kaspersky

Kaspersky Embedded Systems Security

目录

关于 Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security 保护运行 Microsoft® Windows® 的计算机和其他嵌入式系统（以下也称为受保护设备）抵御病毒和其他计算机威胁。Kaspersky Embedded Systems Security 用户是负责公司网络反病毒保护的公司网络管理员和专业人员。

您可以在运行 Windows 的各种嵌入式系统上安装 Kaspersky Embedded Systems Security，包括以下设备类型：

- ATM（自动柜员机）
- POS（销售终端）

可通过以下方式管理 Kaspersky Embedded Systems Security：

- 通过与 Kaspersky Embedded Systems Security 安装在同一台受保护设备上或安装在其他设备上的应用程序控制台来管理
- 在命令行中使用命令
- 通过 Kaspersky Security Center 管理控制台

Kaspersky Security Center 程序也可以集中管理运行 Kaspersky Embedded Systems Security 的多台受保护设备。

您可以查看针对“系统监控器”应用的 Kaspersky Embedded Systems Security 性能计数器以及 SNMP 计数器和陷阱。

Kaspersky Embedded Systems Security 组件和功能

应用程序包括以下组件：

- **实时文件保护**。Kaspersky Embedded Systems Security 在对象被访问时扫描对象。Kaspersky Embedded Systems Security 扫描以下对象：
  - 文件
  - 交换文件系统流（NTFS 流）
  - 在本地硬盘驱动器和可移动驱动器上的主引导记录和引导扇区
- **按需扫描**。Kaspersky Embedded Systems Security 可在指定区域运行单独的扫描，以检测病毒和其他计算机安全威胁。应用程序会扫描受保护设备上的文件、RAM 和自动运行对象。
- **应用程序启动控制**。该组件可跟踪用户启动应用程序的尝试并控制受保护设备上的应用程序启动。
- **设备控制**。该组件可控制外部设备的注册和使用，以便保护设备在与 USB 连接的闪存驱动器或其他类型的外部设备交换文件时，免受可能产生的计算机安全威胁。
- **防火墙管理**。此组件提供管理 Windows 防火墙的能力：配置设置和操作系统防火墙规则，并阻止从外部配置防火墙的任何可能性。
- **文件完整性监控**。Kaspersky Embedded Systems Security 可以检测任务设置中指定的监控范围内的文件更改。这些更改可能表示受保护设备遭到安全入侵。
- **日志审查**。此组件根据 Windows 事件日志的审查结果，对受保护环境的完整性进行监控。

该应用程序中部署了以下功能：

- **数据库更新**和**软件模块更新**。Kaspersky Embedded Systems Security 会从 Kaspersky 的 FTP 或 HTTP 更新服务器、Kaspersky Security Center 管理服务器或其他更新源下载应用程序数据库和模块更新。

- **隔离**。Kaspersky Embedded Systems Security 通过将疑似感染对象从其原始位置移动到*隔离*文件夹来隔离这些对象。出于安全目的，隔离文件夹中的对象以加密形式存储。

- **备份**。对于被归类为"*已感染*"的对象，Kaspersky Embedded Systems Security 会在对其进行清除或删除之前，在*备份*中存储这些对象的加密副本。

- **管理员和用户通知**。您可以对该程序进行配置，通知访问受保护设备的管理员和用户有关 Kaspersky Embedded Systems Security 操作中的事件和设备上反病毒保护的状态。

- **导入和导出设置**。可以将 Kaspersky Embedded Systems Security 设置导出到 XML 配置文件，也可以将配置文件中的设置导入到 Kaspersky Embedded Systems Security 中。可以将所有应用程序设置或仅将单个组件的设置保存到配置文件。

- **应用模板**。可以在受保护设备的文件资源树或列表中手动配置节点的安全性设置，并将配置好的设置值保存为模板。然后可在 Kaspersky Embedded Systems Security 保护和扫描任务中使用该模板来配置其他节点的安全设置。

- **管理 Kaspersky Embedded Systems Security 功能的访问权限**。您可以为用户和用户组配置管理 Kaspersky Embedded Systems Security 的权限和管理应用程序注册的 Windows 服务的权限。

- **将事件写入到 Windows 事件日志**。Kaspersky Embedded Systems Security 将记录有关软件组件设置的信息、当前任务状态、任务运行过程中发生的事件、与 Kaspersky Embedded Systems Security 管理相关的事件，以及 Kaspersky Embedded Systems Security 错误诊断所需的信息。

- **信任区域**。您可以从保护范围或扫描范围中生成排除列表，Kaspersky Embedded Systems Security 将在按需和实时计算机保护任务中应用该列表。

- **漏洞利用防御**。您可以使用注入进程的代理来保护进程内存免受漏洞利用。

新增功能

新版本的 Kaspersky Embedded Systems Security 包含以下功能和改进：

- 现支持以下操作系统：
  - Windows 10 22H2
  - Windows 11 22H2
- 在“设备控制”任务中，您可以为规则范围使用掩码，仅允许受信任用户或用户组访问设备，并根据添加设备的 Kaspersky Security Center 网络列表中的数据创建规则。
- 扩展了“应用程序启动控制”任务的触发条件集：您可以通过定义的命令行启动程序，并且可以选择多个条件。
- 引入了使用适用于 Windows 的 AMSI 技术扫描可执行脚本的新组件。
- 防火墙管理任务：添加了出站连接规则，以及 ICMPv4 和 ICMPv6 连接管理。
- 为 Kaspersky Security Center 策略引入了故障诊断部分：您可以管理跟踪文件设置和 Dump 文件设置。此外，您可以在安装期间使用命令行实用程序 kavshell.exe 和安装程序命令行 setup.exe 管理这些选项。受 Kaspersky Embedded Systems Security 保护的设备的跟踪管理选项和转储管理选项在 Kaspersky Security Center 远程诊断实用程序中可用。
- 在安装期间，您可以使用安装程序命令行选择待迁移到新版本 Kaspersky Embedded Systems Security 的保存数据的范围。
- 添加了以下产品安装前提条件：操作系统必须支持具有 SHA-256 签名的证书。
- 为“日志检查”任务添加了“将事件发布到 Windows 事件日志”。
- 所有类型的安装包（带反病毒数据库和不带反病毒数据库）在安装过程中都会自动创建数据库更新任务。

应用程序发布版本是累积的，其中会包括早期版本中已解决的问题。

有关 Kaspersky Embedded Systems Security 的信息来源

本节列出了有关应用程序的信息来源。

您可以根据问题的重要性级别和紧迫程度选择最合适的信息来源。

独立检索信息源

您可以使用以下来源查找有关 Kaspersky Embedded Systems Security 的信息：

- Kaspersky 网站上的 Kaspersky Embedded Systems Security 页面。
- 技术支持网站（知识库）上的 Kaspersky Embedded Systems Security 页面。
- 手册。

如果您没有找到问题的解决方案，请与 Kaspersky 技术支持联系。

需要具有 Internet 连接才能使用在线信息来源。

Kaspersky 网站上的 Kaspersky Embedded Systems Security 页面

在 Kaspersky Embedded Systems Security 页面上，您可以查看有关该应用程序及其功能和特性的常规信息。

Kaspersky Embedded Systems Security 页面包含指向 eStore 的链接。您可以在其中购买应用程序或续订授权许可。

知识库中的 Kaspersky Embedded Systems Security 页面

知识库是技术支持网站的一部分。

知识库中的 Kaspersky Embedded Systems Security 页面包含一些文章，它们提供了有用的信息和建议，并解答了如何购买、安装和使用该应用程序的常见问题。

知识库文章不仅可以解答与 Kaspersky Embedded Systems Security 有关的问题，而且还可以解答与其他 Kaspersky 应用程序有关的问题。知识库文章可能还包含技术支持新闻。

Kaspersky Embedded Systems Security 文档

《Kaspersky Embedded Systems Security 管理员指南》包含有关应用程序安装、卸载、设置配置和使用的信息。

在论坛上讨论卡巴斯基应用程序

您可以在我们的论坛上与其他用户和卡巴斯基专家讨论与卡巴斯基应用程序相关的问题。

在论坛上，您可以查看现有主题，留下评论，也可以创建新讨论主题。

Kaspersky Embedded Systems Security

本节介绍了 Kaspersky Embedded Systems Security 的功能、组件以及分发包，并提供了 Kaspersky Embedded Systems Security 的硬件和软件要求列表。

分发包

分发包包括备受欢迎的应用程序，您可以用它来执行以下操作：

- 启动 Kaspersky Embedded Systems Security 安装向导。
- 启动 Kaspersky Embedded Systems Security 控制台安装向导。
- 启动将安装 Kaspersky Embedded Systems Security 管理插件的安装向导以通过 Kaspersky Security Center 管理应用程序。
- 转到 Kaspersky 网站上的 Kaspersky Embedded Systems Security 页面。
- 访问技术支持网站。
- 阅读有关 Kaspersky Embedded Systems Security 当前版本的信息。

\console 文件夹包含应用程序控制台的安装文件（“Kaspersky Embedded Systems Security 管理工具”组件集）。

\product 文件夹包含：

- 用于在运行 32 位或 64 位 Microsoft Windows 操作系统的受保护设备上安装 Kaspersky Embedded Systems Security 组件的文件。
- 用于安装管理插件的文件，以便通过 Kaspersky Security Center 管理 Kaspersky Embedded Systems Security。
- 程序发布时最新反病毒数据库的压缩文件。
- 包含最终用户授权许可协议和隐私策略文本的文件。

\product_no_avbases 文件夹包含不带反病毒数据库的 Kaspersky Embedded Systems Security 组件和管理插件的安装文件。

\setup 文件夹包含问候程序启动文件。

分发包文件保存在不同的文件夹中，具体位置取决于它们的目标用途（请参见以下表格）。

Kaspersky Embedded Systems Security 分发包文件

文件	用途
autorun.inf	从可移动驱动器安装应用程序时，Kaspersky Embedded Systems Security 安装向导的自动运行文件。
release_notes.txt	该文件包含发布信息。
migration.txt	该文件介绍从以前的应用程序版本进行迁移。
setup.exe	问候程序启动文件（启动 setup.hta）。

\console\esstools_x86.msi	Windows Installer 软件包；在运行 32 位 Microsoft Windows 操作系统的受保护设备上安装应用程序控制台。
\console\esstools_x64.msi	Windows Installer 软件包；在运行 64 位 Microsoft Windows 操作系统的受保护设备上安装应用程序控制台。
\console\setup.exe	该文件启动组件的“管理工具”组件集（包括应用程序控制台）的安装向导；它可使用在安装向导中指定的设置启动 esstools.msi 安装包文件。
\product\bases.cab	程序发布时最新反病毒数据库的压缩文件。
\product\setup.exe	用于在受保护设备上通过向导安装 Kaspersky Embedded Systems Security 的文件；它使用向导中指定的安装设置启动安装包文件 ess.msi。
\product\ess_x86.msi	Windows Installer 软件包；在运行 32 位 Microsoft Windows 操作系统的受保护设备上安装 Kaspersky Embedded Systems Security 的“使用反病毒基础技术保护计算机”配置。 如果选择“使用反病毒基础技术保护计算机”配置，则默认包括除“防火墙管理”和“性能计数器”组件之外的所有 Kaspersky Embedded Systems Security 组件。 在不使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用反病毒基础技术保护计算机”配置时，将添加以下组件来自动扩展应用程序组件集： • 实时文件保护 • 按需扫描 • 网络威胁防护
\product\ess_x64.msi	Windows Installer 软件包；在运行 64 位 Microsoft Windows 操作系统的受保护设备上安装 Kaspersky Embedded Systems Security 的“使用反病毒基础技术保护计算机”配置。 如果选择“使用反病毒基础技术保护计算机”配置，则默认包括除“防火墙管理”和“性能计数器”组件之外的所有 Kaspersky Embedded Systems Security 组件。 在不使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用反病毒基础技术保护计算机”配置时，将添加以下组件来自动扩展应用程序组件集： • 实时文件保护 • 按需扫描 • 网络威胁防护
\product\ess.kud	Kaspersky Unicode 定义格式的文件，带有用于通过 Kaspersky Security Center 远程安装 Kaspersky Embedded Systems Security 的安装包的说明。
\product\klcfginst.exe	管理插件的安装程序，以便通过 Kaspersky Security Center 管理 Kaspersky Embedded Systems Security。如果您计划使用管理插件来

	管理 Kaspersky Embedded Systems Security，请在每台已安装 Kaspersky Security Center 管理控制台的服务器上安装该插件。
\product\license.txt	最终用户授权许可协议和隐私策略的文本。
\product_long_term\setup.exe	用于在受保护设备上通过向导安装 Kaspersky Embedded Systems Security 的文件；它使用向导中指定的安装设置启动安装包文件 ess.msi。
\product_long_term\ess_x86.msi	Windows Installer 软件包；在运行 32 位 Microsoft Windows 操作系统的受保护设备上安装 Kaspersky Embedded Systems Security 的“使用默认拒绝技术保护计算机”配置。 启用更新的组件不包括在“使用默认拒绝技术保护计算机”配置中。 如果选择“使用默认拒绝技术保护计算机”配置，则默认包含以下组件： • Core • 漏洞利用防御 • 应用程序启动控制 • 系统托盘图标 在使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用默认拒绝技术保护计算机”配置时，将删除以下组件来自动缩减应用程序组件集： • 实时文件保护 • 按需扫描 • 启用更新的组件 建议使用此配置来保护资源有限的系统。在这种情况下，您可以长期激活应用程序，并且“应用程序启动控制”组件提供计算机保护。
\product_long_term\ess_x64.msi	Windows Installer 软件包；在运行 64 位 Microsoft Windows 操作系统的受保护设备上安装 Kaspersky Embedded Systems Security 的“使用默认拒绝技术保护计算机”配置。

	启用更新的组件不包括在“使用默认拒绝技术保护计算机”配置中。 如果选择“使用默认拒绝技术保护计算机”配置，则默认包含以下组件： • Core • 漏洞利用防御 • 应用程序启动控制 • 系统托盘图标 在使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用默认拒绝技术保护计算机”配置时，将删除以下组件来自动缩减应用程序组件集： • 实时文件保护 • 按需扫描 • 启用更新的组件 建议使用此配置来保护资源有限的系统。在这种情况下，您可以长期激活应用程序，并且“应用程序启动控制”组件提供计算机保护。
\product_long_term\ess_light.kud	Kaspersky Unicode 定义格式的文件，带有用于通过 Kaspersky Security Center 远程安装 Kaspersky Embedded Systems Security 的安装包的说明。
\product_long_term\klcfginst.exe	管理插件的安装程序，以便通过 Kaspersky Security Center 管理 Kaspersky Embedded Systems Security。如果您计划使用管理插件来管理 Kaspersky Embedded Systems Security，请在每台已安装 Kaspersky Security Center 管理控制台的服务器上安装该插件。
\product_long_term\license.txt	最终用户授权许可协议和隐私策略的文本。
\setup\setup.hta	问候程序启动文件。

硬件和软件要求

在安装 Kaspersky Embedded Systems Security 之前，您必须从设备中卸载其他反病毒应用程序。

对受保护设备的软件要求

您可以在运行 32 位或 64 位 Microsoft Windows 操作系统的设备上安装 Kaspersky Embedded Systems Security。

Windows Installer 3.1 是在运行 Microsoft Windows XP 的受保护设备上正常安装和使用应用程序所必需的。

要在运行嵌入式操作系统的受保护设备上安装和使用 Kaspersky Embedded Systems Security，“筛选管理器”组件是必需的。

为了让 Kaspersky Embedded Systems Security 正确运行，Windows 需要 SHA-2 支持。有关详细信息，请参阅：https://support.kaspersky.com/15728。

您可以在运行下列 32 位或 64 位 Microsoft Windows 操作系统的设备上安装 Kaspersky Embedded Systems Security：

- 工作站：
  - Windows XP 专业版 SP2 32 位/64 位
  - Windows XP 专业版 SP3 32 位
  - Windows 7 专业版/企业版/旗舰版 SP1 32 位/64 位
  - Windows 8 专业版/企业版 32 位/64 位
  - Windows 8.1 专业版/企业版 32 位/64 位
  - Windows 10 版本 1507 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 LTSC 2015 版本 1507 32 位/64 位
  - Windows 10 RS1 版本 1607 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 LTSC 2016 版本 1607 32 位/64 位
  - Windows 10 RS2 版本 1703 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 RS3 版本 1709 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 RS4 版本 1803 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 RS5 版本 1809 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 LTSC 2019 版本 1809 32 位/64 位
  - Windows 10 19H2 版本 1909 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 21H2 版本 21H2 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 10 LTSC 2021 版本 21H2 32 位/64 位
  - Windows 10 22H2 版本 22H2 家庭版/专业版/教育版/企业版 32 位/64 位
  - Windows 11 21H2 版本 21H2 家庭版/专业版/教育版/企业版 64 位

- Windows 11 22H2 版本 2H2 家庭版/专业版/教育版/企业版 64 位

- 嵌入式系统：
  - Windows XP Embedded SP2 (WEPOS) 32 位/64 位
  - Windows XP Embedded SP3 (POS Ready 2009) 32 位
  - Windows 7 SP1 Embedded 32 位/64 位
  - Windows Embedded 8.1 Industry Pro 32 位/64 位
  - Windows Embedded 8.0 Industry Pro 32 位/64 位
  - Windows 10 IoT 32 位/64 位

对受保护设备的硬件要求

受保护设备的硬件要求会随着安装的 Windows 操作系统而有所变化：

- 使用 Windows XP（32 位/64 位）、Windows Embedded POS Ready 32 位 或 Windows Embedded POS Ready 7 操作系统的设备的硬件要求：
  - 最低配置：
    - 磁盘空间要求：
      - 安装“应用程序启动控制”组件 – 50 MB。
      - 安装所有 Kaspersky Embedded Systems Security 组件 – 2 GB。
    - 内存：
      - 256 MB，仅在运行 Microsoft Windows 操作系统的设备上安装“应用程序启动控制”组件。
      - 512 MB，执行所有组件的完整安装。
    - 处理器要求：
      - 32 位 Microsoft Windows 操作系统：

        1.4 GHz 单核处理器
        Intel® Pentium® III
      - 64 位 Microsoft Windows 操作系统：

        1.4 GHz 单核处理器
        Intel Pentium IV
  - 推荐配置：
    - 磁盘空间要求：
      - 安装“应用程序启动控制”组件 – 2 GB。

- 安装所有 Kaspersky Embedded Systems Security 组件 – 4 GB。
- 内存：1 GB。
- 处理器要求：2.4 GHz 四核处理器。

- 运行 Windows Embedded 7、Windows Embedded 8 或 Windows Embedded 10 操作系统的设备的硬件要求：
  - 最低配置：
    - 磁盘空间要求：
      - 安装“应用程序启动控制”组件 – 50 MB。
      - 安装所有 Kaspersky Embedded Systems Security 组件 – 2 GB。
    - 内存：1 GB。
    - 处理器要求：1.4 Ghz 单核处理器英特尔奔腾 IV。
  - 推荐配置：
    - 磁盘空间要求：
      - 安装“应用程序启动控制”组件 – 2 GB。
      - 安装所有 Kaspersky Embedded Systems Security 组件 – 4 GB。
    - 内存：1 GB。
    - 处理器要求：2.4 GHz 四核处理器。
- 运行 Windows 7（64位）、Windows 8（64 位）、Windows 10（64 位） 或 Windows 11（64 位）操作系统的设备的硬件要求：
  - 最低配置：
    - 磁盘空间要求：
      - 安装“应用程序启动控制”组件 – 50 MB。
      - 安装所有 Kaspersky Embedded Systems Security 组件 – 2 GB。
    - 内存：
      - 1 GB，仅在运行 Microsoft Windows 操作系统的设备上安装“应用程序启动控制”组件。
      - 2 GB，执行所有组件的完整安装。
    - 处理器要求：1.4 Ghz 单核处理器英特尔奔腾 IV。
  - 推荐配置：
    - 磁盘空间要求：
      - 安装“应用程序启动控制”组件 – 2 GB。

        - 安装所有 Kaspersky Embedded Systems Security 组件 – 4 GB。
    - 内存：
        - 2 GB，仅在运行 Microsoft Windows 操作系统的设备上安装“应用程序启动控制”组件。
        - 4 GB，执行所有组件的完整安装。
    - 处理器要求：2.4 GHz 四核处理器。
- 运行 Windows 7（32位）、Windows 8（32 位） 或 Windows 10（32 位）操作系统的设备的硬件要求：
    - 最低配置：
        - 磁盘空间要求：
            - 安装“应用程序启动控制”组件 – 50 MB。
            - 安装所有 Kaspersky Embedded Systems Security 组件 – 2 GB。
        - 内存：
            - 256 MB，仅在运行 Microsoft Windows 操作系统的设备上安装“应用程序启动控制”组件。
            - 1 GB，执行所有组件的完整安装。
        - 处理器要求：
            - 32 位 Microsoft Windows 操作系统：

            1.4 GHz 单核处理器
            Intel Pentium III

            - 64 位 Microsoft Windows 操作系统：

            1.4 GHz 单核处理器
            Intel Pentium IV
    - 推荐配置：
        - 磁盘空间要求：
            - 安装“应用程序启动控制”组件 – 2 GB。
            - 安装所有 Kaspersky Embedded Systems Security 组件 – 4 GB。
        - 内存：1 GB。
        - 处理器要求：2.4 GHz 四核处理器。

功能要求和限制

本节介绍 Kaspersky Embedded Systems Security 组件的附加功能要求和现有限制。

安装和卸载

以下是安装和卸载限制列表：

- 为了让 Kaspersky Embedded Systems Security 正确运行，Windows 需要 SHA-2 支持。
- 安装应用程序时，如果 Kaspersky Embedded Systems Security 安装文件夹的指定路径长度超过 150 个字符，屏幕上可能会出现警告。该警告不影响安装过程：您可以正常安装并运行 Kaspersky Embedded Systems Security。
- 如果需要安装 SNMP 协议支持组件，倘若 SNMP 服务正在运行，请确保重新启动 SNMP 服务。
- 如果需要在运行嵌入式操作系统的设备上安装和运行 Kaspersky Embedded Systems Security，请确保安装“筛选管理器”组件。
- 无法通过 Microsoft Active Directory® 组策略安装 Kaspersky Embedded Systems Security 管理工具。
- 如果从已安装应用程序组件列表中排除反病毒保护节点，则该节点会在安装完成后从可用组件列表中消失。要安装反病毒保护节点的组件，请从安装包启动“安装向导”，因为安装包中包含完整的组件列表。
- 如果安装了 Kaspersky Embedded Systems Security 管理控制台，“安装向导”可能会提示重新启动计算机。在这种情况下，重启不是强制性的。结束安装管理控制台的用户的会话并再次登录系统即可。
- 如果您在运行无法接收定期更新的较旧操作系统的受保护设备上安装应用程序，请确保安装以下根证书：
  - DigiCert Assured ID Root CA
  - DigiCert_High_Assurance_EV_Root_CA
  - DigiCertAssuredIDRootCA

  如果未安装指定的根证书，应用程序可能无法正常运行。我们建议您尽快安装证书。

文件完整性监控

默认情况下，“文件完整性监控”不监控系统文件夹或文件系统清理文件的更改，以免有关操作系统不断执行的例程文件更改的信息混杂在任务报告中。您无法在监控范围中包含此类文件夹。

监控范围中排除以下文件夹和文件：

- 文件 id 从 0 到 33 的 NTFS 清理文件
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\

- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

应用程序会排除顶层文件夹。

该组件不监控绕过 ReFS/NTFS 文件系统的文件更改（通过 BIOS、LiveCD 等进行的文件更改）。

防火墙管理

以下是防火墙管理限制列表：

- 您应该指定多个地址，否则无法使用 IPv6。
- 预设的防火墙策略支持受保护设备与管理服务器之间的基本交互方案。要充分利用 Kaspersky Security Center 功能，您需要配置端口规则。您可以在 Kaspersky Security Center 知识库中找到有关端口号、协议及其功能的信息。
- 安装应用程序并为任务配置规则后，应用程序会在防火墙管理任务启动时控制 Windows 防火墙规则和规则组的修改。要更新状态并添加所需的规则，请确保重新启动防火墙管理任务。
- 当防火墙管理任务启动时，拒绝规则和监控传出流量的规则会自动从操作系统防火墙设置中删除。

其他限制

“按需扫描”和“实时文件保护”的限制：

- 不能扫描已连接的 MTP 设备。
- 如果没有 SFX 压缩文件扫描，压缩文件扫描不可用：如果 Kaspersky Embedded Systems Security 的保护设置中启用了压缩文件扫描，应用程序会自动扫描压缩文件和 SFX 压缩文件中的对象。如果没有压缩文件扫描，SFX 压缩文件扫描仍可用。
- 如果同时启用了“对启动进程的更深度分析(分析结束之前将阻止进程启动)”复选框和 KSN 使用服务，则任何接收 URL 网址作为参数的启动进程都将被阻止，即使选择了“仅统计”模式。为避免阻止此进程，请选择以下选项之一：
  - 禁用 KSN 使用服务
  - 禁用对启动进程的更深度分析(分析结束之前将阻止进程启动)复选框

  推荐选项：禁用“对启动进程的更深入分析”复选框

授权：

- 如果密钥使用 SUBST 命令创建，或者密钥文件的路径是网络路径，则无法通过安装向导使用密钥激活应用程序。
- 如果计划使用 Kaspersky Security Center 代理服务器在客户端设备上激活产品，请在安装 Kaspersky Security Center 网络代理时在此设备上禁用 VDI 优化。

更新：

- 默认情况下，应用程序图标在安装 Kaspersky Embedded Systems Security 关键模块更新后隐藏。
- 运行 Windows XP 或 Windows Server® 2003 操作系统的受保护设备不支持 KLRAMDISK。

界面：

- 在应用程序控制台中，隔离区、备份区、系统审核日志或任务日志中的过滤区分大小写。
- 在应用程序控制台中配置保护或扫描范围时，只能使用一个掩码，并且只能在路径末尾使用。以下是正确的掩码示例：“C:\Temp\Temp*”、“C:\Temp\Temp???.doc”和“C:\Temp\Temp*.doc”。此限制不影响信任区域的配置。

安全性：

- 如果操作系统的用户账户控制功能已启用，则用户账户必须属于 KAVWSEE 管理员组，才能通过双击任务栏通知区域中的应用程序图标来打开应用程序控制台。否则，需要以被允许打开小型诊断窗口或 Microsoft 管理控制台管理单元的用户身份登录。
- 如果启用了用户账户控制，则无法通过 Microsoft Windows 程序和功能窗口卸载应用程序。

与 Kaspersky Security Center 集成：

- 收到更新包后，管理服务器会先验证数据库更新，然后再将更新发送到网络上的受保护设备。管理服务器不验证软件模块更新。
- 当借助网络列表（隔离、备份）使用将动态数据传输到 Kaspersky Security Center 的组件时，确保在“与管理服务器交互”设置中选中所需复选框。

漏洞利用防御：

- 如果当前环境配置中未加载 apphelp.dll 库，则“漏洞利用防御”不可用。

- “漏洞利用防御”组件与运行 Microsoft Windows 10 操作系统的受保护设备上的 Microsoft EMET 实用程序不兼容：如果在安装了 EMET 的受保护设备上安装“漏洞利用防御”组件，Kaspersky Embedded Systems Security 会阻止 EMET。

- “漏洞利用防御”组件与 SQL Server® 2012 数据库引擎不兼容。如果在装有 MS SQL Server 2012 的计算机上安装 Kaspersky Embedded Systems Security，必须将数据库服务器的 sqlos.dll 库添加到“漏洞利用防御”任务的排除列表中。

安装和卸载应用程序

本节提供安装和卸载 Kaspersky Embedded Systems Security 的逐步说明。

适用于 Windows Installer 服务的 Kaspersky Embedded Systems Security 软件组件代码

\product_long_term\ess_x86.msi 和 \product_long_term\ess_x64.msi 文件旨在安装 Kaspersky Embedded Systems Security 的“使用默认拒绝技术保护计算机”配置，\product\ess_x86.msi 和 \product\ess_x64.msi 文件旨在安装 Kaspersky Embedded Systems Security 的“使用反病毒基础技术保护计算机”配置。

如果选择“使用反病毒基础技术保护计算机”配置，则默认包括除“防火墙管理”和“性能计数器”组件之外的所有 Kaspersky Embedded Systems Security 组件。

在不使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用反病毒基础技术保护计算机”配置时，将添加以下组件来自动扩展应用程序组件集：

- 实时文件保护
- 按需扫描
- 网络威胁防护

启用更新的组件不包括在“使用默认拒绝技术保护计算机”配置中。

如果选择“使用默认拒绝技术保护计算机”配置，则默认包含以下组件：

- Core
- 漏洞利用防御
- 应用程序启动控制
- 系统托盘图标

在使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用默认拒绝技术保护计算机”配置时，将删除以下组件来自动缩减应用程序组件集：

- 实时文件保护
- 按需扫描
- 启用更新的组件

建议使用此配置来保护资源有限的系统。在这种情况下，您可以长期激活应用程序，并且“应用程序启动控制”组件提供计算机保护。

\console\esstools_x86.msi 和 \console\esstools_x64.msi 文件安装“管理工具”集内的所有软件组件。

以下各节列出了适用于 Windows Installer 服务的 Kaspersky Embedded Systems Security 组件代码。您可以使用这些组件代码来定义从命令行安装 Kaspersky Embedded Systems Security 时要安装的组件列表。

Kaspersky Embedded Systems Security 软件组件

下表包含 Kaspersky Embedded Systems Security 软件组件的代码和描述。

Kaspersky Embedded Systems Security 软件组件的描述

组件	标识符	执行的功能
基本功能	Core	此组件包含基本应用程序功能集合并确保其操作。 如果在从命令行安装 Kaspersky Embedded Systems Security 时指定了其他 Kaspersky Embedded Systems Security 组件，但未指定核心组件，则核心组件被自动安装。
应用程序启动控制	AppCtrl	此组件监控用户尝试启动应用程序的情况，并根据指定的应用程序启动控制规则允许或拒绝应用程序启动。 它在“应用程序启动控制”任务中执行。
设备控制	DevCtrl	此组件跟踪将外部设备连接到受保护设备的尝试，并根据指定的设备控制规则允许或拒绝使用这些设备。 该组件在“设备控制”任务中实施。
反病毒保护	AVProtection	此组件提供反病毒保护并包含以下组件： • 按需扫描 • 实时文件保护 • 网络威胁防护
网络威胁防护	IDS	此组件扫描入站网络流量中是否存在典型网络攻击活动。在检测到以您的计算机为目标的网络攻击企图时，Kaspersky Embedded Systems Security 将阻止攻击计算机的网络活动。
按需扫描	Ods	此组件安装 Kaspersky Embedded Systems Security 系统文件，并提供按需扫描任务（根据请求扫描受保护设备上的对象）。
实时文件保护	Oas	此组件在受保护设备上的文件被访问时对这些文件执行病毒扫描。 其执行“实时文件保护”任务。
卡巴斯基安全网络使用	Ksn	此组件基于 Kaspersky 云技术提供保护。 它执行“KSN 使用”任务（向卡巴斯基安全网络服务发送请求及从该服务接收结论）。
文件完整性监控	Fim	此组件可记录指定监控范围内针对文件执行的操作。 该组件执行“文件完整性监控”任务。
注册表访问监控	RegMonitor	此组件可以监控使用任务设置中定义的监控范围内的特定注册表分支和注册表项执行的操作。 该组件可实现“注册表访问监控”。
漏洞利用防御	AntiExploit	此组件可管理设置，以便保护设备内存中的进程所使用的内存。
防火墙管理	Firewall	该组件使通过 Kaspersky Embedded Systems Security 图形用户界面管理 Windows 防火墙成为可能。 该组件执行防火墙管理任务。
用来与	AKIntegration	该组件在 Kaspersky Embedded Systems Security 和 Kaspersky

Kaspersky Security Center 网络代理进行集成的模块		Security Center 网络代理之间提供连接。 如果想通过 Kaspersky Security Center 管理应用程序，请在受保护设备上安装此组件。
日志审查	LogInspector	此组件根据 Windows 事件日志的审查结果，对受保护环境的完整性进行监控。
“系统监控器”性能计数器组	PerfMonCounters	此组件可安装一组系统监控器性能计数器。当 Kaspersky Embedded Systems Security 与其他程序一起使用时，性能计数器可以测量 Kaspersky Embedded Systems Security 的性能，并确定受保护设备上的潜在瓶颈。
SNMP 计数器和陷阱	SnmpSupport	此组件通过 Microsoft Windows 上的简单网络管理协议（SNMP）发布 Kaspersky Embedded Systems Security 计数器和陷阱。仅当 Microsoft SNMP 服务安装在同一受保护设备上时，此组件才能安装在受保护设备上。
通知区域中的 Kaspersky Embedded Systems Security 图标	TrayApp	此组件在受保护设备的任务托盘通知区域中显示 Kaspersky Embedded Systems Security 图标。Kaspersky Embedded Systems Security 图标显示设备保护的状态，可用于在 Microsoft 管理控制台（如果已安装）中打开 Kaspersky Embedded Systems Security 控制台以及“关于应用程序”窗口。

“管理工具”软件组件

下表包含“管理工具”软件组件的代码和说明。

“管理工具”软件组件说明

组件	代码	组件功能
Kaspersky Embedded Systems Security 管理单元	MmcSnapin	此组件通过 Kaspersky Embedded Systems Security 控制台安装用于管理应用程序的 Microsoft 管理控制台管理单元。 如果在从命令行安装“管理工具”过程中指定了其他组件，而未指定 MmcSnapin 组件，将自动安装该组件。

Kaspersky Embedded Systems Security 安装后的系统更改

当 Kaspersky Embedded Systems Security 和“管理工具”集（包括应用程序控制台）同时安装时，Windows Installer 服务将对受保护设备进行以下修改：

- 在受保护设备和安装了应用程序控制台的受保护设备上创建 Kaspersky Embedded Systems Security 文件夹。
- 注册 Kaspersky Embedded Systems Security 服务。
- 创建 Kaspersky Embedded Systems Security 用户组。
- 在系统注册表中注册 Kaspersky Embedded Systems Security 项。

下文介绍了这些更改。

受保护设备上的 Kaspersky Embedded Systems Security 文件夹

安装 Kaspersky Embedded Systems Security 后，受保护设备上会创建以下文件夹：

- Kaspersky Embedded Systems Security 默认安装文件夹，其中包含 Kaspersky Embedded Systems Security 可执行文件，具体取决于操作系统位集。因此，默认安装文件夹如下所示：
  - 在 32 位版本的 Microsoft Windows 中：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - 在 64 位版本的 Microsoft Windows 中：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security
- 管理信息库 (MIB) 文件，其中包含 Kaspersky Embedded Systems Security 通过 SNMP 协议发布的计数器和挂钩的说明：
  - %Kaspersky Embedded Systems Security%\mibs
- 64 位版本的 Kaspersky Embedded Systems Security 可执行文件（将仅在 64 位版本 Microsoft Windows 中安装 Kaspersky Embedded Systems Security 的过程中创建该文件夹）：
  - %Kaspersky Embedded Systems Security%\x64
- Kaspersky Embedded Systems Security 服务文件：
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Dskm

  对于 Windows XP，Kaspersky Lab 文件夹的路径为 %ALLUSERSPROFILE%\Application Data
- 具有更新源设置的文件：

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Update
- 使用“复制更新”任务下载的数据库和软件模块更新（该文件夹将在第一次使用“复制更新”任务下载更新时创建）。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Update\Distribution
- 任务日志和系统审核日志。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Reports
- 当前使用的数据库集。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Bases\Current
- 数据库的备份副本；每次更新数据库时都将覆盖这些副本。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Bases\Backup
- 在执行更新任务过程中创建的临时文件。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Bases\Temp
- 隔离的对象（默认文件夹）。

%ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Quarantine

- 备份中的对象（默认文件夹）。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Backup

- 从备份和隔离还原的对象（用于还原对象的默认的文件夹）。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Restored

在应用程序控制台安装过程中创建的文件夹

应用程序控制台默认安装文件夹，其中包含"管理工具"文件，具体取决于操作系统位集。因此，默认安装文件夹如下所示：

- 在 32 位版本的 Microsoft Windows 中：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
- 在 64 位版本的 Microsoft Windows 中：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

Kaspersky Embedded Systems Security 服务

以下 Kaspersky Embedded Systems Security 服务使用本地系统 (SYSTEM) 账户启动：

- Kaspersky Security 服务 (KAVFS) – 用于管理 Kaspersky Embedded Systems Security 任务和工作流的基本 Kaspersky Embedded Systems Security 服务。
- Kaspersky Security 管理服务 (KAVFSGT) – 此服务用于通过应用程序控制台管理 Kaspersky Embedded Systems Security 应用程序。
- Kaspersky Security 漏洞利用防御服务 (KAVFSSLP) - 用作将安全设置传输给外部安全代理并接收有关安全事件数据的媒介的服务。

Kaspersky Embedded Systems Security 组

"ESS 管理员"是受保护设备上的用户组，其中的用户对 Kaspersky Security 管理服务和所有 Kaspersky Embedded Systems Security 功能拥有完全访问权限。

系统注册表键

安装 Kaspersky Embedded Systems Security 后，将创建以下系统注册表项：

- Kaspersky Embedded Systems Security 的属性：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Kaspersky Embedded Systems Security 事件日志设置（Kaspersky 事件日志）：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Kaspersky Embedded Systems Security 管理服务的属性：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- 性能计数器设置：

- 在 32 位版本的 Microsoft Windows 中：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
- 在 64 位版本的 Microsoft Windows 中：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]

- SNMP 协议支持组件设置：
  - 在 32 位版本的 Microsoft Windows 中：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\SnmpAgent]
  - 在 64 位版本的 Microsoft Windows 中：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\SnmpAgent]
- Dump 文件设置：
  - 在 32 位版本的 Microsoft Windows 中：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\CrashDump]
  - 在 64 位版本的 Microsoft Windows 中：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\CrashDump]
- 跟踪文件设置：
  - 在 32 位版本的 Microsoft Windows 中：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\Trace]
  - 在 64 位版本的 Microsoft Windows 中：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\Trace]
- 应用程序的任务和功能的配置：
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\Environment]

Kaspersky Embedded Systems Security 进程

Kaspersky Embedded Systems Security 将启动下表中描述的进程。

Kaspersky Embedded Systems Security 进程

文件名	用途
kavfswp.exe	Kaspersky Embedded Systems Security 工作流
kavtray.exe	系统托盘图标的进程
kavfsmui.exe	小型诊断窗口组件的进程
kavshell.exe	命令行实用工具进程
kavfsrcn.exe	Kaspersky Embedded Systems Security 远程管理进程
kavfs.exe	Kaspersky Security 服务进程
kavfsgt.exe	Kaspersky Security 管理服务进程
kavfswh.exe	Kaspersky Security 漏洞利用防御服务进程

Windows Installer 服务的安装和卸载设置及命令行选项

本节包含安装和卸载 Kaspersky Embedded Systems Security 的设置的说明、这些设置的默认值、用于更改安装设置的键，以及这些设置的可能值。在从命令行安装 Kaspersky Embedded Systems Security 时，这些键可以和 Windows Installer 服务的 `msiexec` 命令的标准键一起使用。

Windows Installer 中的安装设置和命令行选项

- 接受最终用户授权许可协议的条款：您必须接受条款才能安装 Kaspersky Embedded Systems Security。

  `EULA=<值>` 命令行选项的可能值如下：

  - `0` - 拒绝最终用户授权许可协议条款（默认值）。
  - `1` - 接受最终用户授权许可协议条款。

- 接受隐私策略的条款：您必须接受条款才能安装 Kaspersky Embedded Systems Security。

  `PRIVACYPOLICY=<值>` 命令行选项的可能值如下：

  - `0` – 拒绝隐私策略条款（默认值）。
  - `1` – 接受隐私策略条款。

- 如果未安装 KB4528760 更新，允许安装 Kaspersky Embedded Systems Security。有关 KB4528760 更新的详细信息，请访问 Microsoft 网站。

  `SKIPCVEWINDOWS10=<值>` 命令行选项的可能值如下：

  - `0` – 如果未安装 KB4528760 更新，则取消安装 Kaspersky Embedded Systems Security（默认值）。
  - `1` – 如果未安装 KB4528760 更新，允许安装 Kaspersky Embedded Systems Security。

  > KB4528760 更新修复了 CVE-2020-0601 安全漏洞。有关 CVE-2020-0601 安全漏洞的详细信息，请访问 Microsoft 网站。

- 安装 Kaspersky Embedded Systems Security，并在更新期间恢复先前版本的定义设置。

  RESTOREDEFSETTINGS=<值> 命令行选项的可能值如下：

  - `0` – 更新期间将先前版本的所有数据传输到新版本（默认值）。
  - `1` – 在更新期间仅将包含激活数据和私钥的文件传输到新版本 ([drive]:\ProgramData\Kaspersky Lab\<产品>\<版本>\Data\product.dat)。先前版本的所有其他数据，例如设置、反病毒数据库、报告、隔离和备份对象，都将被删除。

- 安装 Kaspersky Embedded Systems Security ，并在更新期间保留先前版本的报告。

  KEEP_REPORTS=<值> 命令行选项的可能值如下：

  - `0` – 更新期间将先前版本的所有数据（报告除外）传输到新版本 ([drive]:\ProgramData\Kaspersky Lab\<产品>\<版本>\Reports)。报告已删除。

- 1 – 更新期间将先前版本的所有数据（如设置、反病毒数据库、报告、隔离和备份对象）传输到新版本（默认值）。

- 安装 Kaspersky Embedded Systems Security 并初步扫描活动进程和本地驱动器的引导扇区。

  PRESCAN=<值> 命令行选项的可能值如下：

  - 0 – 在安装过程中不执行对活动进程和本地驱动器引导扇区的初步扫描（默认值）。
  - 1 – 在安装过程中执行对活动进程和本地驱动器引导扇区的初步扫描。

- 安装过程中将保存 Kaspersky Embedded Systems Security 文件的目标文件夹。可以指定其他文件夹。

  INSTALLDIR=<文件夹的完整路径> 命令行选项的默认值如下：

  - Kaspersky Embedded Systems Security：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - 管理工具：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - 在 x64 位版本的 Microsoft Windows 中：%ProgramFiles(x86)%

- "实时文件保护"任务在 Kaspersky Embedded Systems Security 启动后立即启动。开启该设置可在 Kaspersky Embedded Systems Security 启动时启动"实时文件保护"（推荐）。

  EULA=<值> 命令行选项的可能值如下：

  - 1 – 启动（默认值）。
  - 0 – 不启动。

- 根据 Microsoft Corporation 的建议从保护范围中排除的对象。在"实时文件保护"任务中，从保护范围中排除设备上 Microsoft Corporation 推荐排除的对象。当反病毒应用程序拦截或修改受保护设备上某些应用程序使用的文件时，这些应用程序可能变得不稳定。例如，Microsoft Corporation 将某些域控制器应用程序包括在此类对象列表中。

  ADDMSEXCLUSION=<值> 命令行选项的可能值如下：

  - 1 – 排除（默认值）。
  - 0 – 不排除。

- 按照 Kaspersky 建议从保护范围中排除的对象。在"实时文件保护"任务中，从保护范围中排除设备上 Kaspersky 推荐排除的对象。

  ADDKLEXCLUSION=<值> 命令行选项的可能值如下：

  - 1 – 排除（默认值）。
  - 0 – 不排除。

- 允许远程连接到应用程序控制台。默认情况下，不允许远程连接到安装在受保护设备上的应用程序控制台。安装过程中，可允许连接。Kaspersky Embedded Systems Security 针对所有端口使用 TCP 协议为进程 kavfsgt.exe 创建允许规则。

  ALLOWREMOTECON=<值> 命令行选项的可能值如下：

  - 1 - 允许。
  - 0 – 拒绝（默认值）。

- 密钥文件的路径 (`LICENSEKEYPATH`
)

  。默认情况下，Windows Installer 会尝试在分发包的 \product 文件夹中查找扩展名为 .key 的文件。如果 \product 文件夹包含多个密钥文件，Windows Installer 将选择过期日期最晚的密钥文件。可以预先将密钥文件保存到 \product 文件夹中，也可以使用“**添加密钥**”设置为密钥文件指定其他路径。您可以在安装 Kaspersky Embedded Systems Security 后使用所选的管理工具（例如，应用程序控制台）添加密钥。如果您在应用程序安装期间未添加密钥，Kaspersky Embedded Systems Security 将不会发挥功能。

- 配置文件的路径。Kaspersky Embedded Systems Security 从在应用程序中创建的指定配置文件导入设置。Kaspersky Embedded Systems Security 不会从配置文件导入密码，例如用于启动任务的账户密码或用于连接代理服务器的密码。一旦导入设置，将要手动输入所有密码。如果未指定配置文件，安装后应用程序将开始使用默认设置。

  `CONFIGPATH=<配置文件名>` 的默认值未指定。

- “**在操作系统启动时扫描**”任务的模式 (SCANSTARTUP_BLOCKING)。如果您在没有 SCANSTARTUP_BLOCKING 密钥的安装模式下安装 Kaspersky Embedded Systems Security，则“**在操作系统启动时扫描**”任务会将以下参数分配给“**扫描范围**”设置：

  - **对受感染对象和其他对象执行的操作：仅通知**
  - **对疑似感染对象执行的操作：仅通知**

  如果您在使用 SCANSTARTUP_BLOCKING 密钥的安装模式下安装 Kaspersky Embedded Systems Security，则“**在操作系统启动时扫描**”任务会将以下参数分配给“**扫描范围**”设置：

  - **对受感染对象和其他对象执行的操作：执行推荐的操作**
  - **对疑似感染对象执行的操作：执行推荐的操作**

  在操作系统启动时扫描任务是自动创建的。默认情况下，应用“**仅通知**”模式。在这种情况下，在设备上部署 Kaspersky Embedded Systems Security 后，如果在扫描期间未发现系统服务问题，您可以启用“**在操作系统启动时扫描**”任务。如果应用程序将关键系统服务检测为受感染或可能受感染的对象，“**仅通知**”模式会让您有时间找出原因并解决问题。如果应用程序应用“**执行建议的操作**”模式，这将调用**清除。如果清除操作失败则删除**，清除或删除系统文件可能会导致操作系统启动出现严重问题。

- “为应用程序控制台启用网络连接”选项用于在另一台设备上安装 Kaspersky Embedded Systems Security 控制台。您可以从安装了 Kaspersky Embedded Systems Security 控制台的另一台设备远程管理设备保护。在 Microsoft Windows 防火墙中开放端口 135 (TCP)，允许通过网络连接到可执行文件 kavfsrcn.exe 以远程管理 Kaspersky Embedded Systems Security，并授予对 DCOM 应用程序的访问权限。安装完成后，将用户添加到“ESS 管理员”组中，以允许他们远程管理应用程序并允许通过网络连接到受保护设备上的 Kaspersky Security 管理服务（kavfsgt.exe 文件）。在另一台设备上安装 Kaspersky Embedded Systems Security 控制台后，您可以阅读有关其他配置的更多信息。

  `ADDWFEXCLUSION=<值>` 命令行选项的可能值如下：

  - `1` - 允许。
  - `0` – 拒绝（默认值）。

- 禁用不兼容软件检查。使用此设置，可在受保护设备上后台安装应用程序期间启用或禁用不兼容软件检查。无论此设置的值如何，在安装 Kaspersky Embedded Systems Security 期间，该应用程序始终警告受保护设备上安装的该应用程序的其他版本。

  `SKIPINCOMPATIBLESW=<值>` 命令行选项的可能值如下：

  - `0` - 执行不兼容软件检查（默认值）。

- 1 - 不执行不兼容软件检查。

Windows Installer 中的卸载设置和命令行选项

- 还原已隔离的对象。

  RESTOREQTN=<值> 命令行选项的可能值如下：

  - 0 – 删除隔离内容（默认值）。
  - 1 – 将隔离内容还原到 RESTOREPATH 参数指定的文件夹的 \Quarantine 子文件夹中。

- 还原备份内容。

  RESTOREBCK=<值> 命令行选项的可能值如下：

  - 0 – 删除备份内容（默认值）。
  - 1 – 将备份内容还原到 RESTOREPATH 参数指定的文件夹的 \Backup 子文件夹中。

- 输入当前密码以确认卸载（如果已启用密码保护）。

  UNLOCK_PASSWORD=<指定密码> 的默认值未指定。

- 还原对象的文件夹。还原的对象将保存到指定的文件夹。

  RESTOREPATH=<文件夹的完整路径> 命令行选项的默认值为 %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Restored

Kaspersky Embedded Systems Security 安装和卸载日志

如果使用安装（卸载）向导安装（卸载）Kaspersky Embedded Systems Security，Windows Installer 服务会创建安装（卸载）日志。一个名为 ess_v3.2_install_<uid>.log（其中 <uid> 是唯一的 8 字符日志标识符）的日志文件将保存在用于启动 setup.exe 文件的账户所属用户的 %temp% 文件夹中。

如果从“**修改或删除**”菜单运行应用程序控制台或 Kaspersky Embedded Systems Security 的“**修改或删除**”选项，将在 %temp% 文件夹中自动创建一个名为 ess_3.2_maintenance.log 的日志文件。

默认情况下，如果从命令行安装或卸载 Kaspersky Embedded Systems Security，将不会创建安装日志文件。

要安装 Kaspersky Embedded Systems Security 并在磁盘 C:\ 上创建日志文件：

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

安装计划

本节介绍 Kaspersky Embedded Systems Security 管理工具集，以及使用向导、命令行、使用 Kaspersky Security Center 和通过 Active Directory 组策略安装和卸载 Kaspersky Embedded Systems Security 的特殊方面。

在开始安装 Kaspersky Embedded Systems Security 前，请计划安装的主要阶段。

1. 确定管理和配置 Kaspersky Embedded Systems Security 所使用的管理工具。
2. 选择安装所需的应用程序组件。
3. 选择安装方法。

选择管理工具

确定将用于配置 Kaspersky Embedded Systems Security 设置和管理该应用程序的管理工具。可以使用应用程序控制台、命令行实用工具和 Kaspersky Security Center 管理控制台管理 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 控制台

Kaspersky Embedded Systems Security 控制台是添加到 Microsoft 管理控制台的独立管理单元。您可以通过安装在受保护设备或公司网络中其他设备上的应用程序控制台来管理 Kaspersky Embedded Systems Security。

您可以将多个 Kaspersky Embedded Systems Security 管理单元添加到在作者模式下打开的 Microsoft 管理控制台的单个副本中，以便用它来管理多台已安装 Kaspersky Embedded Systems Security 的设备的保护。

应用程序控制台包含在"管理工具"应用程序组件集内。

命令行实用工具

您可以从受保护设备的命令行管理 Kaspersky Embedded Systems Security。

命令行实用工具包含在 Kaspersky Embedded Systems Security 软件组件组中。

Kaspersky Security Center

如果 Kaspersky Security Center 用于公司设备反病毒保护的集中管理，您可以通过 Kaspersky Security Center 管理控制台管理 Kaspersky Embedded Systems Security。

必须安装以下组件：

- **用来与 Kaspersky Security Center 网络代理进行集成的模块**。该组件包含在 Kaspersky Embedded Systems Security 软件组件组中。它允许 Kaspersky Embedded Systems Security 与网络代理通信。将用来与 Kaspersky Security Center 网络代理进行集成的模块安装到受保护设备上。
- **Kaspersky Security Center 网络代理**。在每台受保护设备上安装该组件。该组件支持受保护设备上安装的 Kaspersky Embedded Systems Security 与 Kaspersky Security Center 管理控制台之间的交互。网络代理安装文件包含在 Kaspersky Security Center 分发包文件夹中。
- **Kaspersky Embedded Systems Security 3.2 管理插件**.此外，在安装了 Kaspersky Security Center 管理服务器的受保护设备上通过管理控制台安装管理插件，以便管理 Kaspersky Embedded Systems Security。此插件提供了通过 Kaspersky Security Center 进行应用程序管理的界面。管理插件安装文件 \product\klcfginst.exe 包含在 Kaspersky Embedded Systems Security 分发包中。

选择安装类型

指定 Kaspersky Embedded Systems Security 安装的软件组件后，您需要选择应用程序安装方法。

根据网络体系结构和以下状况选择安装方法：

- 是需要特殊的 Kaspersky Embedded Systems Security 安装设置，还是推荐的安装设置。
- 所有受保护设备的安装设置均相同，还是每台受保护设备使用特定的安装设置。

Kaspersky Embedded Systems Security 可以使用安装向导以互动方式安装，也可以在静默模式下，通过从命令行运行带安装设置的安装包文件进行安装，后者无需用户参与。使用 Active Directory 组策略或使用 Kaspersky Security Center 远程安装任务可对 Kaspersky Embedded Systems Security 执行集中远程安装。

Kaspersky Embedded Systems Security 可以在单台受保护设备上安装和配置，其设置保存到一个配置文件中；该文件随后可用于在其他受保护设备上安装 Kaspersky Embedded Systems Security。请注意，当使用 Active Directory 组策略安装应用程序时，此功能不存在。

启动安装向导

安装向导可以用于：

- 通过分发包中包含的 \product\setup.exe 文件在受保护设备上安装 Kaspersky Embedded Systems Security 组件。
- 通过分发包中的 \console\setup.exe 文件在受保护设备或其他 LAN 主机上安装 Kaspersky Embedded Systems Security 控制台。

从命令行以必要的安装设置运行安装包文件

如果不以任何命令行选项启动安装包文件，则 Kaspersky Embedded Systems Security 将以默认设置安装。可以使用 Kaspersky Embedded Systems Security 选项修改安装设置。

应用程序控制台可以安装在受保护设备和/或管理员工作站上。

您还可以使用示例命令安装 Kaspersky Embedded Systems Security 和应用程序控制台。

通过 Kaspersky Security Center 集中安装

如果 Kaspersky Security Center 在您的网络中的用途是管理网络设备的反病毒保护，则可以使用远程安装任务在多台设备上安装 Kaspersky Embedded Systems Security。

要使用 Kaspersky Security Center 安装 Kaspersky Embedded Systems Security 的受保护设备可以与 Kaspersky Security Center 在同一域中，也可以在不同的域中，或完全不在任何域中。

使用 Active Directory 组策略集中安装

可以使用 Active Directory 组策略在受保护设备上安装 Kaspersky Embedded Systems Security。应用程序控制台可以安装在受保护设备或管理员工作站上。

可以仅使用推荐的安装设置安装 Kaspersky Embedded Systems Security。

要通过 Active Directory 组策略安装 Kaspersky Embedded Systems Security 的受保护设备必须位于同一域和同一组织单元中。在登录 Microsoft Windows 前，在受保护设备启动时执行安装。

使用向导安装和卸载应用程序

本节介绍通过安装向导安装和卸载 Kaspersky Embedded Systems Security 和应用程序控制台，并包含有关 Kaspersky Embedded Systems Security 的附加配置以及要在安装后执行的操作的信息。

使用安装向导安装

以下各节包含有关安装 Kaspersky Embedded Systems Security 和应用程序控制台的信息。

要安装和继续使用 Kaspersky Embedded Systems Security：

1. 在受保护设备上安装 Kaspersky Embedded Systems Security。
2. 在您打算用来管理 Kaspersky Embedded Systems Security 的设备上安装应用程序控制台。
3. 如果应用程序控制台已经安装在网络中的其他设备上，而不是安装在受保护设备上，请执行附加配置以允许应用程序控制台用户远程管理 Kaspersky Embedded Systems Security。
4. 安装 Kaspersky Embedded Systems Security 后执行操作。

Kaspersky Embedded Systems Security 安装

在安装 Kaspersky Embedded Systems Security 之前，请执行以下操作：

1. 确保受保护设备上未安装其他反病毒程序。
2. 确保用来启动安装向导的账户属于受保护设备上的管理员组。

完成上述操作后，继续安装程序。按照安装向导说明，指定 Kaspersky Embedded Systems Security 的安装设置。可以在安装向导的任何一个步骤停止 Kaspersky Embedded Systems Security 安装过程。若要停止安装，请在安装向导窗口中单击“**取消**”按钮。

您可以阅读有关安装（卸载）设置的更多信息。

要使用安装向导安装 Kaspersky Embedded Systems Security：

1. 在受保护设备上启动 setup.exe 文件。
2. 在打开的窗口的“**安装**”部分中，单击“使用默认拒绝技术保护计算机”或“使用反病毒保护计算机”链接。

如果选择“使用反病毒基础技术保护计算机”配置，则默认包括除“防火墙管理”和“性能计数器”组件之外的所有 Kaspersky Embedded Systems Security 组件。

在不使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用反病毒基础技术保护计算机”配置时，将添加以下组件来自动扩展应用程序组件集：

- 实时文件保护
- 按需扫描
- 网络威胁防护

启用更新的组件不包括在“使用默认拒绝技术保护计算机”配置中。

如果选择“使用默认拒绝技术保护计算机”配置，则默认包含以下组件：

- Core
- 漏洞利用防御
- 应用程序启动控制
- 系统托盘图标

在使用特征分析和反病毒数据库来保护计算机的应用程序版本上安装 Kaspersky Embedded Systems Security 的“使用默认拒绝技术保护计算机”配置时，将删除以下组件来自动缩减应用程序组件集：

- 实时文件保护
- 按需扫描
- 启用更新的组件

建议使用此配置来保护资源有限的系统。在这种情况下，您可以长期激活应用程序，并且“应用程序启动控制”组件提供计算机保护。

3. 在 Kaspersky Embedded Systems Security 安装向导的欢迎页面，单击“**下一步>**”按钮。

   将打开“**最终用户授权许可协议和隐私策略**”窗口。

4. 查看授权许可协议和隐私策略的条款。

5. 如果您同意最终用户授权许可协议和隐私策略的条款和条件，请选中“**我确认我已完全阅读、理解并接受此最终用户授权许可协议的条款和条件**”和**我知道并同意，我的数据将按照隐私策略中的规定进行处理和传输（包括传输到第三国家和地区）。 我确认我已完全阅读并理解了隐私策略**。

   如果您不接受最终用户授权许可协议和/或隐私策略，安装将中止。

6. 单击“**下一步>**”按钮。

   将打开“**自定义安装**”窗口。

7. 选择要安装的组件。

仅在受保护设备上已安装 Microsoft Windows SNMP 服务时，Kaspersky Embedded Systems Security 的“SNMP 协议支持”组件才会出现在推荐安装的组件列表中。

8. 若要取消所有更改，请在“**自定义安装**”窗口中单击“**重置**”按钮。单击“**下一步>**”按钮。
9. 在“**选择目标文件夹**”窗口中：
   - 如果需要，指定 Kaspersky Embedded Systems Security 文件将复制到的文件夹。
   - 如果需要，单击“**磁盘**”按钮查看有关本地驱动器上可用空间的信息。

   单击“**下一步>**”按钮。
10. 在“**高级安装设置**”窗口中，配置以下安装设置：
    - **安装应用程序后启用实时保护**。
    - **将 Microsoft 推荐的文件添加到排除列表**。
    - **将卡巴斯基推荐的文件添加到排除列表**

      单击“**下一步>**”按钮。
11. 在“**从配置文件导入设置**”窗口中：
    a. 指定配置文件以从在任何先前兼容版本的应用程序中创建的现有配置文件导入 Kaspersky Embedded Systems Security 设置。
    b. 单击“**下一步>**”按钮。
12. 在“**激活应用程序**”窗口中，执行下列操作之一：
    - 如果您想要激活应用程序，请指定 Kaspersky Embedded Systems Security 密钥文件以激活应用程序。
    - 如果您想要稍后激活应用程序，请单击“**下一步>**”按钮。
    - 如果密钥文件先前已保存在分发包的 \product 文件夹中，该文件的名称将显示在“**密钥**”字段中。

      若要使用存储在其他文件夹的密钥文件添加密钥，请指定密钥文件。

      添加密钥文件后，窗口中将显示授权许可信息。Kaspersky Embedded Systems Security 会显示计算出的授权许可过期日期。授权许可期限从您添加密钥开始生效，在不迟于密钥文件过期日期前失效。

      单击“**下一步>**”按钮在应用程序中应用密钥文件。
13. 在“**已准备好安装**”窗口中单击“**安装**”按钮。向导将开始安装 Kaspersky Embedded Systems Security 组件。
14. 安装完成后将打开“**安装完成**”窗口。
15. 选中“**查看发布说明**”复选框，在安装向导结束后查看有关发布的信息。
16. 单击“**完成**”。

安装向导关闭。安装完成后，如果已添加激活密钥，即可使用 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 控制台安装

按照安装向导说明配置应用程序控制台的安装设置。可以在安装向导的任何一个步骤停止安装过程。若要停止安装，请在安装向导窗口中单击“**取消**”按钮。

要安装应用程序控制台：

1. 确保用来运行安装向导的账户属于设备上的管理员组。
2. 在受保护设备上运行 setup.exe 文件。
   将打开欢迎窗口。
3. 单击“**安装 Kaspersky Embedded Systems Security 控制台**”链接。
   将打开“安装向导”欢迎窗口。
4. 单击“**下一步>**”按钮。
5. 在打开的窗口中，查看最终用户授权许可协议和隐私策略的条款，然后选中“**我确认我已完全阅读、理解并接受此最终用户授权许可协议的条款和条件**”标题下的复选框以继续安装。
6. 单击“**下一步>**”按钮。
   将打开“**高级安装设置**”窗口。
7. 在“**高级安装设置**”窗口中：
   - 如果希望使用应用程序控制台来管理安装在远程设备上的 Kaspersky Embedded Systems Security，请选中“**允许远程访问**”复选框。
   - 要打开“**自定义安装**”窗口并选择组件：
     a. 单击“**高级**”按钮。
        将打开“**自定义安装**”窗口。
     b. 从列表中选择“管理工具”组件。
        默认情况下，安装所有组件。
     c. 单击“**下一步>**”按钮。

   您可以找到有关 Kaspersky Embedded Systems Security 组件的更多详细信息。

8. 在“**选择目标文件夹**”窗口中：
   a. 如果需要，指定要安装的文件应保存到的其他文件夹。
   b. 单击“**下一步>**”按钮。
9. 在“**已准备好安装**”窗口中单击“**安装**”按钮。
   安装向导将开始安装选定的组件。
10. 单击“**完成**”。

安装向导关闭。将在受保护设备上安装应用程序控制台。

如果"管理工具"集已安装在网络中除受保护设备以外的任何设备上，请配置高级设置。

在其他设备上安装应用程序控制台以后的高级设置

如果应用程序控制台已经安装在网络中的其他设备上，而不是安装在受保护设备上，请执行以下操作，以允许用户远程管理 Kaspersky Embedded Systems Security：

- 在受保护设备上将 Kaspersky Embedded Systems Security 用户添加到 ESS 管理员组中。
- 如果受保护设备使用 Windows 防火墙或第三方防火墙，则允许 Kaspersky Security 管理服务 (kavfsgt.exe) 的网络连接。
- 如果在运行 Microsoft Windows 的设备上安装应用程序控制台期间未选中"**允许远程访问**"复选框，则通过设备的防火墙手动允许应用程序控制台的网络连接。

远程设备上的应用程序控制台使用 DCOM 协议从受保护设备上的 Kaspersky Security 管理服务接收关于 Kaspersky Embedded Systems Security 事件的信息（如对象扫描、任务完成等）。需要在"Windows 防火墙设置"中允许应用程序控制台的网络连接，才能在应用程序控制台和 Kaspersky Security 管理服务之间建立连接。

在安装了应用程序控制台的远程设备上，执行以下操作：

- 确保允许远程匿名访问 COM 应用程序（但不是远程启动和激活 COM 应用程序）。
- 在 Windows 防火墙中开放 TCP 端口 135 并允许 Kaspersky Embedded Systems Security 远程管理进程的可执行文件 kavfsrcn.exe 的网络连接。

  安装应用程序控制台的设备将使用 TCP 端口 135 访问受保护设备并接收响应。
- 配置 Windows 防火墙的出站规则以允许连接。

  与单个协议具有固定端口的传统 TCP/IP 和 UDP/IP 服务不同，DCOM 会为远程 COM 对象动态分配端口。如果客户端（其中安装了应用程序控制台）与 DCOM 端点（受保护设备）之间存在防火墙，则必须开放很大范围的端口。

配置任何其他软件或硬件防火墙应该应用相同步骤。

如果在配置受保护设备与安装了应用程序控制台的设备之间的连接时，应用程序控制台处于打开状态：

1. 关闭应用程序控制台。
2. 等待至 Kaspersky Embedded Systems Security 远程管理进程 kavfsrcn.exe 结束。
3. 重新启动应用程序控制台。

   将应用新的连接设置。

允许匿名远程访问 COM 应用程序

设置的名称可能有所不同，具体取决于安装的 Windows 操作系统。

要允许匿名远程访问 COM 应用程序：

1. 在安装了 Kaspersky Embedded Systems Security 控制台的远程设备上，打开组件服务控制台。
2. 选择“**开始**” → “**运行**”。
3. 输入命令 `dcomcnfg`。
4. 单击“**确定**”。
5. 展开受保护设备上**组件服务控制台**中的“**计算机**”节点。
6. 打开“**我的计算机**”节点的上下文菜单。
7. 选择“**属性**”。
8. 在“**属性**”窗口的“**COM 安全**”选项卡上，单击“**访问权限**”设置组中的“**编辑限制**”按钮。
9. 请确保在“**允许远程访问**”窗口中为“匿名登录”用户选中“**允许远程访问**”复选框。
10. 单击“**确定**”。

允许 Kaspersky Embedded Systems Security 远程管理进程的网络连接

设置的名称可能有所不同，具体取决于安装的 Windows 操作系统。

要在 Windows 防火墙中开放 TCP 端口 135 并允许 Kaspersky Embedded Systems Security 远程管理进程的网络连接：

1. 关闭远程设备上的 Kaspersky Embedded Systems Security 控制台。
2. 执行以下步骤之一：
   - 在 Microsoft Windows XP SP2 或更高版本中：
     a. 选择“**开始** > **Windows 防火墙**”。
     b. 在“**Windows 防火墙**”窗口（或“Windows 防火墙设置”）中，单击“**排除**”选项卡上的“**添加端口**”按钮。
     c. 在“**名称**”字段中指定端口名称 RPC (TCP/135) 或输入其他名称，例如“Kaspersky Embedded Systems Security DCOM”，并在“**端口名称**”字段中指定端口号 (135)。
     d. 选择“**TCP**”协议。
     e. 单击“**确定**”。
     f. 单击“**排除**”选项卡上的“**添加**”按钮。
   - 在 Microsoft Windows 7 或更高版本中：
     a. 选择“**开始**” > “**控制面板**” > “**Windows 防火墙**”。

b. 在“**Windows 防火墙**”窗口中，选择“**允许程序或功能通过 Windows 防火墙**”。

c. 在“**允许程序通过 Windows 防火墙通信**”窗口中单击“**允许其他程序**”按钮。

3. 在“**添加程序**”窗口中指定 kavfsrcn.exe 文件。该文件位于在使用 Microsoft 管理控制台安装 Kaspersky Embedded Systems Security 控制台的过程中指定的目标文件夹中。

4. 单击“**确定**”。

5. 在“**Windows 防火墙（Windows 防火墙设置）**”窗口中，单击“**确定**”按钮。

添加 Windows 防火墙的出站规则

设置的名称可能有所不同，具体取决于安装的 Windows 操作系统。

要为 Windows 防火墙添加出站规则：

1. 选择“**开始**” > “**控制面板**” > “**Windows 防火墙**”。

2. 在“**Windows 防火墙**”窗口中，单击“**高级设置**”链接。
将打开“**高级安全 Windows 防火墙**”窗口。

3. 选择“**出站规则**”子节点。

4. 在“**操作**”窗格中单击“**新建规则**”选项。

5. 在打开的“**新建出站规则向导**”窗口中，选择“**端口**”选项，然后单击“**下一步**”。

6. 选择“**TCP**”协议。

7. 在“**特定远程端口**”字段中，指定以下允许传出连接的端口范围：1024-65535。

8. 在“**操作**”窗口中，选择“**允许连接**”选项。

9. 保存新规则，然后关闭“**高级安全 Windows 防火墙**”窗口。

Windows 防火墙现在将允许应用程序控制台与 Kaspersky Security 管理服务之间进行网络连接。

在安装 Kaspersky Embedded Systems Security 后执行的操作

如果您已激活 Kaspersky Embedded Systems Security，该应用程序会在安装后立即启动保护和扫描任务。如果在安装 Kaspersky Embedded Systems Security 期间选中“**安装应用程序后启用实时保护**”（默认选项），当设备的文件系统对象被访问时，应用程序会扫描这些对象。Kaspersky Embedded Systems Security 将在每个星期五的 20:00 运行“关键区域扫描”任务。

推荐在安装 Kaspersky Embedded Systems Security 后执行下列步骤：

- 启动应用程序数据库更新任务。安装后 Kaspersky Embedded Systems Security 将使用应用程序分发包中的数据库扫描对象。

我们推荐立即更新 Kaspersky Embedded Systems Security 数据库，因为它们可能已过期。

然后，应用程序将根据任务中配置的默认计划每小时更新一次数据库。

- 如果安装 Kaspersky Embedded Systems Security 之前受保护设备上未安装任何具有实时文件保护的反病毒软件，请在设备上运行“关键区域扫描”。
- 配置有关 Kaspersky Embedded Systems Security 事件的管理员通知。

启动和配置 Kaspersky Embedded Systems Security 数据库更新任务

要在安装后更新应用程序数据库：

1. 在“数据库更新”任务设置中，配置与更新源的连接 – Kaspersky HTTP 或 FTP 更新服务器。
2. 启动“数据库更新”任务。

您的网络中可能未配置 Web 代理自动发现协议 (WPAD) 以在 LAN 中自动检测代理服务器设置。而且，在访问代理服务器时，您的网络可能需要身份验证。

要为访问代理服务器指定可选的代理服务器设置和身份验证设置：

1. 打开“**Kaspersky Embedded Systems Security**”节点的上下文菜单。
2. 选择“**属性**”项。
   将打开“**应用程序设置**”窗口。
3. 选择“**连接设置**”选项卡。
4. 在“**代理服务器设置**”部分中，选中“**使用指定的代理服务器**”复选框。
5. 在“**地址**”字段中输入代理服务器地址，在“**端口**”字段中输入代理服务器的端口号。
6. 在“**代理服务器身份验证设置**”部分的下拉列表中选择必要的身份验证方法：
   - **使用 NTLM 身份验证**，如果代理服务器支持内置的 Microsoft Windows NTLM 身份验证。Kaspersky Embedded Systems Security 将使用在该任务设置中指定的用户账户访问代理服务器（默认情况下，该任务将在**本地系统 (SYSTEM)** 用户账户下运行）。
   - **使用带用户名和密码的 NTLM 身份验证**，如果代理服务器支持内置的 Microsoft Windows NTLM 身份验证。Kaspersky Embedded Systems Security 将使用指定的账户来访问代理服务器。输入用户名和密码，或从列表中选择用户。
   - **应用用户名和密码**，以选择基本身份验证。输入用户名和密码，或从列表中选择用户。
7. 在“**应用程序设置**”窗口中单击“**确定**”。

要配置与 Kaspersky 的更新服务器的连接，在“数据库更新”任务中：

1. 通过以下方式之一启动应用程序控制台：

- 在受保护设备上打开应用程序控制台。要执行此操作，请选择“开始” > “所有程序” > “Kaspersky Embedded Systems Security” > “管理工具” > “Kaspersky Embedded Systems Security 3.2 控制台”。
- 如果应用程序控制台已在不受保护的设备上启动，请连接到受保护设备：

  a. 在应用程序控制台树中打开“Kaspersky Embedded Systems Security”节点的上下文菜单。

  b. 选择“连接至其他计算机”项。

  c. 在“选择受保护设备”窗口中，选择“其他设备”，然后在文本字段中，指定受保护设备的网络名称。

  如果用于登录 Microsoft Windows 的账户没有 Kaspersky Security 管理服务的访问权限，请指示具有所需权限的账户。

将打开应用程序控制台窗口。

2. 在应用程序控制台树中，展开“更新”节点。
3. 选择“数据库更新”子节点。
4. 在结果窗格中单击“属性”链接。
5. 在打开的“任务设置”窗口中，打开“连接设置”选项卡。
6. 选中“使用代理服务器设置连接至 卡巴斯基更新服务器”。
7. 在“任务设置”窗口中单击“确定”。

将保存“数据库更新”任务中连接更新源的设置。

要运行“数据库更新”任务，请执行下列操作：

1. 在应用程序控制台树中，展开“更新”节点。
2. 在“数据库更新”子节点的上下文菜单中，选择“启动”项。

“数据库更新”任务启动。

成功完成该任务后，您可以在 Kaspersky Embedded Systems Security 节点的结果窗格中查看安装的最新数据库更新的发布日期。

关键区域扫描

更新 Kaspersky Embedded Systems Security 数据库后，使用“关键区域扫描”任务扫描受保护设备是否存在恶意软件。

要运行“关键区域扫描”任务：

1. 在应用程序控制台树中展开“按需扫描”节点。
2. 在“关键区域扫描”子节点的上下文菜单中，选择“启动”命令。

任务启动；结果窗格中显示任务状态“正在运行”。

要查看任务日志，请执行下列操作：

在“**关键区域扫描**”节点的结果窗格中，单击“**打开任务日志**”链接。

修改组件集和修复 Kaspersky Embedded Systems Security

可以添加或删除 Kaspersky Embedded Systems Security 组件。您需要先停止“实时文件保护”任务，才能删除“实时文件保护”组件。其他情况下，无需停止实时文件保护任务或 Kaspersky Security 服务。

如果应用程序管理受密码保护，Kaspersky Embedded Systems Security 会在您在安装向导中尝试删除组件或修改组件集时请求密码。

要修改 Kaspersky Embedded Systems Security 组件集：

1. 在“**开始**”菜单中，选择“**所有程序**” > “**Kaspersky Embedded Systems Security**” > “**修改或删除 Kaspersky Embedded Systems Security**”。

   将打开安装向导的“**修复或卸载安装**”窗口。

2. 选择“**修改组件集**”。单击“**下一步>**”按钮。

   将打开“**自定义安装**”窗口。

3. 在“**自定义安装**”窗口的可用组件列表中，选择要从 Kaspersky Embedded Systems Security 添加或删除的组件。为此，请执行以下操作：

   - 要更改组件集，请单击所选组件名称旁边的按钮。然后在上下文菜单中选择：
     - “**组件将被安装在本地硬盘上**”（如果您想要安装一个组件）；
     - “**程序将在本地硬盘上安装组件及其子组件**”（如果您想要安装一组组件）。
   - 要删除先前安装的组件，请单击所选组件名称旁边的按钮。然后在上下文菜单中选择“**组件将变为不可用**”。

   单击“**下一步>**”按钮。

4. 在“**已准备好安装**”窗口中，通过单击“**安装**”按钮确认软件组件集的更改。

5. 在安装完成后打开的窗口中，单击“**确定**”按钮。

将根据指定设置修改 Kaspersky Embedded Systems Security 组件集。

如果在 Kaspersky Embedded Systems Security 运行期间出现问题（Kaspersky Embedded Systems Security 崩溃；任务崩溃或无法启动），可以对 Kaspersky Embedded Systems Security 执行修复。您可在保存 Kaspersky Embedded Systems Security 的当前设置时执行修复，或选择一个选项以将所有 Kaspersky Embedded Systems Security 设置重置为默认值。

要在应用程序或任务崩溃后修复 Kaspersky Embedded Systems Security：

1. 在“**开始**”菜单中，选择“**所有程序**”。

2. 选择“**Kaspersky Embedded Systems Security**”。

3. 选择“**修改或删除 Kaspersky Embedded Systems Security**”。
   将打开安装向导的“**修复或卸载安装**”窗口。

4. 选择“**修复已安装组件**”。单击“**下一步>**”按钮。
   这会打开“**修复已安装组件**”窗口。

5. 在“**修复已安装组件**”窗口中，如果您希望重置应用程序设置并使用其默认设置还原 Kaspersky Embedded Systems Security，则选中“**恢复推荐的应用程序设置**”复选框。单击“**下一步>**”按钮。

6. 在“**准备进行修复**”窗口中，通过单击“**安装**”按钮确认修复操作。

7. 在修复操作完成后打开的窗口中，单击“**确定**”按钮。

将使用指定设置修复 Kaspersky Embedded Systems Security。

使用安装向导卸载

本节包含有关使用安装/卸载向导从受保护设备上删除 Kaspersky Embedded Systems Security 和应用程序控制台的说明。

Kaspersky Embedded Systems Security 卸载

卸载 Kaspersky Embedded Systems Security 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

在不同 Windows 操作系统中，设置的名称可能有所不同。

可以使用安装/卸载向导从受保护设备卸载 Kaspersky Embedded Systems Security。

从受保护设备卸载 Kaspersky Embedded Systems Security 后，可能需要重新启动计算机。重启可以推迟。

如果操作系统使用 UAC 功能（用户账户控制）或对应用程序的访问受密码保护，则不能通过 Windows 控制面板卸载、修复和安装应用程序。

如果应用程序管理受密码保护，Kaspersky Embedded Systems Security 会在您在安装向导中尝试删除组件或修改组件集时请求密码。

要卸载 Kaspersky Embedded Systems Security：

1. 在“**开始**”菜单中，选择“**所有程序**”。

2. 选择“**Kaspersky Embedded Systems Security**”。

3. 选择“**修改或删除 Kaspersky Embedded Systems Security**”。
   将打开安装向导的“**修复或卸载安装**”窗口。

4. 选择“**删除软件组件**”。单击“**下一步>**”按钮。
   将打开“**高级应用程序卸载设置**”窗口。

5. 如有必要，在“**高级应用程序卸载设置**”窗口中：

   a. 选中“**导出隔离对象**”复选框，以从 Kaspersky Embedded Systems Security 隔离区导出对象。默认取消选中该复选框。

   b. 选中“**导出备份对象**”复选框，以从 Kaspersky Embedded Systems Security 备份区导出对象。默认取消选中该复选框。

   c. 单击“**保存到**”按钮并选择您希望将对象导出到的文件夹。默认情况下，会将对象导出到 %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall。
      单击“**下一步>**”按钮。

6. 在“**已准备好卸载**”窗口中，通过单击“**卸载**”按钮确认卸载。

7. 在卸载完成后打开的窗口中，单击“**确定**”按钮。

Kaspersky Embedded Systems Security 将从受保护设备卸载。

Kaspersky Embedded Systems Security 控制台卸载

> 在不同 Windows 操作系统中，设置的名称可能有所不同。

您可以使用安装/卸载向导，从受保护设备卸载应用程序控制台。

卸载应用程序控制台后，无需重新启动受保护设备。

要卸载应用程序控制台，请执行下列步骤：

1. 在“**开始**”菜单中，选择“**所有程序**”。

2. 选择“**Kaspersky Embedded Systems Security**”。

3. 选择“**修改或删除 Kaspersky Embedded Systems Security**”。
   将打开向导的“**修复或卸载安装**”窗口。

4. 选择“**删除软件组件**”并单击“**下一步>**”按钮。

5. 将打开“**已准备好卸载**”窗口。单击“**卸载**”按钮。
   将打开“**卸载完成**”窗口。

6. 单击“**确定**”。

此时，卸载完成，且安装向导关闭。

从命令行安装和卸载应用程序

本节介绍了从命令行安装和卸载 Kaspersky Embedded Systems Security 的详细信息，包含从命令行安装和卸载 Kaspersky Embedded Systems Security 的命令的示例，以及从命令行添加和移除 Kaspersky Embedded Systems Security 组件的命令的示例。

关于从命令行安装和卸载 Kaspersky Embedded Systems Security

卸载 Kaspersky Embedded Systems Security 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

在使用密钥指定安装设置后，可以从命令行运行 \product\ess_x86.msi 或 \product\ess_x64.msi 安装包文件，来安装或卸载 Kaspersky Embedded Systems Security，以及添加或删除其组件。

“管理工具”集可以安装在受保护设备或网络上的其他设备上，以便在本地或远程与应用程序控制台配合使用。若要执行该操作，请使用 \console\esstools.msi 安装包。

在安装了该应用程序的受保护设备上，使用包含在管理员组中的账户执行安装。

如果在没有附加密钥的受保护设备上运行 \product\ess_x86.msi 或 \product\ess_x64.msi 文件，将使用推荐的安装设置安装 Kaspersky Embedded Systems Security。

您可以使用 ADDLOCAL 命令行选项，并列出选定组件或组件集的代码，来分配要安装的组件集。

安装 Kaspersky Embedded Systems Security 的命令示例

本节提供安装 Kaspersky Embedded Systems Security 所使用的命令示例。

在运行 32 位版本的 Microsoft Windows 的受保护设备上，运行分发包中带有 x86 后缀的文件。在运行 64 位版本的 Microsoft Windows 的受保护设备上，运行分发包中带有 x64 后缀的文件。

有关使用 Windows Installer 标准命令和命令行选项的详细信息，提供在 Microsoft 提供的文档中。

从 setup.exe 文件安装 Kaspersky Embedded Systems Security 的示例

若要在无需与用户互动的情况下使用推荐的安装设置安装 Kaspersky Embedded Systems Security，请运行以下命令：

```
\product\setup.exe /s /p EULA=1 /p PRIVACYPOLICY=1
```

您可以使用以下设置安装 Kaspersky Embedded Systems Security：

- 仅安装“实时文件保护”和“按需扫描”组件
- 在启动 Kaspersky Embedded Systems Security 时不运行“实时文件保护”
- 不排除 Microsoft Corporation 建议从扫描范围中排除的文件

要安装"设备控制"等组件，请运行以下命令：

```
\product\setup.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

当您在具有安装 <RPODUCT_NAME_NOM_FULL> 后会导致系统故障的网络设备和 SCSI 设备的计算机上安装 Kaspersky Embedded Systems Security 时，可以将以下可选密钥与此命令一起使用：

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

启用 (1) 或禁用 (0) 网络适配器连接拦截。

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>`

启用 (1) 或禁用 (0) SCSI 适配器连接拦截。

用于安装的命令列表：运行 .msi 文件

若要在无需与用户互动的情况下使用推荐的安装设置安装 Kaspersky Embedded Systems Security，请运行以下命令：

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

若要使用推荐的安装设置安装 Kaspersky Embedded Systems Security 并显示安装界面，请运行以下命令：

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

要使用推荐的安装设置安装 Kaspersky Embedded Systems Security，并在达到定义的最大跟踪文件数后启用跟踪文件轮换，请运行以下命令：

```
msiexec /i ess.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1
PRIVACYPOLICY=1
```

请注意，`TRACE_FOLDER` 是必需参数。

为 `TRACE_MAX_ROLL_COUNT` 参数引入了以下条件：

- 如果指定了该参数，则使用您定义的最大跟踪文件数启用跟踪文件轮换。可用值范围：1 到 999。
- 如果参数指定 0 作为最大跟踪文件数的值，则禁用跟踪文件轮换。
- 如果指定了该参数，并且最大跟踪文件数的值无效或超过 1-999 个文件的允许范围，则使用默认值 5 作为最大跟踪文件数来启用跟踪文件轮换。
- 如果未指定参数：
  - 如果设备上已配置跟踪文件轮换，则设置保持不变。您输入的参数将被应用程序忽略。
  - 如果设备上尚未配置跟踪文件轮换，则使用默认值 5 作为最大跟踪文件数来启用跟踪文件轮换。

若要安装 Kaspersky Embedded Systems Security 并使用密钥文件 C:\0000000A.key 激活：

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

若要安装 Kaspersky Embedded Systems Security 并初步扫描活动进程和本地驱动器的引导扇区，请运行以下命令：

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

要将 Kaspersky Embedded Systems Security 安装在安装文件夹 C:\ESS 中，请运行以下命令：

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

若要安装 Kaspersky Embedded Systems Security 并将名为 ess.log 的安装日志文件保存在存储 Kaspersky Embedded Systems Security msi 文件的文件夹中，请运行以下命令：

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

若要安装 Kaspersky Embedded Systems Security 控制台，请运行以下命令：

```
msiexec /i esstools.msi /qn EULA=1
```

若要安装 Kaspersky Embedded Systems Security 并使用密钥文件 C:\0000000A.key 激活，并且根据配置文件 C:\settings.xml 中的设置配置 Kaspersky Embedded Systems Security，请运行以下命令：

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1
PRIVACYPOLICY=1
```

若要在 Kaspersky Embedded Systems Security 受密码保护的情况下安装应用程序补丁，请运行以下命令：

```
msiexec /p "<msp 文件名及路径>" UNLOCK_PASSWORD=<密码>
```

在安装 Kaspersky Embedded Systems Security 后执行的操作

如果您已激活 Kaspersky Embedded Systems Security，该应用程序会在安装后立即启动保护和扫描任务。如果在安装 Kaspersky Embedded Systems Security 期间选中“**安装应用程序后启用实时保护**”选项，当设备的文件系统对象被访问时，应用程序会扫描这些对象。Kaspersky Embedded Systems Security 将在每个星期五的晚上 8 点运行“关键区域扫描”任务。

建议在安装 Kaspersky Embedded Systems Security 后执行下列步骤：

- 启动 Kaspersky Embedded Systems Security 数据库更新任务。安装后 Kaspersky Embedded Systems Security 将使用其分发包中的数据库扫描对象。建议立即更新 Kaspersky Embedded Systems Security 数据库。为此，您必须运行“数据库更新”任务。然后将根据默认计划，每小时更新一次数据库。

  例如，您可以通过运行以下命令来启动“数据库更新”任务：

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
  /PROXYPWD:123456
  ```

  在此情况下，将从 卡巴斯基更新服务器下载 Kaspersky Embedded Systems Security 数据库更新。与更新源的连接是通过代理服务器（代理服务器地址：proxy.company.com，端口：8080）使用内置的 Windows NTLM 身份验证以某个账户访问服务器来建立的（用户名：inetuser；密码：123456）。

- 如果安装 Kaspersky Embedded Systems Security 之前受保护设备上未安装任何具有实时文件保护的反病毒软件，请对设备运行“关键区域扫描”。

要使用命令行启动“关键区域扫描”任务：

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

此命令可将任务日志保存在当前文件夹内名为 scancritical.log 的文件中。

- 配置有关 Kaspersky Embedded Systems Security 事件的管理员通知。

添加/删除组件。命令示例

应用程序启动控制组件被自动安装。

要安装按需扫描组件，请运行以下命令：

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

或

```
\product\setup.exe /s /p ADDLOCAL=Oas,Ods
```

在您添加组件到列表后，Kaspersky Embedded Systems Security 重新安装现有组件并安装指定的组件。

要删除安装的组件，请运行以下命令：

```
msiexec /i ess.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

要安装新组件，请运行以下命令：

```
msiexec /i ess.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

您列出要安装和删除的组件后，Kaspersky Embedded Systems Security 会相应地安装和删除这些组件。

Kaspersky Embedded Systems Security 卸载。命令示例

要从受保护设备卸载 Kaspersky Embedded Systems Security，请运行以下命令：

```
msiexec /x ess.msi /qn
```

或

- 对于 32 位操作系统：
  ```
  msiexec /x {2CE8D225-8F60-49C9-82E3-C143D10D3CD4} /qn
  ```
- 对于 64 位操作系统：
  ```
  msiexec /x {86D803C7-215D-4B46-A726-ED5AF57FC05D} /qn
  ```

要卸载 Kaspersky Embedded Systems Security 控制台，请运行以下命令：

```
msiexec /x esstools.msi /qn
```

或

```
msiexec /x {71FB9E57-9F23-4D72-B762-E0314EF3C814} /qn
```

要从已启用密码保护的设备上卸载 Kaspersky Embedded Systems Security，请执行以下命令：

- 对于 32 位操作系统：
  ```
  msiexec /x {2CE8D225-8F60-49C9-82E3-C143D10D3CD4} UNLOCK_PASSWORD=*** /qn
  ```
- 对于 64 位操作系统：
  ```
  msiexec /x {86D803C7-215D-4B46-A726-ED5AF57FC05D} UNLOCK_PASSWORD=*** /qn
  ```

返回代码

下表包含了命令行返回代码的列表。

返回代码

代码	描述
1324	目标文件夹名称包含无效的字符。
25001	没有足够权限安装 Kaspersky Embedded Systems Security。要安装该应用程序，请使用本地管理员权限启动安装向导。
25003	Kaspersky Embedded Systems Security 不能安装在运行此版本的 Microsoft Windows 的设备上。请启动用于 64 位版本 Microsoft Windows 的安装向导。
25004	检测到不兼容的软件。要继续安装，请卸载以下软件：<不兼容软件列表>。
25010	指定的路径不能用于保存已隔离的对象。
25011	用于保存已隔离的对象的文件夹名包含无效的字符。
26251	无法下载性能计数器 DLL。
26252	无法下载性能计数器 DLL。
27300	不能安装驱动程序。
27301	不能卸载驱动程序。
27302	不能安装网络组件。已达到所支持的筛选设备的最大数量。
27303	无法找到反病毒数据库。

使用 Kaspersky Security Center 安装和卸载应用程序

本节包含有关通过 Kaspersky Security Center 安装 Kaspersky Embedded Systems Security 的常规信息。本节还介绍了如何通过 Kaspersky Security Center 安装和卸载 Kaspersky Embedded Systems Security 以及安装 Kaspersky Embedded Systems Security 后执行的操作。

有关通过 Kaspersky Security Center 安装的常规信息

您可以通过 Kaspersky Security Center，使用远程安装任务来安装 Kaspersky Embedded Systems Security。

完成远程安装任务后，将在多台受保护设备上使用相同的设置安装 Kaspersky Embedded Systems Security。

所有受保护设备可以组合到一个管理组中，并且可以创建组任务来在该组的受保护设备上安装 Kaspersky Embedded Systems Security。

您可以创建一个任务，在不属于相同管理组的一组受保护设备上远程安装 Kaspersky Embedded Systems Security。创建该任务时，您必须生成应安装 Kaspersky Embedded Systems Security 的各个受保护设备的列表。

有关远程安装任务的详细信息，请参见 *Kaspersky Security Center 帮助*。

安装或卸载 Kaspersky Embedded Systems Security 的权限

在除下述以外的所有情况下，在远程安装（删除）任务中指定的账户必须包含在每个受保护设备的管理员组中：

- 如果 Kaspersky Security Center 网络代理已安装在要安装 Kaspersky Embedded Systems Security 的受保护设备上（不论这些受保护设备位于哪个域，或它们是否属于任何域）。

  如果受保护设备上尚未安装网络代理，可以使用远程安装任务安装它和 Kaspersky Embedded Systems Security。在安装网络代理之前，请确保要在该任务中指定的账户包含在每台受保护设备的管理员组中。

- 要安装 Kaspersky Embedded Systems Security 的所有受保护设备都和管理服务器在同一个域中，且管理服务器以“**域管理员**”账户身份注册（如果该账户在该域的受保护设备上具有本地管理员的权限）。

默认情况下，在使用“**强制安装**”方法时，远程安装任务从运行管理服务器的账户运行。

在强制安装（卸载）模式下对多组受保护设备执行组任务或其他任务时，受保护设备上的账户必须具有以下权限：

- 远程执行应用程序的权限。
- **Admin$** 共享的权限。
- **作为服务登录**的权限。

通过 Kaspersky Security Center 安装 Kaspersky Embedded Systems Security

有关生成安装包和创建远程安装任务的详细信息，请参见《Kaspersky Security Center 实施指南》。

如果希望以后通过 Kaspersky Security Center 管理 Kaspersky Embedded Systems Security，请确保符合以下条件：

- 安装了 Kaspersky Security Center 管理服务器的受保护设备上还安装了管理插件（Kaspersky Embedded Systems Security 分发包中的 \product\klcfginst.exe 文件）。
- Kaspersky Security Center 网络代理安装在受保护设备上。如果 Kaspersky Security Center 网络代理未安装在受保护设备上，可以使用远程安装任务同时安装它和 Kaspersky Embedded Systems Security。

也可以将多台设备组合到一个管理组中，以便以后使用 Kaspersky Security Center 策略和组任务管理保护设置。

要使用远程安装任务安装 Kaspersky Embedded Systems Security：

1. 启动 Kaspersky Security Center 管理控制台。
2. 在 Kaspersky Security Center 中，展开“**高级**”节点。
3. 展开“**远程安装**”子节点。
4. 在“**安装包**”子节点的结果窗格中，单击“**创建安装包**”按钮。
5. 选择“**创建 Kaspersky 应用程序的安装包**”安装包类型。
6. 输入安装包名称。
7. 指定 Kaspersky Embedded Systems Security 分发包中的 ess.kud 文件为安装包文件。
   将打开“**最终用户授权许可协议和隐私策略**”窗口。
8. 如果您同意最终用户授权许可协议和隐私策略的条款和条件，请选中“**我确认我已完全阅读、理解并接受此最终用户授权许可协议的条款和条件**”和**我知道并同意，我的数据将按照隐私策略中的规定进行处理和传输（包括传输到第三国家和地区）。 我确认我已完全阅读并理解了隐私策略。**

   您必须接受授权许可协议和隐私策略才能继续。

9. 要更改要安装的 Kaspersky Embedded Systems Security 组件集以及安装包中的默认安装设置：
   a. 在 Kaspersky Security Center 中，展开“**远程安装**”节点。
   b. 在“**安装包**”子节点的结果窗格中，打开已创建的 Kaspersky Embedded Systems Security 安装包的上下文菜单，然后选择“**属性**”。
   c. 在“**属性：<安装包名称>**”窗口中打开“**设置**”部分。

      在“**要安装的组件**”设置组中，选中要安装的 Kaspersky Embedded Systems Security 组件名称旁边的复选框。

   d. 要指定默认文件夹以外的目标文件夹，请在“**目标文件夹**”字段指定文件夹名称和路径。
      目标文件夹的路径可以包含系统环境变量。如果该文件夹在受保护设备上不存在，将进行创建。
   e. 在“**高级安装设置**”组中，配置以下设置：
      - 安装前扫描受保护设备以检测病毒
      - 安装应用程序后启用实时保护
      - 将 **Microsoft** 推荐的文件添加到排除列表
      - 将卡巴斯基推荐的文件添加到排除列表
      - 启用在操作系统启动时延迟启动 **Kaspersky Security** 服务
   f. 在“**属性：<安装包名称>**”窗口中，单击“**确定**”。
10. 在“**安装包**”节点中，创建一个任务，在选定的受保护设备（管理组）上远程安装 Kaspersky Embedded Systems Security。配置任务设置。

要了解创建和配置远程安装任务的详细信息，请参见 *Kaspersky Security Center 帮助*。

11. 运行 Kaspersky Embedded Systems Security 远程安装任务。

Kaspersky Embedded Systems Security 将安装于在任务中指定的受保护设备上。

在安装 Kaspersky Embedded Systems Security 后执行的操作

安装 Kaspersky Embedded Systems Security 后，推荐更新设备上的 Kaspersky Embedded Systems Security 数据库，如果在安装 Kaspersky Embedded Systems Security 之前，设备上未安装启用实时保护功能的反病毒应用程序，则还推荐对设备执行关键区域扫描。

如果安装了 Kaspersky Embedded Systems Security 的受保护设备在 Kaspersky Security Center 中属于同一个管理组，您可以使用以下方法执行这些任务：

1. 为安装了 Kaspersky Embedded Systems Security 的受保护设备组创建“数据库更新”任务。将 Kaspersky Security Center 管理服务器设置为更新源。
2. 创建状态为“关键区域扫描”的“按需扫描”组任务。Kaspersky Security Center 根据此任务的结果（而不是根据“关键区域扫描”任务的结果）评估组中每台受保护设备的安全状态。
3. 为受保护设备组创建新的策略。在策略属性的“**应用程序设置**”部分中，停用本地系统按需扫描任务的计划启动，并在“**运行本地系统任务**”子部分的设置中停用对管理组受保护设备的数据库更新任务。

您还可以配置有关 Kaspersky Embedded Systems Security 事件的管理员通知。

通过 Kaspersky Security Center 安装应用程序控制台

有关创建安装包和远程安装任务的详细信息，请参见《Kaspersky Security Center 实施指南》。

要使用远程安装任务安装应用程序控制台，请执行下列操作：

1. 在 Kaspersky Security Center 管理控制台中，展开“**高级**”节点。
2. 展开“**远程安装**”子节点。
3. 在“安装包”子节点的结果窗格中，单击“**创建安装包**”按钮。在创建新的安装包时：
   a. 在“**新建安装包向导**”窗口中，选择“**创建指定可执行文件的安装包**”作为安装包类型。
   b. 输入新安装包名称。
   c. 选择 Kaspersky Embedded Systems Security 分发包文件夹中的 \console\setup.exe 文件，然后选中“**将整个文件夹复制到安装包**”复选框。
   d. 使用“**可执行文件启动设置（可选）**”字段中的 ADDLOCAL 命令行选项来执行应用程序控制台的安装。应用程序控制台安装在默认安装文件夹中。确保指定“EULA=1”参数。否则无法安装组件。

      ```
      /s /p "ADDLOCAL=MmcSnapin EULA=1"
      ```

      或者在“**可执行文件启动设置（可选）**”字段中，您可以使用 ADDLOCAL 命令行选项修改要安装的组件集，并使用 INSTALLDIR 命令行选项指定默认文件夹以外的目标文件夹。例如，要在 C:\KasperskyConsole 文件夹中执行应用程序控制台的独立安装，请使用以下命令行选项：

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
```

4. 在"**安装包**"子节点中，创建一个任务，在选定的受保护设备（管理组）上远程安装应用程序控制台。配置任务设置。

   要了解创建和配置远程安装任务的详细信息，请参见 Kaspersky Security Center 帮助。

5. 运行远程安装任务。

应用程序控制台安装到该任务指定的受保护设备上。

通过 Kaspersky Security Center 卸载 Kaspersky Embedded Systems Security

卸载 Kaspersky Embedded Systems Security 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

如果网络设备上的 Kaspersky Embedded Systems Security 管理受密码保护，在创建用于卸载多个应用程序的任务时请输入密码。如果密码保护未通过 Kaspersky Security Center 策略集中管理，Kaspersky Embedded Systems Security 将从设备成功卸载，在该设备上输入的密码与设置值匹配。不会从其他受保护设备卸载 Kaspersky Embedded Systems Security。

要卸载 Kaspersky Embedded Systems Security：

1. 在 Kaspersky Security Center 管理控制台中，创建并启动应用程序删除任务。
2. 在该任务中，选择卸载方法（与选择安装方法类似，请参见上一节）并指定管理服务器将用来访问受保护设备的账户。您可以仅使用默认卸载设置卸载 Kaspersky Embedded Systems Security。

通过 Active Directory 组策略安装和卸载

本节介绍了通过 Active Directory 组策略安装和卸载 Kaspersky Embedded Systems Security。本节还包含有关通过组策略安装 Kaspersky Embedded Systems Security 后执行的操作的信息。

通过 Active Directory 组策略安装 Kaspersky Embedded Systems Security

您可以通过 Active Directory 组策略在多台受保护设备上安装 Kaspersky Embedded Systems Security。您可以用相同的方式安装应用程序控制台。

要安装 Kaspersky Embedded Systems Security 或应用程序控制台的受保护设备必须在同一个域中和一个组织单元中。

要使用策略安装 Kaspersky Embedded Systems Security 的受保护设备的操作系统必须为相同的位数（32 位或 64 位）。

您必须具有域管理员权限。

要安装 Kaspersky Embedded Systems Security，请使用 ess_x86.msi 或 ess_x64.msi 安装包。要安装应用程序控制台，请使用 esstools.msi 安装包。

有关使用 Active Directory 组策略的详细信息，提供在 Microsoft 提供的文档中。

若要安装 Kaspersky Embedded Systems Security （或应用程序控制台）：

1. 将对应于已安装的 Microsoft Windows 操作系统版本位数（32 位或 64 位）的 msi 文件保存到域控制器上的公共文件夹中。
2. 将密钥文件保存在域控制器上的同一公共文件夹中。
3. 在域控制器上的相同公共文件夹中，创建一个包含以下内容的 install_props.json 文件，表示您接受授权许可协议和隐私策略的条款。

```
{
"EULA": "1",
"PRIVACYPOLICY": "1"
}
```

4. 在域控制器上，为受保护设备所属的组创建新策略。
5. 使用“**组策略对象编辑器**”，在“**计算机配置**”节点中创建新的安装包。以 UNC 格式（通用命名约定）指定 Kaspersky Embedded Systems Security（或应用程序控制台） msi 文件的路径。
6. 在选定组的“**计算机配置**”节点和“**用户配置**”节点中，选中 Windows Installer 的“**始终使用提升的权限安装**”复选框。
7. 使用 `gpupdate /force` 命令应用更改。

Kaspersky Embedded Systems Security 将在该组的受保护设备重新启动后安装到这些设备上。

在安装 Kaspersky Embedded Systems Security 后执行的操作

在受保护设备上安装 Kaspersky Embedded Systems Security 后，推荐您立即更新应用程序数据库并运行关键区域扫描。您可以从应用程序控制台执行这些操作。

您还可以配置有关 Kaspersky Embedded Systems Security 事件的管理员通知。

通过 Active Directory 组策略卸载 Kaspersky Embedded Systems Security

卸载 Kaspersky Embedded Systems Security 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

如果在受保护设备组中使用了 Active Directory 组策略安装 Kaspersky Embedded Systems Security（或应用程序控制台），则可以使用该策略卸载 Kaspersky Embedded Systems Security（或应用程序控制台）。

您可以仅使用默认卸载参数卸载应用程序。

有关使用 Active Directory 组策略的详细信息，提供在 Microsoft 提供的文档中。

如果应用程序管理受密码保护，则无法使用 Active Directory 组策略卸载 Kaspersky Embedded Systems Security。

要卸载 Kaspersky Embedded Systems Security（或应用程序控制台）：

1. 在域控制器上，从要卸载 Kaspersky Embedded Systems Security 或应用程序控制台的受保护设备中选择组织单元。
2. 在“**组策略编辑器**”中选择为安装 Kaspersky Embedded Systems Security 所创建的策略，在“**软件安装**”节点（“**计算机配置 > 软件设置 > 软件安装**”）中打开 Kaspersky Embedded Systems Security （或应用程序控制台）安装包的上下文菜单，然后选择“**所有任务 > 删除**”命令。
3. 选择卸载方法“**立即从用户处和计算机中卸载软件**”。
4. 使用 `gpupdate /force` 命令应用更改。

Kaspersky Embedded Systems Security 将在受保护设备重启后和登录 Microsoft Windows 前从受保护设备中删除。

检查 Kaspersky Embedded Systems Security 功能。使用 EICAR 测试病毒

本节介绍 EICAR 测试病毒以及如何使用 EICAR 测试病毒检查 Kaspersky Embedded Systems Security 的实时文件保护和按需扫描功能。

关于 EICAR 测试病毒

测试病毒的用途是验证反病毒应用程序的运行情况。它由欧洲计算机反病毒研究协会 (EICAR) 开发。

测试病毒不是恶意对象，不包含针对设备的可执行代码，但大部分供应商的反病毒应用程序将它识别为威胁。

包含该测试病毒的文件被称为 eicar.com。您可以从 EICAR 网站 下载该文件。

在将该文件保存在设备硬盘驱动器上的文件夹之前，确保已在该驱动器上禁用实时文件保护。

eicar.com 文件包含一个文本行。在扫描该文件时，Kaspersky Embedded Systems Security 会检测该文本行中的测试威胁，向该文件分配“**已感染**”状态并删除它。有关在该文件中检测到的威胁的信息，将显示在应用程序控制台和任务日志中。

您可以使用 eicar.com 文件来检查 Kaspersky Embedded Systems Security 如何清除感染对象以及如何检测可能已感染对象。要执行此操作，请使用文本编辑器打开该文件，将以下表格中列出的其中一个前缀添加到文件中文本行的开头，并将该文件保存为新的名称，例如 eicar_cure.com。

