KASPERSKY lab

Kaspersky Embedded Systems Security

管理手冊

應用程式版本：2.2.0.605

親愛的使用者：

感謝您選擇 Kaspersky Lab 作為您的安全軟體提供商。我們希望本文件能幫助您使用我們的產品。

文件修訂日期：2018.10.29

https://www.kaspersky.com
https://support.kaspersky.com/

內容

關於本手冊

Kaspersky Embedded Systems Security 2.2.0.605（下文稱為“ Kaspersky Embedded Systems Security 2.2”、“ 應用程式”）管理手冊的編寫目的是，供在所有受防護裝置上安裝和管理 Kaspersky Embedded Systems Security 2.2 的專家，以及使用 Kaspersky Embedded Systems Security 2.2 為各組織提供技術支援的專家使用。

本手冊包含有關配置和使用 Kaspersky Embedded Systems Security 2.2 的資訊。

本手冊還可協助您瞭解有關應用程式的資訊來源以及獲得技術支援的方法。

本章內容

本手冊說明主旨

Kaspersky Embedded Systems Security 2.2 管理員手冊由以下章節組成：

有關 Kaspersky Embedded Systems Security 2.2 的資訊來源

本章節介紹程式的相關資訊來源。

Kaspersky Embedded Systems Security 2.2

本節介紹了 Kaspersky Embedded Systems Security 2.2 的功能、元件以及分發套件，並提供了 Kaspersky Embedded Systems Security 2.2 的硬體和軟體需求清單。

安裝和移除應用程式

本節提供安裝和移除 Kaspersky Embedded Systems Security 2.2 的逐步說明。

應用程式介面

本節包含有關 Kaspersky Embedded Systems Security 2.2 介面元素的資訊。

應用程式授權

本章節提供與應用程式產品授權有關的主要概念的資訊。

啟動和停止 Kaspersky Embedded Systems Security 2.2

本節包含有關啟動和停止 Kaspersky Embedded Systems Security 2.2 管理外掛程式（下文稱為管理外掛程式）和 Kaspersky Security 服務的資訊。

關於 Kaspersky Embedded Systems Security 2.2 功能的存取權限

本節包含有關 Kaspersky Embedded Systems Security 2.2 和應用程式註冊的 Windows® 服務的管理權限的資訊，以及如何設定這些權限的說明。

建立和設定政策

本節包含有關使用卡巴斯基安全管理中心政策在多台電腦上管理 Kaspersky Embedded Systems Security 2.2 的資訊。

使用卡巴斯基安全管理中心建立和管理工作

本節包含有關 Kaspersky Embedded Systems Security 2.2 工作、如何建立工作、配置工作設定，以及啟動和停止工作的資訊。

管理應用程式設定

本章節包含有關在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 一般設定的資訊。

即時電腦防護

本節提供有關“即時電腦防護”工作的資訊：即時檔案防護、KSN 使用以及弱點利用防禦功能。它還提供了有關如何設定即時防護工作和管理受防護電腦的安全設定說明。

本機活動控制

本節提供有關用於控制應用程式啟動和透過 USB 連線到外部裝置的 Kaspersky Embedded Systems Security 2.2 功能的資訊。

網路活動控制

本節包含有關“防火牆管理”工作的資訊。

系統稽核

本節包含有關檔案完整性監控工作以及稽核作業系統記錄功能的資訊。

與協力廠商系統整合

本節介紹 Kaspersky Embedded Systems Security 2.2 與協力廠商功能和技術的整合。

從命令列使用 Kaspersky Embedded Systems Security 2.2

本節描述從命令列使用 Kaspersky Embedded Systems Security 2.2。

聯絡技術支援

本章節提供有關如何與 Kaspersky Lab 技術支援服務聯絡的資訊。

詞彙表

本章節包含文件中提到的專業術語及其自訂的清單。

AO Kaspersky Lab

本章節包含有關 AO Kaspersky Lab 的資訊。

有關協力廠商程式碼資訊

本章節提供有關程式中使用的協力廠商代碼資訊。

商標聲明

本章節列出本文中協力廠商的商標聲明。

索引

本章節使您可以在文件中快速尋找所需的資訊。

文件說明

本文件使用以下約定（參閱下表）。

步驟 1.　　文件說明

範例文件	文件約定的說明
注意...	警告使用紅色字型和括號來註明。警告含有可能造成您的資料遺失以及硬體或作業系統故障的潛在危險資訊。
我們建議您使用...	註釋使用括號表示。註釋包含補充和參考資訊。
範例： ...	示範區域採用藍色背景，並且帶有“示範”標題。
更新是指... 發生了“資料庫已過期”事件。	下列的項目使用斜體字來註明： • 新的專有名詞 • 程式狀態和事件名稱
點擊 ENTER 鍵。 點擊 ALT+F4。	鍵盤鍵名稱用粗體顯示並採用大寫。 以“+”號相連的按鍵名稱表示按鍵組合。這些按鍵必須同時點擊。
點擊“**啟用**”按鈕。	應用程式介面內容（例如，輸入欄位、選單項和按鈕）的名稱以粗體顯示。
► *要設定工作排程：*	步驟標題以斜體顯示，並伴以箭頭符號。
在命令列中，輸入 help 隨後會出現以下訊息： 使用 dd:mm:yy 格式指定日期。	下列類型的文件內容用特殊字型顯示： • 命令列語法 • 應用程式顯示在視窗中的資訊文字 • 使用者必須輸入的資料
<使用者名稱>	變數放在角括號中。您應該根據具體情況用對應的值取代變數，取代時要省略角括號。

有關 Kaspersky Embedded Systems Security 2.2 的資訊來源

本章節介紹程式的相關資訊來源。

您可依據問題的緊急或重要等級，來選取最適宜的來源。

本章內容

可供自行查詢的資料來源

您可以使用以下來源尋找有關 Kaspersky Embedded Systems Security 2.2 的資訊：

- Kaspersky Lab 網站上的 Kaspersky Embedded Systems Security 2.2 頁面。
- 技術支援網站（知識庫中）的 Kaspersky Embedded Systems Security 2.2 頁面。
- 手冊。

如果您有無法自行排除的問題，請聯絡 Kaspersky Lab 技術支援部門 https://support.kaspersky.com/。

若要使用 Kaspersky Lab 網站資訊來源，您必須連線網際網路。

Kaspersky Lab 網站上的 Kaspersky Embedded Systems Security 2.2 頁面

在 Kaspersky Embedded Systems Security 2.2 頁面 (https://www.kaspersky.com/enterprise-security/embedded-systems) 上，您可以檢視有關程式、它的功能和特色的基本資訊。

Kaspersky Embedded Systems Security 2.2 頁面包含指向 eStore 的連結。您可以在此購買或續約產品授權。

知識庫中的 Kaspersky Embedded Systems Security 2.2 頁面

知識庫是技術支援網站的一部分。

知識庫 (https://support.kaspersky.com/kess2) 中的 Kaspersky Embedded Systems Security 2.2 頁面上，您可以閱讀文章，這些文章提供實用的資訊、建議以及有關如何購買、安裝和使用程式的常見問題解答。

知識庫文章不僅可以解答與 Kaspersky Embedded Systems Security 2.2 有關的問題，而且還可以解答與其他 Kaspersky Lab 應用程式有關的問題。它們還可能包含來自技術支援服務的新聞。

Kaspersky Embedded Systems Security 2.2 文件

《Kaspersky Embedded Systems Security 2.2 管理手冊》包含有關應用程式安裝、移除、設定配置和使用的資訊。

在網路論壇上討論 Kaspersky Lab 的應用程式

如果您的問題不需要立即性的回答，您可以在我們的論壇 http://forum.kaspersky.com/ 中與 Kaspersky Lab 專家及其他使用者進行討論。

在此論壇中，您可以檢視現有主旨、發表評論並建立新的討論主旨。

Kaspersky Embedded Systems Security 2.2

本節介紹了 Kaspersky Embedded Systems Security 2.2 的功能、元件以及分發套件，並提供了 Kaspersky Embedded Systems Security 2.2 的硬體和軟體需求清單。

本章內容

關於 Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 防護執行 Microsoft® Windows 的電腦和其他嵌入式系統免受病毒和其他電腦威脅。Kaspersky Embedded Systems Security 2.2 使用者是負責公司網路病毒防護的系統管理員和專業人員。

您可以在執行 Windows 的各種嵌入式系統上安裝 Kaspersky Embedded Systems Security 2.2, 包括以下裝置類型：

- ATM（自動櫃員機）；
- POS（銷售點）。

可透過以下方式管理 Kaspersky Embedded Systems Security 2.2：

- 透過與 Kaspersky Embedded Systems Security 2.2 安裝在同一台電腦上或安裝在其他電腦上的應用程式主控台來管理。
- 在命令列中使用指令。
- 透過卡巴斯基安全管理中心管理主控台。

卡巴斯基安全管理中心也可以集中管理執行 Kaspersky Embedded Systems Security 2.2 的多台電腦。

您可以檢視針對“系統監控”應用的 Kaspersky Embedded Systems Security 2.2 效能計數器以及 SNMP 計數器和 TRAP。

Kaspersky Embedded Systems Security 2.2 元件和功能

應用程式包含以下元件：

- **即時檔案防護**。Kaspersky Embedded Systems Security 2.2 在物件被存取時掃描物件。Kaspersky Embedded Systems Security 2.2 可掃描以下物件：
  - 檔案
  - 交換檔案系統執行緒（NTFS 執行緒）
  - 本機硬碟磁碟機和卸除式裝置上的主開機紀錄區和啟動磁區

- **自訂掃描**。Kaspersky Embedded Systems Security 2.2 可在指定區域執行單獨的掃描，以偵測病毒和其他電腦安全威脅。應用程式會掃描受防護電腦上的檔案、RAM 和啟動物件。
- **應用程式啟動控制**。該元件可跟蹤使用者在受防護電腦上啟動應用程式的嘗試並控制應用程式啟動。
- **裝置控制**。該元件可控制大容量儲存器和 CD/DVD 磁碟機的註冊和使用，以便防護電腦在與 USB 連線的快閃記憶體磁碟機或其他類型的外部裝置交換檔案時，免受可能產生的電腦安全威脅。
- **防火牆管理**。此元件提供管理 Windows 防火牆的能力：配置設定和作業系統防火牆規則，並封鎖從外部配置防火牆的任何可能性。
- **檔案完整性監控**。Kaspersky Embedded Systems Security 2.2 可以偵測工作設定中指定的監控範圍內的檔案變更。這些變更可能表示受防護電腦遭到安全入侵。
- **記錄審查**。此元件根據 Windows 事件記錄的審查結果，對受防護環境的完整性進行監控。

應用程式中佈署了以下功能：

- **資料庫更新與軟體模組更新**。Kaspersky Embedded Systems Security 2.2 會從 Kaspersky Lab 的 FTP 或 HTTP 更新伺服器、卡巴斯基安全管理中心管理伺服器或其他更新來源中下載應用程式資料庫和模組更新。
- **隔離**。Kaspersky Embedded Systems Security 2.2 透過將疑似被感染的物件從原始位置移動到*隔離*來進行隔離。出於安全考慮，物件以加密形式儲存在隔離中。
- **備份**。對於被歸類為“*受感染*”或“*疑似感染*”的物件，Kaspersky Embedded Systems Security 2.2 會在對其進行解毒或刪除之前，在*備份*中儲存這些物件的加密副本。
- **管理員和使用者通知**。您可以對此程式進行設定，通知存取受防護電腦的管理員和使用者，有關 Kaspersky Embedded Systems Security 2.2 操作中的事件和電腦上病毒防護的狀態。
- **匯入和匯出設定**。可以將 Kaspersky Embedded Systems Security 2.2 設定匯出到 XML 設定檔，也可以將設定檔中的設定匯入到 Kaspersky Embedded Systems Security 2.2 中。可以將所有應用程式設定或僅將單個元件的設定儲存到設定檔。
- **套用範本**。可以在電腦的檔案資源樹狀目錄或清單中手動配置節點的安全設定，並將配置好的設定值儲存為範本。然後可在 Kaspersky Embedded Systems Security 2.2 防護和掃描工作中使用該範本來設定其他節點的安全設定。
- **管理 Kaspersky Embedded Systems Security 功能的存取權限**。您可以為使用者和使用者群組設定管理 Kaspersky Embedded Systems Security 2.2 的權限和管理應用程式註冊的 Windows 服務的權限。
- **將事件寫入到應用程式事件記錄**。Kaspersky Embedded Systems Security 2.2 將記錄有關軟體元件設定的資訊、目前工作狀態、工作執行過程中發生的事件、與 Kaspersky Embedded Systems Security 2.2 管理相關的事件，以及 Kaspersky Embedded Systems Security 2.2 錯誤診斷所需的資訊。
- **信任區域**。您可以從防護範圍或掃描範圍中生成排除清單，Kaspersky Embedded Systems Security 2.2 將在自訂和即時防護工作中套用該清單。
- **弱點利用防禦**。您可以使用注入處理程序的代理來防護處理程序記憶體免受弱點利用。

新增功能

Kaspersky Embedded Systems Security 2.2 提供以下新功能和改進：

- 支援新版本的 Microsoft Windows 作業系統。

  基於 ELAM 和 PPL 技術的自我防禦機制：現在，當安裝應用程式時，它會自動註冊 ELAM 驅動程式，該驅動程式可以使用 Protected Process Light 內容啟動 Kaspersky Security 服務 (kavfs.exe)。這樣可以增強應用程式的自我防禦能力並預防大範圍的攻擊。

  當應用程式安裝在執行 Microsoft Windows 10 RS2（內部版本號 15063）或更高的系統上時該功能可用。

- 支援在 Microsoft OneDrive 上檢查和處理儲存的雲端檔案。

- 軟體分發控制子系統的可行性得到改善。

  現在，您可以指明哪些安裝檔案可以為從中提取的整個檔案鏈傳遞受信任的安裝套件內容。這使在啟用了“應用程式啟動控制”的電腦上提高軟體安裝過程的穩定性成為了可能，但增加授權應用程式啟動的數量也擴大了潛在受攻擊的區域。建議在佈署複雜的軟體期間使用此選項，包括在軟體分發過程中必須重新啟動伺服器時。

- 與 WMI 工具整合。

  現在，在安裝應用程式時，將在本機電腦上的 WMI 根命名空間中自動建立 Kaspersky Security 命名空間。您可以使用支援 WMI 查詢的用戶端解決方案來獲取有關應用程式及其元件的資料。

- 使用 KAVSHELL OMSINFO 指令延伸了顯示有關應用程式及其元件的資訊格式：現在，您可以獲取有關應用程式啟動控制工作狀態的資訊以及有關已安裝的應用程式模組關鍵更新的資訊。

- 使用緊湊型診斷介面改進管理和監控應用程式狀態的可能性：

  - 現在，您可以在小型診斷視窗的統計標籤上檢視已安裝元件的統計計數器。
  - 存取小型診斷視窗時不需要密碼，即使密碼防護功能處於開啟狀態：應用程式套用管理也只能根據指定的使用者權限限制對小型診斷視窗中可用的資訊和控制元素的存取。

- 從版本 2.2 開始，應用程式能夠在作業系統以安全模式啟動期間提供基本電腦防護。

  預設情況下，應用程式在執行於安全模式的電腦上不工作。要使應用程式在作業系統以安全模式啟動時啟動，請將以下 Windows 登錄機碼中的 LoadInSafeMode 參數設定為等於 1：

  HKLM\SYSTEM\CurrentControlSet\services\klam\Parameters

  > 在以安全模式啟動的電腦上執行時，應用程式的功能將受到限制。

- 卡巴斯基安全管理中心報告受到支援：您現在可以檢視有關應用程式元件狀態的報告以及兩種類型的有關已禁止的應用程式的報告。

  僅當使用卡巴斯基安全管理中心 11 時才支援此功能。

- 變更安裝資料夾和修改應用程式元件關鍵登錄檔分支的使用者存取權限現在受到限制。

分發套件

安裝套件包含常用的應用程式，您可以用它來執行以下操作：

- 啟用 Kaspersky Embedded Systems Security 2.2 安裝精靈。
- 啟用 Kaspersky Embedded Systems Security 2.2 主控台安裝精靈。
- 啟動將安裝 Kaspersky Embedded Systems Security 2.2 管理外掛程式的安裝精靈以透過卡巴斯基安全管理中心管理應用程式。
- 閱讀《管理手冊》。
- 閱讀《使用者手冊》。
- 轉到 Kaspersky Lab 網站上的 Kaspersky Embedded Systems Security 2.2 頁面。
- 存取技術支援網站 (https://support.kaspersky.com/)。
- 閱讀有關 Kaspersky Embedded Systems Security 2.2 目前版本的資訊。

\console 資料夾包含用於安裝應用程式主控台的檔案（元件的“Kaspersky Embedded Systems Security 2.2 管理工具”集）。

\product 資料夾包含：

- 用於在執行 32 位元或 64 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Embedded Systems Security 2.2 元件的檔案。
- 用於安裝管理外掛程式的檔案，以便透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security 2.2。
- 程式發佈時最新病毒資料庫的壓縮檔案。
- 包含最終使用者產品授權協議和隱私政策文字的檔案。

\product_no_avbases 資料夾包含 Kaspersky Embedded Systems Security 2.2 元件和外掛程式的安裝檔案，不包含病毒資料庫。

\setup 資料夾包含問候程式啟動檔案。

分發工具套件檔案儲存在不同的資料夾中，具體位置取決於它們的目標用途（請參見以下表格）。

步驟 2. Kaspersky Embedded Systems Security 2.2 分發套件檔案

檔案	用途
autorun.inf	從卸除式介質安裝應用程式時，Kaspersky Embedded Systems Security 2.2 安裝精靈的自動執行檔案。
ess_admin_guide_zh.pdf	管理手冊。
ess_user_guide_zh.pdf	使用者手冊。
release_notes.txt	該檔案包含發佈資訊。
setup.exe	程式安裝檔案（啟動 setup.hta）。
\console\esstools_x86(x64).msi	Windows 安裝程式安裝套件；在受防護電腦上安裝應用程式主控台。

檔案	用途
\console\setup.exe	該檔案啟動元件的“管理工具”元件集（包括應用程式主控台）的安裝精靈；它可使用在安裝精靈中指定的設定啟動 esstools.msi 安裝套件檔案。
\product\bases.cab	程式發佈時最新病毒資料庫的壓縮檔案。
\product\setup.exe	該檔案啟動用於在受防護電腦上安裝 Kaspersky Embedded Systems Security 2.2 的精靈；它使用在精靈中指定的安裝設定啟動安裝套件檔案 ess.msi。
\product\ess_x86(x64).msi	Windows 安裝程式安裝套件；在受防護電腦上安裝 Kaspersky Embedded Systems Security 2.2。
\product\ess.kud	Kaspersky Unicode 定義格式的檔案，帶有用於透過卡巴斯基安全管理中心遠端安裝 Kaspersky Embedded Systems Security 2.2 的安裝套件的描述。
\product\klcfginst.exe	管理外掛程式的安裝程式，以便透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security 2.2。 如果您預計用它來管理 Kaspersky Embedded Systems Security 2.2，請在每台已安裝卡巴斯基安全管理中心管理主控台的電腦上安裝該管理外掛程式。
\product\license.txt	最終使用者產品授權協議和隱私政策的文字。
\product\migration.txt	該檔案介紹從以前的應用程式版本進行移轉。
\setup\setup.hta	程式安裝檔案。

您可以從安裝 CD 執行分發套件檔案。如果您已預先將安裝套件複製到本機硬碟，請確認安裝套件檔案的完整性。

硬體和軟體需求

在安裝 Kaspersky Embedded Systems Security 2.2 之前，您必須先從伺服器移除其他防毒程式。

對受防護電腦的硬體需求

一般需求：

- 採用單處理器和多處理器配置的 x86 相容系統。
- 採用單處理器和多處理器配置的 x64 相容系統。

磁碟磁區：

- 安裝“應用程式啟動控制”元件 – 50 MB。
- 安裝所有 Kaspersky Embedded Systems Security 2.2 元件 – 500 MB。

RAM：

- 256 MB – 在執行 Microsoft® Windows 作業系統的電腦上只安裝“應用程式啟動控制”元件。
- 512 MB – 在執行 Microsoft Windows 作業系統的電腦上執行所有元件的完整安裝。

最低處理器需求：

- 對於 32 位元 Microsoft Windows 作業系統：Intel® Pentium® III。
- 對於 64 位元 Microsoft Windows 作業系統：Intel Pentium IV。

對受防護電腦的軟體需求

您可以在執行 32 位元或 64 位元 Microsoft Windows 作業系統的伺服器上安裝 Kaspersky Embedded Systems Security 2.2。

在執行 Microsoft Windows XP 的電腦上，應用程式正常安裝和工作需要 Windows Installer 3.1。

要在執行嵌入式作業系統的裝置上安裝和使用 Kaspersky Embedded Systems Security 2.2，“篩選管理器”和“管理支援工具”元件是必需的。

您可以在執行下列 32 位元或 64 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Embedded Systems Security 2.2：

- Windows XP Embedded SP3
- Windows XP Pro SP2 / SP3
- Windows Embedded POSReady 2009
- Windows Embedded Standard 7 SP1
- Windows Embedded Enterprise 7 SP1
- Windows Embedded POSReady 7
- Windows 7 Professional / Enterprise SP1
- Windows Embedded 8.1 Industry Professional / Enterprise
- Windows Embedded 8.1 Professional
- Windows Embedded 8.0 Standard
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise

安裝和移除應用程式

本節提供安裝和移除 Kaspersky Embedded Systems Security 2.2 的逐步說明。

本章內容

Kaspersky Embedded Systems Security 2.2 軟體元件及對應的 Windows Installer 服務代碼

預設情況下，\server\ess_x86(x64).msi 檔案會安裝所有 Kaspersky Embedded Systems Security 2.2 元件。您可透過在自訂安裝中包含此元件來安裝它。

\client\esstools_x86(x64).msi 檔案安裝“管理工具”集內所有的軟體元件。

以下各節列出 Kaspersky Embedded Systems Security 2.2 元件在 Windows Installer 服務中對應的代碼。透過命令列安裝 Kaspersky Embedded Systems Security 2.2 時，可使用這些代碼來定義要安裝的元件清單。

本章節說明項目

Kaspersky Embedded Systems Security 2.2 軟體元件

下表含有 Kaspersky Embedded Systems Security 2.2 軟體元件的代碼和說明。

步驟 3. Kaspersky Embedded Systems Security 2.2 軟體元件的說明

元件	代碼	執行功能
基本功能	Core	此元件包含基本應用程式功能集合並確保其操作。
應用程式啟動控制	AppCtrl	此元件監控使用者執行應用程式的嘗試，並根據設定的應用程式啟動控制規則來允許或拒絕這些應用程式啟動。 它在“應用程式啟動控制”工作中執行。
裝置控制	DevCtrl	此元件跟蹤將 USB 大容量儲存器連線到受防護電腦的嘗試，並根據指定的裝置控制規則來允許或拒絕這些裝置的使用。 該元件在“裝置控制”工作中實施。
病毒防護	AVProtection	此元件確保病毒防護並包含以下元件： • 自訂掃描 • 即時檔案防護
自訂掃描	Ods	此元件安裝 Kaspersky Embedded Systems Security 2.2 系統檔案和自訂掃描工作（依要求掃描受防護電腦的物件）。 如果您從命令列安裝 Kaspersky Embedded Systems Security 2.2 時，指定其他 Kaspersky Embedded Systems Security 2.2 元件，但未指定 Core 元件，將自動安裝 Core 元件。
即時檔案防護	Oas	此元件在受防護電腦上的檔案被存取時對這些檔案執行病毒防護掃描。 其執行“即時檔案防護”工作。
使用卡巴斯基安全網路	Ksn	此元件根據 Kaspersky Lab 雲端技術提供防護。 它執行“KSN 使用”工作（向卡巴斯基安全網路服務傳送請求及從該服務接收結論）。
檔案完整性監控	Fim	此元件可記錄指定監控範圍內針對檔案執行的操作。 該元件執行檔案完整性監控工作。
弱點利用防禦	AntiExploit	此元件可管理設定，以便防護受防護電腦記憶體中的處理程序所使用的記憶體。
防火牆管理	Firewall	此元件可透過 Kaspersky Embedded Systems Security 2.2 圖形化使用者介面來管理 Windows 防火牆。 關於防火牆管理工作。
整合卡巴斯基安全管理中心網路代理模組	AKIntegration	建立 Kaspersky Embedded Systems Security 2.2 與卡巴斯基安全管理中心網路代理程式的連線。 如果想透過卡巴斯基安全管理中心管理應用程式，請在受防護電腦上安裝此元件。

元件	代碼	執行功能
記錄審查	LogInspector	此元件根據 Windows 事件記錄的審查結果，對受防護環境的完整性進行監控。
“系統監控器”效能計數器群組。	PerfMonCounters	此元件可安裝一組系統監控效能計數器。效能計數器可用來衡量 Kaspersky Embedded Systems Security 2.2 的效能，並在使用 Kaspersky Embedded Systems Security 2.2 與其他程式時找出電腦上的潛在影響。
SNMP 計數器與 TRAP	SnmpSupport	此元件可透過 Microsoft Windows 中的簡單網路管理通訊協定 (SNMP) 發佈 Kaspersky Embedded Systems Security 2.2 計數器與 TRAP。只有受防護電腦上安裝了 Microsoft SNMP 時，才能在同一電腦上安裝此元件。
工作列通知區域中的 Kaspersky Embedded Systems Security 2.2 圖示	TrayApp	此元件在受防護電腦的工作列通知區域顯示 Kaspersky Embedded Systems Security 2.2 圖示。Kaspersky Embedded Systems Security 2.2 圖示顯示電腦防護的狀態，可以用於在 Microsoft 管理主控台（如果已安裝）和“**關於本應用程式**”視窗中開啟 Kaspersky Embedded Systems Security 2.2 主控台。
命令列實用工具	Shell	可透過受防護電腦的命令列管理 Kaspersky Embedded Systems Security 2.2。

軟體元件的“管理工具”集

下表含有“管理工具”集軟體元件的代碼及說明。

步驟 4.　“管理工具”軟體元件說明

元件	代碼	元件功能
Kaspersky Embedded Systems Security 2.2 嵌入式管理	MmcSnapin	此元件透過 Kaspersky Embedded Systems Security 2.2 主控台安裝 Microsoft 管理主控台管理單元。 如果您透過命令列安裝管理工具時，指定其他元件，但未指定 MmcSnapin 元件，將自動安裝此元件。
說明	Help	.chm 說明檔案，儲存在 Kaspersky Embedded Systems Security 2.2 管理工具檔案資料夾中。您可以使用“**開始**”功能表或透過在應用程式主控台視窗處於開啟狀態時按 **F1** 鍵，來開啟說明檔案。
文件	Help	Kaspersky Embedded Systems Security 2.2 新增了 Kaspersky Lab Web 資源的捷徑，其中提供了 PDF 格式的《管理手冊》和《使用者手冊》。該捷徑在“開始”功能表中提供。

安裝 Kaspersky Embedded Systems Security 2.2 後系統的變更

當 Kaspersky Embedded Systems Security 2.2 和應用程式主控台（“管理工具”集）同時安裝時，Windows Installer 服務將對受防護電腦進行以下變更：

- 在受防護電腦和安裝了應用程式主控台的電腦上建立 Kaspersky Embedded Systems Security 2.2 資料夾。
- 註冊 Kaspersky Embedded Systems Security 2.2 服務。
- 建立 Kaspersky Embedded Systems Security 2.2 使用者群組。
- 在系統登錄檔中註冊 Kaspersky Embedded Systems Security 2.2 機碼。

這些變更在下表說明。

Kaspersky Embedded Systems Security 2.2 資料夾

步驟 5. 受防護電腦上的 Kaspersky Embedded Systems Security 2.2 資料夾

資料夾	Kaspersky Embedded Systems Security 2.2 檔案
Kaspersky Embedded Systems Security 2.2 預設安裝資料夾： 在 Microsoft Windows 32 位元版本中 – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\ 在 Microsoft Windows 64 位元版本中 – %ProgramFiles(x86)%\Kaspersky Embedded Systems Security\	Kaspersky Embedded Systems Security 2.2 可執行檔（安裝期間指定的目的資料夾）。
%Kaspersky Embedded Systems Security%\mibs 資料夾	管理資訊庫 (MIB) 檔案，這些檔案包含 Kaspersky Embedded Systems Security 2.2 透過 SNMP 通訊協定發佈的計數器與 TRAP 說明。
%Kaspersky Embedded Systems Security%\x64 資料夾	64 位元版本 Kaspersky Embedded Systems Security 2.2 可執行檔（將僅在 64 位元版本 Microsoft Windows 中安裝 Kaspersky Embedded Systems Security 2.2 的過程中建立該資料夾）。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Data\ ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Embedded Systems Security\2.2\Dskm\	Kaspersky Embedded Systems Security 2.2 服務檔案。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\	更新來源設定檔。

資料夾	Kaspersky Embedded Systems Security 2.2 檔案
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\Distribution\	使用“複製更新”工作下載的資料庫和軟體模組更新（在第一次使用“複製更新”工作下載更新時會建立此資料夾）。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Reports\	工作記錄和系統稽核記錄。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Current\	目前使用的資料庫。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Backup\	資料庫的備份副本；每次更新資料庫時將會覆寫。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Temp\	執行更新工作時所建立的暫存檔。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Quarantine\	隔離的物件（預設資料夾）。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Backup\	備份中的物件（預設資料夾）。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored\	從備份儲存和隔離還原的物件（還原物件的預設資料夾）。

步驟 6. 在應用程式主控台安裝過程中建立的資料夾

資料夾	Kaspersky Embedded Systems Security 2.2 主控台檔案
應用程式主控台預設安裝資料夾： • 在 Microsoft Windows 32 位元版本中 – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ • 在 Microsoft Windows 64 位元版本中 – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\	“管理工具”檔案（安裝 Kaspersky Embedded Systems Security 2.2 主控台時指定的目的資料夾）。

Kaspersky Embedded Systems Security 2.2 服務

使用“本機系統 (SYSTEM)”帳戶啟動 Kaspersky Embedded Systems Security 2.2 服務。

步驟 7. Kaspersky Embedded Systems Security 2.2 服務

服務	用途
Kaspersky Security 服務 (KAVFS)	管理 Kaspersky Embedded Systems Security 2.2 工作和工作流的基本 Kaspersky Embedded Systems Security 2.2 服務。
Kaspersky Security 管理服務 (KAVFSGT)	此服務用於透過應用程式主控台進行 Kaspersky Embedded Systems Security 2.2 應用程式管理。

Kaspersky Embedded Systems Security 2.2 群組

步驟 8. Kaspersky Embedded Systems Security 2.2 群組

群組	用途
ESS 管理員	受防護電腦上的一個群組，其中的使用者有權存取 Kaspersky Security 管理服務和 Kaspersky Embedded Systems Security 2.2 所有的功能。

系統登錄註冊參數

步驟 9. 系統登錄註冊參數

機碼	用途
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Kaspersky Embedded Systems Security 2.2 服務內容。
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Kaspersky Embedded Systems Security 2.2 事件記錄設定（Kaspersky 事件記錄）。
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Kaspersky Embedded Systems Security 2.2 管理服務內容。

機碼	用途
Microsoft Windows 32 位元版本： [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] 在 Microsoft Windows 64 位元版本中： [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]。	效能計數器設定。
Microsoft Windows 32 位元版本： [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\SnmpAgent] 在 Microsoft Windows 64 位元版本中： [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\SnmpAgent]	SNMP 協定支援元件設定。
Microsoft Windows 32 位元版本： [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\CrashDump] 在 Microsoft Windows 64 位元版本中： [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\CrashDump]	Dump 檔案寫設定。
Microsoft Windows 32 位元版本： [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\Trace] 在 Microsoft Windows 64 位元版本中： [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Trace]	偵錯檔案設定。
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Environment]	應用程式的工作和功能的配置。

Kaspersky Embedded Systems Security 2.2 處理程序

Kaspersky Embedded Systems Security 2.2 將啟動下表中敘述的處理程序。

步驟 10. Kaspersky Embedded Systems Security 2.2 處理程序

檔案名稱	用途
kavfswp.exe	Kaspersky Embedded Systems Security 2.2 工作流
kavtray.exe	系統欄圖示的處理程序
kavshell.exe	命令列實用工具處理程序
kavfsrcn.exe	Kaspersky Embedded Systems Security 2.2 遠端管理處理程序
kavfs.exe	Kaspersky Security 服務處理程序
kavfsgt.exe	Kaspersky Security 管理服務處理程序
kavfswh.exe	Kaspersky Security 弱點利用防禦服務處理程序

Windows Installer 服務的安裝和移除設定及命令列選項

下表包含安裝和移除 Kaspersky Embedded Systems Security 2.2 的參數說明和預設值，以及變更 Kaspersky Embedded Systems Security 安裝參數值及可變動參數。透過命令列安裝 Kaspersky Embedded Systems Security 2.2 時，您可以使用參數及 Windows Installer 服務中 msiexec 指令適用的標準指令。

步驟 11. Windows Installer 中的安裝參數和命令列選項

設定	Windows Installer 命令列選項及其可能值	預設值	敘述
接受最終使用者產品授權協議條款	EULA=<設定值> 0 – 不同意接受最終使用者產品授權協議條款。 1 – 同意接受最終使用者產品授權協議條款。	0	您必須接受使用者產品授權協議條款，才能安裝 Kaspersky Embedded Systems Security 2.2。
接受隱私政策條款	PRIVACYPOLICY=<值> 0 – 拒絕隱私政策條款。 1 – 接受隱私政策條款。	0	您必須接受隱私政策條款，才能安裝 Kaspersky Embedded Systems Security 2.2。
目的資料夾	INSTALLDIR=<資料夾完整路徑>	Kaspersky Embedded Systems Security 2.2: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security 管理工具：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools 在 x64 位元版本的 Microsoft Windows 中 :%ProgramFiles(x86)%。	安裝過程中將儲存在 Kaspersky Embedded Systems Security 2.2 檔案的資料夾。 您可指定不同的資料夾。
Kaspersky Embedded Systems Security 2.2 啟動時啟動即時檔案防護工作（**安裝應用程式後啟用即時防護**）	RUNRTP=<設定值> 1 – 啟動； 0 – 不啟動。	1	開啟該設定，在 Kaspersky Embedded Systems Security 2.2 啟動時啟動即時檔案防護（建議）。

設定	Windows Installer 命令列選項及其可能值	預設值	敘述
Microsoft Corporation 建議的掃描排除項目（**將 Microsoft 建議的檔案新增到排除清單**）	ADDMSEXCLUSION=<設定值> 1 – 排除； 0 – 不排除。	1	在“即時檔案防護”範圍中排除 Microsoft Corporation 建議排除的電腦上的物件。 當防毒應用程式攔截或修改檔案時，電腦上某些應用程式可能變得較不穩定。例如，當 Microsoft Corporation 將某些網域控制站應用程式納入此類物件清單時。
根據 Kaspersky Lab 建議從掃描範圍中排除的物件（**將 Kaspersky Lab 建議的檔案新增到排除清單**）	ADDKLEXCLUSION=<設定值> 1 – 排除； 0 – 不排除。	1	在“即時檔案防護”範圍中排除 Kaspersky Lab 建議排除的電腦上的物件。
允許遠端連線到應用程式主控台。	ALLOWREMOTECON=<值> 1 – 允許； 0 – 拒絕。	0	預設情況下，不允許遠端連線到安裝在受防護電腦上的應用程式主控台。安裝過程中，可允許連線。Kaspersky Embedded Systems Security 2.2 針對所有連接埠使用 TCP 協定為處理程序 kavfsgt.exe 建立允許規則。
金鑰檔案的路徑（**金鑰**）	LICENSEKEYPATH=<金鑰檔案名稱>	分發工具套件中的 \product 目錄	預設情況下，安裝程式會嘗試尋找分發套件的 \product 資料夾中是否有副檔名為 .key 的檔案。 如果 \product 資料夾包含多個金鑰檔案，安裝程式將選擇到期日期最晚的金鑰檔案。 您可預先將金鑰檔案儲存在 \product 資料夾中，或使用“**新增金鑰**”設定指定另一個檔案路徑。

設定	Windows Installer 命令列選項及其可能值	預設值	敘述
			您可以在安裝 Kaspersky Embedded Systems Security 2.2 後使用所選的管理工具（例如，應用程式主控台）新增金鑰。如果您在應用程式安裝期間未新增金鑰，Kaspersky Embedded Systems Security 2.2 將不會發揮功能。
設定檔路徑	CONFIGPATH=<設定檔名稱>	未指定	Kaspersky Embedded Systems Security 2.2 從在應用程式中建立的指定設定檔匯入設定。 Kaspersky Embedded Systems Security 2.2 無法從設定檔匯入密碼，例如，用來啟動工作的帳戶密碼或用來連線代理伺服器的密碼。一旦匯入設定，將需手動輸入所有密碼。 如果未指定設定檔，安裝後應用程式將開始使用預設設定。

設定	Windows Installer 命令列選項及其可能值	預設值	敘述
啟用主控台的網路連線	ADDWFEXCLUSION=<設定值> **1** – 允許； **0** – 拒絕。	0	使用該選項在另一台電腦上安裝 Kaspersky Embedded Systems Security 2.2。您可以從安裝了 Kaspersky Embedded Systems Security 2.2 主控台的另一台裝置遠端管理電腦防護。 在 Microsoft Windows 防火牆中開啟連接埠 135 (TCP)，允許透過網路連線 Kaspersky Embedded Systems Security 2.2 遠端管理的執行檔 kavfsrcn.exe，并允許存取 DCOM 應用程式。 安裝完成後，將使用者新增到“ESS 管理員”群組中，以允許他們遠端管理應用程式，並允許透過網路連線到電腦上的 Kaspersky Security 管理服務（kavfsgt.exe 檔案）。 您可以閱讀有關 Kaspersky Embedded Systems Security 2.2 主控台安裝到其他電腦上時的附加配置的詳細資訊（請參見第 39 頁上的“在其他電腦上安裝應用程式主控台以後的進階設定”部分）。
停用不相容軟體檢查	SKIPINCOMPATIBLESW=<值> 0 – 不相容軟體檢查已執行 1 – 不相容軟體檢查未執行	0	使用此設定可在應用程式在裝置上進行背景安裝過程中，啟用或停用不相容軟體檢查。 在 Kaspersky Embedded Systems Security 2.2 安裝過程中，無論此設定的值如何，應用程式將始終對已安裝在裝置上的其他版本的應用程式發出警告。

步驟 12. Windows Installer 中的移除設定和命令列選項

設定	Windows Installer 命令列選項及其可能值	預設值
還原隔離的物件	RESTOREQTN=<設定值> **0** – 刪除隔離內容； **1** – 將隔離內容還原到 RESTOREPATH 參數所指定的資料夾的 \Quarantine 子資料夾中。	0 – 刪除
還原備份儲存區內容	RESTOREBCK=<設定值> **0** – 刪除備份內容； **1** – 將備份內容還原到 RESTOREPATH 參數所指定的資料夾 \Backup 子資料夾中。	0 – 刪除
輸入目前密碼以確認刪除（如果已啟用密碼防護）	UNLOCK_PASSWORD=<指定的密碼>	未指定
還原物件的資料夾	RESTOREPATH=<資料夾完整路徑> 還原的物件將儲存到指定的資料夾。	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored

Kaspersky Embedded Systems Security 2.2 安裝和移除記錄

如果您透過安裝/移除精靈來安裝或移除 Kaspersky Embedded Systems Security 2.2，Windows Installer 服務會建立一個安裝（移除）記錄。ess_install_<uid>.log 記錄檔案（其中 <uid> 是八個字元的唯一記錄識別碼）將儲存在啟動 setup.exe 檔案之使用者帳戶下的 %temp% 資料夾中。

如果從“**開始**”功能表執行應用程式主控台或 Kaspersky Embedded Systems Security 2.2 的“**修改或移除**”選項，將在 %temp% 資料夾中自動建立 ess_2.2_maintenance.log。

預設情況下，若您是從命令列安裝或移除 Kaspersky Embedded Systems Security 2.2，就不會建立該安裝檔案記錄。

► *要安裝 Kaspersky Embedded Systems Security 2.2 並在磁碟 C:\ 上建立記錄檔案：*

- 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

安裝排程

本節包含 Kaspersky Embedded Systems Security 2.2 管理工具集的說明以及 Kaspersky Embedded Systems Security 2.2 安裝和移除的特殊方面：使用精靈（請參見第 35 頁上的“使用精靈安裝和移除應用程式”部分）、命令列（請參見第 46 頁上的“從命令列安裝和移除應用程式”部分）、透過卡巴斯基安全管理中心（請參見第 51 頁上的“使用卡巴斯基安全管理中心安裝和移除應用程式”部分）以及透過 Active Directory® 群組政策（請參見第 55 頁上的“透過 Active Directory 群組政策安裝和移除”部分）。

在您開始安裝 Kaspersky Embedded Systems Security 2.2 之前，請先規劃它的安裝排程。

1. 確定您要用來管理 Kaspersky Embedded Systems Security 2.2 及其設定的管理工具。
2. 選擇必須安裝的應用程式元件（請參閱第 21 頁上的“Kaspersky Embedded Systems Security 2.2 軟體元件以及它們在 Windows Installer 服務中對應的代碼”部分）。
3. 選擇安裝方式。

本章節說明項目

選擇管理工具

決定要用來設定及管理 Kaspersky Embedded Systems Security 2.2 的管理工具。可以使用應用程式主控台、命令列實用工具和卡巴斯基安全管理中心管理主控台管理 Kaspersky Embedded Systems Security 2.2。

Kaspersky Embedded Systems Security 2.2 主控台

Kaspersky Embedded Systems Security 2.2 主控台是新增到 Microsoft 管理主控台的獨立管理元件。您可以透過安裝在受防護電腦或公司網路中其他電腦上的應用程式主控台來管理 Kaspersky Embedded Systems Security 2.2。

您可以將多個 Kaspersky Embedded Systems Security 2.2 管理單元新增到在作者模式下開啟的 Microsoft 管理控制台的單個副本中，以便用它來管理多台已安裝 Kaspersky Embedded Systems Security 2.2 的電腦的防護。

應用程式主控台含在“管理工具”應用程式元件集內。

命令列實用工具

您可透過受防護電腦的命令列來管理 Kaspersky Embedded Systems Security 2.2。

命令列實用工具含在 Kaspersky Embedded Systems Security 2.2 軟體元件集中。

卡巴斯基安全管理中心

若您為了集中管理公司電腦的病毒防護工作而使用卡巴斯基安全管理中心，您可使用卡巴斯基安全管理中心的管理主控台來管理 Kaspersky Embedded Systems Security 2.2。

必須安裝下列元件：

- **整合卡巴斯基安全管理中心網路代理模組**。此模組含在 Kaspersky Embedded Systems Security 2.2 的軟體元件中。它可確保 Kaspersky Embedded Systems Security 2.2 與網路代理的通信。請在受防護電腦上安裝與卡巴斯基安全管理中心網路代理程式整合的模組。
- **卡巴斯基安全管理中心網路代理**。請在每一台受防護電腦上安裝此元件。該元件支援電腦上安裝的 Kaspersky Embedded Systems Security 2.2 與卡巴斯基安全管理中心管理主控台之間的互動。網路代理程式安裝檔案包含在卡巴斯基安全管理中心的分發套件資料夾中。
- **Kaspersky Embedded Systems Security 2.2 管理外掛程式**。此外，安裝該外掛程式，以在安裝了卡巴斯基安全管理中心管理伺服器的電腦上透過管理主控台管理 Kaspersky Embedded Systems Security 2.2。此外掛程式透過卡巴斯基安全管理中心來管理應用程式。管理外掛程式安裝檔案 \product\klcfginst.exe 包含在 Kaspersky Embedded Systems Security 2.2 分發套件中。

選擇安裝類型

指定 Kaspersky Embedded Systems Security 2.2 安裝的軟體元件後（請參閱第 21 頁上的“Kaspersky Embedded Systems Security 2.2 軟體元件以及它們在 Windows Installer 服務中對應的代碼”部分），您需要選擇應用程式安裝方法。

根據網路架構並參考下列情況選擇安裝方法：

- 將需要設定特殊的 Kaspersky Embedded Systems Security 2.2 安裝設定，還是將使用建議的安裝設定（請參見第 28 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）。
- 所有電腦的安裝設定均相同，還是每台電腦使用特定的安裝設定。

使用者可使用背景模式在命令列指定適當的安裝設定，或利用互動式安裝精靈安裝 Kaspersky Embedded Systems Security 2.2。您可使用 Active Directory 群組政策或卡巴斯基安全管理中心遠端安裝工作，以遠端方式統一安裝 Kaspersky Embedded Systems Security 2.2。

Kaspersky Embedded Systems Security 2.2 可以安裝在單台電腦上，對執行及其儲存到設定檔中的設定進行配置；建立的檔案可以用於在其他電腦上安裝 Kaspersky Embedded Systems Security 2.2（使用 Active Directory 群組政策安裝該應用程式時，這種情況不適用）。

啟動安裝精靈

您可使用安裝精靈安裝下列內容：

- 將 Kaspersky Embedded Systems Security 2.2 元件（請參加第 22 頁上的“Kaspersky Embedded Systems Security 2.2 軟體元件”部分）從分發套件中包含的 \product\setup.exe 檔案安裝到受防護電腦上。
- 將 Kaspersky Embedded Systems Security 2.2 主控台（請參見第 38 頁上的“Kaspersky Embedded Systems Security 2.2 主控台安裝”部分）從安裝套件的 \client\setup.exe 檔案安裝到受防護電腦或其他 LAN 主機上。

透過命令列使用必要的安裝設定來啟動安裝套件檔案

如果不以任何命令列選項啟動安裝套件檔案，則 Kaspersky Embedded Systems Security 2.2 將以預設設定安裝。可以使用 Kaspersky Embedded Systems Security 2.2 選項修改安裝設定。

應用程式主控台可以安裝在受防護電腦和/或管理員工作站上。

您還可以使用示例指令安裝 Kaspersky Embedded Systems Security 2.2 和應用程式主控台（請參見第 46 頁上的“從命令列安裝和移除應用程式”部分）。

透過卡巴斯基安全管理中心集中安裝

如果卡巴斯基安全管理中心在您的網路中的用途是管理網路電腦的病毒防護，則可以透過執行卡巴斯基安全管理中心遠端安裝工作，在多台電腦上安裝 Kaspersky Embedded Systems Security 2.2。

您希望透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security 2.2（請參見第 51 頁上的“使用卡巴斯基安全管理中心安裝和移除應用程式”部分）的電腦可以與卡巴斯基安全管理中心位於同一網域中，也可以在不同的網域中，或完全不屬於任何一個網域。

使用 Active Directory 群組政策集中安裝

您可使用 Active Directory 群組政策在受防護電腦上安裝 Kaspersky Embedded Systems Security 2.2。應用程式主控台可以安裝在受防護電腦或管理員工作站上。

您可使用預設的安裝設定安裝 Kaspersky Embedded Systems Security 2.2。

使用 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security 2.2（請參見第 55 頁上的“透過 Active Directory 群組政策安裝和移除”部分）的電腦必須位於相同網域和相同的組織單元中。安裝作業會在電腦啟動，登入 Microsoft Windows 之前執行。

基於精靈安裝和移除應用程式

本節包含透過安裝精靈進行 Kaspersky Embedded Systems Security 2.2 和應用程式主控台安裝和移除的說明，以及有關在安裝時要執行的其他 Kaspersky Embedded Systems Security 2.2 配置和操作的資訊。

本章節說明項目

使用安裝精靈進行安裝

以下各節包含有關安裝 Kaspersky Embedded Systems Security 2.2 和應用程式主控台的資訊。

► *若要安裝及使用 Kaspersky Embedded Systems Security 2.2 服務，請執行以下步驟：*

1. 在受防護電腦上安裝 Kaspersky Embedded Systems Security 2.2。
2. 在您打算用來管理 Kaspersky Embedded Systems Security 2.2 的電腦上安裝應用程式主控台。
3. 如果應用程式主控台已經安裝在網路中的其他電腦上，而不是安裝在受防護電腦上，請執行額外調整以允許應用程式主控台使用者遠端管理 Kaspersky Embedded Systems Security 2.2。
4. 在安裝 Kaspersky Embedded Systems Security 2.2 後執行操作。

本章節說明項目

Kaspersky Embedded Systems Security 2.2 安裝

在安裝 Kaspersky Embedded Systems Security 2.2 前，請執行以下步驟：

- 確認電腦上未安裝任何防毒程式。
- 確認用來啟動安裝精靈的帳戶已註冊到受防護電腦上的管理員群組中。

完成上述操作後，繼續安裝程式。依照安裝精靈的指示，指定安裝 Kaspersky Embedded Systems Security 2.2 的設定。您可在任何安裝步驟停止 Kaspersky Embedded Systems Security 2.2 安裝程式。若要停止安裝，請在安裝精靈視窗中點擊“**取消**”。

您可閱讀更多有關安裝（移除）設定的詳細資訊（請參閱第 28 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）。

► *使用安裝精靈安裝 Kaspersky Embedded Systems Security 2.2：*

1. 在電腦上啟動歡迎檔案 setup.exe。
2. 在開啟的視窗中的“**安裝**”部分，點擊“**安裝 Kaspersky Embedded Systems Security 2.2**”連結。
3. 在 Kaspersky Embedded Systems Security 2.2 安裝精靈的歡迎頁面，點擊“**下一步**”按鈕。

   將開啟“**EULA 和隱私政策**”視窗。
4. 檢視產品授權協議和隱私政策的條款。

5. 如果您同意 EULA 和隱私政策的條款和條件，請選中“**此 EULA 的條款和條件**”和“**描述資料處理的隱私政策**”核取方塊以繼續安裝。

   如果您不接受 EULA 和/或隱私政策，則終止安裝。

6. 點擊“**下一步**”按鈕。

   將開啟“**自訂安裝**”視窗。

7. 選擇要安裝的元件。

   預設情況下，建議安裝集包括除“防火牆管理”元件外的所有 Kaspersky Embedded Systems Security 2.2 元件。

   只有在電腦安裝了 Microsoft Windows SNMP 服務的情況下，建議的安裝元件清單中才會出現 Kaspersky Embedded Systems Security 2.2 的“SNMP 協定支援”元件。

8. 要取消所有變更，請從“**自訂安裝**”視窗中點擊“**重設**”按鈕。點擊“**下一步**”按鈕。
9. 在“**選擇目的資料夾**”視窗中：
   - 如有需要，請指定另一個 Kaspersky Embedded Systems Security 2.2 副本檔案要放置的資料夾位置。
   - 如果需要，點擊“**磁碟**”按鈕檢視有關本地磁碟機上可用空間的資訊。

   點擊“**下一步**”按鈕。
10. 在“**進階安裝設定**”視窗中，配置以下安裝設定：
    - **安裝應用程式後啟用即時防護**。
    - **將 Microsoft 建議的檔案新增到排除清單**。
    - **將 Kaspersky Lab 建議的檔案新增到排除清單**。

      點擊“**下一步**”按鈕。
11. 在開啟的“**從設定檔匯入設定**”視窗中：
    a. 指定設定檔以從在任何先前相容版本的應用程式中建立的現有設定檔匯入 Kaspersky Embedded Systems Security 2.2 設定。
    b. 點擊“**下一步**”按鈕。
12. 在“**啟動應用程式**”視窗中，執行下列操作之一：
    - 如果您想要啟動應用程式，請指定 Kaspersky Embedded Systems Security 2.2 金鑰檔案以啟動應用程式。
    - 如果您想要稍後啟動應用程式，請點擊“**下一步**”按鈕。
    - 如果您之前將授金鑰案儲存在發行套件的 \server 資料夾中，該檔案的名稱將會在“**金鑰**”欄位中出現。

      若要使用儲存在其他資料夾的金鑰檔案新增金鑰，請指定金鑰檔案。

      新增金鑰檔案後，視窗中將顯示授權資訊。Kaspersky Embedded Systems Security 2.2 會顯示經過計算的授權到期日。此日期自啟用金鑰開始計算，並於金鑰檔案的“有效期間”到期前結束。

      點擊“**下一步**”按鈕在應用程式中套用金鑰。

13. 在“**已準備安裝**”視窗中按“**安裝**”按鈕。精靈將開始安裝 Kaspersky Embedded Systems Security 2.2 元件。
14. 完成安裝時，會開啟“**安裝完成**”視窗。
15. 選取“**檢視發佈說明**”核取方塊，可於安裝精靈完成安裝時檢視發佈資訊。
16. 點擊“**確定**”。

將關閉“安裝精靈”視窗。完成安裝時，如果已新增啟動金鑰，即可使用 Kaspersky Embedded Systems Security 2.2。

Kaspersky Embedded Systems Security 2.2 主控台安裝

依照安裝精靈說明調整應用程式主控台的安裝設定。您可於安裝精靈的任何一個步驟停止安裝程序。若要停止安裝，請在安裝精靈視窗中點擊“**取消**”按鈕。

► *若要安裝應用程式主控台，請執行以下步驟：*

1. 確認執行安裝精靈的帳戶，已加入電腦管理員群組中。
2. 在電腦上執行歡迎檔案 setup.exe。

   隨即會開啟一個歡迎安裝程式視窗。
3. 點擊“**安裝 Kaspersky Embedded Systems Security 2.2 主控台**”連結。

   隨即會開啟“安裝精靈”歡迎視窗。點擊“**下一步**”按鈕。
4. 在開啟的視窗中檢視最終使用者產品授權協議和隱私政策的條款，並選擇**此 EULA 的條款和條件**和**描述資料處理的隱私政策**，以繼續安裝。點擊“**下一步**”按鈕。

   將開啟“**進階安裝設定**”視窗。
5. 在“**進階安裝設定**”視窗中：
   - 如果希望使用應用程式主控台管理遠端電腦上安裝的 Kaspersky Embedded Systems Security 2.2，請選中“**允許遠端存取**”核取方塊。
   - 將開啟“**自訂安裝**”視窗並選擇元件：
     a. 點擊“**進階**”按鈕。

        將開啟“**自訂安裝**”視窗。
     b. 從清單中選擇“管理工具”集的元件。

        預設情況下，安裝所有元件。
     c. 點擊“**下一步**”按鈕。

> 您可以找到有關 Kaspersky Embedded Systems Security 2.2 軟體元件的更多詳細資訊（請參閱第 21 頁上的“Kaspersky Embedded Systems Security 2.2 軟體元件以及它們在 Windows Installer 服務中對應的代碼”部分）。

6. 在“**選擇目的資料夾**”視窗中：
   a. 如有需要，可指定一個不同的資料夾來儲存安裝檔案。
   b. 點擊“**下一步**”按鈕。
7. 在“**已準備安裝**”視窗中按“**安裝**”按鈕。

   該精靈將開始安裝所選的元件。
8. 點擊“**確定**”。

將關閉“安裝精靈”視窗。將在受防護電腦上安裝應用程式主控台。

如果“管理工具”集已經安裝在網路中的其他電腦上，而不是安裝在受防護電腦上，請調整“進階設定”（請參閱第 39 頁上的“在其他電腦上安裝應用程式主控台以後的進階設定”部分）。

在其他電腦上安裝應用程式主控台以後的進階設定

如果應用程式主控台已經安裝在其他電腦上，而不是安裝在受防護電腦上，請執行下述操作，以允許使用者遠端管理 Kaspersky Embedded Systems Security 2.2：

- 在受防護的電腦上將 Kaspersky Embedded Systems Security 2.2 使用者新增到 ESS 管理員群組中。
- 如果受防護電腦使用 Windows 防火牆或協力廠商防火牆，則允許 Kaspersky Security 管理服務 (kavfsgt.exe) 進行網路連線（請參見第 73 頁上的“關於 Kaspersky Security 管理服務的存取權限”部分）。
- 如果在執行 Microsoft Windows 的電腦上安裝應用程式主控台期間未選中“**允許遠端存取**”核取方塊，則應該透過電腦的防火牆手動允許應用程式主控台的網路連線。

允許應用程式主控台的網路連線

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

遠端電腦上的應用程式主控台將使用 DCOM 協定從受防護電腦上的 Kaspersky Security 管理服務接收關於 Kaspersky Embedded Systems Security 2.2 事件的資訊（如物件掃描、工作完成等）。需要在“Windows 防火牆設定”中允許應用程式主控台的網路連線，才能在應用程式主控台和 Kaspersky Security 管理服務之間建立連線。

在安裝了應用程式主控台的遠端電腦上，執行以下操作：

- 確保允許遠端匿名存取 COM 應用程式（但不是遠端啟動和啟動 COM 應用程式）。
- 在 Windows 防火牆上開啟 TCP 連接埠 135 並允許 Kaspersky Embedded Systems Security 2.2 遠端管理處理程序的可執行檔 kavfsrcn.exe 的網路連線。

  安裝應用程式主控台的用戶端電腦將使用連接埠 TCP 135 存取受防護電腦並接收回應。
- 設定 Windows 防火牆輸出規則以允許連線。

  與單個協定具有固定連接埠的傳統 TCP/IP 和 UDP/IP 服務不同，DCOM 會為其遠端連線的 COM 物件動態分配連接埠。如果用戶端（其中安裝了應用程式主控台）與 DCOM 端點（受防護伺服器）之間存在防火牆，應開放很大範圍的連接埠。

