动为程序组件配置交互端口，请选中“**手动设置本地端口**”选项，并指定以下设置的值：

   - **连接到网络代理的端口**。在此字段中，指定用于将 iOS MDM 服务连接到网络代理的端口。默认端口号是 9799。
   - **连接到 iOS MDM 服务的本地端口**。在此字段中，指定用于将网络代理连接到 iOS MDM 服务的本地端口。默认端口号是 9899。

   > 建议您使用默认值。

5. 在向导的“**移动设备服务器外部地址**”窗口的“**移动设备服务器远程连接的网址**”字段中，指定要安装 iOS MDM 服务器的客户端设备地址。

   此地址将用于连接受管理移动设备到 iOS MDM 服务。此客户端设备必须可用于连接 iOS MDM 设备。

   您可以以以下任意方式指定客户端设备地址：

   - 设备 FQDN（例如 mdm.example.com）
   - 设备 NetBIOS 名称

   > 您无需在地址段添加 URL 格式或端口号：这些值会自动添加。

当向导完成时，iOS MDM 服务器被安装到客户端设备。iOS MDM 服务器将显示在控制台树“**移动设备管理**”文件夹中。

在静默模式安装 iOS MDM 服务器

Kaspersky Security Center 允许您在静默模式安装 iOS MDM 服务器到本地计算机，即没有安装设置的交互输入。

要在静默模式安装 iOS MDM 服务器到本地设备：

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才使用下面的命令。
2. 运行以下命令：

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <setup_parameters>"
   ```

   其中“`setup_parameters`”是一系列设置，其各自的值用空格隔开（`PROP1=PROP1VAL PROP2=PROP2VAL`）。setup.exe 文件位于服务器文件夹，它是 Kaspersky Security Center 分发包的一部分。

下表列出了在静默模式下安装 iOS MDM 服务器时可用到的参数名称和可能的值。参数可以按任何顺序指定。

参数名称	参数描述	可用值
EULA	是否接受最终用户授权许可协议条款。该参数是必须的。	• 1 – 我已完全阅读、理解并接受最终用户授权许可协议的条款。 • 其它值或没有值 – 我不接受授权许可协议的条款（将不会执行安装）。
DONT_USE_ANSWER_FILE	是否在 iOS MDM 服务器安装设置中使用 XML 文件。 XML 文件包含在安装包或存储在管理服务器。您不必指定文件的额外路径。 该参数是必须的。	• 1 – 不使用 XML 参数文件。 • 其它值，或未定义值 – 使用 XML 参数文件。
INSTALLDIR	iOS MDM 服务器安装文件夹。 该参数是可选的。	字符串值，例如 `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	连接 iOS MDM 服务到网络代理的本地端口。 默认端口号是 9799。 该参数是可选的。	数字值。
LOCALSERVERPORT	连接网络代理到 iOS MDM 服务的本地端口。 默认端口号是 9899。 该参数是可选的。	数字值。
EXTERNALSERVERPORT	连接设备到 iOS MDM 服务器的端口。 默认端口号是 443。 该参数是可选的。	数字值。
EXTERNAL_SERVER_URL	要安装 iOS MDM 服务器的客户端设备的外部地址。此地址将用于连接受管理移动设备到 iOS MDM 服务。此客户端设备必须可用于通过 iOS MDM 连接。 地址不能包含 URL 和端口号，因为这些值将被自动添加。 该参数是可选的。	• 设备 FQDN（例如 mdm.example.com） • 设备 NetBIOS 名称 • 设备 IP 地址
WORKFOLDER	iOS MDM 服务器工作文件夹。 如果未指定工作文件夹，数据将被写入默认文件夹。 该参数是可选的。	字符串值，例如 `WORKFOLDER=\"C:\work\"`
MTNCY	多个虚拟服务器使用 iOS MDM 服务器。 该参数是可选的。	• 1 – iOS MDM 服务器将被多个虚拟管理服务器使用。 • 其它值或没有值 – iOS MDM 服务器将不被多个虚拟管理服务器使用。

例如：

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

iOS MDM 服务器安装参数在 安装 iOS MDM 服务器 部分给出。

iOS MDM 服务器部署方案

要安装的 iOS MDM 服务器副本数量可以基于可用硬件或所覆盖的移动设备总数来选择。

记住，对于单一 Kaspersky Device Management for iOS 的安装所推荐的最大移动设备数量是 50,000。为了降低负载，设备轮询可以在几个安装了 iOS MDM 服务器的服务器上分发。

iOS MDM 设备的身份验证通过用户证书执行(任何安装在设备上的配置文件都包含设备所有者的证书)。因此，iOS MDM 服务器部署拥有两个部署方案：

- 简易方案
- 涉及 Kerberos constrained delegation (KCD) 的部署方案

简易部署方案

当在简易方案下部署 iOS MDM 服务器时，移动设备直接连接到 iOS MDM Web 服务。此种情况下，管理服务器发布的用户证书仅可以被应用与设备身份验证。与公共密钥基础架构(PKI)的整合对用户证书不可用。

涉及 Kerberos constrained delegation (KCD) 的部署方案

要使用具有 Kerberos 约束委派 (KCD) 的部署方案，必须满足以下要求：

- 管理服务器和 iOS MDM 服务器位于组织的内部网络上。
- 正在使用支持 KCD 的反向代理。

该部署方案包含以下：

- 与支持 KCD 的反向代理集成
- 使用 KCD 对移动设备做身份验证
- 与 PKI 整合以应用用户证书

当使用该部署方案时，您必须做以下操作：

- 在管理控制台的 iOS MDM Web 服务设置中，选中“**确保和 Kerberos Constrained Delegation 兼容**”复选框。
- 作为 iOS MDM Web 服务的证书，指定当 iOS MDM Web 服务发布在反向代理时定义的自定义证书。
- iOS 设备的用户证书必须由域中的 Certificate Authority (CA) 发布。如果域包含多个根 CAs，用户证书必须由当 iOS MDM Web 服务发布在反向代理时指定的 CA 发布。

  您可以通过以下方法确保用户证书与 CA 发布需求兼容：

  - 在新建 iOS MDM 配置文件向导和证书安装向导中指定用户证书。
  - 将管理服务器与域的 PKI 整合并在证书发布规则中定义对应的设置：

    1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**证书**”子文件夹。
    2. 在**证书**文件夹的工作区中，单击“**配置证书发布规则**”按钮以打开“**证书发布规则**”窗口。
    3. 在“**与 PKI 整合**”区域，配置与公共密钥基础架构的整合。
    4. 在“**移动证书发布**”区域，指定证书源。

以下是使用以下假定设置 Kerberos Constrained Delegation (KCD) 的例子：

- iOS MDM Web 服务正运行在端口 443。
- 具有反向代理的设备的名称是firewall.mydom.local。
- iOS MDM Web 服务设备名称是 iosmdm.mydom.local。
- iOS MDM Web 服务的外部发布名称是 iosmdm.mydom.global。

http/iosmdm.mydom.local 的服务主体名称

在域中，您必须为 iOS MDM Web 服务设备注册服务主体名称(SPN)(iosmdm.mydom.local)：

```
setspn -a http/iosmdm.mydom.local iosmdm
```

配置具有反向代理 (firewall.mydom.local) 的设备的域属性

要授权流量，将具有反向代理的设备(firewall.mydom.local) 托付给由 SPN 定义的服务 (http/iosmdm.mydom.local)。

要将具有反向代理的设备托付给由 SPN 定义的服务 (http/iosmdm.mydom.local)，管理员必须执行以下操作：

1. 在名为“活动目录用户和计算机”的 Microsoft Management Console 中，选择安装了反向代理的设备 (firewall.mydom.local)。
2. 在设备属性窗口，在**授权**选项卡，设置**信任此计算机到指定服务的授权**切换键到**使用任何身份验证协议**。
3. 添加 SPN (http/iosmdm.mydom.local) 到**该账户可以展示已授权凭证的服务**列表。

已发布 Web 服务的特殊(自定义)证书(iosmdm.mydom.global)

您必须在 FQDN iosmdm.mydom.global 上为 iOS MDM Web 服务发布特殊(自定义)证书，并在管理控制台的 iOS MDM Web 服务设置中指定它替换默认证书。

请注意证书容器(带有 p12 或 pfx 扩展名的文件)必须也包含根证书链(公共密钥)。

在反向代理上发布 iOS MDM Web 服务

在反向代理上，对于从移动设备到 iosmdm.mydom.global 端口 443 的流量，您必须在 SPN(http/iosmdm.mydom.local)上配置 KCD，使用为 FQDN(iosmdm.mydom.global)发布的证书。请注意，正发布和已发布的 Web 服务必须共享相同的服务器证书。

接收 APNs 证书

> 如果您已经有 APNs 证书，请考虑更新它而不是创建一个新的。当您将现有的 APNs 证书替换为新创建的证书时，管理服务器将失去对当前连接的 iOS 移动设备的管理能力。

当在 APNs 证书向导第一步中创建了证书签翻请求 (CSR)，其私钥存储在您设备的 RAM 中。因此，向导的所有步骤必须在应用程序的单一会话中完成。

要安装 APNs 证书，请执行以下操作：

1. 在控制台树的**移动设备管理**文件夹，选择**移动设备服务器**文件夹。
2. 在“**移动设备服务器**”文件夹的工作区中，选择 iOS MDM 服务器。
3. 在 iOS MDM 服务器的上下文菜单中，选择“**属性**”。

   这将打开 iOS MDM 服务器的“属性”窗口。

4. 在 iOS MDM 服务器的“属性”窗口中，选择“**证书**”区域。

5. 在“**证书**”区域的“**Apple 推送通知证书**”设置组中，单击“**请求新证书**”按钮。
   此时会启动接收 APNs 证书向导，并打开“**请求新证书**”窗口。

6. 创建证书签发请求文件（CSR）。要达成此举，请进行以下操作：

   a. 单击“**创建 CSR**”按钮。

   b. 在打开的“**创建 CSR**”窗口中，指定一个请求名称，公司和部门的名称、您所在的城市、区域和国家。

   c. 单击“**保存**”按钮，并制定保存您的 CSR 的文件名称。

   证书的私钥将保存在设备的存储中。

7. 使用您的 CompanyAccount 发送已创建的带符号的 CSR 文件到 Kaspersky。

   > 仅当您在 CompanyAccount 门户网站上上传了允许使用移动设备管理的密钥，您的 CSR 的签名才可用。

   在您的在线请求进程中，您将收到由 Kaspersky 签名的 CSR 文件。

8. 使用随机的 Apple ID 将签名的 CSR 文件发送至 Apple Inc. 网站。

   > 我们建议您不要使用个人 Apple ID。可创建一个专用 Apple ID 作为企业 ID。创建 Apple ID 后，将其连接至组织的邮箱，不要连接至员工邮箱。

   您的 CSR 经由 Apple Inc.处理后，您将收到 APNs 证书的公钥。保存文件至磁盘。

9. 连同生成 CSR 时创建的私钥一起，导出 APNs 证书文件，格式为 PFX。要执行此操作：

   a. 在“**请求新的 APNs 证书**”窗口中，单击“**完成 CSR**”按钮。

   b. 在**打开**窗口，选择从 Apple Inc. 的 CSR 中收到的证书公钥文件，然后单击“**打开**”按钮。
      证书导出过程将开始。

   c. 在接下来的窗口中，输入私钥密码并单击**确定**。
      该密码将被用于在 iOS MDM 服务器上的 APNs 证书安装。

   d. 在“**保存 APNs 证书**”窗口，指定 APNs 证书文件名，选择文件夹并单击“**保存**”。

证书的私钥和公钥会组合起来，APNs 证书将保存为 PFX 格式。此后，您可以安装 APNs 证书到 iOS MDM 服务器。

续费 APNs 证书

要续费 APNs 证书，请执行以下操作：

1. 在控制台树的**移动设备管理**文件夹，选择**移动设备服务器**文件夹。

2. 在“**移动设备服务器**”文件夹的工作区中，选择 iOS MDM 服务器。

3. 在 iOS MDM 服务器的上下文菜单中，选择“**属性**”。
   这将打开 iOS MDM 服务器的“属性”窗口。

4. 在 iOS MDM 服务器的“属性”窗口中，选择“**证书**”区域。

5. 在“**证书**”区域的“**Apple 推送通知证书**”设置组中，单击“**续费**”按钮。
   此时会启动 APNs 证书续费向导，并打开“**续费 APNs 证书**”窗口。

6. 创建证书签发请求文件（CSR）。要达成此举，请进行以下操作：

   a. 单击“**创建 CSR**”按钮。

   b. 在打开的“**创建 CSR**”窗口中，指定一个请求名称，公司和部门的名称、您所在的城市、区域和国家。

   c. 单击“**保存**”按钮，并制定保存您的 CSR 的文件名称。

   证书的私钥将保存在设备的存储中。

7. 使用您的 CompanyAccount 发送已创建的带符号的 CSR 文件到 Kaspersky。

   > 仅当您在 CompanyAccount 门户网站上上传了允许使用移动设备管理的密钥，您的 CSR 的签名才可用。

   在您的在线请求进程中，您将收到由 Kaspersky 签名的 CSR 文件。

8. 使用随机的 Apple ID 将签名的 CSR 文件发送至 Apple Inc. 网站。

   > 我们建议您不要使用个人 Apple ID。可创建一个专用 Apple ID 作为企业 ID。创建 Apple ID 后，将其连接至组织的邮箱，不要连接至员工邮箱。

   您的 CSR 经由 Apple Inc.处理后，您将收到 APNs 证书的公钥。保存文件至磁盘。

9. 请求证书的公共密钥。要达成此举，请进行以下操作：

   a. 转到苹果推送证书门户。要登录到门户，使用在证书初始化请求时接收到的 Apple ID。

   b. 在证书列表，选择 APSP 名称（“APSP: <number>”格式）匹配 iOS MDM 服务器使用证书的 APSP 名称的证书，然后单击“**续费**”按钮。
      APNs 证书被续费。

   c. 保存在门户上创建的证书。

10. 连同生成 CSR 时创建的私钥一起，导出 APNs 证书文件，格式为 PFX。要达成此举，请进行以下操作：

    a. 在“**续费 APNs 证书**”窗口中，单击“**完成 CSR**”按钮。

    b. 在**打开**窗口，选择从 Apple Inc. 的 CSR 中收到的证书公钥文件，单击**打开**窗口。
       将开始证书导出过程。

c. 在接下来的窗口中，输入私钥密码并单击**确定**。

该密码将被用于在 iOS MDM 服务器上的 APNs 证书安装。

d. 在打开的“**续费 APNs 证书**”窗口，指定 APNs 证书文件名，选择文件夹并单击“**保存**”。

证书的私钥和公钥会组合起来，APNs 证书将保存为 PFX 格式。

配置备用 iOS MDM 服务器证书

使用 iOS MDM 服务器功能可以颁发备用证书。该证书用于 iOS MDM 配置文件，以确保在 iOS MDM 服务器证书到期后无缝切换受管理 iOS 设备。

如果您的 iOS MDM 服务器使用 Kaspersky 颁发的默认证书，则可以在 iOS MDM 服务器证书到期之前颁发备用证书（或将您自己的自定义证书指定为备用证书）。默认情况下，iOS MDM 服务器证书到期前 60 天会自动颁发备用证书。iOS MDM 服务器证书到期后，备用 iOS MDM 服务器证书将立即成为主证书。公钥通过配置文件分发给所有受管理设备，因此您不必手动传输。

要颁发 iOS MDM 服务器备用证书或指定自定义备用证书：

1. 在控制台树的“**移动设备管理**”文件夹，选择“**移动设备服务器**”子文件夹。
2. 在移动设备服务器列表中，选择相关的 iOS MDM 服务器，然后在右侧窗格中，单击“**配置 iOS MDM 服务器**”按钮。
3. 在打开的 iOS MDM 服务器设置窗口中，选择“**证书**”区域。
4. 在设置的“**备用证书**”块中，执行以下操作之一：

- 如果您计划继续使用自签名证书（即 Kaspersky 颁发的证书）：

  a. 单击“**发布**”按钮。

  b. 在打开的“**激活日期**”窗口中，选择两个选项之一，来确定必须应用备用证书的日期：

  - 如果要在当前证书到期时应用备用证书，则选择“**当前证书过期时**”选项。
  - 如果要在当前证书过期之前应用备用证书，则选择“**在指定周期后(天)**”选项。在此选项旁边的输入字段中，指定一个期间，在该期间后备用证书必须替换当前证书。

  > 您指定的备用证书的有效期不能超过当前 iOS MDM 服务器证书的有效期。

  c. 单击“**确定**”按钮。

  备用 iOS MDM 服务器证书即被发布。

- 如果您计划使用您的证书颁发机构颁发的自定义证书：

  a. 单击“**添加**”按钮。

  b. 在打开的“文件资源管理器”窗口中，指定存储在您的设备上的 PEM、PFX 或 P12 格式的证书文件，然后单击“**打开**”按钮。

  您的自定义证书即被指定为备用 iOS MDM 服务器证书。

您已指定备用 iOS MDM 服务器证书。备用证书的详细信息显示在设置的“**备用证书**”块中（证书名称、颁发者名称、到期日期以及必须应用备用证书的日期（如果有））。

将 APNs 证书安装至 iOS MDM 服务器

收到 APNs 证书后，您必须将其安装至 iOS MDM 服务器。

要安装 APNs 证书到 iOS MDM 服务器：

1. 在控制台树的**移动设备管理**文件夹，选择**移动设备服务器**文件夹。
2. 在“**移动设备服务器**”文件夹的工作区中，选择 iOS MDM 服务器。
3. 在 iOS MDM 服务器的上下文菜单中，选择“**属性**”。
   这将打开 iOS MDM 服务器的“属性”窗口。
4. 在 iOS MDM 服务器的“属性”窗口中，选择“**证书**”区域。
5. 在“**证书**”区域的“**Apple 推送通知证书**”设置组中，单击“**安装**”按钮。
6. 选中包含 APNs 证书的 PFX 文件。
7. 输入在导出 APNs 证书时指定的私有密钥密码。

APNs 证书将安装在 iOS MDM 服务器上。证书详情将在“**证书**”区域的 iOS MDM 服务器属性窗口中显示。

配置到苹果推送通知服务的访问

要确保 iOS MDM Web 服务的正常功能和移动设备到管理员命令的响应，您需要在 iOS MDM 服务器设置中指定苹果推送通知服务证书(也叫 APNs 证书)。

与苹果推送通知（以下称为 APNs）的交互中，iOS MDM Web 服务通过端口 2197(出站) 连接到 api.push.apple.com 的外部地址。因此，iOS MDM Web 服务请求访问 17.0.0.0/8 地址范围的端口 TCP 2197。从 iOS 设备端访问到端口 TCP 5223 的 17.0.0.0/8 地址范围。

如果您要通过代理服务器从 iOS MDM Web 服务访问到 APNs，您必须在安装了 iOS MDM Web 服务的设备上执行以下操作：

1. 添加以下字符串到注册表：

   - 对于 32 位操作系统：

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<代理主机名称>"
"ApnProxyPort"="<代理端口>"
"ApnProxyLogin"="<代理登录名>"
"ApnProxyPwd"="<代理密码>"
```

   - 对于 64 位操作系统：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<代理主机名称>"
"ApnProxyPort"="<代理端口>"
"ApnProxyLogin"="<代理登录名>"
"ApnProxyPwd"="<代理密码>"
```

2. 重启 iOS MDM Web 服务。

在移动设备上发布和安装共享证书

要发布共享证书给用户:

1. 在控制台树的“**用户账户**”文件夹中，选择用户账户。
2. 在用户账户的上下文菜单中，选择“**安装证书**”。

   启动证书安装向导。遵照向导的说明操作。

当向导完成时，证书将被创建并且添加到用户的证书列表中。

用户将下载已发布的证书，以及包含 iOS MDM 配置文件的安装包。

移动设备连接到 iOS MDM 服务器后，iOS MDM 配置文件的设置将应用到用户设备。管理员将能够在连接后管理该设备。

用户连接到 iOS MDM 服务器的移动设备将显示在控制台树的“**移动设备管理**”文件夹的“**移动设备**”子文件夹中。

添加 KES 设备到受管理设备列表

要使用 Google Play™ 链接添加 KES 设备到受管理设备列表：

1. 在控制台树中，选择“**用户账户**”文件夹。

   默认情况下，“**用户账户**”文件夹是“**高级**”文件夹的子文件夹。

2. 选择您要将其移动设备添加到受管理设备列表的用户账户。

3. 右击并在用户账户的上下文菜单中，选择“**添加移动设备**”。

   启动移动设备连接向导。在向导的“**证书源**”窗口中，您必须指定创建管理服务器用以识别移动设备的共享证书的方法。您可以使用下列可用方法之一指定一个共享证书：

   - 自动创建共享证书，通过管理服务器工具，然后发送证书到设备。
   - 指定共享证书文件。

4. 在向导的“**设备类型**”窗口中，选择“**到 Google Play 的链接**”。

5. 在向导的“**用户通知方法**”窗口中，定义证书创建的移动设备用户通知设置（通过 SMS 消息、通过电子邮件或通过在向导完成时显示信息）。

6. 在向导的证书信息窗口中，单击“**完成**”按钮关闭向导。

向导结束操作后，一个链接和二维码将被发送到用户的移动设备，从而允许用户从 Google Play 下载 Kaspersky Endpoint Security。用户通过使用链接或扫描二维码转到 Google Play。此后，设备操作系统会提示用户接受 Kaspersky Endpoint Security for Android 安装。Kaspersky Endpoint Security for Android 下载并安装后，移动设备连接到管理服务器并下载共享证书。当证书安装在移动设备后，设备就会显示在控制台树“**移动设备管理**”文件夹下的“**移动设备**”子文件夹中。

如果 Kaspersky Endpoint Security for Android 先前已经被安装到移动设备，用户必须自己从管理员处接收并输入连接管理服务器的设置。定义了连接设置后，移动设备连接到管理服务器。管理员为设备发布共享证书并发送给用户带有证书下载登录名和密码的邮件消息或 SMS 消息。用户下载并安装共享证书。当证书安装在移动设备后，设备就会显示在控制台树“**移动设备管理**”文件夹下的“**移动设备**”子文件夹中。此种情况下，Kaspersky Endpoint Security for Android 不被下载和再次安装。

将 KES 设备连接至管理服务器

根据连接设备到管理服务器的方法，对 KES 设备 Kaspersky Device Management for iOS 有两个部署方案：

- 直接连接设备到管理服务器来部署的方案
- 涉及支持 Kerberos 约束委派的反向代理的部署方案

直接连接设备到管理服务器

KES 设备可以直接连接到管理服务器的端口 13292。

根据使用的身份验证方法，连接 KES 设备到管理服务器有两个选项：

- 使用用户证书连接设备
- 不用用户证书连接设备

使用用户证书连接设备

当连接带有用户证书的设备时，设备与通过管理服务器工具被分配证书的用户账户相关联。

此种情况下，双向 SSL 身份验证（双向认证）将被使用。管理服务器和设备都将使用证书认证。

不用用户证书连接设备

当连接没有用户证书的设备时，设备不与任何管理服务器上的用户账户关联。然而，当设备接收任何证书时，设备将与通过管理服务器工具被分配证书的用户相关联。

当连接设备到管理服务器时，将应用单向 SSL 身份验证，这意味着仅管理服务器使用证书进行身份验证。设备获取用户证书后，身份验证类型将变更为双向 SSL 身份验证(双向 SSL 身份验证，共有身份验证)。

连接 KES 设备到 Kerberos constrained delegation (KCD) 服务器的方案

连接 KES 设备到 Kerberos constrained delegation (KCD) 管理服务器的方案包括如下：

- 与支持 KCD 的反向代理集成。
- 将 Kerberos Constrained Delegation (KCD) 用于移动设备身份验证。
- 与公共密钥基础架构(PKI)整合以应用用户证书。

当使用该连接方案时，请注意以下几点：

- 连接 KES 设备到反向代理的类型必须是“双向 SSL 身份验证”，就是，设备必须通过先前用户证书连接到反向代理。为此，您不要整合用户证书到 Kaspersky Endpoint Security for Android 安装包。该 KES 包必须由设备指定的管理服务器创建。
- 您必须指定特定(自定义)证书，而不是移动协议的默认服务器证书：
  1. 在管理服务器的属性窗口，在**设置**区域，选择**为移动设备打开端口**复选框，然后在下拉列表中选择**添加证书**。
  2. 在打开的窗口中，指定当到移动协议的访问点被发布在管理服务器时设置在反向代理上的证书。
- KES 设备的用户证书必须由域中的 Certificate Authority (CA) 发布。记住，如果域包含多个多个根 CA，用户证书必须被该 CA 发布，这已设置在反向代理发布中。

  您可以通过以下方法确保用户证书与上述需求兼容：
  - 在新建安装包向导和证书安装向导中指定用户证书。
  - 将管理服务器与域的 PKI 整合并在证书发布规则中定义对应的设置：
    1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**证书**”子文件夹。
    2. 在**证书**文件夹的工作区中，单击“**配置证书发布规则**”按钮以打开“**证书发布规则**”窗口。
    3. 在“**与 PKI 整合**”区域，配置与公共密钥基础架构的整合。
    4. 在“**移动证书发布**”区域，指定证书源。

以下是使用以下假定设置 Kerberos Constrained Delegation (KCD) 的例子：

- 管理服务器到移动协议的访问点被设置成端口 13292。
- 具有反向代理的设备的名称是firewall.mydom.local。
- 管理服务器设备名称是 ksc.mydom.local。
- 访问点到移动协议的外部发布地址是 kes4mob.mydom.global。

管理服务器域账户

您必须创建运行管理服务器服务的域账户(例如，KSCMobileSrvcUsr)。您可以在安装管理服务器或使用 klsrvswch 实用工具时指定管理服务器服务账户。klsrvswch 实用工具位于管理服务器安装文件夹。默认安装路径：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

域账户必须由以下原因指定：

- KES 设备管理功能是管理服务器的一部分。
- 要确保 Kerberos Constrained Delegation (KCD) 的正常功能，接收端(例如，管理服务器)必须运行在域账户下。

http/kes4mob.mydom.local 的服务主体名称

在域中，在 KSCMobileSrvcUsr 账户下，添加 SPN 以在管理服务器设备的端口 13292 发布移动协议服务。对于管理服务器设备 kes4mob.mydom.local，将是如下：

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

配置具有反向代理 (firewall.mydom.local) 的设备的域属性

要授权流量，您必须将反向代理设备(tmg.mydom.local) 托付给由 SPN 定义的服务 (http/kes4mob.mydom.local:13292)。

要将具有反向代理的设备托付给由 SPN 定义的服务 (http/kes4mob.mydom.local:13292)，管理员必须执行以下操作：

1. 在名为"活动目录用户和计算机"的 Microsoft Management Console 中，选择安装了反向代理的设备 (firewall.mydom.local)。
2. 在设备属性窗口，在**授权**选项卡，设置**信任此计算机到指定服务的授权**切换键到**使用任何身份验证协议**。
3. 在**该账户可以展示已授权凭证的服务**列表，添加 SPN http/kes4mob.mydom.local:13292。

要发布的特定(自定义)证书(kes4mob.mydom.global)

要发布管理服务器移动协议，您必须发布一个 FQDN kes4mob.mydom.global 特定(自定义)证书并在管理控制台中管理服务器的移动协议设置中指定它以代替默认服务器证书。为此，在管理服务器的属性窗口，在**设置**区域，选择**为移动设备打开端口**复选框，然后在下拉列表中选择**添加证书**。

请注意服务器证书容器(带有 .p12 或 .pfx 扩展名的文件)必须也包含根证书链(公共密钥)。

配置在反向代理上发布

在反向代理上，对于从移动设备到端口 kes4mob.mydom.global 端口 13292 的流量，您必须在 SPN (http/kes4mob.mydom.local:13292) 上配置 KCD，使用为 FQND kes4mob.mydom.global 发布的证书。请注意，正发布和已发布的访问点(管理服务器端口 13292)必须共享相同的服务器证书。

使用 Firebase Cloud Messaging

为了确保及时将命令交付到 Android 操作系统管理的 KES 设备上， Kaspersky Security Center 使用推送通知机制。KES 设备和管理服务器之间通过 Firebase Cloud Messaging（以下简称 FCM）交换推送通知。在 Kaspersky Security Center 管理控制台中，可以指定 Firebase Cloud Messaging 的设置从而将 KES 设备连接到服务。

要检索 Firebase Cloud Messaging 的设置，您必须有 Google 账户。

要启用对 FCM 的使用：

1. 在管理控制台中，选择“**移动设备管理**”节点以及“**移动设备**”文件夹。
2. 在“**移动设备**”文件夹的上下文菜单中，选择**属性**。
3. 在文件夹属性中，选择“**Firebase Cloud Messaging 设置**”区域。
4. 在**Firebase 项目编号**字段中，指定 FCM 发件人 ID。
5. 在**私钥文件 (JSON 格式)**字段中，选择私钥文件。

在下次同步管理服务器时，由 Android 操作系统管理的 KES 设备将被连接到 Firebase Cloud Messaging。

通过单击“**重置设置**”按钮，您可以编辑 Firebase Cloud Messaging 的设置。

当切换到不同的 Firebase 项目时，您需要等待 10 分钟才能恢复 FCM。

FCM 服务在以下地址范围内运行：

- 从 KES 设备端，需要对以下地址的端口 443 (HTTPS)、5228 (HTTPS)、5229 (HTTPS) 和 5230 (HTTPS) 的访问：
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Google's ASN 15169 中列出的所有 IP 地址

- 从管理服务器端，需要对以下地址的端口 443 (HTTPS) 的访问：
  - fcm.googleapis.com
  - Google's ASN 15169 中列出的所有 IP 地址

如果代理服务器设置（**高级/配置互联网访问**）已在管理控制台的管理服务器属性中指定，则这些设置将用于与 GFCM 交互中。

配置 FCM：获取发件人 ID 和私钥文件

要配置 FCM：

1. 在 Google 门户注册。
2. 转到Firebase 控制台。
3. 执行以下操作之一：
   - 要创建新项目，请单击**创建项目**并按照屏幕上的说明进行操作。
   - 打开现有项目。
4. 单击齿轮图标并选择**项目设置**。
   “**项目设置**”窗口将开启。
5. 选择**Cloud Messaging**选项卡。
6. 从**Firebase Cloud Messaging API (V1)**部分中的**发件人 ID**字段检索相关的发件人 ID。
7. 选择**服务账户**选项卡，然后单击**生成新私钥**。
8. 在打开的窗口中，单击**生成密钥**以生成并下载私钥文件。

Firebase Cloud Messaging 现已配置。

与公共密钥基础架构整合

与公共密钥基础架构(PKI)整合旨在管理服务器对域用户证书的发布。

管理员可以在管理控制台中为用户分配域证书。这可以使用以下方法完成：

- 在证书安装向导中从文件中给用户分配特定（自定义）证书。
- 执行与 PKI 的整合并分配 PKI 以作为制定类型证书或所有类型证书的证书源。

通过单击“**与公钥基础架构整合**”链接，可以在“**移动设备管理**”/“**证书**”文件夹的工作区中使用与 PKI 集成的设置。

用于域用户证书发布的与 PKI 整合的常规原则

在管理控制台，单击“**与公钥基础架构整合**”链接（在“**移动设备管理**”/“**证书**”文件夹的工作区）指定一个域账户，管理服务器将使用该域账户通过域的 CA 发布域用户证书（以下称为执行与 PKI 整合的账户）。

请注意以下：

- 与 PKI 整合的设置允许您为所有类型的证书指定默认模板。请注意，证书发布规则（通过单击“**配置证书发布规则**”按钮，规则在“**移动设备管理**”/“**证书**”文件夹的工作区中可用）允许您为每种类型的证书指定各自的模板。
- 特殊 Enrollment Agent (EA) 证书必须安装在管理服务器设备，在与 PKI 整合的账户的证书存储库中。Enrollment Agent (EA) 证书由域 CA (Certificate Authority) 管理员发布。

与 PKI 整合的账户必须满足以下标准：

- 它是域用户。
- 它是发起与 PKI 的整合的管理服务器设备本地管理员。
- 它具有*作为服务登录*的权限。
- 管理服务器设备必须在此账户下运行至少一次以创建永久用户配置文件。

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server（以下简称“Web 服务器”）是 Kaspersky Security Center 的一个组件。Web 服务器用于发布独立安装包、移动设备独立安装包、iOS MDM 配置文件、以及共享文件夹的文件。

所创建的 iOS MDM 配置文件和安装包被自动发布在 Web 服务器并在第一次下载后被删除。管理员可以通过任意方式如电子邮件等将新链接发送给用户。

通过单击链接，用户可将所需信息下载至移动设备。

Web 服务器设置

如果需要 Web 服务器的 fine-tuning，管理控制台 Web 服务器属性提供为 HTTP (8060) 和 HTTPS (8061) 更改端口。除了更改端口，您可以为 HTTPS 替换服务器证书并为 HTTP 更改 Web 服务器的 FQDN。

Kaspersky Security Center 的安装

本部分描述了 Kaspersky Security Center 组件的安装。如果您只希望在一台设备上本地安装应用程序，则两种安装选项可用：

- **标准**。该选项用在您要尝试 Kaspersky Security Center 并在网络中的小区域测试其操作的时候。在标准安装期间，您仅配置数据库。您还可以仅安装 Kaspersky 应用程序的管理插件的默认集合。如果您有过使用 Kaspersky Security Center 的经验，因此您可以在标准安装后指定所有相关设置，您也可以使用标准安装。

- **自定义**。自定义安装允许您修改 Kaspersky Security Center 设置，例如共享文件夹路径、账户和连接管理服务器的端口，以及数据库设置。自定义安装允许您指定安装哪些 Kaspersky 管理插件。如果必要，您可以在静默模式启动自定义安装。

如果网络中至少已成功安装一台管理服务器，您可以通过远程安装任务使用强制安装方式将服务器安装到同一网络中的其他设备上。创建远程安装任务时，应使用管理服务器安装包：ksc_<版本号>.<内部版本号>_full_<本地化语言>.exe。

如果您要安装全功能 Kaspersky Security Center 组件，或升级当前版本到这些组件，请使用该包。

如果要部署 Kaspersky Security Center 故障转移集群，您需要在集群的所有节点上都安装 Kaspersky Security Center。

准备安装

在启动安装之前执行以下操作。

- **检查硬件和软件要求**

  请确保设备的硬件和软件满足管理服务器和管理控制台的要求。

- **选择并安装数据库管理系统 (DBMS)**

  Kaspersky Security Center 将其信息存储在由 DBMS 管理的数据库中。在 Kaspersky Security Center 之前在网络上安装 DBMS（详细了解如何选择 DBMS）。如果您决定安装 PostgreSQL 或 Postgres Pro DBMS，请为超级用户指定密码。如果未指定密码，管理服务器可能无法连接到数据库。

  建议将管理服务器安装在专用服务器上，而不是域控制器上。但是，如果在用作只读域控制器 (RODC) 的服务器上安装 Kaspersky Security Center，则不得在本地（同一设备上）安装 Microsoft SQL Server (SQL Express)。在这种情况下，如果需要在本地安装 DBMS，建议您（在另一台设备上）远程安装 Microsoft SQL Server (SQL Express)，或者使用 MySQL、MariaDB 或 PostgreSQL。

- **为管理服务器、网络代理和管理控制台准备文件夹**

  管理服务器、网络代理和管理控制台应安装在已禁用大小写敏感的文件夹中。此外，管理服务器共享文件夹和 Kaspersky Security Center 隐藏文件夹 (%ALLUSERSPROFILE%\KasperskyLab\adminkit) 也必须禁用区分大小写。

- **删除旧的网络代理**

  服务器版本的网络代理将与管理服务器一起安装在设备中。管理服务器无法与常规版本的网络代理一起安装。如果服务器版本的网络代理已经安装在设备中，请删除它，然后重新开启管理服务器的安装。网络代理的服务器版本详见安装 Kaspersky Security Center 后系统的变化。

- **检查账户**

  安装 Kaspersky Security Center 需要执行安装所在设备的管理员权限。

  Kaspersky Security Center 支持受管理服务账户和群组受管理服务账户。如果您的域中使用了这些类型的账户，并且您想指定其中一个账户作为管理服务器服务的账户，则首先将账户安装在要安装管理服务器的同一设备上。关于在本地设备上安装受管服务账户的详细信息，请参阅正式的 Microsoft 文档。

使用 DBMS 的账户

要安装和使用管理服务器，您需要一个用于运行管理服务器安装程序（以下也称为“安装程序”）的 Windows 账户、一个用于启动管理服务器服务的 Windows 账户以及一个用于访问 DBMS 的内部 DBMS 账户。您可以创建新账户或使用现有账户。所有这些账户都需要特定权限。所需账户组及其权限取决于以下标准：

- DBMS 类型：
  - Microsoft SQL Server（带有 Windows 身份验证和 SQL Server 身份验证）
  - MySQL 或 MariaDB
  - PostgreSQL 或 Postgres Pro
- DBMS 位置：
  - **本地 DBMS**。*本地 DBMS* 是与管理服务器安装在同一设备上的 DBMS。
  - **远程 DBMS**。*远程 DBMS* 是安装在其他设备上的 DBMS。
- 管理服务器数据库创建的方法：
  - **自动**。在安装管理服务器的过程中，您可以使用安装程序自动创建一个管理服务器数据库（以下简称“服务器数据库”）。
  - **手动**。您可以使用第三方应用程序（例如 SQL Server Management Studio）或脚本来创建空数据库。之后，您可以在管理服务器安装期间将此数据库指定为服务器数据库。

为账户授予权限时，请遵循最低权限原则。这意味着授予的权限应以足以执行所需操作为限。

下表包含有关在安装和启动管理服务器之前应授予账户的系统权限和 DBMS 权限的信息。

带有 Windows 身份验证的 Microsoft SQL Server

如果您选择 SQL Server 作为 DBMS，则可以使用 Windows 身份验证来访问 SQL Server。为用于运行安装程序的 Windows 账户和用于启动管理服务器服务的 Windows 账户配置系统权限。在 SQL Server 上，为这些 Windows 账户创建登录信息。根据服务器数据库的创建方法，如下表所述向这些账户授予所需的 SQL Server 权限。有关如何配置账户权限的更多信息，请参见配置用于 SQL Server 的账户（Windows 身份验证）。

DBMS：带有 Windows 身份验证的 Microsoft SQL Server（包含 Express 版本）

	自动创建数据库（由安装程序）	手动创建数据库（由管理员）
运行安装程序的账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。 • 本地 DBMS：一个本地管理员账户或域账户。	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。 • 本地 DBMS：一个本地管理员账户或域账户。

运行安装程序的账户权限	• 系统权限：本地管理员权限。
	• SQL Server 权限：
	  • 服务器级别角色：sysadmin。
		• 系统权限：本地管理员权限。
		• SQL Server 权限：
		  • 服务器级别角色：公共。
		  • 服务器数据库的数据库角色成员：db_owner，public。
		  • 服务器数据库的默认架构：dbo。

管理服务器服务账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。
	• 本地 DBMS：
	  • 一个由管理员选择的 Windows 账户。
	  • 一个由安装程序自动创建的 KL-AK-* 格式账户。
		• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。
		• 本地 DBMS：
		  • 一个由管理员选择的 Windows 账户。
		  • 一个由安装程序自动创建的 KL-AK-* 格式账户（在这种情况下，我们不建议生成 KL-AK-* 账户）。

管理服务器服务账户权限	• 系统权限：安装程序分配的所需权限。
	• SQL Server 权限：安装程序分配的所需权限。
		• 系统权限：安装程序分配的所需权限。
		• SQL Server 权限：
		  • 服务器级别角色：公共。
		  • 服务器数据库的数据库角色成员：db_owner，public。
		  • 服务器数据库的默认架构：dbo。

带有 SQL Server 身份验证的 Microsoft SQL Server

如果您选择 SQL Server 作为 DBMS，则可以使用 SQL Server 身份验证来访问 SQL Server。为用于运行安装程序的 Windows 账户和用于启动管理服务器服务的 Windows 账户配置系统权限。在 SQL Server 上，创建一个带密码的登录名以用于身份验证。然后向该 SQL Server 账户授予下表中列出的所需权限。有关如何配置账户权限的更多信息，请参见配置用于 SQL Server 的账户（SQL Server 身份验证）。

DBMS：带有 SQL Server 身份验证的 Microsoft SQL Server（包含 Express 版本）

	自动创建数据库（由安装程序）	手动创建数据库（由管理员）
运行安装程序的账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。 • 本地 DBMS：一个本地管理员账户或域账户。	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。 • 本地 DBMS：一个本地管理员账户或域账户。
运行安装程序的账户权限	系统权限：本地管理员权限。	系统权限：本地管理员权限。

管理服务器服务账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。
	• 本地 DBMS：
	  • 一个由管理员选择的 Windows 账户。
	  • 一个由安装程序自动创建的 KL-AK-* 格式账户。
		• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。
		• 本地 DBMS：
		  • 由管理员选择的 Windows 用户账户。
		  • 一个由安装程序自动创建的 KL-AK-* 格式账户。

管理服务器服务账户权限	系统权限：安装程序分配的所需权限。	系统权限：安装程序分配的所需权限。

	自动创建数据库（由安装程序）	手动创建数据库（由管理员）

用于 SQL Server 身份验证的登录权限	创建数据库和安装管理服务器所需的 SQL Server 权限：
	• 服务器级别角色：公共。
	• *主*数据库的数据库角色成员：db_owner。
	• *主*数据库的默认架构：dbo。
	• 权限：
	  • CONNECT ANY DATABASE
	  • CONNECT SQL
	  • CREATE ANY DATABASE
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE（如果启用了**Always On**选项）
	使用管理服务器所需的 SQL Server 权限：
	• 服务器级别角色：公共。
	• 服务器数据库的数据库角色成员身份：db_owner。
	• 服务器数据库的默认架构：dbo。
	• 权限：
	  • CONNECT SQL
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE（如果启用了**Always On**选项）
	  • VIEW ANY DEFINITION
		SQL Server 权限：
		• 服务器级别角色：公共。
		• 服务器数据库的数据库角色成员身份：db_owner。
		• 服务器数据库的默认架构：dbo。
		• 权限：
		  • CONNECT SQL
		  • VIEW ANY DATABASE
		  • VIEW ANY DEFINITION

为管理服务器数据恢复配置 SQL Server 权限

要从备份中恢复管理服务器数据，请在用于安装管理服务器的 Windows 账户下运行 klbackup 实用程序。在启动 klbackup 实用程序之前，请在授予与此 Windows 账户关联的 SQL Server 登录权限。SQL Server 权限因管理服务器版本而异。对于 14.2 或更高版本的管理服务器，您可以授予 sysadmin 服务器级角色或 dbcreator 服务器级角色。

用于管理服务器数据库恢复的 SQL Server 权限

14.2 或更高版本的管理服务器	其他管理服务器版本

• SQL Server 权限：
  • 服务器级别角色：dbcreator。
• 权限：
  • VIEW ANY DEFINITION
在启动 klbackup 实用程序之前，请指定 KLSRV_SKIP_ADJUSTING_DBMS_ACCESS 服务器标志。使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。此后，在命令行中执行以下命令：
`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL 和 MariaDB

如果您选择 MySQL 或 MariaDB 作为 DBMS，请创建一个 DBMS 内部账户并为此账户授予下表中列出的所需权限。安装程序和管理服务器服务使用此内部 DBMS 账户访问 DBMS。请注意，数据库创建方法不影响所需权限集。有关如何配置账户权限的更多信息，请参阅配置用于 MySQL 和 MariaDB 的账户。

DBMS：MySQL 和 MariaDB

	自动或手动创建数据库
运行安装程序的账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。 • 本地 DBMS：一个本地管理员账户或域账户。
运行安装程序的账户权限	系统权限：本地管理员权限。

管理服务器服务账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。
	• 本地 DBMS：
	  • 一个由管理员选择的 Windows 账户。
	  • 一个由安装程序自动创建的 KL-AK-* 格式账户。

管理服务器服务账户权限	系统权限：安装程序分配的所需权限。
DBMS 内部账户权限	架构权限： • 管理服务器数据库：ALL（不包括 GRANT OPTION）。 • 系统方案（mysql 和 sys）：SELECT、SHOW VIEW。 • sys.table_exists 存储过程：EXECUTE（如果您使用 MariaDB 10.5 或更早版本作为 DBMS，则无需授予 EXECUTE 权限）。 所有方案的全局权限：PROCESS、SUPER。

有关如何将数据从共享表空间移动到每表一个文件表空间的详细信息，请参阅在 MySQL 和 MariaDB DBMS 中将数据从共享表空间移动到每表一个文件表空间。

配置管理服务器数据恢复的权限

您授予内部 DBMS 账户的权限足以从备份中恢复管理服务器数据。要开始恢复，请在用于安装管理服务器的 Windows 账户下运行 klbackup 实用程序。

PostgreSQL 或 Postgres Pro

如果您选择 PostgreSQL 或 Postgres Pro 作为 DBMS，您可以使用 *Postgres* 用户（默认的 Postgres 角色）或创建一个新的 Postgres 角色（以下简称"角色"）来访问 DBMS。根据服务器数据库的创建方法，如下表所述向角色授予所需权限。有关如何配置角色权限的更多信息，请参阅配置用于 PostgreSQL 或 Postgres Pro 的账户。

DBMS：PostgreSQL 或 Postgres Pro

	自动创建数据库		手动创建数据库
运行安装程序的账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。 • 本地 DBMS：一个本地管理员账户或域账户。		• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。 • 本地 DBMS：一个本地管理员账户或域账户。
运行安装程序的账户权限	系统权限：本地管理员权限。		系统权限：本地管理员权限。

管理服务器服务账户	• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。
	• 本地 DBMS：
	  • 一个由管理员选择的 Windows 账户。
	  • 一个由安装程序自动创建的 KL-AK-* 格式账户。
			• 远程 DBMS：仅限一个安装 DBMS 的远程设备的域账户。
			• 本地 DBMS：
			  • 一个由管理员选择的 Windows 账户。
			  • 一个由安装程序自动创建的 KL-AK-* 格式账户。

管理服务器服务账户权限	系统权限：安装程序分配的所需权限。		系统权限：安装程序分配的所需权限。
Postgres 角色的权限	*Postgres* 用户不需要额外权限。	新角色的权限： `CREATEDB`。	对于新角色： • 针对管理服务器数据库的权限：`ALL`。 • 针对公共架构中所有表的权限：`ALL`。 • 针对公共架构中所有序列的权限：`ALL`。

配置管理服务器数据恢复的权限

要从备份中恢复管理服务器数据，请在用于安装管理服务器的 Windows 账户下运行 klbackup 实用程序。请注意，用于访问 DBMS 的 Postgres 角色必须具有针对管理服务器数据库的所有者权限。

配置 SQL Server 的使用账户（Windows 身份验证）

先决条件

在为账户分配权限之前，请执行以下操作：

1. 确保您以本地管理员账户登录系统。
2. 安装 SQL Server 的使用环境。
3. 确保您有一个安装管理服务器的 Windows 账户。
4. 确保您有一个启动管理服务器服务的 Windows 账户。
5. 在 SQL Server 上，为用于运行管理服务器安装程序（以下也简称为“安装程序”）的 Windows 账户创建一个登录名。另外，为用于启动管理服务器服务的 Windows 账户创建一个登录名。

如果您使用 SQL Server Management Studio，请在登录属性窗口的“**常规**”页面选择“**Windows 身份验证**”选项。

> 如果您想要在位于不同 Windows 域中的设备上安装管理服务器和 SQL 服务器，请注意这些域必须具有双向信任关系以确保管理服务器正确运行，包括运行任务和应用策略。有关与各种 DBMS 使用的所需账户和账户权限的信息，请参见使用 DBMS 的账户。

配置账户以安装管理服务器（自动创建管理服务器数据库）

要配置用于安装管理服务器的账户：

1. 在 SQL Server 上，将 sysadmin 服务器级别角色分配给用于运行安装程序的 Windows 账户的登录名。
2. 以用于运行安装程序的 Windows 账户登录系统。
3. 运行管理服务器安装程序。
   管理服务器设置向导启动。遵照向导的说明操作。
4. 选择“管理服务器自定义安装”选项。
5. 选择“Microsoft SQL Server 作为 DBMS”来存储管理服务器数据库。
6. 选择“Microsoft Windows 身份验证模式”，通过 Windows 账户在管理服务器和 SQL Server 之间建立连接。
7. 指定用于启动管理服务器服务的 Windows 账户。
   您可以选择之前为其创建了 SQL Server 登录名的 Windows 用户账户。或者，您可以使用安装程序自动创建 KL-AK-* 格式的新 Windows 账户。在这种情况下，安装程序会自动为此账户创建一个 SQL Server 登录名。无论选择何种账户，安装程序都会将所需的系统权限和 SQL Server 权限分配给管理服务器服务账户。

安装完成后，将创建服务器数据库并向管理服务器服务账户分配所有所需的系统权限和 SQL Server 权限。管理服务器进入就绪状态。

配置账户以安装管理服务器（手动创建管理服务器数据库）

要配置用于安装管理服务器的账户：

1. 在 SQL Server 上创建一个空数据库。此数据库将用作管理服务器数据库（以下也简称为“服务器数据库”）。
2. 对于为 Windows 账户创建的两个 SQL Server 登录名，指定公共服务器级别角色，然后配置到所创建数据库的映射：
   - 服务器级别角色：公共
   - 数据库角色成员：db_owner、public
   - 默认方案：dbo
3. 以用于运行安装程序的 Windows 账户登录系统。
4. 运行管理服务器安装程序。
   管理服务器设置向导启动。遵照向导的说明操作。
5. 选择“管理服务器自定义安装”选项。
6. 选择“Microsoft SQL Server 作为 DBMS”来存储管理服务器数据库。
7. 将所创建数据库的名称指定为管理服务器数据库名称。
8. 选择“Microsoft Windows 身份验证模式”，通过 Windows 账户在管理服务器和 SQL Server 之间建立连接。
9. 指定用于启动管理服务器服务的 Windows 账户。
   您可以选择之前为其创建了 SQL Server 登录名并配置登录权限的 Windows 用户账户。

不建议您自动创建 KL-AK-* 格式的新 Windows 账户。在这种情况下，安装程序会创建一个您尚未为其创建和配置 SQL Server 账户的新 Windows 账户。管理服务器将无法使用此账户来启动管理服务器服务。如果需要创建 KL-AK-* Windows 账户，安装后请勿启动管理控制台。改为执行以下操作：

1. 停止 kladminserver 服务。
2. 在 SQL Server 上，为创建的 KL-AK-* Windows 账户创建一个 SQL Server 登录名。
3. 向此 SQL Server 登录名授予权限并配置到所创建数据库的映射：
   - 服务器级别角色：公共
   - 数据库角色成员：db_owner、public
   - 默认方案：dbo
4. 重新启动 kladminserver 服务，然后运行管理控制台。

安装完成后，管理服务器将使用所创建数据库来存储服务器数据。管理服务器进入就绪状态。

配置 SQL Server 的使用账户（SQL Server 身份验证）

先决条件

在为账户分配权限之前，请执行以下操作：

1. 确保您以本地管理员账户登录系统。
2. 安装 SQL Server 的使用环境。
3. 确保您有一个安装管理服务器的 Windows 账户。
4. 确保您有一个启动管理服务器服务的 Windows 账户。
5. 在 SQL Server 上，启用 SQL Server 身份验证模式。

   如果您使用的是 SQL Server Management Studio，在 SQL Server 属性窗口的“**安全**”页面，选择“**SQL Server 和 Windows 身份验证模式**”选项。
6. 在 SQL Server 上，创建一个带密码的登录名。管理服务器安装程序（以下也简称为“安装程序”）和管理服务器服务将使用此 SQL Server 账户访问 SQL Server。

   如果您使用的是 SQL Server Management Studio，在登录属性窗口的“**常规**”页面，选择“**SQL Server 身份验证**”选项。

如果您想要在位于不同 Windows 域中的设备上安装管理服务器和 SQL 服务器，请注意这些域必须具有双向信任关系以确保管理服务器正确运行，包括运行任务和应用策略。有关与各种 DBMS 使用的所需账户和账户权限的信息，请参见使用 DBMS 的账户。

配置账户以安装管理服务器（自动创建管理服务器数据库）

要配置用于安装管理服务器的账户：

1. 在 SQL Server 上，将 SQL Server 账户映射到默认 *主* 数据库。*主* 数据库是管理服务器数据库（以下也简称为“服务器数据库”）的模板。在安装程序创建服务器数据库之前，*主* 数据库用于映射。向 SQL Server 账户授予以下权限：
   - 服务器级别角色：公共
   - *主* 数据库的数据库角色成员：db_owner
   - *主* 数据库的默认方案：dbo
   - 权限：
     - CONNECT ANY DATABASE
     - CONNECT SQL

- CREATE ANY DATABASE
- VIEW ANY DATABASE

2. 以用于运行安装程序的 Windows 账户登录系统。
3. 运行安装程序。
   管理服务器设置向导启动。遵照向导的说明操作。
4. 选择“管理服务器自定义安装”选项。
5. 选择“Microsoft SQL Server 作为 DBMS”来存储管理服务器数据库。
6. 指定管理服务器数据库名称。
7. 选择“SQL Server 身份验证模式”，通过创建的 SQL Server 账户在管理服务器和 SQL Server 之间建立连接。然后指定 SQL Server 账户凭证。
8. 指定用于启动管理服务器服务的 Windows 账户。
   您可以选择现有的 Windows 用户账户或使用安装程序创建 KL-AK-* 格式的新 Windows 账户。无论选择何种账户，安装程序都会将所需的系统权限分配给管理服务器服务账户。

安装完成后，将创建服务器数据库并向管理服务器服务账户分配所有所需的系统权限。管理服务器进入就绪状态。

您可以取消到*主*数据库的映射，因为安装程序已创建了一个服务器数据库，并在管理服务器安装期间配置了到该数据库的映射。

由于自动创建数据库需要比正常使用管理服务器更多的权限，因此您可以撤销一些权限。在 SQL Server 上，选择 SQL Server 账户，然后为使用管理服务器授予以下权限：

- 服务器级别角色：公共
- 服务器数据库的数据库角色成员：db_owner
- 服务器数据库的默认方案：dbo
- 权限：
  - CONNECT SQL
  - VIEW ANY DATABASE

配置账户以安装管理服务器（手动创建管理服务器数据库）

要配置用于安装管理服务器的账户：

1. 在 SQL Server 上创建一个空数据库。此数据库将用作管理服务器数据库。
2. 在 SQL Server 上，向 SQL Server 账户授予以下权限：
   - 服务器级别角色：公共。
   - 所创建数据库的数据库角色成员：db_owner。

- 所创建数据库的默认方案：dbo。
- 权限：
  - CONNECT SQL
  - VIEW ANY DATABASE

3. 以用于运行安装程序的 Windows 账户登录系统。
4. 运行安装程序。

   管理服务器设置向导启动。遵照向导的说明操作。
5. 选择“管理服务器自定义安装”选项。
6. 选择“Microsoft SQL Server 作为 DBMS”来存储管理服务器数据库。
7. 将所创建数据库的名称指定为管理服务器数据库名称。
8. 选择“SQL Server 身份验证模式”，通过创建的 SQL Server 账户在管理服务器和 SQL Server 之间建立连接。然后指定 SQL Server 账户凭证。
9. 指定用于启动管理服务器服务的 Windows 账户。

   您可以选择现有的 Windows 用户账户或使用安装程序创建 KL-AK-* 格式的新 Windows 账户。无论选择何种账户，安装程序都会将所需的系统权限分配给管理服务器服务账户。

安装完成后，管理服务器将使用所创建数据库来存储管理服务器数据。向管理服务器服务账户分配所有所需的系统权限。管理服务器进入就绪状态。

配置 MySQL 和 MariaDB 的使用账户

先决条件

在为账户分配权限之前，请执行以下操作：

1. 确保您以本地管理员账户登录系统。
2. 安装 MySQL 或 MariaDB 的使用环境。
3. 确保您有一个安装管理服务器的 Windows 账户。
4. 确保您有一个启动管理服务器服务的 Windows 账户。

配置安装管理服务器的账户

要配置用于安装管理服务器的账户：

1. 在安装 DBMS 时创建的根账户下运行 MySQL 或 MariaDB 的使用环境。

2. 创建一个带密码的内部 DBMS 账户。管理服务器安装程序（以下也简称为“安装程序”）和管理服务器服务将使用此内部 DBMS 账户访问 DBMS。向此账户授予以下权限：

   - 架构权限：
     - 管理服务器数据库：ALL（不包括 `GRANT OPTION`）
     - 系统方案（mysql 和 sys）：`SELECT`，`SHOW VIEW`
     - sys.table_exists 存储过程：`EXECUTE`
   - 所有方案的全局权限：`PROCESS`、`SUPER`。

   要创建内部 DBMS 账户并向此账户授予所需的权限，请运行以下脚本（此脚本中的 DBMS 登录名是 *KSCAdmin*，管理服务器数据库名称是 *kav*）：

   ```
   /* Create a user named KSCAdmin */
   CREATE USER 'KSCAdmin'
   /* Specify a password for KSCAdmin */
   IDENTIFIED BY '< 密码 >';
   ```

   如果您使用 MySQL 8.0 或更早版本作为 DBMS，请注意这些版本不支持“缓存 SHA2 密码”身份验证。将默认身份验证从“缓存 SHA2 密码”更改为“MySQL 本机密码”：

   - 要创建使用“MySQL本机密码”身份认证的 DBMS 账户，执行以下命令：

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '< 密码 >';
     ```

   - 要更改现有 DBMS 账户的身份验证，执行以下命令：

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '< 密码 >';
     ```

   ```
   /* Grant privileges to KSCAdmin */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   GRANT SUPER ON *.* TO 'KSCAdmin';
   ```

   > 如果您使用 MariaDB 10.5 或更早版本作为 DBMS，则无需授予 EXECUTE 权限。在这种情况下，从脚本中排除以下命令：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`。

3. 要查看向 DBMS 账户授予的权限的列表，请运行以下脚本：

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. 要手动创建管理服务器数据库，请运行以下脚本（此脚本中的管理服务器数据库名称是 *kav*）：

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   使用您在创建 DBMS 账户的脚本中指定的相同数据库名称。

5. 以用于运行安装程序的 Windows 账户登录系统。

6. 运行安装程序。

   管理服务器设置向导启动。遵照向导的说明操作。

7. 选择“管理服务器自定义安装”选项。

8. 选择“MySQL 或 MariaDB 作为 DBMS”来存储管理服务器数据库。

9. 指定管理服务器数据库名称。使用您在脚本中指定的相同数据库名称。

10. 指定您通过脚本创建的 DBMS 账户的凭证。

11. 指定用于启动管理服务器服务的 Windows 账户。

    您可以选择现有的 Windows 用户账户或使用安装程序自动创建 KL-AK-* 格式的新 Windows 账户。无论选择何种账户，安装程序都会将所需的系统权限分配给管理服务器服务账户。

安装完成后，将创建管理服务器数据库，管理服务器进入就绪状态。

在 MySQL 或 MariaDB DBMS 中将数据从共享表空间移动到每个表一个文件的表空间

对于 MySQL 和 MariaDB DBMS，您可以通过以下方式存储数据：

- 作为共享表空间，当所有用户数据库的数据存储在单个文件中（通常在`ibdata1`文件中）时。
- 作为每个表一个文件的表空间，为每个表创建一个单独的数据空间作为单独的文件。

使用共享表空间会增加表空间碎片的风险。由于无法执行`SHRINK`操作，共享表空间中的文件可能会占用大约 90% 的磁盘空间。这会对磁盘子系统的性能产生负面影响。因此，选择每个表一个文件的表空间很有用。

本文介绍如何将数据从共享表空间移动到每个表一个文件的表空间。如果其他应用程序也使用 MySQL 或 MariaDB DBMS，则必须将这些应用程序的数据库移动到每个表独享文件的表空间。

> 我们建议您仅在使用管理服务器的 MySQL 或 MariaDB DBMS 时才执行该过程。
> 将数据从共享表空间移动到每个表一个文件的表空间可能会增加磁盘子系统的负载。

先决条件

在开始之前，请确保：

- 您通过运行数据备份任务或klbackup 实用程序创建了管理服务器数据的备份副本。
- 您创建了其他应用程序的备份副本，这些应用程序的数据库由 MySQL 或 MariaDB DBMS（如有）管理。
- 在安装了 DBMS 的设备上，在带有数据库的分区中，有一个可用磁盘空间。

所需磁盘空间是当前数据库总大小（`ibdata1`文件的当前大小）的 150%。

过程

要将数据从共享表空间移动到每个表一个文件的表空间：

1. 停止 Kaspersky Security Center 管理服务器服务和其他使用您要为其执行此过程的 DBMS 实例的应用程序。
2. 根据 DBMS 版本，以超级用户身份登录到您的 DBMS，然后在任何方便的应用程序中运行 `fix_tablespace.sql` 脚本。

   您可以单击这些链接查看 `fix_tablespace.sql` 脚本：

   查看适用于 MySQL 5.7 和 MariaDB 10.1+ 的脚本

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

   查看适用于 MySQL 8.0+ 的脚本

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
```

```
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

您不得停止脚本执行。
如果没有发生 DBMS 错误，但您终止了脚本执行，请再次运行脚本，或者停止执行此过程的步骤，重新启动 DBMS 服务，然后从备份中恢复管理服务器数据。

3. 在 my.cnf 文件的`[mysqld]`部分中，将`innodb_file_per_table`参数设置为`1`。
4. 重新启动 MySQL 或 MariaDB 服务。
5. 启动 Kaspersky Security Center 管理服务器服务。

数据被从共享表空间移动到每个表一个文件表空间。

配置 PostgreSQL 和 Postgres Pro 的使用账户

先决条件

在为账户分配权限之前，请执行以下操作：

1. 确保您以本地管理员账户登录系统。
2. 安装 PostgreSQL 和 Postgres Pro 的使用环境。
3. 配置与 Kaspersky Security Center 15.1 配合使用的 PostgreSQL 或 Postgres Pro 服务器。

4. 确保您有一个安装管理服务器的 Windows 账户。

5. 确保您有一个启动管理服务器服务的 Windows 账户。

配置账户以安装管理服务器（自动创建管理服务器数据库）

要配置用于安装管理服务器的账户：

1. 运行 PostgreSQL 和 Postgres Pro 的使用环境。

2. 选择一个 Postgres 角色来访问 DBMS。您可以使用以下角色之一：

   - *Postgres* 用户（默认 Postgres 角色）。

     如果您使用 *Postgres* 用户，则无需为其授予额外的权限。

   - 新的 Postgres 角色。

     如果您希望使用新的 Postgres 角色，请创建该角色，然后为其授予 CREATEDB 权限。为此，请运行以下脚本（此脚本中的角色是 *KSCAdmin*）：

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '< 密码 >' CREATEDB;
     ```

     创建的角色将作为管理服务器数据库（以下也简称为“服务器数据库”）的所有者。

3. 以用于运行管理服务器安装程序（以下也简称为“安装程序”）的 Windows 账户登录系统。

4. 运行安装程序。

   管理服务器设置向导启动。遵照向导的说明操作。

5. 选择“管理服务器自定义安装”选项。

6. 选择“PostgreSQL 或 Postgres Pro 作为 DBMS”来存储管理服务器数据库。

7. 指定服务器数据库名称。安装程序将自动创建服务器数据库。

8. 指定 Postgres 角色的凭证。

9. 指定用于启动管理服务器服务的 Windows 账户。

   您可以选择现有的 Windows 用户账户或使用安装程序自动创建 KL-AK-* 格式的新 Windows 账户。无论选择何种账户，安装程序都会将所需的系统权限分配给管理服务器服务账户。

安装完成后，将自动创建服务器数据库，管理服务器进入就绪状态。

配置账户以安装管理服务器（手动创建管理服务器数据库）

要配置用于安装管理服务器的账户：

1. 运行 Postgres 的使用环境。

2. 使用 *Postgres*数据库中的*Postgres*登录。

3. 创建一个新的 Postgres 角色（在本例中，该角色是*KSCAdmin*）：

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '< 密码 >';
   ```

4. 创建管理服务器数据库（在本例中，管理服务器数据库名称为*KAV*）：

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   如果发生“新编码 (UTF8) 与模板数据库编码不兼容”错误，请使用以下命令创建数据库：
   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;
   ```
   而不是：
   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

5. 为该角色授予管理服务器数据库的所有权限：

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   确保该角色对管理服务器数据库具有默认的 CONNECT 和 TEMPORARY 权限。

6. 为创建的 Postgres 角色授予以下权限：

   - 针对公共架构中所有表的权限：ALL
   - 针对公共架构中所有序列的权限：ALL

   为此，请以 *Postgres* 用户角色登录服务器数据库，然后运行以下脚本（此脚本中的角色是 *KSCAdmin*）：

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. 以用于运行安装程序的 Windows 账户登录系统。

8. 运行管理服务器安装程序。
   管理服务器设置向导启动。遵照向导的说明操作。

9. 选择“管理服务器自定义安装”选项。

10. 选择“PostgreSQL 或 Postgres Pro 作为 DBMS”来存储管理服务器数据库。

11. 指定服务器数据库名称。使用您在脚本中指定的相同数据库名称。请注意，数据库名称区分大小写。

12. 指定 Postgres 角色的凭证。

13. 指定用于启动管理服务器服务的 Windows 账户。
    您可以选择现有的 Windows 用户账户或使用安装程序自动创建 KL-AK-* 格式的新 Windows 账户。无论选择何种账户，安装程序都会将所需的系统权限分配给管理服务器服务账户。

安装完成后，管理服务器将使用所创建数据库来存储管理服务器数据。管理服务器进入就绪状态。

方案：对 Microsoft SQL Server 进行身份验证

本节中的信息仅适用于 Kaspersky Security Center 使用 Microsoft SQL Server 作为数据库管理系统的配置。

为了保护 Kaspersky Security Center 传输到或传输自数据库的数据以及数据库中存储的数据免受未经授权的访问，必须加密 Kaspersky Security Center 与 SQL Server 之间的通信。提供安全通信的最可靠方法是在同一设备上安装 Kaspersky Security Center 和 SQL Server，并对这两个应用程序使用共享内存机制。在所有其他情况下，建议使用 SSL 或 TLS 证书对 SQL Server 实例进行身份验证。您可以使用来自可信证书颁发机构 (CA) 的证书或自签名证书。建议您使用来自可信 CA 的证书，因为自签名证书仅提供有限保护。

SQL Server 身份验证分阶段进行：

1. **根据证书要求，为 SQL Server 生成自签名 SSL 或 TLS 证书**

   如果您已经有 SQL Server 证书，请跳过此步骤。

   SSL 证书仅适用于 2016 (13.x) 之前的 SQL Server 版本。在 SQL Server 2016 (13.x) 及更高版本中，使用 TLS 证书。

   例如，要生成 TLS 证书，请在 PowerShell 中输入以下命令：

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   > 在命令中，对于 SQL_HOST_NAME，如果主机包含在域中，则必须键入 SQL Server 主机名；如果主机不包含在域中，则必须键入主机的*完全限定域名* (FQDN)。在管理服务器安装向导中必须指定相同名称（主机名或 FQDN）作为 SQL Server 实例名称。

2. **在 SQL Server 实例上添加证书**

   此阶段的说明取决于运行 SQL Server 的平台。有关详细信息，请参阅官方文档：

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   要在故障转移集群上使用证书，必须在故障转移集群的每个节点上安装证书。有关详细信息，请参阅 Microsoft 文档。

3. **分配服务账户权限**

   确保运行 SQL Server 服务所使用的服务账户具有完全控制权限以访问私钥。有关详细信息，请参阅 Microsoft 文档。

4. **将证书添加到 Kaspersky Security Center 的受信任证书列表中**

   在管理服务器设备上，将证书添加到受信任证书列表中。有关详细信息，请参阅 Microsoft 文档。

5. **在 SQL Server 实例与 Kaspersky Security Center 之间启用加密连接**

   在管理服务器设备上，为环境变量 `KLDBADO_UseEncryption` 设置值 `1`。例如，在 Windows Server 2012 R2 中，可以通过在“**系统属性**”窗口的“**高级**”选项卡上单击“**环境变量**”来更改环境变量。添加一个新变量，将其命名为 `KLDBADO_UseEncryption`，然后设置值 `1`。

6. **使用 TLS 1.2 协议的其他配置**

如果使用 TLS 1.2 协议，则另外执行以下操作：

- 确保已安装的 SQL Server 版本是 64 位应用程序。
- 在管理服务器设备上安装 Microsoft OLE DB 驱动程序。有关详细信息，请参阅 Microsoft 文档。
- 在管理服务器设备上，为环境变量 `KLDBADO_UseMSOLEDBSQL` 设置值 `1`。例如，在 Windows Server 2012 R2 中，可以通过在“**系统属性**”窗口的“**高级**”选项卡上单击“**环境变量**”来更改环境变量。添加一个新变量，将其命名为 `KLDBADO_UseMSOLEDBSQL`，然后设置值 `1`。

  如果 OLE DB 驱动程序版本为 19 或更高版本，还需设置值 `MSOLEDBSQL19` 为环境变量 `KLDBADO_ProviderName`。

7. **在 SQL Server 命名实例上启用 TCP/IP 协议**

   如果使用 SQL Server 命名实例，则另外启用 TCP/IP 协议并为 SQL Server 数据库引擎分配一个 TCP/IP 端口号。在管理服务器安装向导中配置 SQL Server 连接时，在“**SQL Server 实例名称**”字段中指定 SQL Server 主机名和端口号。

场景：验证 MySQL 服务器

我们建议您使用 TLS 证书对 MySQL 服务器进行身份验证。您可以使用来自可信证书颁发机构 (CA) 的证书或自签名证书。

管理服务器支持 MySQL 的单向和双向 SSL 身份验证。

启用单向 SSL 身份验证

请按照以下步骤为 MySQL 配置单向 SSL 身份验证：

1 为 MySQL 服务器生成自签名 TLS 证书

在 PowerShell 中，将目录更改为要存储证书的文件夹。执行以下命令：

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)
$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)
$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)
$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)
$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)
$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@
$CertLeafPemKey = @”
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@
$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@
# Output to file
$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii
$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

这些命令可为当前用户创建证书并将证书导出为 PEM 格式。您只需要导出的 PEM 文件来验证服务器。要从 Windows 中删除创建的证书，请在 PowerShell 中执行以下命令：

```
certmgr.msc
```

在**个人** → **证书**文件夹中定位创建的证书并将其删除。

2 创建服务器标志文件

使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

使用 klscflag 实用程序来创建 KLSRV_MYSQL_OPT_SSL_CA 服务器标志并指定证书的路径作为其值。

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem的路径> -t s
```

3 配置数据库

在 my.cnf 文件中指定证书。在文本编辑器中打开 my.cnf 文件并将以下行添加到 [mysqld] 部分中：

```
[mysqld]
```

```
ssl-ca="...\mysqlcerts\ca-cert.pem"

ssl-cert="...\mysqlcerts\server-cert.pem"

ssl-key="...\mysqlcerts\server-key.pem"
```

启用双向 SSL 身份验证

请按照以下步骤为 MySQL 配置双向 SSL 身份验证：

1. **创建服务器标志文件**

   使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

   使用 klscflag 实用程序来创建服务器标记并指定证书文件的路径作为其值：

   ```
   ca-cert.pem> -t s的klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <路径

   server-cert.pem> -t s的klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <路径

   server-key.pem> -t s的klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <路径
   ```

2. **指定密码（可选）**

   如果 server-key.pem 需要密码，请创建 KLSRV_MARIADB_OPT_TLS_PASPHRASE 标记并指定密码作为其值：

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <passphrase> -t s
   ```

3. **配置数据库**

   在 my.cnf 文件中指定证书。在文本编辑器中打开 my.cnf 文件并将以下行添加到 [mysqld] 部分中：

   ```
   [mysqld]

   ssl-ca="...\ca-cert.pem"

   ssl-cert="...\server-cert.pem"

   ssl-key="...\server-key.pem"
   ```

场景：验证 PostgreSQL 服务器

我们建议您使用 TLS 证书对 PostgreSQL 服务器进行身份验证。您可以使用来自可信证书颁发机构 (CA) 的证书或自签名证书。请使用来自可信 CA 的证书，因为自签名证书仅提供有限保护。

管理服务器支持 PostgreSQL 的单向和双向 SSL 身份验证。

PostgreSQL 服务器的认证分为几个阶段进行：

1. **为 PostgreSQL 服务器生成证书**

   在基于 OpenSSL 的跨平台实用程序中，执行以下命令：

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj
   "/CN=psql"

   chmod og-rwx psql.key
   ```

2. **为管理服务器生成证书**

运行以下命令。CN 值应与代表管理服务器连接到 PostgreSQL 的用户名匹配。默认情况下，用户名设置为 postgres。

```
openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
```

```
chmod og-rwx postgres.key
```

3. **配置客户端证书身份验证**

修改 pg_hba.conf 如下：

```
hostssl all all 0.0.0.0/0 md5
```

确保 pg_hba.conf 不包含以`host`开头的记录。

4. **指定 PostgreSQL 证书**

单向 SSL 身份验证

修改 postgresql.conf 如下（指定 .crt 和 .key 文件的正确路径）：

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

双向 SSL 身份验证

修改 postgresql.conf 如下（指定 .crt 和 .key 文件的正确路径）：

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **重新启动 PostgreSQL 守护进程**

运行以下命令：

```
systemctl restart postgresql-14.service
```

6. **指定管理服务器的服务器标志**

单向 SSL 身份验证

使用 klscflag 实用程序来创建 KLSRV_POSTGRES_OPT_SSL_CA 服务器标记并指定证书的路径作为其值。

使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

运行以下命令：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <path to psql.crt> -t s
```

双向 SSL 身份验证

使用 klscflag 实用程序来创建服务器标记并指定证书文件的路径作为其值。

使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

运行以下命令：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <path to psql.crt> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <path to postgres.crt> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <path to postgres.key> -t s
```

如果 postgres.key 需要密码，请创建 KLSRV_POSTGRES_OPT_TLS_PASPHRASE 标记并指定密码作为其值：

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <passphrase> -t s
```

7. **重启管理服务器服务**

管理服务器安装建议

该部分包含了如何安装管理服务器的建议。该部分还提供了使用管理服务器上的共享文件夹以便部署网络代理到客户端设备的方案。

在失败转移集群上为管理服务器服务创建账户

默认下，安装程序自动为管理服务器服务创建非特权账户。该行为对于在常规设备上安装管理服务器来说是最方便的。

然而，在失败转移的集群上安装管理服务器需要不同的方案：

1. 为管理服务器服务创建非特权域账户，并把它们作为以 KLAdmins 为名称的全局域安全组的成员。
2. 在管理服务器安装程序中，指定为服务创建的域账户。

定义共享文件夹

当安装管理服务器时，您可以指定共享文件夹位置。您也可以在安装后，在管理服务器属性中指定共享文件夹位置。默认下，共享文件夹将被创建在管理服务器所在设备(对 **Everyone** 子组具有读权限)。然而，在一些情况下(例如高负载或需要从隔离网络访问)，最好放置共享文件夹到专用文件资源。

共享文件夹在网络代理部署中偶尔使用。

> 共享文件夹必须禁用大小写敏感。

使用管理服务器工具通过活动目录组策略远程安装

如果目标设备位于 Windows 域(没有工作组)中，初始化部署(安装网络代理和安全应用程序到未被管理的设备)必须通过活动目录组策略执行。部署使用 Kaspersky Security Center 远程安装标准任务执行。如果网络规模较大，最好放置共享文件夹到专用文件资源以便降低管理服务器设备磁盘子系统的负载。

通过传送 UNC 路径到独立包远程安装

如果组织网络设备用户具有本地管理员权限，另一个初始化部署方法就是创建一个独立网络代理安装包(或者一个与安全应用程序一起的"连结的"网络代理安装包)。在您创建独立包后，发送给用户一个位于共享文件夹中的安装包的链接。当用户点击链接时安装开始。

从管理服务器共享文件夹更新

在反病毒更新任务中，您可以配置从管理服务器共享文件夹更新。如果任务被分配了大量设备，最好放置共享文件夹到专用文件资源。

安装操作系统镜像

操作系统镜像总是通过共享文件夹安装：设备从共享文件夹读取操作系统镜像。如果镜像部署被分配了大量组织设备，最好放置共享文件夹到专用文件资源。

指定管理服务器地址

当安装管理服务器时，您可以指定管理服务器地址。该地址将用作创建网络代理安装包时的默认地址。

作为管理服务器地址，您可以指定以下内容：

- 管理服务器的 NetBIOS 名称，默认指定
- 管理服务器的完全限定域名 (FQDN) （如果组织网络上的域名系统 (DNS) 已配置且运行正常）
- 外部地址（如果管理服务器安装在非管制区域 (DMZ) 中）

此后，您将可以通过使用管理控制台工具更改管理服务器地址；地址将不会在所创建的网络代理安装包中自动更改。

标准安装

标准安装是使用应用程序文件默认路径的管理服务器安装，安装默认插件集，不启用移动设备管理。

要在本地设备上安装 Kaspersky Security Center 管理服务器：

运行 ksc_<版本号>.<内部版本号>_full_<本地化语言>.exe 可执行文件。

提示您选择要安装的 Kaspersky 程序的窗口将打开。在程序选择窗口，点击**安装 Kaspersky Security Center 管理服务器**链接启动管理服务器服务器安装向导。遵照向导的说明操作。

步骤 1：查看授权许可协议和隐私策略

在安装向导的此步骤，您必须阅读您和 Kaspersky 之间的授权许可协议以及隐私策略。

还可能会提示阅读 Kaspersky Security Center 分发包中可用应用程序管理插件的授权许可协议和隐私策略。

请认真阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私政策的所有条款，请通过选中相应的复选框进行确认。

在您选择两个复选框后，你设备上的应用程序安装将继续。

如果您不接受许可协议或隐私策略，请单击“**取消**”按钮，取消安装。

步骤 2：选择安装方法

在安装类型选择窗口，选择**标准**。

标准安装用在您要尝试 Kaspersky Security Center 并在企业网络中的小区域测试其操作的时候。在标准安装期间，您仅配置数据库。您不指定任何管理服务器设置：它们的默认值被使用。标准安装不允许您选择要安装的管理插件；仅默认的插件集被安装。在标准安装期间，不创建移动设备安装包。然而，您可以稍后在管理控制台创建它们。

步骤 3：安装 Kaspersky Security Center Web Console

该步骤仅在您使用 64 位操作系统时显示。否则，该步骤不被显示，因为 Kaspersky Security Center Web Console 不工作在 32 位操作系统下。

默认情况下，将同时安装 Kaspersky Security Center Web Console 和基于 MMC 的管理控制台。

如果要只安装 Kaspersky Security Center Web Console：

1. 选择“**仅安装此项**”。
2. 在下拉列表中选择“**基于 Web 的控制台**”。

管理服务器安装完成后，将自动开始安装 Kaspersky Security Center Web Console。

如果您只想安装基于 MMC 的管理控制台：

1. 选择“**仅安装此项**”。
2. 在下拉列表中选择“**基于 MMC 的控制台**”。

步骤 4：选择网络规模

指定要安装 Kaspersky Security Center 的网络的大小。向导会视网络中的设备数量来配置应用程序的安装和界面外观，以使其匹配。

下表列出了在不同的网络规模下程序安装设置和程序界面外观的不同。

选择不同网络规模时安装设置的区别

设置	1–100 台受管理设备	101–1000 台受管理设备	1001–5000 台受管理设备	多于 5000 台受管理设备
显示从属和虚拟管理服务器的节点，以及与从属和虚拟管理服务器相关的所有设置（仅在基于 MMC 的管理控制台中可用）	不适用	不适用	适用	适用
在管理服务器和管理组的属性窗口中显示**安全**部分（仅在基于 MMC 的管理控制台中可用）	不适用	不适用	适用	适用
在客户端设备上随机分配更新任务的启动时间	不适用	以 5 分钟为间隔	以 10 分钟为间隔	以 10 分钟为间隔

如果将管理服务器连接至 MySQL 5.7 或 SQL Express 数据库服务器，不建议使用该应用程序管理 10,000 台以上的设备。对于 MariaDB 数据库管理系统，建议的受管理设备最大数量为 20000。

步骤 5：选择数据库

在向导的这一步，选择将用于存储管理服务器数据库的以下数据库管理系统 (DBMS) 之一：

- **Microsoft SQL Server 或 SQL Server Express**
- **MySQL 或 MariaDB**
- **PostgreSQL 或 Postgres Pro**

建议将管理服务器安装在专用服务器上，而不是域控制器上。但是，如果在用作只读域控制器 (RODC) 的服务器上安装 Kaspersky Security Center，则不得在本地（同一设备上）安装 Microsoft SQL Server (SQL Express)。在这种情况下，如果需要在本地安装 DBMS，建议您（在另一台设备上）远程安装 Microsoft SQL Server (SQL Express)，或者使用 MySQL、MariaDB 或 PostgreSQL。

管理服务器数据库结构在 klakdb.chm 文件中提供，该文件位于 Kaspersky Security Center 安装文件夹中。该文件也可在卡巴斯基门户的存档中找到：klakdb.zip。

步骤 6：配置 SQL Server

在向导的这一步，根据您选择的数据库管理系统 (DBMS)，指定以下连接设置：

- 如果在上一步中选择了“**Microsoft SQL Server 或 SQL Server Express**”：
  - 在**SQL Server 实例名称**字段，指定网络中的 SQL Server 名称。要查看网络上的所有 SQL Server 列表，请单击“**浏览**”按钮。默认情况下该字段为空。

    如果通过自定义端口连接到 SQL Server，则将 SQL Server 主机名与端口号一起指定，用逗号分隔，例如：

    ```
    SQL_Server_host_name,1433
    ```

    如果使用证书加密管理服务器与 SQL Server 之间的通信，请在“**SQL Server 实例名称**”字段中指定在生成证书时使用的主机名。如果使用 SQL Server 命名实例，则将 SQL Server 主机名与端口号一起指定，用逗号分隔，例如：

    ```
    SQL_Server_name,1433
    ```

    如果在同一主机上使用多个 SQL Server 实例，则另外指定实例名称，并用反斜杠分隔，例如：

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    如果企业网络上的 SQL Server 启用了 Always On 功能，请在**SQL Server 实例名称**字段中指定可用性组侦听器的名称。请注意，当启用 Always On 功能时管理服务器仅支持同步提交可用性模式。
  - 在“**数据库名称**”字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。

如果此阶段您要在正安装 Kaspersky Security Center 的设备上安装 SQL Server，您必须终止安装 Kaspersky Security Center，并在 SQL Server 安装完成后重新启动 Kaspersky Security Center 的安装。支持的 SQL Server 版本在系统需求中列出。

如果您要在远程设备上安装 SQL Server，则无需中断 Kaspersky Security Center 安装向导。安装 SQL Server，然后继续安装 Kaspersky Security Center。

- 如果在上一步中选择了“**MySQL 或 MariaDB**”：
  - 在**SQL Server 实例名称**字段，指定 DBMS 实例名称。默认下，名称是要安装 Kaspersky Security Center 的设备的 IP 地址。
  - 在**端口**字段，指定管理服务器连接到 DBMS 的端口。默认端口号是 3306。
  - 在“**数据库名称**”字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。
- 如果在上一步中选择了“**PostgreSQL 或 Postgres Pro**”：
  - 在**PostgreSQL 或 Postgres Pro Server**字段，指定 DBMS 实例名称。默认下，名称是要安装 Kaspersky Security Center 的设备的 IP 地址。
  - 在**端口**字段，指定管理服务器连接到 DBMS 的端口。默认端口号是 5432。
  - 在“**数据库名称**”字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。

步骤 7：选择身份验证模式

确定在将管理服务器连接至数据库管理系统 (DBMS) 时使用的身份验证模式。

您可以根据所选 DBMS 从以下身份验证模式中进行选择：

- 对于 SQL Express 或 Microsoft SQL Server，请选择以下选项之一：
  - **Microsoft Windows 身份验证模式**。使用启动管理服务器的用户来验证权限。
  - **SQL Server 身份验证模式**。如果选择此选项，则会使用在窗口中指定的账户来验证访问权限。填写**账户**和 **密码** 字段。

    要查看输入的密码，单击并按住“**显示**”按钮。

  对于两个身份验证模式，应用程序检查数据库是否可用。如果数据库不可用，则显示错误消息，且您必须提供正确的凭证。

  如果管理服务器数据库存储在另外一台设备上，并且管理服务器账户无法访问该数据库服务器，则在安装或升级管理服务器时必须使用 SQL Server 身份验证模式。可能发生这种情况的情形为：存储数据库的设备在域之外，或管理服务器已安装在 LocalSystem 账户之下。

- 对于 MySQL、MariaDB、PostgreSQL 或 Postgres Pro，请指定账户和密码。

步骤 8：在硬盘驱动器上解压并安装文件

Kaspersky Security Center 组件的安装配置完成后，便可以开始在硬盘驱动器上安装文件。

如果安装需要其他程序，安装向导将在开始安装 Kaspersky Security Center 之前，在“**安装先决条件**”页面中通知您。所需程序将在您单击“**下一步**”按钮后自动安装。

在最后一页，您可以选择启动哪个控制台以使用 Kaspersky Security Center：

- **启动基于 MMC 的管理控制台**
- **启动 Kaspersky Security Center Web Console**
  该选项仅在您在先前步骤中选择了安装 Kaspersky Security Center Web Console 时可用。

您也可以点击**完成**以关闭向导而不使用 Kaspersky Security Center。您可以稍后随时开始使用。

在管理控制台或者 Kaspersky Security Center Web Console 第一次启动时，您可以执行应用程序初始化设置。

安装向导完成后，以下程序组件便会安装在操作系统所在的硬盘驱动器：

- 管理服务器（以及服务器版本的网络代理）
- 基于 Microsoft Management Console 的管理控制台
- Kaspersky Security Center Web Console（如果您选择安装）
- 应用程序管理插件在分发包中可用

另外，Microsoft Windows Installer 4.5 如果先前未安装，则将被安装。

自定义安装

自定义安装是指在管理服务器安装过程中您可以选择要安装的组件并指定应用程序被安装到的文件夹。

使用该安装类型，您可以配置数据库和管理服务器，以及安装不包含在标准安装中的组件或众多 Kaspersky 安全应用程序的管理插件。您也可以启用移动设备管理。

要在本地设备上安装 Kaspersky Security Center 管理服务器：

运行 ksc_<版本号>.<内部版本号>_full_<本地化语言>.exe 可执行文件。

提示您选择要安装的 Kaspersky 程序的窗口将打开。在程序选择窗口，点击**安装 Kaspersky Security Center 管理服务器**链接启动管理服务器服务器安装向导。遵照向导的说明操作。

步骤 1：查看授权许可协议和隐私策略

在安装向导的此步骤，您必须阅读您和 Kaspersky 之间的授权许可协议以及隐私策略。

还可能会提示阅读 Kaspersky Security Center 分发包中可用应用程序管理插件的授权许可协议和隐私策略。

请认真阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私政策的所有条款，请通过选中相应的复选框进行确认。

在您选择两个复选框后，你设备上的应用程序安装将继续。

如果您不接受许可协议或隐私策略，请单击“**取消**”按钮，取消安装。

步骤 2：选择安装方法

在安装类型选择窗口，指定 **自定义**。

自定义安装允许您修改 Kaspersky Security Center 设置，例如共享文件夹路径、账户和连接管理服务器的端口，以及数据库设置。自定义安装允许您指定安装哪些 Kaspersky 管理插件。在自定义安装期间，您可以通过启用相关选项为移动设备创建安装包。

步骤 3：选择要安装的组件

选择您希望安装的 Kaspersky Security Center 管理服务器组件：

- **移动设备管理**。如果您要在 Kaspersky Security Center 安装向导运行时为移动设备创建安装包，则选择此复选框。您也可以在管理服务器安装后，使用管理控制台工具手动创建移动设备安装包。
- **SNMP 代理**。此组件接收通过 SNMP 协议收集管理服务器的统计信息。此组件仅在程序安装在装有 SNMP 的设备上时可用。

  安装 Kaspersky Security Center 后，用于接收统计数据的 .mib 文件将放在程序安装文件夹下的 SNMP 子文件夹中。

网络代理和管理控制台未显示在组件列表中。这些组件将自动安装，您无法取消它们的安装。

在本步，您需要指定管理服务器组件的安装文件夹。默认情况下，这些组件将安装到 <磁盘>:\Program Files\Kaspersky Lab\Kaspersky Security Center 中。如果文件夹不存在，则会在安装过程中自动创建。您可以使用“**浏览**”按钮更改目标文件夹。

步骤 4：安装 Kaspersky Security Center Web Console

该步骤仅在您使用 64 位操作系统时显示。否则，该步骤不被显示，因为 Kaspersky Security Center Web Console 不工作在 32 位操作系统下。

默认情况下，将同时安装 Kaspersky Security Center Web Console 和基于 MMC 的管理控制台。

如果要只安装 Kaspersky Security Center Web Console：

1. 选择“**仅安装此项**”。
2. 在下拉列表中选择“**基于 Web 的控制台**”。

管理服务器安装完成后，将自动开始安装 Kaspersky Security Center Web Console。

如果您只想安装基于 MMC 的管理控制台：

1. 选择“**仅安装此项**”。
2. 在下拉列表中选择“**基于 MMC 的控制台**”。

步骤 5：选择网络规模

指定要安装 Kaspersky Security Center 的网络的大小。向导会视网络中的设备数量来配置应用程序的安装和界面外观，以使其匹配。

下表列出了在不同的网络规模下程序安装设置和程序界面外观的不同。

选择不同网络规模时安装设置的区别

设置	1–100 台受管理设备	101–1000 台受管理设备	1001–5000 台受管理设备	多于 5000 台受管理设备
显示从属和虚拟管理服务器的节点，以及与从属和虚拟管理服务器相关的所有设置（仅在基于 MMC 的管理控制台中可用）	不适用	不适用	适用	适用
在管理服务器和管理组的属性窗口中显示**安全**部分（仅在基于 MMC 的管理控制台中可用）	不适用	不适用	适用	适用
在客户端设备上随机分配更新任务的启动时间	不适用	以 5 分钟为间隔	以 10 分钟为间隔	以 10 分钟为间隔

如果将管理服务器连接至 MySQL 5.7 或 SQL Express 数据库服务器，不建议使用该应用程序管理 10,000 台以上的设备。对于 MariaDB 数据库管理系统，建议的受管理设备最大数量为 20000。

步骤 6：选择数据库

在向导的这一步，选择将用于存储管理服务器数据库的以下数据库管理系统 (DBMS) 之一：

- **Microsoft SQL Server 或 SQL Server Express**
- **MySQL 或 MariaDB**
- **PostgreSQL 或 Postgres Pro**

建议将管理服务器安装在专用服务器上，而不是域控制器上。但是，如果在用作只读域控制器 (RODC) 的服务器上安装 Kaspersky Security Center，则不得在本地（同一设备上）安装 Microsoft SQL Server (SQL Express)。在这种情况下，如果需要在本地安装 DBMS，建议您（在另一台设备上）远程安装 Microsoft SQL Server (SQL Express)，或者使用 MySQL、MariaDB 或 PostgreSQL。

管理服务器数据库结构在 klakdb.chm 文件中提供，该文件位于 Kaspersky Security Center 安装文件夹中。该文件也可在卡巴斯基门户的存档中找到：klakdb.zip。

步骤 7：配置 SQL Server

在向导的这一步，根据您选择的数据库管理系统 (DBMS)，指定以下连接设置：

- 如果在上一步中选择了“**Microsoft SQL Server 或 SQL Server Express**”：
  - 在**SQL Server 实例名称**字段，指定网络中的 SQL Server 名称。要查看网络上的所有 SQL Server 列表，请单击“**浏览**”按钮。默认情况下该字段为空。

    如果通过自定义端口连接到 SQL Server，则将 SQL Server 主机名与端口号一起指定，用逗号分隔，例如：

    ```
    SQL_Server_host_name,1433
    ```

    如果使用证书加密管理服务器与 SQL Server 之间的通信，请在“**SQL Server 实例名称**”字段中指定在生成证书时使用的主机名。如果使用 SQL Server 命名实例，则将 SQL Server 主机名与端口号一起指定，用逗号分隔，例如：

    ```
    SQL_Server_name,1433
    ```

    如果在同一主机上使用多个 SQL Server 实例，则另外指定实例名称，并用反斜杠分隔，例如：

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    如果企业网络上的 SQL Server 启用了 Always On 功能，请在**SQL Server 实例名称**字段中指定可用性组侦听器的名称。请注意，当启用 Always On 功能时管理服务器仅支持同步提交可用性模式。
  - 在“**数据库名称**”字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。

  如果此阶段您要在正安装 Kaspersky Security Center 的设备上安装 SQL Server，您必须终止安装 Kaspersky Security Center，并在 SQL Server 安装完成后重新启动 Kaspersky Security Center 的安装。支持的 SQL Server 版本在系统需求中列出。

  如果您要在远程设备上安装 SQL Server，则无需中断 Kaspersky Security Center 安装向导。安装 SQL Server，然后继续安装 Kaspersky Security Center。
- 如果在上一步中选择了“**MySQL 或 MariaDB**”：
  - 在**SQL Server 实例名称**字段，指定 DBMS 实例名称。默认下，名称是要安装 Kaspersky Security Center 的设备的 IP 地址。
  - 在**端口**字段，指定管理服务器连接到 DBMS 的端口。默认端口号是 3306。
  - 在“**数据库名称**”字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。
- 如果在上一步中选择了“**PostgreSQL 或 Postgres Pro**”：
  - 在**PostgreSQL 或 Postgres Pro Server**字段，指定 DBMS 实例名称。默认下，名称是要安装 Kaspersky Security Center 的设备的 IP 地址。
  - 在**端口**字段，指定管理服务器连接到 DBMS 的端口。默认端口号是 5432。
  - 在“**数据库名称**”字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。

步骤 8：选择身份验证模式

确定在将管理服务器连接至数据库管理系统 (DBMS) 时使用的身份验证模式。

您可以根据所选 DBMS 从以下身份验证模式中进行选择：

- 对于 SQL Express 或 Microsoft SQL Server，请选择以下选项之一：
  - **Microsoft Windows 身份验证模式**。使用启动管理服务器的用户来验证权限。
  - **SQL Server 身份验证模式**。如果选择此选项，则会使用在窗口中指定的账户来验证访问权限。填写**账户**和 **密码** 字段。

    要查看输入的密码，单击并按住“**显示**”按钮。

  对于两个身份验证模式，应用程序检查数据库是否可用。如果数据库不可用，则显示错误消息，且您必须提供正确的凭证。

  如果管理服务器数据库存储在另外一台设备上，并且管理服务器账户无法访问该数据库服务器，则在安装或升级管理服务器时必须使用 SQL Server 身份验证模式。可能发生这种情况的情形为：存储数据库的设备在域之外，或管理服务器已安装在 LocalSystem 账户之下。

- 对于 MySQL、MariaDB、PostgreSQL 或 Postgres Pro，请指定账户和密码。

步骤 9：选择账户以启动管理服务器

选择用于启动管理服务器作为服务的账户。

- **自动生成账户**。应用程序创建名为 KL-AK-* 的账户，kladminserver 服务在该账户下运行。

  如果您计划将共享文件夹和 DBMS 放置在管理服务器所在设备。

- **选择账户**。管理服务器服务(kladminserver)将在您选择的账户下运行。

  例如，如果您计划使用其他设备上任意版本的 SQL Server 实例（包括 SQL Express）作为 DBMS，且/或您计划查找其他设备上的共享文件夹，您必须选择域账户。

  Kaspersky Security Center 支持受管理服务账户 (MSA) 和受管理服务账户组 (gMSA)。如果这些账户类型在您的域中被使用，您可以选择它们之一作为管理服务器服务账户。

  在指定 MSA 或 gMSA 之前，必须在将要安装管理服务器的同一设备上安装该账户。如果尚未安装该账户，则取消管理服务器安装，安装该账户，然后重新启动管理服务器安装。关于在本地设备上安装受管服务账户的详细信息，请参阅正式的 Microsoft 文档。

  要指定 MSA 或 gMSA：

  1. 单击“**浏览**”按钮。
  2. 在打开的窗口中，单击**对象类型**按钮。
  3. 选择“**服务账户**”类型并单击“**确定**”。
  4. 选择相关账户并点击**确定**。

您选择的账户必须有不同的权限，取决于您计划使用的 DBMS。

出于安全原因，请不要分配权限状态到您运行管理服务器的账户。

管理服务器账户今后不能更改。您需要重新安装故障转移集群以使用另一个管理服务器账户。

步骤 10：选择账户以运行 Kaspersky Security Center 服务

在设备上选择即将运行 Kaspersky Security Center 服务的账户:

- **自动生成账户**。Kaspersky Security Center 在 kladmins 组的设备上创建名为 KlScSvc 的本地账户。Kaspersky Security Center 服务将在已创建的账户下运行。
- **选择账户**。Kaspersky Security Center 服务将运行在您选择的账户下。

  您将必须选择域账户，如果您要保存报告到不同设备的文件夹，或基于您组织的安全策略。如果您安装管理服务器到失败转移集群，您也可能必须选择域账户。

出于安全原因，请不要分配权限状态到您运行服务的账户。

KSN 代理服务 (ksnproxy)、卡巴斯基激活代理服务器服务 (klactprx) 和卡巴斯基身份验证门户服务 (klwebsrv) 将在所选账户下运行。

步骤 11：选择共享文件夹

定义执行以下操作时将使用的共享文件夹的位置和名称:

- 存储远程安装程序所需的文件（这些文件会在创建安装包过程中复制到管理服务器）。
- 将从更新源下载的更新存储到管理服务器。

系统将为所有用户启用文件共享（只读）。

您可以选择以下两个选项之一:

- **创建共享文件夹**。创建新文件夹。在文本框中，指定文件夹路径。
- **选择现有共享文件夹**。选择一个已有的共享文件夹。

共享文件夹可以是正在安装程序的设备上的本地文件夹，也可以是企业网络中任何客户端设备上的远程目录。您可以单击“**浏览**”按钮选择共享文件夹，也可以在相应的字段中输入共享文件夹的 UNC 路径（例如，\\server\Share）手动指定。

默认情况下，安装程序将在为 Kaspersky Security Center 组件选择的安装文件夹中创建一个名为 KLSHARE 的本地子文件夹。

您稍后可以根据需要定义共享文件夹。

步骤 12：配置与管理服务器的连接

配置到管理服务器的连接：

- **端口**

  用于连接至管理服务器的端口号。
  默认端口号是 14000。

- **SSL 端口**

  用于安全地连接至管理服务器的安全套接字层 （SSL） 端口号。
  默认端口号是 13000。

- **加密密钥长度**

  选择加密密钥长度：1024 bit 或 2048 bit。

  1024 位加密密钥少量占用 CPU，但它被认为是过时的，因为由于技术说明，它无法提供可靠的加密。而且，现有硬件可能与 1024 位密钥的 SSL 证书不兼容。
  2048 位加密密钥满足所有加密标准。然而，使用 2048 位加密密钥可能增加 CPU 负载。
  默认下，**2048 bit(最大安全)**被选中。

您还可以稍后更改连接管理服务器的参数，如下所示：

- 您可以稍后在管理服务器属性的**连接端口**部分更改端口和 SSL 端口号。有关管理服务器连接端口的更多信息，请参阅Kaspersky Security Center 使用的端口。

- 使用 klsetsrvcert 实用程序更换管理服务器证书时，可以使用 `-o RsaKeyLen:<key length>` 参数来更改加密密钥长度。

步骤 13：定义管理服务器地址

请用下列方式之一指定管理服务器地址：

- **DNS 域名**。如果网络中包含 DNS 服务器并且客户端设备可以用它接收管理服务器地址，则您可以使用此方法。

- **NetBIOS 名称**。如果客户端设备使用 NetBIOS 协议接收管理服务器地址，或者网络中可使用 WINS 服务器，则您可以使用此方法。

- **IP 地址**。如果管理服务器拥有不会随后变更的静态 IP 地址，则您可以使用此方法。

如果在 Kaspersky Security Center 故障转移集群的活动节点上安装 Kaspersky Security Center，并且在准备集群节点时已创建从属网络适配器，则指定此适配器的 IP 地址。否则，请输入您使用的第三方负载平衡器的 IP 地址。

步骤 14：用于连接移动设备的管理服务器地址

如果选择了安装“移动设备管理”组件，则安装向导会出现这一步。

在**移动设备连接地址**窗口中，指定管理服务器的外部地址以连接本地网络之外的移动设备。您可以指定管理服务器的 IP 地址或域名系统 (DNS)。

步骤 15：选择应用程序管理插件

选择需要与 Kaspersky Security Center 一起安装的应用程序管理插件。

为了搜索方便，插件被根据安全对象类型分成了组。

步骤 16：在硬盘驱动器上解压并安装文件

Kaspersky Security Center 组件的安装配置完成后，便可以开始在硬盘驱动器上安装文件。

如果安装需要其他程序，安装向导将在开始安装 Kaspersky Security Center 之前，在“**安装先决条件**”页面中通知您。所需程序将在您单击“**下一步**”按钮后自动安装。

在最后一页，您可以选择启动哪个控制台以使用 Kaspersky Security Center：

- **启动基于 MMC 的管理控制台**
- **启动 Kaspersky Security Center Web Console**
  该选项仅在您在先前步骤中选择了安装 Kaspersky Security Center Web Console 时可用。

您也可以点击**完成**以关闭向导而不使用 Kaspersky Security Center。您可以稍后随时开始使用。

在管理控制台或者 Kaspersky Security Center Web Console 第一次启动时，您可以执行应用程序初始化设置。

部署 Kaspersky Security Center 故障转移集群

本节包含有关 Kaspersky Security Center 故障转移集群的常规信息，以及有关在网络中准备和部署 Kaspersky Security Center 故障转移集群的说明。

方案：部署Kaspersky Security Center 故障转移集群

Kaspersky Security Center 故障转移集群提供 Kaspersky Security Center 的高可用性，并在出现故障时最大限度地减少管理服务器的停机时间。故障转移集群基于安装在两台计算机上的两个相同 Kaspersky Security Center 实例。其中一个实例用作主动节点，另一个实例用作被动节点。主动节点管理客户端设备的保护，而被动节点准备在主动节点出现故障时承担主动节点的所有功能。当出现故障时，被动节点成为主动节点，主动节点成为被动节点。

先决条件

您拥有满足故障转移集群要求的硬件。

阶段

Kaspersky 应用程序部署分阶段进行：

1. **为 Kaspersky Security Center 服务创建账户**

   创建一个新的域组（在该情景中为此组使用名称“KLAdmins”），然后在两个节点和文件服务器上均为该组授予本地管理员权限。然后创建两个新的域用户账户（在该情景中为这些账户使用名称“ksc”和“rightless”），并将这些账户添加到 KLAdmins 域组。

   将要安装 Kaspersky Security Center 的用户账户添加到之前创建的 KLAdmins 域组。

2. **文件服务器准备**

   准备将用作 Kaspersky Security Center 故障转移集群组件的文件服务器。确保该文件服务器满足硬件和软件要求，为 Kaspersky Security Center 数据创建两个共享文件夹，并配置这两个共享文件夹的访问权限。

   操作说明：为 Kaspersky Security Center 故障转移集群准备文件服务器

3. **准备主动和被动节点**

   准备两台具有相同硬件和软件的设备，它们将用作主动和被动节点。

   操作说明：为 Kaspersky Security Center 故障转移集群准备节点

4. **数据库管理系统 (DBMS) 安装**

   选择任一受支持的 DBMS，然后在专用设备上安装 DBMS。对于如何安装 DBMS 的信息，请参考其文档。

5. **Kaspersky Security Center 安装**

   在两个节点上均以故障转移集群模式安装 Kaspersky Security Center。您必须先在要作为主动主机的设备上安装 Kaspersky Security Center，然后在被动主机上进行安装。

   您必须在非集群节点的单独设备上安装 Kaspersky Security Center Web Console。

   操作说明：在 Kaspersky Security Center 故障转移集群节点上安装 Kaspersky Security Center

6. **测试故障转移集群**

   检查您是否正确配置了故障转移集群以及它是否正常工作。例如，您可以停止主动节点上的 Kaspersky Security Center 服务之一：kladminserver、klnagent、ksnproxy、klactprx 或 klwebsrv。服务停止后，保护管理必须自动切换到被动节点。

结果

Kaspersky Security Center 故障转移集群已部署。请熟悉导致主动和被动节点切换的事件。

关于 Kaspersky Security Center 故障转移集群

Kaspersky Security Center 故障转移集群提供 Kaspersky Security Center 的高可用性，并在出现故障时最大限度地减少管理服务器的停机时间。故障转移集群基于安装在两台计算机上的两个相同 Kaspersky Security Center 实例。其中一个实例用作主动节点，另一个实例用作被动节点。主动节点管理客户端设备的保护，而被动节点准备在主动节点出现故障时承担主动节点的所有功能。当出现故障时，被动节点成为主动节点，主动节点成为被动节点。

使用故障转移集群不会影响基于筛分向导的计算。

使用卡巴斯基事件日志功能进行故障排除。

切换条件

如果主动节点上发生以下任何事件，故障转移集群会将客户端设备的保护管理从主动节点切换到被动节点：

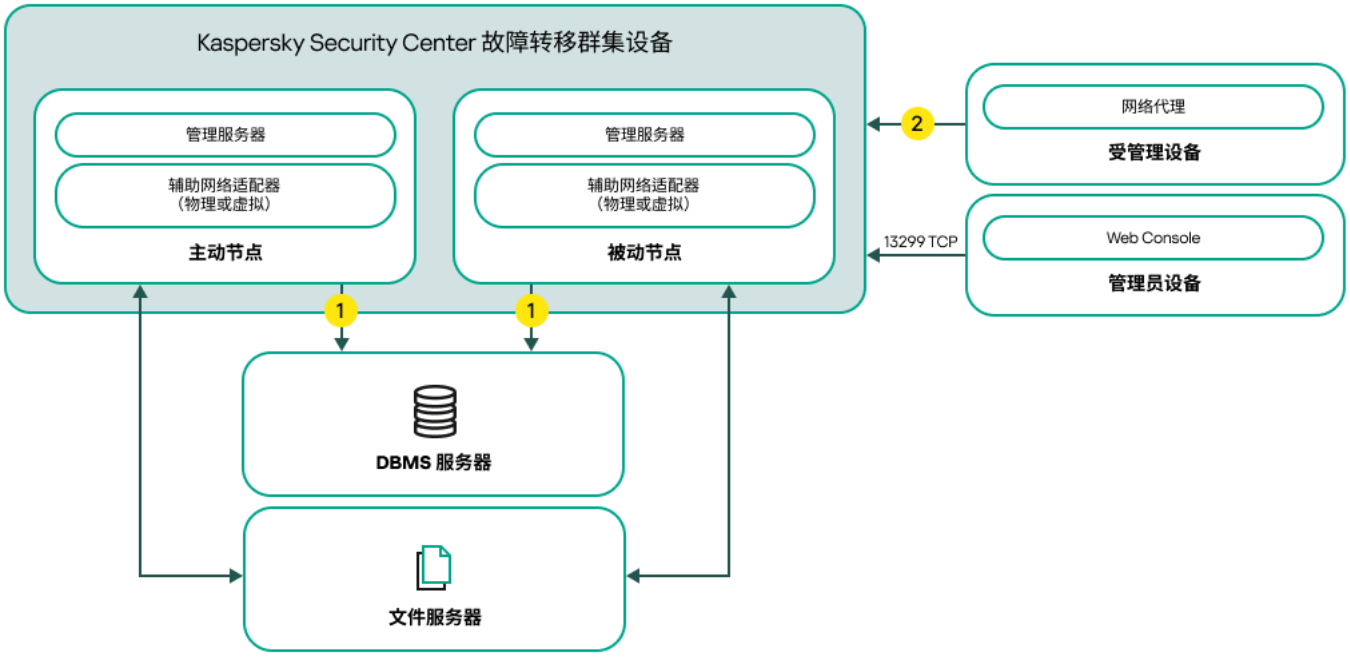
- 由于软件或硬件故障，主动节点损坏。
- 由于维护活动，主动节点暂时停止。
- 至少一个 Kaspersky Security Center 服务（或进程）故障或被用户故意终止。Kaspersky Security Center 服务如下：kladminserver、klnagent、klactprx 和 klwebsrv。
- 主动节点与文件服务器上的存储之间的网络连接中断或终止。

Kaspersky Security Center 故障转移集群自动管理所有 Kaspersky Security Center 服务。请勿手动重启服务。

部署方案

您可以选择以下方案之一来部署 Kaspersky Security Center 故障转移集群：

- 使用从属网络适配器的方案。
- 使用第三方负载均衡器的方案。

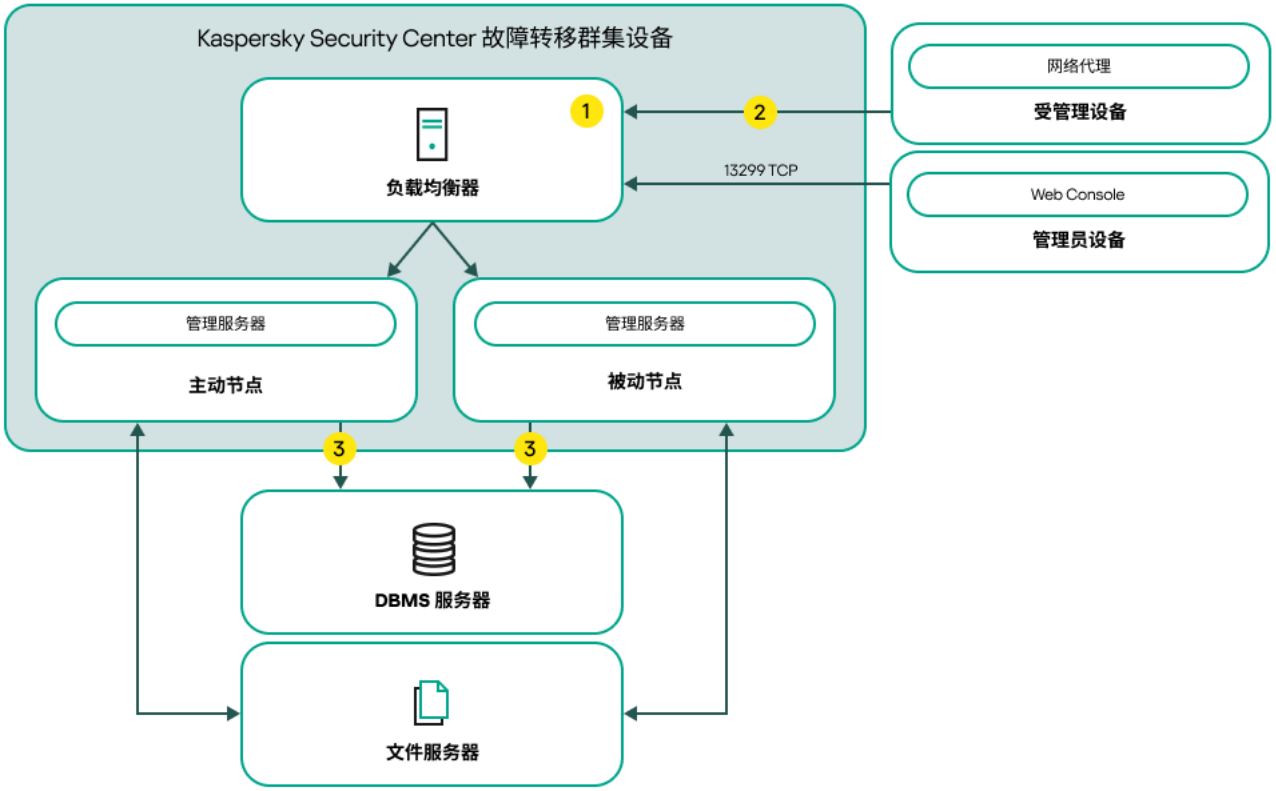


使用从属网络适配器的方案

方案图例：

1 管理服务器发送数据到数据库。在数据库所在的设备上开放必要的端口，例如，MySQL Server 的端口 3306，或 Microsoft SQL Server 的端口 1433。请参阅 DBMS 文档以获取相关信息。

2 在受管理设备上，打开以下端口：TCP 13000、UDP 13000 和 TCP 17000。



使用第三方负载均衡器的方案

方案图例：

1 在负载均衡器设备上，打开所有管理服务器端口：TCP 13000、UDP 13000、TCP 13299 和 TCP 17000。

> 如果您想使用 klakaut 实用程序进行自动化，您还必须打开 TCP 13291 端口。

2 在受管理设备上，打开以下端口：TCP 13000、UDP 13000 和 TCP 17000。

3 管理服务器发送数据到数据库。在数据库所在的设备上开放必要的端口，例如，MySQL Server 的端口 3306，或 Microsoft SQL Server 的端口 1433。请参阅 DBMS 文档以获取相关信息。

为 Kaspersky Security Center 故障转移集群准备文件服务器

文件服务器是 Kaspersky Security Center 故障转移集群的必需组件。

要准备文件服务器：

1. 确保文件服务器满足硬件和软件要求。
2. 确保文件服务器和两个节点（主动和被动）包含在同一个域中，或者文件服务器是域控制器。
3. 在文件服务器上，创建两个共享文件夹。其中一个用于保存有关故障转移集群状态的信息。另一个用于存储 Kaspersky Security Center 的数据和设置。您在配置 Kaspersky Security Center 的安装时将指定共享文件夹的路径。

4. 为以下用户账户和组授予对所创建的共享文件夹的完全访问权限（共享权限和 NTFS 权限）：

   - 域组 KLAdmins。
   - 用户账户 $<node1>和 $<node2>。这里，<node1> 和 <node2> 是主动节点和被动节点的设备名称。

文件服务器已准备就绪。要部署 Kaspersky Security Center 故障转移集群，请按照此方案中的进一步说明进行操作。

为 Kaspersky Security Center 故障转移集群准备节点

准备两台设备作为 Kaspersky Security Center 故障转移集群的主动和被动节点。

要为 Kaspersky Security Center 故障转移集群准备节点：

1. 确保有两台符合硬件和软件要求的设备。这两台设备将用作故障转移集群的主动和被动节点。
2. 确保文件服务器和两个节点均包含在同一个域中。
3. 执行以下操作之一：

   - 在每个节点上，配置一个从属网络适配器。

     从属网络适配器可以是物理或虚拟适配器。如果要使用物理网络适配器，请使用标准操作系统工具连接并配置它。如果要使用虚拟网络适配器，请使用第三方软件创建它。

     确保满足以下条件：

     - 从属网络适配器被禁用。

       您可以创建处于禁用状态的从属网络适配器或在创建后禁用它们。

     - 两个节点上的从属网络适配器必须具有相同的 IP 地址。

   - 使用第三方负载平衡器。例如，您可以使用 nginx 服务器。在这种情况下，请执行以下操作：

     a. 提供一台基于 Linux 且安装了 nginx 的专用设备。

     b. 配置负载平衡。设置主动节点为主服务器，被动节点为备份服务器。

     c. 在 nginx 服务器上，打开所有管理服务器端口：TCP 13000、UDP 13000、TCP 13299 和 TCP 17000。

     > 如果您想使用 klakaut 实用程序进行自动化，您还必须打开 TCP 13291 端口。

4. 重新启动节点和文件服务器。
5. 将您在文件服务器准备步骤中创建的两个共享文件夹映射到各个节点。您必须将共享文件夹映射为网络驱动器。映射文件夹时，可以选择任意空驱动器号。要访问共享文件夹，请使用您在方案的第 1 步中创建的用户账户的凭据。

节点已准备就绪。要部署 Kaspersky Security Center 故障转移集群，请按照方案中的进一步说明进行操作。

在 Kaspersky Security Center 故障转移集群节点上安装 Kaspersky Security Center

Kaspersky Security Center 分别安装在 Kaspersky Security Center 故障转移集群的两个节点上。首先，在主动节点上安装该应用程序，然后在被动节点上安装。安装时，选择哪个节点是主动节点，哪个节点是被动节点。

只有 KLAdmins 域组中的用户可以在每个节点上安装 Kaspersky Security Center。

要在 Kaspersky Security Center 故障转移集群的主动节点上安装 Kaspersky Security Center：

1. 运行 ksc_15.1_<build number>_full_<language>.exe 可执行文件。

   将打开一个窗口，提示您选择要安装的 Kaspersky 应用程序。在程序选择窗口，点击**安装 Kaspersky Security Center 管理服务器**链接启动管理服务器服务器安装向导。遵照向导的说明操作。

2. 请认真阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款，在**我确认我已完整阅读、理解和接受**部分选择以下复选框：

   - **该 EULA 的条款和条件**
   - **描述数据处理的隐私策略**

   在您选择两个复选框后，你设备上的应用程序安装将继续。

   如果您不接受许可协议或隐私策略，请单击“**取消**”按钮，取消安装。

3. 选择“**Kaspersky Security Center 故障转移集群的主要节点**”在主动节点上安装应用程序。

4. 在“**共享文件夹**”窗口中，执行以下操作：

   - 在“**状态共享**”和“**数据共享**”字段中，指定要在准备文件服务器期间在其上创建的共享文件夹的路径。
   - 在“**状态共享驱动器**”和“**数据共享驱动器**”字段中，选择要在准备节点期间将共享文件夹映射到的网络驱动器。
   - 选择集群连接模式：通过从属网络适配器或第三方负载平衡器。

5. 执行自定义安装的其他步骤，从第 3 步开始。

   在第 13 步，如果您在准备集群节点时已创建从属网络适配器，则指定该适配器的 IP 地址。否则，请输入您使用的第三方负载平衡器的 IP 地址。

Kaspersky Security Center 安装在主动节点上。

要在 Kaspersky Security Center 故障转移集群的被动节点上安装 Kaspersky Security Center：

1. 运行 ksc_15.1_<build number>_full_<language>.exe 可执行文件。

   将打开一个窗口，提示您选择要安装的 Kaspersky 应用程序。在程序选择窗口，点击**安装 Kaspersky Security Center 管理服务器**链接启动管理服务器服务器安装向导。遵照向导的说明操作。

2. 请认真阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款，在**我确认我已完整阅读、理解和接受**部分选择以下复选框：

   - **该 EULA 的条款和条件**
   - **描述数据处理的隐私策略**

   在您选择两个复选框后，你设备上的应用程序安装将继续。

   如果您不接受许可协议或隐私策略，请单击“**取消**”按钮，取消安装。

3. 选择“**Kaspersky Security Center 故障转移集群的辅助节点**”在被动节点上安装应用程序。

4. 在“**共享文件夹**”窗口中的“**状态共享**”字段中，指定共享文件夹的路径，该文件夹中包含有关在准备文件服务器期间在其上创建的集群状态的信息。

5. 单击“**安装**”按钮。安装完成后，单击“**完成**”按钮。

Kaspersky Security Center 安装在被动节点上。现在，您可以测试 Kaspersky Security Center 故障转移集群，以确保配置正确并且集群正常工作。

手动启动和停止集群节点

您可能需要停止整个 Kaspersky Security Center 故障转移集群或临时分离集群的一个节点才能进行维护。如果是这种情况，请按照本节中的说明进行操作。请勿尝试通过任何其他方式启动或停止与故障转移集群相关的服务或进程。这可能会导致数据丢失。

启动和停止整个故障转移集群以进行维护

要启动或停止整个故障转移集群：

1. 在主动节点上，转到 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. 打开命令行，然后运行以下命令之一：

   - 要停止集群，请运行：`klfoc -stopcluster --stp klfoc`
   - 要启动集群，请运行：`klfoc -startcluster --stp klfoc`

   启动还是停止故障转移集群取决于您运行的命令。

维护其中一个节点

要维护其中一个节点：

1. 在主动节点上，使用 `klfoc -stopcluster --stp klfoc` 命令停止故障转移集群。

2. 在要维护的节点上，转到 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

3. 打开命令行，然后运行 `detach_node.cmd` 命令将节点从集群中分离。

4. 在主动节点上，使用 `klfoc -startcluster --stp klfoc` 命令启动故障转移集群。

5. 执行维护活动。

6. 在主动节点上，使用 `klfoc -stopcluster --stp klfoc` 命令停止故障转移集群。

7. 在维护后的节点上，转到 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

8. 打开命令行，然后运行 `attach_node.cmd` 命令将节点连接到集群。

9. 在主动节点上，使用 `klfoc -startcluster --stp klfoc` 命令启动故障转移集群。

该节点维护完毕并连接到故障转移集群。

在 Windows 服务器故障转移集群上安装管理服务器

在故障转移集群上安装管理服务器的过程与在独立设备上进行标准安装和自定义安装不同。

在包含集群的公用数据存储的节点上执行本节描述的过程。

要在集群上安装 Kaspersky Security Center 管理服务器：

运行 ksc_<版本号>.<内部版本号>_full_<本地化语言>.exe 可执行文件。

提示您选择要安装的 Kaspersky 程序的窗口将打开。在程序选择窗口，点击**安装 Kaspersky Security Center 管理服务器**链接启动管理服务器服务器安装向导。遵照向导的说明操作。

步骤 1：查看授权许可协议和隐私策略

在安装向导的此步骤，您必须阅读您和 Kaspersky 之间的授权许可协议以及隐私策略。

还可能会提示阅读 Kaspersky Security Center 分发包中可用应用程序管理插件的授权许可协议和隐私策略。

请认真阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私政策的所有条款，请通过选中相应的复选框进行确认。

在您选择两个复选框后，你设备上的应用程序安装将继续。

如果您不接受许可协议或隐私策略，请单击“**取消**”按钮，取消安装。

步骤 2：选择集群上的安装类型

选择集群上的安装类型：

- **集群（在所有集群节点上安装）**
  这是推荐的选项。如果选择此选项，管理服务器将同时安装在集群的所有节点上。

在“选择管理控制台进行安装”这一步中，您将需要选择将安装在当前集群节点上的控制台。如果仅在集群节点上安装控制台，万一节点出现故障，您将无法访问管理服务器。我们建议在这一步中，对于所有集群节点，均选择基于 MMC 的管理控制台进行安装。安装管理服务器后，在不是集群节点的单独设备上安装 Kaspersky Security Center Web Console。这样，您可以在集群节点出现故障时使用 Kaspersky Security Center Web Console 来管理管理服务器。

- **本地（仅在此设备上安装）**

  如果选择此选项，管理服务器将仅安装在当前节点上，就像安装在独立服务器上一样，并且管理服务器不会像集群感知应用程序一样工作。例如，如果管理服务器不需要容错，您可能会想要选择此选项以节省共享存储空间。如果当前节点发生故障，则必须将管理服务器安装在另一个节点上，并从备份中还原管理服务器状态。

后面的步骤与使用标准或自定义安装方法时相同，从安装方法选择步骤开始。

步骤 3：指定虚拟管理服务器的名称

指定新的虚拟管理服务器的网络名称。您将能够使用该名称将管理控制台或 Kaspersky Security Center Web Console 连接到管理服务器。

您指定的名称必须与群集名称不同。

步骤 4：指定虚拟管理服务器的网络详细信息

要指定新的虚拟管理服务器实例的网络详细信息：

1. 在“**要使用的网络**”中，选择当前集群节点连接到的域网络。
2. 做以下之一：
   - 如果所选网络中使用 DHCP 分配 IP 地址，请选中“**使用 DHCP**”选项。
   - 如果所选网络中未使用 DHCP，请指定所需的 IP 地址。

     您指定的 IP 地址必须与集群 IP 地址不同。
3. 单击“**添加**”以应用指定的设置。

   您将能够使用自动分配或指定的 IP 地址将管理控制台或 Kaspersky Security Center Web Console 连接到管理服务器。

步骤 5：指定群集组

集群组是一种特殊的故障转移集群角色，其中包含所有节点的公用资源。您有两个选项：

- 创建新的集群组。

  在大多数情况下，建议使用此选项。新的集群组将包含与管理服务器实例相关的所有公用资源。

- 选择现有集群组。

  如果要使用已经与现有集群组关联的公用资源，请选择此选项。例如，如果要使用与现有集群组关联的存储，并且没有其他存储可用于新集群组，则最好使用此选项。

步骤 6：选择群集数据存储

要选择集群数据存储：

1. 在“**可用存储库**”中，选择将安装虚拟管理服务器实例的公用资源的数据存储。
2. 如果所选数据存储包含多个卷，请在“**磁盘驱动器上的可用部分**”下，选择所需卷。
3. 在“**安装路径**”中，输入将安装虚拟管理服务器实例的公用数据存储的路径。

数据存储已选择。

步骤 7：指定用于远程安装的账户

指定将用于在集群的被动节点上远程安装虚拟管理服务器实例的用户名和密码。

您指定的账户必须被授予集群所有节点的管理特权。

步骤 8：选择要安装的组件

选择您希望安装的 Kaspersky Security Center 管理服务器组件：

- **移动设备管理**。如果您要在 Kaspersky Security Center 安装向导运行时为移动设备创建安装包，则选择此复选框。您也可以在管理服务器安装后，使用管理控制台工具手动创建移动设备安装包。
- **SNMP 代理**。此组件接收通过 SNMP 协议收集管理服务器的统计信息。此组件仅在程序安装在装有 SNMP 的设备上时可用。

  安装 Kaspersky Security Center 后，用于接收统计数据的 .mib 文件将放在程序安装文件夹下的 SNMP 子文件夹中。

网络代理和管理控制台未显示在组件列表中。这些组件将自动安装，您无法取消它们的安装。

在本步，您需要指定管理服务器组件的安装文件夹。默认情况下，这些组件将安装到 <磁盘>:\Program Files\Kaspersky Lab\Kaspersky Security Center 中。如果文件夹不存在，则会在安装过程中自动创建。您可以使用“**浏览**”按钮更改目标文件夹。

步骤 9：选择网络规模

指定要安装 Kaspersky Security Center 的网络的大小。向导会视网络中的设备数量来配置应用程序的安装和界面外观，以使其匹配。

下表列出了在不同的网络规模下程序安装设置和程序界面外观的不同。

选择不同网络规模时安装设置的区别

设置	1–100 台受管理设备	101–1000 台受管理设备	1001–5000 台受管理设备	多于 5000 台受管理设备
显示从属和虚拟管理服务器的节点，以及与从属和虚拟管理服务器相关的所有设置（仅在基于 MMC 的管理控制台中可用）	不适用	不适用	适用	适用
在管理服务器和管理组的属性窗口中显示**安全**部分（仅在基于 MMC 的管理控制台中可用）	不适用	不适用	适用	适用
在客户端设备上随机分配更新任务的启动时间	不适用	以 5 分钟为间隔	以 10 分钟为间隔	以 10 分钟为间隔

如果将管理服务器连接至 MySQL 5.7 或 SQL Express 数据库服务器，不建议使用该应用程序管理 10,000 台以上的设备。对于 MariaDB 数据库管理系统，建议的受管理设备最大数量为 20000。

步骤 10：选择数据库

在向导的这一步，选择将用于存储管理服务器数据库的以下数据库管理系统 (DBMS) 之一：

- **Microsoft SQL Server 或 SQL Server Express**
- **MySQL 或 MariaDB**
- **PostgreSQL 或 Postgres Pro**

建议将管理服务器安装在专用服务器上，而不是域控制器上。但是，如果在用作只读域控制器 (RODC) 的服务器上安装 Kaspersky Security Center，则不得在本地（同一设备上）安装 Microsoft SQL Server (SQL Express)。在这种情况下，如果需要在本地安装 DBMS，建议您（在另一台设备上）远程安装 Microsoft SQL Server (SQL Express)，或者使用 MySQL、MariaDB 或 PostgreSQL。

管理服务器数据库结构在 klakdb.chm 文件中提供，该文件位于 Kaspersky Security Center 安装文件夹中。该文件也可在卡巴斯基门户的存档中找到：klakdb.zip。

步骤 11：配置 SQL Server

在向导的这一步，根据您选择的数据库管理系统 (DBMS)，指定以下连接设置：

- 如果在上一步中选择了“**Microsoft SQL Server 或 SQL Server Express**”：
  - 在**SQL Server 实例名称**字段，指定网络中的 SQL Server 名称。要查看网络上的所有 SQL Server 列表，请单击“**浏览**”按钮。默认情况下该字段为空。

    如果通过自定义端口连接到 SQL Server，则将 SQL Server 主机名与端口号一起指定，用逗号分隔，例如：

    ```
    SQL_Server_host_name,1433
    ```

    如果使用证书加密管理服务器与 SQL Server 之间的通信，请在“**SQL Server 实例名称**”字段中指定在生成证书时使用的主机名。如果使用 SQL Server 命名实例，则将 SQL Server 主机名与端口号一起指定，用逗号分隔，例如：

    ```
    SQL_Server_name,1433
    ```

    如果在同一主机上使用多个 SQL Server 实例，则另外指定实例名称，并用反斜杠分隔，例如：

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

如果企业网络上的 SQL Server 启用了 Always On 功能，请在**SQL Server 实例名称**字段中指定可用性组侦听器的名称。请注意，当启用 Always On 功能时管理服务器仅支持同步提交可用性模式。

- 在"**数据库名称**"字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。

如果此阶段您要在正安装 Kaspersky Security Center 的设备上安装 SQL Server，您必须终止安装 Kaspersky Security Center，并在 SQL Server 安装完成后重新启动 Kaspersky Security Center 的安装。支持的 SQL Server 版本在系统需求中列出。

如果您要在远程设备上安装 SQL Server，则无需中断 Kaspersky Security Center 安装向导。安装 SQL Server，然后继续安装 Kaspersky Security Center。

- 如果在上一步中选择了"**MySQL 或 MariaDB**"：
  - 在**SQL Server 实例名称**字段，指定 DBMS 实例名称。默认下，名称是要安装 Kaspersky Security Center 的设备的 IP 地址。
  - 在**端口**字段，指定管理服务器连接到 DBMS 的端口。默认端口号是 3306。
  - 在"**数据库名称**"字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。
- 如果在上一步中选择了"**PostgreSQL 或 Postgres Pro**"：
  - 在**PostgreSQL 或 Postgres Pro Server**字段，指定 DBMS 实例名称。默认下，名称是要安装 Kaspersky Security Center 的设备的 IP 地址。
  - 在**端口**字段，指定管理服务器连接到 DBMS 的端口。默认端口号是 5432。

在"**数据库名称**"字段中，指定被创建用来存储管理服务器数据的 DBMS 的名称。默认值是 *KAV*。

步骤 12：选择身份验证模式

确定在将管理服务器连接至数据库管理系统 (DBMS) 时使用的身份验证模式。

您可以根据所选 DBMS 从以下身份验证模式中进行选择：

- 对于 SQL Express 或 Microsoft SQL Server，请选择以下选项之一：
  - **Microsoft Windows 身份验证模式**。使用启动管理服务器的用户来验证权限。
  - **SQL Server 身份验证模式**。如果选择此选项，则会使用在窗口中指定的账户来验证访问权限。填写**账户**和 **密码** 字段。

    要查看输入的密码，单击并按住"**显示**"按钮。

对于两个身份验证模式，应用程序检查数据库是否可用。如果数据库不可用，则显示错误消息，且您必须提供正确的凭证。

如果管理服务器数据库存储在另外一台设备上，并且管理服务器账户无法访问该数据库服务器，则在安装或升级管理服务器时必须使用 SQL Server 身份验证模式。可能发生这种情况的情形为：存储数据库的设备在域之外，或管理服务器已安装在 LocalSystem 账户之下。

对于 MySQL、MariaDB、PostgreSQL 或 Postgres Pro，请指定账户和密码。

步骤 13：选择账户以启动管理服务器

选择用于启动管理服务器作为服务的账户。

- **自动生成账户**。应用程序创建名为 KL-AK-* 的账户，kladminserver 服务在该账户下运行。

  如果您计划将共享文件夹和 DBMS 放置在管理服务器所在设备。

- **选择账户**。管理服务器服务(kladminserver)将在您选择的账户下运行。

  例如，如果您计划使用其他设备上任意版本的 SQL Server 实例（包括 SQL Express）作为 DBMS，且/或您计划查找其他设备上的共享文件夹，您必须选择域账户。

  Kaspersky Security Center 支持受管理服务账户 (MSA) 和受管理服务账户组 (gMSA)。如果这些账户类型在您的域中被使用，您可以选择它们之一作为管理服务器服务账户。

  在指定 MSA 或 gMSA 之前，必须在将要安装管理服务器的同一设备上安装该账户。如果尚未安装该账户，则取消管理服务器安装，安装该账户，然后重新启动管理服务器安装。关于在本地设备上安装受管服务账户的详细信息，请参阅正式的 Microsoft 文档。

  要指定 MSA 或 gMSA：

  1. 单击“**浏览**”按钮。
  2. 在打开的窗口中，单击**对象类型**按钮。
  3. 选择“**服务账户**”类型并单击“**确定**”。
  4. 选择相关账户并点击**确定**。

您选择的账户必须有不同的权限，取决于您计划使用的 DBMS。

出于安全原因，请不要分配权限状态到您运行管理服务器的账户。

管理服务器账户今后不能更改。您需要重新安装故障转移集群以使用另一个管理服务器账户。

步骤 14：选择账户以运行 Kaspersky Security Center 服务

在设备上选择即将运行 Kaspersky Security Center 服务的账户:

- **自动生成账户**。Kaspersky Security Center 在 kladmins 组的设备上创建名为 KlScSvc 的本地账户。Kaspersky Security Center 服务将在已创建的账户下运行。
- **选择账户**。Kaspersky Security Center 服务将运行在您选择的账户下。

  您将必须选择域账户，如果您要保存报告到不同设备的文件夹，或基于您组织的安全策略。如果您安装管理服务器到失败转移集群，您也可能必须选择域账户。

出于安全原因，请不要分配权限状态到您运行服务的账户。

KSN 代理服务 (ksnproxy)、卡巴斯基激活代理服务器服务 (klactprx) 和卡巴斯基身份验证门户服务 (klwebsrv) 将在所选账户下运行。

步骤 15：选择共享文件夹

定义执行以下操作时将使用的共享文件夹的位置和名称：

- 存储远程安装程序所需的文件（这些文件会在创建安装包过程中复制到管理服务器）。
- 将从更新源下载的更新存储到管理服务器。

系统将为所有用户启用文件共享（只读）。

您可以选择以下两个选项之一：

- **创建共享文件夹**。创建新文件夹。在文本框中，指定文件夹路径。
- **选择现有共享文件夹**。选择一个已有的共享文件夹。

共享文件夹可以是正在安装程序的设备上的本地文件夹，也可以是企业网络中任何客户端设备上的远程目录。您可以单击“**浏览**”按钮选择共享文件夹，也可以在相应的字段中输入共享文件夹的 UNC 路径（例如，\\server\Share）手动指定。

默认情况下，安装程序将在为 Kaspersky Security Center 组件选择的安装文件夹中创建一个名为 KLSHARE 的本地子文件夹。

您稍后可以根据需要定义共享文件夹。

步骤 16：配置与管理服务器的连接

配置到管理服务器的连接：

- **端口**

  用于连接至管理服务器的端口号。
  默认端口号是 14000。

- **SSL 端口**

  用于安全地连接至管理服务器的安全套接字层 （SSL） 端口号。
  默认端口号是 13000。

- **加密密钥长度**

  选择加密密钥长度：1024 bit 或 2048 bit。

  1024 位加密密钥少量占用 CPU，但它被认为是过时的，因为由于技术说明，它无法提供可靠的加密。而且，现有硬件可能与 1024 位密钥的 SSL 证书不兼容。
  2048 位加密密钥满足所有加密标准。然而，使用 2048 位加密密钥可能增加 CPU 负载。
  默认下，**2048 bit(最大安全)**被选中。

您还可以稍后更改连接管理服务器的参数，如下所示：

- 您可以稍后在管理服务器属性的**连接端口**部分更改端口和 SSL 端口号。有关管理服务器连接端口的更多信息，请参阅Kaspersky Security Center 使用的端口。
- 使用 klsetsrvcert 实用程序更换管理服务器证书时，可以使用 `-o RsaKeyLen:<key length>` 参数来更改加密密钥长度。

步骤 17：定义管理服务器地址

指定管理服务器地址。您可以选择以下选项之一：

- **DNS 域名**。如果网络中包含 DNS 服务器并且客户端设备可以用它接收管理服务器地址，则您可以使用此方法。
- **NetBIOS 名称**。如果客户端设备使用 NetBIOS 协议接收管理服务器地址，或者网络中可使用 WINS 服务器，则您可以使用此方法。
- **IP 地址**。如果管理服务器拥有不会随后变更的静态 IP 地址，则您可以使用此方法。

步骤 18：用于连接移动设备的管理服务器地址

如果选择了安装“移动设备管理”组件，则安装向导会出现这一步。

在**移动设备连接地址**窗口中，指定管理服务器的外部地址以连接本地网络之外的移动设备。您可以指定管理服务器的 IP 地址或域名系统 (DNS)。

步骤 19：在硬盘驱动器上解压并安装文件

Kaspersky Security Center 组件的安装配置完成后，便可以开始在硬盘驱动器上安装文件。

如果安装需要其他程序，安装向导将在开始安装 Kaspersky Security Center 之前，在“**安装先决条件**”页面中通知您。所需程序将在您单击“**下一步**”按钮后自动安装。

在最后一页，您可以选择启动哪个控制台以使用 Kaspersky Security Center：

- **启动基于 MMC 的管理控制台**
- **启动 Kaspersky Security Center Web Console**

  该选项仅在您在先前步骤中选择了安装 Kaspersky Security Center Web Console 时可用。

您也可以点击**完成**以关闭向导而不使用 Kaspersky Security Center。您可以稍后随时开始使用。

在管理控制台或者 Kaspersky Security Center Web Console 第一次启动时，您可以执行应用程序初始化设置。

在静默模式下安装管理服务器

管理服务器可以在静默模式下安装，即，无需交互式输入安装设置。

要在静默模式下将管理服务器安装至本地设备：

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才使用下面的命令。
2. 阅读隐私策略。仅当您理解并同意您的数据将按照隐私策略中所述进行处理和传输（包括传输到第三方国家）后，才使用下面的命令。
3. 运行命令

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <安装参数>"
```

这里“`setup_parameters`”是一系列参数，其各自的值用空格隔开（`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`）。setup.exe 文件位于服务器文件夹，它是 Kaspersky Security Center 分发包的一部分。

下表列出了在静默模式下安装管理服务器时可用到的参数名称和可能的值。

静默模式下安装管理服务器的参数

参数名称	参数描述	可用值
EULA	是否接受授权许可协议条款。	• 1 – 我已完全阅读、理解并接受最终用户授权许可协议的条款。 • 其它值或没有值 – 我不接受授权许可协议的条款（将不会执行安装）。
PRIVACYPOLICY	是否接受隐私策略条款。	• 1 – 我了解并同意我的数据将按照《隐私策略》中的说明进行处理和传输（包括第三国家/地区）。我确认已完全阅读并理解《隐私策略》。 • 其它值或没有值 – 我不接受隐私策略的条款（将不会执行安装）。
INSTALLATIONMODETYPE	管理服务器安装类型。	• 标准 – 标准安装。 • 自定义 – 自定义安装。
INSTALLDIR	管理服务器安装文件夹的路径。	字符串值。
ADDLOCAL	要安装的管理服务器组件列表（以逗号隔开）。	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 管理服务器安装正常运行的最小组件列表： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`。
NETRANGETYPE	网络大小（网络中设备的数量）。	• NRT_1_100 - 从 1 到 100 个设备。 • NRT_100_1000 - 101 到 1000 台设备。 • NRT_GREATER_1000 - 多于 1,000 台设备。
SRV_ACCOUNT_TYPE	指定管理服务器作为服务运行时使用的账户的模式。	• SrvAccountDefault – 自动创建账户。 • SrvAccountUser – 手动指定账户。此种情况下，您必须指定 `SERVERACCOUNTNAME` 和 `SERVERACCOUNTPWD` 参数的值。
SERVERACCOUNTNAME	管理服务器作为服务运行时使用的账户的名称。如果 SRV_ACCOUNT_TYPE=SrvAccountUser，您必须为参数指定值。	字符串值。

参数名称	参数描述	可用值
SERVERACCOUNTPWD	用于启动管理服务器作为服务的账户密码。如果 SRV_ACCOUNT_TYPE=SrvAccountUser，您必须为参数指定值。	字符串值。
SERVERCER	管理服务器证书密钥长度（位）。	• 1 – 管理服务器证书的密钥长度为 2048 位。 • 未指定值 – 管理服务器证书的密钥长度 1024 位。
DBTYPE	为存储管理服务器数据库而创建的数据库类型。 此参数是必需的。	• MySQL – 将使用 MySQL 或 MariaDB 数据库。此种情况下，您必须指定 MYSQLSERVERNAME、MYSQLSERVERPORT、MYSQLDBNAME、MYSQLACCOUNTNAME 和 MYSQLACCOUNTPWD 参数的值。 • MSSQL – Microsoft SQL Server (SQL Express) 数据库将被使用。此种情况下，您必须指定 MSSQLSERVERNAME、MSSQLDBNAME 和 MSSQLAUTHTYPE 参数的值。 • POSTGRES - 将使用 PostgreSQL 或 Postgres Pro 数据库。在这种情况下，您必须指定 POSTGRESSERVERNAME、POSTGRESSERVERPORT、POSTGRESDBNAME、POSTGRESACCOUNTNAME 和 POSTGRESACCOUNTPWD 参数的值。
MYSQLSERVERNAME	SQL Server 完整名称。如果 DBTYPE=MySQL，您必须为参数指定值。	字符串值。
MYSQLSERVERPORT	连接至 SQL Server 的端口号。如果 DBTYPE=MySQL，您必须为参数指定值。	数字值。
MYSQLDBNAME	为存储管理服务器数据库而创建的数据库名称。如果 DBTYPE=MySQL，您必须为参数指定值。	字符串值。
MYSQLACCOUNTNAME	连接到数据库的账户名称。如果 DBTYPE=MySQL，您必须为参数指定值。	字符串值。
MYSQLACCOUNTPWD	连接到数据库的账户密码。如果 DBTYPE=MySQL，您必须为参数指定值。	字符串值。
MSSQLSERVERNAME	SQL Server 完整名称。如果 DBTYPE=MSSQL，您必须为该参数指定值。	字符串值。
MSSQLDBNAME	数据库名称。如果 DBTYPE=MSSQL，您必须为该参数指定值。	字符串值。
MSSQLAUTHTYPE	连接到 SQL Server 的授权类型。如果 DBTYPE=MSSQL，您必须为该参数指定值。	• Windows – Microsoft Windows 身份验证模式。 • SQLServer – SQL Server 身份验证模式。此种情况下，您必须指定 MSSQLACCOUNTNAME 和 MSSQLACCOUNTPWD 参数的值。
MSSQLACCOUNTNAME	连接至 SQL Server 的账户名称。如果 MSSQLAUTHTYPE=SQLServer，您必须为参数指定值。	字符串值。
MSSQLACCOUNTPWD	连接至 SQL Server 的账户密码。如果 MSSQLAUTHTYPE=SQLServer，您必须为参数指定值。	字符串值。
CREATE_SHARE_TYPE	指定共享文件夹的方法。	• Create—创建新共享文件夹。此种情况下，您必须指定 SHARELOCALPATH 和 SHAREFOLDERNAME 参数的值。 • ChooseExisting – 选择现有文件夹。此种情况下，您必须指定 EXISTSHAREFOLDERNAME 参数的值。
SHARELOCALPATH	本地文件夹完整路径。您必须指定参数值，如果 CREATE_SHARE_TYPE=Create	字符串值。
SHAREFOLDERNAME	共享文件夹网络名称。如果 CREATE_SHARE_TYPE=Create，您必须为参数指定值。	字符串值。
EXISTSHAREFOLDERNAME	现有共享文件夹的完整路径。 如果 CREATE_SHARE_TYPE=ChooseExisting，您必须为该参数指定值。	字符串值。
SERVERPORT	连接至管理服务器的端口号。	数字值。
SERVERSSLPORT	使用 SSL 协议加密连接到管理服务器的端口号。	数字值。

参数名称	参数描述	可用值
SERVERADDRESS	管理服务器地址。	字符串值。
MOBILESERVERADDRESS	用于连接移动设备的管理服务器地址。	字符串值。

有关管理服务器安装设置的详细描述，请参阅“自定义安装”部分。

在管理员工作站安装管理控制台

你可以在管理员工作站上单独安装管理控制台，并使用该控制台通过网络对管理服务器进行管理。

要在管理员工作站上安装管理控制台：

1. 运行 setup.exe 可执行文件。

   提示您选择要安装的 Kaspersky 程序的窗口将打开。

2. 在程序选择窗口，点击**仅安装 Kaspersky Security Center 管理控制台**链接运行管理控制台服务器安装向导。遵照向导的说明操作。

3. 选择目标文件夹。默认情况下，目标文件夹将为 <驱动器>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console。如果此文件夹不存在，则系统会在安装过程中自动创建。您可以使用“**浏览**”按钮更改目标文件夹。

4. 在安装向导的最后一页，单击“**开始**”按钮启动管理控制台的安装程序。

当向导完成后，管理控制台将被安装在管理员工作站中。

要在静默模式下在管理员工作站上安装管理控制台：

1. 阅读最终用户授权许可协议。只有在您理解并接受最终用户授权许可协议的条款后，才使用下面的命令。

2. 在 Kaspersky Security Center 分发包的 `Distrib\Console` 文件夹中，使用以下命令运行 setup.exe 文件：

   ```
   setup.exe /s /v"EULA=1"
   ```

   如果要从 `Distrib\Console\Plugins` 文件夹安装所有管理插件连同管理控制台，请运行以下命令：

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   如果要指定从 `Distrib\Console\Plugins` 文件夹安装的管理插件连同管理控制台，请在 "/p" 项后指定插件，并用分号分隔：

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   其中 `P1`、`P2`、`P3` 是与 `Distrib\Console\Plugins` 文件夹中的插件文件夹名称对应的插件名称。例如：

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

管理控制台和管理插件（如果有）将安装在管理员的工作站上。

安装好管理控制台后，您必须连接到管理服务器。为此，请运行管理控制台，然后在打开的窗口中，指定装有管理服务器的设备名称或 IP 地址，以及用于连接管理服务器的账户设置。建立与管理服务器的连接后，您就可以使用该管理控制台管理反病毒保护系统了。

您可以使用标准的 Microsoft Windows 添加/删除工具卸载管理控制台。

安装 Kaspersky Security Center 后系统的变化

管理控制台图标

在设备上安装管理控制台后，系统会显示其图标，允许您启动管理控制台。可以在“**开始**”→“**程序**”→“**Kaspersky Security Center**”菜单中找到管理控制台。

管理服务器和网络代理服务

管理服务器和网络代理将作为服务安装在设备上，其属性如下所示。该表也包含了安装管理服务器后应用于设备上的其他服务的属性。

Kaspersky Security Center 服务属性

组件	服务名称	显示服务名称	账户
管理服务器	kladminserver	Kaspersky Security Center 管理服务器	安装过程中，用户定义的或专用的 KL-AK-* 格式的账户被创建
网络代理	klnagent	Kaspersky Security Center 网络代理	本地系统
访问 Kaspersky Security Center Web Console 和管理组织内网的 Web 服务器	klwebsrv	Kaspersky 网络论坛	专用非授权 KlScSvc 账户
激活代理服务器	klactprx	Kaspersky 的激活代理服务器	专用非授权 KlScSvc 账户
KSN 代理服务器	ksnproxy	卡巴斯基安全网络代理服务器	专用非授权 KlScSvc 账户

如果您在 Kaspersky Security Center 故障转移群集节点上安装Kaspersky Security Center，klfocsvc_klfoc 服务将变得可用。klnagent_klfoc 和 klfocsvc_klfoc 服务在本地系统账户下运行。kladminserver_klfoc 服务必须在“ksc”账户下运行，其他服务在“rightless”账户下运行。必须将“ksc”和“rightless”账户添加到具有本地管理员权限的 KLAdmins 组中。为了确保 Kaspersky Security Center 正常工作，您必须仅使用“ksc”和“rightless”账户来运行服务。我们不建议使用具有相同权限的其他账户。下表包含在 Kaspersky Security Center 故障转移群集上安装管理服务器后应用在设备上的服务的属性。

安装在 Kaspersky Security Center 故障转移集群中的 Kaspersky Security Center 服务的属性

组件	服务名称	显示服务名称	账户
管理服务器	kladminserver_klfoc	Kaspersky Security Center 管理服务器	ksc
网络代理	klnagent_klfoc	Kaspersky Security Center 网络代理	本地系统
访问 Kaspersky Security Center Web Console 和管理组织内网的 Web 服务器	klwebsrv_klfoc	Kaspersky 网络论坛	无权限
激活代理服务器	klactprx_klfoc	卡巴斯基激活代理服务器	无权限
KSN 代理服务器	ksnproxy_klfoc	卡巴斯基安全网络代理服务器	无权限
Kaspersky Security Center 故障转移集群	klfocsvc_klfoc	Kaspersky Security Center 故障转移集群	本地系统

Kaspersky Security Center Web Console 服务

如果在设备上安装 Kaspersky Security Center Web Console，将部署以下服务（请参见下表）：

Kaspersky Security Center Web Console 服务

显示服务名称	账户
Kaspersky Security Center 服务 Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	网络服务
Kaspersky Security Center 产品插件服务器	NT Service/KSCWebConsolePlugin
Kaspersky Security Center Web Console 管理服务	本地系统
Kaspersky Security Center Web Console 消息队列	NT Service/KSCWebConsoleMessageQueue

网络代理服务器版本

服务器版本的网络代理将与管理服务器一起安装在设备中。服务器版本的网络代理是管理服务器的一部分，会同管理服务器一起安装和删除，并且只能与本地安装的管理服务器进行交互。配置网络代理到管理服务器的连接不是必须的步骤：配置会通过程序功能进行实施，因为这些组件已安装在同一设备中。服务器版本的网络代理会以相同的属性进行安装，以便作为标准的网络代理，并且可执行相同的应用程序管理功能。此版本由管理组（该管理组要包含管理服务器的客户端设备）的策略管理。对于服务器版本的网络代理来说，除服务器更改任务意外的所有任务均创建在管理服务器提供的范围之内。

网络代理无法被安装到已经安装了管理服务器的设备。

您可以查看管理服务器、网络代理的各项服务的属性，也可以使用标准的 Microsoft Windows 管理工具监控其操作：Computer management\Services。有关 Kaspersky 管理服务器服务活动的信息已注册，并存储在 Microsoft Windows 系统日志中，而且是在安装管理服务器的设备上的一个单独的卡巴斯基事件日志分支中。

我们建议您不要手动开始和停止服务，且不要在服务设置中修改服务账户。如果必要，您可以使用 klsrvswch 实用程序修改管理服务器服务账户。请注意，您必须使用安装管理服务器时所用的具有管理员权限的账户在管理服务器设备上启动 klsrvswch 实用程序。

用户账户和安全组

管理服务器安装程序默认创建以下账户：

- KL-AK-*：管理服务器服务账户
- KlScSvc：管理服务器轮询的其他服务账户
- KlPxeUser：操作系统部署账户

如果您在运行安装程序时为管理服务器服务和其他服务选择其他账户，指定的账户被使用。

将自动在安装管理服务器的设备上创建名为 KLAdmins 与 KLOperators 的本地安全组及各自的权限集。

不建议在域控制器上安装管理服务器；但是如果在域控制器上安装管理服务器，则必须以域管理员权限启动安装程序。在这种情况下，安装程序将自动创建名为 KLAdmins 和 KLOperators 的域安全组。如果在不是域控制器的设备上安装管理服务器，则必须以本地管理员权限启动安装程序。在这种情况下，安装程序将自动创建名为 KLAdmins 和 KLOperators 的本地安全组。

配置邮件通知时，您可能需要在邮件服务器上创建一个账户以进行 ESMTP 身份验证。

卸载程序

您可以使用标准的 Microsoft Windows 添加/删除工具卸载 Kaspersky Security Center。删除程序需要启动可以删除设备中所有应用程序组件（包括插件）的向导。该向导会使默认浏览器打开一个带有投票的网页，您可以在其中告诉我们您选择停止使用 Kaspersky Security Center 的原因。如果您未在向导的操作过程中选择删除共享文件夹 (KLSHARE)，则可以在所有相关任务完成后手动将其删除。

卸载应用程序后，它的一些文件可能保持在系统临时文件夹。

应用程序卸载任务创建向导会建议您存储管理服务器的备份副本。

当应用程序从 Microsoft Windows 7 和 Microsoft Windows 2008 中卸载时，应用程序卸载任务创建向导可能会提前终止。这可以通过禁用操作系统中的用户账户控制 (UAC) 并重新启动应用程序删除来避免。

关于升级 Kaspersky Security Center

本节包含有关如何从先前版本升级 Kaspersky Security Center 的信息。可以通过不同方式升级 Kaspersky Security Center，具体取决于 Kaspersky Security Center 是安装在“本地”还是安装在“Kaspersky Security Center 故障转移集群节点”上。

升级期间，严禁管理服务器和其他应用程序同时使用 DBMS。

请注意，如果您将管理服务器升级到版本 15.1，则无法创建网络代理版本 15 或早期版本的新安装包。但是，先前创建的安装包仍然可用。

从先前版本升级 Kaspersky Security Center 时，支持的卡巴斯基应用程序的所有已安装插件都会保留。管理服务器插件和网络代理插件会自动升级（同时适用于管理控制台和 Kaspersky Security Center Web Console）。

从先前版本升级 Kaspersky Security Center

以下主题描述了建议的升级准备步骤：升级 Kaspersky Security Center 和受管理安全应用程序。

您可以在安装了早期版本管理服务器（从版本 11 (11.0.0.1131b) 开始）的设备上安装管理服务器版本 15.1。当升级至版本 15.1 时，上一管理服务器版本的所有数据和设置都将被保留下来。

如果安装管理服务器期间出现问题，您可以使用升级前创建的管理服务器数据备份副本恢复旧版管理服务器。

如果网络中已安装至少一个新版管理服务器，则可以通过使用管理服务器安装包的远程安装任务升级网络上的其他管理服务器。

如果部署了 Kaspersky Security Center 故障转移集群，还可以在其节点上“升级 Kaspersky Security Center。

要升级早期版本的管理服务器到版本 15.1：

1. 运行版本 15.1 的 ksc_15.1_<内部版本号>_full_<语言>.exe 安装文件（您可以从卡巴斯基网站下载该文件）。
2. 在打开的窗口中，单击“**安装 Kaspersky Security Center**”链接以启动管理服务器安装向导。遵照向导的说明操作。
3. 阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款，在**我确认我已完整阅读、理解和接受**部分选择以下复选框：
   - **该 EULA 的条款和条件**
   - **描述数据处理的隐私策略**

   在您选择两个复选框后，你设备上的应用程序安装将继续。安装向导提示您创建早期版本管理服务器数据的备份。

   Kaspersky Security Center 支持从使用旧版管理服务器创建的备份中恢复数据。
4. 如果要创建管理服务器数据的备份，请在打开的“**备份管理服务器数据**”窗口中进行指定。

   备份通过 klbackup 实用程序创建。该实用程序包含在分发包中，且位于 Kaspersky Security Center 安装文件夹的根目录下。
5. 按照安装向导安装管理服务器版本 15.1。

   如果显示一条消息指示 Kaspersky Security Center Web Console 服务忙，则单击“向导”窗口中的“**忽略**”按钮。

   我们建议您避免终止安装向导。如果在管理服务器安装步骤取消升级，可能导致 Kaspersky Security Center 的升级版本失效。
6. 对于安装了早期版本网络代理的设备，请创建并运行新版本网络代理远程安装任务。

   我们建议您将 Linux 网络代理升级到与 Kaspersky Security Center 相同的版本。

   完成远程安装任务后，网络代理版本将升级。

   在基于 Linux 的资产上运行以下命令以删除不再需要的依赖项：
   - 对于基于 Debian 的资产，运行以下命令之一：
     - `apt-get -y autoremove`
     - `apt -y autoremove`

- 对于基于 RPM 的资产，运行以下命令之一：
  - `dnf autoremove`
  - `yum autoremove`

在 Kaspersky Security Center 故障转移集群节点上升级 Kaspersky Security Center

可以在安装了较早版本的管理服务器（从版本 13.2 开始）的每个 Kaspersky Security Center 故障转移群集节点上安装管理服务器版本 15.1。当升级至版本 15.1 时，上一管理服务器版本的所有数据和设置都将被保留下来。

如果之前在本地设备上安装 Kaspersky Security Center，则还可以在这些设备上升级 Kaspersky Security Center。

要在 Kaspersky Security Center 故障转移集群节点上升级 Kaspersky Security Center：

1. 在集群的活动节点上执行以下操作：
   a. 运行 ksc_15.1_<build number>_full_<language>.exe 可执行文件。

   将打开一个窗口，提示您选择要更新的卡巴斯基应用程序。单击“**安装 Kaspersky Security Center 管理服务器**”链接以启动管理服务器安装向导。按照向导的说明进行操作。

   b. 阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款，在**我确认我已完整阅读、理解和接受**部分选择以下复选框：
      - **该 EULA 的条款和条件**
      - **描述数据处理的隐私策略**

   选中两个复选框以继续安装。

   如果不接受授权许可协议或隐私政策，请单击“**取消**”按钮取消升级。
2. 在 Kaspersky Security Center 故障转移群集的被动节点上执行与主动节点相同的操作。
3. 启动集群。

这样，您就在 Kaspersky Security Center 故障转移集群节点上安装了最新版本的管理服务器。

在 Microsoft 故障转移集群节点上升级 Kaspersky Security Center

可以在安装了较早版本的管理服务器（从版本 13.2 开始）的每个 Microsoft 故障转移群集节点上升级管理服务器版本 15.1。当升级至版本 15.1 时，上一管理服务器版本的所有数据和设置都将被保留下来。

若要在 Microsoft 故障转移集群节点上升级 Kaspersky Security Center，请在集群的任何节点上执行以下操作：

1. 运行 ksc_15.1_<build number>_full_<language>.exe 可执行文件。

   将打开一个窗口，提示您选择要更新的卡巴斯基应用程序。单击"**安装 Kaspersky Security Center 管理服务器**"链接以启动管理服务器安装向导。按照向导的说明进行操作。

2. 阅读授权许可协议和隐私策略。如果您同意授权许可协议和隐私策略的所有条款，在**我确认我已完整阅读、理解和接受**部分选择以下复选框：

   - **该 EULA 的条款和条件**
   - **描述数据处理的隐私策略**

   选中两个复选框以继续安装。

   如果不接受授权许可协议或隐私政策，请单击"**取消**"按钮取消升级。

3. 在**集群上的安装类型**窗口中，选择**集群（安装在所有集群节点上）**。

   接下来，安装程序将在集群的所有节点上配置并完成管理服务器的升级。升级期间，无法更改管理服务器设置。

这样，您就在 Microsoft 故障转移集群节点上安装了最新版本的管理服务器。

Kaspersky Security Center 的初始化配置

本部分介绍了在安装 Kaspersky Security Center 后必须执行的步骤以执行其初始设置。

强化指南

强化指南专为安装管理 Kaspersky Security Center 的专业人员，以及为使用 Kaspersky Security Center 的企业提供技术支持的人员而设计。

强化指南描述了配置 Kaspersky Security Center 及其组件的建议和功能，旨在降低其危害的风险。

配置之前，请使用管理服务器数据备份任务或 klbackup 实用程序创建 Kaspersky Security Center 管理服务器备份副本并将其保存在安全位置。

强化指南包括以下信息：

- 选择管理服务器架构
- 配置与管理服务器的安全连接
- 配置访问管理服务器的账户
- 管理管理服务器和客户端设备的保护
- 配置受管理应用程序的保护

- 管理服务器维护
- 将信息传输到第三方应用程序

在您开始使用管理服务器之前，Kaspersky Security Center 会提示您阅读强化指南的简要版本。

请注意，在您确认已阅读强化指南之前，您不能使用管理服务器。

要阅读强化指南：

1. 打开管理控制台或 Kaspersky Security Center Web Console 并登录控制台。控制台将检查您是否确认阅读了当前版本的强化指南。

   如果您尚未阅读强化指南，一个窗口会打开并显示它的简要版本。

2. 执行以下操作之一：

   - 如果要以文本文档形式查看强化指南的简要版本，请单击“**在新窗口中打开**”链接。
   - 如果您想查看强化指南完整版，请单击“**打开在线帮助中的强化指南**”链接。

3. 阅读强化指南后，选择“**我确认我已完全阅读并理解强化指南**”复选框，然后单击“**接受**”按钮。

现在，您可以使用管理服务器。

当新版本的强化指南出现时，Kaspersky Security Center 将提示您阅读它。

管理服务器快速启动向导

该部分提供了管理服务器快速启动向导的信息。

关于快速启动向导

该部分提供了管理服务器快速启动向导的信息。

管理服务器快速启动向导允许您创建最少的必要任务和策略，调整最少的设置，下载和安装受管理 Kaspersky 应用程序的插件以及创建受管理 Kaspersky 应用程序的安装包。当向导运行时，您可以对应用程序做以下更改：

- 下载并安装受管理应用程序的插件。快速启动向导完成后，已安装的管理插件列表将显示在管理服务器属性窗口的**高级 → 有关已安装应用程序管理插件的详情**区域。
- 创建受管理 Kaspersky 应用程序的安装包。快速启动向导完成后，Network Agent for Windows 和受管理 Kaspersky 应用程序的安装包将显示在“**管理服务器**”→“**高级**”→“**远程安装**”→“**安装包**”列表中。
- 添加可自动分发至管理组内的设备的密钥文件或激活码。快速启动向导完成后，有关授权许可密钥的信息将显示在“**管理服务器**”→“**卡巴斯基授权许可**”列表以及管理服务器属性窗口的“**授权许可密钥**”区域中。
- 配置与卡巴斯基安全网络 (KSN) 的交互。

- 为管理服务器和受管理应用程序的操作事件通知设置邮件传送配置（成功的通知传送需要消息服务在管理服务器和所有接收端设备上运行）。快速启动向导完成后，电子邮件通知设置将显示在管理服务器属性窗口的“**通知**”区域。

- 调整设备上安装的应用程序的更新设置和漏洞修复设置。

- 为工作站和服务器创建保护策略，以及为受管理设备的顶级层级创建恶意软件扫描任务、更新下载任务和数据备份任务。快速启动向导完成后，创建的任务将显示在“**管理服务器**”→“**任务**”列表中，与受管理应用程序的插件相对应的策略将显示在“**管理服务器**”→“**策略**”列表中。

快速启动向导会为受管理应用程序（例如 Kaspersky Endpoint Security for Windows）创建策略，除非已经为**受管理设备**组创建了此类策略。如果**受管理设备**组不存在具有相同名称的任务，则快速启动向导将创建任务。

在管理控制台中，Kaspersky Security Center 首次启动后，会自动提示您运行快速启动向导。您还可以在任意时刻手动启动快速启动向导。

开始管理服务器快速启动向导

在安装管理服务器后，在第一次连接时，应用程序自动提示您运行快速启动向导。您还可以在任意时刻手动启动快速启动向导。

要手动启动快速启动向导：

1. 在控制台树中，选择**管理服务器**节点。

2. 从节点的上下文菜单中，选择“**所有任务**” → “**管理服务器快速启动向导**”。

   向导提示您执行管理服务器初始化配置。遵照向导的说明操作。

如果再次启动“快速启动向导”，则上次运行向导时创建的任务和策略无法再次创建。

步骤 1：配置代理服务器

指定管理服务器的互联网连接设置。您必须配置互联网连接才能使用卡巴斯基安全网络和为 Kaspersky Security Center 及受管理的卡巴斯基应用程序下载反病毒数据库更新。

如果您要在连接到互联网时使用代理服务器，请选择“**使用代理服务器**”选项。如果选择此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

- **地址**

  Kaspersky Security Center 用于连接到互联网的代理服务器地址。

- **端口号**

  将建立 Kaspersky Security Center 代理服务器连接的端口号。

- **对本地地址不使用代理服务器**

  将不会使用代理服务器连接本地网络的设备。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  如果选中“**使用代理服务器**”复选框，则该输入字段可用。

- **用户名**

  用于与代理服务器建立连接的用户账户（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

- **密码**

  建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

  要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

您可以稍后从快速启动向导单独配置互联网访问。

步骤 2：选择应用程序激活方法

选择以下 Kaspersky Security Center 激活选项之一：

- **通过插入您的激活码**

  *激活码*是一串由20个字符数字组成的唯一序列。您可以输入激活码来添加一个密钥来激活 Kaspersky Security Center。购买 Kaspersky Security Center 后，您将通过您指定的电子邮件地址收到激活码。

  若要使用激活码激活应用程序，您需要互联网来建立与 Kaspersky 激活服务器的连接。

  如果选择了此激活选项，则可以启用“**自动分发授权许可密钥到受管理设备**”选项。

  如果启用此选项，授权许可密钥将自动部署到受管理设备。

  如果禁用此选项，则可以稍后在管理控制台树的“**Kaspersky 授权许可**”节点中将授权许可密钥部署到受管理设备。

  如果由于某种原因，输入激活码激活未成功，您可以通过指定密钥文件来激活应用程序。

- **通过指定密钥文件**

  *密钥文件*是 Kaspersky 提供的 .key 扩展名的文件。密钥文件被用来激活应用程序。

  密钥文件的获取方法请参见以下章节：关于密钥文件。

  若使用密钥文件激活程序，您无需连接至 Kaspersky 激活服务器。

  如果选择了此激活选项，则可以启用“**自动分发授权许可密钥到受管理设备**”选项。

  如果启用此选项，授权许可密钥将自动部署到受管理设备。

  如果禁用此选项，则可以稍后在管理控制台树的“**Kaspersky 授权许可**”节点中将授权许可密钥部署到受管理设备。

- **通过高推迟应用程序激活**

  应用程序将使用基本功能操作，没有移动设备管理也没有漏洞和补丁管理。

如果您选择延迟应用程序激活，您可以稍后在任意时刻添加授权许可密钥。

步骤 3：选择保护范围和操作系统

选择网络中正在使用的保护区域和操作系统。选择这些选项时，将为 Kaspersky 服务器上的应用程序管理插件和分发包指定过滤器，您可以下载这些插件和分发包以将其安装在网络中的客户端设备上。选择选项：

- **范围**

  您可以选择以下保护区域：

  - **工作站**。如果要保护网络中的工作站，请选择此选项。默认情况下选定“工作站”选项。
  - **文件服务器和存储**。如果要保护网络中的文件服务器，请选择此选项。
  - **移动设备**。如果要保护公司或公司员工拥有的移动设备，请选择此选项。如果选择此选项，但未提供具有移动设备管理功能的授权许可，则会显示一条消息，通知您需要提供具有移动设备管理功能的授权许可。如果您不提供授权许可，则不能使用移动设备功能。
  - **虚拟化**。如果要保护网络中的虚拟机，请选择此选项。
  - **Kaspersky 反垃圾邮件**。如果要保护组织中的邮件服务器免受垃圾邮件、欺诈和恶意软件的侵扰，请选择此选项。

- **操作系统**

  您可以选择以下平台：

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - 其他

  有关受支持的操作系统的信息，请参阅硬件和软件要求。

您可以稍后从可用包列表中选择卡巴斯基应用程序包，是从快速启动向导单独配置。为了简化对所需包的搜索，您可以通过以下标准筛选可用包列表：

- 保护区域
- 已下载软件的类型（分发包、实用程序、插件或 Web 插件）
- 卡巴斯基应用程序的版本

- 卡巴斯基应用程序的本地化语言

步骤 4：选择受管理应用程序的插件

选择要安装的受管理应用程序插件。将显示位于 Kaspersky 服务器上的插件列表。该列表根据在向导的上一步中选择的选项进行筛选。默认情况下，完整列表包括所有语言的插件。要仅显示特定语言的插件，请从“**显示管理控制台本地化语言或**”下拉列表选择语言。插件列表包括以下多列：

- **应用程序名称**

  将根据您在上一步中选择的保护区域和平台来选择插件。

- **应用程序版本**

  该列表包括 Kaspersky 服务器上所有版本的插件。默认情况下，将选择最新版本的插件。

- **本地化语言**

  默认情况下，插件的本地化语言由您在安装 Kaspersky Security Center 时选择的语言来定义。您可以在“**显示管理控制台本地化语言或**”下拉列表中指定其他语言。

选择插件后，它们的安装将在单独的窗口中自动启动。要安装某些插件，您必须接受 EULA 条款。阅读 EULA 文本，选择“**我接受授权许可协议的条款**”选项，然后单击“**安装**”按钮。如果您不接受 EULA 条款，则不会安装该插件。

安装完成后，关闭安装窗口。

您也可以稍后选择管理插件，是从快速启动向导单独配置。

步骤 5：下载分发包并创建安装包

Kaspersky Endpoint Security for Windows 包括用于存储在客户端设备上的信息的加密工具。要下载可满足组织需求的有效 Kaspersky Endpoint Security for Windows 分发包，请参考组织的客户端设备所在国家/地区的法律。

在“**加密类型**”窗口，选择以下加密类型之一：

- 强加密 (AES256)。此加密类型使用 256 位密钥长度。
- 简单加密 (AES56)。此加密类型使用 56 位密钥长度。

只有选择“**工作站**”作为保护范围并选择“**Microsoft Windows**”作为平台时，才显示“**加密类型**”窗口。

选择加密类型之后，将显示这两种加密类型的分发包列表。列表中选中了具有所选加密类型的分发包。分发包语言与 Kaspersky Security Center 语言相对应。如果不存在与 Kaspersky Security Center 语言对应的 Kaspersky Endpoint Security for Windows 分发包，则选择英语分发包。

在列表中，您可以通过“**显示管理控制台本地化语言或**”下拉列表来选择分发包语言。

受管理应用程序的分发可能需要安装 Kaspersky Security Center 的特定最低版本。

在列表中，您可以选择与“**加密类型**”窗口中选择的分发包不同的任何加密类型的分发包。选择 Kaspersky Endpoint Security for Windows 的分发包后，将开始下载与组件和平台相对应的分发包。您可以在“**下载状态**”列中监控下载进度。快速启动向导完成后，Network Agent for Windows 和受管理 Kaspersky 应用程序的安装包将显示在“**管理服务器**”→“**高级**”→“**远程安装**”→“**安装包**”列表中。

要完成某些分发包的下载，您必须接受 EULA。当您单击“**接受**”按钮时，将显示 EULA 文本。要继续进行向导的下一步，您必须接受 EULA 的条款和条件以及 Kaspersky 隐私策略的条款和条件。选中与 EULA 和 Kaspersky 隐私策略有关的选项，然后单击“**全部接受**”按钮。如果您不接受条款和条件，则将取消分发包的下载。

在您接受 EULA 的条款和条件以及 Kaspersky 隐私策略的条款和条件之后，将继续下载分发包。下载完成后，将显示“**已创建安装包**”状态。稍后，您可以使用安装包在客户端设备上部署 Kaspersky 应用程序。

您可以手动创建安装包，单独从快速启动向导执行。转到管理控制台树中的**管理服务器→高级→远程安装→ 安装包**。

步骤 6：配置卡巴斯基安全网络使用

您可以获得卡巴斯基安全网络中信誉数据库的访问权限，以确保在遇到威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的效力并降低误报的风险。

阅读显示在窗口中的 KSN 声明。指定设置以转发 Kaspersky Security Center 操作信息到卡巴斯基安全网络知识库。您可以选择以下选项之一：

- **我同意使用卡巴斯基安全网络**

  安装在客户端设备上的 Kaspersky Security Center 和受管理应用程序将自动将其操作详情传输到卡巴斯基安全网络。参与卡巴斯基安全网络确保了包含病毒和其他威胁的数据库的快速更新，该数据库确保了对紧急安全威胁的快速响应。

- **我不同意使用卡巴斯基安全网络**

  Kaspersky Security Center 和受管理应用程序将不向卡巴斯基安全网络提供任何信息。

  如果选择此选项，则将禁用卡巴斯基安全网络。

如果您下载了 Kaspersky Endpoint Security for Windows 插件，则会显示两个 KSN 声明 - Kaspersky Security Center 的 KSN 声明和 Kaspersky Endpoint Security for Windows 的 KSN 声明。其插件已被下载的其他受管理 Kaspersky 应用程序的 KSN 声明显示在单独的窗口中，您必须分别接受（或不接受）每个声明。

您也可以稍后在管理控制台的管理服务器属性窗口中设置管理服务器到卡巴斯基安全网络 (KSN) 的访问。

步骤 7：配置邮件通知

配置如何发送 Kaspersky 应用程序在受管理设备上操作期间所记录的事件的相关通知。这些设置用作管理服务器的默认设置。

要配置发生在 Kaspersky 应用程序上的事件的通知传送，使用以下设置：

- **收件人(电子邮件地址)**

  应用程序将给其发送通知的用户的邮件地址。您可以输入一个或更多地址；如果您输入多个地址，使用分号分隔。

- **SMTP 服务器**

  您组织邮件服务器的地址。

  如果您输入多个地址，使用分号分隔。您可以使用下列值：

  - IPv4 或 IPv6 地址
  - 设备的 Windows 网络名称（NetBIOS 名称）
  - SMTP 服务器的 DNS 名称

- **SMTP 服务器端口**

  SMTP 服务器的通信端口号。如果您使用多个 SMTP 服务器，则通过指定的通信端口与它们建立连接。默认端口号是 25。

- **使用 ESMTP 身份验证**

  启用 ESMTP 身份验证支持。当选择了该复选框时，您可以在“**用户名**”和“**密码**”字段指定 ESMTP 身份验证设置。默认情况下已清除该选框。

- **设置**

  指定下列设置：

  - **主题**（电子邮件的主题）
  - **发件人电子邮件地址**
  - **SMTP 服务器的 TLS 设置**

  您可以为 SMTP 服务器指定 TLS 设置：

  您可以禁用 TLS，如果 SMTP 服务器支持 TLS，则使用此协议，您也可以强制仅使用 TLS。如果您选择仅使用 TLS，请指定用于 SMTP 服务器身份验证的证书，并选择是要允许通过任何版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，如果选择仅使用 TLS，还可以为 SMTP 服务器上的客户端身份验证指定证书。

  - 浏览 SMTP 服务器证书文件：

  您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

  - 浏览客户端证书文件：

您可以使用从任何来源（例如，从任何受信任证书颁发机构）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

- X-509 证书：

  指定带有证书的文件和带有私钥的文件。您可以按任何顺序上传这些文件。上传这两个文件时，必须指定用于解码私钥的密码。如果私钥未加密，则密码可以为空值。

- pkcs12容器：

  您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

您可以通过单击“**发送测试消息**”按钮测试新邮件通知设置。

您也可以稍后独立于快速启动向导配置事件通知。

步骤 8：配置更新管理

配置管理客户端设备上安装的更新的设置。

仅当您提供带有漏洞和补丁管理选项的授权许可密钥时，才能配置这些设置。

在设置的“**搜索并安装更新**”组中，您可以选择 Kaspersky Security Center 更新搜索和安装的模式：

- **搜索所需更新**

  如果您没有*查找漏洞和所需更新*任务，系统会自动创建该任务。
  默认情况下已选中该选项。

- **查找并安装所需更新**

  如果没有“*查找漏洞和所需更新*”和“*安装所需更新并修复漏洞*”任务，它们会自动创建。

在设置的“**Windows Server Update Services**”组中，您可以选择更新同步来源：

- **使用域策略中定义的更新源**

  客户端设备将根据域策略设置下载 Windows Update 更新。如果没有网络代理策略，它会自动创建。

- **使用管理服务器作为 WSUS 服务器**

  客户端设备将从管理服务器下载 Windows Update 更新。如果没有“*执行 Windows 更新同步*”任务和网络代理策略，它们会自动创建。

您可以创造*查找漏洞和所需更新*和*安装所需更新并修复漏洞*任务，单独从快速启动向导执行。要将管理服务器用作 WSUS 服务器，请创建“*执行 Windows Update 同步*”任务，然后选中网络代理策略中的“**使用管理服务器作为 WSUS 服务器**”选项。

步骤 9：创建初始保护配置

“**配置初始保护**”窗口显示自动创建的策略和任务列表。创建以下策略和任务：

- Kaspersky Security Center 网络代理策略
- 之前安装了管理插件的受管理卡巴斯基应用程序的策略
- “管理服务器维护”任务
- “备份管理服务器数据”任务
- “将更新下载至管理服务器存储库”任务
- 查找漏洞和所需更新任务
- 安装更新任务

等待策略和任务完成创建，然后转到向导的下一步。

如果您已下载并安装了 Kaspersky Endpoint Security for Windows 10 Service Pack 1 以及更高版本（直到 11.0.1）的插件，则在创建策略和任务期间，将打开一个窗口，用于对 Kaspersky Endpoint Security for Windows 信任域进行初始配置。应用程序将提示您添加被 Kaspersky 验证过的供应商到信任域，以便从扫描中排除他们的应用程序以防止它们被自动阻止。您可以立即创建推荐的排除项，或稍后创建排除项列表，方法是在控制台树中选择以下项：**策略** → Kaspersky Endpoint Security 属性菜单 → **高级威胁防护** → **信任域** → **设置** → **添加**。扫描排除项列表在使用应用程序的任意时刻都可以编辑。

管理员可使用 Kaspersky Endpoint Security for Windows 中集成的工具执行信任域操作。有关如何执行操作的详细说明和加密功能的说明，请参阅 Kaspersky Endpoint Security for Windows 在线帮助。

要完成信任域的初始配置并返回向导，单击“**确定**”。

单击“**下一步**”。该按钮在所有策略和任务被创建后可用。

您还可以稍后独立于快速启动向导创建所需的任务和策略。

步骤 10：连接移动设备

如果您先前在向导设置中启用了**移动设备**保护范围，请指定受管理组织中企业移动设备的连接设置。如果您未启用**移动设备**保护范围，该步骤将跳过。

在向导的该步骤，执行以下操作：

- 配置移动设备连接端口
- 配置管理服务器身份验证
- 创建或管理证书

- 设置常规证书的发布、自动更新和加密
- 为移动设备创建移动规则

要设置移动设备连接端口：

1. 单击“**移动设备连接**”字段右侧的“**配置**”按钮。
2. 在下拉列表中，选择**配置端口**。
   此时将打开管理服务器属性窗口，显示“**附加端口**”区域。
3. 在“**附加端口**”区域，您可以指定移动设备连接设置：
   - **激活代理服务器的 SSL 端口**

     SSL 端口号，以将 Kaspersky Endpoint Security for Windows 连接到 Kaspersky 的激活服务器。
     默认端口号是 17000。
   - **为移动设备打开端口**

     移动设备连接到授权许可服务器的端口被打开。您可以在以下字段定义端口号和其他设置。
     默认情况下已启用该选项。
   - **移动设备同步端口**

     移动设备连接到管理服务器并与其交换数据的端口号。默认端口号是 13292。
     如果端口 13292 被用于其他目的，您可以分配其他端口。
   - **移动设备激活端口**

     用于将 Kaspersky Endpoint Security for Android 连接到 Kaspersky 激活服务器的端口。
     默认端口号是 17100。
   - **打开 UEFI 保护设备和 KasperskyOS 设备的端口**

     UEFI 保护设备可以连接到管理服务器。
   - **UEFI 保护设备和 KasperskyOS 设备的端口**

     如果启用了**打开 UEFI 保护设备和 KasperskyOS 设备的端口**选项，您可以更改端口号。默认端口号是 13294。
   - **Prometheus 开放端口**

     Prometheus pull 请求的端口。默认端口号是 13296。
4. 单击“**确定**”以保存更改并返回到快速启动向导。

您将必须配置管理服务器的移动设备身份验证和移动设备的管理服务器身份验证。如果您需要，您可以稍后配置身份验证，是从快速启动向导单独配置。

要配置管理服务器的移动设备身份验证：

1. 单击“**移动设备连接**”字段右侧的“**配置**”按钮。
2. 在下拉列表中，选择**配置身份验证**。

   此时将打开管理服务器属性窗口，显示“**证书**”区域。
3. 在“**管理服务器的移动设备身份验证**”设置组为移动设备选择身份验证选项，并在“**管理服务器的 UEFI 保护设备身份验证**”设置组为 UEFI 保护设备选择身份验证选项。

   当管理服务器与客户端设备交换数据时，它通过使用证书来验证。

   默认下，管理服务器使用管理服务器安装过程中创建的证书。如果您想，您可以添加新证书。

要添加新证书（可选）：

1. 选择“**其他证书**”。

   此时会显示“**浏览**”按钮。
2. 单击“**浏览**”按钮。
3. 在打开的窗口，指定证书设置：

   - **证书类型**

     在该下拉列表中，您可以选择证书类型：

     - **X.509 证书**。如果该选项被选中，您应该指定证书的私钥以及开放证书：
       - **私钥(.prk, .pem)**。在该字段，单击**浏览**按钮以 PKCS #8 (*.prk) 格式指定证书的私钥。
       - **公钥(.cer)**。在该字段，单击**浏览**按钮以 PEM (*.cer) 格式指定公钥。
     - **PKCS #12 容器**。如果您选择该选项，您可以通过单击**浏览**按钮并填充**证书文件**字段从而以 P12 或 PFX 格式指定证书。

   - 激活时间：

     - **立即**

       在您单击“**确定**”后当前证书将被新证书立即代替。

       先前连接的移动设备将不能连接到管理服务器。

     - **该时间段过期后，天**

       如果选中该选项，将生成备用证书。在指定天数后当前证书将被新证书代替。备用证书的有效日期显示在“**证书**”区域。

建议您提前计划重新发布。必须在指定期限到期之前将备用证书下载到移动设备。当前证书被新证书替换后，先前连接的没有备用证书的移动设备将不能连接到管理服务器。

4. 单击“**属性**”按钮查看选择的管理服务器证书设置。

要通过管理服务器重新发布证书：

1. 选择**通过管理服务器发布的证书**。
2. 单击“**重新发布**”按钮。
3. 在打开的窗口，指定以下设置：
   - 连接地址：
     - **使用旧连接地址**

       移动设备要连接的管理服务器地址将保持不变。

       默认情况下已选中该选项。

     - **更改连接地址到**

       如果您要让移动设备连接到其他地址，在该字段指定相关地址。

       如果移动设备连接地址被更改，必须发布新的证书。旧证书将在所连接的移动设备上不可用。先前连接的设备将不能连接到管理服务器，因此将不再可管理。

   - 激活时间：
     - **立即**

       在您单击“**确定**”后当前证书将被新证书立即代替。

       先前连接的移动设备将不能连接到管理服务器。

     - **该时间段过期后，天**

       如果选中该选项，将生成备用证书。在指定天数后当前证书将被新证书代替。备用证书的有效日期显示在“**证书**”区域。

       建议您提前计划重新发布。必须在指定期限到期之前将备用证书下载到移动设备。当前证书被新证书替换后，先前连接的没有备用证书的移动设备将不能连接到管理服务器。

4. 单击“**确定**”以保存更改并返回到“**证书**”窗口。
5. 单击“**确定**”以保存更改并返回到快速启动向导。

要设置用于由管理服务器识别移动设备的常规类型证书的发布、自动更新和加密：

1. 单击“**移动设备身份验证**”字段右侧的“**配置**”按钮。

   此时将打开“**证书发布规则**”窗口，显示“**移动证书发布**”区域。

2. 如果必要，在“**发布设置**”区域指定以下设置：

- **证书生命周期，天**

  证书生命周期（天）。默认的证书生命周期是 365 天。此时间段过期后，移动设备将不能连接到管理服务器。

- **证书源**

  为移动设备选择常规类型源：证书由管理服务器发布，或被手动指定。

  如果已在“**与 PKI 整合**”区域中配置了与公共密钥基础架构 (PKI) 的集成，则可以修改证书模板。此种情况下，以下模板分类字段可用：

- **默认模板**

  使用由外部证书源发布的证书 – 证书中心 – 在默认模板下。

  默认情况下已选定该选项。

- **其他模板**

  选择用于发布证书的模板。您可在该域中指定证书模板。“**刷新列表**”按钮可更新证书模板的列表。

3. 如果必要，在“**自动更新设置**”区域为证书的自动发布指定以下设置：

- **当证书剩余此天数时续费**

  当前证书到期前管理服务器应当发布新证书的剩余天数。例如，如果字段值为 4，管理服务器会在当前证书到期的前 4 天发布新的证书。默认值是 7。

- **如果可能，自动重新发布证书**

  选择此选项可为**当证书剩余此天数时续费**字段中指定的天数自动重新颁发证书。如果证书是手动定义的，则无法自动续订，并且启用的选项将不起作用。

  默认情况下已禁用该选项。

  证书由认证中心自动重新发布。

4. 如果必要，在“**密码保护**”设置区域，指定在安装过程中解密证书的设置。

   选择“**在证书安装过程中提示密码**”选项以在证书被安装到移动设备上时提示用户输入密码。密码仅用一次 – 在安装证书到移动设备时。

   证书将通过管理服务器自动生成并发送到您指定的电子邮件地址。您可以指定用户的电子邮件地址，或您自己的电子邮件地址，如果您要使用其他方法转发密码到用户。

   您可以使用滚动条在证书解密密码中指定字符数。

   需要密码提示选项，例如，以在独立 Kaspersky Endpoint Security for Android 安装包中保护共享证书。密码保护将防止入侵者通过从 Kaspersky Security Center Web Server 窃取独立安装包获取到共享证书的访问。

   如果禁用此选项，证书在安装过程中被自动解密，且用户不被提示密码。默认情况下已禁用该选项。

5. 单击“**确定**”以保存更改并返回到快速启动向导窗口。

   单击“**取消**”按钮返回快速启动向导而不保存任何更改。

要启用移动移动设备到您选择的管理组的功能，

在“**移动设备自动移动**”字段中，选择“**为移动设备创建移动规则**”选项。

如果选择了“**为移动设备创建移动规则**”选项，应用程序自动创建移动规则以移动运行 Android 和 iOS 的设备到“**受管理设备**”组：

- 安装了 Kaspersky Endpoint Security for Android 和移动证书的 Android 操作系统
- 安装了 iOS MDM 配置文件（带有共享证书）的 iOS 操作系统

如果此规则已经存在，应用程序不再创建它。

默认情况下已禁用该选项。

Kaspersky 不再支持 Kaspersky Safe Browser。

步骤 11：下载更新

Kaspersky Security Center 和受管理的 Kaspersky 应用程序的反病毒数据库更新会自动下载。这些更新是从 Kaspersky 服务器下载的。

要从快速启动向导单独下载更新，请创建和配置 *“将更新下载至管理服务器存储库”*任务。

步骤 12：设备发现

“**网络轮询**”窗口显示由管理服务器执行的网络轮询状态的信息。

您可以查看由管理服务器检测到的网络设备并通过点击窗口下部的链接接收关于“**设备发现**”窗口的帮助。

您可以稍后从快速启动向导单独轮询您的网络。使用管理控制台配置 Windows 域、Active Directory、IP 范围和 IPv6 网络轮询。

步骤 13：关闭快速启动向导

在快速启动向导完成窗口，如果您想自动安装反病毒应用程序和/或网络代理到您网络中的设备，请选择“**运行远程安装向导**”选项。

要完成向导，请单击**完成**按钮。

配置管理控制台与管理服务器的连接

管理控制台通过 SSL 端口 TCP 13291 连接到管理服务器。klakaut 自动化对象可以使用同一端口。

端口 TCP 14000 仅可以用于连接管理控制台、分发点、从属管理服务器和 klakaut 自动化对象，以及用于从客户端设备接收数据。

通常 SSL 端口 TCP 13000 仅可以被网络代理、从属管理服务器和 DMZ 中的主管理服务器使用。在一些情况下，管理控制台可能需要通过 SSL 端口 13000 连接：

- 如果单个 SSL 端口被用于“管理控制台”和其他活动（从客户端设备接收数据、连接分发点、连接从属管理服务器）。
- 如果 klakaut 自动化对象未直接连接到管理服务器，而是通过 DMZ 中的分发点。

要允许通过端口 13000 的管理控制台连接：

1. 打开安装了管理服务器的设备的注册表（例如，在**开始 → 运行**菜单使用 regedit 命令）。
2. 转至以下分支：
   - 对于 32 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 对于 64 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. 对于 LP_ConsoleMustUsePort13291 (DWORD) 键，设置 00000000 值。
   该键指定的默认值是 1。
4. 重启管理服务器服务。

结果，您将可以通过端口 13000 连接管理控制台到管理服务器。

配置管理服务器的互联网连接设置

您必须配置互联网连接才能使用卡巴斯基安全网络和为 Kaspersky Security Center 及受管理的卡巴斯基应用程序下载反病毒数据库更新。

要指定管理服务器的互联网访问设置：

1. 在控制台树中，选择“**管理服务器 %s**”节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口中，转到**高级 → 配置互联网访问** 。
4. 如果您要在连接到互联网时使用代理服务器，请选择“**使用代理服务器**”选项。如果选择此选项，字段可用于输入设置。为代理服务器连接指定以下设置：
   - **地址**

     Kaspersky Security Center 用于连接到互联网的代理服务器地址。

- **端口号**

  将建立 Kaspersky Security Center 代理服务器连接的端口号。

- **对本地地址不使用代理服务器**

  将不会使用代理服务器连接本地网络的设备。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  如果选中“**使用代理服务器**”复选框，则该输入字段可用。

- **用户名**

  用于与代理服务器建立连接的用户账户（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

- **密码**

  建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

  要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

您还可以使用快速启动向导配置互联网访问。

连接漫游设备

本节介绍如何将漫游设备（即，位于主网络外部的受管理设备）连接到管理服务器。

方案：通过连接网关连接漫游设备

此方案描述了如何将位于主网络外部的受管理设备连接到管理服务器。

先决条件

该方案具有以下先决条件：

- 在组织的网络中已规划一个隔离区域 (DMZ)。
- 公司网络上已部署 Kaspersky Security Center 管理服务器。

阶段

此方案的实施分为几个阶段：

1. **选择 DMZ 中的客户端设备**

   此设备将用作连接网关。您选择的设备必须符合连接网关的要求。

2. **以连接网关角色安装网络代理**

   我们建议您使用本地安装在所选设备上安装网络代理。

   默认情况下，安装文件位于：\\<服务器名称>\KLSHARE\PkgInst\NetAgent_<版本号>

   在网络代理安装向导的“**连接网关**”窗口中，选择“**使用网络代理作为 DMZ 连接网关**”。此模式同时激活连接网关角色，并通知网络代理等待来自管理服务器的连接，而不是建立与管理服务器的连接。

   或者，您可以在 Linux 设备上安装网络代理，并将网络代理配置为连接网关，但是要注意在 Linux 设备上运行的网络代理的限制列表。

3. **在防火墙中允许与连接网关的连接**

   为确保管理服务器可以实际连接到 DMZ 中的连接网关，请在管理服务器与连接网关之间的所有防火墙中允许与 TCP 端口 13000 的连接。

   如果连接网关在互联网上没有真实 IP 地址，而是位于网络地址转换 (NAT) 后面，请配置规则以通过 NAT 转发连接。

4. **针对外部设备创建管理组**

   在“**受管理设备**”组下创建一个新组。该新组将包含外部受管理设备。

5. **将连接网关连接到管理服务器**

   您配置的连接网关正在等待来自管理服务器的连接。但是，管理服务器未在受管理设备中列出具有连接网关的设备。这是因为连接网关尚未尝试建立与管理服务器的连接。因此，您需要一个特殊程序来确保管理服务器发起与连接网关的连接。

   执行以下操作：

   1. 添加连接网关作为分发点。
   2. 将连接网关从“**未分配的设备**”组移动到您针对外部设备创建的组。

   连接网关连接并配置完毕。

6. **将外部台式设备连接到管理服务器**

   通常，外部台式设备不在周界内移动。因此，在安装网络代理时，需要将这些计算机配置为通过网关连接到管理服务器。

7. **设置外部台式设备的更新**

   如果将安全应用程序更新配置为从管理服务器下载，则外部设备将通过连接网关下载更新。这有两个缺点：

   - 这是不必要的流量，占用了公司的互联网通信通道的带宽。
   - 这不一定是获取更新的最快方法。对于外部设备来说，从 Kaspersky 更新服务器接收更新很可能更实惠、更快捷。

执行以下操作：

1. 将所有外部设备移至您先前创建的单独管理组。
2. 从更新任务中排除具有外部设备的组。
3. 针对具有外部设备的组创建单独的更新任务。

8. **将移动中的笔记本电脑连接到管理服务器**

   移动中的笔记本电脑有时在网络内部，有时在网络外部。为实现有效管理，您需要它们根据所在位置以不同方式连接到管理服务器。为了有效利用流量，它们还需要根据所在位置从不同来源接收更新。

   您需要配置针对漫游用户的规则：连接配置文件和网络位置描述。每个规则都定义了移动中的笔记本电脑必须根据所在位置连接到的管理服务器实例，以及必须从中接收更新的管理服务器实例。

方案：通过 DMZ 中的从属管理服务器连接漫游设备

如果要将位于主网络外部的受管理设备连接到管理服务器，可以使用位于隔离区 (DMZ) 中的从属管理服务器来实现。

先决条件

在您开始之前，确保您已做了如下：

- 在组织的网络中已规划一个 DMZ。
- 组织的内部网络上已部署 Kaspersky Security Center 管理服务器。

阶段

此方案的实施分为几个阶段：

1. **选择 DMZ 中的客户端设备**

   在 DMZ 中，选择将用作从属管理服务器的客户端设备。

2. **安装 Kaspersky Security Center 管理服务器**

   在此客户端设备上安装 Kaspersky Security Center 管理服务器。

3. **创建管理服务器层级**

   如果将从属管理服务器放置在 DMZ 中，则从属管理服务器必须接收来自主管理服务器的连接。为此，添加新管理服务器作为从属管理服务器，以便主管理服务器通过端口 13000 连接到从属管理服务器。当组合两个管理服务器到一个层级，确保端口 13291 在两个管理服务器上都可以访问。管理控制台通过端口 13291 连接到管理服务器。

4. **将不在办公室的受管理设备连接到从属管理服务器**

   您可以将不在办公室的设备连接到 DMZ 中的管理服务器，其连接方式与在管理服务器和位于主网络中的受管理设备之间建立连接的方式相同。不在办公室的受管理设备通过端口 13000发起连接。

关于连接漫游设备

一些受管理设备始终在主网络外部（例如，公司区域分支机构中的设备；自助服务终端、ATM 和安装在各个销售点的终端；员工家庭办公室中的设备）。一些设备不时在外围移动（例如，访问区域分支机构或客户办公室的用户的笔记本电脑）。

您仍然需要监视和管理对漫游设备的保护 - 接收这些设备的保护状态的实际信息，并确保设备上面的安全应用程序为最新。这是非常必要的，例如，如果某台设备在远离主网络时被入侵，那么只要它连接到主网络，就可能成为传播威胁的平台。要将漫游设备连接到管理服务器，可以使用两种方法：

- 隔离区域 (DMZ) 中的连接网关

  查看数据流量方案：LAN 上的管理服务器、互联网上的受管理设备、正在使用的连接网关

- DMZ 中的管理服务器

  查看数据流量方案：DMZ 中的管理服务器、互联网上的受管理设备

DMZ 中的连接网关

将漫游设备连接到管理服务器的推荐方法是在组织的网络中组织一个 DMZ，并在该 DMZ 中安装连接网关。外部设备将连接到连接网关，网络内部的管理服务器将通过连接网关发起与设备的连接。

与其他方法相比，此方法更安全：

- 您不需要开放从网络外部访问管理服务器的权限。
- 遭到入侵的连接网关不会对网络设备的安全性构成高风险。连接网关本身实际不进行任何管理，也不建立任何连接。

而且，连接网关不需要很多硬件资源。

但是，此方法的配置过程更复杂：

- 要将设备用作 DMZ 中的连接网关，您需要安装网络代理并以特定方式将其连接到管理服务器。
- 不能在所有情况下都使用同一个地址连接到管理服务器。在外围，不仅需要使用不同的地址（连接网关地址），还需要不同的连接模式：通过连接网关。
- 还需要为不同位置的笔记本电脑定义不同的连接设置。

要将连接网关添加到先前配置的网络：

1. 以连接网关模式安装网络代理。
2. 在要连接到新添加的连接网关的设备上重新安装网络代理。

DMZ 中的管理服务器

另一种方法是在 DMZ 中安装一个管理服务器。

此配置不如其他方法安全。在这种情况下，要管理外部笔记本电脑，管理服务器必须接受来自互联网上任何地址的连接。它仍然将管理内部网络中的所有设备，但是从 DMZ 进行管理。因此，被入侵的服务器可能造成巨大损失，尽管发生此类事件的可能性很低。

如果 DMZ 中的管理服务器不管理内部网络中的设备，则风险将大大降低。例如，服务提供商可以使用这种配置来管理客户的设备。

在以下情况下，您可能要使用此方法：

- 如果您熟悉安装和配置管理服务器，并且不想执行其他程序来安装和配置连接网关。
- 如果您需要管理更多设备。管理服务器的最大容量为 100,000 个设备，而连接网关最多可支持 10,000 个设备。

此解决方案也可能存在困难：

- 管理服务器需要更多硬件资源，而且另外需要一个数据库。
- 设备的信息将存储在两个不相关的数据库中（网络内的管理服务器数据库和 DMZ 中的另一个数据库），这会使监控复杂化。
- 要管理所有设备，需要将管理服务器连接到一个层级中，这不仅使监控复杂化，也使管理复杂化。从属管理服务器实例给管理组的可能结构加上了限制。您必须决定如何以及将哪些任务和策略分发到从属管理服务器实例。
- 配置外部设备从外部使用 DMZ 中的管理服务器以及从内部使用主管理服务器，并不比将它们配置为通过网关使用有条件连接简单。
- 高安全风险。遭到入侵的管理服务器实例使得入侵其受管理的笔记本电脑更容易。如果发生这种情况，黑客只需要等待其中一台笔记本电脑返回公司网络，即可继续对局域网进行攻击。

将外部台式设备连接到管理服务器

始终在主网络外部的台式设备（例如，公司区域分支机构中的设备；自助服务终端、ATM 和安装在各个销售点的终端；员工家庭办公室中的设备）无法直接连接到管理服务器。它们必须通过安装在隔离区域 (DMZ) 中的连接网关连接到管理服务器。在这些设备上安装网络代理时，将进行此配置。

要将外部台式设备连接到管理服务器：

1. 创建一个新的网络代理安装包。
2. 打开创建的安装包的属性，转至“**高级**”区域，然后选中“**通过使用连接网关连接到管理服务器**”选项。

   “**通过使用连接网关连接到管理服务器**”设置与“**使用网络代理作为 DMZ 连接网关**”设置不兼容。您不能同时启用这两个设置。

3. 在“**连接网关地址**”中，指定连接网关的公共地址。

   如果连接网关位于网络地址转换 (NAT) 后面并且没有自己的公用地址，请配置 NAT 网关规则以将连接从公用地址转发到连接网关的内部地址。

4. 基于已创建的安装包创建独立安装包。

5. 通过电子方式或可移动驱动器将独立安装包传送到目标设备。

6. 从独立包安装网络代理。

外部台设备机即连接到管理服务器。

关于漫游用户的连接配置文件

便携式电脑（也叫“设备”）的漫游用户需要更改连接到管理服务器的方法或者根据当前设备在企业网络中的位置在管理服务器之间进行切换。

连接配置文件仅支持运行 Windows 和 macOS 的设备。

使用单一管理服务器的不同地址

网络代理设备从组织网络或内部网可以连接到管理服务器。该情况可能需要网络代理使用不同的地址以连接到管理服务器：对于互联网连接的外部管理服务器地址和对于内部网络连接的内部管理服务器地址。

为此，您必须添加配置文件(为了从互联网连接到管理服务器)到网络代理策略。在策略属性中添加配置文件（**连接**区域，**连接配置文件**子区域）。在配置文件创建窗口，您必须禁用“**仅用来接收更新**”选项，并选择“**与此配置文件中指定的管理服务器设置同步连接设置**”选项。如果您使用连接网关访问管理服务器（例如，在“互联网访问：DMZ 中作为连接网关的网络代理”部分描述的 Kaspersky Security Center 配置中），您必须在连接配置文件的对应字段指定连接网关地址。

根据当前网络在管理服务器之间进行切换

如果组织有带有多个管理服务器的多个办公室，并且一些网络代理设备在期间进行移动，您需要网络代理连接到设备所在的本地网络中的管理服务器。

此种情况下，您必须为每个办公室在网络代理策略属性中创建连接管理服务器的配置文件，除了原始归属管理服务器所在的主办公室。您必须在连接配置文件中指定管理服务器地址并启用或禁用“**仅用来接收更新**”选项：

- 在使用本地服务器下载更新时，如果您需要网络代理与归属管理服务器同步，则选择该选项。
- 如果网络代理必须被本地管理服务器完全管理，则禁用此选项。

此后，您必须设置切换到新创建的配置文件的条件：每个办公室至少一个条件，除了归属办公室。每个条件的目的包括办公室网络环境条目的检测。如果条件是真，对应配置文件被激活。如果没有条件是真，网络代理切换到归属管理服务器。

为漫游用户创建连接配置文件

管理服务器连接配置文件仅在运行 Windows 和 macOS 的设备上可用。

若要为漫游用户创建网络代理连接至管理服务器的连接配置文件，请执行以下操作：

1. 在控制台树中，为您要创建配置文件以连接网络代理到管理服务器的客户端设备选择一个管理组。
2. 执行以下操作之一：
   - 如果您要为组中的所有设备创建连接配置文件，请在组工作区的“**策略**”选项卡中，选择一个网络代理策略。打开所选策略的属性窗口。
   - 如果您要为组中的设备创建连接配置文件，在组工作区的“**设备**”选项卡选择该设备，然后执行以下操作：
     a. 打开所选设备的属性窗口。
     b. 在设备属性窗口的“**应用程序**”区域中，选择网络代理。
     c. 打开网络代理属性窗口。
3. 在属性窗口的“**连接**”区域中，选择“**连接配置文件**”子区域。
4. 在“**管理服务器连接配置文件**”设置组中，单击“**添加**”按钮。
   默认下，连接配置文件列表包含<离线模式>和<归属管理服务器>配置文件。您不能编辑或删除配置文件。
   <离线模式>配置文件不指定任何服务器以连接。因此，当切换到该配置文件后，当客户端设备上安装的应用程序在漫游工作策略下运行时，网络代理不会试图连接到任何管理服务器。如果设备与网络断开连接，可以使用 <离线模式> 配置文件。
   <归属管理服务器> 配置文件用于指定在网络代理安装过程中选择的管理服务器的连接。当设备在外部网络中运行了一段时间后重新连接到管理服务器时，<归属管理服务器>配置文件被应用。
5. 在打开的“**新配置文件**”窗口中，配置连接配置文件：
   - **配置文件名称**
     在该输入字段中，您可以查看或更改连接配置文件名称。
   - **管理服务器**
     客户端设备在配置文件激活期间必须连接的管理服务器地址。
   - **端口**
     用于连接的端口号。
   - **SSL 端口**
     使用 SSL 协议时的连接端口号。
   - **使用 SSL**
     如果启用此选项，则使用 SSL 协议通过安全端口建立连接。
     默认情况下已启用该选项。我们建议您不要禁用此选项，以便您的连接保持安全。

- 单击“**配置通过代理服务器的连接**”链接以配置通过代理服务器的连接：如果您要在连接到互联网时使用代理服务器，请选择“**使用代理服务器**”选项。如果选择此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

  - **代理服务器地址**

    Kaspersky Security Center 用于连接到互联网的代理服务器地址。

  - **端口号**

    将建立 Kaspersky Security Center 代理服务器连接的端口号。

  - **代理服务器身份验证**

    如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

    如果选中“**使用代理服务器**”复选框，则该输入字段可用。

  - **用户名** （如果选中“**代理服务器身份验证**”选项，则该字段可用）

    用于与代理服务器建立连接的用户账户（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

  - **密码**（如果选中“**代理服务器身份验证**”选项，则该字段可用）

    建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

    要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

- **连接网关设置**

  通过客户端设备连接管理服务器的网关地址。

- **启用漫游模式**

  如果启用此选项，则在通过该配置文件连接的情况下，客户端设备上安装的应用程序将使用漫游模式设备的策略配置文件，以及漫游策略。如果没有为应用程序定义漫游策略，则使用激活策略。

  如果禁用此选项，则应用程序将使用已激活的策略。

  默认情况下已禁用该选项。

- **仅用来接收更新**

  如果启用此选项，则该配置文件将仅被客户端设备上安装的应用程序用来下载更新。对于其他操作，程序将使用在网络代理安装过程中定义的初始连接设置连接管理服务器。

  默认情况下已启用该选项。

- **与此配置文件中指定的管理服务器设置同步连接设置**

  如果启用此选项，网络代理将使用配置文件属性中指定的设置连接至管理服务器。

  如果禁用此选项，网络代理将使用安装期间已指定的原始设置连接至管理服务器。

  如果禁用“**仅用来接收更新**”选框，则此选项可用。

  默认情况下已禁用该选项。

6. 选择“**当管理服务器不可用时启用漫游模式**”选项，以允许在管理服务器不可用的任何连接尝试时，安装在客户端设备上的应用程序以漫游模式使用设备的策略配置文件和漫游策略。如果没有为应用程序定义漫游策略，则使用激活策略。

程序将为漫游用户创建一个用于将网络代理连接至管理服务器的配置文件。当网络代理使用此配置文件连接到管理服务器后，客户端设备上安装的应用程序将使用处于漫游模式的设备的策略或漫游策略。

关于将网络代理切换到其他管理服务器

网络代理连接至管理服务器的初始设置在安装网络代理时定义。要将网络代理切换到其他管理服务器，您可以使用切换规则。只有运行 Windows 或 macOS 的设备上安装的网络代理支持此功能。

切换规则可以在更改以下网络参数时触发：

- 默认网关地址。
- Dynamic Host Configuration Protocol (DHCP) 服务器的 IP 地址。
- 子网的 DNS 后缀。
- 网络 DNS 服务器的 IP 地址。
- Windows 域可访问性。此参数仅适用于运行 Windows 的设备。
- 子网地址和掩码。
- 网络 WINS 服务器的 IP 地址。此参数仅适用于运行 Windows 的设备。
- 客户端设备的 DNS 或 NetBIOS 名称。
- SSL 连接地址可访问性。

如果创建了将网络代理切换至其他管理服务器的规则，网络代理将以下列方式响应网络参数的更改：

- 如果网络设置符合已创建的规则之一，网络代理将连接至该规则中指定的管理服务器。如果该规则中已经启用漫游切换策略，客户端设备上的应用程序将切换至漫游策略。
- 如果未应用任何规则，网络代理将回滚至安装过程中指定的管理服务器连接默认设置。客户端设备上安装的应用程序将回滚至活动策略。
- 如果无法访问管理服务器，网络代理将使用用户漫游策略。

仅当在网络代理策略设置中启用“**当管理服务器不可用时启用漫游模式**”选项时，网络代理才会切换到漫游策略。

网络代理连接至管理服务器的设置保存在连接配置文件中。在连接配置文件中，您可以创建将客户端设备切换至漫游策略的规则，并可对配置文件进行配置，使其仅可用于下载更新。

根据网络位置创建网络代理切换规则

根据网络位置切换网络代理仅在运行 Windows 和 macOS 的设备上可用。

若要创建一个当网络设置改变时将网络代理从一个管理服务器切换至另一个的规则，请执行以下操作：

1. 在控制台树中，为要通过网络位置描述创建网络代理切换规则的设备选择一个管理组。
2. 执行以下操作之一：
   - 如果您要为组中的所有设备创建规则，请在组工作区的“**策略**”选项卡中，选择一个网络代理策略。打开所选策略的属性窗口。
   - 如果您要为从组中选择的设备创建规则，请转到组工作区，在“**设备**”选项卡选择设备，然后执行以下操作：
     a. 打开所选设备的属性窗口。
     b. 在设备属性窗口的“**应用程序**”区域中，选择网络代理。
     c. 打开网络代理属性窗口。
3. 在打开的**属性**窗口的“**连接**”区域中，选择“**连接配置文件**”子区域。
4. 在“**网络位置设置**”区域中，单击“**添加**”按钮。
5. 在打开的“**新描述**”窗口中，配置网络位置描述并切换规则。指定以下网络位置描述设置：
   - **网络位置描述名称**

     网络位置描述名称不能超过 255 字符或包含特殊字符，例如 ("*<>?\/:|).
   - **使用连接配置文件**

     在该下拉列表中，您可以指定网络代理用于连接至管理服务器的连接配置文件。该配置文件将在网络位置描述条件被满足时使用。连接配置文件包含网络代理连接到管理服务器的设置；它还定义了客户端设备切换到漫游策略的时间。配置文件仅用于下载更新。
6. 在“**切换条件**”区域，单击“**添加**”按钮创建网络位置描述条件列表。
   使用逻辑运算符 AND 可组合规则中的条件。要基于网络位置描述触发切换规则，所有的规则切换条件必须被满足。
7. 在下拉列表中，选择与客户端设备连接到的网络特征变化相对应的值：
   - **默认连接网关地址**—主要网络网关的地址已更改。
   - **DHCP 服务器地址**—网络 Dynamic Host Configuration Protocol (DHCP) 服务器的 IP 地址已更改。

- **DNS 域**—子网的 DNS 后缀已更改。
- **DNS 服务器地址**—网络 DNS 服务器的 IP 地址已更改。
- **Windows 域可访问性(仅 Windows)**—更改客户端设备连接到的 Windows 域的状态。仅对运行 Windows 的设备使用此设置。
- **子网**—可更改子网地址和掩码。
- **WINS 服务器地址(仅 Windows)** – 网络 WINS 服务器的 IP 地址已更改。仅对运行 Windows 的设备使用此设置。
- **名称可解析性** – 客户端设备的 DNS 或 NetBIOS 名称已更改。
- **SSL 连接地址可访问性** – 客户端设备可以或无法（取决于您选择的选项）与指定服务器建立 SSL 连接（名称:端口）。对于每个服务器，都可以额外指定一个 SSL 证书。在这种情况下，网络代理除了检查 SSL 连接的功能外，还会验证服务器证书。如果证书不匹配，连接将失败。连接频率为每分钟一次。

8. 在打开的窗口中，指定网络代理切换到其他管理服务器的条件值。窗口的名称取决于先前步骤中选择的值。指定切换条件的以下设置：

   - **参数值**

     在该字段中，您可以为所创建的条件添加一个或多个值。

   - **至少符合列表中的一个参数值**

     如果选中该选项，只要符合**参数值**列表中指定的任何值就会满足条件。
     默认情况下已选定该选项。

   - **不符合列表中的任意参数值**

     如果选中该选项，**参数值**列表中不存在条件的值，则满足条件。

9. 在“**新描述**”窗口，选择“**描述已启用**”选项来启用新网络位置描述的使用。

一个新的网络位置描述的切换规则将被创建；当满足其条件时，网络代理将使用此规则指定的配置文件连接至管理服务器。

系统将根据它们在列表中出现的顺序查看是否有与网络布局相匹配的网络位置描述。如果某个网络有多个匹配的描述，将使用第一个。您可以使用**向上**按钮和**向下**按钮更改列表中的规则顺序。

事件通知

该部分描述了如何选择方法传送关于客户端设备上事件的管理员通知，以及如何配置事件通知设置。

它也描述了如何使用 Eicar 测试病毒测试事件通知的分发。

配置事件通知

Kaspersky Security Center 允许您配置将客户端设备上发生的事件通知管理员的方法，并允许您配置通知：

- 电子邮件。当发生事件时，程序将向指定的电子邮件地址发送通知。您可以编辑通知文本。
- SMS。当发生事件时，程序将向指定的电话号码发送通知。您可以配置 SMS 通知以便通过邮件网关发送。
- 可执行文件。当设备上发生事件时，将在管理员工作站上启动该可执行文件。管理员可以通过该可执行文件接收已发生事件参数。

要配置客户端设备上发生的事件的通知，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。
3. 单击“**配置通知和事件导出**”链接并在下拉列表中选择“**配置通知**”值。
   这会打开**属性：事件**窗口。
4. 在“**通知**”区域，选择通知方法（通过邮件、SMS 或者运行可执行文件）并定义通知设置：

   - **电子邮件**

     “**电子邮件**”选项卡允许您配置事件的电子邮件通知。

     在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。

     在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

     - IPv4 或 IPv6 地址
     - 设备的 Windows 网络名称（NetBIOS 名称）
     - SMTP 服务器的 DNS 名称

     在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

     如果启用“**使用 DNS MX 查找**”选项，则可以将多个 IP 地址 MX 记录用于同一个 SMTP 服务器 DNS 名称。同一 DNS 名称可能有多个 MX 记录，这些记录具有不同的电子邮件接收优先级。管理服务器将尝试按 MX 记录优先级的升序向 SMTP 服务器发送电子邮件通知。默认情况下已禁用该选项。

     如果启用“**使用 DNS MX 查找**”选项但不启用 TLS 设置，建议您将服务器设备上的 DNSSEC 设置用作发送电子邮件通知的额外保护措施。

     单击“**设置**”链接以定义其他通知设置：

     - 主题名称（电子邮件的主题名称）
     - 发件人电子邮件地址
     - ESMTP 身份验证设置

如果为 SMTP 服务器启用了 ESMTP 身份验证选项，则必须指定在 SMTP 服务器上进行身份验证的账户。

- SMTP 服务器的 TLS 设置：

  - **不使用 TLS**

    如果要禁用电子邮件加密，则可以选择此选项。

  - **如果 SMTP 服务器支持，则使用 TLS**

    如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

  - **始终使用 TLS，检查服务器证书的有效性**

    如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以为 SMTP 服务器指定 TLS 设置：

- 浏览 SMTP 服务器证书文件：

您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

- 浏览客户端证书文件：

您可以使用从任何来源（例如，从任何受信任证书颁发机构）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

- X-509 证书：

您必须指定一个证书文件和一个私钥文件。这两个文件不相互依赖，文件的加载顺序也不重要。加载这两个文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

- pkcs12容器：

您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

通知消息字段包含程序发送的事件信息的标准文本。该文本包含代替参数，例如事件名称、设备名称和域名。您可以通过添加其他带有事件的更多相关详情的替代参数来编辑消息文本。替代参数列表通过点击字段右侧的按钮可用。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接可指定应用程序在指定时间段可以发送的最大通知数量。

单击“**发送测试消息**”按钮以检查是否已正确配置通知。应用程序应向您指定的电子邮件地址发送测试通知。

- SMS

SMS 选项卡允许您配置传输各种事件的 SMS 通知到手机。SMS 消息通过邮件网关发送。

在**收件人（电子邮件地址）**字段，指定程序发送通知的邮件地址。您可以在该字段指定多个地址，以分号分隔。通知将被传送到指定邮件地址关联的电话号码。

在 **SMTP 服务器**字段，指定邮件服务器地址，以分号分隔。您可以使用下列值：

- IPv4 或 IPv6 地址
- 设备的 Windows 网络名称（NetBIOS 名称）
- SMTP 服务器的 DNS 名称

在 **SMTP 服务器端口**字段，指定 SMTP 服务器通信端口号。默认端口号是 25。

单击“**设置**”链接以定义其他通知设置：

- 主题名称（电子邮件的主题名称）
- 发件人电子邮件地址
- ESMTP 身份验证设置

如果为 SMTP 服务器启用了 ESMTP 身份验证选项，则必要时可以指定在 SMTP 服务器上进行身份验证的账户。

- SMTP 服务器的 TLS 设置

您可以禁用 TLS，如果 SMTP 服务器支持 TLS，则使用此协议，您也可以强制仅使用 TLS。如果您选择仅使用 TLS，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，如果选择仅使用 TLS，还可以为 SMTP 服务器上的客户端身份验证指定证书。

- 浏览 SMTP 服务器证书文件

您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到 Kaspersky Security Center。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。“**通知消息**”字段包含标准文本，其中包含有关应用程序在事件发生时发送的事件的信息。该文本包含代替参数，例如事件名称、设备名称和域名。您可以通过添加其他带有事件的更多相关详情的替代参数来编辑消息文本。替代参数列表通过点击字段右侧的按钮可用。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接以指定应用程序在指定时间间隔内可以发送的最大通知数量。

单击“**发送测试消息**”按钮检查您是否正确配置了通知。应用程序应向您指定的收件人发送测试通知。

- **要运行的可执行文件**

如果选择该通知方法，您可以在输入字段指定事件发生时要启动的应用程序。

点击**配置通知限制数**链接允许您指定应用程序在指定时间段可以发送的最大通知数量（通知数量 / 分钟数）。

点击**发送测试消息**按钮允许您检查您是否正确配置了通知：应用程序发送测试通知到您指定的邮件地址。

5. 在“**通知消息**”字段，输入事件发生时应用程序要发送的文本。
   您可以使用文本字段右边的下拉列表来添加事件详情的替代设置（例如，事件描述、发生时间等等）。

   如果通知文本包含 % 字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

6. 单击“**发送测试消息**”按钮以检查通知是否已正确配置。
   程序发送测试通知到指定用户。

7. 单击“**确定**”保存更改。

经过调整的通知设置将应用于客户端设备上发生的所有事件。

您可以在管理服务器设置、策略设置或应用程序设置的“**事件配置**”区域覆盖特定事件的通知设置。

测试通知

为了检查事件通知是否可以发送，程序将在客户端设备上使用 Eicar 测试“病毒”检测通知。

要验证事件通知的发送，请执行以下操作：

1. 停止客户端设备上的实时文件系统保护任务，将 EICAR 测试“病毒”复制到客户端设备。现在重新启用文件系统的实时保护。

2. 为管理组中的客户端设备或特定设备运行扫描任务，包括带有 EICAR“病毒”的设备。
   如果扫描任务配置正确，程序会检测到测试“病毒”。如果通知配置正确，您将收到检测到病毒的通知。
   在**管理服务器**节点的工作区，在“**事件**”选项卡，“**最近事件**”分类显示检测“病毒”记录。

EICAR 测试“病毒”不包含任何危害您设备的代码。不过，多数厂商的安全应用程序都将该文件视为病毒。您可以从 EICAR 官方网站 上下载该测试“病毒”。

通过运行可执行文件显示的事件通知

Kaspersky Security Center 可通过运行可执行文件将客户端设备上发生的事件通知管理员。可执行文件必须包含另外一个可执行文件，而后者具有要转发给管理员的事件的占位符（请见下表）。

描述事件的占位符

占位符	占位符描述
%SEVERITY%	事件严重级别。可能值： • **信息** • **警告** • **错误** • **严重**
%COMPUTER%	发生事件的设备的名称。 设备名称的最大长度为 256 个字符。

占位符	占位符描述
%DOMAIN%	发生事件的设备的域名称。
%EVENT%	事件类型的名称。 事件类型名称的最大长度为 50 个字符。
%DESCR%	事件描述。 描述的最大长度为 1000 个字符。
%RISE_TIME%	事件创建时间。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	任务名称。 任务名称的最大长度为 100 个字符。
%KL_PRODUCT%	应用程序名称。
%KL_VERSION%	应用程序版本号。
%KLCSAK_EVENT_SEVERITY_NUM%	事件严重编号。可能值： • 1—**信息** • 2—**警告** • 3—Error • 4—**严重**
%HOST_IP%	发生事件的设备的 IP 地址。
%HOST_CONN_IP%	发生事件的设备的连接 IP 地址。

例如：
事件通知由某个可执行文件（例如，script1.bat）发出，在该可执行文件中，将启动具有 %COMPUTER% 占位符的另一个可执行文件（例如，script2.bat）。当发生事件时，将在管理员的设备上运行 script1.bat 文件，而该文件随后运行具有 %COMPUTER% 占位符的 script2.bat 文件。管理员将接收到发生事件的设备的名称。

使用 TLS 的加密通信

要修复您组织企业网络中的漏洞，您可以使用 TLS 协议启用流量加密。您可以在管理服务器和 iOS MDM 服务器上启用 TLS 加密协议和支持的密码套件。Kaspersky Security Center 支持 TLS 协议版本 1.0、1.1、1.2 和 1.3。您可以选择所需的加密协议和加密套件。

Kaspersky Security Center 使用自签发证书。不需要 iOS 设备的附加配置。您也可以使用您自己的证书。Kaspersky 专家建议使用由受信任证书当局发布的证书。

管理服务器

要在管理服务器上配置允许的加密协议和加密套件：

1. 使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. 使用 SrvUseStrictSslSettings 标志在管理服务器上配置允许的加密协议和加密套件。输入以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <value> -t d
   ```

   指定 SrvUseStrictSslSettings 标志的<value>参数：

   - 4—仅启用 TLS 1.2 和 TLS 1.3 协议。此外，还启用了具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的加密套件（向后兼容 Kaspersky Security Center 先前版本需要这些加密套件）。这是默认值。

TLS 1.2 协议支持的密码套件：

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- AES256-GCM-SHA384（具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密码套件）
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

TLS 1.3 协议支持的密码套件：

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

- 5 —仅启用 TLS 1.2 和 TLS 1.3 协议。对于 TLS 1.2 和 TLS 1.3 协议，支持下面列出的特定密码套件。

  TLS 1.2 协议支持的密码套件：

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  TLS 1.3 协议支持的密码套件：

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

我们不建议使用 0、1、2 或 3 作为 SrvUseStrictSslSettings 标志的参数值。这些参数值对应于不安全的 TLS 协议版本（TLS 1.0 和 TLS 1.1 协议）和不安全的密码套件，仅用于向后兼容早期 Kaspersky Security Center 版本。

3. 重新启动以下 Kaspersky Security Center 15.1 服务：

   - 管理服务器
   - Web 服务器
   - 激活代理

使用 TLS 协议进行流量加密被启用。

您可以使用 KLTR_TLS12_ENABLED 和 KLTR_TLS13_ENABLED 标志分别启用对 TLS 1.2 和 TLS 1.3 协议的支持。这些标志默认启用。

要启用或禁用对 TLS 1.2 和 TLS 1.3 协议的支持：

1. 运行 klscflag 实用程序。

   使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. 使用管理员权限在 Windows 命令提示符处输入以下命令之一：

   - 使用此命令启用或禁用对 TLS 1.2 协议的支持：

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <value> -t d
     ```

   - 使用此命令启用或禁用对 TLS 1.3 协议的支持：

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <value> -t d
     ```

   指定标志的< 值 >参数：

   - `1` — 启用对 TLS 协议支持。
   - `0`—禁用对 TLS 协议的支持。

iOS MDM 服务器

iOS 设备和 iOS MDM 服务器之间的连接默认被加密。

要在 iOS MDM 服务器上配置允许的加密协议和加密套件：

1. 打开安装了 iOS MDM 服务器的客户端设备的注册表（例如，在**开始** → **运行**菜单使用 regedit 命令）。
2. 转至以下分支：

   - 对于 32 位系统：

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor

   - 对于 64 位系统：

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI

3. 创建名为 `StrictSslSettings` 的键。

4. 指定 DWORD 做为键类型。

5. 设置键值：

   - 2 — 启用 TLS 1.0、TLS 1.1 和 TLS 1.2 协议。
   - 3 — 仅启用 TLS 1.2 协议（默认值）。

6. 重启 Kaspersky Security Center iOS MDM 服务器服务。

配置界面

您可以配置 Kaspersky Security Center 界面：

- 根据所使用的功能，在控制台树、工作区和对象（文件夹、区域）的属性窗口中显示和隐藏对象。
- 显示和隐藏主窗口的元素（例如，控制台树或“**操作**”和“**视图**”等标准菜单）。

要根据当前使用的功能集配置 Kaspersky Security Center 界面：

1. 在控制台树中，选择**管理服务器**节点。
2. 在应用程序主窗口的菜单栏上，选择“**视图**”→“**配置界面**”。
3. 在打开的“**配置界面**”窗口中，使用以下复选框配置界面元素的显示：

   - **显示漏洞和补丁管理**

     如果启用此选项，则“**远程安装**”文件夹将显示“**部署设备映像**”子文件夹，“**存储库**”文件夹将显示“**硬件**”子文件夹。

     如果快速启动向导尚未完成，则默认情况下禁用此选项。快速启动向导完成后，默认情况下启用此选项。

     如果此选项被禁用，即使您拥有**系统管理授权许可，菜单项创建 RDP 会话**“创建 RDP 会话”**Windows 桌面共享**“Windows 桌面共享”也不可用。

   - **显示数据加密和保护**

     如果启用此选项，则控制台树将显示“**数据加密和保护**”文件夹。

     默认情况下已启用该选项。

   - **显示端点控制设置**

     如果启用此选项，Kaspersky Endpoint Security for Windows 策略属性窗口的“**安全控制**”区域中将显示以下子区域：

     - **应用程序控制**
     - **设备控制**

- **Web 控制**
- **自适应异常控制**

如果禁用此选项，则“**安全控制**”区域中不会显示上述子区域。

默认情况下已启用该选项。

- **显示移动设备管理**

如果启用此选项，则“**移动设备管理**”功能可用。重新启动应用程序后，控制台树将显示“**移动设备**”文件夹。

默认情况下已启用该选项。

- **显示从属管理服务器**

如果选中此复选框，则控制台树将显示管理组中的从属管理服务器和虚拟管理服务器节点。与从属管理服务器和虚拟管理服务器相关的功能（例如，在从属管理服务器上创建用于远程安装应用程序的任务）将可用。

默认情况下已清除该选框。

- **显示安全设置区域**

如果启用此选项，管理服务器、管理组和其他对象的属性窗口中将显示“**安全**”区域。使用此选项可以为用户和用户组提供自定义的对象使用权限。

默认情况下已禁用该选项。

4. 单击“**确定**”。

要应用某些更改，您必须关闭应用程序主窗口，然后再次将其打开。

要配置应用程序主窗口中的元素显示：

1. 在应用程序主窗口的菜单栏上，选择“**视图**”→“**配置**”。
2. 在打开的“**配置视图**”窗口中，使用复选框配置主窗口元素的显示。
3. 单击“**确定**”。

发现网络设备

该部分描述了安装 Kaspersky Security Center 后必须采取的操作。

情景：发现网络设备

您必须在安装安全应用程序之前执行设备发现。管理服务器可接收已发现设备的信息，并允许您通过策略管理这些设备。需要定期进行网络轮询以更新网络中可用设备的列表。

在开始网络轮询之前，请确保已启用 SMB 协议。否则，Kaspersky Security Center 无法发现轮询网络中的设备。要启用 SMB 协议，请按照适用于您的操作系统的说明进行操作。

发现网络设备按以下阶段进行：

1. **发现设备**

   快速启动向导通过初始设备发现指引您，并帮助您查找网络设备，例如计算机、平板电脑和移动电话。您也可以手动执行设备发现。

2. **配置计划轮询**

   决定您要定期使用哪些轮询类型。启用所需的类型并配置轮询计划。您可以参考网络轮询频率建议。

3. **设置规则以添加发现的设备到管理组（可选）**

   如果新设备出现在您的网络中，则它们将在定期轮询期间被发现，并自动包含在“**未分配的设备**”组中。您可以设置设备移动规则以自动分配设备到**受管理设备**组。您也可以配置保留规则。

   如果您跳过第 3 步，新发现的设备将分配给**未分配的设备**组。如果需要，可以手动将这些设备移动到“**受管理设备**”组。如果您手动将这些设备移动到“**受管理设备**”组，您可以分析每台设备的信息并决定您是否要将它移动到管理组以及移动到具体哪个组。

结果

完成方案可以导致如下：

- Kaspersky Security Center 管理服务器发现网络中的设备并提供您它们的信息。
- 未来轮询被设置并根据指定的计划工作。
- 新发现的设备按照配置的规则排列。（或者，如果没有配置规则，设备将保留在**未分配的设备**组中）。

未分配的设备

此部分介绍如何管理企业网络中未包含在管理组中的设备。

设备发现

该部分描述了 Kaspersky Security Center 中可用的设备发现类型并给出使用每种类型的信息。

管理服务器通过常规轮询接收网络结构信息和网络设备信息。信息被记录到管理服务器数据库。管理服务器可使用下列类型的轮询：

- **Windows 网络轮询**。管理服务器可以执行两种 Windows 网络轮询：快速和完整。在快速轮询过程中，管理服务器只从所有网络域和工作组中设备的 NetBIOS 名称列表检索信息。在完整轮询中，需要每台客户端设备的跟多信息，例如操作系统名称、IP 地址、DNS 名称和 NetBIOS 名称。默认下，快速和完整轮询都被启用。Windows 网络轮询可能发现设备失败，例如，如果端口 UDP 137、UDP 138、TCP 139 在路由器上或被防火墙关闭。

- **活动目录轮询**。管理服务器接收活动目录单元结构以及活动目录组中设备的 DNS 名称的信息。默认情况下已启用该轮询类型。如果您使用活动目录，我们建议您使用活动目录轮询；否则，管理服务器不发现任何设备。如果您使用活动目录但是一些网络设备不列为成员，这些设备无法通过活动目录轮询发现。

- **IP 范围轮询**。管理服务器使用 ICMP 包或 NBNS 协议轮询指定的 IP 范围，并编制一组完整的关于这些 IP 范围内的设备的数据。默认情况下已禁用该轮询类型。如果您使用 Windows 网络轮询和/或活动目录轮询，不建议您使用该轮询类型。

- **Zeroconf 轮询**。使用零配置网络（也称为 *Zeroconf*）轮询 IPv6 网络的分发点。默认情况下已禁用该轮询类型。如果分发点运行 Linux，则可以使用 Zeroconf 轮询。

如果设置并启用了设备移动规则，则新发现的设备将自动包含在“**受管理设备**”组中。如果未启用移动规则，新发现的设备将自动包含在“**未分配的设备**”组。

您可以为每种类型修改设备发现设置。例如，您可能想要修改轮询计划或者设置是否轮询整个域森林还是仅指定域。

在开始网络轮询之前，请确保已启用 SMB 协议。否则，Kaspersky Security Center 无法发现轮询网络中的设备。要启用 SMB 协议，请按照适用于您的操作系统的说明进行操作。

Windows 网络轮询

关于 Windows 网络轮询

在快速轮询过程中，管理服务器只从所有网络域和工作组中设备的 NetBIOS 名称列表检索信息。在完整轮询中，以下信息被从每个客户端设备请求：

- 操作系统名称
- IP 地址
- DNS 名称
- NetBIOS 名称

快速轮询和完整轮询都需要以下：

- 端口 UDP 137/138、TCP 139、UDP 445、TCP 445、必须在网络中可用。
- SMB 协议已启用。
- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在管理服务器上启用。

- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在客户端设备上启用：
  - 至少一台设备上，如果网络设备数量不超过 32。
  - 对每 32 台网络设备至少一台设备上。

完整轮询仅在快速轮询至少运行了一次时可以运行。

查看和修改 Windows 网络轮询设置

要修改 Windows 网络轮询的设置，请执行以下操作：

1. 在控制台树的“**设备发现**”文件夹，选择“**域**”子文件夹。
   您可以通过单击**立即轮询**按钮从“**未分配的设备**”文件夹转到“**设备发现**”文件夹。
   在“**域**”子文件夹的工作区，将显示设备列表。

2. 单击**立即轮询**。
   域属性窗口将开启。如果您想，修改 Windows 网络轮询设置：

   - **启用 Windows 网络轮询**

     默认情况下已选中该选项。如果您不想执行 Windows 网络轮询（例如，如果您认为活动目录轮询已足够），您可以清空该选项。

   - **设置快速轮询计划**

     默认间隔是 15 分钟。
     在快速轮询过程中，管理服务器只从所有网络域和工作组中设备的 NetBIOS 名称列表检索信息。
     下次轮询接收的数据替换旧数据。
     有以下轮询计划选项可用：

     - **每 N 天**

       轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
       默认下，轮询每天运行一次，从当前系统日期和时间开始。

     - **每 N 分钟**

       轮询定期运行，按照指定分钟间隔，从指定的时间开始。
       默认下，轮询每五分钟运行一次，从当前系统时间开始。

     - **按星期中的天数**

       轮询定期运行，在指定星期的指定时间。
       默认下，轮询每周五 18:00:00 P.M. 运行。

     - **每个月在所选周的指定天**

轮询定期运行，在指定月日的指定时间。

默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已启用该选项。

- **设置完整轮询计划**

  默认间隔是一小时。下次轮询接收的数据替换旧数据。

  有以下轮询计划选项可用：

  - **每 N 天**

    轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。

    默认下，轮询每天运行一次，从当前系统日期和时间开始。

  - **每 N 分钟**

    轮询定期运行，按照指定分钟间隔，从指定的时间开始。

    默认下，轮询每五分钟运行一次，从当前系统时间开始。

  - **按星期中的天数**

    轮询定期运行，在指定星期的指定时间。

    默认下，轮询每周五 18:00:00 P.M. 运行。

  - **每个月在所选周的指定天**

    轮询定期运行，在指定月日的指定时间。

    默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

  - **运行错过的任务**

    如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

    如果启用该选项，管理服务器在它切换回来后立即启动轮询。

    如果禁用该选项，管理服务器等待下一次计划轮询。

    默认情况下已启用该选项。

如果您要立即执行轮询，请单击“**立即轮询**”。两种轮询将启动。

在虚拟管理服务器上，可以在“**设备发现**”区域中分发点的属性窗口中查看和编辑轮询 Windows 网络的设置。

活动目录轮询

如果您使用活动目录则使用活动目录轮询；否则，建议使用其他类型的轮询。如果您使用活动目录但是一些网络设备不列为成员，这些设备无法通过活动目录轮询发现。

无论后续轮询的结果如何，Active Directory 轮询结果都会存储在管理服务器上 30 天。

在开始网络轮询之前，请确保已启用 SMB 协议。否则，Kaspersky Security Center 无法发现轮询网络中的设备。要启用 SMB 协议，请按照适用于您的操作系统的说明进行操作。

浏览和修改活动目录轮询设置

要查看和修改活动目录组的轮询设置，请执行以下操作：

1. 在控制台树的“**设备发现**”文件夹，选择“**活动目录**”子文件夹。

   或者，您可以通过单击“**立即轮询**”按钮从“**未分配的设备**”文件夹转到“**设备发现**”文件夹。

2. 单击**配置轮询**。

   活动目录属性窗口打开。如果您想，修改活动目录轮询设置：

   - **启用活动目录轮询**

     默认情况下已选中该选项。然而，如果您不使用活动目录，轮询不获取任何结果。此种情况下，您可以清空该选项。

   - **设置轮询计划**

     默认间隔是一小时。

     有以下轮询计划选项可用：

     - **每 N 天**

       轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。

       默认下，轮询每天运行一次，从当前系统日期和时间开始。

     - **每 N 分钟**

       轮询定期运行，按照指定分钟间隔，从指定的时间开始。

       默认下，轮询每五分钟运行一次，从当前系统时间开始。

     - **按星期中的天数**

轮询定期运行，在指定星期的指定时间。

默认下，轮询每周五 18:00:00 P.M. 运行。

- **每个月在所选周的指定天**

  轮询定期运行，在指定月日的指定时间。

  默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已启用该选项。

- **高级**

  您可以选择要轮询的活动目录域：

  - Kaspersky Security Center 所属的活动目录域。
  - Kaspersky Security Center 所属的域森林。
  - 活动目录域的指定列表。

    如果您选择该选项，您可以添加域到轮询范围：

    - 单击“**添加**”按钮。
    - 在对应的字段，指定域控制器地址、访问它的账户名称和密码。
    - 单击“**确定**”保存更改。

    您可以在列表上选择域控制器地址并点击**修改**或**删除**按钮以修改或删除它。

  - 单击“**确定**”保存更改。

如果您要立即执行轮询，请单击“**立即轮询**”按钮。

在虚拟管理服务器上，可以在“**设备发现**”区域中分发点的属性窗口中查看和编辑轮询活动目录组的设置。

IP 范围轮询

管理服务器使用 ICMP 包或 NBNS 协议轮询指定的 IP 范围，并编制一组完整的关于这些 IP 范围内的设备的数据。默认情况下已禁用该轮询类型。

对于 Microsoft Active Directory 或 Samba 域控制器内的所有基于 Linux 的主机，请在`/etc/samba/smb.conf`文件中指定`netbios name`和`workgroup`参数。否则，轮询结果可能包含重复的主机。

在开始网络轮询之前，请确保已启用 SMB 协议。否则，Kaspersky Security Center 无法发现轮询网络中的设备。要启用 SMB 协议，请按照适用于您的操作系统的说明进行操作。

浏览和修改 IP 范围轮询设置

要查看和修改 IP 范围组的轮询设置，请执行以下操作：

1. 在控制台树的“**设备发现**”文件夹，选择“**IP 范围**”子文件夹。
   您可以通过单击“**立即轮询**”从“**未分配的设备**”文件夹转到“**设备发现**”文件夹。
2. 如果需要，在“**IP 范围**”子文件夹中单击“**添加子网**”以添加用于轮询的 IP 范围，然后单击“**确定**”。
3. 单击**配置轮询**。
   IP 范围属性窗口将开启。如果您想，您可以修改 IP 范围轮询的设置：

   - **启用 IP 范围轮询**

     默认情况下不选中该选项。如果您使用 Windows 网络轮询和/或活动目录轮询，不建议您使用该轮询类型。

   - **设置轮询计划**

     默认间隔是 420 分钟。下次轮询接收的数据替换旧数据。
     有以下轮询计划选项可用：

     - **每 N 天**

       轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
       默认下，轮询每天运行一次，从当前系统日期和时间开始。

     - **每 N 分钟**

       轮询定期运行，按照指定分钟间隔，从指定的时间开始。
       默认下，轮询每五分钟运行一次，从当前系统时间开始。

     - **按星期中的天数**

       轮询定期运行，在指定星期的指定时间。
       默认下，轮询每周五 18:00:00 P.M. 运行。

     - **每个月在所选周的指定天**

       轮询定期运行，在指定月日的指定时间。

默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已启用该选项。

如果您要立即执行轮询，请单击“**立即轮询**”。该按钮仅在您选择了“**启用 IP 范围轮询**”时可用。

在虚拟管理服务器上，可以在“**设备发现**”区域的分发点属性窗口中查看和编辑轮询 IP 范围的设置。在轮询 IP 范围期间发现的客户端设备将显示在虚拟管理服务器的“**域**”文件夹中。

Zeroconf 轮询

只有基于 Linux 的分发点支持此轮询类型。

分发点可以轮询具有 IPv6 地址的设备的网络。在这种情况下，不指定 IP 范围，并且分发点使用零配置网络（称为 *Zeroconf*）轮询整个网络。要开始使用 Zeroconf，您必须在分发点上安装 avahi-browse 实用程序。

要启用 Zeroconf 轮询：

1. 在控制台树的“**设备发现**”文件夹，选择“**IP 范围**”子文件夹。

   您可以通过单击“**立即轮询**”从“**未分配的设备**”文件夹转到“**设备发现**”文件夹。

2. 单击**配置轮询**。

3. 在打开的 IP 范围属性窗口中，选择“**使用 Zeroconf 技术启用轮询**”。

之后，分发点开始轮询您的网络。在这种情况下，指定的 IP 范围将被忽略。

使用 Windows 域查看和更改域设置

要修改域设置，请执行以下操作：

1. 在控制台树的“**设备发现**”文件夹，选择“**域**”子文件夹。

2. 以下列方式之一选择一个域并打开其属性窗口：

   - 从域的上下文菜单中选择“**属性**”。
   - 通过点击“**显示组属性**”链接。

属性：<域名>窗口将打开，您可以在其中配置所选域。

为未分配的设备配置保留规则

Windows 网络轮询完成后，发现的设备被放置到“未分配的设备”管理组的子组。该管理组可以在**高级 → 设备发现 → 域**中找到。**域**文件夹是父组。它包含以对应域为名称的子组和在网络轮询过程中发现的工作组。父组可能也包含移动设备管理组。您可以为父组和每个子组配置未分配的设备的保留规则。保留规则不取决于网络轮询设置并在网络轮询被禁用时也工作。

要为未分配的设备配置保留规则：

1. 在控制台树的“**设备发现**”文件夹，执行下列操作之一：

   - 要配置父组设置，右击“**域**”子文件夹并选择“**属性**”。
     父组属性窗口将开启。
   - 要配置子组设置，右击其名称并选择**属性**。
     子组属性窗口将开启。

2. 在“**设备**”区域，指定以下设置：

   - **当设备处于非活动状态超过指定天数时，从组中删除设备**

     如果启用该选项，您可以指定设备被从组中自动移除的时间间隔。默认下，该选项也被分发到子组。默认时间间隔是 7 天。
     默认情况下已启用该选项。

   - **从父组继承**

     如果启用该选项，设备在当前组的保留期从父组继承且无法被更改。
     该选项仅对子组可用。
     默认情况下已启用该选项。

   - **强制子组继承**

     该设置值将被分发到子组，但在子组的属性中这些设置被锁定。
     默认情况下已禁用该选项。

   您的更改已保存并应用。

使用 IP 范围

您可以自定义现有的 IP 范围并创建新子网。

创建 IP 范围

要创建 IP 范围，请执行以下操作：

1. 在控制台树的“**设备发现**”文件夹，选择“**IP 范围**”子文件夹。
2. 在文件夹的上下文菜单中，选择**新建 → IP 范围**。
3. 在打开的“**新 IP 范围**”窗口中设置新的 IP 范围。

新的 IP 范围将显示在“**IP 范围**”文件夹中。

浏览和更改 IP 范围设置

要修改 IP 范围设置，请执行以下操作：

1. 在控制台树的“**设备发现**”文件夹，选择“**IP 范围**”子文件夹。
2. 以下列方式之一选择一个 IP 范围并打开其属性窗口：
   - 从 IP 范围的上下文菜单中选择“**属性**”。
   - 通过点击“**显示组属性**”链接。

系统将打开**属性：<IP 范围名称>**窗口，您可以在该窗口中配置选定的 IP 范围的属性。

使用活动目录组查看和修改组设置

要修改活动目录组设置，请执行以下操作：

1. 在控制台树的“**设备发现**”文件夹，选择“**活动目录**”子文件夹。
2. 通过以下方式之一选择一个活动目录组并打开其属性窗口：
   - 从 IP 范围的上下文菜单中选择“**属性**”。
   - 通过点击“**显示组属性**”链接。

系统将打开**属性：<活动目录组名称>**窗口，在其中可以配置选定的活动目录组。

创建将设备自动移至管理组的规则

您可以将设备配置为在企业网络轮询中发现后将其自动移至管理组。

要配置将设备自动移至管理组的规则：

1. 在控制台树中，选择“**未分配的设备**”文件夹。
2. 在该文件夹的工作区，点击“**配置规则**”。

   这会打开**属性：未分配的设备**窗口。在“**移动设备**”区域，配置自动移动设备至管理组的规则。

列表中的第一条适用规则（从列表的顶部到底部）将应用于设备。

在客户端设备上使用 VDI 动态模式

虚拟基础架构可以使用临时虚拟机部署企业网络。Kaspersky Security Center 检测到临时虚拟机和他们在管理服务器数据库的附加信息。用户使用完临时虚拟机后，这些虚拟机将从虚拟架构中移除。然而，以后虚拟机的记录可以保存在管理服务器数据库中。并且，没有虚拟机可以在管理控制台显示。

为了防止不存在的虚拟机被保存，Kaspersky Security Center 支持动态模式的虚拟桌面基础架构 (VDI)。管理员可以在被安装到临时虚拟机的网络代理安装包的属性中启动支持动态 VDI。

当临时虚拟机被禁用，网络代理通知管理服务器该虚拟机已被禁用。如果虚拟机被成功禁用，它将从连接到管理服务器的设备列表中被移除。如果虚拟机被禁用错误，网络代理没有发送禁用虚拟机的通知到管理服务器，使用备份方案。使用这个方案，和管理服务器尝试同步三次未成功后，虚拟机从连接管理服务器的设备列表移除。

在网络代理安装包属性中启用 VDI 动态模式

要启用 VDI 动态模式，请执行以下操作：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
2. 在网络代理安装包的上下文菜单中，选择“**属性**”。

   属性：Kaspersky Security Center 网络代理窗口将开启。
3. 在“**属性：Kaspersky Security Center 网络代理**”窗口中，选择“**高级**”区域。
4. 在“**高级**”区域中，选择“**启用 VDI 动态模式**”选项。

   要安装网络代理的设备将成为 VDI 的一部分。

搜索组成 VDI 的设备

要搜索组成 VDI 的未分配的设备，请执行以下操作：

1. 从“**未分配的设备**”文件夹的上下文菜单中选择“**搜索**”。

   要查看属于虚拟桌面基础架构的所有设备的列表，请从**搜索**文件夹的上下文菜单中选择**管理服务器**。

2. 在**搜索**窗口的**虚拟机**选项卡上，在**是**设置组中选择**虚拟桌面基础架构的一部分**。

3. 单击“**立即查找**”按钮。

   属于虚拟桌面基础架构的未分配的设备的列表将显示。

将组成 VDI 的设备移至管理组

要将组成 VDI 的设备移至管理组，请执行以下操作：

1. 在“**未分配的设备**”文件夹的工作区中，点击“**配置规则**”。
   这将打开“**未分配的设备**”文件夹的属性窗口。

2. 在“**未分配的设备**”文件夹属性窗口的“**移动设备**”区域中，单击“**添加**”按钮。
   “**新规则**”窗口将开启。

3. 在“**新规则**”窗口中，选择“**虚拟机**”区域。

4. 在“**这是一台虚拟机**”下拉列表中，选择“**是**”。

   将会创建一个将设备迁移至管理组的规则。

设备清单

用于清查设备的硬件清单（**存储库 → 硬件**）以两种方式填充：自动和手动。每次网络轮询后，所有检测到的设备都会自动添加到列表中；但是，如果您不希望轮询网络，也可以手动添加设备。您可以手动将其他设备添加到列表中，例如路由器、打印机或设备硬件。

您可以在设备的属性中查看并编辑有关该设备的详细信息。

硬件列表可能包含以下类型的设备：

- 计算机
- 移动设备
- 网络设备
- 虚拟设备
- OEM 组件
- 计算机周边设备
- 已连接设备
- VoIP 电话
- 网络存储库

管理员可以将“*企业设备*”属性分配给所检测到的设备。管理员可以在设备的属性中手动分配该属性，或者指定自动分配该属性的条件。在这种情况下，系统将按设备类型分配“*企业设备*”属性。

Kaspersky Security Center 允许注销设备。为此，请在设备属性中选择“**设备已写入**”选项。此类设备不会显示在设备列表中。

管理员可以在“**硬件**”文件夹管理可编程逻辑控制器 (PLC) 的列表。管理 PLC 列表的详细信息提供在 *Kaspersky Industrial CyberSecurity for Nodes 用户指南*。

添加有关新设备的信息

若要添加网络中新设备的信息，请执行以下操作：

1. 在控制台树的“**存储库**”文件夹中，选择“**硬件**”子文件夹。
2. 在“**硬件**”文件夹的工作区中单击“**添加设备**”按钮，打开“**新设备**”窗口。
   “**新设备**”窗口将开启。
3. 在“**新设备**”窗口中，从“**类型**”下拉列表中选择您要添加的设备类型。
4. 单击“**确定**”。
   此时将打开设备属性窗口，显示“**常规**”区域。
5. 在“**常规**”区域中使用设备数据填写输入字段。“**常规**”区域将显示以下设置：
   - **企业设备**。如果您希望将“*企业*”属性分配给该设备，请选择该选框。您可以使用该属性搜索“**硬件**”文件夹中的设备。
   - **设备已写入**。如果您不希望该设备显示在“**硬件**”文件夹中的设备列表中，请选中该复选框。
6. 单击“**应用**”。

新设备将显示在“**硬件**”文件夹的工作区中。

配置用于定义企业设备的标准

若要配置企业设备的检测标准，请执行以下操作：

1. 在控制台树的“**存储库**”文件夹中，选择“**硬件**”子文件夹。
2. 在“**硬件**”文件夹的工作区，点击“**附加操作**”按钮并在下拉列表中选择“**设置企业设备规则**”。
   “硬件属性”窗口打开。

3. 在硬件属性窗口的“**企业设备**”区域中，选择将“*企业*”属性分配给该设备的方法：

   - **为设备手动设置 “企业” 属性**。在设备属性窗口的“**常规**”区域中手动将“*企业硬件*”属性分配给该设备。
   - **为设备自动设置 “企业” 属性**。在设置的“**通过设备类型**”区域中指定应用程序自动为其分配“*企业*”属性的设备类型。

     此选项仅影响通过网络轮询添加的设备。对于手动添加的设备，请手动设置“*企业*”属性。

4. 单击“**确定**”。

企业设备的检测标准得到配置。

配置自定义字段

要配置设备的自定义字段：

1. 在控制台树的“**存储库**”文件夹中，选择“**硬件**”子文件夹。
2. 在“**硬件**”文件夹的工作区，点击“**附加操作**”按钮并在下拉列表中选择“**配置自定义数据字段**”。
   “硬件属性”窗口打开。
3. 在“硬件属性”窗口，选择“**自定义字段**”区域并点击“**添加**”按钮。
   “**添加字段**”窗口将打开。
4. 在“**添加字段**”窗口，指定将在硬件属性中显示的自定义字段的名称。
   您可以使用独立名称创建多个自定义字段。
5. 单击“**确定**”。

添加的自定义字段显示在硬件属性的“**自定义字段**”区域。您可以使用自定义字段提供设备的特别信息。例如，这可以是硬件的内部订购号。

授权许可

本节介绍与 Kaspersky Security Center 15.1 授权许可有关的常规概念。

超出了授权许可限制事件

Kaspersky Security Center 允许您获取客户端设备上安装的 Kaspersky 应用程序的授权许可达到限制的事件信息。

授权许可达到限制的此类事件的重要级别根据以下规则定义：

- 如果当前使用单一授权许可的单元的数量达到该授权许可所覆盖的单元总数的 90% 和 100% 之间，事件等级就是**信息**重要级别。
- 如果当前使用单一授权许可的单元的数量达到该授权许可所覆盖的单元总数的 100% 和 110% 之间，事件等级就是**警告**重要级别。
- 如果当前使用单一授权许可的单元的数量超过该授权许可所覆盖的单元总数的 110%，事件等级就是**严重事件**重要级别。

关于授权许可

本节包含有关通过 Kaspersky Security Center 管理的 Kaspersky 应用程序授权许可的信息。

关于授权许可

*授权许可*是根据签名授权许可合约（最终用户授权许可协议）条款授予的在有限时间内使用 Kaspersky Security Center 的权限。

服务范围和有效期取决于根据其使用应用程序的授权许可。

提供以下授权许可类型：

- *试用*

  用于试用该应用程序的免费授权许可。试用版授权许可通常拥有较短的有效期。

  试用版授权许可过期后，Kaspersky Security Center 的所有功能都会被禁用。要继续使用该程序，您需要购买商业版的授权许可。

  您只能在试用授权许可下使用该应用程序一个试用期。

- *商业*

  付费授权许可。

  当商业授权许可到期时，应用程序的主要功能将被禁用。要继续使用 Kaspersky Security Center，您必须续费您的商业授权许可。商业授权许可过期后，您将无法继续使用该应用程序，必须将其从设备中删除。

  我们建议在授权许可过期之前进行续费，以确保保护不受中断，防御所有安全威胁。

关于最终用户授权许可协议

最终用户授权许可协议（授权许可协议或 EULA）是您和 AO Kaspersky Lab 之间具有约束力的合作协议，其中规定了您使用该程序应遵守的条款。

在您开始使用应用程序之前请认真阅读授权许可协议。

Kaspersky Security Center 及其组件（例如网络代理）具有自己的 EULA。

您可以使用以下方法浏览 Kaspersky Security Center 最终用户授权许可协议的条款：

- 在 Kaspersky Security Center 安装期间。
- 如果阅读包含在 Kaspersky Security Center 分发包的 license.txt 文档。
- 如果阅读在 Kaspersky Security Center 安装文件夹的 license.txt 文档。
- 通过从卡巴斯基网站下载 license.txt 文件。

您可以使用以下方法查看 Network Agent for Windows、Network Agent for Mac 和 Network Agent for Linux 的最终用户授权许可协议的条款：

- 从 Kaspersky Web 服务器下载网络代理分发包期间。
- 在安装 Network Agent for Windows、Network Agent for Mac 或 Network Agent for Linux 期间。
- 通过阅读 Network Agent for Windows、Network Agent for Mac 或 Network Agent for Linux 分发包中包含的 license.txt 文档。
- 通过阅读 Network Agent for Windows、Network Agent for Mac 或 Network Agent for Linux 安装文件夹中的 license.txt 文档。
- 通过从卡巴斯基网站下载 license.txt 文件。

当您安装程序时同意了最终用户授权许可协议，这表明您接受了最终用户授权许可协议的条款。如果您不接受授权许可协议的条款，请取消应用程序安装且不再使用应用程序。

关于授权许可证书

*授权许可证书*是随着您收到的一个密钥文件和激活码一起的文档。

授权许可证书包含下面的提供授权许可的信息：

- 授权许可 ID 或订单号
- 授予授权许可的用户信息
- 可以使用提供的授权许可激活的应用程序信息
- 授权许可单元数量限制（例如，在该授权许可下，设备上的应用程序可以被使用）
- 授权许可期限的开始日期
- 授权许可到期日期或授权许可期限
- 授权许可类型

关于授权许可密钥

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

您可以使用下面的方法添加一个授权许可密钥到应用程序：通过应用*密钥文件*或输入*激活码*。为应用程序添加授权许可后，将在应用程序界面中显示该授权许可密钥的唯一字母数字序列。

如果违反授权许可协议的条款，Kaspersky 可能会阻止授权许可密钥。如果授权许可已被阻止，要使用应用程序，您需要添加另外一个授权许可密钥。

授权许可密钥可以是活动密钥或附加（备用）密钥。

*活动授权许可密钥*是应用程序当前使用的授权许可密钥。活动授权许可密钥可以被添加为商业授权许可。应用程序只能拥有一个活动授权许可密钥。

*附加（或备用）授权许可密钥*是允许用户使用应用程序，但是当前未使用的授权许可密钥。与当前授权许可密钥相关联的授权许可过期时，附加授权许可密钥将自动成为当前活动授权许可密钥。只有在添加了活动授权许可密钥之后，才可以添加附加授权许可密钥。

试用授权许可密钥仅可以被当作活动授权许可密钥添加。试用授权许可密钥不可以被当作附加授权许可密钥添加。

关于密钥文件

*密钥文件*是 Kaspersky 提供的 .key 扩展名的文件。密钥文件设计用于通过添加授权许可密钥激活应用程序。

在购买 Kaspersky Security Center 或预定试用版本的 Kaspersky Security Center 后，您通过您指定的邮件地址可以收到密钥文件。

您不需要连接到 Kaspersky 激活服务器以使用密钥文件激活应用程序。

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

若要恢复您的密钥文件，执行下面任何的操作：

- 联系授权许可销售商。
- 使用您有效的激活码，通过卡巴斯基网站接收密钥文件。
- 从其他管理服务器导出授权许可密钥文件。

关于订阅

*Kaspersky Security Center 订阅*是在所选设置（订阅过期时间、受保护设备数量）下使用程序的订购。您可以和您的服务提供商（例如，互联网提供商）注册您的 Kaspersky Security Center 订阅。订阅可以自动或手动续费，您也可以取消订阅。

订阅可以是限期的（例如，一年）或不限期的。如果要在限期订阅后继续使用 Kaspersky Security Center，您必须续费订阅。无限制订阅如果已经预付给服务提供商了，则会在到期日自动续费。

当受限制订阅过期时，可为您提供一个使产品继续工作的宽限期以便您及时续费。宽限期的可用性和期限由服务提供商提供。

要在订阅下使用 Kaspersky Security Center，您必须应用从服务提供商收到的激活码。

您仅可以在订阅过期后或者取消订阅后为 Kaspersky Security Center 申请不同的激活码。

取决于服务提供商，订阅管理可能的操作也会不同。服务提供商可以不提供订阅宽限期，因此程序会失去它的功能。

订阅激活码无法用于激活 Kaspersky Security Center 的早期版本。

在订阅下使用应用程序时，Kaspersky Security Center 在指定时间间隔自动尝试访问激活服务器，直到订阅过期。这将确保有关订阅的信息与激活服务器同步。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。您可以在服务提供商网站续费您的订阅。

您可以手动更新有关订阅的信息，而无需等待Kaspersky Security Center 访问激活服务器。例如，当您更改订阅设置时，这可能会有用。

手动更新订阅信息：

1. 在控制台树中，选择“**卡巴斯基授权许可**”文件夹。
2. 单击**其他操作**，然后从下拉列表中选择**将订阅设置与授权许可服务器同步**。

   有关订阅的信息将在激活服务器上得到更新。

关于激活码

*激活码*是一串由20个字符数字组成的唯一序列。您可以输入激活码来添加授权许可密钥以激活 Kaspersky Security Center。在购买 Kaspersky Security Center 或预定试用版本的 Kaspersky Security Center 后，通过您指定的邮件地址可以收到激活码。

若要使用激活码激活应用程序，您需要互联网来建立与 Kaspersky 激活服务器的连接。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。

当程序被激活码激活后，程序有时发送有规律的请求到 Kaspersky 激活服务器，以便检查当前授权许可密钥状态。您必须提供给程序互联网连接以使其能够发送请求。

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

> 您不能使用密钥文件来激活受管理应用程序；只接受激活码。

撤销对最终用户授权许可协议的同意

如果您决定停止保护客户端设备，则可以卸载受管理的 Kaspersky 应用程序并撤销这些应用程序的最终用户授权许可协议 (EULA)。

要撤销受管理 Kaspersky 应用程序的 EULA：

1. 在控制台树中，选择“**管理服务器**”→“**高级**”→“**已接受的 EULA**”。
   将显示在创建安装包时、无缝安装更新时或部署 Kaspersky Security for Mobile 时接受的 EULA 列表。
2. 在该列表中，选择要撤销的 EULA。
   您可以查看 EULA 的以下属性：
   - EULA 的接受日期。
   - 接受 EULA 的用户名。
   - EULA 条款的链接。
   - 与 EULA 关联的对象列表：安装包的名称、无缝更新的名称、移动应用程序的名称。
3. 单击“**撤销 EULA**”按钮。
   在打开的窗口中，系统提示您必须卸载与 EULA 对应的 Kaspersky 应用程序。
4. 单击按钮以确认撤销。
   Kaspersky Security Center 会检查是否已删除安装包（对应于您要撤销其 EULA 的受管理 Kaspersky 应用程序）。
   您只能撤销已删除其安装包的受管理 Kaspersky 应用程序的 EULA。

EULA 即被撤销。它不会显示在“**管理服务器**”→“**高级**”→“**已接受的 EULA**”部分的 EULA 列表中。您不能使用已撤销 EULA 的 Kaspersky 应用程序保护客户端设备。

关于数据提供

传输到第三方的数据

使用软件的移动设备管理功能时，为了及时通过推送通知机制将命令传递到运行 Android 操作系统的设备，需使用 Google Firebase Cloud Messaging 服务。如果用户已配置 Google Firebase Cloud Messaging 服务的使用，则用户接受以自动模式向 Google Firebase Cloud Messaging 服务提供以下信息：推送通知必须发送至的 Kaspersky Endpoint Security for Android 应用程序的安装 ID。

要阻止与 Google Firebase Cloud Messaging 服务交换信息，用户必须将 Google Firebase Cloud Messaging 服务的使用设置回滚至出厂设置值。

使用软件的移动设备管理功能时，为了及时通过推送通知机制将命令传递到运行 iOS 操作系统的设备，需使用 Apple Push Notification Service (APNs)。如果用户在 iOS MDM 服务器上安装了 APNs 证书，创建了 iOS MDM 配置文件（其中包含用于将 iOS 移动设备连接到软件的设置集合），并将此配置文件安装在移动设备上，则表示用户同意以自动模式向 APNs 提供以下信息：

- 令牌 - 设备的推送令牌。服务器在向设备发送推送通知时使用此令牌。
- PushMagic - 推送通知中必须包含的字符串。字符串值由设备生成。

本地处理的数据

Kaspersky Security Center 设计用于在组织网络中集中执行基本的管理和维护任务。Kaspersky Security Center 为管理员提供组织网络安全级别详细信息的访问权限；Kaspersky Security Center 允许管理员配置基于 Kaspersky 应用程序的所有保护组件。Kaspersky Security Center 执行以下主要功能：

- 检测组织网络中的设备及其用户
- 创建用于设备管理的管理组层级
- 在设备上安装卡巴斯基应用程序
- 管理已安装应用程序的设置和任务
- 管理 Kaspersky 和第三方应用程序的更新，以及查找和修复漏洞
- 在设备上激活 Kaspersky 应用程序
- 管理用户账户
- 查看设备上的卡巴斯基应用程序运行信息
- 查看报告

为执行其主要功能，Kaspersky Security Center 可以接收、存储和处理以下信息：

- 通过扫描 Windows 域、 Active Directory 或 Samba 域控制器或通过扫描 IP 范围收到的有关组织网络上的设备的信息。管理服务器独立获取数据或从充当分发点的网络代理接收数据。
- 来自 Active Directory 和 Samba 的有关组织单位、域、用户和组的信息。管理服务器独立获取数据或从充当分发点的网络代理接收数据。
- 受管理设备详细信息。网络代理将下面列出的数据从设备传输到管理服务器。用户在管理控制台界面或 Kaspersky Security Center Web Console 界面中输入设备的显示名称和说明：
  - 用于设备识别的受管理设备及其组件的技术说明：设备显示名称和描述、Windows 域名和类型、 Windows 环境中的设备名称、DNS 域和 DNS 名称、IPv4 地址、IPv6地址、网络位置、MAC 地址、序号、操作系统类型、设备是否为虚拟机以及虚拟机监控程序类型，以及设备是否为动态虚拟机（作为 VDI 的一部分）。
  - 审计受管理设备以及就特定补丁和更新是否适用做出决策所需的受管理设备及其组件的其他说明：Windows 更新代理 (WUA) 状态、操作系统体系结构、操作系统供应商、操作系统内部版本号、操作系统发行版 ID、操作系统位置文件夹、虚拟机类型（如果设备是虚拟机）—虚拟机类型；管理设备的虚拟管理服务器的名称；云设备数据（云区域、VPC、云可用区域、云子网、云放置区）。
  - 受管理设备上的操作的详细信息：上次更新的日期和时间、设备在网络中最后一次可见的时间、重新启动等待状态以及设备打开的时间。
  - 设备用户账户及其工作会话的详细信息。
- 通过在受管理设备上运行远程诊断接收到的数据：跟踪文件、系统信息、设备上安装的卡巴斯基应用程序的详细信息、转储文件、事件日志、从卡巴斯基技术支持接收到的运行诊断脚本的结果。
- 分发点运行统计数据（如果设备是分发点）。网络代理将数据从设备传输到管理服务器。
- 用户在管理控制台或 Kaspersky Security Center Web Console 中输入的分发点设置。

- 将移动设备连接到管理服务器所需的数据：证书、移动连接端口、管理服务器连接地址。用户在管理控制台或 Kaspersky Security Center Web Console 中输入数据。
- 使用 iOS MDM 协议传输的移动设备详细信息。下面列出的数据从移动设备传输到管理服务器：
  - 用于设备识别的移动设备及其组件的技术说明：设备名称、型号、操作系统名称和内部版本号、设备型号、IMEI 号、UDID、MEID、序列号、内存数量、调制解调器固件版本、蓝牙 MAC 地址、Wi-Fi MAC 地址和 SIM 卡详细信息（作为 SIM 卡 ID 一部分的 ICCID）。
  - 受管理设备使用的移动网络详细信息：移动网络类型、当前使用的移动网络名称、家庭移动网络名称、移动网络操作员设置版本、语音漫游状态、数据漫游状态、家庭网络国家代码、居住国代码、当前使用的网络代码和加密级别。
  - 移动设备的安全设置：密码使用和其与策略设置的遵从、配置文件列表和用于安装第三方应用程序的 provisioning 配置文件。
  - 与管理服务器的上一次同步日期和设备管理状态。
- 设备上安装的 Kaspersky 应用程序的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器：
  - 受管理设备上安装的 Kaspersky 应用程序的设置：Kaspersky 应用程序名称和版本、状态、实时保护状态、上次设备扫描日期和时间、检测到的威胁数、无法清除的对象数、应用程序组件的可用性和状态、反病毒数据库的上次更新时间和版本、Kaspersky 应用程序设置和任务的详细信息、活动和备用授权许可密钥的信息、应用程序安装日期和 ID。
  - 应用程序操作统计信息：与受管理设备上的 Kaspersky 应用程序组件状态变化有关的事件和与应用程序组件发起的任务的性能有关的事件。
  - 卡巴斯基应用程序定义的设备状态。
  - Kaspersky 应用程序分配的标签。
  - Kaspersky 应用程序的已安装和适用的更新集合。
- Kaspersky Security Center 组件和 Kaspersky 受管理应用程序的事件中包含的数据。网络代理将数据从设备传输到管理服务器。
- 将 Kaspersky Security Center 与 SIEM 系统集成以进行事件导出所需的数据。用户在管理控制台或 Kaspersky Security Center Web Console 中输入数据。
- 策略和策略配置文件中显示的 Kaspersky Security Center 组件和 Kaspersky 受管理应用程序的设置。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。
- Kaspersky Security Center 组件和 Kaspersky 受管理应用程序的任务设置。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。
- 漏洞和补丁管理功能处理的数据。网络代理将下面列出的数据从设备传输到管理服务器：
  - 受管理设备上安装的应用程序和补丁的详细信息（应用程序注册表）。
  - 有关在受管理设备上检测到的硬件的信息（硬件注册表）。

如果网络代理安装在运行 Windows 的设备上，它会向管理服务器发送有关设备硬件的以下信息：

- RAM
- 大容量存储设备
- 主板
- CPU
- 网络适配器
- 监控器
- 视频适配器
- 声卡

如果网络代理安装在运行 Linux 或 macOS 的设备上，它会向管理服务器发送有关设备硬件的以下信息（如果该信息由操作系统提供）：

- 总 RAM 容量
- 大容量存储设备总容量
- 主板
- CPU
- 网络适配器

- 在受管理设备上检测到的第三方软件中的漏洞的详细信息。
- 受管理设备上安装的第三方应用程序的可用更新的详细信息。
- WSUS 功能发现的 Microsoft 更新的详细信息。
- WSUS 功能发现的必须在设备上安装的 Microsoft 更新列表。

- 在隔离的管理服务器上下载更新以修复受管理设备上的第三方软件漏洞所需的数据。用户使用管理服务器 klscflag 实用程序输入和传输数据。
- Kaspersky Security Center 在云环境（Amazon Web Services、Microsoft Azure、Google Cloud、Yandex Cloud）下工作所需的数据。用户在管理控制台或 Kaspersky Security Center Web Console 中输入数据。
- 应用程序的用户类别。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。
- “应用程序控制”功能在受管理设备上检测到的可执行文件的详细信息。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。相应应用程序的帮助文件中提供了完整的数据列表。
- 备份区中放置的文件的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。
- 隔离区中放置的文件的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- Kaspersky 专家为进行详细分析而请求的文件详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- 自适应异常控制规则的状态和触发的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- 安装或连接到受管理设备并被"设备控制"功能检测到的外部设备（内存单元、信息传输工具、信息硬拷贝工具和连接总线）的详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- 有关加密设备和加密状态的信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。

- 使用 Kaspersky 应用程序的数据加密功能在设备上执行的数据加密的错误详细信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- 受管理可编程逻辑控制器 (PLC) 列表。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- 创建威胁发展链所需的数据。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- 有关组织员工尝试访问云服务的信息。受管理应用程序通过网络代理将数据从设备传输到管理服务器。相应应用程序的帮助文件中提供了完整的数据列表。

- Kaspersky Security Center 与 Kaspersky Managed Detection and Response 服务集成（必须安装 Kaspersky Security Center Web Console 专用插件）所需的数据：集成启动令牌、集成令牌和用户会话令牌。用户在 Kaspersky Security Center Web Console 界面中输入集成启动令牌。Kaspersky MDR 服务通过专用插件传输集成令牌和用户会话令牌。

- 输入的激活码或指定的密钥文件的详细信息。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。

- 用户账户：名称、描述、全名、电子邮件地址、主要电话号码、密码、管理服务器生成的 secret key 以及用于两步验证的一次性密码。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。

- 身份和访问管理器在与 Kaspersky Security Center 集成的 Kaspersky 应用程序之间进行集中身份验证和提供单点登录 (SSO) 所需的数据：身份和访问管理器的安装和配置设置、身份和访问管理器用户会话、身份和访问管理器令牌、客户端应用程序状态和资源服务器状态。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。

- 管理对象的修订历史。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。

- 用户在其上创建修订的设备 IP 地址。IP 地址由管理服务器自动定义。

- 已删除的管理对象的注册表。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。

- 从文件创建的安装包以及安装设置。用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入数据。

- 在 Kaspersky Security Center Web Console 中显示 Kaspersky 公告所需的数据。用户在 Kaspersky Security Center Web Console 界面中输入数据。

- Kaspersky Security Center Web Console 中的受管理应用程序插件运行所需的数据，以及这些插件在常规运行期间保存在管理服务器数据库中的数据。相应应用程序的帮助文件中介绍了提供数据的描述和方式。

- Kaspersky Security Center Web Console 用户设置：界面的本地化语言和主题、监控面板显示设置、有关通知状态（已读/未读）的信息、电子表格中的列状态（显示/隐藏）、训练模式进度。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- Kaspersky Security Center 组件和 Kaspersky 受管理应用程序的卡巴斯基事件日志。卡巴斯基事件日志存储在每个设备上，永远不会传输到管理服务器。
- 受管理设备与 Kaspersky Security Center 组件的安全连接的证书。用户使用管理服务器 klsetsrvcert 实用程序输入数据。
- 用于对组织内部 Web 资源建立信任的证书。用户在 Kaspersky Security Center Web Console 界面中输入数据。
- Kaspersky Security Center 在云环境（例如 Amazon Web Services (AWS)、Microsoft Azure、Google Cloud 和 Yandex.Cloud）中运行所需的数据。管理服务器从运行它的虚拟机接收数据。
- 有关用户接受与 Kaspersky 的法律协议的条款和条件的信息。
- 用户在以下组件中输入的管理服务器数据：
  - 管理控制台
  - Kaspersky Security Center Web Console
  - 使用 klscflag 实用程序时的命令行终端
  - 通过 klakaut 自动化对象和 Kaspersky Security Center OpenAPI 与管理服务器交互的组件
- 用户在管理控制台或 Kaspersky Security Center Web Console 界面中输入的任何数据。

如果应用以下方法之一，则上面列出的数据可以在 Kaspersky Security Center 中显示：

- 用户在以下组件的界面中输入数据：
  - 管理控制台
  - Kaspersky Security Center Web Console
  - 使用 klscflag 实用程序时的命令行终端
  - 通过 klakaut 自动化对象和 Kaspersky Security Center OpenAPI 与管理服务器交互的组件
- 网络代理会自动从设备接收数据，并将其传输到管理服务器。
- 网络代理接收由 Kaspersky 受管理应用程序检索的数据，并将其传输到管理服务器。Kaspersky 受管理应用程序处理的数据列表在相应应用程序的帮助文件中提供。
- 管理服务器可独立获取有关联网设备的信息或从充当分发点的网络代理接收信息。
- 通过使用 iOS MDM 协议，数据从移动设备传输到管理服务器。

列出的数据存储在管理服务器数据库中。用户名和密码以加密格式存储。

上面列出的所有数据都只能通过 Dump 文件、跟踪文件或 Kaspersky Security Center 组件的日志文件（包括安装程序和实用程序创建的日志文件）传输到 Kaspersky。

Kaspersky Security Center 组件的 Dump 文件、跟踪文件和日志文件包含管理服务器、网络代理、管理控制台、iOS MDM 服务器和 Kaspersky Security Center Web Console 的随机数据。这些文件可能包含个人和敏感数据。Dump 文件、跟踪文件和日志文件以非加密形式存储在设备上。Dump 文件、跟踪文件和日志文件不会自动传输到 Kaspersky；然而，管理员可以在技术支持要求下手动传输数据到 Kaspersky 以便解决 Kaspersky Security Center 的操作问题。

单击管理控制台或 Kaspersky Security Center Web Console 中的链接，即表示用户同意自动传输以下数据：

- Kaspersky Security Center 代码
- Kaspersky Security Center 版本
- Kaspersky Security Center 本地化
- 授权许可 ID
- 授权许可类型
- 授权许可是否是通过合作伙伴购买的

通过每个链接提供的数据列表取决于链接的目的和位置。

Kaspersky 以匿名形式使用接收的数据，并且只用于常规统计。摘要统计根据原始收到的信息自动生成，不包含任何个人或机密数据。一旦积累了新数据，就会擦除以前的数据（一年一次）。摘要统计无限存储。

Kaspersky 按照法律和相应的 Kaspersky 规则来保护所收到的任何信息。数据均通过安全渠道传输。

Kaspersky Security Center 授权许可选项

Kaspersky Security Center 可以在以下模式中工作：

- **无需授权许可（基本功能）**

  在应用程序启动或者商业授权许可过期后，Kaspersky Security Center 以这种模式工作。在管理控制台基本功能支持下的 Kaspersky Security Center 作为保护企业网络的 Kaspersky 应用程序的一部分被传送。您也可以从卡巴斯基网站下载。

- **商业授权许可**

  如果需要不包括在管理控制台的基本功能中的其它功能，您必须购买商业授权许可。

  在管理服务器属性窗口中添加授权许可密钥时，请确保添加让您使用 Kaspersky Security Center 的授权许可密钥。您可以在 Kaspersky 网站上找到此信息。每个解决方案网页都包含该解决方案包括的应用程序列表。管理服务器可接受不受支持的授权许可密钥，例如Kaspersky Endpoint Security Cloud 的授权许可密钥，但此类授权许可密钥除了管理控制台的基本功能外，不提供任何新功能。

功能或属性	Kaspersky Security Center 操作模式	
	没有授权许可	商业授权许可
管理控制台的基本功能 下列功能可用： • 创建用于管理远程办公室网络或客户端组织网络的虚拟管理服务器。 • 创建一个管理组层级结构，作为一个单一实体管理特定设备。 • 远程安装应用程序。 • 对安装在客户端设备上的应用程序的集中配置。 • 控制组织的反病毒安全状态。 • 管理用户角色。 • 应用程序操作中的统计数据和报告，以及关于严重事件的通知。 • 集中化操作被移至隔离区和备份区的文件以及被推迟进程的文件。 • “加密和数据保护”管理。 • 查看和编辑现有的已授权的应用程序组。 • 查看和手动编辑网络轮询期间发现的硬件组件列表。 • 查看可用于远程安装的操作系统镜像的列表。	✓	✓
漏洞和补丁管理：基本功能 以下任务不需要商业授权许可： • *查找漏洞和所需更新*任务 通过此任务，Kaspersky Security Center 接收检测到的漏洞列表以及受管理设备上安装的第三方软件的所需更新列表。 • “*安装 Windows Update 更新*”任务 此任务只可用于安装 Windows Update 更新。要使用此任务，您必须在任务设置中手动指定所需的更新。 • *修复漏洞*任务 “*修复漏洞*”任务使用针对 Microsoft 软件的建议修补程序和针对第三方软件的用户修补程序。要使用此任务，您必须手动为任务设置中的漏洞指定用户修补程序。	✓	✓
漏洞和补丁管理：高级功能 下列功能可用： • 根据您定义的规则，远程安装软件更新并自动修复漏洞。 • 使用管理服务器作为 Windows 服务器更新服务 (WSUS) 服务器，以集中模式和设定频率为设备上的 Windows 更新服务提供更新。	—	✓

功能或属性	Kaspersky Security Center 操作模式	
	没有授权许可	商业授权许可
基于 MMC 的管理控制台中的移动设备管理功能 移动设备管理功能用于管理 iOS MDM 和 Android 移动设备。 以下功能适用于管理 iOS MDM 设备： • 添加 Kaspersky Security Center 管理下的新设备。 • 创建和编辑配置文件，在移动设备上安装配置文件。 • 通过 App Store®、使用清单文件 (.plist) 或使用移动安装包 (.ipa) 在移动设备上安装应用程序。 • 在 iOS MDM 设备上执行命令，包括锁定移动设备、重置移动设备密码以及从移动设备删除所有数据。 以下功能适用于管理 Android 设备： • 添加 Kaspersky Security Center 管理下的新设备。 • 通过策略管理 Kaspersky Endpoint Security for Android。 • 在设备上执行命令。 移动设备管理功能的管理单元是移动设备。移动设备连接到移动设备服务器之后，即被认定为受管理。	—	✓（必须将授权许可密钥添加到管理服务器属性中。）
Kaspersky Security Center Web Console 中的移动设备保护 Kaspersky Security Center Web Console 为您提供以下功能来管理安卓和 iOS 移动设备： • 添加 Kaspersky Security Center 管理下的新设备。 • 通过策略管理 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS。 • 通过相关协议发送命令到移动设备和执行命令。	—	✓（必须在每个移动设备上添加授权许可密钥。）
系统管理 下列功能可用： • 安装操作系统和应用程序。 Kaspersky Security Center 允许您创建操作系统镜像，以及将其部署在网络客户端设备上，也可以执行远程安装 Kaspersky 或其他供应商的应用程序。您可以从设备上捕捉操作系统镜像并将这些镜像传输至管理服务器。此类操作系统镜像将存储在管理服务器上的专用文件夹内。参考设备的操作系统镜像被捕获并通过安装包创建任务创建。您可以将获得的镜像部署在尚未安装操作系统的新联网设备上。在这种情况下将使用名为 Preboot eXecution Environment （PXE） 的技术。 • 已授权应用程序组管理。 • 通过名为远程桌面连接的 Microsoft® Windows® 组件远程连接到客户端设备的权限。 • 通过 Windows 桌面共享远程连接到客户端设备。 • 通过**卡巴斯基远程桌面会话查看器**进行远程连接。	—	✓

功能或属性	Kaspersky Security Center 操作模式	
	没有授权许可	商业授权许可
与云环境集成 Kaspersky Security Center 不仅适用于内部设备，还为云环境中的工作提供了特殊功能，例如云环境配置向导。Kaspersky Security Center 可与以下虚拟机一起使用： • Amazon EC2 实例 • Microsoft Azure 虚拟机 • Google Cloud 虚拟机实例 • Yandex.Cloud 虚拟机	—	✓
将事件导出到 SIEM 系统：使用 Syslog 协议 使用 Syslog 协议，您可以转发发生在 Kaspersky Security Center 管理服务器上和受管理设备上安装的 Kaspersky 应用程序中的任意事件。Syslog 协议是标准消息记录协议。您可以用它将事件导出到任何 SIEM 系统。	✓	✓

Kaspersky Security Center 和受管理应用程序的授权许可功能

管理服务器和受管理应用程序的授权许可涉及以下方面：

- 您仅可以添加授权许可密钥或有效激活码到管理服务器以激活“漏洞和补丁管理”、“移动设备管理”或“与 SIEM 系统集成”。Kaspersky Security Center 的某些功能只能根据活动密钥文件或添加到管理服务器的有效激活码来访问。
- 您可以为受管理应用程序添加多个激活码和密钥文件到管理服务器存储库。

关于 Kaspersky Security Center 授权许可

如果您使用密钥文件激活授权许可功能（例如，“移动设备管理”），但是您也想使用其他授权许可功能（例如，“漏洞和补丁管理”），您必须从您的服务提供商购买密钥文件以激活这两个功能，且您必须使用该密钥文件激活管理服务器。

受管理应用程序的授权许可功能

对于受管理应用程序的授权许可，激活码或密钥文件可以自动部署，或以其他任何便捷方法部署。以下方法可用以部署激活码或密钥文件：

- 自动部署

  如果您使用不同的受管理应用程序，且您必须将特定密钥文件或激活码部署到设备，请选择其他方法部署激活码或密钥文件。

Kaspersky Security Center 允许您自动部署可用授权许可密钥到设备。例如，三个授权许可密钥被存储在管理服务器存储库。您已为所有三个授权许可密钥选择了**自动分发授权许可密钥到受管理设备**复选框。Kaspersky 安全应用程序—例如，Kaspersky Endpoint Security for Windows— 被安装到组织设备。发现必须部署授权许可密钥的新设备。比如，应用程序确定存储库中的以下两个授权许可密钥可以部署到设备：授权许可密钥 *Key_1* 和授权许可密钥 *Key_2*。这些授权许可密钥之一被部署到设备。此种情况下，无法预见两个授权许可密钥中的哪个将被部署到设备，因为自动部署授权许可密钥不提供给任何管理员活动。

当部署授权许可密钥时，设备为该授权许可密钥重新计算。您必须确保部署授权许可密钥的设备数量不超过授权许可限制。如果设备数量超过授权许可限制，所有不被授权许可覆盖的设备将被分配*严重*状态。

- 添加密钥文件或激活码到受管理应用程序安装包

  如果您使用安装包安装受管理应用程序，您可以在该安装包中或在应用程序策略中指定激活码或密钥文件。授权许可密钥将在下一次设备与管理服务器同步时被部署到受管理应用程序。

- 通过为受管理应用程序添加授权许可密钥任务来进行部署

  如果您选择使用为受管理应用程序添加授权许可密钥任务，您可以选择要部署到设备的授权许可密钥并以任何便捷的方法选择设备—例如，通过选择管理组或设备分类。

- 手动添加激活码或密钥文件到设备

Kaspersky 应用程序。集中部署

该部分描述了远程安装 Kaspersky 应用程序和从网络设备卸载它们的方法。

在客户端设备上部署应用程序之前，请确保客户端设备的硬件和软件满足相应的要求。

网络代理是一个给客户端设备提供管理服务器连接的组件。因此，它必须安装在要连接到远程集中控制系统的每个客户端设备上。安装有管理服务器的设备只能使用服务器版的网络代理。该版本包括在管理服务器中，与管理服务器一起安装和删除。在该设备中无需安装网络代理。

网络代理可以象应用程序那样远程安装或本地安装。在通过管理控制台集中安装安全应用程序期间，您可以随安全应用程序一起安装网络代理。

网络代理根据相应的 Kaspersky 应用程序不同而不同。在某些情况下，网络代理只能本地安装（有关详细信息，请参阅响应的应用程序的文档）。您仅必须安装网络代理到客户端设备一次。

Kaspersky 应用程序 使用管理插件通过管理控制台管理。因此，要通过 Kaspersky Security Center 访问应用程序管理界面，必须在管理员工作站上安装相应管理插件。

您可以在管理员工作站的 Kaspersky Security Center 主窗口执行应用程序远程安装。

要远程安装软件，您必须创建远程安装任务。

创建的远程安装任务将根据计划启动。您可以手动停止任务，来中断安装过程。

如果应用程序的远程安装返回错误，请确保满足设备准备要求。

您可以使用部署报告来跟踪 Kaspersky 程序的远程安装进度。

关于 Kaspersky Security Center 列出的应用程序的管理的详细信息，请参阅相应应用程序的文档。

替换第三方安全应用程序

通过 Kaspersky Security Center 进行 Kaspersky 安全应用程序的安装可能需要卸载与正在安装的应用程序不兼容的第三方软件。Kaspersky Security Center 提供几种卸载第三方应用程序的方法。

通过使用安装程序卸载不兼容应用程序

该选项仅在基于 Microsoft 管理控制台的管理控制台可用。

卸载不兼容应用程序的安装程序方法被各种应用程序支持。如果在该安全应用程序安装包的属性窗口中选中了（“**不兼容的应用程序**”区域）“**自动卸载不兼容的应用程序**”选项，在安全应用程序安装之前，所有不兼容的应用程序被自动卸载。

当配置应用程序远程安装时卸载不兼容应用程序

您可以在配置安全应用程序远程安装时启用“**自动卸载不兼容的应用程序**”选项。在基于 Microsoft Management Console（MMC） 的管理控制台，该选项在远程安装向导可用。在 Kaspersky Security Center Web Console，您可以在保护部署向导中找到该选项。当该选项被启用时，Kaspersky Security Center 在安装安全应用程序到受管理设备之前卸载不兼容的应用程序。

说明：

- 管理控制台：使用远程安装向导移除不兼容的应用程序
- Kaspersky Security Center Web Console：安装前卸载不兼容的应用程序

通过专用任务卸载不兼容的应用程序

要卸载不兼容的应用程序，使用**远程卸载应用程序**任务。该任务应该在安全应用程序安装任务运行之前运行在设备。例如，在安装任务中，您可以选择计划类型“**在完成其他任务时**”，这里，其他任务就是“**远程卸载应用程序**”。

该卸载方法在安全应用程序无法正确卸载不兼容应用程序时是很有用的。

管理控制台操作说明：创建任务。

使用远程安装任务安装应用程序

Kaspersky Security Center 允许您远程安装应用程序到设备，使用远程安装任务。那些任务通过专门向导被创建被分配到设备。要更快和更便捷地分配任务，您可以在向导窗口中指定设备（最多 1000 部设备），使用以下方法之一：

- **选择管理服务器检测到的网络设备**。此种情况下，任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。
- **手动指定设备地址或从列表导入地址**。您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定预定义分类或您所创建的自定义分类。
- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。

为了避免在未安装网络代理的客户端设备上安装应用程序时可能出现的问题，您必须按照通过 Kaspersky Security Center 的远程安装任务强制部署中所述进行操作。

安装应用程序到所选设备

要安装应用程序到所选设备：

1. 在控制台树中，选择“**任务**”文件夹。
2. 单击“**创建任务**”按钮，执行任务创建。

   “新任务向导”启动。遵照向导的说明操作。

   在新任务向导的“**选择任务类型**”窗口的 **Kaspersky Security Center 管理服务器**节点中，选择“**远程安装应用程序**”作为任务类型。

   新任务向导将在特定设备上创建一组远程安装所选应用程序的任务。新创建的任务显示在“**任务**”文件夹工作区。
3. 手动运行任务，或者等待按任务设置中的计划来启动任务。

远程安装任务完成时，所选应用程序将安装在所选设备上。

在管理组中的客户端设备上安装应用程序

要在管理组中的客户端客户端设备上安装应用程序：

1. 连接控制相关管理组的管理服务器。
2. 在控制台树中选择管理组。
3. 在组工作区中，选择“**任务**”选项卡。
4. 单击“**创建任务**”按钮，执行任务创建。

"新任务向导"启动。遵照向导的说明操作。

在新任务向导的"**选择任务类型**"窗口的 **Kaspersky Security Center 管理服务器**节点中，选择"**远程安装应用程序**"作为任务类型。

新任务向导将创建一个远程安装所选应用程序的组任务。新任务将显示在"**任务**"选项卡的管理组工作区中。

5. 手动运行任务，或者等待按任务设置中的计划来启动任务。

远程安装任务完成时，所选应用程序将安装在管理组中的客户端设备上。

通过活动目录组策略安装应用程序

Kaspersky Security Center 允许您使用 Active Directory 组策略在受管理设备上安装 Kaspersky 应用程序。

使用 Active Directory 组策略，可以只从包含网络代理的安装包安装应用程序。

要使用活动目录组策略安装应用程序，请执行以下操作：

1. 开始使用远程安装向导配置应用程序安装。
2. 在"远程安装向导"的"**定义远程安装任务设置**"窗口中，选中"**在 Active Directory 组策略中指定安装包的安装**"选项。
3. 在远程安装向导的**选择账户以访问设备**窗口，选择**需要账户(不使用网络代理)**选项。
4. 在安装了 Kaspersky Security Center 的设备上添加带有管理员权限的账户或包含在"组策略创建器所有者"域组的账户。
5. 为所选账户授予权限：
   a. 转到"**控制面板**"→"**管理工具**"，然后打开"**组策略管理**"。
   b. 单击具有所需域的节点。
   c. 单击"**委派**"区域。
   d. 在"**权限**"下拉列表中，选择"**链接 GPO**"。
   e. 单击**添加**。
   f. 在打开的"**选择用户、计算机或组**"窗口中，选择所需账户。
   g. 单击"**确定**"关闭"**选择用户、计算机或组**"窗口。
   h. 在"**组和用户**"列表中，选择刚添加的账户，然后单击"**高级**"→"**高级**"。
   i. 在"**权限条目**"列表中，双击刚添加的账户。
   j. 授予以下权限：
      - **创建组对象**
      - **删除组对象**

- **创建组策略容器对象**
- **删除组策略容器对象**

k. 单击“**确定**”保存更改。

6. 按照向导的说明定义其他设置。
7. 手动运行创建的远程安装任务，或等待计划启动。

这将启动以下远程安装序列：

1. 任务运行时，系统将在包含指定集合中的客户端设备的每个域中创建以下对象：
   - 名称 **Kaspersky_AK{GUID}** 下的组策略对象（GPO）。
   - 对应于 GPO 的安全组。此安全组包括该任务涵盖的客户端设备。安全组的内容定义了 GPO 的范围。
2. Kaspersky Security Center 直接从应用程序的名为“KLSHARE”的共享网络文件夹在客户端设备上安装所选 Kaspersky 应用程序。在 Kaspersky Security Center 安装文件夹中，系统将创建一个辅助子文件夹，其中包含安装应用程序所需的 .msi 文件。
3. 新设备添加到任务范围后，会在任务下次启动后添加到安全组。如果在任务计划中选中“**运行错过的任务**”选项，则设备将立即添加到安全组。
4. 设备从任务范围中删除后，会在任务下次启动后从安全组中删除。
5. 从 Active Directory 中删除任务后，GPO、GPO 的链接和相应的安全组也会删除。

如果要使用 Active Directory 应用其他安装方案，您可以手动配置所需设置。例如，以下情况可能需要该操作：

- 当反病毒保护管理员没有权限更改某些域的活动目录时
- 原始安装包必须存储在单独的网络资源上时
- 当需要将 GPO 链接到特定的活动目录单元时

通过活动目录使用备用安装方案的以下选项可用：

- 如果直接从 Kaspersky Security Center 共享文件夹进行安装，您必须在 GPO 属性中为所需应用程序指定 .msi 文件（位于安装包的 exec 子文件夹中）。
- 如果必须将安装包放置在其他网络资源上，您必须将整个 exec 文件夹的内容复制过去，因为除了扩展名为 .msi 的文件外，该文件夹还包含创建安装包时生成的配置文件。要安装与该程序相关联的授权许可密钥，请将许可文件一起复制到该文件夹中。

在 macOS 设备上远程安装应用程序

要使用远程安装任务在运行 macOS 的设备上安装应用程序：

1. 创建一个由安装包和 .sh 安装脚本组成的压缩档案。
2. 在“新任务向导”中禁用“**下载之前验证操作系统类型**”选项。

或者，您可以使用**远程执行脚本**任务。以下文章介绍了如何为此任务配置文件：使用远程执行脚本任务在设备上远程安装应用程序。

在从属管理服务器上安装应用程序

要在从属管理服务器上安装应用程序：

1. 与控制相关从属管理服务器的管理服务器建立连接。
2. 确保每个所选的从属管理服务器上都有与要安装的应用程序对应的安装包。如果任何从属服务器缺少安装包，请使用安装包分发任务进行分发。
3. 以下列方式之一，创建在从属管理服务器安装应用程序的任务：
   - 如果要为所选管理组中的从属管理服务器创建任务，请为该组创建远程安装组任务。
   - 如果您要为特定从属管理服务器创建任务，请为特定设备创建远程安装任务。

   部署任务创建向导启动，来指导您创建远程安装任务。遵照向导的说明操作。

   在新任务向导的“**选择任务类型**”窗口的“**Kaspersky Security Center 管理服务器**”区域中，打开“**高级**”文件夹，然后选择“**将应用程序远程安装到从属管理服务器**”作为任务类型。

   新任务向导将创建在特定从属管理服务器上远程安装所选应用程序的任务。
4. 手动运行任务，或者等待按任务设置中的计划来启动任务。

远程安装任务完成时，所选应用程序将安装在特定的从属管理服务器上。

使用远程安装向导安装应用程序

要安装卡巴斯基应用程序，您可以使用远程安装向导。远程安装向导允许使用特别创建的安装包或直接从分发包来远程安装应用程序。

要想在未安装网络代理的客户端设备上正确进行远程安装，必须打开下列端口：TCP 139 和 445；UDP 137 和 138。默认情况下，域中所有设备的这些端口均已打开。如果出现网络错误，请参阅 Kaspersky Security Center 知识库。

要使用远程安装向导将应用程序安装到所选设备上：

1. 在控制台树中，找到“**远程安装**”文件夹并选择“**安装包**”子文件夹。
2. 在该文件夹的工作区，选择您要安装的应用程序的安装包。
3. 在安装包的上下文菜单中，选择“**安装应用程序**”。

   远程安装向导启动。

4. 在“**选择设备以安装**”窗口中，您可以创建安装了该应用程序的设备列表：

- **安装到受管理设备组**

  如果选择该选项，程序将为该设备组创建远程安装任务。

- **选择设备以安装**

  如果选择该选项，程序将为指定的设备创建远程安装任务。这些特定设备可以包含受管理的设备和未分配的设备。

5. 在“**定义远程安装任务设置**”窗口，指定应用程序远程安装设置。

   在“**强制下载安装包**”设置组中，指定如何将安装程序所需的文件分发到客户端设备中。

- **使用网络代理**

  如果启用此选项，安装包通过安装在客户端设备上的网络代理传送到客户端设备。

  如果禁用此选项，则使用客户端的操作系统传送安装包。

  如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。

  默认情况下已启用该选项。

- **通过管理服务器使用操作系统资源**

  如果启用此选项，文件将使用客户端设备的操作系统工具通过管理服务器传送到客户端设备。如果客户端设备上未安装网络代理，但是客户端设备与管理服务器在同一网络，则可以启用此选项。

  默认情况下已启用该选项。

- **通过分发点使用操作系统资源**

  如果启用此选项，安装包使用操作系统工具通过分发点传送到客户端设备。如果网络中存在不止一个分发点，那么您可以选择本选项。

  如果启用“**使用网络代理**”选项，仅在网络代理工具不可用时才通过操作系统工具传送文件。

  默认情况下，已经为虚拟管理服务器上创建的远程安装任务启用此选项。

- **尝试安装的次数**

  如果，运行远程安装任务时，Kaspersky Security Center 安装应用程序到受管理设备失败不超过指定次数，Kaspersky Security Center 停止传送安装包到该受管理设备且不再在该设备上启动安装程序。

  “尝试安装的次数”选项允许您节省受管理设备资源，以及减少流量（卸载、MSI 文件运行和错误消息）。

  重复的任务启动尝试可能提示设备具有妨碍安装的问题。管理员应该在指定安装尝试次数内解决该问题（例如，通过分配足够磁盘空间、卸载不兼容的应用程序或修改妨碍安装的其他应用程序设置）并重启任务（手动或按计划）。

  如果安装始终未完成，问题被视为无法解决且后续任务启动被认为是不必要的资源和流量浪费。

当任务被创建时，尝试次数被设置为`0`。返回错误的安装程序的每次运行都增加计数。

如果指定的尝试次数被超过且设备已准备好应用程序安装，您可以增加**尝试安装的次数**参数的值并启动任务以安装应用程序。或者，您可以创建新的远程安装任务。

定义由其他管理服务器管理的客户端设备做什么：

- **在所有设备上安装**

  应用程序将被安装到由其他管理服务器管理的设备。
  默认情况下已选中该选项。如果您在网络中只有一台管理服务器，您不必更改该设置。

- **仅安装到通过该管理服务器管理的设备**

  应用程序将仅被安装到由该管理服务器管理的设备。如果您在网络中有多个管理服务器且需要避免它们之间的冲突，请选择该选项。

定义附加设置：

- **如果已经安装应用程序则不再重新安装**

  如果启用此选项，则如果选定的应用程序已安装到该客户端设备上，将不再重新安装它。
  如果禁用此选项，仍将安装应用程序。
  默认情况下已启用该选项。

- **在活动目录组策略中指定安装包的安装**

  如果启用此选项，安装包将使用 Active Directory 组策略进行安装。
  如果选择网络代理安装包，则该选项可用。
  默认情况下已禁用该选项。

6. 在**选择授权许可密钥**窗口，选择授权许可密钥和分发方法：

- **不将授权许可密钥放置到安装包(推荐)**

  密钥被自动分发到所兼容的所有设备：
  - 如果自动分发在密钥属性中启用。
  - 如果**添加密钥**任务已创建。

- **将授权许可密钥放置到安装包**

  密钥与安装包一起被分发到设备。

  我们不建议您使用该方法分发密钥，因为将启用对安装包存储库的共享读取访问权限。

如果安装包不包含授权许可密钥，**选择授权许可密钥**窗口将显示出来。

如果安装包中包含授权许可密钥，则会显示“**授权许可密钥属性**”窗口，其中包含授权许可密钥的详情。

7. 在**选择操作系统重启选项**窗口，指定安装应用程序时需要重启操作系统时设备是否被重启：

- **不重启设备**

  如果选择该选项，安全应用程序安装后设备不被重启。

- **重启设备**

  如果选择该选项，安全应用程序安装后设备将被重启。

- **提示用户操作**

  如果选中该选项，则在安装安全应用程序后，会向用户显示通知，告知用户需要重启设备。使用“**修改**”链接，您可以修改消息文本、消息显示期限和自动重启时间。

  默认情况下已选定该选项。

- **强行关闭锁定会话中的应用程序**

  如果启用此选项，已阻止的设备上的应用程序将在重启前被强制关闭。

  默认情况下已禁用该选项。

8. 在**选择账户以访问设备**窗口，您可以添加用于启动远程安装任务的账户：

- **不需要账户(网络代理已安装)**

  如果该选项被选中，您不是必须指定一个账户，并在该账户下运行程序的安装。将使用运行管理服务器服务的账户运行该任务。

  如果网络代理未安装在客户端设备上，该选项不可用。

- **需要账户(不使用网络代理)**

  如果您为其分配远程安装任务的设备上未安装网络代理，请选择此选项。在这种情况下，您可以指定用户账户或 SSH 证书来安装应用程序。

  - **本地账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地账户**，然后指定用户账户凭据。

    您可以指定多个用户账户，例如，没有一个账户拥有分配任务所对应的所有设备上的全部所需权限时。在此情况下，已经添加的所有账户都用于从上到下按顺序运行该任务。

  - **SSH 证书**。如果要在基于 Linux 的客户端设备上安装应用程序，您可以指定 SSH 证书而不是用户账户。单击**添加**按钮，选择**SSH 证书**，然后指定证书的私钥和公钥。

    要生成私钥，您可以使用 ssh-keygen 实用程序。请注意，Kaspersky Security Center 支持 PEM 格式的私钥，但 ssh-keygen 实用程序默认生成 OPENSSH 格式的 SSH 密钥。Kaspersky Security Center 不支持 OPENSSH 格式。要以支持的 PEM 格式创建私钥，请在 ssh-keygen 命令中添加“-m PEM”选项。例如：

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
```

