KASPERSKY

Kaspersky Security for Windows Server

管理手冊

產品版本：10.1.0.622

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 年 3 月 26 日

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

KASPERSKY

內容

關於本手冊

Kaspersky Security for Windows Server 10.1.0.622（下文稱為“Kaspersky Security 10.1 for Windows Server”）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 Security 10.1 for Windows Server 的專家，以及使用 Kaspersky Security 10.1 for Windows Server 為各組織提供技術支援的專家使用。

本管理手冊包含有關設定和使用 Kaspersky Security 10.1 for Windows Server 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

本手冊說明主題

Kaspersky Security 10.1 for Windows Server 管理手冊由以下章節組成：

有關 Kaspersky Security 10.1 for Windows Server 的資訊來源

本章節介紹程式的相關資訊來源。

Kaspersky Security 10.1 for Windows Server

本節介紹了 Kaspersky Security 10.1 for Windows Server 的功能、元件以及分發套件，並提供了 Kaspersky Security 10.1 for Windows Server 的硬體和軟體需求清單。

安裝和移除 Kaspersky Security 10.1 for Windows Server

本節提供安裝和移除 Kaspersky Security 10.1 for Windows Server 的逐步說明。

應用程式介面

本節包含有關 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server

本節包含有關啟動和停止 Kaspersky Security 10.1 for Windows Server 管理外掛程式（下文稱為 Kaspersky Security 10.1 for Windows Server 管理外掛程式）和 Kaspersky Security Service 的資訊。

關於 Kaspersky Security 10.1 for Windows Server 功能的存取權限

本節包含有關 Kaspersky Security 10.1 for Windows Server 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個伺服器上管理 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 一般設定的資訊。

即時伺服器防護

本節提供有關即時防護工作（即時檔案防護、指令碼監控、KSN 使用和弱點利用防禦）的資訊。它還提供有關如何設定即時防護工作和管理受防護伺服器的安全設定說明。

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 Security 10.1 for Windows Server 功能的資訊。

網路活動控制

本節包含有關防火牆和加密勒索軟體防護工作的資訊。

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。

監控效能。Kaspersky Security 10.1 for Windows Server 計數器

本章節包含有關 Kaspersky Security 10.1 for Windows Server 計數器的資訊：系統監控效能計數器以及 SNMP 計數器和 TRAP。

從命令列使用 Kaspersky Security 10.1 for Windows Server

本節敘述從命令列使用 Kaspersky Security 10.1 for Windows Server。

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）。

表 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 Security 10.1 for Windows Server 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程度，來選取最適宜的來源。

本章內容

可供自行查詢的資料來源

您可以檢視以下關於 Kaspersky Security 10.1 for Windows Server 的資訊來源：

- Kaspersky Lab 網站上的 Kaspersky Security 10.1 for Windows Server 頁面。
- 技術支援網站（知識庫）中的 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 頁面

在 Kaspersky Security 10.1 for Windows Server 頁面 https://www.kaspersky.com/small-to-medium-business-security/windows-server-security 上，您可以檢視有關程式、它的功能和特色的基本資訊。

Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 頁面

知識庫是技術支援網站的一部分。

知識庫 https://support.kaspersky.com/ksws10/ 中的 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 文件

《Kaspersky Security 10.1 for Windows Server 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，您可以檢視現有主題、發表評論並建立新的討論主題。

Kaspersky Security 10.1 for Windows Server

本節介紹了 Kaspersky Security 10.1 for Windows Server 的功能、元件以及分發套件，並提供了 Kaspersky Security 10.1 for Windows Server 的硬體和軟體需求清單。

本章內容

關於 Kaspersky Security 10.1 for Windows Server

Kaspersky Security 10.1 for Windows Server（以前稱為“Kaspersky Anti-Virus for Windows Servers Enterprise Edition”）為執行於 Microsoft® Windows® 作業系統上的伺服器和網路附加儲存提供防護，使它們免受病毒危害以及避免伺服器在檔案交換過程中可能面臨的其他電腦安全威脅。Kaspersky Security 10.1 for Windows Server 是專為中大型企業的網路環境而設計。Kaspersky Security 10.1 for Windows Server 管理者是負責公司網路病毒防護的系統管理員和專業人員。

您可以在以下伺服器上安裝 Kaspersky Security 10.1 for Windows Server：

- 終端伺服器。
- 列印伺服器。
- 應用程式伺服器。
- 網域控制站。
- 用作防護網路附加儲存的伺服器。
- 檔案伺服器 – 這類伺服器感染病毒的可能性較高，因為它們會與使用者工作站進行檔案交換。

可透過以下方式管理 Kaspersky Security 10.1 for Windows Server：

- 透過與 Kaspersky Security 10.1 for Windows Server 安裝在同一台伺服器上或安裝在其他電腦上的 Kaspersky Security 10.1 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的管理主控台來管理。

卡巴斯基安全管理中心也可以集中管理執行 Kaspersky Security 10.1 for Windows Server 的多個伺服器。

您可以檢視針對“系統監控器”應用的 Kaspersky Security 10.1 for Windows Server 效能計數器以及 SNMP 計數

器和陷阱。

Kaspersky Security 10.1 for Windows Server 元件和功能

應用程式包含以下元件：

- **即時防護**。Kaspersky Security 10.1 for Windows Server 在物件被存取時掃描物件。Kaspersky Security 10.1 for Windows Server 掃描以下物件：
  - 檔案
  - 檔案交換系統執行緒（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 Security 10.1 for Windows Server 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。
- **RPC-網路儲存防護**和 **ICAP-網路儲存防護**。在執行 Microsoft Windows 作業系統的伺服器上安裝的 Kaspersky Security 10.1 for Windows Server，可以防護網路附加儲存，使其免受病毒危害和透過檔案交換侵入伺服器的其他安全威脅。
- **應用程式啟動控制**。該元件可跟蹤使用者嘗試啟動應用程式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。
- **加密勒索軟體防護**和**用於 NetApp 的加密勒索軟體防護**。這兩個元件透過封鎖出現惡意活動的主機來防護伺服器上的分享資料夾和網路附加儲存免受惡意加密。
- **指令碼監控**。此元件控制使用 Microsoft Windows 指令碼技術建立的指令碼的執行。
- **流量安全**。此元件攔截並掃描透過 Web 流量傳輸的物件（包括郵件），以偵測已知電腦和受防護伺服器上的其他威脅。
- **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，以及封鎖配置防火牆設定的所有其他方法。
- **檔案完整性監控**。Kaspersky Security 10.1 for Windows Server 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**和**軟體模組更新**。Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 透過將可疑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“*已感染*”或“*可疑感染*”的物件，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 設定匯出到 XML 設定檔，也可以將設定檔中的設定匯入到 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 管理相關的事件，以及 Kaspersky Security 10.1 for Windows Server 錯誤診斷所需的資訊。
- **分級儲存**。Kaspersky Security 10.1 for Windows Server 可在分級儲存管理模式（HSM 系統）中執行。HSM 系統允許在快速本機硬碟和慢速外接儲存硬碟之間移動資料。
- **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 Security 10.1 for Windows Server 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。
- **封鎖的主機**。如果在嘗試存取伺服器共用網路資料夾的遠端主機上偵測到任何惡意活動，可以封鎖這些主機。

新增功能

Kaspersky Security 10.1 for Windows Server 是防護公司伺服器和資料儲存系統的解決方案。可用的防護範圍（執行 Windows 的伺服器、資料儲存系統）和功能元件集取決於所購買的產品授權類型。

Kaspersky Security 10.1 for Windows Server 改進並完全保留了程式先前版本的功能，同時增加了新的防護元件。

新的 Kaspersky Security 10.1 for Windows Server 帶來以下新元件：

- 新增的流量安全元件（請參見第 177 頁上的“流量安全”部分）：現在，除了透過電子郵件傳送的威脅，您的伺服器還可以抵禦透過 HTTP 或 HTTPS 流量傳送的 Web 威脅。該新元件支援以下防護方案：
  - 使用 Kaspersky Security 10.1.0.***Microsoft Outlook® 載入項（下文稱為“Kaspersky Security 10.1 Microsoft Outlook 載入項”）實現的電子郵件流量病毒防護和釣魚防護；
  - Web 流量的病毒防護和釣魚防護；
  - 使用惡意網址資料庫實現的連結驗證；
  - 使用基於雲端的惡意網址資料庫實現的連結驗證；
  - 使用連結和憑證規則實現的 Web 控制；
  - 基於類別的 Web 資源控制；
  - 連線時 Web 伺服器憑證的驗證。

流量由採用以下三種設定之一的 ICAP 服務防護：

- 外部代理：分析從外部代理伺服器重定向的流量（不使用網路驅動程式）。
- 重定向器：分析從在終端工作階段中啟動的瀏覽器重定向的流量（不使用網路驅動程式）。程式使用內部系統代理。
- 驅動程式攔截器：在終端工作階段中使用網路驅動程式攔截流量。

- 新的用於 NetApp 的加密勒索軟體防護元件：現在您可以使用安裝了 Kaspersky Security 10.1 for Windows Server 的伺服器防護所連線的 NetApp 網路附加儲存免受惡意加密。

請參見《網路附加儲存實施手冊》。

- 新的裝置控制元件（請參見第 216 頁上的“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”部分）：現在您可以建立程式用來允許或封鎖與外部資料儲存裝置（USB 和 MTP 連線的大容量儲存裝置、CD/DVD 裝置）進行檔案交換的規則清單。
- 新的弱點利用防禦元件（請參見第 169 頁上的“弱點利用防禦”部分）：現在您可以配置設定以使用攻擊緩解技術防護處理程序免受弱點利用。
- 新的檔案完整性監控元件（請參見第 232 頁上的“檔案完整性監控”部分）：現在您可以指出您想要監控其完整性的物件。
- 新的記錄審查元件（請參見第 238 頁上的“記錄審查”部分）：現在您可以為 Windows 事件記錄生成記錄審查規則，並設定啟發式分析在 Windows 事件記錄中的使用。
- 新的與外部 SIEM 系統整合的能力（請參見第 147 頁上的“ 配置 SIEM 整合設定”部分）：現在您可以對使用 syslog 協定將應用程式記錄匯出到外部事件聚合系統的設定進行配置。
- 新的跟蹤受防護裝置的 USB 連線（請參見第 214 頁上的“關於裝置控制工作”部分）的能力：現在您可以對有關各種類型的裝置與受防護電腦建立的 USB 連線的通知的設定進行配置。
- 安全事件記錄（第 147 頁上）實施：現在您可以在單個記錄中檢視應用程式元件記錄的所有指出受防護系統可能遭到入侵的事件。
- 新的防火牆管理元件（請參見第 221頁上的“防火牆管理”部分）：現在您可以透過 Kaspersky Security 10.1 for Windows Server 的圖形使用者介面管理 Windows 防火牆規則。
- 新的掃描 USB 大容量儲存裝置的能力（請參見第 139 頁上的“抽取式磁碟機掃描”部分）：現在您可以在大容量儲存裝置連線到受防護電腦時掃描這些裝置。
- 新的啟用應用程式管理的密碼防護的能力（請參見第 92 頁上的 “Kaspersky Security 10.1 for Windows Server 功能的受密碼防護的存取”部分）：現在您還可以防護 Kaspersky Security 10.1 for Windows Server，使用密碼限制對關鍵操作的存取。
- 新的來自受信任分發套件的自動允許應用程式啟動的能力（請參見第 205 頁上的“設定軟體分發控制”部分）：現在您可以在“應用程式啟動控制”工作設定中為分發套件新增排除項目，以簡化在安裝或更新軟體時允許檔案啟動的過程。
- 增加了新的執行病毒防護掃描和防護 Microsoft Windows Server 2016 容器的能力（請參見第 152 頁上的“關於即時檔案防護工作”部分）。
- 簡化的封鎖不信任主機（請參見“封鎖不信任主機。封鎖的主機”部分（在第 142 頁上））：現在“加密勒

索軟體防護”元件和“即時檔案防護”元件將攻擊主機的標識號新增到“封鎖的主機”儲存中。可以在防護工作設定中停用“封鎖的主機”儲存的填充。還可以在“管理伺服器主控台”的集中清單中檢視所有已封鎖的主機。

- 最佳化了為信任區域生成受信任處理程序的規則清單的能力（請參見第 136 頁上的“新增受信任處理程序”部分）：現在您可以根據校驗和、只根據路徑，或同時根據路徑和校驗和來排除處理程序。
- 簡化並延伸了填充應用程式啟動控制規則清單的機制（請參見第 209 頁上的“ 關於在卡巴斯基安全管理中心中生成所有電腦的應用程式啟動控制規則”部分）：新增了同時使用在本機主機和政策中配置的規則清單的能力，以及在卡巴斯基安全管理中心中根據工作事件生成規則的新機制。

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：

- 啟動 Kaspersky Security 10.1 for Windows Server 安裝精靈。
- 啟動 Kaspersky Security 10.1 for Windows Server 主控台安裝精靈。
- 啟動將安裝 Kaspersky Security 10.1 for Windows Server 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》。
- 閱讀《網路儲存防護實施手冊》。
- 轉到 Kaspersky Lab 網站上的 Kaspersky Security 10.1 for Windows Server 頁面 https://www.kaspersky.com/small-to-medium-business-security/windows-server-security。
- 存取技術支援網站 https://support.kaspersky.com/。
- 閱讀有關 Kaspersky Security 10.1 for Windows Server 目前版本的資訊。

\client 資料夾包含用於安裝 Kaspersky Security 10.1 主控台的檔案（元件的“Kaspersky Security 10.1 for Windows Server Administration Tools”集）。

\server 資料夾包含：

- 用於在運行 32 位元或 64 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Security 10.1 for Windows Server 元件的檔案。
- 用於安裝外掛程式的檔案，以便透過卡巴斯基安全管理中心管理 Kaspersky Security 10.1 for Windows Server 。
- 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。

\setup 資料夾包含問候程式啟動檔案。

\email_plugin 資料夾包含 Kaspersky Security 10.1 Microsoft Outlook 載入項安裝套件。

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）。

表 2. Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 安裝精靈的自動執行檔案。
ks4ws_admin_guide_zht.pdf	管理手冊。
ks4ws_user_guide_zht.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（啟動 setup.hta）。
\client\ks4wstools_x86(x64).msi	Microsoft Windows 安裝程式安裝套件；在受防護伺服器上安裝 Kaspersky Security 10.1 主控台。
\client\setup.exe	該檔案啟動元件的“管理工具”元件集（包括 Kaspersky Security 10.1 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 ks4wstools.msi 安裝套件檔案。
\server\bases.cab	程式發佈時最新病毒資料庫的壓縮檔案。
\server\setup.exe	該檔案啟動用於在受防護的伺服器上安裝 Kaspersky Security 10.1 for Windows Server 的精靈；使用在精靈中指定的安裝設定啟動安裝套件檔案 ks4ws.msi。
\server\ks4ws_x86(x64).msi	Microsoft Windows 安裝程式安裝套件；在受防護伺服器上安裝 Kaspersky Security 10.1 for Windows Server。
\server\ks4ws.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 Security 10.1 for Windows Server 的安裝套件的說明。
\server\klcfginst.exe	外掛程式安裝程式，以便透過卡巴斯基安全管理中心管理 Kaspersky Security 10.1 for Windows Server。 如果您預計用它來管理 Kaspersky Security 10.1 for Windows Server，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。
\server\license.txt	最終使用者產品授權協議和隱私政策的文字。
\setup\setup.hta	程式安裝檔。
\email_plugin\ksmail_x86(x64).msi	Microsoft Windows 安裝程式安裝套件；在受防護伺服器上安裝 Kaspersky Security 10.1 Microsoft Outlook 載入項。

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

本節列出了 Kaspersky Security 10.1 for Windows Server 的硬體和軟體需求。

本章內容

佈署 Kaspersky Security 10.1 for Windows Server 的伺服器需求

在安裝 Kaspersky Security 10.1 for Windows Server 之前，您必須先從伺服器移除其他防毒程式。

無需移除 Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition 或 Kaspersky Security 10 for Windows Server 即可安裝 Kaspersky Security 10.1 for Windows Server。

伺服器的硬體需求

一般需求：

- 與 x86-64 相容的單核或多核系統
- 磁碟空間需求：
  - 用於安裝所有應用程式元件：70 MB
  - 用於下載和儲存應用程式的病毒資料庫：2 GB（建議）
  - 用於在隔離和備份儲存物件：400 MB（建議）
  - 用於儲存記錄：1 GB（建議）

最低需求：

- 處理器：1.4 GHz 單核。
- RAM：1GB。
- 磁碟機子系統：4 GB 可用空間。

建議需求：

- 處理器：2.4 GHz 四核。
- RAM：2 GB。
- 磁碟機子系統：4 GB 可用空間。

伺服器的軟體需求

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 Security 10.1 for Windows Server。

為使 Kaspersky Security 10.1 for Windows Server 正常安裝和執行 ，伺服器必須先安裝 Microsoft Windows Installer 3.1。

您可以在執行以下 32 位元 Microsoft Windows 作業系統的伺服器上安裝 Kaspersky Security 10.1 for Windows Server：

- Windows Server® 2003 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 或更高版本
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 或更高版本

您可以在執行以下 64 位元 Microsoft Windows 作業系統的伺服器上安裝 Kaspersky Security 10.1 for Windows Server：

- Windows Server 2003 Standard / Enterprise / Datacenter SP2
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 或更高版本
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 或更高版本
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 或更高版本
- Windows Hyper-V® Server 2008 R2 SP1 或更高版本
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint Server 2011
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server
- Windows Server 2012 Core Standard / Datacenter
- Windows Storage Server 2012
- Windows Hyper-V Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Core Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server
- Windows Server 2016 Core Standard / Datacenter
- Windows Storage Server 2016
- Windows Hyper-V Server 2016

Microsoft Windows 不再支援以下作業系統：Windows Server 2003 Standard / Enterprise / Datacenter SP2、Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 32 位元/64 位元。在 Kaspersky Lab 方面，對執行這些作業系統的伺服器的技術支援可能有限制。

您可以在下列終端伺服器上安裝 Kaspersky Security 10.1 for Windows Server：

- 基於 Windows Server 2008 的 Microsoft 遠端桌面伺服器
- 基於 Windows Server 2008 R2 的 Microsoft 遠端桌面伺服器
- 基於 Windows Server 2012 的 Microsoft 遠端桌面伺服器
- 基於 Windows Server 2012 R2 的 Microsoft 遠端桌面伺服器
- 基於 Windows Server 2016 的 Microsoft 遠端桌面伺服器
- Citrix XenApp 6.0、6.5、7.0、7.5 - 7.9、7.15
- Citrix XenDesktop 7.0、7.1、7.5 - 7.9、7.15

網路附加儲存防護的需求

Kaspersky Security 10.1 for Windows Server 可以用來防護以下網路附加儲存：

- 帶有以下作業系統之一的 NetApp：
  - 在 7-mode 下的 Data ONTAP 7.x 和 Data ONTAP 8.x
  - 在叢集模式下的 Data ONTAP 8.2.1 或以上版本
- 含有以下軟體的 Dell™ EMC™ Celerra™ / VNX™：
  - EMC DART 6.0.36 或以上版本
  - Celerra (CAVA) Anti-Virus Agent 4.5.2.3 或以上版本
- 含有作業系統 OneFS™ 7.0 或更高版本系統的 DELL EMC Isilon™
- 在以下某一個平台上執行 Hitachi NAS：
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080
- IBM NAS 系列 IBM System Storage N 系列
- Oracle® NAS Systems 系列 Oracle ZFS Storage Appliance
- Dell Compellent™ FS8600 平台上的 Dell NAS

對安裝 Kaspersky Security 10.1 主控台的電腦需求

電腦的硬體需求

建議記憶體大小：最小 128 MB。

可用磁碟空間：30 MB。

電腦的軟體需求

您可以在執行 32 位元或 64 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Security 10.1 主控台。

為支援 Kaspersky Security 10.1 主控台的安裝和執行，該電腦應安裝有 Microsoft Windows Installer 3.1。

您可以在執行以下 32 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Security 10.1 主控台：

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 或更高版本
- Microsoft Windows XP Professional SP2 或更高版本
- Microsoft Windows Vista® Editions
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

您可以在執行以下 64 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Security 10.1 主控台：

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 或更高版本
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 或更高版本
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint™ Server 2011
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server
- Windows Storage Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server
- Windows Storage Server 2016
- Microsoft Windows XP Professional Edition SP2 或更高版本

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

功能要求和限制

本節介紹了 Kaspersky Security 10.1 for Windows Server 元件的其他功能要求和現有限制。

本章節說明項目

安裝和移除

- 在應用程式安裝過程中，如果新的 Kaspersky Security 10.1 for Windows Server 安裝資料夾的路徑包含的符號多於 150 個，將顯示一個警告。該警告不會影響安裝過程：Kaspersky Security 10.1 for Windows Server 將成功安裝並執行。
- 如果安裝 SNMP 協定支援元件，必須重新啟動 SNMP 服務（如果該服務正在執行）。
- 要在嵌入式作業系統管理的裝置上安裝和執行 Kaspersky Security 10.1 for Windows Server，必須安裝“篩選管理員”元件。
- 不能透過 Microsoft Active Directory® 群組政策安裝 Kaspersky Security 10.1 for Windows Server 管理工具。
- 在執行早期作業系統的電腦（不能接收定期更新）上安裝應用程式時，需要檢查以下根憑證：DigiCert Assured ID Root CA、DigiCert_High_Assurance_EV_Root_CA、DigiCertAssuredIDRootCA。缺少指定的憑證可導致應用程式執行不正確。建議以任何可能的方式安裝指定憑證。
- 無法透過“開始”功能表移除 Kaspersky Security 10.1 主控台。可以使用“**新增/移除程式**”視窗中的連結移除 Kaspersky Security 10.1 主控台。

流量安全

- 該元件只在執行高於 Microsoft Windows Server 2008 R2 的作業系統的伺服器上可用。
- 當使用加密權杖建立 Web 連線時，不能驗證流量。
- 不建議將 VPN 流量包括在防護範圍中（連接埠 1723）。
- 不能使用 IPv6 格式的 IP 位址碼。
- 如果在工作設定中選中了“**不信任具有無效憑證的 Web 伺服器**”核取方塊，應用程式會將自簽章憑證視為無效並封鎖此類連線。
- 應用程式只處理 TCP 封包。
- 郵件威脅防護不掃描傳出郵件流量。
- 建議在佈署“流量安全”元件之前安裝管理外掛程式，因為管理伺服器的網路代理在連線到應用程式時會偵測“流量安全”元件。如果在安裝管理外掛程式之前已安裝“流量安全”並且工作已啟動，請重新啟動“流量安全”工作。
- “流量安全”不適用於 Yandex.Disk、Dropbox。
- VPN 限制：透過 Microsoft VPN 連線合約工作時，可能出現問題。
- 如果在驅動程式攔截器模式下透過 KSC 執行安裝，“流量安全”會封鎖從 MMC 主控台到卡巴斯基安全管理中心伺服器的連線，就像該連線類型使用不受信任的憑證一樣。
- 該元件會封鎖連線到使用舊技術生成根憑證（例如，sha1 憑證）的網站。
- “**不掃描大於以下大小的物件**”值不能超過 100Mb。如果指定了較大值，並且 Internet 連線速度較慢，接收大檔案可能會有困難。推薦值為 20 Mb。
- 如果滿足以下條件，應用程式會將 HTTPS 連線辨識為危險連線並封鎖它們：
  - 工作在“**驅動程式攔截器**”模式下執行。
  - 流量從外部裝置重定向。
  - 重定向流量所來自的裝置受 Kaspersky Security 10.1 for Windows Server 防護，並且預設“流量安全”工作已執行至少一次。

我們不推薦使用“**重定向器**”模式檢查從外部電腦重定向的流量：除了前面提到的誤報外，此設定還可能導致伺服器負載高並降低應用程式效能。

檔案完整性監控

預設情況下，“檔案完整性監控”不監控系統資料夾或檔案系統內務檔案的變更，以防止有關常式檔案變更（由作業系統不斷執行）的資訊進入工作報告。使用者不能手動將此類資料夾包括在監控範圍內。

以下資料夾/檔案排除在監控範圍之外：

- 檔案 ID 為 0 至 33 的 NTFS 內務檔案

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

應用程式排除頂級資料夾。

該元件不監控繞過 ReFS/NTFS 檔案系統的檔案變更（透過 BIOS、LiveCD 等進行的檔案變更）。

防火牆管理

- 當指定的套用規則範圍只包含一個位址時，不能使用 IPv6 格式的 IP 位址。
- 預設防火牆政策規則保證了在本機電腦和管理伺服器之間進行互動的基本方案的執行。要完全使用卡巴斯基安全管理中心功能，需要手動設定連接埠規則。有關連接埠號、協定及其功能的資訊包含在卡巴斯基安全管理中心知識庫（文章 ID：9297）中。
- 如果在安裝應用程式時未將 Windows 防火牆規則和規則群組新增到工作設定中，則在防火牆管理工作的不斷查詢期間，應用程式不會控制這些規則的修改。要更新狀態並包括此類別規則，必須重新啟動防火牆管理工作。

- 對於 Microsoft Windows Server 系列作業系統、2008 及更高版本：必須在安裝“防火牆管理”元件之前啟動 Windows 防火牆服務（預設啟動）。
- “防火牆管理”工作啟動時，會自動從作業系統的防火牆設定中移除以下類型的規則：
  - 拒絕規則；
  - 監控傳出流量的規則。

其他限制

自訂掃描、即時檔案防護：

- 在連線掃描時 MTP 裝置不可用。
- 不進行 SFX 壓縮檔案掃描則無法進行壓縮檔案物件掃描：如果在 Kaspersky Security 10.1 for Windows Server 的防護設定中啟用了壓縮檔案掃描，則應用程式會自動掃描壓縮檔案和 SFX 壓縮檔案中的物件。不進行壓縮檔案物件掃描時可進行 SFX 壓縮檔案掃描。

電腦控制和診斷：

- 如果受防護伺服器執行的作業系統是 Microsoft Windows Server 2008 R2 或更高版本，則“裝置控制”工作的防護範圍包括 MTP 連線裝置。
- “記錄審查”工作僅在執行 Windows Server 2008 或更高版本並已安裝更新且作為網域控制器的電腦上偵測潛在的 Kerberos 攻擊模式 (MS14-068)。

授權：

- 如果金鑰位於使用 SUBST 指令建立的磁碟上，或者如果指定了金鑰檔案的網路路徑，則不能透過安裝精靈使用金鑰啟動應用程式。

更新：

- 安裝 Kaspersky Security 10.1 for Windows Server 關鍵模組更新後，應用程式圖示預設處於隱藏狀態。
- 執行 Windows XP 或 Windows Server 2003 作業系統的電腦不支援 KLRAMDISK。

介面：

- 在 Kaspersky Security 10.1 主控台中，如果在“隔離”、“備份”、“系統稽核記錄”或“工作記錄”工作中使用篩選，應該保留大小寫。
- 在 Kaspersky Security 10.1 主控台中配置防護範圍或掃描範圍時，只能在路徑末尾使用一個遮罩。正確的遮罩使用範例：“C:\Temp\Temp*”或“C:\Temp\Temp???.doc”或“C:\Temp\Temp*.doc”。限制不影響信任區域配置。

安全性：

- 如果作業系統設定中的使用者帳戶控制已啟動，使用者帳戶必須屬於 KAVWSEE 管理員群組才能透過按兩下工作列通知區域中的應用程式圖示來開啟 Kaspersky Security 10.1 主控台。在其他情況下，將開啟“關於應用程式”視窗。
- 如果使用者帳戶控制已啟動，則不能透過 Microsoft Windows 的“程式和功能”視窗移除應用程式。

與卡巴斯基安全管理中心整合：

- 管理伺服器在收到更新套件後和將更新傳送到網路電腦之前，會檢查資料庫更新的有效性。管理伺服器不檢查收到的軟體模組更新的有效性。
- 當使用借助網路清單將動態變化的資料傳送到卡巴斯基安全管理中心的元件時（“隔離”、“備份”），確保在“與管理伺服器互動”設定中已選中必需核取方塊。

弱點利用防禦：

- 如果目前環境配置中未載入 apphelp.dll 庫，則弱點利用防禦不可用。
- “弱點利用防禦”元件與執行 Microsoft Windows 10 作業系統的電腦上的 Microsoft EMET 實用工具不相容：如果在已安裝 EMET 的電腦上安裝“弱點利用防禦”元件，Kaspersky Security 10.1 for Windows Server 將封鎖 EMET。

用於 NetApp 的加密勒索軟體防護：

- 如果將 FlexGroup 容器用於執行新作業系統（ONTAP 9 及更高版本）的 NAS，則無法為這些伺服器提供加密勒索軟體防護。
- 網路附加儲存 NetApp 上的檔案威脅偵測功能在 7-mode 下受限。
- 用於 NetApp 的加密勒索軟體防護只在叢集模式下可用。
- 一個伺服器只能使用一個網路介面和一個 IP v4 位址。

封鎖的主機儲存：啟用“加密勒索軟體防護”或“即時檔案防護”元件後持續執行。

ICAP-網路儲存防護：受防護儲存的內容的管理取決於儲存設定。例如，如果儲存不允許移除偵測到的受感染物件，則無法執行此操作。HP 3Par 儲存只能工作在封鎖存取模式下。無法使用信任區域。

RPC-網路儲存防護：Active Directory 是叢集模式必需的。

KSN 使用：對於 Windows Vista 及更早版本，此元件不支援網頁防護和郵件防護的統計資訊。

安裝和移除應用程式

本節提供安裝和移除 Kaspersky Security 10.1 for Windows Server 的逐步說明。

本章內容

Kaspersky Security 10.1 for Windows Server 軟體元件及對應的 Windows Installer 服務代碼

預設情況下，\server\ks4ws_x86(x64).msi 檔案會安裝所有 Kaspersky Security 10.1 for Windows Server 元件。您可透過在自訂安裝中包含此元件來安裝它。

\client\ks4wstools_x86(x64).msi 檔案安裝“管理工具”集內所有的軟體元件。

下列各節列出適用於 Windows Installer 服務的 Kaspersky Security 10.1 for Windows Server 元件代碼。透過命令列安裝 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 軟體元件