为确保 Kaspersky Embedded Systems Security 处理带有前缀的 eicar.com 文件，在“**对象保护**”安全设置部分中，为 Kaspersky Embedded Systems Security 的“实时计算机保护”任务和“默认按需扫描”任务设置“**所有对象**”值。

EICAR 文件中的前缀

前缀	扫描后的文件状态和 Kaspersky Embedded Systems Security 操作
无前缀	**Kaspersky Embedded Systems Security 向对象分配“已感染”状态并删除它。**
SUSP-	Kaspersky Embedded Systems Security 向启发式分析检测到的对象分配“**疑似感染**”状态并删除它，因为不会清除可能已感染对象。
WARN-	Kaspersky Embedded Systems Security 向对象（对象的代码与已知威胁的代码部分匹配）分配“**疑似感染**”状态并删除它，因为不会清除可能已感染对象。
CURE-	Kaspersky Embedded Systems Security 向对象分配“**已感染**”状态并清除它。如果成功清除，则文件中的全部文本将用“CURE”一词代替。

检查实时文件保护和按需扫描功能

安装 Kaspersky Embedded Systems Security 后，您可以确认 Kaspersky Embedded Systems Security 发现包含恶意代码的对象。要进行检查，可以使用 EICAR 的测试病毒。

要检查“实时文件保护”功能：

1. 从 EICAR 网站 下载 eicar.com 文件。将它保存到网络中任一设备的本地驱动器上的公共文件夹中。

   在将该文件保存到文件夹之前，请确保对该文件夹禁用实时文件保护。

2. 如果要检查网络用户通知是否正常工作，请确保受保护设备和保存 eicar.com 文件的设备均启用了 Microsoft Windows Messenger 服务。

3. 在受保护设备上打开应用程序控制台。

4. 使用以下其中一种方法，将保存的 eicar.com 文件复制到受保护设备的本地驱动器上：

   - 若要通过“终端服务”窗口进行通知测试，请在使用远程桌面连接实用程序连接到受保护设备后，将 eicar.com 文件复制到受保护设备。
   - 若要通过“Microsoft Windows Messenger 服务”进行通知测试，请使用设备的网络位置从您保存 eicar.com 文件的设备复制它。

如果满足以下条件，则“实时文件保护”正常工作：

- eicar.com 文件已从受保护设备删除。
- 在应用程序控制台中，任务日志的状态为“*关键*”。日志中新增一行有关 eicar.com 文件中的威胁的信息。
- 以下 Microsoft Windows Messenger 服务消息将出现在您从中复制文件的设备上：`Kaspersky Embedded Systems Security 在 <发生事件的时间> 阻止了对计算机 <设备的网络名称> 上的 <设备上的文件的路径>\eicar.com 的访问。原因：检测到威胁。病毒：EICAR-Test-File。用户名：<用户名>。计算机名称：<从中复制该文件的设备的网络名称>。`

确保 Microsoft Windows Messenger 服务在从中复制 eicar.com 文件的设备上运行。

要检查按需扫描功能：

1. 从 EICAR 网站 下载 eicar.com 文件。将它保存到网络中任一设备的本地驱动器上的公共文件夹中。

   在将该文件保存到文件夹之前，请确保对该文件夹禁用实时文件保护。

2. 打开应用程序控制台并展开应用程序控制台树中的“**按需扫描**”节点。
3. 选择“**关键区域扫描**”子节点。
4. 在“**扫描范围设置**”选项卡上，打开“**网络**”节点的上下文菜单，然后选择“**添加网络文件**”。
5. 以 UNC（通用命名惯例）格式输入 eicar.com 文件在远程设备上的网络路径。
6. 选择**对象路径**复选框，将添加的网络路径包含在扫描范围内。
7. 运行“关键区域扫描”任务。

如果满足以下条件，则按需扫描正常运行：

- eicar.com 文件已从设备的硬盘驱动器中删除。
- 在应用程序控制台中，任务日志的状态为“*关键*”。“关键区域扫描”任务日志中新增一行有关 eicar.com 文件中的威胁的信息。

应用程序界面

您可以使用以下界面控制 Kaspersky Embedded Systems Security：

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

Kaspersky Security Center 管理控制台

Kaspersky Security Center 允许您远程安装和卸载、启动和停止 Kaspersky Embedded Systems Security、配置应用程序设置、更改可用应用程序组件集、添加密钥以及启动和停止任务。

可以使用 Kaspersky Embedded Systems Security 管理插件通过 Kaspersky Security Center 管理应用程序。有关 Kaspersky Security Center 界面的详细信息，请参见 *Kaspersky Security Center 帮助*。

Kaspersky Security Center Web 控制台和云控制台

Kaspersky Security Center Web 控制台（以下简称“Web 控制台”）是一个 Web 应用程序，用于集中执行主要任务以管理和维护组织网络的安全系统。Web 控制台是提供用户界面的 Kaspersky Security Center 组件。有关 Kaspersky Security Center Web 控制台的详细信息，请参阅 *Kaspersky Security Center 帮助*。

Kaspersky Security Center 云控制台（以下简称“云控制台”）是基于云的解决方案，用于保护和管理组织网络。有关 Kaspersky Security Center 云控制台的详细信息，请参阅 *Kaspersky Security Center 云控制台帮助*。

使用 Web 控制台和云控制台可以执行以下操作：

- 监控组织安全系统的状态。
- 在网络中的设备上安装 Kaspersky 应用程序。
- 管理已安装的应用程序。
- 查看有关安全系统状态的报告。

应用程序授权

本节提供了与应用程序授权有关的主要概念的信息。

关于最终用户授权许可协议

*最终用户授权许可协议*是您与 AO Kaspersky Lab 之间达成的约束协议，其中规定了使用应用程序时应遵循的条款。

请仔细查看最终用户授权许可协议的条款，然后再开始使用程序。

您可以通过以下方式阅读描述数据处理和传输的最终用户授权许可协议和隐私策略的条款：

- 在安装 Kaspersky Embedded Systems Security 期间。
- 安装后从"开始"菜单（"所有程序" > "Kaspersky Embedded Systems Security" > "EULA 和隐私策略"）访问。
- 在安装卡巴斯基反欺诈云期间。
- 阅读分发包中包含的 license.txt 文件。
- 在卡巴斯基网站 (https://www.kaspersky.ru/business/eula)。

一旦在安装程序时确认您同意最终用户授权许可协议，即表示您接受最终用户授权许可协议的条款。如果您不接受最终用户授权许可协议的条款，则必须中止程序安装，且不得使用程序。

关于授权许可

*授权许可*是指在有限时间内使用程序的权限，通过最终用户授权许可协议向您授予。

有效的授权许可授权您根据最终用户授权许可协议的条款使用该应用程序，并在必要时获得技术支持。

服务范围和应用程序使用期限取决于用于激活应用程序的授权许可类型。

您可以通过两种方式激活应用程序：

- 使用密钥文件，授予您商业授权许可下的使用权
- 使用激活码购买商业授权许可

您可以购买 Kaspersky Embedded Systems Security 标准授权许可或者 Kaspersky Embedded Systems Security Compliance Edition 扩展授权许可，后者包含三个附加系统检查组件：文件完整性监控、日志审查和注册表访问监控。

当商业授权许可到期时，应用程序将继续运行，但以下功能将不可用：

- 与卡巴斯基安全网络集成
- Kaspersky Embedded Systems Security 数据库更新

如果您删除授权许可密钥，应用程序继续运行，**按需扫描**和**实时文件保护**任务保持可用，但是所有其他任务和 Kaspersky Embedded Systems Security 数据库更新都不可用。如果卡巴斯基将您的授权许可添加到拒绝列表，也会发生同样的情况。

要继续使用 Kaspersky Embedded Systems Security 的所有功能，必须续订授权许可。

为确保最大限度地保护您的设备，我们推荐您在授权许可到期之前进行续订。

确保附加密钥的过期日期晚于活动密钥

关于授权许可证书

*授权许可证书*是您与密钥文件或激活码（如果适用）一起收到的文档。

授权许可证书包含有关当前授权许可的以下信息：

- 订单号
- 有关被授予授权许可的用户的信息
- 有关可以使用所提供的授权许可激活的应用程序的信息
- 授权单元数限制（例如，运行可以使用所提供的授权许可的应用程序的设备数量）
- 授权许可有效开始日期
- 授权许可到期日期或授权许可期限
- 授权许可类型

关于密钥

*密钥*是一串位数据，您可以根据最终用户授权许可协议的条款通过密钥来激活并在激活后使用应用程序。密钥是由 Kaspersky 生成的。

您可以通过密钥文件在应用程序中添加授权许可。在应用程序中添加密钥后，将在应用程序界面中以唯一的字母数字序列形式显示该密钥。

Kaspersky 可以针对违反授权许可协议的行为将密钥添加到拒绝列表中。如果阻止了您的密钥，则必须添加其他密钥以使应用程序正常工作。

密钥可以是“活动密钥”或“附加密钥”。

*活动密钥*是指当前正在使用的密钥文件以使应用程序正常工作。可以将商业授权许可或试用授权许可的密钥添加为活动密钥。应用程序只能有一个活动密钥。

*附加密钥*是指确认有权使用应用程序但当前未使用的密钥。在与当前活动密钥关联的授权许可过期时，附加密钥将自动变为活动密钥。只有在具有活动密钥时，才能添加附加密钥。

关于密钥文件

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

您在购买 Kaspersky Embedded Systems Security 或订购 Kaspersky Embedded Systems Security 试用版时提供的电子邮件地址将收到密钥文件。

您不需要连接到 Kaspersky 激活服务器，即可使用密钥文件激活应用程序。

如果意外删除了密钥文件，您可以将其还原。例如，您可能需要密钥文件来注册 Kaspersky CompanyAccount。

要还原密钥文件，请执行以下任一操作：

- 联系授权许可销售商。
- 使用您的可用激活码通过 Kaspersky 网站接收密钥文件。

关于激活码

*激活码*是由 20 个字母和数字组成的唯一序列。您必须输入激活码才能添加用于激活 Kaspersky Embedded Systems Security 的密钥。您在购买 Kaspersky Embedded Systems Security 或订购 Kaspersky Embedded Systems Security 试用版时提供的电子邮件地址将收到激活码。

要使用激活码激活应用程序，您需要 Internet 访问权限以连接到 Kaspersky 激活服务器。

如果您在安装应用程序后丢失了激活码，可以将其恢复。例如，您可能需要激活码才能注册 Kaspersky CompanyAccount。要恢复您的激活码，请联系您购买授权许可的卡巴斯基实验室合作伙伴。

关于数据提供

Kaspersky Embedded Systems Security 的授权许可协议（特别是“数据处理条款”部分）指定了本指南中指示的发送和处理数据的条款、责任及过程。在接受授权许可协议前，请仔细查看其条款以及授权许可协议链接到的所有文档。

Kaspersky 在您使用应用程序时收到的数据受到保护并按照隐私策略 www.kaspersky.com/Products-and-Services-Privacy-Policy 进行处理。

授权许可协议和隐私策略的条款在 Kaspersky Embedded Systems Security 安装期间作为分发包的一部分提供，在安装后可以从“开始”菜单（“**所有程序**” > “**Kaspersky Embedded Systems Security** > “**EULA 和隐私策略**”）访问。

卸载 Kaspersky Embedded Systems Security 期间，Kaspersky Embedded Systems Security 在受保护设备上存储的所有数据都将被删除。

接受授权许可协议的条款，即表示您同意自动将以下数据发送到 Kaspersky：

- 为支持接收更新的机制 - 有关已安装的应用程序及其激活的信息：已安装的应用程序及其完全版本的标识符，包括内部版本号、类型以及授权许可标识符、安装标识符、更新任务标识符。

- 为在应用程序出错时使用导航到知识库文章的功能（重定向器服务）- 有关应用程序和链接类型的信息：名称、区域设置以及应用程序的完全版本号、重定向链接的类型和错误标识符。
- 为管理数据处理的确认 - 有关授权许可协议和规定了数据传输条款的其他文档的接受状态的信息：授权许可协议或其他文档（接受或拒绝作为其一部分的数据处理条款）的标识符和版本；表示用户操作（确认或撤消接受条款）的属性；数据处理条款接受的状态更改的日期和时间。

本地数据处理

在执行本指南所述的应用程序主要功能时，Kaspersky Embedded Systems Security 会在受保护计算机上本地处理和存储一系列数据。

下表包含有关 Kaspersky Embedded Systems Security 对报告中包含的数据进行本地处理和存储的信息。

对报告中包含的数据进行处理和存储

功能区域	事件注册
使用类型	Kaspersky Embedded Systems Security 本地存储数据，并将数据发送到管理服务器。管理服务器数据库存储有关在受管理的受保护设备上发生的应用程序事件的信息。
存储	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<产品版本>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • 管理服务器数据库
安全措施	访问控制列表。
存储期	Kaspersky Embedded Systems Security 将一直存储数据，直到卸载 Kaspersky Embedded Systems Security 为止。 卸载 Kaspersky Embedded Systems Security 期间，Kaspersky Embedded Systems Security 在受保护设备上存储的所有数据都将被删除。
用途	提供主要功能。

Kaspersky Embedded Systems Security 不会删除 Windows 事件日志中的事件，包括在卸载 Kaspersky Embedded Systems Security 期间。

为提供事件注册功能，Kaspersky Embedded Systems Security 在本地处理以下数据：

- 所处理文件的名称、校验和（MD5、SHA-256）和属性，以及它们在被扫描介质上的完整路径。
- Kaspersky Embedded Systems Security 对扫描的文件所采取的操作。
- 对受保护计算机上的被扫描文件采取的用户操作。
- 有关对受保护网络或受保护设备执行任何操作的用户账户的信息。
- 添加到设备控制规则中的设备的设备实例路径值。

- 有关系统上运行的进程和脚本的信息：可执行文件的校验和（MD5、SHA-256）以及完整路径，有关数字证书的信息。
- Windows 防火墙设置。
- Windows 事件日志条目。
- 对受保护计算机上的被扫描文件采取操作的用户账户的名称。
- 正在启动的可执行文件实例，以及这些文件的类型、名称、校验和和属性。
- 有关网络活动的信息：
  - 被阻止的外部设备的 IP 地址。
  - 处理的 IP 地址。
- 有关 Windows USN 日志状态的信息。

下表包含有关 Kaspersky Embedded Systems Security 处理的服务数据的信息。服务数据包括：程序参数、隔离文件和备份文件、程序服务数据库中的信息、授权许可数据。

下表包含有关 Kaspersky Embedded Systems Security 对用户指定的参数的数据进行本地处理和存储的信息。

对用户指定的参数的数据进行处理和存储

功能区域	所有 Kaspersky Embedded Systems Security 功能
使用类型	Kaspersky Embedded Systems Security 本地存储数据，并将数据发送到管理服务器。数据存储在管理服务器数据库中。 应用程序本地处理的数据不会自动发送到 Kaspersky 或其他第三方系统。
存储	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<产品版本>\ • 管理服务器数据库
安全措施	访问控制列表。
处理周期	Kaspersky Embedded Systems Security 将一直存储数据，直到卸载 Kaspersky Embedded Systems Security 为止。 卸载 Kaspersky Embedded Systems Security 期间，Kaspersky Embedded Systems Security 在受保护设备上存储的所有数据都将被删除。 Kaspersky Embedded Systems Security 不会删除导出到配置文件中的参数的数据。 如果在安装向导中选中“**导出隔离对象**”和“**导出备份对象**”复选框，则 Kaspersky Embedded Systems Security 不会删除隔离对象和备份对象。
用途	提供主要功能。

为达到指定目的，Kaspersky Embedded Systems Security 在本地处理以下数据：

- 隔离区或备份区中放置的对象。
- 有关 Kaspersky Embedded Systems Security 运行任务所使用的用户账户的信息（用户名和密码）。

- Kaspersky Embedded Systems Security 密码。
- 已阻止的登录会话的 IP 地址和标识符。
- Windows 防火墙设置和 Windows 防火墙规则设置。
- 添加到"应用程序启动控制"任务规则中的可执行文件的校验和（MD5、SHA-256）和路径。
- 添加到设备控制规则中的设备的设备实例路径值。
- 有关包括在 Kaspersky Embedded Systems Security 任务范围中的文件和文件夹的信息。
- 保护范围中包括或排除的 IP 地址。
- 有关 Windows 事件日志中的事件的信息。
- 有关使用 iSwift 或 iChecker 技术进行的检测的信息。
- 排除设置中指定的校验和（MD5、SHA-256）、完整路径和掩码。
- 有关添加到受信任区域中的进程的信息。
- 有关已添加的授权许可密钥的信息。
- 有关数字证书的信息。
- 在扫描过程中从压缩文件或其他复合对象中解压缩的文件。

作为应用程序基本功能的一部分，Kaspersky Embedded Systems Security 处理并存储数据，包括记录应用程序事件和接收诊断数据。本地处理的数据按照配置和应用的应用程序设置进行保护。

Kaspersky Embedded Systems Security 允许您为本地处理的数据配置保护级别（管理 Kaspersky Embedded Systems Security 功能的访问权限，事件注册。Kaspersky Embedded Systems Security 日志）：您可以更改访问进程数据的用户权限，更改此类数据的数据保留期，完全或部分禁用涉及数据记录的功能，以及更改介质上用于记录数据的文件夹的路径和属性。

应用程序本地处理的数据不会自动发送到 Kaspersky 或其他第三方系统。

默认情况下，从受保护设备删除 Kaspersky Embedded Systems Security 后，将删除该应用程序运行期间本地处理的所有数据。

带诊断信息的文件（跟踪和 dump 文件）、Windows 事件日志中的应用程序事件以及具有导出的 Kaspersky Embedded Systems Security 设置的文件 - 建议手动删除这些文件。

有关处理包含应用程序诊断数据的文件的详细信息，请参阅本指南的相应章节。

您可以通过操作系统的标准方式删除包含 Kaspersky Embedded Systems Security 程序事件的 Windows 事件日志文件。

通过应用程序辅助组件处理本地数据

Kaspersky Embedded Systems Security 安装包包含应用程序辅助组件，这些辅助组件可以安装在设备上，即使该设备未安装 Kaspersky Embedded Systems Security。这些辅助组件为：

- 应用程序控制台。该组件包含在 Kaspersky Embedded Systems Security 管理工具集中，由 Microsoft 管理控制台管理单元表示。

- 管理插件。该组件提供与 Kaspersky Security Center 应用程序的完全集成。

当执行本指南所述的主要应用程序功能时，应用程序辅助组件本地处理一组数据并将数据存储在安装了这些组件的受保护设备上，即使它们与 Kaspersky Embedded Systems Security 分开安装也是如此。

这些应用程序组件本地处理并存储以下数据：

- 应用程序控制台：应用程序控制台上次远程连接到的安装了 Kaspersky Embedded Systems Security 的受保护设备的名称（IP 地址或域名）；在 Microsoft 管理控制台管理单元中配置的显示参数；用户上次通过应用程序控制台在其中选择了对象（使用通过单击"浏览"按钮打开的系统对话框）的文件夹的相关数据。应用程序控制台跟踪文件还可能包含以下数据：建立了远程连接的安装了 Kaspersky Embedded Systems Security 应用程序的受保护设备的名称，以及用于建立远程连接的用户账户的名称。

- 管理插件可以处理和暂时存储 Kaspersky Embedded Systems Security 处理的数据；例如，应用程序任务和组件的配置参数、Kaspersky Security Center 策略的参数、网络列表中发送的数据。

下表包含有关 Kaspersky Embedded Systems Security 对写入 dump 和跟踪文件的数据进行本地处理和存储的信息。

Kaspersky Embedded Systems Security 本地处理并存储以下写入 dump 和跟踪文件的数据：

- 有关 Kaspersky Embedded Systems Security 对受保护设备执行的操作的信息。

- 有关 Kaspersky Embedded Systems Security 处理的对象的信息。

- 有关 Kaspersky Embedded Systems Security 处理的受保护设备上的活动的信息。

- 有关 Kaspersky Embedded Systems Security 运行期间发生的错误的信息。

辅助组件处理的数据不会自动发送到 Kaspersky 或其他第三方系统。

默认情况下，在卸载这些应用程序辅助组件后，这些组件在运行期间本地处理的数据都将被删除。

应用程序辅助组件的跟踪文件是例外，建议手动删除这些文件。

跟踪和 dump 文件中的数据

Kaspersky Embedded Systems Security 可以根据设置在 Kaspersky Embedded Systems Security 运行期间将调试信息写入跟踪文件，以供技术支持之用。

Kaspersky Embedded Systems Security 的 dump 文件由操作系统在应用程序崩溃期间生成，并在下次崩溃时被覆盖。

跟踪和 dump 文件可以包括用户的任何个人数据或组织的机密数据。

请勿在组织策略禁止提交数据的设备上使用 Kaspersky Embedded Systems Security。

默认情况下，Kaspersky Embedded Systems Security 不记录调试信息。

跟踪和 dump 文件不会在生成它们的主机之外自动提交。可以使用标准文本文件查看器查看跟踪文件的内容。跟踪和 dump 文件无限期保留，并且在卸载 Kaspersky Embedded Systems Security 时不会被删除。

调试信息对于技术支持很有用。

未提供特殊机制来限制对跟踪和 dump 文件的访问。管理员可以将此数据配置为写入受保护文件夹。

默认情况下，未配置跟踪和 dump 文件文件夹的路径。要使用跟踪和 dump 文件夹，管理员必须指定它。

跟踪和 dump 文件中的数据可以包含：

- Kaspersky Embedded Systems Security 在主机上执行的操作。
- 有关 Kaspersky 端点代理处理的对象的信息。
- Kaspersky 端点代理运行期间出现的错误。

使用密钥文件激活应用程序

您可以应用密钥文件激活 Kaspersky Embedded Systems Security。

如果已经为 Kaspersky Embedded Systems Security 添加了活动密钥，并且您添加另一个密钥作为活动密钥，则新密钥会替换之前添加的密钥。之前添加的密钥将被删除。

如果已经为 Kaspersky Embedded Systems Security 添加了附加密钥，并且您添加另一个密钥作为附加密钥，则新密钥会替换之前添加的密钥。之前添加的附加密钥将被删除。

如果已经为 Kaspersky Embedded Systems Security 添加了活动密钥和附加密钥，并且您添加新密钥作为活动密钥，则新密钥会替换之前添加的活动密钥；附加密钥不会被删除。

要使用密钥文件激活 Kaspersky Embedded Systems Security：

1. 在应用程序控制台树中，展开“**授权**”节点。
2. 在“**授权**”节点的结果窗格中，单击“**添加密钥**”链接。
3. 在打开的窗口中，单击“**浏览**”按钮。
4. 选择具有 .key 扩展名的密钥文件。

   还可以添加密钥作为附加密钥。若要添加密钥作为附加密钥，请选中“**作为附加密钥使用**”复选框。

5. 单击“**确定**”。

将会应用选定的密钥文件。“**授权**”节点将提供有关添加的密钥的信息。

使用激活码激活应用程序

要使用激活码激活应用程序，受保护设备必须连接到 Internet。

您可以使用激活码激活 Kaspersky Embedded Systems Security。

使用此方法激活应用程序时，Kaspersky Embedded Systems Security 将数据发送到激活服务器来验证所输入的代码：

- 如果激活码验证成功，应用程序将激活。
- 如果激活码验证失败，将显示相应通知。在这种情况下，您必须联系向您销售 Kaspersky Embedded Systems Security 授权许可的软件供应商。
- 如果已超过激活码的激活数量，将显示相应通知。应用程序激活过程中断，应用程序会建议您联系 Kaspersky 技术支持。

您可以通过应用程序控制台使用激活码激活 Kaspersky Embedded Systems Security，或者通过管理插件或 Web 插件创建“激活应用程序”组任务来进行激活。

要通过应用程序控制台使用激活码激活 Kaspersky Embedded Systems Security：

1. 在应用程序控制台树中，展开“**授权**”节点。
2. 在“**授权**”节点的结果窗格中，单击“**添加激活码**”链接。
3. 在打开的窗口的“**激活码**”字段中输入激活码。
   - 如果要将激活码用作附加密钥，请启用“**作为附加密钥使用**”复选框。
   - 如果要查看授权许可信息，请单击“**显示授权许可信息**”按钮；信息将显示在“**授权许可信息**”组框中。
4. 单击“**确定**”。

   Kaspersky Embedded Systems Security 会将有关应用的激活码的信息发送到激活服务器。

查看有关当前授权许可的信息

查看授权信息

有关当前授权许可的信息显示在应用程序控制台的 **Kaspersky Embedded Systems Security** 节点的详细信息窗格中。密钥可以具有以下状态：

- **检查密钥状态** – Kaspersky Embedded Systems Security 正在检查已应用的密钥文件或激活码，等待有关当前密钥状态的响应。
- **授权许可过期日期** – Kaspersky Embedded Systems Security 已激活，且在指定日期和时间之前有效。在以下情况下，密钥状态以黄色突出显示：
  - 授权许可将在 14 天后过期，并且未应用任何附加密钥。
  - 添加的密钥已被添加到拒绝列表且将被阻止。
- **授权许可已过期** – 由于授权许可已过期，Kaspersky Embedded Systems Security 未激活。状态红色高亮显示。
- **已违反最终用户授权许可协议** – 由于违反了最终用户授权许可协议的条款，Kaspersky Embedded Systems Security 未激活。状态红色高亮显示。

- **密钥在拒绝列表中** – 添加的密钥已被卡巴斯基阻止并添加到拒绝列表，例如密钥被第三方用来非法激活应用程序。状态红色高亮显示。

查看有关当前授权许可的信息

要查看有关当前授权许可的信息，

在应用程序控制台树中，展开“**授权**”节点。

有关当前授权许可的常规信息显示在“**授权**”节点的详细信息窗格中（请参见下表）。

“授权”节点中有关授权许可的常规信息

字段	描述
激活码	激活码。如果您使用激活码激活应用程序时，则填写此字段。
激活状态	有关应用程序的激活状态的信息。“**授权**”节点的详细信息窗格的“**激活状态**”列可具有以下状态： • **已应用** – 如果您已使用激活码或密钥文件激活应用程序。 • **激活** – 如果您已应用激活码激活应用程序，但激活过程尚未最终完成。应用程序激活完成并且节点的详细信息窗格的内容刷新后，状态更改为“**已应用**”。 • **激活错误** – 如果应用程序激活失败。您可在任务日志中查看激活不成功的原因。
密钥	用于激活应用程序的密钥。
授权许可类型	授权许可类型：商用或试用。
过期日期	与活动密钥相关联的授权许可的到期日期和时间。
激活码状态或密钥状态	激活码状态或密钥状态：*活动*或*附加*。

要查看有关授权许可的详细信息，

在“**授权**”节点上，打开包含您要展开的授权许可数据的行的上下文菜单，然后选择“**属性**”。

在“**密钥属性**”窗口中，“**常规**”选项卡显示有关当前授权许可的详细信息，“**高级**”选项卡显示有关客户的信息以及 Kaspersky 或向您出售 Kaspersky Embedded Systems Security 的经销商的联系人详细信息（请参见下表）。

“属性：<激活码状态或密钥状态>”窗口中的详细授权许可信息

字段	描述
“常规”选项卡	
密钥	用于激活应用程序的密钥。
密钥添加日期	密钥添加到应用程序的日期。
授权许可类型	授权许可类型：商用或试用。
到期前的天数	与活动密钥相关联的授权许可在到期前所剩的天数。
过期日	与活动密钥相关联的授权许可的到期日期和时间。如果在无期限订阅下激活应用程序，此字段的

期	值为*无期限*。如果 Kaspersky Embedded Systems Security 无法确定授权许可过期日期，则此字段的值设置为*未知*。
应用程序	使用密钥文件或激活码激活的应用程序的名称。
密钥使用限制	对使用密钥的限制（如果有）。
符合技术支持条件	有关 Kaspersky 或其合作伙伴之一是否将在授权许可期限下提供技术支持的信息。
“高级”选项卡	
关于授权许可的信息	当前授权许可密钥。
支持信息	Kaspersky 或其提供技术支持的合作伙伴的联系人详细信息。如果不提供技术支持，则此字段可为空。
所有者信息	有关授权许可所有者的信息：客户名称和获取授权许可的组织的名称。

授权许可到期后的功能限制

授权许可到期后，以下限制将应用于功能组件：

- 除了“实时文件保护”、“按需扫描”和“应用程序完整性控制”任务以外，所有任务都将停止。
- 无法启动除了“实时文件保护”、“按需扫描”和“应用程序完整性控制”以外的所有任务。这些任务继续使用旧的反病毒数据库运行。
- 漏洞利用防御功能受限制：
  - 进程受保护至重新启动为止。
  - 新进程无法添加到保护范围中。

其他功能（存储库、日志、诊断信息）仍将可用。

续订授权许可

默认情况下，当授权许可还有 14 天就要到期时，Kaspersky Embedded Systems Security 会通知您即将到期的情况。在这种情况下，“**Kaspersky Embedded Systems Security**”节点的结果窗格中将以黄色突出显示“**授权许可过期日期**”状态。

您可以在到期日期前使用附加密钥续订授权许可。这可确保在当前授权许可到期后和您使用新的授权许可激活应用程序之前继续保护您的设备。

要续订授权许可：

1. 获取新的激活码或密钥文件。
2. 在应用程序控制台树中，打开“**授权**”节点。

3. 在“**授权**”节点的结果窗格中执行以下操作之一：

- 如果您想要使用密钥文件续订授权许可：

  a. 单击“**添加密钥**”链接。

  b. 在打开的窗口中，单击“**浏览**”按钮。

  c. 选择具有 .key 扩展名的新密钥文件。

  d. 选中“**作为附加密钥使用**”复选框。

- 如果您想要使用激活码续订授权许可：

  a. 单击“**添加激活码**”链接。

  b. 在打开的窗口中输入购买的激活码。

  c. 选中“**作为附加密钥使用**”复选框。

> 应用激活码需要 Internet 连接。

4. 单击“**确定**”。

当前 Kaspersky Embedded Systems Security 授权许可到期后，会添加并自动应用附加密钥。

删除密钥

您可以删除添加的密钥。

如果向 Kaspersky Embedded Systems Security 添加了附加密钥，并且您删除了活动密钥，则附加密钥会自动变为活动密钥。

> 如果您删除所添加的密钥，则可以通过重新应用密钥文件来将其还原。

删除所添加的密钥：

1. 在应用程序控制台树中，选择“**授权**”节点。
2. 在包含有关已添加密钥的信息的表格中的“**授权**”节点的结果窗格中，选择您要删除的密钥。
3. 在包含有关所选密钥的信息的行的上下文菜单中，选择“**删除**”。
4. 在确认窗口中单击“**是**”按钮以确认您希望删除该密钥。

选定的密钥将被删除。

使用管理插件

本节提供有关 Kaspersky Embedded Systems Security 管理插件的信息，并介绍如何管理一台或一组受保护设备上安装的应用程序。

从 Kaspersky Security Center 管理 Kaspersky Embedded Systems Security

您可以通过 Kaspersky Embedded Systems Security 管理插件，使用安装并包含在管理组中的 Kaspersky Embedded Systems Security 集中管理多个受保护的设备。Kaspersky Security Cente r还可以在管理组中分别配置每个受保护的设备。

*管理组*通过 Kaspersky Security Center 手动创建。该组包括您要为其配置相同的控制和保护设置并已安装了 Kaspersky Embedded Systems Security 的多个设备。有关使用管理组的详细信息，请参见 *Kaspersky Security Center 帮助*。

如果 Kaspersky Embedded Systems Security 在某台受保护设备上的运行受活动 Kaspersky Security Center 策略的控制，则该台受保护设备的应用程序设置不可用。

可通过以下方式通过 Kaspersky Security Center 管理 Kaspersky Embedded Systems Security：

- **使用 Kaspersky Security Center 策略**。可使用 Kaspersky Security Center 策略为一组设备远程定义相同的保护设置。在活动策略中指定的任务设置的优先级高于在应用程序控制台中本地配置或在 Kaspersky Security Center 的"**属性：<受保护设备名称>**"窗口中远程配置的任务设置。

  您可使用策略配置常规应用程序设置、实时计算机保护任务设置、本地活动控制任务设置和计划的本地系统任务启动设置。

- **使用 Kaspersky Security Center 组任务**。使用 Kaspersky Security Center 组任务可远程配置任务的通用设置，一组设备具有过期期限。

  您可使用组任务激活应用程序，配置"按需扫描"任务设置，更新任务设置，以及"应用程序启动控制规则生成器"任务设置。

- **使用一组设备的任务**。使用一组设备的任务允许远程配置通用任务设置，不属于任何管理组的受保护设备具有有限执行期限。

- **使用单个设备的属性窗口**。在"**属性：<受保护设备名称>**"窗口中，您可远程配置管理组中包含的单台受保护设备的任务设置。如果选中的受保护设备不受活动 Kaspersky Security Center 策略的控制，您可配置常规应用程序设置和所有 Kaspersky Embedded Systems Security 任务的设置。

Kaspersky Security Center 可以配置应用程序设置和高级功能，还可以使用日志和通知。您可以为一组受保护设备和单台受保护设备配置这些设置。

管理应用程序设置

本部分包含有关在 Kaspersky Security Center Web 控制台中配置 Kaspersky Embedded Systems Security 常规设置的信息。

导航

了解如何通过所选界面导航到所需任务设置。

通过策略打开常规设置

要通过策略打开 Kaspersky Embedded Systems Security 的应用程序设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在打开的“**属性：<策略名称>**”窗口中，选择“**应用程序设置**”部分。
6. 在您要配置的设置的子部分中单击“**设置**”按钮。

在应用程序属性窗口中打开常规设置

要打开单台受保护设备的 Kaspersky Embedded Systems Security 属性窗口：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**设备**”选项卡。
4. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：
   - 双击受保护设备的名称。
   - 在受保护设备的上下文菜单中选择“**属性**”项。

   将打开“**属性：<受保护设备名称>**”窗口。
5. 在“**应用程序**”部分中，选择“**Kaspersky Embedded Systems Security 3.2**”。
6. 单击“**属性**”按钮。
   将打开“**Kaspersky Embedded Systems Security 3.2 设置**”窗口。
7. 选择“**应用程序设置**”部分。

在 Kaspersky Security Center 中配置常规应用程序设置

您可以通过 Kaspersky Security Center 为一组受保护设备或一台受保护设备配置 Kaspersky Embedded Systems Security 常规设置。

在 Kaspersky Security Center 中配置扩展性、界面和扫描设置

要配置扩展性、界面和扫描设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**应用程序设置**”部分的“**扩展性、界面和扫描设置**”子部分，单击“**设置**”。
5. 在“**高级应用程序设置**”窗口的“**常规**”选项卡上，配置以下设置：
   - 在“**扩展性设置**”部分中，配置用于定义 Kaspersky Embedded Systems Security 使用的进程数的设置：
     - 自动检测扩展性设置
     - 手动设置工作进程数
       - 用于实时保护的进程数
       - 后台按需扫描任务的进程数
   - 在“**用户交互**”部分中，通过清除或选中“**在任务栏中显示系统托盘图标**”复选框来配置是否在通知区域中显示应用程序系统托盘图标。
6. 在“**扫描设置**”选项卡上，配置以下设置：
   - 扫描后还原文件属性
   - 限制扫描线程的 CPU 使用率
     - 上限(百分比)
   - 用于存储在扫描期间创建的临时文件的文件夹
7. 在“**分级存储**”选项卡上，选择访问分级存储的选项。
8. 单击“**确定**”。

将保存配置的应用程序设置。

在 Kaspersky Security Center 中配置安全性设置

要手动配置安全设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**应用程序设置**”部分中，单击“**安全性和可靠性**”子部分中的“**设置**”按钮。
5. 在“**安全设置**”窗口中，配置以下设置：
   - 在“**密码保护设置**”区域中，启用或禁用“保护应用程序进程免受外部威胁”选项。
   - 在“**密码保护设置**”部分中，设置用于保护访问 Kaspersky Embedded Systems Security 功能的密码。
   - 在“**自我防御**”部分，您可以配置当应用程序返回错误或终止时 Kaspersky Embedded Systems Security 任务的恢复设置。
     - 执行任务恢复
     - 可靠性设置
   - 在“**恢复按需扫描任务不超过(次数)**”部分，指定在切换为 UPS 备份电源后 Kaspersky Embedded Systems Security 对受保护设备产生的负荷的限制：
     - 不启动已计划扫描任务
     - 停止当前扫描任务
   - 在“**密码保护设置**”部分中，设置用于保护访问 Kaspersky Embedded Systems Security 功能的密码。
6. 单击“**确定**”。

将保存扩展性和可靠性设置。

使用 Kaspersky Security Center 配置连接设置

配置的连接设置用于将 Kaspersky Embedded Systems Security 连接到更新和激活服务器，以及在将应用程序与 KSN 服务集成期间使用。

若要配置连接设置，请执行以下步骤：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**应用程序设置**”部分中，单击“**连接**”子部分中的“**设置**”按钮。
   将打开“**连接设置**”窗口。
5. 在“**连接设置**”窗口中，配置以下设置：
   - 在“**代理服务器设置**”部分中，选择代理服务器使用设置：
     - 不使用代理服务器。
     - 使用指定的代理服务器。
     - 代理服务器和端口号的 IP 地址或符号名称。
     - 对于本地地址不使用代理服务器。
   - 在“**代理服务器身份验证设置**”部分中，指定身份验证设置：
     - 在下拉列表中选择身份验证设置。
       - **不使用身份验证** - 不执行身份验证。默认选择该方式。
       - **使用 NTLM 身份验证** - 使用由 Microsoft 开发的 NTLM 网络身份验证协议执行身份验证。
       - **使用带用户名和密码的 NTLM 身份验证** - 通过由 Microsoft 开发的 NTLM 网络身份验证协议，使用名称和密码执行身份验证。
       - **应用用户名和密码** - 使用用户名和密码执行身份验证。
     - 需要时，输入用户名和密码。
   - 在“**授权**”部分中，清除或选中“**激活应用程序时使用 Kaspersky Security Center 作为代理服务器**”。
6. 单击“**确定**”。

将保存配置的连接设置。

配置本地系统任务的计划启动

您可以使用策略，根据管理组中的每个受保护设备上本地配置的计划，允许或阻止启动本地系统按需扫描任务和更新任务：

- 如果特定类型的本地系统任务的计划启动受到策略禁止，则这些任务将不会按照计划在受保护设备上执行。您可以手动启动该本地系统任务。
- 如果特定类型的本地系统任务的计划启动被策略允许，则这些任务将按照为此任务进行的本地配置的计划参数来执行。

默认情况下，策略会禁止本地系统任务的启动。

如果更新或按需扫描受 Kaspersky Security Center 组任务的管理，我们推荐不要允许本地系统任务启动。

如果不使用组更新或按需扫描任务，则允许在策略中启动本地系统任务。Kaspersky Embedded Systems Security 将执行应用程序数据库和模块更新，并根据默认计划启动所有本地系统按需扫描任务。

您可使用策略允许或阻止以下本地系统任务的计划启动：

- 按需扫描任务：关键区域扫描、隔离区扫描、在操作系统启动时扫描、应用程序完整性控制、基线文件完整性监控。
- 更新任务：数据库更新、软件模块更新、复制更新。

如果受保护设备被从管理组中排除，将自动启用本地系统任务计划。

要在策略中允许或阻止 Kaspersky Embedded Systems Security 本地系统任务的计划启动：

1. 在管理控制台树的“**管理服务**”节点中，展开所需的组并选择“**策略**”选项卡。
2. 在“**策略**”选项卡上，在受保护设备组上的 Kaspersky Embedded Systems Security 本地系统任务计划启动的策略的上下文菜单中，选择“**属性**”。
3. 在“**属性：<策略名称>**”窗口中，打开“**应用程序设置**”部分。在“**运行本地系统任务**”部分中，单击“**设置**”按钮并执行以下操作之一：
   - 选中“**按需扫描任务**”和“**更新任务和复制更新任务**”复选框以允许所列任务的计划启动。
   - 清除“**按需扫描任务**”和“**更新任务和复制更新任务**”复选框以禁用所列任务的计划启动。

   选择或清除该复选框将不会影响任何此类本地自定义任务的启动设置。
4. 确保您所配置的策略为活动策略且应用于选定受保护设备组。
5. 单击“**确定**”。

配置的任务计划设置将应用于选定的任务。

在 Kaspersky Security Center 中配置隔离和备份设置

在 Kaspersky Security Center 中配置常规备份设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择要为其配置应用程序设置的管理组。

3. 在选定的管理组的详细窗格中执行以下操作之一：

   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

   > 如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**补充**”部分中，单击“**存储**”子部分中的“**设置**”按钮。

5. 使用“**存储设置**”窗口的“**备份**”选项卡配置以下备份设置：

   - 若要指定备份文件夹，请使用“**备份文件夹**”字段在受保护设备的本地驱动器上选择所需的文件夹，或输入文件夹的完整路径。
   - 若要设置最大备份容量，请选中“**最大备份容量(MB)**”复选框，然后在输入字段中指定相关值（单位为 MB）。
   - 若要设置备份可用空间阈值：
     - 定义“**最大备份容量(MB)**”设置的值。
     - 选择“**可用空间阈值(MB)**”复选框。
     - 指定备份文件夹中的可用空间最小值（单位为 MB）。
   - 若要指定用于保存恢复对象的文件夹，请执行以下操作之一：
     - 在“**还原设置**”部分中，选择受保护设备的本地驱动器上的相关文件夹。
     - 在“**用于还原对象的目标文件夹**”字段中，输入文件夹的名称及其完整路径。

6. 在“**存储设置**”窗口的“**隔离**”选项卡上，配置以下隔离设置：

   - 若要更改隔离文件夹，请在“**隔离区文件夹**”输入字段中指定文件夹在受保护设备本地驱动器上的完整路径。
   - 若要设置最大隔离容量，请选中“**隔离区最大容量(MB)**”复选框，然后在输入字段中指定此参数的值（单位为 MB）。
   - 若要设置隔离中的最小可用空间量，请选中“**隔离区最大容量(MB)**”复选框和“**可用空间阈值(MB)**”复选框，然后在输入字段中指定此参数的值（单位为 MB）。
   - 若要更改将隔离中的对象还原到的文件夹，请在“**用于还原对象的目标文件夹**”字段中指定文件夹在受保护设备本地驱动器上的完整路径。

7. 单击“**确定**”。

将保存配置的隔离和备份设置。

创建和配置策略

本节提供有关使用 Kaspersky Security Center 策略在多个受保护设备上管理 Kaspersky Embedded Systems Security 的信息。

可以创建全局性 Kaspersky Security Center 策略，以便管理多个安装了 Kaspersky Embedded Systems Security 的设备上的保护。

策略在一个管理组的所有受保护设备上实施该策略中指定的 Kaspersky Embedded Systems Security 设置、功能和指定任务。

可以为一个管理组依次创建和实施多个策略。该策略当前对管理控制台中具有*活动*状态的组有效。

Kaspersky Embedded Systems Security 系统审核日志中记录了有关策略实施情况的信息。可在应用程序控制台的“**系统审核日志**”节点中查看该信息。

Kaspersky Security Center 提供一种在受保护设备上应用策略的方式：*禁止更改策略*。应用某个策略后，Kaspersky Embedded Systems Security 会使用您在受保护设备上的策略属性中选择的 图标所对应的设置值。在这种情况下，Kaspersky Embedded Systems Security 不会使用应用该策略之前有效的设置值。Kaspersky Embedded Systems Security 不会应用在策略属性中选择的 图标所对应的活动策略设置值。

如果策略为活动的，则策略中标记 图标的设置的值在应用程序控制台中显示，但无法编辑。其他设置的值（策略中标记 图标）可在应用程序控制台中编辑。

活动策略中配置的且标记 图标的设置也会阻止在 Kaspersky Security Center 的“**属性：<受保护设备名称>**”窗口中针对一台受保护设备进行更改。

在禁用活动策略后，使用活动策略指定并发送到受保护设备的设置将保存在本地任务设置中。

如果策略为实时计算机保护任务定义了设置，并且如果此类任务当前正在运行，则一旦应用该策略，便将立即修改该策略所定义的任何设置。如果任务未运行，则设置将在该任务启动时应用。

创建策略

创建策略的过程涉及下列步骤：

1. 使用策略向导创建策略。可以使用向导对话框配置实时计算机保护任务设置。
2. 配置策略设置。在已创建策略的“**属性：<策略名称>**”窗口中，您可以定义实时计算机保护任务设置、Kaspersky Embedded Systems Security 常规设置、隔离和备份设置、任务日志的详细级别以及有关 Kaspersky Embedded Systems Security 事件的用户和管理员通知。

若要为一组运行已安装 Kaspersky Embedded Systems Security 的受保护设备创建策略：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点，然后选择包含您希望为其创建策略的受保护设备的管理组。
2. 在选定管理组的详细信息窗格中，选择“**策略**”选项卡，然后单击“**创建策略**”链接以启动向导并创建策略。

   将打开“**新建策略向导**”窗口。

3. 在“选择要为其创建组策略的应用程序”窗口中，选择 Kaspersky Embedded Systems Security，然后单击“下一步”。

4. 在“名称”字段中输入组策略名称。

   策略名称不能包含以下符号：" * < : > ? \ | 。

5. 要应用以前版本的应用程序中使用的策略配置：

   a. 选中“使用先前应用程序版本的策略设置”复选框。

   b. 单击“选择”按钮。

   c. 选择要应用的策略。

   d. 单击“下一步”。

6. 在“选择操作类型”窗口中，选择以下选项之一：

   - “新建”，以创建具有默认设置的新策略。
   - “导入使用以前版本的 Kaspersky Embedded Systems Security 创建的策略”，以将导入的策略用作模板。
   - 单击“浏览”，然后选择含有现有策略的配置文件。

7. 在“实时计算机保护”窗口中，根据需要配置“实时文件保护”、“KSN 使用”任务、“漏洞利用防御”和“脚本监控”。允许或阻止在网络上的受保护设备上使用配置的策略任务：

   - 单击 按钮可允许更改网络受保护设备上的任务设置，并阻止应用策略中配置的任务设置。
   - 单击 按钮可拒绝更改网络受保护设备上的任务设置，并允许应用策略中配置的任务设置。

   新创建的策略使用实时计算机保护任务的默认设置。

   - 要编辑“实时文件保护”任务的默认设置，请单击“实时文件保护”子部分中的“设置”按钮。在打开的窗口中，根据需要配置任务。单击“确定”。
   - 要编辑“KSN 使用”任务的默认设置，请单击“KSN 使用”子部分中的“设置”按钮。在打开的窗口中，根据需要配置任务。单击“确定”。

     要启动“KSN 使用”任务，您需要接受“KSN 数据处理”窗口中的 KSN 声明。

   - 要编辑“漏洞利用防御”组件的默认设置，请单击“漏洞利用防御”子部分中的“设置”按钮。在打开的窗口中，根据需要配置该功能。单击“确定”。

8. 在“为应用程序创建组策略”窗口中选择下列策略状态之一：

   - “活动策略”，如果您希望在创建策略后立即应用该策略。如果组中已经存在活动策略，则会将其停用并应用新策略。
   - “非活动策略”，如果您不希望立即应用所创建的策略。在此情况下，可在以后激活该策略。

- 选中“**创建策略后立即打开策略属性**”复选框以在单击“**下一步**”按钮后自动关闭**新建策略向导**并配置新创建的策略。

9. 单击“**完成**”按钮。

所创建的策略将显示在选定管理组的“**策略**”选项卡上的策略列表中。在“**属性：<策略名称>**”窗口中，您可配置 Kaspersky Embedded Systems Security 的其他设置、任务和功能。

创建新策略后，会创建一组允许规则，以防止应用程序被阻止并确保其持续运行。您可以在任务设置中查看默认规则。以下是详细信息和限制。

默认情况下，Kaspersky Embedded Systems Security 会在您创建新策略时为传入网络流量创建一组规则：

- Kaspersky Security Center 网络代理 Windows 桌面共享进程的两个允许规则位于 %Program Files% 和 %Program Files (x86)%。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- 本地端口 15000 的两个允许规则。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。

默认情况下，Kaspersky Embedded Systems Security 在您创建新策略时为传出网络流量创建一组规则：

- Kaspersky Embedded Systems Security 服务的两个允许规则位于 %Program Files% 和 %Program Files (x86)%。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- Kaspersky Embedded Systems Security 工作流程的两个允许规则位于 %Program Files% 和 %Program Files (x86)%。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- 本地端口 13000 的两个允许规则。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。

Kaspersky Embedded Systems Security 策略设置部分

常规

在“**常规**”部分中，您可配置以下策略设置：

- 指定策略状态。
- 为父策略和子策略配置继承设置。

事件通知

在“**事件通知**”部分中，您可配置以下事件类别的设置：

- *严重事件*
- *功能故障*
- *警告*

- *信息消息*
  可以使用“**属性**”按钮来配置选定事件的以下设置：
- 指定有关记录事件的信息的存储位置和保留期限。
- 指定所记录事件的通知方式。

应用程序设置

应用程序设置的设置部分

部分	选项
扩展性、界面和扫描设置	在“**扩展性、界面和扫描设置**”子部分中，可以单击“**设置**”按钮来配置以下设置： • 选择手动或自动配置扩展性设置。 • 配置应用程序图标显示设置。
安全性和可靠性	在“**安全性和可靠性**”子部分中，可以单击“**设置**”按钮来配置以下设置： • 配置任务运行设置。 • 指定当受保护设备使用 UPS 电源运行时应用程序的行为。 • 启用或禁用应用程序功能的密码保护。
连接	在“**连接**”子部分中，可以使用“**设置**”按钮来配置与更新服务器、激活服务器和 KSN 连接的以下代理服务器设置： • 配置代理服务器设置。 • 指定代理服务器身份验证设置。
运行本地系统任务	在“**运行本地系统任务**”子部分中，可以使用“**设置**”按钮来根据受保护设备上配置的计划允许或阻止启动以下本地系统任务： • 按需扫描任务。 • 更新任务和复制更新任务。

补充

补充的设置部分

部分	选项
信任区域	单击“**信任区域**”子部分上的“**设置**”按钮，以配置以下信任区域应用程序设置： • 创建信任区域排除项列表。 • 启用或禁用文件备份操作的扫描。 • 创建受信任进程列表。
可移动驱动器扫描	在“**可移动驱动器扫描**”子部分中，可以使用“**设置**”按钮来配置可移动驱动器的

	扫描设置。
应用程序管理的用户访问权限	在“应用程序管理的用户访问权限”子部分中，可以配置管理 Kaspersky Embedded Systems Security 的用户权限和用户组权限。
Kaspersky Security 服务管理的用户访问权限	在“Kaspersky Security 服务管理的用户访问权限”子部分中，可以配置管理 Kaspersky Security 服务的用户权限和用户组权限。
存储	在“存储”子部分中，单击“设置”按钮以配置以下“隔离”、“备份”和“阻止的主机”设置： • 指定您想要放置隔离或备份对象的文件夹的路径。 • 配置备份和隔离的最大大小，并指定可用空间阈值。 • 指定您想要放置从隔离区或备份区恢复的对象的文件夹路径。 • 配置阻止主机的时长。

实时计算机保护

实时计算机保护的设置部分

部分	选项
实时文件保护	在“实时文件保护”子部分中，可以单击“设置”按钮来配置以下任务设置： • 指定保护模式。 • 配置启发式分析的使用。 • 配置信任区域的使用。 • 指定保护范围。 • 设置选定保护范围的安全级别：您可选择预定义的安全级别或手动配置安全性设置。 • 配置任务启动设置。
KSN 使用	在“KSN 使用”子部分中，可以单击“设置”按钮来配置以下任务设置： • 指定要对 KSN 不信任的对象执行的操作。 • 配置 Kaspersky Security Center 作为 KSN 代理服务器的数据传输和使用。 单击“数据处理”按钮可接受或拒绝 KSN 声明，并配置数据交换设置。
漏洞利用防御	在“漏洞利用防御”子部分中，可以单击“设置”按钮来配置以下任务设置： • 选择进程内存保护模式。 • 指定降低漏洞利用风险的操作。 • 添加到和编辑受保护的进程列表。

本地活动控制

"本地活动控制的设置"部分

部分	选项
应用程序启动控制	在"**应用程序启动控制**"子部分中，可以单击"**设置**"按钮来配置以下任务设置： • 选择任务运行模式。 • 配置控制随后应用程序启动的设置。 • 指定应用程序启动控制规则的范围。 • 配置 KSN 的使用。 • 配置任务启动设置。
设备控制	在"**设备控制**"子部分中，可以单击"**设置**"按钮来配置以下任务设置： • 选择任务运行模式。 • 配置任务启动设置。

网络活动控制

网络活动控制的设置部分

部分	选项
防火墙管理	在"**防火墙管理**"子部分中，可以单击"**设置**"按钮来配置以下任务设置： • 配置防火墙规则。 • 配置任务启动设置。

系统审查

系统审查的设置部分

部分	选项
文件完整性监控	在"**文件完整性监控**"子部分中，可以配置对表示受保护设备上遭到安全入侵的文件更改的控制。
日志审查	在"**日志审查**"部分中，可以根据 Windows 事件日志分析结果配置受保护设备的完整性监控。

日志和通知

日志和通知的设置部分

部分	选项
任务日志	在"**任务日志**"子部分中，可以单击"**设置**"按钮来配置以下设置： • 为选定的软件组件指定日志事件的重要性级别。 • 指定任务日志存储设置。

	• 指定 SIEM 与 Kaspersky Security Center 的集成的设置。
事件通知	在“**事件通知**”子部分中，可以单击“**设置**”按钮来配置以下设置： • 指定“*检测到对象*”、“*检测到不受信任的外部设备并限制该设备*”和“*网络会话被列为不信任*”事件的用户通知设置。 • 为“**通知设置**”部分中的事件列表中选定的任何事件指定管理员通知设置。
与管理服务器交互	在“**与管理服务器交互**”部分中，可以单击“**设置**”按钮来选择 Kaspersky Embedded Systems Security 将报告给管理服务器的对象类型（包括隔离对象和备份对象）。

故障诊断

故障诊断部分的设置

部分	选项
故障排除设置	在“**故障排除设置**”子部分中，可以配置以下选项： • 选择该选项以**启用跟踪**。 • 定义**跟踪文件的文件夹**。 • 指定**详细程度**。 • 定义**跟踪文件的最大大小**。 • 选择该选项以**删除最早的跟踪文件**。 • 定义**一个跟踪日志的最大文件数**。 组策略设置和本地设置会引入匹配参数。要了解有关选项及其限制的更多信息，请参阅本地设置配置。您可以在本地设备上以及在多个设备的组策略中为参数设置不同的值，并应用以下条件。 • 在 Kaspersky Security Center 服务器上配置的组策略设置的优先级高于本地设置。 • 在本地设备上配置的组策略设置的优先级低于本地设置。
Dump 文件设置	在 **Dump 文件设置**子部分中，您可以根据需要配置以下选项： • 选择**创建 Dump 文件**选项。 • 定义 **Dump 文件文件夹**。 组策略设置和本地设置会引入匹配参数。要了解有关选项及其限制的更多信息，请参阅本地设置配置。您可以在本地设备上以及在多个设备的组策略中为参数设置不同的值，并应用以下条件。 • 在 Kaspersky Security Center 服务器上配置的组策略设置的优先级高于本地设置。 • 在本地设备上配置的组策略设置的优先级低于本地设置。

修订历史

在“**修订历史**”部分中，可以管理修订：与当前版本或其他策略对比、添加修订说明、保存修订到文件或执行回滚。

配置策略

在现有策略的**属性：<策略名称>**窗口中，您可以配置：

- Kaspersky Embedded Systems Security 常规设置。
- 隔离和备份设置。
- 受信任区域、实时计算机保护和本地活动控制设置。
- 任务日志的详细级别。
- 配置有关 Kaspersky Embedded Systems Security 事件的用户和管理员通知。
- 用于管理应用程序和 Kaspersky Security 服务的访问权限。

要配置策略设置：

1. 在 Kaspersky Security Center 管理控制台树中展开“**受管理设备**”节点。
2. 展开您希望为其配置关联策略设置的管理组，然后打开详细信息窗格中的“**策略**”选项卡。
3. 选择您想要配置的策略，然后使用以下方法之一打开“**属性：<策略名称>**”窗口：
   - 在策略上下文菜单中选择“**属性**”选项。
   - 在所选策略的右侧详细信息窗格中，单击“**配置策略**”链接。
   - 双击所选策略。
4. 在“**策略状态**”部分的“**常规**”选项卡上，启用或禁用策略。为此，请选择以下选项之一：
   - **活动策略**，如果您希望在选定管理组内的所有受保护设备上应用策略。
   - **非活动策略**，如果您不希望以后在选定管理组内的所有受保护设备上激活策略。

   当管理 Kaspersky Embedded Systems Security 时，“**漫游策略**”设置不可用。
5. 在“**事件配置**”、“**应用程序设置**”、“**补充**”、“**日志和通知**”以及“**修订历史**”部分中，可以修改应用程序配置（参见下表）。
6. 在“**实时计算机保护**”、“**本地活动控制**”、“**网络活动控制**”和“**系统审查**”中，配置应用程序设置和应用程序启动设置（参见下表）。

   您可通过 Kaspersky Security Center 策略启用或禁用在管理组内的所有受保护设备上执行任何任务。

   您可为每个单个软件组件配置在所有网络受保护设备上应用策略设置。

7. 单击“**确定**”。

将在策略中应用配置的设置。

使用 Kaspersky Security Center 创建和配置任务

本节包含有关 Kaspersky Embedded Systems Security 任务、如何创建任务、配置任务设置，以及启动和停止任务的信息。

关于 Kaspersky Security Center 中的任务创建

您可为管理组和受保护设备集创建组任务。您可以通过 Kaspersky Security Center 创建以下任务类型：

- 激活应用程序
- 复制更新
- 数据库更新
- 软件模块更新
- 数据库更新回滚
- 按需扫描
- 应用程序完整性控制
- 基线文件完整性监控
- 应用程序启动控制规则生成器
- 设备控制规则生成器

您可采用以下方式创建本地和组任务：

- 对于一台受保护设备：在“**属性 <受保护设备名称>**”窗口的“**任务**”部分中。
- 对于管理组：在选定受保护设备组的节点的结果窗格中的“**任务**”选项卡上。
- 对于一组受保护设备：在“**设备选择**”节点的结果窗格中。

> 您可以使用策略禁用同一管理组中所有受保护服务器上的更新和按需扫描本地系统任务的计划。

有关 Kaspersky Security Center 中任务的常规信息，请参见 *Kaspersky Security Center 帮助*。

使用 Kaspersky Security Center 创建任务

要在 Kaspersky Security Center 管理控制台中创建新任务：

1. 采用以下方式之一启动任务向导：

   - 若要创建本地任务：

     a. 展开管理控制台树中的“**受管理设备**”节点，并且选择受保护设备所属的组。

     b. 在结果窗格的“**设备**”选项卡上，打开受保护设备的上下文菜单，然后选择“**属性**”。

     c. 在打开的窗口中，单击“**任务**”部分中的“**添加**”按钮。

   - 创建组任务：

     a. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

     b. 选择要为其创建任务的管理组。

     c. 在结果窗格中，打开“**任务**”选项卡，然后选择“**创建任务**”。

   - 要为自定义的一组受保护设备创建任务：

     a. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

     b. 选择包含受保护设备的管理组。

     c. 选择一台受保护设备或自定义的一组受保护设备。

     d. 从“**执行操作**”下拉列表中，选择“**创建任务**”选项。

   将打开任务向导窗口。

2. 在标题“**Kaspersky Embedded Systems Security 3.2**”下的“**选择任务类型**”窗口中，选择要创建的任务的类型。

3. 如果选择了除“数据库更新回滚”、“应用程序完整性控制”或“应用程序激活”以外的任何任务类型，将打开“**设置**”窗口。根据任务类型，设置可能有所变化：

   - 创建按需扫描任务。

   - 要创建更新任务，请根据您的需要配置任务设置：

     a. 在“**更新源**”窗口中选择更新源。

     b. 单击“**连接设置**”按钮。在“**连接设置**”窗口中，配置连接到更新源时的代理服务器访问设置。

   - 若要创建“软件模块更新”任务，请在“**有关应用程序软件模块更新的设置**”窗口中配置所需应用程序模块更新设置：

     a. 选择是复制并安装关键软件模块更新，还是仅检查它们的可用性而不安装。

     b. 如果选择了“**复制并安装关键软件模块更新**”：则可能需要重启受保护设备才能应用已安装的软件模块。如果希望任务完成时 Kaspersky Embedded Systems Security 自动重新启动受保护设备，请选中“**允许操作系统重启**”复选框。

     c. 若要获得有关 Kaspersky Embedded Systems Security 模块升级的信息，请选择“**接收有关可用的计划软件模块更新的信息**”。

Kaspersky 不会在更新服务器上发布计划的更新软件包以供自动安装；您可以手动从 Kaspersky 网站下载这些更新软件包。可以配置有关“**有新的计划软件模块更新可用**”事件的管理员通知。该通知将包含我们网站的 URL，以便您从中下载计划的更新。

- 若要创建“复制更新”任务，请在“**复制更新设置**”窗口中指定更新集和目标文件夹。
- 要创建“应用程序激活”任务：
  a. 在“**激活设置**”窗口中，指定您要使用的密钥文件来激活应用程序。
  b. 如果您想要创建用于续订授权许可的任务，请选中“**作为附加密钥使用**”复选框。
- 创建“应用程序启动控制规则生成器”任务。
- 创建“设备控制规则生成器”任务。

4. 配置任务计划。
   可以为除“数据库更新回滚”任务以外的所有任务类型配置计划。
5. 单击“**确定**”。
6. 如果是为一组受保护设备创建任务，请选择将执行该任务的受保护设备网络（或组）。
7. 在“**选择账户以运行任务**”窗口中，指定您要用于运行该任务的账户。
8. 在“**定义任务名称**”窗口中，输入任务名称（长度不得超过 100 个字符），不得包含符号" * < > ? \ | : 。
   建议将任务类型添加到任务名称中（例如，“按需扫描共享文件夹”）。
9. 在“**完成创建任务**”窗口中：
   a. 如果您希望任务在创建后立即启动，请选中“**向导完成后运行任务**”复选框。
   b. 单击“**完成**”。

所创建的任务将显示在“**任务**”列表中。

在 Kaspersky Security Center 的应用程序设置窗口中配置本地任务

要配置单台网络受保护设备的本地任务或常规应用程序设置：

1. 展开 Kaspersky Security Center 管理服务器树中的“**受管理设备**”节点，并且选择受保护设备所属的组。
2. 在结果窗格中，选择“**设备**”选项卡。
3. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：
   - 双击受保护设备的名称。
   - 打开受保护设备名称的上下文菜单，然后选择“**属性**”项。

   将打开“**属性：<受保护设备名称>**”窗口。
4. 要配置本地任务设置，请执行以下步骤：

a. 转至“**任务**”部分。

b. 在任务列表中，选择要配置的本地任务：

- 在任务列表中双击任务名称。
- 选择任务名称，然后单击“**属性**”按钮。
- 在所选任务的上下文菜单中，选择“**属性**”。
  将打开“**属性：<任务名称>**”窗口。

5. 若要配置应用程序设置，请执行以下步骤：

a. 转至“**应用程序**”部分。

b. 在安装的应用程序列表中，选择要配置的应用程序：

- 在安装的应用程序列表中双击应用程序名称。
- 在安装的应用程序列表中选择应用程序名称，然后单击“**属性**”按钮。
- 在安装程序的列表中打开应用程序名称的上下文菜单，然后选择“**属性**”项。
  将打开“**<应用程序名称> 设置**”窗口。

如果应用程序当前受 Kaspersky Security Center 策略控制，且该策略禁止更改应用程序设置，则您无法通过“**<应用程序名称> 设置**”窗口编辑这些设置。

在 Kaspersky Security Center 中配置组任务

从 Kaspersky Security Center 云控制台管理 Kaspersky Embedded Systems Security 时，不能手动添加自定义 HTTP 和 FTP 服务器或网络文件夹。

要为多个受保护设备配置组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：

- 在创建的任务列表中双击任务名称。
- 在创建的任务列表中选择任务名称，然后单击“**配置任务**”链接。
- 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

在“**通知**”部分中，配置任务事件通知设置。关于如何配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

5. 根据所配置的任务类型，执行下列操作之一：

- 要配置按需扫描任务：
  - 在“**扫描范围**”部分中，配置扫描范围。
  - 在“**选项**”部分中，配置任务优先级水平及与其他软件组件的集成。
- 要配置更新任务，请根据您的需要调整任务设置：
  - 在“**设置**”部分中，配置更新源设置和磁盘子系统优化。
  - 单击“**连接设置**”按钮以配置更新源连接设置。
- 要配置“软件模块更新”任务：
  - 转到“**有关应用程序软件模块更新的设置**”部分。
  - 选择要执行的操作：复制并安装软件模块的关键更新或仅检查它们。
- 若要配置“复制更新”任务，请在“**复制更新设置**”部分中指定更新集和目标文件夹。
- 要配置“应用程序激活”任务：
  - 在“**激活设置**”部分中，应用您要使用的密钥文件来激活应用程序。
  - 如果您想要添加用于续订授权许可的激活码或密钥文件，请选中“**作为附加密钥使用**”复选框。
- 要配置设备控制允许规则的自动生成，请在“**设置**”部分中指定将用于创建允许规则列表的设置。

6. 在“**计划**”部分中配置任务计划。您可以计划所有任务类型，但“数据库更新回滚”除外。

7. 在“**账户**”部分中，指定将使用其权限运行任务的账户。关于此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

8. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。关于配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

9. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。

将保存新配置的组任务设置。

下表汇总了可配置的组任务设置。

Kaspersky Embedded Systems Security 组任务设置

Kaspersky Embedded Systems Security 任务类型	“属性：<任务名称>”窗口中的部分	任务设置
应用程序启动	设置	在配置“应用程序启动控制规则生成器”任务设置时，您可以选择如何创建允

控制规则生成器		许规则： • 基于正在运行的应用程序创建允许规则 • 为以下文件夹中的应用程序创建允许规则
	选项	当创建应用程序启动控制的允许规则时，您可以指定执行的操作： • 使用数字证书 • 使用数字证书主题和指纹 • 证书丢失则使用 • 使用 SHA256 哈希 • 为用户或用户组生成规则 您可以使用 Kaspersky Embedded Systems Security 在任务完成时创建的允许规则列表为配置文件配置设置。
	计划	您可以配置设置以安排任务。
设备控制规则生成器	设置	• 选择运行模式：考虑曾经连接过的所有外部设备上的系统数据，或仅考虑当前连接的外部设备。 • 使用 Kaspersky Embedded Systems Security 在任务完成时创建的允许规则列表为配置文件配置设置。
	计划	您可以配置按计划启动任务的设置。
激活应用程序	激活设置	要激活应用程序或续订授权许可，可以添加密钥文件。
	计划	您可以配置按计划启动任务的设置。
复制更新	更新源	您可以将 Kaspersky Security Center 管理服务器或 卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。 如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。
	“连接设置”窗口	在链接自“更新源”部分的“连接设置”窗口中，您可以指定是否应使用代理服务器来建立与 卡巴斯基更新服务器或任何其他服务器的连接。
	复制更新设置	您可指定用于复制的更新集。 在“用于本地存储已复制更新的文件夹”字段中，指定 Kaspersky Embedded Systems Security 将用于存储已复制更新的文件夹的路径。
	计划	您可以配置按计划启动任务的设置。
数据库更新	设置	您可在“更新源”组框中将 Kaspersky Security Center 管理服务器或 卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。 如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。 在“磁盘 I/O 使用情况优化”部分中，您可以配置能够减少磁盘子系统工作负载的功能： • 降低磁盘 I/O 上的负载 • 用于优化的 RAM (MB)

	“连接设置”窗口	在链接自“**更新源**”部分的“**连接设置**”窗口中，您可以指定是否应使用代理服务器来建立与 卡巴斯基更新服务器或任何其他服务器的连接。
	计划	您可以配置按计划启动任务的设置。
软件模块更新	更新源	您可以将 Kaspersky Security Center 管理服务器或 卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。 如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。
	“连接设置”窗口	在“**更新源连接设置**”组框中，您可以指定是否应使用代理服务器来建立与 卡巴斯基更新服务器或任何其他服务器的连接。
	有关应用程序软件模块更新的设置	您可指定关键软件模块更新可用或已安装时 Kaspersky Embedded Systems Security 应执行的操作，还可指定 Kaspersky Embedded Systems Security 是否应接收有关计划的更新的信息。
	计划	您可以配置按计划启动任务的设置。
按需扫描设置	扫描范围	您可指定“按需扫描”任务的扫描范围，并配置安全级别设置。
	“按需扫描设置”窗口	在链接自“**扫描范围**”部分的“**按需扫描设置**”窗口中，可以选择预定义安全级别之一，或手动自定义安全级别。
	选项	您可激活或取消激活为“按需扫描”任务使用启发式分析，并在“**启发式分析**”组框中使用滑块设置分析级别。 在“**与其他组件集成**”组框中，可以配置以下设置： • 为“按需扫描”任务应用受信任区域。 • “为按需扫描应用 KSN 使用”任务。 • 设置“按需扫描”任务的优先级：在后台模式下执行任务（低优先级）或将任务视为关键区域扫描。
	计划	您可以配置按计划启动任务的设置。
应用程序完整性控制	计划	您可以配置按计划启动任务的设置。
基线文件完整性监控	计划	您可以配置按计划启动任务的设置。

对于“数据库更新回滚”任务，可在“**通知**”和“**任务范围的排除项**”部分中仅配置由 Kaspersky Security Center 控制的标准任务设置。

有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

激活应用程序任务

要配置“激活应用程序”任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中选择任务名称，然后单击“**配置任务**”链接。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

   在“**通知**”部分中，配置任务事件通知设置。关于如何配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
5. 在“**激活设置**”部分中，指定您要使用的密钥文件来激活应用程序。如果您想要添加用于延长授权许可的密钥，请选中“**作为附加密钥使用**”复选框。
6. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。
7. 在“**账户**”部分中，指定将使用其权限运行任务的账户。
8. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。

   有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
9. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。

   将保存新配置的组任务设置。

更新任务

要配置“复制更新”、“数据库更新”或“软件模块更新”任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中选择任务名称，然后单击“**配置任务**”链接。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

在“**通知**”部分中，配置任务事件通知设置。关于如何配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

5. 在“**更新源**”部分中，执行以下操作：

   a. 选择更新源：

   - Kaspersky Security Center 管理服务器。
   - 卡巴斯基更新服务器。
   - 自定义 HTTP 或 FTP 服务器或网络文件夹。

   要将 SMB 共享文件夹用作更新源，您需要指定用户账户以启动任务。

   如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。

   b. 单击“**连接设置**”按钮。

   c. 在打开的“**连接设置**”窗口中，配置使用代理服务器连接到 卡巴斯基更新服务器和其他服务器。

   d. 对于数据库更新任务，在“**磁盘 I/O 使用情况优化**”部分中，可以配置能够减少磁盘子系统工作负载的功能：

   “**磁盘 I/O 使用情况优化**”部分仅适用于数据库更新任务。

   - 降低磁盘 I/O 上的负载
   - 用于优化的 RAM (MB)

6. 对于“软件模块更新”任务，在“**有关应用程序软件模块更新的设置**”部分中，指定当关键软件模块更新可用或计划更新信息可用时，Kaspersky Embedded Systems Security 应该执行哪些操作。

   您还可以指定安装关键更新时，Kaspersky Embedded Systems Security 应该执行哪些操作。

   “**有关应用程序软件模块更新的设置**”部分仅适用于“软件模块更新”任务。

7. 对于“复制更新”任务，在“**复制更新设置**”部分中，指定更新集和目标文件夹。

   “**复制更新设置**”部分仅适用于“复制更新”任务。

8. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。

9. 在“**账户**”部分中，指定将使用其权限运行任务的账户。

   有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

10. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。

将保存新配置的组任务设置。

对于“数据库更新回滚”任务，可在“**通知**”和“**任务范围的排除项**”部分中仅配置由 Kaspersky Security Center 控制的标准任务设置。有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

应用程序完整性控制

要配置“应用程序完整性控制”组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中选择任务名称，然后单击“**配置任务**”链接。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

   在“**通知**”部分中，配置任务事件通知设置。关于如何配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
5. 在“**设备**”部分中，选择要为其配置“应用程序完整性控制”任务的设备。
6. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。
7. 在“**账户**”部分中，指定将使用其权限运行任务的账户。
8. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。

   有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
9. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。

   将保存新配置的组任务设置。

在 Kaspersky Security Center 中配置故障诊断设置

如果在操作 Kaspersky Embedded Systems Security 时发生问题（例如，应用程序崩溃），则可以对其进行诊断。为此，您可以为 Kaspersky Embedded Systems Security 进程启用跟踪文件和 Dump 文件的创建，并将这些文件发送给卡巴斯基技术支持进行分析。

Kaspersky Embedded Systems Security 不会自动发送任何跟踪或 Dump 文件。诊断数据只能由具有所需权限的用户发送。

Kaspersky Embedded Systems Security 会以未加密的形式将信息写入到跟踪文件和 Dump 文件。保存文件的文件夹由用户选择，由操作系统配置和 Kaspersky Embedded Systems Security 设置管理。您可以配置访问权限并只允许所需用户访问日志、跟踪文件和 dump 文件。

要在 Kaspersky Security Center 中配置故障诊断设置：

1. 在 Kaspersky Security Center 管理控制台中，打开“应用程序设置”窗口。
2. 打开“**故障诊断**”部分。
3. 如果希望应用程序将调试信息写入文件，请在“**故障排除设置**”子部分中选中“**启用跟踪**”复选框。
4. 在“**跟踪文件文件夹**”字段中，指定 Kaspersky Embedded Systems Security 将保存跟踪文件的本地文件夹的绝对路径。

   该文件夹必须事先创建，并且必须可供 SYSTEM 账户写入。您不能指定网络文件夹、驱动器和环境变量。
5. 配置调试信息的详细级别。
6. 指定**跟踪文件最大大小(MB)**。

   可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小设置为 50 MB。
7. 如果您希望应用程序在达到最大跟踪文件数后删除最早的文件，请选中“**删除最旧的跟踪文件**”复选框。
8. 指定**一个跟踪日志的最大文件数**。

   可用值：1 到 999。默认情况下，最大文件数设置为 5。该字段仅当选中“**删除最旧的跟踪文件**”复选框时才可用。
9. 如果您希望应用程序创建 Dump 文件，请选中“**创建 Dump 文件**”复选框。
10. 在“**Dump 文件文件夹**”字段中，指定 Kaspersky Embedded Systems Security 将保存 Dump 文件的本地文件夹的绝对路径。

    该文件夹必须事先创建，并且必须可供 SYSTEM 账户写入。您不能指定网络文件夹、驱动器和环境变量。
11. 单击“**确定**”。

已配置的应用程序设置将应用于受保护设备上。

管理任务计划

您可以为计划 Kaspersky Embedded Systems Security 任务。

计划任务

您可以在应用程序控制台中计划本地系统和自定义任务。您无法在应用程序控制台中计划组任务。

要使用管理插件计划组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择受保护设备所属的组。
3. 在结果窗格中，选择“**任务**”选项卡。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 双击任务的名称。
   - 打开任务名称的上下文菜单，然后选择“属性”项。
5. 选择“**计划**”部分。
6. 在“**计划设置**”设置块中，选中“**按计划运行**”复选框。

   如果 Kaspersky Security Center 策略阻止按需扫描任务和更新任务的计划，则这些任务的计划设置字段将不可用。

7. 根据需要配置计划设置。为此，请执行以下操作：
   a. 在“**频率**”列表中，选择以下值之一：
      - **每小时**，如果您希望该任务在指定的小时数内间隔运行，请在“**每 <数量> 小时**”字段中指定小时数。
      - **每天**，如果您希望该任务在指定的天数内间隔运行，请在“**每 <数量> 天**”字段中指定天数。
      - **每周**，如果您希望该任务以指定周数为间隔运行，请在“**每 <数量> 周**”字段中指定周数。指定要启动任务的星期中的日期（默认在星期一启动任务）。
      - **应用程序启动时**，如果您希望在每次启动 Kaspersky Embedded Systems Security 时运行该任务。
      - **应用程序数据库更新后**，如果您希望在每次更新应用程序数据库后运行该任务。

   b. 在“**开始时间**”字段中指定首次启动任务的时间。

   c. 在“**开始日期**”字段中，指定计划启动的日期。

   在计划了任务的开始时间、日期和频率之后，将显示下一次启动的预估时间。

   转到“**计划**”选项卡，然后打开“**任务设置**”窗口。在窗口上部的**下次开始**字段中，显示了预计启动时间。每次打开窗口时，此估计启动时间都会更新并显示。

   如果 Kaspersky Security Center 策略设置禁止启动计划的本地系统任务，则“**下次开始**”字段将显示“**被策略阻止**”值。

8. 根据需要使用“**高级**”选项卡来配置以下计划设置。

- 在“**任务停止设置**”部分中：
  a. 选中“**持续时间**”复选框，并在右侧的字段中输入任务执行的最长持续时间（小时和分钟）。
  b. 选中“**暂停开始于**”复选框，并在右侧的字段中输入暂停任务执行的时间间隔（小于 24 小时）的开始值和结束值。
- 在“**高级设置**”部分中：
  a. 选中“**取消计划开始于**”复选框，并指定停止应用计划的日期。
  b. 选中“**运行错过的任务**”复选框以允许启动跳过的任务。
  c. 选中“**在该时间间隔内随机化任务开始时间**”复选框，并按分钟指定该值。

9. 单击“**确定**”。
10. 单击“**应用**”按钮保存任务启动设置。

如果要使用 Kaspersky Security Center 配置单个任务的应用程序设置，请参见“在 Kaspersky Security Center 的应用程序设置窗口中配置本地任务”部分。

启用和禁用计划任务

可在配置计划设置之前或之后启用和禁用计划任务。

要启用或禁用任务启动计划：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择受保护设备所属的组。
3. 在结果窗格中，选择“**任务**”选项卡。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 双击任务的名称。
   - 打开任务名称的上下文菜单，然后选择“属性”项。
5. 选择“**计划**”部分。
6. 执行以下操作之一：
   - 如果您希望启用任务的启动计划，请选中“**按计划运行**”复选框。
   - 如果您希望禁用任务的启动计划，请清除“**按计划运行**”复选框。

不会删除已配置的任务启动计划设置，并将在计划的下一次任务启动时间应用该设置。

7. 单击“**确定**”。

8. 单击“**应用**”。

将保存已配置的任务启动计划设置。

Kaspersky Security Center 中的报告

Kaspersky Security Center 中的报告包含有关受管理设备状态的信息。报告基于管理服务器上存储的信息。

从 Kaspersky Security Center 11 开始，对于 Kaspersky Embedded Systems Security，以下类型的报告可用：

- 有关应用程序组件状态的报告
- 有关已禁止的应用程序的报告
- 有关在测试模式下禁止的应用程序的报告

有关所有 Kaspersky Security Center 报告以及如何配置它们的详细信息，请参阅 *Kaspersky Security Center 帮助*。

有关 Kaspersky Embedded Systems Security 组件状态的报告

您可以监视所有网络设备的保护状态，并获得每个设备上的组件集的结构化概览。

报告显示每个组件的以下状态之一：*正在运行*、*已暂停*、*已停止*、*故障*、*未安装*、*正在启动*。

*未安装*状态指的是组件，而不是应用程序本身。如果未安装应用程序，Kaspersky Security Center 会分配 N/A（不可用）状态。

您可以创建组件选择并使用筛选来显示具有指定组件集和状态的网络设备。

有关创建和使用选择的详细信息，请参见 *Kaspersky Security Center 帮助*。

要在应用程序设置中查看组件状态：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点，然后选择您希望为其配置应用程序设置的管理组。
2. 选择“**设备**”选项卡，然后打开“应用程序设置”窗口。
3. 选择“**组件**”部分。
4. 查看状态表。

要查看 Kaspersky Security Center 标准报告：

1. 在管理控制台树中选择“**管理服务器 <管理服务器名称>**”节点。

2. 打开“**报告**”选项卡。

3. 双击“**有关应用程序组件状态的报告**”列表项。
   将生成报告。

4. 查看以下报告详细信息：

   - 图形化图表。
   - 组件和安装了每个组件的网络设备总数以及设备所属的组的汇总表格。
   - 指定了组件状态、版本、设备和组的详细表格。

有关在活动模式和测试模式下禁止的应用程序的报告

根据“应用程序启动控制”任务的结果，可以生成两种类型的报告：有关已禁止的应用程序的报告（如果在活动模式下启动该任务）和有关在测试模式下禁止的应用程序的报告（如果在仅统计模式下启动该任务）。这两种报告显示了有关网络的受保护设备上阻止的应用程序的信息。每个报告都针对所有管理组生成，并累积来自受保护设备上安装的所有 Kaspersky 应用程序的数据。

要查看有关在仅统计模式下禁止的应用程序的报告：

1. 在“仅统计”模式下启动“应用程序启动控制”任务。

2. 在管理控制台树中选择“**管理服务器 <管理服务器名称>**”节点。

3. 打开“**报告**”选项卡。

4. 双击“**有关在测试模式下禁止的应用程序的报告**”项。
   将生成报告。

5. 查看以下报告详细信息：

   - 显示阻止启动次数最多的前 10 个应用程序的图形化图表。
   - 应用程序阻止行为的汇总表格，其中指定可执行文件名、原因、阻止时间和发生阻止的设备数量。
   - 指定了有关设备、文件路径和阻止条件的数据的详细表格。

要查看有关在活动模式下禁止的应用程序的报告：

1. 在“活动”模式下启动“应用程序启动控制”任务。

2. 在管理控制台树中选择“**管理服务器 <管理服务器名称>**”节点。

3. 打开“**报告**”选项卡。

4. 双击“**有关禁止的应用程序的报告**”项。
   将生成报告。

此报告包含的阻止数据与有关在测试模式下禁止的应用程序的报告相同。

使用 Kaspersky Embedded Systems Security 控制台

本节提供有关 Kaspersky Embedded Systems Security 控制台的信息，并介绍了如何使用安装在受保护设备或其他设备上的应用程序控制台来管理该应用程序。

关于 Kaspersky Embedded Systems Security 控制台

Kaspersky Embedded Systems Security 控制台是可以添加到 Microsoft 管理控制台的独立管理单元。

您可以通过安装在受保护设备或公司网络中其他设备上的应用程序控制台来管理应用程序。

在其他设备上安装应用程序控制台后，需要进行高级配置。

您可以在分配给不同域的不同受保护设备上安装应用程序控制台和 Kaspersky Embedded Systems Security。在这种情况下，从应用程序向应用程序控制台发送信息可能会受到限制。例如，任何应用程序任务启动之后，其在应用程序控制台中的状态可能保持不变。

安装应用程序控制台时，安装向导在安装文件夹中创建了 kavfs.msc 文件并将 Kaspersky Embedded Systems Security 管理单元添加到 Microsoft Windows 独立管理单元的列表。

您可以从“开始”菜单启动应用程序控制台。可以运行 Kaspersky Embedded Systems Security 管理单元 msc 文件，也可以将其作为树中的一个新元素添加到 Microsoft 管理控制台中。

在 64 位版本的 Microsoft Windows 下，Kaspersky Embedded Systems Security 管理单元只能添加到 32 位版本的 Microsoft 管理控制台中。要添加 Kaspersky Embedded Systems Security 管理单元，请通过执行以下命令从命令行打开 Microsoft 管理控制台：mmc.exe / 32。

可以将多个 Kaspersky Embedded Systems Security 管理单元添加到在作者模式下打开的一个 Microsoft 管理控制台中。然后，您可以管理安装了 Kaspersky Embedded Systems Security 的多个设备的保护。

Kaspersky Embedded Systems Security 控制台界面

本节介绍程序界面的主要元素。

Kaspersky Embedded Systems Security 控制台窗口

Kaspersky Embedded Systems Security 控制台以节点的形式显示在 Microsoft 管理控制台树中。

与其他受保护设备上安装的 Kaspersky Embedded Systems Security 建立连接后，将在节点名称后面附加已安装应用程序的受保护设备的名称和建立连接时所使用的用户账户名称：**Kaspersky Embedded Systems Security <受保护设备名称> 作为 <账户名称>**。连接到与应用程序控制台安装在同一台受保护设备上的 Kaspersky Embedded Systems Security 时，节点名称为 **Kaspersky Embedded Systems Security**。

应用程序控制台树

应用程序控制台树显示 **Kaspersky Embedded Systems Security** 节点和应用程序功能组件的子节点。

Kaspersky Embedded Systems Security 节点包括以下子节点：

- **实时计算机保护**：管理实时计算机保护任务和 KSN 服务。“**实时计算机保护**”节点允许配置以下任务：
  - **实时文件保护**
  - **KSN 使用**
  - **漏洞利用防御**
- **计算机控制**：控制受保护设备上安装的应用程序的启动以及外部设备连接。“**计算机控制**”节点允许配置以下任务：
  - **应用程序启动控制**
  - **设备控制**
  - **防火墙管理**
- **自动规则生成器**：配置“应用程序启动控制”任务和“设备控制”任务的组和系统规则的自动生成。
  - **应用程序启动控制规则生成器**
  - **设备控制规则生成器**
  - 规则生成组任务 **<任务名称>**（如果有）
    使用 Kaspersky Security Center 创建组任务。您无法通过应用程序控制台管理组任务。
- **系统审查**：配置文件操作控制和 Windows 事件日志审查设置。
  - **文件完整性监控**
  - **日志审查**
- **按需扫描**：管理按需扫描任务。每个任务具有单独的节点：
  - **在操作系统启动时扫描**
  - **关键区域扫描**
  - **隔离区扫描**
  - **应用程序完整性控制**
  - 自定义任务 **<任务名称>**（如有）

  该节点显示安装应用程序时创建的系统任务、自定义任务，以及使用 Kaspersky Security Center 创建并发送到受保护设备的组按需扫描任务。
- **更新**：管理 Kaspersky Embedded Systems Security 数据库和模块更新以及将更新复制到本地更新源文件夹中。此节点包含一些子节点，以管理每个更新任务和上次**回滚应用程序数据库更新**任务：
  - **数据库更新**

- 软件模块更新
- 复制更新
- 回滚应用程序数据库更新

该节点显示使用 Kaspersky Security Center 创建并发送到受保护设备的所有自定义和组更新任务。

- **存储**：管理隔离和备份设置。
  - 隔离
  - 备份
- **日志和通知**：管理本地任务日志、安全日志和 Kaspersky Embedded Systems Security 系统审核日志。
  - 安全日志
  - 系统审核日志
  - 任务日志
- **授权**：添加或删除 Kaspersky Embedded Systems Security 授权许可密钥，查看授权许可详细信息。

详细信息窗格

详细信息窗格显示有关选定节点的信息。如果选择 **Kaspersky Embedded Systems Security** 节点，详细信息窗格将显示有关当前设备保护状态的信息，以及有关 Kaspersky Embedded Systems Security、其功能组件的保护状态和授权许可到期日期的信息。

Kaspersky Embedded Systems Security 节点的上下文菜单

可使用 **Kaspersky Embedded Systems Security** 节点的上下文菜单项执行以下操作：

- **连接至其他计算机**。连接至其他设备以管理其上安装的 Kaspersky Embedded Systems Security。也可以单击 **Kaspersky Embedded Systems Security** 节点的详细信息窗格右下角的链接来执行此操作。
- **启动服务 / 停止服务**。启动或停止应用程序或选定任务。要执行这些操作，您还可以使用工具栏上的按钮。也可以在程序任务的上下文菜单中执行这些操作。
- **配置可移动驱动器扫描设置**。配置通过 USB 端口连接到受保护设备的可移动驱动器的扫描。
- **配置信任区域设置**。查看和配置受信任区域设置。
- **修改应用程序管理的用户权限**。查看和配置 Kaspersky Embedded Systems Security 功能的访问权限。
- **修改 Kaspersky Security 服务管理的用户权限**。查看和配置 Kaspersky Security 服务管理用户权限。
- **导出设置**。将应用程序设置保存到 XML 格式的配置文件中。也可以在应用程序任务的上下文菜单中执行此操作。
- **导入设置**。从 XML 格式的配置文件中导入应用程序设置。也可以在应用程序任务的上下文菜单中执行此操作。

- **关于应用程序和可用模块更新的信息**。查看有关 Kaspersky Embedded Systems Security 和当前可用应用程序模块更新的信息。
- **刷新**。刷新应用程序控制台窗口的内容。也可以在应用程序任务的上下文菜单中执行此操作。
- **属性**。查看和配置 Kaspersky Embedded Systems Security 或选定任务的设置。也可以在应用程序任务的上下文菜单中执行此操作。

  > 也可以使用 **Kaspersky Embedded Systems Security** 节点的详细信息窗格中"**应用程序属性**"链接或工具栏上的按钮执行此操作。

- **帮助**。查看 Kaspersky Embedded Systems Security 帮助信息。也可以在应用程序任务的上下文菜单中执行此操作。

Kaspersky Embedded Systems Security 任务的工具栏和上下文菜单

可以使用应用程序控制台树中每个任务的上下文菜单项来管理 Kaspersky Embedded Systems Security 任务。

可使用上下文菜单项执行以下操作：

- **启动/停止**。启动或停止任务执行。要执行这些操作，您还可以使用工具栏上的按钮。
- **恢复/暂停**。恢复或暂停执行任务。要执行这些操作，您还可以使用工具栏上的按钮。此操作适用于"实时计算机保护"任务和"按需扫描"任务。
- **添加任务**。新建自定义任务。此操作适用于按需扫描任务。
- **打开日志**。查看和管理任务日志。此操作适用于所有任务。
- **删除任务**。删除自定义任务。此操作适用于按需扫描任务。
- **设置模板**。管理模板。此操作适用于"实时文件保护"和"按需扫描"。

通知区域中的系统托盘图标

每次重启受保护设备之后，当 Kaspersky Embedded Systems Security 自动启动时，系统托盘图标将显示在任务栏通知区域 中。如果在应用程序安装期间安装了"系统托盘图标"组件，则默认情况下将显示该图标。

系统托盘图标的外观反映了当前设备保护状态。有两种状态：

	活动（彩色图标）- 当前至少有以下一个任务正在运行：实时文件保护、应用程序启动控制
	不活动（灰色图标）- 当前未运行以下任何任务：实时文件保护、应用程序启动控制

右键单击系统托盘图标可打开该图标的上下文菜单。

上下文菜单提供了多个可显示应用程序窗口的命令（请参见下表）。

系统托盘图标中的上下文菜单命令

命令	描述

打开应用程序控制台	打开 Kaspersky Embedded Systems Security 控制台（如已安装）。
打开小型诊断窗口	打开小型诊断窗口。
关于应用程序	打开“关于应用程序”窗口，其中包含有关 Kaspersky Embedded Systems Security 的信息。 对于注册的 Kaspersky Embedded Systems Security 用户，“关于应用程序”窗口包含有关已安装的紧急更新的信息。
隐藏	隐藏任务栏通知区域中的系统托盘图标。

您可以随时重新显示隐藏的系统托盘图标。

要再次显示系统托盘图标，

在 Microsoft Windows 的“开始”菜单中，选择“所有程序” > “**Kaspersky Embedded Systems Security**” > “系统托盘图标”。

设置的名称可能有所不同，具体取决于安装的操作系统。

在 Kaspersky Embedded Systems Security 的常规设置中，您可以启用或禁用系统托盘图标在每次受保护设备重启后应用程序自动启动时的显示。

通过其他设备上的应用程序控制台管理 Kaspersky Embedded Systems Security

可以通过远程设备上安装的应用程序控制台管理 Kaspersky Embedded Systems Security。

要使用远程设备上的 Kaspersky Embedded Systems Security 控制台管理应用程序，请确保：

- 远程设备上的应用程序控制台用户已添加到受保护设备上的 ESS 管理员组。
- 如果在受保护设备上启用 Windows 防火墙，将允许 Kaspersky Security 管理服务进程 (kavfsgt.exe) 连接网络。
- 在安装 Kaspersky Embedded Systems Security 的过程中，在“安装向导”窗口中选中“允许远程访问”复选框。

如果远程设备上的 Kaspersky Embedded Systems Security 受密码保护，输入密码以通过应用程序控制台来访问应用程序管理。

通过应用程序控制台配置常规应用程序设置

Kaspersky Embedded Systems Security 的常规设置和故障诊断设置设定了应用程序的常规运行条件。您可以通过这些设置来控制 Kaspersky Embedded Systems Security 所使用的工作进程数，在异常终止后恢复 Kaspersky Embedded Systems Security 任务，维护日志，在异常终止后创建 Kaspersky Embedded Systems Security 进程的 Dump 文件，以及配置其他常规设置。

如果 Kaspersky Security Center 活动策略阻止对应用程序设置的更改，则无法在应用程序控制台中配置这些设置。

要配置 Kaspersky Embedded Systems Security 设置：

1. 在应用程序控制台树中，选择“**Kaspersky Embedded Systems Security**”节点并执行以下操作之一：
   - 在节点的详细信息窗格中，单击“**应用程序属性**”链接。
   - 在节点上下文菜单中选择“**属性**”。

   将打开“**应用程序设置**”窗口。
2. 在打开的窗口中，根据需要配置 Kaspersky Embedded Systems Security 常规设置：
   - 可在“**扩展性和界面**”选项卡上配置以下设置：
     - 在“**扩展性设置**”部分：
       - 用于实时计算机保护的进程数
       - 后台按需扫描任务的工作进程数
   - 在“**用户交互**”部分中，选择在每个应用程序启动后，系统托盘图标是否将显示在任务栏中。
   - 可在“**安全性和可靠性**”选项卡上配置以下设置：
     - 在“**密码保护设置**”区域中，配置对应用程序进程的保护。
     - 在“**密码保护设置**”部分中，配置应用程序功能的密码保护设置。
     - 在“**自我防御**”部分中，指定按需扫描任务崩溃后恢复该任务的尝试次数。
   - 在“**恢复按需扫描任务不超过(次数)**”部分，指定在切换为 UPS 备份电源后 Kaspersky Embedded Systems Security 执行的操作。
   - 在“**扫描设置**”选项卡上：
     - 扫描后还原文件属性
     - 限制扫描线程的 CPU 使用率
     - 上限(百分比)
     - 用于存储在扫描期间创建的临时文件的文件夹
   - 在“**连接设置**”选项卡上：
     - 在“**代理服务器设置**”部分中，指定代理服务器设置。
     - 在“**代理服务器身份验证设置**”部分中，指定在代理服务器上进行身份验证所需的身份验证类型和详细信息。
     - 在“**授权**”部分中，指定是否将 Kaspersky Security Center 用作应用程序激活的代理服务器。

- 在“**故障诊断**”选项卡上：
  - 如果您希望应用程序将调试信息写入文件，请在“**故障排除设置**”子部分中选中“**启用跟踪**”复选框。
  - 在“**跟踪文件夹**”字段中，指定 Kaspersky Embedded Systems Security 将保存跟踪文件的本地文件夹的绝对路径。

    该文件夹必须事先创建，并且必须可供 SYSTEM 账户写入。您不能指定网络文件夹、驱动器和环境变量。
  - 配置调试信息的详细级别。
  - 指定**跟踪文件的最大大小**。

    可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小设置为 50 MB。
  - 如果您希望应用程序在达到最大跟踪文件数后删除最早的文件，请选中“**删除最旧早的跟踪文件**”复选框。
  - 指定**一个跟踪日志的最大文件数**。

    可用值：1 到 999。默认情况下，最大文件数设置为 5。该字段仅当选中“**删除最早的跟踪文件**”复选框时才可用。
  - 如果您希望应用程序创建 Dump 文件，请选中“**创建 Dump 文件**”复选框。
  - 在“**Dump 文件文件夹**”字段中，指定 Kaspersky Embedded Systems Security 将保存 Dump 文件的本地文件夹的绝对路径。

    该文件夹必须事先创建，并且必须可供 SYSTEM 账户写入。您不能指定网络文件夹、驱动器和环境变量。

Kaspersky Embedded Systems Security 会以未加密的形式将信息写入到跟踪文件和 Dump 文件。保存文件的文件夹由用户选择，由操作系统配置和 Kaspersky Embedded Systems Security 设置管理。您可以配置访问权限并只允许所需用户访问日志、跟踪文件和 dump 文件。

3. 单击“**确定**”。

Kaspersky Embedded Systems Security 设置即被保存。

管理 Kaspersky Embedded Systems Security 任务

本节包含有关如何创建、配置、启动和停止 Kaspersky Embedded Systems Security 任务的信息。

Kaspersky Embedded Systems Security 任务类别

Kaspersky Embedded Systems Security 中的实时计算机保护、计算机控制、按需扫描和更新功能作为任务实现。

您可以使用应用程序控制台树中的任务上下文菜单、工具栏和快速访问任务栏来管理这些任务。可在结果窗格中查看任务状态信息。任务管理操作记录在系统审核日志中。

Kaspersky Embedded Systems Security 任务分为两种类型：*本地*和*组*。

本地任务

本地任务只能在为其创建的受保护设备上执行。根据启动方式，存在以下几种类型的本地任务：

- **本地系统任务**。这些任务在安装 Kaspersky Embedded Systems Security 过程中自动创建。您可以编辑除“隔离区扫描”和“数据库更新回滚”任务之外的所有本地系统任务的设置。无法重命名或删除本地系统任务。您可以同时运行本地系统和自定义按需扫描任务。

- **本地自定义任务**。在应用程序控制台中，您可创建按需扫描任务。在 Kaspersky Security Center 中，您可创建按需扫描、数据库更新、数据库更新回滚和复制更新任务。您可以重命名、配置和删除自定义任务。可同时运行多个自定义任务。

组任务

您可以从 Kaspersky Security Center 管理组任务和受保护设备集任务。所有组任务都是自定义任务。组任务也显示在应用程序控制台中。在应用程序控制台中，只能查看组任务的状态。您不能使用应用程序控制台来管理或配置组任务。

手动启动、暂停、恢复和停止任务

您可以只暂停和恢复实时计算机保护和按需扫描任务。不能手动暂停或恢复其他任务。

要启动、暂停、恢复或停止任务：

1. 在应用程序控制台中，打开任务的上下文菜单。
2. 选择以下任务之一：“**启动**”、“**暂停**”、“**恢复**”或“**停止**”。

   该操作将执行并记录到系统审核日志中。

当您恢复按需扫描任务时，Kaspersky Embedded Systems Security 将从暂停扫描的对象恢复扫描。

管理任务计划

您可以为计划 Kaspersky Embedded Systems Security 任务。

配置任务计划设置

在应用程序控制台中，您可以计划何时启动本地系统和自定义任务。但是，您无法计划何时启动组任务。

要计划任务：

1. 打开您要计划的任务的上下文菜单。
2. 选择“**属性**”。

将打开“**任务设置**”窗口。

3. 在打开的窗口中的“**计划**”选项卡上，选中“**按计划运行**”复选框。

4. 按照以下步骤指定计划设置：

   a. 在“**频率**”下拉菜单中，选择以下之一：

   - **每小时**：每小时运行一次任务；在“**每<数字>小时**”字段中指定小时数。
   - **每天**：每天运行一次任务；在“**每<数字>天**”字段中指定天数。
   - **每周**：每周运行一次任务；在“**每<数字>周**”字段中指定周数。指定要启动任务的星期中的日期（默认在星期一启动任务）。
   - **应用程序启动时**：每次启动 Kaspersky Embedded Systems Security 时运行该任务。
   - **应用程序数据库更新后**：每次更新应用程序数据库后运行该任务。

   b. 在“**开始时间**”字段中，指定首次启动任务的时间。

   c. 在“**开始日期**”字段中，指定首次启动任务的日期。

   指定了任务启动频率之后，将在窗口顶部的“**下次开始**”字段中显示任务的首次启动时间、计划的开始应用日期以及预计的下一次任务启动时间的相关信息。每次打开“**任务设置**”窗口的“**计划**”选项卡时，将更新并显示下次任务开始的估计时间。

   如果 Kaspersky Security Center 活动策略设置禁止启动计划的本地系统任务，则“**下次开始**”字段将显示“**被策略阻止**”值。

5. 使用“**高级**”选项卡可以指定以下计划设置：

- 在“**任务停止设置**”部分中：

  a. 选择“**持续时间**”复选框。在右侧的字段中，以小时和分钟为单位输入任务最大持续时间。

  b. 选择“**暂停开始于**”复选框。在右侧的字段中，输入何时暂停和恢复任务（24 小时之内）。

- 在“**高级设置**”部分中：

  a. 选择“**取消计划开始于**”复选框，然后指定任务计划的结束日期。

  b. 选中“**运行错过的任务**”复选框以启动跳过的任务。

  c. 选中“**在该时间间隔内随机启动任务**”复选框，并按分钟指定该值。

6. 单击“**确定**”。

将保存任务计划设置。

启用和禁用计划任务

可在指定任务计划设置之前或之后启用和禁用已计划的任务。

要启用或禁用已计划任务的启动：

1. 在应用程序控制台树中，打开已计划任务的上下文菜单。
2. 选择“**属性**”。
   将打开“**任务设置**”窗口。
3. 在打开的窗口的“**计划**”选项卡上，选择以下选项之一：
   - 选择“**按计划运行**”复选框可启用已计划任务的启动。
   - 清除“**按计划运行**”复选框可禁用已计划任务的启动。

     任务计划设置不会被删除，而是在您下次启用计划任务启动时应用。
4. 单击“**确定**”。

   将保存任务计划设置。

使用用户账户启动任务

您可以在系统账户下启动任务，也可以指定其他账户。

关于使用账户启动任务

您可以指定运行以下 Kaspersky Embedded Systems Security 任务的账户：

- 应用程序启动控制规则生成器
- 设备控制规则生成器
- 按需扫描
- 更新

默认情况下，使用系统账户权限运行这些任务。

在以下情况下，推荐您使用具有正确访问权限的其他账户：

- **更新**任务：如果您已指定在网络上其他设备的公共文件夹作为更新源。
- **更新**任务：如果使用带有内置 Windows NTLM 身份验证的代理服务器来访问更新源。
- **按需扫描**任务：如果系统账户对已扫描的对象不具有访问权限（例如，对受保护设备上的共享文件夹中的文件的访问权限）。
- **应用程序启动控制规则生成器**任务：如果将生成的规则导出到系统账户无法访问的配置文件（例如，受保护设备上的某个共享文件夹）。

您可以使用系统账户权限运行更新、按需扫描和规则生成器任务。如果此设备与受保护设备在同一个域中注册，则 Kaspersky Embedded Systems Security 将执行这些任务并访问网络中的另一台设备上的共享文件夹。在这种情况下，系统账户必须具有对这些文件夹的访问权限。Kaspersky Embedded Systems Security 将使用账户**<域名\设备名称>**的权限来访问该设备。

指定用户账户以启动任务

要指定用于启动任务的账户：

1. 在应用程序控制台树中，打开要使用特定账户启动的任务的上下文菜单。
2. 选择“**属性**”。
   将打开“**任务设置**”窗口。
3. 在打开的窗口的“**运行账户**”选项卡上，请按照下列步骤操作：
   a. 选择“**用户名**”。
   b. 输入您要使用的账户的用户名和密码。

      选定用户必须在受保护设备上经过注册，或者与该受保护设备在同一域中。

   c. 确认密码。
4. 单击“**确定**”。

将保存修改的设置。

导入和导出设置

本节说明如何导出 Kaspersky Embedded Systems Security 设置。您还将学习如何将特定的软件设置导出到 XML 配置文件，以及如何将这些设置从配置文件导入回应用程序。