設定任何其他軟體或硬體防火牆應該套用相同步驟。

如果在配置受防護電腦與已安裝應用程式主控台電腦之間的連線時應用程式主控台已經開啟，則關閉應用程式主控台，等待 Kaspersky Embedded Systems Security 2.2 遠端管理處理程序 kavfsrcn.exe 結束，然後再重新啟動應用程式主控台。已套用新的連線設定。

► *為了允許匿名遠端存取 COM 應用程式，請執行以下步驟：*

1. 在安裝了 Kaspersky Embedded Systems Security 2.2 主控台的遠端電腦上，開啟元件服務主控台。
2. 選擇“**開始** > **執行**”。
3. 輸入指令 dcomcnfg。
4. 點擊“**確定**”。
5. 展開電腦上**元件服務主控台**中的“**電腦**”節點。
6. 開啟“**我的電腦**”節點的內容功能表。
7. 選擇“**內容**”。
8. 在“**內容**”視窗的“**COM 安全**”標籤上，點擊“**存取權限**”設定群組中的“**編輯限制**”按鈕。
9. 請確認在“**允許遠端存取**”視窗中為“匿名登入”使用者選定“**允許遠端存取**”的核取方塊。
10. 點擊“**確定**”。

► *在 Windows 防火牆中的連接埠 TCP 135 並允許 Kaspersky Embedded Systems Security 2.2 遠端管理處理程序的可執行檔的網路連線：*

1. 關閉遠端電腦上的 Kaspersky Embedded Systems Security 2.2 主控台。
2. 執行以下步驟之一：
   - 在 Microsoft Windows XP 或 Microsoft Windows Vista® 中：
     a. 在 Microsoft Windows XP SP2 或以上版本中，選擇“**開始**”→“**Windows 防火牆**”。

        在 Microsoft Windows Vista 中，選擇“**開始**”→“**主控台**”→“**Windows 防火牆**”，然後在“**Windows 防火牆**”視窗中選擇指令“**變更設定**”。
     b. 在“Windows 防火牆”視窗（或“Windows 防火牆設定”）中點擊“**排除**”選項上的“**新增連接埠**”按鈕。
     c. 在“**名稱**”欄位中指定連接埠名稱 RPC (TCP/135) 或輸入其他名稱，例如“Kaspersky Embedded Systems Security 2.2 DCOM”，並在“**連接埠名稱**”欄位中指定連接埠號 (135)。
     d. 選擇“**TCP**”協定。
     e. 點擊“**確定**”。
     f. 點擊“**排除**”標籤上的“**新增**”按鈕。
   - 在 Microsoft Windows 7 或更高版本中：
     a. 選擇“**開始** > **控制台** > **Windows 防火牆**”。
     b. 在“**Windows 防火牆**”視窗中，選擇“**允許程式或功能透過 Windows 防火牆**”。
     c. 在“**允許程式透過 Windows 防火牆通訊**”視窗中點擊“**允許其他程式...**”按鈕。

3. 在“**新增程式**”視窗中指定 kavfsrcn.exe 檔案。該檔案位於在使用 Microsoft 管理主控台安裝 Kaspersky Embedded Systems Security 2.2 主控台的過程中指定的目的資料夾中。
4. 點擊“**確定**”。
5. 在“**Windows 防火牆（Windows 防火牆設定）**”視窗中，點擊“**確定**”按鈕。

► *新增 Windows 防火牆輸出規則：*

1. 選擇“**開始** > **控制台** > **Windows 防火牆**”。
2. 在“**Windows 防火牆**”視窗中，點擊“**進階設定**”連結。

   將開啟“**進階安全 Windows 防火牆**”視窗。
3. 選擇“**輸出規則**”子節點。
4. 在“**操作**”窗格中點擊“**新建規則**”選項。
5. 在開啟的“**新建輸出規則精靈**”視窗中，選擇“**連接埠**”選項，然後點擊“**下一步**”。
6. 選擇“**TCP**”協定。
7. 在“**特定遠端連接埠**”欄位中，指定以下允許傳出連線的連接埠範圍：1024-65535。
8. 在“**操作**”視窗中，選擇“**允許連線**”選項。
9. 儲存新規則，然後關閉“**進階安全 Windows 防火牆**”視窗。

Windows 防火牆現在將允許應用程式主控台與 Kaspersky Security 管理服務之間進行網路連線。

在安裝 Kaspersky Embedded Systems Security 2.2 後執行的操作

如果您已啟動，Kaspersky Embedded Systems Security 2.2，該應用程式會在安裝後立即啟動防護和掃描工作。如果在安裝 Kaspersky Embedded Systems Security 2.2 期間選中“**安裝應用程式後啟用即時防護**”（預設選項），當電腦的檔案系統物件被存取時，應用程式會掃描這些物件。Kaspersky Embedded Systems Security 2.2 將在每週五的 20:00 執行“關鍵區域掃描”工作。

建議在安裝 Kaspersky Embedded Systems Security 2.2 後執行下列步驟：

- 啟動應用程式資料庫更新工作。安裝後，Kaspersky Embedded Systems Security 2.2 會使用應用程式發行套件中所含的資料庫掃描物件。

  我們建議立即更新 Kaspersky Embedded Systems Security 2.2 資料庫，因為它們可能已過期。

  之後，應用程式將根據預設排程每小時更新一次資料庫。
- 如果安裝 Kaspersky Embedded Systems Security 2.2 之前受防護電腦上未安裝任何具有即時檔案防護的病毒防護軟體，請在電腦上執行“關鍵區域掃描”。
- 配置有關 Kaspersky Embedded Systems Security 2.2 事件的管理員通知。

本章節說明項目

啟動和配置 Kaspersky Embedded Systems Security 2.2 資料庫更新工作

► *要在安裝後更新應用程式資料庫，請執行以下操作：*

1. 在“資料庫更新”工作設定中，配置與更新來源的連線 – Kaspersky Lab HTTP 或 FTP 更新伺服器。
2. 啟動“資料庫更新”工作。

► *要設定與 Kaspersky Lab 更新伺服器連線，請在“資料庫更新”工作中執行以下操作：*

1. 透過以下方式之一啟動應用程式主控台：
   - 在受防護的電腦上開啟應用程式主控台。要執行此操作，請選取“**開始** > **所有程式** > **Kaspersky Embedded Systems Security 2.2** > **管理工具** > **Kaspersky Embedded Systems Security 2.2 主控台**”。
   - 如果應用程式主控台已在不受防護的電腦上啟動，請連線到受防護的電腦：
     a. 在應用程式主控台樹狀目錄中開啟“**Kaspersky Embedded Systems Security**”節點的內容功能表。
     b. 選擇“**連線至其他電腦**”項。
     c. 在“**選擇電腦**”視窗中，選擇“**其他電腦**”，然後在文字欄位中，指定受防護電腦的網路名稱。

     > 如果用於登入到 Microsoft Windows 的帳戶沒有 Kaspersky Security 管理服務的存取權限（請參見第 73 頁上的“關於 Kaspersky Security 管理服務的存取權限”部分），請指定具有所需權限的帳戶。

   將開啟應用程式主控台視窗。
2. 在應用程式主控台樹狀目錄中，展開“**更新**”節點。
3. 選擇“**資料庫更新**”子節點。
4. 在詳細資訊視窗中點擊“**內容**”連結。
5. 在開啟的“**工作設定**”視窗中，開啟“**連線設定**”標籤。
6. 執行以下操作：
   a. 如果網路上未設定 Web 代理自動發現協定 (WPAD) 自動偵測區網中的代理伺服器設定，請指定代理伺服器設定：在“**代理伺服器設定**”部分中，選擇“**使用自訂代理伺服器設定**”核取方塊，在“**位址**”欄位輸入位址，最後在“**連接埠**”欄位輸入代理伺服器的連接埠號。
   b. 如果存取代理伺服器時需要身分驗證，在“**代理伺服器身分驗證設定**”部分的下拉清單中選擇必要的身分驗證方法：
      - 如果代理伺服器支援內建 Microsoft Windows NTLM 驗證方式，請**使用 NTLM 身分驗證**方式。Kaspersky Embedded Systems Security 2.2 將使用工作設定中指定的使用者帳戶存取代理伺服器（預設情況下，該工作會在“**本機系統（系統）**”使用者帳戶下執行）。
      - 如果代理伺服器支援內建 Microsoft Windows NTLM 驗證方式，請**使用帶使用者名稱和密碼的 NTLM 身分驗證**方式。Kaspersky Embedded Systems Security 2.2 將使用您指定的帳戶來存取代理伺服器。輸入使用者名稱與密碼，或從清單選擇一個使用者。
      - **套用使用者名稱和密碼**，以選擇基本驗證。輸入使用者名稱與密碼，或從清單選擇一個使用者。
7. 在“**工作設定**”視窗中點擊“**確定**”。

將儲存“資料庫更新”工作中連線更新來源的設定。

► *要執行“資料庫更新”工作，請執行以下操作：*

1. 在應用程式主控台樹狀目錄中，展開“**更新**”節點。
2. 在“**資料庫更新**”子節點的內容功能表中，選擇“**啟動**”項。

“資料庫更新”工作啟動。

工作成功完成後，您可檢視 **Kaspersky Embedded Systems Security** 節點所安裝最新的資料庫更新發佈的日期。

關鍵區域掃描

更新 Kaspersky Embedded Systems Security 2.2 資料庫後，使用“關鍵區域掃描”工作掃描電腦中是否有惡意程式。

► *若要執行“關鍵區域掃描”工作，請執行以下步驟：*

1. 在應用程式主控台樹狀目錄中展開“**自訂掃描**”節點。
2. 在“**關鍵區域掃描**”子節點的內容功能表中，選擇“**啟動**”指令。

工作啟動；工作區域中顯示工作狀態“**正在執行**”。

► *要檢視工作記錄，請執行下列操作：*

在“**關鍵區域掃描**”節點的詳細資訊視窗中，點擊“**開啟記錄**”連結。

修改元件集和還原 Kaspersky Embedded Systems Security 2.2

您可新增或移除 Kaspersky Embedded Systems Security 2.2 元件。您需要先停止“即時檔案防護”工作，才能刪除“即時檔案防護”元件。其他情況下，將不需停止即時檔案防護工作或 Kaspersky Security 服務。

如果應用程式管理存取受密碼防護，Kaspersky Embedded Systems Security 2.2 會在您在設定精靈中的其他步驟中嘗試移除或修改元件集時請求密碼。

► *要修改 Kaspersky Embedded Systems Security 2.2 元件集：*

1. 在“**開始**”功能表中，選擇“**所有程式 > Kaspersky Embedded Systems Security 2.2 > 修改或移除**”。

   將開啟安裝精靈的“**修改、修復或移除安裝**”視窗。
2. 選擇“**修改元件集**”。點擊“**下一步**”按鈕。

   將開啟“**自訂安裝**”視窗。
3. 在“**自訂安裝**”視窗的可用元件清單中，選擇希望新增到 Kaspersky Embedded Systems Security 2.2 中或希望移除的元件。為此，請執行以下操作：
   - 要變更元件集，請點擊所選元件名稱旁邊的按鈕，並在內容功能表中選擇：
     - “**元件將被安裝在本機硬碟上**”（如果您想要安裝一個元件）；
     - “**程式將在本機磁碟上安裝元件及其子元件**”（如果您想要安裝一組元件）。
   - 要刪除先前安裝的元件，請點擊所選元件名稱旁邊的按鈕，並在內容功能表中選擇“**元件將變為不可用**”。

   點擊“**安裝**”按鈕。

4. 在“**已準備安裝**”視窗中，透過點擊“安裝”按鈕確認軟體元件集的變更。
5. 在安裝完成後開啟的視窗中，點擊“**確定**”按鈕。

將根據指定設定修改 Kaspersky Embedded Systems Security 2.2 元件集。

如果 Kaspersky Embedded Systems Security 2.2 於運作時發生問題（Kaspersky Embedded Systems Security 2.2 當機；工作損毀或無法啟動），您可嘗試還原 Kaspersky Embedded Systems Security 2.2。您可在儲存 Kaspersky Embedded Systems Security 2.2 的目前設定時執行還原，或選擇一個選項以將所有 Kaspersky Embedded Systems Security 2.2 設定重設為預設值。

► *要在應用程式或工作崩潰後還原 Kaspersky Embedded Systems Security 2.2，請執行以下步驟：*

1. 在“**開始**”功能表中，選擇“**所有程式 > Kaspersky Embedded Systems Security 2.2 > 修改或移除**”。

   隨即會開啟該精靈的“**修改、修復或移除**”視窗。
2. 選擇“**修復已安裝元件**”。點擊“**下一步**”按鈕。

   這會開啟“**修復已安裝元件**”視窗。
3. 在“**修復已安裝元件**”視窗中，如果您希望重設已配置的應用程式設定並使用其預設設定還原 Kaspersky Embedded Systems Security 2.2，則選中“**還原建議的應用程式設定**”核取方塊。點擊“**安裝**”按鈕。
4. 在“**準備進行修復**”視窗中，透過點擊“**安裝**”按鈕確認修復操作。
5. 在修復完成後開啟的視窗中，點擊“**確定**”按鈕。

將根據指定設定還原 Kaspersky Embedded Systems Security 2.2。

使用安裝精靈移除

本節包含有關使用安裝精靈從受防護電腦上移除 Kaspersky Embedded Systems Security 2.2 和應用程式主控台的說明。

Kaspersky Embedded Systems Security 2.2 移除

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

您可使用安裝/移除安裝精靈來移除受防護電腦上的 Kaspersky Embedded Systems Security 2.2。

從受防護電腦上移除 Kaspersky Embedded Systems Security 2.2 後，可能需要重新啟動電腦。您也可以稍後再重新啟動。

如果作業系統使用 UAC 功能（使用者帳戶控制）或對應用程式的存取受密碼防護，則不能透過 Windows 主控台移除、還原和安裝應用程式。

如果應用程式管理存取受密碼防護，Kaspersky Embedded Systems Security 2.2 會在您在設定精靈中的其他步驟中嘗試移除或修改元件集時請求密碼。

► *要移除 Kaspersky Embedded Systems Security 2.2：*

1. 在“**開始**”功能表中，選擇“**所有程式 > Kaspersky Embedded Systems Security 2.2 > 修改或移除**”。

   將開啟安裝精靈的“**修改、修復或移除安裝**”視窗。

2. 選擇“**移除軟體元件**”。點擊“**下一步**”按鈕。

   將開啟“**進階應用程式移除設定**”視窗。

3. 如有必要，在“**進階應用程式移除設定**”視窗中：

   a. 選中“**匯出隔離區物件**”核取方塊以便 Kaspersky Embedded Systems Security 2.2 匯出已隔離的物件。預設取消選定該核取方塊。

   b. “**匯出備份區物件**”核取方塊，以便從 Kaspersky Embedded Systems Security 2.2 備份區匯出物件。預設取消選定該核取方塊。

   c. 點擊“**儲存到**”按鈕並選擇您希望將正在還原的物件匯出到的資料夾。預設情況下，會將物件匯出到 %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\Uninstall。

   點擊“**下一步**”按鈕。

4. 在“**已準備移除**”視窗中，透過點選“**移除**”按鈕確認移除。

5. 在移除完成後開啟的視窗中，點擊“**確定**”按鈕。

Kaspersky Embedded Systems Security 2.2 將從受防護電腦移除。

Kaspersky Embedded Systems Security 2.2 主控台移除

> 在不同 Windows 作業系統中，設定的名稱可能會有所不同。

您可以使用安裝/移除精靈，從電腦移除應用程式主控台。

移除應用程式主控台後，無需重新啟動電腦。

► *要移除應用程式主控台，請執行下列步驟：*

1. 在“**開始**”功能表中，選擇“**所有程式 > Kaspersky Embedded Systems Security > 管理工具 >修改或移除**”。

2. 將開啟精靈的“**修改、修復或移除**”視窗。

   選擇“**移除軟體元件**”並點擊“**下一步**”按鈕。

3. 隨即會開啟“**已準備移除**”視窗。點擊“**刪除**”按鈕。

   將開啟“**移除完成**”視窗。

4. 點擊“**確定**”。

此時，移除完成，且安裝精靈關閉。

透過命令列安裝或移除應用程式

本章節介紹從命令列安裝和移除 Kaspersky Embedded Systems Security 2.2 的詳細資訊，包含從命令列安裝和移除 Kaspersky Embedded Systems Security 2.2 的指令範例，以及從命令列新增和移除 Kaspersky Embedded Systems Security 2.2 元件的指令範例。

本章節說明項目

關於從命令列安裝和移除 Kaspersky Embedded Systems Security 2.2

當您使用金鑰指定安裝設定後，可透過命令列執行 \product\ess_x86(x64).msi 安裝套件檔案，來安裝或移除 Kaspersky Embedded Systems Security 2.2，以及新增或移除其元件。

您可在受防護電腦或網路的另一台電腦上安裝“管理工具”集，以本機或遠端方式和應用程式主控台搭配使用。若要安裝，請使用 \client\esstools.msi 安裝套件。

使用應用程式所安裝之電腦的管理員群組帳戶權限來執行安裝。

如果在沒有備用金鑰的受防護電腦上執行其中一個 \product\ess_x86(x64).msi 檔案，將使用建議的安裝設定安裝 Kaspersky Embedded Systems Security 2.2。

您可使用 ADDLOCAL 命令列選項，透過列出所選的元件或元件集的代碼，來指定要安裝的元件集。

安裝 Kaspersky Embedded Systems Security 2.2 的指令範例

本章節介紹安裝 Kaspersky Embedded Systems Security 2.2 所用的指令範例。

在執行 32 位元版本的 Microsoft Windows 的電腦上，執行發行套件中帶有 x86 尾碼的檔案。在執行 64 位元版本的 Microsoft Windows 的電腦上，執行發行套件中帶有 x64 尾碼的檔案。

有關使用 Windows Installer 標準指令和命令列選項的詳細資訊，提供在 Microsoft 供應的文件中。

從檔案 setup.exe 安裝 Kaspersky Embedded Systems Security 2.2 的指令範例

► *若不想以使用者互動模式安裝 Kaspersky Embedded Systems Security 2.2，而想以預設的安裝設定來安裝，請執行以下指令：*

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

► *使用下列設定安裝 Kaspersky Embedded Systems Security 2.2：*

- 僅安裝“即時檔案防護”和“自訂掃描”元件；
- 在啟動 Kaspersky Embedded Systems Security 2.2 時不執行即時防護；
- 不要從 Microsoft Corporation 建議排除的掃描檔案中排除；

請執行以下指令：

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

用於安裝的指令範例：執行安裝套件的 .msi 檔案

► *若不想以使用者互動模式安裝 Kaspersky Embedded Systems Security 2.2，而想以預設的安裝設定來安裝，請執行以下指令：*

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

► *若要以預設安裝設定安裝 Kaspersky Embedded Systems Security 2.2、顯示安裝介面，請執行以下指令：*

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

► *若要安裝 Kaspersky Embedded Systems Security 2.2 並使用金鑰檔案 C:\0000000A.key 啟動：*

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

► *要事先掃描活動的處理程序與本機磁碟的開機磁區，再安裝 Kaspersky Embedded Systems Security 2.2，請執行以下指令：*

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

► *若要安裝 Kaspersky Embedded Systems Security 2.2 並將檔案儲存在目的資料夾 C:\ESS 中，請執行以下指令：*

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

► *若要安裝 Kaspersky Embedded Systems Security 2.2：將名稱為 ess.log 的安裝記錄檔案儲存到儲存了 Kaspersky Embedded Systems Security 2.2 安裝套件的 msi 檔案的資料夾，並執行以下指令：*

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

► *若要安裝 Kaspersky Embedded Systems Security 2.2 主控台，請執行以下指令：*

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

► *若要使用 C:\0000000A.key 檔案的金鑰安裝 Kaspersky Embedded Systems Security 2.2 ：根據 C:\settings.xml 設定檔所敘述的配置設定 Kaspersky Embedded Systems Security 2.2，請執行以下指令：*

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

► *若要在 Kaspersky Embedded Systems Security 2.2 受密碼防護的情況下安裝應用程式修補程式，請執行以下指令：*

msiexec /p "<msp 檔案名及路徑>" UNLOCK_PASSWORD=<密碼>

在安裝 Kaspersky Embedded Systems Security 2.2 後執行的操作

如果您已啟動，Kaspersky Embedded Systems Security 2.2，該應用程式會在安裝後立即啟動防護和掃描工作。如果在安裝 Kaspersky Embedded Systems Security 2.2 期間選中“**安裝應用程式後啟用即時防護**”（預設選項），當電腦的檔案系統物件被存取時，應用程式會掃描這些物件。Kaspersky Embedded Systems Security 2.2 將在每週五的 20:00 執行“關鍵區域掃描”工作。

建議在安裝 Kaspersky Embedded Systems Security 2.2 後執行下列步驟：

- 啟用 Kaspersky Embedded Systems Security 2.2 資料庫更新工作。安裝後 Kaspersky Embedded Systems Security 2.2 將使用分發套件中所含的資料庫掃描物件。我們建議立即更新 Kaspersky Embedded Systems Security 2.2 資料庫。若要進行更新，您必須執行“資料庫更新”工作。之後，資料庫將根據預設排程，每小時更新一次。

  例如，您可執行以下指令來啟動“資料庫更新”工作：

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

  在此情況下，將從 Kaspersky Lab 更新伺服器下載 Kaspersky Embedded Systems Security 2.2 資料庫。與更新來源的連線是透過代理伺服器（代理伺服器位址：proxy.company.com，連接埠：8080）使用內建的 Windows NTLM 身分驗證以某個帳戶存取伺服器來建立的（使用者名稱：inetuser，密碼：123456）。

- 如果安裝 Kaspersky Embedded Systems Security 2.2 之前受防護電腦上未安裝任何具有即時檔案防護的病毒防護軟體，請對電腦執行“關鍵區域掃描”。

  ► *若要使用命令列啟動“關鍵區域掃描 ”工作：*

  KAVSHELL SCANCRITICAL /W:scancritical.log

  此指令會將工作記錄儲存在目前資料夾內名為 scancritical.log 檔案中。

- 配置有關 Kaspersky Embedded Systems Security 2.2 事件的管理員通知。

新增/移除元件。指令範例

應用程式啟動控制元件已自動安裝。您不必透過新增或移除 Kaspersky Embedded Systems Security 2.2 元件，在 ADDLOCAL 指令設定值清單中指定此元件。

► *要將“自訂掃描”元件新增到已安裝的元件，請執行以下指令：*

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

或

\server\setup.exe /s /p "ADDLOCAL=Oas,Ods"

如果您將要安裝的元件與已安裝的元件枚舉在一起，則 Kaspersky Embedded Systems Security 2.2 將重新安裝現有的元件。

► *要刪除已安裝的元件，請執行以下指令：*

msiexec /i ess.msi "ADDLOCAL=Oas,AppCntrl,Ksn,AntiExploit,DevCtrl,Firewall,LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,RamDisk REMOVE=Ods,Fim" /qn

Kaspersky Embedded Systems Security 2.2 移除。指令範例

► *要從受防護電腦移除 Kaspersky Embedded Systems Security 2.2，請執行以下指令：*

msiexec /x ess.msi /qn

或

- 對於 32 位元作業系統：

msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} /qn

- 對於 64 位元作業系統：

msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} /qn

► *要移除 Kaspersky Embedded Systems Security 2.2 主控台，請執行以下指令：*

msiexec /x esstools.msi /qn

或

- 對於 32 位元作業系統：

msiexec /x {A727008F-F8CC-4B35-848A-1AECEEF22178} /qn

- 對於 64 位元作業系統：

msiexec /x {D978C311-2D2D-41A3-8158-BDF97149CCD4} /qn

► *要從已啟用密碼防護的受防護電腦上移除 Kaspersky Embedded Systems Security 2.2，請執行以下指令：*

- 對於 32 位元作業系統：

  msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} UNLOCK_PASSWORD=*** /qn

- 對於 64 位元作業系統：

  msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} UNLOCK_PASSWORD=*** /qn

回傳代碼

以下表格包含命令列的回傳代碼清單。

步驟 13. 回傳代碼

代碼	敘述
1324	目的資料夾名稱包含無效的字元。
25001	沒有足夠權限安裝 Kaspersky Embedded Systems Security 2.2。要安裝該應用程式，請使用本機管理員權限啟動安裝精靈。
25003	Kaspersky Embedded Systems Security 2.2 不能安裝在執行此版本的 Microsoft Windows 的電腦上。請啟動用於 64 位元版本 Microsoft Windows 的安裝精靈。
25004	偵測到不相容的軟體。要繼續安裝，請移除以下軟體：<不相容軟體清單>。
25010	指定的路徑不能用於儲存已隔離的物件。
25011	用於儲存已隔離的物件的資料夾名包含無效的字元。
26251	無法下載效能計數器 DLL。
26252	無法下載效能計數器 DLL。
27300	不能安裝驅動程式。
27301	不能移除驅動程式。
27302	不能安裝網路元件。已達到所支援的篩選裝置的最大數量。
27303	無法找到病毒特徵碼資料庫。

使用卡巴斯基安全管理中心安裝和移除應用程式

本章節包含有關透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security 2.2 的一般資訊。同時也介紹如何透過卡巴斯基安全管理中心安裝和移除 Kaspersky Embedded Systems Security 2.2 以及安裝 Kaspersky Embedded Systems Security 2.2 後的操作。

本章節說明項目

透過卡巴斯基安全管理中心進行安裝的一般資訊

您可以透過卡巴斯基安全管理中心，使用遠端安裝工作來安裝 Kaspersky Embedded Systems Security 2.2。

完成遠端安裝工作後，將在多台電腦上使用相同的設定安裝 Kaspersky Embedded Systems Security 2.2。

您可將所有電腦整合到一個管理員群組中，然後建立一個群組工作，並將 Kaspersky Embedded Systems Security 2.2 安裝到該群組的電腦上。

您可以建立一個工作，在不屬於相同管理群組的一群組電腦上遠端安裝 Kaspersky Embedded Systems Security 2.2。建立此工作時，您必須建立一份要安裝 Kaspersky Embedded Systems Security 2.2 的各個電腦的清單。

有關遠端安裝工作的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

安裝或移除 Kaspersky Embedded Systems Security 2.2 的權限

遠端安裝（移除）工作中所指定的帳戶必須加入每一台受防護電腦的管理員群組中，但以下情況除外：

- 當您想安裝 Kaspersky Embedded Systems Security 2.2 的電腦上已安裝卡巴斯基安全管理中心網路代理程式時（不管電腦屬於哪一個網域或電腦是否屬於任何網域）。

  如果電腦上尚未安裝網路代理程式，您可使用遠端安裝工作安裝網路代理程式與 Kaspersky Embedded Systems Security 2.2。安裝網路代理程式前，務必確認工作中所指定的帳戶已加入每台電腦的管理員群組中。

- 要安裝 Kaspersky Embedded Systems Security 2.2 的電腦都在相同網域中作為管理伺服器使用，且管理伺服器已註冊到“**網域管理員**”帳戶下時（如果此帳戶在該網域電腦上有本機管理員權限）。

預設情況下，使用“**遠端安裝**”方式進行安裝時，遠端安裝工作會在執行管理伺服器下的帳戶執行。

以強制安裝（移除）模式執行群組工作或整組電腦的工作時，用戶端電腦上的帳戶必須有下列權限：

- 遠端執行應用程式的權限。
- 存取 **Admin$** 資源的權限。
- **作為服務登入**權限。

透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security 2.2 的步驟

如需更多有關生成安裝套件和遠端安裝工作的資訊，請參閱《卡巴斯基安全管理中心實施手冊》。

如果希望以後透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security 2.2，請確保符合以下條件：

- 安裝了卡巴斯基安全管理中心管理伺服器的電腦上還安裝了管理外掛程式（Kaspersky Embedded Systems Security 2.2 分發套件中的 \product\klcfginst.exe 檔案）。
- 請在受防護電腦上安裝卡巴斯基安全管理中心網路代理。如果電腦上尚未安裝網路代理程式，您可使用遠端安裝工作一起安裝網路代理程式與 Kaspersky Embedded Systems Security 2.2。

您也可以先將多台電腦整合在同一個管理群組中，以便之後使用卡巴斯基安全管理中心政策和群組工作管理防護設定。

► *要以遠端安裝工作安裝 Kaspersky Embedded Systems Security 2.2：*

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 在卡巴斯基安全管理中心中，展開“**遠端安裝**”節點，並在“**安裝套件**”子節點中，選擇“**為 Kaspersky Lab 應用程式建立安裝套件**”選項。
3. 輸入安裝套件名稱。
4. 指定 Kaspersky Embedded Systems Security 2.2 分發套件中的 ess.kud 檔案為安裝套件檔案。

   將開啟“**EULA 和隱私政策**”視窗。
5. 如果您同意 EULA 和隱私政策的條款和條件，請選中“**此 EULA 的條款和條件**”和“**描述資料處理的隱私政策**”核取方塊以繼續安裝。

   您必須接受授權協議和隱私政策才能繼續。
6. 要變更要安裝的 Kaspersky Embedded Systems Security 2.2 元件集（請參見第 43 頁上的“修改元件集和還原 Kaspersky Embedded Systems Security 2.2”部分）以及安裝套件中的預設安裝設定（請參見第 28 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）：

   a. 在卡巴斯基安全管理中心中，展開“**遠端安裝**”節點。

   b. 在“**安裝套件**”子節點工作區中，開啟已建立 Kaspersky Embedded Systems Security 2.2 安裝套件的內容功能表，然後選擇“**內容**”。

c. 在“**設定**”部分的“**內容：<安裝套件名稱>**”視窗中，執行以下操作：

a. 在“**要安裝的元件**”設定群組中，選中您想安裝的 Kaspersky Embedded Systems Security 2.2 元件名稱旁邊的核取方塊。

b. 要指定預設資料夾以外的目的資料夾，請在“**目的資料夾**”欄位指定資料夾名稱和路徑。

目的資料夾的路徑可能包含系統環境變數。電腦上若沒有您指定的資料夾，就會建立資料夾。

c. 在“**進階安裝設定**”群組中，配置以下設定：

- 在安裝之前對電腦進行病毒掃描。
- 安裝應用程式後啟用即時防護。
- 將 Microsoft 建議的檔案新增到排除清單。

d. 將 Kaspersky Lab 建議的檔案新增到排除清單。

d. 在“**內容：<安裝套件名稱>**”視窗，點擊“**確定**”。

7. 在“**安裝套件**”節點中，於選定電腦（管理群組）上建立 Kaspersky Embedded Systems Security 2.2 的遠端安裝工作。配置工作設定。

要了解建立和配置遠端安裝工作的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

8. 執行 Kaspersky Embedded Systems Security 2.2 的遠端安裝工作。

將會在工作中指定的電腦上安裝 Kaspersky Embedded Systems Security 2.2。

在安裝 Kaspersky Embedded Systems Security 2.2 後執行的操作

安裝 Kaspersky Embedded Systems Security 2.2 後，建議更新電腦上的 Kaspersky Embedded Systems Security 2.2 資料庫；若安裝 Kaspersky Embedded Systems Security 2.2 前，電腦上未安裝任何防毒應用程式並啟用即時防護功能，則還建議掃描電腦的關鍵區域。

如果您已安裝 Kaspersky Embedded Systems Security 2.2 的電腦位於卡巴斯基安全管理中心的同一個管理群組中，您可使用以下這些工作：

1. 為安裝了 Kaspersky Embedded Systems Security 2.2 的電腦群組建立“資料庫更新”工作。將卡巴斯基安全管理中心管理伺服器設定為更新來源。
2. 依需要使用“關鍵區域掃描”狀態建立“自訂掃描”群組工作。卡巴斯基安全管理中心根據此工作的執行結果（而不是根據關鍵區域掃描工作的結果）評估群組中每台電腦的安全狀態。
3. 為電腦群組建立新的政策。在“**系統工作**”標籤上已建立的政策內容中，根據需要取消啟動系統掃描工作的排程啟動，以及管理群組的電腦上的資料庫更新工作。

您還可以配置有關 Kaspersky Embedded Systems Security 2.2 事件的管理員通知。

透過卡巴斯基安全管理中心安裝應用程式主控台

如需更多有關建立套件和遠端安裝工作的資訊，請參閱*卡巴斯基安全管理中心實施手冊*。

► *要使用遠端安裝工作安裝應用程式主控台，請執行下列操作：*

1. 在卡巴斯基安全管理中心管理主控台中，展開“**遠端安裝**”節點，並在“**安裝套件**”子節點中以 client\setup.exe 檔案建立新的安裝套件。建立新的安裝套件時：
   - 在“**為安裝選擇分發套件**”視窗中，從 Kaspersky Embedded Systems Security 2.2 分發套件資料夾中選擇 client\setup.exe 檔案，然後選中“**將更新從儲存區複製到安裝套件**”核取方塊。
   - 如有需要，可以使用 ADDLOCAL 命令列選項來修改要在**可執行檔啟用設定**（可選）欄位中安裝的元件集，並修改目的資料夾。

     例如，若要在 C:\KasperskyConsole 資料夾中安裝應用程式主控台但不安裝說明檔案和文件，請執行以下指令：

     ```
     /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1
     PRIVACYPOLICY=1"
     ```
2. 在“**安裝套件**”節點中，建立一個工作，於選定電腦（管理群組）上遠端安裝應用程式主控台。配置工作設定。

   要了解建立和配置遠端安裝工作的詳細資訊，請參見*卡巴斯基安全管理中心說明*。
3. 執行已建立的遠端安裝工作。

應用程式主控台安裝到此工作指定的電腦上。

透過卡巴斯基安全管理中心移除 Kaspersky Embedded Systems Security 2.2

如果網路電腦上的 Kaspersky Embedded Systems Security 2.2 管理存取受密碼防護，在建立多個應用程式移除工作時輸入密碼。如果密碼防護未被應用程式集中管理，則將從存取受防護伺服器成功移除，在該電腦上輸入的密碼與設定值比對。不會從其餘電腦移除 Kaspersky Embedded Systems Security 2.2。

► *要移除 Kaspersky Embedded Systems Security 2.2，請在卡巴斯基安全管理中心管理主控台中執行下列步驟：*

1. 在卡巴斯基安全管理中心管理主控台中，建立並啟動應用程式刪除工作。
2. 在工作中，選擇移除方法（與選擇安裝方法類似，請參見以上章節）並指定管理伺服器將使用其權限來定址電腦的帳戶。您只能使用預設移除設定移除 Kaspersky Embedded Systems Security 2.2（請參閱第 28 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）。

透過 Active Directory 群組政策進行安裝和移除

本章節介紹透過 Active Directory 群組政策安裝和移除 Kaspersky Embedded Systems Security 2.2。同時也包含有關透過群組政策安裝 Kaspersky Embedded Systems Security 2.2 後的操作資訊。

本章節說明項目

透過 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security 2.2

您可透過 Active Directory 群組政策在多台電腦上安裝 Kaspersky Embedded Systems Security 2.2。您可以用相同的方式安裝應用程式主控台。

要安裝 Kaspersky Embedded Systems Security 2.2 或應用程式主控台的電腦必須在一個網域中和一個組織單元中。

使用政策協助您安裝 Kaspersky Embedded Systems Security 2.2 之電腦上所安裝的作業系統版本（32 位元或 64 位元）必須一致。

您必須有該網域的管理員權限。

要安裝 Kaspersky Embedded Systems Security 2.2，請使用 ess_x86(x64).msi 安裝套件。要安裝應用程式主控台，請使用 esstools.msi 安裝套件。

有關使用 Active Directory 群組政策的詳細資訊，提供在 Microsoft 供應的文件中。

► *若要安裝 Kaspersky Embedded Systems Security 2.2（或應用程式主控台）：*

1. 將安裝套件的 msi 檔案儲存到網域控制器的公用資料夾中，该安裝套件要和已安裝的 Microsoft Windows 作業系統的字長（32 位元和 64 位元）相對應。
2. 在網域控制器上，為電腦所屬的群組建立新政策。
3. 使用“**群組政策物件編輯器**”，在“**電腦設定**”節點中建立新的安裝套件。以 UNC 格式（通用命名慣例）指定 Kaspersky Embedded Systems Security 2.2（或應用程式主控台）安裝套件 msi 檔案的路徑。
4. 如同所選群組的“**使用者設定**”與“**電腦設定**”節點一樣，選中 Windows Installer 的“**永遠以較高的權限安裝**”核取方塊。
5. 使用 gpupdate /force 指令採納變更。

電腦重新啟動並登入 Microsoft Windows 前，就會在該群組的電腦上安裝 Kaspersky Embedded Systems Security 2.2。

在安裝 Kaspersky Embedded Systems Security 2.2 後執行的操作

在受防護電腦上安裝 Kaspersky Embedded Systems Security 2.2 後，建議您立即更新應用程式資料並執行關鍵區域掃描。您可以從應用程式主控台執行這些操作（請參見第 41 頁上的“在安裝 Kaspersky Embedded Systems Security 2.2 後執行的操作”部分）。

您還可以配置有關 Kaspersky Embedded Systems Security 2.2 事件的管理員通知。

透過 Active Directory 群組政策移除 Kaspersky Embedded Systems Security 2.2

如果您使用 Active Directory 群組政策在群組電腦上安裝 Kaspersky Embedded Systems Security 2.2（或應用程式主控台），則可以使用該政策移除 Kaspersky Embedded Systems Security 2.2（或應用程式主控台）。

您可以僅使用預設的移除參數來移除應用程式。

有關使用 Active Directory 群組政策的詳細資訊，提供在 Microsoft 供應的文件中。

如果應用程式管理存取受密碼防護，使用 Active Directory 群組政策移除 Kaspersky Embedded Systems Security 2.2 不可用。

► *要移除 Kaspersky Embedded Systems Security 2.2（或應用程式主控台）：*

1. 在網域控制器上選擇您要刪除其上面的 Kaspersky Embedded Systems Security 2.2 或應用程式主控台的電腦所在的組織單元。
2. 在“**群組政策編輯器**”中選擇為安裝 Kaspersky Embedded Systems Security 2.2 所建立的政策，在“**軟體安裝**”節點（“**電腦配置** > **軟體設定** > **軟體安裝**”）中開啟 Kaspersky Embedded Systems Security 2.2（或應用程式主控台）安裝套件的內容功能表，然後選擇“**所有工作** > **刪除**”指令。
3. 選擇刪除方法“**立即從使用者處和電腦中移除軟體**”。
4. 使用 gpupdate /force 指令採納變更。

電腦重新啟動並登入 Microsoft Windows 前，就會在電腦群組上移除 Kaspersky Embedded Systems Security 2.2。

Kaspersky Embedded Systems Security 2.2 功能檢查。使用 EICAR 測試病毒

本章節介紹 EICAR 測試病毒和如何使用 EICAR 測試病毒驗證 Kaspersky Embedded Systems Security 2.2 的即時防護和自訂掃描功能。

本章節說明項目

關於 EICAR 測試病毒

測試病毒的設計目的在於驗證防毒應用程式的運作功能。它由歐洲電腦防毒協會 (EICAR) 所開發。

測試病毒並非真正的病毒，並且不包含針對電腦的程式碼。 不過，大部份廠商的防毒應用程式可透過它來辨認威脅。

含有此測試病毒的檔案稱為 eicar.com。您可從 EICAR 網站 http://www.eicar.org/anti_virus_test_file.htm 下載此檔案。

在您將該檔案下載到電腦硬碟中的資料夾前，請確認已停用該磁碟機的即時檔案防護。

eicar.com 檔案含有一行文字。掃描檔案時，Kaspersky Embedded Systems Security 2.2 會偵測到這行文字中有“威脅”等字，接著對檔案指派“**受感染**”狀態並刪除檔案。檔案中偵測到的威脅資訊將出現在應用程式主控台及工作記錄中。

您可使用 eicar.com 檔案來檢查 Kaspersky Embedded Systems Security 2.2 解毒已感染物件及偵測潛在疑似感染物件的方法。要進行檢查，使用文字編輯器開啟 eicar.com 檔案，將該檔案開頭幾行文字所列的前置詞加入另一個新建檔案中，然後以新的檔案名稱（例如 eicar_cure.com）儲存。

為確保 Kaspersky Embedded Systems Security 2.2 處理帶有首碼的 eicar.com 檔案，在“**物件防護**”安全設定部分中，為 Kaspersky Embedded Systems Security 2.2 即時檔案防護工作和預設自訂掃描工作設定“**所有物件**”值。

步驟 14. EICAR 檔案前置詞

前置詞	掃描後的檔案狀態及 Kaspersky Embedded Systems Security 2.2 操作
無前置詞	Kaspersky Embedded Systems Security 2.2 會指派“**受感染**”狀態給物件並刪除物件。
SUSP-	Kaspersky Embedded Systems Security 2.2 會指派“**疑似感染**”狀態給物件（啟發式分析偵測到的）使用並刪除物件（無法解毒疑似感染物件）。
WARN-	Kaspersky Embedded Systems Security 2.2 會指派“**疑似感染**”狀態給物件（物件代碼與已知威脅部分代碼相符）並刪除物件（無法解毒疑似感染物件）。

前置詞	掃描後的檔案狀態及 Kaspersky Embedded Systems Security 2.2 操作
無前置詞	Kaspersky Embedded Systems Security 2.2 會指派“**受感染**”狀態給物件並刪除物件。
CURE-	Kaspersky Embedded Systems Security 2.2 會指派“**受感染**”狀態給物件並解毒物件。如果解毒成功，則檔案中整段文字將以 "CURE" 取代。

即時防護和自訂掃描測試

安裝 Kaspersky Embedded Systems Security 2.2 後，您可確認 Kaspersky Embedded Systems Security 2.2 發現含有惡意程式碼的物件。要進行檢查，您可以使用 EICAR 測試病毒（請參見第 57 頁上的“關於 EICAR 測試病毒”部分）。

► *若要檢查“即時防護”，請執行以下步驟：*

1. 從 EICAR 網站 http://www.eicar.org/anti_virus_test_file.htm 下載 eircar.com 檔案。將它儲存到網路上任何一台電腦的本機磁碟公用資料夾中。

   在您將檔案儲存到資料夾前，請確認已停用該資料夾的即時檔案防護設定。

2. 如果您想檢查網路使用者通知的功能，請確保受防護電腦與儲存有 eicar.com 檔案的電腦均啟用了 Microsoft Windows Messenger 服務。
3. 開啟應用程式主控台。
4. 使用以下其中一種方法，將儲存的 eicar.com 檔案複製到受防護電腦的本機磁碟上：
   - 若要透過“終端服務”視窗進行通知測試，請在使用遠端桌面連線實用程式連線到電腦後，將 eicar.com 檔案複製到電腦。
   - 若要透過“Microsoft Windows Messenger 服務”進行測試通知，請使用電腦的網路位置從您儲存 eicar.com 檔案的電腦複製它。

即時檔案防護工作只有在下列條件符合時才會運作：

- eicar.com 檔案已從受防護電腦刪除。
- 在應用程式主控台中，工作記錄的狀態為“**重要**”。記錄中出現一行與 eicar.com 檔案中威脅有關的資訊。（若要檢視工作記錄，請展開應用程式主控台樹狀結構與“**即時電腦防護**”節點，選擇“即時檔案防護”工作並在“**開啟記錄**”上的詳細資訊面板進行點擊。）
  - 一條 Microsoft Windows Messenger 服務訊息將出現在您從中複製檔案的電腦上，如下所示：Kaspersky Embedded Systems Security 2.2 在 <發生事件的時間> 封鎖了對電腦 <電腦的網路名稱> 上的 <電腦上的檔案的路徑>\eicar.com 的存取。原因：偵測到威脅。病毒名稱：EICAR-Test-File。使用者名稱: 使用者名稱。電腦名稱：<從中複製該檔案的電腦網路名稱>。

   在從中複製 eicar.com 檔案的電腦上，確保 Microsoft Windows Messenger Service 正在執行。

► *要檢查“自訂掃描”功能，請執行以下步驟：*

1. 從 EICAR 網站 http://www.eicar.org/anti_virus_test_file.htm 下載 eircar.com 檔案。將它儲存到網路上任何一台電腦的本機磁碟公用資料夾中。

   在您將檔案儲存到資料夾前，請確認已停用該資料夾的即時檔案防護設定。

2. 開啟應用程式主控台。
3. 執行以下操作：
   a. 在應用程式主控台樹狀目錄中展開“**自訂掃描**”節點。
   b. 選擇“**關鍵區域掃描**”子節點。
   c. 在“**設定掃描範圍**”標籤上，開啟“**網路**”節點上的內容功能表，並選擇“**新增網路檔案**”。
   d. 以 UNC 格式（通用命名慣例）輸入 eicar.com 檔案在遠端電腦中的網路路徑。
   e. 選取將網路路徑新增到掃描範圍的核取方塊。
   f. 執行“關鍵區域掃描”工作。

自訂掃描只有在下列條件符合時才會運作：

- 電腦硬碟上的 eicar.com 檔案已刪除。
- 在應用程式主控台中，工作記錄的狀態為“**重要**”；在“關鍵區域掃描”工作的執行記錄中，有一行與 eicar.com 檔案中威脅有關的資訊。（要檢視工作記錄，請展開應用程式主控台樹狀結構與“**自訂掃描**”節點，選擇“關鍵區域掃描”工作並在詳細資訊面板上的“**開啟記錄**”進行點擊。）

應用程式介面

您可以透過本機應用程式主控台和管理外掛程式控制 Kaspersky Embedded Systems Security 2.2。《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》介紹了本機應用程式主控台的操作。卡巴斯基安全管理中心管理主控台介面用於操作管理外掛程式。有關卡巴斯基安全管理中心介面的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

應用程式授權

本章節提供與應用程式產品授權有關的主要概念的資訊。

本章內容

關於最終使用者產品授權協議

*最終使用者產品授權協議*是您和 AO Kaspersky Lab 之間達成的約束協議，它規定了您在使用所購買的軟體時須遵循的條款。

請仔細檢視最終使用者產品授權協議的條款，然後再開始使用程式。

您可以透過以下方法檢視使用者產品授權協議的條款：

- 在 Kaspersky Embedded Systems Security 2.2 安裝期間
- 閱讀 license.txt 檔案。本檔案包含在應用程式的安裝套件中

一旦在安裝程式時確認您同意最終使用者產品授權協議，即表示您接受最終使用者產品授權協議的條款。如果您不接受最終使用者產品授權協議的條款，則必須中止程式安裝，且不得使用程式。

關於產品授權

產品授權是根據使用者授權協議在有限時間內授予您使用本程式的權利。

有效的產品授權可使您享有以下各種服務：

- 依照使用者產品授權協議的條款使用應用程式
- 技術支援

服務範圍和應用程式使用條款取決於啟動應用程式的產品授權類型。

使用購買的正式產品授權的金鑰檔案啟動應用程式。

正式產品授權是指購買應用程式時授予的付費產品授權。

Kaspersky Embedded Systems Security 2.2 提供兩種類型的正式產品授權：

- Kaspersky Embedded Systems Security 標準產品授權
- Kaspersky Embedded Systems Security Compliance Edition 延伸產品授權，包括兩個附加的系統檢查元件：“檔案完整性監控”和“記錄審查”。

正式版產品授權到期後，應用程式將在受限功能模式下繼續執行（例如無法更新 Kaspersky Embedded Systems Security 2.2 資料庫）。要繼續在全功能模式下使用 Kaspersky Embedded Systems Security 2.2，您必須對您的正式版產品授權進行續約。

為確保最大限度防護您的電腦免受安全威脅，我們建議您在產品授權到期之前進行續約。

確保您新增的備用金鑰的到期日期晚於啟動金鑰。

關於產品授權憑證

*產品授權憑證*是一個與金鑰檔案或啟動碼（如果適用）一起提供給您的證明文件。

產品授權憑證包含以下有關所提供的產品授權的相關資訊：

- 訂單號
- 有關被授予產品授權的使用者的資訊
- 有關可以使用所提供的產品授權啟動的應用程式的資訊
- 授權單元數限制（例如，執行可以使用所提供的產品授權的應用程式的裝置數量）
- 產品授權有效開始日期
- 產品授權到期日期或產品授權期限
- 產品授權類型

關於啟動碼

*啟動碼*是由 20 個字母和數字組成的唯一序列。您必須輸入啟動碼才能新增用於啟動 Kaspersky Embedded Systems Security 2.2 的金鑰。您在購買 Kaspersky Embedded Systems Security 2.2 時提供的電子郵件信箱會收到啟動碼。

要使用啟動碼啟動應用程式，您需要 Internet 存取權限以連線到 Kaspersky Lab 啟動伺服器。

如果您在安裝應用程式後遺失了啟動碼，可以將其還原。例如，您可能需要啟動碼才能註冊 Kaspersky CompanyAccount。要還原啟動碼，請聯絡 Kaspersky Lab 技術支援。

關於金鑰

*金鑰*是一串位資料，您可以依照最終使用者產品授權協議的條款透過該金鑰來啟動並在啟動後使用程式。金鑰是由 Kaspersky Lab 建立的。

您可以透過金鑰檔案在應用程式中新增產品授權。在應用程式中新增金鑰後，將在應用程式介面中以唯一的字母數字序列形式顯示。

Kaspersky Lab 可能會由於某個產品授權違反授權協議而將其新增到黑名單中。如果封鎖了您的金鑰，則必須新增其他金鑰以使應用程式正常工作。

金鑰可以是“啟動金鑰”或“備用金鑰”。

*啟動金鑰*是指目前正在使用的金鑰檔案以使應用程式正常工作。可以將正式產品授權的金鑰新增為啟動金鑰。應用程式只能有一個啟動金鑰。

*備用金鑰*使用者可新增一組目前尚未使用的金鑰。在與目前啟動金鑰關聯的產品授權到期時，備用金鑰將自動變為啟動金鑰。只有在具有啟動金鑰時，才能新增備用金鑰。

關於金鑰檔案

*金鑰檔案*是一個從 Kaspersky Lab 收到的帶有 .key 副檔名的檔案。金鑰檔案主要是用來啟動應用程式金鑰。

您在購買 Kaspersky Embedded Systems Security 2.2 時提供的電子郵件信箱會收到金鑰檔案。

您不需要連線到 Kaspersky Lab 啟動伺服器，即可利用金鑰檔案啟動應用程式。

如果金鑰檔案被意外刪除，可使用以下還原方法。您可能需要使用金鑰檔案在 Kaspersky CompanyAccount 中進行註冊。

要還原金鑰檔案，應該執行以下任何操作：

- 聯絡技術支援 https://support.kaspersky.com/。
- 在 Kaspersky Lab 網站上，根據現有的啟動碼獲取金鑰檔案。

關於資料提供

Kaspersky Embedded Systems Security 2.2 的授權協議（特別是“資料處理條款”部分）指定了本手冊中指示的傳送和處理資料的條款、責任及過程。在接受授權協議前，請仔細檢視其條款以及授權協議連結到的所有文件。

Kaspersky Lab 在您使用應用程式時收到的資料受到防護並按照隱私政策 https://www.kaspersky.com/products-and-services-privacy-policy 進行處理。

接受授權協議的條款，即表示您同意自動將以下資料傳送到 Kaspersky Lab：

- 為支援接收更新的機制 - 有關已安裝的應用程式及其啟動的資訊 :已安裝的應用程式及其完全版本的識別碼，包括內部版本號、類型以及產品授權識別碼、安裝識別碼、唯一更新工作識別碼。
- 為在應用程式出錯時使用導航到知識庫文章的功能（重定向器服務）- 有關應用程式和連結類型的資訊，具體為：名稱、區域設定以及應用程式的完全版本號、重定向連結的類型和錯誤識別碼。
- 為管理資料處理的確認 - 有關授權協議和規定了資料傳輸條款的其他文件的接受狀態的資訊：授權協議或其他文件（接受或拒絕作為其一部分的資料處理條款）的識別碼和版本；表示使用者操作（確認或撤銷接受條款）的內容；資料處理條款接受的狀態變更的日期和時間。

您可以透過以下方法檢視使用者產品授權協議的條款：

- 在應用程式安裝過程中，Kaspersky Embedded Systems Security 2.2 安裝精靈將在請求接受產品授權協議條款的步驟中顯示產品授權協議的全文。
- 隨時檢視 TXT 檔案 (license.txt)，其中包含產品授權協議全文。此檔案連同應用程式安裝檔案一同包含在 Kaspersky Embedded Systems Security 2.2 分發套件中。

本機資料處理

在執行本手冊所述的應用程式主要功能時，Kaspersky Embedded Systems Security 2.2 會在受防護電腦上本機處理和儲存一系列資料：

- 有關掃描的檔案和偵測的物件的資訊，例如，被處理檔案的名稱和內容以及它們在被掃描介質上的完整路徑、對掃描的檔案執行的操作、對受防護網路或受防護電腦執行任何操作的使用者的帳戶、被掃描裝置的名稱和相關資料、有關系統上執行的處理程序的資訊；
- 有關作業系統活動和設定的資訊，例如，Windows 防火牆設定、Windows 事件記錄項目、使用者帳戶的名稱、可執行檔的啟動，這些檔案的校驗和以及內容。

作為應用程式基本功能的一部分，Kaspersky Embedded Systems Security 2.2 處理並儲存資料，特別是記錄應用程式事件和接收診斷資料。本機處理的資料按照配置和應用的應用程式設定進行防護。

Kaspersky Embedded Systems Security 2.2 允許您為本機處理的資料配置防護等級：您可以變更存取處理程序資料的使用者權限，變更此類別資料的資料保留期，完全或部分停用涉及資料記錄的功能，以及變更磁碟機上用於記錄資料的資料夾的路徑和內容。

有關對涉及資料處理的應用程式功能進行配置以及處理的資料儲存的預設設定的詳細資訊，請參見本手冊的相應章節。

預設情況下，在移除 Kaspersky Embedded Systems Security 2.2 後，將刪除本機電腦上儲存的所有資料，但包含診斷資訊（偵錯檔案和傾印檔案）的檔案以及應用程式活動的 Windows 事件記錄除外。您需要手動刪除這些檔案。有關設定診斷過程的詳細資訊，請參見本手冊的相應章節。

移除應用程式時，可以儲存備份和隔離儲存的內容。

使用金鑰啟動應用程式

您可以套用金鑰啟動 Kaspersky Embedded Systems Security 2.2。

如果已經為 Kaspersky Embedded Systems Security 2.2 新增了啟動金鑰，並且您新增另一個金鑰作為啟動金鑰，則新金鑰會取代之前新增的金鑰。之前安裝的啟動金鑰會被刪除。

如果已經為 Kaspersky Embedded Systems Security 2.2 新增了備用金鑰，並且您新增另一個金鑰作為備用金鑰，則新金鑰會取代之前新增的金鑰。之前安裝的備用金鑰會被刪除。

如果已經為 Kaspersky Embedded Systems Security 2.2 新增了啟動金鑰和備用金鑰，並且您新增新金鑰作為啟動金鑰，則新金鑰會取代之前新增的啟動金鑰；備用金鑰不會被刪除。

► *要啟動 Kaspersky Embedded Systems Security 2.2：*

1. 在應用程式主控台樹狀目錄中，展開“**授權**”節點。
2. 在“**授權**”節點的詳細資訊窗格中，點擊“**新增金鑰**”連結。
3. 在開啟的視窗中，點擊“**瀏覽**”按鈕並選擇具有 .key 副檔名的授權檔案。

   還可以將金鑰作為備用金鑰新增。若要新增備用金鑰，請選中“**作為備用金鑰使用**”核取方塊。

4. 點擊“**確定**”。

將會套用選定的金鑰。可在“**授權**”節點上檢視有關新增的金鑰的資訊。

檢視有關目前產品授權的資訊

檢視授權資訊

有關目前產品授權的資訊顯示在應用程式主控台的 **Kaspersky Embedded Systems Security** 節點的詳細資訊窗格中。金鑰狀態可以是以下值：

- **檢查金鑰狀態** – Kaspersky Embedded Systems Security 2.2 正在檢查已新增的金鑰檔案或應用的啟動碼，等待有關目前金鑰狀態的回應。
- **產品授權到期日期** – Kaspersky Embedded Systems Security 2.2 已啟動，且在指定日期和時間之前有效。在以下情況下，金鑰狀態突出顯示為黃色：
  - 產品授權將在 14 天後到期，且未新增備用金鑰或啟動碼。
  - 新增的金鑰已被列入黑名單且將被封鎖。
- **程式未啟動** – 由於尚未新增金鑰或尚未套用啟動碼，Kaspersky Embedded Systems Security 2.2 未啟動。狀態紅色高亮顯示。
- **產品授權已到期** – 由於產品授權已到期，Kaspersky Embedded Systems Security 2.2 未啟動。狀態紅色高亮顯示。
- **已違反最終使用者產品授權協議** – 由於違反了最終使用者產品授權協議（請參見第 60 頁上的“關於最終使用者產品授權協議”部分）的條款，Kaspersky Embedded Systems Security 2.2 未啟動。狀態紅色高亮顯示。
- **金鑰已被列入黑名單** – 新增的金鑰檔案已被 Kaspersky Lab 封鎖並列入黑名單，例如，金鑰被協力廠商用來非法啟動程式。狀態紅色高亮顯示。