下表含有 Kaspersky Security 10.1 for Windows Server 軟體元件的代碼和說明。

表 3. Kaspersky Security 10.1 for Windows Server 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伺服器的嘗試，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。
流量安全	WebGW	此元件處理 Web 流量（包括透過郵件服務接收的流量）並攔截並掃描透過 Web 流量傳輸的物件，以偵測已知電腦和受防伺服器上的其他威脅。
病毒防護	AVProtection	此元件確保防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 Security 10.1 for Windows Server 系統檔案和自訂掃描工作（依要求掃描受防護伺服器的物件）。 如果您從命令列安裝 Kaspersky Security 10.1 for Windows Server 時，指定其他 Kaspersky Security 10.1 for Windows Server 元件，但未指定 Core 元件，將自動安裝 Core 元件。
即時檔案防護	Oas	此元件在受防護伺服器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。
卡巴斯基安全網路的使用	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，以便防護受防護伺服器記憶體中的處理程序所使用的記憶體。

元件	代碼	執行功能
防火牆管理	Firewall	此元件可透過 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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，請在受防護伺服器上安裝此元件。
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。
RPC-網路儲存防護	RPCProt	此元件防護 RPC-網路儲存（範例 NetApp 網路附加儲存），使其免受病毒以及透過檔案交換方式侵入伺服器的其他電腦安全威脅。
ICAP-網路儲存防護	ICAPProt	此元件防護 ICAP-網路儲存（範例 EMC Isilon），使其免受病毒危害和透過檔案交換方式侵入伺服器的其他安全威脅。
用於 NetApp 的加密勒索軟體防護	AntiCryptorNAS	此元件為網路附加儲存上的資料夾提供加密防護。如果偵測到任何惡意加密，Kaspersky Security 10.1 for Windows Server 將封鎖對受防護網路附加儲存的資料夾的存取。
“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器效能計數器。效能計數器可用來衡量 Kaspersky Security 10.1 for Windows Server 的效能，並在使用 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 計數器與 TRAP。伺服器上需先安裝 Microsoft SNMP，才能安裝此元件。
通知區域中的 Kaspersky Security 10.1 for Windows Server 圖示	TrayApp	此元件在受防護伺服器的工作列通知區域顯示 Kaspersky Security 10.1 for Windows Server 圖示。Kaspersky Security 10.1 for Windows Server 圖示除了會顯示伺服器防護的狀態，還可在 MMC（如果已安裝）中開啟 Kaspersky Security 10.1 主控台及“關於程式”視窗。
命令列實用工具	Shell	可透過受防護伺服器的命令列管理 Kaspersky Security 10.1 for Windows Server。

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。

表 4. “管理工具”軟體元件說明

元件	代碼	元件功能
Kaspersky Security 10.1 for Windows Server 管理單元	MmcSnapin	此元件透過 Kaspersky Security 10.1 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。
Help	Help	.chm 說明檔案，儲存在 Kaspersky Security 10.1 for Windows Server 管理工具檔案資料夾中。您可以使用“**開始**”功能表或透過在 Kaspersky Security 10.1 主控台視窗處於開啟狀態時按 **F1** 鍵，來開啟說明檔案。
文件	Docs	Kaspersky Security 10.1 for Windows Server 在受防護伺服器上儲存了 PDF 格式的《網路附加儲存防護實施手冊》、《管理手冊》和《使用者手冊》。您可從“**開始**”功能表開啟所有手冊。

Kaspersky Security 10.1 for Windows Server 安裝後的系統變更

當您將 Kaspersky Security 10.1 for Windows Server 和 Kaspersky Security 10.1 主控台（管理工具）一起安裝時，Windows Installer 服務將對電腦作出下列變更：

- 在受防護伺服器與安裝 Kaspersky Security 10.1 主控台的電腦上建立 Kaspersky Security 10.1 for Windows Server 資料夾。
- 註冊 Kaspersky Security 10.1 for Windows Server 服務。
- 建立 Kaspersky Security 10.1 for Windows Server 使用者群組。
- 在系統登錄檔中註冊 Kaspersky Security 10.1 for Windows Server 項。

這些變更在下表說明。

Kaspersky Security 10.1 for Windows Server 資料夾

表 5. 受防護伺服器上的 Kaspersky Security 10.1 for Windows Server 資料夾

資料夾	Kaspersky Security 10.1 for Windows Server 檔案
資料夾 %Kaspersky Security 10.1 for Windows Server%；預設情況下： 在 Microsoft Windows 32 位元版本中 – %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server\ 在 Microsoft Windows 64 位元版本中 – %ProgramFiles(x86)%\Kaspersky Security 10.1 for Windows Server\	Kaspersky Security 10.1 for Windows Server 可執行檔（安裝期間指定的目的資料夾）。
%Kaspersky Security 10.1 for Windows Server%\mibs 資料夾	管理資訊庫 (MIB) 檔案，這些檔案包含 Kaspersky Security 10.1 for Windows Server 透過 SMNP 通訊協定發佈的計數器與 TRAP 說明。
%Kaspersky Security 10.1 for Windows Server%\x64 資料夾	64 位元版本 Kaspersky Security 10.1 for Windows Server 可執行檔（只有在 64 位元 Microsoft Windows 版本下安裝 Kaspersky Security 10.1 for Windows Server 期間才會建立此資料夾）。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Security for Windows Server\10.1\Dskm\	Kaspersky Security 10.1 for Windows Server 服務檔案。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\	更新來源設定檔。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\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 Security for Windows Server\10.1\Reports\	工作記錄和系統稽核記錄。

資料夾	Kaspersky Security 10.1 for Windows Server 檔案
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Current\	目前使用的資料庫。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\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 Security for Windows Server\10.1\Bases\Temp\	執行更新工作時所建立的暫存檔。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Quarantine\	隔離的物件（預設資料夾）。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Backup\	備份中的物件（預設資料夾）。
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored\	從備份儲存和隔離還原的物件（還原物件的預設資料夾）。

表 6. 安裝 Kaspersky Security 10.1 主控台時所建立的資料夾

資料夾	Kaspersky Security 10.1 for Windows Server 檔案
資料夾 %Kaspersky Security 10.1 for Windows Server%；預設情況下： • 在 Microsoft Windows 32 位元版本中 – %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server\ 在 Microsoft Windows 64 位元版本中 – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server\	“管理工具”檔案（安裝 Kaspersky Security 10.1 主控台時指定的目標資料夾）。

Kaspersky Security 10.1 for Windows Server 服務

使用“本機系統（SYSTEM）”帳戶啟動的 Kaspersky Security 10.1 for Windows Server 服務。

表 7. Kaspersky Security 10.1 for Windows Server 服務

服務	用途
Kaspersky Security Service (KAVFS) 服務	管理 Kaspersky Security 10.1 for Windows Server 工作和工作流的基本 Kaspersky Security 10.1 for Windows Server 服務

服務	用途
Kaspersky Security Management Service (KAVFSGT)	此服務用於透過 Kaspersky Security 10.1 主控台進行 Kaspersky Security 10.1 for Windows Server 應用程式管理
Kaspersky Security Broker 服務 (KAVFSWH)	一種服務，作為將安全設定傳輸給外部安全代理並接收有關安全事件資料的中間層。
Kaspersky Security Script Checker (KAVFSSCS)	此服務和“指令碼監控”工作一起啟動，並且允許控制使用 Microsoft Windows 指令碼技術建立的指令碼的執行。

Kaspersky Security 10.1 for Windows Server 群組

表 8. Kaspersky Security 10.1 for Windows Server 群組

群組	用途
KAVWSEE 管理員	受防護伺服器上的一個群組，其中的使用者有權存取 Kaspersky Security Management Service 和 Kaspersky Security 10.1 for Windows Server 所有的功能。

系統登錄註冊參數

表 9. 系統登錄註冊參數

鍵	用途
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Kaspersky Security 10.1 for Windows Server 服務內容。
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Kaspersky Security 10.1 for Windows Server 事件記錄設定（Kaspersky 事件記錄）。
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Kaspersky Security 10.1 for Windows Server 管理服務內容。
Microsoft Windows 32 位元版本： [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] Microsoft Windows 64 位元版本： [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\WSEE\10.1\SnmpAgent] Microsoft Windows 64 位元版本： [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\SnmpAgent]	SNMP 協定支援元件設定。

鍵	用途
Microsoft Windows 32 位元版本： HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump\ Microsoft Windows 64 位元版本： HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump\	Dump 檔案寫設定。
Microsoft Windows 32 位元版本： HKEY_LOCAL_MACHINE\Software\KasperskyLab\WSEE\10.1\Trace\ Microsoft Windows 64 位元版本： HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.1\Trace\	偵錯記錄設定。
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Environment]	應用程式的工作和功能的配置。

Kaspersky Security 10.1 for Windows Server 處理程序

Kaspersky Security 10.1 for Windows Server 將啟動下表中敘述的處理程序。

表 10. Kaspersky Security 10.1 for Windows Server 處理程序

檔案名稱	用途
kavfswp.exe	Kaspersky Security 10.1 for Windows Server 工作流。
kavtray.exe	Kaspersky Security 10.1 for Windows Server 工作列圖示的處理程序。
kavshell.exe	命令列實用工具處理程序
kavfsrcn.exe	Kaspersky Security 10.1 for Windows Server 遠端管理處理程序。
kavfs.exe	Kaspersky Security Service 處理程序
kavfsgt.exe	Kaspersky Security Management Service 處理程序
kavfswh.exe	Kaspersky Security Broker 主機服務外部控制流程
kavfsscs.exe	Kaspersky Security Script Checker Service

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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 時，您可以使用參數及 Windows Installer 服務中 msiexec 指令適用的標準指令。

表 11. Windows Installer 中的安裝參數和命令列選項

設定	預設值	Windows Installer 命令列選項及其可能值	敘述
接受最終使用者授權協議條款	不同意接受使用者授權合約。	EULA=<設定值> 0 - 不同意接受使用者授權協議條款。 1 - 同意接受使用者授權協議條款。	您必須接受最終使用者授權協議條款，才能安裝 Kaspersky Security 10.1 for Windows Server。
接受隱私政策條款	拒絕隱私政策條款	PRIVACYPOLICY=<值> 0 – 拒絕隱私政策條款。 1 – 接受隱私政策條款。	您必須接受隱私政策條款，才能安裝 Kaspersky Security 10.1 for Windows Server。
目的資料夾	Kaspersky Security 10.1 for Windows Server：%ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server 管理工具：%ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server Admins Tools 在 x64 位元版本的 Microsoft Windows 中：%ProgramFiles(x86)%。	INSTALLDIR=<資料夾完整路徑>	安裝過程中將儲存在 Kaspersky Security 10.1 for Windows Server 檔案的資料夾。 您可指定不同的資料夾。
Kaspersky Security 10.1 for Windows Server 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**）	啟動	RUNRTP=<設定值> 1 - 啟動； 0 - 不啟動。	開啟該設定，在 Kaspersky Security 10.1 for Windows Server 啟動時啟動即時檔案防護和指令碼監控（推薦）。

設定	預設值	Windows Installer 命令列選項及其可能值	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**）	排除	ADDMSEXCLUSION=<設定值> 1 - 排除; 0 - 不排除。	在“即時檔案防護”範圍中排除 Microsoft Corporation 推薦伺服器排除的物件。 當防毒應用程式攔截或修改檔案時，伺服器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**）	排除	ADDKLEXCLUSION=<設定值> 1 - 排除; 0 - 不排除。	在“即時檔案防護”範圍中排除 Kaspersky Lab 推薦伺服器排除的物件。
允許遠端連線到 Kaspersky Security 10.1 主控台。	拒絕	ALLOWREMOTECON= <值> 1 - 允許； 0 - 拒絕。	預設情況下，不允許遠端連線到安裝在受防護電伺服器上的 Kaspersky Security 10.1 主控台。安裝過程中，可允許連線。Kaspersky Security 10.1 for Windows Server 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。

設定	預設值	Windows Installer 命令列選項及其可能值	敘述
金鑰檔案的路徑（**金鑰**）	發行套件中的 \server 目錄	LICENSEKEYPATH=<金鑰檔案名稱>	預設情況下，安裝程式會嘗試尋找分發套件的 \server 資料夾中是否有副檔名為 .key 的檔案。 如果 \server 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 \server 資料夾中，或使用“**新增金鑰**”設定指定另一個檔案路徑。 安裝 Kaspersky Security 10.1 for Windows Server 後，您也可以選擇透過管理工具（例如 Kaspersky Security 10.1 主控台）加入金鑰。如果您在應用程式安裝期間未新增金鑰，Kaspersky Security 10.1 for Windows Server 將不會發揮功能。
設定檔路徑	未指定	CONFIGPATH=<設定檔名稱>	Kaspersky Security 10.1 for Windows Server 從在應用程式中建立的指定設定檔匯入設定。 Kaspersky Security 10.1 for Windows Server 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	預設值	Windows Installer 命令列選項及其可能值	敘述
啟用主控台的網路連線	已停用	ADDWFEXCLUSION=<設定值> **1** - 允許； **0** - 拒絕。	使用該選項在另一台伺服器上安裝 Kaspersky Security 10.1 for Windows Server。您可以從安裝了 Kaspersky Security 10.1 主控台的另一台電腦遠端管理電腦防護。 在 Microsoft Windows 防火牆中開啟連接埠 135 (TCP)，允許透過網路連線 Kaspersky Security 10.1 for Windows Server 遠端管理的執行檔 kavfsrcn.exe，並允許存取 DCOM 應用程式。 安裝完成後，將使用者新增到“KAVWSEE 管理員”群組中，以允許他們遠端管理應用程式（如果伺服器在 Microsoft Windows Server 2008 上執行）並允許透過網路連線到電腦上的 Kaspersky Security Management Service（kavfsgt.exe 檔案）。 您可以閱讀有關 Kaspersky Security 10.1 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 50 頁上的“在其他電腦上安裝 Kaspersky Security 10.1 主控台以後的進階設定”部分）。
停用不相容軟體檢查	檢查已執行	SKIPINCOMPATIBLESW = <值> 0 - 不相容軟體檢查已執行 1 - 不相容軟體檢查未執行	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 Security 10.1 for Windows Server 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。

表 12. Windows Installer 中的移除設定和命令列選項

設定	預設值	敘述、Windows Installer 命令列選項及其可能值
還原隔離的物件	刪除	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。
還原備份儲存區內容	刪除	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。
輸入目前密碼以確認刪除(如果已啟用密碼防護)	未指定	UNLOCK_PASSWORD=<指定的密碼>
還原物件的資料夾	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored	RESTOREPATH=<資料夾完整路徑> 還原的物件將儲存在此設定所指定的資料夾中： 隔離的物件將儲存在 \Quarantine 子資料夾中。 備份物件 - 儲存在 \Backup 子資料夾中。

Kaspersky Security 10.1 for Windows Server 安裝和移除記錄

如果您透過安裝/解除安裝精靈來安裝或解除安裝 Kaspersky Security 10.1 for Windows Server，Windows Installer 服務會建立一個安裝（解除安裝）記錄檔。ks4ws_install_<uid>.log 記錄檔（其中 <uid> 是八個字元的唯一記錄識別碼）將儲存在啟動 setup.exe 檔之使用者帳戶下的 %temp% 資料夾中。

預設情況下，若您是從命令列安裝或解除安裝 Kaspersky Security 10.1 for Windows Server，就不會建立該安裝檔記錄。

► *要安裝 Kaspersky Security 10.1 for Windows Server 並在磁碟 C:\ 上建立記錄檔案 ks4ws.log：*

- msiexec /i ks4ws_x86.msi /l*v C:\log.txt /qn EULA=1
- msiexec /i ks4ws_x64.msi /l*v C:\log.txt /qn EULA=1

安裝排程

本節包含 Kaspersky Security 10.1 for Windows Server 管理工具集的說明以及 Kaspersky Security 10.1 for Windows Server 安裝和移除的特殊方面：使用精靈（請參見第 46 頁上的“基於精靈安裝和移除應用程式”部分）、命令列（請參見第 58 頁上的“透過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 63 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 67 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 Security 10.1 for Windows Server 之前，請先規劃它的安裝排程。

1. 確定您要用來管理 Kaspersky Security 10.1 for Windows Server 及其設定的管理工具。
2. 選擇必須安裝的產品元件（請參閱第 31 頁“Kaspersky Security 10.1 for Windows Server 軟體元件及對應的 Windows Installer 服務代碼”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 Security 10.1 for Windows Server 的管理工具。您可使用 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 。

Kaspersky Security 10.1 主控台

Kaspersky Security 10.1 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伺服器或公司網路中其他電腦上的 Kaspersky Security 10.1 主控台來管理 Kaspersky Security 10.1 for Windows Server。

您可以將多個 Kaspersky Security 10.1 for Windows Server 管理元件新增到在授權模式中開啟單獨的 Microsoft 管理主控台中，以便用它來管理多台已安裝 Kaspersky Security 10.1 for Windows Server 的伺服器防護。

Kaspersky Security 10.1 主控台含在產品元件的“管理工具”群組中。

命令列實用工具

您可透過受防護伺服器的命令列來管理 Kaspersky Security 10.1 for Windows Server。

命令列實用工具含在 Kaspersky Security 10.1 for Windows Server 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，您可使用管理中心的管理主控台來管理 Kaspersky Security 10.1 for Windows Server。

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**。此元件包含在 Kaspersky Security 10.1 for Windows Server 的軟體元件群組中。它可確保 Kaspersky Security 10.1 for Windows Server 與網路代理的通信。請在受防護伺服器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**。請在每一台受防護伺服器上安裝此程式。該元件支援伺服器上安裝的 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server。此外掛程式透過卡巴斯基安全管理中心來管理應用程式。此外掛程式安裝檔案 \server\klcfginst.exe 包含在 Kaspersky Security 10.1 for Windows Server 分發套件中。

選擇安裝類型

指定 Kaspersky Security 10.1 for Windows Server 安裝的軟體元件後（請參閱第 31 頁“Kaspersky Security 10.1 for Windows Server 軟體元件及對應的 Windows Installer 服務代碼”部分）。

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 Security 10.1 for Windows Server 安裝設定，還是將使用推薦的安裝設定（請參見第 38 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）。
- 所有伺服器是否採用相同的安裝設定或個別為每個伺服器使用不同的設定。

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 Security 10.1 for Windows Server。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 Security 10.1 for Windows Server。

您可在單一伺服器上安裝 Kaspersky Security 10.1 for Windows Server、設定操作模式或將設定值儲存到設定檔中，之後在其他伺服器上使用建立的檔案來安裝 Kaspersky Security 10.1 for Windows Server（但若使用 Active Directory 群組政策安裝產品，此功能將不適用）。

啟動安裝精靈

您可使用安裝精靈安裝下列內容：

- 將 Kaspersky Security 10.1 for Windows Server 元件（請參加第 32 頁上的“Kaspersky Security 10.1 for Windows Server 軟體元件”部分）從分發套件中包含的 \server\setup.exe 檔案安裝到受防護伺服器上。
- 將 Kaspersky Security 10.1 主控台（請參見第 49 頁上的“Kaspersky Security 10.1 主控台安裝”部分）從安裝套件的 \client\setup.exe 檔案安裝到受防護伺服器或其他 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 Security 10.1 for Windows Server 將以預設設定安裝。可以使用 Kaspersky Security 10.1 for Windows Server 選項修改安裝設定。

您可在受防護伺服器和/或管理員工作站上安裝 Kaspersky Security 10.1 主控台。

Kaspersky Security 10.1 for Windows Server 和 Kaspersky Security 10.1 主控台的安裝範例指令可以在“從命令列安裝和移除 Kaspersky Security 10.1 for Windows Server”部分中找到（請參見第 58 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

若您在網路上使用卡巴斯基安全管理中心管理電腦上的病毒防護工作，便可使用管理中心的遠端安裝工作將 Kaspersky Security 10.1 for Windows Server 安裝在多台伺服器上。

您希望透過卡巴斯基安全管理中心安裝 Kaspersky Security 10.1 for Windows Server（請參見第 63 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）的伺服器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 群組政策在受防護伺服器上安裝 Kaspersky Security 10.1 for Windows Server。您可在受防護伺服器或管理員工作站上安裝 Kaspersky Security 10.1 主控台。

您可使用預設的安裝設定安裝 Kaspersky Security 10.1 for Windows Server。

使用 Active Directory 群組政策安裝 Kaspersky Security 10.1 for Windows Server （請參見第 67 頁上的“透過 Active Directory 群組政策安裝和移除”部分）的伺服器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 Security 10.1 for Windows Server 和 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 和 Kaspersky Security 10.1 主控台的資訊。

► *若要安裝及使用 Kaspersky Security 10.1 for Windows Server，請執行以下步驟：*

1. 在受防護伺服器上安裝 Kaspersky Security 10.1 for Windows Server。
2. 在您打算用來管理 Kaspersky Security 10.1 for Windows Server 的電腦上安裝 Kaspersky Security 10.1 主控台。
3. 如果 Kaspersky Security 10.1 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伺服器上，請執行額外調整以允許主控台使用者遠端管理 Kaspersky Security 10.1 for Windows Server。
4. 在安裝 Kaspersky Security 10.1 for Windows Server 後執行的操作。

本章節說明項目

Kaspersky Security 10.1 for Windows Server 安裝

在安裝 Kaspersky Security 10.1 for Windows Server 之前，請執行以下步驟：

- 確認電腦上未安裝任何防毒程式。無需移除 Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition 或 Kaspersky Security 10 for Windows Server 即可安裝 Kaspersky Security 10.1 for Windows Server。
- 確認用來啟動安裝精靈的帳戶已登錄到受防護伺服器上的管理員群組中。

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 Security 10.1 for Windows Server 的設定。您可在任何安裝步驟停止 Kaspersky Security 10.1 for Windows Server 安裝程序。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 38 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 Security 10.1 for Windows Server：*

1. 在伺服器上啟動歡迎檔案 setup.exe。
2. 在開啟的視窗中的“安裝”部分，點擊“**安裝 Kaspersky Security 10.1 for Windows Server**”連結。
3. 在 Kaspersky Security 10.1 for Windows Server 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，請選中“**此 EULA 的條款和條件**”和“**敘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。

   如果伺服器已安裝任何相容版本的應用程式，將開啟“**已偵測到程式的先前版本**”視窗。

   如果未偵測到先前版本的應用程式，則執行這些說明的第 8 步。
7. 要從應用程式的先前版本升級，請點擊“**安裝**”按鈕。安裝精靈會將應用程式升級到 Kaspersky Security 10.1 for Windows Server，並在新版本中儲存相容設定。升級完成後，安裝精靈將開啟“**完全安裝**”視窗（繼續執行本指示的步驟 15）。

   “**在安裝前快速掃描電腦**”視窗將開啟。

8. 在“**在安裝前快速掃描電腦**”中，選中“**掃描電腦病毒**”核取方塊，執行系統記憶體及本機伺服器磁碟開機磁區的防毒掃描。點擊“**下一步**”按鈕。完成掃描程序時，該精靈會開啟一個結果報告視窗。

   此視窗顯示有關已掃描伺服器物件有關的資訊，包括：已掃描的物件總數、偵測到的威脅類型數目、偵測到的已感染和可疑物件數目、Kaspersky Security 10.1 for Windows Server 從記憶體中刪除的危險或可疑處理程序數目，以及此應用程式無法刪除的危險和可疑處理程序數目。

   若要檢視掃描的物件有哪些，請按下“**已處理物件清單**”按鈕。

9. 點擊“**在安裝前快速掃描電腦**”視窗中的“**下一步**”按鈕。

   將開啟“**自訂安裝**”視窗。

10. 請選擇您想安裝的元件，

    預設情況下，推薦安裝集包括除防火牆管理和指令碼監控元件外的所有 Kaspersky Security 10.1 for Windows Server 元件。

    > 只有在伺服器安裝了 Microsoft Windows SNMP 服務的情況下，推薦的安裝元件清單中才會出現 Kaspersky Security 10.1 for Windows Server 的 “SNMP 通訊協定支援”元件。

11. 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。
12. 在“**選擇目的資料夾**”視窗中：
    - 如有需要，請指定另一個 Kaspersky Security 10.1 for Windows Server 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。
13. 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。
14. 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 Security 10.1 for Windows Server 設定。
    b. 點擊“**下一步**”按鈕。
15. 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 Security 10.1 for Windows Server 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。

您無法透過安裝精靈使用啟動碼啟動應用程式。如果您想要使用啟動碼啟動應用程式，您需要在安裝後輸入啟動碼。

新增金鑰檔案後，視窗中將顯示授權資訊。Kaspersky Security 10.1 for Windows Server 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。

16. 在“**已準備好安裝**”視窗中按“安裝”按鈕。精靈將開始安裝 Kaspersky Security 10.1 for Windows Server 元件。
17. 完成安裝時，會開啟“**安裝完成**”視窗。
18. 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。
19. 點擊“**確定**”。

將關閉“安裝精靈”視窗。完成安裝時，就可以使用 Kaspersky Security 10.1 for Windows Server （若已新增啟動金鑰）。

Kaspersky Security 10.1 主控台安裝

依照安裝精靈的指示，調整 Kaspersky Security 10.1 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，請在精靈視窗中點擊“**取消**”。

► *要安裝 Kaspersky Security 10.1 主控台，請執行下列步驟：*

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 Security 10.1 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授權協議和隱私政策的條款，並選擇**此 EULA 的條款和條件**和**敘述資料處理的隱私政策**，以繼續安裝。點擊“**下一步**”按鈕。
5. 在“**進階安裝設定**”視窗中：
   - 如果您想使用 Kaspersky Security 10.1 主控台管理遠端電腦上安裝的 Kaspersky Security 10.1 for Windows Server，請核取“**允許遠端存取**”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 Security 10.1 for Windows Server 軟體元件的更多詳細資訊（請參閱第 31 頁上的“Kaspersky Security 10.1 for Windows Server 軟體元件及對應的 Windows Installer 服務代碼”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“**已準備好安裝**”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。在受防護伺服器上安裝 Kaspersky Security 10.1 主控台。

如果您是在另一台電腦上安裝“管理工具”集，而不是在受防護伺服器上安裝，請進行“進階設定”（請參閱第 50 頁上的“在其他電腦上安裝 Kaspersky Security 10.1 主控台以後的進階設定”部分）。

在其他電腦上安裝 Kaspersky Security 10.1 主控台的進階設定

如果 Kaspersky Security 10.1 主控台已經安裝在其他電腦上，而不是安裝在受防護伺服器上，請執行下述操作，以允許使用者遠端系統管理 Kaspersky Security 10.1 for Windows Server：

- 在受防護的伺服器上將 Kaspersky Security 10.1 for Windows Server 使用者新增到 KAVWSEE 管理員群組中。
- 如果受防護伺服器使用 Windows 防火牆或協力廠商防火牆，則允許 Kaspersky Security Management Service (kavfsgt.exe) 進行網路連線。
- 如果在執行 Microsoft Windows 的電腦上安裝 Kaspersky Security 10.1 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 Kaspersky Security 10.1 主控台的網路連線。

本章節說明項目

關於 Kaspersky Security Management Service 的存取權限

> 您可以檢視 Kaspersky Security 10.1 for Windows Server 服務的清單。

在安裝過程中，Kaspersky Security 10.1 for Windows Server 會註冊 Kaspersky Security 10.1 for Windows Server 管理服務 (KAVFSGT)。若要透過安裝在其他電腦上的 Kaspersky Security 10.1 主控台來管理程式，使用其權限與 Kaspersky Security 10.1 for Windows Server 建立連線的帳戶必須對受防護伺服器上的 Kaspersky Security 10.1 for

Windows Server 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所有 Kaspersky Security Management Service 的權限：受防護伺服器上的管理員群組的使用者，以及安裝 Kaspersky Security 10.1 for Windows Server 時在受防護伺服器上建立的 KAVWSEE 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 Management Service。

您不能透過配置 Kaspersky Security 10.1 for Windows Server 來允許或封鎖使用者存取 Kaspersky Security 10.1 for Windows Server 管理服務。

如果在受防護的伺服器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 Security 10.1 for Windows Server。

允許 Kaspersky Security 10.1 主控台的網路連線

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

遠端電腦上的 Kaspersky Security 10.1 主控台將使用 DCOM 協議從受防護伺服器上的 Kaspersky Security 10.1 for Windows Server 管理服務接收關於 Kaspersky Security 10.1 for Windows Server 的事件資訊（物件掃描、工作完成等等）。需要在“Windows 防火牆設定”中允許透過網路連線 Kaspersky Security 10.1 主控台，才能在 Kaspersky Security 10.1 主控台和 Kaspersky Security 10.1 for Windows Server 管理服務之間建立連線。

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 防火牆上打開 TCP 135 連接埠並允許 Kaspersky Security 10.1 for Windows Server 遠端系統管理程序的可執行檔 kavfsrcn.exe 的網路連線。

  安裝 Kaspersky Security 10.1 主控台的用戶端電腦將使用連線埠 TCP 135 存取受防護伺服器並接收伺服器回應。

如果在配置受防護伺服器與已安裝 Kaspersky Security 10.1 主控台伺服器之間的連線時主控台已經開啟，則請關閉 Kaspersky Security 10.1 主控台，等待 Kaspersky Security 10.1 for Windows Server 遠端系統管理程序 kavfsrcn.exe 結束，然後再重新啟動主控台。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 Kaspersky Security 10.1 主控台的伺服器上，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. 展開伺服器上元件服務主控台中的“**電腦**”節點。
6. 開啟“**我的電腦**”節點的上下文功能表。
7. 選擇“**內容**”。
8. 在“**內容**”視窗的“**COM 安全性**”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**”。

► *若要開啟 Windows 防火牆中的連接埠 TCP 135 並允許到 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 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**”欄位中指定部件名稱 RPC (TCP/135) 或輸入其他名稱，例如“Kaspersky Security 10.1 for Windows Server DCOM”，並在“**埠號名稱**”欄位中指定埠號 (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 > 主控台 > Windows 防火牆**”。在“**Windows 防火牆**”視窗中，選擇“**允許程式或功能透過 Windows 防火牆**”。
     b. 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。在使用 MMC 安裝 Kaspersky Security 10.1 主控台的過程中，該檔案位於指定為目的資料夾的資料夾中。
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。

為 Kaspersky Security Management Service 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。

若要建立 Kaspersky Security 10.1 主控台與 Kaspersky Security Management Service 之間的連線，您需要允許服務的網路連線透過受防護伺服器上的防火牆。

如果 Kaspersky Security 在 Microsoft Windows Server 2003/2008/2012/2012 R2 下執行，則需設定網路連線。