关于导入和导出设置

可以将 Kaspersky Embedded Systems Security 设置导出到 XML 配置文件，也可以将配置文件中的设置导入到 Kaspersky Embedded Systems Security 中。可以将所有应用程序设置或仅将单个组件的设置保存到配置文件。

在将 Kaspersky Embedded Systems Security 的所有设置导出到文件时，将保存常规程序设置以及下列 Kaspersky Embedded Systems Security 组件和功能的设置：

- 实时文件保护
- KSN 使用
- 设备控制

- 应用程序启动控制
- 设备控制规则生成器
- 应用程序启动控制规则生成器
- 按需扫描任务
- 文件完整性监控
- 日志审查器
- Kaspersky Embedded Systems Security 数据库和软件模块更新
- 隔离
- 备份
- 日志
- 管理员和用户通知
- 受信任区域
- 漏洞利用防御
- 密码保护

此外，还可以在文件中保存 Kaspersky Embedded Systems Security 的常规设置及用户账户的权限。

无法导出组任务设置。

Kaspersky Embedded Systems Security 将导出程序所使用的所有密码，例如，用于运行任务或连接代理服务器的用户账户设置。导出的密码以加密的形式保存在配置文件中。只有该受保护设备上安装的 Kaspersky Embedded Systems Security 未重新安装或更新，才能使用它导入密码。

您无法使用安装在其他受保护设备上的 Kaspersky Embedded Systems Security 导入之前保存的密码。将设置导入至其他受保护设备之后，必须手动输入所有密码。

如果在导出时 Kaspersky Security Center 策略有效，则应用程序将导出该策略所使用的指定值。

您可以从包含 Kaspersky Embedded Systems Security 单个组件参数的配置文件（例如从未安装全部组件的 Kaspersky Embedded Systems Security 创建的文件）导入设置。导入设置后，只有该配置文件中包含的那些 Kaspersky Embedded Systems Security 设置会发生变化。所有其他设置保持不变。

导入设置时，已被阻止的活动 Kaspersky Security Center 策略的设置不会发生更改。

导出设置

要将设置导出到配置文件：

1. 在应用程序控制台树中，执行以下操作之一：

- 在 **Kaspersky Embedded Systems Security** 节点的上下文菜单中，选择“**导出设置**”可导出所有 Kaspersky Embedded Systems Security 设置。
- 在特定任务的上下文菜单中，选择“**导出设置**”可导出程序的单个功能组件的设置。
- 要导出“受信任区域”设置：
  a. 在应用程序控制台树中，打开“**Kaspersky Embedded Systems Security**”节点上下文菜单。
  b. 选择“**配置信任区域设置**”。
  将打开“**信任区域**”窗口。
  c. 单击“**导出**”按钮。
  将打开“设置导出向导”。

2. 按照**导出设置向导**中的说明操作：指定您要用于保存设置的配置文件的名称和路径。
指定路径时可以使用系统环境变量，但不能使用用户环境变量。

> 如果在导出时 Kaspersky Security Center 策略有效，则应用程序将导出该策略使用的设置。

3. 单击“**已完成应用程序设置导出过程**”窗口中的“**关闭**”按钮。

设置导出向导将关闭并保存导出设置。

导入设置

要从保存的配置文件导入设置：

1. 在应用程序控制台树中，执行以下操作之一：
   - 在 **Kaspersky Embedded Systems Security** 节点的上下文菜单中，选择“**导入设置**”可导入所有 Kaspersky Embedded Systems Security 设置。
   - 在特定任务的上下文菜单中，选择“**导入设置**”可导入应用程序的单个功能组件的设置。
   - 要导入“受信任区域”设置：
     a. 在应用程序控制台树中，打开 **Kaspersky Embedded Systems Security** 节点的上下文菜单。
     b. 选择“**配置信任区域设置**”。
     将打开“**信任区域**”窗口。
     c. 单击“**导入**”按钮。
     将打开设置导入向导。
2. 按照**导入设置向导**中的说明操作：指定带有要导入的设置的配置文件。

> 将 Kaspersky Embedded Systems Security 设置或其功能组件常规设置导入到在受保护设备之后，无法恢复到先前的设置。

3. 在“**已完成应用程序设置导入**”窗口中，单击“**关闭**”按钮。

   设置导入向导将关闭并保存已导入的设置。

4. 在应用程序控制台工具栏中，单击“**刷新**”按钮。

   应用程序控制台窗口将显示已导入的设置。

如果受保护设备上的 Kaspersky Embedded Systems Security 进行了重新安装或更新，Kaspersky Embedded Systems Security 不会从在其他受保护设备上或同一受保护设备上创建的文件导入密码（用于启动任务或连接到代理服务器的账户凭据）。导入完成后，必须手动输入密码。

使用安全性设置模板

本节包含有关在 Kaspersky Embedded Systems Security 保护和扫描任务中使用安全性设置模板的信息。

关于安全性设置模板

可以在受保护设备的文件资源树或列表中，手动配置节点的安全性设置，并将配置好的设置值保存为模板。然后可在 Kaspersky Embedded Systems Security 保护和扫描任务中，使用该模板来指定其他节点的安全设置。

可使用模板来指定以下 Kaspersky Embedded Systems Security 任务的安全性设置：

- 实时文件保护
- 在操作系统启动时扫描
- 关键区域扫描
- 按需扫描任务

应用到受保护设备文件资源树中的父节点的模板中的安全性设置将应用到所有子节点中。以下情况中父节点的模板将不会不应用于子节点：

- 如果单独指定子节点的安全设置。
- 如果子节点为虚拟节点。这种情况下，必须针对每个虚拟节点单独应用模板。

创建安全性设置模板

要手动将节点的安全性设置保存到模板：

1. 在应用程序控制台树中，选择要为其创建安全性设置模板的任务。
2. 在所选任务的详细信息窗格中，单击“**配置保护范围**”或“**配置扫描范围**”链接。
3. 在受保护设备的网络文件资源树或列表中，选择要查看的模板。

4. 在“**安全级别**”选项卡上，单击“**另存为模板**”按钮。
   将打开“**模板属性**”窗口。
5. 在“**模板名称**”字段中，输入模板名称。
6. 在“**描述**”字段中，输入其他模板信息。
7. 单击“**确定**”。

安全设置模板即被保存。

查看模板中的安全性设置

要在您创建的模板中查看安全性设置：

1. 在应用程序控制台树中，选择带有要查看的安全性设置模板的任务。
2. 在选定任务的上下文菜单中，选择“**设置模板**”。
   将打开“**模板**”窗口。
3. 在模板列表中，选择要查看的模板。
4. 单击“**查看**”按钮。

将打开“**<模板名称>**”窗口。“**常规**”选项卡显示模板名称和有关模板的其他信息。“**选项**”选项卡列出了模板中保存的安全性设置。

应用安全性设置模板

要将模板中的安全性设置应用于所选节点：

1. 在应用程序控制台树中，选择要对其应用安全性设置模板的任务。
2. 在所选任务的详细信息窗格中，单击“**配置保护范围**”或“**配置扫描范围**”链接。
3. 在受保护设备的网络文件资源树或列表中，打开要对其应用模板的节点或项的上下文菜单。
4. 选择“**应用模板**”→“**<模板名称>**”。
5. 单击“**保存**”按钮。

这会将安全性设置模板应用于受保护设备的文件资源树中的选定节点。选定节点的“**安全级别**”选项卡上的值将更改为“**自定义**”。

如果模板的安全性设置应用到受保护设备文件资源树中的父节点，这些设置也将应用到所有子节点。

您可以在受保护设备的文件资源树中单独配置子节点的保护或扫描范围。在这种情况下，应用到父节点的模板安全性设置不会自动应用到子节点。

要将模板中的安全性设置应用于所有选定节点：

1. 在应用程序控制台树中，选择要对其应用安全性设置模板的任务。
2. 在所选任务的详细信息窗格中，单击“**配置保护范围**”或“**配置扫描范围**”链接。
3. 在受保护设备网络文件资源树或列表中，选择一个父节点，以将模板应用于选定的节点及其子节点。
4. 在上下文菜单中，选择“**应用模板 → <模板名称>**”。
5. 单击“**保存**”按钮。

将对受保护设备文件资源树中的父节点和所有子节点应用安全性设置模板。选定节点的“**安全级别**”选项卡上的值将更改为“**自定义**”。

删除安全性设置模板

要删除安全性设置模板：

1. 在应用程序控制台树中，选择带有要删除的安全性设置模板的任务。
2. 在选定任务的上下文菜单中，选择“**设置模板**”。
   将打开“**模板**”窗口。

   在“**按需扫描**”父节点的结果窗格中，可以查看按需扫描任务的设置模板。
3. 在模板列表中，选择要删除的模板。
4. 单击“**删除**”按钮。
   将打开一个窗口，提示您确认删除。
5. 在打开的窗口中，单击“**是**”。

将删除所选模板。

您可以应用安全性设置模板来保护或扫描受保护设备的文件资源树中的节点。在这种情况下，删除模板后，此类节点的安全性设置将保持不变。

查看保护状态和 Kaspersky Embedded Systems Security 信息

要查看有关 Kaspersky Embedded Systems Security 的设备保护状态的信息，

在应用程序控制台树中选择“**Kaspersky Embedded Systems Security**”节点。

默认情况下，将自动刷新应用程序控制台的详细信息窗格中的信息：

- 对于本地连接，每 10 秒钟刷新一次。

- 对于远程连接，每 15 秒钟刷新一次。

您可以手动刷新信息。

*要在“**Kaspersky Embedded Systems Security**”节点中手动刷新信息，*

请在“**Kaspersky Embedded Systems Security**”节点的上下文菜单中选择“**刷新**”命令。

应用程序控制台的详细信息窗格中会显示以下应用程序信息：

- “卡巴斯基安全网络使用”状态。
- 设备保护状态。
- 有关数据库和应用程序模块更新的信息。
- 实际诊断数据。
- 受保护设备控制任务的数据。
- 授权许可信息。
- 与 Kaspersky Security Center 的集成状态：已安装与应用程序连接的 Kaspersky Security Center 的服务器的详细信息；有关活动策略控制的应用程序任务的信息。

使用不同的颜色指示保护状态：

- *绿色*。根据配置的设置运行任务。保护处于活动状态。
- *黄色*。任务未启动，已暂停或已停止。可能会发生安全威胁。推荐您配置并启动任务。
- *红色*。任务完成，但出现错误，或任务运行时检测到安全威胁。推荐您启动任务或采取措施消除检测到的安全威胁。

此块中的某些详细信息（例如，任务名称或检测到的威胁数量）为单击后将转至相关任务的节点或打开任务日志的链接。

“**卡巴斯基安全网络使用情况**”部分显示当前任务状态，例如，*正在运行*、*已停止*或*从未执行*。该指示器可以使用以下值：

- 绿色表示“KSN 使用”任务正在运行，并且对状态的文件请求正在发送到 KSN。
- 黄色表示其中一项声明已被接受，但任务未运行；或任务正在运行，但文件请求未发送到 KSN。

计算机保护

“**计算机保护**”部分（请参见下表）显示有关设备当前保护状态的信息。

有关设备保护状态的信息

“保护”部分	信息
设备	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下

保护状态指示器	值： • 绿色 – 默认显示此颜色，指示“实时文件保护”组件已安装且任务正在运行。 • 黄色 –“实时文件保护”组件未安装，且“关键区域扫描”任务已长时间未执行。 • 红色 –“实时文件保护”任务未运行。
实时文件保护	**任务状态** - 当前任务状态，例如，“*正在运行*”或“*已停止*”。 **检测到** - Kaspersky Embedded Systems Security 检测到的对象数量。例如，如果 Kaspersky Embedded Systems Security 在五个文件中检测到一个恶意应用程序，该字段中的值将增加 1。如果检测到的恶意应用程序数量超过 0，此值突出显示为红色。
关键区域扫描	**上次扫描日期** – 上次在关键区域扫描病毒和其他计算机安全威胁的日期和时间。 *从未执行* - 在过去 30 天或更长时间（默认值）内没有执行关键区域扫描任务时所发生的一个事件。您可以更改产生此事件的阈值。
漏洞利用防御	**状态** – 漏洞利用防御技术的当前状态，例如，“*已应用*”或“*未应用*”。 **防御模式** – 可用的两个模式之一，在配置进程内存保护的过程中选择：**发现漏洞利用时终止**或**仅统计**。 **保护的进程** – 根据选定的模式添加到保护范围并处理的进程总数。
已备份对象	*已超过备份可用空间阈值* – 当备份可用空间量接近指定限制时会发生该事件。Kaspersky Embedded Systems Security 继续将对象移至备份区。在这种情况下，“**已用空间**”字段高亮显示为黄色。 *已超过最大备份容量* – 当备份大小已达到指定限制时会发生此事件。Kaspersky Embedded Systems Security 继续将对象移至备份区。在这种情况下，“**已用空间**”字段高亮显示为红色。 **已备份对象** - 当前在备份区中的对象数量。 **已用空间** – 已使用的备份空间量。

更新

“**更新**”部分（请参见下表）显示有关反病毒数据库和应用程序模块的更新程度的信息。

有关 Kaspersky Embedded Systems Security 数据库和模块状态的信息

“更新”部分	信息
数据库和软件模块状态指示器	带有部分名称的面板的颜色反映了应用程序数据库和模块的状态。该指示器可以使用以下值： • 绿色 – 默认显示此颜色，指示应用程序数据库处于最新状态，并且最近的数据库更新任务已成功完成。 • 黄色 – 数据库已过期，或上次数据库更新任务失败。 • 红色 – 发生*应用程序数据库已严重过期*或*应用程序数据库已损坏*事件。
数据库更新和软件模块更新	**数据库状态** – 数据库更新状态的评估。 它可以是以下值： • **应用程序数据库为最新** – 应用程序数据库在之前 7 天内进行过更新（默认）。 • **应用程序数据库已过期** – 应用程序数据库在之前 7 至 14 天内进行过更新（默认）。

	• **应用程序数据库已严重过期** – 应用程序数据库在超过 14 天前进行过更新（默认）。您可以更改用于生成*应用程序数据库为最新*和*应用程序数据库已严重过期*的事件的阈值。 **数据库发布日期** - 最近数据库更新的发布日期和时间。日期和事件指定为 UTC 格式。 **最新完成的"数据库更新"任务的状态** – 最新数据库更新的日期和时间。日期和时间根据受保护设备的当地时间指定。如果发生"*失败*"事件，则字段为红色。 **可用模块更新数** – 可供下载和安装的 Kaspersky Embedded Systems Security 模块更新数量。 **已安装模块更新数** – 已安装的 Kaspersky Embedded Systems Security 模块更新数量。

控制

"**控制**"部分（请参见下表）显示有关"应用程序启动控制"、"设备控制"和"防火墙管理"任务的信息。

有关受保护设备控制状态的信息

"控制"部分	信息
受保护设备控制状态指示器	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下值： • 绿色 – 默认显示此颜色，指示"应用程序启动控制"组件已安装，且任务在"**活动**"模式下运行。 • 黄色 -"应用程序启动控制"在"**仅统计**"模式下运行。 • 红色 –"应用程序启动控制"任务未运行或失败。
应用程序启动控制	**任务状态** - 当前任务状态，例如，"*正在运行*"或"*已停止*"。 **运行模式** –"应用程序启动控制"任务的两种可用模式之一："**活动**"或"**仅统计**"。 **应用程序启动被拒绝** – 在"应用程序启动控制"任务运行期间，尝试启动 Kaspersky Embedded Systems Security 已阻止的应用程序的次数。如果已阻止的应用程序启动次数超过 0，则该字段为红色。 **平均处理时间(毫秒)** – Kaspersky Embedded Systems Security 处理尝试在受保护设备上启动应用程序所用的时间。
设备控制	**任务状态** - 当前任务状态，例如，"*正在运行*"或"*已停止*"。 **运行模式** –"设备控制"任务的两种可用模式之一："**活动**"或"**仅统计**"。 **已阻止的设备** – 在执行"设备控制"任务期间，Kaspersky Embedded Systems Security 阻止的连接外部设备的尝试次数。如果已阻止的外部设备数量超过 0，则该字段值为红色。
防火墙管理	**任务状态** - 当前任务状态，例如，"*正在运行*"或"*已停止*"。 **阻止的连接尝试次数** – 被指定防火墙规则阻止的与受保护设备的连接的数量。

诊断

"**诊断**"部分（请参见下表）显示有关"文件完整性监控"和"日志审查"任务的信息。

有关系统审查状态的信息

“诊断”部分	信息
诊断状态指示器	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下值： • 绿色 – 默认显示此颜色，指示一个或两个系统审查组件已安装，且任务正在运行。 • 黄色 – 两个组件均已安装，但其中一个系统审查任务未运行；发生“*未运行*”事件。 • 红色 - 其中一个任务失败。
文件完整性监控	**任务状态** - 当前任务状态，例如，“*正在运行*”或“*已停止*”。 **未批准的文件操作** – 对监控范围内的文件的更改次数。这些更改可能表示受保护设备遭到安全入侵。
日志审查	**任务状态** - 当前任务状态，例如，“*正在运行*”或“*已停止*”。 **所配置规则的违规** – 根据来自 Windows 事件日志的数据，所记录的违规数量。基于指定的任务规则或使用启发式分析来确定此数量。

Kaspersky Embedded Systems Security 授权信息显示在 **Kaspersky Embedded Systems Security** 节点的详细信息窗格左下角的行中。

您可以按照应用程序属性配置 Kaspersky Embedded Systems Security 属性。

可以按照“连接至其他计算机”链接连接到其他受保护设备。

从 Web 控制台和云控制台使用 Web 插件

本节提供有关 Kaspersky Embedded Systems Security 管理插件的信息，并介绍如何管理一台或一组受保护设备上安装的应用程序。

从 Web 控制台和云控制台管理 Kaspersky Embedded Systems Security

您可以通过 Kaspersky Embedded Systems Security Web 插件，使用安装并包含在管理组中的 Kaspersky Embedded Systems Security 集中管理多个受保护的设备。Kaspersky Security Center Web 控制台和 Kaspersky Security Center 云控制台还运行您分别配置管理组中的每个受保护设备。

*管理组*在 Kaspersky Security Center Web 控制台上手动创建。该组包括您要为其配置相同的控制和保护设置并已安装了 Kaspersky Embedded Systems Security 的多个设备。有关使用管理组的详细信息，请参见 *Kaspersky Security Center 帮助*。

如果 Kaspersky Embedded Systems Security 在某台受保护设备上的运行受活动 Kaspersky Security Center 策略的控制，则该台受保护设备的应用程序设置不可用。

可通过以下方式通过 Kaspersky Security Center Web 控制台管理 Kaspersky Embedded Systems Security：

- **使用 Kaspersky Security Center 策略**。可使用 Kaspersky Security Center 策略为一组设备远程配置相同的保护设置。在活动策略中指定的任务设置的优先级高于在应用程序控制台中本地配置或在 Kaspersky Security Center Web 控制台的设备属性窗口中远程配置的任务设置。您可使用策略配置常规应用程序设置、实时计算机保护任务设置、本地活动控制任务设置和计划的本地系统任务启动设置。

- **使用 Kaspersky Security Center 组任务**。使用 Kaspersky Security Center 组任务可远程配置任务的通用设置，一组设备具有过期期限。您可使用组任务激活应用程序，配置“按需扫描”任务设置，更新任务设置，以及“应用程序启动控制规则生成器”任务设置。

- **使用一组设备的任务**。使用一组设备的任务允许远程配置通用任务设置，不属于任何管理组的受保护设备具有有限执行期限。

- **使用单个设备的属性窗口**。在设备属性窗口中，您可远程配置管理组中包含的单台受保护设备的任务设置。如果选中的受保护设备不受活动 Kaspersky Security Center 策略的控制，您可配置常规应用程序设置和所有 Kaspersky Embedded Systems Security 任务的设置。

Kaspersky Security Center Web 控制台和 Kaspersky Security Center 云控制台允许您配置应用程序设置和高级功能，并可使用日志和通知。您可以为一组受保护设备和单台受保护设备配置这些设置。

Web 插件限制

与 Kaspersky Embedded Systems Security 管理插件相比，Kaspersky Embedded Systems Security Web 插件具有以下限制：

- 要添加用户或用户组，您需要使用安全描述符定义语言 (SDDL) 指定安全描述符字符串。

- 无法为“实时文件保护”任务更改预定义安全级别。

- 无法使用数字证书或 Kaspersky Security Center 事件创建“应用程序启动控制”任务规则。

- 无法根据连接的设备或系统数据生成“设备控制”任务规则。

管理应用程序设置

本部分包含有关在 Kaspersky Security Center Web 控制台中配置 Kaspersky Embedded Systems Security 常规设置的信息。

在 Web 插件中配置常规应用程序设置

您可以在 Web 插件中为一组受保护设备或一台受保护设备配置 Kaspersky Embedded Systems Security 常规设置。

在 Web 插件中配置扩展性、界面和扫描设置

要配置扩展性设置和应用程序界面：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**应用程序设置**”部分。
5. 在“**扩展性、界面和扫描设置**”子部分中，单击“**设置**”。
6. 按下表所述配置设置。

扩展性设置

设置	描述
自动检测扩展性设置	Kaspersky Embedded Systems Security 自动控制使用的进程数量。 这是默认值。
手动设置工作进程数	Kaspersky Embedded Systems Security 根据指定的值控制有效的工作进程数。
用于实时保护的进程数	实时计算机保护任务组件使用的最大进程数。如果选择了“**手动设置工作进程数**”选项，该输入字段才可用。
后台按需扫描任务的进程数	在后台模式下运行“按需扫描”任务时“按需扫描”组件使用的最大进程数。如果选择了“**手动设置工作进程数**”选项，该输入字段才可用。
在任务栏中显示系统托盘图标	配置是否在通知区域中显示系统托盘图标。
扫描后还原文件属性	当 Kaspersky Embedded Systems Security 执行按需扫描任务时，每个被扫描文件的上次访问时间都会更新。扫描后，Kaspersky Embedded Systems Security 会将文件的上次访问时间重置为初始值。 此行为可能导致为未更改的文件创建备份副本，从而影响备份系统的工作。这也可能导致文件更改跟踪应用程序中出现错误检测。

	默认情况下，启用此选项。
限制扫描线程的 CPU 使用率	Kaspersky Embedded Systems Security 在按需扫描任务期间会将对受保护设备 CPU 的使用率限制为“**上限(百分比)**”字段中指定的值。 启用此选项可能会对 Kaspersky Embedded Systems Security 的性能产生负面影响。 默认情况下，禁用此选项。
上限(百分比)	Kaspersky Embedded Systems Security 的最大允许 CPU 使用率。 如果选择了“限制扫描线程的 CPU 使用率”选项，则该输入字段可用。
用于存储在扫描期间创建的临时文件的文件夹	Kaspersky Embedded Systems Security 在扫描期间需要将压缩文件解压缩到的文件夹。 默认情况下，使用 C:\Windows\Temp 文件夹。
HSM 系统设置	选择用于访问分级存储的选项。

在 Web 插件中配置安全设置

若要手动配置安全性设置，请执行以下步骤：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**应用程序设置**”部分。
5. 单击“**安全性和可靠性**”子部分中的“**设置**”。
6. 按下表所述配置设置。

安全性设置

设置	描述
保护应用程序进程免受外部威胁	如果选中“保护应用程序进程免受外部威胁”复选框，应用程序将保护其进程，防止被注入代码或进程数据被访问。 启用或禁用该选项时，无需重新启动应用程序服务即可应用更改。 默认启用该选项。
执行任务恢复	该复选框用于允许或禁止当应用程序返回错误或终止时 Kaspersky Embedded Systems Security 任务的恢复。 如果选中该复选框，则当应用程序返回错误或终止时，Kaspersky Embedded Systems Security 会自动恢复 Kaspersky Embedded Systems Security 任务。 如果清除该复选框，则当应用程序返回错误或终止时，Kaspersky Embedded Systems Security 不会恢复 Kaspersky Embedded Systems Security 任务。 默认选中该复选框。

恢复按需扫描任务的尝试次数不超过 (1 - 10)	Kaspersky Embedded Systems Security 返回错误后尝试恢复“按需扫描”任务的次数。如果选中“**执行任务恢复**”复选框，则该输入字段才可用。
不启动已计划扫描任务	该复选框用于启用或禁用在受保护设备切换为 UPS 电源后、恢复标准电源前启动计划扫描任务。 如果选中该复选框，在受保护设备切换为 UPS 电源后、恢复标准电源前 Kaspersky Embedded Systems Security 不会启动计划扫描任务。 如果清除该复选框，不论电源如何，Kaspersky Embedded Systems Security 都会启动计划扫描任务。 默认选中该复选框。
停止当前扫描任务	该复选框用于启用或禁用在受保护设备切换为 UPS 电源后运行扫描任务的选项。 如果选中该复选框，Kaspersky Embedded Systems Security 会在受保护设备切换为 UPS 电源后暂停运行扫描任务。 如果清除该复选框，Kaspersky Embedded Systems Security 会在受保护设备切换为 UPS 电源后继续运行扫描任务。 默认选中该复选框。
应用密码保护	设置密码以保护对 Kaspersky Embedded Systems Security 功能的访问。

在 Web 插件中配置连接设置

配置的连接设置用于将 Kaspersky Embedded Systems Security 连接到更新和激活服务器，以及在将应用程序与 KSN 服务集成期间使用。

若要配置连接设置，请执行以下步骤：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**应用程序设置**”部分。
5. 在“**扩展性、界面和扫描设置**”子部分中，单击“**设置**”。
6. 按下表所述配置设置。

连接设置

设置	描述
不使用代理服务器	如果选择此选项，Kaspersky Embedded Systems Security 会直接连接到 KSN 服务，而不使用任何代理服务器。
使用指定的代理服务器设置	如果选择此选项，Kaspersky Embedded Systems Security 会使用手动指定的代理服务器设置连接到 KSN。
对于本地地址不使用代理服务器	此复选框用于在访问与安装了 Kaspersky Embedded Systems Security 的受保护设备位于同一网络上的设备时启用或禁用代理服务器。

	如果选中该复选框，则会直接通过托管已安装了 Kaspersky Embedded Systems Security 的受保护设备的网络访问设备。不使用代理服务器。 如果清除该复选框，将使用代理服务器连接到本地设备。 默认选中该复选框。
代理服务器身份验证设置	指定身份验证设置
不使用身份验证	不执行身份验证。默认选择该方式。
使用 NTLM 身份验证	使用由 Microsoft 开发的 NTLM 网络身份验证协议执行身份验证。
使用带用户名和密码的 NTLM 身份验证	使用由 Microsoft 开发的 NTLM 网络身份验证协议执行带用户名和密码的身份验证。
应用用户名和密码	使用用户名和密码执行身份验证。

配置本地系统任务的计划启动

您可以使用策略来允许或阻止本地系统“按需扫描”任务和“更新”任务的启动。此操作根据管理组中每个受保护设备上本地配置的计划来完成：

- 如果特定类型的本地系统任务的计划启动受到策略禁止，则这些任务将不会按照计划在受保护设备上执行。您可以手动启动该本地系统任务。
- 如果特定类型的本地系统任务的计划启动被策略允许，则这些任务将按照为此任务进行的本地配置的计划参数来执行。

默认情况下，策略会禁止本地系统任务的启动。

如果更新或按需扫描受 Kaspersky Security Center 组任务的管理，我们推荐不要允许本地系统任务启动。

如果不使用组更新或按需扫描任务，则允许在策略中启动本地系统任务：Kaspersky Embedded Systems Security 将执行应用程序数据库和模块更新，并根据默认计划启动所有本地系统按需扫描任务。

您可使用策略允许或阻止以下本地系统任务的计划启动：

- 按需扫描任务：关键区域扫描、隔离区扫描、在操作系统启动时扫描、应用程序完整性控制、基线文件完整性监控。
- 更新任务：数据库更新、软件模块更新、复制更新。

如果受保护设备被从管理组中排除，将自动启用本地系统任务计划。

要在策略中允许或阻止 Kaspersky Embedded Systems Security 本地系统任务的计划启动：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。

2. 单击要配置的策略名称。

3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。

4. 选择“**应用程序设置**”部分。

5. 单击“**运行本地系统任务**”子部分中的“**设置**”。

6. 按下表所述配置设置。

本地系统任务的计划启动设置

设置	描述
允许启动按需扫描任务	选中或清除该复选框可允许或禁止按需扫描任务的计划启动。
允许启动更新任务和复制更新任务	选中或清除该复选框可允许或禁止更新任务和复制更新任务的计划启动。

在 Web 插件中配置隔离和备份设置

要在 Kaspersky Security Center 中配置常规隔离和备份设置：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。

2. 单击要配置的策略名称。

3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。

4. 选择“**补充**”部分。

5. 单击“**存储**”子部分中的“**设置**”。

6. 按下表所述配置设置。

隔离和备份设置

设置	描述
备份文件夹	指定备份文件夹。
最大备份容量(MB)	设置最大备份容量。
可用空间阈值(MB)	指定备份文件夹中的可用空间最小值。
用于还原对象的目标文件夹	指定用于保存恢复对象的文件夹。
隔离区文件夹	指定备份文件夹。
隔离区最大容量(MB)	设置最大备份容量。
可用空间阈值(MB)	指定备份文件夹中的可用空间最小值。
用于还原对象的目标文件夹	指定用于保存恢复对象的文件夹。
网络会话阻止期限	指定被阻止的网络会话在多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

创建和配置策略

本节提供有关使用 Kaspersky Security Center 策略在多个受保护设备上管理 Kaspersky Embedded Systems Security 的信息。

可以创建全局性 Kaspersky Security Center 策略，以便管理多个安装了 Kaspersky Embedded Systems Security 的设备上的保护。

策略在一个管理组的所有受保护设备上实施指定的 Kaspersky Embedded Systems Security 设置、功能和任务。

可以为一个管理组依次创建和实施多个策略。该策略当前对管理控制台中具有*活动*状态的组有效。

Kaspersky Embedded Systems Security 系统审核日志中记录了有关策略实施情况的信息。可在应用程序控制台的“**系统审核日志**”节点中查看该信息。

Kaspersky Security Center 提供一种在受保护设备上应用策略的方式：*禁止更改策略*。应用策略后，Kaspersky Embedded Systems Security 将使用您在受保护设备上的策略属性中为其选择了图标的设置。在这种情况下，将使用所选设置，而不是应用策略之前生效的设置。Kaspersky Embedded Systems Security 不会应用在策略属性中为其选择了 图标的活动策略设置。

如果策略为活动的，则策略中标记 图标的设置的值在应用程序控制台中显示，但无法编辑。其他设置的值（策略中标记 图标）可在应用程序控制台中编辑。

活动策略中配置的且标记 图标的设置也会阻止在 Kaspersky Security Center 的“**属性：<受保护设备名称>**”窗口中针对一台受保护设备进行更改。

在禁用活动策略后，使用活动策略指定并发送到受保护设备的设置将保存在本地任务设置中。

如果策略为任何实时计算机保护任务定义了设置，并且如果此类任务当前正在运行，则一旦应用该策略，便将立即修改该策略所定义的设置。如果任务未运行，则设置将在该任务启动时应用。

创建策略

要创建策略：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击“**添加**”按钮。
3. 将打开“**新建策略**”窗口。
4. 在“**选择应用程序**”部分中，选择 Kaspersky Embedded Systems Security，然后单击“**下一步**”。
5. 在“**常规**”选项卡上，可以执行以下操作：
   - 更改策略名称。

     策略名称不能包含以下符号：" * < : > ? \ | 。

- 选择策略状态：
  - **活动**。下一次同步后，该策略将用作计算机上的活动策略。
  - **非活动**。备份策略。如有必要，可以将非活动策略切换为活动状态。
  - **漫游**。当计算机离开组织网络周界时，将激活该策略。
- 配置设置的继承：
  - **从父策略继承设置**。如果开启此切换按钮，则策略设置值从顶级策略继承。如果为父策略设置了，则无法编辑策略设置。
  - **强制继承子策略中的设置**。如果该切换按钮开启，则策略设置的值将传播到子策略。在子策略设置中，将自动选中"**从父策略继承设置**"复选框。子策略设置继承自父策略，但标记了 的设置除外。如果为父策略设置了，则无法编辑子策略设置。

6. 在"**应用程序设置**"选项卡上，根据需要配置策略设置。

7. 单击"**保存**"。

所创建的策略将显示在选定管理组的"**策略和配置文件**"选项卡上的策略列表中。在"**<策略名称>**"窗口中，您可配置 Kaspersky Embedded Systems Security 的其他设置、任务和功能。

创建新策略后，会创建一组允许规则，以防止应用程序被阻止并确保其持续运行。您可以在任务设置中查看默认规则。以下是详细信息和限制。

默认情况下，Kaspersky Embedded Systems Security 会在您创建新策略时为传入网络流量创建一组规则：

- Kaspersky Security Center 网络代理 Windows 桌面共享进程的两个允许规则位于 %Program Files% 和 %Program Files (x86)%。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- 本地端口 15000 的两个允许规则。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。

默认情况下，Kaspersky Embedded Systems Security 在您创建新策略时为传出网络流量创建一组规则：

- Kaspersky Embedded Systems Security 服务的两个允许规则位于 %Program Files% 和 %Program Files (x86)%。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- Kaspersky Embedded Systems Security 工作流程的两个允许规则位于 %Program Files% 和 %Program Files (x86)%。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- 本地端口 13000 的两个允许规则。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。

Kaspersky Embedded Systems Security 策略设置部分

常规

在“**常规**”部分中，您可配置以下策略设置：

- 指定策略状态。
- 为父策略和子策略配置继承设置。

事件配置

在“**事件配置**”部分中，您可配置以下事件类别的设置：

- *严重事件*
- *功能故障*
- *警告*
- *信息消息*

可以使用“**属性**”按钮来配置选定事件的以下设置：

- 指定有关记录事件的信息的存储位置和保留期限。
- 指定所记录事件的通知方式。

应用程序设置

应用程序设置的设置部分

部分	选项
扩展性、界面和扫描设置	在“**扩展性、界面和扫描设置**”子部分中，可以单击“**设置**”按钮来配置以下设置： • 选择手动或自动配置扩展性设置。 • 配置应用程序图标显示设置。
安全性和可靠性	在“**安全性和可靠性**”子部分中，可以单击“**设置**”按钮来配置以下设置： • 配置任务运行设置。 • 指定当受保护设备使用 UPS 电源运行时应用程序的行为。 • 启用或禁用应用程序功能的密码保护。
连接	在“**连接**”子部分中，可以使用“**设置**”按钮来配置与更新服务器、激活服务器和 KSN 连接的以下代理服务器设置： • 配置代理服务器设置。 • 指定代理服务器身份验证设置。
运行本地系统任务	在“**运行本地系统任务**”子部分中，可以使用“**设置**”按钮来根据受保护设备上配置的计划允许或阻止启动以下本地系统任务： • 按需扫描任务。

	• 更新任务和复制更新任务。

补充

补充的设置部分

部分	选项
信任区域	单击“**信任区域**”子部分上的“**设置**”按钮，以配置以下信任区域应用程序设置： • 创建信任区域排除项列表。 • 启用或禁用文件备份操作的扫描。 • 创建受信任进程列表。
可移动驱动器扫描	在“**可移动驱动器扫描**”子部分中，可以使用“**设置**”按钮来配置可移动驱动器的扫描设置。
应用程序管理的用户访问权限	在“**应用程序管理的用户访问权限**”子部分中，可以配置管理 Kaspersky Embedded Systems Security 的用户权限和用户组权限。
Kaspersky Security 服务管理的用户访问权限	在“**Kaspersky Security 服务管理的用户访问权限**”子部分中，可以配置管理 Kaspersky Security 服务的用户权限和用户组权限。
存储	在“**存储**”子部分中，单击“**设置**”按钮以配置以下“隔离”、“备份”和“阻止的主机”设置： • 指定您想要放置隔离或备份对象的文件夹的路径。 • 配置备份和隔离的最大大小，并指定可用空间阈值。 • 指定您想要放置从隔离区或备份区恢复的对象的文件夹路径。 • 配置关于隔离和备份对象到管理服务器的信息的传输。 • 配置阻止主机的时长。

实时计算机保护

实时服务器保护的设置部分

部分	选项
实时文件保护	在“**实时文件保护**”子部分中，可以单击“**设置**”按钮来配置以下任务设置： • 指定保护模式。 • 配置启发式分析的使用。 • 配置信任区域的使用。 • 指定保护范围。 • 设置选定保护范围的安全级别：您可选择预定义的安全级别或手动配置安全性设置。

	• 配置任务启动设置。
KSN 使用	在“KSN 使用”子部分中，可以单击“设置”按钮来配置以下任务设置： • 指定要对 KSN 不信任的对象执行的操作。 • 配置 Kaspersky Security Center 作为 KSN 代理服务器的数据传输和使用。
漏洞利用防御	在“漏洞利用防御”子部分中，可以单击“设置”按钮来配置以下任务设置： • 选择进程内存保护模式。 • 指定降低漏洞利用风险的操作。 • 添加到和编辑受保护的进程列表。

本地活动控制

“本地活动控制的设置”部分

部分	选项
应用程序启动控制	在“应用程序启动控制”子部分中，可以单击“设置”按钮来配置以下任务设置： • 选择任务运行模式。 • 配置控制随后应用程序启动的设置。 • 指定应用程序启动控制规则的范围。 • 配置 KSN 的使用。 • 配置任务启动设置。
设备控制	在“设备控制”子部分中，可以单击“设置”按钮来配置以下任务设置： • 选择任务运行模式。 • 配置任务启动设置。

网络活动控制

网络活动控制的设置部分

部分	选项
防火墙管理	在“防火墙管理”子部分中，可以单击“设置”按钮来配置以下任务设置： • 配置防火墙规则。 • 配置任务启动设置。

系统审查

系统审查的设置部分

部分	选项
文件完整性监控	在“**文件完整性监控**”子部分中，可以配置对表示受保护设备上遭到安全入侵的文件更改的控制。
日志审查	在“**日志审查**”部分中，可以根据 Windows 事件日志分析结果配置受保护设备的完整性监控。

日志和通知

日志和通知的设置部分

部分	选项
任务日志	在“**任务日志**”子部分中，可以单击“**设置**”按钮来配置以下设置： • 为选定的软件组件指定日志事件的重要性级别。 • 指定任务日志存储设置。 • 指定 SIEM 与 Kaspersky Security Center 的集成的设置。
事件通知	在“**事件通知**”子部分中，可以单击“**设置**”按钮来配置以下设置： • 指定“*检测到对象*”、“*检测到并限制不受信任的大容量存储*”和“*不信任主机列表*”事件的用户通知设置。 • 为“**通知设置**”部分中的事件列表中选定的任何事件指定管理员通知设置。
与管理服务器交互	在“**与管理服务器交互**”子部分中，可以单击“**设置**”按钮来选择 Kaspersky Embedded Systems Security 将报告给管理服务器的对象类型。

修订历史

在“**修订历史**”部分中，可以管理修订：与当前版本或其他策略对比、添加修订说明、保存修订到文件或执行回滚。

使用 Kaspersky Security Center 创建和配置任务

本节包含有关 Kaspersky Embedded Systems Security 任务、如何创建任务、配置任务设置，以及启动和停止任务的信息。

关于 Web 插件中的任务创建

您可为管理组和受保护设备集创建组任务。可以创建以下类型的任务：

- 激活应用程序

- 复制更新
- 数据库更新
- 软件模块更新
- 数据库更新回滚
- 按需扫描
- 应用程序完整性控制
- 基线文件完整性监控
- 应用程序启动控制规则生成器
- 设备控制规则生成器

您可采用以下方式创建本地和组任务：

- 对于一台受保护设备：在“**属性 <受保护设备名称>**”窗口的“**任务**”部分中。
- 对于管理组：在选定受保护设备组的节点的详细信息窗格中的“**任务**”选项卡上。
- 对于一组受保护设备：在“**设备选择**”节点的详细信息窗格中。

> 您可以使用策略禁用同一管理组中所有受保护服务器上的更新和按需扫描本地系统任务的计划。

有关 Kaspersky Security Center 中任务的常规信息，请参见 *Kaspersky Security Center 帮助*。

在 Web 插件中创建任务

要在 Kaspersky Security Center 管理控制台中创建新任务：

1. 采用以下方式之一启动任务向导：
   - 若要创建本地任务：
     a. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。
     b. 单击“**组**”选项卡以选择受保护设备所属的管理组。
     c. 单击受保护设备名称。
     d. 在打开的“**<设备名称>**”窗口中，选择“**任务**”选项卡。
     e. 单击“**添加**”。
   - 创建组任务：
     a. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。
     b. 单击“**组**”选项卡以选择要为其创建任务的管理组。

c. 单击“**添加**”。

- 要为自定义的一组受保护设备创建任务：

  a. 在 Web 控制台的主窗口中，选择“**设备**”→“**设备选择**”。

  b. 选择要为其创建任务的选择项。

  c. 单击“**开始**”。

  d. 在“**选择结果**”窗口中，选择要为其创建任务的设备。

  e. 单击“**新建任务**”。

将打开任务向导窗口。

2. 在“**应用程序**”下拉列表中，选择“**Kaspersky Embedded Systems Security**”。

3. 在“**任务类型**”下拉列表中，选择要创建的任务的类型。

   如果选择了除“数据库更新回滚”、“应用程序完整性控制”或“应用程序激活”以外的任何任务类型，将打开设置窗口。

4. 根据所选的任务类型，执行下列操作之一：

   - 创建按需扫描任务。
   - 要创建更新任务，请根据您的需要配置任务设置：

     a. 在“**数据库更新源**”部分中选择更新源。

     b. 在“**连接设置**”窗口中，配置代理服务器设置。

   - 在创建“软件模块更新”任务后，在“**软件模块更新**”窗口中配置所需应用程序模块更新设置：

     a. 选择是复制并安装关键软件模块更新，还是仅检查它们的可用性而不安装。

     b. 如果选择了“**复制并安装关键软件模块更新**”：则可能需要重启受保护设备才能应用已安装的软件模块。如果希望任务完成时 Kaspersky Embedded Systems Security 自动重新启动受保护设备，请选中“**允许操作系统重启**”复选框。

     c. 若要获得有关 Kaspersky Embedded Systems Security 模块升级的信息，请选择“**接收有关可用的计划软件模块更新的信息**”。

     Kaspersky 不会在更新服务器上发布计划的更新软件包以供自动安装；您可以手动从 Kaspersky 网站下载这些更新软件包。可以配置有关“**有新的计划软件模块更新可用**”事件的管理员通知。该通知将包含我们网站的 URL，以便您从中下载计划的更新。

   - 要创建“复制更新”任务，请在“**复制更新**”窗口中指定更新集和目标文件夹。
   - 要创建“应用程序激活”任务：

     a. 在“**Kaspersky Security Center 存储中的密钥列表**”窗口中，指定您要用来激活应用程序的密钥文件。

     b. 如果您想要创建用于续订授权许可的任务，请选中“**作为附加密钥使用**”复选框。

   - 创建和配置“应用程序启动控制规则生成器”任务。

- 创建和配置“设备控制规则生成器”任务。

5. 单击“**下一步**”。
6. 如果是为一组受保护设备创建任务，请选择将执行该任务的受保护设备网络（或组）。
7. 单击“**下一步**”。
8. 如果要配置任务设置，请在“**完成创建**”窗口中选中“**创建完成后打开任务详细信息**”复选框。
9. 单击“**完成**”按钮。

所创建的任务将显示在“**任务**”列表中。

在 Web 插件中配置组任务

要为多个受保护设备配置组任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**<任务名称>**”窗口。
3. 根据所配置的任务类型，执行下列操作之一：
   - 要配置按需扫描任务：
     a. 在“**扫描范围**”部分中，配置扫描范围。
     b. 在“**选项**”部分中，配置任务优先级水平及与其他软件组件的集成。
   - 要配置更新任务，请根据您的需要调整任务设置：
     a. 在“**更新源**”部分中，配置更新源和代理服务器设置。
     b. 在“**优化**”部分中，配置磁盘子系统优化。
   - 若要配置“软件模块更新”任务，请在“**高级设置**”部分中选择要执行的操作：复制并安装软件模块的关键更新或仅进行检查。
   - 若要配置“复制更新”任务，请在“**复制更新设置**”部分中指定更新集和目标文件夹。
   - 要配置“激活应用程序”任务，请应用您要用于激活应用程序的密钥文件。如果您想要添加用于续订授权许可的激活码或密钥文件，请选中“**作为附加密钥使用**”复选框。
   - 要配置设备控制允许规则的自动生成，请指定将用于创建允许规则列表的设置。
4. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。
5. 在“**账户**”部分中的“**设置**”选项卡上，指定将使用其权限运行任务的账户。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
6. 单击“**保存**”。

将保存新配置的组任务设置。

在 Web 插件中配置激活应用程序任务

要配置“激活应用程序”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**<任务名称>**”窗口。
3. 在“**通用**”部分中，指定您要使用的密钥文件来激活应用程序。如果您想要添加用于延长授权许可的密钥，请选中“**作为附加密钥使用**”复选框。
4. 在“**计划**”部分中配置任务计划。
5. 在“**<任务名称>**”窗口中，单击“**确定**”。

在 Web 插件中配置更新任务

要配置“复制更新”、“数据库更新”或“软件模块更新”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**<任务名称>**”窗口。
3. 在“**更新源**”部分中，配置更新源设置：
   - 在“**数据库更新源**”部分中，将 Kaspersky Security Center 管理服务器或 卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。
     如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。

     > 要将 SMB 共享文件夹用作更新源，您需要指定用户账户以启动任务。

     > 通过云控制台配置更新任务时，只有“**分发点**”和“**卡巴斯基更新服务器**”设置可用于指定更新源。

   - 在“**连接设置**”部分中，配置使用代理服务器连接到 卡巴斯基更新服务器和其他服务器。
4. 在数据库更新任务的“**优化**”部分中，可以配置能够减少磁盘子系统工作负载的功能：
   - 磁盘 I/O 使用情况优化
   - 用于优化的 RAM (400 - 9999 MB)

5. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。

6. 在“**<任务名称>**”窗口中，单击“**确定**”。

在 Web 插件中配置故障诊断设置

如果在 Kaspersky Embedded Systems Security 运行期间出现问题（例如 Kaspersky Embedded Systems Security 崩溃），您可以对其进行诊断。为此，您可以为 Kaspersky Embedded Systems Security 进程启用跟踪文件和 Dump 文件的创建，并将这些文件发送给卡巴斯基技术支持进行分析。

Kaspersky Embedded Systems Security 不会自动发送任何跟踪或 Dump 文件。诊断数据只能由具有所需权限的用户发送。

Kaspersky Embedded Systems Security 会以未加密的形式将信息写入到跟踪文件和 Dump 文件。保存文件的文件夹由用户选择，由操作系统配置和 Kaspersky Embedded Systems Security 设置管理。您可以配置访问权限并只允许所需用户访问日志、跟踪文件和 dump 文件。

要在 Kaspersky Security Center 中配置故障诊断设置：

1. 在 Kaspersky Security Center 管理控制台中，打开“应用程序设置”窗口。

2. 打开“**故障诊断**”部分。

3. 如果希望应用程序将调试信息写入文件，请在“**故障排除设置**”子部分中选中“**启用跟踪**”复选框。

4. 在“**跟踪文件文件夹**”字段中，指定 Kaspersky Embedded Systems Security 将保存跟踪文件的本地文件夹的绝对路径。

   该文件夹必须事先创建，并且必须可供 SYSTEM 账户写入。您不能指定网络文件夹、驱动器和环境变量。

5. 配置调试信息的详细级别。

6. 指定**跟踪文件最大大小(MB)**。

   可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小设置为 50 MB。

7. 如果您希望应用程序在达到最大跟踪文件数后删除最早的文件，请选中“**删除最旧的跟踪文件**”复选框。

8. 指定**一个跟踪日志的最大文件数**。

   可用值：1 到 999。默认情况下，最大文件数设置为 5。该字段仅当选中“**删除最旧的跟踪文件**”复选框时才可用。

9. 如果您希望应用程序创建 Dump 文件，请选中“**创建 Dump 文件**”复选框。

10. 在“**Dump 文件文件夹**”字段中，指定 Kaspersky Embedded Systems Security 将保存 Dump 文件的本地文件夹的绝对路径。

    该文件夹必须事先创建，并且必须可供 SYSTEM 账户写入。您不能指定网络文件夹、驱动器和环境变量。

11. 单击“**确定**”。

已配置的应用程序设置将应用于受保护设备上。

管理任务计划

您可以配置 Kaspersky Embedded Systems Security 任务的启动计划，并配置按计划运行任务的设置。

计划任务

您可以在应用程序控制台中计划本地系统和自定义任务。您无法在应用程序控制台中计划组任务。

要使用 Web 插件计划组任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**<任务名称>**”窗口。
3. 选择“**应用程序设置**”部分。
4. 在“**计划**”部分中，选中“**按计划运行**”复选框。

   如果 Kaspersky Security Center 策略阻止按需扫描任务和更新任务的计划，则这些任务的计划设置字段将不可用。

5. 根据需要配置计划设置。为此，请执行以下操作：
   a. 在“**频率**”列表中，选择以下值之一：
      - **每小时**，如果您希望该任务在指定的小时数内间隔运行，请在“**每 <数量> 小时**”字段中指定小时数。
      - **每天**，如果您希望该任务在指定的天数内间隔运行，请在“**每 <数量> 天**”字段中指定天数。
      - **每周**，如果您希望该任务以指定周数为间隔运行，请在“**每 <数量> 周**”字段中指定周数。指定将启动任务的星期中的日期（默认在星期一启动任务）。
      - **应用程序启动时**，如果您希望在每次启动 Kaspersky Embedded Systems Security 时运行该任务。
      - **应用程序数据库更新后**，如果您希望在每次更新应用程序数据库后运行该任务。

   b. 在“**开始时间**”字段中指定首次启动任务的时间。
   c. 在“**开始日期**”字段中，指定计划启动的日期。
6. 在“**任务停止设置**”部分中：
   a. 选中“**持续时间**”复选框，并在右侧的字段中输入任务执行的最长持续时间（小时和分钟）。
   b. 选中“**暂停任务**”复选框，并在右侧的字段中输入暂停任务执行的时间间隔（小于 24 小时）的开始值和结束值。
7. 在“**高级计划设置**”部分中：

a. 选中“**取消计划**”复选框，并指定停止应用计划的日期。

b. 选中“**运行错过的任务**”复选框以允许启动跳过的任务。

c. 选中“**在该时间间隔内随机化任务开始时间**”复选框，并按分钟指定该值。

8. 单击“**保存**”按钮保存任务启动设置。

启用和禁用计划任务

可在配置计划设置之前或之后启用和禁用计划任务。

要启用或禁用任务启动计划：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**<任务名称>**”窗口。
3. 选择“**应用程序设置**”部分。
4. 选择“**计划**”部分。
5. 执行以下操作之一：
   - 如果您希望启用任务的启动计划，请选中“**按计划运行**”复选框。
   - 如果您希望禁用任务的启动计划，请清除“**按计划运行**”复选框。

     不会删除已配置的任务启动计划设置，并将在计划的下一次任务启动时间应用该设置。
6. 单击“**保存**”。

将保存已配置的任务启动计划设置。

Kaspersky Security Center 中的报告

Kaspersky Security Center 中的报告包含有关受管理设备状态的信息。报告基于管理服务器上存储的信息。

从 Kaspersky Security Center 11 开始，对于 Kaspersky Embedded Systems Security，以下类型的报告可用：

- 有关应用程序组件状态的报告
- 有关已禁止的应用程序的报告
- 有关在测试模式下禁止的应用程序的报告

有关所有 Kaspersky Security Center 报告以及如何配置它们的详细信息，请参阅 *Kaspersky Security Center 帮助*。

有关 Kaspersky Embedded Systems Security 组件状态的报告

您可以监视所有网络设备的保护状态，并获得每个设备上的组件集的结构化概览。

报告显示每个组件的以下状态之一：*正在运行*、*已暂停*、*已停止*、*故障*、*未安装*、*正在启动*。

*未安装*状态指的是组件，而不是应用程序本身。如果未安装应用程序，Kaspersky Security Center Web 控制台会分配 N/A（不可用）状态。

您可以创建组件选择并使用筛选来显示具有指定组件集和状态的网络设备。

有关创建和使用选择的详细信息，请参见 *Kaspersky Security Center 帮助*。

要在应用程序设置中查看组件的状态：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。
2. 单击受保护设备名称。
3. 在“**常规**”选项卡上，选择“**组件**”部分。
4. 查看状态表。

此表中不提供有关漏洞利用防御组件状态的信息。

要查看 Kaspersky Security Center Web 控制台标准报告：

1. 选择“**监控和报告**”→“**报告**”。
2. 选择“**有关应用程序组件状态的报告**”列表项，然后单击“**显示报告**”按钮。
   将生成报告。
3. 查看以下报告详细信息：
   - 图形化图表。
   - 组件和安装了每个组件的网络设备总数以及设备所属的组的汇总表格。
   - 指定了组件状态、版本、设备和组的详细表格。

有关在活动模式和测试模式下禁止的应用程序的报告

根据“应用程序启动控制”任务的结果，可以生成两种类型的报告：有关已禁止的应用程序的报告（如果在活动模式下启动该任务）和有关在测试模式下禁止的应用程序的报告（如果在仅统计模式下启动该任务）。这两种报告显示了有关网络的受保护设备上阻止的应用程序的信息。每个报告都针对所有管理组生成，并累积来自受保护设备上安装的所有 Kaspersky 应用程序的数据。

要查看有关在仅统计模式下禁止的应用程序的报告：

1. 在“仅统计”模式下启动“应用程序启动控制”任务。
2. 选择“**监控和报告**”→“**报告**”。
3. 选择“**有关在测试模式下禁止的应用程序的报告**”列表项，然后单击“**显示报告**”按钮。
   将生成报告。
4. 查看以下报告详细信息：
   - 显示阻止启动次数最多的前 10 个应用程序的图形化图表。
   - 应用程序阻止行为的汇总表格，其中指定可执行文件名、原因、阻止时间和发生阻止的设备数量。
   - 指定了有关设备、文件路径和阻止条件的数据的详细表格。

要查看有关在活动模式下禁止的应用程序的报告：

1. 在“活动”模式下启动“应用程序启动控制”任务。
2. 选择“**监控和报告**”→“**报告**”。
3. 选择“**有关在测试模式下禁止的应用程序的报告**”列表项，然后单击“**显示报告**”按钮。
   将生成报告。

此报告包含的阻止数据与有关在测试模式下禁止的应用程序的报告相同。

小型诊断窗口

本节介绍如何使用小型诊断窗口查看受保护设备状态或当前活动，以及如何配置 dump 和跟踪文件写入。

关于小型诊断窗口

“小型诊断窗口”组件（也称为“CDI”）连同“系统托盘图标”组件独立于应用程序控制台安装和卸载，可在受保护设备上未安装应用程序控制台时使用。CDI 通过系统托盘图标启动，或通过运行受保护设备上的应用程序文件夹中的 kavfsmui.exe 启动。

在 CDI 窗口中可执行以下操作：

- 查看有关常规应用程序状态的信息。
- 查看已发生的安全事件。
- 查看受保护设备上的当前活动。
- 启动或停止写入 dump 和跟踪文件。
- 打开应用程序控制台。
- 打开含有已安装更新和可用补丁列表的“**关于应用程序**”窗口。

即使对 Kaspersky Embedded Systems Security 功能的访问受密码保护，CDI 仍然可用。无需任何密码。

CDI 组件不能通过 Kaspersky Security Center 进行配置。

通过小型诊断窗口查看 Kaspersky Embedded Systems Security 状态

要打开“小型诊断窗口”窗口，请执行以下操作：

1. 右键单击工具栏通知区域中的 Kaspersky Embedded Systems Security 系统托盘图标。
2. 选择“**打开小型诊断窗口**”选项。
   “**小型诊断窗口**”窗口将打开。

在“**保护状态**”选项卡上查看密钥、实时计算机保护任务和更新任务的当前状态。使用不同的颜色来向用户通知保护状态（参见下表）。

小型诊断窗口保护状态。

部分	状态
实时保护状态	在以下任一情况（满足任意条件）下，面板呈*绿色*： • 推荐配置： • “实时文件保护”任务以默认设置启动。

	• “应用程序启动控制”任务在“**活动**”模式下以默认设置启动。
	• 可接受配置：
	  • “实时文件保护”任务由用户配置。
	  • “应用程序启动控制”任务设置被修改。

	如果满足以下一个或多个条件，面板呈*黄色*： • “实时文件保护”任务暂停（用户暂停或按计划暂停）。 • “应用程序启动控制”任务在“**仅统计**”模式下启动。 • “漏洞利用防御”和“应用程序启动控制”在“**仅统计**”模式下启动。
	如果同时满足以下两个条件，面板呈*红色*： • “实时文件保护”组件未安装或者任务停止或暂停。 • “应用程序启动控制”组件未安装或任务在“**仅统计**”模式下启动。
授权	如果当前授权许可有效，面板呈*绿色*。
	*黄色*面板表示发生以下事件之一： • *检查授权许可状态*。 • *授权许可将在 14 天后过期，且未添加附加密钥或激活码。* • *添加的密钥已被添加到拒绝列表且将被阻止。*
	*红色*面板表示发生以下事件之一： • *应用程序未激活* • *授权许可已过期* • *已违反最终用户授权许可协议* • *密钥在拒绝列表中*
更新	应用程序数据库处于最新状态时，面板呈*绿色*。
	应用程序数据库已过期时，面板呈*黄色*。
	应用程序数据库已严重过期时，面板呈*红色*。

查看安全事件统计

“**统计**”选项卡显示所有安全事件。单独块中显示的每个保护任务统计说明了事件数量和上次发生事件的日期和时间。记录某个事件后，块颜色变为红色。

要查看统计：

1. 右键单击工具栏通知区域中的 Kaspersky Embedded Systems Security 系统托盘图标。
2. 选择“**打开小型诊断窗口**”选项。
   “**小型诊断窗口**”窗口将打开。
3. 打开“**统计**”选项卡。
4. 查看保护任务的安全事件。

查看当前应用程序活动

在该选项卡上，您可以查看当前任务和应用程序进程的状态，并迅速获得关于所发生的严重事件的通知。

使用不同的颜色指示应用程序活动状态：

- 在“**任务**”部分中：
  - *绿色*。没有达到显示黄色或红色的条件。
  - *黄色*。很长时间未扫描关键区域。
  - *红色*。符合以下至少一个条件：
    - 未启动任何任务和没有为任何任务设置启动计划。
    - 应用程序启动错误将记录为严重事件。
- 在“**卡巴斯基安全网络**”部分中：
  - *绿色*。“KSN 使用”任务已启动。
  - *黄色*。KSN 声明被接受，但任务未启动。

要查看受保护设备上的当前应用程序活动：

1. 右键单击工具栏通知区域中的 Kaspersky Embedded Systems Security 系统托盘图标。
2. 选择“**打开小型诊断窗口**”选项。
   “**小型诊断窗口**”窗口将打开。
3. 打开“**当前应用程序活动**”选项卡。
4. 在“**任务**”部分中查看以下信息：
   - **长时间未扫描关键区域。**

     仅当应用程序返回相应的关键区域扫描警告时，才会显示该字段。

   - **正在运行**
   - **执行失败**

- 由计划定义的下次启动

5. 在“卡巴斯基安全网络”部分中查看以下信息：
   - KSN 已开启，文件信誉服务已启用或保护关闭。
   - KSN 已开启，文件信誉服务已启用，应用程序统计信息正在发送到 KSN。

     应用程序将发送有关在“实时文件保护”任务和“按需扫描”任务执行过程中检测到的恶意软件（包括欺诈软件）的信息，以及有关扫描过程中的错误的调试信息。
     如果在“KSN 使用”任务设置中选中“发送卡巴斯基安全网络统计信息”复选框，将显示该字段。

6. 在“与 Kaspersky Security Center 集成”部分中查看以下信息：
   - 允许本地管理。
   - 已应用策略：<管理服务器名称>。

配置 Dump 和跟踪文件写入

您可以通过 CDI 配置 dump 和跟踪文件的写入。

还可以通过应用程序控制台配置故障诊断。

要开始写入 dump 和跟踪文件，请执行以下操作：

1. 右键单击工具栏通知区域中的 Kaspersky Embedded Systems Security 系统托盘图标。
2. 选择“打开小型诊断窗口”选项。
   “小型诊断窗口”窗口将打开。
3. 打开“故障排除”选项卡。
4. 如果必要，更改以下跟踪设置：
   a. 选中启用跟踪复选框。
   b. 单击“浏览”按钮以指定 Kaspersky Embedded Systems Security 将会保存跟踪文件的文件夹。
      将对所有组件启用跟踪（采用默认参数，使用“*调试*”级别的详细信息，默认最大日志大小为 50 MB）。
5. 如果必要，更改以下 Dump 文件设置：
   a. 选中“在以下文件夹中创建故障 Dump 文件”复选框。
   b. 单击“浏览”按钮以指定 Kaspersky Embedded Systems Security 将会保存 Dump 文件的文件夹。
6. 单击“应用”按钮。
   将应用新配置。

更新 Kaspersky Embedded Systems Security 数据库和软件模块

本节提供有关 Kaspersky Embedded Systems Security 数据库和软件模块更新任务、复制更新和回滚 Kaspersky Embedded Systems Security 数据库更新的信息，以及有关如何配置数据库和软件模块更新任务的说明。

关于更新任务

Kaspersky Embedded Systems Security 提供四种系统更新任务：数据库更新、软件模块更新、复制更新和数据库更新回滚。

默认情况下，Kaspersky Embedded Systems Security 每小时连接一次更新源（Kaspersky 的更新受保护设备之一）。您可配置所有更新任务，除“数据库更新回滚”任务外。修改了任务设置后，Kaspersky Embedded Systems Security 会在下次启动任务时应用新值。

不允许暂停和恢复更新任务。

数据库更新

默认情况下，Kaspersky Embedded Systems Security 会将数据库从更新源复制到设备，并通过运行“实时计算机保护”任务来立即开始使用这些数据库。“按需扫描”任务在下次启动时开始使用更新的数据库。

默认情况下，Kaspersky Embedded Systems Security 每小时运行一次“数据库更新”任务。

软件模块更新

默认情况下，Kaspersky Embedded Systems Security 检查更新源上是否有软件模块更新可用。要开始使用安装的软件模块，需要重启受保护设备和/或重启 Kaspersky Embedded Systems Security。

默认情况下，Kaspersky Embedded Systems Security 将在每周五下午 4:00（根据受保护设备的区域时间设置）运行“软件模块更新”任务。在执行任务期间，应用程序会检查 Kaspersky Embedded Systems Security 模块的重要计划更新的可用性，而不分发这些更新。

复制更新

默认情况下，在执行任务期间，Kaspersky Embedded Systems Security 会下载数据库更新文件，并将它们保存到指定的网络或本地文件夹，不进行应用。

默认情况下，禁用“复制更新”任务。

数据库更新回滚

执行任务期间，Kaspersky Embedded Systems Security 将数据库恢复为使用之前安装的更新。

默认情况下，禁用“数据库更新回滚”任务。

关于软件模块更新

Kaspersky 会发布 Kaspersky Embedded Systems Security 模块的更新包。更新包可以为*紧急*（或*关键*）或已计划。关键更新包可修复漏洞和错误；已计划包可添加新功能或增强现有功能。

紧急（关键）更新包会上传到 卡巴斯基更新服务器。您可以使用"软件模块更新"任务来配置自动安装这些更新包。默认情况下，Kaspersky Embedded Systems Security 将在每周五下午 4:00（根据受保护设备的区域时间设置）运行"软件模块更新"任务。

Kaspersky 不会在其用于自动更新的更新服务器上发布已计划更新包；已计划更新包可从 Kaspersky 网站进行下载。"软件模块更新"任务可用于接收有关计划的 Kaspersky Embedded Systems Security 更新发布的信息。

关键更新可以从 Internet 获取并应用于每台受保护设备，或者将一台受保护设备用作中间设备，将所有更新复制给它，然后再将更新分发给网络受保护设备。若要复制并保存更新而不进行安装，请使用"复制更新"任务。

在安装模块更新之前，Kaspersky Embedded Systems Security 会为之前安装的模块创建备份副本。如果软件模块更新过程中断或产生错误，Kaspersky Embedded Systems Security 将自动恢复为使用之前安装的软件模块。您可以手动将软件模块回滚到之前安装的更新。

在安装下载的更新期间，Kaspersky Security 服务会自动停止，然后重新启动。

关于数据库更新

存储于受保护设备上的 Kaspersky Embedded Systems Security 数据库将很快过期。Kaspersky 的病毒分析师每天会检测到几百个新威胁，他们会为这些威胁创建识别记录，然后将其添加到应用程序数据库更新中。数据库更新是一个文件或一套文件，其中包含自上次更新以来发现的可识别新发现威胁的记录。若要保持所需级别的设备保护，推荐您定期接收数据库更新。

默认情况下，如果 Kaspersky Embedded Systems Security 数据库在所安装的数据库更新创建后一周内未更新，将发生"*应用程序数据库已过期*"事件。如果数据库在两周内没有更新，则会发生"*应用程序数据库已严重过期*"事件。数据库当前状态信息显示在应用程序控制台树的 **Kaspersky Embedded Systems Security** 节点的结果窗格中。您可以使用 Kaspersky Embedded Systems Security 常规设置来指定这些事件出现之前的不同天数。您还可以配置关于这些事件的管理员通知。

Kaspersky Embedded Systems Security 会从 Kaspersky 的 FTP 或 HTTP 更新服务器、Kaspersky Security Center 管理服务器或其他更新源下载应用程序数据库和模块更新。

您可以将更新下载至每个受保护设备，或者将一个受保护设备用作中间设备，将所有更新复制给它，然后再将更新分发给其他受保护设备。如果使用 Kaspersky Security Center 来集中管理公司内的设备保护，则可以使用 Kaspersky Security Center 管理服务器作为下载更新的中介。

可以手动启动数据库更新任务，也可以按计划启动。默认情况下，Kaspersky Embedded Systems Security 每小时运行一次"数据库更新"任务。

如果更新下载过程中断或者产生错误，Kaspersky Embedded Systems Security 将自动切换至使用上次更新的数据库。如果 Kaspersky Embedded Systems Security 数据库损坏，可以手动回滚至先前安装的更新。

组织内使用的反病毒数据库和模块的更新方案

更新任务中更新源的选择取决于用于更新组织内数据库和程序模块的方案。

您可以使用以下方案在受保护设备上更新 Kaspersky Embedded Systems Security 数据库和模块：

- 直接通过互联网将更新下载到每个受保护设备（方案 1）。
- 通过互联网将更新下载到中间设备，然后再将更新从该设备分发到受保护设备。

安装了以下所列软件的任何设备均可用作中间设备：

- Kaspersky Embedded Systems Security（方案 2）。
- Kaspersky Security Center 管理服务器（方案 3）。

使用中间设备进行更新不仅可减少 Internet 流量，还提供了额外的网络受保护设备安全性。

下面说明了列出的更新方案。

方案 1。直接从 Internet 更新数据库和模块

要配置直接通过互联网进行 Kaspersky Embedded Systems Security 更新：

在每个受保护设备上，在“数据库更新”任务和“软件模块更新”任务的设置中，将 Kaspersky 的更新服务器指定为更新源。

您可以将拥有更新文件夹的其他 HTTP 或 FTP 服务器配置为更新源。

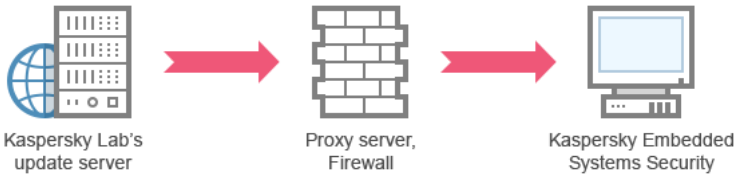

图 1：直接从 Internet 更新数据库和模块

方案 2。通过一个受保护设备更新数据库和模块

要配置通过一个受保护设备进行 Kaspersky Embedded Systems Security 更新：

1. 将更新复制到选定的受保护设备。为此，请执行以下操作：
   - 在选定受保护设备上配置“复制更新”任务设置：
     a. 指定 Kaspersky 的更新服务器作为更新源。
     b. 指定用作保存更新的文件夹的共享文件夹。
2. 将更新分发到其他受保护设备。为此，请执行以下操作：
   - 在每台受保护设备上，配置“数据库更新”任务和“软件模块更新”任务的设置（请参见下图）：
     a. 对于更新源，在中间设备驱动器上指定一个用于保存下载的更新的文件夹。

Kaspersky Embedded Systems Security 将通过一个受保护设备获取更新。

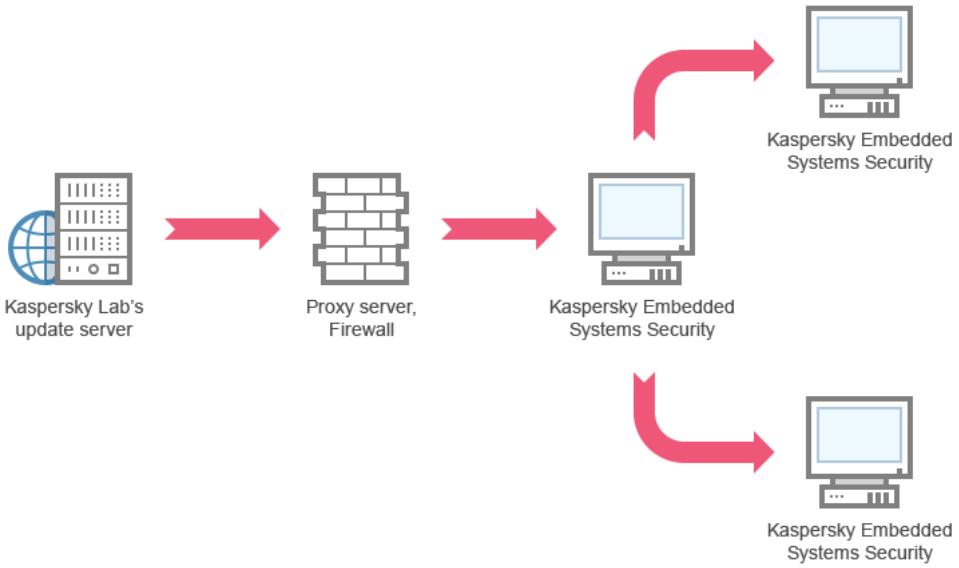

图 2：通过一个受保护设备更新数据库和模块

方案 3。通过 Kaspersky Security Center 管理服务器更新数据库和模块

如果使用 Kaspersky Security Center 集中管理反病毒设备保护，则可通过局域网中安装的 Kaspersky Security Center 管理服务器下载更新（请参见下图）。

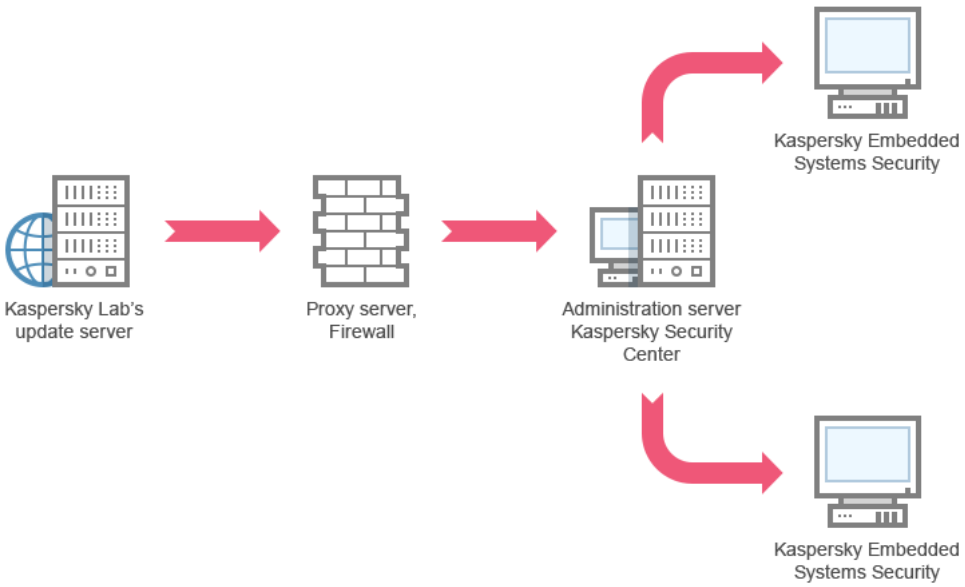

图 3：通过 Kaspersky Security Center 管理服务器更新数据库和模块

要配置通过 Kaspersky Security Center 管理服务器进行 Kaspersky Embedded Systems Security 更新：

1. 将更新从 Kaspersky 的更新服务器下载到 Kaspersky Security Center 管理服务器。为此，请执行以下操作：
   - 为指定的一组受保护设备配置“按管理服务器检索更新”任务：
     a. 指定 Kaspersky 的更新服务器作为更新源。
2. 将更新分发到受保护设备。为此，请执行以下操作之一：
   - 在 Kaspersky Security Center 上，配置反病毒数据库（应用程序模块）更新组任务以将更新发布到受保护设备：

a. 在任务计划中，指定“**管理服务器获取更新之后**”作为启动频率。

管理服务器将在每次接收到更新时启动该任务（推荐方法）。

不能在应用程序控制台中指定“**管理服务器获取更新之后**”启动频率。

- 在每个受保护设备上，配置“数据库更新”任务和“软件模块更新”任务：

  a. 指定 Kaspersky Security Center 管理服务器作为更新源。

  b. 如有必要，配置任务计划。

如果 Kaspersky Embedded Systems Security 反病毒数据库很少更新（从每月一次至每年一次），则能够检测到危险的可能性就会降低，且假报警的频率会随着应用程序组件的增加而增大。

Kaspersky Embedded Systems Security 将通过 Kaspersky Security Center 管理服务器获取更新。

如果您计划使用 Kaspersky Security Center 管理服务器分发更新，请将网络代理（Kaspersky Security Center 分发包中包含的一个应用程序组件）安装到每台受保护设备上。这可确保受保护设备上的管理服务器与 Kaspersky Embedded Systems Security 进行互动。有关网络代理以及使用 Kaspersky Security Center 对其进行配置的详细信息，请参见 *Kaspersky Security Center 帮助*。

配置更新任务

本节提供有关如何配置 Kaspersky Embedded Systems Security 更新任务的说明。

配置使用 Kaspersky Embedded Systems Security 更新源的设置

对于除“数据库更新回滚”任务外的每个更新任务，您可指定一个或多个更新源，添加用户定义的更新源，以及配置与指定源的连接设置。

在修改了更新任务设置后，将不会在正运行的更新任务中立即应用新设置。仅当重新启动任务时才会应用配置的设置。

要指定更新源的类型：

1. 在应用程序控制台树中，展开“**更新**”节点。
2. 选择与要配置的更新任务相应的子节点。
3. 在所选节点的结果窗格中，单击“**属性**”链接。

   将打开“**任务设置**”窗口的“**常规**”选项卡。
4. 在“**更新源**”部分中，选择 Kaspersky Embedded Systems Security 更新源的类型：

   - Kaspersky Security Center 管理服务器

- 卡巴斯基更新服务器
- 自定义 HTTP 或 FTP 服务器或网络文件夹

5. 如有需要，为用户定义的更新源配置高级设置：

   a. 单击“**自定义 HTTP 或 FTP 服务器或网络文件夹**”链接。

      1. 在打开的“**更新服务器**”窗口中，选中或清除用户定义的更新源旁边的复选框，以便开始或停止使用它们。

      2. 单击“**确定**”。

   b. 在“**更新源**”部分的“**常规**”选项卡中，选中或清除“如果指定的服务器不可用，则使用 卡巴斯基更新服务器”复选框。

6. 在“**任务设置**”窗口中，选择“**连接设置**”选项卡以配置用于连接到更新源的设置：

   - 清除或选中“使用代理服务器设置连接至 卡巴斯基更新服务器”复选框。
   - 清除或选中“使用代理服务器设置连接至其他服务器”复选框。

   有关配置用于访问代理服务器的可选代理服务器设置和身份验证设置的信息，请参阅“启动和配置 Kaspersky Embedded Systems Security 数据库更新任务”部分。

7. 单击“**确定**”。

Kaspersky Embedded Systems Security 更新源的已配置设置将被保存并在下次任务启动时应用。

您可管理用户定义的 Kaspersky Embedded Systems Security 更新源列表。

编辑用户定义的应用程序更新源列表：

1. 在应用程序控制台树中，展开“**更新**”节点。
2. 选择与要配置的更新任务相应的子节点。
3. 在所选节点的结果窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口的“**常规**”选项卡。
4. 单击“**自定义 HTTP 或 FTP 服务器或网络文件夹**”链接。
   将打开“**更新服务器**”窗口。
5. 执行以下操作：

   - 要添加新的用户定义更新源，请单击“**添加**”，然后在输入字段中指定 FTP 或 HTTP 服务器上包含更新文件的文件夹的地址。以 UNC（通用命名约定）格式指定本地或网络文件夹。按 **ENTER** 键。
     默认情况下，已添加的文件夹用作更新源。
   - 要禁用用户定义的更新源，则清除列表中的更新源旁边的复选框。
   - 要启用用户定义的更新源，则选中列表中的更新源旁边的复选框。

- 若要更改 Kaspersky Embedded Systems Security 访问用户定义更新源的顺序，请使用“**上移**”和“**下移**”按钮将选定的源向列表的开头或末尾移动，具体取决于是在其他源之前还是之后使用该源。
- 若要更改用户定义的更新源的路径，请在列表中选择源，单击“**编辑**”按钮，在输入字段中进行所需的更改，然后按 **ENTER** 键。
- 若要删除用户定义的源，请在列表中选择该源，然后按“**删除**”按钮。

  您无法从列表中删除剩余的唯一一个用户定义的源。

6. 单击“**确定**”。

将保存用户定义的应用程序更新源列表的更改。

在运行数据库更新任务时优化磁盘 I/O

运行“数据库更新”任务时，Kaspersky Embedded Systems Security 会将更新文件存储在受保护设备的本地磁盘上。您可以在运行更新任务时将更新文件存储在 RAM 中的虚拟驱动器上，从而降低受保护设备的磁盘 I/O 子系统的工作负载。

此功能可用于 Microsoft Windows 7 操作系统及更高版本。

在运行“数据库更新”任务时使用此功能，会在操作系统中出现一个额外的逻辑驱动器。任务完成之后，此逻辑驱动器将从操作系统中删除。

要降低数据库更新任务期间受保护设备的磁盘 I/O 子系统的工作负载：

1. 在应用程序控制台树中，展开“**更新**”节点。
2. 选择“**数据库更新**”子节点。
3. 在“**数据库更新**”节点的结果窗格中，单击“**属性**”链接。

   将打开“**任务设置**”窗口的“**常规**”选项卡。
4. 在“**磁盘 I/O 使用情况优化**”部分中，定义以下设置：
   - 清除或选中“降低磁盘 I/O 上的负载”复选框。
   - 在“**用于优化的 RAM (MB)**”字段中，指定内存量（以 MB 为单位）。操作系统临时分配指定的 RAM 容量，用于在运行任务时存储更新文件。默认 RAM 大小为 512 MB。最小 RAM 大小为 400 MB。

     在启用磁盘子系统优化功能的情况下运行“数据库更新”任务时，根据为该功能分配的 RAM 大小，可能会发生以下情况之一：

     - 如果该值太小，则分配的 RAM 大小可能不足以完成数据库更新任务（例如，在第一次更新过程中），这将导致任务完成并出现错误。

       在这种情况下，建议为磁盘子系统优化功能分配更多 RAM。
     - 如果该值太大，则在“数据库更新”任务开始时，可能无法在 RAM 中创建选定大小的虚拟驱动器。因此，磁盘子系统优化功能将自动禁用，“数据库更新”任务将在没有优化功能的情况下运行。

在这种情况下，建议为磁盘子系统优化功能分配更少 RAM。

5. 单击“**确定**”。

已配置的设置将被保存，并在下次任务启动时应用。

配置复制更新任务设置

要配置复制更新任务：

1. 在应用程序控制台树中，展开“**更新**”节点。
2. 选择“**复制更新**”子节点。
3. 在“**复制更新**”节点的结果窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。
4. 在“**常规**”和“**连接设置**”选项卡上，配置使用更新源的设置。
5. 在“**常规**”选项卡上的“**复制更新设置**”部分：
   - 指定复制更新的条件：
     - 复制数据库更新。
     - 复制关键软件模块更新。
     - 复制数据库更新和关键软件模块更新。
   - 指定 Kaspersky Embedded Systems Security 用来分发下载的更新的本地或网络文件夹。
6. 在“**计划**”和“**高级**”选项卡上，配置任务启动计划。
7. 在“**运行账户**”选项卡上，将任务配置为使用特定用户账户启动。
8. 单击“**确定**”。

已配置的设置将被保存，并在下次任务启动时应用。

配置软件模块更新任务设置

要配置“软件模块更新”任务：

1. 在应用程序控制台树中，展开“**更新**”节点。
2. 选择“**软件模块更新**”子节点。
3. 在“**软件模块更新**”节点的结果窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。
4. 在“**常规**”和“**连接设置**”选项卡上，配置使用更新源的设置。

5. 在“**常规**”选项卡上的“**更新设置**”部分，配置用于更新应用程序模块的设置：
   - 仅检查可用的关键软件模块更新
   - 复制并安装关键软件模块更新
   - 允许操作系统重启
   - 接收有关可用的计划软件模块更新的信息
6. 在“**计划**”和“**高级**”选项卡上，配置任务启动计划。默认情况下，Kaspersky Embedded Systems Security 将在每周五下午 4:00（根据受保护设备的区域时间设置）运行“软件模块更新”任务。
7. 在“**运行账户**”选项卡上，将任务配置为使用特定用户账户启动。
8. 单击“**确定**”。

已配置的设置将被保存，并在下次任务启动时应用。

Kaspersky 不会在更新服务器上发布计划的更新软件包以供自动安装；您可以手动从 Kaspersky 网站下载这些更新软件包。您可以配置有关“*有新的关键更新和计划更新可用*”事件的管理员通知；该通知将包含可以下载计划更新的网页的 URL。

回滚 Kaspersky Embedded Systems Security 数据库更新

在执行数据库更新之前，Kaspersky Embedded Systems Security 会创建先前使用的数据库的备份副本。如果更新中断或产生错误，Kaspersky Embedded Systems Security 将自动恢复为使用之前安装的数据库。

如果在您已更新数据库后出现任何问题，则可通过“数据库更新回滚”任务将数据库回滚到之前安装的更新。

若要启动“数据库更新回滚”任务，请执行下列操作：

在“**回滚应用程序数据库更新**”节点的结果窗格中，单击“**启动**”链接。

回滚应用程序模块更新

在不同 Windows 操作系统中，设置的名称可能有所不同。

在应用软件模块更新之前，Kaspersky Embedded Systems Security 会为当前使用的模块创建备份副本。如果模块更新过程中断或产生错误，Kaspersky Embedded Systems Security 将自动恢复为使用最近所安装更新的模块。

要回滚软件模块，请使用 Microsoft Windows 中的“**安装和删除应用程序**”功能。

更新任务统计

更新任务运行时，将显示自任务启动以来下载的数据量的实时信息，以及其他任务执行统计信息。

任务完成或停止后，该信息可以在任务日志中查看。

要查看更新任务统计：

1. 在应用程序控制台树中，展开“**更新**”节点。
2. 选择与要查看其统计的任务相应的子节点。

   任务统计显示在选定节点的结果窗格的“**统计**”部分中。

如果您正查看“数据库更新”任务或“复制更新”任务，则“**统计**”部分将显示截至目前 Kaspersky Embedded Systems Security 已下载的数据量（“**已接收数据**”）。

下表包含了软件模块更新任务的详情。

有关“软件模块更新”任务的信息

字段	描述
已接收数据	已下载数据的总量。
可用关键更新	可进行安装的关键更新数。
可用的计划更新	可进行安装的计划更新数。
应用更新时出错	如果该字段的值不为零，则表明未应用更新。可在任务日志中查看导致出错的更新的名称。

隔离对象和复制备份

本节提供了有关在清除或删除之前备份检测到的恶意对象的信息，以及有关隔离疑似感染对象的信息。

隔离可能已感染对象。隔离

本节介绍如何隔离可能已感染的对象以及配置隔离设置。

关于隔离疑似感染对象

Kaspersky Embedded Systems Security 通过将疑似感染对象从其原始位置移动到*隔离*文件夹来隔离这些对象。出于安全目的，隔离文件夹中的对象以加密形式存储。

查看隔离对象

您可以从应用程序控制台的“**隔离**”节点查看已隔离的对象。

要查看隔离对象：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**隔离**”子节点。

   有关已隔离对象的信息显示在选定节点的结果窗格中。

要在已隔离对象列表中查找所需对象，

排序对象或筛选对象。

排序隔离的对象

默认情况下，已隔离对象列表中的对象按照隔离日期倒序排列。要查找所需对象，可以按包含对象信息的列来排序对象。如果关闭“**隔离**”节点，然后重新打开，则将保存排序结果；如果关闭应用程序控制台，则保存 msc 文件，然后从该文件重新打开排序结果。

要排序对象：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**隔离**”子节点。
3. 在“**隔离**”节点的结果窗格中，选择想要用于对列表中的对象进行排序的列标题。

   列表中的对象将基于选定设置排序。

筛选隔离的对象

要查找所需的已隔离对象，可以筛选列表中的对象，例如只显示满足您指定的筛选标准（筛选器）的那些对象。如果关闭再重新打开“**隔离**”节点，或者先关闭应用程序控制台，保存 msc 文件，再从该文件重新打开应用程序控制台，将保存筛选结果。

要指定一个或多个筛选：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**隔离**”子节点。
3. 在节点名称的上下文菜单中，选择“**筛选器**”。
   将打开“**筛选设置**”窗口。
4. 若要添加筛选器，请执行以下步骤：
   a. 在“**字段名称**”列表中，选择将构成筛选基础的字段。
   b. 在“**运算符**”列表中选择筛选条件。列表中的筛选条件可能有所不同，具体取决于您在“**字段名称**”列表中选择的值。
   c. 在“**字段值**”字段中输入筛选值，或者从列表中进行选择。
   d. 单击“**添加**”按钮。

   已添加的筛选将出现在“**筛选设置**”窗口的筛选列表中。对添加的每个过滤器重复步骤a-d。使用过滤器时，请遵循以下准则：

   - 要使用逻辑运算符“AND”组合多个筛选，请选择“**如果满足所有条件**”。
   - 要使用逻辑运算符“OR”组合多个筛选，请选择“**如果满足任一条件**”。
   - 要删除筛选，请在筛选列表中选择要删除的筛选，然后单击“**删除**”按钮。
   - 要编辑筛选，请从“**筛选设置**”窗口的列表中选择筛选。然后在“**字段名称**”、“**运算符**”或“**字段值**”字段中更改所需值，并单击“**替换**”按钮。
5. 添加所有筛选后，单击“**应用**”按钮。

   将保存已创建的筛选器。

要恢复显示所有已隔离对象，

在“**隔离**”节点的上下文菜单中，选择“**删除筛选**”。

隔离区扫描

默认情况下，每次数据库更新之后，Kaspersky Embedded Systems Security 都会执行“隔离区扫描”本地系统任务。下表描述了任务设置。无法修改“隔离区扫描”任务的设置。

您可以配置任务启动计划，手动启动它以及修改用于启动任务的账户权限。

通过在更新数据库后扫描隔离对象，Kaspersky Embedded Systems Security 可能将某些对象重新归类为未被感染：此类对象的状态会更改为“误报”。其他对象可被重新归类为已感染，在这种情况下，Kaspersky Embedded Systems Security 会根据“隔离区扫描”任务设置（清除，或清除失败则删除）所指定来处理此类对象。

隔离区扫描任务设置

隔离区扫描任务设置	值
扫描范围	隔离区文件夹
安全设置	对于整个扫描范围都一样；它们的值在下一个表中提供

“隔离区扫描”任务中的扫描设置

安全性设置	值
扫描对象	包含在扫描范围内的所有对象
性能	已禁用
对受感染对象和其他对象执行的操作	清除，如果无法清除则删除
对疑似感染对象执行的操作	跳过
排除文件	否
不检测	否
超过以下时间则停止扫描(秒)	未配置
不扫描大于以下大小的对象(MB)	未配置
扫描 NTFS 交换数据流	已启用
扫描磁盘引导扇区和 MBR	已禁用
使用 iChecker 技术	已禁用
使用 iSwift 技术	已禁用
扫描复合对象	• 压缩文件* • SFX 压缩文件* • 打包的对象* • 嵌入的 OLE 对象* *“仅扫描新文件和已修改的文件”已禁用。
检查文件内的 Microsoft 签名	未执行
使用启发式分析	已启用深度分析级别
信任区域	未应用

还原已隔离的对象

Kaspersky Embedded Systems Security 以加密形式将疑似感染对象放入隔离文件夹中，以保护受保护设备免受任何可能的有害影响。

您可以从隔离区还原任意对象。在以下情况下，可能需要这样做：

- 使用更新的数据库进行隔离区扫描之后，对象的状态更改为“**误报**”或“**已清除**”。
- 您认为该对象对于受保护设备无害，并且要使用它。如果您不希望 Kaspersky Embedded Systems Security 在后续扫描期间将该对象隔离，可以将该对象从“实时文件保护”任务和“按需扫描”任务的处理中排除。要执行此操作，请在这些任务的“**排除文件**”（按文件名）或“**不检测**”安全性设置中指定对象，或者将对象添加到信任区域。

在还原对象时，您可以选择将保存还原的对象的位置：原始位置（默认）、受保护设备上用于存储还原对象的特殊文件夹，或者安装应用程序控制台的受保护设备上的自定义文件夹或者网络中的其他设备。

您可以指定受保护设备上用于存储还原对象的文件夹。您可以为需要扫描的对象配置特殊的安全性设置。该文件夹的路径由隔离设置予以设置。

从隔离区中还原对象可能会导致受保护设备感染病毒。

您可以还原对象，并将其副本保存到隔离文件夹中以备稍后使用，例如数据库更新之后重新扫描对象。

如果已隔离的对象包含于复合对象中（例如压缩文件），Kaspersky Embedded Systems Security 还原期间将不会将隔离对象包括在复合对象中，而是将隔离对象单独保存到选定的文件夹。

您可以还原一个或多个对象。

若要还原已隔离的对象，请执行以下步骤：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**隔离**”子节点。
3. 在“**隔离**”节点的结果窗格中执行以下操作之一：
   - 要还原一个对象，请从要还原的对象的上下文菜单中选择“**还原**”。
   - 要还原多个对象，请使用 **CTRL** 或 **SHIFT** 键选择想要还原的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**还原**”。

   将打开“**还原对象**”窗口。
4. 在“**还原对象**”窗口中，为每个选定对象指定将保存还原对象的文件夹。

   对象的名称显示在窗口上部的“**对象**”字段中。如果选定了多个对象，系统将显示选定对象列表中第一个对象的名称。
5. 执行以下步骤之一：
   - 要将对象还原到原始位置，请选择“**还原到源文件夹**”。
   - 要将对象还原到设置中的适用于还原对象位置所指定的文件夹，请选择“**还原到默认还原文件夹**”。
   - 要将对象保存在安装了应用程序控制台的受保护设备上的其他文件夹或共享文件夹，请选择“**还原到本地计算机上的文件夹**”，然后选择所需文件夹或指定文件夹路径。

6. 如果希望于还原之后在*隔离*文件夹中保存对象的副本，请清除“**还原对象后从存储删除对象**”复选框。

7. 要为其余选定对象应用指定的还原条件，请选中“**应用到所有选定对象**”复选框。

   所有选定对象都将还原并保存在指定位置。如果选择了“**还原到源文件夹**”，则每个对象都将保存到其原始位置；如果选择了“**还原到默认还原文件夹**”或“**还原到本地计算机上的文件夹**”，则所有对象都将保存到一个指定的文件夹。

8. 单击“**确定**”。

   Kaspersky Embedded Systems Security 将开始还原选定对象的第一个对象。

9. 如果指定位置已存在拥有该名称的对象，则系统将打开“**拥有该名称的对象已存在**”窗口。

   a. 选择以下 Kaspersky Embedded Systems Security 操作之一：

   - **替换**，将现有对象替换为还原对象。
   - **重命名**，使用其他名称保存还原的对象。在输入字段中输入新还原对象的文件名和完整路径。
   - “**通过添加后缀重命名**”，通过为对象文件名添加后缀重命名还原对象。在输入字段中输入后缀。

   b. 如果选择了多个对象进行还原，则选中“**应用到所有选定对象**”复选框以将选定操作（**替换**或**重命名**）应用于其余选定对象。如果选择了“**重命名**”，“**应用到所有选定对象**”复选框将不可用。

   c. 单击“**确定**”。

   对象将被还原。有关还原操作的信息将记录到系统审核日志中。

   如果您在“**还原对象**”窗口中未选中“**应用到所有选定对象**”，“**还原对象**”窗口可能再次打开。使用该窗口可指定保存下个选定对象的位置（请参见该流程的步骤 4）。

将对象移到隔离

您可以手动隔离文件。

要隔离文件：

1. 在应用程序控制台树中，打开“**隔离**”节点的上下文菜单。

2. 选择“**添加**”。

3. 在“**打开**”窗口中，选择磁盘上您想要隔离的文件。

4. 单击“**确定**”。

   Kaspersky Embedded Systems Security 将隔离选定文件。

从隔离删除对象

根据“隔离区扫描”任务设置，如果在使用更新的数据库进行隔离区扫描期间对象状态更改为“*已感染*”，并且 Kaspersky Embedded Systems Security 无法清除这些对象，Kaspersky Embedded Systems Security 将自动从隔离区文件夹删除这些对象。Kaspersky Embedded Systems Security 不会从隔离中删除其他对象。

可以从隔离区删除一个或多个对象。

要从隔离区删除一个或多个对象：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**隔离**”子节点。
3. 执行以下步骤之一：
   - 要删除一个对象，请从对象名称的上下文菜单中选择“**删除**”。
   - 要删除多个对象，请使用 **Ctrl** 或 **Shift** 键选择想要删除的对象，并在其中任何一个选定对象上打开上下文菜单，然后选择“**删除**”。
4. 在确认窗口中单击“**是**”按钮以确认操作。

将从隔离区删除选定对象。

发送疑似感染对象到 Kaspersky 以供分析

如果某个文件的行为使您怀疑该文件可能包含威胁，并且 Kaspersky Embedded Systems Security 认定该文件需要清理，则您可能遇到未知威胁，而该威胁的签名尚未添加到数据库。您可以将此文件发送到 Kaspersky 以供分析。Kaspersky 的反病毒分析人员将对文件进行分析，如果检测到文件中包含新威胁，则将在数据库中添加记录标识该威胁。当您在数据库更新之后重新扫描对象时，有可能 Kaspersky Embedded Systems Security 将此对象标识为已感染，并能够将其清除。您不仅能够保留对象，而且能够阻止病毒爆发。

仅能发送已隔离的文件以供分析。已隔离的文件会以加密形式存储，且在发送时不会被安装在邮件服务器上的反病毒应用程序删除。

授权许可到期后，无法将隔离的对象发送到 Kaspersky 进行分析。

要将待分析的文件发送给 Kaspersky：

1. 如果文件未被隔离，请首先将其移至**隔离**。
2. 在“**隔离**”节点中，打开想要发送以进行分析的文件的上下文菜单，然后选择上下文菜单中的“**发送对象进行分析**”。
3. 如果您确定要发送选定对象以供分析，在打开的确认窗口中，单击“**是**”。
4. 如果安装了应用程序控制台的受保护设备上已配置邮件客户端，则将创建新电子邮件。查看该消息并单击“**发送**”按钮。

   “**收件人**”字段包含 Kaspersky 电子邮件地址 newvirus@kaspersky.com。“主题”字段将包含“已隔离的对象”文本。

   消息正文将包含以下文本：“此文件将发送到 Kaspersky 以供分析”。您可以在消息正文中包含有关该文件的任何附加信息：您为何认定该文件为可能已感染或存在危险、该文件的行为如何或该文件对系统有何影响。

   一个名为 <对象名称>.cab 的压缩文件将附加到邮件。该压缩文件将包含一个 <uuid>.klq 文件，其中包含加密形式的对象；一个 <uuid>.txt 文件，其中包含有关 Kaspersky Embedded Systems Security 提取的对象的信息；以及一个 Sysinfo.txt 文件，其中包含有关受保护设备上安装的 Kaspersky Embedded Systems Security 和操作系统的以下信息：

   - 操作系统的名称和版本。

- Kaspersky Embedded Systems Security 的名称和版本。
- 已安装的最新数据库更新的发布日期。
- 活动密钥。

Kaspersky 的反病毒分析人员需要上述信息才能更快更有效地分析您的文件。但是，如果您不想发送此信息，可以删除压缩文件中的 Sysinfo.txt 文件。

如果具有应用程序控制台的受保护设备上未安装邮件客户端，则应用程序会提示您将选定已加密对象保存到文件。手动将该文件发送到 Kaspersky。

要将加密的对象保存到文件：

1. 在打开的提示保存对象的窗口中，单击“**确定**”。
2. 选择受保护设备的驱动器上的文件夹或网络文件夹，其中将保存包含对象的文件。

会将对象保存到 CAB 文件。

配置隔离设置

您可配置隔离设置。保存后将立即应用新的隔离设置。

要配置隔离设置：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 打开“**隔离**”子节点的上下文菜单。
3. 选择“**属性**”。
4. 在“**隔离属性**”窗口中，根据您的要求配置所需的隔离设置：
   - 在“**隔离设置**”部分中：
     - 隔离区文件夹
     - 隔离区最大容量(MB)
     - 可用空间阈值(MB)

     如果隔离中的对象大小超过最大隔离容量或超过可用空间阈值，在您继续将对象放入隔离时，Kaspersky Embedded Systems Security 将通知您此情况。
   - 在“**还原设置**”部分中：
     - 用于还原对象的目标文件夹
5. 单击“**确定**”。

将保存新配置的隔离设置。

隔离统计

您可以查看有关已隔离的对象数量的信息，即，隔离统计。

要查看隔离统计，

在应用程序控制台树的“**隔离**”节点的上下文菜单中，选择“**统计**”。

“**隔离统计**”窗口将显示当前存储在隔离区的对象数量的相关信息（请参见下表）：

字段	描述
疑似感染的对象	Kaspersky Embedded Systems Security 发现的疑似感染的对象数。
已使用的隔离区空间	隔离文件夹中的数据总量。
误报	因在使用更新的数据库进行隔离区扫描期间归类为未被感染而获得“*误报*”状态的对象数。
对象已清除	隔离区扫描之后获得“*已清除*”状态的对象数。
对象总数	隔离中的对象总数。

制作对象的备份副本。备份

本节提供了有关在清除或删除之前备份检测到的恶意对象以及配置备份的说明。

关于备份对象之后再清除或删除

对于被归类为“*已感染*”的对象，Kaspersky Embedded Systems Security 会在对其进行清除或删除之前，在*备份*中存储这些对象的加密副本。

如果该对象是复合对象的一部分（例如压缩文件的一部分），Kaspersky Embedded Systems Security 会将此复合对象整体保存在备份中。例如，如果 Kaspersky Embedded Systems Security 检测到邮件数据库中的其中一个对象感染病毒，则会备份整个邮件数据库。

Kaspersky Embedded Systems Security 放入备份中的大型文件可能会降低系统速度，并减少硬盘驱动器上的可用磁盘空间。

您可以将文件从备份还原到其原始文件夹或还原到受保护设备上的其他文件夹或者局域网中的其他设备。文件可以从备份区还原，例如，如果某个已感染文件包含重要信息，但 Kaspersky Embedded Systems Security 无法在不破坏其完整性和丢失信息的前提下清除病毒。

从备份中还原文件可能会导致受保护设备感染病毒。

查看备份中存储的对象

只能使用应用程序控制台中的“**备份**”节点查看备份文件夹中的对象。您无法使用 Microsoft Windows 文件管理器查看这些文件。

要查看备份中的对象，

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**备份**”子节点。

   有关置于备份中的对象的信息显示在选定节点的结果窗格中。

若要在备份中的对象列表中查找所需对象，

排序对象或筛选对象。

排序备份中的文件

默认情况下，按备份日期倒序排序备份中的文件。要查找所需文件，可以根据结果窗格中任意列的内容排序文件。

如果关闭再重新打开“**备份**”节点，或者先关闭应用程序控制台，保存 msc 文件，再从该文件重新打开应用程序控制台，将保存排序结果。

要排序备份中的文件：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**备份**”子节点。
3. 在**备份**的文件列表中，选择想要用于排序对象的列标题。

   将基于选定标准排序备份中的文件。

筛选备份中的文件

要在备份中查找所需文件，您可以筛选文件：在“**备份**”节点中只显示满足您指定的筛选标准（筛选器）的那些文件。

如果关闭再重新打开“**备份**”节点，或者先关闭应用程序控制台，保存 msc 文件，再从该文件重新打开应用程序控制台，将保存排序结果。

要筛选备份中的文件：

1. 在应用程序控制台树中，打开“**备份**”节点的上下文菜单，并选择“**筛选器**”。

   将打开“**筛选设置**”窗口。

2. 若要添加筛选器，请执行以下步骤：

   a. 在“**字段名称**”列表中，选择将构成筛选基础的字段。

   b. 在“**运算符**”列表中选择筛选条件。列表中的筛选条件可能有所不同，具体取决于您在“**字段名称**”字段中选择的值。

   c. 在“**字段值**”字段中输入筛选值或者选择筛选值。

   d. 单击“**添加**”按钮。

   已添加的筛选将出现在“**筛选设置**”窗口的筛选列表中。对添加的每个过滤器重复这些步骤。使用过滤器时，可以使用以下准则：

   - 要使用逻辑运算符“AND”组合多个筛选，请选择“**如果满足所有条件**”。
   - 要使用逻辑运算符“OR”组合多个筛选，请选择“**如果满足任一条件**”。
   - 要删除筛选，请在筛选列表中选择要删除的筛选，然后单击“**删除**”按钮。
   - 若要编辑筛选，请从“**筛选设置**”窗口的筛选列表中选择筛选，修改“**字段名称**”、“**运算符**”或“**字段值**”字段中的所需值，并单击“**替换**”按钮。

   添加所有筛选后，单击“**应用**”按钮。只有与您指定的筛选相匹配的文件将显示在列表中。

要显示备份中存储的对象列表中包括的所有文件，

在“**备份**”节点的上下文菜单中，选择“**删除筛选**”。

从备份还原文件

Kaspersky Embedded Systems Security 以加密形式将文件存储在备份文件夹中，以保护受保护设备免受可能的有害影响。

所有文件都可以从备份还原。

在下列情况下可能需要还原对象：

- 原始受感染文件包含了重要信息，而 Kaspersky Embedded Systems Security 无法保持其完整性，因而该文件中的信息变得不可用。
- 您认为文件对受保护设备无害并且要使用它。如果您不希望 Kaspersky Embedded Systems Security 将该文件视为已感染或疑似感染，则在后续扫描期间，可以将其从“实时文件保护”任务和“按需扫描”任务的处理中排除。为此，请在相应任务的“**排除文件**”设置或“**不检测**”设置中指定文件。

> 从备份中还原文件可能会导致受保护设备感染病毒。

还原文件时，您可以选择用于保存文件的位置：原始位置（默认）、受保护设备上用于存储还原对象的特殊文件夹、或者安装应用程序控制台的受保护设备上的自定义文件夹或者网络中的其他设备。