9. 在“**开始安装**”窗口，点击**下一步**按钮在所选设备上创建和启动远程安装任务。

   如果“**开始安装**”窗口中选中了“**在远程安装向导完成后不运行任务**”选项，远程安装任务将不启动。您可以以后手动启动此任务。对应于应用程序安装包名称的任务名称：**<安装包名称>的安装**。

要使用远程安装向导将应用程序安装到管理组设备上：

1. 连接控制相关管理组的管理服务器。
2. 在控制台树中选择管理组。
3. 在组的工作区，点击“**执行操作**”按钮并在下拉列表中选择“**安装应用程序**”。

   此操作将启动应用程序远程安装向导。遵照向导的说明操作。
4. 在此向导的最后一步，单击“**下一步**”，创建并启动所选设备上的远程安装任务。

当远程安装向导完成时，Kaspersky Security Center 执行以下操作：

- 为应用程序安装创建安装包（如果之前未创建）。安装包位于“**远程安装**”文件夹的“**安装包**”子文件夹中，其名称与应用程序的名称和版本相对应。在将来，您可以使用该安装包安装程序。
- 为特定设备或管理组创建并启动远程安装任务。新创建的远程安装任务存储于“**任务**”文件夹中，或被添加至为管理组创建的任务中。您可以以后手动启动此任务。对应于应用程序安装包名称的任务名称：**<安装包名称>的安装**。

使用管理插件

Kaspersky 应用程序使用管理插件通过管理控制台管理。每个可以通过 Kaspersky Security Center 管理的 Kaspersky 应用程序都包含一个管理插件。使用应用程序管理插件，可以在管理控制台中执行以下操作：

- 创建和编辑应用程序策略和设置以及应用程序任务的设置。
- 获取有关应用程序任务和应用程序事件的信息，以及从客户端设备接收的应用程序操作统计信息。

查看已安装插件及其版本列表：

1. 在管理控制台树中，右键单击**管理服务器<Server_name>**，然后选择**属性**。
2. 单击**高级 → 有关已安装应用程序管理插件的详情**。

已安装的管理插件及其版本的列表显示在右侧窗格中。

在 Kaspersky Security Center 初始设置期间运行管理服务器快速启动向导时，您可以安装受管理应用程序的插件。此外，您还可以手动安装管理插件。

手动安装管理插件：

1. 从卡巴斯基技术支持网页下载卡巴斯基应用程序的管理插件和所需版本（例如 Kaspersky Endpoint Security for Windows 12.6）。
2. 如果管理控制台正在运行，请将其关闭。

3. 解压下载的插件文件并运行 klcfginst.msi 或 klcfginst.exe 文件。按照安装向导的说明进行操作。

4. 安装完成后，运行管理控制台并确保该插件显示在已安装插件列表中，如上一过程中所述。

安装支持受管理应用程序快速启动向导的管理插件后，运行管理控制台时，该向导将自动启动。您可以按照受管理应用程序快速启动向导的步骤创建默认的卡巴斯基应用程序策略和任务。仅当您在初始安装插件后运行管理控制台，或将管理插件更新为与尚未创建任务和策略的卡巴斯基应用程序的其他版本兼容的版本后，该向导才会自动启动。您也可以手动启动受管理应用程序快速启动向导。

要手动启动受管理应用程序快速启动向导：

1. 在控制台树中，选择**管理服务器**节点。

2. 在管理服务器节点的上下文菜单中，选择“**所有任务**”→“**受管理应用程序快速启动向导**”。

3. 受管理应用程序快速启动向导将启动。按照向导步骤创建默认的卡巴斯基应用程序策略和任务。

要删除管理插件：

1. 如果管理控制台正在运行，请将其关闭。

2. 打开 Windows 注册表编辑器。

3. 找到以下密钥：

   - 32 位系统：`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins`。
   - 64 位系统：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins`。

   该密钥包含已安装的管理插件。对于每个插件，`DisplayName`值包含插件名称，`UninstallString`值包含卸载插件的命令。

4. 找到要卸载的插件的密钥，并将其`UninstallString`值复制到剪贴板。

5. 将值粘贴到命令字符串中并使用系统管理员权限运行它。

管理插件版本不得早于卡巴斯基受管理应用程序版本。如果您更新设备上的卡巴斯基应用程序，则必须安装相同版本的管理插件。

当您打开在早期版本的插件中创建的策略时，系统将要求您接受卡巴斯基安全网络声明。

当您卸载 Kaspersky Security Center Web Console 时，所有管理插件也会被卸载。

如果您在高于受管理应用程序版本的插件版本中打开并保存策略，则策略将被更新，并且您将无法在早期版本的插件中打开它。

查看保护部署报告

您可以使用“保护部署报告”来监控网络保护部署的进度。

要查看保护部署报告：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 在“**报告**”文件夹工作区中，选择名为“**保护部署报告**”的报告模板。

工作区将显示报告。该报告包含网络中所有设备的保护部署信息。

您可以生成新的保护部署报告，并制定该报告中要包含的数据类型：

- 用于管理组
- 用于特定设备
- 用于设备分类
- 用于所有设备

如果安全应用程序被安装并且实时保护被启用，Kaspersky Security Center 认定保护已被部署在设备。

应用程序的远程卸载

Kaspersky Security Center 允许您从设备远程卸载应用程序，通过远程卸载任务。那些任务通过专门向导被创建被分配到设备。要更快和更便捷地分配任务到设备，您可以在向导窗口中指定设备，使用以下方法之一：

- **选择管理服务器检测到的网络设备**。此种情况下，任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。
- **手动指定设备地址或从列表导入地址**。您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定预定义分类或您所创建的自定义分类。
- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。

远程移除问题

当进行远程移除第三方应用程序时，管理员可能会遇到警告说，“远程卸载已在该设备上结束，但是有警告：要移除的应用程序未安装。”该问题通常发生在要移除的应用程序仅为当前登录的单个用户安装。如果用户未登录，此类应用程序将不可见，无法远程移除。

该行为与同一设备上供多个用户使用的应用程序不同，对于后者应用程序全球可见，可供设备的所有用户访问。

在 Kaspersky Security Center 内，应用程序注册表算法用不同方式处理供单个用户使用的应用程序和供多个用户使用的应用程序：

- 多用户应用程序在实时、最新的安装应用程序列表内进行维护。
- 单用户应用程序使用缓存机制进行监控。

  如果用户在应用程序检测时登录，Kaspersky Security Center 会缓存关于该用户的应用程序的信息。即时用户随后退出，Kaspersky Security Center也会根据缓冲的数据继续将这些应用程序显示为已安装，尽管它们不再在设备上可见或可供访问。

该差异可能会导致 Kaspersky Security Center 根据缓冲的数据将应用程序识别为已安装而应用程序移除任务失败，因为当用户退出时应用程序无法访问。

默认情况下，缓冲的应用程序数据的生命周期被设为 30 天。管理员可以修改此设置以缩短缓冲持续时长，从而将显示的数据和设备上实际的应用程序可见性之间的差异降到最低程度。

要将缓冲生命周期调整到 1 小时（3600 秒钟），请在管理服务器上运行以下命令：

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

运行此命令后，重启管理服务器以便更改生效。

有关安装的应用程序的信息源

网络代理可从以下注册表键值提取有关 Windows 设备上安装的软件的信息：

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为所有用户安装的应用程序的信息。
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为所有用户安装的应用程序的信息。
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为当前用户安装的应用程序的信息。
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为特定用户安装的应用程序的信息。

从管理组的客户端设备中远程卸载应用程序

要从管理组的客户端设备中远程卸载应用程序：

1. 连接控制相关管理组的管理服务器。
2. 在控制台树中选择管理组。
3. 在组工作区中，选择“**任务**”选项卡。

4. 单击“**新任务**”按钮，执行任务创建。

   “新任务向导”启动。遵照向导的说明操作。

   在新任务向导“**选择任务类型**”窗口的 **Kaspersky Security Center 管理服务器**节点中，在“**高级**”文件夹中选择“**远程卸载应用程序**”作为任务类型。

   新任务向导将创建一个远程部署所选应用程序的组任务。新任务将显示在“**任务**”选项卡的管理组工作区中。

5. 手动运行任务，或者等待按任务设置中的计划来启动任务。

远程卸载任务完成时，所选应用程序将从管理组中的客户端设备中删除。

从所选设备中远程卸载应用程序

要从所选设备中远程卸载应用程序：

1. 在控制台树中，选择“**任务**”文件夹。

2. 通过单击“**新任务**”来运行任务创建。

   “新任务向导”启动。遵照向导的说明操作。

   在新任务向导“**选择任务类型**”窗口的 **Kaspersky Security Center 管理服务器**节点中，在“**高级**”文件夹中选择“**远程卸载应用程序**”作为任务类型。

   新任务向导将创建一个从特定设备上远程卸载所选应用程序的任务。新创建的任务显示在“**任务**”文件夹工作区。

3. 手动运行任务，或者等待按任务设置中的计划来启动任务。

远程卸载任务完成时，所选应用程序从特定的设备中卸载。

使用安装包

创建远程安装任务时，系统将使用包含必要的软件安装参数的安装包。

> 安装包可能包含密钥文件。我们建议您避免共享对包含密钥文件的安装包的访问。

您可以多次使用同一个安装包。

管理服务器创建的安装包将被移至控制台树且位于“**远程安装**”文件夹下的“**安装包**”子文件夹中。安装包存储于管理服务器的共享文件夹下的“Package”子文件夹中。

如果需要，您可以按照**删除对象安装包**安装包子文件夹中删除安装包。

> 请勿手动更改共享文件夹中安装包的内容。如果需要，您可以创建安装包的副本，进行必要的更改，并创建新的安装任务。

创建安装包

本文介绍了创建以下类型的安装包的过程：

- 卡巴斯基应用程序的安装包
- 指定的可执行文件的安装包
- 来自卡巴斯基数据库的应用程序安装包

> 您不需要手动创建安装包以远程安装网络代理。它会在 Kaspersky Security Center 安装期间自动创建并存储在“**安装包**”文件夹中。如果用于远程安装网络代理的安装包已经被删除，您可以通过在 Kaspersky Security Center 分发包的“NetAgent”文件夹中选择“nagent.kud”文件重新创建。

要创建安装包：

1. 连接至必要的管理服务器。
2. 在控制台树中，选择**高级 → 远程安装 → 安装包**。
3. 以下列方法之一开始创建新的安装包：
   - 右键单击**安装包**文件夹，然后从上下文菜单中选择**新建→安装包**。
   - 在安装包列表的空白处单击鼠标右键，然后从上下文菜单中选择**创建→安装包**。
   - 在安装包列表管理区域，单击“**创建安装包**”。

   新安装包向导启动。
4. 单击相应的图标选择以下安装包类型之一：
   - 卡巴斯基应用程序的安装包。
   - 指定的可执行文件的安装包。
   - 来自卡巴斯基数据库的应用程序安装包。
5. 指定要创建的安装包的名称。
   您可以指定任何名称。
6. 通过以下方式之一选择要为其创建安装包的应用程序或可执行文件：
   - 单击**浏览**按钮，然后在标准 Windows**打开**窗口中，选择位于可用磁盘上的所需应用程序的分发包。
     如果您选择为卡巴斯基应用程序或指定的可执行文件创建安装包，则此选项适用。
   - 单击**浏览**按钮，然后在**选择应用程序**窗口中选择所需应用程序的分发包。
     如果您选择从卡巴斯基数据库为应用程序创建安装包，则此选项适用。

如果您正在为管理服务器创建安装包，请选择 sc.kud 文件。sc.kud 文件位于 Kaspersky Security Center 分发包的根文件夹中。

不在安装包参数中显示授权账户的任何细节。

7. 审阅最终用户授权许可协议和隐私策略。

   在为应用程序创建安装包时，您可能会被提示查看并接受该应用程序的最终用户授权许可协议和隐私政策。

   阅读这两份文件。如果您同意授权许可协议和隐私政策的所有条款，请通过选中相应的复选框进行接受。

   您的设备上的应用程序安装将继续，安装包创建将恢复。

   当创建 Kaspersky Endpoint Security for Mac 的安装包时，您可以选择最终用户授权许可协议和隐私策略的语言。

8. 如有必要，启用系统组件自动安装。

   如果您正在从卡巴斯基数据库为应用程序创建安装包，则可以启用必要系统组件自动安装。新安装包向导显示所选程序的所有可用的系统组件列表。任何时候您都可以在安装包属性中访问此列表。

   如果您正在创建补丁安装包，则该列表包括部署此补丁所需的所有系统组件。

9. 单击**完成**按钮即可完成包创建过程。

新安装包向导完成后，新安装包将显示在控制台树的“**安装包**”文件夹的工作区中。

创建独立安装包

您和组织中的设备用户可以使用独立安装包在设备上手动安装应用程序。

独立安装包是一个可执行文件 (installer.exe)，您可以将其存储在 Web 服务器或共享文件夹中，或通过其他方法传输到客户端设备。您也可以通过电子邮件发送独立安装包的链接。在客户端设备上，用户可以在本地运行接收到的文件以安装应用程序，而无需涉及 Kaspersky Security Center。

确保独立安装包不可用于未经授权的人员。

您可以为 Kaspersky 应用程序以及适用于 Windows、macOS 和 Linux 平台的第三方应用程序创建独立安装包。要为第三方应用程序创建独立安装包，必须首先创建一个自定义安装包。

创建独立安装包的源是管理服务器上已创建列表中的安装包。

要创建独立安装包：

1. 在控制台树中，选择**管理服务器 → 高级 → 远程安装 → 安装包**。

   此时会显示管理服务器上可用的安装包的列表。

2. 在安装包列表中，选择要为其创建独立包的安装包。

3. 在上下文菜单中，选择**创建独立安装包**。

   独立安装包创建向导启动。使用**下一步**按钮进行向导。

4. 在向导的第一页上，如果您选择了 Kaspersky 应用程序安装包，并且希望将网络代理与所选应用程序一起安装，请确保“**网络代理和该应用程序一起安装**”选项已启用。

   默认情况下已启用该选项。如果您不确定设备上是否安装了网络代理，建议启用此选项。如果设备上已经安装了网络代理，则在安装带有网络代理的独立安装包之后，网络代理将更新为较新的版本。

   如果禁用此选项，则网络代理将不会安装在设备上，并且该设备将不受管理。

   如果管理服务器上已经存在用于所选应用程序的独立安装包，则向导会通知您这一事实。在这种情况下，您必须选择以下操作之一：

   - **创建独立安装包**。例如，如果要为新的应用程序版本创建独立安装包，并且还希望保留为先前的应用程序版本创建的独立安装包，请选择此选项。新的独立安装包位于另一个文件夹中。
   - **使用现有的独立安装包**。如果要使用现有的独立安装包，请选择此选项。安装包创建过程将不会开始。
   - **重新编译现有的独立安装包**。如果要再次为同一应用程序创建独立安装包，请选择此选项。独立安装包位于同一文件夹中。

5. 在向导的下一页上，选择“**将未分配的设备移动到此组**”选项，并指定在安装网络代理后要将客户端设备移至的管理组。

   默认情况下，设备移至“**受管理设备**”组。

   如果您不想在网络代理安装后将客户端设备移至管理组，请选择“**不移动设备**”选项。

6. 在向导的下一页上，当完成独立安装包创建过程时，将显示独立包创建的结果以及独立包的路径。

   您可以单击链接并执行以下任一操作：

   - 打开含有独立安装包的文件夹。
   - 通过电子邮件发送已创建的独立安装包的链接。要执行此操作，您必须启动电子邮件应用程序。
   - 用于在网站上发布链接的示例 HTML 代码。在与 TXT 格式关联的应用程序中创建并打开 TXT 文件。在该文件中，显示 <a> HTML 标签及属性。

7. 在向导的下一页上，如果要打开独立安装包列表，请启用**打开独立包列表**选项。

8. 单击**完成**按钮。

   “独立安装包创建向导”关闭。

此时会创建独立安装包，并将其放置在管理服务器共享文件夹的 PkgInst 子文件夹中。您可以通过单击安装包列表上方的“**查看独立包列表**”按钮来查看独立包列表。

创建自定义安装包

您可以使用自定义安装包执行以下操作：

- 在客户端设备上安装任何应用程序（例如文本编辑器），例如，通过任务安装。
- 创建独立安装包。

自定义安装包是一个包含一组文件的文件夹。创建自定义安装包的源是*存档文件*。存档文件包含一个或多个必须包含在自定义安装包中的文件。创建自定义安装包后，您可以指定命令行参数，例如以静默模式安装应用程序。

要创建自定义安装包：

1. 在控制台树中，选择**管理服务器 → 高级 → 远程安装 → 安装包**。
   此时会显示管理服务器上可用的安装包的列表。
2. 在安装包列表上方，单击“**创建安装包**”按钮。
   新安装包向导启动。使用**下一步**按钮进行向导。
3. 在向导的第一页上，选择“**为指定的可执行文件创建安装包**”。
4. 在向导的下一页上，指定自定义安装包名称。
5. 在向导的下一页上，单击“**浏览**”按钮，然后在标准 Windows “**打开**”窗口中，选择位于可用磁盘上的存档文件以创建自定义安装包。
   您可以上传 ZIP、CAB、TAR 或 TAR.GZ 压缩包。无法从 SFX（自解压存档）文件创建安装包。
   文件将下载到 Kaspersky Security Center 管理服务器。
6. 在向导的下一页上，指定可执行文件的命令行参数。
   您可以指定命令行参数，以静默模式从安装包中安装应用程序。指定命令行参数是可选的。
   如果需要，请配置以下选项：
   - **将整个文件夹复制到安装包**

     如果可执行文件伴随应用程序安装所需的附加文件，则选择该选项。在您启用该选项之前，确保所有所需文件都存储在相同文件夹。如果启用该选项，应用程序添加文件夹的全部内容，包括指定的可执行文件，到安装包。

   - **对被 Kaspersky Security Center 识别的应用程序转换设置到推荐值**

     如果指定应用程序的信息被包含在 Kaspersky 数据库，应用程序将以推荐设置安装。
     如果您在“**可执行文件命令行**”字段中输入了参数，则会使用建议的设置来重写它们。
     默认情况下已启用该选项。
     Kaspersky 数据库由 Kaspersky 分析家创建和维护。对于每个添加到数据库的应用程序，Kaspersky 分析家定义最优的安装设置。设置被定义以确保成功将应用程序远程安装到客户端设备。当您运行将更新下载至管理服务器存储库任务时，数据库在管理服务器上被自动更新。

   创建自定义安装包的过程开始。
   该向导将在过程完成时通知您。
   如果未创建自定义安装包，则会显示相应的消息。
7. 单击**完成**按钮关闭向导。

您创建的安装包将下载到管理服务器共享文件夹的 Packages 子文件夹中。下载后，自定义安装包将显示在安装包列表中。

在管理服务器上的安装包列表中，您可以查看和编辑自定义安装包属性。

查看和编辑自定义安装包的属性

创建自定义安装包后，可以查看有关安装包的常规信息，并在属性窗口中指定安装设置。

要查看和编辑自定义安装包的属性：

1. 在控制台树中，选择**管理服务器 → 高级 → 远程安装 → 安装包**。
   此时会显示管理服务器上可用的安装包的列表。
2. 在安装包的上下文菜单中，选择**属性**。
   此时将打开所选安装包的属性窗口。
3. 查看以下信息：
   - 安装包名称
   - 打包到自定义安装包中的应用程序名称
   - 应用程序版本
   - 安装包创建日期
   - 管理服务器上自定义安装包的路径
   - 可执行文件命令行
4. 指定下列设置：
   - 安装包名称
   - **安装所需的常规系统组件**

     如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

     如果禁用该选项，您可能必须手动安装先决条件。

     默认情况下已禁用该选项。

     仅当 Kaspersky Security Center 识别添加到安装包中的应用程序时，此选项才可用。
   - **可执行文件命令行**

     如果应用程序需要更多参数以进行静默安装，在该字段指定它们。参考供应商文档以获取详情。

     您也可以输入其他参数。

该选项仅适用于未基于 Kaspersky 应用程序创建的软件包。

5. 单击**确定**或**应用**按钮以保存更改（如果有）。

新设置被保存。

从 Kaspersky Security Center 分发包中获取网络代理安装包

您可以从 Kaspersky Security Center 分发包中获取网络代理安装包，而无需安装 Kaspersky Security Center。然后您可以使用安装包在客户端设备上安装网络代理。

要从 Kaspersky Security Center 分发包中获取网络代理安装包：

1. 从 Kaspersky Security Center 分发工具包运行 ksc_<版本号>.<内部版本号>_full_<本地化语言>.exe 可执行文件。
2. 在打开的窗口中，单击“**抽取安装包**”链接。
3. 在安装包列表中，选中网络代理安装包旁边的复选框，然后单击“**下一步**”按钮。
4. 如有必要，单击“**浏览**”按钮更改显示的要将安装包解压缩到的文件夹。
5. 单击“**抽取**”按钮。
   应用程序将解压缩网络代理安装包。
6. 该进程完成后，单击“**关闭**”按钮。

网络代理安装包被解压到选定的文件夹中。

您可以使用安装包通过以下方法之一安装网络代理：

- 本地，通过从解压缩的文件夹中运行 setup.exe 文件
- 通过静默安装
- 通过使用 Microsoft Windows 组策略

将安装包分发至从属管理服务器

要将安装包分发至从属管理服务器：

1. 与控制相关从属管理服务器的管理服务器建立连接。
2. 以下列方式之一，创建向从属管理服务器分发安装包的任务：
   - 如果要为所选管理组中的从属管理服务器创建任务，请为该组启动组任务创建。
   - 如果您要为特定从属管理服务器创建任务，请为特定设备启动任务创建。

“新任务向导”启动。遵照向导的说明操作。

在新任务向导的“**选择任务类型**”窗口的“**Kaspersky Security Center 管理服务器**”节点中，在“**高级**”文件夹中选择“**分发安装包**”作为任务类型。

新任务向导将创建将所选安装包分发至从属管理服务器的任务。

3. 手动运行任务，或者按照任务设置中指定的计划等待任务启动。

所选安装包将被复制到特定从属管理服务器中。

通过分发点分发安装包

您可以使用分发点，在管理组内分发安装包。

当从管理服务器收到安装包后，分发点将会使用 IP 多播分发，自动将其分发至客户端设备。管理组中安装包的 IP 多点传送仅发生一次。如果客户端设备在分发时与公司网络断开了连接，当安装任务启动时，客户端设备上的网络代理将自动从分发点上下载必要的安装包。

将应用程序部署结果传输至 Kaspersky Security Center

在您创建了应用程序安装包后，您可以对其进行配置以便所有应用程序安装结果的诊断信息都会被发送到 Kaspersky Security Center。对于 Kaspersky 应用程序安装包，程序安装结果的传输或诊断信息默认已被配置，无需多余的配置。

要为安装到 Kaspersky Security Center 的应用程序配置诊断信息：

1. 导航至由 Kaspersky Security Center 为为所选应用程序创建的安装包文件夹。您可以在安装 Kaspersky Security Center 时指定的共享文件夹中找到该文件夹。

2. 打开后缀为 .kpd 或 .kud 的文件进行编辑（比如在 Microsoft Windows Notepad 编辑器中编辑）。

   该文件的格式为常规配置 .ini 文件格式。

3. 在文件中添加下列行：

   ```
   [SetupProcessResult]
   Wait=1
   ```

   此命令配置 Kaspersky Security Center 等待安装包要创建的应用程序设置完毕并分析安装程序返回码。如果您要禁止传输诊断数据，请将 Wait 键值设为 0。

4. 添加成功安装的返回码的说明。为此，请在文件中添加下列行：

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   方括号包含可选键。

命令行的语法：

- `<return code>`。安装程序返回码对应的任何数字。返回码数字是任意的。
- `<description>`。安装结果的文字说明。您可忽略此说明。

5. 添加安装失败的返回码的说明。为此，请在文件中添加下列行：

```
[SetupProcessResult_ErrorCodes]
<return code>=[<description>]
<return code 1>=[<description>]
...
```

这些行的语法与成功安装的返回码语法是相同的。

6. 保存所有更改，关闭 .kpd 或 .kud 文件。

这样，关于用户定义的应用程序的安装结果将在 Kaspersky Security Center 的日志中注册，并将显示在事件列表、报告和任务运行日志中。

为安装包定义 KSN 代理服务器地址

如果管理服务器的地址或域发生变化，您可以为安装包定义 KSN 代理服务器地址。

要为安装包定义 KSN 代理服务器地址：

1. 在控制台树的“**远程安装**”文件夹中，双击“**安装包**”子文件夹。
2. 在打开的菜单中，选择“**属性**”。
3. 在打开的属性窗口中，选择“**常规**”子区域。
4. 在属性窗口的“**常规**”子区域中，输入 KSN 代理服务器的地址。

安装包将默认使用该地址。

接收应用程序的最新版本

Kaspersky Security Center 允许接收 Kaspersky 服务器上存储的企业应用程序最新版本。

要接收 Kaspersky 企业应用程序的最新版本：

1. 执行以下操作之一：

   - 在控制台树中，选择含有所需管理服务器名称的节点，确保已选择“**监控**”选项卡，然后在“**部署**”部分中单击“**有卡巴斯基应用程序的新版本可用**”链接。

     当管理服务器在 Kaspersky 服务器上发现了新版本的企业应用程序时，“**有卡巴斯基应用程序的新版本可用**”链接将变为可见。

   - 在控制台树中，选择“**高级 → 远程安装 → 安装包**”，然后在工作区中单击“**附加操作**”，从下拉列表中选择“**查看卡巴斯基应用程序的当前版本**”。

   这将显示 Kaspersky 应用程序当前版本的列表。

2. 您可以筛选卡巴斯基应用程序列表以简化对所需应用程序的搜索。

   在**当前应用程序版本**窗口的顶部，单击**过滤器**链接以按以下条件筛选应用程序列表：

   - **组件**。使用此标准按网络上正在使用的保护区域筛选卡巴基斯应用程序列表。
   - **已下载软件的类型**。使用此标准按应用程序类型筛选卡巴基斯应用程序列表。
   - **要显示的软件产品和更新**。使用此标准按特定版本显示可用的卡巴斯基应用程序。
   - **软件和更新的显示语言**。使用此标准显示采用特定本地化语言的卡巴斯基应用程序。

   单击**应用**按钮应用选定的过滤器。

3. 从列表中选择请求的应用程序。

4. 通过单击在“**分发包网址**”字符串中的链接下载应用程序分发包。

   受管理应用程序的更新可能需要安装 Kaspersky Security Center 的特定最低版本。如果此版本高于当前版本，则会显示这些更新，但无法批准。此外，在升级 Kaspersky Security Center 之前，无法从此类更新创建安装包。系统会提示您将 Kaspersky Security Center 实例升级到所需的最低版本。

如果针对所选应用程序显示“**下载应用程序并创建安装包**”按钮，可以单击此按钮来下载应用程序分发包并自动创建安装包。Kaspersky Security Center 下载应用程序分发包到管理服务器，存储于安装 Kaspersky Security Center 时指定的共享文件夹下。自动创建的安装包显示在控制台树“**远程安装**”文件夹的“**安装包**”子文件夹中。

“**当前应用程序版本**”窗口关闭后，“**有卡巴斯基应用程序的新版本可用**”链接将从“**部署**”区域中消失。

您可以为新版本应用程序创建安装包，并在控制台树的“**远程安装**”文件夹的“**安装包**”子文件夹中管理新创建的安装包。

您也可以在“**安装包**”文件夹的工作区中单击“**查看卡巴斯基应用程序的当前版本**”链接，以打开“**当前应用程序版本**”窗口。

为远程安装准备 Windows 设备

远程安装应用程序到客户端设备时可能会因下列原因返回错误：

- 该任务已成功在该设备上执行。
  在此情况下，该任务无需再执行。
- 任务开始后，设备被关闭。
  在此情况下，请打开设备，然后重新启动此任务。
- 管理服务器与客户端设备上安装的网络代理之间无连接。
  要确定问题原因，请使用客户端设备的远程诊断实用程序 (klactgui)。
- 如果设备上未安装网络代理，远程安装过程中可能出现下列问题：
  - 客户端设备启用了“**禁用简单文件共享**”。
  - 客户端设备上未运行服务器服务。
  - 客户端设备上的相关端口被关闭。
  - 用于执行任务的账户权限不足。

  为了避免在未安装网络代理的客户端设备上安装应用程序时可能出现的问题，您必须按照通过 Kaspersky Security Center 的远程安装任务强制部署中所述进行操作。

之前使用 riprep 实用程序准备设备进行远程安装。现在这被认为是一种配置操作系统的过时方法。不建议在比 Windows XP 和 Windows Server 2003 R2 更新版本的操作系统上使用 riprep 实用程序。

准备 Linux 设备并在 Linux 设备上远程安装网络代理

网络代理安装包括两个步骤：

- Linux 设备准备
- 网络代理远程安装

Linux 设备准备

要准备运行 Linux 的设备以远程安装网络代理：

1. 确保您要在上面安装 Network Agent for Linux 的设备运行受支持的 Linux 分类。
2. 使用应用程序界面或从卡巴斯基网站下载网络代理安装包。

3. 确保目标 Linux 设备上安装了以下软件：

   - Sudo（对于 Ubuntu 10.04，Sudo 版本为 1.7.2p1 或更高）
   - Perl 语言解释器版本 5.10 或更高版本
   - ps实用程序

4. 测试设备配置：

   a. 检查是否您可以通过 SSH 客户端（例如 PuTTY）连接到设备。

   如果您无法连接到设备，打开文件 `/etc/ssh/sshd_config` 并确保以下设置具有以下相关值：

   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

   如果您可以毫无问题地连接到设备，请不要修改 /etc/ssh/sshd_config 文件；否则在运行远程安装任务时可能会遇到 SSH 认证失败的情况。

   保存文件（如果必要）并使用 `sudo service ssh restart` 命令重启 SSH 服务。

   b. 禁用要连接设备的用户账户的 sudo 密码。

   c. 使用 sudo 的 `visudo` 命令打开 sudoers 配置文件。

   在打开的文件中，添加以下行到文件末尾：`<username> ALL = (ALL) NOPASSWD: ALL`。此种情况下，< 用户名 > 是将用于通过 SSH 连接设备的用户账户。如果您使用的是 Astra Linux 操作系统，请在 /etc/sudoers 文件中添加包含以下文本的最后一行：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. 保存并关闭 sudoers 文件。

   e. 通过 SSH 再次连接设备并确保 Sudo 服务不提示您输入密码；您可以使用 `sudo whoami` 命令来操作。

5. 打开 `/etc/systemd/logind.conf` 文件，然后做以下操作：

   - 指定“no”作为“KillUserProcesses”设置的值：`KillUserProcesses=no`。
   - 对于“KillExcludeUsers”设置，输入要执行远程安装的账户的用户名，例如，`KillExcludeUsers=root`。

   如果目标设备正在运行 Astra Linux，请在 `/home/<` 用户名 `>/.bashrc` 文件中添加 `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 字符串，其中 < 用户名 > 是用于使用 SSH 进行设备连接的用户账户。

   要应用更改的设置，重启 Linux 设备或执行以下命令：

   ```
   sudo systemctl restart systemd-logind.service
   ```

6. 如果您想在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，首先安装 insserv-compat 软件包以配置网络代理。

7. 如果要在封闭软件环境模式下运行 Astra Linux 操作系统的设备上安装网络代理，请执行额外的步骤来准备 Astra Linux 设备。

8. 如果要在使用操作系统 RED OS 7.3.4 或更高版本或 MSVSPHERE 9.2 或更高版本的设备上安装网络代理，请安装 libxcrypt-compat 包以确保网络代理正确运行。

网络代理远程安装

要在 Linux 设备上远程安装网络代理：

1. 下载并创建安装包：

   a. 在设备上安装之前，请确保该包安装了所有的先决条件（程序和库）。

   您可以自行查看每个包的先决条件，使用 Linux 分发包的实用工具。关于更多实用工具的详情，请参考您的操作系统文档。

   b. 要创建远程安装包，使用以下文件：

   - klnagent.kpd
   - akinstall.sh
   - 网络代理的 .deb 或 .rpm 包

2. 使用以下设置创建远程安装任务：

   - 在新任务向导的**设置**页面，选择**通过管理服务器使用操作系统资源**复选框。清空所有其他复选框。
   - 在"**选择账户以运行任务**"页面，请指定通过 SSH 进行设备连接的用户账户设置。

3. 运行远程安装任务。使用 `su` 命令的选项保护环境：`-m, -p, --preserve-environment`。

准备运行 SUSE Linux Enterprise Server 15 的设备以安装网络代理

要在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，

在安装网络代理之前，运行以下命令：

```
sudo zypper install insserv-compat
```

这使您能够安装 insserv-compat 软件包并正确配置网络代理。

运行 `rpm -q insserv-compat` 命令来检查软件包是否已经安装。

如果您的网络包含大量运行 SUSE Linux Enterprise Server 15 的设备，您可以使用配置和管理公司基础架构的专用软件。通过使用此软件，您可以一次在所有必要的设备上自动安装 insserv-compat 软件包。例如，您可以使用 Puppet、Ansible、Chef，或者您可以制作自己的脚本 — 使用任何方便的方法。

如果设备没有 SUSE Linux Enterprise 的 GPG 签名密钥，您可能会遇到以下警告：`Package header is not signed!` 选择 `i` 选项以忽略警告。

除了安装 insserv-compat 软件包外，请确保您已完全准备好 Linux 设备。之后，部署和安装网络代理。

准备 macOS 设备以远程安装网络代理

要准备运行 macOS 的设备以远程安装网络代理：

1. 确保目标 macOS 设备上安装了 sudo。
2. 测试设备配置：
   a. 确保端口 22 在客户端设备上打开。为此，在“**系统偏好**”中打开“**共享**”窗格，然后确保选中“**远程登录**”复选框。

      您只能通过端口 22 来通过 Secure Shell (SSH) 连接到客户端设备。您不能更改端口号。

      您可以使用 `ssh <设备名称>` 命令远程登录到 macOS 设备。在“**共享**”窗格中，可以使用“**允许访问**”选项来设置允许访问 macOS 设备的用户范围。

   b. 禁用要连接设备的用户账户的 sudo 密码。

      在终端中使用 `sudo visudo` 命令打开 sudoers 配置文件。在打开的文件中，在“用户特权指定”条目中指定以下内容：`username ALL = (ALL) NOPASSWD: ALL`。在这种情况下，`username` 代表通过 SSH 进行设备连接的用户账户。

   c. 保存并关闭 sudoers 文件。

   d. 通过 SSH 再次连接设备并确保 Sudo 服务不提示您输入密码；您可以使用 `sudo whoami` 命令来操作。
3. 下载并创建安装包：
   a. 使用以下方法之一下载网络代理安装包：

      - 在控制台树中，打开“**远程安装**”→“**安装包**”的上下文菜单，然后选择“**显示当前应用程序版本**”以从可用安装包中选择
      - 从技术支持网站 https://support.kaspersky.com/ 下载相关版本的网络代理
      - 向技术支持专家索取安装包

   b. 要创建远程安装包，使用以下文件：

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg
4. 使用以下设置创建远程安装任务：

- 在新任务向导的**设置**页面，选择**通过管理服务器使用操作系统资源**复选框。清空所有其他复选框。
- 在“**选择账户以运行任务**”页面，要运行任务，请指定通过 SSH 进行设备连接的用户账户设置。

客户端设备已准备好通过您创建的相应任务远程安装网络代理。

Kaspersky 应用程序：授权许可和激活

此部分描述了使用受管理 Kaspersky 应用程序的授权许可密钥时相关的 Kaspersky Security Center 功能。

Kaspersky Security Center 使您可以集中为客户端设备上的 Kaspersky 应用程序分发授权许可密钥、监控其使用情况，以及续订授权许可。

使用 Kaspersky Security Center 添加授权许可密钥时，该密钥的设置会保存在管理服务器上。应用程序会根据该信息生成一份授权许可密钥使用情况的报告，并通知管理员密钥属性中指定的授权许可期满日期，以及是否违反此限制。您可以在管理服务器设置内配置授权许可密钥使用情况的通知。

受管理应用程序的授权许可

安装到受管理设备上的 Kaspersky 应用程序必须通过将密钥文件或激活码应用到每个应用程序来获得授权。密钥文件或激活码可以按以下方法部署：

- 自动部署
- 受管理应用程序安装包
- 受管理应用程序的“*添加授权许可密钥*”任务
- 受管理应用程序的手动激活

您可以通过上面列出的任何方法添加新的活动或备用授权许可密钥。卡巴斯基应用程序当前使用一个活动密钥并存储一个备用密钥以在活动密钥到期后应用。您为其添加授权许可密钥的应用程序可定义密钥是活动密钥还是备用密钥。密钥定义不依赖于您用于添加新授权许可密钥的方法。

自动部署

如果您使用不同的受管理应用程序，且您必须将特定密钥文件或激活码部署到设备，请选择其他方法部署激活码或密钥文件。

Kaspersky Security Center 允许您自动部署可用授权许可密钥到设备。例如，三个授权许可密钥被存储在管理服务器存储库。您已为所有三个授权许可密钥选择了“**自动分发授权许可密钥到受管理设备**”复选框。Kaspersky 安全应用程序—例如，Kaspersky Endpoint Security for Windows— 被安装到组织设备。发现必须部署授权许可密钥的新设备。应用程序决定，例如，存储库中的两个授权许可密钥可以被部署到设备：授权许可密钥 *Key_1*和授权许可密钥 *Key_2*。这些授权许可密钥之一被部署到设备。此种情况下，无法预见两个授权许可密钥中的哪个将被部署到设备，因为自动部署授权许可密钥不提供给任何管理员活动。

当部署授权许可密钥时，设备为该授权许可密钥重新计算。您必须确保部署授权许可密钥的设备数量不超过授权许可限制。如果设备数量超过授权许可限制，所有不被授权许可覆盖的设备将被分配*严重*状态。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 管理控制台：
  - 添加授权许可密钥到管理服务器存储库
  - 自动分发授权许可密钥

  或

- Kaspersky Security Center Web Console：
  - 添加授权许可密钥到管理服务器存储库
  - 自动分发授权许可密钥

请注意，在以下情况下，自动分发的授权许可密钥可能不会显示在虚拟管理服务器存储库中：

- 授权许可密钥对于应用程序无效。
- 虚拟管理服务器没有受管理设备。
- 授权许可密钥已用于由另一个虚拟管理服务器管理的设备，并且已达到设备数量限制。

添加密钥文件或激活码到受管理应用程序安装包

对于安全应用程序，该选项不被推荐。添加到安装包的密钥文件或激活码可能被盗用。

如果您使用安装包安装受管理应用程序，您可以在该安装包中或在应用程序策略中指定激活码或密钥文件。授权许可密钥将在下一次设备与管理服务器同步时被部署到受管理应用程序。

说明：

- 管理控制台：
  - 创建安装包
  - 安装应用程序到客户端设备

  或

- Kaspersky Security Center Web Console：添加授权许可密钥到安装包

通过为受管理应用程序添加授权许可密钥任务来进行部署

如果您选择使用为受管理应用程序*添加授权许可密钥*任务，您可以选择要部署到设备的授权许可密钥并以任何便捷的方法选择设备–例如，通过选择管理组或设备分类。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 管理控制台：
  - 添加授权许可密钥到管理服务器存储库
  - 部署授权许可密钥到客户端设备

  或

- Kaspersky Security Center Web Console：
  - 添加授权许可密钥到管理服务器存储库
  - 部署授权许可密钥到客户端设备

手动添加激活码或密钥文件到设备

您可以激活本地安装的 Kaspersky 应用程序，通过使用应用程序界面提供的工具。请参考已安装应用程序的文档。

查看使用中授权许可密钥的相关信息

要查看使用中授权许可密钥的相关信息，

在控制台树中，选择“**卡巴斯基授权许可**”文件夹。

文件夹工作区将显示客户端设备上使用的授权许可密钥列表。

授权许可密钥旁边会显示一个图标，指示使用类型：

- – 已从连接至管理服务器的客户端设备上收到授权许可密钥的相关信息。该授权许可密钥文件存储在管理服务器之外。
- – 授权许可密钥存储在管理服务器存储库中。已禁用该授权许可密钥的自动分发。
- – 授权许可密钥存储在管理服务器存储库中。已启用该授权许可密钥的自动分发。

您可以打开客户端设备属性窗口的“**应用程序**”区域，来查看客户端设备上的应用程序激活使用了哪些授权许可密钥等相关信息。

为了定义虚拟管理服务器授权许可密钥的最新设置，管理服务器每天至少发送一次请求到 Kaspersky 激活服务器。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。

如果授权许可密钥接收自客户端设备，则您无法导出它为文件。

添加授权许可密钥到管理服务器存储库

要添加授权许可密钥到管理服务器存储库：

1. 在控制台树中，选择“**卡巴斯基授权许可**”文件夹。
2. 使用以下方法之一启动授权许可密钥的添加任务：
   - 在授权许可密钥列表的上下文菜单中选择“**添加激活码或密钥文件**”。
   - 在授权许可密钥列表的工作区中，单击“**添加激活码或密钥文件**”链接。
   - 单击“**添加激活码或密钥文件**”按钮。

   “添加授权许可密钥向导”启动。
3. 选择您希望如何激活管理服务器：使用激活码或使用密钥文件。
4. 指定您的激活码或密钥文件。
5. 如果您想立即在网络上分发相关的授权许可密钥，选择 **自动分发授权许可密钥到受管理设备**。如果不选择此选项，您可以稍后手动分发授权许可密钥。

   结果，密钥文件被下载，添加授权许可密钥向导结束。您现在可以在卡巴斯基授权许可列表中看到添加的授权许可密钥。

删除管理服务器授权许可密钥

要删除管理服务器授权许可密钥：

1. 在管理服务器的上下文菜单中，选择“**属性**”。
2. 在打开的管理服务器属性窗口中，选择“**授权许可密钥**”区域。
3. 通过点击“**删除**”按钮来删除授权许可密钥。

   这样就可以删除授权许可密钥了。

如果添加了备用授权许可密钥，则删除先前的活动授权许可密钥后，备用授权许可密钥将自动变为活动授权许可密钥。

管理服务器的活动授权许可密钥被删除后，漏洞和补丁管理以及移动设备管理功能将不可用。您可以重新添加已删除的授权许可密钥或添加新的授权许可密钥。

部署授权许可密钥到客户端设备

Kaspersky Security Center 允许您使用*授权许可密钥分发*任务将授权许可密钥分发至客户端设备。

在部署之前，请将授权许可密钥添加到管理服务器存储库。

要将授权许可密钥分发至客户端设备，请执行以下操作：

1. 在控制台树中，选择“**卡巴斯基授权许可**”文件夹。
2. 在授权许可密钥列表的工作区，单击“**自动分发授权许可密钥到受管理设备**”按钮。
   “**应用程序激活任务创建向导**”将会启动。使用“**下一步**”按钮继续向导操作。
3. 在应用程序列表中，选择要为创建任务的应用程序。
4. 在向导的**添加密钥**步骤中，使用以下选项之一添加授权许可密钥：
   - 选择“**激活码**”选项以从 Kaspersky Security Center 存储库添加激活码。
     单击**选择**。在打开的窗口中，选择激活码，然后单击**确定**。
   - 选择**密钥文件或密钥**选项，然后执行以下操作：
     a. 单击**选择**。
     b. 在上下文菜单中，选择以下选项之一：
     - **$SelectKeyIdDropdownOption1**。
       在打开的窗口中，从您的设备中选择密钥文件，然后单击**打开**。
     - **$SelectKeyIdDropdownOption2**。
       在打开的窗口中，从 Kaspersky Security Center 存储库中选择密钥，然后单击**确定**。
5. 如果要替换活动授权许可密钥，请清除默认的**用作备用密钥**复选框。
   例如，当组织发生变化时，设备上需要另一个组织的密钥时，或者重新颁发了密钥，新授权许可比当前授权许可更早到期，等等，需要这样做。为了避免错误，您必须清除**用作备用密钥**复选框。
   如果您想了解有关向 Kaspersky Security Center Windows 添加授权许可密钥时可能出现的问题及其解决方法的更多信息，请参阅Kaspersky Security Center 知识库。
6. 检查授权许可密钥信息，然后单击**下一步** 。
7. 在向导的此步骤中，选择要向其分配添加密钥任务的设备。您可以通过以下方式指定设备（最多 1000 部设备）：
   - **选择管理服务器检测到的网络设备**。此种情况下，任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。
   - **手动指定设备地址或从列表导入地址**。您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定预定义分类或您所创建的自定义分类。
- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。

8. 在向导的“**配置任务计划**”步骤，为任务启动创建计划：

- **计划开始**：
  - **一次**

    该任务在指定的日期和时间运行一次（默认情况下，在创建任务的当天）。

  - **手动**

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。

  - **当新更新下载至存储库时**

    当新更新下载至存储库后任务运行。例如，您可能想要对“查找漏洞和所需更新”任务使用该计划。

  - **在检测到病毒爆发时**

    任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：
    - 用于工作站和文件服务器的反病毒
    - 用于周边防护的反病毒
    - 用于邮件系统的反病毒

    默认情况下选定所有应用程序类型。
    您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

  - **在完成其他任务时**

    当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

    您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

- 在搜索栏中输入任务名称，即可根据名称搜索任务。
- 单击排序图标可按名称对任务进行排序。
  默认情况下，任务按字母顺序升序排列。
- 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

9. 在向导的**定义任务名称**步骤中，指定任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

10. 在向导的“**完成任务创建**”步骤，单击“**完成**”按钮关闭向导。
    如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

使用“**应用程序激活任务创建向导**”创建的任务是针对控制台树的“**任务**”文件夹中存储的特定设备的任务。

您也可以使用任务创建向导为管理组和客户端设备创建组或本地授权许可密钥分发任务。

自动分发授权许可密钥

如果密钥位于管理服务器上的授权许可密钥存储区中，则 Kaspersky Security Center 允许将这些授权许可密钥自动分发至受管理设备。自动分发授权许可密钥不适用于**未分配的设备**文件夹中的设备。

要将授权许可密钥自动分发至受管理设备，请执行以下操作：

1. 在控制台树中，选择“**卡巴斯基授权许可**”文件夹。
2. 在文件夹的工作区，选择您要自动发布到设备的授权许可密钥。
3. 使用以下方法之一打开选定授权许可密钥的属性窗口：
   - 通过从授权许可密钥上下文菜单中选择“**属性**”。
   - 通过在选定授权许可密钥的信息框中，单击“**查看授权许可密钥属性**”链接。
4. 在打开的授权许可密钥属性窗口中，选中“**自动分发的授权许可密钥**”复选框。关闭授权许可密钥属性窗口。

   授权许可密钥将被自动分发到所有兼容设备。

授权许可密钥分发是通过网络代理执行的。没有为应用程序创建授权许可密钥分发任务。

在自动分发授权许可密钥的过程中，会考虑授权许可的设备数量限制（授权许可限制在授权许可密钥的属性中设置。）如果达到授权许可限制，则此授权许可密钥在设备上的分发将自动停止。

虚拟管理服务器自动从其存储库和管理服务器的存储库中分发授权许可密钥。我们建议您：

- 使用“*添加授权许可密钥*”任务来选择必须部署到设备的授权许可密钥。
- 避免在虚拟管理服务器设置中禁用“**允许从该虚拟管理服务器自动部署授权许可密钥到它的设备**”选项。否则，虚拟管理服务器将不会向设备分发授权许可密钥，包括来自管理服务器存储库的授权许可密钥。

如果您选择授权许可密钥属性窗口中的**自动分发的授权许可密钥**复选框，授权许可密钥会立即分发在您的网络上。如果不选择此选项，您可以稍后手动分发授权许可密钥。

创建和浏览授权许可密钥使用报告

要在客户端设备上创建授权许可密钥使用报告：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 选择名为**授权许可密钥使用报告**的报告模板，或者创建相同类型的新报告模板。

授权许可密钥使用报告的工作区会显示客户端设备中使用的活动和备用授权许可密钥的相关信息。报告也包含使用授权许可密钥的设备和授权许可密钥属性中指定的限制的相关信息。

查看有关应用程序授权许可密钥的信息

要了解 Kaspersky 应用程序正在使用哪些授权许可密钥：

1. 在 Kaspersky Security Center 控制台树，选择“**受管理设备**”节点并转到“**设备**”选项卡。
2. 右键单击以打开相关设备的上下文菜单并选择“**属性**”。
3. 在打开的“设备属性”窗口中，选择“**应用程序**”区域。
4. 在显示的应用程序列表中，选择要查看其授权许可密钥的应用程序，然后单击“**属性**”按钮。
5. 在打开的应用程序属性窗口中，选择“**授权许可密钥**”区域。
   相关信息显示在此区域的工作区中。

导出授权许可密钥文件

如果您的授权许可密钥被意外删除，您想要恢复它，您可以从其他管理服务器导出授权许可密钥文件。

要导出授权许可密钥文件，您必须在**导出密钥文件：密钥管理**功能区域中拥有**常规功能**权限。

如果授权许可密钥接收自客户端设备，则您无法导出它。

要导出授权许可密钥：

1. 在控制台树中，选择“**卡巴斯基授权许可**”文件夹。
2. 在该列表中，选择要导出为文件的授权许可密钥。
3. 在打开的信息框中，单击**导出密钥文件**链接。
4. 在打开的窗口中，指定要保存授权许可密钥文件的文件夹的路径，然后指定文件名。之后，单击**“保存”**。

   授权许可密钥文件以 .key format 格式被导出至选定的文件夹。

如果您导出的授权许可密钥文件已作为激活码被添加到管理服务器存储库，并且您想要将导出的授权许可密钥文件添加到另一台管理服务器的存储库，则必须将其作为激活码而不是作为密钥文件添加。否则，就会发生错误。您必须在任何方便的文本编辑器中打开导出的授权许可密钥文件，然后复制激活码。

配置网络保护

本节包含有关手动配置策略和任务、用户角色、构建管理组结构和任务层级的信息。

方案：配置网络保护

快速启动向导使用默认设置创建策略和任务。这些设置可能不是最佳的，甚至是组织不允许的。因此，我们建议您微调这些策略和任务并创建其他策略和任务（如果它们对于您的网络而言是必需的）。

先决条件

在您开始之前，确保您已做了如下：

- 安装了 Kaspersky Security Center 管理服务器
- 安装了 Kaspersky Security Center Web Console（可选）
- 完成了 Kaspersky Security Center 主安装方案
- 完成了快速启动向导，或在“**受管理设备**”管理组中手动创建了以下策略和任务：
  - Kaspersky Endpoint Security 策略
  - 更新 Kaspersky Endpoint Security 的组任务
  - 网络代理策略
  - *查找漏洞和所需更新*任务

分阶段配置网络保护：

1. **设置和传播卡巴斯基应用程序策略和策略配置文件**

   要为安装在受管理设备上的卡巴斯基应用程序配置和传播设置，您可以使用两种不同的安全管理方法–以设备为中心或以用户为中心。这两种方法也可以被合并。要实现以设备为中心的安全管理，您可以使用提供在基于 Microsoft Management Console 的管理控制台或 Kaspersky Security Center Web Console 的工具。以用户为中心的安全管理仅可以通过 Kaspersky Security Center Web Console 实现。

2. **配置任务以远程管理 Kaspersky 应用程序**

   检查使用快速启动向导创建的任务并按需要调整它们。

   说明：

   - 管理控制台：
     - 为 Kaspersky Endpoint Security 设置组任务
     - 计划“查找漏洞和所需更新”任务
   - Kaspersky Security Center Web Console：
     - 为 Kaspersky Endpoint Security 设置组任务
     - “查找漏洞和所需更新”任务设置

   如果必要，创建附加任务以管理安装在客户端设备上的 Kaspersky 应用程序。

3. **评估和限制数据库上的事件负载**

   受管理应用程序操作相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

   说明：

   - 管理控制台：设置事件最大数量
   - Kaspersky Security Center Web Console：设置事件最大数量

结果

当您完成该方案时，您将通过配置卡巴斯基应用程序、任务以及管理服务器接收的事件来保护您的网络：

- 卡巴斯基应用程序是根据策略和策略配置文件配置的。
- 应用程序通过一组任务进行管理。
- 设置可以存储在数据库中的最大事件数。

当网络保护配置完成时，您可以继续配置 Kaspersky 数据库和应用程序的常规更新。

有关如何配置对 Kaspersky Sandbox 检测到的威胁的自动响应的详细信息，请参阅 Kaspersky Sandbox 2.0 在线帮助。

策略设置和传播：以设备为中心的方法

当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

先决条件

在开始之前，确保已安装 Kaspersky Security Center 管理服务器和 Kaspersky Security Center Web Console（选装）。如果您安装了 Kaspersky Security Center Web Console，您可能也想考虑以用户为中心的安全管理作为以设备为中心的安全管理的备选或附加选项。

阶段

以设备为中心的卡巴斯基应用程序管理方案包含以下步骤：

1. **配置应用程序策略**

   通过为每个应用程序创建策略来配置安装在受管理设备上的卡巴斯基应用程序设置。策略集将被传播到客户端设备。

   当您在快速启动向导中配置网络保护时，Kaspersky Security Center 为以下应用程序创建默认策略：

   - Kaspersky Endpoint Security for Windows——适用于基于 Windows 的客户端设备
   - Kaspersky Endpoint Security for Linux——适用于基于 Linux 的客户端设备

如果您通过使用该向导完成了配置过程，您不必为该应用程序创建新策略。转到 Kaspersky Endpoint Security 策略的手动设置。

如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

说明：

- 管理控制台：创建策略
- Kaspersky Security Center Web Console：创建策略

2. **创建策略配置文件（可选）**

   如果您想让单一管理组中的设备在不同策略设置下运行，为这些设备创建策略配置文件。策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在受管理设备上活动。

   通过使用配置文件激活条件您可以应用不同的策略配置文件，例如，到特定单元中的设备或到活动目录安全组，具有特别硬件配置或被特别标签标记。使用标签过滤满足特别标准的设备。例如，您可以创建叫做 *Windows* 的标签，使用该标签标记所有运行 Windows 操作系统的设备，然后指定该标签作为策略配置文件激活条件。结果，安装在所有 Windows 设备上的 Kaspersky 应用程序将被使用它们自己的策略配置文件管理。

   说明：

   - 管理控制台：
     - 创建策略配置文件
     - 创建策略配置文件激活规则
   - Kaspersky Security Center Web Console：
     - 创建策略配置文件
     - 创建策略配置文件激活规则

3. **传播策略和策略配置文件到受管理设备**

   默认情况下，管理服务器每 15 分钟自动与受管理设备同步一次。您可以避免自动同步并通过使用强制同步命令手动运行同步。在您创建或更改策略或策略配置文件后，也会强制同步。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。

   如果您使用 Kaspersky Security Center Web Console，您可以检查策略和策略配置文件是否被传送到设备。Kaspersky Security Center 在设备属性中指定传送日期和时间。

   说明：

   - 管理控制台：强制同步
   - Kaspersky Security Center Web Console：强制同步

结果

当以设备为中心的方案完成时，卡巴斯基应用程序根据指定的设置被配置并通过策略层级传播。

配置的应用程序策略和策略配置文件将被自动应用到添加到管理组的新设备。

关于以设备为中心和以用户为中心的安全管理方法

您可以从设备功能的立场和从用户角色的立场管理安全设置。第一种方法叫做*以设备为中心的安全管理*，第二种叫做*以用户为中心的安全管理*。要应用不同的应用程序设置到不同的设备，您可以使用两种方法的任意或组合。要实现以设备为中心的安全管理，您可以使用提供在基于 Microsoft Management Console 的管理控制台或 Kaspersky Security Center Web Console 的工具。以用户为中心的安全管理仅可以通过 Kaspersky Security Center Web Console 实现。

以设备为中心的安全管理使您可以根据特定于设备的功能将不同的安全应用程序设置应用于受管理设备。例如，您可以将不同的设置应用于分配给不同管理组的设备。您还可以通过在活动目录中使用这些设备或通过它们的硬件规格来区分这些设备。

以用户为中心的安全管理使您可以将不同的安全应用程序设置应用于不同的用户角色。您可以创建多个用户角色，为每个用户分配合适的用户角色，并为具有不同角色的用户所拥有的设备定义不同的应用程序设置。例如，您可能要应用不同的应用程序设置到会计和人力资源（HR）人员的设备。结果，当实现了以用户为中心的安全管理时，每个部门–财务部门和人事部门–具有自己的卡巴斯基应用程序设置配置。设置配置定义了哪些应用程序设置可以被用户更改以及哪些被强制设置并被管理员锁定。

通过使用以用户为中心的安全管理，您可以应用特别应用程序设置到单个用户。这可能用在员工在公司有独一角色或您要监控与个别人的设备相关的安全问题时。取决于该员工在公司的角色，您可以扩展或限制该员工更改应用程序设置的权限。例如，您可能要扩展在本地办公室管理客户端设备的系统管理员的权限。

您也可以组合以设备为中心的安全管理和以用户为中心的安全管理方法。例如，您可以为每个管理组配置特定的应用程序策略，然后为企业的一个或几个用户角色创建策略配置文件。此种情况下，策略和策略配置文件按照以下优先级进行应用：

1. 为以设备为中心的安全管理创建的策略被应用。
2. 它们根据策略配置文件属性被策略配置文件修改。
3. 策略被与用户角色关联的策略配置文件修改。

Kaspersky Endpoint Security 策略的手动设置

本节提供关于如何配置 Kaspersky Endpoint Security 策略的建议，该策略由快速启动向导创建。您可以在策略属性窗口中执行设置。

当编辑设置时，请记住您必须点击相关设置之上的锁图标以便允许在工作站上使用该值。

在高级威胁防护区域配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

在**高级威胁防护**区域中，您可以为 Kaspersky Endpoint Security for Windows 配置卡巴斯基安全网络的使用。您还可以配置 Kaspersky Endpoint Security for Windows 模块，例如行为检测、漏洞利用防御、主机入侵防御和修复引擎。

在**卡巴斯基安全网络**子区域，建议您启用**卡巴斯基安全网络**选项。使用此选项有助于重新分发和优化网络流量。如果“**卡巴斯基安全网络**”选项被禁用，您可以启用直接“使用 KSN 服务器”。

在关键威胁防护部分配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

在策略属性窗口的**基本威胁防护**区域，建议您在**防火墙**和**文件威胁防护**子区域指定附加设置。

防火墙子区域包含允许您控制客户端设备上应用程序的网络活动的设置。客户端设备使用分配了“公共”、“本地”或“受信任”状态的网络。根据网络状态，Kaspersky Endpoint Security 可以选择允许或拒绝设备上的网络活动。向组织添加新网络时，您必须为其分配适当的网络状态。例如，如果客户端设备是笔记本电脑，则建议使用公共或受信任的网络，因为笔记本电脑有时连接的不是本地网络。在**防火墙**子区域，您可以检查是否为组织所用的网络分配了正确的状态。

要查看网络列表：

1. 在策略属性中，转到**基本威胁防护 → 防火墙**。
2. 在**可用网络**区域中，单击**设置**按钮。
3. 在打开的**防火墙**窗口中，转到**网络**选项卡以查看网络列表。

在**文件威胁防护**子区域，您可以禁用网络驱动器扫描。网络驱动器扫描可以显著提高网络驱动器负载。在文件服务器上执行间接扫描更方便。

要禁用网络驱动器扫描：

1. 在策略属性中，转到**基本威胁防护 → 文件威胁防护**。
2. 在**安全级别**区域中，单击**设置**按钮。
3. 在打开的**文件威胁防护**窗口中，在**常规**选项卡，清空**所有网络驱动器**复选框。

在常规设置部分配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

在策略属性窗口的**常规设置**区域，建议您在**报告和存储**和**界面**子区域指定附加设置。

在**报告和存储**子区域，转到**到管理服务器的数据传输**区域。**关于已启动的应用程序**复选框用于指示管理服务器数据库是否保存网络设备上所有软件模块的所有版本相关信息。如果勾选该复选框，保存的信息可能需要 Kaspersky Security Center 数据库上的大量磁盘空间（几十 GB）。如果在顶级策略中勾选了**关于已启动的应用程序**复选框，则取消勾选。

如果管理控制台以集中模式管理组织网络上的威胁防护，请禁用在工作站显示 Kaspersky Endpoint Security for Windows 用户界面。为此，在**界面**子区域，转到**用户交互**区域，然后选择**不显示用户界面**选项。

要在工作站上启用密码保护，请在**界面**子区域，转到**密码保护**区域，单击**设置**按钮，然后选择**启用密码保护**复选框。

在事件配置区域配置策略

在**事件配置**区域，您应该禁用保存任何事件到管理服务器，除了以下事件：

- 在**严重**选项卡上：
  - *应用程序自动运行已禁用*
  - *访问被拒绝*
  - *已禁止应用程序启动*
  - *无法清除*
  - *违反了最终用户授权许可协议*
  - *无法加载加密模块*
  - *不能同时启动两项任务*
  - *检测到活动威胁。应该启动高级清除*
  - *检测到网络攻击*
  - *未更新所有组件*
  - *激活错误*
  - *启用便携模式时出错*
  - *与 Kaspersky Security Center 交互时出错*
  - *禁用便携模式时出错*
  - *更改应用程序组件时出错*
  - *应用文件加密/解密规则时出错*
  - *无法应用策略*
  - *进程已终止*
  - *网络活动已阻止*
- 在**功能失败**选项卡上：*任务设置无效，未应用设置*

- 在**警告**选项卡上：
  - *自我保护被禁用*
  - *备用密钥不正确*
  - *用户选择了退出加密策略*
- 在“**信息**”选项卡上：*禁止应用程序在测试模式下启动*

Kaspersky Endpoint Security 更新组任务的手动设置

Kaspersky Endpoint Security 版本 10 和后续版本的最优和建议计划选项是“**当新更新下载至存储库时**”（当“**使用任务启动自动随机延迟**”复选框被选中时）。

Kaspersky Endpoint Security 设备扫描组任务的手动设置

快速启动向导创建扫描设备的组任务。默认情况下，为任务分配“**在星期五下午 7:00 运行**”计划，并且取消选中“**运行错过的任务**”复选框。

这意味着如果组织中的设备在星期五关闭，例如在下午 6:30 关闭，设备扫描任务将永远不会运行。您必须基于组织的工作规则为该任务设置最方便的计划。

计划“查找漏洞和所需更新”任务

快速启动向导为网络代理创建*查找漏洞和所需更新*任务。默认情况下，为任务分配**在星期二下午 7:00 运行**计划，并且取消选中**运行错过的任务**复选框。

如果组织的工作规则要在此时关闭所有设备，*查找漏洞和所需更新*任务将在设备再次开启时运行，也就是，在星期三早晨。此活动可能不是必须的，因为漏洞扫描可能增加 CPU 和磁盘子系统负载。您必须基于组织的工作规则为该任务设置最方便的计划。

更新安装和漏洞修复组任务的手动设置

该快速启动向导为网络代理创建更新安装和漏洞修复组任务。默认情况下，任务设置为在每天 01:00 AM 自动随机运行，并且未启用“**运行错过的任务**”选项。

如果组织工作规则整夜关闭所有设备，则更新安装将永远不会运行。您必须基于组织的工作规则为漏洞扫描任务设置最方便的计划。值得注意的是，更新的安装可能需要重启设备。

设置事件存储库中的最大事件数量

在管理服务器属性窗口的“**事件存储库**”部分，您可以通过限制事件记录数和存储期限来编辑管理服务器数据库的事件存储设置。当您指定事件最大数时，应用程序计算用于指定数目的存储空间的大概大小。您可以使用该大概计算来评估您在磁盘上是否具有足够空间以避免数据库溢出。管理服务器数据库的默认容量是 400,000 个事件。最大建议的数据库容量是 45,000,000 个事件。

应用程序每 10 分钟检查一次数据库。如果事件数达到指定的最大值加 10,000，应用程序将删除最旧的事件，以便仅保留指定的最大事件数。

当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入卡巴斯基事件日志。新事件被列队，然后在删除操作后被保存到数据库。

要限制存储在管理服务器事件存储库中的事件的数量：

1. 右击管理服务器，然后选择**属性**。

   管理服务器属性窗口将打开。

2. 在“**事件存储库**”区域的工作区，指定存储在数据库中事件的最大数量。

3. 单击“**确定**”。

此外，您可以更改任何任务的设置，以保存与任务进度相关的事件，或者只保存任务执行结果。为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

设置有关已修复漏洞的信息的最长保存期限

要设置数据库中有关受管理设备上已修复的漏洞的信息的最长存储期限：

1. 右击管理服务器，然后选择**属性**。

   管理服务器属性窗口将打开。

2. 在“**事件存储库**”区域的工作区中，指定数据库中有关已修复漏洞的信息的最长存储期限。

   默认情况下，存储期限为 90 天。

3. 单击“**确定**”。

有关已修复漏洞的信息的最长存储期限即限制为指定天数。之后，管理服务器维护任务将从数据库中删除过时信息。

管理任务

Kaspersky Security Center 通过创建和运行不同任务来管理设备上安装的应用程序。安装、启用和停用程序、扫描文件、更新数据库和软件模块以及程序的其他操作均需要任务。

任务又被细分为以下类型：

- *组任务*。在所选管理组中的设备上执行的任务。
- *管理服务器任务*。在管理服务器上执行的任务。
- *特定设备的任务*。在所选设备上执行的任务，与设备属于哪个管理组无关。
- *本地任务*。在特定设备上执行的任务。

如果应用程序的管理插件安装在管理员工作站上，只能创建应用程序任务。

您可以通过下方法之一来生成创建任务的设备列表（最多 1000 部设备）：

- 通过选择管理服务器发现的网络设备。
- 通过手动指定设备列表。您可以使用 IP 地址（或 IP 范围）、NetBIOS 名称或 DNS 名称作为设备地址。
- 通过包含有要添加的设备地址的 .txt 文件来导入设备列表（每一个计算机地址必须单独一行）。

  如果通过文件导入或手动创建设备列表，且设备是以名称定义，则列表可以只包含其信息已在设备连接或设备发现中输入到管理服务器数据库中的设备。

您可以为每个应用程序创建不管多少个组任务、特定设备的任务或本地任务。

在网络代理与管理服务器相连时，设备上安装的应用程序将与 Kaspersky Security Center 数据库交换任务信息。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。当应用程序未运行时，所有运行的任务均被取消。

已完成任务结果保存在 Microsoft Windows 和 Kaspersky Security Center 的事件日志中，既集中在管理服务器上，又位于每个设备上。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

管理支持多承租的应用程序的任务详情

支持多承租的应用程序的组任务根据管理服务器和客户端设备层级被应用到应用程序。创建任务的虚拟管理服务器必须处于安装应用程序的客户端设备的相同或更低管理组。

在对应于任务执行结果的事件中，服务提供商管理员可以看到执行任务的设备的信息。对比下，租户管理显示在**多租户节点**。

创建任务

在管理控制台，您可以在管理组文件夹直接创建组任务，也可以在“**任务**”文件夹的工作区创建。

要在管理组文件夹创建组任务：

1. 在控制台树中，选择您要为其创建任务的管理组。
2. 在组工作区中，选择“**任务**”选项卡。
3. 单击“**创建任务**”按钮，执行任务创建。

   “新任务向导”启动。遵照向导的说明操作。

*要在“**任务**”文件夹的工作区创建任务：*

1. 在控制台树中，选择“**任务**”文件夹。
2. 单击“**完成**”按钮，执行任务创建。

   “新任务向导”启动。遵照向导的说明操作。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

创建管理服务器任务

管理服务器执行下列任务：

- 传送报告
- 将更新下载至管理服务器存储库
- 备份管理服务器数据
- 管理服务器维护
- 执行 Windows 更新同步
- 基于参考设备 OS 镜像创建安装包
- 远程安装应用程序
- 远程卸载应用程序
- 分发安装包
- 将应用程序远程安装到从属管理服务器

在虚拟管理服务器上，只有自动报告传送任务和基于参考设备操作系统镜像创建安装包的任务可用。虚拟管理服务器的存储库将显示已下载至主管理服务器的更新。虚拟管理服务器的数据备份与主管理服务器的数据备份一起进行。

要创建管理服务器任务，请执行以下操作：

1. 在控制台树中，选择“**任务**”文件夹。
2. 通过下列方式开始创建任务：
   - 在控制台树的“**任务**”文件夹的上下文菜单中，选择**新建 → 任务**。
   - 在“**任务**”文件夹工作区中单击“**创建任务**”按钮。

“新任务向导”启动。遵照向导的说明操作。

“将更新下载至管理服务器存储库”、“执行 Windows 更新同步”、“管理服务器维护”和“*备份管理服务器数据*”任务只能创建一次。如果已经为管理服务器创建了“*将更新下载至管理服务器存储库*”、“*管理服务器维护*”、“*备份管理服务器数据*”和“*执行 Windows 更新同步*”任务，则它们将不会显示在新任务向导的任务类型选择窗口中。

为特定设备创建任务

在 Kaspersky Security Center 中，您可以为特定设备创建任务。加入组合的设备可以被包含在各种管理组中，也可以被排除在外。Kaspersky Security Center 能够为特定设备执行以下主要任务：

- 远程安装应用程序
- 将消息发送至用户
- 更改管理服务器
- 受管理设备
- 验证更新
- 分发安装包
- 将应用程序远程安装到从属管理服务器
- 远程卸载应用程序

要为特定设备创建任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 通过下列方式开始创建任务：
   - 在控制台树的“**任务**”文件夹的上下文菜单中，选择**新建 → 任务**。
   - 在“**任务**”文件夹工作区中单击“**创建任务**”按钮。

“新任务向导”启动。遵照向导的说明操作。

创建本地任务

要为设备创建本地任务，请执行以下操作：

1. 在包含该设备的组的工作区中，选择“**设备**”选项卡。
2. 在“**设备**”选项卡的设备列表中，选择要为其创建本地任务的设备。
3. 使用下列方式之一为所选设备创建任务：
   - 通过点击“**执行操作**”按钮并在下拉列表中选择“**创建任务**”。
   - 在设备的工作区中，单击“**创建任务**”链接。
   - 按如下方式使用设备属性：
     a. 在设备的上下文菜单中，选择“**属性**”。
     b. 在打开的设备属性窗口中，选择“**任务**”区域，然后单击“**添加**”。

“新任务向导”启动。遵照向导的说明操作。

您可以在相应的 Kaspersky 应用程序指南中找到关于如何创建和配置本地任务的详细任务。

在嵌套组工作区中显示继承的组任务

要启用在嵌套组的工作区中显示继承的组任务功能，请执行以下操作：

1. 在嵌套组的工作区中，选择“**任务**”选项卡。
2. 在“**任务**”选项卡的工作区，单击**显示继承的任务**按钮。

继承的任务将显示在带有以下图标的任务列表中：

- —如果它们从主管理服务器上创建的组中继承。
- —如果它们从顶级组继承。

如果启用了继承模式，继承的任务只能在最初创建的组中进行编辑。继承的任务不能在继承该任务的组中进行编辑。

在任务启动前自动开启设备

Kaspersky Security Center 不会在已关闭的设备上运行任务。您可以将 Kaspersky Security Center 配置为在开始任务之前使用 LAN 唤醒功能自动开启这些设备。

要配置在开始任务之前自动开启设备：

1. 在任务属性窗口中，选择“**计划**”区域。
2. 要配置对设备的操作，请单击“**高级**”链接。
3. 在打开的“**高级**”窗口中，选中“**使用 Wake-On-LAN 功能在任务启动之前开启设备(分钟)**”复选框，然后指定时间间隔（以分钟为单位）。

这样，在开始任务前的指定分钟数内，Kaspersky Security Center 会使用 LAN 唤醒功能开启设备并加载设备上的操作系统。该任务完成后，如果设备用户未登录系统，设备会自动关闭。请注意，Kaspersky Security Center 仅自动关闭使用 LAN 唤醒功能开启的设备。

Kaspersky Security Center 只能在支持 LAN 唤醒 (WoL) 标准的设备上自动启动操作系统。

在任务结束后自动关闭设备

Kaspersky Security Center 允许您用这种方法配置任务，以便其所分发的设备在任务完成后自动关闭。

要在任务结束后自动关闭设备：

1. 在任务属性窗口中，选择“**计划**”区域。
2. 点击“**高级**”链接以打开窗口配置设备操作。
3. 在打开的“**高级**”窗口中，选择“**任务完成后关闭设备**”复选框。

限制任务运行时间

要限制任务在设备上运行的时间：

1. 在任务属性窗口中，选择“**计划**”区域。
2. 单击“**高级**”，打开用于配置客户端设备操作的窗口。
3. 在打开的“**高级**”窗口中，选中“**如果任务运行超过该时间则停止(分钟)**”复选框，并以分钟为单位指定时间间隔。

如果超过特定时间间隔，设备上任务还未完成的话，Kaspersky Security Center 将自动停止该任务。

导出任务

您可以将组任务和特定设备的任务导出至文件。管理服务器任务也将无法导出。

要导出任务，请执行以下操作：

1. 从任务的上下文菜单中，选择**所有任务 → 导出**。
2. 在打开的“**另存为**”窗口中，指定文件的名称和路径。
3. 单击“**保存**”按钮。

本地用户的权限不能被导出。

导入任务

您可以导入组任务和特定设备的任务。管理服务器任务也将无法导入。

要导入任务，请执行以下操作：

1. 选择必须导入任务的列表：
   - 如果您希望将任务导入到组任务列表中，请在相关管理组的工作区中选择“**任务**”选项卡。
   - 如果您希望将任务导入到特定设备的任务列表中，请从控制台树中选择“**任务**”文件夹。
2. 使用下列方式之一导入任务：
   - 从任务列表的上下文菜单中，选择**所有任务 → 导入**。
   - 单击任务列表管理块中的“**从文件导入任务**”链接。
3. 在打开的窗口中，指定您想要导入的任务文件路径。
4. 单击“**打开**”按钮。

任务显示在任务列表。

如果新导入的任务与现有任务具有相同的名称，则导入的任务在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

转换任务

您可以使用 Kaspersky Security Center，将早期版本的 Kaspersky 应用程序的任务转换为最新版程序的任务。

以下程序的任务可以进行转换：

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

若要转换任务，请执行以下操作：

1. 在控制台树中，选择您希望为其转换任务的管理服务器。
2. 在管理服务器的上下文菜单，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启动。遵照向导的说明操作。

当向导完成操作后，新任务将被创建。该任务将使用早期版本程序的任务设置。

手动启动和停止任务

您可以使用以下方法之一手动启动和停止任务：在任务的上下文菜单中或在已分配任务的客户端设备的属性窗口中。

> 仅允许包含在 KLAdmins 组中的用户从设备的上下文菜单启动组任务。

从上下文菜单或任务的属性窗口启动或停止任务：

1. 在任务列表中，选择一个任务。
2. 通过下列方式开始启动或停止任务：
   - 通过从任务的上下文菜单中，选择“**开始**”或“**停止**”。
   - 通过在任务属性窗口的“**常规**”区域，单击“**开始**”或“**停止**”。

从上下文菜单或客户端设备的属性窗口启动或停止任务：

1. 在设备列表中，选择一个设备。
2. 通过下列方式开始启动或停止任务：
   - 在设备的上下文菜单中，选择**所有任务 → 运行任务**。从任务列表选择相关任务。
     为其分配任务的设备的列表将替换为所选设备。任务启动。
   - 通过在设备属性窗口的“**任务**”区域单击启动按钮（ ）或停止按钮（ ）。

手动暂停和恢复任务

要手动暂停和恢复任务，请执行以下操作：

1. 在任务列表中，选择一个任务。
2. 使用下列方法之一来暂停或恢复任务：
   - 在任务的上下文菜单中，选择“**暂停**”或“**恢复**”。
   - 通过在任务属性窗口中选择“**常规**”区域，并点击“**暂停**”或“**恢复**”。

监视任务执行

要监视任务执行，

在任务属性窗口中，选择“**常规**”区域。

“**常规**”区域的中间部分显示当前任务状态。

浏览保存在管理服务器中的任务运行结果

Kaspersky Security Center 允许您查看组任务、特定设备的任务和管理服务器任务的运行结果。

要查看任务结果：

1. 在任务属性窗口中，选择“**常规**”部分。
2. 单击“**结果**”链接打开“**任务结果**”窗口。

要查看从属管理服务器的任务结果：

1. 在任务属性窗口中，选择“**常规**”区域。
2. 单击“**结果**”链接打开“**任务结果**”窗口。
3. 单击“**从属服务器的统计信息**”。
4. 选择要显示“**任务结果**”窗口的从属服务器。

配置任务运行结果信息的过滤条件

Kaspersky Security Center 允许您过滤组任务、特定设备的任务以及管理服务器任务的运行结果。但无法过滤本地任务。

要设置对任务运行结果的信息过滤，请执行以下操作：

1. 在任务属性窗口中，选择“**常规**”区域。
2. 点击“**结果**”链接打开**任务结果**窗口。
   窗口上部的表包含为其分配任务的所有设备列表。窗口下部的表显示在选定的设备上执行的任务的结果。
3. 右击相关表格，打开上下文菜单并选择“**过滤器**”。
4. 在打开的“**设置过滤器**”窗口，在“**事件**”、“**设备**”和“**时间**”区域定义过滤器设置。单击“**确定**”。

任务结果窗口将显示符合过滤器指定设置的信息。

要修改任务回滚更改

要修改任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在“**任务**”文件夹的工作区，选择一个任务并使用上下文菜单转到任务属性窗口。
3. 做相关更改。

   > 在“**任务范围排除项**”区域，您可以设置不应用任务的子组列表。

4. 单击“**应用**”。

对任务所做的更改将保存在任务属性窗口的“**修订历史**”区域。

如果必要，您可以回滚对任务所做的更改。

要回滚对任务所做的更改：

1. 在控制台树中，选择“**任务**”文件夹。
2. 选择必须回滚更改的任务，使用上下文菜单转到任务属性文件夹。
3. 在任务属性窗口中，选择“**修订历史**”区域。
4. 在任务修订列表中，选择您要回滚的修订号。
5. 单击“**高级**”按钮并在下拉列表中选择“**回滚**”值。

比较任务

您可以比较相同类型的任务：例如，您可以比较两个恶意软件扫描任务，但是您无法比较恶意软件扫描任务和更新安装任务。比较之后，您收到任务设置相同点和不同点报告。您可以打印任务比较报告或者保存为文件。当公司中不同的规则被分配给相同类型的不同任务时，您可能需要任务比较。例如，会计部门员工的病毒扫描任务仅是扫描本地磁盘和他们的设备，然而销售部门的员工由于要与客户联络，他们的恶意软件扫描任务是扫描本地硬盘和电子邮件。您不必查看所有任务设置以找出不同点；您可以简单地使用比较。

您仅可以比较相同类型的任务。

任务仅可以成对比较。

您可以用以下方法之一比较任务：通过选择一个任务并与另一个比较，或者通过从任务列表中比较任意两个任务。

要选择一个任务并与另一个进行比较：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在“**任务**”文件夹的工作区，选择您要与另一个进行比较的任务。
3. 从任务的上下文菜单中，选择**所有任务 → 与其他任务比较**。
4. 在“**选择一个任务**”窗口，选择要比较的任务。
5. 单击“**确定**”。

   一个 HTML 格式的比较两个任务的报告被显示。

要从任务列表比较两个任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在“**任务**”文件夹的任务列表，按 **Shift** 或 **Ctrl** 键选择两个相同类型的任务。
3. 在上下文菜单中，选择“**比较**”。

   一个 HTML 格式的比较所选任务的报告被显示。

当任务被比较时，如果密码不同，星号(******)被显示在任务比较报告。

如果密码在任务属性中被更改，星号(******)被显示在修订比较报告。

启动任务的账户

您可以指定在哪个账户下运行任务。

例如，要执行按需扫描任务，您必须具有对要扫描对象的访问权限；要执行更新任务，您需要具有授权代理服务器用户权限。为运行任务指定账户的能力可允许您避免用户运行没有必需访问权限的任务时按需扫描任务和更新任务出现问题。

执行远程安装/卸载任务期间，系统会使用指定的账户将安装或卸载应用程序所需的文件下载到客户端设备，以防网络代理未安装或不可用。如果网络代理已安装并且可用，则会根据任务设置使用账户，使用 Microsoft Windows 实用程序仅从共享文件夹中提供文件。在这种情况下，账户必须在设备上拥有以下权限：

- 远程启动应用程序的权限。
- 使用 Admin$ 资源的权限。
- *作为服务登录*的权限。

如果文件由网络代理提供给设备，则不会使用账户。所有文件复制和安装操作便会由**网络代理**（**LocalSystem 账户**）执行。

导出任务执行的历史记录

如果遇到任何任务问题，您可能需要调查潜在的原因。为此，您可以导出并进一步分析任务执行历史记录。

要导出任务执行历史记录：

1. 在设备上的目录中创建一个空的 TXT 文件。
   任务执行历史记录将被导出到此文件。
2. 打开任务结果窗口。
3. 在任务结果窗口的上方，选择正在经历问题的设备。
4. 在任务结果窗口的下方（所选设备的执行历史记录显示于此），选择一个或者多个事件。
   若要选择多个事件，请使用 **Shift** 或者 **Ctrl** 键。
5. 右击所选事件打开上下文菜单并选择“**导出**”。
   事件导出向导启动。
6. 在向导的**导出文件**步骤，单击**浏览**按钮，然后选择创建用于导出任务执行历史记录的 TXT 文件。
   如果您只想要导出所选事件，请启用选项**仅导出选定事件**。
   如果您想要导出任务执行的整个历史记录（所有事件），则必须禁用**仅导出选定事件** 。
7. 单击“**下一步**”按钮。
8. 在向导的**导出类型**步骤，启用以下选项之一：
   - **导出为制表符分隔的 Unicode 文本**
     如果导出的数据包括多种语言的特殊字符和符号，且您需要确保当包含导出数据的 TXT 文件在不同应用程序中打开时所有字符得到准确保留，请启用此选项。

- **导出为制表符分隔的文本**

  如果您想要维护与可能不支持 Unicode 的旧系统 或者应用程序的兼容性，请启用此选项。

9. 单击“**下一步**”按钮完成向导。

任务执行历史记录被导出到选定的 TXT 文件。

更改任务密码向导

对于非本地任务，可以指定必须在其下运行任务的账户。您可以在任务创建过程中或在现有任务的属性中指定账户。如果根据组织的安全性说明使用了指定的账户，则这些说明可能需要不时更改账户密码。账户密码过期且您设置了新密码后，任务将无法启动，直到您在任务属性中指定了新的有效密码。

更改任务密码向导使您可以在指定账户的所有任务中自动将旧密码替换为新密码。或者，您可以在每个任务的属性中手动进行操作。

要启动更改任务密码向导：

1. 在控制台树中，选择**任务**节点。
2. 从节点的上下文菜单中，选择**更改任务密码向导**。

遵照向导的说明操作。

步骤 1：指定凭证

在“**账户**”和“**密码**”字段中，指定系统中（例如，Active Directory 中）当前有效的新凭据。当您切换到向导的下一步时，Kaspersky Security Center 将检查指定的账户名是否与每个非本地任务的属性中的账户名匹配。如果账户名匹配，则任务属性中的密码将自动替换为新的密码。

如果您填写“**旧密码(可选)**”字段，Kaspersky Security Center 仅为找到账户名和旧密码的任务替换密码。替换将自动执行。在所有其他情况下，您必须选择要在向导的下一步执行的操作。

步骤 2：选择要采取的操作

如果未在向导的第一步中指定旧密码，或者指定的旧密码与任务中的密码不匹配，则需要选择要对找到的任务执行的操作。

对于具有“*需要批准*”状态的每个任务，请确定是要删除任务属性中的密码还是将其替换为新密码。如果选择删除密码，该任务将切换为以默认账户运行。

步骤 3：查看结果

在向导的最后一步，查看每个找到的任务的结果。要完成向导，请单击**完成**按钮。

为属于虚拟管理服务器的管理组创建层级结构

创建虚拟管理服务器后，它将默认包含名为“**受管理设备**”的管理组。

创建从属于虚拟管理服务器的管理组层次结构的过程与创建从属于物理管理服务器的管理组层次结构的过程相同。

> 您不能将从属和虚拟管理服务器添加至属于虚拟管理服务器的管理组。这是由于虚拟管理服务器的限制。

策略和策略配置文件

在 Kaspersky Security Center Web Console 中，可以为 Kaspersky 应用程序创建策略。该部分描述了策略和策略配置文件，并提供创建和修改它们的说明。

策略层级，使用策略配置文件

本部分提供有关如何应用策略到管理组设备的信息。本部分还提供有关策略配置文件的信息。

策略层级

在 Kaspersky Security Center，您使用策略来定义一个单一设置集到多个设备。例如，应用程序 P 的策略范围，为管理组 G 定义，包含安装了应用程序 P 的部署在组 G 和其子组的受管理设备， 除了在属性中清空了**从父组继承**复选框的子组。

策略通过设置旁边的锁图标（）不同于本地设置。如果一个设置（或设置组）在策略属性中被锁定，您必须首先在创建有效设置时使用该设置（或设置组），其次，必须将设置或设置组写入 downstream 策略。

在设备上创建有效设置可以如此描述：所有未锁定的设置值必须来自策略，然后被本地设置覆盖，然后结果集被来自策略的锁定设置的值覆盖。

相同应用程序的策略通过管理组层级互相影响：来自 upstream 策略的锁定设置覆盖来自 downstream 策略的相同设置。

漫游用户有特殊策略。该策略在设备切换到漫游模式时在设备上生效。漫游策略不通过管理组层级影响其他策略。

策略配置文件

仅通过管理组层级应用策略到设备可能在许多环境下不方便。有必要创建单一策略的几个实例，这些实例对于不同的管理组在一两个设置上有所不同，可以在将来同步这些策略的内容。

为帮助您避免此类问题，Kaspersky Security Center 支持*策略配置文件*。策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在客户端设备（计算机或移动设备）上活动。激活配置文件会修改配置文件激活之前已在计算机上活动的策略设置。这些设置将使用已在配置文件中指定的值。

以下限制被施加在策略配置文件：

- 策略可以包含最多 100 个配置文件。
- 策略配置文件不能包含其他配置文件。
- 策略配置文件不能包含通知设置。

配置文件内容

策略配置文件包含以下组成部分：

- Name。带有相同名称的配置文件通过管理组层级互相影响。
- 策略设置子集。不同于包含所有设置的策略，配置文件仅包含实际所需的设置(锁定设置)。
- 激活条件是设备属性的逻辑表达。配置文件仅在配置文件激活条件为真是活动(补充策略)。在其他所有情况，配置文件是非激活和忽略的。以下设备属性可以被包含在逻辑表达：
  - 漫游模式状态。
  - 网络环境属性 — 网络代理连接的活动规则的名称。
  - 设备上指定标签的出现和消失。
  - 设备在活动目录组织单元（OU）上的分配：明确(设备在指定 OU 中)，或不明确(设备是 OU，以嵌套级别包含在指定 OU)。
  - 设备在活动目录安全组中的成员关系（明确或不明确）。
  - 活动目录安全组中设备所有者的成员关系（明确或不明确）。
- 配置文件禁用复选框。被禁用的配置文件总是被忽略，并且它们的激活条件不被验证。
- 配置文件优先级。不同配置文件的激活条件是独立的，因此几个配置文件可以一起激活。如果活动配置文件包含设置的非重叠集合，将不会发生问题。然而，如果两个活动配置文件包含不同的相同设置的值，将发生歧义。该歧义可以通过策略优先级避免：歧义变量的值将来自高优先级的配置文件(在配置文件列表中评级较高)。

策略通过层级互相影响时的配置文件行为

带有相同名称的配置文件根据策略合并规则合并到一起。upstream 策略的配置文件比 downstream 策略的配置文件拥有更高优先级。如果编辑设置在 upstream 策略中被禁止(锁定)，downstream 策略使用 upstream 策略的配置文件激活条件。如果编辑设置在 upstream 策略中被允许，downstream 策略的配置文件激活条件被使用。

既然策略配置文件可能在激活条件中包含"**设备已离线**"属性，配置文件完全替换漫游用户策略功能，后者将不被支持。

漫游用户的策略可能包含配置文件，但是它们配置文件仅可以在设备切换到漫游模式后激活。

策略设置继承

策略是为管理组指定。策略设置可以是*继承的*，即是在其所在管理组的子组被接收。因此，父组策略也叫*父策略*。

您可以启用或禁用继承的两个选项：**从父组策略中继承设置**和**强制继承子策略设置**：

- 如果您对子策略启用**从父策略继承设置**，并在父策略中锁定一些设置，那么您无法为子组更改这些设置。然而，您可以更改在父策略中未锁定的设置。
- 如果您对子策略禁用**从父策略继承设置**，那么您可以更改子组中的所有设置，即便一些设置在父策略中是锁定的。
- 如果您为父组启用**强制继承子策略设置**，这将为每个子策略启用**从父策略继承设置**。此种情况下，您无法为任何子策略禁用该选项。所有在父策略中被锁定的设置被强制继承到子组，且您无法在子组中更改这些设置。
- 在**受管理设备**组的策略中，**从父策略继承设置**不影响任何设置，因为**受管理设备**组没有任何上游组，因此不继承任何策略。

默认下，**从父组策略中继承设置**选项已为新策略启用。

如果一个策略具有配置文件，所有子策略都继承这些配置文件。

管理策略

客户端设备上安装的应用程序是通过定义策略集中配置的。

为管理组中的应用程序创建的策略将显示在工作区中的**策略**选项卡上。在每个策略名称前面会显示一个状态的图标。

删除或撤回某个策略后，应用程序会继续在该策略指定的设置中运行。这些设置随后可以被手动更改。

策略将按如下方式应用：如果某个设备正在运行驻留任务（实时保护任务），它们将使用新的设置值保持运行。所有已启动的定期任务（按需扫描，程序数据库更新）均保持运行，且设置值不变。下次，它们将使用新设置值运行。

带有多项支持的应用程序的策略被继承到更低级别管理组以及更高级别管理组：策略被传播到所有安装了应用程序的客户端设备。

如果管理服务器为分层构建，从属管理服务器将从主管理服务器接收策略，然后将其发布至客户端设备。启用继承后，则可以在主管理服务器上修改策略设置。然后，从属管理服务器上的策略也将进行相应更改。

如果主从管理服务器之间的连接中止，从属服务上的策略将继续有效，使用应用的设置。重新建立连接后，主管理服务器上修改的策略设置将分发到从属管理服务器。

如果禁用继承，您可以独立更改从属管理服务器上的策略设置，不受主管理服务器的影响。

如果管理服务器和客户端设备之间的连接中止，客户端设备将使用漫游策略（如果定义）的策略，或者继续使用所应用的策略设置，直至重新建立连接。

策略向从属管理服务器分配的结果将显示在主管理服务器控制台的“策略属性”窗口。

向客户端设备分发策略的结果将显示在所连接的管理服务器的策略属性窗口中。

不在策略设置中使用私人数据。例如，避免指定域管理员密码。

创建策略

在管理控制台中，可以直接在要为其创建策略的管理组文件夹中或“**策略**”文件夹的工作区中创建策略。

在管理组文件夹创建策略：

1. 在控制台树中，选择您要为其创建策略的管理组。
2. 在该组的工作区中，选择“**策略**”选项卡。
3. 通过单击“**新策略**”按钮运行新策略向导。

   新策略向导启动。遵照向导的说明操作。

*要在“**策略**”文件夹的工作区创建策略：*

1. 在控制台树中，选择“**策略**”文件夹。
2. 通过单击“**新策略**”按钮运行新策略向导。

   新策略向导启动。遵照向导的说明操作。

您可以为该组中的一个应用程序创建多个策略，但一次只能激活一个策略。当您创建新的活动策略时，先前的活动策略将变为不活动状态。

创建策略时，您可以指定应用程序正常运行所需的最小的一组参数。所有其他值都会被为应用程序本地安装时所应用的默认值。您可以在策略创建后更改策略。

不在策略设置中使用私人数据。例如，避免指定域管理员密码。

在策略应用后更改的 Kaspersky 应用程序设置将在其各自指南中详细介绍。

在策略被创建后，被锁定的设置（标记以锁定图标 ）即在客户端设备上生效，无论先前为应用程序指定了什么设置。

在子组中显示继承的策略

要为嵌套的管理组启用继承策略显示，请执行以下操作：

1. 在控制台树中，选择管理组以显示其继承策略。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 在策略列表的上下文菜单中，选择“**查看**”→“**继承的策略**”。

继承的策略将显示在带有以下图标的策略列表中：

- —如果它们从主管理服务器上创建的组中继承。
- —如果它们从顶级组继承。

当启用设置继承模式后，继承的策略只能在创建该策略的组中修改。在继承该策略的组中，不能更改该策略。

激活策略

要为所选组激活策略，请执行以下操作：

1. 在该组的工作区中，在“**策略**”选项卡中，选择必须激活的策略。
2. 要激活该策略，请执行下列操作之一：
   - 在该策略的上下文菜单中，选择“**活动策略**”。
   - 在策略属性窗口中，打开“**常规**”区域，然后从“**策略状态**”设置组中选择“**活动策略**”。

该策略即对所选管理组激活了。

> 策略应用大量客户端设备后，管理服务器的负载和网络流量在一段时间内会显著增加。

在出现病毒爆发事件时自动激活策略

要使策略在出现病毒爆发事件时自动激活，请执行以下操作：

1. 在管理服务器属性窗口中，打开“**病毒爆发**”区域。
2. 单击“**配置在病毒爆发事件发生时要激活的策略**”链接，打开“**策略激活**”窗口，然后将该策略添加至检测到病毒爆发后要激活的所选策略列表。

> 如果策略在*病毒爆发*事件中激活，您仅可以使用手动模式返回到先前策略。

应用漫游策略

当设备与企业网络断开时，漫游策略将生效。

要应用漫游策略：

在策略属性窗口中，打开“**常规**”部分，然后在“**策略状态**”设置组中，选择“**漫游策略**”。

漫游策略将应用于从企业网络断开的设备。

修改策略回滚更改

要修改策略：

1. 在控制台树中，选择“**策略**”文件夹。
2. 在“**策略**”文件夹的工作区，选择一个策略并使用上下文菜单转到策略属性窗口。
3. 做相关更改。
4. 单击“**应用**”。

对策略所做的更改将保存在策略属性的“**修订历史**”区域。

如果必要，您可以回滚对策略所做的更改。

要回滚对策略所做的更改：

1. 在控制台树中，选择“**策略**”文件夹。
2. 选择必须回滚更改的策略，使用上下文菜单转到策略属性文件夹。
3. 在策略属性窗口中，选择“**修订历史**”区域。
4. 在策略修订列表中，选择您要回滚的修订号。
5. 单击“**高级**”按钮并在下拉列表中选择“**回滚**”值。

比较策略

您可以为单个受管理应用程序比较两个策略。比较之后，您收到策略设置相同点和不同点报告。例如，您可能在不同办公室的不同管理员为单个受管理应用程序创建了多个策略时，或者在单个顶级策略被所有本地办公室继承并修改时必须比较这些策略。您可以用以下方法之一比较策略：通过选择一个策略并与另一个比较，或者通过从策略列表中比较任意两个策略。

> 您只能比较修订历史中具有当前修订的策略。

要将策略与另一个进行比较：

1. 在控制台树中，选择“**策略**”文件夹。
2. 在“**策略**”文件夹的工作区，选择您要与另一个进行比较的策略。
3. 在策略的上下文菜单中，选择**与其他策略比较** 。
4. 在“**选择策略**”窗口，选择要与之比较的策略。
5. 单击“**确定**”。

一个把相同应用程序的两个策略相比较的 HTML 格式的报告被显示。

要从策略列表比较两个策略：

1. 在“**策略**”文件夹的策略列表，使用 **Shift** 或 **Ctrl** 键以为单个受管理应用程序选择策略。
2. 在上下文菜单中，选择“**比较**”。

一个把相同应用程序的两个策略相比较的 HTML 格式的报告被显示。

比较 Kaspersky Endpoint Security for Windows 策略设置的报告还提供策略配置文件比较详情。您可以最小化策略配置文件比较结果。要最小化，点击区域名称旁的箭头图标 (▲)。

查看策略分发状态图

在 Kaspersky Security Center 中，您可以查看每个设备上策略执行的结果。

要查看每个设备上的策略分发状态：

1. 在组的工作区中的**策略**选项卡上，选择要为其查看分发状态的策略。
   右侧窗格中的图表显示策略执行概览。
2. 单击**详细资料**。
   策略强制执行结果窗口打开。
   您可以将策略执行结果导出到 CSV 文件或 TXT 文件。

删除策略

要删除策略，请执行以下操作：

1. 在管理组的工作区中，在“**策略**”选项卡上，选择要删除的策略。
2. 以下列方式之一删除策略：
   - 在策略的上下文菜单中，选择“**删除**”。
   - 在所选策略的信息框中，单击“**删除策略**”链接。

复制策略

要复制策略，请执行以下操作：

1. 在所需组工作区的“**策略**”选项卡上，选择一个策略。
2. 在策略的上下文菜单中，选择“**复制**”。
3. 在控制台树中，选择您要添加该策略的组。
   您可以将策略添加至复制该策略的组中。
4. 从所选组的策略列表的上下文菜单中，在“**策略**”选项卡上，选择“**粘贴**”。

系统会将所有策略设置连同策略一起复制并应用到目标组的设备上。如果在同一组内复制和粘贴策略，策略名称后会自动添加 **（<下一个序列号>）** 索引，例如： **（1）** 、 **（2）** 。

> 活动策略在其复制时将变为不活动策略。如有需要，您可以将其激活。

导出策略

要导出策略，请执行以下操作：

1. 以下列方式之一导出策略：
   - 在策略的上下文菜单中，选择**所有任务 → 导出**。
   - 在所选策略的信息框中，单击“**导出策略到文件**”链接。
2. 在打开的“**另存为**”窗口中，指定策略文件的名称和路径。单击“**保存**”按钮。

导入策略

要导入策略，请执行以下操作：

1. 在相关组工作区的“**策略**”选项卡中，选择下列策略导入方法之一：
   - 通过从策略列表的上下文菜单中选择**所有任务 → 导入**。
   - 在策略列表的管理区块中，单击**从文件导入策略**按钮。
2. 在打开的窗口中，指定您要导入策略的文件路径。单击“**打开**”按钮。

导入的策略显示在策略列表中。策略的设置和配置文件也将会导入。无论导出期间选择的策略处于什么状态，导入的策略均处于非活动状态。您可以在策略属性中更改策略状态。

> 如果新导入的策略与现有策略有相同的名称，则导入的策略在名称后会附加一个 **（<下一个序列号>）** 索引，例如：**(1)**、**(2)**。

转换策略

Kaspersky Security Center 可将早期版本的受管理卡巴斯基应用程序的策略转换为相同应用程序最新版本的策略。转换后的策略保留更新前指定的当前管理员设置，并包括来自应用程序最新版本的新设置。如果策略被转换为受管理卡巴斯基应用程序的最新版本，则您无法在安装了早期版本应用程序插件的应用程序管理服务器上打开该策略。卡巴斯基应用程序的管理插件确定是否可以对这些应用程序的策略进行转换。有关为每个受支持的卡巴斯基应用程序转换策略的信息，请参阅以下列表中的相关帮助文档：

- **卡巴斯基工作站应用程序：**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial CyberSecurity：**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (集中部署不被支持)
- **卡巴斯基移动设备应用程序：**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **卡巴斯基文件服务器应用程序：**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **卡巴斯基虚拟机应用程序：**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless

- **卡巴斯基邮件系统和 SharePoint/协作服务器应用程序：**
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **卡巴斯基针对性攻击检测应用程序：**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **卡巴斯基 KasperskyOS 设备应用程序：**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite（卡巴斯基瘦客户端插件）

若要转换策略，请执行以下操作：

1. 在控制台树中，选择您希望为其转换策略的管理服务器。
2. 在管理服务器的上下文菜单，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启动。遵照向导的说明操作。

向导完成后，将使用当前管理员的策略设置和最新版本卡巴斯基应用程序的新设置来创建新策略。

管理策略配置文件

策略配置文件是策略的一组命名设置集合，当设备状态满足特定激活规则时，它会在客户端设备（计算机或移动设备）上激活。激活配置文件会修改配置文件激活之前已在计算机上活动的策略设置。这些设置将使用已在配置文件中指定的值。

策略配置文件用于单一管理组中的设备在不同策略设置下运行。例如，可能发生管理组中的一些设备的策略设置必须被更改的情况。这种情况下，您可以为该策略配置策略配置文件，这允许您编辑管理组中所选设备的策略设置。例如，策略禁止在“用户”管理组的所有设备上运行 GPS 导航软件。GPS 导航软件仅在“用户”管理组中的单个设备上是必须的——该设备属于所雇佣的导游。您可以标记该设备为“导游”并重新配置策略配置文件，以便它仅允许 GPS 软件在标记为“导游”的设备上运行，同时保持所有剩余策略设置。这种情况下，如果标记为“导游”的设备出现在“用户”管理组，它将被允许运行 GPS 导航软件。运行 GPS 导航软件仍将在“用户”管理组的其他设备上被禁止，除非它们也被标记为“导游”。

配置文件仅被以下策略支持：

- Kaspersky Endpoint Security for Windows 策略
- Kaspersky Endpoint Security for Mac 策略
- Kaspersky Mobile Device Management 插件版本 10 Service Pack 1 到版本 10 Service Pack 3 Maintenance Release 1 的策略
- Kaspersky Device Management for iOS 插件策略

- Kaspersky Security for Virtualization 5.1 Light Agent for Windows 的策略
- Kaspersky Security for Virtualization 5.1 Light Agent for Linux 的策略

策略配置文件简化了策略应用的客户端设备的管理：

- 策略配置文件设置可能不同于策略设置。
- 您无需维护和手动应用仅有几项设置不同的单个策略的多个实例。
- 您无需为漫游用户单独分配策略。
- 您可以导出和导入策略配置文件，以及基于现有策略配置文件创建新的策略配置文件。
- 一个策略可以拥有多个活动策略配置文件。仅满足设备上激活规则的配置文件才能应用到该设备。
- 配置文件服从策略层级。一个继承策略包括所有高级别策略的配置文件。

配置文件的优先级

为策略创建的配置文件按照优先级降序排列。例如，如果在列表中配置文件 X 比配置文件 Y 更高，则 X 比后者具有更高优先级。多个配置文件可以同时应用到一个设备。如果设置值在不同配置文件中有变化，最高优先级配置文件中的值将被应用到该设备。

配置文件激活规则

当激活规则触发时，策略配置文件在客户端设备上激活。*激活规则*是个条件集合，当满足时，则在设备上开启策略配置文件。激活规则可以包含以下条件：

- 客户端设备的网络代理用一组指定的连接参数连接管理服务器，例如服务器地址，端口号，等。
- 客户端设备已离线。
- 已为客户端设备分配了指定标签。
- 客户端设备被显性(设备立即位于所选单元)或隐性(设备位于嵌套单元)放置于活动目录特定单元，设备或其所有者位于活动目录安全组。
- 客户端设备属于指定拥有者，或者设备所有者包含在 Kaspersky Security Center 的安全组里。
- 客户端设备所有者被分配了特殊角色。

管理组的层次结构中的策略

如果您正在低级别管理组中创建策略，该新策略继承高级别组中活动策略的所有配置文件。相同名称的配置文件被删除。高级别组的策略配置文件拥有更高优先级。例如，在管理组 *A* 中，策略 *P（A）* 具有配置文件 *X1*、*X2* 和 *X3*（按优先级降序排列）。在管理组 *A* 的子组管理组 *B* 中，策略 *P（B）* 是使用配置文件 *X2*、*X4*、*X5* 创建的。然后，我们将使用策略 *P（A）* 来修改 *P（B）*，这样策略 *P（B）* 中的配置文件列表将显示为：*X1*、*X2*、*X3*、*X4*、*X5*（以降序排列优先级）。配置文件 *X2* 的优先级将取决于策略 *P（B）* 的 *X2* 和策略 *P（A）* 的 *X2* 的初始状态。在策略 *P(B)* 被创建后，策略 *P(A)* 不再显示在子组 *B*。

每次您启动网络代理，启用和禁用离线模式，或编辑为客户端设备分配的标签列表时，将会重新评估活动策略。例如，RAM 大小在设备上增加，从而激活拥有大 RAM 的设备上的策略配置文件。

策略配置文件的属性和限制

配置文件具有以下属性：

- 非活动策略的配置文件对客户端设备没有任何影响。
- 如果一个策略被设置为**漫游策略**状态，该策略的配置文件也会在设备从企业网络断开连接时得到应用。
- 配置文件不支持对可执行文件的访问的静态分析。
- 策略配置文件无法包含事件通知的任何设置。
- 如果设备使用 UDP 端口 15000 连接到管理服务器，则在为设备分配标签时，相应的策略配置文件在 1 分钟内被激活。
- 当您创建策略配置文件激活规则时，您可以为网络代理连接到管理服务器使用规则。

创建策略配置文件

配置文件的创建仅适用于以下应用程序的策略：

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows 和更新版本
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Kaspersky Mobile Device Management 插件版本 10 Service Pack 1 到 10 Service Pack 3 Maintenance Release 1
- Kaspersky Device Management for iOS 插件
- 适用于 Windows 和 Linux 的 Kaspersky Security for Virtualization 5.1 Light Agent

要创建策略配置文件：

1. 在控制台树中，选择您要为其创建策略配置文件的管理组。
2. 在该管理组的工作区中，选择“**策略**”选项卡。
3. 选择策略并使用上下文菜单切换到策略属性窗口。
4. 打开策略属性窗口中的“**策略配置文件**”区域并单击“**添加**”按钮。
   新策略配置文件向导启动。
5. 在向导的“**策略配置文件名称**”窗口，指定以下内容：
   a. 策略配置文件的名称
      配置文件名称不能包括 100 个以上字符。
   b. 策略配置文件状态(*已启用*或*已禁用*)
      我们建议您仅在完成了策略配置文件激活条件后创建和启动不活动的策略配置文件。

6. 选择“**关闭新策略配置文件向导后，转到策略配置文件激活规则的配置**”复选框以启动新策略配置文件激活规则向导。请按照向导的步骤进行操作。

7. 在策略配置文件属性窗口编辑策略配置文件设置，以您请求的方式。

8. 通过单击“**确定**”保存更改。

   配置文件被保存。配置文件将在满足激活条件的设备上激活。

您可以为单个策略创建多个配置文件。为策略创建的配置文件显示在“**策略配置文件**”区域中的策略属性中。您可以修改策略配置文件并更改配置文件优先级，以及删除配置文件。

修改策略配置文件

编辑策略配置文件的设置

只有 Kaspersky Endpoint Security for Windows 的策略才支持编辑策略配置文件。

修改策略配置文件：

1. 在控制台树中，选择必须为其修改策略配置文件的管理组。

2. 在该组的工作区中，选择“**策略**”选项卡。

3. 选择策略并使用上下文菜单切换到策略属性窗口。

4. 打开策略属性中的“**策略配置文件**”区域。

   此部分包含已为策略创建的配置文件的列表。配置文件按照它们的优先级显示在该列表中。

5. 选择策略配置文件并单击“**属性**”按钮。

6. 在属性窗口中配置配置文件：

   - 如果需要，请在“**常规**”区域中更改配置文件名称，并使用“**启用配置文件**”复选框来启用或禁用配置文件。
   - 在“**激活规则**”区域中，编辑配置文件激活规则。
   - 在相应的区域中编辑策略设置。

7. 单击“**确定**”。

您已修改的设置将在设备与管理服务器同步之后生效（如果策略配置文件处于活动状态），或在激活规则触发之后生效（如果策略配置文件处于非活动状态）。

更改策略配置文件的优先级

策略配置文件的优先级决定了配置文件在客户端设备上的激活顺序。如果为不同策略配置文件设置了相同激活规则，则会使用优先级。

例如：已创建了以下两个策略配置文件：*配置文件 1*和*配置文件 2*，它们的差异是某一个设置分别使用各自的值（*值 1*和*值 2*）。*配置文件 1*的优先级高于配置文件 *2*。此外，还有一些配置文件，它们的优先级低于*配置文件 2*。这些配置文件的激活规则是相同的。

当激活规则触发时，*配置文件 1*将被激活。设备上的设置将使用*值 1*。如果您删除了*配置文件 1*，则*配置文件 2*将有最高的优先级，因此设置将使用*值 2*。

在策略配置文件列表上，配置文件按照它们各自的优先级显示。优先级最高的配置文件排列在最前。您可以使用向上箭头 和向下箭头 按钮更改配置文件优先级。

删除策略配置文件

要删除策略配置文件：

1. 在控制台树中，选择您要为其删除策略配置文件的管理组。
2. 在该管理组的工作区中，选择“**策略**”选项卡。
3. 选择策略并使用上下文菜单切换到策略属性窗口。
4. 打开 Kaspersky Endpoint Security 策略属性中的“**策略配置文件**”区域。
5. 选择您要删除的策略配置文件并单击“**删除**”按钮。

策略配置文件将被删除。活动状态将传递到在设备上触发的激活规则的另一个策略配置文件，或者传递到策略。

创建策略配置文件激活规则

要创建策略配置文件激活规则：

1. 在控制台树中，选择您要为其创建策略配置文件激活规则的管理组。
2. 在该组的工作区中，选择“**策略**”选项卡。
3. 选择策略并使用上下文菜单切换到策略属性窗口。
4. 选择策略属性窗口中的“**策略配置文件**”区域。
5. 选择您需要创建激活规则的策略配置文件，然后点击“**属性**”按钮。
   “策略配置文件”窗口打开。
   如果策略配置文件列表为空，您可以创建策略配置文件。
6. 选择“**激活规则**”区域，然后点击“**添加**”按钮。
   新策略配置文件激活规则向导开启。
7. 在“**策略配置文件激活规则**”窗口，选择影响您当前所创建策略配置文件激活的条件旁边的复选框：
   - **策略配置文件激活常规规则**

     选择该复选框根据设备离线模式状态设置设备上的策略配置文件激活规则、连接管理服务器规则和分配给设备的标记。

- **活动目录使用规则**

  选择该复选框根据设备在活动目录组织单元中的出现或者设备在活动目录安全组中的成员关系设置设备上的策略配置文件激活规则。

- **特殊设备所有者规则**

  选择该复选框根据设备所有者设置设备上的策略配置文件激活规则。

- **硬件说明书规则**

  选择该复选框根据内存和逻辑处理器数量设置设备上的策略配置文件激活规则。

向导的附加页面数量取决于您在第一步选择的设置。您可以稍后修改策略配置文件激活规则。

8. 在“**常规条件**”窗口，指定以下设置：

   - 在“**设备已离线**”字段的在下拉列表中指定设备在网络中出现的条件：

     - **是**

       设备在外部网络，管理服务器不可用。

     - **否**

       设备在网络中，因此管理服务器可用。

     - **未选择值**

       将不应用标准。

   - 如果管理服务器连接规则在此设备上已执行/未执行，请在“**设备位于指定的网络位置**”框中，使用下拉列表设置策略配置文件激活：

     - **已执行 / 未执行**

       策略配置文件激活条件(规则是否被执行)。

     - **规则名称**

       用于连接到管理服务器的设备网络位置描述，它的条件必须被满足(或不满足)以便激活策略配置文件。

       用于连接到管理服务器的设备网络位置描述可以在网络代理切换规则中被创建或配置。

如果选中“**策略配置文件激活常规规则**”复选框，则将显示“**常规条件**”窗口。

9. 在“**使用标签的条件**”窗口，指定以下设置：

- **标签列表**

  在标签列表中，通过选中与相应标签对应的选框，可以指定策略配置文件中的设备包含规则。

  您可以通过列表上方的字段添加新标签到列表，并单击“**添加**”按钮。

  策略配置文件包含具有选定标签的设备。如果清除选框，则将不应用该标准。默认情况下已清除这些选框。

- **应用到没有指定标签的设备**

  如果必须转换标签分类，则启用此选项。

  如果启用此选项，策略配置文件将包含未带有所选标签的描述的设备。如果禁用此选项，则不应用该标准。

  默认情况下已禁用该选项。

如果选中“**策略配置文件激活常规规则**”复选框，则将显示“**使用标签的条件**”窗口。

10. 在**使用活动目录的条件**窗口，指定以下设置：

- **在活动目录安全组中的设备所有者成员关系**

  如果启用此选项，其所有者是指定安全组成员的设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **在活动目录安全组中的设备成员关系**

  如果启用此选项，设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **在活动目录组织单元中的设备分配**

  如果启用此选项，指定 Active Directory 组织单元 (OU) 中包括的设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。

  默认情况下已禁用该选项。

如果选中了**使用活动目录的条件**复选框，则会显示**活动目录使用规则**窗口。

11. 在**使用设备所有者的条件**窗口，指定以下设置：

- **设备所有者**

  启用此选项可根据设备所有者在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

  - 设备属于指定的拥有者（"="符号）。
  - 设备不属于指定的拥有者（“#”符号）。

    如果启用该选项，配置文件根据配置的标准在设备上激活。启用此选项时，您可以指定设备所有者。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **设备所有者包含在内部安全组**

  启用此选项可通过所有者在 Kaspersky Security Center 内部安全组中的资格在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

  - 设备所有者是指定安全组的成员（"="符号）。
  - 设备所有者不是指定安全组的成员（“#”符号）。

    如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定 Kaspersky Security Center 的安全组。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **由设备所有者特定角色激活策略配置文件**

  选择该选项以在设备上根据所有者角色配置和启用配置文件激活规则。从现有角色列表手动添加角色。

  如果启用该选项，配置文件根据配置的标准在设备上激活。

如果选中“**使用设备所有者的条件**”复选框，则将显示“**特殊设备所有者规则**”窗口。

12. 在**使用设备说明的条件**窗口，指定以下设置：

- **内存大小(MB)**

  启用此选项可通过设备上可用 RAM 容量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

  - 该设备内存大小小于指定值("<" 符号)。
  - 该设备内存大小大于指定值(">" 符号)。

  如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的 RAM 卷。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **逻辑处理器数量**

  启用此选项可通过设备上逻辑处理器数量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

  - 设备上逻辑处理器数量少于或等于指定值 （"<" 符号）。
  - 设备上逻辑处理器数量大于或等于指定值 （">" 符号）。

  如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的逻辑处理器数量。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

如果选中**硬件说明书规则**复选框，将显示**使用设备说明的条件**窗口。

13. 在“**策略配置文件激活规则名称**”窗口的“**规则名称**”字段，指定规则的名称。

配置文件将被保存。当触发激活规则时，将在设备上激活该配置文件。

为配置文件创建的策略配置文件激活规则显示在策略配置文件属性的“**激活规则**”区域。您可以修改或删除任何策略配置文件激活规则。

多个激活规则可以被一起触发。

设备移动规则

建议使用*设备移动规则*自动分配设备到管理组。设备移动规则由三个主要部分组成：名称、执行条件（带设备属性的逻辑表达式）和目标管理组。如果设备属性满足规则执行条件，则规则移动设备到目标管理组。

所有设备移动规则都有优先级。管理服务器检查设备属性是否满足每条规则的执行条件（按优先级进行升序排列）。如果设备属性满足某条规则的执行条件，设备被移动到目标组，至此规则处理在该设备上完成。如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

设备移动规则可以被间接创建。例如，在安装包或远程安装任务的属性中，您可以指定安装网络代理后设备必须被移动到的管理组。而且，设备移动规则可以被 Kaspersky Security Center 管理员明确创建，在移动规则列表。列表位于管理控制台的“**未分配的设备**”组属性中。

默认情况下，设备移动规则用于设备到管理组的一次性初始分配。规则仅移动“**未分配的设备**”组的设备一次。一旦设备被该规则移动，该规则不会再次移动该设备，即便您把设备手动放回“**未分配的设备**”组。这是应用移动规则的推荐方法。

您可以移动已经被分配的设备到一些管理组。为此，在规则的属性中，请清空“**仅移动不属于任何管理组的设备**”复选框。

应用移动规则到已经分配到一些管理组中的设备会显著增加管理服务器负载。

仅移动不属于任何管理组的设备复选框在自动创建的移动规则的属性中被锁定。当您添加*远程安装应用程序*任务或创建独立安装包时，会创建此类规则。

您可以创建重复影响单一设备的移动规则。

我们强烈建议您避免从一个组重复移动单一设备到另一个组(例如，为了应用特别策略到该设备，运行特别组任务，或者通过特别分发点更新设备)。

此类方案不被支持，因为它们显著增加了管理服务器负载和网络流量。这些方案也与 Kaspersky Security Center 的操作原则冲突(尤其在访问权限、事件和报告方面)。必须找到其他解决方案，例如，通过使用策略配置文件、设备分类的任务、根据标准方案分配网络代理。

克隆设备移动规则

当您必须创建多个带有相似设置的设备移动规则时，您可以克隆现有规则然后更改所克隆规则的设置。例如，当您必须具有几个带有不同 IP 范围和目标组的相似的设备移动规则时，这是有用的。

要克隆设备移动规则：

1. 打开主应用程序窗口。
2. 在“**未分配的设备**”文件夹，单击“**配置规则**”。
   属性：未分配的设备窗口打开。
3. 在“**移动设备**”区域，选择您要克隆的设备移动规则。
4. 单击**克隆规则**。

   所选设备移动规则的克隆将被添加到列表的结尾。

新规则以禁用状态被创建。您可以在任何时候编辑和启用规则。

软件分类

监控应用程序运行的主要工具是 *Kaspersky 类别*(也叫 *KL 类别*)。KL 类别帮助 Kaspersky Security Center 管理员简化软件分类和减少到受管理设备的流量。

用户类别必须仅对无法被分类成现有 KL 类别的应用程序创建(例如，对于自定义软件)。基于应用程序安装包(MSI)或带有安装包的文件夹创建的用户类别。

如果有未通过 KL 类别分类的大软件集可用，最好创建一个自动更新的类别。每次对包含分发包的文件夹进行修改时，可执行文件的校验和将被自动添加到该类别。

不要为文件夹“我的文档”、%windir%、%ProgramFiles% 和 %ProgramFiles(x86)% 创建自动更新类别的软件。在这些文件夹的文件轮询受频繁更改的影响，这将导致增加管理服务器负载和网络流量。您必须为软件集创建专用文件夹并定期添加新条目。

安装应用程序到客户端组织设备的先决条件

在客户组织的设备上远程安装应用程序与在企业内远程安装的步骤相同。

要在客户端组织机构的设备上安装应用程序，应执行下列操作：

- 首次在客户端组织机构的设备上安装应用程序之前，应在其上安装网络代理。

  当通过 Kaspersky Security Center 的服务提供商配置网络代理安装包时，应在安装包的属性窗口中调整下列设置：

  - 在“**连接**”区域，“**管理服务器**”字串中指定与虚拟管理服务器相同的地址。该服务管理器是在安装网络代理至分发点时所指定的。
  - 在“**高级**”区域，选择“**通过使用连接网关连接到管理服务器**”复选框。在“**连接网关地址**”字串，指定分发点地址。您可以使用设备 IP 地址或 Windows 网络中的设备名称。
- 选择“**通过分发点使用操作系统资源**”作为网络代理安装包的下载方法。您可以选择以下下载方法：
  - 如果使用远程安装任务来安装应用程序，您可以以两种方式之一指定下载方法：
    - 在“**设置**”窗口中，创建远程安装任务
    - 在远程安装任务的属性窗口，通过“**设置**”区域
  - 如果使用远程安装向导来安装应用程序，您可以在此向导的“**设置**”窗口中选择下载方法。
- 由分发点用于验证的账户应该拥有在所有客户端设备上访问管理资源的权限。

查看和编辑本地应用程序设置

Kaspersky Security Center 管理系统允许您通过管理控制台在设备上远程管理本地应用程序设置。

*本地应用程序设置*是指设备上的应用程序的设置。您可以使用 Kaspersky Security Center 为管理组中的设备指定本地应用程序设置。

关于 Kaspersky 程序设置的详细说明，请参阅相关指南。

要查看或更改应用程序的本地设置，请执行以下操作：

1. 在相关设备所在的组工作区中，选择“**设备**”选项卡。
2. 在设备属性窗口中的“**应用程序**”区域，选择相关的应用程序。
3. 双击应用程序名称或单击“**属性**”按钮，打开应用程序属性窗口。

这样即可打开所选程序的本地设置窗口，您可以查看并编辑这些设置。

您可以修改未被组策略禁止修改的设置值（例如：未在策略中以锁定图标（🔒）标记的设置）。

更新 Kaspersky Security Center 和受管理应用程序

该部分描述了更新 Kaspersky Security Center 和受管理应用程序的步骤。

方案：定期更新 Kaspersky 数据库和应用程序

本部分提供定期更新 Kaspersky 数据库、软件模块和应用程序的方案。在您完成配置网络保护方案后，您必须维持保护系统的可靠性以确保管理服务器和受管理设备保持受保护状态以防范各种威胁，包括病毒、网络攻击和钓鱼攻击。

网络保护通过更新以下内容保持最新：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center 组件和安全应用程序

当您完成方案时，您可以确保：

- 您的网络被最新的 Kaspersky 软件保护，包括 Kaspersky Security Center 组件和安全应用程序。
- 对网络安全至关重要的反病毒数据库和其他 Kaspersky 数据库始终保持最新。

先决条件

受管理设备必须连接到管理服务器。如果未建立连接，请考虑手动更新卡巴斯基数据库、软件模块和应用程序或直接从卡巴斯基更新服务器 更新。

管理服务器必须连接到互联网。

在您开始之前，确保您已做了如下：

1. 根据通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序的方案将 Kaspersky 安全应用程序部署到受管理设备。
2. 创建了配置了所有所需策略、策略配置文件和任务，根据网络保护配置方案。
3. 分配了适当数量的分发点，与受管理设备和网路拓扑一致。

更新 Kaspersky 数据库和应用程序分阶段进行：

1. **选择更新 scheme**

   您可以使用若干个 scheme 以安装更新到 Kaspersky Security Center 组件和安全应用程序。选择一个或多个满足您网络需求的 scheme。

2. **创建管理服务器的“将更新下载至存储库”任务**

   该任务由 Kaspersky Security Center 快速启动向导自动创建。如果您未运行向导，立即创建任务。

此任务需要从 Kaspersky 更新服务器下载更新到管理服务器的存储库，以及为 Kaspersky Security Center 更新 Kaspersky 数据库和软件模块。更新被下载后，它们可以被传播到受管理设备。

如果您的网络被分配了分发点，更新被从管理服务器存储库自动下载到分发点存储库。此种情况下，分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。

说明：

- 管理控制台：创建管理服务器的“将更新下载至存储库”任务
- Kaspersky Security Center Web Console：创建管理服务器的“将更新下载至存储库”任务

3 创建“将更新下载至分发点存储库”任务（可选）

默认下，更新被从管理服务器下载到分发点。您可以配置 Kaspersky Security Center 直接从 Kaspersky 更新服务器下载更新到分发点。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

当您的网络已分配分发点并已创建“*将更新下载至分发点存储库*”任务时，分发点从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库下载。

说明：

- 管理控制台：创建“将更新下载至分发点存储库”任务
- Kaspersky Security Center Web Console：创建“将更新下载至分发点存储库”任务

4 配置分发点

当您的网络已分配分发点时，确保在所有所需分发点的属性中启用“**部署更新**”选项。当该选项对分发点禁用时，包含在分发点范围中的设备从管理服务器存储库下载更新。

如果您希望受管理设备仅从分发点接收更新，请在网络代理策略中启用“**仅通过分发点分发文件**”选项。

5 通过使用更新下载或差异文件的离线模型来优化更新过程（可选）

您可以通过使用离线模式更新下载（默认启用）或使用 diff 文件优化更新过程。对于每个网段，您必须选择应用哪个功能，因为它们无法同时工作。

当离线模式更新下载被启用时，一旦更新被下载到管理服务器存储库，在安全应用程序请求更新之前，网络代理就下载所需更新到受管理设备。这确保了更新过程的可靠性。要使用此功能，请启用“网络代理策略”中的“**提前从管理服务器下载更新和反病毒数据库(推荐)**”选项。

如果您不使用离线模式更新下载，您通过使用 diff 文件优化管理服务器和受管理设备之间的流量。启用此功能后，管理服务器或分发点将下载差异文件，而不是整个 Kaspersky 数据库或软件模块文件。diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。因此，diff 文件比整个文件占用更少的空间。这导致降低管理服务器之间或分发点和受管理设备之间的流量。要使用此功能，请在“*将更新下载至管理服务器存储库*”任务和/或“*将更新下载至分发点存储库*”任务的属性中启用“**下载差异文件**”选项。

说明：

- 使用 diff 文件更新 Kaspersky 数据库和软件模块
- 管理控制台：启用和禁用离线模式更新下载
- Kaspersky Security Center Web Console：启用和禁用离线模式更新下载

6 验证已下载的更新（可选）

安装下载的更新之前，您可以通过“*更新验证*”任务验证更新。该任务按顺序运行通过测试设备集的设置来配置的设备更新任务和恶意软件扫描任务。获取任务结果时，管理服务器开始或阻止更新传播到剩余设备。

"*更新验证*"任务可以作为"*将更新下载至管理服务器存储库*"任务的一部分执行。在"*将更新下载至管理服务器存储库*"任务的属性中，在管理控制台中启用"**分发前验证更新**"选项或在 Kaspersky Security Center Web Console 中启用"**运行更新验证**"选项。

说明：

- 管理控制台：验证下载的更新
- Kaspersky Security Center Web Console：验证下载的更新

7 批准和拒绝软件更新

默认下，下载的软件更新具有*未定义*状态。您可以更改状态到*已批准*或*已拒绝*。批准的更新总是被安装。如果更新需要查看和接受最终用户授权许可协议的条款，您需要先接受它们。此后，更新可以被传播到受管理设备。未定义的更新仅可以被安装到网络代理和其他 Kaspersky Security Center 组件，与网络代理策略设置一致。您设置了*已拒绝*状态的更新将不被安装到设备。如果安全应用程序的拒绝的更新先前被安装，Kaspersky Security Center 将尝试从所有设备上卸载该更新。

批准和拒绝更新仅适用于安装在 Windows 和 Linux 客户端设备上的网络代理和受管理的卡巴斯基应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。

说明：

- 管理控制台：批准和拒绝软件更新
- Kaspersky Security Center Web Console：批准和拒绝软件更新

8 配置 Kaspersky Security Center 组件的更新和补丁的自动安装

系统将自动安装下载的网络代理更新和补丁以及其他 Kaspersky Security Center 组件。如果在网络代理属性中启用了"**对未定义状态的组件自动安装可应用更新和补丁**"选项，则所有更新在下载到存储库（或多个存储库）后将自动安装。如果禁用此选项，被下载和标注为*未定义*状态的 Kaspersky 补丁将仅在您改变其状态为*已批准*是被安装。

说明：

- 管理控制台：启用和禁用 Kaspersky Security Center 组件的自动更新和补丁
- Kaspersky Security Center Web Console：启用和禁用 Kaspersky Security Center 组件的自动更新和补丁

9 为管理服务器安装更新

管理服务器软件更新不取决于更新状态。更新不会自动安装，且必须由管理员初步在管理控制台的**监控**选项卡（"**管理服务器** <服务器名称>"→"**监控**"）或 Kaspersky Security Center Web Console 的"**通知**"区域（"**监控和报告**"→"**通知**"）上批准。此后，管理员必须明确运行更新安装。

10 为安全应用程序配置更新的自动安装

为受管理应用程序创建*更新*任务，以提供对应用程序、软件模块和 Kaspersky 数据库（包括反病毒数据库）的及时更新。为确保及时更新，我们建议您配置任务计划时选择"**当新更新下载至存储库时**"选项。

如果您的网络包括仅支持 IPv6 的设备，并且您想要定期更新这些设备上安装的安全应用程序，请确保受管理设备上已安装管理服务器版本（版本不早于 13.2）和网络代理（版本不早于 13.2）。

默认下，Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 的更新在您更改更新状态到*已批准*后被安装。您可以在*更新*任务中更改更新设置。

如果更新需要查看和接受最终用户授权许可协议的条款，您需要先接受它们。此后，更新可以被传播到受管理设备。

说明：

- 管理控制台：在设备上自动安装 Kaspersky Endpoint Security 更新
- Kaspersky Security Center Web Console：在设备上自动安装 Kaspersky Endpoint Security 更新

结果

方案完成后，Kaspersky Security Center 配置为在更新下载至管理服务器存储库或分发点存储库后更新 Kaspersky 数据库和已安装的 Kaspersky 应用程序。您然后可以继续监控网络状态。

关于更新 Kaspersky 数据库、软件模块和应用程序

为了确保管理服务器和受管理设备的保护是最新的，您必须提供以下内容的定期更新：

- Kaspersky 数据库和软件模块

  在下载卡巴斯基数据库和软件模块之前，Kaspersky Security Center 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保更新反病毒数据库并保持受管理设备的安全级别是必要的。

- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center 组件和安全应用程序

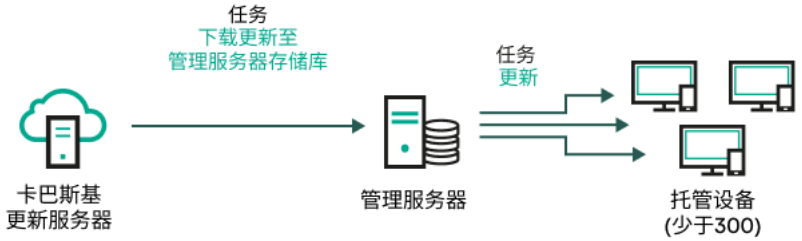
  通过 Kaspersky Security Center，您可以自动更新安装在 Windows 和 Linux 客户端设备上的网络代理和卡巴斯基应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。要更新这些组件，您必须从卡巴斯基网站下载最新版本，然后手动进行安装。

取决于您网络的配置，您可以使用以下方案来下载和分发所需更新到受管理设备：

- 通过使用单个任务：*将更新下载至管理服务器存储库*
- 通过使用两个任务：
  - “*将更新下载至管理服务器存储库*”任务
  - 创建“*将更新下载至分发点存储库*”任务
- 通过本地文件夹、共享文件夹或 FTP 服务器手动
- 直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security
- 如果管理服务器没有互联网连接，则通过本地或网络文件夹

使用“将更新下载至管理服务器存储库”任务

在此方案中，Kaspersky Security Center 通过“*将更新下载至管理服务器存储库*”任务来下载更新。在单一网段包含少于 300 台受管理设备或每个网段包含少于 10 台受管理设备的小网络中，更新直接从管理服务器存储库被分发到受管理设备（参见下图）。

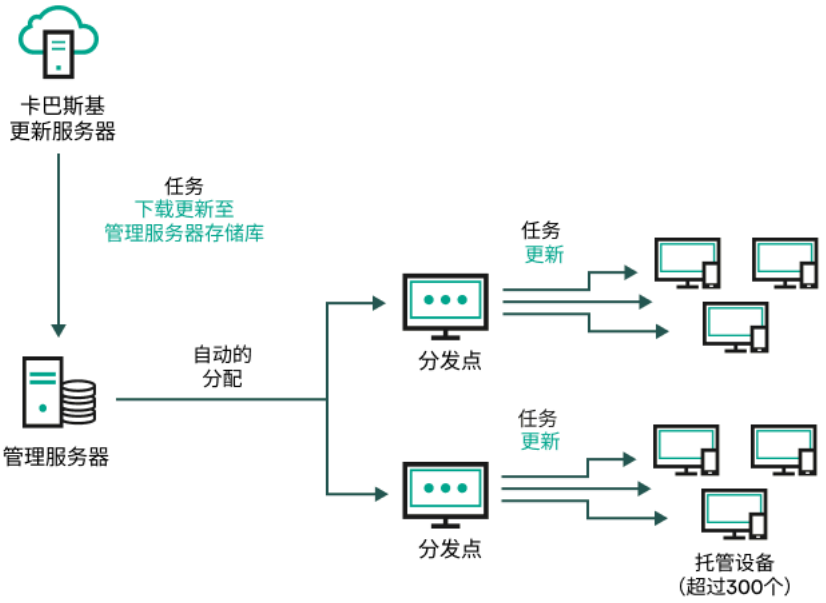


存储库通过使用“将更新下载至管理服务器存储库”任务更新，而不使用分发点

默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

如果您的网络中单一网段包含多于 300 台受管理设备或每个网段包含多于 9 台受管理设备，我们建议您使用分发点传播更新到受管理设备（参见下图）。分发点降低管理服务器负载并优化管理服务器和受管理设备之间的流量。您可以计算数字并配置您网络所需的分发点。

此种方案中，更新被从管理服务器存储库自动下载到分发点存储库。分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。



通过使用“将更新下载至管理服务器存储库”任务更新，并使用分发点

完成“*将更新下载至管理服务器存储库*”任务后，以下更新将下载到管理服务器存储库：

- Kaspersky 数据库和 Kaspersky Security Center 软件模块
  这些更新被自动安装。
- Kaspersky 数据库和受管理设备上安全应用程序的软件模块
  这些更新通过Kaspersky Endpoint Security for Windows 更新任务安装。

- 管理服务器更新

  这些更新不被自动安装。管理员必须明确批准和运行更新安装。

  > 需要本地管理员权限以安装补丁到管理服务器。

- Kaspersky Security Center 模块更新

  默认下，这些更新被自动安装。您可以在网络代理策略中更改设置。

- 安全应用程序更新

  默认情况下，Kaspersky Endpoint Security for Windows 仅安装您批准的更新（您可以通过管理控制台或通过 Kaspersky Security Center Web Console批准更新）。更新通过*更新*任务安装且可以在任务属性中被配置。

> "*将更新下载至管理服务器存储库*"任务在虚拟管理服务器上不可用。虚拟管理服务器的存储库将显示已下载至主管理服务器的更新。

您可以配置在测试设备集上进行更新的操作和错误验证。如果验证成功，更新被分发到其他受管理设备。

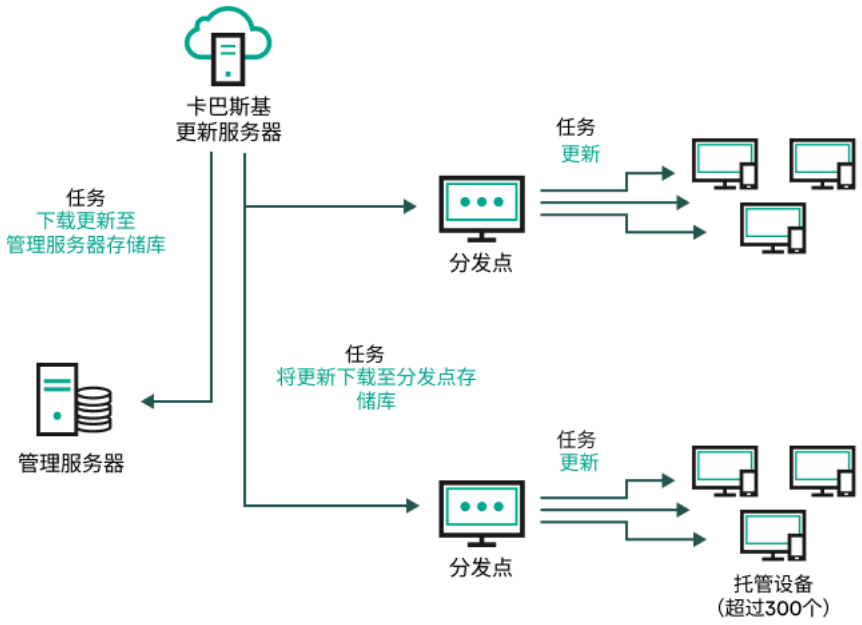
每个卡巴斯基应用程序都从管理服务器请求所需更新。管理服务器集合这些更新并仅下载应用程序请求的更新。这确保了相同更新不被下载多次，且不必要更新不被下载。当运行"*将更新下载至管理服务器存储库*"任务时，管理服务器自动发送以下信息到 Kaspersky 更新服务器以便确保相关版本的 Kaspersky 数据库和软件模块的下载：

- 应用程序 ID 和版本
- 应用程序安装 ID
- 活动密钥 ID
- "*将更新下载至管理服务器存储库*"任务运行 ID

传输的信息都不包含个人数据或其他机密数据。AO Kaspersky Lab 依照法律需求保护信息。

使用两个任务：“将更新下载至管理服务器存储库”任务和“将更新下载至分发点存储库”任务

您可以直接从 Kaspersky 更新服务器下载更新到分发点存储库，而不是从管理服务器存储库，然后分发更新到受管理设备（参见下图）。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。



通过使用“将更新下载至管理服务器存储库”任务和“将更新下载至分发点存储库”任务更新

默认下，管理服务器和分发点与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器和/或分发点使用 HTTP 协议，而不是 HTTPS。

要实施此方案，除了“*将更新下载至管理服务器存储库*”任务外，请创建“*将更新下载至分发点存储库*”任务。此后，分发点将从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库。

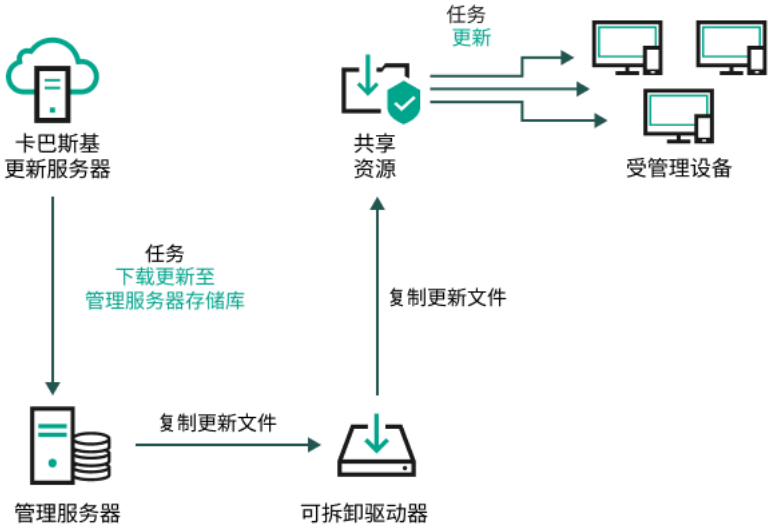
运行 MacOS 的分发点设备无法从 Kaspersky 更新服务器下载更新。

如果一个或多个运行 macOS 的设备在“*将更新下载至分发点存储库*”任务范围内，则该任务将以“*失败*”状态完成，即使该任务在所有 Windows 设备上均已成功完成。

此方案也需要“*将更新下载至管理服务器存储库*”任务，因为该任务被用于下载 Kaspersky 数据库和 Kaspersky Security Center 软件模块。

通过本地文件夹、共享文件夹或 FTP 服务器手动

如果客户端设备未连接到管理服务器，您可以使用本地文件夹或共享资源作为 Kaspersky 数据库、软件模块和应用程序的更新源。在此方案中，您需要从管理服务器存储库复制所需更新到可移动驱动器，然后复制更新到在 Kaspersky Endpoint Security 设置中指定为更新源的本地文件夹或共享资源（参见下图）。



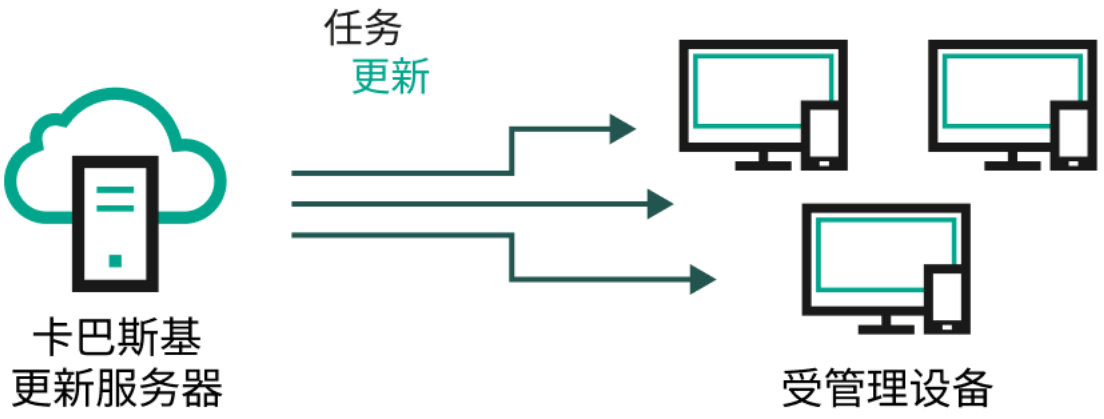
通过本地文件夹、共享文件夹或 FTP 服务器更新

有关 Kaspersky Endpoint Security 中更新源的更多信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助

直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security

在受管理设备上，您可以配置 Kaspersky Endpoint Security 直接从 Kaspersky 更新服务器接收更新（参见下图）。



直接从 Kaspersky 更新服务器更新安全应用程序

在此方案中，安全应用程序不使用 Kaspersky Security Center 提供的存储库。要直接从 Kaspersky 更新服务器接收更新，在安全应用程序界面中指定 Kaspersky 更新服务器作为更新源。有关这些设置的详细信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助

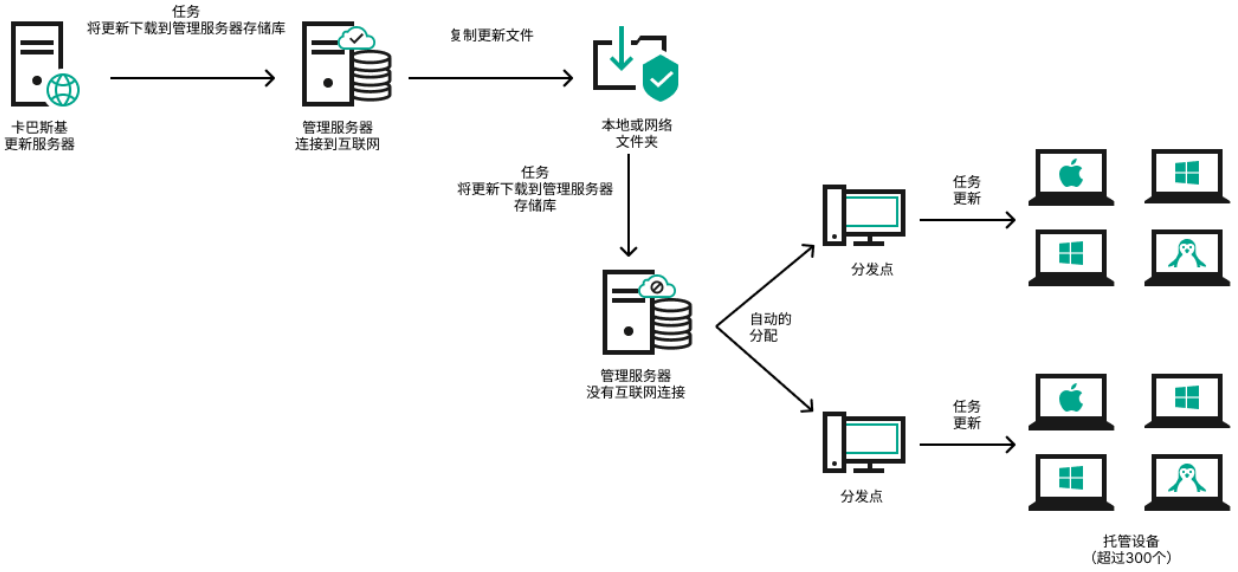
如果管理服务器没有互联网连接，则通过本地或网络文件夹

如果管理服务器没有互联网连接，您可以配置“*将更新下载至管理服务器存储库*”任务以从本地或网络文件夹下载更新。在这种情况下，必须不时地将所需的更新文件复制到指定文件夹。例如，您可以从以下来源之一复制所需的更新文件：

- 具有互联网连接的管理服务器（请参见下图）

  由于管理服务器只下载安全应用程序请求的更新，管理服务器管理的安全应用程序集（有互联网连接的应用程序和没有互联网连接的应用程序）必须匹配。

  如果用于下载更新的管理服务器版本为 13.2 或更早，请打开“*将更新下载至管理服务器存储库*”任务的属性，然后启用“**使用旧方案下载更新**”选项。



如果管理服务器没有互联网连接，则通过本地或网络文件夹更新

- 卡巴斯基更新实用程序

  由于此实用程序使用旧方案下载更新，请打开“*将更新下载至管理服务器存储库*”任务，然后启用“**使用旧方案下载更新**”选项。

关于使用 diff 文件更新 Kaspersky 数据库和软件模块

当 Kaspersky Security Center 从 Kaspersky 更新服务器下载更新时，它通过使用 diff 文件优化流量。您也可以对从网络中其他设备（管理服务器、分发点和客户端设备）获取更新的设备启用对 diff 文件的使用。

关于下载 diff 文件功能

diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。使用 diff 文件节省您公司网络内的流量，因为 diff 文件相比数据库和软件模块的完整文件占据更少的空间。如果对管理服务器或分发点启用 *下载 diff 文件*功能，diff 文件被保存到该管理服务器或分发点。结果，从该管理服务器或分发点获取更新的设备可以使用保存的 diff 文件更新它们的数据库和软件模块。

要优化对 diff 文件的使用，我们建议您根据管理服务器或分发点的更新计划同步从管理服务器或更新代理获取更新的设备的更新计划。然而，即便设备更新频率小于从其获取更新的管理服务器或分发点，流量也被节省。

下载 diff 文件功能仅可以在版本 11 之后的管理服务器和分发点上启用。要在早期版本的管理服务器和分发点上保存 diff 文件，请升级它们到版本 11 或更高版本。

下载 diff 文件功能与离线模式更新下载不兼容。这意味着使用离线模式更新下载的网络代理即便在传送更新到这些网络代理的管理服务器或分发点上启用了下载 diff 文件功能，也不下载 diff 文件。

分发点不对 diff 文件的自动分发使用 IP 多点传送。

启用下载 diff 文件功能

先决条件

方案的先决条件是：

- 管理服务器和分发点被升级到版本 11 或更高版本。
- 离线模式更新下载在网络代理策略设置中被禁用。

阶段

1. **在管理服务器上启用该功能**

   在“将更新下载至管理服务器存储库”任务的设置中启用该功能。

2. **为分发点启用该功能**

   对通过“将更新下载至分发点存储库”任务接收更新的分发点启用该功能。

   然后对从管理服务器接收更新的分发点启用该功能。

   在“网络代理策略设置”中启用了此功能，并且在管理服务器属性的“**分发点**”区域中也已启用（如果手动分配了分发点，并且您想覆盖策略设置）。

要检查下载 diff 文件功能是否被成功启用，您可以在执行方案之前和之后分别测试内部流量。

创建管理服务器的“将更新下载至存储库”任务

管理服务器的“*将更新下载至管理服务器存储库*”任务由 Kaspersky Security Center 快速启动向导自动创建。您只能创建一个“*将更新下载至管理服务器存储库*”任务。因此，要想创建“*将更新下载至管理服务器存储库*”任务，必须先将管理服务器任务列表中的此类任务移除。

要创建“将更新下载至管理服务器存储库”任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 通过下列方式开始创建任务：
   - 在控制台树的“**任务**”文件夹的上下文菜单中，选择**新建 → 任务**。
   - 在“**任务**”文件夹的工作区，单击“**创建任务**”按钮。

   “新任务向导”启动。遵照向导的说明。
3. 在向导的“**选择任务类型**”页面，选择**将更新下载至管理服务器存储库**。
4. 在向导的“**设置**”页面指定任务设置，如下所示：
   - **更新源**

     以下资源可以用作管理服务器的更新源：

     - 卡巴斯基更新服务器

       Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

       默认选择。

     - 主管理服务器

       此资源适用于为从属或虚拟管理服务器创建的任务。

     - 本地或网络文件夹

       包含最新更新的本地或网络文件夹。网络文件夹可以是 FTP 或 HTTP 服务器，或者 SMB 共享。如果网络文件夹需要身份验证，则仅支持 SMB 协议。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

       更新源所使用的 FTP 或 HTTP 服务器或网络文件夹必须包含匹配 Kaspersky 更新服务器所创建的结构的文件夹结构（带有更新）。

   - **其他设置**：
     - **强制从属管理服务器更新**

       如果启用该选项，当新更新下载后管理服务器立刻在从属管理服务器上启动更新任务。更新任务通过使用在从属管理服务器上的任务属性中配置的更新源来启动。

如果禁用此选项，从属管理服务器上的更新任务将根据计划启动。

默认情况下已禁用该选项。

- **复制下载的更新到附加文件夹**

  管理服务器接收更新后，它复制它们到指定文件夹。如果您想要在您的网络上手动管理更新的分发，则使用该选项。

  例如，您可能要在以下情况下使用该选项：您组织的网络包含几个独立子网，且每个子网的设备不能访问其他子网。然而，所有子网中的设备都可以访问通用网络共享。此种情况下，您在子网之一设置管理服务器从 Kaspersky 更新服务器下载更新，启用该选项，然后指定该网络共享。对于其他管理服务器的"将更新下载至存储库"任务中，指定与更新源相同的网络共享。

  如果您选择将下载的更新复制到本地文件夹，则必须在已安装管理服务器的设备上指定文件夹。文件夹路径取决于设备的操作系统。由于本地文件夹位于基于 Linux 的管理服务器上，因此您必须指定 POSIX 路径，例如 /path/to/dir。

  选择位于基于 Linux 的管理服务器上的网络文件夹时，您必须预先确保已安装管理服务器的设备可以通过挂载该文件夹来访问该网络文件夹。对文件夹的访问使用 SMB 协议执行。

  默认情况下已禁用该选项。

  - **在复制完成之前不强制更新设备和从属管理服务器**

    下载更新到客户端设备和从属管理服务器任务仅在这些更新从主更新文件夹被复制到附加更新文件夹后才启动。

    如果客户端设备和从属管理服务器从附加网络文件夹下载更新，则必须启用该选项。

    默认情况下已禁用该选项。

- **使用旧方案下载更新**

  从版本 14 开始，Kaspersky Security Center 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用"**使用旧方案下载更新**"选项。否则，更新下载任务将失败。

  例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

  - 卡巴斯基更新实用程序

    此实用程序使用旧方案下载更新。

  - Kaspersky Security Center 13.2 或更低版本

    例如，您的管理服务器 1 没有互联网连接。在这种情况下，您可以使用具有互联网连接的管理服务器 2 下载更新，然后将更新放置到本地或网络文件夹以将其用作管理服务器 1 的更新源。如果管理服务器 2 的版本为 13.2 或更低，请在管理服务器 1 的任务中启用"**使用旧方案下载更新**"选项。

  默认情况下已禁用该选项。

5. 在向导的“**配置任务计划**”页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期一于当前系统时间运行一次。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - **每天(不支持夏令时)**

    任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

    我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。

    默认下，任务每天于当前系统时间运行一次。

  - **每周**

    任务每周在指定星期和指定时间运行。

  - **按星期中的天数**

    任务在每周指定日期的指定时间定期运行。

    默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

- 在搜索栏中输入任务名称，即可根据名称搜索任务。
- 单击排序图标可按名称对任务进行排序。
  默认情况下，任务按字母顺序升序排列。
- 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

6. 在向导的“**定义任务名称**”页面，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

7. 在向导的“**完成任务创建**”页面，单击“**完成**”按钮关闭向导。
   如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

向导结束后，“**将更新下载至管理服务器存储库**”出现在工作区的管理服务器任务列表中。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

当管理服务器执行“*将更新下载至管理服务器存储库*”任务时，数据库和软件模块更新将从更新源下载并存储在管理服务器共享文件夹中。如果您为管理组创建此任务，它将仅被应用到包含在指定管理组中的网络代理。

这些更新将从管理服务器共享文件夹分发至客户端设备和从属管理服务器。

创建“将更新下载至分发点存储库”任务

运行 macOS 的分发点设备无法从 Kaspersky 更新服务器下载更新。

如果一个或多个运行 macOS 的设备在“*将更新下载至分发点存储库*”任务范围内，则该任务将以“*失败*”状态完成，即使该任务在所有 Windows 设备上均已成功完成。

您可以为管理组创建“*将更新下载至分发点存储库*”任务。该任务将为包含在指定管理组中的分发点运行。

您可以使用该任务，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。如果分发点使用代理服务器连接到互联网，则必须在网络代理策略中指定相应的设置。

要为所选管理组创建“将更新下载至分发点存储库”任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在该文件夹的工作区，点击“**新任务**”按钮。

   “新任务向导”启动。遵照向导的说明。
3. 在向导的“**选择任务类型**”页面，选择“**Kaspersky Security Center 管理服务器**”节点，展开“**高级**”文件夹，然后选择“**将更新下载至分发点存储库**”任务。
4. 在向导的“**设置**”页面指定任务设置，如下所示：

   - **更新源**

     以下资源可以用作分发点的更新源：

     - Kaspersky 更新服务器

       Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

       默认情况下已选中该选项。

     - 本地或网络文件夹

       包含最新更新的本地或网络文件夹。网络文件夹可以是 FTP 或 HTTP 服务器，或者 SMB 共享。如果网络文件夹需要身份验证，则仅支持 SMB 协议。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

       更新源所使用的 FTP 或 HTTP 服务器或网络文件夹必须包含匹配 Kaspersky 更新服务器所创建的结构的文件夹结构（带有更新）。

   - **更新存储文件夹**

     用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

- **使用旧方案下载更新**

  从版本 14 开始，Kaspersky Security Center 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

  例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

  - 卡巴斯基更新实用程序

    此实用程序使用旧方案下载更新。

  - Kaspersky Security Center 13.2 或更低版本

    例如，分发点配置为从本地或网络文件夹获取更新。在这种情况下，您可以使用具有互联网连接的管理服务器下载更新，然后将更新放置到分发点的本地或网络文件夹。如果管理服务器的版本为 13.2 或更低，请在“*将更新下载至分发点存储库*”任务中启用“**使用旧方案下载更新**”选项。

  默认情况下已禁用该选项。

5. 在向导的“**选择管理组**”页面，点击“**浏览**”并选择要应用任务的管理组。

6. 在向导的“**配置任务计划**”页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期一于当前系统时间运行一次。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每天(不支持夏令时)**

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。

  默认下，任务每天于当前系统时间运行一次。

- **每周**

  任务每周在指定星期和指定时间运行。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

7. 在向导的“**定义任务名称**”页面，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

8. 在向导的“**完成任务创建**”页面，单击“**完成**”按钮关闭向导。

   如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

   当向导完成操作时，“**将更新下载至分发点存储库**”出现在目标管理组和控制台“**任务**”工作区的网络代理任务列表。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

执行“*Download updates to the repositories of distribution points*”任务时，数据库和软件模块的更新从更新源下载并存储在共享文件夹。下载的更新将仅被包含在指定管理组的分发点和没有更新下载任务的更新代理使用。

在管理服务器属性窗口的“**区域**”窗格，选择“**分发点**”。在每个分发点的属性中，在“**更新源**”区域，您可以指定更新源（“**从管理服务器检索**”或“**使用强制更新下载任务**”）。默认情况下，已为手动或自动分配的分发点选中“**从管理服务器检索**”。这些分发点将使用“*将更新下载至分发点存储库*”任务的结果。

每个分发点的属性指定了为单个分发点设置的网络文件夹。文件夹名称可能根据不同分发点而变化。因为这个原因，如果任务是为组设备创建，我们不建议您在任务属性中更改网络文件夹。

如果“*将更新下载至分发点存储库*”任务是设备的本地任务，您可以在其属性中更改网络文件夹。

配置管理服务器的“将更新下载至存储库”任务

要配置管理服务器的“将更新下载至存储库”任务：

1. 在“**任务**”控制台树文件夹的工作区，在任务列表中选择**将更新下载至管理服务器存储库**。

2. 以下列方式之一打开任务属性窗口：

   - 通过从任务的上下文菜单中，选择“**属性**”。

   - 在所选任务的区域中，单击“**配置任务**”链接。

   *将更新下载至管理服务器存储库*任务属性窗口将打开。在此窗口中，您可以配置如何将更新下载至管理服务器存储库。

验证已下载的更新

安装更新到受管理设备之前，您可以先通过“*更新验证*”任务检查更新。作为“*将更新下载至管理服务器存储库*”任务的一部分，“*更新验证*”任务会自动执行。管理服务器从更新源下载更新，将其保存在临时存储库并执行“*更新验证*”任务。如果任务成功完成，更新将从临时存储库复制到管理服务器共享文件夹（Kaspersky Security Center 安装文件夹\Share\Updates）。它们被分发到所有以该管理服务器为更新源的客户端设备。

如果“*更新验证*”任务的结果显示位于临时存储库中的更新是错误的，或“*更新验证*”任务发生错误，这些更新不会被复制到共享文件夹。管理服务器保留之前的更新集。此外，计划类型为“**当新更新下载至存储库时**”的任务也不会启动。如果新更新扫描成功完成，在下次启动“*将更新下载至管理服务器存储库*”任务时将执行这些操作。

如果在一台或多台测试设备上出现以下情况，那么更新集合就被认为是无效的：

- 发生了更新任务错误。
- 安全应用程序的实时保护状态在应用更新后更改。
- 运行按需扫描任务过程中发现了一个被感染的对象。
- Kaspersky 程序出现运行时错误。

如果在任何测试设备上未出现以上情况，该更新集就被认为是有效的，“*更新验证*”任务被认为已成功完成。

在开始创建“*更新验证*”任务之前，请执行先决条件：

1. 创建包含多台测试设备的管理组。您将需要该组来验证其更新。

   建议使用网络中具有最可靠的保护和最常用的应用程序配置的设备。这种方法可提高扫描期间病毒检测的质量和可能性，并将误报的风险降至最低。如果在测试设备上检测到病毒，“*更新验证*”任务将被视为不成功。

2. 为 Kaspersky Security Center 支持的应用程序（例如 Kaspersky Endpoint Security for Windows 或 Kaspersky Security for Windows Server）创建*更新*和*恶意软件扫描*任务。创建*更新*和*恶意软件扫描*任务时，请指定具有测试设备的管理组。

   “*更新验证*”任务会在测试设备上依次运行*更新*和*恶意软件扫描*任务，以检查所有更新是否有效。此外，在创建“*更新验证*”任务时，您需要指定*更新*和*恶意软件扫描*任务。

3. 创建“*将更新下载至管理服务器存储库*”任务。

要让 Kaspersky Security Center 将更新分发至客户端设备前对下载的更新进行验证，请执行以下操作：

1. 在“**任务**”文件夹的工作区中，在任务列表中选择“*将更新下载至管理服务器存储库*”任务。
2. 以下列方式之一打开任务属性窗口：
   - 通过从任务的上下文菜单中，选择“**属性**”。
   - 在所选任务工作区中，单击“**配置任务**”链接。
3. 如果“*更新验证*”任务存在，请单击“**浏览**”按钮。在打开的窗口中，在具有测试设备的管理组中选择“*更新验证*”任务。

4. 如果您先前未创建“*更新验证*”任务，请单击“**创建**”按钮。

   这将启动*更新验证*任务向导。遵照向导的说明操作。

5. 单击“**OK**”关闭“*将更新下载至管理服务器存储库*”任务的属性窗口。

自动更新验证被启用。现在，您可以运行“*将更新下载至管理服务器存储库*”任务，它将从更新验证开始。

配置测试策略和辅助任务

在创建“*更新验证*”任务时，管理服务器将生成测试策略、辅助组更新任务以及按需扫描任务。

辅助组更新和按需扫描任务可能需要一些时间。这些任务在“*更新验证*”任务执行时执行。在执行“*将更新下载至存储库*”任务时，执行“*更新验证*”任务。“*将更新下载至存储库*”任务的持续时间包括辅助组更新和按需扫描任务。

您可以更改测试策略和辅助组任务的设置。

要更改测试策略和辅助任务的设置，请执行以下操作：

1. 在控制台树中，选择为其创建“*更新验证*”任务的组。
2. 在该组的工作区中，选择以下选项卡之一：
   - **策略**，如果您希望编辑测试策略设置。
   - **任务**，如果您希望更改辅助任务设置。
3. 在选项卡工作区中选择您希望更改其设置的策略或任务。
4. 以下列方式之一打开策略（任务）属性窗口：
   - 从策略（任务）的上下文菜单中，选择“**属性**”。
   - 在所选策略（任务）的信息框中，单击“**配置策略**”(“**配置任务**”)链接。

要正确验证更新，请在修改测试策略和辅助任务时设置以下限制：

- 在辅助任务设置中：
  - 将所有重要级别为“**严重事件**”和“**功能失败**”的任务保存在管理服务器上。管理服务器将使用这些类型的事件来分析应用程序运行状况。
  - 使用管理服务器作为更新源。
  - 指定任务计划类型：**手动**。
- 在测试策略设置中：
  - 禁用 iChecker 和 iSwift 扫描加速技术（**基本威胁防护 → 文件威胁防护 → 设置 → 其他 → 扫描技术**）。
  - 选择对受感染对象采取的操作：**清除；如果清除失败则删除/清除；如果清除失败则阻止/阻止**。（**基本威胁防护 → 文件威胁防护 → 检测到威胁后的操作**）。

- 在测试策略和辅助任务设置中：

  如果安装软件模块更新后需要重启计算机，必须立即执行。如果设备没有重启，则无法测试此类型的更新。对于一些需要重启的应用程序更新安装，重启可能被阻止，或配置为首先提示用户确认。应在测试策略和辅助任务设置中禁用这些限制规定。

浏览已下载的更新

要查看已下载的更新，

在控制台树的“**存储库**”文件夹，选择“**卡巴斯基数据库和软件模块更新**”子文件夹。

“**卡巴斯基数据库和软件模块更新**”文件夹的工作区中将显示管理服务器中保存的更新列表。

在设备上自动安装 Kaspersky Endpoint Security 更新

您可以在客户端设备上配置 Kaspersky Endpoint Security 自动更新数据库和软件模块。

要在设备上配置下载和自动安装 Kaspersky Endpoint Security 更新：

1. 在控制台树中，选择“**任务**”文件夹。
2. 通过以下方式创建“**更新**”任务：
   - 在控制台树的“**任务**”文件夹的上下文菜单中，选择**新建 → 任务**。
   - 在“**任务**”文件夹工作区中单击“**新任务**”按钮。

   “新任务向导”启动。遵照向导的说明。
3. 在向导的“**选择任务类型**”页面，选择“**Kaspersky Endpoint Security**”做为任务类型，然后选择“**更新**”做为任务子类型。
4. 遵照剩余的向导说明。

   向导完成后，Kaspersky Endpoint Security 更新任务将被创建。新创建的任务显示在“**任务**”文件夹工作区的任务列表。
5. 在“**任务**”文件夹的工作区，选择您已创建的更新任务。
6. 从任务的上下文菜单中，选择“**属性**”。
7. 在打开的任务属性窗口中，在“**区域**”窗格选择“**选项**”。

   在“**选项**”区域，您可以定义本地或移动模式的更新任务设置：
   - **本地模式更新设置**：连接在设备和管理服务器之间建立。
   - **移动模式更新设置**：Kaspersky Security Center 和设备之间不建立特定的连接（比如，当设备没有连接到互联网）。
8. 点击**设置**按钮选择更新源。

9. 选择“**下载应用程序模块更新**”选项，以下载并安装软件模块更新以及应用程序数据库。

   如果选中该复选框，Kaspersky Endpoint Security 在运行更新任务时，通知用户有可用的软件模块更新并且更新包包含软件模块更新。配置更新模块的使用：

   - **安装严重与经批准的更新**。如果软件模块有任何更新，Kaspersky Endpoint Security 自动安装*关键*状态的更新；其余的更新会在您批准后安装。
   - **仅安装批准的更新**。如果软件模块有任何更新，Kaspersky Endpoint Security 在安装批准后安装它们；它们将被通过程序接口或通过 Kaspersky Security Center 本地安装。

   如果软件模块更新需要审查并接受授权许可协议和隐私策略，程序将在用户接受用户授权许可协议和隐私策略的条款后安装更新。

10. 选择“**复制更新到文件夹**”选项，以使应用程序将下载的更新保存到文件夹，然后单击“**浏览**”按钮指定该文件夹。

11. 单击“**确定**”。

更新任务正在运行时，程序发送请求到 Kaspersky 更新服务器。

一些更新需要安装最新版本的管理插件。

离线模式更新下载

受管理设备上的网络代理有时可能不会连接到管理服务器来接收更新。例如，网络代理可能安装在有时没有网络连接的笔记本电脑上。而且，管理员可能会限制设备连接到网络的时间。此种情况下，安装了网络代理的设备无法按照现有计划从管理服务器接收更新。如果您已经使用网络代理配置了受管理应用程序的更新（例如 Kaspersky Endpoint Security），每个更新都请求连接到管理服务器。如果网络代理和管理服务器之间没有建立连接，则无法更新。您可以配置网络代理和管理服务器之间的连接，以便网络代理在指定的时间段连接到管理服务器。最坏的情况是，如果指定的时间段内没有网络连接可用，数据库将不会被更新。除此之外，如果多个受管理应用程序同时尝试访问管理服务器以接收更新，可能会发生问题。此种情况下，管理服务器可能停止响应（类似 DDoS 攻击）。

为了避免上述问题，受管理应用程序的离线模式更新和模块的下载在 Kaspersky Security Center 中实现。该模式提供装置以分发更新，无论是否有管理服务器通信渠道无法访问导致的临时问题。该模式也降低管理服务器负载。

离线模式更新下载如何工作

当管理服务器接收更新时，它通知网络代理(安装网络代理的设备)将用于受管理应用程序的更新。当网络代理接收更新的信息后，它提前从管理服务器下载相关文件。在第一次连接网络代理时，管理服务器发起更新下载。网络代理下载所有更新到客户端设备后，更新对该设备上的应用程序可用。

当客户端设备上的受管理应用程序尝试访问网络代理以更新时，该网络代理检查其是否具有所有的更新。如果在受管理应用程序请求更新之前 25 小时内，更新已从管理服务器收到，则网络代理不连接到管理服务器，而是从本地缓存提供更新给受管理应用程序。当网络代理提供更新到客户端设备上的应用程序时，到管理服务器的连接可能不被建立，但是更新不需要连接。

要在管理服务器上分发负载，设备上的网络代理在管理服务器指定的时间段连接到管理服务器并随机下载更新。该时间段取决于安装了下载更新的网络代理的设备的数量和更新的大小。要降低管理服务器负载，您可以使用网络代理做为分发点。

如果更新下载的离线模式被禁用，更新根据更新下载任务的计划被分发。

默认下，离线模式更新下载已启用。

更新下载的离线模式仅用于通过受管理应用程序检索更新任务时，选中“**当新更新下载至存储库时**”作为计划类型的受管理设备。对于其他受管理设备，以实时模式从管理服务器接收更新的方案被使用。

在以下情况下，我们建议您使用相关管理组网络代理策略的设置来禁用更新下载的离线模式：如果受管理应用程序设置为不从管理服务器，而是从 Kaspersky 服务器或网络文件夹检索更新，并且更新下载任务选择了“**当新更新下载至存储库时**”作为计划类型。

启用和禁用离线模式更新下载

我们建议您避免禁用离线模式更新下载。禁用它可能导致更新传送到设备失败。特殊情况下，Kaspersky 技术支持专家可能建议您清空**提前从管理服务器下载更新和反病毒数据库**复选框。然后，您将必须确保接收 Kaspersky 应用程序更新的任务被设置。

要为管理组启用或禁用离线模式更新下载：

1. 在控制台树中，选择您要启用离线模式更新下载的管理组。
2. 在组工作区中，打开“**策略**”选项卡。
3. 在“**策略**”选项卡，选择网络代理策略。
4. 在策略的上下文菜单中，选择“**属性**”。
   打开网络代理策略的属性窗口。
5. 在策略属性窗口中，选择“**管理补丁和更新**”区域。
6. 选中或清除“**提前从管理服务器下载更新和反病毒数据库(推荐)**”复选框以分别启用或禁用更新下载的离线模式。
   默认下，离线模式更新下载已启用。

这样便启用或禁用了离线模式更新下载。

Kaspersky Security Center 组件的自动更新和补丁

默认情况下，为以下应用程序组件自动安装任何下载的更新和补丁：

- Network Agent for Windows
- 管理控制台
- iOS MDM 服务器

Kaspersky Security Center 组件的自动更新和补丁仅对 Windows 设备可用。您可以禁用这些组件的自动更新和补丁。此种情况下，下载的任何更新和补丁将在您改变其状态到*已批准*后被安装。带有*未定义*状态的更新和补丁将不被安装。

启用和禁用 Kaspersky Security Center 组件的自动更新和补丁

在设备上安装网络代理时，自动安装 Kaspersky Security Center 组件更新和补丁被默认启用。您可以在网络代理安装过程中禁用它，或稍后使用策略禁用。

要在设备上本地安装网络代理时禁用 Kaspersky Security Center 组件自动更新和补丁：

1. 在设备上启动网络代理本地安装。
2. 在**高级设置**步骤，清空**自动安装组件的未定义状态的可应用更新和补丁**复选框。
3. 遵照向导的说明操作。

禁用了 Kaspersky Security Center 组件自动更新和补丁的网络代理将被安装在设备。您可以稍后使用策略启用自动更新和补丁。

要在通过安装包安装网络代理到设备时禁用 Kaspersky Security Center 组件自动更新和补丁：

1. 在控制台树中，选择**远程安装 → 安装包**文件夹。
2. 在 **Kaspersky Security Center 网络代理 <版本号>** 包中，选择“**属性**”。
3. 在安装包属性的“**设置**”区域清除“**对未定义状态的组件自动安装可应用更新和补丁**”复选框。

禁用了 Kaspersky Security Center 组件自动更新和补丁的网络代理将被从该数据包安装。您可以稍后使用策略启用自动更新和补丁。

如果在网络代理安装到设备时选择（清空）了该复选框，您可以后续启用（或禁用）使用网络代理策略自动更新。

要使用网络代理策略启用或禁用 Kaspersky Security Center 组件的自动更新和补丁：

1. 在控制台树中，选择您要启用或禁用自动更新和补丁的管理组。
2. 在组工作区中，打开“**策略**”选项卡。
3. 在“**策略**”选项卡，选择网络代理策略。
4. 在策略的上下文菜单中，选择“**属性**”。
   打开网络代理策略的属性窗口。
5. 在策略属性窗口中，选择“**管理补丁和更新**”区域。
6. 选择或清除“**对未定义状态的组件自动安装可应用更新和补丁**”复选框分别启用或禁用自动更新和修补程序。
7. 为该复选框设置锁。

该策略将被应用到所选设备，且 Kaspersky Security Center 组件自动更新和补丁将在这些设备上被启用（禁用）。

自动分发更新

Kaspersky Security Center 允许在客户端设备和从属管理服务器上自动分发并安装更新。

自动将更新分发至客户端设备

要在更新下载至管理服务器存储库之后立即自动发布所选应用程序更新到客户端设备，请执行以下操作：

1. 连接至管理该客户端设备的管理服务器。
2. 以下列方式之一为所选客户端设备创建一个更新部署任务：
   - 如果要将更新分发至属于所选管理组的客户端设备，请创建选定组的任务。
   - 如果要将更新分发至属于不同管理组或不属于任何管理组的客户端设备，请创建特定设备的任务。

   “新任务向导”启动。按照说明执行以下操作：
   a. 在“**任务类型**”向导窗口中，在所需应用程序节点，选择更新部署任务。

      根据您为其创建更新部署任务的具体应用程序，具体任务名称将显示在“**任务类型**”窗口中。有关所选 Kaspersky 程序的更新任务名称的详细信息，请参阅相应指南。

   b. 在“**计划**”向导窗口中，在“**计划开始**”字段中，选择“**当新更新下载至存储库时**”。

   新建的更新分发任务将在每次更新被下载到管理服务器存储库时在选定设备上启动。

如果已为所选设备创建了所选应用程序的更新分发任务，要在“**计划**”区域的“任务属性”窗口中将更新自动发布至客户端设备，请在“**计划开始**”字段中选择“**当新更新下载至存储库时**”选项。

将更新自动分发至从属管理服务器

要在更新下载至主管理服务器存储库之后立即发布到客户端计算机，请执行以下操作：

1. 在控制台树的主管理服务器节点中，选择“**任务**”文件夹。
2. 在工作区的任务列表，选择管理服务器的“将更新下载至管理服务器存储库”任务。
3. 以下列方式打开所选任务的“**设置**”区：
   - 通过从任务的上下文菜单中，选择“**属性**”。
   - 通过在所选任务的信息框中，单击“**编辑设置**”链接。
4. 在任务属性窗口的“**设置**”区域，选择“**其他设置**”子区域，然后单击“**配置**”链接。

5. 在打开的“**其他设置**”窗口中，选择“**强制从属管理服务器更新**”选框。

6. 在管理服务器更新下载任务的设置中，在任务属性窗口**设置**选项卡中，选中**强制从属管理服务器更新**选框。

当主管理服务器检索到更新后，从属管理服务器上的更新下载任务将自动启动，不管它们的计划如何。

主管理服务器根据安装在从属管理服务器上的应用程序更新反病毒数据库。不需要在主管理服务器上安装额外的插件和创建安装包。

自动分配分发点

我们建议您自动分配分发点。Kaspersky Security Center 随后将自行选择必须为哪些设备分配分发点。

要自动分配分发点：

1. 打开主应用程序窗口。

2. 在控制台树中，选择包含要自动为其分配分发点的管理服务器名称的节点。

3. 在管理服务器的上下文菜单中，单击“**属性**”。

4. 在管理服务器属性窗口的“**区域**”窗格，选择“**分发点**”。

5. 在窗口的右侧，选择“**自动分配分发点**”选项。

> 如果自动指派设备做为分发点被启用，您无法手动配置分发点，也不能编辑分发点列表。

6. 单击“**确定**”。

管理服务器便自动指派和配置分发点。

手动为设备指派分发点

Kaspersky Security Center 允许您指定设备做为分发点。

我们建议您自动分配分发点。此种情况下，Kaspersky Security Center 将自行选择哪个设备要被分配为分发点。然后，如果您由于一些原因必须不自动分配分发点（例如，如果您要使用单独分配的服务器），您可以在计算数量和配置后手动分配分发点。

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

要手动指派设备做为分发点：

1. 在控制台树中，选择**管理服务器**节点。

2. 在管理服务器的上下文菜单中，选择“**属性**”。

3. 在管理服务器属性窗口，选择“**分发点**”区域并单击“**添加**”按钮。如果选择了“**手动分配分发点**”，则此按钮可用。
“**添加分发点**”窗口将开启。

4. 在“**添加分发点**”窗口，执行以下操作：

   a. 选择做为分发点的设备（选择管理组，或指定设备 IP 地址）。选择设备时，请牢记分发点的操作功能以及设备作为分发点的需求。

   b. 指定分发点将向其分发更新的特定设备。您可以指定管理组或者网络位置描述。

5. 单击“**确定**”。

   您添加的分发点将显示在“**分发点**”区域的分发点列表中。

6. 在列表中选择新添加的分发点并点击**属性**按钮来打开属性窗口。

7. 在属性窗口中配置分发点：

   - “**常规**”区域中包含用于设定分发点与客户端设备进行交互的设置。

     - **SSL 端口**

       客户端设备与分发点之间，使用 SSL 进行安全连接的 SSL 端口号。

       默认情况下使用端口 13000。

     - **使用多点传送**

       如果启用此选项，将使用 IP 多点传送自动向组内的客户端设备上分发安装包。

       IP 多点传送减少了将应用程序从安装包安装到一组客户端设备所需的时间，但是增加了在将应用程序安装到单个客户端设备时的安装时间。

     - **IP 多点传送地址**

       用于多点传送的 IP 地址。您可以定义范围是 224.0.0.0 – 239.255.255.255 的 IP 地址

       默认情况下，Kaspersky Security Center 自动分配一个在给定范围内的唯一 IP 多播地址。

     - **IP 多点传送端口号**

       IP 多点传送的端口号。

       默认情况下，端口号指定为 15001。如果运行管理服务器的设备指定为分发点，端口 13001 默认用于 SSL 连接。

     - **部署更新**

       更新被从以下来源分发到受管理设备：

       - 此分发点（如果启用此选项）。
       - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

       如果您使用分发点来部署更新，则可以节省流量，因为您减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。你可以计算分发点的数量以便网络优化流量和负载。

       如果禁用此选项，管理服务器上的更新下载和加载次数可能会增加。默认情况下已启用该选项。

- **部署安装包**

  安装包被从以下来源分发到受管理设备：

  - 此分发点（如果启用此选项）。
  - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

  如果使用分发点部署安装包，您可以节省流量，因为减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。你可以计算分发点的数量以便网络优化流量和负载。

  如果禁用此选项，管理服务器上的安装包下载和加载次数可能会增加。默认情况下已启用该选项。

- **将此分发点用作推送服务器**

  在 Kaspersky Security Center 中，分发点可以用作通过移动协议管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

  如果管理安装了 KasperskyOS 的设备或计划这样做，则必须将分发点用作推送服务器。如果要向客户端设备发送推送通知，也可以将分发点用作推送服务器。

- **推送服务器端口**

  客户端设备将用于连接的分发点上的端口。默认情况下使用端口 13295。

- 在“**范围**”区域，指定分发点发布更新的范围（管理组和/或网络定位）。
- 在“**KSN 代理**”区域，您可以配置应用程序使用分发点从受管理设备转发 KSN 请求。

  - **在分发点端启用 KSN 代理**

    KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

    分发点将卡巴斯基安全网络声明中列出的KSN统计数据发送给卡巴斯基。

    默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器**和**我同意使用卡巴斯基安全网络**选项在管理服务器属性窗口中被启用时起作用。

    您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

  - **转发 KSN 请求到管理服务器**

    分发点从受管理设备转发 KSN 请求到管理服务器。

    默认情况下已启用该选项。

  - **通过互联网直接访问 KSN 云/KPSN**

    分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

    安装了网络代理版本 11（或更早版本）的分发点不能直接访问 KPSN。如果要重新配置分发点以将 KSN 请求发送到 KPSN，请为每个分发点启用“**转发 KSN 请求到管理服务器**”选项。

    安装了网络代理版本 12（或更高版本）的分发点可以直接访问 KPSN。

- **当连接到 KPSN 时忽略代理服务器设置**

  如果您在分发点属性或网络代理策略中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，则启用此选项。否则，从受管理应用程序的请求无法到达 KPSN。

  如果您选择“**通过互联网直接访问 KSN 云/KPSN**”选项，则此选项可用。

- **TCP 端口**

  受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

- **UDP 端口**

  如果需要网络代理通过 UDP 端口连接到管理服务器，启用“**使用 UDP 端口**”选项，并指定“**UDP 端口号**”。默认情况下已启用该选项。连接到管理服务器的默认 UDP 端口是 15000。

- **HTTPS 端口**

  如果需要受管理设备通过 HTTPS 端口连接到 KSN 代理服务器，启用“**使用 HTTPS 端口**”选项，并指定 **HTTPS 端口**号。连接到 KSN 代理服务器的默认 HTTPS 端口是 17111。

- 在“**设备发现**”区域，通过分发点配置 Windows 域、活动目录和 IP 范围的轮询。

  - **Windows 域**

    您可以启用 Windows 域设备发现并为发现设置计划。

  - **活动目录**

    您可以启用活动目录域网络轮询并为轮询设置计划。

    如果您使用 Windows 分发点，则可以选择以下选项之一：

    - **轮询当前活动目录域**。
    - **轮询活动目录域森林**。
    - **仅轮询所选活动目录域**。如果您选择该选项，添加一个或更多活动目录域到列表。

    如果您使用安装了网络代理版本 15 的 Linux 分发点，则只能轮询为其指定地址和用户凭据的 Active Directory 域。当前 Active Directory 域和 Active Directory 域林的轮询不可用。

  - **IP 范围**

    您可以针对 IPv4 范围和 IPv6 网络启用设备发现。

    如果启用“**启用范围轮询**”选项，则可以添加扫描范围并为其设置计划。您可以添加 IP 范围到已扫描范围列表。

    如果启用“**使用 Zeroconf 轮询 IPv6 网络**”选项，分发点将使用零配置网络（也称为 *Zeroconf*）自动轮询 IPv6 网络。在这种情况下，指定的 IP 范围将被忽略，因为分发点会轮询整个网络。如果分发点运行 Linux，则**使用 Zeroconf 轮询 IPv6 网络**选项可用。要使用 Zeroconf IPv6 轮询，您必须在分发点上安装 avahi-browse 实用程序。

- 在“**高级**”区域，指定分发点必须使用以存储发布数据的文件夹。
  - **使用默认文件夹**

    如果您选择此选项，应用程序使用分发点上的网络代理安装文件夹。

  - **使用指定文件夹**

    如果您选择该选项，则可以在下面的字段中指定该文件夹的路径。它可以是分发点上的本地文件夹，也可以是企业网络中任何设备上的目录。

    分发点上用于运行网络代理的用户账户必须具有对指定文件夹的访问权限以进行读写操作。

所选设备作为分发点运行。

仅运行 Windows 操作系统的设备可以定义网络位置。网络位置无法定义在运行其他操作系统的设备上。

从分发点列表删除设备

要从分发点列表删除设备：

1. 在控制台树中，选择**管理服务器**节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口的“**分发点**”区域，选择作为分发点的设备，然后单击“**删除**”按钮。

设备将从分发点列表删除并将停止分发点操作。

如果设备被管理服务器自动指定，则它无法从分发点列表删除。

通过分发点下载更新

Kaspersky Security Center 允许分发点从管理服务器、Kaspersky 服务器或本地网络文件夹接收更新。

如果您不需要指定更新源，我们建议您使用管理组的*将更新下载到分发点存储库*任务。有关详细信息，请参阅以下主题：创建将更新下载到分发点存储库任务。

要为分发点配置更新下载：

1. 在控制台树中，选择**管理服务器**节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口的“**分发点**”区域，选择要通过其发送更新到组中客户端设备的分发点。

4. 点击**属性**按钮以打开所选分发点的属性窗口。

5. 在分发点属性窗口中选择“**更新源**”区域。

6. 为分发点选择更新源：

   - 要允许分发点从管理服务器自动接收更新，选择**从管理服务器接收**：

     - **下载 diff 文件**

       该选项启用下载 diff 文件功能。

       默认情况下已启用该选项。

   - 要允许分发点使用任务接收更新，请选择“**使用强制更新下载任务**”：

     - 如果设备上已存在此任务，点击**浏览**按钮，并在出现的列表中选择该任务。
     - 如果设备上不存在此任务，点击**新任务**按钮以创建任务。“新任务向导”启动。遵照向导的说明操作。

     “将更新下载至分发点存储库”任务是个本地任务。您必须为每个做为分发点的设备创建一个新的任务。

分发点将从指定的更新源接收更新。

从存储库删除软件更新

要从管理服务器存储库删除软件更新：

1. 在控制台树的“**高级**”→“**应用程序管理**”文件夹中，选择“**软件更新**”子文件夹。
2. 在“**软件更新**”文件夹的工作区中，选择要删除的更新。
3. 在更新的上下文菜单中，选择**删除更新文件**。

软件更新将被从管理服务器存储库删除。

集群模式下为 Kaspersky 应用程序安装补丁

Kaspersky Security Center 仅支持为集群模式中的 Kaspersky 应用程序手动安装补丁。

要为 Kaspersky 应用程序安装补丁：

1. 现在补丁到集群的每个节点。
2. 在活动节点运行补丁安装。
3. 等待补丁成功安装。

4. 在所有集群的子节点上运行补丁。

   如果您从命令行运行补丁，使用 `-CLUSTER_SECONDARY_NODE` 键。

   补丁被安装到集群的所有节点。

5. 手动运行 Kaspersky 集群服务。

集群的每个节点作为安装了网络代理的设备显示在管理控制台。

关于已安装补丁的信息，请参见“**软件更新**”文件夹或者 Kaspersky 应用程序软件模块更新版本报告。

在客户端设备上管理第三方应用程序

Kaspersky Security Center 允许您管理安装在客户端设备上的 Kaspersky 或其他供应商的程序。

管理员可以进行以下操作：

- 基于指定标准创建应用程序类别。
- 使用特殊创建的规则管理应用程序类别。
- 管理设备上的应用程序运行。
- 执行清单、维护设备上安装软件的注册表。
- 修复安装在设备上软件的漏洞。
- 安装 Windows Update 和其他软件制造商的更新到设备。
- 为已授权应用程序组监控授权许可密钥的使用。

关于第三方应用程序

Kaspersky Security Center 可以帮助您更新客户端设备上安装的第三方软件，并修复第三方软件的漏洞。Kaspersky Security Center 只能将第三方软件从当前版本更新到最新版本。

> 第三方软件列表可以更改，并动态更新。您可以通过在基于 MMC 的管理控制台和 Kaspersky Security Center Web Console 中查看可用更新列表来检查是否可以使用 Kaspersky Security Center 来更新第三方软件（安装在用户设备上）。

以下概述的步骤仅用于查看可通过 Kaspersky Security Center 更新的第三方软件列表。按照以下步骤访问相关信息，无需启动任何任务。

要查看可在 Kaspersky Security Center Web Console 中通过 Kaspersky Security Center 更新的第三方软件列表，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在向导的“**新任务设置**”步骤中，指定以下设置：
   a. 在“**应用程序**”下拉列表中，选择**Kaspersky Security Center**。
   b. 在“**任务类型**”字段中，选择“**安装所需更新并修复漏洞**”。
4. 在向导的“**任务范围**”步骤中，选择“**受管理设备**”选项。
5. 在向导的“**指定更新安装规则**”步骤中，点击“**添加**”按钮。
   规则创建向导开始。使用“**下一步**”按钮继续向导操作。
6. 在向导的“**选择规则类型**”步骤中，选择“**第三方更新的规则**”选项。
7. 在向导的**常规条件**步骤中，选择**安装所有更新 (除了拒绝的)**选项，然后单击**下一步**。

第三方软件列表将显示。

要查看可以在基于 MMC 的控制台中通过Kaspersky Security Center 更新的第三方软件列表，您需要漏洞和补丁管理授权许可。否则，**安装所需更新并修复漏洞**任务不可用。

1. 在控制台树中，选择“**受管理设备**”文件夹。
2. 在工作区中，选择“**任务**”选项卡。
3. 单击“**创建任务**”按钮以运行新任务向导。遵照向导的说明。
4. 在该向导的“**选择任务类型**”页面中，选择“**安装所需更新并修复漏洞**”。
5. 在向导的“**指定更新安装规则**”步骤中，点击“**添加**”按钮。
   规则创建向导开始。使用“**下一步**”按钮继续向导操作。
6. 在向导的“**选择规则类型**”步骤中，选择“**第三方更新的规则**”选项。
7. 在向导的**常规条件**步骤中，选择**安装所有更新 (除了拒绝的)**选项，然后单击**下一步**。

   第三方软件列表将显示。

安装第三方软件更新

Kaspersky Security Center 允许您管理安装在客户端设备上的软件更新，并安装所需更新修复 Microsoft 应用程序和其他软件厂商产品的漏洞。

Kaspersky Security Center 通过更新搜索任务搜索更新并下载至更新存储库。完成更新搜索后，程序提供给管理员应用程序可用更新和可以使用该更新修复的漏洞的信息。

Microsoft Windows 的可用更新通过 Windows Update 服务提供。管理服务器可以被用作 Windows Server Update Services（WSUS）服务器。要使用管理服务器作为 WSUS 服务器，您应该配置和 Windows Update 的更新同步。在您配置了和 Windows Update 的数据同步后，管理服务器以集中模式和设置的频率在设备上提供更新到 Windows Update 服务。

您也可以通过网络代理策略管理软件更新。为此，您应该创建一个网络代理策略并在对应的“新策略向导”窗口中配置软件更新。

管理员可以在“**应用程序管理**”文件夹下的“**软件更新**”子文件夹中查看可用更新列表。该文件夹包含了管理服务器检索的可以被分发到设备的 Microsoft 应用程序和其他软件厂商产品的更新列表。查看可用更新信息后，您可以将它们安装到设备。

Kaspersky Security Center 通过删除先前的应用程序并安装新应用程序来更新应用程序。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

确保在主要和从属管理服务器的**配置界面**窗口中启用**显示漏洞和补丁管理**选项。否则，更新搜索任务仅处理 WSUS 更新。

出于安全原因，卡巴斯基技术会自动扫描您使用漏洞和补丁管理功能安装的任何第三方软件更新，以查找恶意软件。这些技术用于自动文件检查，包括病毒扫描、静态分析、动态分析、沙盒环境中的行为分析和机器学习。

卡巴斯基专家不会对可以使用漏洞和补丁管理功能安装的第三方软件更新进行手动分析。此外，卡巴斯基专家不会在此类更新中搜索漏洞（已知或未知）或未记录的功能，也不会对上面段落中指定的更新以外的更新进行其他类型的分析。

在安装更新到所有设备前，您可以运行安装测试来确保安装的更新不会引起设备上应用程序操作的失败。

方案：更新第三方软件

本节提供了更新客户端设备上安装的第三方软件的方案。第三方软件包括 Microsoft 和其他软件供应商的应用程序。Microsoft 应用程序的更新由 Windows Update 服务提供。

先决条件

管理服务器必须连接到互联网才能安装除 Microsoft 软件之外的第三方软件的更新。

默认情况下，管理服务器不需要互联网连接就可以在受管理设备上安装 Microsoft 软件更新。例如，受管理设备可以直接从 Microsoft 更新服务器下载 Microsoft 软件更新，也可以从组织的网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下载。将管理服务器用作 WSUS 服务器时，管理服务器必须连接到互联网。

阶段

更新第三方软件分阶段进行：

1. **搜索所需更新**

要查找受管理设备所需的第三方软件更新，请运行“*查找漏洞和所需更新*”任务。完成此任务后，Kaspersky Security Center 会收到检测到的漏洞列表，以及在任务属性中指定的设备上安装的第三方软件的所需更新。

“*查找漏洞和所需更新*”任务由管理服务器快速启动向导自动创建。如果未运行向导，请立即创建任务或运行快速启动向导。

说明：

- 管理控制台：扫描应用程序中的漏洞，安排“查找漏洞和所需更新”任务
- Kaspersky Security Center Web Console：创建“查找漏洞和所需更新”任务，“查找漏洞和所需更新”任务设置

2 分析找到的更新列表

查看“**软件更新**”列表并决定要安装哪些更新。要查看有关每个更新的详细信息，请单击列表中的更新名称。对于列表中的每个更新，您还可以查看客户端设备上更新安装的统计信息。

说明：

- 管理控制台：查看有关可用更新的信息
- Kaspersky Security Center Web Console：查看有关可用的第三方软件更新的信息

3 配置更新安装

当 Kaspersky Security Center 收到第三方软件更新列表后，您可以使用“*安装所需更新并修复漏洞*”任务或“*安装 Windows Update 更新*”任务将它们安装在客户端设备上。创建这些任务之一。您可以在“**任务**”选项卡上或使用“**软件更新**”列表创建这些任务。

“*安装所需更新并修复漏洞*”任务用于安装 Microsoft 应用程序的更新，包括 Windows Update 服务提供的更新以及其他供应商软件的更新。请注意，仅当您具有漏洞和补丁管理功能的授权许可时，才能创建此任务。

“*安装 Windows Update 更新*”任务不需要授权许可，但只能用于安装 Windows Update 更新。

要安装某些软件更新，您必须接受最终用户授权许可协议 (EULA) 才能安装软件。如果您拒绝 EULA，则不会安装该软件更新。

您可以按计划启动更新安装任务。指定任务计划时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

说明：

- 管理控制台：修复应用程序中的漏洞，查看有关可用更新的信息
- Kaspersky Security Center Web Console：创建“安装所需更新并修复漏洞”任务，创建“安装 Windows Update 更新”任务，查看有关可用的第三方软件更新的信息

4 安排任务

为确保更新列表始终是最新的，请计划“*查找漏洞和所需更新*”任务以不时自动运行该任务。默认情况下，“*查找漏洞和所需更新*”任务设置为手动启动。

如果已创建“*安装所需更新并修复漏洞*”任务，则可以将其运行频率计划成与“*查找漏洞和所需更新*”任务相同或更少。在计划“*安装 Windows Update 更新*”任务时，请注意，对于此任务，您在每次启动此任务之前都必须定义更新列表。

计划任务时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

5 批准和拒绝软件更新（可选）

如果已创建“安装所需更新并修复漏洞”任务，则可以在任务属性中指定更新安装的规则。如果已创建“安装 Windows Update 更新”任务，请跳过此步骤。

对于每条规则，都可以根据更新状态定义要安装的更新："*未定义*"、"*已批准*"或"*已拒绝*"。例如，您可能想为服务器创建一个特定任务，并为该任务设置一条规则，以仅允许安装 Windows Update 更新以及状态为"*已批准*"的更新。之后，手动为要安装的更新设置"*已批准*"状态。在这种情况下，状态为"*未定义*"或"*已拒绝*"的 Windows Update 更新将不会安装到任务中指定的服务器上。

使用"*已批准*"状态管理更新安装对于少量更新来说非常有效。要安装多个更新，请使用可以在"*安装所需更新并修复漏洞*"任务中配置的规则。我们建议仅为那些不符合规则中指定的条件的特定更新设置"*已批准*"状态。当手动批准大量更新时，管理服务器的性能会下降，这可能导致服务器过载。

默认下，下载的软件更新具有*未定义*状态。您可以在"**软件更新**"列表（"**操作**"→"**补丁管理**"→"**软件更新**"）中将状态更改为"*已批准*"或"*已拒绝*"。

说明：

- 管理控制台：批准和拒绝软件更新
- Kaspersky Security Center Web Console：批准和拒绝第三方软件更新

6. **将管理服务器配置为用作 Windows Server Update Services (WSUS) 服务器（可选）**

   默认情况下，Windows Update 更新从 Microsoft 服务器下载到受管理设备。您可以更改此设置以将管理服务器用作 WSUS 服务器。在这种情况下，管理服务器以指定频率将更新数据与 Windows Update 同步，并以集中模式向联网设备上的 Windows Update 提供更新。

   要将管理服务器用作 WSUS 服务器，请创建"执行 Windows Update 同步"任务，然后选中网络代理策略中的"**将管理服务器用作 WSUS 服务器**"复选框。

   说明：

   - 管理控制台：将 Windows Update 中的更新与管理服务器同步，在网络代理策略中配置 Windows 更新
   - Kaspersky Security Center Web Console：创建"执行 Windows Update 同步"任务

7. **运行更新安装任务**

   启动"*安装所需更新并修复漏洞*"任务或"*安装 Windows Update 更新*"任务。启动这些任务后，更新将下载并安装到受管理设备上。任务完成后，请确保它在任务列表中具有"*已成功完成*"状态。

8. **创建有关第三方软件更新安装结果的报告（可选）**

   要查看有关更新安装的详细统计信息，请创建**第三方软件更新安装结果报告**。

   说明：

   - 管理控制台：创建和查看报告
   - Kaspersky Security Center Web Console：生成和查看报告

结果

如果已创建并配置了"*安装所需更新并修复漏洞*"任务，则更新将自动安装到受管理设备上。新更新下载到管理服务器存储库后，Kaspersky Security Center 会检查更新是否满足更新规则中指定的条件。符合条件的所有新更新都将在任务下次运行时自动安装。

如果已创建"*安装 Windows Update 更新*"任务，则仅安装在*安装 Windows Update 更新*任务属性中指定的更新。将来，如果您要安装已下载到管理服务器存储库的新更新，必须将所需更新添加到现有任务中的更新列表，或创建新的"*安装 Windows Update 更新*"任务。

查看有关第三方应用程序可用更新的信息

要查看客户端设备上安装的第三方应用程序的可用更新列表，

在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**软件更新**”子文件夹。

在该文件夹的工作区中，您可以查看设备上所安装应用程序可用的更新。

要查看更新的属性，

在“**软件更新**”文件夹的工作区，从更新的上下文菜单中选择“**属性**”。

在更新的属性窗口中可以查看以下信息：

- 在**常规**区域，您可以查看**更新批准状态**：
  - **未定义**—更新在更新列表中可用，但未获准安装。
  - **已批准**—更新在更新列表中可用并获准安装。
  - **已拒绝**—拒绝安装更新。
- 在**属性**区域，您可以查看**已自动安装**字段的值：
  - 如果“*安装所需更新并修复漏洞*”任务可以安装应用程序更新，将显示“**自动地**”值。该任务会自动从第三方软件供应商提供的网址安装新的更新。
  - 如果 Kaspersky Security Center 无法自动安装应用程序更新，则会显示“**手动**”值。您可以手动安装更新。

  对于 Windows 应用程序更新，不显示“**已自动安装**”字段。
- 需要更新的客户端设备的列表。
- 需要在更新前安装的系统组件列表（先决条件）（如果有的话）
- 更新将修复的软件漏洞。

批准和拒绝软件更新

更新安装任务的设置可能需要对要安装的更新进行批准。您可以批准必须安装的更新并拒绝不能安装的更新。

例如，您可能想先在测试环境中检查更新安装以确保它们不干预设备操作，仅在这之后允许安装这些更新到客户端设备。

使用“*已批准*”状态管理第三方更新安装对于少量更新来说非常有效。要安装多个第三方更新，请使用可以在“*安装所需更新并修复漏洞*”任务中配置的规则。我们建议仅为那些不符合规则中指定的条件的特定更新设置“*已批准*”状态。当手动批准大量更新时，管理服务器的性能会下降，这可能导致服务器过载。

要批准或拒绝一个或几个更新：

1. 在控制台树中，选择**高级 → 应用程序管理 → 软件更新**节点。
2. 在“**软件更新**”文件夹的工作区，单击右上角的“**刷新**”按钮。更新列表显示。
3. 选择您要批准或拒绝的更新。
   所选对象的信息框出现在工作区的右侧。
4. 在“**更新批准状态**”下拉列表，选择“**已批准**”以批准所选更新或选择“**已拒绝**”以拒绝所选更新。
   默认值是“**未定义**”。

您设置了“**已批准**”状态的更新放置在安装队列。

您设置了“**已拒绝**”状态的更新将从先前安装了更新的所有设备中卸载（如果可能）。而且，它们将来也不会被安装到其他设备。

Kaspersky 应用程序的一些更新无法被卸载。如果为这些更新设置了“**已拒绝**”状态，则 Kaspersky Security Center 将不会从以前安装这些更新的设备上将其卸载。然而，这些更新将来也不会被安装到其他设备。如果无法卸载 Kaspersky 应用程序更新，则该属性将显示在更新属性窗口中：在“**区域**”窗格选择“**常规**”，该属性将显示在工作区的“**安装需求**”下。如果您为第三方软件更新设置了**已拒绝**状态，这些更新将不会安装在计划将其安装但并未将其安装的设备上。更新将保持在已将其安装的设备上。如果您必须删除它们，您可以在本地手动删除它们。

使用管理服务器从 Windows 更新同步更新

如果您已经在快速启动向导的“**更新管理设置**”窗口中选择了“**使用管理服务器作为 WSUS 服务器**”，程序将自动创建 Windows Update 同步任务。您可以运行“**任务**”文件夹中的任务。Microsoft 软件更新功能仅在“**执行 Windows 更新同步**”任务成功完成后才可用。

Microsoft 软件更新可能超过 10 GB。确保管理服务器数据库能够容纳此类容量；否则，**执行 Windows 更新同步**任务将失败。**执行 Windows 更新同步**任务不支持 Microsoft SQL Express 数据库。

“**执行 Windows 更新同步**”任务仅从 Microsoft 服务器下载元数据。如果网络不使用 WSUS 服务器，例如每个客户端设备都从外部服务器独立下载 Microsoft 更新。

若要创建使用管理服务器同步 Windows 更新，请执行以下操作：

1. 在控制台树的“**高级**”→“**应用程序管理**”文件夹中，选择“**软件更新**”子文件夹。
2. 单击“**附加操作**”按钮并在下拉列表中选择“**配置 Windows 更新同步**”。
   向导将创建“**任务**”文件夹中显示的“**执行 Windows 更新同步**”任务。
   Windows Update Center 数据检索任务创建向导启动。遵照向导的说明操作。

您还可以通过单击“**创建任务**”在“**任务**”文件夹中创建 Windows Update 同步任务。

Microsoft 定期从该公司的服务器删除过期更新，因此当前更新数量总是介于 200,000 和 300,000 之间。为了减少磁盘空间使用和数据库大小，Kaspersky Security Center 删除 Microsoft 更新服务器上不再存在的过时更新。

当运行“**执行 Windows 更新同步**”任务时，应用程序从 Microsoft 更新服务器接收当前更新列表。下一步，Kaspersky Security Center 编辑过期更新列表。在下次启动“**查找漏洞和所需更新**”任务时，Kaspersky Security Center 会标记所有过时的更新，并为其设置删除时间。在下次启动“**执行 Windows 更新同步**”任务时，将删除标记为 30 天之前删除的所有更新。Kaspersky Security Center 也检查删除了 180 天以上的过期更新，并删除更早的更新。

当“**执行 Windows 更新同步**”任务完成且过时更新被删除时，数据库可能仍保留被删除的更新的哈希码和对应文件到 %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 文件（如果之前已下载）。您可以运行“**管理服务器维护**”任务以从数据库和对应文件中删除这些过期的记录。

步骤 1：定义是否减少流量

在 Kaspersky Security Center 与 Microsoft Windows Update Servers 同步更新时，所有文件的信息被保存在管理服务器数据库。所有更新所需的文件也在与 Windows 更新代理的交互过程中被下载到驱动器。特别地，Kaspersky Security Center 保存快速更新文件的信息到数据库并在必要时下载它们。下载快速更新文件导致驱动器空间的减少。

为了避免磁盘空间减少以及流量降低，可以禁用“**下载快速安装文件**”选项。

如果选择此选项，运行任务时将下载快速更新文件。默认情况下未选定该选项。

步骤 2：应用程序

在该区域中，您可以选择为哪些应用程序下载更新。

如果选中“**所有应用程序**”复选框，更新将为所有现有应用程序以及可能在将来发布的应用程序下载。

默认情况下选中“**所有应用程序**”复选框。

步骤 3：更新类别

在该区域中，您可以选择将哪些类别的更新下载到管理服务器。

如果选中“**所有类别**”复选框，更新将为所有现有更新类别以及可能在将来出现的类别下载。

默认情况下选中“**所有类别**”复选框。

步骤 4：更新语言

在该窗口中，您可以定义将哪些语言的更新下载到管理服务器。选择以下选项之一以下载更新的本地化语言：

- **下载包括新语言在内的所有语言**

  如果选定了该选框，所有可用的更新本地化语言都将被下载至管理服务器。默认情况下已选定该选项。

- **下载选定语言**

  如果选定了该选框，您可以从更新的本地化语言列表中进行选择以便下载到管理服务器中。

步骤 5：选择账户以移动任务

在“**选择账户以运行任务**”窗口，您可以指定在运行任务时使用哪些账户。您可以选择以下选项之一：

- **默认账户**

  在与执行该任务的应用程序相同的账户下运行该任务。

  默认情况下已选定该选项。

- **指定账户**

  填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - **账户**

    运行该任务的账户。

  - **密码**

    任务运行时使用的账户的密码。

步骤 6：配置任务启动计划

在“**配置任务计划**”向导页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

- **每 N 星期**

  任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。
  默认下，任务每星期一于当前系统时间运行一次。

- **每 N 分钟**

  任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。
  默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每天(不支持夏令时)**

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。
  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。
  默认下，任务每天于当前系统时间运行一次。

- **每周**

  任务每周在指定星期和指定时间运行。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。
  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。
  在缺少指定日的月份，任务在最后一天运行。
  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **一次**

  该任务在指定的日期和时间运行一次（默认情况下，在创建任务的当天）。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

默认情况下，开始时间为18:00，且未选择任何日期。

请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是"**手动**"、"**一次**"或"**立即**"，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于"**手动**"、"**一次**"和"**立即**"计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

步骤 7：定义任务名称

在“**定义任务名称**”窗口，指定您正在创建的任务名称。任务名称不能超过 100 个字符，且不能包含任何特殊字符（`"*<>?\:|`）。默认值是*执行 Windows 更新同步*。

步骤 8：完成任务创建

在“**完成任务创建**”窗口，点击“**完成**”按钮完成向导。

如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

新创建的 Windows 更新同步任务将显示在控制台树中“**任务**”文件夹的任务列表。

手动在设备上安装更新

如果您已经在快速启动向导的“**更新管理设置**”页面中选定了“**查找并安装所需更新**”，“*安装所需更新并修复漏洞*”任务将自动创建。您可以在“**任务**”选项卡上的“**受管理设备**”文件夹中运行或停止该任务。

如果您已经在快速启动向导中选定了“**搜索所需更新**”，您可以通过“*安装所需更新并修复漏洞*”任务将软件更新安装至客户端设备。

您可以做以下任意：

- 创建更新安装任务。
- 添加安装更新到现有更新安装任务的规则。
- 在现有更新安装任务的设置中，配置更新的测试安装。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

通过创建安装任务安装更新

您可以做以下任意：

- 创建特定更新安装任务。
- 选择更新并创建它和相似更新的安装任务。

要安装特定更新：

1. 在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**软件更新**”子文件夹。
2. 在工作区，选择您要安装的更新。
3. 做以下任意：
   - 右击列表中的一个所选更新，然后选择**安装更新 → 新任务**。
   - 在所选更新的信息框中，单击“**安装更新(创建任务)**”链接。
4. 在显示的提示中做出安装所有先前应用程序更新的选择。如果您同意在安装所选更新需要时安装连续的应用程序版本，点击**是**。如果您要直接更新应用程序而不安装连续版本，点击**否**。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

   更新安装和漏洞修复任务创建向导启动。遵照向导的说明。
5. 在向导的“**选择操作系统重启选项**”页面，选择客户端设备的操作系统在操作后必须被重启时的操作：
   - **不重启设备**

     客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。
   - **重启设备**

     如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于1和1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于1和1440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

6. 在向导的"**配置任务计划**"页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

- **每 N 星期**

  任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。
  默认下，任务每星期一于当前系统时间运行一次。

- **每 N 分钟**

  任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。
  默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每天(不支持夏令时)**

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。
  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。
  默认下，任务每天于当前系统时间运行一次。

- **每周**

  任务每周在指定星期和指定时间运行。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。
  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。
  在缺少指定日的月份，任务在最后一天运行。
  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

默认情况下，开始时间为18:00，且未选择任何日期。

请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是"**手动**"、"**一次**"或"**立即**"，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于"**手动**"、"**一次**"和"**立即**"计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

7. 在向导的"**定义任务名称**"页面，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

8. 在向导的"**完成任务创建**"页面，单击"**完成**"按钮关闭向导。

   如果您想让任务在向导完成时立即启动，选择"**向导完成时运行任务**"复选框。

向导完成操作后，**任务**文件夹中将显示**安装所需更新并修复漏洞**。

您可以在"*安装所需更新并修复漏洞*"任务属性中启用在安装更新前先自动安装系统组件（先决条件）。当启用了此选项，会在更新前安装所有所需的系统组件。在更新属性中有所需组件列表。

在"*安装所需更新并修复漏洞*"任务属性中，您可以允许安装能够将程序更新至新版本的更新。

如果任务设置提供了安装第三方更新的规则，管理服务器从供应商网站下载所有相关更新。更新保存到管理服务器存储库，然后分发并安装在可应用的设备。

如果任务设置提供了安装 Microsoft 更新的规则并且管理服务器作为 WSUS 服务器，管理服务器下载所有更新到存储库并分发它们到受管理设备。如果网络不使用 WSUS 服务器，例如每个客户端设备都从外部服务器独立下载 Microsoft 更新。

要安装特定和相似更新：

1. 在控制台树的"**高级**" → "**应用程序管理**"文件夹中，选择"**软件更新**"子文件夹。

2. 在工作区，选择您要安装的更新。

3. 单击**运行更新安装向导**按钮。

   更新安装向导开始。

   更新安装向导功能仅在漏洞和补丁管理授权许可下可用。

   遵照向导的说明。

4. 在“**搜索现有的更新安装任务**”页面，指定以下设置：

   - **搜索安装该更新的任务**

     如果启用该选项，更新安装向导搜索安装所选更新的现有任务。

     如果禁用该选项或搜索未检索到可应用任务，更新安装向导提示您为安装更新创建规则或任务。

     默认情况下已启用该选项。

   - **批准更新安装**

     所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

     默认情况下已禁用该选项。

5. 如果您选择搜索现有更新安装任务或搜索检索到一些任务，您可以查看这些任务的属性或手动启动它们。不需要进一步操作。

   否则，点击**新更新安装任务**按钮。

6. 选择安装规则类型以添加到新任务，然后点击**结束**按钮。

7. 在显示的提示中做出安装所有先前应用程序更新的选择。如果您同意在安装所选更新需要时安装连续的应用程序版本，点击**是**。如果您要直接更新应用程序而不安装连续版本，点击**否**。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

   更新安装和漏洞修复任务创建向导启动。遵照向导的说明。

8. 在向导的“**选择操作系统重启选项**”页面，选择客户端设备的操作系统在操作后必须被重启时的操作：

   - **不重启设备**

     客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

   - **重启设备**

     如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

   - **提示用户操作**

     客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

     默认情况下已选定该选项。

     - **重复提示间隔(分钟)**

       如果启用该选项，应用程序以指定频率提示用户重启操作系统。

默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

9. 在向导的“**选择要对其分配任务的设备**”页面，选择以下选项之一：

- **选择管理服务器检测到的网络设备**

  任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。

  例如，您可能要在安装网络代理到未分配的设备的任务中使用该选项。

- **手动指定设备地址或从列表导入地址**

  您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- **分配任务到设备分类**

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。

  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

- **分配任务到管理组**

  任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

  例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

  如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

10. 在向导的“**配置任务计划**”页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期一于当前系统时间运行一次。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - **每天(不支持夏令时)**

    任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

    我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。

    默认下，任务每天于当前系统时间运行一次。

  - **每周**

    任务每周在指定星期和指定时间运行。

  - **按星期中的天数**

    任务在每周指定日期的指定时间定期运行。

    默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**（默认选择）

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

- 在搜索栏中输入任务名称，即可根据名称搜索任务。
- 单击排序图标可按名称对任务进行排序。
  默认情况下，任务按字母顺序升序排列。
- 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

11. 在向导的“**定义任务名称**”页面，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

12. 在向导的“**完成任务创建**”页面，单击“**完成**”按钮关闭向导。
    如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

当向导结束后，系统将创建**安装所需更新并修复漏洞**任务，并显示在“**任务**”文件夹中。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

将程序更新至新版本可能会导致设备上的独立程序的功能故障。

通过添加规则到现有安装任务来安装更新

要通过添加规则到现有安装任务来安装更新：

1. 在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**软件更新**”子文件夹。
2. 在工作区，选择您要安装的更新。
3. 单击**运行更新安装向导**按钮。
   更新安装向导开始。

   > 更新安装向导功能仅在漏洞和补丁管理授权许可下可用。

   遵照向导的说明。
4. 在“**搜索现有的更新安装任务**”页面，指定以下设置：
   - **搜索安装该更新的任务**

     如果启用该选项，更新安装向导搜索安装所选更新的现有任务。

     如果禁用该选项或搜索未检索到可应用任务，更新安装向导提示您为安装更新创建规则或任务。

     默认情况下已启用该选项。
   - **批准更新安装**

     所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

     默认情况下已禁用该选项。
5. 如果您选择搜索现有更新安装任务或搜索检索到一些任务，您可以查看这些任务的属性或手动启动它们。不需要进一步操作。
   否则，点击“**添加更新安装规则**”按钮。
6. 选择您要添加规则的任务，然后单击“**添加规则**”按钮。
   而且，你您可以查看现有任务的属性，手动启动它们，或者创建新任务。
7. 选择规则类型以添加到所选任务，然后点击**结束**按钮。
8. 在显示的提示中做出安装所有先前应用程序更新的选择。如果您同意在安装所选更新需要时安装连续的应用程序版本，点击**是**。如果您要直接更新应用程序而不安装连续版本，点击**否**。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

更新安装新规则被添加到现有**安装所需更新并修复漏洞**任务。

配置更新的测试安装

若要配置更新的测试安装，请执行以下操作：

1. 在控制台树中，在“**任务**”选项卡上“**受管理设备**”文件夹中选择“**安装所需更新并修复漏洞**”任务。
2. 从任务的上下文菜单中，选择“**属性**”。

   “**安装所需更新并修复漏洞**”任务的属性窗口将开启。
3. 在该任务的属性窗口中，在“**测试安装**”区域中，选择可用的测试安装选项之一：

   - **不扫描**。如果您不希望执行更新的测试安装，请选择该选项。
   - **在选定设备上运行扫描**。如果要在选定设备上测试更新安装，请选择该选项。单击“**添加**”按钮，然后选择您需要在其上执行更新测试安装的设备。
   - **在指定组中的设备上运行扫描**。如果要在一组设备上测试更新安装，请选择该选项。在“**指定测试组**”字段中，指定您要在其上执行测试安装的设备组。
   - **在指定百分比的设备上运行扫描**。如果要在一部分设备上测试更新安装，请选择该选项。在“**所有目标设备中测试设备的百分比**”字段中，指定您要在其上执行更新测试安装的设备的百分比。
4. 选择除了“**不扫描**”的任意选项，在“**决定是否继续进行安装所需的时间(小时)**”字段中指定从更新安装测试到开始将更新安装到所有目标设备上必须间隔的小时数。

在网络代理策略中配置 Windows 更新

若要在网络代理策略中配置 Windows 更新，请执行以下操作：

1. 在控制台树中，选择**受管理设备**。
2. 在工作区中，选择“**策略**”选项卡。
3. 选择网络代理策略。
4. 在策略的上下文菜单中，选择“**属性**”。

   打开网络代理策略的属性窗口。
5. 在“**区域**”窗格，选择“**软件更新和漏洞**”。
6. 选中“**使用管理服务器作为 WSUS 服务器**”选项，将 Windows 更新下载到管理服务器，然后通过网络代理将其分发到客户端设备。

   如果未选择此选项，Windows 更新将不会被下载到管理服务器。此种情况下，客户端设备直接从 Microsoft 服务器接收 Windows 更新。
7. 选择用户可以通过使用 Windows Update 手动安装到设备的更新集。

> 在运行 Windows 10 的设备上，如果 Windows Update 已经为设备找到更新，您在“**允许用户管理 Windows Update 更新安装**”下选择的新选项将仅在发现的更新被安装后才被应用。

在下拉列表中选择条目：

- **允许用户安装所有可应用 Windows Update 更新**

  用户可以安装所有可应用到他们设备的 Microsoft Windows Update 更新。

  如果您不希望干预更新安装，请选择该选项。

  当用户手动安装 Microsoft Windows Update 更新时，更新可能从 Microsoft 服务器下载，而不是从管理服务器。如果管理服务器还未下载这些更新，这是可能的。从 Microsoft 服务器下载更新导致额外流量。

- **仅允许用户安装批准的 Windows Update 更新**

  用户可以安装所有可应用到他们设备的和您批准的 Microsoft Windows Update 更新。

  例如，您可能想先在测试环境中检查更新安装以确保它们不干预设备操作，仅在这之后允许安装这些批准的更新到客户端设备。

  当用户手动安装 Microsoft Windows Update 更新时，更新可能从 Microsoft 服务器下载，而不是从管理服务器。如果管理服务器还未下载这些更新，这是可能的。从 Microsoft 服务器下载更新导致额外流量。

- **不允许用户安装 Windows Update 更新**

  用户无法在他们的设备上手动安装 Microsoft Windows Update 更新。所有可应用更新根据您的配置而安装。

  如果您想要集中管理更新的安装则选则此选项。

  例如，您可以想优化更新计划以便网络不过载。您可以计划稍后更新，以便它们不干预用户工作。

8. 选择 Windows 更新搜索模式：

- **主动**

  如果选中该选项，管理服务器支持使用网络代理在客户端设备上从 Windows 更新代理发送请求至更新源：Windows 更新服务器（或简称为 WSUS）。然后，网络代理会将从 Windows 更新代理接收到的信息传送给管理服务器。

  仅在选择*查找漏洞和所需更新*任务的“**连接更新服务器更新数据**”选项时，该选项才生效。

  默认情况下已选定该选项。

- **被动**

  如果您选定该选项，网络代理将从上次同步更新源之后定期从 Windows 更新代理将所检索更新的信息传递给管理服务器。如果 Windows 更新代理没有执行与更新源同步，管理服务器上有关更新的信息将变为过期。

  如果要从更新源的内存缓存中获取更新，请选择此选项。

- **已禁用**

  如果选中该选项，管理服务器不会请求任何有关更新的信息。
  例如，如果您想首先在本地设备上测试更新，请选择此选项。

9. 如果您要扫描运行中的可执行文件以查找漏洞，请选中“**当运行可执行文件时扫描其漏洞**”选项。
10. 确保为您更改的所有设置锁定编辑。否则，更改不适用。
11. 单击“**应用**”。

修复第三方软件漏洞

本部分描述了 Kaspersky Security Center 的功能，这些功能与修复受管理设备上所安装软件中的漏洞有关。

方案：查找和修复第三方软件中的漏洞

该部分提供了在运行 Windows 的受管理设备上查找和修复漏洞的方案。您可以在操作系统和第三方软件（包括 Microsoft 软件）中查找和修复软件漏洞。

先决条件

- Kaspersky Security Center 已部署在您的组织中。
- 您的组织中存在运行 Windows 系统的受管理设备。
- 管理服务器需要互联网连接才能执行以下任务：
  - 针对 Microsoft 软件漏洞生成推荐的修复程序列表。该列表由 Kaspersky 专家创建并定期更新。
  - 修复除 Microsoft 软件以外的第三方软件的漏洞。

阶段

查找和修复软件漏洞的过程分为以下几个阶段：

1. **扫描受管理设备上安装的软件中的漏洞**

   要查找受管理设备上安装的软件中的漏洞，请运行“*查找漏洞和所需更新*”任务。完成此任务后，Kaspersky Security Center 会收到检测到的漏洞列表，以及在任务属性中指定的设备上安装的第三方软件的所需更新。

   “*查找漏洞和所需更新*”任务由 Kaspersky Security Center 快速启动向导自动创建。如果您未运行向导，请立即启动它或手动创建任务。

   说明：

   - 管理控制台：扫描应用程序中的漏洞，安排“查找漏洞和所需更新”任务
   - Kaspersky Security Center Web Console：创建“查找漏洞和所需更新”任务，“查找漏洞和所需更新”任务设置

2 分析检测到的软件漏洞列表

查看“**软件漏洞**”列表，并确定要修复的漏洞。要查看有关每个漏洞的详细信息，请单击列表中的漏洞名称。对于列表中的每个漏洞，您还可以查看受管理设备上关于该漏洞的统计信息。

说明：

- 管理控制台：查看有关软件漏洞的信息，查看受管理设备上漏洞的统计信息
- Kaspersky Security Center Web Console：查看软件漏洞信息，查看受管理设备上漏洞的统计信息

3 配置漏洞修复

检测到软件漏洞后，可以使用“*安装所需更新并修复漏洞*”任务或“*修复漏洞*”任务来修复受管理设备上的软件漏洞。

*安装所需更新并修复漏洞*任务用于更新和修复在受管理设备上安装的第三方软件（包括 Microsoft 软件）中的漏洞。通过此任务，您可以根据某些规则安装多个更新并修复多个漏洞。请注意，仅当您具有漏洞和补丁管理功能的授权许可时，才能创建此任务。为修复软件漏洞，*安装所需更新并修复漏洞*任务将使用建议的软件更新。

*修复漏洞*任务不需要“漏洞和补丁管理”功能的授权许可选项。要使用此任务，必须手动为任务设置中列出的第三方软件中的漏洞指定用户修补程序。“*修复漏洞*”任务使用针对 Microsoft 软件的建议修补程序和针对第三方软件的用户修补程序。

您可以启动漏洞修复向导来自动创建这些任务之一，也可以手动创建这些任务之一。

说明：

- 管理控制台：为第三方软件中的漏洞选择用户修补程序，修复应用程序中的漏洞
- Kaspersky Security Center Web Console：为第三方软件中的漏洞选择用户修补程序，修复第三方软件中的漏洞，创建“安装所需更新并修复漏洞”任务

4 安排任务

为确保漏洞列表始终是最新的，请安排“*查找漏洞和所需更新*”任务以不时自动运行它。建议的平均运行频率是每周一次。

如果您创建了“*安装所需更新并修复漏洞*”任务，则可以安排其与“*查找漏洞和所需更新*”任务相同或更少的频率运行。计划“*修复漏洞*”任务时，请注意，每次启动任务之前，都必须选择 Microsoft 软件的修补程序或为第三方软件指定用户修补程序。

安排任务时，请确保在完成“*查找漏洞和所需更新*”任务之后，开始修复漏洞的任务。

5 忽略软件漏洞（可选）

如果需要，可以忽略在所有受管理设备上或仅在选定受管理设备上要修复的软件漏洞。

说明：

- 管理控制台：忽略软件漏洞
- Kaspersky Security Center Web Console：忽略软件漏洞

6 运行漏洞修复任务

启动*安装所需更新并修复漏洞*任务或*修复漏洞*任务。任务完成后，请确保它在任务列表中具有*已成功完成*状态。

7 创建有关修复软件漏洞的结果报告（可选）

要查看有关已修复漏洞的详细统计信息，请生成漏洞报告。该报告显示有关未修复软件漏洞的信息。因此，您可以了解如何对组织中第三方软件（包括 Microsoft 软件）的漏洞进行查找和修复。

说明：

- 管理控制台：创建和查看报告
- Kaspersky Security Center Web Console：生成和查看报告

8. **检查关于查找和修复第三方软件中漏洞的配置**

   确保已完成以下操作：

   - 获取并查看了受管理设备上的软件漏洞列表
   - 如果需要，可以忽略软件漏洞
   - 配置任务以修复漏洞
   - 安排任务以查找和修复软件漏洞，以便任务依次启动
   - 检查是否已运行修复软件漏洞任务

结果

如果已创建并配置了“*安装所需更新并修复漏洞*”任务，则这些漏洞将自动在受管理设备上修复。运行任务时，它将可用软件更新列表与任务设置中指定的规则相关联。满足规则条件的所有软件更新都将下载到管理服务器存储库中，并将进行安装以修复软件漏洞。

如果创建了“*修复漏洞*”任务，则仅修复 Microsoft 软件中的软件漏洞。

关于查找和修复软件漏洞

Kaspersky Security Center 可检测并修复运行 Microsoft Windows 系列操作系统的受管理设备上的软件漏洞。将在操作系统和第三方软件（包括 Microsoft 软件）中检测漏洞。

> 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）以及 KSN 功能。

查找软件漏洞

为了查找软件漏洞，Kaspersky Security Center 使用已知漏洞数据库的特征。该数据库由 Kaspersky 专家创建。它包含有关漏洞的信息，例如漏洞描述、漏洞检测日期、漏洞严重级别。您可以在卡巴斯基网站查找软件漏洞详情。

Kaspersky Security Center 使用*查找漏洞和所需更新*任务来查找软件漏洞。

在某些情况下，可以使用以下任一方法修复 Microsoft Windows 操作系统中检测到的漏洞：

- 安装操作系统更新。
- 将操作系统升级到较新的版本（例如，从 Windows 10 到 Windows 11）。

在这种情况下，Kaspersky Security Center 会针对同一漏洞显示两个条目。

修复软件漏洞

为修复软件漏洞，Kaspersky Security Center 使用软件供应商发布的软件更新。由于执行以下任务，软件更新元数据会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*。该任务旨在下载 Kaspersky 和第三方软件的更新元数据。该任务由 Kaspersky Security Center 快速启动向导自动创建。您可以手动创建"将更新下载至管理服务器存储库"任务。
- *执行 Windows 更新同步*。该任务旨在下载 Microsoft 软件的更新元数据。

修复漏洞的软件更新可以是完整的分发包，也可以是补丁。修复软件漏洞的软件更新称为*修补程序*。*推荐的修补程序*是 Kaspersky 专家建议安装的修补程序。*用户修补程序*是用户手动指定安装的修补程序。要安装用户修补程序，您必须创建一个包含此修补程序的安装包。

如果您具有带有漏洞和补丁管理功能的 Kaspersky Security Center 授权许可，若要修复软件漏洞，可以使用"*安装所需更新并修复漏洞*"任务。该任务会通过安装建议的修补程序自动修复多个漏洞。对于此任务，您可以手动配置某些规则来修复多个漏洞。

如果您没有具有漏洞和补丁管理功能的 Kaspersky Security Center 授权许可，若要修复软件漏洞，可以使用"*修复漏洞*"任务。借助此任务，您可以通过安装针对 Microsoft 软件的推荐修补程序和针对其他第三方软件的用户修补程序来修复漏洞。

出于安全原因，卡巴斯基技术会自动扫描您使用漏洞和补丁管理功能安装的任何第三方软件更新，以查找恶意软件。这些技术用于自动文件检查，包括病毒扫描、静态分析、动态分析、沙盒环境中的行为分析和机器学习。

卡巴斯基专家不会对可以使用漏洞和补丁管理功能安装的第三方软件更新进行手动分析。此外，卡巴斯基专家不会在此类更新中搜索漏洞（已知或未知）或未记录的功能，也不会对上面段落中指定的更新以外的更新进行其他类型的分析。

> 在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

要修复某些软件漏洞，如果请求接受最终用户授权许可协议 (EULA)，则必须接受 EULA 才能安装软件。如果您拒绝 EULA，则该软件漏洞不会得到修复。

查看软件漏洞信息

要查看在客户端设备上检测到的漏洞列表，

在控制台树的"**高级**" → "**应用程序管理**"文件夹中，选择"**软件漏洞**"子文件夹。

该页面显示受管理设备上检测到的应用程序漏洞的列表。

若要获得有关选定漏洞的信息，

从该漏洞的上下文菜单中选择"**属性**"。

该漏洞的属性窗口将开启，其中显示以下信息：

- 所检测到的漏洞所在的应用程序。
- 检测到该漏洞的设备的列表。
- 漏洞是否已经被修复的信息。

若要查看所有漏洞的报告，

在“**软件漏洞**”文件夹中，单击“**查看漏洞报告**”链接。

系统将会生成设备上所安装应用程序中关于漏洞的报告。您可以通过打开“**报告**”选项卡，在相关管理服务器名称的节点查看此报告。

查看受管理设备上的漏洞统计信息

您可以查看受管理设备上每个软件漏洞的统计信息。统计信息以图表形式展示。图表将显示具有以下状态的设备数量：

- *忽略：<设备数>*。如果您在漏洞属性中手动设置了忽略漏洞的选项，则分配此状态。
- *已修复：<设备数>*。如果修复漏洞的任务成功完成，则分配此状态。
- *计划修复：<设备数>*。如果已创建修复漏洞的任务但该任务尚未执行，则分配此状态。
- *应用补丁：<设备数>*。如果您手动选择了软件更新以修复漏洞，但此软件更新尚未修复漏洞，则分配此状态。
- *需要修复：<设备数>*。如果漏洞仅在某些受管理设备上得到修复，并且需要在更多托管设备上修复漏洞，则分配此状态。

要查看受管理设备上的漏洞统计信息，请执行以下操作：

1. 在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**软件漏洞**”子文件夹。
   该页面显示受管理设备上检测到的应用程序漏洞的列表。
2. 选择要查看其统计信息的漏洞。
   在用于处理选定对象的区块中，会显示漏洞状态图。单击一种状态将打开漏洞处于选定状态的设备列表。

扫描应用程序以查找漏洞

如果您使用了快速启动向导配置了应用程序，系统将自动创建*漏洞扫描*任务。您可以在“**任务**”选项卡上的“**受管理设备**”文件夹中查看该任务。

若要为客户端设备上所安装应用程序创建漏洞扫描任务，请执行以下操作：

1. 在控制台树中，选择**高级 → 应用程序管理**，然后选择“**软件漏洞**”子文件夹。
2. 在工作区中，选择**附加操作 → 配置漏洞扫描**。

   如果漏洞扫描任务已经存在，则显示“**受管理设备**”文件夹的“**任务**”选项卡，并选中现有任务。否则，查找漏洞和所需更新任务创建向导开始。遵照向导的说明。
3. 在“**选择任务类型**”窗口，选择“**查找漏洞和所需更新**”。
4. 在向导的“**设置**”页面指定任务设置，如下所示：

   - **搜索 Microsoft 列出的漏洞和更新**

     当搜索漏洞和更新时，Kaspersky Security Center 使用当前可用的 Microsoft 更新源中有关适用 Microsoft 更新的信息。

     例如，如果您有带有不同 Microsoft 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

     默认情况下已启用该选项。

     有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

   - **连接更新服务器更新数据**

     受管理设备上的“Windows 更新代理”连接到 Microsoft 更新源。以下服务器可以充当 Microsoft 更新源：

     - Kaspersky Security Center 管理服务器（请参阅网络代理策略的设置）
     - 在组织网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows 服务器
     - Microsoft 更新服务器

     如果启用该选项，受管理设备上的 Windows 更新代理将连接到 Microsoft 更新源以刷新适用 Microsoft Windows 更新的信息。

     如果禁用此选项，受管理设备上的 Windows 更新代理将使用以前从 Microsoft 更新源所收到的适用 Microsoft Windows 更新的信息。

     到 Microsoft 更新源的连接可能消耗资源。如果在其他任务中或网络代理策略属性中设置了到该更新源的常规连接，则您可能想要在“**软件更新和漏洞**”区域禁用此选项。如果您不想禁用此选项，则为了减少服务器过载，您可以配置任务计划以随机分配任务启动延迟（不超过 360 分钟）。

     默认情况下已启用该选项。

网络代理策略设置的以下选项的组合定义了获取更新的方式：

- 仅当在**查找漏洞和所需更新连接更新服务器更新数据任务的属性中**启用了*连接到更新服务器以更新数据查找漏洞和所需更新*选项，并且在网络代理策略的设置中**Windows Update 搜索模式**选项被设置为**主动**时，受管理设备上的 Windows 更新代理才会连接到更新服务器以获取更新 。
- 如果您在执行*漏洞扫描*任务时不需要网络代理发起与 Microsoft Windows 更新源的连接并下载更新，您可以将**Windows Update 搜索模式**选项设置为**被动**，同时**连接更新服务器更新数据**选项必须保持启用。这使您可以节省资源并使用以前收到的 Windows 更新来扫描漏洞。如果您以不同的方式配置接收 Microsoft Windows 更新，则可以使用被动模式。如果没有以其他方式配置接收 Microsoft Windows 更新，请不要将**Windows Update 搜索模式**选项设置为**被动**，因为在这种情况下，将永远不会收到有关更新的信息。
- 不管"**连接更新服务器更新数据**"选项的状态如何（启用或禁用），如果"**Windows Update 搜索模式**"选项被设置为"**已禁用**"，Kaspersky Security Center 不会请求有关更新的任何信息。

- **搜索卡巴斯基列出的第三方漏洞和更新**

  如果启用该选项，Kaspersky Security Center 在 Windows 注册表和"**指定文件系统中应用程序高级搜索的路径**"下指定的文件夹中搜索漏洞和第三方应用程序所需更新（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）。支持的第三方应用程序的完整列表由 Kaspersky 管理。

  如果禁用该选项，Kaspersky Security Center 不为第三方应用程序查找漏洞和所需更新。例如，如果您有带有不同 Microsoft Windows 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

- **指定文件系统中应用程序高级搜索的路径**

  Kaspersky Security Center 搜索需要修复漏洞和安装更新的第三方应用程序。您可以使用系统变量。

  指定应用程序安装文件夹。默认下，列表包含大多数应用程序所安装的系统文件夹。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由"**高级诊断文件的最大大小，MB**"值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

5. 在向导的“**配置任务计划**”页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期一于当前系统时间运行一次。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - **每天(不支持夏令时)**

    任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

    我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。

    默认下，任务每天于当前系统时间运行一次。

  - **每周**

    任务每周在指定星期和指定时间运行。

  - **按星期中的天数**

    任务在每周指定日期的指定时间定期运行。

    默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **当新更新下载至存储库时**

  当新更新下载至存储库后任务运行。例如，您可能想要对"查找漏洞和所需更新"任务使用该计划。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

- 在搜索栏中输入任务名称，即可根据名称搜索任务。
- 单击排序图标可按名称对任务进行排序。
  默认情况下，任务按字母顺序升序排列。
- 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

6. 在向导的“**定义任务名称**”页面，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

7. 在向导的“**完成任务创建**”页面，单击“**完成**”按钮关闭向导。
   如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

向导完成操作后，“**查找漏洞和所需更新**”任务将显示在“**任务**”选项卡上“**受管理设备**”文件夹中的任务列表内。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

当“*查找漏洞和所需更新*”任务完成后，管理服务器显示设备上应用程序中发现的漏洞列表；它还显示用来修复漏洞的所有软件更新。

如果您遇到 0x80240033 “Windows 更新代理错误 80240033（“无法下载授权许可条款。”）”，则可以通过 Windows 注册表解决此问题。

当您先后运行两个任务 – 禁用了**下载快速安装文件**的*执行 Windows 更新同步*任务，和*查找漏洞和所需更新*任务 – 时，管理服务器不显示所需软件更新列表。为了查看所需软件更新列表，您必须再次运行*查找漏洞和所需更新*任务。

网络代理从 Windows 更新或管理服务器（如果管理服务器作为 WSUS 服务器）接收任何可用的 Windows 更新和其他 Microsoft 产品更新的信息。在应用程序启动时（如果由策略规定）和客户端设备上的*查找漏洞和所需更新*任务每次例行运行时，信息被传输。

修复应用程序中的漏洞

如果您已经在快速启动向导的“**更新管理设置**”页面中选定了“**查找并安装所需更新**”，“*安装所需更新并修复漏洞*”任务将自动创建。该任务将显示在“**任务**”选项卡上“**受管理设备**”文件夹的工作区中。

否则，您可以做以下任意：

- 创建任务以通过安装可用更新来修复漏洞。
- 添加漏洞修复规则到现有漏洞修复任务。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

通过创建漏洞修复任务来修复漏洞

您可以做以下任意：

- 创建任务以修复多个满足特定规则的漏洞。
- 选择漏洞并创建修复它和相似漏洞的任务。

要修复满足特定规则的漏洞：

1. 在控制台树中，选择要修复漏洞的设备上的管理服务器。
2. 在主应用程序窗口的**查看**菜单，选择“**配置界面**”。
3. 在打开的窗口中，选中**显示漏洞和补丁管理**复选框，然后单击**确定**。
4. 在带有应用程序消息的窗口，点击“**确定**”。
5. 重新启动管理控制台，使更改生效。

6. 在控制台树中，选择“**受管理设备**”文件夹。

7. 在工作区中，选择“**任务**”选项卡。

8. 单击“**创建任务**”按钮以运行新任务向导。遵照向导的说明。

9. 在该向导的“**选择任务类型**”页面中，选择“**安装所需更新并修复漏洞**”。

   如果未显示任务，请检查您的账户是否有对“**系统管理**：**漏洞和补丁管理**”功能区域的**读取**、**调整**和**执行**权限。如果没有这些访问权限，您不能创建和配置“*安装所需更新并修复漏洞*”任务。

10. 在向导的“**设置**”页面指定任务设置，如下所示：

    - **指定更新安装规则**

      这些规则被应用到客户端设备上的更新安装。如果规则未被指定，任务无可执行。对于使用规则操作的信息，请参考更新安装规则。

    - **在设备重启或关闭时开始安装**

      如果启用该选项，更新在设备被重启或关闭时安装。否则，更新根据计划安装。

      如果安装更新可能影响设备性能则使用该选项。

      默认情况下已禁用该选项。

    - **安装所需的常规系统组件**

      如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

      如果禁用该选项，您可能必须手动安装先决条件。

      默认情况下已禁用该选项。

    - **更新过程中允许安装新应用程序版本**

      如果启用该**选项**，如果更新导致软件应用程序新版本的安装，更新将被允许。

      如果禁用该选项，软件不被升级。您可以稍后手动或通过其他任务安装软件的新版本。例如，如果公司基础架构不被新软件版本支持，或者如果您想要在测试基础架构中检查升级，您可能使用该选项。

      默认情况下已启用该选项。

      升级应用程序可能导致安装在客户端设备上的独立应用程序功能异常。

    - **下载更新到设备而不安装**

      如果启用该选项，应用程序下载更新到设备但是不自动安装它们。您可以稍后手动安装下载的更新。

      Microsoft 更新被下载到系统 Windows 存储。第三方应用程序更新（由非 Kaspersky 和 Microsoft 软件供应商开发的应用程序）将会下载到“**下载更新到**”字段中指定的文件夹中。

      如果禁用该选项，更新被自动安装到设备。

默认情况下已禁用该选项。

- **下载更新到**

  该文件夹用于下载第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由"**高级诊断文件的最大大小，MB**"值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

  - **高级诊断文件的最大大小，MB**

    默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

11. 在向导的"**选择操作系统重启选项**"页面，选择客户端设备的操作系统在操作后必须被重启时的操作：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

12. 在向导的“**配置任务计划**”页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期一于当前系统时间运行一次。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每天(不支持夏令时)**

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。

  默认下，任务每天于当前系统时间运行一次。

- **每周**

  任务每周在指定星期和指定时间运行。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

13. 在向导的“**定义任务名称**”页面，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

14. 在向导的“**完成任务创建**”页面，单击“**完成**”按钮关闭向导。

    如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

等待向导完成操作后，系统将创建“**安装所需更新并修复漏洞**”任务，并显示在“**任务**”文件夹中。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

如果任务结果包含 0x80240033 “Windows 更新代理错误 80240033（“无法下载授权许可条款。”）”错误，则可以通过 Windows 注册表解决此问题。

要修复特定漏洞和相似漏洞：

1. 在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**软件漏洞**”子文件夹。

2. 选择您要修复的漏洞。

3. 单击**运行漏洞修复向导**按钮。

   漏洞修复向导启动。

   漏洞修复向导功能仅在漏洞和补丁管理授权许可下可用。

   遵照向导的说明。

4. 在“**搜索现有的漏洞修复任务**”窗口，指定以下参数：

   - **仅显示修复该漏洞的任务**

     如果启用该选项，漏洞修复向导搜索修复所选漏洞的现有任务。

     如果禁用该选项或搜索未检索到可应用任务，漏洞修复向导提示您为修复漏洞创建规则或任务。

     默认情况下已启用该选项。

   - **批准修复该漏洞的更新**

     修复漏洞的更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

     默认情况下已禁用该选项。

5. 如果您选择搜索现有漏洞修复任务或搜索检索到一些任务，您可以查看这些任务的属性或手动启动它们。不需要进一步操作。

   否则，单击**新漏洞修复任务**按钮。

6. 选择漏洞修复规则类型以添加到新任务，然后点击**结束**按钮。

7. 在显示的提示中做出安装所有先前应用程序更新的选择。如果您同意在安装所选更新需要时安装连续的应用程序版本，点击**是**。如果您要直接更新应用程序而不安装连续版本，点击**否**。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

   更新安装和漏洞修复任务创建向导启动。遵照向导的说明。

8. 在向导的"**选择操作系统重启选项**"页面，选择客户端设备的操作系统在操作后必须被重启时的操作：

   - **不重启设备**

     客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

   - **重启设备**

     如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

   - **提示用户操作**

     客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

     默认情况下已选定该选项。

     - **重复提示间隔(分钟)**

       如果启用该选项，应用程序以指定频率提示用户重启操作系统。

       默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

       如果禁用该选项，提示仅显示一次。

     - **在该时间后重启(分钟)**

       提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

       默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

   - **强行关闭锁定会话中的应用程序**

     运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

     如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

默认情况下已禁用该选项。

9. 在向导的“**选择要对其分配任务的设备**”页面，选择以下选项之一：

- **选择管理服务器检测到的网络设备**

  任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。

  例如，您可能要在安装网络代理到未分配的设备的任务中使用该选项。

- **手动指定设备地址或从列表导入地址**

  您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- **分配任务到设备分类**

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。

  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

- **分配任务到管理组**

  任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

  例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

  如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

10. 在向导的“**配置任务计划**”页面，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

- **每 N 星期**

  任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。
  默认下，任务每星期一于当前系统时间运行一次。

- **每 N 分钟**

  任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。
  默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每天(不支持夏令时)**

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。
  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。
  默认下，任务每天于当前系统时间运行一次。

- **每周**

  任务每周在指定星期和指定时间运行。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。
  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。
  在缺少指定日的月份，任务在最后一天运行。
  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

默认情况下，开始时间为18:00，且未选择任何日期。

请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是"**手动**"、"**一次**"或"**立即**"，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于"**手动**"、"**一次**"和"**立即**"计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

11. 在向导的"**定义任务名称**"页面，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

12. 在向导的"**完成任务创建**"页面，单击"**完成**"按钮关闭向导。

    如果您想让任务在向导完成时立即启动，选择"**向导完成时运行任务**"复选框。

当向导完成后，系统将创建"**安装所需更新并修复漏洞**"任务，并显示在"**任务**"文件夹中。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

通过添加规则到现有漏洞修复任务来修复漏洞

要通过添加规则到现有漏洞修复任务来修复漏洞：

1. 在控制台树的"**高级**" → "**应用程序管理**"文件夹中，选择"**软件漏洞**"子文件夹。

2. 选择您要修复的漏洞。

3. 单击**运行漏洞修复向导**按钮。

   漏洞修复向导启动。

   漏洞修复向导功能仅在漏洞和补丁管理授权许可下可用。

   遵照向导的说明。

4. 在"**搜索现有的漏洞修复任务**"窗口，指定以下参数：

- **仅显示修复该漏洞的任务**

  如果启用该选项，漏洞修复向导搜索修复所选漏洞的现有任务。

  如果禁用该选项或搜索未检索到可应用任务，漏洞修复向导提示您为修复漏洞创建规则或任务。

默认情况下已启用该选项。

- **批准修复该漏洞的更新**

  修复漏洞的更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

  默认情况下已禁用该选项。

5. 如果您选择搜索现有漏洞修复任务或搜索检索到一些任务，您可以查看这些任务的属性或手动启动它们。不需要进一步操作。

   否则，单击**添加漏洞修复规则到现有任务**按钮。

6. 选择您要添加规则的任务，然后单击"**添加规则**"按钮。

   而且，你您可以查看现有任务的属性，手动启动它们，或者创建新任务。

7. 选择规则类型以添加到所选任务，然后点击**结束**按钮。

8. 在显示的提示中做出安装所有先前应用程序更新的选择。如果您同意在安装所选更新需要时安装连续的应用程序版本，点击**是**。如果您要直接更新应用程序而不安装连续版本，点击**否**。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

漏洞修复新规则被添加到现有**安装所需更新并修复漏洞**任务。

修复隔离网络中的漏洞

本节介绍要修复已连接到没有互联网访问权限的管理服务器的受管理设备上的第三方软件漏洞所采取的步骤。

方案：修复隔离网络中的第三方软件漏洞

您可以在隔离网络中的受管理设备上安装更新和修复已安装的第三方软件的漏洞。此类网络包括管理服务器和连接到它们但没有接入互联网的受管理设备。要修复此类网络中的漏洞，您需要已连接到互联网的管理服务器。然后，您将能够使用具有互联网访问权限的管理服务器下载补丁（所需更新），然后将补丁传输到隔离的管理服务器。

您可以下载软件供应商发布的第三方软件更新，但无法在隔离的管理服务器上使用 Kaspersky Security Center 下载 Microsoft 软件更新。

要了解在隔离网络中修复漏洞的过程，请参阅此过程的描述和方案。

先决条件

在开始之前，请执行以下操作：

1. 分配一台设备用于连接互联网和下载补丁。该设备将被视为具有互联网访问权限的管理服务器。
2. 在以下设备上安装 Kaspersky Security Center，版本不能低于 14：
   - 分配的设备，将用作具有互联网访问权限的管理服务器
   - 隔离的设备，将用作与互联网隔离的管理服务器（以下称为隔离的管理服务器）
3. 确保每个管理服务器都有足够的磁盘空间用于下载和存储更新和补丁。

阶段

在隔离的管理服务器的受管理设备上安装更新和修复第三方软件漏洞分为以下阶段：

1. **配置具有互联网访问权限的管理服务器**

   准备具有互联网访问权限的管理服务器以处理对所需第三方软件更新的请求和下载补丁。

2. **配置隔离的管理服务器**

   准备隔离的管理服务器，让它们定期形成所需更新列表并处理通过具有互联网访问权限的管理服务器下载的补丁。配置后，隔离的管理服务器不再尝试从互联网下载补丁。相反，它们通过补丁获取更新。

3. **在隔离的管理服务器上传输补丁和安装更新**

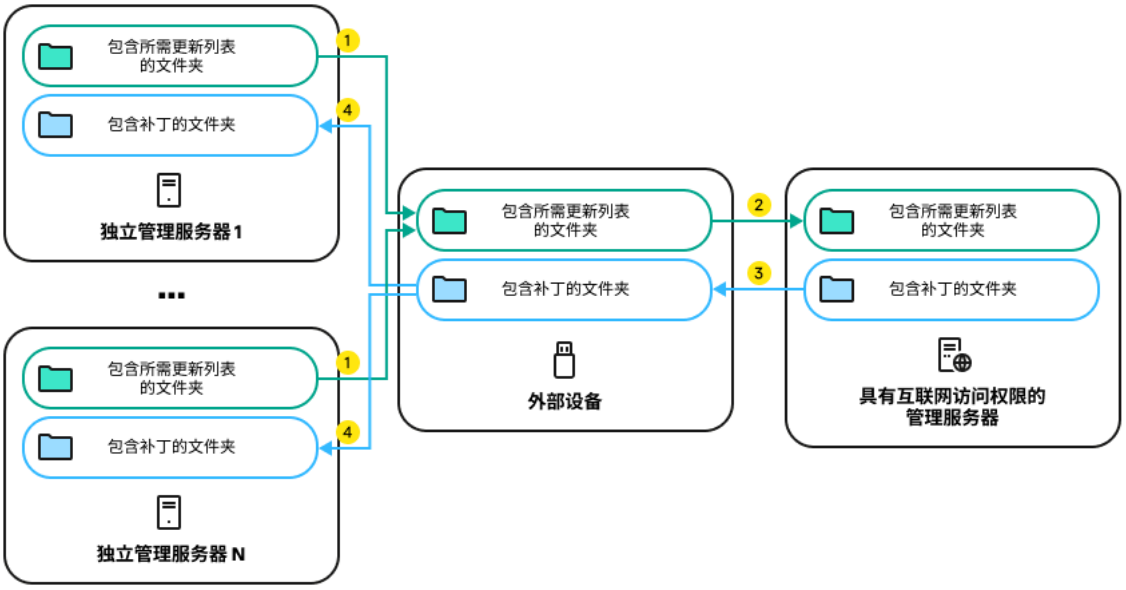
   完成管理服务器配置后，您可以在具有互联网访问权限的管理服务器和隔离的管理服务器之间传输所需的更新列表和补丁。接下来，补丁中的更新将通过“*安装所需更新并修复漏洞*”任务安装到受管理设备上。

结果

这样，第三方软件更新将传输到隔离的管理服务器并通过 Kaspersky Security Center 安装到连接的受管理设备上。配置管理服务器一次就足够了，之后可以根据需要随时获取更新，例如每天一次或多次。

关于修复隔离网络中的第三方软件漏洞

修复隔离网络中的第三方软件漏洞的过程如图所示，介绍如下。您可以定期重复此过程。



在具有互联网访问权限的管理服务器和隔离的管理服务器之间传输补丁和所需更新列表的过程

每个与互联网隔离的管理服务器（以下称为隔离的管理服务器）都会生成一个更新列表，其中的更新需要安装在与管理服务器连接的受管理设备上。所需更新列表存储在一个特定文件夹中，并描述一组二进制文件。每个文件都有一个名称，其中包含带有所需更新的补丁的 ID。因此，列表中的每个文件都指向一个特定补丁。

利用外部设备，可以将所需更新列表从隔离的管理服务器传输到分配的具有互联网访问权限的管理服务器。之后，分配的管理服务器从互联网下载补丁并将它们放在单独的文件夹中。

当所有补丁均已下载并放到它们的特殊文件夹后，将这些补丁移动到您从中获取所需更新列表的每个隔离的管理服务器。将补丁保存到隔离的管理服务器上专门为补丁创建的文件夹中。结果，“*安装所需更新并修复漏洞*”任务在隔离的管理服务器的受管理设备上运行补丁并安装更新。

配置具有互联网访问权限的管理服务器以修复隔离网络中的漏洞

要准备在隔离网络中修复漏洞并传输补丁，请首先配置具有互联网访问权限的管理服务器，然后配置隔离的管理服务器。

要配置具有互联网访问权限的管理服务器：

1. 在安装了管理服务器的磁盘上创建两个文件夹：
   - 所需更新列表的文件夹
   - 补丁文件夹

   您可以随意命名这些文件夹。
2. 使用操作系统的标准管理工具为 KLAdmins 组授予对所创建的文件夹的“修改”访问权限。

3. 使用 klscflag 实用程序将文件夹的路径写入管理服务器属性。

   使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

4. 在 Windows 命令提示时输入以下命令：

   - 要设置补丁文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<文件夹的路径>"`
   - 要设置所需更新列表的文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<文件夹的路径>"`

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<补丁文件夹>"`

5. 如果必要，使用 klscflag 实用程序指定管理服务器检查新补丁请求的频率：
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <以秒为单位的值>`

   默认值是 120 秒。

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. 创建“*查找漏洞和所需更新*”任务以获取有关受管理设备上安装的第三方软件的补丁信息，然后设置任务计划。

7. 创建“*修复漏洞*”任务，指定用于修复漏洞的第三方软件的补丁，并设置任务计划。

   如果您希望该任务在计划中指定的时间之前运行，请手动运行任务。任务启动的顺序很重要。完成“*查找漏洞和所需更新*”任务后必须运行“*修复漏洞*”任务。

8. 重启管理服务器服务。

现在，具有互联网访问权限的管理服务器已准备好下载更新并将更新传输到隔离的管理服务器。在开始修复漏洞之前，配置隔离的管理服务器。

配置隔离的管理服务器以修复隔离网络中的漏洞

完成配置具有互联网访问权限的管理服务器后，准备好网络中的每个隔离的管理服务器，这样您就可以对连接到隔离的管理服务器的受管理设备修复漏洞和安装更新。

要配置隔离的管理服务器，请在每个管理服务器上执行以下操作：

1. 激活漏洞和补丁管理 (VAPM) 功能的授权许可密钥。

2. 在安装了管理服务器的磁盘上创建两个文件夹：

   - 将显示所需更新列表的文件夹
   - 补丁文件夹

   您可以随意命名这些文件夹。

3. 使用操作系统的标准管理工具为 KLAdmins 组授予对所创建的文件夹的“*修改*”权限。

4. 使用 klscflag 实用程序将文件夹的路径写入管理服务器属性。

   使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

5. 在 Windows 命令提示时输入以下命令：

   - 要设置补丁文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v “<文件夹的路径>”`
   - 要设置所需更新列表的文件夹的路径：
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<文件夹的路径>"`

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<补丁文件夹>"`

6. 如果必要，使用 klscflag 实用程序指定隔离的管理服务器检查新补丁的频率：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <以秒为单位的值>`

   默认值是 120 秒。

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. 如果必要，使用 klscflag 实用程序计算补丁的 SHA256 哈希：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   如果输入此命令，您可以确保补丁在传输到隔离管理服务器期间未被修改，并且您已收到包含所需更新的正确补丁。

   默认情况下，Kaspersky Security Center 不计算补丁的 SHA256 哈希。如果启用此选项，在隔离的管理服务器收到补丁后，Kaspersky Security Center 会计算其哈希，并将获取的值与管理服务器数据库中存储的哈希进行比较。如果计算出的哈希与数据库中的哈希不匹配，则会发生错误，您必须更换不正确的补丁。

8. 创建“*查找漏洞和所需更新*”任务以获取有关受管理设备上安装的第三方软件的补丁信息，然后设置任务计划。

9. 创建“*修复漏洞*”任务，指定用于修复漏洞的第三方软件的补丁，并设置任务计划。

   如果您希望该任务在计划中指定的时间之前运行，请手动运行任务。任务启动的顺序很重要。完成“*查找漏洞和所需更新*”任务后必须运行“*修复漏洞*”任务。

10. 重启管理服务器服务。

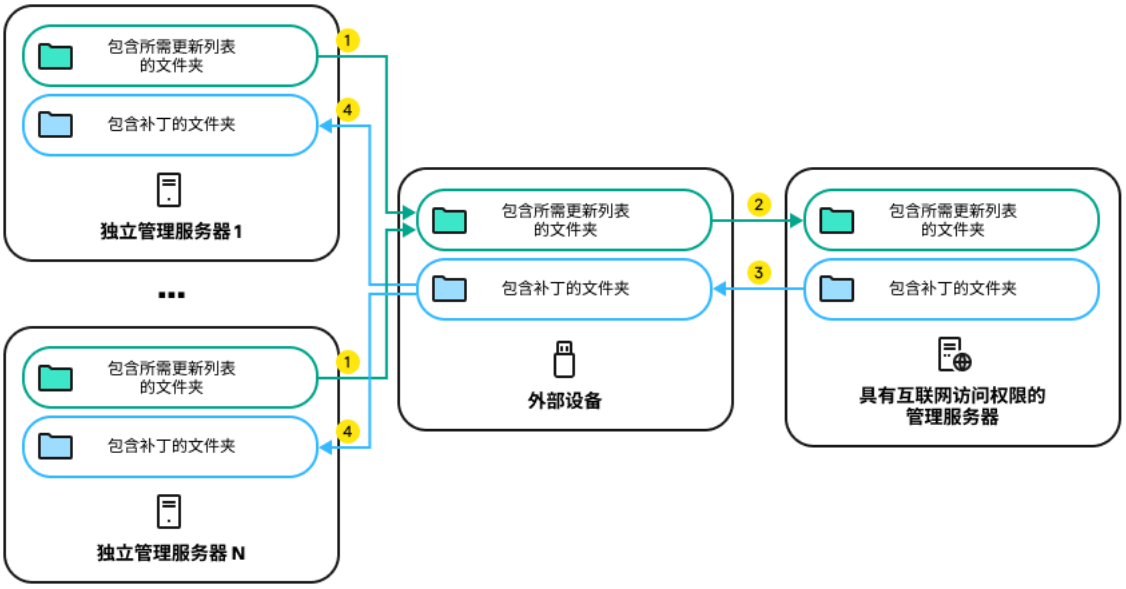
配置所有管理服务器后，您可以移动补丁和所需更新列表，并修复隔离网络中的受管理设备上的第三方软件漏洞。

在隔离网络中传输补丁和安装更新

完成配置管理服务器后，您可以将包含所需更新的补丁从具有互联网访问权限的管理服务器传输到隔离的管理服务器。您可以根据需要随时传输和安装更新，例如每天一次或多次。

> 您需要外部设备（如可移动驱动器）才能在管理服务器之间传输补丁和所需更新的列表。因此，请确保外部设备具有足够的磁盘空间用于下载和存储补丁。

传输补丁和所需更新列表的过程如图所示，说明如下：



在具有互联网访问权限的管理服务器和隔离的管理服务器之间传输补丁和所需更新列表的过程

要在连接到隔离的管理服务器的受管理设备上安装更新和修复漏洞：

1. 启动"*安装所需更新并修复漏洞*"任务（如果尚未运行）。
2. 将外部设备连接到任一隔离的管理服务器。
3. 在外部设备上创建两个文件夹：一个用于所需更新列表，一个用于补丁。您可以随意命名这些文件夹。

   如果您之前创建了这些文件夹，请清除。
4. 从每个独立的管理服务器复制所需更新列表，并将此列表粘贴到外部设备上保存所需更新列表的文件夹中。

   因此，您可以将从所有隔离的管理服务器获取的所有列表合并到一个文件夹中。此文件夹包含二进制文件，其中包含所有隔离的管理服务器所需的补丁 ID。
5. 将外部设备连接到具有互联网访问权限的管理服务器。
6. 从外部设备复制所需更新列表，并将此列表粘贴到具有互联网访问权限的管理服务器上保存所需更新列表的文件夹中。

   所有所需补丁都会自动从互联网下载到管理服务器上的补丁文件夹中。这可能需要几个小时的时间。
7. 确保所有所需补丁均已下载。为此，您可以执行以下操作之一：

   - 检查具有互联网访问权限的管理服务器上的补丁文件夹。所需更新列表中指定的所有补丁都应该下载到必需的文件夹中。如果需要少量补丁，这会更方便。
   - 准备一个特殊的脚本，例如，一个 shell 脚本。如果有大量补丁，将很难自行检查是否已下载所有补丁。在这种情况下，最好将检查自动化。
8. 从具有互联网访问权限的管理服务器复制补丁并粘贴到外部设备上的相应文件夹中。
9. 将补丁传输到每个隔离的管理服务器。将补丁放入它们的特定文件夹。

结果，每个隔离的管理服务器都会创建一个实际的更新列表，这些更新是连接到当前管理服务器的受管理设备所需的。在具有互联网访问权限的管理服务器收到所需更新列表后，管理服务器会从互联网下载补丁。当这些补丁出现在隔离的管理服务器上后，“*安装所需更新并修复漏洞*”任务将处理补丁。因此，更新安装在受管理设备上，第三方软件漏洞得到修复。

当“*安装所需更新并修复漏洞*”任务运行时，不要重新启动管理服务器设备，也不要运行“*备份管理服务器数据*”任务（它也会导致重新启动）。结果，“*安装所需更新并修复漏洞*”任务被中断，并且更新没有安装。在这种情况下，您必须手动重新启动此任务或等待任务按照配置的计划启动。

禁用在隔离网络中传输补丁和安装更新的选项

您可以禁止在隔离的管理服务器上传输补丁，例如，如果您决定将一个或多个管理服务器从隔离网络中移出。这样，您可以减少补丁的数量和下载它们的时间。

要禁用在隔离的管理服务器上传输补丁的选项：

1. 如果要使所有管理服务器脱离隔离状态，请在具有互联网访问权限的管理服务器的属性中，删除用于补丁和所需更新列表的文件夹的路径。如果要在隔离网络中保留一些管理服务器，请跳过此步骤。

   使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

   命令提示时输入以下命令：

   - 要删除补丁文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - 要删除所需更新列表的文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. 如果删除了此管理服务器上文件夹的路径，请重新启动管理服务器服务。

3. 在要解除隔离的每个管理服务器的属性中，删除用于补丁和所需更新列表的文件夹的路径。

   使用管理员权限在 Windows 命令提示符处输入以下命令：

   - 要删除补丁文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - 要删除所需更新列表的文件夹的路径：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. 重新启动已删除文件夹路径的每个管理服务器的服务。

结果是，如果您重新配置了具有互联网访问权限的管理服务器，您将不再通过 Kaspersky Security Center 接收补丁。如果您仅重新配置了一些隔离的管理服务器，例如，将它们从隔离网络中移出，将只会为其余的隔离管理服务器获取补丁。

如果在将来要开始修复已禁用的隔离管理服务器上的漏洞，您必须再次配置这些管理服务器和具有互联网权限的管理服务器。

忽略软件漏洞

您可以忽略要修复的软件漏洞。忽略软件漏洞的原因可能有如下几点：

- 您认为该软件漏洞对您的组织不严重。
- 您了解该软件漏洞修补程序可能会破坏与需要该漏洞修补程序的软件相关的数据。
- 您可以确定该软件漏洞对组织的网络没有危险，因为您使用其他措施来保护受管理设备。

您可以忽略所有受管理设备上或仅选定受管理设备上的软件漏洞。

要忽略所有受管理设备上的软件漏洞，请执行以下操作：

1. 在控制台树的"**高级**"→"**应用程序管理**"文件夹中，选择"**软件漏洞**"子文件夹。
   文件夹的工作区中将显示设备上所安装网络代理在应用程序中所检测到的漏洞的列表。
2. 选择您要忽略的漏洞。
3. 从该漏洞的上下文菜单中选择"**属性**"。
   漏洞的属性窗口打开。
4. 在"**常规**"区域中，选择"**忽略漏洞**"选项。
5. 单击"**确定**"。
   此时将关闭软件漏洞属性窗口。

在所有受管理设备上都会忽略该软件漏洞。

要忽略选定受管理设备上的软件漏洞，请执行以下操作：

1. 打开选定受管理设备的属性窗口，然后选择"**软件漏洞**"区域。
2. 选择软件漏洞。
3. 忽略选定漏洞。

选定设备上的软件漏洞将被忽略。

在完成"*修复漏洞*"任务或"*安装所需更新并修复漏洞*"任务后，将无法修复被忽略的软件漏洞。您可以通过使用过滤器从漏洞列表中排除被忽略的软件漏洞。

为第三方软件中的漏洞选择用户修补程序

要使用"*修复漏洞*"任务，您必须手动指定软件更新以修复任务设置中列出的第三方软件中的漏洞。"*修复漏洞*"任务使用针对 Microsoft 软件的建议修补程序以及针对其他第三方软件的用户修补程序。*用户修补程序*是软件更新，用于修复管理员手动指定的漏洞。

要为第三方软件中的漏洞选择用户修补程序，请执行以下操作：

1. 在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**软件漏洞**”子文件夹。
   文件夹的工作区中将显示设备上所安装网络代理在应用程序中所检测到的漏洞的列表。
2. 选择要为其指定用户修补程序的漏洞。
3. 从该漏洞的上下文菜单中选择“**属性**”。
   漏洞的属性窗口打开。
4. 在**用户修复和其他修复**区域中，单击**添加**按钮。
   此时将显示可用安装包的列表。显示的安装包列表对应于**远程安装 → 安装包**列表。如果尚未创建包含针对所选漏洞用户修补程序的安装包，则可以立即通过启动“新安装包向导”来创建该包。
5. 选择一个或多个安装包，其中包含针对第三方软件漏洞的一个或多个用户修补程序。
6. 单击“**确定**”。

系统会指定包含软件漏洞用户修补程序的安装包。启动“*修复漏洞*”任务后，将安装安装包并修复软件漏洞。

更新安装规则

当在应用程序中修复漏洞时，您必须指定更新安装规则。这些规则决定要安装的更新和要修复的漏洞。

精确设置取决于您是否创建了 Microsoft 应用程序、第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）、或所有应用程序的更新的规则。当创建 Microsoft 应用程序或第三方应用程序规则时，您可以选择特定的应用程序和您要安装更新的应用程序版本。当创建所有应用程序的规则时，您可以选择您要安装的特定更新和您要通过安装更新而修复的漏洞。

要为所有应用程序更新创建规则：

1. 在新任务向导的“**设置**”页面，点击“**添加**”按钮。
   规则创建向导开始。遵照向导的说明。
2. 在**规则类型**页面，选择**所有更新的规则**。
3. 在“**常规标准**”页面，使用下拉列表指定以下设置：

   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：
     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

- **修复严重级别等于或大于该项的漏洞**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

4. 在“**更新**”页面，选择要安装的更新：

   - **安装所有适用的更新**

     安装符合向导“**常规标准**”页面上指定条件的所有软件更新。默认选择。

   - **仅安装列表中的更新**

     仅安装您从列表中手动选择的软件更新。该列表包含所有可用软件更新。

     例如，您可能想要在以下情况下选择特定更新：要在测试环境中检查它们的安装、要仅更新严重应用程序、或者要仅更新特定应用程序。

     - **自动安装所选更新安装所需的所有先前应用程序更新**

       如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

       如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

       例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

       默认情况下已启用该选项。

5. 在“**漏洞**”页面，选择将由安装所选更新修复的漏洞。

   - **修复所有匹配其他标准的漏洞**

     修复符合向导“**常规标准**”页面上指定条件的所有漏洞。默认选择。

   - **仅修复列表中的漏洞**

     仅修复您手动从列表中选择的漏洞。列表包含所有检测到的漏洞。

     例如，您可能想要在以下情况下选择特定漏洞：要在测试环境中检查它们的修复、要仅修复严重应用程序中的漏洞、或者要仅修复特定应用程序中的漏洞。

6. 在**名称**页面，指定您正在创建的规则名称。您可以稍后在所创建任务的属性窗口的**设置**区域更改该名称。

规则创建向导完成操作后，将创建新规则，并显示在新任务向导的“**指定更新安装规则**”字段。

要为 Microsoft 应用程序更新创建规则：

1. 在新任务向导的“**设置**”页面，点击“**添加**”按钮。
   规则创建向导开始。遵照向导的说明。
2. 在“**规则类型**”页面上，选择“**Windows 更新的规则**”。
3. 在“**常规标准**”页面，指定以下设置：
   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：
     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。
   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。
   - **修复 MSRC 严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。
4. 在**应用程序**页面，选择您要安装更新的应用程序和应用程序版本。默认情况下选定所有应用程序。
5. 在“**更新类别**”页面，选择要安装的更新类别。这些类别与 Microsoft Update Catalog 中的类别相同。默认情况下选定所有类别。
6. 在**名称**页面，指定您正在创建的规则名称。您可以稍后在所创建任务的属性窗口的**设置**区域更改该名称。

规则创建向导完成操作后，将创建新规则，并显示在新任务向导的“**指定更新安装规则**”字段。

要为第三方应用程序更新创建规则：

1. 在新任务向导的“**设置**”页面，点击“**添加**”按钮。
   规则创建向导开始。遵照向导的说明。
2. 在“**规则类型**”页面，选择“**第三方更新的规则**”。
3. 在“**常规标准**”页面，指定以下设置：
   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：
     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。
   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。
4. 在“**应用程序**”页面，选择您要安装更新的应用程序和应用程序版本。默认情况下选定所有应用程序。
5. 在**名称**页面，指定您正在创建的规则名称。您可以稍后在所创建任务的属性窗口的**设置**区域更改该名称。

规则创建向导完成操作后，将创建新规则，并显示在新任务向导的“**指定更新安装规则**”字段。

应用程序组

该区域将说明如何管理设备上安装的应用程序组。

创建应用程序类别

Kaspersky Security Center 允许创建设备上所安装应用程序的类别。

您可以通过以下方式创建应用程序类别：

- 管理员指定某个文件夹，所选类别中包括的可执行文件将存放在该文件夹中。
- 管理员指定某个设备，所选类别中包括的可执行文件将存放在该设备中。
- 管理员设置用于将应用程序包括在所选类别的标准。

创建应用程序类别之后，管理员可以为该应用程序类别设置规则。这些规则将定义指定类别中所包括应用程序的行为。例如，您可以阻止或允许启动某个类别中包括的应用程序的启动。

管理设备上的应用程序运行

Kaspersky Security Center 允许您以允许列表模式管理设备上的应用程序启动。详情请参考 Kaspersky Endpoint Security for Windows Online Help。在允许列表模式下，您只可以在选定设备上启动指定类别中包括的应用程序。管理员可以查看每一个设备上的用户运行的应用程序所应用规则的统计分析结果。

清查设备上所安装的软件

Kaspersky Security Center 允许清查 Windows 和 Linux 设备上所安装的软件。网络代理将检索设备上所安装应用程序的所有信息。在清查期间检索到的信息将显示在“**应用程序注册表**”文件夹的工作区中。管理员可以查看任何应用程序相关的信息，包括其版本和生产商。

从单个设备接收的可执行文件数量不能超过 150,000。达到此限制后，Kaspersky Security Center 无法接收新文件。

已授权应用程序组管理

Kaspersky Security Center 允许您创建已授权应用程序的群组。这是一组由满足管理员所设标准的应用程序组成的授权应用程序群组。管理员可以为授权应用程序组指定以下标准：

- 应用程序名称
- 应用程序版本
- 制造商
- 应用程序标签

满足一个或多个标准的应用程序将自动包括在群组中。若要创建一组已授权应用程序，您必须设置至少一个将应用程序包括在此类组中的标准。

每个已授权应用程序组有其自己的授权许可密钥。已授权应用程序组的授权许可密钥定义了该组中包括的应用程序的最大允许安装数量。如果安装数量超过了授权许可密钥中设置的限值，将在管理服务器中记录信息事件。管理员可以指定该授权许可密钥的有效期。到达该日期后，信息事件将记录在管理服务器中。

查看可执行文件信息

Kaspersky Security Center 将检索设备上安装操作系统以来运行过的可执行文件的所有信息。有关可执行文件的信息将显示在“**可执行文件**”文件夹工作区中的主应用程序窗口中。

使用应用程序控制来管理可执行文件

您可以使用“应用程序控制”组件来允许或阻止可执行文件在用户设备上启动。“应用程序控制”组件支持基于 Windows 和基于 Linux 的操作系统。

对于基于 Linux 的操作系统，应用程序控制组件从 Kaspersky Endpoint Security 11.2 for Linux 开始可用。此外，该组件还可用于 Kaspersky Embedded Systems Security for Windows 3.0 或更高版本。

先决条件

- Kaspersky Security Center 已部署在您的组织中。
- Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的策略已创建并处于活动状态。
- Kaspersky Embedded Systems Security for Windows 或 Kaspersky Embedded Systems Security for Linux 的策略已创建并处于活动状态。

阶段

“应用程序控制”使用方案分阶段进行：

1. **形成并查看客户端设备上的可执行文件列表**

   此阶段帮助您了解在受管理设备上发现了哪些可执行文件。查看可执行文件列表，并将其与允许和禁止的可执行文件列表进行比较。对可执行文件的使用限制可能与组织中的信息安全策略有关。

   说明：

   - 管理控制台：可执行文件清单
   - Kaspersky Security Center Web Console：获取并查看客户端设备上存储的可执行文件列表

2. **为组织中使用的可执行文件创建类别**

   分析受管理设备上存储的可执行文件列表。根据分析，为可执行文件创建类别。建议创建一个“工作应用程序”类别，以覆盖组织中使用的标准可执行文件集。如果不同的安全组在工作中使用不同的可执行文件集，则可以为每个安全组创建单独的类别。

   说明：

   - 创建含有手动添加内容的应用程序类别，创建包含来自选定设备的可执行文件的应用程序类别，创建包含来自特定文件夹的可执行文件的应用程序类别。
   - Kaspersky Security Center Web Console：创建含有手动添加内容的应用程序类别，创建包含来自选定设备的可执行文件的应用程序类别，创建包含来自具体文件夹的可执行文件的应用程序类别。

3. **在 Kaspersky Endpoint Security 策略中配置“应用程序控制”**

   使用您在上一阶段创建的类别，在 Kaspersky Endpoint Security 策略中配置“应用程序控制”组件。

说明：

- 管理控制台：配置应用程序在客户端设备上的启动管理
- Kaspersky Security Center Web Console：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

4 在 Kaspersky Embedded Systems Security 策略中配置“应用程序控制”

使用您创建的类别配置 Kaspersky Embedded Systems Security for Windows 策略中的应用程序控制组件。有关应用程序控制组件的更多信息，请参阅Kaspersky Embedded Systems Security for Windows 帮助 或 Kaspersky Embedded Systems Security for Linux 帮助。

如果使用大量规则，加载策略时可能会出现错误。您可以使用以下命令增加最大请求大小（以字节为单位）：

- 对于 JSON 请求：

```
klscflag -fset -pv ".core/.independent" -s KLLIM -n
LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
```

- 对于 HTTP 请求：

```
klscflag -fset -pv ".core/.independent" -s KLLIM -n
LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
```

其中<max_request_size>是以字节为单位的最大请求大小（例如，200000000）。

5 在测试模式下开启“应用程序控制”组件

为确保应用程序控制规则不会阻止用户工作所需的可执行文件，建议在创建新规则后启用应用程序控制规则测试并分析其操作。启用测试后，Kaspersky Endpoint Security for Windows 或 Kaspersky Embedded Systems Security 将不会阻止被应用程序控制规则禁止启动的可执行文件，而是将有关其启动的通知发送到管理服务器。

测试应用程序控制规则时，建议执行以下操作：

- 确定测试周期。测试周期从几天到两个月不等。
- 检查由测试“应用程序控制”操作生成的事件。

Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中启用“**测试模式**”选项。

6 更改“应用程序控制”组件的类别设置

如有必要，请更改“应用程序控制”设置。根据测试结果，您可以将与应用程序控制组件事件相关的可执行文件添加到含有手动添加内容的类别中。

说明：

- 管理控制台：添加事件相关的可执行文件到应用程序类别
- Kaspersky Security Center Web Console：添加事件相关的可执行文件到应用程序类别

7 在操作模式下应用“应用程序控制”的规则

测试应用程序控制规则并完成类别的配置后，您可以在操作模式下应用这些应用程序控制规则。

Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中禁用“**测试模式**”选项。

8 验证“应用程序控制”配置

确保已完成以下操作：

- 为可执行文件创建类别。
- 已使用类别来配置应用程序控制。
- 已在操作模式下应用“应用程序控制”的规则。

结果

方案完成后，可执行文件在受管理设备上的启动受到控制。用户只能运行组织中允许的可执行文件，而不能运行组织中禁止的可执行文件。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

获取并查看客户端设备上存储的可执行文件列表

您可以通过以下方式之一获取存储在客户端设备上的可执行文件列表：

- 在 Kaspersky Endpoint Security 策略中启用应用程序启动通知。
- 创建清查任务。

在 Kaspersky Endpoint Security 策略中启用应用程序启动通知

要启用有关应用程序启动的通知：

1. 打开 Kaspersky Endpoint Security 策略设置，然后转到**常规设置 → 报告和存储**。
2. 在**到管理服务器的数据传输**设置组中，选择**关于启动的应用程序**复选框，保存更改。

当用户尝试启动可执行文件时，关于这些文件的信息将被添加到客户端设备上的可执行文件列表中。Kaspersky Endpoint Security 会将该信息发送到网络代理，然后网络代理将其发送到管理服务器。

创建清单任务

清查可执行文件的功能可用于以下应用程序：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 版本 11.2 及更高版本
- Kaspersky Security for Virtualization 4.0 Light Agent 和更高版本

您可以在获取已安装应用程序相关信息的同时减少数据库的负载。为了节省空间，在安装了一组标准软件的参考设备上运行清单任务。建议设备数量为 1-3。

我们强烈不建议在使用以下数据库时运行清单任务：MySQL、PostgreSQL、SQL Server Express Edition、MariaDB（所有版本）。

要在客户端设备上为可执行文件创建清查任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在“**任务**”文件夹的工作区，单击“**新任务**”按钮。

   “新任务向导”启动。
3. 在向导的“**选择任务类型**”窗口，选择“**Kaspersky Endpoint Security**”做为任务类型，然后选择“**清单**”做为任务子类型，并单击**下一步**。
4. 遵照剩余的向导说明。

   新任务向导完成后，将创建并配置“**清单**”任务。如果需要，可以更改已创建任务的设置。新创建的任务显示在任务列表中。如果需要，可以更改已创建任务的设置。

关于清查任务的详细说明，请参阅以下帮助：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Security for Virtualization Light Agent

执行“**清单**”任务后，将形成受管理设备上存储的可执行文件列表，您可以查看该列表。

清查过程中可检测以下格式的可执行文件（具体取决于您在清单任务属性中选择的选项）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

查看受管理设备上存储的可执行文件列表

要查看客户端设备上存储的可执行文件列表：

在控制台树中，转到**高级** → **应用程序管理** → **可执行文件**。

如有必要，您可以将可执行文件从受管理设备发送到安装有管理控制台的设备。

要发送可执行文件：

1. 在控制台树中，转到**高级 → 应用程序管理 → 可执行文件**。
2. 单击您想要发送到安装有管理控制台的设备的可执行文件的链接。
3. 在打开的窗口中，转到**设备**部分，然后选中要从其发送可执行文件的受管理设备的复选框。

   在发送可执行文件之前，请确保受管理设备与管理服务器有直接连接，方法是选择**不断开与管理服务器的连接**复选框。

4. 单击**发送**按钮，选择目的文件夹，然后单击**确定**。

所选可执行文件被下载，以供进一步发送到安装有管理控制台的设备。

为 Kaspersky Endpoint Security for Windows 策略创建应用程序类别

您可以从“**应用程序类别**”文件夹和 Kaspersky Endpoint Security for Windows 策略的“**属性**”窗口为 Kaspersky Endpoint Security for Windows 策略创建应用程序类别。

*要从“**应用程序类别**”文件夹为 Kaspersky Endpoint Security 策略创建应用程序类别：*

1. 在控制台树中，选择**高级 → 应用程序管理 → 应用程序类别**。
2. 在“**应用程序类别**”文件夹的工作区，单击“**新类别**”按钮。
   新类别向导启动。
3. 在“**类别类型**”页面，选择用户类别类型：
   - **含有手动添加内容的类别**。指定用于分配可执行文件到到所创建类别的标准。
   - “**含有自动添加内容的类别**”。指定其可执行文件将被自动分配到所创建类别的文件夹。

     当创建自动添加内容的类别时，应用程序清查以下文件类型：EXE、COM、DLL、SYS、BAT、PS1、CMD、JS、VBS、REG、MSI、MSC、CPL、HTML、HTM、DRV、OCX 和 SCR。

   - **包含来自所选设备的可执行文件的类别**。指定其可执行文件将被自动分配到类别的设备。
4. 遵照向导的说明操作。

   当向导结束时，自定义应用程序类别被创建。您可以在“**应用程序类别**”文件夹的工作区使用分类列表查看新创建的类别。

如果要将应用程序类别导出为 KLC 文件，请右键单击类别名称，在菜单中选择**导出**，然后在打开的窗口中指定文件名并单击**保存**。

您也可以从**策略**文件夹创建应用程序类别。

*要从 Kaspersky Endpoint Security for Windows 策略的**属性**窗口创建应用程序类别：*

1. 在控制台树中，选择“**策略**”文件夹。
2. 在“**策略**”文件夹的工作区，选择您要为其创建类别的 Kaspersky Endpoint Security 策略。
3. 右击并选择“**属性**”。
4. 在打开的“**属性**”窗口中，在左侧“**区域**”窗格选择**安全控制 → 应用程序控制**。
5. 在“**应用程序控制**”区域的“**控制模式**”和“**操作**”下拉列表中选择允许列表或拒绝列表，然后单击“**添加**”按钮。
   包含类别列表的**应用程序控制规则**窗口打开。
6. 单击“**新建**”按钮。
7. 输入新策略名称并点击**确定**。
   新类别向导启动。
8. 在“**类别类型**”页面，选择用户类别类型：
   - **含有手动添加内容的类别**。指定用于分配可执行文件到到所创建类别的标准。
   - “**含有自动添加内容的类别**”。指定其可执行文件将被自动分配到所创建类别的文件夹。

     当创建自动添加内容的类别时，应用程序清查以下文件类型：EXE、COM、DLL、SYS、BAT、PS1、CMD、JS、VBS、REG、MSI、MSC、CPL、HTML、HTM、DRV、OCX 和 SCR。
   - **包含来自所选设备的可执行文件的类别**。指定其可执行文件将被自动分配到类别的设备。
9. 遵照向导的说明操作。

当向导结束时，自定义应用程序类别被创建。您可以在类别列表查看新创建的类别。

应用程序类别被包含在 Kaspersky Endpoint Security for Windows 中的应用程序控制组件使用。应用程序控制允许管理员对客户端设备上的应用程序启动施加限制—例如，限制某指定类别的应用程序的启动。

创建含有手动添加内容的应用程序类别

您可以指定一组条件作为要在组织中允许或阻止启动的可执行文件的模板。在对应于条件的可执行文件的基础上，您可以创建一个应用程序类别，并在“应用程序控制”组件配置中使用该应用程序类别。

要创建含有手动添加内容的应用程序类别：

1. 在控制台树的**高级 → 应用程序管理**文件夹中，选择“**应用程序类别**”子文件夹。
2. 单击“**新类别**”按钮。
   新类别向导启动。使用**下一步**按钮进行向导。
3. 在**类别类型**向导页面，选择**带有手动添加内容的类别**作为用户类别类型。
4. 在**输入应用程序类别名称**向导”页面上，输入新的应用程序类别名称。

5. 在“**配置包含应用程序到类别的条件**”页面，单击“**添加**”按钮。

6. 在下拉列表，指定相关设置：

- **从可执行文件列表**

  如果选中此选项，可以使用客户端设备上的可执行文件列表来选择可执行文件并将应用程序添加到类别。

- **从文件属性**

  如果选中此选项，您可以指定将要添加到用户应用程序类别的可执行文件的详细数据。

- **文件夹内文件元数据**

  指定客户端设备上包含可执行文件的文件夹。包含在指定文件夹的可执行文件中的元数据将被发送到管理服务器。包含相同元数据的可执行文件将被添加到用户应用程序类别。

- **文件夹中文件的校验和**

  如果选中了此选项，您可以在客户端设备上选择或创建文件夹。在指定文件夹里文件的 MD5 哈希将被发送到管理服务器。和指定文件夹里的文件具有相同哈希的应用程序被添加到用户应用程序类别。

- **文件夹中的文件证书**

  如果选中此选项，则可以指定客户端设备上包含了用证书签名的可执行文件的文件夹。可执行文件的证书被读取并添加到类别的条件中。已按照指定的证书签名的可执行文件将被添加到用户类别。

- **MSI 安装文件元数据**

  如果选中此选框，您可以指定 MSI 安装器文件作为添加应用程序到用户类别的条件。应用程序安装器元数据将被发送到管理服务器。与指定的 MSI 安装程序具有相同元数据的应用程序被添加到用户应用程序类别。

- **应用程序 MSI 安装程序中文件的校验和**

  如果选中此选框，您可以指定 MSI 安装器文件作为添加应用程序到用户类别的条件。应用程序安装程序的哈希将被发送到管理服务器。MSI 安装程序文件哈希与指定哈希相同的应用程序被添加到用户应用程序类别。

- **从 KL 类别**

  如果选中此选项，您可以指定卡巴斯基应用程序类别作为添加应用程序到用户类别的条件。来自指定 Kaspersky 类别的应用程序将被添加到用户应用程序类别。

- **指定应用程序路径(支持掩码)**

  如果选中此选项，您可以指定包含了要添加到用户应用程序类别的可执行文件的客户端设备上的文件或文件夹的路径。您可以使用正则表达式，如*C:\path_to_exe**，例如：*C:\Program Files\Internet Explorer**。

- **从存储库选择证书**

  如果选中此选项，则可以指定来自存储库的证书。类别条件仅匹配由指定证书签名的可执行文件。

  如果您创建并启动了清查任务并在 Kaspersky Endpoint Security 策略中勾选了**"关于已启动的应用程序"复选框**，则会将证书添加到存储库中。您可以执行以下两项操作。

- **驱动器类型**

  如果选中此选项，您可以指定应用程序在其上运行的媒体类型（任意设备或可移动驱动器）。在所选驱动类型上运行的应用程序被添加到用户应用程序类别。

7. 在**创建应用程序类别**向导页面上，单击**完成**按钮。

   Kaspersky Security Center 仅处理数字签名文件的元数据。不能基于没有数字签名的文件创建类别。

   当向导完成时，用户应用程序类别被创建，带有手动添加的内容。您可以在"**应用程序类别**"文件夹的工作区使用分类列表查看新创建的类别。

如果要将应用程序类别导出为 KLC 文件，请右键单击类别名称，在菜单中选择**导出**，然后在打开的窗口中指定文件名并单击**保存**。

创建包括选定设备中的可执行文件的应用程序类别

您可以将选定设备中的可执行文件用作要允许或阻止的可执行文件的模板。基于选定设备中的可执行文件，您可以创建一个应用程序类别，并在"应用程序控制"组件配置中使用该应用程序类别。

要从设备检索可执行文件列表：

1. 确保 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的策略已创建并处于活动状态。在策略中启用应用程序控制组件。
2. 获取客户端设备上存储的可执行文件列表。

要创建包括选定设备中的可执行文件的应用程序类别：

1. 在控制台树的**高级 → 应用程序管理**文件夹中，选择"**应用程序类别**"子文件夹。
2. 单击"**新类别**"按钮。

   新类别向导启动。使用**下一步**按钮进行向导。
3. 在 **类别类型**向导页面，选择**包括来自所选设备的可执行文件的类别**作为用户类别类型。
4. 在**输入应用程序类别名称**向导"页面上，输入新的应用程序类别名称。

5. 在**设置**向导页面上，单击**添加**按钮。

6. 选择一个或多个设备，其可执行文件将用于创建应用程序类别。

7. 指定下列设置：

- **哈希值计算算法**

  取决于您网络设备上安装的安全应用程序版本，您必须为此类别中的文件选择 Kaspersky Security Center 使用的哈希值算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

  未在 SHA256 算法中找到漏洞，它被视为现今最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支持 SHA256 计算。计算 MD5 哈希被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支持。

  为该类别中的文件选择任意 Kaspersky Security Center 使用的哈希值算法选项：

  - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，请选中“**SHA256**”复选框。对于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我们不建议您添加根据可执行文件 SHA256 哈希标准创建的类别。这将导致安全应用程序操作失败。此种情况下，您可以为类别中的文件使用 MD5 加密算法。

  - 如果您的网络上安装了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，请选择“**MD5 哈希**”。您不能添加基于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本的可执行文件的 MD5 校验和标准所创建的类别。此种情况下，您可以为类别中的文件使用 SHA256 加密算法。

  如果您网络上的不同设备同时使用早期和更新版本的 Kaspersky Endpoint Security 10，请同时选中**SHA256**复选框和**MD5 哈希**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)**”复选框被默认选中。

  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)复选框被默认清空。

- **与管理服务器存储库同步数据**

  如果您希望该管理服务器定期检查指定文件夹中的更改，则选择此选项。

  默认情况下已禁用该选项。

  如果启用此选项，请指定检查指定文件夹中的更改的周期（以小时为单位）。默认情况下，扫描间隔为 24 小时。

8. 在“**过滤器**”页面上，指定以下设置：

- **文件类型**

  在此区域中，可以指定用于创建应用程序类别的文件类型。

  所有文件。创建类别时会考虑所有文件。默认情况下已选定该选项。

  仅应用程序类别之外的文件。创建类别时仅考虑应用程序类别之外的文件。

- **文件夹**

  在此区域中，可以指定选定设备中的哪些文件夹包含用于创建应用程序类别的文件。

所有文件夹。创建类别时会考虑所有文件夹。默认情况下已选定该选项。

指定文件夹。创建类别时仅考虑指定文件夹。如果选择此选项，则必须指定文件夹的路径。

9. 在**创建应用程序类别**向导页面上，单击**完成**按钮。

当向导结束时，自定义应用程序类别被创建。您可以在"**应用程序类别**"文件夹的工作区使用分类列表查看新创建的类别。

如果要将应用程序类别导出为 KLC 文件，请右键单击类别名称，在菜单中选择**导出**，然后在打开的窗口中指定文件名并单击**保存**。

创建包括特定文件夹中的可执行文件的应用程序类别

您可以将选定文件夹中的可执行文件用作要在组织中允许或阻止的可执行文件的标准。在选定文件夹中的可执行文件的基础上，您可以创建一个应用程序类别，并在"应用程序控制"组件配置中使用该应用程序类别。

要创建包括特定文件夹中的可执行文件的应用程序类别：

1. 在控制台树的**高级 → 应用程序管理**文件夹中，选择"**应用程序类别**"子文件夹。
2. 单击"**新类别**"按钮。
   新类别向导启动。使用**下一步**按钮进行向导。
3. 在**类别类型**向导页面，选择**包括来自所选设备的可执行文件的类别**作为用户类别类型。
4. 在**输入应用程序类别名称**向导"页面上，输入新的应用程序类别名称。
5. 在**存储库文件夹**向导页面上，单击**浏览**按钮。
6. 指定将用于创建应用程序类别的可执行文件所在的文件夹。
7. 定义下列设置：

- **包含动态链接库 (DLL) 到该类别**

  应用程序类别包含动态链接库(DLL 格式的文件)，应用程序控制组件记录系统中运行的此类库的操作。包含 DLL 文件到类别可能降低 Kaspersky Security Center 的性能。

  默认情况下已清除该选框。

- **包含脚本数据到该类别**

  应用程序类别包含脚本数据，脚本不被 Web 威胁防护阻止。包含脚本数据到类别可能降低 Kaspersky Security Center 的性能。

  默认情况下已清除该选框。

- **哈希值计算算法**：**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)**

  取决于您网络设备上安装的安全应用程序版本，您必须为此类别中的文件选择 Kaspersky Security Center 使用的哈希值算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

  未在 SHA256 算法中找到漏洞，它被视为现今最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支持 SHA256 计算。计算 MD5 哈希被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支持。

  为该类别中的文件选择任意 Kaspersky Security Center 使用的哈希值算法选项：

  - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，请选中“**SHA256**”复选框。对于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我们不建议您添加根据可执行文件 SHA256 哈希标准创建的类别。这将导致安全应用程序操作失败。此种情况下，您可以为类别中的文件使用 MD5 加密算法。

  - 如果您的网络上安装了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，请选择“**MD5 哈希**”。您不能添加基于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本的可执行文件的 MD5 校验和标准所创建的类别。此种情况下，您可以为类别中的文件使用 SHA256 加密算法。

  如果您网络上的不同设备同时使用早期和更新版本的 Kaspersky Endpoint Security 10，请同时选中**SHA256**复选框和**MD5 哈希**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)**”复选框被默认选中。

  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)复选框被默认清空。

- **强制扫描文件夹以查找更改**

  如果启用此选项，应用程序会定期检查“类别内容添加”文件夹的任何变化。您可以在该选框旁的输入字段中指定检查频率（小时）。默认情况下，强制检查的时间间隔为 24 小时。

  如果禁用此选项，应用程序不会强制检查文件夹。如果文件被修改、添加或删除，服务器会尝试访问这些文件。

  默认情况下已禁用该选项。

8. 在**创建应用程序类别**向导页面上，单击**完成**按钮。

   当向导结束时，自定义应用程序类别被创建。您可以在“**应用程序类别**”文件夹的工作区使用分类列表查看新创建的类别。

如果要将应用程序类别导出为 KLC 文件，请右键单击类别名称，在菜单中选择**导出**，然后在打开的窗口中指定文件名并单击**保存**。

添加事件相关的可执行文件到应用程序类别

您可以添加“**应用程序启动被禁止**”和“**测试模式中的应用程序启动被禁止**”事件相关的可执行文件到现有手动添加内容的应用程序类别，或新应用程序类别。

要添加应用程序控制事件相关的可执行文件到应用程序类别：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。
3. 在“**事件**”选项卡，选择所需事件。
4. 在所选事件之一的上下文菜单中，选择“**添加到类别**”。
5. 在打开的“**对事件相关可执行文件所采取的操作**”窗口，指定相关设置：
   您可以选择以下之一：

   - **添加到新的应用程序类别**

     如果您需要创建新的应用程序类别，则选择该选项。
     单击“**确定**”按钮以启动新类别向导。当向导完成时，带有指定设置的类别被创建。
     默认情况下未选定该选项。

   - **添加到现有应用程序类别**

     如果您需要添加规则到现有应用程序类别则选择该选项。在应用程序类别列表中选择相关类别。
     默认情况下已选中该选项。

   在**规则类型**区域，选择以下设置之一：

   - **添加至类别**

     如果您需要添加规则到应用程序类别的条件则选择该选项。
     默认情况下已选中该选项。

   - **添加到排除的规则**

     如果您需要将规则添加到应用程序类别的排除项，则选择该选项。

   在**文件信息类型**区域，选择以下设置之一：

   - **证书详情（或没有证书的文件的 SHA256 哈希）**

     文件可能使用证书签署。多个文件可能使用相同的证书签署。例如，相同应用程序的不同版本可能使用相同的证书签署，或者相同供应商的多个不同应用程序可能使用相同证书签署。当您选择证书时，应用程序的多个版本或相同供应商的多个应用程序可能组成一个类别。
     每个文件都有单独的 SHA256 哈希。当您选择 SHA256 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。
     如果您要将可执行文件的证书详情（或者无证书文件的 SHA256 哈希函数）添加到类别规则，则选择该选项。
     默认情况下已选定该选项。

- **证书详情(无证书文件将被跳过)**

  文件可能使用证书签署。多个文件可能使用相同的证书签署。例如，相同应用程序的不同版本可能使用相同的证书签署，或者相同供应商的多个不同应用程序可能使用相同证书签署。当您选择证书时，应用程序的多个版本或相同供应商的多个应用程序可能组成一个类别。

  如果您要将可执行文件的证书详情添加到类别规则，则选择该选项。如果可执行文件没有证书，该文件将被跳过。该文件的信息将不被添加到类别。

- **仅 SHA256 (没有哈希的文件将被跳过)**

  每个文件都有单独的 SHA256 哈希。当您选择 SHA256 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

  如果您要仅添加可执行文件的 SHA256 哈希详情，则选择该选项。

- **仅 MD5(仅对 Kaspersky Endpoint Security 10 Service Pack 1 版本)**

  每个文件都有单独的 MD5 哈希。当您选择 MD5 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

  如果您要仅添加可执行文件的 MD5 哈希详情，则选择该选项。MD5 哈希码计算功能被 Kaspersky Endpoint Security 10 Service Pack 1 for Windows 和所有早期版本支持。

6. 单击“**确定**”。

配置应用程序在客户端设备上的启动管理

应用程序分类允许您优化在设备上运行的应用程序的管理。您可以创建应用程序类别并为策略配置应用程序控制，因此只有指定类别的应用程序将在应用策略的设备上启动。例如，您创建了包含 *Application_1*和 *Application_2*的类别。在您添加该类别到策略后，仅两个应用程序被允许在应用策略的设备上启动：*Application_1*和 *Application_2*。如果一个用户试图启动不在类别内的应用程序，例如 *Application_3*，该应用程序从启动中被阻止。用户被提示 *Application_3* 被阻止启动，根据应用程序控制规则。您可以基于不同标准从特定文件夹创建自动添加内容类别。此种情况下，文件被从指定文件夹自动添加到类别。应用程序可执行文件被复制到指定文件夹并被自动处理；它们的度量数据被添加到类别。

若要配置应用程序在客户端设备上的启动管理，请执行以下操作：

1. 在控制台树的**高级** → **应用程序管理**文件夹中，选择“**应用程序类别**”子文件夹。

2. 在“**应用程序类别**”文件夹的工作区中创建启动应用程序时要进行管理的应用程序的类别。

3. 在“**受管理设备**”文件夹的“**策略**”选项卡中单击“**新策略**”按钮为 Kaspersky Endpoint Security for Windows 创建新策略，并按照向导说明进行操作。

   如果此类策略已经存在，您可以跳过该步骤。您可以通过策略设置在指定类别中配置应用程序启动管理。新创建的策略显示在“**策略**”选项卡的“**受管理设备**”文件夹中。

4. 从 Kaspersky Endpoint Security for Windows 策略的上下文菜单中选择“**属性**”。

   屏幕上将打开 Kaspersky Endpoint Security for Windows 策略的属性窗口。

5. 在 Kaspersky Endpoint Security for Windows 策略属性窗口中，在“**安全控制** → **应用程序控制**”区域选择“**应用程序控制**”复选框。

6. 单击“**添加**”按钮。

   “**应用程序控制规则**”窗口将开启。

7. 在“**应用程序控制规则**”窗口内，在“**类别**”下拉列表中选择启动规则涵盖的应用程序类别。为所选应用程序类别配置启动规则。

   对于 Kaspersky Endpoint Security 10 Service Pack 2 和更新版本，如果类别基于可执行文件的 MD5 哈希而创建则不被显示。

   对于 Kaspersky Endpoint Security 10 Service Pack 2 早期版本，我们不建议您添加根据可执行文件 SHA256 哈希标准创建的类别。这可能导致应用程序失败。

   配置控制规则的详细步骤提供在 Kaspersky Endpoint Security for Windows 在线帮助。

8. 单击“**确定**”。

应用程序将在根据您创建的规则的指定类别的设备上运行。新创建的规则将显示在 Kaspersky Endpoint Security for Windows 策略属性窗口中的**应用程序控制**区域中。

查看应用到可执行文件的启动规则的统计分析的结果

要查看关于禁止用户运行的可执行文件信息：

1. 在控制台树的“**受管理设备**”文件夹中，选择“**策略**”选项卡。

2. 从 Kaspersky Endpoint Security for Windows 策略的上下文菜单中选择“**属性**”。

   应用程序策略的属性窗口打开。

3. 在“**区域**”窗格，选择“**安全控制**”，然后选择“**应用程序控制**”子区域。

4. 点击**静态分析**按钮。

   访问权限列表分析窗口打开。在窗口左侧，基于活动目录数据的用户列表被显示。

5. 从下拉列表选择用户。

   窗口右侧显示分配给此用户的程序类别。

6. 要查看禁止用户运行的可执行文件，请在“**访问权限列表分析**”窗口单击“**查看文件**”按钮。

   显示禁止的可执行文件列表的窗口打开。

7. 要查看某类别的可执行文件列表，选中一个应用程序类别并单击“**查看类别中的文件**”按钮。

   这将打开窗口显示包含在应用程序类别中的可执行文件列表。

查看应用程序注册表

Kaspersky Security Center 清查所有安装在受管理设备上的软件。

网络代理编辑安装在Windows 或 Linux 设备上的应用程序列表，并把该列表传给管理服务器。对于基于 Windows 的客户端设备，网络代理从 Windows 注册表接收有关已安装应用程序的大部分信息。对于基于 Linux 的客户端设备，包管理器向网络代理提供有关已安装应用程序的信息。