► *要為 Kaspersky Security Management Service 允許網路連線：*

1. 在執行於 Windows Server 下的受防護伺服器上，選擇“**開始 > 主控台 > 安全 > Windows 防火牆**”。
2. 在“**Windows 防火牆設定**”視窗中，選擇“**變更設定**”指令。
3. 在“**排除**”標籤的預定例外清單中，選定相應標誌：“**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**”視窗中指定 kavfsgt.exe 檔案。在使用 MMC 安裝 Kaspersky Security 10.1 for Windows Server 的過程中，該檔案位於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**”。

此時，已為 Kaspersky Security Management Service 啟用網路連線。

在安裝 Kaspersky Security 10.1 for Windows Server 後執行的操作

如果您已啟動 Kaspersky Security 10.1 for Windows Server,該應用程式在安裝後立即啟動防護和掃描工作。如果在安裝 Kaspersky Security 10.1 for Windows Server 期間選中“**安裝應用程式後啟用即時防護**”（預設選項），Kaspersky Security 10.1 for Windows Server 會在存取伺服器檔案系統物件時對它們進行掃描。如果在自訂安裝期間安裝了指令碼監控元件，Kaspersky Security 會在執行指令碼時掃描所有指令碼的程式碼。Kaspersky Security 10.1 for Windows Server 將在每週五的 20:00 執行“關鍵區域掃描”工作。

推薦在安裝 Kaspersky Security 10.1 for Windows Server 後執行下列步驟：

- 啟動 Kaspersky Security 10.1 for Windows Server 資料庫更新工作。安裝後，Kaspersky Security 10.1 for Windows Server 會使用應用程式發行套件中所含的資料庫掃描物件。

  我們推薦立即更新 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 之前受防護伺服器上未安裝任何具有即時檔案防護

的病毒防護軟體，請在伺服器上執行“關鍵區域掃描”。

- 配置有關 Kaspersky Security 10.1 for Windows Server 事件的管理員通知。

本章節說明項目

啟動和配置 Kaspersky Security 10.1 for Windows Server 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. 使用以下方法之一啟動 Kaspersky Security 10.1 主控台：
   - 在受防護的伺服器上開啟 Kaspersky Security 10.1 主控台。要執行此操作，請選擇“**開始 > 程式 > Kaspersky Security 10.1 for Windows Server > 管理工具 > Kaspersky Security 10.1 主控台**”。
   - 如果 Kaspersky Security 10.1 主控台已在不受防護的伺服器上啟動，請連線到受防護的伺服器：
     a. 開啟 Kaspersky Security 10.1 主控台樹狀目錄中的“**Kaspersky Security**”節點的上下文功能表。
     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，指定受防護伺服器的網路名稱。

     如果用於登入到 Microsoft Windows 的帳戶沒有 Kaspersky Security Management Service 的存取權限（請參見第 50 頁上的“關於 Kaspersky Security Management Service 的存取權限”部分），請指定具有所需權限的帳戶。

   Kaspersky Security 10.1 主控台視窗開啟。
2. 在 Kaspersky Security 10.1 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“**埠號**”欄位輸入代理伺服器的埠號。

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 Security 10.1 for Windows Server 將使用工作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 NTLM 身分驗證名稱及密碼**方式。Kaspersky Security 10.1 for Windows Server 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。
- **使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 Kaspersky Security 10.1 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 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 Security 10.1 for Windows Server 資料庫後，使用“掃描關鍵區域”工作掃描伺服器中是否有惡意程式。

► *若要執行“關鍵區域掃描”工作，請執行以下步驟：*

1. 在 Kaspersky Security 10.1 主控台樹狀目錄中，選擇“**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。

修改元件集和復原 Kaspersky Security 10.1 for Windows Server

您可新增或移除 Kaspersky Security 10.1 for Windows Server 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 Service 。

如果應用程式管理存取受密碼防護，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 元件集：*

1. 在“**開始**”功能表中，選擇“**所有程式 > Kaspersky Security 10.1 for Windows Server > 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 Security 10.1 for Windows Server 中或希望刪除的元件。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，並在上下文功能表中選擇：
     - “**元件將被安裝在本地硬碟上**”（如果您想要安裝一個元件）；
     - “**程式將在本地硬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“**已準備好安裝**”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 Security 10.1 for Windows Server 元件集。

如果 Kaspersky Security 10.1 for Windows Server 於運作時發生問題（Kaspersky Security 10.1 for Windows Server 當機；工作損毀或無法啟動），您可嘗試還原 Kaspersky Security 10.1 for Windows Server。您可在儲存 Kaspersky Security 10.1 for Windows Server 的目前設定時執行還原，或您可選擇一個選項以將所有 Kaspersky Security 10.1 for Windows Server 設定重設為其預設值。

► *要在應用程式或工作崩潰後修復 Kaspersky Security 10.1 for Windows Server，請執行以下步驟：*

1. 在“**開始**”功能表中，選擇“**所有程式 > Kaspersky Security 10.1 for Windows Server > 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 Security 10.1 for Windows Server，則選中“**修復推薦的應用程式設定**”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 Security 10.1 for Windows Server。

使用安裝精靈移除

本節包含有關使用安裝精靈從受防護伺服器上刪除 Kaspersky Security 10.1 for Windows Server 和 Kaspersky Security 10.1 主控台的說明。

本章節說明項目

Kaspersky Security 10.1 for Windows Server 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/解除安裝精靈來解除安裝受防護伺服器上的 Kaspersky Security 10.1 for Windows Server。

從受防護伺服器上移除 Kaspersky Security 10.1 for Windows Server 後需重新啟動伺服器。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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server：*

1. 在“**開始**”功能表中，選擇“**所有程式 > Kaspersky Security 10.1 for Windows Server > 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“**移除軟體元件**”。點擊“**下一步**”按鈕。

   隨即會開啟“**進階移除設定**”視窗。
3. 如有必要，在“**進階移除設定**”視窗中：
   a. 選中“**匯出隔離物件**”核取方塊以便 Kaspersky Security 10.1 for Windows Server 匯出已隔離的物件。預設取消選定該核取方塊。
   b. 選中“**匯出隔離物件**”核取方塊，以便從 Kaspersky Security 10.1 for Windows Server 隔離匯出物件。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 Security 10.1 for Windows Server\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 Security 10.1 for Windows Server 將從受防護伺服器移除。

Kaspersky Security 10.1 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。

您可使用安裝/移除安裝精靈來解除安裝伺服器上的 Kaspersky Security 10.1 主控台。

將 Kaspersky Security 10.1 主控台解除安裝後，必須重新啟動伺服器。

► *若要移除 Kaspersky Security 10.1 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 Security 10.1 for Windows Server > 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“**已準備好移除**”視窗。點擊“**移除**”按鈕。

   將開啟“**移除完成**”視窗。
4. 點擊“**確定**”。

此時，刪除完成，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 Security 10.1 for Windows Server 的詳細資訊，包含從命令列安裝和移除 Kaspersky Security 10.1 for Windows Server 的指令範例，以及從命令列新增和移除 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server

當您使用金鑰指定安裝設定後，可透過命令列執行 \server\ks4ws_x86(x64).msi 安裝套件檔案，來安裝或解除安裝 Kaspersky Security 10.1 for Windows Server，以及新增或移除其元件。

您可在受防護伺服器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 Kaspersky Security 10.1 主控台搭配使用。若要安裝，請使用 \client\ks4wstools.msi 安裝套件。

使用應用程式所安裝之伺服器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伺服器上執行其中一個 \server\ks4ws_x86(x64).msi 檔案，將使用推薦的安裝設定安裝 Kaspersky Security 10.1 for Windows Server。

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 Security 10.1 for Windows Server 的指令範例

本章節提供安裝 Kaspersky Security 10.1 for Windows Server 所使用的指令範例。

在執行 32 位元版本的 Microsoft Windows 的伺服器上，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 的伺服器上，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 Security 10.1 for Windows Server 的指令範例

► *若不想以使用者互動模式安裝 Kaspersky Security 10.1 for Windows Server，而想以預設的安裝設定來安裝，請執行以下指令：*

