TREND MICRO

10.0

Worry-Free™ Business Security Standard 和 Advanced Edition

Service Pack 1

管理手冊

Securing Your Journey to the Cloud

趨勢科技股份有限公司保留變更此文件與此處提及之產品的權利，恕不另行通知。安裝及使用產品之前，請先閱讀 Readme 檔、版本資訊和/或適用的最新版文件。您可至趨勢科技網站取得上述資訊：

http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security.aspx

Trend Micro、Trend Micro t-ball 標誌、TrendProtect、TrendSecure、Worry-Free、OfficeScan、ServerProtect、PC-cillin、InterScan 及 ScanMail 是 趨勢科技股份有限公司 的商標或註冊商標。所有其他廠牌與產品名稱則為其個別擁有者的商標或註冊商標。

版權所有 © 2019。趨勢科技股份有限公司。保留所有權利。

文件編號：WFEM108677/190617

發行日期：2019 年 6 月

受美國專利保護，專利編號： 5,951,698 與 7,188,369

本文件介紹了產品的主要功能，並/或提供作業環境的安裝說明。在安裝或使用本產品前，請先閱讀此文件。

如需有關如何使用產品特定功能的詳細資訊，請參閱趨勢科技線上說明中心和/或趨勢科技常見問題集。

趨勢科技十分重視文件品質的提升。如果您對於本文件或其他趨勢科技文件有任何問題、意見或建議，請與我們聯絡，電子郵件信箱為 docs@trendmicro.com。

請至下列網站並給予您對此文件的評估意見：

https://www.trendmicro.com/download/documentation/rating.asp

目錄

序言

序言 xi

Worry-Free Business Security 文件 xii

讀者 xii

文件慣例 xiii

第 1 章：Worry-Free Business Security Standard 及 Advanced 簡介

Trend Micro Worry-Free Business Security 總覽 1-2

本版本中的新功能 1-2

主要功能和優點 1-3

- 趨勢科技主動式雲端截毒技術 1-3
- 檔案信譽評等服務 1-3
- 網頁信譽評等服務 1-4
- 電子郵件信譽評等服務（僅限 Advanced 版） 1-4
- Smart Feedback 1-5
- URL 過濾 1-6

防護優勢 1-6

瞭解安全威脅 1-7

- 病毒和惡意程式 1-7
- 間諜程式和可能的資安威脅程式 1-9
- 垃圾郵件 1-10
- 入侵 1-10
- 惡意行為 1-10
- 偽冒的存取點 1-10
- 網路釣魚事件 1-10
- 大量郵件攻擊 1-11
- 網路安全威脅 1-12

第 2 章：入門

Worry-Free Business Security 網路 2-2

Security Server 2-2
Scan Server 2-2
代理程式 2-3
Web 主控台 2-4
開啟 Web 主控台 2-4
Web 主控台瀏覽 2-8
Web 主控台圖示 2-10

第 3 章：安裝代理程式

Security Agent 安裝 3-2
Security Agent 安裝需求 3-2
Security Agent 安裝考量 3-2
可用的 Security Agent 功能 3-3
Security Agent 安裝和 IPv6 支援 3-4
Security Agent 安裝方法 3-6
從內部網頁安裝 3-7
使用 Login Script Setup 安裝 3-10
以 Client Packager 進行安裝 3-11
以遠端安裝進行安裝 3-14
使用 Vulnerability Scanner 進行安裝 3-17
以電子郵件通知進行安裝 3-27
移轉至 Security Agent 3-28
在 Security Agents 上執行安裝後的工作 3-29
Messaging Security Agent 安裝 3-31
Messaging Security Agent 安裝需求 3-31
安裝 Messaging Security Agent（僅限 Advanced 版） 3-31
移除代理程式 3-33
從 Web 主控台移除代理程式 3-34
從 Web 主控台解除安裝代理程式 3-35
從端點解除安裝 Security Agent 3-36
從 Microsoft Exchange Server 上解除安裝 Messaging Security Agent（僅限 Advanced 版） 3-36

第 4 章：管理裝置

使用裝置樹狀結構 4-2

使用裝置指令 4-4
新增代理程式至群組 4-6
新增群組 4-7
自訂裝置清單欄 4-8
移動代理程式 4-10
在群組之間移動 Security Agent 4-11
使用 Web 主控台在 Security Server 之間移動代理程式 ... 4-11
使用 Client Mover 在 Security Server 之間移動 Security Agent 4-13
複製設定 4-14
複製 Security Agent 群組設定 4-15
複製 Messaging Security Agent 設定（僅限 Advanced 版） 4-15
匯入和匯出 Security Agent 群組的設定 4-16
匯出設定 4-17
匯入設定 4-18

第 5 章：管理 Security Agent 的基本安全設定

Security Agent 的基本安全設定摘要 5-2
掃瞄方法 5-3
設定掃瞄方法 5-4
Security Agent 即時掃瞄 5-6
設定 Security Agent 即時掃瞄 5-6
Machine Learning 5-7
設定 Machine Learning 5-8
行為監控 5-9
設定行為監控 5-10
信任的程式 5-14
設定信任的程式 5-14
隔離目錄 5-15
設定隔離目錄 5-17

網頁信譽評等 5-17
設定 Security Agent 網頁信譽評等 5-19
URL 過濾 5-20
設定 URL 過濾 5-20
核可/封鎖的 URL 5-21
設定核可/封鎖的 URL 5-21
防火牆 5-22
設定防火牆 5-25
使用防火牆例外 5-26
關閉代理程式群組上的防火牆 5-28
關閉所有代理程式上的防火牆 5-29
周邊設備存取控管 5-29
設定周邊設備存取控管 5-29
使用者工具 5-31
設定使用者工具 5-31
代理程式權限 5-32
設定代理程式權限 5-32

第 6 章：管理針對 Messaging Security Agent（僅限 Advanced 版）的基本安全設定

Messaging Security Agent 6-2
Messaging Security Agent 如何掃瞄電子郵件 6-3
預設 Messaging Security Agent 設定 6-4
Messaging Security Agent 的「即時掃瞄」 6-5
設定 Messaging Security Agent 的「即時掃瞄」 6-5
垃圾郵件防護 6-6
電子郵件信譽評等服務 6-7
內容掃瞄 6-8
內容過濾 6-14
管理內容過濾規則 6-14
內容過濾規則的類型 6-18
新增符合所有條件的內容過濾規則 6-19
新增任何符合條件的內容過濾規則 6-21

新增內容過濾監控規則 6-24
建立內容過濾規則例外 6-26
資料遺失防範 6-27
準備工作 6-27
管理「資料遺失防範」規則 6-28
預設「資料遺失防範」規則 6-35
新增「資料遺失防範」規則 6-36
附件封鎖 6-40
設定附件封鎖 6-41
網頁信譽評等 6-43
設定 Messaging Security Agent 的網頁信譽評等 6-44
行動安全防護 6-46
行動安全防護支援 6-47
設定裝置存取控制 6-48
取消暫停的裝置清除 6-49
手動清除裝置 6-50
設定安全策略 6-50
Messaging Security Agent 的隔離功能 6-55
查詢隔離目錄 6-56
檢視查詢結果和採取處理行動 6-57
維護隔離目錄 6-59
設定隔離目錄 6-60
Messaging Security Agent 的通知設定 6-61
設定 Messaging Security Agent 的通知設定 6-62
設定垃圾郵件維護 6-63
管理終端使用者隔離 6-65
趨勢技術支援/偵錯工具 6-66
產生系統偵錯工具報告 6-67
即時監控 6-68
使用「即時監控」 6-68
新增免責聲明至出站的電子郵件 6-69

第 7 章：管理掃瞄

關於掃瞄 7-2

即時掃瞄 7-2
手動掃瞄 7-3
執行手動掃瞄 7-3
預約掃瞄 7-5
設定預約掃瞄 7-6
Security Agent 的掃瞄目標和處理行動 7-8
Messaging Security Agent 的掃瞄目標和處理行動 7-14

第 8 章：管理更新

更新總覽 8-2
可更新的元件 8-3
HotFix、Patch 和 Service Pack 8-8
Security Server 更新 8-9
設定 Security Server 更新來源 8-11
手動更新 Security Server 8-12
為 Security Server 設定預約更新 8-12
還原元件 8-13
Security Agent 和 Messaging Security Agent 更新 8-14
自動更新 8-14
執行手動更新 8-15
代理程式更新提醒和秘訣 8-15
更新代理程式 8-16
設定更新代理程式 8-19

第 9 章：使用即時狀態

即時狀態 9-2
處理行動中心 9-2
歷來的安全威脅偵測 9-7
勒索軟體摘要 9-15
使用授權狀態 9-19
Exchange Server 摘要 9-19
代理程式狀態 9-19

第 10 章：管理通知

使用通知 10-2
設定通知事件 10-4
Token 變數 10-5

第 11 章：管理全域設定

全域設定 11-2
進行 Internet Proxy 伺服器設定 11-2
進行 SMTP 伺服器設定 11-4
進行桌上型電腦/伺服器設定 11-4
進行系統設定 11-8
設定例外清單設定 11-12

第 12 章：使用記錄檔和報告

記錄檔 12-2
使用記錄查詢 12-4
報告 12-5
使用綜合報告 12-5
使用預約報告 12-7
解譯報告 12-9
執行報告和記錄檔維護工作 12-11

第 13 章：執行管理工作

變更 Web 主控台密碼 13-2
使用 Plug-in Manager 13-2
管理產品使用授權 13-2
設定產品更新設定 13-4
設定產品更新通知 13-5
參與 Smart Feedback 系統程式 13-6
變更代理程式的介面語言 13-6

儲存及還原程式設定 13-7
解除安裝 Security Server 13-9

第 14 章：使用管理工具

工具類型 14-2
Trend Micro Remote Manager Agent 14-3
安裝 Trend Micro Remote Manager Agent（Customer Licensing Portal 使用者） 14-4
安裝 Trend Micro Remote Manager Agent（Licensing Management Platform 使用者） 14-6
從受管理伺服器管理代理程式 14-7
備份和還原代理程式設定 14-11
節省磁碟空間 14-13
在 Security Server 上執行 Disk Cleaner 14-13
使用命令列介面在 Security Server 上執行 Disk Cleaner 14-15
節省用戶端上的磁碟空間 14-15
移動 Scan Server 資料庫 14-16
還原加密檔案 14-17
解密及恢復 Security Agent 上的檔案 14-18
解密及恢復 Security Server、自訂隔離目錄或 Messaging Security Agent 上的檔案 14-19
恢復傳輸中立封裝格式的電子郵件 14-20
使用 ReGenID 工具 14-21
管理 SBS 及 EBS 快捷工具列 14-21
手動安裝 SBS 及 EBS 快捷工具列 14-22
使用 SBS 或 EBS 快捷工具列 14-22

附錄 A：Security Agent 圖示

檢查 Security Agent 狀態 A-2
檢視 Windows 工作列上的 Security Agent 圖示 A-4
存取主控台浮動視窗 A-5

附錄 B：Worry-Free Business Security 中的 IPv6 支援

Worry-Free Business Security 和 Security Agent 的 IPv6 支援 B-2
Security Server IPv6 需求 B-2
Messaging Security Agent 需求 B-2
單純 IPv6 伺服器的限制 B-3
純 IPv6 Security Agent 的限制 B-4
設定 IPv6 位址 B-4
顯示 IP 位址的畫面 B-5

附錄 C：技術支援

疑難排解資源 C-2
使用支援入口網站 C-2
安全威脅百科全書 C-2
聯絡趨勢科技 C-3
加速支援要求 C-4
將可疑內容傳送到趨勢科技 C-4
電子郵件信譽評等服務 C-4
檔案信譽評等服務 C-5
網頁信譽評等服務 C-5
其他資源 C-5
下載專區 C-5
文件意見反應 C-6

附錄 D：產品術語詞彙和概念

重要修補程式 D-2
Hot Fix D-2
智慧型掃瞄 D-2
IntelliTrap D-2
入侵偵測系統 D-3
關鍵字 D-4
修補程式 D-8
一般表示式 D-8
掃瞄例外清單 D-16

Service Pack D-22
Trojan Port（特洛伊木馬程式通訊埠） D-22
無法清除病毒的檔案 D-23

索引

索引 IN-1

序言

序言

歡迎使用《Trend Micro™ Worry-Free™ Business Security 管理手冊》。本文件討論使用資訊、代理程式安裝程序及 Security Server 和代理程式管理。

Worry-Free Business Security 文件

Worry-Free Business Security 文件包括下列內容：

表 1. Worry-Free Business Security 文件

文件	說明
安裝和升級手冊	討論安裝 Security Server 以及升級伺服器和代理程式的需求與程序的 PDF 文件
管理手冊	討論使用資訊、用戶端安裝程序及 Security Server 和代理程式管理的 PDF 文件
說明	編譯為 WebHelp 或 CHM 格式的 HTML 檔案，提供「相關指示」、使用建議和特定領域資訊
Readme 檔案	包含已知問題清單和基本安裝步驟。可能也包含「說明」或印刷文件中未提供的最新產品資訊
常見問題集	問題解決方法和疑難排解資訊的線上資料庫。此資料庫提供有關產品已知問題的最新資訊。若要存取常見問題集，請移至下列網站： http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

您可以從下列位置下載最新的 PDF 文件和 Readme 檔：

http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security.aspx

讀者

Worry-Free Business Security 文件適用於下列使用者：

- 安全管理員：負責管理 Worry-Free Business Security，包括 Security Server 和代理程式的安裝與管理。這些使用者必須具備進階網路管理和伺服器管理知識。
- 終端使用者：其電腦上已安裝 Security Agent 的使用者。這些使用者的電腦技術程度從初學者到進階使用者都有。

文件慣例

為協助您輕鬆地尋找和解譯資訊，Worry-Free Business Security 文件會使用下列慣例：

表 2. 文件慣例

慣例	說明
全部大寫	頭字語、縮寫、特定的指令名稱和鍵盤上的按鍵
粗體	功能表和功能表指令、指令按鈕、索引標籤、選項和工作
斜體	參考其他文件或新技術元件
<文字>	表示應該以實際資料取代角括號中的文字。例如，C:\Program Files\<檔案名稱>，可以是 C:\Program Files\sample.jpg。
注意	提供組態設定注意事項或建議
秘訣	提供最佳實作資訊和趨勢科技的建議
警告!	提供可能會對網路上的電腦造成傷害的活動的警告

第 1 章

Worry-Free™ Business Security Standard 及 Advanced 簡介

本章提供 Worry-Free Business Security (Worry-Free Business Security) 的總覽。

Trend Micro Worry-Free Business Security 總覽

Trend Micro Worry-Free Business Security (Worry-Free Business Security) 能夠保護小型企業的使用者與資產不受資料失竊、身分失竊、危險網站與垃圾郵件的威脅（僅限 Advanced 版）。

此文件提供有關 Worry-Free Business Security Standard 和 Advanced 的資訊。只有與 Advanced 版相關的章節會標示為「（僅限 Advanced 版）」。

Worry-Free Business Security 使用趨勢科技主動式雲端截毒技術，具有以下特性：

- 更安全：可以防止病毒、間諜程式、垃圾郵件（僅限 Advanced 版）與網路安全威脅入侵用戶端。URL 過濾功能可以封鎖對危險網站的存取，協助您改善使用者生產力。
- 更具智慧性：快速的掃瞄與持續的更新功能能夠在不影響用戶端效能的前提下阻擋新興安全威脅的入侵。
- 更簡單：Worry-Free Business Security 不僅容易部署、不需要任何管理，還能更有效地偵測安全威脅，讓您專注於業務，完全不用擔心資訊安全。

本版本中的新功能

下表列出這個 Worry-Free Business Security 版本中包含的新功能和增強功能。

功能/增強功能	說明
加強掃瞄	Worry-Free Business Security 現在包括「加強掃瞄」功能，可以更深入掃瞄和清除中毒端點。 如需詳細資訊，請參閱使用裝置樹狀結構 第 4-2 頁和使用裝置指令 第 4-4 頁。

功能/增強功能	說明
增強的無檔案型態惡意程式防護	Worry-Free Business Security 現在使用最新的無檔案型態惡意程式防範技術，保護您的端點抵禦無檔案型態攻擊。
作業系統支援	Worry-Free Business Security 現在支援在下列作業系統上安裝 Security Server 和 Security Agent： • Windows 10 2019 年 5 月更新 • Windows Server 2019

主要功能和優點

Worry-Free Business Security 具備下列功能和優點：

趨勢科技™主動式雲端截毒技術™

趨勢科技™主動式雲端截毒技術™是新一代的雲端用戶端內容安全基礎結構，旨在保護客戶不受安全威脅和網路安全威脅的侵襲。我們提供內部部署及趨勢科技託管兩種解決方案，可以保護使用者在家或隨身使用網路的安全。主動式雲端截毒技術讓輕量型代理程式能使用電子郵件、網頁和檔案信譽評等技術以及安全威脅資料庫的獨特雲端相互關聯性。隨著存取這個網路的產品、服務和使用者越來越多，等於為其使用者建立了一個即時的守望相助系統，因此客戶受到的保護會自動更新和強化。

如需主動式雲端截毒技術的詳細資訊，請造訪：

http://www.trendmicro.com.tw/spn/index.asp

檔案信譽評等服務

檔案信譽評等服務會對照龐大的雲端資料庫檢查每個檔案的信譽。由於惡意程式資訊係存放在雲端裡，因此所有使用者可立即存取。高效能的內容傳送網路與本機快取伺服器可確保在檢查期間將網路延遲影響降到最低。雲端用戶端架

構除了可以大幅減少整體用戶端的容量需求之外，還能夠提供更即時的防護，並消除病毒碼部署的工作負擔。

Security Agent 必須處於雲端截毒掃瞄模式時才能使用檔案信譽評等服務。在本文件中，這些代理程式稱為雲端截毒掃瞄代理程式。未處於雲端截毒掃瞄模式的代理程式不會使用「檔案信譽評等服務」，並且會被稱為標準掃瞄代理程式。Worry-Free Business Security 管理員可將所有或部分代理程式設定為處於雲端截毒掃瞄模式。

網頁信譽評等服務

透過全世界其中一個最大的網域信譽評等資料庫，趨勢科技網頁信譽評等技術會依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析所發現的可疑活動指標等因素來指定信譽評等，以追蹤 Web 網域的可信度。網頁信譽評等會繼續掃瞄網站，並阻擋使用者存取中毒的網站。網頁信譽評等功能有助於確認使用者存取的是安全網頁，且不含任何網路安全威脅，例如惡意程式、間諜程式，以及專門在誘騙使用者提供個人資訊的網路釣魚詐騙手法。為了提高準確度並減少誤判的情形，趨勢科技網頁信譽評等技術會為網站內的特定網頁或連結指定信譽評分，而不是將整個網站進行分類或封鎖，因為通常合法網站只有部分受到駭客入侵，而信譽評等會隨著時間動態變更。

受網頁信譽評等策略約束的代理程式會使用網頁信譽評等服務。Worry-Free Business Security 管理員可以使全部或數個代理程式受網頁信譽評等策略的約束。

電子郵件信譽評等服務（僅限 Advanced 版）

趨勢科技電子郵件信譽評等服務技術會將電子郵件與內含已知垃圾郵件來源的信譽評等服務資料庫進行交叉比對，並透過動態服務即時評估電子郵件寄件者信譽，藉此達到驗證其 IP 位址的目的。信譽評等服務會透過對 IP 位址的「行為」、活動範圍與先前的歷史記錄的持續分析達到更準確的分級目的。根據寄件人 IP 位址，會將惡意電子郵件封鎖於雲端，阻止殭屍程式和 Botnet 等安全威脅侵入網路或使用者的電腦。

「電子郵件信譽評等服務」技術會根據原始郵件傳輸代理程式 (MTA) 的信譽來識別垃圾郵件。這會從 Security Server 卸載工作。藉由啟動「電子郵件信譽評

等服務」，所有的入站 SMTP 流量都會經由 IP 資料庫檢查，以查看原始 IP 位址究竟是沒問題，還是已列入已知垃圾郵件擴散媒介的名單中。

有兩種服務等級可用於「電子郵件信譽評等服務」：

- 標準：「標準」服務會使用資料庫，追蹤大約二十億個 IP 位址的信譽。始終與垃圾郵件遞送有關的 IP 位址，均已新增至資料庫且甚少移除。
- 進階：「進階」服務等級是以查詢 DNS 為基礎且類似「標準」服務的服務。此服務的核心是標準信譽資料庫，以及動態信譽、即時資料庫，封鎖來自已知和可疑垃圾郵件來源的郵件。

發現來自被封鎖的或可疑 IP 位址的電子郵件時，「電子郵件信譽評等服務」(ERS) 會在郵件到達您的通訊基礎架構之前，先加以停止。如果 ERS 封鎖的電子郵件是來自您感覺安全的 IP 位址，則可將該 IP 位址加入「核可的 IP 位址清單」。

Smart Feedback

趨勢科技 Smart Feedback 提供趨勢科技產品之間不間斷的通訊，以及該公司每天 24 小時、一週 7 天的安全威脅研究中心和技術。若是每個單一客戶在執行例行信譽檢查時發現任何新的安全威脅，就會自動更新所有趨勢科技的安全威脅資料庫，以避免任何後續客戶受到該安全威脅的攻擊。

趨勢科技藉由持續處理透過廣大全球客戶和合作夥伴網路收集的安全威脅資訊，提供自動的即時防護以抵禦最新的安全威脅侵襲，同時提供更佳的協同安全防護，就像是自動化的守望相助系統，動員整個社群來保護其中的每個人。因為所收集的安全威脅資訊基於通訊來源的信譽評等而非特定通訊內容，所以客戶個人或商業資訊的隱私一律會受到保護。

舉例來說，會傳送給趨勢科技的資訊包括：

- 檔案總和檢查碼
- 已存取的網站
- 檔案資訊，包括大小與路徑
- 執行檔名稱

您可以隨時從 Web 主控台終止參加此計畫。

如需詳細資訊，請參閱參與 Smart Feedback 系統程式 第 13-6 頁。

秘訣

您即使不參與 Smart Feedback，您的端點也會受到保護。您可以選擇是否參與，而且可以隨時選擇退出。趨勢科技建議您參與 Smart Feedback，以協助為所有的趨勢科技客戶提供更全面的防護。

如需主動雲端截毒技術的詳細資訊，請造訪：

http://www.trendmicro.com.tw/SPN.htm

URL 過濾

URL 過濾可協助您控制網站的存取以減少員工上班打混摸魚的時間、減少 Internet 頻寬用量，同時建立更安全的 Internet 環境。您可以選擇想要的 URL 過濾保護層級，或是自訂要過濾的網站類型。

防護優勢

下表說明 Worry-Free Business Security 的不同元件如何保護您的電腦免於安全威脅入侵。

表 1-1. 防護優勢

安全威脅	防護
病毒/惡意程式。病毒、特洛伊木馬程式、蠕蟲、後門程式和 Rootkit 間諜程式/可能的資安威脅程式。間諜程式、惡意撥號程式、駭客工具、密碼破解應用程式、廣告軟體、惡作劇程式和按鍵記錄程式	檔案型掃瞄（即時掃瞄、手動掃瞄和預約掃瞄）
經由電子郵件傳輸的安全威脅	Security Agent 中的 POP3 郵件掃瞄

安全威脅	防護
網路蠕蟲/病毒和入侵	Security Agent 中的防火牆
可想到的有害網站/網路釣魚網站	Security Agent 中的網頁信譽評等和 URL 過濾
透過 USB 和其他外部裝置散佈的安全威脅	Security Agent 中的周邊設備存取控管
惡意行為	Security Agent 中的行為監控
以端點上執行的文件為目標的勒索軟體程式	Security Agent 中的行為監控和 Machine Learning

瞭解安全威脅

沒有專門的安全防護人員且採用寬鬆的安全策略的組織，即使有基本的安全基礎結構，但仍會遭受越來越多的安全威脅。發現安全威脅之時，安全威脅可能已散佈到許多計算資源，需要耗費大量時間和心力才能完全消除。與安全威脅消除相關的成本可能也是無法預測且非常巨大的。

屬於趨勢科技主動雲端截毒技術一部分的趨勢科技網路安全智慧和雲端伺服器，可辨識並回應新一代安全威脅。

病毒和惡意程式

病毒/惡意程式種類繁多，而且每天都有新的病毒/惡意程式出現。雖然電腦病毒一度在 DOS 或 Windows 中最常見，但是現今卻能利用企業網路、電子郵件系統及網站的弱點造成嚴重損害。