要查看客户端设备上安装的应用程序注册表项，

在控制台树的**高级** → **应用程序管理**文件夹中，选择“**应用程序注册表**”子文件夹。

“**应用程序注册表**”文件夹的工作区显示安装到客户端设备和管理服务器上的应用程序列表。

您可以通过打开其上下文菜单并选择**属性**来查看应用程序详情。应用程序属性窗口会打开，其中显示应用程序详情、其可执行文件的信息以及安装此应用程序的设备列表。

在列表中任意应用程序的上下文菜单中，您可以：

- 添加该应用程序到应用程序类别。
- 分配标签给应用程序。
- 导出应用程序列表到 CSV 文件或 TXT 文件。
- 查看应用程序属性，例如，供应商名称、版本号、可执行文件列表、安装了该应用程序的设备列表、可用软件更新列表或检测到的软件漏洞列表。

要查看满足指定标准的应用程序，可以使用“**应用程序注册表**”文件夹工作区中的过滤字段。

在所选设备的属性窗口的“**应用程序注册表**”区域，您可以查看安装在设备上的应用程序的列表。

生成已安装的应用程序报告

在“**应用程序注册表**”工作区中，您也可以单击“**查看已安装的应用程序报告**”按钮生成包含已安装应用程序详细统计信息的报告，其中包括安装了每个应用程序的设备数量。在**已安装的应用程序报告**页面中打开的报告包含 Kaspersky 应用程序和第三方软件的信息。如果您仅想要安装在客户端设备上的 Kaspersky 应用程序的信息，在**概要**列表，选择 AO Kaspersky Lab。

连接至从属和虚拟管理服务器的设备已安装 Kaspersky 应用程序和第三方软件的信息也被存储在主管理服务器的应用程序注册表中。在您从从属和虚拟管理服务器添加数据后，单击“**查看已安装的应用程序报告**”按钮，在打开的“**已安装的应用程序报告**”页面，您可以查看该信息。

要从从属和虚拟管理服务器添加信息到已安装的应用程序报告：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 在“**报告**”选项卡，选择“**已安装的应用程序报告**”。
4. 从该报告的上下文菜单中选择“**属性**”。
   此时会打开“**属性**”:“**已安装的应用程序报告**”窗口。
5. 在“**管理服务器层级**”区域，选择“**包含来自从属和虚拟管理服务器的数据**”复选框。
6. 单击“**确定**”。

从属和虚拟管理服务器的信息将包含在“**已安装的应用程序报告**”中。

更改软件清查开始时间

Kaspersky Security Center 清查所有安装在 Windows 的受管客户端设备上的软件。

网络代理编辑安装在设备上的应用程序列表，并把该列表传给管理服务器。网络代理从 Windows 注册表自动接收已安装应用程序的信息。

要保存设备资源，网络代理默认在服务启动后 10 分钟便开始接收已安装应用程序的信息。

要更改网络代理服务在设备上运行后软件清查开始的时间：

1. 打开安装网络代理的设备的系统注册表（例如，在本地**开始 → 运行**菜单中使用 regedit 命令）。
2. 转至以下分支：
   - 对于 32 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - 对于 64 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. 对于 KLINV_INV_COLLECTOR_START_DELAY_SEC 注册表键，设置所需的值。
   默认值是 600 秒。
4. 重启网络代理服务。

网络代理服务运行后的软件清查开始时间已更改。

关于第三方应用程序的授权许可密钥管理

Kaspersky Security Center 允许您跟踪受管理设备上安装的第三方应用程序的授权许可密钥使用情况。可以跟踪授权许可密钥使用情况的应用程序列表来自应用程序注册表。对于每个授权许可密钥，都可以指定并跟踪违反以下限制的情况：

- 可以使用该授权许可密钥安装应用程序的设备数量
- 授权许可密钥的到期日期

Kaspersky Security Center 不会检查您是否指定真实的授权许可密钥。您只能跟踪您指定的限制。如果违反了您对授权许可密钥施加的限制之一，管理服务器将注册“信息”、“警告”或“功能失败”事件。

授权许可密钥绑定到应用程序组。应用程序组是一组根据一个或多个条件组合的第三方应用程序。您可以按应用程序的名称、版本、供应商和标签来定义应用程序。如果满足至少一个条件，应用程序即添加到组中。对于每个应用程序组，都可以绑定多个授权许可密钥，但每个授权许可密钥只能绑定到一个应用程序组。

还有一个可以用来跟踪授权许可密钥使用情况的工具是已授权应用程序组的状态报告。此报告提供有关已授权应用程序组当前状态的信息，包括：

- 每个应用程序组的授权许可密钥安装数量
- 使用中的授权许可密钥和空闲的授权许可密钥数量
- 受管理设备上安装的已授权应用程序详细列表

第三方应用程序的授权许可密钥管理工具位于“**第三方授权许可使用**”子文件夹（“**高级**”→“**应用程序管理**”→“**第三方授权许可使用**”）。在此子文件夹中，可以创建应用程序组、添加授权许可密钥并生成已授权应用程序组的状态报告。

仅当在“**配置界面**”窗口中启用“漏洞和补丁管理”选项后，第三方应用程序授权许可密钥管理工具才可用。

创建授权的应用程序组

要创建授权的应用程序组：

1. 在控制台树的“**高级**”→“**应用程序管理**”文件夹中，选择“**第三方授权许可使用**”子文件夹。
2. 点击“**添加已授权应用程序组**”按钮运行“已授权应用程序组添加向导”。
   已授权应用程序组添加向导 启动。
3. 在“**有关已授权应用程序组的详情**”步骤，指定要包括在应用程序组中的应用程序：
   - **已授权应用程序组的名称**
   - **跟踪限制违规**

     如果违反了您对应用程序组的授权许可密钥施加的限制之一，管理服务器将注册“信息”、“警告”或“功能失败”事件：

     - 信息事件：**已授权应用程序组之一的安装即将超过限制(已经使用 95% 以上)**
     - 警告事件：**已授权应用程序组之一的安装即将超过限制**
     - 功能失败事件：**已授权应用程序组之一的安装已超过限制**
       满足指定条件时，仅注册一次事件。下一次，只有在安装数量恢复到正常水平，并且该事件再次发生，才会注册同一事件。一个事件每小时不能注册多次。
   - **将检测到的应用程序添加至该已授权应用程序组的标准**

     指定条件以定义要将哪些应用程序包含在应用程序组中。您可以按应用程序的名称、版本、供应商和标签来定义应用程序。您必须至少指定一个条件。如果满足至少一个条件，应用程序即添加到组中。

4. 在“**输入现存授权许可密钥的数据**”步骤，指定要跟踪的授权许可密钥。选择“**如果授权许可超过限制，将会被控制**”选项，然后添加授权许可密钥：

   a. 单击“**添加**”按钮。

   b. 选择要添加的授权许可密钥，然后单击“**确定**”按钮。如果未列出所需授权许可密钥，请单击“**添加**”按钮，然后指定授权许可密钥属性。

5. 在“**添加已授权应用程序组**”选项卡上，单击“**完成**”按钮。

已授权应用程序组即创建并显示在“**第三方授权许可使用**”文件夹中。

管理已授权应用程序组的授权许可密钥

要创建已授权应用程序组的授权许可密钥，请执行以下操作：

1. 在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**第三方授权许可使用**”子文件夹。
2. 在**第三方授权许可使用**文件夹的工作区中，单击**管理已授权应用程序的授权许可密钥**按钮。
   已授权应用程序的授权许可密钥管理窗口打开。
3. 在“**已授权应用程序的授权许可密钥管理**”窗口中，单击“**添加**”按钮。
   “**授权许可密钥**”窗口打开。
4. 在“**授权许可密钥**”窗口中，指定授权许可密钥的属性和授权许可密钥对已授权应用程序组实施的限制。
   - **名称**。授权许可密钥名称。
   - **注释**。关于选定授权许可密钥的备注。
   - **最大计算机数**。可以使用该授权许可密钥安装应用程序的设备数量。
   - **过期**。授权许可密钥的到期日期。

创建的授权许可密钥显示在“**已授权应用程序的授权许可密钥管理**”窗口。

要将授权许可密钥应用到已授权应用程序组，请执行以下操作：

1. 在控制台树的“**高级**” → “**应用程序管理**”文件夹中，选择“**第三方授权许可使用**”子文件夹。
2. 在“**第三方授权许可使用**”文件夹中，选择您要应用授权许可密钥的已授权应用程序组。
3. 在授权应用程序组的上下文菜单中选择**属性**。
   这将打开授权应用程序组的“属性”窗口。
4. 在已授权应用程序组的属性窗口中的“**授权许可密钥**”区域中选择“**如果授权许可超过限制，将会被控制**”。
5. 单击“**添加**”按钮。
   此时将打开**选择授权许可密钥**窗口。

6. 在**选择授权许可密钥**窗口中，选择您要应用至已授权应用程序组的授权许可密钥。

7. 单击“**确定**”。

授权许可密钥中指定的、对已授权应用程序组施加的限制也将应用到所选的已授权应用程序组。

可执行文件存储库

您可以获取受管理设备上存储的可执行文件列表。要清查可执行文件，必须创建清查任务。

清查可执行文件的功能可用于以下应用程序：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent 和更高版本

从单个设备接收的可执行文件数量不能超过 150,000。达到此限制后，Kaspersky Security Center 无法接收新文件。

在开始之前，请在 Kaspersky Endpoint Security 策略和网络代理策略中启用有关应用程序启动的通知，以便可以将数据传输到管理服务器。

要启用有关应用程序启动的通知：

- 打开 Kaspersky Endpoint Security 策略设置并执行以下操作：
  1. 转到“**常规设置 → 报告和存储**”。
  2. 在“**到管理服务器的数据传输**”区域中，选中“**关于已启动的应用程序**”复选框。
  3. 保存更改。
- 打开网络代理策略设置并执行以下操作：
  1. 转到“**存储库**”区域。
  2. 选中“**已安装应用程序详情**”复选框。
  3. 保存更改。

要在客户端设备上为可执行文件创建清查任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在“**任务**”文件夹的工作区，单击“**新任务**”按钮。
   “新任务向导”启动。

3. 在向导的“**选择任务类型**”窗口，选择“**Kaspersky Endpoint Security**”做为任务类型，然后选择“**清单**”做为任务子类型，并单击**下一步**。

4. 遵照剩余的向导说明。

向导完成后，Kaspersky Endpoint Security 的清查任务已创建。新创建的任务显示在“**任务**”文件夹工作区的任务列表。

清查过程中在设备上检测到的可执行文件列表将显示在“**可执行文件**”文件夹的工作区。

清查过程中，应用程序检测以下格式的可执行文件：MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR 和 HTML 文件。

查看可执行文件信息

要查看在客户端设备上检测到的可执行文件列表，

在控制台树的“**应用程序管理**”文件夹中，选择“**可执行文件**”子文件夹。

“**可执行文件**”文件夹工作区显示了一直在设备上运行的或者在运行 Kaspersky Endpoint Security for Windows 的清查任务时检测到的可执行文件列表。

要查看满足指定标准的可执行文件的详细信息，您可以使用过滤。

要查看可执行文件的属性，

从文件的上下文菜单中，选择“**属性**”。

显示可执行文件信息的窗口将开启，该窗口同时包含了在其上发现可执行文件的设备列表。

监控和报告

该部分描述了 Kaspersky Security Center 的监控和报告功能。这些功能给您一个基础架构、保护状态和统计信息的总览。

在 Kaspersky Security Center 部署之后或操作过程中，您可以配置监控和报告功能以适应您的需要。

- **信号灯**

  管理控制台允许您通过检查信号灯快速评估当前 Kaspersky Security Center 状态和受管理设备。

- **统计**

  保护系统和受管理设备状态的统计信息显示在可以自定义的信息窗格中。

- **报告**

  报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

- **事件**

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

您可以基于 Kaspersky Security Center Web Console 界面上可以配置的设置创建和查看用户定义的事件分类。

方案：监控和报告

该部分提供在 Kaspersky Security Center 中配置监控和报告功能的方案。

先决条件

在您部署 Kaspersky Security Center 到组织网络中后，您可以开始监控它并生成其功能报告。

阶段

组织网络中的监控和报告分步骤进行：

1. **配置设备状态切换**

   熟悉根据特定条件定义设备状态分配的设置。通过更改这些设置，您可以更改带有*严重*或*警告*重要级别的设备数量。

   在配置设备状态切换时，请确保新设置不与您组织的信息安全策略冲突，并且您可以及时对组织网络中的重要安全事件做出反应。

2. **配置客户端设备上的事件通知**

   根据您组织的需求配置客户端设备上的事件通知（通过邮件、SMS 或运行可执行文件）。

3. **更改您的安全网络对病毒爆发事件的响应**

   要调整网络对新事件的响应，您可以在管理服务器属性中更改特定阈值。您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。

4. **管理统计信息**

   根据您组织的需求配置统计信息的显示。

5. **查看您组织网络的安全状态**

   要查看您组织网络的安全状态，可以执行以下任一操作：

   - 在**管理服务器**节点的工作区中的“**统计**”选项卡上，打开“**保护状态**”二级选项卡（页面），然后查看“**实时保护状态**”信息面板
   - 生成并查看**保护状态报告**
   - 生成并查看**错误报告**

6 定位不被保护的客户端设备

要查找不受保护的客户端设备，请转到**管理服务器**节点的工作区，在“**统计**”选项卡上，打开“**保护状态**”二级选项卡（页面），然后查看“**在网络中发现新设备的历史**”信息面板。您还可以生成并查看**保护部署报告**。

7 检查客户端设备保护

要检查客户端设备的保护，请转到**管理服务器**节点的工作区，在“**统计**”选项卡上，打开“**部署**”或“**威胁统计**”二级选项卡（页面），然后查看相关信息面板。您还可以启动并查看“**严重事件**”事件分类。

8 评估和限制数据库上的事件负载

受管理应用程序操作相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

要评估数据库上的事件负载，请计算数据库空间。您还可以限制最大事件数量以避免数据库溢出。

9 查看授权许可信息

要查看授权许可信息，请转到**管理服务器**节点的工作区，在“**统计**”选项卡上，打开“**部署**”二级选项卡（页面），然后查看“**授权许可密钥使用**”信息面板。您还可以生成并查看**授权许可密钥使用报告**。

结果

完成方案后，您被通知您组织网络的保护，因此可以为进一步保护计划操作。

在管理控制台中监控信号灯和记录的事件

管理控制台允许您通过检查信号灯快速评估当前 Kaspersky Security Center 状态和受管理设备。信号灯显示在“**管理服务器**”节点工作区的“**监控**”选项卡。选项卡提供了带有信号灯的六个信息窗格和记录。信号灯是面板左侧的彩色栏。每个带有信号灯的窗格对应于 Kaspersky Security Center 的特定功能范围(参见下表)。

管理控制台中信号灯覆盖的范围

窗格名称	信号灯范围
部署	在组织网络设备上安装网络代理和安全应用程序
管理方案	管理组结构。网络扫描。设备移动规则
保护设置	安全应用程序功能：保护状态、恶意软件扫描
更新	更新和补丁
监控	保护状态
管理服务器	管理服务器功能和属性

每个信号灯可以变换五种颜色(参见下表)。信号灯的颜色取决于 Kaspersky Security Center 的当前状态和记录的事件。

信号灯的颜色码

状态	信号灯颜色	信号灯颜色意义
信息	绿色	不需要管理员介入。
警告	黄色	需要管理员介入。
严重	红色	发生了严重问题。需要管理员介入以解决。
信息	淡蓝色	与受管理设备的潜在或实际威胁无关的事件被记录。
信息	灰色	事件详情不可用或未获取。

管理员的目标是保持“**监控**”选项卡的所有信息窗格上的信号灯是绿色的。

信息窗格还显示影响信号灯和 Kaspersky Security Center 的状态的记录事件（请见下表）。

所记录事件的名称、描述和信号灯颜色

信号灯颜色	事件类型显示名称	事件类型	描述
红色	**%1 台设备上的授权许可已过期**	IDS_AK_STATUS_LIC_EXPAIRED	当商业授权许可已到期时，会发生此类事件。 Kaspersky Security Center 每天检查一次设备上的授权许可是否到期。 当商业授权许可到期时，Kaspersky Security Center 仅提供基本功能。 要继续使用 Kaspersky Security Center，请续费您的商业授权许可。
红色	**安全应用程序没有运行：%1 台设备**	IDS_AK_STATUS_AV_NOT_RUNNING	当设备上安装的应用程序不运行时会发生这种类型的事件。 请确保 Kaspersky Endpoint Security 在设备上运行。
红色	**已禁用保护：%1 台设备**	IDS_AK_STATUS_RTP_NOT_RUNNING	当设备上的安全应用程序已被禁用大于指定的时间段时会发生这种类型的事件。 检查设备上的实时保护当前状态，确保您需要的所有保护组件已启用。
红色	**在设备上检测到软件漏洞**	IDS_AK_STATUS_VULNERABILITIES_FOUND	当*查找漏洞和所需更新*任务在设备上安装的应用程序中检测到指定严重级别的漏洞时，会发生这种类型的事件。 在**应用程序管理**文件夹的**软件更新**子文件夹中检查可用更新列表。该文件夹包含了管理服务器检索的可以被分发到设备的 Microsoft 应用程序和其他软件厂商产品的更新列表。 查看各种更新的信息后，请在设备上安装它们。
红色	**管理服务器上注册了严重事件**	IDS_AK_STATUS_EVENTS_OCCURED	当检测到管理服务器严重事件时会发生这种类型的事件。 检查存储在管理服务器上的事件列表，然后逐个修复严重事件。
红色	**管理服务器上记录了错误事件**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	当管理服务器端记录了意外错误时会发生这种类型的事件。 检查存储在管理服务器上的事件列表，然后逐个修复错误。
红色	**失去与 %1 台设备的连接**	IDS_AK_STATUS_ADM_LOST_CONTROL1	当管理服务器和设备之间的连接丢失时会发生这种类型的事件。 请查看连接设备列表并尝试重新连接它们。
红色	**%1 台设备已长时间未连接到管理服务器**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	当由于设备关闭，设备在指定时间段内未连接到管理服务器时会发生这种类型的事件。 请确保设备已开启且网路代理在运行。
红色	**有 %1 台设备状态不正常**	IDS_AK_STATUS_HOST_NOT_OK	当连接到管理服务器的设备的状态由 *OK* 变为 *严重* 或者 *警告* 时会发生这种类型的事件。 您可以使用Kaspersky Security Center 远程诊断工具解决问题。
红色	**数据库过期：%1 台设备**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	当设备上的反病毒数据库未在指定时间段内更新时会发生这种类型的事件。 按照指示更新卡巴斯基数据库。
红色	**Windows Update 更新检查长时间没有运行的设备：%1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	当“*执行 Windows 更新同步*”任务在指定时间段内未运行时会发生这种类型的事件。 按照指示使用管理服务器从 Windows 更新同步更新。
红色	**Kaspersky Security Center 的 %1 个插件必须安装**	IDS_AK_STATUS_PLUGINS_REQUIRED2	当您需要为卡巴斯基应用程序安装其它插件时会发生这种类型的事件。 从卡巴斯基技术支持网页 下载和安装所需的卡巴斯基应用程序管理插件。

使用报告、统计和通知

本部分将介绍如何在 Kaspersky Security Center 中处理报告、统计信息及事件和设备选项，以及如何配置管理服务器通知。

使用报告

Kaspersky Security Center 的报告包含受管理设备状态的信息。报告根据管理服务器上存储的信息生成。您可以为以下类型的对象创建报告：

- 为根据指定设置创建的设备分类。
- 为管理组。
- 为不同管理组的特定设备。
- 为网络中的所有设备（对部署报告可用）。

程序有标准报告模板分类。也可以创建自定义报告模板。报告将显示在主应用程序窗口，控制台树的“**管理服务器**”文件夹。

创建报告模板

要创建报告模板：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 单击“**新建报告模板**”按钮。

   程序将启动“新报告模板向导”。遵照向导的说明操作。

当向导完成运行后，新建的报告模板将被添加到控制台树的**管理服务器**文件夹中。您可以使用此模板来生成和查看报告。

查看和编辑报告模板属性

您可以查看和编辑报告模板的基本属性，例如，报告模板名称或显示在报告中的字段。

要查看和编辑报告模板属性：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 在报告模板列表，选择所需报告模板。

4. 在所选报告模板的上下文菜单中选择“**属性**”。
   另外，您可以先生成报告，然后单击“**打开报告模板属性**”按钮或“**配置报告列**”按钮。

5. 在打开的窗口中，编辑报告模板属性。每个报告的属性可能仅包含若干以下描述的部分。

- **常规**区域：
  - 报告模板名称
  - **显示条目的最大数量**

    如果启用该选项，显示在表格中的带有详细报告数据的条目数量不超过指定值。

    报告条目首先根据报告模板属性的**字段 → 详细资料字段**区域中指定的规则进行排序，然后仅保存第一个结果条目。带有详细报告数据的表头展示显示的条目数量和匹配其他报告模板设置的可用条目总数。

    如果禁用该选项，带有详细报告数据的表显示所有可用条目。我们不建议您禁用该选项。限制显示的报告条目数量降低数据库管理系统 (DBMS) 负载，也降低生成和导出报告的所需时间。一些报告包含太多条目。如果是这样，您可能难于阅读和分析所有。而且，您的设备可能在生成此报告时内存不够，进而您将无法查看报告。

    默认情况下已启用该选项。默认值是 1000。

  - **打印版本**

    报告输出被优化以用于打印：在一些值之间被添加空格以方便阅读。

    默认情况下已启用该选项。

- **字段**区域。
  选择在报告中要显示的字段，和字段顺序，并配置报告信息是否被存储和按照字段过滤。
- **时间间隔**区域。
  修改报告间隔。有以下可用值：
  - 在两个指定日期之间
  - 从指定日期到报告创建日期
  - 从报告创建日期减去指定天数，到报告创建日期
- **组**、**Device selection**或**Devices**区域。
  更改创建报告的客户端设备集。仅其中一个区域可能被展示，取决于报告模板创建过程中指定的设置。
- “**设置**”区域。
  更改报告设置。精确设置集合取决于特定报告。
- **安全性**区域。**从管理服务器继承设置**

  如果启用该选项，报告的安全设置从管理服务器继承。

  如果禁用该选项，您可以配置报告的安全设置。您可以分配角色到用户或用户组或分配权限到用户或用户组，如报告中所应用。

默认情况下已启用该选项。

如果选中了界面设置窗口中的“**显示安全设置区域**”复选框，则“**安全性**”区域可用。

- **管理服务器层级**区域：
  - **包含来自从属和虚拟管理服务器的数据**

    如果启用该选项，报告包含属于创建模板的管理服务器的从属和虚拟管理服务器的信息。

    如果您要仅从当前管理服务器查看数据，禁用该选项。

    默认情况下已启用该选项。

  - **嵌套级别**

    报告包含位于当前管理服务器下小于或等于指定嵌套级别的从属和虚拟管理服务器的数据。

    默认值是 1。如果您必须从树中位于低级别的从属管理服务器接收信息，您可能要更改该值。

  - **数据等待间隔(分钟)**

    在生成报告之前，创建报告模板的管理服务器等待从属管理服务器的数据指定分钟数。如果在该时间段后未从从属管理服务器接收到数据，报告依然运行。除了实际数据，报告也显示从缓存接收的数据（如果**缓存从属管理服务器数据**选项被启用）或**N/A**（不可用）。

    默认值是 5 分钟。

  - **缓存从属管理服务器数据**

    从属管理服务器定期传输数据到创建报告模板的管理服务器。传输的数据存储在缓存。

    如果在生成报告时当前管理服务器无法从从属管理服务器接收数据，报告显示从缓存接收的数据。数据传输到缓存的日期也被显示。

    启用该选项允许您查看从属管理服务器信息，即便实时数据无法被获取。然而，所显示数据可能过期。

    默认情况下已禁用该选项。

  - **缓存更新频率(小时)**

    从属管理服务器定期传输数据到创建报告模板的管理服务器。您可以指定此时间段（以小时为单位）。如果指定 0 小时，则仅在生成报告时传输数据。

    默认值是 0。

  - **从从属管理服务器传输详细信息**

    在生成的报告中，带有详细报告数据的表格包含创建报告模板的管理服务器的从属管理服务器的数据。

    启用该选项减慢报告生成并增加管理服务器之间的流量。然而，您可以在一个报告中查看所有数据。

除了启用该选项，您可能想分析详细报告数据以检测故障从属管理服务器，然后仅为该故障管理服务器生成相同报告。

默认情况下已禁用该选项。

报告模板中的扩展过滤器格式

在 Kaspersky Security Center 15.1 中，您可以将扩展过滤器格式应用于报告模板。与默认格式相比，扩展过滤器格式提供了更大的灵活性。您可以使用一组过滤器来创建复杂的过滤条件，这些过滤器将在创建报告期间通过 OR 逻辑运算符应用于报告，如下所示：

Filter[1](Field[1] AND Field[2]...AND Field[n]) OR Filter[2](Field[1] AND Field[2]...AND Field[n]) OR...Filter[n](Field[1] AND Field[2]...AND Field[n])

此外，使用扩展过滤器格式，可以为过滤器中的特定字段设置相对时间格式的时间间隔值（例如，通过使用"过去 N 天"条件）。可用性和时间间隔条件集取决于报告模板的类型。

将过滤器转换为扩展格式

仅 Kaspersky Security Center 12 和更高版本支持报告模板的扩展过滤器格式。将默认过滤器转换为扩展格式后，报告模板将与网络中安装了 Kaspersky Security Center 早期版本的管理服务器不兼容。该报告不会收到来自这些管理服务器的信息。

要将报告模板默认过滤器转换为扩展格式，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择"**报告**"选项卡。
3. 在报告模板列表，选择所需报告模板。
4. 在所选报告模板的上下文菜单中选择"**属性**"。
5. 在打开的属性窗口中，选择"**字段**"区域。
6. 在"**详细资料字段**"选项卡中，单击"**转换过滤器**"链接。
7. 在打开的窗口中，单击**确定**按钮。

   对报告模板应用转换为扩展过滤器格式后，这一操作是不可逆的。如果您不小心单击了"**转换过滤器**"链接，则可以通过单击报告模板属性窗口中的"**取消**"按钮来取消更改。

8. 要应用更改，请单击"**确定**"按钮以关闭报告模板属性窗口。

   当报告模板属性窗口再次打开时，将显示新的可用"**过滤器**"区域。在该区域，您可以配置扩展过滤器。

配置扩展过滤器

要在报告模板属性中配置扩展过滤器，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 在报告模板列表中，选择先前转换为扩展过滤器格式的报告模板。
4. 在所选报告模板的上下文菜单中选择“**属性**”。
5. 在打开的属性窗口中，选择“**过滤器**”子区域。
   如果报告模板先前未转换为扩展过滤器格式，则不会显示“**过滤器**”区域。
   在报告模板属性窗口的“**过滤器**”区域，您可以查看和修改应用于报告的过滤器列表。列表中的每个过滤器都有一个唯一的名称，并代表报告中相应字段的一组过滤器。
6. 以下列方式之一打开过滤器设置窗口：
   - 要创建新的过滤器，请单击“**添加**”按钮。
   - 要修改现有过滤器，请选择所需的过滤器，然后单击“**修改**”按钮。
7. 在打开的窗口中，选择并指定过滤器必填字段的值。
8. 单击**确定**按钮以保存更改并关闭窗口。
   如果正在创建新的过滤器，则在单击**确定**按钮之前，必须在**过滤器名称**字段中指定过滤器名称。
9. 单击“**确定**”按钮，关闭报告模板属性窗口。
   报告模板中的扩展过滤器已配置完毕。现在，您可以使用此报告模板创建报告。

创建和浏览报告

要创建和查看报告，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 在报告模板列表中，双击您需要的报告模板。
   所选模板的报告被显示。

该报告将显示下列数据：

- 报告名称和类型、简要描述和报告时间段，以及为哪个设备组生成该报告的相关信息。
- 图表显示最有代表性的报告数据。
- 带有计算好的报告指示器的加固表格。
- 带有详细报告数据的表格。

保存报告

要保存生成的报告，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 在报告模板列表中，选择您需要的报告模板。
4. 在所选报告模板的上下文菜单中选择“**保存**”。

   将启动“报告保存向导”。遵照向导的说明操作。

向导结束后，程序将打开您保存报告文件的文件夹。

> 当您将报告保存为 XLS 文件时，所有相关图像（例如徽标和数据报）都被保存为单独文件。

创建报告发送任务

报告可以被发送。Kaspersky Security Center 中的报告传送由报告传送任务完成。

要创建单个报告传送任务，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 在报告模板列表中，选择您需要的报告模板。
4. 在所选报告模板的上下文菜单中选择“**传送报告**”。

   报告传送任务创建向导启动。遵照向导的说明操作。

要创建多个报告的传送任务，请执行以下操作：

1. 在控制台树，在所需管理服务器名称节点下，选择“**任务**”文件夹。
2. 在“**任务**”文件夹的工作区，单击“**创建任务**”按钮。

   “新任务向导”启动。遵照向导的说明操作。

   新创建的报告传送任务显示在控制台树的“**任务**”文件夹。

> 如果在 Kaspersky Security Center 安装期间指定了电子邮件设置，程序将会自动创建报告传送任务。

步骤 1：选择任务类型

在“**选择任务类型**”窗口，在任务列表中选择“**传送报告**”作为任务类型。

点击**下一步**以继续到下一步。

步骤 2：选择报告类型

在“**选择报告类型**”窗口，在任务创建模板列表，选择报告类型。

点击**下一步**以继续到下一步。

步骤 3：报告操作

在**应用到报告的操作**窗口中，指定以下设置：

- **通过邮件发送报告**

  如果启用此选项，应用程序将通过电子邮件发送生成的报告。

  您可以单击“**邮件通知设置**”链接，配置通过电子邮件发送的报告。如果启用此选项，则该链接可用。

  如果禁用此选项，则应用程序将报告保存到指定文件夹进行存储。

  默认情况下已禁用该选项。

- **保存报告到共享文件夹**

  如果启用此选项，则应用程序将报告保存到该复选框下的字段中指定的文件夹。要保存报告到共享文件夹，指定文件夹的 UNC 路径。此种情况下，在**选择账户以运行任务**窗口，您必须指定用户账户和密码以访问该文件夹。

  如果禁用此选项，则应用程序不将报告保存到文件夹，而是通过电子邮件发送。

  默认情况下已禁用该选项。

- **覆盖相同类型的旧报告**

  如果启用此选项，每次任务启动时的新报告文件会覆盖之前任务启动时保存在报告文件夹中的文件。

  如果禁用此选项，则将不会覆盖报告文件。每次任务启动时，新的报告文件都将保存在报告文件夹中。

  如果选择“**保存报告到文件夹**”，则该复选框可用。

  默认情况下已禁用该选项。

- **指定账户以访问共享文件夹**

  如果启用此选项，您可以指定保存报告到文件夹的账户。如果共享文件夹的 UNC 路径被指定为**应用到报告的操作**窗口的**保存报告到文件夹**设置，您必须指定用户账户和密码以访问该文件夹。

  如果禁用此选项，报告将存储到管理服务器账户下的文件夹。

  如果选择“**保存报告到文件夹**”，则该复选框可用。

  默认情况下已禁用该选项。

当您将报告保存或发送为 XLS 文件时，所有相关图像（例如徽标和数据报）都被保存为单独文件。

点击**下一步**以继续到下一步。

步骤 4：选择账户以移动任务

在“**选择账户以运行任务**”窗口，您可以指定在运行任务时使用哪些账户。您可以选择以下选项之一：

- **默认账户**

  在与执行该任务的应用程序相同的账户下运行该任务。

  默认情况下已选定该选项。

- **指定账户**

  填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - **账户**

    运行该任务的账户。

  - **密码**

    任务运行时使用的账户的密码。

点击**下一步**以继续到下一步。

步骤 5：配置任务计划

在“**配置任务计划**”向导页面，您可以为任务启动创建计划。如果必要，定义以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

  - **每 N 天**

    任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

    默认下，任务每天运行一次，从当前系统日期和时间开始。

  - **每 N 星期**

    任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

    默认下，任务每星期一于当前系统时间运行一次。

- **每 N 分钟**

  任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

  默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每天(不支持夏令时)**

  任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

  我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。

  默认下，任务每天于当前系统时间运行一次。

- **每周**

  任务每周在指定星期和指定时间运行。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

步骤 6：定义任务名称

在“**定义任务名称**”窗口，指定您正在创建的任务名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（`"*<>?\:|`）。

点击**下一步**以继续到下一步。

步骤 7：完成任务创建

在“**完成任务创建**”窗口，点击“**完成**”按钮完成向导。

如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

管理统计信息

保护系统和受管理设备状态的统计信息显示在可以自定义的信息窗格中。统计信息显示在“**统计**”选项卡上**管理服务器**节点的工作区中。该选项卡包含一些第二级选项卡（页面）。每个选项页面显示统计信息窗格，以及企业新闻和 Kaspersky 的其他材料的链接。统计信息以表格或图表（饼状图或柱状图）的形式显示在信息窗格。应用程序运行时，信息窗格中的数据保持实时更新，反映保护应用程序的当前状态。

您可以更改“**统计**”选项卡上的二级选项卡设置，每个选项页面上的信息窗格数量以及信息窗格中的数据显示模式。

*要在“**统计**”选项卡添加带有信息窗格的新二级选项卡，请执行以下操作：*

1. 在“**统计**”选项卡的右上角单击“**自定义视图**”查看按钮。

   统计信息属性窗口打开。该窗口包含当前显示在“**统计**”选项卡的选项页面列表。在该窗口，您可以更改选项卡上页面的显示顺序，添加和删除页面，通过点击**属性**按钮转到页面属性配置。

2. 单击“**添加**”按钮。

   这将打开新页面的属性窗口。

3. 配置新页面：

   - 在“**常规**”区域，指定页面名称。
   - 在“**信息窗格**”区域，单击“**添加**”按钮添加必须在页面上显示的信息面板。

     单击“**信息窗格**”区域的“**属性**”按钮来设置您添加的信息窗格属性：面板中图表的名称、类型和外观，以及用于绘制图表所需的数据。

4. 单击“**确定**”。

带有您所添加的信息窗格的选项页面将显示在“**统计**”选项卡上。点击设置图标 (⚙) 迅速切换到页面配置或所选信息窗格。

配置事件通知

Kaspersky Security Center 允许您配置将客户端设备上发生的事件通知管理员的方法，并允许您配置通知：

- 电子邮件。当发生事件时，程序将向指定的电子邮件地址发送通知。您可以编辑通知文本。
- SMS。当发生事件时，程序将向指定的电话号码发送通知。您可以配置 SMS 通知以便通过邮件网关发送。
- 可执行文件。当设备上发生事件时，将在管理员工作站上启动该可执行文件。管理员可以通过该可执行文件接收已发生事件参数。

要配置客户端设备上发生的事件的通知，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。
3. 单击“**配置通知和事件导出**”链接并在下拉列表中选择“**配置通知**”值。
   这会打开**属性：事件**窗口。
4. 在“**通知**”区域，选择通知方法（通过邮件、SMS 或者运行可执行文件）并定义通知设置：

   - **电子邮件**

     “**电子邮件**”选项卡允许您配置事件的电子邮件通知。

     在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。

     在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

     - IPv4 或 IPv6 地址
     - 设备的 Windows 网络名称（NetBIOS 名称）
     - SMTP 服务器的 DNS 名称

     在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

     如果启用“**使用 DNS MX 查找**”选项，则可以将多个 IP 地址 MX 记录用于同一个 SMTP 服务器 DNS 名称。同一 DNS 名称可能有多个 MX 记录，这些记录具有不同的电子邮件接收优先级。管理服务器将尝试按 MX 记录优先级的升序向 SMTP 服务器发送电子邮件通知。默认情况下已禁用该选项。

     > 如果启用“**使用 DNS MX 查找**”选项但不启用 TLS 设置，建议您将服务器设备上的 DNSSEC 设置用作发送电子邮件通知的额外保护措施。

     单击“**设置**”链接以定义其他通知设置：

     - 主题名称（电子邮件的主题名称）
     - 发件人电子邮件地址
     - ESMTP 身份验证设置

如果为 SMTP 服务器启用了 ESMTP 身份验证选项，则必须指定在 SMTP 服务器上进行身份验证的账户。

- SMTP 服务器的 TLS 设置：

  - **不使用 TLS**

    如果要禁用电子邮件加密，则可以选择此选项。

  - **如果 SMTP 服务器支持，则使用 TLS**

    如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

  - **始终使用 TLS，检查服务器证书的有效性**

    如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以为 SMTP 服务器指定 TLS 设置：

- 浏览 SMTP 服务器证书文件：

您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

- 浏览客户端证书文件：

您可以使用从任何来源（例如，从任何受信任证书颁发机构）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

- X-509 证书：

您必须指定一个证书文件和一个私钥文件。这两个文件不相互依赖，文件的加载顺序也不重要。加载这两个文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

- pkcs12容器：

您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

通知消息字段包含程序发送的事件信息的标准文本。该文本包含代替参数，例如事件名称、设备名称和域名。您可以通过添加其他带有事件的更多相关详情的替代参数来编辑消息文本。替代参数列表通过点击字段右侧的按钮可用。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接可指定应用程序在指定时间段可以发送的最大通知数量。

单击“**发送测试消息**”按钮以检查是否已正确配置通知。应用程序应向您指定的电子邮件地址发送测试通知。

- SMS

SMS 选项卡允许您配置传输各种事件的 SMS 通知到手机。SMS 消息通过邮件网关发送。

在**收件人（电子邮件地址）**字段，指定程序发送通知的邮件地址。您可以在该字段指定多个地址，以分号分隔。通知将被传送到指定邮件地址关联的电话号码。

在 **SMTP 服务器**字段，指定邮件服务器地址，以分号分隔。您可以使用下列值：

- IPv4 或 IPv6 地址
- 设备的 Windows 网络名称（NetBIOS 名称）
- SMTP 服务器的 DNS 名称

在 **SMTP 服务器端口**字段，指定 SMTP 服务器通信端口号。默认端口号是 25。

单击“**设置**”链接以定义其他通知设置：

- 主题名称（电子邮件的主题名称）
- 发件人电子邮件地址
- ESMTP 身份验证设置

如果为 SMTP 服务器启用了 ESMTP 身份验证选项，则必要时可以指定在 SMTP 服务器上进行身份验证的账户。

- SMTP 服务器的 TLS 设置

您可以禁用 TLS，如果 SMTP 服务器支持 TLS，则使用此协议，您也可以强制仅使用 TLS。如果您选择仅使用 TLS，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，如果选择仅使用 TLS，还可以为 SMTP 服务器上的客户端身份验证指定证书。

- 浏览 SMTP 服务器证书文件

您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到 Kaspersky Security Center。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。“**通知消息**”字段包含标准文本，其中包含有关应用程序在事件发生时发送的事件的信息。该文本包含代替参数，例如事件名称、设备名称和域名。您可以通过添加其他带有事件的更多相关详情的替代参数来编辑消息文本。替代参数列表通过点击字段右侧的按钮可用。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接以指定应用程序在指定时间间隔内可以发送的最大通知数量。

单击“**发送测试消息**”按钮检查您是否正确配置了通知。应用程序应向您指定的收件人发送测试通知。

- **要运行的可执行文件**

如果选择该通知方法，您可以在输入字段指定事件发生时要启动的应用程序。

点击**配置通知限制数**链接允许您指定应用程序在指定时间段可以发送的最大通知数量（通知数量 / 分钟数）。

点击**发送测试消息**按钮允许您检查您是否正确配置了通知：应用程序发送测试通知到您指定的邮件地址。

5. 在“**通知消息**”字段，输入事件发生时应用程序要发送的文本。
   您可以使用文本字段右边的下拉列表来添加事件详情的替代设置（例如，事件描述、发生时间等等）。

   如果通知文本包含 % 字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

6. 单击“**发送测试消息**”按钮以检查通知是否已正确配置。
   程序发送测试通知到指定用户。

7. 单击“**确定**”保存更改。

经过调整的通知设置将应用于客户端设备上发生的所有事件。

您可以在管理服务器设置、策略设置或应用程序设置的“**事件配置**”区域覆盖特定事件的通知设置。

为 SMTP 服务器创建证书

要为 SMTP 服务器创建证书：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。
3. 单击“**配置通知和事件导出**”链接并在下拉列表中选择“**配置通知**”值。
   “事件属性”窗口打开。
4. 在“**电子邮件**”选项卡，单击“**设置**”链接打开“**设置**”窗口。
5. 在“**设置**”窗口，单击“**指定证书**”链接打开“**签名证书**”窗口。
6. 在**签名证书**窗口中，单击**浏览**按钮。
   “**证书**”窗口将打开。
7. 在“**证书类型**”下拉列表，指定公有或私有证书类型：
   - 如果选择了私有类型证书 (**PKCS #12 容器**)，指定证书文件和密码。
   - 如果选择了公有类型证书 (**X.509 证书**)：
     a. 指定私有密钥文件（带有 *.prk 或 *.pem 扩展名的文件）。
     b. 指定私有密钥密码。
     c. 指定公有密钥文件（带有 *.cer 扩展名）。
8. 单击“**确定**”。

SMTP 服务器证书被发布。

事件分类

Kaspersky Security Center 和受管理应用程序的操作事件信息保存在管理服务器数据库和 Microsoft Windows 系统日志。您可以在“**事件**”选项卡上**管理服务器**节点工作区中的管理服务器数据库中查看信息。

“**事件**”选项卡的信息以事件分类列表形式展示。每个分类仅包含特殊类型的事件。例如，“设备状态是严重”分类仅包含设备状态变成“严重”的记录。安装应用程序后，“**事件**”选项卡包含一些标准事件分类。您可以创建附加事件分类或者将事件信息导出为文件。

查看事件分类

要查看事件分类，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。
3. 在“**事件分类**”下拉列表，选择相应事件分类。
   如果您想要该分类的事件永久显示在工作区，请单击所选分类旁边的星星图标 (☆)。

   工作区将显示管理服务器上存储的选定类型事件的列表。

您可以在事件列表中将信息排序，采用升序或者降序。

自定义事件分类

要自定义事件分类，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。
3. 在“**事件**”选项卡中打开相关事件分类。
4. 单击“**分类属性**”按钮。

   您可以在随后打开的事件分类属性窗口中配置事件分类。

创建事件分类

要创建事件分类，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。

3. 单击“**创建新分类**”按钮。

4. 在打开的“**新事件分类**”窗口中，输入新分类的名称，然后单击“**确定**”。

   您所指定名称的分类创建于“**事件分类**”下拉列表。

默认情况下，所创建的事件分类将包含管理服务器中存储的所有事件。要让分类中仅显示您需要的事件，您必须自定义该分类。

将事件分类导出至文本文件

要将事件分类导出至文本文件，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。

2. 在该节点的工作区中，选择“**事件**”选项卡。

3. 单击“**导入/导出**”按钮。

4. 在下拉列表中，选择“**导出事件到文件**”。

   事件导出向导启动。遵照向导的说明操作。

从分类中删除事件

要从分类中删除事件：

1. 在控制台树中，选择具有相关管理服务器名称的节点。

2. 在该节点的工作区中，选择“**事件**”选项卡。

3. 使用鼠标、**SHIFT** 或 **CTRL** 键选择要删除的事件。

4. 以下列方式之一删除所选事件：

   - 通过在所选事件的上下文菜单中选择“**删除**”。

     如果您在上下文菜单中选择“**删除所有**”项，则无论您要删除的事件是什么，都将从该分类中删除所显示的所有事件。

   - 通过单击这些事件信息框中的“**删除事件**”链接（如果选择了一个事件）或“**删除事件**”链接（如果选择了多个事件）。

   所选事件被删除。

根据用户请求添加应用程序到排除

当您收到用户请求解锁被错误阻止的应用程序时，您可以从这些应用程序的自适应安全规则创建排除。此后，应用程序将不会在用户设备上被阻止。您可以在管理服务器的“**监控**”选项卡跟踪用户请求号。

要根据用户请求添加被 Kaspersky Endpoint Security 阻止的应用程序到排除：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**事件**”选项卡。
3. 在“**事件分类**”下拉列表中，选择“**用户请求**”。
4. 右击包含您要添加到排除的应用程序的用户请求，然后选择**添加排除**。
   这启动添加排除向导。遵循其说明。

所选应用程序将在下一次客户端设备与管理服务器同步时从“**智能培训状态下的规则触发器**”列表（在控制台树的“**存储库**”下）中排除，且不会再出现在列表中。

设备分类

设备状态的信息显示在控制台树的“**设备分类**”文件夹。

“**设备分类**”文件夹中的信息显示为设备分类列表。每个分类包含满足特定条件的设备。例如，“**处于“严重”状态的设备**”分类仅包含带有*严重*状态的设备。安装应用程序后，“**设备分类**”文件夹将包含一些标准分类。您可以创建其他（自定义）设备分类，将分类导出至文件，或使用从其他文件导入的设置来创建分类。

查看设备分类

要查看设备分类，请执行以下操作：

1. 在控制台树中，选择“**设备分类**”文件夹。
2. 在该文件夹的工作区的“**此分类的设备**”列表中，选择相关设备分类。
3. 单击**运行分类**按钮。
4. 单击“**分类结果**”选项卡。

工作区将显示分类标准所对应的设备列表。

您可以在设备列表中任意栏上以升序或降序进行排序。

配置设备分类

要配置设备分类：

1. 在控制台树中，选择“**设备分类**”文件夹。
2. 在工作区，单击“**分类**”选项卡，然后单击用户分类列表中的相关设备分类。
3. 单击“**分类属性**”按钮。

4. 在打开的属性窗口，指定以下设置：

   - 常规分类属性。
   - 包含设备到该分类必须满足的条件。您可以在选择条件名称并单击“**属性**”按钮后配置条件。
   - 安全设置。

5. 单击“**确定**”。

   设备被应用并保存。

以下是分配设备到分类的条件描述。多个条件使用 OR 逻辑运算符组合在一起：选择范围将包含至少符合列出的一个条件的设备。

常规

在“**常规**”区域，您可以更改分类条件的名称，指定条件是否必须被倒转：

反转分类条件

> 默认情况下已禁用该选项。
>
> 如果启用此选项，指定的分类条件将倒转。此分类将包含所有不符合该条件的设备。
>
> 以下示例展示了反转工作的逻辑：
>
> - **条件**：您的设备上存在操作系统类型为 Linux 且内部版本号为 00.0.000 的设备。
> - **反转条件**：您的设备上存在操作系统类型为非 Linux 且内部版本号为非 00.0.000 的设备，这等价于：存在操作系统类型为非 Linux 或内部版本号为非 00.0.000 的设备。
>
> 因此，选择范围将包括操作系统类型为 Windows 且内部版本号为 00.0.000 的设备，或者 Linux 且内部版本号不为 00.0.000 的设备。

网络

在“**网络**”区域，您可以指定根据网络数据包含设备到分类的标准：

- **设备名称或 IP 地址**

  > 设备的 Windows 网络名称（NetBIOS 名称）或者 IPv4 或 IPv6 地址。

- **Windows 域**

  > 显示指定的 Windows 域中包括的所有设备。

- **管理组**

  显示指定的管理组中包括的设备。

- **描述**

  设备属性窗口中的文本：在“**常规**”区域的“**描述**”字段。
  要描述“**描述**”字段中的文本，您可以使用以下字符：

  - 在单词中：

    - *****。用任意数量的字符替换任何字符串。

    例如：
    要描述单词 **Server** 或 **Server's**，您可以输入 **Server***。

    - **?**。替换任意单个字符。

    例如：
    要描述单词 **Window** 或 **Windows**，您可以输入 **Windo?**。
    星号(*****)或问号(**?**)不能用于查询中的第一个字符。

  - 要查找多个单词：

    - 空格。显示所有在其描述中包含列出的任何单词的设备。

    例如：
    要查找包含“**从属**”或“**虚拟**”单词的短语，可以在查询中包含“**从属 虚拟**”行。

    - **+**。当单词带有加号前缀时，所有搜索结果都将包含该单词。

    例如：
    要查找同时包含“**从属**”和“**虚拟**”的短语，请输入“**+从属+虚拟**”查询。

    - **-**。当单词带有减号前缀时，所有搜索结果都不包含该单词。

    例如：
    要查找包含“**从属**”但不包含“**虚拟**”的短语，请输入“**+从属-虚拟**”查询。

    - **“<某些文本>”**。引号中围绕的文本必须存在于文本中。

    例如：
    要查找包含“**从属服务器**”单词组合的短语，可以在查询中输入“**从属服务器**”。

- **IP 范围**

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。
  默认情况下已禁用该选项。

标签

在“**标签**”区域，您可以基于先前添加到受管理设备的描述的关键字（标签）配置包含设备到分类的标准：

- **如果至少一个指定的标签匹配则应用**

  如果启用此选项，搜索结果将显示包含带有所选标签的描述的设备。
  如果禁用此选项，搜索结果将仅显示包含带有所有标签的描述的设备。
  默认情况下已禁用该选项。

- **必须包含标签**

  如果选择了该选项，搜索结果将显示带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。
  默认情况下已选定该选项。

- **必须排除标签**

  如果选择了该选项，搜索结果将显示不带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

活动目录

在“**活动目录**”区域，您可以配置基于活动目录数据包含设备到分类的标准：

- **设备在活动目录组织单元中**

  如果启用此选项，选择范围将包括输入字段中指定的 Active Directory 组织单元中的设备。
  默认情况下已禁用该选项。

- **包括子组织单元**

  如果启用此选项，选择范围将包括指定域组织单元的所有子组织单元中的设备。
  默认情况下已禁用该选项。

- **该设备是活动目录组成员**

  如果启用此选项，选择范围将包括输入字段中指定的活动目录组中的设备。
  默认情况下已禁用该选项。

网络活动

在“**网络活动**”区域，您可以指定根据网络活动包含设备到分类的标准：

- **该设备是分发点**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

  - **是**。选择范围将包括充当分发点的设备。
  - **否**。选择范围将不包括充当分发点的设备。
  - **未选择值**。将不应用标准。

- **不断开与管理服务器的连接**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

  - **已启用**。分类将包含选中了“**不断开与管理服务器的连接**”复选框的设备。
  - **已禁用**。分类将包含清空了“**不断开与管理服务器的连接**”复选框的设备。
  - **未选择值**。将不应用标准。

- **连接配置文件已切换**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

  - **是**。该分类将包含连接配置文件切换后连接到管理服务器的设备。
  - **否**。该分类将不包含连接配置文件切换后连接到管理服务器的设备。
  - **未选择值**。将不应用标准。

- **上一次连接到管理服务器**

  您可使用此选框设置按上一次连接到管理服务器的时间搜索设备的标准。

  如果选择该选框，则在输入字段中，您可以指定在客户端设备上安装的网络代理和管理服务器之间建立上一次连接的时间间隔（日期和时间）。选择将包括位于指定间隔的设备。

  如果清除此选框，则将不会应用标准。

  默认情况下已清除该选框。

- **网络轮询时检测到新设备**

  搜索最近几天通过网络轮询检测到的新设备。

  如果启用此选项，分类将只包括在“**检测周期 (天)**”字段中指定的天数内通过设备发现检测到的新设备。

  如果禁用此选项，分类将包括通过设备发现检测到的所有设备。

  默认情况下已禁用该选项。

- **设备可见**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **是**。程序在分类中包括网络中当前可见的设备。
  - **否**。应用程序在分类中包括网络中当前不可见的设备。
  - **未选择值**。将不应用标准。

应用程序

在“**应用程序**”区域，您可以配置基于所选的受管理应用程序包含设备到分类的标准：

- **应用程序名称**

  在下拉列表中，可设置按卡巴斯基应用程序名称执行搜索时在分类中包括设备的标准。
  列表仅提供管理员工作站上已安装管理插件的应用程序的名称。
  如果未选择任何应用程序，则将不会应用该标准。

- **应用程序版本**

  在输入字段，可设置按卡巴斯基应用程序版本号执行搜索时在分类中包括设备的标准。
  如果未指定版本号，则将不会应用该标准。

- **关键更新名称**

  在输入字段中，可设置按应用程序名称或更新包编号执行搜索时在分类中包括设备的标准。
  如果字段留空，则将不会应用该标准。

- **上一次模块更新**

  您可以使用此选项来设置按这些设备上安装的程序模块上次更新的时间搜索设备的标准。
  如果选中此选框，则您可以在输入字段中指定执行这些设备上安装的程序模块的上一次更新的时间间隔（日期和时间）。
  如果清除此选框，则将不会应用标准。
  默认情况下已清除该选框。

- **设备通过 Kaspersky Security Center 管理**

  在该下拉列表，您可以包含通过 Kaspersky Security Center 管理的设备到分类：
  - **是**。应用程序包含通过 Kaspersky Security Center 管理的设备。
  - **否**。应用程序在分类中包含不通过 Kaspersky Security Center 管理的设备。
  - **未选择值**。将不应用标准。

- **安全应用程序已安装**

  在该下拉列表，您可以包含已安装安全应用程序的设备到分类：

  - **是**。应用程序包含安装了安全应用程序的设备到分类。
  - **否**。应用程序在分类中包含未安装安全应用程序的设备。
  - **未选择值**。将不应用标准。

操作系统

在“**操作系统**”区域，您可以指定根据操作系统类型包含设备到分类的标准。

- **操作系统版本**

  如果选中该选框，您可以从列表中选择一个操作系统。安装了指定操作系统的设备会包含在搜索结果中。

- **操作系统 bit 大小**

  在该下拉列表中，可选择操作系统的架构，这将决定将移动规则应用到设备（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。默认情况下，不选择列表中的任何选项，这样就不会对操作系统的架构进行定义。

- **操作系统服务包版本**

  在该字段中，可以指定操作系统的更新包版本（采用 *X.Y* 格式），这将决定将移动规则应用到设备的方式。默认情况下，不指定版本值。

- **操作系统内部版本**

  该设置仅应用到 Windows 操作系统。

  操作系统版本号。您可以指定所选操作系统是否必须具有相等、更早或更晚的版本号。您也可以配置对所有版本号的搜索，除了指定版本号。

- **操作系统发布 ID**

  该设置仅应用到 Windows 操作系统。

  操作系统发布 ID。您可以指定所选操作系统是否必须具有相等、更早或更晚的发布 ID。您也可以配置对所有版本 ID 号的搜索，除了指定的版本 ID 号。

设备状态

在“**设备状态**”区域，您可以配置基于受管理应用程序的设备状态的描述包含设备到分类的标准：

- **设备状态**

  在该下拉列表中，您可以选择下列设备状态之一：“*正常*”、“*严重*”或“*警告*”。

- **设备状态描述**

  在该字段中，您可以选中条件旁边的选框，这些条件如果被满足，程序会为设备分配下列状态之一：*正常*、*严重* 或 *警告*。

- **应用程序定义的设备状态**

  您可以在该下拉列表中选择实时保护状态。具有指定实时保护状态的设备将被包括在选择范围中。

保护组件

在“**保护组件**”区域，您可以设置基于保护状态包含设备到分类的标准：

- **数据库发布日期**

  如果选择此选项，您可以按反病毒数据库发布日期搜索客户端设备。在该输入字段中，您可以设置执行搜索的时间间隔。

  默认情况下已禁用该选项。

- **上一次扫描**

  如果启用此选项，您可以按上次恶意软件扫描时间来搜索客户端设备。在该输入字段中，您可以指定执行上一次恶意软件扫描的时段。

  默认情况下已禁用该选项。

- **检测到的威胁总数**

  如果启用此选项，您可以根据发现的病毒数量来搜索客户端设备。在输入字段中，您可以设置发现病毒总数的上限值和下限值。

  默认情况下已禁用该选项。

应用程序注册表

在“**应用程序注册表**”区域，您可以设置基于已安装的应用程序搜索设备的标准：

- **应用程序名称**

  在该下拉列表中，您可以选择应用程序。安装有指定应用程序的设备将包括在选择范围中。

- **应用程序版本**

  在该输入字段中，您可以指定选定应用程序的版本。

- **供应商**

  在该下拉列表中，您可以选择已安装应用程序的生产商。

- **应用程序状态**

  在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

- **根据更新查找**

  如果启用此选项，则搜索操作将使用相关设备内应用程序更新的有关信息来执行。选中复选框后，“**应用程序名称**”、“**应用程序版本**”和“**应用程序状态**”字段将分别更改为“**更新名称**”、“**更新版本**”和“**状态**”。

  默认情况下已禁用该选项。

- **不兼容的安全应用程序名称**

  在该下拉列表中，您可以选择第三方安全应用程序。在搜索过程中，安装有指定程序的设备将包括在选择范围中。

- **应用程序标签**

  在该下拉列表中，您可以选择应用程序标签。所有安装了描述中带有所选标签的应用程序的设备都被包含在设备分类。

- **应用到没有指定标签的设备**

  如果启用此选项，分类将包含未带有所选标签的描述的设备。

  如果禁用此选项，则不应用该标准。

  默认情况下已禁用该选项。

硬件注册表

在“**硬件注册表**”区域，您可以配置基于所安装的硬件包含设备到分类的标准：

- **设备**

  在该下拉列表中，您可以选择单元类型。所有带有该单元的设备被包含在搜索结果。

  该字段支持完整文本搜索。

- **供应商**

  在该下拉列表中，您可以选择单元生产商的名称。所有带有该单元的设备被包含在搜索结果。
  该字段支持完整文本搜索。

- **设备名称**

  在 Windows 网络中的设备名称。具有指定名称的设备将包括在该分类中。

- **描述**

  设备或硬件单元的描述。带有该字段中指定的描述的设备将包括在分类范围内。
  可在设备的属性窗口输入任何格式的设备描述。该字段支持完整文本搜索。

- **设备制造商**

  设备制造商的名称。被指定生产商制造的设备将包括在分类范围内。
  您可以在设备的属性窗口中输入制造商的名称。

- **序列号**

  带该字段中指定序列号的所有硬件设备将包括在该分类中。

- **清单号**

  带有该字段中指定的清单编号的设备将包括在选择范围内。

- **用户**

  该字段中指定用户的所有硬件设备都将包括在该分类中。

- **位置**

  设备或硬件单元的位置（例如，在总部或分公司）。在该字段中指定的位置部署的计算机或其他设备将包括在该分类中。
  您可以在该设备的属性窗口中以任何格式描述设备的位置。

- **CPU 频率 (MHz)**

  CPU 的频率范围。CPU 与这些输入字段（含）中频率范围匹配的设备将包括在分类范围内。

- **虚拟 CPU 内核**

  CPU 中虚拟核心的数量范围。CPU 与这些输入字段（含）中范围匹配的设备将包括在分类范围内。

- **硬盘卷(GB)**

  设备硬盘容量值的范围。硬盘与这些输入字段（含）中范围匹配的设备将包括在分类范围内。

- **内存大小(MB)**

  设备 RAM 大小的值范围。 RAM 与这些输入字段中的范围（含）匹配的设备将包含在分类中。

虚拟机

在“**虚拟机**”区域，您可以设置基于它们是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来包含设备到分类的标准：

- **这是一台虚拟机**

  在该下拉列表中，您可以选择以下选项：
  - **不重要**。
  - **否**。查找非虚拟机设备。
  - **是**。查找虚拟机设备。

- **虚拟机类型**

  在该下拉列表中，您可以选择虚拟机生产商。
  如果在“**这是一台虚拟机**”下拉列表中选择了“**是**”或“**不重要**”值，则该下拉列表可用。

- **虚拟桌面基础架构的一部分**

  在该下拉列表中，您可以选择以下选项：
  - **不重要**。
  - **否**。查找不属于虚拟桌面基础架构的设备。
  - **是**。查找术语虚拟桌面基础架构 （VDI） 一部分的设备。

漏洞和更新

在“**漏洞和更新**”区域，您可以指定根据 Windows 更新源包含设备到分类的标准：

WUA 已切换到管理服务器

您可以在下拉列表中选择以下搜索选项之一：
- **是**。如果选中该选项，搜索结果会包含从管理服务器收到 Windows Update 更新的设备。

- **否**。如果选中该选项，搜索结果将包含从其它源收到 Windows Update 更新的设备。

用户

在“**用户**”区域，您可以设置根据登录到操作系统的用户账户包含设备到分类的标准。

- **最后一次登录系统的用户**

  如果启用此选项，单击“**浏览**”按钮可以指定用户账户。搜索结果包含其上一次登录用户为指定用户的设备。

- **登录系统至少一次的用户**

  如果启用此选项，单击“**浏览**”按钮可以指定用户账户。搜索结果包含指定用户至少登录一次的设备。

影响受管理应用程序状态的问题

在“**影响受管理应用程序状态的问题**”区域，您可以指定根据由受管理应用程序检测到的可能问题列表包含设备到分类的标准。如果至少一个您选择的问题存在于设备，设备将被包含到分类。当您选择几个应用程序的问题时，您可以选择在所有列表中自动选择该问题。

设备状态描述

您可以选择受管理应用程序状态描述的复选框；接收这些状态时，设备将被包含在分类。当您选择几个应用程序的状态时，您可以选择在所有列表中自动选择该状态。

受管理应用程序组件的状态

在“**受管理应用程序组件的状态**”区域，您可以配置根据受管理应用程序组件状态包含设备到分类的标准：

- **数据泄漏防护状态**

  根据数据泄漏防护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- **协作服务器保护状态**

  根据服务器协作保护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- **邮件服务器的反病毒保护状态**

  根据邮件服务器保护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）*搜索设备。*

- **端点传感器状态**

  根据端点传感器组件状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

加密

加密算法

高级加密标准(AES)对称分组密码算法。在下拉列表中，您可以选择加密密钥大小(56 位、128 位、192 位或 256 位)。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

云段

在“**云段**”区域，您可以配置根据相关云段包含设备到分类的标准：

- **设备在云段中**

  如果启用此选项，您可以单击“**浏览**”按钮以指定要搜索的段。

  如果还启用“**包含子对象**”选项，将在指定段的所有子对象上运行搜索。

  搜索结果仅包含所选段的设备。

- **使用 API 发现的设备**

  在下拉列表，您可以选择设备是否由 API 工具检测：

  - **AWS**。设备使用 AWS API 发现，即设备确定在 AWS 云环境中。
  - **Azure**。设备使用 Azure API 发现，即设备确定在 Azure 云环境中。
  - **Google Cloud。**设备使用 Google API 发现，即设备确定在 Google Cloud 环境中。
  - **否**。无法使用 AWS API、Azure API 或 Google API 检测到该设备，即设备位于云环境之外，或者位于云环境中，但是无法使用 API 检测到该设备。
  - **没有值**。此条件不适用。

应用程序组件

该区域包含了在管理控制台中安装了管理插件的这些应用程序的组件列表。

在“**应用程序组件**”区域，您可以指定根据所选应用程序组件的状态和版本号包含设备到分类的标准：

- **状态**

  根据应用程序发送到管理服务器的组件状态搜索设备。您可以选择以下状态之一：*设备上无数据*、*已停止*、*正在启动*、*已暂停*、*运行中*、*故障*或*未安装*。如果安装在受管理设备上的应用程序的所选组件具有指定状态，设备被包含到设备分类。

由应用程序发送的状态：

- *正在启动* - 组件处于初始化进程中。
- *运行中* - 组件被启用且在正常工作。
- *已暂停* - 组件被暂停，例如，在用户在受管理应用程序上停止了保护后。
- *故障* - 组件操作中发生错误。
- *已停止* - 组件被禁用且不在工作。
- *未安装* - 当配置应用程序自定义安装时，用户未选择该组件以安装。

不同于其他状态，*设备上无数据*状态不由应用程序发送。该选项显示应用程序没有所选组件状态的信息。例如，这可能发生在所选组件不属于任何在设备上安装的应用程序时，或设备关闭时。

- **版本**

  根据您在列表中选择的版本号搜索设备。您可以输入版本号，例如 `3.4.1.0`，然后指定所选组件是否必须具有相同、更早或更新版本。您也可以配置对除指定版本外的所有版本进行搜索。

导出设备分类设置到文件

要将设备分类设置导出至文本文件，请执行以下操作：

1. 在控制台树中，选择“**设备分类**”文件夹。
2. 在工作区中的“**分类**”选项卡上，单击用户选择列表中的相关设备分类。

   只能从用户创建的设备分类中导出设置。

3. 单击**运行分类**按钮。
4. 在“**分类结果**”选项卡上，单击“**导出设置**”按钮。
5. 在打开的“**另存为**”窗口中，指定选择设置导出文件的名称，选择用来保存该文件的文件夹，然后单击“**保存**”按钮。

设备分类的设置将保存到指定的文件。

创建设备分类

要创建设备分类，请执行以下操作：

1. 在控制台树中，选择“**设备分类**”文件夹。
2. 在文件夹的工作区，点击“**高级**”并在下拉列表中选择“**创建新分类**”。
3. 在打开的“**新设备分类**”窗口中，输入新分类的名称，然后单击“**确定**”。

在控制台树中的“**设备分类**”文件夹中，将出现以您输入名称命名的新文件夹。默认情况下，新设备分类将包含在其创建此分类的管理服务器上的管理组中的所有设备。要让分类只显示您特别感兴趣的设备，通过点击“**分类属性**”按钮配置分类。

根据导入的设置创建设备分类

要使用导入的设置创建设备分类，请执行以下操作：

1. 在控制台树中，选择“**设备分类**”文件夹。
2. 在文件夹的工作区，点击“**高级**”按钮并在下拉列表中选择“**从文件导入分类**”。
3. 在打开的窗口中，指定您要导入分类设置的文件路径。单击“**打开**”按钮。

此时会在“**设备分类**”文件夹中创建一个“**新分类**”条目。新分类的设置从您指定的文件中被导入。

如果名为“**新分类**”的分类已存在于“**设备分类**”文件夹中，则会将一条 **(<下一个序列号>)** 格式的索引添加到所创建分类的名称中，例如：**(1)**、**(2)**。

在分类中从管理组中删除设备

在使用设备分类时，你可以直接从管理组中删除设备，而不是切换到包含这些设备的管理组。

要从管理组删除设备，请执行以下操作：

1. 在控制台树中，选择“**设备分类**”文件夹。
2. 使用“**Shift**”或“**Ctrl**”键选择您希望移除的设备。
3. 以下列方式之一从管理组中删除所选设备：
   - 在任何所选设备的上下文菜单中选择“**删除**”。
   - 单击“**执行操作**”按钮并在下拉列表中选择“**从组中删除**”。

所选设备即从相应管理组中删除。

监控应用程序安装和卸载

您可以监控受管理设备上特定应用程序（例如特定浏览器）的安装和卸载。要使用此功能，您可以将应用程序从应用程序注册表添加到受监控应用程序的列表中。安装或卸载受监控应用程序时，网络代理将发布相应的事件：“**已安装监控的应用程序**”或“**已卸载监控的应用程序**”。您可以使用事件分类或报告来监控这些事件。

仅当这些事件存储在管理服务器数据库中时，您才可以监控它们。

要将应用程序添加到受监控应用程序的列表，请执行以下操作：

1. 在控制台树的**高级** → **应用程序管理**文件夹中，选择“**应用程序注册表**”子文件夹。
2. 在显示的应用程序列表上方，单击“**显示应用程序注册表属性窗口**”按钮。
3. 在显示的“**监控的应用程序**”窗口中，单击“**添加**”按钮。
4. 在显示的“**选择应用程序名称**”窗口中，从应用程序注册表中选择要监控其安装或卸载的应用程序。
5. 在“**选择应用程序名称**”窗口中，单击“**OK**”按钮。

配置了受监控应用程序列表，并在组织中的受管理设备上安装或卸载受监控应用程序之后，您可以监控相应的事件，例如使用“最近事件”事件分类来监控。

Kaspersky Security Center 组件事件

每个 Kaspersky Security Center 组件都拥有自己的事件类型集。本节列出了 Kaspersky Security Center 管理服务器、网络代理和 iOS MDM 服务器中发生的事件类型。Kaspersky 应用程序中发生的事件类型不在此区域列出。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

事件类型描述的数据结构

对于每个事件类型，它的显示名称、ID、字母码、描述和默认存储期限被提供。

- **事件类型显示名称**。该文本当您配置事件时和它们发生时被显示在 Kaspersky Security Center 中。
- **事件类型 ID**。该数码在您使用第三方工具分析事件时使用。
- **事件类型**（字母码）。该代码用于您使用 Kaspersky Security Center 数据库中提供的公共视图浏览和处理事件时以及事件被导出到 SIEM 系统时。
- **描述**。该文本包含事件发生的情况以及此种情况下您可以做的事。

- **默认存储期限**。这是事件存储在管理服务器数据库的天数，显示在管理服务器事件列表中。该时间段之后，事件被删除。如果事件存储期限值是 0，此类事件被检测但不显示在管理服务器事件列表。如果您配置了保存此类事件到操作系统事件日志，您可以在那里找到它们。

  您可以更改事件存储期限：

  - 管理控制台：设置事件存储期限
  - Kaspersky Security Center Web Console：设置事件存储期限

其他数据可能包含以下字段：

- **Event_id:** ：事件在数据库中的唯一号，被自动生成和分配；不要与**事件类型** ID混淆。
- **Task_id:** ：导致事件（如果有）的任务 ID
- **严重性**：以下严重级别之一（按严重性升序排列）：

  0) 无效的严重级别

  1) 信息

  2) 警告

  3) 错误

  4) 严重

管理服务器事件

该部分包含管理服务器相关事件信息。

管理服务器严重事件

下表显示了具有“**严重**”重要级别的 Kaspersky Security Center 管理服务器事件类型。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

如果您在管理控制台的管理服务器属性窗口中指定了端口，**Kaspersky Security Center 会发布其指标**和关键事件，以供 Prometheus（一个用于监控和警报的系统）获取。Prometheus 获取指标和关键事件，然后为每个事件生成警报。

```
// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"
```

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
已超过授权许可数量限制	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	每天，Kaspersky Security Center 检查是否超过授权许可限制。 当管理服务器发现安装在客户端设备上的 Kaspersky 应用程序超过了授权许可限制，以及由单一授权许可覆盖的当前使用的授权许可单元数量超过了该授权许可覆盖的单元总数的 110%，则该类型的事件发生。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Security Center 决定当授权许可限制被超过时生成事件的规则。	180 天
病毒爆发	26 (对于文件威胁防护)	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。 您可以通过以下方式响应事件： • 您可以在管理服务器属性中配置阈值。 • 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。	180 天
病毒爆发	27 (对于邮件威胁防护)	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。 您可以通过以下方式响应事件： • 您可以在管理服务器属性中配置阈值。 • 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。	180 天
病毒爆发	28 (对于防火墙)	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。 您可以通过以下方式响应事件： • 您可以在管理服务器属性中配置阈值。 • 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。	180 天
设备已失去管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理设备在网络中可见，但指定时间未连接到管理服务器，则该类型的事件发生。 找到什么阻止了设备上网络代理的正常功能。可能的原因包括网络问题和从设备卸载网络代理。	180 天
设备状态是“严重”	4113	KLSRV_HOST_STATUS_CRITICAL	当受管理设备被分配*严重*状态时，该类型的事件发生。您可以配置设备状态被更改到*严重*的条件。	180 天
密钥文件已被添加到拒绝列表	4124	KLSRV_LICENSE_BLACKLISTED	当 Kaspersky 已将您使用的激活码或密钥文件添加到拒绝列表时，会发生该类型事件。 联系技术支持获得更多详情。	180 天
受限制功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	当 Kaspersky Security Center 开始用基本功能操作，没有“漏洞和补丁管理”和“移动设备管理”功能时，该类型的事件发生。 以下是事件发生的原因和正确响应： • 授权许可期限已过期。提供授权许可以使用 Kaspersky Security Center 的完整功能模式（添加有效的激活码或密钥文件到管理服务器）。 • 管理服务器管理比授权许可限制更多的设备。从管理服务器的管理组移动设备到其他管理服务器的管理组（如果其他管理服务器的授权许可限制允许）。	180 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
授权许可即将过期	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	当商业授权许可的失效日期即将到来时，会发生此类事件。 Kaspersky Security Center 每天检查一次授权许可到期日期是否临近。此类型的事件在授权许可到期之前 30 天、15 天、5 天 和 1 天发布。您不能更改天数。如果管理服务器在授权许可到期日之前的指定日期被关闭，则事件直到第二天才发布。 当商业授权许可到期时，Kaspersky Security Center 仅提供基本功能。 您可以通过以下方式响应事件： • 请确保将备用授权许可密钥添加到管理服务器中。 • 如果您使用订阅，请确保续订。如果无限制订阅已在到期日前预付费给服务提供商，则该订阅会自动续订。	180 天
证书已过期	4132	KLSRV_CERTIFICATE_EXPIRED	当移动设备上的客户端移动证书过期时，就会发生此类事件。	180 天
管理服务器证书已过期。	6129	ServerCertificateExpired	当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。 您需要更新过期的证书。	180 天
卡巴斯基应用程序模块更新已撤销	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	如果无缝更新被 Kaspersky 技术专家撤销（这些更新显示 "*已撤销*"状态），例如它们必须更新到新版本，则会发生该类型事件。该事件涉及 Kaspersky Security Center 补丁，但不涉及受管理 Kaspersky 应用程序的模块。事件提供无缝更新未被安装的原因。	180 天
审计：导出到 SIEM 失败	5130	KLAUD_EV_SIEM_EXPORT_ERROR	当由于与 SIEM 系统的连接错误而将事件导出到 SIEM 系统失败时，会发生此类事件。	180 天

管理服务器功能失败事件

下表显示了具有"**功能失败**"重要级别的 Kaspersky Security Center 管理服务器事件类型。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器功能失败事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
运行时错误	4125	KLSRV_RUNTIME_ERROR	由于未知问题，该类型的事件发生。 多数情况下，这些是 DBMS 问题、网络问题和其他软件和硬件问题。 事件详情可以在事件描述中找到。	180 天
已授权应用程序组之一的安装已超过限制	4126	KLSRV_INVLICPROD_EXCEDED	管理服务器定期生成该类型的事件（每小时）。如果您在 Kaspersky Security Center 中管理第三方应用程序的授权许可密钥，并且安装数量超过了第三方应用程序授权许可密钥所设置的限制，则会发生该类型事件。 您可以通过以下方式响应事件： • 查看受管理设备列表。从未使用第三方应用程序的设备上删除该应用程序。 • 为更多设备使用第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。这是一组由满足您所设标准的第三方应用程序组成的授权应用程序群组。	180 天
轮询云段失败	4143	KLSRV_KLCLOUD_SCAN_ERROR	当管理服务器无法在云环境中轮询网段时，将发生此类事件。读取事件描述中的详细信息，并相应做出响应。	未存储

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
将更新复制到指定文件夹失败	4123	KLSRV_UPD_REPL_FAIL	当软件更新被复制到附加共享文件夹时，该类型的事件发生。 您可以通过以下方式响应事件： • 检查用于获取文件夹访问的用户账户是否具有写权限。 • 检查文件夹的用户名和/或密码是否被更改。 • 检查互联网连接，因为它可能是事件原因。遵照指示更新数据库和软件模块。	180 天
没有剩余硬盘空间	4107	KLSRV_DISK_FULL	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	180 天
共享文件夹不可用	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理服务器共享文件夹不可用，则该类型的事件发生。 您可以通过以下方式响应事件： • 检查管理服务器(共享文件夹所在位置)是否已开启并可用。 • 检查文件夹的用户名和/或密码是否被更改。 • 检查网络连接。	180 天
管理服务器数据库不可用	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理服务器数据库不可用则该类型的事件发生。 您可以通过以下方式响应事件： • 检查安装了 SQL Server 的远程服务器是否可用。 • 查看 DBMS 日志以发现管理服务器数据库不可用的原因。例如，因为维护，安装了 SQL Server 的远程服务器可能不可用。	180 天
管理服务器数据库空间不足	4110	KLSRV_DATABASE_FULL	当管理服务器数据库没有剩余空间时，该类型的事件发生。 当管理服务器的数据库达到其容量，以及当不可能再往数据库记录时，管理服务器不工作。 以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应： • 您使用 SQL Server Express 版本 DBMS： 在 SQL Server Express 文档中，查看所用版本的数据库大小限制。可能您的管理服务器数据库已超过了数据库大小限制。 限制存储在管理服务器数据库的事件数量。 在管理服务器数据库中有太多由应用程序控制组件发送的事件。您可以更改与管理服务器数据库中的应用程序控制事件存储有关的 Kaspersky Endpoint Security for Windows 策略的设置。 • 您使用 DBMS 而不是 SQL Server Express Edition： 不限制存储在管理服务器数据库的事件数量。 降低存储在管理服务器数据库的事件数量。 在 DBMS 选项处查看信息。	180 天

管理服务器警告事件

下表显示了具有“**警告**”重要级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
已检测到频繁事件		KLSRV_EVENT_SPAM_EVENTS_DETECTED	当管理服务器在受管理设备上检测到频繁发生的事件时，会发生这种类型的事件。请参阅以下部分了解详情：阻止频繁事件。	90 天
已超过授权许可数量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	每天，Kaspersky Security Center 检查是否超过授权许可限制。 当管理服务器发现安装在客户端设备上的 Kaspersky 应用程序超过了授权许可限制，以及由单一授权许可覆盖的当前使用的授权许可单元数量达到了该授权许可覆盖的单元总数的 100% 到 110%，则该类型的事件发生。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Security Center 决定当授权许可限制被超过时生成事件的规则。	90 天
设备在网络上已长时间没有活动	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	当受管理设备在一段时间内显示出不活动状态时，会发生此类事件。 这种情况通常发生在受管理设备已解除授权时。 您可以通过以下方式响应事件： • 要从受管理设备列表中手动删除该设备。 • 指定时间间隔，经过该间隔后，使用管理控制台或使用 Kaspersky Security Center Web Console 创建“**设备在网络上已长时间没有活动**”事件。 • 指定使用管理控制台或使用 Kaspersky Security Center Web Console 自动将设备自动从组中删除的时间间隔。	90 天
设备名称冲突	4102	KLSRV_EVENT_HOSTS_CONFLICT	当管理服务器将两台或更多受管理设备视为单台设备时，会发生此类事件。 在受管理设备上使用克隆的硬盘驱动器进行软件部署，而没有将参考设备上的网络代理切换到专用磁盘克隆模式时，通常会发生这种情况。 为避免此问题，请在克隆此设备的硬盘驱动器之前将参考设备上的网络代理切换到磁盘克隆模式。	90 天
设备状态是“警告”	4114	KLSRV_HOST_STATUS_WARNING	当受管理设备被分配*警告*状态时，该类型的事件发生。您可以配置设备状态被更改到*警告*的条件。	90 天
已授权应用程序组之一的安装即将超过限制	4127	KLSRV_INVLICPROD_FILLED	当已授权应用程序组中包含的第三方应用程序安装数量达到授权许可密钥属性中指定的最大允许值的 90% 时，将发生此类事件。 您可以通过以下方式响应事件： • 如果某些受管理设备上未使用第三方应用程序，请从这些设备中删除该应用程序。 • 如果您预计第三方应用程序安装数量将在不久的将来超过允许的最大值，请考虑预先获取更多设备的第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。	90 天
证书已被请求	4133	KLSRV_CERTIFICATE_REQUESTED	当自动重新颁发移动设备管理证书失败时，将发生此类事件。 以下是事件的可能原因和对事件的适当响应： • 对禁用了“**如果可能，自动重新发布证书**”选项的证书启动自动重新发布。这可能是由于在证书创建过程中发生的错误所致。可能需要手动重新颁发证书。 • 如果使用与公钥基础结构的集成，则原因可能是用于与 PKI 集成和用于颁发证书的账户缺少 SAM-Account-Name 属性。查看账户属性。	90 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
证书已删除	4134	KLSRV_CERTIFICATE_REMOVED	当管理员删除了移动设备管理的任何类型的证书（通用、邮件、VPN）时，会发生此类事件。 删除证书后，通过此证书连接的移动设备将无法连接到管理服务器。 在调查与移动设备管理相关的故障时，此事件可能会有所帮助。	90 天
证书即将过期	6128	ServerCertificateExpiresSoon	当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。 您需要更新过期的证书。	90 天
APNs 证书已过期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	当 APNs 证书过期时，会发生此类事件。 您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。	未存储
APNs 证书即将过期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	当 APNs 证书距离过期不到 14 天时，会发生此类事件。 当 APNs 证书过期时，您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。 我们建议您在过期日期前安排 APNs 证书续订。	未存储
发送 FCM 消息到移动设备失败	4138	KLSRV_GCM_DEVICE_ERROR	当移动设备管理配置为使用 Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器无法处理从管理服务器收到的某些请求时，会发生此类事件。这意味着某些受管理移动设备不会收到推送通知。 读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FCM 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Firebase 服务文档（参见"下游消息错误响应代码"一章）。	90 天
发送 FCM 消息到 FCM 服务器时发生 HTTP 错误	4139	KLSRV_GCM_HTTP_ERROR	当移动设备管理配置为使用 Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器回复管理服务器请求的 HTTP 代码不是 200（正常）时，会发生此类事件。 以下是事件的可能原因和对事件的适当响应： • FCM 服务器端出现问题。读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FMC 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Firebase 服务文档（参见"下游消息错误响应代码"一章）。 • 代理服务器端出现问题（如果使用代理服务器）。读取事件描述详细信息中的 HTTP 代码，并相应做出响应。	90 天
发送 FCM 消息到 FCM 服务器失败	4140	KLSRV_GCM_GENERAL_ERROR	使用 Firebase Cloud Messaging HTTP 协议时，由于管理服务器端发生意外错误，而发生此类事件。 读取事件描述中的详细信息，并相应做出响应。 如果您自己找不到问题的解决方案，建议与 Kaspersky 技术支持联系。	90 天
硬盘驱动器剩余空间少	4105	KLSRV_NO_SPACE_ON_VOLUMES	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	90 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
管理服务器数据库的剩余空间少	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理服务器数据库受限制则该类型的事件发生。如果您不纠正情况，管理服务器数据库就将达到其容量且管理服务器将不工作。 以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应。 您使用 SQL Server Express 版本 DBMS： • 在 SQL Server Express 文档中，查看所用版本的数据库大小限制。可能您的管理服务器数据库即将超过数据库大小限制。 • 限制存储在管理服务器数据库的事件数量。 • 在管理服务器数据库中有太多由应用程序控制组件发送的事件。您可以更改与管理服务器数据库中的应用程序控制事件存储有关的 Kaspersky Endpoint Security for Windows 策略的设置。 您使用 DBMS 而不是 SQL Server Express Edition： • 不限制存储在管理服务器数据库的事件数量 • 降低存储在管理服务器数据库的事件数量 在 DBMS 选项处查看信息。	90 天
到从属管理服务器的连接已中断	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	当与从属管理服务器的连接中断时，会发生此类事件。 读取安装了从属管理服务器的设备上的卡巴斯基事件日志，并相应做出响应。	90 天
到主管理服务器的连接已中断	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	当与主管理服务器的连接中断时，会发生此类事件。 读取安装了主管理服务器的设备上的卡巴斯基事件日志，并相应做出响应。	90 天
已注册卡巴斯基应用程序模块的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	当管理服务器为需要批准安装的受管理设备上安装的 Kaspersky 软件注册新更新时，会发生此类事件。 使用管理控制台或 Kaspersky Security Center Web Console 批准或拒绝更新。	90 天
超过了数据库中事件数的限制，已开始删除事件	4145	KLSRV_EVP_DB_TRUNCATING	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后开始时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储
超过了数据库中事件数的限制，事件已被删除	4146	KLSRV_EVP_DB_TRUNCATED	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后完成时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改允许存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储
审计(到 SIEM 服务器的连接测试失败)	5120	KLAUD_EV_SIEM_TEST_FAILED	当 SIEM 服务器的测试连接失败时，会发生此类事件。	30 天
自动颁发证书失败		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	如果为移动设备（在移动协议下运行的设备）创建客户端证书时出现错误，则会发生此事件。	90 天

管理服务器信息事件

下表显示了具有“**信息**”重要级别的 Kaspersky Security Center 管理服务器事件。

管理服务器信息事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限	评论
授权许可密钥的 90% 已经使用	4097	KLSRV_EV_LICENSE_CHECK_90	30 天	
已检测到新设备	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 天	
设备已被自动添加到组	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 天	
设备已被根据规则自动移动	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 天	

事件类型显示名称	事件类型 ID	事件类型	默认存储期限	评论
设备已从组中删除：长时间在网络中不活动	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 天	
已授权应用程序组之一的安装即将超过限制(已经使用 95% 以上)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 天	
找到了要发送至卡巴斯基以分析的文件	4131	KLSRV_APS_FILE_APPEARED	30 天	
此移动设备上的 FCM 实例 ID 已被更改	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 天	
更新已被成功复制到指定文件夹	4122	KLSRV_UPD_REPL_OK	30 天	
到从属管理服务器的连接已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 天	
到主管理服务器的连接已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 天	
数据库已更新	4144	KLSRV_UPD_BASES_UPDATED	30 天	
审计：到管理服务器的连接已建立	4147	KLAUD_EV_SERVERCONNECT	30 天	
审计：对象已修改	4148	KLAUD_EV_OBJECTMODIFY	30 天	该事件追踪以下对象中的更改： • 管理组 • 安全组 • 用户 • 包 • 任务 • 策略 • 服务器 • 虚拟服务器
审计：对象状态已更改	4150	KLAUD_EV_TASK_STATE_CHANGED	30 天	例如，当任务以错误失败时会发生该事件。
审计：组设置已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	30 天	
审计：到管理服务器的连接已终止	4151	KLAUD_EV_SERVERDISCONNECT	30 天	
审计：对象属性已被修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 天	该事件追踪以下属性中的更改： • 用户 • 授权许可 • 服务器 • 虚拟服务器
审计：用户权限已被修改	4153	KLAUD_EV_OBJECTACLMODIFIED	30 天	
审计：已从管理服务器导入或导出加密密钥	5100	KLAUD_EV_DPEKEYSEXPORT	30 天	
审计(到 SIEM 服务器的连接测试成功)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 天	当 SIEM 服务器的测试连接成功时，会发生此事件。
备用证书已创建		ServerReserveCertificateCreated	30 天	当管理服务器证书已创建时会发生该事件。

事件类型显示名称	事件类型 ID	事件类型	默认存储期限	评论
证书续费		ServerCertificateRenewed	30 天	当管理服务器证书已续费时会发生该事件。
证书已成功自动颁发		KLSRV_CERTIFICATE_AUTO_ISSUED	30 天	当成功创建移动设备（在移动协议下运行的设备）的证书时，会触发此事件。

仅当针对移动设备和 UEFI 设备的管理服务器服务器证书执行与这些事件对应的操作时，管理服务器才会自动发布**备用证书已创建**、**证书续费**和**证书已成功自动颁发**事件，并在管理控制台中显示这些事件。

网络代理事件

该部分包含管网络代理相关事件信息。

网络代理功能失败事件

下表显示了具有“**功能失败**”严重级别的 Kaspersky Security Center 网络代理事件类型。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理功能失败事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
更新安装错误	7702	KLNAG_EV_PATCH_INSTALL_ERROR	如果Kaspersky Security Center 组件自动更新和补丁未成功，则该类型的事件发生。事件不包含受管理 Kaspersky 应用程序的更新。 阅读事件描述。管理服务器上的 Windows 问题可能是该事件的原因。如果描述提到 Windows 配置的任何问题，解决该问题。	30 天
安装第三方软件更新失败	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	如果“漏洞和补丁管理”和“移动设备管理”功能正在使用且第三方软件更新未成功，则该类型的事件发生。 检查到第三方软件的链接是否合法。阅读事件描述。	30 天
安装 Windows Update 更新失败	7717	KLNAG_EV_WUA_INSTALL_ERROR	如果 Windows 更新未成功，则该类型的事件发生。在网络代理策略中配置 Windows 更新。 阅读事件描述。在 Microsoft 知识库中查找错误。如果您无法自己解决问题，请联系 Microsoft 技术支持。	30 天
用户管理：错误	7723	KLNAG_EV_USR_MNG_ERR	一般警告事件。	30 天
将 sudoers 文件恢复为参考值失败	7726	KLNAG_EV_SUDOER_RESTORED_ERR	事件包含 sudoers 文件替换错误的描述。	30 天
安装根证书失败	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	事件包含证书安装错误的描述。	30 天
移除根证书失败	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	事件包含证书删除错误的描述。	30 天

网络代理警告事件

下表显示具有“**警告**”严重级别的 Kaspersky Security Center 网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理警告事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
在安装软件模块更新期间返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 天
第三方软件更新安装已完成但存在警告	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 天
第三方软件更新安装已延时	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 天
发生了安全问题	549	GNRL_EV_APP_INCIDENT_OCCURED	30 天
KSN 代理已启动。检查 KSN 可用性失败	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 天
用户管理：警告	7722	KLNAG_EV_USR_MNG_WRN	30 天
发现 sudoers 文件与参考值不匹配	7724	KLNAG_EV_SUDOER_DIFFERENT	30 天

网络代理信息事件

下表显示具有“**信息**”严重级别的 Kaspersky Security Center 网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理信息事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
软件模块更新已成功安装	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
软件模块更新安装已启动	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 天
应用程序已安装	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
应用程序已卸载	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
已安装监控的应用程序	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已卸载监控的应用程序	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已安装第三方应用程序	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 天
已添加新设备	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
设备已被删除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
已检测到新设备	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
设备已被授权	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
Windows 桌面共享：文件已读取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 桌面共享：文件已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 桌面共享：应用程序已启动	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 桌面共享：已启动	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 桌面共享：已停止	7716	KLUSRLOG_EV_WDS_END	30 天
第三方软件更新已成功安装	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 天
第三方软件更新安装已开始	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 天
KSN 代理已启动。KSN 可用性检查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天

iOS MDM 服务器事件

该部分包含 iOS MDM 服务器相关事件信息。

iOS MDM 服务器功能失败事件

下表显示具有“**功能失败**”严重级别的 Kaspersky Security Center iOS MDM 服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

iOS MDM 服务器功能失败事件

事件类型显示名称	事件类型	默认存储期限
请求配置文件列表失败	配置文件列表_命令_失败	30 天
安装配置文件失败	安装配置文件_命令_失败	30 天
删除配置文件失败	删除配置文件_命令_失败	30 天
请求 provisioning 配置文件列表失败	PROVISIONING 配置文件列表_命令_失败	30 天
安装 provisioning 配置文件失败	安装 PROVISIONING 配置文件_命令_失败	30 天
删除 provisioning 配置文件失败	删除 PROVISIONING 配置文件_命令_失败	30 天
请求数字证书列表失败	证书列表_命令_失败	30 天
请求已安装应用程序列表失败	已安装应用程序列表_命令_失败	30 天
请求移动设备常规信息失败	设备信息_命令_失败	30 天
请求安全信息失败	安全信息_命令_失败	30 天
锁定移动设备失败	设备锁_命令_失败	30 天
重置密码失败	清除密码_命令_失败	30 天
从移动设备擦除数据失败	擦除设备_命令_失败	30 天
安装应用失败	安装应用程序_命令_失败	30 天
为应用设置兑换代码失败	应用兑换码_命令_失败	30 天
请求受管理应用列表失败	受管理应用程序列表_命令_失败	30 天
删除受管理应用失败	卸载应用程序_命令_失败	30 天
漫游设置已被拒绝	设置漫游设置_命令_失败	30 天
应用操作中发生错误	产品_失败	30 天
命令结果包含无效数据	畸形_命令	30 天
发送推送通知失败	发送_推送_通知_失败	30 天
发送命令失败	发送_命令_失败	30 天
未找到设备	设备_未_发现	30 天

iOS MDM 服务器警告事件

下表显示具有“**警告**”严重级别的 Kaspersky Security Center iOS MDM 服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

iOS MDM 服务器警告事件

事件类型显示名称	事件类型	默认存储期限
检测到连接锁定移动设备的企图	不活动_设备_尝试_已连接	30 天
配置文件已被删除	MDM_配置文件_已_被删除	30 天
检测到重新使用客户端证书的企图	客户端_证书_已_在_使用	30 天
检测到不活动设备	发现_不活动_设备	30 天
兑换代码已请求	需要_兑换_码	30 天
配置文件已被包含到从设备删除的策略	UMDM_配置文件_已_被删除	30 天

iOS MDM 服务器信息事件

下表显示具有“**信息**”严重级别的 Kaspersky Security Center iOS MDM 服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

iOS MDM 服务器信息事件

事件类型显示名称	事件类型	默认存储期限
新移动设备已被连接	新_设备_已连接	30 天
配置文件列表已被成功请求	配置文件列表_命令_成功	30 天
配置文件已被成功安装	安装配置文件_命令_成功	30 天
配置文件已被成功删除	删除配置文件_命令_成功	30 天
Provisioning 配置文件列表已被成功请求	PROVISIONING 配置文件列表_命令_成功	30 天
Provisioning 配置文件已被成功安装	安装 PROVISIONING 配置文件_命令_成功	30 天
Provisioning 配置文件已被成功删除	删除 PROVISIONING 配置文件_命令_成功	30 天
数字证书列表已被成功请求	证书列表_命令_成功	30 天
已安装应用程序列表已被成功请求	已安装应用程序列表_命令_成功	30 天
移动设备常规信息已被成功请求	设备信息_命令_成功	30 天
安全信息已被成功请求	安全信息_命令_成功	30 天
移动设备已被成功锁定	设备锁_命令_成功	30 天
密码已被成功重置	清除密码_命令_成功	30 天
数据已被从移动设备成功擦除	擦除设备_命令_成功	30 天
应用已被成功安装	安装应用程序_命令_成功	30 天
兑换代码已为应用成功设置	应用兑换码_命令_成功	30 天
受管理应用列表已被成功请求	受管理应用程序列表_命令_成功	30 天
受管理应用已被成功删除	删除应用程序_命令_成功	30 天
漫游设置已被成功应用	设置漫游设置_命令_成功	30 天

阻止频繁事件

本节提供有关管理频繁事件阻止、移除对频繁事件的阻止以及将频繁事件列表导出到文件的信息。

关于阻止频繁事件

单个或多个受管理设备上安装的受管理应用程序（例如 Kaspersky Endpoint Security for Windows）可以将许多相同类型的事件发送到管理服务器。接收频繁事件可能会使管理服务器数据库超载并覆盖其他事件。当接收的事件总数超过指定的数据库限制时，管理服务器将开始阻止最频繁的事件。

管理服务器会自动阻止接收频繁事件。您自己不能阻止频繁事件，也不能选择要阻止的事件。

如果要了解某个事件是否被阻止，可以检查该事件是否出现在管理服务器属性的“**阻止频繁事件**”区域中。如果该事件被阻止，可以执行以下操作：

- 如果要防止覆盖数据库，可以继续阻止接收此类事件。
- 例如，如果要查找将频繁事件发送到管理服务器的原因，可以解除阻止频繁事件并继续接收此类事件。
- 如果要继续接收频繁事件直到它们被再次阻止，可以将它们从频繁事件的阻止中移除。

管理频繁事件阻止

管理服务器会自动阻止接收频繁事件，但是您可以停止阻止并继续接收频繁事件。您还可以阻止接收您以前解除阻止的频繁事件。

要管理对频繁事件的阻止：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单并选择“**属性**”。
2. 在管理服务器属性窗口中，转到“**区域**”窗格，然后选择“**阻止频繁事件**”。
3. 在“**阻止频繁事件**”区域中：
   - 选择要阻止接收的事件的“**事件类型**”选项。
   - 取消选择要继续接收的事件的“**事件类型**”选项。
4. 单击“**应用**”按钮。
5. 单击“**确定**”按钮。

管理服务器将接收您取消选择了“**事件类型**”选项的频繁事件，并阻止接收您选择了“**事件类型**”选项的频繁事件。

移除对频繁事件的阻止

您可以移除对频繁事件的阻止并开始接收它们，直到管理服务器再次阻止此类频繁事件。

要移除对频繁事件的阻止：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单并选择“**属性**”。
2. 在管理服务器属性窗口中，转到“**区域**”窗格，然后选择“**阻止频繁事件**”。
3. 在“**阻止频繁事件**”区域中，单击要移除阻止的频繁事件所在的行。
4. 单击“**删除**”按钮。

该频繁事件将从频繁事件列表中删除。管理服务器将接收此类事件。

将频繁事件列表导出到文件

要将频繁事件列表导出到文件：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单并选择“**属性**”。
2. 在管理服务器属性窗口中，转到“**区域**”窗格，然后选择“**阻止频繁事件**”。
3. 单击“**导出到文件**”按钮。
4. 在打开的“**另存为**”窗口中，指定要将列表保存到的文件的路径。
5. 单击“**保存**”按钮。

频繁事件列表上的所有记录都将导出到文件。

控制虚拟机状态的更改

管理服务器保存关于受管理设备的状态的信息，例如硬件注册表和已安装程序的列表，和受管理应用程序设置、任务和策略。如果虚拟机作为受管理设备，用户可以随时使用先前创建的虚拟机镜像功能还原其状态。这会造成管理服务器上的虚拟机状态信息不准确。

例如，管理员于中午 12:00 在管理服务器上创建了保护策略，此策略将于 12:01 开始在虚拟机 VM_1 上运行。在 12:30，VM_1 的用户使用于上午 11:00 创建的镜像还原了虚拟机，从而更改了其状态，则保护策略会在虚拟机上停止运行。但是，管理服务器上会存储此保护策略继续在 VM_1 上生效的错误信息。

Kaspersky Security Center 允许您监控在虚拟机状态上的所有更改。

当于每台设备同步后，管理服务器会生成一个独一无二的 ID，将其保存在设备和管理服务器。在启动下次同步前，管理服务器会比较两端的 ID 值。如果 ID 值不匹配，则管理服务器认为虚拟机已经从镜像还原。管理服务器会重置在此虚拟机上活动的所有策略和任务设置，并向其发送最新的策略和组任务。

使用系统注册表中的信息监控反病毒保护状态

若要使用网络代理记录的信息监控客户端设备上反病毒保护的状态，根据设备的操作系统，请执行以下操作：

- 在运行 Windows 的设备上：

  1. 打开客户端设备的系统注册表（例如，在本地**开始 → 运行**菜单中使用 regedit 命令）。
  2. 转至以下分支：

     - 对于 32 位系统：
       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState
     - 对于 64 位系统：
       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     系统注册表显示客户端设备反病毒保护状态的信息。

- 在运行 Linux 的设备上：

  - 信息包含在单独的文本文件中，每种数据类型一个文件，位于 /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/。

- 在运行 macOS 的设备上：

  - 信息包含在单独的文本文件中，每种数据类型一个文件，位于 /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/。

反病毒保护状态对应于下表中所述的键。

注册表键及其可能值

键（数据类型）	参数值	描述
`Protection_LastConnected (REG_SZ)`	DD-MM-YYYY HH-MM-SS	上次连接至管理服务器的时间和日期（UTC 格式）
`Protection_AdmServer (REG_SZ)`	IP、DNS 名称或 NetBIOS 名称	管理设备的管理服务器的名称
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	设备上安装的网络代理的版本号
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (patch1; patch2; ...; patchN)	设备上安装的网络代理版本（带补丁）的完整编号
`Protection_HostId (REG_SZ)`	设备 ID	设备的 ID
`Protection_DynamicVM (REG_DWORD)`	0 — 否 1 — 是	网络代理以动态 VDI 模式安装
`Protection_AvInstalled (REG_DWORD)`	0 — 否 1 — 是	安全应用程序安装在设备上
`Protection_AvRunning (REG_DWORD)`	0 — 否 1 — 是	实时保护在设备上启用
`Protection_HasRtp (REG_DWORD)`	0 — 否 1 — 是	已安装实时保护组件

键（数据类型）	参数值	描述
Protection_RtpState (REG_DWORD)	实时保护状态：	
	0	未知
	1	已禁用
	2	已暂停
	3	正在启动
	4	已启用
	5	启用高保护级别（最大保护）
	6	启用低保护级别（最快速度）
	7	启用默认（推荐）设置
	8	启用自定义设置
	9	操作失败
Protection_LastFscan (REG_SZ)	DD-MM-YYYY HH-MM-SS	上次全盘扫描时间和日期（UTC 格式）
Protection_BasesDate (REG_SZ)	DD-MM-YYYY HH-MM-SS	程序数据库发布时间和日期（UTC 格式）

当设备显示不活动时查看和配置操作

如果组中的客户端设备不活动，您可以获取关于它的通知。您也可以自动删除此类设备。

要在组中设备显示不活动时查看或配置操作：

1. 在控制台树，右击所请求的管理组名称。
2. 在上下文菜单中，选择**属性**。
   这将打开管理组属性窗口。
3. 在“**属性**”窗口，转到“**设备**”区域。
4. 如果需要，启用或禁用以下选项：

- **当设备处于非活动状态超过指定天数时，通知管理员**

  如果启用该选项，管理员接收不活动设备的通知。您可以指定**设备在网络上已长时间没有活动**事件被创建的时间间隔。默认时间间隔是 7 天。

  默认情况下已启用该选项。

- **当设备处于非活动状态超过指定天数时，从组中删除设备**

  如果启用该选项，您可以指定设备被从组中自动移除的时间间隔。默认时间间隔是 60 天。

  默认情况下已启用该选项。

- **从父组继承**

  该区域的设置将从包含客户端设备的父组继承。如果启用该选项，“**网络中的设备活动**”下的设置将被锁定以阻止更改。

该选项仅在管理组拥有父组时可用。
默认情况下已启用该选项。

- **强制子组继承**

  该设置值将被分发到子组，但在子组的属性中这些设置被锁定。
  默认情况下已禁用该选项。

5. 单击“**确定**”。

   您的更改已保存并应用。

禁用 Kaspersky 公告

在 Kaspersky Security Center Web Console 中，“Kaspersky 公告”区域（**监控和报告** → **Kaspersky 公告**）提供与您的 Kaspersky Security Center 版本和受管理设备上安装的受管理应用程序相关的信息，让您了解最新动态。如果您不想接收 Kaspersky 公告，可以禁用此功能。

Kaspersky 包括两种类型的信息：与安全相关的公告和营销公告。您可以单独禁用每种类型的公告。

要禁用与安全相关的公告：

1. 在控制台树中，选择要对其禁用安全相关公告的管理服务器。
2. 右键单击，然后在显示的上下文菜单中选择“**属性**”。
3. 在打开的管理服务器属性窗口的“**卡巴斯基通告**”区域，禁用“**启用在 Kaspersky Security Center Web Console 中显示卡巴斯基通告**”选项。
4. 单击“**确定**”。

   Kaspersky 公告已禁用。

默认情况下禁用营销公告。仅当启用卡巴斯基安全网络 (KSN) 时，才会收到营销公告。您可以通过禁用 KSN 来禁用此类型的公告。

分发点和连接网关的调整

Kaspersky Security Center 中的管理组结构运行以下功能：

- 设置策略范围

  将相关设置应用到设备还有一种方式：使用*策略配置文件*。此种情况下，策略范围使用标签、Active Directory 组织单元中的设备位置、Active Directory 安全组中的成员关系等进行设置。

- 设置组任务范围

  还有一个不基于管理组层级定义组任务范围的方法：使用设备分类的任务和特定设备的任务。

- 设置设备、虚拟管理服务器和从属管理服务器的访问权限。
- 分配分发点

当建立管理组结构时，您必须考虑到组织网络的拓扑以便最优分配分发点。分发点的最优分发允许您在企业网络中保存流量。

根据组织图表和网络拓扑，以下标准配置可以被应用到管理组结构：

- 单一办公室
- 多个小远程分办公室

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

分发点的标准配置：单一办公室

在标准"单一办公室"配置中，所有设备都在组织网络中，因此它们能看见彼此。组织网络可能包含几部分(网络或网段)，由窄通道连接。

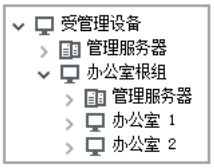
有以下构建管理组结构的方法：

- 构建管理组结构涉及到网络拓扑。管理组结构可能不精确反映网络拓扑。网络各部分之间以及特定管理组相互匹配。您可以使用分发点自动分配或手动分配它们。
- 不考虑网络拓扑而构建管理组结构。此种情况下，您必须禁用分发点自动分配，然后为网络中每个部分的根管理组分配一个或几个设备作为分发点，例如为"**受管理设备**"组。所有分发点将处于相同级别，并将掌控组织网络中所有设备的相同范围。此种情况下，每个网络代理都将连接到具有最短路由的分发点。分发点的路由可以使用 tracert 使用工具跟踪。

分发点的标准配置：多个小远程办公室

该标准配置可用于多个小型远程办公室，它们可能通过互联网与总部联络。每个远程办公室都位于 NAT 之外，就是说，从一个远程办公室到另一个远程办公室的连接是不可能的，因为办公室是彼此隔离的。

配置必须在管理组中体现：必须为每个远程办公室创建各自的管理组（下图中的组**办公室 1** 和**办公室 2**）。



远程办公室包含在管理组结构

必须指定一个或多个分发点给每个办公室的对应管理组。分发点必须是远程办公室中具有足够剩余磁盘空间的设备。部署在**办公室 1** 组的设备，例如，将访问分配到**办公室 1** 管理组的分发点。

如果一些用户在办公室之间移动他们的便携电脑，您必须在远程办公室选择两个或更多设备(除了现有的分发点)并分配它们作为等级管理组的分发点(上图中**办公室根组**)。

例如：便携式电脑部署在**办公室 1** 管理组，然后被移动到对应于**办公室 2** 管理组的办公室。在移动便携式电脑后，网络代理试图访问分配到**办公室 1** 组的分发点，但是那些分发点不可用。然后，网络代理开始尝试访问分配到**办公室根组**的分发点。因为远程办公室是彼此隔离的，尝试访问分配到**办公室根组**管理组的分发点仅在网络代理尝试访问**办公室 2** 组中的分发点时才会成功。就是说，便携式电脑将保持在原始办公室对应的管理组，但是将使用它当时所在办公室的分发点。

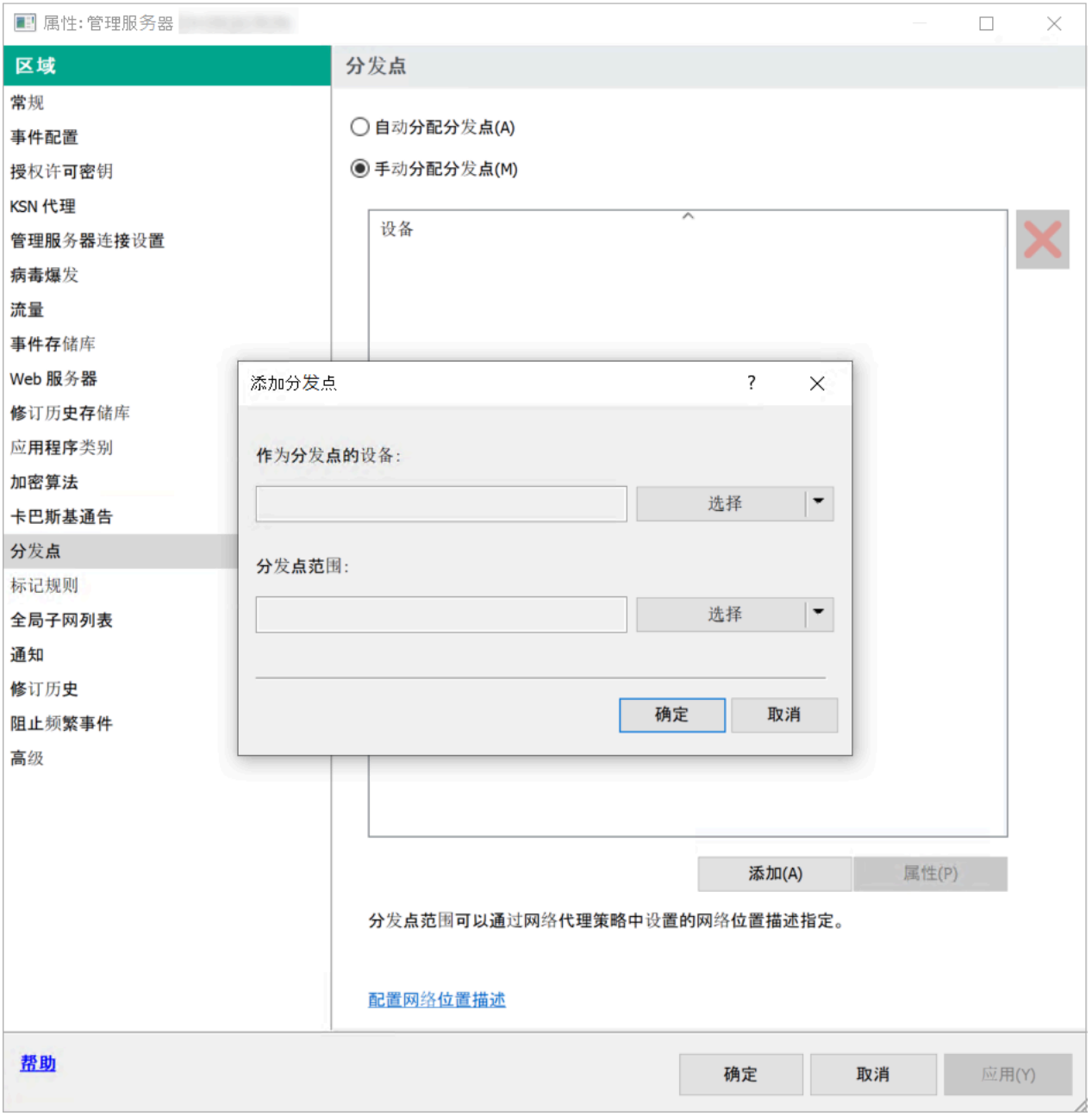
分配受管理设备作为分发点

您可以指定一台设备作为某个管理组的分发点，并在管理控制台中将其配置为连接网关。

要分配设备作为管理组的分发点：

1. 在控制台树中，选择**管理服务器**节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口，选择“**分发点**”区域。
4. 在窗口的右侧，选择“**手动分配分发点**”选项。

5. 单击“**添加**”按钮。



手动分配分发点

这会打开“**添加分发点**”窗口。

6. 在“**添加分发点**”窗口，执行以下操作：

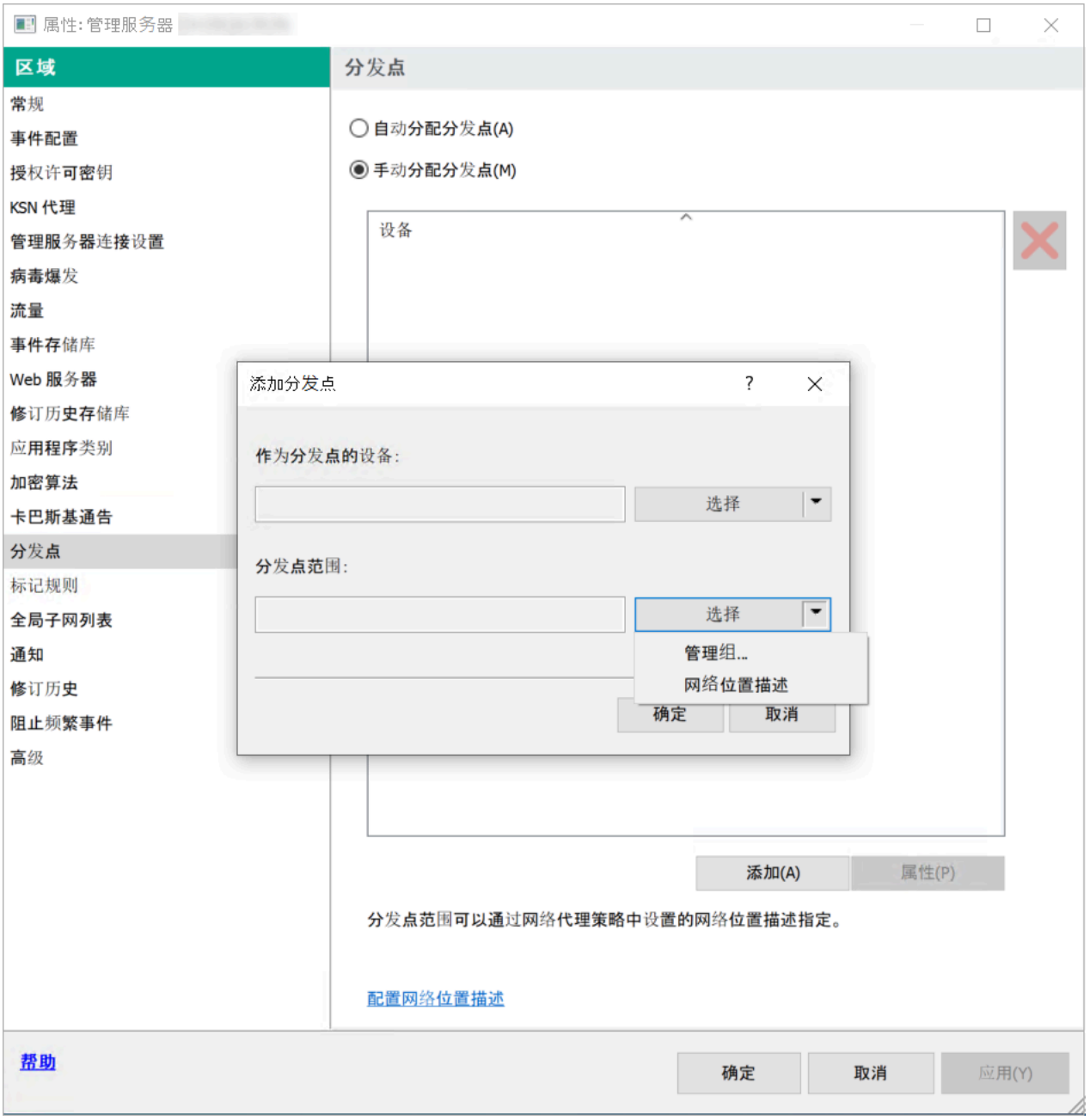
a. 在“**作为分发点的设备**”下，单击“**选择**”分割按钮上的向下（）箭头，然后选择“**从组中添加设备**”选项。

b. 在打开的“**选择设备**”窗口中，选择要用作分发点的设备。

c. 在**分发点范围**下，单击“**选择**”分割按钮上的向下箭头。

d. 指定分发点将向其分发更新的特定设备。您可以指定管理组或者网络位置描述。

e. 单击“**确定**”关闭“**添加分发点**”窗口。



选择分发点范围

您添加的分发点将显示在“**分发点**”区域的分发点列表中。

安装有网络代理并连接到虚拟管理服务器的第一台设备将自动指定为分发点，并配置为连接网关。

连接 Linux 设备作为隔离区域中的网关

要连接 Linux 设备作为隔离区域 (DMZ) 中的网关：

1. 在 Linux 设备上下载并安装网络代理。
2. 运行安装后脚本并按照向导操作以设置本地环境配置。在命令提示符下，运行以下命令：
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. 在询问网络代理模式的步骤中，选择“**用作连接网关**”选项。
4. 在基于 MMC 的管理控制台中，在管理服务器策略的上下文菜单中选择“**属性**”。
5. 在打开的管理服务器属性窗口中，选择“**分发点**”区域。
6. 在打开的“**分发点**”窗口的右侧：
   a. 选择“**手动分配分发点**”选项。
   b. 单击“**添加**”按钮。

   这会打开“**添加分发点**”窗口。
7. 在“**添加分发点**”窗口，执行以下操作：
   a. 在“**作为分发点的设备**”下，单击“**选择**”分割按钮上的向下箭头，然后选择“**按地址在 DMZ 中添加连接网关**”选项。
   b. 在**分发点范围**下，单击“**选择**”分割按钮上的向下箭头。
   c. 指定分发点将向其分发更新的特定设备。您可以指定一个管理组。
   d. 单击“**确定**”关闭“**添加分发点**”窗口。
8. 您添加的分发点将显示在“**分发点**”区域的分发点列表中。
9. 运行 klnagchk 实用程序以检查是否已成功配置与 Kaspersky Security Center 的连接。在命令提示符中，运行：
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
10. 在主菜单中，转到 Kaspersky Security Center 并发现设备。
11. 在打开的窗口中，单击“<设备名称>”。
12. 在下拉列表中，选择“**移至组**”链接。
13. 在打开的“**选择组**”窗口中，单击“**分发点**”链接。
14. 单击“**确定**”。
15. 在命令提示符中执行以下命令，以重启 Linux 客户端上的网络代理服务：
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

连接 Linux 设备作为 DMZ 中的网关完成。

之后，您可以通过配置的连接网关将 Linux 设备连接到管理服务器。仅在完成主要安装方案后再执行这些过程。

通过连接网关将 Linux 设备连接到管理服务器

连接网关可让您将客户端设备从隔离区 (DMZ) 连接到管理服务器。基于 Windows 和 Linux 的设备可以充当连接网关。连接并配置连接网关后，您可以使用此网关将 Linux 设备连接到管理服务器。仅在完成主要安装方案后再执行以下过程。

要通过连接网关将 Linux 设备连接到管理服务器，请在此设备上执行以下操作：

1. 在 Linux 设备上下载并安装网络代理。
2. 在命令提示符中执行以下命令来运行网络代理安装后脚本：
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. 在询问网络代理模式的步骤中，选择“**使用连接网关连接到服务器**”选项，然后输入连接网关的地址。
4. 在命令提示符中使用以下命令，检查与 Kaspersky Security Center 和连接网关的连接：
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   连接网关的地址显示在输出中。

通过连接网关将 Linux 设备连接到管理服务器已完成。您可以使用此设备更新分发、远程安装应用程序以及检索有关联网设备的信息。

在 DMZ 中添加连接网关作为分发点

连接网关等待来自管理服务器的连接，而不是建立与管理服务器的连接。这意味着在连接网关安装到 DMZ 中的某个设备上之后，管理服务器不会在受管理设备中列出该设备。因此，您需要一个特殊程序来确保管理服务器发起与连接网关的连接。

要添加具有连接网关的设备作为分发点：

1. 在控制台树中，选择**管理服务器**节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口，选择“**分发点**”区域。
4. 在窗口的右侧，选择“**手动分配分发点**”选项。
5. 单击“**添加**”按钮。
   这会打开“**添加分发点**”窗口。

6. 在“**添加分发点**”窗口，执行以下操作：

   a. 在“**作为分发点的设备**”下，单击“**选择**”分割按钮上的向下箭头( )，然后选择“**按地址添加 DMZ 连接网关**”选项。

   b. 在打开的“**输入连接网关地址**”窗口中，输入连接网关的 IP 地址（或者如果连接网关可通过名称访问，可输入名称）。

   c. 在**分发点范围**下，单击“**选择**”分割按钮上的向下箭头 。

   d. 指定分发点将向其分发更新的特定设备。您可以指定管理组或者网络位置描述。

      我们建议为外部受管理设备建立一个单独的组。

执行这些操作后，分发点列表包含一个名为“**连接网关的临时条目**”的新条目。

管理服务器几乎会立即尝试连接到您指定了地址的连接网关。如果成功，该条目的名称将更改为连接网关设备的名称。此过程最多需要 5 分钟。

在连接网关的临时条目转换为命名条目的同时，连接网关也会出现在“**未分配的设备**”组中。

要将连接网关添加到之前配置的网络，请在要连接到新添加的连接网关的设备上重新安装网络代理。

自动分配分发点

我们建议您自动分配分发点。Kaspersky Security Center 随后将自行选择必须为哪些设备分配分发点。

要自动分配分发点：

1. 打开主应用程序窗口。
2. 在控制台树中，选择包含要自动为其分配分发点的管理服务器名称的节点。
3. 在管理服务器的上下文菜单中，单击“**属性**”。
4. 在管理服务器属性窗口的“**区域**”窗格，选择“**分发点**”。
5. 在窗口的右侧，选择“**自动分配分发点**”选项。

   如果自动指派设备做为分发点被启用，您无法手动配置分发点，也不能编辑分发点列表。

6. 单击“**确定**”。

管理服务器便自动指派和配置分发点。

关于在选择用作分发点的设备上本地安装网络代理

要允许选为分发点的设备与虚拟管理服务器直接通信，然后作为连接网关，则必须在该设备上本地安装网络代理。

在充当分发点的设备上本地安装网络代理的过程与在任何网络设备上本地安装网络代理的过程相同。

要将设备选为分发点，下列条件必须满足：

- 在本地安装网络代理期间，在安装向导的“**管理服务器**”字段的“**服务器地址**”字段中，指定用来管理设备的虚拟管理服务器的地址。您可以使用设备 IP 地址或 Windows 网络中的设备名称。

  虚拟管理服务器地址使用下列格式：<虚拟服务器所属的物理管理服务器的完整地址>/<虚拟管理服务器的名称>。

- 因此，它可以充当连接网关的角色，打开该设备的所有端口以与管理服务器通信。

当带有指定设置的网络代理安装在设备上后，Kaspersky Security Center 将自动执行下列操作：

- 将此设备包含在虚拟管理服务器的“**受管理设备**”组中。
- 将此设备指定为虚拟管理服务器的“**受管理设备**”组的分发点。

在指定为组织网络“**受管理设备**”组的分发点的设备上本地安装网络代理非常有必要，而且也是足够的。您可以将网络代理远程安装在充当嵌套管理组中的分发点的设备上。为此，请使用“**受管理设备**”组的分发点作为连接网关。

关于使用分发点作为连接网关

如果管理服务器在隔离区 （DMZ） 以外，则该区域的网络代理无法连接管理服务器。

连接具有网络代理的管理服务器时，可使用分发点作为连接网关。分发点打开到管理服务器的端口用以创建连接。当管理服务器启动时，它连接到一个分发点并在整个会话期间维持该连接。

收到管理完全的信号后，分发点会向网络代理发送 UDP 信号，以便运行连接到管理服务器。网络代理收到该信号后会连接到分发点，这会在网络代理和管理服务器之间传输信息。信息交换可以通过 IPv4 或 IPv6 网络进行。

我们建议您使用特殊分配的设备作为连接网关并使用该连接网关覆盖最多 10,000 台客户端设备（包括移动设备）。

要将连接网关添加到先前配置的网络：

1. 以连接网关模式安装网络代理。
2. 在要连接到新添加的连接网关的设备上重新安装网络代理。

将 IP 范围添加到分发点轮询的范围列表中

您可以添加 IP 范围到分发点轮询的范围列表中。

要添加 IP 范围到轮询的范围列表：

1. 在控制台树中，选择**管理服务器**节点。
2. 在节点的上下文菜单中，选择“**属性**”。
3. 在打开的管理服务器属性窗口中，选择“**分发点**”区域。
4. 在列表中，选择必要的分发点，然后单击“**属性**”。
5. 在打开的分发点属性窗口的左侧“**区域**”窗格中，选择**设备发现** → **IP 范围**。
6. 选择“**启用范围轮询**”复选框。
7. 单击“**添加**”按钮。
   “**添加**”按钮仅在您选择了“**启用范围轮询**”复选框时才处于活动状态。
   “**IP 范围**”窗口将开启。
8. 在“**IP 范围**”窗口，输入新 IP 范围名称（默认名称是“新范围”）。
9. 单击“**添加**”按钮。
10. 执行以下操作之一：
    - 使用开始和结束 IP 地址指定 IP 范围。
    - 使用地址和子网掩码指定 IP 范围。
    - 点击**浏览**并从子网全局列表中选择子网。
11. 单击“**确定**”。
12. 单击“**确定**”添加带有指定名称的新范围。

    新范围将出现在轮询的范围列表中。

将分发点用作推送服务器

在 Kaspersky Security Center 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

推送服务器支持最多 50,000 个同时连接的负载。

您可能希望将分发点用作推送服务器，以确保受管理设备和管理服务器之间存在持续连接。某些操作需要持续连接，例如运行和停止本地任务、接收受管理应用程序的统计信息或创建隧道。如果将分发点用作推送服务器，则不必在受管理设备上使用“**不要断开与管理服务器的连接**”选项或将数据包发送到网络代理的 UDP 端口。

要将分发点用作推送服务器：

1. 在控制台树中，选择**管理服务器**节点。
2. 在节点的上下文菜单中，选择“**属性**”。
3. 在打开的管理服务器属性窗口中，选择“**分发点**”区域。
4. 在列表中，选择必要的分发点，然后单击“**属性**”。
5. 在打开的分发点属性窗口中，在“**区域**”窗格的“**常规**”区域中，选择“**将此分发点用作推送服务器**”选项。
6. 指定推送服务器端口号，即客户端设备将用于连接的分发点上的端口。
   默认情况下使用端口 13295。
7. 单击“**确定**”按钮退出分发点属性窗口。
8. 打开网络代理策略设置窗口。
9. 在“**连接**”区域中，转到“**网络**”子区域。
10. 在“**网络**”子区域中，选择“**使用分发点强制连接到管理服务器**”选项。
11. 单击“**确定**”按钮退出窗口。

该分发点将开始用作推送服务器。它现在可以向客户端设备发送推送通知。

如果管理安装了 KasperskyOS 的设备或计划这样做，则必须将分发点用作推送服务器。如果要向客户端设备发送推送通知，也可以将分发点用作推送服务器。

其他日常工作

该部分提供 Kaspersky Security Center 的常规使用建议。

管理管理服务器

本部分提供有关使用管理服务器和如何配置它们的信息。

创建管理服务器层级：添加从属管理服务器

您可以添加管理服务器作为从属管理服务器，从而建立“主/从属”层级。无论您要用于从属的管理服务器是否可以通过管理控制台连接，添加从属管理服务器都是可能的。

当组合两个管理服务器到一个层级，确保端口 13291 在两个管理服务器上都可以访问。端口 13291 用以接收从管理控制台到管理服务器的连接。

连接新管理服务器作为主管理服务器的从属

您可以通过连接其到主管理服务器的端口 13000 来添加管理服务器作为从属。您将需要一个安装了管理控制台的设备，其 TCP 端口 13291 可以被两个管理服务器访问：假定主管理服务器和假定从属管理服务器。

要添加可以通过管理控制台连接的管理服务器作为从属：

1. 确保假定主管理服务器的端口 13000 可用于从从属管理服务器接收连接。
2. 使用管理控制台连接到假定主管理服务器。
3. 选择您要将从属管理服务器添加到的管理组。
4. 在所选组的“**管理服务器**”节点的工作区，单击“**添加从属管理服务器**”链接。

   “添加从属管理服务器向导”启动。
5. 在向导的第一步（输入正在添加到组的管理服务器的地址），输入假定从属管理服务器的网络名称。
6. 遵照向导的说明操作。

“主/从属”层级被创建。主管理服务器将接收从属管理服务器的连接。

如果您没有设备安装了管理控制台，且 TCP 端口 13291 可以在两个管理服务器上访问（例如，如果假定从属管理服务器位于远程办公室且该办公室的系统管理员出于安全原因无法打开到端口 13291 的互联网访问），您将仍可以添加从属管理服务器。

要添加不能通过管理控制台连接的管理服务器作为从属：

1. 确保假定主管理服务器的端口 13000 可用于接收从属管理服务器的连接。
2. 将假定主管理服务器证书写入外部设备，例如闪存驱动器，或将其发送到管理服务器所在的远程办公室的系统管理员。

   管理服务器证书位于相同的管理服务器，在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer。
3. 将假定从属管理服务器的证书写入外部设备，例如闪存驱动器。如果假定从属管理服务器位于远程办公室，联系该办公室的系统管理员以提醒他/她给您发送证书。

   管理服务器证书位于相同的管理服务器，在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer。
4. 使用管理控制台连接到假定主管理服务器。
5. 选择您要将从属管理服务器添加到的管理组。

6. 在“**管理服务器**”节点的工作区，单击“**添加从属管理服务器**”链接。
   “添加从属管理服务器向导”启动。
7. 在向导的第一步（输入地址），置“**从属管理服务器地址(可选)**”字段为空。
8. 在“**从属管理服务器证书文件**”窗口，单击“**浏览**”按钮并选择您保存的从属管理服务器的证书文件。
9. 当向导完成时，使用管理控制台的不同实例连接到假定从属管理服务器。如果管理服务器位于远程办公室，联系该办公室的系统管理员以提醒他/她连接到假定从属管理服务器并执行进一步操作。
10. 在“**管理服务器**”节点的上下文菜单中，选择“**属性**”。
11. 在管理服务器属性中，转到“**高级**”区域，然后转到“**管理服务器层级**”子区域。
12. 选中**该管理服务器是服务器层级中的从属**复选框。
    输入字段可用于数据输入和编辑。
13. 在“**主管理服务器地址**”字段中，输入假定主管理服务器的网络名称。
14. 通过单击“**浏览**”按钮选择先前保存的带有假定主管理服务器证书的文件。
15. 单击“**确定**”。

“主/从属”层级被创建。您可以通过管理控制台连接到从属管理服务器。主管理服务器将接收从属管理服务器的连接。

连接主管理服务器到从属管理服务器

您可以添加新管理服务器作为从属，以便主管理服务器通过端口 13000 连接到从属管理服务器。例如，如果在 DMZ 中放置从属管理服务器，则这样做是可取的。

您将需要一个安装了管理控制台的设备，其 TCP 端口 13291 可以被两个管理服务器访问：假定主管理服务器和假定从属管理服务器。

要添加新管理服务器作为从属并通过端口 13000 连接主管理服务器：

1. 确保假定从属管理服务器的端口 13000 可用于从假定主管理服务器接收连接。
2. 使用管理控制台连接到假定主管理服务器。
3. 选择您要将从属管理服务器添加到的管理组。
4. 在相关管理组的“**管理服务器**”节点的工作区，单击“**添加从属管理服务器**”链接。
   “添加从属管理服务器向导”启动。
5. 在向导的第一步（输入要添加到组的管理服务器的地址），输入假定从属管理服务器的网络名称并选择“**连接主管理服务器到 DMZ 中的从属管理服务器**”复选框。
6. 如果您使用代理服务器连接到假定从属管理服务器，则在向导的第一步选择“**使用代理服务器**”复选框并指定连接设置。
7. 遵照向导的说明操作。

管理服务器层级被创建。从属管理服务器将接收主管理服务器的连接。

连接至管理服务器以及在管理服务器之间切换

启动 Kaspersky Security Center 后，它将尝试连接至管理服务器。如果网络中有多个管理服务器可用，则程序会请求在 Kaspersky Security Center 的上一次会话期间连接的服务器。

当程序在安装后首次启动时，它会尝试连接至在 Kaspersky Security Center 安装过程中指定的管理服务器。

在建立与管理服务器的连接之后，该服务器的文件夹树将显示在控制台树中。

如果已经将多个管理服务器添加至控制台树，您可以在它们之间进行切换。

管理控制台用于每个管理服务器。在第一次连接到新管理服务器之前，确保从管理控制台接收连接的端口 13291 被打开，以及所有用于管理服务器和其他 Kaspersky Security Center 组件间交互的剩余端口。

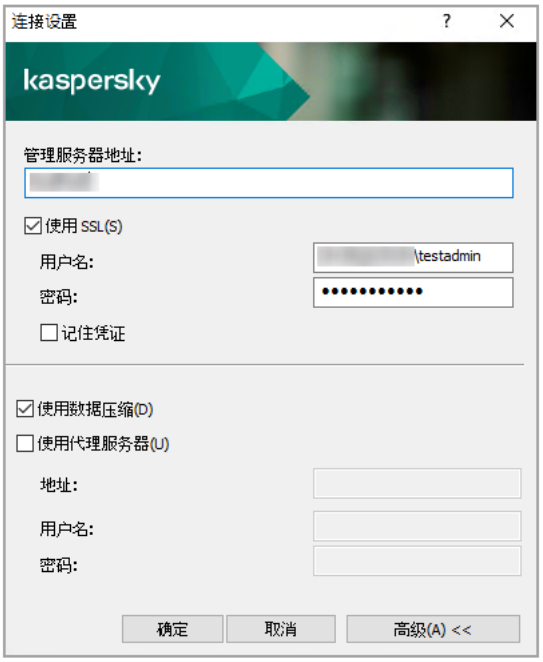
要切换到其他管理服务器，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的上下文菜单中，选择“**连接到管理服务器**”。
3. 在打开的“**连接设置**”窗口中的“**管理服务器地址**”字段，指定您想要连接的管理服务器的名称。您可以指定一个 IP 地址或 Windows 网络中设备的名称作为管理服务器的名称。您可单击“**高级**”按钮配置与管理服务器的连接（请参见下图）。

   要通过与默认端口不同的端口连接到管理服务器，请采用 <管理服务器名称>:<端口> 格式在“**管理服务器地址**”字段中输入值。

   要连接到虚拟管理服务器，请在**管理服务器地址**字段中以 <管理服务器地址>/<虚拟服务器名称> 格式输入值。

没有“**读取**”权限的用户将被拒绝访问管理服务器。



连接至管理服务器

4. 单击“**确定**”可完成在服务器之间的切换。

连接管理服务器之后，程序将更新控制台树中相应节点的文件夹树。

访问管理服务器及其对象的权限

在 Kaspersky Security Center 安装期间，程序会自动创建 **KLAdmins** 和 **KLOperators** 组。这些组被授予连接至管理服务器和处理管理服务器对象的权限。

根据安装 Kaspersky Security Center 时使用的账户类型，系统会创建如下所示的 **KLAdmins** 和 **KLOperators** 组：

- 如果应用程序是在域内包含的用户账户下安装的，则系统会在管理服务器上和包含管理服务器的域内同时创建这些组。
- 如果应用程序是在系统账户下安装的，则系统仅会在管理服务器上创建这些组。

您可以使用操作系统的标准管理工具查看 **KLAdmins** 和 **KLOperators** 组，并且可以修改属于 **KLAdmins** 和 **KLOperators** 组的用户的访问权限。

KLAdmins 组被授予所有访问权限，**KLOperators** 组仅被授予“读取”和“执行”权限。授予 **KLAdmins** 组的权限被锁定。

属于 **KLAdmins** 组的用户称为 *Kaspersky Security Center 管理员*；**KLOperators** 组的用户称为 *Kaspersky Security Center 操作员*。

除 **KLAdmins** 组包含的用户外，系统还会将 Kaspersky Security Center 的管理员权限授予安装有管理服务器的设备的本地管理员。

您可以将本地管理员从拥有 Kaspersky Security Center 管理员权限的用户列表中排除。

所有由 Kaspersky Security Center 管理员启动的操作都将使用管理服务器账户的权限执行。

可通过网络为每个管理服务器创建单独的 **KLAdmins** 组；该组将仅具有该管理服务器所必需的权利。

如果属于相同域的设备被包括在不同管理服务器的管理组中，则域管理员是所有组的 Kaspersky Security Center 管理员。对于这些管理组而言，**KLAdmins** 组是相同的；该组是在安装第一个管理服务器期间创建的。Kaspersky Security Center 管理员启动的所有操作都使用已为其启动这些操作的管理服务器的账户权限执行。

安装应用程序之后，Kaspersky Security Center 的管理员可以：

- 修改授予 **KLOperators** 组的权限。
- 将访问 Kaspersky Security Center 功能的权限授予其他安全组和管理员工作站中注册的单个用户。
- 在每个管理组中分配用户访问权限。

Kaspersky Security Center 管理员可以在选定对象的属性窗口中的“**安全性**”区域中将访问权限分配给每个管理组或管理服务器的其他对象。

您可以使用管理服务器操作中的事件记录跟踪用户活动。事件记录显示在“**事件**”选项卡上的“**管理服务器**”节点中。这些事件具有重要级别“**信息事件**”；事件类型以“**Audit**”开头。

通过互联网连接至管理服务器的条件

如果管理服务器是位于企业网络外部的远程服务器，则客户端设备可通过互联网与其连接。

对于要通过互联网连接到管理服务器的设备，必须满足以下条件：

- 远程管理服务器必须拥有外币 IP 地址且接收端口 13000 必须保持打开（为了连接网络代理）。我们建议您也打开 UDP 端口 13000（为了接收设备关闭通知）。
- 应该首先在设备上安装网络代理。
- 在设备上安装网络代理时，您应该指定远程管理服务器的外部 IP 地址。如果使用安装包进行安装，则在“**设置**”区域的安装包属性中手动指定外部 IP 地址。
- 要使用远程管理服务器来管理设备的应用程序和任务，请在“**常规**”区域中该设备的属性窗口中，选中“**不断开与管理服务器的连接**”复选框。选中该选框之后，请等待管理服务器与远程设备同步。与管理服务器保持连接的客户端设备的数量不得超过 300。

要提高远程管理服务器启动任务的性能，您可以在设备上打开端口 15000。在此情况下，要运行任务，管理服务器将通过端口 15000 向网络代理发送一个专用数据包，而不是等待与设备的同步完成。

到管理服务器的加密连接

您可以使用 TLS（传输层安全）协议来进行客户端设备与管理服务器的数据交换，以及管理控制台与管理服务器的连接。TLS 协议能够识别交互方、将传输数据加密并防止数据在传输过程中被篡改。TLS 协议使用公钥对交互方和加密数据进行身份验证。

当设备连接时验证管理服务器

在客户端设备首次连接到管理服务器时，设备上的网络代理会下载管理服务器证书的副本并将其存储在本地。

如果您在设备本地安装网络代理，您可以手动选择管理服务器证书。

下载的证书将用于在以后的连接中验证管理服务器权限。

在以后的会话中，网络代理将在每次设备与管理服务器连接时请求管理服务器证书，并将其与本地副本进行比较。如果副本不一致，设备将不允许访问管理服务器。

在管理控制台连接期间的管理服务器身份验证

在首次连接管理服务器时，管理控制台将请求管理服务器证书并将其本地保存在管理员工作站中。此后，每次管理控制台尝试连接管理服务器时，均将基于该证书副本验证管理服务器。

如果管理服务器证书与保存在管理员工作站中的副本不符，管理控制台将提示您验证与指定名称的管理服务器之间连接的选择，并下载新的证书。建立连接后，管理控制台将保存新管理服务器证书副本，并在将来用其验证管理服务器。

配置允许连接到管理服务器的 IP 地址允许列表

默认情况下，用户可以在任何可以打开 Kaspersky Security Center Web Console（以下简称 Web Console）或安装了基于 MMC 的管理控制台的设备上登录 Kaspersky Security Center。但是，您可以配置管理服务器，使用户只能从具有允许 IP 地址的设备进行连接。在这种情况下，即使入侵者窃取了 Kaspersky Security Center 账户，也无法登录 Kaspersky Security Center，因为入侵者设备的 IP 地址不在允许列表中。

当用户登录 Kaspersky Security Center 或运行通过 Kaspersky Security Center OpenAPI 与管理服务器交互的应用程序时，将验证 IP 地址。此时，用户的设备尝试与管理服务器建立连接。如果设备的 IP 地址不在允许列表中，则会发生身份验证错误，并且 KLAUD_EV_SERVERCONNECT 事件将通知您尚未建立与管理服务器的连接。

IP 地址允许列表的要求

仅当以下应用程序尝试连接到管理服务器时才会验证 IP 地址：

- Web Console Server

  如果您在一台设备上登录 Web Console，而 Web Console Server 安装在另一台设备上，您可以使用操作系统的标准方式在安装了 Web Console Server 的设备上配置防火墙。然后，如果有人试图登录 Web Console，防火墙将帮助阻止入侵者干扰。

- 管理控制台

- 通过 klakaut 自动化对象与管理服务器交互的应用程序
- 通过 OpenAPI 与管理服务器交互的应用程序，例如 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization

因此，请指定安装了上述应用程序的设备的地址。

您可以设置 IPv4 和 IPv6 地址。您不能指定 IP 地址范围。

如何建立 IP 地址允许列表

如果您之前未设置允许列表，请按照下面的说明操作。

要建立用于登录 Kaspersky Security Center 的 IP 地址允许列表：

1. 在管理服务器设备上，在具有管理员权限的账户下运行命令提示符。
2. 将当前目录更改为 Kaspersky Security Center 安装文件夹（通常为 <磁盘>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）。
3. 使用管理员权限输入以下命令：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 地址>" -t s`

   指定满足上述要求的 IP 地址。多个 IP 地址必须用分号隔开。

   如何只允许一台设备连接到管理服务器的示例：

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   如何允许多台设备连接到管理服务器的示例：

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`
4. 重启管理服务器服务。

您可以在管理服务器上的卡巴斯基事件日志中查看您是否已成功配置 IP 地址允许列表。

如何更改 IP 地址允许列表

您可以像第一次建立允许列表那样进行更改。为此，请运行相同的命令并指定一个新的允许列表：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 地址>" -t s
```

如果要从允许列表中删除某些 IP 地址，请将其重写。例如，您的允许列表包括以下 IP 地址：192.0.2.0; 198.51.100.0; 203.0.113.0。您要删除 198.51.100.0 IP 地址。为此，在命令提示符处输入以下命令：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

不要忘记重新启动管理服务器服务。

如何重置已配置的 IP 地址允许列表

要重置已配置的 IP 地址允许列表：

1. 使用管理员权限在命令提示符处输入以下命令：
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s
   ```
2. 重启管理服务器服务。

之后，不再验证 IP 地址。

使用 klscflag 实用程序关闭端口 13291

管理服务器上的端口 13291 用于接收来自管理控制台的连接。此端口默认开放。如果您不想使用基于 MMC 的管理控制台或 klakaut 实用程序，可以使用 klscflag 实用程序关闭此端口。此实用程序会更改 KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN 参数的值。

要关闭端口 13291：

1. 使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。
2. 在命令行中执行以下命令：
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```
3. 重启 Kaspersky Security Center 管理服务器服务。

端口 13291 即关闭。

要检查端口 13291 是否已成功关闭：

在命令行中执行以下命令：

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

此命令会返回以下结果：

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

`false` 值表示端口已关闭。否则，将显示 `true` 值。

断开与管理服务器的连接

要与管理服务器断开连接，请执行以下操作：

1. 在控制台树中，选择与想要断开连接的管理服务器相对应的节点。
2. 在节点的上下文菜单中，选择“**断开与管理服务器的连接**”。

将管理服务器添加至控制台树

要将管理服务器添加至控制台树，请执行以下操作：

1. 在 Kaspersky Security Center 主窗口，在控制台树选择“**Kaspersky Security Center**”节点。
2. 在该节点的上下文菜单中，选择**新建 → 管理服务器**。

程序将在控制台树中创建一个名为“**管理服务器- <设备名称> （未连接）**”的节点，您可以从该节点连接至安装在网络中的任何管理服务器。

从控制台树中删除管理服务器

要从控制台树中删除管理服务器，请执行以下操作：

1. 在控制台树中，选择与想要删除的管理服务器相对应的节点。
2. 在该节点的上下文菜单中，选择“**删除**”。

将虚拟管理服务器添加至控制台树

要将虚拟管理服务器添加至控制台树，请执行以下操作：

1. 在控制台树中，选择您要为其创建虚拟管理服务器的管理服务器节点。
2. 在管理服务器节点，选择“**管理服务器**”文件夹。
3. 在“**管理服务器**”文件夹的工作区，单击“**添加虚拟管理服务器**”链接。

   此操作将启动“新虚拟管理服务器向导”。
4. 在“**虚拟管理服务器名称**”窗口，指定要创建的虚拟管理服务器名称。

   虚拟管理服务器名称不能包含多于 255 个字符并且不能包括任何特殊字符（"*<>?\:|）。
5. 在“**输入设备到虚拟管理服务器的连接地址**”窗口中，特定设备连接地址

   虚拟管理服务器的连接地址是设备通过其连接到服务器的网络地址。连接地址有两部分：物理管理服务器的网络地址和虚拟管理服务器的名称，以斜线分割。虚拟管理服务器名称将被自动附加。指定的地址将被用于虚拟管理服务器网络代理安装包的默认地址。
6. 在“**创建虚拟管理服务器管理员账户**”窗口，从列表分配用户作为虚拟服务器管理员，或通过单击“**创建**”按钮添加新管理员账户。

   您可以指定多个账户。

名为**管理服务器 <虚拟管理服务器名称>**的节点被创建在控制台树。

更改管理服务器服务账户实用工具 klsrvswch

如果您必须更改在安装 Kaspersky Security Center 时设置的管理服务器服务账户，您可以使用一个名为 klsrvswch 的实用程序，它设计用来更改管理服务器账户。

安装 Kaspersky Security Center 后，该实用程序将被自动复制到程序安装文件夹中。

运行该实用程序的次数不受限制。

您必须使用安装管理服务器时所用的具有管理员权限的账户在管理服务器设备上启动 klsrvswch 实用程序。

klsrvswch 实用程序允许您更改账户类型。例如，如果您使用本地账户，您可以将其更改到域账户或受管理设备账户（反之亦然）。klsrvswch 实用程序不允许您将账户类型更改为组托管服务账户 (gMSA)。

Windows Vista 和后续 Windows 版本不允许对管理服务器使用 LocalSystem 账户。在这些 Windows 版本中，**LocalSystem 账户**选项不被激活。

要更改管理服务器服务账户到域账户，请执行以下操作：

1. 从 Kaspersky Security Center 的安装文件夹运行 klsrvswch 实用程序。默认安装路径：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   该操作还会启动修改管理服务器服务账户的向导。遵照向导的说明操作。

2. 在**管理服务器服务账户**窗口，选择**LocalSystem 账户**。

   在向导结束其操作后，管理服务器账户将更改。管理服务器服务将在“*LocalSystem 账户*”下启动并使用其证书。

要使 Kaspersky Security Center 正确操作，要求用于启动管理服务器服务的账户对承载管理服务器数据库的资源拥有管理员权限。

要更改管理服务器服务账户到用户账户或受管理服务账户：

1. 从 Kaspersky Security Center 的安装文件夹运行 klsrvswch 实用程序。默认安装路径：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   该操作还会启动修改管理服务器服务账户的向导。遵照向导的说明操作。

2. 在**管理服务器服务账户**窗口，选择**自定义账户**。

3. 单击“**立即查找**”按钮。

   “**选择**”窗口将打开。

4. 在**选择用户**窗口，点击**对象类型**按钮。

5. 在对象类型列表，选择**用户**（如果您想要用户账户）或**服务账户**（如果您想要受管理服务账户）并点击**确定**。

6. 在对象名称列表，输入账户名称，或者名称的一部分，并点击**检查名称**。
7. 在匹配名称列表，选择必要的名称，然后点击**确定**。
8. 如果您在**账户密码**窗口选择了**服务账户**，保留**密码**和**确认密码**字段为空。如果您选择了**用户**，输入用户新密码并确认。

管理服务器服务账户将被更改到您选择的账户。

在预先假定的使用 Windows 工具对用户账户进行身份验证的模式下使用 Microsoft SQL Server 时，应该授予其访问数据库的权限。用户账户需要有 Kaspersky Security Center 数据库所有者的权限。默认情况下使用 dbo 方案。

更改 DBMS 凭据

您可能需要更改 DBMS 凭据，例如，出于安全目的执行凭据循环。

要在 Windows 环境下使用 klsrvswch.exe 更改 DBMS 凭据：

1. 启动位于 Kaspersky Security Center 安装文件夹的 klsrvswch 实用程序。默认安装路径：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   您必须使用安装管理服务器时所用的具有管理员权限的账户在管理服务器设备上启动 klsrvswch 实用程序。

2. 单击向导的“**下一步**”按钮，直到到达“**更改 DBMS 访问凭证**”步骤。
3. 在向导的“**更改 DBMS 访问凭证**”步骤，执行以下操作：

   如果使用 Windows 身份验证，则将跳过向导的**更改 DBMS 访问凭证**步骤。

   - 选择**应用新凭证**选项。
   - 在“**账户**”字段中指定一个新的账户名。
   - 在“**密码**”字段中为账户指定新密码。
   - 在“**确认密码**”字段中指定新密码。

   您应该指定 DBMS 中存在的账户的凭据。

4. 单击“**下一步**”按钮。

向导完成后，DBMS 凭据即被更改。

klsrvswch 实用程序只能用于更改 SQL 身份验证的账户密码。不支持更改授权方法。要更改授权方法，请重新安装管理服务器并指定所需的设置。

更改管理服务器共享文件夹

管理服务器共享文件夹在管理服务器安装期间指定。您也可以在管理服务器属性中指定共享文件夹位置。

要更改共享文件夹：

1. 创建网络共享文件夹并配置共享和文件夹结构的权限，以允许**Everyone**子组拥有完全控制权限。
2. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单并选择“**属性**”。
3. 在管理服务器属性窗口的“**区域**”窗格中，选择“**高级**”，然后选择“**管理服务器共享文件夹**”。
4. 在“**管理服务器共享文件夹**”区域中，单击“**更改**”按钮。
5. 选择要用作共享文件夹的文件夹。
6. 单击“**确定**”按钮以关闭管理服务器属性窗口。
7. 为选择用作共享文件夹的文件夹分配 **Everyone** 子组的读取权限。

使用管理服务器节点解决问题

管理控制台左侧面板的控制台树包含管理服务器节点。您可以任意多的管理服务器到控制台树。

控制台树中的管理服务器节点列表通过 Microsoft 管理控制台存储在 .msc 文件的卷影副本中。该文件的卷影副本位于管理控制台设备的 %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ 文件夹。对于每个管理服务器节点，文件包含以下信息：

- 管理服务器地址
- 端口号
- 是否使用 TLS

  该参数取决于用于连接管理控制台到管理服务器的端口号。
- 用户名
- 管理服务器证书

故障解决

当管理控制台连接管理服务器时，本地存储的证书与管理服务器证书相比较。如果证书不匹配，管理控制台生成错误。例如，证书不匹配可能发生在您替换管理服务器证书时。此种情况下，在控制台重新创建管理服务器节点。

要重新创建管理服务器节点：

1. 关闭 Kaspersky Security Center 管理控制台窗口。
2. 删除位于 %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ 的 Kaspersky Security Center 15.1 文件。

3. 运行 Kaspersky Security Center 管理控制台。
   您将被提示连接到管理服务器并接受现有证书。

4. 执行以下操作之一：

   - 通过点击**是**按钮接受现有证书。
   - 要指定您的证书，点击**否**按钮，然后浏览到用于验证管理服务器的证书文件。

证书问题被解决。您可以使用管理控制台连接到管理服务器。

查看和修改管理服务器的设置

您可以在管理服务器的属性窗口中调整其设置。

要打开"属性：管理服务器"窗口，

请在控制台树中管理服务器节点的上下文菜单中选择**属性**。

调整管理服务器的常规设置

您可以在管理服务器属性窗口的"**常规**"、"**管理服务器连接设置**"、"**事件存储库**"和"**安全性**"区域调整管理服务器的常规设置。

如果"**安全性**"区域的显示在管理控制台界面上被禁用，则它不会显示在管理服务器属性窗口。

*要在管理控制台启用"**安全性**"区域的显示：*

1. 在控制台树中，选择您需要的管理服务器。
2. 在主应用程序窗口的**视图**菜单，选择"**配置界面**"。
3. 在打开的"**配置界面**"窗口，选择"**显示安全设置区域**"复选框并点击"**确定**"。
4. 在带有应用程序消息的窗口，点击"**确定**"。

"**安全性**"区域将显示在管理服务器属性窗口。

管理控制台界面设置

您可以调整管理控制台的界面设置，以显示或隐藏与以下功能相关的用户界面控件：

- 漏洞和补丁管理
- 数据加密和保护
- 端点控制设置
- 移动设备管理

- 从属管理服务器
- 安全设置部分

要配置管理控制台界面设置：

1. 在控制台树中，选择您需要的管理服务器。
2. 在主应用程序窗口的**查看**菜单，选择“**配置界面**”。
3. 在打开的“**配置界面**”窗口中，选中要显示的功能旁边的复选框，然后点击“**确定**”。
4. 在带有应用程序消息的窗口，点击“**确定**”。

所选功能将显示在管理控制台界面中。

在管理服务器上的事件处理和存储

关于应用程序和受管理设备运行过程中发生的事件的信息保存在管理服务器数据库中。每个事件都归属于特定类型和严重级别（*严重事件*、*功能失败*、*警告*或*信息*）。基于事件发生的条件，应用程序可以分配不同的严重级别到相同类型的事件。

您可以在管理服务器属性窗口的**事件配置**部分查看分配给事件的类型和严重级别。在**事件配置**部分，您也可以配置管理服务器对每个事件的处理：

- 在管理服务器、设备 OS 事件日志和管理服务器计算机 OS 事件日志中注册事件。
- 通知管理员事件的方法（例如，SMS 或者邮件消息）。

在管理服务器属性窗口的“**事件存储库**”区域，您可以通过限制事件记录数和存储期限来编辑管理服务器数据库的事件存储设置。当您指定事件最大数时，应用程序计算用于指定数目的存储空间的大概大小。您可以使用该大概计算来评估您在磁盘上是否具有足够空间以避免数据库溢出。管理服务器数据库的默认容量是 400,000 个事件。最大建议的数据库容量是 45,000,000 个事件。

应用程序每 10 分钟检查一次数据库。如果事件数达到指定的最大值加 10,000，应用程序将删除最旧的事件，以便仅保留指定的最大事件数。

当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入卡巴斯基事件日志。新事件被列队，然后在删除操作后被保存到数据库。

您可以更改任何任务的设置以保存与任务进度相关的事件，或者仅保存任务执行结果。为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

查看连接到管理服务器的日志

操作期间的连接历史和到管理服务器的连接尝试可以被保存到文件。文件中的信息允许您不仅跟踪网络基础架构中的连接，还有非授权的到管理服务器的访问尝试。

要记录连接管理服务器事件：

1. 在控制台树中，选择您要为其启用连接事件记录的管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。

3. 在打开的属性窗口“**管理服务器连接设置**”区域中，选择“**连接端口**”子区域。

4. 启用**记录管理服务器连接事件**选项。

5. 单击“**确定**”按钮以关闭管理服务器属性窗口。

所有连入管理服务器的后续事件、身份验证结果和 SSL 错误将被保存到 %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog 文件。

控制病毒爆发

Kaspersky Security Center 允许您对病毒爆发威胁做出快速响应。病毒爆发风险通过监控设备上的病毒活动来评估。

您可以配置病毒爆发威胁和采取行动的评估规则；为此，请使用管理服务器属性窗口的“**病毒爆发**”区域。

您可以在管理服务器属性窗口“**事件配置**”区域的*病毒爆发*事件属性窗口中指定*病毒爆发*事件的通知过程。

在安全应用程序操作中，当*检测到恶意对象*事件发生时，*病毒爆发*事件便被生成。因此，您必须保存管理服务器上所有的*检测到恶意对象*事件的信息，从而识别病毒爆发。

您可以在安全应用程序的策略中指定保存关于“*检测到恶意对象*”事件信息的设置。

在对“*检测到恶意对象*”事件进行计数时，程序将仅考虑来自主管理服务器的设备的信息。来自从属管理服务器的信息将不予考虑。对于每个从属服务器，程序都将单独配置*病毒爆发*事件设置。

限制流量

为减少网络中的流量，程序提供了相应的选项，以便限制从指定的 IP 范围和 IP 子网向管理服务器传送数据的速度。

您可以在管理服务器属性窗口的“**流量**”区域中创建和配置流量限制规则。

要创建流量限制规则：

1. 在控制台树中，选择您要为其创建流量限制规则的管理服务器节点。

2. 在管理服务器的上下文菜单中，选择“**属性**”。

3. 在“管理服务器属性”窗口中，选择“**流量**”区域。

4. 单击“**添加**”按钮。

5. 在“**新规则**”窗口，指定以下设置：

   在“**限制流量的 IP 范围**”区域中，您可以选择用于定义限制数据传送速度的子网或范围的方法，然后为选定的方法输入设置值。您可以选择以下方法之一：

   - **使用地址和网络掩码指定范围**

     流量基于子网设置被限制。指定子网地址和子网掩码以定义限制流量的范围。

您也可以点击**浏览**以从子网全局列表添加子网。

- **使用开始和结束地址指定范围**

  流量基于 IP 地址范围被限制。在**开始**和**结束**输入字段指定 IP 地址范围。
  默认情况下已选中该选项。

在“**流量限制**”区域，您可以调整以下数据传输率的限制设置：

- **时间间隔**

  将要实施流量限制的时间段。您可以在输入字段指定时间间隔界限。

- **限制(KB/S)**

  管理服务器的传入和传出数据的最大传输速度。流量限制将在“**时间间隔**”字段中指定的时间间隔内实施。

- **限制剩余时间的流量(KB/S)**

  程序将不仅在“**时间间隔**”字段中指定的时间间隔内限制流量，在其它时间也 同样。
  默认情况下已清除该选框。该字段的值可能与**限制(KB/s)**字段的值不匹配。

首先，流量限制规则影响文件传输。这些规则不应用到管理服务器和网络代理以及主从管理服务器之间的同步产生的流量。

配置 web 服务器

Web 服务器用于发布独立安装包、iOS MDM 配置文件、以及共享文件夹的文件。

您可以定义 Web 服务器连接至管理服务器的设置，也可在管理服务器属性窗口的“**Web 服务器**”区域中设置 Web 服务器证书。

使用内部用户

*内部用户*的账户可用于操作虚拟管理服务器。Kaspersky Security Center 授权应用程序的内部用户拥有真实用户的所有权限。

只能在 Kaspersky Security Center 内创建和使用内部用户账户。系统不会将内部用户的任何数据传送到操作系统。Kaspersky Security Center 将验证内部用户。

您可以在控制台树的“**用户账户**”文件夹配置内部用户的账户。

管理服务器设置的备份和恢复

管理服务器设置和其数据库的备份通过备份任务和 klbackup 实用工具执行。备份副本包括与管理服务器有关的所有主要设置和对象，例如证书、受管理设备上驱动器加密的主密钥、各种授权许可的密钥、管理组的结构及其所有内容、任务、策略等。使用备份副本，您可以尽快恢复管理服务器的操作，为此花费十几分钟到几个小时。

如果没有备份副本可用，失败可能导致证书和管理服务器设置的不可挽回的损失。这将导致要重新开始配置 Kaspersky Security Center，并在组织网络上重新执行网络代理初始化部署。所有受管理设备驱动器加密主密钥也将丢失，导致 Kaspersky Endpoint Security 设备上不可挽回的加密数据丢失。因此，不要忽略使用标准备份任务对管理服务器进行定期备份。

快速启动向导为管理服务器设置创建备份任务，并将其设置为每天凌晨 4:00 运行。备份副本默认保存在文件夹 %ALLUSERSPROFILE%\Application Data\KasperskySC 中。

如果安装在其他设备上的 Microsoft SQL Server 实例被用作 DBMS，您必须通过指定 UNC 路径修改备份任务，这可以通过管理服务器服务和 SQL Server 服务写入，作为存储备份副本的文件夹。这个来自 Microsoft SQL Server DBMS 备份的特殊功能。

如果使用本地 Microsoft SQL Server 实例作为 DBMS，我们还建议将备份副本与管理服务器一起保存到专用介质，以防止它们损坏。

因为备份副本包含重要数据，备份任务和 klbackup 实用工具用于备份副本密码保护。默认下，备份任务使用空密码创建。您必须在备份任务属性中设置密码。忽略该需求将导致管理服务器证书所有密钥、授权许可密钥和受管理设备驱动器加密主密钥保持未加密。

除了常规备份，您必须在每个显著更改之前创建备份副本，包括管理服务器升级和补丁的安装。

如果您使用 Microsoft SQL Server 作为 DBMS，您可以最小化备份副本的大小。为此，请启用 SQL Server 设置中的**压缩备份**复选框。

从备份副本的恢复使用管理服务器实例上刚刚安装的与备份副本具有相同或更新版本的实用工具 klbackup 来执行。

对于要执行还原的管理服务器的实例，必须使用相同类型（例如相同的 SQL Server 或 MariaDB）和相同版本或更新版本的 DBMS。管理服务器版本可以相同（带有相同或更新补丁）或更新。

这部分描述了恢复管理服务器设置和对象的标准方案。

使用文件系统快照降低备份时间

在 Kaspersky Security Center 15.1，管理服务器备份的空闲时间相比早期版本被降低。而且，**使用文件系统快照以备份数据**功能被添加到任务设置。该功能通过使用 klbackup 实用工具提供附加空间降低，这将在备份过程中增加磁盘的卷影副本（这将花费几秒钟）并同时复制数据库（这花费最多几分钟）。当 klbackup 创建磁盘卷影副本和数据库副本时，实用程序再次使管理服务器可连接。

您仅可以在满足这两个条件时使用文件系统快照功能：

- 管理服务器共享文件夹和 %ALLUSERSPROFILE%\KasperskyLab 文件夹位于相同逻辑磁盘以及管理服务器本地。
- %ALLUSERSPROFILE%\KasperskyLab 文件夹不包含任何手动创建的符号链接。

如果任何条件都不能满足，则不使用该功能。此种情况下，应用程序在创建文件系统快照时将返回错误消息。

要使用功能，您必须拥有授予了创建 %ALLUSERSPROFILE% 所在逻辑磁盘的快照的权限的账户。注意，管理服务器服务账户没有此权限。

要使用文件系统快照功能以便降低备份时间：

1. 在**任务**区域，选择备份任务。
2. 在上下文菜单中，选择**属性**。
3. 在打开的"任务属性"窗口中，选择"**设置**"区域。
4. 选择**使用文件系统快照以备份数据**复选框。
5. 在**用户名**和**密码**字段，输入具有创建 %ALLUSERSPROFILE% 所在逻辑磁盘的快照的权限的账户的名称和密码。
6. 单击"**应用**"。

在备份任务的后续启动中，klbackup 实用程序将创建文件系统快照，以便在任务运行中降低管理服务器空闲时间。

管理服务器设备不可操作

如果管理服务器设备由于失败而不可操作，建议您执行以下操作：

- 新管理服务器必须分配相同的地址：NetBIOS 名称、FQDN 或静态 IP(取决于部署网络代理时的设置)。
- 安装管理服务器，使用相同类型、相同版本（或更新）的 DBMS。您可以安装带有相同（或更新）补丁的相同（或更新）版本的服务器。安装后，不要通过向导执行初始化安装。
- 在**开始**菜单中，运行 klbackup 实用程序并执行还原。

管理服务器设置或数据库被损坏

如果管理服务器由于设置或数据库损坏（例如断电）而不可操作，建议您使用以下恢复方案：

1. 扫描被损坏设备上的文件系统。
2. 卸载管理服务器的不可操作版本。

3. 重新安装管理服务器，使用相同类型、相同版本（或更新）的 DBMS。您可以安装带有相同（或更新）补丁的相同（或更新）版本的服务器。安装后，不要通过向导执行初始化安装。

4. 在**开始**菜单，运行 klbackup 实用工具并执行恢复。

禁止用除了通过 klbackup 实用工具的其他方法恢复管理服务器。

任何试图通过第三方软件恢复管理服务器的操作都将不可避免地导致 Kaspersky Security Center 分发节点上的数据的不一致和应用程序操作不正常。

备份复制和管理服务器数据恢复

数据备份允许您将管理服务器从一台设备上转移至其他设备且无数据丢失。通过备份，您可以在移动管理服务器数据库到另一部设备或者升级到更新版本的 Kaspersky Security Center 时恢复数据。此外，您可以使用数据备份将管理服务器数据从 Kaspersky Security Center Windows 移动到 Kaspersky Security Center Linux 的管理下（不支持将数据从 Kaspersky Security Center Linux 移动到 Kaspersky Security Center Windows）。

已安装的管理插件不会被备份。从备份副本恢复管理服务器数据后，您需要下载并重新安装受管理应用程序的插件。

备份管理服务器数据之前，请检查虚拟管理服务器是否已添加到管理组。如果添加了虚拟管理服务器，请确保在备份之前为该虚拟管理服务器分配了管理员。备份后，您将无法授予管理员对虚拟管理服务器的访问权限。请注意，如果管理员账户凭据丢失，您将无法向虚拟管理员服务器分配新管理员。

要备份或恢复 Kaspersky Security Center 故障转移集群，您必须在备份或恢复完成后停止整个集群进行维护，然后重新启动它。

您可以使用以下方式之一创建管理服务器数据的备份副本：

- 通过使用管理控制台创建并运行数据备份任务。
- 通过在已安装管理服务器的设备上运行 klbackup 实用程序。该实用程序包含在 Kaspersky Security Center 分发包。管理服务器安装完毕后，该实用程序位于程序安装时指定文件夹的根目标中。

以下数据保存在管理服务器的备份副本中：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）。
- 有关管理组和客户端设备的结构的配置详情。
- 远程安装的应用程序分发包的存储库。
- 管理服务器证书。

- *更新*文件夹的内容。

  默认情况下，文件夹路径为 C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

只用使用 klbackup 实用程序才能进行管理服务器数据恢复。您必须在刚刚安装的、与备份副本具有相同或更新版本的管理服务器的可运行实例上执行恢复。

“备份管理服务器数据”任务

建立“备份管理服务器数据”任务。

备份任务是一项管理服务器任务；它通过快速启动向导创建。如果由快速启动向导创建的备份任务被删除，您可以手动创建备份任务。

要建立备份管理服务器数据任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 通过下列方式开始创建任务：
   - 在控制台树的“**任务**”文件夹的上下文菜单中，选择**新建 → 任务**。
   - 单击工作区中的“**创建任务**”按钮。

   “新任务向导”启动。遵照向导的说明操作。在该向导的“**选择任务类型**”窗口中，选择名为**备份管理服务器数据**的任务类型。

“**备份管理服务器数据**”任务只能创建单份副本。如果已经为管理服务器创建了管理服务器数据备份任务，它不会显示在“管理服务器备份任务创建向导”的任务类型选择窗口中。

配置“备份管理服务器数据”任务

创建备份任务后，您可以配置任务设置。

要配置管理服务器数据备份任务：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在**备份管理服务器数据**任务的上下文菜单中，选择“**属性**”。

   *管理服务器数据备份*任务的属性窗口将打开。下列属性可用：

- **常规**

  在**常规**部分，您可以指定任务名称，查看任务创建日期、最后命令日期、任务启动的状态和任务结果。

- **通知**

  在**通知**部分，您可以指定与任务执行结果相关的事件的存储设置，以及配置有关任务执行结果的通知。

- **计划**

  在**计划**部分，您可以指定任务启动计划。

- **目标**

  在**目标**部分，您可以指定将存储管理服务器数据备份副本的文件夹路径。

- **设置**

  在**设置**部分，您可以根据需要设置备份保护密码和备份数量。

  您还可以创建存储 %ALLUSERSPROFILE% 文件夹的逻辑磁盘的卷影副本并复制管理服务器数据库。为此，您必须启用**使用文件系统快照以备份数据**选项，然后指定具有创建快照权限的帐户的名称和密码。

- **安全性**

  在**安全性**部分，您可以授予用户和组在管理服务器上执行操作的权限。如果启用了**从管理服务器继承设置**选项，则任务的安全设置将从管理服务器继承。

  如果禁用该选项，您可以配置任务的安全设置。您可以分配角色到用户或用户组或分配权限到用户或用户组，如任务中所应用。

  默认启用**从管理服务器继承设置**"选项。

- **修订历史**

  在**修订历史**部分，您可以跟踪任务修改。您每次保存对任务所做的更改时，修订被创建。

数据备份和恢复实用程序（klbackup）

您可以使用 Kaspersky Security Center 发布套件中附带的 klbackup 实用程序复制管理服务器数据以作备份和将来恢复之用。

klbackup 实用程序可以以以下两种模式运行：

- 交互
- 静默

交互模式下的数据备份和恢复

通过使用 klbackup 实用程序以交互模式创建的备份副本来恢复管理服务器数据可能会出现错误。如果您已安装管理服务器补丁 15.1.0.20748-pf2，然后在禁用**迁移数据库**选项的情况下使用 klbackup 实用程序创建备份副本，则在恢复此副本时会发生错误（对于所有 DBMS，MySQL 和 MariaDB 除外）。如果您已安装管理服务器补丁 15.1.0.20748-pf2，并且想要创建备份副本而不迁移到另一个 DBMS，请使用数据备份任务或从命令行运行 klbackup 实用程序。

若要以交互模式创建管理服务器数据的备份副本，请执行以下操作：

1. 运行位于 Kaspersky Security Center 安装文件夹的 klbackup 实用程序。

   这样将启动备份和恢复向导。

2. 在向导的第一个窗口中，选择"**执行管理服务器数据备份**"。

如果选中了“**仅恢复或备份管理服务器证书**”选项，将只保存管理服务器证书和私钥的备份副本。当您执行从 Kaspersky Security Center Windows 管理服务器迁移到 Kaspersky Security Center Linux 管理服务器时，备份管理服务器证书和私钥可能会有用。此外，您还可以在 Kaspersky Security Center Linux 管理服务器之间以及 Kaspersky Security Center Windows 管理服务器之间迁移受管理设备。有关详细信息，请参阅使用 klbackup 实用程序切换受管理设备至另一台管理服务器的管理下。

单击“**下一步**”。

3. 在向导的下一个窗口中，指定以下选项：

- **备份目标文件夹**
- **迁移数据库**

  如果您当前将管理服务器数据存储在 Microsoft SQL Server 数据库中，并且需要将其迁移到以下数据库之一，请启用此选项： MySQL或MariaDB、PostgreSQL或 Postgres Pro、 Azure SQL。默认情况下已禁用该选项。

  - **迁移到 MySQL/MariaDB 格式**

    如果您当前使用 SQL Server 作为管理服务器的 DBMS，并且希望将数据从 SQL Server 迁移到 MySQL 或 MariaDB DBMS，请启用此选项。Kaspersky Security Center 将创建与 MySQL 和 MariaDB 兼容的备份。之后，您可以将备份中的数据恢复到 MySQL 或 MariaDB。

  - **迁移到 Postgres**

    如果您当前使用 SQL Server 作为管理服务器的 DBMS，并且需要将数据从 SQL Server 迁移到 PostgreSQL 或 Postgres Pro DBMS，请启用此选项。Kaspersky Security Center 将创建与 PostgreSQL 和 Postgres Pro 兼容的备份。之后，您可以将备份中的数据恢复到 PostgreSQL 或 Postgres Pro 中。

    如果您向卡巴斯基技术支持提出请求并为管理服务器安装补丁 15.1.0.20748-pf2 或更新至 Kaspersky Security Center Windows 版本 15.1.0.22239，则此选项可用。

  - **迁移到 Azure 格式**

    如果您当前使用 SQL Server 作为管理服务器的 DBMS 并且希望将数据从 SQL Server 迁移到 Azure SQL DBMS，请启用此选项。Kaspersky Security Center 将创建与 Azure SQL 兼容的备份。之后，您可以将备份中的数据恢复到 Azure SQL。

- **将当前日期和时间包含在备份目标文件夹的名称里**
- **备份的密码**

4. 单击“**下一步**”按钮，开始备份。

5. 如果要在诸如 Amazon Web Services (AWS) 或 Microsoft Azure 之类的云环境中使用数据库，请在“**登录到在线存储**”窗口填写以下字段：

- 对于 AWS：
  - **S3 bucket 名称**

    您为备份创建的 S3 bucket 名称。

  - **访问密钥 ID**

    当您创建了 IAM 用户账户以使用 S3 bucket 存储实例时，您接收到密钥 ID（数字字母序列）。

    如果您在 S3 bucket 上选择了 RDS 数据库则该字段可用。

  - **Secret key**

    您创建IAM 用户账户时接收到的带有访问密钥 ID 的secret key。

    Secret key 的字符显示为星号。在您开始输入 secret key 后，**显示**按钮被显示。点击并按住该按钮一定时间以查看输入的字符。

    如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

- 对于 Microsoft Azure：
  - **Azure 存储账户名**

    您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

  - **Azure 订阅 ID**

    您在 Azure 门户创建了该订阅。

  - **Azure 密码**

    当您创建应用程序 ID 时您收到应用程序 ID 的密码。

    密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

  - **Azure 应用程序 ID**

    您在 Azure 门户创建了该应用程序 ID。

    您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

  - **Azure SQL Server 名称**

    名称和资源组在您的 Azure SQL Server 属性中可用。

- **Azure SQL Server 资源组**

  名称和资源组在您的 Azure SQL Server 属性中可用。

- **Azure 存储访问密钥**

  在您的存储账户属性中可用，在访问密钥区域。您可以使用任何密钥（key1 或 key2）。

若要以交互模式恢复管理服务器数据，请执行以下操作：

1. 运行位于 Kaspersky Security Center 安装文件夹的 klbackup 实用程序。使用与安装管理服务器时相同的账户启动该实用程序。建议您在新安装的管理服务器上运行该实用程序。

   这样将启动备份和恢复向导。

2. 在向导的第一个窗口中，选择 **恢复管理服务器数据**，然后单击“**下一步**”。

   如果选中了“**仅恢复或备份管理服务器证书**”选项，将只恢复管理服务器证书和私钥。

   当您在非活动故障转移群集节点上运行 klbackup 实用程序时，系统将提示您选择以下选项之一：指定管理服务器证书或自动从管理服务器检索数据。

3. 在向导的“**恢复设置**”窗口：

   - 指定包含管理服务器数据备份副本的文件夹。

     如果您在例如 AWS 或 Azure 的云环境中工作，指定存储地址。此外，确保该文件名为 backup.zip。

   - 指定数据备份中输入的密码。

     在恢复数据时，您必须指定在备份过程中输入的密码。如果某个共享文件夹的路径在备份任务完成后发生更改，请检查使用数据恢复任务的操作（恢复任务和远程安装任务）。必要时，编辑这些任务的设置。当从备份文件恢复数据时，没有人可以访问管理服务器的共享文件夹。启动 klbackup 实用程序所使用的账户必须对该共享文件夹具有完全访问权限。

4. 单击“**下一步**”按钮，恢复数据。

静默模式下的数据备份和恢复

要以静默模式创建备份副本或恢复管理服务器数据，

在已安装管理服务器的设备上，利用命令行和所需密钥运行 klbackup。

使用 klbackup 实用程序时，网络代理标志不会被恢复。您需要手动配置网络代理标志。

对于要执行还原的管理服务器的实例，必须使用相同类型的 DBMS。管理服务器版本可以相同（带有相同或更新补丁）或更新。

实用程序命令行语法：

```
klbackup -path <backup path> [-linux_path <SQL Server备份路径>][-node_cert <证书路径>]
[-logfile <日志文件>] [-use_ts]|[-restore] [-password <密码>] [-cert_only] [-online] [-
migrate postgres]
```

如果在 klbackup 实用程序的命令行中没有指定密码，该实用程序将提示您输入密码。

参数描述：

- `-path <备份路径>` — 将信息保存在指定的备份文件夹中，或使用备份文件夹中的数据进行恢复（必填参数）。

  数据库服务器账户和 klbackup 实用程序需要获得对备份文件夹中的数据进行更改的权限。

- `-linux_path <SQL Server 备份路径>` — Linux 上包含 SQL Server 备份数据的文件夹的本地路径。

  数据库服务器账户和 klbackup 实用程序需要获得对 SQL Server 备份文件夹中的数据进行更改的权限。

- `-node_cert <证书路径>` — 用于在恢复后配置非活动故障转移集群节点的服务器证书文件。如果未设置，它将被自动从服务器检索。

  在非活动故障转移群集节点上运行 klbackup 实用程序时，使用此密钥指定服务器证书的路径。

- `-logfile <日志文件>` — 保存关于管理服务器数据备份和恢复的报告。

- `-use_ts` — 保存数据时，将信息复制到备份文件夹中以 `klbackup YYYY-MM-DD # HH-MM-SS` 格式命名的子文件夹中，其中包括当前日期及 UTC 时间的操作时间。如果未指定密钥，信息将保存在备份文件夹的根目录中。

  当您尝试将信息保存至已存储备份副本的文件夹时，系统会返回错误消息。不会更新任何信息。

  `-use_ts` 键允许您维护管理服务器数据压缩文件。例如，如果 `-path` 键指明文件夹 `C:\KLBackups`，则文件夹 `klbackup 2022/6/19 # 11-30-18` 将存储截至 2022 年 6 月 19 日上午 11:30:18 的管理服务器状态信息。

- `-restore` — 恢复管理服务器数据。系统将基于备份文件夹内包含的信息执行数据恢复。如果没有可用密钥，数据将备份至备份文件夹中。

- `-password <password>` — 用于保护敏感数据的密码。

  忘记的密码无法被恢复。没有密码要求。密码长度不受限制，并且可以是零长度（无密码）。

  在恢复数据时，您必须指定在备份过程中输入的密码。如果某个共享文件夹的路径在备份任务完成后发生更改，请检查使用数据恢复任务的操作（恢复任务和远程安装任务）。必要时，编辑这些任务的设置。当从备份文件恢复数据时，没有人可以访问管理服务器的共享文件夹。启动 klbackup 实用程序所使用的账户必须对该共享文件夹具有完全访问权限。建议您在新安装的管理服务器上运行该实用程序。

- `-cert_only` — 仅保存或恢复管理服务器的证书和私钥。

  当您执行从 Kaspersky Security Center Windows 的管理服务器迁移到 Kaspersky Security Center Linux 的管理服务器时，此标志可能有用。此外，您还可以在 Kaspersky Security Center Linux 管理服务器之间以及 Kaspersky Security Center Windows 管理服务器之间迁移受管理设备。

- `-online`—通过创建卷快照来备份管理服务器数据以最小化管理服务器的离线时间。当您使用实用程序恢复数据时，该选项被忽略。当创建备份以迁移到不同的 DBMS 时请勿使用此标志。

- `-archive 0` — 将服务器数据保存为纯文本文件。默认情况下（`-archive 1`），服务器数据存储在存档文件中。

- `-migrate mysql`— 创建存储在与 PostgreSQL（包括 MariaDB）兼容的 SQL Server 数据库中的管理服务器数据的备份。您可以将备份中的数据恢复到 MySQL。

- `-migrate postgres`—创建存储在与 PostgreSQL 和 Postgres Pro 兼容的 SQL Server 数据库中的管理服务器数据备份。您可以将备份中的数据恢复到 PostgreSQL 或 Postgres Pro 中。当您通过管理服务器数据备份执行向 Kaspersky Security Center Linux 的迁移时，请使用此标志。

  如果您向卡巴斯基技术支持提出请求并为管理服务器安装补丁 15.1.0.20748-pf2 或更新至 Kaspersky Security Center Windows 版本 15.1.0.22239，则此选项可用。

使用 klbackup 实用程序切换受管理设备至另一台管理服务器的管理下

klbackup 实用程序可让您切换受管理设备至另一台管理服务器的管理下。您可以在执行迁移时使用 klbackup 实用程序将 Kaspersky Security Center Windows 管理服务器更改为 Kaspersky Security Center Linux 管理服务器。此外，您还可以在 Kaspersky Security Center Linux 管理服务器之间以及 Kaspersky Security Center Windows 管理服务器之间迁移受管理设备。

要使用 klbackup 实用程序切换受管设备至另一台管理服务器的管理下：

1. 在之前的设备上，创建管理服务器证书和私钥的备份副本。

   您可以使用下列可用方法之一指定一个备份副本：

   - 通过使用 klbackup 实用程序界面（仅适用于 Kaspersky Security Center Windows 管理服务器）

     运行位于 Kaspersky Security Center 安装文件夹中的 klbackup 实用程序，然后使用**仅恢复或备份管理服务器证书**选项创建备份。

   - 使用命令提示符（适用于 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 管理服务器 15.1 或更高版本）

     从命令行运行带有 `-cert_only` 键的 klbackup 实用程序，以创建管理服务器证书和私钥的备份副本：

     `klbackup -path <管理服务器证书备份副本的路径> -cert_only`

2. 在之前的设备上，断开管理服务器与网络的连接。

3. 使用另一台管理服务器为设备分配相同的地址。

   可以为新的管理服务器分配 NetBIOS 名称、FQDN 和静态 IP 地址。这取决于部署网络代理时在网络代理安装包中设置了哪个管理服务器地址。或者，您可以使用确定网络代理连接到的管理服务器的连接地址（您可以使用klnagchk 实用程序在受管理设备上获取此地址）。

4. 在具有另一台管理服务器的设备上，从备份副本恢复管理服务器证书和私钥。

   您可以使用下列可用方法之一恢复备份副本：

   - 通过使用 klbackup 实用程序界面（仅适用于 Kaspersky Security Center Windows 管理服务器）

     运行 klbackup 实用程序，然后使用**仅恢复或备份管理服务器证书**选项恢复备份。

   - 使用命令提示符（适用于 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 管理服务器 15.1 或更高版本）

     从命令行运行带有 `-cert_only` 键的 klbackup 实用程序，以恢复管理服务器证书和私钥的备份副本：

     `klbackup -path <管理服务器证书备份副本的路径> -restore -cert_only`

受管理设备受到另一台管理服务器的管理。您可以转至管理服务器并确保受管理设备在网络中可见，并且网络代理已安装并在其上运行（***可见***、**可见**和**网络代理已安装**列中的网络代理正在运行值）。

使用 MySQL 或 MariaDB 时备份和恢复管理服务器数据

您可以使用数据备份将管理服务器数据从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux 的管理下。仅支持使用管理服务器数据备份进行迁移，以便从任何受支持的 Kaspersky Security Center Windows 版本迁移到 Kaspersky Security Center Linux 15.2 或更高版本。

如果您使用 MySQL 或 MariaDB 作为 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的 DBMS，则 `lower_case_table_names` 参数必须与当前和新的 DBMS 匹配。否则，管理服务器数据将被错误迁移。

在 Kaspersky Security Center Windows 上备份管理服务器数据之前，请检查 `lower_case_table_names` 参数值。如果您之前在 DBMS 安装期间没有指定此参数，则使用默认参数值。Windows 的 `lower_case_table_names` 参数的默认值为 `1`。

在为 Kaspersky Security Center Linux 安装 MySQL 或 MariaDB 时，请使用MySQL 网站的说明将 `lower_case_table_names` 参数设置为与 Windows 中此参数指定的值相同的值。如果不指定此参数，则使用默认参数值。对于基于 Linux 的操作系统，`lower_case_table_names` 参数的默认值与 Windows 的默认值不同。

如果要安装 MySQL 8.0，可能无法按照此说明指定 `lower_case_table_names` 参数。在这种情况下，您必须首先安装 MySQL 5.7，使用操作说明指定 `lower_case_table_names` 参数，然后将 MySQL 5.7 升级到 MySQL 8.0。如果当前和新的 DBMS 的 `lower_case_table_names` 参数不匹配，则管理服务器数据将被错误恢复。

优化管理服务器数据的备份和恢复

为了优化管理服务器数据的备份和恢复以减少管理服务器停机时间，请执行以下操作之一：

- 启用**使用文件系统快照以备份数据**选项。

  详细信息请参考以下文章：使用文件系统快照来减少备份时间。

- 配置下列标志：

  使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

  - `KLSRV_BKP_FILES` — 将数据库文件分割为多个较小的文件，从 2 到 32。如果 DBMS 性能受到 CPU 限制，这可以加快备份和恢复。

    例如：

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
    ```

  - `KLSRV_BKP_BACKUP_EXTRA_PARS` — 指定 `COMPRESSION` 和 `MAXTRANSFERSIZE` 参数。如果 DBMS 性能受到文件输入/输出的限制，这可以加快备份速度。

    例如：

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
    MAXTRANSFERSIZE = 4194304"
    ```

  - `KLSRV_BKP_RESTORE_EXTRA_PARS` — 指定 `MAXTRANSFERSIZE` 参数。如果 DBMS 性能受到文件输入/输出的限制，这可以加快恢复速度。

    例如：

```
klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
= 4194304"
```

- `KLSRV_BKP_ONLINE_DB_BACKUP` — 消除备份期间管理服务器的停机时间。仅适用于以下 DBMS：
  - PostgreSQL，Postgres Pro。
  - 具有完整恢复模型的 SQL Server。有关详细信息，请参阅SQL Server 文档。当您启用 `KLSRV_BKP_ONLINE_DB_BACKUP` 标志时，SQL Server DBMS 会自动切换到完整恢复模型。

  例如：

  ```
  klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
  ```

将管理服务器移动至其他设备

如果需要在新设备上使用管理服务器，可以通过以下方式之一进行移动：

- 将管理服务器和数据库服务器移动到新设备（数据库服务器可以与管理服务器一起安装在新设备上，也可以安装在另一台设备上）。
- 将数据库服务器保留在以前的设备上，仅将管理服务器移至新设备。

要将管理服务器移至新设备：

1. 在先前设备上，创建管理服务器数据的备份。

   为此，您可以通过管理控制台运行数据备份任务或运行 klbackup 实用程序。

   > 如果您使用 SQL Server 作为管理服务器的 DBMS，您可以将数据从 SQL Server 迁移到 MySQL 或 MariaDB DBMS。为此，请运行交互模式下的 klbackup 实用程序以创建数据备份。在备份和还原向导**迁移到 MySQL/MariaDB 格式**窗口中启用**备份设置**选项。Kaspersky Security Center 将创建与 MySQL 和 MariaDB 兼容的备份。之后，您可以将备份中的数据恢复到 MySQL 或 MariaDB。

   > 如果希望将数据从 SQL Server 迁移到 Azure SQL DBMS，您还可以启用"**迁移到 Azure 格式**"选项。

2. 在之前的设备上，断开管理服务器与网络的连接。

3. 选择要安装管理服务器的新设备。确保所选设备上的硬件和软件符合管理服务器、管理控制台和网络代理的要求。此外，请检查管理服务器上使用的端口是否可用。

4. 为新设备分配相同地址。

   可以为新的管理服务器分配 NetBIOS 名称、FQDN 和静态 IP 地址。这取决于部署网络代理时在网络代理安装包中设置了哪个管理服务器地址。或者，您可以使用确定网络代理连接到的管理服务器的连接地址（您可以使用klnagchk 实用程序在受管理设备上获取此地址）。

5. 如有需要，在另一台设备上，安装管理服务器将使用的数据库管理系统 (DBMS)。

   数据库可以与管理服务器一起安装在新设备上，也可以安装在另一台设备上。确保该设备满足硬件和软件要求。选择 DBMS 时，请考虑管理服务器覆盖的设备数量。

6. 在新设备上运行管理服务器的安装。

7. 在管理服务器安装期间，配置数据库服务器连接设置。

Microsoft SQL Server 的"连接设置"窗口示例

根据数据库服务器的安装位置，执行以下操作之一：

- **将数据库服务器保留在先前设备上**

  1. 单击**SQL Server 实例名称**字段旁边的**浏览**按钮，然后在出现的列表中选择之前的设备名称。
     请注意，先前设备必须可用于连接新的管理服务器。
  2. 在**数据库名称**字段中输入以前的数据库名称。

- **将数据库服务器移至另一台设备**

  1. 单击**浏览**字段旁边的**SQL Server 实例名称**按钮，然后在出现的列表中选择设备名称。
  2. 在**数据库名称**字段中输入新的数据库名称。
     请注意，新数据库名称必须与先前设备中的数据库名称相匹配。数据库名称必须相同，以便使用管理服务器备份。默认数据库名称是 *KAV*。

8. 安装完成后，在新设备上使用 klbackup 实用程序恢复管理服务器数据。

   如果在先前设备和新设备上使用 SQL Server 作为 DBMS，请注意，新设备上安装的 SQL Server 版本必须不得低于先前设备上安装的 SQL Server 版本。否则，将无法在新设备上恢复管理服务器数据。

9. 打开管理控制台并连接到管理服务器。
10. 验证是否所有受管理设备都连接到了管理服务器。
11. 从以前的设备中卸载管理服务器和数据库服务器。

您也可以使用 Kaspersky Security Center Web Console 将管理服务器和数据库服务器移至另一台设备。

避免多个管理服务器之间的冲突

如果您的网络中有多于一个管理服务器，它们可以看到相同的客户端设备。例如，这可能会导致管理服务器安装已被另一个管理服务器安装的应用程序，以及其他冲突。为了防止应用程序被安装在由另一台管理服务器管理的设备上，您必须在**仅安装到通过该管理服务器管理的设备远程安装应用程序**_任务属性中启用远程安装应用程序仅在通过此管理服务器管理的设备上安装_选项。

如果启用**仅安装到通过该管理服务器管理的设备**选项，然后运行_远程安装应用程序_任务，则会执行检查以确定设备是否由另一台管理服务器管理。对于由另一台管理服务器管理的设备，**由不同管理服务器管理**属性值将被设置为`true`。_远程安装应用程序_任务将不会被应用于这些设备。

由不同管理服务器管理属性值显示在**受管理设备由不同管理服务器管理未分配的设备**列表中的由不同管理服务器管理列中。

您也可以使用"**由不同管理服务器管理**"属性作为以下目的的标准：

- 搜索设备
- 设备分类
- 设备移动规则
- 自动标记规则

若要重设由不同管理服务器管理属性：

1. 在 Kaspersky Security Center Web Console 的主菜单中，转至**发现和部署** → **未分配的设备**。
2. 选择所需的设备，然后单击**删除"由不同管理服务器管理"属性**按钮。

   由不同管理服务器管理属性被重设。

对管理组进行管理

本部分提供有关如何对管理组进行管理的信息。

您可以对管理组采取以下操作：

- 向管理组中添加任何层次结构级别的任意数量的嵌套组。
- 添加设备到管理组。
- 通过将单个设备和整个组移至其他组，改变管理组的层次结构。
- 从管理组中删除嵌套组和设备。
- 将从属服务器和虚拟管理服务器添加至管理组。

- 将设备从管理服务器的管理组移至其他服务器的管理组。
- 定义将哪些 Kaspersky 应用程序自动安装到包括在组中的设备。

仅当您在您要管理的管理组（或这些组所属管理服务器）的**管理组的管理**区域拥有**修改**权限时，您可以执行这些操作。

创建管理组

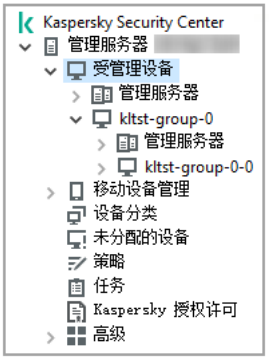
管理组的层次结构是在 Kaspersky Security Center 主程序窗口的“**受管理设备**”文件夹中创建的。管理组以文件夹形式显示在控制台树中（参见下图）。

安装 Kaspersky Security Center 后，“**受管理设备**”文件夹仅包含空的**管理服务器**文件夹。

> 用户界面设置决定了“**管理服务器**”文件夹是否出现在控制台树中。要显示该文件夹，在菜单栏选择“**视图** → **配置界面**”，然后在打开的“**配置界面**”窗口中选择“**显示从属管理服务器**”复选框。

当创建管理组层次结构时，您可以将设备和虚拟机添加到“**受管理设备**”文件夹中，也可以添加嵌套组。您可以将从属和虚拟管理服务器添加到“**管理服务器**”文件夹。

与“**受管理设备**”文件夹一样，每个初始创建的组都是仅包含空的“**管理服务器**”文件夹，用于处理该组中的从属和虚拟管理服务器。有关该组的策略和任务的信息以及该组中包含的设备的信息，将显示在该组的工作区中具有相应名称的选项卡上。



查看管理组层次结构

要创建管理组，请执行以下操作：

1. 在控制台树中，展开“**受管理设备**”文件夹。
2. 如果要在现有管理组中创建子组，则在“**受管理设备**”文件夹中选择与包括新管理组的组对应的子文件夹。
   如果您创建新的顶级管理组，您可以跳过该步骤。
3. 以下列方式之一开始管理组创建过程：
   - 使用上下文菜单中的**新建** → **组**命令。
   - 通过单击主应用程序窗口工作区的“**设备**”选项卡上的“**新组**”按钮。
4. 在打开的“**组名称**”窗口中输入组名称，然后单击“**确定**”。

控制台树中将显示带有指定名称的新管理组文件夹。

程序允许基于活动目录的架构或域网架构创建管理组结构。您也可以从文本文件创建组架构。

要创建管理组结构：

1. 在控制台树中，选择“**受管理设备**”文件夹。
2. 在“**受管理设备**”文件夹的上下文菜单中，选择**所有任务 → 新组结构**。

   新管理组结构向导启动。遵照向导的说明操作。

移动管理组

您可以在组层次结构内移动嵌套的管理组。

管理组与所有嵌套组、从属管理服务器、设备、组策略和任务一起移动。系统将向该组应用与其在管理组层次结构中的新位置相对应的所有设置。

组名称必须在该层次结构的一个级别内唯一。如果在您向其中移动该管理组的文件夹中已有同名的组，则应该更改该管理组的名称。如果尚未更改要移动的组的名称，则在移动该组时，系统将向其名称添加一个 **（<下一个序列号>）** 格式的索引，例如： **（1）** 、 **（2）** 。

> 您不能重命名“**受管理设备**”组，因为它是管理控制台的内置元素。

要将组移至控制台树的其他文件夹，请执行以下操作：

1. 在控制台树中选择要移动的组。
2. 执行以下操作之一：

   - 通过使用上下文菜单移动组：

     1. 从该组的上下文菜单中选择“**剪切**”。
     2. 从您要向其中移动选定组的管理组的上下文菜单中选择“**粘贴**”。

   - 使用主程序菜单移动组：

     a. 从主菜单中选择**操作 → 剪切**。

     b. 在控制台树中选择您必须向其中移动选定组的管理组。

     c. 从主菜单中选择**操作 → 粘贴**。

   - 使用鼠标将组移至控制台树中的其他组。

删除管理组

如果某个管理组不包含从属管理服务器、嵌套组或客户端设备，并且没有为其创建任何组任务或策略，则可以删除该管理组。

在删除某个管理组之前，您必须从该组中删除所有从属管理服务器、嵌套组和客户端设备。

要删除某个组，请执行以下操作：

1. 在控制台树中选择管理组。
2. 执行以下操作之一：
   - 从该组的上下文菜单中选择“**删除**”。
   - 从主程序菜单中选择**操作** → **删除**。
   - 按 **DELETE** 键。

自动创建管理组结构

Kaspersky Security Center 允许您使用组层次结构创建向导来创建管理组的结构。

该向导根据以下数据创建管理组的结构：

- Windows 域和工作组的结构
- “活动目录”组的结构
- 管理员手动创建的文本文件的内容

当文本被生成时，以下需求必须被满足：

- 每个新组的名称必须另起新行；分隔符必须以换行符开头。空白行将被忽略。

  例如：
  Office 1
  Office 2
  Office 3
  程序将在目标组中创建第一个层次结构级别的三个组。

- 必须用反斜杠标记 （/） 输入嵌套组的名称。

  例如：
  Office 1/Division 1/Department 1/Group 1
  程序将在目标组中创建四个相互嵌套的子组。

- 要创建相同层次结构级别的多个嵌套组，您必须指定“组的绝对路径”。

  例如：
  Office 1/Division 1/Department 1
  Office 2/Division 1/Department 1
  Office 1/Division 3/Department 1
  Office 1/Division 4/Department 1
  程序将在目标组中创建第一个层次结构级别 Office 1 的一个组；该组将包括四个具有相同层次结构级别的嵌套组：“Division 1”、“Division 2”、“Division 3”和“Division 4”。这些组中的每个组都将包括“Department 1”组。

通过向导创建管理组层级不影响网络完整性：不替换现有组，而添加新组。客户端设备不能两次被包含在管理组，因为设备在移动到管理组时已从“**未分配的设备**”组删除。

如果在创建管理组结构时，设备由于某些原因（被关闭或从网络断开）未被包含在“**未分配的设备**”组，则该设备将不会自动移动到管理组。您可以在该向导完成后将客户端设备手动添加至管理组。

要启动自动创建管理组结构的过程，请执行以下操作：

1. 在控制台树中选择“**受管理设备**”文件夹。
2. 在“**受管理设备**”文件夹的上下文菜单中，选择**所有任务 → 新组结构**。

新管理组结构向导启动。遵照向导的说明操作。

将应用程序自动安装到管理组中的设备

您可以指定哪些安装包必须用于将 Kaspersky 应用程序自动远程安装到管理组中的客户端设备。

若要配置将程序自动安装至管理组中的设备上，请执行以下操作：

1. 在控制台树中，选择所需的管理组。
2. 打开该管理组的属性窗口。

3. 在“**区域**”面板，选择“**自动安装**”，并在工作区选择应用程序安装包以安装到设备。

4. 单击“**确定**”。

组任务被创建。这些任务将在新客户端设备加入管理组的时候立即在设备上运行。

如果应用程序的一些安装包被选择用于自动安装，安装任务只选择最近的应用程序版本。

管理客户端设备

本部分包含客户端设备的工作信息。

将客户端设备连接至管理服务器

客户端设备和管理服务器之间的连接通过安装在客户端设备上的网络代理建立。

当客户端设备连接至管理服务器时，系统将执行以下操作：

- 自动同步数据：
  - 安装在客户端设备上的应用程序列表同步。
  - 同步策略、应用程序设置、任务和任务设置。
- 按管理服务器检索有关应用程序状况、任务执行和应用程序操作统计数据的最新信息。
- 将事件信息传输至管理服务器进行处理。

根据网络代理设置，定期同步数据（例如，每 15 分钟）。您可以手动设置连接的时间间隔。

一旦有任何事件发生，其信息将被立即发送至管理服务器。

如果管理服务器是位于企业网络外部的远程服务器，则客户端设备可通过互联网与其连接。

对于要通过互联网连接到管理服务器的设备，必须满足以下条件：

- 远程管理服务器必须拥有外币 IP 地址且接收端口 13000 必须保持打开（为了连接网络代理）。我们建议您也打开 UDP 端口 13000（为了接收设备关闭通知）。
- 应该首先在设备上安装网络代理。
- 在设备上安装网络代理时，您应该指定远程管理服务器的外部 IP 地址。如果使用安装包进行安装，则在“**设置**”区域的安装包属性中手动指定外部 IP 地址。
- 要使用远程管理服务器来管理设备的应用程序和任务，请在“**常规**”区域中该设备的属性窗口中，选中“**不断开与管理服务器的连接**”复选框。选中该选框之后，请等待管理服务器与远程设备同步。与管理服务器保持连接的客户端设备的数量不得超过 300。

要提高远程管理服务器启动任务的性能，您可以在设备上打开端口 15000。在此情况下，要运行任务，管理服务器将通过端口 15000 向网络代理发送一个专用数据包，而不是等待与设备的同步完成。

Kaspersky Security Center 允许您配置客户端设备和管理服务器之间的连接，使得当所有操作均完成后，连接仍然保存活动状态。当需要实时监控应用程序状态并且出于某种原因（例如，连接被防火墙保护，不允许打开客户端设备上的端口，客户端设备 IP 地址未知等原因）管理服务器无法建立与客户端计算机的连接时，无中断连接非常必要。您可以在设备属性窗口的"**常规**"区域，建立客户端设备和管理服务器的不间断连接。

我们建议您和最重要的设备建立不间断连接。管理服务器维护的最大同时连接数被限制到 300。

在手动同步时，系统将使用辅助连接方法，该连接将由管理服务器发起。在客户端设备上建立连接前，您必须打开 UDP 端口。管理服务器将向客户端设备的 UDP 端口发送连接请求。作为响应，管理服务器的证书通过验证。如果管理服务器证书与保存在客户端设备的证书副本相符，则连接被建立。

手动同步同样用于获取应用程序状态、任务执行以及应用程序操作统计的最新信息。

手动连接客户端设备至管理服务器。Klmover 工具

如果您需要手动将客户端设备连接至管理服务器，您可在客户端设备上使用 klmover 实用程序。

在客户端设备上安装网络代理时，自动将该实用程序复制到网络代理安装文件夹。

要使用 klmover 实用程序手动将客户端设备连接至管理服务器：

在设备上，从命令行启动 klmover 实用程序。

从命令行启动时，klmover 实用程序可以执行以下操作（根据当前使用的命令键）：

- 将网络代理连接到拥有指定设置的管理服务器；
- 将运行结果记录在事件日志文件中或显示在屏幕上。

对于通过连接网关连接到管理服务器的客户端设备，您不能使用 klmover 实用程序。对于这样的设备，您必须重新配置网络代理或重新安装网络代理并指定连接网关。

实用程序命令行语法：

```
klmover [-logfile <文件名>] [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>]
[-nossl] [-cert <凭证文件路径>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

运行该实用程序需要管理员权限。

参数描述：

- `-logfile <文件名>`—将实用程序运行结果记录到日志文件中。

  默认情况下，信息保存在标准输出流（stdout）中。如果未使用该键值，运行结果和错误信息将显示在屏幕上。

- `-address <服务器地址>`—连接的管理服务器的地址。
  您可以将设备的 IP 地址、NetBIOS 名称或 DNS 名称指定为地址。
- `-pn <端口号>`—用来建立与管理服务器的非加密连接的端口号。
  默认端口号是 14000。
- `-ps <SSL 端口号>`—使用 SSL 与管理服务器建立加密连接时使用的 SSL 端口号。
  默认端口号是 13000。
- `-nossl`—使用非加密连接管理服务器。
  如果未使用该键值，网络代理将通过使用加密的 SSL 协议连接至管理服务器。
- `-cert <验证文件的路径>`—访问管理服务器时使用指定的证书文件作为身份验证。
  如果未使用该键值，网络代理将在首次连接管理服务器时接收证书。
- `-silent`—以静默模式运行实用程序。
  有时候该键值很有用，例如当实用程序从用户注册数据的登录脚本启动时。
- `-dupfix`—如果网络代理不是使用常规方式（带分发包）安装，则实用该键值 - 例如：通过从 ISO 磁盘镜像恢复安装的。
- `-virtserv`—虚拟管理服务器的名称。
- `-cloningmode`—网络代理磁盘克隆模式。
  使用以下参数之一配置磁盘克隆模式：
  - `-cloningmode`—请求磁盘克隆模式的状态。
  - `-cloningmode 1`—启用磁盘克隆模式。
  - `-cloningmode 0`—禁用磁盘克隆模式。
- `-nauninstpwd <password>`—该密钥用于指定网络代理卸载密码。
  该密钥不是必需的。

例如，要将网络代理连接到管理服务器，则运行以下命令：

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

要建立客户端设备与管理服务器之间的通道连接

Kaspersky Security Center 允许通过管理服务器的从管理控制台的 TCP 连接通道，然后通过网络代理到受管理设备上的指定端口。通道设计用于连接网络控制台设备上的客户端应用程序到受管理设备上的 TCP 端口—如果管理控制台和目标设备之间没有直接连接可用。

例如，通道用于连接到远程桌面，可以连接到已存在会话，也可以创建一个新的远程会话。

通道也可以使用外部工具启用。例如，管理员可以运行 putty 实用工具、VNC 客户端和其他工具。

如果用于连接到管理服务器的端口在设备上不可用，则需要客户端设备和管理服务器之间的连接隧道。在以下情况下设备端口可能不可用：

- 远程设备连接到使用 NAT 装置的本地网络。
- 远程设备是本地网络管理服务器的一部分，但是它的端口被防火墙关闭。

要建立客户端设备与管理服务器之间的隧道连接：

1. 在控制台树中选择包括该客户端设备的组文件夹。
2. 在“**设备**”选项卡，选择设备。
3. 在设备的上下文菜单中，选择**所有任务 → 连接通道**。
4. 在打开的“**连接通道**”窗口创建通道。

远程连接至客户端设备桌面

管理员可以通过客户端设备上安装的网络代理获取对设备的远程访问权限。

即使客户端设备的 TCP 和 UDP 端口关闭，也可以通过网络代理远程连接至设备。在与设备建立连接后，管理员会获取对此设备上存储的信息的完全访问权限，以便他或她可以管理其上安装的应用程序。

本节介绍如何通过网络代理建立与 Windows 客户端设备和 macOS 客户端设备的连接。

连接到 Windows 客户端设备

可使用以下方式之一建立与 Windows 客户端设备的远程连接：

- 通过使用名为“远程桌面连接”的标准 Microsoft Windows 组件。
  根据标准 Windows 实用工具 mstsc.exe 的设置通过该实用工具建立到远程桌面的连接。
- 通过使用 Windows 桌面共享技术。

连接到 Windows 客户端设备（使用远程桌面连接）

在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有提前通知的情况下从会话断开连接。

要通过远程桌面连接组件连接到客户端设备的桌面：

1. 在管理控制台树中，选择您需要获取访问权限的设备。
2. 在设备的上下文菜单中，选择**所有任务 → 连接到设备 → 新 RDP 会话**。
   标准 Windows 实用工具 mstsc.exe 将启动，这有助于与远程桌面建立连接。
3. 按照实用工具对话框中显示的说明操作。

在与设备建立连接后，可以在 Microsoft Windows 的远程连接窗口使用桌面。

连接到 Windows 客户端设备（使用 Windows 桌面共享）

当连接到远程桌面的现有会话时，设备上的会话用户会收到来自管理员的连接请求。Kaspersky Security Center 创建的报告中不会保存有关设备上的远程活动及其结果的任何信息。

管理员可以连接至客户端设备上的现有会话而不会断开此会话中的用户。在这种情况下，设备上的管理员和会话用户将共享桌面访问权限。

管理员可以在远程客户端设备上配置用户活动的审核。审核期间，应用程序会保存有关客户端设备上管理员打开和/或修改过的文件的信息。

要通过 Windows 桌面共享连接到客户端设备的桌面，必须符合以下条件：

- 管理员的工作站上安装了 Microsoft Windows Vista 或更高版本。管理服务器设备操作系统的类型对通过 Windows 桌面共享进行连接没有限制。

  要检查您的 Windows 版本是否包含 Windows 桌面共享功能，请确保 Windows 注册表中包含 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 密钥。

- 客户端设备上安装了 Microsoft Windows Vista 或更高版本。

- Kaspersky Security Center 已安装漏洞和补丁管理授权许可。

要通过 Windows 桌面共享连接到客户端设备的桌面：

1. 在管理控制台树中，选择您需要获取访问权限的设备。
2. 在设备的上下文菜单中，选择“**所有任务**” → “**连接到设备**” → “**Windows 桌面共享**”。
3. 在打开的“**选择远程桌面会话**”窗口中，选择您需要连接的设备上的会话。

   如果与设备成功建立连接，设备的桌面将在“**卡巴斯基远程桌面会话查看器**”窗口中可用。
4. 要开始与设备的交互，在“**卡巴斯基远程桌面会话查看器**”窗口的主菜单中，选择**操作 → 交互模式**。

卡巴斯基远程桌面会话查看器实用程序需要商业授权许可。

连接到 macOS 客户端设备

管理员可以使用虚拟网络计算 (VNC) 系统连接到 macOS 设备。

通过安装在管理服务器设备上的 VNC 客户端与远程桌面建立连接。VNC 客户端将键盘和鼠标控制从客户端设备切换到管理员。

当管理员连接到远程桌面时，用户不会收到来自管理员的通知或连接请求。管理员连接到客户端设备上的现有会话，而不会使用户断开此会话。

要通过 VNC 客户端连接到客户端 macOS 设备的桌面，必须符合以下条件：

- VNC 客户端安装在管理服务器设备上。
- 客户端设备上允许远程登录和远程管理。
- 用户已在 macOS 操作系统的“**共享**”设置中允许管理员访问客户端设备。

要通过虚拟网络计算系统连接到客户端设备的桌面：

1. 在管理控制台树中，选择您需要获取访问权限的设备。
2. 在设备的上下文菜单中，选择**所有任务 → 连接通道**。
3. 在打开的“**连接通道**”窗口中，执行以下操作：
   a. 在 **1. 网络端口**部分，指定需要连接的设备的网络端口号。
   默认情况下使用端口 5900。
   b. 在**2. 通道**部分，单击**创建隧道**按钮。
   c. 在 **3. 网络设置**部分，单击**复制** 按钮。
4. 打开 VNC 客户端并将复制的网络属性粘贴到文本字段中。按下“**Enter**”。
5. 在打开的窗口中，查看证书详情。如果您同意使用该证书，单击“**确定**”按钮。
6. 在“**身份验证**”窗口，指定客户端设备的凭证，然后单击“**确定**”。

通过 Windows 桌面共享连接至客户端设备

若要通过 Windows 桌面共享连接至设备，请执行以下操作：

1. 在控制台树的“**设备**”选项卡，选择“**受管理设备**”文件夹。
   该文件夹的工作区显示设备列表。
2. 在您要连接的设备的上下文菜单中，选择**连接到设备 → Windows 桌面共享**。
   选择远程桌面会话窗口打开。
3. 在“**选择远程桌面会话**”窗口中选择用户连接至设备的桌面会话。
4. 单击“**确定**”。

设备被连接。

配置重启客户端设备

当使用、安装或卸载 Kaspersky Security Center 时，您必须重启设备。您仅可以对 Windows 设备指定重启设置。

配置客户端设备的重启:

1. 在控制台树中，选择必须为其配置重启的管理组。
2. 在该组的工作区中，选择“**策略**”选项卡。
3. 在工作区，在策略列表中选择 Kaspersky Security Center 网络代理的策略， 然后在策略的上下文菜单中选择“**属性**”。

4. 在策略属性窗口中，选择“**重启管理**”区域。

5. 如果需要重启设备，选择必须执行的操作：

   - 选择“**不重启操作系统**”阻止自动重启。
   - 选择“**如果必要，自动重启操作系统**”以允许自动重启。
   - 选择“**提示用户操作**”启用提示用户允许重启。

   您可以通过选择对应的复选框和选值框中的时间设置来指定重启请求的频率，强制重启和强制关闭设备上阻塞会话的程序。

6. 单击“**确定**”保存更改并关闭策略属性窗口。

设备的重启将被配置。

审核在远程客户端设备上执行的操作

程序允许对管理员在远程 Windows 客户端设备上的操作启用审核。审核期间，应用程序会保存设备上由管理员打开和/或修改过的文件的相关信息。当满足以下条件时,管理员操作审核可用:

- 漏洞和补丁管理授权许可正在使用中。
- 管理员有权启动共享访问远程设备的桌面。

启用审核在远程客户端设备上执行的操作：

1. 在控制台树中，选择应该为其配置管理员操作审核的管理组。
2. 在该组的工作区中，选择“**策略**”选项卡。
3. 选择 Kaspersky Security Center 网络代理的策略，然后在策略的上下文菜单中选择“**属性**”。
4. 在策略属性窗口中，选择“**Windows 桌面共享**”区域。
5. 选择“**启用审计**”复选框。
6. 在“**读取时要监控的文件掩码**”和“**修改时要监控的文件掩码**”列表中，添加文件掩码，应用程序在审核期间必须在文件掩码上监视操作。

   默认情况下，应用程序监控对扩展名为 txt、rtf、doc、xls、docx 、xlsx、odt 和 pdf 的文件执行的操作。

7. 单击“**确定**”保存更改并关闭策略属性窗口。

因此，配置了管理员在共享桌面访问远程设备上的操作审核。

远程设备上的管理员操作是被一一记录下来的:

- 在远程设备的事件日志中。
- 在远程设备上网络代理文件夹中扩展名为 syslog 的文件中（例如：C:\ProgramData\KasperskyLab\adminkit\1103\logs）。
- 在 Kaspersky Security Center 事件数据库中。

检查客户端设备与管理服务器之间的连接

Kaspersky Security Center 允许您手动或自动检查客户端设备与管理服务器之间的连接。

自动检查连接由管理服务器执行。手动检查连接在客户端设备上执行。

自动检查客户端设备与管理服务器之间的连接

若要启动自动检查客户端设备与管理服务器的连接，请执行以下操作：

1. 在控制台树中选择包括该设备的管理组。
2. 在管理组工作区的“**设备**”选项卡中，选择设备。
3. 在设备的上下文菜单中，选择“**检测设备可访问性**”。

这将打开包含设备可用性信息的窗口。

手动检查客户端设备与管理服务器之间的连接。Klnagchk 工具

您可以通过使用 klnagchk 实用程序手动检查连接和获取客户端设备与管理服务器之间的连接设置信息。klnagchk 实用程序位于网络代理安装文件夹。

从命令行启动时，klnagchk 实用程序能够执行以下操作（根据使用的键值）：

- 显示或记录用以连接设备上网络代理到管理服务器的设置值。
- 将网络代理统计数据（自上次启动以来）和实用程序运行结果记录在事件日志文件中或者显示在屏幕上。
- 尝试在网络代理和管理服务器之间建立连接。
  如果连接尝试失败，实用程序将发送一个 ICMP 包检查装有管理服务器的设备状态。

要使用 klnagchk 实用程序检查客户端设备和管理服务器之间的连接，请执行以下操作：

在安装了网络代理的设备上，以本地管理员账户从命令行启动 klnagchk 实用程序。

实用程序命令行语法：