檢視有關目前產品授權的資訊

► *若要檢視有關目前產品授權的資訊,*

在應用程式主控台樹狀目錄中，展開“**授權**”節點。

有關目前產品授權的一般資訊顯示在“**授權**”節點的詳細資訊視窗中（請參見下表）。

步驟 15. “授權”節點中有關產品授權的一般資訊

欄位	敘述
啟動碼	啟動碼編號。如果您使用啟動碼啟動應用程式時，則填寫此欄位。
啟動狀態	有關應用程式的啟動狀態的資訊。“授權”節點的控制窗格中“啟動狀態”列中的資訊可具有以下值： • **已套用** – 如果您已使用啟動碼或金鑰檔案啟動應用程式。 • **啟動** – 如果您已套用啟動碼啟動應用程式，但啟動過程尚未最終完成。應用程式啟動已完成且節點的詳細資訊窗格的內容已重新整理後，狀態值變更為“已套用”。 • **啟動錯誤** – 如果應用程式啟動失敗。您可在工作記錄中檢視啟動不成功的原因。
金鑰	您用於啟動應用程式的金鑰編號。
產品授權類型	產品授權類型：正式版。
到期日期	與啟動金鑰相關聯的產品授權的到期日期和時間。
啟動碼狀態或金鑰狀態	啟動碼狀態或金鑰狀態：啟動或備用。

► *若要檢視有關產品授權的詳細資訊*

選擇“**授權**”節點，開啟包含您要展開的產品授權資料的字串的內容功能表，然後選擇“**內容**”。在“**內容：<啟動碼狀態或金鑰狀態>**”視窗中，“**一般**”標籤顯示有關目前產品授權的詳細資訊，“**進階**”標籤顯示有關客戶的資訊以及 Kaspersky Lab 或向您出售 Kaspersky Embedded Systems Security 2.2 的轉銷商的聯絡人詳細資訊（請參見下表）。

步驟 16. 內容中產品授權的詳細資訊 ：<啟動碼狀態或金鑰狀態>視窗

欄位	敘述
“一般”標籤	
金鑰	您用於啟動應用程式的金鑰編號。
金鑰新增日期	金鑰新增到應用程式的日期。
產品授權類型	產品授權類型：正式版。
到期剩餘天數	與啟動金鑰相關的產品授權在到期前剩餘的天數。
到期日期	與啟動金鑰相關聯的產品授權的到期日期和時間。如果在無限期訂購下啟動應用程式，此欄位的值為*無限期*。如果 Kaspersky Embedded Systems Security 2.2 無法確定產品授權到期日期，則此欄位的值設定為*未知*。
應用程式	使用金鑰或新增的啟動碼啟動的應用程式的名稱。

欄位	敘述
金鑰使用限制	有關金鑰使用的限制（如果有）。
符合技術支援需求	根據產品授權期限，Kaspersky Lab 或合作夥伴是否提供客戶相關技術支援的資訊。
“其他”標籤	
關於產品授權的資訊	目前產品授權的編號和類型。
支援資訊	Kaspersky Lab 或其提供技術支援的合作夥伴的聯絡人詳細資訊。如果不提供技術支援，則此欄位可為空。
所有者資訊	有關產品授權客戶的資訊：客戶名稱和獲取產品授權的組織的名稱。

產品授權到期後的功能限制

目前產品授權到期後，功能元件的工作中套用以下限制：

- 除了“即時檔案防護”、“自訂掃描”和“應用程式完整性控制”工作以外，所有工作都將停止。
- 拒絕啟動除了“即時防護”、“自訂掃描”和“應用程式完整性控制”工作以外的所有工作。這些工作繼續使用舊的病毒資料庫執行。
- 弱點利用防禦功能受限：
  - 處理程序受防護至重新啟動為止。
  - 新處理程序無法新增到防護範圍中。

其他功能（儲存、記錄、診斷資訊）仍將可用。

續約產品授權

預設情況下，當產品授權還有 14 天就要到期時，Kaspersky Embedded Systems Security 2.2 會通知您這一情況。這種情況下，**Kaspersky Embedded Systems Security** 節點的詳細資訊視窗中的“**產品授權到期日期**”狀態將以黃色突出顯示。

您可以使用備用金鑰或啟動碼在產品授權到期之前續約產品授權。這可確保在現有產品授權到期後和您使用新的產品授權啟動應用程式之前繼續防護您的伺服器。

► *若要更新產品授權，請執行以下步驟：*

1. 購買新的啟動碼或金鑰檔案。
2. 在應用程式主控台樹狀目錄中，開啟“**授權**”節點。
3. 在“**授權**”節點的詳細資訊視窗中執行以下操作之一：
   - 如果您想要使用備用金鑰續約產品授權：
     a. 點擊“**新增**”連結。
     b. 在開啟的視窗中，點擊“**瀏覽**”按鈕並使用 .key 副檔名選擇新的授權檔案。
     c. 選中“**作為備用金鑰使用**”核取方塊。

- 如果您想要使用啟動碼續約產品授權：
  a. 點擊“**新增啟動碼**”連結。
  b. 在開啟的視窗中輸入購買的啟動碼。
  c. 選中“**作為備用金鑰使用**”核取方塊。

應用啟動碼需要網際網路連線。

4. 點擊“**確定**”。

目前 Kaspersky Embedded Systems Security 2.2 產品授權到期後，會新增並自動套用備用金鑰或啟動碼。

刪除金鑰

您可以刪除新增的金鑰。

如果向 Kaspersky Embedded Systems Security 2.2 新增了備用金鑰，並且您刪除了啟動金鑰，則備用金鑰會自動變為啟動金鑰。

如果您刪除所新增的金鑰，則可以透過重新套用金鑰檔案來將其還原。

► *刪除所新增的金鑰：*

1. 在應用程式主控台樹狀目錄中，選擇“**授權**”節點。
2. 在包含有關已新增金鑰的資訊的表格中的“**授權**”節點的詳細資訊窗格中，選擇您要刪除的金鑰。
3. 在包含有關所選金鑰的資訊的行的內容功能表中，選擇“**刪除**”。
4. 在確認視窗中點擊“**是**”按鈕以確認您希望刪除該金鑰。

選定的金鑰將被刪除。

啟動和停止 Kaspersky Embedded Systems Security 2.2 外掛程式

本節包含有關啟動和停止 Kaspersky Embedded Systems Security 2.2 管理外掛程式和 Kaspersky Security 服務的資訊。

本章內容

啟動 Kaspersky Embedded Systems Security 2.2 管理外掛程式

在卡巴斯基安全管理中心中啟動 Kaspersky Embedded Systems Security 2.2 管理外掛程式無需執行額外的操作。在管理員的電腦上安裝該外掛程式後，它會隨卡巴斯基安全管理中心同時啟動。有關啟動卡巴斯基安全管理中心的詳細資訊，請參見《*卡巴斯基安全管理中心說明*》。

啟動和停止 Kaspersky Security 服務

預設情況下，Kaspersky Security 服務會在作業系統啟動時自動啟動。Kaspersky Security 服務將管理執行“即時電腦防護”、“本機活動控制”、“自訂掃描”和更新工作的工作處理程序。

預設情況下，當 Kaspersky Embedded Systems Security 2.2 服務啟動時，將啟動“即時檔案防護”和“在作業系統啟動時掃描”工作以及其他排程在“**在應用程式啟動時**”啟動的工作。

如果停止 Kaspersky Security 服務，則會停止所有正在執行的工作。重新啟動 Kaspersky Security 服務之後，應用程式只會自動啟動其排程中已將啟動頻率設定為“**在應用程式啟動時**”的工作，而其他工作必須手動啟動。

您可以使用 **Kaspersky Embedded Systems Security** 節點的上下文功能表或使用 Microsoft Windows **服務**管理單元啟動和停止 Kaspersky Security 服務。

如果您是受防護電腦上“管理員”群組的成員，您可以啟動和停止應用程式。

► *要使用應用程式主控台停止或啟動應用程式，請執行以下步驟：*

1. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
2. 選擇以下之一項目：
   - **停止服務**
   - **啟動服務**

將啟用或停止 Kaspersky Security 服務。

Kaspersky Embedded Systems Security 2.2 功能的存取權限

本節包含有關 Kaspersky Embedded Systems Security 2.2 和應用程式註冊的 Windows 服務的管理權限的資訊，以及如何設定這些權限的說明。

本章內容

關於 Kaspersky Embedded Systems Security 2.2 的管理權限

預設情況下，為受防護電腦上的管理員群組的使用者，在安裝 Kaspersky Embedded Systems Security 2.2 的過程中在受防護電腦上建立的 ESS 管理員群組以及 SYSTEM 群組的使用者授予對所有 Kaspersky Embedded Systems Security 2.2 功能的存取權限。

有權限存取 Kaspersky Embedded Systems Security 2.2 的“**編輯**”權限功能的使用者可以向其他在受防護電腦上註冊的使用者或者該網域中包含的使用者授予對 Kaspersky Embedded Systems Security 2.2 功能的存取權限。

未在 Kaspersky Embedded Systems Security 2.2 使用者清單中註冊的使用者無法開啟應用程式主控台。

您可以為使用者或使用者群組選擇以下某一個預設的 Kaspersky Embedded Systems Security 2.2 存取權限等級：

- **完整控制** – 存取所有應用程式功能：可檢視和編輯 Kaspersky Embedded Systems Security 2.2 一般設定、元件設定、Kaspersky Embedded Systems Security 2.2 使用者權限，還可以檢視 Kaspersky Embedded Systems Security 2.2 統計。
- **編輯** – 存取除編輯使用者權限以外的所有應用程式功能：可以檢視和編輯 Kaspersky Embedded Systems Security 2.2 一般設定和 Kaspersky Embedded Systems Security 2.2 元件設定。
- **讀取** – 可以檢視 Kaspersky Embedded Systems Security 2.2 一般設定、Kaspersky Embedded Systems Security 2.2 元件設定、Kaspersky Embedded Systems Security 2.2 統計和 Kaspersky Embedded Systems Security 2.2 使用者權限。

您還可以配置進階存取權限（請參閱第 73 頁上的“配置 Kaspersky Embedded Systems Security 2.2 和 Kaspersky Security 服務的存取權限”部分）：允許或封鎖存取特定的 Kaspersky Embedded Systems Security 2.2 功能。

如果您已為某個使用者或群組手動設定存取權限，則為該使用者或群組設定“**特殊權限**”存取層級。

步驟 17. 關於 Kaspersky Embedded Systems Security 2.2 功能的存取權限

使用者權限	敘述
工作管理	可啟動/停止/暫停/還原 Kaspersky Embedded Systems Security 2.2 工作。
建立和刪除自訂掃描工作	可建立和刪除自訂掃描工作。
編輯設定	可執行以下操作： • 從設定檔匯入 Kaspersky Embedded Systems Security 2.2 設定。 • 編輯應用程式設定。
讀取設定	可執行以下操作： • 檢視一般 Kaspersky Embedded Systems Security 2.2 設定和工作設定。 • 將 Kaspersky Embedded Systems Security 2.2 設定匯出到設定檔。 • 檢視工作記錄、系統稽核記錄和通知設定。
管理儲存	可執行以下操作： • 將物件移到隔離。 • 從隔離和備份中刪除物件。 • 從隔離和備份中還原物件。
管理記錄	可刪除工作記錄和清除系統稽核記錄。
讀取記錄	可檢視工作記錄和系統稽核記錄中的病毒防護事件。
讀取統計	可檢視每個 Kaspersky Embedded Systems Security 2.2 工作的統計資訊。
應用程式授權	可以啟動或取消啟動 Kaspersky Embedded Systems Security 2.2。
移除應用程式	可移除 Kaspersky Embedded Systems Security 2.2。
讀取權限	可檢視 Kaspersky Embedded Systems Security 2.2 服務使用者清單和每個使用者的存取權限。
編輯權限	可執行以下操作： • 編輯具有應用程式管理存取權限的使用者清單。 • 編輯 Kaspersky Embedded Systems Security 2.2 功能的使用者存取權限。

關於 Kaspersky Security 服務的管理權限

在安裝過程中，Kaspersky Embedded Systems Security 2.2 在 Windows 中註冊 Kaspersky Security 服務 (KAVFS)，並在內部啟用在啟操作業系統時啟動的功能元件。為了降低協力廠商透過 Kaspersky Security 服務的管理存取應用程式功能和受防護電腦上安全設定的風險，可以從應用程式主控台或管理外掛程式限制管理 Kaspersky Security 服務的權限。

預設情況下，將管理 Kaspersky Security 服務的存取權限授予受防護電腦上“管理員”群組中的使用者，以及具有讀取權限的 SERVICE 和 INTERACTIVE 群組，和具有讀取和執行權限的 SYSTEM 群組。

您無法刪除 SYSTEM 使用者帳戶或編輯此帳戶的權限。如果編輯 SYSTEM 使用者帳戶權限，則當儲存變更時會還原此帳戶的最大權限。

有權存取“編輯權限”等級功能（請參見第 69 頁上的“關於 Kaspersky Embedded Systems Security 2.2 的管理權限”部分）的使用者可以向在受防護電腦上註冊的其他使用者或者該網域中包含的其他使用者授予用於管理 Kaspersky Security 服務的存取權限。

您可以為 Kaspersky Embedded Systems Security 2.2 使用者或使用者群組選擇以下預設的存取權限等級之一以管理 Kaspersky Security 服務：

- **完整控制**：可檢視和編輯 Kaspersky Security 服務的一般設定和使用者權限，以及啟動和停止 Kaspersky Security 服務。
- **讀取**：可檢視 Kaspersky Security 服務一般設定和使用者權限。
- **修改**：可檢視和編輯 Kaspersky Security 服務一般設定和使用者權限。
- **執行**：可啟動和停止 Kaspersky Security 服務。

您還可以設定進階存取權限：允許或拒絕存取指定的 Kaspersky Embedded Systems Security 2.2 功能（請參見下表）。

如果您已為某個使用者或群組手動設定存取權限，則為該使用者或群組設定“**特殊權限**”存取層級。

步驟 18. 限定 Kaspersky Embedded Systems Security 2.2 功能的存取權限

功能	敘述
檢視服務設定	檢視：可檢視 Kaspersky Security 服務一般設定和使用者權限。
從服務管理員請求服務狀態	可從 Microsoft Windows 服務控制管理員請求 Kaspersky Security 服務的執行狀態。
從服務請求狀態	可從 Kaspersky Security 服務請求服務執行狀態。
列出依存服務	可檢視 Kaspersky Security 服務依存的以及依存於 Kaspersky Security 服務的服務清單。
編輯服務設定	可檢視和編輯 Kaspersky Security 服務一般設定和使用者權限。
啟動服務	可啟動 Kaspersky Security 服務。
停止服務	可停止 Kaspersky Security 服務。

功能	敘述
暫停/還原服務	可暫停和還原 Kaspersky Security 服務。
讀取權限	可檢視 Kaspersky Security 服務使用者清單和每個使用者的存取權限。
編輯權限	可執行以下操作： • 新增和刪除 Kaspersky Security 服務使用者。 • 編輯 Kaspersky Security 服務的使用者存取權限。
刪除服務	可在 Microsoft Windows 服務控制管理員中取消註冊 Kaspersky Security 服務。
使用者定義的服務請求	可建立和傳送對 Kaspersky Security 服務的使用者請求。

將 Kaspersky Security 服務註冊為受防護服務

輕度受防護處理程序（也稱為“ PPL”）技術確保作業系統只載入受信任的服務和處理程序。對於要作為受防護服務執行的服務，必須在受防護電腦上安裝*早期啟動惡意軟體防護*驅動程式。

早期啟動惡意軟體防護（也稱為“ ELAM”）驅動程式在網路中的電腦啟動時及協力廠商驅動程式初始化之前為這些電腦提供防護。

ELAM 驅動程式在 Kaspersky Embedded Systems Security 2.2 安裝期間自動安裝，用於在作業系統啟動時將 Kaspersky Security 服務註冊為 PPL。Kaspersky Security 服務 (kavfs.exe) 作為系統防護處理程序啟動後，系統中的其他非受防護處理程序將不能注入執行緒、寫入受防護處理程序的虛擬記憶體或停止服務。

當某個處理程序以 PPL 的形式啟動時，使用者無法對其進行管理，不管分配的使用者權限如何。Microsoft Windows 10 及更高版本作業系統支援使用 ELAM 驅動程式將 Kaspersky Security 服務註冊為 PPL。如果在執行支援 PPL 的作業系統的電腦上安裝 Kaspersky Embedded Systems Security 2.2，Kaspersky Security 服務 (KAVFS) 的權限管理將不可用。

Kaspersky Security 服務會將所有子處理程序作為 PPL 啟動。

► *要將 Kaspersky Embedded Systems Security 2.2 安裝為 PPL，請執行以下指令：*

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

您可以使用命令列配置 PPL 使用。

關於 Kaspersky Security 管理服務的存取權限

您可以檢視 Kaspersky Embedded Systems Security 2.2 服務的清單。

在安裝 Kaspersky Embedded Systems Security 2.2 會註冊 Kaspersky Security 管理服務 (KAVFSGT)。若要透過安裝在其他電腦上的應用程式主控台來管理應用程式，使用其權限與 Kaspersky Embedded Systems Security 2.2 建立連線的帳戶必須對受防護電腦上的 Kaspersky Security 管理服務具有完全存取權限。

預設情況下，系統向以下兩組使用者授予存取 Kaspersky Security 管理服務的權限：受防護電腦上的管理員群組的使用者，以及安裝 Kaspersky Embedded Systems Security 2.2 時在受防護電腦上建立的 ESS 管理員群組的使用者。

您只能透過 Microsoft Windows 的“**服務**”管理單元來管理 Kaspersky Security 管理服務。

您不能透過配置 Kaspersky Embedded Systems Security 2.2 來允許或封鎖使用者存取 Kaspersky Security 管理服務。

如果在受防護電腦上註冊相同的帳戶名稱和密碼，那麼您可以從本機帳戶連線到 Kaspersky Embedded Systems Security 2.2。

配置 Kaspersky Embedded Systems Security 2.2 和 Kaspersky Security 服務的存取權限

您可以編輯允許存取 Kaspersky Embedded Systems Security 2.2 功能和管理 Kaspersky Security 服務的使用者和使用者群組清單，還可以編輯這些使用者和使用者群組的存取權限。

► *要從清單中新增或刪除使用者或群組：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**選項**”部分，執行以下步驟之一：

   - 如果您希望編輯具有管理 Kaspersky Embedded Systems Security 2.2 功能的存取權限的使用者清單，請選擇“**應用程式管理的使用者存取權限**”。
   - 如果您希望編輯具有 Kaspersky Security 服務管理存取權限的使用者清單，請選擇“**Security 服務管理的使用者存取權限**”。

     將開啟“**Kaspersky Embedded Systems Security 2.2 群組權限**”視窗。

4. 在開啟的視窗中，執行以下操作：

   - 要向清單中新增使用者或群組，請點擊“**新增**”按鈕，然後選擇要授予權限的使用者或群組。
   - 要從清單中刪除使用者或群組，請選擇要限制其存取權限的使用者或群組，然後點擊“**刪除**”按鈕。

5. 點擊“**套用**”按鈕。

將新增或刪除所選使用者（群組）。

► *要編輯使用者或群組對管理 Kaspersky Embedded Systems Security 2.2 或 Kaspersky Security 服務的權限：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：

   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**選項**”部分，執行以下步驟之一：

   - 如果您希望編輯具有管理 Kaspersky Embedded Systems Security 2.2 功能的存取權限的使用者清單，請選擇“**修改應用程式管理的使用者權限**”。
   - 如果您希望編輯具有透過 Kaspersky Security 服務管理應用程式的存取權限的使用者清單，請選擇“**修改 Kaspersky Security 服務管理的使用者權限**”。

     將開啟“**Kaspersky Embedded Systems Security 群組權限**”視窗。

4. 在開啟的視窗的“**群組**或使用者”清單中，選擇要變更其權限的使用者或使用者群組。

5. 在“**群組‘ <使用者（群組）>’的權限**”部分中，選中與以下存取權限等級對應“**允許**”或“**封鎖**”核取方塊：
   - **完整控制**：管理 Kaspersky Embedded Systems Security 2.2 或 Kaspersky Security 服務的全套權限。
   - **讀取**：
     - 以下權限用於管理 Kaspersky Embedded Systems Security 2.2：**檢索統計資訊**、**讀取設定**、**讀取記錄**和**讀取權限**。
     - 以下權限用於管理 Kaspersky Security 服務：**讀取服務設定**、**從服務控制管理員請求服務狀態**、**從服務請求狀態**、**讀取依存服務清單**、**讀取權限**。
   - **修改**：
     - 除**編輯權限**之外的所有 Kaspersky Embedded Systems Security 2.2 管理權限。
     - 以下權限用於管理 Kaspersky Security 服務：**修改服務設定**、**讀取權限**。
   - **執行**：以下權限用於管理 Kaspersky Security 服務：**正在啟動服務**、**正在停止服務**、**暫停/還原服務**、**讀取權限**、**使用者定義的服務請求**。
6. 要配置某個使用者或群組的進階權限設定（**特殊權限**），請點擊“**進階**”按鈕。
   a. 在開啟的“**Kaspersky Embedded Systems Security 2.2 進階安全設定**”視窗中，選擇所需的使用者或群組。
   b. 點擊“**編輯**”按鈕。
   c. 在視窗頂部的下拉清單中，選擇存取控制類型（“**允許**”或“**封鎖**”）。
   d. 選中與要為所選使用者或組允許或封鎖的功能對應的核取方塊。
   e. 點擊“**確定**”。
   f. 在“**Kaspersky Embedded Systems Security 2.2 的進階安全設定**”視窗中，點擊“**確定**”。
7. 在“**Kaspersky Embedded Systems Security 的權限**”群組視窗中，點擊“**套用**”按鈕。

已配置的管理 Kaspersky Embedded Systems Security 2.2 或 Kaspersky Security 服務的權限將被儲存。

對 Kaspersky Embedded Systems Security 2.2 功能進行受密碼防護的存取

您可透過配置使用者權限來限制對應用程式管理和已註冊服務的存取（請參見第 69 頁上的“Kaspersky Embedded Systems Security 2.2 功能的存取權限”部分）。您也可在 Kaspersky Embedded Systems Security 2.2 設定中設定密碼防護，以為關鍵操作的執行提供額外防護。

當您嘗試存取以下應用程式功能時，Kaspersky Embedded Systems Security 2.2 會請求密碼：

- 連線到應用程式主控台；
- 移除 Kaspersky Embedded Systems Security 2.2；
- 修改 Kaspersky Embedded Systems Security 2.2 元件；
- 執行命令列指令。

Kaspersky Embedded Systems Security 2.2 介面會在螢幕上隱藏指定密碼。Kaspersky Embedded Systems Security 2.2 將密碼儲存為指定密碼時計算得出的校驗和。

您可匯出並匯入受密碼防護的應用程式配置。由於匯出受防護應用程式配置建立的設定檔包含密碼校驗和以及用於填充密碼字串修飾符的值。

請勿變更設定檔中的校驗和或修飾符。匯入已手動變更的密碼防護配置可能會導致存取應用程式完全被封鎖。

► *若要防護對 Kaspersky Embedded Systems Security 2.2 功能的存取，請執行下列步驟：*

1. 在卡巴斯基安全管理中心的管理主控台樹狀目錄中，展開“**受管理裝置**”節點。展開包含要設定其應用程式設定的電腦的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要設定電腦組的政策設定，請選擇“**政策**”標籤，然後開啟“**<政策名稱> > 內容**”。
   - 如果您想要配置單台電腦的應用程式設定，在卡巴斯基安全管理中心中的**應用程式設定**視窗中開啟所需設定（請參見第 90 頁上的“**在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作**”部分）。
3. 在“**安全**”部分，點擊“**設定**”按鈕。

   將開啟“**安全性設定**”視窗。
4. 在“**密碼防護設定**”部分中，選中“**套用密碼防護**”核取方塊。

   “**密碼**”和“**確認密碼**”欄位變為活動狀態。
5. 在“**密碼**”欄位中，輸入想要用於防護對 Kaspersky Embedded Systems Security 2.2 功能進行存取的值。
6. 在“**確認密碼**”欄位中，再次輸入您的密碼。
7. 點擊“**確定**”。

將儲存指定設定。Kaspersky Embedded Systems Security 2.2 將請求指定密碼以便存取受防護的功能。

此密碼無法還原。遺失密碼會導致完全失去對應用程式的控制。此外，還將無法從受防護電腦移除應用程式。

可以隨時變更或重設應用程式設定中指定的密碼。

► *要重設密碼，*

請清除政策或應用程式設定中的“**套用密碼防護**”核取方塊。

密碼防護將被停用。Kaspersky Embedded Systems Security 2.2 會從應用程式設定刪除舊密碼校驗和。

為 Kaspersky Security 管理服務啟用網路連線

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

► *若要允許受防護電腦上的 Kaspersky Security 管理服務連線網路，請執行以下步驟：*

1. 在執行 Microsoft Windows 的受防護電腦上，選擇“**開始 > 主控台 > 安全性 > Windows 防火牆**”。
2. 在“**Windows 防火牆設定**”視窗中，選擇“**變更設定**”。
3. 在“**排除**”標籤上的預定排除項目清單中，選中以下核取方塊：“**COM + 網路存取**”、“**Windows Management Instrumentation (WMI)**”和“**遠端管理**”。
4. 點擊“**新增程式**”按鈕。
5. 在“**新增程式**”視窗中選擇 kavfsgt.exe 檔案。此檔案儲存在您在應用程式主控台的安裝過程中指定為目的資料夾的資料夾中。
6. 點擊“**確定**”。
7. 在“**Windows 防火牆設定**”視窗中點擊“**確定**”。

將允許受防護電腦上的 Kaspersky Security 管理服務連線網路。

建立和設定政策

本節提供有關使用卡巴斯基安全管理中心政策在多台電腦上管理 Kaspersky Embedded Systems Security 2.2 的資訊。

本章內容

關於政策

可以建立全域性卡巴斯基安全管理中心政策，以便管理多台安裝了 Kaspersky Embedded Systems Security 2.2 的電腦上的防護。

政策在一個管理群組中所有受防護電腦上實行該政策中指定的 Kaspersky Embedded Systems Security 2.2 設定、功能和工作。

可以為一個管理群組依次建立和實行多個政策。在管理主控台中，目前對某個群組有效的政策具有*活動*狀態。

Kaspersky Embedded Systems Security 2.2 系統稽核記錄中記錄了有關政策實行情況的資訊。可在應用程式主控台的“**系統稽核記錄**”節點中檢視該資訊。

卡巴斯基安全管理中心提供一種在本機電腦上套用政策的方式：*禁止變更設定*。當某個政策啟動時，Kaspersky Embedded Systems Security 2.2 將使用政策內容中所選 🔒 圖示旁的設定值，而不是使用套用政策前的這些設定值。Kaspersky Embedded Systems Security 2.2 不會套用政策內容中在其旁邊選擇了 🔓 圖示的活動政策設定的值。

如果政策為活動的，則政策中標記 🔒 圖示的設定的值在應用程式主控台中顯示，但無法編輯。其他設定的值（政策中標記 🔓 圖示）可在應用程式主控台中編輯。

活動政策中配置的且標記 🔒 圖示的設定也會封鎖在“**內容：<電腦名稱>**”視窗中變更一台電腦的卡巴斯基安全管理中心。

在停用活動政策後，使用活動政策指定併傳送到本機電腦的設定將儲存在本機工作設定中。

如果政策為任何“即時防護”工作定義設定時，此工作若正在執行中，則一旦套用政策，便將立即修改該政策所定義的設定。如果該工作未執行，就會在啟動時套用其設定。

建立政策

建立政策的過程涉及下列步驟：

1. 使用政策精靈建立政策。可以使用精靈對話方塊配置即時電腦防護工作設定。
2. 配置政策設定。在已建立政策的“**內容：<政策名稱>**”視窗中，您可以定義即時電腦防護工作設定、Kaspersky Embedded Systems Security 2.2 一般設定、隔離和備份設定、工作記錄的詳細等級以及有關 Kaspersky Embedded Systems Security 2.2 事件的使用者和管理員通知。

► *若要為一組執行已安裝 Kaspersky Embedded Systems Security 2.2 的電腦建立政策，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇包含您希望為其建立政策的電腦的管理群組。
2. 在選定管理群組的詳細資訊視窗中，選擇“**政策**”標籤，然後點擊“**建立政策**”連結以啟動精靈並建立政策。

   將開啟“**新建政策精靈**”視窗。
3. 在“**選擇要為其建立群組政策的應用程式**”視窗中，選擇 Kaspersky Embedded Systems Security 2.2，然後點擊“**下一步**”。
4. 在“**名稱**”欄位中**輸入群組政策名稱**。

   政策名稱不能包含以下符號：" * < : > ? \ |。
5. 要套用先前應用程式版本使用的政策設定：
   a. 選中“**使用先前應用程式版本的政策設定**”核取方塊。
   b. 點擊“**瀏覽**”按鈕，然後選擇要套用的政策。
   c. 點擊“**下一步**”。
6. 在“**選擇操作類型**”視窗中，選擇以下選項之一：
   - “**新增**”，以建立具有預設設定的新政策。
   - “**匯入使用以前版本的 Kaspersky Embedded Systems Security 建立的政策**”，以將該版本政策用作範本。
   - 點擊“**瀏覽**”，然後選擇儲存現有政策的設定檔。
7. 在“**即時電腦防護**”視窗中，根據需要配置“即時檔案防護”、“KSN 使用”工作和弱點利用防禦功能。允許或封鎖在網路上的本機電腦上使用配置的政策工作：
   - 點擊 🔒 按鈕允許變更網路電腦上的工作設定，並封鎖套用政策中配置的工作設定。
   - 點擊 🔓 按鈕拒絕變更網路電腦上的工作設定，並允許套用政策中配置的工作設定。

   新建立的政策使用“即時電腦防護”工作的預設設定。
   - 要編輯“即時檔案防護”工作的預設設定，請點擊“**即時檔案防護**”部分中的“**設定**”按鈕。在開啟的視窗中，根據需要設定工作。點擊“**確定**”。
   - 要編輯“KSN 使用”工作的預設設定，請點擊“**KSN 使用**”部分中的“**設定**”按鈕。在開啟的視窗中，根據需要設定工作。點擊“**確定**”。

要啟動“ KSN 使用”工作，您需要接受“資料處理”視窗中的 KSN 聲明（請參見第 149 頁上的“設定資料處理”部分）。

- 要編輯“弱點利用防禦”工作的預設設定，請點擊“**弱點利用防禦**”部分中的“**設定**”按鈕。在開啟的視窗中，根據需要設定該功能。點擊“**確定**”。

8. 在“**為應用程式建立群組政策**”視窗中選擇下列之一的政策狀態：
   - “**活動政策**”，如果您希望在建立政策後立即套用該政策。如果群組中已經存在活動政策，則會將其停用並套用新政策。
   - “**非活動政策**”，如果您不希望立即套用所建立的政策。在此情況下，可在之後啟動該政策。
   - 選中“**建立政策後立即開啟政策內容**”核取方塊以在點擊“**下一步**”按鈕後自動關閉**新建政策精靈**並設定新建立的政策。
9. 在精靈的“**完成精靈**”視窗中點擊“**完成**”按鈕。

所建立的政策將顯示在選定管理群組的“**政策**”標籤上的政策清單中。在“**內容：<政策名稱>**”視窗中，您可配置 Kaspersky Embedded Systems Security 2.2 的其他設定、工作和功能。

設定政策

在現有政策的“**內容：<政策名稱>**”視窗中，您可以配置 Kaspersky Embedded Systems Security 2.2 一般設定、隔離和備份設定、受信任區域設定、即時防護設定、本機活動控制設定、工作記錄的詳細資訊等級以及有關 Kaspersky Embedded Systems Security 2.2 事件的使用者和管理員通知，用於管理應用程式和 Kaspersky Security 服務的存取權限以及政策設定檔應用程式設定。

► *要配置政策設定：*

1. 在卡巴斯基安全管理中心的管理主控台樹狀目錄中展開“**受管理裝置**”節點。
2. 展開您要為其配置政策設定的管理群組，然後在詳細資訊視窗中選擇“**政策**”子節點。
3. 選擇您設定的政策並使用以下方式之一開啟“**內容：<政策名稱>**”視窗：
   - 在政策的內容功能表中選擇“**內容**”選項。
   - 在所選政策的右側詳細資訊視窗中，點擊“**配置政策**”連結。
   - 雙擊所選政策。
4. 在“**政策狀態**”部分的“**一般**”標籤下，啟用或停用政策。為此，請選擇以下一個選項：
   - **活動政策**，如果您希望在選定管理群組內的所有電腦上套用政策。
   - **非活動政策**，如果您不希望在選定群組內的所有電腦上套用政策。

   當管理 Kaspersky Embedded Systems Security 2.2 時，“**不在辦公室政策**”設定不可用。
5. 在“**事件通知**”、“**應用程式設定**”、“**記錄和通知**”、“**選項**”、“**修訂歷史**”部分中，可以修改應用程式配置（請參見以下表格）。

6. 在“**即時電腦防護**”、“**本機活動控制**”、“**網路活動控制**”和“**系統稽核**”部分中，配置應用程式設定和應用程式啟動設定（請參見以下表格）。

   您可透過卡巴斯基安全管理中心政策啟用或停用在管理群組內的所有電腦上執行任何工作。
   您可為每個單個軟體元件配置在所有網路電腦上套用政策設定。

7. 點擊“**確定**”。

將在政策中套用配置的設定。

有關如何透過應用程式主控台配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

Kaspersky Embedded Systems Security 2.2 政策設定章節

一般

在“**一般**”部分中，您可配置以下政策設定：

- 指定政策狀態。
- 為子政策設定繼承父政策的設定。

事件通知

在“**事件通知**”部分中，您可配置以下事件類別的設定：

- *緊急事件*
- *已失敗*
- *警告*
- *資訊事件*

可以使用“**內容**”按鈕來配置選定事件的以下設定：

- 指定有關記錄事件的資訊的儲存位置和保留期限。
- 指定有關記錄事件的通知方式。

應用程式設定

步驟 19. 應用程式設定的設定部分

章節	選項
延伸性和介面	在“**延伸性和介面**”部分中，可以點擊“**設定**”按鈕來配置以下設定： • 選擇手動或自動配置延伸性設定。 • 配置應用程式圖示顯示設定。
安全性	在“**安全性和可靠性**”部分中，可以點擊“**設定**”按鈕來配置以下設定： • 配置工作執行設定。 • 指定當電腦使用 UPS 電源執行時應用程式的行為。 • 啟用或停用應用程式功能的密碼防護。

章節	選項
連線	在“**連線**”部分中，可以使用“**設定**”按鈕來配置與更新伺服器、啟動伺服器和 KSN 連線的以下代理伺服器設定： • 配置代理伺服器設定。 • 指定代理伺服器身分驗證設定。
執行系統工作	在“**執行系統工作**”子部分中，可以使用“**設定**”按鈕來根據本機電腦上配置的排程允許或封鎖啟動以下系統工作： • 自訂掃描工作。 • 更新工作和複製更新工作。

選項

步驟 20.　選項的設定部分

章節	選項
信任區域	點擊“**信任區域**”部分上的“**設定**”按鈕，以設定以下信任區域應用程式設定： • 建立信任區域排除項目清單。 • 啟用或停用檔案備份操作的掃描。 • 建立受信任處理程序清單。
卸除式磁碟機掃描	點擊“**設定**”按鈕以配置卸除式 USB 磁碟機的掃描設定。
應用程式管理的使用者存取權限	在此部分中，您可以配置用於管理 Kaspersky Embedded Systems Security 2.2 的使用者權限和使用者群組權限。
Security 服務管理的使用者存取權限	在此部分中，您可以配置用於管理 Kaspersky Security 服務的使用者權限和使用者群組權限。
儲存	在“**儲存**”了部分中，點擊“**設定**”按鈕以配置以下“隔離”和“備份”設定： • 指定想要放置隔離或備份物件的資料夾路徑。 • 設定備份和隔離的最大大小，並指定可用空間上限值。 • 指定想要放置隔離或備份還原物件的資料夾路徑。 • 設定關於隔離和備份物件到管理伺服器的資訊的傳輸。

即時電腦防護

步驟 21. “即時電腦防護的設定”部分

章節	選項
即時檔案防護	在“**即時檔案防護**”部分中，可以點擊“**設定**”按鈕來配置以下工作設定： • 指定防護模式。 • 配置啟發式分析的使用。 • 配置信任區域的使用。 • 指定防護範圍。 • 設定選定防護範圍的安全等級：您可選擇預設的安全等級或手動設定安全設定。 • 配置工作啟動設定。
KSN 使用	在“**KSN 使用**”子部分中，可以點擊“**設定**”按鈕來配置以下工作設定： • 指定要對 KSN 不信任的物件執行的操作。 • 配置卡巴斯基安全管理中心作為 KSN 代理伺服器的資料傳輸和使用。 點擊“**資料處理**”按鈕可接受或拒絕 KSN 聲明，並設定可靠的資料交換設定。
弱點利用防禦	在“**弱點利用防禦**”部分中，可以點擊“**設定**”按鈕來配置以下工作設定： • 選擇處理程序記憶體防護模式。 • 指定降低弱點利用風險的操作。 • 新增到和編輯受防護的處理程序清單。

本機活動控制

步驟 22. 本機活動控制的設定部分

章節	選項
應用程式啟動控制	在“**應用程式啟動控制**”部分中，可以點擊“**設定**”按鈕來配置以下工作設定： • 選擇工作執行模式。 • 配置控制隨後應用程式啟動的設定。 • 指定應用程式啟動控制規則的套用範圍。 • 配置 KSN 的使用。 • 配置工作啟動設定。
裝置控制	在“**裝置控制**”部分中，可以點擊“**設定**”按鈕來配置以下工作設定： • 選擇工作執行模式。 • 配置工作啟動設定。

網路活動控制

步驟 23. 網路活動控制的設定部分

章節	選項
防火牆管理	在“**防火牆管理**”部分中，可以點擊“**設定**”按鈕來配置以下工作設定： • 刪除防火牆規則。 • 配置工作啟動設定。

系統稽核

步驟 24. 系統稽核的設定部分

章節	選項
檔案完整性監控	在“**檔案完整性監控**”部分中，可以配置對表示受防護電腦上存在安全衝突的檔案變更的控制。
記錄審查	在“**記錄審查**”部分中，可以根據 Windows 事件記錄分析結果配置受防護電腦的完整性控制。

記錄和通知

步驟 25. 記錄和通知的設定部分

章節	選項
工作記錄	在“**工作記錄**”部分中，可以點擊“**設定**”按鈕以配置以下設定： • 為選定的軟體元件指定記錄事件的重要性等級。 • 指定工作記錄儲存設定。 • 指定 SIEM 與卡巴斯基安全管理中心整合的設定。
事件通知	在“**事件通知**”部分中，可以點擊“**設定**”按鈕以配置以下設定： • 指定*偵測到物件*事件的使用者通知設定。 • 為“**通知設定**”部分中的事件清單中選定的任何事件指定管理員通知設定。
與管理伺服器互動	在**與管理伺服器互動**部分中，可以點擊**設定**按鈕來選擇 Kaspersky Embedded Systems Security 2.2 將報告給管理伺服器的物件類型。

修訂歷史

在“**修訂歷史**”部分中，可以管理修訂：與目前版本或其他政策對比、新增修訂說明、儲存修訂到檔案或執行回溯。

設定本機系統工作的排程啟動

您可以使用政策，根據管理群組中的每台電腦上本機配置的排程允許或封鎖，啟動本機系統自訂掃描工作和更新工作：

- 如果特定類型的本機系統工作的排程啟動受到政策禁止，則這些工作將不會按照排程在本機電腦上執行。您可以手動啟動該本機系統工作。
- 如果特定類型的本機系統工作的排程啟動被政策允許，則這些工作將按照為此工作進行的本機配置的排程參數來執行。

預設情況下，政策會禁止本機系統工作的啟動。

如果更新或自訂掃描受卡巴斯基安全管理中心群組工作的管理，我們建議不要允許本機系統工作啟動。

如果您不使用群組更新或自訂掃描工作，請在政策中允許本機系統工作啟動 :Kaspersky Embedded Systems Security 2.2 將執行應用程式資料庫和模組更新，並按照預設排程啟動所有本機系統自訂掃描工作。

您可使用政策允許或封鎖以下本機系統工作的排程啟動：

- 自訂掃描工作：關鍵區域掃描、隔離區掃描、在作業系統啟動時掃描、軟體模組完整性檢查。
- 更新工作：資料庫更新、軟體模組更新和複製更新。

如果受防護的電腦從管理群組中排除，則系統工作排程將自動啟用。

► *要在政策中允許或封鎖 Kaspersky Embedded Systems Security 2.2 系統工作的排程啟動，請執行以下步驟：*

1. 展開管理主控台中的“**管理服務**”節點，展開所需的群組並在“**政策**”節點中選擇該群組。
2. 在“**政策**”標籤上，在用於配置電腦群組上的 Kaspersky Embedded Systems Security 2.2 系統工作排程啟動的政策的內容功能表，選擇“**內容**”指令。
3. 在“**內容：<政策名稱>**”視窗中，開啟“**應用程式設定**”部分。在“**執行系統工作**”部分中，點擊“**設定**”按鈕並執行以下操作：
   - 選中“**允許啟動自訂掃描工作**”和“**允許啟動更新工作和複製更新工作**”核取方塊以允許所列工作的排程啟動。
   - 清除“**允許啟動自訂掃描工作**”和“**允許啟動更新工作和複製更新工作**”核取方塊以停用所列工作的排程啟動。

   選擇或清除該核取方塊將不會影響任何此類本機自訂工作的啟動設定。
4. 確保您所配置的政策（請參見第 78 頁上的“關於政策”部分）為活動政策且套用於所選電腦群組。
5. 點擊“**確定**”。

將為選定工作應用配置的排程工作啟動設定。

使用卡巴斯基安全管理中心建立和管理工作

本節包含有關 Kaspersky Embedded Systems Security 2.2 工作、如何建立工作、配置工作設定，以及啟動和停止工作的資訊。

本章內容

關於卡巴斯基安全管理中心中的工作建立

您可為管理群組和電腦集建立群組工作。您可建立以下工作類型：

- 啟動應用程式
- 複製更新
- 資料庫更新
- 軟體模組更新
- 資料庫更新回溯
- 自訂掃描
- 應用程式完整性控制
- 應用程式啟動控制規則產生器
- 裝置控制規則產生器

您可採用以下方式建立本機和群組工作：

- 對於一台電腦：在“**內容 <電腦名稱>**”視窗的“**工作**”部分中。
- 對於管理群組：在選定電腦群組的節點的詳細資訊視窗中的“**工作**”標籤上。
- 對於一組電腦：在“**裝置選擇**”節點的詳細資訊視窗中。

使用政策可以停用同一管理群組的所有受防護電腦上的更新和自訂掃描本機系統工作的排程（請參見第 84 頁上的“配置本機系統工作的排程啟動”部分）。

有關卡巴斯基安全管理中心工作的一般資訊，請參閱*卡巴斯基安全管理中心說明*。

使用卡巴斯基安全管理中心建立工作

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *要在卡巴斯基安全管理中心管理主控台中建立新工作：*

1. 採用以下方式之一啟動工作精靈：
   - 若要建立本機工作，請執行以下步驟：
     a. 展開管理主控台樹狀目錄中的“**受管理裝置**”節點，並選擇受防護電腦所屬的群組。
     b. 在詳細資訊視窗的“**裝置**”標籤上，開啟受防護電腦的內容功能表，然後選擇“**內容**”。
     c. 在開啟的視窗中，在“**工作**”部分中點擊“**新增**”按鈕。
   - 建立群組工作：
     a. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其建立工作的群組。
     b. 在詳細資訊視窗中，開啟“**工作**”標籤，然後選擇“**建立工作**”。
   - 要為自訂的一組電腦建立工作，請在卡巴斯基安全管理中心管理主控台樹狀結構中的“**裝置選擇**”節點中，選擇“**建立工作**”。

   將開啟工作精靈視窗。
2. 在標題 **Kaspersky Embedded Systems Security 2.2** 下的“**選擇工作類型**”視窗中，選擇要建立的工作的類型。

3. 如果選擇了除“資料庫更新回溯”或“應用程式啟動”外的任何工作類型，將開啟“**設定**”視窗。根據建立的工作類型，執行下列一種操作：

   - *建立自訂掃描工作*：

     a. 在“**掃描範圍**”視窗中建立掃描範圍。

     根據預設，掃描範圍包括電腦的關鍵區域。掃描範圍在表格中使用圖示 ☑ 標記。

     掃描範圍可以修改：新增特定的預先定義的掃描範圍、磁碟、資料夾及檔案，並為每個新增的範圍指定特定的安全設定。

     - 要從掃描中排除所有關鍵區域，請在每行上開啟內容功能表並選擇“**刪除範圍**”選項。
     - 若要包含預先定義的掃描範圍、磁碟、資料夾、網路物件或檔案，請在“**掃描範圍**”表格上開啟內容功能表並選擇“新增範圍”。在“**新增物件至掃描範圍**”視窗中，選擇“**預設的範圍**”清單中的預設範圍，指定電腦或另外一台網路電腦上的電腦磁碟、資料夾、網路物件或檔案，然後點擊“**確定**”按鈕。
     - 若要從掃描中排除子資料夾或檔案，請在精靈的“**掃描範圍**”視窗中選擇新增的資料夾（磁碟），開啟內容功能表並選擇“**配置**”選項，然後點擊“安全等級”視窗中的“**設定**”按鈕，並在“**自訂掃描**”視窗的“**一般**”標籤中，取消選定“**子資料夾**”和“**子檔案**”）核取方塊。
     - 若要變更掃描範圍安全設定，請在要設定其設定的範圍上開啟內容功能表，然後選擇“**配置**”。在“**自訂掃描設定**”視窗中，選擇預設的安全等級之一，或者點擊“**設定**”按鈕以手動配置安全設定。執行安全設定配置的方式與 Kaspersky Embedded Systems Security 2.2 主控台中相同。
     - 若要略過新增的掃描範圍中的內建物件，請在“**掃描範圍**”表中開啟上下文功能表，選擇“**新增排除項目**”並指定要排除的物件：選擇“預設的範圍”清單中的預設範圍，指定受防護電腦或另外一台網路電腦上的電腦磁碟、資料夾、網路物件或檔案，然後點擊“**確定**”按鈕。
     - 排除的掃描範圍在表中用圖示 ☐ 標記。

     b. 在“**選項**”視窗中執行下列操作。

     如果您希望從工作的掃描範圍中排除 Kaspersky Embedded Systems Security 2.2 信任區域中敘述的物件，則選中“**套用信任區域**”核取方塊。

     如果您排程使用所建立的工作作為關鍵區域掃描工作，請選中“**選項**”視窗中的“**在背景模式下執行工作**”核取方塊。卡巴斯基安全管理中心根據狀態為“*關鍵區域掃描*”的工作執行結果來評估電腦的安全等級，而不僅僅是根據“**關鍵區域掃描**”系統工作的執行結果來進行評估。在建立本機自訂掃描工作時，此核取方塊將無法使用。

     若要向將執行該工作的程序分配基本優先順序“**低**”，請在“**選項**”視窗中選定“**在背景模式下執行工作**”核取方塊。預設情況下，執行 Kaspersky Embedded Systems Security 2.2 工作程序的優先順序為“**中度**”（正常）。將程序的優先順序降低會增加執行工作所需的時間，但是可以對提高其他活動程式的執行速度有所幫助。

- *要建立更新工作*，請根據您的需要配置工作設定：

  a. 在“**更新來源**”視窗中選擇更新來源。

  b. 點擊“**連線設定**”按鈕。將開啟“**連線設定**”視窗。

  c. 在“**連線設定**”視窗上：

     指定 FTP 伺服器模式以便連線到受防護的電腦。

     根據需要修改連線到更新源來時的連線逾時值。

     配置連線到更新來源時的代理伺服器存取設定。

     指定受防護電腦的位置，以便優化更新下載。

- *若要建立“軟體模組更新”工作*，請在“**有關應用程式軟體模組更新的設定**”視窗中配置所需程式模組更新設定：

  a. 選擇複製並安裝重要更新，或者僅檢查它們的可用性而不安裝。

  b. 如果選擇了“**複製並安裝軟體模組的重要更新**”：可能需要重新啟動電腦才能套用已安裝的軟體模組。如果希望工作完成時 Kaspersky Embedded Systems Security 2.2 自動重新啟動電腦，請選定“**允許作業系統重新啟動**”核取方塊。若要停用在工作完成後自動重新啟動電腦的功能，請取消選定“**允許作業系統重新啟動**”核取方塊。

  c. 若要獲得有關 Kaspersky Embedded Systems Security 2.2 模組升級的資訊，請選擇“**接收有關可用的排程軟體模組更新的資訊**”。

     Kaspersky Lab 不會在更新伺服器上發佈排程的軟體更新套件以供自動安裝；您可以手動從 Kaspersky Lab 網站下載這些軟體更新套件。您可以設定有關“**有新的排程軟體模組更新可用**”事件的管理員通知。該通知將包含我們網站的 URL，以便您從中下載排程的更新。

- *若要建立“複製更新”工作*，請在“**複製更新設定**”視窗中指定更新和目的資料夾。

- *若要建立“應用程式啟動”工作*，請在“**啟動設定**”視窗中，套用您要用於啟動應用程式的金鑰檔案。如果您想要建立用於續約產品授權的工作，請選中“**作為備用金鑰使用**”核取方塊。

- *若要建立“應用程式啟動控制規則產生器”工作或“裝置控制規則產生器”工作*，請在“**設定**”視窗中，指定建立允許規則清單所依據的設定：

  a. 指定規則名稱的前置詞（僅適用於“應用程式啟動控制規則產生器”工作）。

  b. 配置以下規則的使用範圍（僅適用於“應用程式啟動控制規則產生器”工作）。點擊“**下一步**”按鈕。

  c. 指定建立允許規則時和工作完成後允許工作將執行的操作（僅適用於“應用程式啟動控制規則產生器”工作）。

4. 配置工作排程（可以為除“資料庫更新回溯”工作以外的所有工作類型配置排程）。在“**排程**”視窗中執行下列操作：

   a. 選定“**依排程執行**”核取方塊以啟用排程；

   b. 指定工作啟動頻率：從“**週期**”清單中選擇以下值之一：**每小時**、**每天**、**每週**、**在應用程式啟動時**、**應用程式資料庫更新後**（也可在以下群組工作中指定啟動頻率“**管理伺服器擷取更新後**”：資料庫更新和軟體模組更新）：

      - 如果選擇了“**每小時**”，請在“**工作開始設定**”配置群組的“**每 <數量> 小時**”中指定小時數。
      - 如果選擇了“**每天**”，請在“**工作開始設定**”配置群組的“**每 <數量> 天**”中指定天數。
      - 如果選擇了“**每週**”，請在“**工作開始設定**”配置群組的“**每 <數量> 週**”中指定週數。指定工作將會在一週中啟動的日期（預設為每週一）。

c. 在“**開始時間**”欄位中，指定工作啟動的時間；在“**開始日期**”欄位中，指定排程生效的日期。

d. 若有需要，指定剩餘的排程設定：按下“**進階**”按鈕並在“**進階排程設定**”視窗中執行下列操作：

- 指定工作執行的最長持續時間：在“**工作停止設定**”配置群組的“**持續時間**”欄位中輸入小時和分鐘數。
- 若要指定 24 小時期間內工作執行暫停的時間間隔，請在“**工作停止設定**”配置群組中的“**暫停開始時間**”和“**結束時間**”欄位中輸入間隔的開始和結束值。
- 若要指定停用排程的日期：選定“**取消排程開始日期**”核取方塊，然後使用“**行事曆**”視窗選擇停用排程的日期。
- 啟用啟動忽略的工作：選定“**執行錯過的工作**”核取方塊。
- 啟用開始時間發佈設定：核取“**在該時間間隔內隨機化工作開始時間**”核取方塊並指定分鐘值。

e. 點擊“**確定**”。

5. 如果工作是為電腦集而建立，則請選擇將在其中執行此工作的電腦網路（群組）。
6. 在“**選擇帳戶以執行工作**”視窗中，指定您希望執行工作的帳戶。
7. 在“**定義工作名稱**”視窗中，輸入工作名稱（不超過 100 個字元），不包含符號 **" * < > ? \ | :**。建議將工作類型新增到它的名稱中（例如，“共用資料夾的自訂掃描”）。
8. 如果希望在建立工作後不久啟動它，則在“**完成建立工作**”視窗中，選中“**精靈完成後執行工作**”核取方塊。點擊“**完成**”按鈕。

建立的工作將會在“**工作**”清單中顯示。

在卡巴斯基安全管理中心的應用程式設定視窗中設定本機工作

► *要在“應用程式設定”視窗中為一台網路電腦配置本機工作或一般應用程式設定，請執行以下工作：*

1. 展開卡巴斯基安全管理中心管理伺服器樹狀結構中的“**受管理裝置**”節點，選擇受防護電腦所屬的群組。
2. 在詳細資訊視窗中，選擇“**裝置**”標籤。
3. 採用以下方法之一開啟“**內容：<電腦名稱>**”視窗：
   - 點擊受防護電腦的名稱。
   - 開啟受防護電腦名稱的上下文功能表，然後選擇“**內容**”。

   內容：<電腦名稱> 視窗開啟。
4. 若要設定本機工作設定，請執行以下步驟：

   a. 轉至“**工作**”部分。
   - 在工作清單中，選擇要配置的本機工作。
   - 在工作清單中雙擊工作名稱。
   - 選擇工作名稱，然後點擊“**內容**”按鈕。
   - 在所選工作的內容功能表中，選擇“**內容**”。

5. 若要設定應用程式設定，請執行以下步驟：

   a. 轉至“**應用程式**”部分。

   - 在安裝的應用程式清單中，選擇要配置的應用程式。
   - 在安裝的應用程式清單中點兩下應用程式名稱。
   - 在安裝的應用程式清單中選擇應用程式名稱，然後點擊“**內容**”按鈕。
   - 在安裝程式的單中開啟程式名稱的內容功能表，然後選擇“**內容**”項。

   如果應用程式目前受卡巴斯基安全管理中心政策管控，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

在卡巴斯基安全管理中心中設定群組工作

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *要為多台電腦配置群組工作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中選擇工作名稱，然後點擊“**配置工作**”連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。
4. 在“**通知**”部分中，配置工作事件通知設定。

   關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

5. 根據配置的工作類型，執行下列一種操作：
   - 要設定自訂掃描工作：
     a. 在“**掃描範圍**”部分中，配置掃描範圍。
     b. 在“**選項**”部分中，配置工作優先順序水準及與其他軟體元件的整合。
   - 要配置更新工作，請根據您的需要調整工作設定：
     a. 在“**設定**”部分中，配置更新來源設定和磁碟子系統使用情況最佳化。
     b. 點擊“**連線設定**”按鈕以配置更新來源連線設定。
   - 若要配置“軟體模組更新”工作，在“**有關應用程式軟體模組更新的設定**”部分中選擇要執行的操作：複製並安裝應用程式模組的重要更新或僅進行檢查。
   - 若要配置“複製更新”工作，請在“**複製更新設定**”視窗中指定更新和目的資料夾。
   - 若要配置“應用程式啟動工作”，在“**啟動設定**”部分中，套用您要用於啟動應用程式的金鑰檔案。如果您想要新增用於續約產品授權的啟動碼或金鑰，請選中“**用作備用啟動碼或金鑰**”核取方塊。
   - 若要配置電腦控制的允許規則的自動建立，請在“**設定**”部分中，指定建立允許規則清單所依據的設定。
6. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
7. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。
8. 如有需要，在“**工作範圍的排除項目**”部分中指定要從工作範圍中排除的物件。關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。
9. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

將儲存新配置的群組工作設定。

下表匯總了可用於配置的群組工作設定。

步驟 26. Kaspersky Embedded Systems Security 2.2 群組工作設定

Kaspersky Embedded Systems Security 2.2 工作類型	“內容：<工作名稱>”視窗中的部分	工作設定
自動規則產生（請參見第 95 頁上的“應用程式啟動控制規則產生器和裝置控制規則產生器工作”部分）	**設定**	在配置“應用程式啟動控制規則產生器”工作設定時，您可以： • 透過新增或刪除資料夾的路徑和指定自動建立的規則允許啟動的檔案類型，來變更防護範圍。 • 考慮目前正在執行的應用程式。

Kaspersky Embedded Systems Security 2.2 工作類型	“內容：<工作名稱>”視窗中的部分	工作設定
	選項	當建立應用程式啟動控制的允許規則時，您可以指定執行的操作： • **使用數位憑證** • **使用數位憑證主旨和指紋** • **憑證遺失則使用** • **使用 SHA256 雜湊** • **為使用者或使用者群組產生規則** 您可以使用 Kaspersky Embedded Systems Security 2.2 在工作完成時建立的允許規則清單為設定檔配置設定。
	排程	您可以配置排程的工作啟動設定。
應用程式啟動（請參見第 97 頁上的“應用程式啟動工作”部分）	**啟動設定**	若要啟動應用程式或續約到期日期，您可新增金鑰。
	排程	您可以配置排程的工作啟動設定。
複製更新（請參見第 98 頁上的“更新工作”部分）	**更新來源**	您可以將卡巴斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。 如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。
	“**連線設定**”視窗	在“**更新來源連線設定**”部分中，您可指定是否應透過代理伺服器與 Kaspersky Lab 更新伺服器或任何其他伺服器建立連線。
	複製更新設定	您可指定用於複製的更新集。 在“**用於本機儲存已複製更新的資料夾**”欄位中，指定 Kaspersky Embedded Systems Security 2.2 將用於儲存已複製更新的資料夾的路徑。
	排程	您可以配置排程的工作啟動設定。

