kaspersky

Kaspersky Security Center 云控制台

目录

Kaspersky 更新服务器
SSL
UEFI 保护设备
不兼容应用程序
事件严重级别
事件存储库
任务
任务设置
保护状态
分发点
卡巴斯基安全网络 （KSN）
卡巴斯基私有安全网络 (KPSN)
反病毒数据库
受管理设备
可用更新
安装包
密钥文件
工作区
广播域
应用程序标签
强制安装
归属管理服务器
授权许可期限
更新
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
程序设置
策略
策略配置文件
管理 Web 插件
管理服务器
管理组
组任务
网络代理
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
设备标签(T)
身份和访问管理(IAM)
身份验证代理

Kaspersky Security Center 云控制台帮助

	**新闻** 了解最新应用程序版本中的新增内容。		**配置网络保护** 通过根据组织要求配置卡巴斯基应用程序策略和任务来管理组织安全。
	**硬件和软件要求** 检查支持什么操作系统和应用程序版本。		**卡巴斯基应用程序：定期更新数据库和软件模块** 维持保护系统的可靠性。
	**Kaspersky Security Center 云控制台的授权许可** 了解有关 Kaspersky Security Center 云控制台在试用模式和商业模式下工作的详细信息。		**监控和报告** 查看您的基础架构、联网设备的保护状态和统计数据以管理组织的当前保护状态。您还可以使用报告。
	**初始配置** 开始使用您的工作区，根据您的需要配置 Kaspersky Security Center 云控制台。		**漏洞和补丁管理** 查找和修复第三方软件中的漏洞
	**迁移到 Kaspersky Security Center 云控制台** 将现有管理组和相关对象从本地 Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台。		**导出事件到 SIEM 系统** 配置使用 Syslog 协议将事件导出到 SIEM 系统。
	**发现网络设备** 发现您组织网络中的现有设备和新设备。		**使用云环境** 保护以下云环境中的虚拟机：Amazon Web Services™、Microsoft Azure™ 和 Google™ Cloud Platform。
	**分发点和/或连接网关的调整** 配置分发点。		**受管理服务提供商 (MSP) 快速入门指南** 如果您是 MSP 管理员，请了解如何使用 Kaspersky Security Center 云控制台。
	**卡巴斯基应用程序：集中部署** 部署 Kaspersky 应用程序。		

新闻

2024 年 4 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 一项新的 Cloud Discovery 功能。此功能允许您监控运行 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。

2024 年 2 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 现在，您可以从受管理设备列表中选择一个或多个设备，然后分配现有任务以在所选设备上运行。任务的当前设备范围将被替换为您选择的设备。
- 您现在可以将设备标签分配给多个设备或一次从多个设备中删除设备标签。从受管理设备列表中，选择设备，然后指定要分配给所选设备或从所选设备中删除的标签。
- 优化了受管理设备列表的外观和用户体验。添加了新列**标签**以及按设备标签筛选设备的功能。

2024 年 1 月更新

Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Security 12.4 for Windows。

2023 年 12 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 您现在可以检查与 SIEM 系统的连接。
- Kaspersky Security Center 云控制台现在支持通过基于 Linux 的分发点轮询 Microsoft Active Directory 域控制器和 Samba 域控制器。
- 远程诊断基于 Linux 的受管理设备。
- Kaspersky Security Center 云控制台现在支持以下 Kaspersky 应用程序：
  - Kaspersky Endpoint Security for Windows 版本 12.3 补丁 A
  - Kaspersky Endpoint Security 12.0 for Linux
  - Kaspersky Endpoint Security 12.0 for Mac
  - Kaspersky Endpoint Agent 3.16
  - Kaspersky Embedded Systems Security 3.3 for Windows
- 由于超出了应用程序功能的范围，两个界面部分被从主菜单中隐藏：

- 加密事件（**操作→数据加密和保护→加密事件**）
- IP 范围 (**发现和部署 → 发现 → IP 范围**)

- 我们更新了 Kaspersky Security Center 云控制台的数据处理协议文本。
- 许多旧的浏览器版本（早于版本 102 的 Firefox ESR）不再受支持。

2023 年 9 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Security Center 云控制台现在支持Kaspersky Embedded Systems Security 3.3 for Linux。
- Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Security 12.2 for Windows。
- 优化使用**资产(设备)**部分中的用户列表时的用户界面。

2023 年 6 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 发布了新的强化指南。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 云控制台和您的网络基础架构。
- Kaspersky Security Center 云控制台现在支持 Kaspersky Endpoint Security 11.3 for Mac。
- Kaspersky Security Center 云控制台现在支持 Kaspersky Endpoint Security 11.4 for Linux。
- 您可以使用 Kaspersky Security Center 云控制台将策略和任务导出到一个文件，然后将事件分类导入到 Kaspersky Security Center Windows 或 Kaspersky Security Center Linux。
- 现在，您可以使用分发点作为网络代理管理的设备的推送服务器。此功能可让您确保在受管理设备和管理服务器之间建立连续的连接。
- 重新组织了该部分的设置，以将Kaspersky Security Center 云控制台与其他卡巴斯基应用程序集成。
- 重组远程诊断部分的用户界面。
- 现在，您可以将设备分类中包含的所有设备的信息一次性保存到 CSV 文件中。
- 用户界面和可用性方面进行了许多改进，包括可选择表中所有项目。

2023 年 3 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Security Center 云控制台现在支持集群和服务器阵列作为受管理设备。如果卡巴斯基应用程序安装在群集节点上，网络代理会将此信息发送到管理服务器。在 Web Console 中，集群和服务器阵列与其他受管理设备分开列出。您可以将每个集群或服务器阵列作为一个单独的、不可分割的对象进行管理。
- Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Security 12.0 for Windows。

- 对于Web Console 中的报告，报告可以包含的最大条目数增加到 2500 个，对于导出到文件的报告，增加到 10,000 个。
- 现在，您可以选择是否要将状态为*正常*的受管理设备包含在保护状态报告中。
- 您现在可以使用以下授权许可之一激活 Kaspersky Security Center 云控制台 ，或将列出的授权许可的授权许可密钥添加到现有工作区：
  - Kaspersky Symphony Security
  - Kaspersky Symphony EDR
  - Kaspersky Symphony MDR
  - Kaspersky Symphony XDR
- Windows XP 网络代理特别版已发布。
- 更新后的 Linux 网络代理支持KSN 代理服务。除了基于 Windows 的分发点之外，您现在还可以使用基于 Linux 的分发点转发来自受管理设备的卡巴斯基安全网络 (KSN) 请求。该功能可让您重新分发和优化网络流量。
- 更新后的 Linux 网络代理支持应用程序注册表功能。网络代理可编写安装在 Linux 受管理设备上的应用程序列表，然后把该列表传给管理服务器。
- 您可以使用 Kaspersky Security Center 云控制台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。

2022 年 11 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Security Center 云控制台现在支持 Kaspersky Endpoint Security 11.3 for Linux。
- Kaspersky Security Center 云控制台现在支持Kaspersky Managed Detection and Response 2.1.18。
- Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Security for Mac 11.2 和 11.2.1 的更新版本，以支持 macOS 13。
- **介绍和教程**部分中的视频已更新。

2022 年 10 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 我们更新了 Kaspersky Security Center 云控制台的数据处理协议文本。
- Kaspersky Security Center 云控制台基础架构现在会通知您工作区没有有效的授权许可密钥，并且如果您不添加新的授权许可密钥，该工作区可能会被删除。
- Kaspersky Security Center 云控制台现在支持 Kaspersky Endpoint Security 11.11.0 for Windows。
- Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Detection and Response Optimum 2.3。
- Kaspersky Embedded Systems Security 3.2 for Windows 受支持。

2022 年 9 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 您现在可以为虚拟管理服务器分配专门的管理员。您可为管理员创建用户帐户，然后授予管理员对虚拟管理服务器的访问权限。指定的管理员只能访问选定的虚拟管理服务器，无法连接到主管理服务器或其他从属管理服务器（无论是物理还是虚拟服务器）。
- 优化了删除 Kaspersky Security Center 云控制台授权许可密钥时的用户体验。新机制可防止您意外删除上一个激活的授权许可密钥。
- 您现在可以使用基于 Linux 的分发点，通过*将更新下载到分发点的存储库*任务来下载卡巴斯基安全应用程序的反病毒数据库。
- Network Agent 现提供日语本地化版本。
- 在 Kaspersky Security Center 云控制台界面中，部分名称的全大写样式已更改为句子样式大写。

2022 年 8 月更新

新语言支持：Kaspersky Security Center 云控制台完全提供日语版本。

2022 年 7 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 新版受支持的卡巴斯基应用程序：
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Security for iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 for Windows
- 我们更新了 Kaspersky Security Center 云控制台的协议和数据处理协议的文本。
- 新语言支持：Kaspersky Security Center 云控制台基础架构现提供日语版本。Kaspersky Security Center 云控制台工作区中的日语支持即将推出。

2022 年 4 月更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Security Center 云控制台现在支持 Kaspersky Endpoint Security 11.9.0 for Windows。
- Kaspersky Security Center 云控制台现在支持日语本地化的 Kaspersky Embedded Systems Security。

2022 年 3 月 9 日更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 实施了与 Kaspersky Endpoint Detection and Response Expert 的集成。
- 实施了事件响应平台（IRP）。现在您可以通过 Kaspersky Security Center 云控制台管理安全事件。
- Kaspersky Security Center 云控制台现在接受Kaspersky Endpoint Detection and Response Expert 的授权许可密钥。授权许可的最小设备数量为 50 台。

2022 年 2 月 11 日更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Embedded Systems Security for Windows 的授权许可现在受支持。
- Kaspersky Endpoint Security 11.8.0 for Windows 受支持。
- 您可以使用日语分发包安装 Kaspersky Endpoint Security 11.8.0 for Windows。
- Kaspersky Endpoint Agent 3.12 受支持。

2021 年 12 月 10 日更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 与内部用户的合作得到改善：
  - 您现在可以在门户上添加新内部用户。
  - 应用程序现在可以防止您减少自己的权利。

2021 年 10 月 18 日更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Detection and Response Optimum 2.0。
- 您现在可以使用 Kaspersky Security Center 云控制台管理运行 Android 的移动设备。
- Kaspersky Marketplace 以新菜单部分的形式提供：您现在可以使用 Kaspersky Security Center 云控制台搜索卡巴斯基应用程序。
- 提供了新的菜单部分卡巴斯基公告。卡巴斯基公告通过提供与受管理设备上安装的卡巴斯基应用程序相关的信息来让您了解情况。Kaspersky Security Center 云控制台会定期更新该部分中的信息。
- 您现在可以通过 Kaspersky Security Center 云控制台管理在 Linux 操作系统下运行的从属管理服务器。

更新于 2021 年 9 月 7 日

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- 现在，您可以使用 Active Directory 联合身份验证服务 (ADFS)通过 Active Directory 帐户登录Kaspersky Security Center 云控制台，而无需创建新的用户帐户。
- Kaspersky Security Center 云控制台现在适用于以下云环境：Amazon Web Services、Microsoft Azure 和 Google Cloud。要保护云环境中的虚拟机（或实例），您需要Kaspersky Hybrid Cloud Security 授权许可之一。提供云环境配置向导。
- 现在，每个工作区的最大设备数量为25,000 台。
- Kaspersky Security Center 云控制台现提供与 SIEM 系统的集成。您可以使用 Syslog 协议将事件导出到 SIEM 系统。
- 您现在可以创建虚拟管理服务器。每个虚拟管理服务器都可以有自己的管理组、策略、任务、报告和事件的结构。您可以使用虚拟管理服务器来管理工作区中具有复杂工作流程的客户组织。但是，您无法将虚拟管理服务器从本地运行的 Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台。
- 您现在可以调整表中列的宽度，并对数据进行排序和搜索。
- 我们改进了 Kaspersky Business Hub 和 Kaspersky Security Center 云控制台的稳定性和可用性。

2020 年 10 月 27 日更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Security 11.6.0 for Windows、Kaspersky Endpoint Security 11.1 for Mac 补丁 A 和Kaspersky Endpoint Agent 3.10（作为Kaspersky Endpoint Detection and Response Optimum 的一部分）。
- 您现在可以使用下列授权许可：
  - Kaspersky Endpoint Detection and Response Optimum
  - 卡巴斯基网络安全解决方案高级版
  - 卡巴斯基全方位安全软件 for Business
- 实施了以下功能：
  - 漏洞和补丁管理
  - 加密管理
  - 应用程序控制
  - 自适应异常控制
  - RDP 会话，包括 Windows 桌面共享
- 导航菜单现在是垂直的，类似于基于 Microsoft 管理控制台的 Kaspersky Security Center 的界面。
- 现提供技术培训视频；他们将帮助您了解该应用程序的工作原理。

2020 年 6 月 30 日更新

Kaspersky Security Center 云控制台的本次更新包括以下新功能和改进：

- Kaspersky Security Center 云控制台现在支持Kaspersky Security 11 for Windows Server （从 2020 年 9 月开始）。
- Kaspersky Security Center 云控制台现在支持Kaspersky Endpoint Agent 3.12和 Kaspersky Endpoint Security 11.4.0 for Windows。
- 快速启动向导得到了改进：一些步骤被删除，步骤顺序进行了稍微更改，一些文本被进行了编辑以提高可用性。
- Kaspersky Security Center 云控制台现在提供意大利语版本。
- 您现在可以通过 Kaspersky Security Center 云控制台界面撤销任何受管理卡巴斯基应用程序的最终用户许可协议 (EULA)。您必须先卸载所选应用程序，再撤销其 EULA。
- 您现在可以删除工作区。如果您将工作区标记为删除，则默认情况下该工作区会在 7 天后被自动删除。不过，您可以强制删除工作区，以便立即将其删除。
- 实现了登录控制台两步验证。

Kaspersky Security Center 云控制台

本部分介绍 Kaspersky Security Center 云控制台的用途及其主要功能和组件。

Kaspersky Security Center 云控制台是由卡巴斯基托管和维护的应用程序。您不必在计算机或服务器上安装 Kaspersky Security Center 云控制台 。Kaspersky Security Center 云控制台允许管理员在公司网络中的设备上安装 Kaspersky 安全应用程序，远程运行扫描和更新任务，以及管理受管理应用程序的安全策略。管理员可以使用详细的控制板，其中提供公司设备状态的快照、详细的报告以及保护策略中的细化设置。

关于 Kaspersky Security Center 云控制台

Kaspersky Security Center 云控制台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。

Kaspersky Security Center 云控制台可让您执行以下操作：

- 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。
- 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。
- 创建虚拟管理服务器并将它们排列在层次结构中。
- 保护您的网络设备，包括工作站和服务器：
  - 管理基于 Kaspersky 应用程序构建的反恶意软件保护系统。
  - 使用检测和响应（EDR 和 MDR）功能（需要Kaspersky Endpoint Detection and Response 和/或 Kaspersky Managed Detection and Response的授权许可），包括：
    - 分析和调查事件
    - 通过创建威胁发展链图进行事件可视化
    - 手动接受或拒绝响应或设置自动接受所有响应
- 使用 Kaspersky Security Center 云控制台作为多租户应用程序。
- 远程管理客户端设备上安装的卡巴斯基应用程序。
- 将卡巴斯基应用程序的授权许可密钥集中部署到客户端设备。
- 为网络上的设备创建和管理安全策略。
- 创建和管理用户账户。
- 创建和管理用户角色 (RBAC)。
- 创建和管理安装在您的网络设备上的应用程序任务。
- 单独查看每个客户组织的安全系统状态报告。

您可以使用基于云的管理控制台来管理 Kaspersky Security Center 云控制台，该控制台可确保您的设备与管理服务器之间通过浏览器进行交互。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。当您使用您的浏览器连接至 Kaspersky Security Center 云控制台时，浏览器将与 Kaspersky Security Center 云控制台服务器建立连接。

管理服务器和连接的数据库管理系统 (DBMS) 部署在云环境中并作为服务提供给您。管理服务器和 DBMS 的维护作为服务的一部分提供。Kaspersky Security Center 云控制台的所有软件组件均保持最新。管理服务器和创建的对象（例如策略和任务）得到定期备份以确保其安全。

Kaspersky Security Center 云控制台是一个多语言应用程序。您可以在任意时刻更改界面语言，而不重新打开应用程序。

Kaspersky Security Center 云控制台的硬件和软件需求

管理控制台

对于客户端设备，Kaspersky Security Center 云控制台的使用仅需要一个浏览器。

> 您只能使用单个浏览器窗口或选项卡来使用 Kaspersky Security Center 云控制台。

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

浏览器：

- Google Chrome 100.0.4896.88 或更高版本（正式版本）
- Microsoft Edge 100 或更高版本
- Safari 15 on macOS
- “Yandex”浏览器 23.5.0.2271
- Mozilla Firefox 扩展支持版本 102.0 或更高版本

网络代理

最小硬件条件：

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

漏洞和补丁管理的最低硬件要求：

- 运行频率为 1.4 GHz 或更高的 CPU。需要 64 位操作系统。
- RAM：8 GB。

- 可用磁盘空间：1 GB。

网络代理支持的操作系统

操作系统。Microsoft Windows	Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32 位 Microsoft Windows Embedded 7 Standard with Service Pack 1 32 位/64 位 Microsoft Windows Embedded 8.1 工业专业版 32 位/64 位 Microsoft Windows 10 Enterprise 2015 LTSB 32 位 / 64 位 Microsoft Windows 10 Enterprise 2016 LTSB 32 位 / 64 位 Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 位 / 64 位 Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 位 / 64 位 Microsoft Windows 10 Enterprise 2019 LTSC 32 位/64 位 Microsoft Windows 10 IoT Enterprise 版 1703 32 位/64 位 Microsoft Windows 10 IoT Enterprise 版 1709 32 位/64 位 Microsoft Windows 10 IoT Enterprise 版 1803 32 位/64 位 Microsoft Windows 10 IoT Enterprise 版 1809 32 位/64 位 Microsoft Windows 10 20H2 IoT Enterprise 32 位/64 位 Microsoft Windows 10 21H2 IoT Enterprise 32 位/64 位 Microsoft Windows 10 IoT Enterprise 32 位/64 位 Microsoft Windows 10 IoT Enterprise version 1909 32 位/64 位 Microsoft Windows 10 IoT Enterprise LTSC 2021 32 位/64 位 Microsoft Windows 10 IoT Enterprise 版 1607 32 位/64 位 Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32 位/64 位 Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32 位/64 位 Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32 位/64 位 Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32 位/64 位 Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32 位/64 位 Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32 位/64 位 Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32 位/64 位 Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32 位/64 位 Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32 位/64 位 Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32 位/64 位 Microsoft Windows 10 Home RS5（2018 年 10 月）32 位/64 位 Microsoft Windows 10 Pro RS5（2018 年 10 月）32 位/64 位 Microsoft Windows 10 Pro for Workstations RS5（2018 年 10 月）32 位/64 位 Microsoft Windows 10 Enterprise RS5（2018 年 10 月）32 位/64 位 Microsoft Windows 10 Education RS5（2018 年 10 月）32 位/64 位 Microsoft Windows 10 Home 19H1 32 位/64 位 Microsoft Windows 10 Pro 19H1 32 位/64 位 Microsoft Windows 10 Pro for Workstations 19H1 32 位/64 位 Microsoft Windows 10 Enterprise 19H1 32 位/64 位

Microsoft Windows 10 Education 19H1 32 位/64 位

Microsoft Windows 10 家庭版 19H2 32 位/64 位

Microsoft Windows 10 专业版 19H2 32 位/64 位

Microsoft Windows 10 专业工作站版 19H2 32 位/64 位

Microsoft Windows 10 企业版 19H2 32 位/64 位

Microsoft Windows 10 教育版 19H2 32 位/64 位

Microsoft Windows 10 Home 20H1（2020 年 5 月更新）32 位/64 位

Microsoft Windows 10 Pro 20H1（2020 年 5 月更新）32 位/64 位

Microsoft Windows 10 Enterprise 20H1（2020 年 5 月更新）32 位/64 位

Microsoft Windows 10 Education 20H1（2020 年 5 月更新）32 位/64 位

Microsoft Windows 10 Home 20H2（2020 年 10 月更新）32 位/64 位

Microsoft Windows 10 Pro 20H2（2020 年 10 月更新）32 位/64 位

Microsoft Windows 10 Enterprise 20H2（2020 年 10 月更新）32 位/64 位

Microsoft Windows 10 Education 20H2（2020 年 10 月更新）32 位/64 位

Microsoft Windows 10 Home 21H1（2021 年 5 月更新）32 位/64 位

Microsoft Windows 10 Pro 21H1（2021 年 5 月更新）32 位/64 位

Microsoft Windows 10 Enterprise 21H1（2021 年 5 月更新）32 位/64 位

Microsoft Windows 10 Education 21H1（2021 年 5 月更新）32 位/64 位

Microsoft Windows 10 Home 21H2（2021 年 10 月更新）32 位/64 位

Microsoft Windows 10 Pro 21H2（2021 年 10 月更新）32 位/64 位

Microsoft Windows 10 Enterprise 21H2（2021 年 10 月更新）32 位/64 位

Microsoft Windows 10 Education 21H2（2021 年 10 月更新）32 位/64 位

Microsoft Windows 10 Home 22H2（2023 年 10 月更新）32 位/64 位

Microsoft Windows 10 Pro 22H2（2023 年 10 月更新）32 位/64 位

Microsoft Windows 10 Enterprise 22H2（2023 年 10 月更新）32 位/64 位

Microsoft Windows 10 Education 22H2（2023 年 10 月更新）32 位/64 位

Microsoft Windows 11 Home 64 位

Microsoft Windows 11 Pro 64 位

Microsoft Windows 11 Enterprise 64 位

Microsoft Windows 11 Education 64 位

Microsoft Windows 11 22H2

Microsoft Windows 8.1 专业版 32 位/64 位

Microsoft Windows 8.1 企业版 32 位/64 位

Microsoft Windows 8 专业版 32 位/64 位

Microsoft Windows 8 企业版 32 位/64 位

Microsoft Windows 7 专业版 Service Pack 1 和更高版本 32 位/64 位

Microsoft Windows 7 企业版/旗舰版 Service Pack 1 和更高版本 32 位/64 位

Microsoft Windows 7 Home Basic/Premium Service Pack 1 及更高版本 32 位/64 位

Microsoft Windows XP Professional Service Pack 3 及更高版本 32 位

Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32 位

Windows MultiPoint Server 2011 Standard/Premium 64 位

	Windows Server 2008 基础版 Service Pack 2 32 位/64 位 Windows Server 2008 Service Pack 2（所有版本）32 位/64 位 Windows Server 2008 R2 Datacenter Service Pack 1 及更高版本 64 位 Windows Server 2008 R2 Enterprise Service Pack 1 及更高版本 64 位 Windows Server 2008 R2 Foundation Service Pack 1 及更高版本 64 位 Windows Server 2008 R2 Core Mode Service Pack 1 及更高版本 64 位 Windows Server 2008 R2 Standard Service Pack 1 及更高版本 64 位 Windows Server 2008 R2 Service Pack 1 (所有版本) 64 位 Windows Server 2012 Server Core 64 位 Windows Server 2012 Datacenter 64 位 Windows Server 2012 Essentials 64 位 Windows Server 2012 Foundation 64 位 Windows Server 2012 Standard 64 位 Windows Server 2012 R2 Server Core 64 位 Windows Server 2012 R2 Datacenter 64 位 Windows Server 2012 R2 Essentials 64 位 Windows Server 2012 R2 Foundation 64 位 Windows Server 2012 R2 Standard 64 位 Windows Server 2016 Datacenter (LTSB) 64 位 Windows Server 2016 Standard (LTSB) 64 位 Windows Server 2016 Server Core (安装选项) (LTSB) 64 位 Windows Server 2019 Standard 64 位 Windows Server 2019 Datacenter 64 位 Windows Server 2019 Core 64 位 Windows Server 2022 Standard 64 位 Windows Server 2022 Datacenter 64 位 Windows Server 2022 Core 64 位
操作系统。Linux	Debian GNU/Linux 12 (Bookworm) Debian GNU/Linux 11.x (Bullseye) 32 位/64 位 Debian GNU/Linux 10.x (Buster) 32 位/64 位 Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位 Ubuntu Server 20.04 LTS (Focal Fossa) 32 位/64 位 Ubuntu Server 18.04 LTS (Bionic Beaver) 32 位/64 位 CentOS Stream 9 64 位 CentOS 7.x 64 位 Red Hat Enterprise Linux Server 9.x 64 位 Red Hat Enterprise Linux Server 8.x 64 位 Red Hat Enterprise Linux Server 7.x 64 位 Red Hat Enterprise Linux Server 6.x 32 位/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 openSUSE 15 64 位

	Oracle Linux 7 64 位 Oracle Linux 8 64 位 Oracle Linux 9 64 位 Linux Mint 20.x 64 位
操作系统。macOS	macOS Big Sur (11.x) macOS Monterey (12.x) macOS Ventura (13.x)

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
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 位
- Microsoft Hyper-V Server 2012 R2 64 位
- Microsoft Hyper-V Server 2016 64 位
- 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 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- 基于内核的虚拟机（网络代理支持的所有 Linux 操作系统）

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

不支持的操作系统和平台

网络代理

不支持以下操作系统：

- Microsoft Windows Embedded POSReady 7 32 位/64 位
- Microsoft Windows Embedded 8 Industry Pro 32 位/64 位
- Microsoft Windows Embedded 8 Industry Enterprise 32 位 / 64 位
- Microsoft Windows Embedded 8 标准版 32 位/64 位
- Microsoft Windows Embedded 8.1 工业企业版 32 位/64 位
- Microsoft Windows Embedded 8.1 工业更新版 32 位/64 位
- Microsoft Windows 10 Home (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Education (Threshold 1, 1507) 32 位/64 位
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32 位
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32 位
- Microsoft Windows 10 Home Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Pro Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Enterprise Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Education Threshold 2（2015 年 11 月更新，1511）32 位/64 位
- Microsoft Windows 10 Mobile Threshold 2（2015 年 11 月更新，1511）32 位
- Microsoft Windows 10 Mobile Enterprise Threshold 2（2015 年 11 月更新，1511）32 位
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32 位/64 位
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32 位
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32 位
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32 位/64 位
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32 位/64 位
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32 位/64 位

- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32 位/64 位
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32 位
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32 位
- Microsoft Windows 10 Mobile RS3 32 位
- Microsoft Windows 10 Mobile Enterprise RS3 32 位
- Microsoft Windows 10 Mobile RS4 32 位
- Microsoft Windows 10 Mobile Enterprise RS4 32 位
- Microsoft Windows 10 Mobile RS5 32 位
- Microsoft Windows 10 Mobile Enterprise RS5 32 位
- Microsoft Windows 8 (Core) 32 位/64 位
- Microsoft Windows 7 专业版 32 位/64 位
- Microsoft Windows 7 企业版/旗舰版 32 位/64 位
- Microsoft Windows 7 Home Basic/Premium 32 位/64 位
- Microsoft Windows Vista Business with Service Pack 1 32 位/64 位
- Microsoft Windows Vista Enterprise with Service Pack 1 32 位/64 位
- Microsoft Windows Vista Ultimate with Service Pack 1 32 位/64 位
- Microsoft Windows Vista Business with Service Pack 2 及更高版本 32 位/64 位
- Microsoft Windows Vista Enterprise with Service Pack 2 及更高版本 32 位/64 位
- Microsoft Windows Vista Ultimate with Service Pack 2 及更高版本 32 位/64 位
- Microsoft Windows XP Professional with Service Pack 2 32 位/64 位
- Microsoft Windows XP Home Service Pack 3 及更高版本 32 位
- Windows Essential Business Server 2008 Standard 64 位
- Windows Essential Business Server 2008 Premium 64 位
- Windows Small Business Server 2003 Standard with Service Pack 1 32 位
- Windows Small Business Server 2003 Premium with Service Pack 1 32 位
- Windows Small Business Server 2008 Standard 64 位
- Windows Small Business Server 2008 Premium 64 位
- Windows Small Business Server 2011 Premium Add-on 64 位

- Windows Small Business Server 2011 Standard 64 位
- Windows Small Business Server 2011 Essentials 64 位
- Windows Home Server 2011 64 位
- Windows MultiPoint Server 2010 Standard 64 位
- Windows MultiPoint Server 2010 Premium 64 位
- Windows MultiPoint Server 2012 Standard/Premium 64 位
- Microsoft Windows 2000 Server 32 位
- Windows Server 2003 Enterprise with Service Pack 2 32 位/64 位
- Windows Server 2003 Standard with Service Pack 2 32 位/64 位
- Windows Server 2003 R2 Enterprise with Service Pack 2 32 位/64 位
- Windows Server 2003 R2 Standard with Service Pack 2 32 位/64 位
- Windows Server 2008 Datacenter Service Pack 1 32 位/64 位
- Windows Server 2008 Enterprise Service Pack 1 32 位/64 位
- Windows Server 2008 Service Pack 1 Server Core 32 位/64 位
- Windows Server 2008 Standard Service Pack 1 32 位/64 位
- Windows Server 2008 Standard 32 位/64 位
- Windows Server 2008 Enterprise 32 位/64 位
- Windows Server 2008 Datacenter 32 位/64 位
- Windows Server 2008 R2 Server Core 64 位
- Windows Server 2008 R2 Datacenter 64 位
- Windows Server 2008 R2 Enterprise 64 位
- Windows Server 2008 R2 Foundation 64 位
- Windows Server 2008 R2 Standard 64 位
- Windows Server 2016 Nano（安装选项）(CBB)
- Windows Storage Server 2008 32 位/64 位
- Windows Storage Server 2008 Service Pack 2 64 位
- Windows Storage Server 2008 R2 64 位
- Windows Storage Server 2012 64 位

- Windows Storage Server 2012 R2 64 位
- Windows Storage Server 2016 64 位
- Windows Storage Server 2019 64 位
- Debian GNU/Linux 7.x（最高 7.8）32 位/64 位
- Debian GNU/Linux 8.x (Jessie) 32 位/64 位
- Debian GNU/Linux 9.x (Stretch) 32 位/64 位
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32 位/64 位
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位/64 位
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 位
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 位/64 位
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 位/64 位
- CentOS 6.x (至 6.6) 64 位
- CentOS 7.x ARM 64 位
- CentOS 8.x 64 位
- SUSE Linux Enterprise Desktop 12（所有服务包）64 位
- SUSE Linux Enterprise Desktop 15 (所有服务包) 64 位
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位
- ALT Server 10 64 位
- ALT Server 9.2 64 位
- ALT Workstation 10 32 位/64 位
- ALT Workstation 9.2 32 位/64 位
- ALT 8 SP Server (LKNV.11100-01) 64 位
- ALT 8 SP Server (LKNV.11100-02) 64 位
- ALT 8 SP Server (LKNV.11100-03) 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
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 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 1.6）64 位
- Astra Linux Common Edition（操作更新 2.12）64 位
- Astra Linux特别版RUSB.10152-02（操作更新4.7）ARM 64位
- Linux Mint 19.x 64 位
- AlterOS 7.5 及更高版本 64 位
- Lotos (Linux 核心版本 4.19.50, DE: MATE) 64 位
- Mageia 4 32 位
- GosLinux IC6 64 位
- RED OS 7.3 64 位
- RED OS 7.3 Server 64 位
- RED OS 7.3 Certified Edition 64 位
- ROSA COBALT 7.9 64 位
- ROSA CHROME 12 64 位
- ROSA Enterprise Linux Server 7.3 64 位
- ROSA Enterprise Linux Desktop 7.3 64 位
- ROSA COBALT Workstation 7.3 64 位
- ROSA COBALT Server 7.3 64 位
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS Sierra (10.12)
- macOS High Sierra (10.13)
- macOS Mojave (10.14)
- macOS Catalina (10.15)

不支持以下虚拟化平台：

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 位
- Microsoft Hyper-V Server 2008 R2 64 位
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 及更高版本 64 位
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

兼容的卡巴斯基应用程序和解决方案

不同产品的授权许可授予不同的卡巴斯基应用程序和解决方案集。

您可以通过 Kaspersky Security Center 云控制台部署和管理以下卡巴斯基应用程序和解决方案：

- Kaspersky Security for Windows Server 11.0.1
- Kaspersky Endpoint Security 12.4 for Windows
- Kaspersky Endpoint Security 12.0 for Linux
- Kaspersky Endpoint Security 12.0 for Mac

- Kaspersky Embedded Systems Security 3.3 for Windows
- Kaspersky Embedded Systems Security 3.3 for Linux
- Kaspersky Endpoint Agent 3.16
- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS

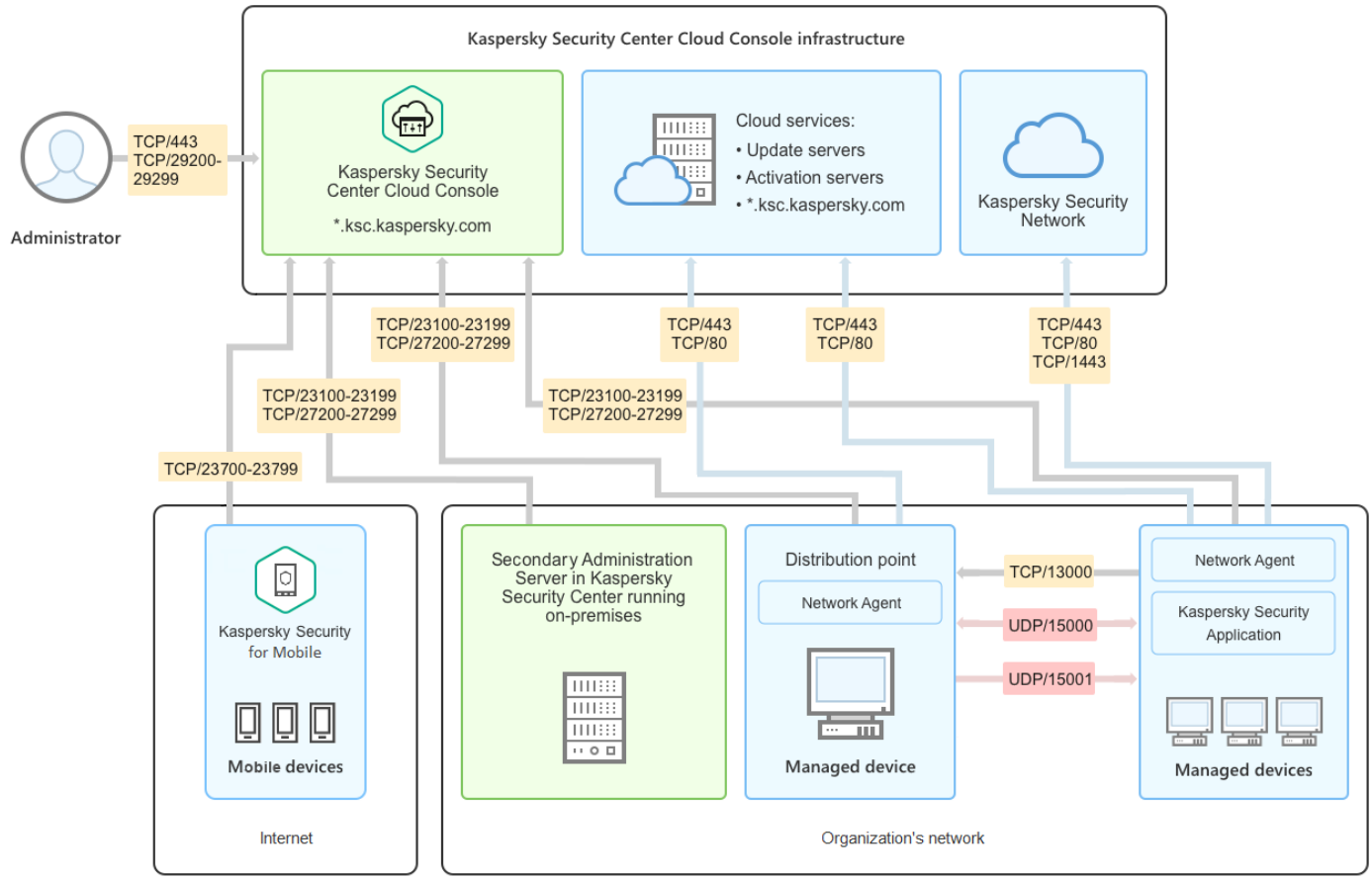
您可以集成以下解决方案来查看和处理安全事件：

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum 2.3
- Kaspersky Endpoint Detection and Response Expert

如果您在受管理设备上安装新的应用程序版本，但对新应用程序版本使用过时的策略而不是更新策略，则应用程序仍会向 Kaspersky Security Center 云控制台提供数据，但 Kaspersky Security Center 云控制台无法如文档的受管理应用程序的已处理数据部分中所述的那样来处理该数据。为了让Kaspersky Security Center 云控制台处理此数据，您必须为新版本的应用程序创建新策略。

架构

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



Kaspersky Security Center 云控制台架构

通过基于云的控制台进行管理的 Kaspersky Security Center 云控制台包括两个主要组件： Kaspersky Security Center 云控制台基础架构和客户的基础架构。

Kaspersky Security Center 云控制台基础架构由以下部分组成：

- **基于云的管理控制台**。提供 Web 界面以创建和维护由 Kaspersky Security Center 云控制台管理的客户端组织网络的保护系统。
- **云服务**。包括更新服务器和激活服务器。
- **卡巴斯基安全网络（KSN）**。包含 Kaspersky 数据库的服务器，该数据库中包含连续更新的文件、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。

客户的基础架构可能包括以下内容：

- **分发点**。安装了网络代理并用于更新发布、网络轮询、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。管理员可选择适当的设备并手动为其分配分发点。
- **受管理设备**。通过 Kaspersky Security Center 云控制台保护的客户网络的计算机。每个受管理设备上必须安装网络代理和卡巴斯基安全应用程序。
- **在本地运行的从属管理服务器**（可选）。您可以使用本地管理服务器来创建管理服务器的层次结构。

Kaspersky Security Center 云控制台使用的端口

要使用 Kaspersky Security Center 云控制台（它是卡巴斯基基础架构的一部分），您必须在客户端设备上打开以下端口以允许互联网连接（请参见下表）：

必须在客户端设备上打开以允许互联网连接的端口

端口（或端口范围）	协议	端口（或端口范围）的用途
23100-23199	TCP (TLS)	从 Kaspersky Security Center 云控制台管理服务器 (*.ksc.kaspersky.com) 上的网络代理和从属管理服务器接收连接。 卡巴斯基基础架构可以使用此范围内的任何端口以及此掩码内的任何网址。端口和网址可能会不时更改。
23700-23799 （仅当管理移动设备时）	TCP (TLS)	接收来自移动设备的连接。 连接到 Kaspersky Security Center 云控制台管理服务器（位于 *.ksc.kaspersky.com）。 卡巴斯基基础架构可以使用此范围内的任何端口以及此掩码内的任何网址。端口和网址可能会不时更改。
27200-27299	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）。 连接到 Kaspersky Security Center 云控制台管理服务器（位于 *.ksc.kaspersky.com）。 卡巴斯基基础架构可以使用此范围内的任何端口以及此掩码内的任何网址。端口和网址可能会不时更改。
29200-29299	TCP (TLS)	使用 klsctunnel 实用程序通过 Kaspersky Security Center 云控制台管理服务器 (*.ksc.kaspersky.com) 建立与受管理设备的隧道连接。 卡巴斯基基础架构可以使用此范围内的任何端口以及此掩码内的任何网址。端口和网址可能会不时更改。
443	HTTPS	连接到 Kaspersky Security Center 云控制台发现服务（位于 *.ksc.kaspersky.com）。 卡巴斯基基础架构可以使用此掩码内的任何网址。
1443	TCP	连接到卡巴斯基安全网络
80	TCP	连接用于检查 *.digicert.com 上 Kaspersky Security Center 证书的有效性。 卡巴斯基基础架构可以使用此掩码内的任何网址。

下表列出了安装网络代理的客户端设备上必须开放的端口。

客户端设备上必须开放的端口

端口号	协议	端口目的	范围
15000	UDP	从连接网关接收数据（如果正在使用）	管理客户端设备
15000	UDP 广播	获取同一广播域内其他网络代理的数据	传送更新和安装包
15001	UDP	接收来自分发点的组播请求（如果正在使用）	从分发点接收更新和安装包

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 云控制台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。

下表列出了在安装网络代理作为分发点的客户端设备上必须打开的其他端口。

端口号	协议	端口目的	范围
13000	TCP (TLS)	接收从网络代理的连接	管理客户端设备、传送更新和安装包
13111（仅当设备上运行 KSN 代理服务时）	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
13295（仅当将分发点用作推送服务器时）	TCP (TLS)	向受管理设备发送推送通知	用作推送服务器的分发点
15111（仅当设备上运行 KSN 代理服务时）	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
17111（仅当设备上运行 KSN 代理服务时）	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

如果您的网络上有一台或多台管理服务器，并且当主管理服务器位于卡巴斯基基础架构中时将它们用作从属管理服务器，请参阅本地运行的 Kaspersky Security Center 使用的端口列表。使用这些端口在从属管理服务器（或多个从属管理服务器）和客户端设备之间进行交互。

Kaspersky Security Center 云控制台界面

Kaspersky Security Center 云控制台通过 Web 界面进行管理。

应用程序窗口包含以下项目：

- 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：

- **介绍和教程**。包含有关如何配置和使用 Kaspersky Security Center 云控制台和安全应用程序的视频。

  在 Mozilla Firefox 浏览器中，如果您在弹窗中播放**介绍和教程**部分中的视频，然后以画中画模式打开该视频，然后关闭弹窗中的视频，则画中画模式也被关闭。

- **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)**。包含管理客户端设备以及任务和卡巴斯基应用程序策略的工具。
- **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、补丁管理和第三方应用程序管理。这还可为您提供访问应用程序存储库的权限。
- **发现和部署**。可让您轮询网络以发现客户端设备，并手动或自动将设备分发到管理组。这还包含快速启动向导和保护部署向导。
- **市场**。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**。包含将 Kaspersky Security Center 云控制台与其他卡巴斯基应用程序集成的设置。它还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**。包含在线帮助的链接和有关卡巴斯基技术支持的信息。它还允许您退出 Kaspersky Security Center 云控制台。

工作区域

工作区显示您选择在应用程序 Web 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。

Kaspersky Security Center 云控制台本地化

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
- 西班牙语
- 西班牙语（拉丁美洲）

Kaspersky Security Center 与 Kaspersky Security Center 云控制台的比较

您可以通过以下方式使用 Kaspersky Security Center：

- 作为云解决方案

  Kaspersky Security Center 将在云环境中安装，Kaspersky 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。

- 作为本地解决方案（基于 Windows 或基于 Linux）

  您可以在本地设备上安装 Kaspersky Security Center，并通过基于 Microsoft 管理控制台的管理控制台或 Kaspersky Security Center Web Console 来管理网络安全系统。

  除了基于 Windows 的应用程序外， Kaspersky Security Center Linux 也可用。Kaspersky Security Center Linux 旨在通过使用基于 Linux 的管理服务器来部署和管理对 Linux 设备的保护，以满足纯 Linux 环境的要求。基于 Windows 的 Kaspersky Security Center 和Kaspersky Security Center Linux 具有不同的功能集。

下表可让您比较 Kaspersky Security Center 和Kaspersky Security Center 云控制台的主要功能。

Kaspersky Security Center 在本地运行与作为云解决方案的功能比较

功能或属性	Kaspersky Security Center 14 在本地运行	Kaspersky Security Center 云控制台
管理服务器位置	本地	云
数据库管理系统 (DBMS) 位置	本地	云
基于 Web 的管理控制台	✓	✓
管理服务器和 DBMS 维护	由客户管理	由卡巴斯基管理
管理服务器层级	✓	✓（Kaspersky Security Center 云控制台的管理服务器只能充当层次结构中的主管理服务器，并且只能用于策略和任务监控）
管理组层级	✓	✓
将受管理设备和相关对象从在本地运行的 Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台	✓	✓
网络轮询	✓	✓（仅按分发点）
受管理设备最大数量	100,000	25,000
对 Windows、Linux 和 macOS 受管理设备的保护	✓	✓
保护移动设备	✓	✓（仅支持 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS）
保护公有云基础架构	✓	✓
以设备为中心的安全管理	✓	✓
应用程序策略	✓	✓
Kaspersky 应用程序的任务	✓	✓
卡巴斯基安全网络	✓	✓
KSN 代理服务器	✓	✓（仅限分发点）
卡巴斯基私有安全网络	✓	–
集中部署 Kaspersky 应用程序的授权许可密钥	✓	✓
将受管理设备切换到另一个管理服务器	✓	–

		（您必须在受管理设备上重新安装网络代理才能将它们切换到另一个管理服务器）
支持虚拟管理服务器	✓	✓
安装第三方软件更新并修复第三方软件漏洞	✓	✓ （修复第三方软件漏洞，只能安装推荐修复）
有关受管理设备上发生的事件的通知	✓	✓
创建和管理用户账户	✓	✓
数据库中事件的最大数量	400,000 （最多可增加至45,000,000）	400,000 （取决于受管理设备的数量）
与 SIEM 系统集成	✓	✓ （仅使用 Syslog 格式和 TLS over TCP 协议）
使用管理服务器作为 WSUS 服务器	✓	–
监控策略和任务的状态	✓	✓
管理组中对集群和服务器阵列的支持	✓ （仅在基于 MMC 的管理控制台中）	–
远程安装操作系统	✓	–
SNMP 支持	✓	–

基本概念

本部分解释与 Kaspersky Security Center 云控制台有关的基本概念。

网络代理

管理服务器和设备之间的交互由 Kaspersky Security Center 云控制台的*网络代理*组件执行。网络代理必须安装在所有使用 Kaspersky Security Center 云控制台来管理 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"
- 设置随操作系统启动而自动启动
- 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。

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。Kaspersky Security Center 云控制台每小时会自动将管理服务器与受管理设备同步几次。管理服务器根据受管理设备的数量设置同步间隔（也称为*心跳*）。

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 云控制台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，您可以将该员工的计算机从会计管理组移动到开发者管理组。然后，该计算机将自动接收开发者的应用程序设置。

管理服务器层级

管理服务器可以排列在"主/从属"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。从属管理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。

Kaspersky Security Center 云控制台管理服务器只能充当主管理服务器，并且只能将本地运行的管理服务器作为从属服务器。

从本地运行的管理服务器迁移到 Kaspersky Security Center 云控制台管理服务器时，您可以按层次结构排列管理服务器。然后，为了缓解迁移，您可以仅将部分受管理设备转移给 Kaspersky Security Center 云控制台管理服务器进行管理。其余受管理设备仍由本地管理服务器管理。这使您能够在有限数量的受管理设备上测试Kaspersky Security Center 云控制台的管理功能。同时，您可以配置策略、任务、报告和其他对象来测试对整个网络的管理和监控。这可让您在必要时切换回到在本地管理服务器上配置的对象。

管理组层次结构中包括的每台设备都只能连接到一个管理服务器。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管理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 云控制台的一个组件，用于管理客户端阻止网络的反病毒保护系统。每个虚拟管理服务器都可以有自己的管理组结构以及自己的管理和监视方式，例如策略、任务、报告和事件。虚拟管理服务器的功能范围可供工作流程复杂的组织使用。

虚拟管理服务器具有以下限制：

- 虚拟管理服务器仅在商业模式的 Kaspersky Security Center 云控制台中受支持。
- 虚拟管理服务器不支持从属管理服务器（包括虚拟服务器）的创建。
- 您无法将虚拟管理服务器从Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台。
- 虚拟管理服务器不能由专门的管理员管理。默认情况下，管理主管理服务器的管理员也管理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。
- 在虚拟管理服务器属性窗口中，区域的数量是有限的。

分发点

*分发点*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。分发点可执行以下功能：

- 将更新和安装包分发到组中的客户端设备（包括使用 UDP 通过组播进行分发）。更新可以通过为分发点创建的更新任务从卡巴斯基更新服务器接收。

  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。

- 通过 Microsoft Windows 工具执行第三方软件和 Kaspersky 程序的远程安装，包括在无网络代理的客户端设备上的安装。

  此功能可让您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。

- 作为代理服务器参与卡巴斯基安全网络。

  运行 Linux 或 macOS 的分发点设备不支持此功能。

  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。通过减少流量，相比 SOAP，使用 HTTP 或 HTTPS 可产生更高性能。

安装了网络代理的设备必须根据管理组手动分配分发点。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。然而，作为分发点的设备可能不包含在它被分配的管理组。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。

Kaspersky Security Center 云控制台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。这可让您避免由于 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 云控制台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中，在**安全问题**区域。

在分配为分发点的设备上运行远程安装任务需要另外的剩余磁盘空间。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剩余磁盘空间。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。

管理 Web 插件

特殊组件 — *管理 Web 插件* — 通过 Kaspersky Security Center 云控制台对 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 云控制台与特定 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。

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 Kaspersky 应用程序和设备的界面
- 应用程序事件传输
- Kaspersky Security Center 云控制台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 云控制台为管理组中的每个 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 Kaspersky 应用程序，只能有一个策略处于活动状态。设备对 Kaspersky 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 云控制台允许您创建*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。

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。

应用程序授权许可

本节提供与应用程序授权许可相关的信息。

Kaspersky Security Center 云控制台的授权许可：场景

在这种情况下，您可以开始在授权许可下使用 Kaspersky Security Center 云控制台和受管理安全应用程序。

Kaspersky Security Center 云控制台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。

如果您已经在使用 Kaspersky Security Center 云控制台，您可以访问卡巴斯基市场查看全系列的卡巴斯基业务解决方案，选择您需要的解决方案，然后继续在卡巴斯基网站上进行购买。

购买授权许可之前在试用模式下查看 Kaspersky Security Center 云控制台的功能

您可以先免费试用 Kaspersky Security Center 云控制台。为此，请创建一个试用工作区，该工作区将在 30 天后终止。如果您想要一个可以无限使用的商业工作区，则必须购买授权许可。

试用模式不允许您随后切换到商业模式。30 天期限到期后，任何试用工作区及其所有内容都将被自动删除。

阶段

方案实施分为几个阶段：

1. **获取用于在商业模式下授权许可 Kaspersky Security Center 云控制台的激活码。购买授权许可（或多个授权许可）**

   不同的授权许可授予不同的卡巴斯基应用程序和服务的使用权，因此您可能需要购买多个授权许可。

   了解您可以购买哪些授权许可以及每个授权许可的最小设备数量。

   Kaspersky Security Center 云控制台是多个卡巴斯基解决方案的一部分。选择您要使用的解决方案并为其购买授权许可。如果您想要购买涵盖10,000 台或更多设备的授权许可，您需要联系卡巴斯基或卡巴斯基合作伙伴之一提出特殊请求。

   使用该表检查哪些漏洞和补丁管理功能可在哪个授权许可下可用。

   如果您想在 Microsoft Azure 等云环境中使用 Kaspersky Security Center 云控制台，请阅读云环境的授权许可选项。

   如果您是管理服务提供商 (MSP)，请阅读有关适用于 MSP 的 Kaspersky Security Center 云控制台许可的信息。

2. **创建工作区时激活 Kaspersky Security Center 云控制台**

   您可以在创建工作区时指定授权许可密钥来激活 Kaspersky Security Center 云控制台 。

   如果您有多个授权许可密钥，请指定其中任意一个，随后您必须在 Kaspersky Security Center 云控制台中添加其他授权许可密钥才能激活受管理的卡巴斯基应用程序。