```
klnagchk [-logfile <文件名>] [-sp] [-savecert <证书文件路径>] [-restart][-sendhb]
```

参数描述：

- `-logfile <文件名>` — 将网络代理和管理服务器之间连接设置的值和实用程序操作结果记录到日志文件中。
  默认情况下，信息保存在标准输出流（stdout）中。如果未使用该键值，设置、运行结果和错误信息将显示在屏幕上。
- `-sp` — 在代理服务器显示用于用户验证的密码。
  如果是通过代理服务器与管理服务器建立的连接，则使用本密钥。

- `-savecert <文件名>` – 在指定文件中保存用于访问管理服务器的证书。
- `-restart` – 实用程序操作完成后启动网络代理。
- `-sendhb` – 启动网络代理与管理服务器的同步。

启动后，klnagchk 实用程序将访问网络代理的配置文件并显示连接参数。这些参数在网络代理安装期间和网络代理策略设置中指定：

- `Current device` – 客户端设备的 Windows 网络名。
- `Network Agent version` – 设备上安装的网络代理版本（带补丁）的完整编号。
- `Administration Server address` – 管理服务器的地址。
- `Use SSL` – 该参数指示连接到管理服务器时是否使用安全连接。
  可能值：
  - 0–不使用安全连接。
  - 1–使用安全连接。
- `Compress traffic` – 该参数指示客户端设备和管理服务器之间的流量是否被压缩。
- `Numbers of the Administration Server SSL ports` – 使用安全连接与管理服务器通信的有效端口数。
- `Numbers of the Administration Server ports` – 使用普通连接与管理服务器通信的有效端口数。
- `Use proxy server` – 指示是否使用代理服务器的参数。
  可能值：
  - 0–不使用代理服务器。
  - 1–使用代理服务器。
- `Address` – 代理服务器的地址和端口，以冒号分隔。仅当使用代理服务器时才会显示此参数。
- `User name` – 用于访问代理服务器的用户名。仅当使用代理服务器时才会显示此参数。
- `Password` – 用于访问代理服务器的密码。仅当使用代理服务器时才会显示此参数。要显示代理服务器密码，需要在命令中使用`sp`密钥。
- `Administration Server certificate` – 指示客户端设备是否具有管理服务器证书的参数。例如，如果网络代理从未成功连接到管理服务器，则证书可能不存在。
  可能值：
  - `not installed` – 客户端设备没有管理服务器证书。
  - `available` – 客户端设备具有管理服务器证书。
- `Open UDP port` – 该参数指示网络代理是否使用 UDP 端口接收来自管理服务器的同步请求。

可能值：

- 0—UDP 端口已关闭，无法接收来自管理服务器的同步请求。
- 1—UDP 端口已打开，可用于接收来自管理服务器的同步请求。

- `Numbers of UDP ports` — 网络代理可以使用的 UDP 端口数。
- `Location name` — 设备的网络位置。
- `State of network location` — 指示客户端设备是否可以从一个管理服务器连接配置文件切换到另一个管理服务器连接配置文件的参数。

  可能值：

  - `Enabled` — 可以为客户端设备切换管理服务器连接配置文件。
  - `Disabled` — 无法为客户端设备切换管理服务器连接配置文件。
- `Profile to use` — 管理服务器的连接配置文件。
- `Condition` — 客户端设备所连接的网络的 IP 地址和子网掩码。
- `Synchronization interval (min)` — 同步之间的标准间隔。
- `Connection timeout (in seconds)` — 连接超时。
- `Send / receive timeout (in seconds)` — 读写操作的连接超时。
- `Device ID` — 网络中的设备标识符。`Device ID`在特定管理服务器管理的客户端设备中是唯一的。
- `Locations of connection gateways` — 通过连接网关将客户端设备连接到管理服务器的参数。
- `Location of distribution points` — 通过分发点将客户端设备连接到管理服务器的参数。
- `Connection with server` — 该参数指示连接网关是否与管理服务器具有持续的连接。仅当客户端设备充当连接网关时才显示该参数。

  可能值：

  - `active`— 连接网关与管理服务器保持持续连接。
  - `inactive`— 连接网关与管理服务器没有持续连接。
- `Connection with server through connection gateway`— 该参数指示是否正确建立了通过连接网关与管理服务器的连接。仅当客户端设备充当连接网关时才显示该参数。

  可能值：

  - `active`— 通过连接网关与管理服务器的连接已正确建立。
  - `inactive`— 通过连接网关与管理服务器的连接建立不正确。

此外，klnagchk 实用程序输出可能包含以下行之一：

- `Administration Server is installed on this device`— klnagchk 实用程序在管理服务器设备上运行。
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`— klnagchk 实用程序在安装了网络代理的设备上以连接网关模式运行。配置的连接网关正在等待来自管理服务器的连接，但管理服务器未将该设备列在管理设备中。您需要确保管理服务器发起与连接网关的连接。
- `This device is a connection gateway`— klnagchk 实用程序在充当连接网关的设备上运行。
- `Acts as a distribution point` — klnagchk 实用程序在充当分发点的设备上运行。

klnagchk 实用程序可检查网络代理服务的状态。如果该服务未运行，实用程序将停止。如果服务正在运行，实用程序将显示以下连接统计信息：

- `Total number of synchronization requests`— 尝试连接客户端设备到管理服务器的次数。
- `The number of successful synchronization request`— 尝试将客户端设备连接到管理服务器的成功次数。
- `Total number of synchronizations`— 尝试将客户端设备设置与管理服务器设置同步的次数。
- `The number of successful synchronizations`— 尝试将客户端设备设置与管理服务器同步的成功次数。
- `Date/time of the last request for synchronization`— 上次连接的日期和时间。

在分析管理服务器和网络代理之间的连接时，需要使用`Total number of synchronization requests`和`The number of successful synchronization request`。仅当管理服务器设置发生更改时（例如，添加了新任务或修改了策略设置），客户端设备设置才会与管理服务器设置同步。否则，`Total number of synchronizations`和`The number of successful synchronizations`参数值保持不变。

有关如何解决网络代理连接到管理服务器的问题的更多信息，请参阅Kaspersky Security Center 常见问题解答。

关于检查设备和管理服务器之间的连接时间

在关闭设备时，网络代理通知管理服务器该事件。在管理控制台，设备显示为已关闭。然而，网络代理无法通知管理服务器所有此类事件。因此，管理服务器会定期分析每台设备的“**连接到管理服务器**”属性（属性值显示在管理控制台“设备”属性中的“**常规**”区域中），并将它与网络代理当前设置中的同步间隔相比较。如果一台设备在超过三次成功的同步间隔后未响应，该设备被标记为已关闭。

在管理服务器上识别客户端设备

客户端设备是基于它们的名称识别的。在所有连接到管理服务器的设备中，设备的名称是唯一的。

当轮询 Windows 网络并发现新计算机时，或者当设备上安装的网络代理首次连接管理服务器时，系统都将会把设备名称传输至管理服务器。默认情况下，该名称与设备在 Windows 网络中的名称（NetBIOS 名）一致。如果某设备的名称已经在管理服务器中注册了，新的设备将在其名称后面按顺序加入数字索引，例如：**<Name>-1**、**<Name>-2**。在该名称下，设备被添加到管理组。

将设备移动至管理组

仅在您在**管理组的管理**区域对源和目标管理组(或对于这些组所属管理服务器)都具有**修改**权限时，您可以从一个管理组移动设备到其他管理组。

要把一台或多台设备包括在一个选定的管理组中，请执行以下操作：

1. 在控制台树中，展开“**受管理设备**”文件夹。
2. 在“**受管理设备**”文件夹中，选择与将包含客户端设备的组相对应的子文件夹。
   如果要将设备加入“**受管理设备**”组中，则可以跳过此步骤。
3. 在所选管理组工作区的“**设备**”选项卡上，使用下列方式之一将设备包含到管理组：
   - 通过在设备列表的信息框中单击“**将设备移动至组**”按钮将设备添加到组中
   - 通过在设备列表的上下文菜单中选择**创建 → 设备**

   移动设备向导启动。按照说明执行操作，选择一种方法将设备移动到组中，创建该组中包括的设备列表。

   如果手动创建设备列表，则可以使用 IP 地址（或 IP 范围）、NetBIOS 名称或 DNS 名称作为设备的地址。您可以在连接设备或设备发现后手动将那些其信息已经添加至管理服务器数据库的设备移动至列表中。

   要从文件导入设备列表，请指定包含要添加的设备的地址列表的 TXT 文件。必须在单独行中指定每个地址。

该向导完成后，管理组中将包括选定的设备，并在管理服务器生成的设备列表中显示其名称。

将设备从“**未分配的设备**”文件夹中拖放到管理组文件夹，即可将其移动至选定管理组。

更改客户端设备的管理服务器

您可以使用“*更改管理服务器*”任务来更改管理客户端设备的管理服务器。

要更改管理客户端设备的管理服务器：

1. 在控制台树中，选择“**任务**”文件夹。
2. 在该文件夹的工作区，点击“**新任务**”按钮。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在向导的**选择任务类型**步骤，选择**Kaspersky Security Center 管理服务器**节点，展开**高级**文件夹，然后选择**更改管理服务器**任务。
4. 在打开的窗口中，单击**确定**按钮确认您同意更改客户端设备管理服务器的条款。

5. 在向导的**设置**步骤，选择要用于管理选定设备的管理服务器：

- **更改到另一个主管理服务器**

  要将客户端设备移动至另一台主管理服务器，请指定以下管理服务器连接设置：

  1. 在**管理服务器**字段中，指定新的主管理服务器的地址。
  2. 在**端口**字段中，指定要连接到管理服务器的端口号。
     默认端口号是 14000。
  3. 在**SSL 端口**字段中，指定主管理服务器上的 SSL 端口号。
     默认端口号是 13000。
  4. 如有必要，请选中**使用代理服务器**复选框。
     如果清除此复选框，则使用直接连接将设备连接到管理服务器。
     如果选择此复选框，请指定代理服务器参数：
     - **代理服务器地址**
     - **代理服务器端口**

     如果您的代理服务器需要身份验证，请在**用户名** 和 **密码**字段中指定与代理服务器建立连接的账户的凭据。我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。
  5. 如有必要，请上传新的管理服务器证书。

- **在该主服务器上更改到另一个虚拟服务器**

  选择此选项可以将客户端设备移动到当前主管理服务器上的虚拟管理服务器。为此，在**虚拟管理服务器名称**字段中，指定必要的虚拟管理服务器的名称。

如有必要，请指定重新启动网络代理之前的等待时间。

6. 在向导的这一步，选择要对其分配任务的设备：

- **选择管理服务器检测到的网络设备**。此种情况下，任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。
- **手动指定设备地址或从列表导入地址**。您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定预定义分类或您所创建的自定义分类。
- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。

7. 在向导的**选择账户以运行任务**步骤中，指定账户设置：

- **默认账户**

  在与执行该任务的应用程序相同的账户下运行该任务。

默认情况下已选定该选项。

- **指定账户**

  填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - **账户**

    运行该任务的账户。

  - **密码**

    任务运行时使用的账户的密码。

8. 在向导的“**配置任务计划**”步骤，您可以为任务启动创建计划。如果必要，指定以下设置：

- **计划开始：**

  选择任务运行计划并配置所选计划。

  - **每天(不支持夏令时)**

    任务定期运行，按照指定天数间隔。计划不支持夏令时(DST)。这意味着在夏令时开始和结束时当时钟向前或向后拨动一小时时，实际任务启动时间不更改。

    我们不建议您使用该计划。它用于向后兼容 Kaspersky Security Center。

    默认下，任务每天于当前系统时间运行一次。

  - **按星期中的天数**

    任务在每周指定日期的指定时间定期运行。

    默认情况下，任务在每周五 6:00:00 PM 运行。

  - **每月**

    任务定期运行，在指定月日的指定时间。

    在缺少指定日的月份，任务在最后一天运行。

    默认下，任务在每月的第一天运行，在当前系统时间。

  - **一次**

    该任务在指定的日期和时间运行一次（默认情况下，在创建任务的当天）。

  - **手动**

    任务不自动运行。您仅可以手动启动。

默认情况下已选定该选项。

- **立即**

  当设备在网络上可见或当设备被纳入任务范围后，任务会立即运行。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

9. 在向导的此步骤中，指定您正在创建的任务的名称。
10. 在向导的“**完成任务创建**”步骤，单击**完成**按钮结束向导。

    如果您想让任务在向导完成时立即启动，选择“**向导完成时运行任务**”复选框。

在任务执行完毕后，为其创建任务的客户端设备将由任务设置中指定的管理服务器进行管理。

如果管理服务器支持加密和数据保护，并且您正在创建*更改管理服务器*任务，将显示警告。警告声明如果有加密数据存储在设备，在新服务器开始管理设备之后，用户将仅可以访问他之前使用过的加密数据。除此之外，将不会提供对加密数据的访问权限。有关不提供加密数据访问权限的情况的详细说明，请参见 Kaspersky Endpoint Security for Windows 帮助。

通过连接网关将连接到管理服务器的设备移动到另一台管理服务器

您可以将通过连接网关连接到管理服务器的设备移动到另一台管理服务器。例如，如果您安装了另一个版本的管理服务器并且不想在设备上重新安装网络代理（因为这可能很耗时），则可能需要这样做。

说明中描述的命令必须在具有管理员权限的账户下在客户端设备上运行。

要将通过连接网关连接的设备移动到另一台管理服务器：

1. 使用`-address <服务器地址>`参数运行klmover 实用程序，切换到新的管理服务器。
2. 运行`klnagchk -nagwait -tl 4`命令。
3. 运行以下命令设置新的连接网关：
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<网关 IP 或者名称>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     在此，`<网关 IP 或者名称>`是可从互联网访问的连接网关的地址。
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000`是连接网关正在监听的 TCP 端口号。
4. 运行`klnagchk -restart -tl 4`命令，启动网络代理服务。

该设备将被移动到新的管理服务器并通过新的连接网关进行连接。

集群和服务器阵列

Kaspersky Security Center 支持集群技术。如果网络代理向管理服务器发送信息确认组成服务器阵列的客户端设备上已安装该应用程序，则该客户端设备就成为一个集群节点。集群将作为单个对象添加在控制台树的“**受管理设备**”文件夹中，并带有服务器图标（ ）。

可以区分集群的一些常见功能：

- 集群及其任何节点始终在同一管理组中。
- 如果管理员尝试移动集群节点，则该节点会移回其原始位置。
- 如果管理员尝试将集群移至其他组，则其所有节点随之一起移动。

远程开启、关闭和重启客户端设备

Kaspersky Security Center 允许您远程管理客户端设备：开机、关机和重启。

要远程管理客户端设备：

1. 连接至管理设备的管理服务器。
2. 使用以下方法之一创建设备管理任务：
   - 如果您要对所选管理组中的设备进行打开、关闭或重启操作，请创建选定组的任务。
   - 如需对各管理组或非组内的设备执行打开、关闭或重启操作，请创建特定设备的任务。

   “新任务向导”启动。遵照向导的说明操作。在新任务向导的“**选择任务类型**”窗口中，选择 **Kaspersky Security Center** 节点，打开“**高级**”文件夹，选择**管理设备**任务。
3. 运行创建的任务。

任务完成后，选定设备将执行所选命令（开启、关闭或重启）。

关于在受管理设备和管理服务器之间使用持续连接

默认下，Kaspersky Security Center 不提供受管理设备和管理服务器之间的持续连接。受管理设备上的网络代理定期建立连接并与管理服务器同步。这些同步会话之间的间隔在网络代理的策略中定义，默认为 15 分钟。如果需要提前同步（例如，强制应用策略），管理服务器将向端口 UDP 15000 上的网络代理发送签名网络数据包。（管理服务器可以通过 IPv4 或 IPv6 网络发送此数据包。）如果管理服务器和受管理设备之间由于任何原因无法通过 UDP 进行连接，则同步将在同步间隔内网络代理和管理服务器之间的下一个例行连接时运行。

但是，如果网络代理和管理服务器之间没有提早连接，则无法执行某些操作。这些操作包括运行和停止本地任务、接收受管理应用程序的统计信息以及创建隧道。要执行这些操作，必须在受管理设备上启用“**不断开与管理服务器的连接**”选项。

关于强制同步

尽管 Kaspersky Security Center 自动为受管理设备同步状态、设置、任务和策略，一些情况下，管理员需要准确知道是否同步已经在指定设备上执行。

在管理控制台受管理设备的上下文菜单中，“**所有任务**”菜单项包含“**强制同步**”命令。当 Kaspersky Security Center 15.1 执行该命令时，管理服务器试图连接到设备。如果该尝试成功，强制同步将被执行。否则，同步将仅在网络代理与管理服务器的下一次计划连接后被强制。

关于连接计划

在网络代理属性窗口，在“**连接**”区域的“**连接计划**”子区域，您可以指定网络代理传送数据到管理服务器的时间间隔。

必要时连接。如果选中此选项，当网络代理需要发送数据到管理服务器时连接才被建立。

在指定时间间隔连接。如果选中此选项，网络代理在指定时间连接到管理服务器。您可以添加若干个连接时间段。

发送消息到设备用户

要发送消息到设备用户：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 以下列方式之一，为设备用户创建消息发送任务：
   - 如果要向属于所选管理组的设备用户发送消息，请创建所选组任务。
   - 如果要向属于不同管理组或不属于任何管理组的设备用户发送消息，请创建特定设备的任务。

   “新任务向导”启动。遵照向导的说明操作。
3. 在新任务向导的任务类型窗口中，选择 **Kaspersky Security Center 管理服务器**节点，打开“**高级**”文件夹，选择**将消息发送至用户**任务。发送消息到用户任务仅对 Windows 设备可用。您也可以在**用户账户**文件夹的用户的上下文菜单中发送消息。
4. 运行创建的任务。

   任务完成后，创建的消息将被发送给选定设备用户。发送消息到用户任务仅对 Windows 设备可用。您也可以在**用户账户**文件夹的用户的上下文菜单中发送消息。

管理 Kaspersky Security for Virtualization

Kaspersky Security Center 支持将虚拟机连接到管理服务器的功能。虚拟机受 Kaspersky Security for Virtualization 保护。有关详细信息，请参阅此应用程序的文档。

配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

要启用更改设备状态到严重：

1. 通过下列方式之一打开属性窗口：
   - 在“**策略**”文件夹，在管理服务器策略的上下文菜单中选择“**属性**”。
   - 在管理组的上下文菜单中选择**属性**。
2. 在打开的**属性**窗口中，在“**区域**”窗格中选择“**设备状态**”。

3. 在右侧窗格中的“**设置状态为“严重”，如果这些被指定**”区域，从列表中选择条件旁边的复选框。

   您只能更改未在父策略中锁定的设置。

4. 双击所选条件的名称，然后在打开的窗口中设置该条件所需的值。

   您不能为以下条件设置值：安全应用程序未安装、安装了不兼容的应用程序、检测到软件漏洞、移动设备设置不遵从策略、检测到未处理的安全问题、应用程序定义的设备状态、设备已失去管理、安全应用程序没有运行、授权许可已过期。

   对于**需要重新启动**条件，您可以指定重启原因。我们建议您选中列表中所有原因旁边的复选框。

5. 单击“**确定**”。

满足指定条件时，受管理设备被分配*严重*状态。

要启用更改设备状态到警告：

1. 通过下列方式之一打开属性窗口：

   - 在“**策略**”文件夹，在管理服务器策略的上下文菜单中选择“**属性**”。
   - 在管理组的上下文菜单中选择**属性**。

2. 在打开的**属性**窗口中，在“**区域**”窗格中选择“**设备状态**”。

3. 在右侧窗格中的“**设置状态为“警告”，如果这些被指定**”区域，从列表中选择条件旁边的复选框。

   您只能更改未在父策略中锁定的设置。

4. 双击所选条件的名称，然后在打开的窗口中设置该条件所需的值。

   您不能为以下条件设置值：安全应用程序未安装、安装了不兼容的应用程序、检测到软件漏洞、移动设备设置不遵从策略、检测到未处理的安全问题、应用程序定义的设备状态、设备已失去管理、安全应用程序没有运行、授权许可已过期。

   对于**需要重新启动**条件，您可以指定重启原因。我们建议您选中列表中所有原因旁边的复选框。

5. 单击“**确定**”。

满足指定条件时，受管理设备被分配*警告*状态。

标记设备和查看分配的标签

Kaspersky Security Center 允许您标记设备。*标签*是设备 ID，可以用于分组、描述或查找设备。分配到设备的标签可以用于创建分类、查找设备以及分发设备到管理组。

您可以手动或自动标记设备。在设备属性中手动标记设备；当您必须标记单个设备时，您可以使用手动标记。自动标记由管理服务器利用指定标记规则来执行。

在管理服务器属性中，您可以给由此管理服务器管理的设备设置自动标记。当指定条件被满足时，设备被自动标记。单个规则对应于每个标记。规则应用到设备网络属性、操作系统、设备上安装的应用程序以及其他设备属性。例如，您可以设置规则以分配*Win*标签到运行 Windows 的所有设备。然后，您可以在创建设备分类时使用该标签；这将帮助您整理所有运行 Windows 的设备，并给它们分配任务。

您也可以使用标签作为策略配置文件在受管理设备上的激活条件，以便仅在带有特殊标签的设备上应用特殊策略配置文件。例如，如果被标记为*Courier*的设备出现在*用户*管理组，且通过标记*Courier*对策略配置文件的激活被启用，则为*用户*组创建的策略将不应用到该设备—但是策略配置文件的配置文件将被应用。策略配置文件可以允许该设备启动一些被策略阻止运行的应用程序。

您可以创建多个标记规则。如果您创建了多个标记规则且规则对应的条件同时被满足，单个设备可以被分配多个标签。您可以在设备属性中查看所有分配的标签列表。每个标记规则可以被启用或禁用。如果规则被启用，它被应用到由管理服务器管理的设备。如果您当前不使用规则，但可能今后需要，您不用删除它；您只需清空"**启用规则**"复选框。此种情况下，规则被禁用；它在"**启用规则**"复选框被再次选中之前不会被执行。如果您必须从标记规则列表临时排除规则然后以后再次包含它，您可能需要禁用规则而不删除。

自动设备标记

您可以在管理服务器"属性"窗口中创建和编辑自动标记规则。

要自动标记设备：

1. 在控制台树中，选择您要为其指定标记规则的管理服务器节点。
2. 在管理服务器的上下文菜单中，选择"**属性**"。
3. 在管理服务器属性窗口，选择"**标记规则**"区域。
4. 在"**标记规则**"区域中，单击"**添加**"按钮。
   "**新规则**"窗口将开启。
5. 在"**新规则**"窗口，配置规则的常规设置：
   - 指定规则名称。
     规则名称不能包含多于 255 个字符并且不能包括任何特殊字符（例如 "*<>?\:|）。
   - 使用"**启用规则**"复选框启用或禁用规则。
     默认情况下选中"**启用规则**"复选框。
   - 在"**标签**"字段中，输入标签名称。
     标签名称不能包含多于 255 个字符并且不能包括任何特殊字符（"*<>?\:|）。
6. 在"**条件**"区域，单击"**添加**"按钮来添加新条件，或单击"**属性**"按钮编辑现有条件。
   "新自动标记规则条件向导"窗口打开。
7. 在"**标签分配条件**"窗口，选择影响标记的条件的复选框。您可以选择多个条件。
8. 根据您选择的标记条件，向导将显示设置对应条件的窗口。设置根据以下条件的规则触发：
   - **设备使用或与特定网络的关联**—设备网络属性，例如 Windows 网络中的设备名称，设备包含在域或 IP 子网中。

     如果为您用于 Kaspersky Security Center 的数据库设置了区分大小写的排序规则，请在指定设备 DNS 名称时保持大小写。否则，自动标记规则将不起作用。

   - **使用活动目录**—设备出现在活动目录组织单元中，设备属于活动目录组。

- **特定应用程序**—设备上是否存在网络代理，操作系统类型、版本和架构。
- **虚拟机**—设备是否属于指定类型的虚拟机。
- **应用程序注册表中的应用程序已安装**—设备上是否存在不同供应商的应用程序。

9. 设置条件后，为其输入名称，然后关闭向导。

   如果必要，您可以为一个规则设置多个条件。此种情况下，在满足至少一个条件时，标签将被分配到设备。您添加的条件将显示在规则属性窗口中。

10. 在“**新规则**”窗口单击“**确定**”，并在管理服务器属性窗口单击“**确定**”。

所创建的规则被强加到被所选管理服务器管理的设备。如果设备的设置满足规则条件，标签被分配到设备。

查看和配置分配到设备的标签

您可以查看分配到设备的所有标签的列表，以及在设备属性窗口中继续设置自动标记规则。

要查看和设置分配到设备的标签：

1. 在控制台树中，选择“**受管理设备**”文件夹。
2. 在“**受管理设备**”文件夹的工作区，选择您要查看所分配的标签的设备。
3. 在移动设备的上下文菜单中，选择“**属性**”。
4. 在设备属性窗口中，选择**标签**区域。

   分配到所选设备的标签列表被显示，以及标签被分配的方式：手动或根据规则。
5. 如果必要，请执行以下操作之一：
   - 要继续设置标记规则，点击**设置自动标记规则**链接（仅对 Windows 可用）。
   - 要重命名标签，选择该标签并点击**重命名**按钮。
   - 要删除标签，选择该标签并点击**删除**按钮。
   - 要手动添加标签，在**标签**区域下方的字段中输入标签，并点击**添加**按钮。
6. 点击**应用**按钮，如果您对**标签**区域做了更改，以便更改生效。
7. 单击“**确定**”。

如果您在设备属性中删除或重命名一个标签，该更改不影响到管理服务器属性中定义的标记规则。更改将仅应用到修改了属性的设备。

客户端设备的远程诊断。Kaspersky Security Center 远程诊断工具

Kaspersky Security Center 远程诊断实用程序（以下称为远程诊断实用程序）可在客户端设备上远程执行下列操作：

- 启用和禁用跟踪、更改跟踪级别、下载跟踪文件。
- 下载系统信息和应用程序设置。
- 下载事件日志。
- 为应用程序创建内存转储文件。
- 开始诊断并下载诊断报告。
- 启动和停止应用程序。

您可以使用从客户端设备下载的事件日志和诊断报告以自行定位问题。同时，Kaspersky 技术支持专家可能让您从客户端设备下载跟踪文件、内存转储文件、事件日志和诊断报告以便让 Kaspersky 进一步分析。

远程诊断实用程序将随管理控制台一起自动安装在设备上。

将远程诊断实用程序连接至客户端设备

要将远程诊断实用程序连接至客户端设备，请执行以下操作：

1. 在控制台树中选择任意管理组。
2. 在工作区的“**设备**”选项卡中，从任何设备的上下文菜单中选择**自定义工具 → 远程诊断**。
   系统将打开远程诊断实用程序的主窗口。
3. 在远程诊断实用程序主窗口的第一个字段中指定您希望用来连接设备的工具：
   - **使用 Microsoft Windows 网络访问**。
   - **使用管理服务器访问**。
4. 如果您在实用程序主窗口的第一个字段中选择了“**使用 Microsoft Windows 网络访问**”，请执行以下操作：
   - 在“**设备**”字段，指定您要连接的设备地址
     您可以使用 IP 地址、NetBIOS 名称或 DNS 名称作为设备地址。
     默认值是运行了实用程序的设备的上下文菜单上显示的地址。
   - 指定连接到该设备的账户：
     - **使用当前用户连接**（默认选择）。使用当前用户账户连接。
     - **使用提供的用户名和密码来连接**。使用提供的用户账户连接。指定所需账户的“**用户名**”和“**密码**”。

只有使用设备的本地管理员账户才可连接到设备。

5. 如果您在实用程序主窗口的第一个字段中选择了“**使用管理服务器访问**”，请执行以下操作：

- 在“**管理服务器**”字段中指定您希望连接设备的管理服务器地址。

  您可以使用 IP 地址、NetBIOS 名称或 DNS 名称作为服务器地址。

  默认值为当前运行实用程序的管理服务器地址。

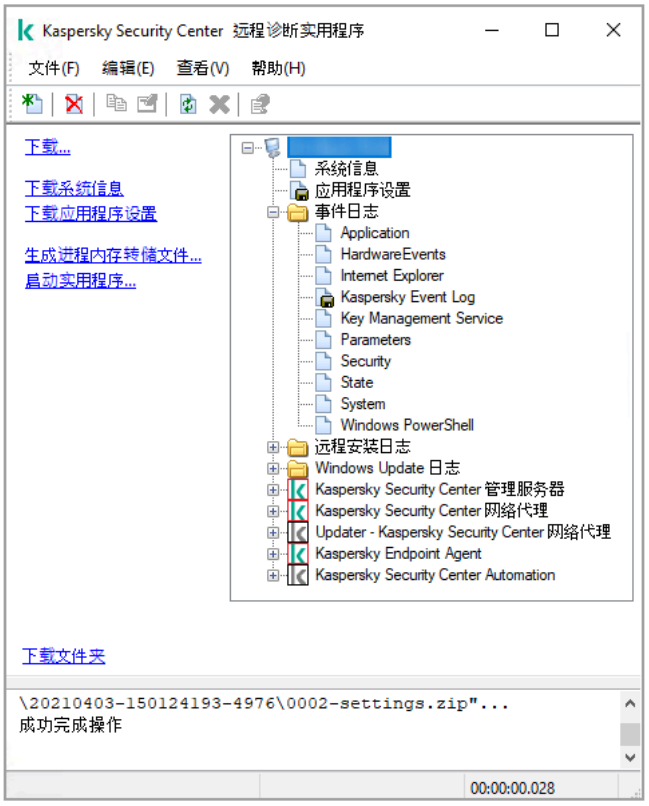
- 如果需要，选择“**使用 SSL**”、“**压缩流量**”和“**属于从属管理服务器的设备**”复选框。

  如果选择了“**属于从属管理服务器的设备**”复选框，则可以通过单击“**浏览**”按钮在“**属于从属管理服务器的设备**”字段中填入管理该设备的从属管理服务器的名称。

6. 要连接设备，请单击“**登录**”按钮。

如果您的账户启用了两步验证，则必须通过两步验证进行授权。

这将打开对设备进行远程诊断的窗口（参见下图）。窗口左侧包含设备远程诊断操作链接。窗口右侧包含实用程序可管理的设备对象树。窗口底部显示实用程序运行进程。



远程诊断实用程序。远程设备诊断窗口

远程诊断实用程序把从设备上下载的文件保存在运行该程序的设备的桌面上。

为应用程序创建内存转储文件

应用程序转储文件允许您查看某个时间点在客户端设备上运行的应用程序的参数。该文件还包含有关为应用程序加载的模块的信息。

不支持从基于 Linux 的设备获取转储。

为了通过远程诊断获取转储，可以使用 kldumper 实用程序。此实用程序旨在根据技术支持专家的要求获取卡巴斯基应用程序进程的转储。有关使用 kldumper 实用程序的要求的详细信息，请参阅Kaspersky Security Center 知识库。

要为应用程序创建转储文件：

1. 在**受管理设备**文件夹的工作区中，在**设备**选项卡上，打开必要设备的上下文菜单，然后选择**自定义工具→远程诊断**。

   Kaspersky Security Center 远程诊断实用程序窗口打开。

2. 将远程诊断实用程序连接至客户端设备。

   这将打开对设备进行远程诊断的窗口。

3. 在窗口左侧，单击**生成进程内存转储文件**链接。

4. 在打开**生成进程内存转储文件**视窗中，指定要为其生成转储文件的应用程序的可执行文件。

5. 单击“**确定**”按钮。

   包含指定应用程序的转储文件的档案被下载。

   如果客户端设备上未运行指定的应用程序，则下载的存档中包含的“结果”文件夹将为空。

   如果指定的应用程序正在运行，但下载失败并出现错误，或者下载的存档中包含的“结果”文件夹为空，请参阅Kaspersky Security Center 知识库。

启用和禁用跟踪，下载跟踪文件

要在远程设备上启用跟踪：

1. 运行远程诊断实用程序，并连接至必要设备。

2. 在设备的对象树中，选择您要启用跟踪的应用程序。

   只有当设备使用管理服务器工具连接时，才能为具有自我保护功能的应用程序启用和禁用跟踪。

   如果您想要启用网络代理跟踪，您也可以通过创建安装所需更新并修复漏洞任务来实现。此种情况下，在网络代理跟踪已在远程诊断实用程序中被禁用时，网络代理依然会写入跟踪信息。

3. 要启用跟踪：

   a. 在远程诊断实用程序窗口左侧，单击“**启用跟踪**”。

   b. 在打开的“**选择跟踪级别**”窗口中，我们建议您保留设置的默认值。当需要时，技术支持专家将指导您配置过程。下列设置可用：

   - **跟踪级别**

     跟踪级别定义跟踪文件包含的详情数据量。

   - “**基于循环的跟踪**”（仅适用于 Kaspersky Endpoint Security）

     应用程序覆盖跟踪信息以防止跟踪文件过量增长。指定用于存储跟踪信息的文件最大数量，以及每个文件的最大大小。如果写入了最大数量的最大大小的跟踪文件，最旧的文件被删除以便新跟踪文件可以被写入。

   c. 单击“**确定**”。

4. 对于 Kaspersky Endpoint Security，技术支持专家可能要求您对系统性能信息启用 Xperf 跟踪。

   要启用 Xperf 跟踪：

   a. 在远程诊断实用程序窗口左侧，单击“**启用 Xperf 跟踪**”。

   b. 在打开的“**选择跟踪级别**”窗口中，根据技术支持专家的请求，选择以下跟踪级别之一：

   - **轻度级别**

     该类型的跟踪文件包含系统最少量信息。

     默认情况下已选定该选项。

   - **深度级别**

     相比于*轻度*类型的跟踪文件，该类型的跟踪文件包含更多详细信息，且可能在*轻度*类型跟踪文件不足以评估性能时被技术支持专家要求。*深度*跟踪文件包含关于系统的硬件、操作系统、应用程序的启动和结束进程列表、用于性能评估的事件和来自 Windows System Assessment 工具的事件的技术信息。

   c. 选择以下跟踪类型之一：

   - **基本类型**

     跟踪信息在 Kaspersky Endpoint Security 应用程序运行期间被接收。

     默认情况下已选定该选项。

   - **重启时类型**

     跟踪信息在操作系统从受管理设备上启动时接收。该跟踪类型在影响系统性能的问题发生时，在设备被开启后和 Kaspersky Endpoint Security 启动之前有效。

d. 您可能被要求启用“**基于循环的跟踪**”选项以防止跟踪文件的过量增长。然后指定跟踪文件的最大大小。当文件达到最大大小时，最旧的跟踪信息被新信息覆盖。

e. 单击“**确定**”。

某些情况下，要启用跟踪，必须重新启动安全应用程序及其任务。

远程诊断工具对所选应用程序启用跟踪。

要下载应用程序的跟踪文件：

1. 运行远程诊断工具并连接到必要的设备，描述在“连接远程诊断工具到客户端设备”。
2. 在应用程序节点的“**跟踪文件**”文件夹，选择所需文件。
3. 在远程诊断实用程序窗口左侧，单击“**下载整个文件**”。
   如果文件较大，则只有最近的跟踪部分可以下载。
   您可以删除突出显示的跟踪文件。禁用跟踪后，您可以删除该文件。

所选文件被下载到窗口下方指定的位置。

要在远程设备上禁用跟踪：

1. 运行远程诊断工具并连接到必要的设备，描述在“连接远程诊断工具到客户端设备”。
2. 在设备的对象树中，选择您要禁用跟踪的应用程序。

   只有当设备使用管理服务器工具连接时，才能为具有自我保护功能的应用程序启用和禁用跟踪。

3. 在远程诊断实用程序窗口左侧，单击“**禁用跟踪**”。

远程诊断工具对所选应用程序禁用跟踪。

下载应用程序设置

要从远程设备下载应用程序设置：

1. 运行远程诊断工具并连接到必要的设备，描述在“连接远程诊断工具到客户端设备”。
2. 在远程诊断实用程序窗口的对象树中，选择设备名称顶层节点。
3. 在远程诊断实用程序窗口的左侧，从以下选项中选择您需要的操作：

   - **下载系统信息**
   - **下载应用程序设置**
   - **生成进程内存转储文件**
     单击此链接后，在打开的窗口中，指定要为其生成内存转储文件的应用程序的可执行文件。

- **启动实用程序**

  单击此链接后，在打开的窗口中，指定实用程序的可执行文件及其运行设置。

所选实用程序将被下载，并启动于设备上。

下载事件日志

要从远程设备下载事件日志：

1. 运行远程诊断工具并连接到必要的设备，描述在"连接远程诊断工具到客户端设备"。
2. 在设备对象树的"**系统事件日志**"文件夹，选择相关日志。
3. 通过点击远程诊断实用程序窗口左侧的**下载事件日志 <事件日志名称>**链接下载所选日志。

所选事件日志被下载到窗口下方指定的位置。

下载多个诊断信息条目

Kaspersky Security Center 远程诊断实用程序允许您下载诊断信息的多个条目，包括事件日志、系统信息、跟踪文件和内存转储文件。

要从远程设备下载诊断信息：

1. 运行远程诊断工具并连接到必要的设备，描述在"连接远程诊断工具到客户端设备"。
2. 在远程诊断实用程序窗口左侧，单击"**下载**"。
3. 选择您要下载的条目旁边的复选框。
4. 单击**开始**。

每个所选条目被下载到窗格下方指定的位置。

开始诊断并下载诊断结果

要为某远程设备应用程序启动诊断并下载其运行结果，请执行以下操作：

1. 运行远程诊断工具并连接到必要的设备，描述在"连接远程诊断工具到客户端设备"。
2. 在设备的对象树中，选择必要的应用程序。
3. 然后通过点击远程诊断实用程序窗口左侧的"**运行诊断**"链接来启动诊断。

   诊断报告将显示在对象树中所选应用程序的节点中。
4. 在对象树中选择新生成的诊断报告，然后单击"**下载文件夹**"链接下载该报告。

所选报告被下载到窗口下方指定的位置。

开始、停止和重新启动应用程序

只有使用管理服务器工具连接设备后，您才能启动、停止和重新启动应用程序。

若要启动、停止和重新启动应用程序，请执行以下操作：

1. 运行远程诊断工具并连接到必要的设备，描述在"连接远程诊断工具到客户端设备"。
2. 在设备的对象树中，选择必要的应用程序。
3. 在远程诊断实用程序窗口的左侧选择操作：
   - **停止应用程序**
   - **重启应用程序**
   - **启动应用程序**

   根据您选择的操作，应用程序被启动、停止或重启。

UEFI 保护设备

*UEFI 保护设备*是在 BIOS 级别集成了适用于 UEFI 的卡巴斯基解决方案或应用程序的设备。整合的保护从系统启动时开始确保设备安全，未整合软件的设备仅在安全应用程序启动后开始保护工作。支持这些设备的管理的 Kaspersky Security Center。

要修改 UEFI 保护设备的连接设置：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在管理服务器的上下文菜单中，选择"**属性**"。
3. 在管理服务器属性窗口，选择**服务器连接设置** → **附加端口**。
4. 在"**附加端口**"区域，修改相关设置：
   - **打开 UEFI 保护设备和 KasperskyOS 设备的端口**

     UEFI 保护设备可以连接到管理服务器。

   - **UEFI 保护设备和 KasperskyOS 设备的端口**

     如果启用了**打开 UEFI 保护设备和 KasperskyOS 设备的端口**选项，您可以更改端口号。默认端口号是 13294。

5. 单击"**确定**"。

受管理设备设置

要查看受管理设备设置：

1. 在控制台树中，选择“**受管理设备**”文件夹。
2. 在文件夹的工作区，选择一个设备。
3. 在设备的上下文菜单中，选择“**属性**”。

此时将打开所选设备的属性窗口，并选中“**常规**”区域。

常规

“**常规**”区域显示有关客户端设备的常规信息。信息基于上一次客户端设备与管理服务器之间的同步接收的数据来提供：

- **名称**

  在该字段中，您可以查看和修改管理组中的客户端设备名称。

- **描述**

  在该字段中，您可以输入客户端设备的附加描述。

- **Windows 域**

  包含设备的 Windows 域或工作组。

- **NetBIOS 名称**

  客户端设备的 Windows 网络名。

- **DNS 名称**

  客户端设备的 DNS 域名称。

- **IP 地址**

  设备 IP 地址。

- **组**

  包括了客户端设备的管理组。

- **上次更新**

  设备上病毒数据库或应用程序最后更新日期。

- **上一次可见**

  设备在网络中最后可见的日期和时间。

- **连接到管理服务器**

  客户端设备上安装的网络代理上一次连接到管理服务器的日期和时间。

- **不断开与管理服务器的连接**

  如果启用此选项，将保持受管理设备和管理服务器之间的持续连接。如果正在使用的不是提供此类连接的推送服务器，您可能希望使用此选项。

  如果禁用此选项且推送服务器不在使用中，受管理设备将仅在同步数据或传输信息时连接至管理服务器。

  选中“**不断开与管理服务器的连接**”选项时的最大设备总数为 300。

  默认情况下已在受管理设备上禁用该选项。此选项在安装了管理服务器的设备上默认启用，即使您尝试禁用它也保持启用状态。

保护。

“**保护**”区域提供有关客户端设备上反病毒保护当前状态的信息：

- **设备状态**

  基于管理员定义的标准分配的关于设备上反病毒保护和网络中设备活动的客户端设备的状态。

- **所有问题**

  该表格包含了客户端设备上安装的受管理应用程序检测到的问题的完整列表。每个问题都伴有一个状态，应用程序建议您分配该状态到该问题的设备。

- **实时保护**

  该字段显示当前的客户端设备实时保护状态。

  当设备状态更改时，新状态仅在客户端设备与管理服务器同步之后显示在设备属性窗口。

- **上一次按需扫描**

  客户端设备上次执行恶意软件扫描的日期和时间。

- **检测到的威胁总数**

  自安装安全应用程序（第一次扫描）或自上次重置威胁计数器以来，在客户端设备上检测到的威胁总数。

- **活动威胁**

  客户端设备上的未处理文件数量。

  该字段移动设备上的未处理文件数量。

- **磁盘加密状态**

  设备本地驱动器上的当前文件加密状态。有关状态的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

应用程序

“**应用程序**”区域列出客户端设备上安装的所有 Kaspersky 应用程序。该区域包含启动按钮 ( ) 和停止按钮 ( )，可让您启动和停止所选的卡巴斯基应用程序（不包括网络代理）。如果受管理设备上的15000 UDP 端口可用，则启用这些按钮来接收来自管理服务器的推送通知。如果受管理设备无法接收推送通知，但启用了与管理服务器的持续连接模式（启用了**常规**部分中的**不断开与管理服务器的连接**选项），则开始和停止按钮也可用。此外，**应用程序**部分包含以下按钮：

- **事件**

  单击该按钮可查看当程序运行时在客户端设备上发生的事件的列表，以及查看该程序的任务结果。

- **统计**

  单击该按钮可查看有关程序的当前统计信息。

- **属性**

  单击该按钮可接收有关程序的信息并配置程序。

任务

在“**任务**”选项卡中，您可以管理客户端设备任务：查看现有任务列表、创建新任务、删除、启动和停止任务、修改任务设置以及查看执行结果。该任务列表由客户端最近一次与管理服务器进行同步的会话期间收到的数据提供。管理服务器请求客户端设备的任务状态详情。

如果受管理设备上的15000 UDP 端口可用，则启用开始 ( )、停止 ( ) 和移除 ( )按钮来接收来自管理服务器的推送通知。如果受管理设备无法接收推送通知，但启用了与管理服务器的持续连接模式（启用了**不断开与管理服务器的连接**部分中的**常规**选项），则开始、停止和移除按钮也可用。

如果未建立连接，则不显示任务状态，按钮被禁用。

事件

“**事件**”选项卡将显示选定客户端设备在管理服务器上所记录的事件。

您可以导出、复制和删除设备事件。

标签

在“**标签**”区域，您可以管理用于查找客户端设备的关键字列表：查看现有标签列表、从列表中分配标签、配置自动标记规则、添加新标签和重命名旧标签以及删除标签。

系统信息

“**常规系统信息**”区域提供有关在客户端设备上安装的应用程序的信息。

已安装的应用程序

在“**应用程序注册表**”区域，您可以查看客户端设备上安装的应用程序及其更新的注册表，您还可以设置应用程序注册表的显示。

如果客户端设备上安装的网络代理将所需信息发送到管理服务器，则将提供有关已安装应用程序的信息。您可以在网络代理或其策略的属性窗口中的“**存储库**”区域中配置将信息发送到管理服务器。

- **只显示不兼容的安全应用程序**

  如果启用此选项，则应用程序列表仅包含不与 Kaspersky 程序兼容的安全应用程序。

  默认情况下已禁用该选项。

- **显示更新**

  如果启用此选项，则应用程序列表不仅包含应用程序而且包含为其所安装的更新包。

  要显示更新列表，需要 100 KB 的流量。如果您关闭列表并重新打开它，您将不得不再次花费 100 KB 的流量。

  默认情况下已禁用该选项。

- **导出到文件**

  点击该按钮导出安装在设备上的应用程序列表到 CSV 文件或 TXT 文件。

- **历史记录**

  点击该按钮查看设备上的应用程序安装事件。以下信息被显示：

  - 应用程序被安装到设备的日期和时间
  - 应用程序名称

- 应用程序版本

- **属性**

  点击该按钮查看在设备上安装的应用程序列表中选中的应用程序的属性。以下信息被显示：

  - 应用程序名称
  - 应用程序版本
  - 应用程序供应商

可执行文件

“**可执行文件**”区域显示在客户端设备上发现的可执行文件。

硬件注册表

在“**硬件注册表**”区域，您可以查看客户端设备上安装的硬件的信息。您可以查看 Windows 设备和 Linux 设备的这一信息。

确保在要从中获取硬件详细信息的 Linux 设备上安装了 lshw 实用程序。根据所使用的 hypervisor，从虚拟机获取的硬件详细信息可能不完整。

如果网络代理安装在运行 Windows 的设备上，它会向管理服务器发送有关设备硬件的以下信息：

- RAM
- 大容量存储设备
- 主板
- CPU
- 网络适配器
- 监控器
- 视频适配器
- 声卡

如果网络代理安装在运行 Linux 或 macOS 的设备上，它会向管理服务器发送有关设备硬件的以下信息（如果该信息由操作系统提供）：

- 总 RAM 容量
- 大容量存储设备总容量
- 主板

- CPU
- 网络适配器

会话

“**会话**”区域仅对 Windows 设备显示，包含有关客户端设备所有者以及在所选客户端设备上工作过的用户账户的信息。

基于活动目录数据生成域用户相关信息。本地用户详情由安装在客户端设备上的 Windows Security Account Manager 提供。

- **设备所有者**

  设备所有者字段显示当管理员需要在客户端设备上执行操作时，他可以联系的用户名。

  分配和**属性**按钮可以用来选择设备所有者和查看拥有者用户信息。

  带有红叉的按钮可以用来删除当前设备所有者。

列表显示使用客户端设备的账户。

- **名称**

  在 Windows 网络中的设备名称。

- **参与者的名字**

  登录至该设备的系统的用户名称（域或本地名称）。

- **账户**

  登录至该设备的用户账户。

- **电子邮件**

  用户电子邮件地址。

- **电话**

  用户电话号码。

安全问题

在**安全问题**选项卡上，可以为客户端设备查看、编辑和创建安全问题。安全问题可以通过安装在客户端设备上的受管 Kaspersky 应用程序自动创建，也可以由管理员手动创建。例如，如果用户定期将恶意软件从其可移动驱动器移至设备，则管理员可以创建安全问题。管理员可以在安全问题文本中提供情况的简要说明和建议的操作（例如对于一个用户的纪律性操作），还可以添加链接到用户。

对其采用了所有必要操作的安全问题被称为*已处理安全问题*。存在的未处理安全问题可被选为将设备的状态更改为*严重*或*警告*的条件。

此部分包含已为设备创建的安全问题的列表。安全问题按严重级别和类型分类。安全问题类型由创建安全问题的卡巴斯基应用程序定义。选中**已处理**列中的复选框即可突出显示列表上的已处理安全问题。

软件漏洞

"**软件漏洞**"区域提供有关客户端设备上安装的第三方应用程序中的漏洞信息。您可以使用列表上方的搜索字段通过名称查找漏洞。

- **导出到文件**

  点击**导出到文件**按钮保存漏洞列表到文件。默认，应用程序导出漏洞列表到 CSV 文件。

- **仅显示可以被修复的漏洞**

  如果启用此选项，该区域会显示可通过使用补丁修复的漏洞。

  如果禁用此选项，该区域会同时显示可通过使用补丁修复的漏洞，以及未发布补丁的漏洞。

  默认情况下已启用该选项。

- **属性**

  在列表中选择一个软件漏洞，然后点击"**属性**"按钮以在单独的窗口中查看所选软件漏洞的属性。在窗口中，您可以执行以下操作：

  - 忽略此受管理设备上的软件漏洞（在管理控制台或 Kaspersky Security Center Web Console 中）。
  - 查看该漏洞的建议修复程序列表。
  - 手动指定软件更新以修复漏洞（在管理控制台或 Kaspersky Security Center Web Console 中）。
  - 查看漏洞实例。
  - 查看现有任务列表以修复漏洞，并创建新任务以修复漏洞。

可用更新

该区域显示在该设备上发现的未安装的软件更新列表。有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **显示已安装的更新**

  如果启用此选项，列表会显示在客户端设备上已安装和未安装的更新。

  默认情况下已禁用该选项。

活动策略

本节显示当前分配给此设备上的 Kaspersky 应用程序策略列表。

- **导出到文件**

  您可以单击“**导出到文件**”按钮将活动策略配置文件列表保存到文件。默认情况下，应用程序导出策略列表到 CSV 文件。

活动策略配置文件

- **活动策略配置文件**

  该列表允许您查看客户端设备上活动的现有策略配置文件信息。您可以使用列表上的搜索栏通过输入策略名称或策略配置文件名称来查找活动策略配置文件。

- **导出到文件**

  您可以点击“**导出到文件**”按钮可将活动策略配置文件列表保存到文件。默认情况下，程序导出策略配置文件列表到 CSV 文件。

分发点

该区域提供设备与之交互的分发点列表。

- **导出到文件**

  单击“**导出到文件**”按钮保存设备与之交互的分发点列表文件。默认下，程序导出设备列表到 CSV 文件。

- **属性**

  点击**属性**按钮查看和配置设备与之交互的分发点。

常规策略设置

常规

在“**常规**”区域，您可以修改策略状态并指定策略设置的继承：

- 在“**策略状态**”块，您可以选择策略的模式：

  - **活动策略**

    如果选择该选项，策略将变为活动状态。

默认情况下已选定该选项。

- **漫游策略**

  如果选择该选项，策略将在设备离开企业网络时变为活动状态。

- **非活动策略**

  如果选择该选项，策略将变为不活动状态，但它仍然存储在“**策略**”文件夹中。如果需要，您可以激活该策略。

- 在“**设置继承**”设置组中，您可以配置策略继承：

  - **从父策略继承设置**

    如果启用此选项，则策略设置值将从上一级组策略继承，因而被锁定。
    默认情况下已启用该选项。

  - **在子策略中强制继承设置**

    如果启用此选项，则在应用策略更改之后，将执行以下操作：
    - 策略设置的值将被传送到管理子组的策略，也就是子策略。
    - 在每个子策略属性窗口**常规**区域的**继承设置**区块，将自动启用**从父策略继承设置**选项。

    如果启用此选项，则子策略设置被锁定。
    默认情况下已禁用该选项。

事件配置

“**事件配置**”区域允许您配置事件记录和事件通知。事件根据重要级别用下面的标签分布：

- **严重**
  “**严重**”选项卡不显示在网络代理策略属性中。
- **功能失败**
- **警告**
- **信息**

在每个选项卡，列表显示在管理服务器上事件类型和默认事件存储的期限（天）。单击“**属性**”按钮，您可以指定列表中已选中的事件日志和通知设置。默认下，为整个管理服务器指定的通用通知设置被用于所有事件类型。然后，您可以更改所需事件类型的特别设置。

例如，在 **警告** 选项卡，您可以配置 **发生了安全问题** 事件类型。此类事件可能会发生，例如，当 分发点的可用磁盘空间 小于 2 GB（至少需要 4 GB 才能远程安装应用程序和下载更新）。若要配置 **发生了安全问题** 事件，选择它并单击 **属性** 按钮。之后，您可以指定存储发生的事件的位置以及如何通知它们。

如果网络代理检测到安全问题，您可以使用受管理设备的设置管理此问题。

要选择多个事件类型，使用 SHIFT 或 CTRL 键；要选择所有类型，使用“**全部选中**”按钮。

网络代理策略设置

若配置网络代理策略：

1. 在控制台树中，选择“**策略**”文件夹。
2. 在文件夹的工作区，选择网络代理策略。
3. 在策略的上下文菜单中，选择“**属性**”。

网络代理策略的属性窗口打开。

> 请参阅比较表格，它详细介绍了根据使用的操作系统类型如何应用以下设置。

常规

在“**常规**”区域，您可以修改策略状态并指定策略设置的继承：

- 在“**策略状态**”块，您可以选择策略的模式：
  - **活动策略**

    如果选择该选项，策略将变为活动状态。
    默认情况下已选定该选项。

  - **漫游策略**

    如果选择该选项，策略将在设备离开企业网络时变为活动状态。

  - **非活动策略**

    如果选择该选项，策略将变为不活动状态，但它仍然存储在“**策略**”文件夹中。如果需要，您可以激活该策略。

- 在“**设置继承**”设置组中，您可以配置策略继承：
  - **从父策略继承设置**

    如果启用此选项，则策略设置值将从上一级组策略继承，因而被锁定。
    默认情况下已启用该选项。

- **在子策略中强制继承设置**

  如果启用此选项，则在应用策略更改之后，将执行以下操作：
  - 策略设置的值将被传送到管理子组的策略，也就是子策略。
  - 在每个子策略属性窗口**常规**区域的**继承设置**区块，将自动启用**从父策略继承设置**选项。

  如果启用此选项，则子策略设置被锁定。

  默认情况下已禁用该选项。

事件配置

“**事件配置**”区域允许您配置事件记录和事件通知。事件根据重要级别用下面的标签分布：

- **严重**

  “**严重**”选项卡不显示在网络代理策略属性中。
- **功能失败**
- **警告**
- **信息**

在每个选项卡，列表显示在管理服务器上事件类型和默认事件存储的期限（天）。单击“**属性**”按钮，您可以指定列表中已选中的事件日志和通知设置。默认下，为整个管理服务器指定的通用通知设置被用于所有事件类型。然后，您可以更改所需事件类型的特别设置。

例如，在 **警告** 选项卡，您可以配置 **发生了安全问题** 事件类型。此类事件可能会发生，例如，当 分发点的可用磁盘空间 小于 2 GB（至少需要 4 GB 才能远程安装应用程序和下载更新）。若要配置 **发生了安全问题** 事件，选择它并单击 **属性** 按钮。之后，您可以指定存储发生的事件的位置以及如何通知它们。

如果网络代理检测到安全问题，您可以使用受管理设备的设置管理此问题。

要选择多个事件类型，使用 SHIFT 或 CTRL 键；要选择所有类型，使用“**全部选中**”按钮。

设置

在“**设置**”区域，您可以配置网络代理策略：

- **仅通过分发点分发文件**

  如果启用此选项，则受管理设备上的网络代理只从分发点检索更新。

  如果禁用此选项，则受管理设备上的网络代理从分发点或管理服务器检索更新。

  请注意，受管理设备上的安全应用程序从每个安全应用程序的更新任务中设置的源检索更新。如果启用“**仅通过分发点分发文件**”选项，请确保在更新任务中将 Kaspersky Security Center 设置为更新源。

  默认情况下已禁用该选项。

- **事件队列的最大大小(MB)**

  在该字段中，您可以指定事件队列可在驱动器上占据的最大空间。

  默认值为 2 MB。

- **应用程序被允许在设备上检索策略扩展数据**

  安装在受管理设备上的网络代理会将有关已应用的安全应用程序策略的信息传输到安全应用程序（例如，Kaspersky Endpoint Security for Windows）。您可以在安全应用程序界面查看传输的信息。

  网络代理传输以下信息：

  - 策略传输至受管理设备的时间。
  - 策略传输至受管理设备时的活动策略的名称。
  - 策略传输至受管理设备时漫游策略的名称（对于Linux 版网络代理不可用）。
  - 策略传输至受管理设备时包含受管理设备的管理组的名称和完整路径。
  - 策略传输至受管理设备时包含其名称和优先级的活动策略配置文件列表。

  您可以使用该信息来确保将正确的策略应用于设备并用于故障排除。默认情况下已禁用该选项。

- **保护网络代理服务免遭非授权的卸载或终止，并防止设置更改**

  当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

  启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

  默认情况下已禁用该选项。

- **使用卸载密码**

  如果启用此选项，则单击“**修改**”按钮可以指定 klmover 实用程序和网络代理远程卸载的密码。

  默认情况下已禁用该选项。

存储库

在“**存储库**”区域，您可以选择将其信息从网络代理发送到管理服务器的对象类型：

- **Windows Update 更新详情**

  如果启用此选项，则有关客户端设备上必须安装的 Microsoft Windows Update 更新的信息将发送至管理服务器。

  有时，即使禁用此选项，更新也会显示在“**可用更新**”区域的设备属性中。例如，如果组织的设备存在可被这些更新修复的漏洞，则可能出现这种情况。

  默认情况下已启用该选项。它仅适用于 Windows。

  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **软件漏洞和对应更新的详情**

  如果启用此选项，则将有关在受管理设备上检测到的第三方软件（包括 Microsoft 软件）中的漏洞信息以及有关修复第三方漏洞（不包括 Microsoft 软件）的软件更新信息发送到管理服务器。

  选择此选项（**软件漏洞和对应更新的详情）**会增加网络负载、管理服务器磁盘负载和网络代理资源消耗。

  默认情况下已启用该选项。它仅适用于 Windows。

  要管理 Microsoft 软件的软件更新，请使用“**Windows Update 更新详情**”选项。

- **硬件注册表的详细信息**

  安装在设备上的网络代理会将设备硬件的相关信息发送到管理服务器。您可以在设备属性中查看硬件详细信息。

  确保在要从中获取硬件详细信息的 Linux 设备上安装了 lshw 实用程序。根据所使用的 hypervisor，从虚拟机获取的硬件详细信息可能不完整。

- **已安装应用程序详情**

  如果启用此选项，则有关客户端设备上安装的应用程序的信息将发送至管理服务器。

  默认情况下已启用该选项。

- **包括补丁信息**

  有关在客户端设备上安装的应用程序补丁的信息将发送到管理服务器。启用此选项可能会增加管理服务器和 DBMS 的负载，并导致数据库数据量的增加。

  默认情况下已启用该选项。它仅适用于 Windows。

如果本区域中的某些设置被网络代理策略禁止，则您无法修改它们。

软件更新和漏洞

在“**软件更新和漏洞**”区域，您可以配置搜索和发布 Windows 更新以及启用扫描可执行文件以发现漏洞：

- **使用管理服务器作为 WSUS 服务器**

  如果启用此选项，Windows 更新将下载到管理服务器。管理服务器提供以集中模式通过网络代理下载更新到客户端设备的 Windows 更新服务。

  如果禁用此选项，则不使用管理服务器下载 Windows 更新。此种情况下，客户端设备自己接收 Windows 更新。

  默认情况下已禁用该选项。

- 在**允许用户管理 Windows Update 更新的安装**下，您可以限制用户可以使用 Windows Update 在他们的设备上手动安装的 Windows 更新。

  在运行 Windows 10 的设备上，如果 Windows Update 已经为设备找到更新，您在“**允许用户管理 Windows Update 更新安装**”下选择的新选项将仅在发现的更新被安装后才被应用。

在下拉列表中选择条目：

- **允许用户安装所有可应用 Windows Update 更新**

  用户可以安装所有可应用到他们设备的 Microsoft Windows Update 更新。

  如果您不希望干预更新安装，请选择该选项。

  当用户手动安装 Microsoft Windows Update 更新时，更新可能从 Microsoft 服务器下载，而不是从管理服务器。如果管理服务器还未下载这些更新，这是可能的。从 Microsoft 服务器下载更新导致额外流量。

- **仅允许用户安装批准的 Windows Update 更新**

  用户可以安装所有可应用到他们设备的和您批准的 Microsoft Windows Update 更新。

  例如，您可能想先在测试环境中检查更新安装以确保它们不干预设备操作，仅在这之后允许安装这些批准的更新到客户端设备。

  当用户手动安装 Microsoft Windows Update 更新时，更新可能从 Microsoft 服务器下载，而不是从管理服务器。如果管理服务器还未下载这些更新，这是可能的。从 Microsoft 服务器下载更新导致额外流量。

- **不允许用户安装 Windows Update 更新**

  用户无法在他们的设备上手动安装 Microsoft Windows Update 更新。所有可应用更新根据您的配置而安装。

  如果您想要集中管理更新的安装则选则此选项。

  例如，您可以想优化更新计划以便网络不过载。您可以计划稍后更新，以便它们不干预用户工作。

- 在“**Windows Update 搜索模式**”设置组中，您可以选择更新搜索模式：

  - **主动**

    如果选中该选项，管理服务器支持使用网络代理在客户端设备上从 Windows 更新代理发送请求至更新源：Windows 更新服务器（或简称为 WSUS）。然后，网络代理会将从 Windows 更新代理接收到的信息传送给管理服务器。

    仅在选择*查找漏洞和所需更新*任务的“**连接更新服务器更新数据**”选项时，该选项才生效。

    默认情况下已选定该选项。

  - **被动**

    如果您选定该选项，网络代理将从上次同步更新源之后定期从 Windows 更新代理将所检索更新的信息传递给管理服务器。如果 Windows 更新代理没有执行与更新源同步，管理服务器上有关更新的信息将变为过期。

    如果要从更新源的内存缓存中获取更新，请选择此选项。

- **已禁用**

  如果选中该选项，管理服务器不会请求任何有关更新的信息。

  例如，如果您想首先在本地设备上测试更新，请选择此选项。

- **当运行可执行文件时扫描其漏洞**

  如果启用此选项，系统将在运行可执行文件时扫描漏洞。

  默认情况下已启用该选项。

重启管理

如果受管理设备的操作系统必须重启才能正确使用、安装或卸载应用程序，您可以在“**重启管理**”区域指定要执行的操作：

- **不重启操作系统**

  操作系统将不重启。

- **如果必要，自动重启操作系统**

  如果必要，操作系统自动重启。

- **提示用户操作**

  程序提示用户重启操作系统。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用此选项，应用程序会以复选框旁边的字段中指定的频率提示用户允许重启操作系统。默认情况下，提示频率为 5 分钟。

    如果禁用此选项，应用程序不会反复提示用户允许重启。

    默认情况下已启用该选项。

  - **在该时间后强制重启(分钟)**

    如果启用此选项，提示用户之后，应用程序强制操作系统在选框旁边字段指定的时间间隔结束后进行重启。

    如果禁用此选项，应用程序不会强制重启。

    默认情况下已启用该选项。

  - **在该时间后强制关闭阻止会话中的应用程序(分钟)**

    用户设备锁定时，程序以强制模式关闭（指定不活动间隔之后自动锁定，或手动锁定）。

如果启用此选项，当输入字段中指定的时间间隔结束后，锁定设备上的应用程序将被强制关闭。

如果禁用此选项，应用程序在锁定的设备上不关闭。

默认情况下已禁用该选项。

Windows 桌面共享

您可以通过“**Windows 桌面共享**”区域启用并配置在使用共享桌面访问时用户的远程设备上执行的管理员操作的审计：

- **启用审计**

  如果启用该选项，远程设备上管理员的操作审计启用。远程设备上的管理员操作是被一一记录下来的:

  - 在远程设备的事件日志中
  - 在位于远程设备上网络代理安装文件夹中的扩展名为 syslog 的文件中
  - Kaspersky Security Center 的事件数据库

  当满足以下条件时,管理员操作审核可用：

  - 漏洞和补丁管理授权许可正在使用中
  - 管理员有权启动共享访问远程设备的桌面

  如果禁用此选项,远程设备上的管理员操作审核被禁用。

  默认情况下已禁用该选项。

- **读取时要监控的文件掩码**

  该列表包含文件掩码.启用审计,程序会监控管理员读取符合掩码的文件并保存读取文件的信息.如果选择了“**启用审计**”选框，则该列表可用。您可以编辑文件掩码,或在列表中添加新掩码.列表中每个新文件掩码需要在全新的一行中指定.

  默认,指定了以下文件掩码:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **修改时要监控的文件掩码**

  该列表包含远程设备上的文件掩码。启用审核时,程序会监控管理员对符合掩码的文件作出的更改,并保存修改的相关信息.如果选择了“**启用审计**”选框，则该列表可用。您可以编辑文件掩码,或在列表中添加新掩码.列表中每个新文件掩码需要在全新的一行中指定.

  默认,指定了以下文件掩码:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

管理补丁和更新

在“**管理补丁和更新**”区域，您可以配置更新的下载和分发以及补丁在受管理设备上的安装：

- **对未定义状态的组件自动安装可应用更新和补丁**

  如果启用此选项，带有*未定义*批准状态的 Kaspersky 应用程序在从更新服务器下载后将被自动安装在受管理设备。

如果禁用此选项，被下载和标注为*未定义*状态的 Kaspersky 补丁将仅在您改变其状态为*已批准*是被安装。

默认情况下已启用该选项。

- **提前从管理服务器下载更新和反病毒数据库(推荐)**

  如果启用此选项，离线模式更新下载被使用。当管理服务器接收更新时，它通知网络代理(安装网络代理的设备)将用于受管理应用程序的更新。当网络代理接收更新的信息后，它提前从管理服务器下载相关文件。在第一次连接网络代理时，管理服务器发起更新下载。网络代理下载所有更新到客户端设备后，更新对该设备上的应用程序可用。

  当客户端设备上的受管理应用程序尝试访问网络代理以更新时，该网络代理检查其是否具有所有的更新。如果在受管理应用程序请求更新之前 25 小时内，更新已从管理服务器收到，则网络代理不连接到管理服务器，而是从本地缓存提供更新给受管理应用程序。当网络代理提供更新到客户端设备上的应用程序时，到管理服务器的连接可能不被建立，但是更新不需要连接。

  如果禁用此选项，离线模式更新下载不被使用。更新根据更新下载任务的计划被分发。

  默认情况下已启用该选项。

连接

“**连接**”区域包含三个嵌套子区域：

- **网络**
- **连接配置文件**（仅适用于 Windows 和 macOS）
- **连接计划**

在“**网络**”子区域，您可以配置到管理服务器的连接，启用 UDP 端口的使用并指定其端口号。下列选项可用：

- 在“**到管理服务器的连接**”设置组，您可以配置到管理服务器的连接并指定同步客户端设备和管理服务器的时间间隔：

  - **压缩网络流量**

    如果启用此选项，则通过减少所传输的流量进而减少管理服务器的负载来提高网络代理的数据传输速度。

    客户端设备上的 CPU 负载可能会增加。

    默认情况下启用该复选框。

  - **在 Microsoft Windows 防火墙中打开网络代理端口**

    如果启用此选项，网络代理工作所需的端口将添加到 Microsoft Windows 防火墙排除列表中。

    默认情况下已启用该选项。

  - **使用 SSL**

    如果启用此选项，则使用 SSL 协议通过安全端口连接管理服务器。

默认情况下已启用该选项。

- **以默认连接设置在分发点(如果可用)上使用连接网关**

  如果启用此选项，分发点上的连接网关在管理组属性指定的设置下使用。

  默认情况下已启用该选项。

- **使用 UDP 端口**

  如果需要网络代理通过 UDP 端口连接到管理服务器，启用“**使用 UDP 端口**”选项，并指定“**UDP 端口号**”。默认情况下已启用该选项。连接到管理服务器的默认 UDP 端口是 15000。

- **UDP 端口号**

  在该字段中，您可以输入 UDP 端口号。默认端口号是 15000。

  使用十进制系统记录。

  如果客户端设备运行在 Windows XP Service Pack 2 系统下，则集成的防火墙会阻止 UDP 端口 15000。请手动打开此端口。

- **使用分发点强制连接到管理服务器**

  如果在分发点设置窗口中选择了“**将此分发点用作推送服务器**”选项，则选择此选项。否则，分发点不会用作推送服务器。

在“**连接配置文件**”子区域，您可以指定网络位置设置，为管理服务器配置连接配置文件，以及在管理服务器不可用时启用漫游模式。

- **网络位置设置**

  网络位置设置用于定义客户端设备所连接的网络属性，并指定当网络特性改变时，网络代理从一个管理服务器连接配置文件切换到另一个配置文件的规则。

- **管理服务器连接配置文件**

  在该区域中，您可以查看和配置网络代理至管理服务器的连接。在该区域，您也可以创建当以下事件发生时，切换网络代理到不同管理服务器的规则：

  - 当客户端设备连接到另一个本地网络时
  - 当设备与组织的本地网络丢失连接时
  - 当连接网关的地址更改或 DNS 服务器地址修改时

  连接配置文件仅支持运行 Windows 和 macOS 的设备。

- **当管理服务器不可用时启用漫游模式**

  如果启用此选项，则在通过该配置文件连接的情况下，客户端设备上安装的应用程序将使用漫游模式设备的策略配置文件，以及漫游策略。如果没有为应用程序定义漫游策略，则使用激活策略。

  如果禁用此选项，则应用程序将使用已激活的策略。

  默认情况下已禁用该选项。

在“**连接计划**”子区域中，您可以指定网络代理发送数据到管理服务器的时间间隔：

- **必要时连接**

  如果选中此选项，当网络代理需要发送数据到管理服务器时连接才被建立。

  默认情况下已选定该选项。

- **在指定时间间隔连接**

  如果选中此选项，网络代理在指定时间连接到管理服务器。您可以添加若干个连接时间段。

分发点

“**分发点**”区域包含四个嵌套子区域：

- **网络轮询**
- **互联网连接设置**
- **KSN 代理**
- **更新**

在“**网络轮询**”子区域，您可以配置网络自动轮询。您可以启用三种类型的轮询，即网络轮询、IP 范围轮询和 Active Directory 轮询：

- **启用网络轮询**

  如果启用此选项，则管理服务器将按照所配置的计划自动轮询网络，单击“**设置快速轮询计划**”和“**设置完整轮询计划**”链接可配置轮询计划。

  如果禁用此选项，管理服务器将以**网络轮询频率(分钟)**字段中指定的时间间隔轮询网络。

  可以在“**Windows 域的轮询频率(分钟)**（适用于快速 Windows 网络轮询）和**网络轮询频率(分钟)**（适用于完整 Windows 网络轮询）”字段中配置 10.2 版之前的网络代理的设备发现间隔。

  默认情况下已禁用该选项。

- **启用 IP 范围轮询**

  如果启用此选项，则分发点将按照所配置的计划自动轮询 IP 范围，单击“**设置轮询计划**”按钮可配置轮询计划。

  如果禁用此选项，则分发点将不轮询 IP 范围。

对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置 IP 范围的轮询频率。如果启用此选项，则该字段可用。

默认情况下已禁用该选项。

- **使用 Zeroconf 轮询 (仅在 Linux 平台上；手动指定的 IP 范围将被忽略)**

  如果启用此选项，分发点将使用零配置网络（也称为 *Zeroconf*）轮询带有 IPv6 设备的网络。在这种情况下，已启用的 IP 范围轮询将被忽略，因为分发点将轮询整个网络。

  要开始使用 Zeroconf，必须满足以下条件：

  - 分发点必须运行 Linux。
  - 您必须在分发点上安装 avahi-browse 实用程序。

  如果禁用此选项，分发点不会轮询带有 IPv6 设备的网络。

  默认情况下已禁用该选项。

- **启用活动目录轮询**

  如果启用此选项，则分发点将按照所配置的计划自动轮询 Active Directory，单击“**设置轮询计划**”链接可配置轮询计划。

  如果禁用此选项，则管理服务器将不轮询 Active Directory。

  对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置活动目录的轮询频率。如果启用此选项，则字段可用。

  默认情况下已禁用该选项。

如果您的分发点在连接到互联网时使用代理服务器，则可以在**互联网连接设置**子部分中指定以下设置：

- **使用代理服务器**

  如果选择该选框，您可以在输入字段中配置代理服务器连接。

  默认情况下已清除该选框。

- **代理服务器地址**

  代理服务器地址。

- **端口号**

  用于连接的端口号。

- **对本地地址不使用代理服务器**

  如果启用此选项，将不使用代理服务器连接本地网络的设备。

  默认情况下已禁用该选项。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。
  默认情况下已清除该选框。

- **用户名**

  建立连接代理服务器的用户账户。

- **密码**

  任务运行时使用的账户的密码。

在“**KSN 代理**”子区域，您可以配置应用程序使用分发点从受管理设备转发 KSN 请求：

- **在分发点端启用 KSN 代理**

  KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。
  分发点将卡巴斯基安全网络声明中列出的KSN统计数据发送给卡巴斯基。
  默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器**和**我同意使用卡巴斯基安全网络**选项在管理服务器属性窗口中被启用时起作用。
  您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

- **转发 KSN 请求到管理服务器**

  分发点从受管理设备转发 KSN 请求到管理服务器。
  默认情况下已启用该选项。

- **通过互联网直接访问 KSN 云/KPSN**

  分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。
  安装了网络代理版本 11（或更早版本）的分发点不能直接访问 KPSN。如果要重新配置分发点以将 KSN 请求发送到 KPSN，请为每个分发点启用“**转发 KSN 请求到管理服务器**”选项。
  安装了网络代理版本 12（或更高版本）的分发点可以直接访问 KPSN。

- **TCP 端口**

  受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

- **使用 UDP 端口**

  如果需要网络代理通过 UDP 端口连接到管理服务器，启用“**使用 UDP 端口**”选项，并指定“**UDP 端口号**”。
  默认情况下已启用该选项。连接到管理服务器的默认 UDP 端口是 15000。

在“**更新**”子区域中，可以通过启用或禁用“**下载差异文件**”选项来指定网络代理是否应该下载差异文件。

修订历史

在“**修订历史**”选项卡，您可以查看网络代理策略修订历史。您可以比较修订、查看修订以及执行高级操作，例如保存修订到文件、回滚到修订和添加/编辑修订描述。

管理用户账户

该区域包含程序支持的用户账户及角色信息。本节包含有关如何创建 Kaspersky Security Center 用户账户和角色的说明。

Kaspersky Security Center 允许您管理用户账户以及账户组。应用程序支持三种账户类型：

- 组织员工的账户。在轮询组织的域控制器时管理服务器检索数据的域用户的账户。
- 本地用户账户。受管理设备上的本地账户，以及安装了管理服务器的设备上的本地账户。
- Kaspersky Security Center 内部用户的账户。您可以创建内部用户账户。这些账户仅在 Kaspersky Security Center 内使用。

使用用户账户

Kaspersky Security Center 允许您管理用户账户以及账户组。该程序支持两种账户类型:

- 组织员工的账户。在轮询组织网络时管理服务器检索数据的用户账户。
- 内部用户账户。当使用虚拟管理服务器时，这些账户被应用。只能在 Kaspersky Security Center 内创建和使用内部用户账户。

您可以通过下列方式之一查看用户账户列表：

- 在控制台树中，转到**高级→用户账户**。
- 在控制台树中，转到**受管理设备→设备** 选项卡 → <设备名称>链接 →**会话** 部分。
  会话部分显示运行 Windows 的设备上具有活动会话的用户账户。

如果满足以下要求，用户账户列表将正确显示：

- 使用与管理服务器相同版本或更高版本的网络代理。
- Active Directory 轮询已启用以显示域用户的账户。
- 在运行 Windows 的受管理设备上，**服务器 (LanmanServer)**服务正在运行。

您可以对用户账户及账户组执行以下操作：

- 通过使用角色配置访问应用程序特性的用户权限。
- 通过使用邮件和 SMS发送消息给用户。
- 查看用户移动设备列表。

- 交付并安装用户移动设备上的证书。
- 查看发布给用户的证书列表。
- 禁用用户账户的两步验证。

添加内部用户账户

要添加新内部用户账户到 Kaspersky Security Center：

1. 在控制台树中，打开“**用户账户**”文件夹。
   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 在工作区，单击“**添加用户**”按钮。
3. 在打开的“**新用户**”窗口，指定新用户账户设置：
   - 用户名 (👨‍💼)

     编辑用户名时要小心。保存更改后，您将不能更改它。

   - **描述**
   - **完整名称**
   - **主电子邮件**
   - **主电话**
   - 连接到 Kaspersky Security Center 的用户的**密码**
     密码必须符合以下规则：
     - 密码的字符长度必须是 8 到 256 位。
     - 密码必须包含以下组中三组的字符：
       - 大写字母 (A-Z)
       - 小写字母 (a-z)
       - 数字 (0-9)
       - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

     要查看输入的密码，单击并按住“**显示**”按钮。

     输入密码的尝试次数有限。默认下，允许的最大密码输入尝试次数是 10。您可以管理允许的密码输入尝试次数，描述在“更改允许的密码输入尝试次数”。

如果用户输入无效的密码指定次数，用户账户被锁定一小时。在用户账户列表，被阻止账户的用户图标 ( ) 被灰掉（不可用）。您仅可以通过更改密码解除阻止用户账户。

- 如果必要，选择“**禁用账户**”复选框以禁止用户连接到应用程序。您可以禁用账户，例如，如果您要事先创建账户但是稍后激活它。
- 如果要启用其他选项以保护用户账户免遭未经授权的修改，请选中“**当账户设置被修改时请求密码**”复选框。如果启用此选项，则修改用户账户设置需要在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限的用户进行授权。

4. 单击“**确定**”。

新创建的用户账户在“**用户账户**”文件夹的工作区中显示。

编辑内部用户账户

要在 Kaspersky Security Center 中编辑内部用户账户：

1. 在控制台树中，打开“**用户账户**”文件夹。
   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 在工作区，双击您要编辑的内部用户账户。
3. 在打开的**属性：<用户名称>**窗口，更改用户账户设置：
   - **描述**
   - **完整名称**
   - **主电子邮件**
   - **主电话**
   - 连接到 Kaspersky Security Center 的用户的**密码**
     密码必须符合以下规则：
     - 密码的字符长度必须是 8 到 256 位。
     - 密码必须包含以下组中三组的字符：
       - 大写字母 (A-Z)
       - 小写字母 (a-z)
       - 数字 (0-9)
       - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

     要查看输入的密码，单击并按住“**显示**”按钮。

输入密码的尝试次数有限。默认下，允许的最大密码输入尝试次数是 10。您可以管理允许的密码输入尝试次数，描述在“更改允许的密码输入尝试次数”。

如果用户输入无效的密码指定次数，用户账户被锁定一小时。在用户账户列表，被阻止账户的用户图标 ( ) 被灰掉（不可用）。您仅可以通过更改密码解除阻止用户账户。

- 如果必要，选择“**禁用账户**”复选框以禁止用户连接到应用程序。您可以禁用账户，例如，在员工离职后。
- 如果要启用其他选项以保护用户账户免遭未经授权的修改，请选择“**当账户设置被修改时请求密码**”选项。如果启用此选项，则修改用户账户设置需要在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限的用户进行授权。

4. 单击“**确定**”。

被编辑的用户账户在“**用户账户**”文件夹的工作区中显示。

更改允许的密码输入尝试次数

Kaspersky Security Center 用户可以输入无效的密码有限次数。达到限制后，用户账户被锁定一小时。

默认下，允许的最大密码输入尝试次数是 10。您可以更改允许的密码输入尝试次数，描述在该部分。

要更改允许的密码输入尝试次数：

1. 打开安装了管理服务器的设备的注册表（例如，在**开始** → **运行**菜单使用 regedit 命令）。
2. 转至以下键：
   - 对于 32 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 对于 64 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. 如果 SrvSplPpcLogonAttempts 值不存在，创建它。值类型是 DWORD。
   默认下，Kaspersky Security Center 被安装后，该值未被创建。
4. 在 SrvSplPpcLogonAttempts 值中指定所需的尝试次数。
5. 单击“**确定**”保存更改。
6. 重启管理服务器服务。

允许的最大密码输入尝试次数被更改。

配置内部用户名称的唯一性检查

您可以配置对 Kaspersky Security Center 内部用户的唯一性检查。内部用户名称唯一性检查仅可以在要创建该用户账户的虚拟管理服务器或主管理服务器上运行，或者在所有虚拟管理服务器和主管理服务器上运行。默认情况下，内部用户名称唯一性在所有虚拟管理服务器和主管理服务器上检查。

要在虚拟管理服务器或主管理服务器上启用内部用户名称唯一性检查：

1. 打开安装了管理服务器的设备的注册表（例如，在**开始 → 运行**菜单使用 regedit 命令）。
2. 转至以下分支：
   - 对于 32 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 对于 64 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. 对于 LP_InterUserUniqVsScope （DWORD） 键，设置 00000001 值。
   该键指定的默认值是 0。
4. 重启管理服务器服务。

名称唯一性检查在创建内部用户的虚拟管理服务器上运行，或者在创建内部用户的主管理服务器上运行。

要在所有虚拟管理服务器和主管理服务器上启用内部用户名称唯一性检查：

1. 打开安装了管理服务器的设备的注册表（例如，在**开始 → 运行**菜单使用 regedit 命令）。
2. 转至以下分支：
   - 对于 64 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - 对于 32 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. 对于 LP_InterUserUniqVsScope （DWORD） 键，设置 00000000 值。
   该键指定的默认值是 0。
4. 重启管理服务器服务。

内部用户名称唯一性检查将在所有虚拟管理服务器和主管理服务器上运行。

添加安全组

您可以添加安全组（用户组），运行组和安全组对程序不同功能访问权限的复杂配置。可为安全组分配与其各自的目的对应的名称。例如，名字可以对应于用户所在办公室地点或者用户所属公司的组织机构单元名称。

一个用户可以属于多个安全组。一个虚拟管理服务器管理的用户账户可以仅属于该虚拟服务器的安全组并仅具有该虚拟服务器的访问权限。

要添加安全组：

1. 在控制台树中，选择“**用户账户**”文件夹。
   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 单击**添加安全组**按钮。
   添加安全组窗口打开。
3. 在“**添加安全组**”窗口，在“**常规**”区域，指定组名称。
   组名称不能包含多于 255 个字符并且不能包含特殊字符，例如 *, <, >, ?, \, :, |。组名称必须唯一。
   您可以在“**描述**”输入字段中输入组描述。填充“**描述**”字段是可选的。
4. 单击“**确定**”。

您添加的安全组显示在控制台树的“**用户账户**”文件夹。您可以添加用户到新创建的组。

添加用户到组

要添加用户到组：

1. 在控制台树中，选择“**用户账户**”文件夹。
   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 在用户账户和组列表，选择您要添加用户的组。
3. 在组属性窗口，选择“**组用户**”区域并点击“**添加**”按钮。
   带有用户列表的窗口打开。
4. 在列表中，选择您要包含在组中的用户。
5. 单击“**确定**”。

用户被添加到组并显示在用户组列表中。

配置对应用程序功能的访问权限。基于角色的访问控制

Kaspersky Security Center 针对 Kaspersky Security Center 和受管理 Kaspersky 应用程序的功能提供了基于角色的访问手段。

您可以通过以下方式之一为 Kaspersky Security Center 用户配置对应用程序功能的访问权限：

- 通过为每个用户或用户组单独配置权限。
- 通过使用一组预定义的权限创建标准用户角色并根据用户的职责范围将这些角色分配给用户。

用户角色（也称为角色）是预定义的对 Kaspersky Security Center 功能或受管理 Kaspersky 应用程序的访问权限集。角色可以分配给用户或用户组。

应用用户角色旨在简化和缩短配置用户对应用程序功能的访问权限的常规程序。角色内的访问权限根据标准任务和用户的职责范围进行配置。

可为用户角色分配与其各自的目的对应的名称。您可在程序中创建无限数量的角色。

您可以将预定义的用户角色与已经配置的权限集一起使用，或者创建新角色并自行配置所需的权限。

应用程序功能的访问权限

下表显示了 Kaspersky Security Center 的功能，以及用于管理关联任务、报告、设置和执行关联用户操作的访问权限。

要执行表中列出的用户操作，用户必须拥有该操作旁边指定的权限。

读取、**写入**和**执行**权限适用于任何任务、报告或设置。除这些权限外，要针对设备分类管理任务、报告或设置，用户还需要拥有“**为设备分类执行操作**”权限。

> 表中缺少的所有任务、报告、设置和安装包均属于“**常规功能：基本功能**”功能区域。

应用程序功能的访问权限

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：管理组的管理	**写入**	• 将设备添加到管理组：**写入** • 从管理组中删除设备：**写入** • 将管理组添加到另一个管理组：**写入** • 将管理组从另一个管理组中删除：**写入**	无	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：访问对象而不考虑它们的 ACLs	**读取**	获取对所有对象的读取权限：**读取**	无	无	无
常规功能：基本功能	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 虚拟服务器的设备移动规则（创建、修改或删除）：**写入**、**为设备分类执行操作** • 获取移动 (LWNGT) 协议自定义证书：**读取** • 设置移动 (LWNGT) 协议自定义证书：**写入** • 获取 NLA 定义的网络列表：**读取** • 添加、修改或删除 NLA 定义的网络列表：**写入** • 查看组的访问控制列表：**读取** • 查看卡巴斯基事件日志：**读取** • 查看用于恢复对 BitLocker 加密的硬盘的访问权限的恢复密钥：**执行**	• “将更新下载至管理服务器存储库” • “提交报告” • “分发安装包” • “在从属管理服务器上远程安装应用程序”	• “保护状态报告” • “威胁报告” • “感染最严重的设备报告” • “反病毒数据库状态报告” • “错误报告” • “网络攻击报告” • “已安装的邮件系统保护应用程序汇总报告” • “已安装的周边防护应用程序汇总报告” • “已安装的应用程序类型汇总报告” • “受感染的设备用户报告” • “事故报告” • “事件报告” • “分发点活动报告” • “从属管理服务器报告” • “设备控制事件报告” • “漏洞报告” • “禁止的应用程序报告” • “Web 控制报告” • “受管理设备加密状态报告” • “大容量存储设备加密状态报告” • “文件加密错误报告” • “加密文件访问被阻止报告” • “加密设备访问权限报告” • “有效用户权限报告” • “权限报告”	无
常规功能：已删除对象	• **读取** • **写入**	• 查看回收站中的已删除对象：**读取** • 删除回收站中的对象：**写入**	无	无	无
常规功能：事件处理	• **删除事件** • **编辑事件通知设置** • **编辑事件记录设置** • **写入**	• 更改事件注册设置：**编辑事件记录设置** • 更改事件通知设置：**编辑事件通知设置** • 删除事件：**删除事件**	无	无	设置： • 病毒爆发设置：创建病毒爆发事件所需的病毒检测数量 • 病毒爆发设置：评估病毒检测的时间段 • 数据库中存储的最大事件数量 • 已删除设备中事件的存储时间段
常规功能：在管理服务器上的操作	• **读取** • **写入** • **执行** • **修改对象** ACL • **为设备分类执行操作**	• 指定用于连接网络代理的管理服务器端口：**写入** • 指定在管理服务器上启动的激活代理端口：**写入** • 指定在管理服务器上启动的移动激活代理端口：**写入** • 指定用于分发独立安装包的 Web 服务器端口：**写入** • 指定用于分发 MDM 配置文件的 Web 服务器端口：**写入**	• “备份管理服务器数据” • “数据库维护”	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
		• 指定用于通过 Kaspersky Security Center Web Console 连接的管理服务器 SSL 端口：**写入** • 指定用于移动连接的管理服务器端口：**写入** • 指定管理服务器数据库中存储的最大事件数量：**写入** • 指定管理服务器可以发送的最大事件数量：**写入** • 指定管理服务器可以发送事件的时间段：**写入**			
常规功能：卡巴斯基应用程序部署	• **管理卡巴斯基补丁** • **读取** • **写入** • **执行** • **为设备分类执行操作**	批准或拒绝安装补丁：**管理卡巴斯基补丁**	无	• “虚拟管理服务器授权许可密钥使用报告” • “Kaspersky 软件版本报告” • “不兼容的应用程序报告” • “Kaspersky 软件模块更新版本报告” • “保护部署报告”	安装包：“Kaspersky”
常规功能：授权许可密钥管理	• **导出密钥文件** • **写入**	• 导出密钥文件：**导出密钥文件** • 修改管理服务器授权许可密钥设置：**写入**	无	无	无
常规功能：强制报告管理	• **读取** • **写入**	• 创建报告而不考虑它们的 ACL：**写入** • 执行报告而不考虑它们的 ACL：**读取**	无	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：管理服务器层级	**配置管理服务器层级**	注册、更新或删除从属管理服务器：**配置管理服务器层级**	无	无	无
常规功能：用户权限	**修改对象 ACL**	• 更改任何对象的“安全”属性：**修改对象 ACL** • 管理用户角色：**修改对象 ACL** • 管理内部用户：**修改对象 ACL** • 管理安全组：**修改对象 ACL** • 管理别名：**修改对象 ACL**	无	无	无
常规功能：虚拟管理服务器	• **管理虚拟管理服务器** • **读取** • **写入** • **执行** • **为设备分类执行操作**	• 获取虚拟管理服务器列表：**读取** • 获取关于虚拟管理服务器的信息：**读取** • 创建、更新或删除虚拟管理服务器：**管理虚拟管理服务器** • 将虚拟管理服务器移动到另一个组：**管理虚拟管理服务器** • 设置管理虚拟服务器权限：**管理虚拟管理服务器**	无	“第三方软件更新安装结果报告”	无
常规功能：加密密钥管理	• **读取** • **写入**	• 导出加密密钥：**读取** • 导入加密密钥：**写入**	无	无	无
移动设备管理：常规	• **连接新设备** • **仅发送信息命令到移动设备** • **发送命令到移动设备** • **管理证书** • **读取** • **写入**	• 获取密钥管理服务还原数据：**读取** • 删除用户证书：**管理证书** • 获取用户证书的公开部分：**读取** • 检查是否启用了公钥基础结构：**读取** • 检查公钥基础结构账户：**读取** • 获取公钥基础结构模板：**读取** • 通过扩展密钥用法证书获取公钥基础结构模板：**读取** • 检查公钥基础结构证书是否被吊销：**读取** • 更新用户证书发行设置：**管理证书** • 获取用户证书发行设置：**读取** • 按应用程序名称和版本获取软件包：**读取** • 设置或取消用户证书：**管理证书** • 续订用户证书：**管理证书** • 设置用户证书标签：**管理证书** • 运行 MDM 安装包的生成；取消生成 MDM 安装包：**连接新设备**	无	无	无
系统管理：连接	• **启动 RDP 会话** • **连接到现有 RDP 会话** • **创建通道** • **在管理员工作站上保存设备文件** • **读取** • **写入** • **执行** • **为设备分类执行操作**	• 创建桌面共享会话：**启动 RDP 会话** • 创建 RDP 会话：**连接到现有 RDP 会话** • 创建隧道：**创建通道** • 保存内容网络列表：**在管理员工作站上保存设备文件**	无	“设备用户报告”	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
系统管理：硬件清单	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 获取或导出硬件清单对象：**读取** • 添加、设置或删除硬件清单对象：**写入**	无	• “硬件注册报告” • “配置更改报告” • “硬件报告”	无
系统管理：网络访问控制	• **读取** • **写入**	• 查看 CISCO 设置：**读取** • 更改 CISCO 设置：**写入**	无	无	无
系统管理：操作系统部署	• **部署 PXE 服务器** • **读取** • **写入** • **执行** • **为设备分类执行操作**	• 部署 PXE 服务器：**部署 PXE 服务器** • 查看 PXE 服务器列表：**读取** • 在 PXE 客户端上启动或停止安装过程：**执行** • 管理 WinPE 驱动程序和操作系统映像：**写入**	“基于参考设备操作系统映像创建安装包”	无	安装包：“操作系统映像”
系统管理：漏洞和补丁管理	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 查看第三方补丁属性：**读取** • 更改第三方补丁属性：**写入**	• “执行 Windows Update 同步” • “安装 Windows Update 更新” • “修复漏洞” • “安装所需更新并修复漏洞”	“软件更新报告”	无
系统管理：远程安装	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 查看基于第三方漏洞和补丁管理的安装包属性：**读取** • 更改基于第三方漏洞和补丁管理的安装包属性：**写入**	无	无	安装包： • “自定义应用程序” • “VAPM 包”
系统管理：软件清单	• **读取** • **写入** • **执行** • **为设备分类执行操作**	无	无	• “已安装的应用程序报告” • “应用程序注册历史记录报告” • “已授权应用程序组状态报告” • “第三方软件授权许可密钥报告”	无

预定义用户角色

分配给 Kaspersky Security Center 用户的用户角色为他们提供了对应用程序功能的访问权限集。

在虚拟服务器上创建的用户无法在管理服务器上被分配角色。

您可以将预定义的用户角色与已经配置的权限集一起使用，或者创建新角色。当创建新角色时，您必须自己设置角色范围并分配对 Kaspersky Security Center 功能的访问权限。Kaspersky Security Center 中有些预定义用户角色可以与特定的职位相关联，例如：**审计员**、**安全官**、**主管**（这些角色从版本 11 开始在 Kaspersky Security Center 中出现）。这些角色的访问权限是根据标准任务和相关职位的职责范围预先配置的。下表显示了角色如何与特定职位相关联。

特定职位角色示例

角色	注释
审计员	允许在通过网络代理以本地管理员权限（Linux 为 root）连接到管理服务器的选定设备上执行所有查看操作和执行任何创建的任务。 我们建议谨慎地将该角色指派给有限数量的用户，这些用户需要它们来履行工作职责。

管理者	允许所有查看操作；不允许其他操作。您可以分配该角色到负责您组织的 IT 安全的安全官和其他管理员。
安全官	允许所有查看操作，允许报告管理；在**系统管理**：**连接**区域授予有限的权限。您可以分配该角色到负责您组织的 IT 安全的安全官。

下表显示了分配给每个预定义用户角色的访问权限。

预定义用户角色的访问权限

角色	描述

管理服务器管理员	允许在以下功能区域的所有操作：
	• **常规功能**：
	  • **基本功能**
	  • **事件处理**
	  • **管理服务器层级**
	  • **虚拟管理服务器**
	• **系统管理**：
	  • **连接**
	  • **硬件清单**
	  • **软件清查**
	授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。

管理服务器操作员	授予在以下所有功能区域的**读取**和**执行**权限：
	• **常规功能**：
	  • **基本功能**
	  • **虚拟管理服务器**
	• **系统管理**：
	  • **连接**
	  • **硬件清单**
	  • **软件清查**

审计员	在“**常规功能**”中，允许功能区域内的所有操作： • **访问对象而不考虑它们的 ACL** • **删除对象** • **强制报告管理** 您可以分配该角色到执行您组织的审计的人。

安装管理员	允许在以下功能区域的所有操作：
	• **常规功能**：
	  • **基本功能**
	  • **Kaspersky 软件部署**
	  • **授权许可密钥管理**
	• **系统管理**：
	  • **操作系统部署**
	  • **漏洞和补丁管理**
	  • **远程安装**
	  • **软件清查**
	授予在“**常规功能：虚拟管理服务器**”功能区域的**读取**和**执行**权限。

角色	描述

安装操作员	授予在以下所有功能区域的**读取**和**执行**权限：
	• **常规功能**：
	  • **基本功能**
	  • **Kaspersky 软件部署**（也授予在该区域的**管理 Kaspersky 补丁**权限）
	  • **虚拟管理服务器**
	• **系统管理**：
	  • **操作系统部署**
	  • **漏洞和补丁管理**
	  • **远程安装**
	  • **软件清查**

Kaspersky Endpoint Security 管理员	允许在以下功能区域的所有操作： • **常规功能：基本功能** • Kaspersky Endpoint Security 区域，包括所有功能 授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。
Kaspersky Endpoint Security 操作员	授予在以下所有功能区域的**读取**和**执行**权限： • **常规功能：基本功能** • Kaspersky Endpoint Security 区域，包括所有功能
主管理员	在“**常规功能**”中，*除*以下区域外，允许功能区域内的所有操作： • **访问对象而不考虑它们的** ACL • **强制报告管理** 授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。

主要操作员	授予在以下所有功能区域的**读取**和**执行**（如果适用）权限：
	• **常规功能**：
	  • **基本功能**
	  • **删除对象**
	  • **管理服务器上的操作**
	  • **卡巴斯基应用程序部署**
	  • **虚拟管理服务器**
	• **移动设备管理：常规**
	• **系统管理**，包括所有功能
	• Kaspersky Endpoint Security 区域，包括所有功能

“移动设备管理”管理员	允许在以下功能区域的所有操作： • **常规功能：基本功能** • **移动设备管理：常规**
“移动设备管理”操作员	授予在“**常规功能**：**基本功能**”功能区域中“**读取**”和“**执行**”的权限。 在“**移动设备管理**：**常规**”功能区域中，授予“**读取**”和“**仅发送信息命令到移动设备**”的权限。
安全官	在“**常规功能**”中，允许以下功能区域中的所有操作： • **访问对象而不考虑它们的** ACL • **强制报告管理** 授予在“**系统管理：连接**”功能区域的“**读取**”、“**写入**”、“**执行**”、“**将设备中的文件保存到管理员工作站**”和“**对设备分类执行操作**”权限。 您可以分配该角色到负责您组织的 IT 安全的安全官。
Self Service Portal 用户	允许在“**移动设备管理：Self Service Portal**”功能区域的所有操作。Kaspersky Security Center 11 和更高版本不支持此功能。

角色	描述
管理者	授予在“**常规功能**：**访问对象而不考虑它们的** ACL”和“**常规功能**：**强制报表管理**”功能区域的**读取**权限。 您可以分配该角色到负责您组织的 IT 安全的安全官和其他管理员。
“漏洞和补丁管理”管理员	允许在“**常规功能**：**基本功能**”和“**系统管理**”（包括所有功能）功能区域的所有操作。
“漏洞和补丁管理”操作员	授予在“**常规功能**：**基本功能**”和“**系统管理**”（包括所有功能）功能区域的**读取**和**执行**（如果适用）权限。

添加用户角色

添加用户角色：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口，在“**区域**”窗格选择“**用户角色**”并单击“**添加**”按钮。

   如果启用了“**显示安全设置区域**”选项，则“**用户角色**”区域可用。

4. 在“**新角色**”属性窗口中，配置以下角色：

   - 在“**区域**”，选择“**常规**”并指定角色名称。
     角色名称不能包括 100 个以上字符。
   - 选择“**权限**”区域，通过选择应用程序功能旁边的“**允许**”和“**拒绝**”复选框配置权限集。

   如果您在主管理服务器上操作，则可以启用“**转发角色列表到从属管理服务器**”选项。

5. 单击“**确定**”。

   角色已添加。

已经为管理服务器创建的用户角色显示在管理服务器属性窗口的“**用户角色**”区域。您可以修改或删除用户角色，也可以为安全组指定角色或选定的用户。

为用户或安全组分配角色

将角色分配给用户或用户组：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在“管理服务器属性”窗口中，选择“**安全性**”区域。

   如果选中了界面设置窗口中的“**显示安全设置区域**”复选框，则“**安全性**”区域可用。

4. 在“**组或用户的名称**”字段，选择将要指派角色的一个用户或一组用户。
   如果用户或用户组未包含在该字段中,您可以点击**添加**按钮进行添加。

当点击**添加**按钮添加用户时, 您可以选择用户认证类型 （Microsoft Windows 或 Kaspersky Security Center）。Kaspersky Security Center 认证用于选择处理虚拟管理服务器的内部用户账户。

5. 选择**角色**标签并点击**添加**按钮。

   “**用户角色**”窗口将开启。该窗口显示已经创建的用户角色。

6. 在**用户角色**窗口，为安全组选择一个角色。

7. 单击“**确定**”。

拥有一组处理管理服务器权限的角色将被指派给用户或安全组。已指派的角色显示在管理服务器属性窗口里**安全性**区域的**角色**标签中。

分配权限到用户和组

您可以给予用户和用户组权限以使用管理服务器和您拥有管理插件的 Kaspersky 程序（例如，Kaspersky Endpoint Security for Windows）的不同功能。

将权限分配给用户或用户组：

1. 在控制台树中，做以下之一：

   - 扩展**管理服务器**节点并选择所需管理服务器的子文件夹。
   - 选择管理组。

2. 在管理服务器或管理组的上下文菜单中，选择“**属性**”。

3. 在打开的管理服务器属性窗口（或管理组属性窗口），在左侧“**区域**”窗格选择“**安全性**”。

   如果选中了界面设置窗口中的“**显示安全设置区域**”复选框，则“**安全性**”区域可用。

4. 在“**安全性**”区域的“**组或用户的名称**”列表选择用户或组。

5. 在工作区下方的权限列表中，在“**权限**”选项卡为用户或组配置权限集：

   a. 点击加号（+）以扩展列表中的节点并获取到权限的访问。

   b. 选择您想要的权限旁边的“**允许**”和“**拒绝**”复选框。

   例子 1： 扩展“**访问对象而不考虑它们的** ACLs”节点或“**已删除对象**”节点，并选择“**读取**”。

   例子 2： 扩展“**基本功能**”节点，并选择“**写入**”。

6. 当您已配置了权限集时，单击“**应用**”。

用户或用户组的权限集将被配置。

管理服务器（或管理组）的权限被分成以下部分：

- 常规功能：
  - 管理组的管理
  - 访问对象而不考虑它们的 ACL
  - 基本功能
  - 删除对象
  - 事件处理
  - 管理服务器操作（仅在管理服务器的属性窗口）
  - 部署 Kaspersky 应用程序
  - 授权许可密钥管理
  - 强制报告管理
  - 服务器层级
  - 用户权限
  - 虚拟管理服务器
- 移动设备管理：
  - 常规
- 系统管理：
  - 连接
  - 硬件清查
  - 网络访问控制
  - 部署操作系统
  - 管理漏洞和补丁
  - 远程安装
  - 软件清查

如果没有为权限选择“**允许**”或“**拒绝**”，则该权限被认为是*未定义*的：它将被拒绝，直到被用户明确拒绝或允许为止。

用户权限是以下各项的集合：

- 用户自己的权限
- 分配给该用户的所有角色的权限
- 用户所属的所有安全组的权限
- 分配到用户所属安全组的所有角色的权限

如果至少一个权限集对权限“**拒绝**”，那么用户被拒绝该权限，即便其他集允许它或保持未定义。

传输用户角色到从属管理服务器

默认情况下，主管理服务器和从属管理服务器的用户角色列表是独立的。您可以配置应用程序自动传输在主管理服务器上创建的用户角色到所有从属管理服务器。用户角色也可以从从属管理服务器传输到其自己的从属管理服务器。

要从主管理服务器传输用户角色到从属管理服务器：

1. 打开主应用程序窗口。
2. 执行以下操作之一：
   - 在控制台树，右击管理服务器的名称，并在上下文菜单中选择**属性**。
   - 如果您有活动管理服务器策略，在**策略**文件夹的工作区，右击该策略并在上下文菜单中选择**属性**。
3. 在管理服务器属性窗口或策略设置窗口的“**区域**”窗格，选择“**用户角色**”。

   如果启用了“**显示安全设置区域**”选项，则“**用户角色**”区域可用。

4. 启用“**转发角色列表到从属管理服务器**”选项。
5. 单击“**确定**”。

   应用程序将主管理服务器的用户角色复制到从属管理服务器。

启用“**转发角色列表到从属管理服务器**选项”并传输用户角色后，不能在从属管理服务器上编辑或删除这些用户角色。当您创建新角色或在主管理服务器上编辑现有角色时，更改被自动复制到从属管理服务器。当您在主管理服务器上删除用户角色时，该角色在从属管理服务器上被保留，但无法被编辑或删除。

从主管理服务器传播到从属管理服务器的角色显示有锁图标 (🔒)。您无法在从属管理服务器上编辑这些角色。

如果您在主管理服务器上创建角色，且在从属管理服务器上有相同名称的角色，新角色被复制到从属管理服务器，其名称后被添加索引，例如，~~1、~~2（索引可以随机）。

如果禁用“**转发角色列表到从属管理服务器**”选项，所有用户角色在从属管理服务器上被保留，但是独立于主管理服务器上的角色。独立后，从属管理服务器上的用户角色可以被编辑或删除。

指派用户作为设备所有者

您可以指定用户做为设备所有者来分配设备到用户。如果您必须在设备上运行一些操作（例如，升级硬件），管理员可以通知设备所有者来授权这些操作。

要指定用户做为设备所有者：

1. 在控制台树中，选择“**受管理设备**”文件夹。
2. 在文件夹工作区的“**设备**”选项卡上，选择您要指定拥有者的设备。
3. 在设备的上下文菜单中，选择“**属性**”。
4. 在设备属性窗口中，选择**系统信息** → **会话**。
5. 单击“**设备所有者**”字段旁边的“**分配**”按钮。
6. 在“**用户分类**”窗口，选择您要指定为设备所有者的用户并单击“**确定**”。
7. 单击“**确定**”。

设备所有者被指定。默认情况下，“**设备所有者**”字段用来自活动目录的值填充并在每次活动目录轮询时更新。您可以在**设备所有者报告**中查看设备所有者。您可以使用新报告向导创建报告。

将消息传送给用户

通过电子邮件将消息发送给用户：

1. 在控制台树的“**用户账户**”文件夹中，选择用户。

   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 在用户的上下文菜单中，选择“**通过邮件通知**”。
3. 在“**将消息发送至用户**”窗口中填写相关字段并单击“**确定**”按钮。

   消息将发送至已在用户属性中指定的电子邮件地址。

将 SMS 消息发送给用户：

1. 在控制台树的“**用户账户**”文件夹中，选择用户。
2. 在用户的上下文菜单中，选择**发送 SMS**。
3. 在“**SMS 文本**”窗口中填写相关字段并单击“**确定**”按钮。

   消息将发送至在用户属性中指定号码的移动设备。

查看用户的移动设备列表

查看用户移动设备列表：

1. 在控制台树的“**用户账户**”文件夹中，选择用户。
   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 在用户账户的上下文菜单中，选择“**属性**”。
3. 在用户账户的属性窗口中，选择“**移动设备**”区域。

在“**移动设备**”区域，您可以查看用户移动设备列表及每个设备的相关信息。您可以点击“**导出到文件**”按钮可将移动设备列表保存到文件。

为用户安装证书

您可以为用户安装三种类型证书:

- 共享证书，用于识别用户的移动设备。
- 邮件证书, 用于设置用户移动设备上的企业邮箱。
- VPN 证书，用于设置用户移动设备上的虚拟私有网络。

将证书发布给用户并安装它：

1. 在控制台树中，打开“**用户账户**”文件夹，选择用户账户。
   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 在用户账户的上下文菜单中，选择“**安装证书**”。

   启动证书安装向导。遵照向导的说明操作。

在证书安装向导结束后，证书将被创建并为用户安装。您可以查看已安装用户证书列表并将其导出到文件。

查看发布给用户的证书列表

查看所有发布给用户的证书列表：

1. 在控制台树的“**用户账户**”文件夹中，选择用户。
   “**用户账户**”文件夹默认是“**高级**”文件夹的子文件夹。
2. 在用户账户的上下文菜单中，选择“**属性**”。
3. 在用户账户的属性窗口中，选择“**证书**”区域。

在“**证书**”区域，您可以查看用户证书列表及每个证书的相关信息。您可以点击“**导出到文件**”按钮将证书列表保存到文件。

关于虚拟管理服务器的管理员

通过虚拟管理服务器管理的企业网络的管理员以该窗口中指定的用户账户启动 Kaspersky Security Center Web Console 以查看反病毒保护详情。

如果需要，可以在虚拟服务器上创建多个管理员账户。

在虚拟服务器上创建的用户无法在管理服务器上被分配角色。

虚拟管理服务器的管理员是 Kaspersky Security Center 的一个内部用户。系统不会将内部用户的任何数据传送到操作系统。Kaspersky Security Center 将验证内部用户。

远程安装操作系统和应用程序

Kaspersky Security Center 允许您创建操作系统镜像，以及将其部署在网络客户端设备上，也可以执行远程安装 Kaspersky 或其他供应商的应用程序。

若要创建操作系统镜像，请在管理服务器上安装 Windows ADK 部署工具 和 Windows ADK 的 Windows PE 加载项 工具。您可以创建任何符合 Kaspersky Security Center 的要求的 Windows 操作系统镜像。

Kaspersky Security Center 不支持 64 位版本的 Windows ADK 和 Windows PE。

捕捉操作系统镜像

Kaspersky Security Center 可以从设备上捕捉操作系统镜像并将这些镜像传输至管理服务器。此类操作系统镜像将存储在管理服务器上的专用文件夹内。参考设备的操作系统镜像被捕获并通过安装包创建任务创建。

操作系统镜像捕捉功能拥有以下特点：

- 无法捕捉管理服务器所在设备的操作系统镜像。
- 捕捉操作系统镜像时，名为 sysprep.exe 的实用程序将重置参考设备的设置。如果您要恢复参考设备的设置，在“操作系统镜像创建向导”中选择“**创建设备状态备份副本**”复选框。
- 镜像捕捉进程提供对参考设备重启的功能。

在新设备上部署操作系统镜像

您可以将获得的镜像部署在尚未安装操作系统的新联网设备上。在这种情况下将使用名为 Preboot eXecution Environment （PXE） 的技术。选择将用作 PXE 服务器的联网设备。该设备必须满足以下要求：

- 应该首先在设备上安装网络代理。
- 该设备上无法激活 DHCP 服务器，因为 PXE 服务器使用 DHCP 服务器的端口。
- 包含该设备的网络分段中不可以包含任何其他 PXE 服务器。

要部署操作系统，必须满足以下条件：

- 设备上必须安装网卡。
- 设备必须连接到网络。
- 引导设备时，必须在 BIOS 中选择“网络引导”选项。

系统将执行以下操作系统部署操作：

1. 客户端设备在启动过程中与 PXE 服务器建立连接。
2. 客户端设备在 Windows Preinstallation Environment （WinPE）内启动。

   将设备添加到 WinPE 中可能需要为 WinPE 配置驱动程序集。

3. 客户端设备将在管理服务器上注册。
4. 管理员可以为客户端设备分配带有操作系统镜像的安装包。

   管理员可以添加所需驱动器到带有操作系统镜像的安装包。管理员也可以指定带有操作系统设置的配置文件以在安装过程中应用。

5. 操作系统将部署在客户端设备上。

管理员可以手动指定尚未连接的客户端设备的 MAC 地址，为它们分配带有操作系统镜像的安装包。选定客户端设备连接至 PXE 服务器时，操作系统将自动安装至这些设备中。

将操作系统镜像部署在已经安装了其他操作系统的设备上

将操作系统镜像部署在已经安装其他操作系统的客户端设备上的操作将由特定设备的远程安装任务执行。

请注意，执行的是操作系统的全新安装。所有数据将被删除。

安装 Kaspersky 和其他供应商的应用程序

管理员可以创建任何应用程序的安装包，在安装包中包含用户指定的任何应用程序，然后通过远程安装任务将应用程序安装到客户端设备上。

创建操作系统镜像

操作系统镜像使用删除参考设备的操作系统镜像任务来创建。

若要创建操作系统镜像制作任务，请执行以下操作：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
2. 单击“**创建安装包**”按钮以运行新安装包向导。

3. 在向导的“**选择安装包类型**”窗口中单击“**使用操作系统镜像创建安装包**”按钮。

4. 遵照向导的说明操作。

   当向导结束时，以**基于参考设备 OS 镜像创建安装包**为名称的管理服务器任务被创建。您可以在“**任务**”文件夹中查看该任务。

当“**基于参考设备 OS 镜像创建安装包**”任务完成后，安装包创建完成，您可以使用该安装包通过 PXE 服务器或远程安装任务在客户端设备上部署操作系统。您可以在“**安装包**”文件夹中查看安装包。

安装操作系统镜像

Kaspersky Security Center 允许您部署桌面和基于服务器的 Windows 操作系统 WIM 镜像到组织网络上的设备。

以下方法可以被用于获取可以用 Kaspersky Security Center 工具部署的操作系统镜像：

- 从包含在 Windows 分发包中的 install.wim 文件导入
- 从参考设备捕获镜像

支持操作系统镜像部署的两个方案：

- 在“干净”（没有安装任何操作系统）设备上部署
- 在运行 Windows 的设备上部署

使用 Windows 预安装环境 (Windows PE) 捕获和部署操作系统镜像。所有目标设备正常运行所需的驱动程序都必须被添加 WinPE。一般情况下，必须添加网络适配器和存储控制器驱动程序。

以下需求必须被满足以便实现镜像部署和捕获方案：

- Windows 自动安装工具包 (WAIK) 版本 2.0 或更高版本，或包含 Windows ADK 的 Windows PE 附加组件的 Windows ADK 必须安装在管理服务器上。如果方案允许在 Windows XP 上安装或捕获镜像，AIK 必须被安装。
- DHCP 服务器必须在目标设备所在的网络中可用。
- 管理服务器的共享文件夹必须为目标设备所在的网络以读取方式打开。如果共享文件夹位于管理服务器，KlPxeUser 账户需要访问权限(该账户在运行管理服务器安装程序时被自动创建)。如果共享文件夹位于管理服务器以外，必须授予每个人访问权限。

当选择要安装的操作系统镜像时，管理员必须明确指定目标设备的 CPU 架构：x86 或 x86-64。

配置 KSN 代理服务器地址

默认情况下，管理服务器的连接名称或者 IP 地址与 KSN 代理服务器地址一致。如果您更改管理服务器的连接名称或者 IP 地址，您必须指定正确的 KSN 代理服务器地址以防止主机设备与 KSN 之间的连接丢失。

要配置 KSN 代理服务器地址：

1. 在控制台树中，转到**高级 → 远程安装 → 安装包**。
2. 在“**安装包**”的上下文菜单中，选择“**属性**”。
3. 在打开的窗口中，在“**常规**”选项卡上指定新 KSN 代理服务器地址。
4. 单击“**应用**”按钮。

此后，指定的地址被用作 KSN 代理服务器地址。我们建议您启用**使用 KSN 代理**选项来优化网络流量。

添加 Windows Preinstallation Environment （WinPE） 的驱动程序

要添加 Windows Preinstallation Environment （WinPE） 的驱动程序：

1. 在控制台树的“**远程安装**”文件夹中，选择“**部署设备镜像**”子文件夹。
2. 在**部署设备镜像**文件夹的工作区中，单击**附加操作**按钮并在下拉列表中选择**配置 Windows 预安装环境 (WinPE)的驱动集**。

   Windows 预安装环境驱动窗口打开。
3. 在“**Windows 预安装环境驱动**”窗口中，单击“**添加**”按钮。

   “**选择驱动程序**”窗口将打开。
4. 在“**选择驱动程序**”窗口，从列表选择驱动程序。

   如果列表中缺少必要的驱动程序，请单击“**添加**”按钮并在打开的“**添加驱动程序**”窗口中指定驱动程序名称和驱动程序分发包文件夹。

   您可以单击“**浏览**”按钮来选择文件夹。

   在“**添加驱动程序**”窗口，单击“**确定**”。
5. 在“**选择驱动程序**”窗口，单击“**确定**”。

   驱动程序将被添加至管理服务器存储库。添加到存储库时，驱动程序将显示在“**选择驱动程序**”窗口中。
6. 在“**Windows 预安装环境驱动**”窗口中，单击“**确定**”按钮。

驱动程序将被添加至 Windows Preinstallation Environment （WinPE）。

将驱动程序添加至带有操作系统镜像的安装包

若要将驱动程序添加至带有操作系统镜像的安装包，请执行以下操作：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
2. 从带有操作系统镜像的安装包的上下文菜单中选择“**属性**”。

   “安装包属性”窗口将开启。
3. 在安装包属性窗口中选择“**附加驱动程序**”区域。

4. 单击“**附加驱动程序**”工作区中的“**添加**”按钮。
   “**选择驱动程序**”窗口将打开。

5. 在“**选择驱动程序**”窗口中选择您要添加到带有操作系统镜像的安装包的驱动程序。
   您可以通过在“**选择驱动程序**”窗口中单击“**添加**”按钮将新驱动程序添加至管理服务器存储库。

6. 单击“**确定**”。

已添加的驱动程序将显示在操作系统镜像安装包属性窗口的“**附加驱动程序**”区域中。

配置 sysprep.exe 实用程序

sysrep.exe 实用工具用于为设备创建操作系统镜像。

若要配置 sysprep.exe 实用程序，请执行以下操作：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。

2. 从带有操作系统镜像的安装包的上下文菜单中选择“**属性**”。
   “安装包属性”窗口将开启。

3. 在安装包属性窗口中选择“**sysprep.exe 设置**”区域。

4. 在“**sysprep.exe 设置**”区域，指定要在客户端设备部署操作系统时使用的配置文件：

   - **使用默认配置文件**。选择该项可以使用捕捉操作系统镜像时默认生成的应答文件。
   - **指定主要设置的自定义值**。选择该选项可以通过用户界面指定设置值。
   - **指定配置文件**。选择该项可以使用自定义的应答文件。

5. 若要应用所做更改，请单击“**应用**”按钮。

在新联网的设备上部署操作系统

若要在尚未安装任何操作系统的新设备上部署操作系统，请执行以下操作：

1. 在控制台树的“**远程安装**”文件夹中，选择“**部署设备镜像**”子文件夹。
   确保“**显示漏洞和补丁管理**”窗口中的“配置界面”选项已启用。否则，**远程安装**文件夹不会显示。

2. 单击**附加操作**按钮并在下拉列表中选择**管理网络中 PXE 服务器的列表**。
   这将打开“**属性**”：“**部署设备镜像**”窗口，其中显示“**PXE 服务器**”区域。

3. 在“**PXE 服务器**”区域，单击“**添加**”按钮，并在打开的“**PXE 服务器**”窗口中选择作为 PXE 服务器的设备。
   您添加的设备显示在 PXE 服务器区域。创建的 WinPE 文件将从管理服务器传输到设备。文件传输过程通常需要 10 分钟。传输完成后，显示的**状态**值将从**正在启动**更改为**就绪**。

4. 在“**PXE 服务器**”区域中选择 PXE 服务器，然后单击“**属性**”按钮。

5. 在选定的 PXE 服务器属性中，在“**PXE 服务器连接设置**”选项卡上配置管理服务器和 PXE 服务器之间的连接。

6. 重新启动您要部署操作系统的客户端设备。

7. 在客户端设备的 BIOS 中选择网络启动安装选项。

   客户端设备将连接至 PXE 服务器，然后显示在“**部署设备镜像**”文件夹的工作区中。

8. 在“**操作**”区域中，单击“**分配安装包**”链接，选择用于将操作系统安装至选定设备的安装包。

   在所选设备上使用 DiskPart 工具检查可用磁盘。在 Windows PE 命令提示符下，键入`diskpart`以打开 DiskPart 工具。键入`list disk`以列出磁盘。

   添加设备并分配安装包之后，操作系统部署将自动在该设备上启动。

9. 若要在客户端设备上取消部署操作系统，请单击“**操作**”区域中的“**取消安装 OS 镜像**”链接。

若要按 MAC 地址添加设备：

- 在“**部署设备镜像**”文件夹，单击“**添加设备 MAC 地址**”打开“**新设备**”窗口，并指定您要添加的设备的 MAC 地址。
- 在“**部署设备镜像**”文件夹，单击“**从文件导入设备 MAC 地址**”以选择包含您要部署操作系统镜像的设备的 MAC 地址列表的文件。

在客户端设备上部署操作系统

若要在已经安装了其他操作系统的客户端设备上部署操作系统，请执行以下操作：

1. 在控制台树，打开“**远程安装**”文件夹并点击“**在受管理设备上部署安装包(工作站)**”链接以运行保护部署向导。

2. 在向导的“**选择安装包**”窗口中指定带有操作系统镜像的安装包。

3. 遵照向导的说明操作。

   当向导结束操作时，将创建远程安装任务以安装操作系统到客户端设备。您可以在“**任务**”文件夹中启动或停止任务。

创建程序安装包

要创建应用程序安装包：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。

2. 单击“**创建安装包**”按钮以运行新安装包向导。

3. 在向导的“**选择安装包类型**”窗口中，单击以下按钮之一：

- **为卡巴斯基应用程序创建安装包**如果您希望为 Kaspersky 的程序创建安装包，请选择该选项。
- **为指定的可执行文件创建安装包**。如果您要通过使用可执行文件为第三方应用程序创建安装包，请选择该选项。通常，可执行文件是应用程序的安装文件。
  - **将整个文件夹复制到安装包**

    如果可执行文件伴随应用程序安装所需的附加文件，则选择该选项。在您启用该选项之前，确保所有所需文件都存储在相同文件夹。如果启用该选项，应用程序添加文件夹的全部内容，包括指定的可执行文件，到安装包。

  - **指定安装参数**

    对于成功的远程安装，多数应用程序要求安装在静默模式执行。如果是这种情况，您必须静默安装参数。

    配置安装设置：

    - **可执行文件命令行**

      如果应用程序需要更多参数以进行静默安装，在该字段指定它们。参考供应商文档以获取详情。

      您也可以输入其他参数。

    - **对被 Kaspersky Security Center 识别的应用程序转换设置到推荐值**

      如果指定应用程序的信息被包含在 Kaspersky 数据库，应用程序将以推荐设置安装。

      如果您在“**可执行文件命令行**”字段中输入了参数，则会使用建议的设置来重写它们。

      默认情况下已启用该选项。

      Kaspersky 数据库由 Kaspersky 分析家创建和维护。对于每个添加到数据库的应用程序，Kaspersky 分析家定义最优的安装设置。设置被定义以确保成功将应用程序远程安装到客户端设备。当您运行将更新下载至管理服务器存储库任务时，数据库在管理服务器上被自动更新。

- **从卡巴斯基数据库中选择一个应用程序来创建安装包**。如果您要从 Kaspersky 数据库选择所需第三方应用程序以创建安装包，则选择此选项。当您将更新下载至管理服务器存储库任务时，数据库被自动创建；应用程序被显示在列表。
- **创建带有操作系统镜像的安装包**。如果必须创建带有参考设备操作系统镜像的安装包，请选择该选项。

  当向导结束时，以**基于参考设备 OS 镜像创建安装包**为名称的管理服务器任务被创建。该任务完成后，安装包创建完成，您可以使用该安装包通过 PXE 服务器或远程安装任务部署操作系统。

4. 遵照向导的说明操作。

当向导完成时，安装包被创建，您可以用其安装应用程序到客户端设备。您可以通过选择控制台树中的“**安装包**”来查看安装包。

为应用程序安装包发布证书

要为应用程序安装包发布证书：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
   默认情况下，“ **远程安装**”文件夹是“**高级**”文件夹的子文件夹。
2. 在“**安装包**”文件夹的上下文菜单中，选择“**高级**”。
   这将打开“**安装包**”文件夹的属性窗口。
3. 在“**安装包**”文件夹的属性窗口，选择“**签署独立包**”区域。
4. 在“**签署独立包**”区域，单击“**指定**”按钮。
   “**证书**”窗口。
5. 在“**证书类型**”字段，指定公有或私有证书类型：
   - 如果选择了“**PKCS #12 容器**”值，指定证书文件和密码。
   - 如果选中了“**X.509 证书**”值：
     a. 指定私有密钥文件（带有 *.prk 或 *.pem 扩展名的文件）。
     b. 指定私有密钥密码。
     c. 指定公有密钥文件（带有 *.cer 扩展名）。
6. 单击“**确定**”。

应用程序安装包的证书被发布。

安装应用程序到客户端设备

若要在客户端设备上安装应用程序，请执行以下操作：

1. 在控制台树中，打开“**远程安装**”文件夹，然后单击“**在受管理设备上部署安装包(工作站)**”运行保护部署向导。
2. 在向导的“**选择安装包**”窗口中指定要安装的应用程序安装包。
3. 遵照向导的说明操作。

   当向导结束时，将创建远程安装任务以安装操作系统到客户端设备。您可以在“**任务**”文件夹中启动或停止任务。

使用保护部署向导，您可以将网络代理安装到运行 Windows、Linux 和 macOS 的客户端设备上。

要在运行 Linux 操作系统的设备上使用 Kaspersky Security Center 管理 64 位安全应用程序，您必须使用 64 位 Linux 网络代理。您可以从技术支持网站下载必要的网络代理版本。

在远程安装网络代理到运行 Linux 的设备之前，您必须 准备设备。

管理对象修订

该区域包含了对象修订管理的信息。Kaspersky Security Center 允许您跟踪对象修改。您每次保存更改到对象时，*修订*被创建。每个修订都有一个数字。

支持修订管理的应用程序对象包括：

- 管理服务器属性
- 策略
- 任务
- 管理组
- 用户账户
- 安装包

您可以对对象修订采取以下操作：

- 将所选修订与当前进行比较
- 比较所选的修订
- 将对象与相同类型的其他对象的所选修订进行比较

- 查看所选修订
- 回滚对对象所做的更改到所选的修订
- 保存修订到 .txt 文件

在任何支持修订管理的对象的属性窗口，“**修订历史**”区域显示了包含以下详情的对象修订列表：

- 对象修订版本
- 对象修改的日期和时间
- 修改对象的用户的名称
- 运行在对象上的操作
- 与对象设置更改相关的修订描述

关于对象修订

您可以对对象修订采取以下操作：

- 将所选修订与当前进行比较
- 比较所选的修订
- 将对象与相同类型的其他对象的所选修订进行比较
- 查看所选修订
- 回滚对对象所做的更改到所选的修订
- 保存修订到 .txt 文件

在任何支持修订管理的对象的属性窗口，“**修订历史**”区域显示了包含以下详情的对象修订列表：

- 对象修订版本
- 对象修改的日期和时间
- 修改对象的用户的名称
- 运行在对象上的操作
- 与对象设置更改相关的修订描述

查看修订历史区域

你可以将对象修订与当前进行比较，比较列表中选择的不同修订，或将对象修订与相同类型的其他对象的修订进行比较。

*要查看对象的"**修订历史**"分区：*

1. 在控制台树中，选择以下对象之一：
   - **管理服务器**节点
   - **策略**文件夹
   - **任务**文件夹
   - 管理组文件夹
   - "**用户账户**"文件夹
   - "**已删除对象**"文件夹
   - "**安装包**"子文件夹，嵌套在"**远程安装**"文件夹中
2. 根据相关对象的位置，做以下之一：
   - 如果对象位于**管理服务器**节点或管理组节点，请右击节点，在上下文菜单中选择"**属性**"。
   - 如果对象位于"**策略**"、"**任务**"、"**用户账户**"、"**已删除对象**"或"**安装包**"文件夹，选择该文件夹，在对应的工作区选择该对象。

   "对象属性"窗口打开。
3. 在左侧的"**区域**"窗格，选择"**修订历史**"。

   修订历史显示在工作区。

比较对象修订

您可以将对象过去修订与当前进行比较，比较列表中选择的不同修订，或将对象修订与相同类型的其他对象的修订进行比较。

要比较对象的修订：

1. 选择一个对象并转到对象的属性窗口。
2. 在属性窗口，转到"**修订历史**"区域。
3. 在工作区，在对象修订列表中，选择修订以比较。
   要选择对象的多个修订，使用 **Shift** 和 **Ctrl** 键。
4. 执行以下操作之一：
   - 单击"**比较**"按钮并在下拉列表中选择一个值：
     - **与当前修订比较**

       选择该选项以将所选修订与当前进行比较。

- **比较所选修订**

  选择该选项以比较两个所选修订。

- **与其他任务比较**

  当使用任务修订时，选择**与其他任务比较**选项以将所选修订与其他任务的修订进行比较。
  当使用策略修订时，选择“**与其他策略比较**”以将所选修订与其他策略修订进行比较。

- 双击修订名称，在打开的修订属性窗口中点击以下按钮：

  - **与当前比较**

    点击该按钮以将所选修订与当前进行比较。

  - **与先前比较**

    点击该按钮以将所选修订与先前进行比较。

一个关于修订比较的 HTML 格式的报告显示在您的默认浏览器。

在该报告中，您可以减少修订设置的一些区域。要减少对象修订设置的区域，点击区域名称旁边的箭头图标 ( )。

管理服务器修订包含所有更改的详情，除了以下部分的详情：

- “**流量**”区域
- **标记规则**区域
- **通知**区域
- “**分发点**”区域
- “**病毒爆发**”区域
  当病毒爆发事件被触发时，在“**病毒爆发**”区域不记录策略激活配置信息。

您可以将已删除对象的修订和现有对象的修订进行比较，但是相反：您不能将现有对象的修订和已删除对象的修订进行比较。

为对象修订和已删除对象信息设置存储期限

对象修订的存储期限和已删除对象的存储期限相同。默认存储期限是 90 天。这对程序的常规审计是足够的。
仅带有**修改**权限的用户在**已删除对象**区域可以更改存储期。

要更改对象修订的存储期和已删除对象的存储期：

1. 在控制台树中，选择您要更改其存储期的管理服务器。
2. 右击并在上下文菜单中选择**属性**。
3. 在打开的管理服务器属性窗口，在“**修订历史存储库**”区域，输入所需的存储期限（天数）。
4. 单击“**确定**”。

对象修订和已删除对象信息将被存储您输入的天数。

查看对象修订

如果您需要了解对象在指定时间段内做了哪些修改，您可以查看对象修订。

要查看对象的修订：

1. 转到对象的“**修订历史**”区域。
2. 在对象修订列表中，选择您想要查看设置的修订。
3. 执行以下操作之一：
   - 单击**查看修订**按钮。
   - 双击修订名称，然后单击“**查看修订**”按钮，打开修订属性窗口。

一个 HTML 格式的包含所选对象修订设置的报告被显示。在该报告中，您可以减少对象修订设置的一些区域。要减少对象修订设置的区域，点击区域名称旁边的箭头图标 ( )。

保存对象修订到文件

你可以保存对象修订到文本文件，例如，以便通过邮件发送。

要保存对象修订到文件：

1. 转到对象的“**修订历史**”区域。
2. 在对象修订列表中，选择您想要保存设置的修订。
3. 单击“**高级**”按钮并在下拉列表中选择“**保存到文件**”值。

修订被保存到 .txt 文件。

回滚更改

如果必要，您可以回滚对对象所做的更改。例如，您可能必须转换策略设置到特定日期的状态。

要回滚对对象所做的更改：

1. 转到对象的“**修订历史**”区域。
2. 在对象修订列表中，选择您必须回滚的修订号。
3. 单击“**高级**”按钮并在下拉列表中选择“**回滚**”值。

   该对象被回滚到所选修订。对象修订列表显示所做的操作记录。修订描述显示了您转换对象所到的修订号的信息。

添加修订描述

您可以为修订添加描述以简化在列表中的修订搜索。

要添加修订描述：

1. 转到对象的“**修订历史**”区域。
2. 在对象修订列表中，选择您想要添加描述的修订。
3. 单击“**描述**”按钮。
4. 在“**对象修订描述**”窗口，输入修订描述的文本。
   默认下，对象修订描述为空。
5. 单击“**确定**”。

对象删除

本部分提供有关删除对象的信息。

您可以删除对象，包括以下：

- 策略
- 任务
- 安装包
- 虚拟管理服务器
- 用户
- 安全组
- 管理组

要删除对象：

1. 打开 Kaspersky Security Center Web Console 的所需部分，然后选择对象。
2. 在工具栏上，单击“**删除**”按钮。
3. 在打开的窗口中，单击“**确定**”以确认您的选择。

所选对象被删除。

当您删除对象时，其信息保留在数据库。已删除对象的信息的存储期限与对象修订的存储期限一致（推荐期限是 90 天）。您仅在权限的**已删除对象**区域具有**修改**权限时才能更改存储期限。

关于删除客户端设备

当您从管理组中删除受管理设备时，应用程序会将设备移至未分配的设备组。删除设备后，已安装的卡巴斯基应用程序——网络代理和安全应用程序（例如 Kaspersky Endpoint Security）——将保留在设备上。

Kaspersky Security Center 根据以下规则处理未分配设备组中的设备：

- 如果您配置了设备移动规则，并且设备符合移动规则的条件，则该设备会根据规则被自动移动到管理组。
- 设备会被存储在未分配的设备组中，并根据设备保留规则自动从组中删除。

  设备保留规则不会影响具有一个或多个使用完整磁盘加密进行加密的驱动器的设备。此类设备不会被自动删除——您只能手动删除它们。如果您需要删除带有加密驱动器的设备，请先解密驱动器，然后再删除该设备。

  > 当您删除带有加密驱动器的设备时，解密驱动器所需的数据也会被删除。如果在删除此类设备（从“**未分配的设备**”或“**受管理设备**”组）时打开的确认窗口中选中“**我了解风险并想要删除选定的设备**”复选框，则表示您知晓数据随后会被删除。

  要解密驱动器，必须满足以下条件：

  - 设备被重新连接到管理服务器以恢复解密驱动器所需的数据。
  - 设备用户记住解密密码。
  - 用于加密驱动器的安全应用程序（例如 Kaspersky Endpoint Security for Windows）仍安装在设备上。

  如果驱动器由卡巴斯基磁盘加密技术加密，您还可以尝试使用 FDERT Restore Utility 恢复数据。

> 在 VDI 中，如果您的设备包含加密驱动器，则删除该设备后，加密驱动器上的信息也会被删除。

当您从未分配的设备组中手动删除设备时，应用程序会从列表中删除该设备。删除设备后，已安装的卡巴斯基应用程序（如果有）将保留在设备上。然后，如果该设备对管理服务器仍然可见并且您配置了常规网络轮询，Kaspersky Security Center 会在网络轮询期间发现该设备并将其添加回未分配的设备组。因此，最好仅当设备对管理服务器不可见时再手动删除设备。

删除对象

您可以删除例如策略、任务、安装包、内部用户和内部安全组的对象，如果您具有修改权限（权限的基本功能类别）（请参阅分配权限到用户和组一文以获得更多信息）。

> 您不能删除远程安装任务中使用的安装包。您必须先停止相应的任务。有关管理组中的自动安装任务的更多信息，请参阅在管理组中的设备上自动安装应用程序文章。

要删除对象：

1. 在控制台树，在所需文件夹的工作区选择一个对象。
2. 执行以下操作之一：
   - 右击该对象并选择**删除**。
   - 按 **DELETE** 键。

   对象将被删除，其信息将被存储在数据库。

查看关于已删除对象的信息

已删除对象的信息存储在**已删除对象**文件夹，存储期与对象修订一致（推荐期限是 90 天）。

仅在权限的**已删除对象**区域具有“**读取**”权限的用户可以查看已删除对象列表（参见分配权限到用户和组以获得更多信息）。

要查看已删除对象列表，

在控制台树，选择“**已删除对象**”（默认情况下，“**已删除对象**”是“**高级**”文件夹的子文件夹）。

如果您在权限的“**已删除对象**”区域没有“读取”权限，则会在“**已删除对象**”文件夹中显示一个空列表。

“**已删除对象**”文件夹的工作区包含以下关于已删除对象的信息：

- **名称**。对象名称。
- **类型**。对象类型，例如策略、任务或安装包。
- **时间**。删除对象的时间。
- **用户**。删除对象的账户名称。

要查看关于对象的更多信息：

1. 在控制台树，选择“**已删除对象**”（默认情况下，“**已删除对象**”是“**高级**”文件夹的子文件夹）。
2. 在“**已删除对象**”工作区，选择您需要的对象。
   使用所选对象的区块出现在工作区的右侧。

3. 执行以下操作之一：

- 单击框中的“**属性**”链接。
- 右击您在工作区中选中的对象，并在上下文菜单中选择“**属性**”。

对象的属性窗口打开，显示以下选项卡：

- **常规**
- **修订历史**

从已删除对象列表永久删除对象

仅在权限的**已删除对象**区域具有“**修改**”权限的用户可以从已删除对象列表永久删除对象（参见分配权限到用户和组以获得更多信息）。

要从已删除对象列表删除对象：

1. 在控制台树，选择所需管理服务器的节点并选择“**已删除对象**”文件夹。
2. 在工作区，选择您要删除的对象。
3. 执行以下操作之一：
   - 按 **DELETE** 键。
   - 在您所选对象的上下文菜单中，选择“**删除**”。
4. 在确认对话框，点击**是**。

对象从已删除对象列表中永久删除。该对象的所有信息（包括修订）被从数据库永久删除。您无法恢复该信息。

移动设备管理

通过 Kaspersky Security Center 的移动设备保护的管理通过使用移动设备管理功能运行，这需要专用授权许可。如果您要管理组织员工拥有的移动设备，您必须启用移动设备管理。

该部分提供了启用、配置和禁用移动设备管理的说明。该部分也描述如何管理已连接至管理服务器的移动设备。

有关 Kaspersky Security for Mobile 的详细信息，请参阅 *Kaspersky Security for Mobile 帮助*。

方案：移动设备管理部署

该部分提供在 Kaspersky Security Center 中配置移动设备管理功能的方案。

先决条件

确保您具有允许访问移动设备管理功能的授权许可。

阶段

移动设备管理功能的部署分步骤进行：

1. **准备端口**

   确保端口 13292 在管理服务器上可用。该端口用于连接移动设备。而且，您可能想要使端口 17100 可用。该端口仅用于受管理移动设备的激活代理服务器；如果受管理移动设备拥有互联网连接，您不必使该端口可用。

2. **启用移动设备管理**

   当您现在或后续运行管理服务器快速启动向导时，可以启用移动设备管理。

3. **指定管理服务器外部地址**

   当您运行管理服务器快速启动向导时可以指定外部地址，或稍后。如果您安装时未选择“移动设备管理”且未在安装向导中指定地址，在安装包属性中指定外部地址。

4. **添加移动设备到受管理设备组**

   添加移动设备到受管理设备组，因此您可以通过策略管理这些设备。您可以在管理服务器快速启动向导的某个步骤中创建移动规则。您也可以稍后创建移动规则。如果您不创建此类规则，您可以手动添加移动设备到受管理设备组。

   您可以直接添加移动设备到受管理设备组，或者您可以为其创建子组（或多个子组）。

   此后任何时候，您可以使用新移动设备连接向导连接任意新移动设备到管理服务器。

5. **为移动设备创建策略**

   要管理移动设备，请在这些设备所属的组中为它们创建一个策略（或多个策略）。您可以在此后的任何时候更改该策略的设置。

结果

您完成这些方案后，您可以使用 Kaspersky Security Center 管理 Android 和 iOS 设备。您可以使用移动设备的证书并向移动设备发送命令。

有关管理 iOS MDM 设备的组策略

要管理 iOS MDM 设备，您可以使用包含在 Kaspersky Security Center 分配工具包里的 Kaspersky Device Management for iOS 的管理插件。Kaspersky Device Management for iOS 允许您为指定 iOS MDM 设备的配置设置创建组策略，而不使用 iPhone® 配置实用程序。

管理 iOS MDM 设备的组策略提供管理员以下选项：

- 配置设备密码安全设置。
- 配置对设备硬件特性的使用，以及移动应用程序的安装与卸载的限制。
- 配置预安装移动应用的使用限制，如 YouTube™、iTunes® Store 或 Safari。

- 配置查看，按设备所在区域限制媒体内容（如电影和电视节目）。
- 配置设备通过代理服务器连接互联网的设置（全球 HTTP 代理）。
- 配置用户用以访问企业应用程序和服务的账户（单点登录 (SSO) 技术）。
- 监控移动设备上互联网的使用（访问网站）。
- 配置使用不同身份验证机制和网络协议的无线网络 （Wi-Fi）、接入点 （APNs）、以及虚拟专用网络 （VPN） 的设置。
- 配置与 AirPlay® 设备的连接设置，以传送照片、音乐以及视频流。
- 配置从设备到 AirPrint™ 打印机无线打印文档的连接设置。
- 配置与 Microsoft Exchange 服务器的同步设置，以及在设备上使用企业邮箱的用户账户。
- 配置用户证书同步 LDAP 目录服务。
- 配置用户证书以连接 CalDAV 和 CardDAV 服务，允许用户访问企业日历和联系人列表。
- 在用户设备上配置 iOS 界面的设置，例如字体或者常用网站图标。
- 在设备上添加新的安全证书。
- 配置 Simple Certificate Enrollment Protocol（SCEP） 服务器的设置以自动检索设备认证中心的证书。
- 为使用移动应用添加自定义设置。

管理 iOS MDM 设备的策略特殊在，它指派到的管理组中包含 iOS MDM 服务器（也称“移动设备服务器”）。该策略中指定的所有设置首先应用到移动设备服务器，然后应用到此类服务器所管理的移动设备上。在管理组的层级结构中，从属移动设备服务器从主移动设备服务器接收该策略设置并分发到移动设备。

有关如何使用组策略以在 Kaspersky Security Center 管理控制台中管理 iOS MDM 设备的详细信息，请参见 *Kaspersky Security for Mobile* 文档。

启用移动设备管理

要管理移动设备，您必须启用移动设备管理。如果您未在快速启动向导中启用该功能，您可以稍后启用它。移动设备管理需要授权许可。

> 启用移动设备管理仅在主管理服务器上可用。

要启用移动设备管理：

1. 在控制台树中，选择“**移动设备管理**”文件夹。
2. 在文件夹的工作区，单击“**启用移动设备管理**”按钮。仅当您之前未启用“**移动设备管理**”时，此按钮才可用。
   此时将显示管理服务器快速启动向导的“**附加组件**”页面。
3. 选择“**启用移动设备管理**”以管理移动设备。

4. 在“**选择应用程序激活方法**”页面，使用密钥文件或激活码激活应用程序。

   如果您不激活移动设备管理功能，则移动设备管理将不可用。

5. 如果您要在连接到互联网时使用代理服务器，在“**用于访问互联网的代理服务器设置**”页面上，选择“**使用代理服务器**”复选框。如果选中了此选框，字段可用于输入设置。为代理服务器连接指定设置。

6. 在“**检查插件和安装包的更新**”页面，选择以下选项之一：

   - **检查插件和安装包是否是最新**

     启动更新状态检查。如果检查检测到一些插件或安装包的过期版本，向导会提示您下载最新版本以代替过期版本。

   - **跳过检查**

     继续工作而不检查插件和安装包是否是最新。例如，您可以在没有互联网连接或要继续使用应用程序过期版本时选择该选项。

     条件对检查更新的检查可能导致应用程序功能不正常。

7. 在“**最新插件版本可用**”页面，下载并安装应用程序版本所需插件的语言的最新版本。更新插件不需要授权许可。

   安装插件和安装包后，应用程序将检查是否移动设备正常工作所需的所有插件均已安装。如果检测到一些插件的过期版本，向导会提示您下载最新版本以代替过期版本。

8. 在“**移动设备连接设置**”页面，设置管理服务器端口。

当向导完成时，将发生以下更改：

- Kaspersky Endpoint Security for Android 策略将被创建。
- Kaspersky Device Management for iOS 策略将被创建。
- 端口将在用于移动设备的管理服务器上被打开。

修改移动设备管理设置

要启用移动设备支持：

1. 在控制台树中，选择“**移动设备管理**”文件夹。
2. 在文件夹的工作区，单击“**移动设备连接端口**”链接。

   此时将显示管理服务器属性窗口的“**附加端口**”区域。

3. 在“**附加端口**”区域，修改相关设置：

- **激活代理服务器的 SSL 端口**
- **为移动设备打开端口**

  移动设备连接到授权许可服务器的端口被打开。您可以在以下字段定义端口号和其他设置。
  默认情况下已启用该选项。

- **移动设备同步端口**

  移动设备连接到管理服务器并与其交换数据的端口号。默认端口号是 13292。
  如果端口 13292 被用于其他目的，您可以分配其他端口。

- **移动设备激活端口**

  用于将 Kaspersky Endpoint Security for Android 连接到 Kaspersky 激活服务器的端口。
  默认端口号是 17100。

4. 单击“**确定**”。

禁用移动设备管理

禁用移动设备管理仅在主管理服务器上可用。

要禁用移动设备管理：

1. 在控制台树中，选择“**移动设备管理**”文件夹。
2. 在该文件夹的工作区，单击“**配置附加组件**”链接。
   此时将显示管理服务器快速启动向导的“**附加组件**”页面。
3. 如果您不想再管理移动设备，请选择“**不启用移动设备管理**”。
4. 单击“**确定**”。

先前连接的移动设备将不能连接到管理服务器。移动设备连接端口和移动设备激活端口将被自动关闭。

为 Kaspersky Endpoint Security for Android 和 Kaspersky Device Management for iOS 创建的策略将不被删除。证书发布规则不会被修改。安装的插件将不被删除。移动设备移动规则将不被删除。

您在受管理移动设备上重新启用了移动设备管理后，您可能需要重新安装移动设备管理所需的移动应用。

使用移动设备命令

该区域包含 Kaspersky Security Center 支持的移动设备管理的命令信息。该区域说明了如何发送命令到移动设备，以及如何在命令日志中查看命令的执行状态。

移动设备管理的命令

Kaspersky Security Center 支持移动设备管理命令。

此命令用于远程移动设备管理。例如，一旦您的移动设备丢失，您可以使用一条命令删除设备上的企业数据。

您可以对如下受管理的移动设备类型使用命令：

- iOS MDM 设备
- Kaspersky Endpoint Security (KES) 设备

每个设备类型支持一组专用的命令。

指定命令的特殊考虑

- 对于所有设备类型，如果“**重置为出厂设置**”命令成功执行，所有数据将从设备删除，设备设置将回滚到它们的出厂值。
- 在 iOS MDM 设备上成功执行“**擦除企业数据**”命令后，将从设备中删除所有已安装的配置文件、provisioning 配置文件、iOS MDM 配置文件以及已选中“**连同 iOS MDM 配置文件一起删除**”复选框的应用程序。
- 如果在 KES 设备上成功执行了“**擦除企业数据**”命令，所有企业数据、联系人条目、SMS 历史记录、通话记录、日程表、互联网连接设置以及用户账户（Google™ 账户除外），都将从设备上删除。对于 KES 设备，内存卡中的所有数据也将删除。
- 在发送“**定位**”命令到 KES 设备之前，您将必须确认您已被授权使用该命令搜索丢失的属于您组织或员工的设备。接收**定位**命令的移动设备未被锁定。

移动设备命令列表

下面的表格显示了 iOS MDM 设备的命令集。

移动设备管理的支持命令：iOS MDM 设备

命令	命令执行结果
锁定	移动设备已锁定。
解锁	PIN 码锁定移动设备被禁用。之前指定的 PIN 码已被重置。
重置为出厂设置	所有数据均从移动设备中删除，设置回滚至默认值。
擦除企业数据	所有已安装的配置文件、provisioning 配置文件、iOS MDM 配置文件以及已选中“**连同 iOS MDM 配置文件一起删除**”复选框的应用程序，都会从设备中删除。
同步设备	移动设备数据与管理服务器同步。
安装配置文件	在移动设备上安装配置文件。

命令	命令执行结果
删除配置文件	从移动设备上删除配置文件。
安装 provisioning 配置文件	在移动设备上安装 provisioning 配置文件。
删除 provisioning 配置文件	从移动设备上删除 provisioning 配置文件。
安装应用	应用被安装在移动设备。
卸载应用	应用从移动设备上卸载。
输入兑换码	为已付费应用输入兑换码。
配置漫游	启用或禁用数据漫游和语音漫游。

下面的表格显示了 KES 设备的命令集。

移动设备管理的支持命令：KES 设备

命令	命令执行结果
锁定	移动设备已锁定。
解锁	PIN 码锁定移动设备被禁用。之前指定的 PIN 码已被重置。
重置为出厂设置	所有数据均从移动设备中删除，设置回滚至默认值。
擦除企业数据	企业数据，通讯录条目，SMS 记录，电话记录，日程表，互联网连接设置，以及用户账户（除了 Google 账户），都已从设备上删除。内存卡数据已被擦除。
同步设备	移动设备数据与管理服务器同步。
定位设备	移动设备已定位并显示在 Google Maps™上。移动运营商收取发送 SMS 消息以及提供互联网连接的费用。
面部照片	移动设备已锁定。照片已经由设备的前置摄像头采集并存储在管理服务器上。可以在命令日志中查看照片。移动运营商收取发送 SMS 消息以及提供互联网连接的费用。
警报	移动设备发出警报。

使用 Firebase Cloud Messaging

为了确保及时将命令交付到 Android 操作系统管理的 KES 设备上， Kaspersky Security Center 使用推送通知机制。KES 设备和管理服务器之间通过 Firebase Cloud Messaging（以下简称 FCM）交换推送通知。在 Kaspersky Security Center 管理控制台中，可以指定 Firebase Cloud Messaging 的设置从而将 KES 设备连接到服务。

要检索 Firebase Cloud Messaging 的设置，您必须有 Google 账户。

要启用对 FCM 的使用：

1. 在管理控制台中，选择“**移动设备管理**”节点以及“**移动设备**”文件夹。
2. 在“**移动设备**”文件夹的上下文菜单中，选择**属性**。
3. 在文件夹属性中，选择“**Firebase Cloud Messaging 设置**”区域。
4. 在**Firebase 项目编号**字段中，指定 FCM 发件人 ID。
5. 在**私钥文件 (JSON 格式)**字段中，选择私钥文件。

在下次同步管理服务器时，由 Android 操作系统管理的 KES 设备将被连接到 Firebase Cloud Messaging。

通过单击“**重置设置**”按钮，您可以编辑 Firebase Cloud Messaging 的设置。

发送命令

发送命令至用户的移动设备：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。
2. 选择您需要发送命令的用户移动设备。
3. 在移动设备的上下文菜单中，选择“**显示命令日志**”。
4. 在“**移动设备管理命令**”窗口，转到您需要发送到移动设备的命令名称的区域，然后单击“**发送命令**”按钮。
   根据您选择的命令，单击“**发送命令**”按钮可以打开应用程序的高级设置窗口。例如，当您发送从移动设备删除 provisioning 配置文件的命令时，程序提示您选择必须从移动设备删除的 provisioning 配置文件。在那个窗口定义命令的高级设置并且确认您的选择。在那之后，命令将被发送到移动设备。
   您可以单击“**重新发送**”按钮再次发送命令到用户的移动设备。
   如果尚未执行已发送的命令，则可以单击“**从队列删除**”按钮以取消执行该命令。
   “**命令日志**”区域显示已发送到移动设备的命令与各自的执行状态。单击“**刷新**”以更新命令列表。
5. 单击“**确定**”以关闭“**移动设备管理命令**”窗口。

查看命令日志中的命令状态

程序在命令日志中保存被发送到移动设备的所有命令的相关信息。命令日志包含每条命令发送到移动设备的时间和日期信息，以及他们的相关状态和命令执行结果的详细描述。例如，假如命令执行失败，日志显示错误的原因。命令日志中的记录最多存储30天。

发送到移动设备的命令有以下状态：

- *运行中* – 命令已发送到移动设备。
- *已完成* – 命令执行已成功完成。
- *已完成，但存在错误* – 命令执行失败。
- *正在删除* – 正在从已发送到移动设备的命令队列中删除该命令。
- *已删除* – 已经从发送到移动设备的命令队列中成功删除该命令。
- *删除时出错* – 无法从已发送到移动设备的命令队列中删除该命令。

程序为每个移动设备保留一个命令日志。

查看已经被发送到移动设备的命令日志：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。
2. 在移动设备列表中，选择您想要查看其命令日志的移动设备。

3. 在移动设备的上下文菜单中，选择“**显示命令日志**”。

   移动设备管理命令窗口打开。“**移动设备管理命令**”窗口区域显示可被发送到移动设备的命令。

4. 选择包含必要命令的区域，并在“**命令日志**”区域中查看有关如何发送和执行命令的信息。

在“**命令日志**”区域，您可以查看已发送到移动设备的命令的列表以及这些命令的详细信息。“**显示命令**”过滤器允许您在列表中仅显示具有选定状态的命令。

使用移动设备证书

该章节包含关于如何处理移动设备证书的信息。

移动设备的根证书生成后固定有效期为 700天。备用证书在到期日前 60 天生成。您可以使用以下命令修改生成备用证书的时间段：

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <`以秒为单位的超时`>`

生成备用证书的时间段需要足够长，以便所有受管理的移动设备能够与管理服务器同步并检索证书。

klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

不支持手动续订移动设备的根证书。

启动证书安装向导

您可以安装以下类型的证书用于用户的移动设备:

- 为识别移动设备的共享证书
- 在移动设备上配置企业邮件的邮件证书
- 在移动设备上配置访问虚拟私有网络的 VPN 证书

若要将证书安装在用户的移动设备上，请执行以下操作：

1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**证书**”子文件夹。
2. 在“**证书**”文件夹的工作区中，单击“**添加证书**”链接，运行证书安装向导。

   遵照向导的说明操作。

在向导完成后，将创建一个证书并将其添加到用户的证书列表；此外，将向用户发送通知，为用户提供下载证书并在移动设备上安装的链接。您可以查看所有证书列表并将其导出到文件。您可以删除和重新交付证书，以及查看他们的属性。

步骤 1：选择证书类型

指定必须安装到用户移动设备上的证书类型：

- **移动证书** — 识别移动设备
- **邮件证书** — 在移动设备上配置企业邮件
- **VPN 证书** — 在移动设备上配置访问虚拟私有网络

步骤 2：选择设备类型

仅在您选择“**邮件证书**”或“**VPN 证书**”作为证书类型时，才会显示此窗口。

指定设备上的操作系统类型：

- **iOS MDM 设备**。如果您必须安装证书到使用 iOS MDM 协议连接到 iOS MDM 服务器的移动设备，则选择该选项。
- **由 Kaspersky Security for Mobile 管理的 KES 设备**。如果您必须安装证书到 KES 设备，则选择该选项。此种情况下，证书将用于每次连接管理服务器时的用户识别。
- **未经用户证书身份验证而连接到管理服务器的 KES 设备**。如果您必须安装证书到不使用证书身份验证的 KES 设备，则选择该选项。此种情况下，在向导的最后一步，管理员必须在“**用户通知方法**”窗口中选择每次连接管理服务器使用的用户身份验证类型。

步骤 3：选择用户

在列表中，选择用户、安全组或您要安装证书的Active Directory 安全组。

在“**用户分类**”窗口，您可以搜索 Kaspersky Security Center 内部用户。您可以点击“**添加**”以添加内部用户。

步骤 4：选择证书源

在该窗口，您可以选择管理服务器用于识别移动设备的证书源。您可以使用下列可用方法之一指定一个证书：

- 自动创建证书，通过管理服务器工具，然后发送证书到设备。
- 指定一个先前创建的证书文件。如果在上一步选择了多个用户则该方法不可用。

如果您必须向用户发送为其移动设备创建证书的通知，请选中“**发布证书**”复选框。

如果用户的移动设备先前已使用证书进行了身份验证，因此无需指定账户名和密码即可接收新证书，请清除“**发布证书**”复选框。此种情况下，将不会显示“**用户通知方法**”窗口。

步骤 5：为证书分配标签

如果在“**设备类型**”中选择了“**iOS MDM 设备**”，则会显示“**证书标签**”窗口。

在下拉列表中，您可以分配标签到用户的 iOS MDM 设备证书。带有所分配标签的证书可能具有设置在 Kaspersky Device Management for iOS 策略属性中的特别参数。

下拉列表提示您选择*证书模板 1*、*证书模板 2*或*证书模板 3*标签。您可以在以下区域配置标签：

- 如果已在“**证书类型**”窗口中选择了“**邮件证书**”，则可以在移动设备 Exchange ActiveSync 账户的属性中配置其标签（**受管理设备** → **策略** → Kaspersky Device Management for iOS 策略属性 → **Exchange ActiveSync** 区域 → **添加** → **高级**）。

- 如果在“**证书类型**”窗口中选择了“**VPN 证书**”证书，则可以在移动设备 VPN 的属性中配置其标签（**受管理设备** → **策略** → Kaspersky Device Management for iOS 策略属性 → **VPN** 区域 → **添加** → **高级**）。如果 L2TP、PPTP 或 IPSec (Cisco™) 连接类型被选择您的 VPN，您无法配置用于 VPN 证书的标签。

步骤 6：指定证书发布设置

在该窗口中，您可以指定以下证书发布设置：

- **不通知用户新证书**

  如果您不想发送用户移动设备证书创建通知到用户，请启用该选项。此种情况下，**用户通知方法**窗口将不被显示。

  该选项仅适用于安装了 Kaspersky Endpoint Security for Android 的设备。

  您可能想要启用该选项，例如，用户移动设备已经被使用证书进行了身份验证，因此不必指定账户名称和密码以接收新证书。

- **允许设备拥有单个证书的多个凭证(仅对于安装了 Kaspersky Endpoint Security for Android 的设备)**

  如果您想让 Kaspersky Security Center 在证书即将过期或丢失于目标设备时自动重新发送证书，请启用该选项。

  证书在过期之前几天被自动发送。您可以在证书发布规则窗口设置天数。

  在一些情况下，证书无法在设备上找到。例如，当用户重新安装 Kaspersky 安全应用程序到设备或重置设备设置和数据到出厂设置时可能发生该情况。此种情况下，Kaspersky Security Center 在下一次设备试图连接到管理服务器时检查设备 ID。如果设备具有证书发布时的相同 ID，应用程序重新发布证书到设备。

步骤 7：选择用户通知方法

如果您选择了“**iOS MDM 设备**”作为设备类型，或者选择了“**不通知用户新证书**”选项，则不会显示此窗口。

在“**用户通知方法**”窗口，您可以配置将证书安装到移动设备的用户通知。

在“**身份验证方法**”字段，指定用户身份验证类型：

- **凭证 (域或别名)**

  此种情况下，用户使用域密码或 Kaspersky Security Center 内部用户密码接收新证书。

- **一次性密码**

  此种情况下，用户接收通过电子邮件或 SMS 发送的一次性密码。该密码必须被输入以接收新证书。

  如果您在“**证书发布设置**”窗口启用（选择）了“**允许多设备使用单一证书（仅对于安装了 Kaspersky 移动设备安全应用程序的设备）**”选项，则该选项更改为“**密码**”。

- **密码**

  此种情况下，密码在每次证书被发送到用户时使用。

  如果您在“**证书发布设置**”窗口禁用（清除）了“**允许多设备使用单一证书（仅对于安装了 Kaspersky 移动设备安全应用程序的设备）**”选项，则该选项更改为“**一次性密码**”。

如果您在“**证书类型**”窗口中选择了“**移动证书**”，或者选择了“**未经用户证书身份验证而连接到管理服务器的 KES 设备**”作为设备类型，则会显示此字段。

选择用户通知选项：

- **当向导完成时显示身份验证密码**

  如果您选择该选项，用户名、Security Account Manager（SAM）中的用户名和每个所选用户接收证书的密码将显示在证书安装向导的最后一步。配置关于已安装的证书将不可用的用户通知。

  当您为多个用户添加证书时，您可以通过点击证书安装向导最后一步的**导出**按钮保存提供的证书到文件。

  如果您在证书安装向导的**用户通知方法**步骤选择了“**凭证 (域或别名)**”，则该选项不可用。

- **通知用户新证书**

  如果您选择该选项，您可以配置关于新证书的用户通知。

  - **通过电子邮件**

    在设置的该组，您可以使用电子邮件消息配置安装新证书到他的/她的移动设备的用户通知。该通知方法仅在启用 SMTP 服务器时可用。

    点击**编辑消息**链接查看和编辑通知消息，如果必要。

- **通过 SMS**

  在该设置组，您可以配置关于使用 SMS 安装证书到移动设备的用户通知。该通知方法仅在启用 SMS 通知 时可用。

  点击**编辑消息**链接查看和编辑通知消息，如果必要。

步骤 8：生成证书

在此步骤中，将创建证书。

您可以点击**完成**退出向导。

证书被生成并显示在“**证书**”文件夹工作区的证书列表中。

配置证书发布规则

证书用于在管理服务器上的设备身份验证。所有受管理移动设备必须拥有证书。您可以配置证书如何被发布。

要配置证书发布规则：

1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**证书**”子文件夹。
2. 在**证书**文件夹的工作区中，单击“**配置证书发布规则**”按钮以打开“**证书发布规则**”窗口。
3. 转到证书类型名称的区域：

   移动证书发布—配置移动设备证书的发布。

   邮件证书发布—配置邮件证书的发布。

   VPN 证书发布—配置 VPN 证书的发布。
4. 在“**发布设置**”区域，配置证书的发布：
   - 指定证书期限（天）。

     移动设备的证书受根证书的到期日期限制。如果您指定的证书期限长于根证书的到期日期，则证书期限将在生成时自动调整。
   - 选择证书来源（“**管理服务器**”或“**手动指定证书**”）。

     管理服务器被选定作为证书的默认来源。
   - 指定证书模板（**默认模板**、**其他模板**）。

     如果“**与 PKI 整合**”区域启用了与公共密钥基础架构整合，模板的配置可用。
5. 在“**自动更新设置**”区域，配置证书的自动更新：
   - 在“**当证书剩余此天数时续费**”字段，指定必须在证书到期之前多少天将其更新。
   - 要启用证书的自动更新，请选择“**如果可能，自动重新发布证书**”复选框。
6. 在“**密码保护**”区域，在证书加密过程中启用和配置密码的使用。

密码保护仅对移动证书可用。

a. 选中**在证书安装过程中提示密码**。

b. 使用滑块定义加密密码中符号的最大数量。

7. 单击“**确定**”。

与公共密钥基础架构整合

需要将应用程序与公共密钥基础架构 （PKI） 集成才能简化为用户发布域证书。整合后，证书自动发布。

支持的最小 PKI 服务器版本是 Windows Server 2008。

您必须配置用于与 PKI 集成的账户。该账户必须满足以下要求：

- 在安装了管理服务器的设备上是域用户或管理员。
- 在安装了管理服务器的设备上被授予 SeServiceLogonRight 权限。

要创建一个永久的用户配置文件,需要在安装了管理服务器的设备上使用已配置的用户账户登录至少一次。在管理服务器设备上的用户证书存储库中，安装域管理员提供的注册代理证书。

配置与公共密钥基础架构的集成:

1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**证书**”子文件夹。
2. 在工作区中，单击“**与公钥基础架构整合**”按钮打开“**证书发布规则**”窗口的“**与 PKI 整合**”区域。
   此时将打开“**证书发布规则**”窗口的“**与 PKI 整合**”区域。
3. 选中**整合 PKI 证书的发行**复选框。
4. 在“**账户**”字段中，指定用来与公钥基础设施集成的用户账户的名称。
5. 在“**密码**”字段中，输入该账户的域密码。
6. 在“**在 PKI 系统中的证书模板名称**”列表中，选择为域用户发布证书的证书模板。
   在 Kaspersky Security Center 指定用户账户下启动一个专用服务。服务用于发布用户域证书。该服务在单击“**刷新列表**”按钮加载证书模板列表时，或者当证书生成时启动。
7. 单击“**确定**”保存设置。

整合后，证书自动发布。

启用支持 Kerberos Constrained Delegation

应用程序支持 Kerberos Constrained Delegation 的使用。

要启用支持 Kerberos Constrained Delegation：

1. 在控制台树中，打开“**移动设备管理**”文件夹。
2. 在控制台树的**移动设备管理**文件夹，选择**移动设备服务器**子文件夹。
3. 在“**移动设备服务器**”文件夹的工作区中，选择 iOS MDM 服务器。
4. 在 iOS MDM 服务器的上下文菜单中，选择“**属性**”。
5. 在 iOS MDM 服务器的“属性”窗口中，选择“**设置**”区域。
6. 在“**设置**”区域中，选择“**确保和 Kerberos Constrained Delegation 兼容**”复选框。
7. 单击“**确定**”。

添加 iOS 移动设备到受管理设备列表

要添加 iOS 移动设备到受管理设备列表，必须递送并在设备上安装共享证书。共享证书由管理服务器使用以识别移动设备。iOS 移动设备共享证书在 iOS MDM 配置文件中提供。在共享证书递送并安装在移动设备之后，移动设备出现在受管理设备列表。

Kaspersky 不再支持 Kaspersky Safe Browser。

您可以通过“移动设备连接向导”将用户的移动设备添加到受管理设备列表中。

要使用共享证书将 iOS 设备连接到管理服务器，请执行以下操作：

1. 通过以下方式之一启动移动设备连接向导：
   - 使用“**用户账户**”文件夹的上下文菜单：
     1. 在控制台树中，展开**高级**文件夹并选择**用户账户**子文件夹。
     2. 在“**用户账户**”文件夹的工作区中，选择要将其移动设备添加到受管理设备列表中的用户、用户组或活动目录用户组。
     3. 右击并在用户账户的上下文菜单中，选择“**添加移动设备**”。
        启动移动设备连接向导。
   - 在“**移动设备**”文件夹的工作区，单击“**添加移动设备**”按钮：
     1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**移动设备**”子文件夹。
     2. 在“**移动设备**”子文件夹的工作区，单击“**添加移动设备**”按钮。
        启动移动设备连接向导。
2. 在向导的“**操作系统**”页面，选择 **iOS** 作为移动设备操作系统类型。
3. 在“**选择 iOS MDM 服务器**”页面上，选择 iOS MDM 服务器。

4. 在“**选择您要管理其移动设备的用户**”页面，选择要将其移动设备添加到受管理设备列表中的用户、安全组或 Active Directory 安全组。

   如果通过在“**用户账户**”文件夹的上下文菜单中选择“**添加移动设备**”来启动向导，则将跳过此步骤。

   如果要将新用户账户添加到列表中，请单击“**添加**”按钮，然后在打开的窗口中输入用户账户属性。如果要修改或查看用户账户属性，请在列表中选择用户账户，然后单击“**属性**”按钮。

5. 在向导的“**证书源**”页面，请指定创建共享证书以供管理服务器识别移动设备的方法。您可以使用下列可用方法之一指定一个共享证书：

   - **通过管理服务器工具发布证书**

     如果您以前没有创建证书，请选择此选项以通过管理服务器工具创建新证书。

     如果选中该选项，iOS MDM 配置文件将由管理服务器生成的证书自动签名。

     默认情况下已选中该选项。

   - **指定证书文件**

     选择此选项可以指定先前创建的证书文件。

     如果在上一步选择了多个用户则该方法不可用。

6. 在向导的“**用户通知方法**”页面，定义通过 SMS 或电子邮件通知移动设备用户关于证书创建信息的设置：

   - **在向导中显示二维码**

     如果您选择该选项，安装包的链接将显示在移动设备连接向导的最后一步。

     如果为设备连接选择了多个用户则该选项不可用。

   - **发送二维码到用户**

     选择此选项允许您配置连接新移动设备的用户通知。

     您可以选择邮件地址类型，指定附加邮件地址以及编辑消息文本。您还可以选择用户电话类型以发送 SMS 消息，指定额外电话号码以及编辑 SMS 消息文本。

     如果未配置 SMTP 服务器，邮件消息无法发送到用户。如果未配置 SMS 通知，SMS 消息无法发送到用户。

7. 在**结果**页面，点击**完成**关闭向导。

iOS MDM 配置文件被自动发布在 Kaspersky Security Center Web Server。移动设备用户收到一条带有用于从 Web 服务器下载 iOS MDM 配置文件的链接的通知。用户点击链接。此后，移动设备操作系统会提示用户接受 iOS MDM 配置文件安装。用户必须在 iOS MDM 配置文件可以被下载到移动设备之前同意安装 iOS MDM 配置文件。当 iOS MDM 配置文件下载完成，且移动设备与管理服务器同步后，设备就会显示在控制台树“**移动设备管理**”文件夹下的“**移动设备**”子文件夹中。

为让用户使用链接转到 Kaspersky Security Center Web Server，与管理服务器的连接端口 8061 必须在移动设备上可用。

添加 Android 移动设备到受管理设备列表

要将 Android 移动设备添加到受管理设备列表，必须递送 Kaspersky Endpoint Security for Android 和共享证书并将其安装在移动设备上。共享证书由管理服务器使用以识别移动设备。在共享证书递送并安装在移动设备之后，移动设备出现在受管理设备列表。

您可以通过“移动设备连接向导”将用户的移动设备添加到受管理设备列表中。该向导提供了两个选项，用于递送和安装共享证书和 Kaspersky Endpoint Security for Android：

- 通过使用 Google Play 链接
- 通过使用来自 Kaspersky Security Center Web Server 的链接

  存储在管理服务器上用于分发的 Kaspersky Endpoint Security for Android 安装包可供安装

启动移动设备连接向导

要启动“移动设备连接向导”，请执行以下操作之一：

- 使用“**用户账户**”文件夹的上下文菜单：

  1. 在控制台树中，展开**高级**文件夹并选择**用户账户**子文件夹。
  2. 在“**用户账户**”文件夹的工作区中，选择要将其移动设备添加到受管理设备列表中的用户、用户组或活动目录用户组。
  3. 右击并在用户账户的上下文菜单中，选择“**添加移动设备**”。

     启动移动设备连接向导。

- 在“**移动设备**”文件夹的工作区，单击“**添加移动设备**”按钮：

  1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**移动设备**”子文件夹。
  2. 在“**移动设备**”子文件夹的工作区，单击“**添加移动设备**”按钮。

     启动移动设备连接向导。

使用 Google Play 链接添加 Android 移动设备

要使用 Google Play 链接在移动设备上安装 Kaspersky Endpoint Security for Android 和共享证书，请执行以下操作：

1. 启动移动设备连接向导。
2. 在向导的“**操作系统**”页面，选择 **Android** 作为移动设备操作系统类型。
3. 在向导的“**在设备上安装 Kaspersky Endpoint Security for Android 的方法**”页面，选择“**从 Google Play 下载应用**”。

4. 在向导的“**选择您要管理其移动设备的用户**”页面，选择要将其移动设备添加到受管理设备列表中的用户、用户组或活动目录用户组。

   如果通过在“**用户账户**”文件夹的上下文菜单中选择“**添加移动设备**”来启动向导，则将跳过此步骤。

   如果要将新用户账户添加到列表中，请单击“**添加**”按钮，然后在打开的窗口中输入用户账户属性。如果要修改或查看用户账户属性，请在列表中选择用户账户，然后单击“**属性**”按钮。

5. 在向导的“**证书源**”页面，请指定创建共享证书以供管理服务器识别移动设备的方法。您可以使用下列可用方法之一指定一个共享证书：

   - **通过管理服务器工具发布证书**

     如果您以前没有创建证书，请选择此选项以通过管理服务器工具创建新证书。

     如果选择此选项，则使用管理服务器工具自动颁发证书。

     默认情况下已选中该选项。

   - **指定证书文件**

     选择此选项可以指定先前创建的证书文件。

     如果在上一步选择了多个用户则该方法不可用。

6. 在向导的“**用户通知方法**”页面，定义通过 SMS 或电子邮件通知移动设备用户关于证书创建信息的设置：

   - **在向导中显示二维码**

     如果您选择该选项，安装包的链接将显示在移动设备连接向导的最后一步。

     如果为设备连接选择了多个用户则该选项不可用。

   - **发送二维码到用户**

     选择此选项允许您配置连接新移动设备的用户通知。

     您可以选择邮件地址类型，指定附加邮件地址以及编辑消息文本。您还可以选择用户电话类型以发送 SMS 消息，指定额外电话号码以及编辑 SMS 消息文本。

     如果未配置 SMTP 服务器，邮件消息无法发送到用户。如果未配置 SMS 通知，SMS 消息无法发送到用户。

7. 在**结果**页面，点击**完成**关闭向导。

向导完成后，一个链接和二维码将被发送到用户移动设备，从而允许下载 Kaspersky Endpoint Security for Android。用户点击链接或扫描二维码。此后，移动设备操作系统会提示用户接受 Kaspersky Endpoint Security for Android 的安装。Kaspersky Endpoint Security for Android 下载并安装后，移动设备连接到管理服务器并下载共享证书。当证书安装在移动设备后，设备就会显示在控制台树中“**移动设备管理**”文件夹下的“**移动设备**”子文件夹中。

使用来自 Kaspersky Security Center Web Server 的链接添加 Android 移动设备

发布在管理服务器的 Kaspersky Endpoint Security for Android 安装包可供安装。

要使用来自 Web Server 的链接在移动设备上安装 Kaspersky Endpoint Security for Android 和共享证书，请执行以下操作：

1. 启动移动设备连接向导。
2. 在向导的“**操作系统**”页面，选择 **Android** 作为移动设备操作系统类型。
3. 在向导的“**在设备上安装 Kaspersky Endpoint Security for Android 的方法**”页面，选择“**从 Kaspersky Security Center 下载应用安装包**”。

   在下面显示的字段中，选择安装包或通过点击“**新建**”创建新安装包。
4. 在向导的“**选择您要管理其移动设备的用户**”页面，选择要将其移动设备添加到受管理设备列表中的用户、用户组或活动目录用户组。

   如果通过在“**用户账户**”文件夹的上下文菜单中选择“**添加移动设备**”来启动向导，则将跳过此步骤。

   如果要将新用户账户添加到列表中，请单击“**添加**”按钮，然后在打开的窗口中输入用户账户属性。如果要修改或查看用户账户属性，请在列表中选择用户账户，然后单击“**属性**”按钮。
5. 在向导的“**证书源**”页面，请指定创建共享证书以供管理服务器识别移动设备的方法。您可以使用下列可用方法之一指定一个共享证书：

   - **通过管理服务器工具发布证书**

     如果您以前没有创建证书，请选择此选项以通过管理服务器工具创建新证书。

     如果选择此选项，则使用管理服务器工具自动颁发证书。

     默认情况下已选中该选项。

   - **指定证书文件**

     选择此选项可以指定先前创建的证书文件。

     如果在上一步选择了多个用户则该方法不可用。
6. 在向导的“**用户通知方法**”页面，定义通过 SMS 或电子邮件通知移动设备用户关于证书创建信息的设置：

   - **在向导中显示二维码**

     如果您选择该选项，安装包的链接将显示在移动设备连接向导的最后一步。

     如果为设备连接选择了多个用户则该选项不可用。

- **发送二维码到用户**

  选择此选项允许您配置连接新移动设备的用户通知。

  您可以选择邮件地址类型，指定附加邮件地址以及编辑消息文本。您还可以选择用户电话类型以发送 SMS 消息，指定额外电话号码以及编辑 SMS 消息文本。

  如果未配置 SMTP 服务器，邮件消息无法发送到用户。如果未配置 SMS 通知，SMS 消息无法发送到用户。

7. 在**结果**页面，点击**完成**关闭向导。

Kaspersky Endpoint Security for Android 移动应用包被自动发布在 Kaspersky Security Center Web Server。移动应用包包含应用、移动设备连接到管理服务器的设置和证书。移动设备用户将接收包含从 Web 服务器下载包的链接的通知。用户点击链接。此后，设备操作系统会提示用户接受移动应用包的安装。如果用户同意，包将被下载到移动设备。当包下载完成，且移动设备与管理服务器同步后，设备就会显示在控制台树"**移动设备管理**"文件夹下的"**移动设备**"子文件夹中。

管理 iOS MDM 设备

本部分介绍通过 Kaspersky Security Center 管理 iOS MDM 设备的高级功能。本程序支持使用以下功能管理 iOS MDM 设备：

- 以集中模式定义受管理 iOS MDM 设备的设置，并通过配置文件限制设备的功能。您可添加或修改配置文件并将其安装到移动设备上。
- 使用 provisioning 配置文件安装应用到移动设备，跳过 App Store。例如，您可使用 provisioning 配置文件在用户移动设备上安装内部企业应用程序。Provisioning 配置文件包含有关应用程序和移动设备的信息。
- 通过 App Store 在 iOS MDM 设备上安装应用程序。将某个应用安装至 iOS MDM 设备之前，您必须将该应用添加至 iOS MDM 服务器。

每 24 个小时向相连的所有 iOS MDM 设备发送一次推送通知，以便将数据与 iOS MDM 服务器同步。

有关配置文件和 provisioning 配置文件,以及安装在 iOS MDM 设备上的应用程序的信息, 请参阅 设备属性窗口。

通过证书签署 iOS MDM 配置文件

您可以通过证书签署 iOS MDM 配置文件。您可以使用您自己颁发的证书，也可以从受信任的证书颁发机构接收证书。

iOS 设备会针对未签名的配置文件显示免责声明，并提示用户在安装配置文件时信任签名者。

要通过证书签署 iOS MDM 配置文件：

1. 在控制台树的"**移动设备管理**"文件夹中，选择"**移动设备**"子文件夹。
2. 在"**移动设备**"文件夹的上下文菜单中，选择**属性**。
3. 在文件夹的属性窗口，选择"**iOS 设备的连接设置**"区域。
4. 单击"**选择证书文件**"字段下边的"**浏览**"按钮。

   "**证书**"窗口。

5. 在“**证书类型**”字段，指定公有或私有证书类型：

   - 如果选择了“**PKCS #12 容器**”值，指定证书文件和密码。
   - 如果选中了“**X.509 证书**”值：

     a. 指定私有密钥文件（带有 *.prk 或 *.pem 扩展名的文件）。

     b. 指定私有密钥密码。

     c. 指定公有密钥文件（带有 *.cer 扩展名）。

6. 单击“**确定**”。

该 iOS MDM 配置文件即通过证书签署。

添加配置文件

要创建配置文件，可以使用 Apple Configurator 2，该程序可从 Apple Inc. 网站获得。Apple Configurator 2 只能在运行 macOS 的设备上工作；如果您没有此类设备可用，可以在带有管理控制台的设备上使用 iPhone Configuration Utility 来代替。但是，Apple Inc.不再支持 iPhone Configuration Utility。

要使用 iPhone Configuration Utility 创建配置文件并将其添加至 iOS MDM 服务器：

1. 在控制台树中，选择“**移动设备管理**”文件夹。
2. 在“**移动设备管理**”文件夹的工作区，选择“**移动设备服务器**”子文件夹。
3. 在“**移动设备服务器**”文件夹的工作区中，选择 iOS MDM 服务器。
4. 在 iOS MDM 服务器的上下文菜单中，选择“**属性**”。
   移动设备服务器属性窗口将打开。
5. 在 iOS MDM 服务器的属性窗口中，选择**配置文件**区域。
6. 在**配置文件**区域中，单击**创建**按钮。
   “**新配置文件**”窗口将打开。
7. 在“**新配置文件**”窗口，为配置文件指定名称和 ID。
   配置文件的 ID 应为独一无二的：需要用“倒序 DNS”的格式指定值，如，*com.companyname.identifier*。
8. 单击“**确定**”。
   iPhone Configuration Utility 随后将启动（如果已安装）。
9. 在 iPhone 配置实用程序中重配置配置文件。
   关于配置文件的设置的描述和如何配置配置文件的介绍，请参阅 iPhone 配置实用工具随附的文档。

在您使用 iPhone 配置实用工具完成配置之后，新的配置文件将显示在 iOS MDM 服务器属性窗口中的**配置文件**区域中。

您可以点击**修改**按钮修改配置文件。

您可以点击**导入**按钮为程序加载配置文件。

您可以点击**导出**按钮可将配置文件保存到文件。

您创建的配置文件必须安装到 iOS MDM 设备。

将配置文件安装至设备

要将配置文件安装至移动设备：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。
2. 在工作区中，通过协议类型（*iOS MDM*）过滤 iOS MDM 设备。
3. 选择您必须安装配置文件的用户移动设备。
   您可以选择多个移动设备同时安装配置文件。
4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。
5. 在“**移动设备管理命令**”窗口，转到“**安装配置文件**”区域，然后单击“**发送命令**”按钮。
   您也可以在移动设备的上下文菜单中选择“**所有命令**”向移动设备发送命令，然后选择“**安装配置文件**”。
   此时会打开“**选择配置文件**”窗口，显示配置文件列表。从列表中选择您必须在移动设备上安装的配置文件。您可以选择在移动设备上同时安装多个配置文件。要选择配置文件范围，请使用 **Shift** 键。要合并配置文件到一个组，使用 **CTRL** 键。
6. 单击“**确定**”发送命令到移动设备。
   执行该命令后，将在用户的移动设备上安装所选择的配置文件。如果命令成功执行，在命令日志中命令的当前状态显示为*已完成*。
   您可以单击“**重新发送**”按钮再次发送命令到用户的移动设备。
   如果尚未执行已发送的命令，则可以单击“**从队列删除**”按钮以取消执行该命令。
   “**命令日志**”区域显示已发送到移动设备的命令与各自的执行状态。单击“**刷新**”以更新命令列表。
7. 单击“**确定**”以关闭“**移动设备管理命令**”窗口。

您可以查看已安装的配置文件，并在必要时将其删除。

从设备中删除配置文件

若要将配置文件从移动设备中删除，请执行以下操作：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。
2. 在工作区中，点击“**iOS MDM**”链接过滤 iOS MDM 设备。
3. 选择您必须删除配置文件的用户移动设备。
   您可以选择多个移动设备同时删除配置文件。

4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。

5. 在“**移动设备管理命令**”窗口，转到“**删除配置文件**”区域，然后单击“**发送命令**”按钮。

   您也可以从设备的上下文菜单中通过选择“**所有命令**”发送命令到移动设备，然后选择“**删除配置文件**”。

   此时会打开“**删除配置文件**”窗口，显示配置文件列表。

6. 从列表中选择您必须从移动设备删除的配置文件。您可以选择多个配置文件从移动设备中同时删除它们。要选择配置文件范围，请使用 **Shift** 键。要合并配置文件到一个组，使用 **CTRL** 键。

7. 单击“**确定**”发送命令到移动设备。

   成功执行该命令后，将从用户的移动设备中删除所选择的配置文件。如果命令被成功执行，命令的当前状态将被显示为*已完成*。

   您可以单击“**重新发送**”按钮再次发送命令到用户的移动设备。

   如果尚未执行已发送的命令，则可以单击“**从队列删除**”按钮以取消执行该命令。

   “**命令日志**”区域显示已发送到移动设备的命令与各自的执行状态。单击“**刷新**”以更新命令列表。

8. 单击“**确定**”以关闭“**移动设备管理命令**”窗口。

通过发布配置文件链接来添加新设备

在管理控制台，管理员使用证书安装向导来创建新的 iOS MDM 配置文件。该向导执行以下操作：

- iOS MDM 配置文件自动发布在 Web 服务器。
- 用户通过 SMS 或电子邮件发送到 iOS MDM 配置文件的链接。在接收链接时，用户安装 iOS MDM 配置文件到移动设备。
- 移动设备连接到 iOS MDM 服务器。

由于 Apple 引入的更严厉的安全策略，在连接运行 iOS 11 的移动设备到启用了与公共密钥基础架构（PKI）的整合的管理服务器时，您必须设置 TLS 1.1 和 TLS 1.2 协议版本。

通过由管理员安装配置文件来添加新设备

要通过安装 iOS MDM 配置文件到移动设备来连接移动设备到 iOS MDM 服务器，管理员必须执行以下操作：

1. 在管理控制台中，打开证书安装向导。
2. 通过在向导窗口中选择“**向导完成后显示证书**”复选框来创建新的 iOS MDM 配置文件。
3. 保存 iOS MDM 配置文件。
4. 通过 Apple Configurator 实用工具安装 iOS MDM 配置文件到用户移动设备。

移动设备连接到 iOS MDM 服务器。

由于 Apple 引入的更严厉的安全策略，在连接运行 iOS 11 的移动设备到启用了与公共密钥基础架构（PKI）的整合的管理服务器时，您必须设置 TLS 1.1 和 TLS 1.2 协议版本。

添加 provisioning 配置文件

要添加 provisioning 配置文件到 iOS MDM 服务器：

1. 在控制台树中，打开“**移动设备管理**”文件夹。
2. 在控制台树的**移动设备管理**文件夹，选择**移动设备服务器**子文件夹。
3. 在“**移动设备服务器**”文件夹的工作区中，选择 iOS MDM 服务器。
4. 在 iOS MDM 服务器的上下文菜单中，选择“**属性**”。
   移动设备服务器属性窗口将打开。
5. 在“**iOS MDM 服务器**”的属性窗口中，转到“**Provisioning 配置文件**”区域。
6. 在“**Provisioning 配置文件**”区域，单击“**导入**”按钮，然后指定 provisioning 配置文件的路径。

   该配置文件将被添加至 iOS MDM 服务器设置中。

   您可以单击**导出**按钮可将 provisioning 配置文件保存到文件。

您可以在 iOS MDM 设备上安装所导入的 provisioning 配置文件。

将 provisioning 配置文件安装至设备

要将 provisioning 配置文件安装至移动设备：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。
2. 在工作区中，通过协议类型（*iOS MDM*）过滤 iOS MDM 设备。
3. 选择您必须安装 provisioning 配置文件的用户移动设备。
   您可以选择多个移动设备同时安装 provisioning 配置文件。
4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。
5. 在“**移动设备管理命令**”窗口，转到“**安装 provisioning 配置文件**”区域，然后单击“**发送命令**”按钮。
   您也可以从移动设备的上下文菜单中通过选择“**所有命令**”发送命令到移动设备，然后选择“**安装 provisioning 配置文件**”。
   此时会打开“**选择 provisioning 配置文件**”窗口，显示 provisioning 配置文件列表。从列表中选择您需要安装在移动设备上的 provisioning 配置文件。您可以选择多个 provisioning 配置文件在移动设备上同时安装它们。要选择 provisioning 配置文件的范围，使用 **Shift** 键。要合并 provisioning 配置文件到一个组，使用 **Ctrl** 键。

6. 单击“**确定**”发送命令到移动设备。

   执行该命令后，将在用户的移动设备上安装所选择的 provisioning 配置文件。如果命令成功执行，其当前状态在命令日志中显示为“*已完成*”。

   您可以单击“**重新发送**”按钮再次发送命令到用户的移动设备。

   如果尚未执行已发送的命令，则可以单击“**从队列删除**”按钮以取消执行该命令。

   “**命令日志**”区域显示已发送到移动设备的命令与各自的执行状态。单击“**刷新**”以更新命令列表。

7. 单击“**确定**”以关闭“**移动设备管理命令**”窗口。

您可以查看已安装的配置文件，并在必要时将其删除。

从设备中删除 provisioning 配置文件

若要将 provisioning 配置文件从移动设备中删除，请执行以下操作：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。

   该文件夹工作区中将显示一个受管理移动设备的列表。

2. 在工作区中，通过协议类型（*iOS MDM*）过滤 iOS MDM 设备。

3. 选择您需要删除 provisioning 配置文件的用户移动设备。

   您可以选择多个移动设备同时删除 provisioning 配置文件。

4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。

5. 在“**移动设备管理命令**”窗口，转到“**卸载 provisioning 配置文件**”区域，然后单击“**发送命令**”按钮。

   您也可以从上下文菜单中通过选择**所有命令**发送命令到移动设备，然后选择**删除 provisioning 配置文件**。

   此时会打开“**删除 provisioning 配置文件**”窗口，显示配置文件列表。

6. 从列表中选择您需要从移动设备删除的 provisioning 配置文件。您可以从移动设备中选择多个 provisioning 配置文件同时删除它们。要选择 provisioning 配置文件的范围，使用 **Shift** 键。要合并 provisioning 配置文件到一个组，使用 **Ctrl** 键。

7. 单击“**确定**”发送命令到移动设备。

   成功执行该命令后，将从用户的移动设备中删除所选择的 provisioning 配置文件。与已删除 provisioning 配置文件相关的应用程序将不可操作。如果命令被成功执行，命令的当前状态将被显示为*已完成*。

   您可以单击“**重新发送**”按钮再次发送命令到用户的移动设备。

   如果尚未执行已发送的命令，则可以单击“**从队列删除**”按钮以取消执行该命令。

   “**命令日志**”区域显示已发送到移动设备的命令与各自的执行状态。单击“**刷新**”以更新命令列表。

8. 单击“**确定**”以关闭“**移动设备管理命令**”窗口。

添加受管理应用程序

将某个应用安装至 iOS MDM 设备之前，您必须将该应用添加至 iOS MDM 服务器。如果已通过 Kaspersky Security Center 将应用程序安装到设备上，则其被视为受管。可通过 Kaspersky Security Center 远程管理受管理应用程序。

要将受管理应用程序安装至 iOS MDM 服务器，请执行以下操作：

1. 在控制台树中，打开“**移动设备管理**”文件夹。
2. 在控制台树的**移动设备管理**文件夹，选择**移动设备服务器**子文件夹。
3. 在“**移动设备服务器**”文件夹的工作区中，选择 iOS MDM 服务器。
4. 在 iOS MDM 服务器的上下文菜单中，选择“**属性**”。
   这将打开 iOS MDM 服务器的“属性”窗口。
5. 在 iOS MDM 服务器的“属性”窗口中，选择“**受管理应用程序**”区域。
6. 在“**受管理应用程序**”区域中单击“**添加**”按钮。
   添加应用程序窗口打开。
7. 在“**添加应用程序**”窗口中的“**应用名称**”字段中，指定要添加的应用程序的名称。
8. 在“**Apple ID 或声明文件链接**”字段中，指定要添加的应用程序的 Apple ID，或指定可用于下载应用程序的清单文件链接。
9. 如果想要在删除 iOS MDM 配置文件时随其从用户移动设备中删除受管理应用程序，请选中“**连同 iOS MDM 配置文件一起删除**”复选框。
10. 如果想要阻止通过 iTunes 备份应用程序数据，请选中“**阻止数据备份**”复选框。
11. 单击“**确定**”。

已添加的应用程序将显示在 iOS MDM 服务器属性窗口的“**受管理应用程序**”区域中。

在移动设备上安装应用

若要在 iOS MDM 移动设备上安装应用，请执行以下操作：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。
2. 选择您想要安装应用的 iOS MDM 设备。
   您可以选择多个移动设备同时安装应用程序。
3. 在移动设备的上下文菜单中，选择“**显示命令日志**”。
4. 在“**移动设备管理命令**”窗口，转到“**安装应用**”区域，然后单击“**发送命令**”按钮。
   您也可以在移动设备的上下文菜单中选择“**所有命令**”向移动设备发送命令，然后选择“**安装应用**”。
   此时会打开“**选择应用**”窗口，显示配置文件列表。从列表中选择您需要在移动设备上安装的应用程序。您可以选择在移动设备上同时安装多个应用程序。选择应用范围，使用 **Shift** 键。要合并应用到一个组，使用 **Ctrl** 键。
5. 点击**确定**按钮发送命令到移动设备。
   执行该命令后，将在用户的移动设备上安装所选择的应用程序。如果命令成功执行，在命令日志中命令的当前状态显示为*已完成*。

您可以单击“**重新发送**”按钮再次发送命令到用户的移动设备。如果尚未执行已发送的命令，则可以单击“**从队列删除**”按钮以取消执行该命令。

“**命令日志**”区域显示已发送到移动设备的命令与各自的执行状态。单击“**刷新**”以更新命令列表。

6. 单击“**确定**”以关闭“**移动设备管理命令**”窗口。

已安装应用程序的信息显示在iOS MDM 移动设备的属性里。您可以从移动设备卸载应用程序，使用命令行日志或移动设备的上下文菜单。

将应用从设备上卸载

若要从移动设备中卸载应用，请执行以下操作：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。

   该文件夹工作区中将显示一个受管理移动设备的列表。

2. 在工作区中, 通过协议类型（*iOS MDM*）过滤 iOS MDM 设备。

3. 选择您必须卸载应用的用户移动设备。

   您可以选择多个移动设备同时卸载应用。

4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。

5. 在“**移动设备管理命令**”窗口，转到“**卸载应用**”区域并单击“**发送命令**”按钮。

   您也可以在移动设备的上下文菜单中选择“**所有命令**”向移动设备发送命令，然后选择“**卸载应用**”。

   这将打开“**卸载应用**”窗口，显示应用程序的列表。

6. 从列表中选择您需要从移动设备卸载的应用。您可以选择多个应用从设备中同时卸载它们。选择应用范围，使用 **Shift** 键。要合并应用到一个组，使用 **Ctrl** 键。

7. 单击“**确定**”发送命令到移动设备。

   成功执行该命令后，将从用户的移动设备中卸载所选择的应用。如果命令被成功执行，命令的当前状态将被显示为*已完成*。

   您可以单击“**重新发送**”按钮再次发送命令到用户的移动设备。

   如果尚未执行已发送的命令，则可以单击“**从队列删除**”按钮以取消执行该命令。

   “**命令日志**”区域显示已发送到移动设备的命令与各自的执行状态。单击“**刷新**”以更新命令列表。

8. 单击“**确定**”以关闭“**移动设备管理命令**”窗口。

在 iOS MDM 移动设备上配置漫游

要配置漫游：

1. 在控制台树中，打开“**移动设备管理**”文件夹。

2. 在“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。

   该文件夹工作区中将显示一个受管理移动设备的列表。

3. 选择您要配置漫游的用户所拥有的 iOS MDM 设备。
   您可以选择多个移动设备同时配置其漫游。

4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。

5. 在“**移动设备管理命令**”窗口，转到“**配置漫游**”区域并单击“**发送命令**”按钮。
   您也可以通过在设备上下文菜单中选择**所有命令 → 配置漫游**发送命令到移动设备。

6. 在“**漫游设置**”窗口，指定相关设置：

   - **启用数据漫游**

     如果启用此选项，iOS MDM 移动设备上将启用数据漫游。iOS MDM 移动设备的用户在漫游时可以上网冲浪。

     默认情况下已禁用该选项。

将针对所选设备配置漫游。

查看有关 iOS MDM 设备的信息

要查看有关 iOS MDM 设备的信息，请执行以下操作：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。

2. 在工作区中，点击“**iOS MDM**”链接过滤 iOS MDM 设备。

3. 选择您要查看信息的移动设备。

4. 从移动设备的上下文菜单中，选择“**属性**”。
   iOS MDM 设备的“属性”窗口随即打开。

该移动设备的属性窗口中将显示已连接的 iOS MDM 设备的相关信息。

将 iOS MDM 设备断开管理

要从 iOS MDM 服务器断开 iOS MDM 设备:

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。

2. 在工作区中，点击“**iOS MDM**”链接过滤 iOS MDM 设备。

3. 选择您你必须断开的移动设备。

4. 在移动设备的上下文菜单中，选择“**删除**”。

iOS MDM 设备将标记在已移除列表中。移动设备从 iOS MDM 服务器的数据库中删除后，会自动从受管理设备列表中删除。移动设备将在一分钟内从 iOS MDM 服务器数据库删除。

iOS MDM 设备断开管理后，所有已安装的配置文件、iOS MDM 配置文件以及应用程序，因为启用了“**连同 iOS MDM 配置文件一起删除**”选项，都将从移动设备中删除。

发送命令到设备

要将命令发送到 iOS MDM 设备：

1. 在管理控制台中，打开“**移动设备管理**”节点。
2. 选择“**移动设备**”文件夹。
3. 在“**移动设备**”文件夹中，选择要发送命令的移动设备。
4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。
5. 在出现的列表中，选择要发送到移动设备的命令。

检查所发送命令的执行状态

要检查已发送到移动设备的命令的执行状态：

1. 在管理控制台中，打开“**移动设备管理**”节点。
2. 选择“**移动设备**”文件夹。
3. 在“**移动设备**”文件夹，选择要检查所选命令执行状态的移动设备。
4. 在移动设备的上下文菜单中，选择“**显示命令日志**”。

管理 KES 设备

在 Kaspersky Security Center 中，可以通过以下方式管理 KES 移动设备：

- 通过使用命令集中管理 KES 设备。
- 查看 KES 设备参数设置的相关信息。
- 通过使用移动应用包安装应用程序。
- 将 KES 设备断开管理。

创建 KES 设备移动应用程序包

Kaspersky Endpoint Security for Android 授权是为 KES 设备创建移动应用程序安装包所必需的。

要创建移动程序安装包：

1. 在控制台树的“**远程安装**”文件夹中，选择“**安装包**”子文件夹。
   默认情况下，“ **远程安装**”文件夹是“**高级**”文件夹的子文件夹。
2. 单击“**附加操作**”按钮并在下拉列表中选择“**管理移动应用包**”。
3. 在**移动应用包管理**窗口中，单击**新建**按钮。
4. 新安装包向导启动。遵照向导的说明操作。

新创建的移动应用程序安装包显示在“**移动应用包管理**”窗口中。

启用基于证书的 KES 设备身份验证

要启用基于证书的 KES 设备身份验证：

1. 打开安装了管理服务器的客户端设备的注册表（例如，在**开始** → **运行**菜单使用 regedit 命令）。
2. 转至以下分支：
   - 对于 32 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 对于 64 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. 创建名为 LP_MobileMustUseTwoWayAuthOnPort13292 的键。
4. 指定 REG_DWORD 做为键类型。
5. 设置键值为 1。
6. 重启管理服务器服务。

在您运行管理服务器服务后，将建立强制的基于证书的、使用共享证书的 KES 设备身份验证。

> KES 设备到管理服务器的第一次连接不需要证书。

默认情况下，禁用基于证书的 KES 设备身份验证。

查看有关 KES 设备的信息

查看有关 KES 设备的信息：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。
   该文件夹工作区中将显示一个受管理移动设备的列表。
2. 在工作区，通过协议类型（*KES*）过滤 KES 设备。

3. 选择您要查看信息的移动设备。

4. 从移动设备的上下文菜单中，选择“**属性**”。

   打开 KES 设备的属性窗口。

该移动设备的属性窗口中将显示已连接的 KES 设备的相关信息。

将 KES 设备断开管理

要将 KES 设备断开管理，用户必须从移动设备上卸载网络代理。用户删除了网络代理后，移动设备详情就从管理服务器数据库删除，因此管理员可以从受管理的设备列表删除移动设备。

要从受管理设备列表中删除 KES 设备：

1. 在控制台树的“**移动设备管理**”文件夹中，选择“**移动设备**”子文件夹。

   该文件夹工作区中将显示一个受管理移动设备的列表。

2. 在工作区，通过协议类型（*KES*）过滤 KES 设备。

3. 选择您必须断开管理的移动设备。

4. 在移动设备的上下文菜单中，选择“**删除**”。

   移动设备就从受管理设备列表中删除了。

   如果 Kaspersky Endpoint Security for Android 未从移动设备上卸载，移动设备在与管理服务器同步后会再次出现在受管理设备列表中。

数据加密和保护

在笔记本、可移动驱动器或硬盘驱动器丢失或被盗时，或者数据被未经授权的用户和应用程序访问时，数据加密能够降低数据意外泄露的风险。

Kaspersky Endpoint Security for Windows 提供数据加密功能。Kaspersky Endpoint Security for Windows 可以加密存储在设备本地驱动器和可移动驱动器上的文件，也可以加密整个可移动驱动器和硬盘驱动器。

数据加密规则通过 Kaspersky Security Center 中定义的策略进行配置。根据现有规则进行的加密和解密将在应用策略时执行。

加密管理功能的可用性由用户界面设置确定。

管理员可以进行以下操作：

- 在设备的本地驱动器上配置和运行文件加密或解密。
- 在可移动驱动器上配置和执行文件加密。
- 创建应用程序访问加密文件的规则。

- 如果文件加密功能在用户设备上受限，则可以创建访问加密文件的密钥文件并将其传递给用户。
- 配置和执行硬盘驱动器加密。
- 管理用户对加密硬盘驱动器和可移动驱动器的访问（管理身份验证代理账户，创建关于账户名和密码还原请求的信息并传送给用户、创建加密设备访问密钥并传送给用户）。
- 查看加密状态和文件加密报告。

管理员可使用 Kaspersky Endpoint Security for Windows 中集成的工具执行这些操作。有关如何执行操作的详细说明和加密功能的说明，请参阅 Kaspersky Endpoint Security for Windows 在线帮助。

对于运行 macOS 操作系统的设备，Kaspersky Security Center 支持加密管理功能。对于支持加密功能的应用程序版本，加密使用 Kaspersky Endpoint Security for Mac 工具配置。有关如何执行操作的详细说明和加密功能的说明，请参阅 *Kaspersky Endpoint Security for Mac 管理员指南*。

查看已加密设备列表

若要查看存储加密信息的设备的列表，请执行以下操作：

1. 在管理服务器控制台树中，选择“**数据加密和保护**”文件夹。
2. 使用以下方法之一打开加密设备列表：
   - 通过点击“**管理加密驱动器**”区域中的“**转到加密驱动器列表**”链接。
   - 通过在控制台树中选择“**加密驱动器**”文件夹。

该工作区中将显示有关存储加密文件的网络中设备的相关信息和以驱动器级别加密的设备的信息。驱动器上的信息加密后，该设备将自动从列表中移除。

您可以在设备列表中任意栏上以升序或降序进行排序。

用户界面设置确定“**数据加密和保护**”文件夹是否出现在控制台树中。

查看加密事件列表

在设备上运行数据加密或解密任务时，Kaspersky Endpoint Security for Windows 会将以下类型的事件信息发送给 Kaspersky Security Center：

- 无法加密或解密文件，或者由于磁盘空间不足无法创建加密的压缩包。
- 无法加密或解密文件，或者由于授权许可问题无法创建加密的压缩包。
- 无法加密或解密文件，或者由于缺少访问权限无法创建加密的压缩包。
- 应用程序被禁止访问加密文件。
- 未知错误。

要查看在设备上加密数据时发生的事件的列表：

1. 在管理服务器控制台树中，选择“**数据加密和保护**”文件夹。
2. 使用以下方式之一打开在加密期间所发生事件的列表：
   - 通过单击**数据加密错误**部分中的**转到错误列表**链接。
   - 通过在控制台树中选择“**加密驱动器**”文件夹。

该工作区中将显示设备上在数据加密期间所发生的任何问题。

您可以对加密事件列表采取以下操作：

- 按升序或降序对任一列中的数据记录进行排序。
- 执行快速记录搜索（通过与任一列表字段中的子字符串进行文本匹配）。
- 将事件列表导出到文本文件。

用户界面设置确定“**数据加密和保护**”文件夹是否出现在控制台树中。

将加密事件列表导出到文本文件

要将加密事件列表导出到文本文件，请执行以下操作：

1. 创建加密事件列表。
2. 从事件列表的上下文菜单中，选择“**导出列表**”。
   “**导出列表**”窗口将打开。
3. 在“**导出列表**”窗口中，指定包含该事件列表的文本文件的名称，选择用来保存它的文件夹，然后单击“**保存**”按钮。
   加密事件列表将被保存到您已经指定的文件。

创建和查看加密报告

您可以生成以下报告：

- “受管理设备加密状态报告”。此报告提供有关各种受管理设备的数据加密的详细信息。例如，该报告显示应用已配置加密规则的策略的设备数量。此外，您还可以了解需要重启的设备数量。该报告还包含有关每个设备的加密技术和算法的信息。
- 大容量存储设备加密状态报告。此报告包含与受管理设备加密状态报告类似的信息，但它仅提供大容量存储设备和可移动驱动器的数据。
- 加密驱动器访问权限报告。此报告显示哪些用户账户可以访问加密驱动器。

- “文件加密错误报告”。该报告包含在设备上运行数据加密或解密任务时相关的错误信息。
- “加密文件访问被阻止报告”。该报告包含了阻止应用程序访问加密文件的信息。如果未经授权的用户或应用程序试图访问加密文件或驱动器，此报告会很有帮助。

要生成设备加密报告：

1. 在控制台树中，选择“**数据加密和保护**”文件夹。
2. 执行以下操作之一：
   - 要生成有关受管理设备加密状态的报告，请单击“**查看大容量存储设备加密状态报告**”链接。
     如果您未配置该报告，新报告模板向导将启动。遵照向导的说明。
   - 要生成有关大容量存储设备加密状态的报告，请在控制台树中选择“**加密驱动器**”子文件夹，然后单击“**查看大容量存储设备加密状态报告**”按钮。

   报告生成将开始。该报告显示在“**管理服务器**”节点的“**报告**”选项卡。

若要生成有关已加密设备访问权限的报告，请执行以下操作：

1. 在控制台树中，选择“**数据加密和保护**”文件夹。
2. 执行以下操作之一：
   - 单击“**管理加密驱动器**”区域中的“**加密驱动器访问权限报告**”链接以启动新报告模板向导。
   - 选择“**加密驱动器**”子文件夹，然后单击“**加密驱动器访问权限报告**”按钮以启动新报告模板向导。
3. 按照“新报告模板向导”的步骤进行操作。

   报告生成将开始。该报告显示在“**管理服务器**”节点的“**报告**”选项卡。

若要生成加密错误报告，请执行以下操作：

1. 在控制台树中，选择“**数据加密和保护**”文件夹。
2. 执行以下操作之一：
   - 在“**数据加密错误**”区域单击“**查看文件加密错误报告**”链接以启动新报告模板向导。
   - 选择“**加密事件**”子文件夹，然后单击“**文件加密错误报告**”链接以启动新报告模板向导。
3. 按照“新报告模板向导”的步骤进行操作。

   报告生成将开始。该报告显示在“**管理服务器**”节点的“**报告**”选项卡。

要生成受管理设备加密状态的报告：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 单击“**新建报告模板**”按钮以启动新报告模板向导。

4. 按照“新报告模板向导”的说明进行操作。在“**选择报告模板类型**”窗口的“**其他**”区域，选择“**受管理设备加密状态报告**”。

   在新报告模板向导结束后，新的报告模板将显示在管理服务器节点的“**报告**”选项卡。

5. 在相关管理服务器节点的“**报告**”选项卡，选择在先前步骤中创建的报告模板。

   报告生成将开始。该报告显示在“**管理服务器**”节点的“**报告**”选项卡。

您也可以通过查看管理服务器节点的“统计”选项卡上的**统计**获取有关设备和可移动驱动器的加密状态是否符合加密策略的信息。

若要生成加密文件访问被阻止报告，请执行以下操作：

1. 在控制台树中，选择具有所需管理服务器名称的节点。
2. 在该节点的工作区中，选择“**报告**”选项卡。
3. 单击“**新建报告模板**”按钮以启动新报告模板向导。
4. 按照“新报告模板向导”的说明进行操作。在“**选择报告模板类型**”窗口的“**其他**”区域，选择“**加密文件访问被阻止报告**”。

   在新报告模板向导结束后，新的报告模板将显示在“**管理服务器**”节点的“**报告**”选项卡。

5. 在“**管理服务器**”节点的“**报告**”选项卡，选择在先前步骤中创建的报告模板。

   报告生成将开始。该报告显示在“**管理服务器**”节点的“**报告**”选项卡。

在管理服务器之间传输加密密钥

如果在受管理设备上启用数据加密功能，加密密钥存储在管理服务器上。加密密钥用于访问加密数据和管理加密策略。

在以下情况下，必须将加密密钥传输到其他管理服务器：

- 您重新配置受管理设备上的网络代理，以将该设备分配给其他管理服务器。如果此设备包含加密数据，则必须将加密密钥传输到目标管理服务器。否则，数据将无法解密。
- 您对连接到由管理服务器 S1 管理的设备 D1 的可移动驱动器进行加密，然后将该可移动驱动器连接到由管理服务器 S2 管理的设备 D2。要访问该可移动驱动器上的数据，必须将加密密钥从管理服务器 S1 传输到管理服务器 S2。
- 您对由管理服务器 S1 管理的设备 D1 上的文件进行加密，然后在由管理服务器 S2 管理的设备 D2 上尝试访问该文件。要访问该文件，必须将加密密钥从管理服务器 S1 传输到管理服务器 S2。

您可以通过以下方式传输加密密钥：

- 自动传输，通过在必须互相传输加密密钥的两个管理服务器的属性中启用“**使用管理服务器层级获取加密密钥**”选项。如果对其中一个管理服务器禁用此选项，则无法自动传输加密密钥。

  在管理服务器属性中启用“**使用管理服务器层级获取加密密钥**”选项后，管理服务器会将其存储库中存储的所有加密密钥发送到层级中上一级的主管理服务器（如果有）。

当您尝试访问加密数据时，管理服务器首先在其自己的存储库中搜索加密密钥。如果启用了“**使用管理服务器层级获取加密密钥**”选项，并且在存储库中找不到所需的加密密钥，则管理服务器还会向主管理服务器（如果有）发送请求，以提供所需的加密密钥。该请求将发送到所有主管理服务器，直到最高层级的服务器。

使用管理服务器层级获取加密密钥选项当前在 Web Console 界面中不可用。如果您无权访问基于 MMC 的管理控制台，请使用主管理服务器来管理加密设备。

- 通过导出和导入包含加密密钥的文件，手动将密钥从一个管理服务器传递到另一个。

  加密密钥的导出和导入是加密密钥管理功能中包含的操作。要执行这些操作，需要通过以下方式之一为 Kaspersky Security Center 用户配置对功能的访问权限：

  - 向自从属管理服务器导出加密密钥的用户授予对加密密钥管理功能的“**读取**”访问权限。
  - 向对目标管理服务器导入加密密钥的用户授予对加密密钥管理功能的“**写入**”访问权限。

要启用在层级内的管理服务器之间自动传输加密密钥：

1. 在控制台树中，选择要为其启用自动传输加密密钥的管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在属性窗口中，选择“**加密算法**”区域。
4. 启用**使用管理服务器层级获取加密密钥**选项。
5. 单击“**确定**”应用更改。

下次同步（心跳）时，加密密钥将传输到主管理服务器（如果有）。该管理服务器还将根据请求将其存储库中的加密密钥提供给从属管理服务器。

要在管理服务器之间手动传输加密密钥：

1. 在管理服务器的控制台树中，选择要从其传输加密密钥的从属管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在属性窗口中，选择“**加密算法**”区域。
4. 单击“**从管理服务器导出加密密钥**”。

   确保向从服务器导出加密密钥的用户授予对加密密钥管理功能的“**读取**”访问权限。
5. 在“**导出加密密钥**”窗口中：
   - 单击“**浏览**”按钮，然后指定文件保存位置。
   - 指定密码以防止文件被未经授权访问。

     记住密码。丢失的密码无法恢复。如果密码丢失，则必须重复导出程序。因此，请记下密码并使其随时可用。
6. 例如，通过共享文件夹或可移动驱动器将文件传输到另一个管理服务器。

7. 在目标管理服务器上，确保 Kaspersky Security Center 管理控制台正在运行。
8. 在管理服务器的控制台树中，选择要将加密密钥传输到的目标管理服务器。
9. 在管理服务器的上下文菜单中，选择“**属性**”。
10. 在属性窗口中，选择“**加密算法**”区域。
11. 单击**导入加密密钥到管理服务器**。
    确保向对服务器导入加密密钥的用户授予对加密密钥管理功能的“**写入**”访问权限。
12. 在“**导入加密密钥**”窗口中：
    - 单击“**浏览**”按钮，然后选择包含加密密钥的文件。
    - 指定密码。
13. 单击“**确定**”。

加密密钥将传输到目标管理服务器。

数据存储库

本部分介绍管理服务器中存储的、用来跟踪客户端设备的情况并进行服务的数据。

控制台树的“**存储库**”文件夹显示用于跟踪客户端设备状态的数据。

“**存储库**”文件夹包含下列对象：

- 分发到客户端设备的管理服务器下载的更新
- 网络上检测的设备列表
- 客户端设备上检测到的授权许可密钥
- 被安全应用程序置于设备隔离区的文件
- 在客户端设备上置于备份区中的文件
- 被安全应用程序推迟扫描的文件

将存储库对象的列表导出到文本文件中

您可以将存储库对象列表导出为文件。

要将存储库对象的列表导出到文本文件中，请执行以下操作：

1. 在控制台树的“**存储库**”文件夹中，选择相关存储库的子文件夹。
2. 在存储库子文件夹中，从上下文菜单中选择“**导出列表**”。
   系统将打开“**导出列表**”窗口，您可以在该窗口中指定文本文件名称和要保存的文件夹路径。

安装包

Kaspersky Security Center 会将 Kaspersky 和第三方供应商的安装包放置到数据存储库中。

*安装包*是安装应用程序所需的一个文件集合。安装包中含有要安装的应用程序的安装设置和初始配置。

如果您希望将程序安装到客户端设备上，请为此程序创建安装包或者使用现有安装包。已创建的安装包的列表位于控制台树“**远程安装**”文件夹的“**安装包**”子文件夹内。

存储库中文件的主状态

安全应用程序扫描设备上的文件以查找已知病毒和其他可能导致威胁的程序，分配状态到文件并放置一些到存储库。

例如，安全应用程序可以做如下：

- 删除文件之前保存其副本到存储库
- 隔离存储库中的疑似被感染文件

文件的主状态显示在下表。您可以在安全应用程序的 Help 系统中获得更多关于对文件所采取的操作的详情。

存储库中文件的状态

状态名称	状态描述
被感染	文件具有已知病毒代码或 Kaspersky 反病毒数据库发现的其他恶意软件信息部分。
未感染	文件中未检测到已知病毒或其他恶意软件。
警告	文件包含匹配已知危险代码的代码片段。
疑似被感染	文件包含已知病毒的修改代码或 Kaspersky 的未知病毒代码。
由用户放置到文件夹	用户手动放置文件到存储库，因为文件行为提高了威胁可疑度。用户可以使用最新数据库扫描该文件以查找威胁。
误报	Kaspersky 应用程序分配已感染状态到未感染的文件，因为其代码类似病毒代码。使用最新数据库扫描后，文件被识别为未感染。
已清除	文件已成功清除。
已删除	文件在处理过程中被删除。
密码保护	文件无法被处理，因为它由密码保护。

智能培训模式中的规则触发

该部分提供了客户端设备上的 Kaspersky Endpoint Security for Windows 中的自适应异常控制规则执行的检测信息。

规则检测客户端设备上的异常行为并可能阻止它。如果规则工作在智能培训模式，它们检测异常行为并发送每个检测的报告到 Kaspersky Security Center 管理服务器。该信息作为列表存储在**存储库**文件夹的**智能培训状态下的规则触发器**子文件夹中。您可以确认检测为正确或添加它们为排除，因此该行为类型不再被认为是异常。

检测信息存储在管理服务器的事件日志中（与其他事件一起）和自适应异常控制报告中。

关于自适应异常控制、规则以及它们的模式和状态的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

查看使用自适应异常控制规则执行的检测列表

要查看使用自适应异常控制规则执行的检测列表：

1. 在控制台树中，选择您需要的管理服务器节点。
2. 选择"**智能培训状态下的规则触发器**"子文件夹（默认下，这是**高级** → **存储库**的子文件夹）。

   列表显示使用自适应异常控制规则执行的检测的以下信息：

   - **管理组**

     设备所属管理组的名称。

   - **设备名称**

     应用规则的客户端设备名称。

   - **名称**

     应用的规则名称。

   - **状态**

     正在排除—如果管理员处理该条目并添加其到排除规则列表。该状态保持到下一次客户端设备与管理服务器同步时，同步之后，该条目从列表消失。

     正在确认—如果管理员处理该条目并确认。该状态保持到下一次客户端设备与管理服务器同步时，同步之后，该条目从列表消失。

     空—如果管理员不处理该条目。

- **规则被触发的总数**

  一个启发式规则中的检测数量，一个进程和一个客户端设备。该数量由 Kaspersky Endpoint Security 计算。

- **用户名**

  运行进程的生成检测的客户端设备用户名称。

- **源进程路径**

  源进程路径，例如，执行操作的进程路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **源进程哈希**

  源进程文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **源对象路径**

  启动进程的对象路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **源对象哈希**

  源文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标进程路径**

  目标进程的路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标进程哈希**

  目标文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标对象路径**

  目标对象的路径（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **目标对象哈希**

  目标文件的 SHA256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

- **已处理**

  异常被检测的日期

要查看每个信息元素的属性：

1. 在控制台树中，选择您需要的管理服务器节点。
2. 选择“**智能培训状态下的规则触发器**”子文件夹（默认下，这是**高级** → **存储库**的子文件夹）。
3. 在**智能培训状态下的规则触发器**工作区中，选择所需的对象。
4. 执行以下操作之一：
   - 在屏幕右侧的信息框单击“**属性**”链接。
   - 右击并在上下文菜单中选择**属性**。

   对象属性窗口打开，显示关于已选择元素的信息。

您可以确认或添加到排除自适应异常控制规则检测列表的任何元素。

要确认元素，

在检测列表中选择元素并点击“**确认**”按钮。

元素的状态被更改为“**正在确认**”。

您的确认将被统计到规则使用的统计信息（对于更多信息请参阅 Kaspersky Endpoint Security 11 for Windows 帮助）。

要添加元素作为排除，

在检测列表右击一个元素（或几个元素）并在上下文菜单中选择**添加到排除**。

添加排除向导启动。按照向导的说明进行操作。

如果您拒绝或确认检测，它将在下一次客户端设备与管理服务器同步时被从检测列表中排除，且它将不再出现在列表。

从自适应异常控制规则添加排除

添加排除向导允许您从 Kaspersky Endpoint Security 自适应异常控制规则添加排除。

您可以通过以下三个过程之一启动向导。

要通过自适应异常控制节点启动添加排除向导：

1. 在控制台树中，选择所需管理服务器节点。
2. 选择“**智能培训状态下的规则触发器**”（默认下，这是**高级** → **存储库**的子文件夹）。

3. 在工作区，在检测列表中右击一个元素（或几个元素）并选择**添加到排除**。

   您可以一次添加 1000 个排除项。如果您选择更多元素且尝试添加它们到排除，将显示错误消息。

添加排除向导启动。

您可以从控制台树的其他节点启动添加排除向导：

- 使用管理服务器主窗口的“**事件**”选项卡（然后使用“**用户请求**”选项或“**最近事件**”选项）。
- **自适应异常控制规则状态报告**，**检测数量**列。

步骤 1：选择应用程序

如果您仅拥有一个 Kaspersky Endpoint Security for Windows 且没有其他支持自适应异常控制规则的应用程序，该步骤可能被跳过。

添加排除向导显示其管理插件允许您添加排除到这些应用程序的策略的 Kaspersky 应用程序列表。从该列表选择应用程序并点击**下一步**以选择要添加排除的策略。

步骤 2：选择策略

向导显示 Kaspersky Endpoint Security 策略列表（带有策略配置文件）。

选择所有策略和您要添加排除的配置文件并点击**下一步**。

步骤 3：运行策略

策略处理过程中向导显示进度条。您可以通过点击**取消**中断策略的运行。

继承的策略无法被更新。如果您没有权限修改策略，该策略将不被更新。

当所有策略运行后（或者如果您中断了运行），报告出现。它显示哪些策略被成功更新（绿色图标）和哪些策略未被更新（红色图标）。

这是向导的最后一步。点击**完成**关闭向导。

隔离区和备份区

安装在客户端设备上的 Kaspersky 反病毒应用程序可能在设备扫描过程中放置文件到隔离区或备份区。

*隔离区*是一个存放文件的特殊区域，包含了疑似被感染的文件或发现时无法杀毒的文件。

*备份区*设计用于存储在杀毒过程中被删除或被修改的文件的备份副本。

Kaspersky Security Center 会创建一个由设备上的 Kaspersky 应用程序放入隔离区或备份区的文件列表。客户端设备上的网络代理将隔离区和备份区文件的信息传输到管理服务器。您可以使用管理控制台来查看设备存储库中的文件属性，对这些存储库执行恶意软件扫描，并删除其中存储的文件。文件状态图标描述在后缀。

Kaspersky Endpoint Security 支持隔离和备份操作。

Kaspersky Security Center 并不会将文件从存储库复制到管理服务器。所有文件均保存在设备存储库中。您可以仅在带有反病毒应用程序的设备上恢复文件。

启用存储库文件远程管理

默认情况下，您无法管理客户端设备存储库中的文件。

要启用客户端设备上存储库文件的远程管理，请执行以下操作：

1. 在控制台树中，选择您要启用存储库文件远程管理的管理组。
2. 在组工作区中，打开“**策略**”选项卡。
3. 在“**策略**”选项卡中选择将文件放入设备存储库中的安全应用程序策略。
4. 在策略设置窗口的“**到管理服务器的数据传输**”设置组中，选择与您希望为其启动远程管理的存储库相应的选框。

> “**到管理服务器的数据传输**”设置组在策略属性窗口的位置以及选框的名称根据当前使用的安全应用程序而定。

查看存储库中的文件属性

要浏览隔离区或备份区文件属性，请执行以下操作：

1. 在控制台树中，选择“**存储库**”文件夹，“**隔离**”或“**备份**”子文件夹。
2. 在“**隔离**”(“**备份**”)文件夹的工作区中，选择您希望浏览其属性的文件。
3. 从文件的上下文菜单中选择“**属性**”。

从存储库删除文件

要将文件从隔离区或备份区移除，请执行以下操作：

1. 在控制台树的“**存储库**”文件夹中，选择“**隔离**”或“**备份**”子文件夹。
2. 在“**隔离**”（或“**备份**”）文件夹的工作区中，使用 **Shift** 和 **Ctrl** 键选择您希望删除的文件。
3. 以下列方式之一删除文件：
   - 通过从文件的上下文菜单中，选择“**删除**”。
   - 通过在所选文件的信息框中单击“**删除**”（如果要删除一个文件，请单击“**删除**”）链接。

将该文件放入客户端设备存储库的安全应用程序将从存储库中删除该文件。

从存储库恢复文件

若要从隔离区或备份区中恢复文件，请执行以下操作：

1. 在控制台树中，选择“**存储库**”文件夹，“**隔离**”或“**备份**”子文件夹。
2. 在“**隔离**”(“**备份**”)文件夹的工作区中，使用 **Shift** 和 **Ctrl** 键选择您希望还原的文件。
3. 以下列方式之一开始恢复文件：
   - 通过从文件的上下文菜单中，选择“**恢复**”。
   - 通过在所选文件的信息框中，单击**恢复**链接。

将该文件放入客户端设备存储库的安全应用程序将把文件恢复至其原始文件夹中。

将存储库中的文件保存到磁盘

Kaspersky Security Center 允许您将那些由安全应用程序放入客户端设备隔离区或备份区的文件的副本保存至磁盘。这些文件将复制到安装了 Kaspersky Security Center 的设备上的指定文件夹中。

要将隔离区或备份区中的文件的副本保存到硬盘驱动器，请执行以下操作：

1. 在控制台树中，选择“**存储库**”文件夹，“**隔离**”或“**备份**”子文件夹。
2. 在“**隔离**”(“**备份**”)文件夹的工作区中，选择希望将其复制到硬盘驱动器的文件。
3. 以下列方式之一开始复制文件：
   - 通过从文件的上下文菜单中，选择“**保存到磁盘**”。
   - 通过在所选文件的信息框中，单击**保存到磁盘**链接。

将该文件放入客户端设备隔离区的那个安全应用程序将把文件副本保存至指定文件夹。

扫描隔离区中的文件

要扫描隔离区中的文件，请执行以下操作：

1. 在控制台树中，选择“**存储库**”文件夹的“**隔离**”子文件夹。
2. 在“**隔离**”文件夹的工作区中，使用 **Shift** 和 **Ctrl** 键选择您希望扫描的文件。
3. 以下列方式之一开始文件扫描：
   - 通过从文件的上下文菜单中，选择“**扫描**”。
   - 通过在所选文件的信息框中，单击**扫描**链接。

应用程序会为那些将所选文件移动至客户端设备隔离区的安全应用程序启动按需扫描任务。

活动威胁

客户端设备上检测到的有关未处理的文件的信息将存储在“**存储库**”文件夹的“**活动威胁**”子文件夹中。

延迟处理和清除在请求时和指定事件发生时被安全应用程序执行。您可以配置推迟的情况处理。

清除未处理文件

要开始清除未处理文件：

1. 在控制台树的“**存储库**”文件夹，选择“**活动威胁**”子文件夹。
2. 在“**活动威胁**”文件夹的工作区中，选择要清除的文件。
3. 以下列方式之一开始为文件清除：
   - 通过从文件的上下文菜单中，选择“**清除**”。
   - 通过在所选文件的信息框中，单击**清除**链接。

然后程序将执行文件杀毒操作。

如果文件被清除，安装在客户端设备上的安全应用程序将其恢复到原始文件夹。文件的相关记录将会从“**活动威胁**”文件夹的列表中删除。如果文件无法被清除，安全应用程序将其从设备删除。文件的相关记录将会从“**活动威胁**”文件夹的列表中删除。

文件清理和删除功能可能会有所不同，具体取决于安装的安全应用程序、其版本和设置。

将未处理的文件保存至磁盘

Kaspersky Security Center 允许您将客户端设备上发现的未处理的文件的副本保存至磁盘。这指的是由应用程序处理或删除的文件。这些文件将复制到安装了 Kaspersky Security Center 的设备上的指定文件夹中。

如果文件在杀毒期间被删除或修改，并且其副本存储在托管设备上的Kaspersky Endpoint Security for Windows存储中，您可以保存文件副本。

要将未处理的文件的副本保存至磁盘，请执行以下操作：

1. 在控制台树的“**存储库**”文件夹，选择“**活动威胁**”子文件夹。
2. 在“**活动威胁**”文件夹的工作区中，选择要复制到硬盘的文件。
3. 以下列方式之一开始复制文件：
   - 通过从文件的上下文菜单中，选择“**保存到磁盘**”。
   - 通过在所选文件的信息框中，单击**保存到磁盘**链接。

安装在发现未处理文件的客户端设备上的安全应用程序将一份文件副本保存至指定文件夹。

从“活动威胁”文件夹中删除文件

*要从“**活动威胁**”文件夹中删除文件，请执行以下操作：*

1. 在控制台树的“**存储库**”文件夹，选择“**活动威胁**”子文件夹。
2. 在“**活动威胁**”文件夹的工作区中，使用 **Shift** 和 **Ctrl** 键选择您希望删除的文件。
3. 以下列方式之一删除文件：
   - 通过从文件的上下文菜单中，选择“**删除**”。
   - 通过在所选文件的信息框中单击“**删除**”（如果要删除一个文件，请单击“**删除**”）链接。

这样，将该文件放入客户端设备存储库的安全应用程序将从存储库中删除该文件。该等文件的相关记录将会从“**活动威胁**”文件夹的列表中删除。

卡巴斯基安全网络 （KSN）

该部分描述如何使用卡巴斯基安全网络 (KSN) 的在线服务基础架构。该部分提供了关于 KSN 的详细描述，介绍了如何启用 KSN，配置对 KSN 的访问，并查看 KSN 代理服务器的使用统计。

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）以及 KSN 功能。

关于 KSN

卡巴斯基安全网络 (KSN) 是一种在线服务的基础架构，可提供对 Kaspersky 在线知识库的访问，其中包含与文件信誉、网络资源和软件相关的信息。使用卡巴斯基安全网络中的数据可确保在遇到新型威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的效力并降低误报的风险。KSN 允许您使用 Kaspersky 的信誉数据库检索有关安装在受管理设备上的应用程序信息。

Kaspersky Security Center 支持以下基础架构解决方案：

- *KSN* 是一种允许您与 Kaspersky Security Network 交换信息的解决方案。一旦加入 KSN，即表示您同意以自动模式将通过 Kaspersky Security Center 管理的客户端设备上安装的卡巴斯基应用程序的操作相关信息发送到 Kaspersky。依照当前KSN 访问设置发送信息。卡巴斯基分析师还分析收到的信息，并将其包含在卡巴斯基安全网络的信誉数据库和统计数据库中。Kaspersky Security Center 默认使用此解决方案。
- *卡巴斯基私有安全网络 (KPSN)* 是一种解决方案，允许安装了卡巴斯基应用程序的设备用户访问卡巴斯基安全网络的信誉数据库和其他统计数据，而无需从用户自己的设备向全球 KSN 发送数据。KPSN 用于由于以下原因无法参与卡巴斯基安全网络的企业客户：
   - 用户设备未连接到互联网。
   - 法律或企业安全策略禁止传输任何数据到国家/地区以外或企业局域网以外。

   您可以在管理服务器属性窗口的 **KSN 代理设置**区域对卡巴斯基私人安全网络设置访问设置。

在运行快速启动向导时，应用程序会提示您加入 KSN。您可以在使用应用程序的任何时间启用或者停止 KSN。

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您升级管理服务器的版本时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的先前版本继续使用 KSN。

启用 KSN 后，Kaspersky Security Center 会检查 KSN 服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保保持受管理设备的安全级别是必要的。

管理服务器管理的客户端设备通过 KSN 代理服务器与 KSN 交互。KSN 代理服务器提供以下功能：

- 即使无法直接访问互联网，客户端设备也可以向 KSN 发送请求、从 KSN 获取信息以及向 KSN 传送信息。
- KSN 代理可缓存处理后的数据，从而减少发送通道的工作负荷以及为等待客户端设备所请求的信息而花费的时间。

您可以在管理服务器的属性窗口的“**KSN 代理设置**”部分配置 KSN 代理服务器。

设置到卡巴斯基安全网络的访问

您可以在管理服务器和分发点上设置到卡巴斯基安全网络 (KSN) 的访问。

要设置管理服务器到卡巴斯基安全网络 (KSN) 的访问：

1. 在控制台树中，选择要为其设置对 KSN 访问的管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口，在“**区域**”窗格选择**KSN 代理 → KSN 代理设置**。
4. 在工作区中，启用“**使用管理服务器作为代理服务器**”选项以使用 KSN 代理服务。

   数据被从客户端设备发送到 KSN，与在这些客户端设备上活动的 Kaspersky Endpoint Security 策略一致。如果清除此选框，数据不会通过 Kaspersky Security Center 从管理服务器以及客户端设备发送到 KSN。但是，客户端设备能够根据其设置直接将数据发送到 KSN（绕过 Kaspersky Security Center）。在客户端设备上活动的 Kaspersky Endpoint Security for Windows 策略决定了哪些数据将被从那些设备发送到 KSN（绕过 Kaspersky Security Center）。
5. 启用“**我同意使用卡巴斯基安全网络**”选项。

   如果启用此选项，客户端设备将发送补丁安装结果到 Kaspersky。启用此选项时，请确保阅读并接受 KSN 声明的条款。

   如果使用的是卡巴斯基私人安全网络，请启用“**配置 KPSN**”选项并单击“**选择 KSN 代理设置文件**”按钮以下载 KPSN 设置（带有 pkcs7 和 pem 扩展名的文件）。下载完设置之后，界面会显示提供商的名称和联系人，以及 KPSN 设置文件的创建日期。

   > 启用 KPSN 时，请注意将分发点配置为直接将 KSN 请求发送到云 KSN。安装了网络代理版本 11（或更早版本）的分发点将继续向云 KSN 发送 KSN 请求。如果要重新配置分发点以将 KSN 请求发送到 KPSN，请为每个分发点启用“**转发 KSN 请求到管理服务器**”选项。您可以在分发点属性或网络代理策略中启用此选项。

   当您选择“**配置 KPSN**”复选框时，将出现关于 KPSN 详情的消息。

如果您在 Kaspersky Security Center 启用“**配置 KPSN**”选项，这些应用程序将接收支持 KPSN 的相关信息。在应用程序设置窗口，在**高级威胁保护**区域的**卡巴斯基安全网络**子区域中，将显示有关选定 KSN 提供者的信息：KSN 或 KPSN。

如果您使用的应用程序版本早于 Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 或早于 Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent，在您运行 KPSN 时，我们建议您使用未启用 KPSN 使用的从属管理服务器。

如果在管理服务器属性窗口的 **KSN 代理 → KSN 代理设置**区域配置了 KPSN，则 Kaspersky Security Center 不发送任何统计数据到卡巴斯基安全网络。

如果您在管理服务器属性中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，请启用“**当连接到 KPSN 时忽略代理服务器设置**”选项。否则，从受管理应用程序的请求无法到达 KPSN。

6. 配置管理服务器到 KSN 代理服务的连接：

   - 在“**连接设置**”下，对于“**TCP 端口**”，指定用于连接到 KSN 代理服务器的 TCP 端口号。连接到 KSN 代理的默认端口是 13111。
   - 如果您要让管理服务器通过 UDP 端口连接到 KSN 代理服务器，请启用“**使用 UDP 端口**”选项，并为“**UDP 端口**”指定端口号。默认情况下，此选项为禁用状态，并且使用 TCP 端口。如果启用此选项，默认将使用 UDP 端口 15111 连接到 KSN 代理服务器。
   - 如果您希望管理服务器通过 HTTPS 端口连接到 KSN 代理，请启用“**使用 HTTPS 的端口**”选项，并指定端口号。默认情况下，此选项为禁用状态，并且使用 TCP 端口。如果启用此选项，默认将使用 HTTPS 端口 17111 连接到 KSN 代理服务器。

7. 启用**通过主管理服务器连接从属管理服务器到 KSN**选项。

   如果启用此选项，则任何层级的从属管理服务器使用主管理服务器作为 KSN 代理服务器。如果禁用此选项，从属管理服务器自己连接到 KSN。该情况下，受管理设备使用从属管理服务器作为 KSN 代理服务器。

   如果从属管理服务器属性中“**KSN 代理设置**”区域的右侧面板中选中了“**使用管理服务器作为代理服务器**”复选框，则从属管理服务器将使用主管理服务器作为代理服务器。

8. 单击“**确定**”。

KSN 访问设置将被保存。

您也可以设置分发点访问 KSN，例如，如果您想降低管理服务器负载。作为 KSN 代理服务器的分发点从受管理设备直接发送 KSN 请求到 Kaspersky，不使用管理服务器。

要设置分发点到卡巴斯基安全网络（KSN）的访问：

1. 确保分发点是手动分配。
2. 在控制台树中，选择**管理服务器**节点。
3. 在管理服务器的上下文菜单中，选择“**属性**”。
4. 在管理服务器属性窗口，选择“**分发点**”区域。

5. 在列表中选择分发点并点击**属性**按钮来打开属性窗口。
6. 在分发点属性窗口，在 **KSN 代理**区域，选择**通过互联网直接访问 KSN 云/KPSN**。
7. 单击“**确定**”。

该分发点将作为 KSN 代理服务器。

启用和禁用 KSN

要启用 KSN:

1. 在控制台树中，选择您希望为其启用 KSN 的管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口的“**KSN 代理**”区域，选择“**KSN 代理设置**”子区域。
4. 选择“**使用管理服务器作为代理服务器**”。

   KSN 代理服务器将被启用。
5. 选择“**我同意使用卡巴斯基安全网络**”复选框。

   KSN 将被启用。

   如果选择了此选框，客户端设备将发送补丁安装结果到 Kaspersky。选中此选框时，您应阅读并接受 KSN 声明的条款。
6. 单击“**确定**”。

要禁用 KSN:

1. 在控制台树中，选择您希望为其启用 KSN 的管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口的“**KSN 代理**”区域，选择“**KSN 代理设置**”子区域。
4. 清除“**使用管理服务器作为代理服务器**”复选框，禁用 KSN 代理服务，或清除“**我同意使用卡巴斯基安全网络**”复选框。

   如果清除选择了此选框，客户端设备将不发送补丁安装结果到 Kaspersky。

   如果您使用 KPSN，请清除“**配置 KPSN**”复选框。

   KSN 将被禁用。
5. 单击“**确定**”。

查看已接受的 KSN 声明

启用卡巴斯基安全网络 (KSN) 时，必须阅读并接受 KSN 声明。您可以随时查看已接受的 KSN 声明。

要查看已接受的 KSN 声明：

1. 在控制台树中，选择启用了 KSN 的管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口的“**KSN 代理**”区域，选择“**KSN 代理设置**”子区域。
4. 单击“**查看接受的 KSN 声明**”链接。

   在打开的窗口中，可以查看已接受的 KSN 声明的文本。

查看 KSN 代理服务器统计信息

*KSN 代理服务器*可确保卡巴斯基安全网络基础架构和由管理服务器管理的客户端设备之间的交互。

使用 KSN 代理服务器提供您以下功能：

- 即使无法直接访问互联网，客户端设备也可以向 KSN 发送请求以及向 KSN 传送信息。
- KSN 代理可缓存处理后的数据，从而减少发送通道的工作负荷以及为等待客户端设备所请求的信息而花费的时间。

在管理服务器属性窗口，你可以配置 KSN 代理服务器并查看 KSN 代理服务器使用统计信息。

要查看 KSN 代理服务器的统计：

1. 在控制台树中，选择需要查看 KSN 统计的管理服务器。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在管理服务器属性窗口的“**KSN 代理**”区域，选择“**KSN 代理统计信息**”子区域。

   此部分显示 KSN 代理服务器运行的实际统计信息（缓存记录的数量、缓存中处理的包的数量以及接收到的包）。此外，如果管理服务器连接到 KSN，则会显示相应的信息消息。

   如果必要，运行这些附加操作：

   - 单击“**刷新**”以更新 KSN 代理服务器使用统计信息。
   - 单击“**导出到文件**”按钮保存统计信息到 CSV 文件。
   - 单击“**检查 KSN 连接**”按钮以检查管理服务器当前是否已连接到 KSN。
4. 单击“**确定**”按钮以关闭管理服务器属性窗口。

接受更新的 KSN 声明

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您更新或升级管理服务器时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的版本继续使用 KSN。

更新或升级管理服务器后，将自动显示更新的 KSN 声明。如果您拒绝更新的 KSN 声明，您仍然可以在以后查看并接受它。

要查看然后接受或拒绝更新的 KSN 声明：

1. 在控制台树中，选择**管理服务器**节点。
2. 在“**监控**”选项卡上的“**监控**”区域中，单击“**接受的卡巴斯基安全网络声明已废弃**”链接。

   将打开“**KSN 声明**”窗口。
3. 仔细阅读 KSN 声明，然后做出决定。如果您接受更新的 KSN 声明，请单击“**我接受授权许可协议的条款**”按钮。如果您拒绝更新的 KSN 声明，请单击“**取消**”按钮。

根据您的选择，KSN 会按照当前或更新的 KSN 声明的条款继续工作。您可以随时在管理服务器的属性中查看接受的 KSN 声明的文本。

使用卡巴斯基安全网络获得增强保护

Kaspersky 通过卡巴斯基安全网络为用户提供更进一层的保护。这种保护方式设计用于防御高级的、持续的威胁和零日攻击。云技术和 Kaspersky 病毒分析专长的通力整合助力 Kaspersky Endpoint Security 成为防御最复杂网络威胁的保护方案不二之选。

您可以在 Kaspersky 网站上获得有关 Kaspersky Endpoint Security 增强保护的详细信息。

检查分发点是否充当 KSN 代理服务器

在分配作为分发点的受管理设备上，可以启用 KSN 代理服务器。当 ksnproxy 服务在设备上运行时，受管理设备充当 KSN 代理服务器。您可以在设备上本地检查、打开或关闭此服务。

您可以将基于 Windows 或基于 Linux 的设备分配为分发点。检查分发点的方法取决于该分发点的操作系统。

要检查基于 Windows 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上的 Windows 中，打开“**服务**”（“**所有程序**”→“**管理工具**”→“**服务**”）。
2. 在服务列表，检查 ksnproxy 服务是否正在运行。

   如果 ksnproxy 服务正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

如果您想，您可以关闭 ksnproxy 服务。在这种情况下，分发点上的网络代理停止参与卡巴斯基安全网络。该需要本地管理员权限。

要检查基于 Linux 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上，显示正在运行的进程列表。
2. 在正在运行的进程列表中，检查 `/opt/kaspersky/ksc64/sbin/ksnproxy` 进程是否 正在运行。

如果 `/opt/kaspersky/ksc64/sbin/ksnproxy` 进程正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

切换在线帮助和离线帮助

如果您没有互联网访问权限，可以使用离线帮助。

要切换在线帮助和离线帮助：

1. 在 Kaspersky Security Center 主窗口的控制台树中选择“**Kaspersky Security Center 15.1**”。
2. 单击“**全局界面设置**”链接。
   设置窗口打开。
3. 在设置窗口中，单击“**使用离线帮助**”。
4. 单击“**确定**”。

   设备被应用并保存。如果需要，可以随时更改回设置，并随时开始使用在线帮助。

导出事件到 SIEM 系统

该部分解释了如何导出 Kaspersky Security Center 注册的事件到外部安全信息和事件管理(SIEM)系统。

配置导出事件到 SIEM 系统

Kaspersky Security Center 允许通过以下方法之一进行配置：导出到任何使用 Syslog 格式的 SIEM 系统、导出到使用 LEEF 和 CEF 格式的 QRadar、Splunk、ArcSight SIEM 系统，或直接从 Kaspersky Security Center 数据库导出事件到 SIEM 系统。完成此方案后，管理服务器会自动将事件发送到 SIEM 系统。

先决条件

在开始配置 Kaspersky Security Center 中的事件导出之前：

- 了解有关事件导出方法的更多信息。
- 确保拥有系统设置的值。

> 您可以按任意顺序执行此方案的步骤。

将事件导出到 SIEM 系统的过程包括以下步骤：

- **配置 SIEM 系统以接收来自 Kaspersky Security Center 的事件。**
  说明：配置 SIEM 系统中的事件导出
- **选择要导出到 SIEM 系统的事件：**

说明：

- 管理控制台：标记要以 Syslog 格式导出的 Kaspersky 应用程序事件、标记要以 Syslog 格式导出的常规事件
- Kaspersky Security Center Web Console：标记要以 Syslog 格式导出的 Kaspersky 应用程序事件、标记要以 Syslog 格式导出的常规事件

- **配置使用以下方法之一将事件导出到 SIEM 系统：**
  - 使用TCP、UDP或TLS over TCP协议。
    说明：
    - 管理控制台：配置导出事件到 SIEM 系统
    - Kaspersky Security Center Web Console：配置导出事件到 SIEM 系统
  - 直接从 Kaspersky Security Center 数据库导出事件（Kaspersky Security Center 数据库提供了一组公共视图；您可以在 klakdb.chm 文档中找到这些公共视图的说明）。

结果

配置导出事件到 SIEM 系统后，如果您选择了要导出的事件，可以查看导出结果。

在您开始之前

当设置在 Kaspersky Security Center 中自动导出事件时，必须指定一些 SIEM 系统设置。建议您提前检查这些设置，以便准备设置 Kaspersky Security Center。

要成功配置自动发送事件到 SIEM 系统，您必须知道以下设置：

- **SIEM 系统服务器地址**

  安装了当前使用的 SIEM 系统的服务器的 IP 地址。在您的 SIEM 系统设置中检查此值。

- **SIEM 系统服务器端口**

  用于建立 Kaspersky Security Center 和您的 SIEM 系统服务器之间连接的端口号。您在 Kaspersky Security Center 设置中和您 SIEM 系统的接收设置中指定该值。

- **协议**

  用于从 Kaspersky Security Center 传输消息到您的 SIEM 系统的协议。您在 Kaspersky Security Center 设置中和您 SIEM 系统的接收设置中指定该值。

关于 Kaspersky Security Center 中的事件

Kaspersky Security Center 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。事件信息保存在管理服务器数据库。您可以导出这些信息到外部 SIEM 系统。导出事件信息到外部 SIEM 系统使 SIEM 系统管理员可以快速响应发生在受管理设备或管理组中的安全系统事件。

事件类型

Kaspersky Security Center 中有以下类型的事件：

- 常规事件。这些事件发生在所有受管理卡巴斯基应用程序中。常规事件的一个示例是病毒爆发常规事件具有严格定义的语法和语义。常规事件用于报告和仪表板等方面。
- 受管理卡巴斯基应用程序特定事件。每个受管理 Kaspersky 应用程序都拥有自己的事件集。

事件源

以下应用程序可以生成事件：

- Kaspersky Security Center 组件：
  - 管理服务器
  - 网络代理
  - iOS MDM 服务器
- 受管理的卡巴斯基应用程序

  有关受管理卡巴斯基应用程序生成的事件的详细信息，请参阅相应应用程序的文档。

您可以在应用程序策略的“**事件配置**”选项卡上查看应用程序可以生成的事件的完整列表。对于管理服务器，您还可以在管理服务器属性中查看事件列表。

事件的重要级别

每个事件都有自己的重要级别。取决于发生的条件，一个事件可以被分配不同的重要级别。四个事件重要级别如下：

- *严重事件*指示发生了可能导致数据丢失、操作系统异常或严重错误的严重问题。
- *功能失败*指示在应用程序操作中或执行过程中发生了严重问题、错误或功能异常。
- *警告*是不严重的事件，但是也指示了今后可能发生的潜在问题。如果在事件发生后应用程序可以被恢复而不丢失数据或功能，则这些事件是警告级别。
- *信息*事件用于提示成功完成操作、应用程序的正常功能或完成了某过程。

每个事件都有一个存储期限，在这时间内您可以在 Kaspersky Security Center 中查看或修改。一些事件默认下不保存在管理服务器数据库，因为它们的存储期限是零。仅可以在管理服务器数据库中保存至少一天的事件可以被导出到外部系统。

关于事件导出

您可以在处理组织和技术级别的安全问题的集中式系统内使用事件导出，提供安全监控服务，以及合并来自不同解决方案的信息。即是提供对网络硬件和应用程序生成的安全警告的实时分析的 SIEM 系统，或者安全操作中心 (SOC)。

这些系统可以从许多源接收数据，包括网络、安全、服务器、数据库和应用程序。SIEM 系统也提供功能以集成监控的数据，以便帮助您避免丢失关键事件。而且，系统执行相关事件和警告的自动分析以通知管理员安全问题。警告可以通过仪表盘实现，或可以通过第三方渠道发送，例如邮件。

从 Kaspersky Security Center 导出事件到外部 SIEM 系统的进程设计两部分：事件发送者 — Kaspersky Security Center 和事件接收者 — SIEM 系统。要成功导出事件，您必须在 SIEM 系统和 Kaspersky Security Center 中进行配置。您可以先配置任意一端。您可以配置 Kaspersky Security Center 中的事件传输，然后配置 SIEM 系统对事件的接收，或者相反。

从 Kaspersky Security Center 发送事件的方法

有三种方法从 Kaspersky Security Center 发送事件到外部系统：

- 通过 Syslog 协议发送事件到任意 SIEM 系统

  使用 Syslog 协议，您可以转发发生在 Kaspersky Security Center 管理服务器上和受管理设备上安装的 Kaspersky 应用程序中的任意事件。Syslog 协议是标准消息记录协议。您可以用它将事件导出到任何 SIEM 系统。

  为此，您需要标记希望中继到 SIEM 系统的事件。您可以在管理控制台或 Kaspersky Security Center Web Console中标记事件。只有标记的事件才会被中继到 SIEM 系统。如果您没有标记任何内容，则不会中继任何事件。

- 通过 CEF 和 LEEF 协议发送事件到 QRadar、Splunk 和 ArcSight 系统

  您可以使用 CEF 和 LEEF 协议导出常规事件。当通过 CEF 和 LEEF 协议导出事件时，您不必能够选择指定事件以导出。相反，所有常规事件都被导出。要将 Kaspersky Security Center 事件转换为 CEF 和 LEEF 格式的事件，您需要使用siem_conversion_rules.xml 文件。该文件包含 Kaspersky Security Center 事件属性列表以及 CEF 和 LEEF 格式的事件的相应属性。此外，siem_conversion_rules.xml 文件包含用于生成与事件对应的消息的规则。该文件包含在 Kaspersky Security Center 分发包。

  不同于 Syslog 协议，CEF 和 LEEF 协议不通用。CEF 和 LEEF 为 SIEM 系统所设计(QRadar、Splunk 和 ArcSight)。因此，当您选择通过这些协议导出事件时，您使用 SIEM 系统所需解析器。

- 直接从 Kaspersky Security Center 数据库到 SIEM 系统

  以该方法导出事件可以用于通过使用 SQL 查询直接从数据库公共视图接收事件。查询结果被保存到 XML 文件，可以用于外部系统的输入数据。仅仅公共视图中的事件可以被直接从数据库中导出。

通过 SIEM 系统接收事件

SIEM 系统必须接收和正确解析来自 Kaspersky Security Center 的事件。因为这些目的，您必须正确配置 SIEM 系统。配置取决于特定的 SIEM 系统。然而，有一些配置所有 SIEM 系统的通用步骤，例如配置接收器和解析器。

关于配置 SIEM 系统中的事件导出

从 Kaspersky Security Center 导出事件到外部 SIEM 系统的进程设计两部分：事件发送者 — Kaspersky Security Center 和事件接收者 — SIEM 系统。必须在 SIEM 系统和 Kaspersky Security Center 中配置事件导出。

您在 SIEM 系统中指定的设置取决于您使用的系统。通常，对于所有 SIEM 系统，您必须设置接收器和消息解析器（可选）以解析接收的事件。

设置接收器

为了接收 Kaspersky Security Center 发送的事件，您必须在您的 SIEM 系统中设置接收器。通常，必须在 SIEM 系统指定以下设置：

- **导出协议或输入类型**

  它是消息传输协议，例如 UDP。该协议必须与您在 Kaspersky Security Center 中指定的协议相同。

- **端口**

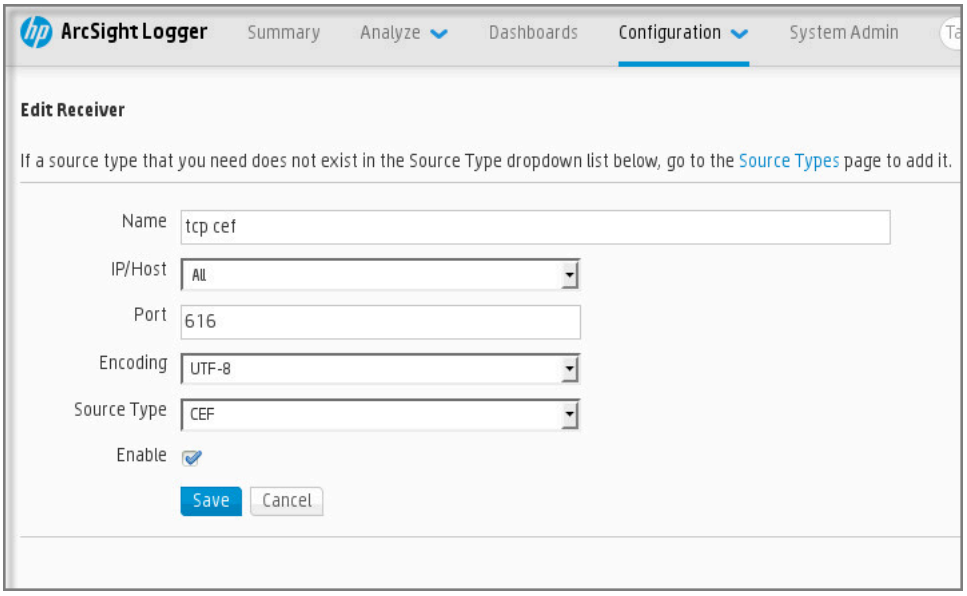
  连接到 Kaspersky Security Center 的端口号。该端口必须与您在 Kaspersky Security Center 中指定的端口相同。

- **消息协议或源类型**

  用于导出事件到 SIEM 系统的协议。它可以是标准协议之一：Syslog、CEF 或 LEEF。SIEM 系统根据您指定的协议选择消息解析器。

根据所使用的 SIEM 系统，您可能需要指定一些附加接收器设置。

下图显示了 ArcSight 的接收器设置截图。



ArcSight 的接收器设置

消息解析器

导出的事件作为消息被传递到 SIEM 系统。这些消息必须正确解析，以便事件信息可以被 SIEM 系统使用。消息解析器是 SIEM 系统的一部分，它们用于拆分消息内容到相关字段，例如事件 ID、严重级别、描述、参数。这将启用 SIEM 系统以处理从 Kaspersky Security Center 接收的事件，以便它们可以被存储在 SIEM 系统数据库。

标记要以 Syslog 格式导出到 SIEM 系统的事件

在启用自动导出事件后，您必须选择将被导出到外部 SIEM 系统的事件。

您可以配置基于以下条件之一导出 Syslog 格式的事件到外部系统：

- 标记常规事件。如果在事件设置或管理服务器设置中标记要在策略中导出的事件，SIEM 系统将接收由特定策略管理的所有应用程序中发生的所标记事件。如果导出的事件在策略中被选中，您将不能为由该策略管理的个别应用程序重新定义所选事件。
- 为受管理应用程序标记事件。如果为受管理设备上安装的受管理应用程序选择要导出的事件，SIEM 系统将仅接收该应用程序中发生的事件。

标记要以 Syslog 格式导出的 Kaspersky 应用程序事件

如果要导出受管理设备上安装的个别受管理应用程序中发生的事件，则标记要为应用程序导出的事件。如果先前导出的事件已在策略中标记，您将不能为此策略管理的个别应用程序重新定义所标记的事件。

要为个别受管理应用程序标记要导出的事件：

1. 在 Kaspersky Security Center 控制台树，选择“**受管理设备**”节点并转到“**设备**”选项卡。
2. 右键单击以打开相关设备的上下文菜单并选择“**属性**”。
3. 在打开的“设备属性”窗口中，选择“**应用程序**”区域。
4. 在显示的应用程序列表中，选择要导出事件的应用程序，然后单击“**属性**”按钮。
5. 在应用程序属性窗口中，选择“**事件配置**”区域。
6. 在显示的事件列表中，选择一个或几个需要导出到 SIEM 系统的事件，并单击“**属性**”按钮。
7. 在出现的事件属性窗口中，选中“**使用 Syslog 导出到 SIEM 系统**”复选框以标记要以 Syslog 格式导出的选定事件。清除“**使用 Syslog 导出到 SIEM 系统**”复选框以取消标记要以 Syslog 格式导出的选定事件。

如果事件属性在策略中定义，该窗口的字段无法被编辑。

"事件属性"窗口

8. 单击"**确定**"保存更改。

9. 在应用程序属性窗口和设备属性窗口中单击"**确定**"。

标记的事件将以 Syslog 格式发送到 SIEM 系统。取消选中"**使用 Syslog 导出到 SIEM 系统**"复选框的事件不会导出到 SIEM 系统。导出将在您启用自动导出和选择要导出的事件后立即开始。配置 SIEM 系统以确保它接收来自 Kaspersky Security Center 的事件。

标记要以 Syslog 格式导出的常规事件

如果您要导出发生在被特定策略管理的所有应用程序中的事件，则标记要在策略中导出的事件。在这种情况下，无法为单个受管理应用程序标记事件。

要标记常规事件以导出到 SIEM 系统：

1. 在 Kaspersky Security Center 控制台树中，选择"**策略**"节点。

2. 右击以打开相关策略的上下文菜单并选择"**属性**"。

3. 在打开的策略属性窗口中，选择"**事件配置**"区域。

4. 在显示的事件列表中，选择一个或几个需要导出到 SIEM 系统的事件，并单击"**属性**"按钮。
   如果您需要选择所有事件，请单击"**全部选择**"按钮。

5. 在出现的事件属性窗口中，选中“**使用 Syslog 导出到 SIEM 系统**”复选框以标记要以 Syslog 格式导出的选定事件。取消选中“**使用 Syslog 导出到 SIEM 系统**”复选框以取消标记要以 Syslog 格式导出的选定事件。

管理服务器事件属性窗口

6. 单击“**确定**”保存更改。

7. 在策略属性窗口，单击“**确定**”。

标记的事件将以 Syslog 格式发送到 SIEM 系统。取消选中“**使用 Syslog 导出到 SIEM 系统**”复选框的事件不会导出到 SIEM 系统。导出将在您启用自动导出和选择要导出的事件后立即开始。配置 SIEM 系统以确保它接收来自 Kaspersky Security Center 的事件。

关于使用 Syslog 格式导出事件

您可以使用 Syslog 格式将管理服务器和受管理设备上安装的其他卡巴斯基应用程序中发生的事件导出到 SIEM 系统。

Syslog 是消息记录协议的标准。它允许分离生成消息的软件、存储消息的系统和报告和分析消息的软件。每个消息都带有设备代码标签，指示生成消息的软件类型，并被分配严重级别。

Syslog 格式由 Request for Comments (RFC) 文档定义，该文档由 Internet Engineering Task Force（互联网标准）发布。RFC 5424 标准用于从 Kaspersky Security Center 导出事件到外部系统。

在 Kaspersky Security Center 中，您可以配置使用 Syslog 格式导出事件到外部系统。

导出过程包含两个步骤：

1. 启用自动事件导出。在该步骤，Kaspersky Security Center 被配置，以便能发送事件到 SIEM 系统。Kaspersky Security Center 在您启用自动导出后立即开始发送事件。

2. 选择事件以导出到外部系统。在该步骤，您可以选择导出哪些事件到 SIEM 系统。

关于使用 CEF 和 LEEF 格式导出事件

您可以使用 CEF 和 LEEF 格式将常规事件以及由卡巴斯基应用程序传输到管理服务器的事件导出到 SIEM 系统。导出事件集是预定义的，您无法选择要导出的事件。在将事件发送到 SIEM系统（QRadar、ArcSight 或 Splunk）之前，需要使用siem_conversion_rules.xml 文件中指定的规则将 Kaspersky Security Center 事件解释为 CEF 和 LEEF 格式的事件。

基于使用的 SIEM 系统选择导出格式。下表显示了 SIEM 系统和对应的导出格式。

导出事件到 SIEM 系统的格式

SIEM 系统	导出格式
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - 用于 IBM®Security QRadar SIEM 的自定义事件格式。QRadar 可以集成、识别和处理 LEEF 事件。LEEF 事件必须使用 UTF-8 字符编码。您可以在 IBM Knowledge Center 查看 LEEF 协议的详情。

- CEF (通用事件格式)—开放式日志管理标准，涉及来自不同的网络设备和应用程序的安全信息的协同工作。CEF 允许您使用通用日志格式，因此数据可以被简易整合以用企业管理系统分析。CEF 事件必须使用 UTF-8 字符编码。

自动导出意味着 Kaspersky Security Center 发送常规事件到 SIEM 系统。事件自动导出在您启用后立即开始。该部分详细解释了如何启用自动事件导出。

配置 Kaspersky Security Center 以导出事件到 SIEM 系统

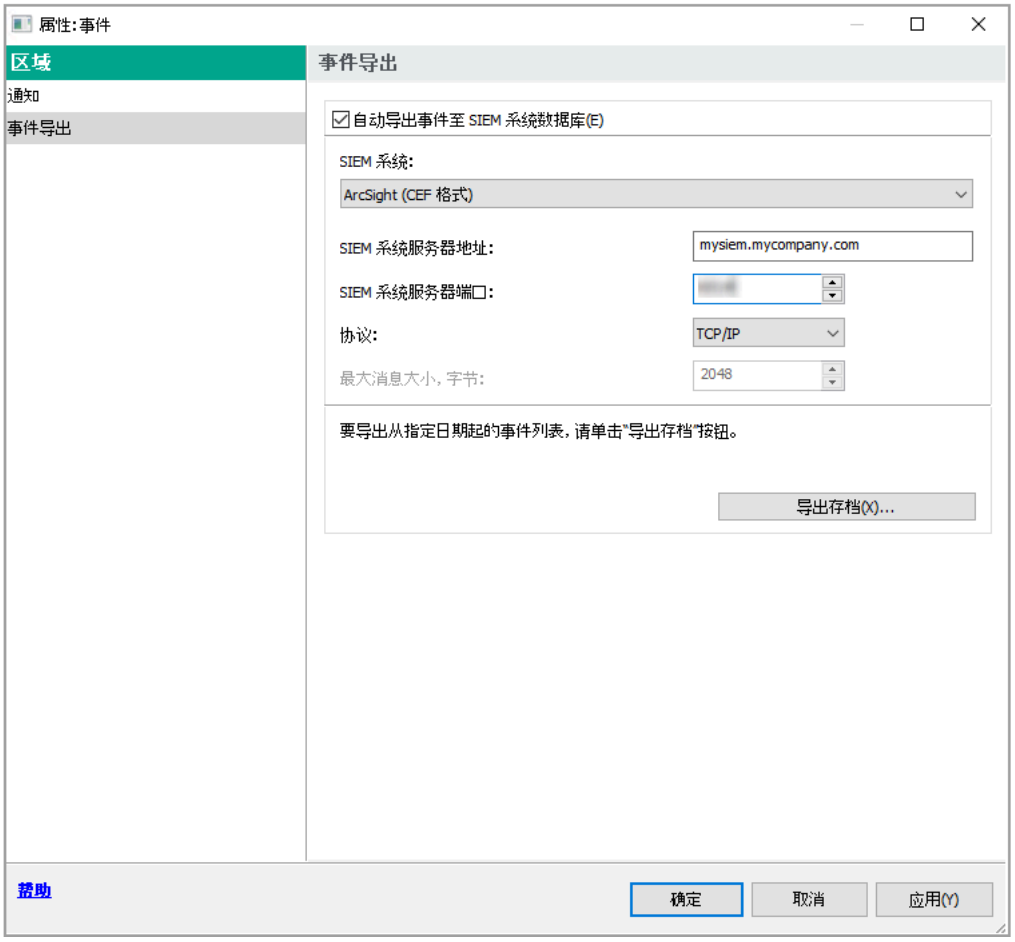
您可以在 Kaspersky Security Center 中启用自动事件导出。

仅常规事件可以通过 CEF 和 LEEF 格式从受管理应用程序导出。用于将事件转换为 CEF 和 LEEF 格式的解释规则在 Kaspersky Security Center 分发套件中包含的siem_conversion_rules.xml文件中指定。应用程序特定事件不能通过 CEF 和 LEEF 格式从受管理应用程序导出。如果您需要导出受管理应用程序的事件或者使用受管理应用程序策略配置的自定义事件集合，则必须以 Syslog 格式导出事件。

要启用自动事件导出：

1. 在 Kaspersky Security Center 控制台树，选择您要导出事件的管理服务器。
2. 在所选管理服务器的工作区中，选择“**事件**”选项卡。
3. 单击“**配置通知和事件导出**”链接旁边的下拉箭头，然后在下拉列表中选择“**配置导出到 SIEM 系统**”。
   此时将打开事件属性窗口，显示“**事件导出**”区域。

4. 在“**事件导出**”区域，指定以下导出设置：



事件属性窗口的事件导出区域

- **自动导出事件至 SIEM 系统数据库**

  选择此复选框以启用自动导出事件至 SIEM 系统。选择该复选框启用**导出事件**区域的所有字段。

- **SIEM 系统**

  选择要导出事件的 SIEM 系统：QRadar®（LEEF 格式）、ArcSight（CEF 格式）、Splunk®（CEF 格式）和 Syslog 格式 (RFC 5424)。

  如果选择 Syslog 格式，则必须指定：

  最大消息大小，字节

  指定 SIEM 系统消息的最大大小。每个事件被一条消息转发。如果消息的精确长度超过指定值，消息被截断且数据可能丢失。默认大小是 2048 字节。如果您在“**SIEM 系统**”字段选择了 Syslog 格式，则该字段可用。

- **SIEM 系统服务器地址**

  指定 SIEM 系统服务器地址。地址可以被指定为 DNS 或 NetBIOS 名称或 IP 地址。

- **SIEM 系统服务器端口**

  指定用于连接至 SIEM 系统服务器的端口号。该端口号必须和 SIEM 系统用于接收事件的端口相同(参见"配置 SIEM 系统")。

- **协议**

  选择该协议用于传输消息到 SIEM 系统。您可以选择TCP、UDP或TLS over TCP协议。

  如果选择 TLS over TCP 协议，则指定以下 TLS 设置：

  - **SIEM 服务器身份验证**

    选择以下方式之一对 SIEM 系统服务器进行身份验证：

    - **通过使用 CA 证书**。您可以接收含有受信任证书颁发机构 (CA) 的证书列表的文件，并将该文件上传到 Kaspersky Security Center。Kaspersky Security Center 会检查 SIEM 系统服务器证书是否也具有受信任 CA 的签名。

      要添加受信任证书，请单击"**浏览**"按钮，然后上传证书。

      如果选择**通过使用 CA 证书**选项，则可以在**服务器证书主题(可选)**字段中指定主题名称。*主题名称*是接收证书的域名。如果 SIEM 系统服务器的域名与 SIEM 系统服务器证书的主题名称不匹配，Kaspersky Security Center 将无法连接到 SIEM 系统服务器。但是，如果您在证书中更改主题名称，则 SIEM 系统服务器可以更改域名。为此，请在"**服务器证书主题(可选)**"字段中指定主题名称。如果任一指定主题名称与 SIEM 系统证书的主题名称匹配，Kaspersky Security Center 将验证 SIEM 系统服务器证书。

    - **通过使用服务器证书的 SHA1 指纹**。您可以在 Kaspersky Security Center 中指定 SIEM 系统证书的 SHA-1 指纹。要添加 SHA-1 指纹，请在选项下的字段中输入。

  - **客户端身份验证**

    对于客户端身份验证，可以插入证书或在 Kaspersky Security Center 中生成证书。

    - **插入证书**。您可以使用从任何来源（例如，从任何受信任 CA）收到的证书。要插入现有证书，请单击**浏览证书**按钮。在打开的"**证书**"窗口中，选择以下证书类型之一，然后指定证书及其私钥：

      - **X.509 证书**。上传在**私钥(*.prk, *.pem)**字段中包含私钥的文件，以及在**证书(*.cer)**字段中包含证书的文件。为此，请单击相应字段右侧的"**浏览**"按钮，然后添加所需的文件。这两个文件不相互依赖，文件的加载顺序也不重要。上传两个文件后，在"**密码**"字段中指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

      - **PKCS #12 容器**。在"**证书文件**"字段中上传包含证书及其私钥的单个文件。为此，请单击字段右侧的"**浏览**"按钮，然后添加所需的文件。上传该文件后，在"**密码**"字段中指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

    - **生成密钥**。您可以在 Kaspersky Security Center 中生成自签名证书。单击**常规证书**按钮，然后在**主题**字段中输入主题名称。客户端证书将为此主题名称生成，此证书的 SHA-1 指纹将显示在"**客户端证书的 SHA1 指纹**"字段中。结果是，Kaspersky Security Center 将存储生成的自签名证书，您可以将证书的公共部分或 SHA-1 指纹传递给 SIEM 系统。

5. 如果要将过去指定日期之后发生的事件导出到 SIEM 系统数据库，请单击"**导出存档**"按钮，然后指定事件导出的开始日期。默认下，事件导出在您启用后立即开始。

6. 要检查 SIEM 系统连接是否已配置，请单击**测试设置**按钮。

   应用程序尝试建立与 SIEM 系统的连接并发送测试事件。如果未建立连接，则会显示错误消息。如果连接已建立，则不会显示任何消息。如果需要，您可以在**事件**选项卡上查看测试事件。

7. 单击“**确定**”。

自动导出事件被启用。

在启用自动导出事件后，您必须选择将被导出到 SIEM 系统的事件。

直接从数据库导出事件

您可以直接从 Kaspersky Security Center 数据库接收事件，而不必使用 Kaspersky Security Center 界面。您可以直接查询公共视图并检索事件数据，也可以基于现有公共视图创建您自己的视图并定位它们以获取所需数据。

公共视图

为了您的方便，在 Kaspersky Security Center 数据库中提供了公共视图集。您可以在 klakdb.chm 文档中找到这些公共视图的描述。

v_akpub_ev_event 公共视图包含一组展示数据库中事件参数的字段集。在 klakdb.chm 文档中您也可以查找对应于其他 Kaspersky Security Center 实体的公共视图信息，例如，设备、应用程序或用户。您可以在您的查询中使用该信息。

该部分包含了使用 klsql2 实用工具执行 SQL 查询的说明以及查询例子。

要创建 SQL 查询或数据库视图，您也可以使用其他程序以操作数据库。关于如何查看连接到 Kaspersky Security Center 数据库的参数的信息，例如实例名称和数据库名称，在对应区域给出。

使用 klsql2 实用工具执行 SQL 查询

本章描述了如何下载和使用 klsql2 实用工具，以及如何使用该实用工具执行 SQL 查询。

要使用 klsql2 实用程序：

1. 在 Kaspersky Security Center 的安装文件夹中寻找 klsql2 实用程序。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。不要使用用于旧版 Kaspersky Security Center 的 klsql2 实用程序版本。

2. 在任何文本编辑器中创建一个扩展名为 .sql 的文件，并将该文件与该实用程序放在同一文件夹中。

3. 在创建的 .sql 文件中，键入所需的 SQL 查询，然后保存该文件。

4. 在 Kaspersky Security Center 管理服务器设备上，在命令行，输入以下命令以从 .sql 文件执行 SQL 查询并保存结果到 result.xml 文件：

   ```
   klsql2 -i src.sql -u <用户名> -p <密码> -o result.xml
   ```

   其中 < username > 和 < password > 是有权访问数据库的用户账户的凭据。

5. 如果需要，输入有权访问数据库的用户账户的登录名和密码。

6. 打开新创建的 result.xml 文件以查看 SQL 查询结果。

您可以编辑 .sql 文件并创建到公共视图的任意 SQL 查询。然后，从命令行，执行您的 SQL 查询并保存结果到文件。

klsql2 实用工具中的 SQL 查询例子

该部分显示 SQL 查询的例子，通过 klsql2 实用工具执行。

以下例子阐述了对过去七天发生在设备上的事件的获取，并根据事件发生时间顺序显示事件。首先显示最近的事件。

Microsoft SQL Server 的示例：

```
SELECT
  /* 事件标识 */
  e.nId,

  /* 事件发生的时间 */
  e.tmRiseTime,

  /* 事件类型的内部名称 */
  e.strEventType,

  /* 事件的显示名称 */
  e.wstrEventTypeDisplayName,

  /* 事件的显示描述 */
  e.wstrDescription,

  /* 事件所在的组名称 */
  e.wstrGroupName,

  /* 发生事件的设备的显示名称 */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* 发生事件的设备的 IP 地址 */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

PostgreSQL 示例：

```
SELECT
  /* 事件标识 */
  "e"."nId",

  /* 事件发生的时间 */
  "e"."tmRiseTime",

  /* 事件类型的内部名称 */
  "e"."strEventType",

  /* 事件的显示名称 */
  "e"."wstrEventTypeDisplayName",

  /* 事件的显示描述 */
  "e"."wstrDescription",

  /* 事件的显示描述 */
  "e"."wstrGroupName",

  /* 发生事件的设备的显示名称 */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* 发生事件的设备的 IP 地址 */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 或 MariaDB 示例：

```
SELECT

  /* 事件标识 */
  `e`.`nId`,

  /* 事件发生的时间 */
  `e`.`tmRiseTime`,

  /* 事件类型的内部名称 */
  `e`.`strEventType`,

  /* 事件的显示名称 */
  `e`.`wstrEventTypeDisplayName`,

  /* 事件的显示描述 */
  `e`.`wstrDescription`,

  /* 设备组名称 */
  `e`.`wstrGroupName`,

  /* 发生事件的设备的显示名称 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* 发生事件的设备的 IP 地址 */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

查看 Kaspersky Security Center 数据库名称

例如，如果需要发送 SQL 查询并从 SQL 脚本编辑器连接到数据库，则了解数据库名称会很有帮助。

要查看 Kaspersky Security Center 数据库名称：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单并选择“**属性**”。
2. 在管理服务器属性窗口的“区域”窗格中，选择“**高级**”，然后选择“**当前数据库详情**”。
3. 在“**当前数据库详情**”区域，注意以下数据库属性（参见下图）：

- **实例名称**

  当前 Kaspersky Security Center 数据库实例名称。默认值是 .*KAV_CS_ADMIN_KIT*。

- **数据库名称**

  Kaspersky Security Center SQL 数据库名称。默认值是 *KAV*。

- **为 Kaspersky Security Center 数据库分配的空间**

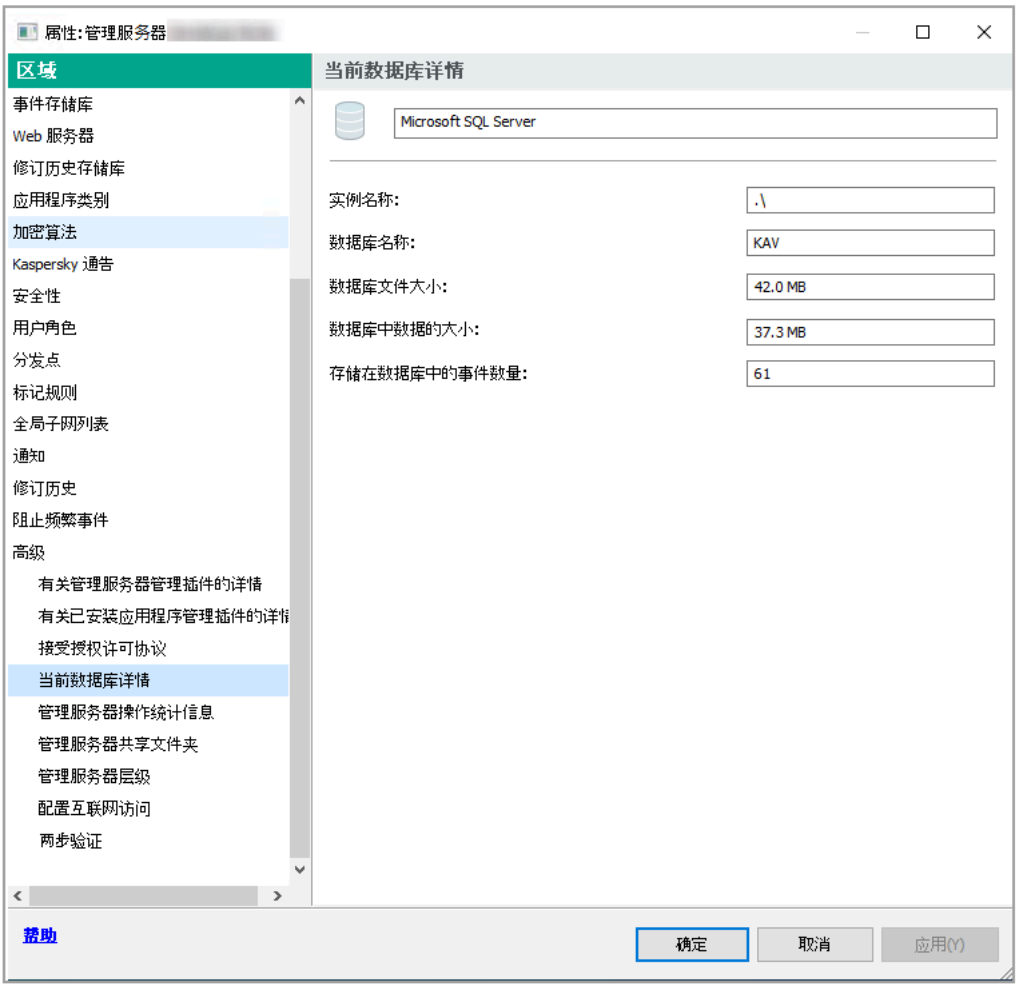
  数据库文件的大小。如果要清理不必要的数据，请使用*管理服务器维护*任务配置数据库压缩。

- **整个数据库中数据的大小**

  DBMS 中当前使用的数据的实际大小。以下文章介绍了如何诊断 DBMS：数据库大小超出限制。

- **存储在数据库中的事件数量**

  当前存储在 DBMS 中的事件数。详细信息请参考以下文章：事件处理和存储。



带有当前管理服务器数据库信息的区域

4. 单击“**确定**”按钮以关闭管理服务器属性窗口。

使用数据库名称在您的 SQL 查询中定位数据库。

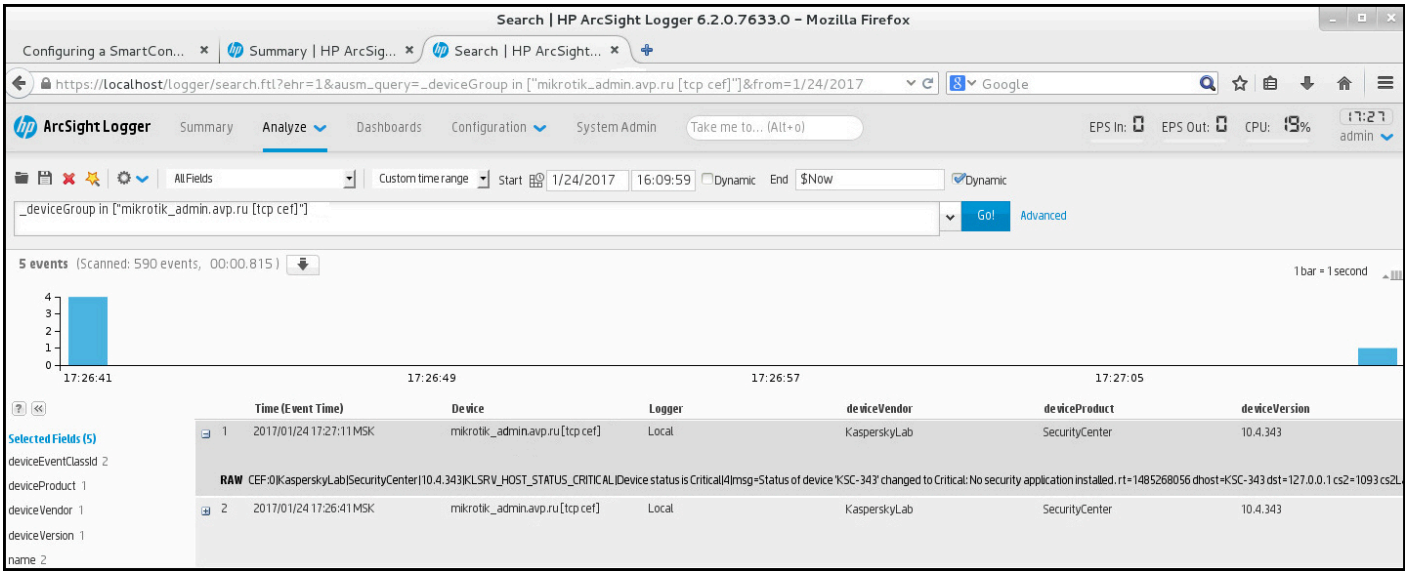
查看导出结果

您可以控制事件导出过程的成功完成。为此，检查带有导出事件的邮件是否被您的 SIEM 系统接收。

如果从 Kaspersky Security Center 发送的事件被接收并被您的 SIEM 系统正确解析，两端的配置被正确完成。否则，检查您在 Kaspersky Security Center 中指定的设置是否与您的 SIEM 系统中的设置一致。

下图显示导出到 ArcSight 的事件。例如，第一个事件是严重的管理服务器事件：“*设备状态为严重*”。

导出事件在您 SIEM 系统中的显示随您使用的 SIEM 系统而不同。



事件例子

使用 SNMP 将统计信息发送到第三方应用程序

本节介绍如何在 Windows 中使用简单网络管理协议 (SNMP) 从管理服务器获取信息。Kaspersky Security Center 包含 SNMP 代理，该代理使用 OID 将管理服务器性能的统计信息传输到辅助应用程序。

本节还包含有关如何解决在 Kaspersky Security Center 中使用 SNMP 时可能遇到的问题的信息。

配置 SNMP 服务以与 Kaspersky Security Center 结合使用

本节介绍如何在 Windows 上配置 SNMP 服务以使用简单网络管理协议 (SNMP) 从管理服务器获取信息。

默认情况下 Windows 上禁用 SNMP 支持。

要在 Windows 中启用 SNMP 支持：

1. 导航到“**控制面板**”。
2. 打开“**添加或删除程序**”菜单。
3. 单击“**启用或关闭 Windows 功能**”。
4. 在 Windows 功能列表中，导航到 SNMP 功能，然后单击“**确定**”。
5. 导航至“**控制面板**”→“**管理工具**”→“**服务**”。
6. 选择 **SNMP 服务**并运行它。
7. 使用 `netstat` 对标准 UDP 端口进行测试，以检查侦听是否正常。

Windows 上启用了 SNMP 支持。

要在 Windows 中配置 SNMP 服务：

1. 确保在常规或静默安装期间安装了Kaspersky Security Center 的**SNMP 代理**组件。
2. 确保**SNMP 服务**和**SNMP 陷阱**Windows 服务正在运行。
3. 确保您的系统上安装了 ManageEngine MIB 浏览器。
4. 在**SNMP Service**服务属性的**安全**选项卡上，添加两个具有以下权限的社区：

社区	权限
kaspersky	通知
public	读写

5. 在**接受来自这些主机的 SNMP 数据包**字段中，添加安装了 ManageEngine MIB 浏览器的设备的 IP 地址，例如 10.10.10.105。
6. 在**陷阱**选项卡上的**社区名称**字段中键入`kaspersky`。
7. 单击“**OK**”保存更改并关闭服务属性窗口。
8. 在 ManageEngine MIB 浏览器中，从 Kaspersky Security Center 安装文件夹加载 adminkit.mib 文件。默认情况下，adminkit.mib 文件位于 <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp 文件夹中。
9. 在 ManageEngine MIB 浏览器窗口的**主机**字段中，添加在其中安装 Kaspersky Security Center 管理服务器的设备的 IP 地址。

SNMP 服务被配置用来使用简单网络管理协议 (SNMP) 从管理服务器获取信息。

SNMP代理和对象标识符

对于 Kaspersky Security Center，SNMP 代理实现为动态库 `klsnmpag.dll`，该库由安装程序在管理服务器安装期间注册。SNMP 代理在 `snmp.exe` 进程（一个 Windows 服务）内工作。第三方应用程序使用 SNMP 接收有关管理服务器性能的统计信息（以计数器的形式出现）。

每个计数器都有一个唯一的*对象标识符*（也称为 OID）。对象标识符是由点分隔的数字序列。管理服务器的对象标识符以 1.3.6.1.4.1.23668.1093 前缀开头。计数器的 OID 是该前缀与描述计数器的后缀的串联。例如，OID 值为 1.3.6.1.4.1.23668.1093.1.1.4 的计数器具有值为 1.1.4 的后缀。

您可以使用 SNMP 客户端（例如 Zabbix）监视系统状态。要获取信息，您可以搜索与信息对应的 OID 值，然后将该值输入到 SNMP 客户端中。然后，SNMP 客户端将返回另一个表示系统状态的值。

计数器和计数器类型的列表位于管理服务器上的 `adminkit.mib` 文件中。*MIB* 代表 Management Information Base。您可以通过专用于请求和显示计数器值的 MIB Viewer 应用程序导入和解析 `.mib` 文件。

从对象标识符获取字符串计数器名称

要使用对象标识符 (OID) 将信息传输到第三方应用程序，您可能需要从该 OID 获取字符串计数器名称。

要从 OID 获取字符串计数器名称：

1. 在文本编辑器中打开位于管理服务器上的 `adminkit.mib` 文件。
2. 找到描述第一个值的命名空间（从左到右）。
   例如，对于 1.1.4 OID 后缀，将是 `"counters" (::= { kladminkit 1 })`。
3. 找到描述第二个值的命名空间。
   例如，对于 1.1.4 OID 后缀，将是 `counters 1`，代表`deployment`。
4. 找到描述第三个值的命名空间。
   例如，对于 1.1.4 OID 后缀，将是 `deployment 4`，代表 `hostsWithAntivirus`。

字符串计数器名称为这些值的串联，例如 `<MIB base namespace>.counters.deployment.hostsWithAntivirus`，它对应于值为 1.3.6.1.4.1.23668.1093.1.1.4 的 OID。

SNMP 的对象标识符的值

下表给出了用于将有关管理服务器性能的信息传输到第三方应用程序的对象标识符（也称为 OID）的值和说明。

用于 SNMP 的对象标识符的值和说明

对象标识符的值	数值数据类型	OID	描述
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	部署状态。状态可以是以下之一： • **信息**。授权许可不再对 N 个设备有效。 • **警告**。以下之一： 总共包含 N 台设备的管理服务器组中有 M 台设备安装了 Kaspersky 应用程序 (N > M)。 N 台设备上的授权许可 L 将在 M 天后到期。 N 台设备上的应用程序安装任务 T 已成功完成，M 台设备需要重新启动。 • **严重**。N 台设备的授权许可已过期。 • **正常**。以上都不是。
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	原因 `deploymentStatus` 表明，管理服务器组包含了太多未安装受管理应用程序的设备。 如果发现几台设备未安装受管理应用程序，值等于 1，否则等于 0。
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	原因 `deploymentStatus` 表明，某些设备上的远程安装任务失败。可以通过 `hostsRemoteInstallFailed` 获取这些设备的数量。
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	原因 `deploymentStatus` 表明，某些设备的授权许可在 7 天后到期。可以通过 `hostsLicenseExpiring` 获取这些设备的数量。
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	原因 `deploymentStatus` 表明，某些设备的授权许可已过期。您可以通过 `hostsLicenseExpired` 获得这些设备的数量。
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	管理服务器组中的设备数。
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	安装了受管理应用程序的管理服务器组中的设备数。
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	远程安装任务失败的设备数。
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	即将过期（少于 7 天）的授权许可密钥的 ID。
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	授权许可密钥已过期的 ID。
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	授权许可到期前的天数。对于此参数，如果距离到期日期还剩不到 7 天，则认为授权许可期限已到期。 如果距离到期日期还剩 7 天以上，则该值为 0。

对象标识符的值	数值数据类型	OID	描述
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	授权许可即将过期（少于 7 天）的设备数。
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	授权许可已到期的设备数。
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	反病毒库更新的当前状态。状态可以是以下之一： • **信息**。管理服务器或设备上的反病毒库已超过 1 天未更新，应用程序安装后不到 1 天。 • **警告**。管理服务器或设备上的反病毒库已超过 3 天没有更新。该值可以在组设置中更改。 • **严重**。管理服务器或设备上的反病毒库已超过 7 天没有更新。该值可以在组设置中更改。 • **正常**。以上都不是。
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	此原因表明，管理服务器长时间未更新。被认为是长时间的时间量在 updatesStatus 中指定。
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	此原因表明某些设备很长时间没有更新（对于**严重**，默认为 7 天或更长时间，对于**警告**为 3 天）。您可以通过 hostsNotUpdated 获得这些设备的数量。
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	管理服务器上次更新反病毒库的时间。
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	包含长期未更新的防病毒库的设备数量（默认情况下，对于**严重**为 7 天或更长时间，对于**警告**为 3 天）。如果有设备处于**严重**更新状态，则仅计算这些设备。您可以通过 updatesStatus 获取更新状态。
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	实时保护的状态。以下之一： • **警告**。以下之一： 在属于管理服务器组的设备上检测到安全漏洞。 加密错误使某些设备更改了保护状态。 长时间未执行全盘扫描。 • **严重**。反病毒保护在管理服务器组中的某些设备上不起作用。 • **正常**。以上都不是。
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	此原因表明某些设备上未运行安全应用程序。您可以通过 hostsAntivirusNotRunning 获得这些设备的数量。
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	此原因表明某些设备上未运行实时保护。您可以通过 hostsRealtimeNotRunning 获取这些设备的数量。
psRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.2.3	实时保护级别与管理员设置的级别不同的设备数量
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	此原因表明有设备包含未消除的对象。您可以通过 hostsNotCuredObject 获得这些设备的数量。
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	此原因表明在某些设备上发现了威胁。您可以通过 hostsTooManyThreats 获得这些设备的数量。
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	此原因表明系统的病毒爆发状态。 如果在一定时间内发现一定数量的病毒，则该值等于 1，否则等于 0。通过使用“病毒攻击”设置，在管理服务器上指定病毒数量和时间量。
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	安全应用程序未运行的设备数。
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	未运行实时保护的设备数。
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	实时保护级别不可接受的设备数。
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	包含未消除对象的设备数。
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	包含威胁的设备数。
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	反病毒全盘扫描的状态。以下之一： • **信息**。自安装应用程序以来，经过的时间不到 7 天。 • **警告**。自安装应用程序以来，超过 7 天未执行反病毒全盘扫描。 • **严重**。自安装应用程序以来，超过 14 天未执行反病毒全盘扫描。 • **正常**。以上都不是。

对象标识符的值	数值数据类型	OID	描述
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	此原因表明，某些设备在一定时间内未经过扫描。您可以通过 hostsNotScannedLately 获得这些设备的数量。时间量在 fullScanStatus 中指定。
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	一定时间内未扫描的设备数。时间量在 fullScanStatus 中指定。
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	管理服务器逻辑网络的状态。以下之一： • **警告**。如果存在无法访问的处于警告状态的设备，或者存在不属于任何管理服务器组的设备。 • **严重**。如果管理服务器已失去某些设备的控制权，或者存在无法访问的处于严重状态的设备。 • **正常**。以上都不是。
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	此原因表明某些设备很长时间未连接到管理服务器（**警告**状态的设备为 7 天或更长，而**严重**状态的设备为 4 天）。您可以通过 hostsNotConnectedLongTime 获得这些设备的数量。
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	此原因表明，管理服务器已失去某些设备的控制权。您可以通过 hostsControlLost 获得这些设备的数量。
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	管理服务器发现的不属于任何管理服务器组的设备数。
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	管理服务器上的组数量。
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	长时间未连接到管理服务器的设备数。被认为是长时间的时间量在 notConnectedLongTime 中指定。
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	不受管理服务器控制的设备数。
eventsStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.6.1	事件子系统的状态。以下之一： • **警告**。以下之一： 管理服务器组的设备长时间未搜索 Windows 更新。 有些设备的状态出现问题。 • **严重**。以下之一： 至少一台设备上存在重要性为“严重”的事件。 至少一台设备上存在重要性为“错误”的事件。 至少一台设备上存在任务未成功完成的事件。 管理服务器组的设备长时间未搜索 Windows 更新。 有些设备的状态出现问题。 • **正常**。以上都不是。
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	原因 eventsStatus 表明，管理服务器上存在一些严重事件。您可以通过 criticalEventsCount 获得这些事件的数量。 如果任何设备上存在至少一个严重事件，则该值等于 1，否则等于 0。
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	管理服务器上的严重事件数。

故障解决

本节列出了使用 SNMP 服务时可能遇到的一些典型问题的解决方案。

第三方应用程序无法连接到 SNMP 服务

确保SNMP 服务已按照配置 SNMP 服务与 Kaspersky Security Center 一起使用部分中所述进行了安装和配置。

SNMP 服务正在工作，但是第三方应用程序无法获取任何值

允许 SNMP 代理跟踪，并确保创建了一个非空文件。这意味着 SNMP 代理已正确注册并运行。之后，在辅助服务设置中允许来自 SNMP 服务的连接。如果辅助服务与 SNMP 代理在同一主机上运行，则 IP 地址列表应包含该主机的 IP 地址或`loopback 127.0.0.1`。

与代理通信的 SNMP 服务应在 Windows 中运行。您可以通过 regedit 在 Windows 注册表中指定 SNMP 代理的路径。

- 在 Windows 10 中：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents

- 在 Windows Vista 和 Windows Server 2008 中：

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

您也可以通过 regedit 允许 SNMP 代理跟踪。

- 对于 32 位系统：

  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug

- 对于 64 位系统：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb

  "TraceLevel"=dword:00000004

  "TraceDir"="C:\\"

值与管理控制台的状态不匹配

为了减少管理服务器上的负载，为 SNMP 代理实施了值缓存。正在实施的缓存与管理服务器上不断变化的值之间的延迟可能导致 SNMP 代理返回的值与实际值不匹配。使用第三方应用程序时，应考虑可能的延迟。

使用云环境

本节提供了 Kaspersky Security Center 在云环境（如 Amazon Web Services、Microsoft Azure 或 Google Cloud）中的部署和维护信息。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

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）以及 KSN 功能。

关于使用云环境

Kaspersky Security Center 15.1 不仅工作在预置设备上，也提供特殊功能以使用云环境。Kaspersky Security Center 可与以下虚拟机一起使用：

- Amazon EC2 实例（以下也称为*实例*）。Amazon EC2 实例是基于 Amazon Web Services (AWS) 平台创建的虚拟机。Kaspersky Security Center 使用 AWS *API*（应用程序编程接口）。
- Microsoft Azure 虚拟机。Kaspersky Security Center 使用 Azure API。
- Google Cloud 虚拟机实例。Kaspersky Security Center 使用 Google API。

您可以在实例或虚拟机上部署 Kaspersky Security Center 以管理云环境中设备的保护，并使用 Kaspersky Security Center 的特殊功能以在云环境中工作。这些功能包括：

- 使用 API 工具轮询云环境中的设备
- 使用 API 工具安装网络代理和安全应用程序到云环境中的设备
- 基于其是否属于指定云段来搜索设备

您也可以使用部署了 Kaspersky Security Center 管理服务器的实例或虚拟机来保护内部部署设备（例如，如果云服务器比物理服务器更容易维修和维护）。如果是这种情况，您像管理服务器安装在了预置设备上一样使用管理服务器。

在从付费 Amazon 系统映像（AMI）（AWS 中）或基于使用的按月付费 SKU（Azure 中）部署的 Kaspersky Security Center 中，“漏洞和补丁管理”（包括与 SIEM 系统的整合）被自动激活；移动设备管理无法被激活。

管理服务器与管理控制台一起安装。Kaspersky Security for Windows Server 也自动安装到管理服务器设备。

您可以使用以下配置云环境向导配置 Kaspersky Security Center，考虑到在云环境中工作的具体情况。

情景：在云环境中部署

本节介绍 Kaspersky Security Center 的部署以在 Amazon Web Services、Microsoft Azure 和 Google Cloud 等云环境中工作。

在部署方案完成后，Kaspersky Security Center 管理服务器和管理控制台将启动并以默认参数配置。由 Kaspersky Security Center 管理的反病毒保护将会部署到所选 Amazon EC2 实例或 Microsoft Azure 虚拟机。然后您可以调整 Kaspersky Security Center 的配置，创建管理组复杂结构和为组创建不同的策略和任务。

在云环境中部署 Kaspersky Security Center 包含以下步骤：

1. 准备工作
2. 部署管理服务器
3. 安装 Kaspersky 反病毒应用程序到需要被保护的虚拟设备

4. 配置更新下载设置

5. 配置设置以管理设备保护状态报告

配置云环境向导旨在执行初始化配置。第一次从现成映像部署 Kaspersky Security Center 时，它将自动启动。您可以随时手动启动该向导。此外，您可以手动运行它执行的所有操作。

我们建议您至少分配一小时用于在云环境中部署 Kaspersky Security Center 管理服务器，以及至少一个工作日用于保护在云环境中的部署。

在云环境中部署 Kaspersky Security Center 分步骤进行：

1. **计划云段配置**

   学习 Kaspersky Security Center 如何在云环境中工作。计划将在何处部署管理服务器（云环境内部还是外部），并确定计划保护多少个云段。如果您计划在云环境外部部署管理服务器，或者如果您计划保护超过 5000 台设备，您将需要手动安装管理服务器。

   要使用 Google Cloud，只能手动安装管理服务器。

2. **计划资源**

   确保您具有部署所需的一切。

3. **订阅 Kaspersky Security Center 现成镜像**

   在 AWS Marketplace 选择现成 AMI 之一，或在 Azure 市场选择基于使用情况按月付费的 SKU，如有必要，根据 Marketplace 规则支付（或使用 BYOL 模型），然后使用该镜像部署安装了 Kaspersky Security Center 的 Amazon EC2 实例/Microsoft Azure 虚拟机。

   该步骤仅在您计划部署管理服务器到云环境中的实例 / 虚拟机上，且您计划为不超过 5000 台设备部署保护时是必要的。否则该步骤不是必要的，而您必须手动安装管理服务器、管理控制台和 DBMS。

   此步骤不可用于 Google Cloud。

4. **决定 DBMS 的位置**

   决定您的 DBMS 的位置。

   如果您计划在云环境外部使用数据库，确保您拥有工作数据库。

   如果您计划使用 Amazon Relational Database Service (RDS)，请在 AWS 云环境中使用 RDS 创建数据库。

   如果您计划使用 Microsoft Azure SQL DBMS，请在 Microsoft Azure 云环境中使用 Azure 数据库服务创建数据库。

   如果您计划使用 Google MySQL，请在 Google Cloud 中创建数据库（有关详细信息，请参见 https://cloud.google.com/sql/docs/mysql）。

5. **将管理服务器和管理控制台（基于 Microsoft Management Console 和/或基于 Web 的控制台）手动安装到所选设备**

   安装管理服务器、管理控制台和 DBMS 到所选设备，如 Kaspersky Security Center 主要安装方案所述。

   该步骤在您计划放置管理服务器到云环境外，或您计划为超过 5000 台设备部署保护时是必要的。然后，确保您的管理服务器符合硬件要求。否则该步骤不必要，并且 AWS Marketplace、Azure 市场或 Google Cloud 中现成镜像形式的 Kaspersky Security Center 订阅已足够。

6. **确保管理服务器具有使用云 API 的权限**

   在 AWS 中，转到 AWS 管理控制台并创建一个 IAM 角色或者一个 IAM 用户账户。创建的 IAM 角色（或 IAM 用户账户）将允许 Kaspersky Security Center 使用 AWS API：轮询云段并部署保护。

   在 Azure，创建一个订阅和一个带有密码的应用程序 ID。Kaspersky Security Center 使用这些凭证以使用 Azure API：轮询云段和部署保护。

在 Google Cloud 中，注册一个项目，获取您的项目 ID 和私钥。Kaspersky Security Center 使用这些凭据通过 Google API 轮询云段。

7 为受保护实例（仅 AWS）创建 IAM 角色

在 AWS 管理控制台，创建一个 IAM 角色，以定义执行对 AWS 的请求的权限集。新创建的角色将被后续分配到新实例。IAM 角色用于使用 Kaspersky Security Center 安装应用程序到实例。

8 使用 Amazon Relational Database Service 或 Microsoft Azure SQL 准备数据库

如果您计划使用 Amazon Relational Database Service（RDS），创建一个 Amazon RDS 数据库实例和一个要备份数据库的 S3 bucket。如果您想让数据库位于管理服务器所在 EC2 实例，或者如果您想让数据库位于其他地方，您可以跳过此步骤。

如果您计划使用 Microsoft Azure SQL，在 Microsoft Azure 中创建一个存储账户和一个数据库。

如果您计划使用 Google MySQL，请在 Google Cloud 中配置您的数据库（有关详细信息，请参见 https://cloud.google.com/sql/docs/mysql）。

9 授权 Kaspersky Security Center 以在云环境中使用

要确保您已授权Kaspersky Security Center 使用云环境并提供激活码或密钥文件以便应用程序可以添加其到授权许可存储。这个阶段可以在配置云环境期间完成。

如果您正使用从基于 BYOL 模型的免费现成 AMI 安装的 Kaspersky Security Center，或者如果您正手动安装 Kaspersky Security Center 而不使用 AMI，该步骤是需要的。这些情况下，您将需要 Kaspersky Security for Virtualization 授权许可或者 Kaspersky Hybrid Cloud Security 授权许可以激活 Kaspersky Security Center。

如果您正使用从现成镜像安装的 Kaspersky Security Center，该步骤不是必须的，且对应的配置云环境向导窗口不被显示。

10 在云环境中授权

向 Kaspersky Security Center 提供 AWS、Azure 或 Google Cloud 凭据，以便 Kaspersky Security Center 可以使用必要权限操作。这个阶段可以在在云环境中授权期间完成。

11 轮询云段以便管理服务器可以接收云段中设备的信息

启动云段轮询。在 AWS 环境中，Kaspersky Security Center 将接收可以基于 IAM 角色或 IAM 用户权限访问的所有实例的地址和名称。在 Microsoft Azure 环境中，Kaspersky Security Center 将接收可以基于阅读者权限访问的所有虚拟机的地址和名称。

然后您可以使用 Kaspersky Security Center 在检测到的实例或虚拟机上安装 Kaspersky 应用程序和其他供应商的软件。

Kaspersky Security Center 定期启动轮询，这意味着新实例或虚拟机将被自动检测出。

12 组合所有网络设备到云管理组

移动所有发现的实例或虚拟机到**受管理设备\云**管理组，以便它们可以集中进行管理。如果您要将设备分配到子组，例如，根据在它们之上安装的操作，您可以在**受管理设备\云**组中创建几个管理组。您可以启用将常规轮询中检测到的所有设备自动移动到**受管理设备\云**组。

13 使用网络代理连接网络设备到管理服务器

安装网络代理到云环境中的设备。网络代理是为设备与管理服务器之间提供通信的 Kaspersky Security Center 组件。网络代理设置默认被自动配置。

您可以在每个设备本地安装网络代理。您也可以使用 Kaspersky Security Center 远程安装网络代理到设备。或者，您可以跳过该步骤并与最新版本的安全应用程序一并安装网络代理。

14 安装安全应用程序的最新版本到网络设备

选择要安装安全应用程序的设备，然后在这些设备上安装最新版本的安全应用程序。您可以在管理服务器上使用 Kaspersky Security Center 执行远程安装或执行本地安装。

您可能需要手动为这些程序创建安装包。

Kaspersky Endpoint Security for Linux 用于运行 Linux 的实例和虚拟机。

Kaspersky Security for Windows Server 用于运行 Windows 的实例和虚拟机。

15. **配置更新设置**

当您启动配置云环境时，**查找漏洞和所需更新**任务被自动创建。您也可以手动创建任务。该任务自动查找和下载所需应用程序更新以便后续使用 Kaspersky Security Center 工具安装到网络设备。

建议在云环境配置完成后完成以下步骤：

1. **配置报告管理**

   您可以在**管理服务器**节点工作区的**监控**选项卡查看报告。您还可以通过电子邮件接收报告。**监控**选项卡中的报告默认可用。要配置通过电子邮件接收报告，请指定应接收报告的电子邮件地址，然后配置报告格式。

结果

该方案完成后，您可以确保初始化配置是成功的：

- 您可以通过管理控制台或 Kaspersky Security Center Web Console 连接到管理服务器。
- Kaspersky 安全应用程序的最新版本被安装并运行在受管理设备。
- Kaspersky Security Center 已为所有受管理设备创建了默认策略和任务。

在云环境中部署 Kaspersky Security Center 的先决条件

在 Amazon Web Services 或 Microsoft Azure 云环境中部署 Kaspersky Security Center 之前，确保您具有以下：

- 互联网访问
- 以下账户之一：
  - Amazon Web Services 账户（用于使用 AWS）
  - Microsoft 账户（用于使用 Azure）
  - Google 账户（用于使用 Google Cloud）
- 以下之一：
  - Kaspersky Security for Virtualization 的授权许可
  - Kaspersky Hybrid Cloud Security 的授权许可
  - 购买此类授权许可的资金（Kaspersky Security for Virtualization 或 Kaspersky Hybrid Cloud Security）
  - 在 Azure 市场支付现成镜像的基金
- 最新版本 Kaspersky Endpoint Security for Linux 和 Kaspersky Security for Windows Server 的指南

云环境中管理服务器的硬件要求

对于云环境中的部署，管理服务器和数据库服务器的要求与物理管理服务器的要求相同（取决于要管理的设备数量）。有关详细信息，请参阅云环境的文档。

云环境中的授权许可选项

使用云环境是 Kaspersky Security Center 基本功能之外的功能，因此需要专用授权许可。

两个 Kaspersky Security Center 授权许可选项可用于云环境：

- 付费 AMI（在 Amazon Web Services 中）或基于使用量的按月付费 SKU（在 Microsoft Azure 中）。

  这授予 Kaspersky Security Center 的授权许可以及 Kaspersky Endpoint Security for Linux 和 Kaspersky Security for Windows Server 的授权许可。您必须按照所使用的云环境的规则进行支付。

  这个模型允许您对一个管理服务器拥有不超过 200 台客户端设备。

- 一个使用专有授权许可的免费、现成镜像，根据 Bring Your Own License (BYOL) 模型。

  对于在 AWS 或 Azure 中的 Kaspersky Security Center 授权，您必须拥有以下应用程序之一的授权许可：

  - Kaspersky Security for Virtualization
  - 卡巴斯基混合云安全

  BYOL 模型允许最多 100,000 台客户端设备对应一个管理服务器。该模型也允许您管理 AWS、Azure 或 Google 环境之外的设备。

  您可以在以下任一情况下选择 BYOL 模型：

  - 您已经拥有 Kaspersky Security for Virtualization 的有效授权许可。
  - 您已经拥有 Kaspersky Hybrid Cloud Security 的有效授权许可。
  - 您要在部署 Kaspersky Security Center 之前购买授权许可。

  在初始化设置阶段，Kaspersky Security Center 提示您提供激活码或密钥文件。

  如果您选择 BYOL，您将不需要支付通过 Azure 市场或 AWS Marketplace 使用 Kaspersky Security Center 的费用。

两种情况下，漏洞和补丁管理被自动激活，且移动设备管理无法被激活。

如果在尝试使用卡巴斯基混合云安全的授权许可激活云环境的功能支持时发生错误，请使用密钥文件。

订阅到 Kaspersky Security Center 时，您获取 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 Kaspersky Security Center 管理服务器 Microsoft Azure 虚拟机。Kaspersky Security for Windows Server 和 Kaspersky Endpoint Security for Linux 的安装包在管理服务器上可用。您可以安装这些应用程序到云环境中的设备。您不必授权这些应用程序。

如果受管理设备超过一星期对管理服务器不可见，该设备上的应用程序（Kaspersky Security for Windows Server 或 Kaspersky Endpoint Security for Linux）将切换到受限功能模式。要再次激活应用程序，您将必须使安装应用程序的设备对管理服务器再次可见。

在云环境中工作的数据库选项

您必须拥有数据库以使用 Kaspersky Security Center。在 AWS、Microsoft Azure 或 Google Cloud 中部署 Kaspersky Security Center 时，有三个选项：

- 在管理服务器设备创建本地数据库。Kaspersky Security Center 使用支持 5000 台受管理设备的 SQL Server Express 数据库。如果 SQL Server Express 版本足够用则选择该选项。
- 在 AWS 云环境中使用 Relational Database Service (RDS) 创建数据库，或者在 Microsoft Azure 云环境中使用 Azure 数据库服务区创建数据库。如果您想使用 DBMS 数据库而不是 SQL Express 则选择该选项。您的数据将被传输到云环境以保存，您将没有任何多余花费。如果您已经预先使用了 Kaspersky Security Center 并在您的数据库中拥有一些数据，您可以传输您的数据到新数据库。

  要在 Google Cloud Platform 上工作，只能使用 Cloud SQL for MySQL。
- 使用现有数据库服务器。如果您已经拥有数据库服务器且想将其用于 Kaspersky Security Center，请选择该选项。如果该服务器位于云环境之外，您的数据将通过互联网传输，这将导致多余花费。

Kaspersky Security Center 在云环境中的部署过程具有创建（选择）数据库的特殊步骤。

使用 Amazon Web Services 云环境

该部分提供了使用 Kaspersky Security Center 在 Amazon Web Services 中工作的步骤。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

关于使用 Amazon Web Services 云环境

您可以在 AWS Marketplace 购买 Amazon 系统映像 (AMI) 格式的 Kaspersky Security Center，它是一个现成的预配置的虚拟机镜像。您可以订阅付费 AMI 或 BYOL AMI，并基于该镜像创建员服务器安装了 Kaspersky Security Center 管理服务器的 Amazon EC2 实例。

要使用 AWS 平台，特别是在 AWS Marketplace 购买应用并创建实例，您需要一个 Amazon Web Services 账户。您可以在 https://aws.amazon.com/cn 创建免费账户。您也可以使用现有 Amazon 账户。

如果您在 AWS Marketplace 订阅了可用的 AMI，您接收带有现成 Kaspersky Security Center 的实例。您不必自己安装应用程序。这种情况下，Kaspersky Security Center 管理服务器将安装在实例上，无需您介入。安装后，您可以启动管理控制台并连接到管理服务器以开始使用 Kaspersky Security Center。

关于更多 AMI 和 AWS Marketplace 如何工作的详情，请访问 AWS Marketplace 帮助页面。对于更多使用 AWS 平台、使用实例和相关概念的信息，请参考 Amazon Web Services 文档。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

为 Amazon EC2 实例创建 IAM 角色和 IAM 用户账户

该部分描述了为了确保管理服务器的正确运行而必须执行的操作。这些操作包括使用 AWS 身份和 Access Management (IAM) 角色和用户账户。还描述了为了在客户端设备上安装网络代理和 Kaspersky Security for Windows Server 以及 Kaspersky Endpoint Security for Linux 而必须执行的操作。

确保 Kaspersky Security Center 管理服务器具有使用 AWS 的权限

Amazon Web Services 云环境中的操作标准规定了一个分配到管理服务器实例以使用 AWS 服务的特别 IAM 角色。IAM 角色是一个 IAM 实体，定义执行到 AWS 服务的请求的权限集的 IAM 实体。IAM 角色提供云段轮询和安装应用程序到实例的权限。

在您创建 IAM 角色并分配其到管理服务器后，您将可以使用该角色部署实例的保护，而不提供任何附加信息到 Kaspersky Security Center。

然而，可能建议您不要在以下情况下为管理服务器创建 IAM 角色：

- 您计划管理保护的设备是 Amazon Web Services 云环境中的 EC2 实例，但是管理服务器位于环境之外。
- 您计划管理不仅您云段中的实例，而且还有使用不同 AWS 账户创建的其他云段中的实例的保护。此种情况下，您将仅需要用于您云段的保护的 IAM 角色。IAM 角色将不被需要以保护其他云段。

此些情况下，不是创建 IAM 角色，您将需要创建 Kaspersky Security Center 用以使用 AWS 服务的 *IAM 用户账户*。在开始使用管理服务器之前，创建带有 *AWS IAM 访问密钥*(也叫 *IAM 访问密钥*)的 IAM 用户账户。

IAM 角色或 IAM 用户账户的创建需要 AWS 管理控制台。要使用 AWS 管理控制台，您将需要 AWS 账户的用户名和密码。

为管理服务器创建 IAM 角色

在您部署管理服务器之前，在 AWS 管理控制台创建带有安装应用程序到实例所需权限的 IAM 角色。有关详细信息，请参阅 AWS 帮助中关于 IAM 角色的部分。

要为管理服务器创建 IAM 角色：

1. 打开 AWS 管理控制台并使用您的 AWS 账户登录。
2. 在“**角色**”区域中，创建一个具有以下权限的角色：
   - **AmazonEC2ReadOnlyAccess**，如果您计划仅运行云段轮询而不打算使用 AWS API 在 EC2 实例中安装应用程序。
   - **AmazonEC2ReadOnlyAccess** 和 **AmazonSSMFullAccess**，如果您计划运行云段查询并使用 AWS API 安装应用程序到 EC2 实例。此种情况下，您将需要分配带有 AmazonEC2RoleforSSM 权限的 IAM 角色到受保护的 EC2 实例。

您将需要分配该角色到用作管理服务器的 EC2 实例。

新创建的角色可用于管理服务器上的所有应用程序。因此，任何运行在管理服务器上的应用程序都能轮询云段或安装应用程序到云段中的 EC2 实例。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

创建 IAM 用户账户以使用 Kaspersky Security Center

如果管理服务器未被分配带有设备发现和安装应用程序到实例的权限的 IAM 角色，则需要 IAM 用户账户以使用 Kaspersky Security Center。相同账户，或者不同账户，如果您使用 S3 bucket，也被管理服务器数据备份任务所需。您可以创建带有所有必要权限的 IAM 用户账户，或者您可以创建两个不同的用户账户。

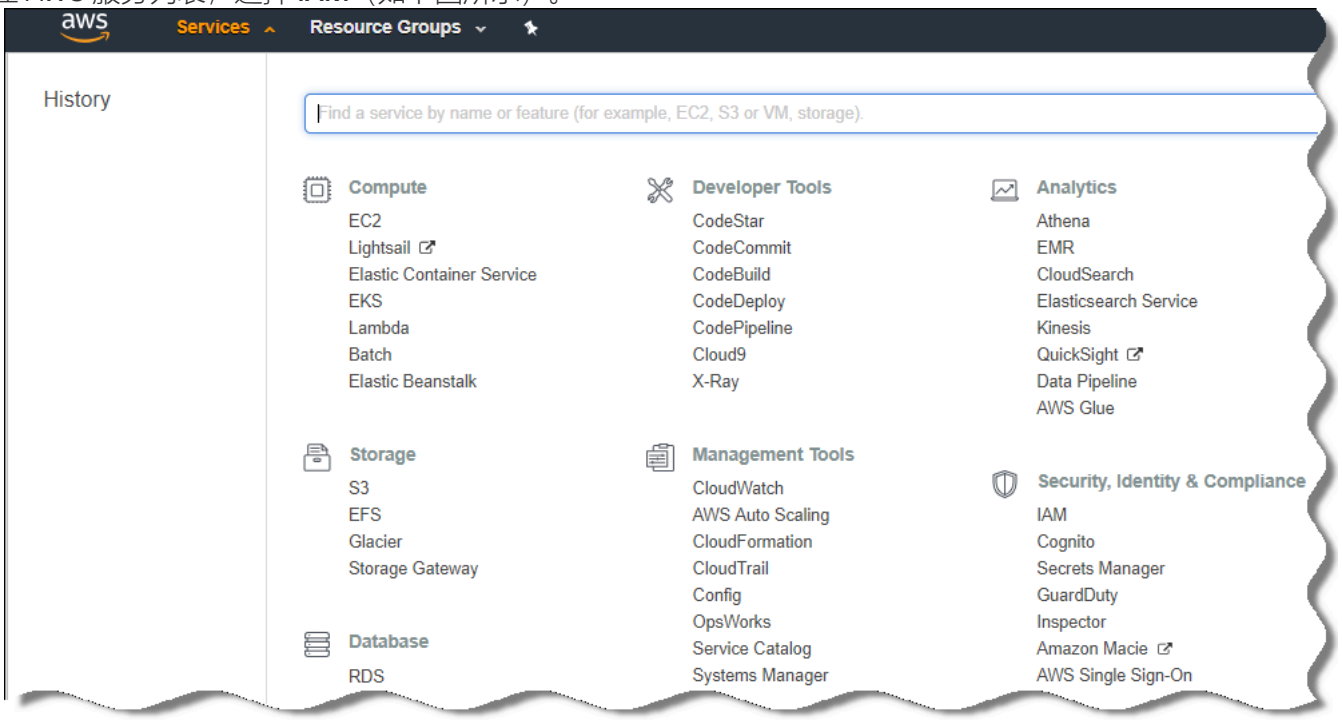
初始化配置过程中您需要提供给 Kaspersky Security Center 的 *IAM 访问密钥*为 IAM 用户自动创建。IAM 访问密钥由访问密钥 ID 和 secret key 组成。关于更多 IAM 服务的详情，请参考以下 AWS 参考页面：

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html。
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2。

要创建带有必要权限的 IAM 用户账户：

1. 打开 AWS 管理控制台 并使用您的账户登录。

2. 在 AWS 服务列表，选择 **IAM**（如下图所示）。



AWS 管理控制台中的服务列表

包含用户名列表和工具使用菜单的窗口打开。

3. 在用户账户相关区域导航，并添加新用户名或名字。

4. 对于添加的用户，指定以下 AWS 属性：

   - 访问类型：**编程访问**。
   - 未设置权限边界。
   - 权限：
     - **ReadOnlyAccess**—如果您计划仅运行云段查询而不计划使用 AWS API 安装应用程序到 EC2 实例。
     - **ReadOnlyAccess** 和 **AmazonSSMFullAccess**—如果您计划运行云段查询并使用 AWS API 安装应用程序到 EC2 实例。此种情况下，您将必须分配带有AmazonEC2RoleforSSM 权限的 IAM 角色到受保护的 EC2 实例。

   您添加权限后，精确查看它们。一旦选择错误，返回上一个界面并再次做出选择。

5. 您创建用户账户后，包含新 IAM 用户的 IAM 访问密钥的表格将出现。访问密钥 ID 显示在**访问密钥 ID**列。Secret key 以星号显示在**秘密访问密钥**列。要查看 secret key，点击**显示**。

新创建的账户显示在对应于您的 AWS 账户的 IAM 用户账户列表。

当在云段中部署 Kaspersky Security Center 时，您必须指定您正在使用 IAM 用户账户并提供访问密钥 ID 和 secret key 给 Kaspersky Security Center。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

为安装应用程序到 Amazon EC2 实例创建 IAM 角色

在您使用 Kaspersky Security Center 在 EC2 实例上开始保护部署之前，在 AWS 管理控制台 创建一个具有安装应用程序到实例所需权限的 IAM 角色。有关详细信息，请参阅 AWS 帮助中关于 IAM 角色 的部分。

IAM 角色是必需的，因此您可以分配它到所有您要使用 Kaspersky Security Center 安装安全应用程序的 EC2 实例。如果您不分配给实例具有必要权限的 IAM 角色，使用 AWS API 工具安装应用程序到该实例将导致错误。

要使用 AWS 管理控制台，您将需要 AWS 账户的用户名和密码。

为安装应用程序到实例创建 IAM 角色：

1. 打开 AWS 管理控制台 并使用您的 AWS 账户登录。
2. 在左侧菜单中，选择“**Roles**”。
3. 单击“**Create Role**”按钮。
4. 在出现的服务列表中，选择 **EC2**，然后在“**Select Your Use Case**”列表中再次选择 **EC2**。
5. 单击“**Next: Permissions**”按钮。
6. 在打开的列表中，选择 **AmazonEC2RoleforSSM** 旁边的复选框。
7. 单击“**Next: Review**”按钮。
8. 为 IAM 角色输入名称和描述并点击“**Create Role**”按钮。
   您创建的角色出现在角色列表，显示您输入的名称和描述。

然后，您可以使用新创建的 IAM 角色创建新的您要通过 Kaspersky Security Center 保护的 EC2 实例，以及使用现有实例进行关联。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

使用 Amazon RDS

该部分描述了必须采取哪些操作以为 Kaspersky Security Center 准备 Amazon Relational Database Service (RDS) 数据库，放置其到选项组，创建 IAM 角色以使用 RDS 数据库，准备 S3 bucket 以存储，和迁移现有数据库到 RDS。

Amazon RDS 是帮助 AWS 用户在 AWS 云环境中设置、操作和测量关系数据库的 Web 服务。如果您想，您可以使用 Amazon RDS 数据库以配合使用 Kaspersky Security Center。

您可以使用以下数据库：

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- 标准 MySQL 5.7

创建 Amazon RDS 实例

如果您要使用 Amazon RDS 作为 DBMS，您必须创建 Amazon RDS 数据库实例。本节介绍如何选择 SQL Express Edition；如果要使用 Aurora MySQL 或标准 MySQL（版本 5.7、8.0），则必须选择这些引擎之一。

要创建 Amazon RDS 数据库实例：

1. 在 https://console.aws.amazon.com 打开 AWS 管理控制台并使用您的账户登录。
2. 使用 AWS 界面，用以下设置创建数据库：
   - 引擎：Microsoft SQL Server、SQL Express 版本
   - DB 引擎版本：SQL Server 2014 12.00.5546.0v1
   - DB 实例类：db.t2.medium
   - 存储类型：常规目的
   - 分配的存储：最小 50 GiB
   - 安全组：Kaspersky Security Center 管理服务器 EC2 实例所在组

   为 RDS 实例创建标识符、用户名和密码。

   您可以在其他所有字段保留默认设置。或者，如果您要自定义您的 Amazon RDS 实例，则更改默认设置。要获得帮助，请参考 AWS 信息页面。
3. 在最后一步，AWS 显示进程结果。如果您要查看您的 Amazon RDS 实例的详情，请单击**查看 DB 实例详情**。如果您要继续操作，开始为您的 Amazon RDS 实例创建选项组。

新 Amazon RDS 实例的创建可能花费几分钟。实例被创建后，您可以利用其使用 Kaspersky Security Center 数据。

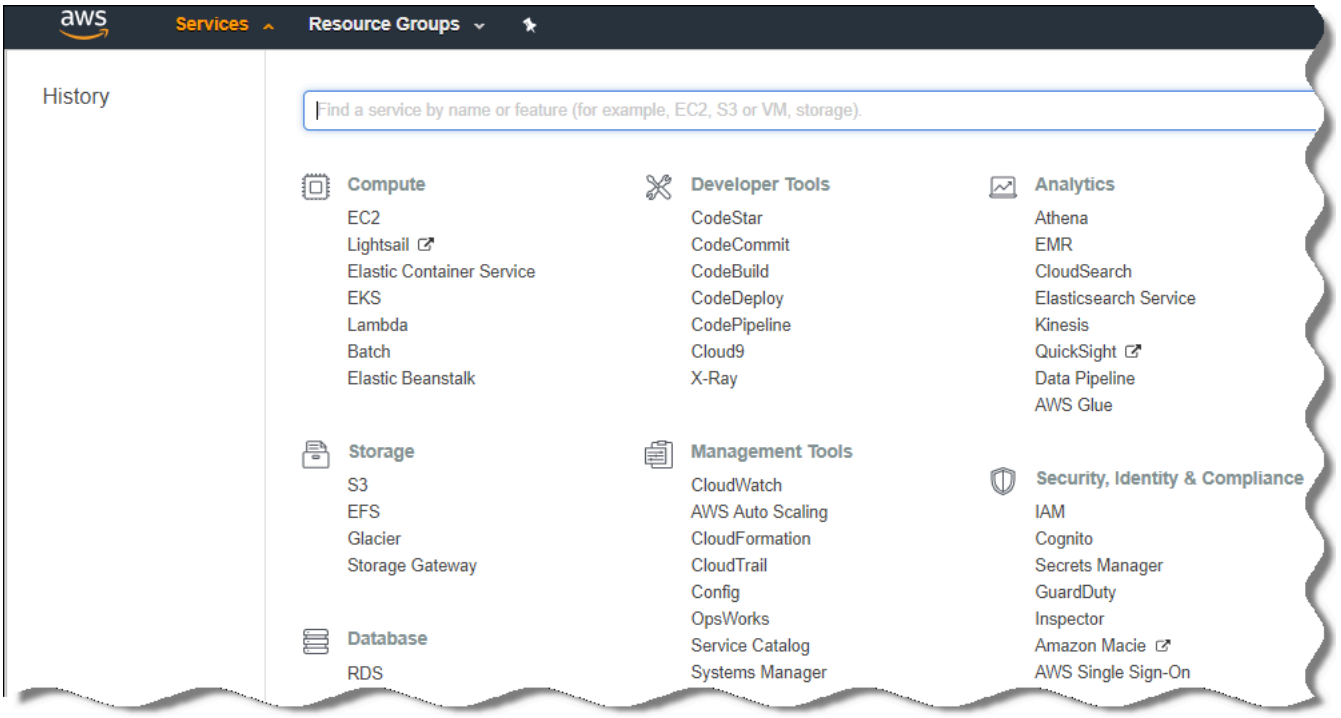
截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

为 Amazon RDS 实例创建选项组

您需要放置您的 Amazon RDS 实例到选项组。

要为您的 Amazon RDS 实例创建选项组：

1. 确保您在 AWS 管理控制台（https://console.aws.amazon.com）且以您的账户登录。
2. 在菜单中，点击**服务**。
   可用服务列表出现（参见下图）。



AWS 管理控制台中的服务列表

3. 在列表中，点击 **RDS**。
4. 在左侧窗格，点击**选项组**。
5. 单击“**创建组**”按钮。
6. 如果您在创建 Amazon RDS 实例阶段选择 SQL Server，使用以下设置创建选项组：
   - 引擎：SQLserver-ex
   - 主引擎版本：12.00

   如果您在创建 Amazon RDS 实例阶段选择不同 SQL 数据库，那么选择对应的引擎。

群组被创建并显示在您的群组列表。

在创建选项组后，放置您的 Amazon RDS 实例到选项组。

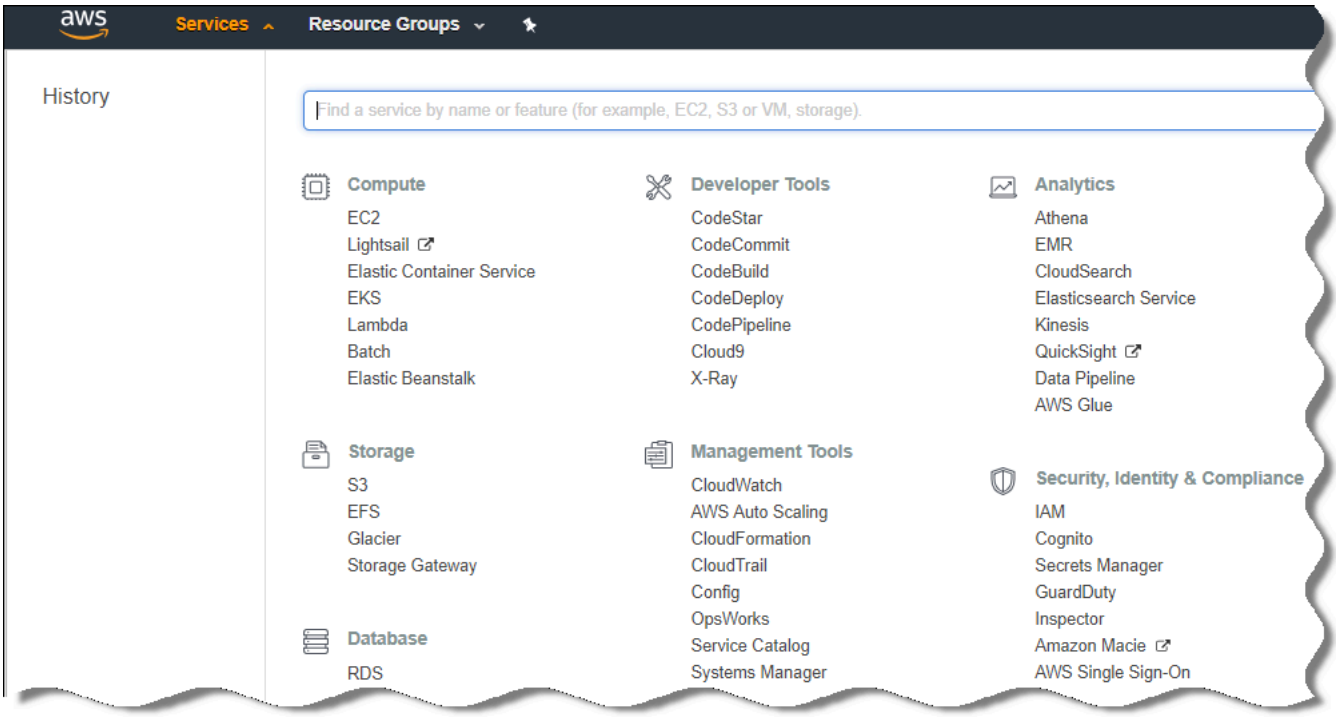
截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

修改选项组

您放置 Amazon RDS 实例的选项组的默认配置不足以使用 Kaspersky Security Center 数据库。您必须添加选项到选项组并创建新 IAM 角色以使用数据库。

要修改选项组并创建新 IAM 角色：

1. 确保您在 AWS 管理控制台（https://console.aws.amazon.com）且以您的账户登录。
2. 在菜单中，点击**服务**。
   可用服务列表出现（参见下图）。



AWS 管理控制台中的服务列表

3. 在列表中，选择 RDS。
4. 在左侧窗格，点击**选项组**。
   选项组列表被显示。
5. 选择您放置您的 Amazon RDS 实例的选项组并点击**添加选项**按钮。
   "**添加选项**"窗口将打开。
6. 在 IAM 角色区域，选择**创建新角色 / 是**选项并输入新 IAM 角色的名称。
   角色使用默认权限集创建。稍后，您将必须更改它的权限。
7. 在 S3 bucket 区域，做以下之一：
   - 如果您没有为数据备份创建 Amazon S3 bucket 实例，选择"**创建新 S3 bucket**"连接并使用 AWS 界面创建新 S3 bucket。
   - 如果您已经为管理服务器数据备份任务创建了 Amazon S3 bucket 实例，从下拉列表选择您的 S3 bucket。
8. 通过点击页面下方的**添加选项**按钮结束添加选项。

您已修改了选项组并创建了新 IAM 角色以使用 RDS 数据库。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

为 IAM 角色修改权限以使用 Amazon RDS 数据库实例

在您添加选项到选项组之后，您必须分配所需权限到您创建的 IAM 角色以使用 Amazon RDS 数据库实例。

要分配所需权限到您创建的 IAM 角色以使用 Amazon RDS 数据库实例：

1. 确保您在 AWS 管理控制台（https://console.aws.amazon.com）且以您的账户登录。
2. 在服务列表中，选择 **IAM**。
   包含用户名列表和工具使用菜单的窗口打开。
3. 在菜单中选择**角色**。
4. 在工作区中显示的 IAM 角色列表，选择您在添加选项到选项组时创建的角色。
5. 使用 AWS 界面，删除 **sqlNativeBackup-<日期>** 策略。
6. 使用 AWS 界面，附加 **AmazonS3FullAccess** 策略到角色。

IAM 角色被分配所需权限以使用 Amazon RDS。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

为数据库准备 Amazon S3 bucket

如果您计划使用 Amazon Relational Database System (Amazon RDS) 数据库，您必须创建保存数据库常规备份的 Amazon Simple Storage Service (Amazon S3) bucket 实例。对于 Amazon S3 和 S3 buckets 的信息，请参考 Amazon 帮助页面。对于创建 Amazon S3 实例的更多信息，请参考 Amazon S3 帮助页面。

要创建 Amazon S3 bucket：

1. 确保 AWS 管理控制台被打开且您已以您的账户登录。
2. 在 AWS 服务列表中，选择 S3。
3. 在控制台中导航以创建 bucket，遵循向导的以下说明。
4. 选择您的管理服务器所在（或将在）的相同区域。
5. 当向导结束时，确保新 bucket 出现在 bucket 列表。

新 S3 bucket 被创建并出现在您的 bucket 列表。当添加选项到选项组时，您必须指定该 bucket。当 Kaspersky Security Center 正在创建*管理服务器数据备份*任务时，您将必须指定您的 S3 bucket 地址给 Kaspersky Security Center。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

迁移数据库到 Amazon RDS

您可以从预置设备迁移您的 Kaspersky Security Center 数据到支持 Amazon RDS 的 Amazon S3 实例。为此，您需要 RDS 数据库的 S3 bucket 和此 S3 bucket 的 带有 AmazonS3FullAccess 权限的 IAM 用户账户。

要执行数据库迁移：

1. 确保您已创建了 RDS 实例（参考 Amazon RDS 参考页面以获得更多信息）。
2. 在您的预置物理管理服务器上，运行 Kaspersky 备份实用程序以备份管理服务器数据。
   您必须确保该文件名为 backup.zip。
3. 复制 backup.zip 文件到安装了管理服务器的 EC2 实例。

   确保您在管理服务器 EC2 实例上有足够磁盘空间。在 AWS 环境中，您可以添加更多的磁盘空间到您的实例以容纳数据库迁移。

4. 在 AWS 管理服务器，以交互模式启动 Kaspersky 备份实用程序。
   这样将启动备份和恢复向导。
5. 在**选择操作**步骤，选择**恢复管理服务器数据**并点击**下一步**。
6. 在“**恢复设置**”步骤，单击“**存储备份副本的文件夹**”旁边的“**浏览**”按钮。
7. 在打开的“**登录到在线存储**”窗口，填充以下字段然后单击“**OK**”：
   - **S3 bucket 名称**

     您的 S3 bucket 名称。
   - **备份文件夹**

     指定用于备份的存储文件夹位置。
   - **访问密钥 ID**

     属于具有使用 S3 bucket 的权限（AmazonS3FullAccess 权限）的 IAM 用户的 AWS IAM 访问密钥 ID。
   - **Secret key**

     属于具有使用 S3 bucket 的权限（AmazonS3FullAccess 权限）的 IAM 用户的 AWS IAM secret key。
8. 选择**从本地备份迁移**选项。**浏览**按钮变得可用。

9. 单击“**浏览**”按钮在 AWS 管理服务器上选择复制了 backup.zip 的文件夹。

10. 点击**下一步**并完成过程。

您的数据将使用您的 S3 bucket 恢复到 RDS 数据库。您可以使用该数据库以便进一步在 AWS 环境中使用 Kaspersky Security Center。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

工作在 Microsoft Azure 云环境

该部分提供了 Kaspersky Security Center 在 Microsoft Azure 提供的云环境的部署和维护信息，以及在云环境中的虚拟机上的保护部署详情。

在从基于使用的按月付费 SKU 部署的 Kaspersky Security Center 中，“漏洞和补丁管理”被自动激活，且“移动设备管理”无法被激活。

关于使用 Microsoft Azure

要使用 Microsoft Azure 平台，特别是要在 Azure 市场购买应用并创建虚拟机，您将需要一个 Azure 订阅。在您部署管理服务器之前，创建带有安装应用程序到虚拟机所需权限的 Azure 应用程序 ID。

如果您在 Azure 市场购买 Kaspersky Security Center 镜像，您可以使用您的现成 Kaspersky Security Center 管理服务器部署虚拟机。要必须选择虚拟机设置，但是您不必自己安装应用程序。安装后，您可以启动管理控制台并连接到管理服务器以开始使用 Kaspersky Security Center。

您也可以使用部署了 Kaspersky Security Center 管理服务器的 Azure 虚拟机以保护预置设备（例如，如果云服务器比物理机更容易服务和维护）。如果是这种情况，您像管理服务器安装在了预置设备上一样使用管理服务器。如果您不计划使用 Azure API 工具，您不需要 Azure 应用程序 ID。此种情况下，Azure 订阅已足够。

创建订阅、应用程序 ID 和密码

要在 Microsoft Azure 环境中使用 Kaspersky Security Center，您需要一个 Azure 订阅、Azure 应用程序 ID 和 Azure 应用程序密码。您可以使用现有订阅，如果您已经拥有。

Azure 订阅授予其所有者到 Microsoft Azure Platform Management Portal 和 Microsoft Azure 服务的访问权限。所有者可以使用 Microsoft Azure Platform 以管理服务，例如 Azure SQL 和 Azure Storage。

要创建 Microsoft Azure 订阅，

转到https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription并按照那里的说明进行操作。

关于创建订阅的更多信息在 Microsoft 网站 可用。您将获得订阅 ID，您将稍后将其与应用程序 ID 和密码一起提供给 Kaspersky Security Center。

要创建和保存 Azure 应用程序 ID 和密码，

1. 转到 https://portal.azure.com 并确保您已登录。
2. 遵照参考页面的说明，创建您的应用程序 ID。
3. 转到应用程序设置的**密钥**区域。
4. 在**密钥**区域，填充**描述**和**过期**字段并置**参数值**字段为空。
5. 点击**保存**。

   当您点击“**保存**”，系统自动使用一个长字符序列填充**参数值**字段。该序列是您的 Azure 应用程序密码（例如，yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=）。描述在您输入时被显示。
6. 复制密码并保存，以便您可以稍后提供应用程序 ID 和密码到 Kaspersky Security Center。

   您仅可以在密码被创建时复制它。稍后，密码不再被显示且您无法恢复它。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

分配角色到 Azure 应用程序 ID

如果您仅想使用设备发现检测虚拟机，您的 Azure 应用程序 ID 必须具有阅读者角色。如果您不仅要检测虚拟机，还想部署保护到虚拟机，您的 Azure 应用程序 ID 必须具有虚拟机创建者角色。

按照 Microsoft 网站上的说明分配角色到您的 Azure 应用程序 ID。

在 Microsoft Azure 中部署管理服务器并选择数据库

要在 Microsoft Azure 环境中部署管理服务器：

1. 使用您的账户登录到 Microsoft Azure。
2. 转到 Azure 门户。
3. 在左侧窗格，点击绿色加号。
4. 在菜单中的搜索字段输入“Kaspersky Hybrid Cloud Security”。

   Kaspersky Hybrid Cloud Security 是 Kaspersky Security Center 和两个实例保护安全应用程序的组合：Kaspersky Endpoint Security for Linux 和 Kaspersky Security for Windows Server。
5. 在结果列表中，选择 Kaspersky Hybrid Cloud Security 或 Kaspersky Hybrid Cloud Security (BYOL)。

   在屏幕的右侧，信息窗口出现。
6. 阅读信息并点击信息窗口后面的“创建”按钮。
7. 填充所有必要字段。使用工具提示获得信息和帮助。

8. 当选择大小时，选择三个共享选项之一。

   在多数情况，8 gigabytes (GB) 内存已足够。然而，在 Azure，您可以在任何时候增加内存和虚拟机其他资源的大小。

9. 当选择数据库时，根据您的计划选择以下之一：

   - 本地—如果您想让数据库位于部署管理服务器的虚拟机。Kaspersky Security Center 带有 SQL Server Express 数据库。如果 SQL Server Express 足够用则选择该选项。
   - 新—如果您想在 Azure 环境中使用新 RDS 数据库。如果您想使用 DBMS 数据库而不是 SQL Server Express 则选择该选项。您的数据将被传输到云环境以保存，您将没有任何多余花费。
   - 现有—如果您想使用现有数据库服务器。此种情况下，您将必须指定其位置。如果该服务器位于 Azure 环境之外，您的数据将通过互联网传输，这将导致多余花费。

10. 当输入订阅 ID 时，使用您之前创建的订阅。

    部署之后，您可以通过 RDP 连接到管理服务器。您可以使用管理控制台来操作管理服务器。

使用 Azure SQL

该部门描述了需要采取什么操作以为 Kaspersky Security Center 准备 Microsoft Azure 数据库、准备 Azure 存储账户和迁移现有数据库到 Azure SQL。

SQL 数据库是一个 Microsoft Azure 中的关系数据库管理服务。

> 截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

创建 Azure 存储账户

您必须在 Microsoft Azure 中创建存储账户以使用 Azure SQL 数据库以部署脚本。

要创建存储账户：

1. 登录到 Azure 门户。
2. 在左侧面板，选择**存储账户**以转到**存储账户**窗口。
3. 在**存储账户**窗口，点击**添加**按钮转到**创建存储账户**窗口。
4. 填充必要字段以创建存储账户：

   - 位置：必须和管理服务器位置相同。
   - 其他字段：您可能选择默认值。

   使用工具提示获得每个字段的信息。
   创建存储账户后，您的存储账户列表被显示。

5. 在您的存储账户列表中，点击新创建的账户名称以查看该账户的信息。

6. 确保您知道资源名称、资源组和该存储账户的访问密钥。您将需要该信息以使用 Kaspersky Security Center。

您可以参考 Azure 网站以获得帮助。

如果您已经拥有存储账户，您可以将其用于 Kaspersky Security Center。

创建 Azure SQL 数据库和 SQL Server

您需要 Azure 环境中的 SQL 数据库和 SQL Server。

要创建 Azure SQL 数据库和 SQL Server：

1. 遵照 Azure 网站的说明。

   当 Microsoft Azure 提示您时您可以创建新服务器；如果您已经拥有 Azure SQL Server，您可以将其用于 Kaspersky Security Center，而不用创建新的。

2. 创建 SQL 数据库和 SQL Server 后，确保您知道其资源名称和资源组：

   a. 转到 https://portal.azure.com 并确保您已登录。

   b. 在左边窗格中，选择**SQL 数据库**。

   c. 从您的数据库列表里点击数据库名称。

   属性窗口打开。

   d. 数据库的名称是资源名称。资源组的名称显示在属性窗口的**概述**部分。

您需要数据库的资源名称和资源组以迁移数据库到 Azure SQL。

迁移数据库到 Azure SQL

在管理服务器被部署到 Azure 环境之后，您可以从预置设备迁移您的 Kaspersky Security Center 数据库到 Azure SQL。您需要一个 Azure 存储账户用于 Azure SQL 数据库。您还必须在您的管理服务器上拥有 Microsoft SQL Server Data-Tier Application Framework (DacFx) 和 SQLSysCLRTypes。

要执行数据库迁移：

1. 确保您创建了 Azure 存储账户。

2. 确保您在管理服务器上拥有 SQLSysCLRTypes 和 DacFx。

   您可以从 Microsoft 官方网站下载 Microsoft SQL Server 数据层应用程序框架 (17.0.1 DacFx) 和 SQLSysCLRTypes（选择与您的 SQL Server 版本对应的版本）。

3. 在您的预置物理管理服务器上，运行 Kaspersky 备份实用程序以备份管理服务器数据（启用"**迁移到 Azure 格式**"选项）。

4. 复制备份文件到管理服务器。

> 确保您在管理服务器 Azure 虚拟机上有足够磁盘空间。在 Azure 环境中，您可以添加更多的磁盘空间到您的虚拟机以容纳数据库迁移。

5. 在位于 Microsoft Azure 环境的管理服务器上，再次以交互模式启动 Kaspersky 备份实用工具。
   这样将启动备份和恢复向导。

6. 在**选择操作**步骤，选择**恢复管理服务器数据**并点击**下一步**。

7. 在“**恢复设置**”步骤，单击“**存储备份副本的文件夹**”旁边的“**浏览**”按钮。

8. 在打开的“**登录到在线存储**”窗口，填充以下字段然后单击“**OK**”：

   - **Azure 存储账户名**

     > 您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

   - **备份文件夹**

     > 指定用于备份的存储文件夹位置。

   - **Azure 订阅 ID**

     > 您在 Azure 门户创建了该订阅。

   - **Azure 应用程序密码**

     > 当您创建应用程序 ID 时您收到应用程序 ID 的密码。
     > 密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

   - **Azure 存储访问密钥**

     > 在您的存储账户属性中可用，在访问密钥区域。您可以使用任何密钥（key1 或 key2）。

   - **Azure SQL Server 名称**

     > 在您的 Azure SQL Server 属性中可用。

   - **Azure SQL Server 资源组**

     > 在您的 Azure SQL Server 属性中可用。

- **Azure 应用程序 ID**

  您在 Azure 门户创建了该应用程序 ID。

  您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

9. 选择**从本地备份迁移**选项。

   浏览按钮变得可用。

10. 点击**浏览**按钮在 AWS 管理服务器选择您复制备份文件的文件夹。

11. 点击**下一步**并完成过程。

    您的数据将使用您的 Azure 存储恢复到 Azure SQL 数据库。您可以使用该数据库以便进一步在 Azure 环境中使用 Kaspersky Security Center。

截至 Kaspersky Security Center 发布之日，本文档中引用的网页地址是正确的。

在 Google Cloud 中工作

本节提供有关在 Google 提供的云环境中使用 Kaspersky Security Center 的信息。

创建客户端电子邮件、项目 ID 和私钥

您可以在 Google Cloud Platform 中将 Google API 与 Kaspersky Security Center 配合使用。Google 账户是必需的。有关详细信息，请参阅 https://cloud.google.com 上的 Google 文档。

您将需要创建并向 Kaspersky Security Center 提供以下凭据：

- **客户端电子邮件**

  客户端电子邮件是用于在 Google Cloud 注册项目的电子邮件地址。

- **项目 ID**

  项目 ID 是您在 Google Cloud 注册项目时收到的 ID。

- **私钥**

  私钥是您在 Google Cloud 注册项目时收到的用作私钥的字符序列。最好复制并粘贴此序列，以免出错。

使用 Google Cloud SQL for MySQL 实例

您可以在 Google Cloud 中创建数据库，并将该数据库用于 Kaspersky Security Center。

Kaspersky Security Center 可与 MySQL 5.7 和 5.6 一起使用。其他版本的 MySQL 尚未经过测试。

要创建和配置 MySQL 数据库：

在浏览器中，转到 https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen，然后按照提供的说明进行操作。

配置 MySQL 数据库时，请使用以下标志：

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

在云环境中准备必要的客户端设备以使用 Kaspersky Security Center

要在其上安装管理服务器、网络代理和 Kaspersky 安全应用程序的设备必须满足以下条件：

- 安全组配置使得以下端口在管理服务器上可用（部署所需的最小端口集）：
  - 8060 HTTP—用于从管理服务器传输网络代理安装包和安全应用程序安装包到受保护实例
  - 8061 HTTPS—用于从管理服务器传输网络代理安装包和安全应用程序安装包到受保护实例
  - 13000 TCP—用于使用 SSL 从受保护实例和从属管理服务器传输数据到主管理服务器
  - 13000 UDP—用于传输实例关闭的信息到管理服务器
  - 14000 TCP—用于不使用 SSL 从受保护实例和从属管理服务器传输数据到主管理服务器

- 13291—用于将管理控制台连接至管理服务器
- 40080—用于部署脚本操作

您可以在 AWS 管理控制台或 Azure 门户配置安全组。如果您要以非默认配置使用 Kaspersky Security Center，请参考知识库。非默认配置的例子包括不安装管理控制台到管理服务器设备而是安装到您的工作站，或使用 KSN 代理服务器。

- UDP 端口 15000 在客户端设备上可用（用于在与管理服务器的交互中接收请求）。
- 在 AWS 云环境：
  - 如果您计划使用 AWS API，安装应用程序到实例的 IAM 角色被设置。
  - 在每个 Amazon EC2 实例上，Systems Manager Agent（SSM 代理）被安装且正在运行。
  - SSM 代理启用 Kaspersky Security Center 以自动安装应用程序到设备和设备组，而不是每次都请求管理员确认。
  - 在运行 Windows 操作系统和从晚于 2016 年11月 的 AMIs 部署的实例上，SSM 代理被安装并正在运行。您将必须在所有其他设备上手动安装 SSM 代理。关于更多安装 SSM 代理到运行 Windows 和 Linux 操作系统的设备的详情，请参考 AWS 帮助页面。
- 在 Microsoft Azure 云环境：
  - 在每个 Azure 虚拟机，Azure VM Agent 被安装且正在运行。

    默认下，新虚拟机被创建时带有 Azure VM Agent，且您不必安装或手动启用它。请参考 Microsoft 帮助页面以获得关于在 Windows 设备和在 Linux 设备上的 Azure VM Agent 详情。
  - 您的 Azure 应用程序 ID 具有以下角色：
    - 阅读者（使用网络轮询发现虚拟机）
    - 虚拟机创建者（部署保护到虚拟机）
    - SQL Server 创建者（在 Microsoft Azure 环境中使用 SQL 数据库）

    如果您要执行所有这些操作，请分配所有三个角色到您的 Azure 应用程序 ID。

创建配置云环境所需的安装包

如果您有以下程序的安装包和管理插件，则可以在 Kaspersky Security Center 中使用配置云环境向导：

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  在即将发布的 Kaspersky Endpoint Security 12.0 for Windows 之后，将可以在云环境中部署 Kaspersky Endpoint Security for Windows。
- Kaspersky Security for Windows Server

在要保护的实例或虚拟机上安装应用程序需要这些安装包。如果没有这些安装包，则必须创建它们。否则，配置云环境向导无法工作。

要创建安装包：

1. 在 Kaspersky 网站下载最新版本的应用程序和插件：
   - Kaspersky Security for Windows Server 的安装程序和管理插件。
   - 用于通过 Kaspersky Security Center 进行远程安装的安装程序文件，以及 Kaspersky Endpoint Security for Linux 的管理插件。
2. 将所有文件保存在安装了管理服务器的实例（或虚拟机）上。
3. 从所有安装包中提取文件。
4. 启动 Kaspersky Security Center。
5. 在控制台树中，转到“**高级**”→“**远程安装**”→“**安装包**”，然后单击“**创建安装包**”。
6. 选择“**创建 Kaspersky 安装包**”。
7. 指定安装包的名称和应用程序安装程序的路径：<文件夹>\<文件名>.kud，然后单击“**下一步**”。
8. 阅读最终用户授权许可协议，选中复选框以确认您接受其条款，然后单击“**下一步**”。

安装包将上传到管理服务器，并将在安装包列表中提供。

在管理服务器上创建安装包并安装管理插件后，即可使用配置云环境。

配置云环境

要使用配置云环境向导配置 Kaspersky Security Center，您必须拥有：

- 云环境的特定凭据：
  - 一个被授予轮询云段权限的 IAM 角色或一个被授予轮询云段权限的 IAM 用户账户（用于使用 Amazon Web Services）
  - 一个 Azure 应用程序 ID、密码和订阅（用于使用 Microsoft Azure）
  - Google 客户端电子邮件、项目 ID 和私钥（用于使用 Google Cloud）
- 安装包：
  - Network Agent for Windows
  - Network Agent for Linux
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux 的 Web 插件

- 至少具有以下一种：
  - Kaspersky Endpoint Security for Windows 安装包和 Web 插件（推荐）
  - Kaspersky Security for Windows Server 的安装包和 Web 插件

如果您不想使用云环境功能（例如，如果您仅想要管理物理客户端设备的保护），您可以关闭配置云环境向导并手动运行标准管理服务器快速启动向导。

配置云环境操作在通过管理控制台第一次连接到管理服务器时自动启动，如果您正在从现成镜像部署 Kaspersky Security Center。您还可以在任意时刻手动启动配置云环境向导。

要手动启动配置云环境向导：

1. 在控制台树中，选择**管理服务器**节点。
2. 从节点的上下文菜单中，选择**All Tasks → 配置云环境**。

平均工作会话时间约 15 分钟。

关于配置云环境向导

配置云环境向导可让您配置 Kaspersky Security Center 以在云环境中工作。

该向导创建以下对象：

- 带有默认设置的网络代理策略
- Kaspersky Endpoint Security for Linux 策略
- Kaspersky Security for Windows Server 策略
- 实例管理组和自动移动实例到该管理组的规则
- 管理服务器数据备份任务
- 在运行 Linux 和 Windows 的设备上安装保护的任务
- 每个受管理设备的任务：
  - 快速恶意软件扫描
  - 更新下载

如果您选择了 BYOL 授权许可选项，配置云环境也会使用密钥文件或激活码激活 Kaspersky Security Center，并将密钥文件或激活码放置到授权许可存储空间中。

步骤 1：选择应用程序激活方法

如果您注册了现成的 AMI 之一（在 AWS Marketplace）或基于使用情况按月付费的 SKU（在 Azure 市场），则不会显示此步骤。在这种情况下，向导会立即进行下一步。但是，对于 Google Cloud，无法购买现成的 AMI。

如果您为 Kaspersky Security Center 选择了BYOL 授权许可选项，向导提示您选择应用程序激活方法。

使用 Kaspersky Security for Virtualization 或 for Kaspersky Hybrid Cloud Security 的激活码（或密钥文件）激活应用程序。

您可以通过以下方式激活应用程序：

- 通过输入激活码。

  在线激活将开始。该过程涉及对指定的激活码的验证，以及对密钥文件的发布和激活。

- 通过指定密钥文件。

  应用程序将检查密钥文件，如果它包含正确信息则激活，或提示您指定其他密钥文件。

Kaspersky Security Center 放置授权许可密钥到授权许可存储区并标记它为受管理设备上自动分发的密钥。

如果您使用标准 Microsoft Windows Remote Desktop Connection 或相似应用程序连接到实例，在远程连接属性中您必须指定用以连接的物理设备驱动器。这确保了您物理设备上的实例到文件的访问，并且允许您选择和指定密钥文件。

使用通过付费 AMI 部署的 Kaspersky Security Center 时，或者对于基于使用量的按月付费 SKU，您无法添加密钥文件或激活码到授权许可存储区。

步骤 2：选择云环境

选择您要部署 Kaspersky Security Center 的云环境：AWS、Azure 或 Google Cloud。

步骤 3：在云环境中授权

AWS

如果您选择了 AWS，指定您具有带有所需权限的 IAM 角色，或者提供给 Kaspersky Security Center 一个 AWS IAM 访问密钥。没有 IAM 角色或 AWS IAM 访问密钥，云段轮询不可用。

为将来轮询云段所使用的连接指定以下设置：

- **连接名称**

  输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。

该名称也将用作云设备的管理组名称。

如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

- **使用 AWS IAM 角色**

  如果您已经为管理服务器创建了 IAM 角色以使用 AWS 服务，则选择该选框。

- **使用 AWS IAM 用户账户**

  如果您拥有带有必要权限的 IAM 用户账户且您可以输入密钥 ID 和 secret key，则选择该选框。

  - **访问密钥 ID**

    IAM 访问密钥 ID 是个字母数字序列。当您在创建 IAM 用户账户时接收密钥 ID。

    如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

  - **Secret key**

    您创建IAM 用户账户时接收到的带有访问密钥 ID 的secret key。

    Secret key 的字符显示为星号。在您开始输入 secret key 后，**显示**按钮被显示。点击并按住该按钮一定时间以查看输入的字符。

    如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

该连接保存在应用程序设置。您只能使用配置云环境创建单个 AWS IAM 访问密钥。后续，您可以指定更多的连接以管理其他云段。

如果您要通过 Kaspersky Security Center 安装应用程序到实例，您必须确保您的 IAM 角色（或与您输入的密钥关联的账户的 IAM 用户）具有所有必要权限。

Azure

如果您选择了 Azure，为将来轮询云段所使用的连接指定以下设置：

- **连接名称**

  输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。

  该名称也将用作云设备的管理组名称。

  如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

- **Azure 应用程序 ID**

  您在 Azure 门户创建了该应用程序 ID。

  您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

- **Azure 订阅 ID**

  您在 Azure 门户创建了该订阅。

- **Azure 应用程序密码**

  当您创建应用程序 ID 时您收到应用程序 ID 的密码。

  密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

- **Azure 存储账户名**

  您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

- **Azure 存储访问密钥**

  您创建 Azure 存储账户以使用 Kaspersky Security Center 时接收密码（密钥）。

  密钥在“Azure 存储账户概述”区域的“密钥”子区域中提供。

该连接保存在应用程序设置。

Google Cloud

如果您选择了 Google Cloud，为将来轮询云段所使用的连接指定以下设置：

- **连接名称**

  输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。

  该名称也将用作云设备的管理组名称。

  如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

- **客户端电子邮件**

  客户端电子邮件是用于在 Google Cloud 注册项目的电子邮件地址。

- **项目 ID**

  项目 ID 是您在 Google Cloud 注册项目时收到的 ID。

- **私钥**

  私钥是您在 Google Cloud 注册项目时收到的用作私钥的字符序列。最好复制并粘贴此序列，以免出错。

该连接保存在应用程序设置。

步骤 4：配置与云的同步并选择后续操作

在该步骤，云段轮询开始，实例的特别管理组被创建。轮询中发现的实例被放置在该组。云段轮询计划被配置(默认每 5 分钟)。

与云同步自动移动规则也被创建。对于每个云网络的后续扫描，检测到的虚拟设备将被移动到“**受管理设备**”\“**云**”组的对应子组。

在“**与云段同步**”页面，您可以定义以下设置：

- **与云段同步管理组结构**

  如果启用该选项，**云**组被自动创建在**受管理设备**组，云设备发现被启动。在每个云网络扫描中检测到的实例和虚拟机被放置到 AWS 组。该组的管理子组结构匹配您的云段结构（在 AWS 中，可用域和放置组不出现在结构中；在 Azure 中，子网不出现在结构中）。未被识别为云环境中实例的设备在**未分配的设备**组。该组结构允许您使用组安装任务安装反病毒应用程序到实例，以及为不同组设置不同的策略。

  如果禁用该选项，**云**组也被创建，且云设备发现也被启动；然而，匹配云段结构的子组不在组中被创建。所有检测到的实例都在**云**管理组，因此显示在单一列表。如果您使用的 Kaspersky Security Center 需要同步，您可以修改**与云同步**规则的属性并强制执行该规则。强加该规则改变云组的子组结构，以便匹配您云段的结构。

  默认情况下已禁用该选项。

- **部署保护**

  如果选择该选项，向导创建任务以安装安全应用程序到实例。向导完成后，保护部署向导自动在您的云段的设备上启动，并且您将可以在这些设备上安装网络代理和安全应用程序。

  Kaspersky Security Center 可以使用其本地工具执行部署。如果您没有权限安装应用程序到 EC2 实例或 Azure 虚拟机，您可以手动配置**远程安装**任务并指定带有所需权限的账户。此种情况下，远程安装任务将不用于使用 AWS API 或 Azure 发现的设备。该任务将仅用于使用活动目录轮询、Windows 域轮询或 IP 范围轮询发现的设备。

  如果未选择该选项，保护部署向导不被启动，安装安全应用程序的任务未在实例上被创建。您可以稍后手动执行这些操作。

对于 Google Cloud，只能使用 Kaspersky Security Center 本机工具执行部署。如果选择了 Google Cloud，“**部署保护**”选项不可用。

步骤 5：步骤 5：在云环境中配置卡巴斯基安全网络

指定设置以转发 Kaspersky Security Center 操作信息到卡巴斯基安全网络知识库。您可以选择以下选项之一：

- **我同意使用卡巴斯基安全网络**

  安装在客户端设备上的 Kaspersky Security Center 和受管理应用程序将自动将其操作详情传输到卡巴斯基安全网络。参与卡巴斯基安全网络确保了包含病毒和其他威胁的数据库的快速更新，该数据库确保了对紧急安全威胁的快速响应。

- **我不同意使用卡巴斯基安全网络**

  Kaspersky Security Center 和受管理应用程序将不向卡巴斯基安全网络提供任何信息。
  如果选择此选项，则将禁用卡巴斯基安全网络。

Kaspersky 建议您参与卡巴斯基安全网络。

步骤 6：步骤 6：在云环境中配置电子邮件通知

在该窗口中，您可以配置如何传递 Kaspersky 应用程序在虚拟客户端设备上操作时记录的事件通知。这些设置将被用作应用程序策略的默认设置。

要配置发生在 Kaspersky 应用程序上的事件的通知传送，使用以下设置：

- **收件人（邮件地址）**

  应用程序将给其发送通知的用户的邮件地址。您可以输入一个或更多地址；如果您输入多个地址，使用分号分隔。

- **SMTP 服务器**

  您组织邮件服务器的地址。
  如果您输入多个地址，使用分号分隔。您可以使用下列值：
  - IPv4 或 IPv6 地址
  - 设备的 Windows 网络名称（NetBIOS 名称）
  - SMTP 服务器的 DNS 名称

- **SMTP 服务器端口**

  SMTP 服务器的通信端口号。如果您使用多个 SMTP 服务器，则通过指定的通信端口与它们建立连接。默认端口号是 25。

- **使用 ESMTP 身份验证**

  启用 ESMTP 身份验证支持。当选择了该复选框时，您可以在“**用户名**”和“**密码**”字段指定 ESMTP 身份验证设置。默认情况下已清除该选框。

您可以通过点击**发送测试消息**按钮测试新邮件通知设置。如果测试消息被**收件人(邮件地址)**字段中指定的地址成功接收，设备被正确配置。

步骤 7：步骤 7：创建云环境保护的初始配置

在该步骤，Kaspersky Security Center 自动创建策略和任务。**配置初始保护**窗口显示应用程序创建的策略和任务列表。

如果您在 AWS 云环境中使用 RDS 数据库，当管理服务器备份任务被创建时，您必须提供 IAM 访问密钥对给 Kaspersky Security Center。此种情况下，填充以下字段：

- **S3 bucket 名称**

  您为备份创建的 S3 bucket 名称。

- **访问密钥 ID**

  当您创建了 IAM 用户账户以使用 S3 bucket 存储实例时，您接收到密钥 ID（数字字母序列）。

  如果您在 S3 bucket 上选择了 RDS 数据库则该字段可用。

- **Secret key**

  您创建IAM 用户账户时接收到的带有访问密钥 ID 的secret key。

  Secret key 的字符显示为星号。在您开始输入 secret key 后，**显示**按钮被显示。点击并按住该按钮一定时间以查看输入的字符。

  如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

如果您在 Azure 云环境中使用 Azure SQL 数据库，当管理服务器备份任务被创建时，您必须提供您的 Azure SQL Server 信息给 Kaspersky Security Center。此种情况下，填充以下字段：

- **Azure 存储账户名**

  您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

- **Azure 订阅 ID**

  您在 Azure 门户创建了该订阅。

- **Azure 应用程序密码**

  当您创建应用程序 ID 时您收到应用程序 ID 的密码。

  密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

- **Azure 应用程序 ID**

  您在 Azure 门户创建了该应用程序 ID。

  您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

- **Azure SQL Server 名称**

  名称和资源组在您的 Azure SQL Server 属性中可用。

- **Azure SQL Server 资源组**

  名称和资源组在您的 Azure SQL Server 属性中可用。

- **Azure 存储访问密钥**

  在您的存储账户属性中可用，在访问密钥区域。您可以使用任何密钥（key1 或 key2）。

如果要在 Google Cloud 中部署管理服务器，则必须选择将用于存储备份副本的文件夹。选择本地设备上的文件夹或虚拟机实例上的文件夹。

下一步按钮在创建完最小保护配置所需的所有策略和任务后可用。

如果要运行任务的设备对管理服务器不可见，则任务仅当设备可见时启动。如果您创建新 EC2 实例或新 Azure 虚拟机，可能需要一些时间使其对管理服务器可见。如果您想把网络代理和安全应用程序立即安装在所有新创建的设备，确保**运行错过的任务**选项对**远程安装应用程序**任务启用。否则，新创建的实例/虚拟机将不会获得网络代理和安全应用程序，直到任务根据计划启动。

步骤 8：步骤 8：选择在安装过程中操作系统必须重启时的操作（对于云环境）

如果您先前选择了“**部署保护**”，您必须选择目标设备操作系统必须重启时的操作。如果您未选择“**部署保护**”选项，那么将跳过此步骤。

选择在安装应用程序过程中设备操作系统必须重启时是否重启实例：

- **不重启设备**

  如果选择该选项，安全应用程序安装后设备不被重启。

- **重启设备**

  如果选择该选项，安全应用程序安装后设备将被重启。

如果您要在重启前强制关闭实例上所有锁定会话中的应用程序，选择**强行关闭锁定会话中的应用程序**复选框。如果该复选框被清空，您将必须手动关闭所有锁定实例中的应用程序。

步骤 9：通过管理服务器接收更新

在此步骤，您可以查看下载管理服务器正确操作所需的必要更新的进度。您可以点击**下一步**按钮以转到向导的最后页面，而不等待下载完成。

向导结束。

检查配置

要检查是否 Kaspersky Security Center 15.1 被正确配置以工作在云环境：

1. 启动 Kaspersky Security Center 且确保您可以通过管理控制台连接到管理服务器。
2. 在控制台树中，选择“**受管理设备**”\“**云**”。
3. 当在**受管理设备\云**组查看任意子组时，确保“**设备**”选项卡显示子组的所有设备。
   如果设备未显示，您可以手动轮询对应的云段以查找它们。
4. 确保“**策略**”选项卡对以下应用程序具有活动策略：
   - Kaspersky Security Center 网络代理
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   如果它们未列出，您可以手动创建它们。
5. 确保“**任务**”选项卡列出以下任务：
   - **备份管理服务器数据**
   - **Windows Server 更新任务**
   - **管理服务器维护**
   - **将更新下载至管理服务器存储库**
   - **查找漏洞和所需更新**
   - **为 Windows 安装保护**
   - **为 Linux 安装保护**
   - **Windows Server 快速扫描任务**
   - **快速扫描**
   - **为 Linux 安装更新**

   如果它们未列出，您可以手动创建它们。

Kaspersky Security Center 15.1 被正确配置以工作在云环境。

云设备组

您可以通过将云设备合并成组来管理它们。在 Kaspersky Security Center 初始化配置阶段，默认情况下会创建“**受管理设备**”\“**云**”管理组，并将在轮询过程中检测到的云设备放置到该组。

如果您在配置同步时选择了**与云段同步管理组结构**选项，则此管理组中子组的结构与您的云段结构相同。（但是，在 AWS 中，可用性区域和置放群组未在结构中表示；在 Microsoft Azure 中，子网未在结构中表示。）在轮询期间检测到的组中的空子组将被自动删除。

您还可以通过组合所有或特定设备手动创建管理组。

默认情况下，“**受管理设备**”\“**云**”组从“**受管理设备**”组继承策略和任务。如果在对应策略和任务的属性设置中选择了**编辑已允许**复选框，您可以更改设置。

网络段轮询

管理服务器通过使用 AWS API、Azure API 或 Google API 工具对云段进行常规轮询来接收有关该网络中网络和设备的结构的信息。Kaspersky Security Center 使用该信息更新“**未分配的设备**”和“**受管理设备**”文件夹的内容。如果您配置了设备自动移动到管理组，检测到的设备将被包含在管理组中。

要允许管理服务器轮询云段，您必须拥有提供了 IAM 角色 或 IAM 用户账户（在 AWS 中），或者提供了应用程序 ID 和密码（在 Azure 中），或者提供了 Google 客户端电子邮件、Google 项目 ID 和私钥的权限。

您可以添加和删除连接，以及为每个云段设置轮询计划。

为云段轮询添加连接

要添加云段轮询连接到可用连接列表：

1. 在控制台树中，选择**设备发现** → **云**节点。
2. 在该窗口的工作区，单击“**配置轮询**”。
   包含云段轮询的可用连接列表的属性窗口打开。
3. 单击“**添加**”按钮。
   连接窗口将打开。
4. 为将用于进一步轮询云段的连接指定云环境的名称：
   云环境

   EC2 实例（或虚拟机）所在环境可以是 Amazon Web Services (AWS)、Microsoft Azure 或 Google Cloud。

如果选择了 AWS，请指定以下设置：

- **连接名称**

  输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。

  该名称也将用作云设备的管理组名称。

  如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

- **使用 AWS IAM 角色**

  如果您已经为管理服务器创建了 IAM 角色以使用 AWS 服务，则选择该选框。

- **使用 AWS IAM 用户账户**

  如果您拥有带有必要权限的 IAM 用户账户且您可以输入密钥 ID 和 secret key，则选择该选框。

  - **访问密钥 ID**

    IAM 访问密钥 ID 是个字母数字序列。当您在创建 IAM 用户账户时接收密钥 ID。

    如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

  - **Secret key**

    您创建IAM 用户账户时接收到的带有访问密钥 ID 的secret key。

    Secret key 的字符显示为星号。在您开始输入 secret key 后，**显示**按钮被显示。点击并按住该按钮一定时间以查看输入的字符。

    如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

配置云环境向导仅允许您指定单个 AWS IAM 访问密钥。后续，您可以指定更多的连接以管理其他云段。

如果选择了 Azure，请指定以下设置：

- **连接名称**

  输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。

  该名称也将用作云设备的管理组名称。

  如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

- **Azure 应用程序 ID**

  您在 Azure 门户创建了该应用程序 ID。

  您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

- **Azure 订阅 ID**

  您在 Azure 门户创建了该订阅。

- **Azure 应用程序密码**

  当您创建应用程序 ID 时您收到应用程序 ID 的密码。

  密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

- **Azure 存储账户名**

  您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

- **Azure 存储访问密钥**

  您创建 Azure 存储账户以使用 Kaspersky Security Center 时接收密码（密钥）。

  密钥在“Azure 存储账户概述”区域的“密钥”子区域中提供。

如果选择了 Google Cloud，请指定以下设置：

- **连接名称**

  输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。

  该名称也将用作云设备的管理组名称。

  如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

- **客户端电子邮件**

  客户端电子邮件是用于在 Google Cloud 注册项目的电子邮件地址。

- **项目 ID**

  项目 ID 是您在 Google Cloud 注册项目时收到的 ID。

- **私钥**

  私钥是您在 Google Cloud 注册项目时收到的用作私钥的字符序列。最好复制并粘贴此序列，以免出错。

5. 如果您想，选择**设置轮询计划**和更改默认设置。

该连接保存在应用程序设置。

在新云段被第一次轮询后，该段对应的子组出现在“**受管理设备**”\“**云**”管理组。

如果您指定不正确的凭证，在云段轮询过程中将不会发现实例，且新子组将不会出现在“**受管理设备**”\“**云**”管理组。

为云段轮询删除连接

如果您不再必须轮询特定云段，您可以从可用连接列表删除对应于段的连接。您还可以删除连接，如果，例如轮询云段的权限被转移给另一个带有不同密钥的 AWS IAM 用户。

要删除连接：

1. 在控制台树中，选择**设备发现** → **云**节点。
2. 在该窗口的工作区，选择“**配置轮询**”。
   包含云段轮询的可用连接列表的窗口打开。
3. 选择您要删除的连接并点击窗口右侧的**删除**按钮。
4. 在打开的窗口中，单击**确定**按钮以确认您的选择。

如果您正从可用连接列表中删除连接，相应段中的设备被自动从对应的管理组删除。

配置轮询计划

云段轮询根据计划执行。您可以设置轮询频率。

轮询频率在配置云环境设置中被自动设置为 5 分钟。您可以在任意时刻更改该值并设置不同的计划。然而，不建议设置大于每 5 分钟一次的轮询频率，因为这可能导致 API 操作错误。

要配置云段轮询计划：

1. 在控制台树中，选择**设备发现** → **云**节点。
2. 在工作区中，点击**配置轮询**。
   “云属性”窗口打开。
3. 在列表中，选择您要的连接并点击**属性**按钮。
   “连接属性”窗口打开。
4. 在属性窗口，点击**设置轮询计划**链接。
   计划窗口将打开。
5. 定义下列设置：
   - **计划开始**

轮询计划选项：

- **每 N 天**

  轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
  默认下，轮询每天运行一次，从当前系统日期和时间开始。

- **每 N 分钟**

  轮询定期运行，按照指定分钟间隔，从指定的时间开始。
  默认下，轮询每五分钟运行一次，从当前系统时间开始。

- **周中天数**

  轮询定期运行，在指定星期的指定时间。
  默认下，轮询每周五 18:00:00 P.M. 运行。

- **每个月所选周的指定天**

  轮询定期运行，在指定月日的指定时间。
  默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。
  如果启用该选项，管理服务器在它切换回来后立即启动轮询。
  如果禁用该选项，管理服务器等待下一次计划轮询。
  默认情况下已启用该选项。

6. 单击“**确定**”保存更改。

轮询计划被配置并保存。

安装应用程序到云环境中的设备

您可以安装以下 Kaspersky 应用程序到云环境中的设备：Kaspersky Security for Windows Server（对于 Windows 设备）和 Kaspersky Endpoint Security for Linux（对于 Linux 设备）。

您要安装保护的客户端设备必须满足在云环境中操作 Kaspersky Security Center 的需求。您必须拥有有效授权许可才能安装应用程序到 AWS 实例、Microsoft Azure 虚拟机或 Google 虚拟机实例。

Kaspersky Security Center 15.1 支持以下情景：

- 客户端设备通过 API 发现；安装也通过 API 执行。对于 AWS 和 Azure 云环境，支持此方案。
- 客户端设备通过活动目录轮询、Windows 域轮询 或 IP 范围轮询被发现；安装通过 Kaspersky Security Center 执行。
- 客户端设备通过 Google API 发现；安装通过 Kaspersky Security Center 执行。对于 Google Cloud，仅支持这种方案。

应用程序的其他安装方法不被支持。

要在虚拟设备上安装应用程序，使用安装包。

要创建任务以远程安装应用程序到实例或通过使用 AWS API 或 Azure API：

1. 在控制台树中，选择“**任务**”文件夹。
2. 单击“**新任务**”按钮。

   “新任务向导”启动。遵照向导的说明操作。
3. 在“**选择任务类型**”页面，选择“**远程安装应用程序**”作为任务类型。
4. 在**选择设备**页面，从“**受管理设备**”\“**云**”组选择相关设备。
5. 如果网络代理未安装在您要安装应用程序的设备上，在“**选择账户以运行任务**”页面选择“**需要账户(不使用网络代理)**”并在窗口右侧单击“**添加**”按钮。在出现的菜单中，选择以下项：

   - **云账户**

     如果您要安装应用程序到 AWS 环境中的实例，且您拥有带有所需权限的 AWS IAM 访问密钥，但不拥有 IAM 角色，请选择该选项。如果您要安装应用程序到 Azure 环境中的设备，也选择该选项。

     在打开的窗口中提供 Kaspersky Security Center 凭证以获取安装应用程序到相关实例的权限。

     选择云环境：AWS 或 Azure。

     在**账户名**字段，输入这些凭证的名称。此名称将显示在运行该任务的账户列表中。

     如果您选择了 AWS，在**访问密钥 ID** 和 **Secret key** 字段，输入有权安装应用程序到指定设备的 IAM 用户账户凭证。

     如果您选择了 Azure，在 **Azure 订阅 ID**和 **Azure 应用程序密码**字段，输入有权安装应用程序到指定设备的 Azure 账户凭证。

     如果您指定错误的凭证，远程安装任务将在所计划的设备上返回错误。

   - **账户**

     对于运行 Windows 的实例，在您不想使用 AWS 或 Azure API 工具安装应用程序时选择该选项。此种情况下，确保您云段中的设备满足必要条件。Kaspersky Security Center 自行安装应用程序，而不使用 AWS API 或 Azure API。

     如果您指定错误的数据，远程安装任务将在所计划的设备上返回错误。

   - **IAM 角色**

     如果您想安装应用程序到 AWS 环境中的实例，且拥有带有所需权限的 IAM 角色，选择该选项。

如果您选择该选项，但不拥有带有所需权限的 IAM 角色，远程安装任务将在所计划的设备上返回错误。

- **SSH 证书**

  对于运行 Linux 的实例，在您不想使用 AWS API 或 Azure API 工具安装应用程序时选择该选项。此种情况下，确保您云段中的设备满足必要条件。Kaspersky Security Center 自行安装应用程序，而不使用 AWS API 或 Azure API。

  要指定 SSH 证书的私钥，您可以使用 ssh-keygen 实用程序生成该私钥。请注意，Kaspersky Security Center 支持 PEM 格式的私钥，但 ssh-keygen 实用程序默认生成 OPENSSH 格式的 SSH 密钥。Kaspersky Security Center 不支持 OPENSSH 格式。要以支持的 PEM 格式创建私钥，请在 ssh-keygen 命令中添加“`-m PEM`”选项。例如：