- 惡作劇程式：類似病毒的程式，往往會在電腦螢幕上作怪。
- 可能的病毒/惡意程式：具有某些病毒/惡意程式特徵的可疑檔案。如需詳細資訊，請參閱趨勢科技安全威脅百科全書：

  https://www.trendmicro.com/vinfo/tw/threat-encyclopedia/

- Rootkit:在使用者未同意或未知曉的情況下就在系統上安裝並執行程式碼的程式（或程式集合）。它會在電腦上使用隱形方式持續存在，且偵測不到。Rootkit 不會感染電腦，卻會在無法偵測到的情況下執行惡意程式碼。在惡意程式執行時或僅在瀏覽惡意網站時，Rootkit 就會透過社交工程安裝在系統上。安裝完成後，攻擊者在系統上幾乎可以執行任何功能，包括遠端存取、竊聽，以及隱藏程序、檔案、登錄機碼和通訊通道。
- 特洛伊木馬程式：此類型的威脅經常使用通訊埠來取得電腦或可執行程式的存取權。特洛伊木馬程式不會進行複製，但會常駐在系統上執行惡意動作，例如開放通訊埠讓駭客進入。傳統的防毒解決方案只能偵測並移除病毒，但卻無法偵測或移除特洛伊木馬程式，特別是已經在系統上執行的特洛伊木馬程式。
- 病毒：會進行複製的程式。為了進行複製，病毒必須將自己附加到其他的程式檔，然後在主程式執行時執行，包括
  - ActiveX 惡意程式碼：常駐在執行 ActiveX™ 控制項之網頁中的程式碼。
  - 開機磁區型病毒：感染分割區或磁碟的開機磁區的病毒。
  - COM 和 EXE 檔案感染型病毒：副檔名為 .com 或 .exe 的可執行程式。
  - Java 惡意程式碼：以 Java™ 撰寫或內嵌於其中的非依附作業系統型病毒碼
  - 巨集型病毒：編碼為應用程式巨集的病毒，通常包含在文件中。
  - 封裝程式：經過壓縮和（或）加密的 Windows 或 Linux™ 可執行程式，通常是特洛伊木馬程式。壓縮可執行檔會使防毒產品更難偵測封裝程式。
  - 測試病毒：行為類似真正病毒的內隱檔案，可以由病毒掃瞄軟體偵測出來。使用測試病毒 (例如：EICAR 測試程式檔)，確認您安裝的防毒程式掃瞄正常。
  - VBScript、JavaScript 或 HTML 病毒：常駐在網頁中且透過瀏覽器下載的病毒。

- 電腦蠕蟲：一種自我包裝的程式（或程式集），可以將具有功能性的本體複製檔或其片段散佈到其他電腦系統，途徑往往是透過電子郵件。
- 其他：未分類到其他任何病毒/惡意程式類型下的病毒/惡意程式。

間諜程式和可能的資安威脅程式

除了病毒/惡意程式，端點還會受到潛在安全威脅的侵襲。間諜程式/可能的資安威脅程式是指未歸類為病毒或特洛伊木馬程式的應用程式或檔案，但還是可能對您網路上的用戶端效能有負面的影響，以及對您的組織形成重大的安全、機密和法律風險。間諜程式/可能的資安威脅程式往往會執行各種不受歡迎和具威脅的行動，例如用快顯視窗騷擾使用者，記錄使用者的按鍵動作以及暴露用戶端弱點使其易受攻擊。

如果您發現 Worry-Free Business Security 無法偵測出是否為可能的資安威脅程式的應用程式或檔案，但是您認為它是一種可能的資安威脅程式，請將其傳送到趨勢科技進行分析：

https://success.trendmicro.com/solution/1059565

類型	說明
間諜程式	蒐集資料（如帳號使用者名稱和密碼），並將資料傳輸至第三方。
廣告軟體	顯示廣告並蒐集資料（如使用者的 web 瀏覽偏好），以便透過 Web 瀏覽器讓使用者成為廣告的目標。
惡意撥號程式	變更用戶端的 Internet 設定，而且可能會強制用戶端透過數據機撥出預先設定的電話號碼。而這些號碼通常是付費電話或國際電話號碼，可能會使您公司的電話費暴增。
惡作劇程式	造成用戶端行為異常（例如：闔上和打開 CD-ROM 托盤），以及顯示大量訊息方塊。
駭客工具	幫助駭客進入電腦。
遠端存取工具	幫助駭客從遠端存取和控制電腦。
密碼破解程式	幫助駭客破解帳號使用者名稱和密碼。

類型	說明
其他	其他潛在惡意程式類型。

垃圾郵件

垃圾郵件是由來路不明的電子郵件（垃圾郵件）所組成，這類郵件通常屬於商業性質，會隨機傳送至多個郵件清單、個人或新聞群組。垃圾郵件有兩種類型：來路不明的商業電子郵件 (UCE) 或來路不明的大型電子郵件 (UBE)。

入侵

入侵是指藉由強制或未經授權的方式，進入網路或用戶端。它也表示略過網路或用戶端的安全防護。

惡意行為

惡意行為指的是軟體對作業系統、登錄項目、其他軟體或檔案和資料夾進行未經授權的變更。

偽冒的存取點

「偽冒的存取點」（亦稱為「Evil Twin」）是用於詐欺 Wi-Fi 存取點的術語，其會顯示為在營運場所內所提供的合法存取點，但實際上是由駭客所設定，以便於無線通訊上進行竊聽。

網路釣魚事件

網路釣魚是一種成長快速的詐騙形式，會利用偽造的合法網站設法誘騙網路使用者透露私人資訊。

通常，無戒備心的使用者會收到一個緊急（且看起來可靠）電子郵件，通知其帳號有問題，必須立即修正，以免帳號被停用。這封電子郵件會提供一個看起來就跟真的一樣的網站 URL。只是複製一個合法電子郵件和合法網站，但接著會變更所謂的後端，由此接收所收集的資料。

這封電子郵件會指示使用者登入網站，確認一些帳號資訊。駭客便會收到使用者提供的資料，如登入名稱、密碼、信用卡號碼或身分證號碼。

網路釣魚詐騙速度快、成本低且容易蔓延。對於那些運用這個詐騙手法的犯罪者而言，也可能大大有利可圖。即使是電腦高手也不容易察覺出網路釣魚。執法單位也難以追緝破案。更糟的是，幾乎可能無法起訴。

任何網站只要您懷疑是網路釣魚網站，請向趨勢科技報告。如需詳細資訊，請參閱將可疑內容傳送到趨勢科技 第 C-4 頁。

大量郵件攻擊

透過電子郵件傳播的病毒/惡意程式，可以藉由中毒電腦的電子郵件用戶端自動以電子郵件傳播病毒/惡意程式，或自行傳播病毒/惡意程式。大量郵件行為指的是感染狀況在 Microsoft Exchange 環境中快速傳播的情況。趨勢科技設計的掃瞄引擎可以偵測大量郵件攻擊的行為模式。這些行為都記錄在病毒碼檔案中，透過「趨勢科技主動式更新伺服器」來更新。

您可以啟動 Messaging Security Agent（僅限 Advanced 版）採取特殊動作，在偵測到大量郵件行為時避免受到大量郵件攻擊。對大量郵件行為設定的處理行動會優先於所有其他處理行動。對付大量郵件攻擊的預設處理行動為「刪除整封郵件」。

例如：您可以設定 Messaging Security Agent 在偵測到受電腦蠕蟲或特洛伊木馬程式感染的郵件時，隔離該郵件。您也可以啟動大量郵件行為，並將代理程式設定為刪除所有符合大量郵件行為模式的郵件。代理程式收到包含蠕蟲（例如 MyDoom 的變種）的郵件。這個蠕蟲會利用它自己的 SMTP 引擎把，它自己傳送到它在中毒電腦上收集到的電子郵件信箱。一旦代理程式偵測到 MyDoom 蠕蟲並辨識出它的大量郵件行為，便會刪除所有包含該蠕蟲的電子郵件；而對並未出現大量郵件行為的蠕蟲，則是採取隔離動作。

網路安全威脅

網路安全威脅包含許多種源自 Internet 的安全威脅。網路安全威脅的手法相當精密，會混用各種檔案和技術，而不是單一檔案或伎倆。例如，網路安全威脅製造者會不斷更改所用的版本或變體。由於網路安全威脅是位於固定的網站位置，而不是在中毒用戶端上，因此網路安全威脅製造者會不斷修改其程式碼，以避免被偵測出來。

在最近幾年，我們將駭客、病毒設計者、垃圾郵件寄發者和間諜程式設計者稱為網路罪犯。網路安全威脅可協助這些人達成兩個目標之一。其中一個目標是竊取資訊進行販賣。此舉的影響是會造成機密資訊洩漏（身分遭竊形式）。中毒用戶端可能也會成為網路釣魚攻擊或其他資訊竊取活動的媒介。在各種影響中，此安全威脅可能造成使用者對網路電子商務失去信心，使得 Internet 交易所需的信任蕩然無存。第二個目標是盜用使用者的 CPU 處理能力，作為從事可獲利活動的設備。這些活動包括傳送垃圾郵件、以分散式阻絕服務攻擊從事勒索行為，或執行「依點擊次數付費」活動。

第 2 章

入門

本章討論如何啟動和執行 Worry-Free Business Security。

Worry-Free Business Security 網路

Worry-Free Business Security 包括下列各項：

- Security Server 第 2-2 頁
- 代理程式 第 2-3 頁
- Web 主控台 第 2-4 頁

Security Server

Worry-Free Business Security 的核心是 Security Server。Security Server 會代管 Web 主控台，也就是 Worry-Free Business Security 的集中式 Web 型管理主控台。Security Server 會將代理程式安裝至網路上的用戶端，使用戶端和代理程式形成代理程式和伺服器的關係。Security Server 能夠從一個集中的位置，來檢視安全狀態資訊、檢視代理程式、設定系統安全，以及下載元件。Security Server 也包含資料庫，儲存已偵測到的 Internet 威脅記錄檔，這些偵測結果是由代理程式報告的。

Security Server 可以執行下列重要功能：

- 安裝、監控和管理代理程式。
- 下載代理程式所需的元件。依預設，Security Server 會從趨勢科技主動式更新伺服器下載元件，然後將元件分發到代理程式。

Scan Server

Security Server 包括一項名為 Scan Server 的服務，在 Security Server 安裝期間會自動安裝該服務。因此，不需要單獨安裝該服務。Scan Server 以處理程序名稱 `iCRCService.exe` 進行執行，且在 Microsoft Management Console 中顯示為「趨勢科技雲端截毒掃瞄服務」。

在 Security Agent 使用名為「雲端截毒掃瞄」的掃瞄方法時，Scan Server 可協助這些代理程式更高效地執行掃瞄。雲端截毒掃瞄過程可描述如下：

- Security Agent 會使用本機雲端病毒碼（傳統病毒碼的輕量型版本），掃瞄用戶端中是否有安全威脅。本機雲端病毒碼中包含病毒碼中提供的大多數安全威脅特徵。
- 如果 Security Agent 無法在掃瞄期間判斷檔案的風險，則會傳送掃瞄查詢到 Scan Server 以驗證該風險。Scan Server 使用雲端病毒碼（其中包含本機雲端病毒碼中未提供的安全威脅特徵）來驗證該風險。
- Security Agent 會「快取」由 Scan Server 提供的掃瞄查詢結果，以提升掃瞄效能。

透過包含一些安全威脅定義，Scan Server 可協助減少 Security Agent 在下載元件時所耗用的頻寬。除了下載病毒碼，Security Agent 還會下載明顯較小的本機雲端病毒碼。

當 Security Agent 無法連線至 Scan Server 時，它們便會將掃瞄查詢傳送到趨勢科技主動式雲端截毒技術，它的功能與 Scan Server 相同。

無法與 Security Server 分開單獨解除安裝 Scan Server。如果您不想使用 Scan Server，請執行以下作業：

1. 在 Security Server 電腦上，開啟 Microsoft Management Console 並關閉「趨勢科技雲端截毒掃瞄服務」。
2. 在 Web 主控台上，瀏覽至「管理 > 全域設定 > 桌上型電腦/伺服器」標籤，然後選取「關閉雲端截毒掃瞄服務」選項，以將 Security Agent 切換至標準掃瞄。

代理程式

代理程式保護用戶端不受安全威脅的侵擾。用戶端包括桌上型電腦、伺服器和 Microsoft Exchange Server。Worry-Free Business Security 代理程式分為：

表 2-1. Worry-Free Business Security 代理程式

代理程式	說明
Security Agent	可保護桌上型電腦和伺服器不受安全威脅和入侵的侵擾

代理程式	說明
Messaging Security Agent（僅限 Advanced 版）	保護 Microsoft Exchange Server 不受透過電子郵件傳播的安全威脅的侵擾

代理程式向安裝它的 Security Server 報告。為了向 Security Server 提供最新的用戶端資訊，代理程式會即時傳送事件狀態資訊。代理程式會報告下列事件：安全威脅偵測、開機、關機、掃瞄開始，以及更新完成等。

Web 主控台

Web 主控台是監控整個企業網路中 Security Agent 的核心。Web 主控台附有一組預設的設定和值，您可以根據自己的安全需求和規格設定這些設定和值。Web 主控台使用諸如 Java、CGI、HTML 和 HTTP 等標準 Internet 技術。

可使用 Web 主控台執行以下作業：

- 將代理程式部署到端點。
- 將代理程式組織到邏輯群組中，以便同時進行組態設定及管理。
- 進行產品設定，然後對端點啟動「手動掃瞄」。
- 接收安全威脅相關活動的通知，並檢視其記錄報告。
- 在端點上偵測到安全威脅時，透過電子郵件接收通知並傳送疫情爆發警訊。

開啟 Web 主控台

您可以從網路上的任何端點使用支援的 Web 瀏覽器開啟 Web 主控台。如需有關瀏覽器需求的詳細資訊，請參閱《系統需求》文件。

步驟

1. 選擇下列其中一個選項，開啟 Web 主控台：

   - 在代管 Security Server 的端點上，移至桌面並按一下 Worry-Free Business Security 捷徑。
   - 在代管 Security Server 的端點上，按一下「Windows 開始功能表 > Trend Micro Worry-Free Business Security > Worry-Free Business Security」。
   - 在網路中的任何端點上開啟 Web 瀏覽器，並在網址列輸入下列內容：

     `https://{Security_Server_Name 或 IP 位址}:{通訊埠號碼}/SMB`

     例如：

     `https://my-test-server:4343/SMB`

     `https://192.168.0.10:4343/SMB`

     `http://my-test-server:8059/SMB`

     `http://192.168.0.10:8059/SMB`

     秘訣

     如果您並未使用 SSL，請輸入 `http`，而非 `https`。HTTP 連線的預設通訊埠為 8059，而 HTTPS 連線的預設通訊埠則為 4343。

     如果環境無法依照 DNS 解析伺服器名稱，請使用伺服器名稱來取代 IP 位址。

   瀏覽器會顯示 Worry-Free Business Security 的登入畫面。

2. 輸入密碼，然後按一下「登入」。

   瀏覽器會顯示「即時狀態」畫面。

接下來需執行的動作

如果您無法存取 Web 主控台，請檢查以下項目。

要檢查的項目	詳細資訊
密碼	如果忘記密碼，請使用「主控台密碼重設工具」來重設密碼。此工具位於 Security Server 上 Windows「開始」功能表的「Trend Micro Worry-Free Business Security」資料夾中。
瀏覽器快取記憶體	如果從舊版的 Worry-Free Business Security 升級，Web 瀏覽器和 Proxy 伺服器的快取記憶體檔案可能導致 Web 主控台無法正常載入。清除瀏覽器和任何 Proxy 伺服器（位於趨勢科技 Security Server 與用來存取 Web 主控台的端點之間）上的快取記憶體。
SSL 憑證	驗證您的 Web 伺服器是否運作正常。如果正使用 SSL，請驗證 SSL 憑證仍有效。如需詳細資訊，請參閱 Web 伺服器文件。

要檢查的項目	詳細資訊
虛擬目錄設定	如果您在 IIS 伺服器執行 Web 主控台，虛擬目錄設定可能會有問題，並會出現下列訊息： 無法顯示此頁面 HTTP 錯誤 403.1 - 禁止：拒絕存取。 Internet 資訊服務 (IIS) 此訊息也會在使用下列其中一種位址來存取主控台時出現： http://{伺服器名稱}/SMB/ http://{伺服器名稱}/SMB/default.htm 不過，如果使用下列位址，主控台可能會開啟而不會發生任何問題： http://{伺服器名稱}/SMB/console/html/cgi/cgichkmasterpwd.exe 如果要解決這個問題，請檢查 SMB 虛擬目錄的執行權限。 如果要啟動程序檔： 1. 開啟「Internet 服務管理員」 (IIS)。 2. 在 SMB 虛擬目錄中，選取「內容」。 3. 選取「虛擬目錄」標籤，並且將執行權限變更成程式檔，而非無。另外，也請變更用戶端安裝虛擬目錄的執行權限。

Web 主控台瀏覽

Web 主控台包含下列主要區段：

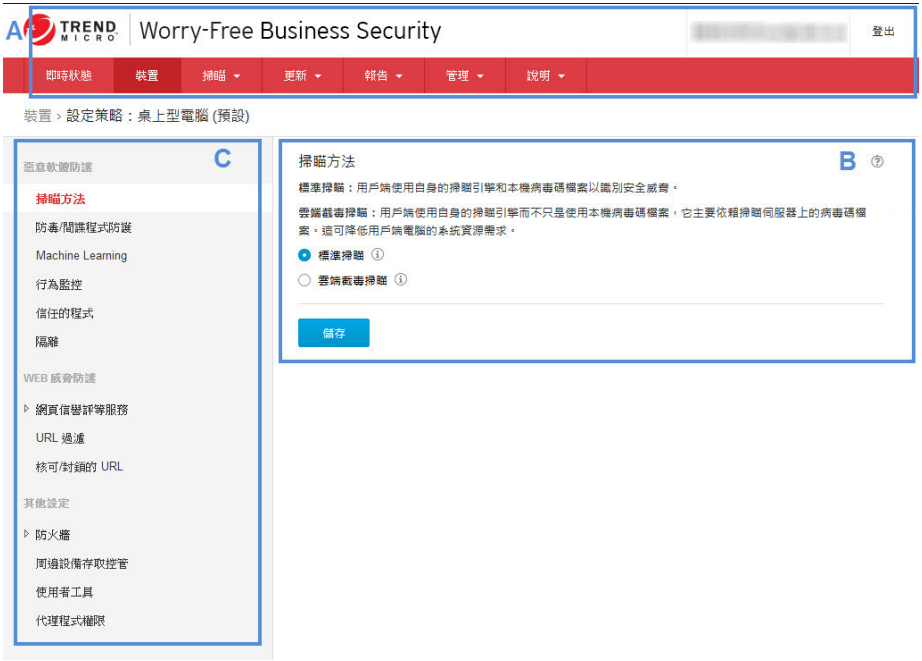


表 2-2. Web 主控台的主要區段

區段	說明
A. 主功能表	Web 主控台的頂端就是主功能表。 還提供「登出」連結，以允許您結束目前的作業階段。
B. 組態設定區域	主功能表項目下方是組態設定區域。使用此區域選取選項，並根據您選取的功能表項目進行設定。

區段	說明
C. 功能表側邊欄（並非所有畫面上均提供）	當您在「裝置」畫面中選擇 Security Agent 群組後，再按一下「設定策略」，即可顯示功能表側邊欄。使用側邊欄可設定安全設定，並掃瞄屬於該群組的桌上型電腦和伺服器。 當您從「裝置」畫面選擇 Messaging Security Agent 時（僅限 Advanced 版），可以使用側邊欄設定安全設定，並掃瞄 Microsoft Exchange Server。

表 2-3. 主功能表區段

功能表項目	說明
即時狀態	監控 Security Agent 的整體安全狀態，以及 Security Server 的運作狀態
裝置	• 自訂代理程式的安全設定 • 在群組之間複製設定
掃瞄	• 掃瞄端點是否有安全威脅 • 排程用戶端的掃瞄作業
更新	• 檢查趨勢科技主動式更新伺服器（或自訂更新來源）是否有最新的更新元件，包括病毒碼檔案、掃瞄引擎、清除元件以及代理程式的更新 • 設定更新來源 • 指定 Security Agent 做為更新代理程式
報告	產生報告以追蹤安全威脅和其他安全相關事件
管理	• 設定異常安全威脅相關事件或系統相關事件的通知 • 設定全域設定以便維護 • 使用管理工具，協助管理網路和用戶端的安全 • 檢視產品使用授權資訊、維護管理員密碼，以及參與 Smart Feedback 計畫，以便在企業環境中進行安全的數位資訊交換 • 自動執行產品更新，並在新更新套件可用時通知使用者

功能表項目	說明
說明	• 搜尋特定內容和主題 • 檢視《管理手冊》 • 存取最新常見問題集 (KB) 資訊 • 檢視安全、銷售、支援和版本資訊

Web 主控台圖示

下表介紹在 Web 主控台中顯示的圖示，並說明它們的用途。

表 2-4. Web 主控台圖示

圖示	說明
	「說明」圖示。開啟線上說明。
	「重新整理」圖示。重新整理目前畫面的檢視。
	展開/收合區段圖示。顯示/隱藏區段。您一次只能展開一個區段。
	「資訊」圖示。顯示特定項目的資訊。
	「自訂通知」圖示。顯示各種通知選項。

第 3 章

安裝代理程式

本章說明安裝 Security Agents and Messaging Security Agents（僅限 Advanced 版）所需的步驟。本章也提供移除這些代理程式的相關資訊。

Security Agent 安裝

在 Windows 用戶端（桌上型電腦和伺服器）上執行 Security Agent 的全新安裝。使用最符合您需求的安裝類型。

安裝 Security Agent 之前，請先關閉用戶端上所有執行中的應用程式。如果安裝時有其他應用程式正在執行，安裝程序可能需要較長的時間來完成。

注意

如需有關升級 Security Agents 至此版本的資訊，請參閱《安裝和升級手冊》。

Security Agent 安裝需求

請造訪下列網站，以取得安裝需求和相容協力廠商產品的完整清單：

http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security.aspx

Security Agent 安裝考量

安裝 Security Agent 之前，請先考量下列事項：

- 代理程式功能：某些 Security Agent 功能在特定 Windows 平台上無法使用。如需詳細資訊，請參閱可用的 Security Agent 功能 第 3-3 頁。
- x64 平台：Security Agent 的簡化版本可在 x64 平台上使用。不過，目前並未提供 IA-64 平台的支援。
- IPv6 支援：Security Agent 可安裝在雙堆疊或純 IPv6 端點上。不過，某些安裝方法可能會有特定需求。

  如需詳細資訊，請參閱 Security Agent 安裝和 IPv6 支援 第 3-4 頁。
- 例外清單：確認已正確設定下列功能的例外清單：

- 行為監控：將重要的用戶端應用程式新增到「核可的程式」清單，以防止 Security Agent 封鎖這些應用程式。如需詳細資訊，請參閱設定行為監控 第 5-10 頁。
- 網頁信譽評等：將您認為安全的網站新增到「核可的 URL 清單」，以防止 Security Agent 封鎖存取這些網站。如需詳細資訊，請參閱設定 Security Agent 網頁信譽評等 第 5-19 頁。

- 代理程式安裝目錄：Security Server 安裝期間，安裝程式會提示您指定代理程式安裝目錄，依預設為 `$ProgramFiles\Trend Micro\Security Agent`。如果您想要將 Security Agent 安裝至其他目錄，請在「管理 > 全域設定 > 系統 > Security Agent 安裝」區段指定新目錄。

可用的 Security Agent 功能

用戶端上可用的 Security Agent 功能取決於用戶端的作業系統。將代理程式安裝至特殊作業系統時，請注意可能不支援某些功能。

表 3-1. Security Agent 功能

功能	Windows 作業系統		
	10	SBS 2011	Server 2012/2012 R2/2016/2019
手動掃瞄（正常和加強）、即時掃瞄和預約掃瞄	是	是	是
防火牆	是	是	是
網頁信譽評等	是	是	是
URL 過濾	是	是	是
行為監控	是	是	是
周邊設備存取控管	是	是	是
損害清除及復原服務	是	是	是

功能	Windows 作業系統		
	10	SBS 2011	Server 2012/2012 R2/2016/2019
郵件掃瞄 (POP3)	是	是	是
手動更新和預約更新	是	是	是
更新代理程式	是	是	是
Agent Plug-in Manager	是	是	是
Smart Feedback	是	是	是
趨勢科技垃圾郵件防護工具列	是 支援的電子郵件用戶端（32 位元和 64 位元）： • Outlook 2010 • Outlook 2013 • Outlook 2016	否	否
HouseCall	是	是	是
案例診斷工具	是	是	是
Wi-Fi 無線警報器	是	否	否

Security Agent 安裝和 IPv6 支援

此主題討論將 Security Agent 安裝到雙堆疊或純 IPv6 用戶端時應考量的事項。

作業系統

Security Agent 只能安裝在支援 IPv6 定址的下列作業系統上：

- Windows SBS 2011

- Windows 10（所有版本）
- Windows Server 2012/2012 R2（所有版本）
- Windows Server 2016（Standard、Datacenter、Essentials）
- Windows Server 2019（Standard、Datacenter、Essentials）

請造訪下列網站，以取得系統需求的完整清單：

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

支援的安裝方法

要將 Security Agent 安裝在純 IPv6 或雙堆疊用戶端時，可以使用所有可用的安裝方法。對於某些安裝方法，需符合特殊需求才能成功地安裝 Security Agent。

表 3-2. 安裝方法和 IPv6 支援

安裝方法	需求/考量
內部網頁和電子郵件通知安裝	如果您要安裝到純 IPv6 用戶端，Security Server 必須是雙堆疊或純 IPv6 用戶端，而且其主機名稱或 IPv6 位址必須是 URL 的一部分。 對於雙堆疊用戶端，安裝狀態畫面中顯示的 IPv6 位址取決於您在「管理 > 全域設定 > 桌上型電腦/伺服器」標籤的「偏好的 IP 位址」區段中選取的選項。
Vulnerability Scanner 和遠端安裝	純 IPv6 Security Server 無法在純 IPv4 用戶端上安裝 Security Agent。同樣地，純 IPv4 Security Server 也無法在純 IPv6 用戶端上安裝代理程式。