3. **将受管理应用程序的授权许可密钥添加到管理服务器存储库**

   在部署授权许可密钥之前，您必须将这些授权许可密钥添加到管理服务器存储库。

您在创建工作区时指定的授权许可密钥会自动添加到管理服务器存储库中。

如果您有多个授权许可密钥，请将一个或多个授权许可密钥逐一添加到 Kaspersky Security Center 云控制台管理服务器存储库。

4. 为受管理应用程序部署授权许可密钥

选择将授权许可密钥（或多个授权许可密钥）部署到您要保护的所有设备的方法：

- 自动部署

  > 如果您使用不同的受管理应用程序并且必须为应用程序部署特定的激活码，请选择另一种部署该激活码的方式。

  Kaspersky Security Center 可让您为受管理应用程序自动部署可用授权许可密钥。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启用了"**自动分发授权许可密钥到受管理设备**"选项。Kaspersky 安全应用程序—例如，Kaspersky Endpoint Security for Windows— 被安装到组织设备。设备上发现新的受管理应用程序，必须为其部署授权许可密钥。例如，存储库中的两个授权许可密钥可以被部署到设备上的受管理应用程序：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为受管理应用程序部署。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，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，安装数量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应用程序数量不超过授权许可限制。如果安装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。

  说明：

  - 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

- 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。

  说明：

  - 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。

5. 检查受管理卡巴斯基应用程序在哪些设备上已激活

要确保正确部署授权许可密钥，请查看用于应用程序的授权许可密钥列表。

6. 配置与授权许可到期相关的事件

配置事件，以便在您的授权许可密钥用完或即将过期时收到通知：

- 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

关于Kaspersky Security Center 云控制台的试用模式

*试用模式*是 Kaspersky Security Center 云控制台的一种特殊模式，旨在让用户熟悉 Kaspersky Security Center 云控制台的功能。在此模式下，您可以在有效期限制为 30 天的工作区内执行活动。创建试用工作区后，试用模式会自动激活。试用模式下可用的功能集与标准卡巴斯基网络安全解决方案高级版授权许可下的范围相同。

在 Kaspersky Security Center 云控制台中，您无需获得管理服务器的许可，因为不支持需要特殊许可的功能。如果您想在试用模式下使用 Kaspersky Security Center 云控制台，您会在创建第一个工作区时自动获得试用授权许可。

试用模式不允许您随后切换到商业模式。30 天期限到期后，任何试用工作区及其所有内容都将被自动删除。

在试用模式下使用 Kaspersky Security Center 云控制台功能有以下限制：

- 您可以创建管理服务器层级。无法创建虚拟管理服务器。
- **授权许可**部分仅可只读。本节禁止所有操作，包括添加和删除授权许可密钥。
- 您无法创建自定义安装包。
- 您无法为用户创建自定义角色。
- 病毒爆发功能不可用。不存储病毒爆发事件，也不发送任何通知。
- **已删除对象**存储库不可用。
- 您无法将批量事件（大量发布的事件）添加到数据库中。
- 不支持将管理服务器从本地模式迁移到云控制台模式。
- 来自管理服务器组件（例如管理服务器或网络代理）的 KSN 统计信息不会发送到卡巴斯基。

应用程序的某些对象的创建也受到一些限制（请参见下表）。如果在尝试创建此类对象时超出任何这些限制，则对象创建将被阻止，并且将显示有关该限制的错误消息。

在试用模式下创建 Kaspersky Security Center 云控制台对象的限制

限制类型	参数值
策略	8
任务	17
授权许可密钥	1
安装包	5
设备分类（不包括预设实例）	5
事件分类（不包括预设实例）	5
设备移动规则	3
相同类型的报告模板	10

内部安全组	20
受管理设备	20

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 云控制台会将您重定向到 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。

授权许可和每个授权许可的最小设备数量

如果您想在商业模式下使用 Kaspersky Security Center 云控制台，您必须在创建第一个工作区之前购买授权许可。下表显示了您可以购买的授权许可以及每个授权许可的最小设备数量（即使您想要保护更少的设备）：

授予使用 Kaspersky Security Center 云控制台的授权许可

授权许可	最小设备数量（即使您想保护较少数量）
卡巴斯基网络安全解决方案标准版支持	商业授权许可：300 对于商业（订阅）授权许可：100
卡巴斯基网络安全解决方案高级版	商业授权许可：300 对于商业（订阅）授权许可：100
卡巴斯基网络安全解决方案完整版	300
Kaspersky Endpoint Detection and Response Optimum	商业授权许可：300 对于商业（订阅）授权许可：100
Kaspersky Endpoint Detection and Response Expert	50
卡巴斯基混合云安全，桌面	商业授权许可：300 对于商业（订阅）授权许可：100
卡巴斯基混合云安全，服务器	50
卡巴斯基混合云安全，核心	20
卡巴斯基混合云安全，CPU	20
卡巴斯基混合云安全企业版，桌面	商业授权许可：300 对于商业（订阅）授权许可：100
卡巴斯基混合云安全企业版，服务器	50
卡巴斯基混合云安全企业版，CPU	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security 合规版	300
Kaspersky Symphony（目前仅在俄罗斯可用）	300
Kaspersky Next EDR Foundations	300 个用户（每个用户授权许可适用于 1 台 PC/Mac 设备和 2 台移动设备）
Kaspersky Next EDR Optimum	300 个用户（每个用户授权许可适用于 1 台 PC/Mac 设备和 2 台移动设备）
Kaspersky Next XDR Expert	250 个用户（每个用户授权许可适用于 1 台 PC/Mac 设备和 2 台移动设备）

每个工作区的最大设备数量为 25,000 台。如果要保护超过 10,000 台设备，则需要创建单独的工作区。为此，请向卡巴斯基技术支持发送请求。该请求必须包含以下信息：

- **用户电子邮件**— 在Kaspersky Security Center 云控制台上注册的用户的电子邮件地址。该用户被授予对所创建的工作区的管理员权限。

  在Kaspersky Security Center 云控制台上创建账户后，您不必注册公司并为其创建工作区。在请求中指定有关公司和工作空间的信息。

- **公司名称**— 您想要使用 Kaspersky Security Center 云控制台的公司名称。

- **公司所在国家/地区**— 公司所在的国家/地区。

- **工作空间名称**— 要为公司创建的工作空间的名称。

- **估计端点计数**— 您想要在新工作区中保护的客户端设备（包括移动设备）的总数。

- **工作区国家/地区** — 您想要将新工作区定位到的国家/地区。该参数会影响存储工作区的数据中心的选择。

  请注意，如果您想要在美国或加拿大定位工作区，请指定州或省以确定数据中心区域。

  公司国家/地区和**工作区国家/地区**参数可能相同。

- **激活码**— 您购买 Kaspersky Security Center 云控制台后收到的激活码。确保您要购买的授权许可涵盖所有必须受到保护的客户端设备。

发送请求后，卡巴斯基专家会注册指定的公司并为其创建工作区。工作区创建完成后，您将收到一封电子邮件通知。您可以在Kaspersky Security Center 云控制台上登录您的账户查看结果。

超出了授权许可限制事件

Kaspersky Security Center 云控制台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。

将激活码分发到受管理设备的方法

安装到受管理设备上的 Kaspersky 应用程序必须通过将激活码应用到每个应用程序来获得授权。您不能使用密钥文件来授权受管理应用程序；只接受激活码。激活码可以按以下方法部署：

- 自动部署

- 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

Kaspersky 应用程序可以同时使用多个授权许可密钥。例如，Kaspersky Endpoint Security for Windows 可以使用两个授权许可密钥—一个用于 Kaspersky Endpoint Security for Windows，另一个用于激活 Endpoint Detection and Response 功能。

此外，卡巴斯基应用程序不仅可以拥有活动授权许可密钥，还可以拥有备用授权许可密钥。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。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。

添加授权许可密钥到管理服务器存储库

使用 Kaspersky Security Center 云控制台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。

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. 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。

部署授权许可密钥到客户端设备

Kaspersky Security Center 云控制台允许您自动或通过添加授权许可密钥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。

要通过添加密钥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**添加密钥**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：

   仅当您在创建添加密钥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. 如果您想将此密钥用作备用密钥，请在向导的**授权许可信息**步骤中启用“**用作备用密钥**”选项。

    在这种情况下，备用密钥将在活动密钥过期后被应用。

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 云控制台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，将开关按钮切换至“**自动分发授权许可密钥到受管理设备**”。
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。

如果您对用于激活受管理设备上的应用程序的订阅授权许可密钥指定了“**自动分发授权许可密钥到受管理设备**”选项，并且同时拥有有效的试用版授权许可密钥，那么您的试用版授权许可密钥将在到期日期前八天自动替换为订阅授权许可密钥。

查看有关管理服务器存储库中正在使用的授权许可密钥的信息

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

查看有关用于特定卡巴斯基应用程序的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，请转到“**发现和部署**”→“**未分配的设备**”。
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**”区域。
4. 在打开的应用程序列表中，选择您要查看其授权许可密钥的应用程序。
5. 在打开的应用程序属性窗口中的“**General**”选项卡上，选择“**License keys**”区域。
   相关信息显示在此区域的工作区中。

从存储库删除授权许可密钥

您可以从管理服务器存储库中删除授权许可密钥。请注意，在以下情况下，Kaspersky Security Center 云控制台会在 90 天后自动删除您的工作区：

- 您删除存储库中手动添加的上一个授权许可密钥（活动的、备用或未使用）。
- 上一个授权许可密钥已过期。

如果您的工作区被删除，您将无法通过 Kaspersky Security Center 云控制台管理网络保护。您还将永久丢失 Kaspersky Security Center 云控制台中的数据。如有必要，您可以手动删除您的工作区。否则，我们建议您在管理服务器存储库中至少保留一个授权许可密钥。

如果删除授权许可密钥并之前添加了备用授权许可密钥，则在先前的活动密钥被删除或过期后，备用授权许可密钥将自动成为活动授权许可密钥。

当您删除部署到受管理设备上的活动授权许可密钥时，应用程序将继续工作在受管理设备。

要从管理服务器存储库删除权许可密钥：

1. 检查管理服务器未使用您要删除的授权许可密钥。如果管理服务器使用了该密钥，则您无法删除该密钥。要执行检查：
   a. 在主菜单，单击管理服务器旁边的设置图标 ()。
      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. 如果所需的活动密钥密钥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。如果所需的授权许可密钥未显示，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. 选择所需的授权许可密钥，然后单击**删除**按钮。

4. 在出现的窗口中，选中**我了解风险，希望删除授权许可密钥**复选框。这意味着，如果您删除最后一个授权许可密钥，您就会意识到随后会删除工作区并失去对受管理设备的控制。下一步，单击“**删除**”按钮。

结果，选定的授权许可密钥被从存储库中删除。

您可以再次添加一个已删除的授权许可密钥或添加一个新授权许可密钥。如果您删除了最后一个授权许可密钥，只要您的工作区未被删除，您还可以添加授权许可密钥。Kaspersky Security Center 云控制台会在删除前 30 天、7 天和 1 天通知工作区管理员。

查看卡巴斯基应用程序未在其中激活的设备的列表

您可以查看安装了卡巴斯基应用程序但未激活（例如，授权许可丢失或已过期）的所有设备的列表。

要查看未激活卡巴斯基应用程序的设备：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。

   将显示任务列表。

2. 单击与相关卡巴斯基应用程序相关的更新任务的名称。

   将显示任务属性窗口，其中包含几个已命名的选项卡。

3. 在任务属性窗口中，选择“**结果**”区域。

   设备列中显示任务成功的设备。

4. 对**设备**列进行排序。

   设备列中显示任务成功的设备。由于缺少授权许可而任务失败的设备是应用程序未激活的设备。

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及其安装包，再撤销其 EULA。必须从管理服务器及其虚拟管理服务器中删除安装包。

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. 在管理服务器属性窗口的**常规**选项卡上，选择**最终用户授权许可协议**部分。

   一个 EULA 列表（在创建安装包或无缝安装更新时接受）将显示 。

3. 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 是否可以撤销

4. 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）列表以及各自的名称和类型

5. 在 EULA 属性窗口的下部，单击“**撤回授权许可协议**”按钮。

   如果只能通过卸载应用程序来撤销选定的 EULA，或者只能在主管理服务器上撤销此 EULA，则将显示有关此限制的通知，而不是**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，则会显示相关通知。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。

6. 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。

如果最后一个授权许可密钥已过期， Kaspersky Security Center 云控制台会在 90 天后自动删除您的工作区。结果，您将无法通过 Kaspersky Security Center 云控制台管理网络保护。您还将永久丢失 Kaspersky Security Center 云控制台中的数据。我们建议您续订过时的授权许可密钥或将新的授权许可密钥添加到管理服务器存储库以保留您的工作区。

要查看有关到期的授权许可或即将到期的授权许可的通知：

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即将到期和已经到期的授权许可。

2. 如果要续订授权许可，请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，即表示您同意将以下数据传输给卡巴斯基：软件 ID、软件版本、软件本地化、授权许可 ID 以及显示授权许可是否由合作伙伴公司提供的属性。需要这些数据来确定您的授权许可的续订条款。

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。

   即将到期的授权许可被续订。

在 Kaspersky Security Center 云控制台中，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

授权许可到期后对 Kaspersky Security Center 云控制台的使用

授权许可到期后， 卡巴斯基可能会授予您长达 90 天的 Kaspersky Security Center 云控制台使用权，无任何限制。在此期间，管理服务器、网络代理和 Kaspersky Security Center 云控制台 Web 界面可以不受限制地工作。Kaspersky Security Center 云控制台还会根据当前 KSN 访问设置向卡巴斯基发送 KSN 统计数据。受管理应用程序仅具有有限的功能（有关详细信息，请参阅这些应用程序的文档）。

当授权许可过期 90 天时， Kaspersky Security Center 云控制台会自动删除您的工作区。如果您想保留工作区，请续订至少一个过期的授权许可密钥或将新的授权许可密钥添加到存储库中。

卡巴斯基安全网络 （KSN）

该区域描述如何使用卡巴斯基安全网络（KSN）的在线服务基础架构。该区域提供了关于 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。

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 可让您使用 Kaspersky 的信誉数据库检索有关安装在客户端设备上的应用程序信息。

一旦加入 KSN，即表示您同意以自动模式将通过 Kaspersky Security Center 云控制台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。

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 声明的先前版本继续使用 KSN。

启用 KSN 后，Kaspersky Security Center 云控制台会检查 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。

启用和禁用 KSN

要启用 KSN:

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 设置**”区域。
3. 将切换按钮切换到**使用卡巴斯基安全网络已启用**位置。
   KSN 已启用。
   如果启用此切换按钮，客户端设备将发送补丁安装结果到 Kaspersky。启用此切换按钮时，您应阅读并接受 KSN 声明的条款。
4. 单击“**保存**”按钮。

要禁用 KSN:

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 设置**”区域。
3. 将切换按钮切换到**使用卡巴斯基安全网络已禁用**位置。
   KSN 已禁用。

如果禁用此切换按钮，客户端设备将不发送补丁安装结果到 Kaspersky。

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 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 声明已更新，当您打开 Kaspersky Security Center 云控制台时，会自动显示该声明。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。您可以稍后查看并接受更新后的 KSN 声明。

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。

授权许可定义

本节包含与通过 Kaspersky Security Center 云控制台管理的卡巴斯基应用程序许可相关的概念的定义。

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 云控制台的权限。

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 云控制台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 云控制台，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：

- 授权许可密钥或订购号
- 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程序。授权许可密钥由 Kaspersky 专家生成。

您可以通过输入*激活码*向应用程序添加授权许可密钥。为程序添加授权许可后，将在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 云控制台。在购买 Kaspersky Security Center 云控制台或预定试用版本的 Kaspersky Security Center 云控制台后，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。

关于订阅

*Kaspersky Security Center 云控制台订阅*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 云控制台订阅。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 云控制台，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 云控制台，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 云控制台申请不同的激活码。

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 云控制台的早期版本。

在订阅下使用应用程序时，Kaspersky Security Center 云控制台在指定时间间隔自动尝试访问激活服务器，直到订阅过期。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。

数据提供

Kaspersky Security Center 云控制台使用户能够通过受管理应用程序的功能来识别和控制连接到 Kaspersky Security Center 云控制台的设备（以及设备所有者）。

数据提供方式：

1. 用户在 Kaspersky Security Center 云控制台界面中输入数据。
2. 网络代理会从设备接收数据，并将其传输到管理服务器。
3. 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。
4. 数据从本地运行的从属管理服务器传输。

Kaspersky Security Center 云控制台会在试用许可期限到期后 30 天、商业许可期限到期后 90 天自动删除工作区。

许可期限到期后，卡巴斯基会将与用户工作区中的警报和事件相关的用户数据保存 30 天。

根据当前授权许可，警报和事件的存储期限为 360 天。在此期限之后，较旧的警报和较旧的事件将被自动删除。

本节中列出的数据的最终删除可能需要长达 24 小时的时间。

发送至卡巴斯基服务器的数据

激活期间发送的数据

在使用激活码激活软件时，为了验证使用该软件的合法性，用户同意定期向卡巴斯基提供以下信息：

- 激活码
- 当前授权许可的唯一激活标识符

卡巴斯基还可以使用此信息生成有关卡巴斯基软件的分发和使用的统计信息。

更新期间发送的数据

从权利持有人的更新服务器收到更新后，为了提高更新机制的质量，用户同意定期向卡巴斯基提供以下信息：

- 从授权许可中收到的软件 ID
- 完整版软件
- 软件授权许可 ID
- 软件安装 ID (PCID)
- 软件更新启动 ID

卡巴斯基还可以使用此信息生成有关卡巴斯基软件的分发和使用的统计信息。

用于确保不间断运行、高效工作以及验证Kaspersky Security Center 云控制台的合法使用的数据

以下信息可用于指定目的：

- 连接到工作区的卡巴斯基安全应用程序的名称和版本，以及安装这些安全应用程序的设备数量。
- 已连接到所有工作区且安装了卡巴斯基安全应用程序的设备数量以及这些已连接设备的分布情况（按类型）。
- 工作区标识符、公司标识符、工作区国家和地区以及工作区创建日期。
- 工作区中的用户数量、工作区中上次身份验证的日期。
- 当前使用的授权许可的详细信息（授权许可类型、设备数量的授权许可限制、连接的设备数量以及先前使用的授权许可的到期日期）。

点击 Kaspersky Security Center 云控制台界面中的链接时传输的数据

单击管理控制台或 Kaspersky Security Center 云控制台中的链接，即表示用户同意自动传输以下数据：

- Kaspersky Security Center 云控制台本地化
- 授权许可 ID
- 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。

工作区运行所需的数据

Kaspersky Security Center 云控制台可处理以下数据：

1. 在组织网络上检测到的设备的详细信息

   网络代理从联网设备接收下列数据并将其传输到管理服务器：

   a. 通过网络轮询接收到的被检测设备及其设备识别所需的组件的技术规格：

   - 活动目录轮询：

     Active Directory 设备：设备的可分辨名称；从域控制器收到的 Windows 域名； Windows环境下的设备名称； NetBIOS 域名；设备的 DNS 域名和DNS 名称；安全账户管理器 (SAM) 账户（登录系统的名称，用于支持运行早期操作系统版本的客户端和服务器，例如 Windows NT 4.0、Windows 95、Windows 98 和 LAN Manager）；域名的专有名称；设备所属组的可分辨名称；管理设备的用户的专有名称；以及设备的全局唯一标识符 (GUID) 和父 GUID。

     轮询 Active Directory 网络时，还会处理以下类型的数据，以便显示有关受管理基础架构的信息以及用户对这些信息的使用，例如在保护部署期间：

   - Active Directory 组织单位：组织单位的可分辨名称；域名的专有名称；组织单位的 GUID 和父 GUID。

- Active Directory 域：从域控制器收到的 Windows 域名；DNS 域；域的 GUID。

- Active Directory 用户：用户的显示名称；用户的专有名称；域名的专有名称；用户组织的名称；用户工作的部门名称；充当用户管理员的另一个用户的可分辨名称；用户的全名； SAM 账户；电子邮件地址;备用电子邮件地址;主要电话号码；备用电话号码；手机号码;用户的职位名称；用户所属组的可分辨名称；用户全局唯一标识符（GUID）；用户安全标识符 (SID)（用于将用户标识为安全主体的唯一二进制值）；用户主体名称 (UPN) — 基于 Internet 标准 RFC 822 的用户的 Internet 样式登录名。UPN 比专有名称更短并且更容易记住。按照约定，UPN 映射到用户电子邮件名称。

- Active Directory 组：组的可分辨名称；电子邮件地址;域名的专有名称；SAM 账户；该组所属的其他组的可分辨名称；SID组；组 GUID。

b. Samba 域轮询：

Samba 设备：设备的可分辨名称；从域控制器收到的域名； NetBIOS 设备名称；NetBIOS 域名；设备的 DNS域名和DNS名称；安全账户管理器（SAM）账户；域名的专有名称；设备所属组的可分辨名称；管理设备的用户的专有名称；设备的全局唯一标识符 (GUID) 和父 GUID。

- Samba 组织单位：组织单位的可分辨名称；域名的专有名称；组织单位的 GUID 和父 GUID。

- Samba域：从域控制器收到的域名；DNS 域；域的 GUID。

- Samba 用户：用户的显示名称；用户的专有名称；用户组织的名称；用户工作的部门名称；充当用户管理员的另一个用户的可分辨名称；用户的全名；SAM 账户；电子邮件地址;备用电子邮件地址;主要电话号码；备用电话号码；手机号码;用户的职位名称；用户所属组的可分辨名称；用户全局唯一标识符（GUID）；用户安全标识符 (SID)（用于将用户标识为安全主体的唯一二进制值）；用户主体名称 (UPN) — 基于 Internet 标准 RFC 822 的用户的 Internet 样式登录名。UPN 比专有名称更短并且更容易记住。按照约定，UPN 映射到用户电子邮件名称。

- Samba 组：组的可分辨名称；电子邮件地址；域名的专有名称；SAM 账户；该组所属的其他组的可分辨名称；SID组；组 GUID。

c. Windows 域轮询：

- Windows 域或工作组名称

- 设备 NetBIOS 名称

- 设备的 DNS 域名和 DNS 名称

- 设备名称和描述

- 设备在网络中可见

- 设备 IP 地址

- 设备类型（工作站、服务器、SQL Server、域控制器等）

- 设备上安装的操作系统的类型

- 设备操作系统的版本

- 设备信息上次更新时间

- 设备在网络中最后可见的时间

d. IP 范围轮询：

- 设备 IP 地址
- 设备 DNS 名称或 NetBIOS 名称
- 设备名称和描述
- 设备 MAC 地址
- 设备在网络中最后可见的时间

2. 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 Kaspersky Security Center 云控制台界面中输入设备的显示名称和说明：

a. 设备识别所需的被管理设备及其组件的技术规格：

- 设备的显示名称（根据 NetBIOS 名称生成，可以手动修改）和描述（手动输入）
- Windows 域名和类型（Windows NT 域/Windows 工作组）
- Windows环境下的设备名称
- 设备的 DNS 域名和 DNS 名称
- 设备 IP 地址
- 设备子网掩码
- 设备网络位置
- 设备 MAC 地址
- 设备上安装的操作系统的类型
- 设备是否是虚拟机以及虚拟机管理程序类型
- 该设备是否是作为虚拟桌面基础架构 (VDI) 一部分的动态虚拟机
- 设备 GUID
- 网络代理实例 ID
- 网络代理安装 ID
- 网络代理永久 ID

b. 审核受管理设备以及决定特定补丁和更新是否适用所需的受管理设备及其组件的其他规范：

- Windows 更新代理 (WUA) 状态
- 操作系统架构
- 操作系统生产商
- 操作系统内部版本号

- 操作系统发布 ID
- 操作系统位置文件夹
- 如果设备是虚拟机——虚拟机类型
- 设备响应等待时间
- 网络代理是否以单机模式运行

c. 有关受管理设备上的活动的详细信息：

- 上次更新的日期和时间
- 设备在网络中最后可见的日期和时间
- 重启等待状态（“需要重启。”）
- 设备开启时间

d. 设备用户账户及其工作会话的详细信息

e. 分发点运行统计数据（如果设备是分发点）：

- 分发点的创建日期和时间
- 工作文件夹名称
- 工作文件夹大小
- 与管理服务器同步的次数
- 设备上次与管理服务器同步的日期和时间
- 传输文件的数量和总大小
- 客户端下载的文件数量和总大小
- 客户端使用传输控制协议 (TCP) 下载的数据量
- 使用组播发送到客户端的数据量
- 客户端使用组播下载的数据量
- 多点传送分发数量
- 组播分发总量
- 上次与管理服务器同步后与客户端的同步次数

f. 管理设备的虚拟管理服务器的名称

g. 云设备详细信息：

- 云区域

- 虚拟私有云 (VPC)
- 云可用区域
- 云子网
- 云放置组

h. 移动设备详细信息。受管理应用程序可将此数据从移动设备传输到管理服务器。受管理应用程序的文档中提供了完整的数据列表。

3. 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：

a. 设备上安装的卡巴斯基受管理应用程序和Kaspersky Security Center 云控制台组件

b. 在受管理设备上安装的卡巴斯基应用程序的设置：

- 卡巴斯基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
- 检测到的威胁总数
- 清除失败的对象数量
- 卡巴斯基安全应用程序的任务
- 应用程序组件的可用性和状态
- 反病毒数据库最后更新时间及版本
- 卡巴斯基应用程序设置详情
- 有关活动授权许可密钥的信息
- 有关备用授权许可密钥的信息
- 应用程序安装日期
- 应用程序安装 ID

c. 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

d. Kaspersky 应用程序定义的设备状态

e. Kaspersky 应用程序分配的标签

f. Kaspersky 应用程序的已安装和适用的更新集合：

- 显示应用程序的名称、版本和语言

- 应用程序的内部名称
- 注册表项中的应用程序名称和版本
- 应用程序的安装文件夹
- 补丁版本
- 已安装的应用程序自动补丁列表
- Kaspersky Security Center 云控制台是否支持该应用程序
- 应用程序是否安装在集群上

g. 设备上的数据加密错误详情：错误 ID、发生时间、操作类型（加密/解密）、错误描述、文件路径、加密规则描述、设备ID、用户名

4. Kaspersky Security Center 云控制台组件和卡巴斯基受管理应用程序的事件。

网络代理将数据从设备传输到管理服务器。

事件的描述可以包含以下数据：

a. 设备名称

b. 设备用户名称

c. 远程连接设备的管理员名称

d. 设备上安装的应用程序的名称、版本和供应商

e. 设备上应用程序安装文件夹的路径

f. 设备上文件的路径和文件名

g. 应用程序名称和运行应用程序的命令行参数

h. 补丁名称、补丁文件名、补丁 ID、补丁修复的漏洞级别、补丁安装错误描述

i. 设备 IP 地址

j. 设备 MAC 地址

k. 设备重启状态

l. 发布事件的任务名称

m. 设备是否切换到单机模式以及切换原因

n. 有关设备上的安全问题的信息：安全问题类型、安全问题名称、严重级别、安全问题描述、卡巴斯基应用程序传输的安全问题详细信息

o. 设备上可用磁盘空间的大小

p. 卡巴斯基应用程序是否以有限功能模式运行、功能范围的 ID

q. 卡巴斯基应用程序设置的新旧值

r. 卡巴斯基应用程序或其任何组件执行操作时发生的错误的描述

5. 策略和策略配置文件中显示的 Kaspersky Security Center 云控制台组件和 Kaspersky 受管理应用程序的设置。

   用户在 Kaspersky Security Center 云控制台界面中输入数据。

6. Kaspersky Security Center 云控制台组件和 Kaspersky 受管理应用程序的任务设置

   用户在 Kaspersky Security Center 云控制台界面中输入数据。

7. 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：

   a. 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）。应用程序可以根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信息来识别：

      - 应用程序/补丁 ID
      - 父应用程序 ID（用于补丁）
      - 应用程序/补丁名称和版本
      - 应用程序/补丁是否是 Windows Installer 的 .msi 文件
      - 应用程序/补丁供应商
      - 本地化语言 ID
      - 应用程序/补丁安装日期
      - 应用程序安装路径
      - 应用程序/补丁供应商的技术支持网站
      - 技术支持电话号码
      - 已安装的应用程序实例 ID
      - 注释
      - 卸载密钥
      - 静默模式安装密钥
      - 补丁分类
      - 有关补丁的其他信息的网址
      - 应用程序的注册表项
      - 应用程序内部版本号
      - 用户 SID
      - 操作系统类型（Windows、Unix）

b. 有关在受管理设备上检测到的硬件的信息（硬件注册表）：

- 设备 ID
- 设备类型（主板、CPU、RAM、大容量存储设备、视频适配器、声卡、网络接口控制器、显示器、光盘设备）
- 设备名称
- 描述
- 供应商
- 序列号
- 修订
- 有关驱动程序的信息：开发人员、版本、描述和发布日期
- 有关 BIOS 的信息：开发者、版本、序列号和发布日期
- 芯片
- 时钟频率
- CPU 核心数
- CPU 线程数
- CPU 平台
- 存储设备转速
- RAM：类型，零件号
- 显存
- 声卡解码器

c. 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：

- 漏洞标识符
- 漏洞严重级别（警告、高、严重）
- 漏洞类型（Microsoft、第三方）
- 描述漏洞的页面的网址
- 漏洞条目创建时间
- 供应商名称
- 本地化供应商名称
- 供应商 ID

- 应用程序名称
- 应用程序的本地化名称
- 应用程序安装代码
- 应用程序版本
- 应用程序本地化语言
- 漏洞描述中的 CVE 标识符列表
- 阻止漏洞的卡巴斯基防护技术（文件威胁防护、行为检测、Web 威胁防护、邮件威胁防护、主机入侵防护、ZETA Shield）
- 在其中检测到漏洞的对象文件的路径
- 漏洞检测时间
- 漏洞描述中知识库文章的 ID
- 漏洞描述中的安全公告 ID
- 漏洞更新列表
- 漏洞是否存在可利用的情况
- 漏洞是否存在恶意软件

d. 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：

- 应用程序名称和版本
- 供应商
- 应用程序本地化语言
- 操作系统
- 按安装顺序排列的补丁列表
- 对其应用了补丁的应用程序的原始版本
- 安装补丁后的应用程序版本
- 补丁 ID
- 版本号
- 安装标志
- 补丁的授权许可协议
- 该补丁是否是安装其他补丁的先决条件
- 所需安装的应用程序及其更新的列表

- 有关补丁的信息源
- 有关补丁的附加信息（网页地址）
- 补丁下载的网址、文件名、版本、修订版和 SHA-256

e. WSUS 功能发现的 Microsoft 更新的详细信息：

- 更新修订版本
- Microsoft 更新类型（驱动程序、软件、类别、Detectoid）
- 根据 Microsoft 安全响应中心 (MSRC) 公告更新重要性级别（低、中、高、严重）
- 与更新相关的 MSRC 公告 ID
- MSRC 知识库中文章的 ID
- 更新名称（标题）
- 更新说明
- 更新安装程序是否是交互式的
- 安装标志
- 更新分类（关键更新、定义更新、驱动程序、功能包、安全更新、服务包、工具、更新汇总、更新、升级）
- 有关应用更新的应用程序的信息
- 最终用户授权许可协议 (EULA) ID
- 最终用户许可协议文本
- 更新安装是否必须接受 EULA
- 有关关联更新的信息（ID 和修订号）
- 更新 ID（全局 Microsoft Windows 更新标识）
- 被取代的更新的 ID
- 是否隐藏更新
- 是否强制更新
- 更新安装状态（不适用、未分配安装、已分配、正在安装、已安装、失败、需要重新启动、未分配安装（新版本））
- 更新的 CVE ID
- 发布更新的公司，或"公司缺失"值

f. WSUS 功能发现的必须在设备上安装的 Microsoft 更新列表。

8. 有关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信息（可能与应用程序注册表中的信息相关联）。描述通过相应应用程序管理的设备的数据的部分给出了完整的数据列表。

   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。

9. 备份区中放置的文件的信息。描述通过相应应用程序管理的设备的数据的部分给出了完整的数据列表。

   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。

10. Kaspersky 专家为进行详细分析而请求的文件信息。描述通过相应应用程序管理的设备的数据的部分给出了完整的数据列表。

    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。

11. 自适应异常控制规则的状态和触发的信息。描述通过相应应用程序管理的设备的数据的部分给出了完整的数据列表。

    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。

12. 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）的信息。描述通过相应应用程序管理的设备的数据的部分给出了完整的数据列表。

    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。

13. 有关警报的数据：

    - 警报中第一个遥测事件的日期和时间
    - 警报中最后一次遥测事件的日期和时间
    - 触发规则的名称（用户在 Kaspersky Security Center 云控制台界面中输入此名称）
    - 警报状态
    - 解析（误报、真报、低优先级）
    - 分配给警报的用户的 ID 和名称
    - Kaspersky Security Center 云控制台数据库中的唯一 ID 以及与警报源事件相关的设备名称
    - 与警报源事件相关的设备用户的 SID 和名称
    - 可观察数据，即与警报源事件相关的可观察数据：
      - IP 地址
      - 文件和文件路径的 MD5 哈希和
      - 网址
      - 域
    - 与警报相关的对象的其他详细信息（从应用程序接收）
    - 警报注解：
      - 添加注解的日期和时间
      - 添加注解的用户

- 注解正文

- 警报变更日志：
  - 变更日期和时间
  - 执行更改的用户
  - 更改说明

14. 有关安全问题的数据：
    - 安全问题中第一个事件的日期和时间
    - 安全问题中最后事件的日期和时间
    - 安全问题名称（用户在 Kaspersky Security Center 云控制台界面中输入此名称）
    - 安全问题的简要描述
    - 安全问题优先级
    - 安全问题状态
    - 为安全问题分配的用户 ID 和名称
    - 解析（误报、真报、低优先级、已合并）
    - 对安全问题的注解：
      - 添加注解的日期和时间
      - 添加注解的用户
      - 注解正文
    - 安全问题变更日志：
      - 变更日期和时间
      - 执行更改的用户
      - 更改说明

15. 由卡巴斯基应用程序的数据加密功能处理的数据。

    受管理应用程序通过网络代理将下列数据从设备传输到管理服务器。用户在 Kaspersky Security Center 云控制台界面中输入驱动的显示名称和说明：

    a. 设备上的驱动器列表：
       - 驱动器名称
       - 加密状态
       - 驱动器类型（启动驱动器、磁盘驱动器）

- 驱动器序列号
- 描述

b. 设备上数据加密错误的详情：

- 错误发生的日期和时间
- 操作类型（加密、解密）
- 错误描述
- 文件路径
- 规则说明
- 设备 ID
- 用户名
- 错误 ID

c. 卡巴斯基应用程序的数据加密设置。
描述通过相应应用程序管理的设备的数据的部分给出了完整的数据列表。

16. 输入的激活码的详细信息。
用户在 Kaspersky Security Center 云控制台界面中输入数据。

17. 用户账户。
用户在 Kaspersky Security Center 云控制台界面中输入以下数据：

a. 名称

b. 描述

c. 完整名称

d. 邮件地址

e. 主电话号码

f. 密码

18. 使用 Active Directory 进行用户身份验证所需的数据：

a. Active Directory 联合身份验证服务 (ADFS) 设置：

- 身份验证提供商的主 URL
- ADFS 的受信任根证书
- ADFS 中生成的客户端 ID
- 用于保护 ADFS 访问的密钥

- 令牌的范围
- 执行集成的 Active Directory 域
- 包含用户 SID 的令牌字段的名称
- 包含用户组 SID 数组的令牌字段的名称

用户在 Kaspersky Security Center 云控制台界面中输入数据。

b. Kaspersky Security Center 云控制台自动从 ADFS 服务器接收的数据：

- 发行人（发行人）
- 用户授权端点（authorization_endpoint）
- 令牌端点（token_endpoint）
- JSON Web 密钥集 URI (jwks_uri)
- 访问令牌颁发者 (access_token_issuer)
- 用户信息端点（userinfo_endpoint）
- 结束会话端点 (end_session_endpoint)
- 令牌签名证书

19. 管理对象的修订历史：管理服务器、管理组、策略、任务、用户/安全组、安装包。
用户在 Kaspersky Security Center 云控制台界面中输入以下数据：

a. 管理服务器

b. 管理组

c. 策略

d. 任务

e. 用户/安全组

f. 安装包

20. 已删除的管理对象的注册表。
用户在 Kaspersky Security Center 云控制台界面中输入数据。

21. 从文件创建的安装包以及安装设置。
用户在 Kaspersky Security Center 云控制台界面中输入数据。

22. 在 Kaspersky Security Center 云控制台中显示 Kaspersky 公告所需的数据：

a. 有关用户使用的受管理卡巴斯基应用程序的信息：应用程序 ID、完整版本号。

b. Kaspersky Security Center 云控制台界面的用户本地化。

c. 有关设备上软件激活的信息：软件授权许可 ID；软件许可期限；软件授权许可到期日期和时间；使用的软件授权许可类型；软件订阅类型；软件订阅到期日期和时间；软件订阅的当前状态；软件订阅当前/更改状态的原因；购买软件授权许可的价目表项目的 ID。

d. 用户在使用本软件时所接受的法律协议信息：法律协议类型；法律协议的版本；指示用户是否已接受法律协议条款的标志。

e. 从权利人收到的公告信息：公告ID；收到公告的时间；收到公告的状态。

用户在 Kaspersky Security Center 云控制台界面中输入数据。

23. Kaspersky Security Center 云控制台用户设置。

用户在 Kaspersky Security Center 云控制台界面中输入以下数据：

a. 用户界面本地化语言

b. 用户界面主题

c. 监控面板显示设置

d. 有关通知状态的信息：已读/尚未读

e. 电子表格中列的状态：显示/隐藏

f. 教程进度

24. 在受管理设备上使用远程诊断功能接收到的数据：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、日志文件、从技术支持接收到的运行诊断脚本的结果。

25. 用户在 Kaspersky Security Center 云控制台界面中输入的数据：

a. 创建管理组层次结构时的管理组名称

b. 配置电子邮件通知时的电子邮件地址

c. 设备标签和标记规则

d. 应用程序标签

e. 应用程序的用户类别

f. 为用户分配角色时的角色名称

g. 有关子网的信息：子网名称、描述、地址和掩码

h. 报告和选择的设置

i. 用户输入的任何其他数据

26. 从本地部署的从属管理服务器接收的数据。

Kaspersky Kaspersky Security Center 在线帮助 中介绍了 Kaspersky Security Center 管理服务器处理的数据。

当连接本地部署的 Kaspersky Security Center管理服务器作为与 Kaspersky Security Center 云控制台相关的从属服务器时，Kaspersky Security Center 云控制台会处理来自从属管理服务器的以下类型的数据：

a. 作为在 Active Directory 网络或 Windows 网络中进行设备发现的结果，或通过扫描 IP 区间而收到的有关组织网络中的设备的信息。

b. 作为 Active Directory 网络轮询的结果而收到的有关 Active Directory 组织单位、域、用户和组的信息。

c. 有关受管理设备及其技术规格的信息，包括设备识别所需的规格、设备用户的账户及其工作会话

d. 使用 Exchange ActiveSync 协议传输的移动设备信息。

e. 使用 iOS MDM 协议传输的移动设备信息。

f. 设备上安装的卡巴斯基应用程序的详细信息：设置、操作统计数据、应用程序定义的设备状态、已安装和适用的更新、标签

g. 通过 Kaspersky Security Center 组件和卡巴斯基受管理应用程序的事件设置传输的信息

h. 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

i. Kaspersky Security Center 组件和 Kaspersky 受管理应用程序的任务设置

j. 漏洞和补丁管理功能处理的数据：应用程序和补丁的详细信息；有关硬件的信息；在受管理设备上检测到的第三方软件漏洞的详细信息；可用于第三方应用程序的更新的详细信息；WSUS 功能发现的 Microsoft 更新的详细信息

k. 应用程序的用户类别

l. “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

m. 备份区中放置的文件的详细信息

n. 隔离区中放置的文件的详细信息

o. Kaspersky 专家为进行详细分析而请求的文件详细信息

p. 自适应异常控制规则的状态和触发的信息

q. 安装或连接到受管理设备并被“应用程序控制”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。

r. 卡巴斯基应用程序的加密设置：加密密钥存储库、设备加密状态

s. 有关使用卡巴斯基应用程序的数据加密功能在设备上执行的数据加密错误的信息

t. 受管理可编程逻辑控制器 (PLC) 列表

u. 输入的激活码的详细信息

v. 用户账户

w. 管理对象的修订历史

x. 已删除的管理对象的注册表

y. 从文件创建的安装包以及安装设置

z. Kaspersky Security Center Web Console 用户设置

aa. 用户在管理控制台或 Kaspersky Security Center 云控制台界面中输入的任何数据

ab. 受管理设备与 Kaspersky Security Center 组件的安全连接的证书

27. 使用远程诊断功能时从受管理设备上传的信息：诊断文件（转储文件、日志文件、跟踪文件等）以及这些文件中包含的数据。

28. Kaspersky Security Center 云控制台与 SIEM 系统集成以进行事件导出所需的数据：

- 连接和身份验证所需的数据：
  - SIEM 系统连接地址和端口
  - SIEM 服务器身份验证证书
  - 用于 SIEM 系统中 Kaspersky Security Center 云控制台客户端身份验证的可信证书和私钥

  用户在 Kaspersky Security Center 云控制台界面中输入数据。
- Kaspersky Security Center 云控制台从 SIEM 系统接收的数据：用于 SIEM 服务器身份验证的 SIEM 服务器证书的公钥。

29. Kaspersky Security Center 云控制台与云环境交互所需的数据：

a. Amazon Web Services (AWS)：

- IAM 用户账户的访问密钥 ID
- IAM 用户账户的密钥

b. Microsoft Azure：

- Azure 应用程序 ID
- Azure 订阅 ID
- Azure 应用程序密码
- Azure 存储库的账户名
- Azure 存储库的账户访问密钥

c. Google Cloud：

- Google 客户端电子邮件
- 项目 ID
- 私钥

用户在 Kaspersky Security Center 云控制台界面中输入数据。

30. 由不受支持的卡巴斯基应用程序传输的数据

当您在已安装卡巴斯基应用程序但 Kaspersky Security Center 云控制台不支持的设备上安装网络代理时，该卡巴斯基应用程序仍会将数据传输到 Kaspersky Security Center 云控制台。（数据列表在应用程序帮助系统的"关于数据提供"部分中提供。）但是，Kaspersky Security Center 云控制台将无法按照处理过程的方式处理不受支持的应用程序传输的数据。描述了 Kaspersky Security Center 云控制台的主要功能。

Kaspersky Security Center 云控制台在线帮助中提供了受支持的卡巴斯基应用程序列表。

受管理应用程序运行所需的数据

以下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：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Security for Windows Server
- Kaspersky Security for Mobile
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux

已处理数据的列表发布在https://ksc.kaspersky.com/Home/LegalDocuments，位于 Kaspersky Security Center 云控制台数据处理协议中。在法律文档网页上，找到名为 Kaspersky Security Center 云控制台协议的文本块，然后向下滚动该文本块到通过相关受管理应用程序管理的设备的数据。您还可以使用浏览器的标准查找功能来达到相同的目的。

本地处理的用户数据

唯一可以在 Kaspersky Security Center 云控制台中部署的 Kaspersky Security Center 组件是网络代理。

本地处理的用户数据列表：

- 用户数据部分列出的所有数据均在卡巴斯基的框架和基础架构内处理，管理员通过 Kaspersky Security Center 云控制台界面输入的数据除外
- 网络代理的卡巴斯基事件日志
- 网络代理踪迹
- 日志，包括网络代理安装程序、Kaspersky Security Center 实用程序创建的日志

网络代理的转储、日志和跟踪文件包含随机数据，并且可能包含个人数据。文件以未加密的方式存储在安装了网络代理的设备上。文件不会自动传输到卡巴斯基。用户可以应技术支持的要求手动将该数据传输至卡巴斯基，以解决 Kaspersky Security Center 操作中的问题。

个人数据的其他处理者

除了卡巴斯基之外，下面还列出了 Kaspersky Security Center 云控制台的工作区相关个人数据的处理者。

组织名称及地址：
Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown
Dublin 18 D18 P521

服务：
Microsoft Azure（数据托管）

"选择用于存储 Kaspersky Security Center 云控制台信息的数据中心"部分列出了处理数据的国家/地区。

关于 Kaspersky Security Center 云控制台的法律文档

要使用 Kaspersky Security Center 云控制台，您必须阅读并表示同意Kaspersky Security Center 云控制台网站上指定的法律文件的条款和条件。当您登录 Kaspersky Security Center 云控制台管理工作区时，您可以查看 AO Kaspersky Lab 网站隐私政策的条款和条件。创建公司工作区时，您可以阅读 Kaspersky Security Center 云控制台协议和 Kaspersky Security Center 云控制台数据处理协议。

在开始使用 Kaspersky Security Center 云控制台之前，请仔细阅读所有法律文件的文本。

卡巴斯基应用程序的最终用户许可协议

最终用户授权许可协议（以下也称为"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，其中规定了您使用卡巴斯基程序应遵守的条款。

您可以使用以下方法浏览最终用户授权许可协议的条款：

- 在创建卡巴斯基应用程序安装包期间显示的窗口中。
- 在受管理设备上卡巴斯基应用程序安装文件夹中的 license.txt 文件中。

您可以随时撤销对最终用户许可协议的接受。

如果您不接受卡巴斯基应用程序许可协议的条款，您将无法使用该应用程序。

强化指南

Kaspersky Security Center 云控制台是由卡巴斯基托管和维护的应用程序。您不必在计算机或服务器上安装 Kaspersky Security Center 云控制台 。Kaspersky Security Center 云控制台允许管理员在公司网络中的设备上安装 Kaspersky 安全应用程序，远程运行扫描和更新任务，以及管理受管理应用程序的安全策略。

Kaspersky Security Center 云控制台旨在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 云控制台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 云控制台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，Kaspersky Security Center 云控制台需要增加保护方法。

强化指南描述了配置 Kaspersky Security Center 云控制台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：

- 配置账户以访问 Kaspersky Security Center 云控制台
- 管理客户端设备保护
- 配置受管理应用程序的保护
- 将信息传输到第三方应用程序

在开始使用 Kaspersky Security Center 云控制台之前，您会被提示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 Kaspersky Security Center 云控制台。

要阅读强化指南：

1. 打开 Kaspersky Security Center 云控制台并登录。Kaspersky Security Center 云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 Online Help 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 Kaspersky Security Center 云控制台。

当新版本的强化指南出现时，Kaspersky Security Center 云控制台将提示您阅读它。

Kaspersky Security Center 云控制台架构

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 云控制台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：

- 管理员工作区的组织以及连接到 Kaspersky Security Center 云控制台的方法
- 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

账户和身份验证

通过 Kaspersky Security Center 云控制台使用两步验证

Kaspersky Security Center 云控制台为用户提供了两步验证。

两步验证可以帮助您提高 Kaspersky Security Center 云控制台中账户的安全性。启用此功能后，每次使用电子邮件地址和密码登录 Kaspersky Security Center 云控制台时，您都会输入额外的一次性安全代码。您可以通过短信或在身份验证器应用程序中生成此代码（取决于您设置的两步验证方法）来接收一次性安全代码。

我们强烈建议不要在与 Kaspersky Security Center 云控制台建立连接的同一台设备上安装验证器应用程序。您可以在移动设备上安装验证器应用程序。

禁止保存管理员密码

如果您使用 Kaspersky Security Center 云控制台，**我们强烈建议不要**在用户设备上安装的浏览器中保存管理员密码。

如果浏览器遭到破坏，入侵者就可以访问已保存的密码。此外，如果保存密码的用户设备被盗或丢失，入侵者就可以访问受保护的数据。

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，用户创建工作区后，将向该用户分配主管理员角色。它对于管理很有用，但从安全角度来看也至关重要，因为主管理员角色拥有广泛的权限。应严格规范向用户分配此角色。

您可以使用具有一组预配置权限的预定义用户角色来管理 Kaspersky Security Center 云控制台。

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 云控制台功能的访问权限。

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。

管理客户端设备保护

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。
- 充当客户端设备的 KSN 代理服务器。

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）。

配置受管理应用程序的保护

配置网络保护

确保您已完成Kaspersky Security Center 云控制台初始配置方案。此方案还包括执行快速启动向导的步骤。

快速启动向导运行时，会创建带有默认参数的策略和任务。这些参数可能不是最佳的，甚至可能在您的组织中被禁止。因此，我们建议配置已创建的策略和任务，并根据组织网络的需要创建其他策略和任务。

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。

启用**使用卸载密码**还会启用 Kaspersky Security Center Web Console 删除工具 (cleaner.exe) 的密码保护。

配置卡巴斯基安全网络

在受管理应用程序的所有策略和 Kaspersky Security Center 云控制台属性中，我们建议启用卡巴斯基安全网络 (KSN) 的使用并接受 KSN 声明。当您更新或升级 Kaspersky Security Center 云控制台时，您可以接受更新后的 KSN 声明。

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。

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

为了及时响应紧急情况，我们建议配置 Kaspersky Security Center 云控制台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。

Kaspersky Security Center 云控制台的初始设置

本节概述了 Kaspersky Security Center 云控制台部署的主要方案，从创建工作区开始，到监控网络保护状态结束。

有关部署本地运行的 Kaspersky Security Center 的信息，请参阅Kaspersky Security Center 在线帮助。

我们建议您至少分配一个工作日来完成此方案。

该方案将指导您完成以下操作：

- 以管理员身份开始使用公司的工作区
- 发现网络上的设备（如有必要，您将分配分发点并在其上手动安装分发包）
- 在客户端设备上部署受管理的卡巴斯基应用程序；配置用于网络保护、监控以及定期更新卡巴斯基数据库、软件模块和应用程序的工具

完成此方案后，将配置基于卡巴斯基应用程序的网络保护。您将能够继续监控网络保护状态。

先决条件

在开始之前：

- 查看Kaspersky Security Center 云控制台的架构以了解主要应用程序组件之间的交互。
- 阅读有关 Kaspersky Security Center 云控制台和受管理应用程序授权许可的信息。
- 确保您拥有 Kaspersky Security Center 云控制台的有效激活码（如果您要创建商业工作区）。

阶段

Kaspersky Security Center 云控制台配置分阶段进行：

1. **配置端口**

   确保所有必要的端口均已打开，以便您的网络和卡巴斯基基础架构之间进行交互。此外，如果您计划使用管理服务器的层次结构，请确保所有必要的端口均已打开，以便与从属管理服务器（或多个从属管理服务器）和客户端设备进行交互。

2. **为您的公司创建工作区**

   创建一个账户，然后为您的公司创建一个工作区。

3. **运行快速启动向导**

   打开和登录 Kaspersky Security Center 云控制台。首次登录时，系统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。

   快速启动向导完成后，您将获得网络代理和安全应用程序的安装包。进一步部署 Kaspersky Security Center 云控制台需要这些安装包。

4. **部署卡巴斯基应用程序**

   执行卡巴斯基应用程序初始部署的方案。方案步骤之一涉及网络轮询操作。需要执行此操作来发现网络的客户端设备。网络轮询及其设置的描述请参见联网设备发现方案。

如果您要部署 Kaspersky Security for Windows Server，请确保该应用程序的数据库是最新的。

5. **授权许可卡巴斯基安全应用程序**

   当卡巴斯基安全应用程序部署到受管理设备时，必须通过向每个应用程序应用激活码来获得应用程序许可。将您的激活码部署到受管理设备上安装的卡巴斯基应用程序。您可以通过多种方式来获得卡巴斯基安全应用程序的许可。