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
  ```

您可以为每个实例通过点击**添加**按钮提供多个凭证。如果不同的云段需要不同的凭证，则为所有段提供凭证。

在向导结束后，应用程序远程安装任务显示在“**任务**”文件夹工作区的任务列表。

在 Microsoft Azure 中，远程安装安全应用程序到虚拟机可能导致删除安装在该虚拟机上的自定义脚本扩展程序。

查看云设备属性

要查看云设备的属性：

1. 在控制台树的“**设备发现**”→“**云**”节点，选择与相关实例所在组对应的子节点。
   如果您不知道相关虚拟设备所在的组，使用搜索功能：
   a. 右键单击“**受管理设备**”→“**云**”节点，然后在上下文菜单中选择“**搜索**”。
   b. 在打开的窗口中，运行搜索。
      如果存在满足您所设置的标准的设备，它们名称和详情将显示在窗口的下部。
2. 右击相关节点的名称。在上下文菜单中，选择**属性**。
   在打开的窗口中，对象属性被显示。
   “**系统信息**”→“**常规系统信息**”区域包含特定于云环境中设备的属性：
   - **使用 API 发现的设备**（**AWS**、**Azure** 或 **Google Cloud**；如果无法使用 API 工具检测到该设备，则显示“**否**”值）。
   - **云区域**。
   - **Cloud VPC**（仅适用于 AWS 和 Google Cloud 设备）。
   - **云可用区域**（仅适用于 AWS 和 Google Cloud 设备）。

- **云子网**。
- **云放置组**（仅当实例属于某个放置组时才显示此单元；否则，不显示此单元）。

您可以点击**导出到文件**按钮导出该信息到 .csv 或 .txt 文件。

与云同步

在配置云环境操作期间，与云同步规则被自动创建。规则允许您从“**未分配的设备**”组自动移动在每次轮询中检测到的实例到“**受管理设备**”\“**云**”组，这样实例就可用于集中管理。默认下，规则在创建后被激活。您可以在任意时刻禁用、修改或强制规则。

要编辑“与云同步”规则的属性和/或强制实施规则：

1. 在控制台树中右击“**设备发现**”节点的名称。
2. 在上下文菜单中，选择**属性**。
3. 在打开的**属性**窗口中，在“**区域**”窗格选择“**移动设备**”。
4. 在工作区的设备移动规则列表中，选择“**与云同步**”，然后单击窗口下部的“**属性**”按钮。
   规则属性窗口打开。
5. 如果必要，在**云段**设置组指定以下设置：

   - **设备位于云段**

     该规则仅应用到位于所选云段的设备。否则，该规则应用到发现的所有设备。
     默认情况下已选定该选项。

     - **包含子对象**

       该规则应用到所选段和其所有嵌套云子区域中的所有设备。否则，该规则仅应用到位于根段的设备。
       默认情况下已选定该选项。

     - **将设备从嵌套对象移动到对应子组**

       如果启用该选项，嵌套对象的设备将被自动移动到对应其结构的子组。
       如果禁用该选项，嵌套对象的设备将被自动移动到云子组的根，而不再分支。
       默认情况下已启用该选项。

       - **创建对应于新检测到设备的容器的子组**

         如果启用该选项，当**受管理设备云**结构没有匹配包含设备的区域的子组，Kaspersky Security Center 将创建这类子组。例如，如果一个子网在设备发现中被发现，带有相同名称的新组将在**受管理设备\云**组下被创建。

如果禁用该选项，Kaspersky Security Center 不创建任何新子组。例如，如果一个子网在网络轮询中被发现，带有相同名称的新组将不在**受管理设备云**组下被创建，且该子组中的设备将被移动到**受管理设备云**组。

默认情况下已启用该选项。

- **删除在云段中未找到匹配的子组**

  如果启用该选项，应用程序从云组删除所有不匹配任何现有云对象的子组。

  如果禁用该选项，未匹配任何现有云对象的子组被保留。

  默认情况下已启用该选项。

如果您在运行配置云环境时启用了“**与云同步**”选项，与云同步规则启用**创建对应于新检测到设备的容器的子组**和**删除在云段中找不到匹配的子组**复选框而创建。

如果您不启用**与云同步**选项，与云同步规则禁用（清空）这些复选框而创建。如果您的 Kaspersky Security Center 需要**受管理设备\云**子组的结构与云段结构匹配，在规则属性中启用**创建对应于新检测到设备的容器的子组**和**删除在云段中找不到匹配的子组**选项，然后强制规则。

6. 在**使用 API 发现的设备**下拉列表，选择以下值之一：
   - **AWS**。设备使用 AWS API 发现，即设备确定在 AWS 云环境中。
   - **Azure**。设备使用 Azure API 发现，即设备确定在 Azure 云环境中。
   - **Google Cloud**。设备使用 Google API 发现，即设备确定在 Google Cloud 环境中。
   - **否**。无法使用 AWS API、Azure API 或 Google API 检测到该设备，即设备位于云环境之外，或者位于云环境中，但是无法使用 API 检测到该设备。
7. **没有值**。此条件不适用。如果必要，在其他区域设置其他规则属性。
8. 如果必要，点击窗口下部的“**强制**”按钮强制规则。

   规则执行向导启动。遵照向导的说明操作。当向导结束后，将运行规则，并且“**受管理设备**”\“**云**”子组的结构将与您的云段结构匹配。
9. 单击“**确定**”按钮。

属性被设置并保存。

要禁用与云规则同步：

1. 在控制台树中右击“**设备发现**”节点的名称。
2. 在上下文菜单中，选择**属性**。
3. 在打开的**属性**窗口中，在“**区域**”窗格选择“**移动设备**”。
4. 在工作区的设备移动规则列表中，禁用（清空）**与云同步**选项并点击**确定**。

规则被禁用且不会再被应用。

在 Yandex.Cloud 中部署 Kaspersky Security Center

您可以在 Yandex.Cloud 中部署 Kaspersky Security Center。仅按使用计费模式可用；不支持云数据库。

在 Yandex.Cloud 中，可以使用以下安全应用程序部署方法：

- 通过 Kaspersky Security Center 的本机方式，即通过“*远程安装*”任务（仅当管理服务器和要保护的虚拟机在同一网段时，才能部署安全程序）
- 通过部署脚本

要在 Yandex.Cloud 中部署 Kaspersky Security Center，您必须拥有 Yandex.Cloud 服务账户。您必须为此账户授予 marketplace.meteringAgent 权限，并将此账户与虚拟机关联（有关详细信息，请参阅 https://cloud.yandex.com/en）。

附录

该部分提供了使用 Kaspersky Security Center 的参考信息和附加说明。

高级功能

该部分将说明 Kaspersky Security Center 设计用于扩展集中式管理设备上应用程序功能的一系列附加选项。

Kaspersky Security Center 操作自动化。klakaut 实用程序

您可以使用 klbackup 自动化 Kaspersky Security Center 的操作。klakaut 实用程序及其帮助系统位于 Kaspersky Security Center 的安装文件夹中。

自定义工具

Kaspersky Security Center 允许您创建*自定义工具*（以下亦简称为*工具*）列表 – 通过上下文菜单的“**自定义工具**”组从管理控制台为客户端设备激活的应用程序。列表中每个工具将与单独的菜单命令（管理控制台使用该命令启动与该工具相关的应用程序）相关联。

应用程序将在管理员工作区中启动。应用程序可接受将远程客户端设备的属性作为命令行参数（NetBIOS 名称、DNS 名称、IP 地址）。到远程设备的连接可使用通道建立。

默认情况下，自定义工具列表包含每个客户端设备的下列服务程序：

- "**远程诊断**"是 Kaspersky Security Center 的远程诊断实用程序。
- "**远程桌面**"是名为远程桌面连接的标准 Microsoft Windows 组件。
- "**计算机管理**"是标准 Microsoft Windows 组件。

要添加或删除自定义工具，或编辑其设置，

在客户端设备的上下文菜单中，选择**自定义工具 → 配置自定义工具**。

自定义工具窗口打开。在此窗口中，您可以添加自定义工具或使用**添加**和**修改**按钮编辑它们的设置。要删除自定义工具，请单击带有红叉图标的删除按钮 (❌)。

网络代理磁盘克隆模式

克隆参考设备的硬盘驱动器是在新设备上安装软件的流行方法。如果网络代理以标准模式运行在参考设备的硬盘驱动器上，会发生以下问题：

带有网络代理的参考磁盘镜像被部署到新设备后，它们以单一图标显示在管理控制台。该问题发生是因为在新设备的克隆结果保持相同的内部数据，这将允许管理服务器关联设备到管理控制台上的图标。

一个特别的*网络代理磁盘克隆模式*允许您避免克隆后在管理控制台错误显示新设备的问题。在您通过克隆磁盘部署软件（带有网络代理）到新设备时使用该模式。

在磁盘克隆模式下，网络代理保持运行，但是不连接到管理服务器。当退出克隆模式时，网络代理删除内部数据，这将导致管理服务器关联多个设备到管理控制台上的单一图标。在完成参考设备镜像的克隆时，新设备显示在管理控制台属性中。

网络代理磁盘克隆模式使用方案

1. 管理员安装网络代理到参考设备。
2. 管理员使用klnagchk实用工具检查网络代理到管理服务器的连接。
3. 管理员启用网络代理磁盘克隆模式。
4. 管理员安装软件和补丁到设备，并重启所需的次数。
5. 管理员克隆参考设备的硬盘驱动器到任意数量的设备。
6. 每个克隆的副本必须满足以下条件：
    a. 设备名称必须更改。
    b. 设备必须重启。
    c. 磁盘克隆模式必须被禁用。

使用 klmover 工具启用和禁用磁盘克隆模式

要启用或禁用网络代理磁盘克隆模式：

1. 在您必须克隆的安装了网络代理的设备上运行 klmover 工具。

   klmover 工具位于网络代理安装文件夹。

2. 要启用磁盘克隆模式，在 Windows 命令提示时输入以下命令：

   `klmover -cloningmode 1`

   网络代理切换到磁盘克隆模式。

3. 要请求磁盘克隆模式的当前状态，在命令行输入以下命令：

   `klmover -cloningmode`

   工具显示是否磁盘克隆模式已启用或禁用。

4. 要禁用磁盘克隆模式，在命令行输入以下命令：

   `klmover -cloningmode 0`

准备安装了网络代理的参考设备以创建操作系统映像

您可能要创建安装了网络代理的参考设备的操作系统镜像，然后在网络设备上部署该镜像。在这种情况下，您将创建尚未在其上启动网络代理的参考设备的操作系统镜像。如果在创建操作系统镜像之前在参考设备上启动网络代理，则管理服务器对从参考设备的操作系统镜像部署的设备的标识将是有问题的。

要准备用于创建操作系统镜像的参考设备，请执行以下操作：

1. 确保在参考设备上安装了 Windows 操作系统，并在该设备上安装了所需的其他软件。
2. 在参考设备上的“Windows 网络连接”设置中，将参考设备从安装了 Kaspersky Security Center 的网络上断开。
3. 在参考设备上，使用 setup.exe 文件启动网络代理的本地安装。

   Kaspersky Security Center 网络代理安装向导启动。遵照向导的说明操作。

4. 在向导的“**管理服务器**”页面上，指定管理服务器 IP 地址。

   如果您不知道管理服务器的确切地址，请输入 localhost。您可以稍后通过将 klmover 实用程序与 `-address` 参数一起使用来更改 IP 地址。

5. 在向导的“**启动应用程序**”页面上，禁用“**安装期间启动应用程序**”选项。
6. 网络代理安装完成后，不要在创建操作系统映像之前重新启动设备。

   如果重启设备，则必须重复为创建操作系统镜像准备参考设备的整个过程。

7. 在参考设备上的命令行中，启动 sysprep 实用程序并执行以下命令：
   `sysprep.exe /generalize /oobe /shutdown`。

参考设备已准备好创建操作系统镜像。

配置从文件完整性监控接收消息

类如 Kaspersky Security for Windows Server 或 Kaspersky Security for Virtualization Light Agent 的受管理应用程序从文件完整性监控发送消息到 Kaspersky Security Center。Kaspersky Security Center 也允许您监控到系统重要组件（例如 Web 服务器和 ATM）的任何更改，并对系统的完整性的破坏做出响应。对于这些目的，您可以从文件完整性监控组件接收消息。文件完整性监控组件允许您不仅监控设备的文件系统，也监控防火墙状态和所连接硬件的状态。

您必须配置 Kaspersky Security Center 以从文件完整性监控组件接收消息，而不使用 Kaspersky Security for Windows Server 或 Kaspersky Security for Virtualization Light Agent。

要配置从文件完整性监控接收消息：

1. 打开安装了管理服务器的设备的注册表（例如，在**开始** → **运行**菜单使用 regedit 命令）。
2. 转至以下分支：
   - 对于 32 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 对于 64 位系统：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. 创建键：
   - 创建键 KLSRV_EVP_FIM_PERIOD_SEC 以指定计算所处理事件数量的时间段。指定下列设置：
     a. 指定 KLSRV_EVP_FIM_PERIOD_SEC 做为键名称。
     b. 指定 DWORD 做为键类型。
     c. 指定介于 43 200 和 172 800 秒之间的时间间隔值范围。默认情况下，时间间隔是 86 400 秒。
   - 创建键 KLSRV_EVP_FIM_LIMIT 以限制指定时间段收到事件的数量。指定下列设置：
     a. 指定 KLSRV_EVP_FIM_LIMIT 做为键名称。
     b. 指定 DWORD 做为键类型。
     c. 指定介于 2 000和 50 000 之间的接收事件数量值范围。默认事件数量是 20 000。
   - 创建键 KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC 以精确计算特定时间间隔的事件数量。指定下列设置：
     a. 指定 KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC 做为键名称。
     b. 指定 DWORD 做为键类型。
     c. 指定介于 120 到 600 秒的值范围。默认时间间隔为 300 秒。

- 创建键 KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC，以便在指定的时间段后，应用程序可以检查在相应时间间隔内处理的事件数量是否少于指定限制。该检查在达到接收事件的限制时执行。如果该条件被满足，应用程序恢复保存事件到数据库。指定下列设置：

  a. 指定 KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC 做为键名称。

  b. 指定 DWORD 做为键类型。

  c. 指定介于 600 到 3 600 秒的值范围。默认时间间隔为 1 800 秒。

如果键未创建，默认值被使用。

4. 重启管理服务器服务。

接收来自文件完整性监控组件的事件的限制将被配置。您可以在报告“**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**”和“**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**”中查看文件完整性监控组件的结果。

管理服务器维护

通过管理服务器维护，您可以腾出管理服务器文件夹中的空间，并通过删除不再需要的对象来减少数据库存储量。这有助于您提高应用程序的性能和运行可靠性。我们建议您至少每周对管理服务器进行一次维护。

管理服务器维护通过专用任务进行。在维护管理服务器时，应用程序执行以下操作：

- 从存储文件夹中删除不必要的文件夹和文件。
- 从表中删除不必要的记录（也称为“悬垂指针”）。
- 清除缓存。
- 维护数据库（如果您使用 SQL Server 或 PostgreSQL 作为 DBMS）：
  - 检查数据库中是否存在错误（仅适用于 SQL Server）。
  - 重组数据库索引。
  - 更新数据库统计信息。
  - 收缩数据库（如果必要）。

要创建管理服务器维护任务，请执行以下操作：

1. 在控制台树中，选择您要为其创建“*管理服务器维护*”任务的管理服务器节点。
2. 选择**任务**文件夹。
3. 在“**任务**”文件夹的工作区，单击“**新任务**”按钮。
   “新任务向导”启动。
4. 在向导的“**选择任务类型**”窗口，选择“**管理服务器维护**”做为任务类型，然后单击“**下一步**”。

5. 如果您必须在维护过程中收缩管理服务器数据库，请在向导的“**设置**”窗口选择“**收缩数据库**”复选框。

6. 遵照剩余的向导说明。

新创建的任务显示在“**任务**”文件夹工作区的任务列表。一个管理服务器仅可以运行一个“*管理服务器维护*”任务。如果已经为管理服务器创建了“*管理服务器维护*”任务，则无法创建新的“*管理服务器维护*”任务。

访问公共 DNS 服务器

如果无法使用系统 DNS 访问卡巴斯基服务器，Kaspersky Security Center 可以按以下顺序使用这些公共 DNS 服务器：

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)

对这些 DNS 服务器的请求可能包含域地址和管理服务器的公共 IP 地址，因为应用程序建立了到 DNS 服务器的 TCP/UDP 连接。如果 Kaspersky Security Center 使用公共 DNS 服务器，则数据处理受相关服务的隐私政策约束。

要通过使用 klscflag 实用程序配置公共 DNS 的使用：

1. 使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装管理服务器的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。
2. 要禁用公共 DNS 的使用，请运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. 要启用公共 DNS 的使用，请运行以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

用户通知方法窗口

在“**用户通知方法**”窗口，您可以配置将证书安装到移动设备的用户通知。

- **在向导中显示二维码**。如果您选择该选项，安装包的链接将显示在移动设备连接向导的最后一步。
- **发送二维码到用户**。如果您选择该选项，您可以指定通知用户有关设备连接的设置。

在设置的“**通过电子邮件**”组，您可以使用邮件消息配置安装新证书到他的/她的移动设备的用户通知。该通知方法仅在启用 SMTP 服务器时可用。

在设置的“**通过 SMS**”组，您可以使用 SMS 配置安装证书到他的/她的移动设备的用户通知。该通知方法仅在启用 SMS 通知 时可用。

如有必要，在设置的“**通过电子邮件**”和“**通过 SMS**”组单击“**编辑消息**”链接来查看和编辑通知消息。

设备分类窗口

从“**设备分类**”列表选择分类。列表包含预定义分类和用户创建的分类。

您可以在“**设备分类**”区域的工作区中查看设备分类的详细信息。

定义新对象名称窗口

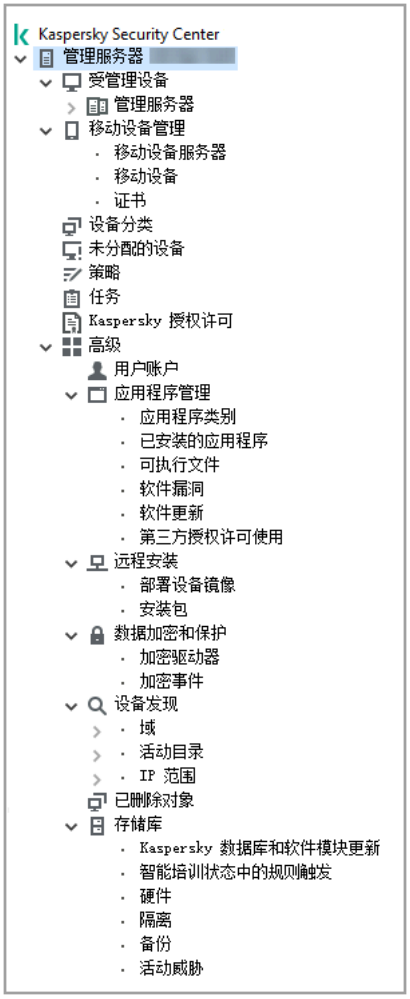
在该窗口，指定新创建对象的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

使用管理界面的功能

该部分将说明您在 Kaspersky Security Center 主窗口中可以执行的操作。

控制台树

控制台树（参见下图）旨在显示企业网络中管理服务器层级结构、其管理组的结构以及应用程序的其他对象，如“**存储库**”或“**应用程序管理**”文件夹。Kaspersky Security Center 的命名空间可以包含多个节点，这些节点包括与层次结构中包括的已安装管理服务器相应的服务器的名称。



控制台树

管理服务器节点

“**管理服务器 – <设备名称>**”节点是一个容器，其中显示了所选管理服务器的结构组织。

管理服务器节点的工作区包含程序和受管理设备当前状态的概要信息。工作区的信息在不同的选项卡间发布：

- **监控**。以实时模式显示应用程序操作信息和客户端设备的当前状态信息。管理员的重要消息（例如漏洞、错误、检测到病毒等消息）用特殊颜色高亮。您可以使用**监控**选项卡上的链接来运行标准的管理员任务（例如在客户端设备安装和配置安全应用程序），也可以转到其它控制台树文件夹。

- **统计**。包含按照标题分组的图表集合（保护状态、反病毒统计信息、更新等等）。这些图表使应用程序操作和客户端设备的当前信息变得可视化。

- **报告**。包含程序生成报告的模版。在该选项卡，您可以使用预设模版创建报告，也可以创建自定义报告模版。
- **事件**窗口。包含程序操作期间注册的事件记录。这些报告按主题发布，为了更好的阅读和过滤。在该选项卡上，您可以查看自动生成的事件分类，也可以创建自定义分类。

“管理服务器”节点的文件夹

“**管理服务器 – <设备名称>**”节点包括以下文件夹：

- **受管理设备**。“管理组”文件夹用于存储、显示、配置和修改管理组的结构、组策略和组任务。
- **移动设备管理**。该文件夹用于管理移动设备。**移动设备管理**文件夹包含以下子文件夹：
  - **移动设备服务器**。用于管理 iOS MDM 服务器。
  - **移动设备**。移动设备用于管理移动设备、KES 和 iOS MDM。
  - **证书**。用于管理移动设备证书。
- **设备分类**。该文件夹用于根据标准（设备分类）在所有受管理设备中快速选择设备。例如，您可以快速选择未安装安全应用程序的设备，然后处理它们（查看列表）。您可以在所选设备上运行特定操作，例如分配给它们一些任务。您可以使用预设分类，也可以创建自定义分类。
- **未分配的设备**。该文件夹包含未包含在任何管理组的设备列表。您可以在未分配设备上运行一些操作，例如，移动它们到管理组或在其上安装应用程序。
- **策略**。该文件夹用于查看和创建策略。
- **任务**。该文件夹用于查看和创建任务。
- Kaspersky **授权许可**。包含 Kaspersky 应用程序的可用授权许可密钥列表。在该文件夹的工作区，您可以将新的授权许可密钥添加到授权许可密钥存储库，将授权许可密钥部署到受管理设备并查看授权许可密钥使用报告。
- **高级**。该文件夹包含对应不同程序功能的子组。

“高级”文件夹。在控制台树移动文件夹

高级文件夹包含以下子文件夹：

- **用户账户**。包含网络用户账户列表。
- **应用程序管理**。用于管理网络设备上安装的应用程序。**应用程序管理**文件夹包含以下子文件夹：
  - **应用程序类别**。用于管理自定义应用程序类别。
  - **应用程序注册表**。包含安装有网络代理的设备上安装的应用程序的列表。
  - **可执行文件**。包含安装有网络代理的客户端设备上存储的可执行文件的列表。
  - **软件漏洞**。包含安装有网络代理的设备上应用程序漏洞的列表。

- **软件更新**。包含管理服务器收到的可以分发到设备的更新的列表。
- **第三方授权许可使用**。包含已授权的应用程序组列表。您可以使用已授权的应用程序组来监控第三方软件（非 Kaspersky 应用程序）的授权许可的使用以及可能的授权许可限制违规。

- **远程安装**。该文件夹用于管理操作系统和应用程序的远程安装。**远程安装**文件夹包含以下子文件夹：
  - **部署设备镜像**。用于在设备上部署操作系统镜像。
  - **安装包**。包含可用于在设备上远程安装应用程序的安装包的列表。
- **数据加密和保护**。该文件夹用于管理对硬盘驱动器和可移动驱动器上用户数据加密的处理。
- **网络轮询**。该文件夹显示管理服务器所在的网络。管理服务器通过定期轮询企业网络中的 Windows 网络、IP 子网和活动目录来接收有关网络结构及其设备的信息。轮询结果显示在相应文件夹（**域**、IP **范围**和**活动目录**）的工作区中。
- **存储库**。该文件夹可以对用于监控设备状态和执行维护的对象进行操作。**存储库**文件夹包含下列子文件夹：
  - **自适应异常检测**。包含由在客户端设备上以智能培训模式工作的 Kaspersky Endpoint Security 规则执行的检测列表。
  - Kaspersky **软件更新和补丁**。包含管理服务器收到的可以分发到设备的更新的列表。
  - **硬件**。包含要连接至组织网络的硬件列表。
  - **隔离**。包含由设备上的反病毒应用程序移至隔离区的对象的列表。
  - **备份**。包含设备清除过程中删除和修改的文件备份副本的列表。
  - **未处理的文件**。包含分配以供反病毒程序以后进行扫描的文件的列表。

您可以包含在**高级**文件夹的子文件夹设置。频繁使用的子文件夹可以被从**高级**文件夹向上移动一个级别。不常使用的子文件夹可以移动到**高级**文件夹。

*要把子文件夹移出**高级**文件夹：*

1. 在控制台树，选择您要移出**高级**文件夹的子文件夹。
2. 在子文件夹的上下文菜单中，选择**查看 → 从高级文件夹移出**。

> 您也可以在**高级**文件夹的工作区将子文件夹移出**高级**文件夹，通过点击该子文件夹的**从高级文件夹移出**链接。

*要将子文件夹移动到**高级**文件夹：*

1. 在控制台树，选择您要移动到**高级**文件夹的子文件夹。
2. 在该子文件夹的上下文菜单中，选择**查看 → 移动到高级文件夹**。

如何在工作区中更新数据

在 Kaspersky Security Center 中，工作区数据(例如设备状态、统计信息和报告)从不被自动更新。

要更新工作区中的数据，请执行以下操作：

- 按 **F5** 键。
- 在控制台树中的对象上下文菜单中，选择“**刷新**”。
- 在工作区中单击刷新图标 ( )。

如何浏览控制台树

要浏览控制台树，您可以使用下列工具栏按钮：

- – 后退一步。
- – 向前一步。
- – 向上一级。

您还可以使用工作区右上角的导航链接。导航链接包含您当在所在控制台树中的文件夹的绝对路径。链接的所有元素（最后一个除外）均链接至控制台树中的对象。

如何在工作区打开对象属性窗口

您可以在对象属性窗口中更改绝大部分管理控制台对象的属性。

要打开工作区中某个对象的属性窗口，请执行以下操作：

- 从对象的上下文菜单中，选择**属性**。
- 选择一个对象，然后按 **ALT+ENTER** 组合键。

如何在工作区中选择一组对象

您可以在工作区选择一组对象。您可以选择一组对象，例如您要创建任务的设备集合。

要选择对象范围，请执行以下操作：

1. 选择范围中的第一个对象，按 **Shift**键。
2. 按住 **Shift** 键，然后选择范围中的最后一个对象。

   该范围将被选定。

要将单独对象进行分组，请执行以下操作：

1. 选择组中的第一个对象，按 **Ctrl** 键。
2. 按住 **Ctrl** 键，然后选择组中的其他对象。

   对象将被分组。

如何在工作区中更改表列集

管理控制台允许您更改工作区中显示的列集。

要在工作区中更改列集，请执行以下操作：

1. 在控制台树中，单击要为其更改列集的对象。
2. 在文件夹的工作区，通过点击“**添加/删除列**”链接打开列集设置配置窗口。
3. 在“**添加/删除列**”窗口中，指定要显示的列集。

参考信息

该部分的表格将为您提供有关管理控制台对象的上下文菜单的概览信息，以及有关控制台树对象和工作区对象的概览信息。

上下文菜单命令

本区域列出管理控制台对象和相应的上下文菜单项（请见下表）。

管理控制台对象的上下文菜单项

对象	菜单项	菜单项用途
上下文菜单的常规项	**搜索**	打开设备搜索窗口。
	刷新	刷新所选对象的显示。
	导出列表	导出当前列表到文件。
	属性	打开所选对象的属性窗口。
	查看 → 添加/删除列	在工作区的对象表格中添加或删除列。
	查看 → 大图标	在工作区中以大图标显示对象。
	查看 → 小图标	在工作区中以小图标显示对象。
	查看 → 列表	在工作区中以列表形式显示对象。
	查看 → 表格	在工作区中以表格形式显示对象。
	查看 → 配置	配置管理控制台元素的显示。
Kaspersky Security Center	**新建 → 管理服务器**	将管理服务器添加至控制台树。
<管理服务器名称>	**连接到管理服务器**	连接到管理服务器。
	断开与管理服务器的连接	断开与管理服务器的连接。
受管理设备	**安装应用程序**	启动远程安装向导。
	查看 → 配置界面	配置界面元素的显示。
	删除	从控制台树中删除管理服务器。
	安装应用程序	为管理组启动远程安装向导。
	重置病毒计数器	重置管理组中包含的设备的病毒计数器。
	查看威胁报告	创建管理组中包含的设备上的威胁和病毒活动报告。
	新建 → 组	创建管理组。
	所有任务 → 新组结构	根据域结构或活动目录，创建管理组结构。
	所有任务 → 显示消息	为管理组中包含的设备启动"用户新消息向导"。
受管理设备 → 管理服务器	**新建 → 从属管理服务器**	启动"添加从属管理服务器向导"。
	新建 → 虚拟管理服务器	启动新虚拟管理服务器向导。
移动设备管理 → 移动设备	**新建 → 移动设备**	连接用户的新移动设备。
移动设备管理 → 证书	**新建 → 证书**	创建证书。
	创建 → 移动设备	连接用户的新移动设备。
设备分类	**新建 → 新分类**	创建设备分类。
	所有任务 → 导入	从文件中导入分类。
卡巴斯基授权许可	**添加激活码或密钥文件**	要添加授权许可密钥到管理服务器存储库。
	激活应用程序	启动应用程序激活任务创建向导。
	授权许可密钥使用报告	创建并显示客户端设备授权许可密钥报告。
应用程序管理 → 应用程序类别	**新建 → 类别**	创建应用程序类别。
应用程序管理 → 应用程序注册表	**过滤器**	配置应用程序列表过滤器。
	监控的应用程序	配置应用程序安装事件发布。
	删除未安装的应用程序	清除不在网络设备上安装的应用程序的详情列表。
应用程序管理 → 软件更新	**接受用于更新的授权许可协议**	接受软件更新的授权许可协议。
应用程序管理 → 第三方授权许可使用	**新建 → 已授权应用程序组**	创建授权的应用程序组。

对象	菜单项	菜单项用途
远程安装 → 安装包	**显示当前应用程序版本**	查看 Web 服务器上可用的最新版 Kaspersky 应用程序的列表。
	新建 → 安装包	创建安装包。
	所有任务 → 更新数据库	更新安装包中的应用程序数据库。
	所有任务 → 显示独立包常规列表	显示为安装包创建的独立包列表。
设备发现 → 域	**所有任务 → 设备活动**	配置管理服务器对网络设备闲置的响应。
设备发现 → IP 范围	**新建 → IP 范围**	创建一个 IP 范围。
存储库 → 卡巴斯基数据库和软件模块更新	**下载更新**	启动管理服务器的"将更新下载至存储库"任务属性窗口。
	更新下载设置	配置管理服务器的"将更新下载至存储库"任务。
	反病毒数据库使用报告	创建并显示数据库版本报告。
	所有任务 → 清除更新存储库	清除管理服务器上的更新存储库。
存储库 → 硬件	**新建 → 设备**	创建新设备。

受管理设备列表。列描述

下表显示受管理设备列表的列名称及各自的描述。

受管理设备列表的列描述

列名称	参数值
名称	客户端设备的 NetBIOS 名称。设备名称的图标说明在附录中提供。
操作系统类型	客户端设备上安装的操作系统的类型。
Windows 域	客户端设备所在的 Windows 域的名称。
网络代理已安装	客户端设备上的网络代理安装结果：*是*、*否*、*未知*。
网络代理正在运行	网络代理的操作结果：*是*、*否*、*未知*。
实时保护	安全应用程序已安装：*是*、*否*、*未知*。
上一次连接到管理服务器	客户端设备已连接到管理服务器的时间。
反病毒数据库上次更新	自受管理设备上次更新以来经过的时间段。
状态	客户端设备的当前状态："*正常*、*严重*、*警告*"。

列名称	参数值

状态描述	客户端设备的条件更改为“*严重*”或“*警告*”的原因。
	客户端设备的状态在以下条件下更改为“*警告*”或“*严重*”：
	• 安全应用程序未安装。
	• 检测到太多病毒。
	• 实时保护级别与管理员设置的级别不同。
	• 恶意软件扫描已长时间未执行。
	• 数据库已过期。
	• 长时间没有连接。
	• 检测到活动威胁。
	• 需要重新启动。
	重新启动设备可能是因为以下原因之一：
	  • 由于未知原因重启。
	  • 应用程序在重启前不会运行。
	  • 需要重启以完成更新；应用程序正在运行。
	  • 需要重启以启动更新。
	  • 需要重启以完成扫描或清除。
	  • 需要重启以完成远程安装/卸载。
	  • 即将完成磁盘的数据加密。
	  您可以在配置设备状态切换时设置原因。
	• 安装了不兼容的应用程序。
	• 检测到软件漏洞。
	• Windows Update 更新检查已长时间未执行。
	• 无效的加密状态。
	• 移动设备设置不遵从策略。
	• 检测到未处理的安全问题。
	• 应用程序定义的设备状态。
	• 设备磁盘空间不足。
	• 授权许可即将过期。
	设备的状态仅由于以下原因更改为“*严重*”：
	• 授权许可已过期。
	• 设备已失去管理。
	• 保护已禁用。
	• 安全应用程序没有运行。
	客户端设备上受管理的 Kaspersky 应用程序可以添加状态描述到列表。Kaspersky Security Center 可以从设备上安装的受管理的 Kaspersky 应用程序接收客户端设备状态描述。如果受管理的应用程序分配到设备的状态不同于被 Kaspersky Security Center 分配的状态，管理控制台显示该状态，这也是对设备安全最关键的事件。例如，如果受管理应用程序分配了*严重*状态到设备，而 Kaspersky Security Center 分配了*警告*状态，管理控制台为该设备显示*严重*状态以及受管理应用程序提供的相关描述。

信息更新	自客户端设备上次与管理服务器成功同步以来（即上次网络扫描以来）经过的时间段。
DNS 名称	客户端设备的 DNS 域名。
DNS 域	主 DNS 前缀。
IP 地址	客户端设备的 IP 地址。建议使用 IPv4 地址。
上一次可见	客户端设备在网络上保持可见的持续时间。
上一次全盘扫描	在用户请求后安全应用程序对客户端设备执行上一次扫描的日期和时间。
检测到的威胁总数	发现的威胁数量。
实时保护状态	实时保护状态：*正在启动*、*运行中*、*正在运行 (最大保护)*、*正在运行 (最快速度)*、*正在运行 (推荐设置)*、*正在运行 (自定义设置)*、*已停止*、*已暂停*、*失败*。
连接 IP 地址	用于连接 Kaspersky Security Center 管理服务器的 IP 地址。
网络代理版本	网络代理版本。
应用程序版本	安装在客户端设备上的安全应用程序版本。
反病毒数据库发布于	反病毒数据库的版本。
系统上次启动	客户端设备上次打开的日期和时间。
需要重新启动	需要重启客户端设备。
分发点	用作此客户端设备的分发点的设备的名称。

列名称	参数值
描述	在网络扫描后接收的客户端设备描述。
加密状态	客户端设备的数据加密状态。
WUA 状态	客户端设备上的 Windows 更新代理的状态。 "*是*"值与通过 Windows 更新从管理服务器接收更新的客户端设备对应。 "*否*"值与通过 Windows 更新从其他来源接收更新的客户端设备对应。
操作系统 bit 大小	客户端设备上安装的操作系统的大小。
垃圾邮件保护状态	垃圾邮件保护组件的状态：*运行中*、*正在启动*、*已停止*、*已暂停*、*失败*、*未知*
数据泄漏防护状态	数据泄漏防护组件的状态：*运行中*、*正在启动*、*已停止*、*已暂停*、*失败*、*未知*
协作服务器保护状态	内容过滤组件的状态：*运行中*、*正在启动*、*已停止*、*已暂停*、*失败*、*未知*
邮件服务器的反病毒保护状态	邮件服务器反病毒保护组件的状态：*运行中*、*正在启动*、*已停止*、*已暂停*、*失败*、*未知*
端点传感器状态	Endpoint Detection and Response 组件 (KATA) 的状态：*运行中*、*正在启动*、*已停止*、*已暂停*、*失败*、*未知*
创建日期	<设备名称> 图标的创建时间。此属性用于相互比较各个事件。
虚拟或从属管理服务器名称	虚拟或从属管理服务器名称。该列仅在包含来自不同管理服务器的设备的列表中可用。
父组	<设备名称> 图标所在的管理组的名称。该列仅在包含来自不同管理服务器的设备的列表中可用。
由不同管理服务器管理	该参数可以采用以下值之一： • 如果在设备上远程安装安全应用程序期间，事实证明该设备由其他管理服务器管理，则为 True。 • 否则为 False。
操作系统内部版本	操作系统版本号。您可以指定所选操作系统是否必须具有相等、更早或更晚的版本号。您也可以配置对所有版本号的搜索，除了指定版本号。
操作系统发布 ID	操作系统发布 ID。您可以指定所选操作系统是否必须具有相等、更早或更晚的发布 ID。您也可以配置对所有版本 ID 号的搜索，除了指定的版本 ID 号。

设备、任务和策略的状态

下表包含显示在管理控制台工作区内和控制台树中显示的图标的列表，这些图标位于设备、任务和策略的一旁。这些图标定义了对象的状态。

设备、任务和策略的状态

图标	状态
	在系统中检测到但未包含在任何管理组中的运行工作站操作系统的设备。
	包含在管理组中且工作站操作系统的状态为"*确定*"的设备。

	包含在管理组中且具有工作站操作系统的状态为“*警告*”的设备。
	包含在管理组中且具有工作站操作系统的状态为“*严重*”的设备。
	包含在管理组中且运行工作站操作系统的已丢失管理服务器连接的设备。
	在系统中检测到并且未包含在任何管理组中的运行服务器操作系统的设备。
	包含在管理组中且服务器操作系统的状态为“*确定*”的设备。
	包含在管理组中且具有服务器操作系统的状态为“*警告*”的设备。
	包含在管理组中且具有服务器操作系统的状态为“*严重*”的设备。
	包含在管理组中且运行服务器操作系统的已丢失管理服务器连接的设备。
	网络中检测到、但不包含在任何管理组中的移动设备。
	包含在管理组中且状态为“*确定*”的移动设备
	包含在管理组中且状态为“*警告*”的移动设备
	包含在管理组中且状态为“*严重*”的移动设备
	包含在管理组中的移动设备，与管理服务器丢失了连接。
	网络中检测到、但不包含在任何管理组中的 UEFI 保护设备。UEFI 保护设备在网络中。
	网络中检测到、但不包含在任何管理组中的 UEFI 保护设备。UEFI 保护设备不在网络中。
	包含在管理组中且状态为“*确定*”的 UEFI 保护设备。UEFI 保护设备在网络中。
	包含在管理组中且状态为“*确定*”的 UEFI 保护设备。UEFI 保护设备不在网络中。
	包含在管理组中且状态为“*警告*”的 UEFI 保护设备。UEFI 保护设备在网络中。
	包含在管理组中且状态为“*警告*”的 UEFI 保护设备。UEFI 保护设备不在网络中。
	包含在管理组中且状态为“*严重*”的 UEFI 保护设备。UEFI 保护设备在网络中。
	包含在管理组中且状态为“*严重*”的 UEFI 保护设备。UEFI 保护设备不在网络中。
	活动策略。
	非活动策略。
	从主管理服务器上创建的组中继承的活动策略。
	从顶级组继承的活动策略。
	状态为“*已计划*”或“*成功完成*”的任务（组任务、管理服务器任务或特定设备的任务）。
	状态为“*运行中*”的任务（组任务、管理服务器任务或特定设备的任务）。
	状态为“*失败*”的任务（组任务、管理服务器任务或特定设备的任务）。
	从主管理服务器上创建的组中继承的任务。
	从顶级组继承的任务。

管理控制台上的文件状态图标

为便于 Kaspersky Security Center 管理控制台中的文件管理，图标显示在文件名称旁边（见下表）。图标显示了客户端设备上 Kaspersky 应用程序分配给文件的状态。图标显示在“**隔离**”、“**备份**”和“**活动威胁**”文件夹的工作区。

状态由安装到客户端设备上的 Kaspersky Endpoint Security 分配到对象。

图标和文件状态的一致性

图标	状态
	带有“*被感染*”状态的文件。
	带有“*警告*”或“*疑似被感染*”状态的文件。
	具有*由用户添加*状态的文件。
	具有*误报*状态的文件。
	带有“*已清除*”状态的文件。
	带有“*已删除*”状态的文件。
	“**隔离**”文件夹中带有“*未感染*”、“*密码保护*”或“*必须被发送到卡巴斯基*”状态的文件。如果图标旁边没有状态描述，这意味着客户端设备上受管理的 Kaspersky 应用程序已经报告了未知状态到 Kaspersky Security Center。
	“**备份**”文件夹中带有“*未感染*”、“*密码保护*”或“*必须被发送到卡巴斯基*”状态的文件。如果图标旁边没有状态描述，这意味着客户端设备上受管理的 Kaspersky 应用程序已经报告了未知状态到 Kaspersky Security Center。
	“**活动威胁**”文件夹中带有“*未感染*”、“*密码保护*”或“*必须被发送到卡巴斯基*”状态的文件。如果图标旁边没有状态描述，这意味着客户端设备上受管理的 Kaspersky 应用程序已经报告了未知状态到 Kaspersky Security Center。

搜索和导出数据

该部分包含数据搜索方法和导出数据的信息。

查找设备

Kaspersky Security Center 允许您按照指定规则查找设备。搜索结果可保存至文本文件。

搜索功能允许您查找以下设备：

- 管理服务器及其从属服务器的管理组中的客户端设备。
- 管理服务器及其从属服务器管理的未分配的设备。

若要查找管理组中的客户端设备，请执行以下操作：

1. 在控制台树中，选择一个管理组文件夹。
2. 从管理组文件夹的上下文菜单中选择“**搜索**”。
3. 在“**搜索**”窗口的选项卡上，指定搜索设备的条件，并单击“**立即查找**”按钮。

   满足指定搜索条件的设备显示在“**搜索**”窗口底部的表格里。

要查找未分配的设备：

1. 在控制台树中，选择“**未分配的设备**”文件夹。
2. 从“**未分配的设备**”文件夹的上下文菜单中选择“**搜索**”。
3. 在“**搜索**”窗口的选项卡上，指定搜索设备的条件，并单击“**立即查找**”按钮。

   满足指定搜索条件的设备显示在“**搜索**”窗口底部的表格里。

若要不考虑设备是否包括在管理组中而进行搜索，请执行以下操作：

1. 在控制台树中，选择“**管理服务器 %s**”节点。
2. 在节点的上下文菜单中，选择“**搜索**”。
3. 在“**搜索**”窗口的选项卡上，指定搜索设备的条件，并单击“**立即查找**”按钮。

   满足指定搜索条件的设备显示在“**搜索**”窗口底部的表格里。

> 在“**搜索**”窗口，您也可以使用窗口右上角的下拉列表搜索管理组和从属管理服务器。如果已经从“**未分配的设备**”文件夹中打开了“**搜索**”窗口，搜索管理组和从属管理服务器功能将不可用。

要查找设备，您可以在“**搜索**”窗口的字段中使用正则表达式。

可以在“**搜索**”窗口中进行全文搜索：

- 在“**网络**”选项卡的“**描述**”字段
- 在“**硬件**”选项卡的“**设备**”、“**供应商**”和“**描述**”字段

设备搜索设置

以下是关于受管理设备搜索设置的描述。搜索结果显示在窗口的下部。

网络

您可以在“**网络**”选项卡上指定根据网络数据搜索设备所使用的标准：

- **设备名称或 IP 地址**

  设备的 Windows 网络名称（NetBIOS 名称）或者 IPv4 或 IPv6 地址。

- **Windows 域**

  显示指定的 Windows 域中包括的所有设备。

- **管理组**

  显示指定的管理组中包括的设备。

- **描述**

  设备属性窗口中的文本：在“**常规**”区域的“**描述**”字段。
  要描述“**描述**”字段中的文本，您可以使用以下字符：

  - 在单词中：

    - ***。用任意数量的字符替换任何字符串。

    例如：
    要描述单词 **Server** 或 **Server's**，您可以输入 **Server***。

    - **?。**替换任意单个字符。

    例如：
    要描述单词 **Window** 或 **Windows**，您可以输入 **Windo?**。
    星号(*)或问号(?)不能用于查询中的第一个字符。

  - 要查找多个单词：

    - 空格。显示所有在其描述中包含列出的任何单词的设备。

    例如：
    要查找包含“**从属**”或“**虚拟**”单词的短语，可以在查询中包含“**从属 虚拟**”行。

    - **+**。当单词带有加号前缀时，所有搜索结果都将包含该单词。

    例如：
    要查找同时包含“**从属**”和“**虚拟**”的短语，请输入“**+从属+虚拟**”查询。

    - **-**。当单词带有减号前缀时，所有搜索结果都不包含该单词。

    例如：

要查找包含“**从属**”但不包含“**虚拟**”的短语，请输入“**+从属-虚拟**”查询。

- **“<某些文本>”**。引号中围绕的文本必须存在于文本中。

例如：
要查找包含“**从属服务器**”单词组合的短语，可以在查询中输入“**从属服务器**”。

- **IP 范围**

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。
  默认情况下已禁用该选项。

- **由不同管理服务器管理**

  您可以选择以下值之一：
  - **是**。仅被其他管理服务器管理的客户端设备被考虑。
  - **否**。仅考虑由同一管理服务器管理的客户端设备。
  - **未选择值**。将不应用标准。

标签

在“**标签**”选项卡，您可以基于先前添加到受管理设备的描述的关键字（标签）配置设备搜索：

- **如果至少一个指定的标签匹配则应用**

  如果启用此选项，搜索结果将显示包含带有所选标签的描述的设备。
  如果禁用此选项，搜索结果将仅显示包含带有所有标签的描述的设备。
  默认情况下已禁用该选项。

- **必须包含标签**

  如果选择了该选项，搜索结果将显示带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。
  默认情况下已选定该选项。

- **必须排除标签**

  如果选择了该选项，搜索结果将显示不带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

活动目录

在“**活动目录**”选项卡，您可以指定应在 Active Directory 组织单位 (OU) 或组中搜索设备。您还可以在选择中包括来自指定 Active Directory OU 的所有子 OU 的设备。要选择设备，请定义以下设置：

- **设备在活动目录组织单元中**

  如果启用此选项，选择范围将包括输入字段中指定的 Active Directory 组织单元中的设备。
  默认情况下已禁用该选项。

- **包括子组织单元**

  如果启用此选项，选择范围将包括指定域组织单元的所有子组织单元中的设备。
  默认情况下已禁用该选项。

- **该设备是活动目录组成员**

  如果启用此选项，选择范围将包括输入字段中指定的活动目录组中的设备。
  默认情况下已禁用该选项。

网络活动

您可以在“**网络活动**”选项卡上指定根据网络活动搜索设备所使用的标准：

- **该设备是分发点**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **是**。选择范围将包括充当分发点的设备。
  - **否**。选择范围将不包括充当分发点的设备。
  - **未选择值**。将不应用标准。

- **不断开与管理服务器的连接**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **已启用**。分类将包含选中了“**不断开与管理服务器的连接**”复选框的设备。
  - **已禁用**。分类将包含清空了“**不断开与管理服务器的连接**”复选框的设备。
  - **未选择值**。将不应用标准。

- **连接配置文件已切换**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **是**。该分类将包含连接配置文件切换后连接到管理服务器的设备。
  - **否**。该分类将不包含连接配置文件切换后连接到管理服务器的设备。
  - **未选择值**。将不应用标准。

- **上一次连接到管理服务器**

  您可使用此选框设置按上一次连接到管理服务器的时间搜索设备的标准。
  如果选择该选框，则在输入字段中，您可以指定在客户端设备上安装的网络代理和管理服务器之间建立上一次连接的时间间隔（日期和时间）。选择将包括位于指定间隔的设备。
  如果清除此选框，则将不会应用标准。
  默认情况下已清除该选框。

- **网络轮询时检测到新设备**

  搜索最近几天通过网络轮询检测到的新设备。
  如果启用此选项，分类将只包括在“**检测周期 (天)**”字段中指定的天数内通过设备发现检测到的新设备。
  如果禁用此选项，分类将包括通过设备发现检测到的所有设备。
  默认情况下已禁用该选项。

- **设备可见**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **是**。程序在分类中包括网络中当前可见的设备。
  - **否**。应用程序在分类中包括网络中当前不可见的设备。
  - **未选择值**。将不应用标准。

应用程序

您可以在“**应用程序**”选项卡上指定根据所选的受管理应用程序搜索设备所使用的标准：

- **应用程序名称**

  在下拉列表中，可设置按卡巴斯基应用程序名称执行搜索时在分类中包括设备的标准。
  列表仅提供管理员工作站上已安装管理插件的应用程序的名称。
  如果未选择任何应用程序，则将不会应用该标准。

- **应用程序版本**

  在输入字段，可设置按卡巴斯基应用程序版本号执行搜索时在分类中包括设备的标准。

如果未指定版本号，则将不会应用该标准。

- **关键更新名称**

  在输入字段中，可设置按应用程序名称或更新包编号执行搜索时在分类中包括设备的标准。

  如果字段留空，则将不会应用该标准。

- **上一次模块更新**

  您可以使用此选项来设置按这些设备上安装的程序模块上次更新的时间搜索设备的标准。

  如果选中此选框，则您可以在输入字段中指定执行这些设备上安装的程序模块的上一次更新的时间间隔（日期和时间）。

  如果清除此选框，则将不会应用标准。

  默认情况下已清除该选框。

- **设备通过 Kaspersky Security Center 管理**

  在该下拉列表，您可以包含通过 Kaspersky Security Center 管理的设备到分类：

  - **是**。应用程序包含通过 Kaspersky Security Center 管理的设备。
  - **否**。应用程序在分类中包含不通过 Kaspersky Security Center 管理的设备。
  - **未选择值**。将不应用标准。

- **安全应用程序已安装**

  在该下拉列表，您可以包含已安装安全应用程序的设备到分类：

  - **是**。应用程序包含安装了安全应用程序的设备到分类。
  - **否**。应用程序在分类中包含未安装安全应用程序的设备。
  - **未选择值**。将不应用标准。

操作系统

在“**操作系统**”选项卡上，您可以设置以下搜索条件，以根据操作系统类型来搜索设备：

- **操作系统版本**

  如果选中该选框，您可以从列表中选择一个操作系统。安装了指定操作系统的设备会包含在搜索结果中。

- **操作系统 bit 大小**

  在该下拉列表中，可选择操作系统的架构，这将决定将移动规则应用到设备（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。默认情况下，不选择列表中的任何选项，这样就不会对操作系统的架构进行定义。

- **操作系统服务包版本**

  在该字段中，可以指定操作系统的更新包版本（采用 *X.Y* 格式），这将决定将移动规则应用到设备的方式。默认情况下，不指定版本值。

- **操作系统内部版本**

  该设置仅应用到 Windows 操作系统。

  操作系统版本号。您可以指定所选操作系统是否必须具有相等、更早或更晚的版本号。您也可以配置对所有版本号的搜索，除了指定版本号。

- **操作系统发布 ID**

  该设置仅应用到 Windows 操作系统。

  操作系统发布 ID。您可以指定所选操作系统是否必须具有相等、更早或更晚的发布 ID。您也可以配置对所有版本 ID 号的搜索，除了指定的版本 ID 号。

设备状态

在“**设备状态**”选项卡，您可以指定基于受管理应用程序的设备状态搜索设备的标准：

- **设备状态**

  在该下拉列表中，您可以选择下列设备状态之一：“*正常*”、“*严重*”或“*警告*”。

- **实时保护状态**

  您可以在该下拉列表中选择实时保护状态。具有指定实时保护状态的设备将被包括在选择范围中。

- **设备状态描述**

  在该字段中，您可以选中条件旁边的选框，这些条件如果被满足，程序会为设备分配下列状态之一：*正常*、*严重* 或 *警告*。

- **应用程序定义的设备状态**

  您可以在该下拉列表中选择实时保护状态。具有指定实时保护状态的设备将被包括在选择范围中。

保护组件

在“**保护组件**”选项卡上，您可以设置按保护状态搜索客户端设备的标准。

- **数据库发布日期**

  如果选择此选项，您可以按反病毒数据库发布日期搜索客户端设备。在该输入字段中，您可以设置执行搜索的时间间隔。

  默认情况下已禁用该选项。

- **上一次扫描**

  如果启用此选项，您可以按上次恶意软件扫描时间来搜索客户端设备。在该输入字段中，您可以指定执行上一次恶意软件扫描的时段。

  默认情况下已禁用该选项。

- **检测到的威胁总数**

  如果启用此选项，您可以根据发现的病毒数量来搜索客户端设备。在输入字段中，您可以设置发现病毒总数的上限值和下限值。

  默认情况下已禁用该选项。

应用程序注册表

在“**应用程序注册表**”选项卡上，您可以根据设备已安装的应用程序配置设备搜索：

- **应用程序名称**

  在该下拉列表中，您可以选择应用程序。安装有指定应用程序的设备将包括在选择范围中。

- **应用程序版本**

  在该输入字段中，您可以指定选定应用程序的版本。

- **供应商**

  在该下拉列表中，您可以选择已安装应用程序的生产商。

- **应用程序状态**

  在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

- **根据更新查找**

  如果启用此选项，则搜索操作将使用相关设备内应用程序更新的有关信息来执行。选中复选框后，“**应用程序名称**”、“**应用程序版本**”和“**应用程序状态**”字段将分别更改为“**更新名称**”、“**更新版本**”和“**状态**”。

  默认情况下已禁用该选项。

- **不兼容的安全应用程序名称**

  在该下拉列表中，您可以选择第三方安全应用程序。在搜索过程中，安装有指定程序的设备将包括在选择范围中。

- **应用程序标签**

  在该下拉列表中，您可以选择应用程序标签。所有安装了描述中带有所选标签的应用程序的设备都被包含在设备分类。

管理服务器层级

如果要在搜索设备时考虑存储在从属管理服务器上的信息，请在“**管理服务器层级**”选项卡上，选中“**包含来自从属管理服务器(等级)的数据**”框，然后在输入字段，您可以指定搜索设备时考虑其信息的从属管理服务器的嵌套级别。默认情况下已清除该选框。

虚拟机

在“**虚拟机**”选项卡，您可以根据它们是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来配置设备搜索：

- **这是一台虚拟机**

  在该下拉列表中，您可以选择以下选项：

  - **不重要**。
  - **否**。查找非虚拟机设备。
  - **是**。查找虚拟机设备。

- **虚拟机类型**

  在该下拉列表中，您可以选择虚拟机生产商。

  如果在“**这是一台虚拟机**”下拉列表中选择了“**是**”或“**不重要**”值，则该下拉列表可用。

- **虚拟桌面基础架构的一部分**

  在该下拉列表中，您可以选择以下选项：

  - **不重要**。
  - **否**。查找不属于虚拟桌面基础架构的设备。
  - **是**。查找术语虚拟桌面基础架构 （VDI） 一部分的设备。

硬件

在“**硬件**”选项卡上，您可以配置如何根据硬件搜索客户端设备：

- **设备**

  在该下拉列表中，您可以选择单元类型。所有带有该单元的设备被包含在搜索结果。
  该字段支持完整文本搜索。

- **供应商**

  在该下拉列表中，您可以选择单元生产商的名称。所有带有该单元的设备被包含在搜索结果。
  该字段支持完整文本搜索。

- **描述**

  设备或硬件单元的描述。带有该字段中指定的描述的设备将包括在分类范围内。
  可在设备的属性窗口输入任何格式的设备描述。该字段支持完整文本搜索。

- **清单号**

  带有该字段中指定的清单编号的设备将包括在选择范围内。

- **CPU 频率 (MHz)**

  CPU 的频率范围。CPU 与这些输入字段（含）中频率范围匹配的设备将包括在分类范围内。

- **虚拟 CPU 内核**

  CPU 中虚拟核心的数量范围。CPU 与这些输入字段（含）中范围匹配的设备将包括在分类范围内。

- **硬盘卷(GB)**

  设备硬盘容量值的范围。硬盘与这些输入字段（含）中范围匹配的设备将包括在分类范围内。

- **内存大小(MB)**

  设备 RAM 大小的值范围。 RAM 与这些输入字段中的范围（含）匹配的设备将包含在分类中。

漏洞和更新

在“**漏洞和更新**”选项卡，您可以设置根据其 Windows 更新源搜索设备的标准：

- **WUA 已切换到管理服务器**

  您可以在下拉列表中选择以下搜索选项之一：
  - **是**。如果选中该选项，搜索结果会包含从管理服务器收到 Windows Update 更新的设备。
  - **否**。如果选中该选项，搜索结果将包含从其它源收到 Windows Update 更新的设备。

用户

在“**用户**”选项卡，您可以设置根据登录到操作系统的用户账户搜索设备的标准。

- **最后一次登录系统的用户**

  如果启用此选项，单击“**浏览**”按钮可以指定用户账户。搜索结果包含其上一次登录用户为指定用户的设备。

- **登录系统至少一次的用户**

  如果启用此选项，单击“**浏览**”按钮可以指定用户账户。搜索结果包含指定用户至少登录一次的设备。

影响受管理应用程序状态的问题

在“**影响受管理应用程序状态的问题**”选项卡，您可以设置根据由受管理应用程序提供的状态描述搜索设备：

- **设备状态描述**

  您可以选择受管理应用程序状态描述的复选框；接收这些状态时，设备将被包含在分类。当您选择几个应用程序的状态时，您可以选择在所有列表中自动选择该状态。

受管理应用程序组件的状态

在“**受管理应用程序组件的状态**”选项卡，您可以设置根据受管理应用程序组件的状态搜索设备的标准：

- **数据泄漏防护状态**

  根据数据泄漏防护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- **协作服务器保护状态**

  根据服务器协作保护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- **邮件服务器的反病毒保护状态**

  根据邮件服务器保护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）*搜索设备。*

- **端点传感器状态**

  根据端点传感器组件状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

加密

- **加密**

  高级加密标准(AES)对称分组密码算法。在下拉列表中，您可以选择加密密钥大小(56 位、128 位、192 位或 256 位)。

  可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

云段

在“**云段**”选项卡，您可以基于设备是否属于特定云段来配置搜索：

- **设备在云段中**

  如果启用此选项，您可以单击“**浏览**”按钮以指定要搜索的段。

  如果还启用“**包含子对象**”选项，将在指定段的所有子对象上运行搜索。

  搜索结果仅包含所选段的设备。

- **使用 API 发现的设备**

  在下拉列表，您可以选择设备是否由 API 工具检测：

  - **AWS**。设备使用 AWS API 发现，即设备确定在 AWS 云环境中。
  - **Azure**。设备使用 Azure API 发现，即设备确定在 Azure 云环境中。
  - **Google Cloud。**设备使用 Google API 发现，即设备确定在 Google Cloud 环境中。
  - **否**。无法使用 AWS API、Azure API 或 Google API 检测到该设备，即设备位于云环境之外，或者位于云环境中，但是无法使用 API 检测到该设备。
  - **没有值**。此条件不适用。

应用程序组件

该区域包含了在管理控制台中安装了管理插件的这些应用程序的组件列表。

在“**应用程序组件**”区域，您可以指定根据所选应用程序组件的状态和版本号包含设备到分类的标准：

- **状态**

  根据应用程序发送到管理服务器的组件状态搜索设备。您可以选择以下状态之一：*设备上无数据*、*已停止*、*正在启动*、*已暂停*、*运行中*、*故障*或*未安装*。如果安装在受管理设备上的应用程序的所选组件具有指定状态，设备被包含到设备分类。

  由应用程序发送的状态：

  - *正在启动* - 组件处于初始化进程中。
  - *运行中* - 组件被启用且在正常工作。
  - *已暂停* - 组件被暂停，例如，在用户在受管理应用程序上停止了保护后。
  - *故障* - 组件操作中发生错误。
  - *已停止* - 组件被禁用且不在工作。
  - *未安装* - 当配置应用程序自定义安装时，用户未选择该组件以安装。

  不同于其他状态，*设备上无数据*状态不由应用程序发送。该选项显示应用程序没有所选组件状态的信息。例如，这可能发生在所选组件不属于任何在设备上安装的应用程序时，或设备关闭时。

- **版本**

  根据您在列表中选择的版本号搜索设备。您可以输入版本号，例如 `3.4.1.0`，然后指定所选组件是否必须具有相同、更早或更新版本。您也可以配置对除指定版本外的所有版本进行搜索。

在字符串变量中使用掩码

允许在字符串变量中使用掩码。创建掩码时，您可以使用以下常规表达式：

- 通配符 （*） – 任意零个或更多字符串。
- 问号 （?） – 任意单个字符。
- [<range>] – 指定范围或集合中的任意单个字符。
  例如：[0–9]–任意数字。[abcdef] - 任何字符 a、b、c、d、e 或 f。

在搜索字段使用正则表达式

你可以在搜索字段使用以下正则表达式来搜索特别字和字符：

- *.代替任何字母序列。若要搜索 Server，Servers，或 Server room，在搜索区域输入 `Server*` 表达式。
- ?。替换任意单个字符。若要搜索 Word 或 Ward，在搜索区域输入 `W?rd` 来表示。

  > 搜索区域的文本不能以问号（?）开头。

- [<range>]。从指定的范围或集合中替换任意单个字符。若要搜索任何数字，在搜索区域输入 `[0-9]` 来表示。若要搜索字母中的一个—a, b, c, d, e, or f—在搜索区域输入 `[abcdef]` 来表示。

在搜索区域使用下面的常规表达式来进行全文本搜索：

- 空格。结果是所有在其描述中包含列出的任何单词的设备。例如，若要搜索短语包含“Secondary”或“Virtual”（或两个都包含），在搜索区域输入“`Secondary Virtual`”表达式。
- 加号 （+）, AND 或 &&。当单词带有加号前缀时，所有搜索结果都将包含该单词。例如，若要搜索包含“Secondary”和“Virtual”的短语，您可以在搜索字段输入以下任意表达式：`+Secondary+Virtual`、`Secondary AND Virtual`、`Secondary && Virtual`。
- OR 或 ||。当放在两个词中间时，它表示可以在文本中找到一个词或另一个词。若要搜索包含“Secondary”或“Virtual”的短语，您可以在搜索字段输入以下任意表达式：`Secondary OR Virtual`、`Secondary || Virtual`。
- 减号 （-）。当单词带有减号前缀时，所有搜索结果都不包含该单词。若要搜索必须包含“Secondary”但不得包含“Virtual”的短语，必须在搜索区域中输入表达式 `+Secondary-Virtual`。
- `"<某些文本>"`。引号中围绕的文本必须存在于文本中。若要搜索短语包含 Secondary Server，您必须在搜索区域输入 `" Secondary Server "` 来表示。

全文本搜索在下面的过滤块可用：

- 在事件列表过滤块中，根据“**事件**”和“**描述**”列进行过滤。
- 在用户账户过滤块，根据“**名称**”列进行过滤。
- 在应用程序注册表过滤块中，如果“**显示在列表**”区域选择了“**不分组**”作为过滤条件，则根据“**名称**”列进行过滤。

从对话框导出列表

在应用程序对话框，您可以导出对象列表到文本文件。

对象列表的导出可以使用对话框区域的“**导出到文件**”按钮。

任务设置

该区域列出了 Kaspersky Security Center 中任务的所有设置。

常规任务设置

本部分包含您可以查看并为大多数任务配置的设置。可用设置列表取决于您正在配置的任务。

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- 操作系统重启设置：
  - **不重启设备**

    客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

  - **重启设备**

    如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

  - **提示用户操作**

    客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

    默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

- 任务计划设置：

  计划的类型可能根据任务而有所不同。

  - **计划开始设置：**

    - **每 N 小时**

      任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

      默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

    - **每 N 天**

      任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

      默认下，任务每天运行一次，从当前系统日期和时间开始。

    - **每 N 分钟**

      任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

      默认下，任务每 30 分钟运行一次，从当前系统时间开始。

    - **按星期中的天数**

      任务在每周指定日期的指定时间定期运行。

      默认情况下，任务在每周五 6:00:00 PM 运行。

    - **每月**

      任务定期运行，在指定月日的指定时间。

      在缺少指定日的月份，任务在最后一天运行。

      默认下，任务在每月的第一天运行，在当前系统时间。

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **一次**

  该任务在指定的日期和时间运行一次（默认情况下，在创建任务的当天）。

- **立即**

  任务在设置保存后立即运行。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **当新更新下载至存储库时**

  当新更新下载至存储库后任务运行。例如，您可能想要对“查找漏洞和所需更新”任务使用该计划。

- **在检测到病毒爆发时**

  任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

- 在搜索栏中输入任务名称，即可根据名称搜索任务。
- 单击排序图标可按名称对任务进行排序。
  默认情况下，任务按字母顺序升序排列。
- 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动随机延迟间隔(分钟)**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- 要分配任务的设备：

  - **选择管理服务器检测到的网络设备**

    任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。

    例如，您可能要在安装网络代理到未分配的设备的任务中使用该选项。

  - **手动指定设备地址或从列表导入地址**

    您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- **分配任务到设备分类**

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。

  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

- **分配任务到管理组**

  任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

  例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

  如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

- 账户设置：

  - **默认账户**

    在与执行该任务的应用程序相同的账户下运行该任务。

    默认情况下已选定该选项。

  - **指定账户**

    填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - **账户**

    运行该任务的账户。

  - **密码**

    任务运行时使用的账户的密码。

如果您的目标设备上未安装网络代理，则必须指定在目标设备上用于访问 admin$ share 的账户。您指定的账户仅用于将数据复制到您的设备。如果您的目标设备上安装了网络代理，则数据将通过网络代理进行复制，您在创建任务时无需指定任何账户。

任务创建后指定的设置

您可以在创建任务后指定以下设置。

- 组任务设置：
  - **分发到子组**

    此选项仅在组任务的设置中可用。
    启用此选项后，任务范围包括：
    - 您在创建任务时选择的管理组。
    - 从属于按组层次结构向下的任何级别的选定管理组的管理组。

    禁用此选项后，任务范围仅包括您在创建任务时选择的管理组。
    默认情况下已启用该选项。

  - **分发到从属和虚拟管理服务器**

    启用此选项后，在主管理服务器上有效的任务也将应用于从属管理服务器（包括虚拟管理服务器）。如果从属管理服务器上已经存在相同类型的任务，则两个任务都将应用于从属管理服务器–现有任务和从主管理服务器继承的任务。
    仅当启用“**分发到子组**”选项时，此选项才可用。
    默认情况下已禁用该选项。

- 高级计划设置：
  - **使用 Wake-On-LAN 功能在任务启动之前开启设备(分钟)**

    设备上的操作系统在任务开始之前的指定时间启动。默认时间段为五分钟。

    如果您想要任务在任务范围内的所有客户端设备上运行，包括任务要启动时关闭的设备，则启用该选项。

    如果您希望在任务完成后自动关闭设备，请启用“**任务完成后关闭设备**”选项。可以在同一窗口中找到此选项。

    默认情况下已禁用该选项。

  - **任务完成后关闭设备**

    例如，您可能想为每周五工作时间后安装更新到客户端设备的更新安装任务启用该选项，然后在周末关闭这些设备。

    默认情况下已禁用该选项。

  - **如果任务运行超过该时间则停止(分钟)**

    在指定时间段过后，任务被自动停止，无论它是否完成。
    如果您想要中断或停止执行时间太长的任务，则启用该选项。

默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

- 通知设置：
  - **保存任务历史记录**块：
    - **在管理服务器上(天)**

      有关任务范围内所有客户端设备上的任务执行的应用程序事件在指定的天数内被存储在管理服务器。当该时间段过后，信息被从管理服务器删除。

      默认情况下已启用该选项。

    - **存储在设备的 OS 事件日志中**

      有关任务执行的应用程序事件被存储在每个客户端设备的本地 Windows 事件日志中。

      默认情况下已禁用该选项。

    - **存储在管理服务器的 OS 事件日志中**

      有关任务范围内所有客户端设备上的任务执行的应用程序事件被集中存储在管理服务器操作系统的 Windows 事件日志中。

      默认情况下已禁用该选项。

    - **保存所有事件**

      如果选择该选项，所有任务相关事件被保存到事件日志。

    - **保存任务进度相关事件**

      如果选择该选项，仅任务执行相关事件被保存到事件日志。

    - **仅保存任务执行结果**

      如果选择该选项，仅任务结果相关事件被保存到事件日志。

  - **通知管理员任务执行的结果**

    您可以选择管理员接收任务执行通知的方法：通过电子邮件、通过 SMS 和通过运行可执行文件。要配置通知，请单击“**设置**”链接。

    默认下，所有通知方法被禁用。

  - **仅通知错误**

    如果该选项被启用，管理员仅在任务执行完成但带有错误时被通知。

    如果该选项被禁用，管理员在每次任务执行完成后被通知。

默认情况下已启用该选项。

- 安全设置
- 任务范围设置：

  取决于任务范围决定的方式，以下设置被展现：

  - **设备**

    如果任务范围由管理组决定，您可以查看该组。这里不可以更改。然而，您可以设置**任务范围排除项**。

    如果任务范围由设备列表决定，您可以通过添加和删除设备修改该列表。

  - **设备分类**

    您可以更改应用程序任务的设备分类。

  - **任务范围排除项**

    您可以指定应用任务的设备组。要排除的组仅可以是应用任务的管理组的子组。

- **修订历史**

“将更新下载至管理服务器存储库”任务设置

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- **更新源**

  以下资源可以用作管理服务器的更新源：

  - 卡巴斯基更新服务器

    Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

    默认选择。

  - 主管理服务器

    此资源适用于为从属或虚拟管理服务器创建的任务。

  - 本地或网络文件夹

    包含最新更新的本地或网络文件夹。网络文件夹可以是 FTP 或 HTTP 服务器，或者 SMB 共享。如果网络文件夹需要身份验证，则仅支持 SMB 协议。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

更新源所使用的 FTP 或 HTTP 服务器或网络文件夹必须包含匹配 Kaspersky 更新服务器所创建的结构的文件夹结构（带有更新）。

- **其他设置**

  强制从属管理服务器更新

  如果启用该选项，当新更新下载后管理服务器立刻在从属管理服务器上启动更新任务。更新任务通过使用在从属管理服务器上的任务属性中配置的更新源来启动。

  如果禁用此选项，从属管理服务器上的更新任务将根据计划启动。

  默认情况下已禁用该选项。

  复制下载的更新到附加文件夹

  管理服务器接收更新后，它复制它们到指定文件夹。如果您想要在您的网络上手动管理更新的分发，则使用该选项。

  例如，您可能要在以下情况下使用该选项：您组织的网络包含几个独立子网，且每个子网的设备不能访问其他子网。然而，所有子网中的设备都可以访问通用网络共享。此种情况下，您在子网之一设置管理服务器从 Kaspersky 更新服务器下载更新，启用该选项，然后指定该网络共享。对于其他管理服务器的“将更新下载至存储库”任务中，指定与更新源相同的网络共享。

  如果您选择将下载的更新复制到本地文件夹，则必须在已安装管理服务器的设备上指定文件夹。文件夹路径取决于设备的操作系统。由于本地文件夹位于基于 Linux 的管理服务器上，因此您必须指定 POSIX 路径，例如 /path/to/dir。

  选择位于基于 Linux 的管理服务器上的网络文件夹时，您必须预先确保已安装管理服务器的设备可以通过挂载该文件夹来访问该网络文件夹。对文件夹的访问使用 SMB 协议执行。

  默认情况下已禁用该选项。

  在复制完成之前不强制更新设备和从属管理服务器

  下载更新到客户端设备和从属管理服务器任务仅在这些更新从主更新文件夹被复制到附加更新文件夹后才启动。

  如果客户端设备和从属管理服务器从附加网络文件夹下载更新，则必须启用该选项。

  默认情况下已禁用该选项。

任务创建后指定的设置

您可以在创建任务后指定以下设置。

- “**设置**”区域，“**更新内容**”块。

  下载差异文件

  该选项启用下载 diff 文件功能。

  默认情况下已禁用该选项。

- **更新验证**区域

  分发前验证更新

  管理服务器从源下载更新并将其保存到临时存储库，然后运行“**更新验证任务**”字段中定义的任务。如果任务成功完成，则将更新从临时存储库复制到管理服务器上的共享文件夹，然后分发到所有将管理服务器作为更新源的设备（启动具有“**当新更新下载至存储库时**”计划类型的任务）。只有在执行“*更新验证*”任务之后，将更新下载至存储库的任务才完成。

  默认情况下已禁用该选项。

  更新验证任务

  该任务在更新被分发到所有以管理服务器作为更新源的设备之前验证更新。

  在此字段中，可以指定先前创建的“*更新验证*”任务。或者，您可以创建新的“*更新验证*”任务。

“将更新下载至分发点存储库”任务设置

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- **更新源**

  以下资源可以用作分发点的更新源：

  - Kaspersky 更新服务器

    Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

    默认情况下已选中该选项。

  - 主管理服务器

    此资源适用于为从属或虚拟管理服务器创建的任务。

  - 本地或网络文件夹

    包含最新更新的本地或网络文件夹。网络文件夹可以是 FTP 或 HTTP 服务器，或者 SMB 共享。如果网络文件夹需要身份验证，则仅支持 SMB 协议。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

    更新源所使用的 FTP 或 HTTP 服务器或网络文件夹必须包含匹配 Kaspersky 更新服务器所创建的结构的文件夹结构（带有更新）。

- **其他设置 → 更新存储文件夹**

  用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

任务创建后指定的设置

您可以在**设置**区域的**更新内容**块中指定以下设置，仅可在创建任务后指定。

下载差异文件

该选项启用下载 diff 文件功能。
默认情况下已禁用该选项。

“查找漏洞和所需更新”任务设置

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- **搜索 Microsoft 列出的漏洞和更新**

  当搜索漏洞和更新时，Kaspersky Security Center 使用当前可用的 Microsoft 更新源中有关适用 Microsoft 更新的信息。
  例如，如果您有带有不同 Microsoft 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。
  默认情况下已启用该选项。
  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

  - **连接更新服务器更新数据**

    受管理设备上的“Windows 更新代理”连接到 Microsoft 更新源。以下服务器可以充当 Microsoft 更新源：

    - Kaspersky Security Center 管理服务器（请参阅网络代理策略的设置）
    - 在组织网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows 服务器
    - Microsoft 更新服务器

    如果启用该选项，受管理设备上的 Windows 更新代理将连接到 Microsoft 更新源以刷新适用 Microsoft Windows 更新的信息。

    如果禁用此选项，受管理设备上的 Windows 更新代理将使用以前从 Microsoft 更新源所收到的适用 Microsoft Windows 更新的信息。

    到 Microsoft 更新源的连接可能消耗资源。如果在其他任务中或网络代理策略属性中设置了到该更新源的常规连接，则您可能想要在“**软件更新和漏洞**”区域禁用此选项。如果您不想禁用此选项，则为了减少服务器过载，您可以配置任务计划以随机分配任务启动延迟（不超过 360 分钟）。

    默认情况下已启用该选项。

网络代理策略设置的以下选项的组合定义了获取更新的方式：

- 仅当在**查找漏洞和所需更新连接更新服务器更新数据任务的属性中**启用了*连接到更新服务器以更新数据查找漏洞和所需更新*选项，并且在网络代理策略的设置中**Windows Update 搜索模式**选项被设置为**主动**时，受管理设备上的 Windows 更新代理才会连接到更新服务器以获取更新 。
- 如果您在执行*漏洞扫描*任务时不需要网络代理发起与 Microsoft Windows 更新源的连接并下载更新，您可以将**Windows Update 搜索模式**选项设置为**被动**，同时**连接更新服务器更新数据**选项必须保持启用。这使您可以节省资源并使用以前收到的 Windows 更新来扫描漏洞。如果您以不同的方式配置接收 Microsoft Windows 更新，则可以使用被动模式。如果没有以其他方式配置接收 Microsoft Windows 更新，请不要将**Windows Update 搜索模式**选项设置为**被动**，因为在这种情况下，将永远不会收到有关更新的信息。
- 不管“**连接更新服务器更新数据**”选项的状态如何（启用或禁用），如果“**Windows Update 搜索模式**”选项被设置为“**已禁用**”，Kaspersky Security Center 不会请求有关更新的任何信息。

- **搜索卡巴斯基列出的第三方漏洞和更新**

  如果启用该选项，Kaspersky Security Center 在 Windows 注册表和“**指定文件系统中应用程序高级搜索的路径**”下指定的文件夹中搜索漏洞和第三方应用程序所需更新（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）。支持的第三方应用程序的完整列表由 Kaspersky 管理。

  如果禁用该选项，Kaspersky Security Center 不为第三方应用程序查找漏洞和所需更新。例如，如果您有带有不同 Microsoft Windows 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

  - **指定文件系统中应用程序高级搜索的路径**

    Kaspersky Security Center 搜索需要修复漏洞和安装更新的第三方应用程序。您可以使用系统变量。

    指定应用程序安装文件夹。默认下，列表包含大多数应用程序所安装的系统文件夹。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

  - **高级诊断文件的最大大小，MB**

    默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

“安装所需更新并修复漏洞”任务设置

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- **指定更新安装规则**

  这些规则被应用到客户端设备上的更新安装。如果规则未被指定，任务无可执行。对于使用规则操作的信息，请参考更新安装规则。

- **在设备重启或关闭时开始安装**

  如果启用该选项，更新在设备被重启或关闭时安装。否则，更新根据计划安装。

  如果安装更新可能影响设备性能则使用该选项。

  默认情况下已禁用该选项。

- **安装所需的常规系统组件**

  如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

  如果禁用该选项，您可能必须手动安装先决条件。

  默认情况下已禁用该选项。

- **更新过程中允许安装新应用程序版本**

  如果启用该**选项**，如果更新导致软件应用程序新版本的安装，更新将被允许。

  如果禁用该选项，软件不被升级。您可以稍后手动或通过其他任务安装软件的新版本。例如，如果公司基础架构不被新软件版本支持，或者如果您想要在测试基础架构中检查升级，您可能使用该选项。

  默认情况下已启用该选项。

  升级应用程序可能导致安装在客户端设备上的独立应用程序功能异常。

- **下载更新到设备而不安装**

  如果启用该选项，应用程序下载更新到设备但是不自动安装它们。您可以稍后手动安装下载的更新。

  Microsoft 更新被下载到系统 Windows 存储。第三方应用程序更新（由非 Kaspersky 和 Microsoft 软件供应商开发的应用程序）将会下载到“**下载更新到**”字段中指定的文件夹中。

  如果禁用该选项，更新被自动安装到设备。

默认情况下已禁用该选项。

- **下载更新到**

  该文件夹用于下载第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

任务创建后指定的设置

您仅可在创建任务后指定以下所列区域的设置。有关任务设置的完整说明，请参阅一般任务设置。

- **常规**。此区域会显示有关任务的一般信息。此外，您还可以指定哪些设备应适用*安装所需更新并修复漏洞*任务：

  - **分发到子组**

    此选项仅在组任务的设置中可用。

    启用此选项后，任务范围包括：

    - 您在创建任务时选择的管理组。
    - 从属于按组层次结构向下的任何级别的选定管理组的管理组。

    禁用此选项后，任务范围仅包括您在创建任务时选择的管理组。

    默认情况下已启用该选项。

  - **分发到从属和虚拟管理服务器**

    启用此选项后，在主管理服务器上有效的任务也将应用于从属管理服务器（包括虚拟管理服务器）。如果从属管理服务器上已经存在相同类型的任务，则两个任务都将应用于从属管理服务器—现有任务和从主管理服务器继承的任务。

    仅当启用“**分发到子组**”选项时，此选项才可用。

默认情况下已禁用该选项。

- 要安装的更新

  在“**要安装的更新**”区域，您可以查看任务安装的更新列表。仅匹配应用的任务设置的更新被显示。

- 更新的安装测试：

  - **不扫描**。如果您不希望执行更新的测试安装，请选择该选项。
  - **在选定设备上运行扫描**。如果要在选定设备上测试更新安装，请选择该选项。单击“**添加**”按钮，然后选择您需要在其上执行更新测试安装的设备。
  - **在指定组中的设备上运行扫描**。如果要在一组设备上测试更新安装，请选择该选项。在“**指定测试组**”字段中，指定您要在其上执行测试安装的设备组。
  - **在指定百分比的设备上运行扫描**。如果要在一部分设备上测试更新安装，请选择该选项。在“**所有目标设备中测试设备的百分比**”字段中，指定您要在其上执行更新测试安装的设备的百分比。

子网全局列表

该区域提供您在规则中可以使用的子网全局列表。

要存储您的网络中的子网信息，您可以为您使用的每个管理服务器设置子网全局列表。该列表帮助您匹配对（IP 地址、掩码）和物理单元，例如分支办公室。您可以在网络规则和设置中使用该列表中的子网。

添加子网到子网全局列表

您可以添加子网和其描述到子网全局列表。

要添加子网到子网全局列表：

1. 在控制台树中，选择您需要的管理服务器节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在打开的“**属性**”窗口中，在“**区域**”窗格选择“**全局子网列表**”。
4. 单击“**添加**”按钮。

   “**新子网**”窗口将开启。
5. 填充以下字段：

   - **常规设置**

     您正添加的子网的子网 IP 地址。

- **子网掩码**

  您正添加的子网的子网掩码。

- **名称**

  子网名称。它必须在子网全局列表中唯一。如果您输入列表中已有的名称，索引将被添加，例如：~~1、~~2。

- **描述**

  描述可能包含一些具有此子网的分支办公室的附加信息。该文本将出现在子网所在的所有列表，例如，在流量限制规则列表。

  该字段不是必须的且可以为空。

6. 单击“**确定**”。

子网出现在子网列表。

在子网全局列表中查看和修改子网属性

您可以在子网全局列表中查看和修改子网属性。

要在子网全局列表中查看和修改子网属性：

1. 在控制台树中，选择您需要的管理服务器节点。
2. 在管理服务器的上下文菜单中，选择“**属性**”。
3. 在打开的**属性**窗口中，在左侧“**区域**”窗格选择“**全局子网列表**”。
4. 在列表，选择您要的子网。
5. 单击“**属性**”按钮。
   “**新子网**”窗口将开启。
6. 如果必要，更改子网设置。
7. 单击“**确定**”。

如果您已做了更改，它们将被存储。

Windows、Linux 和 macOS 网络代理的使用：比较

网络代理的使用取决于设备的操作系统。网络代理策略和安装包设置也根据操作系统不同而不同。下表比较了适用于 Windows、macOS 和 Linux 操作系统的网络代理的功能和使用方案。

网络代理功能	Windows	Linux	macOS
安装			
安装 Kaspersky Security Center 后自动生成网络代理安装包	✓	—	—
在强制模式下安装，使用 Kaspersky Security Center 远程安装任务中的特殊选项	✓	✓	✓
通过向设备用户发送 Kaspersky Security Center 生成的独立包链接来进行安装	✓	✓	✓
通过使用 Kaspersky Security Center 提供的用于处理磁盘镜像的工具，克隆带有操作系统和网络代理的管理员硬盘驱动器镜像进行安装	✓	—	—
通过使用第三方工具克隆带有操作系统和网络代理的管理员硬盘驱动器镜像进行安装	✓	✓	✓
使用用于远程安装应用程序的第三方工具进行安装	✓	✓	✓
通过在设备上运行应用程序安装程序来手动安装	✓	✓	✓
在静默模式下安装网络代理	✓	✓	✓
手动连接客户端设备至管理服务器。klmover 实用程序	✓	✓	✓
自动安装 Kaspersky Security Center 组件的更新和补丁	✓	✓	—
自动分发密钥	✓	✓	✓
强制同步	✓	✓	✓
分发点			
用作分发点	✓	✓	✓
自动分配分发点	✓	✓ 不使用网络定位感知 (NLA)。	✓ 不使用网络定位感知 (NLA)。
网络轮询	✓ • Windows 网络轮询 • IP 范围轮询 • 域控制器轮询（Microsoft Active Directory）	✓ • IP 范围轮询 • Zeroconf 轮询 • 域控制器轮询（Microsoft Active Directory、Samba 4 Active Directory）	—
在分发点端运行 KSN 代理服务	✓	✓	—
通过卡巴斯基更新服务器将更新下载到将更新分发到受管理设备的分发点存储库	✓	✓	— （如果一个或多个运行 Linux 或 macOS 的设备在“将更新下载至分发点存储库”任务范围内，则该任务将以“失败”状态完成，即使该任务在所有 Windows 设备上均已成功完成。）
推送应用程序安装	✓	受限制：无法使用 Linux 分发点在 Windows 设备上执行推送安装。	受限制：无法使用 macOS 分发点在 Windows 设备上执行推送安装。
用作推送服务器	✓	✓	—
处理第三方应用程序			
在设备上远程安装应用程序	✓	—	✓ 请参阅以下文章了解详细信息：在 macOS 设备上远程安装应用程序。

网络代理功能	Windows	Linux	macOS
软件更新	✓	—	—
在网络代理策略中配置操作系统更新	✓	—	—
查看软件漏洞信息	✓	—	—
扫描应用程序以查找漏洞	✓	—	—
清查设备上所安装的软件	✓	✓	—
虚拟机			
在虚拟机上安装网络代理	✓	✓	✓
虚拟桌面基础架构 (VDI) 的优化设置	✓	✓	✓
对动态虚拟机的支持	✓	✓	✓
其他			
使用 Windows 桌面共享来审核远程客户端设备上的操作	✓	—	—
监控反病毒保护状态	✓	✓	✓
管理设备重启	✓	—	—
支持文件系统回滚	✓	✓	✓
使用网络代理作为连接网关	✓	✓	✓
连接管理器	✓	✓	✓
网络代理从一个管理服务器切换到另一个管理服务器（根据网络位置自动切换）	✓	—	✓
检查客户端设备与管理服务器之间的连接。klnagchk 实用程序	✓	✓	✓
远程连接至客户端设备桌面	✓	—	✓ 通过使用虚拟网络计算 (VNC) 系统。
通过迁移向导下载独立安装包	✓	✓	✓
Zeroconf 轮询	—	✓	—
查看客户端设备硬件的信息	✓	✓ 安装在这些设备上的网络代理发送给管理服务器的 Linux 设备硬件信息仅限于管理控制台和Kaspersky Security Center Web Console的受管理设备设置描述中指定的信息。	✓ 安装在这些设备上的网络代理向管理服务器发送的 macOS 设备硬件信息仅限于管理控制台和Kaspersky Security Center Web Console的受管理设备设置描述中指定的信息。

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console （以下也称为 Kaspersky Security Center Web Console）是一个 Web 应用程序，设计用于管理由卡巴斯基应用程序保护的网络的安全系统状态。

使用该应用程序，您可以执行以下操作：

- 管理组织的安全系统状态。
- 将 Kaspersky 应用程序安装到您网络上的设备并管理已安装的应用程序。
- 管理为您网络中的设备所创建的策略。
- 管理用户账户。
- 管理安装在您的网络设备上的应用程序任务。
- 查看有关安全系统状态的报告。
- 管理向系统管理员和其他 IT 专家传送报告的行为。

有关硬件和软件要求的信息，请参阅Web Console 要求。

Kaspersky Security Center Web Console 是一个网络接口，可确保您的设备和管理服务器能够通过浏览器进行通信。管理服务器是一个旨在对您网络中的设备上安装的 Kaspersky 应用程序进行管理的应用程序。管理服务器通过受安全套接字层 （SSL） 保护的通道连接到您的网络的设备。当您使用您的浏览器连接至 Kaspersky Security Center Web Console 时，浏览器将与 Kaspersky Security Center Web Console 服务器建立连接。

您按以下方式操作 Kaspersky Security Center Web Console：

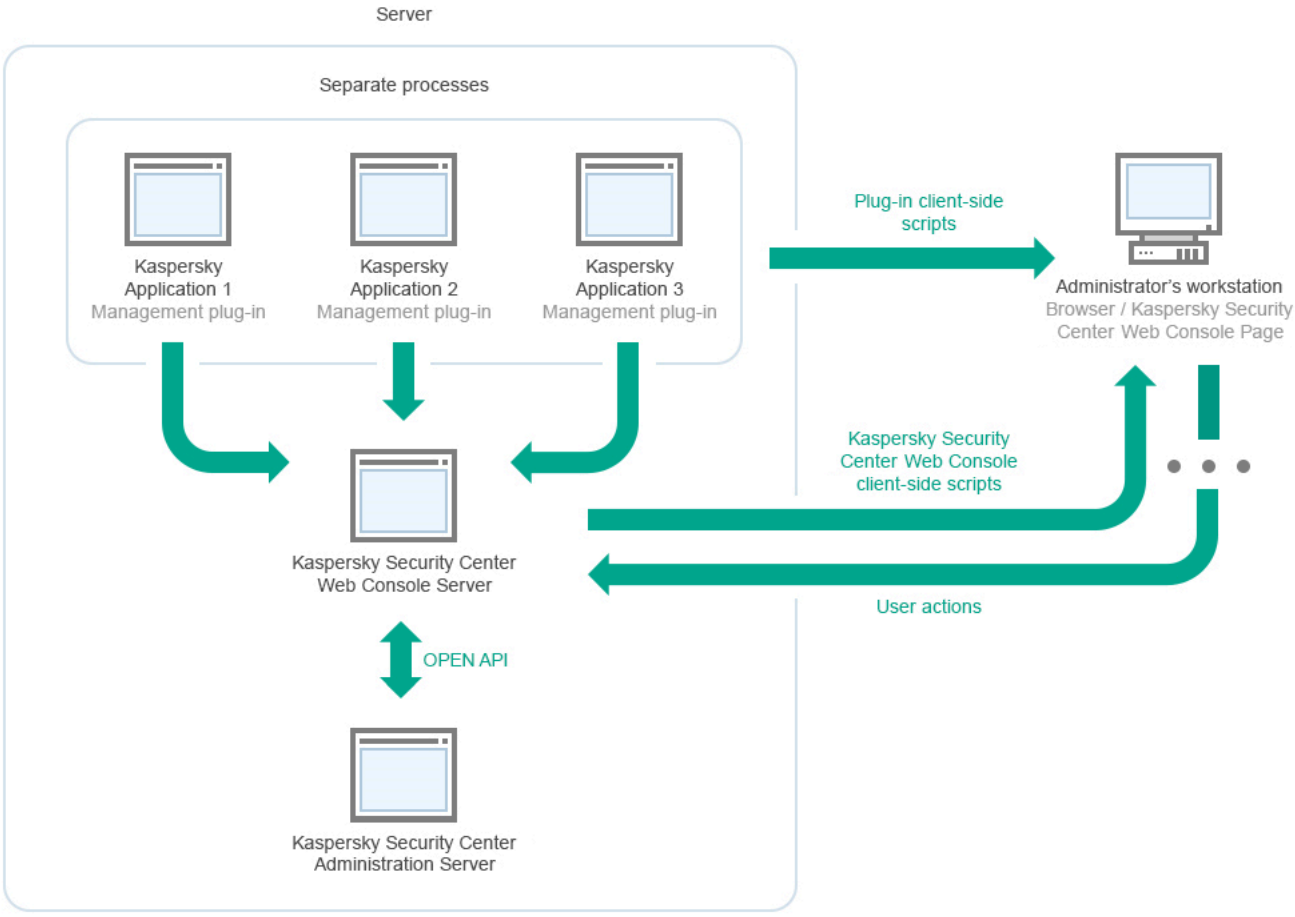
1. 使用浏览器连接至 Kaspersky Security Center Web Console，其中显示了 Web 门户的界面。
2. 使用网页门户控件选择您想要运行的命令。Kaspersky Security Center Web Console执行以下操作：
    - 如果您已选择用于接收信息的命令（例如，查看设备列表），Kaspersky Security Center Web Console 会向管理服务器发送一个信息请求，接收必要数据，然后将其以适合查看的格式发送到浏览器。
    - 如果您已选择用于管理的命令（例如，远程安装应用程序），Kaspersky Security Center Web Console 会从浏览器接收该命令并将其发送到管理服务器。然后，应用程序从管理服务器接收结果并以易于查看的格式将其发送到浏览器。

Kaspersky Security Center Web Console 是一个多语言的应用程序。您可以在任意时刻更改界面语言，而不重新打开应用程序。当您将 Kaspersky Security Center Web Console 与 Kaspersky Security Center 一起安装时，Kaspersky Security Center Web Console 具有和安装文件一样的界面语言。当您仅安装 Kaspersky Security Center Web Console 时，应用程序具有和您的操作系统一样的界面语言。如果 Kaspersky Security Center Web Console 不支持安装文件或操作系统的语言，将默认设置英语。

移动设备管理在 Kaspersky Security Center Web Console 中不被支持。然而，如果您使用 Microsoft 管理控制台添加移动设备到管理组，这些设备也显示在 Kaspersky Security Center Web Console。

Kaspersky Security Center 管理服务器部署图表和 Kaspersky Security Center Web Console

下图显示 Kaspersky Security Center 管理服务器部署图表和 Kaspersky Security Center Web Console



Kaspersky Security Center 管理服务器部署图表和 Kaspersky Security Center Web Console

安装到受保护设备上的 Kaspersky 应用程序管理插件（每个应用程序一个插件）与 Kaspersky Security Center Web Console 服务器一起部署。

作为管理员，您通过使用工作站浏览器来访问 Kaspersky Security Center Web Console。

当您在 Kaspersky Security Center Web Console 执行特定操作时，Kaspersky Security Center Web Console 服务器通过 OpenAPI 与 Kaspersky Security Center 管理服务器交互。Kaspersky Security Center Web Console 服务器从 Kaspersky Security Center 管理服务器请求所需信息并在 Kaspersky Security Center Web Console 显示您的操作结果。

Kaspersky Security Center Web Console 使用的端口

下表列出了安装 Kaspersky Security Center Web Console Server（也称为 Kaspersky Security Center Web Console）的设备上必须开放的端口。

Kaspersky Security Center Web Console 使用的端口

端口号	服务名称	协议	端口目的	范围
2001	Kaspersky Security Center 产品插件服务器	HTTPS	管理插件进程用于接收来自“Kaspersky Security Center Web Console 管理服务”的请求的 API 端口	运行管理插件的 node.exe 进程
1329, 2003	Kaspersky Security Center Web Console 管理服务	HTTPS	用于从同一设备上运行的“Kaspersky Security Center Web Console 管理服务”接收请求的 API 端口	更新 Kaspersky Security Center Web Console 组件
2005	Kaspersky Security Center Web Console	HTTPS	用于从同一设备上运行的“Kaspersky Security Center Web Console 管理服务”接收请求的 API 端口	运行 Kaspersky Security Center Web Console 的 node.exe 进程
3333	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 授权端点端口	身份和访问管理器
4004	Kaspersky OSMP Facade Service	HTTPS	OAuth2.0 身份提供程序端口	身份和访问管理器
4444	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 令牌自检端点端口	身份和访问管理器
8200	—	HTTP	用于通过 HashiCorp Vault 生成证书的 API 端口（有关更多详细信息，请参见 HashiCorp Vault 网站）	安装 Kaspersky Security Center Web Console 并更新 Kaspersky Security Center Web Console 组件
4150, 4151, 4152	Kaspersky Security Center Web Console 消息队列	HTTPS	消息代理的 API 端口，用于 Kaspersky Security Center Web Console 与管理插件的进程间通信	Kaspersky Security Center Web Console 与管理插件之间的交互

下表列出了安装 Kaspersky Security Center Web Console 服务器的设备上不必开放的端口。但是，Kaspersky Security Center Web Console 将这些端口用于身份和访问管理器。

Kaspersky Security Center Web Console 用于身份和访问管理器的端口

端口号	服务名称	协议	端口目的	范围
4445	Kaspersky OSMP KAS Service	HTTPS	从 Kaspersky Security Center Web Console 接收 OAuth2.0 授权端点端口配置的主身份和访问管理器端口（有关 OAuth 2.0 的更多信息，请参见 OAuth 网站）	身份和访问管理器
2444	Kaspersky OSMP Facade Service	HTTPS	用于配置身份和访问管理器的端口	身份和访问管理器
2445	Kaspersky OSMP Facade Service	HTTPS	用于连接“Kaspersky OSMP KAS Service”和“Kaspersky OSMP Facade Service”的端口	身份和访问管理器

Kaspersky Security Center Web Console 界面

Kaspersky Security Center 通过 Kaspersky Security Center Web Console 界面进行管理。

Kaspersky Security Center Web Console 窗口包含以下项目：

- 主菜单位于窗口左侧
- 工作区在窗口右侧

主菜单

主菜单包含以下部分：

- **管理服务器**。显示您当前连接到的管理服务器的名称。单击设置图标 ( ) 打开管理服务器属性。
- **监控和报告**。提供基础架构、保护状态和统计信息的总览。
- **资产（设备）** 。包含资产工具以及任务和卡巴斯基应用程序策略。
- **用户和角色**。可让您管理用户和角色，通过为用户分配角色来配置用户权限，以及将策略配置文件与角色关联。
- **操作**。包含多种操作，包括应用程序授权许可、加密驱动器和加密事件查看和管理以及第三方应用程序管理。您还可以访问应用程序存储库。
- **发现和部署**。可让您轮询网络以发现客户端设备，以及手动或自动将设备分发到管理组。这部分还包含快速启动向导和保护部署向导。
- **Marketplace**。包含有关全系列卡巴斯基业务解决方案的信息，可让您选择所需的解决方案，然后继续在卡巴斯基网站上购买这些解决方案。
- **设置**。可让您备份 Web 插件的当前状态，以便以后能够恢复保存的状态。包含您与界面外观相关的个人设置，例如界面语言或主题。
- **您的账户菜单**。包含指向 Kaspersky Security Center 帮助的链接。您还可以退出 Kaspersky Security Center，并查看 Kaspersky Security Center Web Console 版本和已安装的管理 Web 插件列表。

工作区域

工作区会显示您选择在 Kaspersky Security Center Web Console 界面窗口的各个部分中查看的信息。它还包含可用于配置信息显示方式的控制元素。

固定和取消固定主菜单的各部分

您可以固定 Kaspersky Security Center Web Console 的各部分，以便将其添加到收藏夹中并从主菜单中的“**固定的**”部分快速访问它们。

> 如果没有已固定的元素，则主菜单中不会显示“**固定的**”部分。

您只可以固定显示页面的部分。例如，如果您转到“**资产(设备)**”→“**受管理设备**”，一个包含设备表的页面会打开，这意味着您可以固定“**受管理设备**”部分。如果在主菜单中选择该部分后显示一个窗口或者没有显示任何元素，则您无法固定该部分。

要固定某个部分：

1. 在主菜单中，将鼠标光标悬停在要固定的部分上。
   固定 (📌) 图标将会显示。
2. 点击固定 (📌) 图标。

   该部分被固定并显示在“**固定的**”部分中。

您还可以通过取消固定来从收藏夹中移除元素。

要取消固定某个部分：

1. 在主菜单中，转到“**固定的**”部分。
2. 将鼠标光标悬停在要取消固定的部分上，然后单击取消固定 (📌) 图标。

   该部分被从收藏夹中移除。

情景：Kaspersky Security Center Web Console 安装和初始化设置

该方案描述了如何安装 Kaspersky Security Center 管理服务器和 Kaspersky Security Center Web Console，使用快速启动向导执行管理服务器初始化设置，以及使用保护部署向导安装 Kaspersky 应用程序到受管理设备。

Kaspersky Security Center Web Console 安装和初始化设置分步骤进行：

1. **安装数据库管理系统（DBMS）**

   安装 Kaspersky Security Center 将使用的 DBMS，或者使用现有数据库。

   对于如何安装所选 DBMS 的信息，请参考其文档。

2. **安装管理服务器、管理控制台、网络代理**

   管理控制台和网络代理的服务器版本与管理服务器一起安装。

   在安装 Kaspersky Security Center 管理服务器时，指定您是否要安装 Kaspersky Security Center Web Console 到相同设备。如果您选择安装组件到相同设备，您不必另外安装 Kaspersky Security Center Web Console，因为它是自动安装的。如果您要安装 Kaspersky Security Center Web Console 到不同设备，那么在安装 Kaspersky Security Center 管理服务器后，继续安装 Kaspersky Security Center Web Console。

3. **安装 Kaspersky Security Center Web Console**

   如果您在上一步未选择将 Kaspersky Security Center Web Console 和 Kaspersky Security Center 管理服务器一起安装，请单独安装 Kaspersky Security Center Web Console。您可以将 Kaspersky Security Center Web Console 安装在其他设备或安装了管理服务器的同一设备上。

4. **执行初始化设置**

   当管理服务器安装完成后，在第一次连接到管理服务器时，快速启动向导自动开始。根据现有需求指定管理服务器初始化配置。在初始化配置步骤，向导使用默认设置创建部署保护所需的策略和任务。然而，默认设置可能少于您组织需要的最优设置。您可以编辑策略和任务设置。

5. **Kaspersky Security Center 授权（可选）**

   支持管理控制台基本功能的 Kaspersky Security Center 不需要授权许可。如果您要使用一个或几个附加功能，包括“漏洞和补丁管理”、“移动设备管理”和“与 SIEM 系统整合”，则您需要商业授权许可。您可以在快速启动向导的对应步骤，或者手动为这些功能添加密钥文件或激活码。

6. **发现网络设备**

   此阶段由快速启动向导处理。您也可以手动发现设备。Kaspersky Security Center 接收网络中检测到的所有设备的地址和名称。然后您可以使用 Kaspersky Security Center 在检测到的设备上安装 Kaspersky 应用程序和其他供应商的软件。Kaspersky Security Center 定期启动设备发现，这意味着如果任何新实例出现在网络，它们将被自动检测。

7. **整理设备到管理组**

   该步骤使用快速启动向导执行，但您也可以手动移动检测到的设备到组。

8. **安装网络代理和安全应用程序到网络设备**

   企业网络的保护部署涉及到在设备发现中管理服务器检测到的设备上安装网络代理和安全应用程序(例如，Kaspersky Endpoint Security for Windows)。

   要远程安装应用程序，运行保护部署向导。

   安全应用程序保护设备以防病毒和其他威胁程序。网络代理确保设备和管理服务器之间的通信。网络代理设置默认被自动配置。

   在您开始安装网络代理和安全应用程序到网络设备之前，确保这些设备是可访问的（开启）。

9. **部署授权许可密钥到客户端设备**

   部署授权许可密钥到客户端设备以在这些设备上激活受管理安全应用程序。

10. **安装 Kaspersky Security for Mobile（可选）**

    如果您计划管理公司移动设备，请参见 Kaspersky Security for Mobile 帮助 中提供的说明，以了解有关部署 Kaspersky Endpoint Security for Android 的信息。

11. **配置 Kaspersky 应用程序策略**

    要应用不同应用程序设置到不同设备，您可以使用以设备为中心的安全管理和/或以用户为中心的安全管理。以设备与中心的安全管理可以使用策略和任务 实现。您仅可以应用任务到满足特定条件的设备。要设置筛选设备的条件，使用设备分类和标签。

12. **监控网络保护状态**

    您可以使用仪表板的小部件来监控您的网络，从 Kaspersky 应用程序生成报告，配置和查看从受管理设备上的应用程序接收的事件分类，以及查看通知列表。

安装

该部分描述了 Kaspersky Security Center 和 Kaspersky Security Center Web Console 的安装。

安装 Kaspersky Security Center (标准安装)

该过程描述了如何安装 Kaspersky Security Center。安装之前，您必须安装数据库管理系统。

要 Kaspersky Security Center：

1. 在具有管理员权限的账户下，运行 ksc_<版本号>_full_<本地化语言>.exe 可执行文件。
2. 在应用程序选择窗口，点击**安装 Kaspersky Security Center**。

   Kaspersky Security Center 管理服务器安装向导启动。
3. 开始于欢迎页面，使用**下一步**按钮运行向导。
4. 如果未安装 Microsoft .NET Framework，安装它。
5. 接受授权许可协议和隐私策略的条款。
6. 选择安装类型。对于评估目的，我们建议您保留默认**标准**值。
7. 如果您要安装 Kaspersky Security Center Web Console 到相同的设备，选择**安装 Kaspersky Security Center Web Console** 复选框。

   如果您清空该复选框，您可以稍后安装 Kaspersky Security Center Web Console 到相同或其他设备。
8. 选择网络大小。对于评估目的，我们建议您保留默认**少于 100 台网络设备**值。
9. 选择您先前安装的数据库服务器类型。
10. 指定您先前安装的数据库服务器的连接参数。
11. 指定您先前安装的数据库服务器的身份验证参数。
12. 点击**安装**按钮启动安装。
13. 安装成功完成后，选择您是否要在关闭向导后立即启动管理控制台。

    如果您选择打开 Kaspersky Security Center Web Console，登录界面将打开。然后您将可以通过快速启动向导执行管理服务器的初始化配置。

    您仅可以在 Kaspersky Security Center Web Console 已被安装时打开它。如果您在安装 Kaspersky Security Center 时没有安装 Kaspersky Security Center Web Console，您无法打开它。
14. 在打开的管理控制台窗口，点击安装的管理服务器。
15. 在打开的管理服务器证书窗口，点击**是**按钮以继续。

管理服务器快速启动向导开始，如果您未在基于 Web 的管理控制台运行。

故障解决

如果管理服务器证书窗口不打开并且显示连接错误，尝试以下：

1. 在 Windows，打开**服务**（**控制面板 → 管理工具 → 服务**）。检查 Kaspersky Security Center 网络代理和 Kaspersky Security Center 管理服务器服务是否正在运行。
2. 在 Windows，打开**事件查看器**（**控制面板 → 管理工具 → 事件查看器**）并选择**应用程序和服务日志 → 卡巴斯基事件日志**。确保日志不包含错误，而是包含类似"**管理服务器 <版本号> 正在运行**"的事件。

安装 Kaspersky Security Center Web Console

该部分描述了如何单独安装 Kaspersky Security Center Web Console 服务器 (也叫 Kaspersky Security Center Web Console)。安装之前，您必须安装数据库管理系统和 Kaspersky Security Center 管理服务器。您可以在安装了 Kaspersky Security Center 的同一设备上或在其他设备上安装 Kaspersky Security Center Web Console。

要安装 Kaspersky Security Center Web Console：

1. 在具有管理员权限的账户下，运行 ksc-web-console-<版本号>.<内部版本号>.exe 安装文件。

   这会启动安装向导。

2. 为安装向导选择语言。

3. 在欢迎窗口，点击**下一步**。

4. 在“**授权许可协议**”窗口中，阅读并接受最终用户授权许可协议的条款。安装在您接受最终用户授权许可协议后继续，否则**下一步**按钮不可用。

5. 在“**目标文件夹**”窗口中，选择要安装 Kaspersky Security Center Web Console 的文件夹（默认为 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console）。如果此文件夹不存在，则系统会在安装过程中自动创建。

   您可以使用“**浏览**”按钮更改目标文件夹。

6. 在 **Kaspersky Security Center Web Console 连接设置**窗口，指定以下信息：

   - Kaspersky Security Center Web Console 地址（默认 127.0.0.1）。
   - Kaspersky Security Center Web Console 将用于传入连接的端口，即用于从浏览器访问 Kaspersky Security Center Web Console 的端口（默认为 8080）。

   我们建议您为地址和端口号选择默认值。

   如果需要，您可以点击“**测试**”以确保所选端口可用。

   如果您要启用Kaspersky Security Center Web Console 活动记录，选择适当选项。如果您不选择该选项，Kaspersky Security Center Web Console 日志文件将不被创建。

7. 在**账户设置**窗口，指定账户名称和密码。

   我们建议您使用默认账户。

8. 在**客户端证书**窗口，选择以下之一：

   - **生成新证书**。如果您没有浏览器证书，则推荐该选项。
   - **选择现有证书**。如果您已经拥有浏览器证书，则选择该选项；此种情况下，指定其路径。
   - 如果您选择生成新证书，那么当您打开 Kaspersky Security Center Web Console，浏览器可能会通知您与 Kaspersky Security Center Web Console 的连接不是专用连接，并且 Kaspersky Security Center Web Console 证书无效。出现此警告是因为 Kaspersky Security Center Web Console 证书是自签名证书，并且由 Kaspersky Security Center 自动生成。若要移除此警告，请创建一个在您的基础架构中受信任且满足自定义证书要求的证书。接下来，在**客户端证书**窗口中选择**选择现有证书**选项，然后指定您的自定义证书的路径。

Kaspersky Security Center Web Console 不支持 PFX 格式的证书。要使用这样的证书，必须首先使用基于OpenSSL的跨平台实用程序（例如Windows的OpenSSL） 将其转换为受支持的PEM格式。

9. 在**受信任的管理服务器**窗口，确保您的管理服务器在列表中并点击**下一步**以继续安装程序的最后一个窗口。

   如果您需要将新的管理服务器添加到列表中，请单击"**添加**"按钮。在打开的窗口中，指定新的受信任管理服务器的属性：

   - **管理服务器名称**

     将显示在 Kaspersky Security Center Web Console 登录窗口中的管理服务器名称。

   - **管理服务器地址**

     安装管理服务器的设备的 IP 地址。

   - **管理服务器端口**

     Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认 13299）。

   - **管理服务器证书**

     证书文件存储在安装管理服务器的设备上。管理服务器证书的默认路径：

     - 对于 Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
     - 对于 Linux — /var/opt/kaspersky/klnagent_srv/1093/cert/

     如果您在安装管理服务器的同一台设备上安装 Kaspersky Security Center Web Console，请使用上面给出的路径之一。否则，将证书文件从安装管理服务器的设备复制到安装 Kaspersky Security Center Web Console 的设备，然后指定证书的本地路径。

10. 在"**身份和访问管理器 (IAM)**"窗口中，指定是否要安装身份和访问管理器（也称为 IAM）。如果您选择安装身份和访问管理器，请指定以下端口号：

    - **KAS 管理员端口**。默认情况下，端口 4445 用于从 Kaspersky Security Center Web Console 接收 OAuth2.0 授权端点端口的配置。
    - **门面管理员端口**。默认情况下，端口 2444 用于配置身份和访问管理器。
    - **门面交互端口**。默认情况下，端口 2445 用于 Kaspersky OSMP KAS Service 与 Kaspersky OSMP Facade Service 的连接。

    如果需要，可以更改默认端口号。您将来无法通过 Kaspersky Security Center Web Console 更改它们。

11. 在安装程序的最后一个窗口，点击**安装**以开始安装。

在安装成功完成后，桌面上将出现一个快捷方式，您可以登录到 Kaspersky Security Center Web Console。

如果您未在基于 Microsoft Management Console 的管理控制台中运行管理服务器快速启动向导，则该向导启动。

故障解决

在您键入 URL 后，如果浏览器中未显示 Kaspersky Security Center Web Console，请尝试以下操作：

1. 检查您是否指定了安装了 Kaspersky Security Center Web Console 的设备的正确主机名称或 IP 地址。
2. 检查您要操作的设备是否具有安装了 Kaspersky Security Center Web Console 的设备的访问权限。
3. 检查安装了 Kaspersky Security Center Web Console 的设备的防火墙设置是否允许应用程序 node.exe 通过端口 8080 的入站连接。
4. 在 Windows，打开**服务**。检查 Kaspersky Security Center Web Console 服务是否正在运行。
5. 检查您是否可以使用管理控制台访问 Kaspersky Security Center。
6. 在 Windows，打开**事件查看器**，然后选择**应用程序和服务日志 → 卡巴斯基事件日志**。确保日志不包含错误。

安装 Kaspersky Security Center Web Console，连接到安装在故障转移群集节点上的管理服务器

本节介绍如何安装 Kaspersky Security Center Web Console Server（以下也称为 Kaspersky Security Center Web Console），其连接到安装在 Kaspersky Security Center Linux 故障转移集群节点或 Windows 服务器故障转移集群节点上的管理服务器。在安装 Kaspersky Security Center Web Console 之前，请先安装数据库管理系统和 Kaspersky Security Center 管理服务器，安装在 Kaspersky Security Center 故障转移集群节点或 Windows 服务器故障转移群集节点上。

如果您使用 Windows 服务器故障转移集群，我们建议不要在故障转移集群节点上安装 Kaspersky Security Center Web Console。如果节点出现故障，您将无法访问管理服务器。

要安装连接到安装在故障转移群集节点上的管理服务器的 Kaspersky Security Center Web Console：

1. 请执行 Kaspersky Security Center Web Console 安装步骤的第 1 步至第 8 步。
2. 在第 9 步，在**受信任的管理服务器**窗口中，单击**添加**按钮将故障转移集群添加为受信任的管理服务器。
   在打开的窗口中，指定以下属性：
   - **管理服务器名称**
     将显示在 Kaspersky Security Center Web Console 登录窗口中的集群名称。
   - **管理服务器地址**
     根据故障转移集群类型，指定集群地址：
     - **Kaspersky Security Center 故障转移集群**。如果您在准备集群节点时已创建适配器，则指定从属网络适配器的 IP 地址为集群地址。否则，请指定您使用的第三方负载平衡器的 IP 地址。
     - **Windows Server 故障转移集群**。指定您在创建 Windows 服务器故障转移集群时获得的集群地址。
   - **管理服务器端口**
     Kaspersky Security Center Web Console 用于连接到管理服务器的 OpenAPI 端口（默认 13299）。

- **管理服务器证书**

  管理服务器证书位于 Kaspersky Security Center 故障转移集群或者 Windows 服务器故障转移集群的共享数据存储中。证书文件的默认路径：<shared data folder>\1093\cert\klserver.cer。将证书文件从共享数据存储复制到安装 Kaspersky Security Center Web Console 的设备。指定管理服务器证书的本地路径。

3. 继续运行 Kaspersky Security Center Web Console 的标准安装。

在安装完成后，桌面上将出现一个快捷方式，您可以登录到 Kaspersky Security Center Web Console。

升级 Kaspersky Security Center Web Console

如果要使用更新版本的 Kaspersky Security Center Web Console 而不删除当前安装的实例，可以使用 Kaspersky Security Center Web Console 安装程序中提供的标准升级程序。

要升级 Kaspersky Security Center Web Console：

1. 在具有管理员权限的账户下，运行 ksc-web-console-<版本号>.<内部版本号>.exe 安装文件，其中 <内部版本号> 代表 Kaspersky Security Center Web Console 内部版本，其版本号高于当前安装的实例。

2. 在打开的安装向导窗口中，选择语言，然后单击“**确定**”。

3. 在欢迎窗口中，选择“**升级**”选项，然后单击“**下一步**”。

4. 在“**授权许可协议**”窗口中，阅读并接受最终用户授权许可协议的条款。安装在您接受最终用户授权许可协议后继续，否则**下一步**按钮不可用。

5. 完成安装向导的步骤，直到完成安装。安装时，还可以修改在先前安装期间指定的 Kaspersky Security Center Web Console 设置。当到达“**Kaspersky Security Center Web Console 修改已就绪**”步骤时，单击“**升级**”按钮。等待至应用新设置，然后在安装向导的下一步，单击“**完成**”。还可以单击“**在您的浏览器中启动 Kaspersky Security Center Web Console**”链接立即启动 Kaspersky Security Center Web Console 的已升级实例。

   只有 Kaspersky Security Center Web Console 版本 12.2 或更高版本支持在升级期间修改 Kaspersky Security Center Web Console 设置。

   您的 Kaspersky Security Center Web Console 实例已升级。

用于 Kaspersky Security Center Web Console 的证书

本节介绍如何为 Kaspersky Security Center Web Console 颁发和更换证书，以及如何在管理服务器与 Kaspersky Security Center Web Console 交互时为管理服务器续订证书。

重新颁发 Kaspersky Security Center Web Console 的证书

大多数浏览器对证书有效期施加了限制。为了不超过此限制，Kaspersky Security Center Web Console 证书的有效期限制为 397 天。您可以通过手动颁发新的自签名证书来替换从证书颁发机构 (CA) 收到的现有证书。或者，您可以重新颁发过期的 Kaspersky Security Center Web Console 证书。

不支持自动重新颁发 Kaspersky Security Center Web Console 证书。您必须手动重新颁发过期的证书。

如果已经使用自签名证书，还可以通过安装程序中的标准程序升级 Kaspersky Security Center Web Console 来重新颁发该证书（“**升级**”选项）。

当您打开 Web Console 时，浏览器可能会通知您与 Web Console 的连接不是私有连接，并且 Web Console 证书无效。出现此警告是因为 Web Console 证书是自签名的，并且由 Kaspersky Security Center 自动生成。要移除或防止此警告，可以执行以下操作之一：

- 重新颁发证书时指定自定义证书（推荐选项）。创建在您的基础架构中受信任且满足自定义证书要求的证书。
- 重新颁发 Web Console 证书后，将该证书添加到受信任浏览器证书列表中。我们建议您仅在无法创建自定义证书时才使用此选项。

要在第一次安装 Kaspersky Security Center Web Console 时颁发新证书：

1. 运行 Kaspersky Security Center Web Console 的常规安装。
2. 当到达安装向导的“**客户端证书**”步骤时，选择“**生成新证书**”选项，然后单击“**下一步**”按钮。
3. 完成安装向导的其余步骤，直到完成安装。

   颁发的新 Kaspersky Security Center Web Console 证书的有效期为 397 天。

要重新颁发过期的 Kaspersky Security Center Web Console 证书：

1. 在具有管理员权限的账户下，运行 ksc-web-console-<版本号>.<内部版本号>.exe 安装文件。
2. 在打开的安装向导窗口中，选择语言，然后单击“**确定**”。
3. 在欢迎窗口中，选择“**重新发布证书**”选项，然后单击“**下一步**”。
4. 在下一步，等待至 Kaspersky Security Center Web Console 的重新配置完成，然后单击“**完成**”。

   重新颁发的 Kaspersky Security Center Web Console 证书的有效期将增加 397 天。

如果使用身份和访问管理器，还必须为身份和访问管理器使用的端口重新颁发所有 TLS 证书。当证书过期时，Kaspersky Security Center Web Console 会显示通知。您必须按照通知说明操作。

替换 Kaspersky Security Center Web Console 证书

默认情况下，安装 Kaspersky Security Center Web Console Server 时，该应用程序的浏览器证书会自动生成。您可以使用自定义证书替换自动生成的证书。

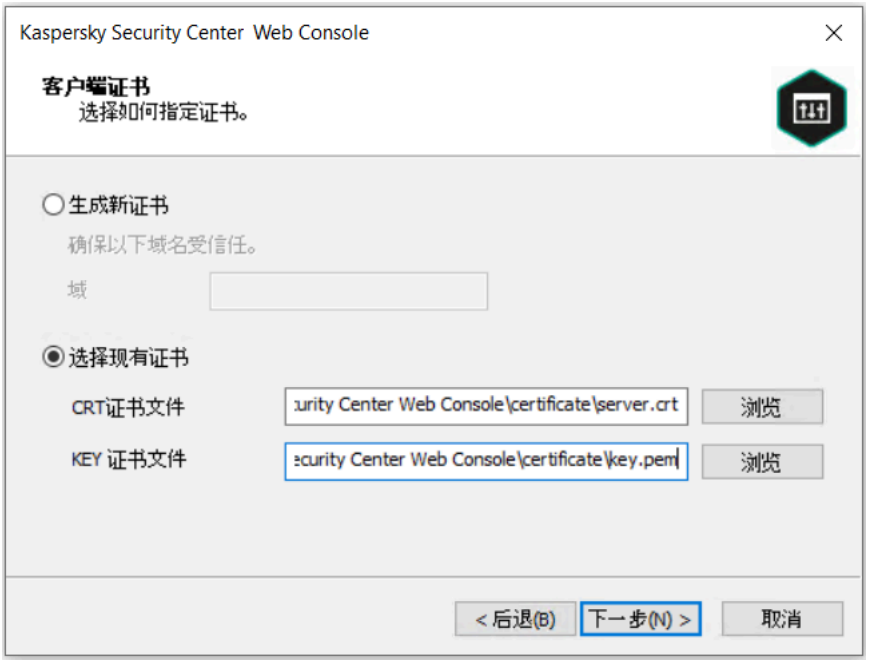
要将 Kaspersky Security Center Web Console Server 的证书替换为自定义证书：

1. 在安装了 Kaspersky Security Center Web Console Server 的设备上，在具有管理员权限的账户下运行 ksc-web-console-<版本号>.<内部版本号>.exe 安装文件。

   这会启动安装向导。

2. 在向导的第一页，选择**升级**选项。

3. 在**客户端证书**页面，选择**选择现有证书**选项并指定自定义证书的路径。



指定客户端证书

4. 在向导的最后一页，点击**修改**以应用设置。

5. 在应用程序重新配置成功完成后，点击**完成**按钮。

Kaspersky Security Center Web Console 使用指定的证书工作。

在 Kaspersky Security Center Web Console 中为受信任的管理服务器指定证书

现有管理服务器证书在过期日期之前被新证书自动替换。您也可以使用自定义证书替换现有管理服务器证书。每次变更证书时，新证书必须在 Kaspersky Security Center Web Console 设置中被指定。否则，Kaspersky Security Center Web Console 将无法连接到管理服务器。

要指定管理服务器新证书：

1. 在管理服务器所在设备上，复制证书文件到（例如大容量）存储设备。

   默认情况下，证书文件存储在以下文件夹中：

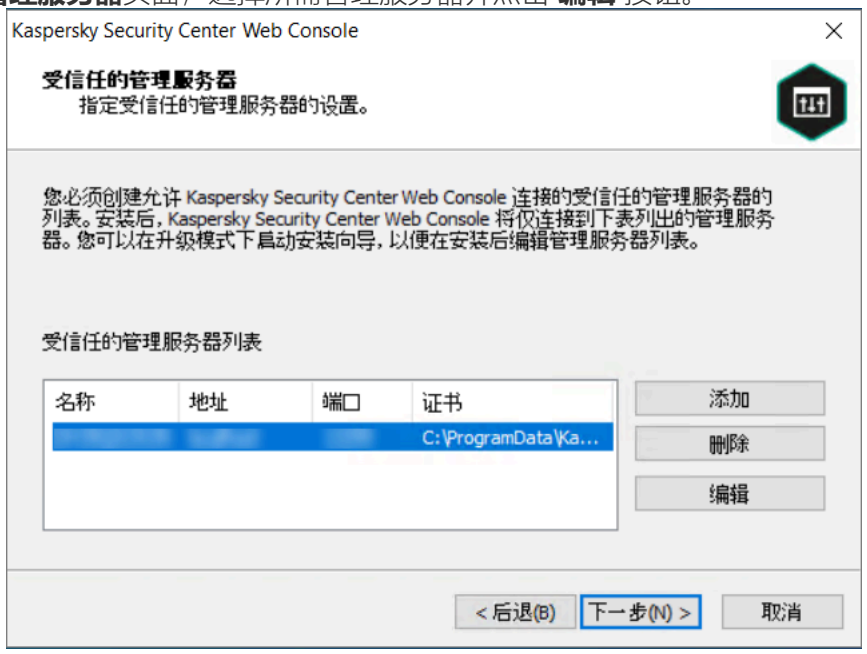
   - 对于 Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - 对于 Linux — /var/opt/kaspersky/klnagent_srv/1093/cert/

2. 在安装了 Kaspersky Security Center Web Console 的设备上，将证书文件放到本地文件夹。

3. 在具有管理员权限的账户下运行 ksc-web-console-<版本号>.<内部版本号>.exe 安装文件。
   这会启动安装向导。

4. 在第一个向导页面上，选择**升级**选项。
   遵照向导的说明操作。

5. 在向导的**受信任的管理服务器**页面，选择所需管理服务器并点击"**编辑**"按钮。



指定受信任管理服务器

6. 在打开的**编辑管理服务器**窗口中，单击"**浏览**按钮，指定新证书文件的路径，然后单击**更新**按钮应用更改。

7. 在向导的**Kaspersky Security Center Web Console 修改已就绪**页面，点击**升级**按钮开始升级。

8. 在应用程序重新配置成功完成后，点击**完成**按钮。

9. 登录到 Kaspersky Security Center Web Console。

Kaspersky Security Center Web Console 使用指定的证书工作。

将 PFX 证书转换为 PEM 格式

要在 Kaspersky Security Center Web Console 中使用 PFX 证书，必须首先使用任何方便的基于 OpenSSL 的跨平台实用程序将该证书转换为 PEM 格式。

要在 Windows 操作系统中将 PFX 证书转换为 PEM 格式：

1. 在基于 OpenSSL 的跨平台实用程序中，执行以下命令：

```
openssl pkcs12 -in <文件名.pfx> -clcerts -nokeys -out server.crt
openssl pkcs12 -in <文件名.pfx> -nocerts -nodes -out key.pem
```

   结果，您将得到一个 .crt 文件形式的公钥和一个受密码保护的 .pem 文件形式的私钥。

2. 确保 .crt 和 .pem 文件生成到存储 .pfx 文件的同一文件夹中。

3. 如果 .crt 或 .pem 文件包含包属性，则使用任何方便的文本编辑器删除这些属性，然后保存文件。

4. 重新启动 Windows 服务。

5. Kaspersky Security Center Web Console 不支持受密码保护的证书。因此，在基于 OpenSSL 的跨平台实用程序中运行以下命令，从 .pem 文件中删除密码：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 输入和输出 .pem 文件不要使用相同名称。

   结果，新的 .pem 文件未加密。无需输入密码即可使用。

.crt 和 .pem 文件已可以使用，因此您可以在 Kaspersky Security Center Web Console 安装程序中指定它们。

要在 Linux 操作系统中将 PFX 证书转换为 PEM 格式：

1. 在基于 OpenSSL 的跨平台实用程序中，执行以下命令：

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <文件名.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 确保证书文件和私钥生成到存储 .pfx 文件的同一目录中。

3. Kaspersky Security Center Web Console 不支持受密码保护的证书。因此，在基于 OpenSSL 的跨平台实用程序中运行以下命令，从 .pem 文件中删除密码：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 输入和输出 .pem 文件不要使用相同名称。

   结果，新的 .pem 文件未加密。无需输入密码即可使用。

.crt 和 .pem 文件已可以使用，因此您可以在 Kaspersky Security Center Web Console 安装程序中指定它们。

从 Kaspersky Security Center Windows 迁移

本节介绍将受管理设备和相关对象（策略、任务、组、标签和其他对象）从 Kaspersky Security Center Windows 迁移到以下对象的过程。

- Kaspersky Security Center 云控制台
- Kaspersky Security Center Linux

迁移到 Kaspersky Security Center 云控制台

您可以从 Kaspersky Security Center Web 控制台执行迁移到 Kaspersky Security Center 云控制台。之后，您可以访问托管在卡巴斯基基础架构中的管理服务器和数据库管理系统 (DBMS)。您不需要物理服务器或 DBMS — 两者都由卡巴斯基专家为您维护。

您可以迁移在 Kaspersky Security Center 云控制台 控制下运行 Windows、Linux 或 macOS 操作系统的受管理设备。如果您的网络包含管理服务器的层次结构，您可以将其保存在 Kaspersky Security Center 云控制台中。此外，您可以传输：

- 受管理应用程序的任务和策略
- 全局任务
- 自定义设备分类
- 管理组结构和包含的设备
- 已分配给迁移设备的标签

完成迁移后，您可以使用 Kaspersky Security Center 云控制台管理设备。同时，传输的对象被保留并且网络代理被重新安装在所有受管理设备上。

有关如何执行迁移的信息和先决条件列表，请参阅 *Kaspersky Security Center 云控制台帮助*。

迁移到 Kaspersky Next XDR Expert

按照此方案，您可以将管理组结构、包含的受管理设备和其他组对象（策略、任务、全局任务、标签和设备分类）从 Kaspersky Security Center Windows 转移到 Kaspersky Next XDR Expert 的管理之下。

限制：

- 从版本 1.0 开始，只能从 Kaspersky Security Center 14.2 Windows 迁移到 Kaspersky Next XDR Expert。
- 您只能使用 Kaspersky Security Center Web Console 来执行此方案。

阶段

迁移方案分阶段进行：

1. **选择迁移方法**

   您可以通过迁移向导迁移到 Kaspersky Next XDR Expert。迁移向导的具体步骤取决于 Kaspersky Security Center Windows 和 Kaspersky Next XDR Expert 的管理服务器是否排列为层次结构：

   - 使用管理服务器层级进行迁移

     如果 Kaspersky Security Center Windows 的管理服务器充当 Kaspersky Next XDR Expert 管理服务器的从属管理服务器，请选择此选项。您可以在 OSMP 控制台中管理迁移过程并在服务器之间切换。如果您更喜欢此选项，可以将管理服务器排列成层次结构以简化迁移过程。为此，请在开始迁移之前创建层次结构。

   - 使用导出文件（ZIP 存档）进行迁移

     如果 Kaspersky Security Center Windows 和 Kaspersky Next XDR Expert 的管理服务器未排列为层次结构，请选择此选项。您可以使用两个控制台管理迁移过程：一个是Kaspersky Security Center Windows 实例，另一个是 OSMP 控制台。在这种情况下，您可以使用在从 Kaspersky Security Center Windows 导出期间创建和下载的导出文件并将此文件导入 Kaspersky Next XDR Expert。

2. **从 Kaspersky Security Center Windows 导出数据**

   打开 Kaspersky Security Center Windows，然后运行迁移向导。

3. **将数据导入 Kaspersky Next XDR Expert**

   继续运行迁移向导，将导出的数据导入 Kaspersky Next XDR Expert。

   如果服务器按层次结构排列，则在同一向导中成功导出后，导入会自动开始。如果服务器未排列为层次结构，您可以在切换到 Kaspersky Next XDR Expert 后继续运行迁移向导。

4. **执行其他操作以手动将对象和设置从 Kaspersky Security Center Windows 转移到 Kaspersky Next XDR Expert（可选步骤）**

   您可能还想传输无法通过迁移向导传输的对象和设置。例如，您还可以执行以下操作：

   - 配置管理服务器的全局任务
   - 配置网络代理策略设置
   - 创建应用程序安装包
   - 创建虚拟服务器
   - 分配和配置分发点
   - 配置设备移动规则
   - 配置自动标记设备规则
   - 创建应用程序类别

5. **将导入的受管理设备转移到 Kaspersky Next XDR Expert 的管理之下**

   要完成迁移，请将导入的受管理设备转移到 Kaspersky Next XDR Expert 的管理之下。您可以通过以下方式之一进行操作：

   - 通过 Kaspersky Security Center 组任务

     使用更改管理服务器任务将管理服务器更改为特定客户端设备的另一台管理服务器。

   - 通过klmover 实用程序

     使用 klmover 实用程序并指定新管理服务器的连接设置。

   - 通过在受管理设备上安装或重新安装网络代理

     创建新的网络代理安装包，并在安装包属性中指定新管理服务器的连接设置。使用安装包通过远程安装任务在导入的受管理设备上安装网络代理。

     您还可以创建并使用独立的安装包在本地安装网络代理。

6. **将网络代理更新到最新版本**

   我们建议您将网络代理升级到与 OSMP 控制台相同的版本。

7. **确保受管理设备在新管理服务器上可见**

   在 Kaspersky Next XDR Expert 管理服务器上，打开受管理设备列表（**资产(设备)** → **受管理设备**），然后检查“**可见**”、“**网络代理已安装**”和“**上一次连接到管理服务器**”列中的值。

其他数据迁移方法

除了迁移向导之外，您还可以传输特定任务和策略：

- 从 Kaspersky Security Center Windows 导出任务，然后导入任务到 Kaspersky Next XDR Expert。
- 从 Kaspersky Security Center Windows 导出策略，然后导入策略到 Kaspersky Next XDR Expert。相关的策略配置文件与选定的策略一起导出和导入。

迁移到 Kaspersky Security Center Linux

通过使用管理服务器数据备份（使用klbackup 实用程序）和迁移向导，可以从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux。

借助下表，您可以比较使用管理服务器数据备份和迁移向导进行迁移的主要功能和限制，以便为组织选择更合适的方案。

迁移方法比较

参数	管理服务器数据备份	迁移向导
迁移过程	创建 Kaspersky Security Center Windows 管理服务器数据的完整备份并将其恢复到 Kaspersky Security Center Linux 管理服务器上	选择并导出管理服务器数据进行迁移，将这些数据导入 Kaspersky Security Center Linux 管理服务器，并将受管理设备切换至 Kaspersky Security Center Linux 管理之下
迁移方法的特点	• 迁移所有管理服务器数据 • 迁移任意数量的受管理设备 • 用于获取 Kaspersky Security Center Windows 管理服务器数据的完整副本并将其传输到 Kaspersky Security Center Linux 管理服务器	• 部分迁移管理服务器数据 • 可以选择要迁移的对象 • 要迁移的管理组或子组最多可包含 10,000 个设备 • 用于部分传输管理服务器数据，仅包括迁移范围内的组对象；迁移范围之外的组对象必须手动恢复
迁移范围	管理服务器数据的完整传输，受管理设备数量不受限制	• 管理组结构 • 管理组中包含的受管理设备（**不超过 10,000 台设备**） • 分配给迁移设备的标签 • 网络代理和受管理应用程序的全局任务（不适用于管理服务器） • 网络代理和受管理应用程序的组任务 • 受管理应用程序的策略 • 报告模板 • 用户角色 • 内部用户和安全组 • 含有手动添加内容的自定义应用程序类别 • 自定义设备分类
未迁移范围	—	• 管理服务器的全局任务 • 保存在管理服务器上的事件 • 远程安装的应用程序分发包的存储库 • 管理服务器证书 • 管理服务器和受管理应用程序使用的授权许可密钥 • 虚拟管理服务器 • 网络代理策略设置 • 设备移动规则 • 设备自动标记规则 • 分发点 • 管理服务器上保存的卡巴斯基应用程序设置
支持迁移的 Kaspersky Security Center 版本	• 任何受支持的 Kaspersky Security Center Windows 版本 • Kaspersky Security Center Linux 版本 15.2 或更高版本	• Kaspersky Security Center Windows 版本 14.2 或更高版本 • Kaspersky Security Center Linux 版本 15 或更高版本
可以进行迁移的 DBMS	• Microsoft SQL Server → MySQL、MariaDB • Microsoft SQL Server → PostgreSQL、Postgres Pro （仅适用于从已安装补丁的 Kaspersky Security Center Windows 版本 14.2 或更高版本迁移至 Kaspersky Security Center Linux 版本 15.3 或更高版本） • MySQL → MySQL、MariaDB • MariaDB → MySQL、MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro（仅适用于从Kaspersky Security Center Windows 版本 15.1 或更高版本迁移到 Kaspersky Security Center Linux 版本 16 或更高版本）	在受支持的 DBMS之间无限制迁移

使用管理服务器数据备份迁移到 Kaspersky Security Center Linux

您可以使用数据备份将 Kaspersky Security Center Windows 管理服务器数据迁移至 Kaspersky Security Center Linux。迁移之前，请确保Kaspersky Security Center Windows 的必要功能在 Kaspersky Security Center Linux 中受支持。

限制：

- 迁移可以在以下 DBMS 之间进行：
  - Microsoft SQL Server → MySQL、MariaDB
  - Microsoft SQL 服务器 → PostgreSQL、 Postgres Pro
  - MySQL → MySQL、MariaDB
  - MariaDB → MySQL、MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- 支持将存储在 Microsoft SQL Server、MySQL 或 MariaDB 数据库中的管理服务器数据从任何受支持的 Kaspersky Security Center Windows 版本迁移到 Kaspersky Security Center Linux 版本 15.2 或更高版本。
- 当从 Kaspersky Security Center Windows 版本 15.1 或更高版本迁移到 Kaspersky Security Center Linux 版本 16 或更高版本时，支持将存储在 PostgreSQL 数据库中的管理服务器数据迁移至 PostgreSQL 或 Postgres Pro。
- 当从 Kaspersky Security Center Windows 版本 14.2 或更高版本迁移到Kaspersky Security Center Linux 版本 15.3 或更高版本时，支持将存储在 Microsoft SQL Server 数据库中的管理服务器数据迁移至 PostgreSQL 或 Postgres Pro。

  要迁移到 PostgreSQL 或 Postgres Pro，您可以执行以下操作之一：
  - 安装 Kaspersky Security Center Windows 管理服务器补丁 15.1.0.20748-pf2。联系卡巴斯基技术支持以获取此补丁。
  - 将 Kaspersky Security Center Windows 更新至版本 15.1.0.22239。
- 如果您使用 MySQL 或 MariaDB 作为 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的 DBMS，则 `lower_case_table_names` 参数必须与当前和新的 DBMS 匹配。

  在创建数据备份之前，请检查 `lower_case_table_names` 参数。随后，在为 Kaspersky Security Center Linux 安装 MySQL 或 MariaDB 时，必须将此参数的值设置为与 Windows 版一致。

阶段

使用管理服务器数据备份进行分阶段迁移：

1. **检查您是否拥有管理员的内部用户账户，以便可以登录管理服务器**

   管理员账户将用于登录 Kaspersky Security Center Linux 管理服务器。如果您没有此账户，并且仅在本地 Windows 账户或域账户下登录，则恢复备份后将无法登录 Kaspersky Security Center Linux 管理服务器。Kaspersky Security Center Linux 管理服务器不支持使用本地 Windows 账户登录。可以使用域账户登录，但可能需要对管理服务器进行额外配置。

   如果您没有管理员账户，则必须在使用 kladduser 实用程序恢复备份副本后创建此账户。

2. **创建 Kaspersky Security Center Windows 管理服务器数据的最新备份副本**

根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 使用的 DBMS 类型，执行以下操作之一：

- 对于将 MySQL 或 MariaDB 迁移到 MySQL 或 MariaDB：在安装了管理服务器的设备上使用klbackup 实用程序或数据备份任务创建备份副本。
- 要将 PostgreSQL 迁移到 PostgreSQL 和将 Postgres Pro 迁移到 Postgres Pro：在已安装管理服务器的设备上使用 klbackup 实用程序或数据备份任务来创建备份副本。
- 对于将 Microsoft SQL Server 迁移到 MySQL 或 MariaDB：使用 klbackup 实用程序创建备份副本，同时启用“**迁移到 MySQL/MariaDB 格式**”选项。
- 对于将 Microsoft SQL Server 迁移到 PostgreSQL 或 Postgres Pro：

  1. 请求卡巴斯基技术支持并安装管理服务器补丁 15.1.0.20748-pf2 以迁移到 PostgreSQL 和 Postgres Pro。

     或者，您可以将 Kaspersky Security Center Windows 更新至版本 15.1.0.22239。

  2. 使用 klbackup 实用程序创建备份副本。

     如果从命令行运行 klbackup，请使用`-migrate postgres`标志。

     如果使用 klbackup 界面，请启用“**迁移到 Postgres 格式**”选项。

创建备份副本后，断开 Kaspersky Security Center Windows 管理服务器与网络的连接。

3 准备一台新设备用于安装 Kaspersky Security Center Linux

在方案的该步骤，执行以下操作：

1. 选择要安装管理服务器的新设备。该设备必须满足硬件和软件要求。此外，请检查管理服务器上使用的端口是否可用。
2. 为新设备分配相同地址。

   可以为新的管理服务器分配 NetBIOS 名称、FQDN 和静态 IP 地址。这取决于部署网络代理时在网络代理安装包中设置了哪个管理服务器地址。或者，您可以使用确定网络代理连接到的管理服务器的连接地址（您可以使用klnagchk 实用程序在受管理设备上获取此地址）。

4 安装和配置 DBMS

在方案的该步骤，执行以下操作：

1. 选择提供最佳性能的 DBMS 类型。考虑联网设备的数量、网络拓扑和网络工作负载。您可以从支持的 DBMS 中选择一个。
2. 根据创建备份时选择的 DBMS 类型安装 DBMS。对于如何安装所选 DBMS 的信息，请参考其文档。

   > 新的数据库版本不得低于当前数据库版本。

3. 配置与 Kaspersky Security Center Linux 配合使用的 DBMS。

5 安装 Kaspersky Security Center Linux

在新设备上安装 Kaspersky Security Center Linux。

安装期间创建的管理员内部用户账户以及从备份恢复管理服务器数据之前创建的其他对象（组、策略、组任务、用户）将在恢复后丢失。这些对象将被备份中包含的容器替换。

6 从备份副本恢复管理服务器数据

在方案的该步骤，执行以下操作：

1. 使用klbackup 实用程序在新设备上恢复管理服务器数据。

2. 如果您没有用于登录 Kaspersky Security Center Windows 管理服务器的管理员内部用户账户，并且使用了本地 Windows 账户或域账户，请使用 kladduser 实用程序创建管理员账户，如下所示：

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   其中`<password>`参数满足以下要求：

   - 用户密码不能少于 8 个字符或超过 256 个字符。
   - 密码必须包含以下组中三组的字符：
     - 大写字母 (A-Z)
     - 小写字母 (a-z)
     - 数字 (0-9)
     - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **安装 Kaspersky Security Center Web Console 和配置管理服务器**

   在方案的该步骤，执行以下操作：

   1. 安装 Kaspersky Security Center Web Console。

      如果之前安装了 Kaspersky Security Center Web Console，请使用相同的响应文件重新安装它。

      使用管理员的内部用户账户登录 Kaspersky Security Center Web Console。

      恢复管理服务器数据后，数据初始化过程通常需要 15 分钟，但时间取决于硬件性能和管理服务器数据的大小。在此期间，Kaspersky Security Center Web Console 可能无法连接并显示错误。

   2. 当数据库中的数据初始化完成后，检查主要管理服务器功能是否正常。验证管理服务器是否与受管理设备同步以及管理服务器数据是否已恢复。

   3. 轮询域控制器可恢复有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。

   4. 如有必要，从以前的设备中卸载管理服务器和数据库服务器。

      同一网络上不能存在多个具有相同连接地址和管理服务器证书的管理服务器。

管理员有权访问原 Kaspersky Security Center Windows 中的管理服务器数据及受管理设备，同时需确保相关功能在 Kaspersky Security Center Linux 受支持。

通过迁移向导迁移到 Kaspersky Security Center Linux

通过使用此方案，您可以将管理组结构、包含的管理设备和其他组对象（策略、任务、全局任务、标签和设备分类）从 Kaspersky Security Center Windows 转移到 Kaspersky Security Center Linux 的管理下。迁移之前，请确保Kaspersky Security Center Windows 的必要功能在 Kaspersky Security Center Linux 中受支持。

限制：

- 只能从 Kaspersky Security Center Windows 版本 14.2 或更高版本迁移到 Kaspersky Security Center Linux 版本 15 或更高版本。
- 您只能使用 Kaspersky Security Center Web Console 来执行此方案。

阶段

迁移方案分阶段进行：

1. **选择迁移方法**

   您可以通过迁移向导迁移到 Kaspersky Security Center Linux。迁移向导步骤取决于 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否排列为层次结构：

   - 使用管理服务器层级进行迁移

     如果 Kaspersky Security Center Windows 管理服务器充当 Kaspersky Security Center Linux 管理服务器的辅助服务器，请选择此选项。您可以在 Kaspersky Security Center Web Console 的单个实例中管理迁移过程并在服务器之间切换。如果您更喜欢此选项，可以将管理服务器排列成层次结构以简化迁移过程。为此，请在开始迁移之前创建层次结构。

   - 使用导出文件（ZIP 存档）进行迁移

     如果 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器未按层次结构排列，请选择此选项。您使用 Kaspersky Security Center Web Console 的两个实例管理迁移过程：一个实例用于 Kaspersky Security Center Windows，另一个实例用于 Kaspersky Security Center Linux。在这种情况下，您将使用在从 Kaspersky Security Center Windows 导出期间创建和下载的导出文件并将此文件导入到 Kaspersky Security Center Linux。

2. **备份 Kaspersky Security Center Windows 管理服务器的证书和私钥（可选步骤）**

   您可能希望通过从备份副本恢复管理服务器的证书和私钥，将受管理设备置于 Kaspersky Security Center Linux 管理服务器的管理之下。在此情况下，备份 Kaspersky Security Center Windows 管理服务器的证书和私钥。然后在第 6 阶段，恢复证书和私钥。

3. **从 Kaspersky Security Center Windows 导出数据**

   打开 Kaspersky Security Center Windows，然后运行迁移向导。

4. **将数据导入到 Kaspersky Security Center Linux**

   继续运行迁移向导将导出的数据导入到Kaspersky Security Center Linux。如果服务器按层次结构排列，则在同一向导中成功导出后，导入会自动开始。如果服务器未按层次结构排列，您可以在切换到Kaspersky Security Center Linux 后继续运行迁移向导。

5. **执行其他操作以手动将对象和设置从 Kaspersky Security Center Windows 传输到 Kaspersky Security Center Linux（可选步骤）**

   您可能还想传输无法通过迁移向导传输的对象和设置。例如，您还可以执行以下操作：

   - 传输管理服务器和受管理应用程序使用的授权许可密钥
   - 配置管理服务器的全局任务
   - 配置网络代理策略设置
   - 创建应用程序安装包

- 创建虚拟服务器
- 分配和配置分发点
- 配置设备移动规则
- 配置自动标记设备规则
- 创建应用程序类别

6. **移动 Kaspersky Security Center Linux 管理的导入的受管理设备**

   要完成迁移，请将导入的受管理设备移至 Kaspersky Security Center Linux 的管理下。您可以通过以下方式之一进行操作：

   - 通过klmover 实用程序

     使用 klmover 实用程序并指定新管理服务器的连接设置。

   - 通过*更改管理服务器*任务

     创建*更改管理服务器*任务，指定导入的受管理设备、新的管理服务器以及其他任务设置。然后运行任务，将受管理设备置于 Kaspersky Security Center Linux 管理服务器的管理之下。

   - 通过删除（如果已安装）并在受管理设备上进一步安装网络代理

     创建新的网络代理安装包，并在安装包属性中指定新管理服务器的连接设置。删除导入的受管理设备上的网络代理，然后使用安装包通过远程安装任务在导入的受管理设备上安装网络代理。您还可以创建并使用独立的安装包在本地安装网络代理。有关详细信息，请参阅切换受 Kaspersky Security Center Linux 管理的受管理设备。

   - 通过从备份副本恢复管理服务器的证书和私钥（仅适用于迁移到 Kaspersky Security Center Linux 15.1 或更高版本）

     为安装了 Kaspersky Security Center Linux 管理服务器设备分配与 Kaspersky Security Center Windows 管理服务器相同的网络地址。使用 `-cert_only` 参数运行 klbackup 实用程序，从您在第 2 阶段保存的备份副本中恢复管理服务器证书和私钥。在命令行中，执行以下命令：`/opt/kaspersky/ksc64/sbin/klbackup -path <管理服务器证书备份副本的路径> -restore -cert_only`。有关详细信息，请参阅使用 klbackup 实用程序切换受管理设备至另一台管理服务器的管理下。

7. **将网络代理更新到最新版本**

   我们建议您将 Linux 网络代理升级到与 Kaspersky Security Center 相同的版本。

8. **确保受管理设备在新管理服务器上可见**

   在 Kaspersky Security Center Linux 管理服务器上，打开受管理设备列表（**资产(设备)→受管理设备**），然后检查**可见**、**网络代理已安装**和**上一次连接到管理服务器**列中的值。

其他数据迁移方法

除了迁移向导之外，您还可以传输特定任务和策略：

- 从 Kaspersky Security Center Windows 导出任务，然后导入任务到 Kaspersky Security Center Linux。
- 从 Kaspersky Security Center Windows 导出特定策略，然后导入政策到 Kaspersky Security Center Linux。相关的策略配置文件与选定的策略一起导出和导入。

从 Kaspersky Security Center Windows 导出组对象

从 Kaspersky Security Center Windows 到 Kaspersky Security Center Linux 的迁移管理组结构、包括的受管理设备和其他组对象，需要您首先选择要导出的数据并创建导出文件。导出文件包含有关要迁移的所有组对象的信息。导出文件将用于以后导入到 Kaspersky Security Center Linux 中。

您可以导出以下对象：

- 受管理应用程序的任务和策略
- 全局任务
- 自定义设备分类
- 管理组结构和包含的设备
- 已分配给迁移设备的标签

开始导出前，请阅读有关迁移到 Kaspersky Security Center Linux 的一般信息。选择迁移方法——使用或不使用 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 管理服务器的层次结构。

通过迁移向导导出受管理设备和相关组对象：

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否被排列成层次结构，执行以下操作之一：
   - 如果服务器被排列成层次结构，打开 Kaspersky Security Center Web Console，然后切换到 Kaspersky Security Center Windows 的服务器。
   - 如果服务器未排列成层次结构，请打开连接到 Kaspersky Security Center Windows 的 Kaspersky Security Center Web Console。
2. 在主菜单中，转到“**操作 → 迁移**”。
3. 要启动向导并按照其步骤操作，请选择要将数据和设置传输到的位置。
   - 如果您要将数据和设置传输到 Kaspersky Security Center 云控制台，请选择**迁移到 Kaspersky Security Center 云控制台**。
   - 如果您要将数据和设置传输到 Kaspersky Security Center Linux 或 Kaspersky XDR Expert，请选择“**迁移到 Kaspersky Security Center Linux 或 Open Single Management Platform**”。
4. 选择要导出的管理组或子组。请确保所选的管理组或子组包含的设备不得超过 10,000 台。
5. 选择将导出其任务和策略的受管理应用程序。仅选择 Kaspersky Security Center Linux 支持的应用程序。不受支持的应用程序的对象仍将被导出，但将不可操作。
6. 使用左侧的链接，以选择全局任务、设备分类和要导出的报告。您可通过“**组对象**”链接在导出中排除自定义角色、内部用户和安全组以及自定义应用程序类别。

导出文件（ZIP 存档）已创建。根据您是否使用管理服务器层次结构支持执行迁移，导出文件将保存如下：

- 如果服务器排列成层次结构，导出文件将被保存到Kaspersky Security Center Web Console 服务器上的临时文件夹中。
- 如果服务器未排列成层次结构，则导出文件将被下载到您的设备。

对于具有管理服务器层次结构支持的迁移，导入会在成功导出后自动开始。对于没有管理服务器层次结构支持的迁移，您可以手动将保存的导出文件导入到 Kaspersky Security Center Linux。

将导出文件导入到 Kaspersky Security Center Linux

要传输有关从 Kaspersky Security Center Windows 导出的受管理设备、对象及其设置的信息，必须将其导入 Kaspersky Security Center Linux 或 Kaspersky Next XDR Expert。

通过迁移向导导入受管理设备和相关组对象：

1. 根据 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux 的管理服务器是否被排列成层次结构，执行以下操作之一：
   - 如果服务器按层次结构排列，则在导出完成后继续执行迁移向导的下一步。在此向导中成功导出后，导入会自动开始（请参阅本说明的步骤 2）。
   - 如果服务器未按层次结构排列：
     a. 打开连接到 Kaspersky Security Center Linux 或 Kaspersky Next XDR Expert 的 Kaspersky Security Center Web Console。
     b. 在主菜单中，转到“**操作** → **迁移**”。
     c. 选择您在从 Kaspersky Security Center Windows 导出过程中创建并下载的导出文件（ZIP 存档）。开始上传导出文件。
2. 导出文件上传成功后，即可继续导入。如果要指定其他导出文件，请单击**更改**链接，然后选择所需的文件。
3. Kaspersky Security Center Linux 管理组的整个层次结构将得以显示。
   选中目标管理组旁边的复选框，导出的管理组的对象（受管理设备、策略、任务和其他组对象）必须还原到该目标管理组。
4. 开始导入组对象。导入期间将无法最小化迁移向导和执行任何并行操作。等待至对象列表中所有项目旁边的刷新图标 (🔄) 均替换为绿色复选标记 (✓)，导入完成。
5. 导入完成后，导出的管理组结构（包括设备详情）将显示在所选目标管理组下。如果还原的对象的名称与现有对象的名称相同，则将为还原的对象添加一个增量后缀。

> 如果在迁移的任务中指定了运行该任务的账户的详细信息，则导入完成后您必须打开该任务并再次输入密码。

如果导入已完成但出现错误，您可以执行以下操作之一：

- 对于具有管理服务器层次结构支持的迁移，您可以再次开始导入导出文件。
- 对于没有管理服务器层次结构支持的迁移，您可以启动迁移向导选择另一个导出文件，然后再次导入。

您可以检查导范围中包含的组对象是否已成功导入到 Kaspersky Security Center Linux。为此，请转到**资产(设备)**部分并确保导入的对象是否出现在相应的子部分中。

请注意，导入的受管理设备显示在**受管理设备**子部分中，但它们在网络中不可见，并且网络代理未安装并在其上运行（**可见**、**网络代理已安装**和**网络代理正在运行**列中的*否*值）。

要完成迁移，您需要将受管理设备切换到Kaspersky Security Center Linux 的管理之下。

将受管理设备切换为受 Kaspersky Security Center Linux 管理

将受管理设备、对象及其设置的信息成功导入 Kaspersky Security Center Linux 后，您需要将受管理设备切换到 Kaspersky Security Center Linux 的管理下才能完成迁移。

您可以通过以下方法之一将受管理设备移至Kaspersky Security Center Linux 下：

- 使用klmover 实用程序。
- 使用*更改管理服务器*任务。
- 从备份副本恢复管理服务器的证书和私钥（仅适用于迁移到 Kaspersky Security Center Linux 15.1 或更高版本）。

  有关详细信息，请参阅主要迁移场景的第 6 阶段。
- 通过远程安装任务在受管理设备上安装网络代理。

要通过安装网络代理将受管理设备切换为由 Kaspersky Security Center Linux 管理：

1. 删除将在 Kaspersky Security Center Linux 管理下切换的导入受管理设备上的网络代理。
2. 切换到 Kaspersky Security Center Windows 的管理服务器。
3. 进入**发现和部署→部署和分配→安装包**，然后打开网络代理现有安装包的属性。

   如果软件包列表中没有网络代理安装包，请下载新的安装包。

   您还可以创建并使用独立的安装包在本地安装网络代理。
4. 在**设置**选项卡上，选择**连接**区域。指定 Kaspersky Security Center Linux 的管理服务器的连接设置。
5. 为导入的受管理设备创建远程安装任务，然后指定重新配置的网络代理安装包。

   您可以通过 Kaspersky Security Center Windows 的管理服务器或通过充当分发点的基于 Windows 的设备安装网络代理。如果您使用管理服务器，请启用**通过管理服务器使用操作系统资源**选项。如果您使用分发点，请启用“**通过分发点使用操作系统资源**”选项。
6. 运行远程安装任务。

远程安装任务成功完成后，请转至 Kaspersky Security Center Linux 的管理服务器并确保受管理设备在网络中可见，并且网络代理已安装并在其上运行（**可见**、**网络代理已安装**和**网络代理正在运行**列中的*“是”*值）。

登录到 Kaspersky Security Center Web Console 并登出

您可以在安装管理服务器和 Web Console 服务器后登录到 Kaspersky Security Center Web Console。您必须知道安装过程中指定的管理服务器的 Web 地址和端口号（默认下，端口号是 8080）。在您的浏览器中，JavaScript 必须被启用。

您可以使用以下方法登录 Kaspersky Security Center Web Console：

- 使用域身份验证

  如果选择此方法，请确保域控制器轮询已激活并且域用户已添加到管理服务器。

- 通过指定域用户名和密码
- 指定管理员的用户名和密码

您想要用于登录 Kaspersky Security Center Web Console 的用户账户必须已分配角色。登录前，请确保域账户或内部用户账户已被分配角色。否则，将会出现登录错误。

使用域身份验证登录

要使用域身份验证登录 Kaspersky Security Center Web Console，请执行以下操作：

1. 在浏览器中，转到 https://<`Kaspersky Security Center Web Console` 地址>:<端口号>
   登录页面显示。
2. 如果您添加若干个受信任的服务器，在管理服务器列表选择您要连接的管理服务器。
   如果您只添加了一个管理服务器，则不会显示管理服务器列表。
3. 执行以下操作之一：
   - 单击**使用域身份验证**按钮。
   - 如果服务器上创建了一个或多个虚拟管理服务器，并且您要使用域身份验证登录到虚拟服务器：
     a. 单击**显示虚拟服务器选项**。
     b. 输入您在创建虚拟服务器时指定的虚拟管理服务器名称。
     c. 单击**使用域身份验证**按钮。
4. 如果为您的账户启用了两步验证，请指定移动设备上的认证应用生成的安全代码。
   如果需要，您可以返回登录页面。

登录后，控制板使用您最后使用的语言和主题显示。您可以通过 Kaspersky Security Center Web Console 导航并使用其操作 Kaspersky Security Center。

指定管理员的用户名和密码来登录

要通过指定管理员的用户名和密码登录 Kaspersky Security Center Web Console，请执行以下操作：

1. 在浏览器中，转到 https://<`Kaspersky Security Center Web Console` 地址>:<端口号>
登录页面显示。
2. 如果您添加若干个受信任的服务器，在管理服务器列表选择您要连接的管理服务器。
如果您只添加了一个管理服务器，则不会显示管理服务器列表。
3. 执行以下操作之一：
   - 要使用域用户账户登录管理服务器：
     a. 输入域用户的用户名和密码。
     您可以采用以下格式之一输入域用户的用户名：
     - 用户名`@dns.domain`
     - `NTDOMAIN\`用户名
     b. 单击**登录**按钮。

     使用域用户账户登录之前，请轮询域控制器以获取域用户列表。
   - 要登录到管理服务器:
     a. 输入本地管理员的用户名和密码。
     b. 单击**登录**按钮。
   - 如果服务器上创建了一个或多个虚拟管理服务器，并且您要登录到虚拟服务器：
     a. 单击**显示虚拟服务器选项**。
     b. 输入您在创建虚拟服务器时指定的虚拟管理服务器名称。
     c. 输入拥有虚拟管理服务器权限的管理员的用户名和密码。
     d. 单击**登录**按钮。
4. 如果为您的账户启用了两步验证，请指定移动设备上的认证应用生成的安全代码。
如果需要，您可以返回登录页面。
5. 如果为您的账户启用了强制更改密码或密码已过期，则会显示密码更改窗口。设置新密码以登录 Kaspersky Security Center Web Console。

登录后，控制板使用您最后使用的语言和主题显示。您可以通过 Kaspersky Security Center Web Console 导航并使用其操作 Kaspersky Security Center。

注销

要注销 Kaspersky Security Center Web Console，请执行以下操作：

在主菜单中，转到您的账户设置，然后选择**登出**。

Kaspersky Security Center Web Console 被关闭，且登录页面被显示。

Kaspersky Security Center Web Console中的身份和访问管理器

本节提供有关身份和访问管理器（也称为 IAM）的信息。

关于身份和访问管理器

身份和访问管理器（也称为 IAM）是一个 Kaspersky Security Center Web Console 组件，允许您在 Kaspersky Security Center Web Console 和 Kaspersky Industrial CyberSecurity for Networks Web 界面之间使用单点登录 (SSO)。IAM 使用 OAuth 2.0 协议来确保 Kaspersky Industrial CyberSecurity for Networks 在 Kaspersky Security Center Web Console 中的授权。

在这种情况下，您通过 Kaspersky Security Center Web Console 获得访问权限的 Kaspersky Industrial CyberSecurity for Networks 被称为*资源服务器*，Kaspersky Security Center Web Console 和 Kaspersky Industrial CyberSecurity for Networks Web 界面被称为 *OAuth 2.0 客户端*。资源服务器是用于多个用户的程序，需要授权。客户端使用*令牌*在资源服务器上进行授权。令牌是一个唯一的字节序列。当令牌过期时，它会自动重新颁发。IAM 用作多个 OAuth 2.0 客户端的单一授权服务器。

您可以在安装 Kaspersky Security Center Web Console 时安装 IAM。可以稍后随时在 Kaspersky Security Center Web Console 设置中启用它。如果 Kaspersky Industrial CyberSecurity 服务器或者 Kaspersky Industrial CyberSecurity Web 界面安装在同一台管理服务器管理的设备上，IAM 会检测到该程序，并且 Kaspersky Security Center Web Console 中会显示一条通知，告知您相关情况。您可以注册 Kaspersky Industrial CyberSecurity for Networks，然后在 Kaspersky Security Center Web Console 和 Kaspersky Industrial CyberSecurity for Networks Web 界面中都使用 SSO。

如果您退出 Kaspersky Security Center Web Console，您在 Kaspersky Industrial CyberSecurity for Networks Web 界面中的会话将结束，您必须再次登录 Kaspersky Security Center Web Console。

启用身份和访问管理器：方案

先决条件

在开始之前，请确保您可以访问 Kaspersky Industrial CyberSecurity for Networks 版本 3.1 或更高版本。

阶段

身份和访问管理器（也称为 IAM）的启用分阶段进行：

1. **检查必要端口**

   确保安装了 Kaspersky Security Center Web Console 的设备上已开放端口 3333、4004 和 4444。使用 OAuth 2.0 需要这些端口。如果需要，您可以在 Kaspersky Security Center Web Console 设置窗口中更改默认端口号。

   除了端口 3333、4004 和 4444，Kaspersky Security Center Web Console 还将端口 4445、2444 和 2445 用于各种目的。

2. **安装身份和访问管理器**

   在 Kaspersky Security Center Web Console 安装期间，指定您要安装身份和访问管理器。如果未指定，请再次运行 Kaspersky Security Center Web Console 安装向导。

3. **配置身份和访问管理器**

   在 Kaspersky Security Center Web Console 设置窗口中，确保"**身份和访问管理器 (IAM)**"切换按钮已启用。此外，指定安装了 Kaspersky Security Center Web Console 的设备的 DNS 名称：客户端应用程序将连接到该设备。

4. **指定令牌设置**

   在 Kaspersky Security Center Web Console 设置窗口中，指定身份和访问管理器将使用的令牌生命周期和授权超时。您可以使用默认值，也可以根据需要指定您自己的值。

5. **授予证书**

   如果您更喜欢使用管理服务器生成的证书，请在 Kaspersky Security Center Web 控制台设置窗口中下载 IAM 使用的端口的根证书并将它们分发到 Kaspersky Security Center Web Console 用户的工作站。否则，当尝试连接到 Kaspersky Security Center Web Console 时，用户的浏览器将显示错误消息。

6. **注册 Kaspersky Industrial CyberSecurity for Networks 服务器和 Kaspersky Industrial CyberSecurity for Networks Web 界面**

   安装 IAM 后，Kaspersky Security Center Web Console 会显示一条消息，指出一个 Industrial CyberSecurity for Networks 服务器（或多个服务器）和一个或多个 Kaspersky Industrial CyberSecurity for Networks Web 界面正在等待注册。单击此消息可注册您的 Kaspersky Industrial CyberSecurity for Networks 服务器（或多个服务器）和 Web 界面（或多个 Web 界面）。

结果

完成此方案后，您将能够在 Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky Security Center Web Console 中使用 SSO 和 IAM。

在 Kaspersky Security Center Web Console 中配置身份和访问管理器

套根据您的需求配置身份和访问管理器：

1. 在主菜单中，转到**设置→身份和访问管理器**。
2. 在**身份和访问管理器**区域，请确保已启用身份和访问管理器。

3. 单击“**设置**”行下的“**身份和访问管理器设备的网络名称**”链接。

4. 指定安装了身份和访问管理器的设备的 DNS 名称。客户端应用程序将连接到此设备。

5. 如果需要，通过单击相关设置组下的“**设置**”链接更改默认令牌设置、证书设置和端口号。

身份和访问管理器已启用并根据您的需求工作。

在 Kaspersky Security Center Web Console 中注册 Kaspersky Industrial CyberSecurity for Networks 应用程序

要开始通过 Kaspersky Security Center Web Console 使用 Kaspersky Industrial CyberSecurity for Networks Web 应用程序，您必须首先在 Kaspersky Security Center Web Console 中注册它。

要注册 Kaspersky Industrial CyberSecurity for Networks 应用程序：

1. 确保完成以下操作：

   - 您已下载并安装 Kaspersky Industrial CyberSecurity for Networks Web 插件。

     不过，您可以稍后在等待 Kaspersky Industrial CyberSecurity for Networks Server 与管理服务器同步时执行此操作。

   - 您已完成单点登录 (SSO) 技术使用准备场景。

   - Kaspersky Industrial CyberSecurity for Networks Web 界面中的必要设置在 Kaspersky Security Center 页面上进行指定。详情请参阅 Kaspersky Industrial CyberSecurity for Networks 在线帮助。

   - 您已以管理员账户登录 Kaspersky Security Center Web 控制台。

   - IAM 已配置。

2. 将安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备从未分配设备组移动到受管设备组：

   a. 在主菜单中，转到**发现和部署** → **未分配的设备**。

   b. 选中安装有 Kaspersky Industrial CyberSecurity for Networks Server 的设备旁边的复选框。

   c. 单击**移动到组**按钮。

   d. 在管理组的层次结构中，选中受管设备组旁边的复选框。

   e. 单击“**移动**”按钮。

3. 前往安装了 Kaspersky Industrial CyberSecurity for Networks Server 的设备的属性。

4. 在设备属性页面的 **常规** 部分，选择“**不要断开与管理服务器的连接**”选项，然后单击“**保存**”按钮。

5. 在设备属性页面，选择**应用程序**区域。

6. 在**应用程序**区域，选择卡巴斯基网络代理。

7. 如果应用程序的当前状态是“*已停止*”，等到它变为“*正在运行*”。

   这最多需要 15 分钟。如果您尚未安装 Kaspersky Industrial CyberSecurity for Networks Web 插件，您可以在等待期间立即安装。

8. 在主菜单中，转到**设置→身份和访问管理器**。

   在“**注册请求**”字段中，显示一个待处理的请求。

9. 点击“**注册请求**”字段下的“**设置**”链接。

10. 在打开的注册客户端列表中，选中 Kaspersky Industrial CyberSecurity for Networks Server 名称旁边的复选框，其状态为“*待办*”，然后单击“**批准**”按钮。

    如果您不想注册 Kaspersky Industrial CyberSecurity for Networks Server，您可以单击“拒绝”按钮并稍后返回此列表。

    点击“**批准**”按钮后，状态会变为*已批准*“，然后变为”*就绪*“。如果状态没有改变，您可以单击“刷新”按钮。

11. 关闭已注册客户端列表并确保“**已注册客户端**”字段中的值增加了。

12. 要在仪表板上添加 Kaspersky Industrial CyberSecurity for Networks 小部件：

    a. 在主菜单中，转到**监控和报告 → 控制板**。

    b. 在仪表板上，单击”**添加或还原 Web 小部件**“按钮。

    c. 在打开的小部件菜单中，选择“**其它**”。

    d. 选择 Kaspersky Industrial CyberSecurity for Networks 小部件。

    您现在可以使用小部件中的链接前往 Kaspersky Industrial CyberSecurity for Networks Web 界面。

完成注册程序后，一个新的按钮**Kaspersky Security Center**出现在 Kaspersky Industrial CyberSecurity for Networks Web 界面的登录页面上。您可以单击此按钮以在您的 Kaspersky Security Center 凭据下登录 Kaspersky Industrial CyberSecurity for Networks Web 界面。

身份和访问管理器的令牌生命周期和授权超时

在配置身份和访问管理器（也称为 IAM）时，您必须指定令牌生命周期和授权超时的设置。默认设置旨在反映安全标准和服务器负载。但是，您可以根据您组织的策略更改这些设置。

当令牌即将到期时，IAM 会自动重新颁发令牌。

下表列出了默认的令牌生命周期设置。

令牌生命周期设置

令牌	默认生命周期（以秒为单位）	描述
身份令牌 (id_token)	86400	OAuth 2.0 客户端（即 Kaspersky Security Center Web Console 或 Kaspersky Industrial CyberSecurity Console）使用的身份令牌。IAM 向客户端发送包含用户信息（即用户配置文件）的 ID 令牌。
访问令牌 (access_token)	86400	OAuth 2.0 客户端用来代表 IAM 标识的资源所有者访问资源服务器的访问令牌。
刷新令牌 (refresh_token)	172800	OAuth 2.0 客户端使用此令牌重新颁发身份令牌和访问令牌。

下表列出了 auth_code 和 login_consent_request 的超时时间。

授权超时设置

设置	默认超时时间（以秒为单位）	描述
授权码 (auth_code)	3600	交换令牌代码的超时时间。OAuth 2.0 客户端将此代码发送到资源服务器并获取访问令牌作为交换。
登录同意请求超时 (login_consent_request)	3600	将用户权限委派给 OAuth 2.0 客户端的超时时间。

有关令牌的更多信息，请参见 OAuth 网站。

要为未检测到鼠标或键盘活动的客户端配置超时：

1. 在 Kaspersky Security Center Web Console 的安装文件夹中，找到并打开 config.json 文件。该文件包含配置空闲客户端超时的参数。
2. 使用`clientIdleTimeout`参数指定时间（以毫秒为单位），在此时间之后不活动的客户端会显示警告弹出窗口。
3. 使用`clientLogoutTimeout`参数指定时间（以毫秒为单位），在此时间之后，不活动的客户端的 IAM 授权将终止。`clientLogoutTimeout`在`clientIdleTimeout`之后按顺序倒计时。

下载和分发 IAM 证书

默认情况下，身份和访问管理器使用管理服务器生成的证书授予浏览器访问 Kaspersky Security Center Web Console 的权限。但是，如果需要，您可以使用自定义证书。无论您使用什么证书，都必须确保 Kaspersky Security Center Web Console 用户用来访问 Kaspersky Security Center Web Console 的所有工作站都信任此证书。

要下载和分发证书：

1. 在主菜单中，转到**设置→身份和访问管理器**。
2. 对于每个证书，单击设置相关设置组下的“**设置**”链接，然后执行以下操作之一：
   - 如果要使用管理服务器在 Kaspersky Security Center Web Console 安装期间生成的证书：
     1. 在打开的证书属性窗口中选择“**管理服务器生成的证书**”。
     2. 单击“**安装**”按钮下载证书。
     3. 将下载的证书分发到 Kaspersky Security Center Web Console 用户用来访问 Kaspersky Security Center Web Console 的所有工作站。
   - 如果您有要使用的证书：
     1. 在打开的证书属性窗口中选择“**自定义 TLS 证书**”。
     2. 选择证书文件和私钥。

3. 单击“**确定**”按钮。

4. 将证书分发到用户用来访问 Kaspersky Security Center Web Console 或 Kaspersky Industrial CyberSecurity Console 的所有工作站。

这些证书授予用户访问 Kaspersky Security Center Web Console 和 Kaspersky Industrial CyberSecurity Console 的权限。

您必须及时重新签发所有证书。管理服务器生成的证书必须手动重新生成。Kaspersky Security Center Web Console 生成的证书 安装程序必须使用安装程序重新生成。

禁用身份和访问管理器

如果希望，您可以禁用身份和访问管理器（也称为 IAM）。

要禁用 IAM，

1. 在主菜单中，转到“**设置 → 整合**”。

2. 在**身份和访问管理器**部分，将**身份和访问管理器**切换按钮切换为禁用。

您稍后可以随时启用 IAM。

如果您通过安装程序更新 Kaspersky Security Center Web Console 并指定您不想安装 IAM，则 Kaspersky Security Center Web Console 将升级并且不会安装 IAM。所有与 Kaspersky Industrial CyberSecurity for Networks 集成有关的信息以及 IAM 配置文件和日志文件都将从您的设备中删除。

使用 NTLM 和 Kerberos 协议配置域身份验证

Kaspersky Security Center 15.1 允许您在 OpenAPI 中通过 NTLM 和 Kerberos 协议使用域身份验证。使用域身份验证允许 Windows 用户在 Kaspersky Security Center Web Console 中启用安全身份验证，而无需在公司网络上重新输入密码（单点登录）。

在 OpenAPI 中通过 Kerberos 协议进行域身份验证具有以下限制：

- 在 Active Directory 中必须使用 Kerberos 协议对 Kaspersky Security Center Web Console 的用户进行身份验证。用户必须具有有效的 Kerberos 票证授予票证（也称为 TGT）。当您对域进行身份验证时，将自动颁发 TGT。

- 您必须在浏览器中配置 Kerberos 身份验证。有关详细信息，请参阅所用浏览器的文档。

如果要通过 Kerberos 协议使用域身份验证，您的网络必须满足以下条件：

- 管理服务器必须在域账户名下运行。

- Kaspersky Security Center Web Console 服务器必须安装在安装管理服务器的同一设备上。

- 您必须为管理服务器账户指定以下服务主体名称 (SPN)：
  - "http/<server.fqnd.name>"
  - "http/<server>"

  这里，<server> 是管理服务器设备的网络名称，<server.fqnd.name> 是管理服务器设备的 FQDN 名称。
- 连接到管理控制台或 Kaspersky Security Center Web Console 时，所指定的管理服务器地址必须与注册了服务主体名称 (SPN) 的地址完全相同。您可以指定 <server.fqnd.name> 或 <server>。
- 要实现免密码登录，在其中将 Kaspersky Security Center Web Console 作为浏览器打开的浏览器进程必须在域账户下运行。

只有 Kaspersky Security Center 15.1 的 OpenAPI 支持 Kerberos 和 NTLM 协议。Kaspersky Security Center Linux 的 OpenAPI 不支持。

配置管理服务器

本部分介绍 Kaspersky Security Center 管理服务器的配置过程和属性。

配置 Kaspersky Security Center Web Console 到管理服务器的连接

要设置管理服务器连接端口：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**连接端口**”区域。

   应用程序显示所选服务器的主要连接设置。

Kaspersky Security Center Web Console 通过 SSL 端口 TCP 13299 连接到管理服务器。klakaut 自动化对象可以使用同一端口。

端口 TCP 14000 仅可以用于连接 Kaspersky Security Center Web Console、分发点、从属管理服务器和 klakaut 自动化对象，以及用于从客户端设备接收数据。

通常 SSL 端口 TCP 13000 仅可以被网络代理、从属管理服务器和 DMZ 中的主管理服务器使用。在一些情况下，Kaspersky Security Center Web Console 可能需要通过 SSL 端口 13000 连接：

- 如果单个 SSL 端口可能被用于 Kaspersky Security Center Web Console 和其他活动（从客户端设备接收数据、连接分发点、连接从属管理服务器）。
- 如果 klakaut 自动化对象未直接连接到管理服务器，而是通过 DMZ 中的分发点。

配置管理服务器连接事件记录

操作期间的连接历史和到管理服务器的连接尝试可以被保存到文件。文件中的信息允许您跟踪不仅您的网络基础设施中的连接，还有非授权的到服务器的访问尝试。

要记录连接管理服务器事件：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**连接端口**”区域。

3. 启用“**记录管理服务器连接事件**”选项。

   与管理服务器的入站连接、身份验证结果和SSL错误的所有进一步事件都将保存到%ProgramData%\KasperskyLab\adminkit\logs\SC.syslog文件中。

指定管理服务器的互联网连接设置

您必须配置互联网连接才能使用卡巴斯基安全网络和为 Kaspersky Security Center 及受管理的卡巴斯基应用程序下载反病毒数据库更新。

要指定管理服务器的互联网访问设置：

1. 在主菜单，单击管理服务器名称旁边的设置图标 ( )。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**配置互联网访问**”区域。

3. 如果您要在连接到互联网时使用代理服务器，请启用“**使用代理服务器**”选项。如果启用此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

   - **地址**

     Kaspersky Security Center 用于连接到互联网的代理服务器地址。

   - **端口号**

     将建立 Kaspersky Security Center 代理服务器连接的端口号。

   - **对本地地址不使用代理服务器**

     将不会使用代理服务器连接本地网络的设备。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  如果选中“**使用代理服务器**”复选框，则该输入字段可用。

- **用户名**

  用于与代理服务器建立连接的用户账户（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

- **密码**

  建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

  要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

您还可以使用快速启动向导配置互联网访问。

设置事件存储库中的最大事件数量

在管理服务器属性窗口的“**事件存储库**”部分，您可以通过限制事件记录数和存储期限来编辑管理服务器数据库的事件存储设置。当您指定事件最大数时，应用程序计算用于指定数目的存储空间的大概大小。您可以使用该大概计算来评估您在磁盘上是否具有足够空间以避免数据库溢出。管理服务器数据库的默认容量是 400,000 个事件。最大建议的数据库容量是 45,000,000 个事件。

应用程序每 10 分钟检查一次数据库。如果事件数达到指定的最大值加 10,000，应用程序将删除最旧的事件，以便仅保留指定的最大事件数。

当管理服务器删除旧事件后，它无法保存新事件到数据库。在此时间段内，拒绝事件的信息被写入卡巴斯基事件日志。新事件被列队，然后在删除操作后被保存到数据库。

要限制存储在管理服务器事件存储库中的事件的数量：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**事件存储库**”区域。指定存储在数据库中的最大事件数量。

3. 单击“**保存**”按钮。

此外，您可以执行以下操作：

- 更改任何任务的设置以保存与任务进度相关的事件，或者仅保存任务执行结果。

- 减少或禁用安装在受管理设备上的管理服务器、网络代理和卡巴斯基应用程序的事件的存储期限。

为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

UEFI 保护设备连接设置

*UEFI 保护设备*是在 BIOS 级别集成了适用于 UEFI 的卡巴斯基解决方案或应用程序的设备。整合的保护从系统启动时开始确保设备安全，未整合软件的设备仅在安全应用程序启动后开始保护工作。支持这些设备的管理的 Kaspersky Security Center。

要修改 UEFI 保护设备的连接设置：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**附加端口**”区域。
3. 修改相关设置：
   - **打开 UEFI 保护设备和 KasperskyOS 设备的端口**

     UEFI 保护设备可以连接到管理服务器。

   - **UEFI 保护设备和 KasperskyOS 设备的端口**

     如果启用了**打开 UEFI 保护设备和 KasperskyOS 设备的端口**选项，您可以更改端口号。默认端口号是 13294。
4. 单击“**保存**”按钮。

UEFI 保护设备现在可以连接到管理服务器。

创建管理服务器层级：添加从属管理服务器

添加从属管理服务器（在未来的主管理服务器上执行）

您可以添加管理服务器作为从属管理服务器，从而建立“主/从属”层级。

要添加可以通过 Kaspersky Security Center Web Console 连接的从属管理服务器：

1. 确保未来主管理服务器的端口 13000 可用于从从属管理服务器接收连接。
2. 在未来主管理服务器上，单击“设置”图标 ( )。
3. 在打开的属性页面上，选择“**管理服务器**”选项卡。
4. 选择您要向其添加管理服务器的管理组名称旁边的复选框。
5. 在菜单行中，单击“**连接从属管理服务器**”。
   “添加从属管理服务器向导”启动。使用“**下一步**”按钮继续向导操作。

6. 填充以下字段：

- **连接主管理服务器到 DMZ 中的从属管理服务器**

  如果从属管理服务器位于隔离区 (DMZ)，选择该选项。

  如果选择此选项，则需要指定**从属服务器地址**参数。

  如果选择此选项，主管理服务器将发起与从属管理服务器的连接。否则，从属管理服务器将发起与主管理服务器的连接。

- **从属管理服务器显示名称**

  从属管理服务器将显示在层级的名称。如果需要，您可以输入 IP 地址作为名称，也可以使用名称，例如"组 1 的从属服务器"。

- **从属管理服务器地址(可选)**

  指定从属管理服务器的 IP 地址或域名。

  如果启用了"**连接主管理服务器到 DMZ 中的从属管理服务器**"选项，则需要此参数。

- **管理服务器 SSL 端口**

  指定主管理服务器上的 SSL 端口号。默认端口号是 13000。

- **管理服务器 API 端口**

  指定主管理服务器上的端口号以通过 OpenAPI 接收连接。默认端口号是 13299。

7. 指定从属管理服务器的证书如果指定了**从属服务器地址**参数，则可以单击"**从从属管理服务器获取**"按钮来获取证书。否则，单击"**浏览证书文件**"按钮并找到证书文件。

8. 指定连接设置：

   - 输入将来的主管理服务器的地址。
   - 如果将来的从属管理服务器使用代理服务器，请输入代理服务器地址和用户凭证以连接到代理服务器。

9. 输入对将来的从属管理服务器具有访问权限的用户的凭证。

10. 如果启用并配置了两步验证，请指定认证应用生成的安全代码。

    如果启用了两步验证，但未针对您指定的账户配置，则可从将来的从属服务器创建层级（请参阅下方说明）。

如果连接设置正确，则与将来的从属服务器建立连接，并建立"主/从属"层级。如果连接失败，请检查连接设置或手动指定将来的从属服务器的证书。

主管理服务器和从属管理服务器之间的连接通过端口 13000 建立。主管理服务器的任务和策略被接收和应用。从属管理服务器显示在主管理服务器上，在添加其的管理组中。

添加从属管理服务器（在未来的从属管理服务器上执行）

如果您无法连接到未来从属管理服务器（例如，它临时被断开或无法连接），您仍可以添加从属管理服务器。

要添加不可以通过 Kaspersky Security Center Web Console 连接的管理服务器作为从属：

1. 将未来主管理服务器的证书文件发送给未来从属管理服务器所在办公室的系统管理员。（例如，您可以将文件写入闪存驱动器等外部设备，或通过电子邮件发送它。）

   证书文件位于未来主管理服务器，在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer。

2. 提示未来从属管理服务器的责任系统管理员做以下事情：

   a. 单击设置图标（）。

   b. 在打开的属性页面上，转到“**常规**”选项卡的“**管理服务器层级**”区域。

   c. 选择**该管理服务器是服务器层级中的从属**选项。

   d. 在“**主管理服务器地址**”字段中，输入将来的主管理服务器的网络名称。

   e. 通过单击“**浏览**”选择先前保存的带有未来主管理服务器证书的文件。

   f. 如有必要，选中“**连接主管理服务器到 DMZ 中的从属管理服务器**”复选框。

   g. 如果通过代理服务器连接到将来的从属管理服务器，则选中“**使用代理服务器**”选项并指定连接设置。

   h. 点击“**保存**”。

“主/从属”层级被创建。主管理服务器开始使用端口 13000 从从属管理服务器接收连接。主管理服务器的任务和策略被接收和应用。从属管理服务器显示在主管理服务器上，在添加其的管理组中。

查看从属管理服务器列表

要查看从属（包括虚拟）管理服务器列表：

在主菜单中，单击“设置”图标（）旁边的管理服务器名称。

从属（包括虚拟）管理服务器下拉列表被显示。

您可以通过单击名称转到任一管理服务器。

管理组也会显示，但它们为灰显，无法在此菜单中进行管理。

如果您在 Kaspersky Security Center Web Console 中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，您可以使用以下方法之一：

- **修改现有的 Kaspersky Security Center Web Console 安装，以将从属服务器添加到受信任的管理服务器列表中**。然后您将能够在 Kaspersky Security Center Web Console 中连接到该虚拟管理服务器。

  1. 在安装了 Kaspersky Security Center Web Console 的设备上，在具有管理员权限的账户下运行 ksc-web-console-<版本号>.<内部版本号>.exe 安装文件。

     安装向导将启动。使用**下一步**按钮继续向导操作。

  2. 选择**升级**选项。
  3. 在“**修改类型**”步骤中，选择“**编辑连接设置**”选项。
  4. 在“**受信任的管理服务器**”步骤中，添加所需的从属管理服务器。
  5. 在最后一步中，单击**修改**以应用新设置。
  6. 在应用程序重新配置成功完成后，点击**完成**按钮。

- 使用 Kaspersky Security Center Web Console 直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 Kaspersky Security Center Web Console 中切换到该虚拟管理服务器。
- 使用基于 MMC 的管理控制台直接连接到虚拟服务器。

删除管理服务器层级

如果不再想拥有管理服务器层级结构，您可以从该层级将其断开连接。

要删除管理服务器层级：

1. 在主菜单，单击主管理服务器名称旁边的“设置”图标 ( )。
2. 在打开的页面上，转到“**管理服务器**选项卡。
3. 在要从其中删除从属管理服务器的管理组中，选择从属管理服务器。
4. 在菜单项目上，单击“**删除**”按钮。
5. 在打开的窗口中，单击“**确定**”以确认您要删除该从属管理服务器。

先前的主管理服务器和从属管理服务器现在彼此独立。层级不再存在。

管理服务器维护

通过管理服务器维护，您可以腾出管理服务器文件夹中的空间，并通过删除不再需要的对象来减少数据库存储量。这有助于您提高应用程序的性能和运行可靠性。我们建议您至少每周维护一次管理服务器。

管理服务器通过专用任务进行维护。在维护管理服务器时，应用程序执行以下操作：

- 从存储文件夹中删除不必要的文件夹和文件。
- 从表中删除不必要的记录（也称为“悬垂指针”）。
- 清除缓存。
- 维护数据库（如果您使用 SQL Server 或 PostgreSQL 作为 DBMS）：
  - 检查数据库中是否存在错误（仅适用于 SQL Server）。
  - 重组数据库索引。
  - 更新数据库统计信息。
  - 收缩数据库（如果必要）。

安装 Kaspersky Security Center 时，会自动创建“管理服务器维护”任务。如果“管理服务器维护”任务被删除，您可以手动创建它。

要创建管理服务器维护任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**添加**”按钮。
   “新任务向导”启动。
3. 在向导的“**新任务设置**”窗口中，选择“**管理服务器维护**”为任务类型并单击“**Next**下一步”按钮。
4. 遵照剩余的向导说明。

新创建的任务显示在任务列表中。一台管理服务器仅可以运行一个“管理服务器维护”任务。如果已经为管理服务器创建了“管理服务器维护”任务，则无法创建新的“管理服务器维护”任务。

配置界面

您可以将 Kaspersky Security Center Web Console 界面配置为显示和隐藏各区域和界面元素，具体取决于所使用的功能。

要根据当前使用的功能集配置 Kaspersky Security Center Web Console 界面：

1. 在主菜单中，转到您的账户设置，然后选择**界面选项**。
2. 在打开的“**界面选项**”窗口中，启用或禁用所需选项。
3. 点击**保存**。

之后，控制台会根据启用的选项在主菜单中显示相应区域。例如，如果您启用**显示 EDR 警告**，则**监控和报告** → **警报**区域会出现在主菜单中。

管理虚拟管理服务器

本部分介绍管理虚拟管理服务器的以下操作：

- 创建虚拟管理服务器
- 启用和禁用虚拟管理服务器
- 为虚拟管理服务器分配管理员
- 更改客户端设备的管理服务器
- 删除虚拟管理服务器

创建虚拟管理服务器

您可以创建虚拟管理服务器并添加它们到管理组。

当您创建虚拟管理服务器时，它会继承主管理服务器的用户列表和所有用户权限。如果用户有权访问主服务器，则该用户也有权访问虚拟服务器。创建后，您可以单独配置对服务器的访问权限。

要创建和添加虚拟管理服务器：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
2. 在打开的页面上，转到“**管理服务器**”选项卡。
3. 选择您要添加虚拟管理服务器到的管理组。
   虚拟管理服务器将管理选定组（包括子组）中的设备。
4. 在菜单行中，单击“**新虚拟管理服务器**”。
5. 在打开的页面上，定义新虚拟管理服务器的属性：
   - **虚拟管理服务器名称**。
   - **管理服务器连接地址**
     您可以指定管理服务器的名称或 IP 地址。
6. 从用户列表中，选择虚拟管理服务器管理员。如果您想，您可以编辑现有账户之一，然后分配其管理员角色，或创建一个新用户账户。
7. 点击“**保存**”。

新的虚拟管理服务器将创建，添加到管理组并显示在“**管理服务器**”选项卡上。

如果您在 Kaspersky Security Center Web Console 中连接到主管理服务器，但无法连接到由从属管理服务器管理的虚拟管理服务器，您可以使用以下方法之一：

- **修改现有的 Kaspersky Security Center Web Console 安装，以将从属服务器添加到受信任的管理服务器列表中**。然后您将能够在 Kaspersky Security Center Web Console 中连接到该虚拟管理服务器。

  1. 在安装了 Kaspersky Security Center Web Console 的设备上，在具有管理员权限的账户下运行 ksc-web-console-<版本号>.<内部版本号>.exe 安装文件。

     安装向导将启动。使用**下一步**按钮继续向导操作。

  2. 选择**升级**选项。

  3. 在“**修改类型**”步骤中，选择“**编辑连接设置**”选项。

  4. 在“**受信任的管理服务器**”步骤中，添加所需的从属管理服务器。

  5. 在最后一步中，单击**修改**以应用新设置。

  6. 在应用程序重新配置成功完成后，点击**完成**按钮。

- 使用 Kaspersky Security Center Web Console 直接连接到在其中创建了虚拟服务器的从属管理服务器。然后您将能够在 Kaspersky Security Center Web Console 中切换到该虚拟管理服务器。

- 使用基于 MMC 的管理控制台直接连接到虚拟服务器。

启用或禁用虚拟管理服务器

当您创建新的虚拟管理服务器时，默认情况下会启用它。您可以随时禁用或再次启用它。禁用或启用虚拟管理服务器等同于关闭或打开物理管理服务器。

要启用或禁用虚拟管理服务器：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。

2. 在打开的页面上，转到“**管理服务器**”选项卡。

3. 选择要启用或禁用的虚拟管理服务器。

4. 在菜单行上，单击“**启用/禁用虚拟管理服务器**”按钮。

   虚拟管理服务器状态被更改为已启用或禁用，具体取决于其先前的状态。更新的状态将显示在管理服务器名称旁边。

为虚拟管理服务器分配管理员

当您在组织中使用虚拟管理服务器时，可能希望为每个虚拟管理服务器分配一名专门的管理员。例如，当您创建虚拟管理服务器来管理组织的独立办公室或部门时，或者如果您是 MSP 提供商并通过虚拟管理服务器来管理您的租户时，这可能很有用。

当您创建虚拟管理服务器时，它会继承主管理服务器的用户列表和所有用户权限。如果用户有权访问主服务器，则该用户也有权访问虚拟服务器。创建后，您可以单独配置对服务器的访问权限。如果您想要仅为虚拟管理服务器分配管理员，请确保该管理员没有主管理服务器的访问权限。

您可以通过向管理员授予虚拟管理服务器的访问权限来为虚拟管理服务器分配管理员。您可以通过以下方式之一授予所需的访问权限：

- 手动配置管理员的访问权限
- 为管理员分配一个或多个用户角色

要登录 Kaspersky Security Center Web Console，虚拟管理服务器的管理员要指定虚拟管理服务器名称、用户名和密码。Kaspersky Security Center Web Console 会对管理员进行身份验证并打开管理员有权访问的虚拟管理服务器。管理员不能在管理服务器之间切换。

先决条件

在开始之前，请确保满足以下条件：

- 虚拟管理服务器已创建。
- 在主管理服务器上，您已为希望为其分配虚拟管理服务器的管理员创建一个账户。
- 您在“**修改对象 ACL** right in the **常规功能** → **用户权限**“修改对象 ACL”权限。

手动配置访问权限

要为虚拟管理服务器分配管理员：

1. 在主菜单，切换到所需的虚拟管理服务器：
   a. 单击当前管理服务器名称右侧的 V 形图标 ()。
   b. 选择所需的管理服务器。
2. 在主菜单，单击管理服务器名称旁边的“设置”图标 ()。
   管理服务器属性窗口将打开。
3. 在“**访问权限**”选项卡上，单击“**添加**”按钮。
   系统会打开主管理服务器和当前虚拟管理服务器的用户的统一列表。
4. 从用户列表中，选择要为虚拟管理服务器分配的管理员账户，然后单击“**确定**”按钮。
   应用程序将所选的用户添加到“**访问权限**”选项卡上的用户列表。
5. 选中已添加账户旁边的复选框，然后单击“**访问权限**”按钮。
6. 配置管理员将拥有的虚拟管理服务器的权限。

要成功进行身份验证，管理员至少必须具有以下权限：

- "**常规功能 → 基本功能**"功能区域中的**读取**权限
- "**常规功能 → 虚拟管理服务器**"功能区域中的**读取**权限

应用程序将修改后的用户权限保存到管理员账户中。

通过分配用户角色配置访问权限

或者，您可以通过用户角色向虚拟管理服务器管理员授予访问权限。例如，如果您想在同一个虚拟管理服务器上分配多个管理员，这可能很有用。如果是这种情况，您可以为管理员账户分配相同的一个或多个用户角色，而不是为多个管理员配置相同的用户权限。

通过分配用户角色为虚拟管理服务器分配管理员：

1. 在主管理服务器上，创建一个新的用户角色，然后指定管理员在虚拟管理服务器上必须拥有的所有所需访问权限。您可以创建多个角色，例如，如果您想要单独访问不同的功能区域。
2. 在主菜单，切换到所需的虚拟管理服务器：
   a. 单击当前管理服务器名称右侧的 V 形图标 (›)。
   b. 选择所需的管理服务器。
3. 向管理员账户分配新角色或多个角色。

应用程序向管理员账户分配角色。

配置对象级别的访问权限

除了分配功能区域级别的访问权限，您还可以在虚拟管理服务器上配置对特定对象的访问，例如对特定管理组或任务的访问。为此，请切换到虚拟管理服务器，然后在对象的属性中配置访问权限。

更改客户端设备的管理服务器

您可以使用"*更改管理服务器*"任务来更改管理客户端设备的管理服务器。任务执行完毕后，选定的客户端设备将由指定的管理服务器管理。

> 您不能对通过连接网关连接到管理服务器的客户端设备使用*更改管理服务器*任务。对于这样的设备，您必须重新配置网络代理或重新安装网络代理并指定连接网关。

要更改管理客户端设备的管理服务器：

1. 在主菜单中，转到"**资产(设备)**" → "**任务**"。
2. 单击**添加**。
   "新任务向导"启动。使用"**下一步**"按钮继续向导操作。

3. 在向导的“**新任务设置**”步骤中，指定以下设置：

   a. 在“**应用程序**”下拉列表中，选择**Kaspersky Security Center**。

   b. 在**任务类型**字段中，选择**更改管理服务器**。

   c. 在**任务名称**字段中，指定您正在创建的任务的名称。
   任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

   d. 选择要将任务分配到的设备：

   - **分配任务到管理组**

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。
     如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

   - **手动指定设备地址或从列表导入地址**

     您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - **分配任务到设备分类**

     该任务被分配到设备分类中的设备。您可以指定现有分类之一。
     例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

4. 在向导的**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。

5. 在向导的该步骤，确认您同意更改客户端设备的管理服务器的条款。

6. 在向导的该步骤，选择要用于管理选定设备的管理服务器：

   - **更改到另一个主管理服务器**

     要将客户端设备移动至另一台主管理服务器，请指定以下管理服务器连接设置：

     1. 在**管理服务器地址**字段中，指定新的主管理服务器的地址。
     2. 在**端口号**字段中，指定要连接到管理服务器的端口号。
        默认端口号是 14000。
     3. 在**SSL 端口**字段中，指定主管理服务器上的 SSL 端口号。
        默认端口号是 13000。
     4. 如有必要，请启用**使用代理服务器**选项。
        如果此选项被禁用，则使用直接连接将设备连接到管理服务器。

如果此选项被启用，请指定代理服务器参数：

- **代理服务器地址**
- **代理服务器端口**

如果您的代理服务器需要身份验证，请在 **用户名** 和 **密码**字段中指定与代理服务器建立连接的账户的凭据。我们建议您指定仅具有代理服务器身份验证所需的最低权限的账户的凭据。

5. 如有必要，请上传新的管理服务器证书。

- **在该主服务器上更改到另一个虚拟服务器**

选择此选项可以将客户端设备移动到当前主管理服务器上的虚拟管理服务器。为此，在**虚拟管理服务器名称**下拉列表中，选择必要的虚拟管理服务器。

7. 在向导的**选择账户以运行任务**步骤中，指定账户设置：

- **默认账户**

在与执行该任务的应用程序相同的账户下运行该任务。
默认情况下已选定该选项。

- **指定账户**

填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - **账户**

    运行该任务的账户。

  - **密码**

    任务运行时使用的账户的密码。

8. 如果要更改默认任务设置，请在向导的**完成任务创建**步骤中启用**创建完成时打开任务详情**选项。
   如果您不启用该选项，任务使用默认设置创建。您可以稍后随时更改默认设置。
9. 单击“**完成**”按钮。
   任务被创建并显示在任务列表。
10. 单击创建的任务的名称以打开任务属性窗口。
11. 如果要更改默认任务设置，请在任务属性窗口中根据需要指定常规任务设置。

12. 单击“**保存**”按钮。

    任务被创建和配置。

13. 运行创建的任务。

    在任务执行完毕后，为其创建任务的客户端设备将由任务设置中指定的管理服务器进行管理。

删除虚拟管理服务器

如果删除虚拟管理服务器，在管理服务器上创建的所有对象（包括策略和任务）也将被删除。由虚拟管理服务器管理的管理组中的受管理设备将被从管理组中删除。要返回 Kaspersky Security Center 管理的设备，请运行网络轮询，然后将找到的设备从未分配的设备组移动到管理组。

要删除虚拟管理服务器：

1. 在主菜单，单击管理服务器名称旁边的“设置”图标 ( )。
2. 在打开的页面上，转到“**管理服务器**”选项卡。
3. 选择要删除的虚拟管理服务器。
4. 在菜单项目上，单击“**删除**”按钮。

虚拟管理服务器被删除。

启用账户保护以防止未经授权的修改

您可以启用一个附加选项以保护用户账户免遭未经授权的修改。如果启用此选项，修改用户账户设置需要具有修改权限的用户的授权。

要启用或禁用账户保护以防止未经授权的修改：

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 单击要为其指定账户保护以防止未经授权的修改的内部用户账户的名称。
3. 在打开的用户设置窗口中，选择“**账户保护**”选项卡。
4. 在“**账户保护**”选项卡上，如果您希望在每次更改或修改账户设置时都请求凭据，则选择“**请求身份验证以检查修改用户账户的权限**”选项。否则，请选择“**无需其他身份验证即允许用户修改此账户**”选项。
5. 单击“**保存**”按钮。

即为用户账户启用账户保护，以防止未经授权的修改。

备份复制和管理服务器数据恢复

数据备份允许您将管理服务器从一台设备上转移至其他设备且无数据丢失。通过备份，您可以在移动管理服务器数据库到另一部设备或者升级到更新版本的 Kaspersky Security Center 时恢复数据。此外，您可以使用数据备份将管理服务器数据从 Kaspersky Security Center Windows 移动到 Kaspersky Security Center Linux 的管理下（不支持将数据从 Kaspersky Security Center Linux 移动到 Kaspersky Security Center Windows）。

已安装的管理插件不会被备份。从备份副本恢复管理服务器数据后，您需要下载并重新安装受管理应用程序的插件。

备份管理服务器数据之前，请检查虚拟管理服务器是否已添加到管理组。如果添加了虚拟管理服务器，请确保在备份之前为该虚拟管理服务器分配了管理员。备份后，您将无法授予管理员对虚拟管理服务器的访问权限。请注意，如果管理员账户凭据丢失，您将无法向虚拟管理员服务器分配新管理员。

要备份或恢复 Kaspersky Security Center 故障转移集群，您必须在备份或恢复完成后停止整个集群进行维护，然后重新启动它。

您可以使用以下方式之一创建管理服务器数据的备份副本：

- 通过使用管理控制台创建并运行数据备份任务。
- 通过在已安装管理服务器的设备上运行 klbackup 实用程序。该实用程序包含在 Kaspersky Security Center 分发包。管理服务器安装完毕后，该实用程序位于程序安装时指定文件夹的根目标中。

以下数据保存在管理服务器的备份副本中：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）。
- 有关管理组和客户端设备的结构的配置详情。
- 远程安装的应用程序分发包的存储库。
- 管理服务器证书。
- *更新*文件夹的内容。

  默认情况下，文件夹路径为 C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

只用使用 klbackup 实用程序才能进行管理服务器数据恢复。您必须在刚刚安装的、与备份副本具有相同或更新版本的管理服务器的可运行实例上执行恢复。

创建数据备份任务

备份任务是管理服务器任务，通过快速启动向导进行创建。如果由快速启动向导创建的备份任务被删除，您可以手动创建备份任务。

若要创建管理服务器数据备份任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**添加**”按钮。
   “新任务向导”启动。
3. 在该向导的“**新任务设置**”窗口中，选择名为“**备份管理服务器数据**”的任务类型。
4. 遵照剩余的向导说明。

该“**备份管理服务器数据**”任务只能在一个副本中创建。如果已经为管理服务器创建了管理服务器数据备份任务，它不会显示在“管理服务器备份任务创建向导”的任务类型选择窗口中。

要配置管理服务器数据备份任务：

1. 在主菜单中，转到**资产(设备)→任务**，然后选择**备份管理服务器数据**任务。
2. 单击**备份管理服务器数据**任务。
   任务属性窗口打开。
3. 如有必要，请根据需要指定常规任务设置。
4. 在**应用程序设置**部分，指定用于存储管理服务器数据备份副本的文件夹路径，设置备份保护密码以及备份副本数量（如果需要）。
5. 单击**保存**以应用更改。

*管理服务器数据备份*任务已配置。

将管理服务器移动至其他设备

如果需要在新设备上使用管理服务器，可以通过以下方式之一进行移动：

- 将管理服务器和数据库服务器移动到新设备（数据库服务器可以与管理服务器一起安装在新设备上，也可以安装在另一台设备上）。
- 将数据库服务器保留在以前的设备上，仅将管理服务器移至新设备。

要将管理服务器和数据库服务器移至新设备：

1. 在先前设备上，创建管理服务器数据的备份。
   为此，您可以通过 Kaspersky Security Center Web Console 运行数据备份任务或运行 klbackup 实用程序。

   如果您使用 SQL Server 作为管理服务器的 DBMS，您可以将数据从 SQL Server 迁移到 MySQL 或 MariaDB DBMS。为此，请运行交互模式下的 klbackup 实用程序以创建数据备份。在备份和还原向导**迁移到 MySQL/MariaDB 格式**窗口中启用**备份设置**选项。Kaspersky Security Center 将创建与 MySQL 和 MariaDB 兼容的备份。之后，您可以将备份中的数据恢复到 MySQL 或 MariaDB。

如果希望将数据从 SQL Server 迁移到 Azure SQL DBMS，您还可以启用"**迁移到 Azure 格式**"选项。

2. 在之前的设备上，断开管理服务器与网络的连接。

3. 选择要安装管理服务器的新设备。确保所选设备上的硬件和软件符合管理服务器、Kaspersky Security Center Web Console 和网络代理的要求。此外，请检查管理服务器上使用的端口是否可用。

4. 为新设备分配相同地址。

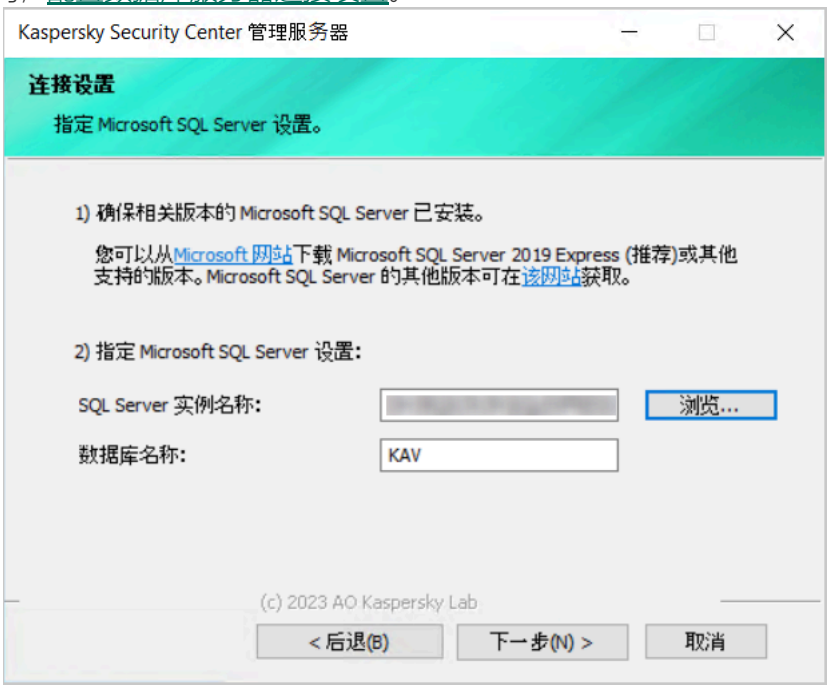
   可以为新的管理服务器分配 NetBIOS 名称、FQDN 和静态 IP 地址。这取决于部署网络代理时在网络代理安装包中设置了哪个管理服务器地址。或者，您可以使用确定网络代理连接到的管理服务器的连接地址（您可以使用klnagchk 实用程序在受管理设备上获取此地址）。

5. 如有需要，在另一台设备上，安装管理服务器将使用的数据库管理系统 (DBMS)。

   数据库可以与管理服务器一起安装在新设备上，也可以安装在另一台设备上。确保该设备满足硬件和软件要求。选择 DBMS 时，请考虑管理服务器覆盖的设备数量。

6. 在新设备上运行管理服务器的安装。

7. 在管理服务器安装期间，配置数据库服务器连接设置。



Microsoft SQL Server 的"连接设置"窗口示例

根据数据库服务器的安装位置，执行以下操作之一：

- **将数据库服务器保留在先前设备上**

  1. 单击**SQL Server 实例名称**字段旁边的**浏览**按钮，然后在出现的列表中选择之前的设备名称。
     请注意，先前设备必须可用于连接新的管理服务器。
  2. 在**数据库名称**字段中输入以前的数据库名称。

- **将数据库服务器移至另一台设备**

  1. 单击**浏览**字段旁边的**SQL Server 实例名称**按钮，然后在出现的列表中选择设备名称。
  2. 在**数据库名称**字段中输入新的数据库名称。

     请注意，新数据库名称必须与先前设备中的数据库名称相匹配。数据库名称必须相同，以便使用管理服务器备份。默认数据库名称是 *KAV*。

8. 安装完成后，在新设备上使用 klbackup 实用程序恢复管理服务器数据。

   如果在先前设备和新设备上使用 SQL Server 作为 DBMS，请注意，新设备上安装的 SQL Server 版本必须不得低于先前设备上安装的 SQL Server 版本。否则，将无法在新设备上恢复管理服务器数据。

9. 打开 Kaspersky Security Center Web Console 并连接到管理服务器。
10. 验证是否所有受管理设备都连接到了管理服务器。
11. 从以前的设备中卸载管理服务器和数据库服务器。

您也可以使用管理控制台，将管理服务器和数据库服务器移至其他设备。

使用 klscmodchk 和 integrity_checker 实用程序检查模块的完整性

Kaspersky Security Center 包含动态链接库、可执行文件、配置文件和接口文件形式的多个二进制模块。入侵者可以用包含恶意代码的其他文件替换一个或多个可执行模块或应用程序文件。为了防止模块和文件替换，Kaspersky Security Center 使用 klscmodchk 和 integrity_checker 实用程序提供组件完整性检查。这些实用程序可检查模块和文件是否有未经授权的更改或损坏。如果模块或应用程序文件的校验和不正确，则被视为已损坏。

klscmodchk 实用程序对以下 Kaspersky Security Center 组件执行完整性检查：

- 管理服务器
- 网络代理
- 带有清单文件的管理控制台的管理插件

integrity_checker 实用程序可对以下 Kaspersky Security Center 组件执行完整性检查：

- 管理服务器
- 网络代理
- Kaspersky Security Center Web Console

这两个实用程序都可根据 kl_file_integrity_manifest.xml 清单文件检查模块完整性，该文件是 Kaspersky Security Center 内部版本的一部分，位于安装程序文件夹中。组件清单文件包含的文件的完整性对于 Kaspersky Security Center 组件的正确运行非常重要。清单文件本身的完整性也会得到检查。

强烈建议不要修改 kl_file_integrity_manifest.xml 清单文件，因为这将使数字签名无效并导致完整性检查失败。

要检查 Kaspersky Security Center 组件的完整性，请运行以下命令之一：

- `$ klscmodchk [ 参数 ]`

  klscmodchk 实用程序使用`--verbose`参数启动 integrity_checker 实用程序并检查模块的完整性。

  klscmodchk 实用程序的参数：

  - `-logfile <log_file_path>`— 指定磁盘上用于记录的文件的路径。默认情况下，信息被输出到控制台。
  - `-chkplugins`—检查已安装的管理控制台管理插件模块（包括清单文件）的完整性。默认情况下，不检查管理插件。
  - `-verbose`— 在完整性检查期间输出扩展信息。

- `$ integrity_checker [ 参数 ] <manifest_file_path>`

  integrity_checker 实用程序的参数：

  - `--help` — 显示 integrity_checker 实用程序帮助。
  - `--version` — 显示 integrity_checker 实用程序版本。
  - `--verbose` — 显示有关实用程序操作的信息。执行完整性检查时，在命令中使用此参数就足够了。

每个清单文件的检查结果以以下格式显示在清单文件名旁边：

- SUCCEEDED — 文件完整性得到确认（返回代码 0）。
- FAILED — 文件完整性未确认（非零返回代码）。

您还可以将完整性检查配置为在启动应用程序时自动运行。默认情况下，自动完整性检查处于禁用状态。

要启用自动完整性检查：

1. 在安装了管理服务器的设备上，在 Windows 命令提示符中输入以下命令：

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. 重启设备(&R)

自动完整性检查已启用。

下次运行 Kaspersky Security Center 时，klscmodchk 实用程序将与管理服务器一起运行，并启动模块完整性检查。完整性检查的结果将被写入卡巴斯基事件日志。

Kaspersky Security Center Web Console 的初始设置

本节介绍在安装 Kaspersky Security Center Web Console 后执行其初始设置所必须采取的步骤。

快速启动向导（Kaspersky Security Center Web Console）

该部分提供了管理服务器快速启动向导的信息。

> 该向导需要互联网连接。如果您的管理服务器无法访问互联网，我们建议您通过 Kaspersky Security Center Web Console 界面手动执行向导的所有步骤。

Kaspersky Security Center 允许您对构建集中式管理系统以实施网络安全威胁防护所需的最小设置集合进行调整。该配置使用快速启动向导执行。当向导运行时，您可以对应用程序做以下更改：

- 添加可自动分发至管理组内的设备的密钥文件或激活码。
- 配置与卡巴斯基安全网络 (KSN) 的交互。如果您允许使用 KSN，则向导会启用可保证 KSN 与设备连接的 KSN 代理服务器服务。
- 为管理服务器和受管理应用程序的操作事件通知设置邮件传送配置（成功的通知传送需要消息服务在管理服务器和所有接收端设备上运行）。
- 为工作站和服务器创建保护策略，以及为受管理设备的顶级层级创建恶意软件扫描任务、更新下载任务和数据备份任务。

  > 快速启动向导仅为其“**受管理设备**”文件夹不包含任何策略的应用程序创建策略。如果已经为受管理设备的顶级层级创建具有相同名称的任务，则快速启动向导不会创建同名任务。

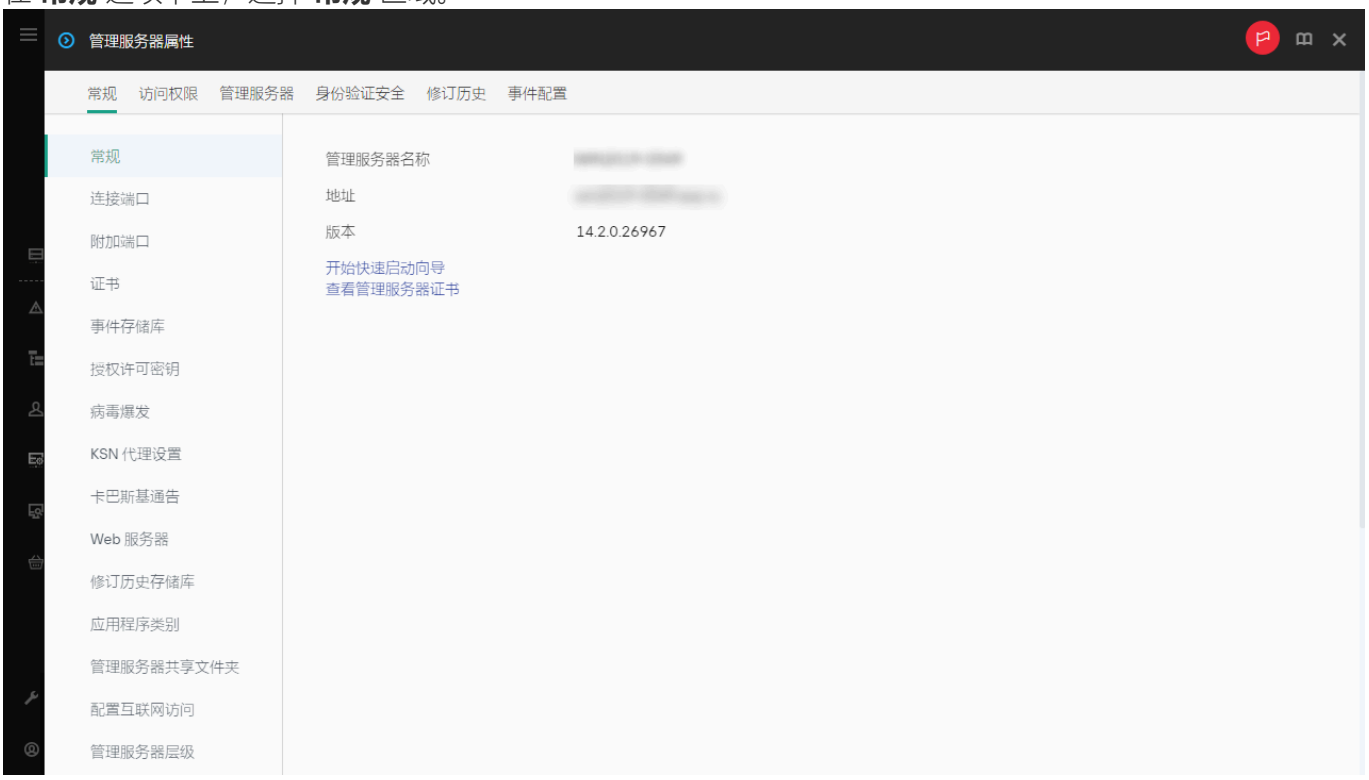
在安装管理服务器后，在第一次连接时，应用程序自动提示您运行快速启动向导。您还可以在任意时刻手动启动快速启动向导。

要手动启动快速启动向导：

1. 在主菜单，单击管理服务器名称旁边的“设置”图标 ( )。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**常规**”区域。



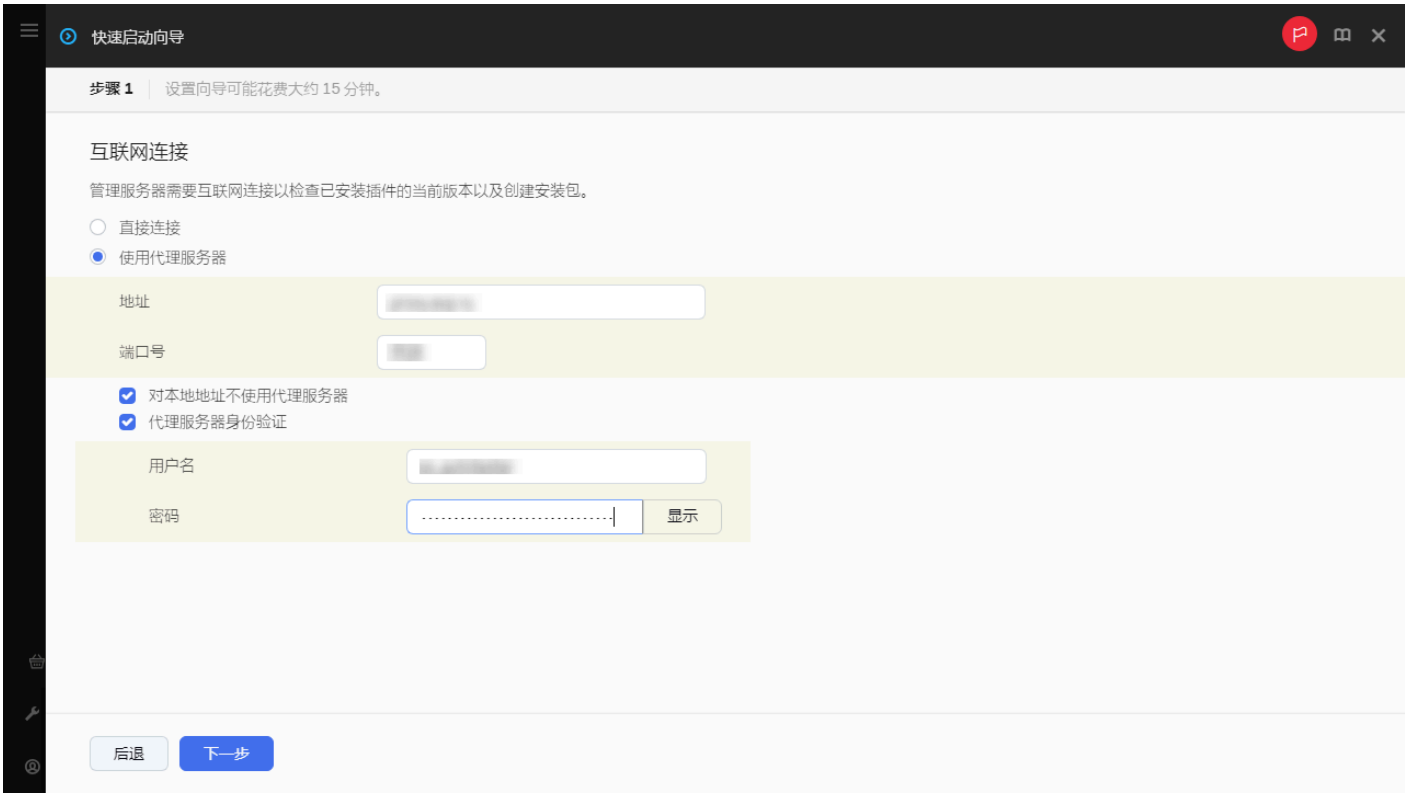
管理服务器属性窗口

3. 单击**开始快速启动向导**。

向导提示您执行管理服务器初始化配置。遵照向导的说明操作。使用“**下一步**”按钮继续向导操作。

步骤 1：指定互联网连接设置

指定管理服务器的互联网连接设置。您必须配置互联网连接才能使用卡巴斯基安全网络和为 Kaspersky Security Center 及受管理的卡巴斯基应用程序下载反病毒数据库更新。



互联网连接设置

如果您要在连接到互联网时使用代理服务器，请启用“**使用代理服务器**”选项。如果启用此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

- **地址**

  Kaspersky Security Center 用于连接到互联网的代理服务器地址。

- **端口号**

  将建立 Kaspersky Security Center 代理服务器连接的端口号。

- **对本地地址不使用代理服务器**

  将不会使用代理服务器连接本地网络的设备。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  如果选中“**使用代理服务器**”复选框，则该输入字段可用。

- **用户名**

  用于与代理服务器建立连接的用户账户（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

- **密码**

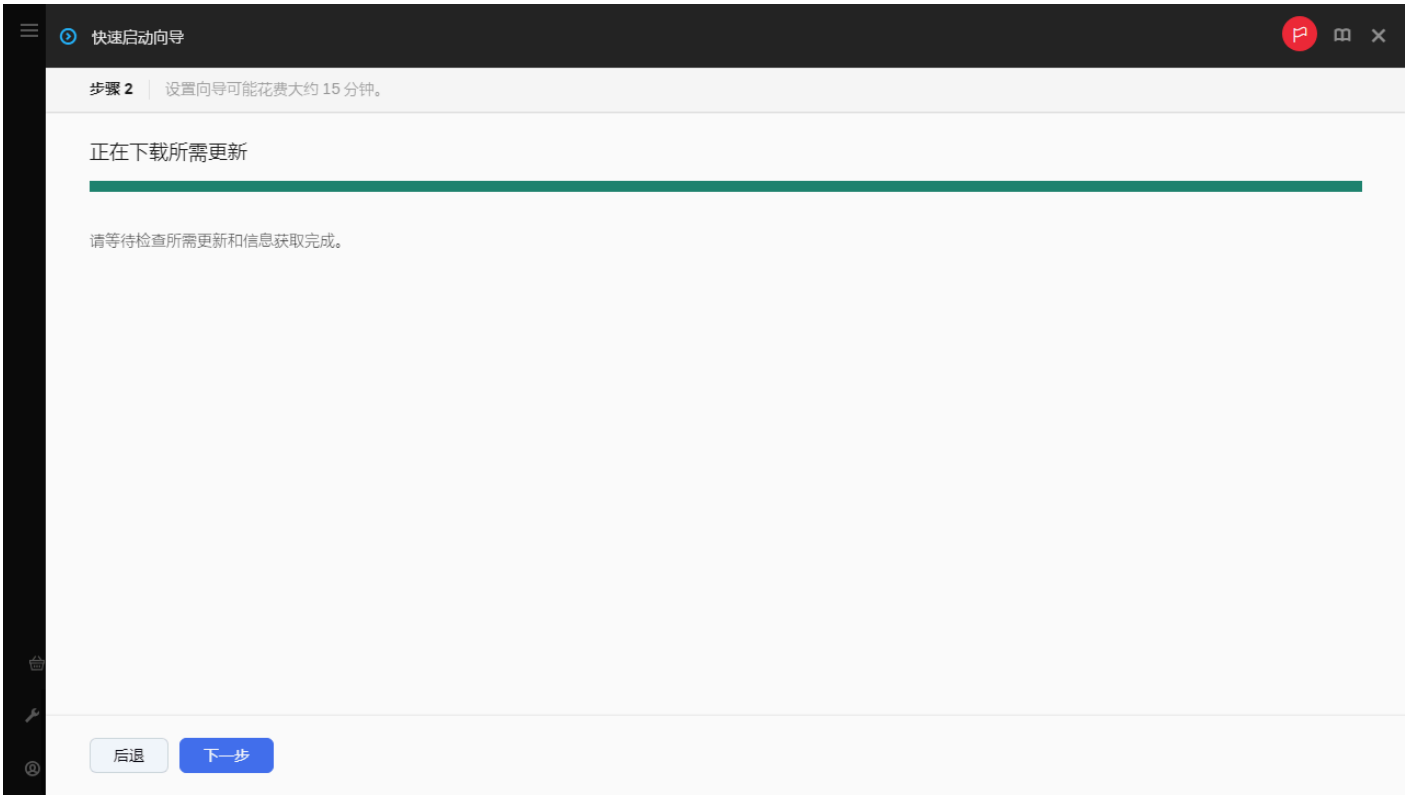
  建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

  要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

您可以稍后从快速启动向导单独配置互联网访问。

步骤 2：下载所需更新

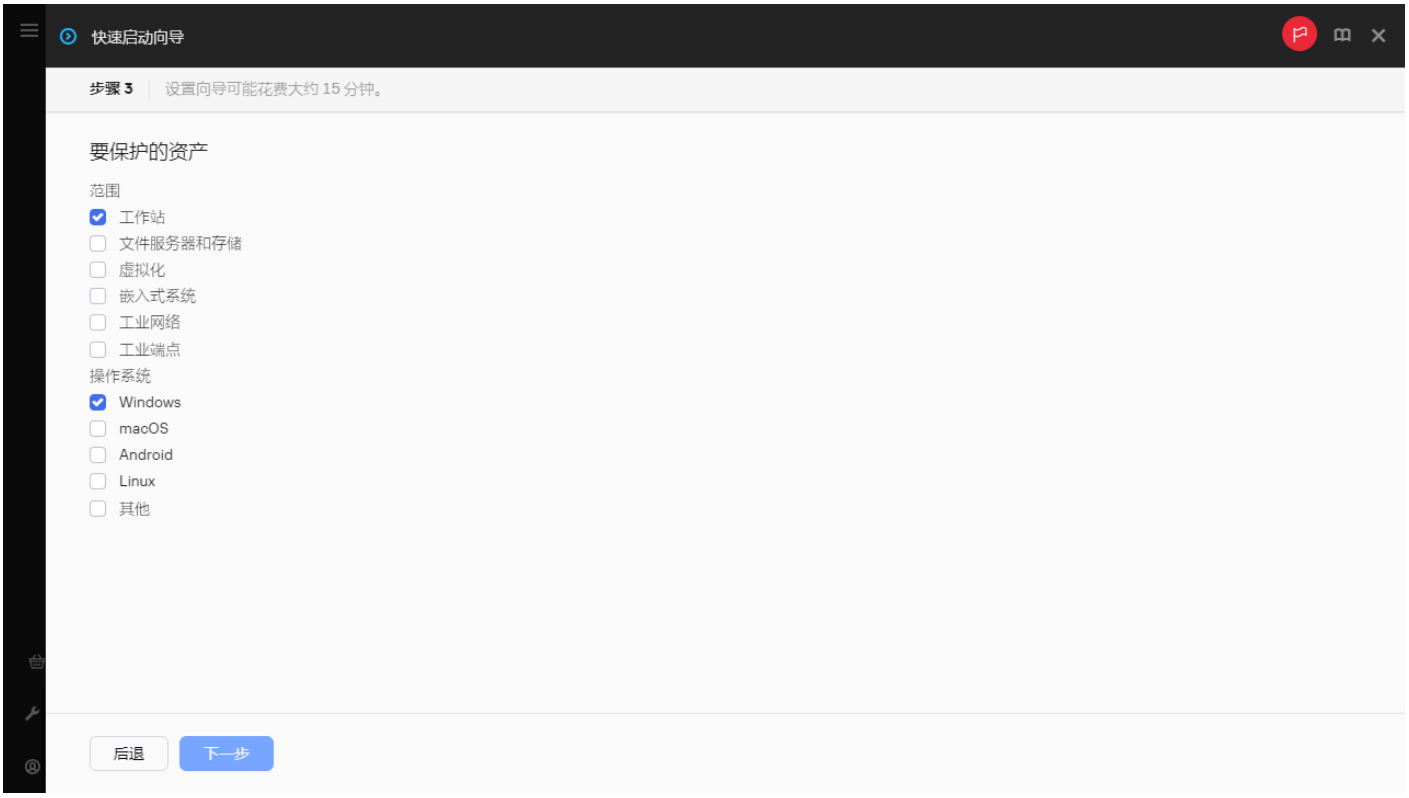
所需更新将从 Kaspersky 服务器自动下载。



正在下载所需更新

步骤 3：选择要保护的资产

选择网络中正在使用的保护区域和操作系统。选择这些选项时，将为 Kaspersky 服务器上的应用程序管理插件和分发包指定过滤器，您可以下载这些插件和分发包以将其安装在网络中的客户端设备上。



选择要保护的资产

选择选项：

- **范围**

  您可以选择以下保护区域：

  - **工作站**。如果要保护网络中的工作站，请选择此选项。默认情况下选定“工作站”选项。
  - **文件服务器和存储**。如果要保护网络中的文件服务器，请选择此选项。
  - **移动设备**。如果要保护公司或公司员工拥有的移动设备，请选择此选项。如果选择此选项，但未提供具有移动设备管理功能的授权许可，则会显示一条消息，通知您需要提供具有移动设备管理功能的授权许可。如果您不提供授权许可，则不能使用移动设备功能。
  - **虚拟化**。如果要保护网络中的虚拟机，请选择此选项。
  - Kaspersky **反垃圾邮件**。如果要保护组织中的邮件服务器免受垃圾邮件、欺诈和恶意软件的侵扰，请选择此选项。
  - **嵌入式系统**。如果您想保护基于 Windows 的嵌入式系统，例如自动取款机 (ATM)，请选择此选项。

- **工业网络**。如果您想要监控工业网络中的安全数据以及来自受卡巴斯基应用程序保护的网络端点的安全数据，请选择此选项。
- **工业端点**。如果要保护工业网络中的单个节点，请选择此选项。

- **操作系统**

  您可以选择以下平台：
  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - 其他

  有关支持的操作系统的更多信息，请参阅“Kaspersky Security Center Web Console 的硬件和软件要求”。

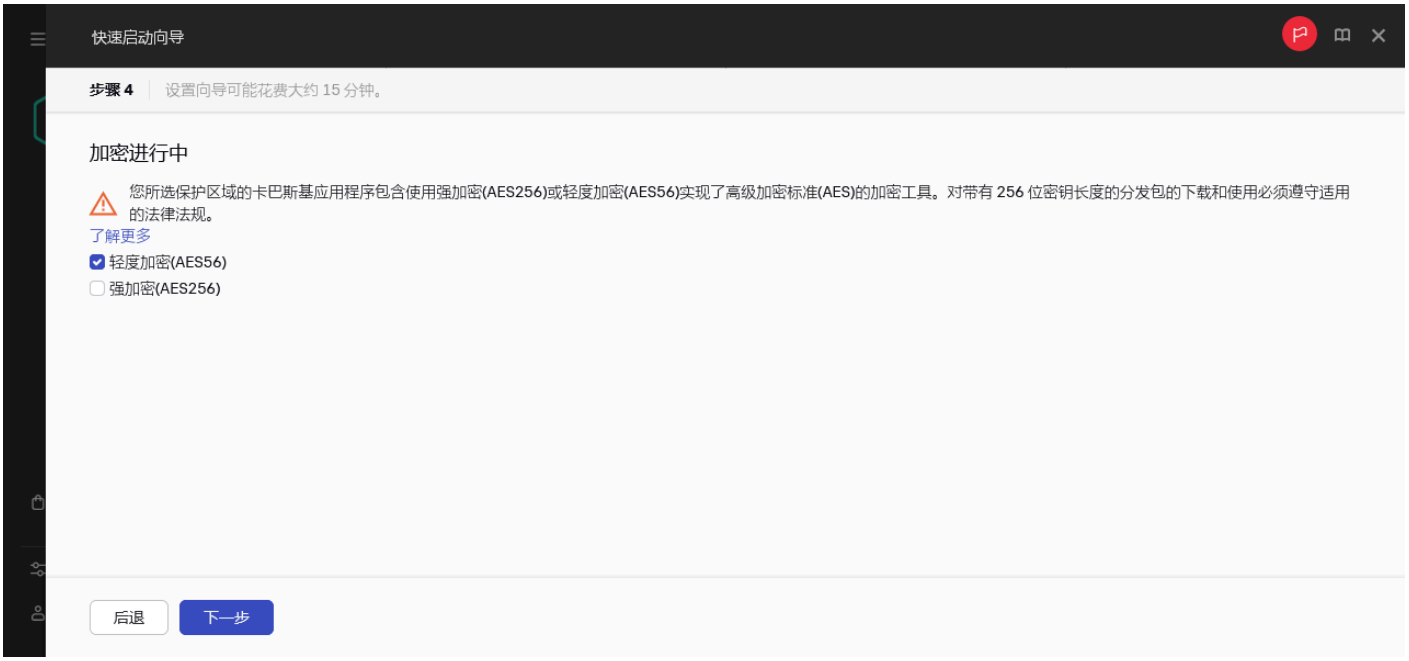
您可以稍后从可用包列表中选择卡巴斯基应用程序包，是从快速启动向导单独配置。为了简化对所需包的搜索，您可以通过各种标准筛选可用包列表。

步骤 4：选择解决方案中的加密

只有选择“工作站”作为保护范围并选择“**工作站**”作为平台时，才显示“**加密进行中**”窗口。

Kaspersky Endpoint Security for Windows 包括用于存储在 Windows 客户端设备上的信息的加密工具。这些加密工具采用以 256 位或 56 位密钥长度实现的高级加密标准 (AES)。

必须按照适用的法律法规下载和使用密钥长度为 256 位的分发包。要下载可满足组织需求的有效 Kaspersky Endpoint Security for Windows 分发包，请参考组织的客户端设备所在国家/地区的法律。



选择解决方案中的加密

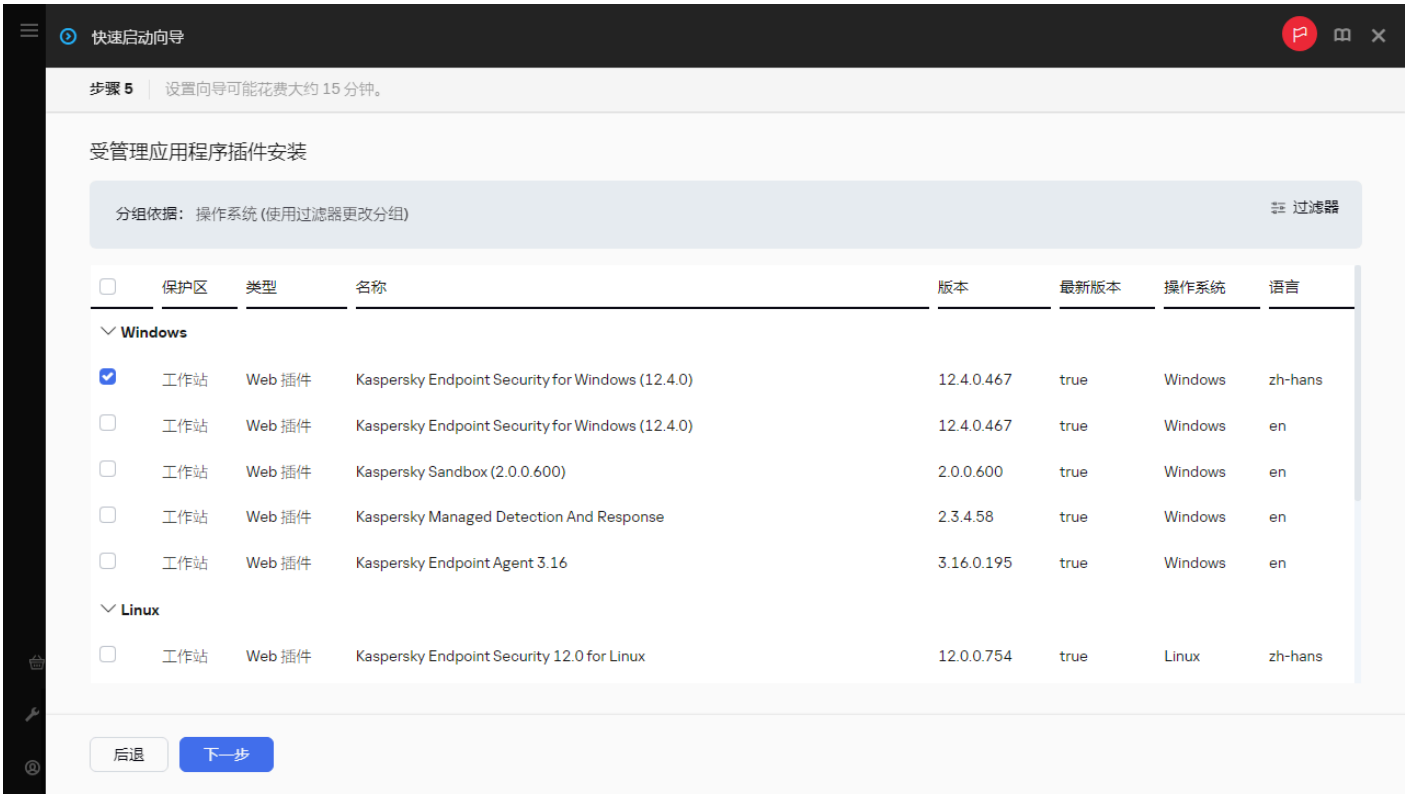
在“**加密进行中**”窗口，选择以下加密类型之一：

- 轻度加密。此加密类型使用 56 位密钥长度。
- 强加密。此加密类型使用 256 位密钥长度。

您可以稍后使用所需的加密类型为 Kaspersky Endpoint Security for Windows 选择分发包，单独从快速启动向导执行。

步骤 5：配置受管理应用程序的插件安装

选择要安装的受管理应用程序插件。将显示位于 Kaspersky 服务器上的插件列表。该列表根据在向导的上一步中选择的选项进行筛选。默认情况下，完整列表包括所有语言的插件。要仅显示特定语言的插件，请使用过滤器。



受管理应用程序插件安装

插件列表包括以下多列：

- **保护范围**

  选定的要保护的区域会显示在此列中。

- **类型**

  插件类型会显示在此列中。

- **名称**

  将根据您在上一步中选择的保护区域和平台来选择插件。

- **版本**

  该列表包括 Kaspersky 服务器上所有版本的插件。默认情况下，将选择最新版本的插件。

- **最新版本**

  该列表示插件版本是否为最新。如果显示**true**值，则对应的插件是最新版本。如果显示**false**值，则对应的插件版本更高。

- **操作系统**

  此列会显示插件操作系统。

- **语言**

  默认情况下，插件的本地化语言由您在安装 Kaspersky Security Center 时选择的语言来定义。您可以在“**显示管理控制台本地化语言或**”下拉列表中指定其他语言。

选择插件后，单击“**下一步**”开始安装。

您可以手动为卡巴斯基应用程序安装管理插件，单独从快速启动向导执行。

快速启动向导会自动安装选定插件。要安装某些插件，您必须接受 EULA 条款。阅读显示的 EULA 文本，选中“**我同意使用卡巴斯基安全网络**”复选框，然后单击“**安装**”按钮。如果您不接受 EULA 条款，则不会安装该插件。

安装所有选定插件后，快速启动向导会自动带您继续下一步。

步骤 6.安装所选插件

快速启动向导会自动安装您在上一步选择的插件。要安装某些插件，您必须接受 EULA 条款。阅读显示的 EULA 文本，选中“**我同意使用卡巴斯基安全网络**”复选框，然后单击“**安装**”按钮。如果您不接受 EULA 条款，则不会安装该插件。

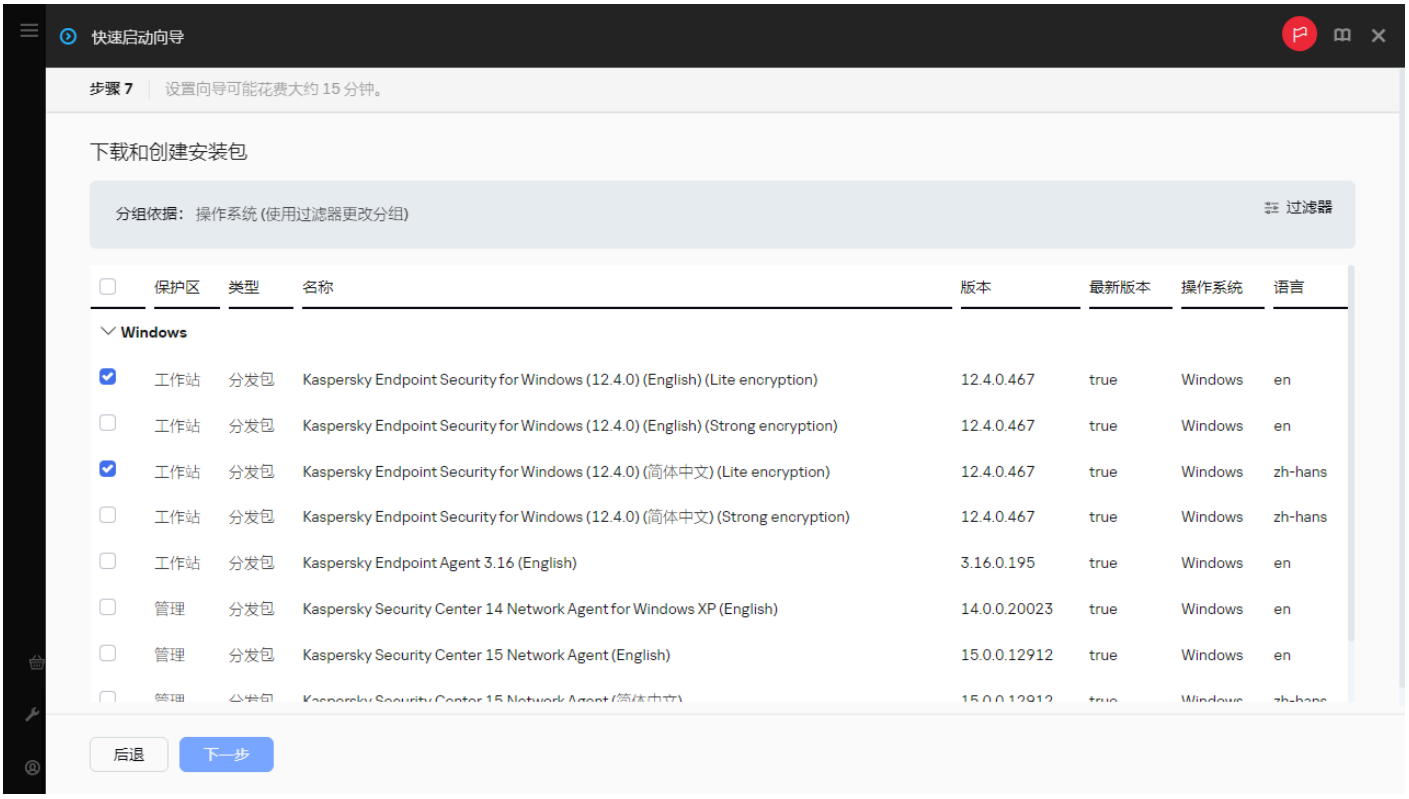
安装所有选定插件后，快速启动向导会自动带您继续下一步。

步骤 7：下载分发包并创建安装包

选择要下载的分发包。

受管理应用程序的分发可能需要安装 Kaspersky Security Center 的特定最低版本。

选择 Kaspersky Endpoint Security for Windows 的加密类型之后，将显示两种加密类型的分发包列表。列表中选中了具有所选加密类型的分发包。您可以选择任意加密类型的分发包。分发包语言与 Kaspersky Security Center 语言相对应。如果不存在与 Kaspersky Security Center 语言对应的 Kaspersky Endpoint Security for Windows 分发包，则选择英语分发包。



下载分发包并创建安装包

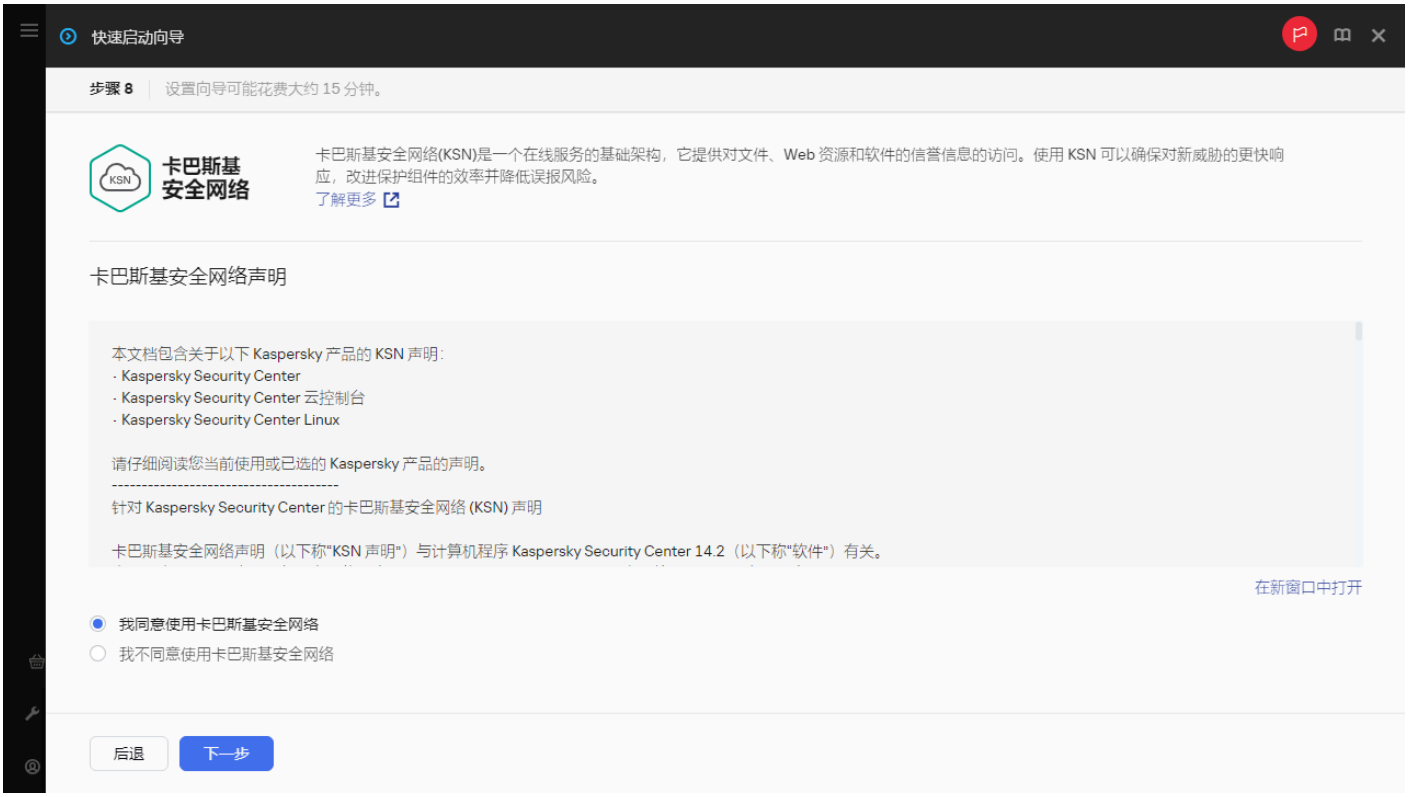
要完成某些分发包的下载，您必须接受 EULA。当您单击“**接受**”按钮时，将显示 EULA 文本。要继续进行向导的下一步，您必须接受 EULA 的条款和条件以及 Kaspersky 隐私策略的条款和条件。如果您不接受条款和条件，则将取消分发包的下载。

在您接受 EULA 的条款和条件以及 Kaspersky 隐私策略的条款和条件之后，将继续下载分发包。稍后，您可以使用安装包在客户端设备上部署 Kaspersky 应用程序。

您可以稍后下载分发包并创建安装包，单独从快速启动向导执行。

步骤 8：配置卡巴斯基安全网络

指定设置以转发 Kaspersky Security Center 操作信息到卡巴斯基安全网络知识库。



配置卡巴斯基安全网络

您可以选择以下选项之一：

- **我同意使用卡巴斯基安全网络**

  安装在客户端设备上的 Kaspersky Security Center 和受管理应用程序将自动将其操作详情传输到卡巴斯基安全网络。参与卡巴斯基安全网络确保了包含病毒和其他威胁的数据库的快速更新，该数据库确保了对紧急安全威胁的快速响应。

- **我不同意使用卡巴斯基安全网络**

  Kaspersky Security Center 和受管理应用程序将不向卡巴斯基安全网络提供任何信息。

  如果选择此选项，则将禁用卡巴斯基安全网络。

您可以稍后设置对卡巴斯基安全网络 (KSN) 的访问，单独从快速启动向导执行。

步骤 9：选择应用程序激活方法

选择以下 Kaspersky Security Center 激活选项之一：

- **通过输入您的激活码**

  *激活码*是一串由20个字符数字组成的唯一序列。您可以输入激活码来添加一个密钥来激活 Kaspersky Security Center。购买 Kaspersky Security Center 后，您将通过您指定的电子邮件地址收到激活码。

  若要使用激活码激活应用程序，您需要互联网来建立与 Kaspersky 激活服务器的连接。

  如果选择了此激活选项，则可以启用“**自动分发授权许可密钥到受管理设备**”选项。

  如果启用此选项，授权许可密钥将自动部署到受管理设备。

  如果禁用此选项，则可以稍后在管理控制台树的“**Kaspersky 授权许可**”节点中将授权许可密钥部署到受管理设备。

- **通过指定密钥文件**

  *密钥文件*是 Kaspersky 提供的 .key 扩展名的文件。密钥文件被用来激活应用程序。

  密钥文件的获取方法请参见以下章节：关于密钥文件。

  若使用密钥文件激活程序，您无需连接至 Kaspersky 激活服务器。

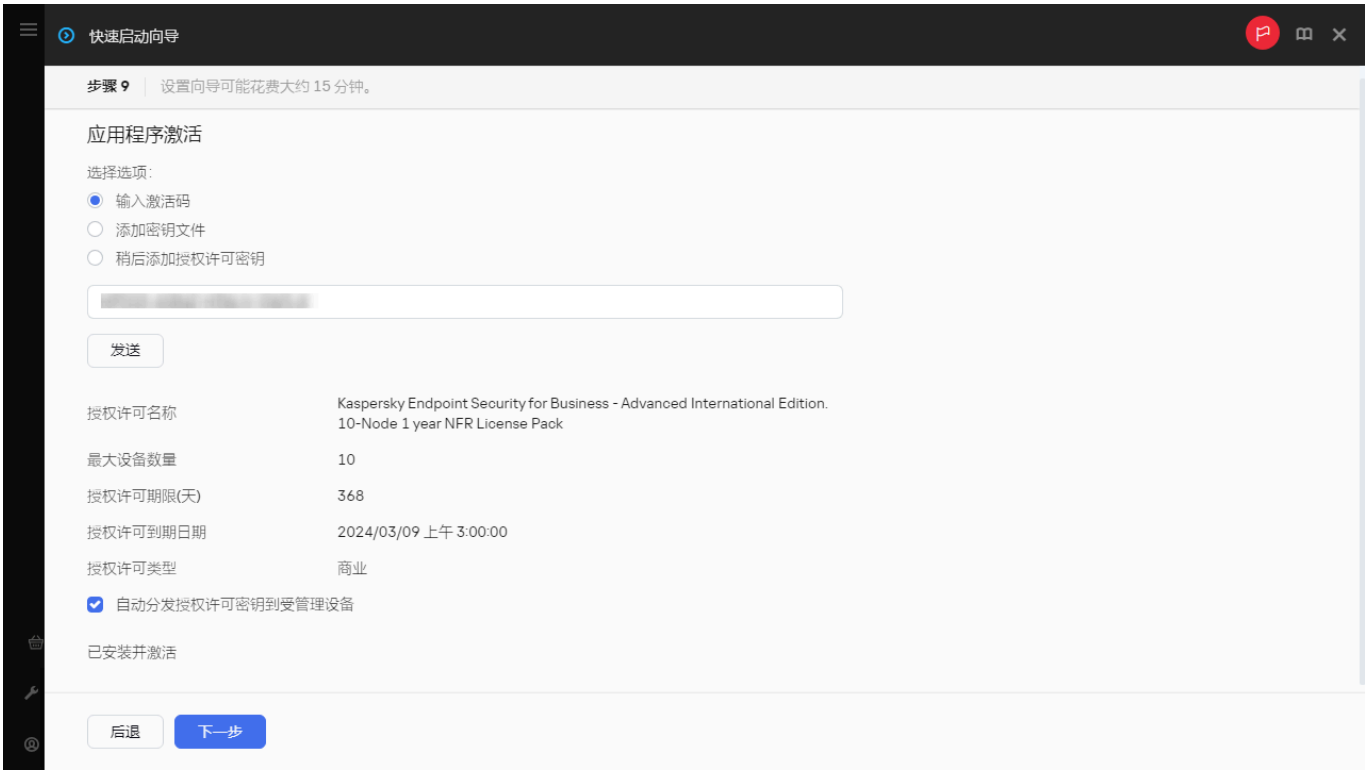
  如果选择了此激活选项，则可以启用“**自动分发授权许可密钥到受管理设备**”选项。

  如果启用此选项，授权许可密钥将自动部署到受管理设备。

  如果禁用此选项，则可以稍后在管理控制台树的“**Kaspersky 授权许可**”节点中将授权许可密钥部署到受管理设备。

- **通过高推迟应用程序激活**

  应用程序将使用基本功能操作，没有移动设备管理也没有漏洞和补丁管理。



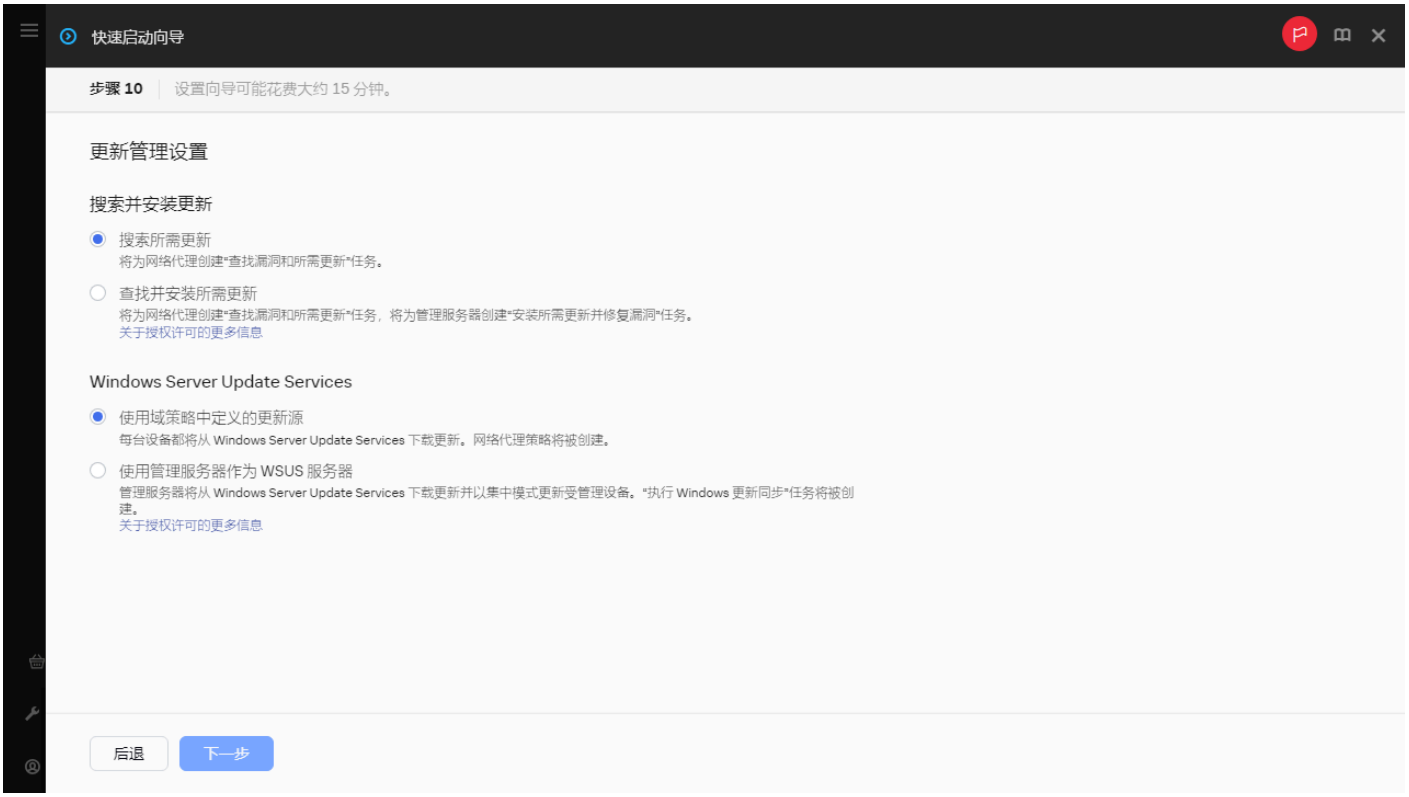
选择应用程序激活方法

如果您选择延迟应用程序激活，您可以在稍后随时选择“**操作**”→“**授权许可**”来添加授权许可密钥。

当使用从付费 AMI 部署的 Kaspersky Security Center 时，或者对于基于使用的按月付费 SKU，您无法指定密钥文件或输入码。

步骤 10：指定第三方更新管理设置

如果您没有“漏洞和补丁管理”授权许可，并且“*查找漏洞和所需更新*”任务已经存在，则不显示此步骤。



第三方更新管理设置

对于第三方软件更新，选择以下选项之一：

- **搜索所需更新**

  如果您没有*查找漏洞和所需更新*任务，系统会自动创建该任务。
  默认情况下已选中该选项。

- **查找并安装所需更新**

  如果没有“*查找漏洞和所需更新*”和“*安装所需更新并修复漏洞*”任务，它们会自动创建。

  此选项仅在“漏洞和补丁管理”授权许可下可用。

对于 Windows Update 更新，选择以下选项之一：

- **使用域策略中定义的更新源**

  客户端设备将根据域策略设置下载 Windows Update 更新。如果没有网络代理策略，它会自动创建。

- **使用管理服务器作为 WSUS 服务器**

  客户端设备将从管理服务器下载 Windows Update 更新。如果没有“*执行 Windows 更新同步*”任务和网络代理策略，它们会自动创建。

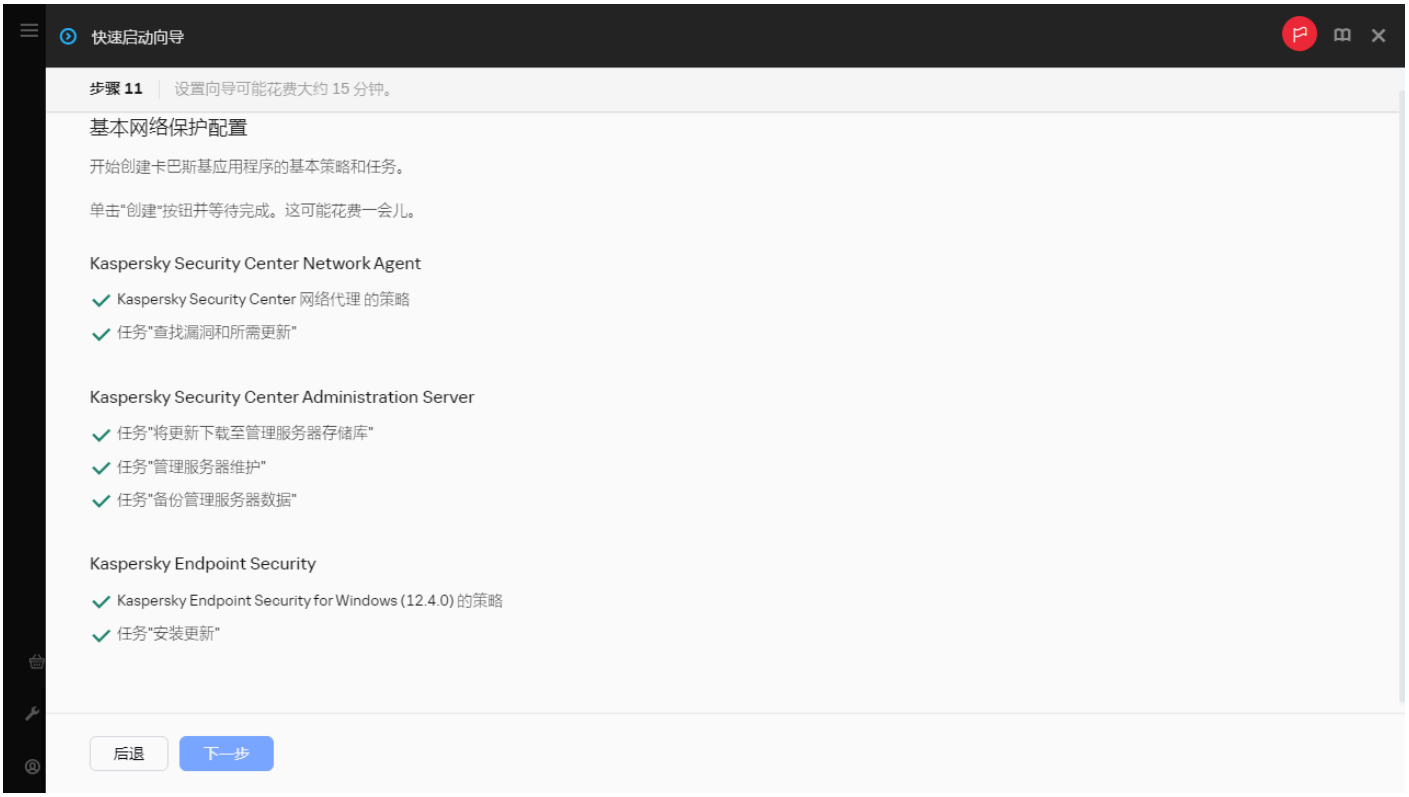
  此选项仅在“漏洞和补丁管理”授权许可下可用。

您可以创造*查找漏洞和所需更新*和*安装所需更新并修复漏洞*任务，单独从快速启动向导执行。要将管理服务器用作 WSUS 服务器，请创建“*执行 Windows Update 同步*”任务，然后选中网络代理策略中的“**使用管理服务器作为 WSUS 服务器**”选项。

步骤 11：创建基本的网络保护配置

您可以检查创建的策略和任务列表。

等待策略和任务完成创建，然后转到向导的下一步。

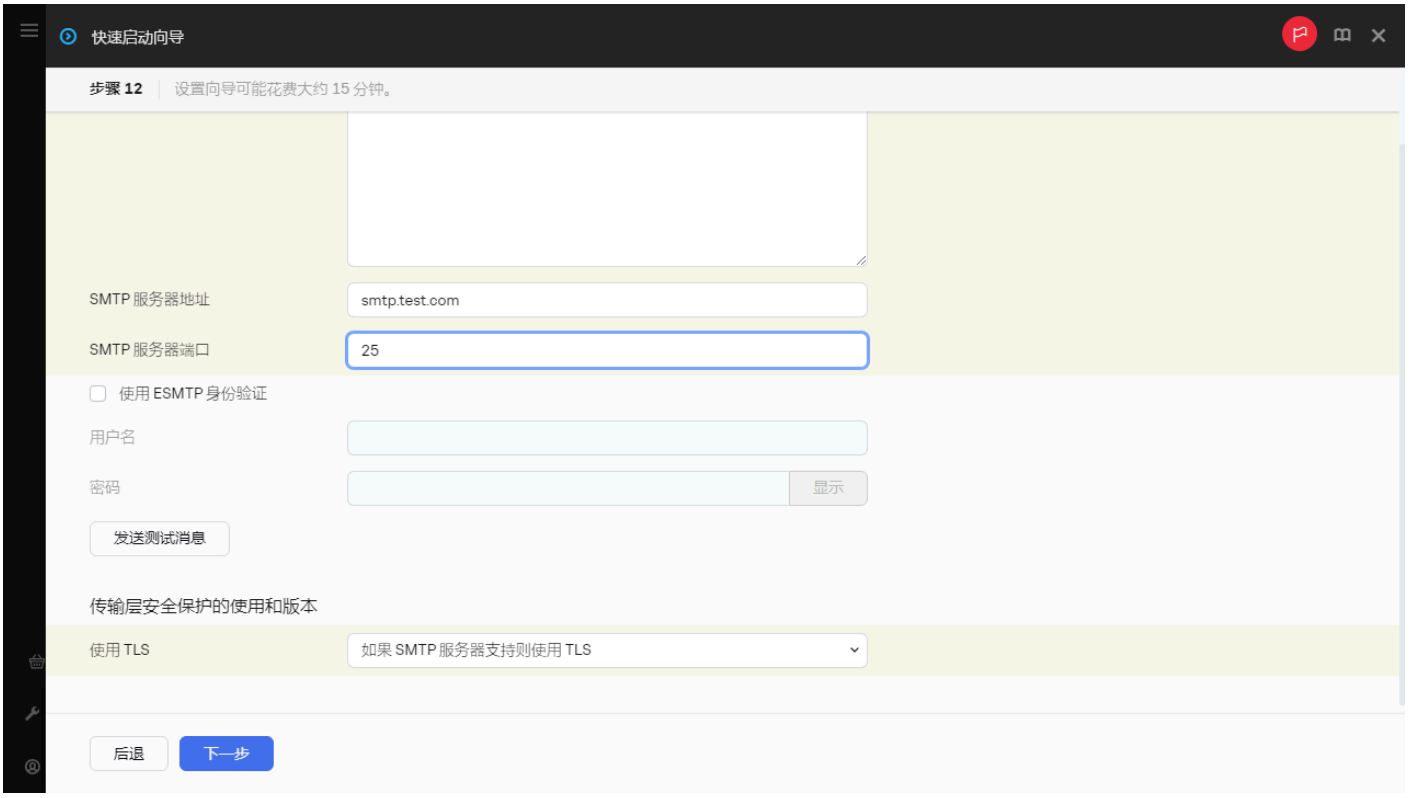


创建基本的网络保护配置

您还可以稍后单独从快速启动向导创建所需的任务和策略。

步骤 12：配置邮件通知

配置如何传递有关在 Kaspersky 应用程序在客户端设备上运行期间记录的事件的通知。这些设置将被用作应用程序策略的默认设置。



配置邮件通知

要配置发生在 Kaspersky 应用程序上的事件的通知传送，使用以下设置：

- **收件人(电子邮件地址)**

  应用程序将给其发送通知的用户的邮件地址。您可以输入一个或更多地址；如果您输入多个地址，使用分号分隔。

- **SMTP 服务器地址**

  您组织邮件服务器的地址。

  如果您输入多个地址，使用分号分隔。您可以使用下列值：

  - IPv4 或 IPv6 地址
  - 设备的 Windows 网络名称（NetBIOS 名称）
  - SMTP 服务器的 DNS 名称

- **SMTP 服务器端口**

  SMTP 服务器的通信端口号。如果您使用多个 SMTP 服务器，则通过指定的通信端口与它们建立连接。默认端口号是 25。

- **使用 ESMTP 身份验证**

  启用 ESMTP 身份验证支持。当选择了该复选框时，您可以在“**用户名**”和“**密码**”字段指定 ESMTP 身份验证设置。默认情况下已清除该选框。

- **使用 TLS**

  您可以指定 SMTP 服务器连接的 TLS 设置：

  - **不使用 TLS**

    如果要禁用电子邮件加密，则可以选择此选项。

  - **如果 SMTP 服务器支持则使用 TLS**

    如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

  - **始终使用 TLS，检查服务器证书的有效性**

    如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

    建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

    如果您选择“**始终使用 TLS，检查服务器证书的有效性**”值，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

  您可以单击“**指定证书**”链接来指定用于 TLS 连接的证书：

  - 浏览 SMTP 服务器证书文件：

    您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

  - 浏览客户端证书文件：

    您可以使用从任何来源（例如，从任何受信任证书颁发机构）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

    - X-509 证书：

      您必须指定一个证书文件和一个私钥文件。这两个文件不相互依赖，文件的加载顺序也不重要。加载这两个文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

- pkcs12容器：

  您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

您可以通过单击“**发送测试消息**”按钮测试新邮件通知设置。

您可以稍后独立于快速启动向导配置事件通知。

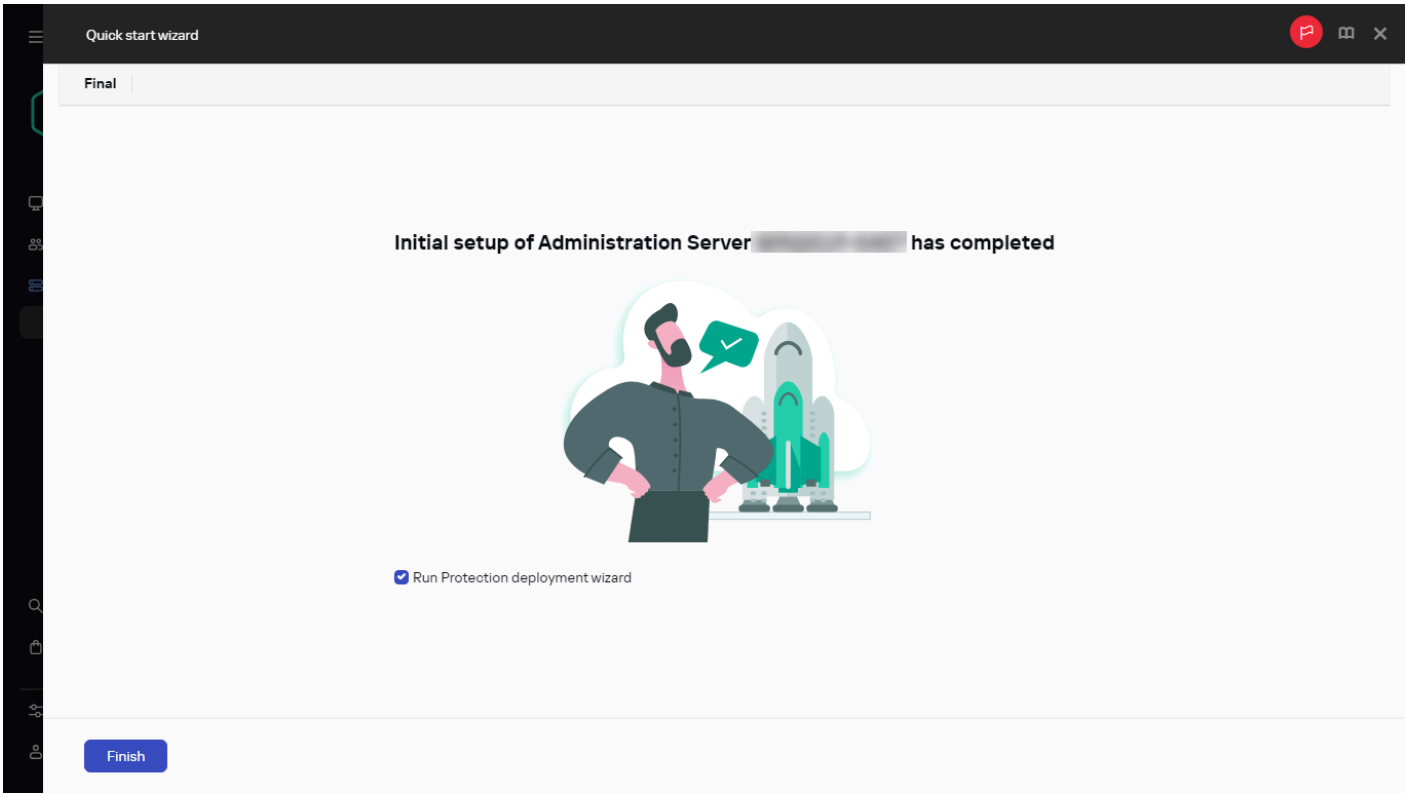
步骤 13：执行网络轮询

管理服务器执行初始轮询。轮询中，进度条被显示。当轮询完成时，“**查看检测到的设备**”链接变得可用。您可以点击该链接查看被管理服务器检测到的网络设备。要返回快速启动向导，点击**返回**键。

您可以稍后从快速启动向导单独轮询您的网络。使用 Kaspersky Security Center Web Console 配置域控制器、Windows 域、IP 范围和 IPv6 网络轮询。

步骤 14：关闭快速启动向导

在快速启动向导完成页面上，如果您希望在网络中的设备上启动反病毒应用程序和/或网络代理的自动安装，请选中“**运行保护和部署向导**”复选框。



快速启动向导的最后一步

要关闭向导，请单击“**完成**”按钮。

连接漫游设备

本节介绍如何将漫游设备（即，位于主网络外部的受管理设备）连接到管理服务器。

方案：通过连接网关连接漫游设备

此方案描述了如何将位于主网络外部的受管理设备连接到管理服务器。

先决条件

该方案具有以下先决条件：

- 在组织的网络中已规划一个隔离区域 (DMZ)。
- 公司网络上已部署 Kaspersky Security Center 管理服务器。

阶段

此方案的实施分为几个阶段：

1. **选择 DMZ 中的客户端设备**

   此设备将用作连接网关。您选择的设备必须符合连接网关的要求。

2. **以连接网关角色安装网络代理**

   我们建议您使用本地安装在所选设备上安装网络代理。

   默认情况下，安装文件位于：\\<服务器名称>\KLSHARE\PkgInst\NetAgent_<版本号>

   在网络代理安装向导的“**连接网关**”窗口中，选择“**使用网络代理作为 DMZ 连接网关**”。此模式同时激活连接网关角色，并通知网络代理等待来自管理服务器的连接，而不是建立与管理服务器的连接。

   或者，您可以在 Linux 设备上安装网络代理，并将网络代理配置为连接网关，但是要注意在 Linux 设备上运行的网络代理的限制列表。

3. **在防火墙中允许与连接网关的连接**

   为确保管理服务器可以实际连接到 DMZ 中的连接网关，请在管理服务器与连接网关之间的所有防火墙中允许与 TCP 端口 13000 的连接。

   如果连接网关在互联网上没有真实 IP 地址，而是位于网络地址转换 (NAT) 后面，请配置规则以通过 NAT 转发连接。

4. **针对外部设备创建管理组**

   在“**受管理设备**”组下创建一个新组。该新组将包含外部受管理设备。

5. **将连接网关连接到管理服务器**

   您配置的连接网关正在等待来自管理服务器的连接。但是，管理服务器未在受管理设备中列出具有连接网关的设备。这是因为连接网关尚未尝试建立与管理服务器的连接。因此，您需要一个特殊程序来确保管理服务器发起与连接网关的连接。

执行以下操作：

1. 添加连接网关作为分发点。
2. 将连接网关从“**未分配的设备**”组移动到您针对外部设备创建的组。

连接网关连接并配置完毕。

6. **将外部台式设备连接到管理服务器**

   通常，外部台式设备不在周界内移动。因此，在安装网络代理时，需要将这些计算机配置为通过网关连接到管理服务器。

7. **设置外部台式设备的更新**

   如果将安全应用程序更新配置为从管理服务器下载，则外部设备将通过连接网关下载更新。这有两个缺点：

   - 这是不必要的流量，占用了公司的互联网通信通道的带宽。
   - 这不一定是获取更新的最快方法。对于外部设备来说，从 Kaspersky 更新服务器接收更新很可能更实惠、更快捷。

   执行以下操作：

   1. 将所有外部设备移至您先前创建的单独管理组。
   2. 从更新任务中排除具有外部设备的组。
   3. 针对具有外部设备的组创建单独的更新任务。

8. **将移动中的笔记本电脑连接到管理服务器**

   移动中的笔记本电脑有时在网络内部，有时在网络外部。为实现有效管理，您需要它们根据所在位置以不同方式连接到管理服务器。为了有效利用流量，它们还需要根据所在位置从不同来源接收更新。

   您需要配置针对漫游用户的规则：连接配置文件和网络位置描述。每个规则都定义了移动中的笔记本电脑必须根据所在位置连接到的管理服务器实例，以及必须从中接收更新的管理服务器实例。

方案：通过 DMZ 中的从属管理服务器连接漫游设备

如果要将位于主网络外部的受管理设备连接到管理服务器，可以使用位于隔离区 (DMZ) 中的从属管理服务器来实现。

先决条件

在您开始之前，确保您已做了如下：

- 在组织的网络中已规划一个 DMZ。
- 组织的内部网络上已部署 Kaspersky Security Center 管理服务器。

阶段

此方案的实施分为几个阶段：

1. **选择 DMZ 中的客户端设备**

   在 DMZ 中，选择将用作从属管理服务器的客户端设备。

2. **安装 Kaspersky Security Center 管理服务器**

   在此客户端设备上安装 Kaspersky Security Center 管理服务器。

3. **创建管理服务器层级**

   如果将从属管理服务器放置在 DMZ 中，则从属管理服务器必须接收来自主管理服务器的连接。为此，添加新管理服务器作为从属管理服务器，以便主管理服务器通过端口 13000 连接到从属管理服务器。当组合两个管理服务器到一个层级，确保端口 13299 在两个管理服务器上都可以访问。Kaspersky Security Center Web Console 通过端口 13299 连接到管理服务器。

4. **将不在办公室的受管理设备连接到从属管理服务器**

   您可以将不在办公室的设备连接到 DMZ 中的管理服务器，其连接方式与在管理服务器和位于主网络中的受管理设备之间建立连接的方式相同。不在办公室的受管理设备通过端口 13000发起连接。

关于连接漫游设备

一些受管理设备始终在主网络外部（例如，公司区域分支机构中的设备；自助服务终端、ATM 和安装在各个销售点的终端；员工家庭办公室中的设备）。一些设备不时在外围移动（例如，访问区域分支机构或客户办公室的用户的笔记本电脑）。

您仍然需要监视和管理对漫游设备的保护 - 接收这些设备的保护状态的实际信息，并确保设备上面的安全应用程序为最新。这是非常必要的，例如，如果某台设备在远离主网络时被入侵，那么只要它连接到主网络，就可能成为传播威胁的平台。要将漫游设备连接到管理服务器，可以使用两种方法：

- 隔离区域 (DMZ) 中的连接网关

  查看数据流量方案：LAN 上的管理服务器、互联网上的受管理设备、正在使用的连接网关

- DMZ 中的管理服务器

  查看数据流量方案：DMZ 中的管理服务器、互联网上的受管理设备

DMZ 中的连接网关

将漫游设备连接到管理服务器的推荐方法是在组织的网络中组织一个 DMZ，并在该 DMZ 中安装连接网关。外部设备将连接到连接网关，网络内部的管理服务器将通过连接网关发起与设备的连接。

与其他方法相比，此方法更安全：

- 您不需要开放从网络外部访问管理服务器的权限。
- 遭到入侵的连接网关不会对网络设备的安全性构成高风险。连接网关本身实际不进行任何管理，也不建立任何连接。

而且，连接网关不需要很多硬件资源。

但是，此方法的配置过程更复杂：

- 要将设备用作 DMZ 中的连接网关，您需要安装网络代理并以特定方式将其连接到管理服务器。
- 不能在所有情况下都使用同一个地址连接到管理服务器。在外围，不仅需要使用不同的地址（连接网关地址），还需要不同的连接模式：通过连接网关。
- 还需要为不同位置的笔记本电脑定义不同的连接设置。

要将连接网关添加到先前配置的网络：

1. 以连接网关模式安装网络代理。
2. 在要连接到新添加的连接网关的设备上重新安装网络代理。

DMZ 中的管理服务器

另一种方法是在 DMZ 中安装一个管理服务器。

此配置不如其他方法安全。在这种情况下，要管理外部笔记本电脑，管理服务器必须接受来自互联网上任何地址的连接。它仍然将管理内部网络中的所有设备，但是从 DMZ 进行管理。因此，被入侵的服务器可能造成巨大损失，尽管发生此类事件的可能性很低。

如果 DMZ 中的管理服务器不管理内部网络中的设备，则风险将大大降低。例如，服务提供商可以使用这种配置来管理客户的设备。

在以下情况下，您可能要使用此方法：

- 如果您熟悉安装和配置管理服务器，并且不想执行其他程序来安装和配置连接网关。
- 如果您需要管理更多设备。管理服务器的最大容量为 100,000 个设备，而连接网关最多可支持 10,000 个设备。

此解决方案也可能存在困难：

- 管理服务器需要更多硬件资源，而且另外需要一个数据库。
- 设备的信息将存储在两个不相关的数据库中（网络内的管理服务器数据库和 DMZ 中的另一个数据库），这会使监控复杂化。
- 要管理所有设备，需要将管理服务器连接到一个层级中，这不仅使监控复杂化，也使管理复杂化。从属管理服务器实例给管理组的可能结构加上了限制。您必须决定如何以及将哪些任务和策略分发到从属管理服务器实例。
- 配置外部设备从外部使用 DMZ 中的管理服务器以及从内部使用主管理服务器，并不比将它们配置为通过网关使用有条件连接简单。
- 高安全风险。遭到入侵的管理服务器实例使得入侵其受管理的笔记本电脑更容易。如果发生这种情况，黑客只需要等待其中一台笔记本电脑返回公司网络，即可继续对局域网进行攻击。

将外部台式设备连接到管理服务器

始终在主网络外部的台式设备（例如，公司区域分支机构中的设备；自助服务终端、ATM 和安装在各个销售点的终端；员工家庭办公室中的设备）无法直接连接到管理服务器。它们必须通过安装在隔离区域 (DMZ) 中的连接网关连接到管理服务器。在这些设备上安装网络代理时，将进行此配置。

要将外部台式设备连接到管理服务器：

1. 创建一个新的网络代理安装包。
2. 打开创建的安装包的属性并转到“**设置** → **高级**”，然后选择“**通过使用连接网关连接到管理服务器**”选项。

   “**通过使用连接网关连接到管理服务器**”设置与“**使用网络代理作为 DMZ 连接网关**”设置不兼容。您不能同时启用这两个设置。

3. 在“**连接网关地址**”字段中，指定连接网关的公共地址。

   如果连接网关位于网络地址转换 (NAT) 后面并且没有自己的公用地址，请配置 NAT 网关规则以将连接从公用地址转发到连接网关的内部地址。

4. 基于已创建的安装包创建独立安装包。
5. 通过电子方式或可移动驱动器将独立安装包传送到目标设备。
6. 从独立包安装网络代理。

外部台设备机即连接到管理服务器。

关于漫游用户的连接配置文件

便携式电脑（也叫“设备”）的漫游用户需要更改连接到管理服务器的方法或者根据当前设备在企业网络中的位置在管理服务器之间进行切换。

连接配置文件仅支持运行 Windows 和 macOS 的设备。

使用单一管理服务器的不同地址

网络代理设备从组织网络或内部网可以连接到管理服务器。该情况可能需要网络代理使用不同的地址以连接到管理服务器：对于互联网连接的外部管理服务器地址和对于内部网络连接的内部管理服务器地址。

为此，请在网络代理策略属性（在“**应用程序设置**”→“**连接**”→“**连接配置文件**”→“**管理服务器连接配置文件**”区域中）中添加管理服务器的互联网连接配置文件。在配置文件创建窗口中，禁用“**仅用来接收更新**”选项并确保选择“**与此配置文件中指定的管理服务器设置同步连接设置**”选项。如果您使用连接网关访问管理服务器（例如，在“互联网访问：DMZ 中作为连接网关的网络代理”部分描述的 Kaspersky Security Center 配置中），您必须在连接配置文件的对应字段指定连接网关地址。

根据当前网络在管理服务器之间进行切换

如果组织有带有多个管理服务器的多个办公室，并且一些网络代理设备在期间进行移动，您需要网络代理连接到设备所在的本地网络中的管理服务器。

在这种情况下，您必须在网络代理策略属性中为每个办公室创建管理服务器的连接配置文件，但原始归属管理服务器所在的主办公室除外。在连接配置文件中指定管理服务器地址并启用或禁用“**仅用来接收更新**”选项：

- 在使用本地服务器下载更新时，如果您需要网络代理与归属管理服务器同步，则选择该选项。
- 如果网络代理必须被本地管理服务器完全管理，则禁用此选项。

此后，您必须设置切换到新创建的配置文件的条件：每个办公室至少一个条件，除了归属办公室。每个条件的目的包括办公室网络环境条目的检测。如果条件是真，对应配置文件被激活。如果没有条件是真，网络代理切换到归属管理服务器。

为漫游用户创建连接配置文件

管理服务器连接配置文件仅在运行 Windows 和 macOS 的设备上可用。

若要为漫游用户创建网络代理连接至管理服务器的连接配置文件，请执行以下操作：

1. 如果要为一组受管理设备创建连接配置文件，请打开该组的网络代理策略。为此，请执行以下操作：
   a. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**“。
   b. 单击当前路径链接。
   c. 在打开的窗口中，选择所需的管理组。
   之后，当前路径即被更改。
   d. 为受管理设备组添加网络代理策略。如果您已经创建网络代理策略，请单击其名称以打开策略属性。
2. 如果要为特定的受管理设备创建连接配置文件，请执行以下操作：
   a. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
   b. 单击受管理设备的名称。
   c. 在打开的受管理设备属性窗口中，转到“**应用程序**”选项卡。
   d. 单击仅应用于选定的受管理设备的网络代理策略的名称。
3. 在打开的属性窗口中，转到“**应用程序设置”→“连接**”→**“连接配置文件”。**
4. 在“**管理服务器连接配置文件**”区域中，单击“**添加**”按钮。
   默认下，连接配置文件列表包含<离线模式>和<归属管理服务器>配置文件。您不能编辑或删除配置文件。
   <离线模式>配置文件不指定任何服务器以连接。因此，网络代理，当切换到该配置文件时，当客户端设备上的应用程序工作在漫游策略下时不试图连接到任何管理服务器。如果设备与网络断开连接，可以使用 <离线模式> 配置文件。

<归属管理服务器> 配置文件用于指定在网络代理安装过程中选择的管理服务器的连接。当设备在外部网络中运行了一段时间后重新连接到管理服务器时，<归属管理服务器>配置文件被应用。

5. 在打开的“**配置配置文件**”窗口中，配置连接配置文件：

- **配置文件名称**

  在该输入字段中，您可以查看或更改连接配置文件名称。

- **管理服务器地址**

  客户端设备在配置文件激活期间必须连接的管理服务器地址。

- **端口号**

  用于连接的端口号。

- **SSL 端口**

  使用 SSL 协议时的连接端口号。

- **使用 SSL 连接**

  如果启用此选项，则使用 SSL 协议通过安全端口建立连接。
  默认情况下已启用该选项。我们建议您不要禁用此选项，以便您的连接保持安全。

- 如果您要在连接到互联网时使用代理服务器，请选择“**使用代理服务器**”选项。如果选择此选项，字段可用于输入设置。为代理服务器连接指定以下设置：

  - **地址**

    Kaspersky Security Center 用于连接到互联网的代理服务器地址。

  - **端口号**

    将建立 Kaspersky Security Center 代理服务器连接的端口号。

  - **代理服务器身份验证**

    如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭据。

  - **用户名**

    用于与代理服务器建立连接的用户账户（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

- **密码**

  建立代理服务器连接的账户所属的用户所设置的密码（如果选中“**代理服务器身份验证**”复选框，则该字段可用）。

  要查看输入的密码，单击并按住“**显示**”按钮足够长时间。

- **连接网关地址**

  通过客户端设备连接管理服务器的网关地址。

- **当管理服务器不可用时启用漫游模式**

  选中此复选框，当管理服务器不可用时，允许客户端设备上安装的应用程序在任何连接尝试中使用处于漫游模式的设备的策略配置文件以及漫游策略。如果没有为应用程序定义漫游策略，则使用激活策略。

  如果禁用此选项，则应用程序将使用已激活的策略。

  默认情况下已清除该选框。

- **仅用来接收更新**

  如果启用此选项，则该配置文件将仅被客户端设备上安装的应用程序用来下载更新。对于其他操作，程序将使用在网络代理安装过程中定义的初始连接设置连接管理服务器。

  默认情况下已启用该选项。

- **与此配置文件中指定的管理服务器设置同步连接设置**

  如果启用此选项，网络代理将使用配置文件属性中指定的设置连接至管理服务器。

  如果禁用此选项，网络代理将使用安装期间已指定的原始设置连接至管理服务器。

  如果禁用“**仅用来接收更新**”选项，则此选项可用。

  默认情况下已禁用该选项。

程序将为漫游用户创建一个用于将网络代理连接至管理服务器的配置文件。当网络代理使用此配置文件连接到管理服务器后，客户端设备上安装的应用程序将使用处于漫游模式的设备的策略或漫游策略。

关于将网络代理切换到其他管理服务器

如果更改了下列网络设置，Kaspersky Security Center 允许您将客户端设备网络代理切换至其他管理服务器：

- **DHCP 服务器地址条件** – 网络 Dynamic Host Configuration Protocol (DHCP) 服务器的 IP 地址已更改。
- **默认连接网关地址条件** – 主要网络网关的地址已更改。
- **DNS 域条件** – 子网的 DNS 后缀已更改。
- **DNS 服务器地址条件** – 网络 DNS 服务器的 IP 地址已更改。
- **WINS 服务器地址条件** – 网络 WINS 服务器的 IP 地址已更改。此设置仅适用于运行 Windows 的设备。

- **名称可解析性条件** – 客户端设备的 DNS 或 NetBIOS 名称已更改。
- **子网条件** – 更改子网地址和掩码。
- **Windows 域可访问性条件** – 更改客户端设备连接到的 Windows 域的状态。此设置仅适用于运行 Windows 的设备。
- **SSL 连接地址可访问性条件** – 客户端设备可以或无法（取决于您选择的选项）与指定服务器建立SSL连接（名称：端口）。您必须使用具有能够处理高负载和频繁的网络代理连接请求的软件的专用服务器。请勿指定管理服务器的端口。对于每个服务器，都可以额外指定一个 SSL 证书。在这种情况下，网络代理除了检查 SSL 连接的功能外，还会验证服务器证书。如果证书不匹配，连接将失败。

只有运行 Windows 或 macOS 的设备上安装的网络代理支持此功能。

网络代理连接至管理服务器的初始设置在安装网络代理时定义。此后，如果创建了将网络代理切换至其他管理服务器的规则，网络代理将以下列方式响应网络设置的更改：

- 如果网络设置符合已创建的规则之一，网络代理将连接至该规则中指定的管理服务器。如果该规则中已经启用漫游切换策略，客户端设备上的应用程序将切换至漫游策略。
- 如果未应用任何规则，网络代理将回滚至安装过程中指定的管理服务器连接默认设置。客户端设备上安装的应用程序将回滚至活动策略。
- 如果无法访问管理服务器，网络代理将使用用户漫游策略。

> 仅当在网络代理策略设置中启用“**当管理服务器不可用时启用漫游模式**”选项时，网络代理才会切换到漫游策略。

网络代理连接至管理服务器的设置保存在连接配置文件中。在连接配置文件中，您可以创建将客户端设备切换至漫游策略的规则，并可对配置文件进行配置，使其仅可用于下载更新。

根据网络位置创建网络代理切换规则

> 根据网络位置切换网络代理仅在运行 Windows 和 macOS 的设备上可用。

若要创建一个当网络设置改变时将网络代理从一个管理服务器切换至另一个的规则，请执行以下操作：

1. 如果要为一组受管理设备创建规则，请打开该组的网络代理策略。为此，请执行以下操作：
   a. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**“。
   b. 单击当前路径链接。
   c. 在打开的窗口中，选择所需的管理组。
   之后，当前路径即被更改。
   d. 为受管理设备组添加网络代理策略。如果您已经创建网络代理策略，请单击其名称以打开策略属性。

2. 如果要为特定的受管理设备创建规则，请执行以下操作：

   a. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。

   b. 单击受管理设备的名称。

   c. 在打开的受管理设备属性窗口中，转到“**应用程序**”选项卡。

   d. 单击仅应用于选定的受管理设备的网络代理策略的名称。

3. 在打开的属性窗口中，转到“**应用程序设置**”→“**连接**”→“**连接配置文件**”。

4. 在“**网络位置设置**”区域中，单击“**添加**”按钮。

5. 在打开的属性窗口中，配置网络位置描述和切换规则。指定以下网络位置描述设置：

   - **描述**

     网络位置描述名称不能超过 255 字符或包含特殊字符，例如 ("*<>?\/:|).

   - **使用连接配置文件**

     在该下拉列表中，您可以指定网络代理用于连接至管理服务器的连接配置文件。该配置文件将在网络位置描述条件被满足时使用。连接配置文件包含网络代理连接到管理服务器的设置；它还定义了客户端设备切换到漫游策略的时间。配置文件仅用于下载更新。

   - **描述已启用**

     选中此复选框可启用新的网络位置描述。

6. 选择网络代理切换规则的条件：

   - **DHCP 服务器地址条件** – 网络 Dynamic Host Configuration Protocol (DHCP) 服务器的 IP 地址已更改。
   - **默认连接网关地址条件** – 主要网络网关的地址已更改。
   - **DNS 域条件** – 子网的 DNS 后缀已更改。
   - **DNS 服务器地址条件** – 网络 DNS 服务器的 IP 地址已更改。
   - **WINS 服务器地址条件** – 网络 WINS 服务器的 IP 地址已更改。此设置仅适用于运行 Windows 的设备。
   - **名称可解析性条件** – 客户端设备的 DNS 或 NetBIOS 名称已更改。
   - **子网条件** – 更改子网地址和掩码。
   - **Windows 域可访问性条件** – 更改客户端设备连接到的 Windows 域的状态。此设置仅适用于运行 Windows 的设备。
   - **SSL 连接地址可访问性条件** – 客户端设备可以或无法（取决于您选择的选项）与指定服务器建立 SSL 连接（名称:端口）。对于每个服务器，都可以额外指定一个 SSL 证书。在这种情况下，网络代理除了检查 SSL 连接的功能外，还会验证服务器证书。如果证书不匹配，连接将失败。

使用逻辑运算符 AND 可组合规则中的条件。要基于网络位置描述触发切换规则，所有的规则切换条件必须被满足。

7. 在条件区域，指定何时应将网络代理切换到另一个管理服务器。为此，请单击“**添加**”按钮，然后设置条件值。

   此外，默认情况下启用“**至少符合列表中的一个参数值**”选项。如果您希望所有指定值都满足条件，可以禁用此选项。

8. 保存更改。

一个新的网络位置描述的切换规则将被创建；当满足其条件时，网络代理将使用此规则指定的配置文件连接至管理服务器。

保护部署向导

要安装卡巴斯基应用程序，您可以使用保护部署向导。保护部署向导允许使用特别创建的安装包或直接从分发包来远程安装应用程序。

保护部署向导执行以下操作：

- 为应用程序安装下载安装包（如果之前未创建）。安装包位于“**发现和部署**”→“**部署和分配**”→“**安装包**”。在将来，您可以使用该安装包安装程序。
- 为特定设备或管理组创建并启动远程安装任务。新创建的远程安装任务存储在“**任务**”区域中。您可以以后手动启动此任务。任务类型为“**远程安装应用程序**”。

如果您想在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，首先安装 insserv-compat 软件包以配置网络代理。

步骤 1：开始保护部署向导

要手动启动保护部署向导，

在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**保护部署向导**”。

保护部署向导启动。使用“**下一步**”按钮继续向导操作。

步骤 2：选择安装包

选择您要安装的应用程序安装包。

如果所需应用程序安装包未列出，请单击“**添加**”按钮，然后从列表中选择应用程序。

步骤 3：选择分发密钥文件或激活码的方法

选择分发密钥文件或激活码的方法：

- **不添加授权许可密钥到安装包**

  密钥被自动分发到所兼容的所有设备：
  - 如果自动分发在密钥属性中启用。
  - 如果**添加密钥**任务已创建。

- **添加授权许可密钥到安装包**

  密钥与安装包一起被分发到设备。

  我们不建议您使用该方法分发密钥，因为将启用对安装包存储库的共享读取访问权限。

如果安装包已经包含密钥文件或激活码，将显示此窗口，但其中只包含授权许可密钥信息。

步骤 4：选择网络代理版本

如果您选择了非网络代理安装包，您也必须安装网络代理，它连接应用程序到 Kaspersky Security Center 管理服务器。

选择网络代理的最新版本。

步骤 5：选择设备

指定要安装应用程序的设备列表：

- **安装到受管理设备**

  如果选择该选项，程序将为该设备组创建远程安装任务。

- **选择设备以安装**

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。
  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

步骤 6：指定远程安装任务设置

在“**远程安装任务设置**”页面，指定应用程序远程安装设置。

在“**强制下载安装包**”设置组中，指定如何将安装程序所需的文件分发到客户端设备中。

- **使用网络代理**

  如果启用此选项，安装包通过安装在客户端设备上的网络代理传送到客户端设备。

  如果禁用此选项，则使用客户端的操作系统传送安装包。

  如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。

  默认情况下已启用该选项。

- **通过分发点使用操作系统资源**

  如果启用此选项，安装包使用操作系统工具通过分发点传送到客户端设备。如果网络中存在不止一个分发点，那么您可以选择本选项。

  如果启用“**使用网络代理**”选项，仅在网络代理工具不可用时才通过操作系统工具传送文件。

  默认情况下，已经为虚拟管理服务器上创建的远程安装任务启用此选项。

- **通过管理服务器使用操作系统资源**

  如果启用此选项，文件将使用客户端设备的操作系统工具通过管理服务器传送到客户端设备。如果客户端设备上未安装网络代理，但是客户端设备与管理服务器在同一网络，则可以启用此选项。

  默认情况下已启用该选项。

当网络上存在分发点时，选择哪个选项都无关紧要。即使管理服务器可用但分发点不可用，安装包也只会通过分发点传输。

定义附加设置：

- **如果已经安装应用程序则不再重新安装**

  如果启用此选项，则如果选定的应用程序已安装到该客户端设备上，将不再重新安装它。

  如果禁用此选项，仍将安装应用程序。

  默认情况下已启用该选项。

- **在活动目录组策略中指定安装包的安装**

  如果启用此选项，安装包将使用 Active Directory 组策略进行安装。

  如果选择网络代理安装包，则该选项可用。

  默认情况下已禁用该选项。

步骤 7：重启管理

如果安装应用程序时操作系统必须重启，指定要执行的操作：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

步骤 8：安装前删除不兼容的应用程序

该步骤仅在您部署的应用程序已知与其他应用程序不兼容时才显示。

如果您想让 Kaspersky Security Center 自动卸载与您部署的应用程序不兼容的应用程序，则选择该选项。

不兼容应用程序列表也被显示。

如果您不选择该选项，应用程序将仅被安装到没有不兼容应用程序的设备。

步骤 9：移动设备到受管理设备

指定设备是否在安装网络代理后必须被移动到管理组。

- **不移动设备**

  设备保留在当前所在组中。未被放置在任何组的设备保持未分配。

- **将未分配的设备移动到此组**

  设备被移动到您选择的管理组。

默认情况下已选择“**不移动设备**”选项。为了安全起见，您可能需要手动移动设备。

步骤 10：选择访问设备的账户

如果必要，添加要用于启动远程安装任务的账户：

- **不需要账户(网络代理已安装)**

  如果该选项被选中，您不是必须指定一个账户，并在该账户下运行程序的安装。将使用运行管理服务器服务的账户运行该任务。

  如果网络代理未安装在客户端设备上，该选项不可用。

- **需要账户(不使用网络代理)**

  如果您为其分配远程安装任务的设备上未安装网络代理，请选择此选项。在这种情况下，您可以指定用户账户或 SSH 证书来安装应用程序。

  - **本地账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地账户**，然后指定用户账户凭据。

    您可以指定多个用户账户，例如，没有一个账户拥有分配任务所对应的所有设备上的全部所需权限时。在此情况下，已经添加的所有账户都用于从上到下按顺序运行该任务。

- **SSH 证书**。如果要在基于 Linux 的客户端设备上安装应用程序，您可以指定 SSH 证书而不是用户账户。单击**添加**按钮，选择**SSH 证书**，然后指定证书的私钥和公钥。

  要生成私钥，您可以使用 ssh-keygen 实用程序。请注意，Kaspersky Security Center 支持 PEM 格式的私钥，但 ssh-keygen 实用程序默认生成 OPENSSH 格式的 SSH 密钥。Kaspersky Security Center 不支持 OPENSSH 格式。要以支持的 PEM 格式创建私钥，请在 ssh-keygen 命令中添加“-m PEM”选项。例如：

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
  ```

步骤 11：开始安装

该页面是向导的最后一步。在该步骤， **远程安装任务**已被成功创建并配置。

默认情况下，未选定“**向导完成时运行任务**”选项。如果您选择该选项， **远程安装任务**将在您完成向导后立即启动。如果您不选择该选项， **远程安装任务**不会启动。您可以以后手动启动此任务。

单击“**确定**”完成保护部署向导的最后一步。

通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序

本节介绍通过 Kaspersky Security Center Web Console 在组织中的客户端设备上部署 Kaspersky 应用程序。

方案：通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序

此方案说明如何通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序。您可以使用快速启动向导和保护部署向导，或者您可以手动完成所有必要步骤。

以下应用程序可以使用 Kaspersky Security Center Web Console 进行部署：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

阶段

Kaspersky 应用程序部署分阶段进行：

1 下载应用程序的管理插件

此阶段由快速启动向导处理。如果您选择不运行向导，手动下载 Kaspersky Endpoint Security for Windows 插件。

如果您计划管理公司移动设备，请按照 Kaspersky Security for Mobile 帮助 中提供的说明来下载和安装 Kaspersky Endpoint Security for Android 的管理插件。

2 下载并创建安装包

此阶段由快速启动向导处理。

通过快速启动向导可以下载带有管理插件的安装包。如果在运行向导时未选择此选项，或者根本没有运行向导，则必须手动下载安装包。

如果在某些设备（例如远程员工的设备）上无法通过 Kaspersky Security Center 安装 Kaspersky 应用程序，则可以为应用程序创建独立安装包。如果您使用独立软件包安装卡巴斯基应用程序，则不必创建和运行远程安装任务，也不必为 Kaspersky Endpoint Security for Windows 创建和配置任务。

3 创建、配置和运行远程安装任务

对于 Kaspersky Endpoint Security for Windows，该阶段是保护部署向导的一部分，它在快速启动向导完成后自动启动。如果您选择不运行保护部署向导，您必须手动创建该任务并手动配置它。

您也可以为不同管理组或不同设备分类手动创建几个远程安装任务。您可以在这些任务中部署应用程序的不同版本。

确保您网络中的所有设备均已被发现；然后运行远程安装任务。

在基于 Linux 的资产上安装 nmap 实用程序。启用网络位置感知功能需要此实用程序。

如果您想在装有 SUSE Linux Enterprise Server 15 操作系统的设备上安装网络代理，首先安装 insserv-compat 软件包以配置网络代理。

如果要在使用操作系统 RED OS 7.3.4 或更高版本或 MSVSPHERE 9.2 或更高版本的设备上安装网络代理，请安装 libxcrypt-compat 包以确保网络代理正确运行。

4 为受管理应用程序创建和配置任务

Kaspersky Endpoint Security for Windows 的*更新安装任务*必须被配置。

该阶段是快速启动向导的一部分：任务被使用默认设置自动创建和配置。如果您未运行向导，您必须手动创建该任务并手动配置它。如果您使用快速启动向导，请确保任务的计划符合您的要求。（默认情况下，任务的预定开始设置为**手动**，但您可能希望选择其他选项。）

其他 Kaspersky 应用程序可能具有其他默认任务。请参考对应应用程序的文档。

确保您创建的每个任务的计划都符合要求。

5 安装 Kaspersky Security for Mobile（可选）

如果您计划管理公司移动设备，请参见 Kaspersky Security for Mobile 帮助 中提供的说明，以了解有关部署 Kaspersky Endpoint Security for Android 的信息。

6 **创建策略**

手动为每个应用程序创建策略或（如果是 Kaspersky Endpoint Security for Windows）通过快速启动向导。您可以使用策略默认设置；您也可以根据需要随时修改策略默认设置。

7 **验证结果**

确保部署成功完成：您的每个应用程序都拥有策略和任务，这些应用程序被安装到受管理设备。

结果

完成方案可以导致如下：

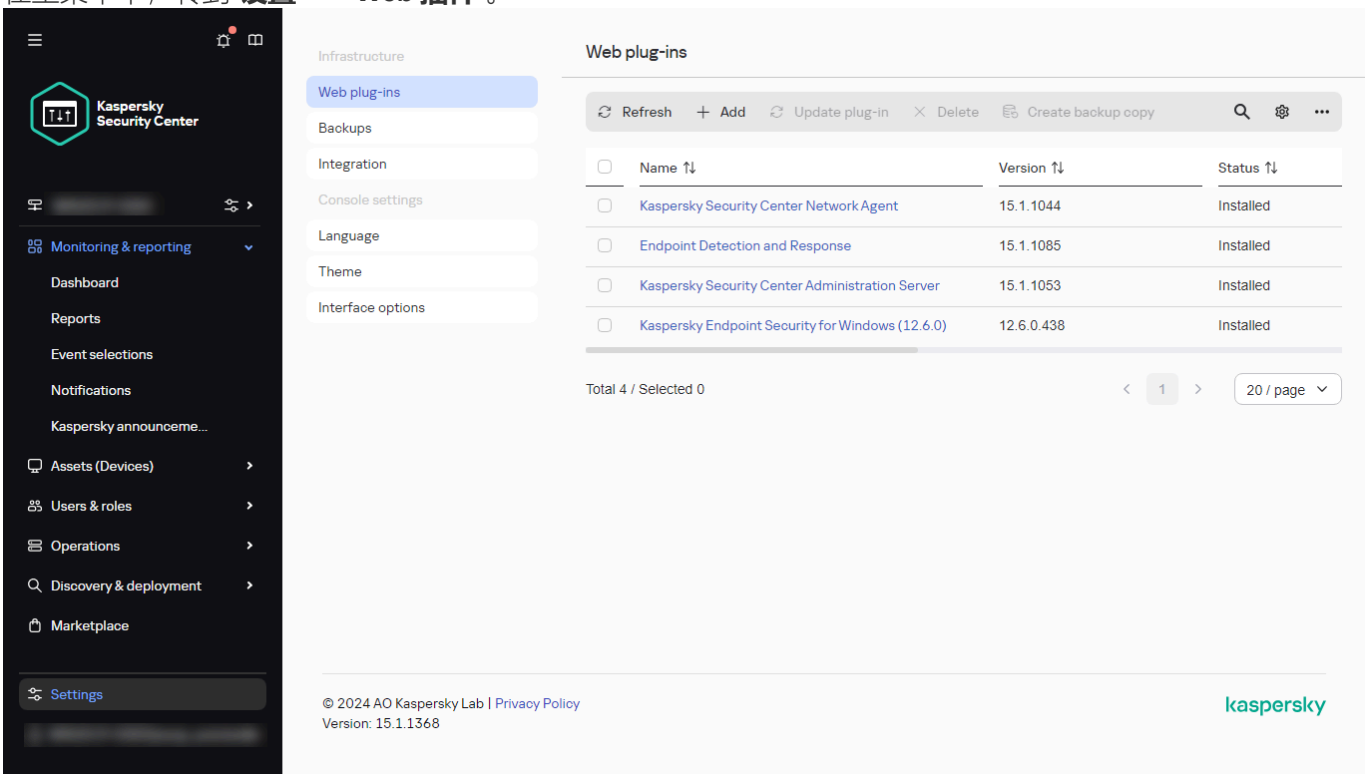
- 所选应用程序的所有所需策略和任务被创建。
- 任务计划根据您的需要被配置。
- 所选应用程序被部署，或者计划在所选客户端设备上部署。

获取 Kaspersky 应用程序插件

要部署 Kaspersky 应用程序，例如 Kaspersky Endpoint Security for Windows，您必须为此应用程序下载管理插件。

要下载 Kaspersky 应用程序的管理插件：

1. 在主菜单中，转到“**设置**” → “**Web 插件**”。



已安装的 Web 插件列表

2. 在打开的窗口中，单击“**添加**”按钮。

   可用插件列表被显示。

3. 在可用插件列表中，通过点击其名称选择您要下载的插件（例如，Kaspersky Endpoint Security 11 for Windows）。

   插件描述页面被显示。

4. 在插件描述页面，点击“**安装插件**”。

5. 当安装完成时，点击“**确定**”。

管理插件使用默认配置被下载并显示在管理插件列表。

您可以从文件添加插件以及更新下载的插件。您可以从卡巴斯基技术支持网页下载管理插件和 Web 管理插件。

要从文件下载或更新插件：

1. 在主菜单中，转到 **设置** → “**Web 插件**”。

2. 执行以下操作之一：

   - 单击**从文件添加**以从文件下载插件。
   - 单击**从文件更新**以从文件下载插件更新。

3. 指定文件和文件签名。

4. 下载指定的文件。

管理插件被从文件下载并显示在管理插件列表。

下载和创建卡巴斯基应用程序的安装包

如果管理服务器可以访问 Internet，则可以从 Kaspersky Web 服务器创建卡巴斯基应用程序的安装包。

要下载并创建卡巴斯基应用程序的安装包：

1. 执行以下操作之一：

   - 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**安装包**”。
   - 在主菜单中，转到“**操作**”→ “**存储库**” → “**安装包**”。

   您可以在屏幕通知列表中查看关于卡巴斯基应用程序的新安装包的通知。如果有关于新安装包的通知，您可以单击通知旁边的链接并转到可用安装包列表。

   此时会显示管理服务器上可用的安装包的列表。

2. 单击**添加**。

   新安装包向导启动。使用“**下一步**”按钮进行向导。

3. 选择“**为卡巴斯基应用程序创建安装包**”。

   将显示 Kaspersky Web 服务器上的可用安装包列表。该列表仅包含与当前版本的 Kaspersky Security Center 兼容的应用程序的安装包。

4. 单击安装包名称。例如，Kaspersky Endpoint Security for Windows (11.1.0)。

带有安装包信息的窗口打开。

如果符合适用的法律法规，您可以下载并使用包含实施强加密的加密工具的安装包。要下载可满足组织需求的有效 Kaspersky Endpoint Security for Windows 安装包，请参考组织的客户端设备所在国家/地区的法律。

5. 阅读信息，然后单击“**下载并创建安装包**”按钮。

   如果分发包无法转换为安装包，将显示“**下载分发包**”按钮而不是“**下载并创建安装包**”。

   下载安装包到管理服务器开始。您可以关闭向导的窗口或继续执行说明的下一步。如果关闭向导的窗口，下载过程将在后台模式下继续。

   如果要跟踪安装包下载过程：

   a. 在主菜单中，转到“**操作**”→“**存储库**”→“**安装包**”→“**进行中()**”。

   b. 在表的“**下载进度**”列和“**下载状态**列”中跟踪操作进度。

   该过程完成后，安装包将添加到“**已下载**”选项卡上的列表中。如果下载过程停止并且下载状态切换为“**接受 EULA**，则单击安装包名称，然后继续执行说明的下一步。

   如果所选分发包中包含的数据大小超过当前限制，将显示错误消息。您可以更改限制值，然后继续创建安装包。

6. 对于一些卡巴斯基应用程序，下载过程中将显示“**显示 EULA**”按钮。如果它不显示，做以下操作：

   a. 单击“**显示 EULA**”按钮以阅读最终用户授权许可协议（EULA）。

   b. 阅读屏幕上显示的 EULA，然后单击“**接受**”。

   在您接受 EULA 后，下载继续。如果您单击“**拒绝**”，下载将停止。

7. 下载完成后，单击“**关闭**”按钮。

所选安装包将下载到管理服务器共享文件夹及 Packages 子文件夹。下载后，安装包出现在安装包列表。

更改自定义安装包数据大小的限制

创建自定义安装包期间解压缩的数据总大小受到限制。默认限制为 1 GB。

如果尝试上传的压缩文件所包含的数据超出当前限制，将显示一条错误消息。从大型分发包创建安装包时，可能必须增加此限制值。

要更改自定义安装包大小的限制值：

1. 在管理服务器设备上，在用于安装管理服务器的账户下运行命令提示符。

2. 将当前目录更改为 Kaspersky Security Center 安装文件夹（通常为 <磁盘>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）。