Kaspersky Embedded Systems Security 2.2 工作類型	“內容：<工作名稱>”視窗中的部分	工作設定
資料庫更新（請參見第 98 頁上的“更新工作”部分）	**設定**	您可在“**更新來源**”部分中將卡巴斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。 如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。 在“磁碟 I/O 使用最佳化”部分中，您可以配置能夠減少磁碟子系統工作負載的功能： • **降低磁碟 I/O 上的負載** • **用於最佳化 RAM(MB)**
	“**連線設定**”視窗	在“**更新來源連線設定**”部分中，您可指定是否應透過代理伺服器與 Kaspersky Lab 更新伺服器或任何其他伺服器建立連線。
	排程	您可以配置排程的工作啟動設定。
軟體模組更新（請參見第 98 頁上的“更新工作”部分）	**更新來源**	您可以將卡巴斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。 如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。
	“**連線設定**”視窗	在“**更新來源連線設定**”部分中，您可指定是否應透過代理伺服器與 Kaspersky Lab 更新伺服器或任何其他伺服器建立連線。
	有關應用程式軟體模組更新的設定	您可指定關鍵軟體模組更新可用或已安裝時 Kaspersky Embedded Systems Security 2.2 應執行的操作，還可指定 Kaspersky Embedded Systems Security 2.2 是否應接收有關排程的更新的資訊。
	排程	您可以配置排程的工作啟動設定。
自訂掃描（請參見第 100 頁上的“建立自訂掃描工作”部分）	**掃描範圍**	您可指定“自訂掃描”工作的掃描範圍，並配置安全等級設定。
	“**自訂掃描設定**”視窗	您可選擇其中一種預定義的安全等級，或手動自訂安全等級。

Kaspersky Embedded Systems Security 2.2 工作類型	“內容：<工作名稱>”視窗中的部分	工作設定
	選項	您可啟動或取消啟動為“自訂掃描”工作使用啟發式分析，並在“**啟發式分析**”部分中使用滑塊設定分析等級。 在“**與其他元件整合**”部分中，可以配置以下設定： • “為自訂掃描應用信任區域”工作。 • “為自訂掃描應用 KSN 使用”工作。 • 設定“自訂掃描”工作的優先順序：在背景模式下執行工作（低優先順序）或將工作視為關鍵區域掃描。
	排程	您可以配置排程的工作啟動設定。
軟體模組完整性檢查（第 99 頁）	**排程**	您可以配置排程的工作啟動設定。

對於資料庫更新回溯等工作，可以在“**通知**”和“**工作範圍的排除項目**”部分中僅配置標準工作設定（由卡巴斯基安全管理中心控制）。有關這些章節的設定配置的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

本章節說明項目

應用程式啟動控制規則產生器和裝置控制規則產生器工作

► *要配置裝置控制規則產生器工作或應用程式啟動控制規則產生器工作，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中選擇工作名稱，然後點擊“**配置工作**”連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。
4. 在“**通知**”部分中，配置工作事件通知設定。
5. 關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

6. 在“**設定**”部分中，您可配置以下設定：
   - 透過新增或刪除資料夾的路徑和指定自動建立的規則允許啟動的檔案類型，來變更防護範圍。
   - 考慮目前正在執行的應用程式。
7. 在**設定**部分中，當建立應用程式啟動控制允許規則時，您可以指定執行的操作：
   - **使用數位憑證**

     如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。此時，應用程式將允許啟動使用帶數位憑證的檔案啟動的程式。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。

     預設選中該選項。
   - **使用數位憑證主旨和指紋**

     使用此核取方塊可啟用或停用將檔案數位憑證的主旨和指紋用作觸發應用程式啟動控制允許規則的條件。選中此核取方塊可指定更嚴格的數位憑證驗證條件。

     如果選中此核取方塊，為其建立規則的檔案的數位憑證主旨和指紋值設定為觸發應用程式啟動控制允許規則的條件。Kaspersky Embedded Systems Security 2.2 將允許使用指定了指紋和數位憑證的檔案啟動的應用程式。

     由於指紋是數位憑證的唯一識別碼且無法偽造，選中此核取方塊會大大地限制基於數位憑證觸發允許規則。

     如果清除此核取方塊，則在作業系統中任何受信任數位憑證的存在被設定為觸發應用程式啟動控制允許規則的條件。

     如果選擇了“**使用數位憑證**”選項，該核取方塊可用。

     預設將會選定該核取方塊。
   - **憑證遺失則使用**

     如果用於建立規則的檔案沒有數位憑證，則可使用此下拉清單選擇用於觸發應用程式啟動控制允許規則的條件。

     - **SHA256 雜湊**。將用於建立規則的檔案的校驗和值設定為觸發允許應用程式啟動控制規則的條件。應用程式將允許啟動使用帶指定校驗和的檔案啟動的程式。
     - **檔案路徑**。將用於建立規則的檔案的路徑設定為觸發允許應用程式啟動控制規則的條件。此時，應用程式將允許啟動使用位於“為以下資料夾中的應用程式建立允許規則”表中的標籤上指定的資料夾中的檔案啟動的程式。
   - **使用 SHA256 雜湊**

     如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的校驗和值指定為規則觸發條件。應用程式將允許啟動使用帶指定校驗和值的檔案啟動的程式。

     當產生的規則需要滿足最終安全等級時，建議使用此選項：SHA256 校驗和可套用為唯一檔案 ID。作為 SHA256 校驗和作為規則觸發條件會將規則使用範圍限制為最多一個檔案。
   - **為使用者或使用者群組產生規則**。

     顯示使用者和/或使用者群組的欄位。應用程式將監控透過指定的使用者和/或使用者群組執行的任何應用程式。

     預設選擇為“**每個人**”。

   您可以使用 Kaspersky Embedded Systems Security 2.2 在工作完成時建立的允許規則清單為設定檔配置設定。

8. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
9. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。
10. 如有需要，在工作範圍的“**排除**”部分中指定要從工作範圍中排除的物件。

    有關此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

11. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

    將儲存新配置的群組工作設定。

啟動應用程式工作

► *若要配置啟動應用程式工作，請執行以下步驟：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中選擇工作名稱，然後點擊“**配置工作**”連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。
4. 在“**通知**”部分中，配置工作事件通知設定。
5. 關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。
6. 在“**啟動設定**”部分中，應用您要使用的金鑰檔案來啟動應用程式。如果您想要新增用於延長產品授權的金鑰，請選中“**作為備用金鑰使用**”核取方塊。
7. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
8. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。
9. 如有需要，在工作範圍的“**排除**”部分中指定要從工作範圍中排除的物件。

    有關此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

10. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

    將儲存新配置的群組工作設定。

更新工作

要配置複製更新、資料庫更新或軟體模組更新工作，請執行以下操作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中選擇工作名稱，然後點擊“**配置工作**”連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。
4. 在“**通知**”部分中，配置工作事件通知設定。

   關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

5. 根據配置的工作類型，執行下列一種操作：
   - 在“**更新來源**”部分中，配置更新來源設定和磁碟子系統使用方式最佳化。
     a. 您可在“**更新來源**”部分中將卡巴斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。

     如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。

     b. 在資料庫更新工作的“**磁碟 I/O 使用最佳化**”部分中，可以配置能夠減少磁碟子系統工作負載的功能：
        - **降低磁碟 I/O 上的負載**

          使用此核取方塊可以啟用或停用透過將更新檔案儲存在記憶體中的虛擬磁碟機上實現磁碟子系統優化的功能。

          如果選中該核取方塊，則啟用該功能。

          預設取消選定該核取方塊。

        - **用於最佳化 RAM(MB)**

          應用程式用於儲存更新檔案的記憶體的大小（以 MB 為單位）。預設記憶體大小為 512 MB。最小記憶體大小為 400 MB。

     c. 點擊“**連線設定**”按鈕，然後在開啟的“**連線設定**”視窗中，為連線到 Kaspersky Lab 更新伺服器和其他伺服器配置代理伺服器的使用。
   - 在軟體模組更新工作的“**有關應用程式軟體模組更新的設定**”章節中，可以指定當有可用的關鍵軟體模組更新或有可用的關於排程更新的資訊時，Kaspersky Embedded Systems Security 2.2 執行什麼操作，且還可以指定當安裝關鍵更新時 Kaspersky Embedded Systems Security 2.2 應執行哪種操作。
   - 在“**複製更新設定**”部分中，為“**複製更新**”工作指定更新集和目的資料夾。

6. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
7. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。

   有關此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

8. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

將儲存新配置的群組工作設定

對於“資料庫更新回溯”工作，可在“**通知**”和工作範圍的“**排除**”部分中僅配置由卡巴斯基安全管理中心控制的標準工作設定。有關此節中配置的設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

軟體模組完整性檢查

► *要配置“軟體模組更新”群組工作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中選擇工作名稱，然後點擊“**配置工作**”連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。
4. 在“**通知**”部分中，配置工作事件通知設定。

   關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

5. 在“**裝置**”部分中，選擇要為其配置“軟體模組完整性檢查”工作的裝置。
6. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
7. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。
8. 如有需要，在工作範圍的“**排除**”部分中指定要從工作範圍中排除的物件。

   有關此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

9. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

   將儲存新配置的群組工作設定。

建立自訂掃描工作

► *在卡巴斯基安全管理中心管理主控台中建立新工作：*

1. 採用以下方式之一啟動工作精靈：
   - 若要建立本機工作，請執行以下步驟：
     a. 展開卡巴斯基安全管理中心管理伺服器樹狀結構中的“**受管理裝置**”節點，選擇受防護電腦所屬的群組。
     b. 在詳細資訊視窗的“**裝置**”標籤上，在包含有關受防護電腦的資訊欄上開啟上下文功能表，然後選擇“**內容**”。
     c. 在開啟的視窗中，在“**工作**”部分中點擊“**新增**”按鈕。
   - 建立群組工作：
     a. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其建立政策的群組。
     b. 在詳細資訊視窗的“**工作**”標籤上開啟內容功能表，然後選擇“**新增 > 工作**”。
   - 要為自訂的一組電腦建立工作，請在卡巴斯基安全管理中心管理主控台樹狀結構中的“**裝置選擇**”節點中，選擇“**建立工作**”。

   將開啟工作精靈視窗。
2. 在“**指定工作名稱**”視窗中，輸入工作名稱（不超過 100 個字元），不包含符號 **| * < > ? \ / | :)**。建議將工作類型新增到它的名稱中（例如，“ 共用資料夾的自訂掃描”）。
3. 在“**工作類型**”視窗中的“**Kaspersky Embedded Systems Security 2.2**”標題下選擇“**自訂掃描**”工作，然後點擊“**下一步**”。
4. 在“**掃描範圍**”視窗中建立掃描範圍：

   根據預設，掃描範圍包括電腦的關鍵區域。掃描範圍在表格中使用圖示 ☑ 標記。排除的掃描範圍在表中用圖示 ☐ 標記。
   掃描範圍可以修改：新增特定的預先定義的掃描範圍、磁碟、資料夾及檔案，並為每個新增的範圍指定特定的安全設定。

   - 要從掃描中排除所有關鍵區域，請在每行上開啟內容功能表並選擇“**刪除範圍**”選項。
   - 要在掃描範圍中包括預定義的掃描範圍、磁碟、資料夾、網路物件或檔案：
     a. 右鍵點擊“**掃描範圍**”表，然後選擇“**新增範圍**”或點擊“**新增**”按鈕。
     b. 在“**新增物件至掃描範圍**”視窗中，選擇“**預設的範圍**”清單中的預設範圍，指定電腦或另外一台網路電腦上的電腦磁碟、資料夾、網路物件或檔案，然後點擊“**確定**”按鈕。
   - 要從掃描中排除子資料夾或檔案，請在精靈的“**掃描範圍**”視窗中選擇已新增的資料夾（磁碟）：
     a. 開啟內容功能表，然後選擇“**配置**”選項。
     b. 在“**安全等級**”視窗中點擊“**設定**”按鈕。
     c. 在“**自訂掃描設定**”設定視窗的“**一般**”標籤上，清除“**子資料夾**和**子檔案**”核取方塊。

- 要變更掃描範圍安全設定：

  a. 開啟您希望配置其設定的範圍的內容功能表，然後選擇“**配置**”。

  b. 在“**自訂掃描設定**”視窗中，選擇預設的安全等級之一，或者點擊“**設定**”按鈕以手動配置安全設定。

  > 安全設定的設定方式與即時檔案防護工作的設定方式相同（請參見第 139 頁上的“手動設定安全設定”部分）。

- 要略過新增的掃描範圍中的嵌入式物件：

  a. 開啟“**掃描範圍**”表的內容功能表，選擇“**新增**”排除。

  b. 指定要排除的物件：在“**預設的範圍**”清單中選擇預設範圍，指定電腦或另一台網路電腦上的電腦磁碟、資料夾、網路物件或檔案。

  c. 點擊“**確定**”按鈕。

5. 在“**選項**”視窗中，配置啟發式分析以及與其他元件的整合：

   - 配置啟發式分析的使用（請參見第 134 頁上的“使用啟發式分析”部分）。
   - 如果您希望從工作的掃描範圍中排除 Kaspersky Embedded Systems Security 2.2 信任區域中敘述的物件，則選中“**套用信任區域**”核取方塊。

     使用此核取方塊可啟用/停用工作的信任區域。

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 會將受信任處理程序的檔案操作新增到工作設定中設定的掃描排除中。

     如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 會在建立即時檔案防護工作的防護範圍時略過受信任處理程序的檔案操作。

     預設將會選定該核取方塊。

   - 如果您想要在工作中使用卡巴斯基安全網路雲端服務，請選中“**使用 KSN 掃描**”核取方塊。

     此核取方塊可啟用/停用在工作中使用卡巴斯基安全網路 (KSN) 雲端服務。

     如果選中該核取方塊，程式將使用從 KSN 服務接收到的資料確保更快速地對新威脅作出回應，並降低誤報的可能性。

     如果清除該核取方塊，則自訂掃描工作將不使用 KSN 服務。

     預設將會選定該核取方塊。

   - 若要向將執行該工作的程序分配基本優先順序“**低**”，請在“**選項**”視窗中選定“**在背景模式下執行工作**”核取方塊。

     該核取方塊將修改工作的優先順序。

     如果選中該核取方塊，工作在作業系統中的優先順序會下降。作業系統根據其他 Kaspersky Embedded Systems Security 2.2 工作和應用程式對 CPU 及電腦檔案系統的負荷，分配用於執行該工作的資源。因此，負荷增加時工作效能將降低，負荷降低時效能將提高。

     如果取消選中該核取方塊，工作啟動和執行時的優先順序將與其他 Kaspersky Embedded Systems Security 2.2 工作和其他程式的優先順序相同。在這種情況下，工作執行的速度將加快。

     預設取消選定該核取方塊。

預設情況下，執行 Kaspersky Embedded Systems Security 2.2 工作程序的優先順序為“**中度**”（正常）。

- 要使用所建立的工作作為關鍵區域掃描工作，請選中“**選項**”視窗中的“**將工作視為關鍵區域掃描**”核取方塊。

  使用該核取方塊可變更工作優先順序：啟用或停用記錄“*關鍵區域掃描*”事件和重新整理電腦防護狀態。卡巴斯基安全管理中心根據狀態為“*關鍵區域掃描*”的工作的執行結果來評估電腦的安全等級。該核取方塊在本機系統和 Kaspersky Embedded Systems Security 2.2 的自訂工作的內容中不可用。您只能在卡巴斯基安全管理中心編輯此設定。

  如果選中此核取方塊，管理伺服器會記錄“關鍵區域掃描已完成”事件並根據工作執行結果重新整理電腦防護狀態。掃描工作具有較高優先順序。

  如果清除此核取方塊，則工作以較低優先順序執行。

  對於“關鍵區域掃描”工作，預設選中該核取方塊。

6. 點擊“**下一步**”。
7. 在“**排程**”視窗中，為工作設定排程（請參見第 107 頁上的“配置工作啟動排程設定”部分）。
8. 指定您想要用來執行工作的使用者帳戶並定義工作名稱。
9. 點擊“**完成**”。

將為所選電腦或電腦群組建立新的自訂掃描工作。

設定自訂掃描工作

► *若要設定現有自訂掃描工作，請執行以下步驟：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中選擇工作名稱，然後點擊“**配置工作**”連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。
4. 在“**通知**”部分中，配置工作事件通知設定。

   關於此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

5. 在“**設定**”部分中，您可執行以下操作：
   a. 在“**掃描範圍**”部分中，選擇您要包含到掃描範圍內的檔案資源旁邊的核取方塊。
   b. 點擊“**配置**”按鈕，然後選擇安全等級。

      您可選擇其中一種預定義的安全等級，或手動自訂安全等級。

   c. 要手動配置安全等級，請在“**自訂掃描設定**”視窗中點擊“**設定**”按鈕。

6. 在“**選項**”部分中，您可執行以下操作：
   a. 啟用或停用**啟發式分析**的使用，並使用“**啟發式分析**”部分中的滑塊設定分析等級。
   b. 配置進階設定（請參見第 100 頁上的“建立自訂掃描工作”部分）。
7. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
8. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。
9. 如有需要，在工作範圍的“**排除**”部分中指定要從工作範圍中排除的物件。

   有關此節中配置設定的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

10. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

    將儲存新配置的群組工作設定。

為自訂掃描工作指定關鍵區域掃描的工作狀態

根據預設，如果“關鍵區域掃描”工作的執行頻率比 Kaspersky Embedded Systems Security 2.2 的“**長時間未執行關鍵區域掃描**”設定，則卡巴斯基安全管理中心將向電腦分配“*警告*”狀態。

► *要為單個管理群組中的所有電腦配置掃描操作，請執行下列步驟：*

1. 建立群組自訂掃描工作。
2. 在工作建立精靈“**選項**”視窗中，選中“**將工作視為關鍵區域掃描**”核取方塊。指定的工作設定（掃描範圍與安全性設定）將套用至群組中的所有電腦。配置工作排程。

   您可以在為一組電腦或電腦群組建立自訂掃描工作時選定“**將工作視為關鍵區域掃描**”核取方塊，也可以稍後在“**內容：<工作名稱>**”視窗中進行選擇。

3. 使用新的或現有政策停用群組電腦上的系統掃描工作的排程啟動（請參見第 84 頁上的“配置本機系統工作的排程啟動”部分）。

隨後，卡巴斯基安全管理中心管理伺服器將評估受防護電腦的安全狀態，並且將根據上次執行具有“關鍵區域掃描”狀態工作的結果而非根據“*關鍵區域掃描*”系統工作的結果通知您有關該安全狀態的資訊。

您可以為群組自訂掃描工作和電腦群組的工作分配“*關鍵區域掃描*”工作狀態。

可以使用應用程式主控台檢視“自訂掃描”工作是否為“關鍵區域掃描”工作。

在應用程式主控台中，“**將工作視為關鍵區域掃描**”核取方塊會顯示在工作設定中，但不可對其進行編輯。

雲端儲存檔案掃描

關於雲端檔案

Kaspersky Embedded Systems Security 2.2 可以與 Microsoft OneDrive 雲端檔案進行互動。該應用程式支援新的“ OneDrive 檔案按需”功能。

> Kaspersky Embedded Systems Security 2.2 不支援其他雲端儲存。

“ OneDrive 檔案按需”幫助您存取您在 OneDrive 中的所有檔案，而無需下載所有檔案和使用裝置上的儲存空間。您可以在需要時將檔案下載到硬碟。

當“ OneDrive 檔案按需”功能開啟時，可以在檔案資源管理器的“**狀態**”列中看到每個檔案旁邊的狀態圖示。每個檔案都具有以下狀態之一：

此狀態圖示指示檔案*僅線上可用*。僅線上檔案不會物理儲存在您的硬碟中。當裝置未連線到 Internet 時，無法開啟僅線上檔案。

此狀態圖示指示檔案*本機可用*。當開啟僅線上檔案時會顯示此圖示，該檔案會下載到您的裝置中。您可以隨時開啟本機可用的檔案，即使沒有 Internet 存取權限。要清理空間，可以將檔案變更回 僅線上。

此狀態圖示指示檔案*儲存在硬碟中並且始終可用*。

雲端檔案掃描

Kaspersky Embedded Systems Security 2.2 只能掃描受防護電腦上本機儲存的雲端檔案。此類 OneDrive 檔案的狀態為 和 。在掃描期間會略過 檔案，因為這些檔案沒有物理儲存在受防護電腦上。

> Kaspersky Embedded Systems Security 2.2 在掃描時不會自動從雲端下載 檔案，即使這些檔案已包括在掃描範圍中。

在各種方案中，雲端檔案由多種 Kaspersky Embedded Systems Security 2.2 工作處理，具體取決於工作類型：

- 即時雲端檔案掃描：您可以將包含雲端檔案的資料夾新增到“即時檔案防護”工作的防護範圍中。當使用者存取該檔案時會對該檔案進行掃描。如果使用者存取 檔案，系統會下載該檔案，該檔案將變為本機可用，並且其狀態將變更為 。這樣該檔案可以被“即時檔案防護”工作處理。
- 自訂雲端檔案掃描：您可以將包含雲端檔案的資料夾新增到“自訂掃描”工作的防護範圍中。該工作會掃描狀態為 和 的檔案。如果在範圍中找到任何 檔案，在掃描期間將略過這些檔案，並在工作記錄中記錄資訊事件，指示所掃描的檔案只是雲端檔案的預留位置，並不存在於本機磁碟機中。
- 應用程式控制規則生成和使用：您可以使用“應用程式啟動控制規則產生器”工作為 和 檔案建立允許和拒絕規則。“應用程式啟動控制”工作應用“預設拒絕”原則和所建立的規則來處理和封鎖雲端檔案。

  > “應用程式啟動控制”工作會封鎖所有雲端檔案啟動，不管它們的狀態如何。應用程式不會將 檔案包括在規則生成範圍中，因為它們沒有物理儲存在硬碟上。由於不能為此類檔案建立任何允許規則，因此對它們實施“預設拒絕”原則。

在 OneDrive 雲端檔案中偵測到威脅時，應用程式會應用執行掃描的工作的設定中指定的操作。這樣，可以將檔案刪除、解毒、移至隔離區或備份。

按照相關 Microsoft OneDrive 文件中概述的原則，對本機檔案的變更將與 OneDrive 中儲存的副本進行同步。

在卡巴斯基安全管理中心中設定當機診斷設定

如果 Kaspersky Embedded Systems Security 2.2 執行期間發生問題（例如，Kaspersky Embedded Systems Security 2.2 當機），且您想要進行診斷，您可啟用建立 Kaspersky Embedded Systems Security 2.2 處理程序的追蹤檔案和傾印檔案，並將這些檔案傳送到 Kaspersky Lab 技術支援進行分析。

Kaspersky Embedded Systems Security 2.2 不會自動傳送任何偵錯或傾印檔案。診斷資料只能由具有相應權限的使用者傳送。

Kaspersky Embedded Systems Security 2.2 會以未加密的形式將資訊寫入到偵錯檔案和傾印檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 2.2 設定管理。您可以配置存取權限（請參見第 69 頁上的“Kaspersky Embedded Systems Security 2.2 功能的存取權限”部分）並僅允許所需使用者存取記錄、偵錯和傾印檔案。

► *要在卡巴斯基安全管理中心中設定當機診斷設定：*

1. 在卡巴斯基安全管理中心的管理主控台中，開啟“**應用程式設定**”（請參見第 90 頁上的“**在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作**”部分）視窗。
2. 開啟“**故障診斷**”部分，然後執行以下操作：
   - 如果您要應用程式將診斷資訊寫入檔案，請選中“**將診斷資訊寫入至檔案**”核取方塊。
     - 在下面的欄位中指定 Kaspersky Embedded Systems Security 2.2 將會儲存偵錯檔案的資料夾。
     - 設定診斷資訊的詳細等級。

       透過該下拉清單，您可以選擇 Kaspersky Embedded Systems Security 2.2 儲存到偵錯檔案的診斷資訊的詳細等級。

       您可以選擇以下一種詳細等級：

       - **緊急事件** - Kaspersky Embedded Systems Security 2.2 僅將和緊急事件有關的資訊儲存到偵錯檔案。
       - **錯誤** - Kaspersky Embedded Systems Security 2.2 將和緊急事件及錯誤有關的資訊儲存到偵錯檔案。
       - **重要事件** - Kaspersky Embedded Systems Security 2.2 將和緊急事件、錯誤及重要事件有關的資訊儲存到偵錯檔案。

- **資訊事件** - Kaspersky Embedded Systems Security 2.2 將和緊急事件、錯誤、重要事件及資訊事件有關的資訊儲存到偵錯檔案。
- **所有診斷資訊** - Kaspersky Embedded Systems Security 2.2 將所有診斷資訊儲存到偵錯檔案。

技術支援代表確定為解決出現的問題而需要設定的詳細等級。

預設的詳細等級設定為“**所有診斷資訊**”。

如果選中“**將診斷資訊寫入至檔案**”核取方塊，該下拉清單才可用。

- 指定偵錯檔案的最大容量。
- 指定要診斷的元件。元件代碼必須用分號分隔。代碼區分大小寫（請參見下表）。

步驟 27. Kaspersky Embedded Systems Security 2.2 子系統代碼

元件代碼	元件名稱
*	所有元件。
gui	使用者介面子系統，Microsoft 管理主控台中的 Kaspersky Embedded Systems Security 2.2 管理單元。
ak_conn	整合網路代理和卡巴斯基安全管理中心的子系統。
bl	控制處理程序，執行 Kaspersky Embedded Systems Security 2.2 控制工作。
wp	工作處理程序，處理病毒防護工作。
blgate	Kaspersky Embedded Systems Security 2.2 遠端管理處理程序。
ods	自訂掃描子系統。
oas	即時檔案防護子系統。
qb	隔離和備份子系統。
scandll	病毒防護掃描輔助模組。
core	基本病毒防護功能子系統。
avscan	病毒防護處理子系統。
avserv	控制病毒防護內核子系統。
prague	基本功能子系統。
updater	更新資料庫和軟體模組的子系統。
snmp	SNMP 協定支援子系統。
perfcount	效能計數器子系統。

Kaspersky Embedded Systems Security 2.2 管理單元 (gui) 和卡巴斯基安全管理中心的管理外掛程式 (ak_conn) 的偵錯設定在這些元件重新啟動後應用。SNMP 協定支援子系統 (snmp) 的偵錯設定在 SNMP 服務重新啟動後應用。效能計數器子系統 (perfcount) 的偵錯設定在所有使用效能計數器的處理程序都重新啟動之後應用。當機診斷設定儲存後，其他 Kaspersky Embedded Systems Security 2.2 子系統的偵錯設定就會立刻套用。

預設情況下，Kaspersky Embedded Systems Security 2.2 記錄所有 Kaspersky Embedded Systems Security 2.2 元件的診斷資訊。

如果選中“**將診斷資訊寫入至檔案**”核取方塊，則該輸入欄位才可用。

- 如果您希望應用程式建立傾印檔案，請選中“**建立傾印檔案**”核取方塊。
  - 在下面的欄位中，指定 Kaspersky Embedded Systems Security 2.2 將用於儲存記憶體傾印檔案的資料夾。

3. 點擊“**確定**”。

已設定的應用程式設定將套用於受防護電腦上。

管理工作排程

您可以配置 Kaspersky Embedded Systems Security 2.2 工作的啟動排程，並配置依排程執行的工作的設定。

本章節說明項目

配置工作啟動排程設定

您可以在應用程式主控台中配置本機系統和自訂工作的啟動排程。您不能為群組工作配置啟動排程。

► *若要配置工作啟動排程設定，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選擇“**受管理裝置**”節點並執行以下操作：
   - 如果想要配置政策設定，請在電腦群組中選擇“**政策 > <政策名稱> > <選擇> >配置 > 工作管理**”。
   - 如果想要使用卡巴斯基安全管理中心配置單個電腦的應用程式設定，請在卡巴斯基安全管理中心中開啟“**工作設定**”（請參見第 90 頁上的“**在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作**”部分）視窗。

   將開啟“**設定**”視窗。
2. 在開啟的視窗中的“**排程**”標籤上，選中“**依排程執行**”核取方塊。

如果卡巴斯基安全管理中心政策封鎖按排程啟動自訂掃描工作和更新工作，則這些工作的排程設定的欄位不可用。

3. 根據需要配置排程設定。為此，請執行以下操作：

   a. 在“**週期**”清單中，選擇以下值之一：

      - **每小時**，如果您希望該工作在指定的小時數內間隔執行，請在“**每 <數量> 小時**”欄位中指定小時數。
      - **每天**，如果您希望該工作在指定的天數內間隔執行，請在“**每 <數量> 天**”欄位中指定天數。
      - **每週**，如果您希望該工作在指定的週數內間隔執行，請在“**每 <數量> 週**”欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。
      - **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 2.2 時執行該工作。
      - **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。

   b. 在“**開始時間**”欄位中指定首次啟動工作的時間。

   c. 在“**開始日期**”欄位中，指定套用排程的開始日期。

   指定了工作啟動頻率之後，將在視窗頂部的“**下次開始**”欄位中顯示工作的首次啟動時間、排程的開始套用日期以及預計下一個工作啟動時間的相關資訊。每次開啟“**工作**”視窗的“**排程**”標籤時，將顯示有關工作的下一次預計啟動時間的最新資訊。
   如果 卡巴斯基安全管理中心的活動政策設定禁止活動排程的系統工作，則將在“**下次開始**”欄位中顯示值“**政策不允許**”（請參見第 84 頁上的“配置本機預定義工作的排程啟動”一節）。

4. 根據需要使用“**進階**”標籤來配置以下排程設定。

   - 在“**工作停止設定**”部分中：
     a. 選中“**持續時間**”核取方塊，並輸入右側欄位中輸入所需的小時數和分鐘數以指定工作執行的最大持續時間。
     b. 選中“**暫停從**”核取方塊，並在右側欄位中輸入時間間隔的開始和結束值，以指定在工作執行的 24 小時中將暫停執行工作的時間間隔。
   - 在“**進階設定**”部分中：
     a. 選中“**取消排程，從**”核取方塊，並指定停止執行排程的日期。
     b. 選定“**執行錯過的工作**”核取方塊以允許啟動略過的工作。
     c. 選中“**在該時間間隔內隨機啟動工作**”核取方塊，並按分鐘指定該值。

5. 點擊“**套用**”按鈕儲存工作啟動設定。

啟用和停用排程工作

可在配置排程設定之前或之後啟用和停用排程工作。

► *要啟用或停用工作啟動排程，請執行以下步驟：*

1. 在應用程式主控台樹狀目錄中，開啟要為其配置啟動排程的工作名稱的內容功能表。
2. 選擇“**內容**”。

   將開啟“**工作設定**”視窗。
3. 在開啟的視窗中的“**排程**”標籤上，執行以下操作之一：
   - 如果您希望啟用工作的啟動排程，請選中“**依排程執行**”核取方塊。
   - 如果您希望停用工作的啟動排程，請清除“**依排程執行**”核取方塊。

     不會刪除已配置的工作啟動排程設定，並將在排程的下一次工作啟動時間套用該設定。
4. 點擊“**套用**”按鈕。

將儲存已配置的工作啟動排程設定。

管理應用程式設定

本章節包含有關在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 一般設定的資訊。

本章內容

從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security 2.2

透過 Kaspersky Embedded Systems Security 2.2 管理外掛程式可以集中管理多台已安裝 Kaspersky Embedded Systems Security 2.2 並包括在管理群組中的電腦。卡巴斯基安全管理中心還可以單獨配置管理群組中包括的每台電腦的操作設定。

“*管理群組*”透過卡巴斯基安全管理中心手動建立並包含您要為其設定相同的控制和防護設定的已安裝 Kaspersky Embedded Systems Security 2.2 的多台電腦。有關使用管理群組的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

如果 Kaspersky Embedded Systems Security 2.2 在某台電腦上的執行受活動卡巴斯基安全管理中心政策的控制，則該電腦的應用程式設定不可用。

可透過以下方式從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security 2.2：

- **使用卡巴斯基安全管理中心政策**。可使用卡巴斯基安全管理中心政策為一組電腦遠端設定相同的防護設定。在活動政策中指定的工作設定的優先順序高於在應用程式主控台中本機設定或在卡巴斯基安全管理中心的“**內容：<電腦名稱>**”視窗中遠端配置的工作設定。

  您可使用政策設定一般應用程式設定、即時防護工作設定、本機活動控制工作設定、排程的系統工作啟動設定和設定檔使用設定。

- **使用卡巴斯基安全管理中心群組工作**。使用卡巴斯基安全管理中心群組工作可為一組電腦遠端配置具有過期期限的工作的通用設定。

- 您可使用群組工作啟動應用程式，設定“自訂掃描”工作設定，更新工作設定，以及“應用程式啟動控制規則產生器”工作設定。

- **使用一組裝置的工作**。使用一組裝置的工作可以為不屬於任何一個管理群組的電腦遠端配置具有有限執行期的通用工作設定。

- **使用單個電腦的內容視窗**。在“**內容：<電腦名稱>**”視窗中，您可遠端配置管理群組中包含的單台電腦的工作設定。 如果選定電腦不受活動卡巴斯基安全管理中心政策的控制，您可設定一般應用程式設定和所有 Kaspersky Embedded Systems Security 2.2 工作的設定。

卡巴斯基安全管理中心可以配置應用程式設定、進階功能，並允許您使用記錄和通知。您可以為一組電腦也可以為單台電腦配置這些設定。

在卡巴斯基安全管理中心中設定一般應用程式設定

您可以從卡巴斯基安全管理中心為一組電腦或一個電腦設定 Kaspersky Embedded Systems Security 2.2 一般設定。

本章節說明項目

在卡巴斯基安全管理中心中配置延展性和介面

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *要配置延伸性設定和應用程式介面，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**應用程式設定**”部分的“**延伸性和介面**”部分，點擊“**設定**”。
4. 在“**延伸性和介面**”視窗的“**一般**”標籤上，配置以下設定：
   - 在“**延伸性設定**”部分中，配置用於定義 Kaspersky Embedded Systems Security 2.2 使用的處理程序數的設定：
     - **自動偵測延伸性設定**。

       Kaspersky Embedded Systems Security 2.2 自動控制使用的處理程序數量。
     - **手動設定工作處理程序數**。

       Kaspersky Embedded Systems Security 2.2 根據指定的值控制有效的工作處理程序數。

       這是預設值。

- **最大活動處理程序數。**

  Kaspersky Embedded Systems Security 2.2 使用的最大處理程序數。如果選擇了“**手動設定工作處理程序數**”選項，該輸入欄位才可用。

- **用於即時防護的處理程序數。**

  即時防護工作元件使用的最大處理程序數。如果選擇了“**手動設定工作處理程序數**”選項，該輸入欄位才可用。

- **背景自訂掃描工作的處理程序數。**

  在背景模式下執行“自訂掃描”工作時“自訂掃描”元件使用的最大處理程序數。如果選擇了“**手動設定工作處理程序數**”選項，該輸入欄位才可用。

在“**使用者互動**”部分中，配置通知區域中應用程式系統欄圖示顯示：清除或選中“**在工作列中顯示系統匣圖示**”核取方塊。

5. 點擊“**確定**”。

將儲存設定的應用程式設定。

在卡巴斯基安全管理中心中配置安全設定

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *若要手動設定安全性設定，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**應用程式設定**”部分中，點擊“**安全性和可靠性**”設定下的“**設定**”按鈕。

4. 在“**安全性設定**”視窗中，配置以下設定：

   - 在“**可靠性設定**”部分，您可以配置當應用程式返回錯誤或終止時 Kaspersky Embedded Systems Security 2.2 工作的還原設定。

     - **重新啟動工作**

       該核取方塊用於允許或禁止當應用程式返回錯誤或終止時 Kaspersky Embedded Systems Security 2.2 工作的還原。

       如果選中該核取方塊，則當應用程式返回錯誤或終止時，Kaspersky Embedded Systems Security 2.2 會自動還原 Kaspersky Embedded Systems Security 2.2 工作。

       如果清除該核取方塊，則當應用程式返回錯誤或終止時，Kaspersky Embedded Systems Security 2.2 不會還原 Kaspersky Embedded Systems Security 2.2 工作。

       預設將會選定該核取方塊。

     - **重啟自訂掃描工作的次數不超過(次)**

       Kaspersky Embedded Systems Security 2.2 返回錯誤後嘗試還原“自訂掃描”工作的次數。如果選中“**重新啟動工作**”核取方塊，則該輸入欄位才可用。

   - 在“**轉換至 UPS 備用電源時的操作**”部分，指定在轉換為 UPS 備用電源後 Kaspersky Embedded Systems Security 2.2 對電腦產生的負荷的限制：

     - **不啟動已排程掃描工作**

       該核取方塊用於啟用或停用在電腦轉換為 UPS 電源後、還原標準電源模式前啟動排程掃描工作。

       如果選中該核取方塊，在電腦轉換為 UPS 電源後、還原標準電源模式前 Kaspersky Embedded Systems Security 2.2 不會啟動排程掃描工作。

       如果清除該核取方塊，不論電源模式如何，Kaspersky Embedded Systems Security 2.2 都會啟動排程掃描工作。

       預設將會選定該核取方塊。

     - **停止目前掃描工作**

       該核取方塊用於啟用或停用在電腦轉換為 UPS 電源後執行執行掃描工作的選項。

       如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 會在電腦轉換為 UPS 電源後暫停執行掃描工作。

       如果消除該核取方塊，Kaspersky Embedded Systems Security 2.2 會在電腦轉換為 UPS 電源後繼續執行掃描工作。

       預設將會選定該核取方塊。

     只有電池電量低於 90% 時，電腦才會轉換到 UPS 電源。

   - 在“**密碼防護設定**”部分中，設定用於防護存取 Kaspersky Embedded Systems Security 2.2 功能的密碼。

5. 點擊“**確定**”。

將儲存延伸性和可靠性設定。

使用卡巴斯基安全管理中心配置連線設定

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

設定的連線設定用於將 Kaspersky Embedded Systems Security 2.2 連線到更新和啟動伺服器，以及在將應用程式與 KSN 服務整合期間使用。

► *若要設定連線設定，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**應用程式設定**”部分中，點擊“**代理伺服器**”部分中的“**設定**”按鈕。

   將開啟“**連線設定**”視窗。
4. 在“**連線設定**”視窗中，配置以下設定：
   - 在“**代理伺服器設定**”部分中，選擇代理伺服器使用設定：
     - **不使用代理伺服器**。

       如果選擇此選項，Kaspersky Embedded Systems Security 2.2 會直接連線到 KSN 服務，而不使用任何代理伺服器。
     - **自動偵測代理伺服器設定**。

       如果選擇此選項，Kaspersky Embedded Systems Security 2.2 會使用 Web 代理自動探索協定 (WPAD) 自動定義與 KSN 服務的連線設定。

       預設選中該選項。
     - **使用自訂代理伺服器設定**。

       如果選擇此選項，Kaspersky Embedded Systems Security 2.2 會使用手動指定的代理伺服器設定連線到 KSN。
     - 代理伺服器和連接埠號的 IP 位址或符號名稱。

- **對於本機位址不使用代理伺服器**。

  該核取方塊用於在存取與安裝了 Kaspersky Embedded Systems Security 2.2 的電腦位於同一網路上的電腦時啟用或停用代理伺服器。

  如果選中該核取方塊，則會直接透過託管已安裝了 Kaspersky Embedded Systems Security 2.2 的電腦的網路存取電腦。而不使用代理伺服器。

  如果取消選中該核取方塊，將套用代理伺服器以連線到本機電腦。

  預設將會選定該核取方塊。

- 在“**代理伺服器身分驗證設定**”部分中，指定身分驗證設定：
  - 在下拉清單中選擇身分驗證設定。
    - **不使用身分驗證** - 不執行身分驗證。預設選擇該方式。
    - **使用 NTLM 身分驗證** - 使用由 Microsoft 開發的 NTLM 網路驗證協定執行身分驗證。
    - **使用帶使用者名稱和密碼的 NTLM 身分驗證** - 透過由 Microsoft 開發的 NTLM 網路驗證協定，使用名稱和密碼執行身分驗證。
    - **套用使用者名稱和密碼** - 使用使用者名和密碼執行身分驗證。
  - 需要時，輸入使用者名稱和密碼。
- 在“**授權**”塊中，清除或選中“**啟動應用程式時使用卡巴斯基安全管理中心作為代理伺服器**”。

5. 點擊“**確定**”。

將儲存設定的連線設定。

配置進階功能

您可以透過卡巴斯基安全管理中心為一組電腦或一個電腦設定 Kaspersky Embedded Systems Security 2.2 進階功能。

本章節說明項目

在卡巴斯基安全管理中心中配置信任區域設定

預設情況下，在剛剛建立的政策和工作中套用信任區域。

► *要配置信任區域設定：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**選項**”部分，點擊“**信任區域**”設定區域中的“**設定**”按鈕。

   將開啟“**信任區域**”視窗。
4. 在“**排除**”標籤上，指定掃描期間 Kaspersky Embedded Systems Security 2.2 要略過的物件：
   - 要建立建議的排除項目，請點擊“**新增建議的排除項目**”按鈕。

     點擊此按鈕允許您透過新增 Microsoft 建議的排除和 Kaspersky Lab 建議的排除來延伸排除清單。
   - 要匯入排除項，請點擊“**匯入**”按鈕，並在開啟的視窗中選擇 Kaspersky Embedded Systems Security 2.2 將視為受信任的檔案。
   - 要手動指定將檔案視為受信任的條件，請點擊“**新增**”按鈕。在開啟的視窗中，指定以下設定：
     - **要掃描的物件**

       將檔案、資料夾、磁碟機或指令碼檔案新增到排除項目。

       如果選中該核取方塊，在使用“**排除使用範圍**”部分中選擇的 Kaspersky Embedded Systems Security 2.2 元件執行掃描時，Kaspersky Embedded Systems Security 2.2 會略過指定的預定義範圍、檔案、資料夾、磁碟機或指令碼檔案。

       預設將會選定該核取方塊。
     - **偵測物件**

       按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書網站上提供了可偵測物件的名稱清單。

       如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過指定的可偵測物件。

       如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 預設將偵測程式中指定的所有物件。

       預設取消選定該核取方塊。

- **排除使用範圍**

  套用規則的 Kaspersky Embedded Systems Security 2.2 工作的名稱。

- 如有必要，在“**註解**”欄位中指定解釋排除的附加資訊。

5. 在“**信任區域**”視窗的“**受信任處理程序**”標籤上，指定掃描期間 Kaspersky Embedded Systems Security 2.2 要略過的處理程序：

   - **不檢查檔案備份操作**

     該核取方塊用於啟用或停用當電腦上安裝的備份工具執行檔案讀取操作時掃描此類操作。

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 會略過由電腦上安裝的備份工具執行的檔案讀取操作。

     如果取消選中該核取方塊，Kaspersky Embedded Systems Security 2.2 會掃描由電腦上安裝的備份工具執行的檔案讀取操作。

     預設將會選定該核取方塊。

   - **不檢查指定處理程序的檔案活動**

     該核取方塊用於啟用或停用掃描受信任處理程序的檔案活動。

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 會在掃描期間略過受信任處理程序的操作。

     如果消除該核取方塊，Kaspersky Embedded Systems Security 2.2 會掃描受信任處理程序的檔案操作。

     預設取消選定該核取方塊。

6. 如有必要，透過點擊“**新增**”按鈕新增不希望掃描其檔案活動的處理程序（請參見第 117 頁上的“新增受信任處理程序”部分）。
7. 點擊“**信任區域**”視窗中的“**確定**”儲存變更。

新增受信任處理程序

► *向受信任處理程序清單中新增一個或多個處理程序：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**選項**”部分，點擊“**信任區域**”設定區域中的“**設定**”按鈕。

   將開啟“**信任區域**”視窗。

4. 在“**受信任處理程序**”標籤上，選中“**不檢查指定處理程序的檔案活動**”核取方塊。
5. 點擊“**新增**”按鈕。
6. 從按鈕內容功能表中選擇以下選項之一：

   - **多個處理程序**。

     在開啟的“**新增受信任處理程序**”視窗中，配置以下設定：

     a. **使用磁碟上的完整處理程序路徑來將它視為受信任**。

        如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將使用檔案的完整路徑來確定該處理程序的信任狀態。

        如果清除該核取方塊，則不考慮將檔案的路徑作為決定處理程序信任狀態的條件。

        預設將會選定該核取方塊。

     b. **使用處理程序檔案雜湊來將它視為受信任**。

        如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將使用選定的檔案雜湊來確定處理程序信任狀態。

        如果清除該核取方塊，則不考慮將檔案雜湊作為決定處理程序信任狀態的條件。

        預設將會選定該核取方塊。

     c. 點擊“**瀏覽**”按鈕以根據可執行處理程序新增資料。

     d. 在開啟的視窗中選擇可執行檔。

        一次只能新增一個可執行檔。重複步驟 c-d 以新增其他可執行檔。

     e. 點擊“**處理程序**”按鈕以根據正在執行的處理程序新增資料。

     f. 在開啟的視窗中選擇處理程序。要選擇多個處理程序，請在選擇時按住 **CTRL** 鍵。

     g. 點擊“**確定**”。

        執行即時檔案防護工作的帳戶在裝有 Kaspersky Embedded Systems Security 2.2 的電腦上必須具有管理員權限，才能檢視活動處理程序清單。您可以按處理程序的可執行檔的檔案名稱、PID 或其在本機電腦上的路徑來對活動處理程序清單中的處理程序進行排序。請注意，只有在本機電腦上或透過卡巴斯基安全管理中心以指定的主機設定使用應用程式主控台時，才能透過點擊“**處理程序**”按鈕來選擇正在執行的處理程序。

   - **一個基於名稱和路徑的處理程序。**

     在開啟的“**手動新增受信任處理程序**”視窗中，配置以下設定：

     a. 輸入可執行檔的路徑（包括檔案名稱）。

     b. 點擊“**確定**”。

- **一個基於物件內容的處理程序。**

  在開啟的“**新增受信任處理程序**”視窗中，配置以下設定：

  a. 點擊“**瀏覽**”按鈕，然後選擇處理程序。

  b. **使用磁碟上的完整處理程序路徑來將它視為受信任**。

  如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將使用檔案的完整路徑來確定該處理程序的信任狀態。

  如果清除該核取方塊，則不考慮將檔案的路徑作為決定處理程序信任狀態的條件。

  預設將會選定該核取方塊。

  c. **使用處理程序檔案雜湊來將它視為受信任**。

  如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將使用選定的檔案雜湊來確定處理程序信任狀態。

  如果清除該核取方塊，則不考慮將檔案雜湊作為決定處理程序信任狀態的條件。

  預設將會選定該核取方塊。

  d. 點擊“**確定**”。

  要將所選處理程序新增到受信任處理程序清單，必須選擇至少一種信任條件。

7. 在“**新增受信任處理程序**”視窗中，點擊“**確定**”按鈕。

選定的檔案或處理程序將新增到“**信任區域**”視窗中的受信任處理程序清單。

套用 not-a-virus 遮罩

not-a-virus 遮罩允許略過可能在掃描過程中被視為有害的合法軟體檔案和 Web 資源。該遮罩影響以下工作：

- 即時檔案防護。
- 自訂掃描。

如果未向排除清單新增該遮罩，Kaspersky Embedded Systems Security 2.2 將對此類別下的軟體或 Web 資源套用在工作設定中指定的操作。

► *要套用 not-a-virus 遮罩：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**選項**”部分，點擊“**信任區域**”設定區域中的“**設定**”按鈕。

   將開啟“**信任區域**”視窗。
4. 如果清除該核取方塊，則在“**排除**”標籤上，捲動清單並選擇具有“**not-a-virus:***”值的行。
5. 點擊“**確定**”。

套用了新設定。

卸除式磁碟機掃描

可以配置透過 USB 連接埠連線到受防護電腦的卸除式磁碟機的掃描。

Kaspersky Embedded Systems Security 2.2 使用自訂掃描工作掃描卸除式磁碟機。當卸除式磁碟機已連線並在完成掃描後刪除工作時，應用程式會自動建立新的自訂掃描工作。系統會根據為卸除式磁碟機掃描定義的預設安全等級來執行建立的工作。您不能配置臨時自訂掃描工作的設定。

當它們在作業系統中註冊為 USB 大容量儲存裝置時，Kaspersky Embedded Systems Security 2.2 將掃描連線的卸除式 USB 磁碟機。如果連線被裝置控制工作封鎖，則應用程式不會掃描卸除式磁碟機。應用程式不會掃描 MTP 連線的行動裝置。

Kaspersky Embedded Systems Security 2.2 允許在掃描期間存取卸除式磁碟機。

每個卸除式磁碟機的掃描結果提供在連線卸除式磁碟機時建立的自訂掃描工作的記錄中。

可以變更卸除式磁碟機掃描元件的設定（請參見以下表格）。

步驟 28. 卸除式磁碟機掃描設定

設定	預設值	敘述
掃描透過 USB 連接的卸除式磁碟機	已清除核取方塊	您可以開啟或關閉透過 USB 連線到受防護電腦上的卸除式磁碟機的掃描。
掃描卸除式磁碟機，如果其儲存資料量未超過 (MB)：	1024 MB	您可透過在卸除式磁碟機上設定最大資料量，來縮小元件的範圍。 如果儲存的資料量超出指定值，Kaspersky Embedded Systems Security 2.2 不會執行卸除式磁碟機掃描。
掃描時使用的安全等級	最佳防護	您可透過選擇以下三個安全等級之一來配置建立的自訂掃描工作： • 最佳防護 • 建議 • 最佳效能 當偵測到已感染、疑似感染和其他物件時使用的算法，以及每個安全等級的其他掃描設定，對應於自訂掃描工作中的預設安全等級。

► *要配置在連線時對卸除式磁碟機進行掃描，請執行以下操作：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**選項**”部分中，點擊“**卸除式磁碟機掃描**”設定塊中的“**設定**”。

   將開啟“**卸除式磁碟機掃描**”視窗。
4. 在“**連接時掃描**”部分中，執行以下操作：
   - 如果想讓 Kaspersky Embedded Systems Security 2.2 在卸除式磁碟機連線時自動掃描，請選擇“**掃描透過 USB 連接的卸除式磁碟機**”核取方塊。
   - 如果需要，選中“**掃描卸除式磁碟機，如果其儲存資料量未超過(MB)**”，然後在右側的欄位中指定最大值。
   - 在“**掃描時使用的安全等級**”下拉清單中，指定卸除式磁碟機掃描所需設定的安全等級。
5. 點擊“**確定**”。

   即會儲存並套用指定設定。

在卡巴斯基安全管理中心中設定存取權限

您可在卡巴斯基安全管理中心中，為一組電腦或單台電腦設定用於管理應用程式和 Kaspersky Security 服務的存取權限。

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *設定用於管理應用程式和 Kaspersky Security 服務的存取權限：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 開啟“**選項**”部分，然後執行以下操作：
   - 要為一個使用者或一組使用者設定管理 Kaspersky Embedded Systems Security 2.2 的存取權限，在“**應用程式管理的使用者存取權限**”部分中點擊“**設定**”按鈕。
   - 要為一個使用者或一組使用者設定管理 Kaspersky Security 服務的存取權限，在“**Security 服務管理的使用者存取權限**”部分中點擊“**設定**”按鈕。
4. 在開啟的視窗中，根據需要設定存取權限（請參見第 69 頁上的“Kaspersky Embedded Systems Security 2.2 功能的存取權限”部分）。

將儲存指定設定。

在卡巴斯基安全管理中心中配置隔離和備份設定

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *在卡巴斯基安全管理中心中管理一般備份設定：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**選項**”部分，點擊“**儲存**”設定區域下的“**設定**”按鈕。
4. 請使用“**儲存**”視窗的“**備份**”標籤配置以下**備份**設定：
   - 若要指定**備份資料夾**，請使用“**備份資料夾**”欄位在受防護電腦的本機硬碟上選擇所需的資料夾，或輸入資料夾的完整路徑。
   - 若要設定最大**備份**容量，請選定“**最大備份空間(MB)**”選擇方塊，然後在輸入欄位中指定此參數的值（單位為 MB）。
   - 若要設置備份中的可用空間值，請定義“**最大備份空間(MB)**”的設定值，選定“**可用空間上限值(MB)**”選框並以 MB 為單位指定**備份**檔案夾中的最小可用空間值。
   - 若要為還原的物件指定資料夾，請在“還原設定”區域中選擇受防護電腦的本機硬碟上的相關資料夾，或者在“**還原物件的指定資料夾**”欄位中輸入資料夾名稱及其完整路徑。
5. 在“**儲存**”視窗的“**隔離**”頁籤上，配置以下**隔離**設定：
   - 若要變更**隔離**資料夾，請在“**隔離**”資料夾輸入欄位中指定受防護電腦本機硬碟上的資料夾完整路徑。
   - 若要設定**隔離**最大容量，請選定“**最大隔離區空間(MB)**”核取方塊，然後在輸入欄位中指定此參數的值（單位為 MB）。
   - 若要設定**隔離**儲存中的最小可用空間量，請選定“**最大隔離區空間(MB)**”核取方塊和“**可用空間上限值(MB)**”核取方塊，然後在輸入欄位中指定此參數值（單位為 MB）。
   - 若要變更將隔離中的物件還原到指定資料夾，請在“**還原物件的指定資料夾**”輸入欄位中指定在受防護電腦本機硬碟上的資料夾完整路徑。
6. 點擊“**確定**”。

將儲存配置的隔離和備份設定。

配置記錄和通知

可以使用卡巴斯基安全管理中心管理主控台為管理員和使用者設定通知，以使其瞭解下列與 Kaspersky Embedded Systems Security 2.2 和受防護電腦上的防毒軟體防護狀態有關的事件：

- 管理員可以收到有關選定類型事件的資訊；
- 存取受防護電腦的區網使用者和終端電腦使用者可以收到與 *偵測到的物件*類型事件有關的資訊。

可以為單台電腦或一組電腦配置有關 Kaspersky Embedded Systems Security 2.2 事件的通知，分別使用選定電腦的“**內容：<電腦名稱>**”視窗或選定管理群組的“**內容：<政策名稱>**”視窗進行配置。

在“**事件**”標籤上或在“**通知設定**”視窗中，可以配置以下類型的通知：

- 可以使用“**事件**”選項（卡巴斯基安全管理中心應用程式的標準標籤）配置有關選定類型事件的管理員通知。有關通知方法的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。
- 在“**通知設定**”視窗中，可以配置管理員通知和使用者通知。

> 在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

您可在視窗中或僅在標籤上配置某些事件種類的通知；您可使用視窗和標籤配置其他事件種類的通知。

> 如果同時在兩個標籤（“**事件**”標籤上和“**通知設定**”視窗中）上使用相同模式配置關於同一類型事件的通知，系統管理員將以相同的模式收到兩次這些事件的通知。

本章節說明項目

配置記錄設定

> 在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *要設定 Kaspersky Embedded Systems Security 2.2 記錄，請執行下列步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**記錄和通知**”部分中，點擊“**工作記錄**”的“**設定**”按鈕。
4. 在“**記錄設定**”視窗中，根據您的需要定義以下 Kaspersky Embedded Systems Security 2.2 設定：
   - 配置記錄中的事件詳細等級。為此，請執行以下操作：
     a. 在“**元件**”清單中，選擇您要設定其詳細等級的 Kaspersky Embedded Systems Security 2.2 元件。
     b. 若要定義選定元件的工作記錄和系統稽核記錄中的詳細等級，請從“**重要性等級**”中選擇所需等級。
   - 要變更記錄的預設位置，請指定資料夾的絕對路徑，或點擊“**瀏覽**”按鈕進行選擇。
   - 指定工作記錄的儲存天數。
   - 指定“**系統稽核記錄**”節點中顯示的資訊儲存天數。
5. 點擊“**確定**”。

已儲存配置的記錄設定。

安全記錄

Kaspersky Embedded Systems Security 2.2 保持有與受防護電腦上的安全入侵或嘗試進行安全入侵相關的事件的記錄。本記錄中記錄以下事件：

- 弱點利用防禦事件。
- 關鍵記錄審查事件。
- 表示嘗試進行安全入侵的緊急事件（對於“即時電腦防護”、“自訂掃描”、“檔案完整性監控”、“應用程式啟動控制”和“裝置控制”工作）。

您可以清除安全記錄以及系統稽核記錄。此外，Kaspersky Embedded Systems Security 2.2 記錄與清除安全記錄相關的系統稽核事件。

配置 SIEM 整合設定

為了減小低效能裝置上的負載和降低由於應用程式記錄量增大而造成系統效能降級的風險，可以透過 Syslog 協定將審查事件和工作效能事件的發佈配置到 *syslog 伺服器*。

syslog 伺服器是用於聚合事件 (SIEM) 的外部伺服器。它可以收集和分析接收到的事件，還可以執行管理記錄的其他操作。

可以在兩種模式中使用 SIEM 整合：

- syslog 伺服器上的重複事件：此模式指定其發佈在記錄設定中進行配置的所有工作效能事件，以及即使被傳送到 SIEM 後仍繼續儲存到本機電腦上的所有系統稽核事件。

  建議使用此模式，以便能夠最大限度地減小受防護電腦上的負載。

- 刪除事件的本機副本：此模式指定將從本機電腦上刪除在應用程式執行過程中註冊和已發佈到 SIEM 的所有事件。

  > 應用程式永遠不會刪除安全記錄的本機版本。

Kaspersky Embedded Systems Security 2.2 可以將應用程式記錄中的事件轉換為 syslog 伺服器支援的格式，以便這些事件能夠被傳輸和被 SIEM 成功識別。應用程式支援轉換為結構化資料格式和 JSON 格式。