Security Agent IP 位址

安裝在支援 IPv6 定址的環境中的 Security Server 可以管理下列 Security Agent：

- 安裝在純 IPv6 用戶端上的 Security Server 可以管理純 IPv6 Security Agent。
- 安裝在雙堆疊用戶端上且已指定 IPv4 和 IPv6 位址的 Security Server，可以管理純 IPv6、雙堆疊和純 IPv4 Security Agent。

安裝或升級 Security Agent 之後，代理程式會使用 IP 位址向 Security Server 註冊。

- 純 IPv6 Security Agent 使用其 IPv6 位址註冊。
- 純 IPv4 Security Agent 使用其 IPv4 位址註冊。
- 雙堆疊 Security Agent 使用其 IPv4 或 IPv6 位址註冊。您可以在「管理 > 全域設定 > 桌上型電腦/伺服器」標籤的「偏好的 IP 位址」區段中，選擇這些代理程式將使用的 IP 位址。

Security Agent 安裝方法

本節提供執行 Security Agent 用戶端的全新安裝時可使用的不同安裝方法的摘要。所有安裝方法都需要目標端點上的本機管理員權限。

如果您要安裝 Security Agent 且要啟動 IPv6 支援，請閱讀 Security Agent 安裝和 IPv6 支援 第 3-4 頁中的指導方針。

表 3-3. 安裝方法

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
內部網頁 支援所有作業系統	是	是	是	否	否	低，如果已預約
電子郵件通知 支援所有作業系統	是	是	是	否	否	高（如果同時啟動多個安裝）
遠端安裝 支援所有作業系統	否	是	否	是	是	低，如果已預約

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
Login Script Setup 支援所有作業系統	否	是	否	是	是	高（如果同時啟動多個安裝）
Client Packager 支援所有作業系統	是	否	是	是	否	低，如果已預約
Trend Micro Vulnerability Scanner (TMVS) 支援 Windows 10 除外的所有作業系統	否	是	否	是	是	低，如果已預約

針對單一地點部署以及嚴格強制執行 IT 策略的組織，IT 系統管理員可以選擇使用遠端安裝或 Login Script Setup 進行部署。

在沒有嚴格強制執行 IT 策略的組織中，趨勢科技建議使用內部網頁安裝 Security Agent。但是若使用這種方法，將要安裝 Security Agent 的終端使用者必須擁有管理員權限。

對於擁有 Active Directory 的網路，遠端安裝是效率較高的方式。如果您的網路並未使用 Active Directory，請使用內部網頁。

從內部網頁安裝

開始之前

若要從內部網頁安裝，需要具備以下項目：

要檢查的項目	需求
Security Server	Security Server 必須安裝在以下系統上： • Windows 7、8.1、10、Server 2008、2008 R2、2012、2012 R2、2016、2019 或 SBS 2008、2011 • 需具有 Internet Information Server (IIS) 7.0、7.5、8.0、8.5、10 或 Apache 2.4
目標端點	• 目標端點必須安裝在 Windows 10、Server 2012、2012 R2、2016、2019 或 SBS 2011 上。 • 目標端點必須具有 Internet Explorer 9.0 或更新版本。 • 使用者必須使用管理員帳號登入端點。 注意 如果目標端點是在桌面作業系統中執行，則請先啟動內建管理員帳號。 如需詳細資訊，請參閱 Microsoft 支援網站 (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account)。
Internet Explorer 安全設定	使用者必須執行下列步驟： 1. 啟動 Internet Explorer 並將 Security Server URL（例如，`https://<Security Server 名稱>:4343/SMB/console/html/client`）新增至信任的網站清單中。存取該清單的方式為：移至「工具 > 網際網路選項 > 安全性」標籤，選取「信任的網站」圖示，然後按一下「網站」。 2. 修改 Internet Explorer 安全性設定，以啟動「自動提示 ActiveX 控制項」。移至「工具 > 網際網路選項 > 安全性」標籤，然後按一下「自訂等級」。
IPv6	如果您擁有的是由純 IPv4、純 IPv6 和雙堆疊端點組成的混合環境，Security Server 必須同時擁有 IPv4 和 IPv6 位址，這樣所有端點才能連線到 Security Server 上的內部網頁。

傳送下列指示給使用者，讓他們從內部網頁安裝 Security Agent。如果要透過電子郵件傳送安裝通知，請參閱以電子郵件通知進行安裝 第 3-27 頁。

步驟

1. 使用管理員帳號登入端點。
2. 開啟 Internet Explorer，然後輸入下列其中一項：
   - Security Server（含 SSL）：

     ```
     https://<Security Server 名稱或 IP 位址>:4343/SMB/
     console/html/client
     ```

   - Security Server（不含 SSL）：

     ```
     http://<Security Server 名稱或 IP 位址>:8059/SMB/console/
     html/client
     ```

3. 按一下「立即安裝」開始安裝 Security Agent。

   安裝便會開始。收到提示時，請允許安裝 ActiveX 控制項。安裝後，Windows 工作列會出現 Security Agent 圖示。

注意

如需 Windows 工作列上顯示的圖示清單，請參閱檢查 Security Agent 狀態 第 A-2 頁。

接下來需執行的動作

如果有使用者反映無法從內部網頁安裝，請嘗試下列方法。

- 使用 Ping 與 Telnet 檢查端點和伺服器之間的通訊是否正常。
- 檢查端點上的 TCP/IP 是否已啟動，以及設定是否正確。
- 如果端點與伺服器之間使用 Proxy 伺服器通訊，請檢查 Proxy 伺服器設定是否正確。
- 在 Web 瀏覽器中，刪除趨勢科技附加元件和瀏覽歷史記錄。

使用 Login Script Setup 安裝

Login Script Setup 可以在未受保護的用戶端登入到網路時，將 Security Agent 自動安裝到該用戶端。Login Script Setup 會將一個名為 AutoPcc.exe 的程式新增至伺服器登入程序檔。

AutoPcc.exe 會將 Security Agent 安裝到未受保護的用戶端，並更新程式檔案和元件。用戶端必須是網域的一部分，才能經由登入程式檔使用 AutoPcc。

如果您已經有現有的登入程式檔，Login Script Setup 會附加執行 AutoPcc.exe 的指令。否則，會建立名稱為 ofcscan.bat 的批次檔案，其中包含執行 AutoPcc.exe 的命令。

Login Script Setup 會在程序檔的檔尾附加下列命令：

```
\\<Server_name>\ofcscan\autopcc
```

說明：

- <Server_name> 是 Security Server 電腦的電腦名稱或 IP 位址。
- 「ofcscan」是 Security Server 上的共享資料夾名稱。
- 「autopcc」是指向安裝 Security Agent 的 autopcc 可執行檔案的連結。

所有 Windows Server 版本上的 Login Script 位置（透過網路登入共享目錄）：

```
\\Windows server\system drive\windir\sysvol\domain\scripts
\ofcscan.bat
```

步驟

1. 在用於執行伺服器安裝的電腦上，開啟 <Security Server 安裝資料夾>\PCCSRV\Admin。
2. 按兩下 SetupUsr.exe。

   接著會載入 Login Script Setup 公用程式。主控台會顯示樹狀結構，顯示網路上的所有網域。

3. 找出要修改其登入程式檔的伺服器，選取該伺服器，然後按一下「選取」。確定伺服器是網域主控站，而且您已具備該伺服器的管理員存取權。

   Login Script Setup 會提示您輸入使用者名稱和密碼。

4. 輸入使用者名稱和密碼。按一下「確定」繼續。

   會出現「使用者選項」畫面。「使用者」清單會顯示登入該伺服器的使用者資料檔。「選定的使用者」清單會顯示要修改其登入程式檔的使用者資料檔。

5. 如果要修改使用者資料檔的登入程式檔，請從「使用者」清單選取使用者資料檔，然後按一下「新增」。

6. 如果要修改所有使用者的登入程式檔，請按一下「全部新增」。

7. 如果要排除之前選取的使用者資料檔，請從「選定的使用者」清單選取名稱，然後按一下「刪除」。

8. 如果要重設選擇，請按一下「全部刪除」。

9. 當所有目標使用者資料檔都位於「選定的使用者」清單中時，請按一下「套用」。

   此時會出現訊息，通知您已成功修改伺服器登入程式檔。

10. 按一下「確定」。

    Login Script Setup 會返回其初始畫面。

11. 如果要關閉 Login Script Setup，請按一下「結束」。

以 Client Packager 進行安裝

Client Packager 可建立安裝套件，而且您可以使用傳統媒體（例如：CD-ROM）將安裝套件傳送給使用者。使用者可以在用戶端上執行該套件，以安裝或升級 Security Agent 和更新元件。

Client Packager 對於以下情況特別有用：

- 部署 Security Agent 或元件到低頻寬遠端辦公室的用戶端時。
- 如果您的環境有連線到 Internet 的限制，處於封閉的 LAN 或缺少 Internet 連線的情況下。

使用 Client Packager 安裝的 Security Agent，會向建立該套件的伺服器回報。

步驟

1. 在 Security Server 電腦上，瀏覽至 `<Server 安裝資料夾>\PCCSRV\Admin\Utility\ClientPackager`。
2. 按兩下 `ClnPack.exe`。

   Client Packager 主控台便會開啟。
3. 選取要針對其建立套件的作業系統。將套件僅部署到執行該類型作業系統的用戶端。如果要部署到另一種類型的作業系統，請建立另一個套件。
4. 為套件選取掃瞄方法。

   如需有關掃瞄方法的詳細資訊，請參閱掃瞄方法 第 5-3 頁。

   套件中包含的元件取決於您選取的掃瞄方法。如果是雲端截毒掃瞄，將會包括所有元件（「病毒碼」除外）。針對標準掃瞄，將包含所有元件（「本機雲端病毒碼」除外）。
5. 選取您要建立的套件類型。

   表 3-4. 用戶端套件類型

套件類型	說明
安裝程式	選取「安裝程式」可以建立符合 Microsoft Installer 套件格式的 MSI 檔案。套件會安裝 Security Agent 程式和 Security Server 上目前可用的元件。 如果目標用戶端已安裝舊版 Security Agent 而您想要升級，請從管理該代理程式的 Security Server 建立 MSI 檔案。否則，代理程式將無法升級。

套件類型	說明
更新	選取「更新」建立包含 Security Server 上目前可用元件的套件。套件將會建立為可執行檔案。如果更新 Security Agent 安裝所在的用戶端上的元件時發生問題，請使用此套件。

6. 按一下「自動安裝」可建立在用戶端背景中安裝的套件，不但用戶端使用者不會察覺，而且也不會顯示安裝狀態視窗。如果您計劃將套件部署到遠端用戶端，請啟動此選項。

7. 安裝 Security Agent 前，如果您不想要掃瞄用戶端是否含有威脅，按一下「關閉安裝前掃瞄（僅適用於初次安裝）」。如果您確定用戶端不含威脅，請執行這項設定。

   如果啟動安裝前掃瞄，安裝程式會掃瞄電腦最容易遭受攻擊的區域中是否有病毒/惡意程式，這些區域如下：

   - 開機區和開機目錄（針對開機型病毒）
   - Windows 資料夾
   - Program files 資料夾

8. 在「來源檔案」旁確認 `ofcscan.ini` 檔案的位置正確。如果要修改路徑，按一下 ...，以瀏覽 `ofcscan.ini` 檔案。依預設，此檔案位於 `<Server 安裝資料夾>\PCCSRV`。

9. 在輸出檔案中，按一下 ... 以指定要建立套件的位置，並輸入套件檔案名稱（例如 `ClientSetup.exe`）。

10. 按一下「建立」。

    Client Packager 建立套件後，會出現「“套件建立成功”」訊息。在您於上一個步驟指定的目錄中尋找套件。

接下來需執行的動作

部署套件至用戶端。

用戶端需求：

- 磁碟空間
  - 標準掃瞄：至少 1.5 GB（建議使用 2 GB）
  - 雲端截毒掃瞄：500 MB

  如果套件掃瞄方法為標準掃瞄，需要 1GB 可用磁碟空間；如果是雲端截毒掃瞄，則需要 500MB。
- Windows Installer 4.5 或更新版本（用以執行 MSI 套件）

套件部署指導方針：

- 將套件傳送給使用者，請他們按兩下檔案（`.msi` 或 `.exe`）執行套件。

  注意

  請將套件僅傳送給其 Security Agent 會向套件建立所在伺服器回報的使用者。

- 指示使用者以滑鼠右鍵按一下套件檔案，然後選取「以管理員身分執行」。
- 如果您使用 Active Directory，可以透過 `.msi` 檔案將 Security Agent 同時自動部署到所有用戶端，而不需要各個使用者分別自行安裝 Security Agent。使用「電腦組態設定」而非「使用者組態設定」，以確保不論登入用戶端的使用者是誰，都能成功安裝 Security Agent。
- 如果新安裝的 Security Agent 無法連線到 Security Server，Security Agent 會繼續使用預設設定。Security Agent 連線至 Security Server 時，會在 Web 主控台取得群組設定。
- 如果您在使用 Client Packager 升級 Security Agent 時碰到任何問題，趨勢科技建議您先解除安裝舊版的代理程式，然後再安裝新版的代理程式。如需解除安裝的指示，請參閱移除代理程式 第 3-33 頁。

以遠端安裝進行安裝

開始之前

從遠端將 Security Agent 安裝到一部或多部連線到網路的端點。

如果要以遠端安裝進行安裝，下列為必要項目：

要檢查的項目	需求
目標端點	• 使用管理員帳號登入每個目標端點。 注意 • 如果目標端點是在桌面作業系統中執行，則請先啟動內建管理員帳號。 如需詳細資訊，請參閱 Microsoft 支援網站 (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account)。 • 在 Windows 10 上執行遠端安裝時，無法使用 Microsoft 帳號登入目標用戶端 • 目標端點不可安裝 Security Server。遠端安裝不會在已執行 Security Server 的端點上安裝 Security Agent。
檔案及印表機共用	在端點上，暫時啟動「檔案及印表機共用」。 注意 如果公司的安全策略是要關閉「Windows 防火牆」，請跳到〈遠端登錄〉一節。 1. 開啟「控制台」中的「Windows 防火牆」。 2. 按一下「允許程式通過 Windows 防火牆」。如果出現提示需要管理員密碼或確認，請輸入密碼或提供確認。會出現「Windows 防火牆設定」視窗。 3. 在「例外」標籤的「程式或通訊埠」清單下，確定已選取「檔案及印表機共用」核取方塊。 4. 按一下「確定」。 5. 在安裝 Security Agent 之後，視需要回復為原始設定。
使用者帳戶控制	關閉「使用者帳戶控制」。

要檢查的項目	需求
	注意 修改下列登錄機碼以關閉「使用者帳戶控制」： `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] “EnableLUA” =dword:00000000.` 在安裝 Security Agent 之後，視需要回復為原始設定。
遠端登錄	暫時啟動「遠端登錄」服務。 1. **注意** 在「執行」視窗中輸入 `services.msc`，以開啟 Microsoft Management Console。 2. 在「遠端登錄」上按一下滑鼠右鍵，然後選取「啟動」。 3. 在安裝 Security Agent 之後，視需要回復為原始設定。
IPv6	雙堆疊 Security Server 可以將 Security Agent 安裝至任何端點。純 IPv6 Security Server 只能將 Security Agent 安裝至純 IPv6 或雙堆疊端點。

步驟

1. 移至「裝置」。
2. 按一下「新增裝置」。
3. 在「電腦類型」區段中，選取「桌上型電腦或伺服器」。
4. 在「方式」區段中，選取「遠端安裝」。
5. 按一下「下一步」。

   隨即顯示新畫面。
6. 在「群組和電腦」方塊中的用戶端清單上，選取用戶端，然後按一下「新增」。會出現提示，要求您輸入用戶端的使用者名稱和密碼。
7. 輸入使用者名稱和密碼，然後按一下「登入」。用戶端便會出現在「選定的電腦」清單方塊中。

8. 重複這些步驟，直到清單顯示「選取的電腦」清單方塊中所有的用戶端為止。
9. 按一下「安裝」。

   會出現確認方塊。
10. 按一下「是」，確認您要將代理程式安裝到用戶端上。

    當程式將 Security Agent 檔案複製到每個用戶端時，會出現進度畫面。

    當 Security Server 完成對用戶端的安裝時，在「選定的電腦」清單方塊的「狀態」欄位，會出現安裝的狀態，而且會出現帶著綠色核取標記的用戶端名稱。

接下來需執行的動作

如果以遠端安裝進行安裝不成功，請執行以下工作：

- 使用 Ping 與 Telnet 檢查用戶端和伺服器之間的通訊是否正常。
- 檢查用戶端上的 TCP/IP 是否已啟動，以及設定是否正確。
- 如果用戶端與伺服器之間使用 Proxy 伺服器通訊，請檢查 Proxy
- 在 Web 瀏覽器中，刪除趨勢科技附加元件和瀏覽歷史記錄。

使用 Vulnerability Scanner 進行安裝

開始之前

執行弱點掃瞄，偵測已安裝的防毒解決方案、搜尋網路上未受保護的用戶端，並在用戶端上安裝 Security Agent。

如果要使用 Vulnerability Scanner 進行安裝，下列為必要項目：

要檢查的項目	需求
要啟動 Vulnerability Scanner 的位置	您可以在 Security Server 或網路中的任何用戶端上啟動 Vulnerability Scanner。用戶端不應執行「終端機伺服器」。
目標用戶端	• 目標用戶端不可安裝 Security Server。Vulnerability Scanner 不會在已經執行 Security Server 的用戶端上安裝 Security Agent。 • 使用者必須擁有管理員權限的帳號以登入用戶端。 注意 如果目標用戶端是在桌面作業系統中執行，則請先啟動內建管理員帳號。如需詳細資訊，請參閱 Microsoft 支援網站 (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account)。

有許多方法可以執行弱點掃瞄。

- 執行手動弱點掃瞄 第 3-18 頁
- 執行 DHCP 掃瞄 第 3-20 頁
- 設定預約弱點掃瞄 第 3-22 頁

執行手動弱點掃瞄

視需要執行弱點掃瞄。

步驟

1. 啟動 Vulnerability Scanner。

若要在以下位置啟動 VULNERABILITY SCANNER：	步驟
Security Server	a. 瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS。 b. 按兩下 TMVS.exe。
網路上的用戶端	a. 在 Security Server 上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。 b. 將 TMVS 資料夾複製到另一個用戶端。 c. 在該用戶端上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

2. 移至「手動掃瞄」區段。
3. 輸入您要檢查的用戶端 IP 位址範圍。
   a. 輸入 IPv4 位址範圍。

      注意
      如果在純 IPv4 或雙堆疊用戶端上執行 Vulnerability Scanner，只能查詢 IPv4 位址範圍。Vulnerability Scanner 只支援類別 B 的 IP 位址範圍，例如 168.212.1.1 到 168.212.254.254。

   b. 對於 IPv6 位址範圍，請輸入 IPv6 字首和長度。

      注意
      如果在純 IPv6 或雙堆疊用戶端上執行 Vulnerability Scanner，只能查詢 IPv6 位址範圍。
4. 按一下「設定」。

   會出現「設定」畫面。
5. 進行弱點掃瞄設定。如需詳細資訊，請參閱弱點掃瞄設定 第 3-24 頁。
6. 按一下「確定」。

   會關閉「設定」畫面。

7. 按一下「開始」。

   弱點掃瞄結果會在「手動掃瞄」標籤下的「結果」表格中顯示。

   注意

   如果電腦執行的是 Windows Server 2008，「結果」表格將不會顯示 MAC 位址資訊。

8. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請按一下「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再按一下「儲存」。

執行 DHCP 掃瞄

在從 DHCP 伺服器要求 IP 位址的用戶端上，執行弱點掃瞄。

Vulnerability Scanner 會監聽第 67 號通訊埠（DHCP 要求的 DHCP 伺服器監聽通訊埠）。如果它偵測到來自用戶端的 DHCP 要求，則會在該用戶端上執行弱點掃瞄。

注意

如果您在 Windows Server 2008 或 Windows 7 上啟動 Vulnerability Scanner，則它將無法偵測 DHCP 要求。

步驟

1. 在位於下列資料夾的 `TMVS.ini` 檔案設定 DHCP 設定：`<Server 安裝資料夾>\PCCSRV\Admin\Utility\TMVS`。

   表 3-5. `TMVS.ini` 檔案中的 DHCP 設定

設定	說明
DhcpThreadNum=x	指定 DHCP 模式的執行緒數量。最小是 3，最大是 100。預設值是 3。

設定	說明
DhcpDelayScan=x	這是在檢查發出要求的電腦是否已安裝防毒軟體之前，以秒為單位的延遲時間。 最小值是 0（不等待），而最大值是 600。預設值是 60。
LogReport=x	0 表示關閉記錄功能，1 表示啟動記錄功能。 Vulnerability Scanner 會將掃瞄結果傳送到 Worry-Free Business Security 伺服器。記錄檔會顯示在 Web 主控台的「系統事件記錄檔」畫面中。
OsceServer=x	這是 Worry-Free Business Security 伺服器的 IP 位址或 DNS 名稱。
OsceServerPort=x	這是 Worry-Free Business Security 伺服器上的 Web 伺服器通訊埠。

2. 啟動 Vulnerability Scanner。

若要在以下位置啟動 VULNERABILITY SCANNER：	步驟
Security Server	a. 瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS。 b. 按兩下 TMVS.exe。
網路上的用戶端	a. 在 Security Server 上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。 b. 將 TMVS 資料夾複製到另一個用戶端。 c. 在該用戶端上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

3. 在「手動掃瞄」區段旁，按一下「設定」。

   會出現「設定」畫面。

4. 進行弱點掃瞄設定。如需詳細資訊，請參閱弱點掃瞄設定 第 3-24 頁。

5. 按一下「確定」。

   會關閉「設定」畫面。

6. 在「結果」表格中，按一下「DHCP 掃瞄」標籤。

   注意

   執行 Windows Server 2008 和 Windows 7 的電腦上不會顯示「DHCP 掃瞄」標籤。

7. 按一下「DHCP 啟動」。

   Vulnerability Scanner 開始監聽 DHCP 要求，並且在用戶端登入網路時對用戶端執行系統弱點預警偵測。

8. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請按一下「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再按一下「儲存」。

設定預約弱點掃瞄

弱點掃瞄會根據預約自動執行。

步驟

1. 啟動 Vulnerability Scanner。

若要在以下位置啟動 VULNERABILITY SCANNER：	步驟
Security Server	a. 瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS。 b. 按兩下 TMVS.exe。
網路上的用戶端	a. 在 Security Server 上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。 b. 將 TMVS 資料夾複製到另一個用戶端。 c. 在該用戶端上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

2. 移至「預約掃瞄」區段。
3. 按一下「新增/編輯」。

   隨即出現「預約掃瞄」畫面。
4. 輸入預約弱點掃瞄的名稱。
5. 輸入您要檢查的電腦 IP 位址範圍。

   a. 輸入 IPv4 位址範圍。

   注意

   如果在純 IPv4 或具有可用 IPv4 位址的雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv4 位址範圍。Vulnerability Scanner 只支援類別 B 的 IP 位址範圍，例如 168.212.1.1 到 168.212.254.254。

   b. 對於 IPv6 位址範圍，請輸入 IPv6 字首和長度。

   注意

   如果在純 IPv6 或具有可用 IPv6 位址的雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv6 位址範圍。
6. 使用 24 小時制時間格式指定開始時間，然後選取預約掃瞄的執行頻率。選擇「每日一次」、「每週一次」或「每月一次」。
7. 如果已設定手動弱點掃瞄設定，且想要使用該設定，請選取「使用目前設定」。如需有關手動弱點掃瞄設定的詳細資訊，請參閱執行手動弱點掃瞄 第 3-18 頁。

   如果未指定手動弱點掃瞄設定，或想要使用另一組設定，請選取「修改設定」，然後按一下「設定」。會出現「設定」畫面。進行掃瞄設定，然後按一下「確定」。如需詳細資訊，請參閱弱點掃瞄設定 第 3-24 頁。
8. 按一下「確定」。

   隨即關閉「預約掃瞄」畫面。您建立的預約弱點掃瞄會顯示在「預約掃瞄」區段下。如果已啟動通知，Vulnerability Scanner 會將預約弱點掃瞄結果傳送給您。

9. 如果要立即執行預約弱點掃瞄，請按一下「立即執行」。

   弱點掃瞄結果會顯示在「預約掃瞄」標籤下的「結果」表格中。

   注意

   如果電腦執行的是 Windows Server 2008，「結果」表格將不會顯示 MAC 位址資訊。

10. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請按一下「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再按一下「儲存」。