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

► *若要使用下列設定安裝 Kaspersky Security 10.1 for Windows Server：*

- 僅安裝“即時檔案防護”和“自訂掃描”元件；
- 在啟動 Kaspersky Security 10.1 for Windows Server 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：

```
\server\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 Security 10.1 for Windows Server，而想以預設的安裝設定來安裝，請執行以下指令：*

  msiexec /i ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1

- *若要以預設安裝設定安裝 Kaspersky Security 10.1 for Windows Server 並顯示安裝介面，請執行以下指令：*

  msiexec /i ks4ws.msi /qf EULA=1 PRIVACYPOLICY=1

- *若要以 C:\0000000A.key 的金鑰檔案安裝 Kaspersky Security 10.1 for Windows Server：*

  msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1

- *要事先掃描啟動的處理程序與本機磁碟的開機磁區，再安裝 Kaspersky Security 10.1 for Windows Server，請執行以下指令：*

  msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1

- *若要安裝 Kaspersky Security 10.1 for Windows Server 並將檔案儲存在目的資料夾 C:\WSEE 中，請執行以下指令：*

  msiexec /i ks4ws.msi INSTALLDIR=C:\WSEE /qn EULA=1 PRIVACYPOLICY=1

- *若要安裝 Kaspersky Security 10.1 for Windows Server 並以 ks4ws.log 檔案儲存安裝記錄檔案（存到 Kaspersky Security 10.1 for Windows Server 安裝套件儲存 msi 檔案的資料夾中），請執行以下指令：*

  msiexec /i ks4ws.msi /l*v ks4ws.log /qn EULA=1 PRIVACYPOLICY=1

- *若要安裝 Kaspersky Security 10.1 主控台，請執行以下指令：*

  msiexec /i ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1

- *若要使用 C:\0000000A.key 檔案的金鑰安裝 Kaspersky Security 10.1 for Windows Server：根據 C:\settings.xml 設定檔所敘述的配置設定 Kaspersky Security 10.1 for Windows Server，請執行以下指令：*

  msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1

在安裝 Kaspersky Security 10.1 for Windows Server 後執行的操作

如果您已啟動 Kaspersky Security 10.1 for Windows Server,該應用程式在安裝後立即啟動防護和掃描工作。如果在安裝 Kaspersky Security 10.1 for Windows Server 期間選中“**安裝應用程式後啟用即時防護**”，Kaspersky Security 10.1 for Windows Server 會在存取伺服器檔案系統物件時對它們進行掃描。如果在自訂安裝期間安裝了指令碼監控元件，

Kaspersky Security 10.1 for Windows Server 會在執行指令碼時掃描所有指令碼的程式碼。Kaspersky Security 10.1 for Windows Server 將在每週五晚上 8 點鐘執行“關鍵區域掃描”工作。

推薦在安裝 Kaspersky Security 10.1 for Windows Server 後執行下列步驟：

- 啟動 Kaspersky Security 10.1 for Windows Server 資料庫更新工作。安裝後，Kaspersky Security 10.1 for Windows Server 會使用發行套件中所含的資料庫掃描物件。我們建議立即更新 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 資料庫。透過代理伺服器（代理伺服器位址：proxy.company.com，連接埠：8080）與更新來源建立連線，使用內置 Windows NTLM 身分驗證存取伺服器（登入帳戶的使用者名稱：inetuser；密碼：123456）。

- 如果安裝 Kaspersky Security 10.1 for Windows Server 之前受防護伺服器上未安裝任何具有即時檔案防護的病毒防護軟體，請執行電腦的關鍵區域掃描。

► *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 Security 10.1 for Windows Server 事件的管理員通知。

新增/移除元件。指令範例

“自訂掃描”元件將自動安裝。您不必透過新增或刪除 Kaspersky Security 10.1 for Windows Server 元件，在 ADDLOCAL 指令設定值清單中指定此元件。

► *要將“應用程式啟動控制”元件新增到已安裝的元件，請執行以下指令：*

msiexec /i ks4ws.msi ADDLOCAL=Oas,AppCtrl /qn EULA=1 PRIVACYPOLICY=1

或

\server\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl EULA=1 PRIVACYPOLICY=1"

如果您將要安裝的元件與已安裝的元件枚舉在一起，則 Kaspersky Security 10.1 for Windows Server 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 ks4ws.msi REMOVE=AppCtrl,WiFiControl /qn EULA=1 PRIVACYPOLICY=1

Kaspersky Security 10.1 for Windows Server 移除。指令範例

► *要解除受防護伺服器上安裝的 Kaspersky Security 10.1 for Windows Server，請執行以下指令：*

msiexec /x ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1

► *要移除 Kaspersky Security 10.1 主控台，請執行以下指令：*

msiexec /x ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1

或

- 對於 32 位元作業系統：

  msiexec /x {232497F6-6572-4934-A6AF-24986952598B} /qn

- 對於 64 位元作業系統：

  msiexec /x {F96C7F1F-9B03-480D-A8F3-19D43CA89090} /qn

► *要從已啟用密碼防護的受防護伺服器上移除 Kaspersky Security 10.1 for Windows Server ，請執行以下指令：*

- 對於 32 位元作業系統：

  msiexec /x {DD1532DD-387B-43C5-8968-7E8130CC8A5E} UNLOCK_PASSWORD=*** /qn

- 對於 64 位元作業系統：

  msiexec /x {D025308B-AA7E-42D6-8058-B2B79A3D71F5} UNLOCK_PASSWORD=*** /qn

► *要從已啟用密碼防護的受防護伺服器上移除 Kaspersky Security 10.1 for Windows Server 外掛程式，請執行以下指令：*

msiexec.exe /x {DA15CF4A-75FF-4C92-AFC2-0A16DC645D2E} UNLOCK_PASSWORD=*** /qn

回傳代碼

以下表格包含命令列的回傳代碼清單。

表 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 Security 10.1 for Windows Server。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 Security 10.1 for Windows Server 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：<不相容的軟體清單>。

代碼	敘述
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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 以及安裝 Kaspersky Security 10.1 for Windows Server 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

您可使用以下卡巴斯基安全管理中心，使用遠端安裝工作來安裝 Kaspersky Security 10.1 for Windows Server。

完成遠端安裝工作後，將可在多個伺服器上使用相同的設定安裝 Kaspersky Security 10.1 for Windows Server。

您可將所有伺服器整合到一個管理員群組中，然後建立一個群組工作，並將 Kaspersky Security 10.1 for Windows Server 安裝到該群組的伺服器上。

您可以建立一個工作，在不屬於相同管理群組的一組伺服器上遠端安裝 Kaspersky Security 10.1 for Windows Server。建立此工作時，您必須建立一份要安裝 Kaspersky Security 10.1 for Windows Server 的各個伺服器的清單。

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 Security 10.1 for Windows Server 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管理伺服器的管理員群組中，但以下情況除外

- 當您想安裝 Kaspersky Security 10.1 for Windows Server 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）。

  如果伺服器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 Security 10.1 for Windows Server。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一台伺服器的管理員群組中。

- 要安裝 Kaspersky Security 10.1 for Windows Server 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（解除安裝）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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server，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伺服器上還安裝了 Kaspersky Security 10.1 for Windows Server 管理外掛程式（Kaspersky Security 10.1 for Windows Server 分發套件中的 \server\klcfginst.exe 檔案）。
- 請在受防護伺服器上安裝卡巴斯基安全管理中心網路代理。如果伺服器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 Security 10.1 for Windows Server。

您也可以先將伺服器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。

► *要藉助遠端安裝工作來安裝 Kaspersky Security 10.1 for Windows Server:*

1. 啟動卡巴斯基安全管理中心的管理主控台。
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 應用程式建立新安裝套件**”選項。

3. 輸入安裝套件名稱。
4. 指定 Kaspersky Security 10.1 for Windows Server 分發套件中的 ks4ws.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，請選中“**此 EULA 的條款和條件**”和“**敘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 Security 10.1 for Windows Server 元件集（請參見第 55 頁上的“修改元件集和復原 Kaspersky Security 10.1 for Windows Server”部分）以及安裝套件中的預設安裝設定（請參見第 38 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）：

   在卡巴斯基安全管理中心中，展開“**遠端安裝**”節點，然後在工作區中的“**安裝套件**”子節點中，開啟已建立 Kaspersky Security 10.1 for Windows Server 安裝套件的上下文功能表，並選擇“**內容**”。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，核取您想安裝的 Kaspersky Security 10.1 for Windows Server 元件名稱旁邊的核取方塊。

   b. 若想指定目標資料夾（不使用預設資料夾），在“**目的資料夾**”欄位中指定資料夾的名稱及路徑。

      目的資料夾的路徑可能包含系統環境變數。伺服器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：

      - 在安裝之前對伺服器進行病毒掃描。
      - 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。
      - 將 Kaspersky Lab 建議的檔案新增到排除清單。

   d. 如果想將 Kaspersky Security 10.1 for Windows Servers 的先前版本中建立的設定檔匯入設定，請指定所需的設定檔。

   e. 在“**內容：<安裝套件名稱>**”視窗，點擊“**確定**”。
7. 在“**安裝套件**”節點中，建立一個工作， 於選定伺服器（管理群組）上遠端安裝 Kaspersky Security 10.1 for Windows Server。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 Security 10.1 for Windows Server 的遠端安裝工作。

Kaspersky Security 10.1 for Windows Server 將安裝於在工作中指定的伺服器上。

在安裝 Kaspersky Security 10.1 for Windows Server 後執行的操作

安裝 Kaspersky Security 10.1 for Windows Server 後，推薦更新伺服器上的 Kaspersky Security 10.1 for Windows Server 資料庫；若安裝 Kaspersky Security 10.1 for Windows Server 前，伺服器上未安裝任何防毒應用程式並啟用即時防護功能，則還推薦掃描伺服器的關鍵區域。

如果您已安裝 Kaspersky Security 10.1 for Windows Server 的伺服器位於卡巴斯基安全管理中心的同一個管理員群組中，您可使用以下這些工作：

1. 為安裝了 Kaspersky Security 10.1 for Windows Server 的伺服器群組建立“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. 替一組伺服器建立新的政策。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，以及管理群組的伺服器上的資料庫更新工作。

您還可以配置有關 Kaspersky Security 10.1 for Windows Server 事件的管理員通知。

透過卡巴斯基安全管理中心安裝 Kaspersky Security 10.1 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*。

► *要以遠端安裝工作安裝 Kaspersky Security 10.1 主控台，請執行以下操作：*

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“**為安裝選擇安裝套件**”中，從 Kaspersky Security 10.1 for Windows Server 分發套件資料夾中選擇 client\setup.exe 檔案，然後選中“**將資料夾複製到安裝套件**”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 Kaspersky Security 10.1 主控台但不安裝說明檔和說明文件，請執行以下指令：

     ```
     /s /p EULA=1 "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 Kaspersky Security 10.1 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。

Kaspersky Security 10.1 主控台將安裝到工作指定的電腦上。

透過卡巴斯基安全管理中心移除 Kaspersky Security 10.1 for Windows Server

如果網路電腦上的 Kaspersky Security 10.1 for Windows Server 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。如果未透過卡巴斯基安全管理中心政策集中管理密碼防護，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server。

► *要移除 Kaspersky Security 10.1 for Windows Server，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伺服器的帳戶。您只能使用預設移除設定移除 Kaspersky Security 10.1 for Windows Server（請參閱第 38 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解除安裝

本章節介紹透過 Active Directory 群組政策安裝和移除 Kaspersky Security 10.1 for Windows Server。同時也包含有關透過群組政策安裝 Kaspersky Security 10.1 for Windows Server 後的操作資訊。

本章節說明項目

透過 Active Directory 群組政策安裝 Kaspersky Security 10.1 for Windows Server

您可透過 Active Directory 群組政策在多台伺服器上安裝 Kaspersky Security 10.1 for Windows Server。您可以用相同的方式安裝 Kaspersky Security 10.1 主控台。

想安裝 Kaspersky Security 10.1 for Windows Server 或 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 之伺服器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 Security 10.1 for Windows Server，請使用 ks4ws_x86(x64).msi 安裝套件。要安裝 Kaspersky

Security 10.1 主控台，請使用 ks4wstools.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。

► *要安裝 Kaspersky Security 10.1 for Windows Server（Kaspersky Security 10.1 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，該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. 在網域控制器上替一組整合的伺服器建立新的政策。
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 Security 10.1 for Windows Server（Kaspersky Security 10.1 主控台）安裝套件 msi 檔的路徑。
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 Security 10.1 for Windows Server。

在安裝 Kaspersky Security 10.1 for Windows Server 後執行的操作

在受防護伺服器上安裝 Kaspersky Security 10.1 for Windows Server 後，推薦您立即更新應用程式資料並執行關鍵區域掃描。您可以從 Kaspersky Security 10.1 主控台執行這些操作（請參見第 53 頁上的“安裝 Kaspersky Security 10.1 for Windows Server 後執行的操作”部分）。

您還可以配置有關 Kaspersky Security 10.1 for Windows Server 事件的管理員通知。

透過 Active Directory 群組政策移除 Kaspersky Security 10.1 for Windows Server

如果您使用 Active Directory 群組政策在群組伺服器上安裝 Kaspersky Security 10.1 for Windows Server（或 Kaspersky Security 10.1 主控台），您可使用這個政策來解除安裝 Kaspersky Security 10.1 for Windows Server（或 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 不可用。

► *要移除 Kaspersky Security 10.1 for Windows Server（Kaspersky Security 10.1 主控台）：*

1. 從您想刪除 Kaspersky Security 10.1 for Windows Server 或 Kaspersky Security 10.1 主控台之伺服器所在的網域控制器選擇組織單位。
2. 選擇替 Kaspersky Security 10.1 for Windows Server 安裝所建立的政策，並在“**群組政策編輯器**”的“**軟體安裝**”節點中（“**電腦配置 > 程式設定 > 軟體安裝**”）開啟 Kaspersky Security 10.1 for Windows Server（或 Kaspersky Security 10.1 主控台）安裝套件的內容功能表，以選擇“**所有工作 > ‘刪除’指令**”。
3. 從所有伺服器中選擇“**立即移除程式**”的移除方法。
4. 使用 gpupdate /force 指令採納變更。

伺服器重新啟動並登入 Microsoft Windows 前，就會從伺服器上移除 Kaspersky Security 10.1 for Windows Server。

Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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，它由歐洲反電腦病毒協會（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防護設定。

eicar.com 檔案含有一行文字。掃描檔案時，Kaspersky Security 10.1 for Windows Server 會偵測到這行文字中有“威脅”等字，接著對檔案指派“**已感染**”狀態並刪除檔案。檔案中偵測到的威脅資訊將出現在 Kaspersky Security 10.1

主控台及工作記錄中。

您可使用 eicar.com 檔案來檢查 Kaspersky Security 10.1 for Windows Server 解毒已感染物件及偵測潛在可疑危險物件的方法。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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 即時檔案防護工作和預設自訂掃描工作設定“**所有物件**”值。

表 14. EICAR 檔案前置詞

前置詞	掃描後的檔案狀態及 Kaspersky Security 10.1 for Windows Server 操作
無前置詞	Kaspersky Security 10.1 for Windows Server 會指派“**已感染**”狀態給物件並刪除物件。
SUSP-	Kaspersky Security 10.1 for Windows Server 會指派“**可疑感染**”狀態給物件（啟發式分析器偵測到的）使用並刪除物（無法解毒可疑物件）件。
WARN-	Kaspersky Security 10.1 for Windows Server 會指派“**可疑感染**”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（無法解毒可疑物件）。
CURE-	Kaspersky Security 10.1 for Windows Server 會指派“**已感染**”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 Security 10.1 for Windows Server 後，您可以確認 Kaspersky Security 10.1 for Windows Server 發現包含惡意程式碼的物件。要進行檢查，您可以使用 EICAR 測試病毒（請參見第 69 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，請確保受防護伺服器與儲存有 eicar.com 檔案的電腦均啟用了 Microsoft Windows Messenger 服務。
3. 開啟 Kaspersky Security 10.1 主控台。
4. 使用以下其中一種方法，將儲存的 eicar.com 檔案複製到受防護伺服器的本機磁碟上：
   - 若要透過“終端機服務”視窗測試通知，請將 eicar.com 檔複製到伺服器。

- 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：

- 受防護伺服器上的 eicar.com 檔已刪除。
- 在 Kaspersky Security 10.1 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 Kaspersky Security 10.1 主控台樹狀結構與“**即時伺服器防護**”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。）
  - 您從中複製該檔案的電腦上會顯示以下 Microsoft Windows Messenger 服務訊息：Kaspersky Security 10.1 for Windows Server 已在<事件發生時間>封鎖對電腦<電腦的網路名稱>上的<電腦上的檔案路徑>\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 Kaspersky Security 10.1 主控台。
3. 執行以下操作：
   a. 在 Kaspersky Security 10.1 主控台樹狀目錄中，選擇“**自訂掃描**”節點。
   b. 選擇“**掃描關鍵區域**”子節點。
   c. 在“**設定掃描範圍**”標籤上，開啟“**網路**”節點上的右鍵功能表，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 Kaspersky Security 10.1 主控台中，工作記錄的狀態為“**重要**”；“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 Kaspersky Security 10.1 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

可以透過本機主控台和卡巴斯基安全管理中心管理外掛程式控制 Kaspersky Security 10.1 for Windows Server。《*Kaspersky Security 10.1 for Windows Server 使用者手冊*》中介紹了使用本機主控台進行的操作。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可以在卡巴斯基安全管理中心的文件中找到。

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

關於最終使用者授權協議

*最終使用者授權協議*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查看使用者授權合約的條款：

- Kaspersky Security 10.1 for Windows Server 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授權協議，即表示您接受最終使用者授權協議的條款。如果您不接受最終使用者授權協議的條款，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：

- 依照使用者授權合約的條款使用應用程式
- 技術支援

服務範圍和程式的使用期限取決於啟動程式時使用的產品授權類型。

可以使用以下產品授權類型：

- *試用*產品授權是針對試用程式提供的免費產品授權。

  試用產品授權的有效期很短。在試用產品授權到期後，Kaspersky Security 10.1 for Windows Server 將無法正常工作。要繼續使用程式，你需要購買一個正式產品授權。

  您只能根據試用產品授權啟動一次程式。

- *正式*產品授權是指購買應用程式時授予的付費產品授權。

  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 Security 資料庫）。要繼續在全功能模式下使用 Kaspersky Security 10.1 for Windows Server，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。

Kaspersky Security 10.1 for Windows Server 不會跟蹤產品授權的到期日期。如果使用已到期的產品授權再次啟動程式（同時最初的啟動碼仍然處於活動狀態），您需要使用有效的產品授權再次新增註冊碼。

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

關於產品授權類型

Kaspersky Security 10.1 for Windows Server 是各種企業防護解決方案的一部分。Kaspersky Security 10.1 for Windows Server 的可用功能取決於所選解決方案。下表顯示了提供的解決方案類型和每種解決方案可用的應用程式功能。

Kaspersky Endpoint Security for Business Basic	
按訂購提供	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理

Kaspersky Endpoint Security for Business Select	
按訂購提供	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理

Kaspersky Endpoint Security for Business Advanced	
按訂購提供	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 應用程式啟動控制 裝置控制 流量安全

Kaspersky Endpoint Security for Business Total	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 應用程式啟動控制 裝置控制 流量安全

Kaspersky Security for File Server	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 應用程式啟動控制 裝置控制 檔案完整性監控 記錄審查 流量安全（外部代理模式不可用）

Kaspersky Security for Data Storage Systems	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 應用程式啟動控制 裝置控制 檔案完整性監控 記錄審查 流量安全 NAS 防護（儲存）+ 用於 NAS 的加密勒索軟體防護

Kaspersky Security for Virtualization	
按訂購提供	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 裝置控制 流量安全

Kaspersky Security for xSP	
按訂購提供	
元件	檔案防護 弱點利用防禦 防火牆管理 流量安全

Kaspersky Hybrid Cloud Security	
按訂購提供	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 裝置控制 流量安全

Kaspersky Hybrid Cloud Security Enterprise	
按訂購提供	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 檔案完整性監控 記錄審查 應用程式啟動控制 裝置控制 流量安全

AWS™ 預付訂購	
元件	檔案防護 弱點利用防禦 加密勒索軟體防護（用於共用資料夾） 防火牆管理 檔案完整性監控 記錄審查 應用程式啟動控制 流量安全 裝置控制

Kaspersky Security Internet Gateway	
元件	檔案防護 弱點利用防禦 防火牆管理 流量安全

關於金鑰

*金鑰*是一串位資料，您可以依照最終使用者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。可以將試用或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。

試用產品授權的金鑰只能新增為啟動金鑰。試用產品授權的金鑰不能新增為備用金鑰。

關於啟動碼

啟動碼 – 這是您購買 Kaspersky Security 10.1 for Windows Server 正式產品授權後接收到的代碼。接收金鑰檔案和透過安裝金鑰檔案啟動應用程式時必須提供此代碼。

啟動碼是一個二十位元的數字和拉丁字母序列，格式為 xxxxx-xxxxx-xxxxx-xxxxx。

應用程式啟動後，將開始計算產品授權期限。如果您購買在多台電腦上使用 Kaspersky Security 10.1 for Windows Server 的產品授權，則當應用程式在第一台電腦上啟動時，即開始計算產品授權期限。

如果啟動碼遺失或啟動後被意外移除，則您必須向 Kaspersky Lab 技術支援傳送請求來復原啟動碼。

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。

在購買 Kaspersky Security 10.1 for Windows Server 或訂購 Kaspersky Security 10.1 for Windows Server 試用版本時，將向您提供的電子郵件位址傳送一個金鑰檔案。

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 Security 10.1 for Windows Server 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 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和授權憑證的資訊：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（確認或復原接受條款）的內容；資料處理條款接受的狀態變更的日期和時間。

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 Security 10.1 for Windows Server 會在受防護伺服器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伺服器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、被啟動的可執行檔的實例，這些檔案的類型、名稱、校驗和以及內容；
- 有關 Web 活動的資訊，例如，處理的 URL、指定的類別、下載的物件的相關資料、處理的數位憑證的內容、處理的電子郵件的相關資料，包括寄件者、收件者、主題、郵件內文和附件；
- 有關網路活動的資訊，包括封鎖的用戶端電腦的 IP 位址。

作為應用程式基本功能的一部分，Kaspersky Security 10.1 for Windows Server 處理並儲存資料，包括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處理和防護。

Kaspersky Security 10.1 for Windows Server 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的詳細資訊，請參見本手冊的相應章節。

使用金鑰啟動應用程式

您可以套用金鑰啟動 Kaspersky Security 10.1 for Windows Server。

如果已經向 Kaspersky Security 10.1 for Windows Server 新增了啟動金鑰，並且您又另外新增一個金鑰作為啟動金鑰，則新金鑰會替換之前新增的金鑰。之前安裝的啟動金鑰會被刪除。

如果已經向 Kaspersky Security 10.1 for Windows Server 新增了備用金鑰，並且您又另外新增一個金鑰作為備用金鑰，則新金鑰會替換之前新增的金鑰。之前安裝的備用金鑰會被刪除。

如果已經向 Kaspersky Security 10.1 for Windows Server 新增了啟動金鑰和備用金鑰，並且您又另外新增一個新金鑰作為啟動金鑰，則新金鑰會替換之前新增的啟動金鑰；備用金鑰不會被刪除。

► *要使用金鑰啟動 Kaspersky Security 10.1 for Windows Server，請執行下列步驟：*

1. 在 Kaspersky Security 10.1 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 Kaspersky Security 10.1 主控台的 **Kaspersky 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 未啟動。狀態紅色高亮顯示。
- **已違反最終使用者授權協議** – 由於違反了最終使用者授權協議（請參見第 73 頁上的“關於最終使用者授權協議”部分）的條款，Kaspersky Security 10.1 for Windows Server 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。
- **訂購已暫停** – 訂購已被臨時暫停。狀態紅色高亮顯示。您可以隨時續約訂購。

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 Kaspersky Security 10.1 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）。

表 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：正式版或試用版。
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，*

在“**授權**”節點上，開啟包含您要展開的產品授權資料的字串的上下文功能表，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 Security 10.1 for Windows Server 的轉銷商的聯絡人詳細資訊（請參見下表）。

表 16. “內容 <金鑰編號>”視窗中的詳細產品授權資訊

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：正式版或試用版。
到期前的天數	與啟動授權相關的產品授權在到期前剩餘的天數。

欄位	敘述
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 Security 10.1 for Windows Server 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。
金鑰使用限制	有關金鑰使用的限制（如果有）。
符合技術支援條件	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。
擁有者資訊	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 Security 10.1 for Windows Server 會通知您這一情況。這種情況下，**Kaspersky 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電腦。

► *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 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Kaspersky Security 10.1 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上下文功能表中，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 Security 10.1 for Windows Server

本節包含有關啟動和停止 Kaspersky Security 10.1 for Windows Server 管理外掛程式和 Kaspersky Security Service 的資訊。

本章內容

啟動卡巴斯基安全管理中心管理外掛程式

啟動與 Kaspersky Security 10.1 for Windows Server 一起工作的卡巴斯基安全管理中心外掛程式時，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 Service

預設情況下，Kaspersky Security Service 會在作業系統啟動時自動啟動。Kaspersky Security Service 將管理執行即時防護、本機活動控制、網路附加儲存防護、自訂掃描和更新工作的工作處理程序。

預設情況下，當 Kaspersky Security 10.1 for Windows Server 服務啟動時，將啟動“即時檔案防護”、“指令碼監控”（若安裝）、“作業系統啟動時掃描”和“應用程式完整性控制”工作以及其他排程在“**應用程式啟動時**”啟動的工作。

如果停止 Kaspersky Security Service ，則會停止所有正在執行的工作。重新開機 Kaspersky Security Service 之後，應用程式只會自動啟動排程已將啟動頻率設定為“**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 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 Service 。

如果您是受防護伺服器上“管理員”群組的成員，您可以啟動和停止 Kaspersky Security 10.1 for Windows Server。

► *要使用管理主控台停止或啟動應用程式，請執行以下步驟：*

1. 在 Kaspersky Security 10.1 主控台樹狀目錄中，開啟 **Kaspersky Security** 節點的上下文功能表。
2. 選擇以下之一項目：
   - **停止服務**。
   - **啟動服務**。

將啟動或停止 Kaspersky Security Service 。

關於 Kaspersky Security 10.1 for Windows Server 功能的存取權限

本節包含有關 Kaspersky Security 10.1 for Windows Server 和該應用程式註冊的 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 Security 10.1 for Windows Server 的管理權限

預設情況下，為受防護的伺服器上的管理員組的使用者，在安裝 Kaspersky Security 10.1 for Windows Server 的過程中在受防護的伺服器上建立的 KAVWSEE 管理員群組以及 SYSTEM 組的使用者授予對所有 Kaspersky Security 10.1 for Windows Server 功能的存取權限。

有權限存取 Kaspersky Security 10.1 for Windows Server 的“**編輯**”權限功能的使用者可以向其他在受防護伺服器上註冊的使用者或者該網域中包含的使用者授予對 Kaspersky Security 10.1 for Windows Server 功能的存取權限。

未在 Kaspersky Security 10.1 for Windows Server 使用者清單中註冊的使用者無法開啟 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 存取權限等級：

- **完全控制** – 存取所有應用程式功能：可檢視和編輯 Kaspersky Security 10.1 for Windows Server 一般設定、元件設定、Kaspersky Security 10.1 for Windows Server 使用者權限，還可以檢視 Kaspersky Security 10.1 for Windows Server 統計。
- **編輯** – 存取除編輯用戶權限以外的所有應用程式功能：可以檢視和編輯 Kaspersky Security 10.1 for Windows Server 的一般設定和 Kaspersky Security 10.1 for Windows Server 元件設定。
- **讀取** – 可以檢視 Kaspersky Security 10.1 for Windows Server 一般設定、Kaspersky Security 10.1 for Windows Server 元件設定、Kaspersky Security 10.1 for Windows Server 統計和 Kaspersky Security 10.1 for Windows Server 使用者權限。

您還可以設定進階存取權限（請參閱第 90 頁上的“配置用於管理 Kaspersky Security 10.1 for Windows Server 和 Kaspersky Security Service 的存取權限”部分）：允許或封鎖存取特定的 Kaspersky Security 10.1 for Windows

Server 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。

表 17. 關於 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 設定。 • 編輯應用程式設定。
讀取設定	可執行以下操作： • 檢視 Kaspersky Security 10.1 for Windows Server 一般設定和工作設定。 • 將 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 工作的統計資訊。
應用程式授權	可啟動或取消啟動 Kaspersky Security 10.1 for Windows Server。
移除應用程式	可移除 Kaspersky Security 10.1 for Windows Server。
讀取權限	可檢視 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 功能的使用者存取權限。

關於 Kaspersky Security Service 的管理權限

在安裝 Kaspersky Security 10.1 for Windows Server 的過程中在 Windows 中註冊 Kaspersky Security Service (KAVFS)，並在內部啟用在啟動作業系統時啟動的功能元件。為了降低協力廠商透過 Kaspersky Security Service 的管理存取應用程式功能和受防護伺服器上安全設定的風險，可以從本機 Kaspersky Security 10.1 主控台或卡巴斯基

安全管理中心管理外掛程式限制管理 Kaspersky Security Service 的權限。

預設情況下，將管理 Kaspersky Security Service 的存取權限授予受防護伺服器上“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 87 頁上的“關於 Kaspersky Security 10.1 for Windows Server 服務的管理權限”部分）的使用者可以向在受防護伺服器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對管理 Kaspersky Security Service 的存取權限。

您可以為 Kaspersky Security 10.1 for Windows Server 使用者或使用者組選擇以下預設的存取權限等級之一以管理 Kaspersky Security Service ：

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

您還可以設定進階存取權限：允許或拒絕存取指定的 Kaspersky Security 10.1 for Windows Server 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。

表 18. 限定 Kaspersky Security 10.1 for Windows Server 功能的存取權限

功能	敘述
檢視服務設定	檢視：可檢視 Kaspersky Security Service 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 Service 的執行狀態。
從服務請求狀態	可從 Kaspersky Security Service 請求服務執行狀態。
列出依存服務	可檢視 Kaspersky Security Service 依存的以及依存于 Kaspersky Security Service 的服務清單。
編輯服務設定	可檢視和編輯 Kaspersky Security Service 一般設定和使用者權限。
啟動服務	可啟動 Kaspersky Security Service。
停止服務	可停止 Kaspersky Security Service。
暫停/還原服務	可暫停和還原 Kaspersky Security Service。
讀取權限	可檢視 Kaspersky Security Service 使用者清單和每個使用者的存取權限。

功能	敘述
編輯權限	可執行以下操作： • 新增和刪除 Kaspersky Security Service 使用者。 • 編輯 Kaspersky Security Service 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 Service。
使用者定義的服務請求	可建立和傳送對 Kaspersky Security Service 的使用者請求。

關於 Kaspersky Security Management Service 的存取權限

您可以檢視 Kaspersky Security 10.1 for Windows Server 服務的清單。

在安裝過程中，Kaspersky Security 10.1 for Windows Server 會註冊 Kaspersky Security 10.1 for Windows Server 管理服務 (KAVFSGT)。若要透過安裝在其他電腦上的 Kaspersky Security 10.1 主控台來管理程式，使用其權限與 Kaspersky Security 10.1 for Windows Server 建立連線的帳戶必須對受防護伺服器上的 Kaspersky Security 10.1 for Windows Server 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所有 Kaspersky Security Management Service 的權限：受防護伺服器上的管理員群組的使用者，以及安裝 Kaspersky Security 10.1 for Windows Server 時在受防護伺服器上建立的 KAVWSEE 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 Management Service。

您不能透過配置 Kaspersky Security 10.1 for Windows Server 來允許或封鎖使用者存取 Kaspersky Security 10.1 for Windows Server 管理服務。

如果在受防護的伺服器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 Security 10.1 for Windows Server。

設定用於管理 Kaspersky Security 10.1 for Windows Server 和 Kaspersky Security Service 的存取權限

您可以編輯允許存取 Kaspersky Security 10.1 for Windows Server 功能和管理 Kaspersky Security Service 的使用

者和使用者組清單，還可以編輯這些使用者和使用者組的存取權限。

► *要從清單中新增或刪除使用者或群組：*

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伺服器的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要設定伺服器組的政策設定，請選擇“**政策**”標籤，然後開啟“**<政策名稱> > 內容**”。
   - 如果您想要配置單個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 108 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“**選項**”部分，執行以下步驟之一：
   - 如果您希望編輯具有管理 Kaspersky Security 10.1 for Windows Server 功能的存取權限的使用者清單，請選擇“**修改應用程式管理使用者權限**”。
   - 如果您希望編輯具有透過 Kaspersky Security Service 管理應用程式的存取權限的使用者清單，請選擇“**修改 Kaspersky Security Service 管理使用者權限**”。

     將開啟“**Kaspersky Security 10.1 for Windows Server 群組的權限**”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）。

► *編輯使用者或群組對管理 Kaspersky Security 10.1 for Windows Server 或 Kaspersky Security Service 的權限：*

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伺服器的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要配置政策設定，在卡巴斯基安全管理中心管理主控台的電腦群組中，選擇**政策**標籤，然後開啟“**<政策名稱> > 選項**”。
   - 如果您想要配置單個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 108 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“**選項**”部分，執行以下步驟之一：
   - 如果您希望編輯具有管理 Kaspersky Security 10.1 for Windows Server 功能的存取權限的使用者清單，請選擇“**修改應用程式管理使用者權限**”。
   - 如果您希望編輯具有透過 Kaspersky Security Service 管理應用程式的存取權限的使用者清單，請選擇“**修改 Kaspersky Security Service 管理使用者權限**”。

     將開啟“**Kaspersky Security 10.1 for Windows Server 群組的權限**”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：
   - **完全控制**：管理 Kaspersky Security 10.1 for Windows Server 或 Kaspersky Security Service 的全套權限。
   - **讀取**：
     - 管理 Kaspersky Security 10.1 for Windows Server 的以下權限：**檢索統計資訊**、**讀取設定**、**讀取記錄**和**讀取**權限。
     - 以下管理 Kaspersky Security Service 的以下權限：**讀取服務設定**、**從服務管理員請求服務狀態**、**從服務請求狀態**、**列出依存服務**、**讀取**權限。
   - **修改**：
     - 除**編輯**權限之外的所有 Kaspersky Security 10.1 for Windows Server 管理權限。
     - 管理 Kaspersky Security Service 的以下權限：**編輯服務設定**、**讀取**權限。
   - **執行**：管理 Kaspersky Security Service 的以下權限：**啟動服務**、**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 Security 10.1 for Windows Server 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. 在開啟的視窗中，點擊“**顯示特殊權限**”連結。
   d. 在視窗頂部的下拉清單中，選擇存取控制類型（“**允許**”或“**封鎖**”）。
   e. 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。
   f. 點擊“**確定**”。
   g. 在“**Kaspersky Security 10.1 for Windows Server 的其他安全設定**”視窗中，點擊“**確定**”。
7. 在“**Kaspersky Security 10.1 for Windows Server 群組的權限**”視窗中，點擊“**套用**”按鈕。

已配置的管理 Kaspersky Security 10.1 for Windows Server 或 Kaspersky Security Service 的權限將被儲存。

對 Kaspersky Security 10.1 for Windows Server 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 87 頁上的“關於 Kaspersky Security 10.1 for Windows Server 功能的存取權限”部分）。您也可在 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會請求密碼：

- 連線到本機 Kaspersky Security 10.1 主控台；
- 移除 Kaspersky Security 10.1 for Windows Server；
- 修改 Kaspersky Security 10.1 for Windows Server 元件。

Kaspersky Security 10.1 for Windows Server 介面會在螢幕上隱藏指定密碼。Kaspersky Security 10.1 for Windows

Server 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配置可能會導致存取應用程式完全被封鎖。

► *若要防護對 Kaspersky Security 10.1 for Windows Server 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伺服器的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要設定伺服器組的政策設定，請選擇“**政策**”標籤，然後開啟“**<政策名稱> > 內容**”。
   - 如果您想要配置單個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 108 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**安全性和可靠性**部分，點擊**設定**按鈕。

   將開啟“**安全性設定**”視窗。
4. 在“**密碼設定**”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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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，還將無法從受防護伺服器移除應用程式。