為了降低將事件傳輸到 SIEM 的不成功的風險，可以定義連線到映像 syslog 伺服器的設定。

映像 syslog 伺服器是一個額外的 syslog 伺服器，如果與主 syslog 伺服器的連線不可用或不能使用主要伺服器，應用程式會自動轉換到該伺服器。

預設情況下，不使用 SIEM 整合。可以啟用和停用 SIEM 整合，並配置功能性設定（請參見以下表格）。

步驟 29. SIEM 整合設定

設定	預設值	敘述
透過 syslog 協定傳送事件到遠端 syslog 伺服器	未套用	可以分別透過選擇或清除該核取方塊來啟用或停用 SIEM 整合。
刪除已被傳送到遠端 syslog 伺服器的事件本機副本	未套用	可以為儲存記錄的本機副本配置設定（透過選擇或清除該核取方塊將它們傳送到 SIEM 後）。
事件格式	結構化資料	可以選擇以下兩種格式之一，應用程式在將事件傳送到 syslog 伺服器以便 SIEM 能夠更好進行識別之前，將其事件轉換為該格式。
連線協定	TCP	可以使用下拉清單來配置透過 UDP 或 TCP 協定與主 syslog 伺服器的連線，以及透過 TCP 協定與映像 syslog 伺服器的連線。

設定	預設值	敘述
主 syslog 伺服器連線設定	IP 位址: 127.0.0.1 連接埠: 514	可以使用適當的欄位來配置用於連線到主 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。
如果無法存取主伺服器則使用映像 syslog 伺服器	未套用	可以使用核取方塊來啟用或停用映像 syslog 伺服器。
映像 syslog 伺服器連線設定	IP 位址: 127.0.0.1 連接埠: 514	可以使用適當的欄位來配置用於連線到主 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。

► *要配置 SIEM 整合設定：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**記錄和通知**”部分中，點擊“**工作記錄**”的“**設定**”按鈕。

   將開啟“**記錄和通知設定**”視窗。
4. 選擇“**SIEM 整合**”標籤。
5. 在“**整合設定**”部分中，選擇“**透過 syslog 協定傳送事件到遠端 syslog 伺服器**”核取方塊。

   該核取方塊可啟用或停用將已發佈的事件傳送到外部 syslog 伺服器的功能。

   如果選中該核取方塊，則應用程式將根據配置的 SIEM 整合設定將已發佈的事件傳送到 SIEM。

   如果清除該核取方塊，則應用程式不執行 SIEM 整合。如果該核取方塊已被清除，則無法配置 SIEM 整合設定。

   預設取消選定該核取方塊。

6. 如果需要，在“**整合設定**”部分中，選擇“**刪除已被傳送到遠端 syslog 伺服器的事件本機副本**”核取方塊。

   該核取方塊可啟用或停用傳送到 SIEM 後記錄本機副本的刪除。

   如果選中該核取方塊，則應用程式在事件被成功發佈到 SIEM 後刪除事件的本機副本。建議在低效能電腦上使用此模式。

   如果清除該核取方塊，則應用程式僅將事件傳送到 SIEM。記錄的副本將繼續儲存在本機。

   預設取消選定該核取方塊。

> “**刪除已被傳送到遠端 syslog 伺服器的事件本機副本**”核取方塊的狀態不會影響儲存安全記錄檔案事件的設定：應用程式永遠不會自動刪除安全記錄事件。

7. 在“**事件格式**”部分中，指定您要將應用程式操作事件轉換為該格式的格式，以便能夠將它們傳送到 SIEM。

   預設情況下，應用程式將它們轉換為結構化資料格式。

8. 在“**連線設定**”部分中：
   - 指定 SIEM 連線協定。
   - 指定用於連線到主 syslog 伺服器的設定。

     可以僅指定 IP 位址為 IPv4 格式。
   - 如果需要，當無法傳送事件到主 syslog 伺服器時，如果想讓應用程式使用其他連線設定，請選擇“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊。
     - 指定用於連線到映像 syslog 伺服器的設定：**IP 位址**和**連接埠**。

       如果已清除“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊，則無法編輯映像 syslog 伺服器的“**IP 位址**”和“**連接埠**”欄位。

       可以僅指定 IP 位址為 IPv4 格式。
9. 點擊“**確定**”。

將套用已配置的 SIEM 整合設定。

配置通知設定

► *要設定 Kaspersky Embedded Systems Security 2.2 通知，請執行下列步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

> 如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**記錄和通知**”部分中，點擊“**事件通知**”設定區域下的“**設定**”按鈕。
4. 在“**通知設定**”視窗中，根據您的需要定義以下 Kaspersky Embedded Systems Security 2.2 設定：
   - 在“**通知設定**”清單中，選擇想要配置其設定的通知類型。
   - 在“**通知使用者**”部分中，配置使用者通知方式。如有必要，輸入通知訊息的文字。
   - 在“**通知管理員**”部分中，配置管理員通知方式。如有必要，輸入通知訊息的文字。如有必要，透過點擊“**設定**”按鈕配置附加通知設定。
   - 在“**事件產生上限值**”部分中，指定 Kaspersky Embedded Systems Security 2.2 記錄“*應用程式資料庫已過期*”、“*應用程式資料庫已嚴重過期*”和“*已很長時間未執行關鍵區域掃描*”事件的時間間隔。
     - **應用程式資料庫已過期（天）**

       自上次資料庫更新以來的天數。

       預設值為 7 天。
     - **資料庫已長時間未更新（天）**

       自上次資料庫更新以來的天數。

       預設值為 14 天。
     - **已很長時間未執行關鍵區域掃描（天）**

       上次成功完成關鍵區域掃描後的天數。

       預設值為 30 天。
5. 點擊“**確定**”。

將儲存設定的通知設定。

配置與管理伺服器的互動

► *要選擇 Kaspersky Embedded Systems Security 2.2 將其有關資訊傳送到卡巴斯基安全管理中心管理伺服器的物件類型：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**記錄和通知**”**部分中**，**點擊**“**與管理伺服器互動**”設定塊中的“設定”按鈕。

   將開啟“**管理伺服器網路清單**”視窗。

4. 在“**管理伺服器網路清單**”視窗中，選擇 Kaspersky Embedded Systems Security 2.2 將其有關資訊傳送到卡巴斯基安全管理中心管理伺服器的物件類型：

   - 隔離的物件。
   - 備份物件。

5. 點擊“**確定**”。

   Kaspersky Embedded Systems Security 2.2 會將有關選定物件類型的資訊傳送到啟動伺服器。

即時電腦防護

本節提供有關以下“ 即時電腦防護”元件的資訊：“ 即時檔案防護”、“ KSN 使用”、“ 弱點利用防禦”。還提供有關如何設定即時防護工作和管理受防護電腦的安全設定說明。

本章內容

即時檔案防護

本節包含有關即時檔案防護工作以及如何設定的資訊。

本章節說明項目

關於“ 即時檔案防護”工作

“ 即時檔案防護”工作執行期間，在存取以下受防護的電腦物件時，Kaspersky Embedded Systems Security 2.2 會對這些物件進行掃描：

- 檔案。
- 交換檔案系統執行緒（NTFS 執行緒）。
- 本機硬碟和外部裝置上的主開機紀錄區和啟動磁區。
- Windows Server® 2016 和 Windows Server 2019 容器檔案。

當任何應用程式將檔案寫入電腦或從電腦上讀取檔案時，Kaspersky Embedded Systems Security 2.2 會攔截此檔案進行掃描以偵測其是否存在威脅；如果偵測到威脅，則執行您所指定的操作：嘗試清除檔案、將其置於隔離或將其刪除。如果檔案未感染或者已成功解毒，Kaspersky Embedded Systems Security 2.2 會將檔案返回給應用程式。

Kaspersky Embedded Systems Security 2.2 會攔截在 Windows Server 2016 和 Windows Server 2019 容器中執行的檔案操作。

*容器*是一個隔離的環境，允許應用程式在不與作業系統直接互動的情況下執行。如果容器位於工作防護範圍內，Kaspersky Embedded Systems Security 2.2 會掃描使用者正在存取的容器檔案是否存在電腦威脅。偵測到威脅時，應用程式將嘗試解毒容器的威脅。如果嘗試成功，容器將繼續工作；如果解毒失敗，容器將關閉。

Kaspersky Embedded Systems Security 2.2 還會偵測在 Windows Subsystem for Linux® 下執行的處理程序是否存在惡意軟體。對於此類處理程序，“ 即時檔案防護”工作將套用目前配置定義的操作。

配置“ 即時檔案防護”工作

預設情況下，“ 即時檔案防護”系統工作將使用下表敘述的設定。您可以變更這些設定值。

步驟 30. “ 即時檔案防護”工作預設值

設定	預設值	敘述
防護範圍	整個電腦，虛擬磁碟機除外。	您可以限制防護範圍。
安全等級	整個防護範圍的一般設定；對應“ **建議**”安全等級。	您可以對電腦檔案資源樹狀目錄中選定的節點執行以下操作： • 套用另一個預設的安全等級。 • 手動編輯安全等級。 • 將選定節點的安全性設定另存為範本以便以後使用。
物件防護模式	存取及修改時。	您可以選擇防護模式，即定義 Kaspersky Embedded Systems Security 2.2 掃描物件所採用的存取類型。
啟發式分析	套用“ **中度**”安全等級。	您可以啟用或停用“ 啟發式分析”並設定分析等級。
套用信任區域	已套用。	可用於所選工作中的一般排除清單。
使用 KSN 防護	已套用。	您可以使用卡巴斯基安全網路雲端服務的基礎架構提高您的電腦防護能力（接受 KSN 聲明後可用）。
工作啟動排程	程式啟動時。	您可以配置排程的工作啟動。

► *若要配置“即時檔案防護”工作設定，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 要編輯“**即時檔案防護**”工作的預設設定，請點擊“**即時檔案防護**”部分中的“**設定**”按鈕。

   將開啟“**即時檔案防護**”視窗。
4. 設定以下工作設定：
   - 在“**一般**”標籤上：
     - 防護模式（請參見第 135 頁上的“選擇防護模式”部分）
     - 使用啟發式分析（第 134 頁上）
     - 與其他 Kaspersky Embedded Systems Security 2.2 元件的整合的設定。
   - 在“**工作管理**”標籤上：
     - 排程工作啟動配置（請參見第 107 頁上的“配置工作啟動排程設定”部分）。
5. 選擇“**防護範圍**”標籤，然後執行以下操作：
   - 點擊“**新增**”或“**編輯**”按鈕編輯防護範圍（請參見第 136 頁上的“‘即時檔案防護’工作的防護範圍”部分）。
     - 在開啟的視窗中，選擇要包含到工作的防護範圍的內容：
       - **預設的範圍**
       - **磁碟、資料夾或網路資料夾**
       - **檔案**
     - 選擇一項預定義安全等級（請參見第 137 頁上的“選擇預定義安全等級”部分）或手動配置防護（請參見第 139 頁上的“手動配置安全設定”部分）設定。
6. 在“**即時檔案防護**”視窗中點擊“**確定**”。

Kaspersky Embedded Systems Security 2.2 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在工作記錄中。

使用啟發式分析

您可以使用啟發式分析並設定 Kaspersky Embedded Systems Security 2.2 工作的分析等級。

► *設定啟發式分析：*

1. 開啟您要為其配置啟發式分析的應用程式設定（請參見第 110 頁上的“從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security 2.2”部分）或政策設定（請參見第 80 頁上的“配置政策”部分）。
2. 清除或選中“**使用啟發式分析**”核取方塊。

   此核取方塊可在物件掃描過程中啟用/停用啟發式分析。

   如果選中該核取方塊，則啟用啟發式分析。

   如果取消選中該核取方塊，則停用啟發式分析。

   預設將會選定該核取方塊。
3. 如有必要，使用滑塊調整分析等級。

   使用滑塊可以調整啟發式分析等級。掃描強度等級用於在威脅搜尋的徹底程度、作業系統資源負荷和掃描所需時間之間建立平衡。

   以下掃描強度等級可用：

   - **輕度**。啟發式分析在可執行檔中執行較少的操作。在該模式下偵測出威脅的可能性較小。掃描速度較快，而且佔用資源較少。
   - **中度**。啟發式分析在可執行檔中執行 Kaspersky Lab 專家建議的多條指令。

     預設選中該等級。
   - **深度**。啟發式分析在可執行檔中執行較多的操作。在該模式下偵測出威脅的可能性較大。掃描使用更多的系統資源、花費更多時間且可導致更多的誤報。

     如果選中“**使用啟發式分析**”核取方塊，則滑塊才可用。
4. 點擊“**確定**”。

設定的工作設定將立即套用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

選擇防護模式

在 即時檔案防護”工作中，可以選擇防護模式。在 **物件防護模式**”部分中，您可以指定 Kaspersky Embedded Systems Security 2.2 在掃描物件時所採用的存取類型。

“ **物件防護模式**”設定中的值套用於在工作中指定的整個防護範圍。無法為防護範圍內的單個節點指定不同的設定值。

► *若要選擇防護模式，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“ **受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“ **政策**”標籤，然後開啟“ **內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“ **裝置**”標籤，然後開啟“ **應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“ **應用程式設定**”視窗編輯這些設定。
3. 在“ **即時電腦防護**”工作的預設設定，請點擊“ **即時檔案防護**”部分中的“ **設定**”按鈕。

   將開啟“ **即時檔案防護**”視窗。
4. 在開啟的視窗中，開啟“ **一般**”標籤，然後選擇要設定的防護模式：
   - **智慧模式**

     Kaspersky Embedded Systems Security 2.2 自行選擇要掃描的物件。在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。在處理程序執行過程中，如果多次調用物件或對該物件進行了修改，則 Kaspersky Embedded Systems Security 2.2 僅在處理程序最後一次儲存物件之後重新掃描該物件。
   - **存取及修改時**

     Kaspersky Embedded Systems Security 2.2 在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。

     預設選中該選項。
   - **存取時**

     Kaspersky Embedded Systems Security 2.2 在物件開啟以進行讀取、執行或修改時掃描所有物件。
   - **執行時**

     僅在存取檔案以執行該檔案時 Kaspersky Embedded Systems Security 2.2 才掃描該檔案。
5. 點擊“ **確定**”。

選中防護模式將生效。

“即時檔案防護”工作的防護範圍

本節提供有關在即時檔案防護工作中建立和管理防護範圍的說明。

本章節說明項目

預設的防護範圍

受防護電腦的檔案資源顯示在“**防護範圍**”標籤上的“**即時檔案防護**”工作設定中。

檔案資源樹狀目錄或清單顯示基於 Microsoft Windows 的配置安全設定所擁有的讀取存取權限的節點。

Kaspersky Embedded Systems Security 2.2 覆寫以下預設防護範圍：

- **本機磁碟**。Kaspersky Embedded Systems Security 2.2 將防護電腦硬碟磁碟機中的檔案。
- **卸除式磁碟機**。Kaspersky Embedded Systems Security 2.2 將防護外部裝置上的檔案，如 CD 或 USB 磁碟機。您可以在防護範圍中包含或排除所有卸除式裝置、單個磁碟、資料夾或檔案。
- **網路**。Kaspersky Embedded Systems Security 2.2 將掃描電腦上執行的應用程式寫入到網路資料夾或從網路資料夾讀取的檔案。當其他電腦上的應用程式存取此類檔案時，Kaspersky Embedded Systems Security 2.2 不會防護此類檔案。
- **虛擬磁碟機**。您可以將動態資料夾和檔案以及臨時連線到電腦的硬碟包含在防護範圍內，例如共用叢集硬碟。

預設情況下，您可以在範圍清單中檢視和配置預設防護範圍；還可以在清單形成期間在設定防護範圍中向該清單新增預設範圍。

預設情況下，防護範圍包括除虛擬磁碟機外的所有預定義區域。

使用 SUBST 指令建立的虛擬磁碟機將不會顯示在應用程式主控台的電腦檔案資源樹狀目錄中。若要將虛擬磁碟機中的物件包含在防護範圍內，請將與此虛擬磁碟機關聯的電腦資料夾包含在防護範圍內。
已連線的網路磁碟也不會顯示在電腦檔案資源清單中。若要將網路磁碟中的物件包含在防護範圍內，請以 UNC 格式指定與該網路磁碟對應的資料夾的路徑。

選擇預設安全等級

可以為電腦檔案資源清單中的選定節點套用下面預定義安全等級之一：“ **最佳效能**”、“ **建議**”和“ **最佳防護**”。這些等級均有各自的安全性設定集（請參閱下表）。

最佳效能

如果除了在電腦上使用 Kaspersky Embedded Systems Security 2.2 外，還在網路內採取了其他電腦安全措施（例如，防火牆和現有安全政策），則建議使用“ **最佳效能**”的安全等級。

建議

“ **建議**”安全等級確保防護與對電腦的效能影響的最佳組合。Kaspersky Lab 專家建議使用該等級，因為它足以防護大多數公司網路上的電腦。預設情況下，將設定“ **建議**”的安全等級。

最佳防護

如果組織的網路有更高的電腦安全要求，則建議使用“ **最佳防護**”安全等級。

步驟 31. 預設安全等級和相應的設定值

選項	安全等級		
	最佳效能	建議	最佳防護
物件防護	依副檔名	依格式	依格式
僅防護新增與變更過的檔案	已啟用	已啟用	已停用
對受感染物件和其他物件執行的操作	封鎖存取並解毒。解毒失敗則刪除	封鎖存取並執行建議的操作	封鎖存取並解毒。解毒失敗則刪除
對疑似感染物件執行的操作	封鎖存取並隔離	封鎖存取並執行建議的操作	封鎖存取並隔離
排除檔案	否	否	否
不偵測	否	否	否
超過以下時間則停止掃描(秒)	60 秒	60 秒	60 秒
不掃描超過此值複合檔案(MB)	8 MB	8 MB	未設定
掃描 NTFS 交換資料串流	是	是	是
掃描開機磁區和 MBR	是	是	是
複合物件防護	• 已封裝的物件* *僅新物件和已修改的物件	• SFX 壓縮檔案* • 已封裝的物件* • 嵌入的 OLE 物件* *僅新物件和已修改的物件	• SFX 壓縮檔案* • 已封裝的物件* • 嵌入的 OLE 物件* *所有物件
在偵測到嵌入物件時完全刪除應用程式無法修改的複合檔案	否	否	是

預設安全等級設定中不包含“**物件防護**”、“**使用 iChecker 技術**”、“**使用 iSwift 技術**”和“**使用啟發式分析**”設定。若變更了“**物件防護**”、“**使用 iChecker 技術**”、“**使用 iSwift 技術**”、“**使用啟發式分析**”，所選的安全等級不會變更。

► *要選擇一個預設安全等級，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**即時電腦防護**”工作的預設設定，請點擊“**即時檔案防護**”部分中的“**設定**”按鈕。

   將開啟“**即時檔案防護**”視窗。
4. 在“**防護範圍**”標籤上，選擇您要配置其安全設定的節點，然後點擊“**配置**”。

   將開啟“**即時檔案防護設定**”視窗。
5. 在下拉清單中選擇所需的安全等級：
   - **最佳防護**
   - **建議**
   - **最佳效能**
6. 點擊“**確定**”。

已儲存新配置的設定。

Kaspersky Embedded Systems Security 2.2 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在工作記錄中。

手動配置安全設定

預設情況下，“即時檔案防護”工作對整個防護範圍使用通用安全設定。這些設定對應于“**建議**”預設安全等級（請參見第 137 頁上的“選擇預設安全等級”部分）。

若要修改安全性設定的預設值，可透過將它們配置為用於整個防護範圍的一般設定，或為電腦檔案資源清單或樹狀目錄中的不同節點配置不同設定。

在使用電腦檔案資源樹狀目錄時，為所選父節點配置的安全設定將自動套用於所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

► *要手動設定所選節點的安全性設定：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**即時電腦防護**”工作的預設設定，請點擊“**即時檔案防護**”部分中的“**設定**”按鈕。

   將開啟“**即時檔案防護**”視窗。
4. 在“**防護範圍**”標籤上，選擇您要配置其安全設定的節點，然後點擊“**配置**”。

   將開啟“**即時檔案防護設定**”視窗。
5. 在“**安全等級**”標籤上，可以選擇任意現有等級或點擊“**設定**”按鈕來設定自訂設定。
6. 您可以根據需求配置選定節點的自訂安全設定：
   - 一般設定（請參見第 140 頁上的“配置一般工作設定”部分）
   - 操作（請參見第 142 頁上的“設定操作”部分）
   - 效能（請參見第 144 頁上的“設定效能”部分）
7. 在“**設定防護範圍**”視窗中點擊“**儲存**”。

將儲存新的防護範圍設定。

配置一般工作設定

► *要配置“即時檔案防護”工作的一般安全設定：*

1. 開啟“**即時檔案防護設定**”視窗（請參見第 139 頁上的“手動配置安全設定”部分）。
2. 選擇“**一般**”標籤。
3. 在“**物件防護**”部分中，指定要包含在防護範圍內的物件類型：
   - **所有物件**

     Kaspersky Embedded Systems Security 2.2 將掃描所有物件。
   - **按格式掃描物件**

     Kaspersky Embedded Systems Security 2.2 僅根據檔案格式掃描可感染的物件。

     Kaspersky Lab 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 2.2 資料庫中。
   - **按病毒資料庫中指定的副檔名清單掃描物件**

     Kaspersky Embedded Systems Security 2.2 僅根據檔案副檔名掃描可感染的物件。

     Kaspersky Lab 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 2.2 資料庫中。
   - **按指定的副檔名清單掃描物件**

     Kaspersky Embedded Systems Security 2.2 根據檔案副檔名掃描檔案。可在“**副檔名清單**”視窗（透過點擊“**編輯**”按鈕開啟）中手動自訂檔案副檔名清單。
   - **掃描開機磁區和 MBR**

     啟用對開機磁區和主引導記錄的防護。

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描電腦的硬碟磁碟機和卸除式磁碟機上的開機磁區和主開機記錄。

     預設將會選定該核取方塊。
   - **掃描 NTFS 交換資料串流**

     掃描 NTFS 檔案系統磁碟機上的替代檔案和資料夾執行緒。

     如果選中該核取方塊，應用程式將掃描疑似感染物件以及與該物件關聯的所有 NTFS 執行緒。

     如果清除該核取方塊，應用程式將只掃描偵測到並被視為疑似感染的物件。

     預設將會選定該核取方塊。
4. 在“**效能**”部分中，選中或清除“**僅防護新增與變更過的檔案**”核取方塊。

   使用此核取方塊可啟用/停用對自上次掃描以來 Kaspersky Embedded Systems Security 2.2 識別為新檔案或已修改的檔案的掃描和防護。

   如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 僅掃描和防護自上次掃描以來被識別為新檔案或已修改的檔案。

如果清除該核取方塊，您可以選擇希望僅掃描和防護新檔案，還是掃描和防護所有檔案而略過檔案的修改狀態。

對於“**最佳效能**”和“**建議**”安全等級，預設選定該核取方塊。如果設定“**最佳防護**”安全等級，則取消選中該核取方塊。

如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的“**全部/僅新建**”連結。

5. 在“**複合物件防護**”部分中，指定要包含在防護範圍內的複合物件：

- **全部/僅新建的壓縮檔案**

  掃描 ZIP、CAB、RAR、ARJ 壓縮檔案及其他壓縮檔案格式。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描壓縮檔案。

  如果取消選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過壓縮檔案。

  預設值取決於所選的安全等級。

- **全部/僅新增 SFX 壓縮檔案**

  掃描自解壓壓縮檔案。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描 SFX 壓縮檔案。

  如果取消選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過 SFX 壓縮檔案。

  預設值取決於所選的安全等級。

  如果取消選中“**壓縮檔案**”核取方塊，則該選項處於活動狀態。

- **全部/僅新建的郵件資料庫**

  掃描 Microsoft Outlook® 和 Microsoft Outlook Express 郵件資料庫檔案。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描郵件資料庫檔案。

  如果取消選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過郵件資料庫檔案。

  預設值取決於所選的安全等級。

- **全部/僅新的封裝的物件**

  掃描由二進位代碼封包程式（例如 UPX 或 ASPack）封包的可執行檔。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描由封包程式封包的可執行檔。

  如果取消選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過由封包程式封包的可執行檔。

  預設值取決於所選的安全等級。

- **全部/僅新建的純文字電子郵件**

  掃描郵件格式檔案，例如 Microsoft Office Outlook 和 Microsoft Outlook Express 郵件。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描郵件格式檔案。

  如果取消選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過郵件格式檔案。

  預設值取決於所選的安全等級。

- **所有/僅新的嵌入 OLE 物件**

  掃描嵌入到檔案中的物件（如 Microsoft Word 巨集或電子郵件附件）。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描嵌入到檔案中的物件。

  如果取消選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過嵌入到檔案中的物件。

  預設值取決於所選的安全等級。

6. 點擊“**儲存**”。

將儲存新的工作配置。

配置操作

► *要為“即時檔案防護”工作配置對受感染的物件和其他偵測到的物件的操作：*

1. 開啟“**即時檔案防護設定**”視窗（請參見第 139 頁上的“手動配置安全設定”部分）。
2. 選擇“**操作**”標籤。
3. 選擇要對受感染的物件和其他偵測到的物件執行的操作：

   - **僅通知**。

     選擇此模式時，Kaspersky Embedded Systems Security 2.2 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

     應該為每個防護區域單獨設定“**僅通知**”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 2.2 會自動將安全等級變更為“**自訂**”。

   - **封鎖存取**。

     選擇此選項時，Kaspersky Embedded Systems Security 2.2 會封鎖對偵測到或疑似感染的物件的存取。您可以在下拉清單中選擇對已封鎖物件的其他操作。

   - **執行附加操作**。

     從下拉清單中選擇操作：

     - **解毒**。
     - **解毒。解毒失敗則刪除**。
     - **刪除**。
     - **建議**。

4. 選擇要對疑似感染的物件執行的操作：

   - **僅通知**。

     選擇此模式時，Kaspersky Embedded Systems Security 2.2 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

     應該為每個防護區域單獨設定“**僅通知**”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 2.2 會自動將安全等級變更為“**自訂**”。

   - **封鎖存取**。

     選擇此選項時，Kaspersky Embedded Systems Security 2.2 會封鎖對偵測到或疑似感染的物件的存取。您可以在下拉清單中選擇對已封鎖物件的其他操作。

   - **執行附加操作**。

     從下拉清單中選擇操作：

     - **隔離**。
     - **刪除**。
     - **建議**。

5. 選擇依威脅類型對物件執行的操作：

   a. 清除或選中“**根據偵測到的物件的類型執行操作**”核取方塊。

      如果選中該核取方塊，可以透過點擊該核取方塊旁邊的“**設定**”按鈕來設定針對每種偵測到的物件類型的主要和次要操作。

      如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 將對指定的物件類型分別執行在“**對受感染物件和其他物件執行的操作**”和“**對疑似感染物件執行的操作**”部分中選擇的操作。

      預設取消選定該核取方塊。

   b. 點擊“**設定**”按鈕。

   c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要和次要操作（如果主要操作失敗）。

   d. 點擊“**確定**”。

6. 選擇要對不可修改的複合物件執行的操作：選擇或清除“**在偵測到嵌入物件時完全刪除應用程式無法修改的複合檔案**”核取方塊。

   此核取方塊用於啟用或停用當偵測到惡意、疑似感染或其他偵測到的子嵌入物件時強制刪除父複合檔案。

   如果選中該核取方塊並且工作設定為刪除受感染和疑似感染的物件，Kaspersky Embedded Systems Security 2.2 會在偵測到惡意或其他嵌入物件時強制刪除整個父複合物件。如果應用程式無法只刪除偵測到的子物件（例如，如果父物件不可修改），將強制刪除父物件及其所有內容。

如果清除該核取方塊並且工作設定為刪除受感染和疑似感染的物件，當父物件不可修改時，Kaspersky Embedded Systems Security 2.2 不會執行所選操作。

預設情況下，對於“**最佳防護**”安全等級選中該核取方塊，對於“**建議**”和“**最佳效能**”安全等級清除該核取方塊。

7. 點擊“**儲存**”。

將儲存新的工作配置。

配置效能

► *要配置“即時檔案防護”工作的效能：*

1. 開啟“**即時檔案防護設定**”視窗（請參見第 139 頁上的“手動配置安全設定”部分）。
2. 選擇“**效能**”標籤。
3. 在“**排除**”部分中：
   - 清除或選中“**排除檔案**”核取方塊。

     按檔案名或檔案名遮罩從掃描中排除檔案。

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過指定的物件。

     如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描所有物件。

     預設取消選定該核取方塊。
   - 清除或選中“**不偵測**”核取方塊。

     按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書網站 http://www.securelist.com 上提供了可偵測物件的名稱清單。

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在掃描期間略過指定的可偵測物件。

     如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 預設將偵測程式中指定的所有物件。

     預設取消選定該核取方塊。
   - 針對每個設定點擊“**編輯**”按鈕以新增排除項目。
4. 在“**進階設定**”部分中：
   - **超過以下時間則停止掃描(秒)**

     限制物件掃描的持續時間。預設值為 60 秒。

     如果選中該核取方塊，則掃描持續時間將限制為指定的值。

     如果取消選中該核取方塊，則對掃描持續時間沒有限制。

     預設將會選定該核取方塊。

- **不掃描超過此值複合檔案(MB)**

  將超過指定大小的物件排除在掃描之外。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 將在病毒掃描期間略過大小超過指定限制值的複合物件。

  如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 將掃描任意大小的複合物件。

  對於“**建議**”和“**最佳效能**”安全等級，預設選中該核取方塊。

- **使用 iSwift 技術**

  iSwift 將資料庫中儲存的檔案 NTFS 識別碼與目前識別碼進行比較。只對識別碼發生變化的檔案（新檔案和自上次掃描 NTFS 系統物件以來修改過的檔案）執行掃描。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 僅掃描自上次掃描 NTFS 系統物件以來新建或修改的檔案。

  如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 在掃描 NTFS 系統檔案時將不考慮檔案建立或修改的日期。

  預設將會選定該核取方塊。

- **使用 iChecker 技術**

  iChecker 會計算並記住掃描的檔案的校驗和。如果物件被修改，校驗和會發生變化。應用程式在掃描工作中比較所有校驗和，並且僅掃描新檔案和自上次掃描檔案以來修改過的檔案。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 僅掃描新檔案和修改的檔案。

  如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 在掃描檔案時將不考慮檔案建立或修改的日期。

  預設將會選定該核取方塊。

5. 點擊“**儲存**”。

將儲存新的工作配置。

KSN 使用

本節包含有關“KSN 使用”工作以及如何設定的資訊。

本章節說明項目

關於“ KSN 使用”工作

卡巴斯基安全網路（也稱為“ KSN”）是一個線上服務的基礎架構，提供存取 Kaspersky Lab 有效的知識庫。該知識庫中包含了檔案信譽、網頁資源和程式的相關資訊。卡巴斯基安全網路允許 Kaspersky Embedded Systems Security 2.2 十分迅速地對新威脅作出反應，提高許多防護元件的效能，以降低誤報可能性。

要啟動“ KSN 使用”工作，您必須接受卡巴斯基安全網路聲明。

Kaspersky Embedded Systems Security 2.2 從卡巴斯基安全網路接收的資訊僅與程式的信譽有關。

加入 KSN 使 Kaspersky Lab 能夠接收有關新威脅類型和來源的資訊，研發出使其失效的方法，並減少應用程式元件中的誤報數量。

有關傳輸、處理、儲存和銷毀有關應用程式使用情況的更多詳細資訊在“ KSN 使用”工作的“資料處理”視窗中和 Kaspersky Lab 網站上的隱私政策中提供。

加入卡巴斯基安全網路完全出於自願。在安裝 Kaspersky Embedded Systems Security 2.2 後，做出有關參加卡巴斯基安全網路的決定。您可以隨時變更有關參加卡巴斯基安全網路的決定。

可在以下 Kaspersky Embedded Systems Security 2.2 工作中使用卡巴斯基安全網路：

- 即時檔案防護。
- 自訂掃描。
- 應用程式啟動控制。

卡巴斯基專屬安全網路

有關如何配置卡巴斯基專屬安全網路（以下稱“專屬 KSN”）的詳細資訊，請參見《*卡巴斯基安全管理中心說明*》。

如果在受防護電腦上使用專屬 KSN，則在“ KSN 使用”工作的“**資料處理**”視窗（參見第 149 頁的“配置資料處理”部分）中，可以透過選擇“**我接受卡巴斯基專屬安全網路聲明的條款**”核取方塊來閱讀 KSN 聲明和啟用該工作。接受該條款，即表示您同意將 KSN 聲明中提到的各類資料（安全請求、統計資料）傳送到 KSN 服務。

接受專屬 KSN 條款後，用於調整全球 KSN 使用的核取方塊將不可用。

如果在“ KSN 使用”工作執行時停用專屬 KSN，則將出現*產品授權衝突*錯誤且工作將停止。要繼續防護電腦，您需要接受“**資料處理**”視窗中的 KSN 聲明並重新啟動該工作。

撤銷接受 KSN 聲明

您可以隨時撤銷接受聲明並停止與卡巴斯基安全網路的任何資料交換。以下操作被視為完全或部分撤銷 KSN 聲明：

- 清除“**傳送關於已掃描檔案的資料**”核取方塊：應用程式停止將掃描的檔案的校驗和傳送到 KSN 服務進行分析。
- 清除“**傳送卡巴斯基安全網路統計資訊**”核取方塊：應用程式停止處理附加 KSN 統計資訊的資料。
- 清除“**我接受卡巴斯基安全網路聲明的條款**”核取方塊：應用程式停止所有與 KSN 相關的資料處理，“KSN 使用”工作停止。
- 移除“KSN 使用”元件：所有與 KSN 相關的資料處理都將停止。
- 移除 Kaspersky Embedded Systems Security 2.2：所有與 KSN 相關的資料處理都將停止。

配置“KSN 使用”工作

您可以變更“KSN 使用”工作的預設設定（請參見下表）。

步驟 32. “KSN 使用”工作預設設定

設定	預設值	敘述
對 KSN 不信任的物件執行的操作	刪除	您可以指定 Kaspersky Embedded Systems Security 2.2 對 KSN 標識為不受信任的物件執行的操作。
資料傳輸	為大小不超過 2 MB 的檔案計算檔案校驗和（MD5 雜湊）。	您可以指定要使用 MD5 演算法為其計算校驗和以提交給 KSN 的檔案的最大大小。如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 將為任意大小的檔案計算 MD5 雜湊校驗和。
KSN 聲明	“**我接受卡巴斯基安全網路聲明的條款**”核取方塊處於清除狀態。	在安裝後決定是否要參加 KSN。您可以隨時變更決定。
傳送卡巴斯基安全網路統計資訊	選中（僅當接受 KSN 聲明時應用）	如果接受 KSN 聲明，將自動傳送 KSN 統計資訊，除非清除相應核取方塊。
傳送關於已掃描檔案的資料	選中（僅當接受 KSN 聲明時應用）	如果接受 KSN 聲明，將傳送自工作啟動以來掃描和分析的檔案的資料。您可以隨時清除該核取方塊。
我接受 Kaspersky Managed Protection 聲明的條款	已解毒	您可以啟用或停用 KMP 服務。僅當在應用程式購買過程中簽訂了附加協議時，該服務才可用。
工作啟動排程	不設定工作的初次啟動排程。	您可以手動啟動該工作或設定排程啟動。
使用卡巴斯基安全管理中心作為 KSN 代理	選中	預設情況下，資料透過卡巴斯基安全管理中心傳送到 KSN。

► *要設定“KSN 使用”工作，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**即時電腦防護**”部分中，點擊“**KSN 使用**”設定塊中的“**設定**”按鈕。

   將開啟“**KSN 使用**”視窗。
4. 在“**一般**”標籤上，配置以下工作設定：
   - 在“**對 KSN 不信任的物件執行的操作**”部分中，指定 Kaspersky Embedded Systems Security 2.2 在偵測到 KSN 確定為不受信任的物件時將執行的操作：
     - **刪除**

       Kaspersky Embedded Systems Security 2.2 將刪除具有 KSN 不信任狀態的物件，並在備份中放置副本。

       預設選中該選項。
     - **記錄資訊**

       Kaspersky Embedded Systems Security 2.2 將在工作記錄中記錄有關具有 KSN 不信任狀態的物件的資訊。Kaspersky Embedded Systems Security 2.2 不會刪除不受信任的物件。
   - 在“**資料傳輸**”部分中，限制要為其計算校驗和的檔案的大小：
     - 清除或選中“**如果檔案大小超過以下大小，則在傳送到 KSN 之前不計算校驗和 (MB)**”核取方塊。

       此核取方塊可啟用或停用為指定大小的檔案計算校驗和，以將此資訊提交至 KSN 服務。

       校驗和計算的持續時間取決於檔案大小。

       如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 不會為超過指定大小（以 MB 為單位）的檔案計算校驗和。

       如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 將為任意大小的檔案計算校驗和。

       預設將會選定該核取方塊。
     - 如果需要，在右側欄位中變更 Kaspersky Embedded Systems Security 2.2 要為其計算校驗和的最大檔案大小。

- 清除或選中“**使用卡巴斯基安全管理中心作為 KSN 代理**”核取方塊。

  該核取方塊允許管理受防護電腦與 KSN 之間的資料傳輸。

  如果清除該核取方塊，管理伺服器和受防護電腦的資料將直接傳送到 KSN（不透過卡巴斯基安全管理中心）。活動政策定義了哪種類型的資料可以直接傳送到 KSN。

  如果選中該核取方塊，所有資料都透過卡巴斯基安全管理中心傳送到 KSN。

  預設將會選定該核取方塊。

  要啟用 KSN 代理，必須接受 KSN 聲明並正確配置卡巴斯基安全管理中心。有關詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

5. 如果需要，在“**工作管理**”標籤上配置工作啟動排程。例如，如果您希望在重新啟動電腦時自動執行工作，可以按排程啟動工作並指定“**在應用程式啟動時**”頻率。

   應用程式將按排程自動啟動“KSN 使用”工作。

6. 在啟動工作前配置資料處理（請參見第 149 頁上的“配置資料處理”部分）。

7. 點擊“**確定**”。

將應用修改的設定。修改設定的日期和時間以及有關修改前後的工作設定的資訊均儲存在工作記錄中。

配置資料處理

► *要設定哪些資料將被 KSN 服務處理並接受 KSN 聲明：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**即時電腦防護**”部分中，點擊“**KSN 使用**”設定塊中的“**資料處理**”按鈕。

   將開啟“**資料處理**”視窗。
4. 在“**統計資訊和服務**”標籤上，閱讀聲明並選中“**我接受卡巴斯基安全網路聲明的條款**”核取方塊。

5. 為提高防護等級，以下核取方塊會自動選中：

   - **傳送關於已掃描檔案的資料**。

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 會將掃描的檔案的校驗和傳送到 Kaspersky Lab。關於每個檔案的安全性的結論基於從 KSN 收到的信譽。

     如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 不會將檔案的校驗和傳送到 KSN。

     請注意，檔案信譽請求可能在受限模式下傳送。限制用於防護 Kaspersky Lab 信譽伺服器免受 DDoS 攻擊。在這種情況下，所傳送的檔案信譽請求的參數由 Kaspersky Lab 專家建立的規則和方法定義，使用者無法在受防護電腦上進行設定。這些規則和方法的更新與應用程式資料庫更新一起接收。如果應用限制，“KSN 使用”工作統計資訊中將顯示“*由 Kaspersky Lab 啟用以防護 KSN 伺服器免受 DDoS 攻擊*”狀態。

     預設將會選定該核取方塊。

   - **傳送卡巴斯基安全網路統計資訊。**

     如果選中該核取方塊，Kaspersky Embedded Systems Security 2.2 會傳送附加統計資訊，其中可能包括個人資料。作為 KSN 統計資訊傳送的所有資料的清單在 KSN 聲明中有所說明。Kaspersky Lab 收到的資料用於改善應用程式質量和提高威脅偵測速率等級。

     如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 不會傳送其他統計資訊。預設將會選定該核取方塊。

   您可以隨時清除這些核取方塊並停止傳送附加資料。

6. 在“**Kaspersky Managed Protection**”標籤上，閱讀聲明並選中“**我接受 Kaspersky Managed Protection 聲明的條款**”核取方塊。

   如果選中該核取方塊，表示您同意將有關受防護電腦活動的統計資訊傳送給 Kaspersky Lab 專家。接收的資料用於持續不停的分析和報告，是防止安全弱點事件所必需的。

   預設取消選定該核取方塊。

   變更“**我接受 Kaspersky Managed Protection 聲明的條款**”核取方塊狀態不會立即啟動或停止資料處理。要套用變更，必須重新啟動 Kaspersky Embedded Systems Security 2.2。

   要使用 KMP 服務，您需要簽訂服務協議並在受防護電腦上執行設定檔。

   要使用 KMP 服務，必須接受“**統計資訊和服務**”標籤上的 KSN 聲明的資料處理條款。

7. 點擊“**確定**”。

   將儲存資料處理配置。

設定其他資料傳輸

Kaspersky Embedded Systems Security 2.2 可以設定為將以下資料傳送到 Kaspersky Lab：

- 掃描的檔案的校驗和（“**傳送關於已掃描檔案的資料**”核取方塊）。
- 附加統計資訊，包括個人資料（“**傳送卡巴斯基安全網路統計資訊**”核取方塊）。

有關傳送到 Kaspersky Lab 的資料的詳細資訊，請參見本手冊的“本機資料處理”部分。

只有選中“**我接受卡巴斯基安全網路聲明的條款**”核取方塊，才能選中或清除相應的核取方塊。

預設情況下，當您接受 KSN 聲明後，Kaspersky Embedded Systems Security 2.2 將傳送檔案的校驗和和附加統計資訊。

步驟 33. 可能的核取方塊狀態和相應條件

核取方塊狀態	“傳送關於已掃描檔案的資料”核取方塊狀態的條件	“傳送卡巴斯基安全網路統計資訊”核取方塊狀態的條件
☑	• 已傳送信譽請求 • 核取方塊可編輯	• 已傳送附加統計資訊 • 核取方塊可編輯
☑	• 未傳送信譽請求 • 核取方塊不可編輯	• 未傳送附加統計資訊 • 核取方塊不可編輯
☐	• 未傳送信譽請求 • 核取方塊可編輯	• 未傳送附加統計資訊 • 核取方塊可編輯
☐	• 未傳送信譽請求 • 核取方塊不可編輯	• 未傳送附加統計資訊 • 核取方塊不可編輯

弱點利用防禦

本節包含有關如何配置處理程序記憶體防護設定的說明。

本章內容

關於弱點利用防禦

Kaspersky Embedded Systems Security 2.2 提供防護處理程序記憶體免受弱點利用的能力。此功能在“弱點利用防禦”元件中實現。可以變更該元件的活動狀態和配置處理程序記憶體防護設定。

該元件透過在受防護的處理程序中插入外部“處理程序防護代理”（“代理”）防護處理程序記憶體免受弱點利用。

“處理程序防護代理”是一個動態載入的 Kaspersky Embedded Systems Security 2.2 模組，該模組可以插入到受防護的處理程序中，以便監控處理程序的完整性並降低被弱點利用的風險。

該代理在受防護的處理程序內的執行需要啟動和停止處理程序：只有處理程序已重新啟動，才能實現首次載入代理到已新增到受防護的處理程序清單中。此外，從受防護的處理程序清單中刪除處理程序後，只有該處理程序已重新啟動才能移除代理。

必須停止代理才能從受防護的處理程序中移除它：如果已移除“弱點利用防禦”元件，則應用程式將凍結環境並強制從受防護的處理程序中移除代理。如果在元件移除過程中在任一受防護處理程序中插入代理，則必須終止受影響的處理程序。可能需要重新啟動電腦（例如，如果系統處理程序正在受到防護）。

如果偵測到受防護的處理程序中存在弱點利用攻擊的跡象，則 Kaspersky Embedded Systems Security 2.2 執行以下操作之一：

- 如果進行弱點利用嘗試，則終止該處理程序。
- 報告處理程序已遭到入侵的事實。

您可採用以下方法之一停止處理程序防護：

- 移除該元件。
- 從受防護的處理程序清單中移除該處理程序並重新啟動該處理程序。

Kaspersky Security 弱點利用防禦服務

受防護的電腦上必須提供 Kaspersky Security 弱點利用防禦服務，這樣“弱點利用防禦”元件才能發揮最大效果。此服務和“弱點利用防禦”元件是建議安裝的一部分。在受防護的電腦上安裝該服務的過程中，將建立和啟動 kavfswh 處理程序。此處理程序從元件將有關受防護的處理程序的資訊傳輸到安全性代理。

Kaspersky Security 弱點利用防禦服務停止後，Kaspersky Embedded Systems Security 2.2 繼續防護已新增到受防護的處理程序清單中的處理程序，同時也載入到新新增的處理程序中，並使用所有可用的弱點利用防禦技術來防護處理程序記憶體。

如果 Kaspersky Security 弱點利用防禦服務已停止，則應用程式將不會接收隨受防護的處理程序出現的有關事件的資訊（包括有關弱點利用攻擊和處理程序終止的資訊）。此外，代理將無法接收新防護設定和新增新處理程序到受防護的處理程序清單中的有關資訊。

弱點利用防禦模式

可以選擇以下一種模式來配置操作，以降低弱點在受防護處理程序中被利用的風險：

- **發現弱點利用時終止**：當嘗試進行弱點利用時，套用此模式可終止處理程序。

  當偵測到嘗試在受防護的關鍵作業系統處理程序中利用弱點時，無論“弱點利用防禦”元件設定中所指定的模式如何，Kaspersky Embedded Systems Security 2.2 都不會終止處理程序。

- **僅通知被利用的處理程序**：應用此模式可以使用“經過篩選的安全審查”中的事件來接收受防護處理程序中的弱點實例的有關資訊。

  如果選擇此模式，則 Kaspersky Embedded Systems Security 2.2 將透過建立事件來記錄所有利用弱點的嘗試。

配置處理程序記憶體防護設定

► *要配置設定以防護新增到受防護的處理程序清單中的處理程序記憶體，請執行以下操作：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**即時電腦防護**”部分中，點擊“**弱點利用防禦**”設定塊中的“**設定**”按鈕。

   將開啟“**弱點利用防禦**”視窗。
4. 在“**弱點利用防禦模式**”部分中，配置以下設定：
   - **防止易受感染的處理程序被弱點利用**。

     如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 可降低受防護處理程序清單中的處理程序被利用弱點的風險。

     如果清除此核取方塊，則 Kaspersky Embedded Systems Security 2.2 不會防護電腦處理程序免遭弱點利用。

     預設取消選定該核取方塊。
   - **發現弱點利用時終止**。

     如果選擇此模式，則 Kaspersky Embedded Systems Security 2.2 在偵測到弱點利用嘗試時（如果已對該處理程序應用積極的攻擊緩解技術），將終止受防護的處理程序。

- **僅通知被利用的處理程序**。

  如果選擇此模式，則 Kaspersky Embedded Systems Security 2.2 透過顯示一個終端視窗報告弱點利用。被入侵的處理程序將繼續執行。

  如果當應用程式在“**發現弱點利用時終止**”模式中執行時 Kaspersky Embedded Systems Security 2.2 偵測到關鍵處理程序中存在弱點利用，則該元件會強制轉換到“**僅通知被利用的處理程序**”模式。

5. 在“**減輕風險的操作**”部分中，配置以下設定：

   - **透過“終端服務”來通知被利用的處理程序。**

     如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 會顯示一個終端視窗，其中有一個說明，解釋防護被啟動的原因以及指示在其中偵測到弱點利用嘗試的處理程序。

     如果清除該核取方塊，則當偵測到弱點利用嘗試或被入侵的處理程序終止時 Kaspersky Embedded Systems Security 2.2 顯示一個終端視窗。無論 Kaspersky Security 弱點利用防禦服務的狀態如何，都會顯示終端視窗。預設將會選定該核取方塊。

   - **即使 Kaspersky Security 服務已停用，也會防止易受感染的處理程序被弱點利用**。

     如果選中此核取方塊，則無論 Kaspersky Security 服務是否運行，Kaspersky Embedded Systems Security 2.2 都將降低弱點在已啟動的處理程序中被利用的風險。Kaspersky Embedded Systems Security 2.2 不會防護 Kaspersky Security 服務停止後新增的處理程序。服務啟動後，所有處理程序將停止弱點利用風險減輕。

     如果清除此核取方塊，則當 Kaspersky Security 服務停止時，Kaspersky Embedded Systems Security 2.2 不會防護處理程序免遭弱點利用。

     預設將會選定該核取方塊。

6. 點擊“**確定**”。

Kaspersky Embedded Systems Security 2.2 將儲存並套用配置的處理程序記憶體防護設定。

新增進行防護的處理程序

“弱點利用防禦”元件預設防護多個處理程序。可以透過清除清單中的相應核取方塊來將處理程序從防護範圍中排除。

► *要向受防護的處理程序清單中新增處理程序：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**即時電腦防護**”部分中，點擊“**弱點利用防禦**”設定塊中的“**設定**”按鈕。

   將開啟“**弱點利用防禦**”視窗。

4. 在“**受防護處理程序**”標籤上，點擊“**瀏覽**”按鈕。

   將開啟標準 Microsoft Windows 資源管理器視窗。

5. 選擇您要新增到該清單的處理程序。

6. 點擊“**開啟**”按鈕。

   處理程序名稱顯示在行中。

7. 點擊“**新增**”按鈕。

   處理程序將被新增到受防護的處理程序清單中。

8. 選擇新增的處理程序，然後點擊“**設定弱點利用防禦技術**”。

   將開啟“**弱點利用防禦技術**”視窗。

9. 選擇其中一個選項以應用攻擊緩解技術：

   - **套用所有可用的弱點利用防禦技術**。

     如果選擇此選項，則不能編輯清單。預設情況下應用所有可用於處理程序的技術。

   - **針對處理程序套用列出的弱點利用防禦技術**。

     如果選擇此選項，則您可以編輯已應用攻擊緩解技術：

     a. 選擇您要套用的技術旁邊的核取方塊，以防護選定的處理程序。

     b. 選中或清除“**套用受攻擊面減少技術來減輕弱點利用風險**”核取方塊。

10. 配置“受攻擊面減少”技術的設定：

    - 輸入其啟動將受到“**拒絕模組**”欄位中受防護的處理程序封鎖的模組的名稱。
    - 在“**不拒絕在網際網路區域中啟動的模組**”欄位中，選擇您要在其下方允許模組啟動的選項旁邊的核取方塊：
      - 網際網路
      - 本機網際網路
      - 受信任的網站
      - 受限制的站台
      - 電腦

      這些設定僅適用於 Internet Explorer®。

11. 點擊“**確定**”。

該處理程序將新增到工作防護範圍中。

弱點利用防禦技術

步驟 34. 弱點利用防禦技術

弱點利用防禦技術	敘述
資料執行防護 (DEP)	資料執行防護封鎖在受防護的記憶體區域中執行任意代碼。
位址空間佈局隨機化 (ASLR)	改變處理程序位址空間內資料結構佈局。
結構化例外處理常式覆蓋防護 (SEHOP)	異常記錄的取代或異常處理程式的取代。
空頁分配	防護重定向空指針。
LoadLibrary 網路調用檢查（ROP 防護）	防止從網路路徑載入 DLL。
可執行檔堆疊（ROP 防護）	封鎖堆疊區域的非授權執行。
RET 防護檢查（ROP 防護）	檢查確保安全調用 CALL 指令。
堆疊透視防護（ROP 防護）	防止將 ESP 堆疊指標重新定位到可執行檔位址。
簡單匯出位址表存取監視 (EAT 存取監視和透過診斷寄存器的 EAT 存取監視）	防止對 kernel32.dll、kernelbase.dll 和 ntdll.dll 匯出位址表的讀取存取
堆噴射分配 (Heapspray)	防止將記憶體分配用於執行惡意程式碼。
執行流模擬（返回導向編程防護）	偵測 Windows API 元件中的可疑指令鏈（潛在 ROP 小工具）。
IntervalProfile 調用監視（協助工具驅動程式防護 (AFDP)）	防止透過 AFD 驅動程式中的弱點進行提權（透過 QueryIntervalProfile 調用在 Ring 0 中執行任意代碼）。
受攻擊面減少 (ASR)	透過受防護的處理程序封鎖啟動易受攻擊的載入項。
處理程序挖空防護 (Hollowing)	防止建立和執行受信任處理程序的惡意副本。
AtomBombing 防護 (APC)	透過非同步程序呼叫 (APC) 利用全域原子表弱點。
CreateRemoteThread 防護 (RThreadLocal)	其他處理程序已在受防護處理程序中建立執行緒。
CreateRemoteThread 防護 (RThreadRemote)	受防護處理程序已在其他處理程序中建立執行緒。

本機活動控制

本節提供有關用於控制應用程式啟動、透過 USB 連線到外部裝置以及 Windows 防火牆的 Kaspersky Embedded Systems Security 2.2 功能的資訊。

本章內容

透過卡巴斯基安全管理中心管理應用程式啟動

您可透過在卡巴斯基安全管理中心上為電腦群組建立應用程式啟動控制規則的常見清單，來允許或拒絕應用程式在公司網路內的所有電腦上啟動。

本章節說明項目

關於使用設定檔在卡巴斯基安全管理中心政策中設定應用程式啟動控制工作

將政策中設定的應用程式啟動控制規則套用於管理群組內的所有電腦。如果一個管理群組包括各種類型的電腦，則每台電腦上的應用程式啟動控制可能需要自訂規則清單。您可使用*政策設定檔*將不同政策套用於單個管理群組內的電腦。

建議將政策設定檔套用於為受統一政策控制的單個管理群組內的不同電腦類型設定應用程式啟動控制規則。這可以最佳化電腦防護，只要指定的規則只涵蓋對於該電腦類型典型的那些應用程式啟動。

根據為管理群組的電腦分配的“*標籤*”為其套用政策設定檔。您可為具有單個標籤的所有群組電腦設定一個政策設定檔。

有關標籤和政策設定檔的詳細資訊以及有關它們的使用說明，請參見*卡巴斯基安全管理中心說明*。

► *在“應用程式啟動控制”工作中套用政策設定檔：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點。展開要為其設定政策設定檔應用程式的管理群組。
2. 根據電腦類型將標籤分配給管理群組內的每台電腦。為此，請執行以下操作：
   - 在選定管理群組的詳細資訊視窗中，開啟“**裝置**”標籤，然後選擇要為其分配標籤的電腦。在所選電腦的“**內容：<電腦名稱>**”視窗中，選擇“**標記**”部分並建立標記清單。點擊“**確定**”。
3. 建立政策設定檔並設定其應用程式以防護管理群組內的電腦。為此，請執行以下操作：
   - 在選定管理群組的詳細資訊視窗中，開啟“**政策**”標籤，然後選擇要為其配置應用程式的設定檔的政策。在所選政策的“**內容：<政策名稱>**”視窗中，開啟“**政策設定檔**”部分，然後點擊“**新增**”按鈕建立新的設定檔。**內容：<設定檔名稱>** 視窗開啟。執行以下操作：
     a. 在“**啟動規則**”部分中，設定設定檔的應用程式範圍，並指定啟動設定檔的條件。
     b. 在“**應用程式啟動控制**”部分中，為您正編輯的設定檔設定應用程式啟動控制規則清單。
     c. 點擊“**確定**”。
4. 在“**內容：<政策名稱>**”視窗中，點擊“**確定**”。

設定的設定檔將應用到與“應用程式啟動控制”工作相關的政策。

配置“應用程式啟動控制”工作設定

可以變更預設的應用程式啟動控制工作設定（請參見以下表格）。

步驟 35. 預設的應用程式啟動控制工作設定

設定	預設值	敘述
工作模式	**僅統計**。該工作根據設定的規則記錄應用程式封鎖和啟動事件。應用程式啟動實際不會被拒絕。	在建立最終規則清單後，您可以為電腦防護選擇“**活動**”模式。
規則管理	**使用政策規則取代本機規則**	可以選擇聯合使用其中的政策指定的規則與本機電腦上的規則的模式。
規則使用範圍	工作控制可執行檔、指令碼和 MSI 資料套件的啟動。	您可以指定要使用規則控制其啟動的檔案類型。
KSN 使用	未使用 KSN 中應用程式聲譽上的資料。	在執行“應用程式啟動控制”工作時，您可以使用 KSN 應用程式聲譽資料。
自動允許為所列應用程式和資料套件分發軟體	未套用。	可以使用安裝程式和設定中指定的應用程式允許軟體分發。預設情況下，僅允許使用 Windows Installer 進行軟體分發。

設定	預設值	敘述
始終允許透過 Windows Installer 進行軟體分發	已套用。	如果透過 Windows Installer 執行操作，您可允許任何軟體安裝或更新。
在沒有可執行的指令時拒絕指令編譯器啟動	未套用。	您可以在沒有可執行的指令時拒絕指令編譯器啟動。
啟動工作	不設定工作的初次啟動排程。	“應用程式啟動控制”工作不會在 Kaspersky Embedded Systems Security 2.2 啟動時自動啟動。您可以手動啟動該工作或設定排程啟動。

► *要設定“應用程式啟動控制”工作一般設定，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**本機活動控制**”部分中，點擊“**應用程式啟動控制**”部分的“**設定**”按鈕。

   將開啟“**應用程式啟動控制**”視窗。
4. 在“**一般**”標籤上，選擇“**模式**”部分的以下設定：

   在“**工作模式**”下拉清單中，指定工作執行模式。

   在此下拉清單中，可選擇應用程式啟動控制工作的模式：

   - **活動**。Kaspersky Embedded Systems Security 2.2 使用指定的規則監控正在執行的任何應用程式。
   - **僅統計**。Kaspersky Embedded Systems Security 2.2 不使用指定的規則監控應用程式啟動，而只是在工作記錄中記錄有關這些啟動事件的資訊。允許啟動所有程式。您可以使用此模式根據工作記錄中記錄的資訊建立應用程式啟動控制規則清單。