11. 若要停止執行預約的弱點掃瞄，移至「預約掃瞄」區段，選取預約的掃瞄，然後按一下「刪除」。

弱點掃瞄設定

執行弱點掃瞄時，進行以下設定。如需有關弱點掃瞄不同類型的詳細資訊，請參閱使用 Vulnerability Scanner 進行安裝 第 3-17 頁。

設定	說明和指示
產品查詢	Vulnerability Scanner 可以檢查目標用戶端上是否有安全防護軟體。 1. 選取要檢查的安全防護軟體。 2. Vulnerability Scanner 使用畫面上顯示的預設通訊埠來檢查軟體。如果軟體管理員變更了預設通訊埠，請進行必要變更，否則 Vulnerability Scanner 將偵測不到軟體。 3. 針對 Norton Antivirus Corporate Edition，您可以按一下「設定」變更逾時設定。
	其他產品查詢設定 如果要設定 Vulnerability Scanner 同時檢查有無安全防護軟體的用戶端數量： 1. 瀏覽至 `<Server 安裝資料夾>\PCCSRV\Admin\Utility\TMVS`，然後使用文字編輯器（例如：記事本）開啟 `TMVS.ini`。 2. 若要設定要檢查的用戶端數量： • 針對手動弱點掃瞄，請變更 `ThreadNumManual` 的值。請指定介於 8 和 64 之間的值。 例如，如果要讓 Vulnerability Scanner 在同一時間檢查 60 部用戶端，請輸入 `ThreadNumManual=60`。 • 針對預約弱點掃瞄，請變更 `ThreadNumSchedule` 的值。請指定介於 8 和 64 之間的值。 例如，如果要讓 Vulnerability Scanner 在同一時間檢查 50 部用戶端，請輸入 `ThreadNumSchedule=50`。 3. 儲存 `TMVS.ini`。
說明擷取設定	當 Vulnerability Scanner 可以「ping」用戶端時，可以擷取用戶端的其他相關資訊。擷取資訊的方法有兩種： • 一般擷取：擷取網域和電腦資訊 • 快速擷取：只擷取電腦名稱

設定	說明和指示
警訊設定	如果要自動將「弱點掃瞄」結果傳送給您自己或您組織中的其他管理員： 1. 選取「將結果以電子郵件寄給系統管理員」。 2. 按一下「設定」，指定電子郵件設定。 3. 在「收件人」中，輸入收件者的電子郵件信箱。 4. 在「寄件人」中，輸入寄件者的電子郵件信箱。 5. 在「SMTP 伺服器」中，輸入 SMTP 伺服器位址。 例如，輸入 `smtp.company.com`。SMTP 伺服器是必要資訊。 6. 在「主旨」中，輸入郵件的新主旨或使用預設的主旨。 7. 按一下「確定」。 如果要通知使用者其電腦未安裝安全防護軟體： 1. 選取「在未受保護的電腦上顯示通知」。 2. 按一下「自訂」設定通知訊息。 3. 在「通知訊息」畫面中輸入新訊息或接受預設訊息。 4. 按一下「確定」。
儲存為 CSV 檔案	將弱點掃瞄結果儲存為逗號分隔值 (CSV) 檔案。 檔案將儲存在啟動 Vulnerability Scanner 的用戶端上。接受預設檔案路徑，或依您的喜好進行變更。

設定	說明和指示
Ping 設定	使用「ping」設定來驗證用戶端是否存在並判斷其作業系統。如果這些設定已關閉，Vulnerability Scanner 會掃瞄所指定 IP 位址範圍中的所有 IP 位址（包含用戶端未使用的位址），因此掃瞄時間會比預期久。 1. 在「封包大小」和「逾時」欄位中，接受或修改預設值。 2. 選取「使用 ICMP OS 特徵鑑別偵測作業系統類型」。 如果選取此選項，Vulnerability Scanner 會判斷用戶端是執行 Windows 或其他作業系統。如果用戶端執行 Windows，Vulnerability Scanner 可以識別其 Windows 版本。
	其他 Ping 設定 如果要設定 Vulnerability Scanner 同時 Ping 的用戶端數量： 1. 瀏覽至 `<Server 安裝資料夾>\PCCSRV\Admin\Utility\TMVS`，然後使用文字編輯器（例如：記事本）開啟 `TMVS.ini`。 2. 變更 `EchoNum` 的值。請指定介於 1 和 64 之間的值。 例如，如果要 Vulnerability Scanner 在同一時間 ping 60 部用戶端，則輸入 `EchoNum=60`。 3. 儲存 `TMVS.ini`。
Security Server 設定	1. 選取「在未受保護的電腦上自動安裝 Security Agent」，將 Security Agent 安裝至 Vulnerability Scanner 將掃瞄的用戶端上。 2. 輸入 Security Server 主機名稱或 IPv4/IPv6 位址，以及通訊埠號碼。Vulnerability Scanner 所安裝的 Security Agent 將向此伺服器回報。 3. 按一下「安裝帳號」設定在登入用戶端時要使用的系統管理認證。在「帳號資訊」畫面中，輸入使用者名稱和密碼，然後按一下「確定」。

以電子郵件通知進行安裝

使用此安裝方法選項可傳送含有安裝程式連結的電子郵件訊息。

步驟

1. 移至「裝置」。
2. 按一下「新增裝置」。
3. 在「電腦類型」區段中，選取「桌上型電腦或伺服器」。
4. 在「方式」區段中選取「電子郵件通知安裝」。
5. 按一下「下一步」。

   隨即顯示新畫面。
6. 輸入電子郵件的主旨和收件者。
7. 按一下「套用」。開啟含有收件者、主旨和安裝程式連結的預設電子郵件用戶端。

移轉至 Security Agent

安裝 Security Agent 時，安裝程式會檢查用戶端上是否已安裝趨勢科技或協力廠商端點安全防護軟體。

安裝程式可執行下列動作：

- 移除用戶端上目前安裝的其他端點安全防護軟體，並取代為 Security Agent
- 偵測其他端點安全防護軟體，但不移除

請造訪下列網站，取得端點安全防護軟體的清單：

http://esupport.trendmicro.com/solution/zh-TW/1060980.aspx

如果用戶端上的軟體無法自動移除，或只能偵測到但無法移除，請先手動解除安裝。視軟體的解除安裝程序而定，解除安裝後，用戶端不一定要重新啟動。

移轉問題和可能的解決方法

由於下列理由，自動解除安裝協力廠商的端點安全防護軟體可能會失敗：

- 其他廠商軟體的版本號碼或產品識別碼不一致。
- 其他廠商軟體的解除安裝程式未正常執行。
- 其他廠商軟體的某些檔案遺失或已損壞。
- 無法清除其他廠商軟體的登錄機碼。
- 其他廠商軟體沒有解除安裝程式。

這些問題的可能解決方法：

- 手動移除其他廠商軟體。
- 停止其他廠商軟體的服務功能。
- 卸載其他廠商軟體的服務功能或處理程序。

在 Security Agents 上執行安裝後的工作

步驟

1. 檢查下列項目：
   - 端點的 Windows「開始」功能表上出現 Security Agent 捷徑。
   - Trend Micro Worry-Free Business Security Agent 列在端點「控制台」的「新增/移除程式」清單中。
   - 在 Web 主控台上，Security Agent 顯示在「裝置」畫面上，並列在「伺服器（預設）」或「桌上型電腦（預設）」群組中（根據端點的作業系統類型而定）。

     注意

     如果您未看到 Security Agent，請從「管理 > 全域設定 > 系統（標籤）> 代理程式連線驗證」執行連線驗證工作。

   - Microsoft 管理主控台顯示下列 Security Agent 服務：
     - Trend Micro Security Agent Listener (`tmlisten.exe`)

- Trend Micro Security Agent RealTime Scan (ntrtscan.exe)
- Trend Micro Security Agent 防火牆 (TmPfw.exe)（如果在安裝期間已啟動防火牆）
- 趨勢科技未經授權的變更阻止服務 (TMBMSRV.exe)（如果在安裝期間已啟動行為監控或周邊設備存取控管）
- 趨勢科技一般用戶端解決方案架構 (TmCCSF.exe)

2. 如果 Security Agent 未顯示在 Web 主控台上，可能是它無法傳送其狀態至伺服器。執行下列任一步驟：

   - 在用戶端上開啟 Web 瀏覽器，於網址文字方塊中輸入 `https://{Trend Micro Security Server_Name}:{通訊埠號碼}/SMB/cgi/cgionstart.exe`，然後按＜ ENTER ＞鍵。

     如果下一個畫面顯示 -2，表示代理程式可以和伺服器進行通訊。因此，這也表示問題可能出在伺服器資料庫，資料庫中可能沒有任何代理程式的記錄。

   - 使用 Ping 與 Telnet 檢查用戶端和伺服器之間的通訊是否正常。
   - 如果您的頻寬有限，請檢查伺服器和用戶端之間是否因為頻寬不足而發生連線逾時。
   - 請檢查伺服器上的 \PCCSRV 資料夾是否有共享的權限，並檢查是否已授與所有使用者完整的控制權限
   - 驗證趨勢科技 Security Server 的 Proxy·伺服器設定是否正確無誤。

3. 使用 EICAR 測試程式檔來測試 Security Agent。

   歐洲電腦防毒研究學會 (EICAR) 已開發出一套測試病毒，可用來測試您的安裝和設定。這個程序檔是沒有作用的文字檔，但是大多數防毒廠商的病毒碼檔案中都含有它的二進位病毒樣式碼。它並不是病毒，也不包含任何程式碼。

   您可以從下面的 URL 下載 EICAR 測試病毒：

   http://www.eicar.org/anti_virus_test_file.htm

   或者，您也可以在文字檔案中輸入下列內容，然後將檔案命名為 eicar.com，以建立自己的 EICAR 測試病毒：

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

注意

測試之前，請先清除快取伺服器和本機瀏覽器中的快取內容。

Messaging Security Agent 安裝

僅在您擁有 Worry-Free Business Security Advanced 版時，才能安裝 Messaging Security Agent。

在 Microsoft Exchange Server 上執行 Messaging Security Agent 的全新安裝。

注意

如需有關升級 Messaging Security Agent 至此版本的資訊，請參閱《安裝和升級手冊》。

Messaging Security Agent 安裝需求

請造訪下列網站，以取得安裝需求的完整清單：

http://docs.trendmicro.com/zh-tw/smb/worry-free-business-security.aspx

安裝 Messaging Security Agent（僅限 Advanced 版）

開始之前

安裝注意事項與提醒：

- 在安裝前或安裝後，皆不需要停止或啟動 Microsoft Exchange 服務。
- 如果端點上留有先前 Messaging Security Agent 安裝的資訊，則無法成功安裝 Messaging Security Agent。請使用 Windows 控制台清除先前安裝所遺留下來的資訊。

  如需詳細資訊，請參閱從 Microsoft Exchange Server 上解除安裝 Messaging Security Agent（僅限 Advanced 版） 第 3-36 頁。
- 如果您要在執行鎖定工具的伺服器上安裝 Messaging Security Agent，請先移除該鎖定工具，以免關閉 IIS 服務而造成安裝失敗。
- Messaging Security Agent 也可在安裝 Security Server 期間安裝。如需詳細資訊，請參閱《安裝和升級手冊》。
- Messaging Security Agent 不支援部分 Microsoft Exchange Server Enterprise 功能，例如資料可用性群組 (DAG)。

步驟

1. 移至「裝置」。
2. 按一下「新增裝置」。
3. 選取「Exchange Server」。
4. 在「Exchange Server 資訊」下，輸入下列資訊：
   - 伺服器名稱：您要在其上安裝代理程式的 Microsoft Exchange Server 名稱。
   - 帳號：內建網域管理員使用者名稱。
   - 密碼：內建網域管理員密碼。
5. 按一下「下一步」。

   安裝精靈會根據要執行的安裝類型來顯示畫面。
   - 全新安裝：Microsoft Exchange Server 上沒有代理程式，並且將安裝代理程式。
   - 升級：Microsoft Exchange Server 上已有舊版代理程式，並且將升級為最新版。

- 不需要安裝：Microsoft Exchange Server 上含有最新版代理程式。如果代理程式目前未出現在「安全群組樹狀結構」中，將會自動新增。
- 無效：安裝代理程式時發生問題。

注意

在「垃圾郵件管理類型」下，會使用「終端使用者隔離」。

6. 在「目錄」下，變更或接受 Messaging Security Agent 安裝預設的目標目錄和共享目錄。預設的目標目錄和共享目錄分別為 `C:\Program Files\Trend Micro\Messaging Security Agent` 和 `C$`。
7. 按一下「下一步」。

   接著會開啟一個新畫面。
8. 確認您在前幾個畫面中指定的 Microsoft Exchange Server 設定正確無誤，然後按一下「下一步」，開始安裝。
9. 如果要檢視安裝的狀態，請按一下「即時狀態」標籤。

移除代理程式

解除安裝代理程式 指令提供下列方式來移除 Security Agent 和 Messaging Security Agent（僅限 Advanced 版）：

- 從 Web 主控台移除代理程式 第 3-34 頁

  此方法適用於離線代理程式。離線代理程式會在 Web 主控台中持續顯示為離線狀態，因為在其中安裝代理程式的用戶端可能已關閉很長時間或已重新格式化，使得代理程式無法解除安裝。

  當您從 Web 主控台移除代理程式時：

  - 代理程式（如果還在用戶端上）不會解除安裝。
  - 伺服器會停止管理代理程式。

- 當代理程式重新與伺服器通訊時（例如，在開啟用戶端後），代理程式將重新新增至 Web 主控台。Security Agent 將會套用其原始群組的設定。如果群組已不存在，代理程式將根據用戶端的作業系統，分組到「伺服器 (預設)」或「桌上型電腦 (預設)」下，並套用該群組的設定。

秘訣

WFBS 還提供了另一種功能來檢查離線代理程式，並將其從 Web 主控台移除。使用此功能可自動完成代理程式移除工作。若要使用此功能，請瀏覽至「管理 > 全域設定 > 系統」標籤，然後移至「移除離線的 Security Agent」區段。

- 從 Web 主控台解除安裝代理程式 第 3-35 頁

  如果您遇到代理程式相關問題，可以解除安裝代理程式（並相應地將其從 Web 主控台中移除）。趨勢科技建議您立即解除安裝代理程式，以防止用戶端遭受安全威脅。

從 Web 主控台移除代理程式

步驟

1. 移至「裝置」。
2. 若要移除 Security Agent，請選取一個群組，然後選取代理程式。若要移除 Messaging Security Agent，請將其選取。

秘訣

如果要選取多個連續的 Security Agents，請先按一下範圍中的第一個代理程式，再按住＜ SHIFT ＞鍵，然後按一下範圍中的最後一個代理程式。如果要選取多個不連續的代理程式，按一下範圍中的第一個代理程式，再按住＜ CTRL ＞鍵，然後按一下您要選取的代理程式。

3. 按一下「詳細資訊 > 解除安裝代理程式」。

   隨即顯示新畫面。

4. 按一下「移除選取的代理程式」。
5. 按一下「套用」。

從 Web 主控台解除安裝代理程式

解除安裝 Messaging Security Agent 時，IIS Admin 服務/Apache 伺服器和所有相關服務皆會自動停止，然後再重新啟動。

步驟

1. 移至「裝置」。
2. 若要解除安裝 Security Agent，請選取一個群組，然後選取代理程式。若要解除安裝 Messaging Security Agent，請將其選取。

   秘訣

   如果要選取多個連續的 Security Agents，請先按一下範圍中的第一個代理程式，再按住＜ SHIFT ＞鍵，然後按一下範圍中的最後一個代理程式。如果要選取多個不連續的代理程式，按一下範圍中的第一個代理程式，再按住＜ CTRL ＞鍵，然後按一下您要選取的代理程式。

3. 按一下「詳細資訊 > 解除安裝代理程式」。

   隨即顯示新畫面。

4. 按一下「解除安裝選取的代理程式」。
5. 按一下「套用」。

   快顯畫面隨即出現，顯示伺服器所傳送的解除安裝通知次數，以及接收通知的代理程式數目。

   注意

   對於 Messaging Security Agent，請在系統提示時輸入對應的 Microsoft Exchange Server 帳號名稱和密碼。

6. 按一下「確定」。
7. 若要驗證代理程式是否已解除安裝，請重新整理「安全設定」畫面。代理程式應不會再出現於「安全群組樹狀結構」中。

從端點解除安裝 Security Agent

視您的組態而定，您可能必須在解除安裝時輸入密碼。如果需要密碼，請確定您只將該密碼提供給需要執行解除安裝程式的使用者；如果該密碼已洩漏給其他使用者，請立即變更密碼。

您可以在「管理 > 全域設定 > 桌上型電腦/伺服器（標籤） > Security Agent 解除安裝密碼」中，設定或關閉密碼。

步驟

1. 按一下「控制台 > 新增或移除程式」。
2. 找到「Trend Micro Worry-Free Business Security Agent」，然後按一下「變更」或「解除安裝」（任一可用選項）。
3. 請遵循畫面上的說明。
4. 如果看到提示，請輸入解除安裝密碼。

   Security Server 會通知使用者解除安裝的進度以及完成結果。使用者不需重新啟動用戶端就能完成解除安裝。

從 Microsoft Exchange Server 上解除安裝 Messaging Security Agent（僅限 Advanced 版）

解除安裝 Messaging Security Agent 時，IIS Admin 服務/Apache 伺服器和所有相關服務皆會自動停止，然後再重新啟動。

步驟

1. 使用管理員權限登入 Microsoft Exchange Server。
2. 按一下「控制台 > 解除安裝程式」。
3. 找到「Trend Micro Messaging Security Agent」，然後按一下「變更」。
4. 請遵循畫面上的說明。

第 4 章

管理裝置

Worry-Free Business Security 會將「裝置」畫面分為兩個主要區段。

- 裝置樹狀結構

  裝置樹狀結構是可展開的邏輯群組清單。可以根據端點類型管理群組，也可以手動設定群組並依據您的需求來安排 Security Agent。

  如需詳細資訊，請參閱使用裝置樹狀結構 第 4-2 頁。

- 群組資訊資料表

  從裝置樹狀結構選取群組後，群組中的 Security Agent 清單會顯示在右側。

  如需詳細資訊，請參閱使用裝置指令 第 4-4 頁。

使用裝置樹狀結構

圖 4-1. 使用裝置樹狀結構指令功能表

若要開啟裝置樹狀結構功能表，請執行下列操作：

- 從裝置樹狀結構選取群組，然後按一下群組名稱旁的齒輪圖示
- 選取 Messaging Security Agent，然後按一下代理程式名稱旁的齒輪圖示

一些指令僅適用於特定群組類型，也可能被停用，具體取決於所選群組的類型。

表 4-1. 裝置樹狀結構指令

指令	說明
新增群組	新增群組至裝置樹狀結構 如需詳細資訊，請參閱新增群組 第 4-7 頁。

指令	說明
開始正常掃瞄	• 對所選群組中的所有端點啟動掃瞄 • 開始掃瞄 Exchange Server
開始加強掃瞄	對所選群組中的所有端點啟動進階掃瞄，以分析和清除正常掃瞄未能移除的安全威脅 注意 執行加強掃瞄可能會影響端點效能，也可能造成誤判數增加。
停止掃瞄	• 對所選群組中的所有端點停止掃瞄 • 停止掃瞄 Exchange Server
設定全域設定	設定安全掃瞄、核可/封鎖的清單、Security Agent 控制和裝置管理的整體 Security Agent 設定。 如需詳細資訊，請參閱全域設定 第 11-2 頁。
設定策略	• 對所選群組中的所有 Security Agent，設定安全設定 如需詳細資訊，請參閱 Security Agent 的基本安全設定摘要 第 5-2 頁。 • 對所選 Messaging Security Agent 設定安全設定 如需詳細資訊，請參閱管理針對 Messaging Security Agent（僅限 Advanced 版）的基本安全設定 第 6-1 頁。
重新命名	變更所選群組的名稱
複製設定	將設定從一個群組複製到另一個群組。目標群組中的 Security Agent 便會採用與來源群組相同的設定 如需詳細資訊，請參閱複製設定 第 4-14 頁。
匯入策略設定	匯入從另一個群組取得的設定 如需詳細資訊，請參閱匯入和匯出 Security Agent 群組的設定 第 4-16 頁。

指令	說明
匯出策略設定	匯出所選群組的設定 如需詳細資訊，請參閱匯入和匯出 Security Agent 群組的設定 第 4-16 頁。
刪除	從裝置樹狀結構刪除群組

使用裝置指令

圖 4-2. 使用裝置指令功能表

從裝置樹狀結構選取群組後，群組中的 Security Agent 清單在資料表中會顯示在右側。資料表頂部的功能表列包含可用來管理 Security Agent 的指令。一些指令僅適用於特定群組類型，也可能被停用，具體取決於所選群組的類型。

使用「裝置」畫面頂部的搜尋列，來使用名稱、標籤或 IP 位址搜尋端點。

秘訣

若要搜尋網路內的端點，您可以輸入部分 IP 位址。例如搜尋 "192" 會傳回其中包含 "192" 的所有 IP 位址，而搜尋 "192." 僅會傳回以 "192" 開頭的所有 IP 位址。但是，無法使用萬用字元和特殊符號（*、+、(、)、-、&）來搜尋端點名稱。

表 4-2. 裝置指令

指令	說明
新增裝置	安裝下列其中一項： • Security Agent：安裝至端點（桌上型電腦或伺服器） • Messaging Security Agent：安裝至 Microsoft Exchange Server（僅限 Advanced 版） 如需詳細資訊，請參閱新增代理程式至群組 第 4-6 頁。
設定策略	對所選群組中的所有 Security Agent，設定安全設定 如需詳細資訊，請參閱 Security Agent 的基本安全設定摘要 第 5-2 頁。
開始正常掃瞄	對所選端點啟動掃瞄
開始加強掃瞄	對所選群組中的所有端點啟動進階掃瞄，以分析和清除正常掃瞄未能移除的安全威脅 注意 執行加強掃瞄可能會影響端點效能，也可能造成誤判數增加。
停止掃瞄	對所選端點停止掃瞄
解除安裝代理程式	從選取的端點移除 Security Agent 如需詳細資訊，請參閱移除代理程式 第 3-33 頁。
重設計數器	為網路上的所有 Security Agent 重設安全威脅偵測計數器。相關的記錄資訊仍可透過「記錄查詢」取得
自訂欄	選擇要在資料表中顯示的欄 如需詳細資訊，請參閱自訂裝置清單欄 第 4-8 頁。
移動 Security Agent	將所選 Security Agent 移動至其他群組或其他 Security Server。 如需詳細資訊，請參閱移動代理程式 第 4-10 頁。

新增代理程式至群組

代理程式在安裝並向 Security Server 回報後，伺服器會將其新增至群組。

- 安裝在伺服器平台上的 Security Agent 會新增至「伺服器（預設）」群組。
- 安裝在桌上型電腦平台上的 Security Agent 會新增至「桌上型電腦（預設）」群組。

注意

您可以移動 Security Agent，將其指定至其他群組。如需詳細資訊，請參閱移動代理程式 第 4-10 頁。

- 每個 Messaging Security Agent（僅限 Advanced 版）即自成群組。無法將多個 Messaging Security Agents 組織為一個群組。

如果「安全群組樹狀結構」上顯示的代理程式數目不正確，可能是代理程式已移除，而伺服器未收到通知（例如，在移除代理程式時，如果用戶端-伺服器通訊中斷）。這會導致伺服器在其資料庫中保留代理程式資訊，並在 Web 主控台上顯示代理程式為離線。重新安裝代理程式時，伺服器會在資料庫中建立新的記錄，並將代理程式視為新增的，導致代理程式重複出現在「安全群組樹狀結構」上。若要檢查是否有重複的代理程式記錄，請使用「管理 > 全域設定 > 系統」中的「代理程式連線驗證」功能。

安裝 Security Agent

請參閱下列主題：

- Security Agent 安裝需求 第 3-2 頁
- Security Agent 安裝考量 第 3-2 頁
- Security Agent 安裝方法 第 3-6 頁
  - 從內部網頁安裝 第 3-7 頁
  - 使用 Login Script Setup 安裝 第 3-10 頁
  - 以 Client Packager 進行安裝 第 3-11 頁

- 以遠端安裝進行安裝 第 3-14 頁
- 使用 Vulnerability Scanner 進行安裝 第 3-17 頁
- 以電子郵件通知進行安裝 第 3-27 頁

- 在 Security Agents 上執行安裝後的工作 第 3-29 頁

安裝 Messaging Security Agent（僅限 Advanced 版）

請參閱下列主題：

- Messaging Security Agent 安裝需求 第 3-31 頁
- 安裝 Messaging Security Agent（僅限 Advanced 版） 第 3-31 頁

新增群組

新增伺服器群組或桌上型電腦群組，其中可包含一或多個 Security Agent。

無法新增包含 Messaging Security Agent 的群組。Messaging Security Agent 在安裝並向 Security Server 回報，即會在「安全群組樹狀結構」中自成小組。

步驟

1. 移至「裝置」。
2. 按一下「新增群組」。

   隨即顯示新畫面。
3. 選取群組類型。
   - 桌上型電腦
   - 伺服器
4. 輸入群組的名稱。
5. 若要將現有群組的設定套用至您新增的群組，按一下「從群組匯入設定」，然後選取群組。僅所選群組類型的群組會顯示。

6. 按一下「儲存」。

自訂裝置清單欄

按一下「裝置清單」頂端的「更多資訊 > 自訂欄」，即可選擇要顯示的欄。

欄	顯示的資訊
適用於 Security Agent	
用戶端	
IP 位址	安裝了代理程式的用戶端 IP 位址
狀態	• 線上：代理程式已連線到 Security Server • 離線：代理程式已與 Security Server 中斷連線
代理程式版本	代理程式的版本
作業系統	安裝了代理程式的用戶端作業系統
架構	• x64：64 位元作業系統 • x86：32 位元作業系統
Exchange 版本	Microsoft Exchange Server 版本
掃瞄	
雲端截毒掃瞄服務 注意 僅在掃瞄方法為雲端截毒掃瞄時，才會顯示此欄。	• 已連線：代理程式已連線到雲端截毒掃瞄服務 • 已中斷連線：代理程式已與雲端截毒掃瞄服務中斷連線 注意 雲端截毒掃瞄服務裝載於 Security Server 上。如果代理程式已中斷連線，表示無法連線到 Security Server，或是雲端截毒掃瞄服務未正常運作（例如，如果服務已停止）。 • 已關閉：代理程式使用標準掃瞄