您可以指定受保护设备上用于存储还原对象的文件夹。您可以为需要扫描的对象配置特殊的安全性设置。此文件夹的路径由“备份设置”指定。

默认情况下，Kaspersky Embedded Systems Security 还原文件时，会在备份区中生成文件的副本。还原之后，您可以从备份删除文件副本。

要从备份还原文件：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**备份**”子节点。
3. 在“**备份**”节点的结果窗格中执行以下操作之一：
   - 要还原一个对象，请从要还原的对象的上下文菜单中选择“**还原**”。
   - 要还原多个对象，请使用 **CTRL** 或 **SHIFT** 键选择想要还原的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**还原**”。

   将打开“**还原对象**”窗口。
4. 在“**还原对象**”窗口中，为每个选定对象指定将保存还原对象的文件夹。

   对象的名称显示在窗口上部的“**对象**”字段中。如果选定了多个对象，系统将显示选定对象列表中第一个对象的名称。
5. 执行以下步骤之一：
   - 要将对象还原到原始位置，请选择“**还原到源文件夹**”。
   - 要将对象还原到设置中的适用于还原对象位置所指定的文件夹，请选择“**还原到默认还原文件夹**”。
   - 要将对象保存在安装了应用程序控制台的受保护设备上的其他文件夹或共享文件夹，请选择“**还原到本地计算机上的文件夹**”，然后选择所需文件夹或指定文件夹路径。
6. 如果您不希望于还原之后在备份文件夹中保存文件的副本，请选中“**还原对象后从存储删除对象**”复选框（默认情况下，清除此复选框）。
7. 要为其余选定对象应用指定的还原条件，请选中“**应用到所有选定对象**”复选框。

   所有选定对象都将还原并保存在指定位置。如果选择了“**还原到源文件夹**”，则每个对象都将保存到其原始位置；如果选择了“**还原到默认还原文件夹**”或“**还原到本地计算机上的文件夹**”，则所有对象都将保存到一个指定的文件夹。
8. 单击“**确定**”。

   Kaspersky Embedded Systems Security 将开始还原选定对象的第一个对象。
9. 如果指定位置已存在拥有该名称的对象，则系统将打开“**拥有该名称的对象已存在**”窗口。
   a. 选择以下 Kaspersky Embedded Systems Security 操作之一：
      - **替换**，将现有对象替换为还原对象。
      - **重命名**，使用其他名称保存还原的对象。在输入字段中输入新还原对象的文件名和完整路径。
      - “**通过添加后缀重命名**”，通过为对象文件名添加后缀重命名还原对象。在输入字段中输入后缀。

b. 如果选择了多个对象进行还原，则选中“**应用到所有选定对象**”复选框以将选定操作（**替换**或**重命名**）应用于其余选定对象。如果选择了“**重命名**”，“**应用到所有选定对象**”复选框将不可用。

c. 单击“**确定**”。

对象将被还原。有关还原操作的信息将记录到系统审核日志中。

如果您在“**还原对象**”窗口中未选中“**应用到所有选定对象**”，“**还原对象**”窗口可能再次打开。使用该窗口可指定保存下个选定对象的位置（请参见该流程的步骤 4）。

从备份删除文件

要从备份中删除一个或多个文件：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**备份**”子节点。
3. 执行以下步骤之一：
   - 要删除一个对象，请从对象名称的上下文菜单中选择“**删除**”。
   - 要删除多个对象，请使用 **Ctrl** 或 **Shift** 键选择想要删除的对象，并在其中任何一个选定对象上打开上下文菜单，然后选择“**删除**”。
4. 在确认窗口中单击“**是**”按钮以确认操作。

将从备份中删除选定文件。

配置备份设置

要配置备份设置：

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 打开“**备份**”子节点的上下文菜单。
3. 选择“**属性**”。
4. 在“**备份属性**”窗口中，根据您的要求配置所需的备份设置：
   在“**备份设置**”部分中：
   - 备份文件夹
   - 最大备份容量(MB)
   - 可用空间阈值(MB)

   如果备份中的对象大小超过最大备份容量或超过可用空间阈值，在您继续将对象放入备份时，Kaspersky Embedded Systems Security 将通知您此情况。

在“**还原设置**”部分中：

- 用于还原对象的目标文件夹

5. 单击“**确定**”。

将保存已配置的备份设置。

备份统计

您可以查看有关当前备份状态的信息，即备份统计。

若要查看备份统计，

请在应用程序控制台树的“**备份**”节点上打开上下文菜单并选择“**统计**”。将打开“**备份统计**”窗口。

“**备份统计**”窗口将显示有关当前备份状态的信息（请参见下表）。

有关当前备份状态的信息

字段	描述
当前备份容量	备份文件夹中的数据量；程序以加密形式计算文件大小
对象总数	备份中当前的对象总数

阻止访问网络资源。被阻止的网络会话

本节介绍如何阻止远程设备和配置被阻止网络会话列表的设置。

关于被阻止的网络会话列表

默认情况下，如果安装了以下任何组件：实时文件保护、网络威胁防护，则可以使用被阻止的网络会话列表。这些组件根据被阻止的网络会话列表，发现对受保护设备或网络附加存储共享文件夹中的对象进行加密、打开或执行的远程尝试。有关所有受保护设备上被阻止的网络会话的信息将发送到 Kaspersky Security Center。Kaspersky Embedded Systems Security 会阻止当前会话，并且就当前会话而言，使共享文件夹或网络附加存储文件夹不可用。

在活动模式下启动至少一个以下任务（在指定条件下）时，将填充被阻止的网络会话列表：

- 对于“实时文件保护”任务：检测到正在访问网络文件资源的设备存在恶意活动，并且“实时文件保护”任务设置中的“**阻止显示恶意活动的网络会话对网络共享资源的访问**”复选框已选中。
- 对于“网络威胁防护”任务：检测到典型的网络攻击活动。

在检测到恶意活动或加密尝试后，该任务会将攻击网络会话的相关信息发送到被阻止的网络会话列表，并且应用程序会为攻击主机的当前会话创建一个*警告*事件。该会话访问受保护共享网络文件夹的尝试都将被阻止。

如果发起攻击网络会话的主机的本地唯一标识符 (LUID) 已添加到被阻止的网络会话列表中，Kaspersky Embedded Systems Security 会确定该主机的 IP 地址，并将其添加到被阻止的网络会话列表中来替换攻击主机的 LUID。

默认情况下，当被阻止的网络会话被添加到列表 30 分钟后，Kaspersky Embedded Systems Security 将从列表中删除该被阻止的网络会话。当网络会话从被阻止的网络会话列表中删除后，对网络文件资源的访问权限将自动恢复。您可以指定在此之后被阻止的网络会话会被自动解除阻止的时间段。

请注意，当限制任何用户账户对存储管理的访问权限时，被阻止的网络会话列表仍将可用。被阻止的网络会话的设置无法更改，除非所选用户账户具有可管理 Kaspersky Embedded Systems Security 的**编辑权限**。

通过管理插件管理被阻止的网络会话列表

在本节中，了解如何通过管理插件界面配置被阻止的网络会话列表的设置。

启用阻止不信任主机

要将出现任何恶意或加密活动的网络会话添加到**被阻止的网络会话列表**并阻止访问网络文件资源，必须有至少一个以下任务在活动模式下运行：

- 实时文件保护
- 网络威胁防护

配置"实时文件保护"任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开"**受管理设备**"节点。
2. 选择"**策略**"选项卡，然后在"**实时文件保护**"块中打开"**<策略名称> >实时计算机保护 > 设置**"。
   将打开"**实时计算机保护**"窗口。
3. 如果您希望 Kaspersky Embedded Systems Security 在"实时文件保护"任务运行时阻止在其中检测到恶意活动的主机访问网络文件资源，请在"**与其他组件集成**"部分中选中"**将显示恶意活动的主机列为不受信任**"复选框。
4. 如果任务尚未启动，请打开"**任务管理**"选项卡：
   a. 选中"**按计划运行**"复选框。
   b. 在下拉列表中选择"**应用程序启动时**"频率。
5. 在"**实时计算机保护**"窗口中，单击"**确定**"。

将保存新配置的设置。

配置"网络威胁防护"任务：

1. 展开 Kaspersky Security Center 管理控制台树中的"**受管理设备**"节点。
2. 选择要为其配置任务的管理组。
3. 选择"**策略**"选项卡。

4. 双击要配置的策略名称。

5. 在打开的“**属性：<策略名称>**”窗口中，选择相应部分。

6. 单击“**网络威胁防护**”子部分中的“**设置**”按钮。
   将打开“**网络威胁防护**”窗口。

7. 打开“**常规**”选项卡。

8. 在“**处理模式**”部分中，选择“检测到攻击时阻止连接”处理模式。

   该复选框用于启用或禁用将出现典型网络攻击活动的主机添加到阻止的主机列表。

   如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，并将出现典型网络攻击活动的主机的 IP 地址添加到阻止的主机列表。

   默认选择该模式。

   您可以在阻止的主机存储中查看阻止的主机列表。

   您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

9. 如果任务尚未启动，请打开“**任务管理**”选项卡：

   a. 选中“**按计划运行**”复选框。

   b. 在下拉列表中选择“**应用程序启动时**”频率。

10. 在窗口中，单击“**确定**”。

11. 将保存新配置的设置。

配置被阻止的网络会话列表的设置

要配置被阻止的网络会话列表：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择要为其配置应用程序设置的管理组。

3. 在选定的管理组的详细窗格中执行以下操作之一：

   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**补充**”部分中，单击“**存储**”子部分中的“**设置**”按钮。

将显示“**存储设置**”窗口。

5. 在“**阻止的网络会话**”选项卡的“**网络会话阻止期限**”部分中，指定被阻止的网络会话在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

6. 单击“**确定**”。

通过应用程序控制台管理被阻止的网络会话列表

在本节中，了解如何通过应用程序控制台界面配置被阻止的网络会话列表的设置。

启用阻止不信任主机

要将出现任何恶意或加密活动的网络会话添加到**被阻止的网络会话列表**并阻止访问网络文件资源，必须有至少一个以下任务在活动模式下运行：

- 实时文件保护
- 网络威胁防护

配置“实时文件保护”任务：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。

2. 选择“**实时文件保护**”子节点。

3. 在结果窗格中单击“**属性**”链接。
   将打开“**任务设置**”窗口。

4. 如果您希望 Kaspersky Embedded Systems Security 在“实时文件保护”任务运行时阻止在其中检测到恶意活动的网络会话，请在“**深度**”部分中选中“**阻止显示恶意活动的网络会话对网络共享资源的访问**”复选框。

5. 如果任务尚未启动，请打开“**计划**”选项卡：

   a. 选中“**按计划运行**”复选框。

   b. 在下拉列表中选择“**应用程序启动时**”频率。

6. 在“**任务设置**”窗口中，单击“**确定**”。

将保存新配置的设置。

配置“网络威胁防护”任务：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。

2. 选择“**网络威胁防护**”子节点。

3. 在“**网络威胁防护**”节点的详细信息窗格中，单击“**属性**”链接。

4. 将打开“**任务设置**”窗口。

5. 打开“**常规**”选项卡。

6. 在“**处理模式**”部分中，选择“检测到攻击时阻止连接”处理模式。

   该复选框用于启用或禁用将出现典型网络攻击活动的主机添加到阻止的主机列表。

   如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，并将出现典型网络攻击活动的主机的 IP 地址添加到阻止的主机列表。

   默认选择该模式。

   您可以在阻止的主机存储中查看阻止的主机列表。

   您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

7. 选中或清除“未运行任务时不停止流量分析”复选框。

   如果选中此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，并根据所选处理模式阻止攻击计算机的网络活动。

   如果清除此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 不会扫描入站网络流量中是否存在典型网络攻击活动，也不回阻止攻击计算机的网络活动。

   默认取消选中该复选框。

8. 如果任务尚未启动，请打开“**计划**”选项卡：

   a. 选中“**按计划运行**”复选框。

   b. 在下拉列表中选择“**应用程序启动时**”频率。

9. 在“**任务设置**”窗口中，单击“**确定**”。

将保存新配置的设置。

配置被阻止的网络会话列表的设置

要配置被阻止的网络会话列表：

1. 在应用程序控制台树中，展开“**存储**”节点。

2. 打开“**阻止的网络会话**”子节点的上下文菜单。

3. 选择“**属性**”菜单选项。

   将显示“**阻止的网络会话列表设置**”窗口。

4. 在“**网络会话阻止期限**”部分中，指定被阻止的网络会话在被阻止多少天、小时和分钟后可以重新获得对网络文件资源的访问权限。

5. 单击“**确定**”。

6. 要恢复对所有被阻止的网络会话的访问：

a. 打开“**阻止的网络会话**”子节点的上下文菜单。

b. 选择“**全部解除阻止**”选项。

所有网络会话都将从列表删除并解除阻止。

7. 要从被阻止的网络会话列表中删除多个会话：

a. 在结果窗格中显示的被阻止的网络会话列表中，选择一个或多个会话。

b. 打开“**阻止的网络会话**”子节点的上下文菜单。

c. 选择“**解除阻止选定项目**”选项。

将解除阻止选定的网络会话。

通过 Web 插件管理被阻止的网络会话列表

在本节中，了解如何通过 Web 插件界面配置被阻止的网络会话列表设置。

启用阻止网络会话

要将出现任何恶意或加密活动的网络会话添加到**阻止的网络会话**并阻止访问这些会话的网络文件资源，必须有至少一个以下任务在活动模式下运行：

- 实时文件保护
- 网络威胁防护

配置“实时文件保护”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时计算机保护**”部分。
5. 单击“**实时文件保护**”子部分中的“**设置**”。
6. 如果您希望 Kaspersky Embedded Systems Security 阻止当前会话并使网络共享资源对在其中检测到恶意活动的网络会话不可用，请在“**与其他组件集成**”部分中选中“**阻止显示恶意活动的网络会话对网络共享资源的访问**”复选框。
7. 如果任务尚未启动，请打开“**任务管理**”选项卡：

a. 选中“**按计划运行**”复选框。

b. 在下拉列表中选择“**应用程序启动时**”频率。

8. 单击“**保存**”。

将保存新配置的设置。

配置被阻止的网络会话列表的设置

要配置被阻止的网络会话列表：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**补充**”部分。
5. 单击“**存储**”子部分中的“**设置**”。
6. 在“**补充**”部分中，单击“**存储**”子部分中的“**设置**”按钮。
   将显示“**存储**”窗口。
7. 在“**阻止的网络会话**”选项卡的“**网络会话阻止期限**”部分中，指定被阻止的网络会话在被阻止多少天、小时和分钟后可以重新获得对网络文件资源的访问权限。
8. 单击“**确定**”。

事件注册。Kaspersky Embedded Systems Security 日志

本节提供有关使用 Kaspersky Embedded Systems Security 日志的信息。

注册 Kaspersky Embedded Systems Security 事件的方式

Kaspersky Embedded Systems Security 的事件分为两组：

- 与 Kaspersky Embedded Systems Security 任务中的对象处理相关的事件。
- 与管理 Kaspersky Embedded Systems Security（例如启动应用程序、创建或删除任务，或者编辑任务设置）有关的事件。

Kaspersky Embedded Systems Security 使用以下方式来记录事件：

- **任务日志**。任务日志包含有关当前任务状态以及执行任务期间发生事件的信息。
- **系统审核日志**。系统审核日志包含有关与管理 Kaspersky Embedded Systems Security 相关的事件的信息。
- **事件日志**。事件日志包含有关诊断 Kaspersky Embedded Systems Security 运行故障所需的事件的信息。可在 Microsoft Windows 事件查看器中查看事件日志。
- **安全日志**。安全日志包含有关与受保护设备上的安全入侵或安全入侵尝试相关的事件的信息。

如果 Kaspersky Embedded Systems Security 运行期间发生问题（例如，Kaspersky Embedded Systems Security 或个别任务异常终止或者无法启动），您可以创建跟踪文件和 Kaspersky Embedded Systems Security 进程的 dump 文件，并将包含该信息的文件发送给 Kaspersky 技术支持进行分析来诊断问题。

Kaspersky Embedded Systems Security 不会自动发送任何跟踪或 Dump 文件。诊断数据只能由具有所需权限的用户发送。

Kaspersky Embedded Systems Security 会以未加密的形式将信息写入到跟踪文件和 Dump 文件。保存文件的文件夹由用户选择，由操作系统配置和 Kaspersky Embedded Systems Security 设置管理。您可以配置访问权限并只允许所需用户访问日志、跟踪文件和 dump 文件。

可通过以下链接下载的文件包含具有以下类别的 Kaspersky Embedded Systems Security 事件完整列表的表格：

- Kaspersky Embedded Systems Security 写入事件日志的事件。

  下载 KESS-WEL-EVENTS.ZIP
- Kaspersky Embedded Systems Security 发送到管理服务器的事件。

  下载 KESS-KSC-EVENTS.ZIP

系统审核日志

Kaspersky Embedded Systems Security 执行与 Kaspersky Embedded Systems Security 管理有关的事件的系统审核。应用程序会记录有关启动应用程序、启动和停止 Kaspersky Embedded Systems Security 任务、更改任务设置、创建和删除按需扫描任务的信息。当您在应用程序控制台中选择“**系统审核日志**”节点时，所有这些事件的记录都会显示在结果窗格中。

默认情况下，Kaspersky Embedded Systems Security 会无限期地存储系统审核日志中的记录。您可以指定系统审核日志中记录的存储周期。

您可以指定一个文件夹以供 Kaspersky Embedded Systems Security 用来存储包含系统审核日志的文件，而不使用默认值。

在系统审核日志中排序事件

默认情况下，系统审核日志节点中的事件按时间倒序显示。

事件可按除“**事件**”列以外的任何列的内容进行排序。

要在系统审核日志中排序事件：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择“**系统审核日志**”子节点。
3. 在结果窗格中，选择要用于排序列表中事件的列标题。

在您下次查看系统审核日志前，将保存排序结果。

在系统审核日志中筛选事件

您可以将系统审核日志配置为仅显示满足指定筛选条件（筛选器）的事件记录。

要在系统审核日志中筛选事件：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 打开“**系统审核日志**”子节点的上下文菜单，然后选择“**筛选器**”。
   将打开“**筛选设置**”窗口。
3. 若要添加筛选器，请执行以下步骤：
   a. 在“**字段名称**”中，选择要筛选事件的列。
   b. 在“**运算符**”列表中选择筛选条件。筛选条件因您在“**字段名称**”列表中选定的项目而有所不同。
   c. 在“**字段值**”中，选择筛选值。
   d. 单击“**添加**”按钮。

   已添加的筛选将出现在“**筛选设置**”窗口的筛选列表中。
4. 如有必要，请执行以下操作之一：

- 要使用逻辑运算符“AND”组合多个筛选，请选择“**如果满足所有条件**”。
- 要使用逻辑运算符“OR”组合多个筛选，请选择“**如果满足任一条件**”。

5. 单击“**应用**”按钮以在系统审核日志中保存筛选条件。

   系统审核日志的事件列表将仅显示满足筛选条件的事件。在您下次查看系统审核日志前，将保存筛选结果。

禁用筛选器：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 打开“**系统审核日志**”子节点的上下文菜单，然后选择“**删除筛选**”。

   系统审核日志的事件列表随后将显示所有事件。

删除系统审核日志中的事件

默认情况下，Kaspersky Embedded Systems Security 会无限期地存储系统审核日志中的记录。您可以指定系统审核日志中记录的存储周期。

可以手动删除系统审核日志中的所有事件。

要删除系统审核日志中的事件：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 打开“**系统审核日志**”子节点的上下文菜单，然后选择“**清除**”。
3. 执行以下步骤之一：
   - 如果要在删除系统审核日志中的事件之前将日志内容另存为 CSV 或 TXT 格式的文件，则单击删除确认窗口中的“**是**”按钮。在打开的窗口中，指定文件的名称和位置。
   - 如果不想将日志内容另存为文件，则单击删除确认窗口中的“**否**”按钮。

系统审核日志将被清除。

任务日志

本节提供有关 Kaspersky Embedded Systems Security 任务日志的信息以及如何管理它们的说明。

关于任务日志

在应用程序控制台中选择“**任务日志**”节点后，结果窗格中会显示有关 Kaspersky Embedded Systems Security 任务执行情况的信息。

在每个任务的日志中，可以查看任务执行情况的统计、自任务启动起应用程序已处理的每个对象的详细信息以及任务设置。

默认情况下，当任务完成后，Kaspersky Embedded Systems Security 将记录存储在任务日志中 30 天。您可以更改记录在任务日志中的存储期间。

您可以指定 Kaspersky Embedded Systems Security 存储包含任务日志的文件所使用的文件夹，而不使用默认的文件夹。还可以选择 Kaspersky Embedded Systems Security 将在任务日志中记录的事件。

在任务日志中查看事件列表

要查看任务日志：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择“**任务日志**”子节点。

Kaspersky Embedded Systems Security 任务日志中保存的事件列表将显示在结果窗格中。

事件可以按任意列进行排序，也可以进行筛选。

排序任务日志

默认情况下，任务日志按时间倒序显示。可以按任意列进行排序。

要排序任务日志：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择“**任务日志**”子节点。
3. 在结果窗格中，选择要用于排序 Kaspersky Embedded Systems Security 任务日志的列标题。

在您下次查看任务日志前，将保存排序结果。

筛选任务日志

您可以配置任务日志列表，以仅显示符合指定的筛选条件（筛选器）的任务日志。

要筛选任务日志：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 打开“**任务日志**”子节点的上下文菜单并选择“**筛选器**”。
   将打开“**筛选设置**”窗口。
3. 若要添加筛选器，请执行以下步骤：
   a. 在“**字段名称**”中，选择要筛选任务日志的列。
   b. 在“**运算符**”列表中选择筛选条件。筛选条件因您在“**字段名称**”列表中选定的项目而有所不同。
   c. 在“**字段值**”中，选择筛选值。

d. 单击“**添加**”按钮。

已添加的筛选将出现在“**筛选设置**”窗口的筛选列表中。

4. 如有必要，请执行以下操作之一：

- 要使用逻辑运算符“AND”组合多个筛选，请选择“**如果满足所有条件**”。
- 要使用逻辑运算符“OR”组合多个筛选，请选择“**如果满足任一条件**”。

5. 单击“**应用**”按钮，以在任务日志列表中保存筛选条件。

任务日志列表仅显示满足筛选条件的任务日志。在您下次查看任务日志前，将保存筛选结果。

禁用筛选器：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 打开“**任务日志**”子节点的上下文菜单并选择“**删除筛选**”。

任务日志列表将显示所有任务日志。

在任务日志中查看有关 Kaspersky Embedded Systems Security 任务的统计和信息

在任务日志中，可以查看自任务开始以来任务中发生的所有事件的详细信息，以及任务执行统计和任务设置。

要查看有关 Kaspersky Embedded Systems Security 任务的统计和信息：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择“**任务日志**”子节点。
3. 在结果窗格中，通过以下某种方法打开“**日志**”窗口：
   - 双击要查看的任务日志。
   - 打开要查看的任务日志的上下文菜单，选择“**查看日志**”。
4. 在打开的窗口中，将显示以下详细信息：
   - “**统计**”选项卡显示任务启动和完成时间及任务统计。
   - “**事件**”选项卡显示任务执行期间记录的事件列表。
   - “**选项**”选项卡显示任务设置。
5. 如有必要，请单击“**筛选器**”按钮以筛选任务日志中的事件。
6. 如有必要，请单击“**导出**”按钮以将任务日志中的数据导出至 CSV 或 TXT 格式的文件中。
7. 单击“**关闭**”按钮。

“**日志**”窗口将关闭。

导出任务日志中的信息

您可以将任务日志中的数据导出至 CSV 或 TXT 格式的文件中。

要导出任务日志中的信息：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择“**任务日志**”子节点。
3. 在结果窗格中，通过以下某种方法打开“**日志**”窗口：
   - 双击要查看的任务日志。
   - 打开要查看的任务日志的上下文菜单，选择“**查看日志**”。
4. 在“**日志**”窗口下部，单击“**导出**”按钮。
   将打开“**另存为**”窗口。
5. 指定要将数据从任务日志导出到的文件的名称、位置、类型和编码。
6. 单击“**保存**”按钮。

   将保存指定设置。

删除任务日志

默认情况下，当任务完成后，Kaspersky Embedded Systems Security 将记录存储在任务日志中 30 天。您可以更改记录在任务日志中的存储期间。

您可以手动删除已经完成的任务日志。

> 对于当前正在运行的任务及其他用户正在使用的任务，不会删除其日志中的事件。

要删除任务日志：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择“**任务日志**”子节点。
3. 执行以下步骤之一：
   - 如果要删除已完成的所有任务的日志，请打开“**任务日志**”子节点的上下文菜单，然后选择“**清除**”。
   - 如果要清除单个任务的日志，则在结果窗格中，打开要清除的任务日志的上下文菜单，然后选择“**删除**”。
   - 如果要清除多个任务的日志：
     a. 在结果窗格中，使用 **Ctrl** 或 **Shift** 键选择要清除的任务日志。

b. 打开任一选定任务日志的上下文菜单，然后选择“**删除**”。

4. 在删除确认窗口中单击“**是**”按钮以确认您要删除这些日志。

选择的任务日志将被清除。任务日志的删除将记录在系统审核日志中。

安全日志

Kaspersky Embedded Systems Security 保持有与受保护设备上的安全入侵或尝试进行安全入侵相关的事件的日志。本日志中记录以下事件：

- 漏洞利用防御事件。
- 关键日志审查事件。
- 表示尝试进行安全入侵的严重事件（对于“实时计算机保护”、“按需扫描”、“文件完整性监控”、“应用程序启动控制”和“设备控制”任务）。

您可以清除安全日志。此外，当清除安全日志时，Kaspersky Embedded Systems Security 会记录一个系统审核事件。

在事件查看器中查看 Kaspersky Embedded Systems Security 事件日志

您可以使用 Microsoft 管理控制台的 Microsoft Windows 事件查看器管理单元来查看 Kaspersky Embedded Systems Security 的事件日志。该日志包含由 Kaspersky Embedded Systems Security 记录且诊断运行故障所需的事件。

可以根据以下标准选择将记录在事件日志中的事件：

- **按事件类型**。
- **按详细级别**。详细级别与日志中记录的事件重要性级别相对应（信息、重要或严重事件）。最详细的级别是“信息”级别，将记录所有事件。最不详细的级别是“关键”级别，只记录关键事件。

要查看 Kaspersky Embedded Systems Security 事件日志：

1. 单击“**开始**”按钮，在搜索栏中输入 `mmc` 命令，然后按 **ENTER** 键。

   Microsoft 管理控制台打开。

2. 选择“**文件 > 添加或删除管理单元**”。

   将打开“**添加或删除管理单元**”窗口。

3. 在可用管理单元列表中，选择“**事件查看器**”管理单元并单击“**添加**”按钮。

   将打开“**选择计算机**”窗口。

4. 在“**选择计算机**”窗口中，指定已安装 Kaspersky Embedded Systems Security 的设备，然后单击“**确定**”。

5. 在“**添加和删除管理单元**”窗口中，单击“**确定**”。

   在 Microsoft 管理控制台树中，将出现“**事件查看器**”节点。

6. 展开“**事件查看器**”节点，并选择“**应用程序和服务日志 > Kaspersky Embedded Systems Security**”子节点。

将打开 Kaspersky Embedded Systems Security 事件日志。

通过应用程序控制台配置日志设置

您可以编辑 Kaspersky Embedded Systems Security 日志的以下设置：

- 事件在任务日志和系统审核日志中存储的时间长度。
- Kaspersky Embedded Systems Security 在其中存储任务日志文件和系统审核日志文件的文件夹的位置。
- *应用程序数据库已过期*、*应用程序数据库已严重过期*和*已很长时间未执行关键区域扫描*的事件生成阈值。
- Kaspersky Embedded Systems Security 在事件查看器中将保存到任务日志、系统审核日志和 Kaspersky Embedded Systems Security 事件日志中的事件。
- 用于将审核事件和任务执行事件通过 Syslog 协议发布到 syslog 服务器的设置。

要配置 Kaspersky Embedded Systems Security 日志，请执行下列步骤：

1. 在应用程序控制台树中，打开“**日志和通知**”节点的上下文菜单，并选择“**属性**”。
   将打开“**日志和通知设置**”窗口。
2. 在“**日志和通知设置**”窗口中，根据需要配置日志。为此，请执行以下操作：
   - 在“**常规**”选项卡上，如有必要，选择 Kaspersky Embedded Systems Security 在事件查看器中将保存到任务日志、系统审核日志和 Kaspersky Embedded Systems Security 事件日志中的事件。为此，请执行以下操作：
     - 在“**组件**”列表中，选择您要设置其详细级别的 Kaspersky Embedded Systems Security 组件。

       对于“实时文件保护”、“按需扫描”和“更新”组件，事件记录在任务日志和事件日志中。对于这些组件，事件表包含“**任务日志**”和“**Windows 事件日志**”列。“隔离”和“备份”组件的事件记录在系统审核日志和事件日志中。对于这些组件，事件表包含“**审核**”和“**Windows 事件日志**”列。

     - 在“**重要性级别**”列表中，选择事件在任务日志、系统审核日志和选定的组件的事件日志中的详细级别。
       在包含事件列表的下表中，使用任务日志、系统审核日志和事件日志，根据当前详细级别记录的事件旁边的复选框被选中。
     - 如果您想手动为选定的组件启用记录特定事件，请执行以下操作：

     a. 在“**重要性级别**”列表中选择“**自定义**”。

     b. 在包含事件列表的表格中，选中您想要记录到任务日志、系统审核日志和事件日志中的事件旁边的复选框。

   - 在“**高级**”选项卡上，配置设备保护状态的日志存储设置和事件生成阈值：
     - 在“**日志存储**”部分中：
       - 日志文件夹
       - 删除早于该天数的任务日志

- 删除早于该天数的系统审核日志事件(天)

- 在“**事件生成阈值**”部分：
  - 指定在经过多少天后，发生*应用程序数据库已过期*、*应用程序数据库已严重过期*和*已很长时间未执行关键区域扫描*事件。

- 在“**SIEM 集成**”选项卡上，配置用于将审核事件和任务执行事件发布到 syslog 服务器的设置。

3. 单击“**确定**”以保存更改。

关于 SIEM 集成

为了减小低性能设备上的负载和降低由于应用程序日志大小增大而造成系统性能降级的风险，可以通过 Syslog 协议将审核事件和任务性能事件的发布配置到 *syslog 服务器*。

syslog 服务器是用于聚合事件 (SIEM) 的外部服务器。它存储和分析收到的事件，并执行其他日志管理操作。

可以在两种模式中使用 SIEM 集成：

- 在 syslog 服务器上复制事件：在此模式下，其发布在日志设置中进行配置的所有任务性能事件以及所有系统审核事件，即使在发送到 SIEM 服务器后仍继续存储在受保护设备上。

  建议使用此模式以尽可能减少受保护设备上的负载。

- 删除事件的本地副本：在此模式下，在应用程序运行过程中注册和发布到 SIEM 的所有事件将从受保护设备中删除。

  > 应用程序永远不会删除安全日志的本地版本。

Kaspersky Embedded Systems Security 可以将应用程序日志中的事件转换为 syslog 服务器支持的格式，以便这些事件能够被传输和被 SIEM 服务器成功识别。应用程序支持转换为结构化数据格式和 JSON 格式。

建议根据使用的 SIEM 服务器的配置来选择事件的格式。

可靠性设置

通过定义连接到镜像 syslog 服务器的设置，可以降低事件传输到 SIEM 服务器不成功的风险。

镜像 syslog 服务器是一个额外的 syslog 服务器，如果与主 syslog 服务器的连接不可用或不能使用主服务器，应用程序会自动切换到该服务器。

Kaspersky Embedded Systems Security 还使用系统审核事件来通知您尝试连接 SIEM 服务器不成功以及将事件发送到 SIEM 服务器时出错。

配置 SIEM 集成设置

默认情况下，不使用 SIEM 集成。您可以启用和禁用 SIEM 集成，并配置相关设置（参见下表）。

SIEM 集成设置

设置	默认值	描述
通过 syslog 协议发送事件到远程 syslog 服务器	未应用	可以分别通过选择或清除该复选框来启用或禁用 SIEM 集成。
删除已被发送到远程 syslog 服务器的事件本地副本	未应用	可以通过选中或清除复选框来配置将日志发送到 SIEM 服务器后存储日志本地副本的设置。
事件格式	结构化数据	可以选择两种格式之一，应用程序在将事件发送到 syslog 服务器以便 SIEM 服务器能够更好进行识别之前，将事件转换为该格式。
连接协议	TCP	可以使用下拉列表来配置通过 UDP 或 TCP 协议与主 syslog 服务器和镜像 syslog 服务器的连接。
主 syslog 服务器连接设置	IP 地址：127.0.0.1 端口：514	可以使用适当的字段来配置用于连接到主 syslog 服务器的 IP 地址和端口。 可以指定 IP 地址仅为 IPv4 格式。
如果无法访问主服务器则使用镜像 syslog 服务器	未应用	可以使用复选框来启用或禁用镜像 syslog 服务器。
镜像 syslog 服务器连接设置	IP 地址：127.0.0.1 端口：514	可以使用适当的字段来配置用于连接到镜像 syslog 服务器的 IP 地址和端口。 可以指定 IP 地址仅为 IPv4 格式。

要配置 SIEM 集成设置：

1. 在应用程序控制台树中，打开“**日志和通知**”节点的上下文菜单。
2. 选择“**属性**”。
   将打开“**日志和通知设置**”窗口。
3. 选择“**SIEM 集成**”选项卡。
4. 在“**集成设置**”部分中，选择“**通过 syslog 协议发送事件到远程 syslog 服务器**”复选框。
5. 如果需要，在“**集成设置**”部分中，选中“**删除已被发送到远程 syslog 服务器的事件本地副本**”复选框。

   “**删除已被发送到远程 syslog 服务器的事件本地副本**”复选框的状态不会影响保存安全日志事件的设置：应用程序永远不会自动删除安全日志事件。
6. 在“**事件格式**”部分中，指定您要将应用程序事件转换成的格式，以便能够将它们发送到 SIEM 服务器。
   默认情况下，应用程序将它们转换为结构化数据格式。
7. 在“**连接设置**”部分中：
   - 指定 SIEM 连接协议。
   - 指定用于连接到主 syslog 服务器的设置。
     只能指定 IPv4 格式的 IP 地址。

- 当无法发送事件到主 syslog 服务器时，如果想让应用程序使用其他连接设置，请选中“**如果无法访问主服务器则使用镜像 syslog 服务器**”复选框。

  指定以下用于连接到镜像 syslog 服务器的设置：“**地址**”和“**端口**”。

  如果已清除“**如果无法访问主服务器则使用镜像 syslog 服务器**”复选框，则无法编辑镜像 syslog 服务器的“**地址**”和“**端口**”字段。

  只能指定 IPv4 格式的 IP 地址。

8. 单击“**确定**”。

   将应用已配置的 SIEM 集成设置。

通过管理插件配置日志和通知设置

可以使用 Kaspersky Security Center 管理控制台为管理员和用户配置有关 Kaspersky Embedded Systems Security 运行中的以下事件和设备的反病毒保护状态的通知：

- 管理员可以收到有关选定类型事件的信息。
- 访问受保护设备的 LAN 用户和终端受保护设备用户可以收到有关*检测到对象*事件的信息。

可使用选定受保护设备的“**属性:<受保护设备名称>**”窗口为单个受保护设备，或使用选定管理组的“**属性：<策略名称>**”窗口为一组受保护设备配置有关 Kaspersky Embedded Systems Security 事件的通知。

在“**事件通知**”选项卡上或在“**通知设置**”窗口中，可以配置以下类型的通知：

- 可以使用“**事件通知**”选项卡（Kaspersky Security Center 中的标准选项卡）配置有关选定类型事件的管理员通知。有关通知方法的详细信息，请参见 *Kaspersky Security Center 帮助*。
- 在“**通知设置**”窗口中，可以配置管理员通知和用户通知。

某些事件类型的通知只能在窗口或选项卡中配置；其他事件类型的通知可以同时在窗口和选项卡中配置。

如果在“**事件通知**”选项卡上和“**通知设置**”窗口中使用相同模式配置关于同一类型事件的通知，系统管理员将以相同的模式收到两次这些事件的通知。

配置任务日志设置

要配置 Kaspersky Embedded Systems Security 日志，请执行下列步骤：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**日志和通知**”部分中，单击“**任务日志**”子部分中的“**设置**”按钮。
5. 在“**日志设置**”窗口中，根据您的需要定义以下 Kaspersky Embedded Systems Security 设置：
   - 配置日志中的事件的详细级别。为此，请执行以下操作：
     a. 在“**组件**”列表中，选择您要设置其详细级别的 Kaspersky Embedded Systems Security 组件。
     b. 若要定义选定组件的任务日志和系统审核日志中的详细级别，请从“**重要性级别**”中选择所需级别。
   - 要更改日志的默认位置，请指定文件夹的绝对路径，或单击“**浏览**”按钮进行选择。
   - 指定任务日志的存储天数。
   - 指定“**系统审核日志**”节点中显示的信息的存储天数。
6. 单击“**确定**”。

已保存配置的日志设置。

安全日志

Kaspersky Embedded Systems Security 保持有与受保护设备上的安全入侵或尝试进行安全入侵相关的事件的日志。本日志中记录以下事件：

- 漏洞利用防御事件。
- 关键日志审查事件。
- 表示尝试进行安全入侵的严重事件（对于“实时计算机保护”、“按需扫描”、“文件完整性监控”、“应用程序启动控制”和“设备控制”任务）。

您可以清除安全日志。此外，当清除安全日志时，Kaspersky Embedded Systems Security 会记录一个系统审核事件。

配置 SIEM 集成设置

为了减小低性能设备上的负载和降低由于应用程序日志大小增大而造成系统性能降级的风险，可以通过 Syslog 协议将审核事件和任务性能事件的发布配置到 *syslog 服务器*。

syslog 服务器是用于聚合事件 (SIEM) 的外部服务器。它存储和分析收到的事件，并执行其他日志管理操作。

可以在两种模式中使用 SIEM 集成：

- 在 syslog 服务器上复制事件：在此模式下，其发布在日志设置中进行配置的所有任务性能事件以及所有系统审核事件，即使在发送到 SIEM 服务器后仍继续存储在受保护设备上。

  建议使用此模式以尽可能减少受保护设备上的负载。

- 删除事件的本地副本：在此模式下，在应用程序运行过程中注册和发布到 SIEM 的所有事件将从受保护设备中删除。

  应用程序永远不会删除安全日志的本地版本。

Kaspersky Embedded Systems Security 可以将应用程序日志中的事件转换为 syslog 服务器支持的格式，以便这些事件能够被传输和被 SIEM 服务器成功识别。应用程序支持转换为结构化数据格式和 JSON 格式。

为降低事件传输到 SIEM 服务器不成功的风险，您可以定义连接到镜像 syslog 服务器的设置。

镜像 syslog 服务器是一个额外的 syslog 服务器，如果与主 syslog 服务器的连接不可用或不能使用主服务器，应用程序会自动切换到该服务器。

默认情况下，不使用 SIEM 集成。您可以启用和禁用 SIEM 集成，并配置相关设置（参见下表）。

SIEM 集成设置

设置	默认值	描述
通过 syslog 协议发送事件到远程 syslog 服务器	未应用	可以分别通过选择或清除该复选框来启用或禁用 SIEM 集成。
删除已被发送到远程 syslog 服务器的事件本地副本	未应用	可以通过选中或清除复选框来配置将日志发送到 SIEM 服务器后存储日志本地副本的设置。
事件格式	结构化数据	可以选择两种格式之一，应用程序在将事件发送到 syslog 服务器以便 SIEM 服务器能够更好进行识别之前，将事件转换为该格式。
连接协议	TCP	可以使用下拉列表来配置通过 UDP 或 TCP 协议与主 syslog 服务器的连接，以及通过 TCP 协议与镜像 syslog 服务器的连接。
主 syslog 服务器连接设置	IP 地址：127.0.0.1 端口：514	可以使用适当的字段来配置用于连接到主 syslog 服务器的 IP 地址和端口。 可以指定 IP 地址仅为 IPv4 格式。
如果无法访问主服务器则使用镜像 syslog 服务器	未应用	可以使用复选框来启用或禁用镜像 syslog 服务器。
镜像 syslog 服务器连接设置	IP 地址：127.0.0.1 端口：514	可以使用适当的字段来配置用于连接到镜像 syslog 服务器的 IP 地址和端口。 可以指定 IP 地址仅为 IPv4 格式。

要配置 SIEM 集成设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**日志和通知**”部分中，单击“**任务日志**”子部分中的“**设置**”按钮。

   将打开“**日志和通知设置**”窗口。

5. 选择“**SIEM 集成**”选项卡。

6. 在“**集成设置**”部分中，选择“通过 syslog 协议发送事件到远程 syslog 服务器”复选框。

7. 如果需要，在“**集成设置**”部分中，选中“删除已被发送到远程 syslog 服务器的事件本地副本”复选框。

   “**删除已被发送到远程 syslog 服务器的事件本地副本**”复选框的状态不会影响保存安全日志事件的设置：应用程序永远不会自动删除安全日志事件。

8. 在“**事件格式**”部分中，指定您要将应用程序事件转换成的格式，以便能够将它们发送到 SIEM 服务器。

   默认情况下，应用程序将它们转换为结构化数据格式。

9. 在“**连接设置**”部分中：

   - 指定 SIEM 连接协议。
   - 指定用于连接到主 syslog 服务器的设置。

     只能指定 IPv4 格式的 IP 地址。
   - 当无法发送事件到主 syslog 服务器时，如果想让应用程序使用其他连接设置，请选中“**如果无法访问主服务器则使用镜像 syslog 服务器**”复选框。

     指定以下用于连接到镜像 syslog 服务器的设置：“**地址**”和“**端口**”。

     如果已清除“**如果无法访问主服务器则使用镜像 syslog 服务器**”复选框，则无法编辑镜像 syslog 服务器的“**地址**”和“**端口**”字段。

     只能指定 IPv4 格式的 IP 地址。

10. 单击“**确定**”。

将应用已配置的 SIEM 集成设置。

配置通知设置

要配置 Kaspersky Embedded Systems Security 通知，请执行以下步骤：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。

- 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

  如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**日志和通知**”部分中，单击“**事件通知**”子部分中的“**设置**”按钮。
5. 在“**通知设置**”窗口中，根据您的需要定义以下 Kaspersky Embedded Systems Security 设置：
   - 在“**通知设置**”列表中，选择想要配置其设置的通知类型。
   - 在“**通知用户**”部分中，配置用户通知方式。如有必要，输入通知消息的文本。
   - 在“**通知管理员**”部分中，配置管理员通知方式。如有必要，输入通知消息的文本。如有必要，通过单击“**设置**”按钮配置附加通知设置。
   - 在“**事件生成阈值**”部分中，指定 Kaspersky Embedded Systems Security 记录“*应用程序数据库已过期*”、“*应用程序数据库已严重过期*”和“*已很长时间未执行关键区域扫描*”事件的时间间隔。
     - 应用程序数据库已过期(天)
     - 应用程序数据库已严重过期(天)
     - 已很长时间未执行关键区域扫描(天)
6. 单击“**确定**”。

将保存配置的通知设置。

配置与管理服务器的交互

要选择 Kaspersky Embedded Systems Security 将其有关信息发送到 Kaspersky Security Center 管理服务器的对象类型：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**日志和通知**”部分中，单击“**与管理服务器交互**”子部分中的“**设置**”按钮。

   将打开“**管理服务器网络列表**”窗口。

5. 在“**管理服务器网络列表**”窗口中，选择 Kaspersky Embedded Systems Security 将其有关信息发送到 Kaspersky Security Center 管理服务器的对象类型：

   - 隔离的对象。
   - 已备份对象。

6. 单击“**确定**”。

   Kaspersky Embedded Systems Security 会将有关选定对象类型的信息发送到管理服务器。

通知设置

本节提供有关采用何种方式向 Kaspersky Embedded Systems Security 的用户和管理员通知应用程序事件和设备保护状态的信息，并说明如何配置通知。

管理员和用户通知方式

您可以将应用程序配置为将 Kaspersky Embedded Systems Security 运行中的以下事件和设备的反病毒保护状态通知给管理员和访问设备的用户。

- 管理员可以收到有关选定类型事件的信息。
- 访问设备的 LAN 用户和终端设备用户可以收到有关“实时文件保护”任务中“*检测到对象*”类型的事件的信息。

在应用程序控制台中，可以使用多种方式激活管理员或用户通知：

- 用户通知方式：
  a. 终端服务工具。
     如果受保护设备用作终端，则可以应用此方法来通知终端受保护设备。
  b. 消息服务工具。
     您可以通过 Microsoft Windows 消息服务应用此方式来进行通知。
- 管理员通知方式：
  a. 消息服务工具。
     您可以通过 Microsoft Windows 消息服务应用此方式来进行通知。
  b. 运行可执行文件。
     此方法是在发生事件时运行受保护设备本地驱动器上存储的可执行文件。
  c. 通过电子邮件发送。
     该方式使用电子邮件传输消息。

您可以为单个事件类型创建消息文本。它可以包括用以说明事件的消息字段。默认情况下，应用程序使用默认消息通知用户。

配置管理员和用户通知

事件通知设置使您可以选择配置和编写消息文本的方式。

要配置事件通知设置：

1. 在应用程序控制台树中，打开“**日志和通知**”节点的上下文菜单，并选择“**属性**”。
   将打开“**日志和通知设置**”窗口。
2. 在“**通知**”选项卡中，选择通知模式：

a. 从“**事件类型**”列表中选择您希望为其选择通知方式的事件。

b. 在“**通知管理员**”或“**通知用户**”组设置中，选中您希望配置的通知方式旁边的复选框。

只能为以下事件配置用户通知：“**检测到对象**”事件、“**检测到不受信任的外部设备并限制该设备**”事件和“**网络会话被列为不信任**”事件。

3. 添加消息文本：

a. 单击“**消息文本**”按钮。

b. 在打开的窗口中输入要在相应的事件消息中显示的文本。

您可以为多个事件类型创建相同消息：为一个事件类型选择通知方式后，使用 **Ctrl** 或 **Shift** 键选择要使用相同消息的其他事件类型，然后单击“**消息文本**”按钮。

a. 若要添加有关事件信息的字段，请单击“**宏**”按钮，然后从下拉列表中选择相关字段。事件信息字段在本部分中的表中有所说明。

b. 若要还原默认事件消息文本，请单击“**按默认**”按钮。

4. 要配置选定事件的管理员通知方式，请选择“**通知**”选项卡，单击“**通知管理员**”部分中的“**设置**”按钮，并在“**高级设置**”窗口中配置选定的方式。为此，请执行以下操作：

a. 对于电子邮件通知，请打开“**电子邮件**”选项卡，然后在相应的字段中指定收件人的电子邮件地址（地址使用分号隔开）、SMTP 服务器的名称或网络地址以及端口号。如有必要，请指定在“**主题**”和“**发件人**”字段中显示的文本。在“**主题**”字段中也可以包括有关事件信息的变量（请参见下表）。

如果您希望在连接 SMTP 服务器时应用用户账户身份验证，请在“**身份验证设置**”组中选择“**使用 SMTP 身份验证**”，然后指定要身份验证其用户账户的用户的名称和密码。

b. 对于使用 Windows Messenger 服务的通知，请在“**Windows Messenger 服务**”选项卡上创建通知收件人受保护设备的列表：对于您希望添加的每台受保护设备，请单击“**添加**”按钮并在输入字段中输入其网络名称。

c. 要运行可执行文件，请在受保护设备的本地驱动器上选择当发生事件时在受保护设备上执行的文件，或在“**可执行文件**”选项卡上输入其完整路径。输入用于执行文件的用户名和密码。

指定可执行文件的路径时可使用系统环境变量；不允许使用用户环境变量。

如果您希望限制一种事件类型在一段时间内的消息数量，请在“**高级**”选项卡上选择“**发送相同通知不超过**”，然后指定次数和时间间隔。

5. 单击“**确定**”。

将保存配置的通知设置。

事件信息字段

变量	描述
%EVENT_TYPE%	事件类型。
%EVENT_TIME%	事件时间。
%EVENT_SEVERITY%	重要性级别。
%OBJECT%	对象名称（在“实时计算机保护”和“按需扫描”任务中）。

	“软件模块更新”任务包括更新的名称和带有更新信息的网页地址。
%VIRUS_NAME%	根据病毒百科全书分类确定的对象名称。该名称包含在 Kaspersky Embedded Systems Security 检测对象时返回的检测到的对象全名中。您可以在任务日志中查看检测到的对象的全名。
%VIRUS_TYPE%	根据 Kaspersky 分类确定的检测到的对象类型，例如“病毒”或“木马”。它包含在 Kaspersky Embedded Systems Security 发现被感染的对象或疑似感染的对象时返回的检测到的对象全名中。您可以在任务日志中查看检测到的对象的全名。
%USER_COMPUTER%	在“实时文件保护”任务中，访问了设备上的对象的用户的受保护设备名称。
%USER_NAME%	在“实时文件保护”任务中，访问设备上的对象的用户的名称。
%FROM_COMPUTER%	发出通知的受保护设备的名称。
%EVENT_REASON%	发生事件的原因（某些事件没有该字段）。
%ERROR_CODE%	错误代码（仅用于“内部任务错误”事件）。
%TASK_NAME%	任务名称（仅适用于与任务性能相关的事件）。

启动和停止 Kaspersky Embedded Systems Security

本节包含有关启动应用程序控制台的信息，以及有关启动和停止 Kaspersky Security 服务的信息。

启动 Kaspersky Embedded Systems Security 管理插件

在 Kaspersky Security Center 中启动 Kaspersky Embedded Systems Security 管理插件无需执行额外的操作。在管理员的受保护设备上安装该插件后，它会与 Kaspersky Security Center 一起启动。有关启动 Kaspersky Security Center 的详细信息，请参见 *Kaspersky Security Center 帮助*。

从开始菜单启动 Kaspersky Embedded Systems Security 控制台

在不同 Windows 操作系统中，设置的名称可能有所不同。

要从"开始"菜单启动应用程序控制台：

1. 在"**开始**"菜单中，选择"**程序**" > "**Kaspersky Embedded Systems Security**" > "**管理工具**" > "**Kaspersky Embedded Systems Security 控制台**"。

要向应用程序控制台中添加其他管理单元，请以作者模式启动应用程序控制台。

要在作者模式下启动应用程序控制台：

1. 在"**开始**"菜单中，选择"**程序**" > "**Kaspersky Embedded Systems Security**" > "**管理工具**"。
2. 在应用程序控制台的上下文菜单中，选择"**作者**"命令。

   将以作者模式启动应用程序控制台。

如果已在受保护设备上启动应用程序控制台，应用程序控制台窗口将打开。

如果在非受保护设备上启动了应用程序控制台，请连接到受保护设备。

要连接到受保护设备：

1. 在应用程序控制台树中，打开 **Kaspersky Embedded Systems Security** 节点的上下文菜单。
2. 选择"**连接至其他计算机**"命令。

   将打开"**选择受保护设备**"窗口。
3. 在打开的窗口中选择"**其他设备**"。
4. 在右侧的输入字段中指定受保护设备的网络名称。
5. 单击"**确定**"。

   应用程序控制台将连接到受保护设备。

如果用来登录 Microsoft Windows 的用户账户没有足够权限来访问受保护设备上的 Kaspersky Security 管理服务，则选中“**使用以下用户进行连接**”复选框，然后指定具有所需权限的其他用户账户。

启动和停止 Kaspersky Security 服务

默认情况下，Kaspersky Security 服务会在操作系统启动后立即自动启动。Kaspersky Security 服务管理的工作进程执行“实时计算机保护”、“计算机控制”、“按需扫描”和更新任务。

默认情况下，当 Kaspersky Embedded Systems Security 启动时，将启动“实时文件保护”和“在操作系统启动时扫描”任务以及其他计划在“**应用程序启动时**”启动的任务。

如果停止 Kaspersky Security 服务，则会停止所有正在运行的任务。重新启动 Kaspersky Security 服务之后，应用程序只会自动启动已计划为在“**应用程序启动时**”运行的任务，而其他任务必须手动启动。

您可以使用 **Kaspersky Embedded Systems Security** 节点的上下文菜单或使用 Microsoft Windows 服务管理单元启动和停止 Kaspersky Security 服务。

如果您是受保护设备上“管理员”组的成员，您可以启动和停止 Kaspersky Embedded Systems Security。

要使用应用程序控制台停止或启动应用程序：

1. 在应用程序控制台树中，打开 **Kaspersky Embedded Systems Security** 节点的上下文菜单。
2. 选择以下项之一：
   - **停止服务**。
   - **启动服务**。

将启动或停止 Kaspersky Security 服务。

在操作系统安全模式下启动 Kaspersky Embedded Systems Security

本节提供有关在操作系统安全模式下工作的 Kaspersky Embedded Systems Security 的信息。

关于在操作系统安全模式下工作的 Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security 组件可以在操作系统以安全模式加载时启动。除了 Kaspersky Security 服务 (kavfs.exe)，还将加载 klam.sys 驱动程序。它用于在操作系统启动期间将 Kaspersky Security 服务注册为受保护服务。有关详细信息，请参见“将 Kaspersky Security 服务注册为受保护服务”部分。

Kaspersky Embedded Systems Security 可以在操作系统的以下安全模式下启动：

- 最小安全模式 - 选择操作系统安全模式的标准选项时，将启动此模式。此时，Kaspersky Embedded Systems Security 可以启动以下组件：
  - 实时文件保护。
  - 按需扫描。

- 应用程序启动控制和应用程序启动控制规则生成器。
- 日志审查。
- 文件完整性监控。
- 基线文件完整性监控。
- 应用程序完整性控制。

网络安全模式 – 在此模式下，操作系统以带有网络驱动程序的安全模式加载。除了在最小安全模式下启动的组件，Kaspersky Embedded Systems Security 在此模式下还可以启动以下组件：

- 数据库更新。
- 软件模块更新。

在安全模式下启动 Kaspersky Embedded Systems Security

默认情况下，在操作系统以安全模式加载时，不启动 Kaspersky Embedded Systems Security。

要使 Kaspersky Embedded Systems Security 在操作系统安全模式下启动：

1. 启动 Windows 注册表编辑器 (C:\Windows\regedit.exe)。
2. 打开系统注册表的 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] 项。
3. 打开 LoadInSafeMode 参数。
4. 将值设置为 `1`。
5. 单击“**确定**”。

要取消 Kaspersky Embedded Systems Security 在操作系统安全模式下启动：

1. 启动 Windows 注册表编辑器 (C:\Windows\regedit.exe)。
2. 打开系统注册表的 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] 项。
3. 打开 LoadInSafeMode 参数。
4. 将值设置为 `0`。
5. 单击“**确定**”。

Kaspersky Embedded Systems Security 自我保护

本节提供有关 Kaspersky Embedded Systems Security 自我保护机制的信息。

关于 Kaspersky Embedded Systems Security 自我保护

Kaspersky Embedded Systems Security 具有自我保护机制，可防止该应用程序的文件夹、内存进程和系统注册表项被修改或删除。

防止包含已安装的 Kaspersky Embedded Systems Security 组件的文件夹被更改

Kaspersky Embedded Systems Security 会阻止任何用户账户对包含已安装的应用程序组件的文件夹进行重命名和删除。默认情况下，应用程序安装文件夹的路径如下：

- 在 32 位版本的 Microsoft Windows 中：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- 在 64 位版本的 Microsoft Windows 中：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

防止 Kaspersky Embedded Systems Security 注册表项被更改

Kaspersky Embedded Systems Security 会限制对以下注册表分支和注册表项的访问，这些注册表项提供了应用程序驱动程序和服务的加载：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2]（64 位版本的 Microsoft Windows 上）
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\Trace]

更改这些注册表分支和注册表项的权限仅授予给本地系统 (SYSTEM) 账户。用户和管理员账户被授予只读权限。

防止程序服务部件内存发生更改

为了保护程序服务部件不受第三方进程的影响，Kaspersky Embedded Systems Security 驱动程序限制对以下可执行文件的访问：

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

默认情况下，第三方进程对 Kaspersky Embedded Systems Security 服务部件内存的访问受到限制。

您可以在 Kaspersky Embedded Systems Security 控制台和 Kaspersky Embedded Systems Security 管理插件策略属性中启用自我防御功能。

将 Kaspersky Security 服务注册为受保护服务

轻度受保护进程（也称为“PPL”）技术确保操作系统只加载受信任的服务和进程。对于要作为受保护服务运行的服务，必须在受保护设备上安装*早期启动反恶意软件*驱动程序。

早期启动反恶意软件（也称为“ELAM”）驱动程序在网络中的设备启动时及第三方驱动程序初始化之前为这些设备提供保护。

ELAM 驱动程序在 Kaspersky Embedded Systems Security 安装期间自动安装，用于在操作系统启动时将 Kaspersky Security 服务注册为 PPL。Kaspersky Security 服务 (KAVFS) 作为系统保护进程启动后，系统中的其他非受保护进程将不能注入线程、写入受保护进程的虚拟内存或停止服务。

当某个进程以 PPL 的形式启动时，用户无法对其进行管理，不管分配的用户权限如何。Microsoft Windows 10 及更高版本操作系统支持使用 ELAM 驱动程序将 Kaspersky Security 服务注册为 PPL。如果在运行支持 PPL 的操作系统的服务器上安装 Kaspersky Embedded Systems Security，Kaspersky Security 服务 (KAVFS) 的权限管理将不可用。

要将 Kaspersky Embedded Systems Security 安装为 PPL，请运行以下命令：

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

管理 Kaspersky Embedded Systems Security 功能的访问权限

本节包含有关 Kaspersky Embedded Systems Security 和该应用程序注册的操作系统服务的管理权限的信息，以及如何配置这些权限的说明。

关于 Kaspersky Embedded Systems Security 的管理权限

默认情况下，为受保护设备上的管理员组的用户、在安装 Kaspersky Embedded Systems Security 的过程中在受保护设备上创建的 ESS 管理员组的用户以及 SYSTEM 组授予对所有 Kaspersky Embedded Systems Security 功能的访问权限。

对 Kaspersky Embedded Systems Security 有"编辑"权限访问级别的用户可以向受保护设备上注册的其他用户或者该域中包含的用户授予对 Kaspersky Embedded Systems Security 功能的访问权限。

未在 Kaspersky Embedded Systems Security 用户列表中注册的用户无法打开应用程序控制台。

您可以为用户或用户组选择以下预设访问权限级别之一：

- **完全控制** – 所有应用程序功能的访问权限：可以查看和编辑 Kaspersky Embedded Systems Security 常规设置、组件设置和 Kaspersky Embedded Systems Security 用户权限，还可以查看 Kaspersky Embedded Systems Security 统计。
- **修改** – 除编辑用户权限以外的所有应用程序功能的访问权限：可以查看和编辑 Kaspersky Embedded Systems Security 常规设置和 Kaspersky Embedded Systems Security 组件设置。
- **读取** – 可以查看 Kaspersky Embedded Systems Security 常规设置、Kaspersky Embedded Systems Security 组件设置、Kaspersky Embedded Systems Security 统计和 Kaspersky Embedded Systems Security 用户权限。

您还可以配置高级访问权限：允许或阻止访问 Kaspersky Embedded Systems Security 的特定功能。

如果您已为某个用户或组手动配置访问权限，则为该用户或组设置"**特殊权限**"访问级别。

关于 Kaspersky Embedded Systems Security 功能的访问权限

用户权限	描述
任务管理	可启动/停止/暂停/恢复 Kaspersky Embedded Systems Security 任务。
创建和删除按需扫描任务	可创建和删除按需扫描任务。
编辑设置	可执行以下操作： • 从配置文件导入 Kaspersky Embedded Systems Security 设置。 • 编辑应用程序设置。
读取设置	可执行以下操作： • 查看 Kaspersky Embedded Systems Security 常规设置和任务设置。 • 将 Kaspersky Embedded Systems Security 设置导出到配置文件。 • 查看任务日志、系统审核日志和通知的设置。
管理存储库	可执行以下操作： • 将对象移到隔离。 • 从隔离和备份中删除对象。 • 从隔离和备份中恢复对象。
管理日志	可删除任务日志和清除系统审核日志。
读取日志	可查看任务日志和系统审核日志中的反病毒事件。

读取统计	可查看每个 Kaspersky Embedded Systems Security 任务的统计。
应用程序授权	能激活 Kaspersky Embedded Systems Security。
卸载应用程序	可卸载 Kaspersky Embedded Systems Security。
读取权限	可查看 Kaspersky Embedded Systems Security 用户和用户访问权限的列表。
编辑权限	可执行以下操作： • 编辑具有应用程序管理访问权限的用户列表。 • 编辑 Kaspersky Embedded Systems Security 功能的用户访问权限。

关于管理注册服务的权限

安装过程中，Kaspersky Embedded Systems Security 会在 Windows 中注册 Kaspersky Security 服务 (KAVFS) 和 Kaspersky Security 管理服务 (KAVFSGT) 以及 Kaspersky Security 漏洞利用防御 (KAVFSSLP)。

在 Microsoft Windows 10 及更高版本的操作系统上，可以使用 ELAM 驱动程序将 Kaspersky Security 服务注册为轻度受保护进程。当某个进程以 PPL 的形式启动时，用户无法对其进行管理，不管分配的用户权限如何。如果在运行支持 PPL 的操作系统的受保护设备上安装 Kaspersky Embedded Systems Security，权限管理将不可用于 Kaspersky Security 服务 (KAVFS)。

Kaspersky Security 服务

默认情况下，将管理 Kaspersky Security 服务的访问权限授予受保护设备上“管理员”组中的用户，以及具有读取权限的 SERVICE 和 INTERACTIVE 组，和具有读取和执行权限的 SYSTEM 组。

具有“编辑权限”级别访问权限的用户可以向在受保护服务器上注册的其他用户或者该域中包含的其他用户授予对管理 Kaspersky Security 服务的访问权限。

Kaspersky Security 管理服务

要通过安装在其他受保护设备上的应用程序控制台来管理应用程序，使用其权限与 Kaspersky Embedded Systems Security 建立连接的账户必须对受保护设备上的 Kaspersky Security 管理服务具有完全访问权限。

默认情况下，系统向以下两组用户授予访问所有 Kaspersky Security 管理服务的权限：受保护设备上的管理员组的用户，以及安装 Kaspersky Embedded Systems Security 时在受保护设备上创建的 ESS 管理员组的用户。

只能通过 Microsoft Windows 服务管理单元管理 Kaspersky Security 管理服务。

Kaspersky Security 漏洞利用防御

默认情况下，将管理 Kaspersky Security 漏洞利用防御服务的访问权限授予受保护设备上“管理员”组中的用户，以及具有读取和执行权限的 SYSTEM 组。

关于 Kaspersky Security 管理服务的访问权限

您可以查看 Kaspersky Embedded Systems Security 服务的列表。

在安装过程中，Kaspersky Embedded Systems Security 会注册 Kaspersky Security 管理服务 (KAVFSGT)。要通过安装在其他受保护设备上的应用程序控制台来管理应用程序，用来连接到 Kaspersky Embedded Systems Security 的账户必须对受保护设备上的 Kaspersky Security 管理服务具有完全访问权限。

默认情况下，系统向以下两组用户授予访问所有 Kaspersky Security 管理服务的权限：受保护设备上的管理员组的用户，以及安装 Kaspersky Embedded Systems Security 时在受保护设备上创建的 ESS 管理员组的用户。

只能通过 Microsoft Windows 服务管理单元管理 Kaspersky Security 管理服务。

您不能通过配置 Kaspersky Embedded Systems Security 来允许或阻止用户访问 Kaspersky Security 管理服务。

您可以从本地账户连接到 Kaspersky Embedded Systems Security，只要在受保护设备上注册具有相同用户名和密码的账户即可。

关于 Kaspersky Security 服务的管理权限

在安装过程中，Kaspersky Embedded Systems Security 在 Windows 中注册 Kaspersky Security 服务 (KAVFS)，并在内部启用在启动操作系统时启动的功能组件。为了降低第三方通过 Kaspersky Security 服务的管理访问应用程序功能和受保护设备上安全性设置的风险，可以从应用程序控制台或管理插件限制管理 Kaspersky Security 服务的权限。

默认情况下，用于管理 Kaspersky Security 服务的访问权限被授予受保护设备上管理员组中的用户。读取权限被授予 SERVICE 和 INTERACTIVE 组，读取和执行权限被授予 SYSTEM 组。

您无法删除 SYSTEM 用户账户或编辑此账户的权限。如果编辑 SYSTEM 账户的权限，则当保存更改时会恢复此账户的最大权限。

有权访问需要“编辑”权限的功能的用户可以向在受保护设备上注册的其他用户或者该域中包含的其他用户授予对管理 Kaspersky Security 服务的访问权限。

您可以为 Kaspersky Embedded Systems Security 用户或用户组选择以下预设的权限级别之一以管理 Kaspersky Security 服务：

- **完全控制**：可查看和编辑 Kaspersky Security 服务的常规设置和用户权限，以及启动和停止 Kaspersky Security 服务。
- **读取**：可查看 Kaspersky Security 服务常规设置和用户权限。
- **修改**：可查看和编辑 Kaspersky Security 服务常规设置和用户权限。
- **执行**：可启动和停止 Kaspersky Security 服务。

您还可以配置高级访问权限：允许或拒绝访问指定的 Kaspersky Embedded Systems Security 功能（请参见下表）。

如果您已为某个用户或组手动配置访问权限，则为该用户或组设置“**特殊权限**”访问级别。

Kaspersky Security 服务功能的访问权限

功能	描述
查看服务配置	可查看 Kaspersky Security 服务常规设置和用户权限。
从服务控制管理器请求服务状态	可从 Microsoft Windows 服务控制管理器请求 Kaspersky Security 服务的执行状态。
从服务请求状态	可从 Kaspersky Security 服务请求服务执行状态。
读取依存服务列表	可查看 Kaspersky Security 服务依存的以及依存于 Kaspersky Security 服务的服务列表。
编辑服务设置	可查看和编辑 Kaspersky Security 服务常规设置和用户权限。
启动服务	可启动 Kaspersky Security 服务。
停止服务	可停止 Kaspersky Security 服务。
暂停/恢复服务	可暂停和恢复 Kaspersky Security 服务。
读取权限	可查看 Kaspersky Security 服务用户列表和每个用户的访问权限。
编辑权限	可执行以下操作： • 添加和删除 Kaspersky Security 服务用户。 • 编辑 Kaspersky Security 服务的用户访问权限。
删除服务	可在 Microsoft Windows 服务控制管理器中取消注册 Kaspersky Security 服务。
用户定义的服务请求	可创建和发送对 Kaspersky Security 服务的用户请求。

通过管理插件管理访问权限

在本节中，学习如何导航管理插件界面，以及如何为网络中的一台或所有受保护设备配置访问权限。

配置 Kaspersky Embedded Systems Security 和 Kaspersky Security 服务的访问权限

您可以编辑有权访问 Kaspersky Embedded Systems Security 功能和管理 Kaspersky Security 服务的用户和用户组列表。还可以编辑这些用户和用户组的访问权限。

要从列表中添加或删除用户或组：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：

- 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
- 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

  如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**补充**”部分，执行以下步骤之一：
   - 如果您希望编辑具有用于管理 Kaspersky Embedded Systems Security 功能的访问权限的用户列表，请单击“**应用程序管理的用户访问权限**”子部分中的“**设置**”。
   - 如果您希望编辑具有用于管理 Kaspersky Security 服务的访问权限的用户列表，请单击“**Kaspersky Security 服务管理的用户访问权限**”子部分中的“**设置**”。

     将打开“**Kaspersky Embedded Systems Security 3.2 的权限**”组窗口。
5. 在打开的窗口中，执行以下操作：
   - 要向列表中添加用户或组，请单击“**添加**”按钮，然后选择要授予权限的用户或组。
   - 要从列表中删除用户或组，请选择要限制其访问权限的用户或组，然后单击“**删除**”按钮。
6. 单击“**应用**”按钮。

将添加或删除所选用户（组）。

要编辑用户或组对管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服务的权限：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**补充**”部分，执行以下步骤之一：
   - 如果您希望编辑具有用于管理 Kaspersky Embedded Systems Security 功能的访问权限的用户列表，请单击“**应用程序管理的用户访问权限**”子部分中的“**设置**”。
   - 如果您希望编辑具有用于通过 Kaspersky Security 服务管理应用程序的访问权限的用户列表，请单击“**Kaspersky Security 服务管理的用户访问权限**”子部分中的“**设置**”。

     将打开“**Kaspersky Embedded Systems Security 的权限**”组窗口。
5. 在打开的窗口的“**组或用户名**”列表中，选择要更改其权限的用户或用户组。

6. 在“**<用户（组）> 的权限**”部分中，选中与以下访问权限级别对应的“**允许**”或“**拒绝**”复选框：

   - **完全控制**：可管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服务的全套权限。
   - **读取**：
     - 用于管理 Kaspersky Embedded Systems Security 的以下权限：**检索统计**、**读取设置**、**读取日志**和**读取权限**。
     - 用于管理 Kaspersky Security 服务的以下权限：**读取服务设置**、**从服务控制管理器请求状态**、**从服务请求状态**、**读取依存服务列表**、**读取权限**。
   - **修改**：
     - 除**编辑权限**之外的所有 Kaspersky Embedded Systems Security 管理权限。
     - 用于管理 Kaspersky Security 服务的以下权限：**修改服务设置**、**读取权限**。
   - **特殊权限**：用于管理 Kaspersky Security 服务的以下权限：**正在启动服务**、**停止服务**、**暂停/恢复服务**、**读取权限**、**用户定义的服务请求**。

7. 要配置某个用户或组的高级权限（**特殊权限**），请单击“**高级**”按钮。

   a. 在打开的“**Kaspersky Embedded Systems Security 高级安全性设置**”窗口中，选择所需的用户或组。

   b. 单击“**编辑**”按钮。

   c. 在窗口顶部的下拉列表中，选择访问控制类型（“**允许**”或“**阻止**”）。

   d. 选中与要为所选用户或组允许或阻止的功能旁边的复选框。

   e. 单击“**确定**”。

   f. 在“**Kaspersky Embedded Systems Security 高级安全性设置**”窗口中，单击“**确定**”。

8. 在“**Kaspersky Embedded Systems Security 的权限**”组窗口中，单击“**应用**”按钮。

已配置的用于管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服务的权限将被保存。

对 Kaspersky Embedded Systems Security 功能进行受密码保护的访问

您可通过配置用户权限来限制对应用程序管理和已注册服务的访问。您也可在 Kaspersky Embedded Systems Security 设置中设置密码保护，以提供关键操作的额外保护。

当您尝试访问以下应用程序功能时，Kaspersky Embedded Systems Security 会请求密码：

- 连接到应用程序控制台；
- 卸载 Kaspersky Embedded Systems Security；
- 修改 Kaspersky Embedded Systems Security 组件；
- 执行命令行命令。

Kaspersky Embedded Systems Security 界面会在屏幕上隐藏指定密码。输入密码后，Kaspersky Embedded Systems Security 将密码存储为计算得出的校验和。

多次尝试失败后，Kaspersky Embedded Systems Security 不会检查密码强度，也不会阻止密码输入。

创建密码时，建议满足以下条件：

- 密码不包含账户名或计算机名。
- 密码长度至少为 8 个字符。
- 密码包含的字符与以下至少三个类别匹配：
  - 大写拉丁字母 (A-Z)；
  - 小写拉丁字母 (a-z)；
  - 数字 (0-9)；
  - 感叹号 (!)、美元符号 ($)、英镑符号 (#) 和百分号 (%)。

您可导出和导入受密码保护的应用程序配置。通过导出受保护应用程序配置而创建的配置文件包含密码校验和以及用于填充密码字符串的修饰符值。

请勿更改配置文件中的校验和或修饰符。导入已手动更改的密码保护配置可能会导致访问应用程序完全被阻止。

要保护对 Kaspersky Embedded Systems Security 功能的访问权限：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。选择包含要配置其应用程序设置的受保护设备的管理组。
2. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要配置一组受保护设备的策略设置，请选择“**策略**”选项卡，然后通过上下文菜单打开“**<策略名称>**”的属性。
   - 如果要为单个受保护设备配置应用程序设置，请在 Kaspersky Security Center 的“应用程序设置”窗口中打开所需设置。
3. 在“**应用程序设置**”选项卡的“**安全性和可靠性**”部分中，单击“**设置**”按钮。
   将打开“**安全设置**”窗口。
4. 在“**密码保护设置**”部分中，选中“**应用密码保护**”复选框。
   “**密码**”和“**确认密码**”字段变为活动状态。
5. 在“**密码**”字段中，输入想要用于保护对 Kaspersky Embedded Systems Security 功能进行访问的密码。
6. 在“**确认密码**”字段中，再次输入您的密码。
7. 单击“**确定**”。

将保存指定设置。Kaspersky Embedded Systems Security 将请求指定密码以访问受保护的功能。

此密码无法恢复。丢失密码会导致完全失去对应用程序的控制。此外，还将无法从受保护设备卸载应用程序。

您可以随时重置密码。为此，请清除“**应用密码保护**”复选框并保存更改。密码保护将被禁用，旧密码校验和将被删除。使用新密码重复密码创建过程。

通过应用程序控制台管理访问权限

在本节中，学习如何导航应用程序控制台界面以及如何配置受保护设备的访问权限。

配置用于管理 Kaspersky Embedded Systems Security 和 Kaspersky Security 服务的访问权限

您可以编辑有权访问 Kaspersky Embedded Systems Security 功能和管理 Kaspersky Security 服务的用户和用户组列表。还可以编辑这些用户和用户组的访问权限。

要从列表中添加或删除用户或组：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**补充**”部分，执行以下步骤之一：
   - 如果您希望编辑具有用于管理 Kaspersky Embedded Systems Security 功能的访问权限的用户列表，请单击“**应用程序管理的用户访问权限**”子部分中的“**设置**”。
   - 如果您希望编辑具有用于管理 Kaspersky Security 服务的访问权限的用户列表，请单击“**Kaspersky Security 服务管理的用户访问权限**”子部分中的“**设置**”。

     将打开“**Kaspersky Embedded Systems Security 3.2 的权限**”组窗口。
5. 在打开的窗口中，执行以下操作：
   - 要向列表中添加用户或组，请单击“**添加**”按钮，然后选择要授予权限的用户或组。
   - 要从列表中删除用户或组，请选择要限制其访问权限的用户或组，然后单击“**删除**”按钮。
6. 单击“**应用**”按钮。

将添加或删除所选用户（组）。

要编辑用户或组对 Kaspersky Embedded Systems Security 或 Kaspersky Security 服务的管理权限：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**补充**”部分，执行以下步骤之一：
   - 如果您希望编辑具有用于管理 Kaspersky Embedded Systems Security 功能的访问权限的用户列表，请单击“**应用程序管理的用户访问权限**”子部分中的“**设置**”。
   - 如果您希望编辑具有用于通过 Kaspersky Security 服务管理应用程序的访问权限的用户列表，请单击“**Kaspersky Security 服务管理的用户访问权限**”子部分中的“**设置**”。

     将打开“**Kaspersky Embedded Systems Security 的权限**”组窗口。
5. 在打开的窗口的“**组或用户名**”列表中，选择要更改其权限的用户或用户组。
6. 在“**<用户（组）> 的权限**”部分中，选中与以下访问权限级别对应的“**允许**”或“**拒绝**”复选框：
   - **完全控制**：可管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服务的全套权限。
   - **读取**：
     - 用于管理 Kaspersky Embedded Systems Security 的以下权限：**检索统计**、**读取设置**、**读取日志**和**读取权限**。
     - 用于管理 Kaspersky Security 服务的以下权限：**读取服务设置**、**从服务控制管理器请求状态**、**从服务请求状态**、**读取依存服务列表**、**读取权限**。
   - **修改**：
     - 除**编辑权限**之外的所有 Kaspersky Embedded Systems Security 管理权限。
     - 用于管理 Kaspersky Security 服务的以下权限：**修改服务设置**、**读取权限**。
   - **特殊权限**：用于管理 Kaspersky Security 服务的以下权限：**正在启动服务**、**停止服务**、**暂停/恢复服务**、**读取权限**、**用户定义的服务请求**。
7. 要配置某个用户或组的高级权限（**特殊权限**），请单击“**高级**”按钮。
   a. 在打开的“**Kaspersky Embedded Systems Security 高级安全性设置**”窗口中，选择所需的用户或组。
   b. 单击“**编辑**”按钮。

c. 在窗口顶部的下拉列表中，选择访问控制类型（“允许”或“阻止”）。

d. 选中与要为所选用户或组允许或阻止的功能旁边的复选框。

e. 单击“确定”。

f. 在“Kaspersky Embedded Systems Security 高级安全性设置”窗口中，单击“确定”。

8. 在“Kaspersky Embedded Systems Security 的权限”组窗口中，单击“应用”按钮。

9. 已配置的用于管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服务的权限将被保存。

对 Kaspersky Embedded Systems Security 功能进行受密码保护的访问

您可通过配置用户权限来限制对应用程序管理和已注册服务的访问。您也可在 Kaspersky Embedded Systems Security 设置中设置密码保护，以提供关键操作的额外保护。

当您尝试访问以下应用程序功能时，Kaspersky Embedded Systems Security 会请求密码：

- 连接到应用程序控制台；
- 卸载 Kaspersky Embedded Systems Security；
- 修改 Kaspersky Embedded Systems Security 组件；
- 执行命令行命令。

Kaspersky Embedded Systems Security 界面会在屏幕上隐藏指定密码。输入密码后，Kaspersky Embedded Systems Security 将密码存储为计算得出的校验和。

多次尝试失败后，Kaspersky Embedded Systems Security 不会检查密码强度，也不会阻止密码输入。

创建密码时，建议满足以下条件：

- 密码不包含账户名或计算机名。
- 密码长度至少为 8 个字符。
- 密码包含的字符与以下至少三个类别匹配：
  - 大写拉丁字母 (A-Z)；
  - 小写拉丁字母 (a-z)；
  - 数字 (0-9)；
  - 感叹号 (!)、美元符号 ($)、英镑符号 (#) 和百分号 (%)。

您可导出和导入受密码保护的应用程序配置。通过导出受保护应用程序配置而创建的配置文件包含密码校验和以及用于填充密码字符串的修饰符值。

请勿更改配置文件中的校验和或修饰符。导入已手动更改的密码保护配置可能会导致访问应用程序完全被阻止。

要保护对 Kaspersky Embedded Systems Security 功能的访问权限：

1. 在应用程序控制台树中，选择“**Kaspersky Embedded Systems Security**”节点并执行以下操作之一：
   - 在节点的结果窗格中，单击“**应用程序属性**”链接。
   - 在节点的上下文菜单中选择“**属性**”。

   将打开“**应用程序设置**”窗口。
2. 在“**安全性和可靠性**”选项卡上的“**密码保护设置**”部分中，选中“**应用密码保护**”复选框。
   “**密码**”和“**确认密码**”字段变为活动状态。
3. 在“**密码**”字段中，输入想要用于保护对 Kaspersky Embedded Systems Security 功能进行访问的密码。
4. 在“**确认密码**”字段中，再次输入密码。
5. 单击“**确定**”。

此密码无法恢复。丢失密码会导致完全失去对应用程序的控制。此外，还将无法从受保护设备卸载应用程序。

您可以随时重置密码。为此，请清除“**应用密码保护**”复选框并保存更改。密码保护将被禁用，旧密码校验和将被删除。使用新密码重复密码创建过程。

通过 Web 插件管理访问权限

在本节中，学习如何导航 Web 插件界面，以及如何为网络中的一台或所有受保护设备配置访问权限。

配置 Kaspersky Embedded Systems Security 和 Kaspersky Security 服务的访问权限

要配置用户或组的访问权限，您需要使用安全描述符定义语言 (SDDL) 指定安全描述符字符串。有关安全描述符字符串的详细信息，请访问 Microsoft 网站。

要配置用户或组的访问权限：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**补充**”部分。

5. 执行以下步骤之一：

   - 如果您希望编辑具有用于管理 Kaspersky Embedded Systems Security 功能的访问权限的用户列表，请单击“**应用程序管理的用户访问权限**”子部分中的“**设置**”。
   - 如果您希望编辑具有用于管理 Kaspersky Security 服务的访问权限的用户列表，请单击“**Kaspersky Security 服务管理的用户访问权限**”子部分中的“**设置**”。

6. 通过在“**应用程序管理的用户访问权限**”或“**Kaspersky Security 服务管理的用户访问权限**”窗口中指定安全描述符字符串来添加用户或组。

7. 单击“**确定**”。

对 Kaspersky Embedded Systems Security 功能进行受密码保护的访问

您可通过配置用户权限来限制对应用程序管理和已注册服务的访问。您也可在 Kaspersky Embedded Systems Security 设置中设置密码保护，以提供关键操作的额外保护。

当您尝试访问以下应用程序功能时，Kaspersky Embedded Systems Security 会请求密码：

- 连接到应用程序控制台；
- 卸载 Kaspersky Embedded Systems Security；
- 修改 Kaspersky Embedded Systems Security 组件；
- 执行命令行命令。

Kaspersky Embedded Systems Security 界面会在屏幕上隐藏指定密码。输入密码后，Kaspersky Embedded Systems Security 将密码存储为计算得出的校验和。

多次尝试失败后，Kaspersky Embedded Systems Security 不会检查密码强度，也不会阻止密码输入。

创建密码时，建议满足以下条件：

- 密码不包含账户名或计算机名。
- 密码长度至少为 8 个字符。
- 密码包含的字符与以下至少三个类别匹配：
  - 大写拉丁字母 (A-Z)；
  - 小写拉丁字母 (a-z)；
  - 数字 (0-9)；
  - 感叹号 (!)、美元符号 ($)、英镑符号 (#) 和百分号 (%)。

您可导出和导入受密码保护的应用程序配置。通过导出受保护应用程序配置而创建的配置文件包含密码校验和以及用于填充密码字符串的修饰符值。

请勿更改配置文件中的校验和或修饰符。导入已手动更改的密码保护配置可能会导致访问应用程序完全被阻止。

要保护对 Kaspersky Embedded Systems Security 功能的访问权限：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**应用程序设置**”部分。
5. 在“**安全性和可靠性**”部分中，单击“**设置**”按钮。
6. 在“**密码保护设置**”部分中，选中“**应用密码保护**”复选框。
7. 在“**密码**”字段中，输入想要用于保护对 Kaspersky Embedded Systems Security 功能进行访问的密码。
8. 单击“**确定**”。

将保存指定设置。Kaspersky Embedded Systems Security 将请求指定密码以访问受保护的功能。

此密码无法恢复。丢失密码会导致完全失去对应用程序的控制。此外，还将无法从受保护设备卸载应用程序。

您可以随时重置密码。为此，请清除“**应用密码保护**”复选框并保存更改。密码保护将被禁用，旧密码校验和将被删除。使用新密码重复密码创建过程。

实时文件保护

本节包含有关实时文件保护任务以及如何配置的信息。

关于“实时文件保护”任务

“实时文件保护”任务运行期间，在访问以下受保护设备对象时，Kaspersky Embedded Systems Security 会对这些对象进行扫描：

- 文件。
- NTFS 交换数据流。
- 本地硬盘驱动器和外部设备上的主引导记录和引导扇区。

当任何应用程序将文件写入受保护设备或从受保护设备上读取文件时，Kaspersky Embedded Systems Security 会拦截此文件进行扫描以检测其是否存在威胁；如果检测到威胁，则执行默认操作或您指定的操作：尝试清除文件、移至隔离区或将其删除。在清除或删除前，Kaspersky Embedded Systems Security 会将源文件的加密副本保存到备份文件夹。

Kaspersky Embedded Systems Security 还会检测在 Windows Subsystem for Linux® 下运行的进程是否存在恶意软件。对于此类进程，“实时文件保护”任务将应用当前配置定义的操作。

关于任务保护范围和安全设置

默认情况下，实时文件保护任务将保护设备文件系统中的所有对象。如果不需要对文件系统中的所有对象进行安全保护，或者您想从任务范围中排除任何对象，则可以限制保护范围。

在应用程序控制台中，保护范围以 Kaspersky Embedded Systems Security 可以监控的设备文件资源树或列表的形式显示。默认情况下，设备的网络文件资源以列表形式显示。

在管理插件中，只有列表视图可用。

要在应用程序控制台中以树形式显示网络文件资源，

请打开“**保护范围设置**”窗口左上角部分中的下拉列表，然后选择“**树视图**”。

无论受保护设备的文件资源以列表还是树的形式显示，节点图标的含义均如下：

☑节点包含在保护范围内。

☐节点排除在保护范围之外。

☑该节点至少有一个子节点排除在扫描范围之外，或子节点的安全性设置与父节点的安全性设置不同（仅限树视图）。

如果选择了所有子节点，但未选择父节点，则显示 ☑ 图标。在这种情况下，在为所选子节点创建了保护范围后，如果父节点所包含的文件和文件夹发生更改，将自动忽略这些更改。

使用应用程序控制台，您还可以添加虚拟驱动器到保护范围中。虚拟节点的名称以蓝色显示。

安全性设置

任务安全设置可以配置为保护范围中包括的所有节点或项的通用设置，或配置为设备文件资源树或列表中各个节点或项的不同设置。

为所选父节点配置的安全设置将自动应用到其所有子节点。父节点的安全设置不会应用到单独配置的子节点。

可以使用以下方法之一配置选定保护范围的设置：

- 选择三个预定义安全级别中的一个。
- 手动为文件资源树或列表中的选定节点或项配置安全性设置（安全级别更改为"自定义"）。

可以将节点或项的一组设置保存为模板，以便以后应用至其他节点或项。

关于虚拟保护范围

Kaspersky Embedded Systems Security 不仅可以扫描硬盘驱动器和可移动驱动器上的现有文件夹和文件，还可以扫描由各种应用程序和服务在受保护设备上动态创建的驱动器。

如果所有设备对象均包含在保护范围内，则这些动态节点将自动包含在保护范围内。但是，如果您要为这些动态节点的安全性设置指定特殊值，或者只选择了设备的一部分进行保护，则为了将虚拟驱动器、文件或文件夹包含在保护范围内，您必须首先在应用程序控制台中创建它们：即指定虚拟保护范围。创建的驱动器、文件和文件夹将仅存在于应用程序控制台中，而不在受保护设备的文件结构中。

如果在创建保护范围时选择了所有子文件夹或文件，但未选择父文件夹，则父文件夹中将显示的所有虚拟文件夹或文件都不会自动包含在受保护范围内。应在应用程序控制台中创建这些文件夹或文件的"虚拟副本"并添加到保护范围内。

预定义的保护范围

文件资源树或列表显示基于配置的 Microsoft Windows 安全设置所拥有读取访问权限的节点。

Kaspersky Embedded Systems Security 覆盖以下预定义保护范围：

- **本地硬盘驱动器**。Kaspersky Embedded Systems Security 将保护设备硬盘驱动器上的文件。
- **可移动驱动器**。Kaspersky Embedded Systems Security 将保护外部设备上的文件，如 CD 或可移动驱动器。您可以在保护范围中包含或排除所有可移动驱动器、单个磁盘、文件夹或文件。
- **网络**。Kaspersky Embedded Systems Security 将保护设备上运行的应用程序写入到网络文件夹或从网络文件夹读取的文件。当其他受保护设备上的应用程序访问此类文件时，Kaspersky Embedded Systems Security 不会保护此类文件。
- **虚拟驱动器**。虚拟文件夹、文件和临时连接到设备的驱动器可包含在保护范围内，例如，常规群集驱动器。

默认情况下，您可以在范围列表中查看和配置预定义保护范围；还可以在列表形成期间在保护范围设置中向该列表添加预定义范围。

默认情况下，保护范围包括除虚拟驱动器外的所有预定义区域。

使用 SUBST 命令创建的虚拟驱动器不会显示在应用程序控制台的受保护设备文件资源树中。要将虚拟驱动器中的对象包含在保护范围内，请将与该虚拟驱动器关联的设备文件夹包含在保护范围内。

已连接的网络驱动器也不会显示在受保护设备文件资源列表中。若要将网络驱动器中的对象包含在保护范围内，请按 UNC 格式指定与该网络驱动器对应的文件夹的路径。

关于预定义安全级别

可以为受保护设备文件资源树或文件资源列表中的选定节点应用以下预定义安全级别之一：“**最优性能**”、“**推荐**”和“**最佳保护**”。每个级别都包含其自有的预定义安全设置集合（请参见下表）。

最优性能

如果您的网络除了在受保护设备上使用 Kaspersky Embedded Systems Security 外，还有其他受保护设备安全措施，例如防火墙和现有安全策略，则建议使用“**最优性能**”安全级别。

推荐

“**推荐**”安全级别确保保护与对设备的性能影响的最佳组合。Kaspersky 专家推荐此级别，因为其足以保护大多数公司网络上的设备。默认情况下，将设置“**推荐**”安全级别。

最佳保护

如果组织的网络有更高的设备安全要求，则推荐使用“**最佳保护**”安全级别。

预设安全级别和对应的设置值

选项	安全级别		
	最优性能	推荐	最佳保护
对象保护	按扩展名	按格式	按格式
仅保护新文件和已修改的文件	已启用	已启用	已禁用
对受感染对象和其他对象执行的操作	阻止访问并清除。清除失败则删除	仅通知	阻止访问并清除。清除失败则删除
对疑似感染对象执行的操作	阻止访问并隔离	仅通知	阻止访问并隔离
排除文件	否	否	否
不检测	否	否	否
超过以下时间则停止扫描(秒)	60 秒	60 秒	60 秒

不扫描大于该值的复合对象(MB)	8 MB	8 MB	未设置
扫描 NTFS 交换数据流	是	是	是
扫描磁盘引导扇区和 MBR	是	是	是
复合对象保护	• 打包的对象* *仅新对象和已修改的对象	• SFX 压缩文件* • 打包的对象* • 嵌入的 OLE 对象* *仅新对象和已修改的对象	• SFX 压缩文件* • 打包的对象* • 嵌入的 OLE 对象* *所有对象
在检测到嵌入对象时完全删除应用程序无法修改的复合文件	否	否	是

预定义安全级别的设置中不包括“对象保护”、“使用 iChecker 技术”、“使用 iSwift 技术”和“使用启发式分析”设置。如果在选择了其中一个预定义的安全级别之后编辑“对象保护”、“使用 iChecker 技术”、“使用 iSwift 技术”或“使用启发式分析”安全设置，选择的安全级别将不会发生更改。

“实时文件保护”任务中默认扫描的文件扩展名

默认情况下，Kaspersky Embedded Systems Security 将扫描具有以下扩展名的文件：

- *386*；
- *acm*；
- *ade*、*adp*；
- *asp*；
- *asx*；
- *ax*；
- *bas*；
- *bat*；
- *bin*；
- *chm*；
- *cla*、*clas**；
- *cmd*；
- *com*；

- *cpl；*
- *crt；*
- *dll；*
- *dpl；*
- *drv；*
- *dvb；*
- *dwg；*
- *efi；*
- *emf；*
- *eml；*
- *exe；*
- *fon；*
- *fpm；*
- *hlp；*
- *hta；*
- *htm、html*；*
- *htt；*
- *ico；*
- *inf；*
- *ini；*
- *ins；*
- *isp；*
- *jpg、jpe；*
- *js、jse；*
- *lnk；*
- *mbx；*
- *msc；*
- *msg；*

- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*

- *swf；*
- *sys；*
- *the；*
- *them*；*
- *tsp；*
- *url；*
- *vb；*
- *vbe；*
- *vbs；*
- *vxd；*
- *wma；*
- *wmf；*
- *wmv；*
- *wsc；*
- *wsf；*
- *wsh；*
- *do?；*
- *md?；*
- *mp?；*
- *ov?；*
- *pp?；*
- *vs?；*
- *xl?。*

“实时文件保护”任务默认设置

默认情况下，“实时文件保护”任务将使用下表描述的设置。您可以更改这些设置的值。

“实时文件保护”任务默认设置

设置	默认值	描述

保护范围	整个受保护设备，虚拟驱动器除外。	使用此选项更改保护范围。
安全性设置	整个保护范围的常规设置；对应“**推荐**”安全级别。	您可以对受保护设备文件资源列表或树中选定的节点执行以下操作： • 选择不同的预定义安全级别 • 手动更改安全性设置 您可以将选定节点的一组安全性设置保存为模板，以便在以后将其应用至其他节点。
对象保护模式	**智能模式**	使用此选项可以选择保护模式，即定义 Kaspersky Embedded Systems Security 扫描对象所采用的访问尝试类型。
启发式分析	应用“**中度**”安全级别。	可以启用或禁用“启发式分析”并配置分析级别。
应用信任区域	已应用。	可以在选定任务中使用的常规排除列表。
在保护中使用 KSN	已应用。	使用此选项可以使用卡巴斯基安全网络云服务提高您的设备保护能力（如果接受 KSN 声明则可用）。
任务启动计划	程序启动时。	使用此选项可以配置计划任务启动。
阻止显示恶意活动的网络会话对网络共享资源的访问	未应用。	使用此选项可以阻止当前会话并添加在被阻止主机存储部分中检测到恶意活动的主机 IP 或主机 LUID。
检测到活动感染时启动关键区域扫描	已应用。	在检测到活动感染时，Kaspersky Embedded Systems Security 将创建并启动临时的“关键区域扫描”任务。

通过管理插件管理“实时文件保护”任务

在本节中，学习如何导航管理插件界面，以及如何为网络中的一台或所有受保护设备配置任务设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开“实时文件保护”任务的策略设置

要通过 Kaspersky Security Center 策略打开“实时文件保护”任务设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。

5. 在打开的“**属性：<策略名称>**”窗口中，选择“**实时计算机保护**”部分。

6. 单击“**实时文件保护**”子部分中的“**设置**”按钮。
   将打开“**实时文件保护**”窗口。

如果某个受保护设备受 Kaspersky Security Center 活动策略管理，且该策略禁止更改应用程序设置，则无法通过应用程序控制台编辑这些设置。

打开“实时文件保护”任务属性

要打开单台网络设备的“实时文件保护”任务设置窗口：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择要为其配置任务的管理组。

3. 选择“**设备**”选项卡。

4. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：

   - 双击受保护设备的名称。

   - 在受保护设备的上下文菜单中选择“**属性**”项。

   将打开“**属性：<受保护设备名称>**”窗口。

5. 在“**任务**”部分中，选择“**实时文件保护**”任务。

6. 单击“**属性**”按钮。
   将打开“**属性：实时文件保护**”窗口。

配置“实时文件保护”任务

要配置“实时文件保护”任务设置：

1. 打开“实时文件保护”窗口。

2. 配置以下任务设置：

   - 在“**常规**”选项卡上：

     - 拦截参数

     - 启发式分析

     - 与其他组件集成

   - 在“**任务管理**”选项卡上：

- 计划任务启动设置。

3. 选择“保护范围”选项卡，然后执行以下操作：

- 单击“添加”或“编辑”按钮编辑保护范围。
  - 在打开的窗口中，选择要包含到任务保护范围的内容：
    - 预定义范围
    - 磁盘、文件夹或网络位置
    - 文件
  - 选择一项预定义安全级别或手动配置保护设置。

4. 在“实时文件保护”窗口中单击“确定”。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。设置修改日期和时间以及修改前后任务设置值保存在系统审核日志中。

选择保护模式

在“实时文件保护”任务中，可以选择保护模式。在“对象保护模式”部分中，您可以指定 Kaspersky Embedded Systems Security 扫描对象时的访问尝试类型。

“对象保护模式”设置的值应用于任务中指定的整个保护范围。无法为保护范围内的单个节点指定不同的设置值。

要选择保护模式：

1. 打开“实时文件保护”窗口。
2. 在打开的窗口中，打开“常规”选项卡，然后选择要设置的保护模式：
   - 智能模式
   - 访问和修改时
   - 访问时
   - 运行时
   - 对启动进程的更深度分析(分析结束之前将阻止进程启动)
3. 单击“确定”。

选中保护模式将生效。

配置启发式分析以及与其他应用程序组件的集成

要启动“KSN 使用”任务，您必须接受卡巴斯基安全网络声明。

要配置启发式分析以及与其他组件的集成：

1. 打开“实时文件保护”窗口。
2. 在“**常规**”选项卡上，清除或选中“使用启发式分析”复选框。
3. 如有必要，使用滑块调整分析级别。
4. 在“**与其他组件集成**”部分中，配置以下设置：
   - 选中或清除“应用信任区域”复选框。
   - 选中或清除“在保护中使用 KSN”复选框。

     在“KSN 使用”任务设置中必须选中“**发送关于已扫描文件的数据**”复选框。

   - 选中或清除“**阻止显示恶意活动的网络会话对网络共享资源的访问**”复选框。
   - 选中或清除“检测到活动感染时启动关键区域扫描”复选框。
5. 单击“**确定**”。

配置的任务设置将立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

计划任务

您可以在应用程序控制台中计划本地系统和自定义任务。您无法在应用程序控制台中计划组任务。

要使用管理插件计划组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择受保护设备所属的组。
3. 在结果窗格中，选择“**任务**”选项卡。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 双击任务的名称。
   - 打开任务名称的上下文菜单，然后选择“属性”项。
5. 选择“**计划**”部分。
6. 在“**计划设置**”设置块中，选中“**按计划运行**”复选框。

如果 Kaspersky Security Center 策略阻止按需扫描任务和更新任务的计划，则这些任务的计划设置字段将不可用。

7. 根据需要配置计划设置。为此，请执行以下操作：

a. 在“**频率**”列表中，选择以下值之一：

- **每小时**，如果您希望该任务在指定的小时数内间隔运行，请在“**每 <数量> 小时**”字段中指定小时数。
- **每天**，如果您希望该任务在指定的天数内间隔运行，请在“**每 <数量> 天**”字段中指定天数。
- **每周**，如果您希望该任务以指定周数为间隔运行，请在“**每 <数量> 周**”字段中指定周数。指定要启动任务的星期中的日期（默认在星期一启动任务）。
- **应用程序启动时**，如果您希望在每次启动 Kaspersky Embedded Systems Security 时运行该任务。
- **应用程序数据库更新后**，如果您希望在每次更新应用程序数据库后运行该任务。

b. 在“**开始时间**”字段中指定首次启动任务的时间。

c. 在“**开始日期**”字段中，指定计划启动的日期。

在计划了任务的开始时间、日期和频率之后，将显示下一次启动的预估时间。

转到“**计划**”选项卡，然后打开“**任务设置**”窗口。在窗口上部的**下次开始**字段中，显示了预计启动时间。每次打开窗口时，此估计启动时间都会更新并显示。

如果 Kaspersky Security Center 策略设置禁止启动计划的本地系统任务，则“**下次开始**”字段将显示“**被策略阻止**”值。

8. 根据需要使用“**高级**”选项卡来配置以下计划设置。

- 在“**任务停止设置**”部分中：
  a. 选中“**持续时间**”复选框，并在右侧的字段中输入任务执行的最长持续时间（小时和分钟）。
  b. 选中“**暂停开始于**”复选框，并在右侧的字段中输入暂停任务执行的时间间隔（小于 24 小时）的开始值和结束值。
- 在“**高级设置**”部分中：
  a. 选中“**取消计划开始于**”复选框，并指定停止应用计划的日期。
  b. 选中“**运行错过的任务**”复选框以允许启动跳过的任务。
  c. 选中“**在该时间间隔内随机化任务开始时间**”复选框，并按分钟指定该值。

9. 单击“**确定**”。

10. 单击“**应用**”按钮保存任务启动设置。

如果要使用 Kaspersky Security Center 配置单个任务的应用程序设置，请参见“在 Kaspersky Security Center 的应用程序设置窗口中配置本地任务”部分。

创建和配置任务保护范围

要通过 Kaspersky Security Center 创建和配置任务保护范围：

1. 打开“实时文件保护”窗口。
2. 选择“**保护范围**”选项卡。
   已经受任务保护的所有项目都列在“**保护范围**”表中。
3. 单击“**添加**”按钮向列表中添加新项目。
   将打开“**将对象添加至保护范围**”窗口。
4. 选择对象类型以将其添加到保护范围中：
   - **预定义范围**，将一个预定义范围包含在设备的保护范围中。然后在下拉列表中，选择所需的保护范围。
   - **磁盘、文件夹或网络位置**，将单个驱动器、文件夹或网络对象包括在保护范围中。然后通过单击“**浏览**”按钮选择所需的保护范围。
   - **文件**，将单个文件包括在保护范围中。然后通过单击“**浏览**”按钮选择所需的保护范围。

     如果某个对象已经作为保护范围的排除添加，则不能再将其添加到保护范围中。
5. 要从保护范围中排除单个项目，请清除这些项目名称旁边的复选框，或者执行以下步骤：
   a. 右键单击保护范围打开其上下文菜单。
   b. 在上下文菜单中，选择“**添加排除**”选项。
   c. 在“**添加排除**”窗口中选择对象类型，将按照将对象添加到保护范围中时使用的步骤，将该对象类型作为保护范围的排除添加。
6. 要修改保护范围或现有排除，请选择所需保护范围上下文菜单中的“**编辑范围**”选项。
7. 若要在网络文件资源列表中隐藏之前添加的保护范围或排除，请在所需保护范围的上下文菜单中选择“**删除范围**”选项。

   将保护范围从网络文件资源列表中删除时，该保护范围也从“实时文件保护”任务范围中删除。
8. 单击“**确定**”。

“保护范围设置”窗口关闭。将保存新配置的设置。

只有保护范围中至少包含一个设备文件资源节点时，才可启动“**实时文件保护**”任务。

为按需扫描任务选择预定义的安全级别

可以为设备文件资源列表中的选定节点应用以下预定义安全级别之一：“**最优性能**”、“**推荐**”和“**最佳保护**”。

要选择其中一个预定义安全级别：

1. 打开“**属性：实时文件保护**”窗口。
2. 选择“**保护范围**”选项卡。
3. 在受保护设备列表中，选择一个包含在保护范围中的项目以设置预定义安全级别。
4. 单击“**配置**”按钮。
   将打开“**实时文件保护设置**”窗口。
5. 在“**安全级别**”选项卡上，选择要应用的安全级别。
   该窗口将显示与选定安全级别相对应的安全性设置列表。
6. 单击“**确定**”。
7. 单击“**属性：实时文件保护**”窗口中的“**确定**”。
   将保存已配置的任务设置，这些设置会立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

手动配置安全性设置

默认情况下，“实时文件保护”任务对整个保护范围使用通用安全设置。这些设置对应于“**推荐**”预定义安全级别。

可以通过将安全性设置配置为用于整个保护范围的常规设置，或配置为设备文件资源列表或树中节点的单个项目的不同设置，来修改安全性设置的默认值。

要手动配置选定节点的安全设置：

1. 打开“**实时文件保护**”窗口。
2. 在“**保护范围**”选项卡上，选择您要配置其安全设置的节点，然后单击“**配置**”。
   将打开“**实时文件保护设置**”窗口。
3. 在“**安全级别**”选项卡上，单击“**设置**”按钮以自定义配置。
4. 您可以根据要求配置选定节点的自定义安全性设置：
   - 常规设置
   - 操作
   - 性能
5. 在“**实时文件保护**”窗口中单击“**确定**”。

将保存新的保护范围设置。

配置常规任务设置

要配置“实时文件保护”任务的常规安全设置：

1. 打开“实时文件保护设置”窗口。
2. 选择“**常规**”选项卡。
3. 在“**对象保护**”部分中，指定要包含在保护范围内的对象类型：
   - 所有对象
   - 按格式扫描对象
   - 按反病毒数据库中指定的扩展名列表扫描对象
   - 按指定的扩展名列表扫描对象
   - 扫描磁盘引导扇区和 MBR
   - 扫描 NTFS 交换数据流
4. 在“**性能**”组框中，选中或清除“仅保护新文件和已修改的文件”复选框。