   預設情況下，“應用程式啟動控制”工作在“**僅統計**”模式下執行。

- 清除或選中“**在此檔案的所有後續啟動中重複針對首次檔案啟動執行的操作**”核取方塊。

  使用此核取方塊可啟用或停用第二次和後續基於快取中儲存的事件資訊啟動應用程式的嘗試的啟動控制。

  如果選中此核取方塊，Kaspersky Embedded Systems Security 2.2 基於工作在應用程式初次開機時已提交的結論允許或拒絕應用程式重新啟動。例如，如果規則允許應用程式初次開機，則有關此操作的資訊將儲存在快取中，第二次和所有後續重新啟動也將被允許，而不進行任何額外的重複檢查。

  如果清除此核取方塊，Kaspersky Embedded Systems Security 2.2 會在應用程式每次嘗試啟動時進行分析。

  預設將會選定該核取方塊。

- 清除或選中“**在沒有可執行的指令時拒絕指令編譯器啟動**”核取方塊。

  如果選中此核取方塊，Kaspersky Embedded Systems Security 2.2 將拒絕命令列編譯器啟動，即使允許編譯器啟動。只有滿足以下兩個條件，才能在沒有指令的情況下啟動命令列：

  - 允許命令列編譯器啟動。
  - 允許執行的指令。

  如果清除該核取方塊，Kaspersky Embedded Systems Security 2.2 只考慮命令列啟動的允許規則。如果未套用任何允許規則或可執行處理程序沒有 KSN 信任狀態，啟動將被拒絕。如果套用了允許規則或處理程序具有 KSN 信任狀態，可以在有或沒有要執行的指令的情況下啟動命令列。

  Kaspersky Embedded Systems Security 2.2 可辨識以下命令列編譯器：

  - cmd.exe
  - powershell.exe
  - python.exe
  - perl.exe

5. 在“**規則**”部分中，配置應用規則的設定：

   a. 點擊“**規則清單**”按鈕以新增工作啟動控制的允許規則。

   > Kaspersky Embedded Systems Security 2.2 無法辨識包含斜線“/”的路徑。請使用反斜線“\”來正確輸入路徑。

   b. 選擇套用規則的模式：

   - **使用政策規則取代本機規則**。

     應用程式將針對電腦群組上的應用程式啟動控制套用政策中指定的規則清單。不能建立、編輯或套用本機規則清單。

   - **將政策規則新增到本機規則**。

     應用程式將與本機規則清單一起套用政策中指定的規則清單。可以使用“應用程式啟動控制規則產生器”工作編輯本機規則清單。

   > 預設情況下，Kaspersky Embedded Systems Security 2.2 將根據憑證套用允許指令碼、MSI 套裝軟體和啟動檔案的兩種預設規則。

6. 在“**規則使用範圍**”部分中，指定以下設定：

- **將規則套用於可執行檔**。

  該核取方塊可啟用/停用控制程式可執行檔的啟動。

  如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將使用指定的規則（規則設定指定可執行檔的範圍）允許或封鎖程式可執行檔的啟動。

  如果清除此核取方塊，則 Kaspersky Embedded Systems Security 2.2 不使用指定的規則控制程式可執行檔的啟動。允許啟動程式可執行檔。

  預設將會選定該核取方塊。

- **監控 DLL 模組的載入**。

  使用此核取方塊啟用/停用 DLL 模組載入的監控

  如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將使用指定的規則（規則設定指定可執行檔的範圍）允許或封鎖 DLL 模組的下載。

  如果清除此核取方塊，則 Kaspersky Embedded Systems Security 2.2 不使用指定的規則監控 DLL 模組的下載。允許 DLL 模組的下載。

  如果選中“將規則套用於可執行檔”核取方塊，則此核取方塊可用。

  預設取消選定該核取方塊。

> 監控 DLL 模組下載可能會影響作業系統效能。

- **將規則套用於指令碼和 MSI 資料套件**。

  使用此核取方塊啟用/停用指令碼和 MSI 資料套件的啟動。

  如果選中此核取方塊，Kaspersky Embedded Systems Security 2.2 將使用指定的規則（規則設定將指令碼和 MSI 資料套件指定為範圍）允許或封鎖指令碼和 MSI 資料套件執行。

  如果清除此核取方塊，則 Kaspersky Embedded Systems Security 2.2 不使用指定的規則控制指令碼和 MSI 資料套件的啟動。將允許指令碼和 MSI 資料套件的啟動。

  預設將會選定該核取方塊。

7. 在“**KSN 使用**”部分中，配置以下應用程式啟動設定：

- **拒絕 KSN 不信任的應用程式**。

  此核取方塊用於啟用或停用根據應用程式在 KSN 中的信譽進行應用程式啟動控制。

  如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將封鎖在 KSN 中具有不受信任狀態的任何應用程式執行。套用於 KSN 不信任的應用程式的應用程式啟動控制允許規則將不會觸發。選中此核取方塊將會提供額外的惡意軟體防護。

  如果清除此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將不考慮 KSN 不信任的程式的聲譽，並將根據適用於此類程式的規則允許或封鎖啟動程式。

  預設取消選定該核取方塊。

- **允許 KSN 信任的應用程式**。

  此核取方塊用於啟用或停用根據應用程式在 KSN 中的信譽進行應用程式啟動控制。

  如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將允許具有 KSN 信任狀態的應用程式執行。拒絕套用於 KSN 信任的應用程式的應用程式啟動控制規則具有更高的優先順序：如果 KSN 服務認為應用程式受信任，則將拒絕應用程式啟動。

  如果清除此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將不考慮 KSN 信任的程式的聲譽，並將根據適用於此類程式的規則允許或封鎖啟動程式。

  預設取消選定該核取方塊。

- 允許啟動 KSN 中信任的應用程式的使用者和/或使用者群組。

8. 在“**軟體分發控制**”標籤上，配置軟體分發控制的設定（請參見第 164 頁上的“配置軟體分發控制”部分）。
9. 在“**工作管理**”標籤上，配置排程的工作啟動設定（請參見第 107 頁上的“配置工作啟動排程設定”部分）。
10. 在“**工作設定**”視窗中點擊“**確定**”。

Kaspersky Embedded Systems Security 2.2 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在工作記錄中。

關於軟體分發控制

如果您需要同時考慮受防護電腦上的軟體分發控制，應用程式啟動控制規則的生成可能很複雜。例如，在其中安裝的軟體會定期自動更新的電腦。在這種情況下，需要在每次軟體更新後更新允許規則的清單，以便在“應用程式啟動控制”工作設定中考慮新建立的檔案。為了簡化軟體分發方案中的啟動控制，可以使用“應用程式啟動控制”子系統。

軟體分發套件（也稱為“套件”）表示要在電腦上安裝的軟體應用程式。每個套件都包含至少一個應用程式，除了應用程式外，可能還包含單個檔案、更新，甚至單個指令，尤其是在您安裝軟體應用程式或更新時。

“軟體分發控制”子系統作為附加排除清單實施。向該清單中新增軟體分發套件時，應用程式將允許解壓縮這些受信任套件並自動啟動由受信任套件建立或修改的軟體。提取的檔案可以繼承主分發套件的受信任內容。*主分發套件*是由使用者新增到軟體分發控制排除清單並成為受信任套件的分發套件。

Kaspersky Embedded Systems Security 2.2 只控制完整週期的軟體分發。如果第一次啟動受信任套件時軟體分發控制關閉，或者“應用程式啟動控制”元件未安裝，應用程式將無法正確處理由受信任套件修改的檔案的啟動。

如果在“應用程式啟動控制”工作設定中清除“**將規則套用於可執行檔**”核取方塊，軟體分發控制將不可用。

軟體分發快取

借助動態生成的*軟體分發快取*（也稱為“分發快取”），Kaspersky Embedded Systems Security 2.2 在受信任套件與軟體分發過程中建立的檔案之間建立連線。第一個套件啟動時，Kaspersky Embedded Systems Security 2.2 將偵測該套件的軟體分發過程中建立的所有檔案，並將檔案的校驗和及路徑儲存在分發快取中。隨後，預設允許啟動分發快取中儲存的所有檔案。

您不能透過使用者介面檢視、清除或手動修改分發快取。快取由 Kaspersky Embedded Systems Security 2.2 填充和控制。

您可以將分發快取匯出到設定檔（XML 格式），同時使用命令列選項清除快取。

► *要將分發快取匯出到設定檔，請執行以下指令：*

kavshell appcontrol /config /savetofile:<full path> /sdc

► *要清除分發快取，請執行以下指令：*

kavshell appcontrol /config /clearsdc

Kaspersky Embedded Systems Security 2.2 每 24 小時更新一次分發快取。如果先前允許的檔案的完整路徑或校驗和發生變化，應用程式將從分發快取中刪除該檔案記錄。如果“應用程式啟動控制”工作在活動模式下啟動，將封鎖該檔案進一步啟動。

提取檔案處理

第一次啟動受信任套件時，該套件的所有提取檔案的受信任內容會被繼承。如果在第一次啟動後清除該核取方塊，該套件的所有提取檔案的繼承仍將保留。要重設最初套用於所有提取檔案的繼承，您需要在再次啟動受信任分發套件之前清除分發快取並清除“**允許從該分發套件提取鏈中啟動到所有檔案**”核取方塊。

由受信任的主分發套件建立的提取檔案和套件會獲取受信任內容，因為它們的校驗和在第一次開啟排除清單中的軟體分發套件時被新增到分發快取中。因此，分發套件本身和該套件的所有提取檔案也將被信任。預設情況下，受信任內容整合的等級數量是無限的。

作業系統重新啟動後，提取檔案將保留受信任內容。

檔案處理在軟體分發控制設定（請參見第 164 頁上的“設定軟體分發控制”部分）中透過選擇或清除“**允許從該分發套件提取鏈中啟動到所有檔案**”核取方塊來進行設定。

例如，您將包含一些其他套件和應用程式的 test.msi 套件新增到排除清單中並選中該核取方塊。在這種情況下，將允許執行或提取 test.msi 套件中包含的所有套件和應用程式（如果它們包含其他檔案）。此方案適用於所有嵌套等級上的提取檔案。

如果將 test.msi 套件新增到排除清單中並清除“**允許從該分發套件提取鏈中啟動到所有檔案**”核取方塊，應用程式只會將受信任內容分配到直接從主受信任套件提取的套件和可執行檔（在第一個等級上嵌套）。此類檔案的校驗和儲存在分發快取中。在第二個和更後面等級上嵌套的所有檔案都將被“預設拒絕”原則封鎖。

與應用程式啟動控制規則清單的互動

軟體分發控制子系統的受信任套件清單是一個排除項目清單，該清單擴大了但未更換應用程式啟動控制規則清單。

拒絕應用程式啟動控制規則具有最高優先順序：受信任套件的解壓縮和新檔案或已修改檔案的啟動將被封鎖（如果這些套件和檔案受應用程式啟動控制拒絕規則影響）。

軟體分發控制排除項目適用於受信任套件和這些套件建立或修改的檔案（如果應用程式啟動控制清單中沒有拒絕規則適用於這些套件和檔案）。

使用 KSN 結論

不受信任 KSN 結論的優先順序高於軟體分發控制排除項目：受信任套件的解壓縮或者該套件建立和修改的檔案的啟動將被封鎖（如果從 KSN 收到了這些檔案的不信任結論）。

配置軟體分發控制

► *要新增受信任分發套件，請執行以下操作：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**本機活動控制**”部分中，點擊“**應用程式啟動控制**”部分的“**設定**”按鈕。

   將開啟“**應用程式啟動控制**”視窗。
4. 在選定的標籤上，選中“**自動允許為所列應用程式和資料套件分發軟體**”核取方塊。

   使用此核取方塊可啟用和停用自動建立使用清單中指定的安裝套件啟動的所有檔案的排除項目。

   如果選中此核取方塊，應用程式會自動允許受信任分發套件中的檔案啟動。可以編輯應用程式和啟動允許的安裝套件清單。

   如果清除此核取方塊，應用程式不會應用清單中指定的排除項目。

   預設取消選定該核取方塊。

如果在“**應用程式啟動控制**”工作設定中選中“**將規則套用於可執行檔**”核取方塊，則您可選中“**自動允許為所列應用程式和資料套件分發軟體**”。

5. 根據需要清除“**始終允許透過 Windows Installer 進行軟體分發**”核取方塊。

   使用此核取方塊可啟用和停用自動建立透過 Windows Installer 執行的所有檔案的排除項目。

   如果選中此核取方塊，應用程式將始終允許透過 Windows Installer 安裝的檔案啟動。

   如果清除此核取方塊，將不會無條件允許應用程式，即使該應用程式是透過 Windows Installer 啟動的。

   預設將會選定該核取方塊。

   如果未選中“**自動允許為所列資料套件分發軟體**”核取方塊，則此核取方塊不可編輯。

在絕對必要時才建議清除“**始終允許透過 Windows Installer 進行軟體分發**”核取方塊。關閉此功能可導致更新作業系統檔案時出現問題，還會封鎖從分發套件提取的檔案啟動。

6. 如果需要，請選擇“**始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發**”核取方塊。

   透過使用 System Center Configuration Manager，該核取方塊可以自動開啟或關閉軟體分發。

   如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 使用 System Center Configuration Manager 自動允許 Microsoft Windows 佈署。應用程式僅允許透過背景智慧傳輸服務進行軟體分發。

   應用程式可控制具有以下副檔名的物件的啟動：

   - .exe
   - .msi

   預設取消選定該核取方塊。

應用程式可控制電腦上從套裝軟體遞送到安裝/更新的軟體分發週期。如果在電腦上安裝應用程式之前已執行分發的任何階段，則應用程式不會控制處理程序。

7. 要編輯受信任分發套件的清單，請點擊“**變更分發套件清單**”，然後在開啟的視窗中選擇以下方法之一：

   - **新增一個分發套件**。

     a. 點擊“**瀏覽**”按鈕，然後選擇可執行檔或分發套件。

        “**信任條件**”部分會使用有關選定檔案的資料自動進行填充。

     b. 清除或選中“**允許從該分發套件提取鏈中啟動到所有檔案**”核取方塊。

     c. 選擇兩個可用條件選項中的一個，用於決定檔案或安裝套件是否受信任：

        - **使用數位憑證**

          如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。此時，應用程式將允許啟動使用帶數位憑證的檔案啟動的程式。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。

        - **使用 SHA256 雜湊**

          如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的校驗和值指定為規則觸發條件。應用程式將允許啟動使用帶指定校驗和值的檔案啟動的程式。

          當產生的規則需要滿足最終安全等級時，建議使用此選項：SHA256 校驗和可套用為唯一檔案 ID。作為 SHA256 校驗和作為規則觸發條件會將規則使用範圍限制為最多一個檔案。

          預設選中該選項。

- **按雜湊新增多個分發套件**。

  您可以選擇無限數量的可執行檔和分發套件，並同時將它們新增到清單。Kaspersky Embedded Systems Security 2.2 將檢查雜湊並允許作業系統啟動指定的檔案。

- **變更選定的分發套件**。

  使用此選項可以選擇不同的可執行檔或分發套件，或變更信任條件。

- **從檔案匯入分發套件清單**。

  可以從設定檔匯入受信任分發套件的清單。被 Kaspersky Embedded Systems Security 2.2 識別的檔案必須滿足以下參數:

  - 檔案具有文本副檔名。
  - 檔案包含結構化成行清單的資訊，其中每一行包含的資料用於一個受信任的檔案。
  - 檔案必須包含以下格式之一的清單：
    - <檔案名稱>：<雜湊 SHA256>。
    - <雜湊 SHA256>*<檔案名稱>。

  在“**開啟**”視窗中，指定包含受信任分發套件清單的設定檔。

8. 如果要刪除受信任清單中以前新增的應用程式或分發套件，請點擊“**刪除分發套件**”按鈕。將允許執行提取檔案。

   要封鎖提取檔案啟動，請在受防護電腦上移除應用程式，或在應用程式啟動控制工作設定中建立拒絕規則。

9. 點擊“**確定**”。

已儲存新配置的設定。

啟用預設允許模式

預設允許模式允許所有應用程式啟動，只要它們沒有被規則或 KSN 不信任結論所封鎖。可以透過新增特定允許規則來啟用預設允許模式。您可以僅為指令碼或為所有可執行檔啟用預設允許模式。

► *要新增預設允許規則：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：

   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。

   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**本機活動控制**”部分中，點擊“**應用程式啟動控制**”部分的“**設定**”按鈕。
4. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。

   將開啟“**應用程式啟動控制規則**”視窗。
5. 點擊“**新增**”按鈕，在開啟的內容功能表中，選擇“**新增一項規則**”選項。

   將開啟“**規則設定**”視窗。
6. 在“**名稱**”欄位中，輸入規則的名稱。
7. 在“**類型**”下拉清單中，選擇“**允許**”規則類型。
8. 在“**範圍**”下拉清單中，選擇將由規則控制執行的檔案類型：
   - **可執行檔**，如果希望規則控制應用程式可執行檔的啟動。
   - **指令碼和 MSI 資料套件**，如果希望規則控制指令碼和 MSI 資料套件的啟動。
9. 在“**規則觸發條件**”部分中，選擇“**檔案路徑**”選項。
10. 輸入以下遮罩：**?:**
11. 在“**規則設定**”視窗中點擊“**確定**”。

Kaspersky Embedded Systems Security 2.2 將套用預設允許模式。

關於在卡巴斯基安全管理中心中建立所有電腦的應用程式啟動控制規則

您可使用卡巴斯基安全管理中心工作和原則立即為公司網路上的所有電腦和電腦組建立應用程式啟動控制規則清單。如果企業網路沒有參考機器，並且您不能根據該參考機器上安裝的應用程式使用工作來自動生成允許規則以建立一個通用清單時，建議使用該方案。

“應用程式啟動控制”元件安裝後具有兩個預定義的允許規則：

- 具有作業系統信任憑證的指令碼和 MSI 的允許規則。
- 具有作業系統信任憑證的可執行檔的允許規則。

您可採用兩種方式透過卡巴斯基安全管理中心建立應用程式啟動控制規則清單：

- 為應用程式啟動控制使用“應用程式啟動控制規則產生器”群組工作。

  當使用此方案時，群組工作會為網路上的每個電腦建立其自己的應用程式啟動控制規則清單，並將這些清單儲存到指定共用網路資料夾中的 XML 檔案。然後，您可將建立的規則清單手動匯入卡巴斯基安全管理中心政策的“應用程式啟動控制”工作。您可以將卡巴斯基安全管理中心政策設定為當“應用程式啟動控制規則產生器”群組工作完成後，自動將已建立的規則新增到“應用程式啟動控制”規則清單中。

  當您需要馬上建立應用程式啟動控制規則清單時，建議使用此方案。建議僅當允許規則的應用程式範圍包含您知道安全的檔案的資料夾時，才設定“應用程式啟動控制規則產生器”工作的排程啟動。

  在網路中使用“應用程式啟動控制”政策之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果不提供組織的政策用於網路中的共用網路資料夾，則建議為測試電腦群組或範本機上的電腦控制規則啟動“規則產生器”工作。

- 對於“應用程式啟動控制”工作在“**僅統計**”模式下執行，基於卡巴斯基安全管理中心中建立的工作事件報告。

  當使用此方案時，Kaspersky Embedded Systems Security 2.2 不拒絕應用程式啟動，但當“應用程式啟動控制”在“**僅統計**”模式下執行時，它將在卡巴斯基安全管理中心的“**事件**”部分中報告所有網路電腦上的所有允許和拒絕的應用程式啟動。卡巴斯基安全管理中心會基於工作記錄建立拒絕的應用程式啟動事件的統一清單。

  您需要設定工作執行期限，以便可在指定時間期限內執行所有可能的受防護電腦和電腦群組操作方案以及至少一次重新啟動。然後，隨著將規則新增到“應用程式啟動控制”工作中，您可從儲存的卡巴斯基安全管理中心事件報告檔案（採用 TXT 格式）匯入有關應用程式啟動的資料，並基於此資料為此類應用程式建立應用程式啟動控制允許規則。

  如果公司網路包含大量不同類型的電腦（請參見第 157 頁上的“關於使用設定檔在卡巴斯基安全管理中心政策中配置應用程式啟動控制工作”部分）（安裝了不同的軟體集合），則建議使用此方案。

- 根據透過卡巴斯基安全管理中心接收到的拒絕應用程式啟動事件，無需建立和匯入設定檔。

  要使用此功能，必須在有效的卡巴斯基安全管理中心政策下執行本機電腦上的應用程式啟動控制工作。在本例中，本機電腦上的所有事件均被傳送到管理伺服器。

建議當網路電腦上安裝的應用程式集合變更時更新規則清單（例如，當安裝更新或重新安裝作業系統時）。建議在“**僅統計**”模式中使用“應用程式啟動控制規則產生器”工作或“應用程式啟動控制”政策，執行在測試管理群組中的電腦上，以便生成經過更新的規則清單。測試管理群組包含在網路電腦上安裝新的應用程式之前對這些應用程式進行測試啟動所需的電腦。

新增允許規則之前，請選擇其中一個可用的規則應用模式（請參見第 158 頁上的“配置應用程式啟動控制工作設定”部分）。卡巴斯基安全管理中心政策規則清單將僅顯示由政策指定的那些規則，與規則應用模式無關。本機規則清單將顯示所有已套用的規則 — 本機規則和透過政策新增的規則。

本章節說明項目

從卡巴斯基安全管理中心事件建立允許規則

► *要使用應用程式啟動控制中的“從卡巴斯基安全管理中心事件為應用程式建立允許規則”選項，請執行以下操作：*

1. 在卡巴斯基安全管理中心的管理主控台中，展開“**受管理裝置**”節點。
2. 展開您要為其配置政策設定的管理群組，然後在詳細資訊視窗中選擇“**政策**”標籤。
3. 在您希望配置政策的內容功能表中選擇“**內容**”。

   內容：<內容名稱> 視窗開啟。
4. 在“**本機活動控制**”部分中，點擊“**應用程式啟動控制**”部分的“**設定**”按鈕。
5. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。

   將開啟“**應用程式啟動控制規則**”視窗。
6. 點擊“**新增**”按鈕，然後在該按鈕的內容功能表中選擇“**從卡巴斯基安全管理中心事件為應用程式建立允許規則**”。
7. 選擇將規則新增到先前建立的應用程式啟動控制規則清單中的政策：
   - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
   - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
   - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

   將開啟“**產生應用程式啟動控制規則**”視窗。
8. 配置以下請求設定：
   - **管理伺服器位址**
   - **連接埠**
   - **使用者**
   - **密碼**
9. 選擇您希望生成工作依據的事件類型：
   - **僅統計資訊模式：應用程式啟動被拒絕**。
   - **應用程式啟動被拒絕**。
10. 從“**請求事件在以下期間內生成**”下拉清單中選擇時間段。
11. 點擊“**產生規則**”按鈕。
12. 點擊“**應用程式啟動控制規則**”視窗中的“**儲存**”按鈕。

    將使用基於安裝了卡巴斯基安全管理中心管理主控台的電腦的系統資料建立的新規則填充“應用程式啟動控制”政策中的規則清單。

    如果政策中已指定應用程式啟動控制規則清單，則 Kaspersky Embedded Systems Security 2.2 將從封鎖事件中新增選定的規則到已指定的規則。不新增具有相同雜湊的規則，因為清單中的所有規則都必須是唯一的。

從 XML 設定檔匯入應用程式啟動控制規則

您可匯入“應用程式啟動控制規則產生器”群組工作完成後建立的報告，並將它們作為允許規則清單套用於所設定的政策中。

當“應用程式啟動控制規則產生器”群組工作完成後，應用程式會將建立的允許規則匯入指定的共用網路資料夾中儲存的 XML 檔案。包含規則清單的每個檔案基於所執行的檔案分析及在公司網路上的每個單獨電腦上啟動的應用程式建立。這些清單包含類型與“應用程式啟動控制規則產生器”群組工作中指定的類型比對的檔案和應用程式的允許規則。

在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 2.2 功能元件的設定的過程與在應用程式主控台中對這些元件的設定進行本機配置相似。有關如何配置工作設定和應用程式功能的詳細說明，請參見《*Kaspersky Embedded Systems Security 2.2 使用者手冊*》的相關章節。

► *若要基於自動建立的允許規則清單為一組電腦指定應用程式啟動的允許規則，請執行以下步驟。*

1. 在所設定電腦群組的主控台中的“**工作**”標籤上，建立一個“應用程式啟動控制規則產生器”群組工作或選擇一個現有工作。
2. 在建立的“應用程式啟動控制規則產生器”群組工作的內容中或在工作精靈中，指定以下設定：
   - 在“**通知**”部分中，設定用於儲存工作執行報告的設定。

     有關此節中配置設定的詳細說明，請參見 *卡巴斯基安全管理中心說明*。
   - 在“**設定**”部分中，指定所建立規則將允許啟動的應用程式類型。您可編輯包含允許的應用程式的資料夾的內容：從工作範圍排除預設資料夾或手動新增新資料夾。
   - 在“**選項**”部分中，指定工作在執行時及完成後的操作。指定規則建立條件，以及將這些規則匯出至其中的檔案的名稱。
   - 在“**排程**”部分中設定工作啟動排程設定。
   - 在“**帳戶**”部分中，指定將用於執行工作的使用者帳戶。
   - 在“**工作範圍的排除項目**”部分中，指定要從工作範圍排除的電腦群組。

     Kaspersky Embedded Systems Security 2.2 不會為在排除的電腦上啟動的應用程式的允許規則。
3. 在所設定電腦群組的主控台上的“**工作**”標籤上，從群組工作清單中選擇您已建立的應用程式啟動控制規則產生器，然後點擊“**啟動**”按鈕啟動工作。

   工作完成後，自動建立的允許規則清單將儲存在共用網路資料夾中的 XML 檔案中。

   在網路中使用“應用程式啟動控制”政策之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果不提供組織的政策用於網路中的共用網路資料夾，則建議為測試電腦群組或範本機上的電腦控制規則啟動“規則產生器”工作。

4. 將建立的允許規則清單新增到“應用程式啟動控制”工作。為此，在所設定政策的內容的“應用程式啟動控制”工作設定中：

   a. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。

      將開啟“**應用程式啟動控制規則**”視窗。

   b. 點擊“**新增**”按鈕，然後在開啟的清單中選擇“**從 XML 檔案匯入規則**”。

   c. 選擇將自動建立的允許規則新增到先前建立的“應用程式啟動控制”規則清單中的政策：

      - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
      - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
      - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

   d. 在開啟的 Microsoft Windows 標準視窗中，選擇“應用程式啟動控制規則產生器”群組工作完成後建立的 XML 檔案。

   e. 在“**應用程式啟動控制規則**”和“**工作設定**”視窗中點擊“**確定**”。

5. 如果您希望將建立的規則套用於控制應用程式啟動，則在政策中的應用程式啟動控制工作的內容中，選擇“**活動**”工作執行模式。

基於每台單獨的電腦上的工作執行自動建立的允許規則將被套用於所設定政策涵蓋的所有網路電腦。在這些電腦上，應用程式將允許僅啟動已為其建立允許規則的這些應用程式。

從有關受封鎖應用程式的卡巴斯基安全管理中心報告的檔案中匯入規則

您可從在“**僅統計**”模式下完成應用程式啟動控制工作後卡巴斯基安全管理中心中建立的報告匯入有關受封鎖應用程式啟動的資料，並使用此資料在所設定政策中建立應用程式啟動控制允許規則清單。

建立應用程式啟動控制工作期間發生的附隨報告時，您可跟蹤啟動受封鎖的應用程式。

將資料從受封鎖應用程式報告匯入到政策設定時，確保您所使用的清單僅包含希望允許啟動的應用程式。

► *若要基於來自卡巴斯基安全管理中心的被封鎖應用程式報告為一組電腦指定應用程式啟動允許規則，請執行以下步驟：*

1. 在政策內容的應用程式啟動控制工作設定中，選擇“**僅統計**”操作模式。
2. 在“**事件**”部分中的政策內容中，確保：
   - 應用程式啟動被拒絕事件的“**緊急事件**”標籤顯示超過“**僅統計**”模式下排程的工作執行時間的事件儲存時間（預設值為 30 天）。
   - “*僅統計：應用程式啟動被拒絕*”事件的“**警告**”標籤顯示超過“**僅統計**”模式下排程的工作執行時間的事件儲存時間（預設值為 30 天）。

     當達到“**儲存時間**”列中指定的期限時，則有關記錄的事件的資訊會被刪除且不會反映在報告檔案中。在“**僅統計**”模式下執行應用程式啟動控制工作之前，確保工作執行時間不超過為指定事件設定的儲存時間。

3. 當工作完成後，將記錄的事件匯出到 TXT 檔案：
   a. 為此，在“應用程式啟動控制”工作的內容中，展開“**記錄和通知**”節點。
   b. 在“**事件**”子節點中，基於“*封鎖*”條件建立一系列事件，以檢視應用程式啟動控制工作將封鎖啟動的應用程式。
   c. 在選擇的詳細資訊視窗中，點擊“**將事件匯出到檔案**”清單以將有關受封鎖應用程式啟動的報告儲存到 TXT 檔案。

   在政策中匯入和應用建立的報告之前，確保報告僅包含有關您希望允許啟動的應用程式的資料。

4. 將有關受封鎖應用程式啟動的資料匯入到應用程式啟動控制工作。為此，在政策內容的“應用程式啟動控制”工作設定中：
   a. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。

      將開啟“**應用程式啟動控制規則**”視窗。
   b. 點擊“**新增**”按鈕，然後在該按鈕的內容功能表中選擇“**從卡巴斯基安全管理中心報告匯入封鎖的應用程式的資料**”。
   c. 選擇將來自根據卡巴斯基安全管理中心報告建立的清單的規則新增到先前設定的應用程式啟動控制規則清單的政策：
      - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
      - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
      - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
   d. 在開啟的 Microsoft Windows 標準視窗中，選擇已將來自受封鎖應用程式啟動報告的事件匯出到的 TXT 檔案。
   e. 在“應用程式啟動控制規則”和“**工作設定**”視窗中點擊“**確定**”。

根據有關受封鎖應用程式的卡巴斯基安全管理中心報告建立的規則將被新增到應用程式啟動控制規則清單。

透過卡巴斯基安全管理中心管理裝置連線

您可以通過卡巴斯基安全管理中心為多組電腦建立統一的電腦控制清單，從而允許或限制快閃記憶體磁碟機和其他大容量儲存連線到網路上的所有電腦。

本章節說明項目

關於裝置控制工作

Kaspersky Embedded Systems Security 2.2 控制大容量儲存和 CD/DVD 光碟機的註冊和使用，以防護電腦免受電腦安全性威脅的侵害，與快閃記憶體磁碟機或透過 USB 連線的其他類型的外部裝置進行檔案交換的過程中可能出現這些威脅。大容量儲存是可連線到電腦以複製或儲存檔案的外部裝置。

Kaspersky Embedded Systems Security 2.2 控制以下 USB 外部裝置連線：

- USB 連線的快閃記憶體磁碟機
- CD/DVD ROM 磁碟機
- USB 連線的軟碟磁碟機
- USB 連線的 MTP 行動裝置

Kaspersky Embedded Systems Security 2.2 會通知您透過 USB 連線的所有裝置，並在工作和事件記錄中記錄相應事件。事件詳細資訊包括裝置類型和連線路徑。“裝置控制”工作啟動後，Kaspersky Embedded Systems Security 2.2 將檢查並列出透過 USB 連線的所有裝置。您可以在卡巴斯基安全管理中心通知設定章節中配置通知。

“裝置控制”工作監控外部裝置透過 USB 連線到受防護電腦的所有連線嘗試，如果沒有此類裝置的允許規則，則封鎖連線。封鎖連線後，裝置將不可用。

應用程式為每個連線的大容量儲存裝置規定了以下狀態之一：

- *受信任*。您想允許其進行檔案交換的裝置。產生規則清單後，裝置實例路徑值將包含在至少一個規則的使用範圍中。
- *不受信任*。您想限制其進行檔案交換的裝置。裝置實例路徑不會包含在任何允許規則使用範圍中。

您可以使用“裝置控制規則產生器”工作為外部裝置建立允許規則，以允許資料交換。您還可以延伸已指定規則的使用範圍。不能手動建立允許規則。

Kaspersky Embedded Systems Security 2.2 使用*裝置實例路徑*值標識在系統中註冊的大容量儲存。裝置實例路徑是專門為每個外部裝置指定的預設功能。將在每個外部裝置的 Windows 內容中為其指定“裝置實例路徑”值，並且該值將在產生規則期間由 Kaspersky Embedded Systems Security 2.2 自動確定。

裝置控制工作可在兩種模式下執行：

- **活動**。Kaspersky Embedded Systems Security 2.2 會將規則套用於控制快閃記憶體磁碟機和其他外部裝置的連線，並根據預設拒絕原則和指定允許規則允許或封鎖使用所有裝置。允許使用受信任外部裝置。預設情況下，封鎖使用不受信任的外部裝置。

  如果當“裝置控制”工作在活動模式下執行前您認為不受信任的外部裝置連線到受防護電腦，應用程式不會封鎖該裝置。建議您手動斷開不信任裝置或重新啟動電腦。否則，不會將“預設拒絕”原則套用於裝置。

- **僅統計**。Kaspersky Embedded Systems Security 2.2 不會控制快閃記憶體磁碟機和其他外部裝置的連線，但僅記錄有關外部裝置在受防護電腦上的連接和註冊，以及有關相連裝置觸發的裝置控制允許規則的資訊。允許使用所有外部裝置。預設設定此模式。

  您可以基於工作執行期間記錄的資訊對規則建立套用此模式。

關於透過卡巴斯基安全管理中心建立所有電腦的裝置控制規則

您可使用卡巴斯基安全管理中心工作立即為公司網路上的所有電腦和電腦組建立裝置控制規則清單。

您可採用兩種方式透過卡巴斯基安全管理中心建立裝置控制規則清單：

- 使用“裝置控制規則產生器”群組工作。

  根據此方案，群組工作會基於有關所有曾經連線到受防護電腦的大容量儲存器的各個電腦系統資料產生規則清單。該工作還會考慮在工作執行的那一刻處於連接狀態的所有大容量儲存器。群組工作完成時，Kaspersky Embedded Systems Security 2.2 會為在網路中註冊的所有大容量儲存裝置建立允許規則清單，並將這些清單儲存在指定資料夾內的 XML 檔案中。然後，您可以在裝置控制政策設定中手動匯入建立的規則。與本機電腦上的工作不同的是，政策不允許設定在“應用程式啟動控制規則產生器”群組工作完成時將建立的規則自動新增到裝置控制規則清單。

  建議使用該方案在裝置控制政策首次以應用活動規則模式啟動之前建立允許規則清單。

  > 在網路中使用裝置控制政策之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果不提供組織的政策用於網路中的共用網路資料夾，則建議為測試電腦群組或範本機上的電腦控制規則啟動“規則產生器”工作。

- 對於在“**僅統計**”模式下執行的“裝置控制”工作，基於卡巴斯基安全管理中心中建立的工作事件報告。

  根據此方案，Kaspersky Embedded Systems Security 2.2 不會限制大容量儲存裝置連線，但會記錄當裝置控制工作以“**僅統計**”模式執行時所有網路電腦上發生的所有裝置連接和大容量儲存註冊的相關資訊；可在卡巴斯基安全管理中心的“**事件**”部分中找到記錄的資訊。卡巴斯基安全管理中心會基於工作記錄建立大容量儲存限制和允許事件的統一清單。

  您應該配置工作執行時段，在該時段內將允許所有大容量儲存裝置連線。然後，隨著將規則新增到“裝置控制”工作中，您可從儲存的卡巴斯基安全管理中心事件報告檔案（採用 TXT 格式）匯入有關裝置連線的資料，並基於此資料為此類裝置建立裝置控制允許規則。匯入的記錄所依據的事件種類不會影響建立的規則類型；只建立允許規則。

  若要為大量新的大容量儲存裝置新增允許規則以及為透過 MTP 連線的受信任行動裝置產生規則，則建議使用此方案。

- 基於有關所連線的大容量儲存器的系統資料（使用裝置控制政策設定中的“基於系統資料產生規則”選項）。

  根據此方案，Kaspersky Embedded Systems Security 2.2 會為曾經或目前連線到安裝有卡巴斯基安全管理中心的電腦的大容量儲存建立允許規則。

  若要為少量您希望在網路中的所有電腦上信任的新的大容量儲存器產生規則，則建議使用此方案。

- 基於目前已連線裝置的有關資料（使用“**基於連接的裝置產生規則**”）。

  在本方案中，Kaspersky Embedded Systems Security 2.2 僅為目前已連線的裝置生成允許規則。可以選擇要為其生成允許規則的一個或多個裝置。

  > Kaspersky Embedded Systems Security 2.2 無法存取透過 MTP 連線的行動裝置的系統資料。您不能使用基於有關所有連線的裝置的系統資料的規則清單填寫方案，為透過 MTP 連線的行動裝置建立允許規則。

基於有關連線到網路電腦的外部裝置的系統資料產生規則

您可以使用三個方案，基於有關曾經或目前連線的所有大容量儲存的 Windows 資料產生規則（（請參見第 174 頁上的“關於透過卡巴斯基安全管理中心建立所有電腦的裝置控制規則”部分）：

- 使用“裝置控制規則產生器”群組工作。可在規則建立過程中使用此方案，以便將所有曾經連接過的、由所有網路電腦上的系統註冊的大容量儲存考慮在內。
- 使用“裝置控制”政策設定中的“**基於系統資料產生規則**”選項。可在規則建立過程中使用此方案，以便將所有曾經連接過的、由安裝卡巴斯基安全管理中心管理主控台的電腦上的系統註冊的大容量儲存考慮在內。
- 使用裝置控制政策設定和“裝置控制規則產生器”工作設定中的“**基於連接的裝置產生規則**”。產生允許規則時，如果想要僅考慮目前已連線到受防護電腦上的裝置的有關資料，請使用此方法。

Kaspersky Embedded Systems Security 2.2 無法存取透過 MTP 連線的行動裝置的系統資料。您不能使用基於有關所有連線的裝置的系統資料的規則清單填寫方案，為透過 MTP 連線的行動裝置建立允許規則。

本章節說明項目

使用“裝置控制規則產生器”工作建立規則

► *若要使用“裝置控制規則產生器”工作為一組電腦指定裝置控制規則，請執行以下步驟。*

1. 在所設定伺服器群組的主控台中的“**工作**”標籤上，建立一個“裝置控制規則產生器”群組工作或選擇一個現有工作。
2. 在建立的“應用程式啟動控制規則產生器”群組工作的內容中或在工作精靈中，指定以下設定：
   - 在“**通知**”部分中，設定用於儲存工作執行報告的設定。
   - 在“**設定**”部分中，指定工作在完成後的操作。指定建立的規則將匯出到的檔案名稱。
   - 在“**排程**”部分中設定工作啟動排程設定。
3. 在所設定電腦群組的主控台上的“**工作**”標籤上，從群組工作清單中選擇您已建立的“裝置控制規則產生器”，然後點擊“**啟動**”按鈕啟動工作。

   工作完成後，自動建立的允許規則清單將儲存在共用網路資料夾中的 XML 檔案中。

   在網路中使用裝置控制政策之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果不提供組織的政策用於網路中的共用網路資料夾，則建議為測試電腦群組或範本機上的電腦控制規則啟動“規則產生器”工作。

4. 將建立的允許規則清單新增到“裝置控制”工作。為此，在所設定政策的內容的“裝置控制”工作設定中：
   a. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。

      將開啟“**裝置控制規則**”視窗。
   b. 點擊“**新增**”按鈕，然後在開啟的清單中選擇“**從 XML 檔案匯入規則**”。
   c. 選擇將自動建立的允許規則新增到先前建立的“裝置控制”規則清單中的政策：
      - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
      - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
      - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
   d. 在開啟的 Microsoft Windows 標準視窗中，選擇“裝置控制規則產生器”群組工作完成後建立的 XML 檔案。
   e. 在“裝置控制規則”和“**工作設定**”視窗點擊“**確定**”。
5. 如果想要應用建立的裝置控制規則，請在“**裝置控制**”政策設定中選擇“**活動**”工作模式。

基於每台單獨的電腦上的系統資料自動建立的允許規則將被套用於所設定政策涵蓋的所有網路電腦。在這些電腦上，應用程式將僅允許已為其建立允許規則的那些裝置進行連接。

基於卡巴斯基安全管理中心政策中的系統資料建立允許規則

► *若要使用“裝置控制”政策中的“**基於系統資料產生規則**”選項指定允許規則，請執行以下步驟：*

1. 如有必要，將您希望信任的新的大容量儲存器連線到安裝了卡巴斯基安全管理中心管理主控台的電腦。
2. 在卡巴斯基安全管理中心的管理主控台中，展開“**受管理裝置**”節點。
3. 展開您要為其配置政策設定的管理群組，然後在詳細資訊視窗中選擇“**政策**”標籤。
4. 在您希望配置政策的內容功能表中選擇“**內容**”。
5. **內容：<內容名稱>** 視窗開啟。
6. 在政策設定中，開啟“裝置控制”工作設定並執行以下步驟：
   a. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。

      將開啟“**裝置控制規則**”視窗。
   b. 點擊“**新增**”按鈕，在開啟的內容功能表中，選擇“**基於系統資料產生規則**”選項。
   c. 選擇將允許規則新增到先前建立的“裝置控制”規則清單中的政策：
      - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
      - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
      - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
7. 在“**裝置控制規則**”和“**工作設定**”視窗點擊“**確定**”。

“裝置控制”政策中的規則清單將使用基於安裝了卡巴斯基安全管理中心管理主控台的電腦的系統資料建立的新規則填充。

為已連線的裝置建立規則

► *若要使用“ 裝置控制”政策中的“* ***基於系統資料產生規則****”選項指定允許規則，請執行以下步驟：*

1. 在卡巴斯基安全管理中心的管理主控台中，展開“ **受管理裝置**”節點。
2. 展開您要為其配置政策設定的管理群組，然後在詳細資訊視窗中選擇“ **政策**”標籤。
3. 在您希望配置政策的內容功能表中選擇“ **內容**”。
4. **內容：<內容名稱>** 視窗開啟。
5. 在“ **本機活動控制**”部分中，點擊“ **裝置控制**”部分的“ **設定**”按鈕。
6. 在“ **一般**”標籤上，點擊“ **規則清單**”按鈕。

   將開啟“ **裝置控制規則**”視窗。
7. 點擊“ **新增**”按鈕，然後在內容功能表中，選擇“ **基於連接的裝置產生規則**”。

   將開啟“ **基於系統資料產生規則**”視窗。
8. 在偵測到的已連線到受防護電腦的裝置清單中，選擇您要為其生成允許規則的裝置。
9. 點擊為所選裝置“ **新增**”規則按鈕。
10. 在“ **裝置控制**”視窗中點擊“ **儲存**”按鈕。

“ 裝置控制”政策中的規則清單將使用基於安裝了卡巴斯基安全管理中心管理主控台的電腦的系統資料建立的新規則填充。

從有關受限制裝置的卡巴斯基安全管理中心報告的檔案中匯入規則

您可從在“ **僅統計**”模式下完成裝置控制工作後卡巴斯基安全管理中心中產生的報告匯入有關受限制裝置連線的資料，並使用此資料在所配置政策中產生裝置控制允許規則清單。

建立裝置控制工作期間發生的附隨報告時，您可跟蹤其連接受限制的裝置。

將資料從受限制裝置報告匯入到政策設定時，確保您所使用的清單僅包含希望允許連線的裝置。

► *若要基於有關受限制裝置的卡巴斯基安全管理中心報告為一組電腦指定裝置連接允許規則，請執行以下步驟：*

1. 在“裝置控制”工作設定的政策內容中，選擇“**僅統計**”模式。
2. 在“**事件**”部分中的政策內容中，確保：
   - “*已限制大容量儲存*”事件的“**緊急事件**”標籤顯示超過“**僅統計**”模式下排程的工作執行時間的事件儲存時間（預設值為 30 天）。
   - “*僅統計：已偵測到不受信任的大容量儲存*”事件的“**警告**”標籤顯示超過“**僅統計**”模式下排程的工作執行時間的事件儲存時間（預設值為 30 天）。

   當達到“**儲存時間**”列中指定的期限時，則有關記錄的事件的資訊會被刪除且不會反映在報告檔案中。在“**僅統計**”模式下執行裝置控制工作之前，確保工作執行時間不超過為指定事件配置的儲存時間。
3. 當工作完成後，將記錄的事件匯出到 TXT 檔案。為此，展開“**記錄和通知**”節點，然後在“**事件**”子節點中，基於“*被拒絕*”條件建立一系列事件，以檢視裝置控制工作將限制其連線的裝置。在選擇的詳細資訊視窗中，點擊“**將事件匯出到檔案**”清單以將有關受封鎖應用程式啟動的報告儲存到 TXT 檔案。

   在政策中匯入和應用建立的報告之前，確保報告僅包含有關您希望允許其連線的裝置的資料。
4. 將有關受限制裝置連線的資料匯入“裝置控制”政策。為此，在所設定政策的內容的“裝置控制”工作設定中，執行以下步驟：
   a. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。

      將開啟“**裝置控制規則**”視窗。
   b. 點擊“**新增**”按鈕，然後在該按鈕的內容功能表中選擇“**從卡巴斯基安全管理中心報告匯入封鎖的裝置的資料**”。
   c. 選擇將來自根據卡巴斯基安全管理中心報告建立的清單的規則新增到先前設定的裝置控制規則清單的政策：
      - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
      - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
      - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
   d. 在開啟的 Microsoft Windows 標準視窗中，選擇已將來自受限制裝置報告的事件匯出到的 TXT 檔案。
   e. 在“**裝置控制規則**”和“**工作設定**”視窗點擊“**確定**”。

根據有關受限制裝置的卡巴斯基安全管理中心報告建立的規則將被新增到裝置控制規則清單。

網路活動控制

本節包含有關“防火牆管理”工作的資訊。

防火牆管理

本節包含有關防火牆管理工作以及如何設定的資訊。

本章節說明項目

關於防火牆管理工作

Kaspersky Embedded Systems Security 2.2 會提供一個可靠且符合人體工程學的解決方案，以便使用防火牆管理工作防護網路連線。

防火牆管理工作不會執行獨立的網路流量篩選，但它允許您透過 Kaspersky Embedded Systems Security 2.2 圖形介面管理 Windows 防火牆。在防火牆管理工作期間，Kaspersky Embedded Systems Security 2.2 接管對作業系統防火牆的設定和政策的管理，並封鎖進行任何外部防火牆配置。

在應用程式安裝期間，防火牆管理元件會讀取並複製 Windows 防火牆狀態及所有指定規則。此後，只能變更規則集和規則參數，且防火牆只能在 Kaspersky Embedded Systems Security 2.2 中開啟或關閉。

如果在安裝 Kaspersky Embedded Systems Security 2.2 期間 Windows 防火牆關閉，則在安裝完成後將不會執行防火牆管理工作。如果在安裝應用程式期間 Windows 防火牆開啟，則會在安裝完成後執行防火牆管理工作，從而封鎖指定規則不允許的所有網路連線。

預設情況下，不會安裝防火牆管理元件，因為其未包括在建議安裝元件集中。

防火牆管理工作強制封鎖工作的指定規則不允許的所有傳入和傳出連接。

該工作會定期輪詢 Windows 防火牆並監控其狀態。預設情況下，輪詢間隔設定為 1 分鐘且無法變更。如果在輪詢期間 Kaspersky Embedded Systems Security 2.2 偵測到 Windows 防火牆設定和防火牆管理工作設定之間存在不比對，應用程式會強制應用作業系統防火牆上的工作設定。

使用 Windows 防火牆的逐分鐘輪詢，Kaspersky Embedded Systems Security 2.2 可以監控：

- Windows 防火牆的執行狀態。
- 安裝 Kaspersky Embedded Systems Security 2.2 後其他應用程式或工具新增的規則的狀態（例如，使用 wf.msc 的某個連接埠/應用程式新增的新應用程式規則）。

當向 Windows 防火牆套用新規則時，Kaspersky Embedded Systems Security 2.2 會在 **Windows 防火牆**管理單元中建立 Kaspersky Embedded Systems Security 群組規則集。此規則集可統一 Kaspersky Embedded Systems Security 2.2 使用防火牆管理工作建立的所有規則。在輪詢期間，應用程式不會每分鐘監控 Kaspersky Embedded Systems Security 群組中的規則，且該規則不會自動與防火牆管理工作設定中指定的規則清單同步。

► *要手動更新 Kaspersky Embedded Systems Security 群組規則，*

請重新啟動 Kaspersky Embedded Systems Security 2.2 防火牆管理工作。

您還可使用 **Windows 防火牆**管理單元手動編輯 Kaspersky Embedded Systems Security 群組規則。

如果按卡巴斯基安全管理中心群組政策管理 Windows 防火牆，則防火牆管理工作無法啟動。

關於防火牆規則

防火牆管理工作使用工作執行期間強制套用於 Windows 防火牆的允許規則控制傳入和傳出網路流量的篩選。

初次開機工作時，Kaspersky Embedded Systems Security 2.2 會讀取 Windows 防火牆設定中指定的所有傳入網路流量規則，並將其複製到防火牆管理工作設定。然後，應用程式根據以下規則執行：

- 如果在 Windows 防火牆設定中建立新規則（在安裝新應用程式期間手動或自動建立），Kaspersky Embedded Systems Security 2.2 會刪除該規則。
- 如果從 Windows 防火牆設定中刪除現有規則，Kaspersky Embedded Systems Security 2.2 會還原該規則。
- 如果在 Windows 防火牆設定中變更現有規則的參數，Kaspersky Embedded Systems Security 2.2 會回溯變更。
- 如果在防火牆管理設定中建立新規則，Kaspersky Embedded Systems Security 2.2 會將該規則強制套用於 Windows 防火牆。
- 如果從防火牆管理設定中刪除現有規則，Kaspersky Embedded Systems Security 2.2 會從 Windows 防火牆設定中強制刪除該規則。

Kaspersky Embedded Systems Security 2.2 不會使用封鎖規則或控制傳出網路流量的規則。在防火牆管理工作啟動後，Kaspersky Embedded Systems Security 2.2 會從 Windows 防火牆設定中刪除所有此類規則。

您可為傳入網路流量設定、刪除和編輯篩選規則。

您無法在防火牆管理工作設定中指定新規則以控制傳出網路流量。Kaspersky Embedded Systems Security 2.2 中指定的所有防火牆規則僅控制傳入網路流量。

您可管理以下類型的防火牆規則：

- 應用程式規則。
- 連接埠規則。

應用程式規則

此類型的規則允許指定應用程式的目的網路連線。這些規則的觸發條件基於可執行檔的路徑。

您可管理應用程式規則：

- 新增新規則。
- 刪除現有規則。
- 啟用或停用指定規則。
- 編輯指定規則的參數：指定規則名稱、可執行檔的路徑以及規則使用範圍。

連接埠規則

此類型的規則允許指定連接埠和協定 (TCP/UDP) 的網路連線。這些規則的觸發條件基於連接埠號和協定類型。

您可管理連接埠規則：

- 新增新規則。
- 刪除現有規則。
- 啟用或停用指定規則。
- 編輯指定規則的參數：設定規則名稱、連接埠號、協定類型以及規則的應用範圍。

連接埠規則的範圍比應用程式規則的範圍要廣。透過基於連接埠規則允許連線，會下降受防護電腦的安全等級。

啟用和停用防火牆規則

► *要啟用或停用篩選傳入網路流量的現有規則，請執行以下操作：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。

3. 在“**網路活動控制**”部分中，點擊“**防火牆管理**”設定塊中的“**設定**”按鈕。
4. 在開啟的視窗中點擊“**規則清單**”按鈕。

   將開啟“**規則清單**”視窗。
5. 根據想要修改其狀態的規則類型，選擇“**應用程式**”或“**連接埠**”。
6. 在規則清單中，選擇要修改其狀態的規則，然後執行以下操作之一：
   - 如果您想要啟用已停用的規則，選中規則名稱左側的核取方塊。

     將啟用所選規則。
   - 如果您想要停用已啟用的規則，清除規則名稱左側的核取方塊。

     將停用所選規則。
7. 在“**規則清單**”視窗中，點擊“**儲存**”。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

手動新增防火牆規則

您只能新增和編輯應用程式和連接埠的規則。您無法新增新的群組規則或編輯現有群組規則。

► *要新增篩選傳入網路流量的新規則或編輯現有規則，請執行以下操作：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**網路活動控制**”部分中，點擊“**防火牆管理**”設定塊中的“**設定**”按鈕。
4. 在開啟的視窗中點擊“**規則清單**”按鈕。

   將開啟“**規則清單**”視窗。

5. 根據您要新增的規則類型，選擇“**應用程式**”或“**連接埠**”標籤，然後執行以下操作之一：
   - 要編輯現有規則，在規則清單中選擇要編輯的規則，然後點擊“**編輯**”。
   - 要新增新規則，點擊“**新增**”。

     根據配置的規則類型，將開啟“**連接埠規則**”視窗或“**應用程式規則**”視窗。
6. 在開啟的視窗中，執行以下操作：
   - 如果您使用的是應用程式規則，請執行以下操作：
     a. 輸入已編輯規則的“**規則名稱**”。
     b. 指定您透過修改此規則允許其連線的應用程式的可執行檔的“**應用程式路徑**”。

        您可手動或透過使用“**瀏覽**”按鈕設定路徑。
     c. 在“**規則套用範圍**”欄位中，指定將為其套用已修改規則的網路位址。

        > 您只能使用 IPv4 IP 位址。
   - 如果您使用的是連接埠規則，請執行以下操作：
     a. 輸入已編輯規則的“**規則名稱**”。
     b. 指定應用程式將允許連線的“**連接埠號**”。
     c. 選擇應用程式將允許連線的協定類型 (TCP/UDP)。
     d. 在“**規則套用範圍**”欄位中，指定將為其套用已修改規則的網路位址。

        > 您只能使用 IPv4 IP 位址。
7. 在“**應用程式規則**”或“**連接埠規則**”視窗中，點擊“**確定**”。
8. 在“**防火牆規則**”視窗中，點擊“**儲存**”。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

刪除防火牆規則

您只能刪除應用程式和連接埠規則。您無法刪除現有群組規則。

► *要刪除篩選傳入網路流量的現有規則，請執行以下操作：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**網路活動控制**”部分中，點擊“**防火牆管理**”設定塊中的“**設定**”按鈕。
4. 在開啟的視窗中點擊“**規則清單**”按鈕。

   將開啟“**規則清單**”視窗。
5. 根據想要修改器狀態的規則類型，選擇“**應用程式**”或“**連接埠**”標籤。
6. 在規則清單中，選擇要刪除的規則。
7. 點擊“**刪除**”按鈕。

   將刪除所選規則。
8. 在“**防火牆規則**”視窗中，點擊“**儲存**”。

將儲存指定防火牆管理工作設定。新規則參數將傳送到 Windows 防火牆。

系統稽核

本節包含有關檔案完整性監控工作以及稽核作業系統記錄功能的資訊。

本章內容

檔案完整性監控

本節包含有關啟動和設定“檔案完整性監控”工作的資訊。

本章節說明項目

關於“檔案完整性監控”工作

“檔案完整性監控”工作的設計目的是為了跟蹤針對工作設定中指定的監控範圍內的特定檔案和資料夾執行的操作。可以使用該工作來刪除可能對受防護的電腦造成安全入侵的檔案變更。還可以配置監控被中斷期間要對其進行跟蹤的檔案變更。

當監控範圍暫時位於工作範圍之外時（例如，如果工作停止或如果受防護的電腦上沒有物理顯示受防護的裝置），會出現*監控中斷*。一旦重新連線大容量儲存裝置，Kaspersky Embedded Systems Security 2.2 將報告監控範圍內偵測到的檔案操作。

如果由於重新安裝“檔案完整性監控”元件造成指定監控範圍內的工作停止執行，則不構成監控中斷。這種情況下，“檔案完整性監控”工作並未執行。

環境要求

要啟動“檔案完整性監控”工作，必須滿足以下條件：

- 受防護的電腦上必須安裝有支援 ReFS 和 NTFS 檔案系統的儲存裝置。
- 必須啟用 Windows USN 記錄。元件查詢此記錄來獲取有關檔案操作的資訊。

> 如果為某個磁區建立規則後啟用了 USN 記錄且已啟動“檔案完整性監控”工作，則必須重啟該工作。如果不重啟，則監控過程中不會套用該規則。

排除監控範圍

可以建立監控範圍排除項目（請參見第 190 頁上的“配置監控規則”部分）。排除針對每個單獨的規則進行指定，並且僅對指定的監控範圍產生作用。可以為每個規則指定無限數量的排除。

> 排除比監控範圍具有更高的優先順序，且即使指定的資料夾或檔案位於監控範圍內，也不受工作的監控。如果其中一個規則的設定指定的監控範圍比排除中指定的資料夾具有更低的等級，則當工作執行時將不會考慮監控範圍。