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，執行以下操作：*

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伺服器的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要設定伺服器組的政策設定，請選擇“**政策**”標籤，然後開啟“**<政策名稱> > 內容**”。
   - 如果您想要配置單個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 108 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**安全性和可靠性**部分，點擊**設定**按鈕。

   將開啟“**安全性設定**”視窗。
4. 在“**密碼設定**”組框中，清除“**套用密碼防護**”核取方塊。

“**密碼**”和“**確認密碼**”欄位會清除並變為非活動狀態。

5. 點擊“**確定**”。

即會停用密碼防護。Kaspersky Security 10.1 for Windows Server 會從應用程式設定移除舊密碼校驗和。

為 Kaspersky Security Management Service 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。

► *若要允許受防護伺服器上的 Kaspersky Security Management Service 連線網路，請執行以下步驟：*

1. 在執行 Microsoft Windows Server 的受防護伺服器上，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**”標籤的預定例外清單中，選擇以下核取方塊：“**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 Kaspersky Security 10.1 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**”。

將允許受防護伺服器上的 Kaspersky Security Management Service 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個伺服器上管理 Kaspersky Security 10.1 for Windows Server 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，以便管理多個已安裝 Kaspersky Security 10.1 for Windows Server 的伺服器防護。

政策在一個管理群組中所有受防護伺服器上實行該政策中指定的 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 系統稽核記錄中記錄了有關政策實行情況的資訊。您可在 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Kaspersky Security 10.1 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 Kaspersky Security 10.1 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”或“網路附加儲存防護”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防護設定。
2. 配置政策設定。在已建立政策的“**內容：<政策名稱>**”視窗中，您可以定義即時防護設定、Kaspersky Security

10.1 for Windows Server 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 Security 10.1 for Windows Server 事件的使用者和管理員通知。

► *若要為一組執行已安裝 Kaspersky Security 10.1 for Windows Server 的伺服器建立政策，請執行以下步驟：*

1. 展開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伺服器的管理群組。
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。
3. 在“**輸入應用程式群組政策的名稱**”視窗的“**名稱**”欄位中，輸入所建立政策的名稱。政策名稱不能包含以下符號：" * < : > ? \ / |)。
4. 在“**選擇用於建立群組政策的應用程式**”視窗的“**應用程式名稱**”標題下面，選擇“Kaspersky Security 10.1 for Windows Server”。
5. 在“**選擇操作類型**”視窗中，選擇以下選項之一：
   - **建立**，用預設為新建政策設定的設定建立新政策。
   - **匯入使用先前的 Kaspersky Security for Windows Server 版本建立的政策**，使用該版本政策作為範本。

     點擊“**瀏覽**”，然後選擇儲存現有政策的設定檔。
6. 在“**即時伺服器防護**”視窗中，根據需要配置“即時檔案防護”和“KSN 使用”工作設定。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。

   新建政策使用即時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“**選項**”視窗，根據需要配置工作設定。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“**選項**”視窗，根據需要配置工作設定。點擊“**確定**”。

   如果接受 KSN 聲明，則“KSN 使用”工作可用。
7. 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，則該現有政策將變為非活動政策，而您建立的政策將被啟動。
   - “**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。
8. 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 Security 10.1 for Windows Server 的其他設定、工作和功能。

設定政策

在現有政策的“**<政策名稱> 內容**”視窗中，您可以配置 Kaspersky Security 10.1 for Windows Server 一般設定、隔離和備份設定、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 Security 10.1 for Windows Server 事件的使用者和管理員通知，用於管理應用程式和 Kaspersky Security Service 的存取權限和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. 選擇您想要設定的政策，然後使用以下方法之一開啟“**<政策名稱> 內容**”視窗：
   - 在政策的上下文功能表中選擇“**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伺服器上套用政策。
   - **非活動政策**，如果您不希望在選定組內的所有伺服器上套用政策。

   當您管理 Kaspersky Security 10.1 for Windows Server 時，“**離線使用者政策**”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“**即時伺服器防護**”、“**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伺服器上執行任何工作。
   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 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 使用者手冊*》的相關章節。

Kaspersky Security 10.1 for Windows Server 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

表 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，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**”部分，可以點擊“**設定**”按鈕來配置以下設定： • 配置工作執行設定。 • 指定當伺服器使用 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。
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**”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

表 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。

章節	選項
卸除式磁碟機掃描	在**卸除式磁碟機掃描**部分中，可以使用**設定**按鈕來配置卸除式 USB 磁碟機的掃描設定。
應用程式管理的使用者存取權限	在**應用程式管理的使用者存取權限**部分中，可以配置管理 Kaspersky Security 10.1 for Windows Server 的使用者權限和使用者群組權限
Security Service 管理的使用者存取權限	在**Security Service 管理的使用者存取權限**部分中，可以配置管理 Kaspersky Security Service 的使用者權限和使用者群組權限。
儲存	在“**儲存**”部分，點擊“**設定**”按鈕以配置以下“隔離”、“備份”和“封鎖的主機”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。 • 配置主機封鎖期限。

即時伺服器防護

表 21. 即時伺服器防護的設定部分

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**”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。 • 配置工作執行。 • 配置將卡巴斯基安全管理中心用作 KSN 代理伺服器的設定。 • 接受 KSN 聲明。 • 配置工作啟動設定。
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。

章節	選項
指令碼監控	在“**指令碼監控**”工作中，點擊“**設定**”按鈕配置以下工作執行設定： • 允許或封鎖執行可疑危險指令碼。 • 配置啟發式分析的使用。 • 配置信任區域的應用。 • 配置工作執行設定。

本機活動控制

表 22. “本機活動控制”部分的設定

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

表 23. “網路活動控制”部分的設定

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。
加密勒索軟體防護	在“**加密勒索軟體防護**”部分中，可以點擊“**設定**”按鈕來配置以下工作設定： • 設定加密勒索軟體防護的防護範圍。 • 配置工作啟動設定。

系統稽核

表 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，可以配置表示受防護伺服器上存在安全衝突的檔案變更的控制。
記錄審查	在“**記錄稽核**”部分中，可以根據 Windows 事件記錄分析結果配置受防護伺服器的完整性控制。

記錄和通知

表 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，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，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 Security 10.1 for Windows Server 將報告給管理伺服器的物件類型。

網路附加儲存防護

表 26. 網路附加儲存防護的設定部分

章節	選項
即時檔案防護(RPC)	在“**即時檔案防護(RPC)**”部分中，可以點擊“**設定**”按鈕來配置以下設定： • 啟發式分析使用。 • 網路附加儲存連線設定。 • 工作防護範圍。
即時檔案防護(ICAP)	在“**即時檔案防護(ICAP)**”部分中，可以點擊“**設定**”按鈕來配置以下設定： • ICAP 服務連線設定。 • 與其他元件的整合。 • 安全等級。
用於 NetApp 的加密勒索軟體防護	在“**用於 NetAPP 的加密勒索軟體防護**”部分中，可以點擊“**設定**”按鈕來配置以下設定： • 工作模式。 • 啟發式分析使用。 • 連線和身分驗證設定。 • 指定防護範圍中的排除項目。

要檢視有關“網路附加儲存防護”工作的詳細資訊，請參見 *Kaspersky Security 10.1 for Windows Server 網路附加儲存防護實施手冊*。

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個伺服器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。

如果不使用群組更新或自訂掃描工作，則在政策中允許本機系統工作啟動：Kaspersky Security 10.1 for Windows Server 將執行應用程式資料庫和模組更新，並根據預設排程啟動所有本機系統的自訂掃描工作。

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。

如果受防護的伺服器從管理群組中排除，則系統工作排程將自動啟用。

► *若要在政策中允許或封鎖 Kaspersky Security 10.1 for Windows Server 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，在用於配置伺服器群組上的 Kaspersky Security 10.1 for Windows Server 系統工作排程啟動的政策的上下文功能表，選擇“**內容**”指令。
3. 在“**<政策名稱>內容**”視窗中，開啟“**應用程式內容**”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 95 頁上的“關於政策”部分）為活動政策且套用於管理伺服器群組。
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 Security 10.1 for Windows Server 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伺服器上的更新和自訂掃描本機系統工作的排程（請參見第 102 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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 使用者手冊*》的相關章節。

► *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，選擇受防護伺服器所屬的群組。
     b. 在詳細資訊視窗的“**裝置**”標籤上，在包含有關受防護伺服器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工作的群組。
     b. 在詳細資訊視窗的“**工作**”標籤上開啟上下文功能表，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，請輸入工作名稱（不超過 100 個字元），不包含符號 I *<>?\/|:)。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 Security 10.1 for Windows Server**”標題下選擇要建立的工作的類型。

4. 如果您選擇了除“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“**工作設定**”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，掃描範圍包括伺服器的關鍵區域。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，請在每行上開啟上下文功能表並選擇“**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**”表格上開啟上下文功能表並選擇“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，指定伺服器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），開啟上下文功能表並選擇“**設定**”選項，然後點擊“安全等級”視窗中的“**設定**”按鈕，並在“**自訂掃描設定**”視窗的“**一般**”標籤中，取消選定“**子資料夾**”（“**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上下文功能表，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 Security 10.1 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**”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。

  a. 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 Security 10.1 for Windows Server 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“*掃描關鍵區域*”的工作執行結果來評估伺服器的安全等級，而不僅僅是根據“**掃描關鍵區域**”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 Security 10.1 for Windows Server 工作程序的優先順序為“**中**”（“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“**LAN 設定**”按鈕。將開啟“**連線設定**”視窗。

  c. 在“**連線**”設定上：

  指定 FTP 伺服器模式以便連線到受防護的伺服器。

  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。

指定受防護伺服器的位置，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“為應用程式模組下載並安裝重要更新或僅檢查它們的可用性”。

  b. 如果選擇了“**複製並安裝關鍵軟體模組更新**”：可能需要重新開機伺服器才能套用已安裝的軟體模組。如果希望工作完成時 Kaspersky Security 10.1 for Windows Server 自動重新啟動伺服器，請選定“**允許作業系統重新開機**”核取方塊。若要停用在工作完成後自動重新啟動伺服器的功能，請取消選定“**允許作業系統重新開機**”核取方塊。

  c. 若要獲得有關 Kaspersky Security 10.1 for Windows Server 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“**新的排程應用程式軟體模組更新可用**”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或啟動碼。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“裝置控制的規則產生器”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）。

5. 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“**按排程運行**”核取方塊以啟用排程；

   b. 指定工作啟動頻率：在“**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**”（也可在以下組工作中指定啟動頻率“**管理伺服器擷取更新之後**”：“資料庫更新”和“軟體模組更新”）：

      - 如果選擇了“**每小時**”，請在“**工作啟動設定**”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“**工作啟動設定**”配置群組的“**每 <數量> 天**”中指定天數。
      - 如果選擇了“**每週**”，請在“**工作啟動設定**”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**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**”值群組中的“**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“**日曆**”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“**隨機執行工作的時間間隔**”核取方塊並指定分鐘值。

e. 點擊“**確定**”。

6. 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）。
7. 在“**指定使用者帳戶以執行工作**”視窗中，指定您希望執行工作的帳戶。
8. 如果希望在建立工作後不久啟動它，則在“**完成工作建立**”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”視窗中為一台網路伺服器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，選擇受防護伺服器所屬的群組。
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：
   - 雙擊受防護伺服器的名稱。
   - 開啟受防護伺服器名稱的上下文功能表，然後選擇“**內容**”。

   將開啟“**內容：<電腦名稱>**”視窗。
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。
      - 在所選工作的上下文功能表中，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上下文功能表，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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 使用者手冊*》的相關章節。

► *為多個電腦配置群組工作：*

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。展開您想要為其設定應用程式工作設定的電腦的管理群組。
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雙擊工作名稱。
   - 在建立的工作清單中選擇工作名稱，然後點擊“**變更參數**”連結。
   - 在建立的工作清單中開啟工作名稱的上下文功能表，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“**設定**”部分中，建立掃描範圍。
     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“**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。
     b. 點擊“**連線設定**”以配置一般連線設定和更新來源連線設定。

- 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**”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，應用您要用於啟動應用程式的金鑰檔案或啟動碼。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。
- 若要配置伺服器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。

表 27. Kaspersky Security 10.1 for Windows Server 群組工作設定

Kaspersky Security 10.1 for Windows Server 工作類型	內容：<工作名稱>視窗章節	工作設定
自動規則生成（“應用程式啟動控制規則產生器”工作和“裝置控制規則產生器”工作）。	**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 Security 10.1 for Windows Server 工作類型	內容：<工作名稱>視窗章節	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** 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。 • **使用數位憑證主題和指紋** 使用此核取方塊可啟用或停用將檔案數位憑證的主題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題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 Security 10.1 for Windows Server 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。

Kaspersky Security 10.1 for Windows Server 工作類型	內容：<工作名稱>視窗章節	工作設定
		• **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。 當建立的規則必須滿足終極安全等級時，建議使用此選項：SHA256 校驗可以作為唯一檔案 ID 應用。作為 SHA256 校驗和作為規則引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。 • **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“**全部**”。 您可以使用 Kaspersky Security 10.1 for Windows Server 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。
啟動應用程式	**應用程式設定**	若要啟動應用程式或續約過期日期，您可新增啟動碼或金鑰檔案。
	排程	您可以配置排程的工作啟動設定。
複製更新	**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 ► *要開啟“**連線設定**”視窗，* 在“**更新來源**”部分中點擊“**連線設定**”按鈕。	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。

Kaspersky Security 10.1 for Windows Server 工作類型	內容：<工作名稱>視窗章節	工作設定
	複製更新設定	您可指定用於複製的更新集。 在“**已複製更新的本機存放區資料夾**”欄位中，指定 Kaspersky Security 10.1 for Windows Server 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。
資料庫更新	**更新來源**	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片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。 • **用於最佳化記憶體(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	“**連線設定**”視窗 ► *要開啟“連線設定”視窗，* 在“**更新來源**”部分中點擊“**連線設定**”按鈕。	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	**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。

Kaspersky Security 10.1 for Windows Server 工作類型	內容：<工作名稱>視窗章節	工作設定
	“**連線設定**”視窗 ► *要開啟“**連線設定**”視窗，* 在“**更新來源**”部分中點擊“**連線設定**”按鈕。	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 Security 10.1 for Windows Server 應執行的操作，還可指定 Kaspersky Security 10.1 for Windows Server 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	**設定**	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 ► *開啟“自訂掃描設定”視窗：* 在“**掃描範圍**”部分中點擊“**設定**”按鈕。	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。
	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**”塊中使用滑塊設定分析等級。 在“**進階設定**”部分中，您可配置以下設定： • 套用“自訂掃描”工作的信任區域 • 套用“自訂掃描”工作的 KSN 使用 • 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	**排程**	您可以配置排程的工作啟動設定。

對於工作（如，資料庫更新回溯），您可在“**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的管理主控台樹狀目錄中，展開“**受管理裝置**”節點。展開您想要為其設定應用程式工作設定的電腦的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。開啟工作的右鍵功能表，然後選擇“**內容**”。

   將開啟“**內容：<工作名稱>**”視窗。
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。
   - **使用數位憑證主題和指紋**

     使用此核取方塊可啟用或停用將檔案數位憑證的主題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題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 Security 10.1 for Windows Server 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應用程式啟動控制允許規則的條件。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應用程式啟動控制允許規則的條件。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。

  當建立的規則必須滿足終極安全等級時，建議使用此選項：SHA256 校驗可以作為唯一檔案 ID 應用。作為 SHA256 校驗和作為規則引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。

- **為使用者或使用者群組建立規則**。

  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 Security 10.1 for Windows Server 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的管理主控台樹狀目錄中，展開“**受管理裝置**”節點。展開您想要為其設定應用程式工作設定的電腦的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。

3. 在先前建立的組工作清單中，選擇您要配置的工作。開啟工作的右鍵功能表，然後選擇“**內容**”。

   將開啟“**內容：<工作名稱>**”視窗。

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的管理主控台樹狀目錄中，展開“**受管理裝置**”節點。展開您想要為其設定應用程式工作設定的電腦的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。開啟工作的右鍵功能表，然後選擇“**內容**”。

   將開啟“**內容：<工作名稱>**”視窗。

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。

- **用於最佳化記憶體(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。

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 Security 10.1 for Windows Server 執行什麼操作，且還可以指定當安裝關鍵更新時 Kaspersky Security 10.1 for Windows Server 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。
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。

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的管理主控台樹狀目錄中，展開“**受管理裝置**”節點。展開您想要為其設定應用程式工作設定的電腦的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。開啟工作的右鍵功能表，然後選擇“**內容**”。

   將開啟“**內容：<工作名稱>**”視窗。

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，選擇受防護伺服器所屬的群組。
     b. 在詳細資訊視窗的“**裝置**”標籤上，在包含有關受防護伺服器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**”標籤上開啟上下文功能表，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，請輸入工作名稱（不超過 100 個字元），不包含符號 I *<>?\/|:)。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 Security 10.1 for Windows Server**”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，掃描範圍包括伺服器的關鍵區域。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，請在每行上開啟上下文功能表並選擇“**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. 在“**掃描範圍**”表中按右鍵，然後選擇“**新增範圍**”。
  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，指定伺服器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. 開啟右鍵功能表，然後選擇“**設定**”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右鍵功能表，然後選擇“**設定**”。
  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。

  執行安全設定配置的方式與 Kaspersky Security 10.1 主控台中相同。
- 要略過新增的掃描範圍中的嵌入式物件：
  a. 開啟“**掃描範圍**”表的上下文功能表，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，指定伺服器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 155 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會將受信任處理程式的檔案操作新增到工作設定中設定的掃描排除項目中。

     如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 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式的檔案操作。

     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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 工作程序的優先順序為“中”（“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*”事件和重新整理伺服器防護狀態。卡巴斯基安全管理中心根據狀態為“*掃描關鍵區域*”的工作的執行結果來評估伺服器的安全等級。該核取方塊在本機系統和 Kaspersky Security 10.1 for Windows Server 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伺服器防護狀態。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 125 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**”。

將為所選伺服器或伺服器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的管理主控台樹狀目錄中，展開“**受管理裝置**”節點。展開您想要為其設定應用程式工作設定的電腦的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。開啟工作的右鍵功能表，然後選擇“**內容**”。

   將開啟“**內容：<工作名稱>**”視窗。
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。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 119 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“掃描關鍵區域”工作的執行頻率比 Kaspersky Security 10.1 for Windows Server 的“**已經有很長時間未掃描關鍵區域**”設定的指定頻率低，則卡巴斯基安全管理中心會為伺服器指定“*警告*”狀態。

► *若要設定掃描單一管理群組中的所有伺服器，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伺服器上的系統掃描工作的排程啟動（請參閱第 102 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伺服器的安全狀態，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 Kaspersky Security 10.1 主控台檢視“自訂掃描”工作是否為“關鍵區域掃描”工作。

在 Kaspersky Security 10.1 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。

在卡巴斯基安全管理中心中設定當機診斷設定

如果 Kaspersky Security 10.1 for Windows Server 執行期間發生問題（例如，Kaspersky Security 10.1 for Windows Server 當機），且您想要進行診斷，您可啟用建立 Kaspersky Security 10.1 for Windows Server 處理程序的偵錯檔案和傾印檔案，並將這些檔案傳送到 Kaspersky Lab 技術支援進行分析。

Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 設定管理。您可以配置存取權限（請參見第 87 頁上的“關於 Kaspersky Security 10.1 for Windows Server 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 108 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調試資訊寫入檔案，請選中“**將調試資訊寫入偵錯檔案**”核取方塊。
     - 在下面的欄位中指定 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 儲存到偵錯檔案的調試資訊的詳細等級。

       您可以選擇以下一種詳細等級：

       - **緊急事件** - Kaspersky Security 10.1 for Windows Server 僅將和緊急事件有關的資訊儲存到偵錯檔案。
       - **錯誤** - Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。
- **所有調試資訊** - Kaspersky Security 10.1 for Windows Server 將所有調試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“**所有調試資訊**”。

如果選中“**將調試資訊寫入偵錯檔案**”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）。

表 28. Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 控制工作。
wp	工作處理程序，處理病毒防護工作。
blgate	Kaspersky Security 10.1 for Windows Server 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 協議支援子系統
perfcount	效能計數器子系統。

Kaspersky Security 10.1 for Windows Server 管理單元 (gui) 和卡巴斯基安全管理中心的 Kaspersky Security 10.1 for Windows Server 外掛程式 (ak_conn) 的偵錯設定在這些元件重新開機後應用。SNMP 協定支援子系統 (snmp) 的跟蹤設定在 SNMP 服務重新啟動後應用。效能計數器子系統 (perfcount) 的跟蹤設定在所有使用效能計數器的處理程序都重新開機之後應用。當機診斷設定儲存後，其他 Kaspersky Security 10.1 for Windows Server 子系統的偵錯設定就會立刻應用。

預設情況下，Kaspersky Security 10.1 for Windows Server 記錄所有 Kaspersky Security 10.1 for Windows Server 元件的調試資訊。

如果選中“**將調試資訊寫入偵錯檔案**”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 Security 10.1 for Windows Server 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應用於受防護伺服器上。

管理工作排程

您可以配置 Kaspersky Security 10.1 for Windows Server 工作的啟動排程，並配置按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 Kaspersky Security 10.1 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。

► *若要配置工作排程設定，請執行以下操作：*

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，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 108 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“**頻率**”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）。
      - **應用程式啟動時**，如果您希望在每次啟動 Kaspersky Security 10.1 for Windows Server 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“**工作設定**”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啟動政策設定禁止啟動排程的系統工作，則將在“**下次開始**”欄位中顯示值“**被政策封鎖**”（請參見第 102 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“**隨機執行工作的時間間隔**”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 Kaspersky Security 10.1 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上下文功能表。
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“**按排程執行**”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 Security 10.1 for Windows Server 一般設定的資訊。

本章內容

關於透過卡巴斯基安全管理中心管理 Kaspersky Security 10.1 for Windows Server 的方式

透過卡巴斯基安全管理中心外掛程式安裝 Kaspersky Security 10.1 for Windows Server 並包含到管理群組中，可以集中管理多台伺服器。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伺服器的操作設定。

“*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 Security 10.1 for Windows Server 的多個伺服器。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 Security 10.1 for Windows Server 在某台伺服器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。

可透過以下方式透過卡巴斯基安全管理中心管理 Kaspersky Security 10.1 for Windows Server：

- **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伺服器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 Kaspersky Security 10.1 for Windows Server 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、網路附加儲存防護工作設定、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遠端設定工作的通用設定，一組伺服器具有過期期限。

  您可使用工作群組啟動應用程式，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允許遠端設定通用工作設定，不屬於任何一個管理群組的伺服器具有有限執行期限。

- **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個伺服器的工作設定。如果選中伺服器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 Security 10.1 for Windows Server 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。您可以為一組伺服器也可以為單台伺服器配置這些設定。

在卡巴斯基安全管理中心中設定一般應用程式設定

您可以透過卡巴斯基安全管理中心為一組伺服器或一個伺服器設定 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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，設定用於定義 Kaspersky Security 10.1 for Windows Server 使用的處理程序

數的設定：

- **自動偵測延伸性設定**。

  Kaspersky Security 10.1 for Windows Server 自動控制使用的處理程序數量。

  這是預設值。

- **手動設定工作處理程序數**。

  Kaspersky Security 10.1 for Windows Server 根據指定的值控制有效的工作處理程序數。

  - **最大活動處理程序數。**

    Kaspersky Security 10.1 for Windows Server 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，設定在工作列通知區域中顯示 Kaspersky Security 10.1 for Windows Server 工作列圖示：清除或選中“**在工作列中顯示應用程式圖示**”核取方塊。

5. 在“**分級儲存**”標籤上，選擇以下選項之一來存取分級儲存：

   - **非 HSM 系統**

     在執行“自訂掃描”工作時，Kaspersky Security 10.1 for Windows Server 不使用 HSM 系統設定。

     預設選中該選項。

   - **HSM 系統使用重新分析點**

     在“自訂掃描”工作期間，Kaspersky Security 10.1 for Windows Server 會使用重新分析點掃描遠端儲存中的檔案。

   - **HSM 系統使用延伸檔案內容**

     用於還原物件的資料夾的路徑，路徑格式為 UNC（通用命名慣例）。

     預設路徑為 C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\。

   - **未知的 HSM 系統**

     在“自訂掃描”工作期間，Kaspersky Security 10.1 for Windows Server 會掃描所有檔案，包括遠端儲存中的檔案。

     不建議選擇該選項。

如果您不使用 HSM 系統，請不要變更“HSM 系統設定”的預設值（非 HSM 系統）。

6. 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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 工作的還原設定。
     - **執行工作還原**

       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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會自動還原 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 不會還原 Kaspersky Security 10.1 for Windows Server 工作。

       預設將會選定該核取方塊。
     - **還原自訂掃描工作的次數不超過(次)**

Kaspersky Security 10.1 for Windows Server 傳回錯誤後嘗試還原“自訂掃描”工作的次數。如果選中“**執行工作還原**”核取方塊，則該輸入欄位才可用。

   - 在“**切換到 UPS 備用電源時的操作**”部分，指定在切換為 UPS 備用電源後 Kaspersky Security 10.1 for

Windows Server 對伺服器產生的負荷的限制：

- **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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會在電腦轉換為 UPS 電源後暫停執行掃描工作。

  如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 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。

- 在“**密碼防護設定**”部分中，設定用於防護存取 Kaspersky Security 10.1 for Windows Server 功能的密碼。

1. 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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 使用者手冊*》的相關章節。

設定的連線設定用於將 Kaspersky Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會使用 Web 代理自動探索協定 (WPAD) 自動定義與 KSN 服務的連接設定。

       預設選中該選項。
     - **使用指定的代理伺服器設定**。

       如果選擇此選項，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 的電腦位於同一網路上的電腦時啟用/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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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。
   - 要匯入排除項目，請點擊“**匯入**”按鈕，並在開啟的視窗中選擇 Kaspersky Security 10.1 for Windows Server 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**

       檔案名稱、檔案名稱遮罩、本機或卸除式電腦磁碟機、本機或網路資料夾、預設範圍等。
     - **偵測物件**

       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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 工作的名稱。
   - 如有必要，在“**備註**”欄位中指定解釋排除的附加資訊。

5. 在“**信任區域**”視窗的“**信任處理程序**”標籤上，指定掃描期間 Kaspersky Security 10.1 for Windows Server 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伺服器上安裝的備份工具執行檔案讀取操作掃描此類操作。

     如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 會略過由伺服器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 Security 10.1 for Windows Server 會掃描由伺服器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。

   - **不要限制應用程式活動**

     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 Security 10.1 for Windows Server 會在掃描期間略過受信任處理程序的操作。

     如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 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 136 頁上的“新增信任處理程序”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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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. 從按鈕上下文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 Security 10.1 for Windows Server 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. **使用處理程序檔案哈希來將它視為受信任**。

     果選中此核取方塊，則 Kaspersky Security 10.1 for Windows Server 將使用選定的檔案哈希來確定處理程序信任狀態。

     如果清除該核取方塊，則不考慮將檔案的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 Security 10.1 for Windows Server 的伺服器上必須具有管理員權限，才能檢視活動程序清單。您可以按程序的執行檔名、PID 或其在本機伺服器上的路徑來對活動程序清單中的程序進行排序。請注意，只有在本機伺服器上或透過卡巴斯基安全管理中心以指定的主機設定使用 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 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. **使用處理程序檔案哈希來將它視為受信任**。

  果選中此核取方塊，則 Kaspersky Security 10.1 for Windows Server 將使用選定的檔案哈希來確定處理程序信任狀態。

  如果清除該核取方塊，則不考慮將檔案的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“**新增信任的應用程式**”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 遮罩允許跳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。
- 指令碼監控。
- RPC-網路儲存防護。
- 流量安全。

如果未向排除清單新增該遮罩，Kaspersky Security 10.1 for Windows Server 將對此類別下的軟體或 Web 資源套用在工作設定中設定的操作。

► *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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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伺服器上的卸除式磁碟機的掃描。

Kaspersky Security 10.1 for Windows Server 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。

如果您已安裝不帶病毒資料庫的 Kaspersky Security 10.1 for Windows Server，則將無法執行卸除式磁碟機掃描。

當它們在作業系統中註冊為 USB 大容量儲存裝置時，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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）。

表 29. 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 連線到受防護伺服器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 Security 10.1 for Windows Server 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、可疑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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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，為一組電腦或單個電腦設定用於管理應用程式和 Kaspersky Security Service 的存取權限。

在卡巴斯基安全管理中心中配置 Kaspersky Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 使用者手冊*》的相關章節。

► *設定用於管理應用程式和 Kaspersky Security Service 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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 Service 的存取權限，在“**Security Service 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 87 頁上的“ 關於 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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“**儲存設定**”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**”欄位在受防護伺服器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(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”區域中選擇受防護伺服器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“**儲存設定**”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伺服器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伺服器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。