   如果清除该复选框，要在可用选项之间切换，请单击每个复合对象类型对应的“**全部/仅新建**”链接。

5. 在“**复合对象保护**”部分中，指定要包含在保护范围内的复合对象：
   - 全部/仅新的压缩文件
   - 全部/仅新的 SFX 压缩文件
   - 全部/仅新的电子邮件数据库
   - 全部/仅新的打包的对象
   - 全部/仅新的纯文本电子邮件
   - 全部/仅新的嵌入的 OLE 对象
6. 单击“**保存**”。

将保存新的任务配置。

配置操作

要配置在“实时文件保护”任务期间对受感染的对象和其他检测到的对象的操作：

1. 打开“实时文件保护设置”窗口。
2. 选择“操作”选项卡。
3. 选择要对受感染的对象和其他检测到的对象执行的操作：
   - 仅通知。
   - 阻止访问。
   - 执行附加操作。
     从下拉列表中选择操作：
     - 清除。
     - 清除；清除失败时则删除。
     - 删除。
     - 推荐。
4. 选择要对疑似感染的对象执行操作：
   - 仅通知。
   - 阻止访问。
   - 执行附加操作。
     从下拉列表中选择操作：
     - 隔离。
     - 删除。
     - 推荐。
5. 根据检测的对象类型配置要对对象执行的操作：
   a. 清除或选中“根据检测到的对象的类型执行操作”复选框。
   b. 单击“设置”按钮。
   c. 在打开的窗口中，选择针对每种检测到的对象类型的主要操作和次要操作（如果主要操作失败则执行）。
   d. 单击“确定”。
6. 选择要对不可修改的复合文件执行的操作：选中或清除“在检测到嵌入对象时完全删除应用程序无法修改的复合文件”复选框。
7. 单击“保存”。

将保存新的任务配置。

配置性能

要配置“实时文件保护”任务的性能设置：

1. 打开“实时文件保护设置”窗口。
2. 选择“**性能**”选项卡。
3. 在“**排除**”部分中：
   - 清除或选中“排除文件”复选框。
   - 清除或选中“不检测”复选框。
   - 针对每个设置单击“**编辑**”按钮以添加排除项。
4. 在“**高级设置**”部分中：
   - 超过以下时间则停止扫描(秒)
   - 不扫描大于该值的复合对象(MB)
   - 使用 iSwift 技术
   - 使用 iChecker 技术

通过应用程序控制台管理“实时文件保护”任务

在本节中，学习如何导航应用程序控制台界面以及如何在受保护设备上配置任务设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开“实时文件保护”任务设置

要打开常规任务设置窗口：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**实时文件保护**”子节点。
3. 在结果窗格中单击“**属性**”链接。
   将打开“**任务设置**”窗口。

打开“实时文件保护”任务范围设置

要打开“实时文件保护”任务的保护范围设置窗口：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**实时文件保护**”子节点。
3. 在结果窗格中单击“**配置保护范围**”链接。
   打开“**保护范围设置**”窗口。

配置“实时文件保护”任务

要配置“实时文件保护”任务设置：

1. 打开“**任务设置**”窗口。
2. 在“**常规**”选项卡上，配置以下任务设置：
   - 对象保护模式
   - 启发式分析
   - 与其他组件集成
3. 在“**计划**”和“**高级**”选项卡上，指定计划的启动设置。
4. 在“**任务设置**”窗口中单击“**确定**”。
   将保存修改的设置。
5. 在“**实时文件保护**”节点的结果窗格中，单击“**配置保护范围**”链接。
6. 执行以下操作：
   - 在设备文件资源树或列表中，选择要包含在任务保护范围内的节点或项目。
   - 选择一项预定义安全级别或手动配置对象保护设置。
7. 在“**保护范围设置**”窗口中，单击“**保存**”按钮。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。设置修改日期和时间以及修改前后的任务设置值保存在系统审核日志中。

选择保护模式

在“实时文件保护”任务中，可以选择保护模式。在“**对象保护模式**”部分中，您可以指定 Kaspersky Embedded Systems Security 扫描对象时的访问尝试类型。

“**对象保护模式**”设置的值应用于任务中指定的整个保护范围。无法为保护范围内的单个节点指定不同的设置值。

要选择保护模式：

1. 打开“任务设置”窗口。
2. 在打开的窗口中，打开“常规”选项卡，然后选择要设置的保护模式：
   - 智能模式
   - 访问和修改时
   - 访问时
   - 运行时
   - 对启动进程的更深度分析(分析结束之前将阻止进程启动)
3. 单击“确定”。

选中保护模式将生效。

配置启发式分析以及与其他应用程序组件的集成

要启动“KSN 使用”任务，您必须接受卡巴斯基安全网络声明。

要配置启发式分析以及与其他组件的集成：

1. 打开“任务设置”窗口。
2. 在“常规”选项卡上，清除或选中“使用启发式分析”复选框。
3. 如有必要，使用滑块调整分析级别。
4. 在“与其他组件集成”部分中，配置以下设置：
   - 选中或清除“应用信任区域”复选框。
     单击“受信任区域”链接打开“受信任区域”设置。
   - 选中或清除“在保护中使用 KSN”复选框。

     在“KSN 使用”任务设置中必须选中“发送关于已扫描文件的数据”复选框。
   - 选中或清除“阻止显示恶意活动的网络会话对网络共享资源的访问”复选框。
   - 选中或清除“检测到活动感染时启动关键区域扫描”复选框。
5. 单击“确定”。

将应用新配置的设置。

配置任务计划设置

在应用程序控制台中，您可以计划何时启动本地系统和自定义任务。但是，您无法计划何时启动组任务。

要计划任务：

1. 打开您要计划的任务的上下文菜单。
2. 选择“**属性**”。
   将打开“**任务设置**”窗口。
3. 在打开的窗口中的“**计划**”选项卡上，选中“**按计划运行**”复选框。
4. 按照以下步骤指定计划设置：
   a. 在“**频率**”下拉菜单中，选择以下之一：
      - **每小时**：每小时运行一次任务；在“**每<数字>小时**”字段中指定小时数。
      - **每天**：每天运行一次任务；在“**每<数字>天**”字段中指定天数。
      - **每周**：每周运行一次任务；在“**每<数字>周**”字段中指定周数。指定要启动任务的星期中的日期（默认在星期一启动任务）。
      - **应用程序启动时**：每次启动 Kaspersky Embedded Systems Security 时运行该任务。
      - **应用程序数据库更新后**：每次更新应用程序数据库后运行该任务。
   b. 在“**开始时间**”字段中，指定首次启动任务的时间。
   c. 在“**开始日期**”字段中，指定首次启动任务的日期。

   指定了任务启动频率之后，将在窗口顶部的“**下次开始**”字段中显示任务的首次启动时间、计划的开始应用日期以及预计的下一次任务启动时间的相关信息。每次打开“**任务设置**”窗口的“**计划**”选项卡时，将更新并显示下次任务开始的估计时间。

   如果 Kaspersky Security Center 活动策略设置禁止启动计划的本地系统任务，则“**下次开始**”字段将显示“**被策略阻止**”值。
5. 使用“**高级**”选项卡可以指定以下计划设置：
   - 在“**任务停止设置**”部分中：
     a. 选择“**持续时间**”复选框。在右侧的字段中，以小时和分钟为单位输入任务最大持续时间。
     b. 选择“**暂停开始于**”复选框。在右侧的字段中，输入何时暂停和恢复任务（24 小时之内）。
   - 在“**高级设置**”部分中：
     a. 选择“**取消计划开始于**”复选框，然后指定任务计划的结束日期。
     b. 选中“**运行错过的任务**”复选框以启动跳过的任务。
     c. 选中“**在该时间间隔内随机启动任务**”复选框，并按分钟指定该值。

6. 单击“**确定**”。

将保存任务计划设置。

创建保护范围

本节提供有关在实时文件保护任务中创建和管理保护范围的说明。

配置网络文件资源的视图

要在配置保护范围设置期间选择网络文件资源的视图：

1. 打开“保护范围设置”窗口。
2. 打开窗口左上角部分中的下拉列表，然后选择以下选项之一：
   - 选择“**树视图**”选项以树的形式显示网络文件资源。
   - 选择“**列表视图**”选项以列表形式显示网络文件资源。

   默认情况下，受保护设备的网络文件资源以列表形式显示。
3. 单击“**保存**”按钮。

创建保护范围

创建“实时文件保护”任务范围的过程取决于所选网络文件资源视图。您可以查看树或列表（设置为默认）形式的网络文件资源。

要对任务应用新的保护范围设置，必须重启“实时文件保护”任务。

要使用网络文件资源树创建保护范围：

1. 打开“保护范围设置”窗口。
2. 在窗口的左侧部分中，打开网络文件资源树以显示所有节点和子节点。
3. 执行以下操作：
   - 要从保护范围中排除单个节点，请清除这些节点名称旁边的复选框。
   - 要从保护范围中包含单个节点，请清除“**我的计算机**”复选框，然后执行以下步骤：
     - 如果要将某一类型的所有驱动器包含在保护范围内，请选中所需磁盘类型名称对应的框（例如，若要添加设备上的所有可移动驱动器，请选中“**可移动驱动器**”复选框）。

- 如果要将某种类型的单个磁盘包含在保护范围内，请展开包含该类型驱动器列表的节点，然后选中所需驱动器名称旁边的框。例如，若要选择可移动驱动器 F:，请展开“**可移动驱动器**”节点，然后选中驱动器 **F:** 对应的框。

- 如果您想要仅包含驱动器上的单个文件夹或文件，请选中该文件夹或文件名称旁边的复选框。

4. 单击“**保存**”按钮。

“**保护范围设置**”窗口关闭。将保存新配置的设置。

要使用网络文件资源列表创建保护范围：

1. 打开“保护范围设置”窗口。

2. 要从保护范围中包含单个节点，请清除“**我的计算机**”复选框，然后执行以下步骤：

   a. 右键单击保护范围打开其上下文菜单。

   b. 在按钮的上下文菜单中，选择“**添加保护范围**”。

   c. 在“**添加保护范围**”窗口中，选择一个对象类型以将其添加到保护范围中：

   - **预定义范围**，将一个预定义范围包含在设备的保护范围中。然后在下拉列表中，选择所需的保护范围。

   - **磁盘、文件夹或网络位置**，将单个驱动器、文件夹或网络对象包括在保护范围中。然后通过单击“**浏览**”按钮选择所需的范围。

   - **文件**，将单个文件包括在保护范围中。然后通过单击“**浏览**”按钮选择所需的范围。

   如果某个对象已经作为保护范围的排除添加，则不能再将其添加到保护范围中。

3. 要从保护范围中排除单个节点，请清除这些节点名称旁边的复选框，或者执行以下步骤：

   a. 右键单击保护范围打开其上下文菜单。

   b. 在上下文菜单中，选择“**添加排除**”选项。

   c. 在“**添加排除**”窗口中选择对象类型，将按照将对象添加到保护范围中时使用的步骤，将该对象类型作为保护范围的排除添加。

4. 要修改保护范围或现有排除，请选择所需保护范围上下文菜单中的“**编辑范围**”选项。

5. 若要在网络文件资源列表中隐藏之前添加的保护范围或排除，请在所需保护范围的上下文菜单中选择“**从列表删除**”选项。

   将保护范围从网络文件资源列表中删除时，该保护范围也从“实时文件保护”任务范围中删除。

6. 单击“**保存**”按钮。

“**保护范围设置**”窗口关闭。将保存新配置的设置。

只有保护范围中至少包含一个设备文件资源节点时，才可启动“实时文件保护”任务。

如果指定了复杂的保护范围，例如，为设备文件资源树中多个节点的设置指定了不同的安全值时，可能会导致在访问对象时，扫描对象的速度缓慢。

在保护范围内包含网络对象

您可以按照 UNC（通用命名惯例）格式指定网络驱动器、文件夹或文件的路径以将它们添加至保护范围。

您可以在系统账户下扫描网络文件夹。

要将网络位置添加到保护范围：

1. 打开“保护范围设置”窗口。
2. 打开左上角部分中的下拉列表，然后选择“**树视图**”。
3. 在“**网络**”节点的上下文菜单中：
   - 选择“**添加网络文件夹**”，如果您想要向保护范围中添加网络文件夹。
   - 选择“**添加网络文件**”，如果您想要向保护范围中添加网络文件。
4. 输入 UNC 格式的网络文件夹或文件路径。
5. 按 **ENTER** 键。
6. 选中新添加的网络对象旁边的复选框以将其包含在保护范围内。
7. 如有必要，更改已添加的网络对象的安全性设置。
8. 单击“**保存**”按钮。

将保存修改的任务设置。

创建虚拟保护范围

仅当保护/扫描范围以文件资源树的形式显示时，您才可通过添加单个虚拟驱动器、文件夹或文件来扩展保护/扫描范围。

要将虚拟驱动器添加到保护范围：

1. 打开“保护范围设置”窗口。
2. 打开窗口左上角的下拉列表部分，然后选择**树视图**。

3. 打开“**虚拟驱动器**”节点的上下文菜单。

4. 选择“**添加虚拟驱动器**”选项。

5. 在可用名称列表中，为所创建的虚拟驱动器选择名称。

6. 选中驱动器旁的复选框以将该驱动器包含在保护范围内。

7. 在“**保护范围设置**”窗口中，单击“**保存**”按钮。

将保存新配置的设置。

要将虚拟文件夹或虚拟文件添加到保护范围：

1. 打开“保护范围设置”窗口。

2. 打开左上角部分中的下拉列表，然后选择“**树视图**”。

3. 打开要添加文件夹或文件的虚拟驱动器的上下文菜单，然后选择以下选项之一：

   - **添加虚拟文件夹**，如果您想要向保护范围中添加虚拟文件夹。
   - **添加虚拟文件**，如果您想要向保护范围中添加虚拟文件。

4. 在输入字段中指定文件夹或文件的名称。

5. 在包含所创建文件夹或文件的名称的行中，选中相应的复选框以将该文件夹或文件包含在保护范围内。

6. 在“**保护范围设置**”窗口中，单击“**保存**”按钮。

将保存修改的任务设置。

手动配置安全性设置

默认情况下，实时计算机保护任务对整个保护范围使用通用安全设置。这些设置对应于“**推荐**”预定义安全级别。

可以通过将安全性设置配置为用于整个保护范围的常规设置，或配置为设备文件资源列表或树中节点的单个项目的不同设置，来修改安全性设置的默认值。

在使用受保护设备文件资源树时，为所选父节点配置的安全性设置将自动应用于所有子节点。父节点的安全设置不会应用到单独配置的子节点。

要手动配置安全设置：

1. 打开“保护范围设置”窗口。

2. 在左侧窗口部分中，选择用于配置安全设置的节点。
   可以为保护范围内的选定节点或项目应用包含安全设置的预定义模板。
   在窗口的左侧部分，您可以选择网络文件资源的视图，创建保护范围或创建虚拟保护范围。

3. 在窗口的右侧部分，执行下列操作之一：

   - 在“**安全级别**”选项卡上，选择要应用的安全级别。

- 在以下选项卡中，根据要求配置选定节点或项目的所需安全设置：
  - 常规
  - 操作
  - 性能

4. 在“保护范围设置”窗口中，单击“保存”按钮。

将保存新的保护范围设置。

为实时文件保护任务选择预定义安全级别

可以为受保护设备文件资源树或列表中的选定节点应用以下预定义安全级别之一：“最优性能”、“推荐”和“最佳保护”。

要选择其中一个预定义安全级别：

1. 打开“保护范围设置”窗口。
2. 在受保护设备网络文件资源树或列表中，选择要设置预定义安全级别的节点或项。
3. 确保选定的节点或项包含在保护范围中。
4. 在窗口右侧的“安全级别”选项卡中，选择要应用的安全级别。
   该窗口将显示与选定安全级别相对应的安全性设置列表。
5. 单击“保存”按钮。
   将保存任务设置，并将这些设置立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

配置常规任务设置

要配置“实时文件保护”任务的常规安全设置：

1. 打开“保护范围设置”窗口。
2. 选择“常规”选项卡。
3. 在“对象保护”部分中，指定要包含在保护范围内的对象：
   - 所有对象
   - 按格式扫描对象
   - 按反病毒数据库中指定的扩展名列表扫描对象
   - 按指定的扩展名列表扫描对象

- 扫描磁盘引导扇区和 MBR
- 扫描 NTFS 交换数据流

4. 在“性能”组框中，选中或清除“仅保护新文件和已修改的文件”复选框。

> 如果清除该复选框，要在可用选项之间切换，请单击每个复合对象类型对应的“全部/仅新建”链接。

5. 在“复合对象保护”部分中，指定要包含在保护范围内的复合对象：
   - 全部/仅新的压缩文件
   - 全部/仅新的 SFX 压缩文件
   - 全部/仅新的电子邮件数据库
   - 全部/仅新的打包的对象
   - 全部/仅新的纯文本电子邮件
   - 全部/仅新的嵌入的 OLE 对象
6. 单击“保存”。

将保存新的任务配置。

配置操作

要为“实时文件保护”任务配置对受感染的对象和其他检测到的对象的操作：

1. 打开“保护范围设置”窗口。
2. 选择“操作”选项卡。
3. 选择要对受感染的对象和其他检测到的对象执行的操作：
   - 仅通知。
   - 阻止访问。
   - 执行附加操作。
     从下拉列表中选择操作：
     - 清除。
     - 清除；清除失败时则删除。
     - 删除。
     - 推荐。
4. 选择要对疑似感染的对象执行操作：

- 仅通知。
- 阻止访问。
- 执行附加操作。
  从下拉列表中选择操作：
  - 隔离。
  - 删除。
  - 推荐。

5. 根据检测的对象类型配置要对对象执行的操作：
   a. 清除或选中“根据检测到的对象的类型执行操作”复选框。
   b. 单击“设置”按钮。
   c. 在打开的窗口中，选择针对每种检测到的对象类型的主要操作和次要操作（如果主要操作失败则执行）。
   d. 单击“确定”。
6. 选择要对不可修改的复合文件执行的操作：选中或清除“在检测到嵌入对象时完全删除应用程序无法修改的复合文件”复选框。
7. 单击“保存”。

将保存新的任务配置。

配置性能

要配置“实时文件保护”任务的性能设置：

1. 打开“保护范围设置”窗口。
2. 选择“性能”选项卡。
3. 在“排除”部分中：
   - 清除或选中“排除文件”复选框。
   - 清除或选中“不检测”复选框。
   - 针对每个设置单击“编辑”按钮以添加排除项。
4. 在“高级设置”部分中：
   - 超过以下时间则停止扫描(秒)
   - 不扫描大于该值的复合对象(MB)
   - 使用 iSwift 技术

- 使用 iChecker 技术

实时文件保护任务统计

实时文件保护任务运行时，您可以查看有关 Kaspersky Embedded Systems Security 自任务启动以来已处理的对象数量的详细实时信息。

要查看"实时文件保护"任务统计：

1. 在应用程序控制台树中，展开"**实时计算机保护**"节点。
2. 选择"**实时文件保护**"子节点。

   任务统计显示在选定节点的结果窗格的"**统计**"部分中。

可以查看 Kaspersky Embedded Systems Security 自启动以来已处理的对象的信息（请参见下表）。

实时文件保护任务统计

字段	描述
检测到	Kaspersky Embedded Systems Security 检测到的对象数量。例如，如果 Kaspersky Embedded Systems Security 在五个文件中检测到一个恶意对象，该字段中的值将增加 1。
检测到受感染和其他对象	Kaspersky Embedded Systems Security 发现并归类为"已感染"的对象数量，或者发现的可被入侵者用来破坏设备或个人数据的合法软件文件数量。
检测到疑似感染的对象	Kaspersky Embedded Systems Security 检测到的疑似感染对象数。
对象未清除	Kaspersky Embedded Systems Security 因以下原因未清除的对象数： • 检测到的对象是无法清除的类型。 • 清除期间出现错误。
对象未移至隔离区	Kaspersky Embedded Systems Security 尝试隔离未成功（例如，由于磁盘空间不足）的对象数。
对象未删除	Kaspersky Embedded Systems Security 尝试删除未成功（例如，其他应用程序阻止访问对象）的对象数。
对象未扫描	Kaspersky Embedded Systems Security 在保护范围中无法扫描（例如，其他应用程序阻止访问对象）的对象数。
对象未备份	Kaspersky Embedded Systems Security 尝试在备份中保存副本但未成功（例如，由于磁盘空间不足）的对象数。
处理错误	对其处理产生错误的对象数。
对象已清除	Kaspersky Embedded Systems Security 已清除的对象的数量。
已移至隔离区	Kaspersky Embedded Systems Security 已隔离的对象的数量。
已移动到备份	Kaspersky Embedded Systems Security 保存到备份的对象副本数。
对象已删除	Kaspersky Embedded Systems Security 已删除的对象的数量。

受密码保护的对象	因受到密码保护而被 Kaspersky Embedded Systems Security 跳过的对象（例如压缩文件）数量。
已损坏的对象	Kaspersky Embedded Systems Security 由于对象格式损坏而跳过的对象数。
对象已处理	Kaspersky Embedded Systems Security 已处理的对象的总数。

通过单击详细信息窗格中“**管理**”部分的“**打开任务日志**”链接，可以在任务日志中查看实时文件保护任务统计。

如果“实时文件保护任务日志”窗口中的“**事件总数**”字段的值大于 0，则推荐手动处理“**事件**”选项卡上的任务日志中的事件。

通过 Web 插件管理“实时文件保护”任务

在本部分中，学习如何通过 Web 插件界面管理“实时文件保护”任务。

配置“实时文件保护”任务

无法通过 Web 插件为“实时文件保护”任务更改预定义安全级别。

要通过 Web 插件配置“实时文件保护”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时计算机保护**”部分。
5. 单击“**实时文件保护**”子部分中的“**设置**”。
6. 按下表所述配置设置。

“实时文件保护”任务设置

设置	描述
智能模式	Kaspersky Embedded Systems Security 自行选择扫描对象。对象在打开时被扫描，如果对象进行了修改，则在保存对象后重新扫描该对象。如果进程多次访问并修改对象，只有进程最后一次保存对象后，Kaspersky Embedded Systems Security 才会重新扫描对象。
访问时	Kaspersky Embedded Systems Security 在对象打开以进行读取、执行或修改时扫描所有对象。
访问和修改时	Kaspersky Embedded Systems Security 在对象打开时扫描该对象，如果对象进行了修改，则在对象保存后重新扫描该对象。 默认选中该选项。

运行时	仅在访问文件以执行该文件时，Kaspersky Embedded Systems Security 才扫描该文件。
对启动进程的更深度分析(分析结束之前将阻止进程启动)	Kaspersky Embedded Systems Security 对启动进程执行更长时间的分析，检测到威胁的可能性更高。在分析结束之前，将阻止进程启动。
使用启发式分析	此复选框可在对象扫描过程中启用/禁用启发式分析。 如果选中该复选框，则启用启发式分析。 如果取消选中该复选框，则禁用启发式分析。 默认选中该复选框。
启发式分析级别	启发式分析级别用于在威胁搜索的彻底程度、操作系统资源负荷和扫描所需时间之间建立平衡。 以下扫描灵敏度级别可用： • **轻度**。启发式分析在可执行文件中执行较少指令。在该模式下检测出威胁的可能性较小。扫描速度较快，而且占用资源较少。 • **中度**。启发式分析执行 Kaspersky 专家推荐的可执行文件指令数。 默认选中该级别。 • **深度**。启发式分析在可执行文件中执行较多指令。在该模式下检测出威胁的可能性较大。扫描使用更多系统资源、花费更多时间且可生成更多误报。 如果选中“**使用启发式分析**”复选框，则该设置可用。
应用信任区域	使用此复选框可启用/禁用任务的受信任区域。 如果选中该复选框，Kaspersky Embedded Systems Security 会将受信任进程的文件操作添加到任务设置中配置的扫描排除中。 如果清除该复选框，Kaspersky Embedded Systems Security 会在创建任务的保护范围时忽略受信任进程的文件操作。 默认选中该复选框。
在保护中使用 KSN	该复选框可启用或禁用 KSN 服务的使用。 如果选中该复选框，应用程序将使用卡巴斯基安全网络数据确保应用程序更快速地对新威胁做出响应，并降低误报的可能性。 如果清除该复选框，则任务将不使用 KSN 服务。 默认选中该复选框。
阻止显示恶意活动的网络会话对网络共享资源的访问	该复选框会启用或禁用阻止当前会话，并控制网络共享资源对当前会话的可用性。 如果选中该复选框，Kaspersky Embedded Systems Security 会阻止当前会话，并且就当前会话而言，使网络共享资源对在被阻止的主机存储部分检测到恶意活动的主机不可用 如果清除该复选框，则不应用条件并且 Kaspersky Embedded Systems Security 正常运行。 默认取消选中该复选框。 您可以在阻止的主机存储中查看阻止的主机列表。

	您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。
检测到活动感染时启动关键区域扫描	如果选中此复选框，在检测到活动感染时，Kaspersky Embedded Systems Security 将创建并启动临时的“关键区域扫描”任务。当“关键区域扫描”临时任务完成后，Kaspersky Embedded Systems Security 会删除此临时任务。 如果清除此复选框，在检测到活动感染时，Kaspersky Embedded Systems Security 不会创建和启动“关键区域扫描”任务。 默认选中该复选框。
保护范围	您可以配置保护范围的安全性设置。

配置任务保护范围

要配置“实时文件保护”任务的保护范围：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时计算机保护**”部分。
5. 单击“**实时文件保护**”子部分中的“**设置**”。
6. 选择“**保护范围**”部分。
7. 执行以下操作之一：
   - 单击“**添加**”按钮以添加新规则。
   - 选择一个现有规则，然后单击“**编辑**”按钮。

   将打开“**编辑范围**”窗口。
8. 将切换按钮切换到“**活动**”，然后选择一个对象类型。
9. 在“**对象保护**”部分中，配置以下设置：
   - **对象保护模式**：
     - 所有对象
     - 按格式扫描对象
     - 按反病毒数据库中指定的扩展名列表扫描对象
     - 按指定的扩展名列表扫描对象
   - 扫描磁盘引导扇区和 **MBR**

- 扫描 NTFS 交换数据流

10. 在“对象保护”部分中，选中或清除“仅保护新文件和已修改的文件”复选框。
11. 在“复合对象保护”部分中，指定要包含在扫描范围内的复合对象：
    - 压缩文件
    - SFX 压缩文件
    - 打包的对象
    - 电子邮件数据库
    - 纯文本电子邮件
    - 嵌入的 OLE 对象
    - 在检测到嵌入对象时完全删除应用程序无法修改的复合文件
12. 选择要对受感染的对象和其他检测到的对象执行的操作：
    - 仅通知。
    - 阻止访问。
    - 执行附加操作。
      从下拉列表中选择操作：
      - 清除。
      - 清除；清除失败时则删除。
      - 删除。
      - 推荐。
13. 选择要对疑似感染的对象执行操作：
    - 仅通知。
    - 阻止访问。
    - 执行附加操作。
      从下拉列表中选择操作：
      - 隔离。
      - 删除。
      - 推荐。
14. 根据检测的对象类型配置要对对象执行的操作：
    a. 清除或选中“根据检测到的对象的类型执行操作”复选框。

b. 单击“**设置**”按钮。

c. 在打开的窗口中，选择针对每种检测到的对象类型的主要操作和次要操作（如果主要操作失败则执行）。

d. 单击“**确定**”。

15. 在“**排除**”部分中，配置以下设置：

- 清除或选中“排除文件”复选框。
- 清除或选中“不检测”复选框。

16. 在“**性能**”部分中，配置以下设置：

- 超过以下时间则停止扫描(秒)
- 不扫描大于该值的复合对象(MB)
- 使用 iSwift 技术
- 使用 iChecker 技术

17. 单击“**确定**”按钮。

KSN 使用

本节包含有关“KSN 使用”任务以及如何配置的信息。

关于“KSN 使用”任务

卡巴斯基安全网络（也称为“KSN”）是一个在线服务的基础架构，提供访问 Kaspersky 有效的知识库。该知识库中包含了文件信誉、网页资源和程序的相关信息。卡巴斯基安全网络允许 Kaspersky Embedded Systems Security 迅速对新威胁作出反应，提高许多保护组件的性能，以降低误报可能性。

要启动“KSN 使用”任务，您必须接受卡巴斯基安全网络声明。

Kaspersky Embedded Systems Security 从卡巴斯基安全网络接收的信息仅与程序的信誉有关。

加入 KSN 使 Kaspersky 能够接收有关新威胁类型和来源的信息，研发出使其失效的方法，并减少应用程序组件中的误报数量。

有关传输、处理、存储和销毁有关应用程序使用情况的更多详细信息在“KSN 使用”任务的“**数据处理**”窗口中和 Kaspersky 网站上的隐私策略中提供。

加入卡巴斯基安全网络完全出于自愿。在安装 Kaspersky Embedded Systems Security 后，做出有关参加卡巴斯基安全网络的决定。您可以随时更改有关参加卡巴斯基安全网络的决定。

可在以下 Kaspersky Embedded Systems Security 任务中使用卡巴斯基安全网络：

- 实时文件保护。
- 按需扫描。
- 应用程序启动控制。

卡巴斯基专属安全网络

有关如何配置卡巴斯基专属安全网络（以下称为“私有 KSN”）的详细信息，请参见 *Kaspersky Security Center 帮助*。

如果在设备上使用私有 KSN，则在“KSN 使用”任务的“数据处理”窗口中，可以通过选中“**我接受参加卡巴斯基安全网络的条款**”复选框来阅读 KSN 声明和启用该任务。接受该条款，即表示您同意将 KSN 声明中提到的各类数据（安全请求、统计数据）发送到 KSN 服务。

接受私有 KSN 条款后，用于调整全球 KSN 使用的复选框将不可用。

如果在“KSN 使用”任务运行时禁用私有 KSN，则将出现*授权许可冲突*错误且任务将停止。要继续保护设备，您需要接受“**数据处理**”窗口中的 KSN 声明并重新启动该任务。

撤消接受 KSN 声明

您可以随时撤消接受声明并停止与卡巴斯基安全网络的任何数据交换。以下操作被视为完全或部分撤消 KSN 声明：

- 清除“**发送关于已扫描文件的数据**”复选框：应用程序停止将扫描的文件的校验和发送到 KSN 服务进行分析。
- 清除“**发送卡巴斯基安全网络统计信息**”复选框：应用程序停止处理附加 KSN 统计的数据。
- 清除“**我接受参加卡巴斯基安全网络的条款**”复选框：应用程序停止所有与 KSN 相关的数据处理，“KSN 使用”任务停止。
- 卸载“KSN 使用”组件：所有与 KSN 相关的数据处理都将停止。
- 卸载 Kaspersky Embedded Systems Security：所有与 KSN 相关的数据处理都将停止。
- 卸载 Kaspersky Embedded Systems Security 授权许可密钥或授权许可被暂停：所有与 KSN 相关的数据处理停止。

“KSN 使用”任务默认设置

您可以更改“KSN 使用”任务的默认设置（请参见下表）。

“KSN 使用”任务默认设置

设置	默认值	描述
对 KSN 不信任的对象执行的操作	删除	您可以指定 Kaspersky Embedded Systems Security 对被 KSN 标识为不受信任的对象执行的操作。
数据传输	为大小不超过 2 MB 的文件计算文件校验和（MD5 哈希）。	您可以指定要使用 MD5 算法为其计算校验和以提交给 KSN 的文件的最大大小。如果清除该复选框，Kaspersky Embedded Systems Security 将为任意大小的文件计算 MD5 哈希。
任务启动计划	不设置任务的首次启动计划。	您可以手动启动该任务或配置计划启动。
使用 Kaspersky Security Center 作为 KSN 代理	选中	默认情况下，数据通过 Kaspersky Security Center 发送到 KSN。 只能通过管理插件更改此设置。
我接受参加卡巴斯基安全网络的条款	已清除	如果选中，即接受安装后加入 KSN。您可以随时更改决定。
发送卡巴斯基安全网络统计信息	选中（仅当接受 KSN 声明时应用）	如果接受 KSN 声明，将自动发送 KSN 统计，除非清除相应复选框。
发送关于已扫描文件的数据	选中（仅当接受 KSN 声明时应用）	如果接受 KSN 声明，将发送自任务启动以来扫描和分析的文件的数据。您可以随时清除该复选框。

通过管理插件管理“KSN 使用”

在本节中，学习如何通过管理插件配置“KSN 使用”任务和数据处理。

配置“KSN 使用”任务

要配置“KSN 使用”任务：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**实时计算机保护**”部分中，单击“**KSN 使用**”子部分中的“**设置**”按钮。
   将打开“**KSN 使用**”窗口。
5. 在“**常规**”选项卡上，配置以下任务设置：
   - 在“**对 KSN 不信任的对象执行的操作**”部分中，指定 Kaspersky Embedded Systems Security 在检测到 KSN 确定为不受信任的对象时将执行的操作：
     - 删除
     - 记录信息
   - 在“**数据传输**”部分中，限制要为其计算校验和的文件的大小：
     - 清除或选中“如果文件大小超过以下大小(MB)，则在发送到 KSN 之前不计算校验和”复选框。
     - 如果需要，在右侧字段中更改 Kaspersky Embedded Systems Security 要为其计算校验和的最大文件大小。
   - 在“**KSN 代理**”部分中，清除或选中“使用 Kaspersky Security Center 作为 KSN 代理”复选框。

     要启用 KSN 代理，必须接受 KSN 声明并正确配置 Kaspersky Security Center。有关详细信息，请参见 *Kaspersky Security Center 帮助*。
6. 如果需要，在“**任务管理**”选项卡上配置任务启动计划。例如，如果您希望在重新启动受保护设备时自动运行任务，可以按计划启动任务并指定“**应用程序启动时**”频率。
   应用程序将按计划自动启动“KSN 使用”任务。
7. 在启动任务前配置数据处理。
8. 单击“**确定**”。

将应用修改的设置。修改设置的日期和时间以及有关修改前后的任务设置的信息均保存在系统审核日志中。

配置数据处理

要配置哪些数据将被 KSN 服务处理并接受 KSN 声明：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**实时计算机保护**”部分中，单击“**KSN 使用**”子部分中的“**数据处理**”按钮。
   将打开“**KSN 数据处理**”窗口。
5. 在“**统计信息和服务**”选项卡上，阅读声明并选中“**我接受参加卡巴斯基安全网络的条款**”复选框。
6. 为提高保护级别，以下复选框会自动选中：
   - 发送关于已扫描文件的数据。
   - 发送卡巴斯基安全网络统计信息。

   您可以随时清除这些复选框并停止发送附加数据。
7. “发送卡巴斯基安全网络统计信息”复选框默认情况下处于选中状态。如果您不希望 Kaspersky Embedded Systems Security 将其他统计发送到 Kaspersky，可以随时清除该复选框。
8. 单击“**确定**”。
   将保存数据处理配置。

通过应用程序控制台管理“KSN 使用”

在本节中，学习如何通过应用程序控制台配置“KSN 使用”任务和数据处理。

配置“KSN 使用”任务

要配置“KSN 使用”任务：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**KSN 使用**”子节点。
3. 在结果窗格中单击“**属性**”链接。
   将打开“**任务设置**”窗口的“**常规**”选项卡。
4. 配置任务：
   - 在“**对 KSN 不信任的对象执行的操作**”部分中，指定 Kaspersky Embedded Systems Security 在检测到 KSN 确定为不受信任的对象时将执行的操作：
     - 删除
     - 记录信息
   - 在“**数据传输**”部分中，限制要为其计算校验和的文件的大小：
     - 清除或选中“**如果文件大小超过以下大小(MB)，则在发送到 KSN 之前不计算校验和**”复选框。
     - 如果需要，在右侧字段中更改 Kaspersky Embedded Systems Security 要为其计算校验和的最大文件大小。
5. 如果需要，在“**计划**”和“**高级**”选项卡上配置任务启动计划。例如，如果您希望在重新启动受保护设备时自动运行该任务，可以启用按计划启动任务并指定“**应用程序启动时**”的启动频率。
   应用程序将按计划自动启动“KSN 使用”任务。
6. 在启动任务前配置数据处理。
7. 单击“**确定**”。

将应用修改的设置。修改设置的日期和时间以及有关修改前后的任务设置的信息均保存在系统审核日志中。

配置数据处理

要配置哪些数据将被 KSN 服务处理并接受 KSN 声明：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**KSN 使用**”子节点。
3. 在结果窗格中单击“**数据处理**”链接。
   将打开“**数据处理**”窗口。
4. 在“**统计信息和服务**”选项卡上，阅读声明并选中“**我接受参加卡巴斯基安全网络的条款**”复选框。
5. 为提高保护级别，以下复选框会自动选中：
   - 发送关于已扫描文件的数据。
   - 发送卡巴斯基安全网络统计信息。

您可以随时清除这些复选框并停止发送附加数据。

6. “发送卡巴斯基安全网络统计信息”复选框默认情况下处于选中状态。如果您不希望 Kaspersky Embedded Systems Security 将其他统计发送到 Kaspersky，可以随时清除该复选框。

7. 单击“**确定**”。

将保存数据处理配置。

通过 Web 插件管理“KSN 使用”

要通过 Web 插件配置“KSN 使用”任务和数据处理：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。

2. 单击要配置的策略名称。

3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。

4. 选择“**实时计算机保护**”部分。

5. 单击“**KSN 使用**”子部分中的“**设置**”。

6. 按下表所述配置设置。

通过管理插件设置配置“KSN 使用”任务和数据处理

设置	描述
删除	Kaspersky Embedded Systems Security 将删除具有 KSN 不信任状态的对象，并在备份中放置副本。 默认选中该选项。
记录信息	Kaspersky Embedded Systems Security 将在任务日志中记录有关具有 KSN 不信任状态的对象的信息。Kaspersky Embedded Systems Security 不会删除不受信任的对象。
如果文件大小超过以下大小，则在发送到 KSN 之前不计算校验和	此复选框可启用或禁用为指定大小的文件计算校验和，以将此信息提交至 KSN 服务。 校验和计算的持续时间取决于文件大小。 如果选中此复选框，则 Kaspersky Embedded Systems Security 不会为超过指定大小（以 MB 为单位）的文件计算校验和。 如果清除该复选框，Kaspersky Embedded Systems Security 将为任意大小的文件计算校验和。 默认选中该复选框。
我确认我已完全阅读、理解并接受参加卡巴斯基安全网络的条款	选中此复选框即表示您确认您已阅读并接受卡巴斯基安全网络声明的条款。
发送关于已扫描文件的数据	如果选中该复选框，Kaspersky Embedded Systems Security 会将扫描的文件的校验和发送到 Kaspersky。关于每个文件的安全性的结论基于从 KSN 收到的信誉。

	如果清除该复选框，Kaspersky Embedded Systems Security 不会将文件的校验和发送到 KSN。 请注意，文件信誉请求可能在受限制模式下发送。限制用于保护 Kaspersky 信誉服务器免受 DDoS 攻击。在这种情况下，所发送的文件信誉请求的参数由 Kaspersky 专家建立的规则和方法定义，用户无法在受保护设备上进行配置。这些规则和方法的更新与应用程序数据库更新一起接收。如果应用限制，“KSN 使用”任务统计中将显示“*由 Kaspersky 启用以保护 KSN 服务器免受 DDoS*”状态。 默认选中该复选框。
同意处理数据作为卡巴斯基安全网络统计的一部分	如果选中该复选框，Kaspersky Embedded Systems Security 会发送附加统计，其中可能包含个人数据。作为 KSN 统计发送的所有数据的列表在 KSN 声明中有所说明。Kaspersky 收到的数据用于改善应用程序质量和提高威胁检测速率级别。 如果清除该复选框，Kaspersky Embedded Systems Security 不会发送其他统计。 默认选中该复选框。
任务管理	您可以配置按计划启动任务的设置。

配置其他数据传输

Kaspersky Embedded Systems Security 可以配置为将以下数据发送到 Kaspersky：

- 扫描的文件的校验和（“**发送关于已扫描文件的数据**”复选框）。
- 附加统计信息，包括个人数据（“**发送卡巴斯基安全网络统计信息**”复选框）。

有关发送到 Kaspersky 的数据的详细信息，请参见本指南的“本地数据处理”部分。

只有选中“**我接受参加卡巴斯基安全网络的条款**”复选框，才能选中或清除相应的复选框。

默认情况下，当您接受 KSN 声明后，Kaspersky Embedded Systems Security 将发送文件的校验和和附加统计。

仅当 Kaspersky Security Center 策略阻止数据处理设置的更改时，“**我接受参加卡巴斯基安全网络的条款**”复选框才可编辑。

可能的复选框状态和相应条件

复选框状态	“发送关于已扫描文件的数据”复选框状态的条件	“发送卡巴斯基安全网络统计信息”复选框状态的条件	“我接受参加卡巴斯基安全网络的条款”复选框状态的条件
☑	• 已发送信誉请求 • 复选框可编辑	• 已发送附加统计 • 复选框可编辑	• 已接受卡巴斯基安全网络声明的条款 • 复选框可编辑
☑	• 已发送信誉请求 • 复选框不可编辑	• 已发送附加统计 • 复选框不可编辑	• 已接受卡巴斯基安全网络声明的条款 • 复选框不可编辑

☐	• 未发送信誉请求 • 复选框可编辑	• 未发送附加统计 • 复选框可编辑	• 未接受卡巴斯基安全网络声明的条款 • 复选框可编辑
☐	• 未发送信誉请求 • 复选框不可编辑	• 未发送附加统计 • 复选框不可编辑	• 未接受卡巴斯基安全网络声明的条款 • 复选框不可编辑

“KSN 使用”任务统计

在执行“KSN 使用”任务期间，可以实时查看 Kaspersky Embedded Systems Security 自启动以来已处理的对象数量的相关详细信息。有关任务执行期间发生的所有事件的信息记录在任务日志中。

要查看“KSN 使用”任务统计：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**KSN 使用**”子节点。

任务统计显示在选定节点的详细信息窗格的“**统计**”部分中。

您可以查看自任务启动以来 Kaspersky Embedded Systems Security 已处理对象的相关信息（请参见下表）。

“KSN 使用”任务统计

字段	描述
请求发送错误	对其处理产生任务错误的 KSN 请求数。
统计信息已形成	发送到 KSN 的生成的统计包数量。
对象已删除	Kaspersky Embedded Systems Security 在运行“KSN 使用”任务时删除的对象数。
已移动到备份	Kaspersky Embedded Systems Security 已将其副本保存到备份的对象数。
对象未删除	Kaspersky Embedded Systems Security 尝试删除但操作失败的对象数，例如，由于其他应用程序阻止访问对象。有关此类对象的信息记录在任务日志中。
对象未备份	Kaspersky Embedded Systems Security 尝试在备份中保存副本但操作失败的对象数，例如，由于磁盘空间不足。程序不会清除或删除无法移动到备份中的文件。有关此类对象的信息记录在任务日志中。
受限	该状态表示应用程序是否在受限制模式下发送文件信誉请求。根据卡巴斯基专家的建议，在受限

模式	制模式下，Kaspersky Embedded Systems Security 仅发送文件信誉请求的一部分。

网络威胁防护

本节包含有关“网络威胁防护”任务以及如何配置该任务的信息。

关于“网络威胁防护”任务

> “网络威胁防护”只能安装在运行 Microsoft Windows 7 及更高版本或 Windows Server 2008 R2 及更高版本的设备上。

“网络威胁防护”任务会扫描入站网络流量中是否存在典型网络攻击活动。在检测到以您的计算机为目标的网络攻击企图时，Kaspersky Embedded Systems Security 将阻止攻击计算机的网络活动。然后，您的屏幕将显示一条警告，指出有网络攻击的企图，并显示有关攻击计算机的信息。

默认情况下，“网络威胁防护”任务在“**检测到攻击时阻止连接**”模式下运行。在此模式下，Kaspersky Embedded Systems Security 会将出现典型网络攻击活动的主机的 IP 地址添加到阻止的主机列表中。

您可以在阻止的主机存储中查看阻止的主机列表。

您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

在以下情况下，将从阻止的主机列表中删除出现典型网络攻击活动的主机的 IP 地址：

- Kaspersky Embedded Systems Security 已卸载。
- 手动从阻止的主机列表中删除了 IP 地址。
- 主机阻止期限已到期。
- “网络威胁防护”任务已停止，并且清除了“**未运行任务时不停止流量分析**”复选框。
- “**检测到攻击时阻止连接**”模式已关闭。

“网络威胁防护”任务默认设置

“网络威胁防护”任务使用下表描述的默认设置。您可以更改这些设置的值。

“网络威胁防护”任务默认设置

设置	默认值	描述
处理模式	检测到攻击时阻止连接	“网络威胁防护”任务可以在“直通”、“仅通知网络攻击”或“检测到攻击时阻止连接”模式下启动。

		该复选框用于启用或禁用将出现典型网络攻击活动的主机添加到阻止的主机列表。 如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，并将出现典型网络攻击活动的主机的 IP 地址添加到阻止的主机列表。 默认选择该模式。 您可以在阻止的主机存储中查看阻止的主机列表。 您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。 如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，但不会阻止攻击计算机的网络活动。 如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，但不会记录有关检测到的活动的事件，也不会阻止攻击计算机的网络活动。 例如，当受保护设备的性能下降时，可以使用此模式。
排除	不应用排除列表。	指定要从任务保护范围中排除的区域。
计划设置	默认情况下，当 Kaspersky Embedded Systems Security 启动时，“网络威胁防护”任务自动启动。	您可以配置该计划。

通过应用程序控制台配置“网络威胁防护”任务

在本节中，学习如何通过应用程序控制台界面管理“网络威胁防护”任务。

常规任务设置

要配置常规任务设置：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**网络威胁防护**”子节点。
3. 在“**网络威胁防护**”节点的详细信息窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。

4. 打开“**常规**”选项卡。

5. 在“**处理模式**”部分中选择处理模式：

- 直通。

  如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，但不会记录有关检测到的活动的事件，也不会阻止攻击计算机的网络活动。

  例如，当受保护设备的性能下降时，可以使用此模式。

- 仅通知网络攻击。

  如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，但不会阻止攻击计算机的网络活动。

- 检测到攻击时阻止连接。

  该复选框用于启用或禁用将出现典型网络攻击活动的主机添加到阻止的主机列表。

  如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，并将出现典型网络攻击活动的主机的 IP 地址添加到阻止的主机列表。

  默认选择该模式。

  您可以在阻止的主机存储中查看阻止的主机列表。

  您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

6. 选中或清除“未运行任务时不停止流量分析”复选框。

   如果选中此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，并根据所选处理模式阻止攻击计算机的网络活动。

   如果清除此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 不会扫描入站网络流量中是否存在典型网络攻击活动，也不回阻止攻击计算机的网络活动。

   默认取消选中该复选框。

7. 单击“**确定**”。

添加排除

要添加“网络威胁防护”任务的排除项，请执行以下步骤：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。

2. 选择“**网络威胁防护**”子节点。

3. 在“**网络威胁防护**”节点的详细信息窗格中，单击“**属性**”链接。

   将打开“**任务设置**”窗口。

4. 在“**排除**”选项卡上，选中“不控制排除的 IP 地址”复选框。

   如果选中此复选框，Kaspersky Embedded Systems Security 不会扫描排除的 IP 地址的入站网络流量。
   如果清除该复选框，Kaspersky Embedded Systems Security 不会应用排除列表。

5. 指定 IP 地址，然后单击“**添加**”按钮。

6. 单击“**确定**”。

通过管理插件配置“网络威胁防护”任务

在本节中，学习如何通过管理插件界面管理“网络威胁防护”任务。

常规任务设置

要配置常规任务设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择要为其配置应用程序设置的管理组。

3. 在选定的管理组的详细窗格中执行以下操作之一：

   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**实时计算机保护**”部分中，单击“**网络威胁防护**”子部分中的“**设置**”按钮。
   将打开“**网络威胁防护**”窗口。

5. 打开“**常规**”选项卡。

6. 在“**处理模式**”部分中选择处理模式：

   - 直通。

     如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，但不会记录有关检测到的活动的事件，也不会阻止攻击计算机的网络活动。
     例如，当受保护设备的性能下降时，可以使用此模式。

   - 仅通知网络攻击。

如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，但不会阻止攻击计算机的网络活动。

- 检测到攻击时阻止连接。

  该复选框用于启用或禁用将出现典型网络攻击活动的主机添加到阻止的主机列表。

  如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，并将出现典型网络攻击活动的主机的 IP 地址添加到阻止的主机列表。

  默认选择该模式。

  您可以在阻止的主机存储中查看阻止的主机列表。

  您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

7. 选中或清除“未运行任务时不停止流量分析”复选框。

   如果选中此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，并根据所选处理模式阻止攻击计算机的网络活动。

   如果清除此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 不会扫描入站网络流量中是否存在典型网络攻击活动，也不回阻止攻击计算机的网络活动。

   默认取消选中该复选框。

8. 单击“**确定**”。

添加排除

要添加“网络威胁防护”任务的排除项，请执行以下步骤：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**实时计算机保护**”部分中，单击“**网络威胁防护**”子部分中的“**设置**”按钮。

   将打开“**网络威胁防护**”窗口。

5. 在“**排除**”选项卡上，选中“不控制排除的 IP 地址”复选框。

如果选中此复选框，Kaspersky Embedded Systems Security 不会扫描排除的 IP 地址的入站网络流量。
如果清除该复选框，Kaspersky Embedded Systems Security 不会应用排除列表。

6. 指定 IP 地址，然后单击“**添加**”按钮。
7. 单击“**确定**”。

通过 Web 插件配置“网络威胁防护”任务

在本节中，学习如何通过 Web 插件界面管理“网络威胁防护”任务。

常规任务设置

要配置常规任务设置：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时计算机保护**”部分。
5. 单击“**网络威胁防护**”子部分中的“**设置**”。
6. 打开“**常规**”选项卡。
7. 在“**处理模式**”部分中选择处理模式：

- 直通。

  如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，但不会记录有关检测到的活动的事件，也不会阻止攻击计算机的网络活动。
  例如，当受保护设备的性能下降时，可以使用此模式。

- 仅通知网络攻击。

  如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，但不会阻止攻击计算机的网络活动。

- 检测到攻击时阻止连接。

该复选框用于启用或禁用将出现典型网络攻击活动的主机添加到阻止的主机列表。

如果选择此模式，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，记录有关检测到的活动的事件，并将出现典型网络攻击活动的主机的 IP 地址添加到阻止的主机列表。

默认选择该模式。

您可以在阻止的主机存储中查看阻止的主机列表。

您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

8. 选中或清除“未运行任务时不停止流量分析”复选框。

如果选中此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 会扫描入站网络流量中是否存在典型网络攻击活动，并根据所选处理模式阻止攻击计算机的网络活动。

如果清除此复选框，当“网络威胁防护”任务停止后，Kaspersky Embedded Systems Security 不会扫描入站网络流量中是否存在典型网络攻击活动，也不回阻止攻击计算机的网络活动。

默认取消选中该复选框。

9. 单击“**确定**”。

添加排除

要添加“网络威胁防护”任务的排除项，请执行以下步骤：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时计算机保护**”部分。
5. 单击“**网络威胁防护**”子部分中的“**设置**”。
6. 在“**排除**”选项卡上，选中“**不控制排除的 IP 地址**”复选框。

如果选中此复选框，Kaspersky Embedded Systems Security 不会扫描排除的 IP 地址的入站网络流量。

如果清除该复选框，Kaspersky Embedded Systems Security 不会应用排除列表。

7. 指定 IP 地址，然后单击“**添加**”按钮。
8. 单击“**确定**”。

应用程序启动控制

本节包含有关“应用程序启动控制”任务以及如何配置的信息。

关于“应用程序启动控制”任务

在运行“应用程序启动控制”任务时，Kaspersky Embedded Systems Security 会监控用户启动应用程序的尝试，并允许或拒绝这些应用程序启动。“应用程序启动控制”任务依赖于“默认拒绝”原则，这意味着任务设置中不允许的任何应用程序都会被自动阻止。

您可以使用以下方法之一允许应用程序启动：

- 设置受信任的应用程序的允许规则。
- 启动时在 KSN 中检查受信任应用程序的声誉。

该任务为拒绝应用程序启动赋予最高优先级。例如，如果某个应用程序被阻止规则之一阻止启动，该应用程序将被拒绝启动，不管 KSN 的受信任结论如何。而且，如果应用程序不受 KSN 服务信任，但包括在允许规则范围中，此应用程序会被拒绝启动。

所有启动应用程序的尝试将记录在任务日志中。

“应用程序启动控制”任务可以运行在以下两种模式之一：

- **活动**。Kaspersky Embedded Systems Security 使用一组规则来控制处于应用程序启动控制规则范围内的应用程序的启动。应用程序启动控制规则的范围在该任务的设置中指定。如果应用程序处于应用程序启动控制规则范围内，并且任务设置不满足任何指定规则，此应用程序会被拒绝启动。

  不在“应用程序启动控制”任务设置中指定的任何规则范围内的应用程序会被拒绝启动，不管“应用程序启动控制”任务设置如何。

  如果未创建任何规则或为一台受保护设备创建了超过 65,535 条规则，则“**应用程序启动控制**”任务无法在活动模式下启动。

- **仅统计**。Kaspersky Embedded Systems Security 不使用应用程序启动控制规则来允许或拒绝应用程序启动。相反，它只记录有关应用程序启动、正在运行的应用程序所满足的规则以及如果任务在“**活动**”模式下运行已执行的操作的信息。所有应用程序均允许启动。默认设置此模式。

  您可以使用此模式基于任务日志中记录的信息创建应用程序启动控制规则。

您可根据以下方案之一配置“应用程序启动控制”任务：

- 高级规则配置及其在应用程序启动控制中的使用。
- 基本规则配置和应用程序启动控制的 KSN 使用。

如果操作系统文件在“应用程序启动控制”任务的范围内，建议在创建应用程序启动控制规则时确保新创建的规则允许此类应用程序。否则，操作系统可能无法启动。

Kaspersky Embedded Systems Security 还会拦截在 Linux 的 Windows 子系统下启动的进程（从 UNIX™ shell 或命令行解释器运行的脚本除外）。对于此类进程，“应用程序启动控制”任务将应用当前配置定义的操作。“应用程序启动控制规则生成器”任务会检测应用程序启动，并为在 Linux 的 Windows 子系统下运行的应用程序生成相应规则。

关于应用程序启动控制规则

应用程序启动控制规则的工作原理

应用程序启动控制规则的操作基于以下组件：

- 规则类型。

  应用程序启动控制规则可以允许或拒绝应用程序启动。相应地，它们被称为*允许*或*拒绝*规则。要为“应用程序启动控制”创建允许规则列表，可以使用规则生成器生成允许规则或在“**仅统计**”模式下使用“应用程序启动控制”任务。您也可以手动添加允许规则。

- 用户和/或用户组。

  应用程序启动控制规则可以按用户或用户组控制指定应用程序的启动。

- 规则使用范围。

  应用程序启动控制规则可应用于*可执行文件*、*脚本*和 *MSI 安装包*。

- 规则触发条件。

  应用程序启动控制规则会控制满足规则设置中指定的一个或多个标准的文件的启动：由指定*数字证书*签名、匹配指定 *SHA256 哈希*、位于指定*路径*和匹配指定*命令行*参数。您应该选择至少一个选项。否则不会添加应用程序启动控制规则。

  如果将“**数字证书**”设置为规则触发条件，则创建的规则会控制操作系统中所有受信任应用程序的启动。您可通过选中以下复选框为此条件设置更加严格的条件：

  - 使用主题
  - 使用指纹

  > 指纹最严格地限制了基于数字证书的应用程序启动规则的触发，因为指纹唯一标识了数字证书且无法伪造，这一点与数字证书的主题不同。

您可以指定应用程序启动控制规则的排除。应用程序启动控制规则的排除基于用于触发规则的相同条件：数字证书、SHA256 哈希和文件路径。对于某些允许规则时，可能需要指定应用程序启动控制规则的排除：例如，如果您希望允许用户从 C:\Windows 路径启动应用程序，同时阻止启动文件 Regedit.exe。

> 如果操作系统文件在“应用程序启动控制”任务的范围内，建议在创建应用程序启动控制规则时确保新创建的规则允许此类应用程序。否则，操作系统可能无法启动。

管理应用程序启动控制规则

您可以对应用程序启动控制规则执行以下操作：

- 手动添加规则。

- 自动生成和添加规则。
- 删除规则。
- 将规则导出到文件。
- 检查所选文件是否存在允许执行这些文件的规则。
- 根据指定的条件筛选列表中的规则。

关于软件分发控制

如果您还需要控制受保护设备（例如，所安装软件会定期自动更新的受保护设备）上的软件分发，则应用程序启动控制规则生成器可能很复杂。在这种情况下，必须在每次软件更新后更新允许规则的列表，以便在“应用程序启动控制”任务设置中考虑新创建的文件。为了简化软件分发方案中的启动控制，可以使用“软件分发控制”子系统。

软件分发包（下文称为“软件包”）表示要在受保护设备上安装的软件应用程序。每个软件包都包含至少一个应用程序，除了应用程序外，可能还包含单个文件、更新，甚至单个命令，尤其是在您安装软件应用程序或更新时。

“软件分发控制”子系统作为附加排除列表实施。将软件分发包添加到此列表时，应用程序允许解压缩这些受信任包，并允许受信任包所安装或修改的软件自动启动。提取的文件可以继承主分发包的受信任属性。*主分发包*是由用户添加到软件分发控制排除列表并成为受信任包的软件包。

Kaspersky Embedded Systems Security 仅控制完整软件分发周期。如果第一次启动受信任包时软件分发控制关闭，或者“应用程序启动控制”组件未安装，应用程序将无法正确处理由受信任包修改的文件的启动。

如果在“应用程序启动控制”任务设置中清除“**将规则应用于可执行文件**”复选框，软件分发控制将不可用。

软件分发缓存

Kaspersky Embedded Systems Security 使用动态生成的软件分发缓存（“分发缓存”）在受信任包与软件分发期间创建的文件之间建立关系。第一次启动软件包时，Kaspersky Embedded Systems Security 将检测该软件包在软件分发过程中创建的所有文件，并将文件校验和及路径存储在分发缓存中。然后默认允许分发缓存中的所有文件启动。

您不能通过用户界面查看、清除或手动修改分发缓存。缓存由 Kaspersky Embedded Systems Security 填充和控制。

您可以将分发缓存导出到配置文件（XML 格式），同时使用命令行选项清除缓存。

要将分发缓存导出到配置文件，请执行以下命令：

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

要清除分发缓存，请执行以下命令：

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security 每 24 小时更新一次分发缓存。如果先前允许的文件的校验和发生变化，应用程序将从分发缓存中删除此文件的记录。如果“应用程序启动控制”任务在活动模式下启动，后续启动该文件的尝试将被阻止。如果先前允许的文件的完整路径发生变化，后续启动该文件的尝试不会被阻止，因为校验和存储在分发缓存内。

处理提取的文件

第一次启动软件包时，从受信任软件包提取的所有文件都会继承受信任属性。如果在第一次启动后清除该复选框，从软件包提取的所有文件都将保留继承的属性。要重置所有提取文件中的继承属性，您需要在再次启动受信任分发包之前清除分发缓存并清除“**允许进一步分发通过此分发包创建的程序**”复选框。

在第一次打开排除列表中的软件分发包时，受信任的主分发包所创建的提取文件和包会在它们的校验和被添加到分发缓存时继承受信任属性。因此，分发包本身和从该分发包提取的所有文件也将被信任。默认情况下，受信任属性的继承级别数是无限制的。

操作系统重新启动后，提取的文件将保留受信任属性。

文件处理在“软件分发控制”设置中通过选中或清除“**允许进一步分发通过此分发包创建的程序**”复选框来进行配置。

例如，假设您将包含几个其他包和应用程序的 test.msi 包添加到排除列表中并选中该复选框。在这种情况下，将允许运行或提取 test.msi 包中包含的所有包和应用程序（如果它们包含其他文件）。此方案适用于所有嵌套级别上的提取文件。

如果将 test.msi 包添加到排除列表中并清除“**允许进一步分发通过此分发包创建的程序**”复选框，应用程序只会将受信任属性分配到直接从主受信任包提取的包和可执行文件（在第一个嵌套级别上）。此类文件的校验和存储在分发缓存中。在第二个和更后面的嵌套级别上的所有文件都将被“默认拒绝”原则阻止。

使用应用程序启动控制规则列表

软件分发控制子系统的受信任包列表是一个排除项列表，该列表扩大了但未替换应用程序启动控制规则列表。

拒绝应用程序启动控制规则具有最高优先级：受信任包的解压缩和新文件或已修改文件的启动将被阻止（如果这些包和文件受应用程序启动控制拒绝规则影响）。

软件分发控制排除项适用于受信任包和这些包创建或修改的文件（如果应用程序启动控制列表中没有拒绝规则适用于这些包和文件）。

使用 KSN 结论

KSN 的文件不受信任的结论具有比软件分发控制排除项更高的优先级：如果 KSN 报告受信任包创建过修改的文件不受信任，则受信任包的解压缩和这些文件的启动都将被阻止。

而且，在从受信任包解压缩后，所有子文件都将被允许运行，不管是否在应用程序启动控制范围内使用 KSN。此时，“**拒绝 KSN 不信任的应用程序**”和“**允许 KSN 信任的应用程序**”复选框的状态不影响“**允许进一步分发通过此分发包创建的程序**”复选框的操作。

关于“应用程序启动控制”任务的 KSN 使用

要启动“KSN 使用”任务，您必须接受 KSN 声明。

如果有关某个应用程序声誉的 KSN 数据被“应用程序启动控制”任务使用，则 KSN 应用程序声誉将被视为允许或拒绝该应用程序启动的条件。如果 KSN 在用户尝试启动某个应用程序时向 Kaspersky Embedded Systems Security 报告该应用程序不受信任，应用程序启动将被拒绝。如果 KSN 在用户尝试启动某个应用程序时向 Kaspersky Embedded Systems Security 报告该应用程序受信任，应用程序启动将被允许。KSN 可与应用程序启动控制规则一起使用，或作为拒绝应用程序启动的独立条件。

使用 KSN 结论作为拒绝应用程序启动的独立条件

此方案允许在受保护设备上安全地控制应用程序启动，而无需对规则列表进行高级配置。

您可以将 KSN 结论连同唯一指定的规则一起应用于 Kaspersky Embedded Systems Security。该应用程序将仅允许启动 KSN 中信任的或指定规则允许的应用程序。

对于此类方案，推荐设置一条根据数字证书允许应用程序启动的规则。

按照“默认拒绝”策略，将拒绝所有其他应用程序。当没有应用任何规则时，使用 KSN 来保护设备免受 KSN 认为会造成威胁的应用程序的侵害。

与应用程序启动控制规则一起应用 KSN 结论

将 KSN 结论与应用程序启动控制规则同时使用时，以下条件适用：

- 如果某个应用程序包括在至少一条拒绝规则的范围内，Kaspersky Embedded Systems Security 将始终拒绝该应用程序的启动。如果应用程序被视为受 KSN 信任，则相应结论具有较低优先级且不被考虑；仍将拒绝应用程序启动。这允许您扩展阻止的应用程序列表。
- 如果禁止启动在 KSN 中不受信任的应用程序并且某个应用程序在 KSN 中不受信任，则 Kaspersky Embedded Systems Security 将始终拒绝该应用程序启动。如果为应用程序设置了允许规则，则此规则具有较低优先级且不被考虑；仍将拒绝应用程序启动。这样可以保护设备免受被 KSN 视为威胁（但在首次配置规则时未被考虑）的应用程序的侵害。

关于应用程序启动控制规则生成

您可使用 Kaspersky Security Center 任务和策略同时为公司网络上的所有受保护设备和受保护设备组创建应用程序启动控制规则列表。如果公司网络没有参考计算机，并且您无法基于模板机上安装的应用程序创建允许规则列表，则建议使用下面列出的方案。

您可以通过应用程序控制台在本地运行“应用程序启动控制规则生成器”任务，以基于单台受保护设备上运行的应用程序创建规则列表。

“应用程序启动控制”组件安装后具有两条预设的允许规则：

- 针对操作系统信任的脚本和带证书的 Windows Installer 软件包的允许规则。
- 针对操作系统信任的带证书的可执行文件的允许规则。

您可以使用以下方式之一在 Kaspersky Security Center 一侧创建应用程序启动控制规则列表：

- 使用“应用程序启动控制规则生成器”组任务。

在此方案下，一个组任务会为网络上的每台受保护设备生成其自己的应用程序启动控制规则列表，并将这些列表保存到指定共享文件夹中的 XML 文件。“应用程序启动控制规则生成器”任务生成的 XML 文件包含任务启动前任务设置中指定的允许规则。不会为指定任务设置中不允许启动的应用程序创建任何规则。默认情况下将拒绝此类应用程序启动。然后，您可将创建的规则列表手动导入 Kaspersky Security Center 策略的“应用程序启动控制”任务。

您可将生成的规则配置为自动导入“应用程序启动控制”任务的规则列表中。

当您需要快速创建应用程序启动控制规则列表时，推荐使用此方案。建议仅当应用的允许规则包含您知道安全的文件夹和文件时，才配置“应用程序启动控制规则生成器”任务的计划启动。

在网络中使用“应用程序启动控制”任务之前，请确保所有受保护设备都能够访问共享文件夹。如果组织的策略未规定使用网络中的共享文件夹，建议在测试受保护设备组中的受保护设备或模板机上启动“应用程序启动控制规则生成器”任务。

- 基于在“**仅统计**”模式下运行的“应用程序启动控制”任务在 Kaspersky Security Center 中生成的任务事件报告。

  在此方案下，Kaspersky Embedded Systems Security 不拒绝应用程序启动。相反，当“应用程序启动控制”在“**仅统计**”模式下运行时，它会在 Kaspersky Security Center 中的管理服务器节点的工作区的“**事件**”选项卡中报告所有网络受保护设备中所有已允许和已拒绝的应用程序启动。Kaspersky Security Center 使用报告来生成一个拒绝了应用程序启动的事件列表。

  您需要配置任务执行期限，以便在指定时间期限内执行所有可能的涉及受保护设备和受保护设备组的方案以及至少一次受保护设备重新启动。任务执行期限结束后，您可从保存的 Kaspersky Security Center 事件报告（TXT 格式）导入应用程序启动数据，并基于该数据为此类应用程序生成应用程序启动控制允许规则。

  如果公司网络包含大量不同类型的受保护设备（安装了不同的软件），则推荐使用此方案。

- 根据通过 Kaspersky Security Center 接收到的拒绝应用程序启动事件，无需创建和导入配置文件。

  要使用此功能，必须在有效的 Kaspersky Security Center 策略下运行受保护设备上的应用程序启动控制任务。在本例中，受保护设备上的所有事件均被发送到管理服务器。

推荐当网络受保护设备上安装的应用程序集合更改时（例如，安装更新或重新安装操作系统时）更新规则列表。建议通过在测试管理组中的受保护设备上以“**仅统计**”模式运行“应用程序启动控制规则生成器”任务或“应用程序启动控制”任务来生成更新的规则列表。测试管理组包含在网络受保护设备上安装新的应用程序之前对这些应用程序的启动进行测试所需的受保护设备。

包含允许规则列表的 XML 文件基于在受保护设备上启动的任务分析创建。为了在生成规则列表时将网络上使用的所有应用程序考虑在内，建议在模板机上以“**仅统计**”模式启动“应用程序启动控制规则生成器”任务和“应用程序启动控制”任务。

在基于参考计算机上启动的应用程序生成允许规则之前，确保模板机是安全的，并且不包含任何恶意软件。

添加允许规则之前，请选择其中一个可用的规则应用模式。Kaspersky Security Center 策略规则列表将仅显示由策略指定的那些规则，与规则应用模式无关。本地规则列表包括所有已应用的规则 — 本地规则和通过策略添加的规则。

“应用程序启动控制”任务默认设置

默认情况下，“应用程序启动控制”任务具有下表所述的设置。您可以更改这些设置的值。

“应用程序启动控制”任务默认设置

设置	默认值	描述
任务模式	**仅统计**。该任务根据设置的规则记录拒绝的启动事件和允许的启动事件。应用程序启动实际不会被拒绝。	在生成最终规则列表后，您可以选择**"活动"**模式。
在此文件的所有后续启动中重复针对首次文件启动执行的操作	未应用	您可以为文件随后的所有启动重复执行该文件第一次启动时的操作。
在没有可执行的命令时拒绝命令解释器启动	未应用。	您可以在没有可执行的命令时拒绝命令行解释器启动。
规则管理	**将策略规则添加到本地规则**	可以选择将策略中指定的规则与受保护设备上的规则一起应用的模式。
规则使用范围	该任务控制可执行文件、脚本和 MSI 包的启动。该任务还监控 DLL 模块的加载。	您可以指定要使用规则控制其启动的文件类型。
KSN 使用	不使用 KSN 应用程序声誉数据。	在运行"应用程序启动控制"任务时，您可以使用 KSN 应用程序声誉数据。
自动允许通过所列应用程序和软件包分发软件	未应用。	可以使用安装程序和设置中指定的应用程序允许软件分发。默认情况下，仅允许使用 Windows Installer 来进行软件分发。
始终允许通过 Windows Installer 进行软件分发	已应用（仅当**"自动允许通过所列应用程序和软件包分发软件"**设置启用时可以更改）。	如果通过 Windows Installer 执行操作，您可允许任何软件安装或更新。
始终允许使用后台智能传输服务通过 SCCM 进行软件分发	未应用（仅当**"自动允许通过所列应用程序和软件包分发软件"**设置启用时可以更改）。	可以使用 System Center Configuration Manager 开启或关闭自动软件分发。
任务启动	不设置任务的首次启动计划。	"应用程序启动控制"任务不会在 Kaspersky Embedded Systems Security 启动时自动启动。您可以手动启动该任务或配置计划启动。

"应用程序启动控制规则生成器"任务的默认设置

设置	默认值	描述
允许规则名称前缀	与安装了 Kaspersky Embedded Systems Security 的受保护设备的名称相同。	您可以更改允许规则的名称前缀。
允许规则的使用范围	默认情况下，允许规则的范围包括以下文件类别： • 位于以下文件夹中的具有 EXE 扩展名的文件：C:\Windows、C:\Program Files (x86) 和 C:\Program Files • 存储在 C:\Windows 文件夹中的 MSI 安装包 • 存储在 C:\Windows 文件夹中的脚本	您可以通过添加或删除文件夹路径并指定将被自动生成的规则允许启动的文件类型来更改保护范围。您还可以在创建允许规则时忽略正在运行的应用程序。

	该任务还会为所有正在运行的应用程序创建规则，而不管其位置和格式。	
生成允许规则的条件	使用数字证书主题和指纹；为所有用户和用户组生成规则。	在生成允许规则时，可以使用 SHA256 哈希。 您可以选择需要为其自动生成允许规则的用户和用户组。
任务完成时的操作	允许规则添加到应用程序启动控制规则列表；新规则与现有规则合并；重复规则被删除。	您可以将规则添加到现有规则，而不进行合并和删除重复规则，或将现有规则替换为新的允许规则，或配置将允许规则导出到文件。
任务启动设置及权限	在系统账户下启动任务。	您可以允许“应用程序启动控制规则生成器”任务在系统账户下或使用指定用户的权限启动。
任务启动计划	不设置任务的首次启动计划。	“应用程序启动控制规则生成器”任务不会在 Kaspersky Embedded Systems Security 启动时自动启动。您可以手动启动该任务或配置计划启动。

通过管理插件管理应用程序启动控制

在本节中，学习如何导航管理插件界面，以及如何为网络中的一台或所有受保护设备配置任务设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开“应用程序启动控制”任务的策略设置

要通过 Kaspersky Security Center 策略打开“应用程序启动控制”任务设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在打开的“**属性：<策略名称>**”窗口中，选择“**本地活动控制**”部分。
6. 单击“**应用程序启动控制**”子部分中的“**设置**”按钮。
   将打开“**应用程序启动控制**”窗口。

根据需要配置策略。

打开应用程序启动控制规则列表

要通过 Kaspersky Security Center 打开应用程序启动控制规则列表：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在打开的“**属性：<策略名称>**”窗口中，选择“**本地活动控制**”部分。
6. 单击“**应用程序启动控制**”子部分中的“**设置**”按钮。
   将打开“**应用程序启动控制**”窗口。
7. 在“**常规**”选项卡上，单击“**规则列表**”按钮。
   将打开“**应用程序启动控制规则**”窗口。

根据需要配置规则列表。

打开“应用程序启动控制规则生成器”任务向导和属性

要开始创建“应用程序启动控制规则生成器”任务：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**任务**”选项卡。
4. 单击“**创建任务**”按钮。
   将打开“**新建任务向导**”窗口。
5. 选择“**应用程序启动控制规则生成器**”任务。
6. 单击“**下一步**”。
   将打开“**设置**”窗口。

要配置现有“应用程序启动控制规则生成器”任务：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**任务**”选项卡。

4. 双击 Kaspersky Security Center 任务列表中的任务名称。

   将打开“**属性：应用程序启动控制规则生成器**”窗口。

有关配置该任务的详细信息，请参见“配置‘应用程序启动控制规则生成器’任务”部分。

配置“应用程序启动控制”任务设置

要配置常规“应用程序启动控制”任务设置：

1. 打开“应用程序启动控制”窗口。
2. 在“**常规**”选项卡上，选择“**任务模式**”部分的以下设置：
   - 在“任务模式”下拉列表中，指定任务模式。
   - 清除或选中“在此文件的所有后续启动中重复针对首次文件启动执行的操作”复选框。
   - 清除或选中“在没有可执行的命令时拒绝命令解释器启动”复选框。
3. 在“**规则管理**”部分中，配置应用规则的设置：
   a. 单击“**规则列表**”按钮以添加“应用程序启动控制”任务的允许规则。

   > Kaspersky Embedded Systems Security 无法识别包含斜线“/”的路径。请使用反斜线“\”来正确输入路径。

   b. 选择应用规则的模式：
   - **使用策略规则替换本地规则**。

     应用程序将针对受保护设备组上的应用程序启动控制应用策略中指定的规则列表。不能创建、编辑或应用本地规则列表。
   - **将策略规则添加到本地规则**。

     应用程序将与本地规则列表一起应用策略中指定的规则列表。可以使用“应用程序启动控制规则生成器”任务编辑本地规则列表。
4. 在“**规则使用范围**”部分中，指定以下设置：
   - 将规则应用于可执行文件。
   - 监控 DLL 模块的加载。

     > 控制 DLL 模块的加载可能影响操作系统的性能。
   - 将规则应用于脚本和 MSI 数据包。
5. 在“**KSN 使用**”组框中，配置以下应用程序启动设置：
   - 拒绝 KSN 不信任的应用程序。

- 允许 KSN 信任的应用程序。
- 允许启动 KSN 中信任的应用程序的用户和/或用户组。

6. 在“**软件分发控制**”选项卡上，配置软件分发控制的设置。
7. 在“**任务管理**”选项卡上，配置计划的任务启动设置。
8. 在“**应用程序启动控制**”窗口中单击“**确定**”。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

配置软件分发控制

要添加受信任分发包：

1. 打开“**应用程序启动控制**”窗口。
2. 在“**软件分发控制**”选项卡上，选中“自动允许通过所列应用程序和软件包分发软件”复选框。

   如果在“**应用程序启动控制**”任务设置中选中“**常规**”选项卡中的“**将规则应用于可执行文件**”复选框，则您可选中“**自动允许通过所列应用程序和软件包分发软件**”。

3. 根据需要清除“始终允许通过 Windows Installer 进行软件分发”复选框。

   仅当在绝对必要时才推荐清除“**始终允许通过 Windows Installer 进行软件分发**”复选框。关闭此功能可能导致更新操作系统文件出问题，还可能阻止从分发包中提取的文件启动。

4. 如果需要，请选中“始终允许使用后台智能传输服务通过 SCCM 进行软件分发”复选框。

   应用程序控制受保护设备上从软件包传送到安装或更新的软件分发周期。如果在受保护设备上安装应用程序之前已执行分发的任何阶段，则应用程序不会控制过程。

5. 要创建允许列表或编辑受信任分发包的现有列表，请单击“**更改分发包列表**”，然后在出现的窗口中选择以下方法之一：
   - **添加一个分发包**。
     a. 单击“**浏览**”按钮。
     b. 选择可执行文件或分发包。
     “**信任条件**”部分会使用有关选定文件的数据自动进行填充。
     c. 清除或选中“**允许进一步分发通过此分发包创建的程序**”复选框。
     d. 选择两个可用条件选项中的一个，用于决定文件或分发包是否受信任：
     - **使用数字证书**

- 使用 SHA256 哈希

- **按哈希添加多个分发包**。

  您可以选择无限数量的可执行文件和分发包，并同时将它们添加到列表。Kaspersky Embedded Systems Security 将检查哈希并允许操作系统启动指定的文件。

- **更改选定的分发包**。
  使用此选项可以选择不同的可执行文件或分发包，或更改信任条件。

- 从文件导入分发包列表。
  在“**打开**”窗口中，指定包含受信任分发包列表的配置文件。

6. 如果要删除受信任列表中以前添加的应用程序或分发包，请单击“**删除分发包**”按钮。将允许运行提取的文件。

   要阻止提取的文件启动，请在受保护设备上卸载应用程序，或在应用程序启动控制任务设置中创建拒绝规则。

7. 单击“**确定**”。

将保存新配置的设置。

配置“应用程序启动控制规则生成器”任务

要配置“应用程序启动控制规则生成器”任务：

1. 打开“属性：应用程序启动控制规则生成器”窗口。
2. 在“**通知**”部分中，配置任务事件通知设置。

   关于此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

3. 在“**设置**”部分中，您可配置以下设置：
   - 为规则名称添加前缀。
   - 选择如何创建允许规则：
     - 基于正在运行的应用程序创建允许规则
     - 为以下文件夹中的应用程序创建允许规则
4. 在“**选项**”部分中，可以指定在创建应用程序启动控制允许规则时执行的操作：
   - 使用数字证书
   - 使用数字证书主题和指纹
   - 证书丢失则使用

- **SHA256 哈希**。将用于生成规则的文件的校验和设置为触发应用程序启动控制允许规则的条件。应用程序将允许启动使用带指定校验和的文件启动的程序。
- **文件路径**。将用于生成规则的文件的路径设置为触发应用程序启动控制允许规则的条件。此时，应用程序将允许启动使用位于“**设置**”部分的“**为以下文件夹中的应用程序创建允许规则**”表中指定的文件夹中的文件启动的程序。

- 使用 SHA256 哈希
- 为用户或用户组生成规则。

您可以使用 Kaspersky Embedded Systems Security 在任务完成时创建的允许规则列表为配置文件配置设置。

5. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。
6. 在“**账户**”部分中，指定将使用其权限运行任务的账户。
7. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。

> 有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

8. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。
   将保存新配置的组任务设置。

通过 Kaspersky Security Center 配置应用程序启动控制规则

了解如何使用“应用程序启动控制”任务根据各种条件生成规则列表，或手动创建允许或拒绝规则。

添加应用程序启动控制规则

要添加应用程序启动控制规则：

1. 打开“应用程序启动控制规则”窗口。
2. 单击“**添加**”按钮。
3. 在按钮的上下文菜单中，选择“**添加一项规则**”。
   将打开“**规则设置**”窗口。
4. 指定以下设置：
   a. 在“**名称**”字段中，输入规则的名称。
   b. 在“**类型**”下拉列表中，选择规则类型：
      - **允许**，如果您希望规则根据规则设置中指定的条件允许应用程序启动。
      - **拒绝**，如果您希望规则根据规则设置中指定的条件阻止应用程序启动。

c. 在“**范围**”下拉列表中，选择将由规则控制执行的文件类型：

- **可执行文件**，如果您希望规则控制可执行文件的启动。
- **脚本和 MSI 数据包**，如果希望规则控制脚本和 MSI 数据包的启动。

d. 在“**用户或用户组**”字段中，指定根据规则类型将允许或不允许启动程序的用户。为此，请执行以下操作：

1. 单击“**浏览**”按钮。
2. 将打开标准 Microsoft Windows“**选择用户或组**”窗口。
3. 指定用户和/或用户组列表。
4. 单击“**确定**”。

e. 如果您希望从特定文件获取“**规则触发条件**”部分中列出的规则触发条件的值：

1. 单击“**从文件属性设置规则触发条件**”按钮。
   将打开标准 Microsoft Windows“**打开**”窗口。
2. 选择文件。
3. 单击“**打开**”按钮。
   文件中的条件值显示在“**规则触发条件**”组框的字段中。默认选择文件属性中提供有其数据的条件。

f. 在“**规则触发条件**”组框中，根据需要选择以下一个或多个选项：

- **数字证书**，如果您希望规则控制使用数字证书签名的文件启动的应用程序的启动：
  - 如果您希望规则控制由仅具有指定标题的数字证书签名的文件的启动，请选中“**使用主题**”复选框。
  - 如果您希望规则仅控制使用具有指定指纹的数字证书签名的文件的启动，请选中“**使用指纹**”复选框。
- **SHA256 哈希**，如果您希望规则控制使用其校验和与指定值匹配的文件启动的程序的启动。
- **文件路径**，如果您希望规则控制使用位于指定路径的文件启动的程序的启动。
  - **命令行**，如果您希望规则能控制使用命令行字段中指定的参数启动的程序的启动。选择“**文件路径**”选项后，该字段将启用。将已启动进程的命令行参数指定为条件时，您可以使用 ? 和 * 字符作为掩码。

  > Kaspersky Embedded Systems Security 无法识别包含斜线“/”的路径。请使用反斜线“\”来正确输入路径。

  > 指定对象时，可以使用 ? 和 * 字符作为文件掩码。

您应该选择至少一个选项。否则不会添加应用程序启动控制规则。

g. 如果希望添加规则排除：

1. 在“从规则排除”部分中，单击“添加”按钮。

   将打开“从规则排除”窗口。

2. 在“名称”字段中，输入排除项的名称。

3. 指定从应用程序启动控制规则中排除应用程序文件的设置。可单击“基于文件属性设置排除”按钮从文件属性填充设置字段。

   - 数字证书
   - 使用主题
   - 使用指纹
   - SHA256 哈希
   - 文件路径

4. 单击“确定”。

5. 如有必要，重复步骤 (i)-(iv) 以添加更多排除。

5. 在“规则设置”窗口中单击“确定”。

创建的规则显示在“应用程序启动控制规则”窗口中的列表中。

启用默认允许模式

“默认允许”模式允许所有应用程序启动，只要它们未被规则或被 KSN 的不受信任结论阻止。可以通过添加特定允许规则来启用默认允许模式。您可以仅为脚本或为所有可执行文件启用“默认允许”模式。

要添加默认允许规则：

1. 打开“应用程序启动控制规则”窗口。

2. 单击“添加”按钮，然后在该按钮的上下文菜单中选择“添加一项规则”。

   将打开“规则设置”窗口。

3. 在“名称”字段中，输入规则的名称。

4. 在“类型”下拉列表中，选择“允许”规则类型。

5. 在“范围”下拉列表中，选择将由规则控制执行的文件类型：

   - **可执行文件**，如果希望规则控制可执行文件的启动。
   - **脚本和 MSI 数据包**，如果希望规则控制脚本和 MSI 数据包的启动。

6. 在“规则触发条件”组框中，选择“文件路径”选项。

7. 输入以下掩码：`?:\`

8. 在“规则设置”窗口中单击“确定”。

Kaspersky Embedded Systems Security 将应用默认允许模式。

从 Kaspersky Security Center 事件创建允许规则

要在"应用程序启动控制"中从 Kaspersky Security Center 事件为应用程序创建允许规则：

1. 打开"应用程序启动控制规则"窗口。
2. 单击"**添加**"按钮，然后在该按钮的上下文菜单中选择"**从 Kaspersky Security Center 事件为应用程序创建允许规则**"。
3. 选择将规则添加到先前创建的应用程序启动控制规则列表中的原则：
   - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
   - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
   - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。

   将打开"**生成应用程序启动控制规则**"窗口。
4. 选择您希望规则生成任务使用的事件类型：
   - **仅统计模式: 应用程序启动被拒绝**。
   - **应用程序启动被拒绝**。
5. 从"**请求在以下期间内生成的事件**"下拉列表中选择时间段。
6. 选中或清除"生成规则时优先考虑使用哈希"复选框。

   如果选中此复选框，则当文件的校验和与证书均可用时，Kaspersky Embedded Systems Security 将使用文件的校验和来生成规则。

   如果清除此复选框，则当文件的校验和与证书均可用时，Kaspersky Embedded Systems Security 将使用文件的数字证书来生成规则。
7. 单击"**生成规则**"按钮。
8. 单击"**应用程序启动控制规则**"窗口中的"**保存**"按钮。

   将使用基于安装了 Kaspersky Security Center 管理控制台的受保护设备的系统数据生成的新规则填充"应用程序启动控制"任务中的规则列表。

   如果策略中已指定应用程序启动控制规则列表，则 Kaspersky Embedded Systems Security 将从阻止事件中添加选定的规则到已指定的规则。不添加具有相同哈希的规则，因为列表中的所有规则都必须是唯一的。

从有关受阻止应用程序的 Kaspersky Security Center 报告中导入规则

您可从在“仅统计”模式下运行“应用程序启动控制”任务后 Kaspersky Security Center 中生成的报告导入有关受阻止应用程序启动的数据，并使用此数据在所配置策略中生成应用程序启动控制允许规则列表。

生成有关“应用程序启动控制”任务期间发生的事件的报告后，您可以跟踪被阻止启动的应用程序。

将数据从有关受阻止应用程序的报告导入到策略设置时，确保您所使用的列表仅包含您希望允许启动的应用程序。

要根据 Kaspersky Security Center 中的受阻止应用程序报告为一组受保护设备指定应用程序启动控制允许规则：

1. 打开“应用程序启动控制”窗口。
2. 在“任务模式”部分中，选择“仅统计”模式。
3. 在“事件通知”部分中的策略属性中，确保：
   - 对于关键事件，应用程序启动被拒绝事件的任务日志保留期超过以“仅统计”模式运行任务的计划期（默认值为 30 天）。
   - 对于重要性级别为“警告”的事件，仅统计模式: 应用程序启动被拒绝事件的任务日志保留期超过以“仅统计”模式运行任务的计划期（默认值为 30 天）。

     当事件保留期过后，有关记录的事件的信息会被删除且不会反映在报告文件中。在“仅统计”模式下运行“应用程序启动控制”任务之前，确保任务运行时间不超过为指定事件配置的时间段。
4. 当任务完成后，将记录的事件导出到 TXT 文件：
   a. 在 Kaspersky Security Center 中的“管理服务器”节点的工作区中，选择“事件”选项卡。
   b. 单击“创建选择”按钮以基于“阻止”条件创建一系列事件，以查看“应用程序启动控制”任务将阻止启动的应用程序。
   c. 在所选项的结果窗格中，单击“将事件导出到文件”以将受阻止应用程序启动报告保存到 TXT 文件。

   在策略中导入和应用生成的报告之前，确保报告仅包含有关您希望允许启动的应用程序的数据。
5. 将有关受阻止应用程序启动的数据导入到应用程序启动控制任务。为此，在策略属性的“应用程序启动控制”任务设置中：
   a. 在“常规”选项卡上，单击“规则列表”按钮。
   将打开“应用程序启动控制规则”窗口。
   b. 单击“添加”按钮，然后在该按钮的上下文菜单中选择“从 Kaspersky Security Center 报告导入阻止的应用程序的数据”。
   c. 选择将来自根据 Kaspersky Security Center 报告创建的列表的规则添加到先前配置的应用程序启动控制规则列表的原则：
      - 添加到现有规则，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
      - 替换现有规则，如果您希望将现有规则替换为导入的规则。

- **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。

d. 在打开的标准 Microsoft Windows 窗口中，选择已将来自受阻止应用程序启动报告的事件导出到的 TXT 文件。

e. 单击“**应用程序启动控制规则**”窗口中的“**保存**”。

根据有关受阻止应用程序的 Kaspersky Security Center 报告创建的规则将被添加到应用程序启动控制规则列表。

从 XML 文件导入应用程序启动控制规则

您可导入由“应用程序启动控制规则生成器”组任务生成的报告，并将它们作为允许规则列表应用于所配置的策略中。

当“应用程序启动控制规则生成器”组任务完成后，应用程序会将创建的允许规则导入指定的共享文件夹中保存的 XML 文件。包含规则列表的每个文件通过对公司网络中每台单独受保护设备上执行的文件和启动的应用程序进行分析所创建。这些列表包含类型与“应用程序启动控制规则生成器”组任务中指定的类型匹配的文件和应用程序的允许规则。

要根据自动生成的允许规则列表为一组受保护设备指定应用程序启动控制允许规则：

1. 在所配置受保护设备组的详细信息窗格中的“**任务**”选项卡上，创建一个“应用程序启动控制规则生成器”组任务或选择一个现有任务。

2. 在创建的“应用程序启动控制规则生成器”组任务的属性中或在任务向导中，指定以下设置：

   - 在“**通知**”部分中，配置用于保存任务执行报告的设置。

     有关此节中配置设置的详细说明，请参见 *Kaspersky Security Center 帮助*。

   - 在“**设置**”部分中，指定所创建规则将允许启动的应用程序类型。您可编辑包含允许的应用程序的文件夹集合：从任务范围排除默认文件夹或手动添加新文件夹。

   - 在“**选项**”部分中，指定任务在运行时及完成后执行的操作。指定规则生成条件和生成的规则将导出到的文件的名称。

   - 在“**计划**”部分中配置任务启动计划设置。

   - 在“**账户**”部分中，指定将用于执行任务的用户账户。

   - 在“**任务范围的排除项**”部分中，指定要从任务范围排除的受保护设备组。

     Kaspersky Embedded Systems Security 不会为在排除的受保护设备上启动的应用程序创建允许规则。

3. 在所配置受保护设备组的详细信息窗格上的“**任务**”选项卡上，从组任务列表中选择您已创建的“应用程序启动控制规则生成器”任务，然后单击“**启动**”按钮启动任务。

   任务完成后，自动生成的允许规则列表将保存在共享文件夹中的 XML 文件中。

在网络中使用“应用程序启动控制”任务之前，请确保所有受保护设备都能够访问共享文件夹。如果组织的策略未规定使用网络中的共享文件夹，建议在测试受保护设备组中的受保护设备或参考计算机上启动“应用程序启动控制规则生成器”任务。

4. 要将生成的允许规则列表添加到“应用程序启动控制”任务：

   a. 打开“应用程序启动控制规则”窗口。

   b. 单击“**添加**”按钮，然后在打开的列表中选择“**从 XML 文件导入规则**”。

   c. 选择将自动生成的允许规则添加到先前创建的应用程序启动控制规则列表中的原则：

   - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
   - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
   - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。

   d. 在打开的标准 Microsoft Windows 窗口中，选择“应用程序启动控制规则生成器”组任务完成后创建的 XML 文件。

   e. 单击“**应用程序启动控制规则**”窗口中的“**保存**”。

5. 如果您希望将创建的规则应用于控制应用程序启动，则在策略中的“应用程序启动控制”任务属性中，为任务选择“**活动**”模式。

基于每台单独的受保护设备上的任务运行自动生成的允许规则将被应用于所配置策略涵盖的所有网络受保护设备。在这些受保护设备上，应用程序将允许仅启动已为其创建允许规则的这些应用程序。

检查应用程序启动

在应用所配置的应用程序启动控制规则前，您可以测试任何应用程序以确定该应用程序会触发哪些应用程序启动控制规则。

默认情况下，Kaspersky Embedded Systems Security 将拒绝启动不被单个规则允许启动的应用程序。为避免拒绝启动重要的应用程序，您需要为它们创建允许规则。

如果某个应用程序的启动受多条不同类型的规则控制，拒绝规则将优先：即使应用程序只在一条拒绝规则下，也将拒绝该应用程序启动。

要测试应用程序启动控制规则：

1. 打开“应用程序启动控制规则”窗口。
2. 在打开的窗口中，单击“**显示文件规则**”按钮。

   将打开标准的 Microsoft Windows 窗口。
3. 选择要测试其启动控制的文件。

指定文件的路径显示在搜索字段中。列表包含在启动所选文件时将触发的所有规则。

创建“应用程序启动控制规则生成器”任务

要创建和配置“应用程序启动控制规则生成器”任务设置：

1. 打开“新建任务向导”中的“**设置**”窗口。
2. 进行以下配置：
   - 指定规则名称前缀。
   - 配置允许规则使用范围。
3. 单击“**下一步**”。
4. 指定 Kaspersky Embedded Systems Security 必须执行的操作：
   - 生成允许规则时。
   - 任务完成后。
5. 在“**计划**”窗口中，设置计划的任务启动设置。
6. 单击“**下一步**”。
7. 在“**选择账户以运行任务**”窗口中，指定要使用的账户。
8. 单击“**下一步**”。
9. 指定任务名称。
10. 单击“**下一步**”。

    任务名称不应超过 100 个字符，并且不能包含以下符号：" * < > & \ : |

    将打开“**完成创建任务**”窗口。
11. 您可以通过选中“**向导完成后运行任务**”复选框来在向导完成后运行任务。
12. 单击“**完成**”完成创建任务。

要在 Kaspersky Security Center 中配置现有规则，

打开“**属性：应用程序启动控制规则生成器**”窗口并调整上述设置。

有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

限制任务使用范围

要限制"应用程序启动控制规则生成器"任务的范围：

1. 打开"属性：应用程序启动控制规则生成器"窗口。
2. 选择如何创建允许规则：
   - 基于正在运行的应用程序创建允许规则
   - 为以下文件夹中的应用程序创建允许规则
3. 单击"确定"。

将保存指定设置。

自动规则生成期间要执行的操作

要配置在"应用程序启动控制规则生成器"任务运行期间 Kaspersky Embedded Systems Security 要执行的操作：

1. 打开"属性：应用程序启动控制规则生成器"窗口。
2. 打开"选项"选项卡。
3. 在"生成允许规则时"部分中，配置以下设置：
   - 使用数字证书
   - 使用数字证书主题和指纹
   - 证书丢失则使用
     - **SHA256 哈希**。将用于生成规则的文件的校验和设置为触发应用程序启动控制允许规则的条件。应用程序将允许启动使用带指定校验和的文件启动的程序。
     - **文件路径**。将用于生成规则的文件的路径设置为触发应用程序启动控制允许规则的条件。此时，应用程序将允许启动使用位于"**设置**"部分的"**为以下文件夹中的应用程序创建允许规则**"表中指定的文件夹中的文件启动的程序。
   - 使用 SHA256 哈希
   - 为用户或用户组生成规则。
4. 单击"确定"。

将保存指定设置。

自动规则生成完成后要执行的操作

要配置在"应用程序启动控制规则生成器"任务完成后 Kaspersky Embedded Systems Security 要执行的操作：

1. 打开"属性：应用程序启动控制规则生成器"窗口。
2. 打开"选项"选项卡。

3. 在“**任务完成后**”部分中，配置以下设置：
   - 将允许规则添加到应用程序启动控制规则列表。
   - 添加原则。
   - **将允许规则导出到文件**。
   - 将受保护设备详细信息添加到文件名。
4. 单击“**确定**”。

将保存指定设置。

通过应用程序控制台管理应用程序启动控制

在本节中，学习如何导航应用程序控制台界面以及如何在受保护设备上配置任务设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开“应用程序启动控制”任务设置

要通过应用程序控制台打开“应用程序启动控制”常规任务设置：

1. 在应用程序控制台树中，展开“**计算机控制**”节点。
2. 选择“**应用程序启动控制**”子节点。
3. 在“**应用程序启动控制**”子节点的详细信息窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。

打开应用程序启动控制规则窗口

要通过应用程序控制台打开应用程序启动控制规则列表：

1. 在应用程序控制台树中，展开“**计算机控制**”节点。
2. 选择“**应用程序启动控制**”子节点。
3. 在“**应用程序启动控制**”节点的结果窗格中，单击“**应用程序启动控制规则**”链接。
   将打开“**应用程序启动控制规则**”窗口。
4. 根据需要配置规则列表。

打开“应用程序启动控制规则生成器”任务设置

要配置“应用程序启动控制规则生成器”任务：

1. 在应用程序控制台树中，展开“**自动规则生成器**”节点。
2. 选择“**应用程序启动控制规则生成器**”子节点。
3. 在“**应用程序启动控制规则生成器**”子节点的结果窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。
4. 根据需要配置任务。

配置“应用程序启动控制”任务设置

要配置常规“应用程序启动控制”任务设置：

1. 打开“**任务设置**”窗口。
2. 配置以下任务设置：
   - 在“**常规**”选项卡上：
     - “应用程序启动控制”任务模式。
     - 任务中的规则使用范围。
     - KSN 使用。
   - “**软件分发控制**”选项卡上的软件分发控制设置。
   - “**计划**”和“**高级**”选项卡上的任务启动计划设置。
3. 在“**任务设置**”窗口中单击“**确定**”。
   将保存修改的设置。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

选择“应用程序启动控制”任务的模式

要配置“应用程序启动控制”任务的模式：

1. 打开“**任务设置**”窗口。
2. 在“**常规**”选项卡上的“任务模式”下拉列表中，指定任务模式。

3. 清除或选中“在此文件的所有后续启动中重复针对首次文件启动执行的操作”复选框。

每次修改“应用程序启动控制”任务设置后，Kaspersky Embedded Systems Security 都会创建一个新的缓存事件列表。这意味着“应用程序启动控制”按照当前安全设置执行。

4. 清除或选中“在没有可执行的命令时拒绝命令解释器启动”。

5. 在“**任务设置**”窗口中单击“**确定**”。

将保存指定设置。

所有启动应用程序的尝试都将记录在任务日志中。

配置“应用程序启动控制”任务的范围

要定义“应用程序启动控制”任务的范围：

1. 打开“任务设置”窗口。

2. 在“**常规**”选项卡上的“**规则使用范围**”部分中，指定以下设置：

- 将规则应用于可执行文件
- 监控 DLL 模块的加载

  控制 DLL 模块的加载可能影响操作系统的性能。

- 将规则应用于脚本和 MSI 数据包

3. 在“**任务设置**”窗口中单击“**确定**”。

将保存指定设置。

配置 KSN 使用

要配置“应用程序启动控制”任务的 KSN 服务的使用：

1. 打开“任务设置”窗口。

2. 在“**常规**”选项卡上的“**KSN 使用**”部分中，指定 KSN 服务的使用设置：

- 如果必要，选中“拒绝 KSN 不信任的应用程序”复选框。
- 如果必要，请选中“允许 KSN 信任的应用程序”复选框。
- 如果选择了“**允许 KSN 信任的应用程序**”复选框，则请指定可以在 KSN 中启动应用程序的用户和/或用户组。为此，请执行以下操作：

a. 单击“**编辑**”按钮。

将打开标准的 Microsoft Windows“**选择用户或组**”窗口。

> 默认情况下，允许所有用户访问 KSN 中受信任的程序。

b. 指定用户和/或用户组列表。

c. 单击“**确定**”。

3. 在“**任务设置**”窗口中单击“**确定**”。

将保存指定设置。

软件分发控制

要添加受信任分发包：

1. 打开“任务设置”窗口。
2. 在“**软件分发控制**”选项卡上，选中“自动允许通过所列应用程序和软件包分发软件”复选框。

> 如果在“**应用程序启动控制**”任务设置中选中“**常规**”选项卡中的“**将规则应用于可执行文件**”复选框，则您可选中“**自动允许通过所列应用程序和软件包分发软件**”。

3. 根据需要清除“始终允许通过 Windows Installer 进行软件分发”复选框。

> 仅当在绝对必要时才推荐清除“**始终允许通过 Windows Installer 进行软件分发**”复选框。关闭此功能可能导致更新操作系统文件出问题，还可能阻止从分发包中提取的文件启动。

4. 如果需要，请选中“始终允许使用后台智能传输服务通过 SCCM 进行软件分发”复选框。

> 应用程序控制受保护设备上从软件包传送到安装或更新的软件分发周期。如果在受保护设备上安装应用程序之前已执行分发的任何阶段，则应用程序不会控制过程。

5. 要创建允许列表或编辑受信任分发包的现有列表，请单击“**更改分发包列表**”，然后在出现的窗口中选择以下方法之一：

- **添加一个分发包**。

a. 单击“**浏览**”按钮。

b. 选择可执行文件或分发包。

“**信任条件**”部分会使用有关选定文件的数据自动进行填充。

c. 清除或选中“**允许进一步分发通过此分发包创建的程序**”复选框。

d. 选择两个可用条件选项中的一个，用于决定文件或分发包是否受信任：

- 使用数字证书
- 使用 SHA256 哈希

- 按哈希添加多个分发包。

  您可以选择无限数量的可执行文件和分发包，并同时将它们添加到列表。Kaspersky Embedded Systems Security 将检查哈希并允许操作系统启动指定的文件。

- 更改选定的分发包。
  使用此选项可以选择不同的可执行文件或分发包，或更改信任条件。
- 从文件导入分发包列表。
  在“打开”窗口中，指定包含受信任分发包列表的配置文件。

6. 如果要删除受信任列表中以前添加的应用程序或分发包，请单击“删除分发包”按钮。将允许运行提取的文件。

   要阻止提取的文件启动，请在受保护设备上卸载应用程序，或在应用程序启动控制任务设置中创建拒绝规则。

7. 单击“确定”。

将保存新配置的设置。

配置应用程序启动控制规则

了解如何使用“应用程序启动控制”任务生成、导入和导出规则列表，或手动创建允许或拒绝规则。

添加应用程序启动控制规则

要添加应用程序启动控制规则：

1. 打开“应用程序启动控制规则”窗口。
2. 单击“添加”按钮。
3. 在按钮的上下文菜单中，选择“添加一项规则”。
   将打开“规则设置”窗口。
4. 指定以下设置：
   a. 在“名称”字段中，输入规则的名称。
   b. 在“类型”下拉列表中，选择规则类型：
      - 允许，如果您希望规则根据规则设置中指定的条件允许应用程序启动。
      - 拒绝，如果您希望规则根据规则设置中指定的条件阻止应用程序启动。

c. 在“**范围**”下拉列表中，选择将由规则控制执行的文件类型：

- **可执行文件**，如果您希望规则控制可执行文件的启动。
- **脚本和 MSI 数据包**，如果希望规则控制脚本和 MSI 数据包的启动。

d. 在“**用户或用户组**”字段中，指定根据规则类型将允许或不允许启动程序的用户。为此，请执行以下操作：

1. 单击“**浏览**”按钮。
2. 将打开标准 Microsoft Windows“**选择用户或组**”窗口。
3. 指定用户和/或用户组列表。
4. 单击“**确定**”。

e. 如果您希望从特定文件获取“**规则触发条件**”部分中列出的规则触发条件的值：

1. 单击“**从文件属性设置规则触发条件**”按钮。
   将打开标准 Microsoft Windows“**打开**”窗口。
2. 选择文件。
3. 单击“**打开**”按钮。
   文件中的条件值显示在“**规则触发条件**”组框的字段中。默认选择文件属性中提供有其数据的条件。

f. 在“**规则触发条件**”组框中，根据需要选择以下一个或多个选项：

- **数字证书**，如果您希望规则控制使用数字证书签名的文件启动的应用程序的启动：
  - 如果您希望规则控制由仅具有指定标题的数字证书签名的文件的启动，请选中“**使用主题**”复选框。
  - 如果您希望规则仅控制使用具有指定指纹的数字证书签名的文件的启动，请选中“**使用指纹**”复选框。
- **SHA256 哈希**，如果您希望规则控制使用其校验和与指定值匹配的文件启动的程序的启动。
- **文件路径**，如果您希望规则控制使用位于指定路径的文件启动的程序的启动。
  - **命令行**，如果您希望规则能控制使用命令行字段中指定的参数启动的程序的启动。选择“**文件路径**”选项后，该字段将启用。将已启动进程的命令行参数指定为条件时，您可以使用 ? 和 * 字符作为掩码。