6. **配置网络保护**

   执行网络保护配置以微调通过快速启动向导创建的策略和任务。

7. **定期更新 Kaspersky 数据库、软件模块和应用程序**

   为了保护您的网络免受病毒和其他威胁，您必须配置卡巴斯基数据库、软件模块和应用程序的定期更新。

8. **更新第三方软件并修复第三方软件漏洞（可选）**

   Kaspersky Security Center 云控制台使您能够管理 Microsoft 应用程序的更新 安装在客户端设备上。您还可以修复 Microsoft 应用程序中的漏洞 通过安装所需的更新。

9. **配置网络防护状态监控工具**

   选择和配置小部件、报告和其他工具，使您能够监控网络保护状态。

部署并配置 Kaspersky Security Center 云控制台后，您可以继续监控网络保护状态。

工作区管理

本节介绍如何在 Kaspersky Security Center 云控制台中使用账户和工作区。

关于 Kaspersky Security Center 云控制台中的工作区管理

使用 Kaspersky Security Center 云控制台，您可以做以下事情：

- 创建账户。
- 编辑账户。
- 注册公司并创建工作区。
- 编辑有关公司和工作区的信息。
- 删除工作区和公司。
- 删除账户。

Kaspersky Security Center 云控制台入门

本节介绍如何注册并开始使用 Kaspersky Security Center 云控制台。

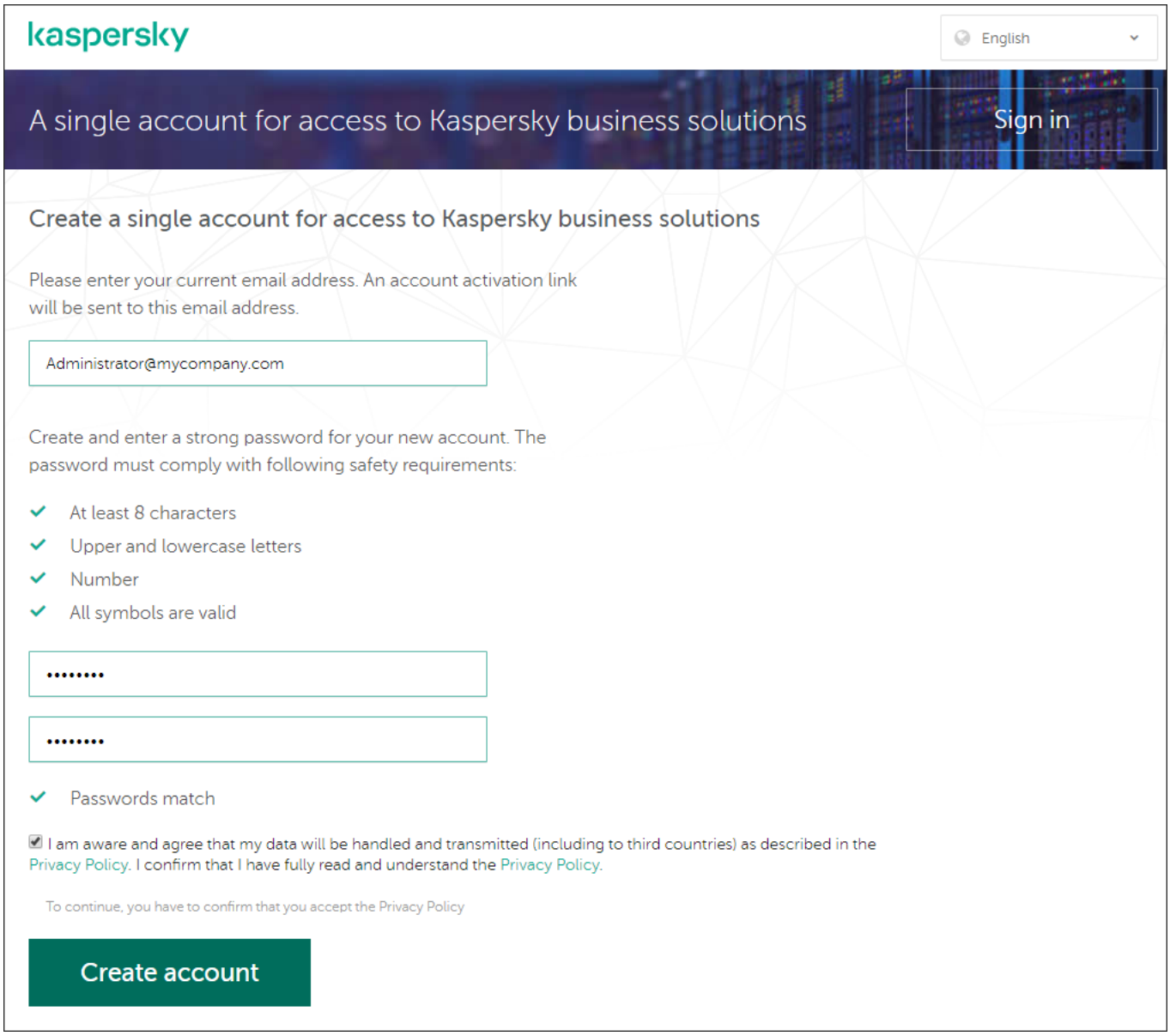
注册 Kaspersky Security Center 云控制台包括以下步骤：

1. 创建并确认账户。
2. 注册公司并创建工作区。

创建账户

要在 Kaspersky Security Center 云控制台中创建账户：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。
2. 单击 Kaspersky Security Center 云控制台开始页面上的**创建账户**按钮。
3. 在**创建用于访问卡巴斯基业务解决方案的单一账户**页面上，输入账户的电子邮件地址、密码和密码确认（见下图）。



在 Kaspersky Security Center 云控制台中创建账户

4. 单击**隐私政策**链接并仔细阅读隐私政策文本。

5. 如果您知道并同意您的数据将按照隐私政策中的描述进行处理和传输（包括传输到第三国），并且您确认您已完全阅读并理解隐私政策，请选中同意文本旁边的复选框根据隐私政策进行数据处理，然后单击**创建账户**按钮。

   如果您不接受隐私政策，请勿使用 Kaspersky Security Center 云控制台。

   仅当您选中该复选框后，该按钮才可用。

   将显示一个页面，提示您检查电子邮件。来自卡巴斯基的消息将发送到您指定的电子邮件地址。该消息包含用于完成账户创建过程的链接。

6. 关闭页面并打开邮箱中的电子邮件。

7. 单击卡巴斯基发送的消息中的链接进入您的账户页面。

8. 在**用户账户激活**页面上，单击**继续**按钮完成账户激活。

在 Kaspersky Security Center 云控制台中创建账户已完成。

注册公司并创建工作区

创建账户后，您可以立即注册公司并为其创建工作区。

如果您想要保护超过 10,000 台设备，则无需在 Kaspersky Security Center 云控制台 上注册公司并创建工作区如下所述。相反，请向卡巴斯基技术支持发送请求。在请求中，指定有关您的公司和您要创建的工作区的信息。

目前您只能注册一家公司并创建一个工作区。在 Kaspersky Security Center 云控制台的未来版本中，您将能够为您的公司创建其他工作区。通过为每个公司分支机构创建单独的工作区，这将帮助您将公司结构映射到工作区。

在您开始之前，确保了解如下内容：

- 您打算使用该软件解决方案的公司名称。
- 公司所在的国家。如果公司位于美国或加拿大，您还必须知道所在州或省。
- 您想要保护的公司计算机和移动设备的总数。

要在 Kaspersky Security Center 云控制台中注册公司并创建工作区：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台 。
2. 单击 Kaspersky Security Center 云控制台开始页面上的**"登录"**按钮。
3. 输入您在创建账户时指定的电子邮件地址和密码，然后单击**"登录"**按钮。
   创建工作区向导启动。使用**下一步**按钮进行向导。
4. 在向导**的步骤 01： Kaspersky Security Center 云控制台的使用条款**页面上，执行以下操作：
   a. 仔细阅读软件解决方案的协议、隐私政策和数据处理协议。
   b. 如果您同意本协议和数据处理协议的条款和条件，并且您知道并同意您的数据将按照隐私政策中的描述进行处理和传输（包括向第三国），并且您确认您已充分阅读并理解隐私政策，选中所列三个文档旁边的复选框，然后单击**"接受"**按钮。

   如果您不同意条款和条件，请勿使用 Kaspersky Security Center 云控制台。

   如果单击**"拒绝"**按钮，工作区创建过程将终止。
5. 在向导的**步骤 02：公司信息**页面上，指定贵公司的主要详细信息。
   填充以下字段：
   - **贵公司名称**（必填）

指定您打算使用该软件解决方案的公司名称。您可以输入最长 255 个字符的字符串。该字符串可以包含大写和小写字符、数字、空格、点、逗号、减号、破折号和下划线。指定的公司名称将显示在 Kaspersky Security Center 云控制台中。

- **附加公司描述**字段（可选）

  您可以指定有关您注册的公司的其他信息。您可以输入最长 255 个字符的字符串。该字符串可以包含大写和小写字符、数字、空格、点、逗号、减号、破折号和下划线。

6. 在向导的**步骤 03：工作区信息**页面上，指定有关您要为公司创建的工作区的信息。

   填充以下要求的字段：

   - **工作区名称**。指定您打算在其中使用软件解决方案的工作区的名称。您可以输入最长 255 个字符的字符串。该字符串可以包含大写和小写字符、数字、空格、点、逗号、减号、破折号和下划线。指定的工作区名称将显示在 Kaspersky Security Center 云控制台中。
   - **国家**。在下拉列表中，选择您的工作区所在的国家/地区。如果您选择美国或加拿大，还请在此字段下方显示的**州**下拉列表中指定州或省。
   - **设备数量**。输入您要在此工作区中保护的计算机和移动设备的总数。

     在输入字段中，您可以输入 300 到 10,000 之间的数字。

7. 在向导**的步骤 04：新工作区的授权许可**页面上，执行以下操作之一：

   - 如果您想尝试 Kaspersky Security Center 云控制台，请单击**我想请求试用工作区**链接。

     我们建议您将自己的设备连接到试用工作区，并测试对设置的任何修改，并记下结果。

     > 您将无法通过输入激活码将试用工作区切换到商业模式。要切换到商业模式，您必须删除工作区并重新创建它。

   - 如果您想在商业模式下使用 Kaspersky Security Center 云控制台，请输入激活码并单击**验证**按钮。

公司注册和 Kaspersky Security Center 云控制台中工作区的创建已完成。

准备好工作区后，您会收到一封电子邮件，其中包含用于访问工作区的链接。

打开 Kaspersky Security Center 云控制台工作区

为 Kaspersky Security Center 云控制台创建工作区后，该工作区会自动打开。稍后，您可以打开工作区，如本节中所述。

如果您是虚拟管理服务器的管理员，则您只能访问虚拟管理服务器。登录并打开工作区后， Kaspersky Security Center 云控制台为您提供虚拟管理服务器的界面。您无法切换到主管理服务器或其他从属管理服务器。

> 虚拟管理服务器的管理员必须有权访问单个虚拟管理服务器。如果您没有主服务器的访问权限，但有多个虚拟服务器的访问权限，您将无法登录 Kaspersky Security Center 云控制台。

要打开 Kaspersky Security Center 云控制台工作区：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。

2. 通过指定用户名和密码在 Kaspersky Security Center 云控制台上登录您的账户。

3. 如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。

   门户页面显示您作为管理员的公司及其工作区列表。

4. 单击所需工作区的名称或**"转到工作区"**链接以继续进入该工作区。

   有时，工作区可能因维护而不可用。如果是这种情况，您将无法继续访问 Kaspersky Security Center 云控制台工作区。

   > 您无法打开标记为删除的工作区。

5. 如果自您接受其条款和条件后 Kaspersky Security Center 云控制台的任何法律文档发生更改，门户页面将显示更改的文档。

   执行以下操作：

   a. 仔细阅读显示的文档。

   b. 如果您同意所显示文档的条款和条件，请选中所列文档旁边的复选框，然后单击**我接受条款**按钮。

   > 如果您不同意条款和条件，请停止使用所选的卡巴斯基软件解决方案。

   > 如果单击**"我拒绝"**按钮，操作将终止。

您的 Kaspersky Security Center 云控制台工作区将打开。

退出 Kaspersky Security Center 云控制台

完成工作后，您应该通过注销 Kaspersky Security Center 云控制台来安全地关闭当前会话。

要退出 Kaspersky Security Center 云控制台，

在主菜单中，转到您的账户设置，然后选择**登出**。

Kaspersky Security Center 云控制台被关闭，且账户页面被显示。如有必要，您可以关闭此浏览器页面。您工作区中的所有数据都将被保存。

管理公司和工作区列表

本节介绍如何在 Kaspersky Security Center 云控制台中查看您账户下注册的公司信息和工作区列表、更改有关公司和工作区的信息以及删除工作区和公司。

目前您只能注册一家公司并创建一个工作区。在 Kaspersky Security Center 云控制台的未来版本中，您将能够为您的公司创建其他工作区。通过为每个公司分支机构创建单独的工作区，这将帮助您将公司结构映射到工作区。

编辑有关公司和工作区的信息

您可以修改有关公司和将公司添加到 Kaspersky Security Center 云控制台时指定的工作区的信息。

要修改有关公司和/或工作区的信息：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。
2. 通过指定用户名和密码在 Kaspersky Security Center 云控制台上登录您的账户。
3. 如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。
   门户页面显示您作为管理员的公司及其工作区列表。
4. 如果您想编辑公司名称和描述，请执行以下操作：
   a. 单击包含公司信息的区域中的**编辑**（ ）图标。
   b. 根据需要修改公司名称和/或描述。
   c. 单击“**保存**”按钮。
      要取消更改，请单击**“取消”**按钮。
5. 如果要编辑工作区名称，请执行以下操作：
   a. 单击包含工作区信息的区域中的**编辑**（ ）图标。
   b. 根据需要修改工作区名称。
   c. 单击“**保存**”按钮。
      要取消更改，请单击**“取消”**按钮。

修改后的信息将显示在 Kaspersky Security Center 云控制台中。

删除工作区和公司

公司的工作区可以手动或自动删除。删除最后一个工作区后，公司信息也会自动删除。

手动删除

如果公司决定停止使用该工作区，您可以删除该公司的工作区。

> 删除工作区后，所有安全应用程序将保留在受管理设备上。因此，我们建议在删除工作区之前禁用所有安全应用程序的密码保护或从受管理设备中卸载安全应用程序。

要删除工作区和公司：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。

2. 通过指定用户名和密码在 Kaspersky Security Center 云控制台上登录您的账户。

3. 如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。

   门户页面显示您作为管理员的公司及其工作区列表。

4. 选择您要删除的工作区。

5. 在右侧包含所选工作区的部分中，单击**删除**（ ） 图标。

   “删除工作区”窗口将打开。

6. 在**“删除工作区”**窗口中，确认您要删除该工作区。

工作区被标记为删除。工作区的信息块以红色边框突出显示。

工作区的信息块复制在页面底部的**“标记为删除”**部分中。

您无法转到标记为删除的工作区并对其进行管理。

如果您无法将工作区标记为删除，请联系卡巴斯基技术支持。卡巴斯基的技术支持工程师收到您的请求后，工作区和公司将被删除。

标记为删除的工作区在标记后可能会保留该状态 7 天。7 天后，它们将被自动删除。

在此期间，您可以强制删除标记为删除的工作区或取消删除工作区。

强制删除工作区：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。

2. 通过指定用户名和密码在 Kaspersky Security Center 云控制台上登录您的账户。

3. 如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。

   门户页面显示您作为管理员的公司及其工作区列表。

4. 在**“标记为删除”**部分中，在标记为删除的工作区的信息块中，单击**“强制删除”**选项。

   “删除工作区”窗口将打开。

5. 在**“删除工作区”**窗口中，输入要删除的工作区的 ID。

   系统会提示您确认工作区 ID，以确保您没有错误地删除工作区。工作区删除后将无法恢复。

   工作区 ID 显示在其名称下的工作区信息部分中。

6. 在**删除工作区**窗口，单击“**OK**”。

工作区即被删除。有关用户、受管理设备及其设置的所有数据都将被删除。

自动删除

Kaspersky Security Center 云控制台自动删除工作区：

- 试用授权许可到期后 30 天。
- 管理服务器存储库中的所有商业或订阅授权许可到期后 90 天。
- 删除存储库中手动添加的最后一个授权许可密钥（有效、保留或未使用）后 90 天。

Kaspersky Security Center 云控制台会在删除前 30 天、7 天和 1 天通知工作区管理员。

取消删除工作区

您可以取消删除已标记为删除的工作区。

> 您无法取消删除已删除的工作区。

要取消删除工作区：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。
2. 通过指定用户名和密码在 Kaspersky Security Center 云控制台上登录您的账户。
3. 如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。

   门户页面显示您作为管理员的公司及其工作区列表。
4. 在**“标记为删除”**部分中，在标记为删除的工作区的信息块中，单击**“取消删除”**链接。

工作区删除已取消。您现在可以转到工作区并继续使用它。

管理对公司及其工作区的访问

本部分包含有关授予和撤销对公司及其工作区的访问权限的信息。

Kaspersky Security Center 云控制台为您提供两种访问级别：

- **管理员**

  具有此访问级别的用户可以完全管理公司及其工作区。
- **用户**

  具有此访问级别的用户可以查看可用工作区列表并进入这些工作区。

授予对您的公司及其工作区的访问权限

如果您希望其他用户能够登录您的公司并根据所选的访问级别对其进行管理，您可以授予对您的公司及其工作区的访问权限。

在您授予用户访问权限之前，用户必须在 Kaspersky Security Center 云控制台中创建账户。

要授予对您的公司及其工作区的访问权限：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。
2. 通过指定用户名和密码在 Kaspersky Security Center 云控制台上登录您的账户。
3. 如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。

   门户页面显示您作为管理员的公司及其工作区列表。
4. 单击**显示访问控制**链接。

   有权访问公司的账户列表不断扩大。
5. 单击**授予访问权限**链接。
6. 在**电子邮件地址**字段中，指定您要授予访问权限的账户的电子邮件地址。
7. 在**访问级别**列表中，选择要分配给输入账户的访问级别：

   - **管理员**

     具有此访问级别的用户可以完全管理公司及其工作区。
   - **用户**

     具有此访问级别的用户可以查看可用工作区列表并进入这些工作区。

   您不能向同一公司内的同一账户授予多个访问级别。
8. 单击“**授予**”按钮。

指定的账户被授予对您的公司及其工作区的访问权限。用户可以根据选择的访问级别登录公司并进行管理。

如果您已授予账户**“用户”**访问级别，则必须为添加的用户分配角色。否则，用户将无法进入工作区。

撤销对您的公司及其工作区的访问权限

如果您不再希望用户能够登录您的公司并对其进行管理（例如，在用户退出公司后），您可以撤销对您的公司及其工作区的访问权限。

您无法撤销自己对公司的访问权限。

要撤销对您的公司及其工作区的访问权限：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。

2. 通过指定用户名和密码在 Kaspersky Security Center 云控制台上登录您的账户。

3. 如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。

   门户页面显示您作为管理员的公司及其工作区列表。

4. 单击**显示访问控制**链接。

   有权访问公司的账户列表不断扩大。

5. 单击**撤销**( )图标位于您要撤销其访问权限的账户旁边。

6. 在打开的**"撤消对公司的访问权限"**窗口中，单击**"确定"**确认操作。

所选账户对您的公司及其工作区的访问权限将被撤销。用户无法再登录公司并进行管理。

重置您的密码

如果您忘记了Kaspersky Security Center 云控制台账户的密码，您可以通过重置密码来恢复对账户的访问权限。

重置账户密码：

1. 在您的浏览器中，转到Kaspersky Security Center 云控制台。

2. 单击**登录**按钮，然后单击**忘记密码？**关联。

3. 输入您在创建账户时指定的电子邮件地址。

4. 单击**重置密码**。

   包含重置密码链接的电子邮件将发送到指定地址。

5. 单击电子邮件中的链接。

6. 在打开的窗口中，输入新密码并确认。

7. 如果您配置了秘密问题，请回答此问题。

   如果您设置了两步验证，请输入通过短信发送给您或在身份验证器应用程序中生成的一次性安全代码（取决于您设置的两步验证方法）。

8. 单击**继续**。

   用于登录 Kaspersky Security Center 云控制台的新密码已保存。

如果您没有收到电子邮件，请检查您输入的电子邮件地址、垃圾邮件文件夹，然后重试。如果您重试时没有收到消息，则您指定的电子邮件地址可能未在网站上注册。请联系卡巴斯基技术支持。

在 Kaspersky Security Center 云控制台中编辑账户设置

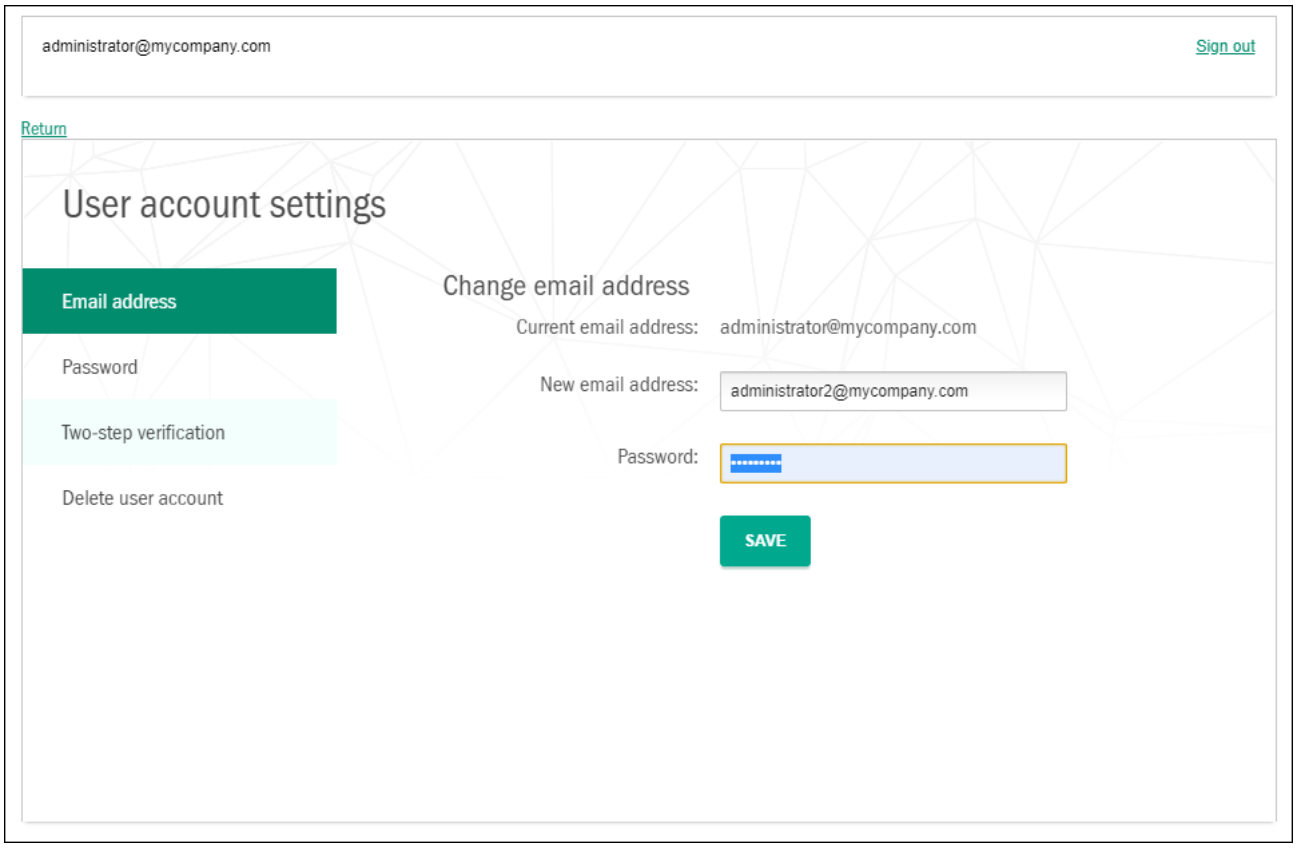
本部分提供有关如何在 Kaspersky Security Center 云控制台中编辑和删除账户的说明。

更改电子邮件地址

要在 Kaspersky Security Center 云控制台的账户设置中更改您的电子邮件地址：

1. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。
   用户账户设置窗口打开。

2. 选择**电子邮件地址**部分（见下图）。



在 Kaspersky Security Center 云控制台的账户设置中更改电子邮件地址

电子邮件地址部分显示您当前的电子邮件地址、用于输入新地址的输入字段、用于输入密码的输入字段以及**保存**按钮。

3. 在**新电子邮件地址**输入字段中，输入您的新电子邮件。
   请仔细输入地址。如果您输入的地址无效，您将无法继续访问您的账户并使用 Kaspersky Security Center 云控制台。

4. 在**密码**输入字段中，输入您当前的密码。

5. 单击**"保存"**按钮。

6. 单击**"返回"**链接返回 Kaspersky Security Center 云控制台，或单击**"退出"**链接退出门户。

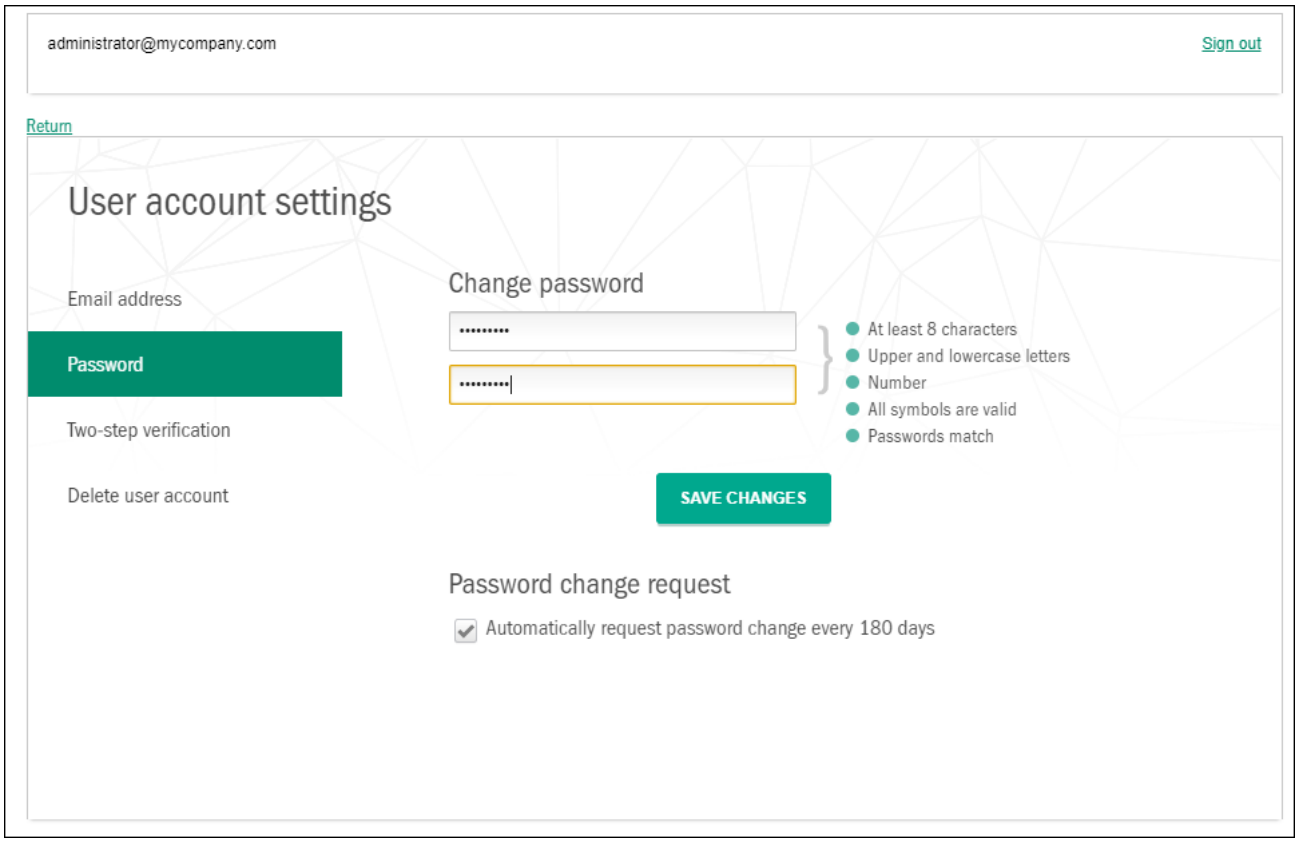
您的电子邮件地址现已在 Kaspersky Security Center 云控制台账户设置和"我的卡巴斯基"中更改帐号设定。系统会向您的新电子邮件地址发送一条消息，通知您用于访问账户的电子邮件地址已更改。下次登录 Kaspersky Security Center 云控制台时，您必须指定新的电子邮件地址。

更改密码

要在 Kaspersky Security Center 云控制台的账户设置中更改密码：

1. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。
   用户账户设置窗口打开。

2. 选择**密码**部分（见下图）。



在 Kaspersky Security Center 云控制台中更改账户密码

   此部分显示用于输入新密码并确认的字段，以及**"保存更改"**按钮。

3. 输入新密码并在相应的输入字段中确认。
   密码输入字段的右侧显示了密码要求。在遵守要求之前，您无法保存新密码。

4. 选中或清除**每 180 天自动请求更改密码**复选框。
   默认情况下已选中该选框。

5. 单击**"保存更改"**按钮。

6. 单击**"返回"**链接返回 Kaspersky Security Center 云控制台，或单击**"退出"**链接退出门户。

   您的密码现已更改。登录 Kaspersky Security Center 云控制台和登录"我的卡巴斯基"时，您必须输入新密码。

使用两步验证

本节介绍两步验证，可以帮助您提高 Kaspersky Security Center 云控制台中账户的安全性。

关于两步验证

两步验证可以帮助您提高 Kaspersky Security Center 云控制台中账户的安全性。启用此功能后，每次使用电子邮件地址和密码登录 Kaspersky Security Center 云控制台时，您都会输入额外的一次性安全代码。通过两步验证，犯罪分子如果窃取或猜出您的密码，就无法登录您的账户，他们也必须能够访问您的手机。此外，启用两步验证后，如果您忘记密码，则必须输入额外的一次性安全码。

设置两步验证后，您有责任确保手机的物理安全并保持对您的电话号码的访问。

您可以通过以下方式之一获取一次性安全码：

- 安全代码通过短信发送到您的手机号码。

  在这种情况下，如果您无法访问您的手机，您将无法在 Kaspersky Security Center 云控制台中登录您的账户，直到您恢复对您的电话号码的访问。

- 安全代码在安装在移动设备上的认证应用中生成。

  我们强烈建议您使用身份验证器应用程序设置两步验证。在这种情况下，即使您的手机未连接到互联网或移动网络，您也可以登录您的账户。

  我们仅测试了 Google Authenticator 和 Microsoft Authenticator 与 Kaspersky Security Center 云控制台的兼容性，并且这些应用程序当时是免费使用的。这些应用程序的界面可能不支持您的首选语言。在使用应用程序之前，还请检查其 GDPR 合规性和隐私政策。卡巴斯基与这些应用程序的任何所有者没有任何赞助、认可或以其他方式关联。

  > Microsoft Authenticator 只能安装在移动设备上。

  我们还建议您在手机以外的设备上安装身份验证器应用程序。如果您的手机丢失或被盗，这将允许您登录您的账户。

  在这种情况下，如果您无法访问您的手机，并且您在其他设备上没有身份验证器应用程序，则在您恢复对您的电话号码的访问之前，您将无法在 Kaspersky Security Center 云控制台中登录您的账户。之后，使用通过短信发送的安全码。

> 如果您之前配置了密保问题以在密码丢失时恢复密码，则在您设置两步验证后，密保问题功能将被永久禁用。

方案：设置两步验证

两步验证可以帮助您提高 Kaspersky Security Center 云控制台中账户的安全性。完成本部分中的方案后，将设置您的账户的两步验证。

方案实施分为几个阶段：

1. **添加您的电话号码**

   在此阶段，您可以通过短信设置两步验证。

2. **安装和配置身份验证器应用程序**

   安装和配置身份验证器应用。

我们强烈建议您使用身份验证器应用程序设置两步验证。在这种情况下，即使您的手机未连接到互联网或移动网络，您也可以登录您的账户。

我们还建议您在手机以外的设备上安装身份验证器应用程序。如果您的手机丢失或被盗，这将允许您登录您的账户。

3 **更改您的电话号码**

如有必要，您可以更改用于两步验证的电话号码。

设置短信两步验证

设置短信两步验证：

1. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。

   用户账户设置窗口打开。

2. 选择**两步验证**部分。

3. 单击**设置**按钮。

4. 在**“输入您的当前密码”**下，指定您在 Kaspersky Security Center 云控制台中的账户密码，然后单击**“继续”**按钮。

5. 在**“指定您的手机号码”**下，指定您想要在两步验证中使用的手机号码，然后单击**“下一步”**按钮。

   > 您最多可以将同一个电话号码用于五个账户。

   6 位安全码将发送到指定的电话号码。

6. 在**确认您的电话号码**下，输入收到的安全码。

设置两步验证。现在，每次您使用电子邮件地址和密码登录时，或者如果您忘记了密码，您都需要输入通过短信发送到指定电话号码获得的一次性安全代码。

您现在可以安装和配置身份验证器应用程序、更改您的电话号码或禁用两步验证。

使用身份验证器应用设置两步验证

身份验证器应用程序不能在 Kaspersky Security Center 云控制台中用作独立的验证方法。您必须首先通过短信设置两步验证。如果您通过手机号码禁用两步验证，则通过身份验证器应用程序进行的验证将自动关闭。通过短信和应用程序设置验证后，您将能够在登录页面上选择验证方法，或者在忘记密码时选择验证方法。

要通过身份验证器应用程序设置两步验证：

1. 设置短信两步验证。

2. 下载、安装并运行您要使用的认证应用。

我们仅测试了 Google Authenticator 和 Microsoft Authenticator 与 Kaspersky Security Center 云控制台的兼容性，并且这些应用程序当时是免费使用的。这些应用程序的界面可能不支持您的首选语言。在使用应用程序之前，还请检查其 GDPR 合规性和隐私政策。卡巴斯基与这些应用程序的任何所有者没有任何赞助、认可或以其他方式关联。

Microsoft Authenticator 只能安装在移动设备上。

如果需要，您可以使用其他应用，但风险自负。您使用的应用必须支持 6 位安全代码。

我们还建议您在手机以外的设备上安装身份验证器应用程序。如果您的手机丢失或被盗，这将允许您登录您的账户。

3. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。

   用户账户设置窗口打开。

4. 选择**两步验证**部分。

5. 单击**获取密钥**按钮。

6. 在**“输入您的当前密码”**下，指定您在 Kaspersky Security Center 云控制台中的账户密码，然后单击**“继续”**按钮。

   门户页面显示 16 个字符的密钥和二维码。

7. 在每台设备上的认证应用中，创建一个账户并输入显示的密钥。或者，您也可以使用手机扫描二维码。在这种情况下，该账户将自动创建。请参阅您的应用程序的文档以获取更多信息。

   您的认证应用中会生成 6 位安全代码。

8. 验证您的应用程序中生成的安全代码在每台设备上是否相同。

9. 在 Kaspersky Security Center 云控制台中，输入生成的安全代码。

设置了认证应用的两步验证。现在，每次使用电子邮件地址和密码登录时，或者如果忘记密码，您都需要输入在认证应用中生成的一次性安全代码。

您现在可以禁用认证应用的使用或完全禁用两步验证。

更改您的手机号码

修改短信两步验证使用的手机号码：

1. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。

   用户账户设置窗口打开。

2. 选择**两步验证**部分。

3. 在**“电话号码”**下，单击**“更改电话号码”**链接。

4. 在**“指定您的手机号码”**下，指定要在两步验证中使用的新手机号码，然后单击**“下一步”**按钮。

5. 在**“输入您的当前密码”**下，指定您在 Kaspersky Security Center 云控制台中的账户密码，然后单击**“继续”**按钮。

   6 位安全码将发送到指定的电话号码。

6. 在**确认您的电话号码**下，输入收到的安全码。

您的手机号码已更改。现在，一次性安全代码将发送到新的电话号码。

禁用两步验证

如果您不想再使用两步验证，可以禁用它，如本节中所述。

禁用两步验证会降低您账户的安全性。我们强烈建议您继续使用两步验证。

如果您设置了短信两步验证，则可以禁用两步验证。如果您通过认证应用设置了两步验证，则可以禁用该应用程序或完全禁用两步验证。

要禁用认证应用的使用：

1. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。

   用户账户设置窗口打开。

2. 选择**两步验证**部分。

3. 在**认证应用**下，单击**禁用认证应用**链接。

4. 在**“输入您的当前密码”**下，指定您在 Kaspersky Security Center 云控制台中的账户密码，然后单击**“继续”**按钮。

   验证器应用使用已被禁用。删除了验证器应用程序的两步验证设置。您现在可以删除身份验证器应用中的账户。

   稍后，您可以再次通过身份验证器应用设置两步验证。

要完全禁用两步验证：

1. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。

   用户账户设置窗口打开。

2. 选择**两步验证**部分。

3. 在**电话号码**下，单击**禁用两步验证**链接。

4. 在**“输入您的当前密码”**下，指定您在 Kaspersky Security Center 云控制台中的账户密码，然后单击**“继续”**按钮。

   两步验证已禁用。如果您通过身份验证器应用使用了两步验证，则两步验证的设置将被删除。您现在可以删除身份验证器应用中的账户。

   稍后，您可以再次设置两步验证。

在 Kaspersky Security Center 云控制台中删除帐户

如果您想停止使用 Kaspersky Security Center 云控制台，您可以删除您的账户。

删除账户时，与该账户关联的所有数据都会丢失。

删除账户后，您将无法再访问 Kaspersky Endpoint Security Cloud、Kaspersky Security for Microsoft Office 365 和 Kaspersky Security Center 云控制台中的工作区。如果您是工作区中唯一的管理员，则该工作区将被正式删除。此外，您将无法访问“我的卡巴斯基”账户。

要在 Kaspersky Security Center 云控制台中删除账户：

1. 在 Kaspersky Security Center 云控制台中，单击包含您的账户名的链接，然后选择**管理用户账户**。
   用户账户设置窗口打开。
2. 选择**删除用户账户**部分。
   删除用户账户部分显示有关账户删除后果的信息，以及该信息下方的**删除**按钮。
3. 请阅读有关账户删除的信息，然后单击**“删除”**按钮。
   将打开**“输入您的用户账户密码”**窗口。
4. 在密码输入字段中，输入您的密码，然后单击**继续**按钮。

您的账户已被删除。

选择用于存储 Kaspersky Security Center 云控制台信息的数据中心

Kaspersky Security Center 云控制台的工作区是使用基于 Microsoft Azure 云平台的全球数据中心网络中的服务器创建的。托管工作区的数据中心的选择取决于您在 Kaspersky Security Center 云控制台中注册工作区时指定的国家/地区（请参见下表）。安全应用程序的分发包托管在与工作区相同的服务器上。

将公司位置与 Microsoft Azure 区域相匹配

公司所在国家	微软数据中心区域
阿根廷	巴西南部
波利维亚	巴西南部
巴西	巴西南部
智利	巴西南部
哥伦比亚	巴西南部
厄瓜多尔	巴西南部
圭亚那	巴西南部
秘鲁	巴西南部
巴拉圭	巴西南部
苏里南	巴西南部
乌拉圭	巴西南部
委内瑞拉	巴西南部

安提瓜和巴布达	美国东部
安圭拉岛	美国东部
阿鲁巴	美国东部
巴巴多斯	美国东部
圣巴泰勒米岛	美国东部
博内尔岛、圣尤斯特歇斯岛和萨巴岛	美国东部
伯利兹	美国东部
哥斯达黎加	美国东部
古巴	美国东部
库拉索岛	美国东部
多米尼加	美国东部
多米尼加共和国	美国东部
格林纳达	美国东部
瓜德罗普	美国东部
危地马拉	美国东部
洪都拉斯	美国东部
海地	美国东部
牙买加	美国东部
圣基茨和尼维斯联邦	美国东部
开曼群岛	美国东部
圣卢西亚	美国东部
圣马丁岛	美国东部
马提尼克岛	美国东部
蒙特塞拉特	美国东部
尼加拉瓜	美国东部
巴拿马	美国东部
波多黎各	美国东部
圣马丁岛	美国东部
特立尼达和多巴哥	美国东部
圣文森特和格林纳丁斯	美国东部
英属维尔京群岛	美国东部
美属维尔京群岛	美国东部
日本	美国东部
加拿大（新不伦瑞克省）	美国东部
加拿大（纽芬兰和拉布拉多）	美国东部
加拿大（新斯科舍省）	美国东部

加拿大（安大略省）	美国东部
加拿大（爱德华王子岛）	美国东部
加拿大（魁北克）	美国东部
美利坚合众国（阿拉巴马州）	美国东部
美利坚合众国（阿肯色州）	美国东部
美利坚合众国（康涅狄格州）	美国东部
美利坚合众国（哥伦比亚特区）	美国东部
美利坚合众国（特拉华州）	美国东部
美利坚合众国（佛罗里达州）	美国东部
美利坚合众国（乔治亚州）	美国东部
美利坚合众国（爱荷华州）	美国东部
美利坚合众国（伊利诺伊州）	美国东部
美利坚合众国（印第安纳州）	美国东部
美利坚合众国（肯塔基州）	美国东部
美利坚合众国（路易斯安那州）	美国东部
美利坚合众国（马萨诸塞州）	美国东部
美利坚合众国（马里兰州）	美国东部
美利坚合众国（缅因州）	美国东部
美利坚合众国（密歇根州）	美国东部
美利坚合众国（明尼苏达州）	美国东部
美利坚合众国（密苏里州）	美国东部
美利坚合众国（密西西比州）	美国东部
美利坚合众国（北卡罗来纳州）	美国东部
美利坚合众国（新罕布什尔州）	美国东部
美利坚合众国（新泽西州）	美国东部
美利坚合众国（纽约）	美国东部
美利坚合众国（俄亥俄州）	美国东部
美利坚合众国（宾夕法尼亚州）	美国东部
美利坚合众国（罗德岛州）	美国东部
美利坚合众国（南卡罗来纳州）	美国东部
美利坚合众国（田纳西州）	美国东部
美利坚合众国（弗吉尼亚州）	美国东部
美利坚合众国（佛蒙特州）	美国东部
美利坚合众国（威斯康星州）	美国东部
美利坚合众国（西弗吉尼亚州）	美国东部
阿尔巴尼亚	北欧（爱尔兰）

波西尼亚及黑塞哥维那	北欧（爱尔兰）
保加利亚	北欧（爱尔兰）
白俄罗斯	北欧（爱尔兰）
捷克共和国	北欧（爱尔兰）
丹麦	北欧（爱尔兰）
爱沙尼亚	北欧（爱尔兰）
芬兰	北欧（爱尔兰）
英国	北欧（爱尔兰）
格陵兰	北欧（爱尔兰）
希腊	北欧（爱尔兰）
克罗地亚	北欧（爱尔兰）
匈牙利	北欧（爱尔兰）
爱尔兰	北欧（爱尔兰）
冰岛	北欧（爱尔兰）
吉尔吉斯斯坦	北欧（爱尔兰）
哈萨克斯坦	北欧（爱尔兰）
立陶宛	北欧（爱尔兰）
拉脱维亚	北欧（爱尔兰）
摩尔多瓦共和国	北欧（爱尔兰）
黑山	北欧（爱尔兰）
马其顿共和国	北欧（爱尔兰）
蒙古	北欧（爱尔兰）
挪威	北欧（爱尔兰）
波兰	北欧（爱尔兰）
罗马尼亚	北欧（爱尔兰）
塞尔维亚	北欧（爱尔兰）
俄罗斯联邦	北欧（爱尔兰）
瑞典	北欧（爱尔兰）
斯洛文尼亚	北欧（爱尔兰）
斯洛伐克	北欧（爱尔兰）
塔吉克斯坦	北欧（爱尔兰）
土库曼斯坦	北欧（爱尔兰）
乌兹别克斯坦	北欧（爱尔兰）
加拿大（艾伯塔省）	美国西部
加拿大（不列颠哥伦比亚省）	美国西部
加拿大（马尼托巴省）	美国西部

加拿大（西北地区）	美国西部
加拿大（努勒维特）	美国西部
加拿大（育空地区）	美国西部
加拿大（萨斯喀彻温省）	美国西部
墨西哥	美国西部
美利坚合众国（阿拉斯加）	美国西部
美利坚合众国（亚利桑那州）	美国西部
美利坚合众国（加利福尼亚州）	美国西部
美利坚合众国（科罗拉多州）	美国西部
美利坚合众国（夏威夷）	美国西部
美利坚合众国（爱达荷州）	美国西部
美利坚合众国（堪萨斯州）	美国西部
美利坚合众国（蒙大拿州）	美国西部
美利坚合众国（北达科他州）	美国西部
美利坚合众国（内布拉斯加州）	美国西部
美利坚合众国（新墨西哥州）	美国西部
美利坚合众国（内华达州）	美国西部
美利坚合众国（俄克拉荷马州）	美国西部
美利坚合众国（俄勒冈州）	美国西部
美利坚合众国（南达科他州）	美国西部
美利坚合众国（德克萨斯州）	美国西部
美利坚合众国（犹他州）	美国西部
美利坚合众国（华盛顿）	美国西部
美利坚合众国（怀俄明州）	美国西部
美利坚合众国（其他行政区划）	美国东部
其他国家	西欧（荷兰）

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 云控制台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客户端设备的公共 IP 地址，因为网络代理建立了到 DNS 服务器的 TCP/UDP 连接。如果 Kaspersky Security Center 云控制台使用公共 DNS 服务器，则数据处理受相关服务的隐私政策约束。

方案：创建通过 Kaspersky Security Center 云控制台管理的管理服务器层次结构

此方案描述了创建通过 Kaspersky Security Center 云控制台管理的管理服务器层次结构所必须执行的操作，服务器从而承担主管理服务器的角色。此层次结构随后可用于将受管理设备和对象从Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台，以及通过 Kaspersky Security Center 云控制台管理从属管理服务器和设备。

Kaspersky Security Center 云控制台只能充当主管理服务器，而本地运行的管理服务器只能充当从属管理服务器。其他分层方案不可用。

先决条件

在开始之前，请确保满足以下先决条件：

- 将内部运行的管理服务器升级到版本 12 或更高版本。
- 在内部运行的管理服务器上安装 Kaspersky Security Center Web Console。
- 为要通过 Kaspersky Security Center 云控制台管理的应用程序安装 Web 插件。
- 将受管理应用程序升级到 Kaspersky Security Center 云控制台支持的版本。
- 确保本地运行的管理服务器上的“下载管理服务器存储库更新”任务没有将主管理服务器指定为更新源；如有必要，相应地修改任务设置。

创建层次结构后，Kaspersky Security Center 云控制台中有效的策略和任务将应用到从属管理服务器上，从而取代其现有策略和任务。如果您想避免此行为，请在创建层次结构之前删除Kaspersky Security Center 云控制台的所有策略和任务。或者，您可以在其设置中将每个Kaspersky Security Center 云控制台策略的状态更改为**不活动**，并在每个Kaspersky Security Center 云控制台任务的设置中禁用**分发到从属和虚拟管理服务器**”选项。

如有必要，您可以随时删除管理服务器的层次结构。

层次结构创建的阶段

基本方案提供了无法通过 Internet 访问的从属管理服务器。但是，如果可以通过 Internet 访问从属管理服务器，则下面描述的某些步骤中的一组操作可能会有所不同。此外，在这种情况下必须跳过某些步骤。

管理服务器层次结构的创建包括以下阶段：

1. **检索从属管理服务器的证书**

   如果从属管理服务器可通过互联网访问，请跳过此步骤。

在本地运行的 Kaspersky Security Center Web Console 中，打开管理服务器属性，然后在**常规**选项卡上打开**常规**部分。单击**查看管理服务器证书**链接。CER 格式的证书文件会自动保存在浏览器设置中指定的文件夹中。

2. 从 Kaspersky Security Center 云控制台检索连接设置和证书

如果从属管理服务器可通过互联网访问，请跳过此步骤。

在 Kaspersky Security Center 云控制台中，打开管理服务器属性，然后在**常规**选项卡上打开**管理服务器层级**部分。以下连接设置将显示：

- HDS 地址

  显示用于连接到托管发现服务 (HDS) 的网址。

- HDS 端口

  显示用于连接 HDS 的端口号。

该部分还包含两个链接：

- 查看管理服务器证书

  单击此链接将开始下载 Kaspersky Security Center 云控制台实例证书的公钥。

- HDS 根 CA 证书

  单击此链接将开始下载 .pem 格式的文件，其中包含由证书颁发机构 (CA) 颁发的受信任根证书列表。该文件设计供从属管理服务器使用：需要它来验证 HDS 证书。

通过使用剪贴板或任何其他方便的方式手动复制连接设置，并将它们保存到任何方便格式的文件中。单击**查看管理服务器证书**链接并等待证书文件下载。单击**HDS 根 CA 证书**链接并等待下载包含证书颁发机构颁发的受信任根证书列表的文件。这两个文件都保存到浏览器设置中指定的文件夹中。

3. 选择用于连接的从属管理服务器

在管理服务器属性中，转到**管理服务器**选项卡。在管理组的层次结构中，选中要包含从属管理服务器及其所有受管理设备的管理组旁边的复选框。单击**连接从属管理服务器**按钮。

在打开的页面上，在**从属管理服务器显示名称**字段中指定从属管理服务器必须在层次结构中显示的名称。它只是为了您的方便而使用，因此如有必要，它可以与实际的从属管理服务器名称不同。单击“**下一步**”。

如果可以通过互联网访问从属管理服务器，则还必须在从属**从属管理服务器地址(可选)**字段中指定从属管理服务器的地址。

在下一页上，单击**浏览**按钮并指定您从从属管理服务器保存的 .pem 文件。单击“**下一步**”。

4. 启用并配置代理服务器

此步骤中描述的操作是可选的。仅当您的连接需要使用代理服务器时才执行它们。

单击“**下一步**”。在**定义如何将从属管理服务器连接到主管理服务器**页面上，您可以根据需要启用和配置代理服务器的使用。选中**使用代理服务器**复选框并指定以下代理设置：

- 地址

  代理服务器地址。

- 用户名

  登录代理服务器的用户名。

- 密码

  登录代理服务器的密码。

5. **指定身份验证设置并将从属管理服务器添加到层次结构中**

   单击“**下一步**”。在**从属管理服务器凭证**页面上，指定以下设置：

   - 用户名

     您登录从属管理服务器所使用的用户名。

   - 密码

     用于登录从属管理服务器的密码。

   单击**下一步**并等待从属管理服务器出现在层次结构中。

   如果从属管理服务器可通过互联网访问，它将连接到主管理服务器。

   如果从属管理服务器可通过互联网访问，并且两个管理服务器之间的连接已成功建立，则跳过所有后续步骤。

   如果无法通过互联网访问从属管理服务器，它将变为可见，但您必须在从属管理服务器上执行其他操作才能获得对其的控制。

6. **在本地运行的 Kaspersky Security Center Web Console 中配置连接**

   在本地运行的 Kaspersky Security Center Web Console 中，打开管理服务器属性，然后在**常规**选项卡上打开**管理服务器层级**部分。选中**该管理服务器是服务器层级中的从属**复选框。在**主管理服务器类型**列表中，选择 **Kaspersky Security Center 云控制台**选项。