3. 根据管理服务器安装的类型，使用管理员权限输入以下命令之一：

- 普通本地安装：

  ```
  klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes>
  ```

- 在 Kaspersky Security Center 故障转移集群上安装：

  ```
  klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes> --stp klfoc
  ```

- 在 Windows 服务器故障转移集群上安装：

  ```
  klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <字节数> --stp cluster
  ```

其中 <number of bytes> 是十六进制或十进制格式的字节数。

例如，如果要求的限制为 2 GB，您可以指定十进制值 2147483648 或十六进制值 0x80000000。在这种情况下，对于管理服务器的本地安装，您可以使用以下命令：

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
```

自定义安装包数据大小的限制即被更改。

下载 Kaspersky 应用程序的分发包

在 Kaspersky Security Center Web Console 中，可以下载和保存 Kaspersky 应用程序的分发包。您可以使用分发包手动安装应用程序，而不使用 Kaspersky Security Center。

要下载和保存 Kaspersky 应用程序的分发包：

1. 在主菜单中，转到 **操作 → 卡巴斯基应用程序 → 当前应用程序版本**。

   可用分发包、插件和补丁列表打开。Kaspersky Security Center 仅显示与其当前版本兼容的项目。

2. 在列表中，点击您要下载的包名称。

   包描述打开。

3. 阅读说明，然后单击“**下载并创建安装包**”按钮。

   如果分发包无法转换为安装包，将显示“**下载分发包**”按钮而不是“**下载并创建安装包**”。

   下载安装包到管理服务器开始。

所选的安装包或分发包被下载到管理服务器共享文件夹，到 **Packages** 子文件夹。下载后，安装包出现在安装包列表。

检查 Kaspersky Endpoint Security 是否已成功部署

要确保您已正确部署 Kaspersky 应用程序（例如 Kaspersky Endpoint Security）：

1. 使用 Kaspersky Security Center Web Console，确保您具有如下：
   - 您使用的 Kaspersky Endpoint Security 和/或其他安全应用程序的策略。
   - Kaspersky Endpoint Security for Windows 任务：*快速扫描*任务和*安装更新*任务（如果您使用 Kaspersky Endpoint Security for Windows）。
   - 您使用的其他安全应用程序任务。
2. 在选择用于安装的受管理设备之一上，确保以下：
   - 已安装 Kaspersky Endpoint Security 或其他 Kaspersky 安全应用程序。
   - 在 Kaspersky Endpoint Security 上，文件威胁防护、Web 威胁防护和邮件威胁防护设置与您为该设备创建的策略匹配。
   - Kaspersky Endpoint Security 服务可以被手动停止和启动。
   - 可以被手动停止和启动的组任务。

创建独立安装包

您和组织中的设备用户可以使用独立安装包在设备上手动安装应用程序。

独立安装包是一个可执行文件 (installer.exe)，您可以将其存储在 Web 服务器或共享文件夹中，通过电子邮件发送，或通过其他方法传输到客户端设备。在客户端设备上，用户可以在本地运行接收到的文件以安装应用程序，而无需涉及 Kaspersky Security Center。您可以为 Kaspersky 应用程序以及适用于 Windows、macOS 和 Linux 平台的第三方应用程序创建独立安装包。要为第三方应用程序创建独立安装包，必须创建自定义安装包。

确保独立安装包不可用于未经授权的人员。

要创建独立安装包：

1. 执行以下操作之一：
   - 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**安装包**”。
   - 在主菜单中，转到“**操作**”→ “**存储库**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。
2. 在安装包列表中选择安装包，然后在列表上方单击“**部署**”按钮。
3. 选择**使用独立包**选项。
   独立安装包创建向导启动。使用**下一步**按钮进行向导。

4. 如果随着所选的应用程序安装网络代理，请确保已启用“**网络代理和该应用程序一起安装**”选项。

   显示的选项取决于您为其创建独立安装包的应用程序。

   默认情况下已启用该选项。如果您不确定设备上是否安装了网络代理，建议启用此选项。如果设备上已经安装了网络代理，则在安装带有网络代理的独立安装包之后，网络代理将更新为较新的版本。

   如果禁用此选项，则网络代理将不会安装在设备上，并且该设备将不受管理。

   如果管理服务器上已经存在用于所选应用程序的独立安装包，则向导会通知您这一事实。在这种情况下，您必须选择以下操作之一：

   - **创建独立安装包**。例如，如果要为新的应用程序版本创建独立安装包，并且还希望保留为先前的应用程序版本创建的独立安装包，请选择此选项。新的独立安装包位于另一个文件夹中。
   - **使用现有的独立安装包**。如果要使用现有的独立安装包，请选择此选项。安装包创建过程将不会开始。
   - **重新编译现有的独立安装包**。如果要再次为同一应用程序创建独立安装包，请选择此选项。独立安装包位于同一文件夹中。

5. 在“**移动到受管理设备列表**”步骤中，默认已启用“**不移动设备**”选项。如果您不希望在安装网络代理后将客户端设备移至任何管理组，请将此选项保持启用状态。

   如果要在安装网络代理后移动客户端设备，请选择“**将未分配的设备移动到此组**”选项并指定要将客户端设备移至的管理组。默认情况下，设备移至“**受管理设备**”组。

6. 独立安装包创建过程完成后，单击“**完成**”按钮。

   独立安装包创建向导关闭。

此时会创建独立安装包，并将其放置在管理服务器共享文件夹的 PkgInst 子文件夹中。您可以通过单击安装包列表上方的“**查看独立包列表**”按钮来查看独立包列表。

查看独立安装包列表

您可以查看独立安装包列表以及每个独立安装包的属性。

要查看所有安装包中独立安装包的列表：

在列表上方，单击“**查看独立包列表**”按钮。

在独立安装包列表中，其属性显示如下：

- **包名称**。根据安装包中包含的应用程序名称和应用程序版本自动形成的独立安装包名称。
- **应用程序名称**。独立安装包中包含的应用程序名称。
- **应用程序版本**。
- **网络代理安装包名称**。仅当独立安装包中包含网络代理时，才显示该属性。
- **网络代理版本**。仅当独立安装包中包含网络代理时，才显示该属性。
- **大小**。文件大小（MB）。

- **组**。安装网络代理后，客户端设备将移动到的组的名称。
- **创建日期**。独立安装包的创建日期和时间。
- **修改日期**。独立安装包的修改日期和时间。
- **路径**。独立安装包所在文件夹的完整路径。
- **网址**。独立安装包位置的网址。
- **文件哈希**。该属性用于证明独立安装包没有被第三方更改，并且用户拥有的文件与您创建并传输给用户的文件相同。

要查看特定安装包的独立安装包列表：

在列表中选择安装包，然后在列表上方单击“**查看独立包列表**”按钮。

在独立安装包列表中，您可以执行以下操作：

- 通过单击“**发布**”按钮在 Web 服务器上发布独立安装包。您将独立安装包链接发送给的用户可以下载已发布的独立安装包。
- 通过单击“**取消发布**”按钮取消在 Web 服务器上发布独立安装包。未发布的独立安装包只能被您和其他管理员下载。
- 通过单击“**下载**”按钮将独立安装包下载到设备上。
- 通过单击“**通过电子邮件发送**”按钮发送带有独立安装包链接的电子邮件。
- 通过单击“**删除**”按钮删除独立安装包。

创建自定义安装包

您可以使用自定义安装包执行以下操作：

- 在客户端设备上安装任何应用程序（例如文本编辑器），例如通过任务。
- 创建独立安装包。

自定义安装包是一个包含一组文件的文件夹。创建自定义安装包的源是*存档文件*。存档文件包含一个或多个必须包含在自定义安装包中的文件。创建自定义安装包时，您可以指定命令行参数，例如以静默模式安装应用程序。

如果您有漏洞和补丁管理 (VAPM) 功能的活动授权许可密钥，则可以转换相关自定义安装包的默认安装设置，并使用 Kaspersky 专家建议的值。仅当相应的可执行文件包含在第三方应用程序的 Kaspersky 数据库中时，才会在创建自定义安装包的过程中自动转换设置。

要创建自定义安装包：

1. 执行以下操作之一：

   - 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**安装包**”。
   - 在主菜单中，转到“**操作**”→ “**存储库**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。

2. 单击**添加**。
   新安装包向导启动。使用**下一步**按钮进行向导。

3. 选择“**从文件创建安装包**”

4. 指定包名称并单击“**浏览**”按钮。
   将在浏览器中打开一个标准 Windows“**打开**”窗口，允许您选择一个文件来创建安装包。

5. 选择可用磁盘上的压缩文件。
   您可以上传 ZIP、CAB、TAR 或 TAR.GZ 压缩文件。无法从 SFX（自解压存档）文件创建安装包。

   > 如果要在安装包安装过程中转换设置，请确保“**向导结束后，对被 Kaspersky Security Center 识别的应用程序转换设置到推荐值**”复选框被选中，然后单击“**下一步**”。

   开始将文件上传到 Kaspersky Security Center 管理服务器。

   > 如果启用了建议的安装设置，则 Kaspersky Security Center 15.1 将检查可执行文件是否包含在第三方应用程序的 Kaspersky 数据库中。如果检查成功，您会收到一条通知，通知您文件已被识别。设置已转换，并且自定义安装包已创建。不需要进一步操作。单击**完成**按钮关闭向导。

6. 选择一个文件（从所选压缩文件中提取的文件列表中选择），然后指定可执行文件的命令行参数。
   您可以指定命令行参数，以静默模式从安装包中安装应用程序。指定命令行参数是可选的。
   创建安装包的过程将开始。
   该向导将在过程完成时通知您。
   如果未创建安装包，则会显示相应的消息。

7. 单击**完成**按钮关闭向导。

   您创建的安装包将下载到管理服务器共享文件夹的 Packages 子文件夹中。下载后，安装包出现在安装包列表。

在管理服务器上的可用安装包列表中，通过单击带有自定义安装包名称的链接，您可以：

- 查看安装包的以下属性：
  - **名称**。自定义安装包名称。
  - **源**。应用程序供应商名称。
  - **应用程序**。打包到自定义安装包中的应用程序名称。

- **版本**。应用程序版本。
- **语言**。打包到自定义安装包中的应用程序的语言。
- **大小(MB)**。安装包的大小。
- **操作系统**安装包适合的操作系统的类型。
- **创建日期**。安装包创建日期。
- **修改日期**。安装包修改日期。
- **类型**。安装包的类型。

- 更改安装包名称和命令行参数。该功能仅适用于未基于 Kaspersky 应用程序创建的安装包。

如果在自定义安装包创建过程中将安装包安装设置转换为推荐值，则会在自定义安装包属性的“**设置**”选项卡上出现两个额外区域：“**设置**”和“**安装进程**”。

“**设置**”区域包含下表所示的属性：

- **名称**。此列显示分配给安装参数的名称。
- **类型**。此列显示安装参数的类型。
- **值**。此列显示由安装参数定义的数据类型（Bool、Filepath、Numeric、Path 或 String）。

“**安装进程**”部分包含一个表，该表描述了自定义安装包中包括的更新的以下属性：

- **名称**。更新名称。
- **描述**。更新说明。
- **来源**。更新的来源，即由 Microsoft 发布还是由其他第三方开发商发布。
- **类型**。更新类型，即用于驱动程序还是用于应用程序。
- **类别**。针对 Microsoft 更新显示的 Windows Server Update Services (WSUS) 类别（关键更新、定义更新、驱动程序、Feature Pack、安全更新、Service Pack、工具、更新汇总、更新或升级）。
- **根据 MSRC 的重要级别**。Microsoft 安全响应中心 (MSRC) 定义的更新重要级别。
- **重要级别**。Kaspersky 定义的更新重要级别。
- **补丁重要级别（用于 Kaspersky 应用程序的补丁）**。补丁的重要级别（如果用于 Kaspersky 应用程序）。
- **文章**。知识库中描述更新的文章的标识符 (ID)。
- **公告**。描述更新的安全公告的 ID。
- **未分配安装**。显示更新是否具有“未分配安装”状态。
- **待安装**。显示更新是否具有“待安装”状态。

- **正在安装**。显示更新是否具有“正在安装”状态。
- **已安装**。显示更新是否具有“已安装”状态。
- **失败**。显示更新是否具有“失败”状态。
- **需要重新启动**。显示更新是否具有“需要重新启动”状态。
- **已注册**。显示注册更新的日期和时间。
- **以交互模式安装**。显示更新是否需要在安装过程中与用户交互。
- **撤销**。显示更新的撤销日期和时间。
- **更新批准状态**。显示更新是否被批准安装。
- **修订**。显示更新的当前修订号。
- **更新 ID**。显示更新的 ID。
- **应用程序版本**。显示应用程序将更新到的版本号。
- **被替代**。显示可以替代该更新的其他更新。
- **替代**。显示该更新可以替代的其他更新。
- **您必须接受授权许可协议的条款**。显示更新是否需要接受最终用户授权许可协议 (EULA) 的条款。
- **供应商**。显示更新供应商的名称。
- **应用程序系列**。显示更新所属的应用程序系列的名称。
- **应用程序**。显示更新所属的应用程序的名称。
- **语言**。显示更新本地化的语言。
- **未分配安装（新版本）**。显示更新是否具有“未分配安装（新版本）”状态。
- **需要先决条件安装**。显示更新是否具有“需要安装先决条件”状态。
- **下载模式**。显示更新下载的模式。
- **是补丁**。显示更新是否为补丁。
- **未安装**。显示更新是否具有“未安装”状态。

将安装包分发至从属管理服务器

Kaspersky Security Center 允许您创建安装包用于卡巴斯基应用程序和第三方应用程序，以及将安装包分发至客户端设备并从包中安装应用程序。要优化主管理服务器上的负载，您可以将安装包分发至从属管理服务器。之后，从属服务器将安装包传输到客户端设备，然后您可以在客户端设备上远程安装应用程序。

要将安装包分发至从属管理服务器：

1. 请确保从属管理服务器连接至主管理服务器。
2. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
   将显示任务列表。
3. 单击“**添加**”按钮。
   “新任务向导”启动。遵照向导的说明。
4. 在**新任务设置**页面的**应用程序**下拉列表中，选择**Kaspersky Security Center**。然后，从**任务类型**下拉列表中选择**分发安装包**，然后指定任务名称。
5. 在“**任务范围**”页面，通过以下方式之一选择任务分配到的设备：
   - 如果要为特定管理组中的所有从属管理服务器创建任务，选择该组，然后为它创建组任务。
   - 如果要为特定的从属管理服务器创建任务，选择这些服务器，然后为它们创建任务。
6. 在“**分发的安装包**”页面，选择要复制到从属管理服务器的安装包。
7. 指定一个账户，以该账户来运行“*分发安装包*”任务。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输入该账户的凭据。
8. 在**完成任务创建**页面上，您可以启用**创建完成时打开任务详情**选项以打开任务属性窗口，然后修改默认任务设置。或者，您可以稍后随时配置任务设置。
9. 单击“**完成**”按钮。
   为了将安装包分发至从属管理服务器而创建的任务显示在任务列表中。
10. 您可以手动运行该任务，或者等待任务按照您在任务设置中指定的时间表启动。

任务完成后，所选的安装包将复制到指定的从属管理服务器。

使用远程安装任务安装应用程序

Kaspersky Security Center 允许您远程安装应用程序到设备，使用远程安装任务。那些任务通过专门向导被创建被分配到设备。要更快和更便捷地分配任务，您可以在向导窗口中指定设备（最多 1000 部设备），使用以下方法之一：

- **选择管理服务器检测到的网络设备**。此种情况下，任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。
- **手动指定设备地址或从列表导入地址**。您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
- **分配任务到设备分类**。此种情况下，任务被分配到先前创建的分类中的设备。您可以指定预定义分类或您所创建的自定义分类。
- **分配任务到管理组**。此种情况下，任务被分配到先前创建的管理组中的设备。

为了避免在未安装网络代理的客户端设备上安装应用程序时可能出现的问题，您必须按照通过 Kaspersky Security Center 的远程安装任务强制部署中所述进行操作。

远程安装应用程序

本节包含有关如何在管理组、具有特定 IP 地址的设备或选择的受管理设备上远程安装应用程序的信息。

要在特定设备上安装应用程序：

1. 在主菜单中，转到“**资产(设备)**”→“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。
3. 在**任务类型**字段中，选择**远程安装应用程序**。
4. 您可以选择以下选项之一：

   - **分配任务到管理组**

     任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
     例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。
     如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

   - **手动指定设备地址或从列表导入地址**

     您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
     您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - **分配任务到设备分类**

     该任务被分配到设备分类中的设备。您可以指定现有分类之一。
     例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

   *远程安装应用程序*任务为指定设备创建。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。
5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。
   可用设置取决于在上一步中选择的选项。
6. 在**安装包**步骤中，指定以下设置：

   - 在“**选择安装包**”字段中，选择要安装的应用程序的安装包。
   - 在**强制下载安装包**设置组中，指定如何将安装程序所需的文件分发到客户端设备中。

当网络上存在分发点时，选择哪个选项都无关紧要。即使管理服务器可用但分发点不可用，安装包也只会通过分发点传输。

- **使用网络代理**

  如果启用此选项，安装包通过安装在客户端设备上的网络代理传送到客户端设备。

  如果禁用此选项，则使用客户端的操作系统传送安装包。

  如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。

  默认情况下已启用该选项。

- **通过分发点使用操作系统资源**

  如果启用此选项，安装包使用操作系统工具通过分发点传送到客户端设备。如果网络中存在不止一个分发点，那么您可以选择本选项。

  如果启用"**使用网络代理**"选项，仅在网络代理工具不可用时才通过操作系统工具传送文件。

  默认情况下，已经为虚拟管理服务器上创建的远程安装任务启用此选项。

- **通过管理服务器使用操作系统资源**

  如果启用此选项，文件将使用客户端设备的操作系统工具通过管理服务器传送到客户端设备。如果客户端设备上未安装网络代理，但是客户端设备与管理服务器在同一网络，则可以启用此选项。

  默认情况下已启用该选项。

- 在**同时下载的最大数量**字段中，指定管理服务器可以同时向其传输文件的最大允许客户端设备数。
- 在**安装尝试最大数量**字段中，指定安装程序运行的最大允许次数。

  如果超过参数中指定的尝试次数，Kaspersky Security Center 将不再在设备上启动安装程序。若要重新启动*远程安装应用程序*任务，请增加**安装尝试最大数量**参数的值然后启动任务。或者，您可以创建新的"*远程安装应用程序*"任务。

- 如果您从一个卡巴斯基应用程序迁移到另一个应用程序，且当前应用程序受到密码保护，请在"**卸载当前卡巴斯基应用程序的密码**"字段中输入密码。请注意，在迁移期间，您当前的卡巴斯基应用程序将被卸载。

仅当您在**卸载当前卡巴斯基应用程序的密码**设置组中选择了**使用网络代理**选项时，**强制下载安装包**字段才可用。

当使用*远程安装应用程序*任务安装 Kaspersky Endpoint Security for Windows for Windows 时，您只能使用卸载密码来执行 Kaspersky Security for Windows Server 到 Kaspersky Endpoint Security for Windows 的迁移场景。在安装其他组件时使用卸载密码可能会导致安装错误。

要成功完成迁移方案，请确保满足以下先决条件：

- 您正在使用适用于 Windows 的 Kaspersky Security Center Network Agent 14.2 或更高版本。
- 您正在运行 Windows 的设备上安装应用程序。

- 定义附加设置：
  - **如果已经安装应用程序则不再重新安装**

    如果启用此选项，则如果选定的应用程序已安装到该客户端设备上，将不再重新安装它。

    如果禁用此选项，仍将安装应用程序。

    默认情况下已启用该选项。

  - **下载之前验证操作系统类型**

    在将文件传输到客户端设备之前，Kaspersky Security Center 将检查安装实用程序设置是否适用于客户端设备的操作系统。如果设置不适用，Kaspersky Security Center 不会传输文件，也不会尝试安装应用程序。例如，要将某个应用程序安装到某个管理组的设备（这些设备运行各种操作系统），可以将安装任务分配给管理组，然后启用此选项以跳过操作系统与所需设备不同的设备。

  - **在活动目录组策略中指定安装包的安装**

    如果启用此选项，安装包将使用 Active Directory 组策略进行安装。

    如果选择网络代理安装包，则该选项可用。

    默认情况下已禁用该选项。

  - **提示用户关闭运行中应用程序**

    运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

    如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

    如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

    默认情况下已禁用该选项。

- 选择要在哪些设备上安装应用程序：
  - **在所有设备上安装**

    应用程序将被安装到由其他管理服务器管理的设备。

    默认情况下已选中该选项。如果您在网络中只有一台管理服务器，您不必更改该设置。

  - **仅安装到通过该管理服务器管理的设备**

    应用程序将仅被安装到由该管理服务器管理的设备。如果您在网络中有多个管理服务器且需要避免它们之间的冲突，请选择该选项。

- 指定设备是否在安装后必须被移动到管理组：

  - **不移动设备**

    设备保留在当前所在组中。未被放置在任何组的设备保持未分配。

  - **移动未分配的设备到所选组 (仅可以选择单一组)**

    设备被移动到您选择的管理组。

  注意默认情况下已选择“**不移动设备**”选项。为了安全起见，您可能需要手动移动设备。

7. 在向导的这一步，指定在安装应用程序期间是否必须重新启动设备：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

默认情况下已禁用该选项。

8. 如有必要，在**选择账户以访问设备**步骤，添加将用于启动*远程安装应用程序*任务的账户：

- **不需要账户(网络代理已安装)**

  如果该选项被选中，您不是必须指定一个账户，并在该账户下运行程序的安装。将使用运行管理服务器服务的账户运行该任务。

  如果网络代理未安装在客户端设备上，该选项不可用。

- **需要账户(不使用网络代理)**

  如果您为其分配远程安装任务的设备上未安装网络代理，请选择此选项。在这种情况下，您可以指定用户账户或 SSH 证书来安装应用程序。

  - **本地账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地账户**，然后指定用户账户凭据。

    您可以指定多个用户账户，例如，没有一个账户拥有分配任务所对应的所有设备上的全部所需权限时。在此情况下，已经添加的所有账户都用于从上到下按顺序运行该任务。

  - **SSH 证书**。如果要在基于 Linux 的客户端设备上安装应用程序，您可以指定 SSH 证书而不是用户账户。单击**添加**按钮，选择**SSH 证书**，然后指定证书的私钥和公钥。

    要生成私钥，您可以使用 ssh-keygen 实用程序。请注意，Kaspersky Security Center 支持 PEM 格式的私钥，但 ssh-keygen 实用程序默认生成 OPENSSH 格式的 SSH 密钥。Kaspersky Security Center 不支持 OPENSSH 格式。要以支持的 PEM 格式创建私钥，请在 ssh-keygen 命令中添加"-m PEM"选项。例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
    ```

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

   如果启用了"**创建完成时打开任务详情**"选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。

10. 在任务列表中，选择已创建的任务，然后单击**启动**。

    或者等待任务按照您在任务设置中指定的时间表启动。

远程安装任务完成后，选定的应用程序即安装在指定设备上。

通过活动目录组策略安装应用程序

Kaspersky Security Center 允许您使用 Active Directory 组策略在受管理设备上安装 Kaspersky 应用程序。

使用 Active Directory 组策略，可以只从包含网络代理的安装包安装应用程序。

要使用 Active Directory 组策略安装应用程序：

1. 运行保护部署向导。遵照向导的说明操作。
2. 在保护部署向导的**远程安装任务设置**页面上，启用**在活动目录组策略中指定安装包的安装**。
3. 在**选择账户以访问设备**页面上，选择**需要账户(不使用网络代理)**选项。
4. 在安装了 Kaspersky Security Center 的设备上添加带有管理员权限的账户或包含在“组策略创建器所有者”域组的账户。
5. 为所选账户授予权限：
   a. 转到“**控制面板**”→“**管理工具**”，然后打开“**组策略管理**”。
   b. 单击具有所需域的节点。
   c. 单击“**委派**”区域。
   d. 在“**权限**”下拉列表中，选择“**链接 GPO**”。
   e. 单击**添加**。
   f. 在打开的“**选择用户、计算机或组**”窗口中，选择所需账户。
   g. 单击“**确定**”关闭“**选择用户、计算机或组**”窗口。
   h. 在“**组和用户**”列表中，选择刚添加的账户，然后单击“**高级**”→“**高级**”。
   i. 在“**权限条目**”列表中，双击刚添加的账户。
   j. 授予以下权限：
      - **创建组对象**
      - **删除组对象**
      - **创建组策略容器对象**
      - **删除组策略容器对象**
   k. 单击“**确定**”保存更改。
6. 按照向导的说明定义其他设置。
7. 手动运行创建的远程安装任务，或等待计划启动。

这将启动以下远程安装序列：

1. 任务运行时，系统将在包含指定集合中的客户端设备的每个域中创建以下对象：
   - 名称 **Kaspersky_AK{GUID}** 下的组策略对象（GPO）。
   - 对应于 GPO 的安全组。此安全组包括该任务涵盖的客户端设备。安全组的内容定义了 GPO 的范围。

2. Kaspersky Security Center 直接从应用程序的名为“KLSHARE”的共享网络文件夹在客户端设备上安装所选 Kaspersky 应用程序。在 Kaspersky Security Center 安装文件夹中，系统将创建一个辅助子文件夹，其中包含安装应用程序所需的 .msi 文件。

3. 新设备添加到任务范围后，会在任务下次启动后添加到安全组。如果在任务计划中选中“**运行错过的任务**”选项，则设备将立即添加到安全组。

4. 设备从任务范围中删除后，会在任务下次启动后从安全组中删除。

5. 从 Active Directory 中删除任务后，GPO、GPO 的链接和相应的安全组也会删除。

如果要使用 Active Directory 应用其他安装方案，您可以手动配置所需设置。例如，以下情况可能需要该操作：

- 当反病毒保护管理员没有权限更改某些域的活动目录时
- 原始安装包必须存储在单独的网络资源上时
- 当需要将 GPO 链接到特定的活动目录单元时

通过活动目录使用备用安装方案的以下选项可用：

- 如果直接从 Kaspersky Security Center 共享文件夹进行安装，您必须在 GPO 属性中为所需应用程序指定 .msi 文件（位于安装包的 exec 子文件夹中）。
- 如果必须将安装包放置在其他网络资源上，您必须将整个 exec 文件夹的内容复制过去，因为除了扩展名为 .msi 的文件外，该文件夹还包含创建安装包时生成的配置文件。要安装与该程序相关联的授权许可密钥，请将许可文件一起复制到该文件夹中。

在从属管理服务器上安装应用程序

要在从属管理服务器上安装应用程序：

1. 与控制相关从属管理服务器的管理服务器建立连接。

2. 确保每个所选的从属管理服务器上都有与要安装的应用程序对应的安装包。如果在任何从属服务器上都找不到安装包，请分发它。为此，创建一个任务类型为**分发安装包**任务。

3. 创建在从属管理服务器上远程安装应用程序的任务。选择**将应用程序远程安装到从属管理服务器**任务类型。

   “新任务向导”将创建一个任务，用于在特定从属管理服务器上远程安装向导中选择的应用程序。

4. 手动运行该任务，或者按照任务设置中指定的计划等待任务启动。

远程安装任务完成后，选定的应用程序即安装在从属管理服务器上。

指定 Unix 设备上的远程安装设置

使用远程安装任务在 Unix 设备上安装应用程序时，可以为该任务指定 Unix 特定的设置。创建任务后，这些设置在任务属性中可用。

要为远程安装任务指定 Unix 特定的设置：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击要为其指定 Unix 特定设置的远程安装任务的名称。
   任务属性窗口打开。
3. 转到“**应用程序设置**”→“**Unix 特定的设置**”。
4. 指定下列设置：
   - **为根账户设置密码(仅对通过 SSH 的部署)**

     如果在目标设备上不指定密码就无法使用 sudo 命令，则选择此选项，然后指定 root 账户的密码。Kaspersky Security Center 会将密码以加密形式传输到目标设备，解密密码，然后以具有指定密码的 root 账户的身份启动安装过程。

     Kaspersky Security Center 不会使用该账户或指定的密码创建 SSH 连接。
   - **指定目标设备上具有执行权限的临时文件夹的路径(仅对通过 SSH 的部署)**

     如果目标设备上的 /tmp 目录没有执行权限，则选择此选项，然后指定具有执行权限的目录路径。Kaspersky Security Center 使用指定的目录作为通过 SSH 进行访问的临时目录。应用程序会将安装包放在该目录中并运行安装过程。
5. 单击“**保存**”按钮。

指定的任务设置即被保存。

启动和停止卡巴斯基应用程序

您可以使用*启动或停止应用程序*任务在受管设备上启动和停止卡巴斯基应用程序。

要创建启动或停止应用程序任务：

1. 在主菜单中，转到“**资产(设备)**” →“**任务**”。
2. 单击**添加**。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
3. 在**应用程序**下拉列表中，选择要为其建立任务的应用程序。
   如果您之前已为这些应用程序添加了管理 Web 插件，则卡巴斯基应用程序将显示在列表中。
4. 在**任务类型**列表中选择**应用程序激活**任务。
5. 在**任务名称**字段中，指定新任务的名称。
   任务名称不能超过 100 个字符并且不能包括任何特殊字符 ("*<>?\:|)。
6. 选择要将任务分配到的设备。

7. 在“**应用程序**”窗口中，执行以下操作：

   - 选中要为其创建任务的应用程序名称旁边的复选框。
   - 选择**启动应用程序**或**停止应用程序**选项。

8. 如果要修改默认任务设置，请启用“**创建完成时打开任务详情**”步骤的“**完成任务创建**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

9. 单击“**完成**”按钮。

   任务被创建并显示在任务列表。

10. 点击创建的任务的名称以打开任务属性窗口。

11. 在任务属性窗口中，根据需要指定常规任务设置，然后保存设置。

    任务被创建和配置。

要运行任务，请在任务列表中选择它，然后单击“**开始**”按钮。

移动设备管理

通过 Kaspersky Security Center 的移动设备保护的管理通过使用移动设备管理功能运行，这需要专用授权许可。如果您要管理组织员工拥有的移动设备，请启用和配置移动设备管理。

移动设备管理可让您管理员工的 Android 设备。保护由设备上安装的 Kaspersky Endpoint Security for Android 移动应用程序提供。此移动应用程序可确保保护移动设备免受 Web 威胁、病毒和其他构成威胁的程序的侵害。要通过 Kaspersky Security Center Web Console 进行集中管理，您必须在安装了 Kaspersky Security Center Web Console 的设备上安装以下 Web 管理插件：

- Kaspersky Security for Mobile 插件
- Kaspersky Endpoint Security for Android 插件

有关移动设备的保护部署和管理的信息，请参阅 Kaspersky Security for Mobile 帮助。

在 Kaspersky Security Center Web Console 中修改移动设备管理设置

要修改移动设备管理设置：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**附加端口**”区域。

3. 修改相关设置：

   - **为移动设备打开端口**

     如果启用该切换开关，则将在管理服务器上打开移动设备端口。

     仅在已安装移动设备管理组件时才可以使用移动设备端口。

如果未启用该切换开关，则管理服务器上的移动设备端口将不被使用。
默认情况下已禁用该切换开关。

- **移动设备同步端口**

  用于连接移动设备到管理服务器的端口号。默认端口号是 13292。
  使用十进制系统记录。

- **移动设备激活端口**

  用于将 Kaspersky Endpoint Security for Android 连接到 Kaspersky 激活服务器的端口。
  默认端口号是 17100。

4. 单击“**保存**”按钮。

移动设备现在可以连接到管理服务器。

替换第三方安全应用程序

通过 Kaspersky Security Center 进行 Kaspersky 安全应用程序的安装可能需要卸载与正在安装的应用程序不兼容的第三方软件。Kaspersky Security Center 提供几种卸载第三方应用程序的方法。

通过使用安装程序卸载不兼容应用程序

该选项仅在基于 Microsoft 管理控制台的管理控制台可用。

卸载不兼容应用程序的安装程序方法被各种应用程序支持。如果在该安全应用程序安装包的属性窗口中选中了（“**不兼容的应用程序**”区域）“**自动卸载不兼容的应用程序**”选项，在安全应用程序安装之前，所有不兼容的应用程序被自动卸载。

当配置应用程序远程安装时卸载不兼容应用程序

您可以在配置安全应用程序远程安装时启用“**自动卸载不兼容的应用程序**”选项。在基于 Microsoft Management Console（MMC） 的管理控制台，该选项在远程安装向导可用。在 Kaspersky Security Center Web Console，您可以在保护部署向导中找到该选项。当该选项被启用时，Kaspersky Security Center 在安装安全应用程序到受管理设备之前卸载不兼容的应用程序。

说明：

- 管理控制台：使用远程安装向导移除不兼容的应用程序
- Kaspersky Security Center Web Console：安装前卸载不兼容的应用程序

通过专用任务卸载不兼容的应用程序

要卸载不兼容的应用程序，使用**远程卸载应用程序**任务。该任务应该在安全应用程序安装任务运行之前运行在设备。例如，在安装任务中，您可以选择计划类型"**在完成其他任务时**"，这里，其他任务就是"**远程卸载应用程序**"。

该卸载方法在安全应用程序无法正确卸载不兼容应用程序时是很有用的。

管理控制台操作说明：创建任务。

发现网络设备

该部分描述网络设备的搜索和发现。

Kaspersky Security Center 允许您按照指定规则查找设备。您可以保存搜索结果到文本文件。

搜索和发现功能允许您查找以下设备：

- Kaspersky Security Center 管理服务器及其从属管理服务器的管理组中的受管理设备。
- 由 Kaspersky Security Center 管理服务器及其从属管理服务器管理的未分配设备。

情景：发现网络设备

您必须在安装安全应用程序之前执行设备发现。管理服务器可接收已发现设备的信息，并允许您通过策略管理这些设备。需要定期进行网络轮询以更新网络中可用设备的列表。

在开始网络轮询之前，请确保已启用 SMB 协议。否则，Kaspersky Security Center 无法发现轮询网络中的设备。要启用 SMB 协议，请按照适用于您的操作系统的说明进行操作。

发现网络设备按以下阶段进行：

1. **发现设备**

   快速启动向导通过初始设备发现指引您，并帮助您查找网络设备，例如计算机、平板电脑和移动电话。您也可以手动执行设备发现。

2. **配置计划轮询**

   决定您要定期使用哪些轮询类型。启用所需的类型并配置轮询计划。您可以参考网络轮询频率建议。

3. **设置规则以添加发现的设备到管理组（可选）**

   如果新设备出现在您的网络中，则它们将在定期轮询期间被发现，并自动包含在"**未分配的设备**"组中。您可以设置设备移动规则以自动分配设备到**受管理设备**组。您也可以配置保留规则。

   如果您跳过第 3 步，新发现的设备将分配给**未分配的设备**组。如果需要，可以手动将这些设备移动到"**受管理设备**"组。如果您手动将这些设备移动到"**受管理设备**"组，您可以分析每台设备的信息并决定您是否要将它移动到管理组以及移动到具体哪个组。

结果

完成方案可以导致如下：

- Kaspersky Security Center 管理服务器发现网络中的设备并提供您它们的信息。
- 未来轮询被设置并根据指定的计划工作。
- 新发现的设备按照配置的规则排列。（或者，如果没有配置规则，设备将保留在**未分配的设备**组中）。

设备发现

该部分描述了 Kaspersky Security Center 中可用的设备发现类型并给出使用每种类型的信息。

管理服务器通过常规轮询接收网络结构信息和网络设备信息。信息被记录到管理服务器数据库。管理服务器可使用下列类型的轮询：

- **Windows 网络轮询**。管理服务器可以执行两种 Windows 网络轮询：快速和完整。在快速轮询过程中，管理服务器只从所有网络域和工作组中设备的 NetBIOS 名称列表检索信息。在完整轮询中，需要每台客户端设备的跟多信息，例如操作系统名称、IP 地址、DNS 名称和 NetBIOS 名称。默认下，快速和完整轮询都被启用。Windows 网络轮询可能发现设备失败，例如，如果端口 UDP 137、UDP 138、TCP 139 在路由器上或被防火墙关闭。
- **域控制器轮询**。管理服务器或分发点可检索有关域结构以及域中包含的设备的 DNS 名称的信息。默认情况下已启用该轮询类型。如果所有联网设备都是域的成员，我们建议您使用域控制器轮询。如果某些联网设备未包含在域中，则域控制器轮询无法发现这些设备。
- **IP 范围轮询**。管理服务器使用 ICMP 包或 NBNS 协议轮询指定的 IP 范围，并编制一组完整的关于这些 IP 范围内的设备的数据。默认情况下已禁用该轮询类型。如果您使用 Windows 网络轮询和/或活动目录轮询，不建议您使用该轮询类型。
- **Zeroconf 轮询**。使用零配置网络（也称为 *Zeroconf*）轮询 IPv6 网络的分发点。默认情况下已禁用该轮询类型。如果分发点运行 Linux，则可以使用 Zeroconf 轮询。

如果设置并启用了设备移动规则，则新发现的设备将自动包含在“**受管理设备**”组中。如果未启用移动规则，新发现的设备将自动包含在“**未分配的设备**”组。

您可以为每种类型修改设备发现设置。例如，您可能想要修改轮询计划或者设置是否轮询整个域森林还是仅指定域。

在开始网络轮询之前，请确保已启用 SMB 协议。否则，Kaspersky Security Center 无法发现轮询网络中的设备。要启用 SMB 协议，请按照适用于您的操作系统的说明进行操作。

Windows 网络轮询

关于 Windows 网络轮询

在快速轮询过程中，管理服务器只从所有网络域和工作组中设备的 NetBIOS 名称列表检索信息。在完整轮询中，以下信息被从每个客户端设备请求：

- 操作系统名称
- IP 地址
- DNS 名称
- NetBIOS 名称

快速轮询和完整轮询都需要以下：

- 端口 UDP 137/138、TCP 139、UDP 445、TCP 445、必须在网络中可用。
- SMB 协议已启用。
- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在管理服务器上启用。
- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在客户端设备上启用：
  - 至少一台设备上，如果网络设备数量不超过 32。
  - 对每 32 台网络设备至少一台设备上。

完整轮询仅在快速轮询至少运行了一次时可以运行。

查看和修改 Windows 网络轮询设置

要修改 Windows 网络轮询属性：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**Windows 域**”。
2. 单击“**属性**”按钮。
   Windows 域属性窗口将开启。
3. 通过使用“**启用 Windows 网络轮询**”切换按钮启用或禁用 Windows 网络轮询。
4. 配置轮询计划。默认下，快速轮询每 15 分钟运行一次，完整轮询每 60 分钟运行一次。
   轮询计划选项：
   - **每 N 天**

     轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。

默认下，轮询每天运行一次，从当前系统日期和时间开始。

- **每 N 分钟**

  轮询定期运行，按照指定分钟间隔，从指定的时间开始。

- **按星期中的天数**

  轮询定期运行，在指定星期的指定时间。

- **每个月在所选周的指定天**

  轮询定期运行，在指定月日的指定时间。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已禁用该选项。

5. 保存 Windows 网络轮询的属性。

   属性被保存并应用到所有发现的 Windows 域和工作组。

手动运行轮询

要立即运行轮询，

单击“**开始快速轮询**”或“**开始完整轮询**”。

轮询完成后，您可以通过选中域名旁边的复选框，然后单击“**设备**”按钮，在“**Windows 域**”页面查看发现的设备列表。

IP 范围轮询

开始，Kaspersky Security Center 从其所在设备的网络设置获取 IP 轮询范围。如果设备地址是 192.168.0.1 且子网掩码是 255.255.255.0，Kaspersky Security Center 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center 从 192.168.0.1 到 192.168.0.254 之间轮询所有地址。

对于 Microsoft Active Directory 或 Samba 域控制器内的所有基于 Linux 的主机，请在`/etc/samba/smb.conf`文件中指定`netbios name` 和 `workgroup`参数。否则，轮询结果可能包含重复的主机。

Kaspersky Security Center 可以通过反向 DNS 查找或使用 NBNS 协议轮询 IP 范围：

- **反向 DNS 查找**

Kaspersky Security Center 尝试使用标准 DNS 请求为指定范围的每个 IP 地址执行反向名称解析到 DNS 名称。如果该操作成功，服务器发送 `ICMP ECHO REQUEST`（和 ping 命令相同）到所接收名称。如果设备响应，其信息被添加到 Kaspersky Security Center 数据库。反向名称解析对于排除具有 IP 地址但不是计算机的网络设备是必要的，例如网络打印机或路由器。

该轮询方法依赖正确配置的本地 DNS 服务。它必须具有反向查询域。在使用活动目录的网络中，此类域被自动维护。但是在这些网络中，IP 子网轮询不比活动目录轮询提供更多信息。而且，小网络的管理员经常不配置反向查询区，因为它对许多网络服务来说是不必要的。由于所有这些原因，IP 子网轮询默认被禁用。

- **NBNS 协议**

  如果由于某种原因无法在您的网络中进行反向名称解析，Kaspersky Security Center 将使用 NBNS 协议轮询 IP 地址范围。如果对某个 IP 地址的请求返回 NetBIOS 名称，则有关此设备的信息将添加到 Kaspersky Security Center 数据库。

在开始网络轮询之前，请确保已启用 SMB 协议。否则，Kaspersky Security Center 无法发现轮询网络中的设备。要启用 SMB 协议，请按照适用于您的操作系统的说明进行操作。

浏览和修改 IP 范围轮询设置

要浏览和修改 IP 范围轮询设置：

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**IP 范围**”。
2. 单击“**属性**”按钮。

   IP 轮询属性窗口将开启。
3. 通过使用“**允许轮询**”切换按钮启用或禁用 IP 轮询。
4. 配置轮询计划。默认下，IP 轮询每 420 分钟（七小时）运行一次。

   当指定轮询间隔时，确保该设置不超过 IP 地址生命周期参数值。如果 IP 地址在 IP 地址生命周期中不被轮询所验证，该 IP 地址被从轮询结果中自动删除。默认下，轮询结果的生命期是 24 小时，因为动态 IP 地址（使用 Dynamic Host Configuration Protocol (DHCP)）分配每 24 小时更改一次。

   轮询计划选项：

   - **每 N 天**

     轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。

     默认下，轮询每天运行一次，从当前系统日期和时间开始。

   - **每 N 分钟**

     轮询定期运行，按照指定分钟间隔，从指定的时间开始。

   - **按星期中的天数**

     轮询定期运行，在指定星期的指定时间。

- **每个月在所选周的指定天**

  轮询定期运行，在指定月日的指定时间。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。

  如果启用该选项，管理服务器在它切换回来后立即启动轮询。

  如果禁用该选项，管理服务器等待下一次计划轮询。

  默认情况下已禁用该选项。

5. 单击“**保存**”按钮。

   属性包保存并应用到所有 IP 范围。

手动运行轮询

要立即运行轮询，

单击“**开始轮询**”。

添加和修改 IP 范围

开始，Kaspersky Security Center 从其所在设备的网络设置获取 IP 轮询范围。如果设备地址是 192.168.0.1 且子网掩码是 255.255.255.0，Kaspersky Security Center 自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center 从 192.168.0.1 到 192.168.0.254 之间轮询所有地址。您可以修改自动定义的 IP 范围或添加自定义 IP 范围。

您只能创建 IPv4 地址范围。如果启用 Zeroconf 轮询，Kaspersky Security Center 将轮询整个网络。

要添加新 IP 范围：

1. 在主菜单中，转到“**发现和部署**” →“**发现**”→“**IP 范围**”。
2. 要添加新 IP 范围，请单击“**添加**”按钮。
3. 在打开的窗口，指定以下设置：

- **IP 范围名称**

  IP 范围名称。您可能想指定 IP 范围本身作为名称，例如，"192.168.0.0/24"。

- **IP 间隔或子网地址和掩码**

  通过指定开始和结束地址或子网地址和子网掩码设置 IP 范围。您也可以通过点击“**浏览**”按钮选择现有 IP 范围之一。

- **IP 地址生命周期(小时)**

  当指定该参数时，确保它超过轮询计划中设置的轮询间隔。如果 IP 地址在 IP 地址生命周期中不被轮询所验证，该 IP 地址被从轮询结果中自动删除。默认下，轮询结果的生命期是 24 小时，因为动态 IP 地址（使用 Dynamic Host Configuration Protocol (DHCP)）分配每 24 小时更改一次。

4. 如果要轮询已添加的子网或区间，则选择“**启用 IP 范围轮询**”。否则，您添加的子网或间隔将不被轮询。

5. 单击“**保存**”按钮。

新 IP 范围被添加到 IP 范围列表。

您可以使用“**开始轮询**”按钮分别对每个 IP 范围运行轮询。轮询完成后，可以使用“**设备**”按钮查看发现的设备列表。默认下，轮询结果的寿命是 24 小时，且等于 IP 地址生命周期设置。

要添加子网到现有 IP 范围：

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**IP 范围**”。

2. 点击您要添加到子网的 IP 范围名称。

3. 在打开的窗口中，单击“**添加**”按钮。

4. 通过使用地址或者掩码指定子网，或者通过使用 IP 范围中的第一个和最后一个 IP 地址。或者，单击“**浏览**”按钮来添加一个现有子网。

5. 单击“**保存**”按钮。

   新子网被添加到 IP 范围。

6. 单击“**保存**”按钮。

IP 范围的新设置被保存。

您可以添加无限多的子网。命名 IP 范围不被允许重叠，IP 范围中的非命名子网没有此限制。您可以对每个 IP 范围独立启用和禁用轮询。

Zeroconf 轮询

只有基于 Linux 的分发点支持此轮询类型。

分发点可以轮询具有 IPv6 地址的设备的网络。在这种情况下，不指定 IP 范围，并且分发点使用零配置网络（称为 *Zeroconf*）轮询整个网络。要开始使用 Zeroconf，您必须在分发点上安装 avahi-browse 实用程序。

要启用 IPv6 网络轮询：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**IP 范围**”。

2. 单击“**属性**”按钮。

3. 在打开的窗口中，打开“**使用 Zeroconf 轮询 IPv6 网络**”切换按钮。

之后，分发点开始轮询您的网络。在这种情况下，指定的 IP 范围将被忽略。

域控制器轮询

Kaspersky Security Center 支持轮询 Microsoft Active Directory 域控制器和 Samba 域控制器。

Kaspersky Security Center 仅允许您使用 Linux 分发点轮询 Samba 域控制器。对于 Samba 域控制器，Samba 4 用作 Active Directory 域控制器。

当您轮询域控制器时，管理服务器或分发点会检索有关域中包含的设备的域结构、用户账户、安全组和 DNS 名称的信息。

如果所有联网设备都是域的成员，我们建议使用域控制器轮询。如果某些联网设备未包含在域中，则域控制器轮询无法发现这些设备。

先决条件

轮询域控制器之前，请确保允许通过防火墙或代理服务器连接到域控制器。还要确保域控制器上启用了以下协议：

- 轻量级目录访问协议 (LDAP)
- 简单身份验证和安全层 (SASL)

  如果使用 SASL 身份验证建立与域控制器的连接，则使用此协议。管理服务器和分发点仅支持 DIGEST-MD5 机制。
- 安全套接字层上的轻量级目录访问协议 (LDAPS)

  如果您需要通过加密连接来连接到域控制器，则使用此协议。

确保域控制器设备上的以下端口可用：

- 389 表示 LDAP 协议和简单身份验证（包括 SASL）
- 636 表示 LDAPS 协议

对于 Microsoft Active Directory 或 Samba 域控制器内的所有基于 Linux 的主机，您必须在 `/etc/samba/smb.conf` 文件中指定 `netbios name` 和 `workgroup` 参数。否则，轮询结果可能包含重复的主机。

如果 Microsoft Active Directory 域包含多个域控制器，则不支持在域轮询期间选择特定控制器。将与检测到的第一个域控制器建立连接。为确保与 Microsoft Active Directory 域进行正确的身份验证，证书的“使用者备用名称 (SAN)”字段必须包含此域中包含的所有域控制器的地址，以及 Microsoft Active Directory 域的 NetBIOS 名称。

使用管理服务器进行域控制器轮询

您使用管理服务器仅可轮询 Microsoft Active Directory 域控制器。

要使用管理服务器轮询域控制器：

1. 在主菜单中，转到“**发现和部署**” → “**发现**” → “**域控制器**”。
2. 单击**轮询设置**。
   域控制器轮询设置窗口将打开。
3. 选择**启用域控制器轮询**选项。
4. 在**高级设置**部分中，指定轮询范围：
   - **轮询当前域**
     选择此选项可以轮询 Kaspersky Security Center 所属的域。
   - **轮询整个域森林**
     选择此选项可以轮询 Kaspersky Security Center 所属的域森林。
   - **轮询指定域**
     选择此选项可以轮询具有指定地址和用户凭据的域。
5. 如果必要，指定轮询计划：默认间隔是一小时。下次轮询接收的数据会完全替换旧数据。
   有以下轮询计划选项可用：
   - **每 N 天**

     轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
     默认下，轮询每天运行一次，从当前系统日期和时间开始。
   - **每 N 分钟**

     轮询定期运行，按照指定分钟间隔，从指定的时间开始。
   - **按星期中的天数**

     轮询定期运行，在指定星期的指定时间。
   - **每个月在所选周的指定天**

     轮询定期运行，在指定月日的指定时间。
   - **运行错过的任务**

     如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。
     如果启用该选项，管理服务器在它切换回来后立即启动轮询。
     如果禁用该选项，管理服务器等待下一次计划轮询。
     默认情况下已禁用该选项。

如果您更改域安全组中的用户账户，这些更改将在您轮询域控制器一小时后显示在 Kaspersky Security Center 中。

6. 单击**保存**以应用更改。

7. 如果您要立即执行轮询，请单击“**开始轮询**”按钮。

使用分发点进行域控制器轮询

您还可以使用分发点轮询 Microsoft Active Directory 域控制器和 Samba 域控制器。基于 Windows 或 Linux 的受管理设备可以充当分发点。

对于 Linux 分发点，支持对 Microsoft Active Directory 域控制器和 Samba 域控制器进行轮询。
对于 Windows 分发点，仅支持 Microsoft Active Directory 域控制器的轮询。
使用 Mac 分发点进行轮询不受支持。

要使用分发点配置域控制器轮询：

1. 打开分发点属性。

2. 选择**域控制器轮询**部分。

3. 选择**启用域控制器轮询**选项。

4. 选择要轮询的域控制器。
   如果您使用 Linux 分发点，请在“**轮询指定域**”部分中单击“**添加**”，然后指定域控制器的地址和用户凭据。
   如果您使用 Windows 分发点，则可以选择以下选项之一：

   - **轮询当前域**
   - **轮询整个域森林**
   - **轮询指定域**

5. 如果需要，单击“**设置轮询计划**”按钮以指定轮询计划选项。
   轮询仅根据指定的时间表开始。无法手动启动轮询。

轮询完成后，域结构将显示在**域控制器**部分。

如果设置并启用了设备移动规则，则新发现的设备将自动包含在“**受管理设备**”组中。如果未启用移动规则，新发现的设备将自动包含在“**未分配的设备**”组。

发现的用户账户可用于Kaspersky Security Center Web Console 中的域身份验证。

身份验证和连接到域控制器

轮询域时进行身份验证并连接到域控制器

当使用 Linux 分发点轮询域控制器时，分发点识别连接协议以建立与域控制器的初始连接。该协议用于将来与域控制器的所有连接。在建立与域控制器的初始连接时，您可以使用网络代理标志（KLNAG_LDAP_TLS_REQCERT 和 KLNAG_LDAP_SSL_CACERT）来更改连接选项。您可以按照本文所述使用 klscflag 配置网络代理标志。

与域控制器的初始连接过程如下：

1. Linux 分发点尝试通过 LDAPS 连接到域控制器。

   默认情况下不需要证书验证。将 KLNAG_LDAP_TLS_REQCERT 标记设置为 1 以强制执行证书验证。

   KLNAG_LDAP_TLS_REQCERT 标记的可能值：

   - 0—已请求证书，但如果未提供证书或证书验证失败，则 TLS 连接仍被视为成功创建（默认值）。
   - 1—需要严格验证 LDAP 服务器证书。

   默认情况下，如果未指定 KLNAG_LDAP_SSL_CACERT 标志，则使用与操作系统相关的证书颁发机构 (CA) 的路径来访问证书链。使用 KLNAG_LDAP_SSL_CACERT 标志指定自定义路径。

2. 如果 LDAPS 连接失败，Linux 分发点将尝试使用 SASL (DIGEST-MD5) 通过非加密的 TCP 连接来连接到域控制器。

配置标记

您可以使用 klscflag 实用程序来配置标志。

在 Linux 分发点上，运行命令行，然后将当前目录更改为包含 klscflag 实用程序的目录。默认情况下，在 Linux 分发点上，klscflag 实用程序位于 /opt/kaspersky/ksc64/sbin 中。

例如，以下命令强制执行证书验证：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

配置 Samba 域控制器

Kaspersky Security Center 支持仅在 Samba 4 上运行的 Linux 域控制器。

Samba 域控制器支持与 Microsoft Active Directory 域控制器相同的架构扩展。您可以使用 Samba 4 架构扩展启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这是一个可选操作。

我们建议启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容。这将确保 Kaspersky Security Center 和 Samba 域控制器之间的正确交互。

要启用 Samba 域控制器与 Microsoft Active Directory 域控制器完全兼容：

1. 执行以下命令以使用 RFC2307 架构扩展：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. 在 Samba 域控制器中启用架构更新。为此，请将以下行添加到 `/etc/samba/smb.conf` 文件中：

   ```
   dsdb:schema update allowed = true
   ```

   > 如果架构更新完成时出现错误，则需要对充当架构主机的域控制器执行完整还原。

对于 Samba 域控制器内的所有基于 Linux 的主机，在 `/etc/samba/smb.conf` 文件中指定 `netbios name` 和 `workgroup` 参数。否则，轮询结果可能包含重复的主机。

为未分配的设备配置保留规则

Windows 网络轮询完成后，发现的设备被放置到“未分配的设备”管理组的子组。该管理组可以在“**发现和部署**”→“**发现**”→“**Windows 域**”中找到。“**Windows 域**”文件夹是父组。它包含以对应域为名称的子组和在轮询过程中发现的工作组。父组可能也包含移动设备管理组。您可以为父组和每个子组配置未分配的设备的保留规则。保留规则不取决于设备发现设置并在设备发现被禁用时也工作。

设备保留规则不会影响具有一个或多个使用完整磁盘加密进行加密的驱动器的设备。此类设备不会被自动删除——您只能手动删除它们。如果您需要删除带有加密驱动器的设备，请先解密驱动器，然后再删除该设备。

要为未分配的设备配置保留规则：

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**Windows 域**”。
2. 执行以下操作之一：
   - 要配置父组的设置，请单击“**属性**”按钮。
     Windows 域属性窗口将开启。
   - 要配置子组设置，点击其名称。
     子组属性窗口将开启。
3. 定义下列设置：
   - **当设备处于非活动状态超过指定天数时，从组中删除设备**

     如果启用该选项，您可以指定设备被从组中自动移除的时间间隔。默认下，该选项也被分发到子组。默认时间间隔是 7 天。
     默认情况下已启用该选项。
   - **从父组继承**

     如果启用该选项，设备在当前组的保留期从父组继承且无法被更改。
     该选项仅对子组可用。
     默认情况下已启用该选项。

- **强制子组继承**

  该设置值将被分发到子组，但在子组的属性中这些设置被锁定。
  默认情况下已禁用该选项。

4. 单击“**接受**”按钮。

您的更改已保存并应用。

设备清单

用于清查设备的硬件清单（**操作 → 存储库 → 硬件**）以两种方式填充：自动和手动。每次网络轮询后，所有检测到的设备都会自动添加到列表中；但是，如果您不希望轮询网络，也可以手动添加设备。您可以手动将其他设备添加到列表中，例如路由器、打印机或设备硬件。

您可以在设备的属性中查看并编辑有关该设备的详细信息。

硬件列表可能包含以下类型的设备：

- 计算机
- 移动设备
- 网络设备
- 虚拟设备
- OEM 组件
- 计算机周边设备
- 已连接设备
- VoIP 电话
- 网络存储库

管理员可以将“*企业设备*”属性分配给所检测到的设备。管理员可以在设备的属性中手动分配该属性，或者指定自动分配该属性的条件。在这种情况下，系统将按设备类型分配“*企业设备*”属性。

Kaspersky Security Center 允许注销设备。为此，请在设备属性中选择“**写入**”选项。此类设备不会显示在设备列表中。

管理员可以在“**硬件**”文件夹管理可编程逻辑控制器 (PLC) 的列表。管理 PLC 列表的详细信息提供在 *Kaspersky Industrial CyberSecurity for Nodes 用户指南*。

添加有关新设备的信息

若要添加网络中新设备的信息，请执行以下操作：

1. 在主菜单中，转到**操作 → 存储库 → 硬件**。
2. 单击**添加**按钮打开**新设备**窗口。
3. 在“**新设备**”窗口中，从“**设备类型**”下拉列表中选择您要添加的设备类型。
4. 单击“**确定**”。
   此时将打开设备属性窗口，显示“**常规**”区域。
5. 在“**常规**”区域中使用设备数据填写输入字段。“**常规**”区域将显示以下设置：
   - **企业设备**。如果您希望将“*企业*”属性分配给该设备，请选择该选框。您可以使用该属性搜索“**硬件**”文件夹中的设备。
   - **写入**。如果您不希望该设备显示在“**硬件**”文件夹中的设备列表中，请选中该复选框。
6. 单击“**应用**”。

新设备将显示在“**硬件**”页面的工作区中。

配置用于定义企业设备的标准

若要配置企业设备的检测标准，请执行以下操作：

1. 在主菜单中，转到**操作 → 存储库 → 硬件**。
2. 在**硬件**页面顶部，单击**设置企业设备规则**链接。
   设置企业设备规则面板被调用。
3. 在**设置企业设备规则**面板中，启用**为设备自动设置 “企业” 属性**。指定为其自动分配*企业*属性的设备类型。

   此选项仅影响通过网络轮询添加的设备。对于手动添加的设备，请手动设置“*企业*”属性。

4. 单击“**确定**”。

企业设备的检测标准得到配置。

Kaspersky 应用程序：授权许可和激活

此部分描述了使用受管理 Kaspersky 应用程序的授权许可密钥时相关的 Kaspersky Security Center 功能。

Kaspersky Security Center 使您可以集中为客户端设备上的 Kaspersky 应用程序分发授权许可密钥、监控其使用情况，以及续订授权许可。

使用 Kaspersky Security Center 添加授权许可密钥时，该密钥的设置会保存在管理服务器上。应用程序会根据该信息生成一份授权许可密钥使用情况的报告，并通知管理员密钥属性中指定的授权许可期满日期，以及是否违反此限制。您可以在管理服务器设置内配置授权许可密钥使用情况的通知。

受管理应用程序的授权许可

安装到受管理设备上的 Kaspersky 应用程序必须通过将密钥文件或激活码应用到每个应用程序来获得授权。密钥文件或激活码可以按以下方法部署：

- 自动部署
- 受管理应用程序安装包
- 受管理应用程序的“*添加授权许可密钥*”任务
- 受管理应用程序的手动激活

您可以通过上面列出的任何方法添加新的活动或备用授权许可密钥。卡巴斯基应用程序当前使用一个活动密钥并存储一个备用密钥以在活动密钥到期后应用。您为其添加授权许可密钥的应用程序可定义密钥是活动密钥还是备用密钥。密钥定义不依赖于您用于添加新授权许可密钥的方法。

自动部署

如果您使用不同的受管理应用程序，且您必须将特定密钥文件或激活码部署到设备，请选择其他方法部署激活码或密钥文件。

Kaspersky Security Center 允许您自动部署可用授权许可密钥到设备。例如，三个授权许可密钥被存储在管理服务器存储库。您已为所有三个授权许可密钥选择了“**自动分发授权许可密钥到受管理设备**”复选框。Kaspersky 安全应用程序—例如，Kaspersky Endpoint Security for Windows— 被安装到组织设备。发现必须部署授权许可密钥的新设备。应用程序决定，例如，存储库中的两个授权许可密钥可以被部署到设备：授权许可密钥 *Key_1*和授权许可密钥 *Key_2*。这些授权许可密钥之一被部署到设备。此种情况下，无法预见两个授权许可密钥中的哪个将被部署到设备，因为自动部署授权许可密钥不提供给任何管理员活动。

当部署授权许可密钥时，设备为该授权许可密钥重新计算。您必须确保部署授权许可密钥的设备数量不超过授权许可限制。如果设备数量超过授权许可限制，所有不被授权许可覆盖的设备将被分配*严重*状态。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 管理控制台：
  - 添加授权许可密钥到管理服务器存储库
  - 自动分发授权许可密钥

  或

- Kaspersky Security Center Web Console：
  - 添加授权许可密钥到管理服务器存储库
  - 自动分发授权许可密钥

请注意，在以下情况下，自动分发的授权许可密钥可能不会显示在虚拟管理服务器存储库中：

- 授权许可密钥对于应用程序无效。
- 虚拟管理服务器没有受管理设备。
- 授权许可密钥已用于由另一个虚拟管理服务器管理的设备，并且已达到设备数量限制。

添加密钥文件或激活码到受管理应用程序安装包

对于安全应用程序，该选项不被推荐。添加到安装包的密钥文件或激活码可能被盗用。

如果您使用安装包安装受管理应用程序，您可以在该安装包中或在应用程序策略中指定激活码或密钥文件。授权许可密钥将在下一次设备与管理服务器同步时被部署到受管理应用程序。

说明：

- 管理控制台：
  - 创建安装包
  - 安装应用程序到客户端设备

  或
- Kaspersky Security Center Web Console：添加授权许可密钥到安装包

通过为受管理应用程序添加授权许可密钥任务来进行部署

如果您选择使用为受管理应用程序*添加授权许可密钥*任务，您可以选择要部署到设备的授权许可密钥并以任何便捷的方法选择设备–例如，通过选择管理组或设备分类。

部署之前，密钥文件或激活码必须添加到管理服务器存储库。

说明：

- 管理控制台：
  - 添加授权许可密钥到管理服务器存储库
  - 部署授权许可密钥到客户端设备

  或

- Kaspersky Security Center Web Console：
  - 添加授权许可密钥到管理服务器存储库
  - 部署授权许可密钥到客户端设备

手动添加激活码或密钥文件到设备

您可以激活本地安装的 Kaspersky 应用程序，通过使用应用程序界面提供的工具。请参考已安装应用程序的文档。

添加授权许可密钥到管理服务器存储库

要添加授权许可密钥到管理服务器存储库：

1. 在主菜单中，转到“**操作**”→“**授权许可**”→“**卡巴斯基授权许可**”。
2. 单击“**添加**”按钮。
3. 选择您要添加的内容：
   - **添加密钥文件**
     单击“**选择密钥文件**”按钮并浏览到您要添加的 .key 文件。
   - **输入激活码**
     在文本字段指定激活码并单击“**发送**”按钮。
4. 单击“**关闭**”按钮。

授权许可密钥或几个授权许可密钥被添加到管理服务器存储库。

添加管理服务器授权许可密钥

要添加管理服务器授权许可密钥：

1. 在管理服务器的上下文菜单中，选择“**属性**”。
2. 在打开的管理服务器属性窗口中，选择“**授权许可密钥**”区域。
3. 在**活动授权许可密钥**部分，单击**编辑**按钮。
4. 在打开的窗口中，单击**添加**按钮添加授权许可密钥。
   “添加授权许可密钥向导”启动。

向导完成后，您可以根据相应的授权许可检查管理控制台中是否显示了这些功能。

部署授权许可密钥到客户端设备

Kaspersky Security Center Web Console 允许您自动或通过“**应用程序激活**”任务将授权许可密钥分发至客户端设备。您可以使用该任务将密钥分发给特定的设备组。在通过任务分发授权许可密钥过程中，不考虑授权许可对设备数量的限制。当达到许可限制时，使用自动密钥分发自动停止授权许可密钥的分发。

如果您启用自动分发授权许可密钥，请不要创建**应用程序激活**任务来将该密钥分发给客户端设备。否则，由于频繁同步会增加管理服务器的负载。

在部署之前，请将授权许可密钥添加到管理服务器存储库。

*要通过**应用程序激活**任务将授权许可密钥分发到客户端设备：*

1. 在主菜单中，转到“**资产(设备)**” →“**任务**”。
2. 单击**添加**。

   “**新任务向导**”启动。使用“**下一步**”按钮进行向导。
3. 在**应用程序**下拉列表中，选择要为其添加授权许可密钥的应用程序。
4. 在**任务类型**列表中选择**应用程序激活**任务。
5. 在**任务名称**字段中，指定新任务的名称。
6. 选择要将任务分配到的设备。
7. 在向导的**选择授权许可密钥**步骤中，单击**添加密钥**链接以添加授权许可密钥。
8. 在密钥添加窗格中，使用以下选项之一添加授权许可密钥：

   仅当您在创建**应用程序激活**任务之前未将授权许可密钥添加到管理服务器存储库时，才需要添加授权许可密钥。

   - 选择**输入激活码**选项以输入激活码，然后执行以下操作：

     a. 指定激活码，然后单击**发送**按钮。

     有关授权许可密钥的信息将显示在密钥添加窗格中。

     b. 单击“**保存**”按钮。

     如果您想要自动将授权许可密钥分发到受管理设备，请启用**自动分发授权许可密钥到受管理设备**选项。

     密钥添加窗格将关闭。

- 选择**添加密钥文件**选项以添加密钥文件，然后执行以下操作：

  a. 单击**选择密钥文件**按钮。

  b. 在打开的窗口中，选择一个密钥文件，然后单击“**打开**”按钮。
  有关授权许可密钥的信息将显示在授权许可密钥添加窗格中。

  c. 单击“**保存**”按钮。

  > 如果您想要自动将授权许可密钥分发到受管理设备，请启用**自动分发授权许可密钥到受管理设备**选项。

  密钥添加窗格将关闭。

9. 在密钥表中选择授权许可密钥。

10. 在向导的**授权许可信息**步骤中，如果要替换活动授权许可密钥，请清除默认的**用作备用密钥**复选框。
    例如，当组织发生变化时，设备上需要另一个组织的密钥时，或者重新颁发了密钥，新授权许可比当前授权许可更早到期，等等，需要这样做。为了避免错误，您必须清除**用作备用密钥**复选框。
    如果您想了解有关向 Kaspersky Security Center 添加授权许可密钥时可能出现的问题及其解决方法的更多信息，请参阅Kaspersky Security Center 知识库。

11. 在向导的“**完成任务创建**”步骤启用“**创建完成时打开任务详情**”选项以修改默认任务设置。
    如果您不启用该选项，任务将使用默认设置创建。您可以稍后修改默认设置。

12. 单击“**完成**”按钮。
    向导将创建任务。如果启用了“**创建完成时打开任务详情**”选项，任务属性窗口将自动打开。在此窗口中，您可以指定常规任务设置，并根据需要更改任务创建期间指定的设置。

    > 您还可以通过单击任务列表中已创建任务的名称来打开任务属性窗口。

    任务被创建、配置并显示在任务列表中。

13. 要运行任务，请在任务列表中选择它，然后单击“**开始**”按钮。
    您还可以在任务属性窗口的**计划**选项卡上设置任务启动计划。
    有关计划启动设置的详细说明，请参阅常规任务设置。

当任务完成时，授权许可密钥将被部署到所选设备。

自动分发授权许可密钥

如果密钥位于管理服务器上的授权许可密钥存储区中，则 Kaspersky Security Center 允许将这些授权许可密钥自动分发至受管理设备。

要将授权许可密钥自动分发至受管理设备，请执行以下操作：

1. 在主菜单中，转到“**操作**” → “**授权许可**” → “**卡巴斯基授权许可**”。

2. 选择您要自动发布到设备的授权许可密钥名称。

3. 在打开的授权许可密钥属性窗口中，选中“**自动分发授权许可密钥到受管理设备**”复选框。

4. 单击“**保存**”按钮。

授权许可密钥将被自动分发到所有兼容设备。

授权许可密钥分发是通过网络代理执行的。没有为应用程序创建授权许可密钥分发任务。

在自动分发授权许可密钥过程中，授权许可对设备数量的限制得到考虑。授权许可限制在授权许可密钥属性中设置。如果达到授权许可限制，对该授权许可密钥的分发自动停止。

请注意，在以下情况下，自动分发的授权许可密钥可能不会显示在虚拟管理服务器存储库中：

- 授权许可密钥对于应用程序无效。
- 虚拟管理服务器没有受管理设备。
- 授权许可密钥已用于由另一个虚拟管理服务器管理的设备，并且已达到设备数量限制。

虚拟管理服务器自动从其存储库和管理服务器的存储库中分发授权许可密钥。我们建议您：

- 使用“*添加授权许可密钥*”任务来选择必须部署到设备的授权许可密钥。
- 避免在虚拟管理服务器设置中禁用“**允许从该虚拟管理服务器自动部署授权许可密钥到它的设备**”选项。否则，虚拟管理服务器将不会向设备分发授权许可密钥，包括来自管理服务器存储库的授权许可密钥。

如果您选择授权许可密钥属性窗口中的**自动分发授权许可密钥到受管理设备**复选框，授权许可密钥会立即分发在您的网络上。如果不选择此选项，您可以稍后使用任务分发授权许可密钥。

自动分发在主管理服务器上配置的授权许可密钥不会扩展到由非虚拟从属管理服务器管理的设备。

查看使用中授权许可密钥的相关信息

要查看添加到管理服务器存储库的授权许可密钥列表：

在主菜单中，转到“**操作**” → “**授权许可**” → “**卡巴斯基授权许可**”。

显示的列表包含添加到管理服务器存储库的密钥文件和激活码。

要查看关于授权许可密钥的详细信息：

1. 在主菜单中，转到“**操作**” → “**授权许可**” → “**卡巴斯基授权许可**”。
2. 点击所需授权许可密钥的名称。

在打开的授权许可密钥属性窗口，您可以查看：

- 在“**常规**”选项卡上—关于授权许可密钥的主要信息
- 在“**设备**”选项卡上—授权许可密钥用于激活已安装 Kaspersky 应用程序的客户端设备列表

要查看哪些授权许可密钥被部署到特定客户端设备：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。
2. 点击所需设备的名称。
3. 在打开的设备属性窗口中，选择“**应用程序**”选项卡。
4. 点击您要查看其授权许可密钥信息的应用程序名称。
5. 在打开的应用程序属性窗口中，选择“**常规**”选项卡，然后打开“**授权许可**”区域。

将显示有关活动和备用授权许可密钥的主要信息。

为了定义虚拟管理服务器授权许可密钥的最新设置，管理服务器每天至少发送一次请求到 Kaspersky 激活服务器。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。

从存储库删除授权许可密钥

当删除管理服务器附加功能（例如漏洞和补丁管理或移动设备管理）的活动授权许可密钥后，对应功能将不可用。如果添加了备用授权许可密钥，则删除先前的活动授权许可密钥后，备用授权许可密钥将自动变为活动授权许可密钥。

当删除部署到受管理设备上的活动授权许可密钥后，应用程序将继续在受管理设备上运行。

要从管理服务器存储库中删除密钥文件或激活码：

1. 请确认管理服务器未使用您要删除的密钥文件或激活码。如果管理服务器使用了该密钥，则无法删除该密钥。要执行检查：
   a. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
      管理服务器属性窗口将打开。
   b. 在“**常规**”选项卡上，选择“**授权许可密钥**”区域。
   c. 如果所需的密钥文件或激活码显示在打开的区域中，请单击“**删除活动授权许可密钥**”按钮，然后确认操作。之后，管理服务器不再使用被删除的授权许可密钥，但该密钥仍保留在管理服务器存储库中。如果所需的密钥文件或激活码未显示，管理服务器不会使用该密钥文件或激活码。
2. 在主菜单中，转到“**操作**”→“**授权许可**”→“**卡巴斯基授权许可**”。
3. 选择所需的密钥文件或激活码，然后单击**删除**按钮。

所选密钥文件或激活码即从存储库中删除。

您可以重新添加已删除的授权许可密钥或添加新的授权许可密钥。

撤销对最终用户授权许可协议的同意

如果您决定停止保护某些客户端设备，可以撤销任何受管理 Kaspersky 应用程序的最终用户授权许可协议 (EULA)。您必须先卸载所选应用程序，再撤销其 EULA。

在虚拟管理服务器上接受的 EULA 可以在虚拟管理服务器或主管理服务器上撤销。在主管理服务器上接受的 EULA 只能在主管理服务器上撤销。

要撤销受管理 Kaspersky 应用程序的 EULA：

1. 在管理服务器属性窗口中的“**常规**”选项卡上，选择“**最终用户授权许可协议**”区域。
   将显示在创建安装包时、无缝安装更新时或部署 Kaspersky Security for Mobile 时接受的 EULA 列表。
2. 在该列表中，选择要撤销的 EULA。
   您可以查看 EULA 的以下属性：
   - EULA 的接受日期
   - 接受 EULA 的用户名
3. 单击任意 EULA 的接受日期以打开其属性窗口，其中显示以下数据：
   - 接受 EULA 的用户名
   - EULA 的接受日期
   - EULA 的唯一标识符 (UID)
   - EULA 的全文
   - 链接到 EULA 的对象（安装包、无缝更新、移动应用程序）列表以及各自的名称和类型
4. 在 EULA 属性窗口的下部，单击“**撤回授权许可协议**”按钮。

   如果存在任何对象（安装包以及各自的任务）阻止撤销 EULA，则会显示相应通知。在删除这些对象之前，无法继续撤销。

   在打开的窗口中，系统提示您必须先卸载与 EULA 对应的 Kaspersky 应用程序。
5. 单击按钮以确认撤销。

EULA 即被撤销。它不再显示在“**最终用户授权许可协议**”区域的授权许可协议列表中。EULA 属性窗口关闭；不再安装应用程序。

续订 Kaspersky 应用程序授权许可

您可以续订已到期或即将到期（少于 30 天内）的 Kaspersky 应用程序授权许可。

要续订到期的授权许可或即将到期的授权许可：

1. 做以下之一：

   - 在主菜单中，转到“**操作**”→“**授权许可**”→“**卡巴斯基授权许可**”。
   - 在主菜单中，转到“**监控和报告**”→“**控制板**”，然后单击通知旁边的“**查看即将到期的授权许可**”链接。

   “**卡巴斯基授权许可**”窗口打开，您可以在其中查看和续订授权许可。

2. 单击所需授权许可旁边的“**续费授权许可**”链接。

   单击授权许可续订链接，即表示您同意向 Kaspersky 传输以下有关 Kaspersky Security Center 的信息：版本、您使用的本地化、软件授权许可 ID（即您要续订的授权许可 ID）以及您是否通过合作伙伴公司购买了授权许可。

3. 在打开的授权许可续订服务窗口中，按照说明续订授权许可。

   授权许可即被续订。

在 Kaspersky Security Center Web Console 中，当授权许可即将到期时，会按照以下计划显示通知：

- 到期前 30 天
- 到期前 7 天
- 到期前 3 天
- 到期前 24 小时
- 授权许可到期后

使用 Kaspersky Marketplace 选择 Kaspersky 商业解决方案

市场 是主菜单中的一个区域，可让您查看整套 Kaspersky 商业解决方案，选择您需要的解决方案，并在 Kaspersky 网站上进行购买。您可以使用筛选功能，以便仅查看适合您的组织和信息安全系统要求的解决方案。选择解决方案后，Kaspersky Security Center 会将您重定向到 Kaspersky 网站上的相关网页，以了解有关该解决方案的更多信息。每个网页都可让您继续购买或包含有关购买过程的说明。

在“**市场**”区域中，可以使用以下条件筛选 Kaspersky 解决方案：

- 要保护的设备（端点、服务器和其他类型的资产）数量：
  - 50-250
  - 250–1000
  - 大于 1000

- 组织的信息安全团队的成熟度：

  - **基础**

    这是只有一个 IT 团队的企业的典型成熟度。自动阻止最大可能数量的威胁。

  - **最佳**

    这是在 IT 团队内具有特定 IT 安全功能的企业的典型成熟度。在此级别，所需的解决方案使公司能够应对商品威胁以及绕过现有预防机制的威胁。

  - **专家**

    这是具有复杂和分布式 IT 环境的企业的典型成熟度。IT 安全团队成熟或者公司拥有 SOC（安全运营中心）团队。所需的解决方案使公司能够应对复杂威胁和针对性攻击。

- 您要保护的资产类型：

  - **端点**：员工的工作站、物理机和虚拟机、嵌入式系统
  - **服务器**：物理和虚拟服务器
  - **云**：公有、私有或混合云环境；云服务
  - **网络**：局域网、IT 基础设施
  - **服务**：Kaspersky 提供的安全相关服务

要查找和购买 Kaspersky 商业解决方案：

1. 在主菜单中，转到“**市场**”。

   默认情况下，该区域显示所有可用的 Kaspersky 商业解决方案。

2. 要仅查看适合您组织的解决方案，请在筛选器中选择所需的值。

3. 点击您要购买或想要了解更多信息的解决方案。

   您将被重定向到解决方案网页。您可以按照屏幕上的说明进行购买。

配置网络保护

本节包含有关手动配置策略和任务、用户角色、构建管理组结构和任务层级的信息。

方案：配置网络保护

快速启动向导使用默认设置创建策略和任务。这些设置可能不是最佳的，甚至是组织不允许的。因此，我们建议您微调这些策略和任务并创建其他策略和任务（如果它们对于您的网络而言是必需的）。

先决条件

在您开始之前，确保您已做了如下：

- 安装了 Kaspersky Security Center 管理服务器
- 安装了 Kaspersky Security Center Web Console（可选）
- 完成了 Kaspersky Security Center 主安装方案
- 完成了快速启动向导，或在“**受管理设备**”管理组中手动创建了以下策略和任务：
  - Kaspersky Endpoint Security 策略
  - 更新 Kaspersky Endpoint Security 的组任务
  - 网络代理策略
  - *查找漏洞和所需更新*任务

分阶段配置网络保护：

1. **设置和传播卡巴斯基应用程序策略和策略配置文件**

   要为安装在受管理设备上的卡巴斯基应用程序配置和传播设置，您可以使用两种不同的安全管理方法–以设备为中心或以用户为中心。这两种方法也可以被合并。要实现以设备为中心的安全管理，您可以使用提供在基于 Microsoft Management Console 的管理控制台或 Kaspersky Security Center Web Console 的工具。以用户为中心的安全管理仅可以通过 Kaspersky Security Center Web Console 实现。

2. **配置任务以远程管理 Kaspersky 应用程序**

   检查使用快速启动向导创建的任务并按需要调整它们。

   说明：

   - 管理控制台：
     - 为 Kaspersky Endpoint Security 设置组任务
     - 计划“查找漏洞和所需更新”任务
   - Kaspersky Security Center Web Console：
     - 为 Kaspersky Endpoint Security 设置组任务
     - “查找漏洞和所需更新”任务设置

   如果必要，创建附加任务以管理安装在客户端设备上的 Kaspersky 应用程序。

3. **评估和限制数据库上的事件负载**

   受管理应用程序操作相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

   说明：

   - 管理控制台：设置事件最大数量
   - Kaspersky Security Center Web Console：设置事件最大数量

结果

当您完成该方案时，您将通过配置卡巴斯基应用程序、任务以及管理服务器接收的事件来保护您的网络：

- 卡巴斯基应用程序是根据策略和策略配置文件配置的。
- 应用程序通过一组任务进行管理。
- 设置可以存储在数据库中的最大事件数。

当网络保护配置完成时，您可以继续配置 Kaspersky 数据库和应用程序的常规更新。

有关如何配置对 Kaspersky Sandbox 检测到的威胁的自动响应的详细信息，请参阅 Kaspersky Sandbox 2.0 在线帮助。

关于以设备为中心和以用户为中心的安全管理方法

您可以从设备功能的立场和从用户角色的立场管理安全设置。第一种方法叫做*以设备为中心的安全管理*，第二种叫做*以用户为中心的安全管理*。要应用不同的应用程序设置到不同的设备，您可以使用两种方法的任意或组合。要实现以设备为中心的安全管理，您可以使用提供在基于 Microsoft Management Console 的管理控制台或 Kaspersky Security Center Web Console 的工具。以用户为中心的安全管理仅可以通过 Kaspersky Security Center Web Console 实现。

以设备为中心的安全管理使您可以根据特定于设备的功能将不同的安全应用程序设置应用于受管理设备。例如，您可以将不同的设置应用于分配给不同管理组的设备。您还可以通过在活动目录中使用这些设备或通过它们的硬件规格来区分这些设备。

以用户为中心的安全管理使您可以将不同的安全应用程序设置应用于不同的用户角色。您可以创建多个用户角色，为每个用户分配合适的用户角色，并为具有不同角色的用户所拥有的设备定义不同的应用程序设置。例如，您可能要应用不同的应用程序设置到会计和人力资源（HR）人员的设备。结果，当实现了以用户为中心的安全管理时，每个部门–财务部门和人事部门–具有自己的卡巴斯基应用程序设置配置。设置配置定义了哪些应用程序设置可以被用户更改以及哪些被强制设置并被管理员锁定。

通过使用以用户为中心的安全管理，您可以应用特别应用程序设置到单个用户。这可能用在员工在公司有独一角色或您要监控与个别人的设备相关的安全问题时。取决于该员工在公司的角色，您可以扩展或限制该员工更改应用程序设置的权限。例如，您可能要扩展在本地办公室管理客户端设备的系统管理员的权限。

您也可以组合以设备为中心的安全管理和以用户为中心的安全管理方法。例如，您可以为每个管理组配置特定的应用程序策略，然后为企业的一个或几个用户角色创建策略配置文件。此种情况下，策略和策略配置文件按照以下优先级进行应用：

1. 为以设备为中心的安全管理创建的策略被应用。
2. 它们根据策略配置文件属性被策略配置文件修改。
3. 策略被与用户角色关联的策略配置文件修改。

策略设置和传播：以设备为中心的方法

当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

先决条件

在开始之前，确保已安装 Kaspersky Security Center 管理服务器和 Kaspersky Security Center Web Console（选装）。如果您安装了 Kaspersky Security Center Web Console，您可能也想考虑以用户为中心的安全管理作为以设备为中心的安全管理的备选或附加选项。

阶段

以设备为中心的卡巴斯基应用程序管理方案包含以下步骤：

1. **配置应用程序策略**

   通过为每个应用程序创建策略来配置安装在受管理设备上的卡巴斯基应用程序设置。策略集将被传播到客户端设备。

   当您在快速启动向导中配置网络保护时，Kaspersky Security Center 为以下应用程序创建默认策略：

   - Kaspersky Endpoint Security for Windows——适用于基于 Windows 的客户端设备
   - Kaspersky Endpoint Security for Linux——适用于基于 Linux 的客户端设备

   如果您通过使用该向导完成了配置过程，您不必为该应用程序创建新策略。转到 Kaspersky Endpoint Security 策略的手动设置。

   如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

   说明：

   - 管理控制台：创建策略
   - Kaspersky Security Center Web Console：创建策略

2. **创建策略配置文件（可选）**

   如果您想让单一管理组中的设备在不同策略设置下运行，为这些设备创建策略配置文件。策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与“基本”策略不同的设置，并在受管理设备上活动。

   通过使用配置文件激活条件您可以应用不同的策略配置文件，例如，到特定单元中的设备或到活动目录安全组，具有特别硬件配置或被特别标签标记。使用标签过滤满足特别标准的设备。例如，您可以创建叫做 *Windows* 的标签，使用该标签标记所有运行 Windows 操作系统的设备，然后指定该标签作为策略配置文件激活条件。结果，安装在所有 Windows 设备上的 Kaspersky 应用程序将被使用它们自己的策略配置文件管理。

   说明：

   - 管理控制台：
     - 创建策略配置文件
     - 创建策略配置文件激活规则
   - Kaspersky Security Center Web Console：
     - 创建策略配置文件
     - 创建策略配置文件激活规则

3. **传播策略和策略配置文件到受管理设备**

   默认情况下，管理服务器每 15 分钟自动与受管理设备同步一次。您可以避免自动同步并通过使用强制同步命令手动运行同步。在您创建或更改策略或策略配置文件后，也会强制同步。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。

   如果您使用 Kaspersky Security Center Web Console，您可以检查策略和策略配置文件是否被传送到设备。Kaspersky Security Center 在设备属性中指定传送日期和时间。

   说明：

   - 管理控制台：强制同步
   - Kaspersky Security Center Web Console：强制同步

结果

当以设备为中心的方案完成时，卡巴斯基应用程序根据指定的设置被配置并通过策略层级传播。

配置的应用程序策略和策略配置文件将被自动应用到添加到管理组的新设备。

策略设置和传播：以用户为中心的方法

本部分介绍以用户为中心的集中配置安装到受管理设备上的卡巴斯基应用程序的方案。当您完成该方案后，应用程序将在所有受管理设备上被配置，与您定义的应用程序策略和策略配置文件一致。

> 此方案可通过 Kaspersky Security Center Web Console 版本 13 或更高版本实施。

先决条件

在开始之前，确保已成功安装 Kaspersky Security Center 管理服务器和 Kaspersky Security Center Web Console，并已完成主要安装方案。您也可能要考虑以设备为中心的安全管理作为以用于为中心的方案的附加选项。了解更多两个管理方法的详情。

过程

以用户为中心的卡巴斯基应用程序管理方案包含以下步骤：

1. **配置应用程序策略**

   通过为每个应用程序创建策略来配置安装在受管理设备上的 Kaspersky 应用程序设置。策略集将被传播到客户端设备。

   当您在快速启动向导配置您网络的保护时，Kaspersky Security Center 为 Kaspersky Endpoint Security 创建默认策略。如果您通过使用该向导完成了配置过程，您不必为该应用程序创建新策略。转到 Kaspersky Endpoint Security 策略的手动设置。

   如果您有几个管理服务器和/或管理组的层级结构，从属管理服务器和子管理组默认从主管理服务器继承策略。您可以强制子组和从属管理服务器的继承以防止上游策略设置的修改。如果您仅要一部分设置被强制继承，您可以在上游策略中锁定它们。剩余未锁定的设置将可以在下流策略中修改。创建的策略层级将允许您有效管理管理组中的设备。

   说明：创建一个策略

2. **指定设备所有者**

   分配受管理设备到对应用户。

   说明：指派用户作为设备所有者

3. **为您的企业定义用户角色**

   联想您企业的员工所做的不同工作。您必须根据他们的角色划分所有员工。例如，您可以按照部门、专业或职位划分他们。然后您将需要为每个组创建用户角色。记住，每个用户角色将拥有其自己的策略配置文件，包含该角色特有的应用程序设置。

4. **创建用户角色**

   为每个员工组创建和配置用户角色或使用预定义用户角色。用户角色将包含到应用程序功能的访问权限组。

   说明：创建一个用户角色

5. **定义每个用户角色范围**

   对于每个创建的用户角色，定义用户和/或安全组以及管理组。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

   说明：编辑用户角色范围

6. **创建策略配置文件**

   为您企业中的每个用户角色创建策略配置文件。策略配置文件决定了哪些设置将被根据用户角色应用到用户设备上的应用程序。

   说明：创建一个策略配置文件

7. **关联策略配置文件与用户角色**

   关联创建的策略配置文件与用户角色。此后：策略配置文件对具有特定角色的用户活动。策略配置文件中配置的设置将被应用到安装于用户设备上的卡巴斯基应用程序。

   说明：关联策略配置文件到角色

8. **传播策略和策略配置文件到受管理设备**

   默认情况下，管理服务器每 15 分钟自动与受管理设备同步一次。同步过程中，新的或更改的策略和策略配置文件被传播到受管理设备。您可以避免自动同步并通过使用强制同步命令手动运行同步。一旦同步完成，策略和策略配置文件被传送和应用到安装的卡巴斯基应用程序。

   您可以检查策略和策略配置文件是否被传送到了设备。Kaspersky Security Center 在设备属性中指定传送日期和时间。

   说明：强制同步

结果

当以用户为中心的方案完成时，卡巴斯基应用程序根据指定的设置被配置并通过策略和策略配置文件层级传播。

对于新用户，您将必须创建新账户，分配一个创建的用户角色，并分配设备到用户。配置的应用程序策略和策略配置文件将被自动应用到该用户的新设备。

网络代理策略设置

若配置网络代理策略：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。
2. 单击网络代理策略的名称。
   网络代理策略的属性窗口打开。

请参阅比较表格，它详细介绍了根据使用的操作系统类型如何应用以下设置。

常规

在该选项卡上，可以修改策略状态并指定策略设置的继承：

- 在“**策略状态**”下，可以选择一种策略模式：
  - **活动**

    如果选择该选项，策略将变为活动状态。
    默认情况下已选定该选项。
  - **不活动**

    如果选择该选项，策略将变为不活动状态，但它仍然存储在“**策略**”文件夹中。如果需要，您可以激活该策略。
- 在“**设置继承**”设置组中，您可以配置策略继承：
  - **从父策略继承设置**

    如果启用此选项，则策略设置值将从上一级组策略继承，因而被锁定。
    默认情况下已启用该选项。
  - **在子策略中强制继承设置**

    如果启用此选项，则在应用策略更改之后，将执行以下操作：
    - 策略设置的值将被传送到管理子组的策略，也就是子策略。
    - 在每个子策略属性窗口**常规**区域的**继承设置**区块，将自动启用**从父策略继承设置**选项。

    如果启用此选项，则子策略设置被锁定。
    默认情况下已禁用该选项。

事件配置

在该选项卡上，您可以配置事件记录和事件通知。事件按照“**事件配置**”选项卡上以下区域中的重要级别进行分布：

- **功能失败**
- **警告**
- **信息**

在每个区域中，事件类型列表显示在管理服务器上事件类型和默认事件存储的期限（天）。单击事件类型后，您可以指定有关列表中选择的事件的事件记录和通知的设置。默认下，为整个管理服务器指定的通用通知设置被用于所有事件类型。然后，您可以更改所需事件类型的特别设置。

例如，在“**警告**”区域中，您可以配置 **发生了安全问题** 事件类型。此类事件可能会发生，例如，当 分发点的可用磁盘空间 小于 2 GB（至少需要 4 GB 才能远程安装应用程序和下载更新）。若要配置“**发生了安全问题**”事件，单击它并指定存储发生的事件的位置以及如何通知它们。

如果网络代理检测到安全问题，您可以使用受管理设备的设置管理此问题。

应用程序设置

设置

在“**设置**”区域，您可以配置网络代理策略：

- **仅通过分发点分发文件**

  如果启用此选项，则受管理设备上的网络代理只从分发点检索更新。

  如果禁用此选项，则受管理设备上的网络代理从分发点或管理服务器检索更新。

  请注意，受管理设备上的安全应用程序从每个安全应用程序的更新任务中设置的源检索更新。如果启用“**仅通过分发点分发文件**”选项，请确保在更新任务中将 Kaspersky Security Center 设置为更新源。

  默认情况下已禁用该选项。

- **事件队列的最大大小(MB)**

  在该字段中，您可以指定事件队列可在驱动器上占据的最大空间。

  默认值为 2 MB。

- **应用程序被允许在设备上检索策略扩展数据**

  安装在受管理设备上的网络代理会将有关已应用的安全应用程序策略的信息传输到安全应用程序（例如，Kaspersky Endpoint Security for Windows）。您可以在安全应用程序界面查看传输的信息。

网络代理传输以下信息：

- 策略传输至受管理设备的时间。
- 策略传输至受管理设备时的活动策略的名称。
- 策略传输至受管理设备时漫游策略的名称（对于Linux 版网络代理不可用）。
- 策略传输至受管理设备时包含受管理设备的管理组的名称和完整路径。
- 策略传输至受管理设备时包含其名称和优先级的活动策略配置文件列表。

您可以使用该信息来确保将正确的策略应用于设备并用于故障排除。默认情况下已禁用该选项。

- **保护网络代理服务免遭非授权的卸载或终止，并防止设置更改**

当启用该选项时，网络代理被安装到受管理设备之后，没有所需权限组件无法被卸载或重新配置。网络代理服务无法被停止。此选项对域控制器没有影响。

启用此选项可保护以本地管理员权限操作的工作站上的网络代理。

默认情况下已禁用该选项。

- **使用卸载密码**

如果启用此选项，则单击“**修改**”按钮可以指定 klmover 实用程序和网络代理远程卸载的密码。

默认情况下已禁用该选项。

存储库

在“**存储库**”区域，您可以选择将其信息从网络代理发送到管理服务器的对象类型。如果本区域中的某些设置被网络代理策略禁止，则您无法修改它们。

- **已安装应用程序详情**

如果启用此选项，则有关客户端设备上安装的应用程序的信息将发送至管理服务器。

默认情况下已启用该选项。

- **包括补丁信息**

有关在客户端设备上安装的应用程序补丁的信息将发送到管理服务器。启用此选项可能会增加管理服务器和 DBMS 的负载，并导致数据库数据量的增加。

默认情况下已启用该选项。它仅适用于 Windows。

- **Windows Update 更新详情**

如果启用此选项，则有关客户端设备上必须安装的 Microsoft Windows Update 更新的信息将发送至管理服务器。

有时，即使禁用此选项，更新也会显示在“**可用更新**”区域的设备属性中。例如，如果组织的设备存在可被这些更新修复的漏洞，则可能出现这种情况。

默认情况下已启用该选项。它仅适用于 Windows。

有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **软件漏洞和对应更新的详情**

  如果启用此选项，则将有关在受管理设备上检测到的第三方软件（包括 Microsoft 软件）中的漏洞信息以及有关修复第三方漏洞（不包括 Microsoft 软件）的软件更新信息发送到管理服务器。

  选择此选项（**软件漏洞和对应更新的详情）**会增加网络负载、管理服务器磁盘负载和网络代理资源消耗。

  默认情况下已启用该选项。它仅适用于 Windows。

  要管理 Microsoft 软件的软件更新，请使用“**Windows Update 更新详情**”选项。

- **硬件注册表的详细信息**

  安装在设备上的网络代理会将设备硬件的相关信息发送到管理服务器。您可以在设备属性中查看硬件详细信息。

  确保在要从中获取硬件详细信息的 Linux 设备上安装了 lshw 实用程序。根据所使用的 hypervisor，从虚拟机获取的硬件详细信息可能不完整。

软件更新和漏洞

在“**软件更新和漏洞**”区域，您可以配置搜索和发布 Windows 更新以及启用扫描可执行文件以发现漏洞：

- **使用管理服务器作为 WSUS 服务器**

  如果启用此选项，Windows 更新将下载到管理服务器。管理服务器提供以集中模式通过网络代理下载更新到客户端设备的 Windows 更新服务。

  如果禁用此选项，则不使用管理服务器下载 Windows 更新。此种情况下，客户端设备自己接收 Windows 更新。

  默认情况下已禁用该选项。

- 您可以限制用户在其设备上手动使用 Windows Update 安装的 Windows 更新。

  在运行 Windows 10 的设备上，如果 Windows Update 已经为设备找到更新，您在“**允许用户管理 Windows Update 更新安装**”下选择的新选项将仅在发现的更新被安装后才被应用。

  在下拉列表中选择条目：

  - **允许用户安装所有可应用 Windows Update 更新**

    用户可以安装所有可应用到他们设备的 Microsoft Windows Update 更新。

如果您不希望干预更新安装，请选择该选项。

当用户手动安装 Microsoft Windows Update 更新时，更新可能从 Microsoft 服务器下载，而不是从管理服务器。如果管理服务器还未下载这些更新，这是可能的。从 Microsoft 服务器下载更新导致额外流量。

- **仅允许用户安装批准的 Windows Update 更新**

  用户可以安装所有可应用到他们设备的和您批准的 Microsoft Windows Update 更新。

  例如，您可能想先在测试环境中检查更新安装以确保它们不干预设备操作，仅在这之后允许安装这些批准的更新到客户端设备。

  当用户手动安装 Microsoft Windows Update 更新时，更新可能从 Microsoft 服务器下载，而不是从管理服务器。如果管理服务器还未下载这些更新，这是可能的。从 Microsoft 服务器下载更新导致额外流量。

- **不允许用户安装 Windows Update 更新**

  用户无法在他们的设备上手动安装 Microsoft Windows Update 更新。所有可应用更新根据您的配置而安装。

  如果您想要集中管理更新的安装则选则此选项。

  例如，您可以想优化更新计划以便网络不过载。您可以计划稍后更新，以便它们不干预用户工作。

- 在“**Windows Update 搜索模式**”设置组中，您可以选择更新搜索模式：

  - **活动**

    如果选中该选项，管理服务器支持使用网络代理在客户端设备上从 Windows 更新代理发送请求至更新源：Windows 更新服务器（或简称为 WSUS）。然后，网络代理会将从 Windows 更新代理接收到的信息传送给管理服务器。

    仅在选择*查找漏洞和所需更新*任务的“**连接更新服务器更新数据**”选项时，该选项才生效。

    默认情况下已选定该选项。

  - **被动**

    如果您选定该选项，网络代理将从上次同步更新源之后定期从 Windows 更新代理将所检索更新的信息传递给管理服务器。如果 Windows 更新代理没有执行与更新源同步，管理服务器上有关更新的信息将变为过期。

    如果要从更新源的内存缓存中获取更新，请选择此选项。

  - **已禁用**

    如果选中该选项，管理服务器不会请求任何有关更新的信息。

    例如，如果您想首先在本地设备上测试更新，请选择此选项。

- **当运行可执行文件时扫描其漏洞**

  如果启用此选项，系统将在运行可执行文件时扫描漏洞。

  默认情况下已启用该选项。

重启管理

如果受管理设备的操作系统必须重启才能正确使用、安装或卸载应用程序，您可以在“**重启管理**”区域指定要执行的操作：

- **不重启操作系统**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **如果必要，自动重启操作系统**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于1和1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后强制重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于1和1440 分钟之间。

  - **强行关闭锁定会话中的应用程序**

    运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

    如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

默认情况下已禁用该选项。

Windows 桌面共享

您可以通过“**Windows 桌面共享**”区域启用并配置在使用共享桌面访问时用户的远程设备上执行的管理员操作的审计：

- **启用审计**

  如果启用该选项，远程设备上管理员的操作审计启用。远程设备上的管理员操作是被一一记录下来的:

  - 在远程设备的事件日志中
  - 在位于远程设备上网络代理安装文件夹中的扩展名为 syslog 的文件中
  - Kaspersky Security Center 的事件数据库

  当满足以下条件时,管理员操作审核可用：

  - 漏洞和补丁管理授权许可正在使用中
  - 管理员有权启动共享访问远程设备的桌面

  如果禁用此选项,远程设备上的管理员操作审核被禁用。

  默认情况下已禁用该选项。

- **读取时要监控的文件掩码**

  该列表包含文件掩码.启用审计,程序会监控管理员读取符合掩码的文件并保存读取文件的信息.如果选择了“**启用审计**”选框，则该列表可用。您可以编辑文件掩码,或在列表中添加新掩码.列表中每个新文件掩码需要在全新的一行中指定.

  默认,指定了以下文件掩码:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **修改时要监控的文件掩码**

  该列表包含远程设备上的文件掩码。启用审核时,程序会监控管理员对符合掩码的文件作出的更改,并保存修改的相关信息.如果选择了“**启用审计**”选框，则该列表可用。您可以编辑文件掩码,或在列表中添加新掩码.列表中每个新文件掩码需要在全新的一行中指定.

  默认,指定了以下文件掩码:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

管理补丁和更新

在“**管理补丁和更新**”区域，您可以配置更新的下载和分发以及补丁在受管理设备上的安装：

- **对未定义状态的组件自动安装可应用更新和补丁**

  如果启用此选项，带有*未定义*批准状态的 Kaspersky 应用程序在从更新服务器下载后将被自动安装在受管理设备。

如果禁用此选项，被下载和标注为*未定义*状态的 Kaspersky 补丁将仅在您改变其状态为*已批准*是被安装。

默认情况下已启用该选项。

- **提前从管理服务器下载更新和反病毒数据库(推荐)**

  如果启用此选项，离线模式更新下载被使用。当管理服务器接收更新时，它通知网络代理(安装网络代理的设备)将用于受管理应用程序的更新。当网络代理接收更新的信息后，它提前从管理服务器下载相关文件。在第一次连接网络代理时，管理服务器发起更新下载。网络代理下载所有更新到客户端设备后，更新对该设备上的应用程序可用。

  当客户端设备上的受管理应用程序尝试访问网络代理以更新时，该网络代理检查其是否具有所有的更新。如果在受管理应用程序请求更新之前 25 小时内，更新已从管理服务器收到，则网络代理不连接到管理服务器，而是从本地缓存提供更新给受管理应用程序。当网络代理提供更新到客户端设备上的应用程序时，到管理服务器的连接可能不被建立，但是更新不需要连接。

  如果禁用此选项，离线模式更新下载不被使用。更新根据更新下载任务的计划被分发。

  默认情况下已启用该选项。

连接

“**连接**”区域包含三个子区域：

- **网络**
- **连接配置文件**
- **连接计划**

在“**网络**”子区域中，可以配置与管理服务器的连接，启用 UDP 端口和指定 UDP 端口号。

- 在“**连接到管理服务器**”设置组，您可以配置到管理服务器的连接并指定同步客户端设备和管理服务器的时间间隔：

  - **同步间隔(分钟)**

    网络代理同步管理服务器的受管理设备。我们建议您设置同步间隔（也叫心跳）为每 10,000 台受管理设备 15 分钟。

    如果同步间隔设置为少于 15 分钟，则每 15 分钟执行一次同步。如果同步间隔设置为 15 分钟或更长时间，则以指定的同步间隔执行同步。

  - **压缩网络流量**

    如果启用此选项，则通过减少所传输的流量进而减少管理服务器的负载来提高网络代理的数据传输速度。

    客户端设备上的 CPU 负载可能会增加。

    默认情况下启用该复选框。

- **在 Microsoft Windows 防火墙中打开网络代理端口**

  如果启用此选项，网络代理和管理服务器工作所需的端口将添加到 Microsoft Windows 防火墙排除列表中。

  默认情况下已启用该选项。

- **使用 SSL 连接**

  如果启用此选项，则使用 SSL 协议通过安全端口连接管理服务器。

  默认情况下已启用该选项。

- **以默认连接设置在分发点(如果可用)上使用连接网关**

  如果启用此选项，分发点上的连接网关在管理组属性指定的设置下使用。

  默认情况下已启用该选项。

- **使用 UDP 端口**

  如果需要网络代理通过 UDP 端口连接到管理服务器，启用“**使用 UDP 端口**”选项，并指定“**UDP 端口号**”。默认情况下已启用该选项。连接到管理服务器的默认 UDP 端口是 15000。

- **UDP 端口号**

  在该字段中，您可以输入 UDP 端口号。默认端口号是 15000。

  使用十进制系统记录。

  如果客户端设备运行在 Windows XP Service Pack 2 系统下，则集成的防火墙会阻止 UDP 端口 15000。请手动打开此端口。

- **使用分发点强制连接到管理服务器**

  如果在分发点设置窗口中选择了“**将此分发点用作推送服务器**”选项，则选择此选项。否则，分发点不会用作推送服务器。

在“**连接配置文件**”子区域中，可以指定网络位置设置并在管理服务器不可用时启用漫游模式：

- **网络位置设置**

  网络位置设置用于定义客户端设备所连接的网络属性，并指定当网络特性改变时，网络代理从一个管理服务器连接配置文件切换到另一个配置文件的规则。

- **管理服务器连接配置文件**

  在该区域中，您可以查看和配置网络代理至管理服务器的连接。在该区域，您也可以创建当以下事件发生时，切换网络代理到不同管理服务器的规则：

  - 当客户端设备连接到另一个本地网络时
  - 当设备与组织的本地网络丢失连接时
  - 当连接网关的地址更改或 DNS 服务器地址修改时

  连接配置文件仅支持运行 Windows 和 macOS 的设备。

- **当管理服务器不可用时启用漫游模式**

  如果启用此选项，则在通过该配置文件连接的情况下，客户端设备上安装的应用程序将使用漫游模式设备的策略配置文件，以及漫游策略。如果没有为应用程序定义漫游策略，则使用激活策略。

  如果禁用此选项，则应用程序将使用已激活的策略。

  默认情况下已禁用该选项。

在“**连接计划**”子区域中，您可以指定网络代理发送数据到管理服务器的时间间隔：

- **必要时连接**

  如果选中此选项，当网络代理需要发送数据到管理服务器时连接才被建立。

  默认情况下已选定该选项。

- **在指定时间间隔连接**

  如果选中此选项，网络代理在指定时间连接到管理服务器。您可以添加若干个连接时间段。

通过分发点的网络轮询

在“**通过分发点的网络轮询**”区域中，可以配置网络自动轮询。您可以使用以下选项启用轮询并设置其频率：

- **Windows 网络**

  如果启用此选项，则管理服务器将按照所配置的计划自动轮询网络，单击“**设置快速轮询计划**”和“**设置完整轮询计划**”链接可配置轮询计划。

  如果禁用此选项，管理服务器将以**网络轮询频率(分钟)**字段中指定的时间间隔轮询网络。

  可以在“**Windows 域的轮询频率(分钟)**（适用于快速 Windows 网络轮询）和**网络轮询频率(分钟)**（适用于完整 Windows 网络轮询）”字段中配置 10.2 版之前的网络代理的设备发现间隔。

  默认情况下已禁用该选项。

- **Zeroconf**

  如果启用此选项，分发点将使用零配置网络（也称为 *Zeroconf*）轮询带有 IPv6 设备的网络。在这种情况下，已启用的 IP 范围轮询将被忽略，因为分发点将轮询整个网络。

  要开始使用 Zeroconf，必须满足以下条件：

  - 分发点必须运行 Linux。
  - 您必须在分发点上安装 avahi-browse 实用程序。

  如果禁用此选项，分发点不会轮询带有 IPv6 设备的网络。

  默认情况下已禁用该选项。

- **IP 范围**

  如果启用此选项，则分发点将按照所配置的计划自动轮询 IP 范围，单击“**设置轮询计划**”按钮可配置轮询计划。

  如果禁用此选项，则分发点将不轮询 IP 范围。

  对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置 IP 范围的轮询频率。如果启用此选项，则该字段可用。

  默认情况下已禁用该选项。

- **域控制器**

  如果启用此选项，则分发点将按照所配置的计划自动轮询 Active Directory，单击“**设置轮询计划**”链接可配置轮询计划。

  如果禁用此选项，则管理服务器将不轮询 Active Directory。

  对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置活动目录的轮询频率。如果启用此选项，则字段可用。

  默认情况下已禁用该选项。

  如果启用此选项，则分发点将按照所配置的计划自动轮询域控制器，单击“**设置轮询计划**”按钮可配置轮询计划。

  如果禁用此选项，则分发点将不轮询域控制器。

  对于 10.2 版之前的网络代理，可在“**轮询间隔(分钟)**”字段中配置域控制器轮询频率。如果启用此选项，则字段可用。

  默认情况下已禁用该选项。

分发点网络设置

如果分发点在连接到互联网时使用代理服务器，则您可以在**分发点网络设置**部分中指定以下设置：

- **使用代理服务器**
- **地址**

- **端口号**
- **对本地地址不使用代理服务器**

  如果启用此选项，将不使用代理服务器连接本地网络的设备。

  默认情况下已禁用该选项。

- **代理服务器身份验证**

  如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。

  默认情况下已清除该选框。

- **用户名**
- **密码**

KSN 代理(分发点)

在“**KSN 代理(分发点)**”区域，您可以配置应用程序使用分发点从受管理设备转发 Kaspersky Security Network (KSN) 请求：

- **在分发点端启用 KSN 代理**

  KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

  分发点将卡巴斯基安全网络声明中列出的KSN统计数据发送给卡巴斯基。

  默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器**和**我同意使用卡巴斯基安全网络**选项在管理服务器属性窗口中被启用时起作用。

  您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

- **转发 KSN 请求到管理服务器**

  分发点从受管理设备转发 KSN 请求到管理服务器。

  默认情况下已启用该选项。

- **通过互联网直接访问 KSN 云/KPSN**

  分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

  安装了网络代理版本 11（或更早版本）的分发点不能直接访问 KPSN。如果要重新配置分发点以将 KSN 请求发送到 KPSN，请为每个分发点启用“**转发 KSN 请求到管理服务器**”选项。

  安装了网络代理版本 12（或更高版本）的分发点可以直接访问 KPSN。

- **端口**

  受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

- **UDP 端口**

  如果需要网络代理通过 UDP 端口连接到管理服务器，启用“**使用 UDP 端口**”选项，并指定“**UDP 端口号**”。
  默认情况下已启用该选项。连接到管理服务器的默认 UDP 端口是 15000。

更新(分发点)

在**更新(分发点)**区域，您可以启用下载差异文件功能，以便分发点以差异文件的形式从卡巴斯基更新服务器获取更新。

本地账户管理(仅限 Linux)

“**本地账户管理(仅限 Linux)**”部分包括三个子部分：

- **用户证书管理**
- **添加或编辑适用的本地管理员组**
- **上传参考文件以保护用户设备上的 sudoers 文件以防更改**

在“**用户证书管理**”子部分中，您可以指定要安装的根证书。例如，这些证书可用于验证网站或网络服务器的真实性。

- **安装根证书**

  如果启用此选项，则添加到表中的证书将安装在指定的设备上。
  如果禁用此选项，则不会在指定设备上安装任何证书。
  默认情况下已禁用该选项。

- **添加**

  单击此按钮会打开一个窗口，您可以在其中添加证书。
  证书必须小于 10 MB。
  Kaspersky Security Center 支持具有 CER、CRT、CERT、PEM 和 KEY 扩展名的证书。

在“**添加或编辑适用的本地管理员组**”子部分中，您可以管理本地管理员组。例如，在撤销本地管理员权限时会使用这些组。您还可以使用“**特权设备用户报告(仅限 Linux)**”检查特权用户账户列表。

- **添加**

  单击此按钮会打开一个窗口，您可以在其中添加本地管理员组。

- **编辑**

  单击此按钮会打开一个窗口，您可以在其中编辑本地管理员组。
  如果选中本地管理员组旁边的复选框，则此按钮可用。

- **删除**

  单击此按钮会从表中删除所选的本地管理员组。

  如果选中本地管理员组旁边的复选框，则此按钮可用。

在“**上传参考文件以保护用户设备上的 sudoers 文件以防更改**”子部分中，您可以配置对 sudoers 文件的控制。具有权限的组和设备用户由设备上的 sudoers 文件定义。sudoers 文件位于 `/etc/sudoers`。您可以上传参考 sudoers 文件，以防止 sudoers 文件被更改。这可以防止对 sudoers 文件进行不必要的更改。

无效的参考 sudoers 文件可能会导致用户的设备出现故障。

- **控制 sudoer 文件**

  如果启用此选项，sudoers 文件将由当前参考 sudoers 文件替换。

  如果禁用此选项，sudoers 文件将保持不变。

  默认情况下已禁用该选项。

- **参考 sudoer 文件**

  此字段显示上传的参考 sudoers 文件的名称。

- **上传**

  单击此按钮会打开一个窗口，您可以在其中上传参考 sudoers 文件。

- **当前参考 sudoer 文件**

  单击此按钮会显示当前 sudoers 文件的内容。

修订历史

在此选项卡上，您可以查看策略修订列表和回滚策略更改（如有必要）。

网络代理策略设置：按操作系统比较

下表显示了您可以在管理控制台和Kaspersky Security Center Web Console中使用哪些网络代理策略来设置具有特定操作系统的网络代理。

网络代理策略设置：按操作系统比较

策略区域	Windows	macOS	Linux
常规	✓	✓	✓
事件配置	✓	✓	✓

策略区域	Windows	macOS	Linux
设置	✓	✓	✓ 下列选项可用： • **仅通过分发点分发文件** • **事件队列的最大大小(MB)** • **应用程序被允许在设备上检索策略扩展数据**
存储库	✓	✓ "**硬件注册表的详细信息**"选项可用。	✓ 下列选项可用： • **已安装应用程序详情** • **硬件注册表的详细信息**
软件更新和漏洞	✓	—	—
重启管理	✓	—	—
Windows 桌面共享	✓	—	—
管理补丁和更新	✓	—	—
连接→网络	✓	✓	✓ 除了**在 Microsoft Windows 防火墙中打开网络代理端口**选项之外。
连接→连接配置文件	✓	✓	—
连接→连接计划	✓	✓	✓
通过分发点的网络轮询	✓ 只有**Windows 网络**, **IP 范围**和**域控制器**选项可用。	—	✓ 下列选项可用： • **Zeroconf** • **IP 范围** • **域控制器**
分发点网络设置	✓	✓	✓
KSN 代理(分发点)	✓	—	✓
更新(分发点)	✓	—	✓
修订历史	✓	✓	✓

启用和禁用网络代理的低资源消耗模式

在低资源消耗模式下，您可以限制安装在客户端设备上的网络代理的 RAM 使用量。默认情况下，低资源消耗模式被禁用。

在低资源消耗模式下，无法执行以下功能：

- 无法指定网络代理作为分发点（无论是手动还是自动）。
- 网络代理不会在单独的文本文件中记录有关网络代理状态的信息。
- 网络代理不支持离线模式的更新下载。
- 以下组件和进程被禁用：
  - 获取有关第三方更新和漏洞的信息。
  - 在分发点端运行 KSN 代理。
  - 将更新上传到分发点存储库。

- 绕过 DNS 服务器阻止。
- 获取有关可用磁盘空间的信息。

禁用低资源消耗模式后，组件和进程会恢复运行。

要启用低资源消耗模式：

1. 在客户端设备上的命令行中执行以下命令：

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. 重启网络代理。
3. 要检查低资源消耗模式是否启用，请在 Windows 中打开**事件查看器**，然后选择**应用程序和服务日志→卡巴斯基事件日志**。

   确保日志包含诸如**Kaspersky Security Center 网络代理在低资源消耗模式下工作之**类的事件。

低资源消耗模式已启用。

要禁用低资源消耗模式：

1. 在客户端设备上的命令行中执行以下命令：

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. 重启网络代理。
3. 要检查低资源消耗模式是否禁用，请在 Windows 中打开**事件查看器**，然后选择**应用程序和服务日志→卡巴斯基事件日志**。

   确保最后一个 klnagent 事件不包含消息**Kaspersky Security Center 网络代理正在低资源消耗模式下工作** 。

低资源消耗模式被禁用。

您还可以使用*远程执行脚本任务*远程启用低资源消耗模式。

Kaspersky Endpoint Security 策略的手动设置

本部分提供有关如何配置 Kaspersky Endpoint Security 策略的建议。您可以在策略属性窗口中执行设置。编辑设置时，请单击相关设置组右侧的锁定图标，将指定的值应用到工作站。

配置卡巴斯基安全网络

卡巴斯基安全网络 (KSN) 是云服务的基础设施，包含有关文件、网络资源和软件信誉的信息。卡巴斯基安全网络使 Kaspersky Endpoint Security for Windows 能够更快地响应不同类型的威胁，增强保护组件的性能，并降低误报的可能性。有关卡巴斯基安全网络的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要指定推荐的 KSN 设置：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**高级威胁防护**”→“**卡巴斯基安全网络**”。
4. 确保**卡巴斯基安全网络**选项被启用。使用此选项有助于重新分发和优化网络流量。

   如果您使用Managed Detection and Response，您必须为分发点启用**卡巴斯基安全网络**选项并启用扩展 KSN 模式。
5. 如果 KSN 代理服务不可用，则启用对 KSN 服务器的使用。KSN 服务器可能位于 Kaspersky 端（当 KSN 被使用）或第三方端（当 KPSN 被使用）。
6. 单击“**确定**”。

推荐的 KSN 设置被指定。

检查受防火墙保护的网络列表

确保 Kaspersky Endpoint Security for Windows 防火墙保护您的所有网络。默认情况下，防火墙保护具有以下连接类型的网络：

- **公用网络**。安全应用程序、防火墙或过滤器不保护此类网络中的设备。
- **本地网络**。此网络中的设备对文件和打印机的访问受限。
- **受信任网络**。此类网络中的设备受到保护，免受攻击和对文件和数据的未授权访问。

如果您配置了自定义网络，请确保防火墙保护该网络。为此，请检查 Kaspersky Endpoint Security for Windows 策略属性中的网络列表。该列表可能不包含所有网络。

有关防火墙的更多信息，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要查看网络列表：

1. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**基本威胁防护**”→“**防火墙**”。
4. 在“**可用网络**”下，单击“**网络设置**”链接。
   网络连接窗口将打开。该窗口显示网络列表。
5. 如果列表中缺少网络，请添加该网络。

禁用网络驱动扫描

当 Kaspersky Endpoint Security for Windows 扫描网络驱动器时，会给它们带来很大的负载。在文件服务器上执行间接扫描更方便。

您可以在 Kaspersky Endpoint Security for Windows 策略属性中禁用网络驱动器扫描。有关这些策略属性的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要禁用网络驱动器扫描：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**基本威胁防护**”→“**文件威胁防护**”。
4. 在**保护范围**下，禁用**所有网络驱动器**选项。
5. 单击“**确定**”。

网络驱动器扫描被禁用。

从管理服务器内存中排除软件详细信息

建议管理服务器不要保存有关在网络设备上启动的软件模块的信息。这样管理服务器内存不会超限。

您可以在 Kaspersky Endpoint Security for Windows 策略属性中禁用保存此信息。

要禁用对已安装软件模块信息的保存：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**常规设置**”→“**报告和存储**”。
4. 在**到管理服务器的数据传输**下，禁用在顶级策略中仍然被启用的**关于已启动的应用程序**复选框。
   当选中该复选框时：如果选中此复选框，管理服务器数据库保存网络设备上所有软件模块的所有版本信息。该信息可能需要 Kaspersky Security Center 数据库上的大量磁盘空间(几十 G)。

已安装软件模块的信息不被保存到管理服务器数据库。

配置对工作站上的 Kaspersky Endpoint Security for Windows 界面的访问

如果必须通过 Kaspersky Security Center 在集中模式下管理组织网络上的威胁防护，请在 Kaspersky Endpoint Security for Windows 策略属性中指定接口设置，如下所述。这样，您将防止未经授权访问工作站上的 Kaspersky Endpoint Security for Windows 以及更改 Kaspersky Endpoint Security for Windows 设置。

有关这些策略属性的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

要指定推荐的界面设置：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，转到“**应用程序设置**”→“**常规设置**”→“**界面**”。
4. 在**用户交互**下，选择**不显示用户界面**选项。这禁用了 Kaspersky Endpoint Security for Windows 用户界面在工作站上的显示，这样，其用户将无法更改 Kaspersky Endpoint Security for Windows 的设置。
5. 在**密码保护**下，启用切换开关。这降低了对工作站上 Kaspersky Endpoint Security for Windows 设置进行未经授权或意外更改的风险。

Kaspersky Endpoint Security for Windows 界面的推荐设置被指定。

在管理服务器数据库中保存重要的策略事件

为了避免管理服务器数据溢出，我们建议您仅保存重要事件到数据库。

要配置注册重要事件到管理服务器数据库：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Windows 策略。
   所选策略的属性窗口打开。
3. 在策略属性中，打开“**事件配置**”选项卡。
4. 在“**严重**”区域中，单击“**添加事件**”并仅选中以下事件旁边的复选框：
   - *违反了最终用户授权许可协议*
   - *应用程序自动运行已禁用*
   - *激活错误*
   - *检测到活动威胁。应该启动高级清除*
   - *无法清除*
   - *检测到先前打开的危险链接*

- *进程已终止*
- *网络活动已阻止*
- *检测到网络攻击*
- *已禁止应用程序启动*
- *访问被拒绝(本地数据库)*
- *访问被拒绝 (KSN)*
- *本地更新错误*
- *不能同时启动两项任务*
- *与 Kaspersky Security Center 交互时出错*
- *未更新所有组件*
- *应用文件加密/解密规则时出错*
- *启用便携模式时出错*
- *禁用便携模式时出错*
- *无法加载加密模块*
- *无法应用策略*
- *更改应用程序组件时出错*

5. 单击“**确定**”。
6. 在“**功能失败**”区域中，单击“**添加事件**”并选中“*任务设置无效。设置未应用。*
7. 单击“**确定**”。
8. 在“**警告**”区域中，单击“**添加事件**”并仅选中以下事件旁边的复选框：
   - *自我保护被禁用*
   - *保护组件已禁用*
   - *备用密钥不正确*
   - *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)*
   - *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)*
   - *对象已删除*
   - *对象已清除*
   - *用户选择了退出加密策略*

- *文件已被管理员从 Kaspersky Anti Targeted Attack Platform 服务器上的隔离区恢复*
- *文件已被管理员隔离在 Kaspersky Anti Targeted Attack Platform 服务器上*
- *发送给管理员的应用程序启动阻止消息*
- *发送给管理员的设备访问阻止消息*
- *发送给管理员的网页访问阻止消息*

9. 单击“**确定**”。
10. 在“**信息**”区域中，单击“**添加事件**”并仅选中以下事件旁边的复选框：
    - *对象的备份副本已创建*
    - *禁止应用程序在测试模式下启动*
11. 单击“**确定**”。

注册重要事件到管理服务器数据库被配置。

Kaspersky Endpoint Security 更新组任务的手动设置

Kaspersky Endpoint Security 的最优和建议计划选项是“**当新更新下载至存储库时**”（当“**使用任务启动自动随机延迟**”复选框被选中时）。

授予对“设备控制”阻止的外部设备的离线访问权限

在 Kaspersky Endpoint Security for Windows 策略的“设备控制”组件中，您可以管理用户对安装在客户端设备上或连接到客户端设备的外部设备（例如，硬盘驱动器、照相机或 Wi-Fi 模块）的访问权限。这样可以在连接此类外部设备时保护客户端设备免受感染，并防止数据丢失或泄漏。

如果需要授予对“设备控制”阻止的外部设备的临时访问权限，但是无法将设备添加到受信任设备列表中，可以授予对外部设备的临时离线访问权限。离线访问意味着客户端设备无法访问网络。

只有在 Kaspersky Endpoint Security for Windows 策略设置的**应用程序设置 → 安全控制 → 设备控制**区域中启用了“**允许临时访问请求**”选项时，才能授予对“设备控制”阻止的外部设备的离线访问权限。

授予对“设备控制”阻止的外部设备的离线访问权限包括以下阶段：

1. 在 Kaspersky Endpoint Security for Windows 对话窗口中，想要访问已阻止的外部设备的设备用户要生成请求访问文件并将其发送给 Kaspersky Security Center 管理员。
2. 获得此请求后，Kaspersky Security Center 管理员将创建一个访问密钥文件，然后将其发送给设备用户。
3. 在 Kaspersky Endpoint Security for Windows 对话窗口中，设备用户激活该访问密钥文件并获得对外部设备的临时访问权限。

要授予对“设备控制”阻止的外部设备的离线访问权限：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
   将显示受管理设备列表。
2. 在此列表中，选择请求访问被“设备控制”阻止的外部设备的用户设备。
   只能选择一台设备。
3. 在受管理设备列表上方，单击省略号按钮（ **...** ），然后单击“**授予移动模式设备访问权限**”按钮。
4. 在打开的 **应用程序设置** 窗口的“**设备控制**”区域中，单击“**浏览**”按钮。
5. 选择您从用户那里收到的请求访问文件，然后单击“**打开**”按钮。该文件应具有 AKEY 格式。
   将显示用户请求访问的锁定设备的详细信息。
6. 指定“**访问持续时间**”设置的值。
   此设置定义您允许用户访问锁定设备的时长。默认值是用户在创建请求访问文件时指定的值。
7. 指定访问密钥可以在设备上激活的时间段。
   此设置定义用户可以使用提供的访问密钥激活对已阻止设备的访问权限的时间期间。
8. 单击“**保存**”按钮。
   这将打开标准的 Microsoft Windows “**保存访问密钥**”窗口。
9. 选择要在其中保存包含已阻止设备访问密钥的文件的目标文件夹。
10. 单击“**保存**”按钮。

结果，当您向用户发送访问密钥文件，然后用户在 Kaspersky Endpoint Security for Windows 对话窗口中将其激活后，用户可以在特定期间内临时访问已阻止的设备。

远程删除应用程序或软件更新

要从选定设备中远程删除应用程序或软件更新：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。
   “新任务向导”启动。使用**下一步**按钮进行向导。
3. 对于 Kaspersky Security Center 应用程序，选择“**远程卸载应用程序**”任务类型。
4. 指定您正创建的任务的名称。
   任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择要将任务分配到的设备。

6. 选择要删除的软件种类，然后选择要删除的特定应用程序、更新或补丁：

- **卸载受管理应用程序**

  显示卡巴斯基应用程序列表。选择要删除的应用程序。

- **卸载不兼容的应用程序**

  显示与 Kaspersky 安全应用程序或 Kaspersky Security Center 不兼容的应用程序列表。选中要删除的应用程序旁边的复选框。

- **从应用程序注册表中卸载应用程序**

  默认情况下，网络代理会向管理服务器发送有关受管理设备上安装的应用程序的信息。已安装应用程序的列表存储在应用程序注册表中。

  要从应用程序注册表中选择应用程序：

  a. 单击“**要卸载的应用程序**”字段，然后选择要删除的应用程序。

  如果您选择 Kaspersky Security Center 网络代理，则运行任务时，状态“*已成功完成*”将显示删除进程已开始。如果删除 Kaspersky Security Center 网络代理，状态不会改变。如果任务失败，状态更改为“*失败*”。

  b. 指定卸载选项：

  - **卸载模式**

    选择要如何删除应用程序：

    - **自动定义卸载命令**

      如果应用程序具有应用程序供应商定义的卸载命令，则 Kaspersky Security Center 将使用此命令。我们建议您选择此选项。

    - **指定卸载命令**

      如果要指定您自己的应用程序卸载命令，请选择此选项。

      我们建议您先尝试使用“**自动定义卸载命令**”选项来卸载应用程序。如果通过自动定义的命令卸载失败，则使用您自己的命令。

      在该字段中键入卸载命令，然后指定以下选项：

      仅当未自动检测到默认命令时使用此命令进行卸载

      Kaspersky Security Center 会检查所选应用程序是否具有应用程序供应商定义的卸载命令。如果找到，Kaspersky Security Center 将使用该命令，而不使用在“**应用程序卸载命令**”字段中指定的命令。

      我们建议您启用此选项。

- **应用程序成功卸载后执行重启**

  如果应用程序要求在成功卸载后重新启动受管理设备上的操作系统，操作系统将自动重新启动。

- **卸载指定的应用程序更新、补丁或第三方应用程序**

  显示更新、补丁和第三方应用程序的列表。选择要删除的项目。

  显示的列表是常规的应用程序和更新列表，并不对应于受管理设备上安装的应用程序和更新。选择项目之前，建议您确保在任务范围中定义的设备上安装了应用程序或更新。您可以通过属性窗口查看安装了应用程序或更新的设备列表。

  要查看设备列表：

  a. 单击应用程序或更新的名称。

  属性窗口打开。

  b. 打开“**设备**”区域。

  还可以在设备属性窗口中查看已安装的应用程序和更新列表。

7. 指定客户端设备将如何下载卸载实用程序：

- **使用网络代理**

  通过这些客户端设备上安装的网络代理将文件传送到客户端设备。

  如果禁用此选项，则使用 Microsoft Windows 工具传送文件。

  如果任务已分配给安装了网络代理的设备，我们建议您启用此选项。

- **通过管理服务器使用操作系统资源**

  使用管理服务器操作系统工具将文件传输到客户端设备。如果客户端设备上未安装网络代理，但是客户端设备与管理服务器在同一网络，则可以启用此选项。

- **通过分发点使用操作系统资源**

  使用操作系统工具通过分发点将文件传输到客户端设备。如果网络中存在不止一个分发点，则可以启用此选项。

  如果启用“**使用网络代理**”选项，仅当网络代理工具不可用时才通过操作系统工具传送文件。

- **同时下载的最大数量**

  管理服务器可以同时向其传输文件的最大允许客户端设备数。该数字越大，应用程序的卸载速度越快，但管理服务器上的负载也越高。

- **尝试卸载的最大次数**

  如果在运行“*远程卸载应用程序*”任务时，Kaspersky Security Center 未能在由参数指定的安装程序运行次数内卸载受管理设备上的应用程序，Kaspersky Security Center 将停止向该受管理设备传送卸载实用程序，并且不再在该设备上启动安装程序。

  “**尝试卸载的最大次数**”参数允许您节省受管理设备资源，以及减少流量（卸载、MSI 文件运行和错误消息）。

  重复的任务启动尝试可能表示设备上存在妨碍卸载的问题。管理员应在指定的卸载尝试次数内解决问题，然后重新启动该任务（手动或按计划）。

  如果卸载始终未完成，问题被视为无法解决且后续任务启动被认为是不必要的资源和流量浪费。

  创建任务时，尝试计数器设置为 `0`。设备上的安装程序每次运行返回错误时，计数器读数都会递增。

  如果已超过参数中指定的尝试次数，且设备已准备好应用程序卸载，您可以增加“**尝试卸载的最大次数**”参数的值并启动任务以卸载应用程序。或者，您可以创建新的“*远程卸载应用程序*”任务。

- **下载之前验证操作系统类型**

  在将文件传输到客户端设备之前，Kaspersky Security Center 将检查安装实用程序设置是否适用于客户端设备的操作系统。如果设置不适用，Kaspersky Security Center 不会传输文件，也不会尝试安装应用程序。例如，要将某个应用程序安装到某个管理组的设备（这些设备运行各种操作系统），可以将安装任务分配给管理组，然后启用此选项以跳过操作系统与所需设备不同的设备。

- **使用卸载密码**

  如果您在上一步中选择了**卸载受管理应用程序**，然后在**要卸载的应用程序**字段中指定了 Kaspersky Security Center 网络代理，则会显示此参数。

  如果您之前在网络代理策略设置中设置了网络代理远程卸载的密码，请选中**使用卸载密码**复选框，然后在**密码**字段中输入卸载密码。如果您没有设置网络代理远程卸载的密码，请勿选择该复选框。

8. 指定操作系统重新启动设置：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。

  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

9. 如果必要，添加要用于启动远程卸载任务的账户：

- **不需要账户(网络代理已安装)**

  如果该选项被选中，您不是必须指定一个账户，并在该账户下运行程序的安装。将使用运行管理服务器服务的账户运行该任务。

  如果网络代理未安装在客户端设备上，该选项不可用。

- **需要账户(不使用网络代理)**

  如果您为其分配*远程卸载应用程序*任务的设备上未安装网络代理，请选择此项。在这种情况下，您可以指定用户账户或 SSH 证书来卸载应用程序。

  - **本地账户**。如果该选项被选中，请指定将运行应用程序安装程序的用户账户。单击**添加**按钮，选择**本地账户**，然后指定用户账户凭据。

    您可以指定多个用户账户，例如，没有一个账户拥有分配任务所对应的所有设备上的全部所需权限时。在此情况下，已经添加的所有账户都用于从上到下按顺序运行该任务。

  - **SSH 证书**。如果要从基于 Linux 的客户端设备上卸载应用程序，您可以指定 SSH 证书而不是用户账户。单击**添加**按钮，选择**SSH 证书**，然后指定证书的私钥和公钥。

    要生成私钥，您可以使用 ssh-keygen 实用程序。请注意，Kaspersky Security Center 支持 PEM 格式的私钥，但 ssh-keygen 实用程序默认生成 OPENSSH 格式的 SSH 密钥。Kaspersky Security Center 不支持 OPENSSH 格式。要以支持的 PEM 格式创建私钥，请在 ssh-keygen 命令中添加“-m PEM”选项。

    例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
    ```

10. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

11. 单击“**完成**”按钮。
    任务被创建并显示在任务列表。

12. 点击创建的任务的名称以打开任务属性窗口。

13. 在任务属性窗口中，指定常规任务设置。

14. 单击“**保存**”按钮。

15. 手动运行任务，或者按照任务设置中指定的计划等待任务启动。

    远程卸载任务完成后，所选应用程序从选定设备中删除。

远程卸载问题

有时远程卸载第三方应用程序可能会在结束时出现以下警告：“远程卸载已在该设备上结束，但是有警告：要移除的应用程序未安装。”当要卸载的应用程序已经被卸载或者仅为单个用户安装时，会发生该问题。如果用户未登录，则为单个用户安装的应用程序（也称为按用户发放的应用程序）不可见且无法进行远程卸载。

该行为与供多个用户在同一台设备上使用的应用程序（也称为按设备发放的应用程序）不同。按设备发放的应用程序可供设备上的所有用户看见和访问。

因此，按用户发放的应用程序必须在用户登录时才能卸载。

有关安装的应用程序的信息源

网络代理可从以下注册表键值提取有关 Windows 设备上安装的软件的信息：

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为所有用户安装的应用程序的信息。
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为所有用户安装的应用程序的信息。
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为当前用户安装的应用程序的信息。
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含有关为特定用户安装的应用程序的信息。

任务

该部分描述了 Kaspersky Security Center 使用的任务。

关于任务

Kaspersky Security Center 通过创建和运行*任务*来管理设备上安装的 Kaspersky 应用程序。安装、启用和停用程序、扫描文件、更新数据库和软件模块以及程序的其他操作均需要任务。

特定应用程序的任务可以使用 Kaspersky Security Center Web Console 创建，仅在该应用程序的管理插件安装在 Kaspersky Security Center Web Console 服务器上时。

任务可以在管理服务器和设备上执行。

管理服务器上执行的任务包含以下：

- 自动分发报告
- 将更新下载至存储库
- 备份管理服务器数据
- 数据库维护

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

  本地任务可以被管理员通过管理控制台工具修改，或者被远程设备用户修改(例如，通过安全应用程序界面)。如果本地任务同时被管理员和受管理设备用户修改，管理员的修改将生效，因为其具有更高优先级。

- *组任务* — 在特定组的所有设备上执行的任务。

  除非在任务属性中指定了其他项，组任务也影响所选组的所有子组。组任务还影响（可选）已连接到部署在该组或其任意子组中的从属和虚拟管理服务器的设备。

- *全局任务* — 在一组设备上执行的任务，与设备是否包含在某个组中无关。

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务执行结果保存在每台设备的操作系统事件日志、管理服务器上的操作系统事件日志和管理服务器数据库中。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

关于任务范围

*任务范围*是执行任务的设备集合。范围的类型包括以下：

- 对于*本地任务*，范围是设备本身。
- 对于*管理服务器任务*，范围是管理服务器。
- 对于*组任务*，范围是包含在组中的设备列表。

当创建*全局任务*时，您可以使用以下方法指定范围：

- 手动指定特定设备。

  您可以使用 IP 地址（或 IP 范围）、NetBIOS 名称或 DNS 名称作为设备地址。

- 从包含要添加的设备地址的 TXT 文件导入设备列表（每个地址必须单独一行）。

  如果通过文件导入设备列表或手动创建设备列表，且如果设备是以名称定义，则列表可以只包含其信息已被输入到管理服务器数据库中的设备。而且，信息必须在设备被连接或设备发现中输入。

- 指定设备分类。

  后续，任务范围随着包含在分类中的设备集的更改而更改。设备分类可以基于设备属性（包含安装在设备上的软件）创建，也可以基于分配到设备的标签来创建。设备分类是指定任务范围的最灵活的方法。

  设备分类的任务总是按管理服务器计划运行。这些任务无法运行在缺少管理服务器连接的设备上。使用其他方法指定范围的任务直接运行在设备上，且因此不取决于到管理服务器的设备连接。

设备分类的任务不会按设备本地时间运行；相反，它们将按照管理服务器本地时间运行。使用其他方法指定范围的任务以设备本地时间运行。

创建任务

要创建任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵循其说明。
3. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。
4. 单击“**完成**”按钮。

任务被创建并显示在任务列表。

要创建分配给所选设备的新任务：

1. 在主菜单中，转到“**资产(设备)**”→“**受管理设备**”。

   将显示受管理设备列表。

2. 在受管理设备列表中，选中设备旁边的复选框以为其运行任务。您可以使用搜索和过滤功能来查找您正在寻找的设备。

3. 单击**运行任务**按钮，然后选择**添加一个新任务**。

   “新任务向导”启动。

   在向导的第一步中，您可以删除被选择包括在任务范围中的设备。按照向导的说明进行操作。

4. 单击“**完成**”按钮。

任务为选定的设备创建。

手动启动任务

应用程序根据每个任务的属性中指定的计划设置来启动任务。您可以随时从任务列表中手动启动任务。或者，您也可以在“**受管理设备**”列表中选择设备，然后对这些设备启动现有任务。

要手动启动任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。

2. 在任务列表中，选中要启动的任务旁边的复选框。

3. 单击“**开始**”按钮。

任务启动。您可以在“**状态**”列中或单击“**结果**按钮”来检查任务状态。

查看任务列表

您可以查看在 Kaspersky Security Center 中创建的任务列表。

要查看任务列表，

在主菜单中，转到“**资产(设备)**” → “**任务**”。

将显示任务列表。这些任务按与它们相关的应用程序的名称分组。例如，“*远程卸载应用程序*”任务与管理服务器相关，“*查找漏洞和所需更新*”任务涉及网络代理。

要查看任务的属性，

单击任务的名称。

将显示任务属性窗口，其中包含几个已命名的选项卡。例如，“**任务类型**”显示在“**常规**”选项卡上，任务计划显示在“**计划**”选项卡上。

常规任务设置

本部分包含您可以查看并为大多数任务配置的设置。可用设置列表取决于您正在配置的任务。

任务创建过程中指定的设置

您可以在创建任务时指定以下设置。一些设置也可以在所创建任务的属性中修改。

- 操作系统重启设置：
  - **不重启设备**

    客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

  - **重启设备**

    如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

  - **提示用户操作**

    客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

    默认情况下已选定该选项。

  - **重复提示间隔(分钟)**

    如果启用该选项，应用程序以指定频率提示用户重启操作系统。

    默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于1和1440 分钟之间。

    如果禁用该选项，提示仅显示一次。

  - **在该时间后重启(分钟)**

    提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

    默认情况下已启用该选项。默认延时是 30 分钟。可用值介于1和1440 分钟之间。

  - **强行关闭锁定会话中的应用程序**

    运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

    如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

默认情况下已禁用该选项。

- 任务计划设置：

  计划的类型可能根据任务而有所不同。

  - **启动任务设置：**

    - **每 N 小时**

      任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

      默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

    - **每 N 天**

      任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

      默认下，任务每天运行一次，从当前系统日期和时间开始。

    - **每 N 分钟**

      任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

      默认下，任务每 30 分钟运行一次，从当前系统时间开始。

    - **按星期中的天数**

      任务在每周指定日期的指定时间定期运行。

      默认情况下，任务在每周五 6:00:00 PM 运行。

    - **每月**

      任务定期运行，在指定月日的指定时间。

      在缺少指定日的月份，任务在最后一天运行。

      默认下，任务在每月的第一天运行，在当前系统时间。

    - **手动**

      任务不自动运行。您仅可以手动启动。

      默认情况下已选定该选项。

- **一次**

  该任务在指定的日期和时间运行一次（默认情况下，在创建任务的当天）。

- **立即**

  任务在设置保存后立即运行。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **当新更新下载至存储库时**

  当新更新下载至存储库后任务运行。例如，您可能想要对“查找漏洞和所需更新”任务使用该计划。

- **在检测到病毒爆发时**

  任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

- 在搜索栏中输入任务名称，即可根据名称搜索任务。
- 单击排序图标可按名称对任务进行排序。
  默认情况下，任务按字母顺序升序排列。
- 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- 要分配任务的设备：

  - **选择管理服务器检测到的网络设备**

    任务被分配到特定设备。特定设备可以包含管理组的设备和未分配的设备。

    例如，您可能要在安装网络代理到未分配的设备的任务中使用该选项。

  - **手动指定设备地址或从列表导入地址**

    您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

    您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- **分配任务到设备分类**

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。
  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

- **分配任务到管理组**

  任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
  例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。
  如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

- 账户设置：

  - **默认账户**

    在与执行该任务的应用程序相同的账户下运行该任务。
    默认情况下已选定该选项。

  - **指定账户**

    填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

  - **账户**

    运行该任务的账户。

  - **密码**

    任务运行时使用的账户的密码。

任务创建后指定的设置

您可以在创建任务后指定以下设置。

- 组任务设置：

  - **分发到子组**

    此选项仅在组任务的设置中可用。
    启用此选项后，任务范围包括：
    - 您在创建任务时选择的管理组。
    - 从属于按组层次结构向下的任何级别的选定管理组的管理组。

    禁用此选项后，任务范围仅包括您在创建任务时选择的管理组。

默认情况下已启用该选项。

- **分发到从属和虚拟管理服务器**

  启用此选项后，在主管理服务器上有效的任务也将应用于从属管理服务器（包括虚拟管理服务器）。如果从属管理服务器上已经存在相同类型的任务，则两个任务都将应用于从属管理服务器—现有任务和从主管理服务器继承的任务。

  仅当启用“**分发到子组**”选项时，此选项才可用。

  默认情况下已禁用该选项。

- 高级计划设置：

  - **使用 Wake-On-LAN 功能在任务启动之前开启设备**

    设备上的操作系统在任务开始之前的指定时间启动。默认时间段为五分钟。

    如果您想要任务在任务范围内的所有客户端设备上运行，包括任务要启动时关闭的设备，则启用该选项。

    如果您希望在任务完成后自动关闭设备，请启用“**任务完成后关闭设备**”选项。可以在同一窗口中找到此选项。

    默认情况下已禁用该选项。

  - **任务完成后关闭设备**

    例如，您可能想为每周五工作时间后安装更新到客户端设备的更新安装任务启用该选项，然后在周末关闭这些设备。

    默认情况下已禁用该选项。

  - **如果任务运行超过该时间则停止**

    在指定时间段过后，任务被自动停止，无论它是否完成。

    如果您想要中断或停止执行时间太长的任务，则启用该选项。

    默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

- 通知设置：

  - **保存任务历史记录**块：

    - **存储在管理服务器数据库上(天)**

      有关任务范围内所有客户端设备上的任务执行的应用程序事件在指定的天数内被存储在管理服务器。当该时间段过后，信息被从管理服务器删除。

      默认情况下已启用该选项。

- **存储在设备的 OS 事件日志中**

  有关任务执行的应用程序事件被存储在每个客户端设备的本地 Windows 事件日志中。

  默认情况下已禁用该选项。

- **存储在管理服务器的 OS 事件日志中**

  有关任务范围内所有客户端设备上的任务执行的应用程序事件被集中存储在管理服务器操作系统的 Windows 事件日志中。

  默认情况下已禁用该选项。

- **保存所有事件**

  如果选择该选项，所有任务相关事件被保存到事件日志。

- **保存任务进度相关事件**

  如果选择该选项，仅任务执行相关事件被保存到事件日志。

- **仅保存任务执行结果**

  如果选择该选项，仅任务结果相关事件被保存到事件日志。

- **通知管理员任务执行的结果**

  您可以选择管理员接收任务执行通知的方法：通过电子邮件、通过 SMS 和通过运行可执行文件。要配置通知，请单击“**设置**”链接。

  默认下，所有通知方法被禁用。

- **仅通知错误**

  如果该选项被启用，管理员仅在任务执行完成但带有错误时被通知。

  如果该选项被禁用，管理员在每次任务执行完成后被通知。

  默认情况下已启用该选项。

- 安全设置。

- 任务范围设置。

  取决于任务范围决定的方式，以下设置被展现：

  - **设备。**

    如果任务范围由管理组决定，您可以查看该组。这里不可以更改。然而，您可以设置**任务范围排除项**。

如果任务范围由设备列表决定，您可以通过添加和删除设备修改该列表。

- **设备分类**

  您可以更改应用程序任务的设备分类。

- **任务范围排除项**

  您可以指定应用任务的设备组。要排除的组仅可以是应用任务的管理组的子组。

- **修订历史**。

导出任务

Kaspersky Security Center 允许您将任务及其设置保存到 KLT 文件。您可以使用此 KLT 文件将保存的任务导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要导出任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 选中要导出的任务旁边的复选框。
   您不能同时导出多个任务。如果您选择了多个任务，**导出**按钮将被禁用。管理服务器任务也将无法导出。
3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定任务文件的名称和路径。单击“**保存**”按钮。
   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则任务文件会自动保存在“**下载**”文件夹。

导入任务

Kaspersky Security Center 允许您从 KLT 文件导入任务。KLT 文件包含导出的任务及其设置。

要导入任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**导入**”按钮。
3. 单击**浏览**按钮选择要导入的任务文件。
4. 在打开的窗口中，指定 KLT 任务文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个任务文件。
   任务处理启动。

5. 任务成功处理后，选择要向其分配任务的设备。为此，请选择以下选项之一：

- **分配任务到管理组**

  任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。

  例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。

  如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

- **手动指定设备地址或从列表导入地址**

  您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- **分配任务到设备分类**

  该任务被分配到设备分类中的设备。您可以指定现有分类之一。

  例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

6. 指定任务范围。

7. 单击**完成**按钮以完成任务导入。

出现包含导入结果的通知。如果任务成功导入，可以单击“**详细资料**”链接以查看任务属性。

成功导入后，任务会显示在任务列表中。任务设置和时间表也会一起导入。任务将根据其时间表启动。

如果新导入的任务与现有任务具有相同的名称，则导入的任务在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

启动更改任务密码向导

对于非本地任务，可以指定必须在其下运行任务的账户。您可以在任务创建过程中或在现有任务的属性中指定账户。如果根据组织的安全性说明使用了指定的账户，则这些说明可能需要不时更改账户密码。账户密码过期且您设置了新密码后，任务将无法启动，直到您在任务属性中指定了新的有效密码。

更改任务密码向导使您可以在指定账户的所有任务中自动将旧密码替换为新密码。或者，您可以在每个任务的属性中手动更改此密码。

要启动更改任务密码向导：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。

2. 单击**管理启动任务的账户凭证**。

   遵照向导的说明操作。

步骤 1：指定凭证

指定系统中（例如，Active Directory 中）当前有效的新凭据。当您切换到向导的下一步时，Kaspersky Security Center 将检查指定的账户名是否与每个非本地任务的属性中的账户名匹配。如果账户名匹配，则任务属性中的密码将自动替换为新的密码。

要指定新账户，请选择一个选项：

- **使用当前账户**

  该向导使用您当前登录 Kaspersky Security Center Web Console 所使用的账户名。然后手动在“**在任务中使用的当前密码**”字段中指定账户密码。

- **指定不同账户**

  指定必须启动任务的账户名。然后在“**在任务中使用的当前密码**”字段中指定账户密码。

如果您填写“**先前密码(可选，如果您要使用当前密码替换它)**”字段，Kaspersky Security Center 仅为找到账户名和旧密码的任务替换密码。替换将自动执行。在所有其他情况下，您必须选择要在向导的下一步执行的操作。

步骤 2：选择要采取的操作

如果未在向导的第一步中指定先前密码，或者指定的旧密码与任务属性中的密码不匹配，则必须选择要对找到的任务执行的操作。

要选择对任务的操作：

1. 选中要对其选择操作的任务旁边的复选框。
2. 执行以下操作之一：
   - 要删除任务属性中的密码，请单击“**删除凭证**”。
     任务将切换为在默认账户下运行。
   - 要将密码替换为新密码，请单击“**即便旧密码错误或未指定也强制密码更改**”。
   - 要取消密码更改，请单击“**未选择操作**”。

移至向导的下一步后，将应用所选操作。

步骤 3：查看结果

在向导的最后一步，查看每个找到的任务的结果。要完成向导，请单击**完成**按钮。

创建“远程执行脚本”任务

您可以创建“*远程执行脚本*”任务来在客户端设备上执行安装包并远程安装应用程序。

安装包包含一个 ZIP 压缩文件，其中包含一组用于在客户端设备上执行的脚本以及一个 manifest.json 文件。在本文中了解有关创建此类安装包的更多信息。

> 此任务只能在具有 Linux 网络代理的设备上启动。

要启动“远程执行脚本”任务：

1. 转到“**新任务向导**”并选择“**远程执行脚本**”任务类型。
2. 输入任务名称并选择将分配任务的设备。单击“**下一步**”按钮。
3. 根据 ZIP 压缩文件选择一个带有 manifest.json 文件的安装包，用于远程执行。

   如果您不想在已完成该任务的设备上重新运行该任务，请打开“**不在已完成此任务的设备上启动此任务**”选项。
4. 选择账户以运行该任务。

   如果选择默认账户，则该任务将由网络代理（root 账户）执行。

   > 当“*远程执行脚本*”任务启动时，无法更改分配给它的账户。要更改任务分配到的账户，请在任务设置中停止任务，然后使用正确的账户详细信息重新创建任务。
5. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。
6. 单击“**完成**”按钮。

   “*远程执行脚本*”任务创建完成并显示在任务列表。

> 从“*远程执行脚本*”任务接收数据后，网络代理会限制所有用户（管理员和任务设置中指定的用户除外）对接收的数据的访问。

使用“远程执行脚本”任务在设备上远程安装应用程序

可以使用“*远程执行脚本*”任务通过创建自定义安装包在客户端设备上远程安装应用程序。

在本文中了解如何为此任务准备压缩文件。

要创建用于在客户端设备上远程安装应用程序的安装包，您为此任务上传的压缩文件中必须包含以下文件：

- <包名称>.deb
- **install.sh**

  ```
  sudo apt-get install <包名称>.deb
  ```

- **manifest.json**

  远程安装应用程序的 JSON 架构

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "< 如果需要，请输入参数 >",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

  数组描述

  1. version—清单文件和任务的版本。

     目前唯一可接受的值是 1。

  2. actions 数组的元素决定了任务中执行的脚本的组成和顺序。

     脚本的执行顺序对应于数组中元素的索引（位置）。

  3. 对于 actions 数组的每个元素，定义了以下元素。

     a. type—脚本中可执行命令的类型。目前，该值始终为 execute。

     b. path—压缩文件中脚本文件的路径。

     c. args—作为可执行命令的一部分传递给脚本的参数。

     d. results—根据任务结果定义进一步操作的数组。

        1. code—返回脚本的值。

        2. next—下一步要完成的操作。 continue 操作表示继续执行下一个脚本（actions 数组中的元素）； break 操作表示停止任务。

     e. default_next—如果脚本返回的值不包含在 results 中而执行的操作。

当“*远程执行脚本*”任务启动时，网络代理会将安装包与应用程序一起上传到客户端设备。当客户端设备接收到安装包后，该设备上的网络代理会解析 manifest.json 文件，并根据结果定义脚本和操作的执行顺序并开始执行。

当“*远程执行脚本*”任务完成后，应用程序将安装到客户端设备上。

配置“远程执行脚本”任务的通知和监控

您可以为“*远程执行脚本*”任务配置监控、事件保存行为和通知。

要查看“远程执行脚本”任务的状态：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
   将显示任务列表。
2. 选择任务并单击“**设备历史**”。
   显示任务的进度。

要配置事件保存行为：

1. 在任务列表中，单击任务并转到“**设置**”选项卡。
2. 在“**通知**”部分中，单击“**设置**”按钮。
3. 选择以下选项之一来确定任务完成后应用程序的行为方式：
   - **保存所有事件**。
   - **保存任务进度相关事件**。
   - **仅保存任务执行结果**。
     事件保存在“**设备历史**”和“**事件存储库**”中。
     默认只保存任务执行结果。

     > 若选择“**保存所有事件**”，则仅保存任务执行结果。
4. 如果您要将事件保留在管理服务器数据库、管理服务器事件日志或设备上，请启用相应的选项。

在本文中了解有关配置通知的更多信息。

为“远程执行脚本”任务准备压缩文件

基于 manifest.json 文件的“*远程执行脚本*”任务的压缩文件必须满足以下要求：

- 压缩文件格式：ZIP。
- 总大小：不超过 1 GB。
- 压缩文件中的文件和文件夹的数量不受限制。
- 压缩文件的清单文件必须与下面的架构匹配，并且必须命名为 manifest.json。仅在设备上执行任务期间验证架构。
  清单文件的 JSON 架构和数组的描述

JSON 架构

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
```

```
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

清单文件示例

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- 压缩文件的结构必须如下：

  `manifest.json`

  `<file1>`