> Kaspersky Embedded Systems Security 无法识别包含斜线“/”的路径。请使用反斜线“\”来正确输入路径。

> 指定对象时，可以使用 ? 和 * 字符作为文件掩码。

您应该选择至少一个选项。否则不会添加应用程序启动控制规则。

g. 如果希望添加规则排除：

1. 在“从规则排除”部分中，单击“添加”按钮。

   将打开“从规则排除”窗口。

2. 在“名称”字段中，输入排除项的名称。

3. 指定从应用程序启动控制规则中排除应用程序文件的设置。可单击“基于文件属性设置排除”按钮从文件属性填充设置字段。

   - 数字证书
   - 使用主题
   - 使用指纹
   - SHA256 哈希
   - 文件路径

4. 单击“确定”。

5. 如有必要，重复步骤 (i)-(iv) 以添加更多排除。

5. 在“规则设置”窗口中单击“确定”。

创建的规则显示在“应用程序启动控制规则”窗口中的列表中。

启用默认允许模式

“默认允许”模式允许所有应用程序启动，只要它们未被规则或被 KSN 的不受信任结论阻止。可以通过添加特定允许规则来启用默认允许模式。您可以仅为脚本或为所有可执行文件启用“默认允许”模式。

要添加默认允许规则：

1. 打开“应用程序启动控制规则”窗口。

2. 单击“添加”按钮。

3. 在按钮的上下文菜单中，选择“添加一项规则”。

   将打开“规则设置”窗口。

4. 在“名称”字段中，输入规则的名称。

5. 在“类型”下拉列表中，选择“允许”规则类型。

6. 在“范围”下拉列表中，选择将由规则控制执行的文件类型：

   - **可执行文件**，如果希望规则控制可执行文件的启动。
   - **脚本和 MSI 数据包**，如果希望规则控制脚本和 MSI 数据包的启动。

7. 在“规则触发条件”组框中，选择“文件路径”选项。

8. 输入以下掩码：`?:\`

9. 在“**规则设置**”窗口中单击“**确定**”。

Kaspersky Embedded Systems Security 将应用默认允许模式。

根据“应用程序启动控制”任务事件创建允许规则

要创建包含根据“应用程序启动控制”任务事件生成的允许规则的配置文件：

1. 以“仅统计”模式启动“应用程序启动控制”任务，以便在任务日志中记录有关受保护设备上的所有应用程序启动的信息。
2. 当任务在“**仅统计**”模式下运行完成后，通过单击“**应用程序启动控制**”节点详细信息窗格的“**管理**”部分中的“**打开任务日志**”按钮，打开任务日志。
3. 在“**日志**”窗口中，单击“**基于事件生成规则**”。

Kaspersky Embedded Systems Security 将会生成一个 XML 配置文件，其中包含基于“**仅统计**”模式下的“应用程序启动控制”任务事件的规则列表。您可以在“应用程序启动控制”任务中应用此规则列表。

在应用根据记录的任务事件生成的规则列表前，建议查看并手动处理列表，以确定指定规则允许关键文件（例如系统文件）启动。

无论任务模式如何，所有任务事件都将记录在任务日志中。您可以根据当任务在“**活动**”模式下运行时所创建的日志来生成包含规则列表的配置文件。除了紧急情况外，不建议使用此方案，因为在“**活动**”模式下运行任务前必须生成最终规则列表才能使其生效。

导出应用程序启动控制规则

要将应用程序启动控制规则导出到配置文件：

1. 打开“**应用程序启动控制规则**”窗口。
2. 单击“**导出到文件**”按钮。

   将打开标准的 Microsoft Windows 窗口。
3. 在打开的窗口中，指定想要将规则导出到其中的文件。如果不存在此类文件，则将创建它。如果具有指定名称的文件已存在，其内容在规则导出后将被覆盖。
4. 单击“**保存**”按钮。

规则设置将导出到指定文件。

从 XML 文件导入应用程序启动控制规则

要导入应用程序启动控制规则：

1. 打开“**应用程序启动控制规则**”窗口。
2. 单击“**添加**”按钮。

3. 在按钮的上下文菜单中，选择“从 XML 文件导入规则”。

4. 指定添加导入规则的方法。要执行此操作，请从“从 XML 文件导入规则”按钮的上下文菜单中选择一个选项：

   - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
   - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
   - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。

   将打开标准 Microsoft Windows“打开”窗口。

5. 在“打开”窗口中，选择包含应用程序启动控制规则的 XML 文件。

6. 单击“打开”按钮。

   导入的规则将显示在“应用程序启动控制规则”窗口中的列表中。

删除应用程序启动控制规则

要删除应用程序启动控制规则：

1. 打开“应用程序启动控制规则”窗口。

2. 在列表中，选择要删除的一项或多项规则。

3. 单击“删除选定项目”按钮。

4. 单击“保存”按钮。

   将删除所选应用程序启动控制规则。

配置“应用程序启动控制规则生成器”任务

要配置“应用程序启动控制规则生成器”任务设置：

1. 打开“应用程序启动控制规则生成器”任务的“任务设置”窗口。

2. 配置以下设置：

   - 在“常规”选项卡上：
     - 指定规则名称前缀。
     - 配置允许规则使用范围。
   - 在“操作”选项卡上，指定 Kaspersky Embedded Systems Security 必须执行的操作。
   - 在“计划”和“高级”选项卡上，配置计划任务启动设置。
   - 在“运行账户”选项卡上，配置使用账户权限的任务启动设置。

3. 在“**任务设置**”窗口中单击“**确定**”。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息。

限制任务使用范围

要限制“应用程序启动控制规则生成器”任务的范围：

1. 打开“**应用程序启动控制规则生成器**”任务的“任务设置”窗口。
2. 选择如何创建允许规则：
   - 基于正在运行的应用程序创建允许规则。
   - 为以下文件夹中的应用程序创建允许规则。
3. 在“**任务设置**”窗口中单击“**确定**”。

将保存指定设置。

自动规则生成期间要执行的操作

要配置 Kaspersky Embedded Systems Security 在“应用程序启动控制规则生成器”任务运行时和完成后执行的操作：

1. 打开“**应用程序启动控制规则生成器**”任务的“任务设置”窗口。
2. 打开“**选项**”选项卡。
3. 在“**生成允许规则时**”部分中，配置以下设置：
   - 使用数字证书
   - 使用数字证书主题和指纹
   - 证书丢失则使用
     - **SHA256 哈希**。将用于生成规则的文件的校验和设置为触发应用程序启动控制允许规则的条件。应用程序将允许启动使用带指定校验和的文件启动的程序。
     - **文件路径**。将用于生成规则的文件的路径设置为触发应用程序启动控制允许规则的条件。此时，应用程序将允许启动使用位于“**设置**”部分的“**为以下文件夹中的应用程序创建允许规则**”表中指定的文件夹中的文件启动的程序。
   - 使用 SHA256 哈希
   - 为用户或用户组生成规则。
4. 在“**任务完成后**”部分中，配置以下设置：

- 将允许规则添加到应用程序启动控制规则列表。
- 添加原则。
- 将允许规则导出到文件。
- 将受保护设备详细信息添加到文件名。

5. 在“**任务设置**”窗口中单击“**确定**”。

将保存指定设置。

自动规则生成完成后要执行的操作

要配置在“应用程序启动控制规则生成器”任务完成后 Kaspersky Embedded Systems Security 要执行的操作：

1. 打开“**应用程序启动控制规则生成器**”任务的“**任务设置**”窗口。
2. 打开“**选项**”选项卡。
3. 在“**任务完成后**”部分中，配置以下设置：
   - 将允许规则添加到应用程序启动控制规则列表。
   - 添加原则。
   - 将允许规则导出到文件。
   - 将受保护设备详细信息添加到文件名。
4. 在“**任务设置**”窗口中单击“**确定**”。

将保存指定设置。

通过 Web 插件管理应用程序启动控制

要通过 Web 插件管理“应用程序启动控制”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**本地活动控制**”部分。
5. 单击“**应用程序启动控制**”子部分中的“**设置**”。
6. 按下表所述配置设置。

“应用程序启动控制”任务设置

设置	描述

任务模式	在此下拉列表中，可选择“应用程序启动控制”任务的模式： • 活动。Kaspersky Embedded Systems Security 使用指定的规则控制任何应用程序的启动。 • 仅统计。Kaspersky Embedded Systems Security 不使用指定的规则控制应用程序启动。相反，它仅在任务日志中记录有关启动事件的信息。所有应用程序均允许启动。您可以使用此模式根据任务日志中记录的有关拒绝的应用程序启动的信息应用程序启动控制规则生成器列表。 默认情况下，“应用程序启动控制”任务在“仅统计”模式下运行。
在此文件的所有后续启动中重复针对首次文件启动执行的操作	此复选框用于启用或禁用根据缓存中存储的事件信息对第二次和后续应用程序启动尝试的启动控制。 如果选中该复选框，Kaspersky Embedded Systems Security 将根据任务针对应用程序第一次启动的结论允许或拒绝应用程序的后续启动。例如，如果规则允许了第一次应用程序启动，则有关此决定的信息将存储在缓存中，第二次和所有后续启动也将被允许，而不进行重复检查。 如果清除该复选框，Kaspersky Embedded Systems Security 会在每次尝试启动应用程序时分析该应用程序。 默认取消选中该复选框。
在没有可执行的命令时拒绝命令解释器启动	如果选中该复选框，Kaspersky Embedded Systems Security 将拒绝命令行解释器启动，即使允许解释器启动。只有同时满足以下两个条件时，才能在没有命令的情况下启动命令行解释器： • 允许命令行解释器启动。 • 要执行的命令获得允许。 如果清除该复选框，Kaspersky Embedded Systems Security 在启动命令行解释器时只考虑允许规则。如果未应用任何允许规则或可执行进程不受 KSN 信任，启动将被拒绝。如果应用了允许规则或进程受 KSN 信任，则无论是否有要执行的命令，都可以启动命令行解释器。 Kaspersky Embedded Systems Security 可识别以下命令行解释器： • cmd.exe • powershell.exe • python.exe • perl.exe 默认取消选中该复选框。
将规则应用于可执行文件	该复选框用于启用或禁用可执行文件的启动控制。 如果选中此复选框，则 Kaspersky Embedded Systems Security 将使用指定的规则（其设置指定可执行文件为范围）允许或阻止程序可执行文件的启动。 如果清除此复选框，则 Kaspersky Embedded Systems Security 不使用指定的规则控制程序可执行文件的启动。将允许可执行文件启动。 默认选中该复选框。
监控 DLL 模块的加载	该复选框用于启用或禁用 DLL 模块的加载控制。 如果选中此复选框，则 Kaspersky Embedded Systems Security 将使用指定的规则（其设置将可执行文件指定为范围）允许或阻止 DLL 模块的加载。

	如果清除此复选框，则 Kaspersky Embedded Systems Security 不使用指定的规则控制 DLL 模块的加载。将允许 DLL 模块加载。 如果选中“**将规则应用于可执行文件**”复选框，则该复选框处于活动状态。 默认选中该复选框。
将规则应用于脚本和 MSI 数据包	该复选框用于启用或禁用脚本和 MSI 数据包的启动。 如果选中此复选框，Kaspersky Embedded Systems Security 将使用指定的规则（其设置将脚本和 MSI 数据包指定为范围）允许或阻止脚本和 MSI 数据包启动。 如果清除此复选框，则 Kaspersky Embedded Systems Security 不使用指定的规则控制脚本和 MSI 数据包的启动。将允许脚本和 MSI 数据包的启动。 默认选中该复选框。
拒绝 KSN 不信任的应用程序	此复选框用于启用或禁用根据 KSN 中的应用程序声誉数据进行应用程序启动控制。 如果选中此复选框，则 Kaspersky Embedded Systems Security 将阻止任何在 KSN 中不受信任的应用程序运行。适用于在 KSN 中不受信任的应用程序的应用程序启动控制允许规则不会被触发。选中此复选框将会提供额外的恶意软件防护。 如果清除此复选框，则 Kaspersky Embedded Systems Security 将不考虑 KSN 中不受信任的应用程序的声誉，并根据适用于此类应用程序的规则允许或阻止启动。 默认取消选中该复选框。
允许 KSN 信任的应用程序	此复选框用于启用或禁用根据 KSN 中的应用程序声誉数据进行应用程序启动控制。 如果选中此复选框，则 Kaspersky Embedded Systems Security 将允许在 KSN 中受到信任的应用程序运行。适用于 KSN 信任的应用程序的拒绝应用程序启动控制规则具有更高优先级：如果某个应用程序受到 KSN 服务信任，应用程序启动将被拒绝。 如果清除此复选框，则 Kaspersky Embedded Systems Security 将不考虑 KSN 信任的应用程序的声誉，并根据适用于此类应用程序的规则允许或阻止启动。 默认取消选中该复选框。
允许运行 KSN 信任的应用程序的用户和/或用户组	如果选中“**允许 KSN 信任的应用程序**”复选框，则可以在此处指定允许启动 KSN 信任的应用程序的用户和用户组。 默认情况下，指定以下用户：**Everyone** 和 **NT AUTHORITY\SYSTEM**。
规则	为“应用程序启动控制”任务配置允许或拒绝规则。
软件分发控制	您可以添加受信任分发包。
任务管理	您可以配置按计划启动任务的设置。

设备控制

本节包含有关“设备控制”任务以及如何配置的信息。

关于设备控制任务

Kaspersky Embedded Systems Security 控制外部设备和 CD/DVD 驱动器的注册和使用，以保护设备免受计算机安全威胁的侵害，与闪存驱动器或通过 USB 连接的其他类型的外部设备进行文件交换的过程中可能出现这些威胁。

Kaspersky Embedded Systems Security 控制以下 USB 外部设备连接：

- USB 连接的闪存驱动器
- CD/DVD ROM 驱动器
- USB 连接的软盘驱动器
- USB 连接的网络适配器
- USB 连接的 MTP 移动设备

Kaspersky Embedded Systems Security 会通知您通过 USB 连接的所有设备，并在任务和事件日志中记录相应事件。事件详细信息包括设备类型和连接路径。“设备控制”任务启动后，Kaspersky Embedded Systems Security 将检查并列出通过 USB 连接的所有设备。您可以在 Kaspersky Security Center 通知设置部分中配置通知。

“设备控制”任务监控外部设备通过 USB 连接到受保护设备的所有连接尝试，如果没有此类设备的允许规则，则阻止连接。阻止连接后，设备将不可用。

应用程序为每个连接的外部设备规定了以下状态之一：

- *受信任*。您想允许其进行文件交换的设备。生成规则列表后，*设备实例路径*值将包含在至少一个规则的使用范围中。
- *不受信任*。您想限制其进行文件交换的设备。设备实例路径不会包含在任何允许规则的使用范围中。

您可以使用“设备控制规则生成器”任务为外部设备创建允许规则，以允许数据交换。您还可以扩展已指定规则的使用范围。不能手动创建允许规则。

Kaspersky Embedded Systems Security 使用“设备实例路径”值标识在系统中注册的外部设备。设备实例路径是专门为每个外部设备指定的默认功能。将在每个外部设备的 Windows 属性中为其指定“设备实例路径”值，并且该值将在生成规则期间由 Kaspersky Embedded Systems Security 自动确定。

设备控制任务可在两种模式下运行：

- 活动。Kaspersky Embedded Systems Security 会将规则应用于控制闪存驱动器和其他外部设备的连接，并根据默认拒绝原则和指定允许规则允许或阻止使用所有设备。允许使用受信任外部设备。默认情况下，阻止使用不受信任的外部设备。

如果当"设备控制"任务在**活动**模式下运行前您认为不受信任的外部设备连接到受保护设备，应用程序不会阻止该设备。推荐您手动断开不信任设备或重启受保护设备。否则，不会将"默认拒绝"原则应用于设备。

- **仅统计**。Kaspersky Embedded Systems Security 不会控制闪存驱动器和其他外部设备的连接，但仅记录有关外部设备在受保护设备上的连接和注册，以及有关相连设备触发的设备控制允许规则的信息。允许使用所有外部设备。默认设置此模式。

  您可以基于任务运行期间记录的有关阻止设备的信息对规则生成应用此模式。

关于设备控制规则

对于 MTP 连接的移动设备，Kaspersky Embedded Systems Security 不应用允许规则。

如果当前连接到或曾经连接到受保护设备的每台设备的信息存储在系统注册表中，将为每台设备生成具有唯一性的规则。

要生成设备控制的允许规则：

- 应用"设备控制规则生成器"任务。
- 以"仅统计"模式运行设备控制任务。
- 应用有关之前连接的设备的系统信息。
- 扩展已指定规则的使用范围。

Kaspersky Embedded Systems Security 支持的设备控制规则的最大数量为 3072。

下文介绍了设备控制规则。

规则类型

规则类型允许为*允许*。如果闪存驱动器和其他外部设备不包含在任何允许规则的使用范围内，默认情况下，设备控制任务会阻止所有这些设备连接。

触发条件和规则使用范围

设备控制规则基于*设备实例路径*识别闪存驱动器和其他外部设备。设备实例路径是设备建立连接并注册为外部设备或 CD/DVD 驱动器（例如，IDE 或 SCSI）时系统分配给设备的唯一条件。

无论用于连接的总线如何，Kaspersky Embedded Systems Security 都控制 CD/DVD 驱动器的连接。当通过 USB 安装此类设备时，操作系统会注册两个设备实例路径值：针对外部设备和针对 CD/DVD 驱动器（例如，IDE 或 SCSI）。要直接连接此类设备，必须设置每个实例路径值的允许规则。

Kaspersky Embedded Systems Security 自动定义设备实例路径并将获取的值解析为以下元素：

- 设备制造商 (VID)
- 设备控制器类型 (PID)
- 设备序列号

您不能手动设置设备实例路径。允许规则触发条件定义规则使用范围。默认情况下，新创建的规则使用范围包括一台初始设备，具体是哪台设备取决于 Kaspersky Embedded Systems Security 基于哪台设备的属性生成该规则。您可以配置创建的规则设置中的值并使用掩码扩展规则使用范围。

初始设备值

Kaspersky Embedded Systems Security 用于生成允许规则以及在 Windows 设备管理器中为每台连接的设备显示的设备属性。

初始设备值包含以下信息：

- **设备实例路径**。根据此属性，Kaspersky Embedded Systems Security 定义规则触发条件并填充以下字段："**规则属性**"窗口的"**规则使用范围**"部分中的"**制造商 (VID)**"、"**控制器类型 (PID)**"、"**序列号**"。
- **友好名称**。设备制造商在设备属性中设置的明确名称。

Kaspersky Embedded Systems Security 会在生成规则时自动定义初始设备值。以后您可以使用这些值识别生成规则时所依据的设备。初始设备值无法编辑。

描述

您可以在"**用户或用户组**"字段中为创建的每个设备控制规则添加更多信息，例如，您可以记录所连接的闪存驱动器的名称或定义其所有者。描述显示在"**设备控制规则**"窗口内的相应图表中。

描述和初始设置值不用于触发规则，只为了帮助用户识别设备。

关于设备控制规则生成

您可以从在"设备控制"或"设备控制规则生成器"任务运行期间自动生成的 XML 文件导入设备控制允许规则。

默认情况下，如果任何闪存驱动器或其他外部设备不包含在指定的设备控制规则的使用范围内，Kaspersky Embedded Systems Security 会限制这些设备的连接。

设备控制规则生成目标和方案

规则生成方案	目标
设备控制规则生成器任务	• 在设备控制任务第一次启动之前，为之前连接受信任设备添加允许规则。 • 为受保护设备网络中的受信任设备生成规则列表。
基于系统数据的规则生成	为一台或多台外部设备添加允许规则，这些设备的数据已存储在系统中。

根据有关当前连接的设备的数据生成规则	需要信任少量新外部设备时，更新已经指定的规则列表。
“仅统计”模式中的设备控制任务	为大量受信任设备生成允许规则。

设备控制规则生成器任务使用

在“设备控制规则生成器”任务完成时生成的 XML 文件包含其数据曾存储在系统注册表中的那些闪存驱动器和其他外部设备的允许规则。

在规则生成过程中使用此方案可考虑系统在所有网络受保护设备上注册的所有连接过的外部设备，或只考虑当前连接到所有网络受保护设备的设备的数据。该任务还会考虑在任务运行的那一刻处于连接状态的所有外部设备。组任务完成时，Kaspersky Embedded Systems Security 会为在网络中注册的所有外部设备生成允许规则列表，并将这些列表保存在指定文件夹内的 XML 文件中。然后，您可以在设备控制任务设置中手动导入生成的规则。与受保护设备上的任务不同的是，策略不允许配置在“设备控制规则生成器”组任务完成时将创建的规则自动添加到设备控制规则列表。

推荐在设备控制任务第一次启动之前使用此方案生成允许规则列表，以便生成的允许规则涵盖受保护设备上使用的所有受信任外部设备。

使用有关所有连接的设备的系统数据

在任务运行期间，Kaspersky Embedded Systems Security 会收到有关曾经或当前连接到受保护设备的所有外部设备的系统数据，并在“**基于系统信息生成规则**”窗口的列表中显示检测到的设备。

对于检测到的每个设备，Kaspersky Embedded Systems Security 会分析制造商 (VID)、控制器类型 (PID)、友好名称、序列号和设备实例路径的值。您可以为其数据存储在系统中的任何外部设备生成允许规则，并直接将新创建的规则添加到设备控制规则列表中。

根据此方案，Kaspersky Embedded Systems Security 会为曾经或当前连接到安装有 Kaspersky Security Center 的受保护设备的外部设备生成允许规则。

需要信任少量新外部设备时，推荐使用此方案更新已经指定的规则列表。

有关当前连接的设备的数据使用

在本方案中，Kaspersky Embedded Systems Security 仅为当前已连接的外部设备生成允许规则。可以选择要为其生成允许规则的一个或多个外部设备。

“仅统计”模式中的设备控制任务的使用

将基于任务日志生成在“**仅统计**”模式的设备控制任务完成时收到的 XML 文件。

在任务运行期间，Kaspersky Embedded Systems Security 会记录有关与受保护设备连接的闪存驱动器和其他外部设备的信息。您可以基于任务事件生成允许规则并将它们导出到 XML 文件。以“**仅统计**”模式启动任务之前，推荐您配置任务运行时段，以便在该时段内，将执行与受保护设备的所有可能的外部设备连接。

如果需要允许大量新的外部设备，推荐使用此方案更新已经生成的规则列表。

如果根据此方案在模板机上生成规则列表，您可以在通过 Kaspersky Security Center 配置“设备控制”任务时应用生成的允许规则列表。这样，您可以允许在所有受保护设备上使用连接到模板机的外部设备。

关于设备控制规则生成器任务

“设备控制规则生成器”任务可以基于有关曾连接到受保护设备的所有外部设备的系统数据，自动为连接的闪存驱动器和其他外部设备创建允许规则列表。

在任务完成后，Kaspersky Embedded Systems Security 会创建一个 XML 配置文件，其中包含所有检测到的外部设备的允许规则列表，或者直接在“设备控制”列表中添加生成的规则，具体取决于“设备控制规则生成器”设置。随后，应用程序将允许自动为其生成允许规则的设备。

生成的规则和添加到任务中的规则显示在“**设备控制规则**”窗口中。

“设备控制”任务默认设置

默认情况下，“设备控制”任务具有下表所述的设置。您可以更改这些设置的值。

默认设备控制任务设置

设置	默认值	描述
任务模式	**仅统计**	该任务记录有关根据指定的规则阻止或允许的外部设备的信息。实际上，不会阻止外部设备。 您可以为设备保护选择“**活动**”模式以实际阻止使用外部设备。
当未运行设备控制任务时允许使用所有外部设备	未应用	无论设备控制任务状态如何，Kaspersky Embedded Systems Security 都阻止使用外部设备。与外部设备交换文件时，可提供最佳保护级别，以防止计算机安全威胁。 您可以调整设置，以便 Kaspersky Embedded Systems Security 在设备控制任务未运行时允许使用所有外部设备。
任务启动计划	不设置任务的首次启动计划。	“设备控制”任务不会在 Kaspersky Embedded Systems Security 启动时自动启动。 您可以配置任务启动计划。

“设备控制规则生成器”任务的默认设置

设置	默认值	描述
任务模式	**考虑曾经连接过的所有外部设备的系统数据**	任务运行模式。 您可以选择“**仅考虑当前连接的外部设备**”任务模式。
任务完成时的操作	将允许规则添加到设备控制规则列表；新规则与现有规则合并；删除重复的规则。	您可以将规则添加到现有规则，而不进行合并并删除重复的规则，或将现有规则替换为新的允许规则，或配置将允许规则导出到文件。
任务启动计划	不设置任务的首次启动计划。	“设备控制规则生成器”任务不会在 Kaspersky Embedded Systems Security 启动时自动启动。您可以手动启动该任务或配置计划启动。

通过管理插件管理设备控制

在本节中，学习如何通过管理插件界面进行导航，以及如何通过 Kaspersky Security Center 为受保护设备组生成规则列表来管理任意外部设备与网络上所有受保护设备的连接。

导航

了解如何通过所选界面导航到所需任务设置。

打开“设备控制”任务的策略设置

要通过 Kaspersky Security Center 策略打开“设备控制”任务设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在打开的“**属性：<策略名称>**”窗口中，选择“**本地活动控制**”部分。
6. 在“**设备控制**”子部分中单击“**设置**”按钮。
   将打开“**设备控制**”窗口。
7. 根据需要配置策略。

打开设备控制规则列表

要通过 Kaspersky Security Center 打开设备控制规则列表：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在打开的“**属性：<策略名称>**”窗口中，选择“**本地活动控制**”部分。
6. 在“**设备控制**”子部分中单击“**设置**”按钮。
   将打开“**设备控制**”窗口。
7. 在“**常规**”选项卡上，单击“**规则列表**”按钮。
   将打开“**设备控制规则**”窗口。
8. 根据需要配置策略。

打开“设备控制规则生成器”任务向导和属性

要初始化“设备控制规则生成器”任务的创建：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**任务**”选项卡。
4. 单击“**创建任务**”按钮。
   将打开“**新建任务向导**”窗口。
5. 选择“**设备控制规则生成器**”任务。
6. 单击“**下一步**”。
   将打开“**设置**”窗口。

要配置现有“设备控制规则生成器”任务：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**任务**”选项卡。
4. 双击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**属性：设备控制规则生成器**”窗口。

有关配置该任务的详细信息，请参见“配置‘设备控制规则生成器’任务”部分。

配置“设备控制”任务

要配置“设备控制”任务设置：

1. 打开“**设备控制**”窗口。
2. 在“**常规**”选项卡上，配置以下任务设置：
   - 在“**任务模式**”部分中，选择以下任务模式之一：
     - 活动。

       如果当“设备控制”任务在活动模式下运行前您认为不受信任的外部设备连接到受保护设备，应用程序不会阻止该设备。推荐您手动断开不信任设备或重启受保护设备。否则，不会将“默认拒绝”原则应用于设备。

     - 仅统计。

- 选中或清除“当未运行设备控制任务时允许使用所有外部设备”复选框。

3. 单击“**规则列表**”按钮以编辑设备控制规则列表。
4. 如有必要，在“**任务管理**”选项卡上配置计划的任务启动设置。
5. 在“**设备控制**”窗口中单击“**确定**”。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

配置“设备控制规则生成器”任务

要配置“设备控制规则生成器”任务：

1. 打开“**属性：设备控制规则生成器**”窗口。
2. 在“**通知**”部分中，配置任务事件通知设置。

   关于此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

3. 在“**设置**”部分中，您可配置以下设置：
   - 选择运行模式：考虑曾经连接过的所有外部的系统数据，或仅考虑当前连接的外部设备。
   - 使用 Kaspersky Embedded Systems Security 在任务完成时创建的允许规则列表为配置文件配置设置。
4. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。
5. 在“**账户**”部分中，指定将使用其权限运行任务的账户。
6. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。

   有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

7. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。
   将保存新配置的组任务设置。

通过 Kaspersky Security Center 配置设备控制规则

学习如何使用设备控制任务根据各种条件生成规则列表，或手动创建允许或拒绝规则。

基于 Kaspersky Security Center 策略中的系统数据创建允许规则

*要使用设备控制任务中的“**基于系统数据生成规则**”选项指定允许规则：*

1. 如有必要，将您希望信任的新的外部设备连接到安装了 Kaspersky Security Center 管理控制台的受保护设备。

2. 打开“设备控制规则”窗口。

3. 单击“**添加**”按钮，在打开的上下文菜单中，选择“**基于系统数据生成规则**”选项。

4. 在“**基于系统信息生成规则**”窗口中，选择一个设备。

5. 单击“**为所选设备添加规则**”。

6. 在“**设备控制规则**”窗口中单击“**保存**”按钮。

“设备控制”任务中的规则列表将使用基于安装了 Kaspersky Security Center 管理控制台的受保护设备的系统数据生成的新规则填充。

为已连接的设备生成规则

*要使用设备控制任务中的“**基于连接的设备生成规则**”选项指定允许规则：*

1. 打开“设备控制规则”窗口。

2. 单击“**添加**”按钮，然后在上下文菜单中，选择“**基于连接的设备生成规则**”。
   将打开“**基于系统信息生成规则**”窗口。

3. 在检测到的已连接到受保护设备的设备列表中，选择您要为其生成允许规则的设备。

4. 单击“**为所选设备添加规则**”按钮。

5. 在“**设备控制规则**”窗口中单击“**保存**”按钮。

“设备控制”任务中的规则列表将使用基于安装了 Kaspersky Security Center 管理控制台的受保护设备的系统数据生成的新规则填充。

基于 Kaspersky Security Center 注册表生成规则

*要使用“设备控制”任务中的“**基于连接的设备生成规则**”选项指定允许规则：*

1. 打开“设备控制规则”窗口。

2. 单击“**添加**”按钮，然后在上下文菜单中，选择“**基于连接的设备生成规则**”。
   将打开“**基于系统信息生成规则**”窗口。

3. 点击“**刷新列表**”获取可用设备列表，并选择想为其生成允许规则的设备。此外，您可以在“**搜索**”字段中指定“**友好名称**”以筛选设备并加快选择速度。

4. 单击“**为所选设备添加规则**”按钮。

5. 在“**设备控制规则**”窗口中单击“**保存**”按钮。

“设备控制”任务中的规则列表将由基于 Kaspersky Security Center 注册表生成的新规则填充。

查看“设备控制”规则的属性

要查看“**设备控制**”规则的属性：

1. 打开“**设备控制**”窗口。
2. 在“**常规**”选项卡上，单击“**规则列表**”按钮并双击所选规则。

   将出现“**规则属性**”窗口。

“设备控制”规则的属性

属性	描述
应用规则	使用此选项启用或禁用规则应用程序。
制造商 (VID)	您可以指定设备制造商的完整 VID 或使用 * 作为掩码。* 代表任何制造商。 如果为“制造商 (VID)”字段选中了“使用掩码”复选框，则将使用 * 字符代替复选框被选中的字段的数据，并且在应用规则时不会考虑这些数据。
控制器类型 (PID)	您可以指定控制器的完整 PID 或使用 * 作为掩码。* 代表任何类型的控制器。 如果为“控制器类型 (PID)”字段选中了“使用掩码”复选框，则将使用 * 字符代替复选框被选中的字段的数据，并且在应用规则时不会考虑这些数据。
序列号	您可以指定设备的完整序列号或使用 * 和 ? 作为掩码。 * 代表任何字符序列，包括空序列。 ? 代表序列中的一个字符。 如果为“序列号”字段选中了“使用掩码”复选框，则将使用 * 字符代替复选框被选中的字段的数据，并且在应用规则时不会考虑这些数据。 如果您选择了“**使用掩码**”选项，但未在“**序列号**”字段中输入任何字符，然后保存设置并关闭窗口，则应用程序会应用 * 作为“**序列号**”属性的掩码，并且在应用规则时不会考虑该字段。
设备实例路径	所连接设备的标识符。 您不能修改属性。该字段仅作提供信息之用。该应用程序不应用该字段进行设备控制。
友好名称	制造商设置的设备名称。 您不能修改属性。该字段仅作提供信息之用。该应用程序不应用该字段进行设备控制。
用户或用户组	您可以指定有权访问所选 USB 设备的用户账户或用户组。 操作系统显示所有连接的 USB 设备。您只能访问您拥有相应访问权限的 USB 驱动器。
描述	默认设备描述。 如有必要，请在“描述”字段中指定有关规则的附加信息。例如，指定受规则影响的设备。

从有关被阻止设备的 Kaspersky Security Center 报告中导入规则

您可从在“仅统计”模式下完成“设备控制”任务后 Kaspersky Security Center 中生成的报告导入有关被阻止设备连接的数据，并使用此数据在所配置策略中生成设备控制允许规则列表。

生成设备控制任务期间发生的事件报告时，您可跟踪其连接受限制的设备。

要基于有关被阻止设备的 Kaspersky Security Center 报告为一组受保护设备指定设备连接允许规则：

1. 在“**事件通知**”部分中的策略属性中，确保：

   - 对于“**关键事件**”重要性级别，“*检测到不受信任的外部设备并限制该设备*”事件的任务日志的存储时间段超过在“**仅统计**”模式下的运行计划时间段（默认值为 30 天）。
   - 对于“**警告**”重要性级别，“*仅统计: 检测到不受信任的外部设备*”事件的任务日志的存储时间段超过在“**仅统计**”模式下的任务运行计划时间段（默认值为 30 天）。

   > 当事件的存储时间段过后，有关记录的事件的信息会被删除且不会反映在报告文件中。在“**仅统计**”模式下运行设备控制任务之前，确保任务运行时间不超过为指定事件配置的存储时间。

2. 以“**仅统计**”模式启动“设备控制”任务。

   a. 在 Kaspersky Security Center 中的“**管理服务器**”节点的工作区中，选择“**事件**”选项卡。

   b. 单击“**创建选择**”按钮并基于“*检测到不受信任的外部设备并限制该设备*”条件创建一系列事件，以查看“设备控制”任务将限制其连接的设备。

   c. 在所选项的结果窗格中，单击“**将事件导出到文件**”链接以将有关限制的连接的报告保存到 TXT 文件。

> 在策略中导入和应用生成的报告之前，确保报告仅包含有关您希望允许其连接的设备的数据。

3. 将有关受限制设备连接的数据导入设备控制任务：

   a. 打开“设备控制规则”窗口。

   b. 单击“**添加**”按钮，然后在该按钮的上下文菜单中选择“**从 Kaspersky Security Center 报告导入阻止的设备的数据**”。

   c. 选择将来自根据 Kaspersky Security Center 报告创建的列表的规则添加到先前配置的设备控制规则列表的原则：

      - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
      - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
      - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。

   d. 在打开的 Microsoft Windows 标准窗口中，选择已将来自受限制设备报告的事件导出到的 TXT 文件。

   e. 在“**设备控制规则**”窗口中单击“**保存**”按钮。

4. 在“**设备控制**”窗口中单击“**确定**”。

根据有关受限制设备的 Kaspersky Security Center 报告创建的规则将被添加到设备控制规则列表。

使用“设备控制规则生成器”任务创建规则

要使用“设备控制规则生成器”任务为一组受保护设备指定允许设备控制规则：

1. 打开“新建任务向导”中的“**设置**”窗口。

2. 进行以下配置：

   - 在“**模式**”部分中：
     - **考虑曾经连接过的所有外部设备的系统数据**。
     - **仅考虑当前连接的外部设备**。
   - 在“**任务完成后**”部分中：
     - **将允许规则添加到设备控制规则列表**。
     - **添加原则**。
     - **将允许规则导出到文件**。
     - **将受保护设备详细信息添加到文件名**。

3. 单击“**下一步**”。
4. 在“**计划**”窗口中，设置计划的任务启动设置。
5. 单击“**下一步**”。
6. 在“**选择账户以运行任务**”窗口中，指定要使用的账户。
7. 单击“**下一步**”。
8. 指定任务名称。
9. 单击“**下一步**”。

   任务名称不应超过 100 个字符，并且不能包含以下符号：" * < > & \ : |

   将打开“**完成创建任务**”窗口。
10. 您可以通过选中“**向导完成后运行任务**”复选框来在向导完成后运行任务。
11. 单击“**完成**”完成创建任务。
12. 在所配置受保护设备组的工作区上的“**任务**”选项卡上，从组任务列表中选择您已创建的“设备控制规则生成器”。
13. 单击“**启动**”按钮启动任务。

    任务完成后，自动生成的允许规则列表将保存在共享文件夹中的 XML 文件中。

    在网络中使用设备控制策略之前，请确保所有受保护设备都能够访问共享网络文件夹。如果组织的策略未规定在网络中使用共享网络文件夹，则推荐为测试受保护设备组或模板机上的受保护设备控制规则启动“设备控制规则生成器”任务。

将生成的规则添加到设备控制规则列表

要将生成的允许规则列表添加到"设备控制"任务：

1. 打开"设备控制规则"窗口。
2. 单击"**添加**"按钮。
3. 在"**添加**"按钮的上下文菜单中选择"**从 XML 文件导入规则**"选项。
4. 选择将自动生成的允许规则添加到先前创建的设备控制规则列表中的原则：
   - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
   - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
   - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。
5. 在打开的 Microsoft Windows 标准窗口中，选择"设备控制规则生成器"组任务完成后创建的 XML 文件。
6. 单击"**打开**"。
   XML 文件中所有生成的规则将按照所选原则添加到列表中。
7. 在"**设备控制规则**"窗口中单击"**保存**"按钮。
8. 如果想要应用生成的设备控制规则，请在"**设备控制**"策略设置中选择"**活动**"任务模式。

基于每台单独的受保护设备上的系统数据自动生成的允许规则将被应用于所配置策略涵盖的所有网络受保护设备。在这些受保护设备上，应用程序将仅允许已为其创建允许规则的那些设备进行连接。

通过应用程序控制台管理设备控制

在本节中，学习如何导航应用程序控制台界面以及如何在受保护设备上配置任务设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开"设备控制"任务设置

要通过应用程序控制台打开"设备控制"任务设置：

1. 在应用程序控制台树中，展开"**计算机控制**"节点。
2. 选择"**设备控制**"子节点。

3. 在“**设备控制**”子节点的详细信息窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。
4. 根据需要配置任务。

打开“设备控制规则”窗口

要通过应用程序控制台打开设备控制规则列表：

1. 在应用程序控制台树中，展开“**计算机控制**”节点。
2. 选择“**设备控制**”子节点。
3. 在“**设备控制**”节点的结果窗格中，单击“**设备控制规则**”链接。
   将打开“**设备控制规则**”窗口。
4. 根据需要配置规则列表。

打开“设备控制规则生成器”任务设置

要配置“设备控制规则生成器”任务：

1. 在应用程序控制台树中，展开“**自动规则生成器**”节点。
2. 选择“**设备控制规则生成器**”子节点。
3. 在“**设备控制规则生成器**”子节点的结果窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。
4. 根据需要配置任务。

配置设备控制任务设置

要配置“设备控制”任务设置：

1. 打开“**任务设置**”窗口。
2. 在“**常规**”选项卡上，配置以下任务设置：
   - 在“**任务模式**”部分中，选择以下任务模式之一：
     - 活动。

如果当“设备控制”任务在活动模式下运行前您认为不受信任的外部设备连接到受保护设备，应用程序不会阻止该设备。推荐您手动断开不信任设备或重启受保护设备。否则，不会将“默认拒绝”原则应用于设备。

- 仅统计。

- 选中或清除“当未运行设备控制任务时允许使用所有外部设备”复选框。

3. 如果必要，在“**计划**”和“**高级**”选项卡上，配置计划的任务启动设置。

4. 要编辑设备控制规则列表，请在“**设备控制**”节点的结果窗格的下部，单击“**设备控制规则**”链接。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

配置设备控制规则

了解如何使用“设备控制”任务生成、导入和导出规则列表，或手动创建允许或拒绝规则。

从 XML 文件导入设备控制规则

要导入设备控制规则：

1. 打开“设备控制规则”窗口。

2. 单击“**添加**”按钮。

3. 在按钮的上下文菜单中，选择“**从 XML 文件导入规则**”。

4. 指定添加导入规则的方法。要执行此操作，请从“**从 XML 文件导入规则**”按钮的上下文菜单中选择一个选项：

   - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。

   - **替换现有规则**，如果您希望将现有规则替换为导入的规则。

   - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。

   将打开标准 Microsoft Windows“**打开**”窗口。

5. 在“**打开**”窗口中，选择包含设备控制规则的设置的 XML 文件。

6. 单击“**打开**”按钮。

导入的规则将显示在“**设备控制规则**”窗口中的列表中。

基于设备控制任务事件填写规则列表

要基于“设备控制”任务事件创建包含设备控制规则列表的配置文件：

1. 以“仅统计”模式启动设备控制任务，以记录与受保护设备连接的闪存驱动器和其他外部设备的所有事件。
2. “仅统计”模式中的任务完成后，通过单击“**设备控制**”节点结果窗格的“**管理**”部分中的“**打开任务日志**”按钮，打开任务日志。
3. 在“**日志**”窗口中，单击“**基于事件生成规则**”。

Kaspersky Embedded Systems Security 将会创建一个 XML 配置文件，其中包含基于“**仅统计**”模式中的“设备控制”任务事件生成的规则列表。您可以在“设备控制”任务中应用此列表。

在应用基于任务事件生成的规则列表之前，推荐您仔细检查，然后手动处理规则列表，以确保指定的规则没有允许不信任设备。

在将包含任务事件 XML 文件转换为规则列表期间，应用程序将为所有注册的事件生成允许规则，包括设备限制。

无论任务模式如何，所有任务事件都将记录在任务日志中。您可以基于处于“**活动**”模式的任务事件创建包含规则列表的配置文件。除非出现紧急情况，例如任务效率要求在任务以活动模式运行之前生成最终规则列表版本，否则不推荐使用此方案。

为一个或多个外部设备添加允许规则

设备控制任务中支持手动逐个添加规则的功能。但是，如果您需要为一个或多个新外部设备添加规则，可以使用“**基于系统数据生成规则**”选项。如果应用此方案，应用程序将使用有关所有曾经连接过的外部设备的 Windows 数据，并且还允许当前连接的设备，以填写允许规则列表。

要为当前连接的一个或多个外部设备添加允许规则：

1. 打开“设备控制规则”窗口。
2. 单击“**添加**”按钮。
3. 在打开的上下文菜单中，选择“**基于系统数据生成规则**”选项。
4. 在打开的窗口中，查看检测到的设备列表并选择要在受保护设备上信任的一个或多个设备。
5. 单击“**为所选设备添加规则**”按钮。

将会生成新规则并添加到设备控制规则列表中。

删除设备控制规则

要删除设备控制规则：

1. 打开“设备控制规则”窗口。
2. 在列表中，选择要删除的一项或多项规则。
3. 单击“**删除选定项目**”按钮。

4. 单击“**保存**”按钮。

将删除所选设备控制规则。

导出设备控制规则

要将设备控制规则导出到配置文件：

1. 打开“设备控制规则”窗口。
2. 单击“**导出到文件**”按钮。

   将打开标准的 Microsoft Windows 窗口。
3. 在打开的窗口中，指定想要将规则导出到其中的文件。如果不存在此类文件，则将创建它。如果具有指定名称的文件已存在，则将在导出规则后重写其内容。
4. 单击“**保存**”按钮。

规则及其设置将导出到指定文件中。

激活和停用设备控制规则

您可以激活和停用已创建的设备控制规则，而不必删除它们。

要激活或停用已创建的设备控制规则：

1. 打开“设备控制规则”窗口。
2. 在指定规则列表中，通过双击要配置其属性的规则，打开“**规则属性**”窗口。
3. 在打开的窗口中，选中或清除“应用规则”复选框。
4. 单击“**确定**”。

将为指定规则保存和显示规则应用状态。

扩展设备控制规则使用范围

每个自动生成的设备控制规则都只涵盖一个外部设备。您可以通过在任何指定规则的属性中设置设备实例路径掩码，来手动扩展规则使用范围。

应用设备实例路径可减少指定的总规则数并简化规则处理。但是扩展规则使用范围可能会降低外部设备控制效率。

要在设备控制规则属性中应用设备实例路径掩码：

1. 打开“设备控制规则”窗口。
2. 在打开的窗口中，选择一个规则以使用其属性来应用掩码。

3. 通过双击选定的设备控制规则，打开“**规则属性**”窗口。

4. 在打开的窗口中，执行以下操作：

   - 如果您希望选定规则允许所有符合指定的设备制造商信息的外部设备的连接，请选中“**制造商 (VID)**”字段旁边的“**使用掩码**”复选框。
   - 如果您希望选定规则允许所有符合指定的控制器类型信息的外部设备的连接，请选中“**控制器类型 (PID)**”字段旁边的“**使用掩码**”复选框。
   - 如果您希望选定规则允许所有符合指定的设备序列号信息的外部设备的连接，请选中“**序列号**”字段旁边的“**使用掩码**”复选框。

   如果在至少一个字段中选中了“**使用掩码**”复选框，则将使用 * 字符代替复选框被选中的字段的数据，并且在应用规则时不会考虑这些数据。

5. 指定有权访问所选 USB 设备的用户账户或用户组。操作系统显示所有连接的 USB 设备。您只能访问您拥有相应访问权限的 USB 设备。

6. 如有必要，请在“**用户或用户组**”字段中指定有关规则的附加信息。例如，指定受规则影响的设备。

7. 单击“**确定**”。

将保存新配置的规则属性。规则使用范围将根据指定的设备实例路径掩码进行扩展。

配置设备控制规则生成器任务

要配置“设备控制规则生成器”任务：

1. 在应用程序控制台树中，展开“**自动规则生成器**”节点。

2. 选择“**设备控制规则生成器**”子节点。

3. 在“**设备控制规则生成器**”节点的结果窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。

4. 在“**常规**”选项卡上的“**任务模式**”部分中选择任务运行模式：

   - **考虑曾经连接过的所有外部设备的系统数据**。
   - **仅考虑当前连接的外部设备**。

5. 在“**任务完成后**”部分中，指定 Kaspersky Embedded Systems Security 在任务完成后必须执行的操作：

   - 将允许规则添加到设备控制规则列表。
   - 添加原则。
   - 将允许规则导出到文件。
   - 将受保护设备详细信息添加到文件名。

6. 在“**计划**”和“**高级**”选项卡上，配置计划的任务启动设置。

7. 在“**任务设置**”窗口中单击“**确定**”。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

通过应用程序控制台 Web 插件管理设备控制

在本节中，您将学习如何导航 Web 插件界面以及如何在受保护设备上配置任务设置。

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**本地活动控制**”部分。
5. 在“**设备控制**”子部分中单击“**设置**”。
6. 按下表所述配置设置。

设备控制任务设置

设置	描述
活动	Kaspersky Embedded Systems Security 会将规则应用于控制可移动驱动器和其他外部设备的连接，并根据默认拒绝原则和指定允许规则允许或阻止使用所有设备。允许使用受信任外部设备。默认情况下，阻止使用不受信任的外部设备。
仅统计	Kaspersky Embedded Systems Security 不会控制可移动驱动器和其他外部设备的连接，但仅记录有关外部设备在受保护设备上的连接和注册，以及有关相连设备触发的设备控制允许规则的信息。允许使用所有外部设备。默认设置此模式。
当未运行设备控制任务时允许使用所有外部设备	使用此复选框可允许或阻止在“设备控制”任务未运行时使用外部设备。 如果选择该复选框且“设备控制”任务未运行，则 Kaspersky Embedded Systems Security 允许在受保护设备上使用任何外部设备。 如果清除此复选框，应用程序在以下情况下将阻止在受保护设备上使用不受信任的外部设备：“设备控制”任务未运行或 Kaspersky Security 服务已关闭。推荐使用该选项以最大限度保护您的计算机在与外部设备交换文件时免受安全威胁。 默认取消选中该复选框。
设备控制规则	您可以编辑设备控制规则列表。
任务管理	您可以配置按计划启动任务的设置。

防火墙管理

本节包含有关防火墙管理任务以及如何配置它的信息。

关于防火墙管理任务

Kaspersky Embedded Systems Security 会提供一个可靠方便的解决方案，以便使用防火墙管理任务保护网络连接。

防火墙管理任务不会执行独立的网络流量过滤，但它允许您通过 Kaspersky Embedded Systems Security 图形界面管理 Windows 防火墙。在防火墙管理任务期间，Kaspersky Embedded Systems Security 接管对操作系统防火墙的设置和策略的管理，并阻止任何配置防火墙的外部尝试。

在应用程序安装期间，防火墙管理组件会读取并复制 Windows 防火墙状态及所有指定规则。此后，只能更改规则集和规则参数，且防火墙只能在 Kaspersky Embedded Systems Security 中打开或关闭。

如果在安装 Kaspersky Embedded Systems Security 期间 Windows 防火墙关闭，则在安装完成后将不会执行防火墙管理任务。如果在安装应用程序期间 Windows 防火墙打开，则会在安装完成后执行防火墙管理任务，从而阻止指定规则不允许的所有网络连接。

默认情况下，不会安装防火墙管理组件，因为其未包括在推荐安装组件集中。

防火墙管理任务强制阻止任务的指定规则不允许的所有传入和传出连接。

该任务会定期轮询 Windows 防火墙并监控其状态。默认情况下，轮询间隔设置为 1 分钟且无法更改。如果 Kaspersky Embedded Systems Security 检测到 Windows 防火墙设置和防火墙管理任务设置之间存在不匹配，应用程序会强制应用操作系统防火墙上的任务设置。

每分钟轮询 Windows 防火墙时，Kaspersky Embedded Systems Security 监控以下信息：

- Windows 防火墙的运行状态。
- 安装 Kaspersky Embedded Systems Security 后其他应用程序或工具添加的规则的状态（例如，使用 wf.msc 为某个端口/应用程序添加的新应用程序规则）。

将新规则应用于 Windows 防火墙时，Kaspersky Embedded Systems Security 会在 Windows 防火墙管理单元中创建一个 Kaspersky Security 组规则集。该规则集包含 Kaspersky Embedded Systems Security 使用“防火墙管理”任务创建的所有规则。在轮询期间，应用程序不会监控 Kaspersky Security 组中的规则，且该规则不会自动与防火墙管理任务设置中指定的规则列表同步。

要手动更新 Kaspersky Security 组规则，

请重新启动 Kaspersky Embedded Systems Security 防火墙管理任务。

您还可使用 Windows 防火墙管理单元手动编辑 Kaspersky Security 组规则。

如果按 Kaspersky Security Center 组策略管理 Windows 防火墙，则防火墙管理任务无法启动。

关于防火墙规则

防火墙管理任务使用任务执行期间强制应用于 Windows 防火墙的允许规则控制传入和传出网络流量的过滤。

首次启动任务时，Kaspersky Embedded Systems Security 会读取 Windows 防火墙设置中指定的所有传入网络流量规则，并将其复制到防火墙管理任务设置。然后，应用程序根据以下规则运行：

- 如果在 Windows 防火墙设置中创建新规则（在安装新应用程序期间手动或自动创建），Kaspersky Embedded Systems Security 会删除该规则。
- 如果从 Windows 防火墙设置中删除现有规则，则重新启动任务后 Kaspersky Embedded Systems Security 会还原该规则。
- 如果在 Windows 防火墙设置中更改现有规则的参数，Kaspersky Embedded Systems Security 会回滚更改。
- 如果在防火墙管理设置中创建新规则，Kaspersky Embedded Systems Security 会将该规则强制应用于 Windows 防火墙。
- 如果从防火墙管理设置中删除现有规则，Kaspersky Embedded Systems Security 会从 Windows 防火墙设置中强制删除该规则。

您可以管理不同类型的防火墙规则：针对应用程序和针对端口。

安装和删除应用程序时默认规则的行为

在安装过程中，会创建一组允许规则，以防止与 Kaspersky Embedded Systems Security 一起安装的应用程序被阻止并确保其持续运行。以下是详细信息和限制。

默认情况下，当您在运行任何支持的 Windows 操作系统版本的设备上安装应用程序时，Kaspersky Embedded Systems Security 会为传入网络流量创建一组规则：

- Kaspersky Embedded Systems Security 控制台的允许规则，位于应用程序安装文件夹中。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- 本地端口 15000 的两个允许规则（如果 Kaspersky Security Center 网络代理安装在设备上）。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。

默认情况下，当您在运行 Windows 7 或更高版本的设备上安装应用程序时，Kaspersky Embedded Systems Security 会为传出网络流量创建一组规则：

- Kaspersky Security Management 的允许规则，位于应用程序安装文件夹中。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- Kaspersky Embedded Systems Security 的允许规则，位于应用程序安装文件夹中。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。
- 本地端口 13000 的两个允许规则（如果 Kaspersky Security Center 网络代理安装在设备上）。状态：启用。允许的外部地址：任何。协议：TCP 和 UPD – 每个协议一个规则。

当您卸载 Kaspersky Embedded Systems Security 时，应用程序将删除所有创建的防火墙规则，但由 Kaspersky Security Center 网络代理创建的规则除外，例如 Kaspersky Security Center WDS 和 Kaspersky Administration Kit。此外，该应用程序还删除了适用于 Windows 7 及更高版本的 ICMPv4 和 ICMPv6 的规则。

当您卸载 Kaspersky Embedded Systems Security 时，该应用程序会为 Windows 7 以前版本的操作系统启用所有 ICMP 连接。

应用程序规则

此类型的规则允许指定应用程序的目标网络连接。这些规则的触发条件基于可执行文件的路径。

您可管理应用程序规则：

- 添加新规则。
- 删除现有规则。
- 启用或禁用指定规则。
- 编辑指定规则的参数：指定规则名称、可执行文件的路径以及规则使用范围。

端口规则

此类型的规则允许指定端口和协议 (TCP/UDP) 的网络连接。这些规则的触发条件基于端口号和协议类型。

您可管理端口规则：

- 添加新规则。
- 删除现有规则。
- 启用或禁用指定规则。
- 编辑指定规则的参数：设置规则名称、端口号、协议类型以及规则的应用范围。

端口规则涉及的范围比应用程序规则的范围要广。通过基于端口规则允许连接，会降低受保护设备的安全级别。

防火墙管理任务默认设置

防火墙管理任务使用下表描述的默认设置。您可以更改这些设置的值。

防火墙管理任务默认设置

设置	默认值	描述
入站连接	阻止	您可以配置传入流量规则的设置以阻止或允许入站连接。 默认情况下，规则类型与策略类型相反。例如，对于默认拒绝策略，规则的默认值设置为“**允许**”。对于默认允许策略，规则的默认值设置为“**阻止**”。您可以根据需要更改规则的类型。
出站连接	允许	您可以配置传出流量规则的设置以阻止或允许出站连接。

		默认情况下，规则类型与策略类型相反。例如，对于默认拒绝策略，规则的默认值设置为“**允许**”。对于默认允许策略，规则的默认值设置为“**阻止**”。您可以根据需要更改规则的类型。
允许 ICMP 连接	**已禁用**	此选项通过 ICMPv4 和 ICMPv6 协议同时控制传入和传出 ICMP 连接。 如果启用该选项，Kaspersky Embedded Systems Security 将忽略为入站连接或出站连接设置配置的“**阻止**”值。选中的“**允许 ICMP 连接**”选项具有更高的优先级。
任务启动计划	N/A	“防火墙管理”任务不会在 Kaspersky Embedded Systems Security 启动时自动启动。 您可以配置任务启动计划。

通过管理插件管理防火墙规则

在本节中，学习如何通过管理插件界面管理防火墙规则。

启用和禁用防火墙规则

要启用或禁用过滤传入网络流量的现有规则，请执行以下操作：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**网络活动控制**”部分中，单击“**防火墙管理**”子部分中的“**设置**”按钮。
5. 单击打开的窗口中的“**规则列表**”按钮。
   将打开“**入站防火墙规则**”窗口。
6. 根据想要修改其状态的规则类型，单击“**入站**”或“**出站**”链接，然后选择“**应用程序**”或“**端口**”选项卡。
7. 在规则列表中，选择要修改其状态的规则，然后执行以下操作之一：
   - 如果您想要启用已禁用的规则，选中规则名称左侧的复选框。
     将启用所选规则。
   - 如果您想要禁用已启用的规则，清除规则名称左侧的复选框。
     将禁用所选规则。
8. 在“**入站防火墙规则**”窗口中，单击“**确定**”。

9. 在“**防火墙管理**”窗口中，单击“**确定**”。

10. 在“**属性：<策略名称>**”窗口中，单击“**确定**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

手动添加防火墙规则

您只能添加和编辑应用程序和端口的规则。不能新增或编辑现有组规则。

要添加过滤传入网络流量的新规则或编辑现有规则：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择要为其配置应用程序设置的管理组。

3. 在选定的管理组的详细窗格中执行以下操作之一：

   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

   如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**网络活动控制**”部分中，单击“**防火墙管理**”子部分中的“**设置**”按钮。

5. 在出现的“**防火墙管理**”窗口中，在“**常规**”选项卡上，根据您要配置的连接类型，单击“**入站或出站**”子部分旁边的“**规则列表**”按钮。

   为入站和出站连接配置规则时，请注意以下选项和限制：

   - 默认情况下，规则类型与策略类型相反。例如，对于默认拒绝策略，规则的默认值设置为“**允许**”。对于默认允许策略，规则的默认值设置为“**阻止**”。您可以根据需要更改规则的类型。
   - 如果将本地应用程序控制台连接到运行任何操作系统的远程设备，或者将本地应用程序控制台连接到运行 Windows 7 或更高版本的本地设备，则可以配置默认任务设置。
   - 如果将本地应用程序控制台连接到运行 Windows 7 以前版本的操作系统的本地设备，则无法配置默认防火墙任务设置。

6. 在出现的窗口中，选择“**应用程序**”或“**端口**”选项卡并执行以下操作之一：

   - 要编辑现有规则，在规则列表中选择要编辑的规则，然后单击“**编辑**”。
   - 要添加新规则，单击“**添加**”。

     根据配置的规则类型，将打开“**应用程序规则**”窗口或“**端口规则**”窗口。

7. 在出现的窗口中，执行以下操作：

   - 如果您使用的是应用程序规则，请执行以下操作：

a. 在“**规则名称**”字段中，输入所编辑规则的名称。

b. 在“**规则操作**”列表中，根据需要选择“**允许**”或“**阻止**”选项。

c. 指定您通过修改规则允许其连接的应用程序的可执行文件的“**应用程序路径**”。
您可手动或通过使用“**浏览**”按钮设置路径。

d. 在“**规则操作**”字段中，指定将为其应用已修改规则的网络地址。

只能使用 IPv4 地址。

- 如果您使用的是端口规则，请执行以下操作：

a. 在“**规则名称**”字段中，输入所编辑规则的名称。

b. 在“**规则操作**”列表中，根据需要选择“**允许**”或“**阻止**”选项。

c. 在“**本地端口**”子部分中，指定适用的“端口号或端口范围”。

当您设置端口以建立网络连接时，请注意以下选项和限制。

对于入站连接，您可以为本地设备定义端口设置。对于出站连接，您可以为远程设备定义端口设置。

对于“**端口号**”选项，可用值为 1–65535。

对于“**端口范围**”选项，可用值为 1–10、20–30000 和 1–65535。

端口设置限制如下：

- 要为运行在 Windows XP 下的本地设备设置网络连接，您只能在端口设置中指定一个端口，因为 Windows XP 不支持端口范围设置。
- 要为在 Windows XP 下运行的远程设备设置网络连接，您可以指定“**端口范围**”，但该规则仅适用于定义范围的第一个端口，因为 Windows XP 不支持端口范围设置。

d. 选择应用程序将允许连接的协议类型 (TCP/UDP)。

e. 在“**规则操作**”字段中，指定将为其应用已修改规则的网络地址。

只能使用 IPv4 地址。

8. 在“**应用程序规则**”或“**端口规则**”窗口中，单击“**确定**”。

9. 在“**防火墙管理**”窗口中，单击“**确定**”。

10. 在“**属性：<策略名称>**”窗口中，单击“**确定**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

删除防火墙规则

您只能删除应用程序和端口规则。您无法删除现有组规则。

要删除过滤传入网络流量的现有规则，请执行以下操作：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**网络活动控制**”部分中，单击“**防火墙管理**”子部分中的“**设置**”按钮。
5. 单击打开的窗口中的“**规则列表**”按钮。
   将打开“**入站防火墙规则**”窗口。
6. 根据想要修改其状态的规则类型，选择“**应用程序**”或“**端口**”选项卡。
7. 在规则列表中，选择要删除的规则。
8. 单击“**删除**”按钮。
   将删除所选规则。
9. 在“**入站防火墙规则**”窗口中，单击“**确定**”。
10. 在“**防火墙管理**”窗口中，单击“**确定**”。
11. 在“**属性：<策略名称>**”窗口中，单击“**确定**”。

将保存指定防火墙管理任务设置。新规则参数将发送到 Windows 防火墙。

通过应用程序控制台管理防火墙规则

在本节中，学习如何通过应用程序控制台界面管理防火墙规则。

启用和禁用防火墙规则

要启用或禁用过滤传入网络流量的现有规则，请执行以下操作：

1. 在应用程序控制台树中，展开“**计算机控制**”节点。
2. 选择“**防火墙管理**”子节点。

3. 在“**防火墙管理**”节点的详细信息窗格中，单击“**防火墙规则**”链接。
   将出现“**防火墙规则**”窗口。

4. 根据想要修改其状态的规则类型，单击“**入站**”或“**出站**”链接，然后选择“**应用程序**”或“**端口**”选项卡。

5. 在规则列表中，选择要修改其状态的规则，然后执行以下操作之一：

   - 如果您想要启用已禁用的规则，选中规则名称左侧的复选框。
     将启用所选规则。
   - 如果您想要禁用已启用的规则，清除规则名称左侧的复选框。
     将禁用所选规则。

6. 在“**防火墙规则**”窗口中，单击“**保存**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

手动添加防火墙规则

要添加过滤传入网络流量的新规则或编辑现有规则：

1. 在应用程序控制台树中，展开“**计算机控制**”节点。

2. 选择“**防火墙管理**”子节点。

3. 根据您要配置的连接类型，在“**防火墙管理**”节点的详细信息窗格中，单击“入站或出站连接”链接。

   为入站和出站连接配置规则时，请注意以下选项和限制：

   - 默认情况下，规则类型与策略类型相反。例如，对于默认拒绝策略，规则的默认值设置为“**允许**”。对于默认允许策略，规则的默认值设置为“**阻止**”。您可以根据需要更改规则的类型。
   - 如果将本地应用程序控制台连接到运行任何操作系统的远程设备，或者将本地应用程序控制台连接到运行 Windows 7 或更高版本的本地设备，则可以配置默认任务设置。
   - 如果将本地应用程序控制台连接到运行 Windows 7 以前版本的操作系统的本地设备，则无法配置默认防火墙任务设置。

4. 在出现的窗口中，选择“**应用程序**”或“**端口**”选项卡并执行以下操作之一：

   - 要编辑现有规则，在规则列表中选择要编辑的规则，然后单击“**编辑**”。
   - 要添加新规则，单击“**添加**”。
     根据配置的规则类型，将打开“**应用程序规则**”窗口或“**端口规则**”窗口。

5. 在出现的窗口中，执行以下操作：

   - 如果您使用的是应用程序规则，请执行以下操作：

     a. 在“**规则名称**”字段中，输入所编辑规则的名称。

     b. 在“**规则操作**”列表中，根据需要选择“**允许**”或“**阻止**”选项。

c. 指定您通过修改规则允许其连接的应用程序的可执行文件的“**应用程序路径**”。
您可手动或通过使用“**浏览**”按钮设置路径。

d. 在“**规则操作**”字段中，指定将为其应用已修改规则的网络地址。

只能使用 IPv4 地址。

- 如果您使用的是端口规则，请执行以下操作：

a. 在“**规则名称**”字段中，输入所编辑规则的名称。

b. 在“**规则操作**”列表中，根据需要选择“**允许**”或“**阻止**”选项。

c. 在“**本地端口**”子部分中，根据需要指定“端口号”或“端口范围”。

当您设置端口以建立网络连接时，请注意以下选项和限制。

对于入站连接，您可以为本地设备定义端口设置。对于出站连接，您可以为远程设备定义端口设置。

对于“**端口号**”选项，可用值为 1–65535。

对于“**端口范围**”选项，可用值为 1–10、20–30000 和 1–65535。

端口设置限制如下：

- 要为运行在 Windows XP 下的本地设备设置网络连接，您只能在端口设置中指定一个端口，因为 Windows XP 不支持端口范围设置。
- 要为在 Windows XP 下运行的远程设备设置网络连接，您可以指定“**端口范围**”，但该规则仅适用于定义范围的第一个端口，因为 Windows XP 不支持端口范围设置。

d. 选择应用程序将允许连接的协议类型 (TCP/UDP)。

e. 在“**规则操作**”字段中，指定将为其应用已修改规则的网络地址。

只能使用 IPv4 地址。

6. 在“**应用程序规则**”或“**端口规则**”窗口中，单击“**确定**”。

7. 在“**防火墙规则**”窗口中，单击“**保存**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

删除防火墙规则

您只能删除应用程序和端口规则。您无法删除现有组规则。

要删除过滤传入网络流量的现有规则，请执行以下操作：

1. 在应用程序控制台树中，展开“**计算机控制**”节点。
2. 选择“**防火墙管理**”子节点。
3. 在“**防火墙管理**”节点的详细信息窗格中，单击“**防火墙规则**”链接。
   将出现“**防火墙规则**”窗口。
4. 根据想要修改其状态的规则类型，选择“**应用程序**”或“**端口**”选项卡。
5. 在规则列表中，选择要删除的规则。
6. 单击“**删除**”按钮。
   将删除所选规则。
7. 在“**防火墙规则**”窗口中，单击“**保存**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

通过 Web 插件管理防火墙规则

要通过 Web 插件配置防火墙规则：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**网络活动控制**”部分。
5. 在“**防火墙管理**”子部分中单击“**设置**”。
6. 按下表所述配置设置。

防火墙管理任务设置

设置	描述
应用程序规则	您可管理应用程序规则。 此类型的规则允许指定应用程序的目标网络连接。这些规则的触发条件基于可执行文件的路径。
端口规则	您可管理端口规则。 此类型的规则允许指定端口和协议 (TCP/UDP) 的网络连接。这些规则的触发条件基于端口号和协议类型。
任务管理	您可以配置按计划启动任务的设置。

启用和禁用防火墙规则

要启用或禁用过滤传入网络流量的现有规则，请执行以下操作：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。

2. 单击要配置的策略名称。

3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。

4. 选择“**网络活动控制**”部分。

5. 在“**防火墙管理**”子部分中单击“**设置**”。

6. 根据您要修改其状态的规则的类型，选择“**应用程序规则**”或“**端口规则**”选项卡。

7. 在规则列表中，选择要修改其状态的规则，然后执行以下操作之一：

   - 如果您想要启用已禁用的规则，请开启规则名称左侧的切换按钮。
   - 如果您想要禁用已启用的规则，请关闭规则名称左侧的切换按钮。

8. 单击“**确定**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

手动添加防火墙规则

要添加过滤传入网络流量的新规则或编辑现有规则：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。

2. 单击要配置的策略名称。

3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。

4. 选择“**网络活动控制**”部分。

5. 在“**防火墙管理**”子部分中单击“**设置**”。

6. 根据您要修改其状态的规则的类型，选择“**应用程序入站或出站规则**”选项卡或“**端口入站或出站规则**”选项卡，然后执行以下操作之一：

   为入站和出站连接配置规则时，请注意以下选项和限制：

   - 默认情况下，规则类型与策略类型相反。例如，对于默认拒绝策略，规则的默认值设置为“**允许**”。对于默认允许策略，规则的默认值设置为“**阻止**”。您可以根据需要更改规则的类型。
   - 如果将本地应用程序控制台连接到运行任何操作系统的远程设备，或者将本地应用程序控制台连接到运行 Windows 7 或更高版本的本地设备，则可以配置默认任务设置。
   - 如果将本地应用程序控制台连接到运行 Windows 7 以前版本的操作系统的本地设备，则无法配置默认防火墙任务设置。

   - 要编辑现有规则，请选择要编辑的规则，然后单击“**编辑**”。
   - 要添加新规则，单击“**添加**”。

7. 在屏幕的右侧部分，执行以下操作：

- 如果您使用的是应用程序规则，请执行以下操作：

  a. 如果要应用创建的规则，请选中“**使用规则**”复选框。

  b. 在“**规则名称**”字段中，输入所编辑规则的名称。

  c. 在“**规则操作**”列表中，根据需要选择“**允许**”或“**阻止**”选项。

  d. 指定您通过修改此规则允许其连接的应用程序的可执行文件的“**应用程序路径**”。

  e. 在“**规则应用范围**”字段中，指定将为其应用已修改规则的网络地址。

  只能使用 IPv4 地址。

- 如果您使用的是端口规则，请执行以下操作：

  a. 如果要应用创建的规则，请选中“**使用规则**”复选框。

  b. 在“**规则名称**”字段中，输入所编辑规则的名称。

  c. 指定应用程序将允许连接的“端口号或端口范围”。

  当您设置端口以建立网络连接时，请注意以下选项和限制。

  对于入站连接，您可以为本地设备定义端口设置。对于出站连接，您可以为远程设备定义端口设置。

  对于“**端口号**”选项，可用值为 1–65535。

  对于“**端口范围**”选项，可用值为 1–10、20–30000 和 1–65535。

  端口设置限制如下：

  - 要为运行在 Windows XP 下的本地设备设置网络连接，您只能在端口设置中指定一个端口，因为 Windows XP 不支持端口范围设置。
  - 要为在 Windows XP 下运行的远程设备设置网络连接，您可以指定“**端口范围**”，但该规则仅适用于定义范围的第一个端口，因为 Windows XP 不支持端口范围设置。

  d. 选择应用程序将允许连接的协议类型 (TCP/UDP)。

  e. 在“**规则应用范围**”字段中，指定将为其应用已修改规则的网络地址。

  只能使用 IPv4 地址。

8. 单击“**确定**”。

9. 在“**防火墙管理**”窗口中，单击“**确定**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

删除防火墙规则

> 您只能删除应用程序和端口规则。您无法删除现有组规则。

要删除过滤传入网络流量的现有规则，请执行以下操作：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**网络活动控制**”部分。
5. 在“**防火墙管理**”子部分中单击“**设置**”。
6. 根据您要删除的规则的类型，选择“**应用程序规则**”或“**端口规则**”选项卡。
7. 在规则列表中，选择要删除的规则。
8. 单击“**删除**”按钮。
   将删除所选规则。
9. 单击“**确定**”。

将保存指定任务设置。新规则参数将发送到 Windows 防火墙。

文件完整性监控

本节包含有关启动和配置“文件完整性监控”任务的信息。

关于“文件完整性监控”任务

“文件完整性监控”任务的设计目的是为了跟踪针对任务设置中指定的监控范围内的特定文件和文件夹执行的操作。可以使用该任务来删除可能对受保护设备造成安全入侵的文件更改。还可以配置监控被中断期间要对其进行跟踪的文件更改。

当监控范围暂时位于任务范围之外时（例如，如果任务停止或如果受保护设备上没有物理显示外部设备），会出现*监控中断*。一旦重新连接外部设备，Kaspersky Embedded Systems Security 将报告监控范围内检测到的文件操作。

如果由于重新安装“文件完整性监控”组件造成指定监控范围内的任务停止运行，则不构成监控中断。这种情况下，“文件完整性监控”任务并未运行。

环境要求

要启动“文件完整性监控”任务，必须满足以下条件：

- 受保护设备上必须使用 ReFS 或 NTFS 文件系统。
- 必须启用 Windows USN 日志。组件查询此日志来获取有关文件操作的信息。

  如果为某个卷创建规则后启用了 USN 日志且已启动“文件完整性监控”任务，则必须重启该任务。如果不重启，则监控过程中不会应用该规则。

排除监控范围

您可以创建排除监控范围。排除针对每个单独的规则进行指定，并且仅对指定的监控范围产生作用。可以为每个规则指定无限数量的排除。

排除比监控范围具有更高的优先级，且即使指定的文件夹或文件位于监控范围内，也不受任务的监控。如果其中一个规则的设置指定的监控范围比排除中指定的文件夹具有更低的级别，则当任务运行时将不会考虑监控范围。

要指定排除，可以使用与用于指定监控范围相同的掩码。

关于文件操作监控规则

“文件完整性监控”任务根据文件操作监控规则运行。可以使用规则触发条件来配置触发任务的条件，以及调整任务日志中记录的已删除文件操作事件的重要性级别。

针对每个监控范围指定了文件操作监控规则。

可以配置以下规则触发条件：

- 受信任用户
- 文件操作标记

受信任用户

默认情况下，应用程序将所有操作视为潜在安全入侵。受信任用户列表为空。可以通过在文件操作监控规则设置中创建受信任用户列表来配置事件重要性级别。

*不受信任用户*是分配给监控范围规则设置中的受信任用户列表中未指定的任何用户的状态。如果 Kaspersky Embedded Systems Security 检测到不受信任用户执行的文件操作，则“文件完整性监控”任务将在任务日志中记录一个严重事件。

*受信任用户*是分配给经过授权可在指定的监控范围内执行文件操作的用户或用户组的状态。如果 Kaspersky Embedded Systems Security 检测到受信任用户执行的文件操作，则“文件完整性监控”任务将在任务日志中记录一个“信息事件”。

Kaspersky Embedded Systems Security 在监控中断期间无法确定发起操作的用户。在此情况下，用户状态被确定为未知。

*未知用户*是在由于任务中断或者数据同步驱动程序或 USN 日志失败导致 Kaspersky Embedded Systems Security 无法获取有关用户的数据时分配给用户的状态。如果 Kaspersky Embedded Systems Security 检测到未知用户执行的文件操作，则“文件完整性监控”任务将在任务日志中记录一个“*警告*事件”。

文件操作标记

当“文件完整性监控”任务运行时，Kaspersky Embedded Systems Security 使用文件操作标记来确定已对文件执行了操作。

文件操作标记是可以对文件操作进行特征化的独特描述符。

每个文件操作可以是针对文件进行的单个操作或系列操作。每个此类操作等同于一个文件操作标记。如果您指定作为规则触发条件的标记在文件操作链中被删除，则应用程序将记录一个事件，表示已执行指定的文件操作。

已记录事件的重要性级别不取决于选定的文件操作标记或事件的数量。

默认情况下，Kaspersky Embedded Systems Security 考虑所有可用的文件操作标记。可以在任务规则设置中手动选择文件操作标记。

文件操作标记

文件操作 ID	文件操作标记	支持的文件系统
BASIC_INFO_CHANGE	已更改文件或文件夹的属性或时间标记	NTFS、ReFS
COMPRESSION_CHANGE	已更改文件或文件夹的压缩	NTFS、ReFS
DATA_EXTEND	已更改文件或文件夹的大小	NTFS、ReFS
DATA_OVERWRITE	已覆盖文件或文件夹中的数据	NTFS、ReFS
DATA_TRUNCATION	已截断文件或文件夹	NTFS、ReFS

EA_CHANGE	已更改扩展的文件或文件夹属性	仅限 NTFS
ENCRYPTION_CHANGE	已更改文件或文件夹的加密状态	NTFS、ReFS
FILE_CREATE	首次创建文件或文件夹	NTFS、ReFS
FILE_DELETE	使用 SHIFT+DEL 组合键永久删除的文件或文件夹	NTFS、ReFS
HARD_LINK_CHANGE	已为创建或删除文件或文件夹的硬链接	仅限 NTFS
INDEXABLE_CHANGE	已更改文件或文件夹的索引状态	NTFS、ReFS
INTEGRITY_CHANGE	已更改命名的文件流的完整性属性	仅限 ReFS
NAMED_DATA_EXTEND	已增大命名的文件流的大小	NTFS、ReFS
NAMED_DATA_OVERWRITE	已覆盖命名的文件流	NTFS、ReFS
NAMED_DATA_TRUNCATION	已截断命名的文件流	NTFS、ReFS
OBJECT_ID_CHANGE	已更改文件或文件夹标识符	NTFS、ReFS
RENAME_NEW_NAME	已为文件或文件夹分配新名称	NTFS、ReFS
REPARSE_POINT_CHANGE	已为文件或文件夹创建新的重分析点或更改其现有重分析点	NTFS、ReFS
SECURITY_CHANGE	已更改文件或文件夹访问权限	NTFS、ReFS
STREAM_CHANGE	已创建新的命名的文件流或更改现有命名的文件流	NTFS、ReFS
TRANSACTED_CHANGE	TxF 事务已更改命名的文件流	仅限 ReFS

“文件完整性监控”任务默认设置

默认情况下，“文件完整性监控”任务具有下表所述的设置。您可以在以下组件中更改设置的值：

- 管理插件
- 应用程序控制台
- Web 插件

“文件完整性监控”任务默认设置

设置	默认值	描述
监控范围	未配置	使用该选项指定将监控其操作的文件夹和文件。将针对指定监控范围内的文件夹和文件生成监控事件。
受信任用户列表	未配置	使用该选项指定用户和/或用户组，其在指定文件夹中的操作将被组件视为安全。
记录监控中断期间发生的文件操作信息	已使用	使用该选项启用或禁用在任务未运行期间在指定的监控范围内执行的文件操作的日志记录。 默认情况下，为不受信任和未知的用户和对象编译统计信息。
阻止对 USN 日志的入侵尝试	已使用	使用该选项启用或禁用对 USN 日志的保护。
应用信任区域	已禁用	选中或清除“应用信任区域”复选框以在为规则配置的监控范围之外信任区域排除项。

检测并阻止所选区域中的所有文件操作	已禁用	如果您要阻止所选监控区域的所有更改，则选中或清除“**检测并阻止所选区域中的所有文件操作**”复选框。
从控制中排除以下文件夹	未应用	使用该选项针对无需监控文件操作的文件夹检查排除项的使用情况。当“文件完整性监控”任务运行时，Kaspersky Embedded Systems Security 将跳过指定为排除项的监控范围。
校验和计算	未应用	使用该选项配置对文件进行更改后的文件校验和计算。
设置文件操作标记	考虑所有可用的文件操作标记	使用该选项指定文件操作标记集。如果在监控范围内执行的文件操作被一个或多个指定标记进行过特征化，则 Kaspersky Embedded Systems Security 会生成一个审核事件。
任务启动计划	不设置任务的首次启动计划	您可以配置按计划启动任务的设置。

通过管理插件管理“文件完整性监控”

在本节中，学习如何通过管理插件配置“文件完整性监控”任务。

配置“文件完整性监控”任务

要配置常规“文件完整性监控”任务设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**系统审查**”部分的“**文件完整性监控**”子部分中，单击“**设置**”按钮。
   将打开“**文件完整性监控**”窗口。
5. 在出现的窗口的“**文件操作监控设置**”选项卡中，配置以下设置：
   - 清除或选中“记录监控中断期间发生的文件操作信息”复选框。

当由于任何原因（拆除硬盘驱动器、用户停止任务、软件错误）任务未运行时，该复选框可以启用或禁用“文件完整性监控”设置中指定的文件操作的监控。

如果选中该复选框，则当“文件完整性监控”任务未运行时，Kaspersky Embedded Systems Security 将记录所有监控范围内的事件。

如果清除该复选框，则当任务未运行时，应用程序将不记录监控范围内的文件操作。

默认选中该复选框。

- 清除或选中“阻止对 USN 日志的入侵尝试”复选框。

  该复选框用于启用或禁用对 USN 日志的保护。

  如果选中该复选框，Kaspersky Embedded Systems Security 将阻止删除 USN 日志或破坏 USN 日志内容的尝试。

  如果清除该复选框，则应用程序不会监控对 USN 日志的更改。

  默认选中该复选框。

- 选中或清除适用的“应用信任区域”复选框。

  如果选中“**应用信任区域**”复选框，在**受信任区域**中配置的**排除项**和**受信任进程**将应用到监控范围以及配置的规则。

  如果清除“**应用信任区域**”复选框，在**受信任区域**中配置的**排除项**和**受信任进程**不会应用到监控范围。

  默认下，复选框被清除。

- 添加任务要监控的监控范围。

6. 在“**任务管理**”选项卡上，基于计划配置用于启动任务的任务设置。
7. 单击“**确定**”以保存更改。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关修改设置的日期和时间的信息保存在系统审核日志中。

配置监控规则

要添加监控范围：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**系统审查**”部分的“**文件完整性监控**”子部分中，单击“**设置**”按钮。
   将打开“**文件完整性监控**”窗口。
5. 在“**监控范围**”部分中，单击“**添加**”按钮。
   将打开“**文件操作监控规则**”窗口。
6. 通过以下方式之一添加监控范围：
   - 如果要通过标准的 Microsoft Windows 对话框来选择文件夹：
     a. 单击“**浏览**”按钮。
        将打开标准的 Microsoft Windows“**浏览文件夹**”窗口。
     b. 在打开的**浏览文件夹**窗口中，选择要监控操作的文件夹，然后单击“**确定**”按钮。
   - 如果想要手动指定监控范围，请使用支持的掩码添加路径：
     - <*.ext> - 带有 <ext> 扩展名的所有文件，与其位置无关
     - <*\name.ext> - 带有 <name> 名称和 <ext> 扩展名的所有文件，与其位置无关
     - <\dir*> - 位于 <\dir> 文件夹中的所有文件
     - <\dir*\name.ext> - <\dir> 文件夹及其所有子文件夹中带有 <name> 名称和 <ext> 扩展名的所有文件

当手动指定监控范围时，请确保路径为以下格式：<卷字母>:\<掩码>。如果缺少卷字母，则 Kaspersky Embedded Systems Security 将不会添加指定的监控范围。

7. 在“**受信任用户**”选项卡中，单击“**添加**”按钮。
   将出现标准的 Microsoft Windows“**选择用户或组**”窗口。
8. 选择在选定监控范围中允许其文件操作的用户或用户组，然后单击“**确定**”按钮。

默认情况下，Kaspersky Embedded Systems Security 将未列入受信任用户列表的所有用户视为不受信任，并为他们生成严重事件。对于受信任用户，将编译统计信息。

9. 选择“**文件操作标记**”选项卡。
10. 执行以下操作以选择多个标记（如适用）：
    a. 选择“**基于以下标记检测文件操作**”选项。
    b. 在可用文件操作列表上，选中要监控的操作旁边的复选框。

默认情况下，Kaspersky Embedded Systems Security 将检测所有文件操作标记，已选择“**基于所有可识别的标记检测文件操作**”选项。

11. 如果您要阻止所选区域的所有文件操作，选择“**检测并阻止所选区域中的所有文件操作**”复选框。

12. 如果执行操作后，您想要 Kaspersky Embedded Systems Security 计算文件校验和，请执行以下操作：

    a. 选中**如果可能，计算文件的校验和。该校验和将可在任务日志中查看**复选框中查看。

    b. 在“**校验和类型**”下拉列表中，选择以下选项之一：

    - **MD5 哈希**
    - **SHA256 哈希**

13. 如果您不希望监控所有文件操作，则在可用文件操作列表中，选中要监控的操作旁边的复选框。

14. 添加排除的监控范围（如果适用）：

    a. 选择“**排除**”选项卡。

    b. 选中“**从控制中排除以下文件夹**”复选框。

    c. 单击“**添加**”按钮。
    将打开“**选择要添加的文件夹**”窗口。

    d. 在打开的窗口中，指定要从监控范围中排除的文件夹。

    e. 单击“**确定**”。
    指定的文件夹被添加到排除范围列表。

15. 在“**文件操作监控规则**”窗口中单击“**确定**”。
    指定的规则设置将应用于“文件完整性监控”任务的选定监控范围。

通过应用程序控制台管理“文件完整性监控”

在本节中，学习如何通过应用程序控制台配置“文件完整性监控”任务。

配置“文件完整性监控”任务设置

要配置常规“文件完整性监控”任务设置：

1. 在应用程序控制台树中，展开“**系统审查**”节点。

2. 选择“**文件完整性监控**”子节点。

3. 在“**文件完整性监控**”节点的结果窗格中，单击“**属性**”链接。
   将出现“**任务设置**”窗口。

4. 在所出现窗口的“**常规**”选项卡上，配置以下设置：

    a. 清除或选中“**记录监控中断期间发生的文件操作信息**”复选框。

当由于任何原因（拆除硬盘驱动器、用户停止任务、软件错误）任务未运行时，该复选框可以启用或禁用“文件完整性监控”设置中指定的文件操作的监控。

如果选中该复选框，则当“文件完整性监控”任务未运行时，Kaspersky Embedded Systems Security 将记录所有监控范围内的事件。

如果清除该复选框，则当任务未运行时，应用程序将不记录监控范围内的文件操作。

默认选中该复选框。

b. 清除或选中“阻止对 USN 日志的入侵尝试”复选框。

该复选框用于启用或禁用对 USN 日志的保护。

如果选中该复选框，Kaspersky Embedded Systems Security 将阻止删除 USN 日志或破坏 USN 日志内容的尝试。

如果清除该复选框，则应用程序不会监控对 USN 日志的更改。

默认选中该复选框。

c. 选中或清除适用的“应用信任区域”复选框。

如果选中“**应用信任区域**”复选框，在**受信任区域**中配置的**排除项**和**受信任进程**将应用到监控范围以及配置的规则。

如果清除“**应用信任区域**”复选框，在**受信任区域**中配置的**排除项**和**受信任进程**不会应用到监控范围。

默认下，复选框被清除。

5. 在“**计划**”和“**高级**”选项卡上，配置任务启动计划。

6. 单击“**确定**”以保存更改。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关修改设置的日期和时间的信息保存在系统审核日志中。

配置监控规则

要添加监控范围：

1. 在应用程序控制台树中，展开“**系统审查**”节点。

2. 选择“**文件完整性监控**”子节点。

3. 在“**文件完整性监控**”节点的结果窗格中，单击“**文件操作监控规则**”链接。
   将打开“**文件操作监控**”窗口。

4. 通过以下方式之一添加监控范围：

   - 如果要通过标准的 Microsoft Windows 对话框来选择文件夹：

     a. 在窗口的左侧，单击“**浏览**”按钮。
        将出现标准的 Microsoft Windows“**浏览文件夹**”窗口。

b. 在**浏览文件夹**窗口中，选择要监控操作的文件夹，然后单击**"确定"**按钮。

c. 单击**"添加"**按钮可让 Kaspersky Embedded Systems Security 开始监控指定监控范围内的文件操作。

- 如果想要手动指定监控范围，请使用支持的掩码添加路径：
  - <*.ext> - 带有 <ext> 扩展名的所有文件，与其位置无关
  - <*\name.ext> - 带有 <name> 名称和 <ext> 扩展名的所有文件，与其位置无关
  - <\dir*> - 位于 <\dir> 文件夹中的所有文件
  - <\dir*\name.ext> - <\dir> 文件夹及其所有子文件夹中带有 <name> 名称和 <ext> 扩展名的所有文件

当手动指定监控范围时，请确保路径为以下格式：<卷字母>:\<掩码>。如果缺少卷字母，则 Kaspersky Embedded Systems Security 将不会添加指定的监控范围。

在屏幕的右侧，**"规则描述"**选项卡将显示受信任用户和为此监控范围选定的文件操作标记。

5. 在添加的监控范围列表中，选择您要配置的范围设置。
6. 选择**"受信任用户"**选项卡。
7. 单击**"添加"**按钮。
   将出现标准的 Microsoft Windows**"选择用户或组"**窗口。
8. 选择针对选定的监控范围 Kaspersky Embedded Systems Security 将视为受信任的用户或用户组。
9. 单击**"确定"**。

默认情况下，Kaspersky Embedded Systems Security 将未列入受信任用户列表的所有用户视为不受信任，并为他们生成严重事件。对于受信任用户，将编译统计信息。

10. 选择**"设置文件操作标记"**选项卡。
11. 如果需要，执行以下操作来选择多个标记：
    a. 选择**"基于以下标记检测文件操作"**选项。
    b. 在可用文件操作列表中，选中要监控的操作旁边的复选框。

默认情况下，Kaspersky Embedded Systems Security 将检测所有文件操作标记，即，已选择**"基于所有可识别的标记检测文件操作"**选项。

12. 如果您要阻止所选区域的所有文件操作，选择**"检测并阻止所选区域中的所有文件操作"**复选框。
13. 如果执行操作后，您想要 Kaspersky Embedded Systems Security 计算文件校验和，请执行以下操作：
    a. 在**"校验和计算"**部分中，选中**"如果可能，在文件更改后计算文件最终版本的校验和。该校验和将可在任务日志中查看"**复选框。

b. 在“**使用该算法计算校验和**”下拉列表中，选择以下选项之一：

- **MD5** 哈希。
- **SHA256** 哈希。

14. 添加排除的监控范围（如果适用）：

a. 选择“**设置排除**”选项卡。

b. 选中“考虑排除的监控范围”复选框。

c. 单击“**浏览**”按钮。
将出现标准的 Microsoft Windows“**浏览文件夹**”窗口。

d. 在**浏览文件夹窗口**中，指定要从监控范围中排除的文件夹。

e. 单击“**确定**”。

f. 单击“**添加**”按钮。
指定的文件夹被添加到排除范围列表。

> 您也可以使用与用于指定监控范围相同的掩码来添加排除的监控范围。

15. 单击“**保存**”按钮以应用新的规则配置。

指定的规则设置将立即应用于“**文件完整性监控**”任务定义的监控范围。

通过 Web 插件管理“文件完整性监控”

在本节中，学习如何通过 Web 插件配置“文件完整性监控”任务。

配置“文件完整性监控”任务

要通过 Web 插件配置“文件完整性监控”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**系统审查**”部分。
5. 单击“**文件完整性监控**”子部分中的“**设置**”。
6. 在出现的“**文件完整性监控**”窗口中，在“**文件操作监控设置**”选项卡上配置以下设置：

a. 清除或选中“记录监控中断期间发生的文件操作信息”复选框。

当由于任何原因（拆除硬盘驱动器、用户停止任务、软件错误）任务未运行时，该复选框可以启用或禁用“文件完整性监控”设置中指定的文件操作的监控。

如果选中该复选框，则当“文件完整性监控”任务未运行时，Kaspersky Embedded Systems Security 将记录所有监控范围内的事件。

如果清除该复选框，则当任务未运行时，应用程序将不记录监控范围内的文件操作。

默认选中该复选框。

b. 清除或选中“阻止对 USN 日志的入侵尝试”复选框。

该复选框用于启用或禁用对 USN 日志的保护。

如果选中该复选框，Kaspersky Embedded Systems Security 将阻止删除 USN 日志或破坏 USN 日志内容的尝试。

如果清除该复选框，则应用程序不会监控对 USN 日志的更改。

默认选中该复选框。

c. 选中或清除适用的“应用信任区域”复选框。

如果选中“**应用信任区域**”复选框，在**受信任区域**中配置的**排除项**和**受信任进程**将应用到监控范围以及配置的规则。

如果清除“**应用信任区域**”复选框，在**受信任区域**中配置的**排除项**和**受信任进程**不会应用到监控范围。

默认下，复选框被清除。

7. 在“**任务管理**”选项卡上，配置任务启动计划。

8. 单击“**确定**”以保存更改。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关修改设置的日期和时间的信息保存在系统审核日志中。

配置监控规则

要添加监控范围：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。

2. 单击要配置的策略名称。

3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。

4. 选择“**系统审查**”部分。

5. 单击“**文件完整性监控**”子部分中的“**设置**”。

6. 在出现的“**文件完整性监控**”窗口中，打开“**文件操作监控设置**”选项卡。

7. 在“**USN 日志**”部分中，单击“**添加**”按钮。
将出现“**文件操作监控规则**”窗口。

8. 在“**监控该范围的文件操作**”中，使用受支持的掩码指定路径：

   - <*.ext> - 带有 <ext> 扩展名的所有文件，与其位置无关
   - <*\name.ext> - 带有 <name> 名称和 <ext> 扩展名的所有文件，与其位置无关
   - <\dir*> - 位于 <\dir> 文件夹中的所有文件
   - <\dir*\name.ext> - <\dir> 文件夹及其所有子文件夹中带有 <name> 名称和 <ext> 扩展名的所有文件

   当手动指定监控范围时，请确保路径为以下格式：<卷字母>:\<掩码>。如果缺少卷字母，则 Kaspersky Embedded Systems Security 将不会添加指定的监控范围。

9. 在“**受信任用户**”选项卡上，执行以下操作之一：

   - 单击“**添加**”按钮，然后在打开的窗口的“**用户名**”字段中，使用 SID 表示法指定用户。
   - 单击“**从管理服务器添加**”按钮，然后在屏幕上出现的窗口中，从列表中选择用户。

   默认情况下，Kaspersky Embedded Systems Security 将未列入受信任用户列表的所有用户视为不受信任，并为他们生成严重事件。对于受信任用户，将编译统计信息。

10. 单击“**确定**”。

11. 选择“**文件操作标记**”选项卡。

12. 执行以下操作以选择多个标记（如适用）：

    a. 选择“**基于以下标记检测文件操作**”选项。

    b. 在可用文件操作列表上，选中要监控的操作旁边的复选框。

    默认情况下，Kaspersky Embedded Systems Security 将检测所有文件操作标记，已选择“**基于所有可识别的标记检测文件操作**”选项。

13. 如果您要阻止所选区域的所有文件操作，选择“**检测并阻止所选区域中的所有文件操作**”复选框。

14. 如果执行操作后，您想要 Kaspersky Embedded Systems Security 计算文件校验和，请执行以下操作：

    a. 选中**如果可能，计算文件的校验和。该校验和将可在任务日志中查看**复选框中查看。

    b. 在“**校验和类型**”下拉列表中，选择以下选项之一：

    - **SHA256 哈希**
    - **MD5 哈希**

15. 如果您不希望监控所有文件操作，则在可用文件操作列表中，选中要监控的操作旁边的复选框。

16. 添加排除的监控范围（如果适用）：

a. 选择“**排除**”选项卡。

b. 选中“**从控制中排除以下文件夹**”复选框。

c. 单击“**添加**”按钮。
将打开“**选择要添加的文件夹**”窗口。

d. 在右侧打开的窗格中，指定要从监控范围中排除的文件夹。

e. 单击“**确定**”。
指定的文件夹被添加到排除范围列表。

17. 在“**文件操作监控规则**”窗口中单击“**确定**”。
指定的规则设置将应用于“文件完整性监控”任务的选定监控范围。

AMSI 扫描程序

本节包含有关“AMSI 扫描器”任务以及如何配置它的信息。

关于 AMSI 扫描程序任务

当“AMSI 扫描器”任务运行时，Kaspersky Embedded Systems Security 控制使用 Microsoft Windows 脚本技术 (Active Scripting)（例如 VBScript 或 JScript®）创建的脚本的执行。该应用程序还可以处理 PowerShell™ 脚本和在安装了反恶意软件扫描接口 (AMSI) 的操作系统上的 Microsoft Office 应用程序中运行的脚本。您可以允许或阻止执行已被发现危险或可能危险的脚本。如果 Kaspersky Embedded Systems Security 将脚本识别为潜在危险，它会根据您选择的操作阻止或允许执行该脚本。如果选择“**阻止**”操作，则应用程序仅在发现脚本安全时才允许执行脚本。

从 Microsoft Windows 10 和 Microsoft Windows Server 2016 操作系统开始，Kaspersky Embedded Systems Security 支持反恶意软件扫描接口 (AMSI)。AMSI 允许应用程序和服务与安装在设备上的任何反恶意软件应用程序集成，以便反恶意软件拦截和扫描所有执行的脚本。

您可以在 Microsoft Windows 网站 上找到有关 AMSI 功能的更多信息。

您可以配置“AMSI 扫描器”任务设置。

默认 AMSI 扫描程序任务设置

“AMSI 扫描器”本地系统任务使用下表描述的默认设置。您可以更改这些设置的值。

默认“AMSI 扫描器”任务设置

设置	默认值	描述
对疑似危险脚本执行的操作	**阻止**	您可以指定在检测到可能存在危险的脚本时要执行的操作：阻止或允许执行该脚本。
启发式分析	应用“**中度**”安全级别。	可以启用或禁用启发式分析。可以配置分析级别。
受信任区域	已使用	可以在选定任务中使用的常规排除列表。

通过管理插件配置 AMSI 扫描程序任务设置

要配置“AMSI 扫描器”任务：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**属性：<策略名称>**”窗口的“**实时服务器保护**”部分中，单击“**AMSI 扫描器**”的“**设置**”。
5. 在“**常规**”选项卡上的“**对疑似危险脚本执行的操作**”部分中，执行以下操作之一：
   - 要允许执行可能存在危险的脚本，请选择“**允许**”。
   - 要阻止执行可能存在危险的脚本，请选择“**阻止**”。
6. 在“**启发式分析**”部分中，执行以下操作之一：
   - 清除或选中“**使用启发式分析**”复选框。
   - 如有必要，使用滑块调整分析级别。
7. 在“**受信任区域**”部分，选中或清除“**应用信任区域**”复选框。
8. 单击“**确定**”。

将应用新配置的设置。

通过应用程序控制台配置 AMSI 扫描程序任务设置

要配置“AMSI 扫描器”任务：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**AMSI 扫描器**”子节点。
3. 在节点的结果窗格中，单击“**属性**”链接。
   将打开“**常规**”选项卡上的“**任务设置**”窗口。
4. 在“**对疑似危险脚本执行的操作**”部分中，执行以下操作之一：
   - 要允许执行可能存在危险的脚本，请选择“**允许**”。
   - 要禁止执行可能存在危险的脚本，请选择“**阻止**”。
5. 在“**启发式分析**”部分中，执行以下操作之一：
   - 清除或选中“**使用启发式分析**”复选框。
   - 如有必要，使用滑块调整分析级别。
6. 在“**受信任区域**”部分，选中或清除“**应用信任区域**”复选框。
7. 单击“**确定**”。

将应用新配置的设置。

通过 Web 插件配置 AMSI 扫描程序任务设置

要配置“AMSI 扫描器”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时服务器保护**”部分。
5. 在“**AMSI 扫描器**”子部分中单击“**设置**”。
6. 在“**常规**”选项卡上的“**对疑似危险脚本执行的操作**”部分中，执行以下操作之一：
   - 要允许执行可能存在危险的脚本，请选择“**允许**”。
   - 要阻止执行可能存在危险的脚本，请选择“**阻止**”。
7. 在“**启发式分析**”部分中，执行以下操作之一：
   - 清除或选中“**使用启发式分析**”复选框。
   - 如有必要，调整“启发式分析的级别”。
8. 在“**受信任区域**”部分，选中或清除“**应用信任区域**”复选框。
9. 单击“**确定**”。

将应用新配置的设置。

AMSI 扫描程序任务统计

当“**AMSI 扫描器**”任务运行时，您可以查看有关 Kaspersky Embedded Systems Security 自任务启动时起处理的脚本数量的信息。

要查看“AMSI 扫描器”任务统计信息：

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**AMSI 扫描器**”子节点。

当前任务统计显示在“**管理**”和“**统计**”部分的节点的结果窗格中。

您可以查看自任务启动以来 Kaspersky Embedded Systems Security 已处理对象的相关信息（请参见下表）。

AMSI 扫描程序任务统计

字段	描述
已阻止的脚本	被 Kaspersky Embedded Systems Security 阻止的脚本数量。

检测到的危险脚本	检测到的危险脚本数量。
检测到的疑似危险脚本	检测到的可能存在危险的脚本的数量。
已处理的脚本	已处理的脚本总数。

注册表访问监控

该部分阐述了如何启动和配置注册表访问监控任务。

关于注册表访问监控任务

“注册表访问监控”任务的设计目的是为了跟踪针对任务设置中定义的监控范围内的特定注册表分支和注册表项执行的操作。该任务跟踪安装在设备上的操作系统内或在监控范围内定义的 Windows Server 2016 及更高版本容器内的操作。可以使用该任务来检测可能对受保护设备造成安全入侵的更改。

要启动“注册表访问监控”任务，您必须配置至少一个监控规则。

关于系统注册表监控规则

“**注册表访问监控**”任务根据系统注册表监控规则运行。可以使用规则触发条件来配置触发任务的条件，以及设置任务日志中记录的已检测事件的重要级别。

针对每个监控范围指定了系统注册表监控规则。

可以配置以下规则触发条件：

- **操作**
- **注册表值**
- **受信任用户**

操作

当注册表访问监控任务启动时，Kaspersky Embedded Systems Security 使用操作列表以监控注册表（参见下表）。

如果检测到指定为规则触发条件的操作，应用程序将记录相应的事件。

已记录事件的重要级别不取决于选定的操作或事件的数量。

默认下，Kaspersky Embedded Systems Security 考虑所有操作。您可以在任务规则设置中手动配置操作列表。

操作

操作	限制	操作系统
创建键	• 对于 Windows XP 和 Windows Server 2003，如果您将**创建键**添加到**操作**列表中，然后选择**根据规则阻止操作**模式，则由于系统限制，不会在指定的操作系统中阻止密钥创建。创建密钥时会向事件日志发送相应的通知。	Windows XP 及更高版本

	• 如果要禁止通过注册表编辑器创建特定键，请为父注册表键创建规则，并确保将**创建子键**添加到**操作**列表中，然后选择**根据规则阻止操作**模式。	
删除键	如果您要删除父键，请确保清除已配置注册表键的受监控**操作**列表上的“**删除键**”和“**删除子键**”选项，因为您只能删除带有子键的父键。	Windows XP 及更高版本
重命名键	N/A	Windows XP 及更高版本
更改键安全设置	N/A	Windows Vista 及更高版本
删除值	N/A	Windows XP 及更高版本
设置值	如果您将**设置值**添加到**操作**列表中，在规则中为键定义默认**值名称**，然后选择**根据规则阻止操作**模式，则不会创建键，因为只能使用默认值创建新键。	Windows XP 及更高版本
创建子键	N/A	Windows XP 及更高版本
删除子键	N/A	Windows XP 及更高版本
重命名子键	N/A	Windows XP 及更高版本
更改子键安全设置	N/A	Windows Vista 及更高版本

注册表值

除了注册表键监控之外，您还可以阻止或监控现有注册表值的更改。有以下选项可用：

- **设置值** - 创建新注册表值或更改现有注册表值。
- **删除值** - 删除现有注册表值。

> 重命名和更改安全设置不适用于注册表值。

受信任用户

默认情况下，应用程序将所有操作视为潜在安全入侵。受信任用户列表为空。可以通过在系统注册表监控规则设置中创建受信任用户列表来配置事件重要性级别。

*不受信任用户*是监控范围规则设置中的受信任用户列表中未指定的任何用户。如果 Kaspersky Embedded Systems Security 检测到不受信任用户执行的操作，则“注册表访问监控”任务将在任务日志中记录一个严重事件。

*受信任用户*是经过授权可在指定的监控范围内执行操作的用户或用户组。如果 Kaspersky Embedded Systems Security 检测到受信任用户执行的操作，则“注册表访问监控”任务将在任务日志中记录一个“信息事件”。

默认注册表访问监控任务设置

“注册表访问监控”任务的默认设置在下表中描述。您可以在以下组件中更改设置的值：

- 管理插件
- 应用程序控制台
- Web 插件

默认注册表访问监控任务设置

设置	默认值	描述
监控范围	未定义	使用该选项定义要监视的父注册表键和子键。该设置是强制性的。如果不定义设置，任务将无法启动。为指定监控范围内的父注册表键和子键生成监控事件。
操作	将选择操作列表中的所有项目	使用该选项通过选择并清除相应的复选框来配置操作列表（如适用）。
注册表值	未定义	使用该选项为定义的监控范围添加、修改和删除要监控的注册表值。
受信任用户	未定义	使用该选项指定有权对指定注册表键执行定义操作的用户和用户组。
任务模式	仅统计	您可以选择任务模式来**根据规则阻止操作**，也可以选择**仅统计**模式来接收通知。
应用信任区域	已禁用	您还可以选中或清除“**应用信任区域**”复选框以在为规则配置的监控范围之外**信任区域**排除项。
任务启动计划	未定义	您可以配置按计划启动任务的设置。