   Kaspersky Security Center Web Console 会检查是否将主管理服务器指定为*“将更新下载到管理服务器存储库”*任务中的更新源。如果将主管理服务器指定为更新源，您将收到相应的警告消息和任务设置的链接。您可以修改设置，然后返回层次结构创建，也可以跳过此操作并继续创建层次结构。

   在**用于在从属管理服务器与主管理服务器之间建立连接的设置**组中，指定以下设置：

   - HDS 服务器地址(来自云控制台上的主管理服务器)

     输入完全限定域名 (FQDN) 格式的 HDS 服务器地址，该地址是您从 Kaspersky Security Center 云控制台的管理服务器属性复制并保存的。

   - HDS 服务器端口

输入您从Kaspersky Security Center 云控制台的管理服务器属性复制并保存的 HDS 服务器端口号。

7. 正在添加文件到从属管理服务器

单击**指定主管理服务器证书**按钮，并指定您从 Kaspersky Security Center 云控制台的管理服务器属性中保存的证书文件。

单击**指定 Hosted Discovery Service 证书**按钮，并指定您从 Kaspersky Security Center 云控制台的管理服务器属性中保存的 .pem 文件。

如果您在 Kaspersky Security Center 云控制台中连接从属管理服务器时启用了代理服务器的使用，请选中**使用代理服务器**复选框并指定与 Kaspersky Security Center 云控制台中相同的代理设置。

如果从属管理服务器位于隔离区 (DMZ)中，您还可以选中"**连接主管理服务器到 DMZ 中的从属管理服务器**"复选框。

从属管理服务器将连接到主管理服务器。

结果

执行上述步骤后，您可以确保层次结构已成功创建：

- 主管理服务器的活动策略在从属管理服务器上生效。主管理服务器的任务被分发到从属管理服务器。如果在组任务设置中启用了**分发到从属和虚拟管理服务器**选项，则每个此类任务也会被分发到从属管理服务器。
- 主管理服务器上针对更改锁定的策略设置在从属管理服务器上的所有策略中显示为针对更改锁定。
- 主管理服务器应用的策略显示在从属管理服务器的策略列表中（**资产(设备)→策略和配置文件**）。
- 主管理服务器分发的组任务显示在从属管理服务器的任务列表中（**资产(设备)→任务**）。
- 在主管理服务器上创建的策略和任务无法在从属管理服务器上修改。
- 在 Kaspersky Security Center 云控制台中，在管理组结构中，从属管理服务器显示在您添加此管理服务器时选择的组内。

迁移到 Kaspersky Security Center 云控制台

本节介绍从在内部运行的 Kaspersky Security Center Web Console 版本 12（或更高版本）迁移到 Kaspersky Security Center 云控制台的过程。

迁移到 Kaspersky Security Center 云控制台的方法

本节提供了有关从内部运行的 Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台的可用方法的信息。

通过使用迁移功能，您可以将联网设备从 Kaspersky Security Center 转移到 Kaspersky Security Center 云控制台的管理之下。您的受管理设备将会切换，并且不会丢失主要设置（如管理组成员）以及基本对象（如与受管理应用程序相关的策略和任务）。

您可以选择两种可用方法中的一种，将管理服务器迁移到 Kaspersky Security Center 云控制台：

- 在没有管理服务器层级的情况下进行迁移：
  - 即使本地管理服务器不是 Kaspersky Security Center 云控制台的从属服务器，也可以将受管理设备和相关对象转移到 Kaspersky Security Center 云控制台。
  - 如果在不同的物理设备上打开 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台，则可能需要传输文件（通过可移动驱动器、电子邮件、共享文件夹或任何其他便捷的方式）。

  如果您的网络包含虚拟管理服务器，您还可以执行迁移。
- 使用管理服务器层级进行迁移：
  - 仅使用 Kaspersky Security Center 云控制台的界面就可以将受管理设备和相关对象转移到 Kaspersky Security Center 云控制台，因此不需要物理转移文件。
  - 需要在内部运行的管理服务器充当 Kaspersky Security Center 云控制台的从属服务器。您可以在开始迁移之前创建这样的层级。

对于全盘加密，Kaspersky Security Center 云控制台仅支持 BitLocker。

方案：在没有管理服务器层级结构的情况下进行迁移

本节介绍将受管理设备和相关对象（例如策略、任务、报告）从在内部运行的 Kaspersky Security Center Web Console 迁移到 Kaspersky Security Center 云控制台的过程。您可以在迁移范围中包括一个管理组，以在 Kaspersky Security Center 云控制台中还原同一管理组。

该组必须包含单个操作系统的受管理设备。如果您的网络包含不同操作系统或 Linux 发行版的设备，请将它们分配到不同的管理组中，然后分别迁移每个组。

完成迁移后，将通过 Kaspersky Security Center 云控制台升级和管理迁移范围内的所有网络代理。

本节中列出的步骤涵盖了当不存在任何管理服务器层级（即，Kaspersky Security Center 云控制台与内部运行的 Kaspersky Security Center Web Console 之间未建立任何连接）时执行的迁移过程。

先决条件

在开始之前，请执行以下操作：

- 将内部运行的管理服务器升级到以下版本：
  - 对于 Windows 设备 - 版本 12 或更高版本
  - 对于 Linux 设备 - 版本 12 补丁 A 或更高版本
- 安装 Kaspersky Security Center Web Console 版本 12.1 或更高版本。
- 将受管理设备上的网络代理升级到版本 12 或更高版本。
- 在 Windows 设备上，使用没有卸载密码的网络代理。
  如果已设置密码，请在 Kaspersky Security Center Web Console 中执行以下操作之一：
  - 禁用“**使用卸载密码**”中的Use uninstallation password选项。
  - 使用*远程卸载应用程序*任务远程卸载网络代理。在任务的**要卸载的应用程序**字段中，选择**Kaspersky Security Center 网络代理**。不要忘记输入卸载密码。
- 将受管理应用程序升级到 Kaspersky Security Center 云控制台支持的版本。
- 确保您有最新版本的受管理应用程序的策略。如果您使用的是过时策略，为受 Kaspersky Security Center Cloud Console 支持的应用程序版本创建新策略。
- 若要使用实际策略，为打算通过 Kaspersky Security Center 云控制台管理的应用程序更新 Web 插件。
- 如果 Kaspersky Security Center Cloud Console 不支持受管理设备中的卡巴斯基应用程序，则卸载这些应用程序，然后将卸载的应用程序替换为受支持的应用程序。
- 解密运行 Windows 操作系统的受管理设备上由 Kaspersky Endpoint Security for Windows 加密（磁盘级或文件级）的所有数据，并通过应用程序策略或在本地禁用受管理设备上的加密功能。有关详细信息，请参阅 Kaspersky Endpoint Security for Windows 的帮助。

  如果 Windows 设备仍存储通过 Kaspersky Endpoint Security for Windows 加密的任何文件或文件夹，则在迁移过程中将取消网络代理升级。一条通知将提示您解密设备上的所有数据并禁用加密功能。

Kaspersky Security Center 云控制台允许每个管理服务器最多管理 25,000 台受管理设备。

迁移阶段

迁移到 Kaspersky Security Center 云控制台包括以下阶段：

1. **计划迁移范围并检查先决条件**

估计迁移过程的范围，即审核要导出的管理组并评估其中的受管理设备数量。此外，确保作为迁移先决条件列出的所有活动均已成功完成。

2. **从 Kaspersky Security Center Web Console 导出受管理设备、对象和设置**

   使用内部运行的 Kaspersky Security Center Web Console 的迁移向导将受管理设备与其对象一起导出。

   > 最大导出文件大小为 4 GB。

3. **将导出文件导入到 Kaspersky Security Center 云控制台**

   将有关受管理设备和对象的信息传输到 Kaspersky Security Center 云控制台。为此，请使用 Kaspersky Security Center 云控制台的迁移向导导入导出文件并创建网络代理独立安装包。

4. **在受管理设备上重新安装网络代理**

   返回到内部运行的 Kaspersky Security Center Web Console 中的迁移向导，以创建远程安装任务。您将能够（立即或稍后）使用此任务在受管理设备上重新安装网络代理并完成迁移过程。

结果

完成迁移后，您可以根据以下条件确定迁移已成功：

- 网络代理已重新安装在所有受管理设备上。
- 所有设备均通过 Kaspersky Security Center 云控制台进行管理。
- 迁移之前有效的所有对象设置均得到保留。

迁移向导

本节提供有关 Kaspersky Security Center 云控制台和 Kaspersky Security Center Web Console 版本 12 或更高版本中的迁移向导的信息。

步骤 1：从 Kaspersky Security Center Web Console 导出受管理设备、对象和设置

将受管理设备从 Kaspersky Security Center Web Console 迁移到 Kaspersky Security Center 云控制台需要您先创建一个导出文件，其中包含有关当前在内部运行的管理服务器上存在的管理组层级的信息。该导出文件还必须包含有关对象及其设置的信息。此导出文件将用于以后导入到 Kaspersky Security Center 云控制台中。

> 最大导出文件大小为 4 GB。

要从 Kaspersky Security Center Web Console 导出对象及其设置：

1. 在 Kaspersky Security Center Web Console 的主菜单中，转至**操作→迁移**。

2. 在迁移向导的欢迎页面上，单击“**下一步**”。将打开“**要导出的受管理设备**”页面，其中显示相应管理服务器的整个管理组层级。

3. 在“**要导出的受管理设备**”页面上，单击“**受管理设备**”组名称旁边的 V 形图标 (>) 以扩展管理组层级。选择要导出的管理组。

   为两个管理组执行从本地运行的 Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台后，这些组的远程安装任务会显示相同的名称。

4. 选择必须将其策略和任务与组对象一起传送到 Kaspersky Security Center 云控制台的受管理应用程序。要选择将导出其对象的受管理应用程序，请在列表中选中其名称旁边的复选框。

   尽管 Kaspersky Security Center 管理服务器在列表上，但是选中相应的复选框不会导出其策略。

   要确保受管理的应用程序受 Kaspersky Security Center 云控制台支持，请单击相应链接。您将被重定向到包含 Kaspersky Security Center 云控制台管理的应用程序列表的在线帮助主题。

   如果选择的应用程序不受 Kaspersky Security Center 云控制台支持，这些应用程序的策略和任务仍将导出并在随后导入，但是您将无法在 Kaspersky Security Center 控制台中管理它们，因为专用插件不可用。

5. 查看默认情况下导出的组对象列表，并在必要时指定要与选定管理组一起导出的非组对象。通过包括或排除各种对象（例如，全局任务、自定义设备分类、报告、自定义角色、内部用户和安全组以及自定义应用程序类别）来配置导出范围。此页面包括以下区域：

   - 全局任务

     受管理应用程序的全局任务以及网络代理的全局任务的列表。

     如果您选择的全局任务应用于特定对象分类，则该分类也将导出。

     尽管管理服务器的全局任务在列表上，但是您无法将其导出；选择这些任务不会影响导出范围。远程安装任务也仍然在导出范围之外，因为它们各自的安装包无法导出。

   - 设备分类

     自定义设备分类列表。

   - 报告

     要导出的报告实例的可编辑列表。

     如果您选择的报告应用于特定对象分类，则该分类也将导出。

     Kaspersky Security Center 云控制台包含与 Kaspersky Security Center Web Console 相同的报告模板集，因此您可以选择仅导出手动创建或重新配置的报告。

- 组对象

  默认情况下要导出的组对象列表。默认情况下，与所选管理组相关的以下对象将全部导出：

  - 管理组结构，即所选管理组的所有子组
  - 要导出的管理组中已包括的设备
  - 已分配给要导出的设备的标签

    如果标签是在 Kaspersky Security Center Web Console 中创建的，但从未分配给任何设备，则该标签不会导出。自动标记规则也不会导出。

  - 已选择的受管理应用程序的组策略

    管理服务器策略和网络代理策略不会导出。

  - 已选择的受管理应用程序的组任务和网络代理组任务

    管理服务器任务不会导出。

  您还可以防止导出某些类型的非组对象：

  - 要取消导出自定义角色（即，仅由用户创建的角色），请选中“**不导出自定义角色**”复选框。
  - 要取消导出内部用户和安全组，请选中“**不导出内部用户和安全组**”复选框。
  - 要取消导出含有手动添加内容的自定义应用程序类别，请选中“**不导出自定义应用程序类别**”复选框。

如果您将各种操作系统的设备转移到 Kaspersky Security Center 云控制台，非组对象只需迁移一次。

迁移向导会检查所选管理组中包含的受管理设备总数。如果此数字超过 10,000，则会出现错误消息。“**下一步**”按钮保持不可用（灰显），直到所选管理组中的受管理设备数量在限制范围内。

6. 定义迁移范围后，单击“**下一步**”开始导出过程。“**创建导出文件**”页面将打开，您可以在该页面上查看迁移范围中包括的每种类型的对象的导出进度。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 (✓)。导出过程完成，并且导出文件自动下载到浏览器设置中定义的默认下载位置。导出文件的名称显示在浏览器窗口的下部。

7. 当显示“**导出已成功完成**”页面后，继续 Kaspersky Security Center 云控制台中执行的下一个阶段。

如果在不同设备上使用 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台，则必须将导出文件复制到可移动驱动器或选择其他文件传输方式。

步骤 2：将导出文件导入到 Kaspersky Security Center 云控制台

要传输有关从 Kaspersky Security Center Web Console 导出的受管理设备、对象及其设置的信息，必须将其导入到工作区中部署的 Kaspersky Security Center 云控制台。这样您可以创建独立安装包，并使用它在受管理设备上重新安装网络代理。

在 Kaspersky Security Center 云控制台中启动迁移向导之前，确保其当前本地化语言与导出过程中 Kaspersky Security Center Web Console 的语言相同。如有必要，请切换语言。

如果之前已在 Kaspersky Security Center 云控制台工作区中完成快速启动向导，则“**受管理设备**”组包括使用默认设置创建的策略和任务。请先删除这些策略和任务，然后再导入从 Kaspersky Security Center Web Console 导出的策略和任务。

要将导出文件导入到 Kaspersky Security Center 云控制台：

1. 在 Kaspersky Security Center 云控制台的主菜单中，转至**操作→迁移**。
2. 在迁移向导的欢迎页面上，单击“**导入**”。在打开的“文件资源管理器”窗口中，浏览到保存导出文件的文件夹来选择导出文件，然后单击“**打开**”。等待至文件上传状态旁边的刷新图标 (🔄) 替换为绿色复选标记 (✓)。
3. 单击“**下一步**”。下一个页面打开，显示 Kaspersky Security Center 云控制台中管理服务器的整个管理组层级。
4. 选中必须将组对象还原到的目标管理组旁边的复选框，然后单击“**下一步**”。迁移向导显示 Kaspersky Security Center 云控制台中可用的网络代理安装包的列表。
5. 选择包含网络代理的相关版本和本地化的安装包，然后单击“**下一步**”。

   只有之前已在 Kaspersky Security Center 云控制台工作区中完成快速启动向导以及执行 Windows 设备迁移时，才选择 Kaspersky Network Agent for Windows 安装包。

   等待至迁移向导创建独立安装包。网络代理的独立安装包的最大文件大小为 200 MB。

   文件将被解压缩并自动下载到浏览器设置中定义的默认下载位置。非组对象和组对象被恢复到目标管理组。

   导入完成后，导出的管理组结构（包括设备详细信息）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。

   如果已导入整个“**受管理设备**”组，建议重命名新导入的子组以避免混淆：

   a. 转到“**组层级**”区域。

   b. 在组树中单击子组的名称。

   c. 在打开的属性窗口的“**名称**”字段中输入其他名称（例如，“已迁移的设备”）。

   建议检查导出范围中包含的对象（策略、任务和受管理设备）是否已成功导入到 Kaspersky Security Center 云控制台。为此，请转到“**资产(设备)**”区域，并查看导入的对象是否出现在“**策略和配置文件**”、“**任务**”和“**受管理设备**”子区域中。

   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。之后，设备开始切换到 Kaspersky Security Center 云控制台。

6. 单击“**完成**”关闭迁移向导窗口。

7. 如果您要再次查找并下载独立安装包， 转到“**发现和部署**” → “**部署和分配**” → “**安装包**”并单击“**查看独立包列表**”按钮。在打开的列表中，选择已创建的独立安装包，然后单击“**下载**”按钮。

如果在不同设备上使用 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台，则必须将独立安装包复制到可移动驱动器或选择其他文件传输方式。

步骤 3：在通过 Kaspersky Security Center 云控制台管理的设备上重新安装网络代理

创建网络代理独立安装包后，可以继续创建远程安装任务。执行此任务将可让您在所有受管理设备上重新安装网络代理，以便通过 Kaspersky Security Center 云控制台切换这些受管理的设备。

为了降低数据丢失的风险，建议您先对一个小型管理组执行操作，该管理组包含的公司网络内受管理设备不应超过 20 个，并且不包含物理服务器。完成这些操作后，检查重新安装是否成功完成，然后继续完整范围的重新安装。

要创建远程安装任务并重新安装网络代理：

1. 返回到内部运行的 Kaspersky Security Center Web Console 中的迁移向导。

我们建议使用迁移向导创建远程安装任务来重新安装网络代理，如下所述。如果需要使用自定义远程安装任务，首先需要从网络代理独立安装包中手动创建自定义安装包。请注意，创建自定义安装包时，必须在可执行文件命令行中指定“-s”键。否则，从此自定义安装包重新安装网络代理会出现错误。

根据迁移向导的当前状态，可以执行以下操作之一：

- 如果导出后尚未关闭迁移向导，并且会话尚未过期，则单击“**转到迁移向导的步骤 3**”按钮。选中“**上传独立安装包**”复选框，然后单击“**选择独立安装包**”按钮。在打开的浏览器窗口中，指定网络代理独立安装包。
- 如果由于某种原因必须再次启动迁移向导，请选中“**上传独立安装包**”复选框，然后单击“**选择独立安装包**”按钮。在打开的浏览器窗口中，指定网络代理独立安装包。之后，迁移向导会再次显示此管理服务器的管理组层级结构。选择您为其创建了导出文件的同一个组，然后单击“**下一步**”。

迁移向导会再次检查所选管理组中包含的受管理设备总数。如果此数字超过 10,000，则会出现错误消息。“**下一步**”按钮保持不可用（灰显），直到所选管理组中的受管理设备数量在限制范围内。

2. 等待至独立安装包上传完毕，然后单击“**下一步**”。迁移向导会为其创建自定义安装包和远程安装任务。任务范围将包括您在“**要导出的受管理设备**”页面上选择的管理组；默认情况下，任务启动时间表将设置为**手动**。迁移向导显示创建进度。等待至刷新图标 (🔄) 替换为绿色复选标记 (✓)，然后单击“**下一步**”。

3. 如有必要，针对本地运行的管理服务器的选定管理组及其所有子组中的设备选中“**运行新创建的远程安装任务**”复选框（默认情况下已清除）。在这种情况下，将在 Kaspersky Security Center 云控制台的管理下切换设备，但仅限于网络代理安装完成后。完整路径将显示到将在其中运行任务的管理组。

只有向 Kaspersky Security Center 云控制台导入完成后，才能启动任务。否则，列表中的设备名称可能重复。

4. 单击“**完成**”关闭迁移向导并为以下目的启动远程安装任务：

   - 升级网络代理实例
   - 切换 Kaspersky Security Center 云控制台管理下的网络代理实例

   如果将“**运行新创建的远程安装任务**”复选框保持清除状态，则稍后可以根据需要手动启动任务。

您可以检查现在可以通过 Kaspersky Security Center 云控制台管理迁移的网络代理实例。为此，转到“**资产(设备)**” → “**受管理设备**”。确保已迁移的受管理设备在“**可见**”、“**网络代理已安装**”和“**网络代理正在运行**”列中具有确认图标（）。此外，确保这些设备没有“*长期未连接*”状态描述。

在有管理服务器层级的情况下进行迁移

本节介绍将受管理设备和相关对象从在内部运行的 Kaspersky Security Center Web Console 迁移到 Kaspersky Security Center 云控制台的过程。该过程涉及层级：在内部运行的 Kaspersky Security Center Web Console 充当从属管理服务器，而 Kaspersky Security Center 云控制台充当主管理服务器。

传输到 Kaspersky Security Center 云控制台的每个管理组都必须包含单个操作系统的受管理设备。如果您的网络包含不同操作系统的设备，请将它们分配到不同的管理组中，然后分别迁移每个组。

完成迁移后，将通过 Kaspersky Security Center 云控制台升级和管理迁移范围内的组中的所有网络代理。

在开始之前，请执行以下操作：

- 将内部运行的管理服务器升级到以下版本：
  - 对于 Windows 设备 - 版本 12 或更高版本
  - 对于 Linux 设备 - 版本 12 补丁 A 或更高版本
- 安装 Kaspersky Security Center Web Console 版本 12.1 或更高版本。
- 将受管理设备上的网络代理升级到版本 12 或更高版本。
- 在 Windows 设备上，使用没有卸载密码的网络代理。

  如果已设置密码，请在 Kaspersky Security Center Web Console 中执行以下操作之一：
  - 禁用“**使用卸载密码**”中的Use uninstallation password选项。
  - 使用*远程卸载应用程序*任务远程卸载网络代理。在任务的**要卸载的应用程序**字段中，选择**Kaspersky Security Center 网络代理**。不要忘记输入卸载密码。
- 将受管理应用程序升级到 Kaspersky Security Center 云控制台支持的版本。
- 确保您有最新版本的受管理应用程序的策略。如果您使用的是过时策略，为受 Kaspersky Security Center Cloud Console 支持的应用程序版本创建新策略。
- 若要使用实际策略，为打算通过 Kaspersky Security Center 云控制台管理的应用程序更新 Web 插件。

- 如果 Kaspersky Security Center Cloud Console 不支持受管理设备中的卡巴斯基应用程序，则卸载这些应用程序，然后将卸载的应用程序替换为受支持的应用程序。

- 解密运行 Windows 操作系统的受管理设备上由 Kaspersky Endpoint Security for Windows 加密（磁盘级或文件级）的所有数据，并通过应用程序策略或在本地禁用受管理设备上的加密功能。有关详细信息，请参阅 Kaspersky Endpoint Security for Windows 的帮助。

  如果 Windows 设备仍存储通过 Kaspersky Endpoint Security for Windows 加密的任何文件或文件夹，则在迁移过程中将取消网络代理升级。一条通知将提示您解密设备上的所有数据并禁用加密功能。

Kaspersky Security Center 云控制台允许每个管理服务器最多管理 25,000 台受管理设备。

要执行迁移到 Kaspersky Security Center 云控制台：

1. 估计迁移过程的范围，即审核要导出的管理组并评估其中的受管理设备数量。确保作为迁移先决条件列出的所有活动均已成功完成。

2. 在 Kaspersky Security Center 云控制台中，转至要迁移其受管理设备的从属管理服务器。

3. 在主菜单中，转到**操作 → 迁移**。

   将打开迁移向导的欢迎页面。

4. 在欢迎页面，单击“**下一步**”。

   将打开“**要导出的受管理设备**”页面，其中显示从属管理服务器的整个管理组层级。

5. 在“**要导出的受管理设备**”页面上，单击“**受管理设备**”组名称旁边的 V 形图标 (>)，然后扩展管理组层级。选择要导出的管理组。

   迁移向导会检查所选管理组中包含的受管理设备总数。如果此数字超过 10,000，则会出现错误消息。“**下一步**”按钮保持不可用（灰显），直到所选管理组中的受管理设备数量在限制范围内。

6. 选择必须将其策略和任务与组对象一起传送到 Kaspersky Security Center 云控制台的受管理应用程序。要选择将导出其对象的受管理应用程序，请在列表中选中其名称旁边的复选框。

   尽管 Kaspersky Security Center 管理服务器在列表上，但是选中相应的复选框不会导出其策略。

   要确保受管理的应用程序受 Kaspersky Security Center 云控制台支持，请单击相应链接。您将被重定向到包含 Kaspersky Security Center 云控制台管理的应用程序列表的在线帮助主题。

   如果选择的应用程序不受 Kaspersky Security Center 云控制台支持，这些应用程序的策略和任务仍将迁移，但是您将无法在 Kaspersky Security Center 云控制台中管理它们，因为专用插件不可用。

7. 查看默认情况下要导出的组对象列表。如果需要，您还可以指定要与所选管理组一起导出的非组对象，例如全局任务、自定义设备分类、报告、自定义角色、内部用户和安全组，以及带有手动添加内容的自定义应用程序类别。此页面包括以下区域：

   - 全局任务

受管理应用程序的全局任务以及网络代理的全局任务的列表。

如果您选择的全局任务应用于特定对象分类，则该分类也将导出。

尽管管理服务器的全局任务在列表上，但是您无法将其导出；选择这些任务不会影响导出范围。远程安装任务也仍然在导出范围之外，因为它们各自的安装包无法导出。

- 设备分类

  自定义设备分类列表。

- 报告

  要导出的报告实例的可编辑列表。

  如果您选择的报告应用于特定对象分类，则该分类也将导出。

  Kaspersky Security Center 云控制台包含与 Kaspersky Security Center Web Console 相同的报告模板集，因此您可以选择仅导出手动创建或重新配置的报告。

- 组对象

默认情况下要导出的组对象列表。默认情况下，与所选管理组相关的以下对象将全部导出：

- 管理组结构，即所选管理组的所有子组
- 要导出的管理组中已包括的设备
- 已分配给要导出的设备的标签

  如果标签是在 Kaspersky Security Center Web Console 中创建的，但从未分配给任何设备，则该标签不会导出。自动标记规则也不会导出。

- 已选择的受管理应用程序的组策略

  管理服务器策略和网络代理策略不会导出。

- 已选择的受管理应用程序的组任务和网络代理组任务

  管理服务器任务不会导出。

您还可以防止导出某些类型的非组对象：

- 要取消导出自定义角色（即，仅由用户创建的角色），请选中“**不导出自定义角色**”复选框。
- 要取消导出内部用户和安全组，请选中“**不导出内部用户和安全组**”复选框。
- 要取消导出含有手动添加内容的自定义应用程序类别，请选中“**不导出自定义应用程序类别**”复选框。

如果您将各种操作系统的设备转移到 Kaspersky Security Center 云控制台，非组对象只需迁移一次。

8. 定义迁移范围后，单击“**下一步**”开始导出过程。“**创建导出文件**”页面将打开，您可以在该页面上查看迁移范围中包括的每种类型的对象的导出进度。等待至对象列表中每个项目旁边的刷新图标 (🔄) 均替换为绿色复选标记 (✓)。导出完成，并且导出文件自动保存到临时文件夹中。下一页将打开，显示充当主管理服务器的 Kaspersky Security Center 云控制台中的整个管理组层级。

9. 选中必须将组对象导入到的管理组旁边的复选框，然后单击“**下一步**”。将文件解压缩，并将非组对象和组对象还原到目标管理组。

   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。

   导入完成后，导出的管理组结构（包括设备详细信息）将显示在所选目标管理组下。非组对象也将被导入。

   导入期间将无法最小化迁移向导和执行任何并行操作。等待至对象列表中每个项目旁边的刷新图标 (🔄) 均替换为绿色复选标记 (✓)，导入完成。之后，设备开始切换到 Kaspersky Security Center 云控制台。

10. 导入完成后，迁移向导将显示 Kaspersky Security Center 云控制台中针对适当操作系统的可用的网络代理安装包列表。选择包含网络代理的相关版本和本地化的安装包。

只有之前已在 Kaspersky Security Center 云控制台工作区中完成快速启动向导以及执行 Windows 设备迁移时，才选择 Kaspersky Network Agent for Windows 安装包。

11. 单击“**下一步**”。

    迁移向导会创建一个新的独立安装包（或使用现有的安装包）和一个基于该安装包的自定义安装包，以及相应的远程安装任务。任务范围包括您在“**要导出的受管理设备**”页面选择的管理组。默认情况下，任务启动计划为**手动**设置。迁移向导显示创建进度。

12. 等待至每个刷新图标 (↻) 均替换为绿色复选标记 (✓)，然后单击“**下一步**”。

13. 如有必要，针对内部运行的 Kaspersky Security Center Web Console 中的选定管理组及其所有子组中的设备选中“**运行新创建的远程安装任务**”复选框（默认情况下清除）。网络代理安装完成后，您可以通过 Kaspersky Security Center 云控制台管理所选设备。完整路径将显示到在其中运行任务的管理组。

    只有向 Kaspersky Security Center 云控制台导入完成后，才能启动远程安装任务。否则，设备可能会重复。

14. 单击“**完成**”关闭迁移向导并为以下目的启动远程安装任务：

    - 升级网络代理实例
    - 通过 Kaspersky Security Center 云控制台管理网络代理实例

    如果将“**运行远程安装任务**”复选框保持清除状态，则稍后可以根据需要手动启动任务。

    您可以检查现在可以通过 Kaspersky Security Center 云控制台管理迁移的网络代理实例。为此，转到“**资产(设备)**” → “**受管理设备**”。确保已迁移的受管理设备在“**可见**”、“**网络代理已安装**”和“**网络代理正在运行**”列中具有确认图标（✓）。此外，确保这些设备没有“*长期未连接*”状态描述。

场景：运行 Linux 或 macOS 操作系统的设备迁移

本节介绍如何将运行 Linux 或 macOS 操作系统的设备从本地运行的 Kaspersky Security Center Web Console 迁移到 Kaspersky Security Center 云控制台。没有管理服务器层次结构的迁移和使用这种层次结构的迁移的基本情景允许将所有设备和相关对象传输到 Kaspersky Security Center 云控制台。但是，如果您的网络不仅包括运行 Windows 的设备，还包括运行 Linux 或 macOS 的设备，则需要分别传输每种操作系统类型的设备。因此，您必须执行多次迁移。

先决条件

在开始之前，请执行以下操作：

- 将内部运行的管理服务器升级到版本 12 补丁 A 或更高版本。
- 安装 Kaspersky Security Center Web Console 版本 12.1 或更高版本。
- 将受管理设备上的网络代理升级到版本 12 或更高版本。

- 将受管理应用程序升级到 Kaspersky Security Center 云控制台支持的版本。
- 确保您有最新版本的受管理应用程序的策略。如果您使用的是过时策略，为受 Kaspersky Security Center Cloud Console 支持的应用程序版本创建新策略。
- 若要使用实际策略，为打算通过 Kaspersky Security Center 云控制台管理的应用程序更新 Web 插件。
- 如果 Kaspersky Security Center Cloud Console 不支持受管理设备中的卡巴斯基应用程序，则卸载这些应用程序，然后将卸载的应用程序替换为受支持的应用程序。

Kaspersky Security Center 云控制台允许每个管理服务器最多管理 25,000 台受管理设备。

迁移阶段

迁移到 Kaspersky Security Center 云控制台包括以下阶段：

1. **按操作系统对受管理设备进行分组**

   如果您的网络包括运行不同操作系统（Windows、Linux 或 macOS）的设备，将每个操作系统的设备置于 Kaspersky Security Center Web Console 的单独管理组中。另外，为每个 Linux 发行版创建一个管理组。例如，如果您有 Debian 和 Red Hat Linux 设备，请将它们分配到不同的管理组中。这将允许您成功执行迁移，因为不同的操作系统需要不同的网络代理安装包。

2. **分别执行每个管理组及其应用程序对象的迁移**

   每个操作系统的受管理设备必须与其策略和任务一起单独迁移。例如，如果您有 Windows、macOS、Ubuntu 和 CentOS 设备，首先，将运行 Windows 操作系统的设备转移到 Kaspersky Security Center 云控制台，然后转移到 macOS、Ubuntu，最后转移到 CentOS。您可以按任意顺序传输受管理设备。

   为此，根据您的网络是否包括从属管理服务器，执行不带管理服务器层次结构的迁移或带有此层级的迁移。迁移过程中，请使用所迁移设备的操作系统对应的网络代理安装包。例如，选择 Kaspersky Security Center 13.2 的 Linux 设备网络代理来执行迁移。

   请注意，非组对象，例如全局任务、自定义设备分类或报告，只需迁移一次。

结果

完成迁移后，您可以根据以下条件确定迁移已成功：

- 在运行 Linux 或 macOS 操作系统的每个受管理设备上重新安装正确版本的网络代理。
- 所有 Linux 或 macOS 设备均通过 Kaspersky Security Center 云控制台进行管理。
- 迁移之前有效的所有对象设置均得到保留。

方案：从Kaspersky Security Center 云控制台反向迁移到 Kaspersky Security Center

您可能希望将受管理设备从Kaspersky Security Center 云控制台迁移到 Kaspersky Security Center 管理服务器。例如，此过程可用于回滚迁移到 Kaspersky Security Center 云控制台。

先决条件

在开始之前，请确保满足以下先决条件：

- Kaspersky Security Center 云控制台可用并且已连接受管理设备。
- Kaspersky Security Center 14.2（或更高版本）管理服务器可用，并具有版本 13 或更高版本的网络代理安装包。

反向迁移阶段

反向迁移包括以下阶段：

1. **在本地 Kaspersky Security Center 管理服务器中创建网络代理独立安装包**

   在本地运行的 Kaspersky Security Center 管理服务器中，创建网络代理独立安装包。

   在创建过程中，您可以选择**将未分配的设备移动到此组**选项来指定安装后要将网络代理移至的管理组。如果您已指定管理组，则会创建一条自动移动规则，该规则会将使用此独立安装包安装的所有网络代理移动到目标管理组。

   > 为确保正确反向迁移，请确保您选择的网络代理版本等于或高于 Kaspersky Security Center 云控制台中使用的版本。

2. **在 Kaspersky Security Center 云控制台中创建自定义安装包**

   在 Kaspersky Security Center 云控制台中，根据您从本地运行的 Kaspersky Security Center 管理服务器创建和保存的独立安装包创建自定义安装包。

   要以静默模式启用软件包安装，请在**可执行文件命令行**行字段中指定 `-s` 键。

3. **创建远程安装任务**

   在 Kaspersky Security Center 云控制台中，使用您创建的自定义安装包创建远程安装任务。

4. **运行远程安装任务**

   启动您创建的远程安装任务。该任务启动指定管理组中所有网络代理的重新安装；它还通过更改连接地址和修改其他连接设置来切换本地运行的 Kaspersky Security Center 管理服务器管理下的网络代理。

   > 如果您在创建独立安装包期间未指定任何目标管理组，则所有设备都将移至**未分配的设备**组。

结果

完成迁移后，您可以根据以下条件确定迁移已成功：

- 之前通过 Kaspersky Security Center 云控制台管理的远程安装任务范围内的所有设备现在均由本地运行的 Kaspersky Security Center 管理服务器管理。
- 设备会自动移至安装包设置中指定的管理组。

> Kaspersky Security Center 云控制台中的远程安装任务无法完成：它不再有目标设备，因为所有目标设备都已修改连接设置。确保错误图标 (!) 已出现在迁移范围内所有设备的受管理设备列表的**可见**列中。

使用虚拟管理服务器进行迁移

如果您现有的 Kaspersky Security Center 本地基础架构中有虚拟管理服务器，则无法使用迁移向导从Kaspersky Security Center 本地迁移到 Kaspersky Security Center 云控制台。此外，您将只能迁移客户的设备。您必须手动创建策略、任务和报告。

您可以执行以下迁移方案之一：

- 通过将客户端设备从虚拟管理服务器移动到主管理服务器
- 通过从虚拟管理服务器执行手动迁移

方案：通过移动设备迁移虚拟管理服务器

要执行从本地运行的 Kaspersky Security Center Web Console 到 Kaspersky Security Center 云控制台的迁移，您可以将设备从虚拟管理服务器移动到主管理服务器。

先决条件

迁移之前，您必须执行多项操作，包括将本地运行的管理服务器升级到版本 12 或更高版本，以及将受管理应用程序升级到 Kaspersky Security Center 云控制台支持的版本。

迁移方案

方案实施分为几个阶段：

1. **为每个虚拟管理服务器创建管理组**

   您可以在本地运行的 Kaspersky Security Center中创建组。

2. **移动客户的设备**

   在本地运行的 Kaspersky Security Center 中，将客户的设备从每个虚拟管理服务器移动到上一阶段创建的相应管理组。

3. **迁移**

   按照针对没有管理服务器层次结构的网络的描述执行迁移。

4. **将设备移至虚拟管理服务器的管理之下（可选步骤）**

   如果您想要通过虚拟管理服务器管理您的客户，请将设备从管理组移动到虚拟管理服务器管理下。

5. **创建策略、任务和报告**

   根据需要创建策略、任务和报告。

结果

完成迁移后，您可以根据以下条件确定迁移已成功：

- 网络代理已重新安装在所有受管理设备上。
- 所有设备均通过 Kaspersky Security Center 云控制台进行管理。
- 迁移之前有效的所有对象设置均得到保留。

方案：使用虚拟管理服务器进行手动迁移

您可以手动从本地运行的 Kaspersky Security Center Web Console 执行迁移到 Kaspersky Security Center 云控制台。

先决条件

迁移之前，您必须执行多项操作，包括将本地运行的管理服务器升级到版本 12 或更高版本，以及将受管理应用程序升级到 Kaspersky Security Center 云控制台支持的版本。

迁移方案

方案实施分为几个阶段：

1. **为每个虚拟管理服务器创建管理组**

   在 Kaspersky Security Center 云控制台中，创建与每个虚拟管理服务器相对应的管理组。

2. **为网络代理创建独立安装包**

   为网络代理创建独立安装包。在创建过程中，指定您在上一阶段创建的管理组。这意味着您必须为每个管理组创建单独的独立安装包。

   此阶段发生在您的 Kaspersky Security Center 云控制台中。

3. **下载独立安装包**

   下载您在上一阶段创建的独立安装包。此阶段发生在您的 Kaspersky Security Center 云控制台中。

4. **使用每个独立安装包创建存档**

   可用的存档类型有：ZIP、CAB、TAR 或 TAR.GZ。

5. **为网络代理创建自定义安装包**

   为网络代理创建自定义安装包。在创建过程中，使用您在上一阶段创建的存档。

   此阶段发生在本地运行的 Kaspersky Security Center 中。

6. **创建远程安装任务**

   创建远程安装任务以从创建的自定义安装包安装网络代理。

   创建任务时，指定对应的管理组。

   此阶段发生在本地运行的 Kaspersky Security Center 中。

7. **运行创建的远程安装任务**

   网络代理已更新。Kaspersky Security Center 云控制台管理服务器将接管对它们的管理。

所有设备都会迁移到 Kaspersky Security Center 云控制台，并放置在您为网络代理创建独立安装包时指定的管理组中。

8. **将设备移至虚拟管理服务器的管理之下（可选步骤）**

   如果您想要通过虚拟管理服务器管理您的客户，请将设备从管理组移动到虚拟管理服务器管理下。

9. **创建策略、任务和报告**

   根据需要创建策略、任务和报告。

结果

完成迁移后，您可以根据以下条件确定迁移已成功：

- 网络代理已重新安装在所有受管理设备上。
- 所有设备均通过 Kaspersky Security Center 云控制台进行管理。

  迁移之前有效的所有对象设置均得到保留。

方案：将设备从虚拟服务器管理下的管理组中移出

您可能希望通过虚拟管理服务器来管理客户。如果您将设备和其他项目从本地 Kaspersky Security Center 迁移到 Kaspersky Security Center 云控制台，则这些设备位于管理组中。要通过虚拟管理服务器管理客户的设备，您必须将设备从管理组移动至虚拟管理服务器管理下。

先决条件

您已经为每个客户创建了一个虚拟管理服务器。

每个客户的所有设备都位于单独的管理组中。

阶段

方案实施分为几个阶段：

1. **为网络代理创建独立安装包**

   切换到每个创建的虚拟管理服务器，然后为网络代理创建独立安装包。您可以通过单击当前管理服务器名称右侧的 V 形图标（）、然后选择所需的管理服务器在主菜单中切换管理服务器。

2. **下载独立安装包**

   下载您在上一阶段创建的独立安装包。

3. **使用每个独立安装包创建存档**

   可用的存档类型有：ZIP、CAB、TAR 或 TAR.GZ。

4. **为网络代理创建自定义安装包**

   为网络代理创建自定义安装包。在创建过程中，使用您在上一阶段创建的存档。

此阶段发生在主管理服务器上。

5. **创建远程安装任务**

   创建远程安装任务以从创建的自定义安装包安装网络代理。

   创建任务时，指定对应的管理组。

   此阶段发生在主管理服务器上。

6. **运行创建的远程安装任务**

   网络代理已更新。设备移动至虚拟管理服务器的管理下。

7. **创建策略、任务和报告**

   根据需要创建策略、任务和报告。

结果

您现在可以使用虚拟管理服务器来管理迁移的客户设备。

快速启动向导

本部分提供有关 Kaspersky Security Center 云控制台快速启动向导的信息。

关于快速启动向导

Kaspersky Security Center 云控制台中的快速启动向导使您能够创建最少的必要任务和策略、调整最少的设置，并开始创建卡巴斯基应用程序的安装包。通过使用向导，您可以对 Kaspersky Security Center 云控制台进行以下更改：

- 开始下载托管卡巴斯基应用程序的安装包。
- 为运行 Windows、Linux 或 macOS 的设备创建网络代理独立安装包。
- 创建 Kaspersky Security Center 网络代理策略。
- 创建“*将更新下载至分发点存储库*”任务。
- 为受管理的卡巴斯基应用程序创建策略和任务
- 配置与卡巴斯基安全网络 (KSN) 的交互。

快速启动向导完成后，网络代理和受管理卡巴斯基应用程序的安装包将出现在**发现和部署 → 部署和分配 → 安装包**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。

在您创建公司工作区并首次启动 Kaspersky Security Center 云控制台后，Kaspersky Security Center 云控制台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。

开始快速启动向导

在您创建公司工作区并首次启动 Kaspersky Security Center 云控制台后，Kaspersky Security Center 云控制台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。

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不会再次创建。

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。
3. 单击**开始快速启动向导**。

   或者，您可以通过选择**发现和部署 → 部署和分配 → 快速启动向导**来启动快速启动向导。

该向导会提示您执行 Kaspersky Security Center 云控制台的初始配置。遵照向导的说明操作。使用**下一步**按钮进行向导。使用**后退**按钮返回到向导的上一步。

步骤 1：选择要下载的安装包

在列表中，选择要安装在客户端设备上的卡巴斯基应用程序。Kaspersky Security Center 云控制台将为所选应用程序创建安装包。之后，您将使用创建的安装包来安装应用程序。

选择下载的安装包时，请注意语言：安装包有多种语言版本。

选择以下应用程序：

- Kaspersky Security Center 网络代理

  选择网络代理安装包时，请考虑以下事项：

  - 应该首先在每台客户端设备上安装网络代理。因此，请选择适合客户端设备上运行的每个操作系统的网络代理。

  - 网络代理必须通过独立安装包手动安装在您选择用作分发点的设备上。需要分发点来执行网络轮询以及在客户端设备上远程安装卡巴斯基安全应用程序。因此，您必须至少选择一个网络代理安装包。当您继续执行向导的后续步骤时，Kaspersky Security Center 云控制台将创建网络代理独立安装包。

    与基于 Windows 的分发点相比，基于 Linux 和 macOS 的分发点的功能有限。强烈建议您选择基于 Windows 的计算机作为分发点。

    您可以选择适用于 Windows、Linux 和 macOS 的网络代理。如果您仅为一种操作系统（例如 macOS）选择网络代理，则将为所选操作系统创建独立的安装包。如果您为多个操作系统选择网络代理，Kaspersky Security Center 云控制台将根据以下优先级仅创建一个独立安装包：Windows 优先级最高，然后是 Linux，最后是 macOS。例如，如果您选择适用于 Linux 和 macOS 的网络代理，则 Kaspersky Security Center 云控制台会创建适用于 Linux 的网络代理的独立安装包。您可以随时为任何这些操作系统手动创建网络代理独立安装包。

- 卡巴斯基安全应用程序

  选择适合组织中客户端设备上安装的操作系统的安装包。

步骤 2：配置代理服务器

如果您的组织使用代理服务器连接到互联网，请在向导的此步骤中指定代理服务器设置。这些设置将添加到网络代理安装包中。安装后，网络代理会自动在每个客户端设备上使用这些设置。

为代理服务器连接指定以下设置：

- **使用代理服务器**
- **地址**
- **端口号**
- **代理服务器身份验证**

  如果启用该选项，您可以在输入字段中为代理服务器身份验证指定凭证。

  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。

- 用户名

  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帐户的凭据。

- 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。

步骤 3：配置卡巴斯基安全网络

如果您在向导的第一步下载了 Kaspersky Endpoint Security for Windows 安装包，则会显示以下应用程序的 KSN 声明文本：

- Kaspersky Endpoint Security for Windows
- 安装在本地设备上的 Kaspersky Security Center
- 安装在云环境中的 Kaspersky Security Center 云控制台

如果您没有下载 Kaspersky Endpoint Security for Windows 安装包，则不会显示该应用程序的 KSN 声明。

在试用模式下，仅显示 Kaspersky Endpoint Security for Windows 的 KSN 声明。

仔细阅读卡巴斯基安全网络声明。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 云控制台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 云控制台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。

默认情况下，KSN 的使用处于禁用状态。稍后，如果您改变主意使用 KSN，则可以在管理服务器属性窗口的 **“KSN 设置”**部分中启用（或禁用）相应选项。

步骤 4：配置第三方更新管理

如果*查找漏洞和所需更新*任务已存在，则不会显示此步骤。

如果您想要获取受管理设备上安装的应用程序的更新列表以及已发现的漏洞和建议的修复程序的列表，请启用**搜索第三方软件更新和漏洞修复**选项。如果启用此选项， Kaspersky Security Center 云控制台将创建*查找漏洞和所需更新*任务。

步骤 5：创建基本的网络保护配置

在向导的此步骤中，单击**创建**按钮以创建客户端设备初始保护所需的对象。

Kaspersky Security Center 云控制台会执行两项操作：

- 使用默认设置创建基本策略和任务

  创建以下策略：

  - Kaspersky Security Center 网络代理策略
  - 受管理 Kaspersky 应用程序策略

  创建以下任务：

  - 创建"*将更新下载至分发点存储库*"任务
  - *查找漏洞和所需更新*任务

    仅当您在**向导的上一步搜索第三方软件更新和漏洞修复**搜索第三方软件更新和漏洞修复选项时，才会创建此任务。
  - 受管理 Kaspersky 应用程序的任务

- 为网络代理创建独立安装包

  您将使用此包在分发点上安装网络代理。Kaspersky Security Center 云控制台根据您在向导的上一步中选择的网络代理安装包创建独立安装包。在创建程序包期间，您必须阅读并接受网络代理 EULA 的条款。创建独立安装包后，系统会提示您将其下载到您当前使用的设备上。

  创建网络代理独立安装包可能需要一些时间。您可以继续执行向导的下一步。该过程将在后台模式下继续。您可以在**进行中()**部分的**安装包**选项卡上跟踪该过程（**发现和部署→部署和分配→安装包**）。

  出于身份验证原因，每个独立安装包都会使用证书进行签名。该证书会不时重新颁发。每次重新颁发证书的过程结束后，Kaspersky Security Center 云控制台都会自动更新所有创建的独立安装包的签名。对于下载的独立安装包，无法进行自动签名更新。因此，使用独立安装包安装应用程序时，可能会出现证书过期、证书错误的情况。此时请重新下载独立安装包。

步骤 6：关闭快速启动向导

在快速启动向导完成页面上，了解在客户端设备上部署卡巴斯基安全应用程序时必须执行的其他操作。按照卡巴斯基应用程序初始部署方案中提供的阶段进行操作。

卡巴斯基应用程序初始部署

本节介绍卡巴斯基应用程序在组织中客户端设备上的初始部署。

方案：卡巴斯基应用程序初始部署

此方案描述如何在 Kaspersky Security Center 云控制台中的客户端设备上安装卡巴斯基应用程序。首先，您必须在网络上部署分发点。然后，您必须通过分发点执行网络轮询并发现网络上的联网设备。之后，您可以在联网设备上部署卡巴斯基应用程序。

该方案完成后，卡巴斯基应用程序将部署在组织网络中选定的客户端设备上。您可以管理所有安装了卡巴斯基应用程序的设备。

先决条件

在开始之前，请确保满足以下先决条件：

- 快速启动向导完成。
- 网络代理和安全应用程序安装包得到创建。
- 地址 https://aes.s.kaspersky-labs.com/endpoints/ 包含在受管理设备防火墙例外中。
- 您拥有有关组织中客户端设备的互联网设置的信息、有关网关的信息以及代理服务器设置。

阶段

Kaspersky 应用程序初始部署分阶段进行：

1. **分配受管理设备作为分发点**

   在 Kaspersky Security Center 云控制台中，分发点用于：

   - 网络轮询和设备发现
   - 在客户端设备上远程安装网络代理
   - 将客户端设备连接到管理服务器（当分发点充当连接网关时）

   选择组织网络上的设备作为管理组的分发点。所选设备必须满足分配点的要求。根据组织网络中客户端设备的数量，选择正确数量的设备作为分发点。

2. **为网络代理创建独立安装包**

   为网络代理创建独立安装包以安装在分发点上。

   如果您的客户端设备无法直接访问互联网来连接到管理服务器，请在网络代理安装包设置中配置连接网关和代理服务器设置。

3. **在所选设备上安装网络代理以充当分发点**

   通过任意方式将网络代理的独立安装包下发至所选设备。例如，您可以将独立安装包复制到可移动驱动器（例如闪存驱动器），或将其放置在共享文件夹中。

在独立安装包文件的**"属性"**窗口中，验证网络代理的独立安装包是否经过卡巴斯基签名。

在所选设备上运行网络代理的独立安装包的安装。网络代理现已根据网络代理安装包的设置进行安装，并连接到管理服务器。带有网络代理的设备被放置在创建网络代理的独立安装包时指定的管理组中。

如果在运行 Microsoft Windows XP Professional for Embedded Systems 32 位的设备上使用独立安装包安装网络代理，安装将失败。要解决此问题，请从 Microsoft 网站预先安装适用于 Windows XP 的更新 KB2868626：https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626。

4. **将安装了网络代理的设备分配为分发点**

   指定安装了网络代理的设备作为分发点。

5. **为分发点配置和执行网络轮询**

   为安装了网络代理的分发点配置网络轮询。作为一个选项，您可以在网络代理策略中配置网络轮询。

   根据计划完成网络轮询后，将发现连接到组织网络的客户端设备并将其放置在**未分配的设备**组中。

6. **为网络代理和受管理卡巴斯基应用程序创建安装包**

   如果您没有启动快速启动向导，或者跳过了创建安装包的步骤，请创建卡巴斯基应用程序的安装包。您必须为网络代理和受管理卡巴斯基应用程序创建适合组织网络上客户端设备上安装的操作系统的安装包。

7. **删除不兼容的第三方安全应用程序**

   如果组织网络上的客户端设备上安装了第三方安全应用程序，请在安装卡巴斯基应用程序之前将其删除。

8. **安装卡巴斯基应用程序到客户端设备**

   创建任务以在组织网络上的客户端设备上安装网络代理和受管理卡巴斯基应用程序。创建任务时，使用**远程安装应用程序**任务类型。对于安装网络代理的任务，请使用**通过分发点使用操作系统资源**选项。对于安装受管理卡巴斯基应用程序的任务，请使用**使用网络代理**选项。创建任务后，您可以配置其设置。确保每个任务的计划都符合要求。首先，必须运行安装网络代理的任务。然后，在客户端设备上安装网络代理后，必须运行安装受管理卡巴斯基应用程序的任务。