欄	顯示的資訊
本機雲端病毒碼/病毒碼	本機雲端病毒碼或病毒碼版本
預約掃瞄	上次預約掃瞄的日期和時間
加強掃瞄	上次加強掃瞄的日期和時間
POP3 掃瞄	• 已啟動 • 已關閉
掃瞄方法	• 雲端：本機和雲端掃瞄 • 例行性：僅本機掃瞄 如需詳細資訊，請參閱掃瞄方法 第 5-3 頁。
正常掃瞄	上次正常掃瞄的日期和時間
安全威脅	
偵測到病毒	偵測到的病毒/惡意程式數目
偵測到間諜程式	偵測到的間諜程式/可能的資安威脅程式數目
偵測到的垃圾郵件	垃圾電子郵件數量
違規的 URL	所存取的禁止 URL 數目
病毒引擎	病毒掃瞄引擎版本
適用於 Messaging Security Agent（僅限 Advanced 版）	
名稱	安裝了代理程式的用戶端主機名稱
IP 位址	安裝了代理程式的用戶端 IP 位址
線上/離線	• 線上：代理程式已連線到 Security Server • 離線：代理程式已與 Security Server 中斷連線
平台	安裝了代理程式的用戶端作業系統
架構	• x64：64 位元作業系統 • x86：32 位元作業系統

欄	顯示的資訊
Exchange 版本	Microsoft Exchange Server 版本
病毒碼	病毒碼版本
病毒引擎	病毒掃瞄引擎版本
代理程式版本	代理程式的版本

移動代理程式

有數種方式可用來移動代理程式。

要移動的代理程式	詳細資訊	如何移動代理程式
Security Agent	在群組之間移動 Security Agent。移動後，代理程式會沿用新群組的設定。	使用 Web 主控台移動一或多個代理程式。請參閱在群組之間移動 Security Agent 第 4-11 頁。
	如果您擁有至少兩個 Security Server，可在伺服器之間移動 Security Agent。 移動後，代理程式將列在另一個 Security Server 的「桌上型電腦（預設）」或「伺服器（預設）」群組中（根據用戶端的作業系統類型而定）。代理程式會沿用新群組的設定。	• 使用 Web 主控台移動一或多個代理程式。請參閱使用 Web 主控台在 Security Server 之間移動代理程式 第 4-11 頁。 • 在用戶端上，執行 Client Mover 工具，移動用戶端上所安裝的代理程式。請參閱使用 Client Mover 在 Security Server 之間移動 Security Agent 第 4-13 頁。

要移動的代理程式	詳細資訊	如何移動代理程式
Messaging Security Agent（僅限 Advanced 版）	如果您擁有至少兩個 Security Server，可在伺服器之間移動 Messaging Security Agent。 移動後，代理程式在另一個 Security Server 上將自成群組，並保有其設定。	使用 Web 主控台一次移動一個代理程式。請參閱使用 Web 主控台在 Security Server 之間移動代理程式 第 4-11 頁。

在群組之間移動 Security Agent

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 請選取要移動的代理程式。

   秘訣

   如果要選取多個連續的 Security Agents，請先按一下範圍中的第一個代理程式，再按住＜ SHIFT ＞鍵，然後按一下範圍中的最後一個代理程式。如果要選取多個不連續的代理程式，按一下範圍中的第一個代理程式，再按住＜ CTRL ＞鍵，然後按一下您要選取的代理程式。

4. 將代理程式拖放至新群組。

使用 Web 主控台在 Security Server 之間移動代理程式

開始之前

在 Security Server 之間移動代理程式時：

- 如果舊版代理程式移動至最新版 Security Server，代理程式將會自動更新。
- 請勿將最新版代理程式移動至舊版 Security Server，因為代理程式將會成為未受管理（代理程式將從其先前的伺服器取消註冊，但無法向其新伺服器註冊，因此將不會顯示在 Web 主控台中）。代理程式將會保有其目前版本，不會降級。
- Security Server 必須為相同語言的版本。
- 記錄代理程式將移動至的 Security Server 的主機名稱和監聽通訊埠。主機名稱和監聽通訊埠可在 Security Server 的「安全設定」畫面上找到（「工作」面板上方）。

步驟

1. 在目前管理代理程式的 Security Server 的 Web 主控台上，移至「裝置」。
2. 若要移動 Security Agent，請選取一個群組，然後選取代理程式。若要移動 Messaging Security Agent，請直接選取該代理程式。
3. 按一下「詳細資訊 > 移動 Security Agent」。

   隨即顯示新畫面。
4. 輸入代理程式將移動至的 Security Server 的主機名稱和監聽通訊埠。
5. 按一下「移動」。
6. 若要檢查代理程式現在是否向另一個 Security Server 回報，請開啟該伺服器的 Web 主控台，在「安全群組樹狀結構」尋找代理程式。

注意

如果 Security Agent 未出現在「安全群組樹狀結構」中，請重新啟動伺服器的 Trend Micro Security Server Master Service。

使用 Client Mover 在 Security Server 之間移動 Security Agent

開始之前

在 Security Server 之間移動代理程式時：

- 如果舊版代理程式移動至最新版 Security Server，代理程式將會自動更新。
- 請勿將最新版代理程式移動至舊版 Security Server，因為代理程式將會成為未受管理（代理程式將從其先前的伺服器取消註冊，但無法向其新伺服器註冊，因此將不會顯示在 Web 主控台中）。代理程式將會保有其目前版本，不會降級。
- Security Server 必須為相同語言的版本。
- 記錄代理程式將移動至的 Security Server 的主機名稱和監聽通訊埠。主機名稱和監聽通訊埠可在 Security Server 的「安全設定」畫面上找到（「工作」面板上方）。
- 使用管理員帳號登入用戶端。

步驟

1. 在用戶端上，開啟命令提示字元。

   注意

   您必須以系統管理員身分開啟命令提示字元。

2. 輸入 `cd` 及 Security Agent 安裝資料夾的路徑。例如：`cd C:\Program Files\Trend Micro\Security Agent`
3. 使用下列語法執行 Client Mover：

   ```
   <可執行檔檔案名稱> -s <伺服器名稱> -p <伺服器監聽通訊埠> -c <用戶端監聽通訊埠> -pwd <代理程式「卸載和解除鎖定」權限密碼>
   ```

表 4-3. Client Mover 參數

參數	說明
<可執行檔檔案名稱>	`IpXfer.exe`（32 位元） `IpXfer_x64.exe`（64 位元）
<伺服器名稱>	目標 Worry-Free Business Security 伺服器（代理程式轉移後所在的伺服器）的名稱
<伺服器監聽通訊埠>	目標 Security Server 的監聽通訊埠（或信任的通訊埠）。
<用戶端監聽通訊埠>	Security Agent 用來與伺服器通訊的通訊埠號碼
<代理程式「卸載和解除鎖定」權限密碼>	用於卸載和解除鎖定 Security Agent 的密碼