```
<file2>
<folder1>/<file3>
<folder2>/<folder3>/<file4>
...
<fileX>
```

manifest.json 是该任务的清单文件。

`<file1>, ...., <fileX>` 是包含待执行脚本的文件集合。

根据清单文件创建安装包

要根据清单文件创建安装包：

1. 执行以下操作之一：
   - 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**安装包**”。
   - 在主菜单中，转到“**操作**”→ “**存储库**” → “**安装包**”。

   此时会显示管理服务器上可用的安装包的列表。
2. 单击**添加**。
   新安装包向导启动。使用“**下一步**”按钮继续向导操作。
3. 选择“**基于带有 manifest.json 文件的 ZIP 压缩包，为“远程执行脚本”任务创建一个安装包**”。
4. 指定包名称并单击“**浏览**”按钮。
   一个标准 Windows“**打开**”窗口将在浏览器中打开，以允许您选择一个文件来创建安装包。
5. 选择可用磁盘上的压缩文件。在本文中了解如何为此任务准备压缩文件。
   该文件开始上传至 Kaspersky Security Center 管理服务器。
   创建安装包的过程将开始。
   该向导将在过程完成时通知您。
   如果未创建安装包，则会显示相应的消息。
6. 单击**完成**按钮关闭向导。

您创建的安装包将下载到管理服务器共享文件夹的 Packages 子文件夹中。下载后，安装包出现在安装包列表。

在管理服务器上的可用安装包列表中，通过单击带有自定义安装包名称的链接，您可以：

- 查看安装包的以下属性：
  - **名称。**自定义安装包名称。
  - **源。**应用程序供应商名称。
  - **版本。**应用程序版本。
  - **创建日期。**安装包创建日期。

- **修改日期。**安装包修改日期。
- **路径。**管理服务器上自定义安装包的路径。

- 更改安装包名称和命令行参数。该功能仅适用于未根据卡巴斯基应用程序创建的安装包。

管理客户端设备

Kaspersky Security Center 允许您管理客户端设备：

- 查看受管理设备的设置和状态，包括群集和服务器阵列。
- 配置分发点。
- 管理任务。

您可以使用管理组将客户端设备合并成一组，并作为一个单元进行管理。一个客户端设备只能包含在一个管理组中。设备可根据 **规则条件** 自动分配到组中：

- 创建设备移动规则。
- 复制设备移动规则。
- 设备移动规则的条件。

您可以使用设备分类来根据条件筛选设备。您还可以标记设备以创建分类、查找设备以及将设备分配到各管理组中。

受管理设备设置

要查看受管理设备设置：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
   将显示受管理设备列表。
2. 在受管理设备列表中，单击带有所需设备名称的链接。

将显示所选设备的属性窗口。

以下选项卡显示在代表主要设置组的属性窗口的上部：

- **常规**

  此选项卡包括以下区域：
  - “**常规**”区域显示有关客户端设备的常规信息。信息基于上一次客户端设备与管理服务器之间的同步接收的数据来提供：
    - **名称**

在该字段中，您可以查看和修改管理组中的客户端设备名称。

- **描述**

  在该字段中，您可以输入客户端设备的附加描述。

- **设备状态**

  基于管理员定义的标准分配的关于设备上反病毒保护和网络中设备活动的客户端设备的状态。

- **完整组名称**

  包括了客户端设备的管理组。

- **反病毒数据库上次更新**

  设备上病毒数据库或应用程序最后更新日期。

- **连接到管理服务器**

  客户端设备上安装的网络代理上一次连接到管理服务器的日期和时间。

- **上一次可见**

  设备在网络中最后可见的日期和时间。

- **网络代理版本**

  安装的网络代理的版本。

- **创建日期**

  Kaspersky Security Center 内的设备创建日期。

- **设备所有者**

  设备所有者的名称。您可以作为设备所有者，通过单击**管理设备所有者**链接分配或删除用户。

- **不断开与管理服务器的连接**

  如果启用此选项，将保持受管理设备和管理服务器之间的持续连接。如果正在使用的不是提供此类连接的推送服务器，您可能希望使用此选项。

如果禁用此选项且推送服务器不在使用中，受管理设备将仅在同步数据或传输信息时连接至管理服务器。

选中“**不断开与管理服务器的连接**”选项时的最大设备总数为 300。

默认情况下已在受管理设备上禁用该选项。此选项在安装了管理服务器的设备上默认启用，即使您尝试禁用它也保持启用状态。

- “**网络**”部分显示有关客户端设备的网络属性的以下信息：
  - **IP 地址**

    设备 IP 地址。
  - **Windows 域**

    包含设备的 Windows 域或工作组。
  - **DNS 名称**

    客户端设备的 DNS 域名称。
  - **NetBIOS 名称**

    客户端设备的 Windows 网络名。
  - **IPv6 地址**
- “**系统**”区域提供有关安装在客户端设备上的操作系统的信息。
  - **操作系统**
  - **CPU 架构**
  - **设备名称**
  - **虚拟机类型**

    虚拟机制造商。
  - **作为 VDI 一部分的动态虚拟机**

    此行显示客户端设备是否是作为 VDI 一部分的动态虚拟机。
- “**保护**”区域提供有关客户端设备上反病毒保护当前状态的以下信息：
  - **可见**

    客户端设备的可见状态。

- **设备状态**

  基于管理员定义的标准分配的关于设备上反病毒保护和网络中设备活动的客户端设备的状态。

- **状态描述**

  客户端设备保护和与管理服务器连接的状态。

- **保护状态**

  该字段显示当前的客户端设备实时保护状态。
  当设备状态更改时，新状态仅在客户端设备与管理服务器同步之后显示在设备属性窗口。

- **上一次全盘扫描**

  客户端设备上次执行恶意软件扫描的日期和时间。

- **检测到的病毒**

  自安装安全应用程序（第一次扫描）或自上次重置威胁计数器以来，在客户端设备上检测到的威胁总数。

- **清除失败的对象**

  客户端设备上的未处理文件数量。
  该字段移动设备上的未处理文件数量。

- **磁盘加密状态**

  设备本地驱动器上的当前文件加密状态。有关状态的说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

- "**应用程序定义的设备状态**"区域提供有关由安装在设备上的受管理应用程序定义的设备状态的信息。该设备状态可能与 Kaspersky Security Center 定义的状态不同。

- **应用程序**

  该选项卡列出了客户端设备上安装的所有卡巴斯基应用程序。该选项卡包含**开始**和**停止**按钮，可让您启动和停止所选的卡巴斯基应用程序（不包括网络代理）。如果受管理设备上的15000 UDP 端口可用，则可以使用这些按钮来接收来自管理服务器的推送通知。如果受管理设备无法接收推送通知，但启用了与管理服务器的持续连接模式（启用了**不断开与管理服务器的连接**部分中的**常规**选项），则**开始**和**停止**按钮也可用。否则，当您尝试启动或停止应用程序时，将显示一条错误消息。您也可以单击应用程序名称以查看有关该应用程序的常规信息、发生在设备上的事件的列表以及应用程序设置。

- **活动策略和策略配置文件**

  此选项卡列出了当前分配给受管理设备上的策略和策略配置文件。

- **任务**

  在“**任务**”选项卡上，您可以管理客户端设备任务：查看现有任务列表、创建新任务、删除、启动和停止任务、修改任务设置以及查看执行结果。该任务列表由客户端最近一次与管理服务器进行同步的会话期间收到的数据提供。管理服务器请求客户端设备的任务状态详情。如果受管理设备上的15000 UDP 端口可用于接收来自管理服务器的推送通知，则会显示任务状态并启用用于管理任务的按钮。如果推送服务器无法触达受管理设备，但启用了与管理服务器的持续连接模式（启用了**常规**部分中的**不断开与管理服务器的连接**选项），则也可以使用对任务的操作。

  如果未建立连接，则不显示状态，按钮被禁用。

- **事件**

  “**事件**”选项卡将显示选定客户端设备在管理服务器上所记录的事件。

  您可以导出、复制和删除设备事件。

- **安全问题**

  在**安全问题**选项卡上，可以为客户端设备查看、编辑和创建安全问题。安全问题可以通过安装在客户端设备上的受管 Kaspersky 应用程序自动创建，也可以由管理员手动创建。例如，如果用户定期将恶意软件从其可移动驱动器移至设备，则管理员可以创建安全问题。管理员可以在安全问题文本中提供情况的简要说明和建议的操作（例如对于一个用户的纪律性操作），还可以添加链接到用户。

  对其采用了所有必要操作的安全问题被称为*已处理安全问题*。存在的未处理安全问题可被选为将设备的状态更改为*严重*或*警告*的条件。

  此部分包含已为设备创建的安全问题的列表。安全问题按严重级别和类型分类。安全问题类型由创建安全问题的卡巴斯基应用程序定义。选中**已处理**列中的复选框即可突出显示列表上的已处理安全问题。

- **标签**

  在“**标签**”区域，您可以管理用于查找客户端设备的关键字列表：查看现有标签列表、从列表中分配标签、配置自动标记规则、添加新标签和重命名旧标签以及删除标签。

- **高级**

  此选项卡包括以下区域：

  - **应用程序注册表**。在此区域，您可以查看客户端设备上安装的应用程序及其更新的注册表，您还可以设置应用程序注册表的显示。

    如果客户端设备上安装的网络代理将所需信息发送到管理服务器，则将提供有关已安装应用程序的信息。您可以在网络代理或其策略的属性窗口中的“**存储库**”区域中配置将信息发送到管理服务器。

    单击应用程序名称将打开一个窗口，其中包含应用程序详细信息以及为该应用程序安装的更新安装包的列表。

  - **可执行文件**。此区域显示在客户端设备上发现的可执行文件。

- **分发点**。该区域提供设备与之交互的分发点列表。

  - **导出到文件**

    单击“**导出到文件**”按钮保存设备与之交互的分发点列表文件。默认下，程序导出设备列表到 CSV 文件。

  - **属性**

    单击“**属性**”按钮查看和配置设备与之交互的分发点。

- **硬件注册表**。在此区域，您可以查看客户端设备上安装的硬件的信息。

  如果网络代理安装在运行 Windows 的设备上，它会向管理服务器发送有关设备硬件的以下信息：

  - RAM
  - 大容量存储设备
  - 主板
  - CPU
  - 网络适配器
  - 监控器
  - 视频适配器
  - 声卡

  如果网络代理安装在运行 Linux 或 macOS 的设备上，它会向管理服务器发送有关设备硬件的以下信息（如果该信息由操作系统提供）：

  - 总 RAM 容量
  - 大容量存储设备总容量
  - 主板
  - CPU
  - 网络适配器

- **可用更新**。该区域显示在该设备上发现的未安装的软件更新列表。

- **软件漏洞**。此区域提供有关客户端设备上安装的第三方应用程序中的漏洞信息。

  要将漏洞保存到文件中，请选择要保存的漏洞旁边的复选框，然后单击“**导出到 CSV**”按钮或“**导出到 TXT**”按钮。

  此部分包含以下设置：

  - **仅显示可以被修复的漏洞**

如果启用此选项，该区域会显示可通过使用补丁修复的漏洞。

如果禁用此选项，该区域会同时显示可通过使用补丁修复的漏洞，以及未发布补丁的漏洞。

默认情况下已启用该选项。

- **漏洞属性**

  单击列表中的软件漏洞名称，以在单独的窗口中查看所选软件漏洞的属性。在窗口中，您可以执行以下操作：

  - 忽略此受管理设备上的软件漏洞（在管理控制台或 Kaspersky Security Center Web Console 中）。
  - 查看该漏洞的建议修复程序列表。
  - 手动指定软件更新以修复漏洞（在管理控制台或 Kaspersky Security Center Web Console 中）。
  - 查看漏洞实例。
  - 查看现有任务列表以修复漏洞，并创建新任务以修复漏洞。

- **远程诊断**。在此区域，您可以执行远程诊断客户端设备。

如果您使用 PostgreSQL、MariaDB 或 MySQL DBMS，则**事件**选项卡可能会显示所选客户端设备的不完整事件列表。当 DBMS 存储大量事件时就会发生这种情况。您可以通过执行以下操作之一来增加显示的事件数量：

- 删除不必要的事件。
- 减少不必要事件的存储期限。

要查看设备管理服务器上记录的完整事件列表，请使用报告。

创建管理组

安装 Kaspersky Security Center 后，管理组层次结构仅包含一个名为“**受管理设备**”的管理组。当创建管理组层次结构时，您可以将设备（包括虚拟机）添加到“**受管理设备**”组，并添加嵌套组（请参见下图）。

查看管理组层次结构

要创建管理组，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 在管理组结构中，选择要包括新管理组的管理组。
3. 单击“**添加**”按钮。
4. 在打开的“**新管理组名称**”窗口中，输入组的名称，然后单击“**添加**”按钮。

   一个具有指定名称的新管理组将出现在管理组层次结构中。

程序允许基于活动目录的架构或域网架构创建管理组结构。您也可以从文本文件创建组架构。

要创建管理组结构：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 单击“**导入**”按钮。

   新管理组结构向导启动。遵照向导的说明操作。

手动将设备添加到管理组

您可以通过创建设备移动规则来自动将设备移动到管理组，或通过将设备从一个管理组移动到另一管理组或将设备添加到选定的管理组来手动移动设备。本部分介绍如何手动将设备添加到管理组。

要手动将一台或多台设备添加到选定的管理组：

1. 在主菜单中，转到**资产(设备)** → **受管理设备**。
2. 单击列表上方的“**当前路径：** <当前路径>”链接。
3. 在打开的窗口中，选择您要添加到设备的管理组。
4. 单击“**添加设备**”按钮。
   移动设备向导启动。
5. 生成要添加到管理组的设备列表。

   您只能添加在连接设备时或设备发现后其信息已经添加至管理服务器数据库的设备。

选择要将设备添加到列表的方式：

- 单击“**添加设备**”按钮，然后通过以下方式之一指定设备：
  - 从管理服务器检测到的设备列表中选择设备。
  - 指定设备 IP 地址或 IP 范围。

    IP地址范围不得包含超过1,048,576个地址。

  - 指定设备的 NetBIOS 名称或 DNS 名称。

    设备名称字段不得包含空格或以下禁止的字符：\ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
- 单击“**从文件导入设备**”按钮以从 .txt 文件导入设备列表。每个设备地址或名称都必须在单独一行中指定。

  该文件不得包含空格或以下禁止的字符：\ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. 查看要添加到管理组的设备列表。您可以通过添加或删除设备来编辑列表。
7. 确保列表正确后，单击“**下一步**”按钮。

向导将处理设备列表并显示结果。处理成功的设备将添加到管理组并以管理服务器生成的名称显示在设备列表中。

手动将设备或者集群移动至管理组

您可以将设备从一个管理组移动到另一个管理组，或从未分配的设备组移动到管理组。

您还可以将集群或服务器阵列从一个管理组移动到另一个管理组。当您将集群或服务器阵列移动到另一个组时，其所有节点都会随之移动，因为集群及其任何节点始终属于同一管理组。当您在“**设备**”选项卡上选择单个集群节点时，“**移动到组**”按钮将变得不可用。

要将一台或多台设备或者集群移动到选定的管理组：

1. 打开要从中移动设备的管理组。为此，请执行以下操作之一：
   - 要打开管理组，请在主菜单中转到“**资产(设备)**”→“**受管理设备**”，单击“**当前路径**”字段中的路径链接，然后在打开的左侧窗格中选择一个管理组。
   - 要打开“**未分配的设备**”组，请转到“**发现和部署**”→“**未分配的设备**”。
2. 如果管理组包含集群或服务器阵列，则“**受管理设备**”区域将被分为两个选项卡：“**设备**”选项卡和“**集群和服务器阵列**”选项卡。打开要移动的对象的选项卡。
3. 选中要移动到其他组的设备或者集群旁边的复选框。
4. 单击**移动到组**按钮。

5. 在管理组的层级中，选中要将选定设备或者集群移动到的管理组旁边的复选框。

6. 单击“**移动**”按钮。

选定设备或者集群将被移动到选定管理组。

创建设备移动规则

您可以设置设备移动规则，即自动分配设备到管理组的规则。

要创建移动规则：

1. 在主菜单中，转到“**资产(设备)**”→“**移动规则**”。

2. 单击**添加**。

3. 在打开的窗口中，在“**常规**”选项卡上指定以下信息：

- **规则名称**

  输入新规则名称。
  如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。

- **管理组**

  选择要自动移动设备的管理组。

- **激活的规则**

  如果启用该选项，规则被启用并在被保存后开始工作。
  如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。

- **仅移动不属于任何管理组的设备**

  如果启用该选项，仅未分配的设备将被移动到所选组。
  如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。

- **应用规则**

  您可以选择以下选项之一：
  - **对每台设备运行一次**
    规则对匹配标准的每台设备应用一次。
  - **对每台设备运行一次，然后在每次网络代理重新安装时**
    规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。

- **持续应用规则**
  规则根据管理服务器自动设置的计划被应用（通常每几个小时）。

4. 在“**规则条件**”选项卡上，指定至少一个标准，设备将依据该标准移至管理组。
5. 单击“**保存**”。

移动规则被创建。它显示在移动规则列表。

列表上的位置越高，规则的优先级越高。要提高或降低移动规则的优先级，请使用鼠标在列表中分别向上或向下移动规则。

如果选择了“**持续应用规则**”选项，则移动规则的应用与优先级设置无关。这些规则会根据管理服务器自动设置的时间表来应用。

如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

复制设备移动规则

您可以复制移动规则，例如，如果您要对不同目标管理组拥有几个相同规则。

要复制现有移动规则：

1. 执行以下操作之一：
   - 在主菜单中，转到“**资产(设备)**”→“**移动规则**”。
   - 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**移动规则**”。

   移动规则列表被显示。
2. 选择您要复制的规则旁边的复选框。
3. 单击**复制**。
4. 在打开的窗口中的“**常规**”选项卡上更改以下信息或不进行任何更改（如果您仅想复制规则而不更改其设置）：
   - **规则名称**

     输入新规则名称。
     如果您正复制规则，新规则与源规则名称相同，但是索引格式 () 被添加到名称，例如：(1)。
   - **管理组**

     选择要自动移动设备的管理组。

- **激活的规则**

  如果启用该选项，规则被启用并在被保存后开始工作。
  如果禁用该选项，规则被创建，但不被启用。直到您启用该选项它才工作。

- **仅移动不属于任何管理组的设备**

  如果启用该选项，仅未分配的设备将被移动到所选组。
  如果禁用该选项，已经属于其他管理组的设备以及未分配的设备将被移动到所选组。

- **应用规则**

  您可以选择以下选项之一：

  - **对每台设备运行一次**
    规则对匹配标准的每台设备应用一次。
  - **对每台设备运行一次，然后在每次网络代理重新安装时**
    规则对匹配标准的每台设备应用一次，然后仅在网络代理被重新安装到这些设备时。
  - **持续应用规则**
    规则根据管理服务器自动设置的计划被应用（通常每几个小时）。

5. 在“**规则条件**”选项卡上，为您希望自动移动的设备指定至少一个标准。
6. 单击“**保存**”。

新移动规则被创建。它显示在移动规则列表。

设备移动规则的条件

当创建或复制将客户端设备移动到管理组的规则时，在“**规则条件**”选项卡上设置移动设备的条件。要确定移动哪些设备，可以使用以下标准：

- 分配给客户端设备的标签。
- 网络参数。例如，您可以移动具有指定范围内 IP 地址的设备。
- 安装在客户端设备上的受管理应用程序，例如网络代理或管理服务器。
- 虚拟机，即客户端设备。
- 有关具有客户端设备的 Active Directory 组织单元 (OU) 的信息。
- 有关具有客户端设备的云段的信息。

您可以在下面找到有关如何在设备移动规则中指定此信息的说明。

如果在规则中指定多个条件，AND 逻辑运算符将生效并且所有条件同时适用。如果不选择任何选项或将某些字段留空，则此类条件不适用。

标签选项卡

在该选项卡上，可以基于先前添加到客户端设备描述的设备标签配置设备移动规则。为此，请选择所需标签。此外，还可以启用以下选项：

- **应用到没有指定标签的设备**

  如果启用此选项，则具有指定标签的所有设备都将从设备移动规则中排除。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

  默认情况下已禁用该选项。

- **如果至少一个指定的标签匹配则应用**

  如果启用此选项，则设备移动规则将应用于具有至少一个选定标签的客户端设备。如果禁用此选项，则设备移动规则应用于具有所有选定标签的设备。

  默认情况下已禁用该选项。

网络选项卡

在此选项卡上，可以指定设备移动规则考虑的设备的网络数据：

- **Windows 网络中的设备名**

  设备的 Windows 网络名称（NetBIOS 名称）或者 IPv4 或 IPv6 地址。

- **Windows 域**

  设备移动规则应用于指定 Windows 域中包含的所有设备。

- **设备的 DNS 名称**

  要移动的客户端设备的 DNS 域名。如果网络包含 DNS 服务器，请填写此字段。

  如果为您用于 Kaspersky Security Center 的数据库设置了区分大小写的排序规则，请在指定设备 DNS 名称时保持大小写。否则，设备移动规则将不起作用。

- **DNS 域**

  设备移动规则应用于指定主 DNS 后缀中包含的所有设备。如果网络包含 DNS 服务器，请填写此字段。

- **IP 范围**

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。

  默认情况下已禁用该选项。

- **用于连接管理服务器的 IP 地址**

  如果启用此选项，则可以设置客户端设备用于连接到管理服务器的 IP 地址。为此，请指定包含所有必要 IP 地址的 IP 范围。

  默认情况下已禁用该选项。

- **设备在 IP 范围中**

  如果启用此选项，您可以选择之前在**IP 范围**部分添加的 IP 范围。相关设备必须包含在所选的 IP 范围内。

  默认情况下已禁用该选项。

- **连接配置文件已更改**

  您可以选择以下值之一：

  - **是**。设备移动规则仅应用于连接配置文件已更改的客户端设备。
  - **否**。设备移动规则仅应用于连接配置文件未更改的客户端设备。
  - **未选择值**。条件不适用。

- **由不同管理服务器管理**

  您可以选择以下值之一：

  - **是**。设备移动规则仅应用于由其他管理服务器管理的客户端设备。这些服务器与配置了设备移动规则的服务器不同。
  - **否**。设备移动规则仅应用于当前管理服务器管理的客户端设备。
  - **未选择值**。条件不适用。

应用程序选项卡

在此选项卡上，可以根据客户端设备上安装的受管理应用程序和操作系统来配置设备移动规则：

- **网络代理已安装**

  您可以选择以下值之一：

  - **是**。设备移动规则仅应用于安装了网络代理的客户端设备。
  - **否**。设备移动规则仅应用于未安装网络代理的客户端设备。
  - **未选择值**。条件不适用。

- **应用程序**

  指定应在客户端设备上安装哪些受管理应用程序，以便设备移动规则应用于这些设备。例如，您可以选择 Kaspersky Security Center 15.1 **网络代理** 或 Kaspersky Security Center 15.1 **管理服务器**。

如果不选择任何受管理应用程序，则条件不适用。

- **操作系统版本**

  您可以根据操作系统版本剔除客户端设备。为此，请指定应在客户端设备上安装的操作系统。结果是，设备移动规则应用于具有选定操作系统的客户端设备。

  如果不启用此选项，则条件不适用。默认情况下，禁用该选项。

- **操作系统 bit 大小**

  您可以按操作系统位数来剔除客户端设备。在“**操作系统 bit 大小**”字段中，您可以选择以下值之一：

  - **未知**
  - **x86**
  - **AMD64**
  - **IA64**

  要检查客户端设备的操作系统位数：

  1. 在主菜单中，转到**资产(设备)** → **受管理设备**区域。
  2. 单击右侧的“**列设置**”按钮 ( )。
  3. 选择**操作系统 bit 大小**选项，然后单击**保存**按钮。

     之后，将显示每个受管理设备的操作系统位数。

- **操作系统服务包版本**

  在该字段中，可以指定操作系统的更新包版本（采用 *X.Y* 格式），这将决定将移动规则应用到设备的方式。默认情况下，不指定版本值。

- **用户证书**

  您可以选择以下值之一：

  - **已安装**。设备移动规则仅应用于具有移动证书的移动设备。
  - **未安装**。设备移动规则仅应用于没有移动证书的移动设备。
  - **未选择值**。条件不适用。

- **操作系统内部版本**

  该设置仅应用到 Windows 操作系统。

您可以指定所选操作系统是否必须具有相等、更早或更晚的版本号。您也可以为除指定内部版本号外的所有内部版本号配置设备移动规则。

- **操作系统发布号**

  该设置仅应用到 Windows 操作系统。

  您可以指定所选操作系统必须具有相同、更早还是更晚的版本号。您也可以为除指定版本号外的所有版本号配置设备移动规则。

虚拟机选项卡

在该选项卡上，可以根据客户端设备是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来配置设备移动规则：

- **这是一台虚拟机**

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动非虚拟机设备。
  - **是**。移动虚拟机设备。

- **虚拟机类型**

- **虚拟桌面基础架构的一部分**

  在该下拉列表中，可以选择以下选项之一：
  - **N/A**。条件不适用。
  - **否**。移动不属于 VDI 的设备。
  - **是**。移动属于 VDI 的设备。

域控制器选项卡

在此选项卡上，您可以指定需要移动域组织单元中包含的设备。您还可以从指定域组织单元的所有子组织单元移动设备：

- **设备包含在以下组织单元中**

  如果启用此选项，则设备移动规则将应用于该选项下的列表中指定的域组织单元中的设备。

  默认情况下已禁用该选项。

- **包括子组织单元**

  如果启用此选项，选择范围将包括指定域组织单元的所有子组织单元中的设备。
  默认情况下已禁用该选项。

- **将设备从子单元移动到对应子组**
- **创建对应于新检测到设备的容器的子组**
- **删除域中不存在的子组**
- **设备包含在以下域安全组中**

  如果启用此选项，设备移动规则将应用于该选项下的列表中指定的域安全组中的设备。
  默认情况下已禁用该选项。

云段选项卡

在此选项卡上，您可以指定需要移动属于特定云段的设备：

- **设备在云段中**

  如果选择此选项，则设备移动规则将应用于属于云段的客户端设备。您可以在该选项下的列表中选择需要添加至子网的云段。
  默认情况下，禁用该选项。

- **包含子对象**

  如果选择此选项，则设备移动规则不仅适用于选择的云段，还适用于该段的子对象。
  默认情况下，禁用该选项。

- **从嵌套对象移动设备到对应子组**
- **创建对应于新检测到设备的容器的子组**
- **删除在云段中未找到匹配的子组**
- **使用 API 发现的设备**

  在下拉列表，您可以选择设备是否由 API 工具检测：
  - **AWS**。设备使用 AWS API 发现，即设备确定在 AWS 云环境中。
  - **Azure**。设备使用 Azure API 发现，即设备确定在 Azure 云环境中。
  - **Google Cloud**。设备使用 Google API 发现，即设备确定在 Google Cloud 环境中。

- **否**。无法使用 AWS API、Azure API 或 Google API 检测到该设备，即设备位于云环境之外，或者位于云环境中，但是无法使用 API 检测到该设备。
- **没有值**。此条件不适用。

关于集群和服务器阵列

Kaspersky Security Center 支持集群技术。如果网络代理向管理服务器发送信息确认组成服务器阵列的客户端设备上已安装该应用程序，则该客户端设备就成为一个集群节点。

如果管理组包含集群或服务器阵列，则“**受管理设备**”页面将显示两个选项卡：一个用于单个设备，另一个用于集群和服务器阵列。受管理设备被检测为集群节点后，集群将被作为单独对象添加到“**集群和服务器阵列**”选项卡。

集群或服务器阵列节点与其他受管理设备一起列在**设备**选项卡上。您可以将节点作为单个设备查看属性并执行其他操作，但不能删除集群节点或将其从集群中单独移动到另一个管理组。您只能删除或移动整个集群。

您可以对集群或服务器阵列执行以下操作：

- 查看属性
- 将集群或服务器阵列移至另一个管理组

  当您将集群或服务器阵列移动到另一个组时，其所有节点都会随之移动，因为集群及其任何节点始终属于同一管理组。
- 删除

  仅当集群或服务器阵列不在组织网络中存在时，删除该集群或服务器阵列才合理。如果集群在您的网络上仍然可见，并且网络代理和卡巴斯基安全应用程序仍然安装在集群节点上， Kaspersky Security Center 会自动将已删除的集群及其节点返回到受管理设备列表。

集群或服务器阵列的属性

要查看集群或服务器阵列的设置：

1. 在主菜单中，转到“**资产(设备)**”→“**受管理设备**”→“**集群和服务器阵列**”。

   集群和服务器阵列的列表将显示。
2. 单击所需集群或服务器阵列的名称。

所选集群或服务器阵列的属性窗口将显示。

常规

常规部分显示有关集群或服务器阵列的常规信息。信息基于上一次集群节点与管理服务器之间的同步接收的数据来提供：

- **名称**
- **描述**

- **Windows 域**

  Windows 域或工作组，包含集群或服务器阵列。

- **NetBIOS 名称**

  集群或服务器阵列的 Windows 网络名称。

- **DNS 名称**

  集群或服务器阵列的 DNS 域名称。

任务

在“**任务**”选项卡中，您可以管理分配给集群或者服务器阵列的任务：查看现有任务列表；创建新任务；删除、启动和停止任务；修改任务设置；查看执行结果。列出的任务与安装在集群节点上的卡巴斯基安全应用程序相关。Kaspersky Security Center 从集群节点接收任务列表和任务状态详细信息。如果未建立连接，则不显示状态。

节点

此选项卡显示集群或服务器阵列中包含的节点列表。您可以单击节点名称来查看设备属性窗口。

卡巴斯基应用程序

属性窗口还可能包含其他选项卡，其中包含与集群节点上安装的卡巴斯基安全应用程序相关的信息和设置。

当设备显示不活动时查看和配置操作

如果组中的客户端设备不活动，您可以获取关于它的通知。您也可以自动删除此类设备。

要在组中设备显示不活动时查看或配置操作：

1. 在主菜单中，转到“**资产(设备)**”→“**组层级**”。
2. 单击所需管理组的名称。
   管理组属性窗口将开启。
3. 在属性窗口中，转到“**设置**”选项卡。
4. 在“**继承**”区域中，启用或禁用以下选项：

   - **从父组继承**

     该区域的设置将从包含客户端设备的父组继承。如果启用该选项，“**网络中的设备活动**”下的设置将被锁定以阻止更改。
     该选项仅在管理组拥有父组时可用。

默认情况下已启用该选项。

- **在子组中强制继承设置**

  该设置值将被分发到子组，但在子组的属性中这些设置被锁定。

  默认情况下已禁用该选项。

5. 在“**设备活动**”区域中，启用或禁用以下选项：

   - **当设备处于非活动状态超过指定天数时，通知管理员**

     如果启用该选项，管理员接收不活动设备的通知。您可以指定**设备在网络上已长时间没有活动**事件被创建的时间间隔。默认时间间隔是 7 天。

     默认情况下已启用该选项。

   - **当设备处于非活动状态超过指定天数时，从组中删除设备**

     如果启用该选项，您可以指定设备被从组中自动移除的时间间隔。默认时间间隔是 60 天。

     默认情况下已启用该选项。

6. 点击“**保存**”。

   您的更改已保存并应用。

关于设备状态

Kaspersky Security Center 为每个受管理设备都分配一个状态。具体状态取决于是否满足用户定义的条件。在某些情况下，为设备分配状态时，Kaspersky Security Center 会考虑设备在网络中的可见性标志（请参见下表）。例如，如果某个受管理设备因满足“*数据库已过期*”条件而被分配“*严重*”状态，稍后为设备设置了可见性标志，则该设备被分配“*正常*”状态。如果 Kaspersky Security Center 在两小时内未在网络中找到设备，则该设备的可见性标志将设置为“*不可见*”。

状态如下：

- “*严重*”或“*严重/可见*”
- “*警告*”或“*警告/可见*”
- “*正常*”或“*正常/可见*”

下表列出了为设备分配“*严重*”或“*警告*”状态所必须满足的默认条件，以及所有可能值。

分配状态到设备的条件

条件	条件描述	可用值
安全应用程序未安装	网络代理已安装到设备，但是安全应用程序未安装。	• 开关按钮被开启。 • 开关按钮被关闭。

条件	条件描述	可用值
检测到太多病毒	一些病毒被病毒检测任务在设备上发现，例如，*恶意软件扫描*任务，且发现的病毒数量超过指定值。	超过 0。
实时保护级别与管理员设置的级别不同	设备在网络中可见，但实时保护级别与管理员在设备状态条件中设置的级别不同。	• 已停止。 • 已暂停。 • 正在运行。
恶意软件扫描已长时间未执行	设备在网络中可见且安全应用程序已安装到设备，但不论*恶意软件扫描*任务还是本地扫描任务都没有在指定时间内未运行。条件仅应用到于 7 天之前或更早添加到管理服务器数据库的设备。	超过1天。
数据库已过期	设备在网络中可见且安全应用程序已安装到设备，但反病毒数据库在指定时间内未在该设备上更新。条件仅应用到于1天之前或更早添加到管理服务器数据库的设备。	超过1天。
长时间没有连接	网络代理已安装到设备，但由于设备关闭，设备在指定时间段内未连接到管理服务器。	超过1天。
检测到活动威胁	"**活动威胁**"文件夹中的未处理的对象的数量超过指定的值。	超过 0 项。
需要重新启动	设备在网络中可见，但应用程序基于所选原因之一在指定时间之前请求设备重启。	超过 0 分钟。
安装了不兼容的应用程序	设备在网络中可见，但通过网络代理执行的软件清查在设备上检测到了不兼容的应用程序。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到软件漏洞	设备在网络中可见且网络代理已安装到设备，但"*查找漏洞和所需更新*"任务在设备应用程序中检测到指定严重级别的漏洞。	• 严重。 • 高。 • 中。 • 如果漏洞无法被修复则忽略。 • 如果为安装分配了更新则忽略。
授权许可已过期	设备在网络中可见，但授权许可已过期。	• 开关按钮被关闭。 • 开关按钮被开启。
授权许可即将过期	设备在网络中可见，但设备上的授权许可即将在指定天数内过期。	少于 0 天。

条件	条件描述	可用值
Windows Update 更新检查已长时间未执行	设备在网络中可见，但“*执行 Windows 更新同步*”任务在指定时间段内未运行。	超过 1 天。
无效的加密状态	网络代理已安装到设备，但设备加密结果等于指定值。	• 由于用户拒绝未遵从策略(仅对外部设备)。 • 由于错误未遵从策略。 • 应用策略时需要重启。 • 未指定加密策略。 • 不支持。 • 当应用策略时。
移动设备设置不遵从策略	移动设备设置不同于 Kaspersky Endpoint Security for Android 策略中指定的设置。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到未处理的安全问题	设备上发现了一些未处理的安全问题。安全问题可以通过安装在客户端设备上的受管卡巴斯基应用程序自动创建，也可以由管理员手动创建。	• 开关按钮被关闭。 • 开关按钮被开启。
应用程序定义的设备状态	设备状态由受管理应用程序定义。 无论 Kaspersky Security Center 的设置如何，受管理设备的状态都可能由受管理应用程序定义。当此状态返回一个由 Kaspersky Security Center 定义的状态后，管理服务器将为受管理设备分配一个最终状态。该状态选自以下两者中最为严重的一项：受管理应用程序返回的状态和管理服务器分配的状态。受管理应用程序定义的状态会附带由受管理应用程序传输的描述。您可以在受管理设备列表的“**状态描述**”列中查看这些描述。	• 开关按钮被关闭。 • 开关按钮被开启。
设备磁盘空间不足	设备剩余磁盘空间少于指定值或设备无法与管理服务器同步。当设备已与管理服务器成功同步且设备上的剩余空间大于或等于指定值时，*严重*或*警告*状态被更改为*正常*状态。	大于 0 MB。
设备已失去管理	在设备发现过程中，设备在网络中可见，但是超过三次尝试与管理服务器同步都失败了。	• 开关按钮被关闭。 • 开关按钮被开启。
保护已禁用	设备在网络中可见，但设备上的安全应用程序已被禁用长于指定的时间段。 在这种情况下，安全应用程序的状态为*stopped*或*failure*，不同于以下状态：*starting*、*running*或*suspended*。	超过 0 分钟。
安全应用程序没有运行	设备在网络中可见且安全应用程序已安装到设备，但其未在运行。	• 开关按钮被关闭。 • 开关按钮被开启。

Kaspersky Security Center 允许您设置管理组中设备状态在指定条件满足时的自动切换。当指定条件满足时，客户端设备被分配以下状态之一：*严重*或*警告*。未满足指定条件时，客户端设备被分配“*正常*”状态。

一个条件的不同值可对应于不同的状态。例如，默认情况下，如果“**数据库已过期**”条件的值为“**超过 3 天**”，将为客户端设备分配“*警告*”状态；如果值为“**超过 7 天**”，则将分配“*严重*”状态。

如果从以前的版本升级 Kaspersky Security Center，则分配“*严重*”或“*警告*”状态所对应的“**数据库已过期**”状态值不变。

配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

要启用更改设备状态到严重：

1. 在主菜单中，转到“**资产(设备)**”→ “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**严重**”。
5. 在右侧窗格的“**设置状态为“严重”，如果这些被指定**”区域中，启用将设备切换为“*严重*”状态的条件。

   > 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。

满足指定条件时，受管理设备被分配*严重*状态。

要启用更改设备状态到警告：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**警告**”。
5. 在右侧窗格的“**设置状态为“警告”，如果这些被指定**”区域中，启用将设备切换为“*警告*”状态的条件。

   > 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。

满足指定条件时，受管理设备被分配*警告*状态。

远程连接至客户端设备桌面

管理员可以通过客户端设备上安装的网络代理获取对设备的远程访问权限。即使客户端设备的 TCP 和 UDP 端口关闭，也可以通过网络代理远程连接至设备。

在与设备建立连接后，管理员会获取对此设备上存储的信息的完全访问权限，以便他或她可以管理其上安装的应用程序。

目标受管理设备的操作系统设置中必须允许远程连接。例如，在 Windows 10 中，此选项为“**允许远程协助连接这台计算机**”（您可以在“**控制面板**”→“**系统和安全**”→“**系统**”→“**远程设置**”中找到此选项）。如果您拥有“漏洞和补丁管理”功能的授权许可，则可以在建立与受管理设备的连接时强制启用此选项。如果您没有授权许可，请在目标受管理设备上本地启用此选项。如果禁用此选项，将无法进行远程连接。

要建立与设备的远程连接，您必须有两个实用程序：

- 名为 klsctunnel 的 Kaspersky 实用程序。该实用程序必须存储在管理员的工作站上。使用此实用程序在客户端设备和管理服务器之间建立隧道连接。

  Kaspersky Security Center 允许通过管理服务器的从管理控制台的 TCP 连接通道，然后通过网络代理到受管理设备上的指定端口。通道设计用于连接网络控制台设备上的客户端应用程序到受管理设备上的 TCP 端口—如果管理控制台和目标设备之间没有直接连接可用。

  如果用于连接到管理服务器的端口在设备上不可用，则需要客户端设备和管理服务器之间的连接隧道。在以下情况下设备端口可能不可用：

  - 远程设备连接到使用 NAT 装置的本地网络。
  - 远程设备是本地网络管理服务器的一部分，但是它的端口被防火墙关闭。

- 名为“远程桌面连接”的标准 Microsoft Windows 组件。根据标准 Windows 实用工具 mstsc.exe 的设置通过该实用工具建立到远程桌面的连接。

  在用户不知道的情况下远程连接到用户的当前桌面会话。一旦管理员连接会话，设备用户将在没有提前通知的情况下从会话断开连接。

要连接到客户端设备的桌面：

1. 在基于 MMC 的管理控制台中，在管理服务器策略的上下文菜单中选择“**属性**”。
2. 在打开的管理服务器属性窗口中，转到“**管理服务器连接设置**”→“**连接端口**”。
3. 确保“**为 Kaspersky Security Center Web Console 打开远程桌面协议端口**”选项已启用。
4. 在 Kaspersky Security Center Web Console 中，转到**资产(设备)→受管理设备**。
5. 在受管理设备列表上方的**当前路径**字段中，单击路径链接。
6. 在打开的左侧窗格中，选择包含您要访问的设备的管理组。
7. 选中要获取访问权限的设备名称旁边的复选框。
8. 单击**连接到远程桌面**按钮。

   远程桌面 (仅 Windows)窗口打开。

9. 启用“**允许受管理设备上的远程桌面连接**”选项。在这种情况下，即使当前受管理设备的操作系统设置中禁止远程连接，也将建立连接。

   仅当您拥有“漏洞和补丁管理”功能的授权许可时，此选项才可用。

10. 单击“**下载**”按钮以下载 klsctunnel 实用程序。

11. 单击“**复制到剪贴板**”按钮从文本字段复制文本。此文本是一个二进制大型对象 (BLOB)，其中包含在管理服务器和受管理设备之间建立连接所需的设置。

    BLOB 有效期为 3 分钟。如果 BLOB 已过期，请重新打开“远程桌面 (仅 Windows)”窗口以生成新的 BLOB。

12. 运行 klsctunnel 实用程序。

    该实用程序窗口打开。

13. 将复制的文本粘贴到文本字段中。

14. 如果使用代理服务器，请选中“**使用代理服务器**”复选框，然后指定代理服务器连接设置。

15. 单击“**打开端口**”按钮。

    将打开远程桌面连接登录窗口。

16. 指定您当前用来登录 Kaspersky Security Center Web Console 的账户的凭据。

17. 单击“**连接**”按钮。

在与设备建立连接后，可以在 Microsoft Windows 的远程连接窗口使用桌面。

通过 Windows 桌面共享连接至客户端设备

管理员可以通过客户端设备上安装的网络代理获取对设备的远程访问权限。即使客户端设备的 TCP 和 UDP 端口关闭，也可以通过网络代理远程连接至设备。

管理员可以连接至客户端设备上的现有会话而不会断开此会话中的用户。在这种情况下，设备上的管理员和会话用户将共享桌面访问权限。

要建立与设备的远程连接，您必须有两个实用程序：

- 名为 klsctunnel 的 Kaspersky 实用程序。该实用程序必须存储在管理员的工作站上。使用此实用程序在客户端设备和管理服务器之间建立隧道连接。

  Kaspersky Security Center 允许通过管理服务器的从管理控制台的 TCP 连接通道，然后通过网络代理到受管理设备上的指定端口。通道设计用于连接网络控制台设备上的客户端应用程序到受管理设备上的 TCP 端口—如果管理控制台和目标设备之间没有直接连接可用。

  如果用于连接到管理服务器的端口在设备上不可用，则需要客户端设备和管理服务器之间的连接隧道。在以下情况下设备端口可能不可用：

  - 远程设备连接到使用 NAT 装置的本地网络。
  - 远程设备是本地网络管理服务器的一部分，但是它的端口被防火墙关闭。

- Windows 桌面共享。当连接到远程桌面的现有会话时，设备上的会话用户会收到来自管理员的连接请求。Kaspersky Security Center 创建的报告中不会保存有关设备上的远程活动及其结果的任何信息。

  管理员可以在远程客户端设备上配置用户活动的审核。审核期间，应用程序会保存有关客户端设备上管理员打开和/或修改过的文件的信息。

要通过 Windows 桌面共享连接到客户端设备的桌面，必须符合以下条件：

- 管理员的工作站上安装了 Microsoft Windows Vista 或更高版本。管理服务器设备操作系统的类型对通过 Windows 桌面共享进行连接没有限制。

  要检查您的 Windows 版本是否包含 Windows 桌面共享功能，请确保 Windows 注册表中包含 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 密钥。

- 客户端设备上安装了 Microsoft Windows Vista 或更高版本。

- Kaspersky Security Center 已安装漏洞和补丁管理授权许可。

要通过 Windows 桌面共享连接到客户端设备的桌面：

1. 在基于 MMC 的管理控制台中，在管理服务器策略的上下文菜单中选择“**属性**”。
2. 在打开的管理服务器属性窗口中，转到“**管理服务器连接设置**”→“**连接端口**”。
3. 确保“**为 Kaspersky Security Center Web Console 打开远程桌面协议端口**”选项已启用。
4. 在 Kaspersky Security Center Web Console 中，转到**资产(设备)→受管理设备**。
5. 在受管理设备列表上方的**当前路径**字段中，单击路径链接。
6. 在打开的左侧窗格中，选择包含您要访问的设备的管理组。
7. 选中要获取访问权限的设备名称旁边的复选框。
8. 单击**Windows 桌面共享**按钮。

   Windows 桌面共享向导打开。
9. 单击“**下载**”按钮下载 klsctunnel 实用程序，等待下载过程完成。

   如果已有 klsctunnel 实用程序，请跳过此步骤。
10. 单击“**下一步**”按钮。
11. 选择要连接的设备上的会话，然后单击“**下一步**”按钮。
12. 在目标设备上的打开的对话框中，用户必须允许桌面共享会话。否则，会话无法进行。

    设备用户确认桌面共享会话后，向导的下一页将打开。
13. 单击“**复制到剪贴板**”按钮从文本字段复制文本。此文本是一个二进制大型对象 (BLOB)，其中包含在管理服务器和受管理设备之间建立连接所需的设置。

    > BLOB 有效期为 3 分钟。如果已过期，请生成一个新的 BLOB。

14. 运行 klsctunnel 实用程序。

    该实用程序窗口打开。

15. 将复制的文本粘贴到文本字段中。

16. 如果使用代理服务器，请选中“**使用代理服务器**”复选框，然后指定代理服务器连接设置。

17. 单击“**打开端口**”按钮。

桌面共享在新窗口中启动。如果要与设备互动，请单击窗口左上角的“菜单”图标 ( )，然后选择**交互模式**。

设备分类

*设备分类*是根据特定条件筛选设备的工具。您可以使用设备分类管理几个设备：例如，查看仅查看这些设备的报告或移动所有这些设备到其他组。

Kaspersky Security Center 提供大量的*预定义分类*（例如，**处于“严重”状态的设备**、**保护已禁用**、**检测到活动威胁**）。预定义分类无法被删除。您也可以创建和配置附加*用户定义分类*。

在用户定义分类中，您可以设置搜索范围并选择所有设备、受管理设备、或者未分配的设备。搜索参数在条件中指定。在设备分类中，您可以创建带有不同搜索参数的多个条件。例如，您可以创建两个条件并指定不同的 IP 范围。如果多个条件被指定，分类显示满足任意条件的设备。相比之下，条件中的搜索参数是附加的。如果 IP 范围和已安装应用程序名称都被指定在一个条件，仅安装了应用程序且 IP 地址处于指定范围的设备被显示。

从设备分类中查看设备列表

Kaspersky Security Center 允许您从设备分类中查看设备列表。

若要从设备分类中查看设备列表：

1. 在主菜单中，转到“**资产(设备)** → **设备分类**或者**发现和部署** → **设备分类**”区域。

2. 在分类列表中，单击设备分类的名称。
   该页面会显示一个表格，其中包含有关设备分类中包含的设备的信息。

3. 您可以按如下方式对设备表中的数据进行分组和筛选：

   - 单击设置图标 ( )，然后选择要在表中显示的列。

   - 单击筛选图标 ( )，然后在调用的菜单中指定并应用筛选条件。
     筛选出的设备表将显示。

您可以在设备分类中选择一个或多个设备，然后单击**新任务**按钮以创建将被应用于这些设备的任务。

要将设备分类中的选定设备移动到另一个管理组，请单击**移动到组**按钮，然后选择目标管理组。

创建设备分类

要创建设备分类，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**”→“**设备分类**”。
   将显示含有设备分类列表的页面。

2. 单击“**添加**”按钮。
   “**设备分类设置**”窗口打开。

3. 输入新分类的名称。

4. 指定包含要被包括在设备分类中的设备的组：

   - **查找任何设备**– 搜索符合选择标准并被包括在**受管理设备**或**未分配的设备**组中的设备。
   - **查找受管理设备** – 搜索符合选择标准并被包括在**受管理设备**组中的设备。
   - **查找未分配的设备**– 搜索符合选择标准并被包括在**未分配的设备**组中的设备。

   您可以启用**包含来自从属管理服务器的数据**复选框以启用搜索满足选择条件并由从属管理服务器管理的设备。

5. 单击“**添加**”按钮。

6. 在打开的窗口中，指定要将设备包括在此分类中所必须满足的条件，然后单击“**确定**”按钮。

7. 单击“**保存**”按钮。

设备分类即被创建并添加到设备分类列表中。

配置设备分类

要配置设备分类：

1. 在主菜单中，转到“**资产(设备)**” → “**设备分类**”。
   将显示含有设备分类列表的页面。

2. 选择相关的用户自定义设备分类，然后单击“**属性**”按钮。
   “**设备分类设置**”窗口打开。

3. 在**常规**选项卡上，单击**新条件**链接。

4. 指定包含设备到该分类必须满足的条件。

5. 单击“**保存**”按钮。

设备被应用并保存。

以下是分配设备到分类的条件描述。多个条件使用 OR 逻辑运算符组合在一起：选择范围将包含至少符合列出的一个条件的设备。

常规

在“**常规**”区域，您可以更改分类条件的名称，指定条件是否必须被倒转：

反转分类条件

默认情况下已禁用该选项。

如果启用此选项，指定的分类条件将倒转。此分类将包含所有不符合该条件的设备。

以下示例展示了反转工作的逻辑：

- **条件**：您的设备上存在操作系统类型为 Linux 且内部版本号为 00.0.000 的设备。
- **反转条件**：您的设备上存在操作系统类型为非 Linux 且内部版本号为非 00.0.000 的设备，这等价于：存在操作系统类型为非 Linux 或内部版本号为非 00.0.000 的设备。

因此，选择范围将包括操作系统类型为 Windows 且内部版本号为 00.0.000 的设备，或者 Linux 且内部版本号不为 00.0.000 的设备。

网络基础架构

在“**网络**”子区域，您可以指定根据网络数据包含设备到分类的标准：

- **设备名称**

  设备的 Windows 网络名称（NetBIOS 名称）或者 IPv4 或 IPv6 地址。

- **域**

  显示指定的 Windows 域中包括的所有设备。

- **管理组**

  显示指定的管理组中包括的设备。

- **描述**

  设备属性窗口中的文本：在“**常规**”区域的“**描述**”字段。
  要描述“**描述**”字段中的文本，您可以使用以下字符：
  - 在单词中：
    - *****。用任意数量的字符替换任何字符串。

    例如：
    要描述单词 **Server** 或 **Server's**，您可以输入 **Server***。

    - **?**。替换任意单个字符。

    例如：
    要描述单词 **Window** 或 **Windows**，您可以输入 **Windo?**。
    星号(*)或问号(?)不能用于查询中的第一个字符。

  - 要查找多个单词：
    - 空格。显示所有在其描述中包含列出的任何单词的设备。

例如:
要查找包含“**从属**”或“**虚拟**”单词的短语，可以在查询中包含“**从属 虚拟**”行。

- **+**。当单词带有加号前缀时，所有搜索结果都将包含该单词。

例如:
要查找同时包含“**从属**”和“**虚拟**”的短语，请输入“**+从属+虚拟**”查询。

- **-**。当单词带有减号前缀时，所有搜索结果都不包含该单词。

例如:
要查找包含“**从属**”但不包含“**虚拟**”的短语，请输入“**+从属-虚拟**”查询。

- **“<某些文本>”**。引号中围绕的文本必须存在于文本中。

例如:
要查找包含“**从属服务器**”单词组合的短语，可以在查询中输入“**从属服务器**”。

- **IP 范围**

  如果启用此选项，您可以输入应该包括相关设备的 IP 范围的初始和最终 IP 地址。
  默认情况下已禁用该选项。

- **由不同管理服务器管理**

  您可以选择以下值之一:
  - **是**。设备移动规则仅应用于由其他管理服务器管理的客户端设备。这些服务器与配置了设备移动规则的服务器不同。
  - **否**。设备移动规则仅应用于当前管理服务器管理的客户端设备。
  - **未选择值**。条件不适用。

在“**域控制器**”子区域，您可以配置基于域成员包含设备到分类的标准:

- **设备在域组织单元中**

  如果启用此选项，选择范围将包括输入字段中指定的域组织单元中的设备。
  默认情况下已禁用该选项。

- **该设备是域安全组成员**

  如果启用此选项，选择范围将包括输入字段中指定的域安全组中的设备。
  默认情况下已禁用该选项。

在“**网络活动**”子区域，您可以指定根据网络活动包含设备到分类的标准：

- **作为分发点**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

  - **是**。选择范围将包括充当分发点的设备。
  - **否**。选择范围将不包括充当分发点的设备。
  - **未选择值**。将不应用标准。

- **不断开与管理服务器的连接**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

  - **已启用**。分类将包含选中了“**不断开与管理服务器的连接**”复选框的设备。
  - **已禁用**。分类将包含清空了“**不断开与管理服务器的连接**”复选框的设备。
  - **未选择值**。将不应用标准。

- **连接配置文件已切换**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：

  - **是**。该分类将包含连接配置文件切换后连接到管理服务器的设备。
  - **否**。该分类将不包含连接配置文件切换后连接到管理服务器的设备。
  - **未选择值**。将不应用标准。

- **上一次连接到管理服务器**

  您可使用此选框设置按上一次连接到管理服务器的时间搜索设备的标准。

  如果选择该选框，则在输入字段中，您可以指定在客户端设备上安装的网络代理和管理服务器之间建立上一次连接的时间间隔（日期和时间）。选择将包括位于指定间隔的设备。

  如果清除此选框，则将不会应用标准。

  默认情况下已清除该选框。

- **网络轮询时检测到新设备**

  搜索最近几天通过网络轮询检测到的新设备。

  如果启用此选项，分类将只包括在“**检测周期 (天)**”字段中指定的天数内通过设备发现检测到的新设备。

  如果禁用此选项，分类将包括通过设备发现检测到的所有设备。

  默认情况下已禁用该选项。

- **设备可见**

  在下拉列表中，可设置执行搜索时在分类中包含设备的标准：
  - **是**。程序在分类中包括网络中当前可见的设备。
  - **否**。应用程序在分类中包括网络中当前不可见的设备。
  - **未选择值**。将不应用标准。

在“**云段**”子区域，您可以配置根据相关云段包含设备到分类的标准：

- **设备在云段中**

  如果启用此选项，您可以从 AWS、Azure 和 Google 云段中选择设备。
  如果还启用“**包含子对象**”选项，将在选定段的所有子对象上运行搜索。
  搜索结果仅包含所选段的设备。

- **使用 API 发现的设备**

  在下拉列表，您可以选择设备是否由 API 工具检测：
  - **是**。使用 AWS、Azure 或 Google API 检测设备。
  - **否**。无法使用 AWS、Azure 或 Google API 检测设备。即设备要么在云环境之外，要么在云环境中，但是无法通过使用 API 检测到。
  - 没有值。此条件不适用。

设备状态

在“**受管理设备状态**”子区域，您可以配置基于受管理应用程序的设备状态的描述包含设备到分类的标准：

- **设备状态**

  在该下拉列表中，您可以选择下列设备状态之一：“*正常*”、“*严重*”或“*警告*”。

- **实时保护状态**

  您可以在该下拉列表中选择实时保护状态。具有指定实时保护状态的设备将被包括在选择范围中。

- **设备状态描述**

  在该字段中，您可以选中条件旁边的选框，这些条件如果被满足，程序会为设备分配下列状态之一：*正常*、*严重* 或 *警告*。

在“**受管理应用程序组件的状态**”子区域，您可以配置根据受管理应用程序组件状态包含设备到分类的标准：

- **数据泄漏防护状态**

  根据数据泄漏防护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- **协作服务器保护状态**

  根据服务器协作保护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

- **邮件服务器的反病毒保护状态**

  根据邮件服务器保护状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）*搜索设备*。

- **端点传感器状态**

  根据端点传感器组件状态（*未知*、*已停止*、*正在启动*、*已暂停*、*运行中*、*失败*）搜索设备。

在“**影响受管理应用程序状态的问题**”子区域，您可以指定根据由受管理应用程序检测到的可能问题列表包含设备到分类的标准。如果至少一个您选择的问题存在于设备，设备将被包含到分类。当您选择几个应用程序的问题时，您可以选择在所有列表中自动选择该问题。

您可以选择受管理应用程序状态描述的复选框；接收这些状态时，设备将被包含在分类。当您选择几个应用程序的状态时，您可以选择在所有列表中自动选择该状态。

系统详情

在“**操作系统**”区域，您可以指定根据操作系统类型包含设备到分类的标准。

- **平台类型**

  如果选中该选框，您可以从列表中选择一个操作系统。安装了指定操作系统的设备会包含在搜索结果中。

- **操作系统服务包版本**

  在该字段中，可以指定操作系统的更新包版本（采用 *X.Y* 格式），这将决定将移动规则应用到设备的方式。默认情况下，不指定版本值。

- **操作系统 bit 大小**

  在该下拉列表中，可选择操作系统的架构，这将决定将移动规则应用到设备（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。默认情况下，不选择列表中的任何选项，这样就不会对操作系统的架构进行定义。

- **操作系统内部版本**

  该设置仅应用到 Windows 操作系统。

  操作系统版本号。您可以指定所选操作系统是否必须具有相等、更早或更晚的版本号。您也可以配置对所有版本号的搜索，除了指定版本号。

- **操作系统发布号**

  该设置仅应用到 Windows 操作系统。

  操作系统发布 ID。您可以指定所选操作系统是否必须具有相等、更早或更晚的发布 ID。您也可以配置对所有版本 ID 号的搜索，除了指定的版本 ID 号。

在“**虚拟机**”区域，您可以设置基于它们是否是虚拟机或虚拟桌面基础架构 (VDI) 的一部分来包含设备到分类的标准：

- **这是一台虚拟机**

  在该下拉列表中，您可以选择以下选项：

  - **未定义**。
  - **否**。查找非虚拟机设备。
  - **是**。查找虚拟机设备。

- **虚拟机类型**

  在该下拉列表中，您可以选择虚拟机生产商。

  如果在“**这是一台虚拟机**”下拉列表中选择了“**是**”或“**不重要**”值，则该下拉列表可用。

- **虚拟桌面基础架构的一部分**

  在该下拉列表中，您可以选择以下选项：

  - **未定义**。
  - **否**。查找不属于虚拟桌面基础架构的设备。
  - **是**。查找术语虚拟桌面基础架构 （VDI） 一部分的设备。

在“**硬件注册表**”子区域，您可以配置基于所安装的硬件包含设备到分类的标准：

确保在要从中获取硬件详细信息的 Linux 设备上安装了 lshw 实用程序。根据所使用的 hypervisor，从虚拟机获取的硬件详细信息可能不完整。

- **设备**

  在该下拉列表中，您可以选择单元类型。所有带有该单元的设备被包含在搜索结果。
  该字段支持完整文本搜索。

- **供应商**

  在该下拉列表中，您可以选择单元生产商的名称。所有带有该单元的设备被包含在搜索结果。
  该字段支持完整文本搜索。

- **设备名称**

  在 Windows 网络中的设备名称。具有指定名称的设备将包括在该分类中。

- **描述**

  设备或硬件单元的描述。带有该字段中指定的描述的设备将包括在分类范围内。
  可在设备的属性窗口输入任何格式的设备描述。该字段支持完整文本搜索。

- **设备制造商**

  设备制造商的名称。被指定生产商制造的设备将包括在分类范围内。
  您可以在设备的属性窗口中输入制造商的名称。

- **序列号**

  带该字段中指定序列号的所有硬件设备将包括在该分类中。

- **清单号**

  带有该字段中指定的清单编号的设备将包括在选择范围内。

- **用户**

  该字段中指定用户的所有硬件设备都将包括在该分类中。

- **位置**

  设备或硬件单元的位置（例如，在总部或分公司）。在该字段中指定的位置部署的计算机或其他设备将包括在该分类中。

  您可以在该设备的属性窗口中以任何格式描述设备的位置。

- **CPU 时钟频率 (MHz)，从**

  CPU 的最小时钟速率。CPU 与输入字段中指定的时钟速率范围（含）相匹配的设备将包含在分类中。

- **CPU 时钟频率 (MHz)，到**

  CPU 的最大时钟速率。CPU 与输入字段中指定的时钟速率范围（含）相匹配的设备将包含在分类中。

- **虚拟 CPU 内核数量，从**

  虚拟 CPU 内核的最小数量。CPU 与输入字段中指定的虚拟核心数范围（含）匹配的设备将包含在分类中。

- **虚拟 CPU 内核数量，到**

  虚拟 CPU 内核的最大数量。CPU 与输入字段中指定的虚拟核心数范围（含）匹配的设备将包含在分类中。

- **硬盘卷(GB)，从**

  设备上硬盘的最小容量。硬盘与输入字段中指定的容量范围（含）匹配的设备将被包括在分类内。

- **硬盘卷(GB)，到**

  设备上硬盘的最大容量。硬盘与输入字段中指定的容量范围（含）匹配的设备将被包括在分类内。

- **内存大小(MB)，从**

  设备 RAM 的最小大小。RAM 与输入字段中指定的大小范围（含）匹配的设备将被包括在分类中。

- **内存大小(MB)**

  设备 RAM 的最大大小。RAM 与输入字段中指定的大小范围（含）匹配的设备将被包括在分类中。

第三方软件详情

在“**应用程序注册表**”子区域，您可以设置基于已安装的应用程序搜索设备的标准：

- **应用程序名称**

  在该下拉列表中，您可以选择应用程序。安装有指定应用程序的设备将包括在选择范围中。

- **应用程序版本**

  在该输入字段中，您可以指定选定应用程序的版本。

- **供应商**

  在该下拉列表中，您可以选择已安装应用程序的生产商。

- **应用程序状态**

  在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

- **根据更新查找**

  如果启用此选项，则搜索操作将使用相关设备内应用程序更新的有关信息来执行。选中复选框后，“**应用程序名称**”、“**应用程序版本**”和“**应用程序状态**”字段将分别更改为“**更新名称**”、“**更新版本**”和“**状态**”。

  默认情况下已禁用该选项。

- **不兼容安全应用程序名称**

  在该下拉列表中，您可以选择第三方安全应用程序。在搜索过程中，安装有指定程序的设备将包括在选择范围中。

- **应用程序标签**

  在该下拉列表中，您可以选择应用程序标签。所有安装了描述中带有所选标签的应用程序的设备都被包含在设备分类。

- **应用到没有指定标签的设备**

  如果启用此选项，分类将包含未带有所选标签的描述的设备。

  如果禁用此选项，则不应用该标准。

  默认情况下已禁用该选项。

在“**漏洞和更新**”子区域，您可以指定根据 Windows 更新源包含设备到分类的标准：

WUA 已切换到管理服务器

您可以在下拉列表中选择以下搜索选项之一：

- **是**。如果选中该选项，搜索结果会包含从管理服务器收到 Windows Update 更新的设备。
- **否**。如果选中该选项，搜索结果将包含从其它源收到 Windows Update 更新的设备。

卡巴斯基应用程序详情

在“**卡巴斯基应用程序**”子区域，您可以配置基于所选的受管理应用程序包含设备到分类的标准：

- **应用程序名称**

  在下拉列表中，可设置按卡巴斯基应用程序名称执行搜索时在分类中包括设备的标准。
  列表仅提供管理员工作站上已安装管理插件的应用程序的名称。
  如果未选择任何应用程序，则将不会应用该标准。

- **应用程序版本**

  在输入字段，可设置按卡巴斯基应用程序版本号执行搜索时在分类中包括设备的标准。
  如果未指定版本号，则将不会应用该标准。

- **关键更新名称**

  在该下拉列表中，您可以选择应用程序的状态（*已安装*、*未安装*）。已安装或未安装指定应用程序的设备，取决于所选状态，将被包含在分类。

  在输入字段中，可设置按应用程序名称或更新包编号执行搜索时在分类中包括设备的标准。
  如果字段留空，则将不会应用该标准。

- **选择模块上次更新的时间段**

  您可以使用此选项来设置按这些设备上安装的程序模块上次更新的时间搜索设备的标准。
  如果选中此选框，则您可以在输入字段中指定执行这些设备上安装的程序模块的上一次更新的时间间隔（日期和时间）。
  如果清除此选框，则将不会应用标准。
  默认情况下已清除该选框。

- **设备通过管理服务器管理**

  在该下拉列表，您可以包含通过 Kaspersky Security Center 管理的设备到分类：
  - **是**。应用程序包含通过 Kaspersky Security Center 管理的设备。
  - **否**。应用程序在分类中包含不通过 Kaspersky Security Center 管理的设备。
  - **未选择值**。将不应用标准。

- **安全应用程序已安装**

  在该下拉列表，您可以包含已安装安全应用程序的设备到分类：

  - **是**。应用程序包含安装了安全应用程序的设备到分类。
  - **否**。应用程序在分类中包含未安装安全应用程序的设备。
  - **未选择值**。将不应用标准。

在“**反病毒保护**”子区域，您可以设置基于保护状态包含设备到分类的标准：

- **数据库发布日期**

  如果选择此选项，您可以按反病毒数据库发布日期搜索客户端设备。在该输入字段中，您可以设置执行搜索的时间间隔。

  默认情况下已禁用该选项。

- **数据库记录数**

  如果启用此选项，可以按数据库记录数量搜索客户端设备。在输入字段中，您可以设置反病毒数据库记录数的上限值和下限值。

  默认情况下已禁用该选项。

- **上一次扫描**

  如果启用此选项，您可以按上次恶意软件扫描时间来搜索客户端设备。在该输入字段中，您可以指定执行上一次恶意软件扫描的时段。

  默认情况下已禁用该选项。

- **检测到的威胁**

  如果启用此选项，您可以根据发现的病毒数量来搜索客户端设备。在输入字段中，您可以设置发现病毒总数的上限值和下限值。

  默认情况下已禁用该选项。

在“**加密**”子区域中，您可以配置基于所选的加密算法包含设备到分类的标准：

加密算法

高级加密标准(AES)对称分组密码算法。在下拉列表中，您可以选择加密密钥大小(56 位、128 位、192 位或 256 位)。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

应用程序组件子区域包含在 Kaspersky Security Center Web Console 中安装了相应管理插件的那些应用程序的组件列表。

在“**应用程序组件**”子区域，您可以指定根据所选应用程序组件的状态和版本号包含设备到分类的标准：

- **状态**

  根据应用程序发送到管理服务器的组件状态搜索设备。您可以选择以下状态之一：*N/A*、*已停止*、*已暂停*、*正在开始*、*正在运行*、*已失败*、*未安装*、*不受授权许可支持*。如果安装在受管理设备上的应用程序的所选组件具有指定状态，设备被包含到设备分类。

  由应用程序发送的状态：

  - *已停止* - 组件被禁用且不在工作。
  - *已暂停* - 组件被暂停，例如，在用户在受管理应用程序上停止了保护后。
  - *正在启动* - 组件处于初始化进程中。
  - *运行中* - 组件被启用且在正常工作。
  - *已失败* - 组件操作中发生错误。
  - *未安装* - 当配置应用程序自定义安装时，用户未选择该组件以安装。
  - *不受授权许可支持* – 授权许可不涵盖所选组件。

  不同于其他状态，*N/A* 状态不由应用程序发送。该选项显示应用程序没有所选组件状态的信息。例如，这可能发生在所选组件不属于任何在设备上安装的应用程序时，或设备关闭时。

- **版本**

  根据您在列表中选择的版本号搜索设备。您可以输入版本号，例如 `3.4.1.0`，然后指定所选组件是否必须具有相同、更早或更新版本。您也可以配置对除指定版本外的所有版本进行搜索。

标签

在“**标签**”区域，您可以基于先前添加到受管理设备的描述的关键字（标签）配置包含设备到分类的标准：

如果至少一个指定的标签匹配则应用

如果启用此选项，搜索结果将显示包含带有所选标签的描述的设备。

如果禁用此选项，搜索结果将仅显示包含带有所有标签的描述的设备。

默认情况下已禁用该选项。

要将标签添加到条件，请单击**添加**按钮，然后通过单击**标签**输入字段来选择标签。指定是否在设备分类中包括或排除具有所选标签的设备。

- **所有带有此标签的设备**

  如果选择了该选项，搜索结果将显示带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

  默认情况下已选定该选项。

- **所有没有此标签的设备**

  如果选择了该选项，搜索结果将显示不带有包含了所选标签的描述的设备。要查找设备，您可以使用星号，它表示任何字符长度的字符串。

用户

在“**用户**”区域，您可以设置根据登录到操作系统的用户账户包含设备到分类的标准。

- **最后一次登录系统的用户**

  如果启用此选项，您可以选择用于配置标准的用户账户。搜索结果包含所选用户上一次登录系统的设备。

- **登录系统至少一次的用户**

  如果启用此选项，单击“**浏览**”按钮可以指定用户账户。搜索结果包含指定用户至少登录一次的设备。

从设备分类中导出设备列表

Kaspersky Security Center 允许您将设备分类中的设备信息保存并导出为 CSV 或 TXT 文件。

若要从设备分类中导出设备列表：

1. 从设备分类中打开包含设备的表格。
2. 使用以下方法之一选择要导出的设备：
   - 要选择特定设备，请选中它们旁边的复选框。
   - 要从当前表格页面选择所有设备，请选中设备表格表头中的复选框，然后选中**全选当前页面**复选框。
   - 要从表中选择所有设备，请选中设备表格表头中的复选框，然后选择**全选**复选框。
3. 单击**导出到 CSV**或**导出到 TXT**按钮。表中包含的有关所选设备的所有信息都将被导出。

请注意，如果您将筛选条件应用于设备表，则只有来自显示列的筛选数据将被导出。

在分类中从管理组中删除设备

在使用设备分类时，你可以直接从管理组中删除设备，而不是切换到包含这些设备的管理组。

要从管理组删除设备，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**设备分类**”或者“**发现和部署**” → “**设备分类**”。
2. 在分类列表中，单击设备分类的名称。
   该页面会显示一个表格，其中包含有关设备分类中包含的设备的信息。
3. 选择要删除的设备，然后单击“**删除**”。
   所选设备即从相应管理组中删除。

设备标签

Kaspersky Security Center 允许您*标记*设备。标签是设备标志，可以用于分组、描述或查找设备。分配到设备的标签可以用于创建分类、查找设备以及分发设备到管理组。

您可以手动或自动标记设备。如果您想标记单个设备，则可以使用手动标记。Kaspersky Security Center 通过以下方式之一执行自动标记：

- 按照指定的标记规则。
- 通过应用程序。

> 我们不建议您使用不同的标记方式来分配相同的标签。例如，如果标签是由规则分配的，则不建议手动将此标签分配给设备。

如果标签是通过规则分配的，则当满足指定的规则时，设备会自动被标记。单个规则对应于每个标记。规则应用到设备网络属性、操作系统、设备上安装的应用程序以及其他设备属性。例如，如果您拥有物理机、Amazon EC2 实例和 Microsoft Azure 虚拟机 hybrid 基础架构，您可以设置分配 `[Azure]` 标签到所有 Microsoft Azure 虚拟机的规则。然后，您可以在创建设备分类时使用该标签；这将帮助您整理所有 Microsoft Azure 虚拟机并给它们分配任务。

> 每个标签只能添加一条自动标记规则。如果为同一标签创建新规则，则会替换之前的规则。

在以下情况下标签从设备上被自动删除：

- 当设备停止满足分配标签的规则的条件时。
- 当分配标签的规则被禁用或删除时。

每个管理服务器的标签列表和规则列表是独立的，包括主管理服务器和从属虚拟管理服务器。规则仅被应用到来自创建规则的相同管理服务器的设备。

创建设备标签

要创建设备标签：

1. 在主菜单中，转到“**资产(设备)**”→“**标签**”→“**设备标签**”。
2. 单击**添加**。
   新标签窗口打开。
3. 在“**标签**”字段中，输入标签名称。
4. 单击“**保存**”保存设置。

新标签出现在设备标签列表。

重命名设备标签

要重命名设备标签：

1. 在主菜单中，转到“**资产(设备)**”→“**标签**”→“**设备标签**”。
2. 单击您要重命名的标签名称。
   标签属性窗口打开。
3. 在“**标签**”字段中，更改标签名称。
4. 单击“**保存**”保存设置。

更新的标签出现在设备标签列表。

删除设备标签

要删除设备标签：

1. 在主菜单中，转到“**资产(设备) → 标签 → 设备标签**”。
2. 在列表中，选择您想要删除的设备标签。
3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击“**是**”。

设备标签被删除。删除的标签被从其分配的所有设备上自动删除。

> 您已删除的标签不会自动从自动标记规则中删除。标签被删除后，它仅在设备第一次满足标签分配条件时被分配到新设备。

如果此标记由应用程序或网络代理分配给设备，则已删除的标记不会自动从设备中删除。若要管理这些标签，请使用 klscflag 实用程序。

查看分配了标签的设备

要查看分配了标签的设备：

1. 在主菜单中，转到“**资产(设备)** → **标签** → **设备标签**“。
2. 单击您要查看所分配设备的标签旁边的“**查看设备**”链接。
   您将被重定向到主菜单的“**受管理设备**”部分，其中的设备将按您单击“**查看设备**”链接的标签进行过滤。
3. 如果您想返回设备标签列表，单击您浏览器的“**后退**”按钮。

查看已分配标签的设备后，您可以创建并分配新标签，也可以将现有标签分配给其他设备。在这种情况下，您必须按标签删除过滤器，选择设备，然后分配标签。

查看分配到设备的标签

要查看分配到设备的标签：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。
2. 单击您要查看其标签的设备名称。
3. 在打开的设备属性窗口中，选择“**标签**”选项卡。

分配给所选设备的标签列表被显示。在“**分配的标签**”列中，您可以看到标签是如何分配的。

在工具栏中，您可以执行以下操作：

- 为设备分配另一个标签。
- 删除已经分配的标签。
- 查看管理服务器上存在的所有设备标签。

您无法在设备上本地查看分配的标签。

手动标记设备

要手动分配标签到设备：

1. 查看分配到您要分配其他标签的设备的标签。
2. 单击**添加**。

3. 在打开的窗口中，执行以下操作之一：

   - 要创建和分配新标签，请选择“**创建新标签**”，然后指定新标签的名称。
   - 要选择现有标签，请选择“**分配现有标签**”，然后在下拉列表中选择所需标签。

4. 单击“**正常**”应用更改。

5. 单击“**保存**”保存设置。

   所选的标签被分配到设备。

从设备上删除分配的标签

要从设备上删除标签：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。

2. 单击您要查看其标签的设备名称。

3. 在打开的设备属性窗口中，选择“**标签**”选项卡。

4. 选择您要删除的条目旁边的复选框。

5. 在列表顶部，单击**取消分配标签？** 按钮。

6. 在打开的窗口中，单击“**是**”。

   标签从设备上删除。

> 未分配的设备标签不被删除。如果您想，您可以手动删除它。

> 您不能手动删除应用程序或网络代理分配给设备的标签。若要管理这些标签，请使用 klscflag 实用程序。

查看自动标记设备规则

要查看自动标记设备规则，

做以下任意：

- 在主菜单中，转到“**资产(设备)**”→“**标签**”→“**自动标记规则**”。
- 在主菜单中，转到“**资产(设备)**”→“**标签**”→“**设备标签**”，然后单击“**设置自动标记规则**”链接。
- 查看分配给设备的标签，然后单击“**设置**”按钮。

自动标记设备规则列表出现。

编辑自动标记设备规则

要编辑自动标记设备规则：

1. 查看自动标记设备规则。
2. 单击您要编辑的规则名称。
   规则设置窗口打开。
3. 编辑规则的常规属性：
   a. 在“**规则名称**”字段中，更改规则名称。
      名称不能包括 256 个以上字符。
   b. 做以下任意：
      - 通过将切换按钮切换到“**规则已启用**”来启用规则。
      - 通过将切换按钮切换到“**规则已禁用**”来禁用规则。
4. 做以下任意：
   - 如果要添加新条件，请单击“**添加**”按钮，然后在打开的窗口中指定新条件的设置。
   - 如果要编辑现有条件，请单击要编辑的条件名称，然后编辑条件设置。
   - 如果要删除条件，请选中要删除的条件名称旁边的复选框，然后单击“**删除**”。
5. 在条件设置窗口中单击“**确定**”。
6. 单击“**保存**”保存设置。

编辑的规则显示在列表。

创建自动标记设备规则

要创建自动标记设备规则：

1. 查看自动标记设备规则。
2. 单击**添加**。
   新规则设置窗口打开。
3. 配置规则的常规属性：
   a. 在“**规则名称**”字段中，输入规则名称。
      名称不能包括 256 个以上字符。

b. 执行以下操作之一：

- 通过将切换按钮切换到“**规则已启用**”来启用规则。
- 通过将切换按钮切换到“**规则已禁用**”来禁用规则。

c. 在“**标签**”字段中，输入新设备标签名称或从列表中选择现有设备标签之一。
名称不能包括 256 个以上字符。

4. 在条件区域中，单击“**添加**”按钮以添加新条件。
新条件设置窗口打开。

5. 输入条件名称。
名称不能包括 256 个以上字符。名称必须在规则内唯一。

6. 设置根据以下条件的规则触发。您可以选择多个条件。

- **网络**—设备网络属性，例如 Windows 网络中的设备名称，或设备是否属于域或 IP 子网。

  如果为您用于 Kaspersky Security Center 的数据库设置了区分大小写的排序规则，请在指定设备 DNS 名称时保持大小写。否则，自动标记规则将不起作用。

- **应用程序**—设备上是否存在网络代理，操作系统类型、版本和架构。
- **虚拟机**—设备属于特定类型的虚拟机。
- **域控制器**—设备出现在 Active Directory 组织单元中，设备属于 Active Directory 组。
- **应用程序注册表**—设备上是否存在不同供应商的应用程序。

7. 单击“**确定**”保存更改。
如果必要，您可以为一个规则设置多个条件。此种情况下，在满足至少一个条件时，标签将被分配到设备。

8. 单击“**保存**”保存设置。

所创建的规则被强加到被所选管理服务器管理的设备。如果设备的设置满足规则条件，标签被分配到设备。

然后，规则被应用到以下情况：

- 自动和间歇性，取决于服务器负载
- 在您编辑规则之后
- 当您手动运行规则时
- 在管理服务器检测到满足规则条件的设备设置的更改或包含此设备的组设置的更改后

您可以创建多个标记规则。如果您创建了多个标记规则且规则对应的条件同时被满足，单个设备可以被分配多个标签。您可以在设备属性中查看所有分配的标签列表。

为自动标记设备运行规则

当规则运行时，规则属性中指定的标签被分配到满足相同规则中指定条件的设备。您仅可以运行活动规则。

要为自动标记设备运行规则：

1. 查看自动标记设备规则。
2. 选择您要运行的活动规则旁边的复选框。
3. 单击**运行规则**按钮。

所选规则被运行。

删除自动标记设备规则

要删除自动标记设备规则：

1. 查看自动标记设备规则。
2. 选择您要删除的规则旁边的复选框。
3. 单击**删除**。
4. 在打开的窗口中，单击“**删除**”。

所选规则被删除。规则属性中指定的标签从所有所分配的设备上取消分配。

> 未分配的设备标签不被删除。如果您想，您可以手动删除它。

使用 klscflag 实用程序管理设备标签

要为设备分配一组标签，您需要在要分配标签的客户端设备上运行 klscflag 实用程序。

klscflag 实用程序会覆盖分配给设备的现有标签。这意味着，您可以通过在命令中指定所需的标签集来添加或删除标签。该实用程序没有用于添加或删除单个标签的单独命令。相反，您会修改整个标签集。

> 在 klscflag 等命令中指定标签名称时，推荐使用一致的大小写方法，例如全部大写。使用全部大写可以帮助避免仅大小写不同的标签的潜在问题，具体取决于 DBMS 配置。

要使用 klscflag 实用程序为您的设备分配标签：

1. 使用管理员权限运行 Windows 命令提示符，然后将当前目录更改为包含 klscflag 实用程序的目录。klscflag 实用程序位于安装网络代理的文件夹中。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\NetworkAgent。

2. 输入以下命令之一：

   - 要分配一组标签：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"标签名称 1\",\"标签名称 2\",\"标签名称 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     其中 `[\"标签名称 1\",\"标签名称 2\",\"标签名称 3\"]` 是您要分配给设备的标签列表。

     如果将方括号留空，这将从设备中删除所有标签：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - 要将新标签分配给现有标签集：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"新标签名称\",\"标签名称 1\",\"标签名称 2\",\"标签名称 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     其中`NEW TAG NAME`是您想要分配给设备的标签的名称，而`TAG NAME 1`、`TAG NAME 2`、`TAG NAME 3`是已分配给设备的标签的名称。

   - 要删除特定标签而不删除已分配给设备的其他标签，请使用更新的标签集运行该命令。

     例如，如果您当前的标签是`TAG NAME 1`、`TAG NAME 2`、`TAG NAME 3`，而您想要删除`TAG NAME 2`，请运行以下命令：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"标签名称 1\",\"标签名称 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. 重启网络代理服务。

   klscflag 实用程序会将指定标签分配给您的设备。

4. 如果您想要确保 klscflag 实用程序已成功分配指定标签，请查看分配给设备的标签。

或者，您可以手动分配设备标签。

策略和策略配置文件

在 Kaspersky Security Center Web Console 中，可以为 Kaspersky 应用程序创建策略。该部分描述了策略和策略配置文件，并提供创建和修改它们的说明。

关于策略和策略配置文件

*策略*是应用于一个管理组和其子组的 Kaspersky 应用程序设置集。您可以在管理组的设备上安装多个 Kaspersky 应用程序。Kaspersky Security Center 为管理组中的每个 Kaspersky 应用程序提供一个策略。策略具有以下状态之一（请参见下表）：

策略的状态

状态	描述
活动	应用于设备的当前策略。对于每个管理组中的卡巴斯基应用程序，只能有一个策略处于活动状态。设备对卡巴斯基应用程序应用活动策略的设置值。
非活动	当前未应用于设备的策略。
漫游	如果选择该选项，策略将在设备离开企业网络时变为活动状态。

策略根据以下规则发挥作用：

- 您可以为单个应用程序配置拥有不同值的多个策略。
- 对于当前应用程序，只能有一个策略处于活动状态。
- 您可以在发生特定事件时激活处于非活动状态的策略。例如，您可以在病毒爆发时强制执行更严格的反病毒保护设置。
- 策略可以有子策略。

通常，您可以将策略用作对紧急情况（如病毒攻击）的准备。例如，如果存在通过闪存驱动器进行的攻击，您可以激活相应策略来阻止访问闪存驱动器。在这种情况下，当前的活动策略将自动变为非活动状态。

为了防止维护多个策略，例如，在不同的场合下只是更改几个设置时，可以使用策略配置文件。

*策略配置文件*是策略设置值的命名子集，用于替换策略的设置值。策略配置文件影响受管理设备上有效设置的形成。*有效设置*是当前应用于设备的一组策略设置、策略配置文件设置和本地应用程序设置。

策略配置文件根据以下规则发挥作用：

- 当出现特定的激活情况时，策略配置文件生效。
- 策略配置文件包含的设置值与策略设置不同。
- 激活策略配置文件会更改受管理设备的有效设置。
- 一个策略可以包含最多 100 个策略配置文件。

关于“锁定”和锁定的设置

每个策略设置都有一个锁定按钮图标 (🔒)。下表显示了锁定按钮的状态：

锁定按钮状态

状态	描述
🔒 未定义 ⚪	如果设置旁边显示打开的锁，并且禁用了切换按钮，则策略中未指定该设置。用户可以在受管理应用程序界面中更改这些设置。这些设置的类型称为“*未锁定*”。
🔒 强制 🟢	如果设置旁边显示关闭的锁，并且启用了切换按钮，则该设置应用于实施策略的设备。用户无法在受管理应用程序界面中修改这些设置的值。这些设置的类型称为“*已锁定*”。

我们强烈建议您关闭要在受管理设备上应用的策略设置的锁定。解锁的策略设置可以由卡巴斯基应用程序设置在受管理设备上重新分配。

您可以使用锁定按钮执行以下操作：

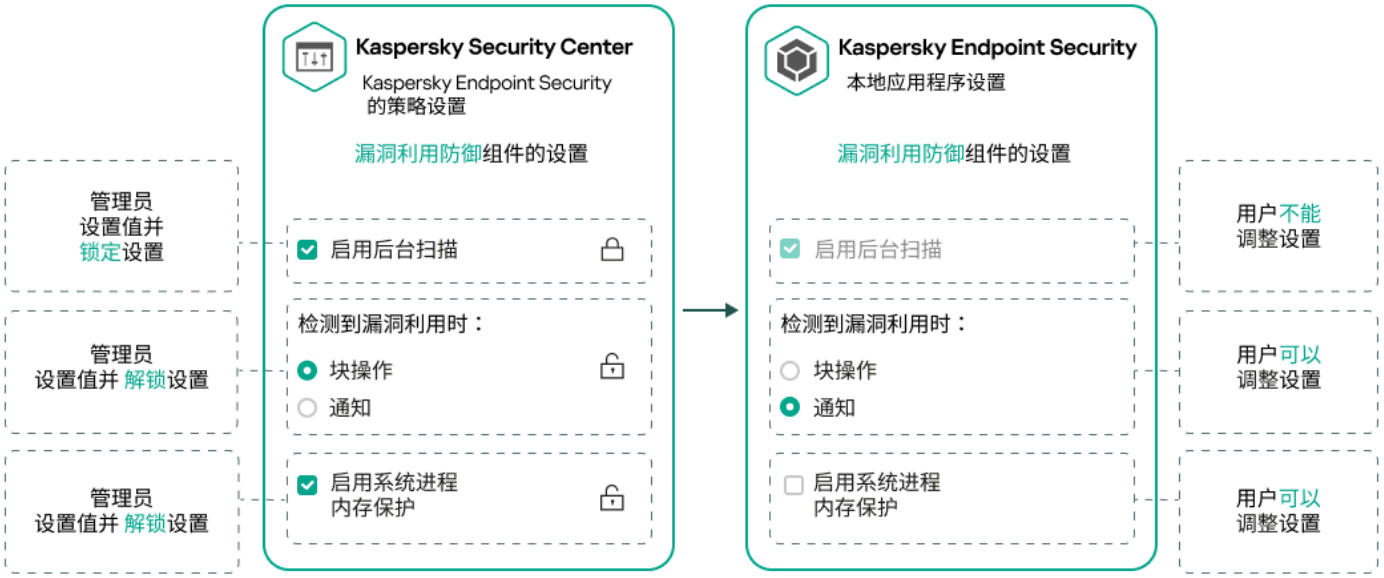
- 锁定管理子组策略的设置
- 在受管理设备上锁定本地卡巴斯基应用程序的设置

因此，已锁定设置用于在受管理设备上实施有效设置。

有效设置实施的过程包括以下操作：

- 受管理设备将应用卡巴斯基应用程序的设置值。
- 受管理设备应用策略的锁定设置值。

策略和受管理卡巴斯基应用程序包含相同的一组设置。配置策略设置时，受管理设备上的卡巴斯基应用程序设置会更改值。您无法调整受管理设备上的已锁定设置（请参见下图）：



锁定和卡巴斯基应用程序设置

策略继承和策略配置文件

本部分提供有关策略和策略配置文件的层级和继承的信息。

策略层级

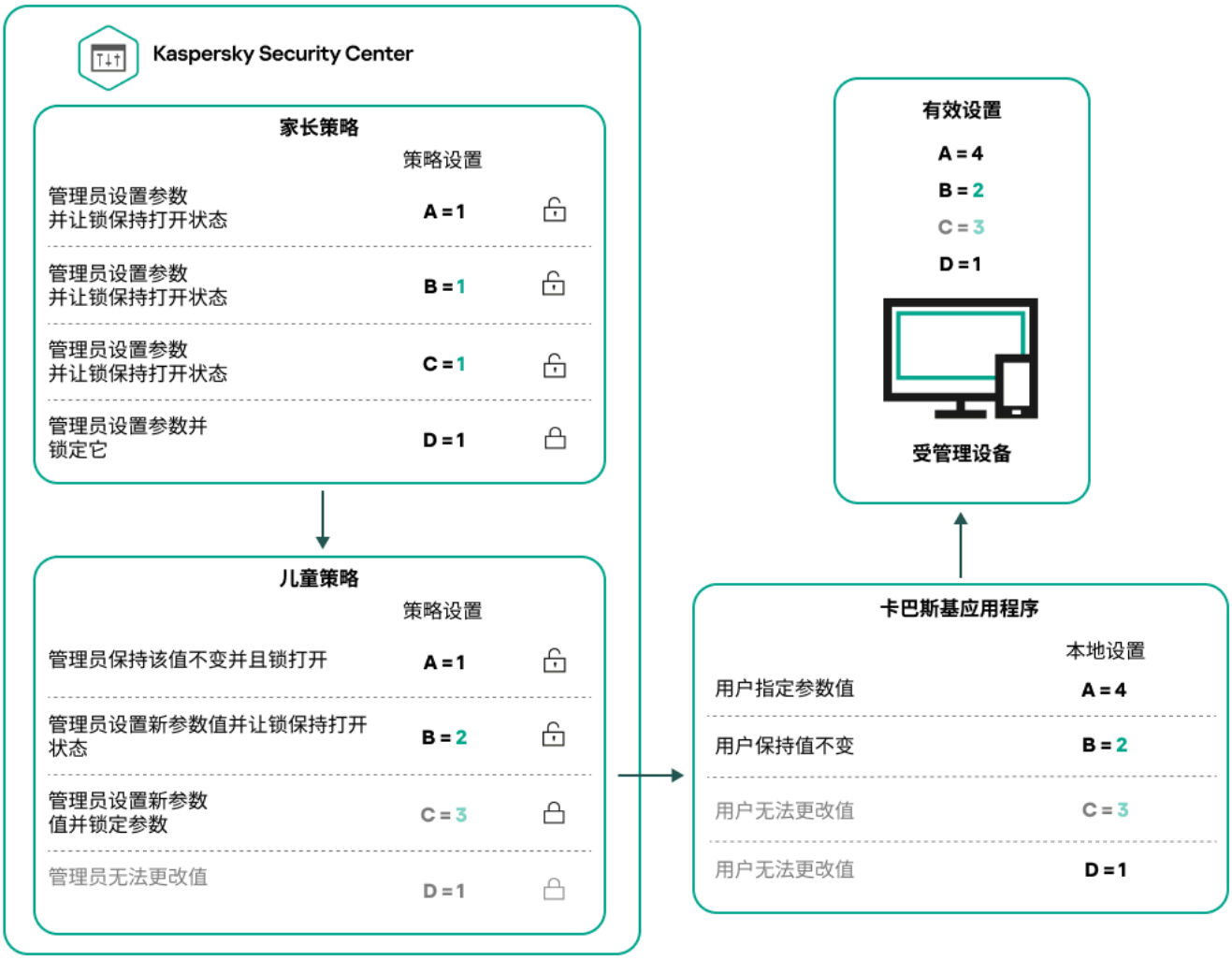
如果不同的设备需要不同的设置，则可以将设备组织到管理组中。

您可以为单个管理组指定策略。策略设置可以被*继承*。继承意味着子组中的策略设置值接收自更高级别的（父）管理组的策略。

因此，父组策略也叫*父策略*。子组策略也称为*子策略*。

默认情况下，管理服务器上存在至少一个受管理设备组。如果要创建自定义组，它们将创建为受管理设备组内的子组。

根据管理组的层级，同一应用程序的策略会互相作用。更高级别（父）管理组的策略中的锁定设置将重新分配子组的策略设置值（请参见下图）。

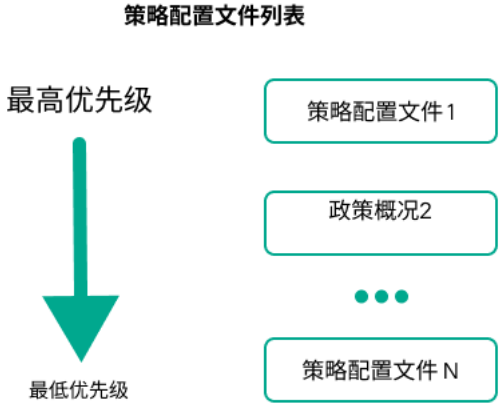


策略层级

策略层级中的策略配置文件

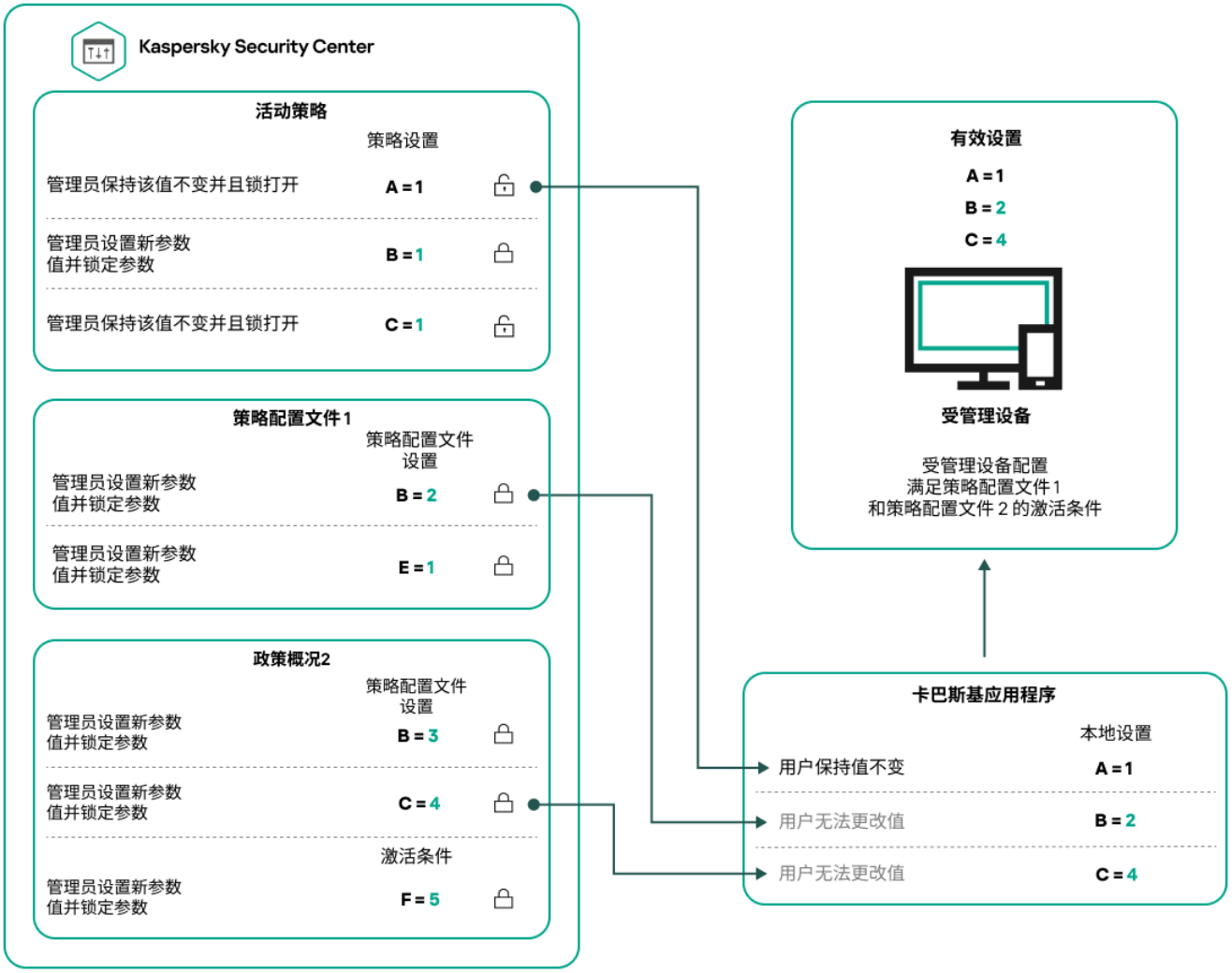
策略配置文件具有以下优先级分配条件：

- 配置文件在策略配置文件列表中的位置指示了其优先级。您可以更改策略配置文件优先级。列表中的最高位置指示最高优先级（请参见下图）。



策略配置文件的优先级定义

- 策略配置文件的激活条件互不依赖。可以同时激活多个策略配置文件。如果多个策略配置文件影响同一设置，则设备将采用策略配置文件中具有最高优先级的设置值（请参见下图）。

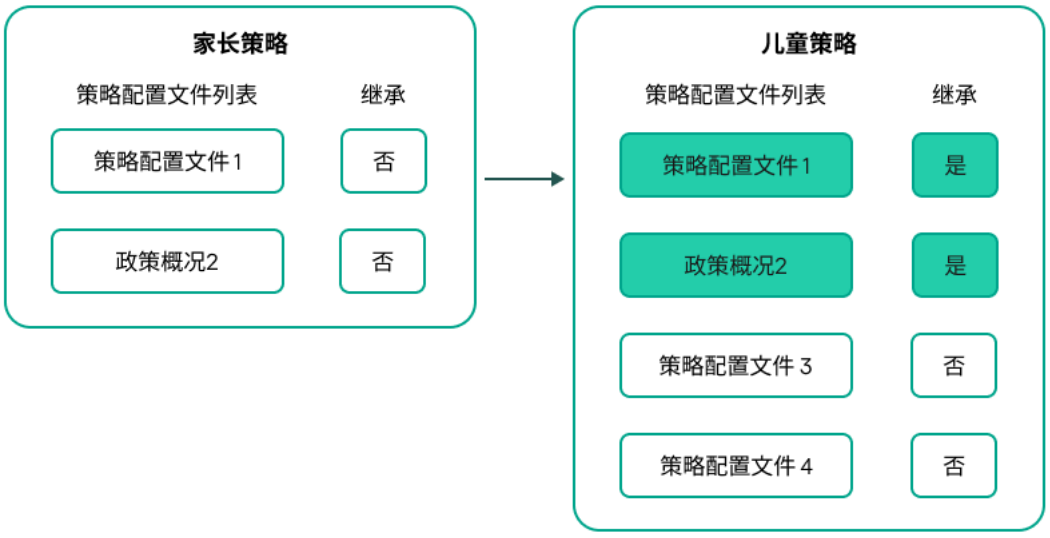


受管理设备配置满足多个策略配置文件的激活条件

继承层级中的策略配置文件

来自不同层次结构级别策略的策略配置文件符合以下条件：

- 较低级别的策略继承较高级别的策略的策略配置文件。从较高级别策略继承的策略配置文件比原始策略配置文件的级别具有更高的优先级。
- 您不能更改继承的策略配置文件的优先级（请参见下图）。



继承策略配置文件

具有相同名称的策略配置文件

如果在不同的层次结构级别中有两个名称相同的策略，则这两个策略按照以下规则起作用：

- 较高级别的策略配置文件的锁定设置和配置文件激活条件将更改较低级别的策略配置文件的设置和配置文件激活条件（请参见下图）。

子配置文件继承父策略配置文件的设置值

- 较高级别的策略配置文件的未锁定设置和配置文件激活条件不会更改较低级别的策略配置文件的设置和配置文件激活条件。

如何在受管理设备上实施设置

在受管理设备上有效设置的实现可以描述如下：

- 所有未锁定的设置的值均取自策略。
- 然后，它们将被受管理应用程序设置的值覆盖。
- 然后，将应用有效策略中的锁定设置值。锁定的设置值会更改解锁的有效设置的值。

管理策略

本部分介绍管理策略并提供有关查看策略列表、创建策略、修改策略、复制策略、移动策略、强制同步、查看策略分发状态图以及删除策略的信息。

查看策略列表

您可以查看为管理服务器或任何管理组创建的策略列表。

要查看策略列表，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**”→“**组层级**”。
2. 在管理组结构中，选择您要查看其策略列表的管理组。

策略列表以表格格式出现。如果没有策略，表格为空。您可以显示或隐藏表格的列，更改它们的顺序，仅查看包含指定值的行，或者使用查找。

创建策略

您可以创建策略；您也可以修改和删除现有策略。

要创建策略：

1. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”。
2. 选择要为其创建策略的管理组：
   - 对于根组。
     在这种情况下，您可以继续下一步。
   - 对于子组：
     a. 单击窗口顶部的当前路径链接。
     b. 在打开的面板中，单击带有所需子组名称的链接。

     当前路径会发生变化以反映所选的子组。
3. 单击**添加**。
   “**选择应用程序**”窗口将打开。
4. 选择您要为其创建策略的应用程序。
5. 单击“**下一步**”。
   新策略设置窗口打开，在其中已选择“**常规**”选项卡。
6. 如果您需要，更改策略的默认名称、默认状态和默认继承设置。
7. 选择“**应用程序设置**”选项卡。
   或者，您可以单击“**保存**”并退出。策略将出现在策略列表，且您可以稍后编辑其设置。
8. 在“**应用程序设置**”选项卡的左侧窗格中选择您需要的类别，并在右侧的结果窗格中编辑策略设置。您可以在每个类别中（区域）编辑策略设置。

设置集合取决于您为其创建策略的应用程序。有关详细信息，请参阅以下内容：

- 管理服务器配置
- 网络代理策略设置
- Kaspersky Endpoint Security for Windows 文档

有关其他安全应用程序设置的详细信息，请参阅相应应用程序的文档。
当编辑设置时，您可以单击“**取消**”以取消上一次操作。

9. 单击“**保存**”保存策略。

该策略显示在策略列表中。

修改策略

要修改策略：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。
2. 单击您要修改的策略。
   策略设置窗口打开。
3. 指定“通用设置”和为其创建策略的应用程序的设置。有关详细信息，请参阅以下内容：
   - 管理服务器配置
   - 网络代理策略设置
   - Kaspersky Endpoint Security for Windows 文档

   有关其他安全应用程序设置的详细信息，请参阅该应用程序的文档。
4. 点击“**保存**”。

对策略所做的更改将保存在策略属性中，并将显示在“**修订历史**”区域中。

常规策略设置

常规

在“**常规**”选项卡中，可以修改策略状态并指定策略设置的继承：

- 在“**策略状态**”块，您可以选择策略的模式：
  - **活动**

    如果选择该选项，策略将变为活动状态。

默认情况下已选定该选项。

- **漫游**

  如果选择该选项，策略将在设备离开企业网络时变为活动状态。

- **不活动**

  如果选择该选项，策略将变为不活动状态，但它仍然存储在“**策略**”文件夹中。如果需要，您可以激活该策略。

- 在“**设置继承**”设置组中，您可以配置策略继承：

  - **从父策略继承设置**

    如果启用此选项，则策略设置值将从上一级组策略继承，因而被锁定。
    默认情况下已启用该选项。

  - **在子策略中强制继承设置**

    如果启用此选项，则在应用策略更改之后，将执行以下操作：
    - 策略设置的值将被传送到管理子组的策略，也就是子策略。
    - 在每个子策略属性窗口**常规**区域的**继承设置**区块，将自动启用**从父策略继承设置**选项。

    如果启用此选项，则子策略设置被锁定。
    默认情况下已禁用该选项。

事件配置

“**事件配置**”区域允许您配置事件记录和事件通知。事件根据重要级别用下面的标签分布：

- **严重**
  “**严重**”区域不显示在网络代理策略属性中。
- **功能失败**
- **警告**
- **信息**

在每个区域，列表显示在管理服务器上事件类型和默认事件存储的期限（天）。单击事件类型允许您指定以下设置：

- **事件注册**

您可以指定存储事件的天数和选择存储事件的位置：

- **使用 Syslog 导出到 SIEM 系统**
- **存储在设备的 OS 事件日志中**
- **存储在管理服务器的 OS 事件日志中**

- **事件通知**

  您可以选择您是否想由以下方法之一被通知事件：

  - **通过邮件通知**
  - **通过 SMS 通知**
  - **通过运行可执行文件或脚本通知**
  - **通过 SNMP 通知**

  默认下，使用在管理服务器属性选项卡中指定的通知设置（例如收件人地址）。如果需要，可以在“**电子邮件**”、“SMS”和“**要运行的可执行文件**”选项卡中更改这些设置。

修订历史

“**修订历史**”选项卡允许您查看策略修订列表和回滚策略更改（如有必要）。

启用和禁用策略继承选项

要在策略中启用或禁用继承选项：

1. 打开所需策略。
2. 打开“**常规**”选项卡。
3. 启用或禁用策略继承：
   - 如果您在子策略中启用“**从父策略继承设置**”，并且管理员在父策略中锁定了一些设置，那么您无法在子组策略中更改这些设置。
   - 如果您在子策略中禁用“**从父策略继承设置**”，那么您可以在子策略中更改所有设置，即便一些设置在父策略中是锁定的。
   - 如果在父组中启用“**在子策略中强制继承设置**”，这将为每个子策略启用“**从父策略继承设置**”选项。此种情况下，您无法为任何子策略禁用该选项。所有在父策略中被锁定的设置被强制继承到子组，且您无法在子组中更改这些设置。
4. 单击“**保存**”按钮保存更改，或单击“**取消**”按钮拒绝更改。

默认情况下，为新策略启用“**从父策略继承设置**”选项。

如果一个策略具有配置文件，所有子策略都继承这些配置文件。

复制策略

您可以从一个管理组复制策略到另一个。

要复制策略到其他管理组：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。
2. 选择您要复制的策略旁边的复选框。
3. 单击“**复制**”按钮。
   在屏幕的右侧，管理组树被显示。
4. 在树中，选择目标组，即，要将策略复制到的组。
5. 单击屏幕底部的“**复制**”按钮。
6. 单击“**确定**”以确认操作。

策略将连带其所有配置文件被复制到目标组。目标组中每个复制的策略的状态将是“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已包含名称与新移动策略的名称一致的策略，那么会在新移动策略的名称后附加一个 （<下一个序列号>） 的索引，例如： （1） 。

移动策略

您可以从一个管理组移动策略到另一个。例如，您要删除一个组，但您要为其他组使用其策略。此种情况下，您最好在删除旧组之前将策略从旧组移动到新组。

> 将策略移至其他管理组时，该策略的修订历史记录将被清除。**修订历史**选项卡仅显示有关最新更改的信息。

要移动策略到其他管理组：

1. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”。
2. 选择您要移动的策略旁边的复选框。
3. 单击“**移动**”按钮。
   在屏幕的右侧，管理组树被显示。
4. 在树中，选择目标组，即，要将策略移动到的组。
5. 单击屏幕底部的“**移动**”按钮。
6. 单击“**确定**”以确认操作。

如果策略不是从资源组继承的，它连带所有配置文件被移动到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果策略是从资源组继承的，它保持在资源组。它连带所有其配置文件被复制到目标组。目标组中的策略状态为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已包含名称与新移动策略的名称一致的策略，那么会在新移动策略的名称后附加一个 （<下一个序列号>） 的索引，例如： （1）。

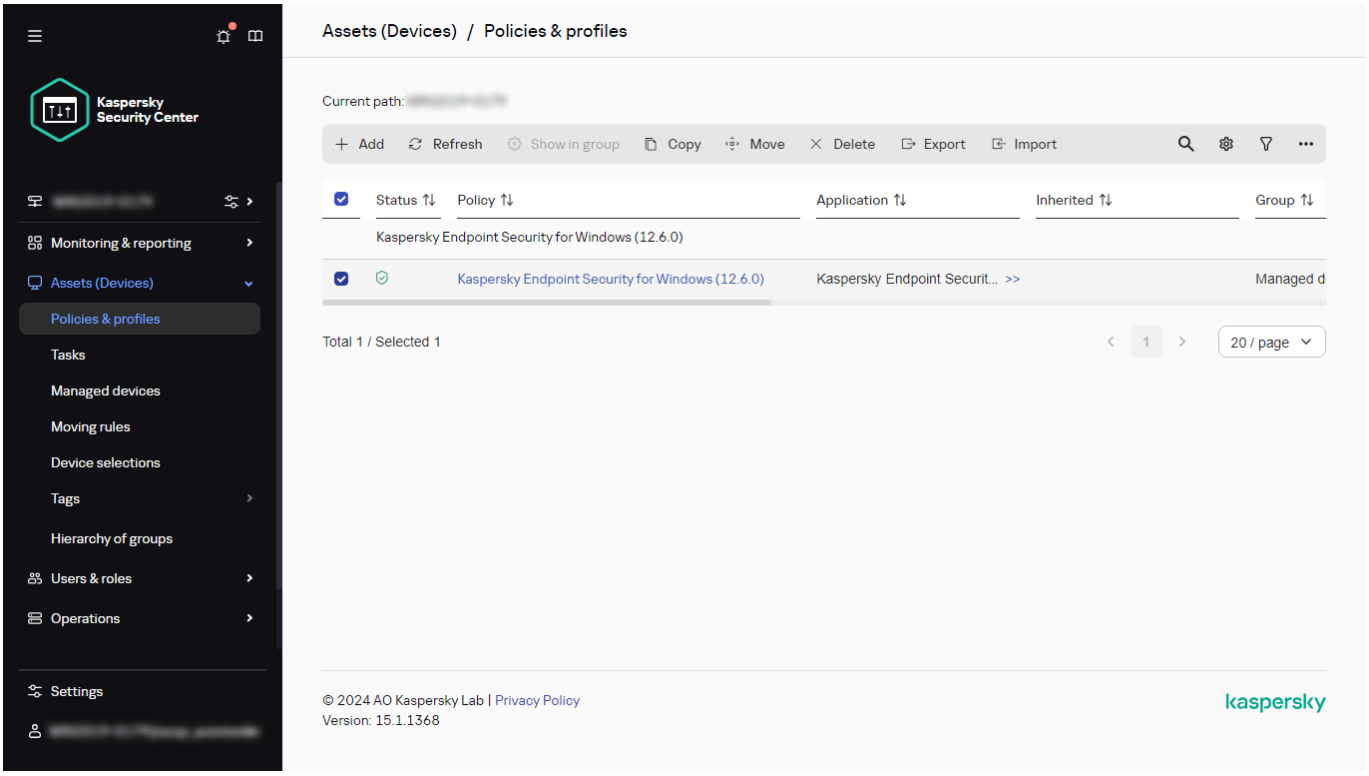
导出策略

Kaspersky Security Center 允许您将策略、其设置和策略配置文件保存到 KLP 文件中。您可以使用此 KLP 文件将保存的策略导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要导出策略，请执行以下操作：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。
2. 选中要导出的策略旁边的复选框。

   您不能同时导出多个策略。如果您选择了多个策略，**导出**按钮将被禁用。



3. 单击“**导出**”按钮。
4. 在打开的“**另存为**”窗口中，指定策略文件的名称和路径。单击“**保存**”按钮。

   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则策略文件会自动保存在“**下载**”文件夹。

导入策略

Kaspersky Security Center 允许您从 KLP 文件导入策略。KLP 文件包含导出的策略、其设置和策略配置文件。

要导入策略，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**”。
2. 单击“**导入**”按钮。
3. 单击**浏览**按钮选择要导入的策略文件。
4. 在打开的窗口中，指定 KLP 策略文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个策略文件。
   策略处理启动。
5. 策略成功处理后，选择要向其应用策略的管理组。
6. 单击**完成**按钮以完成策略导入。

出现包含导入结果的通知。如果策略成功导入，可以单击“**详细资料**”链接以查看策略属性。

成功导入后，策略会显示在策略列表中。策略的设置和配置文件也将会导入。无论导出期间选择的策略处于什么状态，导入的策略均处于非活动状态。您可以在策略属性中更改策略状态。

> 如果新导入的策略与现有策略有相同的名称，则导入的策略在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

查看策略分发状态图

在 Kaspersky Security Center 中，您可以在策略分发状态图中查看每个设备上的策略应用程序状态。

要查看每个设备上的策略分发状态：

1. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”。
2. 选中要针对其查看设备上的分发状态的策略名称旁边的复选框。
3. 在出现的菜单中，选择“**分发**”链接。
   将打开“**<策略名称> 分发结果**”窗口。
4. 在打开的“**<策略名称> 分发结果**”窗口中，将显示策略的**状态描述**。

您可以更改列表中显示的策略分发结果数量。最大设备数量为 100,000。

要更改带有策略分发结果的列表中显示的设备数量：

1. 在主菜单中，转到您的账户设置，然后选择“**界面选项**”。
2. 在**策略分发结果中显示的设备数量限制**中，输入设备数量（最多 100,000）。
   默认情况下，该数字为 5000。
3. 点击“**保存**”。
   设置已保存并应用。

删除策略

如果您不再需要一个策略，您可以删除它。您仅可以删除一个在指定管理组中继承的策略。如果一个策略是继承的，您仅可以在其被创建的上级组删除它。

要删除策略，请执行以下操作：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**”。
2. 选中您要删除的策略旁边的复选框，然后单击“**删除**”。
   如果选择继承的策略，“**删除**”按钮变为不可用（变暗）。
3. 单击“**确定**”以确认操作。

策略连带其所有配置文件被删除。

管理策略配置文件

本节介绍管理策略配置文件并提供有关查看策略配置文件、更改策略配置文件优先级、创建策略配置文件、修改策略配置文件、复制策略配置文件、创建策略配置文件激活规则以及删除策略配置文件的信息。

查看策略配置文件

要查看策略配置文件：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**”。
2. 单击您要查看其配置文件的策略名称。
   策略属性窗口打开，在其中已选择“**常规**”选项卡。
3. 打开“**策略配置文件**”选项卡。

策略配置文件列表以表格格式出现。如果策略没有配置文件，将显示空表。

更改策略配置文件优先级

要更改策略配置文件优先级：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。
2. 在“**策略配置文件**”选项卡上，选中您要更改其优先级的策略配置文件旁边的复选框。

3. 通过单击“**提高优先级**”或“**降低优先级**”来设置策略配置文件在列表中的新位置。
   策略配置文件在列表中的位置越高，其优先级越高。

4. 单击“**保存**”按钮。

所选策略配置文件的优先级被更改并应用。

创建策略配置文件

要创建策略配置文件：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。如果策略没有配置文件，将显示空表。

2. 单击**添加**。

3. 如果您需要，更改配置文件的默认名称和默认继承设置。

4. 选择“**应用程序设置**”选项卡。
   或者，您可以单击“**保存**”并退出。您创建的配置文件会出现在策略配置文件列表中，您可以稍后编辑其设置。

5. 在“**应用程序设置**”选项卡的左侧窗格中选择您需要的类别，并在右侧的结果窗格中编辑策略设置。您可以在每个类别中（区域）编辑策略配置文件设置。
   当编辑设置时，您可以单击“**取消**”以取消上一次操作。

6. 单击“**保存**”保存配置文件。

该配置文件显示在策略配置文件列表中。

修改策略配置文件

只有 Kaspersky Endpoint Security for Windows 的策略才支持编辑策略配置文件。

修改策略配置文件：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。

2. 在“**策略配置文件**”选项卡上，单击要修改的策略配置文件。
   “策略配置文件”窗口打开。

3. 在属性窗口中配置配置文件：

   - 如果必要，在“**常规**”选项卡上，更改配置文件名称并启用或禁用配置文件。
   - 编辑配置文件激活规则。
   - 编辑应用程序设置。

有关安全应用程序设置的详细信息，请参阅相应应用程序的文档。

4. 点击“**保存**”。

您已修改的设置将在设备与管理服务器同步之后生效（如果策略配置文件处于活动状态），或在激活规则触发之后生效（如果策略配置文件处于非活动状态）。

复制策略配置文件

您可以复制策略配置文件到当前策略或其他策略，例如，如果您要对不同策略拥有相同配置文件。您也可以使用复制，如果您想拥有两个或更多仅在少数设置不同的配置文件。

要复制策略配置文件：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。如果策略没有配置文件，将显示空表。
2. 在“**策略配置文件**”选项卡上，选择要复制的策略配置文件。
3. 单击**复制**。
4. 在打开的窗口中，选择您要复制配置文件的策略。
   您可以复制策略配置文件到相同策略或您指定的策略。
5. 单击**复制**。

策略配置文件被复制到您选择的策略。新复制的配置文件具有最低优先级。如果您复制配置文件到相同策略，新复制的配置文件名称将附加 () 索引，例如：(1)、(2)。

稍后，您可以更改配置文件设置，包括它的名称和属性；原始策略配置文件此种情况下将不被更改。

创建策略配置文件激活规则

要创建策略配置文件激活规则：

1. 转到您要的策略的配置文件列表。
   将出现策略配置文件列表。
2. 在“**策略配置文件**”选项卡上，单击需要为其创建激活规则的策略配置文件。
   如果策略配置文件列表为空，您可以创建策略配置文件。
3. 在“**激活规则**”选项卡上，单击“**添加**”按钮。
   策略配置文件激活规则窗口打开。
4. 指定规则名称。

5. 选择影响您当前创建的策略配置文件的激活的条件的复选框：

- **策略配置文件激活常规规则**

  选择该复选框根据设备离线模式状态设置设备上的策略配置文件激活规则、连接管理服务器规则和分配给设备的标记。

  对于该选项，在下一步指定：

  - **设备状态**

    定义设备出现在网络的条件：

    - **在线**—设备在网络中，因此管理服务器可用。
    - **离线**—设备在外部网络，这意味着管理服务器不可用。
    - **N/A**—将不应用标准。

  - **管理服务器连接规则在该设备上活动**

    选择策略配置文件激活条件（规则是否被执行）并选择规则名称。

    规则定义设备网络位置以便连接到管理服务器，它的条件必须被满足(或不满足)以便激活策略配置文件。

    用于连接到管理服务器的设备网络位置描述可以在网络代理切换规则中被创建或配置。

- **特别设备所有者规则**

  对于该选项，在下一步指定：

  - **设备所有者**

    启用此选项可根据设备所有者在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 设备属于指定的拥有者（"="符号）。
    - 设备不属于指定的拥有者（"#"符号）。

      如果启用该选项，配置文件根据配置的标准在设备上激活。启用此选项时，您可以指定设备所有者。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **设备所有者在内部安全组中**

    启用此选项可通过所有者在 Kaspersky Security Center 内部安全组中的资格在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 设备所有者是指定安全组的成员（"="符号）。
    - 设备所有者不是指定安全组的成员（"#"符号）。

      如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定 Kaspersky Security Center 的安全组。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **硬件说明书规则**

  选择该复选框根据内存和逻辑处理器数量设置设备上的策略配置文件激活规则。

  对于该选项，在下一步指定：

  - **内存大小(MB)**

    启用此选项可通过设备上可用 RAM 容量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 该设备内存大小小于指定值("<" 符号)。
    - 该设备内存大小大于指定值(">" 符号)。

    如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的 RAM 卷。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **逻辑处理器数量**

    启用此选项可通过设备上逻辑处理器数量在设备上配置和启用配置文件激活规则。在此复选框下的下拉列表中，可以选择配置文件激活标准：

    - 设备上逻辑处理器数量少于或等于指定值 （"<" 符号）。
    - 设备上逻辑处理器数量大于或等于指定值 （">" 符号）。

    如果启用该选项，配置文件根据配置的标准在设备上激活。您可以指定设备上的逻辑处理器数量。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

- **角色分配规则**

  对于该选项，在下一步指定：

  由设备所有者特定角色激活策略配置文件

  选择该选项以在设备上根据所有者角色配置和启用配置文件激活规则。从现有角色列表手动添加角色。

  如果启用该选项，配置文件根据配置的标准在设备上激活。

- **标签使用规则**

  选择该复选框根据分配到设备的标签设置设备上的策略配置文件激活规则。您可以激活策略配置文件到有或没有所选标签的设备。

  对于该选项，在下一步指定：

  - **标签**

    在标签列表中，通过选中与相应标签对应的选框，可以指定策略配置文件中的设备包含规则。

    您可以通过列表上方的字段添加新标签到列表，并单击“**添加**”按钮。

    策略配置文件包含具有选定标签的设备。如果清除选框，则将不应用该标准。默认情况下已清除这些选框。

- **应用到没有指定标签的设备**

  如果必须转换标签分类，则启用此选项。

  如果启用此选项，策略配置文件将包含未带有所选标签的描述的设备。如果禁用此选项，则不应用该标准。

  默认情况下已禁用该选项。

- **活动目录使用规则**

  选择该复选框根据设备在活动目录组织单元中的出现或者设备在活动目录安全组中的成员关系设置设备上的策略配置文件激活规则。

  对于该选项，在下一步指定：

  - **在活动目录安全组中的设备所有者成员关系**

    如果启用此选项，其所有者是指定安全组成员的设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **在活动目录安全组中的设备成员关系**

    如果启用此选项，设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。默认情况下已禁用该选项。

  - **在活动目录组织单元中的设备分配**

    如果启用此选项，指定 Active Directory 组织单元 (OU) 中包括的设备上的策略配置文件将激活。如果禁用此选项，配置文件激活标准不起作用。

    默认情况下已禁用该选项。

  向导的附加页面数量取决于您在第一步选择的设置。您可以稍后修改策略配置文件激活规则。

6. 检查所配置参数的列表。如果列表正确，请单击“**创建**”。

   配置文件将被保存。当触发激活规则时，将在设备上激活该配置文件。

为配置文件创建的策略配置文件激活规则显示在“**激活规则**”选项卡上的策略配置文件属性中。您可以修改或删除任何策略配置文件激活规则。

多个激活规则可以被一起触发。

删除策略配置文件

要删除策略配置文件：

1. 转到您要的策略的配置文件列表。

   将出现策略配置文件列表。

2. 在“**策略配置文件**”选项卡上，选中要删除的策略配置文件旁边的复选框，然后单击“**删除**”。

3. 在打开的窗口中，单击“**删除**”。

策略配置文件即被删除。如果策略从低级别组继承，配置文件会保留在该组，但变成该组的策略配置文件。这可以消除低级别组设备上安装的受管理应用程序的设置的显著修改。

数据加密和保护

在笔记本电脑或硬盘驱动器丢失或被盗时，或者数据被未经授权的用户和应用程序访问时，数据加密能够降低数据意外泄露的风险。

以下 Kaspersky 应用程序支持加密：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

您可以使用用户界面设置来显示或隐藏与加密管理功能相关的某些界面元素。

我们不建议在 VDI 中启用加密。

加密 Kaspersky Endpoint Security for Windows 中的数据

您可以管理以下类型的加密：

- 在运行 Windows 操作系统的设备上为服务器管理 BitLocker 驱动器加密
- 在运行 Windows 操作系统的设备上为工作站管理卡巴斯基磁盘加密

通过使用 Kaspersky Endpoint Security for Windows 的这些组件，您可以执行启用或禁用加密、查看加密驱动器列表或生成和查看有关加密的报告等活动。

在 Kaspersky Security Center 中通过定义 Kaspersky Endpoint Security for Windows 的策略来配置加密。Kaspersky Endpoint Security for Windows 会根据活动策略执行加密和解密。有关如何配置加密功能的规则和描述的详细说明，请参阅 Kaspersky Endpoint Security for Windows 帮助。

加密 Kaspersky Endpoint Security for Mac 中的数据

您可以在运行 macOS 的设备上使用 FileVault 加密。当使用 Kaspersky Endpoint Security for Mac 时，可以启用或禁用此加密。

在 Kaspersky Security Center 中通过定义 Kaspersky Endpoint Security for Mac 的策略来配置加密。Kaspersky Endpoint Security for Mac 会根据活动策略执行加密和解密。有关加密功能的详细说明，请参阅 Kaspersky Endpoint Security for Mac 帮助。

查看加密驱动器列表

在 Kaspersky Security Center 中，您可以查看有关加密驱动器和在驱动器级别加密的设备的详细信息。驱动器上的信息解密后，该驱动器将自动从列表中移除。

要查看加密驱动器列表，

在主菜单中，转到“**操作**”→“**数据加密和保护**”→“**加密驱动器**”。

如果该区域不在菜单上，则表示它已隐藏。在“用户界面设置”中启用“**显示数据加密和保护**”选项来显示该区域。

您可以将加密驱动器列表导出到 CSV 文件或 TXT 文件。为此，请单击**导出到 CSV**或**导出到 TXT**按钮。

查看加密事件列表

在设备上运行数据加密或解密任务时，Kaspersky Endpoint Security for Windows 会将以下类型的事件信息发送给 Kaspersky Security Center：

- 无法加密或解密文件，或者由于磁盘空间不足无法创建加密的压缩包。
- 无法加密或解密文件，或者由于授权许可问题无法创建加密的压缩包。
- 无法加密或解密文件，或者由于缺少访问权限无法创建加密的压缩包。
- 应用程序被禁止访问加密文件。
- 未知错误。

要查看在设备上加密数据时发生的事件的列表：

在主菜单中，转到“**操作**”→“**数据加密和保护**”→“**加密事件**”。

如果该区域不在菜单上，则表示它已隐藏。在“用户界面设置”中启用“**显示数据加密和保护**”选项来显示该区域。

您可以将加密驱动器列表导出到 CSV 文件或 TXT 文件。为此，请单击**导出到 CSV**或**导出到 TXT**按钮。

或者，您可以检查每个受管理设备的加密事件列表。

要查看受管理设备的加密事件：

1. 在主菜单中，转到“**资产(设备)** → **受管理设备**”。
2. 单击受管理设备的名称。
3. 在**常规**选项卡上，转到**保护**部分。
4. 单击**查看数据加密错误**链接。

创建和查看加密报告

您可以生成以下报告：

- “受管理设备加密状态报告”。此报告提供有关各种受管理设备的数据加密的详细信息。例如，该报告显示应用已配置加密规则的策略的设备数量。此外，您还可以了解需要重启的设备数量。该报告还包含有关每个设备的加密技术和算法的信息。
- 大容量存储设备加密状态报告。此报告包含与受管理设备加密状态报告类似的信息，但它仅提供大容量存储设备和可移动驱动器的数据。
- 加密驱动器访问权限报告。此报告显示哪些用户账户可以访问加密驱动器。
- “文件加密错误报告”。该报告包含在设备上运行数据加密或解密任务时相关的错误信息。
- “加密文件访问被阻止报告”。该报告包含了阻止应用程序访问加密文件的信息。如果未经授权的用户或应用程序试图访问加密文件或驱动器，此报告会很有帮助。

您可以在“**监控和报告 → 报告**”区域中生成任何报告。或者，在**操作→数据加密和保护**区域中，您可以生成以下加密报告：

- 大容量存储设备加密状态报告
- 加密驱动器访问权限报告
- 文件加密错误报告

*要在**数据加密和保护**区域中生成加密报告：*

1. 确保您启用了界面选项中的“**显示数据加密和保护**”选项。
2. 在策略属性中，打开“**事件配置**”选项卡。
3. 在**严重**部分，单击**添加事件**并选中*应用文件加密/解密规则时出错*事件旁边的复选框。
4. 单击“**确定**”。
5. 在主菜单中，转到**操作→数据加密和保护**。
6. 打开以下区域之一：
   - **加密驱动器**可生成大容量存储设备加密状态报告或加密驱动器访问权限报告。
   - **加密事件**可生成文件加密错误报告。
7. 单击您要生成的报告的名称。

报告生成将开始。

授予对处于离线模式的加密驱动器的访问权限

用户可能请求访问加密设备，例如，当受管理设备上未安装 Kaspersky Endpoint Security for Windows 时。在您收到请求后，您可以创建访问密钥文件并将其发送给用户。Kaspersky Endpoint Security for Windows 帮助中提供了所有使用案例和详细说明。

要授予对处于离线模式的加密驱动器的访问权限：

1. 从用户那里获取请求访问文件（具有 FDERTC 扩展名的文件）。按照 Kaspersky Endpoint Security for Windows 帮助 中的说明在 Kaspersky Endpoint Security for Windows 中生成文件。
2. 在主菜单中，转到“**操作**” → “**数据加密和保护**” → “**加密驱动器**”。
   将显示加密驱动器列表。
3. 选择用户请求访问权限的驱动器。
4. 单击**授予移动模式设备访问权限**按钮。
5. 在打开的窗口中，选择与用于加密所选驱动器的 Kaspersky 应用程序相对应的插件。

   如果驱动器是使用 Kaspersky Security Center Web Console 不支持的 Kaspersky 应用程序加密的，则使用基于 Microsoft 管理控制台的管理控制台授予离线访问权限。
6. 按照 Kaspersky Endpoint Security for Windows 帮助 中提供的说明进行操作（请参阅本节末尾的扩展块）。

之后用户可以使用收到的文件来访问加密驱动器和读取驱动器上存储的数据。

用户和用户角色

该部分描述了用户和用户角色，并提供创建和修改它们、分配角色和组到用户以及关联策略配置文件到角色的说明。

关于用于角色

用户角色（也叫*角色*）是包含一组权限集的对象。角色可以与安装在用户设备上的卡巴斯基应用程序设置关联。您可以分配角色到用户集，或者到管理组层级的任何级别、管理服务器或特定对象级别的安全组集。

如果您通过包含虚拟管理服务器的管理服务器层级来管理设备，请注意，您仅可从物理管理服务器创建、修改或删除用户角色。这样，您可以将用户角色传输到从属管理服务器，包括虚拟服务器。

您可以关联用户角色到策略配置文件。如果用户被分配角色，用户将获得执行工作职能所需的安全设置。

一个用户角色可以与特定管理组中的设备用户关联。

用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

使用角色的好处

使用角色的好处之一是您不必为每个受管理设备或用户指定安全设置。公司中的用户和设备数量可能太大，但是需要不同安全设置的不同工作的数量相对较小。

与使用策略配置文件的不同点

策略配置文件是为每个卡巴斯基应用程序创建的策略的属性。角色与许多为不同应用程序创建的策略配置文件相关联。因此，角色是联合特定用户类型的设置到一处的方法。

查看用户账户和会话

Kaspersky Security Center 允许您管理用户账户以及账户组。该程序支持两种账户类型:

- 组织员工的账户。在轮询组织网络时管理服务器检索数据的用户账户。
- 内部用户账户。当使用虚拟管理服务器时，这些账户被应用。只能在 Kaspersky Security Center 内创建和使用内部用户账户。

您可以通过下列方式之一查看用户账户和会话列表：

- 在主菜单中，转到**用户和角色** → **用户和组**。
- 在主菜单中，转到**资产(设备)** →**受管理设备**→<设备名称>链接 →**常规**选项卡 →**常规**部分 →**会话**块。
  会话部分显示运行 Windows 的设备上具有活动会话的用户账户。

如果满足以下要求，用户账户和会话列表将正确显示：

- 使用与管理服务器相同版本或更高版本的网络代理。
- Active Directory 轮询已启用以显示域用户的账户。
- 在运行 Windows 的受管理设备上，**服务器** (**LanmanServer**) 服务正在运行。

配置对应用程序功能的访问权限。基于角色的访问控制

Kaspersky Security Center 针对 Kaspersky Security Center 和受管理 Kaspersky 应用程序的功能提供了基于角色的访问手段。

您可以通过以下方式之一为 Kaspersky Security Center 用户配置对应用程序功能的访问权限：

- 通过为每个用户或用户组单独配置权限。
- 通过使用一组预定义的权限创建标准用户角色并根据用户的职责范围将这些角色分配给用户。

应用用户角色旨在简化和缩短配置用户对应用程序功能的访问权限的常规程序。角色内的访问权限根据标准任务和用户的职责范围进行配置。

可为用户角色分配与其各自的目的对应的名称。您可在程序中创建无限数量的角色。

您可以将预定义的用户角色与已经配置的权限集一起使用，或者创建新角色并自行配置所需的权限。

应用程序功能的访问权限

下表显示了 Kaspersky Security Center 的功能，以及用于管理关联任务、报告、设置和执行关联用户操作的访问权限。

要执行表中列出的用户操作，用户必须拥有该操作旁边指定的权限。

读取、**写入**和**执行**权限适用于任何任务、报告或设置。除这些权限外，要针对设备分类管理任务、报告或设置，用户还需要拥有“**为设备分类执行操作**”权限。

> 表中缺少的所有任务、报告、设置和安装包均属于“**常规功能：基本功能**”功能区域。

应用程序功能的访问权限

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：管理组的管理	**写入**	• 将设备添加到管理组：**写入** • 从管理组中删除设备：**写入** • 将管理组添加到另一个管理组：**写入** • 将管理组从另一个管理组中删除：**写入**	无	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：访问对象而不考虑它们的 ACLs	**读取**	获取对所有对象的读取权限：**读取**	无	无	**常规功能：访问对象而不考虑它们的** ACLs功能区域用于审计目的。当用户被授予此功能区域的**读取**权限时，他们将获得对所有对象的完全**读取**权限，并能够以本地管理员权限（Linux 的 root 权限）在通过网络代理连接到管理服务器的设备上执行任何创建的任务。我们建议谨慎地将这些权限授予有限数量的用户，这些用户需要这些权限来履行工作职责。 即使其他权限禁止对特定对象的读取访问，访问权限也会被授予。
常规功能：基本功能	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 虚拟服务器的设备移动规则（创建、修改或删除）：**写入**、**为设备分类执行操作** • 获取移动 (LWNGT) 协议自定义证书：**读取** • 设置移动 (LWNGT) 协议自定义证书：**写入** • 获取 NLA 定义的网络列表：**读取** • 添加、修改或删除 NLA 定义的网络列表：**写入** • 查看组的访问控制列表：**读取** • 查看卡巴斯基事件日志：**读取** • 查看用于恢复对 BitLocker 加密的硬盘的访问权限的恢复密钥：**执行**	• “将更新下载至管理服务器存储库” • “提交报告” • “分发安装包” • “在从属管理服务器上远程安装应用程序”	• “保护状态报告” • “威胁报告” • “感染最严重的设备报告” • “反病毒数据库状态报告” • “错误报告” • “网络攻击报告” • “已安装的邮件系统保护应用程序汇总报告” • “已安装的周边防护应用程序汇总报告” • “已安装的应用程序类型汇总报告” • “受感染的设备用户报告” • “事故报告” • “事件报告” • “分发点活动报告” • “从属管理服务器报告” • “设备控制事件报告” • “漏洞报告” • “禁止的应用程序报告” • “Web 控制报告” • “受管理设备加密状态报告” • “大容量存储设备加密状态报告” • “文件加密错误报告” • “加密文件访问被阻止报告” • “加密设备访问权限报告” • “有效用户权限报告” • “权限报告”	无
常规功能：已删除对象	• **读取** • **写入**	• 查看回收站中的已删除对象：**读取** • 删除回收站中的对象：**写入**	无	无	无
常规功能：事件处理	• **删除事件** • **编辑事件通知设置**	• 更改事件注册设置：**编辑事件记录设置** • 更改事件通知设置：**编辑事件通知设置** • 删除事件：**删除事**	无	无	设置： • 病毒爆发设置：创建病毒爆发事件所需的病毒检测数量 • 病毒爆发设置：评估病毒检测的时间段 • 数据库中存储的最大事件数量 • 已删除设备中事件的存储时间段

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
	• **编辑事件记录设置** • **写入**	**件**			
常规功能：在管理服务器上的操作	• **读取** • **写入** • **执行** • **修改对象 ACL** • **为设备分类执行操作**	• 指定用于连接网络代理的管理服务器端口：**写入** • 指定在管理服务器上启动的激活代理端口：**写入** • 指定在管理服务器上启动的移动激活代理端口：**写入** • 指定用于分发独立安装包的 Web 服务器端口：**写入** • 指定用于分发 MDM 配置文件的 Web 服务器端口：**写入** • 指定用于通过 Kaspersky Security Center Web Console 连接的管理服务器 SSL 端口：**写入** • 指定用于移动连接的管理服务器端口：**写入** • 指定管理服务器数据库中存储的最大事件数量：**写入** • 指定管理服务器可以发送的最大事件数量：**写入** • 指定管理服务器可以发送事件的时间段：**写入**	• “备份管理服务器数据” • “数据库维护”	无	无
常规功能：卡巴斯基应用程序部署	• **管理卡巴斯基补丁** • **读取** • **写入** • **执行** • **为设备分类执行操作**	批准或拒绝安装补丁：**管理卡巴斯基补丁**	无	• “虚拟管理服务器授权许可密钥使用报告” • “Kaspersky 软件版本报告” • “不兼容的应用程序报告” • “Kaspersky 软件模块更新版本报告” • “保护部署报告”	安装包：“Kaspersky”
常规功能：授权许可密钥管理	• **导出密钥文件** • **写入**	• 导出密钥文件：**导出密钥文件** • 修改管理服务器授权许可密钥设置：**写入**	无	无	无
常规功能：强制报告管理	• **读取** • **写入**	• 创建报告而不考虑它们的 ACL：**写入** • 执行报告而不考虑它们的 ACL：**读取**	无	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：管理服务器层级	**配置管理服务器层级**	注册、更新或删除从属管理服务器：**配置管理服务器层级**	无	无	无
常规功能：用户权限	**修改对象** ACL	• 更改任何对象的“安全”属性：**修改对象** ACL • 管理用户角色：**修改对象** ACL • 管理内部用户：**修改对象** ACL • 管理安全组：**修改对象** ACL • 管理别名：**修改对象** ACL	无	无	无
常规功能：虚拟管理服务器	• **管理虚拟管理服务器** • **读取** • **写入** • **执行** • **为设备分类执行操作**	• 获取虚拟管理服务器列表：**读取** • 获取关于虚拟管理服务器的信息：**读取** • 创建、更新或删除虚拟管理服务器：**管理虚拟管理服务器** • 将虚拟管理服务器移动到另一个组：**管理虚拟管理服务器** • 设置管理虚拟服务器权限：**管理虚拟管理服务器**	无	“第三方软件更新安装结果报告”	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
常规功能：加密密钥管理	**写入**	导入加密密钥：**写入**	无	无	无
移动设备管理：常规	• **连接新设备** • **仅发送信息命令到移动设备** • **发送命令到移动设备** • **管理证书** • **读取** • **写入**	• 获取密钥管理服务还原数据：**读取** • 删除用户证书：**管理证书** • 获取用户证书的公开部分：**读取** • 检查是否启用了公钥基础结构：**读取** • 检查公钥基础结构账户：**读取** • 获取公钥基础结构模板：**读取** • 通过扩展密钥用法证书获取公钥基础结构模板：**读取** • 检查公钥基础结构证书是否被吊销：**读取** • 更新用户证书发行设置：**管理证书** • 获取用户证书发行设置：**读取** • 按应用程序名称和版本获取软件包：**读取** • 设置或取消用户证书：**管理证书** • 续订用户证书：**管理证书** • 设置用户证书标签：**管理证书** • 运行 MDM 安装包的生成；取消生成 MDM 安装包：**连接新设备**	无	无	无
系统管理：连接	• **启动 RDP 会话** • **连接到现有 RDP 会话** • **创建通道** • **在管理员工作站上保存设备文件** • **读取** • **写入** • **执行** • **为设备分类执行操作**	• 创建桌面共享会话：**启动 RDP 会话** • 创建 RDP 会话：**连接到现有 RDP 会话** • 创建隧道：**创建通道** • 保存内容网络列表：**在管理员工作站上保存设备文件**	无	“设备用户报告”	无
系统管理：硬件清单	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 获取或导出硬件清单对象：**读取** • 添加、设置或删除硬件清单对象：**写入**	无	• “硬件注册报告” • “配置更改报告” • “硬件报告”	无
系统管理：网络访问控制	• **读取** • **写入**	• 查看 CISCO 设置：**读取** • 更改 CISCO 设置：**写入**	无	无	无

功能区域	权限	用户操作：执行操作所需的权限	任务	报告	其他
系统管理：操作系统部署	• **部署 PXE 服务器** • **读取** • **写入** • **执行** • **为设备分类执行操作**	• 部署 PXE 服务器：**部署 PXE 服务器** • 查看 PXE 服务器列表：**读取** • 在 PXE 客户端上启动或停止安装过程：**执行** • 管理 WinPE 驱动程序和操作系统映像：**写入**	“基于参考设备操作系统映像创建安装包”	无	安装包：“操作系统映像”
系统管理：漏洞和补丁管理	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 查看第三方补丁属性：**读取** • 更改第三方补丁属性：**写入**	• “执行 Windows Update 同步” • “安装 Windows Update 更新” • “修复漏洞” • “安装所需更新并修复漏洞”	“软件更新报告”	无
系统管理：远程安装	• **读取** • **写入** • **执行** • **为设备分类执行操作**	• 查看基于第三方漏洞和补丁管理的安装包属性：**读取** • 更改基于第三方漏洞和补丁管理的安装包属性：**写入**	无	无	安装包： • “自定义应用程序” • “VAPM 包”
系统管理：软件清单	• **读取** • **写入** • **执行** • **为设备分类执行操作**	无	无	• “已安装的应用程序报告” • “应用程序注册历史记录报告” • “已授权应用程序组状态报告” • “第三方软件授权许可密钥报告”	无
系统管理：远程执行脚本	• **读取** • **写入** • **执行** • **为设备分类执行操作**	用户可以查看任务属性：**读取** 用户可以创建、删除或修改安装包：**写入** 用户可以运行任务：**写入**。在客户端 Linux 设备上，脚本以 root 权限执行。 用户可以运行任务或安排其运行：**执行** 用户可以在所选设备上运行任务：**为设备分类执行操作**	“远程执行脚本”	无	无

预定义用户角色

分配给 Kaspersky Security Center 用户的用户角色为他们提供了对应用程序功能的访问权限集。

在虚拟服务器上创建的用户无法在管理服务器上被分配角色。

您可以将预定义的用户角色与已经配置的权限集一起使用，或者创建新角色。当创建新角色时，您必须自己设置角色范围并分配对 Kaspersky Security Center 功能的访问权限。Kaspersky Security Center 中有些预定义用户角色可以与特定的职位相关联，例如：**审计员**、**安全官**、**主管**（这些角色从版本 11 开始在 Kaspersky Security Center 中出现）。这些角色的访问权限是根据标准任务和相关职位的职责范围预先配置的。下表显示了角色如何与特定职位相关联。

特定职位角色示例

角色	注释
审计员	允许在通过网络代理以本地管理员权限（Linux 为 root）连接到管理服务器的选定设备上执行所有查看操作和执行任何创建的任务。 我们建议谨慎地将该角色指派给有限数量的用户，这些用户需要它们来履行工作职责。
管理者	允许所有查看操作；不允许其他操作。您可以分配该角色到负责您组织的 IT 安全的安全官和其他管理员。
安全官	允许所有查看操作，允许报告管理；在**系统管理**：**连接**区域授予有限的权限。您可以分配该角色到负责您组织的 IT 安全的安全官。

下表显示了分配给每个预定义用户角色的访问权限。

预定义用户角色的访问权限

角色	描述

管理服务器管理员	允许在以下功能区域的所有操作：
	• **常规功能**：
	  • **基本功能**
	  • **事件处理**
	  • **管理服务器层级**
	  • **虚拟管理服务器**
	• **系统管理**：
	  • **连接**
	  • **硬件清单**
	  • **软件清查**
	授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。

管理服务器操作员	授予在以下所有功能区域的**读取**和**执行**权限：
	• **常规功能**：
	  • **基本功能**
	  • **虚拟管理服务器**
	• **系统管理**：
	  • **连接**
	  • **硬件清单**
	  • **软件清查**

审计员	在“**常规功能**”中，允许功能区域内的所有操作： • **访问对象而不考虑它们的 ACL** • **删除对象** • **强制报告管理** 您可以分配该角色到执行您组织的审计的人。

角色	描述

安装管理员	允许在以下功能区域的所有操作：
	• **常规功能**：
	  • **基本功能**
	  • **Kaspersky 软件部署**
	  • **授权许可密钥管理**
	• **系统管理**：
	  • **操作系统部署**
	  • **漏洞和补丁管理**
	  • **远程安装**
	  • **软件清查**
	授予在“**常规功能：虚拟管理服务器**”功能区域的**读取**和**执行**权限。

安装操作员	授予在以下所有功能区域的**读取**和**执行**权限：
	• **常规功能**：
	  • **基本功能**
	  • **Kaspersky 软件部署**（也授予在该区域的**管理 Kaspersky 补丁**权限）
	  • **虚拟管理服务器**
	• **系统管理**：
	  • **操作系统部署**
	  • **漏洞和补丁管理**
	  • **远程安装**
	  • **软件清查**

Kaspersky Endpoint Security 管理员	允许在以下功能区域的所有操作： • **常规功能：基本功能** • Kaspersky Endpoint Security 区域，包括所有功能 授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。
Kaspersky Endpoint Security 操作员	授予在以下所有功能区域的**读取**和**执行**权限： • **常规功能：基本功能** • Kaspersky Endpoint Security 区域，包括所有功能
主管理员	在“**常规功能**”中，*除*以下区域外，允许功能区域内的所有操作： • **访问对象而不考虑它们的 ACL** • **强制报告管理** 授予在“**常规功能：加密密钥管理**”功能区域的**读取**和**写入**权限。

角色	描述

主要操作员	授予在以下所有功能区域的**读取**和**执行**（如果适用）权限：
	• **常规功能**：
	  • **基本功能**
	  • **删除对象**
	  • **管理服务器上的操作**
	  • **卡巴斯基应用程序部署**
	  • **虚拟管理服务器**
	• **移动设备管理：常规**
	• **系统管理**，包括所有功能
	• Kaspersky Endpoint Security 区域，包括所有功能

“移动设备管理”管理员	允许在以下功能区域的所有操作： • **常规功能：基本功能** • **移动设备管理：常规**
“移动设备管理”操作员	授予在“**常规功能**：**基本功能**”功能区域中“**读取**”和“**执行**”的权限。 在“**移动设备管理**：**常规**”功能区域中，授予“**读取**”和“**仅发送信息命令到移动设备**”的权限。
安全官	在“**常规功能**”中，允许以下功能区域中的所有操作： • **访问对象而不考虑它们的** ACL • **强制报告管理** 授予在“**系统管理：连接**”功能区域的“**读取**”、“**写入**”、“**执行**”、“**将设备中的文件保存到管理员工作站**”和“**对设备分类执行操作**”权限。 您可以分配该角色到负责您组织的 IT 安全的安全官。
Self Service Portal 用户	允许在“**移动设备管理：Self Service Portal**”功能区域的所有操作。Kaspersky Security Center 11 和更高版本不支持此功能。
管理者	授予在“**常规功能**：**访问对象而不考虑它们的** ACL”和“**常规功能**：**强制报表管理**”功能区域的**读取**权限。 您可以分配该角色到负责您组织的 IT 安全的安全官和其他管理员。
“漏洞和补丁管理”管理员	允许在“**常规功能**：**基本功能**”和“**系统管理**”（包括所有功能）功能区域的所有操作。
“漏洞和补丁管理”操作员	授予在“**常规功能**：**基本功能**”和“**系统管理**”（包括所有功能）功能区域的**读取**和**执行**（如果适用）权限。

分配对特定对象的访问权限

除了分配服务器级别的访问权限，您还可以配置对特定对象的访问，例如对特定任务的访问。该应用程序允许您指定对以下对象类型的访问权限：

- 管理组
- 任务
- 报告
- 设备分类
- 事件分类

要分配对特定对象的访问权限：

1. 根据对象类型，在主菜单中转到相应区域：
   - **资产(设备) → 组层级**
   - **资产(设备)→任务**
   - **监控和报告 → 报告**
   - **资产(设备)→设备分类**
   - **监控和报告 → 事件分类**
2. 打开要为其配置访问权限的对象的属性。
   要打开管理组或任务的属性窗口，单击对象名称。其他对象的属性可以使用工具栏上的按钮打开。
3. 在属性窗口中，打开**访问权限**部分。
   用户列表将打开。列出的用户和安全组具有对象的访问权限。默认情况下，如果您使用管理组或服务器的层级，则列表和访问权限是从父管理组或主服务器继承的。
4. 为了能够修改列表，启用**使用自定义权限**选项。
5. 配置访问权限：
   - 使用**添加**和**删除**按钮修改列表。
   - 指定用户或安全组的访问权限。执行以下操作之一：
     - 如果要手动指定访问权限，请选择用户或安全组，单击“**访问权限**”按钮，然后指定访问权限。
     - 如果要分配一个用户角色到用户或安全组，请选择用户或安全组，单击“**角色**”按钮，然后选择要分配的角色。
6. 单击“**保存**”按钮。

配置对象的访问权限。

向用户和安全组分配访问权限

您可以授予用户和安全组访问权限，以使用管理服务器的不同功能，例如 Kaspersky Endpoint Security for Linux。

为用户或安全组分配访问权限：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**访问权限**”选项卡上，选中要分配权限的用户或安全组名称旁边的复选框，然后单击“**访问权限**”按钮。
   您不能同时选择多个用户或安全组。如果您选择了多个条目，“**访问权限**”按钮将被禁用。

3. 配置用户或组的权限集：

   a. 使用管理服务器或其他卡巴斯基应用程序的功能扩展节点。

   b. 选择所需功能或访问权限旁边的**允许**或**拒绝**复选框。

   *示例 1：*选中**应用程序集成**节点旁边的**允许**复选框，向用户或组授予对应用程序集成功能（**读取**、**写入**和**执行**）的所有可用访问权限。

   *示例 2：*展开**加密密钥管理**节点，然后选中写入权限旁边**的允许**复选框，以授予用户或组对加密密钥管理功能的**写入**访问权限。

4. 配置访问权限集后，单击**确定**。

用户或用户组的权限集将被配置。

管理服务器（或管理组）的权限被分成以下部分：

- 常规功能：
  - 管理组的管理
  - 访问对象而不考虑它们的 ACLs
  - 基本功能
  - 已删除对象
  - 加密密钥管理
  - 事件处理
  - 在管理服务器上的操作（仅位于管理服务器的属性窗口中）
  - 设备标签
  - 卡巴斯基应用程序部署
  - 授权许可密钥管理
  - 应用程序整合
  - 强制报告管理
  - 管理服务器层级
  - 用户权限
  - 虚拟管理服务器
- 移动设备管理：
  - 常规
  - Self Service Portal

- 系统管理：
  - 连接
  - 远程执行脚本
  - 硬件清单
  - 网络访问控制
  - 操作系统部署
  - 漏洞和补丁管理
  - 远程安装
  - 软件清单

如果没有为访问权限选择“**允许**”或“**拒绝**”，则该访问权限被认为*未定义*：它将被拒绝，直到被用户明确拒绝或允许为止。

用户权限是以下各项的集合：

- 用户自己的权限
- 分配给该用户的所有角色的权限
- 用户所属的所有安全组的权限
- 分配到用户所属安全组的所有角色的权限

如果至少一个权限集对权限“**拒绝**”，那么用户被拒绝该权限，即便其他集允许它或保持未定义。

您还可以将用户和安全组添加至用户角色范围，以使用管理服务器的不同功能。与用户角色关联的设置只应用到属于拥有该角色的用户的设备，并且这些设备只属于与该角色关联的组，包括子组。

添加内部用户账户

如果您想要添加用户账户，请确保您的账户在常规功能：用户权限功能区域中具有修改对象 ACL权限。

要添加新内部用户账户到 Kaspersky Security Center：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击**添加**。
3. 在打开的“**添加用户**”窗口中，指定新用户账户设置：
   - **名称**
   - **密码**

密码必须符合以下规则：

- 密码的字符长度必须是 8 到 256 位。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

要查看输入的密码，请单击。
您可以启用**用户必须在首次登录时更改密码**选项，以在第一次用户身份验证时强制更改密码。

4. 保存更改以完成新用户账户的创建。

新的用户账户将被添加到用户列表中。

要使用已创建的内部用户账户登录 Kaspersky Security Center Web Console，您必须为该帐户分配一个角色。登录前，请确保该内部用户账户已分配角色。否则，将会出现登录错误。

创建安全组

要创建安全组：

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**组**选项卡。
2. 单击**添加**。
3. 在打开的**创建安全组**窗口中，为新安全组指定以下设置：
   - **组名称**
   - **描述**
4. 单击“**保存**”保存设置。

新的安全组已被添加到组列表中。

编辑内部用户账户

如果您想要编辑用户账户，请确保您的账户在常规功能：用户权限功能区域中具有修改对象 ACL权限。

要在 Kaspersky Security Center 中编辑内部用户账户：

1. 在主菜单中，转至**用户和角色 → 用户和组**，然后选择**用户**选项卡。
2. 单击您要编辑的用户账户名称。
3. 在打开的用户设置窗口中的“**常规**”选项卡上，更改用户账户设置：
   - **用户状态**

     如果必要，将切换按钮切换到“**已禁用**”以禁止用户连接到应用程序。您可以禁用账户，例如，在员工离职后。
   - **名称**
   - **完整名称**
   - **描述**
   - **邮件地址**
   - **主电话**
   - **密码**

     如有必要，您可以按如下方式为用户连接到 Kaspersky Security Center 设置新密码：

     a. 单击**更改密码**按钮，然后为用户账户设置新密码。
     密码必须符合以下规则：
     - 密码的字符长度必须是 8 到 256 位。
     - 密码必须包含以下组中三组的字符：
       - 大写字母 (A-Z)
       - 小写字母 (a-z)
       - 数字 (0-9)
       - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

     要查看输入的密码，请单击。

     b. 如有必要，启用**用户必须在首次登录时更改密码**选项，以在下次用户身份验证时强制更改密码。

     c. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定在常规功能：用户权限功能区域中具有修改对象 ACL权限的账户的凭据。
4. 在“**身份验证安全**”选项卡上，可以指定此账户的安全设置。
5. 在“**组**”选项卡上，可以添加用户到安全组。

6. 在“**设备**”选项卡上，可以分配设备到用户。
7. 在“**角色**”选项卡上，可以分配角色到用户。
8. 保存更改以完成用户账户的编辑。

更新的用户账户出现在用户列表中。

编辑安全组

要编辑安全组：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**组**选项卡。
2. 单击您要编辑的安全组名称。
3. 在打开的组设置窗口中，更改安全组设置：
   - 在“**常规**”选项卡上，您可以更改“**名称**”和“**描述**”设置。这些设置仅适用于内部安全组。
   - 在“**用户**”选项卡上，可以添加用户到安全组。此设置仅适用于内部用户和内部安全组。
   - 在“**角色**”选项卡上，可以分配角色到安全组。
4. 单击“**保存**”保存设置。

更改将应用于安全组。

为用户或安全组分配角色

为用户或安全组分配角色：

1. 在主菜单中，转至**用户和角色**→**用户和组**，然后选择**用户**或**组**选项卡。
2. 选择要向其分配角色的用户或安全组的名称。
   您可以选择多个名称。
3. 在菜单项目上，单击“**分配角色**”按钮。
   角色分配向导启动。
4. 按照向导的说明进行操作：选择要分配给所选用户或安全组的角色，然后选择角色的范围。
   用户角色范围是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

拥有一组管理服务器使用权限的角色将被指派给用户（或多个用户，或安全组）。在用户或安全组列表中，**已分配角色**列中会出现一个复选框。

在虚拟服务器上创建的用户无法在管理服务器上被分配角色。

添加用户账户到内部安全组

您仅可以添加内部用户账户到内部安全组。

要添加用户账户到内部安全组：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 选择您要添加到安全组的用户账户旁边的复选框。
3. 单击“**分配组**”按钮。
4. 在打开的“**分配组**”窗口中，选择要将用户账户添加到的安全组。
5. 单击“**保存**”按钮。

用户账户被添加到安全组。您还可以使用组设置将内部用户添加到安全组。

将用户指定为设备所有者

有关如何将用户指定为移动设备所有者的信息，请参阅Kaspersky Secure Mobility Management帮助文档。

要指派用户作为设备所有者：

1. 如果要分配连接到虚拟管理服务器的设备的所有者，请先切换到虚拟管理服务器：
   a. 在主菜单中，单击当前管理服务器名称右侧的 V 形图标 ()。
   b. 选择所需的管理服务器。
2. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
   系统打开一个用户列表。如果您当前连接到虚拟管理服务器，则该列表包括来自当前虚拟管理服务器和主管理服务器的用户。
3. 单击您要分配为设备所有者的用户账户名称。
4. 在打开的用户设置窗口中，选择“**设备**”选项卡。
5. 单击**添加**。
6. 从设备列表中，选择您要分配给用户的设备。
7. 单击“**确定**”。

所选的设备被添加到分配给用户的设备列表。

您可以在“**资产(设备)**”→“**受管理设备**”中执行相同操作，方法是单击要分配的设备名称，然后单击“**管理设备所有者**”链接。

为所有用户配置两步验证

此方案描述如何为所有用户启用两步验证，以及如何从两步验证中排除用户账户。如果您在为其他用户启用两步验证之前没有为您的账户启用两步验证，则应用程序会先打开用于为您的账户启用两步验证的窗口。此方案还描述了如何为您自己的账户启用两步验证。

如果您为账户启用了两步验证，则可以进入为所有用户启用两步验证的阶段。

先决条件

在开始之前：

- 确保您的用户账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，以修改其他用户账户的安全设置。
- 确保管理服务器的其他用户在其设备上安装了认证应用。

阶段

为所有用户启用两步验证分阶段进行：

1. **在设备上安装认证应用**

   您可以安装任何支持基于时间的一次性密码算法 (TOTP) 的应用程序，例如：

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost 验证器
   - Aladdin 2FA

   要检查 Kaspersky Security Center 是否支持您要使用的身份验证器应用，请为所有用户或特定用户启用两步验证。

   其中一个步骤会建议您指定由身份验证器应用生成的安全代码。如果成功，则 Kaspersky Security Center 支持所选的身份验证器。

   我们强烈建议不要在与管理服务器建立连接的同一台设备上安装认证应用。

2. **将认证应用时间与安装了管理服务器的设备的时间同步**

   通过使用外部时间源，确保具有身份验证器应用的设备上的时间和具有管理服务器的设备上的时间与 UTC 同步。否则，两步验证的认证和激活过程中可能会出现失败。

3. **为您的账户启用两步验证，并接收您的账户的 secret key**

   说明：

   - 对于基于 MMC 的管理控制台：为您自己的账户启用两步验证
   - 对于 Kaspersky Security Center Web Console：为您自己的账户启用两步验证

   为您的账户启用两步验证后，可以为所有用户启用两步验证。

4. **为所有用户启用两步验证**

   启用了两步验证的用户必须使用它才能登录到管理服务器。

   说明：

   - 对于基于 MMC 的管理控制台：为所有用户启用两步验证
   - 对于 Kaspersky Security Center Web Console：为所有用户启用两步验证

5. **编辑安全代码颁发者的名称**

   如果您有多个具有相似名称的管理服务器，则可能需要更改安全代码颁发者名称，以便更好地识别不同的管理服务器。

   说明：

   - 对于基于 MMC 的管理控制台：编辑安全代码颁发者的名称
   - 对于 Kaspersky Security Center Web Console：编辑安全代码颁发者的名称

6. **排除不需要启用两步验证的用户账户**

   如果需要，您可以从两步验证中排除用户。具有已排除的账户的用户不必使用两步验证即可登录到管理服务器。

   说明：

   - 对于基于 MMC 的管理控制台：从两步验证中排除账户
   - 对于 Kaspersky Security Center Web Console：从两步验证中排除账户

7. **为您自己的账户配置两步验证**

   如果用户未被排除在两步验证之外，并且尚未为其账户配置两步验证，则他们需要在登录Kaspersky Security Center 时打开的窗口中进行配置。否则，他们将无法按照其权限访问管理服务器。

   说明：

   - 对于基于 MMC 的管理控制台：为您自己的账户配置两步验证
   - 对于 Kaspersky Security Center Web Console：为您自己的账户配置两步验证

结果

完成此方案后：

- 您的账户已启用两步验证。
- 管理服务器的所有用户账户均已启用两步验证，但已排除的用户账户除外。

关于两步验证

为账户启用两步验证后，除了用户名和密码外，还需要一次性安全代码才能登录管理控制台或者 Kaspersky Security Center Web Console。启用域认证后，用户只需输入一次性安全码即可。

要使用两步验证，请在移动设备或计算机上安装可生成一次性安全码的认证应用。您可以使用任何支持基于时间的一次性密码算法 (TOTP) 的应用程序，例如：

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex ID
- Avanpost 验证器
- Aladdin 2FA

要检查 Kaspersky Security Center 是否支持您要使用的身份验证器应用，请为所有用户或特定用户启用两步验证。

其中一个步骤会建议您指定由身份验证器应用生成的安全代码。如果成功，则 Kaspersky Security Center 支持所选的身份验证器。

> 我们强烈建议您保存 secret key 或二维码，并将其保管在安全的地方。万一您失去对移动设备的访问权限，这将帮助您恢复对 Kaspersky Security Center Web Console 的访问权限。

为了保护 Kaspersky Security Center 的使用，您可以为您自己的账户启用两步验证，并为所有用户启用两步验证。

> 您可以从两步验证中排除账户。对于无法接收安全代码进行身份验证的服务账户，这可能是必需的。

规则和限制

为了能够为所有用户激活两步验证并为特定用户停用两步验证：

- 确保您的账户在“**常规功能：用户权限**”功能区域中拥有修改对象 ACL 权限。
- 为账户启用两步验证。

为了能够为所有用户停用两步验证：

- 确保您的账户在“**常规功能：用户权限**”功能区域中拥有修改对象 ACL 权限。
- 使用两步验证登录 Kaspersky Security Center Web Console。

如果在 Kaspersky Security Center 管理服务器 13 或者更高版本上为某个用户账户启用了两步验证，则该用户将无法登录 Kaspersky Security Center Web Console 12、12.1 或 12.2。

重新发布安全密钥

任何用户都可以重新发布用于两步验证的密钥。当用户使用重新发布的安全密钥登录到管理服务器时，将为用户账户保存新的安全密钥。如果用户输入错误的新密钥，则新密钥不会得到保存，当前密钥仍然有效。

安全代码具有一个称为*颁发者名称*的标识符。安全代码颁发者名称用作管理服务器在认证应用中的标识符。安全代码颁发者名称的默认值与管理服务器的名称相同。您可以更改安全代码颁发者的名称。如果更改安全代码颁发者名称，则必须颁发新的 secret key 并将其传递给认证应用。

为您自己的账户启用两步验证（Web Console）

您只能为您自己的账户启用两步验证。

在为账户启用两步验证之前，请确保移动设备上安装了认证应用。确保认证应用中设置的时间与安装了管理服务器的设备的时间设置同步。

要为用户账户启用两步验证：

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 单击您的账户的名称。
3. 在打开的用户设置窗口中，选择“**身份验证安全**”选项卡。
4. 在**身份验证安全**选项卡上：
   a. 选择**请求用户名、密码和安全码(两步验证)**选项。单击“**保存**”按钮。
   b. 在打开的两步验证窗口中，点击**查看如何建立两步验证**。
      在认证应用中输入 secret key 或单击“**查看二维码**”并通过移动设备上的认证应用来扫描二维码以接收一次性安全码。
   c. 在两步验证窗口中，指定由认证应用生成的安全代码，然后单击“**检查和应用**”按钮。
5. 单击“**保存**”按钮。

您的账户已启用两步验证。

为您自己的账户启用两步验证（基于 MMC）

在为账户启用两步验证之前，请确保移动设备上安装了认证应用。确保认证应用中设置的时间与管理服务器的时间同步。

要为账户启用两步验证：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单，然后选择“**属性**”。
2. 在管理服务器属性窗口中，转到“**区域**”窗格，然后选择“**高级**”，再选择“**两步验证**”。
3. 在“**两步验证**”区域中，单击“**设置**”按钮。

   如果您的账户已启用两步验证，点击**“设置”**按钮将重置 secret key，以便您可以重新配置两步验证。

   在打开的两步验证属性窗口中，将显示 secret key。
4. 在认证应用中输入 secret key 以接收一次性安全码。您可以手动将 secret key 输入到认证应用中，或通过移动设备上的认证应用来扫描二维码。
5. 指定认证应用生成的安全码，然后单击“**确定**”按钮退出两步验证属性窗口。
6. 单击“**应用**”按钮。
7. 单击“**确定**”按钮。

您自己的账户已启用两步验证。

对所有用户启用必需的两步验证（Web Console）

如果您的账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且您已通过两步验证进行了身份验证，则可以为管理服务器的所有用户启用两步验证。

要为所有用户启用两步验证：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标（ ）。

   管理服务器属性窗口将打开。
2. 在属性窗口的“**身份验证安全**”选项卡上，将“**所有用户的两步验证**”选项的切换按钮切换到启用位置。

3. 如果您没有为您的账户启用两步验证，则应用程序会打开为您自己的账户启用两步验证的窗口。

   a. 在两步验证窗口中，单击**查看如何建立两步验证**。

   b. 在身份验证器应用程序中手动输入 secret key，或者点击“**查看二维码**”，然后使用移动设备上的身份验证器应用程序扫描该二维码，以获取一次性安全码。

   c. 在两步验证窗口中，指定由认证应用程序生成的安全代码，然后单击“**检查和应用**”按钮。

所有用户均已启用两步验证。从现在开始，除了从两步验证中排除的用户，管理服务器的用户（包括为所有用户启用两步验证之后添加的用户）必须为他们的账户配置两步验证。

为所有用户启用两步验证（基于 MMC）

如果您的账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且您已通过两步验证进行了身份验证，则可以为管理服务器的所有用户启用两步验证。

要为所有用户启用两步验证：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单，然后选择“**属性**”。
2. 在管理服务器属性窗口的“**区域**”窗格中，选择“**高级**”，然后选择“**两步验证**”。
3. 单击“**设置为必须**”按钮为所有用户启用两步验证。
4. 如果您没有为您的账户启用两步验证，则应用程序会打开为您自己的账户启用两步验证的窗口。

   a. 在认证应用中输入 secret key 以接收一次性安全码。您可以手动将 secret key 输入到认证应用中，也可以通过移动设备上的认证应用来扫描二维码以接收一次性安全码。

   b. 指定认证应用生成的安全码，然后单击“**确定**”按钮退出两步验证属性窗口。
5. 在“**两步验证**”区域中，单击“**应用**”按钮，然后单击“**确定**”按钮。

所有用户均已启用两步验证。从现在开始，所有管理服务器的用户，包括启用此选项后添加的用户，都必须为他们的账户配置两步验证，除了那些账户被排除在两步验证之外的用户。

禁用用户账户（Web Console）的两步验证

您可以禁用您自己的账户以及任何其他用户账户的两步验证。

如果您的账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且您已通过两步验证进行了身份验证，则可以对其他用户的账户禁用两步验证。

要禁用用户账户的两步验证：

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 单击要为其禁用两步验证的内部用户账户的名称。这可能是您自己的账户或任何其他用户的账户。

3. 在打开的用户设置窗口中，选择“**账户保护**”选项卡。

4. 如果要禁用用户账户的两步验证，请在“**账户保护**”选项卡上选择“**仅请求用户名和密码**”选项。

5. 单击“**保存**”按钮。

该用户账户已禁用两步验证。

如果您想要为无法使用两步验证登录 Kaspersky Security Center Web Console 的用户恢复访问权限，请禁用此用户账户的两步验证，然后选择上述“**仅请求用户名和密码**”选项。之后，使用您禁用两步验证的用户账户登录 Kaspersky Security Center Web Console，然后再次启用验证。

禁用用户账户的两步验证（基于 MMC）

要禁用您自己的账户的两步验证：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单，然后选择“**属性**”。

2. 在管理服务器属性窗口的“**区域**”窗格中，选择“**高级**”，然后选择“**两步验证**”。

3. 在“**两步验证**”区域中，单击“**禁用**”按钮。

4. 单击“**应用**”按钮。

5. 单击“**确定**”按钮。

您的账户已禁用两步验证。

您可以禁用其他用户账户的两步验证。这在移动设备丢失或损坏等情况下提供了保护。

如果您在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且您已通过两步验证进行了身份验证，则可以对其他用户的账户禁用两步验证。按照以下步骤操作，您也可以禁用您自己的账户的两步验证。

要禁用任意用户账户的两步验证：

1. 在控制台树中，打开“**用户账户**”文件夹。
   默认情况下，“**用户账户**”文件夹是“**高级**”文件夹的子文件夹。

2. 在工作区中，双击要禁用两步验证的用户账户。
   对于所有启用了两步验证的用户账户，“**需要 2FA**”列设置为“**是**”。

3. 在打开的“**属性：<用户名>**”窗口中，选择“**两步验证**”区域。

4. 在“**两步验证**”区域中，选择以下选项：

   - 如果要禁用用户账户的两步验证，请单击“**禁用**”按钮。
   - 如果要从两步验证中排除此用户账户，请选择“**用户仅可以使用用户名和密码通过身份验证**”选项。

5. 单击“**应用**”按钮。

6. 单击“**确定**”按钮。

用户账户的两步验证已禁用。

如果您想要为无法使用两步验证登录管理控制台的用户恢复访问权限，请禁用此用户账户的两步验证，然后在**两步验证**中选择上述“**用户仅可以使用用户名和密码通过身份验证**”。之后，使用您禁用两步验证的用户账户登录管理控制台，然后再次启用验证。

对所有用户禁用必需的两步验证（Web Console）

如果您的账户已启用两步验证，并且在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，则可以对所有用户禁用必需的两步验证。如果您的账户未启用两步验证，则必须先为您的账户启用两步验证，然后才能禁用所有用户的两步验证。

要禁用所有用户的两步验证：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标（ ）。
   管理服务器属性窗口将打开。

2. 在属性窗口的“**身份验证安全**”选项卡上，将“**所有用户的两步验证**”选项的切换按钮切换到禁用位置。

所有用户均已禁用两步验证。对所有用户禁用两步验证并不适用于之前单独启用两步验证的特定账户。

对所有用户禁用必需的两步验证（基于 MMC）

如果您在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，并且您已通过两步验证进行了身份验证，则可以对管理服务器的所有用户禁用必需的两步验证。

要禁用所有用户的两步验证：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单，然后选择“**属性**”。

2. 在管理服务器属性窗口的“**区域**”窗格中，选择“**高级**”，然后选择“**两步验证**”。

3. 单击“**设置为可选**”按钮禁用所有用户的两步验证。

4. 单击“**两步验证**”区域中的“**应用**”按钮。

5. 单击“**两步验证**”区域中的“**确定**”按钮。

所有用户均已禁用两步验证。对所有用户禁用两步验证并不适用于之前单独启用两步验证的特定账户。

从两步验证中排除账户（云控制台）

如果您在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，则可以从两步验证中排除用户账户。

如果某个用户账户从所有用户的两步验证列表中排除，则该用户不必使用两步验证。

对于在身份验证期间无法传递安全代码的服务账户，从两步验证中排除这些账户可能是有必要的。

如果要从两步验证中排除某些用户账户：

1. 如果要排除 Active Directory 账户，则必须执行 Microsoft Active Directory 域控制器轮询，以刷新管理服务器用户列表。
2. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
3. 在属性窗口的“**身份验证安全**”选项卡上的两步验证排除表中，单击“**添加**”按钮。
4. 在打开的窗口中：
   a. 选择要排除的用户账户。
   b. 单击“**确定**”按钮。

所选用户账户即从两步验证中排除。

从两步验证中排除账户（基于 MMC）

如果您的账户在“**常规功能：用户权限**”功能区域中拥有“修改对象 ACL”权限，则可以从两步验证中排除账户。

如果将某个用户账户从两步验证中排除，则该用户无需使用两步验证即可登录到管理控制台或 Kaspersky Security Center Web Console。

对于在身份验证期间无法传递安全代码的服务账户，从两步验证中排除这些账户可能是有必要的。

要从两步验证中排除用户账户：

1. 如果要排除 Active Directory 账户，请执行“Active Directory 轮询”以刷新管理服务器用户列表。
2. 在控制台树中，打开“**用户账户**”文件夹。
   默认情况下，“**用户账户**”文件夹是“**高级**”文件夹的子文件夹。
3. 在工作区中，双击要从两步验证中排除的用户账户
4. 在打开的“**属性：<用户名>**”窗口中，选择“**两步验证**”区域。
5. 在打开的区域中，选择“**用户仅可以使用用户名和密码通过身份验证**”选项。
6. 在“**两步验证**”区域中，单击“**应用**”按钮，然后单击“**确定**”按钮。

此用户账户已从两步验证中排除。您可以在用户账户列表中检查排除的账户。

编辑安全代码颁发者的名称（Web Console）

您可以有多个不同标识符（称为颁发者）来对应不同的管理服务器。您可以更改安全代码颁发者的名称，例如，当管理服务器使用的安全代码颁发者名称与其他管理服务器相似时。默认情况下，安全代码颁发者的名称与管理服务器的名称相同。

更改安全代码颁发者名称后，必须重新颁发新的 secret key 并将其传递给认证应用。

要指定安全代码颁发者的新名称：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在打开的用户设置窗口中，选择“**账户保护**”选项卡。
3. 在“**账户保护**”选项卡上，单击“**编辑**”链接。
   将打开“**编辑安全代码颁发者**”区域。
4. 指定新的安全代码颁发者名称。
5. 单击“**确定**”按钮。

已为管理服务器指定了新的安全代码颁发者名称。

编辑安全代码颁发者的名称（基于 MMC）

您可以有多个不同标识符（称为颁发者）来对应不同的管理服务器。您可以更改安全代码颁发者的名称，例如，当管理服务器使用的安全代码颁发者名称与其他管理服务器相似时。默认情况下，安全代码颁发者的名称与管理服务器的名称相同。

更改安全代码颁发者名称后，必须重新颁发新的 secret key 并将其传递给认证应用。

要指定安全代码颁发者的新名称：

1. 在 Kaspersky Security Center 控制台树中，打开“**管理服务器**”文件夹的上下文菜单，然后选择“**属性**”。
2. 在管理服务器属性窗口的“**区域**”窗格中，选择“**高级**”，然后选择“**两步验证**”。
3. 在“**安全码发布者**”字段中指定新的安全代码颁发者名称。
4. 单击“**两步验证**”区域中的“**应用**”按钮。
5. 单击“**两步验证**”区域中的“**确定**”按钮。

已为管理服务器指定了新的安全代码颁发者名称。

为您自己的账户配置两步验证 (Web Console)

启用两步验证后首次登录 Kaspersky Security Center 时，为您自己的账户配置两步验证的窗口将打开。

在为账户配置两步验证之前，请确保移动设备上安装了认证应用。

通过使用外部时间源，确保具有身份验证器应用的设备上的时间和具有管理服务器的设备上的时间与 UTC 同步。

要为账户配置两步验证：

1. 使用移动设备上的认证应用来生成一次性安全码。为此，请执行以下操作之一：
   - 在身份验证器应用中手动输入密钥。
   - 单击**查看二维码**并使用身份验证器应用扫描二维码。

   安全码将显示在移动设备上。
2. 在两步验证配置窗口中，指定由认证应用生成的安全代码，然后单击“**检查和应用**”按钮。

您的账户已配置两步验证。您可以根据您的权限访问管理服务器。

为您自己的账户配置两步验证（基于 MMC）

启用两步验证后首次登录 Kaspersky Security Center 时，为您自己的账户配置两步验证的窗口将打开。

在为账户配置两步验证之前，请确保移动设备上安装了认证应用。通过使用外部时间源，确保具有身份验证器应用的设备上的时间和具有管理服务器的设备上的时间与 UTC 同步。

要为账户配置两步验证：

1. 使用移动设备上的认证应用来生成一次性安全码。为此，请执行以下操作之一：
   - 在身份验证器应用中手动输入密钥。
   - 使用认证应用扫描二维码。

   安全码将显示在移动设备上。
2. 在“**运行两步验证**”窗口中，指定由认证应用生成的安全码，然后单击“**确定**”按钮。

您的账户已配置两步验证。您可以根据您的权限访问管理服务器。

生成新的 secret key

仅当您通过两步验证获得授权后，才能为您的账户的两步验证生成新的 secret key。

要为用户账户生成新的 secret key：

1. 在主菜单中，转到“**用户和角色**” → “**用户**”。
2. 单击要为其两步验证生成新 secret key 的用户账户的名称。
3. 在打开的用户设置窗口中，选择“**账户保护**”选项卡。
4. 在“**账户保护**”选项卡中，单击“**生成新的私密密钥**”链接。
5. 在打开的两步验证窗口中，指定由认证应用生成的新安全密钥。
6. 单击**检查和应用**按钮。

将为用户生成一个新的 secret key。

如果丢失了移动设备，您可以在另一台移动设备上安装认证应用并生成新的 secret key 以恢复对 Kaspersky Security Center Web Console 的访问权限。

禁止新用户为自己设置两步验证

为了进一步提高 Kaspersky Security Center Web Console 访问安全性，您可以禁止新用户为自己设置两步验证。

如果启用此选项，则被禁用两步验证的用户（例如新域管理员）无法为自己配置两步验证。因此，未经已启用两步验证的另一位 Kaspersky Security Center 管理员的批准，此类用户无法在管理服务器上进行身份验证，也无法登录 Kaspersky Security Center Web Console。

如果为所有用户启用了两步验证，则此选项可用。

要禁止新用户为自己设置两步验证：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在属性窗口的**身份验证安全**选项卡上，将切换按钮**禁止新用户为自己设置两步验证**切换到启用位置。

此选项不会影响添加到两步验证排除的用户账户。

要向被禁用两步验证的用户授予 Kaspersky Security Center Web Console 访问权限，请暂时关闭**禁止新用户为自己设置两步验证**选项，要求用户启用两步验证，然后重新打开该选项。

安装网络代理后将用户指定为 Linux 设备所有者

允许用户注册为 Linux 设备所有者：

1. 在 Kaspersky Security Center Web Console 中，转到“**发现和部署**”→“**部署和分配**”→“**安装包**”。
   安装包列表将打开。
2. 点击网络代理的安装包。
   此时将打开安装包的属性窗口。

3. 在安装包属性窗口中，单击“**设置**”→“**高级**”。

4. 在“**用户注册为设备所有者(仅限 Linux)**”部分中，打开“**允许在安装网络代理后运行用户注册实用工具**”选项，然后单击“**保存**”。

将用户注册为设备所有者的实用程序可以通过客户端设备上的命令行来运行。

要在客户端设备上将用户注册为 Linux 设备所有者：

1. 在客户端设备的命令行中执行以下命令：
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. 如果出现提示，请输入登录名和密码。

   如果登录名和密码包含在网络代理的应答文件中，请在客户端设备的命令行中执行以下命令：
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

如果用户包含在内部安全组中，则登录信息必须包含用户名。

如果用户包含在活动目录安全组中，则登录信息必须包含用户名和域名。

如果为用户启用了两步验证，则必须从应用程序中输入基于时间的一次性密码 (TOTP)。

该用户将被注册为设备所有者。

删除用户或安全组

> 您仅可以删除内部用户或内部安全组。

要删除用户或安全组：

1. 在主菜单中，转至“**用户和角色**” → “**用户和组**”，然后选择“**用户**”或“**组**”选项卡。

2. 选择您要删除的用户或安全组旁边的复选框。

3. 单击**删除**。

4. 在打开的窗口中，单击“**正常**”。

   用户或安全组被删除。

更改用户账户的密码

如果当前密码即将过期或者您想将其更改为更安全的密码，则可能需要更改您自己账户或另一个用户账户的密码。

密码必须符合以下规则：

- 密码的字符长度必须是 8 到 256 位。
- 密码必须包含以下组中三组的字符：
  - 大写字母 (A-Z)
  - 小写字母 (a-z)
  - 数字 (0-9)
  - 特殊字符 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 密码不可以包含任何空格、Unicode 字符以及“.”和“@”按先后顺序的组合。

更改您自己账户的密码

要编辑您的账户密码：

1. 在主菜单中，转到您的账户设置，然后选择**更改密码**。
2. 输入当前密码，然后指定用于连接到 Kaspersky Security Center 的新密码。
   要查看输入的密码，请单击。
3. 如果您的账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定您自己的账户或者在常规功能：用户权限功能区域中具有修改对象 ACL权限的账户的凭据。
4. 如果您在上一步中使用的账户启用了两步验证，请输入移动设备上的认证应用生成的安全代码。

更改内部用户账户的密码

要编辑内部用户账户的密码：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击您要编辑的用户账户名称。
3. 在打开的用户设置窗口的**常规**选项卡上，单击**更改密码**按钮。
4. 为用户连接到 Kaspersky Security Center 设置新密码。
   要查看输入的密码，请单击。
5. 如有必要，启用**用户必须在首次登录时更改密码**选项，以在下次用户身份验证时强制更改密码。
6. 如果用户账户受到保护以防止未经授权的修改，您必须确认您有更改此账户的权限。在**账户保护**窗口中，指定在常规功能：用户权限功能区域中具有修改对象 ACL权限的账户的凭据。
7. 如果您在上一步中使用的账户启用了两步验证，请输入移动设备上的认证应用生成的安全代码。

使用服务器标志配置更改密码的选项

您可以使用 klscflag 实用程序通过以下命令来配置更改密码：

- 配置密码轮换期限（ LP_SplPwdChangePeriodDays标志）

  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <rotation_period>

  其中 <rotation_period>是用户密码过期后的时间段（以天为单位）。可能的值：0–730。如果参数值为 0，则禁用密码轮换。

- 配置需要更改密码的初次警告时间（LP_SplPwdChangeNotificationHours标志）

  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <warning_time>

  其中<warning_time>是用户密码过期之前的时间段（以小时为单位）。在此期间，会显示需要更改密码的通知。可能的值：0–17520。如果参数值为 0，则警告时间为密码轮换周期的 25%。

- 指定**用户必须在首次登录时更改密码**选项的默认值（ LP_SplPwdForceChange标志）

  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <value>

  其中< value >标志的可能值为：

  1—**用户必须在首次登录时更改密码**选项已启用。

  0—**用户必须在首次登录时更改密码**选项被禁用。

要查看当前标志值，请运行以下命令：

klscflag.exe -fget -pv .core/.independent -s KLLIM -n <flag> -t d

其中< 标志 >是LP_SplPwdChangePeriodDays、 LP_SplPwdChangeNotificationHours或LP_SplPwdForceChange标志。

创建用户角色

要创建用户角色：

1. 在主菜单中，转到“**用户和角色**” → “**角色**”。
2. 单击**添加**。
3. 在打开的“**新角色名称**”窗口中，输入新角色名称。
4. 单击“**正常**”应用更改。
5. 在打开的角色属性窗口中，更改角色设置：
   - 在“**常规**”选项卡上，编辑角色名称。
     您无法编辑预定义角色名称。

- 在“**设置**”选项卡上，编辑角色范围和策略以及与角色关联的配置文件。
- 在“**访问权限**”选项卡上，编辑卡巴斯基应用程序的访问权限。

6. 单击“**保存**”保存设置。

新角色出现在用户角色列表。

编辑用户角色

要编辑用户角色：

1. 在主菜单中，转到“**用户和角色**” → “**角色**”。
2. 单击您要编辑的角色名称。
3. 在打开的角色属性窗口中，更改角色设置：
   - 在“**常规**”选项卡上，编辑角色名称。
     您无法编辑预定义角色名称。
   - 在“**设置**”选项卡上，编辑角色范围和策略以及与角色关联的配置文件。
   - 在“**访问权限**”选项卡上，编辑卡巴斯基应用程序的访问权限。
4. 单击“**保存**”保存设置。

更新的角色出现在用户角色列表。

编辑用户角色范围

*用户角色范围*是用户和管理组的组合。与用户角色关联的设置仅应用到属于该角色用户的设备，以及仅在这些设备属于与该角色关联的组（包括子组）时。

要添加用户、安全组和管理组到用户角色范围，您可以使用以下方法之一：

方法 1：

1. 在主菜单中，转至**用户和角色→用户和组**，然后选择**用户**或**组**选项卡。
2. 选择您要添加到用户角色范围的用户或安全组旁边的复选框。
3. 单击“**分配角色**”按钮。
   角色分配向导启动。使用“**下一步**”按钮继续向导操作。
4. 在“**选择角色**”步骤中，选择要分配的用户角色。

5. 在“**定义范围**”步骤中，选择要添加到用户角色范围的管理组。

6. 单击“**分配角色**”按钮关闭窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

方法 2：

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。

2. 单击您要定义范围的角色名称。

3. 在打开的角色属性窗口中，选择“**设置**”选项卡。

4. 在“**角色范围**”区域中，单击“**添加**”。
角色分配向导启动。使用“**下一步**”按钮继续向导操作。

5. 在“**定义范围**”步骤中，选择要添加到用户角色范围的管理组。

6. 在“**选择用户**”步骤中，选择要添加到用户角色范围的用户和安全组。

7. 单击“**分配角色**”按钮关闭窗口。

8. 单击“**关闭**”按钮（×）以关闭角色属性窗口。

所选用户或安全组和所选管理组被添加到用户角色范围。

方法 3：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
管理服务器属性窗口将打开。

2. 在“**访问权限**”选项卡上，选中要添加到用户角色范围的用户或安全组名称旁边的复选框，然后单击“**角色**”按钮。
您不能同时选择多个用户或安全组。如果您选择了多个条目，“**角色**”按钮将被禁用。

3. 在“**角色**”窗口中，选择要分配的用户角色，然后应用并保存更改。
所选用户或安全组被添加到用户角色范围。

删除用户角色

要删除用户角色：

1. 在主菜单中，转到“**用户和角色**” → “**角色**”。

2. 选择您要删除的角色旁边的复选框。

3. 单击**删除**。

4. 在打开的窗口中，单击“**正常**”。

用户角色被删除。

关联策略配置文件到角色

您可以关联用户角色到策略配置文件。此种情况下，该策略配置文件的激活规则基于角色：策略配置文件对具有指定角色的用户可用。

例如，策略禁止在管理组的所有设备上运行 GPS 导航软件。GPS 导航软件仅在“用户”管理组中的单个设备上是必须的——该设备属于导游。此种情况下，您可以分配“导游”角色给其所有者，然后创建一个策略配置文件，允许 GPS 导航软件仅在分配了“导游”角色的用户的设备上运行。所有其他策略设置被保留。仅带有“导游”角色的用户将被允许运行 GPS 导航软件。然后，如果其他员工被分配了“导游”角色，该新员工也在组织的设备上运行导航软件。运行 GPS 导航软件在相同管理组的其他设备上仍将被禁止。

要关联角色到策略配置文件：

1. 在主菜单中，转到“**用户和角色**”→“**角色**”。
2. 选择您要关联策略配置文件的角色名称。

   角色属性窗口打开，在其中已选择“**常规**”选项卡。
3. 选择“**设置**”选项卡并向下滚动至“**策略和配置文件**”区域。
4. 单击**编辑**。
5. 要关联角色到：
   - **现有策略配置文件** — 单击所学策略名称旁边的臂章图标(>)，然后选择您要关联角色的配置文件旁边的复选框。
   - **新策略配置文件**：
     a. 选择您要创建配置文件的策略旁边的复选框。
     b. 单击**新策略配置文件**。
     c. 为新配置文件指定名称并对配置文件设置进行配置。
     d. 单击“**保存**”按钮。
     e. 选择新配置文件旁边的复选框。
6. 单击**分配到角色**。

配置文件被关联到角色并显示在角色属性中。配置文件自动应用到分配了该角色的用户的任意设备。

传输用户角色到从属管理服务器

默认情况下，主管理服务器和从属管理服务器的用户角色列表是独立的。您可以配置应用程序自动传输在主管理服务器上创建的用户角色到所有从属管理服务器。用户角色也可以从从属管理服务器传输到其自己的从属管理服务器。

要从主管理服务器传输用户角色到从属管理服务器：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 转到“**管理服务器层级**”区域。
3. 启用**转发角色列表到从属管理服务器**选项，然后单击**保存** 按钮。

   应用程序将主管理服务器的用户角色复制到从属管理服务器。

启用**转发角色列表到从属管理服务器**选项并传播用户角色后，不能在从属管理服务器上编辑或删除这些用户角色。当您创建新角色或在主管理服务器上编辑现有角色时，更改被自动复制到从属管理服务器。当您在主管理服务器上删除用户角色时，该角色在从属管理服务器上被保留，但无法被编辑或删除。

从主管理服务器传播到从属管理服务器的角色显示为绿色复选标记 (✓)。您无法在从属管理服务器上编辑这些角色。

如果您在主管理服务器上创建角色，且在从属管理服务器上有相同名称的角色，新角色被复制到从属管理服务器，其名称后被添加索引，例如，~~1、~~2（索引可以随机）。

如果禁用“**转发角色列表到从属管理服务器**”选项，所有用户角色在从属管理服务器上被保留，但是独立于主管理服务器上的角色。独立后，从属管理服务器上的用户角色可以被编辑或删除。

修改账户密码

您可以更改本地账户密码，例如当用户忘记本地账户密码或要执行计划的密码更改时。

即使用户尚未登录账户，密码更改也将生效。您还可以更改本地根账户的密码。

> 此任务只能在 Linux 设备上执行。

要更改特定设备上的本地账户密码：

1. 在主菜单中，转到**资产(设备)** → **任务**。
2. 单击**添加**。
   “新任务向导”启动。
3. 在“**任务类型**”字段中，选择“**更改账户密码(仅限 Linux)**”。
4. 您可以选择以下选项之一：

   - **分配任务到管理组**

     > 任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
     > 例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。
     > 如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

- **手动指定设备地址或从列表导入地址**

  > 您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
  > 您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

- **分配任务到设备分类**

  > 该任务被分配到设备分类中的设备。您可以指定现有分类之一。
  > 例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

为指定设备创建“*更改账户密码（仅限 Linux）*”任务。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。

5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。
   可用设置取决于在上一步中选择的选项。

6. 在“**输入账户名和新密码**”步骤中，指定以下设置：

   - 在“**账户名**”字段中，指定要更改密码的账户名称。
   - 在“**新密码**”字段中，指定将要为前一个字段中所指定的账户设置的密码。
     要查看您输入的字符，请单击并按住“**显示**”按钮。
   - 如有必要，请选中“**设置为一次性密码(用户必须在首次登录后更改密码)**”复选框。

     - **设置为一次性密码(用户必须在首次登录后更改密码)**

       > 如果选中此复选框，则在用户首次登录后，系统将提示用户设置新密码。
       > 如果清除此复选框，则在用户首次登录后，系统将不会提示用户设置新密码。
       > 默认情况下已清除该选框。

7. 在**完成任务创建**步骤中，单击**完成**按钮以创建任务并关闭向导。
   如果启用了“**创建完成时打开任务详情**”选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。

8. 在任务列表中，选择已创建的任务，然后单击**启动**。
   或者等待任务按照您在任务设置中指定的时间表启动。

更改账户密码任务完成后，会更改指定设备上的指定本地账户的密码。

> 为了确保正确运行更改账户密码任务，必须在用户设备上禁用 SELinux。

撤销本地管理员权限

您可以从账户中撤销本地管理员权限。这为您提供了对用户账户的额外控制。例如，您可以在一次性分配完成后撤销本地管理员权限。

运行此任务时，会检查指定的本地账户是否属于本地管理员组。这些组在网络代理策略设置中定义。您可以在网络代理策略设置中自定义本地管理员组列表。您还可以使用“**特权设备用户报告(仅限 Linux)**”检查特权用户账户列表。

> 此任务只能在 Linux 设备上执行。

要撤销特定设备上的本地管理员权限：

1. 在主菜单中，转到**资产(设备) → 任务**。
2. 单击**添加**。
   “新任务向导”启动。
3. 在“**任务类型**”字段中，选择“**撤销本地管理员权限(仅限 Linux)**”。
4. 您可以选择以下选项之一：
   - **分配任务到管理组**

     > 任务被分配到包含在管理组中的设备。您可以指定现有组之一或者创建新组。
     > 例如，您可能要使用该选项运行发送消息到用户任务，如果消息针对包含在特定管理组中的设备。
     > 如果任务已分配给管理组，任务属性窗口中将不显示“**安全**”选项卡，因为组任务受其适用的组安全设置限制。

   - **手动指定设备地址或从列表导入地址**

     > 您可以指定您要为其分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。
     > 您可能要使用该选项以对特定子网执行任务。例如，您可能要安装特定应用程序到会计设备，或者扫描疑似被感染子网中的设备。

   - **分配任务到设备分类**

     > 该任务被分配到设备分类中的设备。您可以指定现有分类之一。
     > 例如，您可能要使用该选项在特定操作系统版本的设备上运行任务。

   为指定设备创建“*撤销本地管理员权限（仅限 Linux）*”任务。如果您选择了“**分配任务到管理组**”选项，则任务是组任务。
5. 在**任务范围**步骤，指定管理组、具有特定地址的设备或设备分类。
   可用设置取决于在上一步中选择的选项。
6. 在向导的该步骤，指定以下设置：
   - 在“**操作模式**”设置组中，选择操作模式：
     - **从列出的账户中撤销本地管理员权限**

       > 如果选择此选项，将会从指定的本地账户撤销本地管理员权限。

默认情况下已选定该选项。

- **从本地管理员权限撤销中排除列出的账户**

  如果选择此选项，将会从指定账户外的所有本地账户撤销本地管理员权限。
  默认情况下未选定该选项。

- 指定本地账户：
  - 单击**添加**。
  - 在打开的窗口中，执行以下操作：
    - 在“**账户名**”字段中，指定本地账户的名称。
    - 在“**账户操作**”设置组（仅当选择“**从列出的账户中撤销本地管理员权限**”选项时可用）中，选择操作。
    - **保留账户**

      如果选择此选项，则撤销本地管理员权限后不会删除本地账户。
      默认情况下已选定该选项。

    - **删除账户**

      如果选择此选项，无论本地账户是否具有本地管理员权限，都将被删除。
      默认情况下未选定该选项。

7. 在**完成任务创建**步骤中，单击**完成**按钮以创建任务并关闭向导。
   如果启用了“**创建完成时打开任务详情**”选项，将打开任务设置窗口。在此窗口中，您可以检查任务参数、修改它们或配置任务启动计划（如有必要）。
8. 在任务列表中，选择已创建的任务，然后单击**启动**。
   或者等待任务按照您在任务设置中指定的时间表启动。

当撤销本地管理员权限任务完成后，会从指定设备上的指定本地账户撤销本地管理员权限。

管理对象修订

该区域包含了对象修订管理的信息。Kaspersky Security Center 允许您跟踪对象修改。您每次保存更改到对象时，*修订*被创建。每个修订都有一个数字。

支持修订管理的应用程序对象包括：

- 管理服务器属性
- 策略
- 任务

- 管理组
- 用户账户
- 安装包

您可以对对象修订采取以下操作：

- 查看选定的修订（仅适用于策略）
- 回滚对对象所做的更改到所选的修订
- 将修订保存为 JSON 文件（仅适用于策略）

在任何支持修订管理的对象的属性窗口，“**修订历史**”区域显示了包含以下详情的对象修订列表：

- **修订** — 对象修订版本号。
- **时间** — 对象修改的日期和时间。
- **用户** — 修改对象的用户的名称。
- **用户设备 IP 地址** — 从其修改对象的设备的 IP 地址。
- **Web Console IP 地址** — 修改对象的 Kaspersky Security Center Web Console 的 IP 地址。
- **操作** — 对于对象执行的操作。
- **描述** — 与对象设置更改相关的修订描述。

  默认下，对象修订描述为空。要添加描述到修订，请选择相关修订并单击“**编辑描述**”按钮。在打开的窗口中，输入一些修订描述的文本。

回滚对象到先前修订

如果必要，您可以回滚对对象所做的更改。例如，您可能必须转换策略设置到特定日期的状态。

要回滚对对象所做的更改：

1. 在对象属性窗口中，打开“**修订历史**”选项卡。
2. 在对象修订列表中，选择要回滚更改的修订。
3. 单击**回滚**按钮。
4. 单击“**确定**”以确认操作。

   该对象被回滚到所选修订。对象修订列表显示所做的操作记录。修订描述显示了您转换对象所到的修订号的信息。

回滚操作仅适用于策略和任务对象。

添加修订描述

Kaspersky Security Center 允许您跟踪对象修改。您每次保存更改到对象时，修订被创建。每个修订都有一个数字。

您可以为修订添加描述以简化在列表中的修订搜索。

要添加修订描述：

1. 在对象的属性窗口中，打开“**修订历史**”选项卡。
2. 在对象修订列表中，选择您想要添加描述的修订。
3. 单击“**编辑描述**”按钮。
   “**描述**”窗口打开。
4. 在“**描述**”窗口，输入修订描述的文本。
   默认下，对象修订描述为空。
5. 保存修订描述。

为对象的修订添加描述。

查看并保存策略修订

通过 Kaspersky Security Center，您可以查看在特定时期内对策略所做的修改，并且将有关这些修改的信息保存在文件中。

如果相应的管理 Web 插件支持此功能，则可以查看和保存策略修订。

要查看策略修订：

1. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”。
2. 单击要查看修订的策略，然后转到“**修订历史**”部分。
3. 在策略修订列表中，单击要查看的修订编号。
   如果修订大小超过 10 MB，您将无法使用 Kaspersky Security Center Web Console 进行查看。系统将提示您将所选的修订保存到 JSON 文件。
   如果修订大小不超过 10 MB，则会显示 HTML 格式的报告，其中包含所选策略修订的设置。由于报告显示在弹出窗口中，请确保您的浏览器允许弹出窗口。

要将策略修订保存到 JSON 文件，

在策略修订列表中，选择要保存的修订，然后单击“**保存到文件**”。

修订会保存到 JSON 文件中。

对象删除

本部分提供有关删除对象的信息。

您可以删除对象，包括以下：

- 策略
- 任务
- 安装包
- 虚拟管理服务器
- 用户
- 安全组
- 管理组

要删除对象：

1. 打开 Kaspersky Security Center Web Console 的所需部分，然后选择对象。
2. 在工具栏上，单击“**删除**”按钮。
3. 在打开的窗口中，单击“**确定**”以确认您的选择。

所选对象被删除。

当您删除对象时，其信息保留在数据库。已删除对象的信息的存储期限与对象修订的存储期限一致（推荐期限是 90 天）。您仅在权限的**已删除对象**区域具有**修改**权限时才能更改存储期限。

关于删除客户端设备

当您从管理组中删除受管理设备时，应用程序会将设备移至未分配的设备组。删除设备后，已安装的卡巴斯基应用程序——网络代理和安全应用程序（例如 Kaspersky Endpoint Security）——将保留在设备上。

Kaspersky Security Center 根据以下规则处理未分配设备组中的设备：

- 如果您配置了设备移动规则，并且设备符合移动规则的条件，则该设备会根据规则被自动移动到管理组。
- 设备会被存储在未分配的设备组中，并根据设备保留规则自动从组中删除。

  设备保留规则不会影响具有一个或多个使用完整磁盘加密进行加密的驱动器的设备。此类设备不会被自动删除——您只能手动删除它们。如果您需要删除带有加密驱动器的设备，请先解密驱动器，然后再删除该设备。

  当您删除带有加密驱动器的设备时，解密驱动器所需的数据也会被删除。如果在删除此类设备（从“**未分配的设备**”或“**受管理设备**”组）时打开的确认窗口中选中“**我了解风险并想要删除选定的设备**”复选框，则表示您知晓数据随后会被删除。

要解密驱动器，必须满足以下条件：

- 设备被重新连接到管理服务器以恢复解密驱动器所需的数据。
- 设备用户记住解密密码。
- 用于加密驱动器的安全应用程序（例如 Kaspersky Endpoint Security for Windows）仍安装在设备上。

如果驱动器由卡巴斯基磁盘加密技术加密，您还可以尝试使用 FDERT Restore Utility 恢复数据。

在 VDI 中，如果您的设备包含加密驱动器，则删除该设备后，加密驱动器上的信息也会被删除。

当您从未分配的设备组中手动删除设备时，应用程序会从列表中删除该设备。删除设备后，已安装的卡巴斯基应用程序（如果有）将保留在设备上。然后，如果该设备对管理服务器仍然可见并且您配置了常规网络轮询，Kaspersky Security Center 会在网络轮询期间发现该设备并将其添加回未分配的设备组。因此，最好仅当设备对管理服务器不可见时再手动删除设备。

卡巴斯基安全网络 （KSN）

该部分描述如何使用卡巴斯基安全网络 (KSN) 的在线服务基础架构。该部分提供了关于 KSN 的详细描述，介绍了如何启用 KSN，配置对 KSN 的访问，并查看 KSN 代理服务器的使用统计。

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）以及 KSN 功能。

关于 KSN

卡巴斯基安全网络 (KSN) 是一种在线服务的基础架构，可提供对 Kaspersky 在线知识库的访问，其中包含与文件信誉、网络资源和软件相关的信息。使用卡巴斯基安全网络中的数据可确保在遇到新型威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的效力并降低误报的风险。KSN 允许您使用 Kaspersky 的信誉数据库检索有关安装在受管理设备上的应用程序信息。

Kaspersky Security Center 支持以下基础架构解决方案：

- *KSN* 是一种允许您与 Kaspersky Security Network 交换信息的解决方案。一旦加入 KSN，即表示您同意以自动模式将通过 Kaspersky Security Center 管理的客户端设备上安装的卡巴斯基应用程序的操作相关信息发送到 Kaspersky。依照当前KSN 访问设置发送信息。卡巴斯基分析师还分析收到的信息，并将其包含在卡巴斯基安全网络的信誉数据库和统计数据库中。Kaspersky Security Center 默认使用此解决方案。
- *卡巴斯基私有安全网络 (KPSN)* 是一种解决方案，允许安装了卡巴斯基应用程序的设备用户访问卡巴斯基安全网络的信誉数据库和其他统计数据，而无需从用户自己的设备向全球 KSN 发送数据。KPSN 用于由于以下原因无法参与卡巴斯基安全网络的企业客户：
  - 用户设备未连接到互联网。
  - 法律或企业安全策略禁止传输任何数据到国家/地区以外或企业局域网以外。

  您可以在管理服务器属性窗口的 **KSN 代理设置**区域对卡巴斯基私人安全网络设置访问设置。

在运行快速启动向导时，应用程序会提示您加入 KSN。您可以在使用应用程序的任何时间启用或者停止 KSN。

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您升级管理服务器的版本时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的先前版本继续使用 KSN。

启用 KSN 后，Kaspersky Security Center 会检查 KSN 服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保保持受管理设备的安全级别是必要的。

管理服务器管理的客户端设备通过 KSN 代理服务器与 KSN 交互。KSN 代理服务器提供以下功能：

- 即使无法直接访问互联网，客户端设备也可以向 KSN 发送请求、从 KSN 获取信息以及向 KSN 传送信息。
- KSN 代理可缓存处理后的数据，从而减少发送通道的工作负荷以及为等待客户端设备所请求的信息而花费的时间。

您可以在管理服务器的属性窗口的“**KSN 代理设置**”部分配置 KSN 代理服务器。

设置对 KSN 的访问

您可以在管理服务器和分发点上设置到卡巴斯基安全网络 (KSN) 的访问。

要设置管理服务器到 KSN 的访问：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理设置**”区域。

3. 将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置。

   如果启用此选项，KSN 代理服务器会将数据发送到 KSN，以提高 Kaspersky Security Center 组件的效率并改善卡巴斯基应用程序的性能。数据被从客户端设备发送到 KSN，与在这些客户端设备上活动的 Kaspersky Endpoint Security 策略一致。如果此切换按钮被禁用，则数据不会通过 Kaspersky Security Center 从管理服务器以及客户端设备发送到 KSN。但是，客户端设备能够根据其设置直接将数据发送到 KSN（绕过 Kaspersky Security Center）。在客户端设备上活动的 Kaspersky Endpoint Security 策略决定了哪些数据将被直接从那些设备发送到 KSN（绕过 Kaspersky Security Center）。

4. 将切换按钮切换到**使用卡巴斯基安全网络已启用**位置。

   如果启用此选项，客户端设备将发送补丁安装结果到 Kaspersky。启用此选项时，请确保阅读并接受 KSN 声明的条款。

   如果要使用 KPSN，请将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置，然后单击“**选择 KSN 代理设置文件**”按钮以下载 KPSN 设置（带有 pkcs7 和 pem 扩展名的文件）。下载完设置之后，界面会显示提供商的名称和联系人，以及 KPSN 设置文件的创建日期。

   > 启用 KPSN 时，请注意将分发点配置为直接将 KSN 请求发送到云 KSN。安装了网络代理版本 11（或更早版本）的分发点将继续向云 KSN 发送 KSN 请求。如果要重新配置分发点以将 KSN 请求发送到 KPSN，请为每个分发点启用“**转发 KSN 请求到管理服务器**”选项。您可以在分发点属性或网络代理策略中启用此选项。

   将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置时，将显示一条消息，其中包含有关 KPSN 的详细信息。

以下卡巴斯基应用程序支持 KPSN：

- Kaspersky Security Center
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

如果您在 Kaspersky Security Center 中启用 KPSN，这些应用程序将接收支持 KPSN 的相关信息。在应用程序设置窗口，在**高级威胁保护**区域的**卡巴斯基安全网络**子区域中，将显示有关选定 KSN 提供者的信息：KSN 或 KPSN。

如果您使用的应用程序版本早于 Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 或早于 Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent，在您运行 KPSN 时，我们建议您使用未启用 KPSN 使用的从属管理服务器。

如果在管理服务器属性窗口的“**KSN 代理设置**”区域中配置了 KPSN，则 Kaspersky Security Center 不发送任何统计数据到卡巴斯基安全网络。

5. 如果您在管理服务器属性中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，请启用“**当连接到 KPSN 时忽略代理服务器设置**”选项。否则，从受管理应用程序的请求无法到达 KPSN。
6. 配置管理服务器到 KSN 代理服务的连接：
   - 在“**连接设置**”下，对于“**TCP 端口**”，指定用于连接到 KSN 代理服务器的 TCP 端口号。连接到 KSN 代理的默认端口是 13111。
   - 如果您要让管理服务器通过 UDP 端口连接到 KSN 代理服务器，请启用“**使用 UDP 端口**”选项，并为“**UDP 端口**”指定端口号。默认情况下，此选项为禁用状态，并且使用 TCP 端口。如果启用此选项，默认将使用 UDP 端口 15111 连接到 KSN 代理服务器。
   - 如果您要让管理服务器通过 HTTPS 端口连接到 KSN 代理服务器，请启用“**使用 HTTPS**”选项，并为“**HTTPS 端口**”指定端口号。默认情况下，此选项为禁用状态，并且使用 TCP 端口。如果启用此选项，默认将使用 HTTPS 端口 17111 连接到 KSN 代理服务器。
7. 将切换按钮切换到**通过主管理服务器连接从属管理服务器到 KSN 已启用**位置。

   如果启用此选项，从属管理服务器使用主管理服务器作为 KSN 代理服务器。如果禁用此选项，从属管理服务器自己连接到 KSN。该情况下，受管理设备使用从属管理服务器作为 KSN 代理服务器。

   如果在从属管理服务器属性的“**KSN 代理设置**”区域的右侧面板中将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置，则从属管理服务器将使用主管理服务器作为代理服务器。

8. 单击“**保存**”按钮。

KSN 访问设置将被保存。

您也可以设置分发点访问 KSN，例如，如果您想降低管理服务器负载。作为 KSN 代理服务器的分发点从受管理设备直接发送 KSN 请求到 Kaspersky，不使用管理服务器。

要设置分发点到卡巴斯基安全网络（KSN）的访问：

1. 确保分发点是手动分配。
2. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
3. 在“**常规**”选项卡上，选择“**分发点**”区域。
4. 单击分发点的名称以打开其属性窗口。
5. 在分发点属性窗口的“**KSN 代理**”区域中，启用“**在分发点端启用 KSN 代理**”选项，然后启用“**通过互联网直接访问 KSN 云/KPSN**”选项。
6. 单击“**确定**”。

该分发点将作为 KSN 代理服务器。

启用和禁用 KSN 的使用

要启用 KSN，请执行以下操作：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**KSN 代理设置**”区域。
3. 将切换按钮切换到“**在管理服务器上启用 KSN 代理 已启用**”位置。

KSN 代理服务器被启用并将数据发送到 KSN，以提高 Kaspersky Security Center 组件的效率并改善卡巴斯基应用程序的性能。

1. 根据您使用的KSN 基础设施解决方案，启用相应的切换按钮。
   - 如果使用的是全球 KSN，请将切换按钮切换到“**使用卡巴斯基安全网络已启用**”位置。
     现在可以将数据发送到 KSN。启用此选项时，您必须阅读并接受 KSN 声明的条款。
   - 如果使用的是 KPSN，请将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置，然后单击“**选择 KSN 代理设置文件**”按钮以下载 KPSN 设置（带有 pkcs7 和 pem 扩展名的文件）。下载完设置之后，界面会显示提供商的名称和联系人，以及 KPSN 设置文件的创建日期。
     将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置时，将显示一条消息，其中包含有关 KPSN 的详细信息。
2. 单击“**保存**”按钮。

要禁用 KSN，请执行以下操作：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理设置**”区域。

3. 将切换按钮切换到**在管理服务器上启用 KSN 代理 已禁用**位置，以禁用 KSN 代理服务。

4. 单击“**保存**”按钮。

查看已接受的 KSN 声明

启用卡巴斯基安全网络 (KSN) 时，必须阅读并接受 KSN 声明。您可以随时查看已接受的 KSN 声明。

要查看已接受的 KSN 声明：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**KSN 代理设置**”区域。

3. 单击**查看卡巴斯基安全网络声明**链接。

   在打开的窗口中，可以查看已接受的 KSN 声明的文本。

接受更新的 KSN 声明

您将根据您在启用 KSN 时阅读并接受的 KSN 声明来使用 KSN。如果 KSN 声明有更新，当您升级管理服务器的版本时会向您显示。您可以接受更新的 KSN 声明，也可以拒绝。如果您拒绝，您将根据之前接受的 KSN 声明的版本继续使用 KSN。

升级管理服务器版本后，将自动显示更新的 KSN 声明。如果您拒绝更新的 KSN 声明，您仍然可以在以后查看并接受它。

要查看然后接受或拒绝更新的 KSN 声明：

1. 单击应用程序主窗口右上角的“**查看通知**”链接。
   “**通知**”窗口打开。

2. 单击“**查看更新的 KSN 声明**”链接。
   卡巴斯基安全网络声明更新窗口打开。

3. 阅读 KSN 声明，然后单击以下按钮之一做出决定：

   - **我接受更新的 KSN 声明**
   - **在旧声明下使用 KSN**

   根据您的选择，KSN 会按照当前或更新的 KSN 声明的条款继续工作。您可以随时在管理服务器的属性中查看接受的 KSN 声明的文本。

检查分发点是否充当 KSN 代理服务器

在分配作为分发点的受管理设备上，可以启用 KSN 代理服务器。当 ksnproxy 服务在设备上运行时，受管理设备充当 KSN 代理服务器。您可以在设备上本地检查、打开或关闭此服务。

您可以将基于 Windows 或基于 Linux 的设备分配为分发点。检查分发点的方法取决于该分发点的操作系统。

要检查基于 Windows 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上的 Windows 中，打开“**服务**”（“**所有程序**”→“**管理工具**”→“**服务**”）。
2. 在服务列表，检查 ksnproxy 服务是否正在运行。

   如果 ksnproxy 服务正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

   如果您想，您可以关闭 ksnproxy 服务。在这种情况下，分发点上的网络代理停止参与卡巴斯基安全网络。该需要本地管理员权限。

要检查基于 Linux 的分发点是否充当 KSN 代理服务器：

1. 在分发点设备上，显示正在运行的进程列表。
2. 在正在运行的进程列表中，检查 `/opt/kaspersky/ksc64/sbin/ksnproxy` 进程是否 正在运行。

如果 `/opt/kaspersky/ksc64/sbin/ksnproxy` 进程正在运行，则设备上的网络代理会参与卡巴斯基安全网络，并充当分发点范围内包括的受管理设备的 KSN 代理服务器。

情景：升级 Kaspersky Security Center 和受管理安全应用程序

该部分描述 Kaspersky Security Center 和受管理安全应用程序升级的主要方案。

Kaspersky Security Center 和受管理安全应用程序升级分步骤进行：

1. **检查硬件和软件要求**

   确保您的硬件满足要求并安装所需更新。

2. **计划资源**

   评估您数据库占据的磁盘空间。确保您有足够磁盘空间存储管理服务器设置和数据库的备份副本。

3. **获取 Kaspersky Security Center 的安装文件**

   获取当前版本 Kaspersky Security Center 的可执行文件并保存它到作为管理服务器的设备。阅读您要使用的 Kaspersky Security Center 版本的发布说明。

4. **创建先前版本的备份副本**

   使用数据备份和恢复实用工具创建管理服务器数据的备份副本。您还可以创建备份任务。

   建议导出已安装的插件列表。

5. **运行安装程序**

   运行 Kaspersky Security Center 最新版本的可执行文件。当运行文件时，指定您有备份副本并指定其位置。您的数据将从备份被恢复。

6. **升级受管理应用程序**

   如果有新版本可用，您可以升级应用程序。阅读支持的 Kaspersky 应用程序列表并确保您的 Kaspersky Security Center 版本与该应用程序兼容。然后按照发布说明的描述执行应用程序升级。

结果

升级方案完成后，确保管理服务器新版本已成功安装到 Microsoft Management Console。点击**帮助** → **关于 Kaspersky Security Center**。版本被显示。

要确保您正在 Kaspersky Security Center Web Console 中使用管理服务器的新版本，在屏幕上方点击管理服务器名称旁边的设置图标( )。在打开的管理服务器属性窗口中的"**常规**"选项卡上，选择"**常规**"区域。版本被显示。

如果您需要恢复管理服务器数据，请按照以下主题中描述的步骤操作：交互模式下的数据备份和恢复。

如果您升级受管理安全应用程序，确保它被正确安装在受管理设备。对于更多信息，请参考该应用程序的文档。

更新 Kaspersky 数据库和应用程序

该部分描述了定期更新以下内容必须采取的步骤：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center 组件和安全应用程序

> 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）以及 KSN 功能。

方案：定期更新 Kaspersky 数据库和应用程序

本部分提供定期更新 Kaspersky 数据库、软件模块和应用程序的方案。在您完成配置网络保护方案后，您必须维持保护系统的可靠性以确保管理服务器和受管理设备保持受保护状态以防范各种威胁，包括病毒、网络攻击和钓鱼攻击。

网络保护通过更新以下内容保持最新：

- Kaspersky 数据库和软件模块
- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center 组件和安全应用程序

当您完成方案时，您可以确保：

- 您的网络被最新的 Kaspersky 软件保护，包括 Kaspersky Security Center 组件和安全应用程序。
- 对网络安全至关重要的反病毒数据库和其他 Kaspersky 数据库始终保持最新。

先决条件

受管理设备必须连接到管理服务器。如果未建立连接，请考虑手动更新卡巴斯基数据库、软件模块和应用程序或直接从卡巴斯基更新服务器更新。

管理服务器必须连接到互联网。

在您开始之前，确保您已做了如下：

1. 根据通过 Kaspersky Security Center Web Console 部署 Kaspersky 应用程序的方案将 Kaspersky 安全应用程序部署到受管理设备。
2. 创建了配置了所有所需策略、策略配置文件和任务，根据网络保护配置方案。
3. 分配了适当数量的分发点，与受管理设备和网路拓扑一致。

更新 Kaspersky 数据库和应用程序分阶段进行：

1. **选择更新 scheme**

   您可以使用若干个 scheme 以安装更新到 Kaspersky Security Center 组件和安全应用程序。选择一个或多个满足您网络需求的 scheme。

2. **创建管理服务器的“将更新下载至存储库”任务**

   该任务由 Kaspersky Security Center 快速启动向导自动创建。如果您未运行向导，立即创建任务。

   此任务需要从 Kaspersky 更新服务器下载更新到管理服务器的存储库，以及为 Kaspersky Security Center 更新 Kaspersky 数据库和软件模块。更新被下载后，它们可以被传播到受管理设备。

   如果您的网络被分配了分发点，更新被从管理服务器存储库自动下载到分发点存储库。此种情况下，分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。

   说明：

   - 管理控制台：创建管理服务器的“将更新下载至存储库”任务
   - Kaspersky Security Center Web Console：创建管理服务器的“将更新下载至存储库”任务

3. **创建“将更新下载至分发点存储库”任务（可选）**

   默认下，更新被从管理服务器下载到分发点。您可以配置 Kaspersky Security Center 直接从 Kaspersky 更新服务器下载更新到分发点。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

   当您的网络已分配分发点并已创建“*将更新下载至分发点存储库*”任务时，分发点从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库下载。

   说明：

   - 管理控制台：创建“将更新下载至分发点存储库”任务
   - Kaspersky Security Center Web Console：创建“将更新下载至分发点存储库”任务

4 配置分发点

当您的网络已分配分发点时，确保在所有所需分发点的属性中启用“**部署更新**”选项。当该选项对分发点禁用时，包含在分发点范围中的设备从管理服务器存储库下载更新。

如果您希望受管理设备仅从分发点接收更新，请在网络代理策略中启用“**仅通过分发点分发文件**”选项。

5 通过使用更新下载或差异文件的离线模型来优化更新过程（可选）

您可以通过使用离线模式更新下载（默认启用）或使用 diff 文件优化更新过程。对于每个网段，您必须选择应用哪个功能，因为它们无法同时工作。

当离线模式更新下载被启用时，一旦更新被下载到管理服务器存储库，在安全应用程序请求更新之前，网络代理就下载所需更新到受管理设备。这确保了更新过程的可靠性。要使用此功能，请启用“网络代理策略”中的“**提前从管理服务器下载更新和反病毒数据库(推荐)**”选项。

如果您不使用离线模式更新下载，您通过使用 diff 文件优化管理服务器和受管理设备之间的流量。启用此功能后，管理服务器或分发点将下载差异文件，而不是整个 Kaspersky 数据库或软件模块文件。diff 文件描述了数据库或软件模块的文件的两个版本之间的差异。因此，diff 文件比整个文件占用更少的空间。这导致降低管理服务器之间或分发点和受管理设备之间的流量。要使用此功能，请在“*将更新下载至管理服务器存储库*”任务和/或“*将更新下载至分发点存储库*”任务的属性中启用“**下载差异文件**”选项。

说明：

- 使用 diff 文件更新 Kaspersky 数据库和软件模块
- 管理控制台：启用和禁用离线模式更新下载
- Kaspersky Security Center Web Console：启用和禁用离线模式更新下载

6 验证已下载的更新（可选）

安装下载的更新之前，您可以通过“*更新验证*”任务验证更新。该任务按顺序运行通过测试设备集的设置来配置的设备更新任务和恶意软件扫描任务。获取任务结果时，管理服务器开始或阻止更新传播到剩余设备。

“*更新验证*”任务可以作为“*将更新下载至管理服务器存储库*”任务的一部分执行。在“*将更新下载至管理服务器存储库*”任务的属性中，在管理控制台中启用“**分发前验证更新**”选项或在 Kaspersky Security Center Web Console 中启用“**运行更新验证**”选项。

说明：

- 管理控制台：验证下载的更新
- Kaspersky Security Center Web Console：验证下载的更新

7 批准和拒绝软件更新

默认下，下载的软件更新具有*未定义*状态。您可以更改状态到*已批准*或*已拒绝*。批准的更新总是被安装。如果更新需要查看和接受最终用户授权许可协议的条款，您需要先接受它们。此后，更新可以被传播到受管理设备。未定义的更新仅可以被安装到网络代理和其他 Kaspersky Security Center 组件，与网络代理策略设置一致。您设置了*已拒绝*状态的更新将不被安装到设备。如果安全应用程序的拒绝的更新先前被安装，Kaspersky Security Center 将尝试从所有设备上卸载该更新。

批准和拒绝更新仅适用于安装在 Windows 和 Linux 客户端设备上的网络代理和受管理的卡巴斯基应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。

说明：

- 管理控制台：批准和拒绝软件更新
- Kaspersky Security Center Web Console：批准和拒绝软件更新

8 配置 Kaspersky Security Center 组件的更新和补丁的自动安装

系统将自动安装下载的网络代理更新和补丁以及其他 Kaspersky Security Center 组件。如果在网络代理属性中启用了“**对未定义状态的组件自动安装可应用更新和补丁**”选项，则所有更新在下载到存储库（或多个存储库）后将自动安装。如果禁用此选项，被下载和标注为*未定义*状态的 Kaspersky 补丁将仅在您改变其状态为*已批准*是被安装。

说明：

- 管理控制台：启用和禁用 Kaspersky Security Center 组件的自动更新和补丁
- Kaspersky Security Center Web Console：启用和禁用 Kaspersky Security Center 组件的自动更新和补丁

9. **为管理服务器安装更新**

   管理服务器软件更新不取决于更新状态。更新不会自动安装，且必须由管理员初步在管理控制台的**监控**选项卡（“**管理服务器** <服务器名称>”→“**监控**”）或 Kaspersky Security Center Web Console 的“**通知**”区域（“**监控和报告**”→“**通知**”）上批准。此后，管理员必须明确运行更新安装。

10. **为安全应用程序配置更新的自动安装**

    为受管理应用程序创建*更新*任务，以提供对应用程序、软件模块和 Kaspersky 数据库（包括反病毒数据库）的及时更新。为确保及时更新，我们建议您配置任务计划时选择“**当新更新下载至存储库时**”选项。

    如果您的网络包括仅支持 IPv6 的设备，并且您想要定期更新这些设备上安装的安全应用程序，请确保受管理设备上已安装管理服务器版本（版本不早于 13.2）和网络代理（版本不早于 13.2）。

    默认下，Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 的更新在您更改更新状态到*已批准*后被安装。您可以在*更新*任务中更改更新设置。

    如果更新需要查看和接受最终用户授权许可协议的条款，您需要先接受它们。此后，更新可以被传播到受管理设备。

    说明：

    - 管理控制台：在设备上自动安装 Kaspersky Endpoint Security 更新
    - Kaspersky Security Center Web Console：在设备上自动安装 Kaspersky Endpoint Security 更新

结果

方案完成后，Kaspersky Security Center 配置为在更新下载至管理服务器存储库或分发点存储库后更新 Kaspersky 数据库和已安装的 Kaspersky 应用程序。您然后可以继续监控网络状态。

关于更新 Kaspersky 数据库、软件模块和应用程序

为了确保管理服务器和受管理设备的保护是最新的，您必须提供以下内容的定期更新：

- Kaspersky 数据库和软件模块

  在下载卡巴斯基数据库和软件模块之前，Kaspersky Security Center 会检查卡巴斯基服务器是否可访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS 服务器。这对于确保更新反病毒数据库并保持受管理设备的安全级别是必要的。

- 已安装的 Kaspersky 应用程序，包括 Kaspersky Security Center 组件和安全应用程序

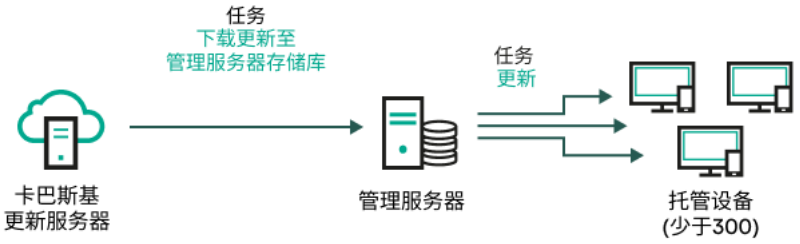
  通过 Kaspersky Security Center，您可以自动更新安装在 Windows 和 Linux 客户端设备上的网络代理和卡巴斯基应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。要更新这些组件，您必须从卡巴斯基网站下载最新版本，然后手动进行安装。

取决于您网络的配置，您可以使用以下方案来下载和分发所需更新到受管理设备：

- 通过使用单个任务：*将更新下载至管理服务器存储库*
- 通过使用两个任务：
  - "*将更新下载至管理服务器存储库*"任务
  - 创建"*将更新下载至分发点存储库*"任务
- 通过本地文件夹、共享文件夹或 FTP 服务器手动
- 直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security
- 如果管理服务器没有互联网连接，则通过本地或网络文件夹

使用"将更新下载至管理服务器存储库"任务

在此方案中，Kaspersky Security Center 通过"*将更新下载至管理服务器存储库*"任务来下载更新。在单一网段包含少于 300 台受管理设备或每个网段包含少于 10 台受管理设备的小网络中，更新直接从管理服务器存储库被分发到受管理设备（参见下图）。

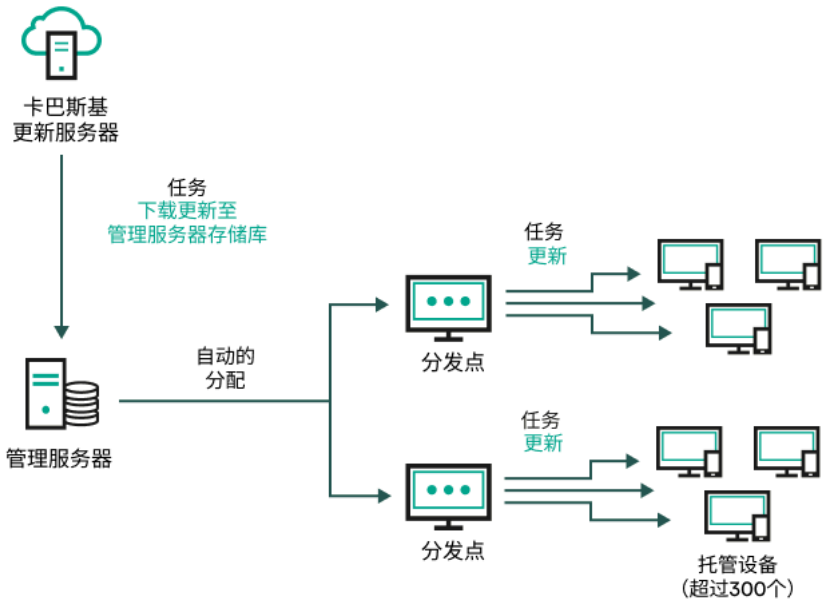


存储库通过使用"将更新下载至管理服务器存储库"任务更新，而不使用分发点

默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

如果您的网络中单一网段包含多于 300 台受管理设备或每个网段包含多于 9 台受管理设备，我们建议您使用分发点传播更新到受管理设备（参见下图）。分发点降低管理服务器负载并优化管理服务器和受管理设备之间的流量。您可以计算数字并配置您网络所需的分发点。

此种方案中，更新被从管理服务器存储库自动下载到分发点存储库。分发点所在范围的受管理设备从分发点存储库下载更新，而不是从管理服务器存储库。



通过使用"将更新下载至管理服务器存储库"任务更新，并使用分发点

完成"*将更新下载至管理服务器存储库*"任务后，以下更新将下载到管理服务器存储库：

- Kaspersky 数据库和 Kaspersky Security Center 软件模块

  这些更新被自动安装。

- Kaspersky 数据库和受管理设备上安全应用程序的软件模块

  这些更新通过Kaspersky Endpoint Security for Windows 更新任务安装。

- 管理服务器更新

  这些更新不被自动安装。管理员必须明确批准和运行更新安装。

  > 需要本地管理员权限以安装补丁到管理服务器。

- Kaspersky Security Center 模块更新

  默认下，这些更新被自动安装。您可以在网络代理策略中更改设置。

- 安全应用程序更新

  默认情况下，Kaspersky Endpoint Security for Windows 仅安装您批准的更新（您可以通过管理控制台或通过 Kaspersky Security Center Web Console批准更新）。更新通过*更新*任务安装且可以在任务属性中被配置。

> "*将更新下载至管理服务器存储库*"任务在虚拟管理服务器上不可用。虚拟管理服务器的存储库将显示已下载至主管理服务器的更新。

您可以配置在测试设备集上进行更新的操作和错误验证。如果验证成功，更新被分发到其他受管理设备。

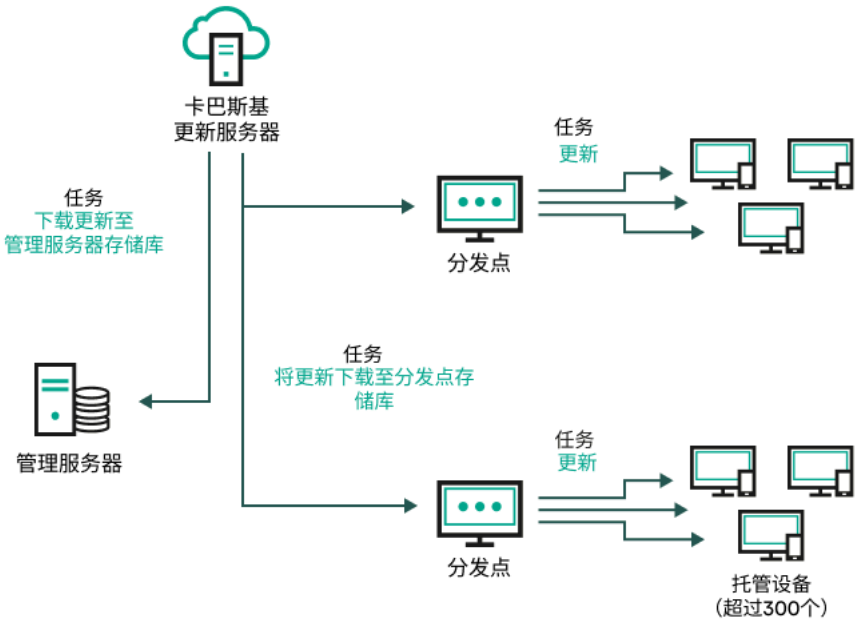
每个卡巴斯基应用程序都从管理服务器请求所需更新。管理服务器集合这些更新并仅下载应用程序请求的更新。这确保了相同更新不被下载多次，且不必要更新不被下载。当运行“*将更新下载至管理服务器存储库*”任务时，管理服务器自动发送以下信息到 Kaspersky 更新服务器以便确保相关版本的 Kaspersky 数据库和软件模块的下载：

- 应用程序 ID 和版本
- 应用程序安装 ID
- 活动密钥 ID
- “*将更新下载至管理服务器存储库*”任务运行 ID

传输的信息都不包含个人数据或其他机密数据。AO Kaspersky Lab 依照法律需求保护信息。

使用两个任务：“将更新下载至管理服务器存储库”任务和“将更新下载至分发点存储库”任务

您可以直接从 Kaspersky 更新服务器下载更新到分发点存储库，而不是从管理服务器存储库，然后分发更新到受管理设备（参见下图）。您可以下载到分发点存储库，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。



通过使用“将更新下载至管理服务器存储库”任务和“将更新下载至分发点存储库”任务更新

默认下，管理服务器和分发点与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器和/或分发点使用 HTTP 协议，而不是 HTTPS。

要实施此方案，除了“*将更新下载至管理服务器存储库*”任务外，请创建“*将更新下载至分发点存储库*”任务。此后，分发点将从 Kaspersky 更新服务器下载更新，而不是从管理服务器存储库。

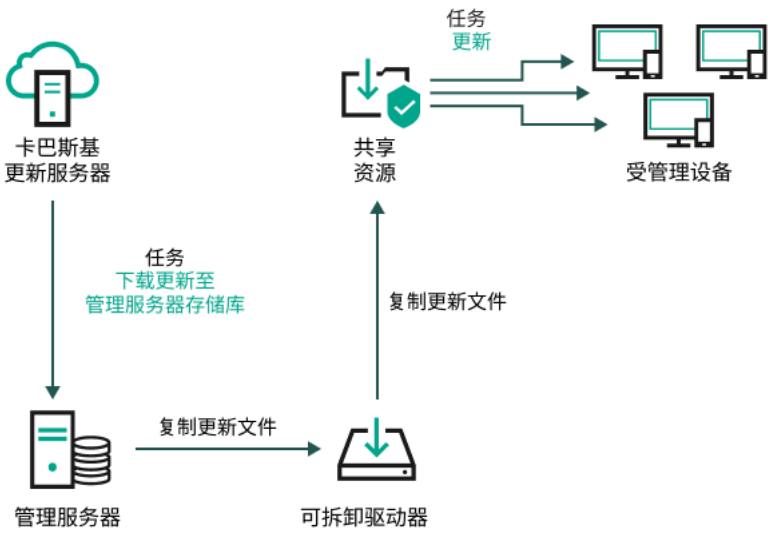
运行 MacOS 的分发点设备无法从 Kaspersky 更新服务器下载更新。

如果一个或多个运行 macOS 的设备在“*将更新下载至分发点存储库*”任务范围内，则该任务将以“*失败*”状态完成，即使该任务在所有 Windows 设备上均已成功完成。

此方案也需要“*将更新下载至管理服务器存储库*”任务，因为该任务被用于下载 Kaspersky 数据库和 Kaspersky Security Center 软件模块。

通过本地文件夹、共享文件夹或 FTP 服务器手动

如果客户端设备未连接到管理服务器，您可以使用本地文件夹或共享资源作为 Kaspersky 数据库、软件模块和应用程序的更新源。在此方案中，您需要从管理服务器存储库复制所需更新到可移动驱动器，然后复制更新到在 Kaspersky Endpoint Security 设置中指定为更新源的本地文件夹或共享资源（参见下图）。



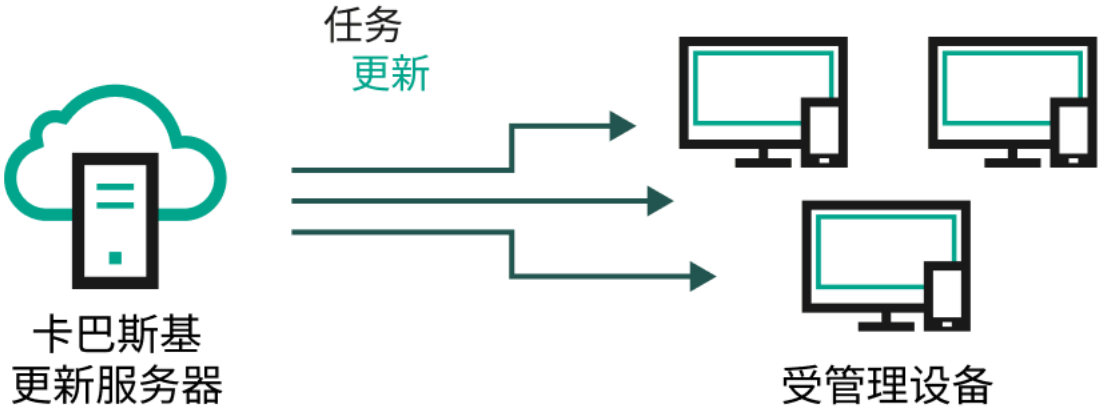
通过本地文件夹、共享文件夹或 FTP 服务器更新

有关 Kaspersky Endpoint Security 中更新源的更多信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助

直接从卡巴斯基更新服务器到受管理设备上的 Kaspersky Endpoint Security

在受管理设备上，您可以配置 Kaspersky Endpoint Security 直接从 Kaspersky 更新服务器接收更新（参见下图）。



直接从 Kaspersky 更新服务器更新安全应用程序

在此方案中，安全应用程序不使用 Kaspersky Security Center 提供的存储库。要直接从 Kaspersky 更新服务器接收更新，在安全应用程序界面中指定 Kaspersky 更新服务器作为更新源。有关这些设置的详细信息，请参见以下帮助文档：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助

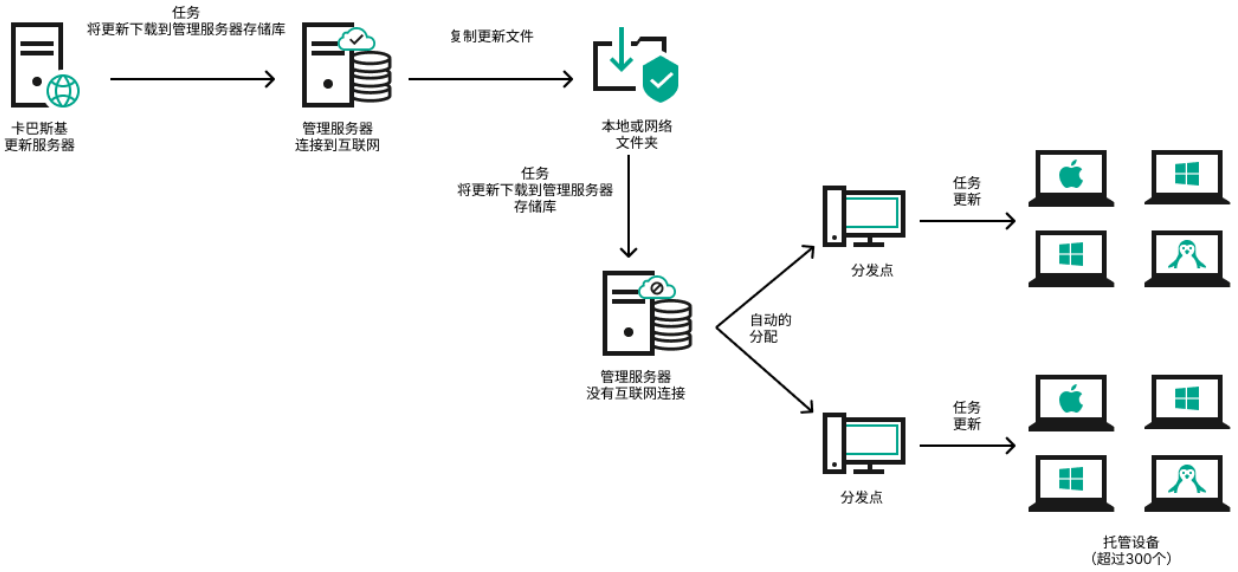
如果管理服务器没有互联网连接，则通过本地或网络文件夹

如果管理服务器没有互联网连接，您可以配置“*将更新下载至管理服务器存储库*”任务以从本地或网络文件夹下载更新。在这种情况下，必须不时地将所需的更新文件复制到指定文件夹。例如，您可以从以下来源之一复制所需的更新文件：

- 具有互联网连接的管理服务器（请参见下图）

  由于管理服务器只下载安全应用程序请求的更新，管理服务器管理的安全应用程序集（有互联网连接的应用程序和没有互联网连接的应用程序）必须匹配。

  如果用于下载更新的管理服务器版本为 13.2 或更早，请打开“*将更新下载至管理服务器存储库*”任务的属性，然后启用“**使用旧方案下载更新**”选项。



如果管理服务器没有互联网连接，则通过本地或网络文件夹更新

- 卡巴斯基更新实用程序

  由于此实用程序使用旧方案下载更新，请打开“*将更新下载至管理服务器存储库*”任务，然后启用“**使用旧方案下载更新**”选项。

创建“将更新下载至管理服务器存储库”任务

管理服务器的“*将更新下载至管理服务器存储库*”任务由 Kaspersky Security Center 快速启动向导自动创建。您只能创建一个“*将更新下载至管理服务器存储库*”任务。因此，只有将“*将更新下载至管理服务器存储库*”任务从管理服务器任务列表中删除后，才能创建此任务。

此任务需要从 Kaspersky 更新服务器下载更新到管理服务器的存储库。更新列表包含：

- 管理服务器数据库和软件模块更新
- Kaspersky 安全应用程序的数据库和软件模块的更新
- Kaspersky Security Center 组件更新
- Kaspersky 安全应用程序更新

更新被下载后，它们可以被传播到受管理设备。

在向受管理设备分发更新之前，可以运行“*更新验证*”任务。这样可以确保管理服务器将正确安装下载的更新，并且安全级别不会由于更新而降低。要在分发更新之前对其进行验证，请配置“*将更新下载至管理服务器存储库*”任务设置中的“**运行更新验证**”选项。

*要创建“**将更新下载至管理服务器存储库**”任务：*

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵照向导的说明操作。
3. 对于 Kaspersky Security Center 应用程序，选择“**将更新下载至管理服务器存储库**”任务类型。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。
6. 单击“**创建**”按钮。

   任务被创建并显示在任务列表。
7. 点击创建的任务的名称以打开任务属性窗口。
8. 在任务属性窗口中的“**应用程序设置**”选项卡上，指定以下设置：

   - **更新源**

     以下资源可以用作管理服务器的更新源：

     - 卡巴斯基更新服务器

       Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。默认下，管理服务器与 Kaspersky 更新服务器通信并使用 HTTPS 协议下载更新。您可以配置管理服务器使用 HTTP 协议，而不是 HTTPS。

       默认选择。
     - 主管理服务器

       此资源适用于为从属或虚拟管理服务器创建的任务。
     - 本地或网络文件夹

包含最新更新的本地或网络文件夹。网络文件夹可以是 FTP 或 HTTP 服务器，或者 SMB 共享。如果网络文件夹需要身份验证，则仅支持 SMB 协议。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

更新源所使用的 FTP 或 HTTP 服务器或网络文件夹必须包含匹配 Kaspersky 更新服务器所创建的结构的文件夹结构（带有更新）。

如果包含更新的共享文件夹受密码保护，请启用“**指定账户以访问更新源的共享文件夹(如果有)**”选项并输入访问所需的账户凭据。

- **更新存储文件夹**

  用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

- 其他设置：

  - **强制从属管理服务器更新**

    如果启用该选项，当新更新下载后管理服务器立刻在从属管理服务器上启动更新任务。更新任务通过使用在从属管理服务器上的任务属性中配置的更新源来启动。

    如果禁用此选项，从属管理服务器上的更新任务将根据计划启动。

    默认情况下已禁用该选项。

  - **复制下载的更新到附加文件夹**

    管理服务器接收更新后，它复制它们到指定文件夹。如果您想要在您的网络上手动管理更新的分发，则使用该选项。

    例如，您可能要在以下情况下使用该选项：您组织的网络包含几个独立子网，且每个子网的设备不能访问其他子网。然而，所有子网中的设备都可以访问通用网络共享。此种情况下，您在子网之一设置管理服务器从 Kaspersky 更新服务器下载更新，启用该选项，然后指定该网络共享。对于其他管理服务器的“将更新下载至存储库”任务中，指定与更新源相同的网络共享。

    如果您选择将下载的更新复制到本地文件夹，则必须在已安装管理服务器的设备上指定文件夹。文件夹路径取决于设备的操作系统。由于本地文件夹位于基于 Linux 的管理服务器上，因此您必须指定 POSIX 路径，例如 /path/to/dir。

    选择位于基于 Linux 的管理服务器上的网络文件夹时，您必须预先确保已安装管理服务器的设备可以通过挂载该文件夹来访问该网络文件夹。对文件夹的访问使用 SMB 协议执行。

    默认情况下已禁用该选项。

  - **在复制完成之前不强制更新设备和从属管理服务器**

    下载更新到客户端设备和从属管理服务器任务仅在这些更新从主更新文件夹被复制到附加更新文件夹后才启动。

    如果客户端设备和从属管理服务器从附加网络文件夹下载更新，则必须启用该选项。

    默认情况下已禁用该选项。

- **更新内容**:
  - **下载差异文件**

    该选项启用下载 diff 文件功能。

    默认情况下已禁用该选项。

- **使用旧方案下载更新**

  从版本 14 开始，Kaspersky Security Center 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

  例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

  - 卡巴斯基更新实用程序

    此实用程序使用旧方案下载更新。

  - Kaspersky Security Center 13.2 或更低版本

    例如，您的管理服务器 1 没有互联网连接。在这种情况下，您可以使用具有互联网连接的管理服务器 2 下载更新，然后将更新放置到本地或网络文件夹以将其用作管理服务器 1 的更新源。如果管理服务器 2 的版本为 13.2 或更低，请在管理服务器 1 的任务中启用“**使用旧方案下载更新**”选项。

  默认情况下已禁用该选项。

- **运行更新验证**

  管理服务器从源下载更新并将其保存到临时存储库，然后运行“**更新验证任务**”字段中定义的任务。如果任务成功完成，则将更新从临时存储库复制到管理服务器上的共享文件夹，然后分发到所有将管理服务器作为更新源的设备（启动具有“**当新更新下载至存储库时**”计划类型的任务）。只有在执行“*更新验证*”任务之后，将更新下载至存储库的任务才完成。

  默认情况下已禁用该选项。

9. 在任务属性窗口中的“**计划**”选项卡上，创建任务启动计划。如果必要，指定以下设置：

- **启动任务：**

  选择任务运行计划并配置所选计划。

  - **手动**

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每 N 小时**

  任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

  默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

- **每 N 天**

  任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

  默认下，任务每天运行一次，从当前系统日期和时间开始。

- **周中天数**

  任务在每周指定日期的指定时间定期运行。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **每个月所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在“*病毒爆发*”事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用“***Turn on the device***”选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。
    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- **如果任务运行超过该时间则停止**

  在指定时间段过后，任务被自动停止，无论它是否完成。

  如果您想要中断或停止执行时间太长的任务，则启用该选项。

  默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

10. 单击“**保存**”按钮。

任务被创建和配置。

当管理服务器执行“*将更新下载至管理服务器存储库*”任务时，数据库和软件模块的更新将从更新源下载并存储在管理服务器的共享文件夹中。如果您为管理组创建此任务，它将仅被应用到包含在指定管理组中的网络代理。

这些更新将从管理服务器共享文件夹分发至客户端设备和从属管理服务器。

验证已下载的更新

安装更新到受管理设备之前，您可以先通过“*更新验证*”任务检查更新。作为“*将更新下载至管理服务器存储库*”任务的一部分，“*更新验证*”任务会自动执行。管理服务器从更新源下载更新，将其保存在临时存储库并执行“*更新验证*”任务。如果任务成功完成，更新将从临时存储库复制到管理服务器共享文件夹。它们被分发到所有以该管理服务器为更新源的客户端设备。

如果“*更新验证*”任务的结果显示位于临时存储库中的更新是错误的，或“*更新验证*”任务发生错误，这些更新不会被复制到共享文件夹。管理服务器保留之前的更新集。此外，计划类型为“**当新更新下载至存储库时**”的任务也不会启动。如果新更新扫描成功完成，在下次启动“*将更新下载至管理服务器存储库*”任务时将执行这些操作。

如果在一台或多台测试设备上出现以下情况，那么更新集合就被认为是无效的：

- 发生了更新任务错误。
- 安全应用程序的实时保护状态在应用更新后更改。
- 运行按需扫描任务过程中发现了一个被感染的对象。
- Kaspersky 程序出现运行时错误。

如果在任何测试设备上未出现以上情况，该更新集就被认为是有效的，“*更新验证*”任务被认为已成功完成。

在开始创建“*更新验证*”任务之前，请执行先决条件：

1. 创建包含多台测试设备的管理组。您将需要此组来验证更新。

   建议使用网络中具有最可靠的保护和最常用的应用程序配置的设备。这种方法可提高扫描期间病毒检测的质量和可能性，并将误报的风险降至最低。如果在测试设备上检测到病毒，“*更新验证*”任务将被视为不成功。

2. 为 Kaspersky Security Center 支持的应用程序（例如 Kaspersky Endpoint Security for Windows 或 Kaspersky Security for Windows Server）创建更新和恶意软件扫描任务。创建更新和恶意软件扫描任务时，请指定具有测试设备的管理组。

   “*更新验证*”任务会在测试设备上依次运行更新和恶意软件扫描任务，以检查所有更新是否有效。此外，在创建“*更新验证*”任务时，您需要指定更新和恶意软件扫描任务。

3. 创建“*将更新下载至管理服务器存储库*”任务。

要让 Kaspersky Security Center 将更新分发至客户端设备前对下载的更新进行验证，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击“**将更新下载至管理服务器存储库**”任务。
3. 在打开的任务属性窗口中，转到“**应用程序设置**”选项卡，然后启用“**运行更新验证**”选项。

4. 如果“*更新验证*”任务存在，请单击“**选择任务**”按钮。在打开的窗口中，在具有测试设备的管理组中选择“*更新验证*”任务。

5. 如果您先前未创建“*更新验证*”任务，请执行以下操作：

   a. 单击“**新任务**”按钮。

   b. 如果要更改预设名称，则在打开的“新任务向导”中指定任务名称。

   c. 选择您先前创建的具有测试设备的管理组。

   d. 首先，选择 Kaspersky Security Center 支持的所需应用程序的更新任务，然后选择恶意软件扫描任务。

   之后，会出现以下选项。我们建议将这些选项保持启用状态：

   - **在数据库更新后重启设备**

     在设备上更新反病毒数据库后，建议重新启动设备。

     默认情况下已启用该选项。

   - **在数据库更新和设备重启后检查实时保护状态**

     如果启用此选项，则“*更新验证*”任务将检查下载到管理服务器存储库的更新是否有效，以及在反病毒数据库更新和设备重启后保护级别是否降低。

     默认情况下已启用该选项。

   e. 指定运行“*更新验证*”任务将使用的账户。您可以使用您的账户并保持“**默认账户**”选项为启用状态。或者，您可以指定另一个用于运行该任务并具有必要访问权限的账户。为此，请选择“**指定账户**”选项，然后输入该账户的凭据。

6. 单击“**保存**”关闭“*将更新下载至管理服务器存储库*”任务的属性窗口。

自动更新验证被启用。现在，您可以运行“*将更新下载至管理服务器存储库*”任务，它将从更新验证开始。

创建“将更新下载至分发点存储库”任务

*将更新下载到分发点存储库*任务仅在运行 Windows 的分发点设备上起作用。运行 Linux 或 MacOS 的分发点设备无法从 Kaspersky 更新服务器下载更新。如果至少有一台运行 Linux 或 macOS 的设备在任务范围内，则该任务将具有*失败*状态。即使在所有 Windows 设备上成功完成任务，它也会在其余设备上返回错误。

您可以为管理组创建“*将更新下载至分发点存储库*”任务。该任务将为包含在指定管理组中的分发点运行。

您可以使用该任务，例如，如果管理服务器和分发点之间的流量比分发点和 Kaspersky 更新服务器之间的流量贵，或者如果您的管理服务器没有互联网访问。

此任务需要从 Kaspersky 更新服务器下载更新到分发点的存储库。更新列表包含：

- Kaspersky 安全应用程序的数据库和软件模块的更新
- Kaspersky Security Center 组件更新
- Kaspersky 安全应用程序更新

更新被下载后，它们可以被传播到受管理设备。

如果分发点使用代理服务器连接到互联网，则您必须在网络代理策略中指定相应的设置。

*要创建“**将更新下载至分发点存储库**”任务，对于选定的管理组：*

1. 在主菜单中，转到“**资产(设备)**”→“**任务**”。
2. 单击“**添加**”按钮。
   “新任务向导”启动。遵照向导的说明操作。
3. 对于 Kaspersky Security Center 应用程序，在“**任务类型**”字段中选择“**将更新下载至分发点存储库**”。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择一个选项按钮以指定管理组、设备分类或应用程序任务的设备。
6. 在“**完成任务创建**”步骤，如果要修改默认任务设置，请启用“**创建完成时打开任务详情**” 选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。
7. 单击“**创建**”按钮。
   任务被创建并显示在任务列表。
8. 点击创建的任务的名称以打开任务属性窗口。
9. 在任务属性窗口的“**应用程序设置**”选项卡上，指定以下设置：

   - **更新源**

     以下资源可以用作分发点的更新源：

     - Kaspersky 更新服务器

       Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

       默认情况下已选中该选项。

     - 本地或网络文件夹

       包含最新更新的本地或网络文件夹。网络文件夹可以是 FTP 或 HTTP 服务器，或者 SMB 共享。如果网络文件夹需要身份验证，则仅支持 SMB 协议。在选择本地文件夹时，您必须在安装了管理服务器的设备上指定一个文件夹。

       更新源所使用的 FTP 或 HTTP 服务器或网络文件夹必须包含匹配 Kaspersky 更新服务器所创建的结构的文件夹结构（带有更新）。

- **更新存储文件夹**

  用于存储已保存更新的指定文件夹的路径。您可以将指定的文件夹路径复制到剪贴板。您不能更改组任务的指定文件夹的路径。

- **下载差异文件**

  该选项启用下载 diff 文件功能。

  默认情况下已禁用该选项。

- **使用旧方案下载更新**

  从版本 14 开始，Kaspersky Security Center 使用新方案下载数据库和软件模块的更新。要使应用程序使用新方案下载更新，更新源包含的更新文件必须具有与新方案兼容的元数据。如果更新源包含的更新文件的元数据仅与旧方案兼容，请启用“**使用旧方案下载更新**”选项。否则，更新下载任务将失败。

  例如，当指定本地或网络文件夹为更新源，并且此文件夹中的更新文件已被以下应用程序之一下载时，您必须启用此选项：

  - 卡巴斯基更新实用程序

    此实用程序使用旧方案下载更新。

  - Kaspersky Security Center 13.2 或更低版本

    例如，分发点配置为从本地或网络文件夹获取更新。在这种情况下，您可以使用具有互联网连接的管理服务器下载更新，然后将更新放置到分发点的本地或网络文件夹。如果管理服务器的版本为 13.2 或更低，请在“*将更新下载至分发点存储库*”任务中启用“**使用旧方案下载更新**”选项。

  默认情况下已禁用该选项。

10. 为任务启动创建计划。如果必要，指定以下设置：

- **启动任务**

  选择任务运行计划并配置所选计划。

  - **手动**

    任务不自动运行。您仅可以手动启动。

    默认情况下已选定该选项。

  - **每 N 分钟**

    任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

    默认下，任务每 30 分钟运行一次，从当前系统时间开始。

  - **每 N 小时**

    任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

    默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

- **每 N 天**

  任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

  默认下，任务每天运行一次，从当前系统日期和时间开始。

- **按星期中的天数**

  任务在每周指定日期的指定时间定期运行。

  默认情况下，任务在每周五 6:00:00 PM 运行。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **每个月在所选周的指定天**

  任务定期运行，在指定月日的指定时间。

  默认情况下，开始时间为18:00，且未选择任何日期。

  > 请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

  您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

- 在搜索栏中输入任务名称，即可根据名称搜索任务。
- 单击排序图标可按名称对任务进行排序。
  默认情况下，任务按字母顺序升序排列。
- 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击**应用**按钮。

- **运行错过的任务**

  该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

  如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

  如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

  默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

11. 单击“**保存**”按钮。

任务被创建和配置。

除了您在任务创建过程中指定的设置，您还可以更改所创建任务的其他属性。

执行“*将更新下载至分发点存储库*”任务时，数据库和软件模块的更新从更新源下载并存储在共享文件夹。下载的更新将仅被包含在指定管理组的分发点和没有更新下载任务的更新代理使用。

启用和禁用 Kaspersky Security Center 组件的自动更新和补丁

管理服务器更新和补丁仅可以手动安装，在获得管理员的明确批准后。

在设备上安装网络代理时，自动安装 Kaspersky Security Center 组件更新和补丁被默认启用。您可以在网络代理安装过程中禁用它，或稍后使用策略禁用。

要在设备上本地安装网络代理时禁用 Kaspersky Security Center 组件自动更新和补丁：

1. 在设备上启动网络代理本地安装。
2. 在**高级设置**步骤，清空**自动安装组件的未定义状态的可应用更新和补丁**复选框。
3. 遵照向导的说明操作。

   禁用了 Kaspersky Security Center 组件自动更新和补丁的网络代理将被安装在设备。您可以稍后使用策略启用自动更新和补丁。

要在通过安装包安装网络代理到设备时禁用 Kaspersky Security Center 组件自动更新和补丁：

1. 在主菜单中，转到“**操作**” → “**存储库**” → “**安装包**”。
2. 点击**Kaspersky Security Center 网络代理 <版本号>**包。
3. 在属性窗口中，打开“**设置**”选项卡。
4. 关闭“**对未定义状态的组件自动安装可应用更新和补丁**”切换按钮。

   禁用了 Kaspersky Security Center 组件自动更新和补丁的网络代理将被从该数据包安装。您可以稍后使用策略启用自动更新和补丁。

如果在网络代理安装到设备时选择（清空）了该复选框，您可以后续启用（或禁用）使用网络代理策略自动更新。

要使用网络代理策略启用或禁用 Kaspersky Security Center 组件的自动更新和补丁：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**“。
2. 点击网络代理策略。
3. 在策略属性窗口中，打开“**应用程序设置**”选项卡。
4. 在“**管理补丁和更新**”区域中，打开或关闭“**对未定义状态的组件自动安装可应用更新和补丁**”切换按钮以分别启用或禁用自动更新和修补。
5. 为该开关按钮设置锁（🔒）。

   该策略将被应用到所选设备，且 Kaspersky Security Center 组件自动更新和补丁将在这些设备上被启用（禁用）。

自动安装 Kaspersky Endpoint Security for Windows 的更新

您可以在客户端设备上配置 Kaspersky Endpoint Security for Windows 自动更新数据库和软件模块。

要在设备上配置下载和自动安装 Kaspersky Endpoint Security for Windows 更新：

1. 在主菜单中，转到“**资产(设备)**”→ “**任务**”。
2. 单击“**添加**”按钮。

   “新任务向导”启动。遵照向导的说明。
3. 对于 Kaspersky Endpoint Security for Windows 应用程序，选择**更新**作为任务子类型。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择任务范围。
6. 指定管理组、设备分类或应用程序任务的设备。
7. 在“**完成任务创建**”步骤，如果要修改默认任务设置，请启用“**创建完成时打开任务详情**” 选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。
8. 单击“**创建**”按钮。

   任务被创建并显示在任务列表。
9. 点击创建的任务的名称以打开任务属性窗口。
10. 在任务属性窗口的“**应用程序设置**”选项卡上，以本地或移动模式定义更新任务设置：

    - **本地模式**: 连接在设备和管理服务器之间建立。
    - **移动模式**: Kaspersky Security Center 和设备之间不建立特定的连接（比如，当设备没有连接到互联网）。
11. 启用您要使用的更新源以更新 Kaspersky Endpoint Security for Windows 的数据库和应用程序模块。如果需要，使用“**上移**”和“**下移**”按钮更改列表中的更新源位置。如果启用了多个更新源，Kaspersky Endpoint Security for Windows 会尝试从列表顶部开始依次进行连接，并通过从第一个可用的更新源处获取更新包来执行更新任务。
12. 启用**安装批准的应用程序模块更新**选项，在更新应用程序数据库同时下载和安装软件模块。

    如果启用该选项，Kaspersky Endpoint Security for Windows 在运行更新任务时，通知用户有可用的软件模块更新并将软件模块更新包含在更新包中。Kaspersky Endpoint Security for Windows 仅安装您设置了“*已批准*”状态的更新；它们将通过应用程序界面或通过 Kaspersky Security Center 在本地安装。

    您也可以启用**自动安装关键应用程序模块更新**选项。如果软件模块有任何更新，Kaspersky Endpoint Security for Windows 将自动安装状态为“*关键*”的更新；其余的更新会在您批准后安装。

    如果软件模块更新需要审查并接受授权许可协议和隐私策略，程序将在用户接受用户授权许可协议和隐私策略的条款后安装更新。
13. 选择**复制更新到文件夹**复选框，程序将已下载的更新保存到指定的文件夹。

14. 计划任务。为确保及时更新，建议您选择“**当新更新下载至存储库时**”选项。

15. 点击“**保存**”。

更新任务正在运行时，程序发送请求到 Kaspersky 更新服务器。

一些更新需要安装最新版本的管理插件。

批准和拒绝软件更新

更新安装任务的设置可能需要对要安装的更新进行批准。您可以批准必须安装的更新并拒绝不能安装的更新。

例如，您可能想先在测试环境中检查更新安装以确保它们不干预设备操作，仅在这之后允许安装这些更新到客户端设备。

批准和拒绝更新仅适用于安装在 Windows 客户端设备上的网络代理和受管理应用程序。不支持管理服务器、Kaspersky Security Center Web Console 和管理 Web 插件的无缝更新。要更新这些组件，您必须从卡巴斯基网站下载最新版本，然后手动进行安装。

要批准或拒绝一个或几个更新：

1. 在主菜单中，转到“**操作**”→“**卡巴斯基应用程序**”→“**无缝更新**”。
   可用更新列表被显示。

   受管理应用程序的更新可能需要安装 Kaspersky Security Center 的特定最低版本。如果此版本高于当前版本，则会显示这些更新，但无法批准。此外，在升级 Kaspersky Security Center 之前，无法从此类更新创建安装包。系统会提示您将 Kaspersky Security Center 实例升级到所需的最低版本。

2. 选择您要批准或拒绝的更新。

3. 单击“**批准**”批准所选更新或单击“**拒绝**”拒绝所选更新。
   默认值是 *未定义*。

   您分配了*已批准*状态的更新被放置在安装队列。

   您分配了*已拒绝*状态的更新被从先前将其安装的设备上卸载（如果可能）。而且，它们将来也不会被安装到其他设备。

Kaspersky 应用程序的一些更新无法被卸载。如果您为其设置了*已拒绝*状态，Kaspersky Security Center 将不会从先前将其安装的设备上卸载这些更新。然而，这些更新将来也不会被安装到其他设备。

如果您为第三方软件更新设置了*已拒绝*状态，这些更新将不会安装在计划将其安装但并未将其安装的设备上。更新将保持在已将其安装的设备上。如果您必须删除更新，您可以在本地手动删除它们。

更新管理服务器

您可以使用更新管理服务器向导安装管理服务器更新。

要安装管理服务器更新：

1. 在主菜单中，转到“**操作**”→“**卡巴斯基应用程序**”→“**无缝更新**”。
2. 以下列方式之一运行更新管理服务器向导。
   - 在更新列表中，单击管理服务器更新的名称，然后在打开的窗口中单击“**运行更新管理服务器向导**”链接。
   - 单击窗口顶部的通知字段中的“**运行更新管理服务器向导**”链接。
3. 在“更新管理服务器向导”窗口中，选择以下选项之一以指定何时安装更新：
   - **现在安装**。如果要立即安装更新，则选择此选项。
   - **延迟安装**。如果要稍后安装更新，则选择此选项。在这种情况下，将显示有关此更新的通知。
   - **忽略更新**。如果您不想安装更新并且不想接收有关此更新的通知，则选择此选项。
4. 如果要在安装更新之前创建管理服务器的备份，则选择“**安装更新前创建管理服务器备份副本**”选项。
5. 单击“**确定**”按钮完成向导。

如果备份过程中断，更新安装过程也会中断。

启用和禁用离线模式更新下载

我们建议您避免禁用离线模式更新下载。禁用它可能导致更新传送到设备失败。在某些情况下，Kaspersky 技术支持专家可能建议您禁用“**提前从管理服务器下载更新和反病毒数据库**”选项。然后，您将必须确保接收 Kaspersky 应用程序更新的任务被设置。

要为管理组启用或禁用离线模式更新下载：

1. 在主菜单中，转到“**资产(设备)**” → “**策略和配置文件**。
2. 单击**组**。
3. 在管理组结构中，选择您要启用离线模式更新下载的管理组。
4. 点击网络代理策略。
   网络代理策略的属性窗口打开。

默认下，子策略的设置从父策略继承且无法被修改。如果您要修改的策略是继承的，您首先需要在所需管理组为网络代理创建新策略。在新创建的策略中，您可以修改未在父策略中锁定的设置。

5. 在“**应用程序设置**”选项卡中，选择“**管理补丁和更新**”区域。

6. 启用或禁用“**提前从管理服务器下载更新和反病毒数据库(推荐)**”选项以分别启用或禁用更新下载的离线模式。

   默认下，离线模式更新下载已启用。

这样便启用或禁用了离线模式更新下载。

更新离线设备上的 Kaspersky 数据库和软件模块

更新受管理设备上的 Kaspersky 数据库和软件模块对于保持设备对病毒和其他威胁的防护是非常重要的任务。管理员通常通过使用管理服务器存储库或分发点存储库来配置定期更新。

当您需要在未连接到管理服务器（主或从）、分发点或互联网的设备（或设备组）上更新数据库和软件模块时，您必须使用其他更新源，例如 FTP 服务器或本地文件夹。此种情况下，您必须使用大容量设备传送所需更新的文件，例如闪存驱动器或外部硬盘驱动器。

您可以从这里复制所需更新：

- 管理服务器。

  为确保管理服务器存储库包含所需的安装在离线设备上的安全应用程序的更新，至少一台受管理的在线设备必须安装了相同的安全应用程序。该应用程序必须配置为通过“将更新下载至管理服务器存储库”任务从管理服务器存储库接收更新。

- 任何安装了相同安全应用程序，并配置为从管理服务器存储库、分发点存储库或直接从 Kaspersky 更新服务器接收更新的设备。

以下是通过从管理服务器存储库复制而更新数据库和软件模块的例子。

要更新离线设备上的 Kaspersky 数据库和软件模块：

1. 连接可移动驱动器到管理服务器所在设备。

2. 复制更新文件到可移动驱动器。

   默认下，更新位于：\\<server name>\KLSHARE\Updates。

   或者，您可以配置 Kaspersky Security Center 定期复制更新到您选择的文件夹。为此，请使用“将更新下载至管理服务器存储库”任务的属性中的“**复制下载的更新到附加文件夹**”选项。如果您指定闪存驱动器或外部硬盘驱动器上的文件夹作为该选项的目标文件夹，该大容量存储设备将总是包含更新的最新版本。

3. 在离线设备上，配置安全应用程序(例如，Kaspersky Endpoint Security for Windows)以从本地文件夹或共享文件夹接收更新，例如 FTP 服务器或共享文件夹。

4. 从可移动驱动器复制更新到您想用作更新源的本地文件夹或共享资源。

5. 在需要安装更新的离线设备上，启动 Kaspersky Endpoint Security for Windows 的更新任务。

更新任务完成后，设备上的 Kaspersky 数据库和软件模块为最新。

备份和恢复 Web 插件

Kaspersky Security Center Web Console 允许您备份 Web 插件的当前状态，以便以后能够恢复保存的状态。例如，您可以在将 Web 插件更新到较新版本之前对其进行备份。更新后，如果较新的版本不符合您的要求或期望，您可以从备份中恢复以前版本的 Web 插件。

要备份 Web 插件：

1. 在主菜单中，转到**设置 → Web 插件**。
2. 在“**Web 插件**”区域中，选择要备份的 Web 插件，然后单击“**创建备份副本**”按钮。

   选定的 Web 插件得到备份。您可以在“**备份**”区域中查看创建的备份。

要从备份中恢复 Web 插件：

1. 在主菜单中，转到“**设置 → 备份**”。
2. 在“**备份**”区域中，选择要恢复的 Web 插件的备份，然后单击“**从备份恢复**”按钮。

   Web 插件将从选定的备份中恢复。

分发点和连接网关的调整

Kaspersky Security Center 中的管理组结构运行以下功能：

- 设置策略范围

  将相关设置应用到设备还有一种方式：使用*策略配置文件*。此种情况下，策略范围使用标签、Active Directory 组织单元中的设备位置、Active Directory 安全组中的成员关系等进行设置。

- 设置组任务范围

  还有一个不基于管理组层级定义组任务范围的方法：使用设备分类的任务和特定设备的任务。

- 设置设备、虚拟管理服务器和从属管理服务器的访问权限。
- 分配分发点

当建立管理组结构时，您必须考虑到组织网络的拓扑以便最优分配分发点。分发点的最优分发允许您在企业网络中保存流量。

根据组织图表和网络拓扑，以下标准配置可以被应用到管理组结构：

- 单一办公室
- 多个小远程分办公室

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

分发点的标准配置：单一办公室

在标准“单一办公室”配置中，所有设备都在组织网络中，因此它们能看见彼此。组织网络可能包含几部分(网络或网段)，由窄通道连接。

有以下构建管理组结构的方法：

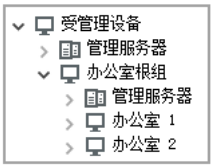
- 构建管理组结构涉及到网络拓扑。管理组结构可能不精确反映网络拓扑。网络各部分之间以及特定管理组相互匹配。您可以使用分发点自动分配或手动分配它们。

- 不考虑网络拓扑而构建管理组结构。此种情况下，您必须禁用分发点自动分配，然后为网络中每个部分的根管理组分配一个或几个设备作为分发点，例如为“**受管理设备**”组。所有分发点将处于相同级别，并将掌控组织网络中所有设备的相同范围。此种情况下，每个网络代理都将连接到具有最短路由的分发点。分发点的路由可以使用 tracert 使用工具跟踪。

分发点的标准配置：多个小远程办公室

该标准配置可用于多个小型远程办公室，它们可能通过互联网与总部联络。每个远程办公室都位于 NAT 之外，就是说，从一个远程办公室到另一个远程办公室的连接是不可能的，因为办公室是彼此隔离的。

配置必须在管理组中体现：必须为每个远程办公室创建各自的管理组（下图中的组**办公室 1**和**办公室 2**）。



远程办公室包含在管理组结构

必须指定一个或多个分发点给每个办公室的对应管理组。分发点必须是远程办公室中具有足够剩余磁盘空间的设备。部署在**办公室 1**组的设备，例如，将访问分配到**办公室 1**管理组的分发点。

如果一些用户在办公室之间移动他们的便携电脑，您必须在远程办公室选择两个或更多设备(除了现有的分发点)并分配它们作为等级管理组的分发点(上图中**办公室根组**)。

例如：便携式电脑部署在**办公室 1**管理组，然后被移动到对应于**办公室 2** 管理组的办公室。在移动便携式电脑后，网络代理试图访问分配到**办公室 1**组的分发点，但是那些分发点不可用。然后，网络代理开始尝试访问分配到**办公室根组**的分发点。因为远程办公室是彼此隔离的，尝试访问分配到**办公室根组**管理组的分发点仅在网络代理尝试访问**办公室 2** 组中的分发点时才会成功。就是说，便携式电脑将保持在原始办公室对应的管理组，但是将使用它当时所在办公室的分发点。

关于分配分发点

您可以手动或者自动将受管设备分配为分发点。

如果手动将受管设备分配为分发点，您可以选择网络中的任何设备。

如果您自动分配分发点，Kaspersky Security Center 只能选择满足以下条件的受管设备：

- 设备有至少 50 GB 的可用磁盘空间。
- 受管设备直接与 Kaspersky Security Center 连接（不通过网关）。
- 受管设备不是笔记本电脑。

> 如果您的网络没有满足指定条件的设备，Kaspersky Security Center 将不会自动将任何设备分配为分发点。

自动分配分发点

我们建议您自动分配分发点。此种情况下，Kaspersky Security Center 将自行选择哪个设备要被分配为分发点。

要自动分配分发点：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 选择“**自动分配分发点**”选项。

   > 如果自动指派设备做为分发点被启用，您无法手动配置分发点，也不能编辑分发点列表。

4. 单击“**保存**”按钮。

管理服务器便自动指派和配置分发点。

手动分配分发点

Kaspersky Security Center 允许您手动指定设备做为分发点。

我们建议您自动分配分发点。此种情况下，Kaspersky Security Center 将自行选择哪个设备要被分配为分发点。然后，如果您由于一些原因必须不自动分配分发点（例如，如果您要使用单独分配的服务器），您可以在计算数量和配置后手动分配分发点。

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

要手动指派设备做为分发点：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。

3. 选择“**手动分配分发点**”选项。

4. 单击“**分配**”按钮。

5. 选择您要制作分发点的设备。
   选择设备时，请牢记分发点的操作功能以及设备做为分发点的需求。

6. 选择您要包含在所选分发点范围的管理组。

7. 单击“**确定**”按钮。
   您添加的分发点将显示在“**分发点**”区域的分发点列表中。

8. 在列表中单击新添加的分发点以打开其属性窗口。

9. 在属性窗口中配置分发点：

   - “**常规**”区域中包含用于设定分发点与客户端设备进行交互的设置：

     - **SSL 端口**

       客户端设备与分发点之间，使用 SSL 进行安全连接的 SSL 端口号。
       默认情况下使用端口 13000。

     - **使用多点传送**

       如果启用此选项，将使用 IP 多点传送自动向组内的客户端设备上分发安装包。
       IP 多点传送减少了将应用程序从安装包安装到一组客户端设备所需的时间，但是增加了在将应用程序安装到单个客户端设备时的安装时间。

     - **IP 多点传送地址**

       用于多点传送的 IP 地址。您可以定义范围是 224.0.0.0 – 239.255.255.255 的 IP 地址
       默认情况下，Kaspersky Security Center 自动分配一个在给定范围内的唯一 IP 多播地址。

     - **IP 多点传送端口号**

       IP 多点传送的端口号。
       默认情况下，端口号指定为 15001。如果运行管理服务器的设备指定为分发点，端口 13001 默认用于 SSL 连接。

     - **远程设备的分发点地址**

       远程设备连接到分发点所用的 IPv4 地址。

- **部署更新**

  更新被从以下来源分发到受管理设备：

  - 此分发点（如果启用此选项）。
  - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

  如果您使用分发点来部署更新，则可以节省流量，因为您减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。你可以计算分发点的数量以便网络优化流量和负载。

  如果禁用此选项，管理服务器上的更新下载和加载次数可能会增加。默认情况下已启用该选项。

- **部署安装包**

  安装包被从以下来源分发到受管理设备：

  - 此分发点（如果启用此选项）。
  - 其他分发点、管理服务器或 Kaspersky 更新服务器（如果禁用此选项）。

  如果使用分发点部署安装包，您可以节省流量，因为减少了下载次数。此外，您可以减轻管理服务器上的负载并在分发点之间重新定位负载。你可以计算分发点的数量以便网络优化流量和负载。

  如果禁用此选项，管理服务器上的安装包下载和加载次数可能会增加。默认情况下已启用该选项。

- **运行推送服务器**

  在 Kaspersky Security Center 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

- **推送服务器端口**

  推送服务器的端口号。您可以指定任何未占用的端口号。

- 在“**范围**”区域，指定分发点发布更新的范围（管理组和/或网络定位）。

  仅运行 Windows 操作系统的设备可以定义网络位置。网络位置无法定义在运行其他操作系统的设备上。

- 如果分发点在管理服务器以外的机器上运行，则在“**更新源**”区域中，可以选择分发点的更新源：

  - **更新源**

    选择分发点的更新源：

    - 要允许分发点从管理服务器接收更新，请选择“**从管理服务器检索**”。
    - 要允许分发点使用任务接收更新，请选择“**使用更新下载任务**”，然后指定“*将更新下载至分发*

点存储库"任务：

- 如果设备上已存在此类任务，请在列表中选择该任务。
- 如果设备上尚不存在此类任务，请单击"**创建任务**"链接创建任务。"新任务向导"启动。遵照向导的说明操作。

- **下载差异文件**

  该选项启用下载 diff 文件功能。

  默认情况下已启用该选项。

- 如果您的分发点在连接到互联网时使用代理服务器，则可以在**互联网连接设置**子部分中指定以下设置：

  - **使用代理服务器**

    如果选择该选框，您可以在输入字段中配置代理服务器连接。
    默认情况下已清除该选框。

  - **代理服务器地址**

    代理服务器地址。

  - **端口号**

    用于连接的端口号。

  - **对本地地址不使用代理服务器**

    如果启用此选项，将不使用代理服务器连接本地网络的设备。
    默认情况下已禁用该选项。

  - **代理服务器身份验证**

    如果选择该选框，您可以在输入字段中为代理服务器身份验证指定凭证。
    默认情况下已清除该选框。

  - **用户名**

    建立连接代理服务器的用户账户。

  - **密码**

    任务运行时使用的账户的密码。

- 在“**KSN 代理**”区域，您可以配置应用程序使用分发点从受管理设备转发 KSN 请求：

  - **在分发点端启用 KSN 代理**

    KSN 代理服务运行在用作分发点的设备上。使用该功能重新分发和优化网络流量。

    分发点将卡巴斯基安全网络声明中列出的KSN统计数据发送给卡巴斯基。

    默认情况下已禁用该选项。启用该选项仅在**使用管理服务器作为代理服务器**和**我同意使用卡巴斯基安全网络**选项在管理服务器属性窗口中被启用时起作用。

    您可以分配活动被动集群节点到分发点并在该节点上启用 KSN 代理服务器。

  - **转发 KSN 请求到管理服务器**

    分发点从受管理设备转发 KSN 请求到管理服务器。

    默认情况下已启用该选项。

  - **通过互联网直接访问 KSN 云/KPSN**

    分发点从受管理设备转发 KSN 请求到 KSN 云或 KPSN。分发点本身上生成的 KSN 请求也直接发送到 KSN 云或 KPSN。

    安装了网络代理版本 11（或更早版本）的分发点不能直接访问 KPSN。如果要重新配置分发点以将 KSN 请求发送到 KPSN，请为每个分发点启用“**转发 KSN 请求到管理服务器**”选项。

    安装了网络代理版本 12（或更高版本）的分发点可以直接访问 KPSN。

  - **当连接到 KPSN 时忽略代理服务器设置**

    如果您在分发点属性或网络代理策略中配置了代理服务器设置，但您的网络架构要求您直接使用 KPSN，则启用此选项。否则，从受管理应用程序的请求无法到达 KPSN。

    如果您选择“**通过互联网直接访问 KSN 云/KPSN**”选项，则此选项可用。

  - **端口**

    受管理设备将用于连接到 KSN 代理服务器的 TCP 端口号。默认端口号是 13111。

  - **使用 UDP 端口**

    如果需要受管理设备通过 UDP 端口连接到 KSN 代理，则启用“**使用 UDP 端口**”选项并指定 UDP 端口号。默认情况下已启用该选项。

  - **UDP 端口**

    受管理设备将用于连接到 KSN 代理服务器的 UDP 端口号。连接到 KSN 代理的默认 UDP 端口是 15111。

- 如果分发点在管理服务器以外的机器上运行，则在“**连接网关**”区域中，可以配置分发点，充当网络代理实例和管理服务器之间连接的网关：

  - **连接网关**

    如果由于您的网络组织而无法在管理服务器和网络代理之间建立直接连接，您可以使用分发点作为管理服务器和网络代理之间的连接网关。

    如果您需要分发点充当网络代理和管理服务器之间的连接网关，请启用此选项。默认情况下已禁用该选项。

  - **从管理服务器建立连接到网关(如果网关位于 DMZ 中)**

    如果管理服务器位于隔离区域 (DMZ) 之外，在局域网中，安装在远程设备上的网络代理无法连接到管理服务器。您可以使用分发点作为具有反向连接的连接网关（管理服务器建立到分发点的连接）。

    如果您需要将管理服务器连接到 DMZ 中的连接网关，请启用此选项。

  - **为 Kaspersky Security Center Web Console 打开本地端口**

    如果您需要 DMZ 中的连接网关为位于 DMZ 中或互联网上的 Web Console 打开一个端口，请启用此选项。指定将用于从 Web Console 连接到分发点的端口号。默认端口号是 13299。

    如果启用“**从管理服务器建立连接到网关(如果网关位于 DMZ 中)**”选项，则此选项可用。

  当通过充当连接网关的分发点将移动设备连接到管理服务器时，您可以启用以下选项：

  - **为移动设备打开端口(仅管理服务器 SSL 身份验证)**

    如果您需要连接网关为移动设备打开一个端口并指定移动设备将用于连接到分发点的端口号，请启用此选项。默认端口号是 13292。移动设备将检查管理服务器证书。建立连接时，仅对管理服务器进行身份验证。

  - **为移动设备打开端口(双向 SSL 身份验证)**

    如果您需要连接网关打开一个端口，该端口将用于管理服务器和移动设备的双向身份验证，请启用此选项。移动设备将检查管理服务器证书，管理服务器也将检查移动设备证书。指定以下参数：

    - 移动设备将用于连接到分发点的端口号。默认端口号是 13293。
    - 移动设备将使用的连接网关的 DNS 域名。用逗号分隔域名。指定的域名将包含在分发点证书中。如果移动设备使用的域名与分发点证书中的通用名称不匹配，则移动设备不会连接到分发点。

      默认 DNS 域名是连接网关的 FQDN 名称。

  在这两种情况下，仅在分发点上建立 TLS 会话期间检查证书。证书不会被转发供管理服务器检查。与移动设备建立 TLS 会话后，分发点使用管理服务器证书创建移动设备和管理服务器之间的同步隧道。如果打开双向 SSL 身份认证的端口，则分发移动设备证书的唯一方式是通过安装包。

- 通过分发点配置 Windows 域、活动目录和 IP 范围的轮询：

  - **Windows 域**

    您可以启用 Windows 域设备发现并为发现设置计划。

  - **域控制器**

    您可以启用活动目录域网络轮询并为轮询设置计划。

    如果您使用 Windows 分发点，则可以选择以下选项之一：

    - **轮询当前活动目录域**。
    - **轮询活动目录域森林**。
    - **仅轮询所选活动目录域**。如果您选择该选项，添加一个或更多活动目录域到列表。

    如果您使用安装了网络代理版本 15 的 Linux 分发点，则只能轮询为其指定地址和用户凭据的 Active Directory 域。当前 Active Directory 域和 Active Directory 域林的轮询不可用。

    您可以对域控制器启用设备发现。

    如果选择“**启用域控制器轮询**”选项，则可以选择要轮询的域控制器并为其指定轮询计划。

    如果使用 Linux 分发点，请在“**轮询指定域**”部分中单击“**添加**”，然后指定域控制器的地址和用户凭据。

    如果使用 Windows 分发点，则可以选择以下选项之一：

    - **轮询当前域**
    - **轮询整个域森林**
    - **轮询指定域**

  - **IP 范围**

    您可以针对 IPv4 范围和 IPv6 网络启用设备发现。

    如果启用“**启用范围轮询**”选项，则可以添加扫描范围并为其设置计划。您可以添加 IP 范围到已扫描范围列表。

    如果启用“**使用 Zeroconf 轮询 IPv6 网络**”选项，分发点将使用零配置网络（也称为 *Zeroconf*）自动轮询 IPv6 网络。在这种情况下，指定的 IP 范围将被忽略，因为分发点会轮询整个网络。如果分发点运行 Linux，则**使用 Zeroconf 轮询 IPv6 网络**选项可用。要使用 Zeroconf IPv6 轮询，您必须在分发点上安装 avahi-browse 实用程序。

- 在**高级**区域，指定分发点必须使用以存储发布数据的文件夹：

  - **使用默认的文件夹**

    如果您选择此选项，应用程序使用分发点上的网络代理安装文件夹。

- **使用指定的文件夹**

  如果您选择该选项，则可以在下面的字段中指定该文件夹的路径。它可以是分发点上的本地文件夹，也可以是企业网络中任何设备上的目录。

  分发点上用于运行网络代理的用户账户必须具有对指定文件夹的访问权限以进行读写操作。

10. 单击“**确定**”按钮。

    所选设备作为分发点运行。

修改管理组的分发点列表

您可以查看为特定管理组分配的分发点列表并通过添加或删除分发点来修改列表。

要查看和修改分配给管理组的分发点列表：

1. 在主菜单中，转到**资产(设备)** → **受管理设备**。
2. 在受管理设备列表上方的**当前路径**字段中，单击路径链接。
3. 在打开的左侧窗格中，选择您要查看其分配的分发点的管理组。

   这将启用**分发点**菜单项。
4. 在主菜单中，转到“**资产(设备)**” → “**分发点**”。
5. 要为管理组添加新的分发点，请单击受管理设备列表上方的**分配**按钮，然后从打开的窗格中选择设备。
6. 要删除分配的分发点，请从列表中选择设备并单击**取消分配**按钮。

   根据于您的修改，新分发点被添加到列表或现有分发点被从列表删除。

强制同步

尽管 Kaspersky Security Center 会自动同步受管理设备的状态、设置、任务和策略，但在某些情况下，您可能希望对指定设备运行强制同步。您可以对以下设备运行强制同步：

- 已安装网络代理的设备
- 正在运行 KasperskyOS 的设备

  在对 KasperskyOS 设备运行强制同步之前，请确保该设备包含在分发点范围内，并且分发点上已启用推送服务器。
- iOS 设备
- Android 设备

  在对 Android 设备运行强制同步之前，您必须配置 Firebase Cloud Messaging。

同步单个设备

要强制同步管理服务器和受管理设备：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
2. 单击要与管理服务器同步的设备名称。
   属性窗口打开，在其中已选择“**常规**”区域。
3. 单击**强制同步**按钮。

应用程序将所选设备与管理服务器同步。

同步多个设备

要在管理服务器和多台受管理设备之间强制同步：

1. 打开管理组的设备列表或设备分类：
   - 在主菜单中，转到**资产(设备)→受管理设备**，单击受管理设备列表上方的**当前路径**字段中的路径链接，然后选择包含要同步的设备的管理组。
   - 运行设备分类以查看设备列表。
2. 选中要与管理服务器同步的设备旁边的复选框。
3. 在受管理设备列表上方，单击省略号按钮 (...)，然后单击**强制同步**按钮。
   应用程序将所选设备与管理服务器同步。
4. 在设备列表中，检查所选设备与管理服务器的上次连接时间是否已更改为当前时间。如果时间未更改，则单击“**刷新**”按钮更新页面内容。

所选设备即与管理服务器同步。

查看策略传送时间

在管理服务器上更改卡巴斯基应用程序策略后，管理员可以检查是否被更改的策略被传输到了特定受管理设备。策略可以在定期同步或者强制同步中传输。

要查看应用程序策略被传输到受管理设备的日期和时间：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
2. 单击要与管理服务器同步的设备名称。
   属性窗口打开，在其中已选择“**常规**”区域。
3. 选择“**应用程序**”选项卡。
4. 选择您要查看策略同步日期的应用程序。
   应用程序策略窗口打开，在其中已选择“**常规**”区域并显示策略传送日期和时间。

启用推送服务器

在 Kaspersky Security Center 中，分发点可以用作通过移动协议管理的设备和由网络代理管理的设备的推送服务器。例如，如果您希望能强制 KasperskyOS 设备与管理服务器同步，则必须启用推送服务器。推送服务器与启用该推送服务器的分发点具有相同的受管理设备范围。如果为同一个管理组分配了多个分发点，则可以在每个分发点上都启用推送服务器。在这种情况下，管理服务器会平衡分发点之间的负载。

您可能希望将分发点用作推送服务器，以确保受管理设备和管理服务器之间存在持续连接。某些操作需要持续连接，例如运行和停止本地任务、接收受管理应用程序的统计信息或创建隧道。如果将分发点用作推送服务器，则不必在受管理设备上使用“**不要断开与管理服务器的连接**”选项或将数据包发送到网络代理的 UDP 端口。

推送服务器支持最多 50,000 个同时连接的负载。

要在分发点上启用推送服务器：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**分发点**”区域。
3. 单击要在其上启用推送服务器的分发点的名称。
   分发点属性窗口将打开。
4. 在“**常规**”区域中，启用“**运行推送服务器**”选项。
5. 在“**推送服务器端口**”字段中，键入端口号。您可以指定任何未占用的端口号。
6. 在“**远程主机地址**”字段中，指定分发点设备的 IP 地址或名称。
7. 单击“**确定**”按钮。

在所选分发点上已启用推送服务器。

在客户端设备上管理第三方应用程序

本节介绍与管理客户端设备上安装的第三方应用程序有关的 Kaspersky Security Center 功能。

安装第三方软件更新

Kaspersky Security Center 允许您管理受管理设备上安装的第三方软件的更新，并通过安装所需更新来修复 Microsoft 应用程序和其他软件厂商产品中的漏洞。

Kaspersky Security Center 通过“*查找漏洞和所需更新*”任务搜索更新。完成此任务后，管理服务器会收到检测到的漏洞列表，以及在任务属性中指定的设备上安装的第三方软件的所需更新。查看可用更新的信息后，您可以将它们安装到设备。

Kaspersky Security Center 通过删除先前的应用程序并安装新应用程序来更新应用程序。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

出于安全原因，卡巴斯基技术会自动扫描您使用漏洞和补丁管理功能安装的任何第三方软件更新，以查找恶意软件。这些技术用于自动文件检查，包括病毒扫描、静态分析、动态分析、沙盒环境中的行为分析和机器学习。

卡巴斯基专家不会对可以使用漏洞和补丁管理功能安装的第三方软件更新进行手动分析。此外，卡巴斯基专家不会在此类更新中搜索漏洞（已知或未知）或未记录的功能，也不会对上面段落中指定的更新以外的更新进行其他类型的分析。

安装第三方软件更新的任务

将第三方软件更新的元数据下载到资源库后，可以使用以下任务在客户端设备上安装更新：

- “*安装所需更新并修复漏洞*”任务

  “*安装所需更新并修复漏洞*”任务用于安装 Microsoft 应用程序的更新，包括 Windows Update 服务提供的更新以及其他供应商软件的更新。请注意，仅当您具有漏洞和补丁管理功能的授权许可时，才能创建此任务。

  完成此任务后，更新将自动安装在受管理设备上。新更新的元数据下载到管理服务器存储库后，Kaspersky Security Center 会检查更新是否满足更新规则中指定的条件。符合条件的所有新更新都将在任务下次运行时自动下载并安装。

- “*安装 Windows Update 更新*”任务

  “*安装 Windows Update 更新*”任务不需要授权许可，但只能用于安装 Windows Update 更新。

  完成此任务后，将仅安装任务属性中指定的更新。将来，如果您要安装已下载到管理服务器存储库的新更新，必须将所需更新添加到现有任务中的更新列表，或创建新的“安装 Windows Update 更新”任务。

将管理服务器用作 WSUS 服务器

Windows Update 服务提供了有关 Microsoft Windows 的可用更新的信息。管理服务器可以用作 Windows Server Update Services (WSUS) 服务器。要将管理服务器用作 WSUS 服务器，请创建“执行 Windows Update 同步”任务，然后选中网络代理策略中的“**将管理服务器用作 WSUS 服务器**”选项。在您配置了和 Windows Update 的数据同步后，管理服务器以集中模式和设置的频率在设备上提供更新到 Windows Update 服务。

方案：更新第三方软件

本节提供了更新客户端设备上安装的第三方软件的方案。第三方软件包括 Microsoft 和其他软件供应商的应用程序。Microsoft 应用程序的更新由 Windows Update 服务提供。

先决条件

管理服务器必须连接到互联网才能安装除 Microsoft 软件之外的第三方软件的更新。

默认情况下，管理服务器不需要互联网连接就可以在受管理设备上安装 Microsoft 软件更新。例如，受管理设备可以直接从 Microsoft 更新服务器下载 Microsoft 软件更新，也可以从组织的网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下载。将管理服务器用作 WSUS 服务器时，管理服务器必须连接到互联网。

阶段

更新第三方软件分阶段进行：

1 搜索所需更新

要查找受管理设备所需的第三方软件更新，请运行“*查找漏洞和所需更新*”任务。完成此任务后，Kaspersky Security Center 会收到检测到的漏洞列表，以及在任务属性中指定的设备上安装的第三方软件的所需更新。

“*查找漏洞和所需更新*”任务由管理服务器快速启动向导自动创建。如果未运行向导，请立即创建任务或运行快速启动向导。

说明：

- 管理控制台：扫描应用程序中的漏洞，安排“查找漏洞和所需更新”任务
- Kaspersky Security Center Web Console：创建“查找漏洞和所需更新”任务，“查找漏洞和所需更新”任务设置

2 分析找到的更新列表

查看“**软件更新**”列表并决定要安装哪些更新。要查看有关每个更新的详细信息，请单击列表中的更新名称。对于列表中的每个更新，您还可以查看客户端设备上更新安装的统计信息。

说明：

- 管理控制台：查看有关可用更新的信息
- Kaspersky Security Center Web Console：查看有关可用的第三方软件更新的信息

3 配置更新安装

当 Kaspersky Security Center 收到第三方软件更新列表后，您可以使用“*安装所需更新并修复漏洞*”任务或“*安装 Windows Update 更新*”任务将它们安装在客户端设备上。创建这些任务之一。您可以在“**任务**”选项卡上或使用“**软件更新**”列表创建这些任务。

“*安装所需更新并修复漏洞*”任务用于安装 Microsoft 应用程序的更新，包括 Windows Update 服务提供的更新以及其他供应商软件的更新。请注意，仅当您具有漏洞和补丁管理功能的授权许可时，才能创建此任务。

“*安装 Windows Update 更新*”任务不需要授权许可，但只能用于安装 Windows Update 更新。

要安装某些软件更新，您必须接受最终用户授权许可协议 (EULA) 才能安装软件。如果您拒绝 EULA，则不会安装该软件更新。

您可以按计划启动更新安装任务。指定任务计划时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

说明：

- 管理控制台：修复应用程序中的漏洞，查看有关可用更新的信息
- Kaspersky Security Center Web Console：创建“安装所需更新并修复漏洞”任务，创建“安装 Windows Update 更新”任务，查看有关可用的第三方软件更新的信息

4 安排任务

为确保更新列表始终是最新的，请计划“*查找漏洞和所需更新*”任务以不时自动运行该任务。默认情况下，“*查找漏洞和所需更新*”任务设置为手动启动。

如果已创建“*安装所需更新并修复漏洞*”任务，则可以将其运行频率计划成与“*查找漏洞和所需更新*”任务相同或更少。在计划“*安装 Windows Update 更新*”任务时，请注意，对于此任务，您在每次启动此任务之前都必须定义更新列表。

计划任务时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

5 批准和拒绝软件更新（可选）

如果已创建“安装所需更新并修复漏洞”任务，则可以在任务属性中指定更新安装的规则。如果已创建“安装 Windows Update 更新”任务，请跳过此步骤。

对于每条规则，都可以根据更新状态定义要安装的更新：“*未定义*”、“*已批准*”或“*已拒绝*”。例如，您可能想为服务器创建一个特定任务，并为该任务设置一条规则，以仅允许安装 Windows Update 更新以及状态为“*已批准*”的更新。之后，手动为要安装的更新设置“*已批准*”状态。在这种情况下，状态为“*未定义*”或“*已拒绝*”的 Windows Update 更新将不会安装到任务中指定的服务器上。

使用“*已批准*”状态管理更新安装对于少量更新来说非常有效。要安装多个更新，请使用可以在“*安装所需更新并修复漏洞*”任务中配置的规则。我们建议仅为那些不符合规则中指定的条件的特定更新设置“*已批准*”状态。当手动批准大量更新时，管理服务器的性能会下降，这可能导致服务器过载。

默认下，下载的软件更新具有*未定义*状态。您可以在“**软件更新**”列表（“**操作**”→“**补丁管理**”→“**软件更新**”）中将状态更改为“*已批准*”或“*已拒绝*”。

说明：

- 管理控制台：批准和拒绝软件更新
- Kaspersky Security Center Web Console：批准和拒绝第三方软件更新

6 将管理服务器配置为用作 Windows Server Update Services (WSUS) 服务器（可选）

默认情况下，Windows Update 更新从 Microsoft 服务器下载到受管理设备。您可以更改此设置以将管理服务器用作 WSUS 服务器。在这种情况下，管理服务器以指定频率将更新数据与 Windows Update 同步，并以集中模式向联网设备上的 Windows Update 提供更新。

要将管理服务器用作 WSUS 服务器，请创建“执行 Windows Update 同步”任务，然后选中网络代理策略中的“**将管理服务器用作 WSUS 服务器**”复选框。

说明：

- 管理控制台：将 Windows Update 中的更新与管理服务器同步，在网络代理策略中配置 Windows 更新
- Kaspersky Security Center Web Console：创建“执行 Windows Update 同步”任务

7 运行更新安装任务

启动“*安装所需更新并修复漏洞*”任务或“*安装 Windows Update 更新*”任务。启动这些任务后，更新将下载并安装到受管理设备上。任务完成后，请确保它在任务列表中具有“*已成功完成*”状态。

8 创建有关第三方软件更新安装结果的报告（可选）

要查看有关更新安装的详细统计信息，请创建**第三方软件更新安装结果报告**。

说明：

- 管理控制台：创建和查看报告
- Kaspersky Security Center Web Console：生成和查看报告

结果

如果已创建并配置了“*安装所需更新并修复漏洞*”任务，则更新将自动安装到受管理设备上。新更新下载到管理服务器存储库后，Kaspersky Security Center 会检查更新是否满足更新规则中指定的条件。符合条件的所有新更新都将在任务下次运行时自动安装。

如果已创建“*安装 Windows Update 更新*”任务，则仅安装在*安装 Windows Update 更新*任务属性中指定的更新。将来，如果您要安装已下载到管理服务器存储库的新更新，必须将所需更新添加到现有任务中的更新列表，或创建新的“*安装 Windows Update 更新*”任务。

安装第三方软件更新

您可以通过创建和运行以下任一任务在受管理设备上安装第三方软件更新：

- *安装所需更新并修复漏洞*

  仅当您具有“漏洞和补丁管理”功能的授权许可时，才能创建“*安装所需更新并修复漏洞*”任务。您可以使用此任务来安装 Microsoft 提供的 Windows Update 更新和其他供应商软件的更新。

- *安装 Windows Update 更新*

  您可以使用“*安装 Windows Update 更新*”任务仅安装 Windows Update 更新。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

作为一种选择，您可以创建任务以通过以下方式安装所需的更新：

- 通过打开更新列表并指定要安装的更新。

  结果，创建了安装所选更新的新任务。作为一个选项，您可以将选定更新添加到现有任务。

- 通过运行更新安装向导。

  更新安装向导功能仅在“漏洞和补丁管理授权许可”下可用。

  该向导简化了更新安装任务的创建和配置，并允许您消除包含相同更新要安装的冗余任务的创建。

使用更新列表安装第三方软件更新

要使用更新列表安装第三方软件更新：

1. 打开更新列表之一：

   - 要打开常规更新列表，请在主菜单中转到**操作 → 补丁管理 → 软件更新**。
   - 要打开受管理设备的更新列表，请在主菜单中转到“**资产(设备)**”→“**受管理设备**”→ <设备名称> →“**高级**”→“**可用更新**”。
   - 要打开特定应用程序的漏洞列表，请在主菜单中转到**操作 → 第三方应用程序 → 应用程序注册表 →** <application name> **→ 可用更新**。

可用更新列表被显示。

2. 选中要下载的更新旁边的复选框。

3. 单击“**安装更新**”按钮。

   要安装某些软件更新，您必须接受最终用户授权许可协议 (EULA)。如果您拒绝 EULA，则不会安装该软件更新。

4. 您可以选择以下选项之一：

   - **新任务**

     新任务向导启动。如果您拥有漏洞和补丁管理授权许可，则会预先选择“*安装所需更新并修复漏洞*”任务。如果您没有授权许可，请默认选择“*安装 Windows Update 更新*”任务。按照向导的步骤完成任务创建。

   - **安装更新(添加规则到指定任务)**

     选择要向其中添加选定更新的任务。如果您拥有漏洞和补丁管理授权许可，请选择“*安装所需更新并修复漏洞*”任务。安装选定更新的新规则将自动添加到选定任务中。如果您没有授权许可，请选择“*安装 Windows Update 更新*”任务。选定更新将添加到任务属性中。

     任务属性窗口打开。单击“**保存**”按钮以保存更改。

   如果您选择了创建任务，则会创建任务并将其显示在“**资产(设备)**”→“**任务**”处的任务列表中。如果您选择了将更新添加到现有任务中，更新将保存在任务属性中。

要安装第三方软件更新，请启动“*安装所需更新并修复漏洞*”任务或“*安装 Windows Update 更新*”任务。您可以手动启动任一任务，也可以在启动的任务的属性中指定计划设置。指定任务计划时，请确保更新安装任务在“*查找漏洞和所需更新*”任务完成后启动。

使用更新安装向导安装第三方软件更新

更新安装向导功能仅在“漏洞和补丁管理授权许可”下可用。

要使用更新安装向导来创建安装第三方软件更新的任务，请执行以下操作：

1. 在主菜单中，转到**操作 → 补丁管理 → 软件更新**。

   可用更新列表被显示。

2. 选中要安装的更新旁边的复选框。

3. 单击**运行更新安装向导**按钮。

   更新安装向导开始。“**选择更新安装任务**”页面显示以下类型的所有现有任务的列表：

   - *安装所需更新并修复漏洞*
   - *安装 Windows Update 更新*
   - *修复漏洞*

   您不能修改最后两种类型的任务来安装新更新。要安装新更新，您只能使用“*安装所需更新并修复漏洞*”任务。

4. 如果您希望向导仅显示安装所选更新的那些任务，则启用“**仅显示安装该更新的任务**”选项。

5. 选择您要执行的操作：

- 要启动任务，请选中任务名称旁边的复选框，然后单击“**开始**”按钮。
- 要将新规则添加到现有任务：

  a. 选中任务名称旁边的复选框，然后单击“**添加规则**”按钮。

  b. 在打开的页面上，配置新规则：

  - **该重要级别的更新的安装规则**

    有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

    如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

    如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

    默认情况下已禁用该选项。

  - **根据 MSRC 的该重要级别的更新的安装规则**

    有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

    如果启用该选项（仅可用于 Windows Update 更新），更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

    如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

    默认情况下已禁用该选项。

  - **该供应商的更新的安装规则**

    此选项仅适用于第三方应用程序的更新。Kaspersky Security Center 仅安装与所选更新由同一供应商提供的应用程序相关的那些更新。未安装拒绝更新和其他供应商提供的应用程序更新。

    默认情况下已禁用该选项。

  - **类型是 的更新的安装规则**
  - **所选更新的安装规则**
  - **批准所选更新**

    所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

    默认情况下已禁用该选项。

  - **自动安装所选更新安装所需的所有先前应用程序更新**

    如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

默认情况下已启用该选项。

c. 单击“**添加**”按钮。

- 要创建任务：

a. 单击“**新任务**”按钮。

b. 在打开的页面上，配置新规则：

- **该重要级别的更新的安装规则**

有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

默认情况下已禁用该选项。

- **根据 MSRC 的该重要级别的更新的安装规则**

有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

如果启用该选项（仅可用于 Windows Update 更新），更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

默认情况下已禁用该选项。

- **该供应商的更新的安装规则**

此选项仅适用于第三方应用程序的更新。Kaspersky Security Center 仅安装与所选更新由同一供应商提供的应用程序相关的那些更新。未安装拒绝更新和其他供应商提供的应用程序更新。

默认情况下已禁用该选项。

- **类型是 的更新的安装规则**
- **所选更新的安装规则**
- **批准所选更新**

所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

默认情况下已禁用该选项。

- **自动安装所选更新安装所需的所有先前应用程序更新**

  如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

  如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

  例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

  默认情况下已启用该选项。

c. 单击“**添加**”按钮。

如果选择启动任务，则可以关闭向导。该任务将在后台模式下完成。不需要进一步操作。

如果您选择了将规则添加到现有任务，则会打开任务属性窗口。新规则已添加到任务属性中。您可以查看或修改规则或其他任务设置。单击“**保存**”按钮以保存更改。

如果选择创建任务，则继续在“新建任务向导”中创建任务。您在更新安装向导中添加的新规则将显示在新任务向导中。完成向导后，“*安装所需更新并修复漏洞*”任务将添加到任务列表中。

创建“查找漏洞和所需更新”任务

通过“查找漏洞和所需更新”任务，Kaspersky Security Center 接收检测到的漏洞列表以及受管理设备上安装的第三方软件的所需更新列表。

快速启动向导运行时，将自动创建“查找漏洞和所需更新”任务。如果未运行向导，可以手动创建该任务。

要创建“查找漏洞和所需更新”任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。遵照向导的说明。
3. 对于 Kaspersky Security Center 应用程序，选择**查找漏洞和所需更新**任务类型。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择要将任务分配到的设备。
6. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。
7. 单击“**创建**”按钮。

   任务被创建并显示在任务列表。
8. 点击创建的任务的名称以打开任务属性窗口。

9. 在任务属性窗口中，指定常规任务设置。

10. 在“**应用程序设置**”选项卡上，指定以下设置：

- **搜索 Microsoft 列出的漏洞和更新**

  当搜索漏洞和更新时，Kaspersky Security Center 使用当前可用的 Microsoft 更新源中有关适用 Microsoft 更新的信息。

  例如，如果您有带有不同 Microsoft 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **连接更新服务器更新数据**

  受管理设备上的“Windows 更新代理”连接到 Microsoft 更新源。以下服务器可以充当 Microsoft 更新源：

  - Kaspersky Security Center 管理服务器（请参阅网络代理策略的设置）
  - 在组织网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows 服务器
  - Microsoft 更新服务器

  如果启用该选项，受管理设备上的 Windows 更新代理将连接到 Microsoft 更新源以刷新适用 Microsoft Windows 更新的信息。

  如果禁用此选项，受管理设备上的 Windows 更新代理将使用以前从 Microsoft 更新源所收到的适用 Microsoft Windows 更新的信息。

  到 Microsoft 更新源的连接可能消耗资源。如果在其他任务中或网络代理策略属性中设置了到该更新源的常规连接，则您可能想要在“**软件更新和漏洞**”区域禁用此选项。如果您不想禁用此选项，则为了减少服务器过载，您可以配置任务计划以随机分配任务启动延迟（不超过 360 分钟）。

  默认情况下已启用该选项。

  网络代理策略设置的以下选项的组合定义了获取更新的方式：

  - 仅当在**查找漏洞和所需更新连接更新服务器更新数据任务的属性中**启用了*连接到更新服务器以更新数据查找漏洞和所需更新*选项，并且在网络代理策略的设置中**Windows Update 搜索模式**选项被设置为**主动**时，受管理设备上的 Windows 更新代理才会连接到更新服务器以获取更新 。
  - 如果您在执行*漏洞扫描*任务时不需要网络代理发起与 Microsoft Windows 更新源的连接并下载更新，您可以将**Windows Update 搜索模式**选项设置为**被动**，同时**连接更新服务器更新数据**选项必须保持启用。这使您可以节省资源并使用以前收到的 Windows 更新来扫描漏洞。如果您以不同的方式配置接收 Microsoft Windows 更新，则可以使用被动模式。如果没有以其他方式配置接收 Microsoft Windows 更新，请不要将**Windows Update 搜索模式**选项设置为**被动**，因为在这种情况下，将永远不会收到有关更新的信息。
  - 不管“**连接更新服务器更新数据**”选项的状态如何（启用或禁用），如果“**Windows Update 搜索模式**”选项被设置为“**已禁用**”，Kaspersky Security Center 不会请求有关更新的任何信息。

- **搜索卡巴斯基列出的第三方漏洞和更新**

  如果启用该选项，Kaspersky Security Center 在 Windows 注册表和“**指定文件系统中应用程序高级搜索的路径**”下指定的文件夹中搜索漏洞和第三方应用程序所需更新（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）。支持的第三方应用程序的完整列表由 Kaspersky 管理。

  如果禁用该选项，Kaspersky Security Center 不为第三方应用程序查找漏洞和所需更新。例如，如果您有带有不同 Microsoft Windows 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

- **指定文件系统中应用程序高级搜索的路径**

  Kaspersky Security Center 搜索需要修复漏洞和安装更新的第三方应用程序。您可以使用系统变量。

  指定应用程序安装文件夹。默认下，列表包含大多数应用程序所安装的系统文件夹。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

11. 单击“**保存**”按钮。

    任务被创建和配置。

如果任务结果包含 0x80240033 “Windows 更新代理错误 80240033（“无法下载授权许可条款。”）”错误警告，则可以通过 Windows 注册表解决此问题。

“查找漏洞和所需更新”任务设置

快速启动向导运行时，将自动创建“*查找漏洞和所需更新*”任务。如果未运行向导，可以手动创建该任务。

除了常规任务设置外，您还可以在创建“*查找漏洞和所需更新*”任务或稍后配置已创建任务的属性时指定以下设置：

- **搜索 Microsoft 列出的漏洞和更新**

  当搜索漏洞和更新时，Kaspersky Security Center 使用当前可用的 Microsoft 更新源中有关适用 Microsoft 更新的信息。

  例如，如果您有带有不同 Microsoft 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

  有关 Microsoft Windows 可选更新的信息未发送至管理服务器。

- **连接更新服务器更新数据**

  受管理设备上的“Windows 更新代理”连接到 Microsoft 更新源。以下服务器可以充当 Microsoft 更新源：

  - Kaspersky Security Center 管理服务器（请参阅网络代理策略的设置）
  - 在组织网络中部署了 Microsoft Windows Server Update Services (WSUS) 的 Windows 服务器
  - Microsoft 更新服务器

  如果启用该选项，受管理设备上的 Windows 更新代理将连接到 Microsoft 更新源以刷新适用 Microsoft Windows 更新的信息。

  如果禁用此选项，受管理设备上的 Windows 更新代理将使用以前从 Microsoft 更新源所收到的适用 Microsoft Windows 更新的信息。

  到 Microsoft 更新源的连接可能消耗资源。如果在其他任务中或网络代理策略属性中设置了到该更新源的常规连接，则您可能想要在“**软件更新和漏洞**”区域禁用此选项。如果您不想禁用此选项，则为了减少服务器过载，您可以配置任务计划以随机分配任务启动延迟（不超过 360 分钟）。

  默认情况下已启用该选项。

  网络代理策略设置的以下选项的组合定义了获取更新的方式：

  - 仅当在**查找漏洞和所需更新连接更新服务器更新数据任务的属性中**启用了*连接到更新服务器以更新数据查找漏洞和所需更新*选项，并且在网络代理策略的设置中**Windows Update 搜索模式**选项被设置为**主动**时，受管理设备上的 Windows 更新代理才会连接到更新服务器以获取更新 。
  - 如果您在执行*漏洞扫描*任务时不需要网络代理发起与 Microsoft Windows 更新源的连接并下载更新，您可以将**Windows Update 搜索模式**选项设置为**被动**，同时**连接更新服务器更新数据**选项必须保持启用。这使您可以节省资源并使用以前收到的 Windows 更新来扫描漏洞。如果您以不同的方式配置接收 Microsoft Windows 更新，则可以使用被动模式。如果没有以其他方式配置接收 Microsoft Windows 更新，请不要将**Windows Update 搜索模式**选项设置为**被动**，因为在这种情况下，将永远不会收到有关更新的信息。
  - 不管“**连接更新服务器更新数据**”选项的状态如何（启用或禁用），如果“**Windows Update 搜索模式**”选项被设置为“**已禁用**”，Kaspersky Security Center 不会请求有关更新的任何信息。

- **搜索卡巴斯基列出的第三方漏洞和更新**

  如果启用该选项，Kaspersky Security Center 在 Windows 注册表和“**指定文件系统中应用程序高级搜索的路径**”下指定的文件夹中搜索漏洞和第三方应用程序所需更新（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）。支持的第三方应用程序的完整列表由 Kaspersky 管理。

  如果禁用该选项，Kaspersky Security Center 不为第三方应用程序查找漏洞和所需更新。例如，如果您有带有不同 Microsoft Windows 更新和第三方应用程序更新设置的不同任务，您可能想要禁用该选项。

  默认情况下已启用该选项。

- **指定文件系统中应用程序高级搜索的路径**

  Kaspersky Security Center 搜索需要修复漏洞和安装更新的第三方应用程序。您可以使用系统变量。

  指定应用程序安装文件夹。默认下，列表包含大多数应用程序所安装的系统文件夹。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

关于任务计划的建议

计划“*查找漏洞和所需更新*”任务时，请确保两个选项“**运行错过的任务**”和“**使用任务启动自动随机延迟**”已启用。

默认情况下，“*查找漏洞和所需更新*”任务设置为手动启动。如果组织的工作区规则规定在此时关闭所有设备，“*查找漏洞和所需更新*”任务将在设备再次开启后运行，即，第二天早晨。此活动可能不是必须的，因为漏洞扫描可能增加 CPU 和磁盘子系统负载。您必须基于组织的工作规则为该任务设置最方便的计划。

创建“安装所需更新并修复漏洞”任务

“*安装所需更新并修复漏洞*”任务仅在漏洞和补丁管理授权许可下可用。

*安装所需更新并修复漏洞*任务用于更新和修复在受管理设备上安装的第三方软件（包括 Microsoft 软件）中的漏洞。通过此任务，您可以根据某些规则安装多个更新并修复多个漏洞。

要使用“*安装所需更新并修复漏洞*”任务安装更新或修复漏洞，可以执行以下任一操作：

- 运行更新安装向导或漏洞修复向导。
- 创建“*安装所需更新并修复漏洞*”任务。
- 向现有的“*安装所需更新并修复漏洞*”任务添加更新安装规则。

要创建“安装所需更新并修复漏洞”任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。
   “新任务向导”启动。遵照向导的说明。
3. 对于 Kaspersky Security Center 应用程序，选择**安装所需更新并修复漏洞**任务类型。
   如果未显示任务，请检查您的账户是否有对“**系统管理**：**漏洞和补丁管理**”功能区域的**读取**、**调整**和**执行**权限。如果没有这些访问权限，您不能创建和配置“*安装所需更新并修复漏洞*”任务。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择要将任务分配到的设备。
6. 指定更新安装规则，然后指定以下设置：

   - **在设备重启或关闭时开始安装**

     如果启用该选项，更新在设备被重启或关闭时安装。否则，更新根据计划安装。
     如果安装更新可能影响设备性能则使用该选项。
     默认情况下已禁用该选项。

   - **安装所需的常规系统组件**

     如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。
     如果禁用该选项，您可能必须手动安装先决条件。
     默认情况下已禁用该选项。

   - **更新过程中允许安装新应用程序版本**

     如果启用该**选项**，如果更新导致软件应用程序新版本的安装，更新将被允许。
     如果禁用该选项，软件不被升级。您可以稍后手动或通过其他任务安装软件的新版本。例如，如果公司基础架构不被新软件版本支持，或者如果您想要在测试基础架构中检查升级，您可能使用该选项。
     默认情况下已启用该选项。

     升级应用程序可能导致安装在客户端设备上的独立应用程序功能异常。

- **下载更新到设备而不安装**

  如果启用该选项，应用程序下载更新到设备但是不自动安装它们。您可以稍后手动安装下载的更新。

  Microsoft 更新被下载到系统 Windows 存储。第三方应用程序更新（由非 Kaspersky 和 Microsoft 软件供应商开发的应用程序）将会下载到“**下载更新到**”字段中指定的文件夹中。

  如果禁用该选项，更新被自动安装到设备。

  默认情况下已禁用该选项。

- **下载更新到**

  该文件夹用于下载第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

7. 指定操作系统重新启动设置：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。
  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。
  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。
  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **在该时间后强制关闭阻止会话中的应用程序(分钟)**

  用户设备锁定时，程序以强制模式关闭（指定不活动间隔之后自动锁定，或手动锁定）。
  如果启用此选项，当输入字段中指定的时间间隔结束后，锁定设备上的应用程序将被强制关闭。
  如果禁用此选项，应用程序在锁定的设备上不关闭。
  默认情况下已禁用该选项。

8. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

9. 单击“**完成**”按钮。
   任务被创建并显示在任务列表。

10. 点击创建的任务的名称以打开任务属性窗口。

11. 在任务属性窗口中，根据需要指定常规任务设置。

12. 单击“**保存**”按钮。
    任务被创建和配置。

如果任务结果包含 0x80240033 “Windows 更新代理错误 80240033（“无法下载授权许可条款。”）”错误警告，则可以通过 Windows 注册表解决此问题。

添加更新安装规则

此功能仅在“漏洞和补丁管理”授权许可下可用。

使用“*安装所需更新并修复漏洞*”任务安装软件更新或修复软件漏洞时，您必须指定更新安装规则。这些规则决定要安装的更新和要修复的漏洞。

精确设置取决于您是否添加了所有更新、Windows Update 更新、第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新的规则。当添加 Windows Update 更新或第三方应用程序更新的规则时，您可以选择特定的应用程序和您要安装更新的应用程序版本。当添加所有更新的规则时，您可以选择您要安装的特定更新和您要通过安装更新进行修复的漏洞。

您可以通过以下方式添加更新安装规则：

- 通过在创建新“安装所需更新并修复漏洞”任务时添加规则。
- 通过在现有的“*安装所需更新并修复漏洞*”任务的属性窗口的**应用程序设置**选项卡中添加规则。
- 通过更新安装向导或漏洞修复向导。

要添加所有更新的规则：

1. 单击“**添加**”按钮。
   规则创建向导开始。使用**下一步**按钮进行向导。
2. 在“**规则类型**”页面，选择“**所有更新的规则**”。
3. 在**常规标准**页面，使用下拉列表指定以下设置：
   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：
     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。
   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。
4. 在**更新**页面，选择要安装的更新：
   - **安装所有适用的更新**

     安装符合向导“**常规标准**”页面上指定条件的所有软件更新。默认选择。
   - **仅安装列表中的更新**

     仅安装您从列表中手动选择的软件更新。该列表包含所有可用软件更新。

例如，您可能想要在以下情况下选择特定更新：要在测试环境中检查它们的安装、要仅更新严重应用程序、或者要仅更新特定应用程序。

- **自动安装所选更新安装所需的所有先前应用程序更新**

  如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

  如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

  例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

  默认情况下已启用该选项。

5. 在**漏洞**页面，选择将由安装所选更新修复的漏洞：

   - **修复所有匹配其他标准的漏洞**

     修复符合向导“**常规标准**”页面上指定条件的所有漏洞。默认选择。

   - **仅修复列表中的漏洞**

     仅修复您手动从列表中选择的漏洞。列表包含所有检测到的漏洞。

     例如，您可能想要在以下情况下选择特定漏洞：要在测试环境中检查它们的修复、要仅修复严重应用程序中的漏洞、或者要仅修复特定应用程序中的漏洞。

6. 在“**名称**”页面，指定您正在添加的规则的名称。您可以稍后在所创建任务的属性窗口的“**设置**”区域更改该名称。

规则创建向导完成操作后，新规则将添加，并显示在新任务向导或任务属性的规则列表中。

要添加 Windows Update 更新的新规则：

1. 单击“**添加**”按钮。

   规则创建向导开始。使用**下一步**按钮进行向导。

2. 在“**规则类型**”页面上，选择“**Windows 更新的规则**”。

3. 在**常规标准**页面，指定以下设置：

   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：

     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

- **修复严重级别等于或大于该项的漏洞**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

- **修复 MSRC 严重级别等于或大于该项的漏洞**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项，更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

4. 在**应用程序**页面，选择您要安装更新的应用程序和应用程序版本。默认情况下选定所有应用程序。
5. 在**更新类别**页面，选择要安装的更新类别。这些类别与 Microsoft Update Catalog 中的类别相同。默认情况下选定所有类别。
6. 在“**名称**”页面，指定您正在添加的规则的名称。您可以稍后在所创建任务的属性窗口的“**设置**”区域更改该名称。

规则创建向导完成操作后，新规则将添加，并显示在新任务向导或任务属性的规则列表中。

要添加第三方应用程序更新的新规则：

1. 单击“**添加**”按钮。

   规则创建向导开始。使用**下一步**按钮进行向导。
2. 在“**规则类型**”页面，选择“**第三方更新的规则**”。
3. 在**常规标准**页面，指定以下设置：

- **要安装的更新集**

  选择必须在客户端设备上安装的更新：

  - **仅安装批准的更新**。这仅安装批准的更新。
  - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
  - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

- **修复严重级别等于或大于该项的漏洞**

  有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

  如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

  如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

  默认情况下已禁用该选项。

4. 在**应用程序**页面，选择您要安装更新的应用程序和应用程序版本。默认情况下选定所有应用程序。

5. 在“**名称**”页面，指定您正在添加的规则的名称。您可以稍后在所创建任务的属性窗口的“设置”区域更改该名称。

规则创建向导完成操作后，新规则将添加，并显示在新任务向导或任务属性的规则列表中。

创建“安装 Windows Update 更新”任务

通过“*安装 Windows Update 更新*”任务可以在受管理设备上安装 Windows Update 服务提供的软件更新。

如果您没有漏洞和补丁管理授权许可，则无法创建“*安装 Windows Update 更新*”类型的新任务。要安装新更新，您可以将其添加到现有的“*安装 Windows Update 更新*”任务中。我们建议您使用“*安装所需更新并修复漏洞*”任务而不是“*安装 Windows Update 更新*”任务。“*安装所需更新并修复漏洞*”任务让您能够根据您定义的规则自动安装多个更新和修复多个漏洞。此外，此任务让您可以安装 Microsoft 以外的软件供应商的更新。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

要创建“安装 Windows Update 更新”任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。

2. 单击**添加**。

   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。

3. 对于 Kaspersky Security Center 应用程序，选择“**安装 Windows Update 更新**”任务类型。

4. 指定您正创建的任务的名称。

   任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

5. 选择要将任务分配到的设备。

6. 单击“**添加**”按钮。

   更新列表打开。

7. 选择要安装的 Windows Update 更新，然后单击“**确定**”。

8. 指定操作系统重新启动设置：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。

  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1440 分钟之间。

  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

9. 指定账户设置：

- **默认账户**

  在与执行该任务的应用程序相同的账户下运行该任务。

默认情况下已选定该选项。

- **指定账户**

  填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

- **账户**

  运行该任务的账户。

- **密码**

  任务运行时使用的账户的密码。

10. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

11. 单击“**完成**”按钮。

    任务被创建并显示在任务列表。

12. 点击创建的任务的名称以打开任务属性窗口。

13. 在任务属性窗口中，根据需要指定常规任务设置。

14. 单击“**保存**”按钮。

任务被创建和配置。

查看有关可用的第三方软件更新的信息

您可以查看客户端设备上安装的第三方软件（包括 Microsoft 软件）的可用更新列表。

要查看客户端设备上安装的第三方应用程序的可用更新列表，

在主菜单中，转到**操作 → 补丁管理 → 软件更新**。

可用更新列表被显示。

您可以指定一个过滤器以查看软件更新列表。单击软件更新列表右上角的“**过滤器**”图标 ( ) 以管理过滤器。您也可以从软件漏洞列表上方的“**预设过滤器**”下拉列表中选择一个预设过滤器。

要查看更新的属性：

1. 单击所需软件更新的名称。
2. 更新的属性窗口将打开，其中显示分组到以下选项卡上的信息：

- **常规**

  此选项卡显示所选更新的常规详细信息：

  - 更新批准状态（可以通过在下拉列表中选择新状态来手动更改）
  - 更新所属的 Windows Server Update Services (WSUS) 类别
  - 更新的注册日期和时间
  - 更新的创建日期和时间
  - 更新的重要级别
  - 更新限制的安装要求
  - 更新所属的应用程序系列
  - 更新适用的应用程序
  - 更新修订号

- **属性**

  此选项卡显示一组属性，这些属性可用于获取有关所选更新的更多信息。根据更新由 Microsoft 发布还是由第三方供应商发布，该属性组会有所不同。

  该选项卡显示 Microsoft 更新的以下信息：

  - 根据 Microsoft 安全响应中心 (MSRC) 定义的更新重要级别
  - 描述该更新的 Microsoft 知识库文章链接
  - 描述该更新的 Microsoft 安全公告文章链接
  - 更新标识符 (ID)

  该选项卡显示第三方更新的以下信息：

  - 更新是补丁还是完整分发包
  - 更新的本地化语言
  - 更新是自动安装还是手动安装
  - 应用更新后是否撤销更新
  - 更新的下载链接

- **设备**

  此选项卡显示已安装所选更新的设备列表。

- **已修复漏洞**

  此选项卡显示所选更新可以修复的漏洞列表。

- **更新融合**

  此选项卡显示为同一应用程序发布的各种更新之间的可能交叉，即，所选更新是否可以取代其他更新，或者反过来被其他更新取代（仅适用于 Microsoft 更新）。

- **安装该更新的任务**

  此选项卡显示一个任务列表，这些任务的范围包括安装所选更新。该选项卡还允许为更新创建新的远程安装任务。

要查看更新安装的统计信息：

1. 选中所需软件更新旁边的复选框。
2. 单击**更新安装状态统计信息**按钮。

   将显示更新安装状态图。单击某个状态将打开其上的更新具有所选状态的设备列表。

您可以查看所选的运行 Windows 的受管理设备上安装的第三方软件（包括 Microsoft 软件）的可用软件更新的信息。

要查看所选受管理设备上安装的第三方软件的可用更新列表：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
   将显示受管理设备列表。
2. 在受管理设备列表中，单击含有要查看其第三方软件更新的设备的名称的链接。
   将显示所选设备的属性窗口。
3. 在所选设备的属性窗口中，选择“**高级**”选项卡。
4. 在左侧窗格中，选择“**可用更新**”区域。如果只想查看已安装的更新，请启用“**显示已安装的更新**”选项。

   将显示所选设备的可用第三方软件更新列表。

将可用软件更新列表导出到文件

您可以在显示第三方软件（包括 Microsoft 软件）的更新列表时将其导出到 CSV 或 TXT 文件。例如，您可以将这些文件发送给信息安全经理或出于统计目的存储它们。

要将所有受管理设备上安装的第三方软件的可用更新列表导出到文本文件：

1. 在主菜单中，转到“**操作**”→“**补丁管理**”→“**软件更新**”。
   该页面显示所有受管理设备上安装的第三方软件的可用更新列表。
2. 单击“**导出到 TXT**”或“**导出到 CSV**”按钮，具体取决于所需导出格式。

包含第三方软件（包括 Microsoft 软件）可用更新列表的文件将下载到您当时使用的设备上。

要将选定受管理设备上安装的第三方软件的可用更新列表导出到文本文件：

1. 打开选定受管理设备上的可用第三方软件更新列表。
2. 选择要导出的软件更新。
   如果要导出完整的软件更新列表，请跳过此步骤。
   如果要导出完整的软件更新列表，则仅导出当前页面上显示的更新。
   如果要只导出已安装的更新，请选中“**显示已安装的更新**”复选框。
3. 单击“**导出到 TXT**”或“**导出到 CSV**”按钮，具体取决于所需导出格式。

包含选定受管理设备上安装的第三方软件（包括 Microsoft 软件）的更新列表的文件将下载到您当时正在使用的设备上。

批准和拒绝第三方软件更新

配置“*安装所需更新并修复漏洞*”任务时，可以创建一条规则，要求待安装的更新处于特定状态。例如，更新规则可以允许安装以下更新：

- 仅限已批准的更新
- 仅限已批准和未定义的更新
- 所有更新，无论更新状态如何

您可以批准必须安装的更新并拒绝不能安装的更新。

使用“*已批准*”状态管理更新安装对于少量更新来说非常有效。要安装多个更新，请使用可以在“*安装所需更新并修复漏洞*”任务中配置的规则。我们建议仅为那些不符合规则中指定的条件的特定更新设置“*已批准*”状态。当手动批准大量更新时，管理服务器的性能会下降，这可能导致服务器过载。

要批准或拒绝一个或几个更新：

1. 在主菜单中，转到“**操作**”→“**补丁管理**”→“**软件更新**”。
   可用更新列表被显示。
2. 选择您要批准或拒绝的更新。
3. 单击“**批准**”批准所选更新或单击“**拒绝**”拒绝所选更新。
   默认值是 *未定义*。

所选更新具有您定义的状态。

作为一个选项，您可以在特定更新的属性中更改批准状态。

要在其属性中批准或拒绝更新：

1. 在主菜单中，转到**操作 → 补丁管理 → 软件更新**。
   可用更新列表被显示。
2. 单击要批准或拒绝的更新的名称。
   更新属性窗口打开。
3. 在“**常规**”区域中，通过更改“**更新批准状态**”选项来选择更新状态。您可以选择“*已批准*”、“*已拒绝*”或“*未定义*”状态。
4. 单击“**保存**”按钮以保存更改。

所选更新具有您定义的状态。

如果您为第三方软件更新设置了**已拒绝**状态，这些更新将不会安装在计划将其安装但并未将其安装的设备上。更新将保持在已将其安装的设备上。如果您必须删除它们，您可以在本地手动删除它们。

创建“执行 Windows Update 同步”任务

*执行 Windows 更新同步*任务仅在漏洞和补丁管理授权许可下可用。

如果要将管理服务器用作 WSUS 服务器，则需要“*执行 Windows 更新同步*”任务。在这种情况下，管理服务器将 Windows Update 下载到数据库，并通过网络代理以集中模式在客户端设备上向 Windows Update 提供更新。如果网络不使用 WSUS 服务器，例如每个客户端设备都从外部服务器独立下载 Microsoft 更新。

“*执行 Windows 更新同步*”任务仅从 Microsoft 服务器下载元数据。当您运行更新安装任务时，Kaspersky Security Center 会下载更新，并且仅下载您选择安装的那些更新。

当运行“**执行 Windows 更新同步**”任务时，应用程序从 Microsoft 更新服务器接收当前更新列表。下一步，Kaspersky Security Center 编辑过期更新列表。在下次启动“**查找漏洞和所需更新**”任务时，Kaspersky Security Center 会标记所有过时的更新，并为其设置删除时间。在下次启动“**执行 Windows 更新同步**”任务时，将删除标记为 30 天之前删除的所有更新。Kaspersky Security Center 也检查删除了 180 天以上的过期更新，并删除更早的更新。

当“**执行 Windows 更新同步**”任务完成且过时更新被删除时，数据库可能仍保留被删除的更新的哈希码和对应文件到 %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 文件（如果之前已下载）。您可以运行“**管理服务器维护**”任务以从数据库和对应文件中删除这些过期的记录。

要创建“执行 Windows 更新同步”任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。
   “新任务向导”启动。遵照向导的说明。
3. 对于 Kaspersky Security Center 应用程序，选择“**执行 Windows 更新同步**”任务类型。

4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。

5. 如果要在运行任务时下载快速更新文件，请启用“**下载快速安装文件**”选项。

   在 Kaspersky Security Center 与 Microsoft Windows Update Servers 同步更新时，所有文件的信息被保存在管理服务器数据库。所有更新所需的文件也在与 Windows 更新代理的交互过程中被下载到驱动器。特别地，Kaspersky Security Center 保存快速更新文件的信息到数据库并在必要时下载它们。下载快速更新文件导致驱动器空间的减少。

   为了避免磁盘空间减少以及流量降低，请禁用“**下载快速安装文件**”选项。

6. 选择您要为其下载更新的应用程序。

   如果选中“**所有应用程序**”复选框，更新将为所有现有应用程序以及可能在将来发布的应用程序下载。

7. 选择要下载到管理服务器的更新类别。

   如果选中“**所有类别**”复选框，更新将为所有现有更新类别以及可能在将来出现的类别下载。

8. 选择要下载到管理服务器的更新的本地化语言。您可以选择以下选项之一：

   - **下载包括新语言在内的所有语言**

     如果选定了该选框，所有可用的更新本地化语言都将被下载至管理服务器。默认情况下已选定该选项。

   - **下载选定语言**

     如果选定了该选框，您可以从更新的本地化语言列表中进行选择以便下载到管理服务器中。

9. 指定运行任务时要使用的账户。您可以选择以下选项之一：

   - **默认账户**

     在与执行该任务的应用程序相同的账户下运行该任务。

     默认情况下已选定该选项。

   - **指定账户**

     填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

10. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

11. 单击“**完成**”按钮。

    任务被创建并显示在任务列表。

12. 点击创建的任务的名称以打开任务属性窗口。

13. 在任务属性窗口中，根据需要指定常规任务设置。

14. 单击“**保存**”按钮。

任务被创建和配置。

自动更新第三方应用程序

某些第三方应用程序可以自动更新。应用程序供应商定义应用程序是否支持自动更新功能。如果受管理设备上安装的第三方应用程序支持自动更新，则可以在应用程序属性中指定自动更新设置。更改自动更新设置后，网络代理会将新设置应用于安装了该应用程序的每个受管理设备。

自动更新设置独立于"漏洞和补丁管理"功能的其他对象和设置。例如，此设置不取决于更新批准状态或更新安装任务，如"*安装所需更新并修复漏洞*"、"*安装 Windows Update 更新*"和"*修复漏洞*"。

要为第三方应用程序配置自动更新设置：

1. 在主菜单中，转到"**操作**"→"**第三方应用程序**"→"**应用程序注册表**"。
2. 单击要为其更改自动更新设置的应用程序的名称。

   为简化搜索，您可以通过"**自动更新状态**"列筛选列表。

   应用程序属性窗口打开。
3. 在"**常规**"区域中，为以下设置选择一个值：

   自动更新状态

   您可以选择以下选项之一：

   - **未定义**

     自动更新功能已禁用。Kaspersky Security Center 使用以下任务来安装第三方应用程序更新："*安装所需更新并修复漏洞*"、"*安装 Windows Update 更新*"和"*修复漏洞*"。
   - **允许**

     供应商发布应用程序更新后，此更新将自动安装在受管理设备上。不需要其他操作。
   - **已阻止**

     应用程序更新不会自动安装。Kaspersky Security Center 使用以下任务来安装第三方应用程序更新："*安装所需更新并修复漏洞*"、"*安装 Windows Update 更新*"和"*修复漏洞*"。
4. 单击"**保存**"按钮以保存更改。

自动更新设置将应用于所选应用程序。

修复第三方软件漏洞

本部分描述了 Kaspersky Security Center 的功能，这些功能与修复受管理设备上所安装软件中的漏洞有关。

方案：查找和修复第三方软件中的漏洞

该部分提供了在运行 Windows 的受管理设备上查找和修复漏洞的方案。您可以在操作系统和第三方软件（包括 Microsoft 软件）中查找和修复软件漏洞。

先决条件

- Kaspersky Security Center 已部署在您的组织中。
- 您的组织中存在运行 Windows 系统的受管理设备。
- 管理服务器需要互联网连接才能执行以下任务：
  - 针对 Microsoft 软件漏洞生成推荐的修复程序列表。该列表由 Kaspersky 专家创建并定期更新。
  - 修复除 Microsoft 软件以外的第三方软件的漏洞。

阶段

查找和修复软件漏洞的过程分为以下几个阶段：

1. **扫描受管理设备上安装的软件中的漏洞**

   要查找受管理设备上安装的软件中的漏洞，请运行“*查找漏洞和所需更新*”任务。完成此任务后，Kaspersky Security Center 会收到检测到的漏洞列表，以及在任务属性中指定的设备上安装的第三方软件的所需更新。

   “*查找漏洞和所需更新*”任务由 Kaspersky Security Center 快速启动向导自动创建。如果您未运行向导，请立即启动它或手动创建任务。

   说明：

   - 管理控制台：扫描应用程序中的漏洞，安排“查找漏洞和所需更新”任务
   - Kaspersky Security Center Web Console：创建“查找漏洞和所需更新”任务，“查找漏洞和所需更新”任务设置

2. **分析检测到的软件漏洞列表**

   查看“**软件漏洞**”列表，并确定要修复的漏洞。要查看有关每个漏洞的详细信息，请单击列表中的漏洞名称。对于列表中的每个漏洞，您还可以查看受管理设备上关于该漏洞的统计信息。

   说明：

   - 管理控制台：查看有关软件漏洞的信息，查看受管理设备上漏洞的统计信息
   - Kaspersky Security Center Web Console：查看软件漏洞信息，查看受管理设备上漏洞的统计信息

3. **配置漏洞修复**

   检测到软件漏洞后，可以使用“*安装所需更新并修复漏洞*”任务或“*修复漏洞*”任务来修复受管理设备上的软件漏洞。

   安装所需更新并修复漏洞 任务用于更新和修复在受管理设备上安装的第三方软件（包括 Microsoft 软件）中的漏洞。通过此任务，您可以根据某些规则安装多个更新并修复多个漏洞。请注意，仅当您具有漏洞和补丁管理功能的授权许可时，才能创建此任务。为修复软件漏洞，*安装所需更新并修复漏洞* 任务将使用建议的软件更新。

*修复漏洞*任务不需要"漏洞和补丁管理"功能的授权许可选项。要使用此任务，必须手动为任务设置中列出的第三方软件中的漏洞指定用户修补程序。"*修复漏洞*"任务使用针对 Microsoft 软件的建议修补程序和针对第三方软件的用户修补程序。

您可以启动漏洞修复向导来自动创建这些任务之一，也可以手动创建这些任务之一。

说明：

- 管理控制台：为第三方软件中的漏洞选择用户修补程序，修复应用程序中的漏洞
- Kaspersky Security Center Web Console：为第三方软件中的漏洞选择用户修补程序，修复第三方软件中的漏洞，创建"安装所需更新并修复漏洞"任务

4 安排任务

为确保漏洞列表始终是最新的，请安排"*查找漏洞和所需更新*"任务以不时自动运行它。建议的平均运行频率是每周一次。

如果您创建了"*安装所需更新并修复漏洞*"任务，则可以安排其与"*查找漏洞和所需更新*"任务相同或更少的频率运行。计划"*修复漏洞*"任务时，请注意，每次启动任务之前，都必须选择 Microsoft 软件的修补程序或为第三方软件指定用户修补程序。

安排任务时，请确保在完成"*查找漏洞和所需更新*"任务之后，开始修复漏洞的任务。

5 忽略软件漏洞（可选）

如果需要，可以忽略在所有受管理设备上或仅在选定受管理设备上要修复的软件漏洞。

说明：

- 管理控制台：忽略软件漏洞
- Kaspersky Security Center Web Console：忽略软件漏洞

6 运行漏洞修复任务

启动*安装所需更新并修复漏洞*任务或*修复漏洞*任务。任务完成后，请确保它在任务列表中具有*已成功完成*状态。

7 创建有关修复软件漏洞的结果报告（可选）

要查看有关已修复漏洞的详细统计信息，请生成漏洞报告。该报告显示有关未修复软件漏洞的信息。因此，您可以了解如何对组织中第三方软件（包括 Microsoft 软件）的漏洞进行查找和修复。

说明：

- 管理控制台：创建和查看报告
- Kaspersky Security Center Web Console：生成和查看报告

8 检查关于查找和修复第三方软件中漏洞的配置

确保已完成以下操作：

- 获取并查看了受管理设备上的软件漏洞列表
- 如果需要，可以忽略软件漏洞
- 配置任务以修复漏洞
- 安排任务以查找和修复软件漏洞，以便任务依次启动
- 检查是否已运行修复软件漏洞任务

结果

如果已创建并配置了"*安装所需更新并修复漏洞*"任务，则这些漏洞将自动在受管理设备上修复。运行任务时，它将可用软件更新列表与任务设置中指定的规则相关联。满足规则条件的所有软件更新都将下载到管理服务器存储库中，并将进行安装以修复软件漏洞。

如果创建了"*修复漏洞*"任务，则仅修复 Microsoft 软件中的软件漏洞。

关于查找和修复软件漏洞

Kaspersky Security Center 可检测并修复运行 Microsoft Windows 系列操作系统的受管理设备上的软件漏洞。将在操作系统和第三方软件（包括 Microsoft 软件）中检测漏洞。

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）以及 KSN 功能。

查找软件漏洞

为了查找软件漏洞，Kaspersky Security Center 使用已知漏洞数据库的特征。该数据库由 Kaspersky 专家创建。它包含有关漏洞的信息，例如漏洞描述、漏洞检测日期、漏洞严重级别。您可以在卡巴斯基网站查找软件漏洞详情。

Kaspersky Security Center 使用*查找漏洞和所需更新*任务来查找软件漏洞。

在某些情况下，可以使用以下任一方法修复 Microsoft Windows 操作系统中检测到的漏洞：

- 安装操作系统更新。
- 将操作系统升级到较新的版本（例如，从 Windows 10 到 Windows 11）。

在这种情况下，Kaspersky Security Center 会针对同一漏洞显示两个条目。

修复软件漏洞

为修复软件漏洞，Kaspersky Security Center 使用软件供应商发布的软件更新。由于执行以下任务，软件更新元数据会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*。该任务旨在下载 Kaspersky 和第三方软件的更新元数据。该任务由 Kaspersky Security Center 快速启动向导自动创建。您可以手动创建"将更新下载至管理服务器存储库"任务。
- *执行 Windows 更新同步*。该任务旨在下载 Microsoft 软件的更新元数据。

修复漏洞的软件更新可以是完整的分发包，也可以是补丁。修复软件漏洞的软件更新称为*修补程序*。*推荐的修补程序*是 Kaspersky 专家建议安装的修补程序。*用户修补程序*是用户手动指定安装的修补程序。要安装用户修补程序，您必须创建一个包含此修补程序的安装包。

如果您具有带有漏洞和补丁管理功能的 Kaspersky Security Center 授权许可，若要修复软件漏洞，可以使用"*安装所需更新并修复漏洞*"任务。该任务会通过安装建议的修补程序自动修复多个漏洞。对于此任务，您可以手动配置某些规则来修复多个漏洞。

如果您没有具有漏洞和补丁管理功能的 Kaspersky Security Center 授权许可，若要修复软件漏洞，可以使用“*修复漏洞*”任务。借助此任务，您可以通过安装针对 Microsoft 软件的推荐修补程序和针对其他第三方软件的用户修补程序来修复漏洞。

出于安全原因，卡巴斯基技术会自动扫描您使用漏洞和补丁管理功能安装的任何第三方软件更新，以查找恶意软件。这些技术用于自动文件检查，包括病毒扫描、静态分析、动态分析、沙盒环境中的行为分析和机器学习。

卡巴斯基专家不会对可以使用漏洞和补丁管理功能安装的第三方软件更新进行手动分析。此外，卡巴斯基专家不会在此类更新中搜索漏洞（已知或未知）或未记录的功能，也不会对上面段落中指定的更新以外的更新进行其他类型的分析。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

要修复某些软件漏洞，如果请求接受最终用户授权许可协议 (EULA)，则必须接受 EULA 才能安装软件。如果您拒绝 EULA，则该软件漏洞不会得到修复。

修复第三方软件漏洞

获取软件漏洞列表后，可以修复运行 Windows 的受管理设备上的软件漏洞。您可以通过创建并运行“*修复漏洞*”任务或“*安装所需更新并修复漏洞*”任务来修复操作系统和第三方软件（包括 Microsoft 软件）中的软件漏洞。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

作为一种选择，您可以通过以下方式创建任务来修复软件漏洞：

- 通过打开漏洞列表并指定要修复的漏洞。

  结果，创建了修复软件漏洞的新任务。作为一个选项，您可以将选定漏洞添加到现有任务。

- 通过运行漏洞修复向导。

  漏洞修复向导仅在“漏洞和补丁管理”授权许可下可用。

  该向导简化了漏洞修复任务的创建和配置，并允许您消除包含相同更新要安装的冗余任务的创建。

使用漏洞列表修复软件漏洞

要修复软件漏洞：

1. 打开漏洞列表之一：

   - 要打开常规漏洞列表，请在主菜单中转到**操作 → 补丁管理 → 软件漏洞**。
   - 要打开受管理设备的漏洞列表，请在主菜单中转到“**资产(设备)**”→“**受管理设备**”→ <设备名称> →“**高级**”→“**软件漏洞**”。
   - 要打开特定应用程序的漏洞列表，请在主菜单中转到**操作 → 第三方应用程序 → 应用程序注册表 →** <application name> **→ 漏洞**。

   将显示一个页面，其中包含第三方软件中的漏洞列表。

2. 在列表中选择一个或多个漏洞，然后单击“**修复漏洞**”按钮。

   如果缺少用于修复所选漏洞之一的推荐软件更新，将显示一条信息消息。

   要修复某些软件漏洞，如果请求接受最终用户授权许可协议 (EULA)，则必须接受 EULA 才能安装软件。如果您拒绝 EULA，则该软件漏洞不会得到修复。

3. 您可以选择以下选项之一：

   - **新任务**

     新任务向导启动。如果您拥有漏洞和补丁管理授权许可，则会预先选择“*安装所需更新并修复漏洞*”任务。如果您没有授权许可，则会预先选择“*修复漏洞*”任务。按照向导的步骤完成任务创建。

   - **修复漏洞(添加规则到指定任务)**

     选择要向其中添加选定漏洞的任务。如果您拥有漏洞和补丁管理授权许可，请选择“*安装所需更新并修复漏洞*”任务。修复选定漏洞的新规则将自动添加到选定任务中。如果您没有授权许可，请选择“*修复漏洞*”任务。选定漏洞将添加到任务属性中。

     任务属性窗口打开。单击“**保存**”按钮以保存更改。

   如果您选择了创建任务，则会创建任务并将其显示在“**资产(设备)**”→“**任务**”处的任务列表中。如果您选择了将漏洞添加到现有任务中，漏洞将保存在任务属性中。

要修复第三方软件漏洞，请启动“*安装所需更新并修复漏洞*”任务或“*修复漏洞*”任务。如果您已创建“*修复漏洞*”任务，您必须手动指定软件更新才能修复任务设置中列出的软件漏洞。

使用漏洞修复向导修复软件漏洞

漏洞修复向导仅在“漏洞和补丁管理”授权许可下可用。

要使用漏洞修复向导来修复软件漏洞：

1. 在主菜单中，转到**操作→补丁管理→软件漏洞**。

   将显示一个页面，其中列出了受管理设备上安装的第三方软件中的漏洞。

2. 选中要修复的漏洞旁边的复选框。

3. 单击**运行漏洞修复向导**按钮。

   漏洞修复向导启动。“**选择漏洞修复任务**”页面显示以下类型的所有现有任务的列表：

   - *安装所需更新并修复漏洞*
   - *安装 Windows Update 更新*
   - *修复漏洞*

   您不能修改最后两种类型的任务来安装新更新。要安装新更新，您只能使用“*安装所需更新并修复漏洞*”任务。

4. 如果您希望向导仅显示那些修复所选漏洞的任务，请启用“**仅显示修复该漏洞的任务**”选项。

5. 选择您要执行的操作：

   - 要启动任务，请选中任务名称旁边的复选框，然后单击“**开始**”按钮。
   - 要将新规则添加到现有任务：

     a. 选中任务名称旁边的复选框，然后单击“**添加规则**”按钮。

     b. 在打开的页面上，配置新规则：

     - **修复该严重级别的漏洞的规则**

       有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

       如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

       如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

       默认情况下已禁用该选项。

     - **通过与所选漏洞的建议定义的更新类型相同的更新来修复漏洞的规则**（仅适用于 Microsoft 软件漏洞）
     - **修复所选供应商的应用程序中的漏洞的规则**（仅适用于第三方软件漏洞）
     - **修复所选应用程序的所有版本中的漏洞的规则**（仅适用于第三方软件漏洞）
     - **修复所选漏洞的规则**
     - **批准修复该漏洞的更新**

       所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

       默认情况下已禁用该选项。

     c. 单击“**添加**”按钮。

- 要创建任务：

  a. 单击“**新任务**”按钮。

  b. 在打开的页面上，配置新规则：

  - **修复该严重级别的漏洞的规则**

    有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

    如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于所选更新的严重性级别（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

    如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

    默认情况下已禁用该选项。

  - **通过与所选漏洞的建议定义的更新类型相同的更新来修复漏洞的规则**（仅适用于 Microsoft 软件漏洞）
  - **修复所选供应商的应用程序中的漏洞的规则**（仅适用于第三方软件漏洞）
  - **修复所选应用程序的所有版本中的漏洞的规则**（仅适用于第三方软件漏洞）
  - **修复所选漏洞的规则**
  - **批准修复该漏洞的更新**

    所选更新将被批准安装。如果一些应用的更新安装规则仅允许安装批准的更新，启用该选项。

    默认情况下已禁用该选项。

  c. 单击“**添加**”按钮。

如果选择启动任务，则可以关闭向导。该任务将在后台模式下完成。不需要进一步操作。

如果您选择了将规则添加到现有任务，则会打开任务属性窗口。新规则已添加到任务属性中。您可以查看或修改规则或其他任务设置。单击“**保存**”按钮以保存更改。

如果选择创建任务，则继续在“新建任务向导”中创建任务。您在漏洞修复向导中添加的新规则将显示在新任务向导中。完成向导后，“*安装必需的更新和修复漏洞*”任务将添加到任务列表中。

创建“修复漏洞”任务

*修复漏洞*任务允许您修复运行 Windows 的受管理设备上的软件漏洞。您可以修复第三方软件（包括 Microsoft 软件）中的软件漏洞。

如果您没有“漏洞和补丁管理”授权许可，则无法创建“*修复漏洞*”类型的新任务。要修复新漏洞，您可以将其添加到现有的*修复漏洞*任务中。我们建议您使用“*安装所需更新并修复漏洞*”任务而不是“*修复漏洞*”任务。“*安装所需更新并修复漏洞*”任务让您能够根据您定义的规则自动安装多个更新和修复多个漏洞。

在受管理设备上更新第三方应用程序或修复第三方应用程序中的漏洞时，可能需要用户交互。例如，如果第三方应用程序当前处于打开状态，则用户可能会被提示将其关闭。

要创建“修复漏洞”任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。使用**下一步**按钮进行向导。
3. 对于 Kaspersky Security Center 应用程序，选择“**修复漏洞**”任务类型。
4. 指定您正创建的任务的名称。

   任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择要将任务分配到的设备。
6. 单击“**添加**”按钮。

   漏洞列表打开。
7. 选择要修复的漏洞，然后单击“**确定**”。

   Microsoft 软件漏洞通常具有建议的修复程序。无需其他操作。对于其他供应商的软件中的漏洞，您首先需要为要修复的每个漏洞指定用户修复程序。然后，您将能够将这些漏洞添加到*修复漏洞*任务。
8. 指定操作系统重新启动设置：

   - **不重启设备**

     客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

   - **重启设备**

     如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

   - **提示用户操作**

     客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

     默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。

  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **强行关闭锁定会话中的应用程序**

  运行应用程序可能会阻止客户端设备重启。例如，如果文档在文档处理应用程序中被编辑且未被保存，则应用程序不允许设备重启。

  如果启用该选项，锁定设备上的此类应用程序在设备重启前被强制关闭。结果，用户可能丢失他们未保存的更改。

  如果禁用该选项，锁定设备不被重启。该设备上的任务状态显示设备需要重启。用户必须手动关闭所有运行在锁定设备上的应用程序并重启这些设备。

  默认情况下已禁用该选项。

9. 指定账户设置：

   - **默认账户**

     在与执行该任务的应用程序相同的账户下运行该任务。

     默认情况下已选定该选项。

   - **指定账户**

     填写“**账户**”和“**密码**”字段以指定用于运行任务的账户的详细信息。该账户必须具有足够的权限才能执行此任务。

   - **账户**

     运行该任务的账户。

   - **密码**

     任务运行时使用的账户的密码。

10. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

11. 单击“**完成**”按钮。

    任务被创建并显示在任务列表。

12. 点击创建的任务的名称以打开任务属性窗口。

13. 在任务属性窗口中，根据需要指定常规任务设置。

14. 单击“**保存**”按钮。

任务被创建和配置。

创建“安装所需更新并修复漏洞”任务

“*安装所需更新并修复漏洞*”任务仅在漏洞和补丁管理授权许可下可用。

*安装所需更新并修复漏洞*任务用于更新和修复在受管理设备上安装的第三方软件（包括 Microsoft 软件）中的漏洞。通过此任务，您可以根据某些规则安装多个更新并修复多个漏洞。

要使用“*安装所需更新并修复漏洞*”任务安装更新或修复漏洞，可以执行以下任一操作：

- 运行更新安装向导或漏洞修复向导。
- 创建“*安装所需更新并修复漏洞*”任务。
- 向现有的“*安装所需更新并修复漏洞*”任务添加更新安装规则。

要创建“安装所需更新并修复漏洞”任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。
   “新任务向导”启动。遵照向导的说明。
3. 对于 Kaspersky Security Center 应用程序，选择**安装所需更新并修复漏洞**任务类型。
   如果未显示任务，请检查您的账户是否有对“**系统管理**：**漏洞和补丁管理**”功能区域的**读取**、**调整**和**执行**权限。如果没有这些访问权限，您不能创建和配置“*安装所需更新并修复漏洞*”任务。
4. 指定您正创建的任务的名称。任务名称不能包含多于 100 个字符并且不能包括任何特殊字符（*<>-_?:\"|）。
5. 选择要将任务分配到的设备。
6. 指定更新安装规则，然后指定以下设置：

   - **在设备重启或关闭时开始安装**

     如果启用该选项，更新在设备被重启或关闭时安装。否则，更新根据计划安装。
     如果安装更新可能影响设备性能则使用该选项。
     默认情况下已禁用该选项。

   - **安装所需的常规系统组件**

     如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

如果禁用该选项，您可能必须手动安装先决条件。

默认情况下已禁用该选项。

- **更新过程中允许安装新应用程序版本**

  如果启用该**选项**，如果更新导致软件应用程序新版本的安装，更新将被允许。

  如果禁用该选项，软件不被升级。您可以稍后手动或通过其他任务安装软件的新版本。例如，如果公司基础架构不被新软件版本支持，或者如果您想要在测试基础架构中检查升级，您可能使用该选项。

  默认情况下已启用该选项。

  升级应用程序可能导致安装在客户端设备上的独立应用程序功能异常。

- **下载更新到设备而不安装**

  如果启用该选项，应用程序下载更新到设备但是不自动安装它们。您可以稍后手动安装下载的更新。

  Microsoft 更新被下载到系统 Windows 存储。第三方应用程序更新（由非 Kaspersky 和 Microsoft 软件供应商开发的应用程序）将会下载到“**下载更新到**”字段中指定的文件夹中。

  如果禁用该选项，更新被自动安装到设备。

  默认情况下已禁用该选项。

- **下载更新到**

  该文件夹用于下载第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新。

- **启用高级诊断**

  如果启用该功能，即便写入跟踪文件在 Kaspersky Security Center 远程诊断实用程序中对网络代理禁用，网络代理也会写入跟踪文件。跟踪轮流写入两个文件中；两个文件的总大小由“**高级诊断文件的最大大小，MB**”值决定。当两个文件都满时，网络代理再次开始写入它们。带有跟踪的文件存储在 %WINDIR%\Temp 文件夹。这些文件在远程诊断实用程序中可以被访问，您可以在那里下载或删除它们。

  如果禁用该功能，网络代理根据 Kaspersky Security Center 远程诊断实用程序中的设置写入跟踪。没有附加跟踪被写入。

  当创建任务时，您不必启用高级诊断。例如，如果某个任务在一些设备上失败并且您希望在另一个任务运行期间获取额外信息，您可能希望稍后使用该功能。

  默认情况下已禁用该选项。

- **高级诊断文件的最大大小，MB**

  默认值是 100 MB，可用值介于 1 MB 和 2048 MB 之间。当您所发送的高级诊断文件信息不足以定位问题时，您可能被 Kaspersky 技术支持专家要求更改默认值。

7. 指定操作系统重新启动设置：

- **不重启设备**

  客户端设备在操作后不被自动重启。要完成操作，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的任务。

- **重启设备**

  如果完成安装需要重启，客户端设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的任务。

- **提示用户操作**

  客户端设备屏幕上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。该选项适用于用户必须可以选择最方便的时间进行重启的工作站。

  默认情况下已选定该选项。

- **重复提示间隔(分钟)**

  如果启用该选项，应用程序以指定频率提示用户重启操作系统。

  默认情况下已启用该选项。默认时间间隔为 5 分钟。可用值介于 1 和 1 440 分钟之间。

  如果禁用该选项，提示仅显示一次。

- **在该时间后重启(分钟)**

  提示用户之后，应用程序在指定时间间隔后强制操作系统重启。

  默认情况下已启用该选项。默认延时是 30 分钟。可用值介于 1 和 1 440 分钟之间。

- **在该时间后强制关闭阻止会话中的应用程序(分钟)**

  用户设备锁定时，程序以强制模式关闭（指定不活动间隔之后自动锁定，或手动锁定）。

  如果启用此选项，当输入字段中指定的时间间隔结束后，锁定设备上的应用程序将被强制关闭。

  如果禁用此选项，应用程序在锁定的设备上不关闭。

  默认情况下已禁用该选项。

8. 如果要修改默认任务设置，请启用“**完成任务创建**”页面上的“**创建完成时打开任务详情**”选项。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

9. 单击“**完成**”按钮。

   任务被创建并显示在任务列表。

10. 点击创建的任务的名称以打开任务属性窗口。

11. 在任务属性窗口中，根据需要指定常规任务设置。

12. 单击“**保存**”按钮。

    任务被创建和配置。

如果任务结果包含 0x80240033 “Windows 更新代理错误 80240033（“无法下载授权许可条款。”）”错误警告，则可以通过 Windows 注册表解决此问题。

添加更新安装规则

此功能仅在“漏洞和补丁管理”授权许可下可用。

使用“*安装所需更新并修复漏洞*”任务安装软件更新或修复软件漏洞时，您必须指定更新安装规则。这些规则决定要安装的更新和要修复的漏洞。

精确设置取决于您是否添加了所有更新、Windows Update 更新、第三方应用程序（由非 Kaspersky 和 Microsoft 软件供应商制作的应用程序）更新的规则。当添加 Windows Update 更新或第三方应用程序更新的规则时，您可以选择特定的应用程序和您要安装更新的应用程序版本。当添加所有更新的规则时，您可以选择您要安装的特定更新和您要通过安装更新进行修复的漏洞。

您可以通过以下方式添加更新安装规则：

- 通过在创建新“安装所需更新并修复漏洞”任务时添加规则。
- 通过在现有的“*安装所需更新并修复漏洞*”任务的属性窗口的**应用程序设置**选项卡中添加规则。
- 通过更新安装向导或漏洞修复向导。

要添加所有更新的规则：

1. 单击“**添加**”按钮。

   规则创建向导开始。使用**下一步**按钮进行向导。

2. 在“**规则类型**”页面，选择“**所有更新的规则**”。

3. 在**常规标准**页面，使用下拉列表指定以下设置：

   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：

     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

默认情况下已禁用该选项。

4. 在**更新**页面，选择要安装的更新：

- **安装所有适用的更新**

  安装符合向导“**常规标准**”页面上指定条件的所有软件更新。默认选择。

- **仅安装列表中的更新**

  仅安装您从列表中手动选择的软件更新。该列表包含所有可用软件更新。

  例如，您可能想要在以下情况下选择特定更新：要在测试环境中检查它们的安装、要仅更新严重应用程序、或者要仅更新特定应用程序。

  - **自动安装所选更新安装所需的所有先前应用程序更新**

    如果在安装所选更新需要时，您同意安装临时应用程序版本，保持该选项被启用。

    如果禁用该选项，仅选定的应用程序版本被安装。如果您想直截了当地更新应用程序，而不尝试安装增量版本，请禁用该选项。如果安装所选更新不能不安装先前版本的应用程序，应用程序更新失败。

    例如，您在设备上安装了应用程序的版本 3，您想更新它到版本 5，但是该应用程序的版本 5 仅可以在版本 4 之上安装。如果启用该选项，软件先安装版本 4，然后安装版本 5。如果禁用该选项，软件更新应用程序失败。

    默认情况下已启用该选项。

5. 在**漏洞**页面，选择将由安装所选更新修复的漏洞：

- **修复所有匹配其他标准的漏洞**

  修复符合向导“**常规标准**”页面上指定条件的所有漏洞。默认选择。

- **仅修复列表中的漏洞**

  仅修复您手动从列表中选择的漏洞。列表包含所有检测到的漏洞。

  例如，您可能想要在以下情况下选择特定漏洞：要在测试环境中检查它们的修复、要仅修复严重应用程序中的漏洞、或者要仅修复特定应用程序中的漏洞。

6. 在“**名称**”页面，指定您正在添加的规则的名称。您可以稍后在所创建任务的属性窗口的“**设置**”区域更改该名称。

规则创建向导完成操作后，新规则将添加，并显示在新任务向导或任务属性的规则列表中。

要添加 Windows Update 更新的新规则：

1. 单击“**添加**”按钮。

   规则创建向导开始。使用**下一步**按钮进行向导。

2. 在“**规则类型**”页面上，选择“**Windows 更新的规则**”。

3. 在**常规标准**页面，指定以下设置：

   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：

     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。

   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。

   - **修复 MSRC 严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Microsoft Security Response Center (MSRC) 设置的严重级别等于或高于列表中选定的值（**低**、**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。

4. 在**应用程序**页面，选择您要安装更新的应用程序和应用程序版本。默认情况下选定所有应用程序。

5. 在**更新类别**页面，选择要安装的更新类别。这些类别与 Microsoft Update Catalog 中的类别相同。默认情况下选定所有类别。

6. 在“**名称**”页面，指定您正在添加的规则的名称。您可以稍后在所创建任务的属性窗口的“**设置**”区域更改该名称。

规则创建向导完成操作后，新规则将添加，并显示在新任务向导或任务属性的规则列表中。

要添加第三方应用程序更新的新规则：

1. 单击“**添加**”按钮。
   规则创建向导开始。使用**下一步**按钮进行向导。
2. 在“**规则类型**”页面，选择“**第三方更新的规则**”。
3. 在**常规标准**页面，指定以下设置：
   - **要安装的更新集**

     选择必须在客户端设备上安装的更新：
     - **仅安装批准的更新**。这仅安装批准的更新。
     - **安装所有更新 (除了拒绝的)**。这安装带有*已批准*或*未定义*批准状态的更新。
     - **安装所有更新 (包括拒绝的)**。这安装所有更新，无论什么批准状态。警惕选择该选项。例如，如果您想要在测试基础架构中检查一些被拒绝的更新的安装，使用该选项。
   - **修复严重级别等于或大于该项的漏洞**

     有时候，软件更新可能损害用户的软件体验。此种情况下，您可能决定仅安装软件操作的关键更新并跳过其他更新。

     如果启用该选项，更新仅修复 Kaspersky 设置的严重级别等于或高于列表中选定的值（**中度**、**高危**或**严重**）的漏洞。严重级别低于选定值的漏洞不被修复。

     如果禁用该选项，更新修复所有漏洞，无论它们的严重级别是什么。

     默认情况下已禁用该选项。
4. 在**应用程序**页面，选择您要安装更新的应用程序和应用程序版本。默认情况下选定所有应用程序。
5. 在“**名称**”页面，指定您正在添加的规则的名称。您可以稍后在所创建任务的属性窗口的“设置”区域更改该名称。

规则创建向导完成操作后，新规则将添加，并显示在新任务向导或任务属性的规则列表中。

为第三方软件中的漏洞选择用户修补程序

要使用“*修复漏洞*”任务，您必须手动指定软件更新以修复任务设置中列出的第三方软件中的漏洞。“*修复漏洞*”任务使用针对 Microsoft 软件的建议修补程序以及针对其他第三方软件的用户修补程序。*用户修补程序*是软件更新，用于修复管理员手动指定的漏洞。

要为第三方软件中的漏洞选择用户修补程序，请执行以下操作：

1. 在主菜单中，转到**操作→补丁管理→软件漏洞**。
   该页面显示在客户端设备上检测到的软件漏洞列表。
2. 在软件漏洞列表中，单击带有要为其指定用户修复的软件漏洞名称的链接。
   漏洞的属性窗口打开。

3. 在左侧窗格中，选择“**用户修复和其他修复**”区域。

   将显示所选软件漏洞的用户修复列表。

4. 单击**添加**。

   此时将显示可用安装包的列表。显示的安装包列表对应于“**操作**”→“**存储库**”→“**安装包**”列表。如果尚未创建包含针对所选漏洞用户修补程序的安装包，则可以立即通过启动“新安装包向导”来创建该包。

5. 选择一个或多个安装包，其中包含针对第三方软件漏洞的一个或多个用户修补程序。

6. 点击**保存**。

   系统会指定包含软件漏洞用户修补程序的安装包。启动“*修复漏洞*”任务后，将安装安装包并修复软件漏洞。

查看有关在所有受管理设备上检测到的软件漏洞的信息

在扫描受管理设备上的软件是否存在漏洞之后，您可以查看在所有受管理设备上检测到的软件漏洞列表。如果运行管理服务器层次结构的任务，则可以只针对所选的管理服务器，查看已检测出漏洞的受管理设备列表。

要查看在所有受管理设备上检测到的软件漏洞列表，

在主菜单中，转到“**操作**”→“**补丁管理**”→“**软件漏洞**”。

该页面显示在客户端设备上检测到的软件漏洞列表。

您还可以生成和查看漏洞报告。

您可以指定一个过滤器以查看软件漏洞列表。单击软件漏洞列表右上角的“**过滤器**”图标 ( ) 以管理过滤器。您也可以从软件漏洞列表上方的“**预设过滤器**”下拉列表中选择一个预设过滤器。

您可以获取列表中任何漏洞的详细信息。

要获取有关软件漏洞的信息：

在软件漏洞列表中，单击带有漏洞名称的链接。

软件漏洞的属性窗口打开。

查看有关在选定受管理设备上检测到的软件漏洞的信息

您可以查看有关在选定的运行 Windows 的受管理设备上检测到的软件漏洞的信息。

要查看在选定受管理设备上检测到的软件漏洞列表：

1. 在主菜单中，转到“**资产(设备)**”→“**受管理设备**”。

   将显示受管理设备列表。

2. 在受管理设备列表中，单击含有要查看在其中检测到的软件漏洞的设备的名称的链接。

   将显示所选设备的属性窗口。

3. 在所选设备的属性窗口中，选择“**高级**”选项卡。

4. 在左侧窗格中，选择“**软件漏洞**”区域。

将显示在选定受管理设备上检测到的软件漏洞列表。

要查看所选软件漏洞的属性，

在软件漏洞列表中单击带有软件漏洞名称的链接。

将显示所选软件漏洞的属性窗口。

查看受管理设备上的漏洞统计信息

您可以查看受管理设备上每个软件漏洞的统计信息。统计信息以图表形式展示。图表将显示具有以下状态的设备数量：

- *忽略：<设备数>*。如果您在漏洞属性中手动设置了忽略漏洞的选项，则分配此状态。
- *已修复：<设备数>*。如果修复漏洞的任务成功完成，则分配此状态。
- *计划修复：<设备数>*。如果已创建修复漏洞的任务但该任务尚未执行，则分配此状态。
- *应用补丁：<设备数>*。如果您手动选择了软件更新以修复漏洞，但此软件更新尚未修复漏洞，则分配此状态。
- *需要修复：<设备数>*。如果漏洞仅在某些受管理设备上得到修复，并且需要在更多托管设备上修复漏洞，则分配此状态。

要查看受管理设备上的漏洞统计信息，请执行以下操作：

1. 在主菜单中，转到“**操作**” → “**补丁管理**” → “**软件漏洞**”。
   该页面显示受管理设备上检测到的应用程序漏洞的列表。

2. 选中所需漏洞旁边的复选框。

3. 单击**设备漏洞统计信息**按钮。

将显示漏洞状态图。单击一种状态将打开漏洞处于选定状态的设备列表。

将软件漏洞列表导出到文件

您可以将显示的漏洞列表导出到 CSV 或 TXT 文件。例如，您可以将这些文件发送给信息安全经理或出于统计目的存储它们。

要将在所有受管理设备上检测到的软件漏洞列表导出到文本文件：

1. 在主菜单中，转到“**操作**” → “**补丁管理**” → “**软件漏洞**”。
   该页面显示受管理设备上检测到的应用程序漏洞的列表。
2. 单击“**导出到 TXT**”或“**导出到 CSV**”按钮，具体取决于所需导出格式。

包含软件漏洞列表的文件将下载到您当时使用的设备上。

要将在选定受管理设备上检测到的软件漏洞列表导出到文本文件：

1. 打开在选定受管理设备上检测到的软件漏洞列表。
2. 选择要导出的软件漏洞。
   如果要导出在受管理设备上检测到的软件漏洞的完整列表，请跳过此步骤。
   如果要导出在受管理设备上检测到的软件漏洞的完整列表，则仅导出当前页面上显示的漏洞。
3. 单击“**导出到 TXT**”或“**导出到 CSV**”按钮，具体取决于所需导出格式。

包含在选定受管理设备上检测到的软件漏洞列表的文件将下载到您当时正在使用的设备上。

忽略软件漏洞

您可以忽略要修复的软件漏洞。忽略软件漏洞的原因可能有如下几点：

- 您认为该软件漏洞对您的组织不严重。
- 您了解该软件漏洞修补程序可能会破坏与需要该漏洞修补程序的软件相关的数据。
- 您可以确定该软件漏洞对组织的网络没有危险，因为您使用其他措施来保护受管理设备。

您可以忽略所有受管理设备上或仅选定受管理设备上的软件漏洞。

要忽略所有受管理设备上的软件漏洞，请执行以下操作：

1. 在主菜单中，转到“**操作**” → “**补丁管理**” → “**软件漏洞**”。
   该页面显示在受管理设备上检测到的软件漏洞列表。
2. 在软件漏洞列表中，单击带有要忽略的软件漏洞名称的链接。
   软件漏洞属性窗口将打开。
3. 在“**常规**”选项卡上，启用“**忽略漏洞**”选项。
4. 单击“**保存**”按钮。
   软件漏洞属性窗口将关闭。

在所有受管理设备上都会忽略该软件漏洞。

要忽略选定受管理设备上的软件漏洞，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
   将显示受管理设备列表。
2. 在受管理设备列表中，单击含有要忽略其中的软件漏洞的设备的名称的链接。
   设备属性窗口打开。
3. 在设备属性窗口中，选择“**高级**”选项卡。
4. 在左侧窗格中，选择“**软件漏洞**”区域。
   将显示在设备上检测到的软件漏洞列表。
5. 在软件漏洞列表中，选择要在选定设备上忽略的漏洞。
   软件漏洞属性窗口将打开。
6. 在软件漏洞属性窗口或“**常规**”选项卡中，启用“**忽略漏洞**”选项。
7. 单击“**保存**”按钮。
   软件漏洞属性窗口将关闭。
8. 关闭设备属性窗口。

选定设备上的软件漏洞将被忽略。

在完成“*修复漏洞*”任务或“*安装所需更新并修复漏洞*”任务后，将无法修复被忽略的软件漏洞。您可以通过使用过滤器从漏洞列表中排除被忽略的软件漏洞。

管理客户端设备上运行的应用程序

本节介绍与管理客户端设备上运行的应用程序有关的 Kaspersky Security Center 功能。

使用应用程序控制来管理可执行文件

您可以使用“应用程序控制”组件来允许或阻止可执行文件在用户设备上启动。“应用程序控制”组件支持基于 Windows 和基于 Linux 的操作系统。

对于基于 Linux 的操作系统，应用程序控制组件从 Kaspersky Endpoint Security 11.2 for Linux 开始可用。此外，该组件还可用于 Kaspersky Embedded Systems Security for Windows 3.0 或更高版本。

先决条件

- Kaspersky Security Center 已部署在您的组织中。
- Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的策略已创建并处于活动状态。
- Kaspersky Embedded Systems Security for Windows 或 Kaspersky Embedded Systems Security for Linux 的策略已创建并处于活动状态。

阶段

“应用程序控制”使用方案分阶段进行：

1. **形成并查看客户端设备上的可执行文件列表**

   此阶段帮助您了解在受管理设备上发现了哪些可执行文件。查看可执行文件列表，并将其与允许和禁止的可执行文件列表进行比较。对可执行文件的使用限制可能与组织中的信息安全策略有关。

   说明：

   - 管理控制台：可执行文件清单
   - Kaspersky Security Center Web Console：获取并查看客户端设备上存储的可执行文件列表

2. **为组织中使用的可执行文件创建类别**

   分析受管理设备上存储的可执行文件列表。根据分析，为可执行文件创建类别。建议创建一个“工作应用程序”类别，以覆盖组织中使用的标准可执行文件集。如果不同的安全组在工作中使用不同的可执行文件集，则可以为每个安全组创建单独的类别。

   说明：

   - 创建含有手动添加内容的应用程序类别，创建包含来自选定设备的可执行文件的应用程序类别，创建包含来自特定文件夹的可执行文件的应用程序类别。
   - Kaspersky Security Center Web Console：创建含有手动添加内容的应用程序类别，创建包含来自选定设备的可执行文件的应用程序类别，创建包含来自具体文件夹的可执行文件的应用程序类别。

3. **在 Kaspersky Endpoint Security 策略中配置“应用程序控制”**

   使用您在上一阶段创建的类别，在 Kaspersky Endpoint Security 策略中配置“应用程序控制”组件。

   说明：

   - 管理控制台：配置应用程序在客户端设备上的启动管理
   - Kaspersky Security Center Web Console：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

4. **在 Kaspersky Embedded Systems Security 策略中配置“应用程序控制”**

   使用您创建的类别配置 Kaspersky Embedded Systems Security for Windows 策略中的应用程序控制组件。有关应用程序控制组件的更多信息，请参阅Kaspersky Embedded Systems Security for Windows 帮助 或 Kaspersky Embedded Systems Security for Linux 帮助。

如果使用大量规则，加载策略时可能会出现错误。您可以使用以下命令增加最大请求大小（以字节为单位）：

- 对于 JSON 请求：

```
klscflag -fset -pv ".core/.independent" -s KLLIM -n
LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
```

- 对于 HTTP 请求：

```
klscflag -fset -pv ".core/.independent" -s KLLIM -n
LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
```

其中`<max_request_size>`是以字节为单位的最大请求大小（例如，`200000000`）。

5 在测试模式下开启“应用程序控制”组件

为确保应用程序控制规则不会阻止用户工作所需的可执行文件，建议在创建新规则后启用应用程序控制规则测试并分析其操作。启用测试后，Kaspersky Endpoint Security for Windows 或 Kaspersky Embedded Systems Security 将不会阻止被应用程序控制规则禁止启动的可执行文件，而是将有关其启动的通知发送到管理服务器。

测试应用程序控制规则时，建议执行以下操作：

- 确定测试周期。测试周期从几天到两个月不等。
- 检查由测试“应用程序控制”操作生成的事件。

Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中启用“**测试模式**”选项。

6 更改“应用程序控制”组件的类别设置

如有必要，请更改“应用程序控制”设置。根据测试结果，您可以将与应用程序控制组件事件相关的可执行文件添加到含有手动添加内容的类别中。

说明：

- 管理控制台：添加事件相关的可执行文件到应用程序类别
- Kaspersky Security Center Web Console：添加事件相关的可执行文件到应用程序类别

7 在操作模式下应用“应用程序控制”的规则

测试应用程序控制规则并完成类别的配置后，您可以在操作模式下应用这些应用程序控制规则。

Kaspersky Security Center Web Console 操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。遵循此说明并在配置过程中禁用“**测试模式**”选项。

8 验证“应用程序控制”配置

确保已完成以下操作：

- 为可执行文件创建类别。
- 已使用类别来配置应用程序控制。
- 已在操作模式下应用“应用程序控制”的规则。

结果

方案完成后，可执行文件在受管理设备上的启动受到控制。用户只能运行组织中允许的可执行文件，而不能运行组织中禁止的可执行文件。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

应用程序控制模式和类别

应用程序控制组件监控用户启动可执行文件的尝试。您可以使用应用程序控制规则来控制可执行文件的启动。

> 应用程序控制组件适用于Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security 11.2 for Linux 及更高版本以及Kaspersky Security for Virtualization Light Agent。本节中的所有说明都介绍适用于 Kaspersky Endpoint Security for Windows 的“应用程序控制”的配置。

其设置与任何应用程序控制规则都不匹配的可执行文件的启动由该组件的选定操作模式管理：

- *拒绝列表*。如果要允许启动除了阻止规则中指定的可执行文件外的所有可执行文件，则使用该模式。默认情况下选择此模式。
- *允许列表*。如果要阻止启动除了允许规则中指定的可执行文件外的所有可执行文件，则使用该模式。

应用程序控制规则是通过可执行文件的类别来实施的。在 Kaspersky Security Center 中，有三种类型的类别：

- 含有手动添加内容的类别。您定义将可执行文件包括在类别中的条件，例如元数据、文件哈希码、文件证书、KL 类别、文件路径。
- 包含来自所选设备的可执行文件的类别。您指定自动包含在该类别中的可执行文件所属的设备。
- 包含来自所选文件夹的可执行文件的类别。您指定自动包含在该类别中的可执行文件所来自的文件夹。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

获取并查看客户端设备上存储的可执行文件列表

您可以通过以下方式之一获取存储在客户端设备上的可执行文件列表：

- 在 Kaspersky Endpoint Security 策略中启用应用程序启动通知。
- 创建清查任务。

在 Kaspersky Endpoint Security 策略中启用应用程序启动通知

要启用有关应用程序启动的通知：

1. 打开 Kaspersky Endpoint Security 策略设置，然后转到**常规设置** → **报告和存储**。
2. 在**到管理服务器的数据传输**设置组中，选择**关于启动的应用程序**复选框，保存更改。

当用户尝试启动可执行文件时，关于这些文件的信息将被添加到客户端设备上的可执行文件列表中。Kaspersky Endpoint Security 会将该信息发送到网络代理，然后网络代理将其发送到管理服务器。

创建清单任务

清查可执行文件的功能可用于以下应用程序：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 版本 11.2 及更高版本
- Kaspersky Security for Virtualization 4.0 Light Agent 和更高版本

您可以在获取已安装应用程序相关信息的同时减少数据库的负载。为了节省数据库空间，在安装了一组标准软件的参考设备上运行清单任务。建议设备数量为 1-3。

我们强烈不建议在使用以下数据库时运行清单任务：MySQL、PostgreSQL、SQL Server Express Edition、MariaDB（所有版本）。

要在客户端设备上为可执行文件创建清查任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
   将显示任务列表。
2. 单击“**添加**”按钮。
   新任务向导启动。遵照向导的说明。
3. 在**新任务设置**页面的**应用程序**下拉列表中，选择 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux，具体取决于客户端设备的操作系统类型。

4. 在“**任务类型**”下拉列表中，选择“**清单**”。

5. 在**完成任务创建**页面上，单击**完成**按钮。

新任务向导完成后，将创建并配置“**清单**”任务。如果需要，可以更改已创建任务的设置。新创建的任务显示在任务列表中。

关于清查任务的详细说明，请参阅以下帮助：

- Kaspersky Endpoint Security for Windows 帮助
- Kaspersky Endpoint Security for Linux 帮助
- Kaspersky Security for Virtualization Light Agent

执行“**清单**”任务后，将形成受管理设备上存储的可执行文件列表，您可以查看该列表。

清查过程中可检测以下格式的可执行文件（具体取决于您在清单任务属性中选择的选项）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

查看受管理设备上存储的可执行文件列表

要查看客户端设备上存储的可执行文件列表：

在主菜单中，转到“**操作**” → “**第三方应用程序**” → “**可执行文件**”。

该页面显示客户端设备上存储的可执行文件列表。

如有必要，您可以将受管理设备的可执行文件发送到 Kaspersky Security Center Web Console 在其中打开的设备。

要发送可执行文件：

1. 在主菜单中，转到“**操作**” → “**第三方应用程序**” → “**可执行文件**”。

2. 单击要发送的可执行文件的链接。

3. 在打开的窗口中，转到**设备**部分，然后选中要从其发送可执行文件的受管理设备的复选框。

在发送可执行文件之前，请确保受管理设备与管理服务器有直接连接，方法是选择**不断开与管理服务器的连接**复选框。

4. 单击“**发送**”按钮。

所选可执行文件将下载以进一步发送到您的 Kaspersky Security Center Web Console 在其中打开的设备。

创建含有手动添加内容的应用程序类别

您可以指定一组条件作为要在组织中允许或阻止启动的可执行文件的模板。在对应于条件的可执行文件的基础上，您可以创建一个应用程序类别，并在"应用程序控制"组件配置中使用该应用程序类别。

要创建含有手动添加内容的应用程序类别：

1. 在主菜单中，转到**操作 → 第三方应用程序 → 应用程序类别**。

   将显示含有应用程序类别列表的页面。

2. 单击"**添加**"按钮。

   新类别向导启动。使用**下一步**按钮进行向导。

3. 在"**选择策略创建方法**"步骤，选择"**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**"选项。

4. 在"**条件**"步骤中，单击"**添加**"按钮以添加在所创建类别中包含文件的条件标准。

5. 在"**条件标准**"步骤中，从列表中选择创建类别时所遵循的规则类型：

   - **从 KL 类别**

     如果选中此选项，您可以指定卡巴斯基应用程序类别作为添加应用程序到用户类别的条件。来自指定 Kaspersky 类别的应用程序将被添加到用户应用程序类别。

   - **从存储库选择证书**

     如果选中此选项，则可以指定来自存储库的证书。类别条件仅匹配由指定证书签名的可执行文件。

     如果您创建并启动了清查任务并在 Kaspersky Endpoint Security 策略中勾选了"**关于已启动的应用程序**"复选框，则会将证书添加到存储库中。您可以执行以下两项操作。

   - **指定应用程序路径 (支持掩码)**

     如果选中此选项，您可以指定包含了要添加到用户应用程序类别的可执行文件的客户端设备上的文件或文件夹的路径。您可以使用正则表达式，如*C:\path_to_exe**，例如：*C:\Program Files\Internet Explorer**。

   - **可移动驱动器**

     如果选中此选项，您可以指定应用程序在其上运行的媒体类型（任意设备或可移动驱动器）。在所选驱动类型上运行的应用程序被添加到用户应用程序类别。

   - **哈希、元数据或证书**：

     - **从可执行文件列表选择**

       如果选中此选项，可以使用客户端设备上的可执行文件列表来选择可执行文件并将应用程序添加到类别。

- **从应用程序注册表选择**

  如果选择此选项，将显示应用程序注册表。从注册表中选择一个应用程序后，窗口将打开，其中的参数将使用您选择的应用程序的元数据进行填充：

  - 文件名。
  - 文件版本。您可以指定版本的精确值或描述一个条件，例如“高于 5.0”。
  - 应用程序名称。
  - 应用程序版本。您可以指定版本的精确值或描述一个条件，例如“高于 5.0”。
  - 供应商。

  请注意，仅阻止满足指定参数的可执行文件的启动，而不阻止您选择的应用程序的启动。如果选定的应用程序元数据与启动应用程序时启动的可执行文件的元数据相匹配，那么您可以继续下一步。否则，您必须手动更改值以匹配可执行文件的元数据。

- **手动指定**

  如果选择此选项，您必须指定文件哈希、元数据或证书作为将应用程序添加到用户类别的条件。

  文件哈希

  取决于您网络设备上安装的安全应用程序版本，您必须为此类别中的文件选择 Kaspersky Security Center 使用的哈希值算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

  未在 SHA256 算法中找到漏洞，它被视为现今最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支持 SHA256 计算。计算 MD5 哈希被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支持。

  为该类别中的文件选择任意 Kaspersky Security Center 使用的哈希值算法选项：

  - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，请选中“**SHA256**”复选框。对于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我们不建议您添加根据可执行文件 SHA256 哈希标准创建的类别。这将导致安全应用程序操作失败。此种情况下，您可以为类别中的文件使用 MD5 加密算法。
  - 如果您的网络上安装了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，请选择“**MD5 哈希**”。您不能添加基于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本的可执行文件的 MD5 校验和标准所创建的类别。此种情况下，您可以为类别中的文件使用 SHA256 加密算法。
  - 如果您网络上的不同设备同时使用早期和更新版本的 Kaspersky Endpoint Security 10，请同时选中**SHA256**复选框和**MD5 哈希**复选框。

  元数据

  如果选择此选项，则可以指定文件名、文件版本、供应商形式的文件元数据。类别条件仅匹配具有相同元数据的可执行文件。

  证书

  如果选中此选项，则可以指定来自存储库的证书。类别条件仅匹配由指定证书签名的可执行文件。

  如果您创建并启动了清查任务并在 Kaspersky Endpoint Security 策略中勾选了“**关于已启动的应用程序**”复选框，则会将证书添加到存储库中。您可以执行以下两项操作。

- **从文件或从 MSI 包/存档文件夹**

  如果选中此选框，您可以指定 MSI 安装器文件作为添加应用程序到用户类别的条件。应用程序安装器元数据将被发送到管理服务器。与指定的 MSI 安装程序具有相同元数据的应用程序被添加到用户应用程序类别。

所选条件将添加到条件列表中。

您可以根据需要为创建应用程序类别添加任意数量的条件。

6. 在“**排除项**”步骤中，单击“**添加**”按钮以添加从所创建类别中排除文件的排除条件标准。

7. 在“**条件标准**”步骤中，从列表中选择规则类型，方式与选择创建类别时所遵循的规则类型相同。

当向导结束时，将创建应用程序类别。它显示在应用程序规则列表中。配置“应用程序控制”时，可以使用已创建的应用程序类别。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

创建包括选定设备中的可执行文件的应用程序类别

您可以将选定设备中的可执行文件用作要允许或阻止的可执行文件的模板。基于选定设备中的可执行文件，您可以创建一个类别，并在“应用程序控制”组件配置中使用该应用程序类别。

要从设备检索可执行文件列表：

1. 确保 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的策略已创建并处于活动状态。在策略中启用应用程序控制组件。

2. 获取客户端设备上存储的可执行文件列表。

要创建包括选定设备中的可执行文件的类别：

1. 在主菜单中，转到“**操作**”→“**第三方应用程序**”→“**应用程序类别**”。

   显示含有类别列表的页面。

2. 单击“**添加**”按钮。

   新类别向导启动。使用**下一步**按钮进行向导。

3. 在“**选择策略创建方法**”步骤中，指定类型名称并选择“**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**”选项。

4. 单击**添加**。

5. 在打开的窗口中，选择一个或多个设备，其可执行文件将用于创建类别。

6. 指定下列设置：

- **哈希值计算算法**

  取决于您网络设备上安装的安全应用程序版本，您必须为此类别中的文件选择 Kaspersky Security Center 使用的哈希值算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

  未在 SHA256 算法中找到漏洞，它被视为现今最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支持 SHA256 计算。计算 MD5 哈希被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支持。

  为该类别中的文件选择任意 Kaspersky Security Center 使用的哈希值算法选项：

  - 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，请选中“**SHA256**”复选框。对于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我们不建议您添加根据可执行文件 SHA256 哈希标准创建的类别。这将导致安全应用程序操作失败。此种情况下，您可以为类别中的文件使用 MD5 加密算法。

  - 如果您的网络上安装了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，请选择“**MD5 哈希**”。您不能添加基于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本的可执行文件的 MD5 校验和标准所创建的类别。此种情况下，您可以为类别中的文件使用 SHA256 加密算法。

  如果您网络上的不同设备同时使用早期和更新版本的 Kaspersky Endpoint Security 10，请同时选中**SHA256**复选框和**MD5 哈希**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)**”复选框被默认选中。

  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)复选框被默认清空。

- **与管理服务器存储库同步数据**

  如果您希望该管理服务器定期检查指定文件夹中的更改，则选择此选项。

  默认情况下已禁用该选项。

  如果启用此选项，请指定检查指定文件夹中的更改的周期（以小时为单位）。默认情况下，扫描间隔为 24 小时。

- **文件类型**

  在此区域中，可以指定用于创建应用程序类别的文件类型。

  所有文件。创建类别时会考虑所有文件。默认情况下已选定该选项。

  仅应用程序类别之外的文件。创建类别时仅考虑应用程序类别之外的文件。

- **文件夹**

  在此区域中，可以指定选定设备中的哪些文件夹包含用于创建应用程序类别的文件。

  所有文件夹。创建类别时会考虑所有文件夹。默认情况下已选定该选项。

指定文件夹。创建类别时仅考虑指定文件夹。如果选择此选项，则必须指定文件夹的路径。

向导完成后，会创建可执行文件的类别。它显示在类别列表中。配置应用程序控制时，可以使用已创建的类别。

创建包括选定文件夹中的可执行文件的应用程序类别

您可以将选定文件夹中的可执行文件用作要在组织中允许或阻止的可执行文件的标准。在选定文件夹中的可执行文件的基础上，您可以创建一个应用程序类别，并在"应用程序控制"组件配置中使用该应用程序类别。

要创建包括选定文件夹中的可执行文件的类别：

1. 在主菜单中，转到"**操作**"→"**第三方应用程序**" → "**应用程序类别**"。
   显示含有类别列表的页面。
2. 单击"**添加**"按钮。
   新类别向导启动。使用**下一步**按钮进行向导。
3. 在"**选择策略创建方法**"步骤中，指定类型名称并选择"**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**"选项。
4. 指定将用于创建该类别的可执行文件所在的文件夹。
5. 定义下列设置：

- **包含动态链接库 (DLL) 到该类别**

  应用程序类别包含动态链接库(DLL 格式的文件)，应用程序控制组件记录系统中运行的此类库的操作。包含 DLL 文件到类别可能降低 Kaspersky Security Center 的性能。

  默认情况下已清除该选框。

- **包含脚本数据到该类别**

  应用程序类别包含脚本数据，脚本不被 Web 威胁防护阻止。包含脚本数据到类别可能降低 Kaspersky Security Center 的性能。

  默认情况下已清除该选框。

- **哈希值计算算法**：**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)**

  取决于您网络设备上安装的安全应用程序版本，您必须为此类别中的文件选择 Kaspersky Security Center 使用的哈希值算法。有关由哈希函数计算的哈希值的信息存储在管理服务器数据库中。

  未在 SHA256 算法中找到漏洞，它被视为现今最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支持 SHA256 计算。计算 MD5 哈希被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支持。

为该类别中的文件选择任意 Kaspersky Security Center 使用的哈希值算法选项：

- 如果网络上安装的所有安全应用程序实例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，请选中“**SHA256**”复选框。对于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我们不建议您添加根据可执行文件 SHA256 哈希标准创建的类别。这将导致安全应用程序操作失败。此种情况下，您可以为类别中的文件使用 MD5 加密算法。

- 如果您的网络上安装了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，请选择“**MD5 哈希**”。您不能添加基于 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本的可执行文件的 MD5 校验和标准所创建的类别。此种情况下，您可以为类别中的文件使用 SHA256 加密算法。

如果您网络上的不同设备同时使用早期和更新版本的 Kaspersky Endpoint Security 10，请同时选中**SHA256**复选框和**MD5 哈希**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)**”复选框被默认选中。

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)复选框被默认清空。

- **强制扫描文件夹以查找更改**

如果启用此选项，应用程序会定期检查“类别内容添加”文件夹的任何变化。您可以在该选框旁的输入字段中指定检查频率（小时）。默认情况下，强制检查的时间间隔为 24 小时。

如果禁用此选项，应用程序不会强制检查文件夹。如果文件被修改、添加或删除，服务器会尝试访问这些文件。

默认情况下已禁用该选项。

向导完成后，会创建可执行文件类别。它显示在类别列表中。您可以在“应用程序控制”配置中使用该类别。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

查看应用程序类别列表

您可以查看已配置的可执行文件类别列表以及每个类别的设置。

要查看应用程序类别列表，

在主菜单中，转到“**操作**” → “**第三方应用程序**” → “**应用程序类别**”。

显示含有类别列表的页面。

要查看应用程序类别的属性，

单击该类别的名称。

显示该类别的属性窗口。这些属性被分组在几个选项卡上。

添加事件相关的可执行文件到应用程序类别

在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”后，以下事件将显示在事件列表中：

- **应用程序启动被禁止**（*严重*事件）。如果已将“应用程序控制”配置为应用规则，则显示此事件。
- **应用程序启动在测试模式中被禁止**（*信息*事件）。如果已将“应用程序控制”配置为测试规则，则显示此事件。
- **向管理员发送的有关应用程序启动禁止的消息**（*警告*事件）。如果已将“应用程序控制”配置为应用规则，并且用户请求访问在启动时被阻止的应用程序，则会显示此事件。

建议创建事件分类以查看与“应用程序控制”操作相关的事件。

您可以将与“应用程序控制”事件相关的可执行文件添加到现有应用程序类别或新的应用程序类别。您只能将可执行文件添加到含有手动添加内容的应用程序类别。

要将与“应用程序控制”事件相关的可执行文件添加到应用程序类别：

1. 在主菜单中，转到“**监控和报告**” → “**事件分类**”。
   将显示事件分类列表。
2. 选择事件分类以查看与“应用程序控制”相关的事件并启动此事件分类。
   如果尚未创建与“应用程序控制”相关的事件分类，可以选择并启动预定义分类，例如“**最近的事件**”。
   将显示事件列表。
3. 选择要将其相关可执行文件添加到应用程序类别的事件，然后单击“**分配到类别**”按钮。
   新类别向导启动。使用**下一步**按钮进行向导。
4. 在向导页面上，指定相关设置：
   - 在“**对事件相关可执行文件所采取的操作**”区域中，选择以下选项之一：
     - **添加到新的应用程序类别**

       如果要基于事件相关的可执行文件创建新的应用程序类别，则选择此选项。
       默认情况下已选定该选项。
       如果选择了此选项，请指定新的类别名称。

     - **添加到现有应用程序类别**

       如果要将事件相关的可执行文件添加到现有应用程序类别，则选择此选项。
       默认情况下未选定该选项。
       如果选择了此选项，请选择要将可执行文件添加到的含有手动添加内容的应用程序类别。

- 在“**规则类型**”区域中，选择以下选项之一：
  - **添加到包含的规则**
  - **添加到排除的规则**
- 在**用作条件的参数**部分中，选择以下选项之一：
  - **证书详情(或没有证书的文件的 SHA256 哈希)**

    文件可能使用证书签署。多个文件可能使用相同的证书签署。例如，相同应用程序的不同版本可能使用相同的证书签署，或者相同供应商的多个不同应用程序可能使用相同证书签署。当您选择证书时，应用程序的多个版本或相同供应商的多个应用程序可能组成一个类别。

    每个文件都有单独的 SHA256 哈希。当您选择 SHA256 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

    如果您要将可执行文件的证书详情（或者无证书文件的 SHA256 哈希函数）添加到类别规则，则选择该选项。

    默认情况下已选定该选项。

  - **证书详情(没有证书的文件将被跳过)**

    文件可能使用证书签署。多个文件可能使用相同的证书签署。例如，相同应用程序的不同版本可能使用相同的证书签署，或者相同供应商的多个不同应用程序可能使用相同证书签署。当您选择证书时，应用程序的多个版本或相同供应商的多个应用程序可能组成一个类别。

    如果您要将可执行文件的证书详情添加到类别规则，则选择该选项。如果可执行文件没有证书，该文件将被跳过。该文件的信息将不被添加到类别。

  - **仅 SHA256 (没有哈希的文件将被跳过)**

    每个文件都有单独的 SHA256 哈希。当您选择 SHA256 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

    如果您要仅添加可执行文件的 SHA256 哈希详情，则选择该选项。

  - **仅 MD5 (停产模式，仅对 Kaspersky Endpoint Security 10 Service Pack 1 版本)**

    每个文件都有单独的 MD5 哈希。当您选择 MD5 哈希时，仅一个对应的文件，例如，定义的应用程序版本，组成类别。

    如果您要仅添加可执行文件的 MD5 哈希详情，则选择该选项。MD5 哈希码计算功能被 Kaspersky Endpoint Security 10 Service Pack 1 for Windows 和所有早期版本支持。

5. 单击“**确定**”。

向导完成后，与“应用程序控制”事件相关的可执行文件将添加到现有应用程序类别或新的应用程序类别。您可以查看您已修改或创建的应用程序类别的设置。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助

- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

创建“应用程序控制”类别后，可以在 Kaspersky Endpoint Security for Windows 策略中使用它们配置“应用程序控制”。

在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”：

1. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”。
   将显示含有策略列表的页面。
2. 单击 **Kaspersky Endpoint Security for Windows** 策略。
   策略设置窗口打开。
3. 转到“**应用程序设置**” → “**Security Controls**” → “**Application Control**”。
   将显示带“应用程序控制”设置的“**应用程序控制**”窗口。
4. “**应用程序控制**”选项默认启用。确保“**应用程序控制已禁用**”切换按钮切换到禁用位置。
5. 在“**应用程序控制设置**”区块设置中，启用操作模式以应用“应用程序控制”规则并允许 Kaspersky Endpoint Security for Windows 阻止应用程序启动。
   如果要测试“应用程序控制”规则，请在“**应用程序控制设置**”区域启用测试模式。在测试模式中，Kaspersky Endpoint Security for Windows 不会阻止应用程序启动，但会在报告中记录有关所触发规则的信息。单击**查看报告**链接可查看此信息。
6. 如果您希望 Kaspersky Endpoint Security for Windows 在用户启动应用程序时监控 DLL 模块的加载，请启用“**控制 DLL 模块加载**”选项。
   有关模块和加载了模块的应用程序的信息将保存到报告中。
   Kaspersky Endpoint Security for Windows 仅监控在选择“**控制 DLL 模块加载**”选项后加载的 DLL 模块和驱动程序。如果您希望 Kaspersky Endpoint Security for Windows 监控所有 DLL 模块和驱动程序，包括在启动 Kaspersky Endpoint Security for Windows 之前加载的 DLL 模块和驱动程序，请在选择“**控制 DLL 模块加载**”选项后重新启动设备。
7. （可选）在“**消息模板**”块中，更改当应用程序被阻止启动时显示的消息模板以及发送给您的电子邮件模板。
8. 在“**应用程序控制模式**”区块设置中，选择“**拒绝列表**”或“**允许列表**”模式。
   默认情况下，选择“**拒绝列表**”模式。
9. 单击“**规则列表设置**”链接。
   将打开“**拒绝列表和允许列表**”窗口，您可以在其中添加应用程序类别。默认情况下，如果选择“**拒绝列表**”模式则选定“**拒绝列表**”选项卡，如果选择“**允许列表**”模式则选定“**允许列表**”选项卡。
10. 在“**拒绝列表和允许列表**”窗口中，单击“**添加**”按钮。
    “**应用程序控制规则**”窗口将开启。
11. 单击“**请选择类别**”链接。
    将打开“**应用程序类别**”窗口。

12. 添加您先前创建的应用程序类别。

    可以单击“**编辑**”按钮来编辑已创建类别的设置。

    可以单击“**添加**”按钮来创建新类别。

    可以单击“**删除**”按钮以从列表中删除类别。

13. 完成应用程序类别列表后，单击“**确定**”按钮。

    “**应用程序类别**”窗口关闭。

14. 在“**应用程序控制规则**”窗口的“**主题及其权限**”区域中，创建要应用“应用程序控制”规则的用户和用户组列表。

15. 单击“**确定**”按钮以保存设置并关闭“**应用程序控制规则**”窗口。

16. 单击“**确定**”按钮以保存设置并关闭“**拒绝列表和允许列表**”窗口。

17. 单击“**确定**”按钮以保存设置并关闭“**应用程序控制**”窗口。

18. 关闭含有 Kaspersky Endpoint Security for Windows 策略设置的窗口。

    “应用程序控制”已配置。策略传播到客户端设备后，可执行文件的启动将受到管理。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

获取并查看客户端设备上安装的应用程序列表

Kaspersky Security Center 清查在运行 Linux 和 Windows 操作系统的受管理客户端设备上安装的所有软件。

网络代理编辑安装在设备上的应用程序列表，并把该列表传给管理服务器。网络代理更新应用程序列表大约需要 10-15 分钟。

对于基于 Windows 的客户端设备，网络代理从 Windows 注册表接收有关已安装应用程序的大部分信息。对于基于 Linux 的客户端设备，包管理器向网络代理提供有关已安装应用程序的信息。

> 如果在 Linux 设备上检测到来自**应用程序注册表**部分的应用程序，则应用程序属性不包含有关相关可执行文件的信息。

要查看受管理设备上安装的应用程序列表：

1. 在主菜单中，转到“**操作**”→“**第三方应用程序**”→“**应用程序注册表**”。

   该页面显示一个表格，其中包含安装在受管理设备上的应用程序。选择应用程序以查看其属性，例如，供应商名称、版本号、可执行文件列表、安装了该应用程序的设备列表、可用软件更新列表和检测到的软件漏洞列表。

2. 您可以按如下方式对包含已安装应用程序的表中的数据进行分组和筛选：

   - 单击表格右上角的“设置”图标 ( )。

     在调用的“**列设置**”菜单中，选择要在表中显示的列。要查看安装应用程序的客户端设备的操作系统类型，请选择“**操作系统类型**”列。

   - 单击表格右上角的过滤器图标 ( )，然后在调用的菜单中指定并应用过滤条件。

     显示筛选出的已安装应用程序表。

要查看特定受管理设备上安装的应用程序列表，

在主菜单中，转到“**设备**”→“**受管理设备**”→“**<设备名称>**”→“**高级**”→“**应用程序注册表**”。在此菜单中，您可以将应用程序列表导出到 CSV 文件或 TXT 文件。

有关应用程序控制的详细信息，请参阅以下帮助主题：

- Kaspersky Endpoint Security for Windows 在线帮助
- Kaspersky Endpoint Security for Linux 在线帮助
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 帮助
- Kaspersky Embedded Systems Security for Linux 帮助

从 Kaspersky 数据库创建第三方应用程序的安装包

Kaspersky Security Center Web Console 允许您使用安装包执行第三方应用程序的远程安装。此类第三方应用程序包含在专用的 Kaspersky 数据库中。当您首次运行*将更新下载至管理服务器存储库任务*时，将自动创建此数据库。

要从 Kaspersky 数据库创建第三方应用程序的安装包，请执行以下操作：

1. 在主菜单中，转到**发现和部署 → 部署和分配 → 安装包**。
2. 单击“**添加**”按钮。
3. 在打开的“新安装包向导”页面上，选择“**从卡巴斯基数据库中选择一个应用程序来创建安装包**”选项，然后单击“**下一步**”。
4. 在打开的应用程序列表中，选择相关应用程序，然后单击“**下一步**”。
5. 在下拉列表中选择相关的本地化语言，然后单击“**下一步**”。

   仅当应用程序提供多种语言选项时，才显示此步骤。

6. 如果系统提示您接受安装授权许可协议，请在打开的“**最终用户授权许可协议**”页面上，单击链接以阅读供应商网站上的“授权许可协议”，然后选中“**我确认我已完整阅读、理解并接受该最终用户授权许可协议的条款和条件**”复选框。
7. 在打开的“**新安装包名称**”页面上，在“**包名称**”字段中，输入安装包的名称，然后单击“**下一步**”。

等待直到新创建的安装包上载到管理服务器。当“新安装包向导”显示消息通知您安装包创建过程成功时，单击“**完成**”。

新创建的安装包将出现在安装包列表中。您可以在创建或重新配置“*远程安装应用程序*”任务时选择此安装包。

从 Kaspersky 数据库查看和修改第三方应用程序安装包的设置

如果您先前已经创建 Kaspersky 数据库中列出的任意第三方应用程序安装包，则可以随后查看和修改这些安装包的设置。

从 Kaspersky 数据库修改第三方应用程序安装包的设置只能在“漏洞和补丁管理”授权许可下进行。

要从 Kaspersky 数据库查看和修改第三方应用程序安装包的设置：

1. 在主菜单中，转到**发现和部署 → 部署和分配 → 安装包**。
2. 在打开的安装包列表中，单击相关安装包的名称。
3. 如有必要，在打开的属性页面上修改设置。
4. 单击“**保存**”按钮。

您修改的设置将会保存。

从 Kaspersky 数据库设置第三方应用程序的安装包

第三方应用程序安装包的设置在以下选项卡上分组：

默认情况下，仅显示下面列出的部分设置，因此您可以通过单击“**过滤器**”按钮并从列表中选择相关列名称来添加相应列。

- “**常规**”选项卡：
  - 包含可以手动编辑的安装包名称的输入字段
  - **应用程序**

    为其创建安装包的第三方应用程序的名称。
  - **版本**

    为其创建安装包的第三方应用程序的版本号。
  - **大小**

    第三方安装包的大小 (KB)。

- **创建日期**

  第三方安装包的创建日期和时间。

- **路径**

  存储第三方安装包的网络文件夹的路径。

- "**安装进程**"选项卡：

  - **安装所需的常规系统组件**

    如果启用该选项，在安装更新之前，应用程序自动安装所需的所有常规系统组件（先决条件）。例如，这些先决条件可以是操作系统更新。

    如果禁用该选项，您可能必须手动安装先决条件。

    默认情况下已禁用该选项。

  - 显示更新属性并包含以下列的表：

    - **名称**

      更新名称。

    - **描述**

      更新说明。

    - **源**

      更新的来源，即由 Microsoft 发布还是由其他第三方开发商发布。

    - **类型**

      更新类型，即用于驱动程序还是用于应用程序。

    - **类别**

      针对 Microsoft 更新显示的 Windows Server Update Services (WSUS) 类别（关键更新、定义更新、驱动程序、Feature Pack、安全更新、Service Pack、工具、更新汇总、更新或升级）。

    - **根据 MSRC 的重要级别**

      Microsoft 安全响应中心 (MSRC) 定义的更新重要级别。

    - **重要级别**

      Kaspersky 定义的更新重要级别。

- **补丁重要级别**

  补丁的重要级别（如果用于 Kaspersky 应用程序）。

- **文章**

  知识库中描述更新的文章的标识符 (ID)。

- **公告**

  描述更新的安全公告的 ID。

- **未指定安装(新版本)**

  显示更新是否具有“未分配安装”状态。

- **即将安装**

  显示更新是否具有“待安装”状态。

- **正在安装**

  显示更新是否具有“正在安装”状态。

- **已安装**

  显示更新是否具有“已安装”状态。

- **失败**

  显示更新是否具有“失败”状态。

- **需要重新启动**

  显示更新是否具有“需要重新启动”状态。

- **注册日期**

  显示注册更新的日期和时间。

- **以交互模式安装**

  显示更新是否需要在安装过程中与用户交互。

- **已撤销**

  显示更新的撤销日期和时间。

- **更新批准状态**

  显示更新是否被批准安装。

- **修订**

  显示更新的当前修订号。

- **更新 ID**

  显示更新的 ID。

- **应用程序版本**

  显示应用程序要更新到的版本号。

- **被替代的**

  显示可以替代该更新的其他更新。

- **替代**

  显示该更新可以替代的其他更新。

- **您必须接受授权许可协议的条款**

  显示更新是否需要接受最终用户授权许可协议 (EULA) 的条款。

- **URL 描述**

  显示更新供应商的名称。

- **应用程序系列**

  显示更新所属的应用程序系列的名称。

- **应用程序**

  显示更新所属的应用程序的名称。

- **本地化语言**

  显示更新本地化的语言。

- **未指定安装(新版本)**

  显示更新是否具有“未分配安装（新版本）”状态。

- **需要安装的先决条件**

  显示更新是否具有“需要安装先决条件”状态。

- **下载模式**

  显示更新下载的模式。

- **是一个补丁**

  显示更新是否为补丁。

- **未安装**

  显示更新是否具有“未安装”状态。

- “**设置**”选项卡，显示在安装过程中用作命令行参数的安装包设置（名称、描述和值）。如果安装包未提供此类设置，则显示相应的消息。您可以修改这些设置的值。

- “**修订历史**”选项卡，显示安装包版本并包含以下列：

  - **修订**– 安装包的修订号。
  - **时间**– 修改安装包设置的日期和时间。
  - **用户** – 修改安装包设置的用户的名称。
  - **操作** – 修订内对安装包执行的操作。
  - **描述** – 与安装包设置更改相关的修订描述。

    默认下，修订描述为空。要添加描述到修订，请选择相关修订，然后单击“**编辑描述**”按钮。在打开的窗口中，输入一些修订描述的文本。

应用程序标签

通过 Kaspersky Security Center，您能够从应用程序注册表中标记应用程序。标签是应用程序标志，可以用于分组或查找应用程序。分配给应用程序的标签可以作为设备分类中的条件。

例如，您可以创建 [浏览器] 标签并将其分配给所有浏览器（例如 Microsoft Internet Explorer、Google Chrome、Mozilla Firefox）。

创建应用程序标签

要创建应用程序标签：

1. 在主菜单中，转到“**操作**”→“**第三方应用程序**”→“**应用程序标签**”。
2. 单击**添加**。
   新标签窗口打开。
3. 输入标签名称。
4. 单击“**确定**”保存更改。

新标签出现在应用程序标签列表。

重命名应用程序标签

要重命名应用程序标签：

1. 在主菜单中，转到“**操作**”→“**第三方应用程序**”→“**应用程序标签**”。
2. 选中要重命名的标签旁边的复选框，然后单击“**编辑**”。
   标签属性窗口打开。
3. 更改标签名称。
4. 单击“**确定**”保存更改。

更新的标签出现在应用程序标签列表。

分配标签到应用程序

要分配一个或多个标签到一个应用程序：

1. 在主菜单中，转到“**操作**”→“**第三方应用程序**”→“**应用程序注册表**”。
2. 单击您要分配标签的应用程序名称。
3. 选择“**标签**”选项卡。
   标签显示所有存在于管理服务器的应用程序标签。对于分配到所选应用程序的标签，“**分配的标签**”列中的复选框处于选中状态。
4. 对于要分配的标签，请选中“**分配的标签**”列中的复选框。
5. 单击“**保存**”保存设置。

标签被分配到应用程序。

从应用程序上删除分配的标签

要从应用程序删除一个或多个标签：

1. 在主菜单中，转到“**操作**” → “**第三方应用程序**” → “**应用程序注册表**”。
2. 单击您要删除标签的应用程序名称。
3. 选择“**标签**”选项卡。

   标签显示所有存在于管理服务器的应用程序标签。对于分配到所选应用程序的标签，“**分配的标签**”列中的复选框处于选中状态。
4. 对于要删除的标签，请清除“**分配的标签**”列中的复选框。
5. 单击“**保存**”保存设置。

标签被从应用程序删除。

已卸载应用程序的标签不被删除。如果您想，您可以手动删除它们。

删除应用程序标签

要删除应用程序标签：

1. 在主菜单中，转到“**操作 → 第三方应用程序 → 应用程序标签**”。
2. 在列表中，选择您想要删除的应用程序标签。
3. 单击“**删除**”按钮。
4. 在打开的窗口中，单击“**确定**”。

应用程序标签被删除。删除的标签被从其分配的所有应用程序上自动删除。

监控和报告

该部分描述了 Kaspersky Security Center 的监控和报告功能。这些功能给您一个基础架构、保护状态和统计信息的总览。

在 Kaspersky Security Center 部署之后或操作过程中，您可以配置监控和报告功能以适应您的需要。

方案：监控和报告

该部分提供在 Kaspersky Security Center 中配置监控和报告功能的方案。

先决条件

在您部署 Kaspersky Security Center 到组织网络中后，您可以开始监控它并生成其功能报告。

组织网络中的监控和报告分步骤进行：

1. **配置设备状态切换**

   熟悉取决于特定条件的设备状态设置。通过更改这些设置，您可以更改带有*严重*或*警告*重要级别的设备数量。当配置设备状态切换时，确保以下：

   - 新设置不与您组织的安全策略信息冲突。
   - 您可以及时对您组织网络中的重要安全事件做出反应。

2. **配置客户端设备上的事件通知**

   说明：

   配置客户端设备上的事件通知（通过邮件、SMS 或运行可执行文件）。

3. **更改您的安全网络对病毒爆发事件的响应**

   您可以在管理服务器属性中更改特定阈值。您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。

4. **对严重、警告、信息通知执行推荐的操作**

   说明：

   对您的组织网络执行推荐的操作

5. **查看您组织网络的安全状态**

   说明：

   - 查看“保护状态”小组件
   - 生成并查看保护状态报告
   - 生成并查看错误报告

6. **定位不被保护的客户端设备**

   说明：

   - 查看新设备小组件
   - 生成并查看保护部署报告

7. **检查客户端设备保护**

说明：

- 根据保护状态和威胁统计类别生成并查看报告
- 启动并查看“严重”事件分类

8. **评估和限制数据库上的事件负载**

   受管理应用程序操作相关的事件信息将被从客户端设备上传输并记录至管理服务器数据库。要降低管理服务器负载，请评估并限制可以存储在数据库中的最大事件数量。

   说明：

   - 数据库空间计算
   - 限制最大事件数量

9. **查看授权许可信息**

   说明：

   - 将“授权许可密钥使用”小组件添加到仪表板并查看
   - 生成并查看授权许可密钥使用报告

结果

完成方案后，您被通知您组织网络的保护，因此可以为进一步保护计划操作。

关于监控和报告的类型

组织网络的安全事件信息存储在管理服务器数据库。基于事件，Kaspersky Security Center Web Console 提供对于您组织网络的以下类型的监控和报告：

- 控制板
- 报告
- 事件分类
- 通知

仪表板

仪表板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

您可以基于 Kaspersky Security Center Web Console 界面上可以配置的设置创建和查看用户定义的事件分类。

通知

通知提醒您事件并帮助您通过执行推荐操作或您认为适当的操作来加速您对这些事件的响应。

仪表板和小部件

本部分包含有关仪表板和仪表板提供的小部件的信息。本节包括有关如何管理小部件和配置小部件设置的说明。

使用仪表板

控制板通过对信息进行图形显示来允许您监控您组织网络的安全趋势。

在 Kaspersky Security Center Web Console 的“**监控和报告**”区域中单击“**控制板**”可打开仪表板。

控制板提供可以自定义的部件。您可以选择大量不同的部件，显示为饼图、表格、图表和列表。部件中显示的信息会自动更新，更新周期为一到两分钟。更新间隔根据不同部件而不同。您可以在任意时刻通过设置菜单在部件上手动刷新数据。

默认下，部件包含存储在管理服务器数据库中的所有事件的信息。

Kaspersky Security Center Web Console 具有以下类别的默认部件集：

- **保护状态**
- **部署**
- **更新**
- **威胁统计**
- **其他**

一些部件具有带链接的文本信息。您可以通过点击链接查看详细信息。

当配置仪表板时，您可以添加您需要的小部件或隐藏您不需要的小部件，更改小部件的大小或外观，移动小部件以及更改它们的设置。

添加小部件到仪表板

要添加小部件到仪表板：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 单击“**添加或还原 Web 小部件**”按钮。
3. 在可用小部件列表，选择您要添加到仪表板的小部件。
   小部件按类别分组。要查看包含在类别中的小部件列表，单击类别名称旁边的臂章图标(>)。
4. 单击“**添加**”按钮。

所选的小部件被添加到仪表板结尾。

您现在可以编辑所添加小部件的展示和参数。

从控制板隐藏工具

要从仪表板隐藏小部件：

1. 在主菜单中，转到“**监控和报告**”→“**控制板**”。
2. 单击您要隐藏的小部件旁边的设置图标（⚙）。
3. 选择**隐藏 Web 小部件**。
4. 在打开的“**警告**”窗口中，单击“**确定**”。

所选小部件被隐藏。稍后，您可以再次添加该小部件到仪表板。

移动工具到控制板

要移动小部件到仪表板：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 单击您要移动的小部件旁边的设置图标（⚙）。
3. 选择**移动**。
4. 单击您要移动小部件的地方。您仅可以选择其他小部件。

所选小部件的地方被清扫。

更改小部件的大小或外观

对于显示图表的小部件，您可以更改其展示–线条图或线形图。对于一些小部件，您可以更改其大小：最小、中度或最大。

要更改小部件展示：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 单击您要编辑的小组件旁边的设置图标（⚙）。
3. 执行以下操作之一：
   - 要显示条形图形式的小组件，请选择“**图表类型：线条**”。
   - 要显示折线图形式的小组件，请选择“**图表类型：线形**”。
   - 要更改小组件占用的区域，请选择以下值之一：
     - **最小**
     - **最小 (仅线条)**
     - **中度 (饼图)**
     - **中度 (线条图)**
     - **最大**

所选小部件的展示被更改。

更改小部件设置

要更改小部件设置：

1. 在主菜单中，转到“**监控和报告** → **控制板**”。
2. 单击您要更改的小组件旁边的“设置”图标 (⚙)。
3. 选择**显示设置**。
4. 在打开的小部件设置窗口，更改所需的小部件设置。
5. 单击“**保存**”保存设置。

所选小部件的设置被更改。

设置集合取决于特定小部件。以下是一些通用设置：

- **Web 小部件范围**（小组件显示其信息的对象集）—例如，管理组或设备分类。
- **选择任务**（小组件显示其信息的任务）。
- **时间间隔**（在小组件中显示信息的时间间隔）—两个指定日期之间；从指定日期到当前日期；或从当前日期减去指定天数。
- **设置状态为"严重"，如果这些被指定**和**设置状态为"警告"，如果这些被指定**（确定交通信号灯颜色的规则）。

更改小部件设置后，您可以手动刷新小部件上的数据。

要刷新小部件上的数据：

1. 在主菜单中，转到"**监控和报告**" → "**控制板**"。
2. 点击您要移动的工具旁边的设置图标（⚙）。
3. 选择**刷新**。

小部件上的数据得到刷新。

关于仅仪表板模式

您可以为不管理网络但希望在 Kaspersky Security Center 中查看网络保护统计信息的员工（例如高层管理人员）配置仅仪表板模式。当用户启用此模式后，只会向用户显示带有一组预定义小部件的仪表板。因此，用户可以监视小部件中指定的统计信息，例如，所有受管理设备的保护状态、最近检测到的威胁数量或网络中最常见的威胁列表。

当用户在仅仪表板模式下工作时，将应用以下限制：

- 主菜单不向用户显示，因此用户无法更改网络保护设置。
- 用户不能对小部件执行任何操作，例如，添加或隐藏小部件。因此，您需要将用户需要的所有小部件都放在仪表板上并进行配置，例如，设置对象计数规则或指定时间间隔。

您不能为自己分配仅仪表板模式。如果要在此模式下工作，请联系系统管理员、受管理服务提供商 (MSP) 或在"**常规功能：用户权限**"功能区域中拥有"**修改对象 ACL**"权限的用户。

配置仅仪表板模式

在开始配置仅仪表板模式之前，确保满足以下先决条件：

- 您在“**常规功能：用户权限**”功能区域中拥有“**修改对象 ACL**”权限。如果您没有此权限，则用于配置模式的选项卡将缺失。
- 您在“**常规功能：基本功能**”功能区域中拥有“**读取**”权限。

如果您的网络中安排了管理服务器层级，若要配置仅仪表板模式，请转到在**用户和角色** → **用户和组** 区域中**用户**选项卡上提供了用户账户的服务器。可以是主服务器或物理从属服务器。无法在虚拟服务器上调整模式。

要配置仅仪表板模式：

1. 在主菜单中，转至**用户和角色** → **用户和组**，然后选择**用户**选项卡。
2. 单击要使用小部件调整仪表板的用户账户名。
3. 在打开的账户设置窗口中，选择“**仪表板**”选项卡。

   在打开的选项卡上，您和用户将看到相同的仪表板。
4. 如果启用了“**在仅仪表板模式下显示控制台**”选项，则对切换按钮进行切换以将其禁用。

   启用此选项后，您也无法更改仪表板。禁用该选项后，您可以管理小部件。
5. 配置仪表板外观。“**仪表板**”选项卡上准备的小部件级供具有可自定义账户的用户使用。用户不能更改小部件的任何设置或大小，也不能从仪表板添加或删除任何小部件。因此，请为用户调整好，以便用户可以查看网络保护统计信息。为此，在“**仪表板**”选项卡上，可以对小部件执行与在“**监控和报告**”→“**控制板**”区域中相同的操作：
   - 向仪表板添加新的小部件。
   - 隐藏用户不需要的小部件。
   - 移动小部件到特定文件夹。
   - 更改小部件的大小或外观。
   - 更改小部件设置。
6. 对切换按钮进行切换以启用“**在仅仪表板模式下显示控制台**”选项。

   之后，只有仪表板可供用户使用。用户可以监视统计信息，但不能更改网络保护设置和仪表板外观。由于为您显示的仪表板与为用户显示的仪表板相同，您也无法更改仪表板。

   如果禁用该选项，则会为用户显示主菜单，因此用户可以在 Kaspersky Security Center 中执行各种操作，包括更改安全设置和小部件。
7. 完成配置仅仪表板模式后，单击“**保存**”按钮。只有这样，准备好的仪表板才会显示给用户。
8. 如果用户想要查看支持的卡巴斯基应用程序的统计信息并需要访问权限来执行此操作，请为用户配置权限。之后，卡巴斯基应用程序数据将在这些应用程序的小部件中显示给用户。

现在用户可以在自定义账户下登录 Kaspersky Security Center 并在仅仪表板模式下监视网络保护统计信息。

报告

本部分介绍如何使用报告、管理自定义报告模板、使用报告模板生成新报告以及创建报告交付任务。

使用报告

报告功能允许您获取您组织网络的详细安全数字信息、保存该信息到文件、通过邮件发送它和打印它。

在 Kaspersky Security Center Web Console 的“**监控和报告**”区域中单击“**报告**”可打开报告。

默认下，报告包含 30 天内的信息。

Kaspersky Security Center 具有以下类别的默认报告集：

- **保护状态**
- **部署**
- **更新**
- **威胁统计**
- **其他**

您可以创建自定义报告模板、编辑报告模板和删除它们。

您可以基于现有模板创建报告、导出报告到文件和创建报告传送任务。

创建报告模板

要创建报告模板：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”
2. 单击**添加**。
   程序将启动“新报告模板向导”。使用“**下一步**”按钮继续向导操作。
3. 输入报告名称并选择报告类型。
4. 在向导的“**范围**”步骤中，选择基于该报告模板，其数据会显示在报告中的客户端设备集合（管理组、设备分类、所选设备或所有网络设备）。

5. 在向导的“**报告周期**”步骤中，指定报告期间。有以下可用值：

   - 在两个指定日期之间
   - 从指定日期到报告创建日期
   - 从报告创建日期减去指定天数，到报告创建日期

   该页对一些报告可能不显示。

6. 单击“**确定**”关闭向导。

7. 执行以下操作之一：

   - 单击“**保存和运行**”按钮以保存新报告模板并基于其运行报告。
     报告模板被保存。报告被生成。
   - 单击“**保存**”按钮保存新报告模板。
     报告模板被保存。

您可以使用新模板来生成和查看报告。

查看和编辑报告模板属性

您可以查看和编辑报告模板的基本属性，例如，报告模板名称或显示在报告中的字段。

要查看和编辑报告模板属性：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。

2. 选中您要查看和编辑其属性的报告模板旁边的复选框。
   另外，您可以先生成报告，然后单击“**编辑**”按钮。

3. 单击**打开报告模板属性**按钮。
   “**编辑报告 <报告名称>**”窗口打开，其中已选择“**常规**”选项卡。

4. 编辑报告模板属性：

   - “**常规**”选项卡：

     - 报告模板名称
     - **显示条目的最大数量**

       如果启用该选项，显示在表格中的带有详细报告数据的条目数量不超过指定值。

       报告条目首先根据报告模板属性的**字段** → **详细资料字段**区域中指定的规则进行排序，然后仅保存第一个结果条目。带有详细报告数据的表头展示显示的条目数量和匹配其他报告模板设置的可用条目总数。

       如果禁用该选项，带有详细报告数据的表显示所有可用条目。我们不建议您禁用该选项。限制显示的报告条目数量降低数据库管理系统 (DBMS) 负载，也降低生成和导出报告的所需时间。一些报告包含太多条目。如果是这样，您可能难于阅读和分析所有。而且，您的设备可能在生成此报告时内存不够，进而您将无法查看报告。

默认情况下已启用该选项。默认值是 1000。

- **组**

  单击“**设置**”按钮以更改为其创建报告的客户端设备集合。对于一些报告类型，按钮可能不可用。实际设置取决于创建报告模板时指定的设置。

- **时间间隔**

  单击“**设置**”按钮以修改报告周期。对于一些报告类型，按钮可能不可用。有以下可用值：

  - 在两个指定日期之间
  - 从指定日期到报告创建日期
  - 从报告创建日期减去指定天数，到报告创建日期

- **包含来自从属和虚拟管理服务器的数据**

  如果启用该选项，报告包含属于创建模板的管理服务器的从属和虚拟管理服务器的信息。

  如果您要仅从当前管理服务器查看数据，禁用该选项。

  默认情况下已启用该选项。

- **嵌套级别**

  报告包含位于当前管理服务器下小于或等于指定嵌套级别的从属和虚拟管理服务器的数据。

  默认值是 1。如果您必须从树中位于低级别的从属管理服务器接收信息，您可能要更改该值。

- **数据等待间隔(分钟)**

  在生成报告之前，创建报告模板的管理服务器等待从属管理服务器的数据指定分钟数。如果在该时间段后未从从属管理服务器接收到数据，报告依然运行。除了实际数据，报告还显示从缓存获取的数据（如果启用了“**缓存从属管理服务器数据**”选项），否则为 **N/A**（不可用）。

  默认值是 5 分钟。

- **缓存从属管理服务器数据**

  从属管理服务器定期传输数据到创建报告模板的管理服务器。传输的数据存储在缓存。

  如果在生成报告时当前管理服务器无法从从属管理服务器接收数据，报告显示从缓存接收的数据。数据传输到缓存的日期也被显示。

  启用该选项允许您查看从属管理服务器信息，即便实时数据无法被获取。然而，所显示数据可能过期。

  默认情况下已禁用该选项。

- **缓存更新频率(小时)**

  从属管理服务器定期传输数据到创建报告模板的管理服务器。您可以指定此时间段（以小时为单位）。如果指定 0 小时，则仅在生成报告时传输数据。

  默认值是 0。

- **从从属管理服务器传输详细信息**

  在生成的报告中，带有详细报告数据的表格包含创建报告模板的管理服务器的从属管理服务器的数据。

  启用该选项减慢报告生成并增加管理服务器之间的流量。然而，您可以在一个报告中查看所有数据。

  除了启用该选项，您可能想分析详细报告数据以检测故障从属管理服务器，然后仅为该故障管理服务器生成相同报告。

  默认情况下已禁用该选项。

- **字段**选项卡

  选择要显示在报告中的字段，使用“**上移**”按钮和“**下移**”按钮更改这些字段的顺序。使用“**添加**”按钮或“**编辑**”按钮指定是否报告中的信息必须排序并按照每个字段进行筛选。

  在“**详细字段过滤器**”区域中，还可以单击“**转换过滤器**”按钮以开始使用扩展筛选格式。通过这种格式可以使用逻辑或运算来组合各个字段中指定的筛选条件。单击该按钮后，“**转换过滤器**”面板在右侧打开。单击“**转换过滤器**”按钮以确认转换。您现在可以使用“**详细资料字段**”区域中的条件来定义转换的筛选器，这些条件通过逻辑或运算进行应用。

  将报告转换为支持复杂筛选条件的格式将使该报告与 Kaspersky Security Center 的早期版本（11 及更早版本）不兼容。此外，转换后的报告将不包含运行此类不兼容版本的从属管理服务器的任何数据。

5. 单击“**保存**”保存设置。
6. 关闭**编辑报告<Report name>**窗口。

更新的报告模板显示在报告模板列表。

导出报告到文件

您可以导出报告到 XML、HTML 或 PDF 文件。

要导出报告到文件：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 选择您要导出到文件的报告旁边的复选框。
3. 单击“**导出报告**”按钮。
4. 在打开的窗口的“**名称**”字段中更改报告文件名。默认下，文件名称与所选的报告模板名称一致。
5. 选择报告文件类型：XML、HTML 或 PDF。
6. 单击“**导出报告**”按钮。

   所选格式的报告将被下载到您的设备—到您设备的默认文件夹—或您浏览器中打开的标准**另存为**窗口将允许您保存文件到您想要的位置。

报告被保存到文件。

生成和浏览报告

要创建和查看报告，请执行以下操作：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 单击要用于创建报告的报告模板的名称。

   将生成并显示使用所选模板的报告。

> 将根据为管理服务器设置的本地化集显示报告数据。

该报告将显示下列数据：

- 在“**概要**”选项卡上：
  - 报告名称和类型、简要描述和报告时间段，以及为哪个设备组生成该报告的相关信息。
  - 图表显示最有代表性的报告数据。
  - 带有计算好的报告指示器的加固表格。
- 在“**详细资料**”选项卡上，显示一个包含详细报告数据的表格。

创建报告发送任务

您可以创建传送所选报告的任务。

要创建报告传送任务：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 选择您要创建报告传送任务的报告模板旁边的复选框。
3. 单击“**创建传送任务**”按钮。
   “新任务向导”启动。使用“**下一步**”按钮继续向导操作。
4. 在向导的“**新任务设置**”步骤中，输入任务名称。
   默认名称为**传送报告**。如果已存在同名任务，则添加序列号 (<N>) 到任务名称中。
5. 在向导的“**报告配置**”步骤中，指定以下设置：
   a. 要使用任务传送的报告模板。
   b. 报告格式：HTML、XLS 或 PDF。
      将报告转换为 PDF 需要 wkhtmltopdf 工具。选择 PDF 选项后，管理服务器会检查设备上是否安装了 wkhtmltopdf 工具。如果未安装该工具，应用程序将显示一条消息，提示必须在管理服务器设备上安装该工具。手动安装该工具，然后继续下一步。

c. 报告是否使用电子邮件连同邮件通知设置一起发送。

您最多可以指定 20 个电子邮件地址。要分隔电子邮件地址，请按 **Enter** 键。您还可以粘贴以逗号分隔的电子邮件地址列表，然后按 **Enter** 键。

d. 报告是否被保存到文件夹，先前在该文件夹中保存的报告是否被覆盖，以及是否使用特定账户访问文件夹（对于共享文件夹）。

6. 在向导的"**配置任务计划**"步骤中，选择任务启动计划。

有以下任务计划选项可用：

- **手动**

  任务不自动运行。您仅可以手动启动。

  默认情况下已选定该选项。

- **每 N 分钟**

  任务定期运行，按照指定分钟数间隔，从任务创建日期的指定时间开始。

  默认下，任务每 30 分钟运行一次，从当前系统时间开始。

- **每 N 小时**

  任务定期运行，按照指定小时数间隔，从指定的日期和时间开始。

  默认下，任务每 6 小时运行一次，从当前系统日期和时间开始。

- **每 N 天**

  任务定期运行，按照指定天数间隔。此外，您可以指定第一个任务运行的日期和时间。如果您为其创建任务的应用程序支持这些附加选项，则这些选项可用。

  默认下，任务每天运行一次，从当前系统日期和时间开始。

- **每 N 星期**

  任务定期运行，按照指定星期数间隔，从指定的星期和时间开始。

  默认下，任务每星期一于当前系统时间运行一次。

- **每月**

  任务定期运行，在指定月日的指定时间。

  在缺少指定日的月份，任务在最后一天运行。

  默认下，任务在每月的第一天运行，在当前系统时间。

- **在指定的日期**

  任务定期运行，在指定月日的指定时间。

默认情况下，开始时间为18:00，且未选择任何日期。

请注意，您选择的是当月的星期几，而不是具体的日期，也不是具体的周数（例如，当月的第一周或第二周）。例如，如果您将光标设置在第一行的**周二**单元格中，这意味着任务将在每月的**第一周**星期二运行。

您可以选择一周中的多个日期。

- **在检测到病毒爆发时**

  任务在"*病毒爆发*"事件发生后运行。选择将监控病毒爆发的应用程序类型。有下列应用程序类型可用：

  - 用于工作站和文件服务器的反病毒
  - 用于周边防护的反病毒
  - 用于邮件系统的反病毒

  默认情况下选定所有应用程序类型。

  您可能想根据报告病毒爆发的安全应用程序类型运行不同的任务。此种情况下，删除您不需要的应用程序类型分类。

- **在完成其他任务时**

  当前任务在其他任务完成后启动。仅当两个任务被分配给同一设备时，此选项才可用。例如，您可能想使用"***Turn on the device***"选项运行开启设备任务，在它完成后，运行*病毒扫描*任务作为触发任务。

  您必须从表中选择触发任务以及该任务必须完成的状态（**成功完成**或**失败**）。

  如有必要，您可以按如下方式搜索、排序和过滤表中的任务：

  - 在搜索栏中输入任务名称，即可根据名称搜索任务。
  - 单击排序图标可按名称对任务进行排序。

    默认情况下，任务按字母顺序升序排列。
  - 单击过滤器图标，在打开的窗口中按组过滤任务，然后单击"**应用**"按钮。

7. 在向导的此步骤中，配置其他任务计划设置：

- 在"**任务计划**"部分中，检查或重新配置先前选择的计划并设置时间间隔、月份或星期中的日期，设置病毒爆发条件或完成另一项任务作为启动任务的触发条件。如果选择了适用的计划，还可以在此部分指定开始时间。
- 在"**附加设置**"部分，指定以下设置：

  - **运行错过的任务**

    该选项决定在任务要启动时客户端设备在网络中不可见时任务的行为。

如果启用该选项，系统将在下一次在客户端设备上运行卡巴斯基应用程序时尝试启动任务。如果任务计划是“**手动**”、“**一次**”或“**立即**”，则设备在网络中变得可见后或包含在任务范围后，会立即启动任务。

如果禁用此选项，则只有计划任务会在客户端设备上运行。对于“**手动**”、“**一次**”和“**立即**”计划，仅在网络上可见的客户端设备上运行任务。例如，您可能想为消耗资源的任务禁用该选项，您仅想在业余时间运行该任务。

默认情况下已禁用该选项。

- **使用任务启动自动随机延迟**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动，即*分布式任务启动*。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  当任务被创建时，根据任务中包含客户端设备的数量，分发启动时间被自动计算。然后，任务总是在计算的开始时间启动。然后当任务设置被编辑或者任务被手动启动时，计算的任务启动时间值被更改。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

- **使用任务启动自动随机延迟间隔**

  如果启用此选项，任务将在指定的时间间隔内随机在客户端设备上启动。当计划任务运行时，分布式任务有助于避免客户端设备同时向管理服务器发出大量请求。

  如果该选项被禁用，任务根据计划在客户端设备上启动。

  默认情况下已禁用该选项。默认时间间隔为一分钟。

- **如果任务运行超过该时间则停止**

  在指定时间段过后，任务被自动停止，无论它是否完成。

  如果您想要中断或停止执行时间太长的任务，则启用该选项。

  默认情况下已禁用该选项。默认任务执行时间是 120 分钟。

8. 在向导的“**选择账户以运行任务**”步骤中，指定用于运行任务的用户账户的凭据。
9. 如果要在创建任务后修改其他任务设置，请在向导的“**完成任务创建**”步骤中启用“**创建完成时打开任务详情**”选项。
10. 单击“**完成**”按钮创建任务并关闭向导。

    报告传送任务被创建。如果启用了“**创建完成时打开任务详情**”选项，任务设置窗口会打开。

删除报告模板

要删除一个或几个报告模板：

1. 在主菜单中，转到“**监控和报告**”→“**报告**”。
2. 选择您要删除的报告模板旁边的复选框。

3. 单击“**删除**”按钮。

4. 在打开的窗口中，单击“**确定**”以确认您的选择。

所选报告模板被删除。如果这些报告模板被包含在报告传送任务中，它们也被从任务删除。

事件和事件选择

本节提供有关事件和事件选择、Kaspersky Security Center 组件中发生的事件类型以及管理频繁事件阻止的信息。

关于 Kaspersky Security Center 事件

Kaspersky Security Center 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。事件信息保存在管理服务器数据库。

事件类型

Kaspersky Security Center 中有以下类型的事件：

- 常规事件。这些事件发生在所有受管理卡巴斯基应用程序中。常规事件的一个示例是病毒爆发常规事件具有严格定义的语法和语义。常规事件用于报告和仪表板等方面。
- 受管理卡巴斯基应用程序特定事件。每个受管理 Kaspersky 应用程序都拥有自己的事件集。

事件源

以下应用程序可以生成事件：

- Kaspersky Security Center 组件：
  - 管理服务器
  - 网络代理
  - iOS MDM 服务器
  - Exchange 移动设备服务器
- 受管理的卡巴斯基应用程序

  有关受管理卡巴斯基应用程序生成的事件的详细信息，请参阅相应应用程序的文档。

您可以在应用程序策略的“**事件配置**”选项卡上查看应用程序可以生成的事件的完整列表。对于管理服务器，您还可以在管理服务器属性中查看事件列表。

事件的重要级别

每个事件都有自己的重要级别。取决于发生的条件，一个事件可以被分配不同的重要级别。四个事件重要级别如下：

- *严重事件*指示发生了可能导致数据丢失、操作系统异常或严重错误的严重问题。
- *功能失败*指示在应用程序操作中或执行过程中发生了严重问题、错误或功能异常。
- *警告*是不严重的事件，但是也指示了今后可能发生的潜在问题。如果在事件发生后应用程序可以被恢复而不丢失数据或功能，则这些事件是警告级别。
- *信息*事件用于提示成功完成操作、应用程序的正常功能或完成了某过程。

每个事件都有一个存储期限，在这时间内您可以在 Kaspersky Security Center 中查看或修改。一些事件默认下不保存在管理服务器数据库，因为它们的存储期限是零。仅可以在管理服务器数据库中保存至少一天的事件可以被导出到外部系统。

使用事件分类

事件分类提供了从管理服务器数据库中选择的指定事件集合的屏幕视图。这些事件集根据以下类别进行分组：

- 按重要级别—**严重事件**、**功能失败**、**警告**和**信息事件**
- 按时间—**最近事件**
- 按类型—**用户请求**和**审计事件**

您可以基于 Kaspersky Security Center Web Console 界面上可以配置的设置创建和查看用户定义的事件分类。

在 Kaspersky Security Center Web Console 的“**监控和报告**”区域中单击“**事件分类**”可使用事件分类。

默认下，事件分类包含 7 天内的信息。

Kaspersky Security Center 拥有默认的事件分类集：

- 不同重要级别的事件：
  - **严重事件**
  - **功能失败**
  - **警告**
  - **信息事件**
- **用户请求**（受管理应用程序事件）
- **最近事件**（上周）
- **审计事件**。

您也可以创建和配置附加用户定义分类。在用户定义分类中，您可以根据设备属性（设备名称、IP 范围和管理组）、根据事件类型和严重级别、根据应用程序和组件名称、以及根据时间间隔来筛选事件。也可以包含任务结果到搜索范围。您也可以单一搜索字段，可以输入一个词或几个词。所有属性（例如事件名称、描述、组件名称）中包含任意所输入词的事件被显示。

对于预定义和用户定义的分类，您可以限制显示事件的数量或者要搜索的记录的数量。两个选项都影响 Kaspersky Security Center 显示事件所花费的时间。数据库越大，过程越耗时。

您可以执行以下操作：

- 编辑事件分类的属性
- 生成事件分类
- 查看事件分类的详细信息
- 删除事件分类
- 从管理服务器数据库中删除事件

创建事件分类

要创建事件分类，请执行以下操作：

1. 在主菜单中，转到“**监控和报告**”→“**事件分类**”。
2. 单击**添加**。
3. 在打开的“**新事件分类**”窗口中，指定新事件分类的设置。在窗口中重复此操作。
4. 单击“**保存**”保存设置。
   确认窗口打开。
5. 要查看事件分类结果，请保持“**转到分类结果**”复选框为选中状态。
6. 单击“**保存**”确认事件分类创建。

如果将“**转到分类结果**”复选框保持选中状态，将显示事件分类结果。否则，新事件分类出现在事件分类列表。

编辑事件分类

要编辑事件分类：

1. 在主菜单中，转到“**监控和报告**”→ “**事件分类**”。
2. 选中您要编辑的事件分类旁边的复选框。
3. 单击“**属性**”按钮。
   事件分类设置窗口打开。

4. 编辑事件分类属性。

> 对于预定义的事件分类，只能编辑以下选项卡上的属性：**常规**（除了分类名称）、**时间**和**访问权限**。

对于用户定义分类，您可以编辑所有属性。

5. 单击“**保存**”保存设置。

编辑的事件分类显示在列表。

查看事件分类列表

要查看事件分类：

1. 在主菜单中，转到“**监控和报告**”→ “**事件分类**”。
2. 选择您要启动的事件分类旁边的复选框。
3. 执行以下操作之一：
   - 如果您要在事件分类结果中配置排序，做以下：
     a. 单击**重新配置排序并开始**按钮。
     b. 在显示的“**重新配置事件分类排序**”窗口中，指定排序设置。
     c. 单击分类的名称。
   - 否则，如果想要以事件在管理服务器上的顺序查看事件列表，请单击分类名称。

事件分类结果被显示。

导出事件分类

Kaspersky Security Center 允许您将事件分类及其设置保存到 KLO 文件。您可以使用此 KLO 文件将保存的事件分类导入到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

> 请注意，您只能导出用户定义的事件分类。Kaspersky Security Center 默认集中的事件分类（预定义分类）无法保存到文件。

要导出事件分类：

1. 在主菜单中，转到“**监控和报告**”→“**事件分类**”。
2. 选中您要导出的事件分类旁边的复选框。
   您不能同时导出多个事件分类。如果您选择了多个分类，**导出**按钮将被禁用。
3. 单击“**导出**”按钮。

4. 在打开的“**另存为**”窗口中，指定事件分类文件名和路径，然后单击**保存**按钮。

   仅当您使用 Google Chrome、Microsoft Edge 或 Opera 时，才会显示“**另存为**”窗口。如果您使用其他浏览器，则事件分类文件会自动保存在“**下载**”文件夹。

导入事件分类

Kaspersky Security Center 允许您从 KLO 文件导入事件分类。KLO 文件包含导出的事件分类及其设置。

要导入事件分类：

1. 在主菜单中，转到**监控和报告 → 事件分类**。
2. 单击“**导入**”按钮，然后选择要导入的事件分类文件。
3. 在打开的窗口中，指定 KLO 文件的路径，然后单击“**打开**”按钮。请注意，您仅可选择一个事件分类文件。

   事件分类处理开始。

出现包含导入结果的通知。如果事件分类导入成功，您可以单击**查看导入详细信息**链接来查看事件分类属性。

成功导入后，事件分类会显示在分类列表中。事件分类的设置也会被导入。

> 如果新导入的事件分类与现有事件分类有相同的名称，则导入的分类在名称后会附加一个 **(<下一个序列号>)** 索引，例如：**(1)**、**(2)**。

查看事件详情

要查看事件详情：

1. 启动事件分类。
2. 单击所需事件的时间。

   “**事件属性**”窗口打开。
3. 在显示的窗口中，您可以做以下：
   - 查看关于所选事件的信息
   - 在事件分类结果中转到上一个事件和下一个事件
   - 转到发生事件的设备
   - 转到包含发生事件的设备的管理组
   - 对于任务相关事件，转到任务属性

导出事件到文件

Kaspersky Security Center 可让您将事件分类中的事件保存到 TXT 文件。

要导出事件到文件：

1. 启动事件分类。
2. 选择所需事件旁边的复选框。
   您还可以选择多个事件或整个事件分类。
3. 单击“**导出到文件**”按钮。

   所选事件被导出到 TXT 文件。

从事件查看对象历史

从创建或修改支持修订管理的对象的事件，您可以切换到对象的修订历史。

要从事件查看对象历史：

1. 启动事件分类。
2. 选择所需事件旁边的复选框。
3. 单击**修订历史**按钮。

   对象修订历史被打开。

删除事件

要删除一个或几个事件：

1. 启动事件分类。
2. 选择所需事件旁边的复选框。
3. 单击“**删除**”按钮。

   所选事件被删除且无法恢复。

删除事件分类

您仅可以删除用户定义的事件分类。预定义事件分类无法被删除。

要删除一个或几个事件分类：

1. 在主菜单中，转到“**监控和报告**” → “**事件分类**”。
2. 选择您要删除的事件分类旁边的复选框。
3. 单击**删除**。
4. 在打开的窗口中，单击“**确定**”。

事件分类被删除。

设置事件存储期限

Kaspersky Security Center 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。事件信息保存在管理服务器数据库。您可能需要将某些事件存储比默认值指定的时间更长或更短的时间。您可以更改事件存储期限的默认设置。

如果您无意将某些事件存储在管理服务器的数据库中，则可以在管理服务器策略和卡巴斯基应用程序策略或在管理服务器属性（仅对于管理服务器事件）中禁用相应设置。这将降低数据库中的事件类型数量。

事件的存储期限越长，数据库达到最大值速度越快。但是，事件的存储期限越长，执行监控和报告任务的时间就越长。

要为管理服务器中的事件设置存储期限：

1. 在主菜单中，转到“ **资产(设备)**” → “**策略和配置文件**“。
2. 单击所需策略的名称。

   您可以选择受管理卡巴斯基应用程序、网络代理或管理服务器的策略。对于管理服务器，您还可以通过单击位于所需管理服务器名称旁边设置图标 ( ) 来配置事件的存储期限。
3. 选择**事件配置**选项卡。

   将显示与“**严重**”区域有关的事件类型列表。如果需要，您可以移动到**功能失败**、**警告**或**信息**部分。
4. 在右侧面板中的事件类型列表中，单击您要更改其存储期限的事件的链接。

   在打开的窗口的“**事件注册**”区域中，启用“**存储在管理服务器数据库上(天)**”切换开关按钮。
5. 在该开关按钮下面的编辑框中，输入存储事件的天数。

6. 如果您不希望在管理服务器数据库中存储事件，请禁用“**存储在管理服务器数据库上(天)**”选项。

> 如果您在管理服务器属性窗口中配置管理服务器事件，并且在 Kaspersky Security Center 管理服务器策略中锁定了事件设置，则无法重新定义事件的存储期限值。

7. 单击**确定**，然后在右侧窗格关闭后，单击**保存**按钮。

   策略的属性窗口关闭。

从现在开始，当管理服务器接收并存储选定类型的事件时，它们将具有更改的存储期限。管理服务器不会更改以前接收的事件的存储期限。

Kaspersky Security Center 组件事件

每个 Kaspersky Security Center 组件都拥有自己的事件类型集。本节列出了 Kaspersky Security Center 管理服务器、网络代理和 iOS MDM 服务器中发生的事件类型。Kaspersky 应用程序中发生的事件类型不在此区域列出。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

事件类型描述的数据结构

对于每个事件类型，它的显示名称、ID、字母码、描述和默认存储期限被提供。

- **事件类型显示名称**。该文本当您配置事件时和它们发生时被显示在 Kaspersky Security Center 中。
- **事件类型 ID**。该数码在您使用第三方工具分析事件时使用。
- **事件类型**（字母码）。该代码用于您使用 Kaspersky Security Center 数据库中提供的公共视图浏览和处理事件时以及事件被导出到 SIEM 系统时。
- **描述**。该文本包含事件发生的情况以及此种情况下您可以做的事。
- **默认存储期限**。这是事件存储在管理服务器数据库的天数，显示在管理服务器事件列表中。该时间段之后，事件被删除。如果事件存储期限值是 0，此类事件被检测但不显示在管理服务器事件列表。如果您配置了保存此类事件到操作系统事件日志，您可以在那里找到它们。

  您可以更改事件存储期限：

  - 管理控制台：设置事件存储期限
  - Kaspersky Security Center Web Console：设置事件存储期限

其他数据可能包含以下字段：

- **Event_id:** ：事件在数据库中的唯一号，被自动生成和分配；不要与**事件类型 ID**混淆。
- **Task_id:** ：导致事件（如果有）的任务 ID
- **严重性**：以下严重级别之一（按严重性升序排列）：

  0) 无效的严重级别

1) 信息
2) 警告
3) 错误
4) 严重

管理服务器事件

该部分包含管理服务器相关事件信息。

管理服务器严重事件

下表显示了具有“**严重**”重要级别的 Kaspersky Security Center 管理服务器事件类型。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

如果您在管理控制台的管理服务器属性窗口中指定了端口，**Kaspersky Security Center 会发布其指标**和关键事件，以供 Prometheus（一个用于监控和警报的系统）获取。Prometheus 获取指标和关键事件，然后为每个事件生成警报。