封鎖不信任主機。封鎖的主機

本節介紹如何封鎖不信任電腦和配置“封鎖的主機”儲存設定。

本章節說明項目

關於封鎖不信任主機

如果安裝以下任一元件，則預設安裝“封鎖的主機”儲存：即時防護、NetApp 的加密勒索軟體防護、加密勒索軟體防護。這些元件根據不信任主機的清單，監控遠端主機對受防護伺服器或網路附加儲存共用網路資料夾的存取嘗試。有關所有受防護伺服器封鎖的主機的資訊將傳送到卡巴斯基安全管理中心。Kaspersky Security 10.1 for Windows Server 會封鎖“封鎖的主機”清單中的所有遠端主機存取伺服器的共用網路資料夾或網路附加儲存資料夾。

在活動模式下啟動以下至少一個工作並且滿足指定條件時，將填充“封鎖的主機”儲存：

- 當“即時檔案防護”工作執行時，如果偵測到正在存取網路檔案資源的電腦存在惡意活動，並且在“即時檔案防護”工作設定中已選中“**將出現惡意活動的主機列為不信任**”核取方塊。
- 當“加密勒索軟體防護”工作執行時，如果偵測到正在存取網路檔案資源的電腦存在惡意加密行為。
- 當“用於 NetApp 的加密勒索軟體防護”工作執行時，如果偵測到對網路附加儲存的勒索軟體攻擊。

偵測到惡意活動或加密嘗試後，工作會將攻擊主機的資訊傳送到“封鎖的主機”儲存，應用程式將為主機封鎖建立一個關鍵事件。從該主機執行的任何存取受防護共用網路資料夾的嘗試都將被封鎖。

預設情況下，當不信任主機被新增到清單 30 分鐘後，Kaspersky Security 10.1 for Windows Server 將從清單中移除該主機。從不信任主機清單刪除電腦後，電腦對網路檔案資源的存取將自動還原。您可以指定之後自動解除封鎖受封鎖主機的時間段。

啟用封鎖不信任主機

要將出現任何惡意或加密活動的主機新增到“**封鎖的主機**”儲存並封鎖這些主機存取網路檔案資源，以下至少一個工作必須在活動模式下執行：

- 即時檔案防護
- 加密勒索軟體防護
- 用於 NetApp 的加密勒索軟體防護

► *配置“即時檔案防護”工作：*

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. 選擇“**政策**”標籤並開啟“**即時檔案防護**”設定塊中的“**<政策名稱> > 即時伺服器防護 > 設定**”。

   將開啟“**即時伺服器防護**”視窗。
3. 如果您想要 Kaspersky Security 10.1 for Windows Server 在執行“即時檔案防護”工作期間封鎖在其上偵測到惡意活動的主機存取網路檔案資源，則在“**與其他元件整合**”部分中，選中“**將出現惡意活動的主機列為不信任**”核取方塊。

4. 如果工作尚未啟動，請開啟“**工作管理**”標籤：
   a. 選定“**按排程執行**”核取方塊。
   b. 在下拉清單中選擇“**應用程式啟動時**”頻率。
5. 在“**即時伺服器防護**”視窗中，點擊“**確定**”。

將儲存新配置的設定。

► *配置“加密勒索軟體防護”工作：*

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. 選擇“**政策**”標籤，然後開啟“**加密勒索軟體防護**”設定塊中的“**<政策名稱 > > 網路活動控制 > 設定**”。
   將開啟“**加密勒索軟體防護**”視窗。
3. 如果工作尚未啟動，請開啟“**工作管理**”標籤：
   a. 選定“**按排程執行**”核取方塊。
   b. 在下拉清單中選擇“**應用程式啟動時**”頻率。
4. 在“**加密勒索軟體防護**”視窗中，點擊“**確定**”。

將儲存新配置的設定。

► *配置“用於 NetAPP 的加密勒索軟體防護”工作：*

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. 選擇“**政策**”標籤，然後開啟“**用於 NetApp 的加密勒索軟體防護**”設定塊中的“**<政策名稱> > 網路附加儲存防護 > 設定**”。
   將開啟“**用於 NetApp 的加密勒索軟體防護**”視窗。
3. 如果工作尚未啟動，請開啟“**工作管理**”標籤：
   a. 選定“**按排程執行**”核取方塊。
   b. 在下拉清單中選擇“**應用程式啟動時**”頻率。
4. 在“**用於 NetApp 的加密勒索軟體防護**”視窗中，點擊“**確定**”。

Kaspersky Security 10.1 for Windows Server 將封鎖出現惡意或加密活動的主機存取網路檔案資源。

配置“封鎖的主機”設定

► *要配置“封鎖的主機”儲存：*

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 108 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. 在“**選項**”部分，點擊“**信任區域**”設定區域中的“**設定**”按鈕。
   將開啟“**儲存設定**”視窗。

您可以透過政策設定配置管理伺服器的主機封鎖期限。要設定主機封鎖期限，請開啟“**<政策名稱> > 進階**”，然後點擊“**設定**”按鈕。在“**封鎖的主機**”標籤上，調整主機封鎖期限。封鎖的主機清單在政策設定中不可用。

3. 開啟“**封鎖的主機**”標籤。
4. 在“**主機封鎖期限**”部分中，指定此後受封鎖主機在被封鎖後還原存取網路檔案資源的天數、小時數和分鐘數。
5. 點擊“**已封鎖的主機清單**”按鈕。
6. 執行以下步驟之一：
   - 在開啟的“**不受信任的主機清單**”視窗中，選擇要還原其存取的主機，然後點擊“**從清單刪除**”按鈕。
   - 點擊“**刪除整個清單**”可刪除不受信任的主機清單中的主機或還原所有已封鎖的主機的存取。
7. 點擊“**確定**”。

   將取消封鎖或從封鎖的主機清單刪除選定的電腦。
8. 點擊“**儲存設定**”視窗中的“**確定**”。

將儲存新配置的“封鎖的主機”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 Security 10.1 for Windows Server 和受防護伺服器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；
- 存取受防護伺服器的區網使用者和終端伺服器使用者可以收到與*偵測到的物件*類型事件有關的資訊。

可使用選定電腦的“**內容：<電腦名稱>**”視窗為單個電腦，或使用選定管理員群組的“**內容：<政策名稱>**”視窗中為一組電腦配置有關 Kaspersky Security 10.1 for Windows Server 事件的通知。

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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 使用者手冊*》的相關章節。

► *要設定 Kaspersky Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。

安全事件記錄

Kaspersky Security 10.1 for Windows Server 保持有與受防護伺服器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。
- 關鍵記錄檢查事件。
- 表示嘗試進行安全入侵的緊急事件（對於“即時防護”、“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 Security 10.1 for Windows Server 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 協議將稽核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伺服器上的負載。

- 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 Security 10.1 for Windows Server 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）。

表 30. 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。
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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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“**事件建立上限值**”部分中，指定 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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，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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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**”標籤上，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. 在開啟的視窗中，選擇 Kaspersky Security 10.1 for Windows Server 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：
   - 有關隔離物件的資訊。
   - 有關備份物件的資訊。
   - 有關封鎖的主機的資訊。
5. 點擊“**確定**”。

Kaspersky Security 10.1 for Windows Server 會將有關選定物件類型的資訊傳送到啟動伺服器。

即時伺服器防護

本節提供有關即時防護工作（即時檔案防護、指令碼監控、KSN 使用和弱點利用防禦）的資訊。它還提供有關如何設定即時防護工作和管理受防護伺服器的安全設定說明。

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伺服器物件時，Kaspersky Security 10.1 for Windows Server 會對這些物件進行掃描：

- 檔案。
- 檔案交換系統執行緒（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 容器檔案。

當任何應用程式將檔案寫入伺服器或從伺服器上讀取檔案時，Kaspersky Security 10.1 for Windows Server 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，則執行預設操作或您所指定的操作：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 Security 10.1 for Windows Server 會將檔案返回給

應用程式。

Kaspersky Security 10.1 for Windows Server 會攔截在 Windows Server 2016 容器中執行的檔案操作。

*容器*是獨立的環境，允許應用程式在不影響作業系統或不被作業系統影響的情況下執行。如果容器位於工作防護範圍內，Kaspersky Security 10.1 for Windows Server 會掃描被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 Security 10.1 for Windows Server 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。

表 31. “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在以後應用於其他節點。
物件防護模式	存取和修改時	您可以選擇防護模式，即定義 Kaspersky Security 10.1 for Windows Server 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。
“KSN 使用”服務	已使用	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。
工作啟動排程	程式啟動時	您可以配置排程的工作啟動設定。
將顯示惡意活動的主機列為不信任	未套用	可以將電腦展示的惡意活動新增到不信任的主機清單中。

► *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：

   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 155 頁上的“選擇防護模式”部分）。
     - 使用啟發式分析（第 155 頁上）
     - 與其他 Kaspersky Security 10.1 for Windows Server 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 125 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 157 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、資料夾或網路位置**
       - **檔案**
     - 選擇一項預設安全等級（請參見第 158 頁上的“選擇預設安全等級”部分）或手動配置防護（請參見第 159 頁上的“手動配置安全設定”部分）。

   > 要對工作應用新的設定防護範圍，必須重啟“即時檔案防護”工作。

6. 在“**即時檔案防護**”視窗中點擊“**確定**”。

Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 128 頁上的“ 關於透過卡巴斯基安全管理中心管理 Kaspersky Security 10.1 for Windows Server 的方式”部分）或政策設定（請參見第 97 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應用到正在執行的工作。如果工作未執行，則將在下次啟動時應用修改後的設定。

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 Security 10.1 for Windows Server 在掃描物件時所採用的存取類型。

“**物件防護模式**”設定中的值應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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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. 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 僅在處理程序最後一次儲存物件之後重新掃描該物件。
   - **存取和修改時**

     Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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

受防護伺服器的檔案資源顯示在“**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 Security 10.1 for Windows Server 覆寫以下預定義防護範圍：

- **本機硬碟磁碟機**。Kaspersky Security 10.1 for Windows Server 將防護伺服器硬碟磁碟機上的檔案。
- **卸除式硬碟**。Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將掃描伺服器上運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 Security 10.1 for Windows Server 不會防護此類檔案。
- **虛擬硬碟**。您可以將動態資料夾和檔案以及臨時連線到伺服器的硬碟包含在防護範圍內，例如共用叢集硬碟。

預設情況下，您可以在網路檔案資源樹狀目錄中檢視和配置預設防護範圍；還可以在網路檔案資源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 命令建立的虛擬硬碟將不會顯示在 Kaspersky Security 10.1 主控台的伺服器檔案資源樹狀目錄中。若要將虛擬硬碟中的物件包含在防護範圍內，

請將與此虛擬磁碟機關聯的伺服器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伺服器檔案資源樹狀目錄中。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所選的節點套用以下一項預設安全設定：“**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

如果除了在伺服器和工作站上使用 Kaspersky Security 10.1 for Windows Server 外，還在網路內採取了其他伺服器安全措施（例如，防火牆和現有安全原則），則建議使用“**最佳效能**”安全等級。

建議

“**建議**”安全等級確保防護與對伺服器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伺服器。預設情況下，將設定“**建議**”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。

表 32. 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
僅防護新的和修改過的檔案	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
對可疑物件執行的操作	封鎖存取並隔離	封鎖存取並隔離	封鎖存取並隔離
排除檔案	否	否	否
不偵測	否	否	否
執行超過以下時間時停止掃描（秒）	60 秒	60 秒	60 秒
不掃描大於該值的複合物件(MB)	8 MB	8 MB	未設定
掃描 NTFS 交換資料串流	是	是	是
掃描開機磁區與 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* • 已封裝的物件* • 內嵌的 OLE 物件* *僅新物件和已修改的物件	• SFX 壓縮檔* • 已封裝的物件* • 內嵌的 OLE 物件* *所有物件

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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. 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 Security 10.1 for Windows Server 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 158 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，或為伺服器檔案資源清單或樹狀目錄中的不同節點配置不同設定。

在使用伺服器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使用網路檔案資源樹狀目錄時的所有子節點。父節點的安全設定不會應用到單獨配置的子節點。

► *若要手動設定所選節點的安全性設定，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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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. 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**”。
5. 點擊“**配置**”按鈕可根據您的需求編輯選定節點的安全設定。為此，請執行以下操作：
   - 在“**一般**”標籤上，配置以下設定（如有必要）：

     在“**物件防護**”部分中，指定要包含在防護範圍內的物件：
     - **所有物件**

       Kaspersky Security 10.1 for Windows Server 掃描所有物件。
     - **按格式掃描物件**

       Kaspersky Security 10.1 for Windows Server 僅根據檔案格式掃描感染物件。

       Kaspersky Lab 編制了該格式清單。它包含在 Kaspersky Security 10.1 for Windows Server 資料庫中。
     - **按病毒資料庫中指定的副檔名清單掃描物件**

       Kaspersky Security 10.1 for Windows Server 僅根據檔案副檔名掃描感染的物件。

       Kaspersky Lab 編制了該副檔名清單。它包含在 Kaspersky Security 10.1 for Windows Server 資料庫中。
     - **按指定的副檔名清單掃描物件**

       Kaspersky Security 10.1 for Windows Server 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。
     - **掃描開機磁區與 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 Security 10.1 for Windows Server 將掃描伺服器的硬碟磁碟機和卸除式磁碟機上的開機磁區和主引導記錄。

       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，Kaspersky Security 10.1 for Windows Server 將掃描其他檔案和資料夾執行緒。

  預設將會選定該核取方塊。

在“**效能**”部分中，選中或清除以下核取方塊：

- **僅防護新的和修改過的檔案**

  使用此核取方塊可啟用/停用對自上次掃描以來 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描和防護所有檔案。

  對於“**最佳效能**”安全等級，預設選定該核取方塊。如果設定“**建議**”或“**最佳防護**”安全等級，則取消選中該核取方塊。

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 Security 10.1 for Windows Server 將掃描壓縮檔案。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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**

  掃描自解壓壓縮檔案。

  如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描 SFX 壓縮檔案。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將掃描郵件資料庫檔案。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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）封包的可執行檔案。

  如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描由封包程式封包的可執行檔案。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將在掃描期間略過由封包程式封包的可執行檔案。

  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 Security 10.1 for Windows Server 將掃描郵件格式檔案。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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/僅新的內嵌 OLE 物件**

  掃描嵌入到檔案中的物件（如 Microsoft Word 宏或電子郵件附件）。

  如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描嵌入到檔案中的物件。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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。

如果選中“**僅防護新檔案和已修改的檔案**”核取方塊，您可以選擇防護所有或僅新的複合物件。如果取消選中“**僅防護新檔案和已修改的檔案**”核取方塊，Kaspersky Security 10.1 for Windows Server 會防護所有指定複合物件。

- 在“**操作**”標籤上，配置以下設定（如有必要）：
  - 選擇對受感染的物件執行的操作。
  - 選擇對可疑的物件執行的操作。
  - 選擇依威脅類型對物件執行的操作。
  - 選擇對不可還原的複合物件執行的操作：選擇或清除“**在偵測到嵌入感染或其他物件時完全刪除無法解毒病毒的複合物件**”核取方塊。

    當偵測到惡意子物件或其他物件時，此核取方塊可啟用或停用強制刪除父物件。

    如果已選中此核取方塊且針對受感染和可疑感染物件選定要執行的操作為“**封鎖存取並刪除**”，則當偵測到惡意子物件或其他物件時，Kaspersky Security 10.1 for Windows Server 將強制刪除整個父物件。如果應用程式無法僅刪除偵測到的子物件（例如，如果父物件不可變），則強制刪除父物件及其所有內容。

如果已清除此核取方塊且針對受感染和可疑感染物件選定要執行的操作為“**刪除**”，則如果父容器為不可變，當偵測到惡意子物件或其他物件時，Kaspersky Security 10.1 for Windows Server 不會針對父容器執行選定的操作。

預設情況下，選中“**最佳防護**”安全等級核取方塊。預設情況下，清除“**建議**”和“**最佳效能**”安全等級核取方塊。

- 在“**效能**”標籤上，配置以下設定（如有必要）：

  在“**排除**”部分中：

  - **排除檔案**

    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 Security 10.1 for Windows Server 將在掃描期間略過指定的物件。

    如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描所有物件。

    預設取消選定該核取方塊。

  - **不偵測**

    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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。

  在“**進階設定**”部分中：

  - **執行超過以下時間時停止掃描（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。

  - **不掃描大於該值的複合物件(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 Security 10.1 for Windows Server 將在病毒掃描期間略過大小超過指定限制值的複合物件。

    如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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 iChecker 技術**

    僅掃描上次掃描後新建和那些修改過的檔案。

如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 僅掃描自上次掃描以來新建或修改的檔案。

如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 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。

- **使用 iSwift 技術**

  僅掃描上次掃描 NTFS 系統物件後新建和那些修改過的檔案。

  如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。

6. 點擊“**確定**”。

已儲存新配置的設定。

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 (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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 從卡巴斯基安全網路接收的資訊僅與程式的信譽和 URL 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 Security 10.1 for Windows Server 後，做出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 Security 10.1 for Windows Server 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。
- 流量安全。
- RPC 網路儲存防護。
- ICAP 網路儲存防護。

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“KPSN”）的詳細資訊，請參見《*卡巴斯基安全管理中心說明*》。

如果您正在受防護電腦上使用卡巴斯基專屬安全網路，則在“KSN 使用”工作的“**資料處理**”視窗（參見第 168 頁的“配置資料處理”部分）中，您可以透過選擇“**我接受加入卡巴斯基專屬安全網路的條款**”閱讀 KPSN 聲明和隨時啟用該工作。接受該條款，即表示您同意將 KPSN 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 KPSN 條款後，調整 Global KSN 使用的核取方塊將變為不可用。

如果“KSN 使用”工作正在執行時停用 KPSN，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，需要接受**資料處理**視窗中的全球 KSN 聲明並重新啟動該工作。

配置“KSN 使用”工作

如果您不接受 KSN 聲明，則無法啟動“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）。

表 33. “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 Security 10.1 for Windows Server 對 KSN 標識為受感染的物件執行的操作。
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 演算法為其計算檢驗碼以提交給 KSN 的檔案的最大大小。如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 將為任意大小的檔案計算 MD5 雜湊校驗碼。
接受卡巴斯基安全網路聲明的條款	未接受	在安裝後決定是否要參加 KSN。您可以隨時變更決定。
同意處理資料作為卡巴斯基安全網路統計資訊的一部分	未接受	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。
接受 Kaspersky Managed Protection 聲明的條款	未接受	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單獨協議，該服務才可用。
工作啟動	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。

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”部分中，點擊“**KSN 使用**”設定塊中的“**設定**”按鈕。

   將開啟“**工作設定**”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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將刪除具有 KSN 受感染狀態的物件，並在備份中放置副本。

預設選中該選項。

- **記錄資訊**

  Kaspersky Security 10.1 for Windows Server 將在工作記錄中記錄有關具有 KSN 受感染狀態的物件的資訊。Kaspersky Security 10.1 for Windows Server 不會刪除受感染物件。

- 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碼，以將此資訊提交至 KSN 服務。

    校驗碼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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。

  a. 如果需要，在右側欄位中指定 Kaspersky Security 10.1 for Windows Server 要為其計算校驗和的最大檔案大小。

  b. 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從受防護伺服器到 KSN 的資料傳輸。

     如果清除該核取方塊，管理伺服器和受防護伺服器的資料不會傳送到 KSN。但是，根據設定，伺服器可以直接向 KSN 傳送資料（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伺服器時自動執行該工作，可以按排程啟動工作並指定“**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 168 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”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“**服務**”標籤上，閱讀聲明並選中“**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：
   - **傳送關於掃描的檔案的資料**。

     如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 不會將檔案的校驗和傳送到 KSN。

     預設將會選定該核取方塊。
   - **傳送關於請求的 URL 的資料**。

     如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 會將有關請求的 Web 資源（包括網址）的資料傳送到 Kaspersky Lab。 關於請求的 Web 資源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 Security 10.1 for Windows Server 不會在 KSN 中檢查 URL 信譽。

     預設將會選定該核取方塊。

     該核取方塊影響“流量安全”工作配置。

   您可以隨時清除這些核取方塊並停止傳送附加資料。
6. 開啟“**統計資訊**”標籤。預設情況下，“**同意處理資料作為卡巴斯基安全網路統計資訊的一部分**”核取方塊已選中。如果您不希望 Kaspersky Security 10.1 for Windows Server 將其他統計資訊傳送到 Kaspersky Lab，可以隨時清除該核取方塊。

   如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 會傳送統計資訊（包括 KSN 聲明中指定的個人資料）。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 Security 10.1 for Windows Server 不會傳送其他統計資訊。

預設將會選定該核取方塊。

7. 在“**Kaspersky Managed Protection**”標籤上，閱讀聲明並選中“**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伺服器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“**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 Security 10.1 for Windows Server。

要使用 KMP 服務，您需要簽訂服務協議並在受防護伺服器上執行設定檔。

要使用 KMP 服務，必須接受“服務”和“統計資訊”標籤上的 KSN 聲明的資料處理條款。

8. 點擊“**確定**”。

將儲存資料處理配置。

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

關於弱點利用防禦工作

Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。可能需要重新啟動伺服器（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 Security 10.1 for Windows Server 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 Broker 主機服務

受防護的伺服器上必須提供 Kaspersky Security Broker 主機服務，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。在受防護的伺服器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 Broker 主機服務停止後，Kaspersky Security 10.1 for Windows Server 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，並使用所有可用的攻擊緩解技術來防護處理程序記憶體。

如果 Kaspersky Security Broker 主機服務已停止，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，應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 Security 10.1 for Windows Server 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“經過篩選的安全稽核”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 Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”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利用弱點**。

     如果選中此核取方塊，則 Kaspersky Security 10.1 for Windows Server 可降低弱點在受防護的處理程序清單的處理程序中被利用的風險。

     如果清除此核取方塊，則 Kaspersky Security 10.1 for Windows Server 不會防護伺服器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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 顯示一個終端視窗。無論 Kaspersky Security Broker 主機服務的狀態如何，都會顯示終端視窗。預設將會選定該核取方塊。

- **即使 Kaspersky Security Service 已停用，也減輕弱點利用的風險**。

  如果選中此核取方塊，則無論 Kaspersky Security Service 是否執行，Kaspersky Security 10.1 for Windows Server 都將降低弱點在已啟動的處理程序中被利用的風險。Kaspersky Security 10.1 for Windows Server 不會防護 Kaspersky Security Service 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 Service 停止時，Kaspersky Security 10.1 for Windows Server 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。

  如果選中此核取方塊，則 Kaspersky Security 10.1 for Windows Server 可降低弱點在受防護的處理程序清單的處理程序中被利用的風險。

  如果清除此核取方塊，則 Kaspersky Security 10.1 for Windows Server 不會防護伺服器處理程序免遭弱點利用。

  預設取消選定該核取方塊。

6. 點擊“**確定**”。

Kaspersky Security 10.1 for Windows Server 將儲存和套用已配置的處理程序防護設定。

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。您可以在受防護處理程序清單中取消選中您不想防護的處理程序。

► *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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”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“**開啟**”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。
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。預設時應用所有技術。

   - **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. 選擇您要應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. 配置攻擊緩解技術“受攻擊面減少”的設定：

    - 輸入其啟動將受到“**不允許模組**”欄位中受防護的處理程序封鎖的模組的名稱。
    - 在“**不禁止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**”。

該處理序將新增到工作防護範圍中。

攻擊緩解技術

表 34. 攻擊緩解技術

攻擊緩解技術	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。
匯出位址表存取監視（EAT 存取監視和透過調試寄存器的 EAT 存取監視器）	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	防止將記憶體分配用於執行惡意程式碼。
執行流模擬（反返回導向編程）	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	透過受防護的處理程序封鎖啟動易受攻擊的載入項。

指令碼監控

本節包含有關“指令碼監控”工作以及如何設定的資訊。

本章節說明項目

關於“指令碼監控”工作

“指令碼監控”工作正在執行期間，Kaspersky Security 10.1 for Windows Server 將控制使用 Microsoft Windows 指令碼技術（或 Active Scripting）建立的指令碼（例如 VBScript 或 JScript®）的執行情況。只有在確定指令碼安全後 Kaspersky Security 10.1 for Windows Server 才會允許執行。Kaspersky Security 10.1 for Windows Server 會檢查指令碼，並自動限制執行其歸為惡意類的指令碼。如果 Kaspersky Security 10.1 for Windows Server 將指令碼識別為可能存在危險，它或按照您選擇的操作封鎖或允許執行指令碼。

預設情況下，“指令碼監控”工作在 Kaspersky Security 10.1 for Windows Server 啟動時自動啟動。

預設情況下，“指令碼監控”元件未作為應用程式的一部分在伺服器上安裝。

該元件的使用可能與受防護伺服器上安裝的某些協力廠商應用程式不相容。在這種情況下，監控協力廠商指令碼可能導致指令碼執行錯誤。建議不使用此類協力廠商應用程式或停用“指令碼監控”工作。如果停用該工作，與指令碼執行安全性相關的風險將提高。

如果您想要使用“指令碼監控”元件，您必須在 Kaspersky Security 10.1 for Windows Server 安裝過程中從已安裝元件清單中手動選擇它。

有關安裝過程中選擇應用程式元件的詳細資訊，請參見*《Kaspersky Security 10.1 for Windows Server 管理手冊》的安裝部分*。

您可以配置“指令碼監控”工作設定。

設定“指令碼監控”工作設定

“指令碼監控”系統工作使用下表敘述的預設設定。您可以變更這些設定值。

表 35. “指令碼監控”工作預設設定

設定	預設值	敘述
執行受感染指令碼	已封鎖	Kaspersky Security 10.1 for Windows Server 始終封鎖執行被識別為受感染的指令碼。
執行可疑危險指令碼	已封鎖	您可以指定在偵測到可疑危險指令碼時要執行的操作：封鎖或允許執行指令碼。
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。
信任區域	已使用	可用於所選工作中的一般排除清單。

► *配置“指令碼監控”工作：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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。

將開啟“**內容：指令碼監控**”視窗。

3. 在“**對可疑危險指令碼執行的操作**”部分中，執行以下操作之一：
   - 要允許執行可疑危險指令碼，請選擇“**允許**”。

     Kaspersky Security 10.1 for Windows Server 將允許執行可疑危險指令碼。
   - 要禁止執行可疑危險指令碼，請選擇“**封鎖**”。

     Kaspersky Security 10.1 for Windows Server 將封鎖執行可疑危險指令碼。

     預設選中該選項。
4. 在“**啟發式分析**”部分中，執行以下操作之一：
   - 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。
   - 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。
5. 在“**信任區域**”部分中，選中或清除“**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 Security 10.1 for Windows Server 會將受信任處理程式的檔案操作新增到工作設定中設定的掃描排除項目中。

   如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 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式的檔案操作。

   預設將會選定該核取方塊。
6. 點擊“**確定**”。

套用了新配置的設定。

流量安全

本節包含有關“流量安全”工作以及如何設定的資訊。

本章節說明項目

關於“流量安全”工作

“流量安全”元件處理 Web 流量（包括透過郵件服務接收的流量）並攔截和掃描透過 Web 流量傳輸的物件，以偵測已知電腦和受防護伺服器上的其他威脅。ICAP 服務掃描傳入流量是否存在威脅，並根據掃描結果和配置的掃描設定來封鎖或允許流量。

Kaspersky Security 10.1 for Windows Server 還會攔截在 Linux 的 Windows 子系統下執行的任何處理程序所請求的流量。對於此類處理程序，“流量安全”工作將套用當前工作配置定義的操作。

預設情況下安裝“流量安全”。安全完成後，將註冊並啟動以下工作：

- Kaspersky Security Broker Host (KAVFSWH)
- Kaspersky Traffic Security (KAVFSPROXY)

該元件提供以下類型的防護：

- 郵件威脅防護：
  - 釣魚防護
  - 針對郵件傳輸的惡意軟體的防護
- Web 威脅防護：
  - 釣魚防護
  - 惡意 URL 掃描

- 針對基於 Web 的惡意軟體的防護
- Web 控制：
  - URL 控制
  - 憑證控制
  - 基於類別的 Web 控制

強烈建議在啟動“流量安全”工作時使用 KSN 服務，以增強威脅偵測。KSN 雲端資料庫比本機病毒資料庫包含更多的 Web 威脅實際資料。多個 Web 控制類別的分析完全基於從 KSN 服務收到的信譽。

流量安全模式

“流量安全”可以在以下模式下執行：

- **驅動程式攔截器：**應用程式使用網路驅動程式攔截流量。它使用網路內核驅動程式攔截並分析指定連接埠的所有傳入流量。
- **重定向器：**應用程式透過配置瀏覽器重定向流量。傳入流量在開啟的終端工作階段中從瀏覽器重定向至內部代理。Kaspersky Security 10.1 for Windows Server 被指定為內部代理。
- **外部代理：**應用程式處理來自外部代理伺服器的流量。流量從外部代理伺服器傳輸到 Kaspersky Security 10.1 for Windows Server。應用程式會分析流量並推薦對外部代理的操作。Kaspersky Security 10.1 for Windows Server 僅與透過 ICAP 協定傳輸流量的代理相容。

關於流量安全規則

Kaspersky Security 10.1 for Windows Server 允許您新增和配置針對憑證和 Web 位址的允許或拒絕規則，並使用預設的類別規則來封鎖不需要的內容。如果工作在**驅動程式攔截器**或**重定向器**模式下執行，可以套用針對憑證的規則。

Web 控制

此類型的控制透過套用針對 Web 位址和憑證的允許和拒絕規則來執行。允許規則的優先順序高於 KSN 結論和簽章分析的優先順序。

可以根據已排定優先順序的結論（從最高到最低）允許或封鎖 URL 或憑證：

1. 允許或拒絕規則。
2. 釣魚防護和病毒資料庫。
3. KSN。
4. 類別。

基於類別的 Web 控制

Kaspersky Security 10.1 for Windows Server 允許您根據類別封鎖 Web 位址。您可以設定用於分類的啟發式分析的等級。基於類別的 Web 控制使用預設的類別清單進行分析。儘管無法修改清單本身，但您可以選擇 Web 資源的類別來允許或封鎖，或者關閉基於類別的控制。“其他”類別包括不在該清單中任何其他類別下的所有 Web 資源。如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 允許所有未分類的 Web 資源。如果清除該核取方塊，將封

鎖所有 Web 資源。

分類的優先順序最低。

預設情況下，Kaspersky Security 10.1 for Windows Server 只套用一種規則：針對 TOR 憑證的拒絕規則。您可以在規則設定中取消選中該規則以允許 TOR 連線。 如果套用該規則，將封鎖所有傳入或傳出 TOR 連線。

“流量安全”還會考慮 not-a-virus 遮罩的結論，它們本身不是病毒，而是可用來破壞受防護伺服器的資源或物件。預設情況下，Kaspersky Security 10.1 for Windows Server 不將 not-a-virus 遮罩套用於類別（請參見第 195 頁上的“配置基於類別的 Web 控制”部分）。

郵件威脅防護

“流量安全”元件可掃描 Microsoft Outlook（2010、2013 和 2016 32 位元/64 位元）中的郵件。郵件威脅防護透過與 Kaspersky Security 10.1 for Windows Server 元件分開安裝的 Kaspersky Security 10.1 Microsoft Outlook 載入項提供。

僅當在受防護伺服器上安裝 Kaspersky Security 10.1 for Windows Server 和 Microsoft Outlook 郵件用戶端後，才能安裝 Kaspersky Security 10.1 Microsoft Outlook 載入項。

► *要安裝該外掛程式，請執行 \email_plugin 資料夾中的 ksmail_x86(x64).msi 套裝軟體。*

郵件威脅防護包括：

- 傳入電子郵件掃描。
- 病毒防護電子郵件掃描。
- 附件（包括已封裝的物件）的病毒掃描。
- 釣魚防護電子郵件掃描。
- 附件（包括已封裝的物件）的釣魚防護掃描。

如果偵測到威脅，Kaspersky Security 10.1 for Windows Server 將：

- 刪除附件。
- 修改受感染的電子郵件內文。
- 記錄*偵測到郵件威脅*事件。

Kaspersky Security 10.1 for Windows Server 在電子郵件被開啟時掃描電子郵件，而在伺服器收到電子郵件時不進行掃描。掃描僅在第一次開啟時執行一次。掃描後的電子郵件和附件儲存在快取中，直到 Outlook 重新啟動。重新啟動後，所有電子郵件在再次開啟時將被掃描。

► *外接程式在啟動時載入到 Microsoft Outlook 郵件用戶端。如果在 Outlook 執行時安裝 Kaspersky Security 10.1 Microsoft Outlook 載入項：*

1. 開啟“**檔案 > 選項 > 外接程式**”。
2. 確保 Kaspersky Security 10.1 Microsoft Outlook 載入項已新增到清單（活動或非活動）之一。
3. 重新啟動 Microsoft Outlook。
4. 檢查 Kaspersky Security 10.1 Microsoft Outlook 載入項的狀態（應變為*活動*）。

配置“流量安全”工作

可以變更“流量安全”工作的預設設定（請參見下表）。

表 36. “流量安全”工作預設設定

設定	預設值	敘述
工作模式	外部代理	ICAP 服務處理來自外部代理伺服器的流量。
網路連接埠號	1345	ICAP 服務的預設連接埠號。
服務 ID	webscan	已安裝的防毒伺服器的位址的 ICAP 服務識別碼。
使用惡意 URL 資料庫掃描網頁連結	已套用	啟用或停用對每個 URL 的簽章分析。
使用釣魚防護資料庫掃描網頁	已套用	啟用或停用基於啟發式分析的釣魚防護掃描。
使用 KSN 防護	已套用	在執行工作時，可以使用 KSN 應用程式信譽資料進行防護。
使用信任區域	已套用	如果需要，可以套用信任區域。
安全等級	建議	選擇並設定病毒防護的安全等級。
工作啟動排程	不設定工作的初次啟動排程。	“流量安全”服務不會自動啟動。您可以手動啟動該工作或設定排程啟動。

► *要配置“流量安全”工作：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108

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“**即時伺服器防護**”部分的“**流量安全**”設定塊中，點擊“**設定**”按鈕。

   將開啟“**流量安全**”視窗。

4. 在“**工作模式**”標籤上，選擇並設定工作執行模式（請參見第 181頁上的“選擇工作執行模式”部分）。
5. 在“**URL 和 Web 處理**”標籤上，配置 URL 的釣魚防護和病毒掃描（請參見第 190 頁上的“配置 URL 和 Web 處理”部分）。
6. 在“**惡意軟體防護**”標籤上，配置啟發式分析和安全等級（請參見第 186 頁上的“配置針對基於 Web 的惡意軟體的防護”部分）。
7. 在“**工作管理**”標籤上，啟動基於排程的工作（請參見第 125 頁上的“管理工作排程”部分）。
8. 點擊“**確定**”。

工作配置即被儲存。

選擇工作執行模式

► *要配置工作執行模式：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”部分的“**流量安全**”設定塊中，點擊“**設定**”按鈕。

   將開啟“**流量安全**”視窗。

4. 在“**一般**”標籤上，從“**工作模式**”下拉清單中選擇一個可用模式：
   - **驅動程式攔截器**（請參見第 182 頁上的“**配置驅動程式攔截器模式**”部分）
   - **重定向器**（請參見第 184 頁上的“**配置重定向器**”部分）
   - **外部代理**

5. 指定 ICAP 服務連線設定（全部三種模式都需要）：

   - **網路連接埠號**

     Kaspersky Security 10.1 for Windows Server 的 ICAP 服務的連接埠號。

   - **服務 ID**

     構成 ICAP 的 RESPMOD URI 參數一部分的 ID（請參閱文件 RFC 3507）。RESPMOD URI 指定為網路儲存區域安裝的病毒防護 ICAP 伺服器的位址。

     例如，如果受防護伺服器的 IP 位址為 192.168.10.10，連接埠號為 1345，ICAP 服務 ID 為 webscan，則對應的 RESPMOD URI 位址為 icap://192.168.10.10/webscan:1345

6. 配置所選工作模式。

   > **外部代理**模式無需任何附加配置。配置在外部代理伺服器上執行。

7. 點擊“**確定**”。

配置即被儲存。

配置驅動程式攔截器模式

► *在“**流量安全**”視窗中：*

1. 選擇“**一般**”標籤。
2. 選擇“**驅動程式攔截器**”工作模式。
3. 在“**工作模式設定**”部分中，配置以下設定：

   - **掃描 HTTPS 流量**。

     如果選中該核取方塊，將解壓縮攔截的加密 HTTPS 流量並掃描其中是否存在威脅。

     如果清除該核取方塊，則不解壓縮加密的 HTTPS 流量。

     預設將會選定該核取方塊。

     > 僅當 HTTPS 連接埠開放時，才能進行掃描。

   - 選擇您要使用的加密協定的版本：
     - **TLS 1.0**
     - **TLS 1.1**
     - **TLS 1.2**

     > 預設選中“**TLS 1.0**”核取方塊，且無法修改。

   - **不要信任具有無效憑證的 Web 伺服器**。

如果選中了“**掃描 HTTPS 流量**”核取方塊，則可以選中該核取方塊。

如果選中該核取方塊，具有無效憑證的網頁將被封鎖（憑證已到期、簽章驗證錯誤、憑證已撤銷等）。

- **安全連接埠**。

  指定用來將來自瀏覽器或網路驅動程式的流量重定向到 Kaspersky Security 10.1 for Windows Server 建立的內部連接埠以偵測基於 Web 的威脅的連接埠號。不推薦修改預設連接埠。該連接埠號不得與任何為 ICAP 服務開放的連接埠相同。如果使用“**重定向器**”工作模式，已在使用的連接埠將列在“**掃描 HTTPS 流量**”欄位中。

4. 要向攔截區域新增連接埠或從中排除連接埠，請點擊“**配置攔截區域**”按鈕。

   將打開“**攔截區域**”視窗。

5. 在“**攔截連接埠**”標籤上選擇以下選項之一：

   - **全部攔截**
   - **攔截指定連接埠**：

     a. 在文字欄位中輸入連接埠號。您可以新增多個連接埠，方法是在連接埠號之間使用分號分隔符號。

     b. 點擊“**新增**”。

     連接埠包括在攔截區域中。

   預設情況下，Kaspersky Security 10.1 for Windows Server 將攔截透過以下連接埠傳輸的流量：80、8080、3128、443。

6. 要在“**排除連接埠**”標籤上指定要從攔截區域中排除的連接埠：

   a. 在文字欄位中輸入連接埠號。您可以新增多個連接埠，方法是在連接埠號之間使用分號分隔符號。

   b. 點擊“**新增**”。

   連接埠從區域中排除。

   預設情況下，Kaspersky Security 10.1 for Windows Server 將排除其他應用程式使用的連接埠，並可能在嘗試讀取透過加密連線傳輸的資料時導致問題：3389、1723、13291。

7. 要在“**排除 IP 位址**”標籤上從攔截區域中排除 IP 位址：

   a. 輸入 IPv4 格式的 IP 位址或遮罩。

   b. 點擊“**新增**”。

   c. 點擊“**確定**”以儲存更改。

8. 要在“**排除處理程序**”標籤上排除需要流量交換的處理程序或可執行檔：

   a. 選中“**針對處理程序套用排除項目**”核取方塊。

   b. 要排除檔案：

      1. 點擊“**可執行檔**”按鈕。

         將顯示標準“**開啟**”視窗。

2. 選擇要排除的可執行檔，然後點擊“**開啟**”。

c. 要排除本機電腦上執行的處理程序：

1. 點擊“**正在執行的處理程序**”按鈕。

將顯示“**活動處理程序**”視窗。

2. 選擇一個目前正在執行的處理程序，然後點擊“**確定**”。

> 不能在卡巴斯基安全管理中心中選擇處理程序。

9. 在“**流量安全**”視窗中，點擊“**確定**”按鈕。

工作模式配置即被儲存。

配置重定向器模式

► *在“流量安全”視窗中：*

1. 選擇“**一般**”標籤。
2. 選擇“**重定向器**”工作模式。
3. 在“**工作模式設定**”部分中，配置以下設定：
   - **掃描 HTTPS 流量**。

     如果選中該核取方塊，將解壓縮攔截的加密 HTTPS 流量並掃描其中是否存在威脅。

     如果清除該核取方塊，則不解壓縮加密的 HTTPS 流量。

     預設將會選定該核取方塊。

     > 僅當 HTTPS 連接埠開放時，才能進行掃描。

   - 選擇您要使用的加密協定的版本：
     - **TLS 1.0**
     - **TLS 1.1**
     - **TLS 1.2**

     > 預設選中“**TLS 1.0**”核取方塊，且無法修改。

   - **檢查後將流量重定向到外部代理**。

     如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 會將已掃描的流量重定向到外部代理（例如，在公司網路內使用的公司代理伺服器）。

     如果清除該核取方塊，流量將直接傳送到內部代理。

   - **代理伺服器位址**。

     用於重定向的內部終端代理伺服器的位址。輸入 IPv4 格式的位址。

   - **連接埠**。

內部代理的連接埠號。

- **安全連接埠**。