例如：

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -pwd Password
```

4. 若要檢查 Security Agent 現在是否向另一個 Security Server 回報，請開啟該伺服器的 Web 主控台，在「安全群組樹狀結構」尋找代理程式。

注意

如果 Security Agent 未出現在「安全群組樹狀結構」中，請重新啟動伺服器的 Trend Micro Security Server Master Service。

複製設定

在 Security Agent 群組之間或 Messaging Security Agent 之間複製設定（僅限 Advanced 版）。

複製 Security Agent 群組設定

使用此功能，可將特定桌上型電腦或伺服器群組的設定套用至同類型的其他群組。無法將伺服器群組的設定複製到桌上型群組，反之亦然。

如果某特定群組類型僅包含一個群組，則會關閉此功能。

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下群組名稱旁的齒輪圖示。
4. 按一下「複製設定」。

   隨即顯示新畫面。
5. 選取將繼承設定的目標群組。
6. 按一下「套用」。

複製 Messaging Security Agent 設定（僅限 Advanced 版）

您只能在共享相同網域的 Messaging Security Agent 之間複製設定。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下 Messaging Security Agent 旁的齒輪圖示。
4. 按一下「複製設定」。

   隨即顯示新畫面。

5. 選取將繼承設定的 Messaging Security Agent。
6. 按一下「套用」。
7. 如果複製不成功，請執行以下作業：
   a. 啟動「登錄編輯程式」(regedit)。
   b. 移至 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`。
   c. 以滑鼠右鍵按一下「winreg > 使用權限」。
   d. 新增目標網域的「Smex Admin Group」，並啟動「允許讀取」。

匯入和匯出 Security Agent 群組的設定

將桌上型電腦或伺服器群組的設定匯出至 `.dat` 檔案以備份設定。您也可以使用 `.dat` 檔案匯入設定至其他群組。

注意

您可以在桌上型電腦與伺服器群組之間互相匯入/匯出設定。設定與群組類型無關。您也可以使用「複製設定」功能，不過該功能視群組類型而定。如需有關「複製設定」功能的詳細資訊，請參閱複製設定 第 4-14 頁。

表 4-4. 可以匯入與匯出的設定

選項	包含設定的畫面	可以匯出/匯入的設定
桌上型電腦群組 ( ) 或伺服器群組 ( )	裝置（裝置 > 設定策略）	• 防毒/間諜程式防護（即時掃瞄） • Machine Learning • 行為監控 • 信任的程式 • 隔離 • 網頁信譽評等 • URL 過濾 • 防火牆 • 周邊設備存取控管 • 使用者工具（僅限桌面群組） • 代理程式權限
	手動掃瞄（掃瞄 > 手動掃瞄）	所有設定
	預約掃瞄（掃瞄 > 預約掃瞄）	所有設定

匯出設定

步驟

1. 移至「裝置」。
2. 選取桌上型電腦/伺服器群組。
3. 按一下群組名稱旁的齒輪圖示。
4. 按一下「匯出策略設定」。

   隨即顯示新畫面。

5. 請點選「匯出」。

   會出現對話方塊。

6. 按一下「儲存」，瀏覽偏好的位置，然後按一下「儲存」。

匯入設定

步驟

1. 移至「裝置」。
2. 選取桌上型電腦/伺服器群組。
3. 按一下「匯入策略設定」。

   隨即顯示新畫面。

4. 按一下「瀏覽」並找到檔案，然後按一下「匯入」。

第 5 章

管理 Security Agent 的基本安全設定

本章說明如何設定 Security Agent 的基本安全設定。

Security Agent 的基本安全設定摘要

表 5-1. Security Agent 的基本安全設定摘要

選項	說明	預設
掃瞄方法	設定啟動或關閉「雲端截毒掃瞄」。	「已啟動」或「已關閉」是在安裝期間所選取。
防毒/間諜程式防護	設定即時掃瞄、防毒及間諜程式防護選項	已啟動（即時掃瞄）
Machine Learning	設定 Machine Learning 選項	已關閉
行為監控	設定行為監控選項	針對桌上型電腦群組啟用 針對伺服器群組關閉
信任的程式	指定不需要監控可疑行為的程式	無
隔離	指定隔離目錄	http://<Security Server 名稱或 IP 位址>
網頁信譽評等	設定「在辦公室中」與「辦公室以外的地方」網頁信譽評等選項	在辦公室中：已啟動，低 辦公室以外的地方：已啟動，中
URL 過濾	URL 過濾可以封鎖違反設定之策略的網站。	已啟動，低
核可/封鎖的 URL	設定全域核可/封鎖的清單。	已關閉
防火牆	設定防火牆選項	已關閉
周邊設備存取控管	設定自動執行和 USB 及網路存取	已關閉
使用者工具	設定 Wi-Fi 無線警報器和趨勢科技垃圾郵件防護工具列	已關閉：Wi-Fi 無線警報器 已關閉：支援的電子郵件用戶端中的垃圾郵件防護工具列

選項	說明	預設
代理程式權限	設定對代理程式主控台設定的存取 關閉 Security Agent 升級和 HotFix 部署	無

掃瞄方法

Security Agent 可以使用兩種掃瞄方法中的任意一種，來掃瞄是否有安全威脅。

- 雲端截毒掃瞄：使用雲端截毒掃瞄的 Security Agent 在本文件中稱為雲端截毒掃瞄用戶端。雲端截毒掃瞄用戶端將受益於檔案信譽評等服務提供的本機掃瞄和雲端查詢。
- 標準掃瞄：不使用雲端截毒掃瞄的 Security Agent 被稱為標準掃瞄用戶端。標準掃瞄用戶端會儲存用戶端的所有元件，並在本機掃瞄所有檔案。

下表提供這兩種掃瞄方法的比較。

表 5-2. 標準掃瞄和雲端截毒掃瞄的比較

比較基準	標準掃瞄	雲端截毒掃瞄
掃瞄行為	標準掃瞄 Security Agent 會在用戶端上執行掃瞄。	• 雲端截毒掃瞄用戶端會在用戶端上執行掃瞄。 • 如果掃瞄期間 Security Agent 無法確定檔案的風險，則此 Security Agent 會將掃描查詢傳送至雲端截毒伺服器（適用於已連線至雲端截毒伺服器的 Security Agent）或趨勢科技主動式雲端截毒技術（適用於已與雲端截毒伺服器斷開連線的 Security Agent），來驗證風險。 注意 Scan Server 是一種在雲端截毒伺服器上執行的服務。 • Security Agent 會「快取」掃瞄查詢結果，以提升掃瞄效能。
元件使用中且已更新	所有 Security Agent 元件（本機雲端病毒碼除外）在更新來源都可用	所有元件（「病毒碼」除外）在更新來源都可用
傳統更新來源	主動式更新伺服器	主動式更新伺服器

設定掃瞄方法

開始之前

安裝 Security Server 時，您可以選擇啟動雲端截毒掃瞄。如果已啟動此選項，則預設掃瞄方法為雲端截毒掃瞄，也就是說所有 Security Agent 都將使用雲端截毒掃瞄。否則，預設為標準掃瞄。您可以根據目前的需要，在這兩種方法之間切換代理程式。例如：

- 如果代理程式目前使用標準掃瞄且掃瞄需要很長時間才能完成，您可以切換至設計為更加快速和高效的雲端截毒掃瞄。如果代理程式上的磁碟空間變得很少，您也可以切換至雲端截毒掃瞄，因為雲端截毒掃瞄代理程式會下載較小的病毒碼，因此需要較少的磁碟空間。

  在切換至雲端截毒掃瞄之前，請移至「管理 > 全域設定」，並按一下「桌上型電腦/伺服器」標籤，然後移至「一般掃瞄設定」區段。請確保「關閉雲端截毒掃瞄服務」已關閉。

- 如果您發現 Security Server 的效能下降（表示它無法及時處理來自代理程式的所有掃瞄查詢），請將代理程式切換至標準掃瞄。

下表列出了切換掃瞄方法時的一些注意事項：

表 5-3. 在掃瞄方法之間切換時的注意事項

注意事項	詳細資訊
Security Server 連線	確定 Security Agent 可連線到 Security Server。只有線上代理程式會收到切換至不同掃瞄方法的通知。離線代理程式在線上時才會收到通知。 此外，請驗證 Security Server 是否具有最新的元件，因為代理程式必須從 Security Server 下載新元件，即，本機雲端病毒碼（對於將切換至雲端截毒掃瞄的代理程式）和病毒碼（對於將切換至標準掃瞄的代理程式）。
要切換的 Security Agent 數目	一次切換相對較少數量的 Security Agent，可確保有效利用 Security Server 資源。當代理程式變更其掃瞄方法時，Security Server 可以執行其他重要工作。
時機	首次切換 Security Agent 時，代理程式必須下載完整版的本機雲端病毒碼（對於將切換至雲端截毒掃瞄的代理程式）或病毒碼（對於將切換至標準掃瞄的代理程式）。 建議您在離峰時段進行切換，以確保下載程序可在短時間內完成。此外，請暫時關閉代理程式上的「立即更新」，以阻止使用者啟動的更新，並在代理程式切換掃瞄方法後，再予以重新啟動。 注意 因此，代理程式將下載較小的增量版本機雲端病毒碼或病毒碼（只要它們經常更新）。

注意事項	詳細資訊
IPv6 支援	離線的純 IPv6 雲端截毒掃瞄代理程式無法將查詢直接傳送到趨勢科技主動式雲端截毒技術。 如果要允許雲端截毒掃瞄代理程式傳送查詢，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 移至「掃瞄方法」。
5. 選取偏好的掃瞄方法。
6. 按一下「儲存」。

Security Agent 即時掃瞄

「即時掃瞄」會一直持續進行。每當開啟、下載、複製或修改檔案時，Security Agent 中的「即時掃瞄」即會掃瞄檔案是否含有安全威脅。

設定 Security Agent 即時掃瞄

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。

3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。

4. 按一下「防毒/間諜程式防護」。

   隨即顯示新畫面。

5. 選取「啟動即時防毒/間諜程式防護」。

6. 設定掃瞄設定。如需詳細資訊，請參閱 Security Agent 的掃瞄目標和處理行動 第 7-8 頁：

   注意

   如果您授與使用者設定其自己的掃瞄設定的權限，則會在掃瞄期間使用使用者設定的設定。

7. 按一下「儲存」。

Machine Learning

趨勢科技 Machine Learning 採用進階機器學習技術來關聯安全威脅資訊，並執行深度檔案分析來偵測新興的未知安全威脅，這透過數位 DNA 指紋、API 對應和其他檔案特徵來實現。Machine Learning 還會對未知或不太普遍的處理程序執行行為分析，以確定是否有新興或未知安全威脅正企圖讓您的網路中毒。

Machine Learning 是一個功能強大的工具，可協助保護您的環境，使其免遭不明安全威脅和零時差攻擊。

偵測類型	說明
檔案	Security Agent 在偵測到未知或不常見的檔案之後，會使用進階安全威脅掃瞄引擎 (ATSE) 掃瞄該檔案，以便擷取檔案特徵，然後將報告傳送給裝載於趨勢科技主動雲端截毒技術上的 Machine Learning 引擎。透過使用惡意程式模擬，Machine Learning 將範例與惡意程式模型進行比較、指定概率分數，並確定檔案可能包含的惡意程式類型。 視您對 Machine Learning 進行的設定而定，Security Agent 可能會嘗試「隔離」受影響的檔案，以防安全威脅繼續擴散到您的整個網路。
處理程序	Security Agent 在偵測到未知或不常見的程序之後，會使用關聯式智慧型引擎監控該程序，然後將行為報告傳送給 Machine Learning 引擎。透過使用行為惡意程式塑型，Machine Learning 將處理程序行為與模型進行比較、指定概率分數，並確定處理程序可能正在執行的惡意程式類型。 視您對 Machine Learning 進行的設定而定，Security Agent 可能會「終止」受影響的程序或程式檔，然後嘗試清除執行該程序或程式檔的檔案。

設定 Machine Learning

注意

Machine Learning 需要以下項目：

- 在「設定策略 > 行為監控」中，啟動行為監控。
- 有效的網際網路連線可連線至主動式雲端截毒技術

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。

4. 按一下「Machine Learning」。
5. 選取「啟動 Machine Learning」。
6. 選取偵測類型以及 Machine Learning 所採取的相關處理行動。

偵測類型	處理行動
檔案	• 隔離：選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關特徵的檔案隔離 • 僅記錄檔：選取此項，即會掃瞄未知檔案並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅
處理程序	• 終止：選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關行為的程序或程式檔終止 重要 「Machine Learning」會嘗試將已執行惡意程序或程式檔的檔案清除。如果清除處理行動不成功，Machine Learning 會將受影響的檔案隔離。 • 僅記錄檔：選取此項，即會掃瞄未知程序或程式檔並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅

7. 按一下「儲存」。

行為監控

Security Agent 會持續監控用戶端上的作業系統或已安裝的軟體是否遭到異常修改。系統管理員（或使用者）可建立例外清單，以允許特定程式在違反受監控變更的情況下啟動，或完全封鎖特定程式。此外，一律允許啟動具備有效數位簽章的程式。

「行為監控」的其他功能可保護 EXE 和 DLL 檔案免遭刪除或修改。啟動「行為監控」後，使用者會建立例外，以核可或封鎖特定程式。此外，使用者可以選取全面保護所有 Intuit QuickBooks 程式。

設定行為監控

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「行為監控」。
5. 視需要更新下列項目：
   - 啟動行為監控

     注意

     如果要允許使用者自訂其「行為監控」設定，請移至「裝置 > {群組} > 設定策略 > 代理程式權限 > 行為監控」，然後選取「允許使用者修改行為監控設定」。
   - 針對已知和潛在的威脅啟動惡意程式行為封鎖：惡意程式行為封鎖是使用病毒碼檔案中定義的一組內部規則來完成的。這些規則會識別惡意程式中常見的已知和可疑安全威脅行為。可疑行為的範例包括突然執行無法解釋的新服務、變更防火牆或修改系統檔案等。

     惡意程式行為監控會提供以下威脅程度掃瞄選項：
     - 已知安全威脅：封鎖與已知威脅相關聯的行為
     - 已知和潛在威脅：封鎖與已知威脅相關聯的行為並對可能是惡意的行為採取處理行動

- 在執行經由 HTTP 下載之新發現的程式之前，先提示使用者（伺服器平台除外）：行為監控會與網頁信譽評等共同運作，針對透過 HTTP 通道或電子郵件應用程式下載的檔案，驗證其普遍程度。偵測到「新發現」的檔案後，系統管理員可選擇在執行檔案前先提示使用者。趨勢科技根據檔案偵測次數或檔案的存留時間長度（由主動式雲端截毒技術判定），將某個程式分類為新發現的程式。

  注意

  對於 HTTP 通道，會掃瞄可執行 (.exe) 檔。對於電子郵件應用程式（僅限 Outlook 和 Windows Live Mail），會掃瞄未受密碼保護的封存 (zip/rar) 檔中的可執行 (.exe) 檔。

- 啟動 Intuit QuickBooks 防護：可防止其他程式對所有 Intuit QuickBooks 檔案和資料夾進行未經授權的變更。啟動此功能將不會影響從 Intuit QuickBooks 程式內部進行的變更，而只會防止檔案遭其他未經授權的應用程式變更。

  支援的產品如下：

  - QuickBooks Simple Start
  - QuickBooks Pro
  - QuickBooks Premier
  - QuickBooks Online

  注意

  所有的 Intuit 執行檔都會有數位簽章，這些檔案的更新將不會遭到封鎖。如果其他嘗試變更 Intuit 二進位檔案的程式，則代理程式會顯示一則訊息，其中包含正在嘗試更新二進位檔案的程式名稱。允許其他程式更新 Intuit 檔案。如果要這樣做，請將所需的程式新增至代理程式的「行為監控例外清單」中。在更新之後，請記得將該程式從例外清單中移除。

- 勒索軟體防護：可防止“「勒索軟體」”安全威脅未經授權修改或加密電腦上的檔案。勒索軟體是一種惡意軟體，會限制存取檔案，並要求付錢才能恢復受影響的檔案。

- 對未經授權的加密或修改啟用文件保護：防止對文件進行未經授權的變更。
  - 自動備份由可疑程式變更的檔案：如果已啟動文件保護，則會自動備份由可疑程式修改的檔案。
- 對通常與勒索軟體相關聯的處理程序啟用封鎖：封鎖通常與綁架嘗試相關聯的處理程序，來防止端點遭受勒索軟體攻擊。
- （僅限桌面群組）啟動程式檢測以偵測和封鎖已遭到破壞的可執行檔：監控處理程序是否有類似勒索軟體的行為，以增強偵測。
- 如果程式展現出與弱點攻擊有關的異常行為，請將其終止：弱點攻擊防護會與程式檢測搭配運作，藉以監控程式的行為，並偵測可能代表攻擊者已攻擊程式弱點的異常行為。偵測到異常行為後，「行為監控」就會終止程式程序。

注意

若要使用「弱點攻擊防護」，您必須選取「啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔」。

注意

若要降低 Worry-Free Business Security 將安全程序偵測為惡意程序的機率，請確認電腦可連上網際網路來使用 趨勢科技 伺服器進行其他驗證程序。

- 例外：例外包括「核可的程式清單」和「封鎖的程式清單」。「核可的程式清單」中的程式即使違反受監控的變更仍可啟動，而「封鎖的程式清單」中的程式則一律無法啟動。
  - 請輸入完整的程式路徑：輸入程式的完整 Windows 或 UNC 路徑。以半形分號 (;) 分隔多個項目。按一下「新增至例外清單」或「新增至封鎖的清單」。您可以視需要使用環境變數指定路徑。
  - 核可的程式清單：此清單中的程式可以啟動。按一下對應的圖示即可刪除項目。

    「核可的程式清單」支援萬用字元和環境變數。

如需支援的環境變數清單，請參閱支援的環境變數 第 5-13 頁。

- 封鎖的程式清單：此清單中的程式始終無法啟動。按一下對應的圖示即可刪除項目。

  「封鎖的程式清單」僅支援萬用字元。

6. 按一下「儲存」。

支援的環境變數

下表列出您在將檔案或資料夾路徑新增到清單時可使用的環境變數。

環境變數	範例	對等的路徑
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

信任的程式

不會監控「信任的程式清單」中的程式是否存在可疑的檔案存取活動。

設定信任的程式

注意

「信任的程式清單」不支援萬用字元和環境變數。

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「信任的程式」。

   隨即顯示新畫面。
5. 如果要將程式從可疑的檔案存取活動監控中排除，請使用特定檔案路徑輸入完整的檔案路徑，然後按一下「新增至信任的程式清單」。

   `<drive_name>:/<path>/<file_name>`

   範例 1：`C:\Windows\system32\regedit.exe`

   範例 2：`D:\backup\tool.exe`

   這可防止駭客在例外清單中使用程式名稱，但卻遺留下可執行的不同檔案路徑。
6. 按一下「儲存」。

隔離目錄

如果中毒檔案的處理行動為「隔離」，Security Agent 即會加密該檔案，並暫時將其移至隔離資料夾，位置如下：

- 從 6.x 或更舊版本升級的代理程式：`<Security Agent 安裝資料夾>\quarantine`
- 新安裝的代理程式，以及從 7.x 或更新版本升級的代理程式：`<Security Agent 安裝資料夾>\SUSPECT\Backup`

Security Agent 會將中毒檔案傳送至中央隔離目錄，您可從 Web 主控台的「裝置 > {群組} > 設定策略 > 隔離」設定該目錄。

預設中央隔離目錄

預設的中央隔離目錄位於 Security Server 上。此目錄採用 URL 格式，並且包含 Security Server 的主機名稱或 IP 位址，例如：`http://server`。對等的絕對路徑為 `<Security Server 安裝資料夾>\PCCSRV\Virus`。

- 如果伺服器同時管理 IPv4 和 IPv6 代理程式，則使用主機名稱，以便全部代理程式都可以將隔離檔案傳送到該伺服器。
- 如果伺服器只具有 IPv4 位址，或只透過其 IPv4 位址進行識別，則只有純 IPv4 和雙堆疊代理程式可以將隔離檔案傳送到該伺服器。
- 如果伺服器只具有 IPv6 位址，或只透過其 IPv6 位址進行識別，則只有純 IPv6 和雙堆疊代理程式可以將隔離檔案傳送到該伺服器。

替代的中央隔離目錄

您可以輸入 URL、UNC 路徑或絕對檔案路徑格式的位置來指定替代的中央隔離目錄。Security Agent 應能夠連線到此目錄。例如，如果目錄將接收來自雙堆疊用戶端和純 IPv6 用戶端的隔離檔案，此目錄應具有 IPv6 代理程式。趨勢科技建議指定雙堆疊目錄、透過其主機名稱識別目錄以及在輸入目錄時，使用 UNC 路徑。

關於指定中央隔離目錄的指導方針

如需何時應使用 URL、UNC 路徑或絕對檔案路徑的相關指引，請參閱下表：

表 5-4. 隔離目錄

隔離目錄	接受的格式	範例	注意事項
Security Server 上的預設目錄	URL	`http:// <伺服器主機名稱或 IP>`	如果您保留預設目錄，請在「管理 > 全域設定 > 系統（標籤） > 隔離維護」區段中，進行目錄的維護設定，例如隔離資料夾的大小。
	UNC 路徑	`\\<伺服器主機名稱或 IP>\ofcscan\Virus`	
Security Server 上的其他目錄	UNC 路徑	`\\<伺服器主機名稱或 IP>\D$\Quarantined Files`	如果您不想使用預設目錄（例如：如果其磁碟空間不足），請輸入其他目錄的 UNC 路徑。如果要進行此動作，請在「管理 > 全域設定 > 系統（標籤） > 隔離維護」區段中輸入對等的絕對路徑，維護設定才能生效。
其他 Security Server 電腦上的目錄（若您在網路上有其他 Security Server）	URL	`http://<Server2主機名稱或 IP>`	確定代理程式可連線到此目錄。如果您指定不正確的目錄，代理程式會保留已隔離的檔案，直到指定正確的隔離目錄為止。在伺服器的病毒/惡意程式記錄檔中，掃瞄結果為「無法將隔離檔案傳送到指定的隔離資料夾」。 如果您使用 UNC 路徑，請確定是否可讓「Everyone」群組共享隔離目錄資料夾，並指定讀取和寫入權限給這個群組。
	UNC 路徑	`\\<其他伺服器的主機名稱或 IP>\ofcscan\Virus`	
網路上的另一部電腦	UNC 路徑	`\\<computer_name>\temp`	
用戶端上的其他目錄	絕對路徑	`C:\temp`	請在下列情況下，指定絕對路徑： • 您想要讓隔離的檔案僅位於用戶端上。 • 您不想讓代理程式將檔案儲存在用戶端中的預設目錄。 如果該路徑不存在，Security Agent 會自動建立。

設定隔離目錄

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「隔離」。

   隨即顯示新畫面。
5. 設定隔離目錄。如需詳細資訊，請參閱隔離目錄 第 5-15 頁。
6. 按一下「儲存」。

網頁信譽評等

網頁信譽評等可防止使用者存取具有潛在安全威脅的 Web 上或嵌入電子郵件中的 URL。網頁信譽評等會根據趨勢科技網頁信譽評等伺服器檢查 URL 的信譽，然後將信譽與電腦上實施的特定網頁信譽評等策略關聯。根據所使用的策略：

- Security Agent 將封鎖或允許對網站的存取。
- Messaging Security Agent（僅限 Advanced 版）將隔離、刪除或標記包含惡意 URL 的電子郵件，或允許傳送郵件（如果 URL 是安全的）。

網頁信譽評等可針對相關偵測，為管理員提供電子郵件通知，並對使用者提供線上通知。

在 Security Agent 中，根據用戶端的所在位置（在辦公室中/辦公室以外的地方），設定不同的安全層級。

如果「網頁信譽評等」封鎖了您認為安全無虞的 URL，請將該 URL 新增至核可的 URL 清單中。

秘訣

為了節省網路頻寬，趨勢科技建議您將企業內部網站新增至網頁信譽評等核可的 URL 清單。

信譽評分

URL 的「信譽評分」會決定其是否為網路安全威脅。趨勢科技則使用專有度量來計算分數。

如果 URL 的分數在定義的門檻值內，趨勢科技會將此 URL 視為 Web 安全威脅；如果分數超過該門檻值，則會將此 URL 視為安全的。

Security Agent 有三種安全層級，可決定允許還是封鎖對 URL 的存取。

- 高：封鎖下列網頁：
  - 危險：經驗證為詐騙網頁或已知的威脅來源
  - 非常可疑：懷疑可能是詐騙網頁或可能的威脅來源
  - 可疑：與垃圾郵件相關或可能遭到破壞
  - 未測試的：雖然趨勢科技會主動測試網頁以確保安全，但使用者仍可能會在造訪新的或較不熱門的網站時遇到未測試的網頁。封鎖對於未測試網頁的存取，可以提高安全，但也會讓人無法存取某些安全的網頁。
- 中：封鎖下列網頁：
  - 危險：經驗證為詐騙網頁或已知的威脅來源
  - 非常可疑：懷疑可能是詐騙網頁或可能的威脅來源
- 低：封鎖下列網頁：
  - 危險：經驗證為詐騙網頁或已知的威脅來源

設定 Security Agent 網頁信譽評等

「網頁信譽評等」可評估任何所要求 URL 的潛在安全威脅，您只要在每次出現 HTTP/HTTPS 要求時，查詢 Trend Micro Security 資料庫即可。

注意

（僅限 Standard 版）設定「在辦公室中」與「辦公室以外的地方」適用的「網頁信譽評等」設定。關閉「位置偵測」時，「辦公室以外的地方」連線將會使用「在辦公室中」的設定。如需有關「位置偵測」的詳細資訊，請參閱進行桌上型電腦/伺服器設定 第 11-4 頁。

如果「網頁信譽評等」和「瀏覽器攻擊防範」都已啟動，則「瀏覽器攻擊防範」會掃瞄「網頁信譽評等」未封鎖的 URL。「瀏覽器攻擊防範」會掃瞄 URL 網頁中的嵌入式物件，例如 jar、class、pdf、swf、html、js 物件。

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「網頁信譽評等 > 在辦公室中」或「網頁信譽評等 > 辦公室以外的地方」。

   隨即顯示新畫面。
5. 視需要更新下列項目：
   - 啟動網頁信譽評等
   - 安全層級：「高」、「中」或「低」
   - 瀏覽器攻擊防範：封鎖包含惡意程式檔的頁面
6. 按一下「儲存」。

URL 過濾

URL 過濾可協助您控制網站的存取以減少員工上班打混摸魚的時間、減少 Internet 頻寬用量，同時建立更安全的 Internet 環境。您可以選擇想要的 URL 過濾保護層級，或是自訂要過濾的網站類型。

注意

為了保護客戶，趨勢科技會自動封鎖包含在大部分地區被認為是非法內容的所有 URL。

設定 URL 過濾

您可以藉由選取「自訂」，選取在一天的不同時間封鎖特定類型的網站。

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「URL 過濾」。

   隨即顯示新畫面。
5. 視需要更新下列項目：
   - 啟動 URL 過濾
   - 過濾強度
     - 高：封鎖已知或潛在的安全威脅、不適當或可能令人不悅的內容，或是封鎖可能會影響產能或頻寬的內容，以及未分級的頁面

- 中：封鎖已知的安全威脅與不適當的內容
- 低：封鎖已知的安全威脅
- 自訂：選取您的個人類別，以及您是否想要在上班時間或休閒時間封鎖這些類別。

- 過濾規則：選取要封鎖的整個類別或子類別。
- 上班時間：凡是未定義於「上班時間」下方的任意天或小時均視為「休閒時間」。

6. 按一下「儲存」。

核可/封鎖的 URL

自動化的 URL 核可和封鎖可協助您控制網站的存取，並建立更安全的 Internet 環境。在「全域設定」中找出核可或封鎖的 URL。

您也可以針對特定群組，建立自訂的 URL 核可和封鎖清單。選取「自訂此群組核可/封鎖的 URL」選項時，Security Agent 會使用群組的自訂核可或封鎖 URL 清單控制網站的存取。

設定核可/封鎖的 URL

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「核可/封鎖的 URL」。

   隨即顯示新畫面。

5. 視需要更新下列項目。
   - 自訂此群組核可/封鎖的 URL：此清單中指定的 URL 會覆寫所有其他設定。
   - 在「要核可的 URL」文字方塊中，輸入要排除在網頁信譽評等和 URL 過濾驗證範圍外的網站 URL。請以分號 (;) 分隔多個 URL。按一下「新增」。

     秘訣

     按一下「從全域設定匯入」，插入所有項目。然後，您可以針對此群組自訂 URL。
   - 在「要封鎖的 URL」文字方塊中，輸入要在 URL 過濾時封鎖的網站 URL。請以分號 (;) 分隔多個 URL。按一下「新增」。

     秘訣

     按一下「從全域設定匯入」，插入所有項目。然後，您可以針對此群組自訂 URL。
6. 按一下「儲存」。

防火牆

防火牆能在用戶端和網路之間建立一道屏障，以封鎖或允許特定類型的網路流量。此外，防火牆會辨識網路封包中可能攻擊用戶端的行為模式。

Worry-Free Business Security 在設定防火牆時有兩個可以選擇的選項：簡易模式和進階模式。簡易模式會使用趨勢科技建議的預設設定來啟動防火牆。使用進階模式自訂防火牆設定。

秘訣

趨勢科技建議您在部署和啟動趨勢科技防火牆之前，先解除安裝其他防火牆軟體。

預設的防火牆簡易模式設定

防火牆提供的預設設定，讓您能夠啟動用戶端防火牆的防護策略。預設值是用來包含用戶端上常會產生的情況，例如必須存取 Internet，以及使用 FTP 下載或上傳檔案等。

注意

依預設，Worry-Free Business Security 會關閉所有新群組和 Security Agent 上的防火牆。

表 5-5. 預設的防火牆設定

設定	狀態
安全層級	低 允許入站和出站流量，只封鎖網路病毒。
入侵偵測系統	已關閉
警訊（傳送）	已關閉

表 5-6. 預設防火牆例外

例外名稱	處理行動	方向	通訊協定	通訊埠
DNS	允許	輸入和輸出	TCP/UDP	53
NetBIOS	允許	輸入和輸出	TCP/UDP	137, 138, 139, 445
HTTPS	允許	輸入和輸出	TCP	443
HTTP	允許	輸入和輸出	TCP	80
Telnet	允許	輸入和輸出	TCP	23
SMTP	允許	輸入和輸出	TCP	25
FTP	允許	輸入和輸出	TCP	21
POP3	允許	輸入和輸出	TCP	110

例外名稱	處理行動	方向	通訊協定	通訊埠
MSA	允許	輸入和輸出	TCP	16372, 16373
LDAP	允許	輸入和輸出	TCP/UDP	389

表 5-7. 根據位置而定的預設防火牆設定

位置	防火牆設定
在辦公室中	關閉
辦公室以外的地方	關閉

傳輸過濾功能

防火牆會過濾所有輸入和輸出，提供根據下列條件封鎖特定傳輸類型的能力：

- 方向（入站/出站）
- 通訊協定 (TCP/UDP/ICMP/ICMPv6)
- 目標通訊埠
- 目標電腦

掃瞄網路病毒

防火牆也會檢查每個封包是否有網路病毒。

狀態檢測

防火牆是一種狀態檢測防火牆，會監控所有與用戶端間的連線，且會記憶所有連線狀態。它可識別任何連線的特定狀況、預測應該採用的處理行動，並偵測一般連線的中斷情況。因此，有效地使用防火牆不僅需要建立資料檔和策略，還需要分析連線和過濾通過防火牆的封包。

一般防火牆驅動程式

「一般防火牆驅動程式」搭配使用「防火牆」的使用者所定義的設定，可以在疫情爆發期間封鎖通訊埠。「一般防火牆驅動程式」也會使用網路病毒碼檔案偵測網路病毒。

設定防火牆

設定辦公室內外的防火牆。關閉「位置偵測」時，「辦公室以外的地方」連線將會使用「在辦公室中」的設定。