```
// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"
```

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

管理服务器严重事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
已超过授权许可数量限制	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	每天，Kaspersky Security Center 检查是否超过授权许可限制。 当管理服务器发现安装在客户端设备上的 Kaspersky 应用程序超过了授权许可限制，以及由单一授权许可覆盖的当前使用的授权许可单元数量超过了该授权许可覆盖的单元总数的 110%，则该类型的事件发生。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Security Center 决定当授权许可限制被超过时生成事件的规则。	180 天
病毒爆发	26 (对于文件威胁防护)	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。 您可以通过以下方式响应事件： • 您可以在管理服务器属性中配置阈值。 • 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。	180 天
病毒爆发	27 (对于邮件威胁防护)	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。 您可以通过以下方式响应事件： • 您可以在管理服务器属性中配置阈值。 • 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。	180 天
病毒爆发	28 (对于防火墙)	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测到的恶意对象数量超过阈值时，该类型的事件发生。 您可以通过以下方式响应事件： • 您可以在管理服务器属性中配置阈值。 • 您还可以创建将被激活的更严格策略，或者创建将在发生此事件时运行的任务。	180 天
设备已失去管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理设备在网络中可见，但指定时间未连接到管理服务器，则该类型的事件发生。 找到什么阻止了设备上网络代理的正常功能。可能的原因包括网络问题和从设备卸载网络代理。	180 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
设备状态是“严重”	4113	KLSRV_HOST_STATUS_CRITICAL	当受管理设备被分配*严重*状态时，该类型的事件发生。您可以配置设备状态被更改到*严重*的条件。	180 天
密钥文件已被添加到拒绝列表	4124	KLSRV_LICENSE_BLACKLISTED	当 Kaspersky 已将您使用的激活码或密钥文件添加到拒绝列表时，会发生该类型事件。 联系技术支持获得更多详情。	180 天
受限制功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	当 Kaspersky Security Center 开始用基本功能操作，没有“漏洞和补丁管理”和“移动设备管理”功能时，该类型的事件发生。 以下是事件发生的原因和正确响应： • 授权许可期限已过期。提供授权许可以使用 Kaspersky Security Center 的完整功能模式（添加有效的激活码或密钥文件到管理服务器）。 • 管理服务器管理比授权许可限制更多的设备。从管理服务器的管理组移动设备到其他管理服务器的管理组（如果其他管理服务器的授权许可限制允许）。	180 天
授权许可即将过期	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	当商业授权许可的失效日期即将到来时，会发生此类事件。 Kaspersky Security Center 每天检查一次授权许可到期日期是否临近。此类型的事件在授权许可到期之前 30 天、15 天、5 天 和 1 天发布。您不能更改天数。如果管理服务器在授权许可到期日之前的指定日期被关闭，则事件直到第二天才发布。 当商业授权许可到期时，Kaspersky Security Center 仅提供基本功能。 您可以通过以下方式响应事件： • 请确保将备用授权许可密钥添加到管理服务器中。 • 如果您使用订阅，请确保续订。如果无限制订阅已在到期日前预付费给服务提供商，则该订阅会自动续订。	180 天
证书已过期	4132	KLSRV_CERTIFICATE_EXPIRED	当移动设备上的客户端移动证书过期时，就会发生此类事件。	180 天
管理服务器证书已过期。	6129	ServerCertificateExpired	当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。 您需要更新过期的证书。	180 天
卡巴斯基应用程序模块更新已撤销	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	如果无缝更新被 Kaspersky 技术专家撤销（这些更新显示“*已撤销*”状态），例如它们必须更新到新版本，则会发生该类型事件。该事件涉及 Kaspersky Security Center 补丁，但不涉及受管理 Kaspersky 应用程序的模块。事件提供无缝更新未被安装的原因。	180 天
审计：导出到 SIEM 失败	5130	KLAUD_EV_SIEM_EXPORT_ERROR	当由于与 SIEM 系统的连接错误而将事件导出到 SIEM 系统失败时，会发生此类事件。	180 天

管理服务器功能失败事件

下表显示了具有“**功能失败**”重要级别的 Kaspersky Security Center 管理服务器事件类型。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器功能失败事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
运行时错误	4125	KLSRV_RUNTIME_ERROR	由于未知问题，该类型的事件发生。 多数情况下，这些是 DBMS 问题、网络问题和其他软件和硬件问题。 事件详情可以在事件描述中找到。	180 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
已授权应用程序组之一的安装已超过限制	4126	KLSRV_INVLICPROD_EXCEDED	管理服务器定期生成该类型的事件（每小时）。如果您在 Kaspersky Security Center 中管理第三方应用程序的授权许可密钥，并且安装数量超过了第三方应用程序授权许可密钥所设置的限制，则会发生该类型事件。 您可以通过以下方式响应事件： • 查看受管理设备列表。从未使用第三方应用程序的设备上删除该应用程序。 • 为更多设备使用第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。这是一组由满足您所设标准的第三方应用程序组成的授权应用程序群组。	180 天
轮询云段失败	4143	KLSRV_KLCLOUD_SCAN_ERROR	当管理服务器无法在云环境中轮询网段时，将发生此类事件。读取事件描述中的详细信息，并相应做出响应。	未存储
将更新复制到指定文件夹失败	4123	KLSRV_UPD_REPL_FAIL	当软件更新被复制到附加共享文件夹时，该类型的事件发生。 您可以通过以下方式响应事件： • 检查用于获取文件夹访问的用户账户是否具有写权限。 • 检查文件夹的用户名和/或密码是否被更改。 • 检查互联网连接，因为它可能是事件原因。遵照指示更新数据库和软件模块。	180 天
没有剩余硬盘空间	4107	KLSRV_DISK_FULL	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	180 天
共享文件夹不可用	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理服务器共享文件夹不可用，则该类型的事件发生。 您可以通过以下方式响应事件： • 检查管理服务器(共享文件夹所在位置)是否已开启并可用。 • 检查文件夹的用户名和/或密码是否被更改。 • 检查网络连接。	180 天
管理服务器数据库不可用	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理服务器数据库不可用则该类型的事件发生。 您可以通过以下方式响应事件： • 检查安装了 SQL Server 的远程服务器是否可用。 • 查看 DBMS 日志以发现管理服务器数据库不可用的原因。例如，因为维护，安装了 SQL Server 的远程服务器可能不可用。	180 天
管理服务器数据库空间不足	4110	KLSRV_DATABASE_FULL	当管理服务器数据库没有剩余空间时，该类型的事件发生。 当管理服务器的数据库达到其容量，以及当不可能再往数据库记录时，管理服务器不工作。 以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应： • 您使用 SQL Server Express 版本 DBMS： 在 SQL Server Express 文档中，查看所用版本的数据库大小限制。可能您的管理服务器数据库已超过了数据库大小限制。 限制存储在管理服务器数据库的事件数量。 在管理服务器数据库中有太多由应用程序控制组件发送的事件。您可以更改与管理服务器数据库中的应用程序控制事件存储有关的 Kaspersky Endpoint Security for Windows 策略的设置。 • 您使用 DBMS 而不是 SQL Server Express Edition： 不限制存储在管理服务器数据库的事件数量。 降低存储在管理服务器数据库的事件数量。 在 DBMS 选项处查看信息。	180 天

管理服务器警告事件

下表显示了具有“**警告**”重要级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器警告事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
已检测到频繁事件		KLSRV_EVENT_SPAM_EVENTS_DETECTED	当管理服务器在受管理设备上检测到频繁发生的事件时，会发生这种类型的事件。请参阅以下部分了解详情：阻止频繁事件。	90 天
已超过授权许可数量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	每天，Kaspersky Security Center 检查是否超过授权许可限制。 当管理服务器发现安装在客户端设备上的 Kaspersky 应用程序超过了授权许可限制，以及由单一授权许可覆盖的当前使用的授权许可单元数量达到了该授权许可覆盖的单元总数的 100% 到 110%，则该类型的事件发生。 即便当该事件发生时，客户端设备是被保护的。 您可以通过以下方式响应事件： • 查看受管理设备列表。删除不在使用的设备。 • 为更多设备提供授权许可（添加有效的激活码或密钥文件到管理服务器）。 Kaspersky Security Center 决定当授权许可限制被超过时生成事件的规则。	90 天
设备在网络上已长时间没有活动	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	当受管理设备在一段时间内显示出不活动状态时，会发生此类事件。 这种情况通常发生在受管理设备已解除授权时。 您可以通过以下方式响应事件： • 要从受管理设备列表中手动删除该设备。 • 指定时间间隔，经过该间隔后，使用管理控制台或使用 Kaspersky Security Center Web Console 创建“**设备在网络上已长时间没有活动**”事件。 • 指定使用管理控制台或使用 Kaspersky Security Center Web Console 自动将设备自动从组中删除的时间间隔。	90 天
设备名称冲突	4102	KLSRV_EVENT_HOSTS_CONFLICT	当管理服务器将两台或更多受管理设备视为单台设备时，会发生此类事件。 在受管理设备上使用克隆的硬盘驱动器进行软件部署，而没有将参考设备上的网络代理切换到专用磁盘克隆模式时，通常会发生这种情况。 为避免此问题，请在克隆此设备的硬盘驱动器之前将参考设备上的网络代理切换到磁盘克隆模式。	90 天
设备状态是“警告”	4114	KLSRV_HOST_STATUS_WARNING	当受管理设备被分配*警告*状态时，该类型的事件发生。您可以配置设备状态被更改到*警告*的条件。	90 天
已授权应用程序组之一的安装即将超过限制	4127	KLSRV_INVLICPROD_FILLED	当已授权应用程序组中包含的第三方应用程序安装数量达到授权许可密钥属性中指定的最大允许值的 90% 时，将发生此类事件。 您可以通过以下方式响应事件： • 如果某些受管理设备上未使用第三方应用程序，请从这些设备中删除该应用程序。 • 如果您预计第三方应用程序安装数量将在不久的将来超过允许的最大值，请考虑预先获取更多设备的第三方授权许可。 您可以使用已授权应用程序组的功能管理第三方应用程序的授权许可密钥。	90 天
证书已被请求	4133	KLSRV_CERTIFICATE_REQUESTED	当自动重新颁发移动设备管理证书失败时，将发生此类事件。 以下是事件的可能原因和对事件的适当响应： • 对禁用了“**如果可能，自动重新发布证书**”选项的证书启动自动重新发布。这可能是由于在证书创建过程中发生的错误所致。可能需要手动重新颁发证书。 • 如果使用与公钥基础结构的集成，则原因可能是用于与 PKI 集成和用于颁发证书的账户缺少 SAM-Account-Name 属性。查看账户属性。	90 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
证书已删除	4134	KLSRV_CERTIFICATE_REMOVED	当管理员删除了移动设备管理的任何类型的证书（通用、邮件、VPN）时，会发生此类事件。 删除证书后，通过此证书连接的移动设备将无法连接到管理服务器。 在调查与移动设备管理相关的故障时，此事件可能会有所帮助。	90 天
证书即将过期	6128	ServerCertificateExpiresSoon	当移动设备和 UEFI 设备的管理服务器证书过期时，会发生此类事件。 您需要更新过期的证书。	90 天
APNs 证书已过期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	当 APNs 证书过期时，会发生此类事件。 您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。	未存储
APNs 证书即将过期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	当 APNs 证书距离过期不到 14 天时，会发生此类事件。 当 APNs 证书过期时，您需要手动续订 APNs 证书并将其安装在 iOS MDM 服务器上。 我们建议您在过期日期前安排 APNs 证书续订。	未存储
发送 FCM 消息到移动设备失败	4138	KLSRV_GCM_DEVICE_ERROR	当移动设备管理配置为使用 Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器无法处理从管理服务器收到的某些请求时，会发生此类事件。这意味着某些受管理移动设备不会收到推送通知。 读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FCM 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Firebase 服务文档（参见"下游消息错误响应代码"一章）。	90 天
发送 FCM 消息到 FCM 服务器时发生 HTTP 错误	4139	KLSRV_GCM_HTTP_ERROR	当移动设备管理配置为使用 Firebase Messaging (FCM) 连接到具有 Android 操作系统的受管理移动设备，并且 FCM 服务器回复管理服务器请求的 HTTP 代码不是 200（正常）时，会发生此类事件。 以下是事件的可能原因和对事件的适当响应： • FCM 服务器端出现问题。读取事件描述详细信息中的 HTTP 代码，并相应做出响应。有关从 FMC 服务器收到的 HTTP 代码以及相关错误的更多信息，请参阅 Firebase 服务文档（参见"下游消息错误响应代码"一章）。 • 代理服务器端出现问题（如果使用代理服务器）。读取事件描述详细信息中的 HTTP 代码，并相应做出响应。	90 天
发送 FCM 消息到 FCM 服务器失败	4140	KLSRV_GCM_GENERAL_ERROR	使用 Firebase Cloud Messaging HTTP 协议时，由于管理服务器端发生意外错误，而发生此类事件。 读取事件描述中的详细信息，并相应做出响应。 如果您自己找不到问题的解决方案，建议与 Kaspersky 技术支持联系。	90 天
硬盘驱动器剩余空间少	4105	KLSRV_NO_SPACE_ON_VOLUMES	当安装管理服务器的设备的硬盘空间不足时，会发生此类事件。 释放设备上的磁盘空间。	90 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
管理服务器数据库的剩余空间少	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理服务器数据库受限制则该类型的事件发生。如果您不纠正情况，管理服务器数据库就将达到其容量且管理服务器将不工作。 以下是根据您使用的 DBMS，该事件的原因，以及到该事件的正确响应。 您使用 SQL Server Express 版本 DBMS： • 在 SQL Server Express 文档中，查看所用版本的数据库大小限制。可能您的管理服务器数据库即将超过数据库大小限制。 • 限制存储在管理服务器数据库的事件数量。 • 在管理服务器数据库中有太多由应用程序控制组件发送的事件。您可以更改与管理服务器数据库中的应用程序控制事件存储有关的 Kaspersky Endpoint Security for Windows 策略的设置。 您使用 DBMS 而不是 SQL Server Express Edition： • 不限制存储在管理服务器数据库的事件数量 • 降低存储在管理服务器数据库的事件数量 在 DBMS 选项处查看信息。	90 天
到从属管理服务器的连接已中断	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	当与从属管理服务器的连接中断时，会发生此类事件。 读取安装了从属管理服务器的设备上的卡巴斯基事件日志，并相应做出响应。	90 天
到主管理服务器的连接已中断	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	当与主管理服务器的连接中断时，会发生此类事件。 读取安装了主管理服务器的设备上的卡巴斯基事件日志，并相应做出响应。	90 天
已注册卡巴斯基应用程序模块的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	当管理服务器为需要批准安装的受管理设备上安装的 Kaspersky 软件注册新更新时，会发生此类事件。 使用管理控制台或 Kaspersky Security Center Web Console 批准或拒绝更新。	90 天
超过了数据库中事件数的限制，已开始删除事件	4145	KLSRV_EVP_DB_TRUNCATING	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后开始时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储
超过了数据库中事件数的限制，事件已被删除	4146	KLSRV_EVP_DB_TRUNCATED	当从管理服务器数据库删除旧事件在管理服务器数据库达到容量后完成时，该类型的事件发生。 您可以通过以下方式响应事件： • 更改允许存储在管理服务器数据库的事件最大数量 • 降低存储在管理服务器数据库的事件数量	未存储
审计(到 SIEM 服务器的连接测试失败)	5120	KLAUD_EV_SIEM_TEST_FAILED	当 SIEM 服务器的测试连接失败时，会发生此类事件。	30 天
自动颁发证书失败		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	如果为移动设备（在移动协议下运行的设备）创建客户端证书时出现错误，则会发生此事件。	90 天

管理服务器信息事件

下表显示了具有“**信息**”重要级别的 Kaspersky Security Center 管理服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。对于管理服务器，您还可以在管理服务器属性中查看和配置事件列表。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

管理服务器信息事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限	评论
授权许可密钥的 90% 已经使用	4097	KLSRV_EV_LICENSE_CHECK_90	30 天	
已检测到新设备	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 天	

事件类型显示名称	事件类型 ID	事件类型	默认存储期限	评论
设备已被自动添加到组	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 天	
设备已被根据规则自动移动	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 天	
设备已从组中删除：长时间在网络中不活动	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 天	
已授权应用程序组之一的安装即将超过限制(已经使用 95% 以上)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 天	
找到了要发送至卡巴斯基以分析的文件	4131	KLSRV_APS_FILE_APPEARED	30 天	
此移动设备上的 FCM 实例 ID 已被更改	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 天	
更新已被成功复制到指定文件夹	4122	KLSRV_UPD_REPL_OK	30 天	
到从属管理服务器的连接已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 天	
到主管理服务器的连接已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 天	
数据库已更新	4144	KLSRV_UPD_BASES_UPDATED	30 天	
审计：到管理服务器的连接已建立	4147	KLAUD_EV_SERVERCONNECT	30 天	当用户使用管理控制台或 Kaspersky Security Center Web Console 连接到管理服务器时，此类事件会发生。这些事件包括已安装基于 MMC 的管理控制台或 Kaspersky Security Center Web Console 服务器的设备的 IP 地址信息。
审计：对象已修改	4148	KLAUD_EV_OBJECTMODIFY	30 天	该事件追踪以下对象中的更改： • 管理组 • 安全组 • 用户 • 包 • 任务 • 策略 • 服务器 • 虚拟服务器
审计：对象状态已更改	4150	KLAUD_EV_TASK_STATE_CHANGED	30 天	例如，当任务以错误失败时会发生该事件。
审计：组设置已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	30 天	
审计：到管理服务器的连接已终止	4151	KLAUD_EV_SERVERDISCONNECT	30 天	

事件类型显示名称	事件类型 ID	事件类型	默认存储期限	评论
审计：对象属性已被修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 天	该事件追踪以下属性中的更改： • 用户 • 授权许可 • 服务器 • 虚拟服务器
审计：用户权限已被修改	4153	KLAUD_EV_OBJECTACLMODIFIED	30 天	
审计：已从管理服务器导入或导出加密密钥	5100	KLAUD_EV_DPEKEYSEXPORT	30 天	
审计：到 SIEM 服务器的连接测试成功	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 天	当 SIEM 服务器的测试连接成功时，会发生此事件。
备用证书已创建		ServerReserveCertificateCreated	30 天	当管理服务器证书已创建时会发生该事件。
证书续费		ServerCertificateRenewed	30 天	当管理服务器证书已续费时会发生该事件。

仅当针对移动设备和 UEFI 设备的管理服务器服务器证书执行与这些事件对应的操作时，管理服务器才会自动发布**备用证书已创建**和**证书续费**事件，并在管理控制台中显示这些事件。

网络代理事件

该部分包含管网络代理相关事件信息。

网络代理功能失败事件

下表显示了具有“**功能失败**”严重级别的 Kaspersky Security Center 网络代理事件类型。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理功能失败事件

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
更新安装错误	7702	KLNAG_EV_PATCH_INSTALL_ERROR	如果Kaspersky Security Center 组件自动更新和补丁未成功，则该类型的事件发生。事件不包含受管理 Kaspersky 应用程序的更新。 阅读事件描述。管理服务器上的 Windows 问题可能是该事件的原因。如果描述提到 Windows 配置的任何问题，解决该问题。	30 天
安装第三方软件更新失败	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	如果“漏洞和补丁管理”和“移动设备管理”功能正在使用且第三方软件更新未成功，则该类型的事件发生。 检查到第三方软件的链接是否合法。阅读事件描述。	30 天
安装 Windows Update 更新失败	7717	KLNAG_EV_WUA_INSTALL_ERROR	如果 Windows 更新未成功，则该类型的事件发生。在网络代理策略中配置 Windows 更新。 阅读事件描述。在 Microsoft 知识库中查找错误。如果您无法自己解决问题，请联系 Microsoft 技术支持。	30 天
用户管理：错误	7723	KLNAG_EV_USR_MNG_ERR	一般警告事件。	30 天

事件类型显示名称	事件类型 ID	事件类型	描述	默认存储期限
将 sudoers 文件恢复为参考值失败	7726	KLNAG_EV_SUDOER_RESTORED_ERR	事件包含 sudoers 文件替换错误的描述。	30 天
安装根证书失败	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	事件包含证书安装错误的描述。	30 天
移除根证书失败	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	事件包含证书删除错误的描述。	30 天

网络代理警告事件

下表显示具有“**警告**”严重级别的 Kaspersky Security Center 网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理警告事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
在安装软件模块更新期间返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 天
第三方软件更新安装已完成但存在警告	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 天
第三方软件更新安装已延时	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 天
发生了安全问题	549	GNRL_EV_APP_INCIDENT_OCCURED	30 天
KSN 代理已启动。检查 KSN 可用性失败	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 天
用户管理：警告	7722	KLNAG_EV_USR_MNG_WRN	30 天
发现 sudoers 文件与参考值不匹配	7724	KLNAG_EV_SUDOER_DIFFERENT	30 天

网络代理信息事件

下表显示具有“**信息**”严重级别的 Kaspersky Security Center 网络代理事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

网络代理信息事件

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
软件模块更新已成功安装	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
软件模块更新安装已启动	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 天
应用程序已安装	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
应用程序已卸载	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
已安装监控的应用程序	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已卸载监控的应用程序	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已安装第三方应用程序	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 天
已添加新设备	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
设备已被删除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
已检测到新设备	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
设备已被授权	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
Windows 桌面共享：文件已读取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 桌面共享：文件已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 桌面共享：应用程序已启动	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 桌面共享：已启动	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 桌面共享：已停止	7716	KLUSRLOG_EV_WDS_END	30 天

事件类型显示名称	事件类型 ID	事件类型	默认存储期限
第三方软件更新已成功安装	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 天
第三方软件更新安装已开始	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 天
KSN 代理已启动。KSN 可用性检查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天

iOS MDM 服务器事件

该部分包含 iOS MDM 服务器相关事件信息。

iOS MDM 服务器功能失败事件

下表显示具有“**功能失败**”严重级别的 Kaspersky Security Center iOS MDM 服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

iOS MDM 服务器功能失败事件

事件类型显示名称	事件类型	默认存储期限
请求配置文件列表失败	配置文件列表_命令_失败	30 天
安装配置文件失败	安装配置文件_命令_失败	30 天
删除配置文件失败	删除配置文件_命令_失败	30 天
请求 provisioning 配置文件列表失败	PROVISIONING 配置文件列表_命令_失败	30 天
安装 provisioning 配置文件失败	安装 PROVISIONING 配置文件_命令_失败	30 天
删除 provisioning 配置文件失败	删除 PROVISIONING 配置文件_命令_失败	30 天
请求数字证书列表失败	证书列表_命令_失败	30 天
请求已安装应用程序列表失败	已安装应用程序列表_命令_失败	30 天
请求移动设备常规信息失败	设备信息_命令_失败	30 天
请求安全信息失败	安全信息_命令_失败	30 天
锁定移动设备失败	设备锁_命令_失败	30 天
重置密码失败	清除密码_命令_失败	30 天
从移动设备擦除数据失败	擦除设备_命令_失败	30 天
安装应用失败	安装应用程序_命令_失败	30 天
为应用设置兑换代码失败	应用兑换码_命令_失败	30 天
请求受管理应用列表失败	受管理应用程序列表_命令_失败	30 天
删除受管理应用失败	卸载应用程序_命令_失败	30 天
漫游设置已被拒绝	设置漫游设置_命令_失败	30 天
应用操作中发生错误	产品_失败	30 天
命令结果包含无效数据	畸形_命令	30 天
发送推送通知失败	发送_推送_通知_失败	30 天
发送命令失败	发送_命令_失败	30 天
未找到设备	设备_未_发现	30 天

iOS MDM 服务器警告事件

下表显示具有“**警告**”严重级别的 Kaspersky Security Center iOS MDM 服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

iOS MDM 服务器警告事件

事件类型显示名称	事件类型	默认存储期限
检测到连接锁定移动设备的企图	不活动_设备_尝试_已连接	30 天
配置文件已被删除	MDM_配置文件_已_被删除	30 天
检测到重新使用客户端证书的企图	客户端_证书_已_在_使用	30 天
检测到不活动设备	发现_不活动_设备	30 天
兑换代码已请求	需要_兑换_码	30 天
配置文件已被包含到从设备删除的策略	UMDM_配置文件_已_被删除	30 天

iOS MDM 服务器信息事件

下表显示具有“**信息**”严重级别的 Kaspersky Security Center iOS MDM 服务器事件。

对于应用程序可以生成的每个事件，您可以在应用程序策略的**事件配置**选项卡上指定通知设置和存储设置。如果想要一次为所有事件配置通知设置，请在管理服务器属性中配置常规通知设置。

iOS MDM 服务器信息事件

事件类型显示名称	事件类型	默认存储期限
新移动设备已被连接	新_设备_已连接	30 天
配置文件列表已被成功请求	配置文件列表_命令_成功	30 天
配置文件已被成功安装	安装配置文件_命令_成功	30 天
配置文件已被成功删除	删除配置文件_命令_成功	30 天
Provisioning 配置文件列表已被成功请求	PROVISIONING 配置文件列表_命令_成功	30 天
Provisioning 配置文件已被成功安装	安装 PROVISIONING 配置文件_命令_成功	30 天
Provisioning 配置文件已被成功删除	删除 PROVISIONING 配置文件_命令_成功	30 天
数字证书列表已被成功请求	证书列表_命令_成功	30 天
已安装应用程序列表已被成功请求	已安装应用程序列表_命令_成功	30 天
移动设备常规信息已被成功请求	设备信息_命令_成功	30 天
安全信息已被成功请求	安全信息_命令_成功	30 天
移动设备已被成功锁定	设备锁_命令_成功	30 天
密码已被成功重置	清除密码_命令_成功	30 天
数据已被从移动设备成功擦除	擦除设备_命令_成功	30 天
应用已被成功安装	安装应用程序_命令_成功	30 天
兑换代码已为应用成功设置	应用兑换码_命令_成功	30 天
受管理应用列表已被成功请求	受管理应用程序列表_命令_成功	30 天
受管理应用已被成功删除	删除应用程序_命令_成功	30 天
漫游设置已被成功应用	设置漫游设置_命令_成功	30 天

阻止频繁事件

本部分提供有关管理频繁事件阻止和移除阻止频繁事件的信息。

关于阻止频繁事件

单个或多个受管理设备上安装的受管理应用程序（例如 Kaspersky Endpoint Security for Windows）可以将许多相同类型的事件发送到管理服务器。接收频繁事件可能会使管理服务器数据库超载并覆盖其他事件。当接收的事件总数超过指定的数据库限制时，管理服务器将开始阻止最频繁的事件。

管理服务器会自动阻止接收频繁事件。您自己不能阻止频繁事件，也不能选择要阻止的事件。

如果要了解某个事件是否被阻止，可以查看通知列表或者检查该事件是否出现在管理服务器属性的“**阻止频繁事件**”区域中。如果该事件被阻止，可以执行以下操作：

- 如果要防止覆盖数据库，可以继续阻止接收此类事件。
- 例如，如果要查找将频繁事件发送到管理服务器的原因，可以解除阻止频繁事件并继续接收此类事件。
- 如果要继续接收频繁事件直到它们被再次阻止，可以将它们从频繁事件的阻止中移除。

管理频繁事件阻止

管理服务器会阻止自动接收频繁事件，但是您可以解除阻止并继续接收频繁事件。您还可以阻止接收您以前解除阻止的频繁事件。

要管理对频繁事件的阻止：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**阻止频繁事件**”区域。
3. 在“**阻止频繁事件**”区域中：
   - 如果要解除阻止接收频繁事件：
     a. 选择要解除阻止的频繁事件，然后单击“**排除**”按钮。
     b. 单击“**保存**”按钮。
   - 如果要阻止接收频繁事件：
     a. 选择要阻止的频繁事件，然后单击“**阻止**”按钮。
     b. 单击“**保存**”按钮。

管理服务器将接收未阻止的频繁事件，并且不接收被阻止的频繁事件。

移除对频繁事件的阻止

您可以移除对频繁事件的阻止并开始接收它们，直到管理服务器再次阻止这些频繁事件。

要移除对频繁事件的阻止：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**阻止频繁事件**”区域。
3. 在“**阻止频繁事件**”区域中，选择要为其移除阻止的频繁事件类型。
4. 点击“**从阻止删除**”按钮。

该频繁事件将从频繁事件列表中移除。管理服务器将接收此类事件。

从 Kaspersky Security for Microsoft Exchange Server 接收事件

受管理应用程序（例如 Kaspersky Endpoint Security for Windows）运行期间发生的事件的信息被从受管理设备传输到管理服务器数据库并在其中注册。默认情况下，来自 Kaspersky Security for Microsoft Exchange Servers 版本 9.0 MR6 和更早版本的事件不在管理服务器数据库中注册。如果 Kaspersky Security for Microsoft Exchange Servers 版本 9.0 MR6 和更早版本安装在您组织的受管理设备上，并且您希望接收来自此应用程序的事件，请使用 klscflag 实用程序启用此应用程序的事件注册。

要为 Kaspersky Security for Microsoft Exchange Servers 启用事件注册：

1. 在管理服务器设备上，在具有管理员权限的账户下运行 Windows 命令提示符。
2. 将您的当前目录更改为 Kaspersky Security Center 安装文件夹（通常为 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）。
3. 运行以下命令之一：

   - 对于安装在 Windows 服务器故障转移集群上的管理服务器：

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - 对于安装在 Kaspersky Security Center 故障转移群集节点上的管理服务器：

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - 对于未在集群上运行的管理服务器：

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

   Kaspersky Security for Microsoft Exchange Servers 的事件注册已启用。

对于 Kaspersky Security for Microsoft Exchange Server，您无法设置事件的存储期限或选择哪些事件必须保存在管理服务器存储库中。你可以设置可以保存在存储库中的最大事件数。此设置适用于从所有卡巴斯基应用程序接收到的事件。

通知和设备状态

本部分包含有关如何查看通知、配置通知传送、使用设备状态和启用更改设备状态的信息。

使用通知

通知提醒您事件并帮助您通过执行推荐操作或您认为适当的操作来加速您对这些事件的响应。

根据选择的通知方法，有以下类型的通知可用：

- 屏幕通知
- 通过 SMS 通知
- 通过电子邮件通知
- 通过可执行文件或脚本通知

屏幕通知

屏幕通知提醒您按照重要级别分组的事件(*严重*、*警告*和*信息*)。

屏幕通知可以有两种状态之一：

- *已查看*。您已对通知执行推荐操作或您已手动为通知分配该状态。
- *未查看*。您未对通知执行推荐操作或您未手动为通知分配该状态。

默认下，通知列表包含*未查看*状态的通知。

您可以通过查看屏幕通知和实时响应它们来监控您的组织网络。

通过电子邮件、SMS 和可执行文件或脚本通知

Kaspersky Security Center 提供通过发送您认为重要的事件的通知来监控您的组织网络。对任意事件，您可以配置通过电子邮件、SMS 或运行可执行文件或脚本进行通知。

在通过电子邮件或 SMS 接收通知时，您可以决定您对事件的响应。此响应应该最适合您组织的网络。通过运行可执行文件或脚本，您预定义对事件的响应。您也可以认为运行可执行文件或脚本是对事件的首选响应。可执行文件运行后，您可以采取其他步骤响应事件。

查看屏幕通知

您可以通过三种方式查看屏幕上的通知：

- 在“**监控和报告**”→“**通知**”区域中。这里，您可以查看预定义类别的通知。
- 您可以打开单独的窗口。此种情况下，您可以标记通知为已查看。
- 在“**监控和报告**”→“**控制板**”区域上的“**所选严重级别的通知**”小组件中。在小组件中，可以仅查看处于“*严重*”和“*警告*”重要级别的事件通知。

您可以执行操作，例如，可以响应事件。

要查看预定义类别的通知：

1. 在主菜单中，转到“**监控和报告**”→ “**通知**”。
   在左侧面板选择“**所有通知**”类别，右侧面板会显示所有通知。
2. 在左侧面板，选择类别之一：
   - **部署**
   - **设备**
   - **保护**
   - **更新**（这包括有关可下载的 Kaspersky 应用程序的通知和有关已下载的反病毒数据库更新的通知）
   - **漏洞利用防御**
   - **管理服务器**（这仅包含管理服务器相关事件）
   - **有用链接**（这包括 Kaspersky 资源的链接，例如 Kaspersky 技术支持、Kaspersky 论坛、授权许可续费页面或 Kaspersky IT 百科全书）

   所选类别的通知列表被显示。列表包含以下：

- 与通知主题相关的图标：部署 ()、保护 ()、更新 ()、设备管理 ()、漏洞利用防御 ()、管理服务器 ()。
- “通知”重要级别。显示以下重要级别的通知：**关键通知** ()、**警告通知** ()、**信息通知**。列表中的通知按重要级别分组。
- **通知**。这包含通知描述。
- **操作**。这包含建议您执行的快速操作链接。例如，通知单击该链接，您可以转到存储库并安装安全应用程序到设备，或查看设备列表或事件列表。您为通知执行推荐操作之后，该通知被分配*已查看*状态。
- **注册的状态**。这包含从通知被注册到管理服务器到现在为止过去的天数或小时数。

要在单独的窗口中按重要级别查看屏幕通知：

1. 在 Kaspersky Security Center Web Console 的右上角，点击旗帜图标()。

如果旗帜图标具有红点，表示有未查看的通知。

列出通知的窗口被打开。默认情况下，将选择“**所有通知**”选项卡，并且通知按重要级别分组：“*严重*”、“*警告*”和“*信息*”。

2. 选择“**系统**”选项卡。

   将显示“*严重*”( ) 和“*警告*”( ) 重要级别通知的列表。通知列表包含以下：

   - 颜色标记。严重通知标记为红色。警告通知标记为黄色。
   - 指示通知主题的图标：部署 ( )、保护 ( )、更新 ( )、设备管理 ( )、漏洞利用防御 ( )、管理服务器 ( )。
   - 通知描述。
   - 旗帜图标。旗帜图标是灰色的，如果通知被分配了*未查看*状态。当您选择灰色旗帜图标并分配*已查看*状态到通知时，图标更改颜色到白色。
   - 推荐操作的链接。单击该链接后执行推荐操作时，通知的状态为*已查看*。
   - 从通知被注册到管理服务器到现在为止过去的天数。

3. 选择“**更多**”选项卡。

   将显示“*信息*”重要级别通知的列表。

   该列表的组织与“**系统**”选项卡上的列表相同（请参见上面说明）。仅有的不同是没有颜色标记。

您可以通过注册在管理服务器上的日期间隔来筛选通知。使用“**显示过滤器**”复选框来管理筛选器。

要在部件上查看屏幕通知：

1. 在“**控制板**”区域中，选择“**添加或还原 Web 小部件**”。
2. 在打开的窗口中，单击“**其他**”类别，选择“**所选严重级别的通知**”小组件，然后单击“添加”。

   该小组件现在显示在“**控制板**”选项卡上。默认情况下，小组件上显示“*严重*”重要级别的通知。

   您可以单击小组件上的“**设置**”按钮并更改小组件设置以查看“*警告*”重要级别的通知。或者，您可以添加另一个小组件：**所选严重级别的通知**，带有“*警告*”重要级别。

   部件上的通知列表由尺寸限制并包含两个通知。这两个通知是关于最近事件的。

部件上的通知列表包含以下：

- 与通知主题相关的图标：部署 ( )、保护 ( )、更新 ( )、设备管理 ( )、漏洞利用防御 ( )、管理服务器 ( )。
- 通知描述和推荐操作的链接。单击该链接后执行推荐操作时，通知的状态为*已查看*。
- 从通知被注册到管理服务器到现在为止过去的天数或小时数。
- 到其他通知的链接。单击该链接后，您将转到“**监控和报告**”区域的“**通知**”区域中的通知视图。

关于设备状态

Kaspersky Security Center 为每个受管理设备都分配一个状态。具体状态取决于是否满足用户定义的条件。在某些情况下，为设备分配状态时，Kaspersky Security Center 会考虑设备在网络中的可见性标志（请参见下表）。例如，如果某个受管理设备因满足“*数据库已过期*”条件而被分配“*严重*”状态，稍后为设备设置了可见性标志，则该设备被分配“*正常*”状态。如果 Kaspersky Security Center 在两小时内未在网络中找到设备，则该设备的可见性标志将设置为“*不可见*”。

状态如下：

- “*严重*”或“*严重/可见*”
- “*警告*”或“*警告/可见*”
- “*正常*”或“*正常/可见*”

下表列出了为设备分配“*严重*”或“*警告*”状态所必须满足的默认条件，以及所有可能值。

分配状态到设备的条件

条件	条件描述	可用值
安全应用程序未安装	网络代理已安装到设备，但是安全应用程序未安装。	• 开关按钮被开启。 • 开关按钮被关闭。
检测到太多病毒	一些病毒被病毒检测任务在设备上发现，例如，*恶意软件扫描*任务，且发现的病毒数量超过指定值。	超过 0。
实时保护级别与管理员设置的级别不同	设备在网络中可见，但实时保护级别与管理员在设备状态条件中设置的级别不同。	• 已停止。 • 已暂停。 • 正在运行。
恶意软件扫描已长时间未执行	设备在网络中可见且安全应用程序已安装到设备，但不论*恶意软件扫描*任务还是本地扫描任务都没有在指定时间内未运行。条件仅应用到于 7 天之前或更早添加到管理服务器数据库的设备。	超过 1 天。
数据库已过期	设备在网络中可见且安全应用程序已安装到设备，但反病毒数据库在指定时间内未在该设备上更新。条件仅应用到于 1 天之前或更早添加到管理服务器数据库的设备。	超过 1 天。
长时间没有连接	网络代理已安装到设备，但由于设备关闭，设备在指定时间段内未连接到管理服务器。	超过 1 天。
检测到活动威胁	“**活动威胁**”文件夹中的未处理的对象的数量超过指定的值。	超过 0 项。
需要重新启动	设备在网络中可见，但应用程序基于所选原因之一在指定时间之前请求设备重启。	超过 0 分钟。
安装了不兼容的应用程序	设备在网络中可见，但通过网络代理执行的软件清查在设备上检测到了不兼容的应用程序。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到软件漏洞	设备在网络中可见且网络代理已安装到设备，但“*查找漏洞和所需更新*”任务在设备应用程序中检测到指定严重级别的漏洞。	• 严重。 • 高。 • 中。 • 如果漏洞无法被修复则忽略。 • 如果为安装分配了更新则忽略。
授权许可已过期	设备在网络中可见，但授权许可已过期。	• 开关按钮被关闭。 • 开关按钮被开启。
授权许可即将过期	设备在网络中可见，但设备上的授权许可即将在指定天数内过期。	少于 0 天。

条件	条件描述	可用值
Windows Update 更新检查已长时间未执行	设备在网络中可见，但“*执行 Windows 更新同步*”任务在指定时间段内未运行。	超过 1 天。
无效的加密状态	网络代理已安装到设备，但设备加密结果等于指定值。	• 由于用户拒绝未遵从策略(仅对外部设备)。 • 由于错误未遵从策略。 • 应用策略时需要重启。 • 未指定加密策略。 • 不支持。 • 当应用策略时。
移动设备设置不遵从策略	移动设备设置不同于 Kaspersky Endpoint Security for Android 策略中指定的设置。	• 开关按钮被关闭。 • 开关按钮被开启。
检测到未处理的安全问题	设备上发现了一些未处理的安全问题。安全问题可以通过安装在客户端设备上的受管卡巴斯基应用程序自动创建，也可以由管理员手动创建。	• 开关按钮被关闭。 • 开关按钮被开启。
应用程序定义的设备状态	设备状态由受管理应用程序定义。 无论 Kaspersky Security Center 的设置如何，受管理设备的状态都可能由受管理应用程序定义。当此状态返回一个由 Kaspersky Security Center 定义的状态后，管理服务器将为受管理设备分配一个最终状态。该状态选自以下两者中最为严重的一项：受管理应用程序返回的状态和管理服务器分配的状态。受管理应用程序定义的状态会附带由受管理应用程序传输的描述。您可以在受管理设备列表的“**状态描述**”列中查看这些描述。	• 开关按钮被关闭。 • 开关按钮被开启。
设备磁盘空间不足	设备剩余磁盘空间少于指定值或设备无法与管理服务器同步。当设备已与管理服务器成功同步且设备上的剩余空间大于或等于指定值时，*严重*或*警告*状态被更改为*正常*状态。	大于 0 MB。
设备已失去管理	在设备发现过程中，设备在网络中可见，但是超过三次尝试与管理服务器同步都失败了。	• 开关按钮被关闭。 • 开关按钮被开启。
保护已禁用	设备在网络中可见，但设备上的安全应用程序已被禁用长于指定的时间段。 在这种情况下，安全应用程序的状态为*stopped*或*failure*，不同于以下状态：*starting*、*running*或*suspended*。	超过 0 分钟。
安全应用程序没有运行	设备在网络中可见且安全应用程序已安装到设备，但其未在运行。	• 开关按钮被关闭。 • 开关按钮被开启。

Kaspersky Security Center 允许您设置管理组中设备状态在指定条件满足时的自动切换。当指定条件满足时，客户端设备被分配以下状态之一：*严重*或*警告*。未满足指定条件时，客户端设备被分配“*正常*”状态。

一个条件的不同值可对应于不同的状态。例如，默认情况下，如果“**数据库已过期**”条件的值为“**超过 3 天**”，将为客户端设备分配“*警告*”状态；如果值为“**超过 7 天**”，则将分配“*严重*”状态。

如果从以前的版本升级 Kaspersky Security Center，则分配“*严重*”或“*警告*”状态所对应的“**数据库已过期**”状态值不变。

配置设备状态切换

您可以更改条件以将*严重*或*警告*状态分配给设备。

要启用更改设备状态到严重：

1. 在主菜单中，转到“**资产(设备)**”→ “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**严重**”。
5. 在右侧窗格的“**设置状态为“严重”，如果这些被指定**”区域中，启用将设备切换为“*严重*”状态的条件。

   > 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。

满足指定条件时，受管理设备被分配*严重*状态。

要启用更改设备状态到警告：

1. 在主菜单中，转到“**资产(设备)**” → “**组层级**”。
2. 在打开的组列表中，单击包含您要更改其设备状态的组名称的链接。
3. 在打开的属性窗口中，选择“**设备状态**”选项卡。
4. 在左侧窗格中，选择“**警告**”。
5. 在右侧窗格的“**设置状态为“警告”，如果这些被指定**”区域中，启用将设备切换为“*警告*”状态的条件。

   > 您只能更改未在父策略中锁定的设置。

6. 在列表中选中条件旁边的单选按钮。
7. 在列表的左上角，单击“**编辑**”按钮。
8. 为所选条件设置所需的值。
   可以不为每个条件设置值。
9. 单击“**确定**”。

满足指定条件时，受管理设备被分配*警告*状态。

配置通知传送

您可以配置发生在 Kaspersky Security Center 中的事件的通知。根据选择的通知方法，有以下类型的通知可用：

- 电子邮件—当发生事件时，Kaspersky Security Center 向指定的电子邮件地址发送通知。
- SMS—当发生事件时，Kaspersky Security Center 向指定的电话号码发送通知。
- 可执行文件—当事件发生时，可执行文件被运行在管理服务器。

要配置发生在 Kaspersky Security Center 中的事件的通知传送：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口打开，**常规**选项卡被选中。
2. 单击“**通知**”区域，在右侧窗格中选择所需通知方法的选项卡：

- **电子邮件**

“**电子邮件**”选项卡允许您配置通过电子邮件发送的事件通知。

在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。

在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

- IPv4 或 IPv6 地址
- 设备的 Windows 网络名称（NetBIOS 名称）
- SMTP 服务器的 DNS 名称

在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

如果启用“**使用 DNS MX 查找**”选项，则可以将多个 IP 地址 MX 记录用于同一个 SMTP 服务器 DNS 名称。同一 DNS 名称可能有多个 MX 记录，这些记录具有不同的电子邮件接收优先级。管理服务器将尝试按 MX 记录优先级的升序向 SMTP 服务器发送电子邮件通知。

> 如果启用“**使用 DNS MX 查找**”选项但不启用 TLS 设置，建议您将服务器设备上的 DNSSEC 设置用作发送电子邮件通知的额外保护措施。

如果启用“**使用 ESMTP 身份验证**”选项，则可以在“**用户名**”和“**密码**”字段中指定 ESMTP 身份验证设置。默认情况下，该选项被禁用，ESMTP 身份验证设置不可用。

您可以指定 SMTP 服务器连接的 TLS 设置：

- **不使用 TLS**

如果要禁用电子邮件加密，则可以选择此选项。

- **如果 SMTP 服务器支持则使用 TLS**

如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

- **始终使用 TLS，检查服务器证书的有效性**

如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”值，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以单击“**指定证书**”链接来指定用于 TLS 连接的证书：

- 浏览 SMTP 服务器证书文件：

您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

- 浏览客户端证书文件：

您可以使用从任何来源（例如，从任何受信任证书颁发机构）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

- X-509 证书：

您必须指定一个证书文件和一个私钥文件。这两个文件不相互依赖，文件的加载顺序也不重要。加载这两个文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

- pkcs12容器：

您必须上传包含证书及其私钥的单个文件。加载该文件时，必须指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

在“**主题**”字段中，指定电子邮件主题。您可以置此字段为空。

在“**主题模板**”下拉列表中，选择主题的模板。由所选模板确定的变量自动放置在“**主题**”字段中。您可以选择几个邮件模板构建邮件主题。

在“**发件人邮件地址**”字段中，指定发件人电子邮件地址。如果您将该字段置空，收件人地址被使用。不建议使用虚假邮件地址。

“**通知消息**”字段包含事件发生时应用程序发送的事件信息标准文本。该文本包含代替参数，例如事件名称、设备名称和域名。您可以通过添加其他带有更新事件详情的替代参数编辑消息文本。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接允许您指定应用程序在指定时间段可以发送的最大通知数量。

单击“**发送测试消息**”按钮允许您检查是否正确配置了通知：应用程序发送测试通知到您指定的电子邮件地址。

- SMS

“**SMS**”选项卡允许您配置将各种事件的 SMS 通知传输到手机。SMS 消息通过邮件网关发送。

在“**SMTP 服务器**”字段中，指定邮件服务器地址，以分号分隔。您可以使用下列值：

- IPv4 或 IPv6 地址
- 设备的 Windows 网络名称（NetBIOS 名称）
- SMTP 服务器的 DNS 名称

在“**SMTP 服务器端口**”字段中，指定 SMTP 服务器通信端口号。默认端口号是 25。

如果启用“**使用 ESMTP 身份验证**”选项，则可以在“**用户名**”和“**密码**”字段中指定 ESMTP 身份验证设置。默认情况下，该选项被禁用，ESMTP 身份验证设置不可用。

您可以指定 SMTP 服务器连接的 TLS 设置：

- **不使用 TLS**

如果要禁用电子邮件加密，则可以选择此选项。

- **如果 SMTP 服务器支持则使用 TLS**

如果要使用 TLS 连接到 SMTP 服务器，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器不使用 TLS 连接 SMTP 服务器。

- **始终使用 TLS，检查服务器证书的有效性**

如果要使用 TLS 身份验证设置，则可以选择此选项。如果 SMTP 服务器不支持 TLS，则管理服务器无法连接 SMTP 服务器。

建议使用此选项以更好地保护与 SMTP 服务器的连接。如果选择此选项，则可以设置 TLS 连接的身份验证设置。

如果您选择“**始终使用 TLS，检查服务器证书的有效性**”值，则可以指定用于 SMTP 服务器身份验证的证书，并选择要允许通过任意版本的 TLS 还是仅允许通过 TLS 1.2 或更高版本进行通信。此外，还可以指定用于 SMTP 服务器上客户端身份验证的证书。

您可以单击“**指定证书**”链接来指定 SMTP 服务器证书文件：

您可以接收含有受信任证书颁发机构的证书列表的文件，并将该文件上传到管理服务器。Kaspersky Security Center 会检查 SMTP 服务器的证书是否也具有受信任证书颁发机构的签名。如果 SMTP 服务器的证书不是从受信任证书颁发机构接收的，Kaspersky Security Center 将无法连接到 SMTP 服务器。

在“**收件人(电子邮件地址)**”字段中，指定应用程序将通知发送到的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。通知将被传送到指定邮件地址关联的电话号码。

在“**主题**”字段中，指定电子邮件主题。

在“**主题模板**”下拉列表中，选择主题的模板。取决于所选模板的变量放置在“**主题**”字段中。您可以选择几个邮件模板构建邮件主题。

在“**发件人邮件地址：如果未指定该设置，收件人地址将被使用。 警告：我们不建议您使用虚假邮件地址**”字段中，指定发件人电子邮件地址。如果您将该字段置空，收件人地址被使用。不建议使用虚假邮件地址。

在“**SMS 消息收件人电话号码**”字段中，指定短信通知收件人的手机号码。

在“**通知消息**”字段中，指定事件发生时应用程序发送的事件信息文本。该文本可以包含替代参数，例如事件名称、设备名称和域名。

如果通知文本包含百分号（%）字符，您必须指定两次以允许消息发送。例如，“CPU 负载是 100%%”。

单击“**配置通知限制数**”链接可指定应用程序在指定时间段可以发送的最大通知数量。

单击“**发送测试消息**”可检查是否正确配置了通知：应用程序发送测试通知到您指定的收件人。

- **要运行的可执行文件**

  如果选择该通知方法，您可以在输入字段指定事件发生时要启动的应用程序。

  在“**当事件发生时要在管理服务器上运行的可执行文件**”字段中指定要运行的文件的文件夹和名称。在指定文件之前，准备文件并指定定义了要在通知消息中发送的事件详情的占位符。您指定的文件夹和文件必须位于管理服务器上。

  单击“**配置通知限制数**”链接允许您指定应用程序在指定时间段可以发送的最大通知数量。

3. 在选项卡上，定义通知设置。
4. 单击“**确定**”按钮以关闭管理服务器属性窗口。

保存的通知传送设置被应用到在 Kaspersky Security Center 中发生的所有事件。

您可以在管理服务器设置、策略设置或应用程序设置的“**事件配置**”区域中覆盖某些事件的通知传送设置。

通过运行可执行文件显示的事件通知

Kaspersky Security Center 可通过运行可执行文件将客户端设备上发生的事件通知管理员。可执行文件必须包含另外一个可执行文件，而后者具有要转发给管理员的事件的占位符（请见下表）。

描述事件的占位符

占位符	占位符描述
%SEVERITY%	事件严重级别。可能值： • **信息** • **警告** • **错误** • **严重**
%COMPUTER%	发生事件的设备的名称。 设备名称的最大长度为 256 个字符。
%DOMAIN%	发生事件的设备的域名称。
%EVENT%	事件类型的名称。 事件类型名称的最大长度为 50 个字符。
%DESCR%	事件描述。 描述的最大长度为 1000 个字符。
%RISE_TIME%	事件创建时间。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	任务名称。 任务名称的最大长度为 100 个字符。
%KL_PRODUCT%	应用程序名称。
%KL_VERSION%	应用程序版本号。
%KLCSAK_EVENT_SEVERITY_NUM%	事件严重编号。可能值： • 1—**信息** • 2—**警告** • 3—**Error** • 4—**严重**
%HOST_IP%	发生事件的设备的 IP 地址。
%HOST_CONN_IP%	发生事件的设备的连接 IP 地址。

例如：
事件通知由某个可执行文件（例如，script1.bat）发出，在该可执行文件中，将启动具有 %COMPUTER% 占位符的另一个可执行文件（例如，script2.bat）。当发生事件时，将在管理员的设备上运行 script1.bat 文件，而该文件随后运行具有 %COMPUTER% 占位符的 script2.bat 文件。管理员将接收到发生事件的设备的名称。

卡巴斯基公告

本部分介绍如何使用、配置和禁用卡巴斯基公告。

关于 Kaspersky 公告

“Kaspersky 公告”区域（**监控和报告** → **Kaspersky 公告**）提供与您的 Kaspersky Security Center 版本和受管理设备上安装的受管理应用程序相关的信息，让您了解最新动态。Kaspersky Security Center 会定期删除过时的公告并添加新信息来更新该区域中的信息。

Kaspersky Security Center 仅显示与当前连接的管理服务器和该管理服务器的受管理设备上安装的 Kaspersky 应用程序相关的 Kaspersky 公告。对于任何类型的管理服务器（主要、从属或虚拟）都单独显示公告。

管理服务器必须具有互联网连接才能接收 Kaspersky 公告。

公告包括以下类型的信息：

- 与安全相关的公告

  与安全相关的公告旨在使网络中安装的卡巴斯基应用程序保持最新并具有完整功能。公告可能包括有关 Kaspersky 应用程序的关键更新、已发现漏洞的修复以及修复 Kaspersky 应用程序中的其他问题的方法的信息。默认情况下启用与安全相关的公告。如果您不想接收这些公告，可以禁用此功能。

  为了显示与您的网络保护配置相对应的信息，Kaspersky Security Center 会将数据发送到 Kaspersky 云服务器，并仅接收与网络中安装的 Kaspersky 应用程序有关的公告。您安装 Kaspersky Security Center 管理服务器时接受的最终用户授权许可协议中描述了可以发送到服务器的数据集。

- 营销公告

  营销公告包括您的卡巴斯基应用程序的特别优惠信息、广告和 Kaspersky 新闻。默认情况下禁用营销公告。仅当启用卡巴斯基安全网络 (KSN) 时，才会收到此类公告。您可以通过禁用 KSN 来禁用营销公告。

  为了仅向您显示可能对保护网络设备和日常任务有帮助的相关信息，Kaspersky Security Center 会将数据发送到 Kaspersky 云服务器并接收相应公告。KSN 声明的“处理的数据”部分中描述了可发送到服务器的数据集。

新信息根据重要性分为以下几个类别：

1. 关键信息
2. 重要新闻
3. 警告
4. 信息

当“Kaspersky 公告”区域中出现新信息时，Kaspersky Security Center Web Console 将显示一个与公告重要级别相对应的通知标签。您可以单击该标签以在“Kaspersky 公告”区域中查看此公告。

您可以指定 Kaspersky 公告设置，包括您要查看的公告类别以及显示通知标签的位置。

指定 Kaspersky 公告设置

在“Kaspersky 公告”区域中，您可以指定 Kaspersky 公告设置，包括您要查看的公告类别以及显示通知标签的位置。

要配置 Kaspersky 公告：

1. 在主菜单中，转到“**监控和报告**” → “**卡巴斯基通告**”。
2. 单击“**设置**”链接。
   将打开“Kaspersky 公告设置”窗口。
3. 指定下列设置：
   - 选择您要查看的公告的重要级别。其他类别的公告将不会显示。
   - 选择您希望显示通知标签的位置。标签可以显示在所有控制台区域，或“**监控和报告**”区域及其子区域。
4. 单击“**确定**”按钮。
   Kaspersky 公告设置已指定。

禁用 Kaspersky 公告

“Kaspersky 公告”区域（**监控和报告** → **Kaspersky 公告**）提供与您的 Kaspersky Security Center 版本和受管理设备上安装的受管理应用程序相关的信息，让您了解最新动态。如果您不想接收 Kaspersky 公告，可以禁用此功能。

Kaspersky 包括两种类型的信息：与安全相关的公告和营销公告。您可以单独禁用每种类型的公告。

要禁用与安全相关的公告：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**卡巴斯基通告**”区域。
3. 将开关按钮切换到“**安全通告已禁用**”位置。
4. 单击“**保存**”按钮。
   Kaspersky 公告已禁用。

默认情况下禁用营销公告。仅当启用卡巴斯基安全网络 (KSN) 时，才会收到营销公告。您可以通过禁用 KSN 来禁用此类型的公告。

要禁用营销公告：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**KSN 代理设置**”区域。
3. 禁用**使用卡巴斯基安全网络已启用**选项。
4. 单击“**保存**”按钮。
   营销公告已禁用。

查看有关威胁检测的信息

您可以启用或禁用显示有关警报的信息。

*要启用或禁用在主菜单中显示“**警报**”区域：*

1. 在主菜单中，转到您的账户设置，然后选择**界面选项**。
2. 在打开的“**界面选项**”窗口中，启用或禁用“**显示 EDR 警告**”选项。
3. 点击**保存**。

控制台会在主菜单的“**监控和报告**”区域中显示“**警报**”子区域。在“**警报**”子区域中，可以查看有关端点设备上的威胁检测的信息。如果添加了 EDR Optimum 的授权许可密钥，则 Kaspersky Security Center Web Console 会自动在主菜单的“**监控和报告**”区域中显示“**警报**”子区域。您还可以添加小部件来显示有关警报的信息。

> 仅当您在启用**警报**选项之前添加了 EDR Optimum 的授权许可密钥时，才会自动显示**显示 EDR 警告**子部分。如果您在启用**显示 EDR 警告**选项后添加了授权许可密钥，则只有在重新启用此选项后才会显示**警报**子部分。

为了在警报卡中正确显示有关检测到的威胁的详细信息，您必须安装Kaspersky Endpoint Agent 插件以及兼容版本的Kaspersky Endpoint Security 插件（Kaspersky Endpoint Security for Linux 12.1 或更高版本、 Kaspersky Endpoint Security for Mac 12.1 或更高版本、或 Kaspersky Endpoint Security for Windows 12.6 或更高版本）。

使用**筛选器**菜单按日期和字段值筛选警报。

对象类型字段包含以下值：

- 未知
- 钓鱼链接
- 病毒
- 木马
- 恶意工具
- 后门程序

- 蠕虫
- 其他应用程序
- 广告软件
- 色情软件
- 危险打包程序
- 危险行为

自动响应字段包含以下值：

- 检测到恶意对象
- 对象已删除
- 对象已清除
- 对象清除失败
- 对象已移动到隔离
- 检测到密码保护的存档
- 检测到的病毒

Cloud Discovery

通过 Kaspersky Security Center，您可以监控运行 Windows 的受管理设备上云服务的使用情况，并阻止对您认为不需要的云服务进行的访问。Cloud Discovery 跟踪用户通过浏览器和桌面应用程序访问这些服务的尝试。它还会对用户尝试通过未加密的连接（例如，使用 HTTP 协议）来访问云服务的活动进行跟踪。此功能可帮助您检测并阻止影子 IT 对云服务的使用。

仅当您在Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 授权许可下激活 Kaspersky Security Center 时，才可以使用阻止功能。

仅当您使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本时，才可以使用阻止功能。该安全应用程序的较早版本仅允许您监控云服务的使用情况。

您可以启用 Cloud Discovery 功能，并选择要启用该功能的安全策略或配置文件。您也可以在每个安全策略或配置文件中单独启用或禁用该功能。对于您不想让用户访问的云服务，您可以阻止对这些云服务的访问。

为了能够阻止对不需要的云服务进行的访问，请确保满足以下先决条件：

- 您使用的是 Kaspersky Endpoint Security 11.2 for Windows 或更高版本。该安全应用程序的较早版本仅允许您监控云服务的使用情况。
- 您已购买某一级别的 Kaspersky Next 授权许可，因此您可以阻止对不需要的云服务进行的访问。有关详细信息，请参阅 Kaspersky Next 帮助。

Cloud Discovery 小部件和 Cloud Discovery 报告会显示有关成功和被阻止的云服务访问尝试的信息。该小部件还会显示每项云服务的风险级别。Kaspersky Security Center 从所有仅受安全策略或配置文件保护的受管理设备（已启用相关功能）中，获取有关云服务使用情况的信息。

使用小部件启用 Cloud Discovery

Cloud Discovery 功能允许您从所有受安全策略保护的受管理设备（已启用相关功能）中，获取有关云服务使用情况的信息。您只能对 Kaspersky Endpoint Security for Windows 策略启用或禁用 Cloud Discovery。

可通过两种方式来启用 Cloud Discovery 功能：

- 使用 Cloud Discovery 小部件。
- 在 Kaspersky Endpoint Security for Windows 策略属性中。

  有关如何在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能的详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助中的 Cloud Discovery 部分。

请注意，您只能在 Kaspersky Endpoint Security for Windows 策略参数中禁用 Cloud Discovery 功能。

为了启用 Cloud Discovery，您必须在“**常规功能：基本功能**”功能区域中具有**写入**权限。

要使用 Cloud Discovery 小部件启用 Cloud Discovery 功能，请执行以下操作：

1. 转到 Kaspersky Security Center。
2. 在主菜单中，转到“**监控和报告**”→“**控制板**”。
3. 在 **Cloud Discovery** 小部件上，单击“**启用**”按钮。

   如果您安装了 Kaspersky Endpoint Security for Windows 版本 12.4，请在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能。有关详细信息，请参阅 Cloud Discovery 部分。

   如果您的 Kaspersky Endpoint Security for Windows 版本低于 12.4，请将 Kaspersky Endpoint Security for Windows 插件更新至版本 12.5。

4. 在打开的“**启用 Cloud Discovery**”窗口中，选择要启用该功能的安全策略，然后单击“**启用**”按钮。

   以下策略设置将自动启用：**将脚本注入到 Web 流量以与网页进行交互**、**Web 会话监控**和**加密连接扫描**。

Cloud Discovery 功能会启用，小部件会被添加到仪表板。

将 Cloud Discovery 小部件添加到仪表板

您可以将 **Cloud Discovery** 小部件添加到仪表板，以监控受管理设备上云服务的使用情况。

如要将 Cloud Discovery 小部件添加到仪表板，您必须在“**常规功能：基本功能**”功能区域中具有**写入**权限。

要将 Cloud Discovery 小部件添加到仪表板，请执行以下操作：

1. 转到 Kaspersky Security Center。
2. 在主菜单中，转到“**监控和报告**”→“**控制板**”。
3. 单击“**添加或还原 Web 小部件**”按钮。
4. 在可用小部件列表中，单击“**其他**”类别旁边的箭头图标 (>)。
5. 选择 **Cloud Discovery** 小部件，然后单击“**添加**”按钮。

   如果 Cloud Discovery 功能被禁用，请按照“使用小部件启用 Cloud Discovery”部分中的说明进行操作。

所选的小部件会添加到仪表板的末端。

查看有关云服务使用情况的信息

您可以查看 **Cloud Discovery** 小部件，其中会显示有关云服务访问尝试的信息。该小部件还会显示每项云服务的风险级别。Kaspersky Security Center 从所有仅受安全配置文件保护的受管理设备（已启用相关功能）中，获取有关云服务使用情况的信息。

在查看之前，请确保：

- Cloud Discovery 小部件已添加到仪表板。
- Cloud Discovery 功能已启用。
- 您在“**常规功能：基本功能**”功能区域中具有**读取**权限。

要查看 Cloud Discovery 小部件，请执行以下操作：

1. 转到 Kaspersky Security Center。
2. 在主菜单中，转到“**监控和报告**”→“**控制板**”。

   Cloud Discovery 小部件会显示在仪表板上。
3. 在 **Cloud Discovery** 小部件的左侧，选择云服务类别。

   小部件右侧的表格会显示在所选类别中用户最常尝试访问的最多五项服务。成功和被阻止的尝试均会计入尝试。
4. 在小部件的右侧，选择特定服务。

   下方的表格会显示最常尝试访问该服务的最多十台设备。在此表中，您可以生成两种类型的报告：成功访问尝试报告和被阻止访问尝试报告。

   此外，您还可以在此表中阻止特定设备访问云服务。

小部件会显示所请求的信息。

在显示的小部件中，您可以执行以下操作：

- 继续转到“**监控和报告**”→“**报告**”部分以查看 Cloud Discovery 报告。
- 阻止或允许访问所选的云服务。

仅当您在Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 授权许可下激活 Kaspersky Security Center 时，才可以使用阻止功能。

仅当您使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本时，才可以使用阻止功能。该安全应用程序的较早版本仅允许您监控云服务的使用情况。

云服务的风险级别

对于每项云服务，Cloud Discovery 都会为您提供风险级别。风险级别可帮助您确定不符合组织安全要求的服务。例如，在决定是否阻止对特定服务的访问时，您可能需要考虑风险级别。

免责声明：风险级别是一个估计指数，并不能说明云服务的质量或服务制造商的任何信息。风险级别只是卡巴斯基专家的建议。

云服务的风险级别显示在 Cloud Discovery 小部件和所有受监控云服务的列表中。

阻止对不需要的云服务进行的访问

您可以阻止用户访问您不希望他们访问的云服务。您也可以允许对之前被阻止的云服务的访问。

您在决定是否阻止对特定服务的访问时，除其他考虑因素外，还可能需要考虑风险级别。

您可以在安全策略或配置文件中阻止或允许对云服务的访问。

可通过两种方法来阻止对不需要的云服务进行的访问：

- 使用 Cloud Discovery 小部件。

  在这种情况下，您可以逐个阻止对服务的访问。

- 在 Kaspersky Endpoint Security for Windows 策略属性中。

  在这种情况下，您可以逐个阻止对服务的访问，也可以一次性阻止整个类别。

  有关如何在 Kaspersky Endpoint Security for Windows 策略属性中启用 Cloud Discovery 功能的详细信息，请参阅 Kaspersky Endpoint Security for Windows 帮助中的 Cloud Discovery 部分。

要使用小部件阻止或允许对云服务的访问，请执行以下操作：

1. 打开 Cloud Discovery 小部件，然后选择所需的云服务。
2. 在**使用该服务的前 10 台设备**面板中，找到要用于阻止或允许该服务的安全策略或配置文件。

3. 在所需行的“**策略或配置文件中的访问状态**”列中，执行以下任一操作：

   - 要阻止该服务，请在下拉列表中选择“**已阻止**”。
   - 要允许该服务，请在下拉列表中选择“**允许**”。

4. 单击“**保存**”按钮。

安全策略或配置文件将会阻止或允许对所选服务的访问。

Kaspersky Security Center Web Console 活动日志

Kaspersky Security Center Web Console 活动日志可以帮助调查软件故障原因。当您就 Kaspersky Security Center Web Console 的故障联系 Kaspersky 技术支持时，Kaspersky 技术支持专家可能向您请求 Kaspersky Security Center Web Console 日志文件。您使用应用程序的整个时间内，Kaspersky Security Center Web Console 日志文件存储在 <Kaspersky Security Center Web Console 安装文件夹>/logs 文件夹。日志文件不会自动发送给 Kaspersky 技术支持专家。

要启用 Kaspersky Security Center Web Console 活动日志，

选中 Kaspersky Security Center Web Console 安装向导的“**Kaspersky Security Center Web Console 连接设置**”窗口中的“**启用 Kaspersky Security Center Web Console 活动记录**”复选框。

日志文件是文本格式。

日志文件名称是<组件名称>.<设备名称>-<文件修订号>.YYYY-MM-DD 格式，其中：

- <组件名称>是 Kaspersky Security Center 组件或 Kaspersky Security Center Web Console 管理插件名称。
- <设备名称>是正在运行<组件名称>的设备的名称。
- <文件修订号>是为在<设备名称>中操作的<组件名称>创建的日子文件号码。一天中，相同<组件名称>和<设备名称>的若干日志文件可以被创建。日志文件的最大大小是 50 MB。当达到最大大小时，新日志文件被创建。新日志文件<文件修订号>增加 1。
- YYYY、MM 和 DD 是日志首次被创建的年、月、日。当新的一天开始时，新的日志文件被创建。

Kaspersky Security Center 与其他解决方案之间的集成

本节介绍如何配置从 Kaspersky Security Center Web Console 访问其他 Kaspersky 应用程序，例如 Kaspersky Managed Detection and Response。此部分还介绍了如何配置导出到 SIEM 系统。

建立后台连接

要让 Kaspersky Security Center Web 控制台执行其后台任务，您必须在 Kaspersky Security Center Web 控制台和管理服务器之间建立后台连接。仅当您的账户在“**常规功能：用户权限**”功能区域中拥有“**修改对象 ACL**”权限时，才能建立此连接。

如果安装 Kaspersky Endpoint Security for Windows 12.6 插件，或者更新低于 11.7 版本的 Kaspersky Endpoint Security for Windows 插件而尚未建立后台连接，将显示必须建立后台连接的通知。此外，您还必须对服务账户授予“**常规功能：对管理服务器的操作**”功能区域的权限。

要建立后台连接：

1. 在主菜单中，转到“**设置** → **整合**”。
2. 在**整合** 区域，将用于建立后台连接的切换按钮切换到位置：**用于整合的后台连接 已启用**。
3. 在打开的“**启用后台连接**”区域中，单击“**确定**”按钮。

即在 Kaspersky Security Center Web Console 与管理服务器之间建立后台连接。管理服务器会为后台连接创建一个账户，该账户用作服务账户以维护 Kaspersky Security Center 与其他 Kaspersky 应用程序或解决方案之间的交互。该服务账户的名称包含 NWCSvcUser 前缀。

出于安全原因，管理服务器每 30 天自动更改一次服务账户的密码。您不能手动删除服务账户。当禁用跨服务连接时，管理服务器会自动删除此账户。管理服务器为每个管理控制台都创建一个服务账户，并将所有服务账户分配到名称为 ServiceNwcGroup 的安全组。在 Kaspersky Security Center 安装过程中，管理服务器会自动创建此安全组。您不能手动删除此安全组。

导出事件到 SIEM 系统

本部分介绍如何配置导出事件到 SIEM 系统。

配置导出事件到 SIEM 系统

Kaspersky Security Center 允许通过以下方法之一进行配置：导出到任何使用 Syslog 格式的 SIEM 系统、导出到使用 LEEF 和 CEF 格式的 QRadar、Splunk、ArcSight SIEM 系统，或直接从 Kaspersky Security Center 数据库导出事件到 SIEM 系统。完成此方案后，管理服务器会自动将事件发送到 SIEM 系统。

先决条件

在开始配置 Kaspersky Security Center 中的事件导出之前：

- 了解有关事件导出方法的更多信息。
- 确保拥有系统设置的值。

> 您可以按任意顺序执行此方案的步骤。

将事件导出到 SIEM 系统的过程包括以下步骤：

- **配置 SIEM 系统以接收来自 Kaspersky Security Center 的事件。**

  说明：配置 SIEM 系统中的事件导出

- **选择要导出到 SIEM 系统的事件：**

说明：

- 管理控制台：标记要以 Syslog 格式导出的 Kaspersky 应用程序事件、标记要以 Syslog 格式导出的常规事件
- Kaspersky Security Center Web Console：标记要以 Syslog 格式导出的 Kaspersky 应用程序事件、标记要以 Syslog 格式导出的常规事件

- **配置使用以下方法之一将事件导出到 SIEM 系统：**
  - 使用TCP、UDP或TLS over TCP协议。
    说明：
    - 管理控制台：配置导出事件到 SIEM 系统
    - Kaspersky Security Center Web Console：配置导出事件到 SIEM 系统
  - 直接从 Kaspersky Security Center 数据库导出事件（Kaspersky Security Center 数据库提供了一组公共视图；您可以在 klakdb.chm 文档中找到这些公共视图的说明）。

结果

配置导出事件到 SIEM 系统后，如果您选择了要导出的事件，可以查看导出结果。

在您开始之前

当设置在 Kaspersky Security Center 中自动导出事件时，必须指定一些 SIEM 系统设置。建议您提前检查这些设置，以便准备设置 Kaspersky Security Center。

要成功配置自动发送事件到 SIEM 系统，您必须知道以下设置：

- **SIEM 系统服务器地址**

  安装了当前使用的 SIEM 系统的服务器的 IP 地址。在您的 SIEM 系统设置中检查此值。

- **SIEM 系统服务器端口**

  用于建立 Kaspersky Security Center 和您的 SIEM 系统服务器之间连接的端口号。您在 Kaspersky Security Center 设置中和您 SIEM 系统的接收设置中指定该值。

- **协议**

  用于从 Kaspersky Security Center 传输消息到您的 SIEM 系统的协议。您在 Kaspersky Security Center 设置中和您 SIEM 系统的接收设置中指定该值。

关于 Kaspersky Security Center 中的事件

Kaspersky Security Center 允许您接收受管理设备上安装的管理服务器和 Kaspersky 应用程序在操作期间发生的事件信息。事件信息保存在管理服务器数据库。您可以导出这些信息到外部 SIEM 系统。导出事件信息到外部 SIEM 系统使 SIEM 系统管理员可以快速响应发生在受管理设备或管理组中的安全系统事件。

事件类型

Kaspersky Security Center 中有以下类型的事件：

- 常规事件。这些事件发生在所有受管理卡巴斯基应用程序中。常规事件的一个示例是病毒爆发常规事件具有严格定义的语法和语义。常规事件用于报告和仪表板等方面。
- 受管理卡巴斯基应用程序特定事件。每个受管理 Kaspersky 应用程序都拥有自己的事件集。

事件源

以下应用程序可以生成事件：

- Kaspersky Security Center 组件：
  - 管理服务器
  - 网络代理
  - iOS MDM 服务器
- 受管理的卡巴斯基应用程序

  有关受管理卡巴斯基应用程序生成的事件的详细信息，请参阅相应应用程序的文档。

您可以在应用程序策略的“**事件配置**”选项卡上查看应用程序可以生成的事件的完整列表。对于管理服务器，您还可以在管理服务器属性中查看事件列表。

事件的重要级别

每个事件都有自己的重要级别。取决于发生的条件，一个事件可以被分配不同的重要级别。四个事件重要级别如下：

- *严重事件*指示发生了可能导致数据丢失、操作系统异常或严重错误的严重问题。
- *功能失败*指示在应用程序操作中或执行过程中发生了严重问题、错误或功能异常。
- *警告*是不严重的事件，但是也指示了今后可能发生的潜在问题。如果在事件发生后应用程序可以被恢复而不丢失数据或功能，则这些事件是警告级别。
- *信息*事件用于提示成功完成操作、应用程序的正常功能或完成了某过程。

每个事件都有一个存储期限，在这时间内您可以在 Kaspersky Security Center 中查看或修改。一些事件默认下不保存在管理服务器数据库，因为它们的存储期限是零。仅可以在管理服务器数据库中保存至少一天的事件可以被导出到外部系统。

关于事件导出

您可以在处理组织和技术级别的安全问题的集中式系统内使用事件导出，提供安全监控服务，以及合并来自不同解决方案的信息。即是提供对网络硬件和应用程序生成的安全警告的实时分析的 SIEM 系统，或者安全操作中心 (SOC)。

这些系统可以从许多源接收数据，包括网络、安全、服务器、数据库和应用程序。SIEM 系统也提供功能以集成监控的数据，以便帮助您避免丢失关键事件。而且，系统执行相关事件和警告的自动分析以通知管理员安全问题。警告可以通过仪表盘实现，或可以通过第三方渠道发送，例如邮件。

从 Kaspersky Security Center 导出事件到外部 SIEM 系统的进程设计两部分：事件发送者 — Kaspersky Security Center 和事件接收者 — SIEM 系统。要成功导出事件，您必须在 SIEM 系统和 Kaspersky Security Center 中进行配置。您可以先配置任意一端。您可以配置 Kaspersky Security Center 中的事件传输，然后配置 SIEM 系统对事件的接收，或者相反。

从 Kaspersky Security Center 发送事件的方法

有三种方法从 Kaspersky Security Center 发送事件到外部系统：

- 通过 Syslog 协议发送事件到任意 SIEM 系统

  使用 Syslog 协议，您可以转发发生在 Kaspersky Security Center 管理服务器上和受管理设备上安装的 Kaspersky 应用程序中的任意事件。Syslog 协议是标准消息记录协议。您可以用它将事件导出到任何 SIEM 系统。

  为此，您需要标记希望中继到 SIEM 系统的事件。您可以在管理控制台或 Kaspersky Security Center Web Console中标记事件。只有标记的事件才会被中继到 SIEM 系统。如果您没有标记任何内容，则不会中继任何事件。

- 通过 CEF 和 LEEF 协议发送事件到 QRadar、Splunk 和 ArcSight 系统

  您可以使用 CEF 和 LEEF 协议导出常规事件。当通过 CEF 和 LEEF 协议导出事件时，您不必能够选择指定事件以导出。相反，所有常规事件都被导出。要将 Kaspersky Security Center 事件转换为 CEF 和 LEEF 格式的事件，您需要使用siem_conversion_rules.xml 文件。该文件包含 Kaspersky Security Center 事件属性列表以及 CEF 和 LEEF 格式的事件的相应属性。此外，siem_conversion_rules.xml 文件包含用于生成与事件对应的消息的规则。该文件包含在 Kaspersky Security Center 分发包。

  不同于 Syslog 协议，CEF 和 LEEF 协议不通用。CEF 和 LEEF 为 SIEM 系统所设计(QRadar、Splunk 和 ArcSight)。因此，当您选择通过这些协议导出事件时，您使用 SIEM 系统所需解析器。

- 直接从 Kaspersky Security Center 数据库到 SIEM 系统

  以该方法导出事件可以用于通过使用 SQL 查询直接从数据库公共视图接收事件。查询结果被保存到 XML 文件，可以用于外部系统的输入数据。仅仅公共视图中的事件可以被直接从数据库中导出。

通过 SIEM 系统接收事件

SIEM 系统必须接收和正确解析来自 Kaspersky Security Center 的事件。因为这些目的，您必须正确配置 SIEM 系统。配置取决于特定的 SIEM 系统。然而，有一些配置所有 SIEM 系统的通用步骤，例如配置接收器和解析器。

关于配置 SIEM 系统中的事件导出

从 Kaspersky Security Center 导出事件到外部 SIEM 系统的进程设计两部分：事件发送者 — Kaspersky Security Center 和事件接收者 — SIEM 系统。必须在 SIEM 系统和 Kaspersky Security Center 中配置事件导出。

您在 SIEM 系统中指定的设置取决于您使用的系统。通常，对于所有 SIEM 系统，您必须设置接收器和消息解析器（可选）以解析接收的事件。

设置接收器

为了接收 Kaspersky Security Center 发送的事件，您必须在您的 SIEM 系统中设置接收器。通常，必须在 SIEM 系统指定以下设置：

- **导出协议或输入类型**

  它是消息传输协议，例如 UDP。该协议必须与您在 Kaspersky Security Center 中指定的协议相同。

- **端口**

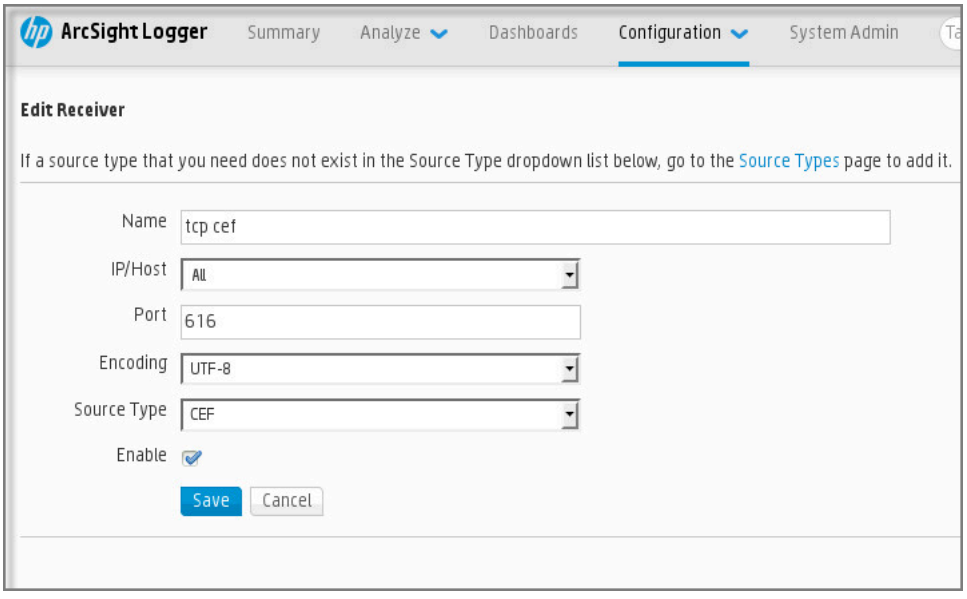
  连接到 Kaspersky Security Center 的端口号。该端口必须与您在 Kaspersky Security Center 中指定的端口相同。

- **消息协议或源类型**

  用于导出事件到 SIEM 系统的协议。它可以是标准协议之一：Syslog、CEF 或 LEEF。SIEM 系统根据您指定的协议选择消息解析器。

根据所使用的 SIEM 系统，您可能需要指定一些附加接收器设置。

下图显示了 ArcSight 的接收器设置截图。



ArcSight 的接收器设置

消息解析器

导出的事件作为消息被传递到 SIEM 系统。这些消息必须正确解析，以便事件信息可以被 SIEM 系统使用。消息解析器是 SIEM 系统的一部分，它们用于拆分消息内容到相关字段，例如事件 ID、严重级别、描述、参数。这将启用 SIEM 系统以处理从 Kaspersky Security Center 接收的事件，以便它们可以被存储在 SIEM 系统数据库。

标记要以 Syslog 格式导出到 SIEM 系统的事件

在启用自动导出事件后，您必须选择将被导出到外部 SIEM 系统的事件。

您可以配置基于以下条件之一导出 Syslog 格式的事件到外部系统：

- 标记常规事件。如果在事件设置或管理服务器设置中标记要在策略中导出的事件，SIEM 系统将接收由特定策略管理的所有应用程序中发生的所标记事件。如果导出的事件在策略中被选中，您将不能为由该策略管理的个别应用程序重新定义所选事件。
- 为受管理应用程序标记事件。如果为受管理设备上安装的受管理应用程序选择要导出的事件，SIEM 系统将仅接收该应用程序中发生的事件。

关于标记要以 Syslog 格式导出到 SIEM 系统的事件

在启用自动导出事件后，您必须选择将被导出到外部 SIEM 系统的事件。

您可以配置基于以下条件之一导出 Syslog 格式的事件到外部系统：

- 标记常规事件。如果在事件设置或管理服务器设置中标记要在策略中导出的事件，SIEM 系统将接收由特定策略管理的所有应用程序中发生的所标记事件。如果导出的事件在策略中被选中，您将不能为由该策略管理的个别应用程序重新定义所选事件。
- 为受管理应用程序标记事件。如果为受管理设备上安装的受管理应用程序选择要导出的事件，SIEM 系统将仅接收该应用程序中发生的事件。

标记要以 Syslog 格式导出的 Kaspersky 应用程序事件

如果要导出受管理设备上安装的特定受管理应用程序中发生的事件，则标记事件为在应用程序策略中导出。在这种情况下，标记的事件将从策略范围内的所有设备中导出。

要为特定受管理应用程序标记要导出的事件：

1. 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”。
2. 单击您要为其标记事件的应用程序的策略。

   策略设置窗口打开。
3. 转到“**事件配置**”区域。
4. 选中要导出到 SIEM 系统的事件旁边的复选框。

5. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”按钮。

> 您也可以在“**事件注册**”区域中标记要导出到 SIEM 系统的事件，通过单击事件链接可打开该区域。

6. 在您标记为导出到 SIEM 系统的一个或多个事件的“**Syslog**”列中会显示一个复选标记 (✓)。

7. 单击“**保存**”按钮。

受管理应用程序中的标记事件已准备好导出到 SIEM 系统。

您可以为特定受管理设备标记要导出到 SIEM 系统的事件。如果先前导出的事件已在应用程序策略中标记，您将不能为受管理设备重新定义所标记的事件。

要为受管理设备标记要导出的事件：

1. 在主菜单中，转到“**资产(设备)**” → “**受管理设备**”。
   将显示受管理设备列表。

2. 在受管理设备列表中单击带有所需设备名称的链接。
   将显示所选设备的属性窗口。

3. 转到“**应用程序**”区域。

4. 在应用程序列表中单击带有所需应用程序名称的链接。

5. 转到“**事件配置**”区域。

6. 选中要导出到 SIEM 的事件旁边的复选框。

7. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”按钮。

> 此外，还可以在“**事件注册**”区域中标记要导出到 SIEM 系统的事件，通过单击事件链接可打开该区域。

8. 在您标记为导出到 SIEM 系统的一个或多个事件的“**Syslog**”列中会显示一个复选标记 (✓)。

从现在开始，如果配置了到 SIEM 系统的导出，管理服务器会将标记的事件发送到 SIEM 系统。

标记要以 Syslog 格式导出的常规事件

您可以标记管理服务器将使用 Syslog 格式导出到 SIEM 系统的常规事件。

要标记常规事件以导出到 SIEM 系统：

1. 执行以下操作之一：

   - 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   - 在主菜单中，转到“**资产(设备)**”→“**策略和配置文件**”，然后单击某个策略的链接。

2. 在打开的窗口中，转到“**事件配置**”选项卡。

3. 单击“**使用 Syslog 标记以导出到 SIEM 系统**”。

此外，还可以在“**事件注册**”区域中标记要导出到 SIEM 系统的事件，通过单击事件链接可打开该区域。

4. 在您标记为导出到 SIEM 系统的一个或多个事件的“**Syslog**”列中会显示一个复选标记 (✓)。

从现在开始，如果配置了到 SIEM 系统的导出，管理服务器会将标记的事件发送到 SIEM 系统。

关于使用 CEF 和 LEEF 格式导出事件

您可以使用 CEF 和 LEEF 格式将常规事件以及由卡巴斯基应用程序传输到管理服务器的事件导出到 SIEM 系统。导出事件集是预定义的，您无法选择要导出的事件。在将事件发送到 SIEM系统（QRadar、ArcSight 或 Splunk）之前，需要使用siem_conversion_rules.xml 文件中指定的规则将 Kaspersky Security Center 事件解释为 CEF 和 LEEF 格式的事件。

基于使用的 SIEM 系统选择导出格式。下表显示了 SIEM 系统和对应的导出格式。

导出事件到 SIEM 系统的格式

SIEM 系统	导出格式
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - 用于 IBM®Security QRadar SIEM 的自定义事件格式。QRadar 可以集成、识别和处理 LEEF 事件。LEEF 事件必须使用 UTF-8 字符编码。您可以在 IBM Knowledge Center 查看 LEEF 协议的详情。

- CEF (通用事件格式)—开放式日志管理标准，涉及来自不同的网络设备和应用程序的安全信息的协同工作。CEF 允许您使用通用日志格式，因此数据可以被简易整合以用企业管理系统分析。CEF 事件必须使用 UTF-8 字符编码。

自动导出意味着 Kaspersky Security Center 发送常规事件到 SIEM 系统。事件自动导出在您启用后立即开始。该部分详细解释了如何启用自动事件导出。

将事件转换为 CEF 或 LEEF 格式

在将事件发送到 SIEM系统（QRadar、ArcSight 或 Splunk）之前，需要使用siem_conversion_rules.xml文件中指定的规则将 Kaspersky Security Center 事件解释为 CEF 和 LEEF 格式的事件。该文件包含在 Kaspersky Security Center 分发包。

siem_conversion_rules.xml 文件包含将事件转换为 CEF 和 LEEF 格式的预定义解释规则。如果想使用额外的事件解释规则，您可以手动将它们添加到文件中。

siem_conversion_rules.xml 文件包括`<product name="SP_QRADAR" vendor="IBM">` 和 `<product name="SP_QRADAR" vendor="IBM">`部分。`<product name="SP_QRADAR" vendor="IBM">`部分包含用于生成 LEEF 格式事件的规则，可以导出到 QRadar SIEM 系统。`<product name="SP_ARCSIGHT" vendor="HP">`部分包含用于生成 LEEF 格式事件的规则，可以导出到 ArcSight 或 Splunk SIEM 系统。

每个部分都有`<common>`子部分，Kaspersky Security Center 事件属性以及 LEEF 格式事件的相应属性位于其中。这些通用属性用于所有可以导出的事件类型。

此外，每个部分都有<event>子部分。每个<event>子部分包含添加到<common>部分中列出的属性中的其他属性。

您可以手动将新的事件生成规则添加到 siem_conversion_rules.xml 文件中。

要添加新的事件生成规则：

1. 将新的<event>子部分添加到<product name="SP_QRADAR" vendor="IBM">或<product name="SP_QRADAR" vendor="IBM">部分，然后指定其他事件属性（如果需要）。

2. 如果事件仅由通用属性组成，<event>子部分将为空。

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- 通用 Kaspersky Security Center 事件属性和相应的 LEEF 事件属性 -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- 具有其他属性的 GNRL_EV_VIRUS_FOUND 事件的生成规则 -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- 通用 Kaspersky Security Center 事件属性和相应的 LEEF 事件属性 -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

关于使用 Syslog 格式导出事件

您可以使用 Syslog 格式将管理服务器和受管理设备上安装的其他卡巴斯基应用程序中发生的事件导出到 SIEM 系统。

Syslog 是消息记录协议的标准。它允许分离生成消息的软件、存储消息的系统和报告和分析消息的软件。每个消息都带有设备代码标签，指示生成消息的软件类型，并被分配严重级别。

Syslog 格式由 Request for Comments (RFC) 文档定义，该文档由 Internet Engineering Task Force（互联网标准）发布。RFC 5424 标准用于从 Kaspersky Security Center 导出事件到外部系统。

在 Kaspersky Security Center 中，您可以配置使用 Syslog 格式导出事件到外部系统。

导出过程包含两个步骤：

1. 启用自动事件导出。在该步骤，Kaspersky Security Center 被配置，以便能发送事件到 SIEM 系统。Kaspersky Security Center 在您启用自动导出后立即开始发送事件。

2. 选择事件以导出到外部系统。在该步骤，您可以选择导出哪些事件到 SIEM 系统。

配置 Kaspersky Security Center 以导出事件到 SIEM 系统

要将事件导出到 SIEM 系统，必须在 Kaspersky Security Center Web Console 中配置导出流程。

在将事件发送到 SIEM系统（QRadar、ArcSight 或 Splunk）之前，需要使用siem_conversion_rules.xml文件中指定的规则将 Kaspersky Security Center 事件解释为 CEF 和 LEEF 格式的事件。

要在 Kaspersky Security Center Web Console 中配置到 SIEM 系统的导出：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。

   管理服务器属性窗口将打开。

2. 在“**常规**”选项卡上，选择“**导出到 SIEM**”区域。

3. 单击“**设置**”链接。

   “**导出设置**”区域将打开。

4. 在“**导出设置**”区域指定设置：

   - **SIEM 系统服务器地址**

     安装了当前使用的 SIEM 系统的服务器的 IP 地址。在您的 SIEM 系统设置中检查此值。

   - **SIEM 系统端口**

     用于建立 Kaspersky Security Center 和您的 SIEM 系统服务器之间连接的端口号。您在 Kaspersky Security Center 设置中和您 SIEM 系统的接收设置中指定该值。

   - **协议**

     选择该协议用于传输消息到 SIEM 系统。您可以选择TCP、UDP或TLS over TCP协议。

     如果选择 TLS over TCP 协议，则指定以下 TLS 设置：

     - **服务器身份验证**

在“**服务器身份验证**”字段中，可以选择值“**受信任证书**”或“**SHA 指纹**”：

- **受信任证书**。您可以接收来自受信任证书颁发机构 (CA) 的完整证书链（包括根证书），并将该文件上传到 Kaspersky Security Center。Kaspersky Security Center 会检查 SIEM 系统服务器的证书链是否也具有受信任 CA 的签名。

  要添加受信任证书，请单击“**浏览 CA 证书文件**”按钮，然后上传证书。

- **SHA 指纹**。您可以在 Kaspersky Security Center 中指定 SIEM 系统的完整证书链（包括根证书）的 SHA1 指纹。要添加 SHA1 指纹，请在“**指纹**”字段中输入，然后单击“**添加**”按钮。

使用“**添加客户端身份验证**”设置，可以生成证书来对 Kaspersky Security Center 进行身份验证。因此，您将使用 Kaspersky Security Center 颁发的自签名证书。在这种情况下，您可以同时使用受信任证书和 SHA 指纹来对 SIEM 系统服务器进行身份验证。

- **添加主题名称/主题备选名称**

  主题名称是接收证书的域名。如果 SIEM 系统服务器的域名与 SIEM 系统服务器证书的主题名称不匹配，Kaspersky Security Center 将无法连接到 SIEM 系统服务器。但是，SIEM 系统服务器的域名在证书中发生变化，则可以更改该域名。在这种情况下，您可以在“**添加主题名称/主题备选名称**”字段中指定主题名称。如果任一指定主题名称与 SIEM 系统证书的主题名称匹配，Kaspersky Security Center 将验证 SIEM 系统服务器证书。

- **添加客户端身份验证**

  对于客户端身份验证，可以插入证书或在 Kaspersky Security Center 中生成证书。

  - **插入证书**。您可以使用从任何来源（例如，从任何受信任 CA）收到的证书。您必须指定以下证书类型之一的证书及其私钥：

    - **X.509 证书 PEM**。在“**证书文件**”字段中上传包含证书的文件，并在“**密钥文件**”字段中上传包含私钥的文件。这两个文件不相互依赖，文件的加载顺序也不重要。上传这两个文件后，在“**密码或证书验证**”字段中指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

    - **X.509 证书 PKCS12**。在“**证书文件**”字段中上传包含证书及其私钥的单个文件。上传该文件后，在“**密码或证书验证**”字段中指定用于解码私钥的密码。如果私钥未编码，则密码可以为空值。

  - **生成密钥**。您可以在 Kaspersky Security Center 中生成自签名证书。结果是，Kaspersky Security Center 将存储生成的自签名证书，您可以将证书的公共部分或 SHA1 指纹传递给 SIEM 系统。

- **数据格式**

您可以选择系统日志、CEF 或 LEEF 格式，具体取决于 SIEM 系统的要求。

如果选择系统日志数据格式，您必须指定：

- **最大消息大小，字节**

指定 SIEM 系统消息的最大大小。每个事件被一条消息转发。如果消息的精确长度超过指定值，消息被截断且数据可能丢失。默认大小是 2048 字节。仅当在“**协议**”字段中选择了系统日志格式后，该字段才可用。

5. 如果需要，您可以从管理服务器数据库中导出压缩的事件，并设置要开始导出的压缩事件的开始日期：

   a. 单击**设置导出起始日期**链接。

   b. 在打开的部分中，在**系统事件导出的起始日期**字段中指定开始日期。

   c. 单击“**正常**”按钮。

6. 将选项切换到“**自动导出事件至 SIEM 系统数据库已启用**”位置。

7. 要检查 SIEM 系统连接是否已配置，请单击**检查连接**按钮。
   与 SIEM 系统的连接已建立，测试事件已发送。将显示连接状态。

   该检查仅针对 TCP 和 TCP over TLS 协议执行。

8. 单击“**保存**”按钮。

到 SIEM 系统的导出已配置。

直接从数据库导出事件

您可以直接从 Kaspersky Security Center 数据库接收事件，而不必使用 Kaspersky Security Center 界面。您可以直接查询公共视图并检索事件数据，也可以基于现有公共视图创建您自己的视图并定位它们以获取所需数据。

公共视图

为了您的方便，在 Kaspersky Security Center 数据库中提供了公共视图集。您可以在 klakdb.chm 文档中找到这些公共视图的描述。

v_akpub_ev_event 公共视图包含一组展示数据库中事件参数的字段集。在 klakdb.chm 文档中您也可以查找对应于其他 Kaspersky Security Center 实体的公共视图信息，例如，设备、应用程序或用户。您可以在您的查询中使用该信息。

该部分包含了使用 klsql2 实用工具执行 SQL 查询的说明以及查询例子。

要创建 SQL 查询或数据库视图，您也可以使用其他程序以操作数据库。关于如何查看连接到 Kaspersky Security Center 数据库的参数的信息，例如实例名称和数据库名称，在对应区域给出。

使用 klsql2 实用工具执行 SQL 查询

本章描述了如何下载和使用 klsql2 实用工具，以及如何使用该实用工具执行 SQL 查询。

要使用 klsql2 实用程序：

1. 在 Kaspersky Security Center 的安装文件夹中寻找 klsql2 实用程序。默认安装路径为 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。不要使用用于旧版 Kaspersky Security Center 的 klsql2 实用程序版本。

2. 在任何文本编辑器中创建一个扩展名为 .sql 的文件，并将该文件与该实用程序放在同一文件夹中。

3. 在创建的 .sql 文件中，键入所需的 SQL 查询，然后保存该文件。

4. 在 Kaspersky Security Center 管理服务器设备上，在命令行，输入以下命令以从 .sql 文件执行 SQL 查询并保存结果到 result.xml 文件：

   ```
   klsql2 -i src.sql -u <用户名> -p <密码> -o result.xml
   ```

   其中 < username > 和 < password > 是有权访问数据库的用户账户的凭据。

5. 如果需要，输入有权访问数据库的用户账户的登录名和密码。

6. 打开新创建的 result.xml 文件以查看 SQL 查询结果。

您可以编辑 .sql 文件并创建到公共视图的任意 SQL 查询。然后，从命令行，执行您的 SQL 查询并保存结果到文件。

klsql2 实用工具中的 SQL 查询例子

该部分显示 SQL 查询的例子，通过 klsql2 实用工具执行。

以下例子阐述了对过去七天发生在设备上的事件的获取，并根据事件发生时间顺序显示事件。首先显示最近的事件。

Microsoft SQL Server 的示例：

```
SELECT
  /* 事件标识 */
  e.nId,

  /* 事件发生的时间 */
  e.tmRiseTime,

  /* 事件类型的内部名称 */
  e.strEventType,

  /* 事件的显示名称 */
  e.wstrEventTypeDisplayName,

  /* 事件的显示描述 */
  e.wstrDescription,

  /* 事件所在的组名称 */
  e.wstrGroupName,

  /* 发生事件的设备的显示名称 */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* 发生事件的设备的 IP 地址 */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

PostgreSQL 示例：

```
SELECT
  /* 事件标识 */
  "e"."nId",

  /* 事件发生的时间 */
  "e"."tmRiseTime",

  /* 事件类型的内部名称 */
  "e"."strEventType",

  /* 事件的显示名称 */
  "e"."wstrEventTypeDisplayName",

  /* 事件的显示描述 */
  "e"."wstrDescription",

  /* 事件的显示描述 */
  "e"."wstrGroupName",

  /* 发生事件的设备的显示名称 */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* 发生事件的设备的 IP 地址 */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 或 MariaDB 示例：

```
SELECT

  /* 事件标识 */
  `e`.`nId`,

  /* 事件发生的时间 */
  `e`.`tmRiseTime`,

  /* 事件类型的内部名称 */
  `e`.`strEventType`,

  /* 事件的显示名称 */
  `e`.`wstrEventTypeDisplayName`,

  /* 事件的显示描述 */
  `e`.`wstrDescription`,

  /* 设备组名称 */
  `e`.`wstrGroupName`,

  /* 发生事件的设备的显示名称 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* 发生事件的设备的 IP 地址 */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

查看 Kaspersky Security Center 数据库名称

如果您要通过 SQL Server、MySQL 或 MariaDB 数据库管理工具访问 Kaspersky Security Center 数据库，您必须知道数据库的名称以便从您的 SQL 脚本编辑器连接。

要查看 Kaspersky Security Center 数据库名称：

1. 在主菜单，单击所需的管理服务器名称旁边的“设置”图标 ( )。
   管理服务器属性窗口将打开。
2. 在“**常规**”选项卡上，选择“**当前数据库详情**”区域。

数据库名称在“**数据库名称**”字段中指定。使用数据库名称在您的 SQL 查询中定位数据库。

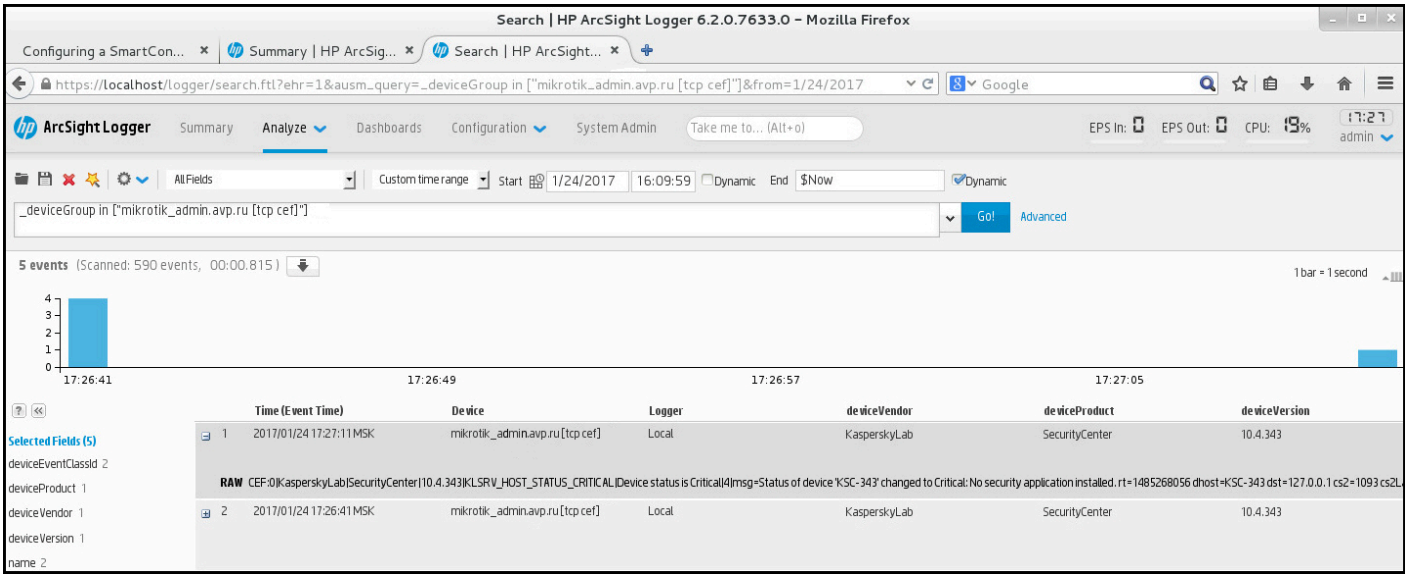
查看导出结果

您可以控制事件导出过程的成功完成。为此，检查带有导出事件的邮件是否被您的 SIEM 系统接收。

如果从 Kaspersky Security Center 发送的事件被接收并被您的 SIEM 系统正确解析，两端的配置被正确完成。否则，检查您在 Kaspersky Security Center 中指定的设置是否与您的 SIEM 系统中的设置一致。

下图显示导出到 ArcSight 的事件。例如，第一个事件是严重的管理服务器事件：“*设备状态为严重*”。

导出事件在您 SIEM 系统中的显示随您使用的 SIEM 系统而不同。



事件例子

在云环境中使用 Kaspersky Security Center Web Console

本节提供了 Kaspersky Security Center Web Console 与部署有关的功能以及在云环境（如 Amazon Web Services、Microsoft Azure 或 Google Cloud）中维护 Kaspersky Security Center 的信息。

要在云环境内工作，您需要特殊的授权许可。如果您没有这样的授权许可，则不会显示与云设备相关的界面元素。

Kaspersky Security Center Web Console 中的云环境配置

要使用配置云环境向导配置 Kaspersky Security Center，您必须拥有：

- 云环境的特定凭据：
  - 一个被授予轮询云段权限的 IAM 角色或一个被授予轮询云段权限的 IAM 用户账户（用于使用 Amazon Web Services）
  - 一个 Azure 应用程序 ID、密码和订阅（用于使用 Microsoft Azure）
  - Google 客户端电子邮件、项目 ID 和私钥（用于使用 Google Cloud）
- 安装包：
  - Network Agent for Windows
  - Network Agent for Linux
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux 的 Web 插件
- 至少具有以下一种：
  - Kaspersky Endpoint Security for Windows 安装包和 Web 插件（推荐）
  - Kaspersky Security for Windows Server 的安装包和 Web 插件

如果从现成镜像部署 Kaspersky Security Center，在通过管理控制台第一次连接到管理服务器时会自动启动配置云环境向导。您还可以在任意时刻手动启动向导。

要手动启动配置云环境向导，

在主菜单中，转到“**发现和部署 → 部署和分配 → 配置云环境**”。

向导启动。

云环境配置的平均工作会话时间是约 15 分钟。

步骤 1：检查需要的插件和安装包

如果您具有下面列出的所有需要的 Web 插件和安装包，则不会显示此步骤。

要配置云环境，您必须具有以下组件：

- 安装包：
  - Network Agent for Windows
  - Network Agent for Linux
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux 的 Web 插件
- 至少具有以下一种：
  - Kaspersky Endpoint Security for Windows 安装包和 Web 插件（推荐）
  - Kaspersky Security for Windows Server 的安装包和 Web 插件
    建议您使用 Kaspersky Endpoint Security for Windows，而非 Kaspersky Security for Windows Server。

Kaspersky Security Center 会自动检测您已有的组件，仅列出缺少的组件。单击“**选择要下载的应用程序**”按钮以下载列出的组件，然后选择需要的插件和安装包。下载组件后，您可以使用“**刷新**”按钮来更新缺少组件列表。

步骤 2：授权应用程序

仅当您使用 BYOL AMI 并且尚未使用 Kaspersky Security for Virtualization 授权许可或 Kaspersky Hybrid Cloud Security 授权许可激活应用程序时，才显示此步骤。

指定授权许可密钥，然后单击“**下一步**”继续。

授权许可密钥即添加到管理服务器存储中。

如果再次运行向导，则不会显示此步骤。

步骤 3：选择云环境和授权

该部分描述仅应用到 Kaspersky Security Center 12.1 或更新版本的功能。

指定下列设置：

- **云环境**

  选择您要部署 Kaspersky Security Center 的云环境：AWS、Azure 或 Google Cloud。
  如果计划使用多个云环境，请选择一种环境，然后再次运行向导。

- **连接名称**

  输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。
  该名称也将用作云设备的管理组名称。
  如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

输入您的凭据以在您指定的云环境中获得授权。

AWS

如果选择了 AWS 作为云段类型，则需要 IAM 角色或 AWS IAM 访问密钥才能进一步轮询云段。

- **分配给 EC2 实例的 AWS IAM 角色**
  如果您拥有具有管理服务器必需权限的 IAM 角色，则选择此选项。

- **AWS IAM 用户**
  如果您拥有 AWS IAM 访问密钥，则选择此选项。输入您的密钥数据：

  - **访问密钥 ID**

    IAM 访问密钥 ID 是个字母数字序列。当您在创建 IAM 用户账户时接收密钥 ID。
    如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

  - **私密密钥**

    您创建IAM 用户账户时接收到的带有访问密钥 ID 的secret key。
    Secret key 的字符显示为星号。在您开始输入 secret key 后，**显示**按钮被显示。点击并按住该按钮一定时间以查看输入的字符。
    如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

    要查看您输入的字符，请单击并按住“**显示**”按钮。

Azure

如果您选择了 Azure 作为云段类型，为将来轮询云段所使用的连接指定以下设置：

- **Azure 应用程序 ID**

  您在 Azure 门户创建了该应用程序 ID。

  您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

- **Azure 订阅 ID**

  您在 Azure 门户创建了该订阅。

- **Azure 应用程序密码**

  当您创建应用程序 ID 时您收到应用程序 ID 的密码。

  密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

  要查看您输入的字符，请单击并按住“**显示**”按钮。

- **Azure 存储账户名**

  您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

- **Azure 存储访问密钥**

  您创建 Azure 存储账户以使用 Kaspersky Security Center 时接收密码（密钥）。

  密钥在“Azure 存储账户概述”区域的“密钥”子区域中提供。

  要查看您输入的字符，请单击并按住“**显示**”按钮。

Google Cloud

如果您选择了 Google Cloud 作为云段类型，为将来轮询云段所使用的连接指定以下设置：

- **客户端邮件地址**

  客户端电子邮件是用于在 Google Cloud 注册项目的电子邮件地址。

- **项目 ID**

  项目 ID 是您在 Google Cloud 注册项目时收到的 ID。

- **私钥**

  私钥是您在 Google Cloud 注册项目时收到的用作私钥的字符序列。最好复制并粘贴此序列，以免出错。

  要查看您输入的字符，请单击并按住“**显示**”按钮。

您指定的连接保存在应用程序设置中。

配置云环境向导仅允许您指定一个段。以后，您可以指定更多的连接以管理其他云段。

单击“**下一步**”继续。

步骤 4：云段轮询，配置与云的同步并选择后续操作

在此步骤中，云段轮询开始，并自动创建一个特殊的云设备管理组。轮询中发现的设备被放置在该组。云段轮询计划即配置完成（默认每 5 分钟轮询一次；您可以在稍后更改此设置）。

与云同步自动移动规则也被创建。对于每个云网络的后续扫描，检测到的虚拟设备将被移动到“**受管理设备**”\“**云**”组的对应子组。

定义下列设置：

- **与云结构同步管理组**

  如果启用该选项，**云**组被自动创建在**受管理设备**组，云设备发现被启动。在每个云网络扫描中检测到的实例和虚拟机被放置到 AWS 组。该组的管理子组结构匹配您的云段结构（在 AWS 中，可用域和放置组不出现在结构中；在 Azure 中，子网不出现在结构中）。未被识别为云环境中实例的设备在**未分配的设备**组。该组结构允许您使用组安装任务安装反病毒应用程序到实例，以及为不同组设置不同的策略。

  如果禁用该选项，**云**组也被创建，且云设备发现也被启动；然而，匹配云段结构的子组不在组中被创建。所有检测到的实例都在**云**管理组，因此显示在单一列表。如果您使用的 Kaspersky Security Center 需要同步，您可以修改**与云同步**规则的属性并强制执行该规则。强加该规则改变云组的子组结构，以便匹配您云段的结构。

  默认情况下已禁用该选项。

- **部署保护**

  如果选择该选项，向导创建任务以安装安全应用程序到实例。向导完成后，保护部署向导自动在您的云段的设备上启动，并且您将可以在这些设备上安装网络代理和安全应用程序。

  Kaspersky Security Center 可以使用其本地工具执行部署。如果您没有权限安装应用程序到 EC2 实例或 Azure 虚拟机，您可以手动配置**远程安装**任务并指定带有所需权限的账户。此种情况下，远程安装任务将不用于使用 AWS API 或 Azure 发现的设备。该任务将仅用于使用活动目录轮询、Windows 域轮询或 IP 范围轮询发现的设备。

  如果未选择该选项，保护部署向导不被启动，安装安全应用程序的任务未在实例上被创建。您可以稍后手动执行这些操作。

如果选择“部署保护”选项，“**正在重启设备**”区域变为可用。在此区域中，必须选择目标设备操作系统必须重启时的操作。选择在安装应用程序过程中设备操作系统必须重启时是否重启实例：

- **不重启**

  如果选择该选项，安全应用程序安装后设备不被重启。

- **重新启动**

  如果选择该选项，安全应用程序安装后设备将被重启。

单击“**下一步**”继续。

对于 Google Cloud，只能使用 Kaspersky Security Center 本机工具执行部署。如果选择了 Google Cloud，“**部署保护**”选项不可用。

步骤 5：选择一个应用程序来为其创建策略和任务

仅当您同时具有 Kaspersky Endpoint Security for Windows 和 Kaspersky Security for Windows Server 的安装包和插件时，才会显示此步骤。如果您只有其中一个应用程序的插件和安装包，则会跳过此步骤，且 Kaspersky Security Center 会为现有应用程序创建策略和任务。

选择您要为其创建策略和任务的应用程序：

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

步骤 6：为 Kaspersky Security Center 配置卡巴斯基安全网络

指定设置以转发 Kaspersky Security Center 操作信息到卡巴斯基安全网络 (KSN) 知识库。您可以选择以下选项之一：

- **我同意使用卡巴斯基安全网络**

  安装在客户端设备上的 Kaspersky Security Center 和受管理应用程序将自动将其操作详情传输到卡巴斯基安全网络。参与卡巴斯基安全网络确保了包含病毒和其他威胁的数据库的快速更新，该数据库确保了对紧急安全威胁的快速响应。

- **我不同意使用卡巴斯基安全网络**

  Kaspersky Security Center 和受管理应用程序将不向卡巴斯基安全网络提供任何信息。
  如果选择此选项，则将禁用卡巴斯基安全网络。

Kaspersky 建议您参与卡巴斯基安全网络。

还可能显示针对受管理应用程序的 KSN 协议。如果您同意使用卡巴斯基安全网络，受管理应用程序会将数据发送到 Kaspersky。如果您不同意加入卡巴斯基卡巴斯基安全网络，受管理应用程序将不会向卡巴斯基发送数据。（您可以稍后在应用程序策略中更改此设置。）

单击“**下一步**”继续。

步骤 7：创建保护的初始配置

您可以检查创建的策略和任务列表。

等待策略和任务创建完成，然后单击“**下一步**”继续。在向导的最后一页，单击“**完成**”按钮退出。

通过 Kaspersky Security Center Web Console 进行云段轮询

管理服务器通过使用 AWS API、Azure API 或 Google API 工具对云段进行常规轮询来接收有关该网络结构（和其中的设备）的信息。Kaspersky Security Center 使用该信息更新未分配的设备和受管理设备文件夹的内容。如果您配置了设备自动移动到管理组，检测到的设备将被包含在管理组中。

要允许管理服务器轮询云段，您必须拥有提供了 IAM 角色 或 IAM 用户账户（在 AWS 中），或者提供了应用程序 ID 和密码（在 Azure 中），或者提供了 Google 客户端电子邮件、Google 项目 ID 和私钥（在 Google Cloud 中）的相应权限。

您可以添加和删除连接，以及为每个云段设置轮询计划。

为云段轮询添加连接

要添加云段轮询连接到可用连接列表：

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**云**”。
2. 在打开的窗口中，单击“**属性**”。
3. 在打开的“**设置**”窗口中，单击“**添加**”。
   云段设置窗口打开。
4. 为将用于进一步轮询云段的连接指定云环境的名称：

   - **云环境**

     选择您要部署 Kaspersky Security Center 的云环境：AWS、Azure 或 Google Cloud。
     如果计划使用多个云环境，请选择一种环境，然后再次运行向导。

   - **连接名称**

     输入连接名称。名称不能包括 256 个以上字符。仅允许 Unicode 字符。
     该名称也将用作云设备的管理组名称。

如果您计划使用多个云环境，则最好在连接名称中包含环境名称，例如“Azure Segment”、“AWS Segment”或“Google Segment”。

5. 输入您的凭据以在您指定的云环境中获得授权。

- 如果选择了 AWS，请指定以下设置：
  - **使用 AWS IAM 角色**

    如果您已经为管理服务器创建了 IAM 角色以使用 AWS 服务，则选择该选框。

  - **AWS IAM 用户账户凭证**

    如果您拥有带有必要权限的 IAM 用户账户且您可以输入密钥 ID 和 secret key，则选择该选框。

    如果您指定了AWS IAM 用户账户凭证，请指定以下设置：

    - **访问密钥 ID**

      IAM 访问密钥 ID 是个字母数字序列。当您在创建 IAM 用户账户时接收密钥 ID。
      如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

    - **私密密钥**

      您创建IAM 用户账户时接收到的带有访问密钥 ID 的secret key。
      Secret key 的字符显示为星号。在您开始输入 secret key 后，**显示**按钮被显示。点击并按住该按钮一定时间以查看输入的字符。
      如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

    要查看您输入的字符，请单击并按住“**显示**”按钮。

- 如果选择了 Azure，请指定以下设置：
  - **Azure 应用程序 ID**

    您在 Azure 门户创建了该应用程序 ID。
    您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

  - **Azure 订阅 ID**

    您在 Azure 门户创建了该订阅。

  - **Azure 应用程序密码**

    当您创建应用程序 ID 时您收到应用程序 ID 的密码。

密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

要查看您输入的字符，请单击并按住“**显示**”按钮。

- **Azure 存储账户名**

  您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

- **Azure 存储访问密钥**

  您创建 Azure 存储账户以使用 Kaspersky Security Center 时接收密码（密钥）。

  密钥在“Azure 存储账户概述”区域的“密钥”子区域中提供。

  要查看您输入的字符，请单击并按住“**显示**”按钮。

如果选择了 Google Cloud，请指定以下设置：

- **客户端邮件地址**

  客户端电子邮件是用于在 Google Cloud 注册项目的电子邮件地址。

- **项目 ID**

  项目 ID 是您在 Google Cloud 注册项目时收到的 ID。

- **私钥**

  私钥是您在 Google Cloud 注册项目时收到的用作私钥的字符序列。最好复制并粘贴此序列，以免出错。

  要查看您输入的字符，请单击并按住“**显示**”按钮。

6. 如果需要，单击“**设置轮询计划**”，然后更改默认设置。

该连接保存在应用程序设置。

在新云段被第一次轮询后，该段对应的子组出现在“**受管理设备**”\“**云**”管理组。

如果您指定不正确的凭证，在云段轮询过程中将不会发现实例，且新子组将不会出现在“**受管理设备**”\“**云**”管理组。

为云段轮询删除连接

如果您不再必须轮询特定云段，您可以从可用连接列表删除对应于该云段的连接。您还可以删除连接，例如，当轮询云段的权限已被转移给其他具有不同凭据的用户时。

要删除连接：

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**云**”。
2. 在打开的窗口中，单击“**属性**”。
3. 在打开的“**设置**”窗口中，单击要删除的云段的名称。
4. 单击**删除**。
5. 在打开的窗口中，单击“**确定**”按钮以确认您的选择。

连接即被删除。云段中与该连接对应的设备会自动从管理组中删除。

通过 Kaspersky Security Center Web Console 配置轮询计划

云段轮询根据计划执行。您可以设置轮询频率。

轮询频率在配置云环境设置中被自动设置为 5 分钟。您可以在任意时刻更改该值并设置不同的计划。然而，不建议设置大于每 5 分钟一次的轮询频率，因为这可能导致 API 操作错误。

要配置云段轮询计划：

1. 在主菜单中，转到“**发现和部署**”→“**发现**”→“**云**”。
2. 在打开的窗口中，单击“**属性**”。
3. 在打开的“**设置**”窗口中，单击要为其配置轮询计划的云段的名称。
   这将打开**云段设置**窗口。
4. 在**云段设置**窗口中，单击**设置轮询计划**按钮。
   这会打开“**计划**”窗口。
5. 在“**计划**”窗口中，定义以下设置：

   - **计划开始**
     轮询计划选项：
     - **每 N 天**

       轮询定期运行，按照指定天数间隔，从指定的日期和时间开始。
       默认下，轮询每天运行一次，从当前系统日期和时间开始。

     - 每 N 分钟

       轮询定期运行，按照指定分钟间隔，从指定的时间开始。
       默认下，轮询每五分钟运行一次，从当前系统时间开始。

- 按星期中的天数

  轮询定期运行，在指定星期的指定时间。
  默认下，轮询每周五 18:00:00 P.M. 运行。

- 每个月在所选周的指定天

  轮询定期运行，在指定月日的指定时间。
  默认情况下，不选择任何日期；默认开始时间为 6:00:00 PM。

- **开始间隔**

  指定 N 的值（分钟或天）。

- **开始于**

  指定何时开始第一次轮询。

- **运行错过的任务**

  如果在计划轮询期间管理服务器被切换掉或不可用，管理服务器可以在切换回来后立即启动轮询，或者等待下次计划轮询。
  如果启用该选项，管理服务器在它切换回来后立即启动轮询。
  如果禁用该选项，管理服务器等待下一次计划轮询。
  默认情况下已启用该选项。

6. 保存更改。

   云段的轮询计划即被配置并保存。

通过 Kaspersky Security Center Web Console 查看云段轮询的结果

您可以查看云段轮询的结果，即查看由管理服务器管理的云设备列表。

要查看云段轮询的结果，

在主菜单中，转到“**发现和部署**”→“**发现**”→“**云**”。

这将显示可用于轮询的云段。

通过 Kaspersky Security Center Web Console 查看云设备的属性

您可以查看每个云设备的属性。

要查看云设备的属性：

1. 在主菜单中，转到 “**资产(设备)**” → “**受管理设备**”。
2. 单击要查看其属性的设备的名称。
   属性窗口打开，在其中已选择“**常规**”区域。
3. 如果要查看特定于云设备的属性，请在属性窗口中选择“**系统**”区域。
   显示的属性取决于设备的云平台。
   对于 AWS 中的设备，将显示以下属性：
   - **使用 API 发现的设备**（值：**AWS**）
   - **云区域**
   - **云 VPC**
   - **云可用区域**
   - **云子网**
   - **云放置组**（仅当实例属于某个放置组时才显示此单元；否则，不显示此单元）

   对于 Azure 中的设备，将显示以下属性：
   - **使用 API 发现的设备**（值：**Microsoft Azure**）
   - **云区域**
   - **云子网**

   对于 Google Cloud 中的设备，将显示以下属性：
   - **使用 API 发现的设备**（值：**Google Cloud**）
   - **云区域**
   - **云 VPC**
   - **云可用区域**
   - **云子网**

与云同步：配置移动规则

在配置云环境操作期间，与云同步规则被自动创建。此规则允许您自动将每次轮询中检测到的设备从未分配的设备组移动到受管理设备\云组，以便对这些设备进行集中管理。默认下，规则在创建后被激活。您可以在任意时刻禁用、修改或强制规则。

要编辑“与云同步”规则的属性和/或强制实施规则：

1. 在主菜单中，转到“**发现和部署**”→“**部署和分配**”→“**移动规则**”。
   这将打开移动规则列表。
2. 在移动规则列表中，选择“**与云同步**”。
   这将打开规则属性窗口。
3. 如有必要，在“**云段**”选项卡的“**规则条件**”选项卡中指定以下设置：

   - **设备在云段中**

     该规则仅应用到位于所选云段的设备。否则，该规则应用到发现的所有设备。
     默认情况下已选定该选项。

   - **包含子对象**

     该规则应用到所选段和其所有嵌套云子区域中的所有设备。否则，该规则仅应用到位于根段的设备。
     默认情况下已选定该选项。

   - **从嵌套对象移动设备到对应子组**

     如果启用该选项，嵌套对象的设备将被自动移动到对应其结构的子组。
     如果禁用该选项，嵌套对象的设备将被自动移动到云子组的根，而不再分支。
     默认情况下已启用该选项。

   - **创建对应于新检测到设备的容器的子组**

     如果启用该选项，当**受管理设备云**结构没有匹配包含设备的区域的子组，Kaspersky Security Center 将创建这类子组。例如，如果一个子网在设备发现中被发现，带有相同名称的新组将在**受管理设备\云**组下被创建。
     如果禁用该选项，Kaspersky Security Center 不创建任何新子组。例如，如果一个子网在网络轮询中被发现，带有相同名称的新组将不在**受管理设备云**组下被创建，且该子组中的设备将被移动到**受管理设备云**组。
     默认情况下已启用该选项。

   - **删除在云段中未找到匹配的子组**

     如果启用该选项，应用程序从云组删除所有不匹配任何现有云对象的子组。
     如果禁用该选项，未匹配任何现有云对象的子组被保留。
     默认情况下已启用该选项。

   如果在使用云环境配置向导时启用了“**与云结构同步管理组**”选项，将创建“**与云同步**”规则并启用“**创建对应于新检测到设备的容器的子组**”和“**删除在云段中未找到匹配的子组**”选项。

如果未启用“**与云结构同步管理组**”选项，将创建“**与云同步**”规则，并禁用（清除）这些选项。如果使用 Kaspersky Security Center 进行的工作需要**受管理设备\云**子组中的子组结构与云段的结构相匹配，请启用规则属性中的“**创建对应于新检测到设备的容器的子组**”和“**删除在云段中未找到匹配的子组**”选项，然后强制执行规则。

4. 在“**使用 API 发现的设备**”下拉列表中，选择以下值之一：

   - **否**。无法使用 AWS API、Azure API 或 Google API 检测到该设备，也就是说，该设备位于云环境之外，或者位于云环境中，但是由于某种原因无法使用 API 检测到该设备。
   - **AWS**。设备使用 AWS API 发现，就是，设备在 AWS 云环境中。
   - **Azure**。设备使用 Azure API 发现，就是，设备在 Azure 云环境中。
   - **Google Cloud**。设备使用 Google API 发现，就是，设备在 Google 云环境中。
   - 没有值。该标准无法被应用。

5. 如果必要，在其他区域设置其他规则属性。

移动规则即被配置。

将应用程序远程安装到 Azure 虚拟机

您必须拥有有效的授权许可才能在 Microsoft Azure 虚拟机上安装应用程序。

Kaspersky Security Center 支持以下情景：

- 客户端设备通过 Azure API 发现；安装也通过 API 执行。使用 Azure API 意味着您只能安装以下应用程序：
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- 客户端设备通过 Azure API 发现；安装通过分发点执行，如果没有分发点，则使用独立安装包手动执行。您可以通过这种方式安装 Kaspersky Security Center 支持的任何应用程序。

要创建在 Azure 虚拟机上远程安装应用程序的任务：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。
   “新任务向导”启动。
3. 遵照向导的说明操作：
   a. 选择**远程安装应用程序**作为任务类型。
   b. 在**安装包**页面上，选择**由 Microsoft Azure API 进行的远程安装**。

c. 选择访问设备的账户时，使用现有的 Azure 账户，或单击“**添加**”并输入您的 Azure 账户的凭证：

- **Azure 账户名**

  为您指定的凭证输入任何名称。此名称将显示在运行该任务的账户列表中。

- **Azure 应用程序 ID**

  您在 Azure 门户创建了该应用程序 ID。

  您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

- **Azure 应用程序密码**

  当您创建应用程序 ID 时您收到应用程序 ID 的密码。

  密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

d. 从**受管理设备\云**组中选择相关的设备。

在向导完成后，应用程序远程安装任务显示在任务列表中。

使用云 DBMS 创建管理服务器数据备份任务

备份任务是管理服务器任务。如果要使用位于云环境（AWS 或 Azure）中的 DBMS，请创建备份任务。

若要创建管理服务器数据备份任务，请执行以下操作：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。
2. 单击**添加**。

   “新任务向导”启动。
3. 在该向导的第一页上的“**应用程序**”列表中，选择“**Kaspersky Security Center 15.1**”，然后在“**任务类型**”列表中选择“**备份管理服务器数据**”。
4. 在向导的相应页面上，指定以下信息：

   - 如果使用 AWS 中的数据库：

     - **S3 bucket 名称**

       您为备份创建的 S3 bucket 名称。

     - **访问密钥 ID**

       当您创建了 IAM 用户账户以使用 S3 bucket 存储实例时，您接收到密钥 ID（数字字母序列）。

       如果您在 S3 bucket 上选择了 RDS 数据库则该字段可用。

- **Secret key**

  您创建IAM 用户账户时接收到的带有访问密钥 ID 的secret key。

  Secret key 的字符显示为星号。在您开始输入 secret key 后，**显示**按钮被显示。点击并按住该按钮一定时间以查看输入的字符。

  如果您选择了 AWS IAM 访问密钥来授权而不是 IAM 角色，该字段可用。

- 如果使用 Microsoft Azure 中的数据库：

  - **Azure 存储账户名**

    您创建了Azure 存储账户名称以使用 Kaspersky Security Center。

  - **Azure 订阅 ID**

    您在 Azure 门户创建了该订阅。

  - **Azure 密码**

    当您创建应用程序 ID 时您收到应用程序 ID 的密码。

    密码的字符显示为星号。在您开始输入密码后，**显示**按钮可用。点击并按住该按钮以查看您输入的字符。

  - **Azure 应用程序 ID**

    您在 Azure 门户创建了该应用程序 ID。

    您仅可以提供一个 Azure 应用程序 ID 用于轮询和其他目的。如果您要轮询其他 Azure 段，您必须先删除现有 Azure 连接。

  - **Azure SQL Server 名称**

    名称和资源组在您的 Azure SQL Server 属性中可用。

  - **Azure SQL Server 资源组**

    名称和资源组在您的 Azure SQL Server 属性中可用。

  - **Azure 存储访问密钥**

    在您的存储账户属性中可用，在访问密钥区域。您可以使用任何密钥（key1 或 key2）。

任务被创建并显示在任务列表。如果启用"**创建完成时打开任务详情**"选项，可以在创建任务后立即修改默认任务设置。如果您不启用该选项，任务使用默认设置创建。您可以稍后随时修改默认设置。

客户端设备的远程诊断

您可以使用远程诊断在 Windows 和 Linux客户端设备上远程执行以下操作：

- 启用和禁用跟踪、更改跟踪等级、下载跟踪文件
- 下载系统信息和应用程序设置
- 下载事件日志
- 为应用程序创建内存转储文件
- 开始诊断并下载诊断报告
- 开始、停止和重新启动应用程序

您可以使用从客户端设备下载的事件日志和诊断报告以自行定位问题。此外，如果您联系 Kaspersky 技术支持，一名技术支持专家可能让您从客户端设备下载跟踪文件、转储文件、事件日志和诊断报告以便让 Kaspersky 进一步分析。

打开远程诊断窗口

要对 Windows 和 Linux 客户端设备执行远程诊断，首先必须打开远程诊断窗口。

要打开远程诊断窗口：

1. 要选择要为其打开远程诊断窗口的设备，请执行以下操作之一：
   - 如果该设备属于管理组，请在主菜单中转到**资产(设备) → 受管理设备**。
   - 如果该设备属于未分配的设备组，请在主菜单中转到“**发现和部署 → 未分配的设备**”。
2. 单击所需设备的名称。
3. 在打开的设备属性窗口中，选择“**高级**”选项卡。
4. 在打开的窗口中，单击“**远程诊断**”。
   这将打开客户端设备的“**远程诊断**”窗口。如果管理服务器和客户端设备之间未建立连接，则会显示错误消息。

或者，如果需要立即获取有关基于 Linux 的客户端设备的所有诊断信息，您可以在此设备上运行 collect.sh 脚本。

启用和禁用应用程序跟踪

您可以启用和禁用应用程序跟踪，包括 Xperf 跟踪。

启用和禁用跟踪

要在远程设备上启用或禁用跟踪：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   “**应用程序管理**”区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择您要启用或禁用跟踪的应用程序。
   远程诊断选项列表将打开。
4. 如果要启用跟踪：
   a. 在列表的“**跟踪**”区域中，单击“**启用跟踪**”。
   b. 在打开的“**修改跟踪级别**”窗口中，我们建议您保留设置的默认值。当需要时，技术支持专家将指导您配置过程。下列设置可用：
      - **跟踪级别**

        跟踪级别定义跟踪文件包含的详情数据量。

      - **基于循环的跟踪**

        应用程序覆盖跟踪信息以防止跟踪文件过量增长。指定用于存储跟踪信息的文件最大数量，以及每个文件的最大大小。如果写入了最大数量的最大大小的跟踪文件，最旧的文件被删除以便新跟踪文件可以被写入。

        此设置仅适用于 Kaspersky Endpoint Security。

   c. 单击“**保存**”。

   将为所选应用程序启用跟踪。某些情况下，要启用跟踪，必须重新启动安全应用程序及其任务。

   在 Linux 客户端设备上，网络代理组件更新程序的跟踪由网络代理设置管理。因此，在运行 Linux 的客户端设备上，此组件的“**启用跟踪**”和“**修改跟踪级别**”选项被禁用。

5. 如果要禁用对所选应用程序的跟踪，请单击“**禁用跟踪**”按钮。
   对所选应用程序的跟踪即被禁用。

启用 Xperf 跟踪

对于 Kaspersky Endpoint Security，技术支持专家可能要求您对系统性能信息启用 Xperf 跟踪。

要启用和配置 Xperf 跟踪或禁用它：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择“Kaspersky Endpoint Security for Windows”。
   Kaspersky Endpoint Security for Windows 的远程诊断选项列表将显示。
4. 在“**Xpref 跟踪**”区域中，单击“**启用 Xperf 跟踪**”。
   如果已经启用 Xperf 跟踪，将显示“**禁用 Xperf 跟踪**”按钮。如果您想要禁用 Kaspersky Endpoint Security for Windows的 Xperf 跟踪，请单击此按钮。
5. 在打开的“**更改 Xperf 跟踪级别**”窗口中，根据技术支持专家的请求，执行以下操作：
   a. 选择以下跟踪级别之一：
   - **轻度级别**

     该类型的跟踪文件包含系统最少量信息。
     默认情况下已选定该选项。

   - **深度级别**

     相比于*轻度*类型的跟踪文件，该类型的跟踪文件包含更多详细信息，且可能在*轻度*类型跟踪文件不足以评估性能时被技术支持专家要求。*深度*跟踪文件包含关于系统的硬件、操作系统、应用程序的启动和结束进程列表、用于性能评估的事件和来自 Windows System Assessment 工具的事件的技术信息。

   b. 选择以下 Xperf 跟踪类型之一：
   - **基本类型**

     跟踪信息在 Kaspersky Endpoint Security 应用程序运行期间被接收。
     默认情况下已选定该选项。

   - **重启时类型**

     跟踪信息在操作系统从受管理设备上启动时接收。该跟踪类型在影响系统性能的问题发生时，在设备被开启后和 Kaspersky Endpoint Security 启动之前有效。

   您可能被要求启用“**循环文件大小(MB)**”选项以防止跟踪文件的过量增长。然后指定跟踪文件的最大大小。当文件达到最大大小时，最旧的跟踪信息被新信息覆盖。

   c. 定义循环文件大小。

   d. 点击“**保存**”。

将启用并配置 Xperf 跟踪。

6. 如果您想要禁用 Kaspersky Endpoint Security for Windows的 Xperf 跟踪，请单击“**Xpref 跟踪**”区域中的“**禁用 Xperf 跟踪**”。

   Xperf 跟踪即被禁用。

下载应用程序的跟踪文件

要下载应用程序的跟踪文件：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。

   应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择要为其下载跟踪文件的应用程序。
4. 在“**跟踪**”区域，单击“**跟踪文件**”按钮。

   这将打开“**设备跟踪日志**”窗口，其中显示了跟踪文件列表。
5. 在跟踪文件列表中，选择要下载的文件。
6. 执行以下操作之一：

   - 单击“**下载**”下载所选文件。您可以选择一个或多个文件进行下载。
   - 下载所选文件的一部分：

     a. 单击“**下载一部分**”。

     您无法同时下载多个文件的部分内容。如果您选择多个跟踪文件，**下载一部分**按钮将被禁用。

     b. 在打开的窗口中，根据需要指定名称和要下载的文件部分。

     对于 Linux 设备，无法编辑文件部分名称。

     c. 单击“**下载**”。

所选文件或其一部分将下载到您指定的位置。

删除跟踪文件

您可以删除不再需要的跟踪文件。

要删除跟踪文件：

1. 打开客户端设备的远程诊断窗口。
2. 在打开的远程诊断窗口中，选择“**事件日志**”选项卡。
3. 在“**跟踪文件**”区域中，单击“**Windows Update 日志**”或“**远程安装日志**”，具体取决于要删除哪些跟踪文件。

Windows Update 日志链接仅适用于基于 Windows 的客户端设备。

这将打开“**设备跟踪日志**”窗口，其中显示了跟踪文件列表。

4. 在跟踪文件列表中，选择一个或多个要删除的文件。
5. 单击“**删除**”按钮。

所选跟踪文件即被删除。

下载应用程序设置

要从客户端设备下载应用程序设置：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
3. 在“**应用程序设置**”区域中，单击“**下载**”按钮下载有关客户端设备上安装的应用程序的设置的信息。

包含信息的 ZIP 存档将被下载到指定位置。

下载事件日志

要从远程设备下载事件日志：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口的“**事件日志**”选项卡上，单击“**所有设备日志**”。
3. 在“**所有设备日志**”窗口中，选择一个或多个相关日志。
4. 执行以下操作之一：
   - 单击“**下载整个文件**”下载所选日志。
   - 下载所选日志的一部分：
     a. 单击“**下载一部分**”。
     您无法同时下载多个日志的部分内容。如果您选择了多个事件日志，**下载一部分**按钮将被禁用。
     b. 在打开的窗口中，根据需要指定名称和要下载的文件部分。
     对于 Linux 设备，无法编辑日志部分名称。
     c. 单击“**下载**”。

所选事件日志或其一部分将被下载到指定的位置。

启动、停止和重新启动应用程序

您可以启动、停止和重新启动客户端设备上的应用程序。

若要启动、停止和重新启动应用程序，请执行以下操作：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择要启动、停止或重新启动的应用程序。
4. 单击以下按钮之一来选择操作：
   - **停止应用程序**
     仅当应用程序当前正在运行时，此按钮才可用。
   - **重启应用程序**
     仅当应用程序当前正在运行时，此按钮才可用。
   - **启动应用程序**
     仅当应用程序当前未运行时，此按钮才可用。

   根据您选择的操作，客户端设备上将启动、停止或重新启动所需应用程序。

如果重新启动网络代理，将显示一条消息，指示设备与管理服务器的当前连接将丢失。

运行 Kaspersky Security Center 网络代理的远程诊断并下载结果

要在远程设备上启动 Kaspersky Security Center 网络代理的诊断并下载结果：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**卡巴斯基应用程序**选项卡。
   应用程序管理区域会显示设备上安装的卡巴斯基应用程序列表。
3. 在应用程序列表中，选择**Kaspersky Security Center 网络代理**。
   远程诊断选项列表将打开。
4. 在“**诊断报告**”部分中，单击“**运行诊断**”按钮。
   这将启动远程诊断过程并生成诊断报告。诊断过程完成后，“**下载诊断报告**”按钮变为可用。
5. 单击“**下载诊断报告**”按钮下载报告。

   报告将被下载到指定位置。

在客户端设备上运行应用程序

如果卡巴斯基技术支持专家要求，您可能需要在客户端设备上运行应用程序。您不必在该设备上安装应用程序。

要在客户端设备上运行应用程序：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**运行远程应用程序**选项卡。
3. 在**应用程序文件**部分中，单击**浏览**按钮以选择包含要在客户端设备上运行的应用程序的 ZIP 存档。

   ZIP 存档必须包含实用程序文件夹。此文件夹包含要在远程设备上运行的可执行文件。

   如有必要，您可以指定可执行文件名和命令行参数。为此，请填写**要在远程设备上运行的存档中的可执行文件**和**命令行参数**字段。
4. 单击**上传和运行**按钮以在客户端设备上运行指定的应用程序。
5. 按照卡巴斯基支持专业人员的指示操作。

为应用程序创建内存转储文件

应用程序转储文件允许您查看某个时间点在客户端设备上运行的应用程序的参数。该文件还包含有关为应用程序加载的模块的信息。

不支持从基于 Linux 的设备获取转储文件。

为了通过远程诊断获取转储文件，可以使用 kldumper 实用程序。此实用程序旨在根据技术支持专家的要求获取卡巴斯基应用程序进程的转储文件。有关使用 kldumper 实用程序的要求的详细信息，请参阅Kaspersky Security Center 知识库。

要为应用程序创建转储文件：

1. 打开客户端设备的远程诊断窗口。
2. 在远程诊断窗口中，选择**运行远程应用程序**选项卡。
3. 在**生成进程内存转储文件**区域中，指定要为其生成转储文件的应用程序的可执行文件。
4. 单击**下载转储文件**按钮。

   包含指定应用程序的转储文件的档案被下载。

   如果客户端设备上未运行指定的应用程序，则下载的存档中包含的“结果”文件夹将为空。

   如果指定的应用程序正在运行，但下载失败并出现错误，或者下载的存档中包含的“结果”文件夹为空，请参阅Kaspersky Security Center 知识库。

在基于 Linux 的客户端设备上运行远程诊断

Kaspersky Security Center 允许您从客户端设备下载基本诊断信息。或者，您可以使用卡巴斯基的 collect.sh 脚本获取有关基于 Linux 的设备的诊断信息。该脚本在需要诊断的 Linux 客户端设备上运行，然后生成一个文件，其中包含诊断信息、该设备的系统信息、应用程序的跟踪文件、设备日志以及被紧急终止的应用程序的转储文件。

我们建议您使用 collect.sh 脚本一次性获取有关 Linux 客户端设备的所有诊断信息。如果通过 Kaspersky Security Center 远程下载诊断信息，您将需要浏览远程诊断界面的所有部分。此外，可能无法完全获得 Linux 设备的诊断信息。

如果您需要将生成的包含诊断信息的文件发送给卡巴斯基技术支持，请在发送文件之前删除所有机密信息。

要使用 collect.sh 脚本从 Linux 客户端设备下载诊断信息：

1. 下载 collect.sh 脚本，它在collect.tar.gz 存档中。
2. 将下载的压缩包复制到需要诊断的 Linux 客户端设备上。
3. 运行以下命令解压 collect.tar.gz 存档：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 执行以下命令指定脚本执行权限：

   ```
   # chmod +x collect.sh
   ```

5. 使用具有管理员权限的账户运行 collect.sh 脚本：

   ```
   # ./collect.sh
   ```

一个包含诊断信息的文件将生成并被保存到 /tmp/$HOST_NAME-collect.tar.gz 文件夹中。

从隔离区和备份中下载和删除文件

本节提供有关如何从 Kaspersky Security Center Web Console 的隔离区和备份中下载和删除文件的信息。

从隔离区和备份区中下载文件

只有满足以下两个条件之一，您才能下载隔离区和备份区中的文件：在设备的设置中启用了“**不断开与管理服务器的连接**”选项，或者正在使用连接网关。否则，下载无法进行。

要将隔离区或备份中的文件的副本保存到硬盘驱动器，请执行以下操作：

1. 执行以下操作之一：
   - 如果要从隔离区保存文件副本，请在主菜单中转到**操作** → **存储库** → **隔离**。
   - 如果要从备份区保存文件副本，请在主菜单中转到**操作** → **存储库** → **备份**。
2. 在打开的窗口中，选择要下载的文件并单击 **下载**。

下载开始。已放置在客户端设备上隔离区中的文件的副本将被保存到指定的文件夹中。

更改 Kaspersky Security Center Web Console 界面的语言

您可以选择 Kaspersky Security Center Web Console 界面的语言。

要更改界面语言：

1. 在主菜单中，转到“**设置**” → “**语言**”。
2. 选择一种受支持的本地化语言。

API 参考指南

本 Kaspersky Security Center OpenAPI 参考指南旨在帮助完成以下任务：

- 自动化和自定义。您可以将您可能不想使用管理控制台手动处理的任务自动化。您还可以实施管理控制台尚不支持的自定义方案。例如，作为管理员，您可以使用 Kaspersky Security Center OpenAPI 创建和运行脚本，这些脚本将有助于开发管理组的结构并使该结构保持最新。

- 自定义开发。例如，您可以为客户开发一个替代的基于 MMC 的管理控制台，该控制台允许执行有限的一组操作。

在 OpenAPI 参考指南中，您可以使用屏幕右侧的搜索字段查找所需的信息。

OPENAPI 参考指南

脚本示例

OpenAPI 参考指南包含下表中列出的 Python 脚本示例。这些示例展示了如何调用 OpenAPI 方法并自动完成保护网络的各种任务，例如，创建"主要/从属"层级，在 Kaspersky Security Center 中运行任务，或分配分发点。您可以按原样运行示例，也可以基于示例创建您自己的脚本。

要调用 OpenAPI 方法并运行脚本：

1. 下载 KlAkOAPI.tar.gz 压缩文件。此压缩文件包括 KlAkOAPI 软件包和示例（您可以从压缩文件或 OpenAPI 参考指南中复制它们）。KlAkOAPI.tar.gz 存档也位于 Kaspersky Security Center 安装文件夹中。

2. 在安装了管理服务器的设备上安装来自 KlAkOAPI.tar.gz 压缩文件的 KlAkOAPI 软件包。

   您只能在安装了管理服务器和 KlAkOAPI 软件包的设备上调用 OpenAPI 方法、运行示例和您自己的脚本。

用户方案与 Kaspersky Security Center OpenAPI 方法示例之间的匹配

示例	示例目的	方案
Log KlAkParams	您可以使用 `KlAkParams` 数据结构提取和处理数据。该示例展示了如何使用此数据结构。 该示例输出可以以不同的方式呈现。您可以获取数据以发送 HTTP 方法或在您的代码中使用它。	监控和报告
创建和删除"主要/从属"层次结构	您可以添加从属管理服务器，并建立"主要/从属"层次结构。或者，您可以断开从属管理服务器与层次结构的连接。	• 创建管理服务器层级：添加从属管理服务器 • 删除管理服务器层级
使用基于 Active Directory 单元的结构创建组层次结构	您可以轮询 Active Directory 单元并形成已发现设备组的层次结构。	创建管理组
使用基于缓存的 Active Directory 单元的结构创建组层次结构	您可以根据之前轮询的 Active Directory 单元形成受管理设备组的层次结构。如果新设备在上次轮询后出现在 Active Directory 中，则不会将它们添加到组中，因为它们不在保存的轮询结果中。	创建管理组
通过连接网关下载网络列表文件到指定设备	您可以通过使用连接网关连接到所需设备上的网络代理，然后将包含网络列表的文件下载到您的设备。	分发点和连接网关的调整
将主管理服务器存储库中存储的授权许可密钥安装到从属管理服务器上	您可以连接到主管理服务器，从中下载所需的授权许可密钥，然后将此密钥传输到层次结构中包含的所有从属管理服务器。	受管理应用程序的授权许可
创建有效用户权限报告	您可以创建不同的报告。例如，您可以使用此示例生成有效用户权限的报告。此报告描述了用户拥有的权限，具体取决于他或她的组和角色。 您可以下载 HTML、PDF 或 Excel 格式的报告。	生成和浏览报告

示例	示例目的	方案
为设备启动任务	您可以通过使用连接网关连接到所需设备上的网络代理，然后允许必要的任务。	手动启动任务
基于 Active Directory 站点和服务创建 IP 子网	您可以根据您使用的 Active Directory 单元创建 IP 子网。 该示例启动对指定 IP 范围的轮询并删除发现的子网，以避免它们与新子网发生冲突。因此，请勿在需要保存子网的网络中运行此示例。 轮询后，示例引用 Active Directory，检查其中的每个设备，并创建 IP 子网。为此，示例使用了所有设备的掩码和 IP 地址。	配置网络保护
为组中的设备注册分发点	您可以将受管理设备分配为分发点（以前称为更新代理）。	更新 Kaspersky 数据库和应用程序
对所有组进行枚举	您可以对管理组采取不同操作。该示例显示了如何执行以下操作： • 获取"受管理设备"根组的标识符 • 在组层次结构中移动 • 检索完整的、扩展的组层次结构以及它们的名称和嵌套	配置管理服务器
枚举任务、查询任务统计信息和运行任务	您可以找到以下信息： • 任务进度历史 • 当前任务状态 • 不同状态的任务数 您还可以运行任务。默认情况下，示例在输出统计信息后运行任务。	监视任务执行
创建并运行任务	您可以创建任务。在示例中指定以下任务参数： • 类型 • 运行方法 • 名称 • 将使用任务的设备组 默认情况下，示例创建了一个"显示消息"类型的任务。您可以为管理服务器的所有受管理设备运行此任务。如有需要，您可以指定自己的任务参数。	创建任务
枚举授权许可密钥	您可以获得安装在管理服务器受管理设备上的 Kaspersky 应用程序的所有活动授权许可密钥的列表。该列表包含关于每个授权许可密钥的详细数据，例如名称、类型或到期日期。	查看使用中授权许可密钥的相关信息
创建和查找内部用户	您可以创建一个账户以进行进一步的工作。	选择账户以启动管理服务器
创建自定义类别	您可以根据所需参数创建应用程序类别。	创建含有手动添加内容的应用程序类别
使用 SrvView 枚举用户	您可以使用 SrvView 类向管理服务器请求详细信息。例如，您可以使用此示例获取用户列表。	管理用户账户

通过 OpenAPI 与 Kaspersky Security Center 交互的应用程序

一些应用程序通过 OpenAPI 与 Kaspersky Security Center 交互。例如，此类应用程序包括 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization。这也可以是您基于 OpenAPI 开发的自定义客户端应用程序。

通过 OpenAPI 与 Kaspersky Security Center 交互的应用程序连接到管理服务器。如果您配置了可连接到管理服务器的 IP 地址允许列表，请添加安装了使用 Kaspersky Security Center OpenAPI 的应用程序的设备的 IP 地址。要了解您使用的应用程序是否通过 OpenAPI 工作，请参阅此应用程序的帮助。

服务提供商最佳实践

该区域提供有关如何配置和使用 Kaspersky Security Center 的信息。

该区域包含如何部署、配置和使用应用程序的建议，描述了解决应用程序操作中的典型问题的方法。

计划 Kaspersky Security Center 部署

当在组织网络中计划 Kaspersky Security Center 组件的部署时，您必须考虑到项目的大小和范围，尤其是以下因素：

- 设备总数
- MSP 客户端数量

一个管理服务器可以支持最多 100,000 台设备。如果组织网络中的设备总数超过 100,000，必须在服务提供商端部署多个管理服务器，并合并到一个方便集中管理的层级。

500 台虚拟服务器可以被创建在单一管理服务器，因此每 500 台 MSP 客户端需要一个单一管理服务器。

在部署计划阶段，必须考虑到特别证书 X.509 到管理服务器的分配。X.509 证书到管理服务器的分配可能用在以下情况（部分列表）：

- 通过 SSL 终端代理检查安全套接层（SSL）流量
- 在证书字段中指定所需值
- 提供所需的证书加密长度

提供到管理服务器的互联网访问

要允许客户端网络设备通过互联网访问管理服务器，您必须启用以下管理服务器端口：

- 13000 TCP—管理服务器 TLS 端口，用于连接部署在客户端网络的网络代理
- 8061 TCP—HTTPS 端口，用于使用管理控制台工具发布独立包
- 8060 TCP—HTTPS 端口，用于使用管理控制台工具发布独立包
- 13292 TCP—TLS 端口，仅在有需要被管理的移动设备时需要

如果您需要提供客户端通过 Kaspersky Security Center Web Console 进行网络管理的基本选项，您也必须打开 Kaspersky Security Center Web Console 端口 8080 TCP (HTTPS port)：

Kaspersky Security Center 标准配置

一个或几个管理服务器被部署到 MSP 服务器。管理服务器数量可以基于可用硬件、服务的 MSP 客户端总数或受管理设备总数来选择。

一个管理服务器可以支持最多 100,000 台设备。您必须考虑今后增加受管理设备的数量的可能性：最好连接较少设备到单一管理服务器。

500 台虚拟服务器可以被创建在单一管理服务器，因此每 500 台 MSP 客户端需要一个单一管理服务器。

如果使用了多个服务器，建议您合并它们到一个层级。使用管理服务器层级允许您避免冗余策略和任务、处理整个受管理设备，使它们看起来是被单一管理服务器管理：例如，搜索设备、创建设备分类和创建报告。

在每个对应于 MSP 客户端的虚拟服务器上，您必须分配一个或几个分发点。如果 MSP 客户端和管理服务器通过互联网连接，最好为分发点创建“*将更新下载至分发点存储库*”任务，这样它们将从 Kaspersky 服务器直接下载更新，而不是从管理服务器。

如果 MSP 客户端网络的一些设备不能直接访问互联网，您必须切换分发点到连接网关模式。此种情况下，MSP 客户端网络中的网络代理将被通过网关而不是直接连接到管理服务器，为了后期同步。

作为管理服务器，很可能无法轮询 MSP 客户端网络，最好把该功能转给分发点。

管理服务器将无法发送通知到 MSP 客户端网络 NAT 以外的受管理设备的端口 15000 UDP。要解决该问题，最好在作为分发点并运行在连接网关模式的设备的属性中启用持续连接到管理服务器模式(**不断开与管理服务器的连接**复选框)。如果分发点总数不超过 300 则持续连接模式可用。

关于分发点

网络代理设备可以用作分发点。在该模式中，网络代理可以运行以下功能：

- 传输文件到客户端设备，包括：
  - 卡巴斯基数据库和软件模块更新

    更新可以从管理服务器或者从卡巴斯基服务器提取。在后一种情况下，“*将更新下载至分发点存储库*”任务必须为作为分发点的设备创建。
  - 第三方软件更新
  - 安装包
  - 将管理服务器用作 WSUS 服务器时的 Windows 更新
- 安装软件（包括网络代理初始化部署）到其他设备。
- 轮询网络以检测新设备并更新现有设备的信息。分发点应用与管理服务器相同的设备发现方法。

在组织网络中部署分发点可以带来以下好处：

- 如果管理服务器作为更新源，则降低其负载。
- 在这种情况下，由于 MSP 客户端网络上的每个设备都没有必要访问卡巴斯基服务器或管理服务器以进行更新，因此优化互联网流量。
- 提供管理服务器到 MSP 客户端网络 NAT 之外的访问(与管理服务器相关)，这允许管理服务器运行以下操作：
  - 在 IPv4 或 IPv6 网络上通过 UDP 向设备发送通知
  - 轮询 IPv4 或 IPv6 网络
  - 执行初始部署
  - 用作推送服务器

为每个管理组分配分发点。此种情况下，分发点的范围包括管理组和其所有子组中的所有设备。然而，作为分发点的设备不必须包含在它被分配的管理组。

您可以让分发点作为连接网关工作。此种情况下，分发点范围内的设备将被通过网关，而不是直接连接到管理服务器。该模式用在不允许在网络代理和管理服务器设备之间建立直接连接的情景。

作为分发点的设备必须被保护，包括物理保护，以防范非授权的访问。

管理服务器层级

一个 MSP 可能运行多个管理服务器。可能不方便管理几个不同的管理服务器，因此可以应用层次结构。两个管理服务器的“主/从”配置提供了以下选项：

- 一个从属管理服务器从主管理服务器继承策略和任务，这防止了重复设置。
- 主管理服务器上的设备分类可以包含从属管理服务器的设备。
- 主管理服务器的报告可以包含从属管理服务器的数据（包括详细信息）。

主管理服务器仅接收来自上面列出的选项范围内的非虚拟从属管理服务器的数据。此限制不适用于虚拟管理服务器，虚拟管理服务器与其主管理服务器共享数据库。

虚拟管理服务器

基于物理管理服务器，可以创建多个虚拟管理服务器，它们与从属管理服务器相似。相比于基于访问控制列表（ACLs）的任意访问模式，虚拟管理服务器模式功能更强大并且提供更高度隔离。除了具有策略和任务的已分配设备的专用管理组结构外，每个虚拟管理服务器还具有自己的未分配设备组、自己的报告集、选定的设备和事件、安装包、移动规则等。为了最大限度地相互隔离 MSP 客户端，我们建议您选择虚拟管理服务器作为要使用的功能。而且，为每个 MSP 客户端创建虚拟管理服务器允许您提供客户端通过 Kaspersky Security Center Web Console 的网络管理的基本选项。

虚拟管理服务器与从属管理服务器非常相似，但是有以下不同点：

- 虚拟管理服务器缺少多数全局设置和自己的 TCP 端口。
- 虚拟管理服务器没有从属管理服务器。
- 虚拟管理服务器没有其他虚拟管理服务器。
- 物理管理服务器可以查看它所有虚拟管理服务器的设备、组、事件和受管理设备上的对象（隔离区条目、应用程序注册表等等）。
- 虚拟管理服务器仅可以扫描连接了分发点的网络。

使用 Kaspersky Endpoint Security for Android 管理移动设备

安装了 Kaspersky Endpoint Security for Android™ 的移动设备(也叫 KES 设备)通过管理服务器管理。Kaspersky Security Center 支持以下管理 KES 设备的功能：

- 将移动设备处理为客户端设备：
  - 管理组中的成员关系
  - 监控，例如查看状态、事件和报告
  - 修改本地设置和为 Kaspersky Endpoint Security for Android 分配策略
- 以集中模式发送命令
- 远程安装移动应用包

管理服务器通过 TLS、TCP 端口 13292 管理 KES 设备。

部署和初始化设置

Kaspersky Security Center 是一个分发的应用程序。Kaspersky Security Center 包含以下应用程序：

- 管理服务器 — 核心组件，设计用于管理组织设备和在 DBMS 中存储数据。
- 管理控制台 — 管理员基本工具。管理控制台与管理服务器一起出货，但是它也可以被单独安装在一个或几个由管理员运行的设备上。
- Kaspersky Security Center Web Console — 设计用于基本操作的管理服务器 Web 界面。您可以安装该组件到满足硬件和软件需求的设备。
- 网络代理 — 设计用于管理安装在设备上的安全应用程序，同时获取设备信息。网络代理安装在组织设备上。

Kaspersky Security Center 在组织网络上的部署运行如下：

- 管理服务器的安装
- Kaspersky Security Center Web Console 的安装
- 管理员设备上管理控制台的安装
- 网络代理和企业设备上安全应用程序的安装

管理服务器安装建议

该部分包含了如何安装管理服务器的建议。该部分还提供了使用管理服务器上的共享文件夹以便部署网络代理到客户端设备的方案。

在失败转移集群上为管理服务器服务创建账户

默认下，安装程序自动为管理服务器服务创建非特权账户。该行为对于在常规设备上安装管理服务器来说是最方便的。

然而，在失败转移的集群上安装管理服务器需要不同的方案：

1. 为管理服务器服务创建非特权域账户，并把它们作为以 KLAdmins 为名称的全局域安全组的成员。
2. 在管理服务器安装程序中，指定为服务创建的域账户。

选择 DBMS

当选择管理服务器使用的数据库管理系统（DBMS）时，您必须考虑到被管理服务器覆盖的设备数量。

下表列出了有效 DBMS 选项，以及它们的使用建议和限制。

对 DBMS 的建议和限制

DBMS	建议和限制
SQL Server Express Edition 2016 或后续版本	如果您打算为少于 10,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。 您可以限制事件存储库中事件的最大数量，以防止数据库溢出。 有关详细信息，请参阅以下主题：数据库空间的计算。 SQL Server Express Edition DBMS 被管理服务器和其他应用程序同时使用是被严格禁止的。 **执行 Windows 更新同步**任务不支持 Microsoft SQL Express 数据库。
本地 SQL Server 版本，而不是 Express 2016 或后续版本	没有限制。
远程 SQL Server 版本，而不是 Express 2016 或后续版本	仅在两台设备都在相同 Windows® 域中时可用；如果域不同，必须在它们之间建立双向信任关系。

DBMS	建议和限制
本地或远程 MySQL 5.5、5.6 或 5.7（MySQL 版本 5.5.1、5.5.2、5.5.3、5.5.4 和 5.5.5 不再被支持）	如果您打算为少于 10,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。
本地或远程 MySQL 8.0.20 或更高版本	如果您打算为少于 50,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。
本地或远程 MariaDB（查看受支持的版本）	如果您打算为少于 20,000 台设备运行单个管理服务器，请使用此 DBMS。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。
PostgreSQL、Postgres Pro（查看支持的版本）	如果您打算为少于 50,000 台设备运行单个管理服务器，请使用这些 DBMS 之一。 建议禁用软件清单任务并禁用（在卡巴斯基 Endpoint Security 策略设置中）管理服务器对已启动应用程序的通知。有关详细信息，请参阅以下主题：数据库空间的计算。

如果您使用 PostgreSQL、MariaDB 或 MySQL DBMS，则**事件**选项卡可能会显示所选客户端设备的不完整事件列表。当 DBMS 存储大量事件时就会发生这种情况。您可以通过执行以下操作之一来增加显示的事件数量：

- 删除不必要的事件。
- 减少不必要事件的存储期限。

要查看设备管理服务器上记录的完整事件列表，请使用报告。

如果将 SQL Server 2019 用作 DBMS，并且未安装累积补丁 CU12 或更高版本，则在安装 Kaspersky Security Center 之后，必须执行以下操作：

1. 使用 SQL Management Studio 连接到 SQL Server。
2. 运行以下命令（如果为数据库选择了其他名称，请使用该名称而不是 KAV）：

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. 重新启动 SQL Server 2019 服务。

否则，使用 SQL Server 2019 可能导致错误，例如"资源池 'internal' 中没有足够的系统内存来运行此查询。"

指定管理服务器地址

当安装管理服务器时，您必须指定管理服务器外部地址。该地址将用作创建网络代理安装包时的默认地址。此后，您将可以通过使用管理控制台工具更改管理服务器主机地址；地址将不会在所创建的网络代理安装包中自动更改。

在客户端组织网络中配置保护

管理服务器安装完成后，管理控制台启动并提示您通过相关向导执行初始化设置。当快速启动向导运行时，以下策略和任务在根管理组中被创建：

- Kaspersky Endpoint Security 策略
- 更新 Kaspersky Endpoint Security 的组任务
- 扫描 Kaspersky Endpoint Security 设备的组任务
- 网络代理策略
- 漏洞扫描任务(网络代理任务)
- 更新安装和漏洞修复任务(网络代理任务)

策略和任务使用默认设置创建，这对组织来说可能是不佳的或不合理的。因此，您必须检查所创建对象的属性并在必要时手动修改它们。

该部分包含了手动配置策略、任务和其他管理服务器设置的信息，以及分发点、构建管理组结构和任务层级以及其他设置的信息。

Kaspersky Endpoint Security 策略的手动设置

本节提供关于如何配置 Kaspersky Endpoint Security 策略的建议，该策略由快速启动向导创建。您可以在策略属性窗口中执行设置。

当编辑设置时，请记住您必须点击相关设置之上的锁图标以便允许在工作站上使用该值。

在高级威胁防护区域配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

在**高级威胁防护**区域中，您可以为 Kaspersky Endpoint Security for Windows 配置卡巴斯基安全网络的使用。您还可以配置 Kaspersky Endpoint Security for Windows 模块，例如行为检测、漏洞利用防御、主机入侵防御和修复引擎。

在**卡巴斯基安全网络**子区域，建议您启用**卡巴斯基安全网络**选项。使用此选项有助于重新分发和优化网络流量。如果“**卡巴斯基安全网络**”选项被禁用，您可以启用直接“使用 KSN 服务器”。

在关键威胁防护部分配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

在策略属性窗口的**基本威胁防护**区域，建议您在**防火墙**和**文件威胁防护**子区域指定附加设置。

防火墙子区域包含允许您控制客户端设备上应用程序的网络活动的设置。客户端设备使用分配了“公共”、“本地”或“受信任”状态的网络。根据网络状态，Kaspersky Endpoint Security 可以选择允许或拒绝设备上的网络活动。向组织添加新网络时，您必须为其分配适当的网络状态。例如，如果客户端设备是笔记本电脑，则建议使用公共或受信任的网络，因为笔记本电脑有时连接的不是本地网络。在**防火墙**子区域，您可以检查是否为组织所用的网络分配了正确的状态。

要查看网络列表：

1. 在策略属性中，转到**基本威胁防护 → 防火墙**。
2. 在**可用网络**区域中，单击**设置**按钮。
3. 在打开的**防火墙**窗口中，转到**网络**选项卡以查看网络列表。

在**文件威胁防护**子区域，您可以禁用网络驱动器扫描。网络驱动器扫描可以显著提高网络驱动器负载。在文件服务器上执行间接扫描更方便。

要禁用网络驱动器扫描：

1. 在策略属性中，转到**基本威胁防护 → 文件威胁防护**。
2. 在**安全级别**区域中，单击**设置**按钮。
3. 在打开的**文件威胁防护**窗口中，在**常规**选项卡，清空**所有网络驱动器**复选框。

在常规设置部分配置策略

对于该区域设置的完整描述，请参考 Kaspersky Endpoint Security 文档。

描述了附加配置操作，我们建议您在 Kaspersky Endpoint Security 的策略属性窗口中执行，在“**常规设置**”区域。

“常规设置”区域，“报告和存储”子区域

在“**到管理服务器的数据传输**”区域中，请注意“**关于已启动的应用程序**”复选框。当选中该复选框时：如果选中此复选框，管理服务器数据库保存网络设备上所有软件模块的所有版本信息。该信息可能需要 Kaspersky Security Center 数据库上的大量磁盘空间(几十 G)。因此，如果**关于已启动的应用程序**复选框依然在顶级策略中被选中，它必须被清空。

“常规设置”区域，“界面”子区域

如果组织网络中的威胁防护必须通过管理控制台集中管理，则必须禁用在工作站上显示 Kaspersky Endpoint Security 用户界面（通过清除“**与用户交互**”区域中的“**显示应用程序界面**”复选框），并启用密码保护（通过选中“**密码保护**”区域中的“密码保护”复选框）。

在事件配置区域配置策略

在**事件配置**区域，您应该禁用保存任何事件到管理服务器，除了以下事件：

- 在**严重**选项卡上：
  - *应用程序自动运行已禁用*
  - *访问被拒绝*
  - *已禁止应用程序启动*
  - *无法清除*
  - *违反了最终用户授权许可协议*
  - *无法加载加密模块*
  - *不能同时启动两项任务*
  - *检测到活动威胁。应该启动高级清除*
  - *检测到网络攻击*
  - *未更新所有组件*
  - *激活错误*
  - *启用便携模式时出错*
  - *与 Kaspersky Security Center 交互时出错*
  - *禁用便携模式时出错*
  - *更改应用程序组件时出错*
  - *应用文件加密/解密规则时出错*
  - *无法应用策略*
  - *进程已终止*
  - *网络活动已阻止*
- 在**功能失败**选项卡上：*任务设置无效，未应用设置*

- 在**警告**选项卡上：
  - *自我保护被禁用*
  - *备用密钥不正确*
  - *用户选择了退出加密策略*
- 在“**信息**”选项卡上：*禁止应用程序在测试模式下启动*

Kaspersky Endpoint Security 更新组任务的手动设置

如果管理服务器作为更新源，Kaspersky Endpoint Security 的最优和建议计划选项是“**当新更新下载至存储库时**”，其中“**使用任务启动自动随机延迟**”复选框被选中。

如果从 Kaspersky 服务器下载更新到存储库的本地任务已在每个分发点上创建，时段性计划将是最优的并被推荐给 Kaspersky Endpoint Security 组更新任务。此种情况下，随机时段值应该被设置为 1 小时。

Kaspersky Endpoint Security 设备扫描组任务的手动设置

快速启动向导创建扫描设备的组任务。默认情况下，为任务分配“**在星期五下午 7:00 运行**”计划，并且取消选中“**运行错过的任务**”复选框。

这意味着如果组织中的设备在星期五关闭，例如在下午 6:30 关闭，设备扫描任务将永远不会运行。您必须基于组织的工作规则为该任务设置最方便的计划。

计划“查找漏洞和所需更新”任务

快速启动向导为网络代理创建*查找漏洞和所需更新*任务。默认情况下，为任务分配**在星期二下午 7:00 运行**计划，并且取消选中**运行错过的任务**复选框。

如果组织的工作规则要在此时关闭所有设备，*查找漏洞和所需更新*任务将在设备再次开启时运行，也就是，在星期三早晨。此活动可能不是必须的，因为漏洞扫描可能增加 CPU 和磁盘子系统负载。您必须基于组织的工作规则为该任务设置最方便的计划。

更新安装和漏洞修复组任务的手动设置

该快速启动向导为网络代理创建更新安装和漏洞修复组任务。默认情况下，任务设置为在每天 01:00 AM 自动随机运行，并且未启用“**运行错过的任务**”选项。

如果组织工作规则整夜关闭所有设备，则更新安装将永远不会运行。您必须基于组织的工作规则为漏洞扫描任务设置最方便的计划。值得注意的是，更新的安装可能需要重启设备。

建立管理组结构和分配分发点

Kaspersky Security Center 中的管理组结构运行以下功能：

- 设置策略范围。

  将相关设置应用到设备还有一种方式：使用策略配置文件。此种情况下，策略范围用（例如）标签、设备在 Active Directory 组织单元中的位置、Active Directory 安全组中的成员关系等设置。

- 设置组任务范围。

  还有一个不基于管理组层级定义组任务范围的方法：使用设备分类的任务和特定设备的任务。

- 设置设备、虚拟管理服务器和从属管理服务器的访问权限。

- 分配分发点。

当建立管理组结构时，您必须考虑到组织网络的拓扑以便最优分配分发点。分发点的最优分发允许您在企业网络中保存流量。

根据组织图表和 MSP 客户端采用的网络拓扑，以下标准配置可以被应用到管理组结构：

- 单一办公室
- 多个独立的小型办公室

标准 MSP 客户端配置：单一办公室

在标准“单一办公室”配置中，所有设备都在组织网络中，因此它们能看见彼此。组织网络可能包含几部分(网络或网段)，由窄通道连接。

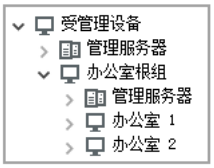
有以下构建管理组结构的方法：

- 构建管理组结构涉及到网络拓扑。管理组结构可能不精确反映网络拓扑。网络各部分之间以及特定管理组相互匹配。您可以使用分发点自动分配或手动分配它们。
- 不考虑网络拓扑而构建管理组结构。此种情况下，您必须禁用分发点自动分配，然后为网络中每个部分的根管理组分配一个或几个设备作为分发点，例如为**受管理设备**组。所有分发点将处于相同级别，并将掌控组织网络中所有设备的相同范围。此种情况下，每个网络代理都将连接到具有最短路由的分发点。分发点的路由可以使用 tracert 使用工具跟踪。

标准 MSP 客户端配置：多个小远程办公室

该标准配置用于一定数量的小远程办公室，它们可能通过互联网与总部联络。每个远程办公室都位于 NAT 之外，就是说，从一个远程办公室到另一个远程办公室的连接是不可能的，因为办公室是彼此隔离的。

配置必须在管理组中体现：必须为每个远程办公室创建各自的管理组（下图中的组**办公室 1**和**办公室 2**）。



远程办公室包含在管理组结构

必须指定一个或多个分发点给每个办公室的对应管理组。分发点必须是远程办公室中具有足够剩余磁盘空间的设备。部署在**办公室 1**组的设备，例如，将访问分配到**办公室 1**管理组的分发点。

如果一些用户在办公室之间移动他们的便携电脑，您必须在远程办公室选择两个或更多设备(除了现有的分发点)并分配它们作为等级管理组的分发点(上图中**办公室根组**)。

例如：便携式电脑部署在**办公室 1**管理组，然后被移动到对应于**办公室 2** 管理组的办公室。在移动便携式电脑后，网络代理试图访问分配到**办公室 1**组的分发点，但是那些分发点不可用。然后，网络代理开始尝试访问分配到**办公室根组**的分发点。因为远程办公室是彼此隔离的，尝试访问分配到**办公室根组**管理组的分发点仅在网络代理尝试访问**办公室 2** 组中的分发点时才会成功。就是说，便携式电脑将保持在原始办公室对应的管理组，但是将使用它当时所在办公室的分发点。

策略层级，使用策略配置文件

本部分提供有关如何应用策略到管理组设备的信息。本部分还提供有关策略配置文件的信息。

策略层级

在 Kaspersky Security Center，您使用策略来定义一个单一设置集到多个设备。例如，应用程序 P 的策略范围，为管理组 G 定义，包含安装了应用程序 P 的部署在组 G 和其子组的受管理设备， 除了在属性中清空了**从父组继承**复选框的子组。

策略通过设置旁边的锁图标（🔒）不同于本地设置。如果一个设置（或设置组）在策略属性中被锁定，您必须首先在创建有效设置时使用该设置（或设置组），其次，必须将设置或设置组写入 downstream 策略。

在设备上创建有效设置可以如此描述：所有未锁定的设置值必须来自策略，然后被本地设置覆盖，然后结果集被来自策略的锁定设置的值覆盖。

相同应用程序的策略通过管理组层级互相影响：来自 upstream 策略的锁定设置覆盖来自 downstream 策略的相同设置。

漫游用户有特殊策略。该策略在设备切换到漫游模式时在设备上生效。漫游策略不通过管理组层级影响其他策略。

策略配置文件

仅通过管理组层级应用策略到设备可能在许多环境下不方便。有必要创建单一策略的几个实例，这些实例对于不同的管理组在一两个设置上有所不同，可以在将来同步这些策略的内容。

为帮助您避免此类问题，Kaspersky Security Center 支持*策略配置文件*。策略配置文件是策略设置的命名子集。该子集随带策略在大设备上分发，在特别条件*配置文件激活条件*下将其补充。配置文件仅包含与"基本"策略不同的设置，并在客户端设备（计算机或移动设备）上活动。激活配置文件会修改配置文件激活之前已在计算机上活动的策略设置。这些设置将使用已在配置文件中指定的值。

以下限制被施加在策略配置文件：

- 策略可以包含最多 100 个配置文件。
- 策略配置文件不能包含其他配置文件。
- 策略配置文件不能包含通知设置。

配置文件内容

策略配置文件包含以下组成部分：

- Name。带有相同名称的配置文件通过管理组层级互相影响。
- 策略设置子集。不同于包含所有设置的策略，配置文件仅包含实际所需的设置(锁定设置)。
- 激活条件是设备属性的逻辑表达。配置文件仅在配置文件激活条件为真是活动(补充策略)。在其他所有情况，配置文件是非激活和忽略的。以下设备属性可以被包含在逻辑表达：
  - 漫游模式状态。
  - 网络环境属性 — 网络代理连接的活动规则的名称。
  - 设备上指定标签的出现和消失。
  - 设备在活动目录组织单元（OU）上的分配：明确(设备在指定 OU 中)，或不明确(设备是 OU，以嵌套级别包含在指定 OU)。
  - 设备在活动目录安全组中的成员关系（明确或不明确）。
  - 活动目录安全组中设备所有者的成员关系（明确或不明确）。
- 配置文件禁用复选框。被禁用的配置文件总是被忽略，并且它们的激活条件不被验证。
- 配置文件优先级。不同配置文件的激活条件是独立的，因此几个配置文件可以一起激活。如果活动配置文件包含设置的非重叠集合，将不会发生问题。然而，如果两个活动配置文件包含不同的相同设置的值，将发生歧义。该歧义可以通过策略优先级避免：歧义变量的值将来自高优先级的配置文件(在配置文件列表中评级较高)。

策略通过层级互相影响时的配置文件行为

带有相同名称的配置文件根据策略合并规则合并到一起。upstream 策略的配置文件比 downstream 策略的配置文件拥有更高优先级。如果编辑设置在 upstream 策略中被禁止(锁定)，downstream 策略使用 upstream 策略的配置文件激活条件。如果编辑设置在 upstream 策略中被允许，downstream 策略的配置文件激活条件被使用。

既然策略配置文件可能在激活条件中包含"**设备已离线**"属性，配置文件完全替换漫游用户策略功能，后者将不被支持。

漫游用户的策略可能包含配置文件，但是它们配置文件仅可以在设备切换到漫游模式后激活。

任务

Kaspersky Security Center 通过创建和运行*任务*来管理设备上安装的 Kaspersky 应用程序。安装、启用和停用程序、扫描文件、更新数据库和软件模块以及程序的其他操作均需要任务。

特定应用程序的任务仅在安装了该应用程序的管理插件时可以被创建。

任务可以在管理服务器和设备上执行。

以下任务在管理服务器上执行：

- 自动分发报告
- 将更新下载至管理服务器存储库
- 备份管理服务器数据
- 数据库维护
- Windows Update 同步
- 基于参考设备的操作系统镜像创建安装包

以下类型的任务在设备上执行：

- *本地任务* — 在特定设备上执行的任务。

  本地任务可以被管理员通过管理控制台工具修改，或者被远程设备用户修改（例如，通过安全应用程序界面）。如果本地任务同时被管理员和受管理设备用户修改，管理员的修改将生效，因为其具有更高优先级。

- *组任务* — 在特定组的所有设备上执行的任务。

  除非在任务属性中指定了其他项，组任务也影响所选组的所有子组。组任务还影响（可选）已连接到部署在该组或其任意子组中的从属和虚拟管理服务器的设备。

- *全局任务* — 在一组设备上执行的任务，与设备是否包含在某个组中无关。

您可以为每个应用程序创建不管多少个组任务、全局任务或本地任务。

您可以更改任务设置、查看任务进度、复制、导出、导入和删除任务。

仅当为其创建任务的应用程序在运行时，才能在设备上启动任务。

任务结果保存在 Microsoft Windows 事件日志和 Kaspersky Security Center 的事件日志中，既集中在管理服务器上，又位于每个设备上。

不在任务设置中包括私人数据。例如，避免指定域管理员密码。

设备移动规则

我们建议您自动分配设备到虚拟服务器上的对应于 MSP 客户端的管理组，使用*设备移动规则*。设备移动规则由三个主要部分组成：名称、执行条件(设备属性逻辑表达)和目标管理组。如果设备属性满足规则执行条件，则规则移动设备到目标管理组。

所有设备移动规则都有优先级。管理服务器检查设备属性以查看它们是否满足每条规则的执行条件（升序优先级）。如果设备属性满足某条规则的执行条件，设备被移动到目标组，至此规则处理在该设备上完成。如果设备属性满足多个规则的条件，设备被移动到具有高优先级的规则的目标组。

设备移动规则可以被间接创建。例如，在安装包或远程安装任务的属性中，您可以指定安装网络代理后设备必须被移动到的管理组。而且，设备移动规则可以被 Kaspersky Security Center 管理员明确创建，在移动规则列表。列表位于管理控制台，在**未分配设备**组属性中。

默认下，设备移动规则用于设备到管理组的一次性初始分配。规则仅移动**未分配的设备**组的设备一次。一旦设备被该规则移动，该规则不会再次移动该设备，即便您把设备手动放回**未分配设备**组。这是应用移动规则的推荐方法。

您可以移动已经被分配的设备到一些管理组。为此，在规则的属性中，清空**仅移动不属于任何管理组的设备**复选框。

应用移动规则到已经分配到一些管理组中的设备会显著增加管理服务器负载。

您可以创建重复影响单一设备的移动规则。

我们强烈建议您避免从一个组重复移动单一设备到另一个组（例如，为了应用特别策略到该设备，运行特别组任务，或者通过特别分发点更新设备）。

此类方案不被支持，因为它们显著增加了管理服务器负载和网络流量。这些方案也与 Kaspersky Security Center 的操作原则冲突(尤其在访问权限、事件和报告方面)。必须找到其他解决方案，例如，通过使用策略配置文件、设备分类的任务、根据标准方案分配网络代理，等等。

软件分类

监控应用程序运行的主要工具是 *Kaspersky 类别*(也叫 *KL 类别*)。KL 类别帮助 Kaspersky Security Center 管理员简化软件分类和减少到受管理设备的流量。

用户类别必须仅对无法被分类成现有 KL 类别的应用程序创建(例如，对于自定义软件)。基于应用程序安装包(MSI)或带有安装包的文件夹创建的用户类别。

如果有未通过 KL 类别分类的大软件集可用，最好创建一个自动更新的类别。每次对包含分发包的文件夹进行修改时，可执行文件的校验和将被自动添加到该类别。

不要为文件夹“我的文档”、%windir%、%ProgramFiles% 和 %ProgramFiles(x86)% 创建自动更新类别的软件。在这些文件夹的文件轮询受频繁更改的影响，这将导致增加管理服务器负载和网络流量。您必须为软件集创建专用文件夹并定期添加新条目。

关于多租户应用程序

Kaspersky Security Center 启用服务提供商管理员和租户管理员来使用支持多租户的 Kaspersky 应用程序。在多租户 Kaspersky 应用程序被安装到服务提供商基础架构后，租户可以开始使用应用程序。

要区分不同租户相关的任务和策略，您必须在 Kaspersky Security Center 中为每个租户创建专用的虚拟管理服务器。所有为一个租户运行的多租户应用程序的任务和策略必须为对应于该租户的虚拟管理服务器的受管理设备管理组而创建。为与主管理服务器相关的管理组创建的任务不影响租户设备。

和服务提供商管理员不同，租户管理员仅可以为租户对应的设备创建和查看任务和应用程序策略。服务提供商管理员和租户管理员可以使用的任务和策略设置集是不同的。一些任务和策略设置对租户管理员不可用。

在租户的分级结构中，为多租户应用程序创建的策略被继承到低级别管理组以及高级别管理组：策略被传播到属于该租户的所有客户端设备。

管理服务器设置的备份和恢复

管理服务器设置和其数据库的备份通过备份任务和 klbackup 实用工具执行。备份副本包括与管理服务器有关的所有主要设置和对象，例如证书、受管理设备上驱动器加密的主密钥、各种授权许可的密钥、管理组的结构及其所有内容、任务、策略等。使用备份副本，您可以尽快恢复管理服务器的操作，为此花费十几分钟到几个小时。

如果没有备份副本可用，失败可能导致证书和管理服务器设置的不可挽回的损失。这将导致要重新开始配置 Kaspersky Security Center，并在组织网络上重新执行网络代理初始化部署。所有受管理设备驱动器加密主密钥也将丢失，导致 Kaspersky Endpoint Security 设备上不可挽回的加密数据丢失。因此，不要忽略使用标准备份任务对管理服务器进行定期备份。

快速启动向导为管理服务器设置创建备份任务，并将其设置为每天凌晨 4:00 运行。备份副本默认保存在文件夹 %ALLUSERSPROFILE%\Application Data\KasperskySC 中。

如果安装在其他设备上的 Microsoft SQL Server 实例被用作 DBMS，您必须通过指定 UNC 路径修改备份任务，这可以通过管理服务器服务和 SQL Server 服务写入，作为存储备份副本的文件夹。这个来自 Microsoft SQL Server DBMS 备份的特殊功能。

如果使用本地 Microsoft SQL Server 实例作为 DBMS，我们还建议将备份副本与管理服务器一起保存到专用介质，以防止它们损坏。

因为备份副本包含重要数据，备份任务和 klbackup 实用工具用于备份副本密码保护。默认下，备份任务使用空密码创建。您必须在备份任务属性中设置密码。忽略该需求将导致管理服务器证书所有密钥、授权许可密钥和受管理设备驱动器加密主密钥保持未加密。

除了常规备份，您必须在每个显著更改之前创建备份副本，包括管理服务器升级和补丁的安装。

如果您使用 Microsoft SQL Server 作为 DBMS，您可以最小化备份副本的大小。为此，请启用 SQL Server 设置中的**压缩备份**复选框。

从备份副本的恢复使用管理服务器实例上刚刚安装的与备份副本具有相同或更新版本的实用工具 klbackup 来执行。

对于要执行还原的管理服务器的实例，必须使用相同类型（例如相同的 SQL Server 或 MariaDB）和相同版本或更新版本的 DBMS。管理服务器版本可以相同（带有相同或更新补丁）或更新。

这部分描述了恢复管理服务器设置和对象的标准方案。

管理服务器设备不可操作

如果管理服务器设备由于失败而不可操作，建议您执行以下操作：

- 新管理服务器必须分配相同的地址：NetBIOS 名称、FQDN 或静态 IP(取决于部署网络代理时的设置)。
- 安装管理服务器，使用相同类型、相同版本（或更新）的 DBMS。您可以安装带有相同（或更新）补丁的相同（或更新）版本的服务器。安装后，不要通过向导执行初始化安装。
- 在**开始**菜单中，运行 klbackup 实用程序并执行还原。

管理服务器设置或数据库被损坏

如果管理服务器由于设置或数据库损坏（例如断电）而不可操作，建议您使用以下恢复方案：

1. 扫描被损坏设备上的文件系统。
2. 卸载管理服务器的不可操作版本。
3. 重新安装管理服务器，使用相同类型、相同版本（或更新）的 DBMS。您可以安装带有相同（或更新）补丁的相同（或更新）版本的服务器。安装后，不要通过向导执行初始化安装。
4. 在**开始**菜单，运行 klbackup 实用工具并执行恢复。

禁止用除了通过 klbackup 实用工具的其他方法恢复管理服务器。

任何试图通过第三方软件恢复管理服务器的操作都将不可避免地导致 Kaspersky Security Center 分发节点上的数据的不一致和应用程序操作不正常。

部署网络代理和安全应用程序

要管理组织设备，您必须在其上安装网络代理。部署分发的 Kaspersky Security Center 到组织设备通常开始于在其上安装网络代理。

在 Microsoft Windows XP 中，网络代理可能错误执行以下操作：直接从卡巴斯基服务器（作为分发点）下载更新；作为 KSN 代理服务器（作为分发点）；检测第三方漏洞（如果漏洞和补丁管理被使用）。

初始化部署

如果已经有网络代理安装在设备，在该设备上远程安装应用程序通过该网络代理运行。要安装的应用程序分发包通过网络代理和管理服务器之间的通信渠道，与管理员定义的安装设置一并传输。为了传递分发包，您可以使用中继分发节点，即分发点、组播传递等。有关如何在已安装网络代理的受管理设备上安装应用程序的更多详细信息，请参阅本节下文。

您可以在运行 Windows 的设备上执行网络代理初始化安装，使用以下方法之一：

- 使用应用程序远程安装的第三方工具。
- 使用 Windows 组策略：使用标准 Windows 组策略管理工具。
- 在强制模式，使用 Kaspersky Security Center 远程安装任务的特殊选项。
- 通过发送设备用户链接到 Kaspersky Security Center 生成的独立包。独立包是包含所选应用程序分发包的定义了设置的可执行模块集合。
- 在设备上手动运行应用程序安装程序。

在非 Microsoft Windows 平台上，您必须在受管理设备上执行网络代理初始化安装，通过现有第三方工具，或者手动发送给用户带有预先配置的分发包的存档。您可以升级网络代理到新版本或安装其他 Kaspersky 应用程序到非 Windows 平台，使用网络代理(已经安装在设备)执行远程安装任务。此种情况下，安装和在 Windows 设备上的安装相同。

当选择部署应用程序到受管理网络的方法和策略时，您必须考虑很多因素（部分列表）：

- 企业网络配置
- 设备总数
- 受管理网络的 Windows 域，可以在这些域修改活动目录组策略
- 对计划了 Kaspersky 应用程序的初始化部署的设备具有本地管理员权限的用户账户(例如，带有本地管理员权限的域用户账户，带有这些设备的管理员权限的统一本地用户账户)
- 管理服务器和 MSP 客户端网络之间网络通道的连接类型和带宽，以及这些网络内部通道的带宽
- 部署之初应用在远程设备上的安全设置(例如 UAC 和简单文件共享模式的使用)

配置安装程序

在开始部署 Kaspersky 应用程序到网络之前，您必须指定安装设置，就是在应用程序安装过程中定义的设置。当安装网络代理时，您应该指定最小值、连接管理服务器和代理设置的地址，也可能需要一些高级设置。取决于您选择的安装方法，您可以用不同方法定义设置。在最简单的情况(在所选设备上的手动交互安装)，所有相关设置都可以通过安装程序用户界面来定义，因为，在一些情况下，初始化部署甚至可以通过发送给用户网络代理分发包链接以及用户必须在安装程序界面输入的设置(管理服务器地址等等)来执行。

该方法不推荐使用，因为它对用户来说不方便，在手动定义设置的时候容易引发风险；它也在设备组上静默安装应用程序时不可用。通常情况下，管理员必须集中指定设置值；这些值可以用于创建独立包。独立包是包含带有由管理员定义的设置的分发包的自解压存档。独立包可以位于允许用户下载的资源(例如，在 Kaspersky Security Center Web Server)，以及允许在所选网络设备上的静默安装。

安装包

定义应用程序安装设置的第一个和主要的方法是通用的，因此适用于所有安装方法，用 Kaspersky Security Center 工具和多数第三方工具。该方法包括在 Kaspersky Security Center 中创建应用程序安装包。

安装包使用以下方法生成：

- 基于包含的*描述符*(带有 .kud 扩展名的包含了安装和结果分析规则以及其他信息的文件)从指定的分发包自动生成
- 从安装程序可执行文件或 Microsoft Windows Installer (MSI) 格式的可执行文件生成标准或所支持应用程序安装包

生成的安装包以包含子文件夹和文件的文件夹形式分层级组织。除了原始分发包，安装包包含可编辑设置(包含安装程序设置和是否在安装结束时重启操作系统等处理规则)以及小的辅助模块。

当创建安装包时，所选应用程序的安装设置值可以被指定在管理控制台用户界面(更多设置可以在所创建的安装包属性中找到)。当通过 Kaspersky Security Center 工具执行远程应用程序安装时，安装包被传送到目标设备，因此运行应用程序安装程序使得所有管理员定义的设置对其可用。当使用第三方工具安装 Kaspersky 应用程序时，您仅需要确保目标设备上整个安装包的可用性，即是分发包和其设置的可用性。安装包被 Kaspersky Security Center 创建并存储在共享文件夹下的专用子文件夹。

不在安装包参数中显示授权账户的任何细节。

有关在通过第三方工具部署之前对卡巴斯基应用程序使用该配置方法的说明，请参阅“使用 Microsoft Windows 组策略部署”部分。

在 Kaspersky Security Center 安装之后，一些安装包被自动生成；它们可用于安装并包含网络代理和 Microsoft Windows 安全应用程序包。

在一些情况下，使用安装包部署应用程序到 MSP 客户端网络需要在对应于 MSP 客户端的虚拟服务器上创建安装包。在虚拟服务器上创建安装包允许您对不同的 MSP 客户端使用不同的安装设置。在第一个实例中，这在处理网络代理安装包时是有用的，因为部署在不同 MSP 客户端网络的网络代理使用不同的地址连接到管理服务器。实际上，连接地址决定了网络代理要连接的服务器。

除了在虚拟管理服务器上立即创建新安装包的可能，虚拟管理服务器上安装包的主要操作模式是从主管理服务器“分发”安装包到虚拟管理服务器。你可以分发所选(或所有)安装包到所选的虚拟管理服务器(包含所有所选管理组的服务器)，使用对应的管理服务器任务。您也可以在创建新虚拟管理服务器时选择主管理服务器的安装包列表。您所选择的安装包将被立即分发到新创建的虚拟管理服务器。

当分发安装包时，它的内容不被整个复制。虚拟管理服务器上的文件存储库，对应于正在被分发的安装包，仅存储该虚拟服务器的设置文件。安装包的主要部分(包括正在安装的应用程序分发包)保持未更改；它仅存储在主管理服务器存储库。这允许您显著提高系统性能并减少所需磁盘卷。当处理分发到虚拟管理服务器的安装包时(例如，当运行远程安装或创建独立安装包时)，主管理服务器原始安装包的数据被使用对应于虚拟管理服务器上的分发包的设置文件“合并”。

尽管应用程序授权许可密钥可以在安装包属性中设置，还是建议避免使用该授权许可分发方法，因为可以轻易获取对文件夹文件的读访问权限。您应该使用自动分发的授权许可密钥，或使用授权许可密钥安装任务。

MSI 属性和转换文件

另一个在 Windows 平台上配置安装的方法是定义 MSI 属性和转换文件。该方法可以用在通过为Microsoft Installer格式的安装设计的第三方工具执行安装的时候，以及通过 Windows 组策略使用标准 Microsoft 工具或用于处理 Windows 组策略的其他第三方工具执行安装的时候。

使用应用程序远程安装的第三方工具部署

当任何应用程序远程安装工具(例如 Microsoft System Center) 都在组织中可用时，可以使用这些工具进行初始化部署。

必须执行以下操作：

- 选择能最好配合部署工具的配置应用程序的方法。
- 定义用于同步安装包设置修改(通过管理控制台界面)和所选的用于从安装包数据部署应用程序的第三方工具的操作的装置。

Kaspersky Security Center 中远程安装任务的常规信息

Kaspersky Security Center 提供远程安装应用程序的众多方法，都实现在远程安装任务中。您可以为指定管理组和特定设备或设备分类创建远程安装任务（此类任务显示在管理控制台，在**任务**文件夹）。当创建任务时，您可以选择安装包(网络代理和/或其他应用程序的安装包)以用此任务安装，并指定定义远程安装方法的设置。

管理组的任务影响指定组的设备和所有管理组子组的设备。如果任务中启用了相应设置，任务将覆盖组及其任何子组中包括的从属管理服务器的设备。

特定设备的任务在每一次运行时根据分类内容刷新客户端设备列表。如果分类包含连接到从属管理服务器的设备，任务也将在那些设备上运行。

要确保远程安装任务在连接到从属管理服务器的设备上成功操作，您必须使用分发任务提前分发您任务使用的安装包到对应的从属管理服务器。

使用 Microsoft Windows 组策略部署

建议您通过 Microsoft Windows 组策略执行网络代理初始化部署，如果满足以下条件：

- 该设备是活动目录域中的成员。
- 到域控制器的访问被授予管理员权限，这允许您创建和修改活动目录组策略。
- 配置的安装包可以被移动到目标受管理设备的网络(到可以被所有目标设备读取的共享文件夹)。
- 部署方案允许您在开始部署网络代理到设备之前，等待下一次目标设备例行重启(或者您可以强制 Windows 组策略应用到这些设备)。

该部署方案包含以下：

- Microsoft Installer 格式的应用程序分发包(MSI 包)位于共享文件夹(目标设备的 LocalSystem 账户对该文件夹具有读权限)。
- 在活动目录组策略中，安装对象被创建用于分发包。
- 安装范围通过指定组织单元(OU)和 / 或安全组设置，包含目标设备。
- 目标设备下一次登录到域中时(设备用户登录到系统之前)，所有已安装的应用程序被检查。如果未找到应用程序，分发包从指定在策略中的资源中下载，然后被安装。

该部署方案的一个好处就是被分配的应用程序在目标设备的操作系统正在加载时被安装，甚至在用户登录到系统之前。即便有带有足够权限的用户卸载了该应用程序，它也将在操作系统下一次重启时被重新安装。该部署方案的劣势是管理员对组策略所做的更改在设备重启之前将不会生效(如果不涉及附加工具)。

您可以使用组策略安装网络代理和其他应用程序，如果它们的安装程序是 Windows Installer 格式。

仅可在静默模式下从 MSI 包安装网络代理，不支持从 MSI 包进行交互式安装。

而且，当选择该部署方案后，您必须评估在应用 Windows 组策略后，从中复制文件到目标设备的文件资源负载。您还必须选择传送所配置的安装包到该资源的方法，以及同步其设置中的相关更改的方法。

通过 Kaspersky Security Center 远程安装任务处理 Microsoft Windows 策略

该部署方法仅在从管理服务器设备可以访问包含目标设备的域控制器时可用，同时管理服务器的共享文件夹(存储安装包)可以从目标设备读取。基于上述原因，该部署方法不被视为对 MSP 可应用。

通过 Microsoft Windows 策略独立安装应用程序

管理员可以用自己名义在 Windows 组策略中创建安装所需的对象。此种情况下，您必须上传数据包到独立文件服务器并提供其链接。

可能有以下安装方案：

- 管理员创建安装包并在管理控制台设置其属性。然后管理员复制 Kaspersky Security Center 共享文件夹中整个 EXEC 子文件夹到组织专用文件资源的文件夹。组策略对象提供组织专用文件资源子文件夹中的包的 MSI 文件的链接。
- 管理员从互联网下载应用程序分发包(包括网络代理包)并将其上传到组织专用文件资源。组策略对象提供组织专用文件资源子文件夹中的包的 MSI 文件的链接。安装设置通过配置 MSI 属性或通过配置 MST 转换文件来定义。

通过 Kaspersky Security Center 远程安装任务的强制部署

要执行网络代理或其他应用程序的初始部署，您可以使用 Kaspersky Security Center 的远程安装任务强制安装选定的安装包，前提是每台设备都有具有本地管理员权限的用户账户。

强制安装也可以在设备无法被管理服务器直接访问时应用：例如，设备在隔离网络中，或者设备在本地网络但管理服务器在 DMZ。

初始部署时，不会安装网络代理。因此，在远程安装任务的设置中，无法选择使用网络代理安装应用程序所需的文件分发。您只能选择通过管理服务器或分发点使用操作系统资源来分发文件。

管理服务器服务必须使用在目标设备上具有管理权限的账户运行。或者，您可以在远程安装任务的设置中指定有权访问 admin$ share 的账户。

默认情况下，远程安装任务使用管理服务器运行所用账户（例如，用于访问 admin$ share 的账户）的凭据连接到设备。仅当目标设备上未安装网络代理时，您才必须在远程安装程序任务设置中指定此帐户。
创建要在基于 Linux 的设备上运行的远程安装程序任务时，必须始终指定一个用于创建 SSH 连接的帐户。

您可以明确指定目标设备(使用列表)、通过选择它们所属的 Kaspersky Security Center 管理组或通过基于指定标准创建设备分类。安装开始时间定义在任务计划中。如果任务属性中启用了**运行错过的任务**设置，任务可以在设备开启时立即运行，或设备被移动到目标管理组时立即运行。

强制安装包括传送安装包到目标设备、随后复制文件到每个目标设备的 admin$ 资源，和在这些设备上远程注册支持服务。传送安装包到目标设备通过 Kaspersky Security Center 的网络交互功能运行。以下条件必须在此种情况下被满足：

- 目标设备可以从管理服务器端或分发点端访问。
- 目标设备的名称解析在网络中运行正常。
- 设备上的管理共享(admin$)保持启用。
- 以下系统服务正在目标设备上运行：
  - 服务器（LanmanServer）
    默认情况下，该服务正在运行。
  - DCOM 服务器进程启动器 (DcomLaunch)
  - RPC 端点映射器 (RpcEptMapper)
  - 远程过程调用 (RpcSs)
- TCP 445 端口在目标设备上打开，以便通过 Windows 工具实现远程访问。

  TCP 139、UDP 137 和 UDP 138 由较旧的协议使用，对于当前应用程序来说不再是必需的。

  防火墙必须允许动态出站访问端口，以便从管理服务器和分发点连接到目标设备。
- 在网络代理部署期间，允许 Active Directory 域策略安全设置提供 NTLM 协议的操作。
- 在运行 Microsoft Windows XP 的目标设备上，简单文件共享模式被禁用。

- 在目标设备上，访问共享和安全模型被设置为*经典 - 本地用户以自身进行身份验证*。它绝不可以是*仅限访客 – 本地用户需要以访客身份进行身份验证*。

- 目标设备是域成员，或带有管理员权限的统一账户提前在目标设备上被创建。

要成功部署网络代理或其他应用程序到未加入 Windows Server 2003 或更高版本的 Active Directory 域的设备，您必须在该设备上禁用远程 UAC。远程 UAC 是阻止本地管理账户访问 admin$ 的原因之一，这对于强制部署网络代理或其他应用程序必不可少。禁用远程 UAC 不会影响本地 UAC。

在未分配到任何 Kaspersky Security Center 管理组的新设备上进行安装时，您可以打开远程安装任务属性并指定网络代理安装后设备要移动到的管理组。

当创建组任务时，记住每个组任务都影响所选组的潜逃组中的所有设备。因此，您必须避免在子组中的重复安装任务。

创建强制安装应用程序的任务的一个简化方法是自动安装。为此，您必须打开管理组属性，打开安装包列表，然后选择必须在该组中设备上安装的包。结果，所选安装包将被自动安装在该组和其所有子组中的所有设备上。包被安装的时间间隔取决于网络吞吐量和网络设备总数。

为了减轻管理服务器在向目标设备传送安装包时的负载，您可以在安装任务中选择通过分发点进行安装。注意，该安装方法给作为分发点的设备增加了大量负载。因此，建议您选择符合分布点要求的设备。如果您使用分发点，您必须确保它们存在于托管目标设备的每个隔离子网中。

使用分发点作为本地安装中心也可以用在与管理服务器具有窄通道通信的子网设备上的安装，此时子网中的通道带宽很高。

文件夹 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 所在分区的磁盘剩余空间必须超过所安装应用程序的分发包的总大小的好几倍。

运行 Kaspersky Security Center 创建的独立包

以上描述的网络代理和其他应用程序的初始化部署方法无法总被实现，因为不可能满足所有可应用条件。此种情况下，您可以通过 Kaspersky Security Center 创建通用可执行文件，叫做*独立安装包*，使用管理员准备的带有相关安装设置的安装包。独立安装包可以被发布在内部 Web 服务器(包含在 Kaspersky Security Center)，如果这是合理的(到该 Web 服务器的外部访问已为目标设备用户配置)，或发布在包含在 Kaspersky Security Center Web Console 中的单独部署的 Web 服务器。您也可以复制独立包到其他 Web 服务器。

您可以使用 Kaspersky Security Center 来给所选用户发送包含当前使用的 Web 服务器中该独立包文件链接的电子邮件，提示他们运行该文件(在交互模式或带有 "-s" 参数的静默模式)。您可以附加独立安装包到电子邮件，然后发送它到对 Web 服务器没有访问权限的设备用户。管理员也可以复制独立包到外部设备，将其传送到相关设备然后稍后运行。

您可以从网络代理包或其他应用程序包创建独立包(例如，安全应用程序)。如果独立包从网络代理和其他应用程序创建，安装和网络代理一起启动。

当创建带有网络代理的独立包时，您可以指定当网络代理安装完成时，新设备(未分配到任何管理组的设备)将被自动移动到的管理组。

独立包可以在交互模式下运行(默认)，显示应用程序安装结果，或者可以运行在静默模式(以参数 "-s" 运行)。静默模式可以用在从脚本安装，例如操作系统镜像部署后要运行的脚本。静默模式安装的结果决定与进程返回代码。

手动安装应用程序的选项

管理员或资深用户可以在交互模式下手动安装应用程序。他们可以使用原始分发包或从其他生成并存储在 Kaspersky Security Center 共享文件夹的安装包。默认下，安装程序在交互模式下运行并提示用户所需的设置值。然而，当使用参数 "-s" 从安装包根目录运行 setup.exe 进程时，安装程序将运行在静默模式，使用配置安装包时定义的设置。

当从安装包的根目录运行 setup.exe 时，包先被复制到临时文件夹，然后应用程序安装程序将从本地文件夹运行。

在安装有网络代理的设备上远程安装应用程序

如果连接到主管理服务器（或任何其从属管理服务器）的可操作网络代理被安装到设备，您可以升级该设备上的网络代理，以及通过网络代理安装、升级或卸载支持的应用程序。

您可以通过在远程安装任务的属性中选择**使用网络代理**复选框来启用该选项。

如果该复选框被选中，带有管理员定义的安装设置的安装包将被通过网络代理和管理服务器之间的通信渠道传输到目标设备。

要优化管理服务器负载和最小化管理服务器和设备之间的流量，最好为每个远程网络或每个多播域分配分发点（请参见“关于分发点”部分和“创建管理组结构和分配分发点”部分）。此种情况下，安装包和安装设置通过分发点从管理服务器分发到目标设备。

而且，您可以使用分发点来多播传送安装包，这将允许您在部署应用程序时显著降低网络流量。

当通过网络代理和管理服务器之间的通信渠道传输安装包到目标设备时，所有准备传输的安装包都将被缓存在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer 文件夹。当使用多个不同类型的大安装包并涉及大量分发点时，该文件夹的尺寸将显著增长。

文件不能从 FTServer 文件夹手动删除。当原始安装包被删除时，对应数据将被自动从 FTServer 文件夹删除。

分发点收到的所有数据被保存到 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp 文件夹。

文件不能从 $FTCITmp 文件夹手动删除。使用该文件夹数据的任务完成后，该文件夹的内容将被永久删除。

因为安装包从中转存储库以优化传输的格式通过管理服务器与网络代理之间的通信渠道进行分发，原始文件夹里的安装包不允许更改。这些更改将不会被管理服务器自动注册。如果您需要手动修改安装包的文件(尽管建议您避免此方案)，您必须在管理控制台编辑安装包的任何设置。在管理控制台编辑安装包的设置导致管理服务器在目标设备传输缓存中更新安装包镜像。

在远程安装任务中管理设备重启

设备经常需要在完成应用程序远程安装时重启(尤其在 Windows)。

如果您使用 Kaspersky Security Center 远程安装任务，在新任务向导或所创建任务的属性窗口（**操作系统重启**区域）中，您可以选择 Windows 设备要求重启时执行的操作：

- **不重启设备**。此种情况下，自动重启不会运行。要完成安装，您必须重启设备(例如，手动或通过设备管理任务)。所需重启的信息将被保存在任务结果和设备状态。该选项适用于在需要持续操作的服务器和其他设备上的安装任务。

- **重启设备**。此种情况下，如果完成安装需要重启，设备总是被自动重启。该选项适用于允许中断操作(关机或重启)的设备上的安装任务。

- **提示用户操作**。此种情况下，客户端设备上将显示重启提醒，提示用户手动重启设备。可以为该选项定义一些高级设置：用户消息文本、消息显示频率以及强制重启（不需要用户确认）的时间间隔。**提示用户操作**最适用于用户需要选择最合适重启时间的工作站。

反病毒应用程序安装包上的数据库更新

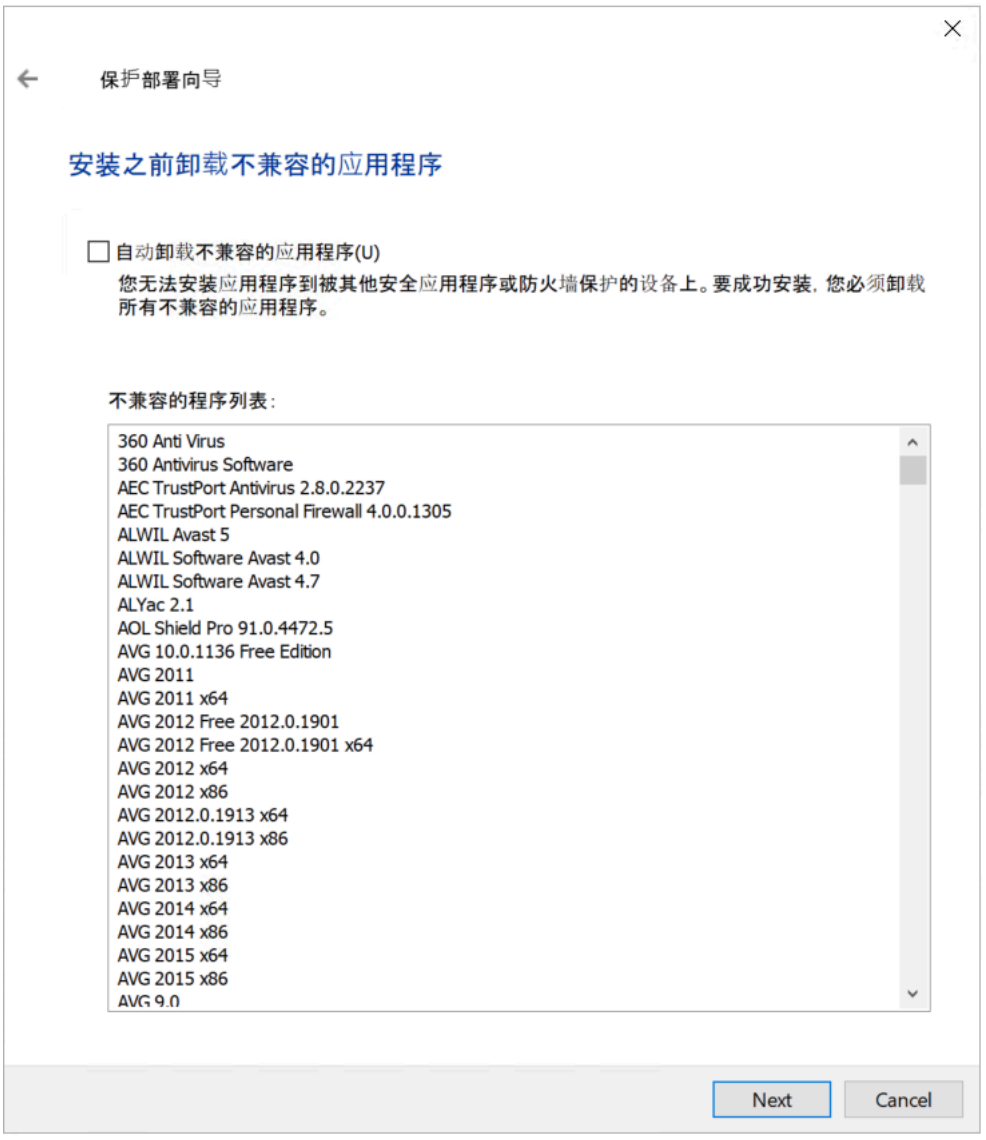
开始保护部署之前，您必须注意要随安全应用程序的分发包一起更新反病毒数据库(包块模块和自动补丁)。最好在开始部署之前更新应用程序安装包中的数据库(例如， 通过使用所选安装包上下文菜单中的相关命令)。这将减少目标设备在完成保护部署后所需的重启次数。如果您的远程安装涉及到从主管理服务器中继到虚拟服务器的安装包，您仅需要更新主服务器原始数据包中的数据库。此种情况下，您不必更新虚拟服务器上中继的数据包中的数据库。

删除不兼容的第三方安全应用程序

通过 Kaspersky Security Center 进行 Kaspersky 安全应用程序的安装可能需要卸载与正在安装的应用程序不兼容的第三方软件。有两种卸载第三方应用程序的方法。

使用安装程序自动卸载不兼容的应用程序

运行安装程序时，它会显示与卡巴斯基应用程序不兼容的应用程序列表：



远程安装向导中显示的不兼容应用程序列表

Kaspersky Security Center 检测到不兼容的软件。相应地，您可以选中“**自动卸载不兼容的应用程序**”复选框以继续安装。如果清除此复选框并且不卸载不兼容的软件，则会发生错误并且不会安装卡巴斯基应用程序。

各种类型的安装都支持自动删除不兼容的应用程序。

通过专用任务卸载不兼容的应用程序

要删除不兼容的应用程序，请使用“*远程卸载应用程序*”任务。该任务应该在安全应用程序安装任务运行之前运行在设备。例如，在安装任务中，可以选择“**在完成其他任务时**”作为计划类型，其中其他任务为“*远程卸载应用程序*”。

该卸载方法在安全应用程序无法正确卸载不兼容应用程序时是很有用的。

使用命令提示符删除受密码保护的网络代理

要远程卸载为其设置了卸载密码的网络代理，您可以使用命令提示符。

如果您丢失或忘记了安装在不再受 Kaspersky Security Center 管理的设备上受密码保护的网络代理的密码，则无法使用 klmover 实用程序、清理工具 (cleaner.exe) 或命令提示符删除网络代理。在这种情况下，您必须在安装了受密码保护的网络代理的设备上重新安装操作系统。

要通过命令提示符卸载网络代理：

1. 将您的卸载密码转换为十六进制代码。

   使用互联网资源、编程环境、文本编辑器或其他合适的工具将您的密码转换为十六进制代码。

   确保用于将生成的十六进制代码分隔成各部分的输出分隔符设置为`00`。例如，十六进制代码`51 77 65 72 74 79`不正确，而十六进制代码`5100770065007200740079 00`是正确的。

2. 在命令提示符中输入以下命令，然后按**ENTER**：

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   您可以在下表中查找您的网络代理的产品代码。

网络代理产品代码

本地化	产品代码
阿拉伯语	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
保加利亚语	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
捷克语	{478A6A0B-D177-4402-B703-808C05C56B13}
英语	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
法语	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
德语	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
匈牙利语	{8899A4D4-D678-49F8-AD96-0B784F58D355}
意大利语	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
日语	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
韩语	{70812A40-973B-4DA1-96B9-C2011280CD99}
波兰语	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
葡萄牙语	{0F05E4E5-5A89-482C-9A62-47CC58643788}
罗马尼亚语	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
俄语	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
简体中文	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
西班牙语	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
西班牙语（墨西哥）	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
繁体中文	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
土耳其语	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

在 Kaspersky Security Center 中使用工具远程安装应用程序以便在受管理设备上运行相关可执行文件

使用新安装包向导，您可以选择任何可执行文件并为其定义命令行设置。为此，您可以添加所选文件或整个文件所在文件夹到安装包。然后，您必须创建远程安装任务并选择所创建的安装包。

当任务正在运行时，带有命令行所定义设置的指定可执行文件将在目标设备上运行。

如果您使用 Microsoft Windows Installer (MSI) 格式的安装程序，Kaspersky Security Center 使用标准工具分子安装结果。

如果有漏洞和补丁管理授权许可可用，Kaspersky Security Center (当为任何企业环境中支持的应用程序创建安装包时)也使用安装和安装结果分析规则。

否则，可执行文件的默认任务将等待运行中进程和所有子进程的完成。在所有运行中进程完成后，任务将被成功完成，不管初始进程的返回码是什么。要更改该任务的此类行为，在创建任务之前，您必须手动修改 Kaspersky Security Center 在新创建的安装包所在的文件夹及其子文件夹中生成的 .kpd 文件。

.kpd 文件使用 ASCII 编码。.kud 文件使用 Unicode 编码。

对于不需要等待运行中进程完成的任务，设置 [SetupProcessResult] 区域的等待设置的值为 0：

```
[SetupProcessResult]
Wait=0
```

对于仅需要等待 Windows 运行中进程，而不是所有子进程完成的任务，设置 [SetupProcessResult] 区域的 WaitJob 设置值为 0，例如：

```
[SetupProcessResult]
WaitJob=0
```

若要任务成功完成或者返回错误（具体取决于运行进程的返回码），创建一个将把错误代码保存到文件的可执行 .bat 文件，例如：

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

然后修改 Kaspersky Security Center 在新创建的安装包的文件夹中生成的 .kud 文件：

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0= 安装成功完成。
[SetupMainResult_ErrorCodes]
1=安装脚本错误
2=自定义错误
```

此种情况下，任何非列表中的返回码都会导致返回错误。

要在任务成功完成或任务结果错误中显示注释，在 [SetupProcessResult_SuccessCodes] 和 [SetupProcessResult_ErrorCodes] 区域根据进程返回码输入错误的简短描述，例如：

```
[SetupProcessResult_SuccessCodes]
0= 安装成功完成
3010=需要重启以完成安装
[SetupProcessResult_ErrorCodes]
1602=安装被用户取消
1603=安装过程中出现致命错误
```

要使用 Kaspersky Security Center 工具管理设备重启(如果需要重启以完成操作)，列出暗示重启的进程返回码，在 [SetupProcessResult_NeedReboot] 区域：

```
[SetupProcessResult_NeedReboot]
3010=
```

监控部署

要监控 Kaspersky Security Center 部署并确保在受管理设备上安装了安全应用程序和网络代理，您必须在“**部署**”区域检查信号灯。该信号灯位于管理控制台主窗口的管理服务器节点工作区。信号灯反映了当前部署状态。安装了网络代理和安全应用程序的设备数量显示在信号灯旁边。当任何安装任务正在运行时，您可以监控它们的进程。如果有任何安装错误发生，错误数量被显示。您可以通过点击链接查看错误详情。

您也可以在“**组**”选项卡上的“**受管理设备**”文件夹的工作区中使用部署方案。图表反映了部署进程，显示没有网络代理、带有网络代理或带有网络代理和安全应用程序的设备数量。

对于更多部署进程（或者特定安装任务的操作）的详情，请打开相关远程安装任务的结果窗口：右击任务并在上下文菜单中选择“**结果**”。窗口显示了两个列表：上面一个包含设备上的任务状态，下面一个包含从上面列表中选择的设备上的任务事件。

部署错误的信息被添加到管理服务器上的卡巴斯基事件日志。错误信息也会出现在“**报告和通知**”文件夹、“**事件**”子文件夹的相应事件分类中。

配置安装程序

该部分提供了 Kaspersky Security Center 安装程序文件和安装设置的信息，以及如何在静默模式安装管理服务器和网络代理的建议。

常规信息

Kaspersky Security Center 15.1 组件(管理服务器、网络代理和管理控制台)的安装程序根据 Windows Installer 技术创建。MSI 包是安装程序的核心。该格式的包允许使用 Windows Installer 的所有好处：可量测性、补丁系统可用性、转换系统、通过第三方解决方案集中安装以及在操作系统中透明注册。

在静默模式下安装(带有响应文件)

管理服务器和网络代理安装程序可以使用响应文件工作(ss_install.xml)，其中整合了不需要用户参与的静默模式安装参数。ss_install.xml 文件位于与 MSI 包相同的文件夹；在静默模式安装时被自动使用。您可以通过命令行参数“/s”启用静默安装模式。

一个大概例子运行如下：

```
setup.exe /s
```

在以静默模式启动安装程序之前，请阅读最终用户授权许可协议 (EULA)。如果 Kaspersky Security Center 分发包不包含带有 EULA 文本的 TXT 文件，您可以从 卡巴斯基网站 下载文件。

ss_install.xml 文件 Kaspersky Security Center 安装程序参数的内部格式的实例。分发包包含带有默认参数的 ss_install.xml 文件。

请不要手动修改 ss_install.xml 文件。该文件可以通过 Kaspersky Security Center 工具修改，当在管理控制台编辑安装包参数时。

要修改管理服务器安装的响应文件：

1. 打开 Kaspersky Security Center 分发包。如果您使用完整的包 EXE 文件，请将其解压缩。
2. 从 Server 文件夹中，打开命令行，然后运行以下命令：

   ```
   setup.exe /r ss_install.xml
   ```

   Kaspersky Security Center 安装程序启动。
3. 按照向导的步骤配置 Kaspersky Security Center 安装。

   当您完成向导时，响应文件会根据您指定的新设置自动修改。

在静默模式下安装网络代理（没有响应文件）

您可以使用单独 .msi 包安装网络代理，以标准方法指定 MSI 属性的值。该方案允许网络代理使用组策略安装。

请勿将安装包重命名为 Kaspersky Network Agent.msi。重命名此包可能会导致将来更新网络代理时出现安装错误。

要避免通过 MSI 包属性定义的参数与响应文件中定义的参数冲突，您可以通过设置属性 `DONT_USE_ANSWER_FILE=1` 来禁用响应文件。MSI 文件位于 Kaspersky Security Center 分发包，在 Packages\NetAgent\exec 文件夹。一个带有 .msi 包的网络代理安装程序运行例子如下。

在静默模式下安装网络代理需要接受最终用户授权许可协议的条款。只有在您完全阅读、理解并接受最终用户授权许可协议的条款后，才使用 `EULA=1` 参数。

```
例如：
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

您也可以通过提前准备响应文件(带有 .mst 扩展名)来定义 msi 包的安装参数。该命令显示如下：

```
例如：
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

您可以在单一命令行中指定几个响应文件。

如果要使用 Windows 安装程序升级网络代理，请运行以下命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

通过 setup.exe 的部分安装配置

当通过 setup.exe 运行应用程序安装时，您可以添加 MSI 任何属性的值到 MSI 包。

该命令显示如下：

例如：
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

管理服务器安装参数

下表描述了安装管理服务器时您可以配置的 MSI 属性。所有参数都是可选的，除了 EULA 和隐私策略。

静默模式下安装管理服务器的参数

MSI 属性	描述	可用值
EULA	是否接受授权许可协议条款（必需）。	• 1 – 我已完全阅读、理解并接受最终用户授权许可协议的条款。 • 其它值或没有值 – 我不接受授权许可协议的条款（将不会执行安装）。
PRIVACYPOLICY	是否接受隐私策略条款（必需）	• 1 – 我了解并同意我的数据将按照《隐私策略》中的说明进行处理和传输（包括第三国家/地区）。我确认已完全阅读并理解《隐私策略》。 • 其它值或没有值 – 我不接受隐私策略的条款（将不会执行安装）。
INSTALLATIONMODETYPE	管理服务器安装类型	• 标准。 • 自定义。
INSTALLDIR	应用程序的安装文件夹	字符串值。
ADDLOCAL	要安装的组件列表(以逗号分隔)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 管理服务器安装正常运行的最小组件列表： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	网络大小	• NRT_1_100 - 从 1 到 100 个设备。 • NRT_100_1000 - 101 到 1000 台设备。 • NRT_GREATER_1000 - 多于 1,000 台设备。
SRV_ACCOUNT_TYPE	指定操作管理服务器服务的用户的方法	• SrvAccountDefault - 将自动创建用户账户。 • SrvAccountUser - 手动定义用户账户。
SERVERACCOUNTNAME	服务用户名	字符串值。
SERVERACCOUNTPWD	服务用户密码	字符串值。
DBTYPE	数据库类型	• MySQL – 将使用 MySQL 或 MariaDB 数据库。 • MSSQL – Microsoft SQL Server (SQL Express) 数据库将被使用。
MYSQLSERVERNAME	MySQL 或 MariaDB 服务器的完整名称	字符串值。
MYSQLSERVERPORT	连接到 MySQL 或 MariaDB 服务器的端口号	数字值。
MYSQLDBNAME	MySQL 或 MariaDB 服务器数据库名称	字符串值。
MYSQLACCOUNTNAME	连接到 MySQL 或 MariaDB 服务器数据库的用户名	字符串值。

MSI 属性	描述	可用值
MYSQLACCOUNTPWD	连接到 MySQL 或 MariaDB 服务器数据库的用户密码	字符串值。
MSSQLCONNECTIONTYPE	MSSQL 数据库使用类型	• InstallMSSEE — 从包安装。 • ChooseExisting – 使用已安装服务器。
MSSQLSERVERNAME	SQL Server 实例的完整名称	字符串值。
MSSQLDBNAME	SQL Server 数据库名称	字符串值。
MSSQLAUTHTYPE	连接到 SQL Server 的身份验证方法	• Windows。 • SQLServer。
MSSQLACCOUNTNAME	以 SQLServer 模式连接到 SQL Server 的用户名	字符串值。
MSSQLACCOUNTPWD	以 SQLServer 模式连接到 SQL Server 的用户密码	字符串值。

CREATE_SHARE_TYPE	指定共享文件夹的方法	• Create—创建新共享文件夹。此种情况下，必须定义以下属性：
		  • SHARELOCALPATH – 本地文件夹路径。
		  • SHAREFOLDERNAME — 文件夹的网络名称。
		• Null — EXISTSHAREFOLDERNAME 必须被正确指定。

EXISTSHAREFOLDERNAME	现有共享文件夹的完整路径	字符串值。
SERVERPORT	连接至管理服务器的端口号	数字值。
SERVERSSLPORT	建立到管理服务器的 SSL 连接的端口号	数字值。
SERVERADDRESS	管理服务器地址	字符串值。
SERVERCERT2048BITS	管理服务器证书密钥长度（位）	• 1 – 管理服务器证书的密钥长度为 2048 位。 • 0 – 管理服务器证书的密钥长度为 1024 位。 • 如果未指定值，管理服务器证书的密钥长度为 2048 位。
MOBILESERVERADDRESS	连接移动设备的管理服务器地址；如果未选择 MobileSupport 组件则忽略	字符串值。

网络代理安装设置

下表描述了安装网络代理时您可以配置的 MSI 属性。所有参数都是可选的，除了 SERVERADDRESS。

MSI 的属性

MSI 属性	描述	可用值
DONT_USE_ANSWER_FILE	从响应文件读取安装参数	• 1 • Null
INSTALLDIR	安装文件夹	
SERVERADDRESS	管理服务器地址(必需)	
SERVERPORT	连接管理服务器的端口号	
SERVERSSLPORT	SSL 连接的端口号	
USESSL	是否使用 SSL 连接	• 1 • Null
OPENUDPPORT	是否打开 UDP 端口	• 1 • Null
UDPPORT	UDP 端口号	
USEPROXY	是否使用代理服务器	• 1 • Null
PROXYADDRESS	代理地址	

MSI 属性	描述	可用值
PROXYPORT	连接管理服务器的端口号	
PROXYLOGIN	连接代理服务器的账户	
PROXYPASSWORD	用于连接到代理服务器的账户的密码。 不在安装包参数中显示授权账户的任何细节。	
GATEWAYMODE	连接网关使用模式	• 0 – 不使用连接网关 • 1 – 使用该网络代理作为连接网关 • 2 – 使用连接网关连接到管理服务器
GATEWAYADDRESS	连接网关地址	
CERTSELECTION	接收证书的方法	• GetOnFirstConnection – 从管理服务器接收证书。 • GetExistent – 选择一个现有证书。如果选择此选项，则必须定义 CERTFILE 属性。
CERTFILE	证书文件路径	
VMVDI	启用 VDI 动态模式	• 1 • Null
LAUNCHPROGRAM	安装后是否启动网络代理服务	• 1 • Null

虚拟基础架构

Kaspersky Security Center 支持虚拟机的使用。您可以在每台虚拟机上安装网络代理和安全应用程序，并可以在虚拟机监控程序级别保护虚拟机。在第一种情况下，您可以使用标准安全应用程序或 Kaspersky Security for Virtualization Light Agent 来保护您的虚拟机。在第二种情况下，您可以使用 Kaspersky Security for Virtualization Agentless。

Kaspersky Security Center 支持虚拟机回滚到先前状态。

降低虚拟机负载的窍门

当安装网络代理到虚拟机时，建议您禁用一些对虚拟机没有用的 Kaspersky Security Center 功能。

在虚拟机或用于生成虚拟机的模版上安装网络代理时，建议执行以下操作：

- 如果要运行远程安装，则在网络代理安装包的属性窗口的“**高级**”区域中，选择“**优化 VDI 设置**”选项。
- 如果要通过向导运行交互式安装，则在向导窗口中选择“**为虚拟基础架构优化网络代理设置**”选项。

选择这些选项将改变网络代理设置，因此以下功能在默认情况下保持禁用状态（在应用策略之前）：

- 获取已安装软件的信息
- 获取硬件信息
- 获取检测到的漏洞信息
- 获取需要更新的信息

通常，这些功能对于虚拟机不必要，因为它们使用统一软件和虚拟硬件。

禁用该功能是不可逆的。如果需要任何被禁用的功能，您可以通过网络代理策略启用它，或通过网络代理本地设置。网络代理本地设置通过管理控制台中相关设备的上下文菜单可用。

对动态虚拟机的支持

Kaspersky Security Center 支持动态虚拟机。如果虚拟架构部署在组织网络，动态（临时）虚拟机可以被用在特定情况。动态虚拟机基于管理员提供的模板以独立名称创建。用户使用了虚拟机一段时间，然后关闭虚拟机，则该虚拟机将从虚拟基础架构中删除。如果 Kaspersky Security Center 部署在组织网络，安装了网络代理的虚拟机将被添加到管理服务器数据库。在您关闭虚拟机后，对应的条目必须从管理服务器数据库中删除。

要运行自动删除虚拟机上的条目的功能，在动态虚拟机的模板上安装网络代理时，请选中“**启用 VDI 动态模式**”选项：

- 对于远程安装—在网络代理安装包的属性窗口（**高级**区域）
- 对于交互式安装 — 在“网络代理安装向导”中进行

> 当安装网络代理到物理设备时，不要选中“**启用 VDI 动态模式**”选项。

如果您要在删除虚拟机后将动态虚拟机的事件存储在管理服务器一段时间，那么，在管理服务器属性窗口，在“**事件存储库**”区域，选择“**设备被删除后存储事件**”选项并指定事件的最大存储期限（天）。

> 我们不建议在动态虚拟机上启用加密驱动器。

对虚拟机复制的支持

复制安装了网络代理的虚拟机或从安装了网络代理的模板创建虚拟机，和捕获和复制硬盘驱动器镜像的网络代理部署相同。因此，常规情况下，当复制虚拟机时，您需要执行与通过复制磁盘镜像部署网络代理时相同的操作。

然而，以下描述的两种情况展示了自动检测复制的网络代理。由于以上原因，您不必运行“通过捕获和复制设备磁盘镜像部署”中描述的复杂操作：

- “**启用 VDI 动态模式**”选项在网络代理被安装时选中：在操作系统每次重启后，该虚拟机将被认为是新设备，无论是否被复制。
- 以下 Hypervisor 之一被使用：VMware™、HyperV® 或 Xen®：网络代理通过更改的虚拟硬件 ID 检测虚拟机的复制。

> 虚拟硬件更改分析并不绝对可靠。在广泛应用该方法之前，您必须在小组虚拟机上测试您组织中使用的当前 hypervisor 版本。

对网络代理设备文件系统回滚的支持

Kaspersky Security Center 是一个分发的应用程序。在安装了网络代理的设备上回滚文件系统到先前状态将导致数据不同步和 Kaspersky Security Center 功能不正常。

文件系统(或一部分)可以在以下情况下回滚：

- 当复制硬件驱动器镜像时。
- 当通过虚拟架构恢复虚拟机状态时。
- 当从备份副本或恢复点恢复数据时。

安装了网络代理的设备上的第三方软件影响 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 文件夹的情景仅是 Kaspersky Security Center 的关键情景。因此，如果可能，您必须总是从恢复进程中排除该文件夹。

因此一些组织的工作规则提供了对设备文件系统的回滚，对安装了网络代理的设备的文件系统回滚的支持被添加到了 Kaspersky Security Center，从版本 10 Maintenance Release 1 开始(管理服务器和网络代理必须是版本 10 Maintenance Release 1 或更新)。当检测到时，这些设备被自动连接到管理服务器，带有完整数据清除和完整同步。

默认下，对文件系统回滚检测的支持在 Kaspersky Security Center 15.1 中被启用。

尽量不要回滚网络代理设备的 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 文件夹，因为完整数据的重新同步需要大量资源。

系统状态回滚在管理服务器设备上是不允许的。管理服务器使用的数据库的回滚也是不允许的。

您可以仅可以使用标准的 klbackup 实用工具从备份副本恢复管理服务器状态。

关于漫游用户的连接配置文件

便携式电脑（也叫“设备”）的漫游用户需要更改连接到管理服务器的方法或者根据当前设备在企业网络中的位置在管理服务器之间进行切换。

连接配置文件仅支持运行 Windows 和 macOS 的设备。

使用单一管理服务器的不同地址

网络代理设备从组织网络或内部网可以连接到管理服务器。该情况可能需要网络代理使用不同的地址以连接到管理服务器：对于互联网连接的外部管理服务器地址和对于内部网络连接的内部管理服务器地址。

为此，您必须添加配置文件(为了从互联网连接到管理服务器)到网络代理策略。在策略属性中添加配置文件（**连接**区域，**连接配置文件**子区域）。在配置文件创建窗口，您必须禁用“**仅用来接收更新**”选项，并选择“**与此配置文件中指定的管理服务器设置同步连接设置**”选项。如果您使用连接网关访问管理服务器（例如，在“互联网访问：DMZ 中作为连接网关的网络代理”部分描述的 Kaspersky Security Center 配置中），您必须在连接配置文件的对应字段指定连接网关地址。

根据当前网络在管理服务器之间进行切换

如果组织有带有多个管理服务器的多个办公室，并且一些网络代理设备在期间进行移动，您需要网络代理连接到设备所在的本地网络中的管理服务器。

此种情况下，您必须为每个办公室在网络代理策略属性中创建连接管理服务器的配置文件，除了原始归属管理服务器所在的主办公室。您必须在连接配置文件中指定管理服务器地址并启用或禁用“**仅用来接收更新**”选项：

- 在使用本地服务器下载更新时，如果您需要网络代理与归属管理服务器同步，则选择该选项。
- 如果网络代理必须被本地管理服务器完全管理，则禁用此选项。

此后，您必须设置切换到新创建的配置文件的条件：每个办公室至少一个条件，除了归属办公室。每个条件的目的包括办公室网络环境条目的检测。如果条件是真，对应配置文件被激活。如果没有条件是真，网络代理切换到归属管理服务器。

部署移动设备管理功能

本节提供有关初始部署移动设备管理功能的信息。

将 KES 设备连接至管理服务器

根据连接设备到管理服务器的方法，对 KES 设备 Kaspersky Device Management for iOS 有两个部署方案：

- 直接连接设备到管理服务器来部署的方案
- 涉及支持 Kerberos 约束委派的反向代理的部署方案

直接连接设备到管理服务器

KES 设备可以直接连接到管理服务器的端口 13292。

根据使用的身份验证方法，连接 KES 设备到管理服务器有两个选项：

- 使用用户证书连接设备
- 不用用户证书连接设备

使用用户证书连接设备

当连接带有用户证书的设备时，设备与通过管理服务器工具被分配证书的用户账户相关联。

此种情况下，双向 SSL 身份验证（双向认证）将被使用。管理服务器和设备都将使用证书认证。

不用用户证书连接设备

当连接没有用户证书的设备时，设备不与任何管理服务器上的用户账户关联。然而，当设备接收任何证书时，设备将与通过管理服务器工具被分配证书的用户相关联。

当连接设备到管理服务器时，将应用单向 SSL 身份验证，这意味着仅管理服务器使用证书进行身份验证。设备获取用户证书后，身份验证类型将变更为双向 SSL 身份验证(双向 SSL 身份验证，共有身份验证)。

连接 KES 设备到 Kerberos constrained delegation (KCD) 服务器的方案

连接 KES 设备到 Kerberos constrained delegation (KCD) 管理服务器的方案包括如下：

- 与支持 KCD 的反向代理集成。
- 将 Kerberos Constrained Delegation (KCD) 用于移动设备身份验证。
- 与公共密钥基础架构(PKI)整合以应用用户证书。

当使用该连接方案时，请注意以下几点：

- 连接 KES 设备到反向代理的类型必须是“双向 SSL 身份验证”，就是，设备必须通过先前用户证书连接到反向代理。为此，您不要整合用户证书到 Kaspersky Endpoint Security for Android 安装包。该 KES 包必须由设备指定的管理服务器创建。
- 您必须指定特定(自定义)证书，而不是移动协议的默认服务器证书：
  1. 在管理服务器的属性窗口，在**设置**区域，选择**为移动设备打开端口**复选框，然后在下拉列表中选择**添加证书**。
  2. 在打开的窗口中，指定当到移动协议的访问点被发布在管理服务器时设置在反向代理上的证书。
- KES 设备的用户证书必须由域中的 Certificate Authority (CA) 发布。记住，如果域包含多个多个根 CA，用户证书必须被该 CA 发布，这已设置在反向代理发布中。

  您可以通过以下方法确保用户证书与上述需求兼容：
  - 在新建安装包向导和证书安装向导中指定用户证书。
  - 将管理服务器与域的 PKI 整合并在证书发布规则中定义对应的设置：
    1. 在控制台树中，展开“**移动设备管理**”文件夹并选择“**证书**”子文件夹。
    2. 在**证书**文件夹的工作区中，单击“**配置证书发布规则**”按钮以打开“**证书发布规则**”窗口。
    3. 在“**与 PKI 整合**”区域，配置与公共密钥基础架构的整合。
    4. 在“**移动证书发布**”区域，指定证书源。

以下是使用以下假定设置 Kerberos Constrained Delegation (KCD) 的例子：

- 管理服务器到移动协议的访问点被设置成端口 13292。
- 具有反向代理的设备的名称是firewall.mydom.local。
- 管理服务器设备名称是 ksc.mydom.local。
- 访问点到移动协议的外部发布地址是 kes4mob.mydom.global。

管理服务器域账户

您必须创建运行管理服务器服务的域账户(例如，KSCMobileSrvcUsr)。您可以在安装管理服务器或使用 klsrvswch 实用工具时指定管理服务器服务账户。klsrvswch 实用工具位于管理服务器安装文件夹。默认安装路径：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

域账户必须由以下原因指定：

- KES 设备管理功能是管理服务器的一部分。
- 要确保 Kerberos Constrained Delegation (KCD) 的正常功能，接收端(例如，管理服务器)必须运行在域账户下。

http/kes4mob.mydom.local 的服务主体名称

在域中，在 KSCMobileSrvcUsr 账户下，添加 SPN 以在管理服务器设备的端口 13292 发布移动协议服务。对于管理服务器设备 kes4mob.mydom.local，将是如下：

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

配置具有反向代理 (firewall.mydom.local) 的设备的域属性

要授权流量，您必须将反向代理设备(tmg.mydom.local) 托付给由 SPN 定义的服务 (http/kes4mob.mydom.local:13292)。

要将具有反向代理的设备托付给由 SPN 定义的服务 (http/kes4mob.mydom.local:13292)，管理员必须执行以下操作：

1. 在名为“活动目录用户和计算机”的 Microsoft Management Console 中，选择安装了反向代理的设备 (firewall.mydom.local)。
2. 在设备属性窗口，在**授权**选项卡，设置**信任此计算机到指定服务的授权**切换键到**使用任何身份验证协议**。
3. 在**该账户可以展示已授权凭证的服务**列表，添加 SPN http/kes4mob.mydom.local:13292。

要发布的特定(自定义)证书(kes4mob.mydom.global)

要发布管理服务器移动协议，您必须发布一个 FQDN kes4mob.mydom.global 特定(自定义)证书并在管理控制台中管理服务器的移动协议设置中指定它以代替默认服务器证书。为此，在管理服务器的属性窗口，在**设置**区域，选择**为移动设备打开端口**复选框，然后在下拉列表中选择**添加证书**。

请注意服务器证书容器(带有 .p12 或 .pfx 扩展名的文件)必须也包含根证书链(公共密钥)。

配置在反向代理上发布

在反向代理上，对于从移动设备到端口 kes4mob.mydom.global 端口 13292 的流量，您必须在 SPN (http/kes4mob.mydom.local:13292) 上配置 KCD，使用为 FQND kes4mob.mydom.global 发布的证书。请注意，正发布和已发布的访问点(管理服务器端口 13292)必须共享相同的服务器证书。

使用 Firebase Cloud Messaging

为了确保及时将命令交付到 Android 操作系统管理的 KES 设备上， Kaspersky Security Center 使用推送通知机制。KES 设备和管理服务器之间通过 Firebase Cloud Messaging（以下简称 FCM）交换推送通知。在 Kaspersky Security Center 管理控制台中，可以指定 Firebase Cloud Messaging 的设置从而将 KES 设备连接到服务。

要检索 Firebase Cloud Messaging 的设置，您必须有 Google 账户。

要启用对 FCM 的使用：

1. 在管理控制台中，选择“**移动设备管理**”节点以及“**移动设备**”文件夹。
2. 在“**移动设备**”文件夹的上下文菜单中，选择**属性**。
3. 在文件夹属性中，选择“**Firebase Cloud Messaging 设置**”区域。
4. 在**Firebase 项目编号**字段中，指定 FCM 发件人 ID。
5. 在**私钥文件 (JSON 格式)**字段中，选择私钥文件。

在下次同步管理服务器时，由 Android 操作系统管理的 KES 设备将被连接到 Firebase Cloud Messaging。

通过单击“**重置设置**”按钮，您可以编辑 Firebase Cloud Messaging 的设置。

当切换到不同的 Firebase 项目时，您需要等待 10 分钟才能恢复 FCM。

FCM 服务在以下地址范围内运行：

- 从 KES 设备端，需要对以下地址的端口 443 (HTTPS)、5228 (HTTPS)、5229 (HTTPS) 和 5230 (HTTPS) 的访问：
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Google's ASN 15169 中列出的所有 IP 地址
- 从管理服务器端，需要对以下地址的端口 443 (HTTPS) 的访问：
  - fcm.googleapis.com
  - Google's ASN 15169 中列出的所有 IP 地址

如果代理服务器设置（**高级/配置互联网访问**）已在管理控制台的管理服务器属性中指定，则这些设置将用于与 GFCM 交互中。

配置 FCM：获取发件人 ID 和私钥文件

要配置 FCM：

1. 在 Google 门户注册。
2. 转到Firebase 控制台。
3. 执行以下操作之一：
   - 要创建新项目，请单击**创建项目**并按照屏幕上的说明进行操作。
   - 打开现有项目。
4. 单击齿轮图标并选择**项目设置**。
   "**项目设置**"窗口将开启。
5. 选择**Cloud Messaging**选项卡。
6. 从**Firebase Cloud Messaging API (V1)**部分中的**发件人 ID**字段检索相关的发件人 ID。
7. 选择**服务账户**选项卡，然后单击**生成新私钥**。
8. 在打开的窗口中，单击**生成密钥**以生成并下载私钥文件。

Firebase Cloud Messaging 现已配置。

与公共密钥基础架构整合

与公共密钥基础架构(PKI)整合旨在管理服务器对域用户证书的发布。

管理员可以在管理控制台中为用户分配域证书。这可以使用以下方法完成：

- 在证书安装向导中从文件中给用户分配特定（自定义）证书。
- 执行与 PKI 的整合并分配 PKI 以作为制定类型证书或所有类型证书的证书源。

通过单击"**与公钥基础架构整合**"链接，可以在"**移动设备管理**"/"**证书**"文件夹的工作区中使用与 PKI 集成的设置。

用于域用户证书发布的与 PKI 整合的常规原则

在管理控制台，单击"**与公钥基础架构整合**"链接（在"**移动设备管理**"/"**证书**"文件夹的工作区）指定一个域账户，管理服务器将使用该域账户通过域的 CA 发布域用户证书（以下称为执行与 PKI 整合的账户）。

请注意以下：

- 与 PKI 整合的设置允许您为所有类型的证书指定默认模板。请注意，证书发布规则（通过单击"**配置证书发布规则**"按钮，规则在"**移动设备管理**"/"**证书**"文件夹的工作区中可用）允许您为每种类型的证书指定各自的模板。
- 特殊 Enrollment Agent (EA) 证书必须安装在管理服务器设备，在与 PKI 整合的账户的证书存储库中。Enrollment Agent (EA) 证书由域 CA (Certificate Authority) 管理员发布。

与 PKI 整合的账户必须满足以下标准：

- 它是域用户。
- 它是发起与 PKI 的整合的管理服务器设备本地管理员。
- 它具有*作为服务登录*的权限。
- 管理服务器设备必须在此账户下运行至少一次以创建永久用户配置文件。

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server（以下简称"Web 服务器"）是 Kaspersky Security Center 的一个组件。Web 服务器用于发布独立安装包、移动设备独立安装包和共享文件夹的文件。

所创建的安装包被自动发布在 Web 服务器并在第一次下载后被删除。管理员可以通过任意方式如电子邮件等将新链接发送给用户。

通过单击链接，用户可将所需信息下载至移动设备。

Web 服务器设置

如果需要 Web 服务器的 fine-tuning，其属性允许您更改 HTTP (8060) 和 HTTPS (8061) 端口。除了更改端口，您可以为 HTTPS 替换服务器证书并为 HTTP 更改 Web 服务器的 FQDN。

其他日常工作

该部分提供 Kaspersky Security Center 的常规使用建议。

在管理控制台中监控信号灯和记录的事件

管理控制台允许您通过检查信号灯快速评估当前 Kaspersky Security Center 状态和受管理设备。信号灯显示在"**管理服务器**"节点工作区的"**监控**"选项卡。选项卡提供了带有信号灯的六个信息窗格和记录。信号灯是面板左侧的彩色栏。每个带有信号灯的窗格对应于 Kaspersky Security Center 的特定功能范围(参见下表)。

管理控制台中信号灯覆盖的范围

窗格名称	信号灯范围
部署	在组织网络设备上安装网络代理和安全应用程序
管理方案	管理组结构。网络扫描。设备移动规则
保护设置	安全应用程序功能：保护状态、恶意软件扫描
更新	更新和补丁
监控	保护状态
管理服务器	管理服务器功能和属性

每个信号灯可以变换五种颜色(参见下表)。信号灯的颜色取决于 Kaspersky Security Center 的当前状态和记录的事件。

信号灯的颜色码

状态	信号灯颜色	信号灯颜色意义
信息	绿色	不需要管理员介入。
警告	黄色	需要管理员介入。
严重	红色	发生了严重问题。需要管理员介入以解决。
信息	淡蓝色	与受管理设备的潜在或实际威胁无关的事件被记录。
信息	灰色	事件详情不可用或未获取。

管理员的目标是保持"**监控**"选项卡的所有信息窗格上的信号灯是绿色的。

信息窗格还显示影响信号灯和 Kaspersky Security Center 的状态的记录事件（请见下表）。

所记录事件的名称、描述和信号灯颜色

信号灯颜色	事件类型显示名称	事件类型	描述
红色	**%1 台设备上的授权许可已过期**	IDS_AK_STATUS_LIC_EXPAIRED	当商业授权许可已到期时，会发生此类事件。 Kaspersky Security Center 每天检查一次设备上的授权许可是否到期。 当商业授权许可到期时，Kaspersky Security Center 仅提供基本功能。 要继续使用 Kaspersky Security Center，请续费您的商业授权许可。
红色	**安全应用程序没有运行：%1 台设备**	IDS_AK_STATUS_AV_NOT_RUNNING	当设备上安装的应用程序不运行时会发生这种类型的事件。 请确保 Kaspersky Endpoint Security 在设备上运行。
红色	**已禁用保护：%1 台设备**	IDS_AK_STATUS_RTP_NOT_RUNNING	当设备上的安全应用程序已被禁用大于指定的时间段时会发生这种类型的事件。 检查设备上的实时保护当前状态，确保您需要的所有保护组件已启用。
红色	**在设备上检测到软件漏洞**	IDS_AK_STATUS_VULNERABILITIES_FOUND	当*查找漏洞和所需更新*任务在设备上安装的应用程序中检测到指定严重级别的漏洞时，会发生这种类型的事件。 在**应用程序管理**文件夹的**软件更新**子文件夹中检查可用更新列表。该文件夹包含了管理服务器检索的可以被分发到设备的 Microsoft 应用程序和其他软件厂商产品的更新列表。 查看各种更新的信息后，请在设备上安装它们。
红色	**管理服务器上注册了严重事件**	IDS_AK_STATUS_EVENTS_OCCURED	当检测到管理服务器严重事件时会发生这种类型的事件。 检查存储在管理服务器上的事件列表，然后逐个修复严重事件。
红色	**管理服务器上记录了错误事件**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	当管理服务器端记录了意外错误时会发生这种类型的事件。 检查存储在管理服务器上的事件列表，然后逐个修复错误。
红色	**失去与 %1 台设备的连接**	IDS_AK_STATUS_ADM_LOST_CONTROL1	当管理服务器和设备之间的连接丢失时会发生这种类型的事件。 请查看连接设备列表并尝试重新连接它们。
红色	**%1 台设备已长时间未连接到管理服务器**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	当由于设备关闭，设备在指定时间段内未连接到管理服务器时会发生这种类型的事件。 请确保设备已开启且网路代理在运行。
红色	**有 %1 台设备状态不正常**	IDS_AK_STATUS_HOST_NOT_OK	当连接到管理服务器的设备的状态由 *OK*变为*严重*或者*警告*时会发生这种类型的事件。 您可以使用Kaspersky Security Center 远程诊断工具解决问题。

信号灯颜色	事件类型显示名称	事件类型	描述
红色	**数据库过期：%1 台设备**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	当设备上的反病毒数据库未在指定时间段内更新时会发生这种类型的事件。 按照指示更新卡巴斯基数据库。
红色	**Windows Update 更新检查长时间没有运行的设备：%1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	当“*执行 Windows 更新同步*”任务在指定时间段内未运行时会发生这种类型的事件。 按照指示使用管理服务器从 Windows 更新同步更新。
红色	**Kaspersky Security Center 的 %1 个插件必须安装**	IDS_AK_STATUS_PLUGINS_REQUIRED2	当您需要为卡巴斯基应用程序安装其它插件时会发生这种类型的事件。 从卡巴斯基技术支持网页 下载和安装所需的卡巴斯基应用程序管理插件。

远程访问受管理设备

该部分提供了远程访问受管理设备的信息。

使用“不要断开与管理服务器的连接”选项提供受管理设备和管理服务器之间的持续连接

如果你不使用推送服务器，则 Kaspersky Security Center 不提供受管理设备和管理服务器之间的持续连接。受管理设备上的网络代理定期建立连接并与管理服务器同步。同步会话之间的时间间隔定义在网络代理策略中。如果需要提前同步，管理服务器（或分发点，如果正在使用）会通过 IPv4 或 IPv6 网络将签名的网络数据包发送到网络代理的 UDP 端口。默认情况下，端口号指定为 15000。如果在管理服务器和受管理设备之间无法通过 UDP 建立连接，则在同步间隔内的下次网络代理和管理服务器常规连接时将运行同步。

如果没有网络代理和管理服务器之间的早期连接，某些操作将无法执行，例如运行和停止本地任务、接收受管理应用程序的统计信息或创建隧道。要解决此问题，如果您不使用推送服务器，可以使用“**不断开与管理服务器的连接**”选项以确保受管理设备和管理服务器之间存在持续连接。

要提供客户端设备与管理服务器之间的持续连接：

1. 在控制台树中，选择“**受管理设备**”文件夹。
2. 在文件夹的工作区中，选择要使用其提供持续连接的受管理设备。
3. 在设备的上下文菜单中，选择“**属性**”。
   所选设备的属性窗口打开。
4. 在显示的窗口的“**常规**”区域中，选择“**不断开与管理服务器的连接**”选项。

持续连接在受管理设备和管理服务器之间被建立。

选中“**不断开与管理服务器的连接**”选项时的最大设备总数为 300。

关于检查设备和管理服务器之间的连接时间

在关闭设备时，网络代理通知管理服务器该事件。在管理控制台，设备显示为已关闭。然而，网络代理无法通知管理服务器所有此类事件。因此，管理服务器会定期分析每台设备的“**连接到管理服务器**”属性（属性值显示在管理控制台“设备”属性中的“**常规**”区域中），并将它与网络代理当前设置中的同步间隔相比较。如果一台设备在超过三次成功的同步间隔后未响应，该设备被标记为已关闭。

关于强制同步

尽管 Kaspersky Security Center 自动为受管理设备同步状态、设置、任务和策略，一些情况下，管理员需要准确知道是否同步已经在指定设备上执行。

在管理控制台受管理设备的上下文菜单中，“**所有任务**”菜单项包含“**强制同步**”命令。当 Kaspersky Security Center 15.1 执行该命令时，管理服务器试图连接到设备。如果该尝试成功，强制同步将被执行。否则，同步将仅在网络代理与管理服务器的下一次计划连接后被强制。

关于隧道

Kaspersky Security Center 允许通过管理服务器的从管理控制台的 TCP 连接通道，然后通过网络代理到受管理设备上的指定端口。通道设计用于连接网络控制台设备上的客户端应用程序到受管理设备上的 TCP 端口—如果管理控制台和目标设备之间没有直接连接可用。

例如，通道用于连接到远程桌面，可以连接到已存在会话，也可以创建一个新的远程会话。

通道也可以使用外部工具启用。例如，管理员可以运行 putty 实用工具、VNC 客户端和其他工具。

层级指南

该部分提供了 Kaspersky Security Center 尺寸信息。

关于本指南

Kaspersky Security Center 15.1（也称为 Kaspersky Security Center）层级指南专为安装管理 Kaspersky Security Center 的专业人员，以及为使用 Kaspersky Security Center 的企业提供技术支持的人员而设计。

所有建议都给予由 Kaspersky Security Center 管理安装了 Kaspersky 软件的设备（包括移动设备）的保护的网络。如果移动设备、或者任何其他受管理设备要被特殊考虑，这将特别阐述。

要在不同的操作条件下获取和维持优化运行，您必须考虑网络设备数量、网络拓扑和您需要的 Kaspersky Security Center 功能集。

此指南提供下列信息：

- Kaspersky Security Center 的限制
- Kaspersky Security Center 关键节点的限制（管理服务器和分发点）：
  - 管理服务器和分发点的硬件需求
  - 管理服务器数量和层级限制
  - 计算分发点的数量和配置
- 数据库中的事件记录配置取决于网络设备的数量
- 性能优化的常见最佳实践
- 特定任务的配置旨在优化 Kaspersky Security Center 的性能
- Kaspersky Security Center 管理服务器和每个受保护设备间的流量率(网络负载)

以下情况下建议参考该文档：

- 当在安装 Kaspersky Security Center 前计划资源时
- 当向部署了 Kaspersky Security Center 的网络计划显著更改时
- 从在受限制网段（测试环境）使用 Kaspersky Security Center 切换到在企业网络上全面部署 Kaspersky Security Center 时
- 当对使用的 Kaspersky Security Center 功能集做更改时

Kaspersky Security Center 的限制信息

下表显示了 Kaspersky Security Center 当前版本的限制。

Kaspersky Security Center 的限制

限制类型	参数值
每个管理服务器的最大受管理设备数量	100,000
选中"**不断开与管理服务器的连接**"选项时的最大设备数	300
管理组最大数量	10,000
要存储的事件的最大数量	45,000,000
策略的最大数量	2000
任务的最大数量	2000
活动目录对象的最大总数（组织单元 (OU) 和用户账户、设备和安全组）	1,000,000
策略中配置文件的最大数量	100
单一主管理服务器的从属管理服务器的最大数量	500
虚拟管理服务器的最大数量	500
单一分发点可以覆盖的最大设备数量（分发点仅可以覆盖非移动设备）	10,000
可以使用单一连接网关的最大设备数量	10,000，包括移动设备
每个管理服务器的最大移动设备数量	100,000 减去固定的受管理设备数量

管理服务器计算

该部分提供了管理服务器设备的软件和硬件需求。也提供了根据组织网络配置计算管理服务器数量和层级的建议。

管理服务器的硬件资源计算

该部分包含为计划管理服务器的硬件资源提供向导的计算。当使用漏洞和补丁管理功能时还建议计算磁盘空间。

DBMS 和管理服务器的硬件需求

下表提供了测试得出的 DBMS 和管理服务器建议最低硬件要求。对于支持的操作系统和 DBMS 的完整列表，请参考硬件和软件需求列表。

管理服务器和 DBMS 位于不同设备，网络中包含 50,000 台设备

安装了管理服务器的设备的配置

硬件	参数值
CPU	4 核，2500 MHz
RAM	8 GB
硬盘驱动器	300 GB，RAID(推荐)
网卡	1 Gbit

安装了 DBMS 服务器的设备的配置

硬件	参数值
CPU	4 核，2500 MHz
RAM	16 GB
硬盘驱动器	200 GB，SATA RAID
网卡	1 Gbit

管理服务器和 DBMS 位于同一设备，网络中包含 50,000 台设备

安装了管理服务器和 DBMS 的设备的配置

硬件	参数值
CPU	8 核，2500 MHz
RAM	16 GB
硬盘驱动器	500 GB，SATA RAID
网卡	1 Gbit

管理服务器和 DBMS 位于不同设备，网络中包含 100,000 台设备

安装了管理服务器的设备的配置

硬件	参数值
CPU	8 核，2.13 GHz
RAM	8 GB
硬盘驱动器	1 TB，RAID
网卡	1 Gbit

安装了 DBMS 的设备的配置

硬件	参数值
CPU	8 核，2.53 GHz
RAM	26 GB
硬盘驱动器	500 GB，SATA RAID
网卡	1 Gbit

测试在以下系统上运行：

- 自动分配分发点在管理服务器上启用，或者分发点根据建议的表格被手动指定。
- 备份任务保存备份副本到位于专用服务器的文件资源。

- 网络代理的同步间隔按下表设置。

网络代理同步间隔

同步间隔（分钟）	受管理设备数量
15	10,000
30	20,000
45	30,000
60	40,000
75	50,000
150	100,000

数据库空间计算

必须在数据库中保留的大约空间可以使用以下公式计算：

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

其中：

- C 是设备数量。
- E 要存储的事件的数量。
- A 是活动目录对象的总数：
  - 设备账户
  - 用户账户
  - 安全组账户
  - 活动目录组织单元

  如果活动目录扫描被禁用，A 等效于 0。
- N 是端点设备上已清查可执行文件的平均数量。
- F 是端点设备的数量，其中可执行文件已清查。

如果您计划在 Kaspersky Endpoint Security 策略设置中启用通知管理服务器您运行的应用程序，您将需要额外空间(0.03 * C GB)在数据库中存储您运行的应用程序信息。

如果管理服务器发布 Windows 更新（做为 Windows Server Update Services 服务器），数据库将需要额外的 2.5 GB。

操作期间，一定的*未占用空间*总是出现在数据库。因此，数据库文件的实际尺寸（默认下，如果您使用 SQL Server 做为 DBMS 的话，是 KAV.MDF 文件）经常是两倍于数据库中被占用空间的尺寸。

不建议明确限制透明日志（默认下，文件 KAV_log.LDF，如果您使用 SQL Server 作为 DBMS）的大小。建议保留 MAXSIZE 参数的默认值。然而，如果您必须限制该文件的大小，请考虑对于 KAV_log.LDF，参数 MAXSIZE 的典型必要最小值是 20480 MB。

磁盘空间计算（使用或不使用漏洞和补丁管理功能）

磁盘空间计算（不使用漏洞和补丁管理功能）

管理服务器需要的磁盘空间 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 文件夹可以使用以下公式估算：

(724 * C + 0.15 * E + 0.17 * A), KB

其中：

- C 是设备数量。
- E 要存储的事件的数量。
- A 是活动目录对象的总数：
  - 设备账户
  - 用户账户
  - 安全组账户
  - 活动目录组织单元

如果活动目录扫描被禁用，A 等效于 0。

附加磁盘空间计算（使用漏洞和补丁管理功能）

- 更新。共享文件夹额外需要至少 4 GB 来存储更新。
- 安装包。如果一些安装包存储在管理服务器，共享文件夹将需要额外磁盘空间，等于所有要安装的安装包的总大小。
- “远程安装”任务。如果管理服务器上有任何远程安装任务，额外的磁盘空间（在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 文件夹）与要安装的所有安装包大小相当。
- 补丁。如果管理服务器需要安装补丁，将需要额外的磁盘空间：
  - 补丁文件夹应该具有与下载的所有补丁的总大小相当的磁盘空间。默认情况下，补丁存储在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 文件夹中。

    您可以使用 klsrvswch 实用程序指定用于存储补丁的不同文件夹。klsrvswch 实用程序位于安装管理服务器的文件夹中。默认安装路径：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

    如果管理服务器被用作 WSUS 服务器，建议您分配至少 100 GB 到该文件夹。
  - %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 文件夹必须具有与现有更新（补丁）安装实例和漏洞修复任务所引用的补丁的总大小相当的磁盘空间。

计算管理服务器的数量和配置

要减少主管理服务器负载，您可以分配另外的管理服务器到每个管理组。每个主管理服务器的从属管理服务器的数量不能超过 500。

我们建议您基于您组织网络的配置来创建管理服务器配置。

有关将动态虚拟机连接到 Kaspersky Security Center 的建议

动态虚拟机（也简称为“动态 VM”）比静态虚拟机消耗更多资源。

有关动态虚拟机的更多信息，请参阅对动态虚拟机的支持。

连接新的动态 VM 时，Kaspersky Security Center 在管理控制台中为此动态 VM 创建一个图标并将该动态 VM 移至管理组。此后，动态 VM 被添加到管理服务器数据库中。管理服务器与安装在此动态 VM 上的网络代理完全同步。

在组织的网络中，网络代理为每个动态 VM 创建以下网络列表：

- 硬件
- 安装的软件
- 检测到的漏洞
- 应用程序控制组件的事件和可执行文件列表

网络代理将这些网络列表传输到管理服务器。网络列表的大小取决于安装在动态 VM 上的组件，并且可能会影响 Kaspersky Security Center 和数据库管理系统的 (DBMS) 性能。注意，负载可能呈非线性增长。

在用户使用完动态 VM 并将其关闭后，该虚拟机将从虚拟基础架构中删除，且有关该虚拟机的条目也将从管理服务器数据库中删除。

所有这些操作都会消耗大量的 Kaspersky Security Center 和管理服务器数据库资源，并会降低 Kaspersky Security Center 和 DBMS 的性能。建议您最多将 20,000 个动态 VM 连接到 Kaspersky Security Center。

如果连接的动态 VM 执行标准操作（例如，数据库更新）并且消耗不超过 80% 的内存和 75-80% 的可用内核，您可以将超过 20,000 个动态 VM 连接到 Kaspersky Security Center。

更改动态 VM 上的策略设置、软件或操作系统可能减少或增加资源消耗。最优资源消耗占比为 80-95%。

分发点和连接网关的计算

该部分提供了用作分发点的设备的硬件需求，以及根据企业网络配置计算分发点和连接网关数量的建议。

分发点需求

要处理多达 10,000 台客户端设备，分发点必须至少满足以下要求（提供了测试台配置）：

- CPU：Intel Core™ i7-7700 CPU 3.60 GHz 4 核。
- RAM：8 GB。
- 可用存储空间：120 GB。

不建议将管理服务器分配为分发点，因为这样会增加管理服务器的负荷。

如果管理服务器上有任何远程安装任务等待，带有分发点的设备也会请求一定的剩余磁盘空间，这些空间与要安装的安装包大小相当。

如果管理服务器上有一个或多个更新（补丁）安装和漏洞修复任务实例，带有分发点的设备也会请求一定的剩余磁盘空间，相当于两倍的补丁总大小。

如果在分发点直接从卡巴斯基更新服务器接收数据库更新和应用程序软件模块的地方使用此方案，则分发点必须连接到互联网。

计算分发点的数量和配置

网络包含越多的客户端设备，就需要越多的分发点。我们建议您禁用分发点的自动分配。当分发点的自动分配被启用时，如果客户端设备数量很大，管理服务器就分配分发点并定义其配置。

使用单独分配的分发点

如果您计划使用特定设备作为分发点(就是，单独分配的服务器)，您可以不使用分发点的自动分配。此种情况下，确保您要分配为分发点的设备具有足够的剩余磁盘空间卷，不定期关闭，且禁用了睡眠模式。

网络中基于网络设备数量被专门分配的包含单一网段的分发点的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	可接受：(N/10,000 + 1)，建议：(N/5000 + 2)，N 是网络设备数量

网络中基于网络设备数量被专门分配的包含多个网段的分发点的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–100	1
大于 100	可接受：(N/10,000 + 1)，建议：(N/5,000 + 2)，N 是网络设备数量

使用标准客户端设备（工作站）作为分发点

如果您计划使用标准客户端设备（就是，工作站）作为分发点，我们建议您按照所示分配分发点（参见下表），以便避免通信渠道和管理服务器过载。

网络中基于网络设备数量作为分发点工作的包含单一网段的工作站的数量

网段中的客户端设备的数量	分发点数量
少于 300	0（不分配分发点）
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

网络中基于网络设备数量作为分发点工作的包含多个网段的工作站的数量

每个网段中的客户端设备的数量	分发点数量
少于 10	0（不分配分发点）
10–30	1
31–300	2
大于 300	(N/300 + 1)，N 是网络设备数量；至少有三台分发点

如果分发点被关闭(或由于某些原因不可用)，其范围内的受管理设备可以访问管理服务器以更新。

连接网关数量计算

如果您计划使用连接网关，我们建议您为该功能指定特别的设备。

一个连接网关可以覆盖最多 10,000 台受管理设备，包括移动设备。

任务和策略事件信息的记录

该部分提供了管理服务器数据库中的事件存储计算，并提供如何最小化事件数量的建议，从而降低管理服务器负载。

默认情况下，每个任务和策略的属性可以用于存储所有任务执行和策略强制执行的相关事件。

然而，如果任务运行过于频繁（例如，每周多于一次）且在大量设备间（例如，多于 10,000 台），事件数量可能过大且事件可能溢出数据库。此种情况下，建议选择任务设置的两个选项中的一个：

- **保存任务进度相关事件**。此种情况下，数据库仅从运行任务的每个设备接收任务启动、进程和完成信息（成功、带有警告或错误）。
- **仅保存任务执行结果**。此种情况下，数据库仅从运行任务的每个设备接收任务完成信息（成功、带有警告或错误）。

如果策略为大数量设备定义（例如，多于 10,000 台），事件数量可能很大且事件可能溢出数据库。此种情况下，建议在策略设置中仅选择最关键的事件并启用它们的记录。建议您禁用所有其他事件的记录。

为此，您将降低数据库中的事件数量，提高与数据库中事件表分析相关的场景的执行速度，并降低严重事件被大数量事件覆盖的风险。

您也可以降低任务或策略相关事件的存储期限。任务相关事件和策略相关事件的默认期限分别是 7 天和 30 天。当更改事件存储期限时，请考虑您的组织采用的工作程序以及系统管理员用以分析每个事件的时间。

建议在以下情况修改事件存储设置：

- 有关组任务中间状态变化的事件和有关应用策略的事件在 Kaspersky Security Center 数据库的所有事件中占据很高比例。
- 卡巴斯基事件日志开始显示事件超过存储限制时的自动删除。

基于每天来自每个设备的事件数量不超过 20 的假设来选择事件记录选项。如果必要，您可以稍微增加该限制，但仅是在您网络中的设备数量相对小时（少于 10,000 台）。

特别考虑和特定任务的优化设置

特定任务受制于基于网络设备数量的特别考虑。该部分提供了此类任务设置的优化配置建议。

设备发现、数据备份任务、管理服务器维护任务和更新 Kaspersky Endpoint Security 的组任务是 Kaspersky Security Center 的基本功能部分。

设备发现频率

不建议增加设备发现的默认频率，因为这可以增加域控制器负载。相反，建议使用您组织需要的最小频率计划轮询。计算最优计划的建议提供在下表。

设备发现计划

网络设备数量	建议的设备发现频率
少于 10,000	默认频率或更低
10,000 或更多	每天一次或更低

管理服务器数据备份任务和管理服务器维护任务

当以下任务运行时管理服务器停止工作：

- 备份管理服务器数据
- 管理服务器维护

当这些任务运行时，数据库无法接收任何数据。

您可能必须重新计划这些任务以便它们和其他管理服务器任务不同时执行。

更新 Kaspersky Endpoint Security 的组任务

如果管理服务器作为更新源，Kaspersky Endpoint Security 10 和后续版本的组更新任务的建议计划选项是“**当新更新下载至存储库时**”，其中“**使用任务启动自动随机延迟**”复选框被选中。

如果从 Kaspersky 服务器下载更新到存储库的本地任务已在每个分发点上创建，时段性计划将被建议给 Kaspersky Endpoint Security 组更新任务。随机时段值必须是一小时。

清查任务

您可以在获取可执行文件相关信息的同时减少数据库的负载。为此，我们建议您在安装了一组标准软件的参考设备上运行 Kaspersky Endpoint Security 清查任务。

管理服务器从单个设备接收的可执行文件数量不能超过 150,000。当 Kaspersky Security Center 达到了该限制，它无法接收任何新文件。

通常，常规客户端设备上的文件数量不超过 60,000。文件服务器上的可执行文件数量可能更大甚至超过 150,000 阈值。

测试度量显示清查任务在安装了 Kaspersky Endpoint Security 11 而未安装第三方应用程序的运行 Windows 7 操作系统的设备上具有以下结果。

- 清空 **DLL 模块清查**和**脚本文件清查**复选框：大约 3000 个文件。
- 选中 **DLL 模块清查**和**脚本文件清查**复选框：10,000 到 20,000 个文件，根据安装的操作系统服务包数量。
- 仅选中**脚本文件清查**复选框：大概 10,000 个文件。

管理服务器和受保护设备间的网络负载详情

该部分提供了一定条件下的网络流量测试度量结果。当您计划网络基础架构和您组织网络中（或管理服务器和其他要保护其设备的组织间）吞吐量时，可以参考该信息。知道了网络吞吐量，您也可以估算不同数据传输操作将花费的时间。

不同方案下的流量消耗

下表显示不同方案下管理服务器和受管理设备之间流量度量测试的结果。

默认下，设备每 15 分钟或更长间隔与管理服务器同步一次。然而，如果您在管理服务器上修改策略或任务的设置，该策略（或任务）所适用的设备会提前进行同步，从而将新设置传输到设备上。

管理服务器和受管理设备间的流量率

方案	从管理服务器到每个受管理设备的流量	从每个受管理设备到管理服务器的流量
安装带有更新数据库的 Kaspersky Endpoint Security 11.7 for Windows	390 MB	3.3 MB
网络代理安装	75 MB	397 KB
网络代理和 Kaspersky Endpoint Security 11.7 for Windows 同时安装	459 MB	3.6 MB
反病毒数据库初始更新，不更新软件包中的数据库（如果参与卡巴斯基安全网络被禁用）	113 MB	1.8 MB
反病毒数据库每日更新（如果参与卡巴斯基安全网络被启用）	22 MB	373 MB

方案	从管理服务器到每个受管理设备的流量	从每个受管理设备到管理服务器的流量
设备数据库更新之前的初始化同步（策略和任务传输）	382 KB	446 KB
在设备上更新数据库之后初始同步	20 KB	157 KB
与管理服务器的同步（根据计划）	18 KB	23 KB
当组策略中单个设备被更改时同步（设置更改时立即）	19 KB	20 KB
当组任务中单个设备被更改时同步（设置更改时立即）	14 KB	11 KB
强制同步	110 KB	109 KB
检测到的病毒事件（1 个病毒）	44 KB	50 KB
检测到病毒事件（10 个病毒）	58 KB	77 KB
启用应用程序注册表列表后的一次性流量	最多 10 KB	最多 12 KB
启用应用程序注册表列表后的每日流量	最多 840 KB	最多 1 MB

24 小时平均流量使用

管理服务器和受管理设备之间的 24 小时平均流量使用情况如下所示：

- 从管理服务器到受管理设备的流量为 840 KB。
- 从受管理设备到管理服务器的流量为 1 MB。

流量测量在以下条件下进行：

- 受管理设备已安装网络代理和 Kaspersky Endpoint Security 11.6 for Windows。
- 设备未被分配为分发点。
- 漏洞和补丁管理未启用。
- 与管理服务器的同步频率是 15 分钟。

联系技术支持

该部分描述如何获取技术支持和其可用条款。

如果获得技术支持

如果您在 Kaspersky Security Center 文档或任何 Kaspersky Security Center 信息源中都找不到问题的解决方案，请联系 Kaspersky 技术支持。技术支持专家将回答关于安装和使用 Kaspersky Security Center 的所有问题。

卡巴斯基在 Kaspersky Security Center 的生命周期内提供支持（请参见应用程序支持生命周期页面）。与技术支持部门联系之前，请阅读支持规则。

您可以使用下列方式之一与技术支持联系：

- 通过访问技术支持网站
- 通过使用 Kaspersky CompanyAccount 门户发送请求到技术支持

通过 Kaspersky CompanyAccount 获得技术支持

Kaspersky CompanyAccount 是一个针对使用 卡巴斯基应用程序的公司的门户。Kaspersky CompanyAccount 门户设计用于方便用户与 Kaspersky 专家之间通过在线请求进行交互。您可以使用 Kaspersky CompanyAccount 跟踪您的在线请求状态并存储它们的历史。

您可在 Kaspersky CompanyAccount 上通过单个账户注册贵组织的所有员工。单个账户允许集中管理已注册员工向 Kaspersky 发送的电子请求，还允许通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户采用以下语言提供：

- 英语
- 西班牙语
- 意大利语
- 德语
- 波兰语
- 葡萄牙语
- 俄语
- 法语
- 日语

要了解有关 Kaspersky CompanyAccount 的更多信息，请访问技术支持网站。

获取管理服务器的转储文件

管理服务器的转储文件包含某一时间点的管理服务器进程的所有信息。管理服务器的转储文件存储在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps 文件夹中。只要 Kaspersky Security Center 正在使用，转储文件就会被存储，当删除时，转储文件会被永久删除。文件不会自动发送给卡巴斯基。

如果管理服务器崩溃，您可以联系卡巴斯基技术支持。技术支持专家可能会要求您将管理服务器的转储文件发送给卡巴斯基以供进一步分析。

转储文件可能包含个人数据。我们建议在将信息发送给卡巴斯基之前，保护信息免受未经授权的访问。

有关程序的信息源

Kaspersky 网站上的 Kaspersky Security Center 页面

在卡巴斯基网站的 Kaspersky Security Center 页面上，您可以查看有关应用程序、程序功能和特性的一般信息。

知识库中的 Kaspersky Security Center 页

*知识库*是 Kaspersky 技术支持网站的一部分。

在知识库的 Kaspersky Security Center 页面上，您可以阅读文章，这些文章提供了有用的信息、建议以及有关如何购买、安装和使用程序的常见问题解答。

知识库中的文章可能提供关于 Kaspersky Security Center 和 Kaspersky 应用程序的问题的答案。知识库中的文章也可能包含技术支持新闻。

在社区讨论 Kaspersky 应用程序

如果您的问题不需要立即回答，您可以在我们的论坛中与卡巴斯基专家和其他用户一起进行讨论。

您可以在论坛上查看讨论主题、发表评论、创建新的讨论主题。

> 需要互联网连接以访问网站资源。

如果您无法找到问题的解决方案，请联系技术支持。

词汇表

Amazon EC2 实例

使用 Amazon Web Service 基于 AMI 镜像创建的虚拟机。

Amazon 系统映像 (AMI)

模板包含运行虚拟机必要的软件配置。多个实例可以基于单个 AMI 创建。

AWS Application Program Interface (AWS API)

AWS 平台的用于 Kaspersky Security Center 的应用程序编程接口。特别地，AWS API 工具用于云段轮询和安装网络代理到实例。

AWS IAM 访问密钥

包含密钥 ID("AKIAIOSFODNN7EXAMPLE"样式)和 secret key ("wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"样式)的组合。这对属于 IAM 用户并用于获取对 AWS 服务的访问。

AWS 管理控制台

查看和管理 AWS 资源的 Web 界面。AWS 管理控制台在 https://aws.amazon.com/cn/console/ 可用。

Cloud Discovery

Cloud Discovery 是云访问安全代理 (CASB) 解决方案的组件，可保护组织的云基础设施。Cloud Discovery 可管理用户对云服务的访问。云服务包括 Microsoft Teams、Salesforce、Microsoft Office 365 等。云服务分为几类，例如*数据交换*、*通信软件*、*电子邮件*。

HTTPS

在浏览器和 Web 服务器之间使用加密传送数据的安全协议。HTTPS 用于访问受限制的信息，如企业或财务数据。

IAM 用户

AWS 服务用户。IAM 用户可能具有执行云段轮询的权限。

IAM 角色

请求 AWS 服务的权限设置。IAM 角色不关联于特定用户或组；它们提供不带 AWS IAM 访问密钥的访问权限。您可以分配 IAM 角色到 IAM 用户、EC2 实例和 AWS 应用程序或服务。

iOS MDM 服务器

安装在客户端设备上的 Kaspersky Security Center 的一个组件，允许通过 Apple Push Notifications （APNs） 将 iOS 移动设备连接至管理服务器并管理 iOS 移动设备。

iOS MDM 设备

通过 iOS MDM 协议连接到 iOS MDM 服务器的移动设备。可通过 iOS MDM 协议连接和管理运行 iOS 操作系统的设备。

iOS MDM 配置文件

用于将 iOS 移动设备连接至管理服务器的设置集合。用户将 iOS MDM 配置文件安装至移动设备，此后，该移动设备将连接至管理服务器。

JavaScript

一种对网页性能进行扩展的编程语言。使用 JavaScript 创建的网页无需使用来自网络服务器的新数据刷新网页即可执行功能（例如，更改界面元素的视图或打开附加窗口）。要查看使用 JavaScript 创建的页面，请在您的浏览器的配置中启用 JavaScript 支持。

Kaspersky Security Center System Health Validator (SHV)

在 Kaspersky Security Center 和 Microsoft NAP 并行运行时，用于检查操作系统运行能力的 Kaspersky Security Center 的一个组件。

Kaspersky Security Center Web Server

Kaspersky Security Center 组件，与管理服务器一同安装。Web 服务器用于通过网络传输独立安装包、iOS MDM 配置文件、以及共享文件夹的文件。

Kaspersky Security Center 操作员

对通过 Kaspersky Security Center 管理的保护系统的状态和操作进行监视的用户。

Kaspersky Security Center 的升级

在已安装该应用程序较早版本的设备上安装新版本 Kaspersky Security Center 的过程。

Kaspersky Security Center 管理员

通过 Kaspersky Security Center 远程集中管理系统来管理应用程序操作的人。

Kaspersky 更新服务器

Kaspersky 程序可以从 Kaspersky 的 HTTP(S) 服务器下载数据库和应用程序模块更新。

KES 设备

连接到 Kaspersky Security Center 管理服务器和通过 Kaspersky Endpoint Security for Android 进行管理的移动设备。

MITM 攻击

中间人。对组织的 IT 基础设施的攻击，其中黑客劫持两个接入点之间的通信链接、中继该链接，并在必要时修改这些接入点之间的连接。

Provisioning 配置文件

应用程序在 iOS 移动设备上运行的设置的集合。Provisioning 配置文件包含有关授权许可的信息，它连接至特定的应用程序。

SSL

互联网和本地网上的使用的数据加密协议。Secure Sockets Layer（SSL）协议用在网络应用程序中，以便在客户端和服务器之间创建安全的连接。

UEFI 保护设备

包含在 BIOS 级别集成了适用于 UEFI 的卡巴斯基解决方案或应用程序的设备。整合的保护从系统启动时开始确保设备安全，未整合软件的设备仅在安全应用程序启动后开始保护工作。

Windows Server 更新服务 （WSUS）

用于将 Microsoft 应用程序的更新发布到组织网络内用户的计算机上的一种应用程序。

不兼容应用程序

第三方开发的反病毒应用程序，或不支持通过 Kaspersky Security Center 管理的 Kaspersky 应用程序。

事件严重级别

在 Kaspersky 程序操作过程中遇到的事件的属性。存在以下严重级别：

- 严重事件
- 功能失败
- 警告
- 信息

根据事件发生时的情况，相同类型的事件可能具有不同的严重级别。

事件存储库

管理服务器数据库的一部分，用于存储发生在 Kaspersky Security Center 中的事件信息。

云环境

基于云平台的组合到网络的虚拟机和其他虚拟资源。

任务

由 Kaspersky 应用程序执行的功能作为任务来实施，例如：实时文件保护、计算机全盘扫描、数据库更新。

任务设置

对于每个任务类型的特别应用程序设置。

保护状态

当前保护状态，反映了计算机安全级别。

共享证书

证书用于识别用户的移动设备。

内部用户

内部用户的账户可用于操作虚拟管理服务器。Kaspersky Security Center 授权应用程序的内部用户拥有真实用户的所有权限。

只能在 Kaspersky Security Center 内创建和使用内部用户账户。系统不会将内部用户的任何数据传送到操作系统。Kaspersky Security Center 将验证内部用户。

分发点

安装了网络代理并用于更新发布、远程安装应用程序、获取管理组（广播域）中计算机信息的计算机。分发点用来降低发布更新时管理服务器的负载并优化网络流量。分发点可以被自动指定、被管理服务器指定或被管理员手动指定。分发点先前叫做更新代理。

卡巴斯基安全网络 （KSN）

云服务基础架构，提供对卡巴斯基数据库的访问权限，其中包含有关文件、网络资源和软件信誉且持续更新的信息。卡巴斯基安全网络确保在遇到新型威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的性能并降低误报的可能性。

卡巴斯基私有安全网络 (KPSN)

“卡巴斯基私有安全网络”允许安装了 Kaspersky 应用程序的设备的用户访问“卡巴斯基安全网络”信誉数据库和其他统计数据，而不从他们的设备发送数据到“卡巴斯基安全网络”。卡巴斯基私有安全网络用于由于以下原因无法参与卡巴斯基安全网络的企业客户：

- 设备未连接到互联网。
- 传输任何数据到国家以外或企业局域网以外被法律或企业安全策略禁止。

反病毒保护服务提供商

提供给客户端组织基于 Kaspersky 解决方案的反病毒保护服务的组织。

反病毒数据库

包含截至反病毒数据库发布时 Kaspersky 已知的计算机安全威胁信息。反病毒数据库中的条目使得恶意代码在被扫描对象中被检测。反病毒数据库由 Kaspersky 专家创建，每小时更新一次。

受管理设备

包括在管理组中的企业网络设备。

可用更新

Kaspersky 应用程序模块的更新集，包含特定时间段积累的关键更新和应用程序架构更改。

备份文件夹

用于存储使用备份实用工具创建的管理服务器数据副本的专用文件夹。

安装包

使用 Kaspersky Security Center 远程管理系统创建的一组用于远程安装 Kaspersky 程序的文件。安装包包含安装应用程序所需的一系列设置，这些设置在安装后立即运行。应用程序默认设置。使用包含在应用程序分发工具中的扩展名为 .kpd 和 .kud 的文件创建安装包。

客户端管理员

客户组织中负责监控反病毒保护状态的员工。

密钥文件

带有.key扩展名的文件，可以用来以试用或商用授权许可使用 Kaspersky 应用程序。

广播域

网络的一个逻辑区域，在这里所有节点可以使用广播通道在 OSI 层（Open Systems Interconnection Basic Reference Model）交换数据。

应用程序商店

Kaspersky Security Center 组件。应用程序商店用于安装应用程序到用户 Android 设备。应用程序商店允许您发布应用程序 APK 文件和链接到 Google Play。

强制安装

远程安装 Kaspersky 应用程序的方法，允许您安装软件到指定客户端设备。为了成功完成强制安装，用于执行该任务的账户必须具有足够的权限，以便在客户端设备上远程启动应用程序。该方法建议用于安装应用程序到运行 Microsoft Windows 操作系统并支持该功能的设备。

强化指南

一组配置 Kaspersky Security Center 及其组件的建议和功能，旨在降低其危害的风险。

归属管理服务器

归属管理服务器是网络代理安装过程中指定的管理服务器。归属管理服务器可在网络代理连接配置文件中被使用。

手动安装

从分发包安装安全应用程序到企业网络中的设备。手动安装需要管理员或其他 IT 专家的参与。通常情况下，如果远程安装发生错误，则执行手动安装。

授权的应用程序组

由管理员根据标准设置（例如，根据供应商）创建的应用程序组，系统将维护已安装至客户端设备的应用程序的统计信息。

授权许可期限

可以访问程序功能并且有权使用附加服务的时间段。您可以使用的服务取决于授权许可的类型。

更新

替换或者添加从 Kaspersky 更新服务器接收到的新文件（数据库或应用程序模块）的过程。

服务提供商管理员

反病毒保护服务提供商的员工。该管理员为基于 Kaspersky 反病毒产品的反病毒保护系统执行安装和维护工作，并且向客户提供技术支持。

本地任务

在单台客户端计算机上定义和运行的任务。

本地安装

将安全应用程序安装在企业网络的设备上，手动安装始于安全应用程序分发包或者预先下载到设备的已发布安装包。

活动授权许可

应用程序当前使用的密钥。

漏洞

操作系统或应用程序存在的缺陷，恶意软件开发者会利用这种缺陷入侵操作系统或应用程序并破坏其完整性。操作系统中的大量漏洞会使操作系统不安全，因为能够入侵操作系统的病毒会导致操作系统或其上所安装的应用程序发生运行故障。

特定设备的任务

从任意管理组分配给一组客户端设备并且在那些设备上执行的任务。

病毒活动性阀值

在特定时间内指定类型的事件被允许发生的最大数量，超过该数量时就被解读为增高的病毒活动并看做是一种病毒爆发威胁。在病毒爆发期间该功能很重要，因为它能够提醒管理员及时响应病毒攻击威胁。

病毒爆发

使设备感染病毒的一系列蓄意尝试。

直接应用程序管理

通过本地界面进行的应用程序管理。

移动设备服务器

Kaspersky Security Center 的一个组件，可以提供对移动设备的访问，允许您通过管理控制台管理这些移动设备。

程序设置

对所有任务类型通用并且掌管应用程序总体操作的应用程序设置，例如：应用程序性能设置、报告设置和备份设置。

策略

策略决定应用程序设置并管理应用程序在管理组中计算机上的配置。必须为每个应用程序都创建单独的策略。您可以为安装在每个管理组中计算机上的应用程序创建多个策略，但是对于管理组中的每个应用程序，一次只能应用一个策略。

管理员工作站

安装了管理控制台或用于打开 Kaspersky Security Center Web Console 的设备。该组件提供了 Kaspersky Security Center 管理界面。

管理员工作站用于配置和管理 Kaspersky Security Center 的服务器部分。使用管理员工作站，管理员基于 Kaspersky 应用程序为企业局域网创建和管理一个集中的反病毒保护系统。

管理员权限

在 Exchange 组织内管理 Exchange 对象所需的用户权限。

管理控制台

基于 Windows 的 Kaspersky Security Center 的组件（也称为基于 MMC 的管理控制台）。此组件提供管理服务器和网络代理的管理服务用户界面。

管理插件

一个提供应用程序管理接口的专用组件，以便通过管理控制台管理该应用程序。每个应用程序都有自己的插件。它包括在可以使用 Kaspersky Security Center 管理的所有 Kaspersky 程序中。

管理服务器

Kaspersky Security Center 的一个组件，可集中存储企业网络内安装的所有 Kaspersky 应用程序的信息。它也可用于管理这些应用程序。

管理服务器客户端（客户端设备）

安装网络代理和运行受管理的 Kaspersky 程序的设备、服务器或工作站。

管理服务器数据备份

使用备份实用工具复制管理服务器数据，以便进行备份和后续的恢复。该实用工具可以保存：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）
- 有关管理组和客户端设备的结构的配置详情
- 用于远程安装应用程序的安装文件存储库（文件夹内容：软件包、卸载更新）
- 管理服务器证书

管理服务器证书

管理服务器用于以下目的的证书：

- 连接到基于 MMC 的管理控制台或 Kaspersky Security Center Web Console 时的管理服务器身份验证
- 受管理设备上管理服务器和网络代理之间的安全交互
- 将主管理服务器连接到从属管理服务器时的管理服务器身份验证

安装管理服务器时会自动创建证书，然后存储在管理服务器上。

管理组

以功能和安装的 Kaspersky 应用程序分组的设备集。设备被分组成一个单一实体以便管理。组可以包含其他组。组策略和组任务可以为组中每个安装的应用程序创建。

组任务

为某个管理组定义并在该管理组中所有客户端设备上执行的任务。

网络代理

Kaspersky Security Center 的一个组件，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。该组件是公司内所有 Microsoft® Windows® 应用程序的通用组件。对于为 Unix 和 macOS 之类的平台开发的 Kaspersky 产品，分别有不同版本的网络代理。

网络位置识别 (NLA)

帮助操作系统识别当前网络的 Windows 服务。NLA 可检测网络变化并调整设备的安全配置。

网络保护状态

当前保护状态，它定义了企业网络设备的安全。网络保护状态包括已安装的安全应用程序、授权许可密钥的使用状态及检测到的威胁的数量和类型等因素。

网络反病毒保护

一组能够降低病毒和垃圾邮件感染组织网络的可能性并防止网络攻击、钓鱼和其他威胁的技术和组织措施。当您使用安全应用程序和服务和应用企业数据安全策略时，网络安全被增加。

虚拟管理服务器

Kaspersky Security Center 组件，用于管理客户组织网络的保护系统。

虚拟管理服务器是从属管理服务器的特例，与物理管理服务器相比，具有以下限制：

- 只能在主管理服务器上创建虚拟管理服务器。
- 虚拟管理服务器在其操作中使用主管理服务器数据库。虚拟管理服务器不支持数据备份和还原任务以及更新扫描和下载任务。
- 虚拟服务器不支持从属管理服务器（包括虚拟服务器）的创建。

补丁重要级别

补丁属性。有五个 Microsoft 补丁和第三方补丁的重要级别：

- 严重
- 高
- 中
- 低
- 未知

第三方补丁或 Microsoft 补丁的重要级别由补丁需要修复的漏洞的最不利的严重级别决定。

设备所有者

设备所有者就是管理员需要在设备上运行操作时可以联系的用户。

身份和访问管理(IAM)

启用了用户到其他 AWS 服务和资源的访问管理的 AWS 服务。

身份验证代理

允许您完成访问已加密硬盘驱动器的身份验证和在可启动磁盘驱动器加密后加载操作系统的界面。

轻量级 Nagent（LWNGT）

用于与移动设备上的 Kaspersky Endpoint Security 进行交互的协议。LWNGT（又称移动协议）起到网络代理的作用，而无需在移动设备上实际安装网络代理。

还原

将对象从隔离区或备份区恢复至其在隔离、清除或删除前所在的原始位置或移动至用户定义的文件夹。

还原管理服务器数据

使用备份实用程序从备份区中保存的信息还原管理服务器数据。该实用程序可以还原：

- 管理服务器数据库（策略、任务、应用程序设置、管理服务器上保存的事件）
- 有关管理组和客户端设备的结构的配置详情
- 用于远程安装应用程序的安装文件存储库（文件夹内容：软件包、卸载更新）
- 管理服务器证书

远程安装

使用 Kaspersky Security Center 提供的服务安装卡巴斯基实验室程序。

连接网关

*连接网关*是以特殊模式运行的网络代理。连接网关接受来自其他网络代理的连接，并通过其自身与服务器的连接将它们与管理服务器建立隧道连接。与普通的网络代理不同，连接网关等待来自管理服务器的连接，而不是建立与管理服务器的连接。

配置文件

包含设置集合和 iOS MDM 移动设备限制的策略。

隔离区域 （DMZ）

隔离区是一段本地网络，其包含响应来自全局网络的请求的服务器。为确保组织的本地网络的安全性，对隔离区中的 LAN 的访问受防火墙的保护。

集中式应用程序管理

使用 Kaspersky Security Center 中提供的管理服务进行远程应用程序管理。

额外（或备用）授权许可密钥

证明程序的使用权限、但是目前尚未使用的密钥。

有关第三方代码的信息

有关第三方代码的信息包含在 legal_notices.txt 文件内，在应用程序安装文件夹内。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

Adobe、 Acrobat、 Flash、 Shockwave 和 PostScript 是 Adobe 在美国和/或其他国家/地区的商标或注册商标。

AMD 和 AMD64 是 Advanced Micro Devices, Inc. 的商标或注册商标。

Amazon、 Amazon Web Services、 AWS、 Amazon EC2、 AWS Marketplace 是 Amazon.com, Inc. 或其附属公司的商标。

Apache是Apache软件基金会在美国和/或其他国家的注册商标或商标。

Apple、AirPlay、AirDrop、AirPrint、App Store、Apple Configurator、AppleScript、FaceTime、FileVault、iBook、iBooks、iCloud、iPad、iPhone、iTunes、Leopard、macOS、Mac、Mac OS、OS X、Safari、Snow Leopard、 Tiger、 QuickTime 和 Touch ID 是 Apple Inc. 的商标。

Arm 是 Arm Limited（或其子公司）在美国和/或其他地方的注册商标。

蓝牙词语，标志和标识都为 Bluetooth SIG, Inc. 所有。

Ubuntu、LTS 是 Canonical Ltd. 的注册商标。

Cisco Systems、Cisco、Cisco Jabber、IOS 是 Cisco Systems, Inc. 和/或其附属公司在美国和某些其他国家/地区的注册商标。

Citrix、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。

Corel 是 Corel Corporation 和/或其附属公司在美国和其他特定国家的注册商标。

Cloudflare、Cloudflare 徽标和 Cloudflare Workers 是 Cloudflare, Inc. 在美国和其他司法管辖区的商标和/或注册商标。

Dropbox 是 Dropbox, Inc. 的商标。

Radmin 是 Famatech 的注册商标。

Firebird 是 Firebird Foundation 的注册商标。

Foxit 是 Foxit Corporation 的注册商标。

FreeBSD 是 FreeBSD foundation 的注册商标。

Google、Android、Chrome、Chromium、Dalvik、Firebase、Google Chrome、Google Earth、Google Play、Google Maps、Hangouts、Google Public DNS 和 YouTube 是 Google, LLC. 的商标。

EulerOS、FusionCompute、FusionSphere 是华为技术有限公司的商标。

Intel、Core、Xeon 是 Intel Corporation 或其子公司的商标。

IBM、QRadar 是 International Business Machines Corporation 在全球众多司法管辖区的注册商标。

Node.js 是 Joyent, Inc. 的商标。

Linux 是 Linus Torvalds 在美国和其他国家的注册商标。

Logitech 是 Logitech 在美国和/或其他国家/地区的注册商标或商标。

Microsoft、Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、Office 365、PowerShell、PowerPoint、SharePoint、SQL Server、OneNote、Outlook、Skype、Tahoma 、Visio、Win32、Windows、Windows PowerShell、Windows Media、Windows Mobile、Windows Server、Windows Phone、Windows Vista 和 Windows Azure 是 Microsoft 公司集团的商标。

CVE 是 The MITRE Corporation 的注册商标。

Mozilla、Firefox、Thunderbird 是 Mozilla Foundation 在美国和其他国家/地区的商标。

Novell 是 Novell Enterprises Inc. 在美国和其他国家/地区的注册商标。

NetWare 是 Novell Inc. 在美国和其他国家/地区的注册商标。

OpenVPN 是 OpenVPN, Inc. 的注册商标。

OpenSSL 是 OpenSSL 软件基金会拥有的商标。

Oracle、Java、JavaScript 和 TouchDown 是 Oracle 和/或其附属公司的注册商标。

Parallels、Parallels 徽标和 Coherence 是 Parallels International GmbH 的商标或注册商标。

Chef 是 Progress Software Corporation 和/或其子公司或附属公司之一在美国和/或其他国家/地区的商标或注册商标。

Puppet 是 Puppet, Inc. 的商标或注册商标。

Python 是 Python Software Foundation 的商标或注册商标。

Red Hat、Fedora 和 Red Hat Enterprise Linux 是 Red Hat Inc. 或其子公司在美国和其他国家/地区的商标或注册商标。

Ansible 是 Red Hat, Inc. 在美国和其他国家/地区的注册商标。

CentOS 是 Red Hat, Inc. 或其附属公司在美国和其他国家/地区的注册商标。

BlackBerry 是 Research In Motion Limited 所有的商标，在美国和/或其他国家注册。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商标。

SAMSUNG 是 SAMSUNG 在美国或其他国家/地区的商标。

Debian 是 Public Interest, Inc. 公司的软件的注册商标。

Splunk、SPL 是 Splunk Inc. 在美国和其他国家/地区的商标和注册商标。

SUSE 是 SUSE LLC 在美国和其他国家/地区的注册商标。

Symbian 是 Symbian Foundation Ltd. 所拥有的商标。

OpenAPI 是 The Linux Foundation 的商标。

UNIX 是在美国和其他国家的注册商标，通过 X/Open Company Limited 授权。

Zabbix 是 Zabbix SIA 的注册商标。

已知问题

Kaspersky Security Center Web Console 具有许多对于应用程序运行并不重要的限制：

- 如果在 Microsoft Windows XP 上安装了网络代理，则无法获取有关受管理应用程序组件的信息。
- 仅当您通过输入激活码将 EDR Optimum 的授权许可密钥添加到管理服务器存储库时，控制台才会在主菜单的**警报**部分中显示**监控和报告**子部分。
- 为了确保加密强度，管理服务器证书必须使用 SHA-2 进行签名，且密钥长度至少为 2048。如果需要重新颁发证书，请参阅Kaspersky Security Center 知识库。
- 如果您在 Kaspersky Security Center 15.1 Web Console 中使用**每 N 天**和**按星期几**计划设置创建任务，然后在早期版本的 Kaspersky Security Center Web Console 或 Kaspersky Security Center 管理控制台中打开该任务（例如，当该任务也应用于基于 Linux 和基于 Windows 的辅助管理服务器时），计划设置可能会显示不正确，或者可能会出现错误。
- 当您在 Kaspersky Security Center Web Console 中配置导出到 SIEM 系统并且选择 UDP 协议时，单击**检查连接**按钮会返回错误，因为 UDP 不会建立连接，资料传输无法得到保证。
- 当您运行任务从基于 Arm 架构并运行 Astra Linux Special Edition RUSB.10015-01（操作更新 1.7）的设备中删除网络代理时，网络代理将被成功删除，但任务列表中当前进度的任务状态会被冻结。
- 尽管 Exchange ActiveSync 不再受支持，Kaspersky Device Management for iOS策略的属性窗口仍然包含**EAS 设备设置**部分。
- 如果 Kaspersky Security Center 安装在设备名称中带有西里尔符号的设备上，并且在管理服务器上启用了 KSN 代理，则通过 HTTPS 连接到 KSN 会失败。
- 当您尝试更改已启用"**请求身份验证以检查修改用户账户的权限**选项的用户账户的属性，然后单击**取消**窗口中的**账户保护**时，会发生意外错误。
- 如果您更改设备上的时间或时区，则必须重新启动 Kaspersky Security Center Web Console 服务。
- 如果设备上使用了代理，并且设置了代理环境变量，则 Kaspersky Security Center Web Console 安装程序可能会冻结。
- 当您导入*将更新下载到分发点存储库*或*更新验证*任务时，**选择任务将被分配到的设备**选项将启用。这些任务不能分配给设备分类或特定设备。如果将*下载更新分配到分发点存储库*或将*更新验证*任务分配到特定设备，则任务将无法正确导入。
- 如果使用安装了网络代理版本 15 的 Linux 分发点执行 Active Directory 轮询，则只能轮询为其指定地址和用户凭据的 Active Directory 域。当前 Active Directory 域和 Active Directory 域林的轮询不可用。
- 运行 Windows 网络轮询后可能找不到客户端设备。
- 在"**添加从属管理服务器向导**中，如果您在将来的从属服务器上指定一个启用了两步验证进行身份验证的账户，向导将以错误结束。要解决此问题，请指定禁用两步验证的账户或从将来的从属服务器创建层级。
- 登录 Kaspersky Security Center Web Console 后，如果您使用域身份验证并指定要连接的虚拟管理服务器，然后注销，再尝试登录主管理服务器，则 Kaspersky Security Center Web Console 会连接到虚拟管理服务器。要连接到主管理服务器，请重新打开浏览器。
- 快速/完整 Windows 网络轮询返回空结果。

- 如果您安装带有身份和访问管理器的 Kaspersky Security Center Web Console，然后更改 Kaspersky Security Center Web Console 的管理服务器，身份和访问管理器不会获得有关新管理服务器的信息。
- 具有多个网络适配器的受管理设备会将未用于连接到管理服务器的网络适配器的 MAC 地址信息发送到管理服务器。
- 当选择 CEF 数据格式时，与 SIEM 的测试连接失败。
- NTLM 身份验证不适用于受保护用户组中的用户账户。