要指定排除，可以使用與用於指定監控範圍相同的遮罩。

關於檔案操作監控規則

“檔案完整性監控”根據檔案操作監控規則執行。可以使用規則觸發條件來配置觸發工作的條件，以及調整工作記錄中記錄的已刪除檔案操作的事件的重要性等級。

針對每個監控範圍指定了檔案操作監控規則。

可以配置以下規則觸發條件：

- 受信任使用者。
- 檔案操作標記。

受信任使用者

預設情況下，應用程式將所有操作視為潛在安全入侵。受信任使用者清單為空。可以透過在檔案操作監控規則設定中建立受信任使用者清單來配置事件重要性等級。

不受信任使用者 – 監控範圍規則設定中的受信任使用者清單中未指定的任何使用者。如果 Kaspersky Embedded Systems Security 2.2 偵測到不受信任使用者執行的檔案操作，則“檔案完整性監控”工作將在工作記錄中記錄一個緊急事件。

受信任使用者 – 經過授權可在指定的監控範圍內執行檔案操作的使用者或使用者群組。如果 Kaspersky Embedded Systems Security 2.2 偵測到受信任使用者執行的檔案操作，則“檔案完整性監控”工作將在工作記錄中記錄一個“資訊事件”。

Kaspersky Embedded Systems Security 2.2 在監控中斷時間內，無法確定啟動操作的使用者。在此情況下，使用者狀態被確定為未知。

未知使用者 – 如果由於工作中斷或者資料同步驅動程式或 USN 記錄失敗導致 Kaspersky Embedded Systems Security 2.2 無法獲取有關使用者的資料，則將此狀態分配給使用者。如果 Kaspersky Embedded Systems Security 2.2 偵測到未知使用者執行的檔案操作，則“檔案完整性監控”工作將在工作記錄中記錄一個“*警告*事件”。

檔案操作標記

當“檔案完整性監控”工作執行時，Kaspersky Embedded Systems Security 2.2 使用檔案操作標記來確定已對檔案執行了操作。

檔案操作標記是可以對檔案操作進行特徵化的獨特敘述符。

每個檔案操作可以是針對檔案進行的單個操作或系列操作。每個此類操作等同於一個檔案操作標記。如果您指定作為規則觸發條件的標記在檔案操作鏈中被刪除，則應用程式將記錄一個事件，表示已執行指定的檔案操作。

已記錄事件的重要性等級不取決於選定的檔案操作標記或事件的數量。

預設情況下，Kaspersky Embedded Systems Security 2.2 考慮所有可用的檔案操作標記。可以在工作規則設定中手動選擇檔案操作標記。

步驟 36. 檔案操作標記

檔案操作 ID	檔案操作標記	支援的檔案系統
BASIC_INFO_CHANGE	已變更檔案或資料夾的內容或時間標記	NTFS、ReFS
COMPRESSION_CHANGE	已變更檔案或資料夾的壓縮	NTFS、ReFS
DATA_EXTEND	已變更檔案或資料夾的大小	NTFS、ReFS
DATA_OVERWRITE	已覆蓋檔案或資料夾中的資料	NTFS、ReFS
DATA_TRUNCATION	已截斷檔案或資料夾	NTFS、ReFS
EA_CHANGE	已變更延伸的檔案或資料夾內容	僅限 NTFS
ENCRYPTION_CHANGE	已變更檔案或資料夾的加密狀態	NTFS、ReFS
FILE_CREATE	首次建立檔案或資料夾	NTFS、ReFS
FILE_DELETE	使用 SHIFT+DEL 組合鍵永久刪除的檔案或資料夾	NTFS、ReFS
HARD_LINK_CHANGE	已為建立或刪除檔案或資料夾的硬連結	僅限 NTFS
INDEXABLE_CHANGE	已變更檔案或資料夾的索引狀態	NTFS、ReFS
INTEGRITY_CHANGE	已變更命名的檔案流的完整性內容	僅限 ReFS
NAMED_DATA_EXTEND	已增大命名的檔案流的大小	NTFS、ReFS
NAMED_DATA_OVERWRITE	已覆蓋命名的檔案流	NTFS、ReFS

檔案操作 ID	檔案操作標記	支援的檔案系統
NAMED_DATA_TRUNCATION	已截斷命名的檔案流	NTFS、ReFS
OBJECT_ID_CHANGE	已變更檔案或資料夾識別碼	NTFS、ReFS
RENAME_NEW_NAME	已為檔案或資料夾分配新名稱	NTFS、ReFS
REPARSE_POINT_CHANGE	已為檔案或資料夾建立新的重分析點或變更其現有重分析點	NTFS、ReFS
SECURITY_CHANGE	已變更檔案或資料夾存取權限	NTFS、ReFS
STREAM_CHANGE	已建立新的命名的檔案流或變更現有命名的檔案流	NTFS、ReFS
TRANSACTED_CHANGE	TxF 事務已變更命名的檔案流	僅限 ReFS

配置“檔案完整性監控”工作

可以變更檔案完整性監控的預設設定（請參見下表）。

步驟 37. 預設的“檔案完整性監控”工作設定

設定	預設值	敘述
監控範圍	未配置	可以指定操作將監控的資料夾和檔案。將針對指定監控範圍內的資料夾和檔案生成監控事件。
受信任使用者清單	未配置	可以指定使用者和/或使用者群組，其在指定目錄中的操作將被元件視為安全。
工作未執行時監控檔案操作	已使用	可以啟用或停用工作未執行期間在指定監控範圍內執行的檔案操作的記錄。
考慮排除的監控範圍	未套用	可以針對無需監控檔案操作的資料夾檢查排除的使用情況。當 檔案完整性監控”執行時, Kaspersky Embedded Systems Security 2.2 將略過指定為排除的監控範圍。
校驗和計算	未套用	可以配置在對檔案做出變更後進行檔案校驗和計算。
考慮檔案操作標記	考慮所有可用的檔案操作標記	可以指定一組檔案操作標記。如果在監控範圍內執行的檔案操作被一個或多個指定標記進行過特徵化，則 Kaspersky Embedded Systems Security 2.2 會生成一個審查事件。
工作啟動排程	不設定工作的初次啟動排程	您可以配置排程的工作啟動設定。

► *要配置一般“檔案完整性監控”工作設定，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**系統稽核**”部分的“**檔案完整性監控**”部分中，點擊“**設定**”按鈕。

   將開啟“**檔案完整性監控**”視窗。
4. 在開啟的視窗的“**檔案操作監控設定**”標籤中，配置監控範圍設定：
   a. 清除或選中“**記錄監控中斷期間發生的檔案操作資訊**”核取方塊。

      當由於任何原因（拆除硬碟磁碟機、使用者停止工作、軟體錯誤）工作未執行時，該核取方塊可以啟用或停用“檔案完整性監控”設定中指定的檔案操作的監控。

      如果選中該核取方塊，則當“檔案完整性監控”工作未執行時，Kaspersky Embedded Systems Security 2.2 將記錄所有監控範圍內的事件。

      如果清除該核取方塊，則當工作未執行時，應用程式將不記錄監控範圍內的檔案操作。

      預設將會選定該核取方塊。

   b. 新增工作要監控的監控範圍（請參見第 190 頁上的“配置監控規則”部分）。
5. 在“**工作管理**”標籤上，啟動基於排程的工作（請參見第 107 頁上的“管理工作排程”部分）。
6. 點擊“**確定**”以儲存變更。

配置監控規則

預設情況下，未指定監控範圍且工作不會監控任何目錄中的檔案操作。

► *要新增監控範圍，請執行以下步驟：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**系統稽核**”部分的“**檔案完整性監控**”部分中，點擊“**設定**”按鈕。

   內容：將開啟“**檔案完整性監控**”視窗。
4. 在“**監控範圍**”部分，點擊“**新增**”按鈕。

   將開啟“**監控範圍**”視窗。
5. 透過以下方式之一新增監控範圍：
   - 如果要透過標準的 Microsoft Windows 對話方塊來選擇資料夾：
     a. 點擊“**瀏覽**”按鈕。

        將開啟標準 Microsoft Windows“瀏覽資料夾”視窗。

     b. 在開啟的視窗中，選擇要監控操作的資料夾，然後點擊“**確定**”按鈕。
   - 如果想要手動指定監控範圍，請使用支援的遮罩新增路徑：
     - <*.ext> - 帶有 <ext> 副檔名的所有檔案，與其位置無關；
     - <*\name.ext> - 帶有 <name> 名稱和 <ext> 副檔名的所有檔案，與其位置無關；
     - <\dir*> - 位於 <\dir> 目錄中的所有檔案；
     - <\dir*\name.ext> - <\dir> 目錄及其所有子目錄中帶有 <name> 名稱和 <ext> 副檔名的所有檔案。

   當手動指定監控範圍時，請確保路徑為以下格式：<磁區字母>:\<遮罩>如果缺少磁區字母，則 Kaspersky Embedded Systems Security 2.2 將不會新增指定的監控範圍。
6. 在“**受信任使用者**”部分，點擊“**新增**”按鈕。

   將開啟標準的 Microsoft Windows“**選擇使用者或群組**”視窗。

7. 選擇在選定的監控範圍內允許其進行檔案操作的使用者或使用者群組，然後點擊“**確定**”按鈕。

   預設情況下，Kaspersky Embedded Systems Security 2.2 將未列入受信任使用者清單的所有使用者視為不受信任（請參見第 186 頁上的“關於檔案操作監控規則”部分），並為他們產生緊急事件。

8. 選擇“**檔案操作標記**”標籤。
9. 如果需要，請執行以下操作來選擇一定數量的標記：
   a. 選擇“**基於以下標記偵測檔案操作**”選項。
   b. 在“可用檔案操作清單”中（請參見第 186 頁上的“關於檔案操作監控規則”部分），選擇您要監控的操作旁邊的核取方塊。

   預設情況下，Kaspersky Embedded Systems Security 2.2 將偵測所有檔案操作標記，已選擇“**基於所有可辨識的標記偵測檔案操作**”選項。

10. 如果執行操作後，您想要 Kaspersky Embedded Systems Security 2.2 計算檔案校驗和，請執行以下操作：
    a. 在“**校驗和計算**”部分中，選擇“**如果可能，在檔案變更後計算檔案最終版本的校驗和**”核取方塊。

       如果選中該核取方塊，則 Kaspersky Embedded Systems Security 2.2 將計算修改後的檔案的校驗和，其中偵測到至少帶有一個選定標記的檔案操作。

       如果透過許多標記偵測到檔案操作，則將僅計算進行所有修改後的最終檔案校驗和。

       如果清除該核取方塊，則 Kaspersky Embedded Systems Security 2.2 將為經過修改的檔案計算校驗和。

       以下情況不會執行任何校驗和計算：

       - 如果檔案變為不可用（例如，由於存取權限的變更造成）。
       - 如果此後在已被刪除的檔案中偵測到檔案操作。

       預設取消選定該核取方塊。

    b. 在“**使用算法計算校驗和**”下拉清單中，選擇以下選項之一：

       - **MD5 雜湊**
       - **SHA256 雜湊**

11. 如果您不想監控“可用檔案操作清單”中的所有檔案操作（請參見第 186 頁上的“關於檔案操作監控規則”部分），並選擇您要監控的操作旁邊的核取方塊。
12. 如果必要，透過執行以下步驟新增排除的監控範圍：
    a. 選擇“**排除**”標籤。
    b. 選中“**考慮排除的監控範圍**”核取方塊。

       該核取方塊可以針對無需監控檔案操作的資料夾停用排除。

       如果選中該核取方塊，則當“檔案完整性監控”工作執行時，Kaspersky Embedded Systems Security 2.2 將略過排除清單中指定的監控範圍。

如果取消選中該核取方塊，則 Kaspersky Embedded Systems Security 2.2 將記錄所有指定監控範圍內的事件。

預設情況下，未選中該核取方塊且排除清單為空。

c. 點擊“**新增**”按鈕。

將開啟“**選擇要新增的資料夾**”視窗。

d. 在開啟的視窗中，指定要從監控範圍中排除的資料夾。

e. 點擊“**確定**”。

指定的資料夾被新增到排除範圍清單。

13. 在“**監控範圍**”視窗中點擊“**確定**”。

指定的規則設定將被套用到選定的“檔案完整性監控”工作的監控範圍。

記錄審查

本節包含有關“記錄審查”工作和工作設定的資訊。

本章節說明項目

關於“記錄審查”工作

當“記錄審查”工作執行時，Kaspersky Embedded Systems Security 2.2 將根據 Windows 事件記錄的審查結果監控受防護環境的完整性。一旦偵測到系統中存在異常行為，應用程式將通知管理員，這些異常行為可能表示存在網路攻擊嘗試。

Kaspersky Embedded Systems Security 2.2 將考慮 Windows 事件記錄，並根據使用者指定的規則或啟發式分析的設定（工作用它來審查記錄）來辨識入侵。

預定義規則和啟發式分析

透過套用基於現有啟發的預定義規則，可以使用“記錄審查”工作來監控受防護系統的狀態。啟發式分析可識別受防護電腦上的異常活動，這些異常活動可作為嘗試攻擊的憑證。用於辨識異常行為的範本包括在預定義規則設定中的可用規則內。

“記錄審查”工作的規則清單中包含七條規則。您可以啟用或停用任何一條規則。您不能刪除現有規則或建立新規則。

可以為監控以下操作事件的規則配置觸發條件：

- 密碼暴力破解偵測
- 網路登入偵測

還可在工作設定中配置排除。當登入由受信任使用者執行或從受信任的 IP 位址執行時，不會啟動啟發式分析。

如果工作不使用啟發式分析，則 Kaspersky Embedded Systems Security 2.2 不會使用啟發來審查 Windows 記錄。預設情況下，啟用啟發式分析。

當套用規則時，應用程式將在“記錄審查”工作記錄中記錄一個*緊急事件*。

自訂記錄審查工作的規則

可以使用工作規則設定來指定和變更在 Windows 記錄中偵測到選定事件時的觸發規則條件。預設情況下，記錄審查工作規則的清單包含四種規則。可以啟用和停用這些規則、刪除規則和編輯規則設定。

可以為每種規則配置以下規則觸發條件：

- Windows 事件記錄中的記錄識別碼清單。

  如果事件內容包含為該規則指定的事件識別碼，則當在 Windows 事件記錄中建立新的記錄時將觸發該規則。也可以為每個指定的規則新增和刪除識別碼。

- 事件來源。

  對於每個規則，可以定義 Windows 事件記錄的子記錄。應用程式將僅在此子記錄中搜尋帶有指定事件識別碼的記錄。您可以選擇其中一個標準子記錄（應用程式、安全性或系統）或在來源選擇欄位中輸入名稱來指定自訂子記錄。

  應用程式不會驗證指定的子記錄是否確實存在於 Windows 事件記錄中。

觸發規則後，Kaspersky Embedded Systems Security 2.2 將在“記錄審查”工作記錄中記錄一個緊急事件。

預設情況下，記錄審查工作不套用自訂規則。

在啟動“記錄審查”工作前，請確保系統稽核政策已正確設定。有關詳細資訊，請參見 Microsoft 文章 (https://technet.microsoft.com/zh-tw/library/cc952128.aspx)。

配置預定義工作規則

► *執行以下操作為“記錄審查”工作配置預定義規則：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
   - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

     如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**系統稽核**”部分中，點擊“**記錄審查**”設定塊中的“**設定**”按鈕。

   將開啟“**記錄審查設定**”視窗。
4. 選擇“**預定義規則**”標籤。
5. 選中或清除“**針對記錄審查套用預定義規則**”核取方塊。

   如果選中此核取方塊，則 Kaspersky Embedded Systems Security 2.2 將套用啟發式分析來偵測受防護電腦上的異常活動。

   如果清除此核取方塊，則未執行啟發式分析且 Kaspersky Embedded Systems Security 2.2 將套用預設或自訂規則來偵測異常活動。

   預設將會選定該核取方塊。

   為了能夠執行工作，必須選擇至少一種記錄審查規則。
6. 從預定義規則清單中選擇您要套用的規則：
   - 系統中存在可能的暴力破解攻擊的模式。
   - 系統中存在可能的 Windows 事件記錄濫用的模式。
   - 偵測到表示已安裝新服務的異常活動。
   - 偵測到使用顯式憑據的異常登入。
   - 系統中存在可能的 Kerberos 偽造 PAC (MS14-068) 攻擊的模式。
   - 偵測到特權內建組 Administrators 發出的異常操作。
   - 在網路登入工作階段期間偵測到異常活動。
7. 要配置選定規則，請點擊“**進階設定**”按鈕。

   將開啟“**記錄審查**”視窗。

8. 在“**暴力破解攻擊偵測**”部分中，設定嘗試次數和這些嘗試出現的期限，這些將被視為啟發式分析的觸發器。
9. 在“**網路登入偵測**”部分中，指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 2.2 將登入嘗試視為異常活動。
10. 選擇“**排除**”標籤。
11. 執行以下操作新增受信任使用者：
    a. 點擊“**瀏覽**”按鈕。
    b. 選擇使用者。
    c. 點擊“**確定**”。

    選定的使用者將被新增到受信任使用者清單中。
12. 執行以下操作新增受信任的 IP 位址：
    a. 輸入 IP 位址。
    b. 點擊“**新增**”按鈕。
13. 輸入的 IP 位址將被新增到受信任的 IP 位址清單中。
14. 在“**工作管理**”標籤上，設定工作啟動排程（請參見第 107 頁上的“配置工作啟動排程設定”部分）。
15. 點擊“**確定**”。

儲存記錄審查工作配置。

配置記錄審查規則

► *執行以下操作可新增和配置新的記錄審查自訂規則：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
    - 要配置一組電腦的應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 80 頁上的“配置政策”部分）。
    - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

    如果某個裝置受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過“**應用程式設定**”視窗編輯這些設定。
3. 在“**系統稽核**”部分中，點擊“**記錄審查**”設定塊中的“**設定**”按鈕。

    將開啟“**記錄審查**”視窗。

4. 在“**記錄審查規則**”標籤上，選擇或清除“**套用記錄審查的自訂規則**”標籤。

   如果選中該核取方塊，則 Kaspersky Embedded Systems Security 2.2 將根據每個規則設定對記錄審查套用自訂規則。您可以新增、刪除或配置記錄審查規則。

   如果清除該核取方塊，則不能新增或修改自訂規則。Kaspersky Embedded Systems Security 2.2 將套用預設規則設定。

   預設將會選定該核取方塊。只有應用程式彈出偵測規則處於活動狀態。

   可以控制是否對記錄審查套用預設的規則。選擇您要對記錄審查套用的規則所對應的核取方塊。

5. 要新增新的自訂規則，請點擊“**新增**”按鈕。

   將開啟“**記錄審查規則**”視窗。

6. 在“**一般**”部分中，輸入有關新規則的以下資訊：

   - **名稱**
   - **來源**

     選擇要將已記錄的事件用於分析的來源記錄。提供以下 Windows 事件記錄類型：

     - 應用程式
     - 安全性
     - 系統

     您可以在“**來源**”欄位中輸入記錄名稱來新增新的自訂記錄。

7. 在“**已觸發的事件 ID**”部分中，指定偵測時將觸發規則的項目 ID：

   a. 輸入 ID 的數值。

   b. 點擊“**新增**”按鈕。

      選定的規則 ID 將被新增到清單中。可以為每個規則新增無限數量的識別碼。

   c. 點擊“**確定**”。

   記錄審查規則將被新增到規則清單中。

在卡巴斯基安全管理中心中報告

卡巴斯基安全管理中心中的報告包含有關受管理裝置狀態的資訊。報告基於管理伺服器上儲存的資訊。

從卡巴斯基安全管理中心 11 開始，對於 Kaspersky Embedded Systems Security 2.2，以下類型的報告可用：

- 有關應用程式元件狀態的資訊
- 有關已禁止的應用程式的報告
- 有關在測試模式下禁止的應用程式的報告

有關所有卡巴斯基安全管理中心報告以及如何配置它們的詳細資訊，請參見*卡巴斯基安全管理中心說明*。

有關應用程式元件狀態的資訊

您可以監視所有網路裝置的防護狀態，並獲得每個裝置上的元件集的結構化概覽。

報告顯示每個元件的以下狀態之一：*正在執行*、*已暫停*、*已停止*、*故障*、*未安裝*、*正在啟動*。

*未安裝*狀態指的是元件，而不是應用程式本身。如果未安裝應用程式，卡巴斯基安全管理中心會分配 N/A（不可用）狀態。

您可以建立元件選擇並使用篩選來顯示具有定義的元件集的網路裝置及其狀態。

有關建立和使用選擇的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

► *要在應用程式設定中檢視元件狀態：*

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 90 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。
3. 選擇“**元件**”部分。
4. 檢視狀態表。

► *要檢視卡巴斯基安全管理中心標準報告：*

1. 在應用程式主控台樹狀目錄中選擇“**管理伺服器 <電腦名稱>**”節點。
2. 開啟“**報告**”標籤。
3. 點擊“**有關應用程式元件狀態的報告**”清單項。

   將生成報告。
4. 檢視以下報告詳細資訊：
   - 圖形化圖表。
   - 元件和安裝了每個元件的網路裝置總數以及裝置所屬的群組的匯總表格。
   - 指定了元件狀態、版本、裝置和群組的詳細表格。

有關在活動模式和統計資訊模式下封鎖的應用程式的報告

根據“應用程式啟動控制”工作（請參見第 157 頁上的“透過卡巴斯基安全管理中心管理應用程式啟動”部分）的執行結果，可以生成兩種類型的報告：有關已禁止的應用程式的報告（如果在**活動**模式下啟動該工作）、有關在測試模式下禁止的應用程式的報告（如果在**僅統計資訊**模式下啟動該工作）。這些報告顯示了有關網路的受防護伺服器上封鎖的應用程式的資訊。每個報告都針對所有管理組生成，並累積來自受防護裝置上安裝的所有 Kaspersky Lab 應用程式的資料。

► *要檢視有關在測試模式下禁止的應用程式的報告：*

1. 在“僅統計”模式下啟動“應用程式控制”工作（請參見第 158 頁上的“配置應用程式啟動控制工作設定”部分）。
2. 在應用程式主控台樹狀目錄中選擇“**管理伺服器 <電腦名稱>**”節點。
3. 開啟“**報告**”標籤。
4. 點擊“**有關在測試模式下禁止的應用程式的報告**”清單項。

   將生成報告。
5. 檢視以下報告詳細資訊：
   - 顯示封鎖啟動次數最多的前十個應用程式的圖形化圖表。
   - 發生的應用程式封鎖的匯總表格，其中指定可執行檔名稱、原因、封鎖時間和發生封鎖的裝置數量。
   - 指定了有關裝置、檔案路徑和封鎖條件的資料的詳細表格。

► *要檢視有關在活動模式下禁止的應用程式的報告：*

1. 在“活動”模式下啟動“應用程式控制”工作（請參見第 158 頁上的“配置應用程式啟動控制工作設定”部分）。
2. 在應用程式主控台樹狀目錄中選擇“**管理伺服器 <電腦名稱>**”節點。
3. 開啟“**報告**”標籤
4. 點擊“**有關禁止的應用程式的報告**”清單項。

   將生成報告。

此報告與有關在測試模式下禁止的應用程式的報告包含相同的資料塊。

從命令列使用 Kaspersky Embedded Systems Security 2.2

本節描述從命令列使用 Kaspersky Embedded Systems Security 2.2。

本章內容

命令列指令

如果您在 Kaspersky Embedded Systems Security 2.2 安裝期間將“命令列實用工具”包含在安裝的功能清單中，則可透過受防護電腦的命令列執行基本的 Kaspersky Embedded Systems Security 2.2 管理指令。

使用命令列指令，您僅可管理那些可以根據 Kaspersky Embedded Systems Security 2.2 分配給您的權限來存取的功能。

某些 Kaspersky Embedded Systems Security 2.2 指令在以下模式下執行：

- 同步模式：管理僅在執行指令後回傳到主控台。
- 非同步模式：管理在執行指令後立即回傳到主控台。

► *在同步模式下中斷指令執行*

按 **Ctrl+C** 鍵盤快速鍵。

輸入 Kaspersky Embedded Systems Security 2.2 指令時，應遵循以下規則：

- 使用大寫和小寫輸入參數和指令。
- 使用空白字元分隔參數。
- 如果將其路徑指定為參數值的檔案/資料夾名稱包含空格，請提供括在引號中的檔案/資料夾路徑，例如 "C:\TEST\test cpp.exe"
- 若有需要，可在檔案名稱或路徑遮罩中使用佔位字元，例如：“C:\Temp\Temp*\”，“C:\Temp\Temp???.doc”，“C:\Temp\Temp*.doc”

在管理 Kaspersky Embedded Systems Security 2.2 所需的所有各項操作中均可使用命令列（請參見下表）。

步驟 38. Kaspersky Embedded Systems Security 2.2 指令

指令	敘述
KAVSHELL APPCONTROL（請參見第 210 頁上的“填寫應用程式啟動控制規則清單 KAVSHELL APPCONTROL”部分）	根據選定的新增原則更新指定的規則清單。
KAVSHELL APPCONTROL /CONFIG（請參見第 208 頁上的“管理應用程式啟動控制工作 KAVSHELL APPCONTROL /CONFIG”部分）	控制“應用程式啟動控制”工作的執行模式
KAVSHELL APPCONTROL /GENERATE（請參見第 208 頁上的“應用程式啟動控制規則產生器 KAVSHELL APPCONTROL /GENERATE”部分）	啟動“應用程式啟動控制規則產生器”工作。
KAVSHELL VACUUM（請參見“Kaspersky Embedded Systems Security 2.2 記錄檔案磁碟整理。KAVSHELL VACUUM”部分（位於第 218 頁上））	對 Kaspersky Embedded Systems Security 2.2 記錄檔案進行磁碟整理。
KAVSHELL PASSWORD	管理密碼防護設定。
KAVSHELL HELP（請參見“顯示 Kaspersky Embedded Systems Security 2.2 指令說明。KAVSHELL HELP”部分（位於第 201 頁上））	顯示 Kaspersky Embedded Systems Security 2.2 指令說明。
KAVSHELL START（請參見第 202 頁上的“啟動和停止 Kaspersky Security 服務 KAVSHELL START, KAVSHELL STOP”部分）	啟用 Kaspersky Embedded Systems Security 2.2 服務。
KAVSHELL STOP（請參見第 202 頁上的“啟動和停止 Kaspersky Security Service KAVSHELL START, KAVSHELL STOP”部分）	停止 Kaspersky Embedded Systems Security 2.2 服務。
KAVSHELL SCAN（請參見“掃描選定區域。KAVSHELL SCAN”部分（位於第 202 頁上））	建立並啟動暫時自訂掃描工作（其掃描範圍和安全設定由指令修飾符設定）。
KAVSHELL SCANCRITICAL（請參見“啟動‘關鍵區域掃描’工作。KAVSHELL SCANCRITICAL”部分（位於第 206 頁上））	啟動關鍵區域掃描系統工作。
KAVSHELL TASK（請參見“非同步管理指定工作。KAVSHELL TASK”部分（位於第 206 頁上））	非同步開始/暫停/繼續/停止選擇的工作/傳回目前工作狀態/統計資訊。
KAVSHELL RTP（請參見“啟動及停止即時防護工作。KAVSHELL RTP”部分（位於第 207 頁上））	開始或停止即時防護工作。
KAVSHELL UPDATE（請參見“啟動 Kaspersky Embedded Systems Security 2.2 資料庫更新工作。KAVSHELL UPDATE”部分（位於第 212 頁上））	啟動 Kaspersky Embedded Systems Security 2.2 資料庫更新工作（其設定使用指令修飾符指定）。

指令	敘述
KAVSHELL ROLLBACK（請參見“回溯 Kaspersky Embedded Systems Security 2.2 資料庫更新。KAVSHELL ROLLBACK”部分（位於第 214 頁上））	將資料庫回溯至之前版本。
KAVSHELL LICENSE（請參見第 215 頁上的“啟動應用程式 KAVSHELL LICENSE”部分）	管理金鑰。
KAVSHELL TRACE（請參見“啟用、設定和停用偵錯記錄。KAVSHELL TRACE”部分（位於第 216 頁上））	啟用或停用偵錯記錄，管理偵錯記錄的設定。
KAVSHELL DUMP（請參見“啟用和停用傾印檔案建立。KAVSHELL DUMP”部分（位於第 219 頁上））	在處理程序異常終止時，啟用或停用 Kaspersky Embedded Systems Security 2.2 處理程序傾印檔案。
KAVSHELL IMPORT（請參見“匯入設定。KAVSHELL IMPORT”部分（位於第 220 頁上））	從預先建立的設定檔匯入 Kaspersky Embedded Systems Security 2.2 設定、功能及工作。
KAVSHELL EXPORT（請參見“匯出設定。KAVSHELL EXPORT”部分（位於第 221 頁上））	將所有 Kaspersky Embedded Systems Security 2.2 設定和現有工作匯出至設定檔。
KAVSHELL DEVCONTROL（請參見“填寫裝置控制規則清單。KAVSHELL DEVCONTROL”部分（位於第 211 頁上））	根據選定的方法新增到已生成的裝置控制規則清單中。

顯示 Kaspersky Embedded Systems Security 2.2 指令說明。KAVSHELL HELP

若要獲得所有 Kaspersky Embedded Systems Security 2.2 指令的清單，請使用以下指令之一：

KAVSHELL

KAVSHELL HELP

KAVSHELL /?

若要獲得指令概覽及其語法，請執行下列一個指令：

KAVSHELL HELP <指令>

KAVSHELL <指令> /?

KAVSHELL HELP 指令範例

若要檢視有關 KAVSHELL SCAN 指令的詳細資訊，請執行下列指令：

KAVSHELL HELP SCAN

啟動和停止 Kaspersky Security Service KAVSHELL START, KAVSHELL STOP

若要執行 Kaspersky Security 服務，請執行指令

KAVSHELL START

預設情況下，Kaspersky Security 服務啟動時，“即時檔案防護”和“系統啟動時掃描”工作以及其他排程在“**在應用程式啟動時**”啟動的工作也會一起啟動。

若要停止 Kaspersky Security 服務，請執行指令

KAVSHELL STOP

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

掃描指定區域。KAVSHELL SCAN

若要開始掃描受防護電腦特定區域的工作，請使用 KAVSHELL SCAN 指令。指令參數指定選定節點的掃描範圍和安全設定。

使用 KAVSHELL SCAN 指令啟動的自訂掃描工作為暫時工作。它僅在執行時才顯示在應用程式主控台中（您無法在應用程式主控台中檢視工作設定）。同一時間，會產生工作效能記錄。它會顯示在應用程式主控台的“**工作記錄**”中。

在自訂掃描工作中指定路徑時，可設定環境變數。如果使用由使用者的環境變數，請使用該使用者的權限執行 KAVSHELL SCAN 指令。

KAVSHELL SCAN 指令在同步模式下執行。

要從命令列啟動現有自訂掃描工作，請使用 KAVSHELL TASK（請參見“非同步管理指定工作。KAVSHELL TASK”部分（位於第 206 頁上））指令。

KAVSHELL SCAN 指令語法

KAVSHELL SCAN <掃描範圍> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<具有掃描範圍清單的檔案路徑>] [/F<A|C|E>] [/NEWONLY] [/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<“遮罩”>] [/ES:<大小>] [/ET:<秒數>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<天數>] [NORECALL]>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<工作記錄檔案的路徑>] [/ANSI] [/ALIAS:<工作別名>]

KAVSHELL SCAN 指令有必要和選用指令參數兩種（請參閱下表）。

KAVSHELL SCAN 指令範例

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

步驟 39. KAVSHELL SCAN 指令修飾符

機碼	敘述
掃描範圍。強制參數。	
<檔案> <資料夾> <網路路徑>	指定掃描範圍 - 檔案清單、資料夾、網路路徑及預先定義的區域。 以 UNC 格式（通用命名慣例）指定網路路徑。 在下列範例中，資料夾 Folder4 未指定路徑 - 它位於執行 KAVSHELL 指令的資料夾中： KAVSHELL SCAN Folder4 如果要檢查的物件名稱包含空格，則必須將其括在引號中。 選定某個資料夾後，Kaspersky Embedded Systems Security 2.2 也會檢查該資料夾的所有子資料夾。 可以使用符號 * 或 ？ 來掃描一組檔案。
/MEMORY	掃描 RAM 中的物件
/SHARED	掃描電腦上的共用資料夾
/STARTUP	掃描啟動物件
/REMDRIVES	掃描卸除式磁碟
/FIXDRIVES	掃描硬碟
/MYCOMP	掃描受防護電腦的所有區域
/L: <帶有掃描範圍清單的檔案路徑>	帶有掃描範圍清單的檔案名稱，包括檔案的完整路徑。 使用換行鍵界定檔案的掃描範圍。如下圖所示，您可指定預先定義的掃描範圍： C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
掃描的物件（檔案類型）。如果您未指定此指令參數值，Kaspersky Embedded Systems Security 2.2 將依據物件格式掃描物件。	
/FA	掃描所有物件
/FC	依據格式掃描物件（預設）。Kaspersky Embedded Systems Security 2.2 只掃描受感染的物件格式清單中所包含的格式物件。

機碼	敘述
/FE	依據副檔名掃描物件。Kaspersky Embedded Systems Security 2.2 只掃描受感染的物件副檔名清單中包含的副檔名物件。
/NEWONLY	僅掃描新增與變更過的檔案。 如果您未提供此指令參數，Kaspersky Embedded Systems Security 2.2 將掃描所有物件。
對受感染物件和其他物件執行的操作。如果未指定此指令參數，Kaspersky Embedded Systems Security 2.2 將執行“**略過**”操作。	
DISINFECT	解毒，如果無法解毒則略過
DISINFDEL	解毒，如果無法解毒則刪除
DELETE	刪除 在最新版本的 Kaspersky Embedded Systems Security 2.2 中保留了 DISINFECT 和 DELETE 設定，以便確保與以前版本的相容性。這兩個設定可以代替關鍵指令 /AI: 和 /AS: 在這種情況下，Kaspersky Embedded Systems Security 2.2 將不會處理疑似感染物件。
REPORT	傳送報告（預設）
AUTO	執行建議的操作
/AS: **對疑似感染物件執行的操作/** 如果未指定此指令參數，Kaspersky Embedded Systems Security 2.2 將執行“**略過**”操作。	
QUARANTINE	隔離
DELETE	刪除
REPORT	傳送報告（預設）
AUTO	執行建議的操作
排除	
/E:ABMSPO	排除以下複合檔案類型的指令參數： A – 壓縮檔案（僅掃描 SFX 壓縮檔案） B – 電子郵件資料庫 M – 一般郵件 S – 壓縮檔案和 SFX 壓縮檔案 P – 已封裝的物件 O – 嵌入 OLE 物件
/EM:<“遮罩”>	透過遮罩排除檔案 您可以指定數個遮罩，例如：EM:“*.txt; *.png; C\Videos*.avi”。
/ET:<秒數>	如果處理物件的速度比 <秒數> 值中所指定的秒數長，則停止處理物件。 預設沒有時間限制。

機碼	敘述
/ES:<大小>	不要掃描比 <大小> 值中所指定之大小 (MB) 還要大的複合物件。 預設情況下，Kaspersky Embedded Systems Security 2.2 掃描所有大小的物件。
/TZOFF	停用“信任區域”排除
進階設定（選項）	
/NOICHECKER	停用 iChecker（預設為啟用狀態）
/NOISWIFT	停用 iSwift（預設為啟用狀態）
/ANALYZERLEVEL:<分析等級>	啟用啟發式分析並配置分析等級。 以下啟發式分析等級可用： 1 – 輕度掃描 2 – 中度掃描 3 – 深度 如果刪除此指令參數，Kaspersky Embedded Systems Security 2.2 將不會使用啟發式分析。
/ALIAS:<工作別名>	此指令參數可讓您指定一個暫時的名稱給自訂掃描工作，工作執行期間需要用此名稱存取工作，例如，使用 TASK 指令檢視工作統計資料。在 Kaspersky Embedded Systems Security 2.2 的所有功能元件的工作別名中，每一個工作別名都必須是唯一的。 如果未指定此指令參數，將使用 scan_<kavshell_pid> 的暫時名稱，例如 scan_1234。在應用程式主控台中，為工作分配掃描物件的名稱（<日期和時間>），例如，掃描物件 8/16/2007 5:13:14 PM。
工作記錄的設定（報告設定）	
/W:<工作記錄檔案的路徑>	如果指定了此指令參數，Kaspersky Embedded Systems Security 2.2 將用該鍵的值定義的名稱儲存工作記錄檔案。 該記錄檔案包含工作執行統計資料、工作開啟及結束（停止）的時間，以及工作中相關事件資訊。 該記錄用於在“事件檢視器”中註冊由工作記錄和 Kaspersky Embedded Systems Security 2.2 事件記錄的設定定義的事件。 您可指定記錄檔案的絕對路徑或相對路徑。如果僅指定了檔案名稱但未指定其路徑，則記錄檔案將於目前所在的資料夾中建立。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔案。 執行工作時，可檢視此記錄檔案。 此記錄會出現在應用程式主控台的“工作記錄”節點中。 如果 Kaspersky Embedded Systems Security 2.2 無法建立記錄檔案，這將不會停止執行此指令，但會顯示一個錯誤訊息。
/ANSI	可以將事件以 ANSI 編碼記錄到工作執行記錄中的指令參數。 若未定義 W 指令參數，將無法套用 ANSI 指令參數。 如果未指定 ANSI 指令參數，將以 UNICODE 編碼產生工作記錄。

啟動“關鍵區域掃描”工作。KAVSHELL SCANCRITICAL

使用 KAVSHELL SCANCRITICAL 指令可使用在應用程式主控台中定義的設定啟動系統自訂掃描工作“關鍵區域掃描”。

KAVSHELL SCANCRITICAL 指令語法

KAVSHELL SCANCRITICAL [/W:<工作記錄檔案的路徑>]

KAVSHELL SCANCRITICAL 指令範例

要執行“關鍵區域掃描”自訂掃描工作，並在目前所在的資料夾中儲存 scancritical.log 工作執行記錄，請執行以下指令：

KAVSHELL SCANCRITICAL /W:scancritical.log

根據上面的 /W 指令語法，您可設定工作記錄的位置（請參閱下表）。

步驟 40. KAVSHELL SCANCRITICAL 指令的 /W 指令語法

機碼	敘述
/W:<工作記錄檔案的路徑>	如果指定了此指令參數，Kaspersky Embedded Systems Security 2.2 將用該鍵的值定義的名稱儲存工作記錄檔案。 該記錄檔案包含工作執行統計資料、工作開啟及結束（停止）的時間，以及工作中相關事件資訊。 該記錄用來註冊工作執行記錄設定與應用程式事件記錄所定義的事件。 您可指定記錄檔案的絕對路徑或相對路徑。如果僅指定了檔案名稱但未指定其路徑，則記錄檔案將於目前所在的資料夾中建立。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔案。 執行工作時，可檢視此記錄檔案。 此記錄會出現在應用程式主控台的“**工作記錄**”節點中。 如果 Kaspersky Embedded Systems Security 2.2 無法建立記錄檔案，這將不會停止執行此指令，但會顯示一個錯誤訊息。

以非同步模式管理指定的工作。KAVSHELL TASK

KAVSHELL TASK 指令可用來管理指定的工作，如執行、暫停、繼續和停止指定工作與檢視目前的工作狀態和統計資訊。此指令應在非同步模式下執行。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL TASK 指令語法

KAVSHELL TASK [<工作名稱別名> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]

KAVSHELL TASK 指令範例

KAVSHELL TASK

KAVSHELL TASK on- access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan- computer /STATE

KAVSHELL TASK 可以不搭配指令參數或搭配一或多個指令參數執行（請參閱下表）。

步驟 41. KAVSHELL TASK 指令修飾符

機碼	敘述
不搭配指令參數	回傳所有現有 Kaspersky Embedded Systems Security 2.2 工作的清單。該清單包含欄位：代替工作名稱、工作類別（系統或自訂）及目前工作狀態。
<工作別名>	除工作名稱外，SCAN TASK 指令中可另外使用 Kaspersky Embedded Systems Security 2.2 指定給工作的簡短工作別名。要檢視 Kaspersky Embedded Systems Security 2.2 工作別名，輸入 KAVSHELL TASK 但不必輸入任何指令參數
/START	以非同步模式開始指定的工作。
/STOP	停止指定的工作。
/PAUSE	暫停指定的工作。
/RESUME	以非同步模式繼續指定的工作。
/STATE	返回目前工作狀態（例如，**正在執行**、**已完成**、**已暫停**、**已停止**、**失敗**、**正在啟動**、**正在還原**）。
/STATISTICS	擷取工作統計資料 – 截至目前為止，從工作開始執行時的物件數資訊。

KAVSHELL TASK 指令的回傳代碼（請參見第 223 頁上的“KAVSHELL TASK 指令的回傳代碼”部分）。

啟動及停止即時防護工作。KAVSHELL RTP

KAVSHELL RTP 指令可用來啟動或停止所有的即時防護工作。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL RTP 指令語法

KAVSHELL RTP {/START | /STOP}

KAVSHELL RTP 指令範例

若要啟動所有即時防護工作，請執行以下指令：

KAVSHELL RTP /START

KAVSHELL RTP 指令可搭配兩個必要指令參數任意一個使用（請參閱下表）。

步驟 42. KAVSHELL RTP 指令參數

機碼	敘述
/START	停止所有即時防護工作：“ 即時檔案防護”和“ KSN 使用”。
/STOP	停止所有即時防護工作。

管理應用程式啟動控制工作 KAVSHELL APPCONTROL /CONFIG

可以使用 KAVSHELL APPCONTROL /CONFIG 指令來配置模式，在該模式中“應用程式啟動控制”工作將執行和監控 DLL 模組的載入。

KAVSHELL APPCONTROL /CONFIG 指令語法

/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<XML 檔案路徑>

KAVSHELL APPCONTROL /CONFIG 指令示例

► *要在“**活動**”模式中執行“應用程式啟動控制”工作而不載入 DLL 並在完成時儲存工作設定，請執行以下指令：*

KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml

可以使用命令列參數來配置“應用程式啟動控制”工作設定（請參閱以下表格）。

步驟 43. KAVSHELL APPCONTROL /GENERATE 指令開關

機碼	敘述
/mode:<applyrules|statistics>	“應用程式啟動控制”工作的執行模式。 您可以選擇以下模式之一： • 活動 – 套用“應用程式啟動控制”規則； • 統計資訊 – 僅統計。
/dll:<no|yes>	啟用或停用 DLL 載入監控。
/savetofile: <XML 檔案路徑>	匯出指定檔案中的指定規則為 XML 格式。
/savetofile: <xml 檔案全名>	將規則清單儲存到檔案。
/savetofile: <XML 檔案全名> /sdc	將軟體分發控制規則清單儲存到檔案。
/clearsdc	從清單中移除軟體分發控制規則。

應用程式啟動控制規則產生器 KAVSHELL APPCONTROL /GENERATE

使用 KAVSHELL APPCONTROL /GENERATE 指令，可以建立應用程式啟動控制規則清單。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL APPCONTROL /GENERATE 指令語法

KAVSHELL APPCONTROL /GENERATE <資料夾路徑> | /source:<包含資料夾清單的檔案路徑> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<使用者或使用者組>] [/export:<XML 檔案路徑>] [/import:<a|r|m>] [/ prefix:<規則名稱首碼>] [/unique]

KAVSHELL APPCONTROL /GENERATE 指令示例

► *若要為指定資料夾中的檔產生規則，請執行以指令：*

KAVSHELL APPCONTROL/GENERATE /source:c\folderslist.txt /export:c:\rules\appctrlrules.xml

► *若要為指定資料夾中所有副檔名的可執行檔產生規則，並在工作完成時，將建立的規則儲存在指定的 XML 檔案中，請執行以下指令：*

KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml

根據鍵語法的不同，您可以為“應用程式啟動控制”工作配置自動規則建立設定（請參見下表）。

步驟 44. KAVSHELL APPCONTROL /GENERATE 指令鍵

機碼	敘述
允許規則使用範圍	
<資料夾路徑>	指定包含可執行檔的資料夾路徑，這些可執行檔需要自動建立的允許規則。
/source: <包含資料夾清單的檔案路徑>	指定包含資料夾清單的 TXT 檔案的路徑，這些資料夾包含需要自動建立的允許規則的可執行檔。
/masks: <edms>	指定包含可執行檔的副檔名，這些可執行檔需要自動建立的允許規則。 您可以將以下副檔名的規則使用範圍檔案包括在內： • e - EXE 檔案 • d - DLL 檔案 • m - MSI 檔案 • s - 指令碼
/runapp	產生允許規則時，應考慮在執行工作的那一刻在受防護電腦上執行的應用程式。
自動建立允許規則時的操作	
/rules: <ch|cp|h>	指定在“應用程式啟動控制”允許規則建立期間要執行的操作： • ch - 使用數位憑證。如果憑證遺失，請使用 SHA256 雜湊。 • cp - 使用數位憑證。如果憑證遺失，請使用可執行檔路徑。 • h - 使用 SHA256 雜湊。

機碼	敘述
/strong	在自動建立“應用程式啟動控制”允許規則時使用數位憑證主旨和指紋。如果指定 /rules: <ch|cp> 鍵，則執行該指令。
/user: <使用者或使用者群組>	指定將套用規則的使用者名或一群組使用者。應用程式將監控透過指定的使用者和/或使用者群組執行的任何應用程式。
應用程式啟動控制規則產生器完成後的操作	
/export: <XML 檔案路徑>	將建立的規則儲存到 XML 檔案中。
/unique	新增安裝有應用程式的電腦的相關資訊，這些資訊是建立應用程式啟動控制允許規則時的依據。
/prefix：<規則名稱的前置詞>	指定用於建立應用程式啟動控制允許規則的名稱首碼。
/import: <a|r|m>	根據選定的新增規則，將建立的規則匯入指定的應用程式啟動控制規則清單中。： • a - **新增到現有規則**（將複製具有相同設定的規則） • r - **取代現有規則**（不新增具有相同參數的規則；如果至少一個規則參數是唯一的，則會新增規則） • m - **與現有規則合併**（不新增具有相同參數的規則；如果至少一個規則參數是唯一的，則會新增規則）

填寫應用程式啟動控制規則清單 KAVSHELL APPCONTROL

使用 KAVSHELL APPCONTROL，您可根據所選原則將規則從 XML 檔新增到應用程式啟動控制工作規則清單，也可以從清單中刪除所有設定的規則。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL APPCONTROL 指令語法

KAVSHELL APPCONTROL /append <XML 檔案路徑> | /replace <XML 檔案路徑> | /merge <XML 檔案路徑> | /clear

KAVSHELL APPCONTROL 指令示例

► *若要根據“新增到現有規則”政策，從 XML 檔案向已經指定的應用程式啟動控制工作規則新增規則，請執行以下指令：*

KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml

根據鍵值語法，您可以選擇從指定的 XML 檔案向應用程式啟動控制定義的規則清單新增新規則的原則（請參見下表）。

步驟 45. KAVSHELL SCAN 指令鍵

機碼	敘述
/append <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。新增原則 - **新增到現有規則**（將複製具有相同設定的規則）。
/replace <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。新增原則 - **取代現有規則**(不新增具有相同參數的規則 :如果至少一個規則參數是唯一的, 則會新增規則)。
/merge <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。新增原則 - **與現有規則合併**（新規則不會複製已設定的規則）。
/clear	填寫應用程式啟動控制規則清單。

填寫裝置控制規則清單。KAVSHELL DEVCONTROL

使用 KAVSHELL DEVCONTROL，您可根據所選原則將規則從 XML 檔新增到裝置控制工作規則清單，也可以從清單中刪除所有設定的規則。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL DEVCONTROL 指令語法

KAVSHELL DEVCONTROL /append <XML 檔案路徑> | /replace <XML 檔案路徑> | /merge <XML 檔案路徑> | /clear

KAVSHELL DEVCONTROL 指令示例

► *若要根據“**新增到現有規則**”原則，從 XML 檔向已經指定的裝置控制工作規則新增規則，請執行以下指令：*

KAVSHELL DEVCONTROL /append c:\rules\devctrlrules.xml

根據鍵值語法，您可以選擇從指定的 XML 檔案向裝置控制定義的規則清單新增新規則的原則（請參見下表）。

步驟 46. KAVSHELL DEVCONTROL 指令參數

機碼	敘述
/append <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。新增原則 - **新增到現有規則**（將複製具有相同設定的規則）。
/replace <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。新增原則 - **取代現有規則**（不新增具有相同參數的規則；如果至少一個規則參數是唯一的，則會新增規則）。
/merge <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。新增原則 - **與現有規則合併**（新規則不會複製已設定的規則）。
/clear	清除裝置控制規則清單。

啟用 Kaspersky Embedded Systems Security 2.2 資料庫更新工作。KAVSHELL UPDATE

KAVSHELL UPDATE 指令可以用於按非同步模式啟動 Kaspersky Embedded Systems Security 2.2 資料庫更新工作。

使用 KAVSHELL UPDATE 指令執行的 Kaspersky Embedded Systems Security 2.2 資料庫更新工作是臨時工作。它僅在執行時顯示在應用程式主控台中。同一時間，會產生工作記錄。它會顯示在應用程式主控台的“**工作記錄**”中。卡巴斯基安全管理中心政策可套用到使用 KAVSHELL UPDATE 指令所建立與啟動的更新工作，以及病毒防護應用程式主控台中所建立的更新工作。有關使用卡巴斯基安全管理中心管理電腦上的 Kaspersky Embedded Systems Security 2.2 的資訊，請參見“使用卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security 2.2”部分。

在此工作中指定更新來源路徑時，可設定環境變數。如果使用了使用者的環境變數，請使用該使用者的權限執行 KAVSHELL UPDATE 指令。

KAVSHELL UPDATE 指令語法

KAVSHELL UPDATE <更新來源路徑 | /AK | /KL> [/NOUSEKL] [/PROXY:<位址>:<連接埠>] [/AUTHTYPE:<0- 2>] [/PROXYUSER:<使用者名稱>] [/PROXYPWD:<密碼>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/TIMEOUT:<秒>] [/REG:<iso3166 程式碼>] [/W:<工作記錄檔案路徑>] [/ALIAS:<工作別名>]

KAVSHELL UPDATE 指令有必要和選用指令參數兩種（請參閱下表）。

KAVSHELL UPDATE 指令範例

► *要啟動自訂的資料庫更新工作，請執行以下指令：*

KAVSHELL UPDATE

► *要使用 \\server\databases 網路資料夾中的更新檔案啟動資料庫更新工作，請執行以下指令：*

KAVSHELL UPDATE \\server\databases

► *若要從 FTP 伺服器 ftp://dnl-ru1.kaspersky-labs.com/ 啟動更新工作並將所有工作事件寫入到 c:\update_report.log 檔案，請執行以下指令：*

KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log

► *要從 Kaspersky Lab 的更新伺服器下載 Kaspersky Embedded Systems Security 2.2 資料庫更新檔案，請透過代理伺服器（代理伺服器位址：proxy.company.com，連接埠 8080）連線更新來源，若要使用內建的 Microsoft Windows NTLM 身分驗證（使用者名稱：Inetuser，密碼：123456）存取電腦，請執行以下指令：*

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

步驟 47. KAVSHELL UPDATE 指令參數

機碼	敘述
更新來源（強制參數）。指定一或多個來源。Kaspersky Embedded Systems Security 2.2 將按照更新來源的清單循序存取更新來源。使用空白鍵界定來源。	
<UNC 格式中的路徑>	使用者定義的更新來源。UNC 格式中的網路更新資料夾路徑。
<URL>	使用者定義的更新來源。更新資料夾所在的 HTTP 或 FTP 伺服器位址。
<本機資料夾>	使用者定義的更新來源。受防護電腦上的資料夾。
/AK	使用卡巴斯基安全管理中心管理伺服器作為更新來源。
/KL	使用 Kaspersky Lab 的更新伺服器作為更新來源。
/NOUSEKL	如果不能使用其他更新來源（預設使用），就不使用 Kaspersky Lab 的更新伺服器。
代理伺服器設定	
/PROXY:<位址>:<連接埠>	代理伺服器的網路名稱或 IP 位址及連接埠。如果未指定該鍵，Kaspersky Embedded Systems Security 2.2 將自動偵測區域網路中使用的代理伺服器設定。
/AUTHTYPE:<0-2>	此指令參數可指定存取代理伺服器的驗證方法。它可能呈現是以下設定值： **0** – 內建的 Microsoft Windows NTLM 身分驗證；Kaspersky Embedded Systems Security 2.2 將與**本機系統** (**SYSTEM**) 帳戶下的代理伺服器聯絡 **1** – 內建的 Microsoft Windows NTLM 身分驗證；Kaspersky Embedded Systems Security 2.2 將與其登入名稱和密碼分別由鍵 /PROXYUSER 和 /PROXYPWD 指定的帳戶下的代理伺服器聯絡 **2** – 透過 /PROXYUSER 和 /PROXYPWD 指令參數指定的登入名稱和密碼進行身分驗證（基本驗證） 如果存取代理伺服器不需要驗證，就不需要指定指令參數。
/PROXYUSER:<使用者名稱>	存取代理伺服器所需的使用者名稱。如果指定了 /AUTHTYPE:0 指令參數值，將忽略 /PROXYUSER:<使用者名稱> 和 /PROXYPWD:<密碼> 指令參數。
/PROXYPWD:<密碼>	存取代理伺服器所需的使用者密碼。如果指定了 /AUTHTYPE:0 指令參數值，將忽略 /PROXYUSER:<使用者名稱> 和 /PROXYPWD:<密碼> 指令參數。如果指定了 /PROXYUSER 指令參數但刪除了 /PROXYPWD，將視密碼為空白值。
/NOPROXYFORKL	不使用代理伺服器設定連線 Kaspersky Lab 的更新伺服器（預設為使用）。
/USEPROXYFORCUSTOM	使用代理伺服器設定連線使用者定義的更新來源（預設為不使用）。
/USEPROXYFORLOCAL	使用代理伺服器連線本機更新來源。如果不指定，將套用**對於本機位址不使用代理伺服器**。
FTP 和 HTTP 伺服器一般設定	
/NOFTPPASSIVE	如果指定了指令參數，Kaspersky Embedded Systems Security 2.2 將使用主動 FTP 伺服器模式連線至受防護電腦。如果未指定指令參數，Kaspersky Embedded Systems Security 2.2 將使用被動 FTP 伺服器模式（如果可能的話）。

機碼	敘述
/TIMEOUT:<秒數>	FTP 或 HTTP 伺服器連線逾時。如果不指定此鍵，Kaspersky Embedded Systems Security 2.2 將使用預設值：10 秒。鍵值必須是整數。
/REG:<iso3166 代碼>	區域設定。從 Kaspersky Lab 的更新伺服器接收更新時需使用此指令參數。Kaspersky Embedded Systems Security 2.2 透過選擇距其所在位置最近的更新伺服器來最佳化受防護電腦上的更新載入過程。 對於此指令參數值，請根據 ISO 3166- 1 標準替受防護的電腦指定所在國家/地區的字母程式碼，例如 /REG: gr 或 /REG:RU。如果省略該鍵或指定不存在的國家/地區代碼，Kaspersky Embedded Systems Security 2.2 將會基於安裝應用程式主控台的電腦上的地區設定偵測受防護電腦的位置。
/ALIAS:<工作別名>	此指令可讓您為工作指派一個暫時名稱，以在工作執行期間用來存取該工作。例如，您可使用 TASK 指令檢視工作統計資料。在 Kaspersky Embedded Systems Security 2.2 的所有功能元件的工作別名中，每一個工作別名都必須是唯一的。 如果未指定 update_<kavshell_pid> 指令參數，將使用 update_1234。在應用程式主控台中自動指派工作的更新資料庫（<日期 時間>），例如更新資料庫 2007/8/16 下午 5:41:02。
/W:<工作記錄檔案的路徑>	如果指定了此指令參數，Kaspersky Embedded Systems Security 2.2 將用該鍵的值定義的名稱儲存工作記錄檔案。 該記錄檔案包含工作執行統計資料、工作開啟及結束（停止）的時間，以及工作中相關事件資訊。 該記錄用於在“事件檢視器”中註冊由工作記錄和 Kaspersky Embedded Systems Security 2.2 事件記錄的設定定義的事件。 您可指定記錄檔案的絕對路徑或相對路徑。如果僅指定檔案名稱但未指定其路徑，則記錄檔案將於目前所在的資料夾中建立。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔案。 執行工作時，可檢視此記錄檔案。 此記錄會出現在應用程式主控台的“**工作記錄**”節點中。 如果 Kaspersky Embedded Systems Security 2.2 無法建立記錄檔案，這將不能停止執行此指令或顯示一個錯誤訊息。

KAVSHELL UPDATE 指令回傳代碼（請參閱第 224 頁）。

回溯 Kaspersky Embedded Systems Security 2.2 資料庫更新。KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 指令可用來執行 Kaspersky Embedded Systems Security 2.2 資料庫回溯系統工作（將 Kaspersky Embedded Systems Security 2.2 資料庫回溯至上一個安裝版）。此指令會同步執行。

指令語法：

KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 指令回傳代碼（請參閱第 225 頁）。

管理記錄審查。KAVSHELL TASK LOG-INSPECTOR

KAVSHELL TASK LOG-INSPECTOR 指令可用於根據 Windows 事件記錄分析來監控環境完整性。

指令語法

KAVSHELL TASK LOG-INSPECTOR

指令範例

KAVSHELL TASK LOG-INSPECTOR /stop

步驟 48. KAVSHELL TASK LOG-INSPECTOR 指令修飾符

機碼	敘述
/START	以非同步模式開始指定的工作。
/STOP	停止指定的工作。
/STATE	返回目前工作狀態（例如，*正在執行*、*已完成*、*已暫停*、*已停止*、*失敗*、*正在啟動*、*正在還原*）。
/STATISTICS	擷取工作統計資料 – 截至目前為止，從工作開始執行時的物件數資訊。

KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼（請參見第 223 頁上的“ KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼”部分）。

啟動應用程式 KAVSHELL LICENSE

可使用 KAVSHELL LICENSE 指令管理 Kaspersky Embedded Systems Security 2.2 金鑰和啟動碼。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL FULLSCAN 指令語法

KAVSHELL LICENSE [/ADD:<金鑰檔案 | 啟動碼>[/R]| /DEL:<金鑰 | 啟動碼編號>]

KAVSHELL SCAN 指令範例

► *要啟動應用程式，請執行以下指令：*

KAVSHELL.EXE LICENSE / ADD: <啟動碼或金鑰>

► *若要檢視有關新增金鑰檔案的資訊，請執行以下指令：*

KAVSHELL LICENSE

► *要移除安裝序號 0000- 000000- 00000001 的產品授權檔案，請執行以下指令：*

KAVSHELL LICENSE /DEL:0000- 000000- 00000001
KAVSHELL LICENSE 指令可搭配指令參數或不搭配指令參數執行（請參閱下表）。

步驟 49. KAVSHELL LICENSE 指令參數

機碼	敘述
不搭配指令參數	該指令會回傳以下相關的安裝產品授權資訊： • 金鑰。 • 產品授權類型（正式版）。 • 與金鑰檔案相關聯的產品授權的有效期限。 • 產品授權檔案狀態（啟動或備用）。如果將此值指定為 *，此金鑰會安裝為備用金鑰。
/ADD:<金鑰檔案名稱或啟動碼>	透過指定的檔案或啟動碼安裝金鑰。 指定金鑰路徑時可以使用系統環境變數；不允許使用者環境變數。
/R	/R 啟動碼或金鑰檔案為 /ADD 啟動碼或金鑰檔案的備用啟動碼或金鑰檔案，代表所安裝的啟動碼或金鑰檔案為備用啟動碼或金鑰檔案。
/DEL:<金鑰或啟動碼>	刪除具有指定編號或選定啟動碼的金鑰檔案。

KAVSHELL LICENSE 指令的回傳代碼（請參見第 225 頁上的“KAVSHELL LICENSE 指令的回傳代碼”部分）。

啟用、設定和停用偵錯記錄。KAVSHELL TRACE

KAVSHELL TRACE 指令可用於為所有 Kaspersky Embedded Systems Security 2.2 子系統啟用和停用跟蹤記錄，以及設定記錄詳細等級。

Kaspersky Embedded Systems Security 2.2 會以未加密的形式將資訊寫入到偵錯檔案和傾印檔案。

KAVSHELL TRACE 指令語法

KAVSHELL TRACE </ON /F:< 偵錯記錄檔案資料夾路徑> [/S:< 記錄大小上限 (MB)>] [/LVL:debug|info|warning|error|critical] | /OFF>

如果您保留了偵錯記錄並想變更它的設定，請輸入 KAVSHELL TRACE 與 /ON 指令參數，並以 /S 和 /LVL 指令參數值指定記錄設定（請參閱下表）。

步驟 50. KAVSHELL TRACE 指令參數

機碼	敘述
/ON	啟用偵錯記錄。
/F:<偵錯記錄的檔案資料夾>	此指令用來指定儲存偵錯記錄檔案的資料夾完整路徑。 如果指定的資料夾路徑不存在，將不會建立偵錯記錄。可使用 UNC（通用命名慣例）格式的網路路徑，但無法指定受防護電腦上網路磁碟機的資料夾路徑。 如果指令參數值指定的資料夾路徑名稱帶有空白字元，此資料夾路徑前後請加上引號，例如：/F:"C\Trace Folder"。 指定偵錯檔案路徑時可以使用系統環境變數；不允許使用者環境變數。
/S: <記錄檔案大小上限 (MB)>	此指令可設定一個偵錯記錄檔案的大小上限。一旦記錄檔案大小達到上限時，Kaspersky Embedded Systems Security 2.2 會將資訊記錄到新檔案中；之前的記錄檔案會被儲存。 如果未指定此指令參數值，一個記錄檔案的大小上限為 50 MB。
/LVL:debug|info|warning|error|critical	該鍵從最大（**所有診斷資訊**）（所有事件都會記錄到記錄中）到最小（**緊急事件**）（僅記錄緊急事件）設定記錄詳細資訊等級。 如果未指定此指令鍵，偵錯記錄中將記錄詳細程度為**所有診斷資訊**的事件。
/OFF	此指令可停用偵錯記錄。

KAVSHELL TRACE 指令範例

► *要使用“**所有診斷資訊**”詳細程度及上限為 200 MB 的記錄檔案大小來啟用偵錯記錄，並將記錄檔案儲存到 C:\Trace Folder 資料夾，請執行以下指令：*

KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200

► *要使用“**重要事件**”詳細程度啟用偵錯記錄，並將記錄檔案儲存到 C:\Trace Folder 資料夾，請執行以下指令：*

KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning

► *要停用偵錯記錄，請執行以下指令：*

KAVSHELL TRACE /OFF

KAVSHELL TRACE 指令的回傳代碼（請參見第 226 頁上的“KAVSHELL TRACE 指令的回傳代碼”部分）。

Kaspersky Embedded Systems Security 2.2 記錄檔案磁碟重組。KAVSHELL VACUUM

使用 KAVSHELL VACUUM 指令，您可以對應用程式記錄檔案進行磁碟整理。這樣可以避免系統錯誤或者在 Kaspersky Embedded Systems Security 2.2 連線到記錄儲存時出現的錯誤。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

建議您應用 KAVSHELL VACUUM 指令，以便在自訂掃描頻繁掃描和更新工作頻繁啟動時優化記錄檔案儲存。在執行該指令時，Kaspersky Embedded Systems Security 2.2 將透過指定的路徑更新受防護電腦上儲存的應用程式記錄檔案的邏輯結構。

預設情況下，應用程式記錄檔案儲存在 C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\2.2\Reports。如果您手動為記錄儲存指定了另一個路徑，KAVSHELL VACUUM 指令將對 Kaspersky Embedded Systems Security 2.2 記錄設定中指定的資料夾中的檔案執行磁碟整理。

對較大的檔案進行磁碟整理會增加 KAVSHELL VACUUM 指令的執行時間。

在執行 KAVSHELL VACUUM 指令期間，將無法執行即時防護和電腦控制工作。持續磁碟整理過程會限制對 Kaspersky Embedded Systems Security 2.2 記錄的存取並拒絕事件記錄。為了避免降低安全等級，建議您提前將 KAVSHELL VACUUM 指令安排在停機時執行。

► *若要對 Kaspersky Embedded Systems Security 2.2 記錄檔案進行磁碟整理，請執行以下指令：*

KAVSHELL VACUUM

如果以本機管理員帳戶權限啟動，則可執行指令。

清除 iSwift 庫。KAVSHELL FBRESET

Kaspersky Embedded Systems Security 2.2 使用的 iSwift 技術可避免應用程式重新掃描上次掃描後未修改的檔案（請參閱**使用 iSwift 技術**）。

Kaspersky Embedded Systems Security 2.2 會在 %SYSTEMDRIVE%\System Volume Information 目錄建立 klamfb.dat 和 klamfb2.dat 檔案，該檔案含有已掃描過的乾淨物件資訊。檔案 klamfb.dat (klamfb2.dat) 隨著 Kaspersky Embedded Systems Security 2.2 掃描的檔案數目的增加而增大。該檔案僅包含有關系統中存在的檔案的目前資訊：如果刪除一個檔案，Kaspersky Embedded Systems Security 2.2 將從 klamfb.dat 清除相關資訊。

要清除某個檔案，請使用指令 KAVSHELL FBRESET。

操作 KAVSHELL FBRESET 指令時請注意以下細節：

- 在 KAVSHELL FBRESET 指令後清除 klamfb.dat 檔案的話，Kaspersky Embedded Systems Security 2.2 不會停用防護（與手動刪除 klamfb.dat 的情況不同）。
- 在 klamfb.dat 中清除資料後，Kaspersky Embedded Systems Security 2.2 可能會增加電腦工作負載。在這種情況下，病毒防護將掃描在清除 klamfb.dat 後第一次存取的所有檔案。掃描 Kaspersky Embedded Systems Security 2.2 後，每一個掃描物件的資訊會再次新增到 klamfb.dat 中。在嘗試存取新物件的情況下，iSwift 技術將避免重新掃描未經變更的檔案。

只有在 SYSTEM 帳戶下啟動命令列時，才能執行 KAVSHELL FBRESET 指令。

啟用和停用建立傾印檔案。KAVSHELL DUMP

您可使用 KAVSHELL DUMP，在 Kaspersky Embedded Systems Security 2.2 處理程序不正常終止的清況下啟用或停用建立記憶體快照（傾印檔案）（請參見下表）。您可隨時替正在處理的 Kaspersky Embedded Systems Security 2.2 處理程序拍攝快照。

為了能夠成功建立傾印檔案，必須在本機系統帳戶 (SYSTEM) 下執行 KAVSHELL DUMP 指令。

KAVSHELL DUMP 指令語法

KAVSHELL DUMP </ON /F:<傾印檔案的資料夾>|/SNAPSHOT /F:<傾印檔案的資料夾> / P:<pid> | /OFF>

KAVSHELL DUMP 指令範例

► *要啟用建立傾印檔案的功能，並將傾印檔案儲存到 C:\Dump Folder 資料夾，請執行以下指令：*

KAVSHELL DUMP /ON /F:”C:\Dump Folder”

► *要使用 ID 1234 將處理程序的傾印檔案儲存到 C:/Dumps 資料夾，請執行以下指令：*

KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234

► *要停用產生傾印檔案的功能，請執行以下指令：*

KAVSHELL DUMP /OFF

步驟 51. KAVSHELL DUMP 指令參數

機碼	敘述
/ON	在不正常終止的情況下，啟用建立處理程序記憶體傾印檔案功能。
/F:<傾印檔案的資料夾路徑>	此指令參數為必要的設定值。它可指定要儲存傾印檔案的資料夾路徑。如果指定的資料夾路徑不存在，將不會建立傾印檔案。可使用 UNC（通用命名慣例）格式的網路路徑，但無法指定受防護電腦上網路磁碟機的資料夾路徑。 在指定包含記憶體傾印檔案的資料夾的路徑時，可以使用系統環境變數；不允許使用使用者環境變數。
/SNAPSHOT	替進行中的特定 Kaspersky Embedded Systems Security 2.2 處理程序拍攝記憶體快照，並將傾印檔案儲存到 /F 指令參數所指定的資料夾路徑中。
/P	Microsoft Windows 工作管理員中會顯示 PID 處理程序識別碼。
/OFF	在不正常終止的情況下，停用建立處理程序的記憶體傾印檔案功能。

KAVSHELL DUMP 指令的回傳代碼（請參閱第 226 頁上的“KAVSHELL DUMP 指令的回傳代碼”部分）。

匯入設定。KAVSHELL IMPORT

您可使用 KAVSHELL IMPORT 指令來匯入受防護電腦上的 Kaspersky Embedded Systems Security 2.2 設定、功能及 Kaspersky Embedded Systems Security 2.2 設定檔及實例等工作。您可使用 KAVSHELL EXPORT 指令建立設定檔。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL IMPORT 指令語法

KAVSHELL IMPORT <設定檔名稱及檔案路徑>

KAVSHELL IMPORT 指令範例

KAVSHELL IMPORT Host1.xml

步驟 52. KAVSHELL IMPORT 指令參數

機碼	敘述
<設定檔名稱及檔案路徑>	設定檔名稱可當作匯入設定來源使用。 指定檔案路徑時可以使用系統環境變數；不允許使用者環境變數。

KAVSHELL IMPORT 指令的回傳代碼（請參閱第 227 頁上的“KAVSHELL IMPORT 指令的回傳代碼”部分）。

匯出設定。KAVSHELL EXPORT

KAVSHELL EXPORT 指令可用來匯出 Kaspersky Embedded Systems Security 2.2 及其現有工作所有的設定，以便之後將設定匯入其他電腦所安裝的 Kaspersky Embedded Systems Security 2.2 實例中（參閱下表）。

KAVSHELL EXPORT 指令語法

KAVSHELL EXPORT <設定檔名稱及檔案路徑>

KAVSHELL EXPORT 指令範例

KAVSHELL EXPORT Host1.xml

步驟 53. KAVSHELL EXPORT 指令參數

機碼	敘述
<設定檔名稱及檔案路徑>	包含設定的設定檔名稱。 設定檔可指派任何副檔名。 指定檔案路徑時可以使用系統環境變數；不允許使用者環境變數。

KAVSHELL EXPORT 指令的回傳代碼（請參閱第 227 頁上的“KAVSHELL EXPORT 指令的回傳代碼”部分）。

與 Microsoft Operations Management Suite 整合。KAVSHELL OMSINFO

使用 KAVSHELL OMSINFO 指令可檢視應用程式的狀態以及病毒資料庫和 KSN 服務偵測到的威脅的相關資訊。關於威脅的資料取自可用的事件記錄。

KAVSHELL OMSINFO 指令語法

KAVSHELL OMSINFO <生成的檔案的完整路徑與檔案名稱>

KAVSHELL OMSINFO 指令範例

KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json

步驟 54. KAVSHELL OMSINFO 指令參數

機碼	敘述
<生成的檔案的路徑與檔案名稱>	生成的檔案的名稱，該檔案將包含應用程式狀態和偵測到的威脅的相關資訊。

命令列回傳代碼

本章節說明項目

KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼

步驟 55. KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-3	權限錯誤
-5	指令語法無效
-6	無效的操作（例如 Kaspersky Embedded Systems Security 2.2 正執行中或已停止執行）
-7	服務未註冊
-8	已停用自動服務啟動。
-9	試圖從另一個失效的使用者帳戶啟動電腦失敗（依預設 Kaspersky Embedded Systems Security 2.2 會從本機系統使用者帳戶執行服務）
-99	未知錯誤

KAVSHELL SCAN 和 KAVSHELL SCANCRITICAL 指令的回傳代碼

步驟 56. KAVSHELL SCAN 和 KAVSHELL SCANCRITICAL 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成（未偵測到威脅）
1	操作已取消
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到含有掃描區域清單的檔案）
-5	指令語法無效或未定義掃描區域
-80	偵測到受感染物件和其他物件
-81	偵測到疑似感染物件
-82	偵測到處理程序錯誤
-83	找到未掃描的物件
-84	偵測到已損毀物件
-85	建立工作執行記錄失敗
-99	未知錯誤
-301	金鑰無效

KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼

步驟 57. KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-6	無效的操作（例如 Kaspersky Embedded Systems Security 2.2 正執行中或已停止執行）
402	工作執行中（適用指令 /STATE）

KAVSHELL TASK 指令的回傳代碼

步驟 58. KAVSHELL TASK 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤

回傳代碼	敘述
-4	找不到物件（找不到工作項目）
-5	指令語法無效
-6	操作無效（例如，工作未執行、工作執行中或無法暫停）
-99	未知錯誤
-301	金鑰無效
401	工作未執行（適用指令 /STATE）
402	工作執行中（適用指令 /STATE）
403	工作已暫停（適用指令 /STATE）
-404	操作執行錯誤（工作狀態改變導至失敗）

KAVSHELL RTP 指令的回傳代碼

步驟 59. KAVSHELL RTP 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到其中一個即時防護工作或全部的即時防護工作）
-5	指令語法無效
-6	操作無效（例如，工作已執行中或已停止工作）
-99	未知錯誤
-301	金鑰無效

KAVSHELL UPDATE 指令的回傳代碼

步驟 60. KAVSHELL UPDATE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
200	所有物件都是最新的（資料庫或程式元件為最新的）
-2	未執行服務
-3	權限錯誤
-5	指令語法無效

回傳代碼	敘述
-99	未知錯誤
-206	指定來源中的更新檔案遺失或檔案格式不明
-209	連線更新來源錯誤
-232	連線代理伺服器時驗證錯誤
-234	連線安全管理中心時發生錯誤
-235	Kaspersky Embedded Systems Security 2.2 在連線到更新來源時未透過身分驗證
-236	應用程式資料庫已損壞
-301	金鑰無效

KAVSHELL ROLLBACK 指令的回傳代碼

步驟 61. KAVSHELL ROLLBACK 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-99	未知錯誤
-221	找不到資料庫備份副本或資料庫已損毀
-222	資料庫備份副本已損毀

KAVSHELL LICENSE 指令的回傳代碼

步驟 62. KAVSHELL LICENSE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限不足無法管理金鑰
-4	找不到指定的金鑰序號
-5	指令語法無效
-6	操作無效（已安裝金鑰）
-99	未知錯誤

回傳代碼	敘述
-301	金鑰無效
-303	授權適用於其他程式

KAVSHELL TRACE 指令的回傳代碼

步驟 63. KAVSHELL TRACE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到偵錯記錄資料夾的指定路徑）
-5	指令語法無效
-6	操作無效（如果已停用偵錯記錄建立功能，試圖執行 KAVSHELL TRACE /OFF 指令）
-99	未知錯誤

KAVSHELL FBRESET 指令的回傳代碼

步驟 64. KAVSHELL FBRESET 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-99	未知錯誤

KAVSHELL DUMP 指令的回傳代碼

步驟 65. KAVSHELL DUMP 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到傾印檔案資料夾的指定路徑；找不到含有指定 PID 的處理程序）

回傳代碼	敘述
-5	指令語法無效
-6	操作無效（如果已停用傾印檔案建立功能，試圖執行 KAVSHELL DUMP/OFF 指令）
-99	未知錯誤

KAVSHELL IMPORT 指令的回傳代碼

步驟 66. KAVSHELL IMPORT 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到匯入設定檔）
-5	無效的語法
-99	未知錯誤
501	操作順利完成，但是執行指令期間出現錯誤 / 備註，例如 Kaspersky Embedded Systems Security 2.2 未匯入某些功能元件的設定
-502	遺失匯入檔案或無法辨識匯入檔案格式
-503	不相容的設定（設定檔從不同的程式或新版或不相容的 Kaspersky Embedded Systems Security 2.2 匯出）

KAVSHELL EXPORT 指令的回傳代碼

步驟 67. KAVSHELL EXPORT 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-5	無效的語法
-10	無法建立設定檔（例如，無法存取檔案路徑中所指定的資料夾）
-99	未知錯誤
501	操作順利完成，但是執行指令期間出現錯誤/備註，例如 Kaspersky Embedded Systems Security 2.2 未匯出某些功能元件的設定

與協力廠商系統整合

本節介紹 Kaspersky Embedded Systems Security 2.2 與協力廠商功能和技術的整合。

本章內容

監控效能。Kaspersky Embedded Systems Security 2.2 計數器

本章節提供有關 Kaspersky Embedded Systems Security 2.2 的統計資訊：系統監控效能計數器以及 SNMP 計數器和 TRAP。

本章內容

系統監視器的效能計數器

本節包含有關安裝期間由 Kaspersky Embedded Systems Security 2.2 在 Microsoft Windows 系統監視器中註冊的效能計數器的資訊。

本章節說明項目

關於 Kaspersky Embedded Systems Security 2.2 SNMP 計數器

預設情況下，“**效能計數器**”元件包含在 Kaspersky Embedded Systems Security 2.2 的已安裝元件中。Kaspersky Embedded Systems Security 2.2 在安裝期間在 Microsoft Windows 系統監視器中註冊其自己的效能計數器。

使用 Kaspersky Embedded Systems Security 2.2 計數器，您可用於監視執行即時防護工作時應用程式的效能。搭配其他應用程式共同執行時，可能會發生空間不足或資源短缺。您可能會診斷出不需要的 Kaspersky Embedded Systems Security 2.2 設定與作業當機。

透過在 Windows 主控台的“**管理**”項目中開啟“**效能**”主控台，來檢視 Kaspersky Embedded Systems Security 2.2 效能計數器。

下列章節列出了計數器定義、獲取讀數的建議時間間隔、上限值以及在計數器值超過 Kaspersky Embedded Systems Security 2.2 設定時的建議。

拒絕需求總數

步驟 68. 拒絕需求總數

名稱	拒絕需求總數
定義	來自檔案攔截驅動程式但未被應用程式處理序接受的物件處理請求總數；從 Kaspersky Embedded Systems Security 2.2 上次啟動時開始計數。 程式會略過物件，要求處理 Kaspersky Embedded Systems Security 2.2 處理程序拒絕的要求。
用途	此計數器可讓您偵測： • 因為 Kaspersky Embedded Systems Security 2.2 的工作程序滿載，造成即時防護品質降低。 • 因檔案截取調度程式失敗，造成即時防護中斷。
標準值/上限值	0/1。
建議的讀取間隔時間	1 小時。
如果值超過上限值時的設定建議	遭拒的處理要求數等於略過的物件數。 視計數器的行為而定，可能會發生以下情況： • 計數器在較長的時間段內顯示了許多被拒絕的請求：由於完全載入了所有 Kaspersky Embedded Systems Security 2.2 處理程序，Kaspersky Embedded Systems Security 2.2 無法掃描物件。 若要避免略過物件，請增加用於完成即時防護工作的應用程式處理序的數量。您可以使用“**最大活動程序數**”和“**用於即時防護的程序數**”等 Kaspersky Embedded Systems Security 2.2 設定。 • 要求遭拒數明顯超過上限值，且還在快速成長中：檔案截取調度程式已失效。Kaspersky Embedded Systems Security 2.2 未在存取物件時對其進行掃描。 重新啟動 Kaspersky Embedded Systems Security 2.2。

略過需求總數

步驟 69. 略過需求總數

名稱	略過請求總數
定義	來自檔案攔截驅動程式且由 Kaspersky Embedded Systems Security 2.2 收到但未產生處理完成事件的物件處理請求總數；從應用程式上次啟動時開始計數。 如果有其中一種工作程序接受物件程序要求，但並未傳送處理完程式事件，則驅動程式會將要求傳遞至其他程序，而計數器“**要求略過總數**”的值會加 1。如果驅動程序已進行過所有工作程序，且無任何程序接受過處理的要求（因為忙碌），或並未傳送處理完程式鍵，Kaspersky Embedded Systems Security 2.2 會略過該物件，而計數器“**要求略過總數**”的值會加 1。
用途	此計數器使您能夠偵測，因為檔案截取調度程式故障而產生的效能降低情況。
標準值/上限值	0/1
建議的讀取間隔時間	1 小時
如果值超過上限值時的設定建議	如果計數器值並非零，表示有一或多個檔案截取調度程式執行緒已凍結，且停止作業。計數器等於目前閒置的執行緒數。 如果掃描速度緩慢，請重新啟動 Kaspersky Embedded Systems Security 2.2 來還原離線的資料流。

因為系統資源不足而未處理的需求數

步驟 70. 因為系統資源不足而未處理的需求數

名稱	因為資源不足而未處理的要求數。
定義	因為系統資源（例如 RAM）不足，而未處理的檔案截取驅動程式要求總數；從上次啟動 Kaspersky Embedded Systems Security 2.2 的時間算起。 Kaspersky Embedded Systems Security 2.2 會略過檔案截取驅動程式未處理其掃描要求的物件。
用途	此計數器可用來消除即時防護品質可能因系統資源不足而降低的情況。
標準值/上限值	0/1。
建議的讀取間隔時間	1 小時。
如果值超過上限值時的設定建議	如果計數器值不為零，則表明 Kaspersky Embedded Systems Security 2.2 工作處理程序需要更多 RAM 來處理請求。 其他應用程式的作用中程序可能會使用所有可用的 RAM。

傳送以供處理的需求數

步驟 71. 傳送以供處理的需求數

名稱	傳送以供處理的需求數。
定義	等待工作處理程序處理的物件數量。

用途	此計數器可用於追蹤 Kaspersky Embedded Systems Security 2.2 工作程序的負載，以及電腦上檔案活動的整體程度。
標準值/上限值	該計數器值可能因電腦上的檔案活動水平而異。
建議的讀取間隔時間	1 分鐘
如果值超過上限值時的設定建議	否

檔案截取調度程式執行緒的平均數

步驟 72. 檔案截取調度程式執行緒的平均數

名稱	檔案截取調度程式執行緒的平均數。
定義	一個處理程序中的檔案攔截調度程式流數量，對於目前參與即時防護工作的所有處理程序而言，則為檔案攔截調度程式流的平均數量。
用途	此計數器可用來消除即時防護品質可能因 Kaspersky Embedded Systems Security 2.2 處理程序滿載而降低的情況。
標準值/上限值	視情況有所不同 / 40
建議的讀取間隔時間	1 分鐘
如果值超過上限值時的設定建議	每個工作程序中最多可建立 60 個檔案截取調度程式執行緒。如果計數器值接近 60，則可能會有工作程序無法處理佇列中下一個檔案截取驅動程式要求的風險，且 Kaspersky Embedded Systems Security 2.2 會略過物件。 請增加用於完成即時防護工作的 Kaspersky Embedded Systems Security 2.2 處理程序的數量。您可以使用“**最大活動程序數**”和“**用於即時防護的程序數**”等 Kaspersky Embedded Systems Security 2.2 設定。

檔案截取調度程式執行緒的最大數

步驟 73. 檔案截取調度程式執行緒的最大數

名稱	檔案截取調度程式執行緒的最大數。
定義	一個處理序中的檔案攔截調度程式流數量；對於目前參與即時防護工作的所有處理程序而言，則為檔案攔截調度程式流的最大數量。
用途	此計數器可讓您偵測與修除因執行中程序負載分配不平均所造成的效能低落。
標準值/上限值	視情況有所不同 / 40
建議的讀取間隔時間	1 分鐘
如果值超過上限值時的設定建議	如果計數器的值超過“**檔案攔截調度程式資訊流平均數量**”計數器的值並繼續增加，則表示 Kaspersky Embedded Systems Security 2.2 正在執行的處理程序分配負載時不夠平均。 重新啟動 Kaspersky Embedded Systems Security 2.2。

已感染物件佇列中的元素數

步驟 74. 已感染物件佇列中的元素數

名稱	已感染物件佇列中的項目數。
定義	目前等候處理（未受感染或已刪除）的已感染物件數。
用途	此計數器可讓您偵測： • 檔案截取調度程式可能失敗，造成即時防護中斷。 • 因不同工作程序與 Kaspersky Embedded Systems Security 2.2 間的處理器時間分配不平均，而造成處理程序過載。 • 病毒爆發。
標準值/上限值	當 Kaspersky Embedded Systems Security 2.2 正在處理已感染或疑似感染物件時，此計數器值可能大於零；但當處理完成時會返回零，或計數器值會長久保持非零的狀態。
建議的讀取間隔時間	1 分鐘
如果值超過上限值時的設定建議	如果此計數器值常久未傳回零： • Kaspersky Embedded Systems Security 2.2 並未處理物件（檔案截取調度程式可能已當機）。 重新啟動 Kaspersky Embedded Systems Security 2.2。 • 處理物件的處理器時間不足。 請確定 Kaspersky Embedded Systems Security 2.2 可取得更多處理時間（例如，降低電腦上其他應用程式的負載）。 • 病毒已爆發。 在“即時檔案防護”工作中有大量已感染或疑似感染物件，也表示病毒爆發。可以在工作統計資訊或工作記錄中檢視有關已偵測到的物件的數量的資訊。

每秒處理的物件數

步驟 75. 每秒處理的物件數

名稱	每秒處理的物件數。
定義	已處理的物件數除以處理那些物件所花的時間量（以相等間隔時間來計算）。
用途	此計數器會反映物件處理的速度；可用於偵測與消除因分配至 Kaspersky Embedded Systems Security 2.2 處理程序的處理器時間不足，或 Kaspersky Embedded Systems Security 2.2 作業錯誤，所造成的電腦效能低落。
標準值/上限值	視情況有所不同 / 無。
建議的讀取間隔時間	1 分鐘。

如果值超過上限值時的設定建議	此計數器中的值，要視 Kaspersky Embedded Systems Security 2.2 設定，以及電腦上來自其他應用程式處理程序的負載而定。 注意一段長時間時計數器數字的平均程度。如果一般程度計數器值的降低，表示可能發生以下其中一種情況： • Kaspersky Embedded Systems Security 2.2 處理程序處理物件的處理器時間不足。 請確定 Kaspersky Embedded Systems Security 2.2 可取得更多處理時間（例如，降低電腦上其他應用程式的負載）。 • Kaspersky Embedded Systems Security 2.2 出錯（多個流空閒）。 重新啟動 Kaspersky Embedded Systems Security 2.2。

Kaspersky Embedded Systems Security 2.2 SNMP 計數器和 TRAP

本節包含有關 Kaspersky Embedded Systems Security 2.2 計數器和 TRAP 的資訊。

本章節說明項目

關於 Kaspersky Embedded Systems Security 2.2 SNMP 計數器和 TRAP

如果要安裝一組病毒防護元件中包括 **SNMP 計數器和 TRAP**，則可以使用簡單網路管理協定 (SNMP) 檢視 Kaspersky Embedded Systems Security 2.2 計數器和 TRAP。

若要從管理員的工作站檢視 Kaspersky Embedded Systems Security 2.2 計數器和 TRAP，請啟動受防護電腦上的 SNMP 服務，並啟動管理員工作站上的 SNMP 和 SNMP TRAP 服務。

Kaspersky Embedded Systems Security 2.2 SNMP 計數器

本節包含介紹 Kaspersky Embedded Systems Security 2.2 SNMP 計數器的設定的表。

本章節說明項目

效能計數器

步驟 76. 效能計數器

計數器	定義
currentRequestsAmount	傳送以供處理的要求數（請參見第 230 頁）
currentInfectedQueueLength	已感染物件佇列中的項目數（請參見第 232 頁上的“已感染物件佇列中的項目數”部分）
currentObjectProcessingRate	每秒處理的物件數（請參見第 232 頁）
currentWorkProcessesNumber	Kaspersky Embedded Systems Security 2.2 所使用的工作處理程序的目前數量

隔離計數器

步驟 77. 隔離計數器

計數器	定義
totalObjects	目前在隔離中的物件數
totalSuspiciousObjects	目前在隔離中的疑似感染物件數
currentStorageSize	隔離中的資料大小總計(MB)

備份計數器

步驟 78. 備份計數器

計數器	定義
currentBackupStorageSize	備份中的資料大小總計(MB)

一般計數器

步驟 79. 一般計數器

計數器	定義
lastCriticalAreasScanAge	自上次對電腦關鍵區域執行完整掃描以來的期限（自完成上一次“*關鍵區域掃描*”的工作後所經過的時間，單位為秒）。
licenseExpirationDate	產品授權到期日期。如果新增了啟動金鑰和備用金鑰，則將顯示與備用金鑰關聯的產品授權到期日期。
currentApplicationUptime	Kaspersky Embedded Systems Security 2.2 自從上次啟動起的執行時間（單位為百分之一秒）。
currentFileMonitorTaskStatus	“即時檔案防護”工作狀態：**開啟** – 正在執行；**關閉** – 已停止或已暫停。

更新計數器

步驟 80. 更新計數器

計數器	定義
avBasesAge	資料庫“時效”（最近一次更新已安裝資料庫的建立日期後所經過的時間，單位為百分之一秒）。

即時防護計數器

步驟 81. 即時防護計數器

計數器	定義
totalObjectsProcessed	上次執行“即時檔案防護”工作時掃描的物件總數
totalInfectedObjectsFound	上次“執行即時檔案防護”工作時受感染和其他的物件總數
totalSuspiciousObjectsFound	上次執行“即時檔案防護”工作時疑似感染的物件總數
totalVirusesFound	上次執行“即時檔案防護”工作時偵測到的威脅總數
totalObjectsQuarantined	Kaspersky Embedded Systems Security 2.2 放入隔離的已感染、疑似感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsNotQuarantined	Kaspersky Embedded Systems Security 2.2 嘗試隔離但無法隔離成功的已感染或疑似感染物件總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsDisinfected	Kaspersky Embedded Systems Security 2.2 解毒的已感染物件總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsNotDisinfected	Kaspersky Embedded Systems Security 2.2 嘗試解毒但無法成功解毒的已感染物件總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsDeleted	Kaspersky Embedded Systems Security 2.2 解毒的已感染、疑似感染和其他物件的總數；自上一次啟動“即時檔案防護”工作的時間算起
totalObjectsNotDeleted	Kaspersky Embedded Systems Security 2.2 嘗試清除但未成功解毒的已感染、疑似感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsBackedUp	Kaspersky Embedded Systems Security 2.2 放入備份中的已感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsNotBackedUp	Kaspersky Embedded Systems Security 2.2 嘗試放入備份中但未成功的已感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起

SNMP TRAP

下表匯總了 Kaspersky Embedded Systems Security 2.2 中的 SNMP TRAP 設定。

步驟 82. Kaspersky Embedded Systems Security 2.2 SNMP TRAP

TRAP	敘述	選項
eventThreatDetected	偵測到威脅。	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventBackupStorageSizeExceeds	已超過最大備份容量。“備份”中的資料大小總計已超過“**最大備份空間 (MB)**”的設定值。Kaspersky Embedded Systems Security 2.2 繼續備份受感染的物件。	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	已達備份可用空間上限值。“**可用空間上限值 (MB)**”指派的備份可用空間量等於或低於指定值。Kaspersky Embedded Systems Security 2.2 繼續備份受感染的物件。	eventDateAndTime eventSeverity eventSource

TRAP	敘述	選項
eventQuarantineStorageSizeExceeds	已超過隔離大小上限。隔離中的資料大小總計已超過“**最大隔離區空間 (MB)**”的指定值。Kaspersky Embedded Systems Security 2.2 繼續隔離疑似感染物件。	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	已達隔離可用空間上限值。“**可用空間上限值 (MB)**”所分配的隔離可用空間容量小於指定值。Kaspersky Embedded Systems Security 2.2 繼續隔離疑似感染物件。	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	隔離發生錯誤。	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	在備份中儲存物件副本時發生錯誤。	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason

TRAP	敘述	選項
eventQuarantineInternalError	隔離發生錯誤。	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	備份錯誤。	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	防毒軟體資料庫已過期。正在計算從上次執行資料庫更新工作（本機工作、群組工作或多組電腦的工作）起的天數。	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	防毒軟體資料庫已長時間未更新。正在計算從上次執行資料庫更新工作（本機工作、群組工作或多組電腦的工作）起的天數。	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Embedded Systems Security 2.2 正在執行。	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Embedded Systems Security 2.2 已停止。	eventSeverity eventDateAndTime eventSource

TRAP	敘述	選項
eventCriticalAreasScanWasntPerformForALongTime	很長時間未掃描關鍵區域。以自上次完成“*關鍵區域掃描*”工作以來的天數進行計算。	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	產品授權已到期。	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	產品授權即將到期。計算距離產品授權到期日之前的天數。	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	工作完成錯誤。	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	執行更新工作時發生錯誤。	eventSeverity eventDateAndTime taskName updaterErrorEventReason

下表敘述 TRAP 的設定及其可用的參數值。

步驟 83.　SNMP TRAP：設定值

設定	說明和可用的參數值
eventDateAndTime	事件時間。
eventSeverity	重要性等級。可用的設定值如下： • critical (1) – 重要 • warning (2) – 警告 • info (3) – 資訊
userName	使用者名稱（例如，嘗試存取已感染檔案之使用者的名稱）。
computerName	電腦名稱（例如，嘗試存取已感染檔案之使用者所用電腦的名稱）。

設定	說明和可用的參數值
eventSource	事件來源：產生事件的功能性元件。可用的設定值如下： • unknown (0) – 不明的功能性元件 • quarantine (1) – 隔離 • backup (2) – 備份 • reporting (3) – 工作記錄 • updates (4) – 更新 • realTimeProtection (5) – 即時檔案防護 • onDemandScanning (6) – 自訂掃描 • product (7) – 與 Kaspersky Embedded Systems Security 2.2 整體操作而不是單個元件操作相關的事件 • systemAudit (8) – 系統稽核記錄
eventReason	事件觸發：是什麼原因引發了該事件。可用的設定值如下： • reasonUnknown (0) – 不明原因 • reasonInvalidSettings (1) – 僅有在無法使用“隔離”或“備份”時，才適用於“隔離”或“備份”的事件（存取權限不足，或在“隔離”設定中指定錯誤的資料夾，例如指定了網路路徑）。在此情況下，Kaspersky Embedded Systems Security 2.2 將使用預設備份或隔離資料夾。
objectName	物件名稱（例如，偵測到含病毒之檔案的名稱）。
threatName	根據病毒百科全書分類確定的物件名稱。該名稱包含在 Kaspersky Embedded Systems Security 2.2 偵測物件時回傳的物件全名中。您可以在工作記錄中檢視偵測到的物件的全名（請參見第 124 頁上的“配置記錄設定”部分）。
detectType	偵測到的威脅類型。 可用的設定值如下： • undefined (0) – 未定義 • virware – 典型病毒與網路蠕蟲 • trojware – 木馬程式 • malware – 其他惡意程式 • adware – 廣告軟體 • pornware – 色情軟體 • riskware – 可能被入侵者用以破壞使用者電腦或資料的合法程式
detectCertainty	偵測威脅的確認等級。可用的設定值如下： • 疑似感染 (suspicious) – Kaspersky Embedded Systems Security 2.2 在物件的一段程式碼中偵測到部分符合不明威脅程式碼的結果。 • Sure（已感染）– Kaspersky Embedded Systems Security 2.2 偵測到的物件程式碼的一部分與已知惡意程式碼部分完全比對。
days	天數（例如，授權到期日前的天數）。
errorCode	錯誤代碼。

設定	說明和可用的參數值
knowledgeBaseId	知識庫文章的位址（例如說明特定錯誤之文章的位址）。
taskName	工作名稱。
updaterErrorEventReason	更新錯誤的原因。可用的設定值如下： • reasonUnknown (0) – 不明原因 • reasonAccessDenied – 存取遭拒 • reasonUrlsExhausted – 已用盡更新來源的清單 • reasonInvalidConfig – 無效的設定檔 • reasonInvalidSignature – 無效的特徵碼 • reasonCantCreateFolder – 無法建立資料夾 • reasonFileOperError – 檔案操作錯誤 • reasonDataCorrupted – 物件已損毀 • reasonConnectionReset – 連線重設 • reasonTimeOut – 已超過連線逾時 • reasonProxyAuthError – 代理驗證錯誤 • reasonServerAuthError – 伺服器驗證錯誤 • reasonHostNotFound – 找不到電腦 • reasonServerBusy – 無法使用伺服器 • reasonConnectionError – 連線錯誤 • reasonModuleNotFound – 找不到物件 • reasonBlstCheckFailed(16) – 檢查列入黑名單的金鑰時發生錯誤。可能是在更新期間同時發佈資料庫更新；請於幾分鐘內再執行一次。

設定	說明和可用的參數值
storageObjectNotAddedEventReason	未備份或隔離物件的原因。可用的設定值如下： • reasonUnknown (0) – 不明原因 • reasonStorageInternalError – 資料庫錯誤；請還原 Kaspersky Embedded Systems Security 2.2。 • reasonStorageReadOnly – 資料庫唯讀；請還原 Kaspersky Embedded Systems Security 2.2。 • reasonStorageIOError – 輸入輸出錯誤：a) Kaspersky Embedded Systems Security 2.2 已損壞，請還原 Kaspersky Embedded Systems Security 2.2；b) 含有 Kaspersky Embedded Systems Security 2.2 檔案的磁碟已損壞。 • reasonStorageCorrupted – 儲存空間已毀損；請還原 Kaspersky Embedded Systems Security 2.2。 • reasonStorageFull – 資料庫已滿，請釋放磁碟空間。 • reasonStorageOpenError – 無法開啟資料庫檔案；請還原 Kaspersky Embedded Systems Security 2.2。 • reasonStorageOSFeatureError – 某些作業系統功能不符合 Kaspersky Embedded Systems Security 2.2 的需求。 • reasonObjectNotFound – 磁碟中沒有放置於隔離中的物件； • reasonObjectAccessError – 使用備份 API 的權限不足；執行操作的帳戶沒有備份操作程式的權限。 • reasonDiskOutOfSpace – 磁碟空間不足。

與 WMI 整合

Kaspersky Embedded Systems Security 2.2 支援與 Windows Management Instrumentation (WMI) 整合：您可以使用支援 WMI 的用戶端系統透過基於 Web 的企業管理 (WBEM) 標準接收資料，以收集有關 Kaspersky Embedded Systems Security 2.2 及其元件的狀態的資訊。

安裝 Kaspersky Embedded Systems Security 2.2 後，它會在系統中註冊專有模組，促使在本機電腦上的 WMI 根命名空間中建立 Kaspersky Embedded Systems Security 2.2 命名空間。透過 Kaspersky Embedded Systems Security 2.2 命名空間可以使用 Kaspersky Embedded Systems Security 2.2 類和實例及其內容。

某些實例內容的值取決於工作類型。

*非週期性工作*是沒有時間限制的應用程式工作，可以持續執行或停止。此類工作不存在執行進度。當工作作為單個事件執行（例如，任一“即時電腦防護”工作偵測受感染物件）時，將不停記錄工作執行的結果。此類型的工作透過卡巴斯基安全管理中心政策進行管理。

*週期性工作*是有時間限制且以百分比形式顯示執行進度的應用程式工作。工作結果在工作完成後生成，並表示為單個項目或變更的應用程式狀態（例如，完成的應用程式資料庫更新、為規則生成工作生成的設定檔）。同一類型的多個週期性工作可以在單台電腦上同時執行（三個具有不同掃描範圍的自訂掃描工作）。可以透過卡巴斯基安全管理中心將週期性工作作為群組工作進行管理。

如果在公司網路中使用工具生成 WMI 命名空間查詢並從 WMI 命名空間接收動態資料，您將能夠接收有關目前應用程式狀態的資訊（請參見下表）。

步驟 84. 有關應用程式的啟動狀態的資訊

實例內容	敘述	值
ProductName	安裝的應用程式的名稱。	不帶版本號的應用程式全名。
ProductVersion	安裝的應用程式的完整版本。	應用程式完整版本號，包括內部版本號。
InstalledPatches	為應用程式佈署的一系列修補程式的顯示名稱。	為應用程式安裝的關鍵修復程式清單。
IsLicenseInstalled	應用程式啟動狀態。	用於啟動應用程式的金鑰的狀態。 可能的值： • False - 尚未在應用程式中設定金鑰或啟動碼。 • True - 已將金鑰或啟動碼新增到應用程式。
LicenseDaysLeft	顯示目前產品授權到期前剩餘的天數。	目前產品授權到期前剩餘的天數。 可能的非正值： • 0 - 產品授權已到期 • -1 - 無法獲取目前金鑰的資訊，或者指定金鑰無法用於啟動應用程式（例如，根據金鑰黑名單將其封鎖）。
AVBasesDatetime	目前病毒資料庫版本的時間戳記。	目前使用中的病毒資料庫的建立日期和時間。 如果已安裝的應用程式不使用病毒資料庫，則該欄位的值為“未安裝”。
IsExploitPreventionEnabled	“弱點利用防禦”元件的狀態。	“弱點利用防禦”元件的狀態。 可能的值： • True -“弱點利用防禦”元件已啟用並正在提供防護。 • False -“弱點利用防禦”元件未提供防護。例如：已停用、未安裝、已違反產品授權協議。
ProtectionTasksRunning	目前正在執行的一系列防護工作。	目前正在執行的防護、控制和監控工作的清單。此欄位應表示所有正在執行的非週期性工作。 如果沒有非週期性工作正在執行，該欄位的值為“否”。

實例內容	敘述	值
IsAppControlRunning	“ 應用程式啟動控制”工作的狀態。	“ 應用程式啟動控制” 工作的狀態。 • True -“ 應用程式啟動控制” 工作目前正在執行。 • False -“ 應用程式啟動控制” 工作目前未執行或“ 應用程式啟動控制” 元件未安裝。
AppControlMode	“ 應用程式啟動控制”工作模式。	敘述“ 應用程式啟動控制” 元件的目前狀態，以及相應工作的選定模式。 可能的值： • 活動 -“ **活動**” 模式在工作設定中選擇。 • 僅統計 “ **僅統計**”模式在工作設定中選擇。 • 未安裝 “ 應用程式啟動控制”元件未安裝。
AppControlRulesNumber	應用程式啟動控制規則總數。	“ 應用程式啟動控制” 工作設定中目前指定的規則數量。
AppControlLastBlocking	“ 應用程式啟動控制” 工作上次在任一模式下封鎖應用程式啟動的時間戳記。	“ 應用程式啟動控制” 元件上次封鎖應用程式啟動時的日期和時間。該欄位包括所有已封鎖的應用程式，不管工作模式為何。 如果在處理 WMI 查詢時未註冊已封鎖的應用程式啟動的實例，該欄位將被分配值“ 否” 。
PeriodicTasksRunning	目前正在執行的一系列週期性工作。	目前正在執行的自訂掃描、更新和清單編制工作的清單。此欄位應包括所有正在執行的週期性工作。 如果目前沒有週期性工作正在執行，則該欄位的值為“ 否” 。
ConnectionState	WMI 提供程式元件與 Kaspersky Security 服務 (KAVFS) 之間的連線的狀態。	有關 WMI 提供程式模組與 Kaspersky Security 服務之間的連線狀態的資訊。 可能的值： • 成功 - 連線已成功建立：WMI 用戶端可以接收有關應用程式狀態的資訊。 • 失敗。錯誤代碼: <代碼> - 由於出現指定代碼的錯誤，無法建立連線。

此資料表示實例內容 KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security，其中：

- KasperskySecurity_ProductInfo 是 Kaspersky Embedded Systems Security 2.2 類別的名稱
- .ProductName=Kaspersky Embedded Systems Security 是 Kaspersky Embedded Systems Security 2.2 關鍵參數

該實例在 ROOT\Kaspersky\Security 命名空間中建立。

聯絡技術支援

本章節提供有關如何與 Kaspersky Lab 技術支援服務聯絡的資訊。

本章內容

如何獲取技術支援

如果您無法透過手冊及相關資源自行排除問題，建議您與技術支援聯絡。技術支援服務專家會為您解答關於安裝和使用該應用程式的任何問題。

技術支援服務僅適用擁有正式版授權的使用者。試用版授權的使用者將不包含在技術支援服務範圍內。

在聯絡技術支援服務前，請閱讀技術支援規則。

可以透過以下方法之一與技術支援部門聯絡：

- 致電技術支援。
- 透過 Kaspersky CompanyAccount 網站 (https://companyaccount.kaspersky.com) 向 Kaspersky Lab 技術支援服務部門傳送問題。

透過 Kaspersky CompanyAccount 取得技術支援

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) 是一種可用於向 Kaspersky Lab 傳送請求，並追蹤 Kaspersky Lab 專家處理請求進度的網頁服務。Kaspersky CompanyAccount 設計用於方便使用者與 Kaspersky Lab 專家之間透過線上請求進行互動。透過使用 Kaspersky CompanyAccount 網站，您可以監視 Kaspersky Lab 專家處理電子請求的進度並儲存電子請求的歷史記錄。

可以在 Kaspersky CompanyAccount 上的單個使用者帳戶中註冊您組織的所有員工。透過使用單一帳戶，您可以集中管理註冊的員工傳送到 Kaspersky Lab 的電子請求，以及在 Kaspersky CompanyAccount 中管理員工的權限。

Kaspersky CompanyAccount 適用於以下語言：

- 英語
- 西班牙語
- 義大利語
- 德語

- 波蘭語
- 葡萄牙語
- 俄語
- 法語
- 日語

有關 Kaspersky CompanyAccount 操作的更多資訊，請參閱技術支援網站 http://support.kaspersky.com/faq/companyaccount_help。

使用偵錯檔案和 AVZ 指令碼

向 Kaspersky Lab 技術支援專家報告問題後，他們可能需求您建立一份包含有關 Kaspersky Embedded Systems Security 2.2 執行情況的資訊的報告，然後將報告傳送給 Kaspersky Lab 技術支援部門。Kaspersky Lab 技術支援專家還可能需要您建立偵錯檔案。偵錯檔案可以追蹤程式指令的每一步執行，以偵測錯誤發生時的程式執行階段。

在 Kaspersky Lab 技術支援專家分析您所傳送的資料後，他們可以建立 AVZ 指令碼並將其傳送給您。透過使用 AVZ 指令碼，可以分析活動處理程序以尋找威脅，掃描電腦以尋找威脅，清除或刪除感染的檔案以及建立系統掃描報告。

爲了提供針對程式問題的更加有效的支援和故障排除，技術支援專家可能需求您暫時變更設定，以便在診斷過程中進行診斷。這可能需要進行以下操作：

- 啟動用於處理和儲存延伸診斷資訊的功能。
- 對於無法透過標準使用者介面元素使用的各個軟體元件，微調這些元件的設定。
- 變更已處理的診斷資訊的儲存和傳輸設定。
- 設定網路流量的攔截和記錄。

AO Kaspersky Lab

Kaspersky Lab 是防護電腦免受諸如病毒和其他惡意軟體、未經請求所傳送的電子郵件（垃圾郵件）以及網路和駭客攻擊等數位威脅的系統的世界知名供應商。

2008 年，Kaspersky Lab 被評為全球四大資訊安全解決方案供應商之一（根據 IDC Worldwide Endpoint Security Revenue by Vendor）。Kaspersky Lab 是俄羅斯家庭使用者首選的電腦防護系統供應商 (IDC Endpoint Tracker 2014)。

Kaspersky Lab 於 1997 年成立於俄羅斯。如今，Kaspersky Lab 已成長為一家在 33 個國家/地區擁有 38 個辦事處的國際性企業集團。並且團隊組織共擁有 3,000 多名的技術專家。

產品。Kaspersky Lab 的產品為家用電腦到大型企業網路的所有系統提供安全防護。

個人產品範圍包括桌上型電腦、筆記型電腦和可攜式電腦，以及智慧型手機和其他行動裝置的安全應用程式。

公司提供用於工作站和行動裝置、虛擬機、檔案伺服器和 Web 伺服器、郵件閘道以及防火牆的防護和控制解決方案和技術。公司的產品群組還包括用於防止 DDoS 攻擊、防護工業控制系統以及防止金融欺詐的專用產品。並透過與集中管理工具整合起來之後，這些解決方案能夠為任何規模的公司和組織提供高效能且自動化的安全防護，以防範各式的電腦威脅。同時，Kaspersky Lab 產品獲得主要測試實驗室的認證，相容於許多供應商的軟體，經過最佳化設定以便應用在多種硬體平台上執行。

Kaspersky Lab 病毒分析人員不捨晝夜地工作。他們每天都會發現成千上萬的新型電腦威脅，並且建立工具以偵測和解毒它們，同時會將這些威脅的簽章加入在 Kaspersky Lab 應用程式所使用的資料庫中。

技術。許多現在已經成為現代防毒工具組成部分的技術最初都是由 Kaspersky Lab 開發的。很多其他開發商在其產品中使用卡巴斯基病毒防護引擎絕非巧合，這包括：Alcatel-Lucent、Alt-N、Asus、BAE Systems、Blue Coat、Check Point、Cisco Meraki、Clearswift、D-Link、Facebook、General Dynamics、H3C、Juniper Networks、Lenovo、Microsoft、NETGEAR、Openwave Messaging、Parallels、Qualcomm、Samsung、Stormshield、Toshiba、Trustwave、Vertu 和 ZyXEL。公司的許多創新性技術都獲得了專利認證。

成就。多年以來，Kaspersky Lab 因為在對抗電腦威脅方面提供的服務贏得數以百計的獎項。在 2014 年由著名奧地利測試實驗室 AV-Comparatives 進行測試和研究後，Kaspersky Lab 贏得多項 Advanced+ 憑證，躋身前兩大供應商之一，且最終被授予最受好評憑證。不過，Kaspersky Lab 最主要的成就來自於全球使用者對它的信賴。Kaspersky Lab 目前在全球間為超過 4 億名使用者及超過 27 萬家的企業使用者提供令人安心的資訊安全防護。

Kaspersky Lab 網站：	https://www.kaspersky.com
病毒百科全書：	https://securelist.com
病毒實驗室：	https://virusdesk.kaspersky.com（用於分析可疑檔案和網站）
Kaspersky Lab 網路論壇：	http://forum.kaspersky.com

有關協力廠商程式碼資訊

有關協力廠商程式碼資訊被包含在文件 legal_notices.txt 中，並位於應用程式的安裝資料夾中。

商標聲明

詞彙表

啟動金鑰

應用程式目前使用的金鑰。

管理伺服器

卡巴斯基安全管理中心的一個元件，可集中儲存公司網路內所有安裝 Kaspersky Lab 應用程式的資訊。它也可用於管理這些應用程式。

病毒特徵碼資料庫

該資料庫中包含截至病毒資料庫發佈日期為止 Kaspersky Lab 已知的電腦安全威脅相關資訊。資料庫中的項目用於在掃描物件時偵測到惡意程式。Kaspersky Lab 的專家維護資料庫每小時更新一次。

壓縮檔案

一個或多個檔案透過壓縮封裝到單個檔案中。壓縮和解壓縮資料需要一個名為壓縮應用程式的專用應用程式。

備份

用來儲存檔案備份副本的特殊儲存，在嘗試解毒或刪除前建立。

解毒

一種處理受感染檔案的方法，該方法會導致完全或部份還原資料，或裁定無法解毒檔案。不是所有的受感染物件都可以解毒。

事件嚴重性

在 Kaspersky Lab 應用程式執行過程中遇到的事件的內容。有四個嚴重等級：

- 緊急事件。
- 錯誤。
- 警告。
- 資訊。

同一類型的事件可能有不同的嚴重等級，具體取決於發生事件時的情況。

誤報

Kaspersky Lab 程式因物件的程式碼與病毒的程式碼類似而將非受感染的物件視為受感染物件的情況。

檔案遮罩

使用萬用字元表示檔案名稱。檔案遮罩中使用的標準萬用字元為 * 和 ?，其中 * 表示任意數量的任意字元，? 表示單個任意字元。

啟發式分析

用於偵測其資訊尚未新增到 Kaspersky Lab 資料庫中的威脅技術。啟發式分析用於透過偵測運作行為，判斷對作業系統構成安全威脅的物件。啟發式分析偵測到的物件將被視為疑似感染。例如，如果一個物件包含惡意物件通常具有的運作行為（檔案開啟、寫入），則可能會將該物件視為疑似感染。

可感染的檔案

一種由於其結構或格式，可被罪犯用作儲存和傳播惡意程式碼的“容器”的檔案。通常為可執行檔，此類檔案副檔名為 .com、.exe 和 .dll。此類檔案被惡意程式碼侵入的風險非常高。

受感染的物件

其部分程式碼完全比對已知惡意軟體部分程式碼的物件。Kaspersky Lab 不建議存取此類物件。

卡巴斯基安全網路 (KSN)

一個雲端服務基礎架構，提供對 Kaspersky Lab 資料庫的存取，該資料庫不斷更新關於檔案、Web 資源和軟體的信譽的資訊。卡巴斯基安全網路允許 Kaspersky Lab 十分迅速地對新威脅作出回應，提高許多防護元件的效能，以降低誤報可能性。

產品授權期限

一個時間段，在此時間段內您可以存取應用程式功能，並有權使用附加服務。您可以使用的服務取決於產品授權的類型。

本機工作

定義為在單台用戶端電腦上執行的工作。

OLE 物件

附加到其他檔案或透過使用物件連結與嵌入 (OLE) 技術嵌入其他檔案的物件。一個 OLE 物件範例是嵌入到 Microsoft Office Word 文件中的 Microsoft Office Excel® 電子表格。

政策

在管理群組內，政策決定應用程式的設定並管理對電腦上安裝的應用程式的配置的存取。必須為每個應用程式建立單獨政策。您可以在每個管理群組內為電腦上安裝的應用程式建立無限數量的不同政策，但在一個管理群組內一次只能對每個應用程式套用一個政策。

防護狀態

目前防護狀態，反映電腦安全性的等級。

隔離

Kaspersky Lab 應用程式將偵測到的疑似感染物件移動到的資料夾。在此以加密形式儲存在隔離，以避免對電腦造成任何影響。

即時防護

應用程式的執行模式，在該模式下即時掃描物件是否存在惡意程式碼。

應用程式將攔截所有開啟任何物件（讀取、寫入或執行）的嘗試，並掃描物件是否存在威脅。未受感染的物件將傳遞給使用者；包含威脅的物件或疑似感染物件將按照工作設定進行處理（解毒、刪除或隔離）。

安全等級

安全等級定義為一組預先配置的應用程式元件設定。

SIEM

一種用於分析來源於各種網路裝置和應用程式的安全事件的技術。

啟動物件

電腦上安裝的作業系統和軟體正常啟動和執行所需的一組應用程式集。每次啟動作業系統時，都會執行這些物件。有些病毒專門感染此類物件，例如，可能會導致作業系統無法啟動。

工作

Kaspersky Lab 應用程式執行的功能以工作形式實現，例如：即時檔案防護、完全電腦掃描和資料庫更新。

工作設定

特定於每個工作類型的應用程式設定。

更新

替換/新增從 Kaspersky Lab 更新伺服器上擷取的新檔案（資料庫或應用程式模組）的過程。

弱點

作業系統或應用程式存在的弱點，惡意軟體研發者會利用這種弱點入侵系統或應用程式並破壞其完整性。作業系統中的許多弱點都會導致作業系統執行不可靠，因為侵入作業系統的病毒可能會導致作業系統本身和安裝的應用程式損壞。

索引

八劃

十三劃