通过管理插件管理“注册表访问监控”

在本节中，了解如何通过管理插件配置“注册表访问监控”任务。

配置注册表访问监控任务设置

要配置常规注册表访问监控任务设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**系统审查**”部分的“**注册表访问监控**”子部分中，单击“**设置**”按钮。

   注册表访问监控窗口出现。
5. 在“**注册表访问监控设置**”选项卡上，配置以下设置：
   - 在**任务模式**组，从列表选择所需的选项：
     - 根据规则阻止操作

       如果您选择**根据规则阻止操作**模式，Kaspersky Embedded Systems Security 阻止为监控范围定义的**操作**。而且，如果选择了**应用信任区域**复选框，Kaspersky Embedded Systems Security 不阻止在**受信任区域**下定义的进程。

       默认下，**仅统计**模式被应用。
     - 仅统计

       如果为监控范围选择了**仅统计**模式，Kaspersky Embedded Systems Security 编译根据配置的规则收集注册表键操作的统计信息。而且，如果选择了**应用信任区域**复选框，Kaspersky Embedded Systems Security 不编译在**受信任区域**下定义的进程的统计信息。

       默认下，**仅统计**模式被应用。
   - 选中或清除适用的“**应用信任区域**”复选框。

     如果选中了**应用信任区域**复选框，在**受信任区域**中配置的**受信任进程**被应用到监控范围以及配置的规则。

     如果清空了**应用信任区域**复选框，在**受信任区域**中配置的**受信任进程**不被应用到监控范围。

     默认下，复选框被清除。
6. 添加任务要监控的监控范围。
7. 在“**任务管理**”选项卡上，配置任务的计划设置。
8. 单击“**确定**”以保存更改。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关修改设置的日期和时间的信息保存在系统审核日志中。

配置监控规则

监控规则会根据在已配置规则列表中的位置逐个应用。

要添加监控范围：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“属性：<策略名称>”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“应用程序设置”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**系统审查**”部分的“**注册表访问监控**”子部分中，单击“**设置**”按钮。
   注册表访问监控窗口出现。
5. 在**监控以下范围的注册表操作**部分，单击**添加**按钮。
6. 在**注册表访问监控区域**窗口，要添加监控范围，使用支持的掩码指定路径。

输入路径时，您可以使用 ? 和 * 作为掩码。

如果您输入路径到根注册表键，请确保指定没有掩码的完整路径，例如 HKEY_USERS。以下是有效的根注册表键列表：

- HKEY_LOCAL_MACHINE
- HKLM
- HKEY_CURRENT_USER
- HKCU
- HKEY_USERS
- HKUS
- HKU
- HKEY_CURRENT_CONFIG
- HKEY_CLASSES_ROOT
- HKCR

在创建规则时，避免对根键使用支持的掩码。
如果您仅指定根键（如 HKEY_CURRENT_USER），或对所有子键使用掩码的根键（如 HKEY_CURRENT_USER*），则将生成大量关于指定子键的通知，这将导致系统性能问题。如果您指定根键，例如 HKEY_CURRENT_USER，或对所有子键使用掩码的根键，例如 HKEY_CURRENT_USER*，并选择**根据规则阻止操作**模式，则系统无法读取或更改系统功能所需的键并无法响应。

7. 在**添加**选项卡，配置适用的操作列表。
8. 如果您要监视特定**注册表值**，请执行以下操作：
   - 在“**注册表值**”选项卡中，单击“**添加**”按钮。
   - 在**注册表值规则**窗口，输入**受控制的操作**并设置**受控制的操作**。
   - 单击“**确定**”以保存更改。
9. 如果您要定义**受信任用户**，请执行以下操作：
   - 在“**受信任用户**”选项卡中，单击“**添加**”按钮。
   - 在**选择用户或组**窗口，选择被授权执行定义操作的用户或用户组。
   - 单击“**确定**”以保存更改。

默认情况下，Kaspersky Embedded Systems Security 将未列入受信任用户列表的所有用户视为不受信任，并为他们生成严重事件。对于受信任用户，将编译统计信息。

10. 在“**注册表访问监控区域**”中单击“**确定**”。

指定的规则设置被立即应用于“**注册表访问监控**”任务定义的监控范围。

通过管理控制台管理“注册表访问监控”

在本节中，学习如何通过应用程序控制台配置“注册表访问监控”任务。

配置注册表访问监控任务设置

要配置常规注册表访问监控任务设置：

1. 在应用程序控制台树中，展开“**系统审查**”节点。
2. 选择“**注册表访问监控**”子节点。
3. 在“**注册表访问监控**”节点的结果窗格中，单击“**属性**”链接。
   将出现“**任务设置**”窗口。
4. 在“**任务设置**”窗口的“**常规**”选项卡上，配置以下设置：
   - 在**任务模式**组，从列表选择所需的选项：
     - 根据规则阻止操作

       如果您选择**根据规则阻止操作**模式，Kaspersky Embedded Systems Security 阻止为监控范围定义的**操作**。而且，如果选择了**应用信任区域**复选框，Kaspersky Embedded Systems Security 不阻止在**受信任区域**下定义的进程。

       默认下，**仅统计**模式被应用。

     - 仅统计

       如果为监控范围选择了**仅统计**模式，Kaspersky Embedded Systems Security 编译根据配置的规则收集注册表键操作的统计信息。而且，如果选择了**应用信任区域**复选框，Kaspersky Embedded Systems Security 不编译在**受信任区域**下定义的进程的统计信息。

       默认下，**仅统计**模式被应用。

   - 选中或清除适用的“应用信任区域”复选框。

如果选中了**应用信任区域**复选框，在**受信任区域**中配置的**受信任进程**被应用到监控范围以及配置的规则。

如果清空了**应用信任区域**复选框，在**受信任区域**中配置的**受信任进程**不被应用到监控范围。

默认下，复选框被清除。

5. 在“**计划**”和“**高级**”选项卡上，配置任务启动计划。

6. 单击“**确定**”以保存更改。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关修改设置的日期和时间的信息保存在系统审核日志中。

配置监控规则

监控规则会根据在已配置规则列表中的位置逐个应用。

要添加监控范围：

1. 在应用程序控制台树中，展开“**系统审查**”节点。

2. 选择“**注册表访问监控**”子节点。

3. 在“**注册表访问监控**”节点的结果窗格中，单击“**注册表访问监控规则**”链接。
   注册表访问监控窗口出现。

4. 在**注册表访问监控**窗口，使用支持的掩码指定路径以**添加系统注册表以监控**并单击**添加**按钮。

   创建规则时，避免对根键使用支持的掩码。
   如果您仅指定根键（如 HKEY_CURRENT_USER），或对所有子键使用掩码的根键（如 HKEY_CURRENT_USER*），将生成大量有关寻址指定子键的通知，这会导致系统性能问题。
   如果您指定根键（如 HKEY_CURRENT_USER），或对所有子键使用掩码的根键（如 HKEY_CURRENT_USER*），并选择了**根据规则阻止操作**模式，则系统无法读取或更改操作系统运行所需的键，并且无法响应。

5. 在所选监控区域的“**操作**”选项卡上，根据需要配置操作列表。

6. 如果您要监视特定**注册表值**，请执行以下操作：

   a. 在“**注册表值**”选项卡中，单击“**添加**”按钮。

   b. 在**注册表值规则**窗口，输入**受控制的操作**并设置所需的**受控制的操作**。

   c. 单击“**确定**”以保存更改。

7. 如果您要定义**受信任用户**，请执行以下操作：

   a. 在“**受信任用户**”选项卡中，单击“**添加**”按钮。

b. 在**选择用户或组**窗口，选择被授权执行定义操作的用户或用户组。

c. 单击“**确定**”以保存更改。

默认情况下，Kaspersky Embedded Systems Security 将未列入受信任用户列表的所有用户视为不受信任，并为他们生成严重事件。对于受信任用户，将编译统计信息。

8. 在“**注册表访问监控区域**”中单击“**保存**”。
指定的规则设置被立即应用于“**注册表访问监控**”任务定义的监控范围。

通过 Web 插件管理“注册表访问监控”

在本节中，学习如何通过 Web 插件配置“注册表访问监控”任务。

配置注册表访问监控任务

要通过 Web 插件配置“注册表访问监控”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**系统审查**”部分。
5. 单击“**注册表访问监控**”子部分中的“**设置**”。
6. 在**注册表访问监控**窗口中，在**注册表访问监控设置**选项卡上，配置以下设置：
   - 在**任务模式**组，从列表选择所需的选项：
     - 根据规则阻止操作

       如果您选择**根据规则阻止操作**模式，Kaspersky Embedded Systems Security 阻止为监控范围定义的**操作**。而且，如果选择了**应用信任区域**复选框，Kaspersky Embedded Systems Security 不阻止在**受信任区域**下定义的进程。

       默认下，**仅统计**模式被应用。

     - 仅统计

       如果为监控范围选择了**仅统计**模式，Kaspersky Embedded Systems Security 编译根据配置的规则收集注册表键操作的统计信息。而且，如果选择了**应用信任区域**复选框，Kaspersky Embedded Systems Security 不编译在**受信任区域**下定义的进程的统计信息。

       默认下，**仅统计**模式被应用。

- 选中或清除适用的“应用信任区域”复选框。

  如果选中了**应用信任区域**复选框，在**受信任区域**中配置的**受信任进程**被应用到监控范围以及配置的规则。

  如果清空了**应用信任区域**复选框，在**受信任区域**中配置的**受信任进程**不被应用到监控范围。

  默认下，复选框被清除。

7. 在“**任务管理**”选项卡上，配置任务启动计划。

8. 单击“**确定**”以保存更改。

Kaspersky Embedded Systems Security 将对正在运行的任务立即应用新设置。有关修改设置的日期和时间的信息保存在系统审核日志中。

配置监控规则

监控规则会根据在已配置规则列表中的位置逐个应用。

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。

2. 单击要配置的策略名称。

3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。

4. 选择“**系统审查**”部分。

5. 单击“**注册表访问监控**”子部分中的“**设置**”。

6. 在出现的“**注册表访问监控**”窗口中，打开“**注册表访问监控设置**”选项卡。

7. 在“**注册表访问监控规则**”部分中，单击“**添加**”按钮。

8. 在**注册表访问监控区域**窗口，使用支持的掩码指定路径来**监控以下范围的注册表操作**。

输入路径时，您可以使用 ? 和 * 作为掩码。

如果您输入路径到根注册表键，请确保指定没有掩码的完整路径，例如 HKEY_USERS。以下是有效的根注册表键列表：

- HKEY_LOCAL_MACHINE
- HKLM
- HKEY_CURRENT_USER
- HKCU
- HKEY_USERS
- HKUS
- HKU
- HKEY_CURRENT_CONFIG
- HKEY_CLASSES_ROOT
- HKCR

创建规则时，避免对根键使用支持的掩码。
如果您仅指定根键（如 HKEY_CURRENT_USER），或对所有子键使用掩码的根键（如 HKEY_CURRENT_USER*），将生成大量有关寻址指定子键的通知，这会导致系统性能问题。
如果您指定根键（如 HKEY_CURRENT_USER），或对所有子键使用掩码的根键（如 HKEY_CURRENT_USER*），并选择了**根据规则阻止操作**模式，则系统无法读取或更改操作系统运行所需的键，并且无法响应。

9. 在所选监控区域的“**操作**”选项卡上，根据需要配置操作列表。
10. 如果您要监视特定**注册表值**，请执行以下操作：
    a. 在“**注册表值**”选项卡中，单击“**添加**”按钮。
    b. 在**注册表值规则**窗口，输入**值掩码**并设置所需的**操作列表**。
    c. 单击“**确定**”以保存更改。
11. 如果您要定义**受信任用户**，请执行以下操作：
    a. 在“**受信任用户**”选项卡中，单击“**添加**”按钮。
    b. 输入**用户名**或单击**设置 SID Everyone**， 以定义有权执行所选操作的用户。
    c. 单击“**确定**”以保存更改。

默认情况下，Kaspersky Embedded Systems Security 将未列入受信任用户列表的所有用户视为不受信任，并为他们生成严重事件。对于受信任用户，将编译统计信息。

12. 在“**注册表访问监控区域**”中单击“**确定**”以保存更改。

    指定的规则设置被立即应用于“**注册表访问监控**”任务定义的监控范围。

日志审查

本节包含有关“日志审查”任务和任务设置的信息。

关于“日志审查”任务

当“日志审查”任务运行时，Kaspersky Embedded Systems Security 将根据 Windows 事件日志的审查结果监控受保护环境的完整性。应用程序在检测到可能表示尝试进行物理攻击的异常行为时会通知管理员。

Kaspersky Embedded Systems Security 会分析 Windows 事件日志，并根据用户指定的规则或启发式分析的设置（任务用它来审查日志）来识别入侵。

预定义规则和启发式分析

通过应用基于现有启发的预定义规则，可以使用“日志审查”任务来监控受保护系统的状态。启发式分析可识别受保护设备上的异常活动，这些异常活动可作为尝试攻击的证据。用于识别异常行为的模板包括在预定义规则设置中的可用规则内。

“日志审查”任务的规则列表中包含七条规则。您可以启用或禁用任一规则。不能删除现有规则或创建新规则。

可以为监控以下操作事件的规则配置触发条件：

- 密码暴力破解检测
- 网络登录检测

还可在任务设置中配置排除。当登录由受信任用户执行或从受信任的 IP 地址执行时，不会激活启发式分析。

如果任务不使用启发式分析，则 Kaspersky Embedded Systems Security 不会使用启发来审查 Windows 日志。默认情况下，启用启发式分析。

当应用规则时，应用程序将在“日志审查”任务日志中记录一个*严重事件*。

自定义日志审查任务的规则

可以使用规则设置来指定和更改在 Windows 日志中检测到选定事件时的触发规则条件。默认情况下，日志审查规则的列表包含四条规则。您可以启用和禁用这些规则、删除规则以及编辑规则设置。

可以为每种规则配置以下规则触发条件：

- Windows 事件日志中的记录标识符列表。

  如果事件属性包含规则中指定的事件标识符，则当在 Windows 事件日志中创建新的记录时将触发该规则。也可以为每个指定的规则添加和删除标识符。

- 事件源。

  对于每条规则，都可以在 Windows 事件日志内定义一个日志。应用程序将仅在此日志中搜索带有指定事件标识符的记录。您可以选择其中一个标准日志（应用程序、安全性或系统）或在源选择字段中输入名称来指定自定义日志。

应用程序不会验证指定的日志是否确实存在于 Windows 事件日志中。

触发规则后，Kaspersky Embedded Systems Security 将在“日志审查”任务日志中记录一个严重事件。

默认情况下，日志审查任务应用自定义规则。

在启动“日志审查”任务前，请确保系统系统审核日志策略已正确设置。有关详细信息，请参见 Microsoft 文章。

“日志审查”任务默认设置

默认情况下，“日志审查”任务具有下表所述的设置。您可以更改这些设置的值。

“日志审查”任务默认设置

设置	默认值	描述
应用日志审查的自定义规则	未应用。	您可以启用、禁用、添加或修改自定义规则。
针对日志审查应用预定义规则	已应用。	您可以启用或禁用启发式分析，它可以检测受保护设备上的异常活动。
暴力破解攻击检测	每 300 秒 10 次登录失败。	您可以设置尝试次数和使用的时间范围，这将被视为启发式分析的触发器。
网络登录	上午 12:00:00。	您可以指定时间间隔的开始和结束时间，在此时间间隔中 Kaspersky Embedded Systems Security 将登录尝试视为异常活动。
排除	未应用。	您可以指定不会触发启发式分析的用户和 IP 地址。
任务启动计划	不设置任务的首次启动计划。	您可以配置按计划启动任务的设置。

通过管理插件管理日志审查规则

在本节中，学习如何通过管理插件添加和配置日志审查规则。

配置预定义任务规则

执行以下操作为“日志审查”任务配置预定义规则：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：

- 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
- 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

> 如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。

4. 在“**系统审查**”部分中，单击“**日志审查**”子部分中的“**设置**”按钮。
   将打开“**日志审查**”窗口。
5. 选择“**预定义规则**”选项卡。
6. 选中或清除“针对日志审查应用预定义规则”复选框。

> 为了能够运行任务，必须选择至少一种日志审查规则。

7. 从预定义规则列表中选择要应用的规则：
   - 系统中存在可能的暴力破解攻击的模式。
   - 系统中存在可能的 Windows 事件日志滥用的模式。
   - 检测到表示已安装新服务的异常活动。
   - 检测到使用显式凭证的异常登录。
   - 系统中存在可能的 Kerberos 伪造 PAC (MS14-068) 攻击的模式。
   - 检测到特权内置组 Administrators 发出的异常操作。
   - 在网络登录会话期间检测到异常活动。
8. 要配置选定规则，请单击“**高级设置**”按钮。
   将打开“**日志审查**”窗口。
9. 在“**暴力破解攻击检测**”部分中，设置用作启发式分析触发器的尝试次数和时间范围。
10. 在“**网络登录检测**”部分中，指定时间间隔的开始和结束时间，在此时间间隔中 Kaspersky Embedded Systems Security 将登录尝试视为异常活动。
11. 选择“**排除**”选项卡。
12. 执行以下操作添加受信任用户：
    a. 单击“**浏览**”按钮。
    b. 选择用户。
    c. 单击“**确定**”。
       选定的用户将被添加到受信任用户列表中。
13. 执行以下操作添加受信任的 IP 地址：

a. 输入 IP 地址。

b. 单击“**添加**”按钮。

14. 输入的 IP 地址将被添加到受信任的 IP 地址列表中。

15. 在“**任务管理**”选项卡上，配置任务启动计划。

16. 在“**日志审查**”窗口中单击“**确定**”。

保存日志审查任务配置。

通过管理插件添加日志审查规则

执行以下操作可添加和配置新的自定义日志审查规则：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单台受保护设备配置应用程序，请选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。

     如果某个活动 Kaspersky Security Center 策略已应用于设备，并且该策略阻止对应用程序设置的更改，则无法在“**应用程序设置**”窗口中编辑这些设置。
4. 在“**系统审查**”部分中，单击“**日志审查**”子部分中的“**设置**”按钮。
   将打开“**日志审查**”窗口。
5. 在“**自定义规则**”选项卡上，选中或清除“**应用日志审查的自定义规则**”选项卡。

   可以控制是否对日志审查应用预设的规则。选择您要对日志审查应用的规则所对应的复选框。
6. 要添加新的自定义规则，请单击“**添加**”按钮。
   将打开“**自定义日志审查规则**”窗口。
7. 在“**常规**”部分中，指定有关新规则的以下信息：
   - **规则名称**
   - **当 Windows 事件日志中出现新条目时，如果在事件参数中发现指定的标识符(ID)，将触发规则**
8. 在“**触发条件**”部分中，指定将触发规则的事件 ID：

   a. 输入 ID。

   b. 单击“**添加**”按钮。

输入的事件 ID 将添加到列表中。可以为每个规则添加无限数量的标识符。

9. 单击“**确定**”。
日志审查规则即添加到规则列表中。

通过应用程序控制台管理日志审查规则

在本节中，学习如何通过应用程序控制台添加和配置日志审查规则。

配置预定义任务规则

执行以下操作可以为日志审查任务配置启发式分析：

1. 在应用程序控制台树中，展开“**系统审查**”节点。
2. 选择“**日志审查**”子节点。
3. 在“**日志审查**”节点的结果窗格中，单击“**属性**”链接。
将打开“**任务设置**”窗口。
4. 选择“**预定义规则**”选项卡。
5. 选中或清除“针对日志审查应用预定义规则”复选框。

> 为了能够运行任务，必须选择至少一种日志审查规则。

6. 从预定义规则列表中选择要应用的规则：
   - 系统中存在可能的暴力破解攻击的模式。
   - 系统中存在可能的 Windows 事件日志滥用的模式。
   - 检测到表示已安装新服务的异常活动。
   - 检测到使用显式凭证的异常登录。
   - 系统中存在可能的 Kerberos 伪造 PAC (MS14-068) 攻击的模式。
   - 检测到特权内置组 Administrators 发出的异常操作。
   - 在网络登录会话期间检测到异常活动。
7. 要配置选定的规则，请转至“**扩展**”选项卡。
8. 在“**暴力破解攻击检测**”部分中，设置用作启发式分析触发器的尝试次数和时间范围。
9. 在“**网络登录**”部分中，指定时间间隔的开始和结束时间，在此时间间隔中 Kaspersky Embedded Systems Security 将登录尝试视为异常活动。

10. 选择“**排除**”选项卡。
11. 执行以下操作添加受信任用户：
    a. 单击“**浏览**”按钮。
    b. 选择用户。
    c. 单击“**确定**”。
    选定的用户将被添加到受信任用户列表中。
12. 执行以下操作添加受信任的 IP 地址：
    a. 输入 IP 地址。
    b. 单击“**添加**”按钮。
    输入的 IP 地址将被添加到受信任的 IP 地址列表中。
13. 选择“**计划**”和“**高级**”选项卡以配置任务启动计划。
14. 在“**任务设置**”窗口中单击“**确定**”。
    保存日志审查任务配置。

通过应用程序控制台添加日志审查规则

要添加和配置新的自定义日志审查规则：

1. 在应用程序控制台树中，展开“**系统审查**”节点。
2. 选择“**日志审查**”子节点。
3. 在“**日志审查**”节点的结果窗格中，单击“**日志审查规则**”链接。
4. 将打开“**日志审查规则**”窗口。
5. 选中或清除对日志审查应用自定义规则。在选中此复选框之前，不应用已配置的规则复选框。

   可以控制是否对“日志审查”任务应用预定义的规则。选择您要对日志审查应用的规则所对应的复选框。

6. 要创建新的自定义规则：
    a. 输入新规则的名称。
    b. 单击“**添加**”按钮。
    创建的规则将添加到常规规则列表中。
7. 要配置任何规则：
    a. 从列表中选择一个规则。
    在窗口的右侧区域中，“**描述**”选项卡将显示有关该规则的常规信息。

新规则的描述为空白。

b. 选择“**规则描述**”选项卡。

8. 在“**常规**”部分中，指定有关新规则的以下信息：

- **规则名称**
- **日志名称**
- **当 Windows 事件日志中出现新条目时，如果在事件参数中发现指定的标识符(ID)，将触发规则**

9. 在“**事件标识符**”部分中，指定将触发规则的事件 ID：

a. 输入事件 ID。

b. 单击“**添加**”按钮。

输入的事件 ID 将添加到列表中。可以为每个规则添加无限数量的标识符。

10. 单击“**保存**”按钮。

将应用已配置的日志审查规则。

通过 Web 插件管理日志审查规则

要通过 Web 插件添加和配置日志审查规则：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**系统审查**”部分。
5. 在“**日志审查**”子部分中单击“**设置**”。
6. 按下表所述配置设置。

“日志审查”任务设置

设置	描述
应用日志审查的自定义规则	您可以启用、禁用、添加或修改自定义规则。 表格中提供设置及自定义规则列表。
针对日志审查应用预定义规则	您可以启用或禁用启发式分析，它可以检测受保护设备上的异常活动。 表格中提供设置及自定义规则列表。
如果使用定义的频率输入不正确的密码，则检测为暴力破解攻击	您可以设置尝试次数和使用的时间范围，这将被视为启发式分析的触发器。
如果在定义的时段内登录，则检	您可以指定时间间隔的开始和结束时间，在此时间间隔中

测为网络登录	Kaspersky Embedded Systems Security 将登录尝试视为异常活动。
用户排除项	您可以指定不会触发启发式分析的用户。
排除的 IP 地址	您可以指定不会触发启发式分析的 IP 地址。
任务管理	您可以配置按计划启动任务的设置。

按需扫描

本节提供有关按需扫描任务的信息，并说明如何配置按需扫描任务设置和受保护设备上的安全性设置。

关于按需扫描任务

Kaspersky Embedded Systems Security 会扫描指定区域，以检测病毒和其他计算机安全威胁。Kaspersky Embedded Systems Security 将扫描受保护设备文件、RAM 以及自动运行对象。

Kaspersky Embedded Systems Security 提供以下按需扫描任务：

- Kaspersky Embedded Systems Security 每次启动时都会执行“在操作系统启动时扫描”任务。Kaspersky Embedded Systems Security 将扫描硬盘驱动器和可移动驱动器的引导扇区和主引导记录、系统内存以及进程内存。Kaspersky Embedded Systems Security 每次运行该任务时，都会创建未感染的引导扇区的副本。如果在这些扇区中检测到威胁，则下次任务启动时，会将这些扇区替换为备份副本。

  “在操作系统启动时扫描”任务是在安装后自动创建的。默认情况下，应用“仅通知”模式。在这种情况下，在设备上部署 Kaspersky Embedded Systems Security 后，如果在扫描期间未发现系统服务问题，您可以启用“在操作系统启动时扫描”任务。如果应用程序将关键系统服务检测为受感染或可能受感染的对象，“仅通知”模式会让您有时间找出原因并解决问题。如果应用程序应用“执行建议的操作” 模式，这将调用清除。如果清除操作失败则删除，清除或删除系统文件可能会导致操作系统启动出现严重问题。

  > 如果受保护设备在睡眠或休眠模式后唤醒，则可能不会执行“在操作系统启动时扫描”任务。仅当受保护设备重新启动或在完全关闭后启动时才执行该任务。

- 默认情况下，根据计划每周执行一次“关键区域扫描”任务。Kaspersky Embedded Systems Security 将扫描操作系统关键区域中的对象：自动运行对象、硬盘驱动器和可移动驱动器的引导扇区和主引导记录、系统内存以及进程内存。应用程序会扫描系统文件夹中的文件，例如 %windir%\system32 中的文件。Kaspersky Embedded Systems Security 将应用与推荐级别对应的安全性设置。您可以修改“关键区域扫描”任务的设置。

- 默认在每次数据库更新后按计划执行“隔离区扫描”任务。无法修改“隔离区扫描”任务范围。

- “应用程序完整性控制”任务每天执行。它提供了检查 Kaspersky Embedded Systems Security 模块是否损坏或修改的选项。检查程序安装文件夹。任务执行统计指示检查的模块数和发现损坏的模块数。默认情况下，任务设置值已定义，无法编辑。可以编辑任务启动计划设置。

此外，您还可以创建自定义按需扫描任务，例如，扫描受保护设备上的共享文件夹的任务。

Kaspersky Embedded Systems Security 可以一次运行多个按需扫描任务。

关于任务扫描范围和安全设置

在应用程序控制台中，选定按需任务的扫描范围以 Kaspersky Embedded Systems Security 可以控制的受保护设备文件资源树或列表的形式显示。默认情况下，受保护设备的网络文件资源以列表视图模式显示。

在管理插件中，只有列表视图可用。

若要在应用程序控制台中以树视图模式显示网络文件资源，

请打开“**扫描范围设置**”窗口中的下拉列表，然后选择“**树视图**”。

项或节点将显示在受保护设备文件资源的列表视图或树视图模式中，如下所示：

☑该节点包括在扫描范围内。

☐该节点已从扫描范围中排除。

☑该节点至少有一个子节点排除在扫描范围之外，或子节点的安全设置与父节点的安全设置不同（仅限树视图模式）。

如果选择了所有子节点，但未选择父节点，则显示 ☑ 图标。在这种情况下，在为所选子节点创建了扫描范围后，如果父节点所包含的文件和文件夹发生更改，将自动忽略这些更改。

使用应用程序控制台，您还可以添加虚拟驱动器到扫描范围中。虚拟节点的名称以蓝色字体显示。

安全性设置

在所选的按需扫描任务中，若要修改默认安全性设置，可通过将它们配置为用于整个保护或扫描范围的常规设置，或为设备文件资源树或列表中的不同节点或项配置不同设置。

为所选父节点配置的安全设置将自动应用到所有子节点。父节点的安全设置不会应用到单独配置的子节点。

您可以使用以下方式之一配置选定扫描范围或保护范围的设置：

- 从三个预定义的安全级别中选择一个级别（**最优性能**、**推荐**或**最佳保护**）。
- 在受保护设备文件资源树或列表中手动更改选定节点或项的安全性设置（安全级别更改为“**自定义**”）。

您可以将一组节点设置保存为模板，以便随后应用至其他节点。

预定义的扫描范围

所选按需扫描任务的受保护设备文件资源树或列表显示在“**扫描范围设置**”窗口中。

文件资源树或列表显示基于配置的 Microsoft Windows 安全设置所拥有读取访问权限的节点。

Kaspersky Embedded Systems Security 包含以下预定义扫描范围：

- **我的计算机**。Kaspersky Embedded Systems Security 扫描整个受保护设备。
- **本地硬盘驱动器**。Kaspersky Embedded Systems Security 扫描受保护设备硬盘驱动器上的对象。您可以在扫描范围中包含或排除所有硬盘驱动器、单个磁盘、文件夹或文件。
- **可移动驱动器**。Kaspersky Embedded Systems Security 扫描外部设备（如 CD 或可移动驱动器）上的文件。您可以在扫描范围中包含或排除所有可移动驱动器、单个磁盘、文件夹或文件。
- **网络**。您可以按照 UNC（通用命名惯例）格式指定网络文件夹或文件的路径以将它们添加至扫描范围。用于启动任务的账户必须拥有对所添加网络文件夹和文件的访问权限。默认情况下，按需扫描任务在系统账户下运行。

已连接的网络驱动器也不会显示在受保护设备文件资源树中。若要在扫描范围中包含网络驱动器上的对象，请以 UNC 格式指定对应于该网络驱动器的文件夹。

- **系统内存**。在启动扫描之后，Kaspersky Embedded Systems Security 将扫描操作系统中正在运行的进程的可执行文件和模块。
- **启动对象**。Kaspersky Embedded Systems Security 扫描注册表项和配置文件所引用的对象，例如 WIN.INI 或 SYSTEM.INI，以及在受保护设备启动时自动启动的应用程序模块。
- **共享文件夹**。您可以将受保护设备上的共享文件夹包含在扫描范围中。
- **虚拟驱动器**。虚拟文件夹、文件以及连接到受保护设备的驱动器可包含在扫描范围内，例如，常规群集驱动器。

使用 SUBST 命令创建的虚拟驱动器不会显示在应用程序控制台的受保护设备文件资源树中。为了扫描虚拟驱动器上的对象，请将与虚拟驱动器关联的受保护设备文件夹包含在扫描范围中。

默认情况下，您可以在网络文件资源树中查看和配置预定义扫描范围；还可以在网络文件资源列表形成期间在扫描范围设置中向该列表添加预定义范围。

默认情况下，“按需扫描”任务在以下范围下运行：

- “在操作系统启动时扫描”任务：
  - **本地硬盘驱动器**
  - **可移动驱动器**
  - **系统内存**
- 关键区域扫描：
  - **本地硬盘驱动器**（排除 Windows 文件夹）
  - **可移动驱动器**
  - **系统内存**
  - **启动对象**
- 其他任务：
  - **本地硬盘驱动器**（排除 Windows 文件夹）
  - **可移动驱动器**
  - **系统内存**
  - **启动对象**
  - **共享文件夹**

在线存储文件扫描

关于云文件

Kaspersky Embedded Systems Security 可以与 Microsoft OneDrive 云文件进行交互。该应用程序支持新的“OneDrive 文件按需”功能。

Kaspersky Embedded Systems Security 不支持其他在线存储。

“OneDrive 文件随选”帮助您访问所有 OneDrive 文件，而无需下载所有文件和使用设备上的存储空间。您可以在需要时将文件下载到硬盘驱动器。

当“OneDrive 按需文件”功能开启时，可以在文件资源管理器的“**状态**”列中看到每个文件旁边的状态图标。每个文件都具有以下状态之一：

此状态图标指示文件*仅在线可用*。仅在线文件不会物理存储在您的硬盘驱动器中。当设备未连接到 Internet 时，无法打开仅在线文件。

此状态图标指示文件*本地可用*。当打开仅在线文件时会显示此图标，该文件会下载到您的设备中。您可以随时打开本地可用的文件，即使没有 Internet 访问权限。要清理空间，可以将文件更改回 仅在线。

此状态图标指示文件*存储在硬盘驱动器中并且始终可用*。

云文件扫描

Kaspersky Embedded Systems Security 只能扫描受保护设备上本地存储的云文件。此类 OneDrive 文件的状态为 和 。在扫描期间会跳过 文件，因为这些文件没有物理存储在受保护设备上。

Kaspersky Embedded Systems Security 在扫描时不会自动从云端下载 文件，即使这些文件已包括在扫描范围中。

在各种方案中，云文件由多种 Kaspersky Embedded Systems Security 任务处理，具体取决于任务类型：

- 实时云文件扫描：您可以将包含云文件的文件夹添加到“实时文件保护”任务的保护范围中。当用户访问该文件时会对其进行扫描。如果用户访问 文件，系统会下载该文件，该文件将变为本地可用，并且其状态将更改为 。这样该文件可以被“实时文件保护”任务处理。
- 按需云文件扫描：您可以将包含云文件的文件夹添加到“按需扫描”任务的扫描范围中。该任务会扫描状态为 和 的文件。如果在范围中找到任何 文件，在扫描期间将跳过这些文件，并在任务日志中记录信息事件，指示所扫描的文件只是云文件的占位符，并不存在于本地驱动器中。
- 应用程序控制规则生成和使用：您可以使用“应用程序启动控制规则生成器”任务为 和 文件创建允许和拒绝规则。“应用程序启动控制”任务应用“默认拒绝”原则和所创建的规则来处理和阻止云文件。

  “应用程序启动控制”任务会阻止所有云文件启动，不管它们的状态如何。应用程序不会将 文件包括在规则生成范围中，因为它们没有物理存储在硬盘驱动器上。由于不能为此类文件创建允许规则，因此对它们实施“默认拒绝”原则。

在 OneDrive 云文件中检测到威胁时，应用程序会应用执行扫描的任务的设置中指定的操作。因此，可以将文件删除、清除、移至隔离区或备份。

按照相关 Microsoft OneDrive 文档中概述的原则，对本地文件的更改将与 OneDrive 中存储的副本进行同步。

关于预定义安全级别

“使用 iChecker 技术”、“使用 iSwift 技术”、“使用启发式分析”和“检查文件内的 Microsoft 签名”安全性设置并未包含在预设安全级别设置中。如果“使用 iChecker 技术”、“使用 iSwift 技术”、“使用启发式分析”和“检查文件内的 Microsoft 签名”等设置发生改变，您选择的预设安全级别不会更改。

可以为设备文件资源树中的选定节点应用以下预定义安全级别之一：“最优性能”、“推荐”或“最佳保护”。每个级别都包含其自有的预定义安全设置（请参见下表）。

最优性能

如果您的网络除了在受保护设备上使用 Kaspersky Embedded Systems Security 外，还有其他受保护设备安全措施，例如防火墙和现有安全策略，则建议使用“最优性能”安全级别。

推荐

“推荐”安全级别确保保护与对设备的性能影响的最佳组合。Kaspersky 专家推荐此级别，因为其足以保护大多数公司网络上的设备。默认情况下，将设置“推荐”安全级别。

最佳保护

如果组织的网络有更高的设备安全要求，则推荐使用“最佳保护”安全级别。

预定义的安全级别和对应的安全性设置值

选项	安全级别		
	最优性能	推荐	最佳保护
扫描对象	按格式	所有对象	所有对象
仅扫描新文件和已修改的文件	已启用	已禁用	已禁用
对受感染对象和其他对象执行的操作	清除。清除失败则删除	执行推荐的操作（清除。清除失败则删除）	清除。清除失败则删除
对疑似感染对象执行的操作	隔离	执行推荐的操作（隔离）	隔离
排除文件	否	否	否
不检测	否	否	否
超过以下时间则停止扫描	60 秒	否	否

(秒)			
不扫描大于该值的复合对象(MB)	8 MB	否	否
扫描 NTFS 交换数据流	是	是	是
扫描磁盘引导扇区和 MBR	是	是	是
扫描复合对象	• SFX 压缩文件* • 打包的对象* • 嵌入的 OLE 对象* * 仅新对象和已修改的对象	• SFX 压缩文件* • 打包的对象* • 嵌入的 OLE 对象* * 所有对象	• 压缩文件* • SFX 压缩文件* • 电子邮件数据库* • 纯文本邮件* • 打包的对象* • 嵌入的 OLE 对象* * 所有对象

关于可移动驱动器扫描

可以配置通过 USB 端口连接到受保护设备的可移动驱动器的扫描。

Kaspersky Embedded Systems Security 使用按需扫描任务扫描可移动驱动器。当可移动驱动器已连接并在完成扫描后删除任务时，应用程序会自动创建新的按需扫描任务。系统会根据为可移动驱动器扫描定义的预定义安全级别来执行创建的任务。您不能配置临时按需扫描任务的设置。

如果您已安装不带反病毒数据库的 Kaspersky Embedded Systems Security，则将无法执行可移动驱动器扫描。

当连接的可移动驱动器在操作系统中注册为 USB 外部设备时，Kaspersky Embedded Systems Security 将扫描这些可移动驱动器。如果连接被设备控制任务阻止，则应用程序不会扫描可移动驱动器。应用程序不会扫描 MTP 连接的移动设备。

Kaspersky Embedded Systems Security 允许在扫描期间访问可移动驱动器。

每个可移动驱动器的扫描结果提供在连接可移动驱动器时创建的按需扫描任务的日志中。

可以更改可移动驱动器扫描组件的设置（请参见以下表格）。

可移动驱动器扫描设置

设置	默认值	描述
扫描通过 USB 连接的可移动驱动器	已清除复选框	您可以打开或关闭通过 USB 连接到受保护设备的可移动驱动器的扫描。
扫描可移动驱动器，如果	8192	您可通过在可移动驱动器上设置最大数据量，来缩小组件的范围。

其存储的数据量未超过 (MB)	MB	如果存储的数据量超出指定值，Kaspersky Embedded Systems Security 不会扫描可移动驱动器。
扫描时使用的安全级别	最佳保护	您可通过选择以下三个安全级别之一来配置创建的按需扫描任务： • **最佳保护** • **推荐** • **最优性能** 当检测到已感染、可能已感染和其他对象时使用的算法，以及每个安全级别的其他扫描设置，对应于按需扫描任务中的预设安全级别。

关于“基线文件完整性监控”任务

在“基线文件完整性监控”任务期间，Kaspersky Embedded Systems Security 不会检查锁定的文件、文件夹、文件快捷方式和云文件。

“基线文件完整性监控”任务通过将文件的哈希（MD5 哈希或 SHA256 哈希）与基线进行比较来对监控范围内文件的完整性进行监控。

当“基线文件完整性监控”任务首次运行时，Kaspersky Embedded Systems Security 通过计算和存储任务监控范围内文件的哈希来创建基线。如果更改了“基线文件完整性监控”任务监控范围，Kaspersky Embedded Systems Security 会在“基线文件完整性监控”任务下次运行时通过计算和存储任务监控范围内文件的哈希来更新基线。如果删除了“基线文件完整性监控”任务，Kaspersky Embedded Systems Security 会删除此“基线文件完整性监控”任务的基线。

您可以使用命令行删除基线，而不删除“基线文件完整性监控”任务。

“基线文件完整性监控”任务会跟踪监控范围内文件的以下更改：

- 监控范围包含基线中不存在的文件
- 监控范围不包含基线中存在的文件
- 监控范围中文件的哈希与基线中此文件的哈希不同

“基线文件完整性监控”任务不会跟踪文件属性和交换流的更改。

如果某个文件或文件夹不可访问，则 Kaspersky Embedded Systems Security 在基线创建过程中不会将此文件或文件夹添加到基线，并且将在运行“基线文件完整性监控”任务期间创建一个关于计算文件校验和失败的事件。

文件或文件夹不可访问可能由于以下原因：

- 指定的路径不存在
- 指定的路径下不存在掩码指定的文件类型
- 指定的文件被锁定

- 指定的文件为空

从上下文菜单中启用按需扫描任务的启动

您可以从 Microsoft Windows 资源管理器的上下文菜单中启用针对一个或多个文件的按需扫描任务的启动。

要从上下文菜单启用按需扫描任务的启动：

1. 创建以下 REG 文件：

```
Windows Registry Editor Version 5.0.0

[HKEY_CLASSES_ROOT\Directory\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\*\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\Directory\shell\kess]

@="Scan with Kaspersky Embedded Systems Security\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess]

@="Scan with Kaspersky Embedded Systems Security\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavshell.exe"="~ RUNASADMIN"
```

> 您需要指定 Kaspersky Embedded Systems Security 安装文件夹的实际位置。

2. 创建具有以下内容的 `scan.cmd` 文件：

```
@echo off
set LOGNAME=%RANDOM%

"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems
Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

echo Scanning is in progress...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

`scan.cmd` 文件必须包含以下信息：

- kavshell.exe 文件的位置。
- 包含扫描结果的临时文件的位置。
- KAVSHELL SCAN 命令的参数。
- 用于在任务完成后关闭控制台窗口的超时值。

3. 将 scan.cmd 文件复制到 [HKEY_CLASSES_ROOT\Directory\shell\kess\command] REG 文件中指定的文件夹。

   示例中使用了 C:\Temp 文件夹。

您无需重新启动操作系统。

默认按需扫描任务设置

默认情况下，按需扫描任务将使用下表所述的设置。您可以配置本地系统和自定义按需扫描任务。

默认按需扫描任务设置

设置	默认值	描述
扫描范围	应用于本地系统和自定义任务： • **在操作系统启动时扫描**：整个受保护设备，排除共享文件夹和自动运行的对象。 • **关键区域扫描**：整个受保护设备，排除共享文件夹和某些操作系统文件。 • 自定义**按需扫描**任务：整个受保护设备。	您可以更改扫描范围。不能为“**隔离区扫描**”和“**应用程序完整性控制**”本地系统任务配置扫描范围。 “**在操作系统启动时扫描**”任务是在安装后自动创建的。默认情况下，应用“**仅通知**”模式。在这种情况下，在设备上部署 Kaspersky Embedded Systems Security 后，如果在扫描期间未发现系统服务问题，您可以启用“**在操作系统启动时扫描**”任务。如果应用程序将关键系统服务检测为受感染或可能受感染的对象，“**仅通知**”模式会让您有时间找出原因并解决问题。如果应用程序应用“**执行建议的操作**”模式，这将调用**清除。如果清除操作失败**则删除，清除或删除系统文件可能会导致操作系统启动出现严重问题。
安全性设置	整个扫描范围的常规设置；对应“**推**	您可以对受保护设备文件资源列表或树中选定的节点执行以下操作： • 选择不同的预定义安全级别

	荐”安全级别。	• 手动更改安全性设置 您可以将选定节点的一组安全性设置保存为模板，以便在以后将其应用至其他节点。
使用启发式分析	与“关键区域扫描”、“在操作系统启动时扫描”和自定义任务的“中度”分析级别结合使用。 与“隔离区扫描”任务的“深度”分析级别结合使用。	可以启用或禁用“启发式分析”并配置分析级别。不能配置“隔离区扫描”任务分析级别。 “应用程序完整性控制”和“基线文件完整性监控”任务不使用启发式分析。
应用信任区域	已应用（不适用于“隔离区扫描”任务）	可以在选定任务中使用的常规排除列表。
在扫描中使用 KSN	已应用	您可以使用卡巴斯基安全网络云服务基础架构提高您的设备保护能力。
以特定权限启动任务的设置	在系统账户下启动任务。	您可以为所有系统和自定义按需扫描任务编辑以特定账户权限启动任务的设置，但“隔离区扫描”和“应用程序完整性控制”任务除外。
在后台模式下执行任务（低优先级）	未应用	您可以配置按需扫描任务的优先级。
任务启动计划	应用于本地系统任务： • 在操作系统启动时扫描 - 应用程序启动时 • 关键区域扫描 - 每周 • 隔离区扫描 - 应用程序数据库更新后	您可以配置计划任务启动的设置。

	• 应用程序完整性控制 - **每天**新建自定义任务中未使用。	
记录扫描执行并更新设备保护状态	执行关键区域扫描后，每周更新一次设备保护状态。	可通过以下方式配置记录关键区域扫描执行日志的相关设置： • 编辑关键区域扫描任务启动计划的设置。 • 编辑关键区域扫描任务的扫描范围。 • 创建自定义按需扫描任务。

通过管理插件管理按需扫描任务

在本节中，学习如何导航管理插件界面，以及如何为网络中的一台或所有受保护设备配置任务设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开按需扫描任务向导

要开始创建新的自定义按需扫描任务：

1. 若要创建本地任务：
   a. 展开 Kaspersky Security Center 管理控制台中的“**受管理设备**”节点。
   b. 选择受保护设备所属的管理组。
   c. 在结果窗格的“**设备**”选项卡上，打开受保护设备的上下文菜单。
   d. 选择“**属性**”菜单选项。
   e. 在打开的窗口中，单击“**任务**”部分中的“**添加**”按钮。

   将打开“**新建任务向导**”窗口。
2. 创建组任务：
   a. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
   b. 选择要为其创建任务的管理组。

c. 打开“**任务**”选项卡。

d. 单击“**创建任务**”按钮。

将打开“**新建任务向导**”窗口。

3. 要为自定义的一组受保护设备创建任务：

a. 在 Kaspersky Security Center 管理控制台树的“**设备选择**”节点中，单击“**运行选择**”按钮以执行设备选择。

b. 打开“**选择结果‘选择名称’**”选项卡。

c. 在“**执行选择**”下拉列表中，选择“**为选择结果创建任务**”选项。

将打开“**新建任务向导**”窗口。

4. 在 Kaspersky Embedded Systems Security 的可用任务列表中选择“**按需扫描**”任务。

5. 单击“**下一步**”。
将打开“**设置**”窗口。

根据需要配置任务设置。

要配置现有按需扫描任务，

双击 Kaspersky Security Center 任务列表中的任务名称。

将打开“**属性：按需扫描**”窗口。

打开按需扫描任务属性

要打开单台受保护设备的按需扫描任务的应用程序属性：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择受保护设备所属的管理组。

3. 选择“**设备**”选项卡。

4. 双击要为其配置扫描范围的受保护设备的名称。
将打开“**属性：<受保护设备名称>**”窗口。

5. 选择“**任务**”部分。

6. 在为设备创建的任务列表中，选择您创建的按需扫描任务。

7. 单击“**属性**”按钮。
将打开“**属性：按需扫描**”窗口。

根据需要配置任务设置。

创建按需扫描任务

要创建自定义按需扫描任务：

1. 打开“新建任务向导”中的“设置”窗口。
2. 选择所需的**任务创建方式**。
3. 单击“**下一步**”。
4. 在“**扫描范围**”窗口中创建扫描范围：

默认情况下，扫描范围包括受保护设备的关键区域。扫描范围在表中用图标 ☑ 标记。排除的扫描范围在表中用图标 ☐ 标记。

可以按如下方式更改扫描范围：添加特定的预设扫描范围、磁盘、文件夹、网络对象和文件，然后为添加的每个范围分配特定的安全性设置。

- 要将所有关键区域从扫描范围中排除，请在每个行上打开上下文菜单，然后选择“**删除范围**”选项。
- 要在扫描范围中包括预定义的扫描范围、磁盘、文件夹、网络对象或文件：
  a. 右键单击“**扫描范围**”表，然后选择“**添加范围**”或单击“**添加**”按钮。
  b. 在“**将对象添加至扫描范围**”窗口中，选择“**预定义范围**”列表中的预定义范围，指定受保护设备或另外一台网络受保护设备上的驱动器、文件夹、网络对象或文件，然后单击“**确定**”按钮。
- 要从扫描中排除子文件夹或文件，请在向导的“**扫描范围**”窗口中选择已添加的文件夹（磁盘）：
  a. 打开上下文菜单，然后选择“**配置**”选项。
  b. 在“**安全级别**”窗口中单击“**设置**”按钮。
  c. 在“**按需扫描设置**”设置窗口的“**常规**”选项卡上，清除“**子文件夹和子文件**”复选框。
- 要更改扫描范围安全性设置：
  a. 打开您希望配置其设置的范围的上下文菜单，然后选择“**配置**”。
  b. 在“**按需扫描设置**”窗口中，选择预定义的安全级别之一，或者单击“**设置**”按钮以手动配置安全性设置。

安全性设置的配置方式与实时文件保护任务的配置方式相同。

- 要跳过添加的扫描范围中的嵌入式对象：
  a. 打开“**扫描范围**”表的上下文菜单，选择“**添加排除**”。
  b. 指定要排除的对象：在“**预定义范围**”列表中选择预定义范围，指定受保护设备或另一台网络受保护设备上的磁盘、文件夹、网络对象或文件。

c. 单击“**确定**”按钮。

5. 在“**选项**”窗口中，配置启发式分析以及与其他组件的集成：

   - 配置启发式分析的使用。
   - 如果您希望从任务的扫描范围中排除已添加到受信任区域列表的对象，则选中“**应用信任区域**”复选框。
   - 如果您想要在任务中使用卡巴斯基安全网络云服务，请选中“**在扫描中使用 KSN**”复选框。
   - 若要向将执行该任务的工作进程分配“*低*”优先级，请在“**在后台模式下执行任务**”窗口中选中“**选项**”复选框。

     默认情况下，执行 Kaspersky Embedded Systems Security 任务的工作进程的优先级为“*中*”（正常）。

   - 要使用所创建的任务作为关键区域扫描任务，请选中“**选项**”窗口中的“**将任务视为关键区域扫描**”复选框。

6. 单击“**下一步**”。
7. 在“**计划**”窗口中，设置计划的任务启动设置。
8. 单击“**下一步**”。
9. 在“**选择账户以运行任务**”窗口中，指定要使用的账户。
10. 单击“**下一步**”。
11. 指定任务名称。
12. 单击“**下一步**”。

    任务名称不应超过 100 个字符，并且不能包含以下符号：" * < > & \ : |

    将打开“**完成创建任务**”窗口。

13. 您可以通过选中“**向导完成后运行任务**”复选框来在向导完成后运行任务。
14. 单击“**完成**”完成创建任务。

将为所选受保护设备或受保护设备组创建新的按需扫描任务。

为按需扫描任务分配关键区域扫描状态

默认情况下，如果“关键区域扫描”任务的执行频率低于 Kaspersky Embedded Systems Security 的“*已很长时间未执行关键区域扫描*”事件生成阈值，则 Kaspersky Security Center 将向受保护设备分配“*警告*”状态。

要为单个管理组中的所有受保护设备配置扫描：

1. 创建组按需扫描任务。

2. 在任务向导的“选项”窗口中，选中“将任务视为关键区域扫描”复选框。指定的任务设置（扫描范围和安全性设置）将应用于该组中的所有受保护设备。配置任务计划。

   您可以在为一组受保护设备创建按需扫描任务时选中“将任务视为关键区域扫描”复选框，或稍后在“属性：<任务名称>”窗口中选中该复选框。

3. 使用新的或现有策略会禁用该组受保护设备上的按需扫描本地系统任务的计划启动。

随后，Kaspersky Security Center 管理服务器将评估受保护设备的安全状态，并且将根据上次运行具有“关键区域扫描”状态的任务的结果而非根据“关键区域扫描”本地系统任务的结果通知您有关该安全状态的信息。

您可以为按需扫描组任务和受保护设备组的任务分配“*关键区域扫描*”状态。

可以使用应用程序控制台查看“按需扫描”任务是否为“关键区域扫描”任务。

在应用程序控制台中，“将任务视为关键区域扫描”复选框会显示在任务属性中，但不可对其进行编辑。

在后台运行按需扫描任务

默认情况下，将为执行 Kaspersky Embedded Systems Security 任务的进程分配“*中度（正常）*”优先级。

可以为将运行按需扫描任务的进程分配“*低*”优先级。将进程的优先级降级会增加执行任务所需的时间，但可能对其他正在运行的程序的进程性能产生有利影响。

多个后台任务可以在单个具有低优先级的工作进程中运行。您可以指定按需扫描后台任务的最大进程数。

要更改现有按需扫描任务的优先级：

1. 打开“属性：按需扫描”窗口。
2. 选中或清除“在后台模式下执行任务”复选框。
3. 单击“确定”。

   将保存已配置的任务设置，并将这些设置立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

记录关键区域扫描执行

默认情况下，设备保护状态显示在 **Kaspersky Embedded Systems Security** 节点的结果窗格中，并在执行关键区域扫描任务后每周更新一次。

设备保护状态的更新时间与设置中已选中“将任务视为关键区域扫描”复选框的按需扫描任务的计划相关联。默认情况下，仅针对“关键区域扫描”任务选中该复选框且无法针对该任务进行修改。

只能在 Kaspersky Security Center 中选择与设备保护状态相关联的按需扫描任务。

配置任务扫描范围

如果在“在操作系统启动时扫描”和“关键区域扫描”任务中修改扫描范围，可以通过修复 Kaspersky Embedded Systems Security 本身的设置来恢复这些任务中的默认扫描范围（“**开始**” > “**程序**” > “**Kaspersky Embedded Systems Security**” > “**修改或删除 Kaspersky Embedded Systems Security**”）。在安装向导中，选择“**修复已安装组件**”，并单击“**下一步>**”。然后选中“**恢复推荐的应用程序设置**”复选框。

要配置现有按需扫描任务的扫描范围：

1. 打开“**属性：按需扫描**”窗口。
2. 选择“**扫描范围**”选项卡。
3. 要在扫描范围中包括项目：
   a. 在扫描范围列表的空白部分中打开上下文菜单。
   b. 选择上下文菜单中的“**添加范围**”选项。
   c. 在打开的“**将对象添加至扫描范围**”窗口中，选择想要添加的对象类型：
      - **预定义范围** - 在受保护设备上添加一个预定义范围。然后在下拉列表中，选择所需扫描范围。
      - **磁盘、文件夹或网络位置** - 在扫描范围中包括单个驱动器、文件夹或网络对象。然后通过单击“**浏览**”按钮选择所需的范围。
      - **文件** - 在扫描范围中包括单个文件。然后通过单击“**浏览**”按钮选择所需的范围。

   如果某个对象已经作为扫描范围的排除添加，则不能再将其添加到扫描范围中。
4. 要从扫描范围中排除单个节点，请清除这些节点名称旁边的复选框，或者执行以下步骤：
   a. 右键单击扫描范围打开其上下文菜单。
   b. 在上下文菜单中，选择“**添加排除**”选项。
   c. 在“**添加排除**”窗口中选择对象类型，将按照将对象添加到扫描范围中时使用的步骤，将该对象类型作为扫描范围的排除添加。
5. 要修改扫描范围或所添加的排除，请选择相应扫描范围上下文菜单中的“**编辑范围**”选项。
6. 若要在网络文件资源列表中隐藏之前添加的扫描范围或排除，请在所需扫描范围的上下文菜单中选择“**删除范围**”选项。

   将扫描范围从网络文件资源列表中删除时，该扫描范围也从“按需扫描”任务范围中排除。
7. 单击“**确定**”按钮。

扫描范围设置窗口关闭。将保存新配置的设置。

为按需扫描任务选择预定义的安全级别

可以为受保护设备文件资源列表中的选定节点应用以下预定义安全级别之一：“**最优性能**”、“**推荐**”和“**最佳保护**”。

要选择其中一个预定义安全级别：

1. 打开“**属性：按需扫描**”窗口。
2. 选择“**扫描范围**”选项卡。
3. 在受保护设备列表中，选择一个包含在扫描范围中的项目以设置预定义安全级别。
4. 单击“**配置**”按钮。
   将打开“**按需扫描设置**”窗口。
5. 在“**安全级别**”选项卡上，选择要应用的安全级别。
   该窗口将显示与选定安全级别相对应的安全性设置列表。
6. 单击“**确定**”按钮。
7. 在“**属性：按需扫描**”窗口中单击“**确定**”按钮。
   将保存已配置的任务设置，这些设置会立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

手动配置安全性设置

默认情况下，按需扫描任务对整个扫描范围使用通用安全性设置。

这些设置对应于“**推荐**”预定义安全级别。

可以通过将安全性设置配置为用于整个扫描范围的常规设置，或配置为受保护设备文件资源列表或树中节点的不同项目的不同设置，来修改安全性设置的默认值。

要手动配置安全设置：

1. 打开“**属性：按需扫描**”窗口。
2. 选择“**扫描范围**”选项卡。
3. 在您要为其配置安全性设置的扫描范围列表中选择项目。

   可以为扫描范围内的选定节点或项目应用包含安全设置的预定义模板。

4. 单击“**配置**”按钮。
   将打开“**按需扫描设置**”窗口。
5. 在以下选项卡上根据要求配置选定节点或项目的安全设置：

- 常规
- 操作
- 性能
- 分级存储

6. 在“**按需扫描设置**”窗口中单击“**确定**”。
7. 在“**扫描范围**”窗口中单击“**确定**”。

将保存新的扫描范围设置。

配置常规任务设置

要配置常规按需扫描任务设置：

1. 打开“**属性：按需扫描**”窗口。
2. 选择“**扫描范围**”选项卡。
3. 单击“**配置**”按钮。
   将打开“**按需扫描设置**”窗口。
4. 单击“**设置**”按钮。
5. 在“**常规**”选项卡的“**扫描对象**”组框中，指定要包含在扫描范围内的对象类型：
   - 扫描对象：
     - 所有对象
     - 按格式扫描对象
     - 按反病毒数据库中指定的扩展名列表扫描对象
     - 按指定的扩展名列表扫描对象
   - 子文件夹
   - 子文件
   - 扫描磁盘引导扇区和 MBR
   - 扫描 NTFS 交换数据流
6. 在“**性能**”组框中，选中或清除“仅扫描新文件和已修改的文件”复选框。

如果清除该复选框，要在可用选项之间切换，请单击每个复合对象类型对应的“**全部/仅新建**”链接。

7. 在“**扫描复合对象**”组框中，指定要包含在扫描范围内的复合对象：
   - 全部/仅新的压缩文件
   - 全部/仅新的 **SFX** 压缩文件
   - 全部/仅新的电子邮件数据库
   - 全部/仅新的打包的对象
   - 全部/仅新的纯文本电子邮件
   - 全部/仅新的嵌入的 **OLE** 对象
8. 单击“**确定**”。

将保存新的任务配置。

配置操作

要配置“按需扫描”任务过程中对受感染的对象和其他检测到的对象的操作：

1. 打开“**属性：按需扫描**”窗口。
2. 选择“**扫描范围**”选项卡。
3. 单击“**配置**”按钮。
   将打开“**按需扫描设置**”窗口。
4. 单击“**设置**”按钮。
5. 选择“**操作**”选项卡。
6. 选择要对受感染的对象和其他检测到的对象执行的操作：
   - 仅通知。
   - **清除**。
   - **清除；清除失败时则删除**。
   - 删除。
   - **执行推荐的操作**。
7. 选择要对疑似感染的对象执行操作：
   - 仅通知。
   - **隔离**。
   - 删除。
   - 执行推荐的操作。

8. 根据检测的对象类型配置要对对象执行的操作：

   a. 清除或选中“根据检测到的对象的类型执行操作”复选框。

   b. 单击“**设置**”按钮。

   c. 在打开的窗口中，选择针对每种检测到的对象类型的主要操作和次要操作（如果主要操作失败则执行）。

   d. 单击“**确定**”。

9. 选择要对不可恢复的复合对象执行的操作：选中或清除“在检测到嵌入对象时完全删除应用程序无法修改的复合文件”复选框。

10. 单击“**确定**”。

将保存新的任务配置。

配置性能

要配置“按需扫描”任务的性能设置：

1. 打开“属性：按需扫描”窗口。
2. 选择“**扫描范围**”选项卡。
3. 单击“**配置**”按钮。
   将打开“**按需扫描设置**”窗口。
4. 单击“**设置**”按钮。
5. 选择“**性能**”选项卡。
6. 在“**排除**”部分中：
   - 清除或选中“排除文件”复选框。
   - 清除或选中“不检测”复选框。
   - 针对每个设置单击“**编辑**”按钮以添加排除项。
7. 在“**高级设置**”部分中：
   - 超过以下时间则停止扫描(秒)
   - 不扫描大于该值的复合对象(MB)
   - 使用 iSwift 技术
   - 使用 iChecker 技术
8. 单击“**确定**”。

将保存新的任务配置。

配置可移动驱动器扫描

要配置在可移动驱动器连接到受保护设备时对其进行的扫描：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。

   在打开的“**属性：<策略名称>**”窗口中，选择“**补充**”部分。
5. 单击“**可移动驱动器扫描**”子部分中的“**设置**”按钮。

   将打开“**可移动驱动器扫描**”窗口。
6. 在“**连接时扫描**”部分中，执行以下操作：
   - 如果想让 Kaspersky Embedded Systems Security 在可移动驱动器连接时自动扫描，请选择“**扫描通过 USB 连接的可移动驱动器**”复选框。
   - 如果需要，选中“**扫描可移动驱动器，如果其存储的数据量未超过(MB)**”，然后在右侧的字段中指定最大值。
   - 在“**扫描时使用的安全级别**”下拉列表中，指定可移动驱动器扫描所需设置的安全级别。
7. 单击“**确定**”。

即会保存并应用指定设置。

配置“基线文件完整性监控”任务

要配置“基线文件完整性监控”组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中选择任务名称，然后单击“**配置任务**”链接。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

   在“**通知**”部分中，配置任务事件通知设置。关于如何配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

5. 在“**扫描范围**”部分中，执行以下操作：

   a. 要将文件夹包括在“基线文件完整性监控”任务范围中：

      1. 单击“**添加**”按钮。
         将打开“**扫描区域属性**”窗口。

      2. 选中或清除“**扫描此区域**”复选框。

      3. 单击“**浏览**”按钮以指定要包括在“基线文件完整性监控”任务范围中的文件夹。

      4. 如果要在“基线文件完整性监控”任务范围中包括所有子文件夹，请选中“**同时扫描子文件夹**”复选框。

   b. 要包括或排除先前添加到“基线文件完整性监控”任务范围中的文件夹，请选中或清除“**扫描范围**”表中文件夹路径左侧的复选框。

   c. 要删除先前添加到“基线文件完整性监控”任务范围中的文件夹，请在“**扫描范围**”表中选择此文件夹，然后单击“**删除**”按钮。

6. 在“**计划**”部分中配置任务计划（您可为除“数据库更新回滚”外的所有任务类型配置计划）。

7. 在“**账户**”部分中，指定将使用其权限运行任务的账户。

8. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。

   有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

9. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。
   将保存新配置的组任务设置。

通过应用程序控制台管理按需扫描任务

在本节中，学习如何导航应用程序控制台界面以及如何在受保护设备上配置任务设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开按需扫描任务设置

要通过应用程序控制台打开按需扫描任务的常规设置：

1. 在应用程序控制台树中展开“**按需扫描**”节点。

2. 选择与要配置的任务相应的子节点。

3. 在子节点结果窗格中，单击“**属性**”链接。
   将打开“**任务设置**”窗口。

打开按需扫描任务范围设置

要通过应用程序控制台打开扫描范围设置窗口：

1. 在应用程序控制台树中展开“**按需扫描**”节点。
2. 选择与要配置的按需扫描任务相应的子节点。
3. 在选定节点的结果窗格中，单击“**配置扫描范围**”链接。
   将打开“**扫描范围设置**”窗口。

创建和配置按需扫描任务

单台受保护设备的自定义任务可以在“**按需扫描**”节点中创建。不能在 Kaspersky Embedded Systems Security 的其他功能组件中创建自定义任务。

要创建和配置新的按需扫描任务：

1. 在应用程序控制台树中，打开“**按需扫描**”节点的上下文菜单。
2. 选择“**添加任务**”。
   将打开“**添加任务**”窗口。
3. 配置以下任务设置：
   - **名称** – 包含不超过 100 个字符的任务名称。可以包含除 **" * < > & \ : |** 以外的任何符号。

     如果未指定任务名称，则无法在“**计划**”、“**高级**”和“**运行账户**”选项卡上保存任务或配置新任务。

   - **描述** – 有关任务的任何附加信息。不超过 2000 个字符。此信息将显示在任务属性窗口中。
   - 使用启发式分析。
   - 在后台模式下执行任务。
   - 应用信任区域。
   - 将任务视为关键区域扫描。
   - 在扫描中使用 KSN。
4. 配置“**计划**”和“**高级**”选项卡上的任务启动计划设置。
5. 在“**运行账户**”选项卡上，配置使用特定账户权限启动任务的设置。

6. 在“**添加任务**”窗口中单击“**确定**”。

   将创建新的自定义按需扫描任务。将在应用程序控制台树中显示包含新任务名称的节点。此操作将会记录到系统审核日志中。

7. 如果需要，在所选节点的结果窗格中，选择“**配置扫描范围**”。

   将打开“**扫描范围设置**”窗口。

8. 在受保护设备文件资源树或列表中，选择要包含在扫描范围内的节点或项。

9. 选择一项预定义安全级别或手动配置扫描设置。

10. 在“**扫描范围设置**”窗口中，单击“**保存**”。

    将在下次启动任务时应用配置的设置。

按需扫描任务中的扫描范围

本节包含有关在“按需扫描”任务中创建和使用扫描范围的信息。

配置网络文件资源的视图

要在配置扫描范围设置期间选择网络文件资源的视图：

1. 打开“扫描范围设置”窗口。
2. 打开窗口左上角部分中的下拉列表，然后选择以下选项之一：
   - 选择“**树视图**”选项以树的形式显示网络文件资源。
   - 选择“**列表视图**”选项以列表形式显示网络文件资源。

   > 默认情况下，受保护设备的网络文件资源以列表形式显示。

3. 单击“**保存**”按钮。

创建扫描范围

如果您正在使用管理员工作站上安装的应用程序控制台远程管理受保护设备上的 Kaspersky Embedded Systems Security，您必须是受保护设备上管理员组成员才能查看文件夹。

> 在不同 Windows 操作系统中，设置的名称可能有所不同。

如果在“在操作系统启动时扫描”和“关键区域扫描”任务中修改扫描范围，可以通过修复 Kaspersky Embedded Systems Security 本身的设置来恢复这些任务中的默认扫描范围（“**开始**” > “**程序**” > “**Kaspersky Embedded Systems Security**” > “**修改或删除 Kaspersky Embedded Systems Security**”）。在安装向导中，选择“**修复已安装组件**”，并单击“**下一步>**”。然后选中“**恢复推荐的应用程序设置**”复选框。

创建按需扫描任务范围的过程取决于选定的网络文件资源视图。您可以将网络文件资源的视图配置为树或列表（默认视图）。

要使用网络文件资源树创建扫描范围：

1. 打开“扫描范围设置”窗口。
2. 在窗口的左侧部分中，打开网络文件资源树以显示所有节点和子节点。
3. 执行以下操作：
   - 要从扫描范围中排除单个节点，请清除这些节点名称旁边的复选框。
   - 要从扫描范围中排除单个节点，请清除“**我的计算机**”复选框，然后执行以下步骤：
     - 如果要将特定类型的所有驱动器包含在扫描范围内，请选中所需驱动器类型名称旁边的复选框（例如，要添加受保护设备上的所有可移动驱动器，请选中“**可移动驱动器**”复选框）。
     - 如果要将特定类型的单个驱动器包含在扫描范围内，请展开包含该类型驱动器的节点，然后选中所需驱动器名称旁边的复选框。例如，要选择可移动驱动器 **F:**，请展开“**可移动驱动器**”节点，然后选中驱动器 **F:** 对应的复选框。
     - 如果您想要仅包含驱动器上的单个文件夹或文件，请选中该文件夹或文件名称旁边的复选框。
4. 单击“**保存**”按钮。

“**扫描范围设置**”窗口将关闭。将保存新配置的设置。

要使用网络文件资源列表创建扫描范围：

1. 打开“扫描范围设置”窗口。
2. 要从扫描范围中排除单个节点，请清除“**我的计算机**”复选框，然后执行以下步骤：
   a. 右键单击扫描范围打开其上下文菜单。
   b. 在按钮的上下文菜单中，选择“**添加扫描范围**”。
   c. 在打开的“**添加扫描范围**”窗口中，选择要添加的对象类型：
      - **预定义范围** - 在受保护设备上添加一个预定义范围。然后在下拉列表中，选择所需扫描范围。
      - **磁盘、文件夹或网络位置** - 在扫描范围中包括单个驱动器、文件夹或网络对象。然后通过单击“**浏览**”按钮选择所需的范围。
      - **文件** - 在扫描范围中包括单个文件。然后通过单击“**浏览**”按钮选择所需的范围。

      如果某个对象已经作为扫描范围的排除添加，则不能再将其添加到扫描范围中。
3. 要从扫描范围中排除单个节点，请清除这些节点名称旁边的复选框，或者执行以下步骤：
   a. 右键单击扫描范围打开其上下文菜单。
   b. 在上下文菜单中，选择“**添加排除**”选项。

c. 在“**添加排除**”窗口中选择对象类型，将按照将对象添加到扫描范围中时使用的步骤，将该对象类型作为扫描范围的排除添加。

4. 要修改添加的扫描范围或排除，请选择所需扫描范围上下文菜单中的“**编辑范围**”选项。

5. 若要在网络文件资源列表中隐藏之前添加的扫描范围或排除，请在相应扫描范围的上下文菜单中选择“**从列表删除**”选项。

将扫描范围从网络文件资源列表中删除时，该扫描范围也从“按需扫描”任务范围中排除。

6. 单击“**保存**”按钮。

“**扫描范围设置**”窗口将关闭。将保存新配置的设置。

在扫描范围内包含网络对象

您可以按照 UNC（通用命名惯例）格式指定网络驱动器、文件夹或文件的路径以将它们添加至扫描范围。

您可以在系统账户下扫描网络文件夹。

要将网络位置添加到扫描范围：

1. 打开“扫描范围设置”窗口。

2. 打开左上角部分中的下拉列表，然后选择“**树视图**”。

3. 在“**网络**”节点的上下文菜单中：

   - 选择“**添加网络文件夹**”，如果您想要向扫描范围中添加网络文件夹。
   - 选择“**添加网络文件**”，如果您想要向扫描范围中添加网络文件。

4. 以 UNC 格式输入网络文件夹或文件的路径，然后按 **ENTER** 键。

5. 选中新添加的网络对象旁边的复选框以将其包含在扫描范围内。

6. 如有必要，更改已添加的网络对象的安全性设置。

7. 单击“**保存**”按钮。

将保存修改的任务设置。

创建虚拟扫描范围

可以将虚拟驱动器、文件夹和文件包含在扫描范围内以创建虚拟扫描范围。

仅当扫描范围以文件资源树的形式显示时，您才可通过添加单个虚拟驱动器、文件夹或文件来扩展扫描范围。

要将虚拟驱动器添加到扫描范围：

1. 打开“扫描范围设置”窗口。
2. 打开左上角部分中的下拉列表，然后选择“**树视图**”。
3. 在受保护设备文件资源树中打开“**虚拟驱动器**”节点的上下文菜单，单击“**添加虚拟驱动器**”，然后从可用名称列表中选择虚拟驱动器名称。
4. 选中已添加的驱动器旁边的复选框，以将该驱动器包括在扫描范围中。
5. 单击“**保存**”按钮。

将保存修改的任务设置。

要将虚拟文件夹或虚拟文件添加到扫描范围：

1. 打开“扫描范围设置”窗口。
2. 打开左上角部分中的下拉列表，然后选择“**树视图**”。
3. 在受保护设备文件资源树中，打开节点的上下文菜单以添加文件夹或文件，然后选择以下选项之一：
   - **添加虚拟文件夹**，如果您想要向扫描范围中添加虚拟文件夹。
   - **添加虚拟文件**，如果您想要向扫描范围中添加虚拟文件。
4. 在输入字段中指定文件夹或文件的名称。
5. 在包含文件夹或文件的名称的行中，选中相应的复选框以将该文件夹或文件包含在扫描范围内。
6. 单击“**保存**”按钮。

将保存修改的任务设置。

配置安全性设置

默认情况下，按需扫描任务对整个扫描范围使用通用安全性设置。

这些设置对应于“**推荐**”预定义安全级别。

可以通过将安全性设置配置为用于整个扫描范围的常规设置，或配置为受保护设备文件资源列表或树中节点的不同项目的不同设置，来修改安全性设置的默认值。

在使用网络文件资源树时，为所选父节点配置的安全性设置将自动应用于所有子节点。父节点的安全设置不会应用到单独配置的子节点。

要手动配置安全设置：

1. 打开“扫描范围设置”窗口。
2. 在窗口的左侧部分中，选择要配置其安全性设置的节点或项。

   可以为扫描范围内的选定节点或项目应用包含安全设置的预定义模板。

在窗口的左侧部分，您可以选择网络文件资源的视图，创建扫描范围或创建虚拟扫描范围。

3. 在窗口的右侧部分，执行下列操作之一：

   - 在“**安全级别**”选项卡上，选择要应用的安全级别。
   - 在以下选项卡上根据要求配置选定节点或项目的所需安全设置：
     - 常规
     - 操作
     - 性能
     - 分级存储

4. 在“**扫描范围设置**”窗口中，单击“**保存**”。

将保存新的扫描范围设置。

为按需扫描任务选择预定义的安全级别

可以为受保护设备文件资源树或列表中的选定节点应用以下预定义安全级别之一：“**最优性能**”、“**推荐**”和“**最佳保护**”。

要选择其中一个预定义安全级别：

1. 打开“扫描范围设置”窗口。
2. 在受保护设备网络文件资源树或列表中，选择要设置预定义安全级别的节点或项。
3. 确保选定的节点或项包含在扫描范围中。
4. 在窗口右侧的“**安全级别**”选项卡中，选择要应用的安全级别。

   该窗口将显示与选定安全级别相对应的安全性设置列表。
5. 单击“**保存**”按钮。

   将保存任务设置，并将这些设置立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

配置常规任务设置

要配置按需扫描任务的常规安全性设置：

1. 打开“扫描范围设置”窗口。
2. 选择“**常规**”选项卡。
3. 在“**扫描对象**”组框中，指定要包含在扫描范围内的对象类型：

- 扫描对象：
  - 所有对象
  - 按格式扫描对象
  - 按反病毒数据库中指定的扩展名列表扫描对象
  - 按指定的扩展名列表扫描对象
- 扫描磁盘引导扇区和 MBR
- 扫描 NTFS 交换数据流

4. 在“性能”组框中，选中或清除“仅扫描新文件和已修改的文件”复选框。

> 要在该复选框处于清除状态时切换可用选项，请单击每个复合对象类型对应的“全部/仅新建”链接。

5. 在“扫描复合对象”组框中，指定要包含在扫描范围内的复合对象：
   - 全部/仅新的压缩文件
   - 全部/仅新的 SFX 压缩文件
   - 全部/仅新的电子邮件数据库
   - 全部/仅新的打包的对象
   - 全部/仅新的纯文本电子邮件
   - 全部/仅新的嵌入的 OLE 对象
6. 单击“保存”。

将保存新的任务配置。

配置操作

要为“按需扫描”任务配置对受感染的对象和其他检测到的对象的操作：

1. 打开“扫描范围设置”窗口。
2. 选择“操作”选项卡。
3. 选择要对受感染的对象和其他检测到的对象执行的操作：
   - 仅通知。
   - 清除。
   - 清除；清除失败时则删除。
   - 删除。

- 执行推荐的操作。

4. 选择要对疑似感染的对象执行操作：

   - 仅通知。
   - 隔离。
   - 删除。
   - 执行推荐的操作。

5. 根据检测的对象类型配置要对对象执行的操作：

   a. 清除或选中“根据检测到的对象的类型执行操作”复选框。

   b. 单击“设置”按钮。

   c. 在打开的窗口中，选择针对每种检测到的对象类型的主要操作和次要操作（如果主要操作失败则执行）。

   d. 单击“确定”。

6. 选择要对不可恢复的复合对象执行的操作：选中或清除“在检测到嵌入对象时完全删除应用程序无法修改的复合文件”复选框。

7. 单击“保存”。

将保存新的任务配置。

配置性能

要配置“按需扫描”任务的性能设置：

1. 打开“扫描范围设置”窗口。

2. 选择“性能”选项卡。

3. 在“排除”部分中：

   - 清除或选中“排除文件”复选框。
   - 清除或选中“不检测”复选框。
   - 针对每个设置单击“编辑”按钮以添加排除项。

4. 在“高级设置”部分中：

   - 超过以下时间则停止扫描(秒)
   - 不扫描大于该值的复合对象(MB)
   - 使用 iSwift 技术
   - 使用 iChecker 技术

5. 单击“保存”。

将保存新的任务配置。

配置分级存储

要为“按需扫描”任务配置对受感染的对象和其他检测到的对象执行的操作：

1. 打开“扫描范围设置”窗口。
2. 选择“分级存储”选项卡。
3. 选择要对文件执行的操作：
   - 不扫描。
   - 仅扫描文件驻留部分。
   - 扫描整个文件。
     如果选择此操作，则可以指定以下操作：
     - 选中或清除“仅当在指定的时间段(天)内访问了文件时”复选框并指定天数。
     - 选中或清除“如果可以，不复制文件到本地硬盘驱动器”复选框。
4. 单击“保存”。

将保存新的任务配置。

扫描可移动驱动器

要在应用程序控制台中配置在可移动驱动器连接到受保护设备时对其进行的扫描：

1. 在应用程序控制台树中，打开“Kaspersky Embedded Systems Security”节点的上下文菜单并选择“配置可移动驱动器扫描设置”选项。
   将打开“可移动驱动器扫描”窗口。
2. 在“连接时扫描”部分中，执行以下操作：
   - 如果想让 Kaspersky Embedded Systems Security 在可移动驱动器连接时自动扫描，请选择“扫描通过 USB 连接的可移动驱动器”复选框。
   - 如果需要，选中“扫描可移动驱动器，如果其存储的数据量未超过(MB)”，然后在右侧的字段中指定最大值。
   - 在“扫描时使用的安全级别”下拉列表中，指定可移动驱动器扫描所需设置的安全级别。
3. 单击“确定”。

即会保存并应用指定设置。

按需扫描任务统计

执行按需扫描任务时，您可以查看有关 Kaspersky Embedded Systems Security 自启动以来已处理的对象数量的信息。

即使任务暂停，也仍可查看该信息。您可以在任务日志中查看任务统计。

要查看按需扫描任务的统计：

1. 在应用程序控制台树中展开“**按需扫描**”节点。
2. 选择您要查看其统计的按需扫描任务。

任务统计显示在选定节点的结果窗格的“**统计**”部分中。

下表给出了 Kaspersky Embedded Systems Security 自启动以来已处理的对象的信息。

按需扫描任务统计

字段	描述
检测到	Kaspersky Embedded Systems Security 检测到的对象数量。例如，如果 Kaspersky Embedded Systems Security 在五个文件中检测到一个恶意对象，该字段中的值将增加 1。
检测到受感染和其他对象	Kaspersky Embedded Systems Security 发现并归类为“已感染”的对象数量，或者发现的未从扫描范围中排除且归类为可被入侵者用来破坏设备或个人数据的合法软件文件数量。
检测到疑似感染的对象	Kaspersky Embedded Systems Security 检测到的疑似感染对象数。
对象未清除	Kaspersky Embedded Systems Security 因以下原因未清除的对象数： • 检测到的对象是无法清除的类型。 • 清除期间出现错误。
对象未移至隔离区	Kaspersky Embedded Systems Security 尝试隔离未成功（例如，由于磁盘空间不足）的对象数。
对象未删除	Kaspersky Embedded Systems Security 尝试删除但无法删除（例如，由于其他应用程序阻止访问对象）的对象数。
对象未扫描	Kaspersky Embedded Systems Security 在保护范围中无法扫描（例如，其他应用程序阻止访问对象）的对象数。
对象未备份	Kaspersky Embedded Systems Security 尝试在备份中保存副本但未成功（例如，由于磁盘空间不足）的对象数。
处理错误	对其处理产生错误的对象数。
对象已清除	Kaspersky Embedded Systems Security 已清除的对象的数量。
已移至隔离区	Kaspersky Embedded Systems Security 已隔离的对象的数量。
已移动到备份	Kaspersky Embedded Systems Security 保存到备份的对象副本数。
对象已删除	Kaspersky Embedded Systems Security 已删除的对象的数量。

受密码保护的对象	因受到密码保护而被 Kaspersky Embedded Systems Security 跳过的对象（例如压缩文件）数量。
已损坏的对象	Kaspersky Embedded Systems Security 由于对象格式损坏而跳过的对象数。
对象已处理	Kaspersky Embedded Systems Security 已处理的对象的总数。

通过单击结果窗格中“**管理**”部分的“**打开任务日志**”链接，还可以在选定任务日志中查看按需扫描任务统计。

建议您在任务完成后手动处理任务日志中“**事件**”选项卡上记录的事件。

创建和配置“基线文件完整性监控”任务

要创建或配置新的“基线文件完整性监控”任务：

1. 在应用程序控制台树中，打开“**系统审查**”节点的上下文菜单。
2. 选择“**创建基线文件完整性监控任务**”。
   将打开“**添加任务**”窗口。
3. 在“**哈希计算算法**”下拉列表中，选择以下选项之一：
   - **MD5**
   - **SHA256**
4. 在“**扫描区域**”表中，执行以下操作：
   a. 要在“基线文件完整性监控”任务范围中添加文件或文件夹：
      1. 单击“**添加**”按钮。
         将打开“**扫描区域属性**”窗口。
      2. 选中或清除“**扫描此区域**”复选框。
      3. 单击“**浏览**”按钮以指定要包括在“基线文件完整性监控”任务范围中的文件或文件夹。
      4. 如果要在“基线文件完整性监控”任务范围中包括所有子文件夹，请选中“**同时扫描子文件夹**”复选框。
      5. 单击“**确定**”。
   b. 要更改先前添加到“基线文件完整性监控”任务范围的文件或文件夹：
      1. 单击“**更改**”按钮。
         将打开“**扫描区域属性**”窗口。
      2. 选中或清除“**扫描此区域**”复选框。
      3. 单击“**浏览**”按钮以指定要包括在“基线文件完整性监控”任务范围中的文件或文件夹。

4. 如果要在“基线文件完整性监控”任务范围中包括或排除所有子文件夹，请选中或清除“**同时扫描子文件夹**”复选框。

5. 单击“**确定**”。

c. 要删除先前添加到“基线文件完整性监控”任务范围中的文件或文件夹，请在“**扫描区域**”表中选择此文件或文件夹，然后单击“**删除**”按钮。

5. 配置“**计划**”和“**高级**”选项卡上的任务启动计划设置。

6. 在“**运行账户**”选项卡上，配置使用特定账户权限启动任务的设置。

7. 在“**添加任务**”窗口中单击“**确定**”。

即创建一个新的自定义“基线文件完整性监控”任务。将在应用程序控制台树中显示包含新任务名称的节点。此操作将会记录到系统审核日志中。

要打开“基线文件完整性监控”任务的设置：

1. 在应用程序控制台树中展开“**系统审查**”节点。

2. 选择与要配置的任务相应的子节点。

3. 在子节点结果窗格中，单击“**属性**”链接。

将打开“**任务设置**”窗口。

通过 Web 插件管理按需扫描任务

在本节中，学习如何针对网络中的一台或所有受保护设备导航 Web 插件界面。

打开按需扫描任务向导

要开始创建新的本地按需扫描任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。

2. 单击“**组**”选项卡以选择受保护设备所属的管理组。

3. 单击受保护设备名称。

4. 在打开的“**<设备名称>**”窗口中，选择“**任务**”选项卡。

5. 单击“**添加**”。

将打开“**添加任务向导**”窗口。

6. 在“**应用程序**”下拉列表中，选择“**Kaspersky Embedded Systems Security**”。

7. 在“**任务类型**”下拉列表中，选择“**按需扫描**”任务。

8. 单击“**下一步**”。

根据需要配置任务设置。

要开始创建新的组按需扫描任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击“**组**”选项卡以选择要为其创建任务的管理组。
3. 单击“**添加**”。
   将打开“**添加任务向导**”窗口。
4. 在“**应用程序**”下拉列表中，选择“**Kaspersky Embedded Systems Security**”。
5. 在“**任务类型**”下拉列表中，选择“**按需扫描**”任务。
6. 单击“**下一步**”。

根据需要配置任务设置。

要开始为自定义组创建新的按需扫描任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**设备选择**”。
2. 选择要为其创建任务的选择项。
3. 单击“**开始**”。
4. 在“**选择结果**”窗口中，选择要为其创建任务的设备。
5. 单击“**新建任务**”。
6. 在“**应用程序**”下拉列表中，选择“**Kaspersky Embedded Systems Security**”。
7. 在“**任务类型**”下拉列表中，选择“**按需扫描**”任务。
8. 单击“**下一步**”。

根据需要配置任务设置。

要配置现有按需扫描任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。

   将打开“**<任务名称>**”窗口。

打开按需扫描任务属性

要打开单台受保护设备的按需扫描任务的应用程序属性：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。
2. 单击“**组**”选项卡以选择受保护设备所属的管理组。

3. 单击受保护设备名称。

4. 在打开的“**<设备名称>**”窗口中，选择“**任务**”选项卡。

5. 在为设备创建的任务列表中，选择您创建的按需扫描任务。

6. 打开“**应用程序设置**”选项卡。

配置任务扫描范围

要配置现有按需扫描任务的扫描范围：

1. 打开按需扫描任务属性。

2. 选择“**扫描范围**”部分。

3. 执行以下操作之一：

   - 单击“**添加**”按钮以添加新规则。
   - 选择一个现有规则，然后单击“**编辑**”按钮。

   将打开“**编辑范围**”窗口。

4. 将切换按钮切换到“**活动**”，然后选择一个对象类型。

5. 在“**对象保护**”部分中，配置以下设置：

   - **对象保护模式**：
     - 所有对象
     - 按格式扫描对象
     - 按反病毒数据库中指定的扩展名列表扫描对象
     - 按指定的扩展名列表扫描对象
   - 子文件夹
   - 子文件
   - 扫描磁盘引导扇区和 **MBR**
   - 扫描 **NTFS** 交换数据流
   - 仅保护新文件和已修改的文件

6. 在“**复合对象保护**”部分中，指定要包含在扫描范围内的复合对象：

   - 压缩文件
   - **SFX** 压缩文件

- 打包的对象
- 电子邮件数据库
- 纯文本电子邮件
- 嵌入的 OLE 对象

7. 在“对受感染对象和其他对象执行的操作”部分中，选择要对受感染对象和其他检测到的对象执行的操作：
   - 仅通知。
   - 清除。
   - 清除；清除失败时则删除。
   - 删除。
   - 推荐。
8. 在“对疑似感染对象执行的操作”部分中，选择要对疑似感染对象执行的操作：
   - 仅通知。
   - 隔离。
   - 删除。
   - 推荐。
9. 在“对疑似感染对象执行的操作”部分中，选中或清除“在检测到嵌入对象时完全删除应用程序无法修改的复合文件”复选框。
10. 在“排除”部分中，配置以下设置：
    - 清除或选中“排除文件”复选框。
    - 清除或选中“不检测”复选框。
11. 在“高级设置”部分中，配置以下设置：
    - 超过以下时间则停止扫描(秒)
    - 不扫描大于该值的复合对象(MB)
    - 使用 iSwift 技术
    - 使用 iChecker 技术
12. 在“脱机文件处理”部分中，选择要对文件执行的操作：
    - 不扫描。
    - 仅扫描文件驻留部分。
    - 扫描整个文件。

如果选择此操作，则可以指定以下操作：

- 选中或清除“**仅当在指定的时间段(天)内访问了文件时**”复选框并指定天数。
- 选中或清除“**如果可以，不复制文件到本地硬盘驱动器**”复选框。

13. 单击“**确定**”按钮。

配置任务设置

要配置现有按需扫描任务的设置：

1. 打开按需扫描任务属性。
2. 选择“**选项**”部分。
3. 清除或选中“使用启发式分析”复选框。
4. 如有必要，使用“启发式分析级别”下拉列表选择分析级别。
5. 在“**与其他组件集成**”部分中，配置以下设置：
   - 如果您希望从任务的扫描范围中排除已添加到受信任区域列表的对象，则选中“应用信任区域”复选框。
   - 如果您想要在任务中使用卡巴斯基安全网络云服务，请选中“在扫描中使用 KSN”复选框。
   - 若要向将执行该任务的工作进程分配“*低*”优先级，请选中“在后台模式下执行任务”复选框。

     默认情况下，执行 Kaspersky Embedded Systems Security 任务的工作进程的优先级为“*中*”（正常）。

   - 要将所创建的任务用作关键区域扫描任务，请选中“将任务视为关键区域扫描”复选框。

受信任区域

本节提供了有关 Kaspersky Embedded Systems Security 中的信任区域的信息，以及如何在运行任务时将对象添加至信任区域的说明。

关于信任区域

受信任区域是保护或扫描范围的排除项列表，您可以生成并应用于按需扫描和实时文件保护任务、新创建的自定义按需扫描任务，以及除隔离扫描任务外的所有系统按需扫描任务。

默认情况下，在实时文件保护和按需扫描任务中应用信任区域。

可以将用于生成信任区域的规则列表导出为 XML 配置文件，然后再将其导入到其他受保护设备上运行的 Kaspersky Embedded Systems Security 中。

受信任进程

应用于实时文件保护任务。

如果受保护设备上某些应用程序访问的文件被 Kaspersky Embedded Systems Security 拦截，则这些应用程序可能不稳定。这些应用程序包括系统域控制器应用程序。

为了避免此类应用程序运行中断，您可以对这些应用程序的正在运行的进程所访问的文件禁用保护（从而在信任区域中创建受信任进程列表）。

Microsoft Corporation 推荐从实时文件保护排除某些 Microsoft Windows 操作系统文件和 Microsoft 应用程序文件，因为程序不会被感染。Microsoft 网站（文章代码：KB822158）上列出了一些此类文件的名称。

您可以在信任区域中启用或禁用受信任进程。

> 如果可执行文件被修改（例如更新），Kaspersky Embedded Systems Security 会将其从受信任进程列表中排除。

应用程序不使用文件在受保护设备上的路径来信任进程。受保护设备上的文件路径仅用于搜索文件、计算校验和以及为用户提供有关可执行文件源的信息。

备份操作

应用于实时计算机保护任务。

当将存储在硬盘驱动器上的数据备份到外部设备时，可以禁用备份操作过程中访问的对象的保护。Kaspersky Embedded Systems Security 将扫描备份应用程序打开并以 FILE_FLAG_BACKUP_SEMANTICS 属性读取的对象。

排除

- 应用于实时文件保护。

- 可在受保护设备的指定区域中检测到的所有对象。
- 在整个保护或扫描范围内按名称或名称掩码指定的可检测对象。

通过管理插件管理信任区域

在本节中，学习如何通过管理插件界面导航，以及如何为网络中的一台或所有受保护设备配置信任区域。

导航

了解如何通过所选界面导航到所需任务设置。

打开信任区域策略设置

要通过 Kaspersky Security Center 策略打开信任区域：

1. 展开 Kaspersky Security Center 管理控制台树中的**"受管理设备"**节点。
2. 选择要为其配置任务的管理组。
3. 选择**"策略"**选项卡。
4. 双击要配置的策略名称。
5. 在打开的**"属性：<策略名称>"**窗口中，选择**"补充"**部分。
6. 在**"信任区域"**子部分中单击**"设置"**按钮。
   将打开**"信任区域"**窗口。

根据需要配置信任区域。

如果某个受保护设备受 Kaspersky Security Center 活动策略管理，且该策略禁止更改应用程序设置，则无法通过应用程序控制台编辑这些设置。

打开信任区域属性窗口

要在"应用程序属性"窗口中配置信任区域：

1. 展开 Kaspersky Security Center 管理控制台树中的**"受管理设备"**节点。
2. 选择要为其配置任务的管理组。
3. 选择**"设备"**选项卡。

4. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：

   - 双击受保护设备的名称。
   - 在受保护设备的上下文菜单中选择“**属性**”项。

   将打开“**属性：<受保护设备名称>**”窗口。

5. 在“**应用程序**”部分中，选择“**Kaspersky Embedded Systems Security 3.2**”。
6. 单击“**属性**”按钮。
   将打开“**Kaspersky Embedded Systems Security 3.2 应用程序设置**”窗口。
7. 选择“**补充**”部分。
8. 在“**信任区域**”子部分中单击“**设置**”按钮。
   将打开“**信任区域**”窗口。

根据需要配置信任区域。

通过管理插件配置信任区域设置

默认情况下，信任区域应用于所有新创建的策略和任务。

要配置信任区域设置：

1. 在“**排除**”选项卡上指定 Kaspersky Embedded Systems Security 在任务执行过程中跳过的对象。
2. 在“**受信任进程**”选项卡上指定 Kaspersky Embedded Systems Security 在任务执行过程中跳过的进程。
3. 应用 not-a-virus 掩码。

添加排除

要通过 Kaspersky Security Center 策略向信任区域添加排除：

1. 打开“信任区域”窗口。
2. 在“**排除**”选项卡上，指定扫描和保护期间 Kaspersky Embedded Systems Security 要跳过的对象：

   - 要创建推荐的排除项，请单击“添加推荐的排除项”按钮。
   - 要导入预配置的排除项，请单击**导入**按钮，然后在打开的窗口中选择存储在设备上的 XML 格式的配置文件。

     XML 文件中的排除项将添加到排除列表中。
   - 要手动指定将对象视为受信任的条件，请单击“**添加**”按钮并继续执行下一步。
     将打开“**排除**”窗口。

3. 如果您单击了**添加**按钮，在“**如果满足以下条件，将不扫描对象**”部分中，指定要从保护/扫描范围中排除的对象以及要从可检测对象中排除的对象：

   - 如果要从保护或扫描范围中排除对象：

     a. 选中“要扫描的对象”复选框。

     b. 单击“**编辑**”按钮。

     将打开“**选择对象**”窗口。

     c. 指定要从扫描范围中排除的对象。

     > 指定对象时，可以使用名称掩码（通过 ? 和 * 字符）和所有类型的环境变量。当启动任务或将新设置应用于正在运行的任务（不适用于按需扫描任务）时，Kaspersky Embedded Systems Security 执行环境变量的解析（将变量替换为其值）。Kaspersky Embedded Systems Security 在用于启动任务的账户下解析环境变量。有关环境变量的详细信息，请参阅 Microsoft 知识库。

     d. 单击“**确定**”。

     e. 如果要从保护或扫描范围中排除指定对象的所有子文件和文件夹，则选中“**应用于子文件夹**”复选框。

   - 如果要指定可检测对象的名称：

     a. 选中“检测对象”复选框。

     b. 单击“**编辑**”按钮。

     将打开“**检测对象列表**”窗口。

     c. 按照病毒百科全书分类指定可检测对象的名称或名称掩码。

     d. 单击“**添加**”按钮。

     e. 单击“**确定**”。

4. 在“排除使用范围”部分中，选中应将排除应用于的任务的名称旁边的复选框。

5. 单击“**确定**”。

排除显示在“**信任区域**”窗口的“**排除**”选项卡上的列表中。

添加受信任进程

要向受信任进程列表中添加一个或多个进程：

1. 打开“信任区域”窗口。

2. 选择“**受信任进程**”选项卡。

3. 选中“不检查文件备份操作”复选框可跳过对文件读取操作的扫描。

4. 选中“不检查指定进程的文件活动”复选框可跳过对受信任进程的文件操作扫描。

5. 要将进程添加至受信任进程列表，请执行以下操作之一：

- 要导入预配置的受信任进程，请单击**导入**按钮，然后在打开的窗口中选择存储在设备上的 XML 格式的配置文件。

  XML 文件中的进程将添加到受信任进程列表中。

- 要手动指定流程，请单击“**添加**”按钮并继续执行下一步。

6. 如果单击了“**添加**”按钮，请在该按钮的上下文菜单中选择以下选项之一：

- **多个进程**。

  在打开的“**添加信任进程**”窗口中，配置以下设置：

  a. 使用磁盘上的完整进程路径来将它视为受信任。

  b. 使用进程文件哈希来将它视为受信任。

  c. 单击“**浏览**”按钮以根据可执行进程添加数据。

  d. 在打开的窗口中选择可执行文件。

  > 一次只能添加一个可执行文件。重复步骤 c-d 以添加其他可执行文件。

  e. 单击“**进程**”按钮以根据正在运行的进程添加数据。

  f. 在打开的窗口中选择进程。要选择多个进程，请在选择时按住 **CTRL** 键。

  g. 单击“**确定**”。

  > 运行实时文件保护任务的账户在装有 Kaspersky Embedded Systems Security 的设备上必须具有管理员权限，才允许查看活动进程列表。您可以按文件名、进程标识符 (PID) 或进程的可执行文件在受保护设备上的路径来对活动进程列表中的进程进行排序。请注意，只有在受保护设备上或通过 Kaspersky Security Center 以指定的主机设置使用应用程序控制台时，才能通过单击“**进程**”按钮来选择正在运行的进程。

- **一个基于文件名和路径的进程**。

  在打开的“**添加进程**”窗口中，执行以下操作：

  a. 输入可执行文件的路径（包括文件名）。

  > 指定对象时，可以使用名称掩码（通过 ? 和 * 字符）和所有类型的环境变量。当启动任务或将新设置应用于正在运行的任务（不适用于按需扫描任务）时，Kaspersky Embedded Systems Security 执行环境变量的解析（将变量替换为其值）。Kaspersky Embedded Systems Security 在用于启动任务的账户下解析环境变量。有关环境变量的详细信息，请参阅 Microsoft 知识库。

  b. 单击“**确定**”。

- **一个基于对象属性的进程**。

  在打开的“**添加受信任进程**”窗口中，配置以下设置：

  a. 单击“**浏览**”按钮以选择进程。

b. 使用磁盘上的完整进程路径来将它视为受信任。

c. 使用进程文件哈希来将它视为受信任。

d. 单击“**确定**”。

要将所选进程添加到受信任进程列表，必须选择至少一种信任条件。

7. 在“**信任区域**”窗口中，单击“**确定**”按钮。

选定的文件或进程将添加到“**信任区域**”窗口中的受信任进程列表。

应用 not-a-virus 掩码

not-a-virus 掩码允许跳过可能被视为有害的合法软件文件和 Web 资源的扫描。该掩码影响以下任务：

- 实时文件保护。
- 按需扫描。

如果未向排除列表添加该掩码，Kaspersky Embedded Systems Security 将对此类别下的软件应用在任务设置中指定的操作。

要应用 not-a-virus 掩码：

1. 打开“**信任区域**”窗口。
2. 如果清除该复选框，则在“**排除**”选项卡上的“**检测对象**”列中，滚动列表并选择具有“not-a-virus:*”的行。
3. 单击“**确定**”。

即应用新配置。

通过应用程序控制台管理信任区域

在本节中，学习如何通过应用程序控制台界面导航以及如何在受保护设备上配置信任区域。

在应用程序控制台中对任务应用信任区域

默认情况下，信任区域应用于“实时文件保护”任务、新建的自定义“按需扫描”任务以及除“隔离区扫描”任务之外的所有系统“按需扫描”任务。

启用或禁用信任区域后，会在运行的任务内立即应用或停止应用指定的排除。

要在 Kaspersky Embedded Systems Security 任务中启用和禁用信任区域：

1. 在应用程序控制台树中，打开要为其配置使用信任区域的任务的上下文菜单。
2. 选择“**属性**”。

将打开“**任务设置**”窗口。

3. 在打开的窗口中，选择“**常规**”选项卡，然后执行以下操作之一：

   - 要在任务中应用信任区域，请选中“**应用信任区域**”复选框。
   - 要在任务中禁用信任区域，请清除“**应用信任区域**”复选框。

4. 如果要配置信任区域设置，请单击“**应用信任区域**”复选框的名称中的链接。
   将打开“**信任区域**”窗口。
   在“**信任区域**”窗口中，配置排除项和受信任进程，然后单击“**确定**”。

5. 单击“**任务设置**”窗口中的“**确定**”保存更改。

在应用程序控制台中配置信任区域设置

要配置信任区域设置：

1. 在“**排除**”选项卡上指定 Kaspersky Embedded Systems Security 在任务执行过程中跳过的对象。
2. 在“**受信任进程**”选项卡上指定 Kaspersky Embedded Systems Security 在任务执行过程中跳过的进程。
3. 对应用程序任务应用信任区域。
4. 应用 not-a-virus 掩码。

将排除添加至信任区域

要通过应用程序控制台手动向信任区域添加排除项：

1. 在应用程序控制台树中，打开 **Kaspersky Embedded Systems Security** 节点的上下文菜单。
2. 选择“**配置信任区域设置**”菜单选项。
   将打开“**信任区域**”窗口。
3. 选择“**排除**”选项卡。
4. 指定 Kaspersky Embedded Systems Security 在扫描和保护过程中跳过的对象：

   - 要导入预配置的排除项，请单击**导入**按钮，然后在打开的窗口中选择存储在设备上的 XML 格式的配置文件。
     XML 文件中的排除项将添加到排除列表中。
   - 要手动指定将对象视为受信任的条件，请单击“**添加**”按钮并继续执行下一步。
     将打开“**排除**”窗口。

5. 如果您单击了**添加**按钮，在“**如果满足以下条件，将不扫描对象**”部分中，指定要从保护/扫描范围中排除的对象以及要从可检测对象中排除的对象：

- 如果要从保护或扫描范围中排除对象：

  a. 选中“要扫描的对象”复选框。

  b. 单击“**编辑**”按钮。
  将打开“**选择对象**”窗口。

  c. 指定要从扫描范围中排除的对象。

  > 指定对象时，可以使用名称掩码（通过 ? 和 * 字符）和所有类型的环境变量。当启动任务或将新设置应用于正在运行的任务（不适用于按需扫描任务）时，Kaspersky Embedded Systems Security 执行环境变量的解析（将变量替换为其值）。Kaspersky Embedded Systems Security 在用于启动任务的账户下解析环境变量。有关环境变量的详细信息，请参阅 Microsoft 知识库。

  d. 单击“**确定**”。

  e. 如果要从保护或扫描范围中排除指定对象的所有子文件和文件夹，则选中“**应用于子文件夹**”复选框。

- 如果要指定可检测对象的名称：

  a. 选中“检测对象”复选框。

  b. 单击“**编辑**”按钮。
  将打开“**检测对象列表**”窗口。

  c. 按照病毒百科全书分类指定可检测对象的名称或名称掩码。

  d. 单击“**添加**”按钮。

  e. 单击“**确定**”。

6. 在“排除使用范围”部分中，选中应将排除应用于的任务的名称旁边的复选框。
7. 单击“**确定**”。

排除显示在“**信任区域**”窗口的“**排除**”选项卡上的列表中。

添加受信任进程

您可以使用以下某种方法将进程添加至受信任进程列表：

- 从受保护设备上正在运行的进程列表中选择进程。
- 选择进程的可执行文件（不管进程当前是否正在运行）。

> 如果进程的可执行文件已修改，Kaspersky Embedded Systems Security 会将此进程从受信任进程列表排除。

要向受信任进程列表中添加一个或多个进程：

1. 在应用程序控制台树中，打开 **Kaspersky Embedded Systems Security** 节点的上下文菜单。

2. 选择“**配置信任区域设置**”菜单选项。

   将打开“**信任区域**”窗口。

3. 选择“**受信任进程**”选项卡。

4. 选中“不检查文件备份操作”复选框可跳过对文件读取操作的扫描。

5. 选中“不检查指定进程的文件活动”复选框可跳过对受信任进程的文件操作扫描。

6. 要将进程添加至受信任进程列表，请执行以下操作之一：

   - 要导入预配置的受信任进程，请单击**导入**按钮，然后在打开的窗口中选择存储在设备上的 XML 格式的配置文件。

     XML 文件中的进程将添加到受信任进程列表中。

   - 要手动指定流程，请单击“**添加**”按钮并继续执行下一步。

7. 如果单击了“**添加**”按钮，请在该按钮的上下文菜单中选择以下选项之一：

   - **多个进程**。

     在打开的“**添加信任进程**”窗口中，配置以下设置：

     a. 使用磁盘上的完整进程路径来将它视为受信任。

     b. 使用进程文件哈希来将它视为受信任。

     c. 单击“**浏览**”按钮以根据可执行进程添加数据。

     d. 在打开的窗口中选择可执行文件。

     > 一次只能添加一个可执行文件。重复步骤 c-d 以添加其他可执行文件。

     e. 单击“**进程**”按钮以根据正在运行的进程添加数据。

     f. 在打开的窗口中选择进程。要选择多个进程，请在选择时按住 **CTRL** 键。

     g. 单击“**确定**”。

     > 运行实时文件保护任务的账户在装有 Kaspersky Embedded Systems Security 的设备上必须具有管理员权限，才允许查看活动进程列表。您可以按文件名、进程标识符 (PID) 或进程的可执行文件在受保护设备上的路径来对活动进程列表中的进程进行排序。请注意，只有在受保护设备上或通过 Kaspersky Security Center 以指定的主机设置使用应用程序控制台时，才能通过单击“**进程**”按钮来选择正在运行的进程。

   - **一个基于文件名和路径的进程**。

     在打开的“**添加进程**”窗口中，执行以下操作：

     a. 输入可执行文件的路径（包括文件名）。

指定对象时，可以使用名称掩码（通过 ? 和 * 字符）和所有类型的环境变量。当启动任务或将新设置应用于正在运行的任务（不适用于按需扫描任务）时，Kaspersky Embedded Systems Security 执行环境变量的解析（将变量替换为其值）。Kaspersky Embedded Systems Security 在用于启动任务的账户下解析环境变量。有关环境变量的详细信息，请参阅 Microsoft 知识库。

b. 单击“**确定**”。

- **一个基于对象属性的进程。**
  在打开的“**添加受信任进程**”窗口中，配置以下设置：

  a. 单击“**浏览**”按钮以选择进程。

  b. 使用磁盘上的完整进程路径来将它视为受信任。

  c. 使用进程文件哈希来将它视为受信任。

  d. 单击“**确定**”。

要将所选进程添加到受信任进程列表，必须选择至少一种信任条件。

8. 在“**信任区域**”窗口中，单击“**确定**”按钮。

选定的文件或进程将添加到“**信任区域**”窗口中的受信任进程列表。

应用 not-a-virus 掩码

not-a-virus 掩码允许跳过可能被视为有害的合法软件文件和 Web 资源的扫描。该掩码影响以下任务：

- 实时文件保护。
- 按需扫描。

如果未向排除列表添加该掩码，Kaspersky Embedded Systems Security 将对此类别下的软件或 Web 资源应用在任务设置中指定的操作。

要应用 not-a-virus 掩码：

1. 在应用程序控制台树中，打开 **Kaspersky Embedded Systems Security** 节点的上下文菜单。
2. 选择“**配置信任区域设置**”菜单选项。
   将打开“**信任区域**”窗口。
3. 选择“**排除**”选项卡。
4. 滚动列表以查找 *not-a-virus:** 值。
5. 选中相应的复选框（如果其处于清除状态）。
6. 单击“**确定**”。

即应用新配置。

通过 Web 插件管理信任区域

要通过 Web 插件管理信任区域：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**补充**”部分。
5. 在“**信任区域**”子部分中单击“**设置**”。
6. 根据需要配置信任区域。

漏洞利用防御

本节包含有关如何配置进程内存保护设置的说明。

关于漏洞利用防御

Kaspersky Embedded Systems Security 提供保护进程内存免受漏洞利用的能力。此功能在“漏洞利用防御”组件中实现。可以更改该组件的活动状态和配置进程内存保护设置。

该组件通过在受保护的进程中插入外部“进程保护代理”（“代理”）保护进程内存免受漏洞利用。

“进程保护代理”是一个动态加载的 Kaspersky Embedded Systems Security 模块，该模块可以插入到受保护的进程中，以便监控进程的完整性并降低被漏洞利用的风险。

该代理在受保护的进程内的运行需要启动和停止进程：只有进程已重启，才能实现首次加载代理到已添加到受保护的进程列表中。此外，从受保护的进程列表中删除进程后，只有该进程已重启才能卸载代理。

必须停止代理才能从受保护的进程中卸载它：如果已卸载“漏洞利用防御”组件，则应用程序将冻结环境并强制从受保护的进程中卸载代理。如果在组件卸载过程中在任一受保护进程中插入代理，则必须终止受影响的进程。可能需要重新启动受保护设备（例如，如果系统进程正在受到保护）。

如果检测到受保护的进程中存在漏洞利用攻击的迹象，则 Kaspersky Embedded Systems Security 执行以下操作之一：

- 如果进行漏洞利用尝试，则终止该进程。
- 报告进程已遭到入侵的事实。

您可采用以下方法之一停止进程保护：

- 卸载该组件。
- 从受保护的进程列表中删除该进程并重启该进程。

Kaspersky Security 漏洞利用防御服务

受保护设备上必须提供 Kaspersky Security 漏洞利用防御服务，这样“漏洞利用防御”组件才能发挥最大效果。此服务和“漏洞利用防御”组件是推荐安装的一部分。在受保护设备上安装该服务的过程中，将创建和启动 kavfswh 进程。此进程从组件将有关受保护的进程的信息传输到安全性代理。

Kaspersky Security 漏洞利用防御服务停止后，Kaspersky Embedded Systems Security 继续保护已添加到受保护的进程列表中的进程，同时也加载到新添加的进程中，并使用所有可用的漏洞利用防御技术来保护进程内存。

如果设备正在运行 Windows 10 或更高版本的操作系统，在 Kaspersky Security 漏洞利用防御服务停止后，应用程序将不会继续保护进程和进程内存。

如果 Kaspersky Security 漏洞利用防御服务已停止，则应用程序将不会接收随受保护的进程出现的有关事件的信息（包括有关漏洞利用攻击和进程终止的信息）。此外，代理将无法接收新保护设置和添加新进程到受保护的进程列表中的有关信息。

漏洞利用防御模式

可以选择以下一种模式来配置所执行的操作，以降低漏洞在受保护进程中被利用的风险：

- **发现漏洞利用时终止**：当尝试进行漏洞利用时，应用此模式可终止进程。

  当检测到尝试在受保护的关键操作系统进程中利用漏洞时，无论“漏洞利用防御”组件设置中所指定的模式如何，Kaspersky Embedded Systems Security 都不会终止进程。

- **仅通知**：应用此模式可以使用安全日志中的事件来接收受保护进程中的漏洞实例的有关信息。
  如果选择此模式，Kaspersky Embedded Systems Security 将创建事件来记录所有漏洞利用尝试。

通过管理插件管理漏洞利用防御

在本节中，学习如何导航管理插件界面，以及如何为网络中的一台或所有受保护设备配置组件设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开漏洞利用防御的策略设置

要通过 Kaspersky Security Center 策略打开漏洞利用防御设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在打开的“**属性：<策略名称>**”窗口中，选择“**实时计算机保护**”部分。
6. 在“**漏洞利用防御**”子部分中单击“**设置**”按钮。
   将打开“**漏洞利用防御**”窗口。

根据需要配置漏洞利用防御。

打开漏洞利用防御属性窗口

要打开漏洞利用防御的属性窗口：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**设备**”选项卡。
4. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：
   - 双击受保护设备的名称。
   - 在受保护设备的上下文菜单中选择“**属性**”项。

   将打开“**属性：<受保护设备名称>**”窗口。
5. 在“**应用程序**”部分中，选择“**Kaspersky Embedded Systems Security 3.2**”。
6. 单击“**属性**”按钮。
   将打开“**Kaspersky Embedded Systems Security 3.2 应用程序设置**”窗口。
7. 选择“**实时计算机保护**”部分。
8. 在“**漏洞利用防御**”子部分中单击“**设置**”按钮。
   将打开“**漏洞利用防御**”窗口。

根据需要配置漏洞利用防御。

配置进程内存保护设置

要配置设置以保护添加到受保护的进程列表中的进程内存，请执行以下操作：

1. 打开“漏洞利用防御”窗口。
2. 在“**漏洞利用防御模式**”设置块中，配置以下设置：
   - 防止易受感染的进程被漏洞利用。
     - 发现漏洞利用时终止。
     - 仅通知。
3. 在“**防御操作**”设置块中，配置以下设置：
   - 通过“终端服务”通知被利用的进程。
   - 即使 Kaspersky Security 服务已禁用，也会防止易受感染的进程被利用漏洞。
4. 在“**漏洞利用防御**”窗口中单击“**确定**”。

Kaspersky Embedded Systems Security 将保存并应用配置的进程内存保护设置。

将进程添加到保护范围

默认情况下，“漏洞利用防御”组件保护多个进程。可以通过清除列表中的相应复选框来将进程从保护范围中排除。

要向受保护的进程列表中添加进程：

1. 打开“漏洞利用防御”窗口。
2. 在“**受保护进程**”选项卡上，单击“**浏览**”按钮。
   将打开一个 Microsoft Windows 资源管理器窗口。
3. 选择您要添加到该列表的进程。
4. 单击“**打开**”按钮。
   进程名称显示在行中。
5. 单击“**添加**”按钮。
   进程将被添加到受保护的进程列表中。
6. 选择添加的进程。
7. 单击“**设置漏洞利用防御技术**”。
   将打开“**漏洞利用防御技术**”窗口。
8. 选择其中一个选项以应用攻击缓解技术：
   - **应用所有可用的漏洞利用防御技术**。
     如果选择此选项，则不能编辑列表。默认情况下，对进程应用所有可用技术。
   - **应用所选的漏洞利用防御技术**。
     如果选择此选项，则您可以编辑已应用攻击缓解技术：
     a. 选择您要应用的技术旁边的复选框，以保护选定的进程。
     b. 选中或清除“**应用攻击面减少技术**”复选框。
9. 配置“受攻击面减少”技术的设置：
   - 输入其启动将受到“**拒绝模块**”字段中受保护的进程阻止的模块的名称。
   - 在“**不拒绝在 Internet 区域中启动的模块**”字段中，选中您要允许模块启动的选项旁边的复选框：
     - **Internet**
     - **本地 Intranet**
     - **受信任 URL**
     - **受限制的 URL**
     - **计算机**

这些设置仅适用于 Internet Explorer®。

10. 单击“**确定**”。

该进程将添加到任务保护范围中。

通过应用程序控制台管理漏洞利用防御

在本节中，学习如何导航应用程序控制台界面以及如何在受保护设备上配置组件设置。

导航

了解如何通过所选界面导航到所需任务设置。

打开漏洞利用防御常规设置

*要打开“**漏洞利用防御设置**”窗口：*

1. 在应用程序控制台树中展开“**实时文件保护**”节点。
2. 选择“**漏洞利用防御**”节点。
3. 在“进程保护设置”部分中，单击“**属性**”链接。
   将打开“**漏洞利用防御设置**”窗口。

根据需要配置漏洞利用防御的常规设置。

打开漏洞利用防御进程保护设置

*要打开“**进程保护设置**”窗口：*

1. 在应用程序控制台树中展开“**实时文件保护**”节点。
2. 选择“**漏洞利用防御**”节点。

在“进程保护设置”部分中，单击“**进程保护参数**”链接。

将打开“进程保护设置”窗口。

根据需要配置漏洞利用防御的进程保护设置。

配置进程内存保护设置

要向受保护的进程列表中添加进程：

1. 打开“漏洞利用防御设置”窗口。
2. 在“**漏洞利用防御模式**”设置块中，配置以下设置：

- 防止易受感染的进程被漏洞利用。
  - 发现漏洞利用时终止。
  - 仅通知。

3. 在“防御操作”设置块中，配置以下设置：
   - 通过“终端服务”通知被利用的进程。
   - 即使 Kaspersky Security 服务已禁用，也会防止易受感染的进程被利用漏洞。
4. 在“漏洞利用防御设置”窗口中单击“确定”。

Kaspersky Embedded Systems Security 将保存并应用配置的进程内存保护设置。

将进程添加到保护范围

默认情况下，“漏洞利用防御”组件保护多个进程。您可以在受保护进程列表中取消选中您不想保护的进程。

要向受保护的进程列表中添加进程：

1. 打开“进程保护设置”窗口。
2. 要添加进程以保护其不被滥用并减少可能的漏洞利用影响，请执行以下操作：
   a. 单击“浏览”按钮。
   将打开标准 Microsoft Windows“打开”窗口。
   b. 在打开的窗口中，选择您要添加到该列表的进程。
   c. 单击“打开”按钮。
   d. 单击“添加”按钮。
   进程将被添加到受保护的进程列表中。
3. 在列表中选择进程。
4. 当前配置显示在“进程保护设置”选项卡上：
   - 进程名称。
   - 正在被执行。
   - 已应用的漏洞利用防御技术。
   - 攻击面减少设置。
5. 要修改应用于该进程的漏洞利用防御技术，请选择“拒绝加载模块”选项卡。
6. 选择其中一个选项以应用攻击缓解技术：
   - 应用所有可用的漏洞利用防御技术。

如果选择此选项，则不能编辑列表。默认情况下，对进程应用所有可用技术。

- **对进程应用列出的漏洞利用防御技术**。
  如果选择此选项，则您可以编辑已应用攻击缓解技术：

  a. 选择您要应用的技术旁边的复选框，以保护选定的进程。

7. 配置“受攻击面减少”技术的设置：

   - 输入其启动将受到“**拒绝模块**”字段中受保护的进程阻止的模块的名称。
   - 在“**不拒绝在 Internet 区域中启动的模块**”部分中，选中您要允许模块启动的选项旁边的复选框：
     - **Internet**
     - **本地 Intranet**
     - **受信任 URL**
     - **受限制的站点**
     - **计算机**

     这些设置仅适用于 Internet Explorer。

8. 单击“**保存**”。

该进程将添加到任务保护范围中。

通过 Web 插件管理漏洞利用防御

在本节中，学习如何导航 Web 插件界面以及如何在受保护设备上配置组件设置。

配置进程内存保护设置

要配置设置以保护添加到受保护的进程列表中的进程内存，请执行以下操作：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时计算机保护**”部分。
5. 在“**漏洞利用防御**”子部分中单击“**设置**”。
6. 打开“**漏洞利用防御设置**”选项卡。
7. 在“**漏洞利用防御模式**”设置块中，配置以下设置：

- 防止易受感染的进程被漏洞利用。
  - 发现漏洞利用时终止。
  - 仅通知。

8. 在“**防御操作**”设置块中，配置以下设置：
   - 通过“**终端服务**”通知被利用的进程。
   - 即使 **Kaspersky Security** 服务已禁用，也会防止易受感染的进程被利用漏洞。
9. 在“**漏洞利用防御**”窗口中单击“**确定**”。

Kaspersky Embedded Systems Security 将保存并应用配置的进程内存保护设置。

将进程添加到保护范围

要配置设置以保护添加到受保护的进程列表中的进程内存，请执行以下操作：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**实时计算机保护**”部分。
5. 在“**漏洞利用防御**”子部分中单击“**设置**”。
6. 打开“**受保护进程**”选项卡。
7. 单击“**添加**”按钮。
8. 将打开“**漏洞利用防御技术**”窗口。
9. 指定进程名称。
10. 选择其中一个选项以应用攻击缓解技术：
    - **应用所有可用的漏洞利用防御技术**。
      如果选择此选项，则不能编辑列表。默认情况下，对进程应用所有可用技术。
    - **应用所选的漏洞利用防御技术**。
      如果选择此选项，则您可以编辑已应用攻击缓解技术：
      a. 选择您要应用的技术旁边的复选框，以保护选定的进程。
      b. 选中或清除“**应用攻击面减少技术**”复选框。
11. 配置“受攻击面减少”技术的设置：
    - 输入其启动将受到“**拒绝模块**”字段中受保护的进程阻止的模块的名称。

- 在“不拒绝在 Internet 区域中启动的模块”字段中，选中您要允许模块启动的选项旁边的复选框：
  - Internet
  - 本地 Intranet
  - 受信任 URL
  - 受限制的 URL
  - 计算机

这些设置仅适用于 Internet Explorer®。

12. 单击“确定”。

该进程将添加到任务保护范围中。

漏洞利用防御技术

漏洞利用防御技术

漏洞利用防御技术	描述
数据执行保护 (DEP)	数据执行保护阻止在受保护的内存区域中执行任意代码。
地址空间布局随机化 (ASLR)	改变进程地址空间内数据结构布局。
结构化异常处理程序覆盖保护 (SEHOP)	异常记录的替换或异常处理程序的替换。
空页分配	保护重定向空指针。
LoadLibrary 网络调用检查（反 ROP）	防止从网络路径加载 DLL。
可执行文件堆栈（反 ROP）	阻止堆栈区域的非授权执行。
反 RET 检查（反 ROP）	检查确保安全调用 CALL 指令。
反堆栈透视（反 ROP）	防止将 ESP 堆栈指针重新定位到可执行文件地址。
简单导出地址表访问监视（EAT 访问监视和通过调试寄存器的 EAT 访问监视）	防止对 kernel32.dll、kernelbase.dll 和 ntdll.dll 导出地址表的读取访问
堆喷射分配 (Heapspray)	防止将内存分配用于执行恶意代码。
执行流模拟（反返回导向编程）	检测 Windows API 组件中可能存在危险的指令链（潜在 ROP 小工具）。
IntervalProfile 调用监视（辅助功能驱动程序保护 (AFDP)）	防止通过 AFD 驱动程序中的漏洞进行提权（通过 QueryIntervalProfile 调用在 Ring 0 中执行任意代码）。
受攻击面减少 (ASR)	通过受保护的进程阻止启动易受攻击的加载项。
反进程挖空 (Hollowing)	防止创建和执行受信任进程的恶意副本。
反 AtomBombing (APC)	通过异步过程调用 (APC) 利用全局原子表漏洞。
反 CreateRemoteThread (RThreadLocal)	其他进程已在受保护进程中创建线程。
反 CreateRemoteThread (RThreadRemote)	受保护进程已在其他进程中创建线程。

与第三方系统集成

本节介绍 Kaspersky Embedded Systems Security 与第三方功能和技术的集成。

系统监控器的性能计数器

本节包含有关安装期间由 Kaspersky Embedded Systems Security 在 Microsoft Windows 系统监视器中注册的性能计数器的信息。

关于 Kaspersky Embedded Systems Security 性能计数器

默认情况下，“性能计数器”组件包含在 Kaspersky Embedded Systems Security 的已安装组件中。Kaspersky Embedded Systems Security 在安装期间在 Microsoft Windows 系统监视器中注册其自己的性能计数器。

使用 Kaspersky Embedded Systems Security 计数器，您可以在运行实时计算机保护任务的同时监控应用程序的性能。当它与其他应用程序一起运行并出现资源不足时，您可以确定瓶颈。您可以诊断 Kaspersky Embedded Systems Security 崩溃并确定不合要求的设置。

通过在 Windows 控制面板的“**管理**”部分中打开“**性能**”控制台，可以查看 Kaspersky Embedded Systems Security 性能计数器。

下列章节列出了计数器定义、获取读数的推荐时间间隔、阈值以及在计数器值超过阈值时推荐的 Kaspersky Embedded Systems Security 设置。

拒绝请求总数

拒绝请求总数

名称	拒绝请求总数
定义	由文件拦截驱动程序发出但未被应用程序进程接受的对象处理请求总数；从 Kaspersky Embedded Systems Security 上次启动时开始计数。 应用程序将跳过被 Kaspersky Embedded Systems Security 进程拒绝处理请求的对象。
用途	该计数器可帮您检测： • 由于 Kaspersky Embedded Systems Security 进程过载而导致的实时计算机保护能力下降。 • 由于文件拦截调度程序故障而导致的实时计算机保护中断。
标准值/阈值	0 / 1。
推荐的读取时间间隔	1 小时。
在计数器值超过阈值时的配置推荐	被拒绝的处理请求数量与跳过的对象数量相对应。 根据计数器行为的不同，可能出现下列情况： • 计数器在较长的时间段内显示了许多被拒绝的请求：由于完全加载了所有 Kaspersky Embedded Systems Security 进程，Kaspersky Embedded Systems Security 无法扫描对象。

	要避免跳过对象，请增加用于完成实时计算机保护任务的应用程序进程的数量。您可以使用“**用于实时保护的进程数**”等 Kaspersky Embedded Systems Security 设置。 • 被拒绝的请求数量大大超过关键阈值并且正在迅速增长：文件拦截调度程序已经崩溃。Kaspersky Embedded Systems Security 在对象被访问时不扫描对象。 重新启动 Kaspersky Embedded Systems Security。

跳过请求总数

跳过请求总数

名称	跳过请求总数
定义	由文件拦截驱动程序发出且被 Kaspersky Embedded Systems Security 收到但未生成处理完成事件的对象处理请求总数；此数字从应用程序上次启动时开始计数。 如果某个对象处理请求被一个工作进程接受但未发送处理完成事件，则驱动程序会将该请求转移给其他进程，并且计数器“**跳过请求总数**”的值将增加 1。如果驱动程序已经遍历所有工作进程，并且没有任何进程收到该处理请求（全部都在忙碌）或发送处理完成事件，则 Kaspersky Embedded Systems Security 将跳过该对象，因此计数器“**跳过请求总数**”的值将增加 1。
用途	该计数器使您能够检测由于文件拦截调度程序故障而出现的性能下降情况。
标准值/阈值	0 / 1
推荐的读取时间间隔	1 小时
在计数器值超过阈值时的配置推荐	如果计数器不为零，则意味着一个或多个文件拦截调度程序流已冻结和关闭。该计数器值对应于当前关闭的流数量。 如果扫描速度不能令人满意，请重启 Kaspersky Embedded Systems Security，以便还原脱机流。

由于缺乏系统资源而未处理的请求数量

由于缺乏系统资源而未处理的请求数量

名称	由于缺乏资源而未处理的请求数量。
定义	来自文件拦截驱动程序但由于缺乏系统资源（例如，RAM）而未处理的请求总数；从 Kaspersky Embedded Systems Security 上次启动时开始计数。 Kaspersky Embedded Systems Security 将跳过未被文件拦截驱动程序处理的对象处理请求。
用途	该计数器可用于检测并消除由于系统资源不足而发生的实时计算机保护质量可能下降的情况。
标准值/阈值	0 / 1。

推荐的读取时间间隔	1小时。
在计数器值超过阈值时的配置推荐	如果计数器值不为零，则表明 Kaspersky Embedded Systems Security 工作进程需要更多 RAM 来处理请求。 其他应用程序的活动进程可能正在使用所有可用的 RAM。

发送以便处理的请求数量

发送以便处理的请求数量

名称	发送以便处理的请求数量。
定义	等待工作进程处理的对象数量。
用途	该计数器可用于监视 Kaspersky Embedded Systems Security 工作进程的负荷以及受保护设备上的总体文件活动水平。
标准值/阈值	该计数器值可能因受保护设备上的文件活动水平而异。
推荐的读取时间间隔	1分钟
在计数器值超过阈值时的配置推荐	N/A

文件拦截调度程序流平均数量

文件拦截调度程序流平均数量

名称	文件拦截调度程序流平均数量。
定义	一个进程中的文件拦截调度程序流数量，对于当前参与实时计算机保护任务的所有进程而言，则为文件拦截调度程序流的平均数量。
用途	该计数器可用于检测并消除由于 Kaspersky Embedded Systems Security 进程满负荷工作而可能导致的实时计算机保护能力下降的情况。
标准值/阈值	随具体情况而异/40
推荐的读取时间间隔	1分钟
在计数器值超过阈值时的配置推荐	在每个工作进程中，最多可以创建 60 个文件拦截调度程序流。如果该计数器接近 60，则存在以下风险：任何工作进程都无法处理文件拦截驱动程序请求队列中的下一个请求，并且 Kaspersky Embedded Systems Security 将跳过该对象。 请增加用于完成实时计算机保护任务的 Kaspersky Embedded Systems Security 进程的数量。您可以使用“**用于实时保护的进程数**”等 Kaspersky Embedded Systems Security 设置。

文件拦截调度程序流最大数量

文件拦截调度程序流最大数量

名称	文件拦截调度程序流最大数量。
定义	一个进程中的文件拦截调度程序流数量，对于当前参与实时计算机保护任务的所有进程

	而言，则为文件拦截调度程序流的最大数量。
用途	该计数器使您能够检测并消除由于正在运行的进程中负荷分配不均而导致的性能下降情况。
标准值/阈值	随具体情况而异/40
推荐的读取时间间隔	1 分钟
在计数器值超过阈值时的配置推荐	如果该计数器的值大大超过“**文件拦截调度程序流平均数量**”计数器的值并继续增加，则表明 Kaspersky Embedded Systems Security 向正在运行的进程分配负荷时不够均匀。 重新启动 Kaspersky Embedded Systems Security。

被感染对象队列中的元素数

被感染对象队列中的元素数

名称	被感染对象队列中的元素数。
定义	当前正在等待处理（清除或删除）的被感染对象的数量。
用途	该计数器可帮您检测： • 由于文件拦截调度程序的潜在故障而导致的实时计算机保护中断。 • 由于处理器时间在不同工作进程和 Kaspersky Embedded Systems Security 之间分配不均而导致的进程过载。 • 病毒爆发。
标准值/阈值	当 Kaspersky Embedded Systems Security 处理被感染对象或可能已感染对象时，该值可能不为零，但是，当处理完成后，该值将返回到零/该值将在很长时间内保持非零。
推荐的读取时间间隔	1 分钟
在计数器值超过阈值时的配置推荐	如果计数器的值在很长时间内没有返回到零，则表明： • Kaspersky Embedded Systems Security 没有处理对象（文件拦截调度程序可能已经崩溃）。 重新启动 Kaspersky Embedded Systems Security。 • 处理对象的处理器时间可能不足。 确保 Kaspersky Embedded Systems Security 获得额外的处理器时间（例如，通过降低受保护设备上其他应用程序的负荷）。 • 发生病毒爆发。 如果在“实时文件保护”任务中发现大量被感染对象或可能已感染对象，则也表明发生了病毒爆发。可以在任务统计或任务日志中查看有关检测到的对象的数量的信息。

每秒钟处理的对象个数

每秒钟处理的对象个数

名称	每秒钟处理的对象个数。

定义	处理的对象数除以处理这些对象所花费的时间（在相等时间间隔内计算）。
用途	该计数器反映了对象处理的速度；可以使用它来检测和消除由于分配给 Kaspersky Embedded Systems Security 进程的处理器时间不足，或由于 Kaspersky Embedded Systems Security 操作出错而导致的受保护设备性能较差的情况。
标准值/阈值	随具体情况而异/无。
推荐的读取时间间隔	1 分钟。
在计数器值超过阈值时的配置推荐	该计数器的值取决于 Kaspersky Embedded Systems Security 设置中设定的值及受保护设备上其他应用程序进程的负荷。 观察较长时间内的平均计数器值。如果一般计数器值下降，则可能发生以下情况之一： • Kaspersky Embedded Systems Security 进程没有足够的处理器时间来处理对象。确保 Kaspersky Embedded Systems Security 获得额外的处理器时间（例如，通过降低受保护设备上其他应用程序的负荷）。 • Kaspersky Embedded Systems Security 出错（多个流空闲）。重新启动 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security SNMP 计数器和陷阱

本节包含有关 Kaspersky Embedded Systems Security 计数器和陷阱的信息。

关于 Kaspersky Embedded Systems Security SNMP 计数器和陷阱

如果要安装的一组反病毒组件中包括 SNMP 计数器和陷阱，则可以使用简单网络管理协议 (SNMP) 查看 Kaspersky Embedded Systems Security 计数器和陷阱。

若要从管理员工作站查看 Kaspersky Embedded Systems Security 计数器和陷阱，请在受保护设备上启动 SNMP 服务，并在管理员工作站上启动 SNMP 和 SNMP 陷阱服务。

Kaspersky Embedded Systems Security SNMP 计数器

本节包含介绍 Kaspersky Embedded Systems Security SNMP 计数器的设置的表。

性能计数器

性能计数器

计数器	定义
currentRequestsAmount	发送以便处理的请求数量
currentInfectedQueueLength	被感染对象队列中的元素数
currentObjectProcessingRate	每秒钟处理的对象个数

currentWorkProcessesNumber	Kaspersky Embedded Systems Security 所使用的工作进程的当前数量

隔离计数器

隔离计数器

计数器	定义
totalObjects	当前位于隔离中的对象数量
totalSuspiciousObjects	当前位于隔离中的可能已感染对象数量
currentStorageSize	隔离区中的数据总量 (MB)

备份计数器

备份计数器

计数器	定义
currentBackupStorageSize	备份区中的数据总量 (MB)

常规计数器

常规计数器

计数器	定义
lastCriticalAreasScanAge	自上次对受保护设备关键区域执行全盘扫描以来的期限（自完成上一次"关键区域扫描"任务以来经过的时间，单位为秒）。
licenseExpirationDate	授权许可过期日期。如果添加了活动密钥和附加密钥，则将显示与附加密钥关联的授权许可的过期日期。
currentApplicationUptime	Kaspersky Embedded Systems Security 自上次启动以来已经运行的时间（单位为百分之一秒）。

更新计数器

更新计数器

计数器	定义
avBasesAge	数据库的"年龄"（自最新安装的数据库更新的创建日期以来所经历的时间，单位为百分之一秒）。

实时文件保护计数器

实时文件保护计数器

计数器	定义

totalObjectsProcessed	自运行上一次“实时文件保护”任务以来扫描的对象总数
totalInfectedObjectsFound	自运行上一次“实时文件保护”任务以来检测到的受感染和其他对象总数
totalSuspiciousObjectsFound	自运行上一次“实时文件保护”任务以来检测到的可能已感染对象总数
totalVirusesFound	自上一次运行“实时文件保护”任务以来检测到的对象总数
totalObjectsQuarantined	Kaspersky Embedded Systems Security 放入隔离的已感染、可能已感染和其他对象的总数；自上一次启动“实时文件保护”任务时开始计算
totalObjectsNotQuarantined	Kaspersky Embedded Systems Security 尝试隔离但未成功隔离的已感染或可能已感染对象的总数；自上一次启动“实时文件保护”任务时开始计算
totalObjectsDisinfected	Kaspersky Embedded Systems Security 清除的已感染对象总数；自上一次启动“实时文件保护”任务时开始计算
totalObjectsNotDisinfected	Kaspersky Embedded Systems Security 尝试清除但未成功清除的已感染对象总数；自上一次启动“实时文件保护”任务时开始计算
totalObjectsDeleted	Kaspersky Embedded Systems Security 删除的已感染、可能已感染和其他对象的总数；自上一次启动“实时文件保护”任务时开始计算
totalObjectsNotDeleted	Kaspersky Embedded Systems Security 尝试删除但未成功删除的已感染、可能已感染和其他对象的总数；自上一次启动“实时文件保护”任务时开始计算
totalObjectsBackedUp	Kaspersky Embedded Systems Security 放入备份中的已感染和其他对象的总数；自上一次启动“实时文件保护”任务时开始计算
totalObjectsNotBackedUp	Kaspersky Embedded Systems Security 尝试放入备份中但未成功的已感染和其他对象的总数；自上一次启动“实时文件保护”任务时开始计算

Kaspersky Embedded Systems Security SNMP 陷阱及其选项

下面汇总了 Kaspersky Embedded Systems Security 中的 SNMP 陷阱选项：

- eventThreatDetected：检测到一个对象。

  陷阱具有以下选项：

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds：已超过最大备份容量。备份区中的数据总量超过“**最大备份容量(MB)**”所指定的值。Kaspersky Embedded Systems Security 继续备份受感染的对象。

陷阱具有以下选项：

- eventDateAndTime
- eventSeverity
- eventSource

- eventThresholdBackupStorageSizeExceeds：已达到备份可用空间阈值。备份区中的可用空间容量小于或等于“**可用空间阈值(MB)**”指定的值。Kaspersky Embedded Systems Security 继续备份受感染的对象。

  陷阱具有以下选项：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds：已超过最大隔离容量。隔离区中数据的总大小已超过“**隔离区最大容量(MB)**”所指定的值。Kaspersky Embedded Systems Security 继续隔离可能已感染对象。

  陷阱具有以下选项：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds：已达到隔离可用空间阈值。“**可用空间阈值(MB)**”所分配的隔离区可用空间容量等于或小于指定值。Kaspersky Embedded Systems Security 继续备份受感染的对象。

  陷阱具有以下选项：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined：隔离错误。

  陷阱具有以下选项：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped：在备份区中保存对象副本时出错。

  陷阱具有以下选项：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError：隔离区内部错误。

  陷阱具有以下选项：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError：备份错误。

  陷阱具有以下选项：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated：反病毒数据库已过期。自上次运行数据库更新任务（本地任务、组任务或受保护设备集任务）以来的天数。

  陷阱具有以下选项：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated：反病毒数据库严重过期。自上次运行数据库更新任务（本地任务、组任务或受保护设备集任务）以来的天数。

  陷阱具有以下选项：

- eventSeverity
- eventDateAndTime
- eventSource
- days

- eventApplicationStarted：Kaspersky Embedded Systems Security 正在运行。
  陷阱具有以下选项：
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown：Kaspersky Embedded Systems Security 已停止。
  陷阱具有以下选项：
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime：很长时间未扫描关键区域。自上次"关键区域扫描"任务完成以来的天数。
  陷阱具有以下选项：
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired：授权许可已过期。
  陷阱具有以下选项：
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon：授权许可即将过期。以距授权许可到期日之前的天数进行计算。
  陷阱具有以下选项：
  - eventSeverity
  - eventDateAndTime

- eventSource
- days

- eventTaskInternalError：任务完成错误。
  陷阱具有以下选项：
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName
- eventUpdateError：运行更新任务时出错。
  陷阱具有以下选项：
  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

Kaspersky Embedded Systems Security SNMP 陷阱选项说明和可能值

下面给出了陷阱选项及其可能值的说明：

- eventDateAndTime：事件日期和时间。
- eventSeverity：重要性级别。
  该选项可以采用以下值：
  - critical (1) - 关键
  - warning (2) - 警告
  - info (3) - 信息
- userName：用户名（例如，尝试访问受感染文件的用户的名称）。
- computerName：受保护设备名称（例如，用户尝试从中访问受感染文件的受保护设备的名称）。
- eventSource：生成了事件的功能组件。
  该选项可以采用以下值：

- unknown (0) - 功能组件未知
- quarantine (1) - 隔离
- backup (2) - 备份
- reporting (3) - 任务日志
- updates (4) - 更新
- realTimeProtection (5) - 实时文件保护
- onDemandScanning (6) - 按需扫描
- product (7) – 与 Kaspersky Embedded Systems Security 整体操作而不是单个组件操作相关的事件
- systemAudit (8) - 系统审核日志

- eventReason：事件触发：什么触发了事件。
  该选项可以采用以下值：
  - reasonUnknown (0) - 原因未知。
  - reasonInvalidSettings (1) - 仅对备份和隔离事件而言，如果隔离或备份不可用（访问权限不足，或隔离设置中指定的文件夹无效 - 例如，指定了网络路径），则显示该值。在此情况下，Kaspersky Embedded Systems Security 将使用默认备份或隔离文件夹。
- objectName：对象名称（例如，在其中检测到病毒的文件的名称）。
- threatName：根据病毒百科全书分类确定的对象名称。该名称包含在 Kaspersky Embedded Systems Security 检测对象时返回的全名中。您可以在任务日志中查看检测到的对象的全名。
- detectType：检测到的对象的类型。
  该选项可以采用以下值：
  - undefined (0) - 未定义
  - virware - 传统病毒和网络蠕虫
  - trojware - 木马
  - malware - 其他恶意应用程序
  - adware - 广告软件
  - pornware - 色情软件
  - riskware - 可能被入侵者用以破坏用户设备或个人数据的合法应用程序
- detectCertainty：威胁检测的确定性级别。
  该选项可以采用以下值：
  - Suspicion（疑似感染）- Kaspersky Embedded Systems Security 检测到对象代码的一部分与已知恶意代码部分存在部分匹配。

- Sure（已感染）- Kaspersky Embedded Systems Security 检测到对象代码的一部分与已知恶意代码部分完全匹配。

- days：天数（例如，授权许可到期日之前的天数）。
- errorCode：错误代码。
- knowledgeBaseId：知识库文章的地址（例如，解释特定错误的文章的地址）。
- taskName：任务名称。
- updaterErrorEventReason：更新错误的原因。
  该选项可以采用以下值：
  - reasonUnknown(0) - 原因未知。
  - reasonAccessDenied – 访问被拒绝。
  - reasonUrlsExhausted – 更新源列表已耗尽。
  - reasonInvalidConfig – 配置文件无效。
  - reasonInvalidSignature – 特征码无效。
  - reasonCantCreateFolder – 无法创建文件夹。
  - reasonFileOperError – 文件错误。
  - reasonDataCorrupted – 对象已损坏。
  - reasonConnectionReset – 连接重置。
  - reasonTimeOut – 已超过连接超时值。
  - reasonProxyAuthError – 代理验证错误。
  - reasonServerAuthError – 服务器验证错误。
  - reasonHostNotFound – 未找到设备。
  - reasonServerBusy – 服务器不可用。
  - reasonConnectionError – 连接错误。
  - reasonModuleNotFound - 对象未找到。
  - reasonBlstCheckFailed(16) – 检查密钥拒绝列表时出错。可能在更新时正在发布数据库更新；请在几分钟后重复更新。
- storageObjectNotAddedEventReason：未备份或未隔离对象的原因。
  该选项可以采用以下值：
  - reasonUnknown (0) - 原因未知。
  - reasonStorageInternalError – 数据库错误；必须还原 Kaspersky Embedded Systems Security。

- reasonStorageReadOnly – 数据库为只读；必须还原 Kaspersky Embedded Systems Security。
- reasonStorageIOError – 输入输出错误：a) Kaspersky Embedded Systems Security 已损坏，必须还原 Kaspersky Embedded Systems Security；b) 含有 Kaspersky Embedded Systems Security 文件的磁盘已损坏。
- reasonStorageCorrupted – 存储已损坏；必须还原 Kaspersky Embedded Systems Security。
- reasonStorageFull – 数据库已满；需要可用磁盘空间。
- reasonStorageOpenError – 无法打开数据库文件；必须还原 Kaspersky Embedded Systems Security。
- reasonStorageOSFeatureError - 某些操作系统功能与 Kaspersky Embedded Systems Security 要求不符。
- reasonObjectNotFound - 要放到隔离区中的对象在磁盘上不存在。
- reasonObjectAccessError – 使用备份 API 的权限不足：用于执行操作的账户不具备备份操作员权限。
- reasonDiskOutOfSpace – 磁盘空间不足。

与 WMI 集成

Kaspersky Embedded Systems Security 支持与 Windows Management Instrumentation (WMI) 集成：您可以使用支持 WMI 的客户端系统通过基于 Web 的企业管理 (WBEM) 标准接收数据，以接收有关 Kaspersky Embedded Systems Security 及其组件的状态的信息。

Kaspersky Embedded Systems Security 安装后，会在系统中注册专有模块以在受保护设备上创建 Kaspersky Embedded Systems Security 命名空间。通过 Kaspersky Embedded Systems Security 命名空间可以使用 Kaspersky Embedded Systems Security 类和实例及其属性。

某些实例属性的值取决于任务类型。

*非周期性任务*是没有时间限制的应用程序任务，可以持续运行或停止。此类任务没有执行进度。当任务作为单个事件运行（例如，任一"实时计算机保护"任务检测受感染对象）时，将持续记录任务结果。此类型的任务通过 Kaspersky Security Center 策略进行管理。

*周期性任务*是有时间限制且以百分比形式显示执行进度的应用程序任务。任务结果在任务完成后生成，并表示为单个项目或更改的应用程序状态（例如，完成的应用程序数据库更新、为规则生成任务生成的配置文件）。在单个受保护设备上可以同时运行多个同一类型的周期性任务（例如，三个具有不同扫描范围的按需扫描任务）。可以通过 Kaspersky Security Center 将周期性任务作为组任务进行管理。

如果在公司网络中使用工具生成 WMI 命名空间查询并从 WMI 命名空间接收动态数据，您将能够接收有关当前应用程序状态的信息（请参见下表）。

有关应用程序状态的信息

实例属性	描述	值
ProductName	已安装的应用程序的名称。	不带版本号的应用程序全名。
ProductVersion	已安装的应用程序的完整版本。	应用程序完整版本号，包括内部版本号。
InstalledPatches	已安装的补丁的显示名称集。	为应用程序安装的关键修复程序列表。
IsLicenseInstalled	应用程序激活状态。	用于激活应用程序的密钥的状态。

		可能的值： • False - 授权许可密钥尚未添加到应用程序。 • True - 授权许可密钥已添加到应用程序。
LicenseDaysLeft	显示当前授权许可到期前剩余的天数。	当前授权许可到期前剩余的天数。 可能的非正值： • 0 - 授权许可已过期。 • -1 - 无法获取当前密钥的信息，或者指定密钥无法用于激活应用程序（例如，根据密钥拒绝列表将其阻止）。
AVBasesDatetime	当前反病毒数据库版本的时间戳。	当前使用中的反病毒数据库的创建日期和时间。 如果已安装的应用程序不使用反病毒数据库，则该字段的值为“未安装”。
IsExploitPreventionEnabled	“漏洞利用防御”组件的状态。	“漏洞利用防御”组件的状态。 可能的值： • True -“漏洞利用防御”组件已启用并正在提供保护。 • False -“漏洞利用防御”组件未提供保护。例如：已禁用、未安装、已违反授权许可协议。
ProtectionTasksRunning	当前正在运行的一系列保护任务。	当前正在运行的保护、控制和监控任务的列表。此字段应表示所有正在运行的非周期性任务。 如果没有非周期性任务正在运行，该字段的值为“无”。
IsAppControlRunning	“应用程序启动控制”任务的状态。	“应用程序启动控制”任务的状态。 • True -“应用程序启动控制”任务当前正在运行。 • False -“应用程序启动控制”任务当前未运行或“应用程序启动控制”组件未安装。
AppControlMode	“应用程序启动控制”任务模式。	描述“应用程序启动控制”组件的当前状态，以及相应任务的选定模式。 可能的值： • 活动 - 任务设置中选择了“**活动**”模式。 • 仅统计 - 任务设置中选择了“**仅统计**”模式。 • 未安装 -“应用程序启动控制”组件未安装。
AppControlRulesNumber	应用程序启动控制规则总数。	“应用程序启动控制”任务设置中当前指定的规则数量。

AppControlLastBlocking	“应用程序启动控制”任务上次在任一模式下阻止应用程序启动的时间戳。	“应用程序启动控制”组件上次阻止应用程序启动时的日期和时间。该字段包括所有已阻止的应用程序，不管任务模式为何。 如果在处理 WMI 查询时未注册已阻止的应用程序启动的实例，该字段将被分配值“无”。
PeriodicTasksRunning	当前正在运行的一系列周期性任务。	当前正在运行的按需扫描、更新和清单编制任务的列表。此字段应包括所有正在运行的周期性任务。 如果当前没有周期性任务正在运行，则该字段的值为“无”。
ConnectionState	WMI 提供程序组件与 Kaspersky Security 服务 (KAVFS) 之间的连接的状态。	有关 WMI 提供程序组件与 Kaspersky Security 服务之间的连接状态的信息。 可能的值： • 成功 - 连接已成功建立：WMI 客户端可以接收应用程序状态。 • 失败。错误代码：<代码> - 由于出现指定代码的错误，无法建立连接。

此数据表示实例属性 KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security，其中：

- KasperskySecurity_ProductInfo 是 Kaspersky Embedded Systems Security 类的名称
- .ProductName=Kaspersky Embedded Systems Security 是 Kaspersky Embedded Systems Security 关键属性

该实例在 ROOT\Kaspersky\Security 命名空间中创建。

从命令行使用 Kaspersky Embedded Systems Security

本节描述从命令行使用 Kaspersky Embedded Systems Security。

命令

您可以使用命令行实用工具组件从受保护设备的命令行执行基本的 Kaspersky Embedded Systems Security 管理命令，该组件包含在 Kaspersky Embedded Systems Security 软件组件组中。

使用命令行只能管理那些可以根据 Kaspersky Embedded Systems Security 分配给您的权限来访问的功能。

某些 Kaspersky Embedded Systems Security 命令在以下模式下执行：

- 同步模式：只有命令完成后，控制权才会返回到控制台。
- 异步模式：命令启动后，控制权立即返回到控制台。

要在同步模式下中断被执行的命令，

按 **Ctrl+C** 键盘快捷键。

输入 Kaspersky Embedded Systems Security 命令时，应遵循以下规则：

- 使用大小写字符输入修饰符和命令。
- 使用空格分隔修饰符。
- 如果指定为一个值的文件/文件夹路径包含空格，请使用引号将路径括起来，例如“`C:\TEST\test cpp.exe`”。
- 如有必要，可以在文件名或路径中使用通配符，例如：“`C:\Temp\Temp*\`”、“`C:\Temp\Temp???.doc`”、“`C:\Temp\Temp*.doc`”。

您可以使用命令行执行 Kaspersky Embedded Systems Security 的管理所需的每个操作（请参见下表）。

Kaspersky Embedded Systems Security 命令

命令	描述
KAVSHELL APPCONTROL	根据选定导入规则更新规则列表。
KAVSHELL APPCONTROL /CONFIG	设置“应用程序启动控制”任务的运行模式
KAVSHELL APPCONTROL /GENERATE	启动“应用程序启动控制规则生成器”任务。
KAVSHELL VACUUM	对 Kaspersky Embedded Systems Security 日志文件进行碎片整理。
KAVSHELL PASSWORD	管理密码保护设置。
KAVSHELL HELP	显示 Kaspersky Embedded Systems Security 命令帮助。
KAVSHELL START	启动 Kaspersky Security 服务。
KAVSHELL STOP	停止 Kaspersky Security 服务。

KAVSHELL SCAN	创建并启动临时按需扫描任务，其扫描范围和安全性设置由命令行选项指定。
KAVSHELL SCANCRITICAL	启动"关键区域扫描"本地系统任务。
KAVSHELL TASK	异步启动、暂停/恢复、停止指定任务，返回当前任务状态/统计。
KAVSHELL RTP	启动或停止所有实时计算机保护任务。
KAVSHELL UPDATE	以命令行选项指定的设置启动数据库更新任务。
KAVSHELL ROLLBACK	将数据库回滚至先前版本。
KAVSHELL LICENSE	添加或删除密钥。显示有关已添加的密钥的信息。
KAVSHELL TRACE	启用或禁用跟踪。管理跟踪设置。
KAVSHELL DUMP	启用或禁用当 Kaspersky Embedded Systems Security 进程异常终止时创建 dump 文件。
KAVSHELL IMPORT	从配置文件中导入常规 Kaspersky Embedded Systems Security 设置、功能和任务。
KAVSHELL EXPORT	将所有 Kaspersky Embedded Systems Security 设置和现有任务导出至配置文件。
KAVSHELL DEVCONTROL	根据选定的方法添加到已生成的设备控制规则列表中。

显示 Kaspersky Embedded Systems Security 命令帮助：KAVSHELL HELP

要查看所有 Kaspersky Embedded Systems Security 命令的列表，请运行以下命令之一：

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

要查看命令及其语法的说明，请运行以下命令之一：