  指定用來將來自瀏覽器或網路驅動程式的流量重定向到 Kaspersky Security 10.1 for Windows Server 建立的內部連接埠以偵測基於 Web 的威脅的連接埠號。不推薦修改預設連接埠。該連接埠號不得與任何為 ICAP 服務開放的連接埠相同。如果使用“**重定向器**”工作模式，已在使用的連接埠將列在“**掃描 HTTPS 流量**”欄位中。

對於**重定向器**模式，作業系統必須配置為透過 Kaspersky Security 10.1 for Windows Server 指定的連接埠傳輸加密流量。

4. 點擊“**確定**”。

工作模式配置即被儲存。

預設安全等級設定

伺服器檔案資源樹狀目錄中所選的節點可套用三個預設安全性設定：“最佳效能”、“建議”和“最高防護”。 這些等級均有各自的安全性設定集（請參閱下表）。

最佳效能

如果除了在伺服器和工作站上使用 Kaspersky Security 10.1 for Windows Server 外，還在網路內採取了其他伺服器安全措施（例如，防火牆和現有安全原則），則建議使用“**最佳效能**”安全等級。

建議

“**建議**”安全等級確保防護與對伺服器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伺服器。預設情況下，將設定“**建議**”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。

表 37. 預設安全等級和相應的安全性設定

選項	安全等級		
	最佳效能	建議	最佳防護
掃描物件	依資料庫中指定的副檔名清單	依格式	所有物件
對受感染物件和其他物件執行的操作	封鎖	封鎖	封鎖
不偵測	否	否	否
執行超過以下時間時停止掃描（秒）	60 秒	60 秒	60 秒
不掃描大於以下大小的物件(MB)	20 MB	20 MB	否

選項	安全等級		
	最佳效能	建議	最佳防護
掃描複合檔案	• 已封裝的物件* * 僅新物件和已修改的物件	• 壓縮檔* • SFX 壓縮檔* • 已封裝的物件* • 內嵌的 OLE 物件* * 僅新物件和已修改的物件	• 壓縮檔* • SFX 壓縮檔* • 已封裝的物件* • 內嵌的 OLE 物件* * 所有物件

配置針對基於 Web 的惡意軟體的防護

以下防護設定也會影響傳入郵件流量。但是，要對受感染的物件和其他偵測到的物件的選定操作只針對郵件附件執行。

► *要設定啟發式分析以偵測透過 Web 流量傳輸的病毒和其他電腦安全威脅：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”部分的“**流量安全**”設定塊中，點擊“**設定**”按鈕。

   將開啟“**流量安全**”視窗。
4. 在“**惡意軟體防護**”標籤上：
   - 選中“**使用啟發式分析**”核取方塊。
   - 設定惡意軟體掃描所需的啟發式分析等級。
   - 從下拉清單中選擇安全等級（請參見第 185 頁上的“預設的安全等級設定”部分）：
     - **建議**
     - **最佳防護**

- **最佳效能**
- **自訂**

5. 在“**敘述**”標籤的下方可以檢視所選安全等級的設定。
6. 開啟“**一般**”標籤，在“**物件防護**”部分中，指定要包含在防護範圍內的物件：
   - **所有物件**

     Kaspersky Security 10.1 for Windows Server 掃描所有物件。
   - **按格式掃描物件**

     Kaspersky Security 10.1 for Windows Server 僅根據檔案格式掃描感染物件。

     Kaspersky Lab 編制了該格式清單。它包含在 Kaspersky Security 10.1 for Windows Server 資料庫中。
   - **按病毒資料庫中指定的副檔名清單掃描物件**

     Kaspersky Security 10.1 for Windows Server 僅根據檔案副檔名掃描感染的物件。

     Kaspersky Lab 編制了該副檔名清單。它包含在 Kaspersky Security 10.1 for Windows Server 資料庫中。
   - **按指定的副檔名清單掃描物件**

     Kaspersky Security 10.1 for Windows Server 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。

     a. 點擊“**修改**”按鈕以編輯副檔名清單。

     b. 在開啟的視窗中，指定副檔名。

     c. 點擊“**新增**”。

     點擊“**按預設**”按鈕用預設的排除副檔名填充清單。
7. 在“**複合物件防護**”部分中，指定要包含在掃描範圍內的複合物件：
   - **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 Security 10.1 for Windows Server 將掃描壓縮檔案。

     如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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。
   - **SFX 壓縮檔案**

     掃描自解壓壓縮檔案。

     如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描 SFX 壓縮檔案。

     如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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。

- **封裝檔案**

  掃描由二進位代碼封包程式（例如 UPX 或 ASPack）封包的可執行檔案。

  如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描由封包程式封包的可執行檔案。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將在掃描期間略過由封包程式封包的可執行檔案。

  預設值取決於所選的安全等級。

- **內嵌的 OLE 物件**

  掃描嵌入到檔案中的物件（如 Microsoft Word 宏或電子郵件附件）。

  如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描嵌入到檔案中的物件。

  如果取消選中該核取方塊，Kaspersky Security 10.1 for Windows Server 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。

8. 在“**操作**”標籤上，選擇要對受感染的物件和其他偵測到的物件執行的操作：

   - **封鎖**

     如果偵測到惡意內容，Kaspersky Security 10.1 for Windows Server 將封鎖載入網頁。將顯示封鎖所請求的網頁的原因，而不顯示網頁。

   - **允許**

     Kaspersky Security 10.1 for Windows Server 不封鎖所請求的網頁，但會記錄有關惡意內容偵測的事件。

9. 在“**效能**”標籤上，配置以下設定：

   - 在“**排除**”部分中，選中或清除“**不偵測**”核取方塊。要設定要排除的物件清單：

     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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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。

a. 點擊“**修改**”按鈕。

b. 在開啟的視窗中，指定物件名稱和遮罩。

c. 點擊“**新增**”。

- 在“**進階設定**”部分中，限制掃描時間間隔和物件大小：
  - **執行超過以下時間時停止掃描（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。

  - **不掃描大於以下大小的物件(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 Security 10.1 for Windows Server 將在病毒掃描期間略過大小超過指定限制值的物件。

    如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 將掃描任意大小的物件。

    對於“**建議**”和“**最佳效能**”安全等級，預設選中該核取方塊。

10. 在“**惡意軟體防護設定**”視窗中點擊“**確定**”。

安全等級配置即被儲存。

配置郵件威脅防護

要使用郵件威脅防護，必須安裝 Kaspersky Security 10.1 Microsoft Outlook 載入項並正確配置受防護伺服器（請參見第 179 頁上的“郵件威脅防護”部分）。

► *要啟用郵件威脅防護：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”部分的“**流量安全**”設定塊中，點擊“**設定**”按鈕。

   將開啟“**流量安全**”視窗。

4. 在“**郵件威脅防護**”標籤上，選中“**啟用郵件威脅防護**”核取方塊。

   如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將對透過 Kaspersky Security 10.1 Microsoft Outlook 載入項傳入的所有郵件執行防毒和釣魚防護掃描。

   如果清除該核取方塊，則不掃描郵件。

   預設將會選定該核取方塊。

5. 點擊“**確定**”。

即儲存變更。

配置 URL 和 Web 處理

► *要根據 KSN 的病毒資料庫和 URL 信譽檢查 Web 資源是否存在網路釣魚威脅並將指定的 Web 位址標識為惡意：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”部分的“**流量安全**”設定塊中，點擊“**設定**”按鈕。

   將開啟“**流量安全**”視窗。

4. 在“**工作模式**”標籤上，選擇並設定工作執行模式（請參見第 181頁上的“選擇工作執行模式”部分）。
5. 在“**URL 和 Web 處理**”標籤上：
   - 清除或選中“**使用惡意 URL 資料庫掃描 Web 連結**”核取方塊。

     如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將對每個 URL 執行簽章分析。

     如果清除該核取方塊，將不使用病毒資料庫掃描 URL。

預設將會選定該核取方塊。

- 清除或選中“**使用釣魚防護資料庫掃描網頁**”核取方塊。

  如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將根據釣魚防護資料庫檢查每個 URL。 釣魚防護掃描基於啟發式分析。

  如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 不偵測網路釣魚攻擊。

  預設將會選定該核取方塊。

  請注意，當配置 URL 的釣魚防護掃描時，釣魚防護會自動套用於電子郵件。

- 清除或選中“**使用信任區域**”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 Security 10.1 for Windows Server 會將受信任處理程式的檔案操作新增到工作設定中設定的掃描排除項目中。

  如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 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式的檔案操作。

  預設將會選定該核取方塊。

- 選中或清除“**使用 KSN 提供防護**”核取方塊。

  該核取方塊可啟用或停用 KSN 服務的使用。

  如果選中該核取方塊，應用程式將使用卡巴斯基安全網路資料確保應用程式更快速地對新威脅做出回應，並降低誤報的可能性。

  如果清除該核取方塊，則工作將不使用 KSN 服務。

  預設將會選定該核取方塊。

  僅當滿足以下所有條件時，URL 的 KSN 信譽才可用：
  a. 在“流量安全”設定中選中“**使用 KSN 提供防護**”核取方塊。
  b. 接受 KSN 聲明。
  c. 選中“**傳送關於請求的 URL 的資料**”（請參見第 165 頁上的“**配置‘KSN 使用’工作**”部分）核取方塊。
  d. “KSN 使用”工作已啟動。

6. 點擊“**確定**”。

URL 和 Web 處理配置即被儲存。

新增基於 URL 的規則

可以新增基於 URL 的規則來拒絕或允許特定 URL。這些規則的優先順序高於任何其他結論的優先順序。

► *要建立新的基於 URL 的規則：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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“**流量安全**”設定塊中，點擊“**規則**”按鈕。

   將開啟“**Web 控制規則**”視窗。
4. 在“**Web 控制**”標籤上，選中“**套用基於 URL 的規則**”核取方塊以套用規則。

   如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將透過套用憑證的自訂拒絕規則來封鎖 HTTPS 憑證。

   如果清除該核取方塊，則不套用規則。

   預設取消選定該核取方塊。

   僅當選中“**掃描 HTTPS 流量**”核取方塊時，該核取方塊才可用。
5. 點擊“**新增**”按鈕以新增新規則。
6. 點擊“**新增**”按鈕的上下文功能表中，選擇“**基於 URL 的規則**”選項。
7. 在開啟的“**基於 URL 的規則**”視窗中：
   a. 輸入規則的名稱。
   b. 選擇規則的**類型**：“**拒絕**”或“**允許**”。
   c. 選中“**套用規則**”核取方塊。
   d. 在下方的欄位中指定 **URL**。
   e. 點擊“**確定**”。
8. 要編輯規則，請在清單中選擇一條規則，然後點擊“**修改**”。
9. 在“**Web 控制規則**”視窗中，點擊“**確定**”。

即套用新規則。

配置 Web 控制

配置規則使用，管理憑證掃描設定和基於類別的 Web 控制。

本章節說明項目

配置憑證掃描

Kaspersky Security 10.1 for Windows Server 允許您掃描和封鎖具有無效和到期憑證的 Web 資源。要設定憑證掃描，必須執行以下步驟：

a. 選擇“**驅動程式攔截器**”或“**重定向器**”模式。
b. 配置“流量安全”工作（請參見第 193 頁上的“選擇和配置工作模式”部分）。
c. 套用 Web 控制規則。
d. 新增並套用憑證規則（請參見第 194 頁上的“新增憑證規則”部分）。

憑證規則只能用於“**驅動程式攔截器**”或“**重定向器**”模式。預設情況下，Kaspersky Security 10.1 for Windows Server 僅建立憑證的拒絕規則。

選擇和配置工作模式

► *要選擇和配置使用憑證的模式：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**即時伺服器防護**”部分的“**流量安全**”設定塊中，點擊“**設定**”按鈕。

   將開啟“**流量安全**”視窗。
4. 在“**一般**”標籤上，從“**工作模式**”下拉清單中選擇支援憑證掃描的模式：
   - **驅動程式攔截器**（請參見第 182 頁上的“**配置驅動程式攔截器模式**”部分）

- **重定向器**（請參見第 184 頁上的“配置重定向器模式”部分）

5. 在“**工作模式設定**”部分中，配置以下設定：
   - **掃描 HTTPS 流量**。

     如果選中該核取方塊，將解壓縮攔截的加密 HTTPS 流量並掃描其中是否存在威脅。

     如果清除該核取方塊，則不解壓縮加密的 HTTPS 流量。

     預設將會選定該核取方塊。

     僅當 HTTPS 連接埠開放時，才能進行掃描。

   - 選擇您要使用的加密協定的版本：
     - **TLS 1.0**
     - **TLS 1.1**
     - **TLS 1.2**

       預設選中“**TLS 1.0**”核取方塊，且無法修改。

6. 點擊“**確定**”。

工作配置即被儲存。

新增憑證規則

憑證規則只能用於“**驅動程式攔截器**”或“**重定向器**”模式。預設情況下，Kaspersky Security 10.1 for Windows Server 僅建立憑證的拒絕規則。

► *要新增或配置憑證規則：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**流量安全**”設定塊中，點擊“**規則**”按鈕。

   將開啟“**Web 控制規則**”視窗。

4. 在“**Web 控制規則**”標籤上，選中“**套用基於憑證的規則**”核取方塊以套用規則。

   如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將透過套用憑證的自訂拒絕規則來封鎖 HTTPS 憑證。

   如果清除該核取方塊，則應用程式將不掃描憑證。

   預設取消選定該核取方塊。

   僅當選中“**掃描 HTTPS 流量**”核取方塊時，該核取方塊才可用。

5. 點擊“**新增**”按鈕以新增新規則。
6. 點擊“**新增**”按鈕的上下文功能表中，選擇“**基於憑證的規則**”選項。
7. 在開啟的“**基於憑證的規則**”視窗中：
   a. 輸入規則的名稱。
   b. 選中“**套用規則**”核取方塊。
   c. 選擇**運算元類型**：**遮罩**或**規則運算式**。
   d. 在“**運算元**”欄位中指定遮罩或運算式。
   e. 點擊“**確定**”。
8. 要編輯規則，請在清單中選擇一條規則，然後點擊“**修改**”。
9. 在“**Web 控制規則**”視窗中，點擊“**確定**”。

即套用新規則。

配置基於類別的 Web 控制

► *要新增或修改基於流量安全類別的規則：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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“**流量安全**”設定塊中，點擊“**規則**”按鈕。

   將開啟“**Web 控制規則**”視窗。

4. 開啟“**分類**”標籤。
5. 選中“**套用網頁流量類別控制規則**”核取方塊。

如果選中該核取方塊，Kaspersky Security 10.1 for Windows Server 將對 Web 資源進行分類別，並封鎖所選類別下的 Web 資源。

如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 不執行分類。

預設取消選定該核取方塊。

類別控制設定變為可用。

6. 選中或清除以下核取方塊：
   - **如果無法分類網頁，則允許存取**。
   - **允許存取可用來破壞伺服器的合法 Web 資源**。
   - **允許存取合法廣告**。
7. 在可用類別清單（請參見第 197 頁上的“類別清單”部分）中：
   - 選中相應的核取方塊可允許類別。

     “**類型**”列變更為“**允許**”。
   - 清除相應的核取方塊可封鎖類別。

     “**類型**”列變更為“**拒絕**”。

   類別清單已預定義，無法修改（您無法新增或移除類別）。
8. 點擊“**確定**”。

規則配置即被儲存。

使用 not-a-virus 遮罩

► *要將 not-a-virus 遮罩用於類別分析：*

1. 在卡巴斯基安全管理中心管理主控台中，開啟設定“KSN 使用”工作（請參見第 165 頁上的“配置‘KSN 使用’工作”部分）。
2. 選中“**傳送關於請求的 URL 的資料**”核取方塊。
3. 啟動“KSN 使用”工作。
4. 在“流量安全”設定視窗（請參見第 180 頁上的“配置‘流量安全’工作”部分）中，選中“**使用 KSN 進行防護**”核取方塊。
5. 在“**Web 控制規則**”視窗中的“**分類**”標籤上，選中“**套用網頁流量類別控制規則**”核取方塊。
6. 在類別清單中，選擇您想要套用 not-a-virus 遮罩的類別。

   所選類別中對應於遮罩的物件不會被“流量安全”工作偵測。

not-a-virus 遮罩的使用在“**信任區域**”設定中配置（請參見第 138 頁上的“套用 not-a-virus 遮罩”部分）。

類別清單

根據標記對 Web 資源進行分析和分類。標記可套用於多個類別（請參見下表）。

表 38. Web 資源類別的標記

標記	敘述	類別清單
18+（成人）	這些類別包括的 Web 資源可能包含成人 (18+) 內容，例如，對暴力、色情或淫穢語言的敘述。	墮胎、成人約會、厭食症、不滿、歧視、性愛、非法藥物、非法軟體、LGBT、性感內衣、非成人約會、裸體主義、政策決定、色情、受全球法律限制、受 RF 法律限制、受俄羅斯聯邦電信資訊和大眾傳媒監管侷限制 (RF)、性教育、性商店、社群網路、自殺、淫穢詞彙、暴力、武器。
孩子	這些類別包括的 Web 資源可能包含孩子內容。例如，教育網站、孩子娛樂網站、關於育兒的論壇和網誌。	為了孩子、受聯邦法律 436 限制 (RF)、學校和大學網頁。
藥物	這些類別包括的 Web 資源可能包含有關麻醉劑和其他合法及非法藥物的資訊。例如，有關分發禁藥或酒精的資訊，或者註冊製藥公司的網站。	墮胎、酒精、厭食症、藥物、健康與美容、非法藥物、藥品、藥房、煙草。
教育	這些類別包括的 Web 資源可能包含教育材料或教學材料。 例如，線上百科全書、知識庫、維基和教育機構的網頁或關於性教育的網頁。	書籍和寫作、教育、為了孩子、資訊技術、線上百科全書、學校和大學網頁、搜尋引擎、性教育。
愛好和娛樂	這些類別包括的 Web 資源可能與娛樂、興趣愛好和休閒活動有關。 例如，各種類型的線上遊戲（包括賭博和社群網路）、關於書籍或打獵的網頁、關於健康與美容的網誌以及新聞源。	成人約會、愛好和娛樂、所有溝通媒介、占星術和奧秘、音訊、視訊和軟體、打賭、網誌、賭場、紙牌遊戲、休閒遊戲、聊天和論壇、電腦遊戲、文化和社會、性愛、時尚、檔案共用、釣魚和打獵、為了孩子、賭博、健康與美容、愛好和娛樂、家庭和家人、幽默、LGBT、性感內衣、彩票、媒體託管和流、藥品、音樂、新聞、非成人約會、裸體主義、線上購物、線上購物（自費）、寵物和動物、色情、餐廳、咖啡館和食物、性商店、社群網路、運動、種子、旅行、電視和廣播、戰爭遊戲。
遊戲	這些類別包括的 Web 資源可能與各種類型的遊戲有關。例如，機會和賭博遊戲、彩票、線上或休閒遊戲，以及關於遊戲的網站和論壇。	休閒遊戲、電腦遊戲、運動、戰爭遊戲。

標記	敘述	類別清單
有害	此類別指包含以下內容的網頁： • “付費玩”的賭博遊戲。 • 賭博集區。 • 涉及購買彩票/號碼的抽獎。	打賭、賭場、紙牌遊戲、電腦遊戲、賭博（延伸）、彩票。
健康與醫療	有關健康生活方式的網頁。可能包括專注於健身、健康飲食以及替代的治療實踐和方法的網站；有關醫療、醫藥、製藥公司以及藥物和補品的網頁。	墮胎、厭食症、藥物（合法和非法）、健康與美容、藥品、藥房、運動。
非法	這些類別可能包括非法的 Web 資源。例如，媒體檔案或安裝套件的非法共用，或者各國法律禁止的網頁。	酒精、音訊、視訊和網站、藥物、檔案共用、非法藥物、非法軟體、彩票、受全球法律限制、受 RF 法律限制、受俄羅斯聯邦電信資訊和大眾傳媒監管侷限制 (RF)、煙草。
IT	一般來說，是指允許使用者（需要或不需要帳戶）將個人訊息傳送給其他使用者的網頁（包括電子郵件服務、社群網路、網誌等）。	匿名代理伺服器、託管和網域服務、非法軟體、資訊技術、搜尋引擎、Web 郵件。
被法律禁止	這些類別包括的 Web 資源可能受聯邦法律管制或與政府或政策有關。	法律和政策、聯邦極端分子名單提及 (RF)、受聯邦法律 436 限制 (RF)、受全球法律限制、受 RF 法律限制、受俄羅斯聯邦電信資訊和大眾傳媒監管侷限制 (RF)。
合法	這些類別可能包括合法的 Web 資源。	酒精、音訊、視訊和網站、藥物、檔案共用、合法廣告、彩票、軍隊、藥房、宗教、性教育、廣告傳單和廣告服務、煙草、戰爭遊戲。
媒體共用	這些類別包括的 Web 資源可能允許檔案共用。 例如，種子、檔案共用網站、音樂和視訊託管、合法和非法內容。	音訊、視訊和軟體、書籍和寫作、檔案共用、為了孩子、Internet 服務、媒體託管和流、音樂、搜尋引擎、種子、電視和廣播。
金錢與支付	這些類別包括的 Web 資源可能與金融和金融交易有關。 例如，銀行官方網站、線上銀行、線上商店和執行轉帳的網頁。	銀行、書籍和寫作、休閒遊戲、電子商務、線上購物（自費）、信用卡支付、支付系統、餐廳、咖啡館和食物、旅行。

標記	敘述	類別清單
線上協作	這些類別包括的 Web 資源可能與線上溝通有關。 例如，專業的網誌和論壇、私人聊天室、社群網路和約會網站。	成人約會、網誌、聊天和論壇、為了孩子、健康與美容、工作搜尋網站、藥品、非成人約會、社群網路、旅行。
精神藥物與藥品	這些類別包括的 Web 資源可能與任何類型的藥品、精神藥物或煙草有關。	藥物（合法和非法）、健康與美容、非法藥物、藥品、藥房、煙草。
性和成人	這些類別包括的 Web 資源可能包含性材料或色情材料。 例如，色情網站、關於性教育的網頁以及關於少數性群體的網站。	成人約會、性愛、LGBT、性感內衣、裸體主義、色情、性教育、性商店。
社會和法律	此類別包括社會和人類別生活的許多方面，包括宗教、宗教組織；政府、政治、法律；家庭和家人；新聞媒體；軍隊和武器。	文化和社會、法律和政治、軍隊、宗教、武器。
購物	這些類別包括的 Web 資源可能與線上購物有關。	書籍和寫作、性感內衣、線上購物、線上購物（自費）、信用卡支付、餐廳、咖啡館和食物、性商店、旅行。
暴力	這些類別包括的 Web 資源可能包含明顯的侵略性表達、殘酷行為敘述、極端主義宣傳或自殺敘述。	不滿、歧視、極端主義和種族主義、釣魚和打獵、仇恨和歧視、聯邦極端分子名單提及 (RF)、軍隊、政策決定 (JP)、受全球法律限制、受 RF 法律限制、受俄羅斯聯邦電信資訊和大眾傳媒監管侷限制 (RF)、自殺、暴力、戰爭遊戲、武器。
Web 服務	這些類別包括的 Web 資源可能提供各種 Web 服務。例如，匿名化、Web 託管或電子郵件服務。	匿名代理伺服器、託管和網域服務、Internet 服務、搜尋引擎、廣告傳單和廣告服務、Web 郵件。

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 Security 10.1 for Windows Server 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伺服器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伺服器上啟動。

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應用於管理群組內的所有伺服器。如果一個管理群組包括各種類型的伺服器，則每個伺服器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伺服器。

建議將政策設定檔應用於為受統一政策控制的單個管理群組內的不同伺服器類型設定應用程式啟動控制規則。這可以最佳化伺服器防護，只要指定的規則只涵蓋對於該伺服器類型典型的那些應用程式啟動。

根據為管理群組的伺服器分配的“*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伺服器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的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. 根據伺服器類型將標籤分配給管理群組內的每個伺服器。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伺服器。在所選電腦的“**內容：<伺服器名稱>**”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伺服器。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。將開啟“**內容：<設定檔名稱>**”視窗。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）。

表 39. 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	**僅統計資訊**。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，您可以為伺服器防護選擇“**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封包分發軟體	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解釋器啟動	未套用。	您可以在沒有可執行的指令時拒絕指令解釋器啟動。
工作啟動	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 Security 10.1 for Windows Server 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 使用指定的規則監控正在執行的任何應用程式。
     - **僅統計資訊**。Kaspersky Security 10.1 for Windows Server 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“**僅統計資訊**”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 Security 10.1 for Windows Server 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開機。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 Security 10.1 for Windows Server 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解釋器啟動**”核取方塊。

  如果選中此核取方塊，Kaspersky Security 10.1 for Windows Server 將拒絕命令列解釋器啟動，即使允許解釋器啟動。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：

  - 允許命令列解釋器啟動。
  - 允許執行的指令。

  如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 可辨識以下命令列解釋器：

  - 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將使用指定的規則（規則設定指定可執行檔案的範圍）允許或封鎖程式可執行檔案的啟動。

  如果清除此核取方塊，則 Kaspersky Security 10.1 for Windows Server 不使用指定的規則控制程式可執行檔案的啟動。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 Security 10.1 for Windows Server 將使用指定的規則（規則設定將可執行檔指定為範圍）允許或封鎖 DLL 模組的下載。

  如果清除此核取方塊，則 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將封鎖在 KSN 中具有不受信任狀態的任何應用程式執行。應用於 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 Security 10.1 for Windows Server 將不考慮 KSN 不信任的程式的聲譽，並將根據適用于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 Security 10.1 for Windows Server 將允許具有 KSN 信任狀態的應用程式的執行。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 Security 10.1 for Windows Server 將不考慮 KSN 信任的程式的聲譽，並將根據適用于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 205 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 125 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 Security 10.1 for Windows Server 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。

配置軟體分發控制

使用軟體分發控制可簡化軟體安裝和更新。如果應用程式由受信任的應用程式或受信任安裝套件啟動，則軟體分發控制允許應用程式自動啟動。在啟動受信任安裝套件後，Kaspersky Security 10.1 for Windows Server 會自動計算每個子檔案的校驗，此後不會將預設拒絕政策套用於此類檔案。Kaspersky Security 10.1 for Windows Server 允許解壓縮受信任安裝套件並允許所有子檔案啟動，除非這些物件被裝置控制工作規則封鎖或者在 KSN 中列為不受信任。

子檔案的編輯或移動可防止檔案啟動。

► *要新增受信任安裝套件，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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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安裝套件中的檔案啟動。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“**自動允許為所列應用程式和資料套件分發軟體**”核取方塊，則此核取方塊不可編輯。

   僅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，還會封鎖安裝套件子檔案啟動。

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 Security 10.1 for Windows Server 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。

應用程式可控制伺服器上從套裝軟體遞送到安裝/更新的軟體分發週期。如果在伺服器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. 要編輯受信任安裝套件的清單，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，然後選擇應用程式啟動檔案或安裝套件。

  “**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. 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。

    當建立的規則必須滿足終極安全等級時，建議使用此選項：SHA256 校驗可以作為唯一檔案 ID 應用。作為 SHA256 校驗和作為規則引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啟動檔案和安裝套件，並同時將它們新增到清單。Kaspersky Security 10.1 for Windows Server 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啟動檔案或安裝套件，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安裝套件的清單。被 Kaspersky Security 10.1 for Windows Server 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，指定包含受信任安裝套件清單的設定檔。

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。將允許執行子檔案。

   為防止子檔案啟動，在受防護伺服器上移除應用程式，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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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，在開啟的上下文功能表中，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：
   - **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 Security 10.1 for Windows Server 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政策立即為公司網路上的所有伺服器和伺服器群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。

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伺服器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，請確保所有受防護伺服器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伺服器控制規則啟動“規則產生器”工作。

- 對於“應用程式啟動控制”工作在“**僅統計資訊**”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 Security 10.1 for Windows Server 不拒絕應用程式啟動，但當“應用程式啟動控制”在“**僅統計資訊**”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伺服器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伺服器和伺服器群組操作方案以及至少一次重新開機。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伺服器（請參見第 200 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。

建議當網路伺服器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“**僅統計資訊**”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伺服器上，以便生成經過更新的規則清單。測試管理群組包含在網路伺服器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伺服器。

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 201 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**”標籤。
3. 在您希望配置政策的上下文功能表中選擇“**內容**”。

   將開啟“**內容：<政策名稱>**”視窗。
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，然後在該按鈕的上下文功能表中選擇“**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“**建立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“**建立規則**”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伺服器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 Security 10.1 for Windows Server 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伺服器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 Security 10.1 for Windows Server 功能元件的設定的過程與在 Kaspersky Security 10.1 主控台中對這些元件的設定進行本機設定相似。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 Security 10.1 for Windows Server 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伺服器指定應用程式啟動的允許規則，請執行以下步驟。*

1. 在所設定伺服器群組的控制台中的“**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。

     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*。
   - 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伺服器群組。

> Kaspersky Security 10.1 for Windows Server 不會建立在排除的伺服器上啟動的應用程式的允許規則。

3. 在所設定伺服器群組的控制台上的“**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，請確保所有受防護伺服器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伺服器控制規則啟動“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**”視窗點擊“**確定**”。
5. 如果您希望將建立的規則應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。

基於每個單獨的伺服器上的工作執行自動建立的允許規則將被應用於所設定政策涵蓋的所有網路伺服器。在這些伺服器上，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“**僅統計資訊**”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伺服器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“**僅統計資訊**”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“**僅統計資訊**”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）。
   - “*僅統計資訊：應用程式啟動被拒絕*”事件的“**警告**”標籤顯示超過“**僅統計資訊**”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“**僅統計資訊**”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，然後在該按鈕的上下文功能表中選擇“**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

您可以透過卡巴斯基安全管理中心為多組伺服器建立統一的伺服器控制清單，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伺服器。

本章節說明項目

關於裝置控制工作

Kaspersky Security 10.1 for Windows Server 控制大容量儲存和 CD/DVD 光碟機的註冊和使用，以防護伺服器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伺服器以複製或儲存檔案的外部裝置。

Kaspersky Security 10.1 for Windows Server 控制以下 USB 外部裝置連線：

- USB 連線的快閃記憶體磁碟機
- CD ROM 磁碟機
- USB 連線的軟碟磁碟機
- USB 連線的 MTP 行動裝置

Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 連線到受防護伺服器的所有連線嘗試，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的使用範圍中。

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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 自動確定。

裝置控制工作可在兩種模式下執行：

- **活動**。Kaspersky Security 10.1 for Windows Server 會將規則應用於控制快閃記憶體磁碟機和其他外部裝置的連線，並根據預設拒絕政策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**模式下執行時您認為不受信任的外部裝置連線到受防護伺服器，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伺服器。否則，不會將“預設拒絕”原則套用於裝置。

- **僅統計資訊**。Kaspersky Security 10.1 for Windows Server 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伺服器上的連接和註冊，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伺服器和伺服器群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伺服器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 Security 10.1 for Windows Server 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啟動控制規則清單。

  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，請確保所有受防護伺服器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伺服器控制規則啟動“規則產生器”工作。

- 對於在“**僅統計資訊**”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 Security 10.1 for Windows Server 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“**僅統計資訊**”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 Security 10.1 for Windows Server 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“**基於連線的裝置產生規則**”）。

  在本方案中，Kaspersky Security 10.1 for Windows Server 僅為目前已連線的裝置建立允許規則。可以選擇要為其生成允許規則的一個或多個裝置。

  Kaspersky Security 10.1 for Windows Server 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 215 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“**基於連線的裝置產生規則**”。產生允許規則時，如果想要僅考慮目前已連線到受防護伺服器上的裝置的有關資料，請使用此方法。

Kaspersky Security 10.1 for Windows Server 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”工作為一組伺服器指定裝置控制規則，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. 在所設定伺服器群組的主控台上的“**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，請確保所有受防護伺服器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伺服器控制規則啟動“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。

基於每個單獨的伺服器上的系統資料自動建立的允許規則將被應用於所設定政策涵蓋的所有網路伺服器。在這些伺服器上，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主控台的電腦。
2. 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。
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上下文功能表中選擇“**內容**”。

5. 將開啟“**內容：<政策名稱>**”視窗。
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，在開啟的上下文功能表中，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**”標籤。
3. 在您希望配置政策的上下文功能表中選擇“**內容**”。
4. 將開啟“**內容：<政策名稱>**”視窗。
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，然後在上下文功能表中，選擇“**基於連線的裝置建立規則**”。

   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伺服器的裝置清單中，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“**僅統計資訊**”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伺服器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“**僅統計資訊**”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“**僅統計資訊**”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）。
   - “*僅統計資訊：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“**僅統計資訊**”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“**僅統計資訊**”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，然後在該按鈕的上下文功能表中選擇“**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和加密勒索軟體防護工作的資訊。

本章內容

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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 圖形介面管理 Windows 防火牆。在防火牆管理工作期間，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 中開啟或關閉。

如果在安裝 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 偵測到 Windows 防火牆設定和防火牆管理工作設定之間存在不匹配，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 Security 10.1 for Windows Server 可以監控：

- Windows 防火牆的執行狀態
- 安裝 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會在 **Windows 防火牆**管理單元中建立 Kaspersky Security 群組規則集。此規則集可統一 Kaspersky Security 10.1 for Windows Server 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 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 Security 10.1 for Windows Server 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 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會刪除該規則。
- 如果從 Windows 防火牆設定中刪除現有規則，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會回溯變更。
- 如果在防火牆管理設定中建立新規則，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會從 Windows 防火牆設定中強制刪除該規則。
- 如果從防火牆管理設定中刪除現有規則，Kaspersky Security 10.1 for Windows Server 會從 Windows 防火牆設定中強制刪除該規則。

Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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、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，會下降受防護伺服器的安全等級。

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：

- 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
- 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 108 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“**埠號**”。
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“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。

手動新增防火牆規則

您只能新增和編輯應用程式和埠的規則。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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**埠號**”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：

   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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“**埠號**”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。

加密勒索軟體防護

本節包含有關“加密勒索軟體防護”工作以及如何設定的資訊。

本章節說明項目

關於“加密勒索軟體防護”工作

“加密勒索軟體防護”工作可從公司網路上的遠端電腦偵測對受防護伺服器的網路檔案資源的惡意加密。

當“加密勒索軟體防護”工作執行時，Kaspersky Security 10.1 for Windows Server 將掃描遠端電腦存取位於受防護伺服器的共用網路資料夾中的檔案的呼叫。如果應用程式認為遠端電腦對網路檔案資源的操作是惡意加密操作，則該電腦將被新增到不信任主機清單，並失去對該共用網路資料夾的存取權限。

如果偵測到的加密活動發生在已排除在加密勒索軟體防護工作範圍之外的資料夾中，則 Kaspersky Security 10.1 for

Windows Server 不會將該活動視為惡意加密。

預設情況下，應用程式封鎖不信任主機對網路檔案資源存取的時間長度為 30 分鐘。

在確定主機活動為惡意活動之前，“加密勒索軟體防護”工作不會封鎖存取網路檔案資源。此過程可能需要花費一些時間，在此期間，加密程式可能會執行惡意活動。

如果“加密勒索軟體防護”工作在“僅統計資訊”模式下執行，Kaspersky Security 10.1 for Windows Server 只在工作記錄中記錄遠端電腦的惡意加密嘗試。

配置“加密勒索軟體防護”工作設定

“加密勒索軟體防護”工作具有以下預設設定：

- **工作模式**。“加密勒索軟體防護”工作可以在“**活動**”或“**僅統計資訊**”模式下啟動。預設設定“**活動**”模式。
- **防護範圍**。Kaspersky Security 10.1 for Windows Server 預設情況下將加密勒索軟體防護工作套用於受防護伺服器的所有共用網路資料夾。您可以透過指定將應用工作的共用資料夾來變更防護範圍。
- **啟發式分析**。Kaspersky Security 10.1 for Windows Server 套用**中度**掃描詳細等級。您可以啟用或停用啟發式分析，並控制掃描詳細等級。
- **排程設定**。預設情況下，不設定工作的初次啟動排程。“加密勒索軟體防護”工作不會在 Kaspersky Security 10.1 for Windows Server 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“加密勒索軟體防護”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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**加密勒索軟體防護**”設定塊中的“**設定**”按鈕。

   將開啟“**加密勒索軟體防護**”視窗。
4. 在開啟的視窗中，設定以下設定：
   - “**一般**”標籤上的工作模式和啟發式分析使用（請參見第 228 頁上的“一般工作設定”部分）。
   - “**防護區域**”標籤上的防護範圍（請參見第 229 頁上的“建立防護範圍”部分）。

- “**排除**”標籤上的排除（請參見第 230 頁上的“新增排除”部分）。
- “**工作管理**”標籤上的排程工作啟動設定（請參見第 125 頁上的“管理工作排程”部分）。

5. 點擊“**確定**”。

Kaspersky Security 10.1 for Windows Server 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。

一般工作設定

► *要配置一般工作設定：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**加密勒索軟體防護**”設定塊中的“**設定**”按鈕。

   將開啟“**加密勒索軟體防護**”視窗。
4. 在“**工作模式**”部分中，選擇以下兩個可用模式之一：
   - **僅統計資訊**。

     如果選擇此模式，所有惡意加密嘗試都會寫入加密勒索軟體防護工作事件記錄，並且不會執行任何操作。預設選擇該方式。
   - **活動**。

     如果選擇此模式，Kaspersky Security 10.1 for Windows Server 在偵測到惡意加密嘗試時將封鎖對遭到入侵的電腦的分享資料夾的存取。
5. 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。
6. 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。

7. 點擊“**確定**”套用新配置。

建立防護範圍

以下類型的防護範圍均適用于“加密勒索軟體防護”工作：

- **預設**。您可以使用預設安裝的防護範圍，將掃描伺服器上的所有共用網路資料夾。選擇“**伺服器上的所有共用網路資料夾**”設定時應用。
- **使用者**。透過選擇要包含在加密防護範圍內的資料夾，可手動設定防護範圍。在選擇了“**僅指定共用資料夾**”設定的情況下應用。

只能使用本機路徑來設定加密勒索軟體防護工作的防護範圍。

► *要設定“加密勒索軟體防護”工作的防護範圍：*

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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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“**加密勒索軟體防護**”設定塊中的“**設定**”按鈕。

   將開啟“**加密勒索軟體防護**”視窗。

4. 在“**防護區域**”標籤上，選擇 Kaspersky Security 10.1 for Windows Server 執行加密勒索軟體防護工作時將掃描的資料夾：
   - **伺服器上的所有共用網路資料夾**。

如果選擇此選項，當執行加密勒索軟體防護工作時，Kaspersky Security 10.1 for Windows Server 將掃描伺服器上的所有共用網路資料夾。

預設選中該選項。

- **僅指定共用資料夾**。

  如果選擇此選項，在執行“加密勒索軟體防護”工作過程中，Kaspersky Security 10.1 for Windows Server 僅掃描伺服器上您手動指定的共用網路資料夾。

5. 要指定您希望包含在加密防護範圍內的伺服器分享資料夾：

   a. 點擊“**新增**”按鈕。

   將開啟“**選擇要新增的資料夾**”視窗。

   b. 點擊“**瀏覽**”按鈕選擇資料夾，或手動輸入目錄。

   c. 點擊“**確定**”。

6. 在“**加密勒索軟體防護**”視窗中點擊“**確定**”。

將儲存指定設定。

新增排除

► *若要新增加密防護範圍的排除項目，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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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“**加密勒索軟體防護**”設定塊中的“**設定**”按鈕。

   將開啟“**加密勒索軟體防護**”視窗。

4. 在“**排除**”標籤上，選中“**套用排除清單**”核取方塊。

   如果選中該核取方塊，當加密勒索軟體防護工作執行後，Kaspersky Security 10.1 for Windows Server 不會偵測在指定區域內出現的惡意加密活動。

   如果清除該核取方塊，Kaspersky Security 10.1 for Windows Server 將偵測所有共用資料夾中的加密活動。