   作为一种选择，您可以创建一个远程安装任务，以在组织网络上的客户端设备上安装网络代理和受管理卡巴斯基应用程序。在这种情况下，在**安装包**中，使用**选择安装包**选项和**选择网络代理**选项；在**强制下载安装包**块中，使用**通过分发点使用操作系统资源**选项。

   您还可以创建多个远程安装任务来为不同的管理组或不同的设备分类安装受管理的卡巴斯基应用程序。

   如果您的客户端设备不在分发点网络内（例如，远程用户的笔记本电脑），则必须通过任何方法创建网络代理独立安装包并将其传送到这些客户端设备。在这些客户端设备上本地安装网络代理独立安装包。然后，您可以按照与分发点发现的其他设备相同的说明在这些远程用户的设备上安装受管理卡巴斯基应用程序。

   运行远程安装任务。

   作为一个选项，要安装卡巴斯基应用程序，您可以启动保护部署向导。

9. **安装 Kaspersky Security for Mobile**

   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。

10. **验证卡巴斯基应用程序的初始部署**

    生成并查看**卡巴斯基软件版本报告**。确保受管理的卡巴斯基应用程序安装在组织中的所有客户端设备上。

对于全盘加密，Kaspersky Security Center 云控制台仅支持 BitLocker。

创建卡巴斯基应用程序的安装包

要在组织中的联网设备上部署卡巴斯基应用程序，您必须在 Kaspersky Security Center 云控制台中创建卡巴斯基应用程序的安装包。

要创建卡巴斯基应用程序安装包：

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有关新安装包的通知。如果有关于新安装包的通知，您可以点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. 在向导的第一页上，选择“**为卡巴斯基应用程序创建安装包**”。

   将显示 Kaspersky Web 服务器上的可用分发包列表。

4. 单击分发包名称。例如，**Kaspersky Endpoint Security for Windows (<版本号>)**。

   带有分发包信息的窗口打开。

5. 阅读信息，然后单击“**下载并创建安装包**”按钮。

   如果分发包无法自动转换为安装包，将显示“**下载分发包**”按钮而不是“**下载并创建安装包**”按钮。在这种情况下，请下载分发包，然后使用下载的文件创建自定义安装包。

   下载安装包开始。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。

   如果您计划执行从 Kaspersky Security Center Web Console到 Kaspersky Security Center 云控制台的迁移，并且您组织的安全法规要求在访问公司网络时使用代理，这可能会影响迁移过程。创建网络代理安装包后，您必须指定代理设置以确保受管理设备上的网络代理实例与Kaspersky Security Center 云控制台工作区之间的连接：

   a. 单击安装包名称。

   b. 在打开的安装包属性窗口中，转到“**设置**”选项卡。

   c. 打开“**连接**”区域。

   d. 选择**使用代理服务器**选项并填写**代理服务器地址**和**代理服务器端口**字段。

6. 对于一些 Kaspersky 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. 点击“**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**”按钮。
   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 (×) 以关闭含有分发包信息的窗口。

安装包已创建。安装包出现在安装包列表。

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。
   在新建任务向导的**新任务**窗口中，在**任务类型**字段中选择**分发安装包**。您还可以在**任务名称**字段中编辑任务的默认名称。
   在下一步中，指定任务范围的从属管理服务器并按照新建任务向导的说明进行操作。完成后，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。

   > 当您为本地运行的从属管理服务器创建分发安装包任务时，分发范围（除了自定义安装包）将仅包括本地运行的 Kaspersky Security Center Web Console 支持的卡巴斯基应用程序的安装包，无论选择哪个分发选项（**所有安装包**或**选择的安装包**）。

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。

为网络代理创建独立安装包

您和组织中的设备用户可以使用独立安装包在设备上在本地安装网络代理。可以为运行 Windows、Linux 或 macOS 的设备创建独立安装包。

> 在 Kaspersky Security Center 云控制台中，您只能为网络代理创建独立安装包。

独立安装包是一个可执行文件。它可由电子邮件发送，也可以其他方式传送传送到客户端设备。收到的文件可以在本地客户端设备上运行已安装网络代理，不涉及 Kaspersky Security Center 云控制台。

对于 Network Agent for Linux 和 Network Agent for macOS，独立安装包是扩展名为 .sh 的脚本文件。当您运行此文件时，脚本会解压附加的存档，其中包含安装包及其设置，然后开始安装。

如果在运行 Microsoft Windows XP Professional for Embedded Systems 32 位的设备上使用独立安装包安装网络代理，安装将失败。要解决此问题，请从 Microsoft 网站预先安装适用于 Windows XP 的更新 KB2868626：https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626。

出于身份验证原因，每个独立安装包都会使用证书进行签名。该证书会不时重新颁发。每次重新颁发证书的过程结束后，Kaspersky Security Center 云控制台都会自动更新所有创建的独立安装包的签名。对于下载的独立安装包，无法进行自动签名更新。因此，使用独立安装包安装应用程序时，可能会出现证书过期、证书错误的情况。此时请重新下载独立安装包。

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”**。

   此时将显示安装包的列表。如果列表中没有网络代理安装包，请手动创建该安装包。

2. 在安装包列表中，单击网络代理安装包的名称。

   显示网络代理安装包的属性窗口。

3. 如有必要，配置网络代理安装包的设置，然后关闭网络代理安装包的属性窗口。

4. 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。

5. 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。

6. 在向导的第一页，如果要将网络代理与所选应用程序一起安装，请确保已启用**“网络代理和该应用程序一起安装”**选项。

   默认情况下已启用该选项。如果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。

7. 在向导的**“移动到受管理设备列表”**页面上，默认情况下已选择**“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，则不要更改选项选择。

   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。

8. 如果您希望在向导完成后显示**打开独立包列表**选项。

9. 单击“**完成**”按钮。
   独立安装包创建向导关闭。

网络代理独立安装包已创建。创建的独立安装包显示在独立安装包列表中，您可以查看。

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：

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**”。

   此时将显示安装包的列表。

2. 在列表上方，单击“**查看独立包列表**”按钮。

将显示独立安装包的列表。

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。
- **网络代理安装包名称**。
- **网络代理版本**。
- **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。
- **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“**下载**”按钮将独立安装包下载到设备上。

出于身份验证原因，每个独立安装包都会使用证书进行签名。该证书会不时重新颁发。每次重新颁发证书的过程结束后，Kaspersky Security Center 云控制台都会自动更新所有创建的独立安装包的签名。对于下载的独立安装包，无法进行自动签名更新。因此，使用独立安装包安装应用程序时，可能会出现证书过期、证书错误的情况。此时请重新下载独立安装包。

- 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：

- 在涉及 Kaspersky Security Center 云控制台的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（包括可执行文件）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，您可以指定命令行选项，例如以静默模式安装应用程序。

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. 在向导的第一页上，选择“**从文件创建安装包**”。
4. 在向导的下一页上，指定安装包名称，然后单击“**浏览**”按钮。

   标准的**“打开”**窗口允许您选择存档文件来创建安装包。
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。

   文件将下载到 Kaspersky Security Center 云控制台管理服务器。

   如果管理服务器检测到存档包含卡巴斯基应用程序，则会显示错误消息。您可以从卡巴斯基网络服务器下载卡巴斯基应用程序的安装包。通过选择**操作 → 卡巴斯基应用程序 → 当前应用程序版本**即可执行此操作。
6. 在向导的下一页上，如果所选存档文件包含多个可执行文件，请选择一个必须运行的可执行文件才能使用创建的安装包安装应用程序。
7. 如果需要，可以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。有关命令行参数的详细信息，请参阅应用程序供应商的文档。

安装包创建开始。

该向导将在过程完成时通知您。

如果未创建安装包，则会显示错误消息。

在 Kaspersky Security Center 云控制台中，管理服务器上所有安装包的总大小限制为 500 MB。如果在创建安装包的过程中超出了总大小限制，请删除之前创建的安装包。安装包的大小显示在其属性中。

8. 单击**完成**按钮关闭向导。

创建的自定义安装包将下载到管理服务器。下载后，安装包出现在安装包列表。

在安装包列表中，您可以查看自定义安装包的以下属性：

- **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)** 。自定义安装包的大小。
- **操作系统**为其创建自定义安装包的操作系统。
- **创建日期**。安装包创建日期。
- **修改日期**。安装包修改日期。
- **类型**。卡巴斯基应用程序或第三方应用程序。

在安装包列表中，通过单击自定义安装包名称的链接，您可以更改命令行参数和自定义安装包名称。

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。

此外，分发点必须具有互联网访问权限且必须始终保持连接。

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。

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。

考虑到基于 Windows、macOS 和 Linux 的设备，有多种设置可用。

“常规”选项卡

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**”块，您可以选择策略的模式：
  - **活动**
  - **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。

事件配置选项卡

通过该选项卡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）。通过单击“**属性**”按钮，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。

应用程序设置选项卡

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，客户端设备仅通过分发点接收更新，而不是直接从更新服务器。

  如果禁用此选项，客户端设备可以从不同的源接收更新：直接从更新服务器和从本地或网络文件夹。

  默认情况下已禁用该选项。

- 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

  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或漫游策略的名称
  - 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
  - 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。“**存储库**”区域的设置仅在运行 Windows 的设备上可用：

- 已安装应用程序详情
- 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。

- 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

软件更新和漏洞

在“**软件更新和漏洞**”区域，您可以配置搜索 Windows 更新以及启用扫描可执行文件以发现漏洞。“**软件更新和漏洞**”区域的设置仅在运行 Windows 的设备上可用：

- 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。

  默认情况下已禁用该选项。

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。“**重启管理**”区域的设置仅在运行 Windows 的设备上可用：

- 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。“**Windows 桌面共享**”区域的设置仅在运行 Windows 的设备上可用：

- 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
  - 在 Kaspersky Security Center 云控制台的事件数据库中

  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**部分中，您可以在受管理设备上配置更新的下载和分发以及补丁的安装：启用或禁用**对未定义状态的组件自动安装可应用更新和补丁**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。

- 在到管理服务器的连接”设置组中，您可以指定以下设置：
  - 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 UDP 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。

  - 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

  如果需要受管理设备通过 UDP 端口连接到 KSN 代理，启用“使用 UDP 端口”选项，并在“UDP 端口”字段中指定端口号。默认情况下已启用该选项。连接到 KSN 代理的默认 UDP 端口是 15111。

- 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“**运行推送服务器**”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，无法向“**管理服务器连接配置文件**”列表添加任何新项目，因此“**添加**”按钮处于不活动状态。预设的连接配置文件也不能修改。

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
- 在指定时间间隔连接

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。轮询设置仅在运行 Windows 的设备上可用。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，则分发点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，则管理服务器将不轮询网络。

  默认情况下已启用该选项。

- 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**”链接可配置轮询计划。

  如果禁用此选项，则分发点将不轮询 IP 范围。

  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

在“**分发点网络设置**”区域中，可以指定互联网连接设置：

- 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 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。

运行 Linux 或 macOS 的分发点设备不支持此功能。

分发点发送列在卡巴斯基安全网络声明中的 KSN 统计信息到 Kaspersky。默认下，KSN 声明位于 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。

默认情况下已禁用该选项。启用该选项仅在**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。

- 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

  如果需要受管理设备通过 UDP 端口连接到 KSN 代理，启用“**使用 UDP 端口**”选项，并在“**UDP 端口**”字段中指定端口号。默认情况下已启用该选项。连接到 KSN 代理的默认 UDP 端口是 15111。

网络代理策略设置：按操作系统比较

下表显示了您可以使用哪些网络代理策略设置来配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	✓	✓	✓
设置	✓	✓ 除了**使用卸载密码**复选框之外。	✓ 除了**使用卸载密码**复选框之外。
存储库	✓	–	✓ 下列选项可用： • 已安装应用程序详情 • 注册硬件表的详细信息
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”复选框。	除了“在 Microsoft Windows 防火墙中打开网络代理端口”复选框。
连接→连接计划	✓	✓	✓
通过分发点的网络轮询	✓ 下列选项可用： • Windows 网络 • IP 范围 • 域控制器（Microsoft Active Directory）	–	✓ 下列选项可用： • IP 范围 • 域控制器（Microsoft Active Directory、Samba 作为 Active Directory）
分发点网络设置	✓	✓	✓
KSN 代理(分发点)	✓	–	✓

网络代理安装包设置

要配置网络代理安装包：

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. 单击带有网络代理安装包名称的链接。

   网络代理安装包的属性窗口打开。窗口中的信息按选项卡和部分分组。

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

- 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

  如果选中此复选框，将自动安装所有下载的网络代理更新和修补程序。

  如果该复选框被清空，所有下载的更新和补丁仅在您更改其状态到*已批准*后被更新。带有*未定义*状态的更新和补丁将不被安装。

  默认情况下已选中该选框。

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：

- 使用 UDP 端口

  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 UDP 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。

- 不使用代理服务器
- 使用代理服务器
  代理服务器地址
  代理服务器端口
- 代理服务器身份验证

  如果启用该选项，您可以在输入字段中为代理服务器身份验证指定凭证。
  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。

  用户名

  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帐户的凭据。

  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。

高级

在**高级**区域，可以配置如何使用连接网关：

- 通过使用连接网关连接到管理服务器
- 连接网关地址
- 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。

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	✓	✓ *除了“在 Microsoft Windows 防火墙中打开网络代理端口”复选框	✓ *除了“在 Microsoft Windows 防火墙中打开网络代理端口”复选框
高级	✓	✓	✓
附加组件	✓	✓	✓
标签	✓	✓ * 除了自动标记规则	✓ * 除了自动标记规则
修订历史	✓	✓	✓

虚拟基础架构

Kaspersky Security Center 云控制台支持虚拟机的使用。为了保护您的虚拟基础架构，您需要在每个虚拟机上安装网络代理。

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 云控制台功能。

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 云控制台支持动态虚拟机。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。安装了网络代理的虚拟机也会添加到管理服务器数据库中。在您关闭该虚拟机后，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）。

对虚拟机复制的支持

Kaspersky Security Center 云控制台支持复制已安装网络代理的虚拟机或从已安装网络代理的模板创建虚拟机。

网络代理可以在以下情况下自动检测虚拟机的复制：

- “**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。

适用于 Windows、macOS 和 Linux 的网络代理的使用：比较

与 Windows 网络代理相比，适用于 MacOS 和 Linux 的网络代理具有一些功能限制。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。

网络代理功能比较

网络代理功能	Windows	Linux	MacOS
		安装	
自动安装网络代理的更新和补丁	✓	–	–
自动分发密钥	✓	✓	✓
通过在设备上运行应用程序安装程序来手动安装	✓	✓	✓
强制同步	✓	✓	✓
		分发点	
网络轮询	✓ • IP 范围轮询 • Windows 网络轮询 • 域控制器轮询	✓ • IP 范围轮询 • 域控制器轮询（Microsoft Active Directory、Samba 作为	–

	（Microsoft Active Directory）	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	✓	✓	– 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。
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。	
处理第三方应用程序			
在设备上远程安装应用程序	✓	–	–
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	✓	–	–
管理设备重启	✓	–	–
连接管理器	✓	✓	✓

远程连接至客户端设备桌面	✓	–	–

分发点属性中显示以下部分，但适用于 macOS 的网络代理不支持相应的功能：

- 更新源
- KSN 代理服务器
- Windows 域
- 活动目录
- IP 范围
- 高级
- 统计

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 云控制台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 云控制台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 云控制台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。

替换第三方安全应用程序

通过 Kaspersky Security Center 云控制台进行 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 云控制台提供几种卸载第三方应用程序的方法。

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。您可以在保护部署向导中找到此选项。当该选项被启用时，Kaspersky Security Center 云控制台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。

通过专用任务卸载不兼容的应用程序

要通过任务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。

手动安装应用程序的选项

您可以在本地设备上安装网络代理，无需涉及 Kaspersky Security Center 云控制台。为此，请按照以下主题中的描述为网络代理创建一个独立安装包：创建独立安装包。将安装包传输到您的客户端设备并安装它。网络代理安装完成后，您可以将该设备用作分发点。

保护部署向导

要安装 Kaspersky 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**”。

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**按钮进行向导。

步骤 1：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 2：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 3：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 4：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。

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。

步骤 5：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 6：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 云控制台自动卸载不兼容的应用程序，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 7：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 8：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，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来安装应用程序。

  要指定运行应用程序安装程序的用户账户，请单击**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。

步骤 9：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。

用于与外部服务交互的网络设置

Kaspersky Security Center 云控制台使用以下网络设置与外部服务交互。

网络设置

网络设置	地址	描述
端口：443 协议：HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	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	更新卡巴斯基数据库、软件模块和应用程序。

	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	
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。
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	更新卡巴斯基数据库、软件模块和应用程序。

	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	
端口：443 协议：HTTPS	ds.kaspersky.com	使用卡巴斯基安全网络。
端口：443、1443 协议：HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	使用卡巴斯基安全网络。
协议：HTTPS	click.kaspersky.com redirect.kaspersky.com	打开界面中的链接。
端口：80 协议：HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	公钥基础设施 (PKI)。
端口：443 协议：HTTPS	https://ipm-klca.kaspersky.com	营销公告。

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。

在您开始之前：

- 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。
- 从卡巴斯基网站下载必要的网络代理安装文件。

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/ksc64/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 云控制台 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。
6. 执行任何 Linux 设备通用的准备步骤。

设备准备好。您现在可以继续安装网络代理。

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. 确保目标 Linux 设备上安装了以下软件：

- Sudo
- Perl 语言解释器版本 5.10 或更高版本

2. 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。

   在您打开的文件中，找到以 `%sudo` 开头的行（如果您使用 CentOS 操作系统，则以 `%wheel` 开头）。在该行下方指定以下内容：`<用户名> 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。

3. 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
   ```

4. 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。

5. 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。

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. 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。

c. 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`。

如果您在早于 20 版本的 Fedora 设备上使用 SSH 安装网络代理，可能返回错误。此种情况下，为了成功安装网络代理，请在 /etc/sudoers 文件注释出默认选项（用注释符号将其围住以防止其被解析）。对于可能导致 SSH 连接问题的默认选项的详细说明，请参考 Bugzilla bugtracker 网站。

移动设备管理

通过 Kaspersky Security Center 云控制台的移动设备保护的管理通过使用移动设备管理功能运行。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 Security for Mobile 应用提供。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。

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。

检测和响应能力

本部分包含有关卡巴斯基解决方案的信息，这些解决方案可集成到 Kaspersky Security Center 云控制台中以向控制台添加检测和响应功能。

关于检测和响应能力

Kaspersky Security Center 云控制台可以将其他卡巴斯基解决方案的功能集成到控制台界面中。例如，您可以将检测和响应功能添加到 Kaspersky Security Center 云控制台的功能中。

检测和响应解决方案旨在保护组织的 IT 基础架构免受复杂的网络威胁。该解决方案的功能将自动威胁检测与响应这些威胁的能力相结合，以抵御复杂的攻击，包括新的漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法。

您可以集成以下解决方案：

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Protection Platform（也称为 EPP）应用程序检测到威胁后， Kaspersky Security Center 云控制台会向警报列表添加新警报。警报包含有关检测到的威胁的详细信息，使您能够分析和调查威胁。您还可以通过创建威胁发展链图来可视化威胁。该图可及时描述检测到的攻击的部署阶段。

  作为响应，您可以选择预定义的响应操作之一，例如，隔离不受信任的对象、将受感染的设备与网络隔离或为不受信任的对象创建执行预防规则。

  有关解决方案激活的信息，请参阅Kaspersky Endpoint Detection and Response Optimum文档。

- Kaspersky Managed Detection and Response

  卡巴斯基 EPP 应用程序检测到威胁后， Kaspersky Security Center 云控制台会将新事件添加到事件列表中。事件包含有关检测到的威胁的详细信息。卡巴斯基或第三方公司的 MDR 安全运营中心 (SOC) 分析师会调查事件并提供解决事件的响应。您可以手动接受或拒绝所提供的措施，或启用自动接受所有响应的选项。

  有关解决方案激活的信息，请参阅Kaspersky Managed Detection and Response 文档。

- Kaspersky Endpoint Detection and Response Expert

  这是适合拥有 SOC 分析师团队的组织的解决方案。检测到的威胁被注册为警报或事件，可以分配给 SOC 分析师进行调查。Kaspersky Endpoint Detection and Response Expert 为您提供有关每个警报或事件的详细信息，以及用于警报和事件管理、威胁搜寻和自定义规则开发的工具。SOC 分析师或安全人员可以手动选择响应操作，也可以采取预定义的自动响应措施。

  有关解决方案激活的信息，请参阅Kaspersky Endpoint Detection and Response Expert 文档。

集成检测和响应功能后界面发生变化

以下卡巴斯基解决方案提供可集成到 Kaspersky Security Center 云控制台界面中的检测和响应功能：

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

下表列出了集成后解决方案在 Kaspersky Security Center 云控制台界面中所做的更改。

卡巴斯基集成解决方案带来的界面变化

解决方案	Kaspersky Security Center 云控制台中的更改
Kaspersky EDR Optimum	添加了以下元素： • **警报**部分（**监控和报告→警报**）。此解决方案检测到的警报列在**“最佳”**选项卡上。 • **控制板**的小部件（**监控和报告→控制板**）。
Kaspersky MDR	添加了以下元素： • **MDR**部分（**监控和报告→ MDR** ）。 • 显示 **MDR** 功能选项（**设置→界面选项→显示 MDR 功能**）。 • **控制板**的小部件（**监控和报告→控制板**）。
Kaspersky EDR Expert	添加了以下元素： • **警报**部分（**监控和报告→警报**）。此解决方案检测到的警报列在**“Expert”**选项卡上。 • **事件**部分（**监控和报告→事件**）。 • **威胁搜索**部分（**监控和报告→威胁搜索**）。 • **自定义规则**部分（**监控和报告→自定义规则**）。 • Kaspersky EDR Expert 的常规设置（**设置→整合→ Kaspersky EDR Expert** ）。 • **控制板**的小部件（**监控和报告→控制板**）。

发现联网设备并创建管理组

本节介绍联网设备的搜索和发现，以及为这些设备创建管理组。

Kaspersky Security Center 云控制台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。

搜索和发现功能可让您查找以下设备：

- Kaspersky Security Center 云控制台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 云控制台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

您必须在初始部署安全应用程序之前执行设备发现。当所有网络设备被发现时，您可以接收它们的信息并通过策略管理。常规网络轮询用于发现是否有新设备以及先前发现的设备是否仍在网络中。

完成该方案后，设备发现已设置完毕，并将根据指定的计划进行。

先决条件

在 Kaspersky Security Center 云控制台中，设备发现由分发点执行。在开始之前，请执行以下操作：

- 决定哪些设备将充当分发点。
- 在您选择的设备上安装网络代理。
- 手动分配设备以作为分发点。

阶段

方案实施分为几个阶段：

1. **选择发现类型**

   决定您要定期使用哪些发现类型。

2. **配置轮询**

   在每个分发点的属性中，启用并配置您选择的网络轮询类型： Windows 网络轮询、域控制器轮询或IP 范围轮询。确保投票时间表满足您组织的需求。

   如果域中包含联网设备，建议使用域控制器轮询。

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“**Unassigned devices**”组中。如果需要，可以设置自动将这些设备移至“**Managed devices**”组的规则。您也可以建立保留规则。

   如果您跳过该规则设置步骤，所有新发现的设备都将转到“**Unassigned devices**”组并保留在那里。如果需要，可以手动将这些设备移动到“**Managed devices**”组。如果您手动将这些设备移动到“**Managed devices**”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哪个组。

网络轮询操作完成后，检查新发现的设备是否按照配置的规则排列。如果未配置任何规则，设备将保留在“**Unassigned devices**”组。

网络轮询

Kaspersky Security Center 云控制台通过定期轮询 Windows 网络、IP 范围、Microsoft Active Directory 域控制器和 Samba 域控制器来接收有关网络结构和该网络上的设备的信息。对于 Samba 域控制器， Samba 4 用作 Active Directory 域控制器。网络轮询可以手动启动，也可以根据计划自动启动。

根据此轮询的结果，Kaspersky Security Center 云控制台更新未分配设备的列表。您还可以配置规则，将新发现的设备自动移至管理组。

Kaspersky Security Center 云控制台使用以下网络轮询方法：

- *IP 范围轮询*。Kaspersky Security Center 云控制台使用互联网控制消息协议 (ICMP) 数据包轮询指定的 IP 范围，并编译这些 IP 范围内的设备上的完整数据集。
- *Windows 网络轮询*。您可以运行两种 Windows 网络轮询中的任意一种：快速或完整。在快速轮询过程中，Kaspersky Security Center 云控制台只从所有域和工作组中设备的 NetBIOS 名称列表获取信息。在完整轮询中，需要每台客户端设备的以下信息，例如操作系统（OS）名称、IP 地址、DNS 名称和 NetBIOS 名称。
- *域控制器轮询*。有关 Active Directory 单元结构以及 Active Directory 组中设备的 DNS 名称的信息将记录到 Kaspersky Security Center 云控制台数据库中。

Windows 网络轮询、**发现和部署**、**域控制器轮询**方法的轮询结果分别显示在**发现** → “发现”部分中。

*IP 范围轮询*方法的轮询结果显示在**发现和部署**→**未分配的设备**部分中。

一台设备可以显示在多个检测区域中。如果在 HQ 域中检测到设备且其地址为 192.168.0.1，则该设备将出现在**Windows 域**部分和**未分配的设备**部分中。您可以修改每种轮询方法的网络轮询设置。例如，您可能想要修改轮询计划或者设置是否轮询整个活动目录森林还是仅指定域。

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 必须在网络中可用。

- 必须使用 Microsoft Computer Browser 服务，且主浏览器计算机必须在分发点上启用。
- 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，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. 单击要用于轮询网络的分发点的名称。
   分发点属性窗口将打开。
4. 选择**Windows 域轮询**部分。
5. 通过使用“**启用网络轮询**”切换按钮启用或禁用 Windows 网络轮询。
6. 配置快速轮询和完整轮询的计划。
7. 单击“**确定**”按钮。

   属性被保存并应用到所有发现的 Windows 域和工作组。

域控制器轮询

Kaspersky Security Center 云控制台支持轮询 Microsoft Active Directory 域控制器和 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，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。域控制器轮询是根据您设置的计划执行的。

先决条件

在轮询域控制器之前，请确保启用以下协议：

- 简单身份验证和安全层 (SASL)
- 轻量级目录访问协议 (LDAP)

确保域控制器设备上的以下端口可用：

- 389 用于 SASL

- 636 用于 TLS

使用分发点进行域控制器轮询

您还可以使用分发点轮询域控制器。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 云控制台中的域身份验证。

查看域控制器轮询结果

要查看域控制器轮询结果：

1. 在主菜单中，转到**发现和部署** → **发现** → **域控制器**。
   发现的组织单元列表被显示。
2. 选择组织单元，然后单击“**设备**”按钮。
   组织单元中的设备列表被显示。

您可以搜索列表和过滤结果。

IP 范围轮询

Kaspersky Security Center 云控制台尝试使用标准 DNS 请求为指定范围的每个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 云控制台数据库。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。如果该域未被配置，IP 子网轮询将没有结果。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。

最初，Kaspersky Security Center 云控制台从用于网络轮询的分发点设备的网络设置获取用于轮询的 IP 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 云控制台自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center 云控制台从 192.168.0.1 到 192.168.0.254 之间轮询所有地址。

如果您使用 Windows 网络轮询和/或 Active Directory 轮询，不建议使用 IP 范围轮询。

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，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. 单击要用于轮询网络的分发点的名称。
   分发点属性窗口将打开。
4. 选择**IP 范围轮询**部分。
5. 通过使用“**启用范围轮询**”切换按钮启用或禁用 IP 轮询。
6. 配置轮询计划。默认下，IP 轮询每 420 分钟（七小时）运行一次。
7. 如有必要，添加或修改要轮询的 IP 范围。
   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。
8. 单击“**确定**”按钮。

属性包保存并应用到所有 IP 范围。

配置 Samba 域控制器

Kaspersky Security Center 云控制台支持仅在 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 云控制台和 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。

如果要正确轮询 Samba 域控制器，您必须在 /etc/samba/smb.conf 文件中指定`netbios` 名称和`workgroup`参数。

添加和修改 IP 范围

最初，Kaspersky Security Center 云控制台从用于网络轮询的分发点设备的网络设置获取用于轮询的 IP 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 云控制台自动包含网络 192.168.0.0/24 到轮询地址。Kaspersky Security Center 云控制台从 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。

要添加新 IP 范围：

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. 单击要用于轮询网络的分发点的名称。
   分发点属性窗口将打开。
4. 选择**IP 范围轮询**部分。
5. 要添加新 IP 范围，请单击“**添加**”按钮。
6. 在打开的窗口，指定以下设置：

   - 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。

- 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。

7. 单击“**确定**”按钮。

新 IP 范围被添加到 IP 范围列表。

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。

分发点和连接网关的调整

Kaspersky Security Center 云控制台中的管理组结构执行以下功能：

- 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。分发点的最优分发可让您在企业网络中节省流量。

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。

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。使用下表计算您的网络所需的分发点数量。

确保您要用作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/5,000 + 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

如果分发点不可用，请手动或直接从卡巴斯基更新服务器更新卡巴斯基数据库、软件模块和应用程序。

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。

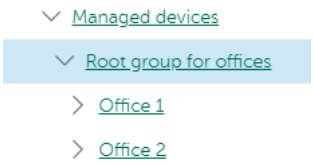
有以下构建管理组结构的方法：

- 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。
- 不考虑网络拓扑而构建管理组结构。此种情况下，您必须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。

手动分配分发点

Kaspersky Security Center 云控制台允许您手动指定设备做为分发点。我们建议您计算数字并配置您网络所需的分发点。

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。

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. 单击“**分配**”按钮。
4. 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。

5. 选择您要包含在所选分发点范围的管理组。

6. 单击“**添加**”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。

7. 在列表中选择新添加的分发点以打开其属性窗口。

8. 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 云控制台自动分配一个在给定范围内的唯一 IP 组播地址。

     - 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。

- 运行推送服务器

在 Kaspersky Security Center 云控制台中，分发点可以充当由网络代理管理的基于 Windows 和 Linux 的设备的推送服务器。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。

- 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。

运行 Linux 或 macOS 的分发点设备不支持此功能。

分发点发送列在卡巴斯基安全网络声明中的 KSN 统计信息到 Kaspersky。默认下，KSN 声明位于 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。

默认情况下已禁用该选项。启用该选项仅在**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。

- 通过分发点配置 Windows 域、活动目录和 IP 范围的轮询：

- Windows 域轮询

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 范围轮询**

  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 Zerocong 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。

9. 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)**" → "**组**"。
2. 在管理组结构中，选择您要查看其分配的分发点的管理组。

3. 单击“**分发点**”选项卡。

4. 通过使用“**分配**”按钮为管理组添加新分发点，或使用“**取消分配**”按钮删除已分配的分发点。

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。

将分发点用作推送服务器

在 Kaspersky Security Center 云控制台中，分发点可以充当由网络代理管理的基于 Windows 和 Linux 的设备的推送服务器。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。

您可以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。如果使用分发点作为推送服务器，则不必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. 单击要用作推送服务器的分发点。

4. 在所选分发点的属性列表中，转到**常规**部分，然后启用**运行推送服务器**选项。

   推送服务器端口输入字段变为可用。

5. 在**推送服务器端口**输入字段中，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。

   > 要在充当推送服务器的分发点和受管理设备之间建立连接，必须手动将指定的推送服务器端口添加到 Microsoft Windows 防火墙排除列表。

6. 单击**“确定”**退出分发点属性窗口，然后单击**“保存”**应用更改。

   启用**运行推送服务器**选项后，将在充当推送服务器的分发点上自动启用不断开与管理服务器的连接选项。此选项提供网络代理和管理服务器之间的早期连接。

7. 打开网络代理策略设置窗口。

8. 转至**连接→网络**，然后启用**使用分发点强制连接到管理服务器**选项。关闭此选项的锁。

9. 另外，在**网络**部分中，您可以禁用**使用 UDP 端口**选项。配置的推送服务器将在受管理设备和管理服务器之间提供连续的连接，而不是通过 UDP 端口发送数据包。

10. 单击“**确定**”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。

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 云控制台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，则可以使用“**不断开与管理服务器的连接**”选项来确保受管理设备与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. 执行以下操作之一：

   - 如果受管理设备直接（即不通过分发点）访问管理服务器：

     a. 在主菜单中，转到 “**设备 → 受管理设备**”。

     b. 单击您想要提供连续连接的设备的名称。
     受管理设备的属性窗口打开。

   - 如果受管理设备通过在网关模式下运行的分发点访问管理服务器，而不是直接访问：

     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“**分发点**”区域。

     c. 在分发点列表中，单击所需分发点的名称。
     将打开所选分发点的属性窗口。

2. 在打开的属性窗口的“**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。

创建管理组

最初，管理组的层次结构包含唯一名为**受管理设备**的管理组。当创建管理组层次结构时，您可以将设备和虚拟机添加到“**受管理设备**”组中，也可以添加子组。对于每个管理组，属性窗口包含有关与该组相关的策略、任务和设备的信息。

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. 选择您要创建新子组的管理组旁边的复选框。
3. 单击“**添加**”按钮。
4. 输入新管理组的名称。
5. 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。

应用程序允许基于 Active Directory 的结构或域网络构创建管理组层次结构。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。

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。

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。本节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。
     - 指定设备的 NetBIOS 名称或 DNS 名称。

       > 设备名称字段不得包含空格、退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、退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)**”→“**组**”→“**<组名称>**”→“**受管理设备**”。
   - 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。

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。

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

在开始之前，请确保您已完成Kaspersky Security Center 云控制台初始配置方案，包括快速启动向导。

当快速启动向导运行时，以下策略和任务在**受管理设备**管理组中被创建：

- 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（网络代理的任务）

阶段

分阶段配置网络保护：

1. **设置和传播 Kaspersky 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 Kaspersky 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。您还可以结合这两种方法。

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：

   - 为 Kaspersky Endpoint Security 设置组任务
   - 创建“*查找漏洞和所需更新*”任务

   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**

   受管理应用程序运行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。

   使用说明：设置最大事件数。

结果

当您完成该方案时，您将通过配置 Kaspersky 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：

- Kaspersky 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。

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。

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 Kaspersky 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

本节提供以设备为中心的集中配置安装到受管理设备上的 Kaspersky 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。

您也可能要考虑以用户为中心的安全管理作为以设备为中心的方案的附加选项。

进程

以设备为中心的 Kaspersky 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 云控制台为 Kaspersky Endpoint Security for Windows 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。

   如果您有几个管理组的层级结构，则子管理组默认从主管理服务器继承策略。您可以强制子组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. **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：

   - 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**

   Kaspersky Security Center 云控制台每小时会自动将管理服务器与受管理设备同步几次。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 Kaspersky 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 云控制台在设备属性中指定传送日期和时间。

   说明：强制同步

结果

当以设备为中心的方案完成时，Kaspersky 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

本节介绍以用户为中心的集中配置安装到受管理设备上的 Kaspersky 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。

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 Kaspersky 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 云控制台为 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。

   如果您有几个管理组的层级结构，则子管理组默认从主管理服务器继承策略。您可以强制子组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 Kaspersky 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**

   Kaspersky Security Center 云控制台每小时会自动将管理服务器与受管理设备同步几次。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 Kaspersky 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 云控制台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，Kaspersky 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。

Kaspersky Endpoint Security 策略的手动设置

本节提供有关如何配置 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) 是云服务的基础架构，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。

您可以在 Kaspersky Endpoint Security for Windows 策略属性窗口的**应用程序设置→高级威胁防护**部分中配置卡巴斯基安全网络工作。

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. 确保启用**“使用管理服务器作为 KSN 代理服务器”**选项。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**KSN 代理**选项并启用扩展 KSN 模式。
5. [可选]启用对 KSN 服务器的使用，如果 KSN 代理服务不可用。为此，请启用**“如果 KSN 代理服务器不可用，则使用卡巴斯基安全网络服务器”**选项。

   KSN 服务器可能位于 Kaspersky 端（当 KSN 被使用）或第三方端（当 KSN 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：

- **公共网络**。反病毒应用程序、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。
- **可信任网络**。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**”→“**关键威胁防护**”→“**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。

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 云控制台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。

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：
   - *最终用户授权许可协议被违反*
   - *应用程序自动运行被禁用*
   - *激活错误*
   - *检测到活动威胁。高级清除应该被启动*
   - *清除不可能*
   - *检测到先前打开的危险链接*
   - *禁止已终止*
   - *网络活动被阻止*
   - *检测到网络攻击*
   - *应用程序启动被禁止*
   - *访问被拒绝（本地库）*
   - *访问被拒绝 (KSN)*
   - *本地更新错误*
   - *无法同时启动两个任务*
   - *与 Kaspersky Security Center 交互错误*
   - *未更新所有组件*
   - *应用文件加密/解密规则错误*
   - *启用便携模式错误*
   - *禁用便携模式错误*

- *无法加载加密模块*
- *策略无法被应用*
- *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：
   - *自我保护已禁用*
   - *保护组件已禁用*
   - *备用密钥不正确*
   - *检测到可以被侵入者用于损害您的计算机或个人数据的合法软件（本地库）*
   - *检测到可以被侵入者用于损害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*
   - *用户已退出加密策略*
   - *文件已由管理员从 Kaspersky Anti Targeted Attack Platform 服务器上的隔离区恢复*
   - *文件被管理员隔离在 Kaspersky Anti Targeted Attack Platform 服务器上*
   - *向管理员发送的有关应用程序启动禁止的消息*
   - *向管理员发送的有关设备访问禁止的消息*
   - *向管理员发送的关于网页访问禁止的消息*
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：
    - *对象备份副本被创建*
    - *应用程序启动在测试模式中被禁止*
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）。

任务

该部分描述了 Kaspersky Security Center 云控制台使用的任务。

关于任务

Kaspersky Security Center 云控制台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*。任务可以在管理服务器和设备上执行。

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。

- *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多个组任务、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。

任务的执行结果保存在每个设备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

您可以在任务列表中创建任务；或者在**受管理设备**列表中选择设备，然后创建分配给所选设备的新任务。

在任务列表中创建任务：

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：

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。

1. 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。
2. 单击**运行任务**按钮，然后选择**创建新任务**。

   “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。
3. 单击“**完成**”按钮。

   任务为选定的设备创建。

查看任务列表

您可以查看在 Kaspersky Security Center 云控制台中创建的任务列表。

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。

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；或在**受管理设备**列表中选择设备，然后为其启动现有任务。

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。

为选择的设备启动任务

您可以在设备列表中选择一台或多台客户端设备，然后启动之前为它们创建的任务。这可让您运行之前为一组特定设备创建的任务。

这会将任务被分配到的设备更改到您在运行任务时选择的设备列表。

要为选择的设备启动任务：

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。

在受管理设备列表中，使用复选框选择要为其运行任务的设备。您可以使用搜索和过滤功能来查找您正在寻找的设备。

1. 单击**运行任务**按钮，然后选择**应用现有任务**。

   现有任务列表将得到显示。

2. 所选设备显示在任务列表上方。如有必要，您可以从此列表中删除设备。除一台设备之外您可以删除所有设备。

3. 在列表中选择所需的任务。您可以使用列表上方的搜索框按名称搜索所需的任务。只能选择一项任务。

4. 单击**保存并启动任务**。

所选任务立即为所选设备启动。任务中的计划启动设置不会更改。

常规任务设置和属性

本节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。

- 要分配任务的设备：

  - 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。

  - 手动指定设备地址或从列表导入地址

    任务被分配到特定设备。您可以通过以下方式指定设备：

    - 指定设备的 IP 地址、NetBIOS 名称或 DNS 名称。
    - 指定 IP 范围。
      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。
    - 选择管理服务器检测到的设备，包括未分配的设备。
      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。

  - 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。

- 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。

- 操作系统重启设置：
  - 不重启

    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。

- 任务计划设置：
  - **计划开始设置：**
    - 手动

      任务不自动运行。您仅可以手动启动。

      默认情况下已启用该选项。

    - 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，任务每六小时运行一次，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 云控制台。

  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

  任务定期运行，在指定星期的指定时间。

  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，不选择任何日期；默认开始时间为 6:00:00 PM。

- 当新更新下载至存储库时

当新更新下载到分发点存储库时，Kaspersky Security Center 云控制台会运行具有此计划的所有任务。网络代理在受管理设备和管理服务器（心跳）之间定期同步期间检查更新的可用性。

例如，您可能希望将此计划用于与安全应用程序（例如 Kaspersky Endpoint Security）相关的更新任务。

如果受管理设备上的网络代理在 25 小时或更长时间内没有检测到新更新，则 Kaspersky Security Center 云控制台会在此设备上运行具有此计划的所有任务。这些任务每小时运行一次，直到检测到新的更新。如果受管理设备与将更新下载到存储库的分发点之间没有连接，Kaspersky Security Center 云控制台也会每小时运行这些任务。

- 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反病毒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。您可以选择先前任务如何结束(成功或带有错误)以触发当前任务的启动。例如，您可能想使用“**开启设备**”选项运行 *管理设备*任务，在它完成后，运行 *病毒扫描*任务。仅当两个任务被分配给同一设备时，此参数才有效。

- 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 Kaspersky 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。

  如果该选项被禁用，则只有已计划的任务将在客户端设备上运行，而对于“**手动**”、“**一次**”和“**立即**”任务，仅会在网络中可见的客户端设备上运行。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。

  默认情况下已启用该选项。

- 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。

- 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：
  - 保存任务历史记录块：
    - 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
    - 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。

- **仅通知错误**
- **通过邮件通知**

- 任务范围设置：
- 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 云控制台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 云控制台允许您从 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。

- 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)**。

管理客户端设备

该部分说明如何管理管理组中的设备。

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。
  - 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。
  - 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 云控制台内的设备创建日期。

- 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
  - 操作系统生产商
  - 操作系统文件夹
  - 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。

- 操作系统内部版本

- “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

    自安装反病毒应用程序（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 云控制台定义的状态不同。

- 应用程序

  此选项卡列出了客户端设备上安装的所有 Kaspersky 应用程序。您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

  此选项卡列出了受管理设备上当前处于活动状态的策略和策略配置文件。

- 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。如果未建立连接，则不显示状态。

- 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。

- 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 Kaspersky 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

    点击**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。

- **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。

- **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 云控制台中）。
- 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 云控制台中）。
- 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。

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 云控制台提供大量的*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 云控制台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

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。
默认情况下已禁用该选项。

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“**活动目录**”子区域，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 Active Directory 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。

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（*设备上无数据*、*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（*设备上无数据*、*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（*设备上无数据*、*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（*设备上无数据*、*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，您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 Kaspersky 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 Kaspersky 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 云控制台管理的设备到分类：

  - **是**。应用程序包含通过 Kaspersky Security Center 云控制台管理的设备。
  - **否**。应用程序在分类中包含不通过 Kaspersky Security Center 云控制台管理的设备。
  - **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

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*。

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。

应用程序组件子区域包含在 Kaspersky Security Center 云控制台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。您也可以配置对所有版本的搜索，除了指定的值。

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。

- 必须被包含

  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。

- 必须被排除

  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。请注意，用户列表已被过滤并显示内部用户。搜索结果将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，您可以选择用于配置标准的用户账户。请注意，用户列表已被过滤并显示内部用户。搜索结果将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 云控制台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。

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到 CSV 或 TXT 文件。

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。

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. 点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 云控制台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 云控制台会考虑设备在网络中的可见性标志（请参见下表）。如果 Kaspersky Security Center 云控制台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，病毒扫描任务，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。	超过 0 天。
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 Kaspersky 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。	• 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	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

没有运行		关闭。 • 开关按钮被开启。

Kaspersky Security Center 云控制台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。

当 Kaspersky Security Center 云控制台为设备分配状态时，对于某些条件（请参见“条件描述”列），将考虑可见性标志。例如，如果某个受管理设备由于满足“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。

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。

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。可以在以下管理服务器之间切换设备管理：

- 主管理服务器及其虚拟管理服务器之一
- 同一主管理服务器的两个虚拟管理服务器

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**按钮进行向导。

3. 对于 Kaspersky Security Center 云控制台应用程序，选择“**更改管理服务器**”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. 选择要用于管理选定设备的管理服务器。

7. 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. 如果在“**完成任务创建**”页面上启用“**创建完成时打开任务详情**”选项，则可以修改默认任务设置。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。
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。
13. 运行创建的任务。

为其创建任务的客户端设备，在任务执行完毕后，将由任务设置中指定的管理服务器进行管理。

关于集群和服务器阵列

Kaspersky Security Center 云控制台现在支持集群技术。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 云控制台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 云控制台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。

设备标签

该部分描述了设备标签，提供了创建和修改它们以及手动或自动标记设备的说明。

关于设备标签

Kaspersky Security Center 云控制台可让您标记设备。*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。当您要标记单个设备时可以使用手动标记。自动标记由 Kaspersky Security Center 云控制台利用指定标记规则来执行。

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，如果您的网络包括运行 Windows、Linux 和 macOS 的设备，您可以设置一条规则，将 [Linux] 标签分配给所有基于 Linux 的设备。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 Linux 设备，并给它们分配任务。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. 点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。要从您的设备中删除标签，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。

设备列表仅显示分配了标签的设备。

要返回设备标签列表，点击您浏览器的**后退**按钮。

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. 点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。

您可以分配其他标签到设备或删除已经分配的标签。您也可以查看管理服务器上存在的所有设备标签。

手动标记设备

要分配标签到设备：

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。

要分配标签到多个设备：

1. 在主菜单中，转到**资产(设备)** → **受管理设备**。
2. 选择要为其分配标签的设备。
3. 单击**标签**，然后从下拉列表中选择**分配**。
4. 在打开的窗口中，从下拉列表中选择一个标签。
   如果需要，您可以选择多个标签。
   您也可以执行以下操作：
   - 通过单击**编辑**（ ）图标编辑标签名称。
     指定标签的新名称，然后单击**保存**按钮。

请注意，该标签也将在设备标签列表中被重命名。

- 通过单击**删除**（ ）图标删除标签。
  在打开的窗口中，单击**删除**。

  请注意，该标签也将被从管理服务器中删除。

5. 单击“**保存**”按钮。

标签将被分配到所需设备。您可以删除已分配的标签。

从设备上删除分配的标签

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。要删除这些标签，请使用 klscflag 实用程序。

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. 点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。

要从多个设备中删除标签：

1. 在主菜单中，转到**资产(设备)** → **受管理设备**。
2. 选择要删除其标签的设备。
3. 单击**标签**，然后从下拉列表中选择**删除**。
4. 在打开的窗口中，选中要删除的标签旁边的复选框。

   该窗口将显示分配给您在步骤 2 中选择的所有设备的所有标签。

5. 单击“**保存**”按钮。

标签将被从设备中删除。

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. 点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 云控制台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。
   - **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。
   - **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。

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 云控制台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。

Kaspersky Security Center 云控制台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。

从存储库下载文件

Kaspersky Security Center 云控制台可让您下载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。文件将复制到您指定的目标。

仅当满足以下条件之一时，您才可以下载文件：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

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. 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。

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. 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，选择要删除的文件并单击 **删除**。
3. 确认您要删除该文件。

已将文件放置在存储库（隔离或备份）中的客户端设备上的安全应用程序将从此存储库中删除相同的文件。

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)** → **组** → **<group name>** → **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. 点击所需设备的名称。
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. 点击“**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， Kaspersky Security Agent 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**”。

   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

仅当满足以下条件之一时，您才可以从客户端设备下载跟踪文件：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

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。
   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

仅当满足以下条件之一时，您才可以从客户端设备下载应用程序：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

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。

从客户端设备下载系统信息

仅当满足以下条件之一时，您才可以从客户端设备将系统信息下载到您的设备：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

要从客户端设备下载系统信息：

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**系统信息**选项卡。
3. 单击**下载**按钮可下载有关客户端设备的系统信息。

包含信息的文件将被下载到指定位置。

下载事件日志

仅当满足以下条件之一时，您才可以从客户端设备将事件日志下载到您的设备：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

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。

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。

运行应用程序的远程诊断并下载结果

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. 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，选择要对其运行远程诊断的应用程序。
   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 Kaspersky 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。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。

生成转储文件仅适用于在 Windows 客户端设备上运行的 32 位进程。对于运行 Linux 的客户端设备和 64 位进程，此功能不受支持。

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，选择单击**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**按钮以保存指定应用程序的转储文件。

   如果指定的应用程序未在客户端设备上运行，则会显示错误消息。

远程连接至客户端设备桌面

您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，您可以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您的工作站上。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 云控制台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。一旦您连接会话，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，必须满足以下条件：

- 客户端设备是管理组的成员，该管理组的分发点启用了**“不与管理服务器断开连接”**选项。
- 在客户端设备设置中，启用“**不要与管理服务器断开连接”**选项。

  选中“**Do not disconnect from the Administration Server**”选项时的最大客户端设备总数为 300。

要连接到客户端设备的桌面：

1. 在主菜单中，转到 “**资产(设备)** → **受管理设备**”。
2. 选中要获取访问权限的设备名称旁边的复选框。
3. 单击**连接到远程桌面**按钮。

   远程桌面 (仅 Windows)窗口打开。
4. 单击“**下载**”按钮以下载 klsctunnel 实用程序。

5. 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。

6. 运行 klsctunnel 实用程序。

   该实用程序窗口打开。

7. 将复制的文本粘贴到文本字段中。

8. 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。

9. 单击“**打开端口**”按钮。

   将打开远程桌面连接登录窗口。

10. 指定您当前用来登录 Kaspersky Security Center 云控制台的账户的凭据。

11. 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

您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。

您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，您和设备上的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您的工作站上。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 云控制台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你的连接请求。Kaspersky Security Center 云控制台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。

  您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：

- 您的工作站上安装了 Microsoft Windows Vista 或更高版本。

  要检查您的 Windows 版本是否包含 Windows 桌面共享功能，请确保 32 位注册表中包含 CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F}。

- 客户端设备上安装了 Microsoft Windows Vista 或更高版本。

- Kaspersky Security Center 云控制台使用漏洞和补丁管理授权许可。

- 客户端设备是管理组的成员，该管理组的分发点启用了**"不要与管理服务器断开连接"**选项，或者在客户端设备设置中启用了此选项。

  注意，选中**"Do not disconnect from the Administration Server"**选项时的最大客户端设备总数为 300。

要通过 Windows 桌面共享连接到客户端设备的桌面：

1. 在主菜单中，转到**资产(设备) → 受管理设备**。
2. 选中要获取访问权限的设备名称旁边的复选框。
3. 单击**Windows 桌面共享**按钮。

   Windows 桌面共享向导打开。
4. 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。
5. 单击**"下一步"**按钮。
6. 选择要连接的设备上的会话，然后单击**"下一步"**按钮。
7. 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，将打开向导的下一页。
8. 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。

9. 运行 klsctunnel 实用程序。

   该实用程序窗口打开。
10. 将复制的文本粘贴到文本字段中。
11. 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。
12. 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**。

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 云控制台管理服务器。该信息作为列表存储在**存储库**文件夹的**智能培训状态中的规则触发**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 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. 在主菜单中，转到**操作 → 存储库**。
2. 单击**智能培训状态中的规则触发**链接。
   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。

- 用户名

  运行进程的生成检测的客户端设备用户名称。

- 已处理

  异常被检测的日期

- 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 SHA-256 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 SHA-256 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 SHA-256 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 SHA-256 哈希（更多信息请参阅 Kaspersky Endpoint Security 帮助）。

要查看每个信息元素的属性：

1. 在主菜单中，转到**操作** → **存储库**。
2. 单击**智能培训状态中的规则触发**链接。
3. 在打开的窗口中，选择您需要的对象。
4. 单击**"属性"**链接。

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 for Windows 文档）。

要添加元素作为排除，

在检测列表中选择元素并点击“**排除**”按钮。

添加排除向导启动。遵照向导的说明操作。

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 for Windows 自适应异常控制规则添加排除。

要通过自适应异常控制节点启动添加排除向导：

1. 在主菜单中，进入**操作→存储库→智能培训状态中的规则触发**。
2. 在打开的窗口中，选择检测列表中的一个元素（或多个元素），然后单击**排除**按钮。
   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。

策略和策略配置文件

在 Kaspersky Security Center 云控制台中，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

*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 云控制台为管理组中的每个 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 Kaspersky 应用程序，只能有一个策略处于活动状态。设备对 Kaspersky 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。

> 您无法创建管理服务器策略。

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
Undefined	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*”。
Enforce	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：

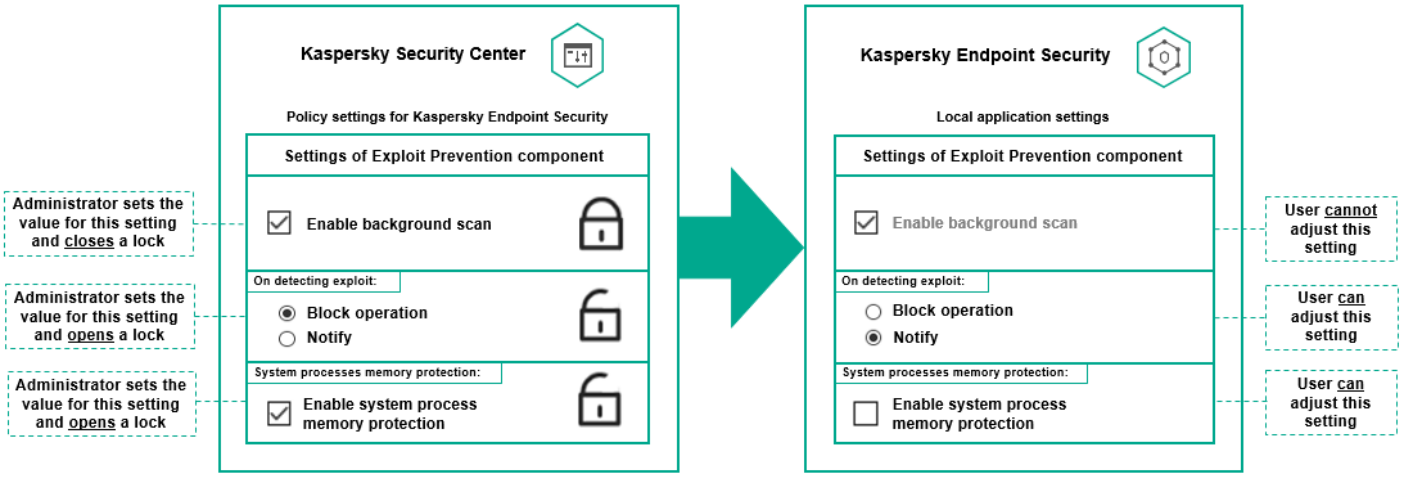
- 锁定管理子组策略的设置
- 在受管理设备上锁定本地 Kaspersky 应用程序的设置

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 Kaspersky 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 Kaspersky 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 Kaspersky 应用程序设置

策略继承和策略配置文件

本节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

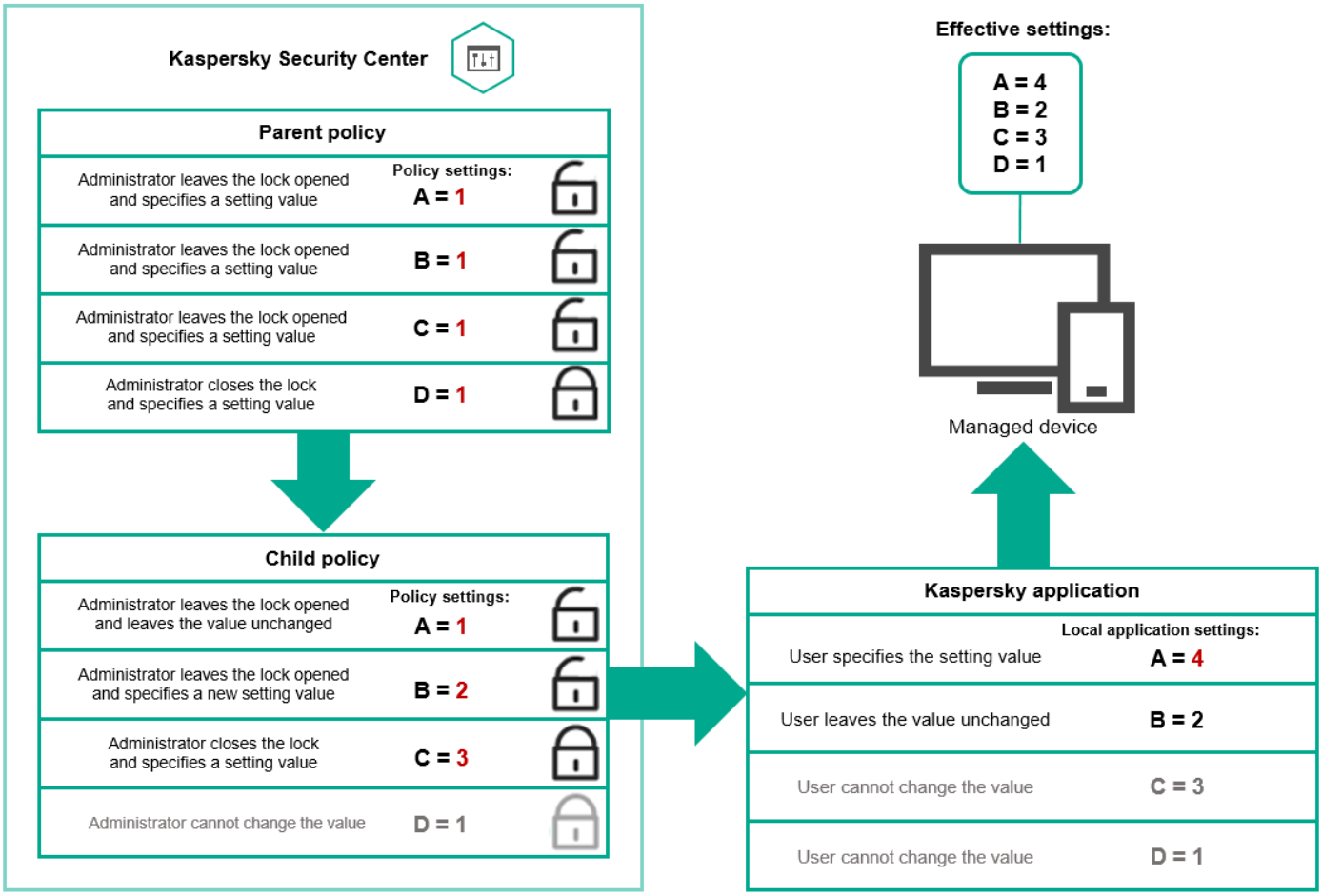
如果不同的设备需要不同的设置，则可以将设备组织到管理组中。

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）。

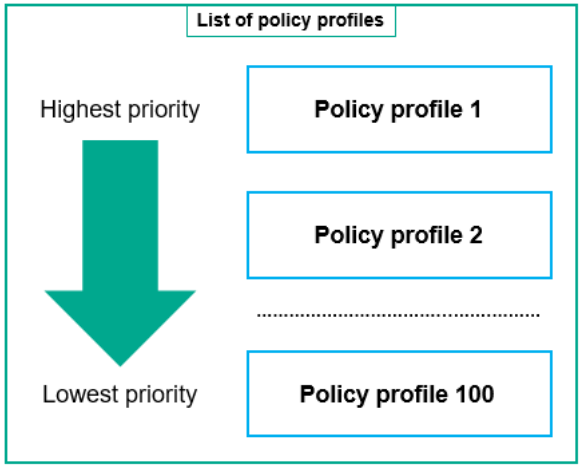


策略层级

策略层级中的策略配置文件

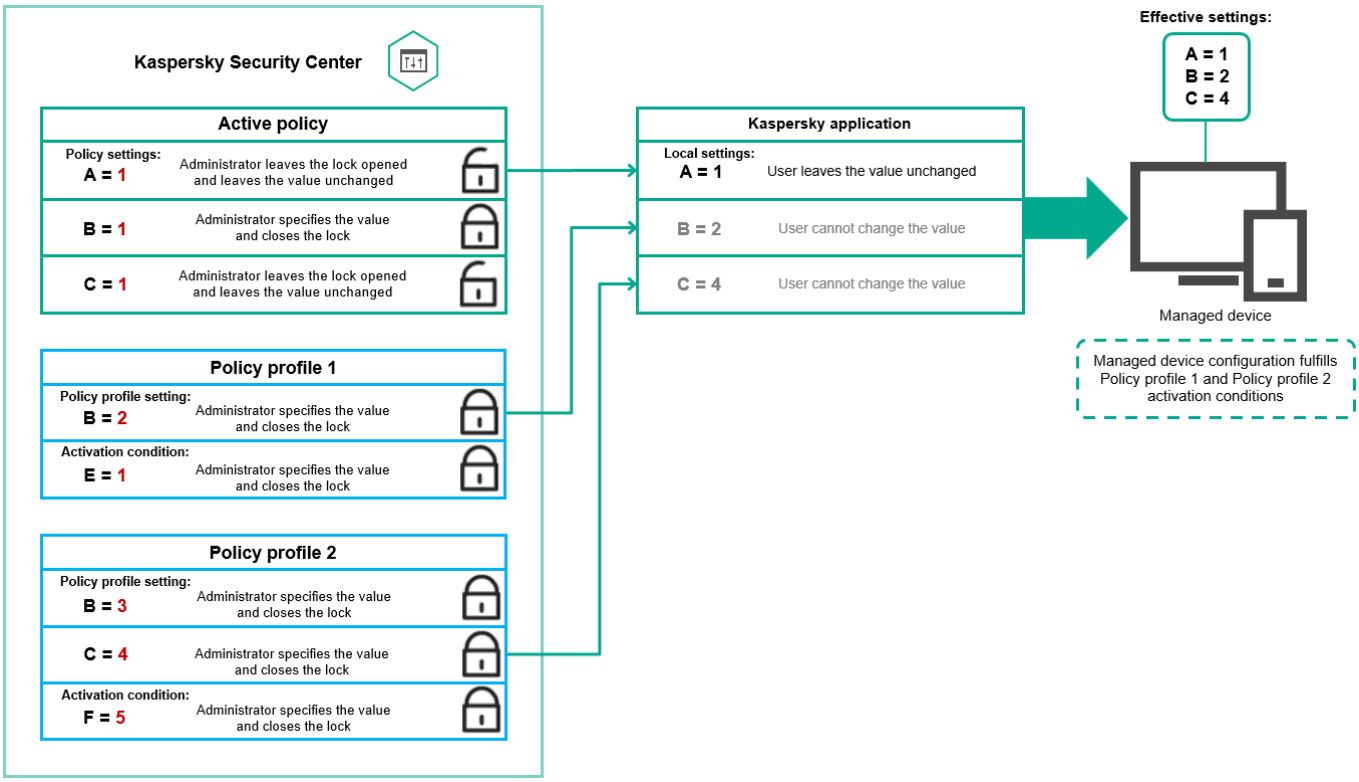
策略配置文件具有以下优先级分配条件：

- 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）。

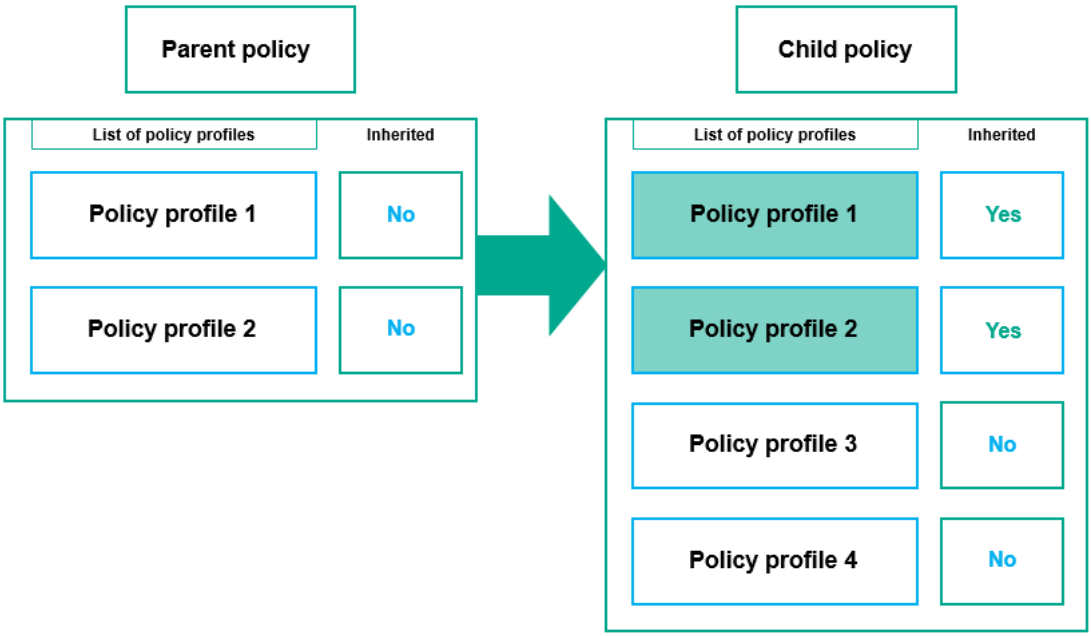


受管理设备配置满足多个策略配置文件的激活条件

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）。

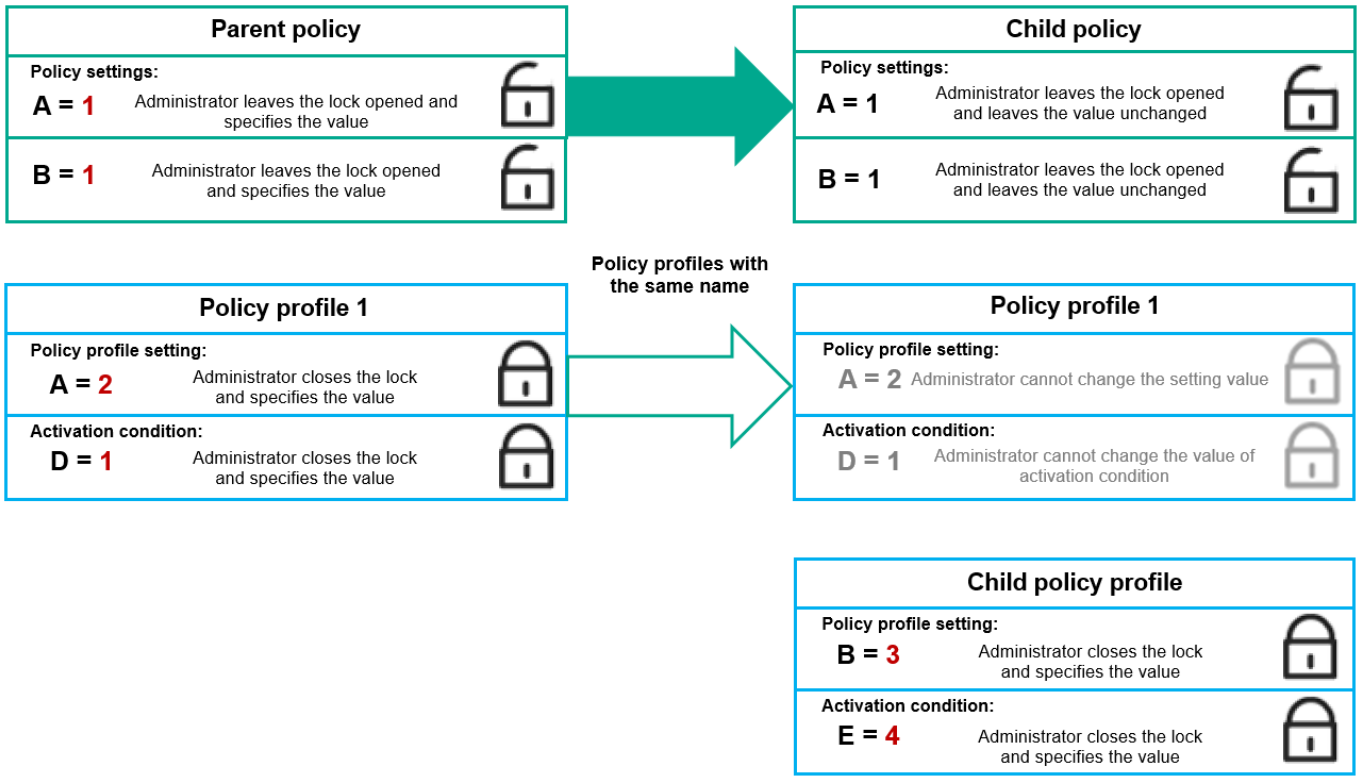


继承策略配置文件

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。

如何在托管设备上实施设置

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

本节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。

> 您无法创建管理服务器策略。

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. 单击**添加**。

   “**选择应用程序**”窗口将打开。
3. 选择您要为其创建策略的应用程序。
4. 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。
5. 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。
6. 单击“**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。
7. 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。

   应用程序设置取决于您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。
8. 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. 点击您要修改的策略。
   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**
  - 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**”区域可让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）。点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：
  - 存储在管理服务器数据库上(天)
  - 存储在设备的 OS 事件日志中
- 事件通知
  您可以选择是否希望通过电子邮件收到有关活动的通知。
  默认情况下，将使用在管理服务器属性选项卡上指定的通知设置(例如收件人地址等)。如果需要，您可以在**电子邮件**选项卡上更改这些设置。

修订历史

“**修订历史**”选项卡可让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。

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 云控制台允许您将策略、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 云控制台允许您从 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 云控制台中，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，单击“**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(如果可用)**。

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**在策略分发结果中显示设备的最大数量**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。

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. 选择**病毒爆发**区域。
3. 在右侧窗格中，单击“**配置在病毒爆发事件发生时要激活的策略**”链接。
   “**策略激活**”窗口将开启。
4. 在与检测病毒爆发的组件有关的区域中—用于工作站和文件服务器的反病毒、用于邮件系统的反病毒或用于周边防护的反病毒—选择所需条目旁边的选项按钮，然后单击“**添加**”。
   将打开含有“**受管理设备**”管理组的窗口。
5. 单击“**受管理设备**”旁边的 V 形图标 ()。
   管理组层级和它们的策略被显示。
6. 在管理组层级和它们的策略中，点击策略名称或检测到病毒爆发时激活的策略的名称。
   要在列表或组中选择所有策略，选择所需名称旁边的复选框。
7. 单击“**保存**”按钮。
   管理组层级和它们的策略的窗口被关闭。

所选的策略被添加到检测到病毒爆发时激活的策略列表。所选策略在病毒爆发中被激活，无论它们是活动的还是非活动的。

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。

强制同步

尽管 Kaspersky Security Center 云控制台自动为受管理设备同步状态、设置、任务和策略，但在某些情况下，您需要确切知道在某一给定时刻是否已为指定设备执行同步。

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. 点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** → **组**”，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. 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 Kaspersky 应用程序策略后，您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. 点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。

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. 点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）。

      请注意，用户列表经过筛选并显示属于内部用户的设备所有者。

      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 云控制台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）。

      请注意，用户列表经过筛选并显示属于内部用户的设备所有者。

      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 云控制台的安全组。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，并点击**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。

加密 Kaspersky Endpoint Security for Windows 中的数据

您可以在运行 Windows 操作系统的服务器或工作站的设备上管理 BitLocker 驱动器加密技术。

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 云控制台中通过定义 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 云控制台中通过定义 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 云控制台中，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。

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. 在主菜单中，转到**操作→数据加密和保护**。
3. 打开**加密驱动器**部分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。
4. 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 云控制台不支持的 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。

关于用户账户

Kaspersky Security Center 云控制台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，管理服务器检索本地用户账户的数据。
- Kaspersky Security Center 云控制台内部用户的账户。您可以在门户上创建内部用户账户。这些账户仅在 Kaspersky Security Center 云控制台内使用。

查看用户账户和安全组表：

1. 在主菜单中，转到**用户和角色 → 用户和组**。
2. 选择**用户**或**组**选项卡。

用户或安全组表将打开。默认情况下，打开的表按**子类型**和**已分配角色**列进行筛选。该表显示已分配角色的内部用户或组。

如果您想查看仅包含本地用户账户的表，请将子**子类型**过滤条件设置为**本地**。

如果切换到从属管理服务器版本 14.2 或更早版本，然后打开用户或安全组列表，则打开的表将仅按**子类型**列进行筛选。默认情况下，不会应用**已分配角色**列的筛选器。筛选后的表将包含具有分配的角色和不具有分配的角色的所有内部用户或安全组。

添加内部用户账户

如果需要，您可以在门户上添加工作区的内部用户。添加内部用户后，您可以在 Kaspersky Security Center 云控制台中为其分配角色。

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 Kaspersky 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 Kaspersky 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。

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 云控制台针对 Kaspersky Security Center 云控制台和受管理 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 云控制台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 云控制台的功能，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“**对设备分类执行操作**”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
常规功能：访问对象而不考虑它们的 ACL	**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** • **对设备分类执行操作**	• 虚拟服务器的设备移动规则（创建、修改或删除）：**写入**、**对设备分类执行操作** • 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**	• “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	• “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”	无

		• 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**	务器上远程安装应用程序”	• “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” • “安全问题报告” • “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”	
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：Kaspersky 软件部署	• 管理 Kaspersky 补丁 • 读取 • 写入 • 执行 • 对设备分类执行操	批准或拒绝安装补丁：管理 Kaspersky 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	安装包：“Kaspersky”

	作			报告” • “Kaspersky 软件模块更新版本报告” • “保护部署报告”	
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
常规功能：管理服务器层级	配置管理服务器的层级	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 • 对设备分类执行操	• 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**	无	“第三方软件更新安装结果报告”	无

	作	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			
常规功能：加密密钥管理	写入	导入加密密钥：写入	无	无	无
系统管理：连接性	• 开始 RDP 会话 • 连接到现有 RDP 会话 • 启动隧道 • 将设备中的文件保存到管理员工作站 • 读取 • 写入 • 执行 • 对设备分类执行操作	• 创建桌面共享会话：创建桌面共享会话的权限 • 创建 RDP 会话：连接到现有 RDP 会话 • 创建隧道：启动隧道 • 保存内容网络列表：将设备中的文件保存到管理员工作站	无	“设备用户报告”	无
系统管理：硬件清单	• 读取 • 写入 • 执行 • 对设备分类执行操作	• 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	• 部署 PXE 服务器：部署 PXE 服务器	“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”

	• 写入 • 执行 • 对设备分类执行操作	• 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			
系统管理：漏洞和补丁管理	• 读取 • 写入 • 执行 • 对设备分类执行操作	• 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 • 对设备分类执行操作	• 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 • 对设备分类执行操作	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 云控制台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，或者创建新角色并自行配置所需的权限。Kaspersky Security Center 云控制台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 云控制台中出现）。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	允许所有报告类型操作、所有查看操作，包括查看已删除对象（授予在“**已删除对象**”区域的**读取**和**写入**权限）。不允许其他操作。您可以分配该角色到执行您组织的审计的人。
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，允许以下功能区域中的所有操作： • 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。

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** • **卡巴斯基软件部署** • **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。
高级安全分析师	授予“常规功能：基本功能”功能区域中的“读取”权限。 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。 授予 Kaspersky Endpoint Detection and Response Expert 解决方案的访问权限。
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。

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。

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 Kaspersky 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。

编辑用户的访问权限

您可以编辑以下对象的用户访问权限：

- 管理服务器
- 管理组
- 任务
- 报告
- 事件分类
- 设备分类

要编辑用户的访问权限：

1. 转到所选对象的**访问权限**选项卡。
2. 选择您想要编辑访问权限的用户。

   如果您选择了自己的用户账户，则无法撤销自己的访问权限。更改将不会被保存。

3. 单击**访问权限**按钮。
4. 在打开的窗口中，编辑所选用户的访问权限。

5. 单击“**确定**”按钮。

该用户的访问权限已更改。

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. 点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 Kaspersky 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、用户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用户组旁边的复选框。
3. 单击“**分配角色**”按钮。
   角色分配向导启动。使用**下一步**按钮进行向导。
4. 在向导的“**选择角色**”页面上，选择要分配的用户角色。
5. 在向导的“**定义范围**”页面上，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。

所选用户或用户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. 点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**按钮进行向导。
5. 在向导的“**定义范围**”页面上，选择要添加到用户角色范围的管理组。
6. 在向导的“**选择用户**”页面上，选择要添加到用户角色范围的用户和用户组。
7. 单击“**分配角色**”按钮关闭窗口。
8. 关闭角色属性窗口。

所选用户或用户组和所选管理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**—点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配置配置文件设置。
     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。

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**新组**。
3. 在**新组**窗口中，为新安全组指定以下设置：
   - **名称**
   - **描述**
4. 单击“**正常**”保存更改。

新的安全组已被添加到安全组列表中。

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. 点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。

添加用户账户到内部组

> 您仅可以添加内部用户账户到内部组。

要添加用户账户到内部组：

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组。
5. 单击“**分配**”按钮。

用户账户被添加到组。您还可以使用组设置将内部用户添加到组。

编辑安全组

> 您仅可以仅删除内部安全组。

要删除用户组：

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. 选择您要删除的用户组旁边的复选框。
3. 单击**删除**，然后在打开的窗口中确认删除。

用户组被删除。

配置 ADFS 集成

要允许在组织中的 Active Directory (AD) 中注册的用户登录 Kaspersky Security Center 云控制台，您必须配置与 Active Directory 联合身份验证服务 (ADFS) 的集成。

Kaspersky Security Center 云控制台支持 ADFS 3 (Windows Server 2016) 或更高版本。

要更改 ADFS 集成设置，您必须具有更改用户权限的访问权限。

在继续之前，请确保您已完成Active Directory 轮询。

配置 ADFS 集成：

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“**ADFS 整合设置**”区域。
3. 复制回调 URL。
   您将需要此 URL 来配置 ADFS 管理控制台中的集成。
4. 在 ADFS 管理控制台中，添加新的应用程序组，然后通过选择**服务器应用程序**模板（Microsoft 界面元素的名称以英文提供）来添加新的应用程序。
   ADFS 管理控制台为新应用程序生成客户端 ID。您将需要客户端 ID 来配置 Kaspersky Security Center 云控制台中的集成。
5. 作为重定向 URI，指定您在管理服务器属性窗口中复制的回调 URL。
6. 生成客户端密钥。您将需要客户端密码才能在 Kaspersky Security Center 云控制台中配置集成。
7. 保存添加的应用程序的属性。
8. 将新的应用程序添加到创建的应用程序组中。这次选择**Web API**模板。
9. 在**“标识符”**选项卡上的**“依赖方标识符”**列表中，添加您之前添加的服务器应用程序的客户端 ID。
10. 在**“客户端权限”**选项卡的**“允许的范围”**列表中，选择**allatclaims**和**openid**范围。
11. 在**“颁发转换规则”**选项卡上，通过选择**“发送 LDAP 属性作为声明”**模板来添加新规则：
    a. 命名规则。例如，您可以将其命名为“Group SID”。
    b. 选择**Active Directory**作为属性存储，然后将**令牌组作为 SID**作为 LDAP 属性映射到“组 SID”作为传出声明类型。
12. 在**发行转换规则**选项卡上，通过选择**使用自定义规则发送声明**模板来添加新规则：
    a. 命名规则。例如，您可以将其命名为“ActiveDirectoryUserSID”。

b. 在**自定义规则**字段中，输入：

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
";objectSID;{0}", param = c.Value);
```