如需有關「位置偵測」的詳細資訊，請參閱進行桌上型電腦/伺服器設定 第 11-4 頁。

依預設，趨勢科技會停用防火牆。

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「防火牆 > 在辦公室中」或「辦公室以外的地方」。
5. 選取「啟動防火牆」。
6. 選取下列選項：
   - 簡易模式：以預設設定啟動防火牆。

     如需詳細資訊，請參閱防火牆 第 5-22 頁。
   - 進階模式：以自訂設定啟動防火牆。
7. 如果您選取「進階模式」，視需要更新下列選項：
   - 安全層級：安全層級可控制要對不在例外清單中的通訊埠執行的流量規則。
     - 高：除了例外清單中所允許的流量外，封鎖所有其他的入站流量和出站流量。
     - 中：除了例外清單中所允許和封鎖的流量外，封鎖所有入站流量且允許所有出站流量。

- 低：除了例外清單中所封鎖的流量外，允許所有其他的入站流量和出站流量。此為「簡易模式」的預設設定。

- 設定
  - 啟動入侵偵測系統：「入侵偵測系統」可辨識網路封包中具有攻擊徵象的病毒碼。

    如需詳細資訊，請參閱入侵偵測系統 第 D-3 頁。

  - 啟動警告訊息：當 Worry-Free Business Security 偵測到違規時，會通知用戶端。
- 例外：將不會封鎖例外清單中的通訊埠。

  如需詳細資訊，請參閱使用防火牆例外 第 5-26 頁。

8. 按一下「儲存」。

使用防火牆例外

「防火牆」例外規則清單所包含的項目，可讓您在加以設定後根據用戶端的通訊埠號碼和 IP 位址允許或封鎖不同類型的網路流量。在疫情爆發期間，Security Server 會套用自動部署的趨勢科技策略例外，以保護您的網路。

例如，在疫情爆發期間，您可能會選擇封鎖所有用戶端傳輸，包括 HTTP 通訊埠（通訊埠 80）。不過，如果您仍然要將 Internet 存取權限授與封鎖的用戶端，則可以將 Web Proxy 伺服器加入例外清單。

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。

4. 按一下「防火牆 > 在辦公室中」或「防火牆 > 辦公室以外的地方」。

   隨即顯示新畫面。

5. 選取「啟動防火牆」。
6. 選取「進階模式」。
7. 如果要新增例外：
   a. 按一下「新增」。

      隨即顯示新畫面。

   b. 輸入例外的名稱。
   c. 在「處理行動」旁，按下列其中一項：
      - 允許所有網路流量
      - 拒絕所有網路流量

   d. 在「方向」旁，按一下「入站」或「出站」，選取要套用例外設定的流量類型。
   e. 從「通訊協定」清單中，選取網路通訊協定的類型：
      - 所有
      - TCP/UDP（預設值）
      - TCP
      - UDP
      - ICMP
      - ICMPv6

   f. 按下列其中一項，以指定用戶端通訊埠：
      - 所有通訊埠（預設值）
      - 範圍：輸入通訊埠範圍
      - 指定的通訊埠：指定個別的通訊埠。請使用逗號 (,) 分隔通訊埠號碼。

g. 在「機器」下，選取要納入例外中的用戶端 IP 位址。例如，如果您選取「拒絕所有網路流量（入站和出站）」並輸入網路上用戶端的 IP 位址，則策略中具有此項例外的用戶端將無法傳送資料到此 IP 位址或接收來自此 IP 位址的資料。按一下下列其中一個項目：

- 所有 IP 位址（預設值）
- 單一 IP：輸入 IPv4 或 IPv6 位址，或主機名稱。如果要將用戶端主機名稱解析為 IP 位址，請按一下解析。
- IP 範圍（適用於 IPv4 或 IPv6）：在「起始」和「結束」欄位中，輸入兩個 IPv4 或兩個 IPv6 位址。不能在一個欄位中輸入 IPv6 位址，而在另一個欄位中輸入 IPv4 位址。
- IP 範圍（適用於 IPv6）：輸入 IPv6 位址字首和長度。

h. 按一下「儲存」。

8. 若要編輯例外，按一下「編輯」，然後在顯示的畫面中修改設定。
9. 如果要在清單中上移或下移例外，請選取該例外，然後按一下「上移」或「下移」，直到例外移到正確的位置。
10. 如果要移除例外，請選取該例外，然後按一下「移除」。

關閉代理程式群組上的防火牆

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。
4. 按一下「防火牆 > 在辦公室中」或「防火牆 > 辦公室以外的地方」。

   隨即顯示新畫面。

5. 選取「關閉防火牆」。
6. 按一下「儲存」。

關閉所有代理程式上的防火牆

步驟

1. 移至「管理 > 全域設定」。
2. 按一下「桌上型電腦/伺服器」。
3. 在「防火牆設定」中，選取「關閉防火牆並解除安裝驅動程式」。
4. 按一下「儲存」。

周邊設備存取控管

周邊設備存取控管可對已連接至端點的外部儲存裝置存取加以規範。具體而言，周邊設備存取控管會對各種透過 USB 接口連接的儲存裝置存取加以限制，但行動裝置和數位相機除外。

設定周邊設備存取控管

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。

4. 按一下「周邊設備存取控管」。
5. 視需要更新下列項目：
   - 啟動周邊設備存取控管
   - 啟動 USB 自動執行防範
   - 權限：同時針對 USB 裝置和網路資源進行設定。

     表 5-8. 周邊設備存取控管權限

權限	裝置上的檔案	輸入的檔案
完整存取	允許的作業：複製、移動、開啟、儲存、刪除、執行	允許的作業：儲存、移動、複製 這表示檔案可以儲存、移動與複製到裝置上。
無存取權限	禁止的作業：所有作業 向使用者顯示裝置與其包含的檔案（例如，從 Windows 檔案總管）。	禁止的作業：儲存、移動、複製
讀取	允許的作業：複製、開啟 禁止的作業：儲存、移動、刪除、執行	禁止的作業：儲存、移動、複製
修改	允許的作業：複製、移動、開啟、儲存、刪除 禁止的作業：執行	允許的作業：儲存、移動、複製
讀取和執行	允許的作業：複製、開啟、執行 禁止的作業：儲存、移動、刪除	禁止的作業：儲存、移動、複製

   - 例外：如果未將特定裝置的讀取權限授予使用者，該使用者仍可以執行或開啟「例外清單」上的任何檔案或程式。

     不過，如果啟動了自動執行防範，即使檔案位於「例外清單」，依然不得執行。

如果要將例外項新增至「例外清單」，請輸入含有路徑或數位簽名的檔案名稱，然後按一下「新增至例外清單」。

6. 按一下「儲存」。

使用者工具

- 垃圾郵件防護工具列：過濾 Microsoft Outlook 中的垃圾郵件、提供統計資料，並可讓您變更特定設定。
- HouseCall：根據存取點 SSID 的有效性、驗證方法及加密需求檢查存取點的可信賴性，從而判斷無線連線是否安全。如果連線不安全，會顯示快顯視窗警告。
- 案例診斷工具：Trend Micro Case Diagnostic Tool (CDT) 會在問題發生時從客戶的產品中收集必要偵錯資訊，也會自動開啟產品的偵錯狀態並根據問題類別收集必要檔案。趨勢科技會使用這項資訊針對產品相關問題進行疑難排解。

  此工具僅在 Security Agent 主控台上可用。
- Client Mover：使用此工具可以將用戶端從某部伺服器移轉到另一部伺服器上。伺服器必須為相同語言的版本和類型。
- 用戶端與伺服器之間的通訊工具：使用此工具對用戶端與伺服器之間的通訊進行疑難排解。

設定使用者工具

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

「設定策略：<群組名稱>」畫面隨即顯示。

4. 按一下「使用者工具」。

   隨即顯示新畫面。

5. 視需要更新下列項目：

   - Wi-Fi 無線警報器：根據無線網路的 SSID、驗證方法和加密需求的有效性，檢查其安全。
   - 垃圾郵件防護工具列：過濾 Microsoft Outlook 中的垃圾郵件。

6. 按一下「儲存」。

代理程式權限

授與代理程式權限可讓使用者修改用戶端上的 Security Agent 設定。

秘訣

如果要在整個組織中強制實施規定的安全策略，趨勢科技建議僅授與使用者有限的權限。如此可確保使用者不會修改掃瞄設定或卸載 Security Agent。

設定代理程式權限

步驟

1. 移至「裝置」。
2. 選取桌上型電腦或伺服器群組。
3. 按一下「設定策略」。

   「設定策略：<群組名稱>」畫面隨即顯示。

4. 按一下「代理程式權限」。

5. 視需要更新下列項目：

區段	權限
防毒/間諜程式防護	• 即時掃瞄設定 • 手動掃瞄設定 • 預約掃瞄設定 • 跳過預約掃瞄
防火牆	防火牆設定
網頁信譽評等 - 繼續瀏覽	將顯示一個連結來讓使用者繼續瀏覽特定的惡意 URL，直到電腦重新啟動。對其他惡意 URL 仍會顯示警告。
URL 過濾 - 繼續瀏覽	將顯示一個連結來讓使用者繼續瀏覽特定的受限制 URL，直到電腦重新啟動。對其他受限制的 URL 仍會顯示警告。
行為監控	允許使用者修改行為監控設定。
信任的程式	允許使用者修改信任的程式清單。
Proxy 伺服器設定	允許使用者設定 Proxy 伺服器設定。 注意 如果關閉此功能，會將 Proxy 伺服器設定重設為預設值。

區段	權限
更新權限	• 允許使用者執行手動更新 • 將趨勢科技的主動式更新用作次要更新來源 • 關閉 Hot Fix 部署 **注意** 同時將 Hot Fix、修補程式、安全修補程式/重要修補程式和 Service Pack 部署到大量 Agent，可能會顯著增加網路流量。請考慮以多個群組啟用此選項，以便交錯進行部署。 啟用此選項還會關閉 Agent 的自動 build 升級（例如，從目前產品版本的測試版 build 到發行版 build），但不會關閉自動版本升級（例如，從 7.x 版到目前版本）。若要關閉自動版本升級，請執行 Security Server 安裝套件，並選擇延遲升級的選項。
用戶端安全等級	防止使用者或其他程序修改趨勢科技程式檔案、登錄和程序。

6. 按一下「儲存」。

第 6 章

管理針對 Messaging Security Agent（僅限 Advanced 版）的基本安全設定

本章說明 Messaging Security Agent，並解釋如何針對代理程式設定即時掃瞄選項、設定垃圾郵件防護、內容過濾、附件封鎖及隔離維護選項。

Messaging Security Agent

Messaging Security Agent 可保護 Microsoft Exchange Server。代理程式會掃瞄 Microsoft Exchange 信箱儲存區收到和寄出的電子郵件，以及在 Microsoft Exchange Server 與外部目的地之間傳遞的電子郵件，藉以防止透過電子郵件傳播的安全威脅。此外，Messaging Security Agent 亦可：

- 減少垃圾郵件
- 根據內容封鎖電子郵件
- 封鎖或限制含附件的電子郵件
- 偵測電子郵件中的惡意 URL
- 防止機密資料外洩

關於 Messaging Security Agent 的重要資訊

- Messaging Security Agent 僅能安裝於 Microsoft Exchange Server 上。
- Messaging Security Agent 不支援部分 Microsoft Exchange Server Enterprise 功能，例如資料可用性群組 (DAG)。
- Web 主控台中的「安全群組樹狀結構」會顯示所有的 Messaging Security Agent。您無法將多個 Messaging Security Agent 合併到一個群組中；每個 Messaging Security Agent 必須分開管理。
- Worry-Free Business Security 會使用 Messaging Security Agent 收集來自 Microsoft Exchange Server 的安全資訊。例如，Messaging Security Agent 會在偵測到垃圾郵件或完成元件更新時，向 Security Server 報告。此資訊會顯示於 Web 主控台中。Security Server 也會使用此資訊，來產生有關 Microsoft Exchange Server 安全狀態的記錄檔和報告。

  每個偵測到的安全威脅都會產生一個記錄檔項目/通知。這表示如果 Messaging Security Agent 在單一電子郵件中偵測到多個安全威脅，則會產生多個記錄檔項目和通知。也可能會發生偵測到數次相同安全威脅的實體，特別是如果有使用 Outlook 2003 的快取模式。當啟動快取模式時，可能會同時在傳輸佇列資料夾和「寄件備份」資料夾（或在「寄件匣」資料夾）中偵測到相同的安全威脅。

- 在執行 Microsoft Exchange Server 2007 的電腦中，Messaging Security Agent 會使用 SQL Server 資料庫。為了防止發生問題，Messaging Security Agent 服務是相依於 SQL Server 服務實體 MSSQL$SCANMAIL 而設計的。每當此實體停止或重新啟動時，下列 Messaging Security Agent 服務也會停止：

  - ScanMail_Master
  - ScanMail_RemoteConfig

  如果 MSSQL$SCANMAIL 停止或重新啟動，請手動重新啟動這些服務。不同的事件，包括 SQL Server 更新時，會造成 MSSQL$SCANMAIL 重新啟動或停止。

Messaging Security Agent 如何掃瞄電子郵件

Messaging Security Agent 會以下列順序掃瞄電子郵件：

1. 掃瞄垃圾郵件（垃圾郵件防護）
   a. 將電子郵件與系統管理員的「核可/封鎖的寄件人」清單進行比較
   b. 檢查網路釣魚事件
   c. 將電子郵件與趨勢科技提供的例外清單進行比較
   d. 將電子郵件與垃圾郵件特徵資料庫進行比較
   e. 套用自動邏輯分析掃瞄規則
2. 掃瞄內容過濾規則違規
3. 掃瞄超過使用者定義之參數的附件
4. 掃瞄病毒/惡意程式（防毒）
5. 掃瞄惡意 URL

預設 Messaging Security Agent 設定

將表格中列出的選項納入考量，以協助您最佳化 Messaging Security Agent 組態。

表 6-1. 趨勢科技對於 Messaging Security Agent 的預設處理動作

掃瞄選項	即時掃瞄	手動掃瞄和預約掃瞄
垃圾郵件防護		
垃圾郵件	將郵件隔離到使用者的垃圾郵件資料夾（如果已安裝 Outlook 垃圾郵件或終端使用者垃圾郵件隔離，則為預設值）	無
網路釣魚	刪除整封郵件	無
內容過濾		
過濾符合任何定義條件的郵件	隔離整個郵件	取代
過濾符合所有定義條件的郵件	隔離整個郵件	無
監控特定電子郵件帳號的郵件內容	隔離整個郵件	取代
建立要排除特定的電子郵件帳號	通過	通過
附件封鎖		
處理行動	以文字/檔案取代附件	以文字/檔案取代附件
其他		
加密和受密碼保護的檔案	暫不處理（處理行動設定為「暫不處理」時，會暫不處理加密及受密碼保護的檔案，而且不會記錄該事件）	暫不處理（處理行動設定為「暫不處理」時，會暫不處理加密及受密碼保護的檔案，而且不會記錄該事件）

掃瞄選項	即時掃瞄	手動掃瞄和預約掃瞄
例外檔案（超出指定掃瞄限制的檔案）	暫不處理（處理行動設定為「暫不處理」時，會暫不處理超出指定掃瞄限制的檔案或郵件內文，而且不會記錄該事件）	暫不處理（處理行動設定為「暫不處理」時，會暫不處理超出指定掃瞄限制的檔案或郵件內文，而且不會記錄該事件）

Messaging Security Agent 的「即時掃瞄」

「即時掃瞄」會一直持續進行。Messaging Security Agent（僅限 Advanced 版）中的即時掃瞄會掃瞄所有收到的郵件、SMTP 郵件、張貼於公共資料夾的文件，以及從其他 Microsoft Exchange Server 複製的所有檔案，藉此防護所有已知的病毒進入點。

設定 Messaging Security Agent 的「即時掃瞄」

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「防毒」。

   隨即顯示新畫面。
5. 選取「啟動即時防毒」。
6. 設定掃瞄設定。如需詳細資訊，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁。
7. 按一下「儲存」。

設定在事件發生時將由誰接收通知。請參閱設定通知事件 第 10-4 頁。

垃圾郵件防護

Worry-Free Business Security 提供兩種方式抵禦垃圾郵件 —「電子郵件信譽評等服務」和「內容掃瞄」。

Messaging Security Agent 使用以下元件過濾電子郵件以防範垃圾郵件和網路釣魚事件：

- 趨勢科技垃圾郵件防護引擎
- 趨勢科技垃圾郵件病毒碼檔案

趨勢科技會經常更新引擎和病毒碼檔案並提供下載檔。Security Server 可以運用手動或預約更新下載這些元件。

垃圾郵件防護引擎使用垃圾郵件的特徵和自動邏輯分析規則來過濾電子郵件。它會掃瞄電子郵件，並且依據與病毒碼檔案中規則及格式的接近程度，對每一封電子郵件指定垃圾郵件指數。接著，Messaging Security Agent 將比較垃圾郵件分數以及使用者定義的垃圾郵件偵測等級。如果垃圾郵件分數超過偵測等級，代理程式將對垃圾郵件採取處理行動。

例如：垃圾郵件的寄件人經常會在電子郵件中使用許多驚嘆號或連續多個驚嘆號 (!!!!)。因此，Messaging Security Agent 偵測到包含此類驚嘆號的訊息，會提高電子郵件的垃圾郵件分數。

秘訣

除了使用「垃圾郵件防護」篩選垃圾郵件之外，還可以設定「內容過濾」過濾郵件標頭、主旨、內文和附件資訊，以濾除垃圾郵件和其他不要的內容。

使用者無法修改「垃圾郵件防護引擎」用來指定垃圾郵件分數的方法，不過可以調整 Messaging Security Agent 判別垃圾郵件的偵測等級。

注意

Microsoft Outlook 可能會自動過濾 Messaging Security Agent 偵測為垃圾郵件的郵件，並將其傳送至「垃圾郵件」資料夾。

電子郵件信譽評等服務

「電子郵件信譽評等服務」技術會根據原始郵件傳輸代理程式 (MTA) 的信譽來判斷垃圾郵件。這會從 Security Server 卸載工作。藉由啟動「電子郵件信譽評等服務」，所有的入站 SMTP 流量都會經由 IP 資料庫檢查，以查看原始 IP 位址是否沒問題，或者該位址已列入已知垃圾郵件傳染媒介的名單中。

有兩種服務等級可用於「電子郵件信譽評等服務」。如下所示：

- 標準：「標準」服務會使用資料庫，追蹤大約二十億個 IP 位址的信譽。始終與垃圾郵件遞送有關的 IP 位址，均已新增至資料庫且甚少移除。
- 進階：「進階」服務等級是以查詢 DNS 為基礎且類似「標準」服務的服務。此服務的核心是標準信譽資料庫，以及動態信譽、即時資料庫，封鎖來自已知和可疑垃圾郵件來源的郵件。

發現來自被封鎖的或可疑 IP 位址的電子郵件時，「電子郵件信譽評等服務」(ERS) 會在郵件到達您的通訊基礎架構之前，先加以停止。

設定電子郵件信譽評等服務

設定「電子郵件信譽評等服務」，以封鎖來自已知或可疑垃圾郵件來源的郵件。此外，建立例外以允許或封鎖來自其他寄件人的郵件。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。

4. 按一下「垃圾郵件防護 > 電子郵件信譽評等服務」。

   隨即顯示新畫面。

5. 從「目標」標籤，視需要更新下列項目：

   - 啟動即時垃圾郵件防護（電子郵件信譽評等服務）
   - 服務等級：
     - 標準
     - 進階
   - 核可的 IP 位址：來自這些 IP 位址的電子郵件永遠不會遭到封鎖。輸入要核可的 IP 位址，然後按一下「新增」。如果需要，您可以從文字檔案匯入 IP 位址的清單。如果要移除 IP 位址，請選取該位址，然後按一下「移除」。
   - 封鎖的 IP 位址：來自這些 IP 位址的電子郵件一律都會遭到封鎖。輸入要封鎖的 IP 位址，然後按一下「新增」。如果需要，您可以從文字檔案匯入 IP 位址的清單。如果要移除 IP 位址，請選取該位址，然後按一下「移除」。

6. 按一下「儲存」。

7. 移至：http://ers.trendmicro.com/ 以檢視報告。

注意

「電子郵件信譽評等服務」是 Web-based 服務。系統管理員僅可從 Web 主控台設定服務等級。

內容掃瞄

「內容掃瞄」會根據郵件內容（而非原始 IP）來辨識垃圾郵件。Messaging Security Agent 會使用趨勢科技的垃圾郵件防護引擎和垃圾郵件病毒碼檔案，在將電子郵件傳遞至「資訊儲存區」之前，先對每封電子郵件進行垃圾郵件篩選。Microsoft Exchange Server 將不會處理遭拒的垃圾郵件，而且郵件最終不會到達使用者信箱。

注意

請勿混淆「內容掃瞄」（根據特徵和自動邏輯分析來執行垃圾郵件防護）與「內容過濾」（根據分類關鍵字來執行電子郵件掃瞄和封鎖）。請參閱內容過濾 第 6-14 頁。

設定內容掃瞄

Messaging Security Agent 會即時偵測垃圾郵件，並執行保護 Microsoft Exchange 用戶端的處理行動。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「垃圾郵件防護 > 內容掃瞄」。

   隨即顯示新畫面。
5. 選取「啟動即時垃圾郵件防護」。
6. 選取「目標」標籤，以選取 Messaging Security Agent 篩選垃圾郵件的方法和垃圾郵件偵測率。

   a. 從垃圾郵件偵測率清單中，選取偵測等級：「低」、「中」或「高」。Messaging Security Agent 會使用此比率篩選所有郵件。

      - 高：這是最嚴格的垃圾郵件偵測等級。Messaging Security Agent 將監控所有電子郵件，搜尋可疑的檔案或文字，但發生垃圾郵件誤判的機率也較高。「垃圾郵件誤判」是指被 Messaging Security Agent 過濾為垃圾郵件的電子郵件，然而這些郵件其實是合法的電子郵件。

- 中：這是預設和建議的設定。Messaging Security Agent 監控時採用的垃圾郵件偵測等級為高，但發生垃圾郵件誤判的機會為中等。
- 低：這是最寬鬆的垃圾郵件偵測等級。Messaging Security Agent 將只過濾最明顯和常見的垃圾郵件，因過濾產生垃圾郵件誤判的機會也相對減低。依據垃圾郵件分數過濾。

b. 按一下「偵測網路釣魚事件」，使 Messaging Security Agent 篩選掉網路釣魚事件。如需詳細資訊，請參閱網路釣魚事件 第 1-10 頁。

c. 新增地址到「核可的寄件人」清單和「封鎖的寄件人」清單。如需詳細資訊，請參閱核可和封鎖的寄件人清單 第 6-11 頁。

- 核可的寄件人：來自這些信箱或網域名稱的電子郵件永遠都不會遭到封鎖。輸入要核可的信箱或網域名稱，然後按一下「新增」。如果需要，您可以從文字檔案匯入信箱或網域名稱的清單。如果要移除信箱或網域名稱，可選取該信箱並按一下移除。
- 封鎖的寄件人：來自這些信箱或網域名稱的電子郵件一律會遭到封鎖。輸入要封鎖的信箱或網域名稱，然後按一下「新增」。如果需要，您可以從文字檔案匯入信箱或網域名稱的清單。如果要移除信箱或網域名稱，可選取該信箱並按一下移除。

注意

Microsoft Exchange 系統管理員會對 Microsoft Exchange Server 維護一份單獨的核可及封鎖的寄件人清單。如果使用者核可的寄件人被管理員列入「封鎖的寄件人清單」，Messaging Security Agent 即會將來自該封鎖寄件人的郵件偵測為垃圾郵件，並對其採取處理行動。

7. 按一下「處理行動」標籤，設定 Messaging Security Agent 偵測到垃圾郵件或網路釣魚事件時所執行的處理行動。

注意

如需有關處理行動的詳細資訊，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁。

Messaging Security Agent 會依據您的組態執行下列其中一項處理行動：

- 將郵件隔離到伺服器端的垃圾郵件資料夾
- 將郵件隔離到使用者的垃圾郵件資料夾

注意

如果您選擇此處理行動，請設定「終端使用者隔離」。如需詳細資訊，請參閱設定垃圾郵件維護 第 6-63 頁。

- 刪除整封郵件
- 加上標記並傳送

8. 按一下「儲存」。

核可和封鎖的寄件人清單

「核可的寄件人」清單就是受信任的電子郵件信箱清單。Messaging Security Agent 不會將這些信箱所傳送的郵件過濾為垃圾郵件，但啟動「偵測網路釣魚事件」時例外。啟動「偵測網路釣魚事件」時，如果代理程式偵測到電子郵件中有網路釣魚事件，那麼即使該電子郵件屬於核可的寄件人清單，也不會傳送這封電子郵件。「封鎖的寄件人」清單就是可疑的電子郵件信箱清單。代理程式永遠將封鎖的寄件人所寄的郵件分類為垃圾郵件，並執行適當的處理行動。

「核可的寄件人」清單有兩種：一種適用於 Microsoft Exchange 系統管理員，另一種適用於終端使用者。

- Microsoft Exchange 管理員的「核可的寄件人」清單和「封鎖的寄件人」清單（在垃圾郵件防護畫面上）控制 Messaging Security Agent 如何處理送往 Microsoft Exchange Server 的電子郵件。
- 終端使用者僅需管理垃圾郵件資料夾，此資料夾是在安裝時建立的。終端使用者的清單只會影響送往每位個別終端使用者的伺服器端信箱儲存區的郵件。

一般指導方針

- Microsoft Exchange Server 上的「核可的寄件人」清單和「封鎖的寄件人」清單會覆寫用戶端上的「核可的寄件人」清單和「封鎖的寄件人」清單。例如，寄件人 user@example.com 位於管理員的「封鎖的寄件人」清

單上，但終端使用者將該信箱新增至其「核可的寄件人」清單中。來自該寄件人的郵件到達 Microsoft Exchange 儲存區，而 Messaging Security Agent 偵測出這些是垃圾郵件，並對這些郵件採取處理行動。如果代理程式採取將郵件「隔離」到使用者垃圾郵件資料夾的處理行動，將會嘗試將郵件傳送到終端使用者的「垃圾郵件」資料夾，但是因為終端使用者已核可該寄件人，所有郵件將會重新導向終端使用者的收件匣。

- 如果您使用的是 Outlook，清單中信箱的數量和大小會有大小限制。為了避免發生系統錯誤，Messaging Security Agent 會限制使用者的核可的寄件人清單中可以包含的地址數量（根據電子郵件信箱的長度和數目計算此限制）。

萬用字元比對

Messaging Security Agent 支援「核可的寄件人」和「封鎖的寄件人」清單的萬用字元比對。使用星號 (*) 做為萬用字元。

Messaging Security Agent 不支援使用者名稱部分的萬用字元比對。但是，如果輸入 *@trend.com 這樣的形式，代理程式還是會視為 @trend.com。

萬用字元只能用於下列情況：

- 旁邊僅接著一個句點，並做為字串的第一個或最後一個字元
- 位於 @ 符號的左邊，並做為字串第一個字元
- 做為功能與萬用字元相同的字串的遺失區段，並位於此字串開頭或結尾

表 6-2. 符合萬用字元的電子郵件地址

病毒碼	符合的範例	不符合的範例
john@example.com	john@example.com	與格式不相同的任何信箱
@example.com *@example.com	john@example.com mary@example.com	john@ms1.example.com john@example.com.us mary@example.com.us

病毒碼	符合的範例	不符合的範例
example.com	john@example.com john@ms1.example.com mary@ms1.rd.example.com mary@example.com	john@example.com.us mary@myexample.com.us joe@example.comon
*.example.com	john@ms1.example.com mary@ms1.rd.example.com joe@ms1.example.com	john@example.com john@myexample.com.us mary@ms1.example.comon
example.com.*	john@example.com.us john@ms1.example.com.us john@ms1.rd.example.com.us mary@example.com.us	john@example.com mary@ms1.example.com john@myexample.com.us
.example.com.	john@ms1.example.com.us john@ms1.rd.example.com.us mary@ms1.example.com.us	john@example.com john@ms1.example.com john@trend.example.us
..*.example.com *****.example.com	與「*.example.com」相同	
example.com example.com example.*.com @*.example.com	無效的格式	

內容過濾

「內容過濾」會根據使用者定義的規則，評估入站和出站的電子郵件。每個規則包含一份關鍵字和片語清單。內容過濾會比較郵件與關鍵字清單，評估郵件的標頭和（或）內容。當內容過濾發現與關鍵字相符的字時，可以採取處理行動以防止不受歡迎的內容傳送到 Microsoft Exchange 用戶端。Messaging Security Agent 對不受歡迎的內容執行處理行動時，可以一併傳送通知。

注意

請勿混淆「內容掃瞄」（根據特徵和自動邏輯分析來執行垃圾郵件防護）與「內容過濾」（根據分類關鍵字來執行電子郵件掃瞄和封鎖）。請參閱內容掃瞄 第 6-8 頁。

系統管理員可以根據郵件的文字，使用內容過濾評估和控制電子郵件傳送。還可以監控入站和出站郵件，檢查郵件中是否存在騷擾、攻擊或其他令人不悅的內容。內容過濾也具備同義字檢查功能，可讓您擴大策略的適用範圍。例如，您可以建立下列檢查規則：

- 性騷擾語言
- 種族歧視語言
- 電子郵件內文中嵌入的垃圾郵件

注意

依預設，不會啟動內容過濾。

管理內容過濾規則

Messaging Security Agent 會在「內容過濾」畫面中顯示所有內容過濾規則。若要存取此畫面，請瀏覽至以下項目：

- 即時掃瞄：

  裝置 > {Messaging Security Agent} > 設定策略 > 內容過濾

- 手動掃瞄：

  掃瞄 > 手動 > {展開 Messaging Security Agent} > 內容過濾

- 預約掃瞄：

  掃瞄 > 預約 > {展開 Messaging Security Agent} > 內容過濾

步驟

1. 檢視規則的摘要資訊，包括：
   - 規則：Worry-Free Business Security 隨附預設規則，會根據以下類別過濾內容：褻瀆言語、種族歧視、性別歧視、惡作劇和連鎖郵件。依預設會關閉這些規則。您可以根據自己的需求，修改或刪除這些規則。如果這些規則均不符合需求，您可以自行新增規則。
   - 處理行動：Messaging Security Agent 會在偵測到不想要的內容時執行此處理行動。
   - 優先順序：Messaging Security Agent 將根據本頁顯示的順序，依序套用各個過濾器。
   - 已啟動：綠色圖示表示已啟動的規則，而紅色圖示表示關閉的規則。
2. 執行下列工作：

工作	步驟
啟動/關閉「內容過濾」	在畫面上方，選取或清除「啟動即時內容過濾」。
新增規則	按一下「新增」。 接著會開啟一個新畫面，您可在此處選擇要新增的規則類型。如需詳細資訊，請參閱內容過濾規則的類型 第 6-18 頁。

工作	步驟
修改規則	a. 按一下規則名稱。 接著會開啟一個新畫面。 b. 畫面中可用的選項取決於規則類型。若要確定規則的類型，可查看畫面上方的導覽列，並記下導覽列中的第二個項目。例如： 內容過濾 >符合任何條件規則 > 編輯規則 如需有關您可以修改的規則設定的詳細資訊，請參閱下列主題： • 新增任何符合條件的內容過濾規則 第 6-21 頁 • 新增符合所有條件的內容過濾規則 第 6-19 頁 注意 手動和預約內容過濾掃瞄中沒有這個規則類型。 • 新增內容過濾監控規則 第 6-24 頁 • 建立內容過濾規則例外 第 6-26 頁

工作	步驟