   預設情況下，未選中該核取方塊且排除清單為空。

5. 點擊“**新增**”按鈕。

   將開啟“**選擇要新增的資料夾**”視窗。

6. 輸入資料夾名稱或點擊“**瀏覽**”選擇資料夾。

7. 點擊“**確定**”。

排除區域即新增到清單中。

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伺服器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伺服器上沒有物理顯示受防護的裝置），會出現*監控中斷*。一旦重新連接大容量儲存器，Kaspersky Security 10.1 for Windows Server 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：

- 受防護的伺服器上必須安裝有支援 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 236 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。可以使用規則觸發標準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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將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。

表 40. 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
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字	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）。

表 41. 預設的“檔案完整性監控”工作設定

設定	值	如何設定
監控範圍	未設定	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	未設定	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 Security 10.1 for Windows Server 將略過指定為排除的監控範圍。
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其中一個指定標記進行過特徵化，則 Kaspersky Security 10.1 for Windows Server 會產生一個監控事件。
檢驗碼計算	未套用	可以配置在對檔案做出變更後進行檔案檢驗碼計算。
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 Security 10.1 for Windows Server 會產生一個稽核事件。
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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第** 97 **頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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 236 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 125 頁上的“管理工作排程”部分）。

6. 點擊“**確定**”以儲存更改。

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：

   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**內容：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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 233 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“**根據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 233 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 Security 10.1 for Windows Server 將偵測所有檔案操作標記，已選擇“**基於所有可識別的標記偵測檔案操作**”選項。

10. 如果執行操作後，您想要 Kaspersky Security 10.1 for Windows Server 計算檔案校驗和，請執行以下操作：
    a. 在“**檢驗和計算**”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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 233 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將考慮 Window 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）來識別入侵。

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伺服器上的異常活動，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 Security 10.1 for Windows Server 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字清單。

  如果事件內容包含為該規則指定的事件識別字，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字。

- 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字的記錄。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 Security 10.1 for Windows Server 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/en-us/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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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“**針對記錄審查套用啟發式分析**”核取方塊。

   如果選中此核取方塊，則 Kaspersky Security 10.1 for Windows Server 將套用啟發式分析來偵測受防護伺服器上的異常活動。

   如果清除此核取方塊，則未執行啟發式分析且 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 125 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：
   - 要為一組伺服器配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”（**請參見第 97 頁上的“配置政策”部分**）視窗。
   - 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 108 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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字。

   c. 點擊“**確定**”。

記錄審查規則將被新增到規則清單中。

從命令列使用 Kaspersky Security 10.1 for Windows Server

本節敘述從命令列使用 Kaspersky Security 10.1 for Windows Server。

本章內容

命令列指令

如果您在 Kaspersky Security 10.1 for Windows Server 安裝期間將“命令列實用工具”包含在安裝的功能清單中，則可透過受防護伺服器的命令列執行基本的 Kaspersky Security 10.1 for Windows Server 管理指令。

使用命令列指令，您僅可管理那些可以根據 Kaspersky Security 10.1 for Windows Server 分配給您的權限來存取的功能。

某些 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 所需的所有各項操作中均可使用命令列（請參見下表）。

表 42. Kaspersky Security 10.1 for Windows Server 指令

指令	敘述
KAVSHELL APPCONTROL（請參見第 255 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 252 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 253 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 Security 10.1 for Windows Server 記錄檔案磁碟整理。KAVSHELL VACUUM”部分（位於第 262 頁上））	對 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 指令說明。KAVSHELL HELP”部分（位於第 245 頁上））	顯示 Kaspersky Security 10.1 for Windows Server 指令說明。
KAVSHELL START（請參見第 245 頁上的“啟動和停止 Kaspersky Security Service KAVSHELL START，KAVSHELL STOP”部分）	啟動 Kaspersky Security 10.1 for Windows Server 服務。
KAVSHELL STOP（請參見第 245 頁上的“啟動和停止 Kaspersky Security Service KAVSHELL START，KAVSHELL STOP”部分）	停止 Kaspersky Security 10.1 for Windows Server 服務。
KAVSHELL SCAN（請參見“掃描選定區域。KAVSHELL SCAN”部分（位於第 246 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 250 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 251 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 251 頁上））	開始或停止即時防護工作。
KAVSHELL UPDATE（請參見“啟動 Kaspersky Security 10.1 for Windows Server 資料庫更新工作。KAVSHELL UPDATE”部分（位於第 256 頁上））	啟動 Kaspersky Security 10.1 for Windows Server 資料庫更新工作（其設定使用指令修飾符指定）。
KAVSHELL ROLLBACK（請參見“回溯 Kaspersky Security 10.1 for Windows Server 資料庫更新。KAVSHELL ROLLBACK”部分（位於第 259 頁上））	將資料庫回復至之前版本。

指令	敘述
KAVSHELL LICENSE（請參見第 260 頁上的“啟動應用程式 KAVSHELL LICENSE”部分）	管理金鑰檔案和啟動碼。
KAVSHELL TRACE（請參見“啟用、設定和停用偵錯記錄。KAVSHELL TRACE”部分（位於第 261 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 264 頁上））	在處理程序異常終止時，啟用或停用 Kaspersky Security 10.1 for Windows Server 處理程序傾印檔案。
KAVSHELL IMPORT（請參見“匯入設定。KAVSHELL IMPORT”部分（位於第 265 頁上））	從預先建立的設定檔匯入 Kaspersky Security 10.1 for Windows Server 設定、功能及工作。
KAVSHELL EXPORT（請參見“匯出設定。KAVSHELL EXPORT”部分（位於第 265 頁上））	將所有 Kaspersky Security 10.1 for Windows Server 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 255 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 Security 10.1 for Windows Server 指令說明。KAVSHELL HELP

若要獲得所有 Kaspersky Security 10.1 for Windows Server 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 Service，請執行指令

KAVSHELL START

預設情況下，Kaspersky Security Service 啟動時，“即時檔案防護”和“作業系統啟動時掃描”工作以及其他排程在“**應用程式啟動時**”啟動的工作也會一起啟動。

若要停止 Kaspersky Security Service ，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伺服器特定區域的工作，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 Kaspersky Security 10.1 主控台中（您無法在 Kaspersky Security 10.1 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 Kaspersky Security 10.1 主控台的“**工作記錄**”中。可將卡巴斯基安全管理中心政策套用於使用 SCAN 指令建立並執行的工作。

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 251 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

表 43. KAVSHELL SCAN 指令修飾符

鍵	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 Security 10.1 for Windows Server 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	掃描伺服器上的共用資料夾。
/STARTUP	掃描啟動物件。
/REMDRIVES	掃描卸除式磁碟。
/FIXDRIVES	掃描硬碟。
/MYCOMP	掃描受防護伺服器所有的區域。
/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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 只掃描受感染的物件格式清單中所包含的格式物件。

鍵	敘述
/FE	依據副檔名掃描物件。Kaspersky Security 10.1 for Windows Server 只掃描受感染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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 中保留了 DISINFECT 和 DELETE 設定，以便確保與以前版本的相容性。可以使用這些設定取代按鍵指令 /AI: 和 /AS: 這種情況下，Kaspersky Security 10.1 for Windows Server 不會處理可疑物件。
REPORT	傳送報告（預設）
AUTO	執行建議的操作
/AS: **針對可疑物件執行的操作**/ 如果未指定此指令參數，Kaspersky Security 10.1 for Windows Server 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（僅掃描 SFX 壓縮檔） B – 電子郵件資料庫 M – 一般郵件 S – 壓縮檔和 SFX 壓縮檔 P - 已封裝的物件 O – 內嵌 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。

鍵	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 Security 10.1 for Windows Server 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。 啟發式分析的強度等級如下： 1 – 輕度掃描 2 – 中度掃描 3 - 深度 如果刪除此指令參數，Kaspersky Security 10.1 for Windows Server 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 命令檢視工作統計資料。在 Kaspersky Security 10.1 for Windows Server 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 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 將用該鍵的值定義的名稱儲存工作記錄檔案。 該記錄檔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“事件檢視器”中 Kaspersky Security 10.1 for Windows Server 事件記錄所定義的事件。 您可指定記錄檔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命令將覆寫現有的記錄檔。 執行工作時，可檢視此記錄檔案。 此記錄會出現在 Kaspersky Security 10.1 主控台“工作記錄”節點中。 如果 Kaspersky Security 10.1 for Windows Server 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“掃描關鍵區域”工作 KAVSHELL SCANCRITICAL

使用 KAVSHELL SCANCRITICAL 指令可使用在 Kaspersky Security 10.1 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“掃描關鍵區域”手動掃描工作，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）。

表 44. KAVSHELL SCANCRITICAL 指令的 /W 指令語法

鍵	敘述
/W:<工作記錄檔案的路徑>	如果指定了此指令參數，Kaspersky Security 10.1 for Windows Server 將用該鍵的值定義的名稱儲存工作記錄檔案。 該記錄檔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命令將覆寫現有的記錄檔。 執行工作時，可檢視此記錄檔案。 此記錄會出現在 Kaspersky Security 10.1 主控台“**工作記錄**”節點中。 如果 Kaspersky Security 10.1 for Windows Server 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）。

表 45. KAVSHELL TASK 指令修飾符

鍵	敘述
不搭配指令參數	回傳所有現有 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 指定給工作的簡短工作別名。要檢視 Kaspersky Security 10.1 for Windows Server 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	回傳目前的工作狀態（例如，**正在執行**、**已完成**、**已暫停**、**已停止**、**已失敗**、**正在啟動**、**還原中**）。
/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 268 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，請執行以下命令：

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）。

表 46. KAVSHELL RTP 指令參數

鍵	敘述
/START	啟動所有即時防護工作：“即時檔案防護”、“指令碼監控”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）。

表 47. KAVSHELL APPCONTROL /GENERATE 指令開關

鍵	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 – 僅統計資訊。

鍵	敘述
/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。

產生應用程式啟動控制規則 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）。

表 48. KAVSHELL APPCONTROL /GENERATE 指令鍵

鍵	敘述
允許規則的使用範圍	
<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。

鍵	敘述
/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伺服器上執行的應用程式。
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。
/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題和指紋。如果指定 /rules: <ch|cp> 鍵，則將執行該指令。
/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伺服器的相關資訊，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）。

表 49. KAVSHELL SCAN 指令鍵

鍵	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）。

表 50. KAVSHELL DEVCONTROL 指令鍵

鍵	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。

啟動 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 資料庫更新工作。

使用 KAVSHELL UPDATE 指令執行的 Kaspersky Security 10.1 for Windows Server 資料庫更新工作是臨時工作。它僅在執行時顯示在 Kaspersky Security 10.1 主控台中。同一時間，會產生工作記錄。它會顯示在 Kaspersky Security 10.1 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 Kaspersky Security 10.1 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 Security 10.1 for Windows Server 的資訊，請參見“使用卡巴斯基安全管理中心管理 Kaspersky Security 10.1 for Windows Server”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

► *若要從 Kaspersky Lab 的更新伺服器下載 Kaspersky Security 10.1 for Windows Server 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）存取伺服器，請執行以下指令：*

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

表 51. KAVSHELL UPDATE 指令參數

鍵	敘述
更新來源（強制參數）。指定一或多個來源。Kaspersky Security 10.1 for Windows Server 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。受防護伺服器上的資料夾。
/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。

鍵	敘述
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 位址及埠號。如果未指定此指令參數，Kaspersky Security 10.1 for Windows Server 將自動偵測本端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 Security 10.1 for Windows Server 將與**本機系統（系統）**帳戶下的代理電腦聯絡 **1** - 內建的 Microsoft Windows NTLM 身分驗證；Kaspersky Security 10.1 for Windows Server 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電腦聯絡 **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 Security 10.1 for Windows Server 將使用主動 FTP 電腦模式連線至受防護伺服器。如果未指定指令參數，Kaspersky Security 10.1 for Windows Server 將使用被動 FTP 電腦模式（如果可能的話）。
/TIMEOUT:<秒數>	FTP 或 HTTP 伺服器連線逾時。如果未指定此指令參數，Kaspersky Security 10.1 for Windows Server 將使用預設值為 10 秒。此指令參數值必須為整數。
/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 Security 10.1 for Windows Server 會選擇與其伺服器最近的更新伺服器，以減輕受防護伺服器上的更新負載。 對於此指令參數值，請根據 ISO 3166- 1 標準替受防護的伺服器指定所在國家/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 Security 10.1 for Windows Server 將會基於安裝 Kaspersky Security 10.1 主控台的電腦上的地區設定偵測受防護伺服器的位置。

鍵	敘述
/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 命令檢視工作統計資料。在 Kaspersky Security 10.1 for Windows Server 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 Kaspersky Security 10.1 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 05:41:02。
/W:<工作記錄檔案的路徑>	如果指定了此指令參數，Kaspersky Security 10.1 for Windows Server 將用該鍵的值定義的名稱儲存工作記錄檔案。 該記錄檔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“事件檢視器”中 Kaspersky Security 10.1 for Windows Server 事件記錄所定義的事件。 您可指定記錄檔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命令將覆寫現有的記錄檔。 執行工作時，可檢視此記錄檔案。 此記錄會出現在 Kaspersky Security 10.1 主控台“**工作記錄**”節點中。 如果 Kaspersky Security 10.1 for Windows Server 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 269 頁）。

回溯 Kaspersky Security 10.1 for Windows Server 資料庫更新。KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 指令可用來執行 Kaspersky Security 10.1 for Windows Server 資料庫回溯系統工作（將 Kaspersky Security 10.1 for Windows Server 資料庫回溯至上一個安裝版）。此命令會同步執行：

指令語法：

KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 指令回傳代碼（請參閱第 269 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

表 52. KAVSHELL TASK LOG-INSPECTOR 指令修飾符

鍵	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	回傳目前的工作狀態（例如，**正在執行**、**已完成**、**已暫停**、**已停止**、**已失敗**、**正在啟動**、**還原中**）。
/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 268 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 Security 10.1 for Windows Server 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:<金鑰檔案編號 | 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: <啟動碼或金鑰編號>

► *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）。

表 53. KAVSHELL LICENSE 指令參數

鍵	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： • 金鑰檔案編號。 • 產品授權類型（正式版或試用版）。 • 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:<金鑰檔案編號或啟動碼>	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 270 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 指令可用來啟用或停用 Kaspersky Security 10.1 for Windows Server 所有子系統的即時偵錯記錄。

Kaspersky Security 10.1 for Windows Server 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）。

表 54. KAVSHELL TRACE 指令參數

鍵	敘述
/ON	啟用偵錯記錄。

鍵	敘述
/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，但無法指定受防護伺服器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的大小上限。一旦記錄檔案大小達到上限時，Kaspersky Security 10.1 for Windows Server 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，一個記錄檔的大小上限為 50 MB。
/LVL:debug|info|warning|error|critical	此指令鍵設定記錄的詳細程度，詳細程度最大（**所有偵錯資訊**）會將所有事件記錄到記錄檔中，程度最小（**緊急事件**）則只會記錄嚴重事件。 如果未指定此指令鍵，偵錯記錄中將記錄詳細程度為**所有偵錯資訊**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 270 頁上的“KAVSHELL TRACE 指令的回傳代碼”部分）。

Kaspersky Security 10.1 for Windows Server 記錄檔案磁碟整理。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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 將透過指定的路徑更新受防護伺服器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 Security 10.1 for Windows Server\10.1\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 Security 10.1 for Windows Server 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伺服器控制工作。持續磁碟整理過程會限制對 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會在 %SYSTEMDRIVE%\System Volume Information 目錄建立 fidbox.dat 檔案，該檔案含有已掃描過的乾淨物件資訊。fidbox.dat 檔案會隨著 Kaspersky Security 10.1 for Windows Server 的掃描檔案數目而變大。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 Security 10.1 for Windows Server 將從 fidbox.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 fidbox.dat 檔案的話，Kaspersky Security 10.1 for Windows Server 不會停用防護（與手動刪除 fidbox.dat 的情況不同）。
- 重設 fidbox.dat 中的資料後，可能會增加 Kaspersky Security 10.1 for Windows Server 的伺服器負載。同時，重設 fidbox.dat 後，Anti-Virus 將掃描所有第一次存取的檔案。掃描 Kaspersky Security 10.1 for Windows Server 後，每一個掃描物件的資訊會再次新增到 fidbox.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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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

表 55. KAVSHELL DUMP 指令參數

鍵	敘述
/ON	在不正常終止的情況下，啟用建立處理程序的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，但無法指定受防護伺服器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 Security 10.1 for Windows Server 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 271 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 指令來匯入受防護伺服器上的 Kaspersky Security 10.1 for Windows Server 設定、功能及 Kaspersky Security 10.1 for Windows Server 設定檔及實例等工作。您可使用 KAVSHELL EXPORT 命令建立設定檔。

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

表 56. KAVSHELL IMPORT 指令參數

鍵	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 271 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 Security 10.1 for Windows Server 及其現有工作所有的設定，以便之後將設定匯入其他伺服器所安裝的 Kaspersky Security 10.1 for Windows Server 實例中。

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

表 57. KAVSHELL EXPORT 指令參數

鍵	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 272 頁上的“KAVSHELL EXPORT 指令的回傳代碼”部分）。

與 MS Operation Management Suite 整合。KAVSHELL OMSINFO

使用 KAVSHELL OMSINFO 指令可檢視應用程式的狀態以及反病毒資料庫和 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名>

KAVSHELL OMSINFO 指令範例

KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json

表 58. KAVSHELL OMSINFO 指令參數

鍵	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

表 59. 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	操作無效（例如 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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

表 60. 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	已取消操作
-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	偵測到受感染和其他物件
-81	偵測到可疑感染物件
-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

表 61. 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	操作無效（例如 Kaspersky Security 10.1 for Windows Server 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

表 62. 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
-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

表 63. 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

回傳代碼	敘述
-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

表 64. 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
-99	未知錯誤
-206	指定來源中的更新檔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 Security 10.1 for Windows Server 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

表 65. KAVSHELL ROLLBACK 指令的回傳代碼

回傳代碼	敘述

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

表 66. 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
-301	金鑰無效
-303	授權適用於其他程式

KAVSHELL TRACE 指令的回傳代碼

表 67. 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）

回傳代碼	敘述
-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

表 68. 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

表 69. 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）
-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

表 70. 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

回傳代碼	敘述
-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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 匯出）

KAVSHELL EXPORT 指令的回傳代碼

表 71. 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 Security 10.1 for Windows Server 未匯出某些功能元件的設定

監控效能。Kaspersky Security 10.1 for Windows Server 計數器

本章節包含有關 Kaspersky Security 10.1 for Windows Server 計數器的資訊：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 Security 10.1 for Windows Server 註冊的 Microsoft Windows 系統監視器的效能計數器的資訊。

本章節說明項目

關於 Kaspersky Security 10.1 for Windows Server SNMP 計數器

預設情況下，“**效能計數器**”元件包含在 Kaspersky Security 10.1 for Windows Server 的已安裝元件中。Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 設定時的建議。

拒絕需求總數

表 72. 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程序接受的物件處理請求總數；從 Kaspersky Security 10.1 for Windows Server 上次啟動時開始計數。 程式會略過物件，要求處理 Kaspersky Security 10.1 for Windows Server 程序拒絕的要求。
用途	此計數器可讓您偵測： • 因為 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 處理程序，Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 未在存取物件時對其進行掃描。 重新啟動 Kaspersky Security 10.1 for Windows Server。

略過需求總數

表 73. 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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

表 74. 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 Security 10.1 for Windows Server 的時間算起。 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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

表 75. 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 Security 10.1 for Windows Server 工作程序的負載，以及伺服器上檔案活動的整體程度。

標準值/上限值	該計數器值可能因伺服器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

表 76. 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 會略過物件。 請增加用於完成即時防護工作的 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 設定。

檔案截取調度程式執行緒的最大數

表 77. 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 Security 10.1 for Windows Server 正在運行的程序分配負載時不夠平均。 重新啟動 Kaspersky Security 10.1 for Windows Server。

已感染物件佇列中的元素數

表 78. 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 Security 10.1 for Windows Server 間的處理器時間分配不平均，而造成程序過載。 • 病毒爆發。
標準值/上限值	當 Kaspersky Security 10.1 for Windows Server 正在處理已感染或可疑物件時，此計數器值可能大於零；但當處理完成時會傳回零，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 Security 10.1 for Windows Server 並未處理物件（檔案截取調度程式可能已當機）。 重新啟動 Kaspersky Security 10.1 for Windows Server。 • 處理物件的處理器時間不足。 請確定 Kaspersky Security 10.1 for Windows Server 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可疑物件，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

表 79. 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 Security 10.1 for Windows Server 程序的處理器時間不足，或 Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 設定，以及伺服器上來自其他應用程式的負載而定。 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 Security 10.1 for Windows Server 處理程序處理物件的處理器時間不足。 請確定 Kaspersky Security 10.1 for Windows Server 可取得更多處理時間（例如，降低伺服器上其他應用程式的負載）。 • Kaspersky Security 10.1 for Windows Server 出錯（多個流空閒）。 重新啟動 Kaspersky Security 10.1 for Windows Server。

Kaspersky Security 10.1 for Windows Server SNMP 計數器和陷阱

本節包含有關 Kaspersky Security 10.1 for Windows Server 計數器和 TRAP 的資訊。

本章節說明項目

關於 Kaspersky Security 10.1 for Windows Server SNMP 計數器和 TRAP

如果要安裝一組防毒元件中包括 **SNMP 計數器和 TRAP**，則可以使用簡單網路管理協定（SNMP）檢視 Kaspersky Security 10.1 for Windows Server 計數器和 TRAP。

若要從管理員的工作站檢視 Kaspersky Security 10.1 for Windows Server 計數器與 TRAP，請啟動受防護伺服器上的 SNMP 服務，並啟動管理員工作站上的 SNMP 與 SNMP TRAP 服務。

Kaspersky Security 10.1 for Windows Server SNMP 計數器

本節包含介紹 Kaspersky Security 10.1 for Windows Server SNMP 計數器的設定的表。

本章節說明項目

效能計數器

表 80. 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 275 頁）
currentInfectedQueueLength	已感染物件佇列中的項目數（請參見第 277 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 277 頁）
currentWorkProcessesNumber	Kaspersky Security 10.1 for Windows Server 所使用的工作處理程序的目前數量

隔離計數器

表 81. 隔離計數器

計數器	定義
totalObjects	目前在隔離中的物件數
totalSuspiciousObjects	目前在隔離中的可疑物件數
currentStorageSize	隔離中的資料大小總計(MB)

備份計數器

表 82. 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

表 83. 一般計數器

計數器	定義
lastCriticalAreasScanAge	伺服器關鍵區域自上次完成掃描以來的期限（自從上次完成“*掃描關鍵區域*”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或啟動碼，則將顯示與備用金鑰或啟動碼關聯的產品授權到期日期。
currentApplicationUptime	Kaspersky Security 10.1 for Windows Server 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

表 84. 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

表 85. 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”工作時可疑的物件總數
totalVirusesFound	上次執行“即時檔案防護”工作時偵測到的威脅總數
totalObjectsQuarantined	Kaspersky Security 10.1 for Windows Server 放入隔離的已感染、可疑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 Security 10.1 for Windows Server 嘗試隔離但無法隔離成功的已感染或可疑物件總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsDisinfected	Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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

計數器	定義
totalObjectsDeleted	Kaspersky Security 10.1 for Windows Server 解毒的已感染、可疑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 Security 10.1 for Windows Server 嘗試清除但未成功解毒的已感染、可疑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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 中的 SNMP TRAP 設定。

表 86. Kaspersky Security 10.1 for Windows Server 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 Security 10.1 for Windows Server 繼續備份受感染的物件。	eventDateAndTime eventSeverity eventSource

TRAP	敘述	選項
eventThresholdBackupStorageSizeExceeds	已達備份可用空上限值。“**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 Security 10.1 for Windows Server 繼續備份受感染的物件。	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	已超過隔離大小上限。隔離中的資料大小總計已超過“**最大隔離空間(MB)**”的指定值。Kaspersky Security 10.1 for Windows Server 會繼續隔離可疑物件。	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 Security 10.1 for Windows Server 會繼續隔離可疑物件。	eventDateAndTime eventSeverity eventSource

TRAP	敘述	選項
eventObjectNotQuarantined	隔離發生錯誤。	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	將物件副本儲存於備份儲存空間時發生錯誤。	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
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

TRAP	敘述	選項
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 Security 10.1 for Windows Server 正在執行。	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Security 10.1 for Windows Server 已停止。	eventSeverity eventDateAndTime eventSource
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

TRAP	敘述	選項
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。

表 87. SNMP TRAP：設定值

設定	說明和可用的參數值
eventDateAndTime	事件時間。
eventSeverity	重要等級。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	伺服器名稱（例如，嘗試存取已感染檔案之使用者所用伺服器的名稱）。
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) – 整體而言與操作 Kaspersky Security 10.1 for Windows Server 而非個別元件相關的事件 • 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）。在這種情況中，Kaspersky Security 10.1 for Windows Server 會使用預設的“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）。

設定	說明和可用的參數值
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 Security 10.1 for Windows Server 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 146 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： • 可疑 (suspicious) - Kaspersky Security 10.1 for Windows Server 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。 • 確定 (Sure) - Kaspersky Security 10.1 for Windows Server 在物件的一段程式碼中偵測到完全符合不明威脅程式碼的結果。
days	天數（例如，授權到期日前的天數）。
errorCode	錯誤代碼。
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。

設定	說明和可用的參數值
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 Security 10.1 for Windows Server。 • reasonStorageReadOnly – 資料庫唯讀；請還原 Kaspersky Security 10.1 for Windows Server。 • reasonStorageIOError – 輸入/輸出錯誤：a) Kaspersky Security 10.1 for Windows Server 已毀損，請還原 Kaspersky Security 10.1 for Windows Server；b) Kaspersky Security 10.1 for Windows Server 檔案所在的磁碟已毀損。 • reasonStorageCorrupted – 儲存空間已毀損；請還原 Kaspersky Security 10.1 for Windows Server。 • 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 Security 10.1 for Windows Server。 • reasonStorageOSFeatureError – 某些作業系統功能不符合 Kaspersky Security 10.1 for Windows Server 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。

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 Security 10.1 for Windows Server 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/（用於掃描可疑檔案和網站）
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

註冊商標和服務標誌均為其各自所有者擁有的財產。

AWS（Amazon Web 服務）是 Amazon.com, Inc. 或其附屬公司在美國和其他國家/地區的商標。

Citrix、XenApp 和 XenDesktop 是 Citrix Systems, Inc.和/或其一個或多個子公司的商標，可能在美國專利及商標局以及其他國家/地區註冊。

Dell 和 Dell Compellent 是 Dell, Inc. 的商標。

Celerra、EMC、Isilon、OneFS 和 VNX 是 EMC Corporation 在美國和其他國家/地區註冊的商標。

Hitachi 是 Hitachi, Ltd. 的商標。

IBM 和 System Storage 是 International Business Machines Corporation 在全世界許多行政轄區的註冊商標。

Excel、Hyper-V、JScript、MultiPoint、Microsoft、Outlook、Windows、Windows Server 和 Windows Vista 是 Microsoft Corporation 在美國和其他國家/地區註冊的商標。

NetApp 和 Data ONTAP 是 NetApp, Inc. 在美國和其他國家/地區的商標或註冊商標。

Linux 是 Linus Torvalds 在美國和/或其他國家/地區註冊的商標。

Mozilla 和 Firefox 是 Mozilla Foundation 的商標。

Oracle 是 Oracle 和/或其附屬公司的註冊商標。

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：

- 關鍵事件。
- 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可疑感染。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可疑感染。

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 不推薦存取此類物件。

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。

釣魚

一種 Internet 詐欺，旨在獲取對使用者機密資料的未授權存取。

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，用於定義電腦安全性的等級。

隔離

Kaspersky Lab 應用程式將偵測到的可疑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；包含威脅的物件或可疑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。

可疑物件

包含修改的已知病毒的程式碼或與病毒的程式碼類似，但 Kaspersky Lab 尚不知道的程式碼的物件。使用啟發式分析偵測可疑物件。

工作

Kaspersky Lab 程式執行的功能是以工作形式呈現，如：即時檔案防護、電腦完整掃描和資料庫更新。

工作設定

特定於每個類型工作的程式設定。

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