13. 在 Kaspersky Security Center 云控制台中，再次打开**ADFS 整合设置**部分。

14. 将切换按钮切换到**ADFS 整合 已启用**位置。

15. 单击**设置**链接，然后指定包含联合服务器的一个或多个证书的文件。

16. 单击**ADFS 整合设置**链接，然后指定以下设置：

- 发布者 URL

  在您的组织中工作的联合服务器的 URL 地址。

  特别是，Kaspersky Security Center 云控制台将“/.well-known/openid-configuration”添加到颁发者 URL 地址，并尝试打开生成的 URL 地址 (issuer_URL/.well-known/openid-configuration) 以自动发现颁发者配置。

- 客户端 ID

  联合服务器生成的用于识别 Kaspersky Security Center 云控制台的客户端 ID。您可以在与 Kaspersky Security Center 云控制台对应的服务器应用程序的属性窗口中的 ADFS 管理控制台中找到客户端 ID。

- 客户端私密

  当您指定与 Kaspersky Security Center 云控制台对应的服务器应用程序的属性时，您会在 ADFS 管理控制台中生成客户端密钥。

- 验证用户的域

  您选择的域成员将能够使用其域账户凭据登录Kaspersky Security Center 云控制台 。完成网络轮询后，域名将显示在列表中。

- ID 令牌中用户 SID 的字段名

  引用 ID 令牌中的用户 SID 的字段名称。需要字段名称来识别 Kaspersky Security Center 云控制台中的用户。默认情况下，ID 令牌中的此字段称为“primarysid”。

- ID 令牌中用户组的 SID 阵列的字段名

  引用包含用户的 Active Directory 安全组的 SID 数组的字段名称。默认情况下，ID 令牌中的此字段称为“groupsid”。

17. 单击“**保存**”按钮。

与 ADFS 的集成已完成。要使用 AD 账户凭据登录 Kaspersky Security Center 云控制台，请使用**ADFS 整合设置**部分中提供的链接（**使用 ADFS 登录 Kaspersky Security Center 云控制台的链接**）。

当您首次通过 ADFS 登录 Kaspersky Security Center 云控制台时，控制台可能会延迟响应。

指派用户作为设备所有者

有关将用户指定为移动设备所有者的信息，请参阅 Kaspersky Security for Mobile 帮助。

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. 点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。

管理对象修订

该区域包含了对象修订管理的信息。

支持修订管理的对象包括：

- 管理服务器
- 策略

- 任务
- 管理组
- 用户账户
- 安装包

关于对象修订

Kaspersky Security Center 云控制台可让您跟踪对象修改。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。

您可以对对象修订采取以下操作：

- 查看所选修订
- 回滚对对象所做的更改到所选的修订

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

  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，输入修订描述的文本。

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**回滚**按钮。

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“**编辑描述**”按钮。
4. 在打开的窗口中，输入修订描述的文本。
   默认下，对象修订描述为空。
5. 点击“**保存**”。

新的描述将显示在修订历史记录表的**“描述”**列中。

对象删除

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

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 云控制台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。

- 该设备被存储在未分配的设备组中，并根据设备保留规则自动从该组中删除。

  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。在这种情况下，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。

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 云控制台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。

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 云控制台组件和安全应用程序

方案：定期更新 Kaspersky 数据库和应用程序

本节提供定期更新 Kaspersky 数据库、软件模块和应用程序的方案。完成网络保护方案配置后，您必须维护保护系统的可靠性。这种维护可确保对受管理设备提供牢固的保护，抵御一系列威胁，包括病毒、网络攻击和网络钓鱼攻击。

您可以使用若干个 scheme 以安装更新到 Kaspersky Security Center 云控制台组件和安全应用程序。选择一个或多个最满足您网络需求的方案。

下面的方案描述了更新方案，该方案意味着将更新下载到分发点存储库。如果受管理设备未连接到分发点，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。

当您完成此方案时，会出现以下结果：

- Kaspersky Security Center 云控制台组件会自动更新，或者仅在您为更新指定 *"已批准"* 状态时更新。
- 卡巴斯基安全应用程序、卡巴斯基数据库和软件模块将根据您指定的计划进行更新。默认下，卡巴斯基安全应用程序仅安装您批准的更新。

您可以配置更新过程以通过以下两种方式之一下载和安装更新：

- 自动地

  在这种情况下，您只需执行此方案一次。您必须计划 *将更新下载至分发点存储库* 任务（如果有）和卡巴斯基安全应用程序的更新任务，并保留网络代理属性中的默认更新设置。

- 手动

  您可以配置更新过程以手动运行卡巴斯基安全应用程序 *将更新下载至分发点存储库* 任务（如果有）和更新任务。您还可以将网络代理配置为仅在指定更新的 *"已批准"* 状态时安装 Kaspersky Security Center 云控制台组件的更新。

先决条件

在您开始之前，确保您已做了如下：

1. 根据通过 Kaspersky Security Center 云控制台部署 Kaspersky 应用程序的方案将 Kaspersky 安全应用程序部署到受管理设备。当执行此方案时，您分配了适当数量的分发点，与受管理设备和网路拓扑一致。
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。

阶段

卡巴斯基数据库和应用程序定期更新的配置分阶段进行：

1. **创建“将更新下载至分发点存储库”任务**

   创建“*将更新下载至分发点存储库*”任务。运行此任务时，Kaspersky Security Center 云控制台会直接从卡巴斯基更新服务器将更新下载到分发点。

   操作说明：创建将更新下载至分发点存储库的任务

2. **配置分发点**

   确保在所有必需的分发点的属性中启用**部署更新**选项。当为分发点禁用此选项时，分发点范围内的设备只能从本地资源或直接从卡巴斯基更新服务器下载更新。

   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。

3. **通过使用 diff 文件优化更新过程（可选）**

   启用该功能将导致降低分发点和受管理设备之间的流量。要使用此功能，请在**下载差异文件**任务的属性中启用*将更新下载至分发点存储库*选项。

   使用说明：使用 diff 文件更新 Kaspersky 数据库和软件模块

4. **定义要安装的更新**

   默认下，下载的软件更新具有*未定义*状态。将状态更改为“*已批准*”或“*已拒绝*”以定义是否应在联网设备上安装此更新。批准的更新总是被安装。未定义的更新仅可以被安装到网络代理和其他 Kaspersky Security Center 云控制台组件，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。

   说明：

   - 关于更新状态
   - 批准和拒绝软件更新

5. **配置 Kaspersky Security Center 云控制台组件的更新和补丁的自动安装**

   默认情况下。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 云控制台组件。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。

   操作说明：启用和禁用 Kaspersky Security Center 云控制台组件的自动更新和补丁

6. **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。我们建议您配置任务计划时选择“**When new updates are downloaded to the repository**”选项。这将确保尽快安装新的更新。

   默认情况下，仅在将更新状态更改为*已批准*后才会安装受管理应用程序的更新。对于 Kaspersky Endpoint Security for Windows，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。

   操作说明：在设备上自动安装 Kaspersky Endpoint Security 更新

方案完成后，您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 云控制台组件和安全应用程序

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：

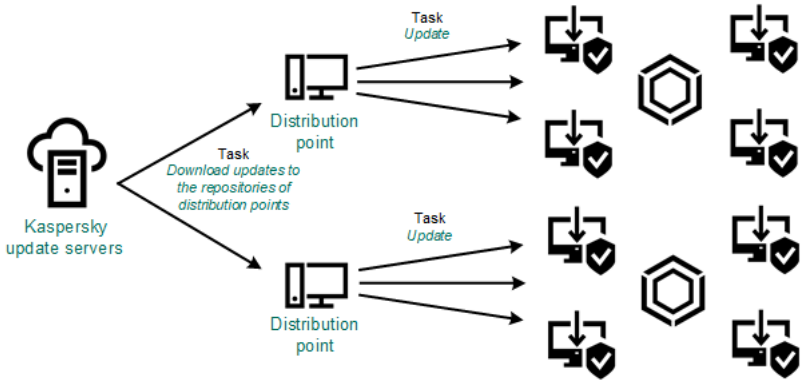
- 使用“*将更新下载至分发点存储库*”任务
- 通过本地文件夹、共享文件夹或 FTP 服务器手动
- 直接从卡巴斯基更新服务器到受管理设备上的安全应用程序

使用“将更新下载至分发点存储库”任务

在此方案中，Kaspersky Security Center 云控制台通过将更新*将更新下载至分发点存储库*。包括在分发点范围中的受管理设备从分发点存储库下载更新（请见下图）。

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“将更新下载至分发点存储库”任务更新

*将更新下载至分发点存储库*任务完成后，以下更新将下载到分发点存储库：

- 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。

- Kaspersky Security Center 云控制台组件更新

  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

  默认下，Kaspersky Endpoint Security for Windows 仅安装您批准的更新。更新通过更新任务安装且可以在任务属性中被配置。

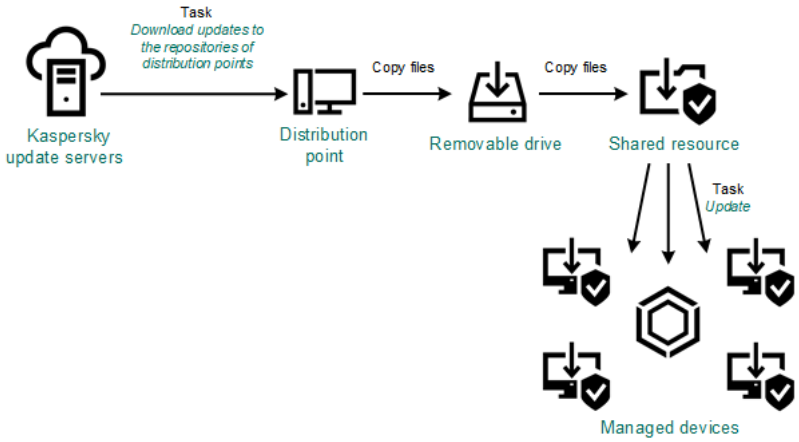
每个 Kaspersky 应用程序都从管理服务器请求所需更新。管理服务器集合这些更新并仅下载应用程序请求的更新到分发点储存库。这确保了相同更新不被下载多次，且不必要更新不被下载。当运行“*将更新下载至分发点存储库*”任务时，管理服务器自动发送以下信息到 Kaspersky 更新服务器以便确保相关版本的 Kaspersky 数据库和软件模块的下载：

- 应用程序 ID 和版本
- 应用程序安装 ID
- 活动密钥 ID
- 下载任务运行 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。

通过本地文件夹、共享文件夹或 FTP 服务器手动

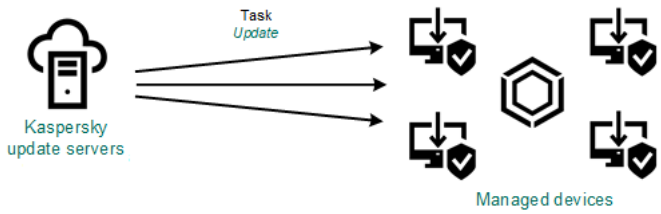
如果客户端设备未连接到分发点，您可以使用本地文件夹或共享资源作为 Kaspersky 数据库、软件模块和应用程序的更新源。在此方案中，您需要从分发点存储库复制所需更新到可移动驱动器，然后复制更新到在 Kaspersky Endpoint Security for Windows 设置中指定的本地文件夹或共享文件夹（参见下图）。



通过本地文件夹、共享文件夹或 FTP 服务器更新

直接从 Kaspersky 更新服务器到受管理设备上的 Kaspersky Endpoint Security for Windows

在受管理设备上，您可以配置 Kaspersky Endpoint Security for Windows 直接从 Kaspersky 更新服务器接收更新（参加下图）。



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 云控制台提供的存储库。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。对于这些设置的完整描述，请参考 Kaspersky Endpoint Security for Windows 文档。

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。

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
- 更新到 Kaspersky Security Center 云控制台组件
- 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。

*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。
3. 对于 Kaspersky Security Center 应用程序云控制台，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. 如果在“**完成任务创建**”步骤启用“**创建完成时打开任务详情**”选项，则可以修改默认任务设置。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。
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。

- 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）。

- 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

  Kaspersky Security Center 云控制台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：

- 计划开始

选择任务运行计划并配置所选计划。

- 手动（默认选择）

  任务不自动运行。您仅可以手动启动。
  默认情况下已启用该选项。

- 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，任务每六小时运行一次，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 云控制台。
  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

  任务定期运行，在指定星期的指定时间。
  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，不选择任何日期；默认开始时间为 6:00:00 PM。

- 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反病毒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。您可以选择先前任务如何结束(成功或带有错误)以触发当前任务的启动。例如，您可能想使用“**开启设备**”选项运行*管理设备*任务，在它完成后，运行*病毒扫描*任务。仅当两个任务被分配给同一设备时，此参数才有效。

- 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 Kaspersky 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。

  如果该选项被禁用，则只有已计划的任务将在客户端设备上运行，而对于“**手动**”、“**一次**”和“**立即**”任务，仅会在网络中可见的客户端设备上运行。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。

  默认情况下已启用该选项。

- 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. 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。

将受管理设备配置为仅从分发点接收更新

受管理设备可以从各种来源检索卡巴斯基数据库、软件模块和卡巴斯基应用程序的更新：直接从更新服务器、从分发点或从本地或网络文件夹。您可以将分发点指定为唯一可能的更新源。

要将受管理设备配置为仅从分发点接收更新：

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**设置**部分中，打开**仅通过分发点分发文件**切换按钮。
5. 为该开关按钮设置锁（🔒）。
6. 单击“**保存**”按钮。

   该策略将应用于选定的设备，并且这些设备将仅从分发点接收更新。

启用和禁用 Kaspersky Security Center 云控制台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 云控制台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 云控制台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 云控制台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 云控制台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，选择**"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 云控制台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在步骤 4 选择（或清空）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 云控制台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，选择**"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. 确保设置（**强制**）锁定（🔒）用于此切换按钮。

该策略将被应用到所选设备，且 Kaspersky Security Center 云控制台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. 如果在“**完成任务创建**”步骤启用“**创建完成时打开任务详情**”选项，则可以修改默认任务设置。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。
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**：此选项卡上的设置定义在设备和管理服务器之间建立连接时设备如何接收更新。
    - **移动模式**：此选项卡上的设置定义当Kaspersky Security Center 云控制台与设备之间未建立连接时（例如，当设备未连接到互联网时）设备如何接收更新。
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。

    当 Kaspersky Security Center 云控制台设置为更新源时，更新将从分发点存储库下载，而不是从管理服务器存储库下载。确保您分配了分发点并创建了*将更新下载至分发点存储库*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。

关于更新状态

*状态*是软件更新的一个属性，它定义是否必须在联网设备上安装特定的软件更新。

更新可以具有以下状态：

- *未定义*

  默认下，下载的软件更新具有*未定义*状态。未定义的更新仅可以被安装到网络代理和其他 Kaspersky Security Center 云控制台组件，与网络代理策略设置一致。

- *已批准*

  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。

- *已拒绝*

  您设置了*已拒绝*状态的更新将不被安装到设备。

您可以更改以下软件的更新状态：

- 网络代理和其他 Kaspersky Security Center 云控制台组件

  默认情况下，会自动安装下载的 Kaspersky Security Center 云控制台组件更新和补丁。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。

  即使您将更新设置为"*已拒绝*"状态，也无法卸载 Kaspersky Security Center 云控制台组件的更新。

- 卡巴斯基安全应用程序

  默认情况下，仅在将更新状态更改为*已批准*后才会安装受管理应用程序的更新。如果安全应用程序的拒绝的更新先前被安装，Kaspersky Security Center 云控制台将尝试从所有设备上卸载该更新。

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。

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 云控制台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。

使用 diff 文件更新 Kaspersky 数据库和软件模块

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 文件可限制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。如果对分发点启用 *下载 diff 文件* 功能，diff 文件被保存到该分发点。结果，从该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，我们建议您同步设备的更新计划与设备从其获取更新的分发点的更新计划。然而，即便设备更新频率小于从其获取更新的分发点，流量也被节省。

分发点不对 diff 文件的自动分发使用 IP 多点传送。

要启用下载 diff 文件功能：

1. 在主菜单中，转到“**资产(设备)**” → “**任务**”。

2. 单击 *将更新下载至分发点存储库* 任务以打开任务属性。

3. 在**应用程序设置**选项卡上，启用**下载差异文件**选项。

4. 单击“**保存**”按钮。

   下载 diff 文件功能已启用。每次运行将更新下载 *将更新下载至分发点存储库* 的 diff 文件。

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。

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分发点存储库来配置定期更新。

当您需要在未连接到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，您必须使用大容量存储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。

您可以从以下源复制所需更新：

- 分发点。

  为确保分发点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，分发点范围中至少有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“*将更新下载至分发点存储库*”任务从分发点存储库接收更新。

- 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。

以下是通过从分发点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. 将可移动驱动器连接到分发点设备。
2. 复制更新文件到可移动驱动器。

   默认情况下，更新位于：%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates。
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。

更新 Kaspersky Security for Windows Server 数据库

您可以在受管理设备上安装 Kaspersky Security for Windows Server ，并且您可能想要启动该应用程序的实时文件保护任务。但是，该应用程序没有正常运行所需的数据库。仅当“*将更新下载到分发点存储库*”任务完成后，数据库才会下载到受管理设备。

如果您想在安装 Kaspersky Security for Windows Server 后立即在受管理设备上启动实时文件保护任务，则必须确保该应用程序的数据库已下载并且是最新的。否则，任务可能无法正常工作。

要确保 Kaspersky Security for Windows Server 数据库是最新的：

1. 确保管理服务器上已完成*将更新下载到分发点存储库*任务。
2. 执行以下操作之一：

- 在实时文件保护任务的设置中，将启动设置为“*应用程序启动时*”，然后重新启动受管理设备。
- 在实时文件保护任务的设置中，手动将开始时间设置为您想要的时间。

Kaspersky Security for Windows Server 中的实时文件保护任务已准备好正常工作。

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 云控制台功能。

关于第三方应用程序

Kaspersky Security Center 云控制台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 云控制台只能将第三方软件从当前版本更新到最新版本。以下列表展示了您可以使用 Kaspersky Security Center 云控制台更新的第三方软件：

第三方软件列表可以更新和扩展新的应用程序。您可以通过在 Kaspersky Security Center 云控制台中查看可用更新列表来检查是否可以使用 Kaspersky Security Center 云控制台更新第三方软件（安装在用户设备上）。

- 7-Zip Developers: 7-Zip
- Adobe Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber
- Code Sector: TeraCopy
- Codec Guide:

    - K-Lite Codec Pack Basic
    - K-Lite Codec Pack Full
    - K-Lite Codec Pack Mega
    - K-Lite Codec Pack Standard
- DbVis Software AB: DbVisualizer
- Decho Corp.:
    - Mozy Enterprise
    - Mozy Home
    - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
    - Radmin
    - Remote Administrator
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- FileZilla 项目： FileZilla
- Firebird Developers: Firebird
- Foxit Corporation:

    - Foxit Reader
    - Foxit Reader Enterprise
- Free Download Manager.ORG: Free Download Manager
- GIMP project: GIMP
- GlavSoft LLC.: TightVNC
- GNU Project: Gpg4win
- Google:
    - Google Earth
    - Google Chrome
    - Google Chrome Enterprise
    - Google Earth Pro
- Inkscape Project: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- Logitech: SetPoint
- LogMeIn, Inc.:
    - LogMeIn
    - Hamachi
    - LogMeIn Rescue Technician Console
- Martin Prikryl: WinSCP
- Mozilla Foundation:
    - Mozilla Firefox
    - Mozilla Firefox ESR
    - Mozilla SeaMonkey
    - Mozilla Thunderbird
- New Cloud Technologies Ltd: MyOffice Standard.Home Edition
- OpenOffice.org: OpenOffice
- Opera Software: Opera

- Oracle Corporation:
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum)
- Simon Tatham: PuTTY
- Skype Technologies: Skype for Windows
- Sober Lemur S.a.s.:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:
  - TeamViewer Host
  - TeamViewer
- Telegram Messenger LLP: Telegram Desktop

- The Document Foundation:
  - LibreOffice
  - LibreOffice HelpPack
- The Git Development Community:
  - Git for Windows
  - Git LFS
- The Pidgin developer community: Pidgin
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
  - VMware Player
  - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop

漏洞和补丁管理的限制

漏洞和补丁管理功能有许多限制，具体取决于您使用的授权许可以及 Kaspersky Security Center 云控制台 的工作模式。

以下授权许可不支持漏洞和补丁管理：

- 卡巴斯基网络安全解决方案标准版支持
- Kaspersky Hybrid Cloud Security

以下授权许可支持漏洞和补丁管理：

- 卡巴斯基网络安全解决方案高级版
- Kaspersky Endpoint Detection and Response Optimum
- 卡巴斯基全方位安全软件 for Business

- 卡巴斯基混合云安全企业版

下表比较了试用模式下、不支持漏洞和补丁管理的授权许可以及支持漏洞和补丁管理的授权许可下Kaspersky Security Center 云控制台的限制。

漏洞和补丁管理的限制

限制	试用模式	商业模式：不支持漏洞和补丁管理的授权许可	商业模式：支持漏洞和补丁管理的授权许可
*安装 Windows Update 更新*任务或*修复漏洞*任务的最大数量	4	4	0（无法创建此类新任务）
*安装所需更新并修复漏洞*任务的最大数量	2	不支持	4
所有*安装所需更新并修复漏洞*任务中的最大规则数	10	不支持	50
可同时处于已*批准*状态的软件更新的最大数量	100	不支持	1000
可以手动添加到任务的最大软件更新数	500	1000	1000
可以手动添加到任务的最大软件漏洞数	500	1000	1000

试用和商业模式以及各种授权许可选项下的漏洞和补丁管理功能的可用性

Kaspersky Security Center 云控制台中漏洞和补丁管理功能的可用性取决于您是在试用模式还是商业模式下使用它，以及您选择的许可选项。使用该表检查哪些漏洞和补丁管理功能可用。

漏洞和补丁管理功能的可用性

漏洞和补丁管理功能	试用模式	商业模式：卡巴斯基网络安全解决方案标准版支持	商业模式：卡巴斯基网络安全解决方案高级版、Kaspersky Endpoint Detection and Response Optimum、卡巴斯基全方位安全软件软件企业版
在运行 Windows 的受管理设备上手动修复 Microsoft 软件中的漏洞 创建“*修复漏洞*”任务	✓	✓	–
在运行 Windows 的受管理设备上手动安装 Microsoft 软件更新 通过*安装 Windows Update 更新*任务安装第三方软件更新	–	✓	✓
基于规则自动安装第三方软件更新并修复第三方软件漏洞 创建*安装所需更新并修复漏洞*任务和安装更新 添加更新安装规则	✓	–	✓

安装第三方软件更新

本节介绍与针对客户端设备上安装的第三方应用程序安装更新有关的 Kaspersky Security Center 云控制台功能。

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。

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 云控制台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：

   - 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，您可以查看受管理设备上更新安装的统计信息。例如，您可以查看未安装、将安装或更新安装失败的所选更新的设备数量。

   操作说明：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 云控制台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产品的更新。

   “*安装 Windows Update 更新*”任务可用于安装 Windows Update 更新。

   软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台 的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

   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。

   说明：

   - 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。默认频率为每周一次。

   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。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。