```
KAVSHELL HELP <命令>

KAVSHELL <命令> /?
```

KAVSHELL HELP 示例

若要查看有关 KAVSHELL SCAN 命令的详细信息，请执行以下命令：

```
KAVSHELL HELP SCAN
```

启动和停止 Kaspersky Security 服务：KAVSHELL START，KAVSHELL STOP

要运行 Kaspersky Security 服务，请执行以下命令：

```
KAVSHELL START
```

默认情况下，Kaspersky Security 服务启动时，“实时文件保护”和“在操作系统启动时扫描”以及计划在“应用程序启动时”启动的其他任务将启动。

要停止 Kaspersky Security 服务，请执行以下命令：

```
KAVSHELL STOP
```

执行此命令可能需要密码。要输入当前密码，请使用 `[/pwd:<密码>]`。

扫描选定区域：KAVSHELL SCAN

要启动扫描受保护设备特定区域的任务，请使用 `KAVSHELL SCAN`。命令行选项指定选定节点的扫描范围和安全性设置。

使用 `KAVSHELL SCAN` 命令启动的按需扫描任务是一个临时任务。它仅在执行时才显示在应用程序控制台中（您无法在应用程序控制台中查看其任务设置）。但是，将生成任务性能日志，并显示在应用程序控制台中的“任务日志”节点下。

为特定区域的扫描任务指定路径时，可以使用环境变量。如果使用用户环境变量，请以相应用户身份执行 `KAVSHELL SCAN` 命令。

`KAVSHELL SCAN` 命令在同步模式下执行。

要从命令行启动现有按需扫描任务，请使用 KAVSHELL TASK 命令。

KAVSHELL SCAN 命令语法

```
KAVSHELL SCAN <扫描范围> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<带有扫描范围列表的文件的路径>] [/F<A|C|E>] [/NEWONLY] [/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"掩码">] [/ES:<大小>] [/ET:<秒数>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<天>] [NORECALL]>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL] [/NOCHECKMSSIGN][/W:<任务日志文件的路径>] [/ANSI] [/ALIAS:<任务别名>]
```

KAVSHELL SCAN 命令有必需和可选参数/选项（请参见下表）。

KAVSHELL SCAN 命令示例

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe "\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

KAVSHELL SCAN 命令行参数/选项

参数/选项	描述
扫描范围。必需参数。	
<文件>	指定扫描范围 - 文件、文件夹、网络路径和预定义区域的列表。 指定通用命名约定 (UNC) 格式的网络路径。 在下面的示例中，指定 Folder4 文件夹时没有路径，表示该文件夹位于运行 KAVSHELL 命令的文件夹中： KAVSHELL SCAN Folder4 如果要扫描的对象的名称包含空格，则必须将其扩在引号内。 如果指定文件夹，Kaspersky Embedded Systems Security 还将扫描其所有子文件夹。 * 或 ? 号可用于扫描一组文件。
<文件夹>	
<网络路径>	
/MEMORY	扫描 RAM 中的对象
/SHARED	扫描受保护设备上的共享文件夹
/STARTUP	扫描自动运行对象
/REMDRIVES	扫描可移动驱动器
/FIXDRIVES	扫描硬盘驱动器
/MYCOMP	扫描受保护设备的所有区域
/L:<包含扫描范围列表的文件的路径>	包含扫描范围列表的文件的完整路径。 使用换行符分隔文件中的扫描范围。您可以指定预定义的扫描区域，如以下包含扫描范围列表的文件内容示例： C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
扫描对象（文件类型）。如果您指定此选项，Kaspersky Embedded Systems Security 将按对象的格式扫描对象。	
/FA	扫描所有对象
/FC	按格式扫描对象（默认）。Kaspersky Embedded Systems Security 只扫描其格式包含在可感染对象格式列表中的对象。
/FE	按扩展名扫描对象。Kaspersky Embedded Systems Security 只扫描其扩展名包含在被感染的对象扩展名列表中的对象。
/NEWONLY	仅扫描新文件和已修改的文件。 如果不指定此选项，Kaspersky Embedded Systems Security 将扫描所有对象。
对受感染对象和其他对象执行的操作。如果不为该修饰符指定值，Kaspersky Embedded Systems Security 将执行“**跳过**”操作。	
DISINFECT	清除，如果无法清除则跳过 最新版本的 Kaspersky Embedded Systems Security 中保留了 DISINFECT 和 DELETE 选项，以确保与以前版本的兼容性。可以使用这些选项代替 /AI 和 /AS 选项。在这种情况下，Kaspersky Embedded Systems Security 不会处理疑似感染对象。

DISINFDEL	清除，如果无法清除则删除
DELETE	删除 最新版本的 Kaspersky Embedded Systems Security 中保存了 DISINFECT 和 DELETE 选项，以确保与以前版本的兼容性。可以使用这些选项代替 /AI 和 /AS 选项。在这种情况下，Kaspersky Embedded Systems Security 不会处理疑似感染对象。
REPORT	发送报告（默认）
AUTO	执行推荐的操作
/AS：**对疑似感染对象执行的操作**。如果不指定此选项，Kaspersky Embedded Systems Security 将执行**"跳过"**操作。	
QUARANTINE	隔离
DELETE	删除
REPORT	发送报告（默认）
AUTO	执行推荐的操作
排除	
/E:ABMSPO	排除以下类型的复合对象： A - 压缩文件（仅扫描 SFX 压缩文件） B - 电子邮件数据库 M - 普通邮件 S - 压缩文件和 SFX 压缩文件 P - 打包的对象 O - 嵌入式 OLE 对象
/EM:<"掩码">	按掩码排除文件 您可以指定多个掩码，例如：`EM:"*.txt; *.png; C\Videos\*.avi"`。
/ET:<秒数>	如果花费时间超过 <秒数> 所指定的秒数，则停止处理对象。 默认情况下，没有时间限制。
/ES:<大小>	不扫描其大小超过 <大小> 值所指定的大小（单位为 MB）的复合对象。 默认情况下，Kaspersky Embedded Systems Security 扫描所有大小的对象。
/TZOFF	禁用"受信任区域"排除
高级设置（选项）	
/NOICHECKER	禁止使用 iChecker（默认为已启用）
/NOISWIFT	禁止使用 iSwift（默认为已启用）
/ANALYZERLEVEL:<启发式分析级别>	启用启发式分析，配置分析级别。 以下启发式分析级别可用： 1 – 轻度 2 – 中度 3 - 深度 如果省略此选项，Kaspersky Embedded Systems Security 将不会使用启发式分析。
/ALIAS:<任务别名>	为按需扫描任务分配一个临时名称，允许您在其运行时对其进行引用，例如，使用 TASK 命令查看其统计信息。在 Kaspersky Embedded Systems Security 的所有组件的任务别名中，每一个任务别名都必须是唯一的。

	如果不指定此选项，则分配 scan_<kavshell_pid> 格式的临时名称，例如 scan_1234。在应用程序控制台中，任务被分配名称“扫描对象 <日期和时间>”，例如，扫描对象 8/16/2007 5:13:14 PM。
任务日志设置（报告设置）	
/W:<任务日志文件的路径>	如果指定了此参数，Kaspersky Embedded Systems Security 将用该参数值指定的名称保存任务日志文件。 日志文件包含任务执行统计、任务的开始和完成（停止）时间以及有关该任务期间发生的事件的信息。 该日志用于在事件查看器中注册由任务日志设置和 Kaspersky Embedded Systems Security 事件日志设置所定义的事件。 您可以指定日志文件的绝对路径或相对路径。如果仅指定文件名而不指定路径，则将在当前文件夹中创建日志文件。 在用相同的日志设置重新启动该命令后，将覆盖现有的日志文件。 在任务运行过程中，可以查看日志文件。 该日志出现在应用程序控制台的“任务日志”节点中。 如果 Kaspersky Embedded Systems Security 无法创建日志文件，它将显示一条错误消息，但仍将执行命令。
/ANSI	此选项使用 ANSI 编码将事件记录到任务日志中。 如果未指定 W 参数，则不会应用 ANSI 选项。 如果未指定 ANSI 选项，将使用 UNICODE 生成任务日志。

启动“关键区域扫描”任务：KAVSHELL SCANCRITICAL

使用 `KAVSHELL SCANCRITICAL` 命令可使用在应用程序控制台中定义的设置启动“关键区域扫描”任务。

KAVSHELL SCANCRITICAL 命令语法

```
KAVSHELL SCANCRITICAL [/W:<任务日志文件的路径>]
```

KAVSHELL SCANCRITICAL 命令示例

要运行“关键区域扫描”任务并将名为 scancritical.log 的任务日志保存到当前文件夹中，请执行以下命令：

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

您可以使用 /W 参数配置任务日志的位置（请参见下表）。

KAVSHELL SCANCRITICAL 命令的 /W 参数的语法

参数/选项	描述
/W:<任务日志文件的路径>	如果指定了此参数，Kaspersky Embedded Systems Security 将用该参数值指定的名称保存任务日志文件。 日志文件包含任务执行统计、任务的开始和完成（停止）时间以及有关该任务期间发生的事件的信息。 该日志用于在事件查看器中注册由任务日志设置和 Kaspersky Embedded Systems Security 事件日志设置所定义的事件。

	您可以指定日志文件的绝对路径或相对路径。如果仅指定文件名而不指定路径，则将在当前文件夹中创建日志文件。 在用相同的日志设置重新启动该命令后，将覆盖现有的日志文件。 在任务运行过程中，可以查看日志文件。 该日志出现在应用程序控制台的“**任务日志**”节点中。 如果 Kaspersky Embedded Systems Security 无法创建日志文件，它将显示一条错误消息，但仍将执行命令。

异步管理任务：KAVSHELL TASK

可以使用 `KAVSHELL TASK` 命令管理指定任务：运行、暂停、恢复和停止任务和查看当前任务状态和统计。该命令在异步模式下执行。

执行此命令可能需要密码。要输入当前密码，请使用 `[/pwd:<密码>]`。

KAVSHELL TASK 命令语法

```
KAVSHELL TASK [<任务别名> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

KAVSHELL TASK 命令示例

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

`KAVSHELL TASK` 命令可以不带参数/选项运行，或带一个或多个参数/选项运行（请参见下表）。

KAVSHELL TASK 命令行参数/选项

参数/选项	描述
无参数	返回所有现有 Kaspersky Embedded Systems Security 任务的列表。该列表包括以下字段：任务别名、任务类别（系统或自定义）和当前任务状态。
<任务别名>	在 SCAN TASK 命令中，不使用任务名称，而是使用它的任务别名，即 Kaspersky Embedded Systems Security 分配给任务的附加缩写名称。要查看 Kaspersky Embedded Systems Security 任务别名，请输入不带任何参数的命令 KAVSHELL TASK。
/START	在异步模式下启动指定任务。
/STOP	停止指定任务。
/PAUSE	暂停指定任务。
/RESUME	在异步模式下恢复指定任务。

/STATE	返回当前任务状态（例如，*正在运行*、*已完成*、*已暂停*、*已停止*、*失败*、*正在启动*、*正在恢复*）。
/STATISTICS	检索任务统计 - 有关从任务启动开始所处理的对象数量的信息

请注意，并非所有 Kaspersky Embedded Systems Security 任务都完全支持 /PAUSE、/RESUME 和 /STATE 键。

KAVSHELL TASK 命令的返回代码。

删除 PPL 属性：KAVSHELL CONFIG

KAVSHELL CONFIG 命令允许您使用在应用程序安装期间安装的 ELAM 驱动程序删除 Kaspersky Security 服务的 PPL（轻度受保护进程）属性。

KAVSHELL CONFIG 命令语法

```
KAVSHELL CONFIG /PPL:<OFF>
```

KAVSHELL CONFIG 命令行参数/选项

参数/选项	描述
/PPL:OFF	删除 Kaspersky Security 服务的 PPL 属性。

启动和停止实时计算机保护任务：KAVSHELL RTP

您可以使用 KAVSHELL RTP 命令启动或停止所有实时计算机保护任务。

执行此命令可能需要密码。要输入当前密码，请使用 [/pwd:<密码>]。

KAVSHELL RTP 命令语法

```
KAVSHELL RTP {/START | /STOP}
```

KAVSHELL RTP 命令示例

要启动所有实时计算机保护任务，请执行以下命令：

```
KAVSHELL RTP /START
```

KAVSHELL RTP 命令必须包括两个选项中的一个（请参见下表）。

KAVSHELL RTP 命令行选项

参数/选项	描述
/START	启动所有实时计算机保护任务：“实时文件保护”和“KSN 使用”。

/STOP	停止所有实时计算机保护任务。

管理应用程序启动控制任务：KAVSHELL APPCONTROL /CONFIG

可以使用 KAVSHELL APPCONTROL /CONFIG 命令来配置模式，在该模式中"应用程序启动控制"任务将运行和监控 DLL 模块的加载。

KAVSHELL APPCONTROL /CONFIG 命令语法

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<XML 文件路径>
```

KAVSHELL APPCONTROL /CONFIG 命令示例

*要在"**活动**"模式中运行"应用程序启动控制"任务而不监控 DLL 加载并在完成时保存任务设置，请运行以下命令：*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

可以使用命令行参数来配置"应用程序启动控制"任务设置（请参见以下表格）。

KAVSHELL APPCONTROL /CONFIG 命令行参数/选项

参数/选项	描述
/mode:<applyrules|statistics>	"应用程序启动控制"任务的运行模式。 您可以选择以下模式之一： • 活动 – 应用"应用程序启动控制规则"； • 统计 – 仅生成统计。
/dll:<no|yes>	启用或禁用 DLL 加载监控。
/savetofile: <XML 文件路径>	将指定规则导出到指示的 XML 格式的文件。
/savetofile: <xml 文件全名>	将规则列表保存到文件。
/savetofile: <xml 文件全名> /sdc	将软件分发控制规则列表保存到文件。
/clearsdc	从列表中删除软件分发控制规则。

应用程序启动控制规则生成器：KAVSHELL APPCONTROL / GENERATE

可以使用 KAVSHELL APPCONTROL /GENERATE 命令生成应用程序启动控制规则列表。

执行此命令可能需要密码。要输入当前密码，请使用 [/pwd:<密码>]。

KAVSHELL APPCONTROL /GENERATE 命令语法

```
KAVSHELL APPCONTROL /GENERATE <文件夹路径> | /source:<包含文件夹列表的文件路径> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<用户或用户组>] [/export:<XML 文件路径>] [/import:<a|r|m>] [/prefix:<规则名称前缀>] [/unique]
```

KAVSHELL APPCONTROL /GENERATE 命令示例

若要为指定文件夹中的文件生成规则，请执行以命令：

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

要为指定文件夹中所有扩展名的可执行文件生成规则，并在任务完成时将生成的规则保存在指定的 XML 文件中，请执行以下命令：

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

您可以使用命令行参数/选项配置“应用程序启动控制”任务的自动规则生成设置（请参见下表）。

KAVSHELL APPCONTROL /GENERATE 命令行参数/选项

参数/选项	描述
允许规则范围	
<文件夹路径>	指定将为其自动生成允许规则的可执行文件所在文件夹的路径。
/source：<包含文件夹列表的文件路径>	指定含有文件夹列表的 TXT 文件的路径，这些文件夹包含将为其自动生成允许规则的可执行文件。
/masks：<edms>	指定将为其自动生成允许规则的可执行文件的扩展名。 可以将具有以下扩展名的文件包括在规则范围中： • e - EXE 文件 • d - DLL 文件 • m - MSI 文件 • s - 脚本
/runapp	生成允许规则时，考虑当前在受保护设备上运行的应用程序。
自动生成允许规则时的操作	
/rules：<ch|cp|h>	指定当生成“应用程序启动控制”任务的允许规则时执行的操作： • ch - 使用数字证书。如果证书缺失，则使用 SHA256 哈希。 • cp - 使用数字证书。如果证书缺失，则使用可执行文件路径。 • h - 使用 SHA256 哈希。
/strong	在自动生成“应用程序启动控制”任务的允许规则时使用数字证书的主题和指纹。如果指定 /rules: <ch|cp> 参数，则将执行该命令。

/user：<用户或用户组>	指定将应用规则的用户或用户组。应用程序将监控通过指定的用户和/或用户组运行的任何应用程序。
“应用程序启动控制规则生成器”任务完成后的操作	
/export：<XML 文件路径>	将生成的规则保存到 XML 文件。
/unique	添加有关安装了特定应用程序的受保护设备的信息，这些应用程序是生成应用程序启动控制允许规则的基础。
/prefix：<规则名称前缀>	为“应用程序启动控制”允许规则的名称指定前缀。
/import：<a|r|m>	根据选定导入规则将生成的规则导入到指定的应用程序启动控制规则列表中： • a - **添加到现有规则**（将复制具有相同设置的规则） • r - **替换现有规则**（不添加具有相同设置的规则；如果至少一个规则设置是唯一的，则会添加规则） • m - **与现有规则合并**（不添加具有相同设置的规则；如果至少一个规则设置是唯一的，则会添加规则）

填写应用程序启动控制规则列表：KAVSHELL APPCONTROL

可以使用 KAVSHELL APPCONTROL 命令根据所选导入规则将规则从 XML 文件添加到应用程序启动控制任务规则列表，以及从列表中删除所有现有规则。

执行此命令可能需要密码。要输入当前密码，请使用 [/pwd:<密码>]。

KAVSHELL APPCONTROL 命令语法

```
KAVSHELL APPCONTROL /append <XML 文件路径> | /replace <XML 文件路径> | /merge <XML 文件路径> | /clear
```

KAVSHELL APPCONTROL 命令示例

要根据“添加到现有规则”导入规则从 XML 文件向现有应用程序启动控制规则添加规则，请执行以下命令：

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

您可以使用命令行参数选择原则来将新规则从指定 XML 文件添加到定义的应用程序启动控制规则列表（请参见下表）。

KAVSHELL APPCONTROL 命令行参数/选项

参数/选项	描述
/append <XML 文件路径>	基于指定的 XML 文件更新应用程序启动控制规则列表。导入规则 - **添加到现有规则**（将复制具有相同设置的规则）。

/replace <XML 文件路径>	基于指定的 XML 文件更新应用程序启动控制规则列表。导入规则 - **替换现有规则**（不添加具有相同设置的规则；如果至少一个规则设置是唯一的，则会添加规则）。
/merge <XML 文件路径>	基于指定的 XML 文件更新应用程序启动控制规则列表。导入规则 - **与现有规则合并**（新规则不会复制现有规则）。
/clear	清除应用程序启动控制规则列表。

填写设备控制规则列表：KAVSHELL DEVCONTROL

可以使用 KAVSHELL DEVCONTROL 命令根据所选导入规则将规则从 XML 文件添加到设备控制任务规则列表，以及从列表中删除所有现有规则。

执行此命令可能需要密码。要输入当前密码，请使用 [/pwd:<密码>]。

KAVSHELL DEVCONTROL 命令语法

```
KAVSHELL DEVCONTROL /append <XML 文件路径> | /replace <XML 文件路径> | /merge <XML 文件路径> | /clear
```

KAVSHELL DEVCONTROL 命令示例

要根据"添加到现有规则"导入规则从 XML 文件向设备控制任务的现有规则添加规则，请执行以下命令：

```
KAVSHELL DEVCONTROL /append c:\rules\devctrlrules.xml
```

您可以使用命令行参数选择用于将新规则从指定 XML 文件添加到定义的设备控制规则列表的导入规则（请参见下表）。

KAVSHELL DEVCONTROL 命令行参数/选项

密钥	描述
/append <XML 文件路径>	基于指定的 XML 文件更新设备控制规则列表。导入规则 - **添加到现有规则**（将复制具有相同设置的规则）。
/replace <XML 文件路径>	基于指定的 XML 文件更新设备控制规则列表。导入规则 - **替换现有规则**（不添加具有相同参数的规则；如果至少一个规则设置是唯一的，则会添加规则）。
/merge <XML 文件路径>	基于指定的 XML 文件更新设备控制规则列表。导入规则 - **与现有规则合并**（新规则不会复制现有规则）。
/clear	清除设备控制规则列表。

启动数据库更新任务：KAVSHELL UPDATE

KAVSHELL UPDATE 命令可以用于按同步模式启动 Kaspersky Embedded Systems Security 数据库更新任务。

使用 KAVSHELL UPDATE 命令启动的数据库更新任务是临时任务。它仅在执行时显示在应用程序控制台中。但是，将生成任务日志，并显示在应用程序控制台的"**任务日志**"中。Kaspersky Security Center 策略可应用于使用 KAVSHELL UPDATE 命令创建和启动的更新任务以及在应用程序控制台中创建的更新任务。有关使用 Kaspersky Security Center 管理受保护设备上的 Kaspersky Embedded Systems Security 的信息，请参见"使用 Kaspersky Security Center 管理 Kaspersky Embedded Systems Security"部分。

在该任务中指定更新源的路径时，可以使用环境变量。如果使用用户环境变量，请以相应用户身份运行 KAVSHELL UPDATE 命令。

KAVSHELL UPDATE 命令语法

```
KAVSHELL UPDATE < 更新源路径 | /AK | /KL> [/NOUSEKL] [/PROXY:<地址>:<端口>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<用户名>] [/PROXYPWD:<密码>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/REG:<iso3166 代码>] [/W:<任务日志文件的路径>] [/ALIAS:<任务别名>]
```

KAVSHELL UPDATE 命令有必需和可选参数/选项（请参见下表）。

KAVSHELL UPDATE 命令示例

要启动自定义的数据库更新任务，请执行以下命令：

```
KAVSHELL UPDATE
```

要使用 \\server\databases 网络文件夹中的更新文件运行数据库更新任务，请运行以下命令：

```
KAVSHELL UPDATE \\server\databases
```

要从 FTP 服务器 ftp://dnl-ru1.kaspersky-labs.com/ 启动数据库更新并将所有任务事件写入到名为 c:\update_report.log 的文件中，请执行以下命令：

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

要从 Kaspersky 的更新服务器下载 Kaspersky Embedded Systems Security 数据库更新，请通过代理服务器（代理服务器地址：proxy.company.com，端口：8080）连接到更新源。要使用内置的 Microsoft Windows NTLM 身份验证及用户名"inetuser"和密码"123456"访问受保护设备，请执行以下命令：

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456
```

KAVSHELL UPDATE 命令行参数/选项

参数/选项	描述
更新源（必需参数）。指定一个或多个源。Kaspersky Embedded Systems Security 将按照更新源的列表顺序访问更新源。使用空格分隔源。	
<UNC 格式路径>	用户定义的更新源。网络更新文件夹的路径（采用 UNC 格式）。
<URL>	用户定义的更新源。更新文件夹所在的 HTTP 或 FTP 服务器地址。
<本地文件夹>	用户定义的更新源。受保护设备上的文件夹。
/AK	将 Kaspersky Security Center 管理服务器用作更新源。
/KL	将 Kaspersky 的更新服务器用作更新源。

/NOUSEKL	如果其他更新源不可用，则不使用 Kaspersky 的更新服务器（默认情况下使用）。
代理服务器设置	
/PROXY:<地址>:<端口>	代理服务器的网络名称或 IP 地址及其端口。如果未指定此参数，Kaspersky Embedded Systems Security 将自动检测局域网中使用的代理服务器设置。
/AUTHTYPE:<0-2>	该参数指定用于访问代理服务器的身份验证方法。它可以是以下值： **0** - Microsoft Windows NTLM 身份验证；Kaspersky Embedded Systems Security 将使用**本地系统 (SYSTEM)** 账户连接代理服务器 **1** - Microsoft Windows NTLM 身份验证；Kaspersky Embedded Systems Security 将使用 /PROXYUSER 和 /PROXYPWD 参数指定的用户名和密码连接代理服务器 **2** - 使用 /PROXYUSER 和 /PROXYPWD 参数指定的用户名和密码进行身份验证（基本身份验证） 如果代理服务器不需要身份验证，则无需指定此参数。
/PROXYUSER:<用户名>	将用于访问代理服务器的用户名。如果指定了 /AUTHTYPE:0，则将忽略 /PROXYUSER:<用户名> 和 /PROXYPWD:<密码> 参数。
/PROXYPWD:<密码>	将用于访问代理服务器的用户密码。如果指定了 /AUTHTYPE:0，则将忽略 /PROXYUSER:<用户名> 和 /PROXYPWD:<密码> 参数。如果指定了 /PROXYUSER 参数但省略了 /PROXYPWD 参数，密码将被视为空字符串。
/NOPROXYFORKL	不使用代理服务器设置连接到 Kaspersky 的更新服务器（默认情况下使用）。
/USEPROXYFORCUSTOM	使用代理服务器设置连接到用户定义的更新源（默认情况下不使用）。
/USEPROXYFORLOCAL	使用代理服务器设置连接到本地更新源。如果未指定，将应用“**对于本地地址不使用代理服务器**”设置。
常规 FTP 和 HTTP 服务器设置	
/NOFTPPASSIVE	如果指定了该键，Kaspersky Embedded Systems Security 将使用主动 FTP 服务器模式连接至受保护设备。如果未指定该键，Kaspersky Embedded Systems Security 将使用被动 FTP 服务器模式（如果可能的话）。
/TIMEOUT:<秒数>	FTP 或 HTTP 服务器连接超时。如果不指定此参数，Kaspersky Embedded Systems Security 将使用默认值 - 10 秒。该值必须是一个整数。
/REG:<iso3166 代码>	区域设置。在从 Kaspersky 的更新服务器接收更新时，将使用此参数。Kaspersky Embedded Systems Security 会选择最近的更新服务器以最大程度地降低受保护设备的负荷。 此参数的值应该是受保护设备所在国家/地区的 ISO 3166-1 alpha-2 代码，例如 /REG: gr 或 /REG:US。如果省略该键或指定无效的国家/地区代码，Kaspersky Embedded Systems Security 将会基于安装应用程序控制台的受保护设备上的区域设置检测受保护设备的位置。
/ALIAS:<任务别名>	通过此参数可以为任务分配临时名称，允许您在任务运行时对其进行引用。例如，可以使用 TASK 命令查看任务统计。在 Kaspersky Embedded Systems Security 的所有组件的任务别名中，每一个任务别名都必须是唯一的。 如果不指定该键，则会使用 update_<kavshell_pid> 格式的临时名称，例如 update_1234。在应用程序控制台中，任务被分配名称“Update-databases <日期和时间>”，例如，Update-databases 8/16/2007 5:41:02 PM。
/W:<任务日志文件的路径>	如果指定了此参数，Kaspersky Embedded Systems Security 将用该参数值指定的名称保存任务日志文件。 日志文件包含任务执行统计、任务的开始和完成（停止）时间以及有关该任务期间发生的事件的信息。

	该日志用于在事件查看器中注册由任务日志设置和 Kaspersky Embedded Systems Security 事件日志设置所定义的事件。 您可以指定日志文件的绝对路径或相对路径。如果仅指定文件名而不指定路径，则将在当前文件夹中创建日志文件。 在用相同的日志设置重新启动该命令后，将覆盖现有的日志文件。 在任务运行过程中，可以查看日志文件。 该日志出现在应用程序控制台的“**任务日志**”节点中。 如果 Kaspersky Embedded Systems Security 无法创建日志文件，它将显示一条错误消息，但仍将执行命令。

KAVSHELL UPDATE 命令的返回代码。

回滚 Kaspersky Embedded Systems Security 数据库更新：KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 命令可用于执行“数据库更新回滚”本地系统任务（将 Kaspersky Embedded Systems Security 数据库回滚到之前安装的版本）。该命令同步执行。

命令语法：

```
KAVSHELL ROLLBACK
```

KAVSHELL ROLLBACK 命令的返回代码。

管理日志审查：KAVSHELL TASK LOG-INSPECTOR

KAVSHELL TASK LOG-INSPECTOR 命令可用于根据 Windows 事件日志的分析来监控环境完整性。

命令语法

```
KAVSHELL TASK LOG-INSPECTOR
```

命令示例

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

KAVSHELL TASK LOG-INSPECTOR 命令行选项

选项	描述
/START	在异步模式下启动指定任务。
/STOP	停止指定任务。
/STATE	返回当前任务状态（例如，*正在运行*、*已完成*、*已暂停*、*已停止*、*失败*、*正在启动*、*正在恢复*）
/STATISTICS	检索任务统计 - 有关从任务启动开始所处理的对象数量的信息。

KAVSHELL TASK LOG-INSPECTOR 命令的返回代码。

激活应用程序：KAVSHELL LICENSE

可使用 KAVSHELL LICENSE 命令管理 Kaspersky Embedded Systems Security 密钥和激活码。

执行此命令可能需要密码。要输入当前密码，请使用 [/pwd:<密码>]。

KAVSHELL LICENSE 命令语法

```
KAVSHELL LICENSE [/ADD:<密钥文件 | 激活码> [/R] | /DEL:<密钥 | 激活码编号>]
```

KAVSHELL LICENSE 命令示例

要激活应用程序，请执行以下命令：

```
KAVSHELL.EXE LICENSE / ADD: <激活码或密钥>
```

若要查看有关所添加密钥文件的信息，请执行以下命令：

```
KAVSHELL LICENSE
```

若要删除所添加的编号为 0000-000000-00000001的授权许可文件，请执行以下命令：

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

KAVSHELL LICENSE 命令可以在带密钥或不带密钥的情况下运行（请参见下表）。

KAVSHELL LICENSE 命令行参数/选项

参数	描述
不带键	该命令返回有关所添加授权许可文件的以下信息： • 密钥。 • 授权许可类型（商业）。 • 与密钥文件相关联的授权许可的有效期限。 • 授权许可文件状态（活动或备用）。如果状态为 *，则密钥已作为附加密钥添加。
/ADD:<密钥文件名称或激活码>	通过指定的文件或激活码添加密钥。 在指定密钥文件路径时，可以使用系统环境变量；不允许使用用户环境变量。
/R	/R 激活码或密钥是 /ADD 激活码或密钥的附加项，表示所添加的激活码或密钥是附加激活码或密钥文件。
/DEL:<密钥或激活码>	删除具有指定编号或激活码的密钥。

KAVSHELL LICENSE 命令的返回代码。

启用、配置和禁用跟踪日志：KAVSHELL TRACE

KAVSHELL TRACE 命令可用于为所有 Kaspersky Embedded Systems Security 子系统启用和禁用跟踪日志，以及设置日志详细级别。

Kaspersky Embedded Systems Security 会以未加密的形式将信息写入到跟踪文件和 Dump 文件。

KAVSHELL TRACE 命令语法

KAVSHELL TRACE </ON /F:<跟踪日志文件文件夹的路径> [/S:<最大日志大小（单位为 MB）>] [/LVL:debug|info|warning|error|critical] [/r:<最大轮换跟踪文件数>] | /OFF>

如果启用了跟踪日志并且您希望更改其设置，请输入 KAVSHELL TRACE 命令并带 /ON 选项，同时使用 /S 和 /LVL 参数指定跟踪日志设置（请参见下表）。

KAVSHELL TRACE 命令键

密钥	描述
/ON	启用跟踪日志。
/F:<包含跟踪日志文件的文件夹>	该参数指定将保存跟踪日志文件的文件夹的完整路径（必需）。 如果指定了不存在的文件夹的路径，则不会创建跟踪日志。不能指定其他受保护设备的网络驱动器上的文件夹路径。 如果该参数指定的路径包含空格，则需要用引号将路径括起来，例如 /F:"C:\Trace Folder"。 在指定跟踪日志文件路径时，可以使用系统环境变量；不允许使用用户环境变量。
/S：<最大日志文件大小（单位为 MB）>	该键设置单个跟踪日志文件的最大大小。一旦日志文件大小达到最大值，Kaspersky Embedded Systems Security 将开始将信息记录到新文件中；上一个日志文件将得到保存。 如果未指定该参数的值，则一个日志文件的最大大小将为 50 MB。
/LVL:debug|info|warning|error|critical	该参数设置日志详细级别，从所有事件都记录到日志中的最大级别（“**所有调试信息**”）到仅记录严重事件的最小级别（“**严重事件**”）。 如果未指定该参数，“**所有调试信息**”详细级别中包括的所有事件都会记录到跟踪日志中。
/r:<最大轮换跟踪文件数>	此参数会启用跟踪文件轮换。如果启用了跟踪文件轮换并且达到了<最大轮换跟踪文件数>，则在创建新文件之前，将删除最早的文件。 可用值：1 到 999。如果未指定该值，则不会启用跟踪文件轮换并且应用程序会返回错误。
/OFF	该选项禁用跟踪日志。

KAVSHELL TRACE 命令示例

*要启用使用"**所有调试信息**"详细级别和最大日志大小 200MB 的跟踪日志，并且将日志文件保存到文件夹 "C:\Trace Folder"，请执行以下命令：*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

*要启用使用"**重要事件**"详细级别的跟踪日志，并且将日志文件保存到文件夹"C:\Trace Folder"，请执行以下命令：*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

*要使用"**重要事件**"详细级别启用跟踪日志，将日志文件保存到"C:\Trace Folder"文件夹，并在达到最大数量 50 个跟踪文件后启用跟踪文件轮换，请执行命令：*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning /r:50
```

要禁用跟踪日志，请执行以下命令：

```
KAVSHELL TRACE /OFF
```

KAVSHELL TRACE 命令的返回代码。

对 Kaspersky Embedded Systems Security 日志文件进行碎片整理：KAVSHELL VACUUM

可以使用 KAVSHELL VACUUM 命令对应用程序日志文件进行碎片整理。这有助于避免由于存储大量包含应用程序事件的日志文件而出现系统和应用程序错误。

执行此命令可能需要密码。要输入当前密码，请使用 [/pwd:<密码>]。

如果按需扫描和更新任务频繁运行，建议应用 KAVSHELL VACUUM 命令最优化日志文件存储。此命令使 Kaspersky Embedded Systems Security 更新存储在受保护设备上指定路径的应用程序日志文件的逻辑结构。

默认情况下，应用程序日志文件存储在"C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Reports"。如果您手动为日志存储指定了另一个路径，KAVSHELL VACUUM 命令将对 Kaspersky Embedded Systems Security 日志设置中指定的文件夹中的文件执行碎片整理。

较大的文件大小会增加 KAVSHELL VACUUM 命令完成碎片整理操作所需的时间。

执行 KAVSHELL VACUUM 命令时，"实时保护"和"计算机控制"任务不可用。碎片整理过程会限制对 Kaspersky Embedded Systems Security 日志的访问并阻止事件日志记录。为避免保护能力下降，建议计划何时运行 KAVSHELL VACUUM 命令。

若要对 Kaspersky Embedded Systems Security 日志文件进行碎片整理，请执行以下命令：

```
KAVSHELL VACUUM
```

此命令需要本地系统账户权限。

清理 iSwift 库：KAVSHELL FBRESET

Kaspersky Embedded Systems Security 使用 iSwift 技术，该技术可使应用程序避免重新扫描自上次扫描以来尚未修改的文件（**使用 iSwift 技术**）。

Kaspersky Embedded Systems Security 在"%SYSTEMDRIVE%\System Volume Information"文件夹中创建 klamfb.dat 和 klamfb2.dat 文件。这两个文件包含有关已扫描的干净对象的信息。文件 klamfb.dat (klamfb2.dat) 随着 Kaspersky Embedded Systems Security 扫描的文件数的增加而增大。它仅包含有关系统中的文件的当前信息：如果删除一个文件，Kaspersky Embedded Systems Security 将从 klamfb.dat 中清除相应信息。

要清理文件，请使用 `KAVSHELL FBRESET` 命令。

使用 `KAVSHELL FBRESET` 命令时，请注意以下说明：

- 使用 KAVSHELL FBRESET 命令清理 klamfb.dat 文件时，Kaspersky Embedded Systems Security 不会暂停保护（与手动删除 klamfb.dat 时的情况不同）。
- 清除 klamfb.dat 中的数据后，Kaspersky Embedded Systems Security 可能会增加受保护设备工作负载。在这种情况下，Kaspersky Embedded Systems Security 将扫描在清除 klamfb.dat 后首次访问的所有文件。扫描后，Kaspersky Embedded Systems Security 将有关每个扫描的对象的信息放回 klamfb.dat。如果有新的访问对象的尝试，iSwift 技术会阻止重新扫描未更改的文件。

只有在 SYSTEM 账户下启动命令行解释器时，才能使用 `KAVSHELL FBRESET` 命令。

启用和禁用 dump 文件创建：KAVSHELL DUMP

可以使用"`KAVSHELL DUMP`"命令启用或禁用在 Kaspersky Embedded Systems Security 进程异常终止时创建进程快照（Dump 文件）（请参见下表）。此外，还可以随时创建正在运行的 Kaspersky Embedded Systems Security 进程的 dump 文件。

为了成功创建 Dump 文件，必须在本地系统账户 (SYSTEM) 下执行 `KAVSHELL DUMP` 命令。

Kaspersky Embedded Systems Security 会以未加密的形式将信息写入到跟踪文件和 Dump 文件。

KAVSHELL DUMP 命令不能用于 x64 进程。

KAVSHELL DUMP 命令语法

```
KAVSHELL DUMP </ON /F:<folder with the dump file>|/SNAPSHOT /F:< 包含 dump 文件的文件夹> /
P:<pid> | /OFF>
```

KAVSHELL DUMP 命令行参数/选项

密钥	描述
/ON	启用当进程异常终止时创建 dump 文件。
/F:<包含 dump 文件的文件夹的路径 >	这是必需参数。它指定将保存 dump 文件的文件夹的路径。不允许指定其他不受保护设备的网络驱动器上的文件夹路径。 在指定 dump 文件的文件夹的路径时，可以使用系统环境变量；不允许使用用户环境变量。
/SNAPSHOT	获取正在运行的具有指定 PID 的进程的内存快照，并将 Dump 文件保存在 /F 参数指定的文件夹中。
/P	进程标识符 (PID) 显示在 Microsoft Windows 任务管理器中。
/OFF	禁用当进程异常终止时创建 dump 文件。

KAVSHELL DUMP 命令的返回代码。

KAVSHELL DUMP 命令示例

要启用创建 dump 文件的功能并且将 dump 文件保存到文件夹"C:\Dump Folder"，请执行以下命令：

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

要为 ID 为 1234 的进程生成 dump 并将其保存到文件夹"C:/Dumps"中，请执行以下命令：

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

要禁用创建 dump 文件的功能，请执行以下命令：

```
KAVSHELL DUMP /OFF
```

导入设置：KAVSHELL IMPORT

您可以使用 `KAVSHELL IMPORT` 命令将 Kaspersky Embedded Systems Security 的设置和当前任务从配置文件导入到受保护设备上的 Kaspersky Embedded Systems Security 副本。可以使用 `KAVSHELL EXPORT` 命令创建配置文件。

执行此命令可能需要密码。要输入当前密码，请使用 `[/pwd:<密码>]`。

KAVSHELL IMPORT 命令语法

```
KAVSHELL IMPORT <配置文件名称和文件路径>
```

KAVSHELL IMPORT 命令示例

```
KAVSHELL IMPORT Host1.xml
```

KAVSHELL IMPORT 命令行参数

参数	描述

<配置文件名称和文件路径>	用作设置导入源的配置文件的名称。 在指定文件路径时，可以使用系统环境变量；不允许使用用户环境变量。

KAVSHELL IMPORT 命令的返回代码。

导出设置：KAVSHELL EXPORT

您可以使用 KAVSHELL EXPORT 命令将 Kaspersky Embedded Systems Security 的所有设置及其当前任务导出到配置文件中，以便日后将其导入到安装在其他受保护设备上的 Kaspersky Embedded Systems Security 副本。

KAVSHELL EXPORT 命令语法

```
KAVSHELL EXPORT <配置文件名称和文件路径>
```

KAVSHELL EXPORT 命令示例

```
KAVSHELL EXPORT Host1.xml
```

KAVSHELL EXPORT 命令行参数

参数	描述
<配置文件名称和文件路径>	将包含设置的配置文件的名称。 可以为配置文件分配任何文件扩展名。 在指定文件路径时，可以使用系统环境变量；不允许使用用户环境变量。

KAVSHELL EXPORT 命令的返回代码。

与 Microsoft Operations Management Suite 集成：KAVSHELL OMSINFO

可以使用 KAVSHELL OMSINFO 命令查看应用程序的状态以及反病毒数据库和 KSN 服务检测到的威胁的相关信息。有关威胁的信息取自可用的事件日志。

KAVSHELL OMSINFO 命令语法

```
KAVSHELL OMSINFO <生成的文件的完整路径与文件名>
```

KAVSHELL OMSINFO 命令示例

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

KAVSHELL OMSINFO 命令行参数

参数	描述
<生成的文件的路径与文件名>	生成的文件的名称，该文件将包含应用程序状态和任何检测到的威胁的相关信息。

管理“基线文件完整性监控”任务：KAVSHELL FIM /BASELINE

可以使用 KAVSHELL FIM /BASELINE 命令来配置“基线文件完整性监控”任务运行和监控 DLL 模块的加载的模式。

执行此命令可能需要密码。要输入当前密码，请使用 [/pwd:<密码>]。

KAVSHELL FIM /BASELINE 命令语法

KAVSHELL FIM /BASELINE [/CREATE: [<监控范围> | /L:<包含监控区域列表的 TXT 文件的路径>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<基线 id> | /ALIAS:<现有别名>]] | [/EXPORT:<TXT 文件的路径> [/BL:<基线 id> | /ALIAS:<现有别名>]] | [/SHOW [/BL:基线 id> | /ALIAS:<现有别名>]] | [/SCAN [/BL:<基线 id> | /ALIAS:<现有别名>]] | [/PWD:<密码>]

KAVSHELL FIM /BASELINE 命令示例

要删除基线，请运行以下命令：

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<基线 id>
```

可以使用命令行参数来配置“基线文件完整性监控”任务设置（请参见以下表格）。

KAVSHELL FIM/ BASELINE 命令行参数/选项

参数/选项	描述
/CREATE	创建新的“基线文件完整性监控”任务。 Kaspersky Embedded Systems Security 将启动新的“基线文件完整性监控”任务以创建基线。
/L	指定包含监控区域列表的 TXT 文件的路径。
/MD5	指定用于计算校验和的 MD5 算法（可选参数）。 /MD5 参数不能与 /SHA256 一起使用。 默认情况下使用 MD5 算法。
/SHA256	指定用于计算校验和的 SHA256 算法（可选参数）。 /SHA256 参数不能与 /MD5 一起使用。 默认情况下使用 MD5 算法。
/SF	将所有子文件夹包括在“基线文件完整性监控”任务范围中（可选参数）。 默认情况下，所有子文件夹都从“基线文件完整性监控”任务范围中排除。
/CLEAR	删除具有指定 <基线 id> 的基线或具有指定 <现有别名> 的任务的基线。 如果 <基线 id> 和 <现有别名> 均未指定，则删除所有基线。 可选参数。

/BL	指定基线的唯一 ID（可选参数）。
/EXPORT	将所有基线的相关数据导出到 TXT 文件。
/SHOW	显示所有基线的相关数据。
/SCAN	以指定的 <基线 id> 或指定的 <现有别名> 启动新的“基线文件完整性监控”任务。
/ALIAS	指定现有任务的名称或新任务的名称。
<监控范围>	指定要包括在“基线文件完整性监控”任务范围中的文件或文件夹。 此参数仅允许指定一个区域。
<包含监控区域列表的 TXT 文件的路径>	指定包含监控区域列表的 TXT 文件的路径。 该文件必须为 UTF-8 编码，并且每个监控区域路径都必须在单独的行中指定。
<TXT 文件的路径>	指定要将所有基准的相关数据导出到的文件的路径。
<基线 id>	指定基线的唯一 ID。 您可以使用 /SHOW 参数来学习基线的 ID。
<现有别名>	指定现有任务的名称。
<新别名>	指定新任务的名称。

命令返回代码

KAVSHELL START 和 KAVSHELL STOP 命令的返回代码

KAVSHELL START 和 KAVSHELL STOP 命令的返回代码

返回代码	描述
0	操作已成功完成
-3	权限错误
-5	命令语法无效
-6	操作无效（例如，Kaspersky Security 服务已经运行或已经停止）
-7	服务未注册
-8	已禁用自动服务启动。
-9	使用其他用户账户启动受保护设备的尝试失败（默认情况下，Kaspersky Security 服务在本地系统用户账户下运行）
-99	未知错误

KAVSHELL SCAN 和 KAVSHELL SCANCRITICAL 命令的返回代码

KAVSHELL SCAN 和 KAVSHELL SCANCRITICAL 命令的返回代码

返回代码	描述
0	操作已成功完成（未检测到威胁）
1	操作已取消
-2	服务未运行
-3	权限错误
-4	未找到对象（未找到包含扫描范围列表的文件）
-5	命令语法无效或扫描范围未定义
-80	检测到受感染和其他对象
-81	检测到疑似感染的对象
-82	检测到处理错误
-83	发现未扫描的对象
-84	检测到损坏的对象
-85	创建任务日志失败
-99	未知错误
-301	密钥无效

KAVSHELL TASK LOG-INSPECTOR 命令的返回代码

KAVSHELL TASK LOG-INSPECTOR 命令的返回代码

返回代码	描述
0	操作已成功完成
-6	操作无效（例如，Kaspersky Security 服务已经运行或已经停止）
402	任务已经运行（针对 /STATE 选项）

KAVSHELL TASK 命令的返回代码

KAVSHELL TASK 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-4	未找到对象（未找到任务）
-5	命令语法无效
-6	操作无效（例如，任务未运行、已经运行或无法暂停）
-99	未知错误
-301	密钥无效

401	任务未运行（针对 /STATE 选项）
402	任务已经运行（针对 /STATE 选项）
403	任务已经暂停（针对 /STATE 选项）
-404	操作失败（任务状态更改导致崩溃）

KAVSHELL RTP 命令的返回代码

KAVSHELL RTP 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-4	未找到对象（未找到一个或所有实时计算机保护任务）
-5	命令语法无效
-6	操作无效（例如，任务已经运行或已经停止）
-99	未知错误
-301	密钥无效

KAVSHELL UPDATE 命令的返回代码

KAVSHELL UPDATE 命令的返回代码

返回代码	描述
0	操作已成功完成
200	所有对象都是最新的（数据库或程序组件是最新的）
-2	服务未运行
-3	权限错误
-5	命令语法无效
-99	未知错误
-206	扩展文件不在指定的源中或具有未知格式
-209	连接到更新源时出错
-232	连接到代理服务器时发生身份验证错误
-234	连接到 Kaspersky Security Center 时出错
-235	Kaspersky Embedded Systems Security 在连接到更新源时未通过身份验证
-236	应用程序数据库已损坏
-301	密钥无效

KAVSHELL ROLLBACK 命令的返回代码

KAVSHELL ROLLBACK 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-99	未知错误
-221	数据库备份副本未找到或已损坏
-222	数据库备份副本已损坏

KAVSHELL LICENSE 命令的返回代码

KAVSHELL LICENSE 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	管理密钥的权限不足
-4	未找到包含指定数字的密钥
-5	命令语法无效
-6	操作无效（密钥已添加）
-99	未知错误
-301	密钥无效
-303	授权许可适用于其他程序

KAVSHELL TRACE 命令的返回代码

KAVSHELL TRACE 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-4	未找到对象（未找到为跟踪日志文件夹指定的路径）
-5	命令语法无效
-6	操作无效（跟踪日志已被禁用时试图执行 KAVSHELL TRACE /OFF 命令）
-99	未知错误

KAVSHELL FBRESET 命令的返回代码

KAVSHELL FBRESET 命令的返回代码

返回代码	描述
0	操作已成功完成
-99	未知错误

KAVSHELL DUMP 命令的返回代码

KAVSHELL DUMP 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-4	未找到对象（未找到为 dump 文件夹指定的路径；未找到具有指定 PID 的进程）
-5	命令语法无效
-6	操作无效（在 dump 文件创建功能已禁用的情况下尝试执行 KAVSHELL DUMP/OFF 命令）
-99	未知错误

KAVSHELL IMPORT 命令的返回代码

KAVSHELL IMPORT 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-4	未找到对象（无法找到可以导入的配置文件）
-5	语法无效
-99	未知错误
501	操作已成功完成，但有一个错误/注释，例如，Kaspersky Embedded Systems Security 未导入某些功能组件的参数
-502	导入文件缺失或其格式无法识别
-503	设置不兼容（配置文件是从其他程序或从 Kaspersky Embedded Systems Security 的更高版本和不兼容版本导出的）

KAVSHELL EXPORT 命令的返回代码

KAVSHELL EXPORT 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-5	语法无效
-10	无法创建配置文件（例如，无权访问在文件路径中指定的文件夹）
-99	未知错误
501	操作已成功完成，但有一个错误/注释，例如，Kaspersky Embedded Systems Security 未导出某些功能组件的参数

KAVSHELL FIM /BASELINE 命令的返回代码

KAVSHELL FIM /BASELINE 命令的返回代码

返回代码	描述
0	操作已成功完成
-2	服务未运行
-3	权限错误
-4	未找到对象（未找到任务）
-5	命令语法无效
-6	无效操作（例如，基线已被删除）
-10	无法创建配置文件（例如，无权访问在文件路径中指定的文件夹）
-12	无效密码
-80	与检测到的基线对象不一致
-85	创建任务日志失败
-99	内部错误
-303	无效授权许可密钥
-502	任务未运行
200	所有对象均与基线一致
501	任务成功完成，但有错误/注释

联系技术支持

本节介绍了获得技术支持的方法以及需要满足的条件。

如何获取技术支持

如果在程序文档或有关程序的任何信息来源中找不到问题的解决方案，推荐您与技术支持联系。技术支持专家将为您解答有关安装和使用应用程序的问题。

技术支持仅适用于购买了应用程序商业授权许可的用户。技术支持不适用于具有试用授权许可的用户。

根据应用程序生命周期提供应用程序支持（请参阅应用程序生命周期页面）。

与技术支持部门联系之前，请通读技术支持规则。

您可以通过借助 Kaspersky CompanyAccount 门户向卡巴斯基技术支持服务部门发送请求来联系技术支持。

通过 Kaspersky CompanyAccount 获取技术支持

Kaspersky CompanyAccount 是一个为使用 Kaspersky 应用程序的公司提供的门户。Kaspersky CompanyAccount 设计用于方便用户与 Kaspersky 专家之间通过在线请求进行交互。通过使用 Kaspersky CompanyAccount 门户，您可以监视 Kaspersky 专家处理电子请求的进度并存储电子请求的历史记录。

可以在 Kaspersky CompanyAccount 上的单个用户账户中注册您组织的所有员工。通过使用单个账户，您可以集中管理注册的员工发送到 Kaspersky 的电子请求，以及通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 适用于以下语言：

- 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。

使用跟踪文件和 AVZ 脚本

向 Kaspersky 技术支持专家报告问题后，他们可能会要求您生成一个包含有关 Kaspersky Embedded Systems Security 运行情况的信息的报告，然后将该报告发送到 Kaspersky 技术支持部门。Kaspersky 技术支持专家还可能会要求您创建一个跟踪文件。可以通过跟踪文件了解应用程序命令的分步执行过程，以确定出现错误的应用程序运行阶段。

在分析您发送的数据后，Kaspersky 技术支持专家可以创建一个 AVZ 脚本并将其发给您。通过使用 AVZ 脚本，可以分析活动进程以查找威胁，扫描受保护设备以查找威胁，清除或删除被感染的文件以及创建系统扫描报告。

术语表

事件严重性

在卡巴斯基应用程序运行过程中遇到的事件的属性。有以下严重级别：

- 严重事件
- 功能故障
- 警告
- 信息

同一类型的事件可能有不同的严重级别，具体取决于发生事件时的情况。

任务

卡巴斯基应用程序执行的功能采用任务形式实施，如：实时文件保护、计算机完全扫描和数据库更新。

任务设置

特定于每种任务类型的应用程序设置。

保护状态

当前保护状态，反映计算机安全性的级别。

卡巴斯基安全网络 (KSN)

一个云服务基础架构，提供对卡巴斯基数据库的访问，该数据库不断更新关于文件、Web 资源和软件的信誉的信息。卡巴斯基安全网络确保卡巴斯基应用程序对威胁做出更快响应，提高一些保护组件的性能，并降低误报可能性。

压缩文件

一个或多个文件通过压缩打包到单个文件中。压缩和解压缩数据需要一个名为“压缩应用程序”的专用应用程序。

反病毒数据库

该数据库中包含截至到反病毒数据库发布日期卡巴斯基已知的计算机安全威胁相关信息。反病毒数据库中的条目用于在扫描的对象中检测恶意代码。反病毒数据库由卡巴斯基的专家创建，并且每小时更新一次。

受感染的对象

其部分代码完全匹配已知恶意软件部分代码的对象。卡巴斯基不推荐访问此类对象。

可感染的文件

一种由于其结构或格式，可被罪犯用作存储和传播恶意代码的"容器"的文件。通常为可执行文件，此类文件扩展名为 .com、.exe 和 .dll。此类文件被恶意代码侵入的风险非常高。

启动对象

计算机上安装的操作系统和软件正常启动和运行所需的一组应用程序。每次启动操作系统时，都会执行这些对象。有些病毒专门感染此类对象，可能会导致操作系统无法启动等问题。

启发式分析

用于检测其信息尚未添加到卡巴斯基数据库中的威胁的技术。启发式分析用于检测行为方式可能对操作系统构成安全威胁的对象。启发式分析检测到的对象将被视为可能已感染。例如，如果一个对象包含恶意对象通常具有的命令序列（打开文件、写入到文件），则可能会将该对象视为可能已感染。

备份

用来存储文件备份副本的特殊存储器，在尝试清除或删除前创建的。

安全信息与事件管理（SIEM）

一种用于分析来源于各种网络设备和应用程序的安全事件的技术。

安全级别

安全级别定义为一组预先配置的应用程序组件设置。

对象链接与嵌入（OLE）对象

附加到其他文件或通过使用对象链接与嵌入 (OLE) 技术嵌入其他文件的对象。一个 OLE 对象示例是嵌入到 Microsoft Office Word 文档中的 Microsoft Office Excel® 电子表格。

授权许可期限

一个时间段，在此时间段内您可以访问应用程序功能，并有权使用附加服务。您可以使用的服务取决于授权许可的类型。

文件掩码

使用通配符表示文件名。文件掩码中使用的标准通配符为 * 和 ?，其中 * 表示任意数量的任意字符，? 表示单个任意字符。

更新

替换或添加从 卡巴斯基更新服务器检索到的新文件（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运行的任务。

活动密钥

应用程序当前使用的密钥。

清除

处理已感染对象的一种方法，清除后可完全或部分恢复数据。并非所有已感染对象都可以清除。

漏洞

恶意软件制造者可能会利用操作系统或应用程序中存在的缺陷，侵入操作系统或应用程序，破坏其完整性。操作系统中的许多漏洞都会导致操作系统运行不可靠，因为侵入操作系统的病毒可能会导致操作系统本身和安装的应用程序损坏。

策略

策略确定应用程序的设置，并控制在管理组内的计算机上配置该应用程序的能力。必须为每个应用程序创建单独策略。您可以为每个管理组内的计算机上安装的应用程序创建多个策略，但在一个管理组内一次只能对每个应用程序应用一个策略。

管理服务器

Kaspersky Security Center 的一个组件，可集中存储公司网络内安装的所有 Kaspersky 应用程序的信息。它也可用于管理这些应用程序。

误报

卡巴斯基应用程序因对象的代码与病毒的代码类似而将未感染的对象视为受感染对象的情况。

隔离

卡巴斯基应用程序将检测到的可能已感染对象移动到的文件夹。为避免对计算机造成任何影响，对象会以加密的形式存储在隔离区。

有关第三方代码信息

有关第三方代码信息包含在文件 legal_notices.txt 中，该文件位于应用程序安装文件夹中。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

Dell Technologies、Dell、EMC、Celerra、VNX 以及其他商标是 Dell Inc. 或其子公司的商标。

Domino、Lotus 和 Lotus Notes 是 International Business Machines Corporation 在全球许多司法管辖区注册的商标。

Intel 和 Pentium 是 Intel Corporation 在美国和/或其他国家/地区的商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft、Active Directory、Forefront、Excel、Hyper-V、Internet Explorer、Lync、Outlook、SharePoint、SQL Server、Windows、Windows Server、Windows Vista、Windows XP 是 Microsoft 集团公司的商标。

NetApp 是 NetApp, Inc. 在美国和/或其他国家/地区的商标或注册商标。

Schneider Electric 是 Schneider Electric 的商标。

Siemens、WinCC 和 Simatic 是 Siemens AG 的注册商标。

CVE 是 MITRE 公司的注册商标。

UNIX 是在美国和其他国家/地区的注册商标，通过 X/Open Company Limited 独家授权。