   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。

   操作说明：常规任务设置

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。

   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*”。

   操作说明：批准和拒绝第三方软件更新

6. **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。

   使用说明：手动启动任务

7. **创建有关第三方软件更新安装结果的报告（可选）**

   为了确保创建任务并安装更新，请创建**第三方软件更新安装结果报告**，并在此报告中查看有关更新安装的详细统计信息。

   操作说明：生成和查看报告

关于第三方软件更新

Kaspersky Security Center 云控制台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 云控制台通过“*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 云控制台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，则系统可能会提示用户将其关闭。

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

  此任务用于安装 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产品的更新。

  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 云控制台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

  此任务只可用于安装 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。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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*

  您可以使用此任务来安装 Microsoft 提供的 Windows Update 更新和其他供应商产品的更新。

- *安装 Windows Update 更新*

  您只能使用此任务来安装 Windows Update 更新。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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，则系统可能会提示用户将其关闭。

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。

  更新安装向导的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。

  该向导简化了更新安装任务的创建和配置，并可让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 → <device name> → 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。根据*Kaspersky Security Center 云控制台模式和您当前的授权许可安装所需更新并修复漏洞*“安装所需更新和修复漏洞”*安装 Windows Update 更新*“安装 Windows 更新更新”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。选择“*安装所需更新并修复漏洞*”任务或“*安装 Windows Update 更新*”任务。如果您选择*安装所需更新并修复漏洞*任务，则用于安装所选更新的新规则将自动添加到所选任务中。如果您选择*安装 Windows Update 更新*任务，所选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

此功能的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。

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（仅适用于 Windows Update 更新）

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（仅适用于第三方应用程序的更新）

  此选项仅适用于第三方应用程序的更新。Kaspersky Security Center 云控制台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（仅适用于 Windows Update 更新）

  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（仅适用于第三方应用程序的更新）

  此选项仅适用于第三方应用程序的更新。Kaspersky Security Center 云控制台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“新任务向导”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 云控制台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 云控制台应用程序，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 云控制台使用当前可用的 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。

    - 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 云控制台管理服务器（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，该信息存储在设备缓存中。

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：

- 仅当启用了“**连接更新服务器更新数据**”选项并且在“**Windows Update 搜索模式**”设置组中选择了“**主动**”选项时，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。
- 如果已启用“**连接更新服务器更新数据**”选项并且在“**Windows Update 搜索模式**”设置组中选择了“**被动**”选项，或者如果已禁用“**连接更新服务器更新数据**”选项，并且在“**Windows Update 搜索模式**”设置组中选择了“**主动**”选项，则受管理设备上的 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，该信息存储在设备缓存中。
- 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），如果已选中“**已禁用**”设置组中的“**Windows Update 搜索模式**”选项，Kaspersky Security Center 云控制台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 云控制台在 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 云控制台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 云控制台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。默认情况下，该列表为空。

- 启用高级诊断

如果启用该功能，即便跟踪在 Kaspersky Security Center 云控制台远程诊断实用程序中对网络代理禁用，网络代理也写入跟踪。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 云控制台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 云控制台使用当前可用的 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。

- 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 云控制台管理服务器（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，该信息存储在设备缓存中。

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：

- 仅当启用了“**连接更新服务器更新数据**”选项并且在“**Windows Update 搜索模式**”设置组中选择了“**主动**”选项时，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。
- 如果已启用“**连接更新服务器更新数据**”选项并且在“**Windows Update 搜索模式**”设置组中选择了“**被动**”选项，或者如果已禁用“**连接更新服务器更新数据**”选项，并且在“**Windows Update 搜索模式**”设置组中选择了“**主动**”选项，则受管理设备上的 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，该信息存储在设备缓存中。
- 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），如果已选中“**已禁用**”设置组中的“**Windows Update 搜索模式**”选项，Kaspersky Security Center 云控制台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 云控制台在 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 云控制台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 云控制台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。默认情况下，该列表为空。

- 启用高级诊断

如果启用该功能，即便跟踪在 Kaspersky Security Center 云控制台远程诊断实用程序中对网络代理禁用，网络代理也写入跟踪。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 云控制台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*任务的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。

*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。此任务可让您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。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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 云控制台应用程序，选择**安装所需更新并修复漏洞**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. 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**"更新下载文件夹"**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。

- 更新下载文件夹

  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，即便跟踪在 Kaspersky Security Center 云控制台远程诊断实用程序中对网络代理禁用，网络代理也写入跟踪。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 云控制台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 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。

- 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. 如果在“**完成任务创建**”页面上启用“**创建完成时打开任务详情**”选项，则可以修改默认任务设置。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。

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

此功能的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。

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

“安装 Windows Update 更新”任务可让您在客户端设备上安装 Windows Update 服务提供的软件更新。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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**按钮进行向导。
3. 对于 Kaspersky Security Center 云控制台应用程序，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，可以创建一条要求要安装的更新处于特定状态的规则。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。

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 云控制台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 云控制台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 云控制台的功能，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：查找和修复软件漏洞

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 云控制台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。

阶段

查找和修复软件漏洞的过程分为以下几个阶段：

1. **扫描客户端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 云控制台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 云控制台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。

   操作说明：创建查找漏洞和所需更新任务

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：

   - 查看软件漏洞信息
   - 查看受管理设备上的漏洞统计信息

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。此任务可让您根据某些规则安装多个更新并修复多个漏洞。此任务的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。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*任务使用 Microsoft 软件的推荐修复程序。

   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。

   操作说明：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。

   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。

   操作说明：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）**

   要查看有关漏洞修复的详细统计信息，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。

   操作说明：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**

   确保以下事项：

   - 受管理设备上的软件漏洞列表不为空。
   - 任务列表中有修复漏洞的任务。
   - 安排任务以查找和修复软件漏洞，以便任务依次启动查看这些任务的属性并比较它们的时间表。
   - 软件漏洞修复任务圆满完成。查看任务属性窗口的**结果**选项卡上的信息。

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分发点存储库中，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 云控制台可检测并修复运行 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。

查找软件漏洞

为了查找软件漏洞，Kaspersky Security Center 云控制台使用已知漏洞数据库和 Windows 更新数据库中的特征。已知漏洞数据库由卡巴斯基专家创建和维护。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 云控制台使用*查找漏洞和所需更新*任务来查找软件漏洞。

修复软件漏洞

为修复软件漏洞，Kaspersky Security Center 云控制台使用软件供应商发布的软件更新。您可以随时查看软件漏洞列表。由于将更新下载到分发点存储库任务运行，软件更新元数据会自动下载到管理服务器存储库和*将更新下载至分发点存储库*。您可以通过 Kaspersky Security Center 云控制台快速启动向导或手动创建此任务。

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*。在 Kaspersky Security Center 云控制台中，您可以使用*建议的修复*来修复漏洞。推荐的修补程序是 Kaspersky 专家建议安装的软件更新。

根据Kaspersky Security Center 云控制台模式和您当前的授权许可，您可以使用*安装所需更新并修复漏洞*任务或*修复漏洞*任务来修复软件漏洞。

*安装所需更新并修复漏洞*任务会自动修复安装推荐修复程序的多个漏洞。对于此任务，您可以手动配置某些规则来修复多个漏洞。

通过*修复漏洞*任务，您可以通过安装 Microsoft 软件的推荐修复程序来修复漏洞。

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。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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，则系统可能会提示用户将其关闭。

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，则该软件漏洞无法得到修复。

有关每个已修复漏洞的信息将在管理服务器上存储 90 天。过了这个时间，它就会被自动删除。

修复软件漏洞

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。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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，则系统可能会提示用户将其关闭。

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。

  此功能的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。

  该向导简化了漏洞修复任务的创建和配置，并可让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 → <device name> → 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。根据Kaspersky Security Center 云控制台模式和您当前的授权许可，将预先选择*安装所需更新并修复漏洞*任务或*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。根据Kaspersky Security Center 云控制台模式和您当前的授权许可，选择“*安装所需更新并修复漏洞*任务或*修复漏洞*任务。如果您选择*安装所需更新并修复漏洞*任务，修复所选漏洞的新规则将自动添加到所选任务中。如果您选择*修复漏洞*任务，则选定的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

漏洞修复向导的可用性取决于您使用的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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。

- **通过使用 类型的更新修复漏洞的规则**（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“新任务向导”后，“*Install required updates and fix vulnerabilities*”任务将添加到任务列表中。

创建“修复漏洞”任务

*修复漏洞*任务可让您修复运行 Windows 的受管理设备上的 Microsoft 软件中的漏洞。

此功能的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。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。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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，则系统可能会提示用户将其关闭。

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 云控制台应用程序，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”。
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. 如果在“**完成任务创建**”页面上启用“**创建完成时打开任务详情**”选项，则可以修改默认任务设置。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。

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*任务的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。

*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。此任务可让您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。

软件更新安装任务有许多限制。这些限制取决于您使用 Kaspersky Security Center 云控制台的授权许可以及 Kaspersky Security Center 云控制台的工作模式。

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 云控制台应用程序，选择**安装所需更新并修复漏洞**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. 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“更新下载文件夹”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。

- 更新下载文件夹

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，即便跟踪在 Kaspersky Security Center 云控制台远程诊断实用程序中对网络代理禁用，网络代理也写入跟踪。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 云控制台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 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。

- 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. 如果在“**完成任务创建**”页面上启用“**创建完成时打开任务详情**”选项，则可以修改默认任务设置。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。

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

此功能的可用性取决于Kaspersky Security Center 云控制台模式和您当前的授权许可。

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。

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。

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。
   如果您只想查看可以修复的软件漏洞，请选中“**仅显示可以被修复的漏洞**”选项。

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>*。如果仅在部分受管理设备修复了漏洞，并且需要在其余受管理设备进行修复，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。您可以通过过滤器从漏洞列表中排除被忽略的软件漏洞。

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. 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. 在打开的页面上，转到**事件存储库**选项卡。

3. 指定已修复漏洞信息在数据库中的最长保存期限。
   默认情况下，试用模式的存储期限为7天，商业模式的存储期限为60天。试用模式的最大限制为 14 天，商业模式的最大限制为 365 天。

4. 点击“保存”。

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。

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云控制台 功能。

方案：应用程序管理

您可以管理客户端设备上的应用程序启动。您可以允许或阻止应用程序在受管理设备上运行。此功能由“应用程序控制”组件实现。您可以管理 Windows 或 Linux 设备上安装的应用程序。

对于基于 Linux 的操作系统，从 Kaspersky Endpoint Security 11.2 for Linux 开始，均提供应用程序控制组件。

先决条件

- Kaspersky Security Center 云控制台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。

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应用程序列表**

   此阶段帮助您了解受管理设备上安装了哪些应用程序。您可以查看应用程序列表，并根据组织的安全策略确定要允许和禁止哪些应用程序。限制可能与组织中的信息安全策略有关。如果您非常清楚受管理设备上安装了哪些应用程序，则可以跳过此阶段。

   使用说明：获取并查看客户端设备上安装的应用程序列表

2. **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。如果您非常清楚受管理设备上安装了哪些可执行文件，则可以跳过此阶段。

   使用说明：获取并查看客户端设备上安装的可执行文件列表

3. **为组织中使用的应用程序创建应用程序类别**

   分析受管理设备上存储的应用程序和可执行文件的列表。在分析基础上，创建应用程序类别。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应用程序集。如果不同的安全组在工作中使用不同的应用程序集，则可以为每个安全组创建单独的应用程序类别。

   根据创建应用程序类别的条件集，可以创建两种类型的应用程序类别。

   操作说明：用手动添加的内容创建应用程序类别，创建包含来自选定设备的可执行文件的应用程序类别

4. **在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”**

   使用您在上一阶段创建的应用程序类别，在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”组件。

   操作说明：在 Kaspersky Endpoint Security for Windows 策略中配置“应用程序控制”

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应用程序，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 将不会阻止被应用程序控制规则禁止启动的应用程序，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。

   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”。

6. **更改“应用程序控制”组件的应用程序类别设置**

   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应用程序类别中。

   操作说明：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应用程序类别的配置后，您可以在操作模式下应用“应用程序控制”的规则。

   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”。

8. **验证“应用程序控制”配置**

   确保以下事项：

   - 应用程序类别列表不为空。查看应用程序类别列表并确保它包含您已配置的类别。
   - 应用程序控制是使用创建的应用程序类别进行配置的。查看 Kaspersky Endpoint Security for Windows策略的设置，并确保您已在**应用程序设置→安全控制→应用程序控制**中配置应用程序控制。
   - 在操作模式下应用“应用程序控制”的规则。检查 Kaspersky Endpoint Security for Windows策略中的模式，并确保您已在**应用程序设置→安全控制**中禁用**测试模式 →应用程序控制**。

结果

方案完成后，将控制受管理设备上的应用程序启动。用户只能启动组织中允许的应用程序，而不能启动组织中禁止的应用程序。

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

关于应用程序控制

“应用程序控制”组件监控用户启动应用程序的尝试，并使用应用程序控制规则来管理应用程序启动。

“应用程序控制”组件可用于 Kaspersky Endpoint Security for Windows 和 Kaspersky Security for Linux（版本 11.2 和更高版本）。本节中的所有说明都介绍适用于 Kaspersky Endpoint Security 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应用程序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应用程序外的所有应用程序，则使用该模式。默认情况下选择*黑名单*模式。
- *允许列表*。如果要阻止启动除了允许规则中指定的应用程序外的所有应用程序，则使用该模式。

应用程序控制规则通过应用程序类别实现。您创建定义特定条件的应用程序类别。在 Kaspersky Security Center 云控制台中，有两种类型的应用程序类别：

- 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。

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

获取并查看客户端设备上安装的应用程序列表

Kaspersky Security Center 云控制台清查在运行 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。

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

获取并查看客户端设备上安装的可执行文件列表

您可以获取受管理设备上安装的可执行文件列表。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 （版本 11.2 及更高版本）

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。为此，我们建议您在安装了一组标准软件的参考设备上运行清单任务。

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**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

执行“**清单**”任务后，将形成受管理设备上安装的可执行文件列表，您可以查看该列表。

清查过程中，将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。

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安装的可执行文件列表。

您还可以将可执行文件从受管理设备发送到卡巴斯基，以检查潜在威胁。

要将受管理设备的可执行文件发送到卡巴斯基：

1. 在主菜单中，转到“**操作**” → “**第三方应用程序**” → “**可执行文件**”。
2. 单击要发送到卡巴斯基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。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。
4. 单击“**发送到卡巴斯基**”按钮。

选定的可执行文件被下载以进一步发送到卡巴斯基。

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。遵照向导的说明。
3. 在向导的“**选择策略创建方法**”页面上，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. 在向导的“**条件**”页面上，单击“**添加**”按钮以添加将文件包括在所创建类别中的条件。
5. 在“**条件标准**”页面上，从列表中选择用于创建类别的规则类型：

- 从 KL 类别

  如果选中此选项，您可以指定 Kaspersky 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空间的证书。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。

- 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夹。

- 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。您可以从注册表中选择应用程序，然后指定以下文件元数据：

    - 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。

  - 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 云控制台使用的哈希值算法。计算的哈希值信息存储在管理服务器数据库。哈希值的存储不显著增加数据库尺寸。

未在 SHA-256 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 SHA-256 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 云控制台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“**SHA-256**”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 SHA-256 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 SHA-256 加密哈希。

- 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**SHA-256**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。元数据将发送到管理服务器。包含相同元数据的可执行文件将添加到该应用程序类别。

证书

如果选中此选项，则可以指定来自存储空间的证书。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。

- 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. 在向导的“**排除项**”页面上，单击“**添加**”按钮以添加将文件从所创建类别中排除的排除条件。

7. 在“**条件标准**”页面上，从列表中选择规则类型，方式与选择用于类别创建的规则类型相同。

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

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。

要创建包括选定设备中的可执行文件的应用程序类别：

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. 在向导的“**选择策略创建方法**”页面上，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应用程序类别。

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 云控制台使用的哈希值算法。计算的哈希值信息存储在管理服务器数据库。哈希值的存储不显著增加数据库尺寸。

     未在 SHA-256 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 SHA-256 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 云控制台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“**SHA-256**”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 SHA-256 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 SHA-256 加密哈希。

     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**SHA-256**复选框和**MD5 哈希**复选框。

     为该类别中的文件计算 SHA-256(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。

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。

查看应用程序类别列表

您可以查看已配置的应用程序类别列表以及每个应用程序类别的设置。

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**”。

将显示含有应用程序类别列表的页面。

要查看应用程序类别的属性，

单击应用程序类别的名称。

将显示应用程序类别的属性窗口。这些属性被分组在几个选项卡上。

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→安全控制→应用程序控制**。

   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。开启切换按钮**应用程序控制已禁用**以禁用该选项。

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**"选项后重新启动计算机。

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

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 SHA-256 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 SHA-256 哈希。当您选择 SHA-256 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 SHA-256 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 SHA-256 (没有哈希的文件将被跳过)

    每个文件都有单独的 SHA-256 哈希。当您选择 SHA-256 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 SHA-256 哈希函数详情，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

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。

从 Kaspersky 数据库创建第三方应用程序安装包只能在“漏洞和补丁管理”授权许可下进行。

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

    显示安装包修订号。

  - 时间

    显示修订的创建时间。

  - 用户

    显示创建了修订的用户账户的名称。

  - 操作

    列出修订内对安装包执行的操作。

  - 描述

    显示为修订添加的文本描述。

应用程序标签

该部分描述了应用程序标签，提供了创建和修改它们以及标记第三方应用程序的说明。

关于应用程序标签

Kaspersky Security Center 云控制台可让您标记第三方应用程序（非卡巴斯基的软件供应商制作的应用程序）。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] 标签并分配其到所有浏览器（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. 点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. 点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。

配置管理服务器

本节介绍 Kaspersky Security Center 管理服务器的配置过程和属性。

创建管理服务器层级：添加从属管理服务器

您可以使本地运行的管理服务器充当从属管理服务器，从而在网络上建立“主/从属”层次结构。对于卡巴斯基基础架构中的管理服务器，网络上的主管理服务器和从属管理服务器都是从属服务器。您可以添加基于 Windows 的管理服务器以及基于 Linux 的管理服务器。

要添加可用于连接的从属管理服务器：

1. 确保未来的从属管理服务器安装了Kaspersky Security Center Web Console 。
2. 在未来的从属管理服务器上，下载管理服务器证书并保存它，以便您可以在“添加从属管理服务器”向导的步骤之一期间将其添加到主管理服务器。
3. 通过 Kaspersky Security Center Web Console 在未来的从属管理服务器上执行以下操作（或者，您可以提示未来从属管理服务器的管理员执行这些操作）：
   a. 在主菜单，单击未来的从属管理服务器名称旁边的“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. 选中**该管理服务器是服务器层级中的从属**选项。
   d. 选择**云控制台**作为主管理服务器的类型。
      用于在从属管理服务器和主管理服务器之间建立连接的设置字段变得可用。
   e. 在**HDS 服务器地址(来自云控制台上的主管理服务器)**和**HDS 服务器端口**字段中，输入Kaspersky Security Center 云控制台主管理服务器的地址和端口。
      您可以在 Kaspersky Security Center 云控制台管理服务器属性窗口**管理服务器层级**”选项卡的**常规**部分中找到 HDS 服务器地址和 HDS 服务器端口。您可以将此数据复制并粘贴到从属管理服务器窗口的字段中。
   f. 单击**指定主管理服务器证书**按钮，然后选择证书。
      您可以在属性窗口**管理服务器层级**选项卡的**常规**部分中单击**“查看管理服务器证书”**按钮，从Kaspersky Security Center 云控制台管理服务器下载此证书。
   g. 单击**指定 Hosted Discovery Service 证书**按钮，然后选择证书。
      您可以在属性窗口**管理服务器层级**选项卡的**常规**部分中单击**HDS 根 CA 证书**按钮，从Kaspersky Security Center 云控制台管理服务器下载此证书。
   h. 如果您使用代理服务器连接到 Kaspersky Security Center 云控制台管理服务器（即您构建的层次结构中的主服务器），请指定该服务器并输入代理服务器凭据。
   i. 如果**连接主管理服务器到 DMZ 中的从属管理服务器**选项。
   j. 单击**“保存”**保存更改并退出窗口。
4. 在主菜单，单击未来主管理服务器名称旁边的“设置”图标 ()。
5. 在打开的属性页面上，单击“**管理服务器**”选项卡。

6. 选择您要向其添加从属管理服务器的管理组名称旁边的复选框。

7. 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。

8. 在向导的第一页，填充以下字段：

   - 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。

9. 如果您使用代理服务器连接到 Kaspersky Security Center 云控制台管理服务器（即未来的主服务器），请指定该服务器并输入代理服务器凭据。

10. 遵照向导的进一步说明。

    向导完成后，“主/从属”层级被建立。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。

创建管理组

最初，管理组的层次结构仅包含一个称为**受管理设备**组的管理组。您可以将设备和子组添加到**受管理设备**组中。

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. 在层次结构中，选择要包括新管理组的管理组。

3. 单击“**添加**”按钮。

4. 在打开的窗口中输入组名称，然后单击“**添加**”。

   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。

配置与已删除设备相关的事件的存储期限

在 Kaspersky Security Center 云控制台中，事件存储在事件存储库中。您无法配置要在事件存储库中存储的事件数量。

在管理服务器属性窗口的**事件存储库**部分中，您可以配置与已删除设备相关的事件的最长存储期限。存储期限是 1000 天。

要配置与已删除设备相关的事件的存储天数：

1. 在主菜单，单击 Kaspersky Security Center 云控制台管理服务器旁边的设置图标 ( )。
   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。
3. 启用**设备被删除后存储事件**选项。
4. 在**最大存储期限(天)**编辑框中指定存储与已删除设备相关的事件的天数。
   与已删除设备相关的事件的存储天数受指定值的限制。

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。

有关事件的汇总电子邮件

在操作过程中， Kaspersky Security Center 云控制台和受管理的卡巴斯基应用程序会生成事件。每个事件都归属于特定类型和严重级别（*严重*、*功能失败*、*警告*或*信息*）。基于事件发生的条件，Kaspersky Security Center 云控制台可以分配不同的严重级别到相同类型的事件。

Kaspersky Security Center 云控制台通过电子邮件自动发送有关事件的通知。Kaspersky Security Center 云控制台发送有关**管理服务器属性**窗口的事件**事件配置**选项卡上列出的事件的通知。通用通知设置适用于所有事件类型。

为了限制必须发送的电子邮件数量，Kaspersky Security Center 云控制台在特定时间段内聚合具有相同严重性级别的事件。这些时间段的值由卡巴斯基专家管理。因此，收件人会根据以下模板获取聚合电子邮件：“已发生 <Number> <Severity_level>（及更低级别）事件”。

通过 Kaspersky Security Center 云控制台管理本地运行的从属管理服务器的限制

使用 Kaspersky Security Center 云控制台中的相应选项切换到本地运行的从属管理服务器后，应用程序会对该从属管理服务器的管理施加特定限制。用户将无法使用以下与 Kaspersky Security Center 云控制台操作相关的设置：

- 在网络代理策略和管理服务器策略的设置中，**事件配置**和**应用程序设置**选项卡不可用；无法制定新的政策。

- 在网络代理任务和管理服务器任务的设置中，**事件配置**和**应用程序设置**选项卡不可用；无法创建新任务。
- 网络代理和管理服务器的管理以及从属管理服务器的属性窗口不可用。
- 快速启动向导不可用。
- 无法修改网络代理和管理服务器事件的存储和通知设置。
- **当前应用程序版本**部分不可用。
- **安装包**部分不可用。

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。

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。

配置界面

您可以将 Kaspersky Security Center 云控制台界面配置为显示和隐藏各区域和界面元素，具体取决于您使用的功能。

要根据当前使用的功能集配置 Kaspersky Security Center 云控制台界面：

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，启用或禁用选项：
   - 显示数据加密和保护

     您可以使用此选项隐藏或显示界面中的**操作 → 数据加密和保护**部分。Kaspersky Security Center 云控制台仅为您自己的用户账户保存此选项的值，而其他用户可以设置不同的值。

   - 显示 MDR 功能

     您可以使用此选项隐藏或显示界面中的**监控和报告→事件**部分。Kaspersky Security Center 云控制台仅为您自己的用户账户保存此选项的值，而其他用户可以设置不同的值。
3. 设置 Kaspersky Security Center 云控制台在策略分发结果中显示的设备数量。
4. 点击"**保存**"。

控制台界面设置根据您的喜好进行配置。

管理虚拟管理服务器

本节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。

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。
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**虚拟管理服务器名称**。

6. 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。

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，请确保该管理员不包括在主管理服务器属性的**访问权限**列表中。

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

分配管理员时，请确保授予对单个虚拟管理服务器的访问权限。有权访问多个虚拟管理服务器的管理员无法登录Kaspersky Security Center 云控制台。

虚拟管理服务器的管理员登录 Kaspersky Security Center 云控制台 的方式与登录主管理服务器的方式相同。Kaspersky Security Center 云控制台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。
- 虚拟服务器管理员创建的账户不包含在任何服务器（主服务器或从属服务器）属性的**访问权限**列表中。
- 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。

应用程序将向管理员账户分配新角色。

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。

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 云控制台管理的设备，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。

监控和报告

该部分描述了 Kaspersky Security Center 云控制台的监控和报告功能。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 云控制台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 云控制台中配置监控和报告功能的方案。

先决条件

在您部署 Kaspersky Security Center 云控制台到组织网络中后，您可以开始监控它并生成其功能报告。

阶段

配置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**

   操作说明：配置客户端设备上的事件通知（通过电子邮件）

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. **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

5. **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

6. 检查客户端设备保护

   说明：

   - 生成并查看来自**保护状态**和**威胁统计**类别的报告
   - 启动并查看**严重事件**分类

7. 查看授权许可信息

   说明：

   - 将“**授权许可密钥使用**”小组件添加到控制板并查看
   - 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 云控制台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

控制板

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。

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 云控制台界面上可以配置的设置创建和查看用户定义的事件分类。

仪表板和小部件

本节包含有关仪表板和仪表板提供的小组件的信息。本节包括有关如何管理小组件和配置小组件设置的说明。

使用控制板

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 云控制台的“**监控和报告**”区域中单击“**控制板**”可打开控制板。

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 云控制台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。

当配置控制板时，您可以添加您需要的部件或隐藏您不需要的部件，更改部件的大小或外观，移动部件以及更改它们的设置。

添加工具到控制板

要添加工具到控制板：

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. 在可用工具列表，选择您要添加到控制板的工具。
   工具按类别分组。要查看包含在类别中的工具列表，点击类别名称旁边的臂章图标(>)。
4. 单击“**添加**”按钮。

所选的工具被添加到控制板结尾。

您现在可以编辑所添加工具的展示和参数。

从控制板隐藏工具

要从控制板隐藏工具：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 点击您要隐藏的工具旁边的设置图标（⚙）。
3. 选择**隐藏 Web 小部件**。
4. 在打开的“**警告**”窗口中，单击“**确定**”。

所选工具被隐藏。稍后，您可以再次添加该工具到控制板。

移动工具到控制板

要移动工具到控制板：

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**移动**。
4. 点击您要移动工具的地方。您仅可以选择其他工具。

所选工具的地方被清扫。

更改部件尺寸或样子

对于显示图表的工具，您可以更改其展示–线条图或线形图。对于一些工具，您可以更改其大小：最小、中度或最大。

要更改工具展示：

1. 在主菜单中，转到“**监控和报告**” → “**控制板**”。
2. 点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**

所选工具的展示被更改。

更改部件设置

要更改工具设置：

1. 在主菜单中，转到“**监控和报告** → **控制板**”。
2. 点击您要更改的小组件旁边的“设置”图标 (⚙)。
3. 选择**显示设置**。
4. 在打开的工具设置窗口，更改所需的工具设置。
5. 单击“**保存**”保存设置。

所选工具的设置被更改。

设置集合取决于特定工具。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 云控制台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 → 用户和角色** 区域中**用户和组**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 云控制台中执行各种操作，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 云控制台并在仅仪表板模式下监视网络保护统计信息。

报告

本节介绍如何使用报告、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 云控制台的“**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 云控制台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：

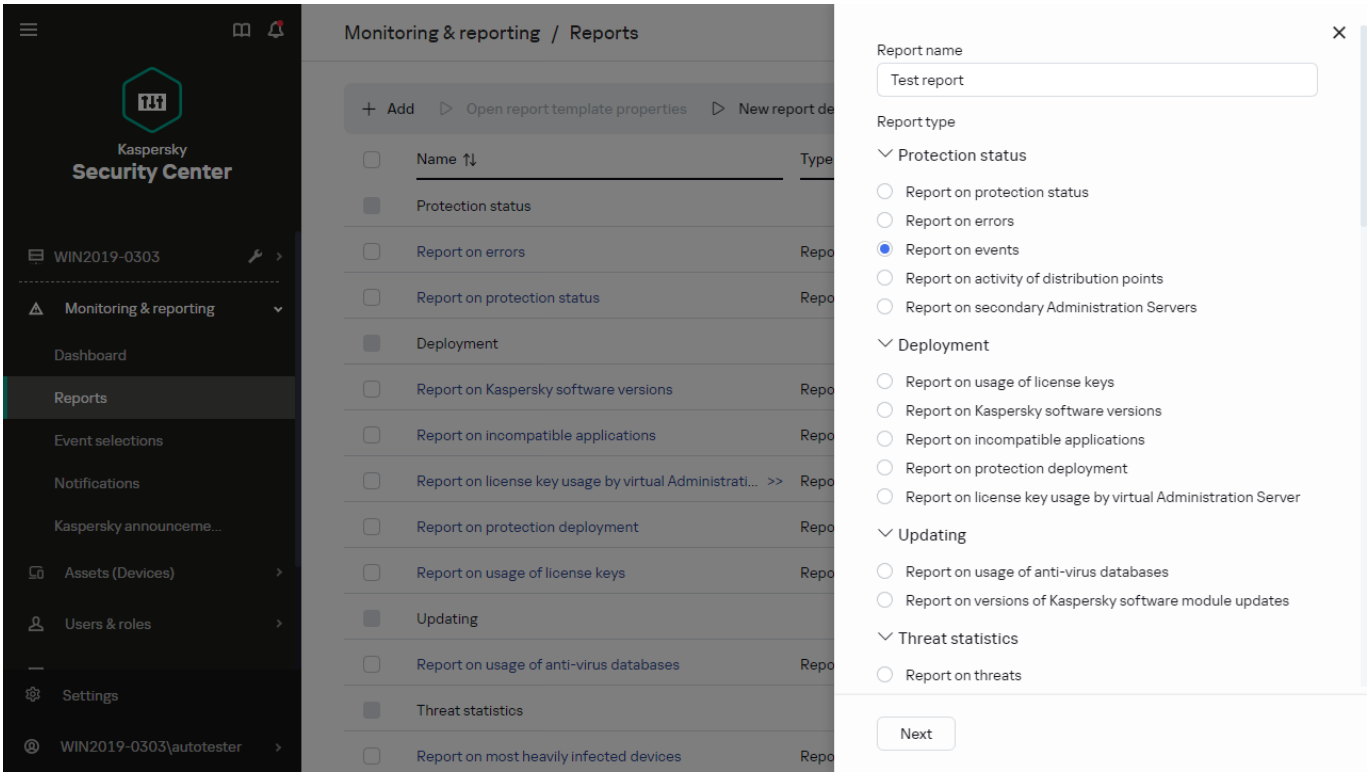
1. 在主菜单中，转到“监控和报告” → “报告”。

报告子区域中的报告模板列表

2. 单击添加。

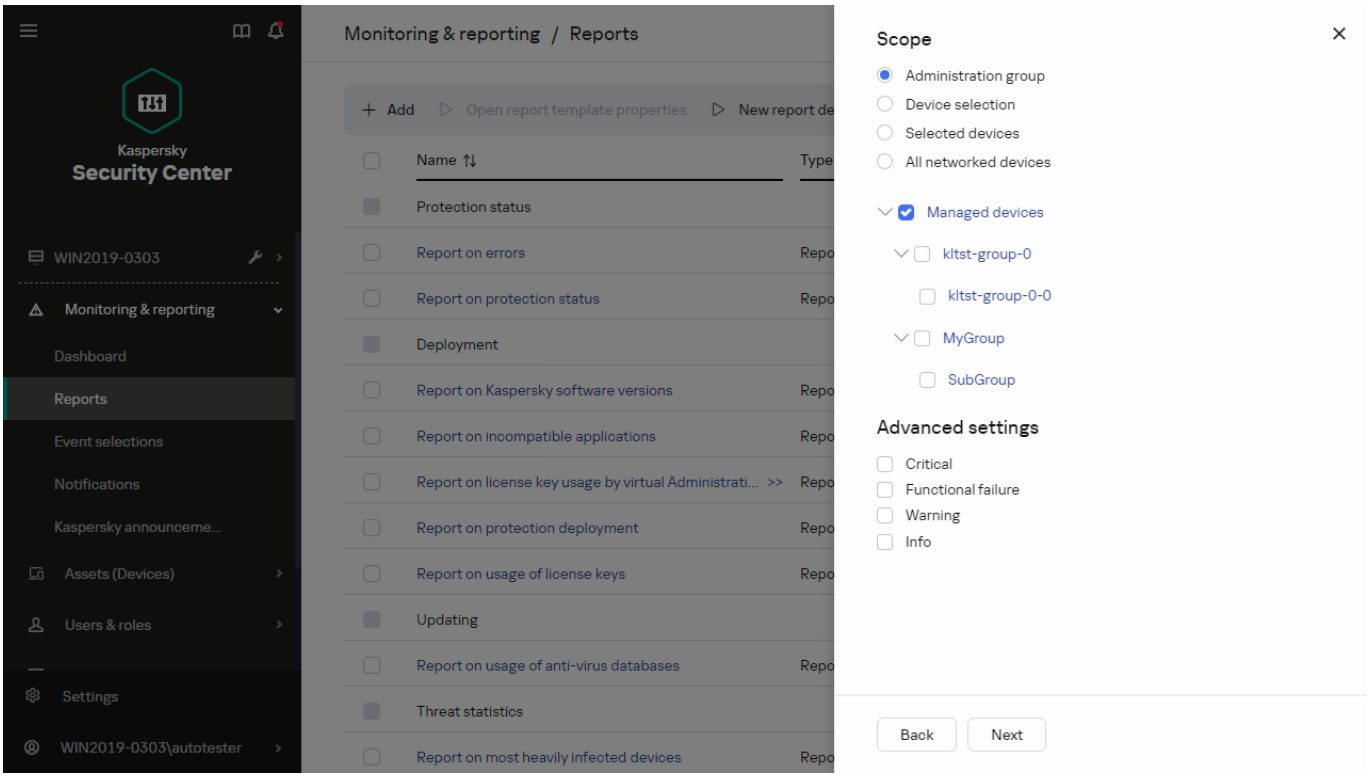
   程序将启动“新报告模板向导”。使用下一步按钮进行向导。

3. 在向导的第一页，输入报告名称并选择报告类型。



新报告模板向导。指定报告模板的名称和类型

4. 在向导的“范围”页面上，选择要基于该报告模板显示其数据到报告的客户端设备集合（管理组、设备分类、所选设备或所有网络设备）。

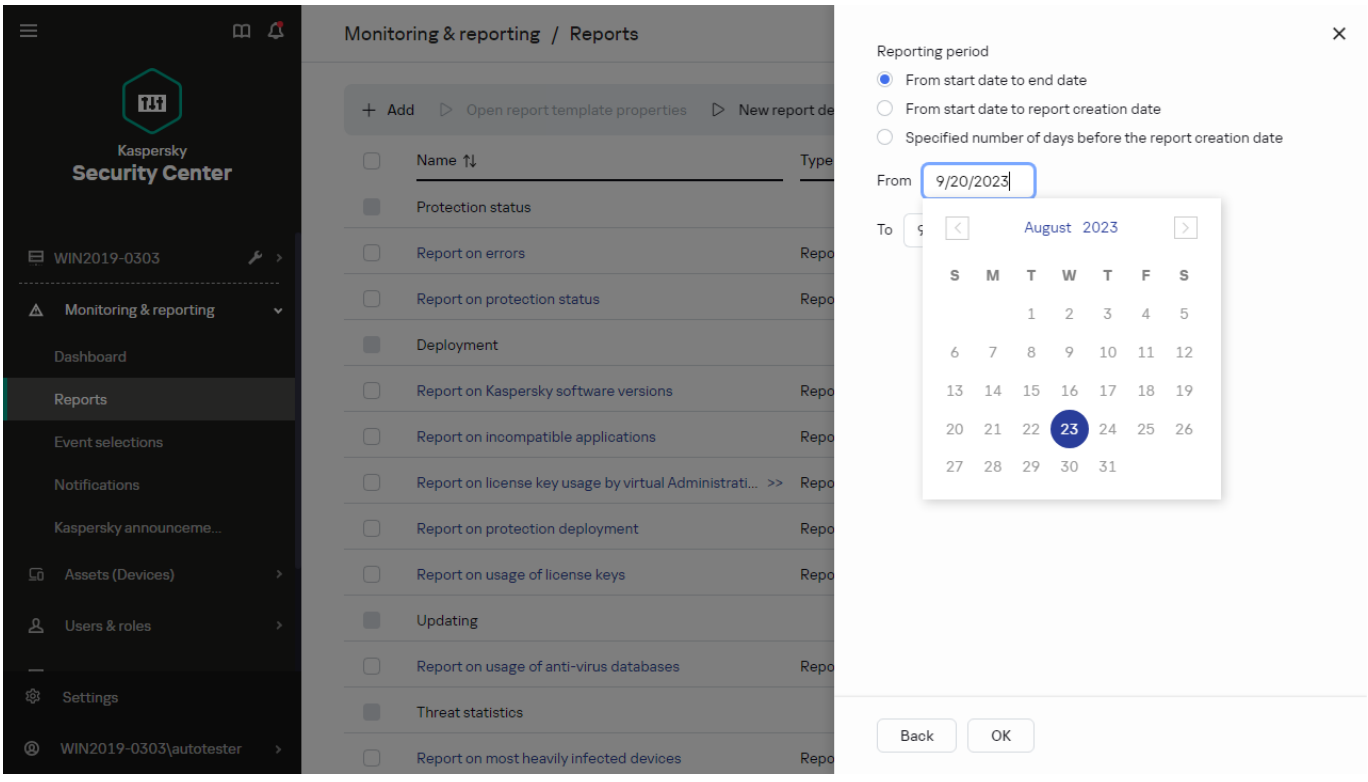


新报告模板向导。指定报告模板范围

5. 在向导的"**报告周期**"页面上，指定报告周期。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。



新报告模板向导。指定报告期间

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。请注意，此选项不会影响将报告导出到文件时可包含在报告中的最大事件数。

       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。

       请注意，Kaspersky Security Center 云控制台界面最多可显示 2500 个条目。如果您需要查看更多数量的事件，请使用报告导出功能。

     - 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

您可以将一份或多份报告保存为 XML、HTML 或 PDF。Kaspersky Security Center 云控制台允许您同时将最多 10 个报告导出为指定格式的文件。

要导出报告到文件：

1. 在主菜单中，转到“**监控和报告**” → “**报告**”。
2. 选择您要导出的报告。

   如果您选择超过 10 个报告，**导出报告**按钮将被禁用。
3. 单击“**导出报告**”按钮。
4. 在打开的窗口中，指定以下导出参数：

   - **文件名**。

     如果您选择导出一份报告，请指定报告文件名。

     如果您选择多个报告，报告文件名将与所选报告模板的名称一致。

   - **最大条目数**。

     指定报告文件中包含的最大条目数。默认值是 10,000。

- **文件格式**。

  选择报告文件类型：XML、HTML 或 PDF。如果导出多个报告，所有选定的报告都会以指定格式保存为单独文件。

5. 单击“**导出报告**”按钮。

报告以指定格式保存到文件。

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。

报告数据仅以英文显示，其他本地化版本不可用。

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. 【可选】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“**新报告传送任务**”按钮。
4. “新任务向导”启动。使用**下一步**按钮进行向导。
5. 在向导的第一页，输入任务名称。默认名称是“**传送报告 (<N>)**”，其中 <N> 是任务序号。

6. 在向导的任务设置页面，指定以下设置：

   a. 要使用任务传送的报告模板。如果您在步骤 2 选择了它们，跳过该步骤。

   b. 报告格式：HTML、XLS 或 PDF。

   c. 报告是否使用电子邮件连同邮件通知设置一起发送。

7. 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**”页面上启用“**创建完成时打开任务详情**”选项。

8. 单击“**创建**”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，将打开任务设置窗口。

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分类、Kaspersky Security Center 云控制台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 云控制台中的事件

Kaspersky Security Center 云控制台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设备组上的安全系统事件。

按类型划分的事件

Kaspersky Security Center 云控制台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 Kaspersky 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控制板等方面。

- 受管理 Kaspersky 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。

按来源划分的事件

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。

以下应用程序可以生成事件：

- Kaspersky Security Center 云控制台组件：
  - 管理服务器
  - 网络代理
- 受管理的卡巴斯基应用程序

  有关受管理的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。

按重要性级别划分的事件

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 云控制台中查看或修改。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。

Kaspersky Security Center 云控制台组件事件

每个 Kaspersky Security Center 云控制台组件都拥有自己的事件类型集。本节列出了 Kaspersky Security Center 云控制台管理服务器和网络代理中发生的事件类型。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 云控制台中。
- **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）。当您使用 Kaspersky Security Center 云控制台数据库中提供的公共视图浏览和处理事件时，将使用此代码。
- **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。

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

该表显示具有"**严重**"重要性级别的 Kaspersky Security Center 云控制台管理服务器事件。

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 云控制台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 云控制台决定当授权许可限制被超过时生成事件的规则。	180 天
病毒	26	GNRL_EV_VIRUS_OUTBREAK	当短时间内在若干受管理设备上检测	180

爆发	(对于文件威胁防护)		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。 • 您也可以创建严格策略以便被激活，或者创建任务以便在事件发生时运行。	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。 • 您也可以创建严格策略以便被激活，或者创建任务以便在事件发生时运行。	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。 • 您也可以创建严格策略以便被激活，或者创建任务以便在事件发生时运行。	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，但一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
受限制功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	当 Kaspersky Security Center 云控制台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 云控制台的完整功能模式	180 天

			（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）。	
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。该天数无法被更改。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 云控制台仅提供基本功能。 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	很快要添加的信息。	180 天
卡巴斯基软件模块更新已撤销	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 云控制台补丁，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

该表显示具有“**功能失败**”重要性级别的 Kaspersky Security Center 云控制台管理服务器事件。

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
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 云控制台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

管理服务器警告事件

该表显示具有“**警告**”重要性级别的 Kaspersky Security Center 云控制台管理服务器事件。

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
已超过授权许可数量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	每天，Kaspersky Security Center 云控制台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：	90天

			• 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 云控制台决定当授权许可限制被超过时生成事件的规则。	
设备在网络上已长时间没有活动	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	很快要添加的信息。	90 天
设备名称冲突	4102	KLSRV_EVENT_HOSTS_CONFLICT	很快要添加的信息。	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达到限制	4127	KLSRV_INVLICPROD_FILLED	很快要添加的信息。	90 天
证书已被请求	4133	KLSRV_CERTIFICATE_REQUESTED	很快要添加的信息。	90 天
证书已删除	4134	KLSRV_CERTIFICATE_REMOVED	很快要添加的信息。	90 天
APNs 证书已过期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	很快要添加的信息。	90 天
APNs 证书即将过期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	很快要添加的信息。	90 天
发送 **FCM** 消息到移动设备失败	4138	KLSRV_GCM_DEVICE_ERROR	很快要添加的信息。	90 天
发送 **FCM** 消息到 **FCM** 服务器时发生 **HTTP** 错误	4139	KLSRV_GCM_HTTP_ERROR	很快要添加的信息。	90 天
发送 **FCM** 消息到 **FCM** 服务器失败	4140	KLSRV_GCM_GENERAL_ERROR	很快要添加的信息。	90 天
到从属管理服务器的连接已中断	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	很快要添加的信息。	90 天

到主管理服务器的连接已中断	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	很快要添加的信息。	90 天
KSN 代理已启动。检查 **KSN** 可用性失败	7719	KSNPROXY_STARTED_CON_CHK_FAILED	很快要添加的信息。	90 天
已注册卡巴斯基软件模块的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	很快要添加的信息。	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。 • 减小存储在管理服务器数据库的事件的列表。	90 天
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。 • 减小存储在管理服务器数据库的事件的列表。	90 天
授权许可即将过期	4128	KLSRV_INVLICPROD_EXPIRED_SOON	很快要添加的信息。	90 天
审计：**SIEM** 服务器连接测试失败	5120	KLAUD_EV_SIEM_TEST_FAILED	当 SIEM 服务器的自动连接测试失败时，会发生此类事件。	90 天

管理服务器信息事件

该表显示具有“**信息**”重要性级别的 Kaspersky Security Center 云控制台管理服务器事件。

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
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
设备已被根据规则自动移动	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	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 （在 Kaspersky Security Center 云控制台中，此事件类型仅适用于从属管理服务器。）	4144	KLSRV_UPD_BASES_UPDATED	30 天
KSN 代理已启动。**KSN** 可用性检查已成功完成	7718	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	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
审计：对象状态已修改	4150	KLAUD_EV_TASK_STATE_CHANGED	30 天
审计：组设置已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	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：**SIEM** 服务器连接测试成功	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30

			天

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

下表显示具有“**功能失败**”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 云控制台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

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

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
设备已被检测	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	7712	KLUSRLOG_EV_FILE_READ	30

取			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

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 云控制台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 云控制台的“**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 云控制台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**
  - **信息消息**
- **用户请求**（受管理应用程序事件）
- **最近事件**（上周）

- 审计事件

  在 Kaspersky Security Center 云控制台中，显示与工作区中的服务操作相关的审核事件。这些事件取决于卡巴斯基专家的行动。这些事件例如包括以下内容：管理服务器端口更改；管理服务器数据库备份；创建、修改和删除用户账户。

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 云控制台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 云控制台允许您将事件分类及其设置保存到 KLT 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 云控制台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 云控制台允许您从 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. 点击所需事件的时间。
   “**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

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。
3. 单击“**导出到文件**”按钮。

所选事件被导出到文件。

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。

记录任务和策略事件信息

本节提供有关如何最大程度地减少 Kaspersky Security Center 云控制台数据库中存储的任务和策略的事件数量的建议。默认情况下，每 1000 台设备有 100,000 个事件。如果超过此限制，新事件将覆盖旧事件。结果，关键事件可能会消失。此外，名为“Events”的管理服务器警告事件**超过了数据库中事件数的限制，事件已被删除**。在这些情况下，我们建议您按照本节中的说明进行操作。

因此，您将提高执行与事件分析相关的方案的速度。此外，这些建议还可以帮助您降低关键事件被大量事件覆盖的风险。

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。但是，如果任务频繁运行（例如，每周运行一次以上），则事件数量可能会太大，并且事件可能会淹没数据库。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，Kaspersky Security Center 云控制台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，Kaspersky Security Center 云控制台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。

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。

如果有关组任务中间状态更改的事件和有关应用策略的事件在 Kaspersky Security Center 云控制台数据库中的所有事件中占据很大份额，建议修改事件存储设置。

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。

通知和设备状态

本节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。

关于通知

Kaspersky Security Center 云控制台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。对于任何事件，您都可以通过电子邮件配置通知。

在通过电子邮件接收通知时，您可以决定您对事件的响应。该响应必须是最适合您组织网络的响应。

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 云控制台中的事件的电子邮件通知。

要配置发生在 Kaspersky Security Center 云控制台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**部分，然后在右侧窗格中定义电子邮件通知设置：
   收件人(电子邮件地址)

   Kaspersky Security Center 云控制台将向其发送通知的电子邮件地址。您可以在该字段指定多个地址，以分号分隔。

   您最多可以指定 24 个电子邮件地址。
3. 单击“**发送测试消息**”按钮可让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。
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 云控制台中发生的所有事件。

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。

卡巴斯基公告

本节介绍如何使用、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 Kaspersky Security Center 云控制台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 云控制台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 云控制台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。

如果多个管理员使用 Kaspersky Security Center 云控制台并且设置了不同的界面语言， Kaspersky Security Center 云控制台将以管理员使用的每种语言显示卡巴斯基公告。当您更改界面语言时，在您退出控制台然后再次登录后，所选语言的卡巴斯基公告会自动添加到该部分。

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 Kaspersky 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。

  > 您无法在 Kaspersky Security Center 云控制台试用模式下禁用与安全相关的公告。

  为了显示与您的网络保护配置相对应的信息，Kaspersky Security Center 云控制台会将数据发送到 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。您在创建公司工作区时接受的 Kaspersky Security Center 云控制台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 Kaspersky 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 云控制台会将数据发送到 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 云控制台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。

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 云控制台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。

> 您无法在 Kaspersky Security Center 云控制台试用模式下禁用与安全相关的公告。

要禁用与安全相关的公告：

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"**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 设置**"区域。
3. 禁用"**我同意使用卡巴斯基安全网络**"选项。
4. 单击"**保存**"按钮。
   营销公告已禁用。

接收授权许可到期警告

要将卡巴斯基网络安全解决方案标准版支持授权许可密钥添加到管理服务器：

1. 在主菜单，单击管理服务器名称旁边的"设置"图标 ()。
   管理服务器属性窗口将打开。
2. 在"**常规**"选项卡上，选择"**License keys**"区域。
3. 单击**选择**。
4. 在打开的窗口中，选择您的授权许可并单击**确定** 。
   或者，如果未显示授权许可，您可以单击**添加新授权许可密钥**并使用您的激活码。

授权许可即添加到管理服务器存储库中。这使得管理服务器在授权许可期限到期前一天生成关键事件“*授权许可即将到期*”，并在授权许可期限到期后生成关键事件“*有限功能模式*”。如果需要，您可以配置通知传送。

如果您将卡巴斯基网络安全解决方案标准版支持授权许可密钥添加到管理服务器存储库，则该授权许可将被视为在一台设备上使用。

Cloud Discovery

Kaspersky Security Center 云控制台允许您监控运行 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。

仅当您购买了其中一项 Kaspersky Next 授权许可时，才可以使用 Cloud Discovery 功能。有关详细信息，请参阅授权许可和每个授权许可的最小设备数量。

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。
- 您已购买其中一项 Kaspersky Next 授权许可，该授权许可能够阻止对不需要的云服务进行的访问。

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 云控制台从所有受安全策略或配置文件（已启用相关功能）保护的受管理设备中，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（已启用相关功能）保护的受管理设备中，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。

为了能够启用 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 云控制台。
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。
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，并且小部件会添加到仪表板。

将 Cloud Discovery 小部件添加到控制板

您可以将 **Cloud Discovery** 小部件添加到控制板，以监控受管理设备上云服务的使用情况。

为了能够将 Cloud Discovery 小部件添加到控制板，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 小部件添加到控制板，请执行以下操作：

1. 转到 Kaspersky Security Center 云控制台。
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控制板的末端。

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 云控制台从所有受安全策略（已启用相关功能）保护的受管理设备中，获取有关云服务使用情况的信息。

在查看之前，请确保：

- Cloud Discovery 小部件已添加到控制板。
- Cloud Discovery 功能已启用。
- 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 云控制台。
2. 在主菜单中，转到“**监控和报告**”→“**控制板**”。
   Cloud Discovery 小部件会显示在控制板上。
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。

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。

仅当您购买了其中一项 Kaspersky Next 授权许可时，才可以使用 Cloud Discovery 功能。有关详细信息，请参阅授权许可和每个授权许可的最小设备数量。

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，您在决定是否阻止对特定服务的访问时，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

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。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。

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)** → **组** → **<group name>** → **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. 点击所需设备的名称。
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. 点击“**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， Kaspersky Security Agent 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**”。
   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

仅当满足以下条件之一时，您才可以从客户端设备下载跟踪文件：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

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。
   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

仅当满足以下条件之一时，您才可以从客户端设备下载应用程序：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

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。

从客户端设备下载系统信息

仅当满足以下条件之一时，您才可以从客户端设备将系统信息下载到您的设备：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

要从客户端设备下载系统信息：

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**系统信息**选项卡。
3. 单击**下载**按钮可下载有关客户端设备的系统信息。

包含信息的文件将被下载到指定位置。

下载事件日志

仅当满足以下条件之一时，您才可以从客户端设备将事件日志下载到您的设备：设备设置中启用了不断开与管理服务器的连接选项、推送服务器正在使用中或存在连接网关正在使用中。否则，下载无法进行。

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。

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。
  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。

运行应用程序的远程诊断并下载结果

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. 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，选择要对其运行远程诊断的应用程序。

   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 Kaspersky 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。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。

> 生成转储文件仅适用于在 Windows 客户端设备上运行的 32 位进程。对于运行 Linux 的客户端设备和 64 位进程，此功能不受支持。

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，选择单击**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**按钮以保存指定应用程序的转储文件。

   如果指定的应用程序未在客户端设备上运行，则会显示错误消息。

在基于 Linux 的客户端设备上运行远程诊断

Kaspersky Security Center 云控制台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 云控制台远程下载诊断信息，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。

导出事件到 SIEM 系统

本节介绍如何配置导出事件到 SIEM 系统。

方案：配置导出事件到 SIEM 系统

本部分提供了配置将事件从管理服务器导出到外部 SIEM 系统的方案。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设备组上的安全系统事件。

先决条件

在开始配置 Kaspersky Security Center 云控制台中的事件导出之前：

- 了解有关事件导出方法的更多信息。
- 确保知道系统设置的值。

您可以按任意顺序执行此方案的步骤。

阶段

将事件导出到 SIEM 系统的过程包括以下阶段：

- **配置 SIEM 系统以接收来自Kaspersky Security Center 云控制台的事件。**

  您必须在 SIEM 系统中配置从Kaspersky Security Center 云控制台接收事件。

- **标记事件以供导出**

  您必须标记要导出到 SIEM 系统的事件。首先，标记所有受管理卡巴斯基应用程序中发生的常规事件。此外，可以标记特定受管理卡巴斯基应用程序的事件。

- **配置 Kaspersky Security Center 云控制台以导出事件到 SIEM 系统**

  您必须配置 Kaspersky Security Center 云控制台才能开始将事件导出到 SIEM 系统。

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 云控制台中自动导出事件时，您必须指定一些 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 云控制台。

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 云控制台和您的 SIEM 系统服务器之间连接的端口号。您在 Kaspersky Security Center 云控制台设置中和您 SIEM 系统的接收设置中指定该值。

- 协议

  用于从 Kaspersky Security Center 云控制台传输消息到您的 SIEM 系统的协议。您在 Kaspersky Security Center 云控制台设置中和您 SIEM 系统的接收设置中指定该值。

关于事件导出

Kaspersky Security Center 云控制台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 云控制台导出事件到外部 SIEM 系统的进程设计两部分：事件发送者，Kaspersky Security Center 云控制台和事件接收者，SIEM 系统。要成功导出事件，您必须在您的 SIEM 系统和 Kaspersky Security Center 云控制台管理控制台进行配置。您可以先配置任意一端。您可以配置 Kaspersky Security Center 云控制台中的事件传输，然后配置 SIEM 系统对事件的接收，或者相反。

事件导出的 Syslog 格式

您可以将 Syslog 格式的事件发送到任何 SIEM 系统。使用 Syslog 格式，您可以转发在管理服务器上和在受管理设备上安装的卡巴斯基应用程序中发生的任意事件。导出 Syslog 格式的事件时，您可以准确选择将转发到 SIEM 系统的事件类型。

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 云控制台的事件。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。

配置在 SIEM 系统中的事件导出

从 Kaspersky Security Center 云控制台导出事件到外部 SIEM 系统的进程设计两部分：事件发送者，Kaspersky Security Center 云控制台和事件接收者，SIEM 系统。你必须在您的 SIEM 系统和 Kaspersky Security Center 云控制台管理控制台中配置事件导出。

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 云控制台发送的事件，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：

- **端口**

  指定用于连接到 Kaspersky Security Center 云控制台的端口号。该端口必须与您在配置 SIEM 系统期间在 Kaspersky Security Center 云控制台中指定的端口相同。

- **消息协议或源类型**

  指定 Syslog 格式。

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。

消息接收器

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、参数等等。这将启用 SIEM 系统以处理从 Kaspersky Security Center 云控制台接收的事件，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

本节介绍如何标记事件以进一步以 Syslog 格式导出到 SIEM 系统。

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，您必须标记将被导出到外部 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. 点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 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 Kaspersky 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 云控制台导出事件到外部系统。

在 Kaspersky Security Center 云控制台中，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 云控制台被配置，以便能发送事件到 SIEM 系统。Kaspersky Security Center 云控制台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 云控制台以导出事件到 SIEM 系统

要将事件导出到 SIEM 系统，必须在 Kaspersky Security Center 云控制台中配置导出流程。

要在 Kaspersky Security Center 云控制台中配置到 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“**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 云控制台和您的 SIEM 系统服务器之间连接的端口号。您在 Kaspersky Security Center 云控制台设置中和您 SIEM 系统的接收设置中指定该值。
   - 协议

您只能使用基于 TCP 协议的 TLS 将消息传输到 SIEM 系统。为此，请指定 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 云控制台。Kaspersky Security Center 云控制台会检查 SIEM 系统服务器的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 CA 证书文件**”按钮，然后上传证书。

  - **SHA 指纹**。您可以在 Kaspersky Security Center 云控制台中指定 SIEM 系统证书的 SHA-1 指纹。要添加 SHA-1 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 云控制台进行身份验证。因此，您将使用 Kaspersky Security Center 云控制台颁发的自签名证书。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 云控制台将无法连接到 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 云控制台将验证 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 云控制台中生成证书。

  - **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 云控制台中生成自签名证书。结果是，Kaspersky Security Center 云控制台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。

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. 在打开的区域的“**导出的起始日期**”字段中，指定开始日期。

   c. 单击“**确定**”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 系统连接是否已成功配置，请单击**检查连接**按钮。

将显示连接状态。

8. 单击“保存”按钮。

到 SIEM 系统的导出已配置。从现在开始，如果您在 SIEM 系统中配置了事件接收，管理服务器会将标记的事件导出到 SIEM 系统。如果设置了导出的开始日期，管理服务器还会从管理服务器数据库中导出从指定日期开始的标记事件。

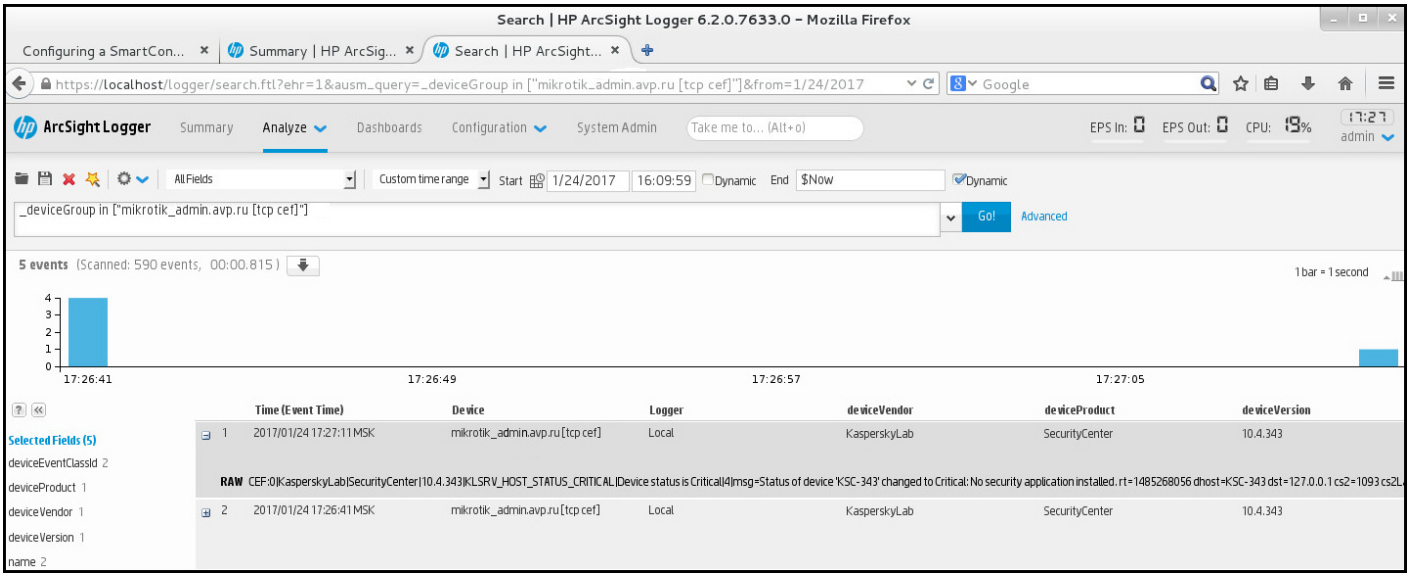
查看导出结果

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 云控制台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 云控制台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

受管理服务提供商 (MSP) 快速入门指南

本快速入门指南适用于受管理服务提供商 (MSP) 的管理员。

Kaspersky Security Center 云控制台支持多租户本指南包含管理客户（租户）账户以及在其设备上安装安全应用程序的提示和最佳实践。

关于 Kaspersky Security Center 云控制台

Kaspersky Security Center 云控制台是由卡巴斯基托管和维护的应用程序。您不必在计算机或服务器上安装 Kaspersky Security Center 云控制台 。Kaspersky Security Center 云控制台允许管理员在公司网络中的设备上安装 Kaspersky 安全应用程序，远程运行扫描和更新任务，以及管理受管理应用程序的安全策略。管理员可以使用详细的控制板，其中提供公司设备状态的快照、详细的报告以及保护策略中的细化设置。

Kaspersky Security Center 云控制台的主要功能

Kaspersky Security Center 云控制台可让您执行以下操作：

- 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。
- 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。
- 创建虚拟管理服务器并将它们排列在层次结构中。
- 保护您的网络设备，包括工作站和服务器：
  - 管理基于 Kaspersky 应用程序构建的反恶意软件保护系统。
  - 使用检测和响应（EDR 和 MDR）功能（需要Kaspersky Endpoint Detection and Response 和/或 Kaspersky Managed Detection and Response的授权许可），包括：
    - 分析和调查事件
    - 通过创建威胁发展链图进行事件可视化
    - 手动接受或拒绝响应或设置自动接受所有响应
- 使用 Kaspersky Security Center 云控制台作为多租户应用程序。
- 远程管理客户端设备上安装的卡巴斯基应用程序。
- 将卡巴斯基应用程序的授权许可密钥集中部署到客户端设备。
- 为网络上的设备创建和管理安全策略。
- 创建和管理用户账户。
- 创建和管理用户角色 (RBAC)。
- 创建和管理安装在您的网络设备上的应用程序任务。

- 单独查看每个客户组织的安全系统状态报告。

关于适用于 MSP 的 Kaspersky Security Center 云控制台授权许可

当您开始使用 Kaspersky Security Center 云控制台时，您可以请求试用工作区（在这种情况下，您将获得嵌入在工作区中的 30 天试用授权许可）或输入商业授权许可的激活码。

> 您无法将试用工作区转换为商业工作区。要在试用授权许可到期后继续使用 Kaspersky Security Center 云控制台，您必须删除试用工作区并使用商业授权许可创建另一个工作区。

稍后，您可以将一个或多个商业授权许可密钥添加到管理服务器存储库。

关于 MSP 的检测和响应能力

Kaspersky Security Center 云控制台可以将其他卡巴斯基应用程序的功能集成到控制台界面中。例如，您可以通过集成以下应用程序将检测和响应功能添加到 Kaspersky Security Center 云控制台的功能中：

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum 是一款旨在保护组织的 IT 基础架构免受复杂网络威胁的解决方案。该解决方案的功能将自动威胁检测与响应这些威胁的能力相结合，以抵御复杂的攻击，包括新的漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法。

  卡巴斯基端点保护平台 (EPP) 应用程序检测到安全事件后，会在 Kaspersky Security Center 云控制台中生成包含有关安全事件的重要数据的详细卡片。事件卡由以下应用程序之一生成：

  - Kaspersky Endpoint Agent 与卡巴斯基 EPP 应用程序一起安装
  - Kaspersky Endpoint Security 11.7.0 for Windows 或更高版本，具有内置 EDR Optimum 功能，不需要额外安装 Kaspersky Endpoint Agent

  事件卡使您能够分析和调查事件。此外，您还可以通过创建威胁发展链图来可视化事件。该图可及时描述检测到的攻击的部署阶段。创建的图表包括有关参与攻击的模块以及这些模块执行的操作的信息。

  您还可以发起一系列响应操作：为不受信任的对象创建执行阻止规则；根据选定的危害指标 (IOC) 在设备组中搜索类似事件；隔离不受信任的对象；将受感染的设备与网络隔离。

  有关应用程序激活的信息，请参阅Kaspersky Endpoint Detection and Response Optimum 文档。

  如果集成，此应用程序会将**警报**部分添加到 Kaspersky Security Center 云控制台的界面（**监控和报告→警报**）。

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response 为那些难以找到专业知识和员工的组织或内部资源有限的组织提供全天候保护，抵御日益增长的威胁，这些威胁可绕过自动安全屏障。卡巴斯基或第三方公司的 MDR SOC 分析师会调查事件并提供对解决事件的响应。您可以手动接受或拒绝所提供的措施，或启用自动接受所有响应的选项。

  有关应用程序激活的信息，请参阅Kaspersky Managed Detection and Response 文档。

  如果集成，此应用程序会将**事件**部分添加到 Kaspersky Security Center 云控制台的界面（**监控和报告 → 事件**）。

您可以随时在 Kaspersky Security Center 云控制台的界面选项部分显示或隐藏引用 Kaspersky Endpoint Detection and Response 或 Kaspersky Managed Detection and Response 功能的界面元素。

Kaspersky Security Center 云控制台入门

完成本部分中的方案后，Kaspersky Security Center 云控制台即可使用。

启动方案

方案实施分为几个阶段：

1. **创建账户**

   若要开始使用 Kaspersky Security Center 云控制台，您需要一个账户。

   若要创建账户：

   1. 打开浏览器并输入以下地址：https: //ksc.kaspersky.com 。
   2. 单击**创建账户**按钮。
   3. 按照屏幕上的说明进行操作。

2. **创建工作区**

   创建账户后，您可以注册您的公司并创建您的工作区。

   当您开始使用 Kaspersky Security Center 云控制台时，您可以请求试用工作区（在这种情况下，您将获得嵌入在工作区中的 30 天试用授权许可）或输入商业授权许可的激活码。

   > 您无法将试用工作区转换为商业工作区。要在试用授权许可到期后继续使用 Kaspersky Security Center 云控制台，您必须删除试用工作区并使用商业授权许可创建另一个工作区。

   注册公司并创建工作区：

   1. 打开浏览器并输入以下地址：https: //ksc.kaspersky.com 。
   2. 单击**登录**按钮。
   3. 按照屏幕上的说明进行操作。

3. **执行 Kaspersky Security Center 云控制台的初始设置**

   首次进入创建的工作区时，系统会自动提示您运行快速启动向导。快速启动向导将指导您创建最少的必要任务和策略、调整最少的设置，并开始创建卡巴斯基应用程序的安装包。按照屏幕上的说明进行操作。

初始设置完成后，Kaspersky Security Center 云控制台即可使用。

有关管理客户设备的建议

本部分包含有关组织要保护的客户设备的建议。

建议取决于您是首次使用 Kaspersky Security Center 还是已经使用本地版本：

- 如果您以前从未使用过 Kaspersky Security Center ，您有两种选择：

- 为每个客户的设备创建虚拟管理服务器（推荐选项）。在这种情况下，每个客户的设备都可以通过独立于其他客户的专用虚拟管理服务器进行管理。同时，您可以使用主管理服务器为所有客户创建通用策略和任务。主管理服务器上生成的报告可以包括来自所有虚拟管理服务器的数据。

- 为每个客户的设备创建一个管理组。如果要进一步划分客户设备，您可以在每个父组下创建从属管理组的层次结构。例如，如果您想对不同部门的员工的设备使用不同的保护设置，您可能需要从属组。

- 如果您已使用在本地运行的 Kaspersky Security Center，则可以将现有管理组和相关对象从Kaspersky Security Center 本地迁移到 Kaspersky Security Center 云控制台。

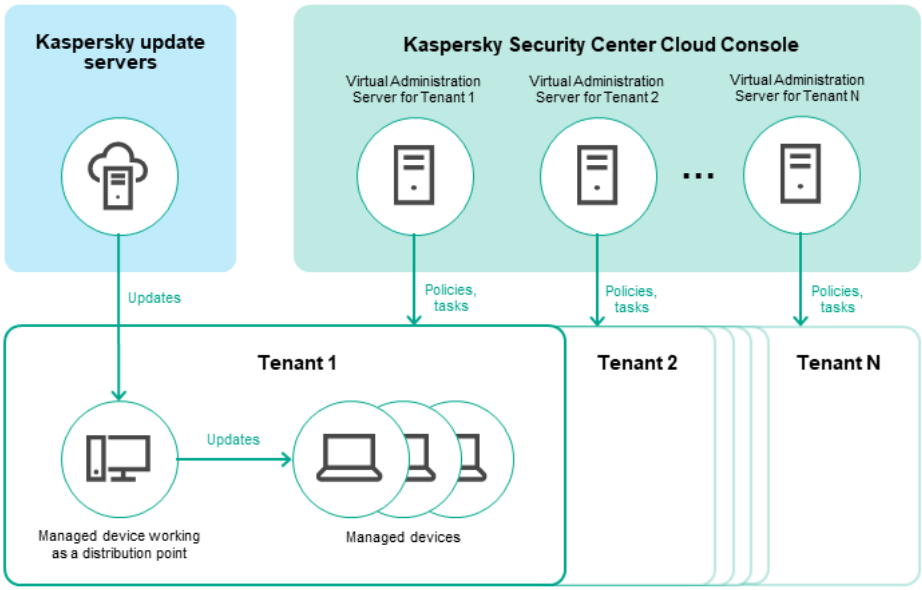
  您无法迁移虚拟管理服务器。迁移管理组和其他对象后，您可以在 Kaspersky Security Center 云控制台中创建虚拟管理服务器。

  继续配置迁移。

虚拟管理服务器的管理员只能从主管理服务器访问该虚拟服务器。在主管理服务器上创建的所有对象都可供虚拟管理服务器的管理员读取（例如，小部件、报告或用户角色）。

MSP 典型部署方案

本节提供 MSP 通常用于管理多个租户的部署方案的描述。该方案基于通过为每个租户单独创建的虚拟管理服务器进行管理。



MSP 典型部署方案

该方案包括以下主要部分：

- *Kaspersky Security Center 云控制台*。为工作区的管理服务提供用户界面。您可以使用 Kaspersky Security Center 云控制台来部署、管理和维护客户组织网络的保护系统。

- *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。

- *虚拟管理服务器*。MSP 管理员通常为每个租户创建一个虚拟管理服务器，以部署、管理和维护相应客户端组织网络的保护系统。

- *租户*。其设备要受到保护的客户组织。

- *受管理设备*。受 Kaspersky Security Center 云控制台保护的客户公司设备。每台需要保护的设备都必须安装网络代理和一个 Kaspersky 安全应用程序。

- *受管理设备作为分发点工作*。安装了网络代理并用于更新发布、网络轮询、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。管理员可选择适当的设备并手动为其分配分发点。

方案：保护部署（通过虚拟管理服务器进行租户管理）

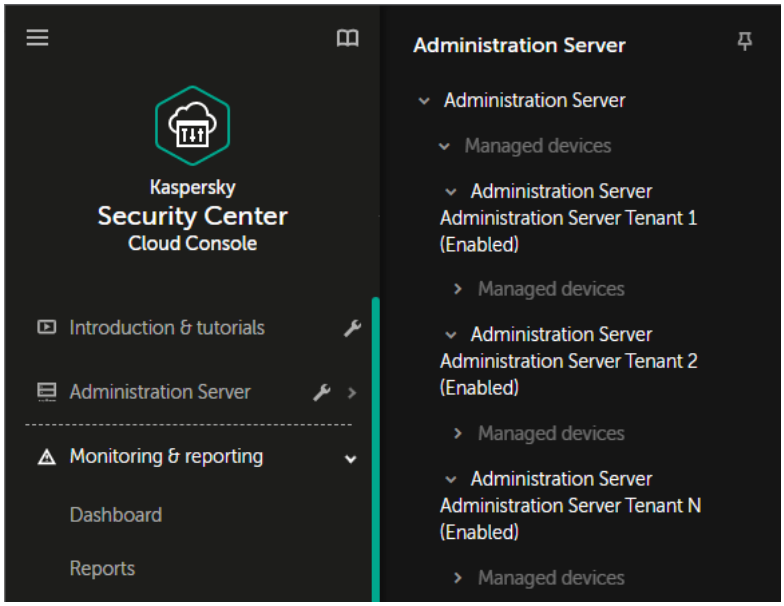
如果您从未使用过 Kaspersky Security Center 并且想要通过虚拟管理服务器管理您的租户，请按照本节中所述进行操作。完成此方案后，您客户的设备将受到保护。

如果您管理多个租户，请分别为每个租户执行该方案。

方案实施分为几个阶段：

1. **创建虚拟管理服务器**

   为您的客户创建虚拟管理服务器。新的虚拟管理服务器出现在管理服务器的层次结构中：



管理服务器层次结构中的虚拟管理服务器

2. **分配受管理设备作为分发点**

   在客户的设备中，决定哪台设备作为分发点。

   一个工作区中的分发点不能超过 100 个。

3. **为网络代理创建独立安装包**

   切换到创建的虚拟管理服务器，然后创建网络代理的独立安装包。您可以通过单击当前管理服务器名称右侧的 V 形图标（）、然后选择所需的管理服务器在主菜单中切换管理服务器。在创建独立安装包期间，指定要将设备移动到的受管理设备管理组。

4. **在所选设备上安装网络代理以充当分发点**

   您可以使用任何适合您的方法：

   - 手动安装

例如，您可以将独立安装包复制到可移动驱动器（例如闪存驱动器）或将其放置在共享文件夹中。

- 使用 Active Directory 进行部署
- 使用远程监控和管理 (RMM) 软件解决方案进行部署

5. **分配分发点**

   指定安装了网络代理的设备作为分发点。

6. **网络轮询**

   通过分发点配置并执行网络轮询。

   Kaspersky Security Center 云控制台提供以下网络轮询方法：

   - IP 范围轮询
   - Windows 网络轮询
   - 活动目录轮询

   根据计划完成网络轮询后，您客户的设备将被发现并放置在**未分配的设备**组中。

7. **移动发现的设备到管理组**

   设置自动将发现的设备移至所需管理组的规则；或手动将这些设备移动到所需的管理组。如果您计划在单个管理组中管理客户的设备，则可以将设备移至受管理设备组。

8. **为网络代理和受管理卡巴斯基应用程序创建安装包**

   创建卡巴斯基应用程序的安装包。

9. **删除不兼容的第三方安全应用程序**

   如果您客户的设备上安装了第三方安全应用程序，请在安装卡巴斯基应用程序之前将其删除。

10. **安装卡巴斯基应用程序到客户端设备**

    创建远程安装任务以在客户的设备上安装网络代理和受管理卡巴斯基应用程序。

    如有必要，您可以创建多个远程安装任务来为不同的管理组或不同的设备分类安装受管理的卡巴斯基应用程序。

    创建任务后，您可以配置其设置。确保每个任务的计划都符合要求。首先，必须运行安装网络代理的任务。在客户的设备上安装网络代理后，必须运行安装受管理卡巴斯基应用程序的任务。

11. **验证卡巴斯基应用程序的初始部署**

    生成并查看**卡巴斯基软件版本报告**。确保受管理的卡巴斯基应用程序安装在客户的所有设备上。

12. **为卡巴斯基应用程序创建策略**

    为所需的卡巴斯基应用程序创建策略。如果您想要为所有客户创建通用策略，请将当前虚拟管理服务器切换到主管理服务器，然后为所需的卡巴斯基应用程序创建策略。

方案：保护部署（通过管理组进行租户管理）

如果您从未使用过 Kaspersky Security Center 并且想要通过管理组管理您的租户，请按照本节中所述进行操作。完成此方案后，您客户的设备将受到保护。

方案实施分为几个阶段：

1. **创建管理组**

   为每个客户创建一个管理组。

2. **规划分发点结构**

   在每个客户的设备中，决定哪台设备作为分发点。

   > 一个工作区中的分发点不能超过 100 个。

3. **为网络代理创建独立安装包**

   为网络代理创建独立安装包。

4. **在选定的设备上安装网络代理以充当分发点**

   在将充当分发点的选定设备上安装网络代理。

   您可以使用任何适合您的方法：

   - 手动安装
     例如，您可以将独立安装包复制到可移动驱动器（例如闪存驱动器）或将其放置在共享文件夹中。
   - 使用 Active Directory 进行部署
   - 使用远程监控和管理 (RMM) 软件解决方案进行部署

5. **分配分发点**

   将安装了网络代理的设备分配为分发点。

6. **网络轮询**

   通过分发点配置并执行网络轮询。

   Kaspersky Security Center 云控制台提供以下网络轮询方法：

   - IP 范围轮询
   - Windows 网络轮询
   - 活动目录轮询

   根据计划完成网络轮询后，您客户的设备将被发现并放置在**未分配的设备**组中。

7. **移动发现的设备到管理组**

   设置自动将发现的设备移至所需管理组的规则；或手动将这些设备移动到所需的管理组。

8. **为网络代理和受管理卡巴斯基应用程序创建安装包**

   如果您没有启动快速启动向导，或者跳过了创建安装包的步骤，请创建卡巴斯基应用程序的安装包。

9. **删除不兼容的第三方安全应用程序**

   如果您客户的设备上安装了第三方安全应用程序，请在安装卡巴斯基应用程序之前将其删除。

10. **在客户的设备上安装 Kaspersky 应用程序**

    创建远程安装任务以在客户的设备上安装网络代理和受管理卡巴斯基应用程序。

如有必要，您可以创建多个远程安装任务来为不同的管理组或不同的设备分类安装受管理的卡巴斯基应用程序。

创建任务后，您可以配置其设置。确保每个任务的计划都符合要求。首先，必须运行安装网络代理的任务。在客户的设备上安装网络代理后，必须运行安装受管理卡巴斯基应用程序的任务。

11. **验证卡巴斯基应用程序的初始部署**

    生成并查看**卡巴斯基软件版本报告**。确保受管理的卡巴斯基应用程序安装在客户的所有设备上。

12. **为卡巴斯基应用程序创建策略**

    转到**资产(设备)→组**菜单；如果您想为所有客户创建通用策略，请选择**管理服务器**。如果要为单个客户创建特定策略，请选择与该客户对应的管理组。为所需的卡巴斯基应用程序创建策略。

联合使用 Kaspersky Security Center 本地部署和Kaspersky Security Center 云控制台

如果您已使用本地运行的 Kaspersky Security Center，则可以将本地运行的现有管理服务器转换为新的 Kaspersky Security Center 云控制台管理服务器的从属管理服务器，如本节所述。

如果您配置 Kaspersky Security Center on-premises 和 Kaspersky Security Center 云控制台的联合使用，您将无法从 Kaspersky Security Center on-premises 迁移到 Kaspersky Security Center 云控制台，除非您删除管理服务器的层次结构。

要创建管理服务器层级，

将本地运行的现有管理服务器添加为从属管理服务器。

适用于 MSP 的卡巴斯基应用程序授权许可

Kaspersky Security Center 云控制台使您可以集中为客户设备上的 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。

如果您管理多个租户，您可以通过以下方式分发授权许可密钥：

- 所有租户都拥有一个授权许可密钥。
- 每个租户都有一个单独的授权许可密钥。

要将授权许可密钥分发到客户的设备：

1. 添加所需授权许可密钥到管理服务器存储库。
2. 执行以下操作之一：
   - 配置自动分发授权许可密钥。

     在这种情况下，Kaspersky Security Center 云控制台会选择适用的授权许可密钥之一，并在每次发现新设备时自动部署它。
   - 配置添加密钥任务以将授权许可密钥分发到设备。

配置任务时，您选择必须部署到设备的授权许可密钥，并选择包含所需设备的管理组。

一项任务只能分发一个授权许可密钥。这意味着，如果您想要分发多个授权许可密钥，则必须为每个授权许可密钥创建一个任务。

安装在客户设备上的卡巴斯基应用程序已激活。

MSP 的监控和报告功能

Kaspersky Security Center 云控制台为您提供监控和报告功能。这些功能给您一个组织基础架构、保护状态和统计信息的总览。

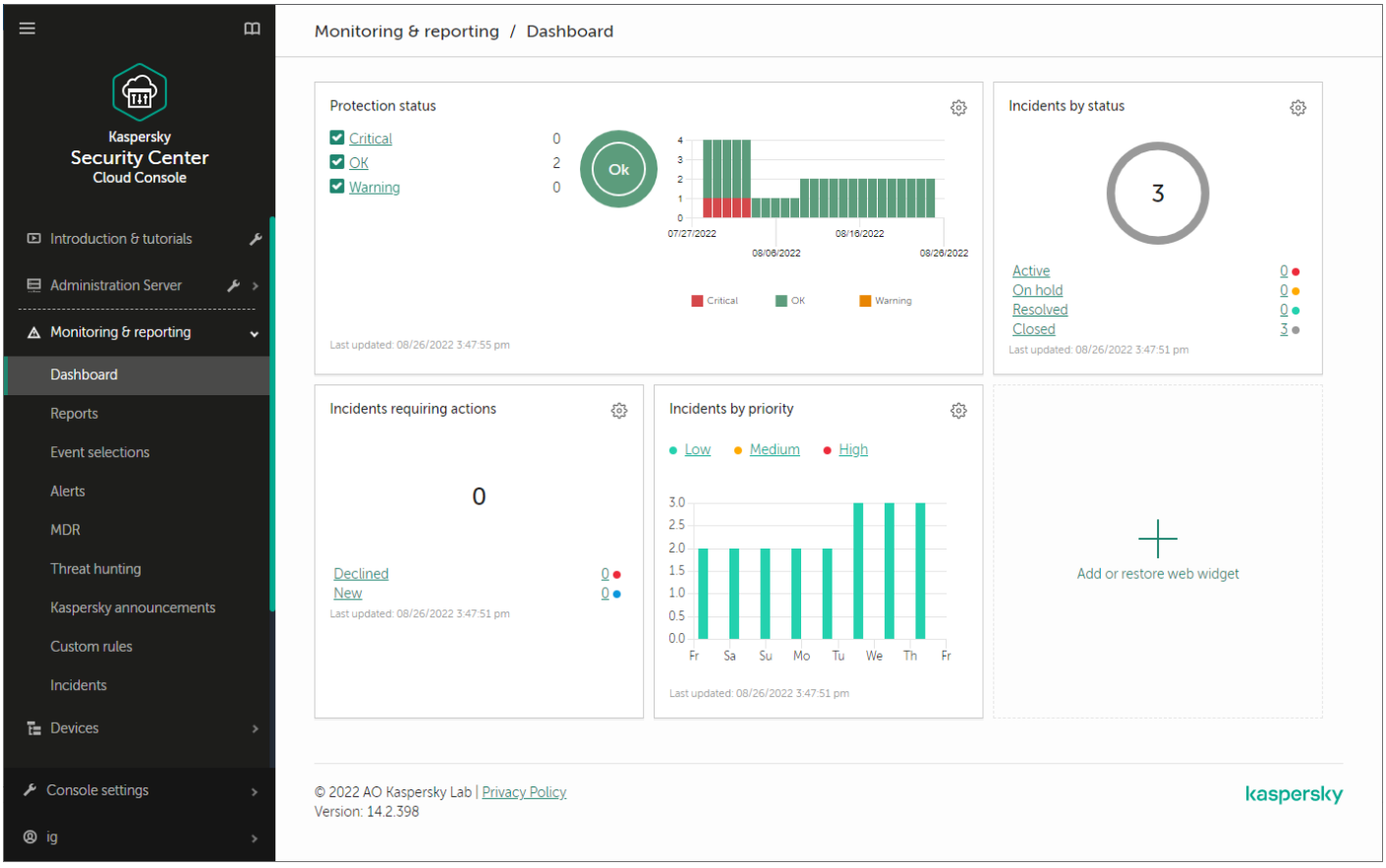
部署 Kaspersky Security Center 云控制台后，您可以配置监控和报告功能以最适合您的需求。

Kaspersky Security Center 云控制台提供以下类型的监控和报告功能：

- 控制板
- 报告
- 事件分类
- 电子邮件通知

控制板

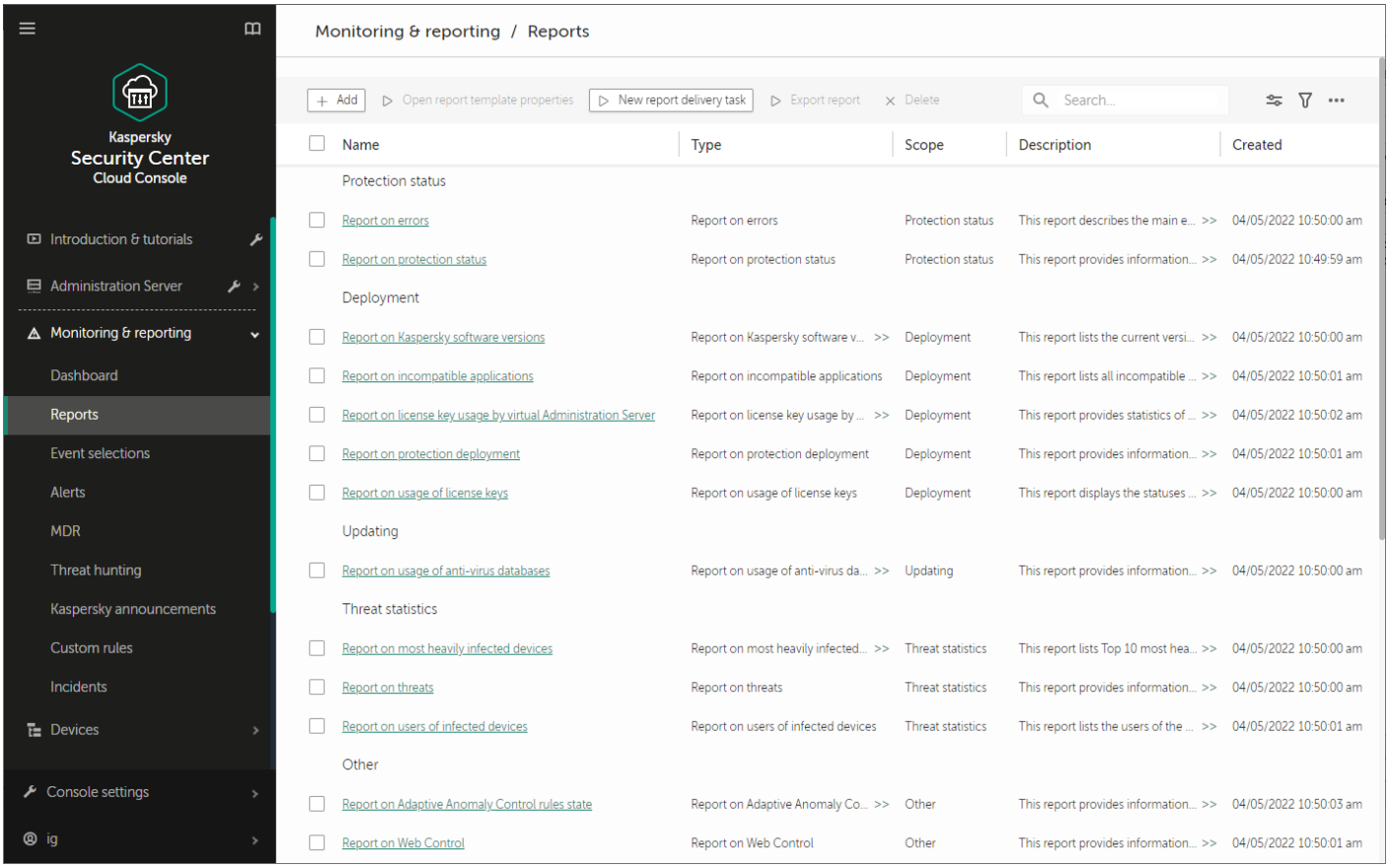
控制板通过对信息进行图形显示来允许您监控您组织网络的安全趋势（请见下图）。



仪表板部分

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。您还可以安排通过电子邮件发送报告（见下图）。



报告部分

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。Kaspersky Security Center 云控制台包含许多预定义的事件分类（例如，**最近事件**和**严重事件**）。此外，您还可以创建自定义事件分类。

电子邮件通知

您可以配置有关 Kaspersky Security Center 云控制台和客户设备上发生的事件的电子邮件通知。

在云环境中使用 Kaspersky Security Center 云控制台

本节提供了 Kaspersky Security Center 云控制台与操作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 云控制台的信息。

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，则与云设备相关的界面元素无法操作。

云环境中的授权许可选项

在 Kaspersky Security Center 云控制台的试用模式和商业模式下都可以在云环境中工作：

- 在试用模式下，您的工作区的整个有效期内都可以使用所有云环境功能。不需要授权许可。
- 在商业模式下，仅当卡巴斯基混合云安全授权许可密钥已在管理服务器属性中添加为活动状态时，云环境功能才可用。

在这两种情况下，漏洞和补丁管理都会自动激活。

尝试使用 Kaspersky Hybrid Cloud Security 的授权许可激活云环境的功能支持时，您可能会遇到错误。

通过 Kaspersky Security Center 云控制台为云环境中的工作做准备

本节介绍如何准备在以下云环境中使用 Kaspersky Security Center 云控制台：

- Amazon Web Services
- Microsoft Azure
- Google Cloud

使用 Amazon Web Services 云环境

该部分提供了使用 Kaspersky Security Center 云控制台在 Amazon Web Services 中工作的步骤。

截至 Kaspersky Security Center 云控制台发布之日，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

要使用 AWS 平台，特别是为了创建实例，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。

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 云控制台发布之日，本文档中引用的网页地址是正确的。

为 Amazon EC2 实例创建 IAM 用户账户

该部分描述了为了确保 Kaspersky Security Center 云控制台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) 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 云控制台具有使用 AWS 的权限

要使用 Kaspersky Security Center 云控制台在 Amazon Web Services 云环境中进行操作，您必须创建一个*IAM 用户账户*， Kaspersky Security Center 云控制台将使用该账户来使用 AWS 服务。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 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。

创建 IAM 用户账户以使用 Kaspersky Security Center 云控制台

使用 Kaspersky Security Center 云控制台需要 IAM 用户账户。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 云控制台的 *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：

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://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**。
     添加权限后，查看它是否准确。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。

截至 Kaspersky Security Center 云控制台发布之日，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 云控制台在 Microsoft Azure 提供的云环境的操作和维护信息，以及在云环境中的虚拟机上的保护部署详情。

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。在开始在 Kaspersky Security Center 云控制台中使用 Microsoft Azure 之前，请创建一个具有在虚拟机上安装应用程序所需权限的 Azure 应用程序 ID。

创建订阅、应用程序 ID 和密码

要在 Microsoft Azure 环境中使用 Kaspersky Security Center 云控制台，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 云控制台。

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 云控制台。

   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 云控制台发布之日，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，还要通过 Azure API 部署保护，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 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 云控制台的信息。

您可以在 Google Cloud Platform 中将 Google API 与 Kaspersky Security Center 云控制台配合使用。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 云控制台提供以下凭据：

- 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。

Kaspersky Security Center 云控制台中的云环境配置向导

要使用该向导配置 Kaspersky Security Center 云控制台，您必须拥有：

- 云环境的特定凭据：
  - 已被授予轮询云段权限的 IAM 用户账户（用于与 Amazon Web Services 配合使用）

- 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

如果您的工作区是使用卡巴斯基混合云安全授权许可创建的，云环境配置向导会在首次连接到 Kaspersky Security Center 云控制台时自动启动。您还可以在任意时刻手动启动云环境配置向导。

要手动启动云环境配置向导：

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。

此向导的平均会话时间是约 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 云控制台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：选择应用程序激活方法

仅当您在创建工作区期间使用了卡巴斯基混合云安全以外的授权许可并且从未将卡巴斯基混合云安全授权许可密钥添加到管理服务器的激活字段时，才会显示此步骤。在这种情况下，您必须使用卡巴斯基混合云安全授权许可激活管理服务器。

步骤 3：选择云环境和授权

指定下列设置：

- 云环境

  选择您要部署 Kaspersky Security Center 云控制台的云环境：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，使用 AWS IAM 访问密钥才能进一步轮询云段。输入以下关键数据：

- 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。

  在您选择 AWS IAM 访问密钥进行授权后，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。

在您选择 AWS IAM 访问密钥进行授权后，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 云控制台。

- **Azure 存储访问密钥**

  您创建 Azure 存储账户以使用 Kaspersky Security Center 云控制台时接收密码（密钥）。

  密钥在“Azure 存储账户概述”区域可用，在“密钥”子区域。

  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。

云环境配置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：分段轮询并配置与云的同步

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（默认每五分钟轮询一次；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**与云结构同步管理组**设置。

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。该组结构可让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 云控制台需要同步，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。

单击“**下一步**”继续。

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 云控制台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 云控制台配置卡巴斯基安全网络

在试用模式下或在虚拟管理服务器上运行Kaspersky Security Center 云控制台时，将跳过此步骤。

指定设置以转发 Kaspersky Security Center 云控制台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 云控制台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 云控制台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安全网络，受管理应用程序不会将数据发送到 Kaspersky。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云控制台进行云段轮询

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 云控制台使用该信息更新“Unassigned devices”和“Managed devices”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。

要允许轮询云段，您必须拥有提供了 IAM 用户账户（在 AWS 中），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。

通过 Kaspersky Security Center 云控制台添加云段轮询连接

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 云控制台的云环境：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，请指定以下内容：
     - 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。
       在您选择 AWS IAM 访问密钥进行授权后，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。
       在您选择 AWS IAM 访问密钥进行授权后，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 云控制台。

- Azure 存储访问密钥

  您创建 Azure 存储账户以使用 Kaspersky Security Center 云控制台时接收密码（密钥）。

  密钥在“Azure 存储账户概述”区域可用，在“密钥”子区域。

  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 云控制台配置轮询计划

云段轮询根据计划执行。您可以设置轮询频率。

轮询频率被云环境配置向导自动设置为五分钟。您可以在任意时刻更改该值并设置不同的计划。然而，不建议设置大于每五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。
   云段设置窗口打开。
4. 在**云段设置**窗口中，单击**设置轮询计划**按钮。
   计划窗口将打开。
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。

- 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。

- 开始间隔 (天)

  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

  如果您的工作区在计划轮询期间不可用，Kaspersky Security Center 云控制台可以在工作区再次可用后立即启动轮询，或等待下一次计划轮询时间。
  如果启用此选项，Kaspersky Security Center 云控制台将在工作区再次可用后立即开始轮询。
  如果禁用该选项，Kaspersky Security Center 云控制台等待下一次计划轮询。
  默认情况下已启用该选项。

6. 单击“保存”保存设置。

云段的轮询计划即被配置并保存。

通过 Kaspersky Security Center 云控制台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**。

将显示可用于轮询的云段。

通过 Kaspersky Security Center 云控制台查看云设备的属性

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

在云环境配置向导操作期间，与云同步规则被自动创建。此规则可让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**。
   移动规则列表将打开。
2. 在移动规则列表中，选择"**与云同步**"。
   规则属性窗口打开。
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 云控制台将创建这类子组。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 云控制台不创建任何新子组。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。如果您的 Kaspersky Security Center 云控制台需要**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**删除在云段中未找到匹配的子组**选项，然后强制规则。

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，即设备位于云环境之外，或者位于云环境中，但是由于某些原因无法使用 API 检测到该设备。
   - **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。
   - 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 云控制台支持以下情景：

- 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 云控制台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。

更改 Kaspersky Security Center 云控制台界面的语言

您可以选择 Kaspersky Security Center 云控制台界面的语言。

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。

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 云控制台文档或任何 Kaspersky Security Center 云控制台信息源中都找不到问题的解决方案，请联系卡巴斯基技术支持。技术支持专家将回答关于安装和使用 Kaspersky Security Center 云控制台的所有问题。

Kaspersky 在 Kaspersky Security Center 云控制台的生命周期内提供支持（请参见产品支持生命周期页面）。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。

卡巴斯基技术支持专家所需的信息

当您联系卡巴斯基技术支持专家时，他们可能会要求您提供以下信息：

- 关于 Kaspersky Security Center 云控制台的一般信息
- 工作区 ID
- 授权许可信息
- 已安装应用程序的数量
- 租户 ID 和状态

您可以在**您的账户菜单→技术支持**部分找到此信息。复制并分享此信息以获得有关您的问题的帮助。

有关程序的信息源

Kaspersky 网站上的 Kaspersky Security Center 云控制台页面

在 Kaspersky 网站的 Kaspersky Security Center 云控制台页面上，您可以查看有关程序、程序功能和特性的一般信息。

知识库中的 Kaspersky Security Center 云控制台页面

*知识库*是 Kaspersky 技术支持网站的一部分。

在 知识库的 Kaspersky Security Center 云控制台页面上，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 云控制台和 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。

在该论坛上，您可以查看讨论主题，发表您的评论，创建新讨论主题。

> 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。

已知问题

Kaspersky Security Center 云控制台具有许多对于应用程序运行并不重要的限制：

- 当您导入*将更新下载到分发点存储库*或*更新验证*任务时，将启用**选择任务将分配到的设备**选项。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。
- Linux 设备的*清单扫描*任务完成后，尝试将收到的文件发送到卡巴斯基进行分析会返回错误。
- 如果您尝试使用 Active Directory 联合身份验证服务 (ADFS) 登录Kaspersky Security Center 云控制台，但缺少所需权限， Kaspersky Security Center 云控制台仍会返回“无效凭据”错误，而不是警告用户缺少权限。
- 对于运行 macOS 的设备，管理设备任务无法正常工作。
- 在“远程诊断”窗口中，单击**下载整个文件**按钮可能无法正确下载。

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 云控制台的应用程序编程接口。具体来说，AWS API 工具用于云段轮询。

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。

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。

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 云控制台上的账户

您必须拥有的账户才能配置 Kaspersky Security Center 云控制台，例如添加和删除用户账户以及配置安全配置文件（安全策略）。此账户可让您使用"我的卡巴斯基"服务。您在开始使用 Kaspersky Security Center 云控制台时创建此账户。

Kaspersky Security Center 云控制台操作者

对通过 Kaspersky Security Center 云控制台管理的保护系统的状态和操作进行监视的用户。

Kaspersky Security Center 云控制台管理员

通过 Kaspersky Security Center 云控制台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。

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

在 BIOS 级别整合了 Kaspersky Anti-Virus for UEFI 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。

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 云控制台管理的 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 云控制台中的事件信息。

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。

分发点

安装了网络代理并用于更新发布、网络轮询、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。管理员可选择适当的设备并手动为其分配分发点。

卡巴斯基安全网络 （KSN）

一种云服务基础架构，可提供对 Kaspersky 数据库的访问，其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。

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

安装了网络代理的计算机或安装了卡巴斯基安全应用程序的移动设备。

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。

安装包

使用 Kaspersky Security Center 云控制台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。

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。

工作区

为特定公司创建的 Kaspersky Security Center 云控制台实例。当客户创建工作区时，卡巴斯基会创建并配置管理公司设备上安装的安全应用程序所需的基础架构和基于云的管理控制台。

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。

应用程序标签

第三方应用程序的标签，可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。

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。

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。

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。

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。

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。

策略配置文件

策略设置的命名子集。该子集随带策略在目标设备上分发，在特别条件配置文件激活条件下将其补充。

管理 Web 插件

一个用于通过 Kaspersky Security Center 云控制台对 Kaspersky 软件进行远程管理的特殊组件。管理插件是 Kaspersky Security Center 云控制台与特定 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。

管理服务器

Kaspersky Security Center 云控制台的一个组件，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 云控制台的一个组件，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 云控制台组件，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：

- 虚拟管理服务器只能作为从属管理服务器运行。
- 虚拟管理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。

设备标签(T)

可以用于分组、描述或查找设备的设备标签。

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。

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。

远程安装

使用 Kaspersky Security Center 云控制台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。

附加订阅密钥

证明程序的使用权限、但是目前尚未使用的密钥。

隔离

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。

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 云控制台中提供的管理服务进行远程应用程序管理。

有关第三方代码的信息

有关第三方代码的信息包含在文件legal_notices.txt中。

文件 legal_notices.txt 也位于 Network Agent for Windows 和 Network Agent for Linux 的安装文件夹中。

有关用于工作区的第三方代码的更多信息，请参阅Kaspersky Endpoint Security Cloud 文档。

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、PostScript、Reader、Shockwave 是 Adobe 在美国和/或其他国家/地区的商标或注册商标。

AMD64 是 Advanced Micro Devices, Inc. 的商标或注册商标。

Amazon、Amazon EC2、Amazon Web Services、AWS、和 AWS Marketplace 是 Amazon.com, Inc. 或其附属公司的商标。

Apache 是 Apache Software Foundation 的注册商标或商标。

Apple、App Store、AppleScript、FileVault、iPhone、iTunes、Mac、Mac OS、macOS、OS X、Safari 和 QuickTime 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、IOS、Cisco Jabber 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 和 XenServer 是 Citrix Systems, Inc. 和/或其附属公司在美国专利及商标局和其他国家的注册商标。

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。

Corel 和 CorelDRAW 是 Corel Corporation 和/或其附属公司在美国和其他国家/地区的注册商标。

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、Dalvik、Firebase、Google Chrome、Google Earth、Google 地图、Google Play、Google Public DNS 是 Google LLC 的商标。

EulerOS 是华为技术有限公司的商标。

Intel 和 Core 是 Intel Corporation 在美国和其他国家/地区注册的商标。

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、ActiveX、BitLocker、Excel、Hyper-V、InfoPath、Internet Explorer、Microsoft Edge、MS-DOS、MultiPoint、Office 365、OneNote、Outlook、PowerPoint、PowerShell、Segoe、Skype、SQL Server、Tahoma 、Visio、Win32、Windows、Windows Azure、Windows Media、Windows Mobile、Windows Phone、Windows Server 和 Windows Vista 是 Microsoft 集团公司的商标。

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。

Oracle、Java、JavaScript 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。

Python 是 Python Software Foundation 的商标或注册商标。

Red Hat、Red Hat Enterprise Linux、CentOS 和 Fedora 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。

BlackBerry 是 Research In Motion Limited 所有的商标，在美国和/或其他国家注册。

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 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。

VMware、VMware vSphere 和 VMware Workstation 是 VMware, Inc. 在美国和/或其他国家的注册商标或商标。

UNIX 是在美国和其他国家的注册商标，通过 X/Open Company Limited 授权。