重新排列規則順序	Messaging Security Agent 會根據「內容過濾」畫面中顯示的順序，套用內容過濾規則到電子郵件。設定規則的套用順序。代理程式會根據每個規則過濾所有電子郵件，直到內容違規事件觸發會阻止再繼續掃瞄的處理行動（例如，刪除或隔離）為止。變更這些規則的順序，以便將內容過濾最佳化。 a. 選取對應至您要變更其順序的規則的核取方塊。 b. 按一下「重新排列順序」。 規則的順序編號旁會出現一個方塊。 c. 在「優先順序」欄方塊中，刪除現有的順序編號並輸入新編號。 注意 請勿輸入大於清單中規則總數的數字。如果輸入大於規則總數的數字，Worry-Free Business Security 會略過此次輸入，不會變更該規則的順序。 d. 按一下「儲存重新排列順序」。 規則會移動到您輸入的優先順序層級，而且所有其他規則編號會對應地變更。 例如，如果您選取規則編號 5，並將它變更為規則編號 3，則規則編號 1 和 2 會維持不變，而規則編號 3 和更大的編號會增加一個編號。
啟動/關閉規則	按一下「已啟動」欄下的圖示。
移除規則	當您刪除規則時，Messaging Security Agent 會更新其他規則的順序，以反映變更。 注意 刪除規則是無法回復的動作，請考慮以關閉規則代替刪除。 a. 選取某個規則。 b. 按一下「移除」。

3. 按一下「儲存」。

內容過濾規則的類型

您可以根據指定條件或是寄件人或收件人的電子郵件信箱，建立規則以過濾電子郵件。可以指定的規則條件包括：要掃瞄的標題欄位、是否要搜尋電子郵件的內文、以及要搜尋的關鍵字。

您可以建立規則，以執行下列作業：

- 過濾符合任何定義條件的郵件：這種規則類型能夠在掃瞄期間過濾任何郵件的內容。如需詳細資訊，請參閱新增任何符合條件的內容過濾規則 第 6-21 頁。
- 過濾符合所有定義條件的郵件：這種規則類型能夠在掃瞄期間過濾任何郵件的內容。如需詳細資訊，請參閱新增符合所有條件的內容過濾規則 第 6-19 頁。

  注意

  手動和預約內容過濾掃瞄中沒有這個規則類型。

- 監控特定電子郵件帳號的郵件內容：這種規則類型可監控特定電子郵件帳號的郵件內容。監控規則與一般內容過濾規則類似，但是只會過濾指定電子郵件帳號的內容。如需詳細資訊，請參閱新增內容過濾監控規則 第 6-24 頁。
- 建立要排除的特定電子郵件帳號：這種類型的規則會建立要排除的特定電子郵件帳號。當您排除特定的電子郵件帳號時，該帳號就不會因為違反內容規則而遭到過濾。如需詳細資訊，請參閱建立內容過濾規則例外 第 6-26 頁。

規則建立完成後，Messaging Security Agent 會開始根據此規則過濾所有輸入和輸出的郵件。如果發生內容違規事件，Messaging Security Agent 會對違規的電子郵件執行處理行動。Security Server 執行的處理行動也會根據規則中設定的處理行動。

新增符合所有條件的內容過濾規則

手動和預約內容過濾掃瞄中沒有這個規則類型。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「內容過濾」。

   隨即顯示新畫面。
5. 按一下「新增」。

   隨即顯示新畫面。
6. 選取「過濾符合所有定義條件的郵件」。
7. 按一下「下一步」。
8. 在「規則名稱」欄位內輸入規則名稱。
9. 選取要過濾不需要內容的郵件部分。Messaging Security Agent 可以依據以下條件過濾電子郵件：
   - 標頭（寄件人、收件人、副本）
   - 主旨
   - 郵件內文或附件的大小
   - 附件檔案名稱

注意

Messaging Security Agent 只在即時掃瞄時支援過濾標題和主旨內容。

10. 按一下「下一步」。
11. 選取 Messaging Security Agent 偵測到不受歡迎的內容時要執行的處理行動。Messaging Security Agent 可以執行下列處理行動（如需說明，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁）：
    - 以文字/檔案取代

      注意

      您無法取代「寄件人」、「收件人」、「副本」或「主旨」欄位中的文字。

    - 隔離整個郵件
    - 隔離郵件部分
    - 刪除整封郵件
    - 封存
    - 暫不處理整封郵件
12. 選取「通知收件者」，設定 Messaging Security Agent 通知內容被過濾之電子郵件的預定收件者。

    選取「不通知外部收件者」，只傳送通知給內部郵件收件者。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。
13. 選取通知寄件人，設定 Messaging Security Agent 通知內容被過濾之電子郵件的寄件人。

    選取不通知外部寄件人，只傳送通知給內部郵件寄件人。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。
14. 在「進階選項」區段中，按一下加號 (+) 圖示展開「封存設定」子區段。
    a. 在「隔離目錄」欄位中，輸入「內容過濾」用來放置已隔離的電子郵件的資料夾路徑，或接受預設值：`<Messaging Security Agent 安裝資料夾>\storage\quarantine`
    b. 在「封存目錄」欄位中，輸入「內容過濾」用來放置已封存的電子郵件的資料夾路徑，或接受預設值：`<Messaging Security Agent 安裝資料夾>\storage\backup for content filter`

15. 按一下加號 (+) 圖示以展開「取代設定」子區段。

    a. 在「取代檔案名稱」欄位中，輸入當觸發使用「以文字/檔案取代」處理行動的規則時，「內容過濾」將用來取代電子郵件的檔案的名稱，或接受預設值。

    b. 在「取代文字」欄位中輸入或貼上取代文字內容，供「內容過濾」在電子郵件觸發處理行動為「以文字/檔案取代」的規則時使用，或接受預設文字。

16. 按一下「完成」。

    精靈會關閉並返回「內容過濾」畫面。

新增任何符合條件的內容過濾規則

- 即時掃瞄：

  裝置 > {Messaging Security Agent} > 設定策略 > 內容過濾

- 手動掃瞄：

  掃瞄 > 手動 > {展開 Messaging Security Agent} > 內容過濾

- 預約掃瞄：

  掃瞄 > 預約 > {展開 Messaging Security Agent} > 內容過濾

步驟

1. 按一下「新增」。

   隨即顯示新畫面。

2. 選取「過濾符合任何定義條件的郵件」。

3. 按一下「下一步」。

4. 在「規則名稱」欄位內輸入規則名稱。

5. 選取要過濾不需要內容的郵件部分。Messaging Security Agent 可以依據以下條件過濾電子郵件：
   - 標頭（寄件人、收件人、副本）
   - 主旨
   - 內文
   - 附件

   注意
   Messaging Security Agent 只在即時掃瞄時支援過濾標題和主旨內容。

6. 按一下「下一步」。
7. 新增要過濾掉不當內容的目標部分時所使用的關鍵字。如需有關使用關鍵字的詳細資訊，請參閱關鍵字 第 D-4 頁。
   a. 如有需要，您可以選取內容過濾是否要區分大小寫。
   b. 視需要從 `.txt` 檔案匯入新的關鍵字檔案。
   c. 定義同義字清單。
8. 按一下「下一步」。
9. 選取 Messaging Security Agent 偵測到不受歡迎的內容時要執行的處理行動。Messaging Security Agent 可以執行下列處理行動（如需說明，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁）：
   - 以文字/檔案取代

     注意
     您無法取代「寄件人」、「收件人」、「副本」或「主旨」欄位中的文字。

   - 隔離整個郵件
   - 隔離郵件部分

- 刪除整封郵件
- 封存

10. 選取「通知收件者」，設定 Messaging Security Agent 通知內容被過濾之電子郵件的預定收件者。

    選取「不通知外部收件者」，只傳送通知給內部郵件收件者。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

11. 選取通知寄件人，設定 Messaging Security Agent 通知內容被過濾之電子郵件的寄件人。

    選取不通知外部寄件人，只傳送通知給內部郵件寄件人。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

12. 在「進階選項」區段中，按一下加號 (+) 圖示展開「封存設定」子區段。

    a. 在「隔離目錄」欄位中，輸入「內容過濾」用來放置已隔離的電子郵件的資料夾路徑，或接受預設值：`<Messaging Security Agent 安裝資料夾>\storage\quarantine`

    b. 在「封存目錄」欄位中，輸入「內容過濾」用來放置已封存的電子郵件的資料夾路徑，或接受預設值：`<Messaging Security Agent 安裝資料夾>\storage\backup for content filter`

13. 按一下加號 (+) 圖示以展開「取代設定」子區段。

    a. 在「取代檔案名稱」欄位中，輸入當觸發使用「以文字/檔案取代」處理行動的規則時，「內容過濾」將用來取代電子郵件的檔案的名稱，或接受預設值。

    b. 在「取代文字」欄位中輸入或貼上取代文字內容，供「內容過濾」在電子郵件觸發處理行動為「以文字/檔案取代」的規則時使用，或接受預設文字。

14. 按一下「完成」。

    精靈會關閉並返回「內容過濾」畫面。

新增內容過濾監控規則

- 即時掃瞄：

  裝置 > {Messaging Security Agent} > 設定策略 > 內容過濾

- 手動掃瞄：

  掃瞄 > 手動 > {展開 Messaging Security Agent} > 內容過濾

- 預約掃瞄：

  掃瞄 > 預約 > {展開 Messaging Security Agent} > 內容過濾

步驟

1. 按一下「新增」。

   隨即顯示新畫面。

2. 選取「監控特定電子郵件帳號的郵件內容」。
3. 按一下「下一步」。
4. 在「規則名稱」欄位內輸入規則名稱。
5. 設定要監控的電子郵件帳號。
6. 按一下「下一步」。
7. 選取要過濾不需要內容的郵件部分。Messaging Security Agent 可以依據以下條件過濾電子郵件：

   - 主旨
   - 內文
   - 附件

   注意

   Messaging Security Agent 只在即時掃瞄時支援過濾電子郵件的這些部分。手動和預約掃瞄時不支援過濾標頭和主旨內容。

8. 新增要過濾掉不當內容的目標部分時所使用的關鍵字。如需有關使用關鍵字的詳細資訊，請參閱關鍵字 第 D-4 頁。

   a. 如有需要，您可以選取內容過濾是否要區分大小寫。

   b. 視需要從 `.txt` 檔案匯入新的關鍵字檔案。

   c. 定義同義字清單。

9. 按一下「下一步」。

10. 選取 Messaging Security Agent 偵測到不受歡迎的內容時要執行的處理行動。Messaging Security Agent 可以執行下列處理行動（如需說明，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁）：

    - 以文字/檔案取代

      注意

      您無法取代「寄件人」、「收件人」、「副本」或「主旨」欄位中的文字。

    - 隔離整個郵件
    - 隔離郵件部分
    - 刪除整封郵件
    - 封存

11. 選取「通知收件者」，設定 Messaging Security Agent 通知內容被過濾之電子郵件的預定收件者。

    選取「不通知外部收件者」，只傳送通知給內部郵件收件者。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

12. 選取通知寄件人，設定 Messaging Security Agent 通知內容被過濾之電子郵件的寄件人。

    選取不通知外部寄件人，只傳送通知給內部郵件寄件人。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

13. 在「進階選項」區段中，按一下加號 (+) 圖示展開「封存設定」子區段。

a. 在「隔離目錄」欄位中，輸入「內容過濾」用來放置已隔離的電子郵件的資料夾路徑，或接受預設值：<Messaging Security Agent 安裝資料夾>\storage\quarantine

b. 在「封存目錄」欄位中，輸入「內容過濾」用來放置已封存的電子郵件的資料夾路徑，或接受預設值：<Messaging Security Agent 安裝資料夾>\storage\backup for content filter

14. 按一下加號 (+) 圖示以展開「取代設定」子區段。

a. 在「取代檔案名稱」欄位中，輸入當觸發使用「以文字/檔案取代」處理行動的規則時，「內容過濾」將用來取代電子郵件的檔案的名稱，或接受預設值。

b. 在「取代文字」欄位中輸入或貼上取代文字內容，供「內容過濾」在電子郵件觸發處理行動為「以文字/檔案取代」的規則時使用，或接受預設文字。

15. 按一下「完成」。

精靈會關閉並返回「內容過濾」畫面。

建立內容過濾規則例外

- 即時掃瞄：

  裝置 > {Messaging Security Agent} > 設定策略 > 內容過濾

- 手動掃瞄：

  掃瞄 > 手動 > {展開 Messaging Security Agent} > 內容過濾

- 預約掃瞄：

  掃瞄 > 預約 > {展開 Messaging Security Agent} > 內容過濾

步驟

1. 按一下「新增」。

隨即顯示新畫面。

2. 選取「建立要排除特定的電子郵件帳號」。
3. 按一下「下一步」。
4. 輸入規則名稱。
5. 在提供的空格內，輸入要從內容過濾排除的電子郵件信箱，然後按一下「新增」。

   該電子郵件信箱會新增至排除的電子郵件信箱清單中。Messaging Security Agent 不會將優先順序低於這個規則的內容規則，套用到此清單中的電子郵件帳號。
6. 確認電子郵件帳號清單無誤後，按一下「完成」。

   精靈會關閉並返回「內容過濾」畫面。

資料遺失防範

使用「資料遺失防範」來防範資料經由外寄郵件遺失。此功能可保護符合設定樣式的資料，例如：身分證號碼、電話號碼、銀行帳號和其他機密商業資訊。

此版本支援下列 Microsoft Exchange 版本：

表 6-3. 支援的 Microsoft Exchange 版本

支援	不支援
2007 x64	2003 x86/x64
2010 x64	2007 x86
	2010 x86

準備工作

監控機密資料是否可能發生遺失情形時，請決定下列項目：

- 必須保護哪些資料以避免未經授權的使用者存取
- 資料位於何處
- 資料透過那種管道、以何種方式傳輸
- 哪些使用者被授權存取或傳輸此資訊

這個重要的稽核通常需要由多個部門提供意見，而且需要公司中熟悉機密資訊的人員協助。下列程序假設您已識別機密資訊，而且已建立有關處理機密商業資訊的安全策略。

「資料遺失防範」功能由三個基本元件組成：

- 規則（要搜尋的樣式）
- 過濾時要排除的網域：
- 核可的寄件人（過濾時要排除的電子郵件帳號）

如需詳細資訊，請參閱管理「資料遺失防範」規則 第 6-28 頁。

管理「資料遺失防範」規則

Messaging Security Agent 會在「資料遺失防範」畫面上（「裝置 > {Messaging Security Agent} > 設定策略 > 資料遺失防範」）顯示所有「資料遺失防範」規則。

步驟

1. 檢視規則的摘要資訊，包括：
   - 規則：Worry-Free Business Security 隨附預設規則（請參閱預設「資料遺失防範」規則 第 6-35 頁）。依預設會關閉這些規則。您可以根據自己的需求，修改或刪除這些規則。如果這些規則均不符合需求，您可以自行新增規則。

秘訣

將滑鼠游標移至規則名稱上，即可檢視規則。系統會使用放大鏡 ( ) 圖示來標示使用一般表示式的規則。

- 處理行動：觸發規則時，Messaging Security Agent 會執行此處理行動。
- 優先順序：Messaging Security Agent 將根據本頁顯示的順序，依序套用各個規則。
- 已啟動：綠色圖示表示已啟動的規則，而紅色圖示表示關閉的規則。

2. 執行下列工作：

工作	步驟
啟動/關閉「資料遺失防範」	在畫面上方，選取或清除「啟動即時資料遺失防範」。
新增規則	按一下「新增」。 接著會開啟一個新畫面，您可在此處選擇要新增的規則類型。如需詳細資訊，請參閱新增「資料遺失防範」規則 第 6-36 頁。
修改規則	按一下規則名稱。 接著會開啟一個新畫面。如需有關您可以修改的規則設定的詳細資訊，請參閱新增「資料遺失防範」規則 第 6-36 頁。

工作	步驟
匯入和匯出規則	從純文字檔匯入一或多個規則（或將規則匯出至純文字檔），如下所示。您也可以使用此檔案來直接編輯規則。 [SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599] RuleName=Bubbly UserExample= Value=Bubbly [SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6] RuleName=Master Card No. UserExample=Value=.REG.\b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
	若要將規則匯出至純文字檔，在清單中選取一或多個規則，然後按一下「匯出」。 **秘訣** 您只能選取一個畫面上顯示的規則。如果要選取目前顯示在其他畫面上的規則，請增加位於「規則」清單表格頂端的「每頁列數」值，以顯示足夠的列數，讓一個畫面可顯示您要匯出的所有規則。

工作	步驟
	若要匯入規則： a. 建立格式如上的純文字檔。您也可以按一下表格下方的「下載更多預設規則」，然後儲存規則。 b. 按一下「匯入」。 此時會開啟新視窗。 c. 按一下「瀏覽」並找到要匯入的檔案，然後按一下「匯入」。 「資料遺失防範」會匯入檔案中的規則，然後附加到目前規則清單結尾。 **秘訣** 如果已經有超過 10 個規則，第一頁將不會顯示匯入的規則。使用規則清單頂端或底端的頁面瀏覽圖示來顯示清單的最後一頁。新匯入的規則應該位於該處。

工作	步驟
重新排列規則順序	Messaging Security Agent 會根據「資料遺失防範」畫面中顯示的順序，套用 Data Loss Prevention 規則到電子郵件。設定規則的套用順序。代理程式會根據每個規則過濾所有電子郵件，直到內容違規事件觸發會阻止再繼續掃瞄的處理行動（例如，刪除或隔離）為止。變更這些規則的順序，以便將「資料遺失防範」最佳化。 a. 選取對應至您要變更其順序的規則的核取方塊。 b. 按一下「重新排列順序」。 規則的順序編號旁會出現一個方塊。 c. 在「優先順序」欄方塊中，刪除現有的順序編號並輸入新編號。 注意 請勿輸入大於清單中規則總數的數字。如果輸入大於規則總數的數字，Worry-Free Business Security 會略過此次輸入，不會變更該規則的順序。 d. 按一下「儲存重新排列順序」。 規則會移動到您輸入的優先順序層級，而且所有其他規則編號會對應地變更。 例如，如果您選取規則編號 5，並將它變更為規則編號 3，則規則編號 1 和 2 會維持不變，而規則編號 3 和更大的編號會增加一個編號。
啟動/關閉規則	按一下「已啟動」欄下的圖示。

工作	步驟
移除規則	當您刪除規則時，Messaging Security Agent 會更新其他規則的順序，以反映變更。 **注意** 刪除規則是無法回復的動作，請考慮以關閉規則代替刪除。 a. 選取某個規則。 b. 按一下「移除」。
排除特定的網域帳號	在公司中，機密商業資訊的交換是日常作業的一部分。此外，如果「資料遺失防範」必須過濾所有內部郵件，則 Security Server 伺服器的處理負載會很高。因為這些原因，您需要設定一或多個預設網域（代表公司的內部郵件流量），這樣「資料遺失防範」才不會過濾從公司網域中的某個電子郵件帳號傳送到另一個電子郵件帳號的郵件。 這個清單會列出所有要略過「資料遺失防範」規則的內部電子郵件（公司網域內）。至少必須輸入一個此類網域。如果使用多個網域，請新增到此清單。 例如：`*@example.com` a. 按一下加號 (+) 圖示以展開「從資料遺失防範排除的特定網域帳號」區段。 b. 將游標放在「新增」欄位，然後使用下列樣式輸入網域：`*@example.com` c. 按一下「新增」。 該網域會出現在「新增」欄位下顯示的清單中。 d. 按一下「儲存」以完成此程序。 **警告!** 在您按下「儲存」之前，「資料遺失防範」不會新增您輸入的網域。如果按下「新增」但並未按下「儲存」，系統不會新增您輸入的網域。

工作	步驟
新增電子郵件帳號至「核可的寄件人清單」	來自核可的寄件人的郵件可不經由「資料遺失防範」過濾直接傳送出您的網路。「資料遺失防範」將略過從例外清單上的電子郵件帳號寄出的任何郵件內容。 a. 按一下加號 (+) 圖示以展開「核可的寄件人」區段。 b. 將游標放在「新增」欄位，然後使用下列樣式輸入完整的電子郵件信箱：`example@example.com` c. 按一下「新增」。 該信箱會出現在「新增」欄位下顯示的清單中。 d. 按一下「儲存」以完成此程序。 **注意** 在您按下「儲存」之前，「資料遺失防範」不會新增您輸入的信箱。如果按下「新增」但並未按下「儲存」，系統不會新增您輸入的信箱。

匯入電子郵件帳號至「核可的寄件人清單」	您可以從純文字檔案（一行放一個電子郵件信箱）匯入電子郵件信箱清單，例如：
	`admin@example.com`
	`ceo@example.com`
	`president@example.com`
	a. 按一下加號 (+) 圖示以展開「核可的寄件人」區段。
	b. 按一下「匯入」。
	此時會開啟新視窗。
	c. 按一下「瀏覽」並找到要匯入的純文字檔，然後按一下「匯入」。
	「資料遺失防範」會匯入檔案中的規則，然後附加到目前清單結尾。

3. 按一下「儲存」。

預設「資料遺失防範」規則

「資料遺失防範」隨附一些預設規則，如下表所示。

表 6-4. 預設「資料遺失防範」規則

規則名稱	範例	一般表示式
Visa 信用卡號碼	4111-1111-1111-1111	.REG.\b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
MasterCard 信用卡號碼	5111-1111-1111-1111	.REG.\b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
American Express 信用卡號碼	3111-111111-11111	.REG.\b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Diners Club/Carte Blanche 信用卡號碼	3111-111111-1111	.REG.[^\d-]((36\d{2}|38\d{2}|30[0-5]\d)-?\d{6}-?\d{4})[^\d-]
IBAN	BE68 5390 0754 7034、FR14 2004 1010 0505 0001 3M02 606、DK50 0040 0440 1162 43	.REG.[^\w](([A-Z]{2}\d{2}[-|\s]?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}[-|\s]){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}[-|\s]){2}[A-Za-z0-9]{3,4}))[^\w]
Swift BIC	BANK US 99	.REG.[^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
ISO 日期	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG.[^\d\/-]([1-2]\d{3}[-\/][0-1]?\d[-\/][0-3]?\d|\d{2}[-\/][0-1]?\d[-\/][0-3]?\d)[^\d\/-]

注意

可從 Web 主控台下載包含更多 DLP 規則的 ZIP 檔案。瀏覽至「安全設定 > {Messaging Security Agent} > 進行設定 > 資料遺失防範」，然後按一下「下載更多預設規則」。

新增「資料遺失防範」規則

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「資料遺失防範」。

   隨即顯示新畫面。
5. 按一下「新增」。

   隨即顯示新畫面。
6. 選取要評估的郵件部分。Messaging Security Agent 可以依據以下條件過濾電子郵件：
   - 標頭（寄件人、收件人、副本）
   - 主旨
   - 內文
   - 附件
7. 新增規則。

   如果要根據關鍵字新增規則：

   a. 選取「關鍵字」。

   b. 在顯示的欄位內輸入關鍵字。關鍵字長度必須介於 1 到 64 個英數字元之間。

   c. 按一下「下一步」。

   如果要根據自動產生的表示式新增規則：

a. 請參閱一般表示式 第 D-8 頁取得有關定義一般表示式的指導方針。

b. 選取「一般表示式（自動產生）」。

c. 在提供的欄位中輸入「規則名稱」。此為必要欄位。

d. 在「範例」欄位中輸入或貼上類型為字串的範例（長度不能超過 40 個字元），供一般表示式用來比對。「範例」欄位下的陰影區域中有一排方塊，英數字元會在該區域中以全部大寫的方式顯示。

e. 如果表示式中有任何常數，請按一下字元顯示所在的方塊選取那些常數。

   按一下每個方塊之後，其框線會變成紅色以指出它是常數，而且自動產生工具會修改陰影區域下顯示的一般表示式。

   注意

   非英數字元（例如：空格、分號和其他標點符號）會被自動視為常數，因此無法自動切換為變數。

f. 若要驗證產生的一般表示式是否符合您想要的樣式，請選取「提供另一個範例以驗證規則（選用）」。

   此選項下方會出現一個測試欄位。

g. 輸入您剛輸入的樣式的另一個範例。

   例如，如果此表示式是要比對樣式為「01-EX?????20??」的一系列帳號，請輸入另一個符合的範例（例如「01-Extreme 2010」），然後按一下「測試」。

   工具會根據現有的一般表示式驗證新的範例，並在新範例符合時在該欄位旁顯示綠色核取記號圖示。如果一般表示式不符合新範例，則該欄位旁會出現紅色的 X 圖示。

   警告!

   使用此工具建立的一般表示式不區分大小寫。這些表示式只能用來比對字元數與您的樣本完全相同的樣式，而無法評估「一或多個」指定字元的樣式。

h. 按一下「下一步」。

如果要根據使用者定義的表示式新增規則：

警告!

一般表示式是強大的字串比對工具。使用這些表示式之前，請確定您已熟悉一般表示式語法。寫得不好的一般表示式會大幅影響效能。趨勢科技建議您從簡單的一般表示式開始。在建立新規則時，請先使用「封存」處理行動，並觀察「資料遺失防範」如何使用該規則來管理郵件。當您有把握規則不會產生無法預期的結果時，才可以變更處理行動。

a. 請參閱一般表示式 第 D-8 頁取得有關定義一般表示式的指導方針。

b. 選取「一般表示式（使用者定義）」。

會顯示「規則名稱」和「一般表示式」欄位。

c. 在提供的欄位中輸入「規則名稱」。此為必要欄位。

d. 在「一般表示式」欄位中輸入一般表示式，其字首為「`.REG.`」，而且長度不能超過 255 個字元（包含字首）。

警告!

將文字貼到此欄位時請特別小心。如果剪貼簿內容包含任何額外的字元（例如：OS 特定的換行符號或 HTML 標記），貼上的表示式將會不正確。因此，趨勢科技建議您手動輸入表示式。

e. 如果要驗證一般表示式是否符合您想要的樣式，請選取「提供另一個範例以驗證規則（選用）」。

此選項下方會出現一個測試欄位。

f. 輸入您剛輸入的樣式的另一個範例（40 個字元以下）。

例如，如果此表示式是要比對樣式為「ACC-?????20??」的一系列帳號，請輸入另一個符合的範例（例如「Acc-65432 2012」），然後按一下「測試」。

工具會根據現有的一般表示式驗證新的範例，並在新範例符合時在該欄位旁顯示綠色核取記號圖示。如果一般表示式不符合新範例，則該欄位旁會出現紅色的 X 圖示。

g. 按一下「下一步」。

8. 選取規則遭到觸發時，Messaging Security Agent 要執行的處理行動（如需說明，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁）：

   - 以文字/檔案取代

     注意

     您無法取代「寄件人」、「收件人」、「副本」或「主旨」欄位中的文字。

   - 隔離整個郵件
   - 隔離郵件部分
   - 刪除整封郵件
   - 封存
   - 暫不處理整封郵件

9. 選取「通知收件者」，設定「資料遺失防範」對特定電子郵件採取處理行動時，Messaging Security Agent 通知預定收件者。

   由於各種原因，封鎖包含機密資訊的郵件時，您可能不想通知外部郵件收件者。選取「不通知外部收件者」，只傳送通知給內部郵件收件者。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

10. 選取通知寄件人，設定 Messaging Security Agent 在 Data Loss Prevention 對特定電子郵件執行處理行動時，通知預定寄件人。

    由於各種原因，封鎖包含機密資訊的郵件時，您可能不想通知外部郵件寄件人。選取不通知外部寄件人，只傳送通知給內部郵件寄件人。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

11. 在「進階選項」區段中，按一下加號 (+) 圖示展開「封存設定」子區段。

    a. 在「隔離目錄」欄位中，輸入「資料遺失防範」用來放置已隔離的電子郵件的資料夾路徑，或接受預設值：`<Messaging Security Agent 安裝資料夾>\storage\quarantine`

b. 在「封存目錄」欄位中，輸入「資料遺失防範」用來放置已封存的電子郵件的資料夾路徑，或接受預設值：`<Messaging Security Agent 安裝資料夾>\storage\backup for content filter`

12. 按一下加號 (+) 圖示以展開「取代設定」子區段。

    a. 在「取代檔案名稱」欄位中，輸入當觸發使用「以文字/檔案取代」處理行動的規則時，「資料遺失防範」將用來取代電子郵件的檔案的名稱，或接受預設值。

    b. 在「取代文字」欄位中輸入或貼上取代文字內容，供「資料遺失防範」在電子郵件觸發處理行動為「以文字/檔案取代」的規則時使用，或接受預設文字。

13. 按一下「完成」。

    精靈會關閉並返回「資料遺失防範」畫面。

附件封鎖

附件封鎖可防止將電子郵件中的附件傳送至 Microsoft Exchange 資訊儲存區。設定 Messaging Security Agent 根據附件類型或附件名稱封鎖附件，然後取代、隔離或刪除含有符合條件之附件的所有郵件。

在「即時掃瞄」、「手動掃瞄」和「預約掃瞄」期間都可以進行封鎖，但是刪除和隔離處理行動不適用於「手動掃瞄」和「預約掃瞄」。

附件的副檔名可以識別檔案類型，例如：`.txt`、`.exe` 或 `.dll`。不過，Messaging Security Agent 是透過檢查檔案標頭（而不是檔名）的方式來確認實際的檔案類型。許多病毒/惡意程式都會與某些檔案類型有密切的關聯。將 Messaging Security Agent 設定成依據檔案類型進行封鎖，可以降低這些檔案類型對 Microsoft Exchange Server 造成的安全威脅。同樣地，特定的攻擊通常也會與特定的檔名有密切關聯。

秘訣

運用封鎖是控制病毒爆發的有效方法。您可以暫時隔離所有高風險的檔案類型，或與已知病毒/惡意程式相關聯的特定名稱檔案。稍後，等您有充裕的時間再來檢查隔離資料夾，並且對中毒檔案執行中毒處理行動。

設定附件封鎖

設定 Microsoft Exchange Server 的附件封鎖選項時，必須設定對含有特定附件的郵件所套用的封鎖規則。

- 即時掃瞄：

  裝置 > {Messaging Security Agent} > 設定策略 > 附件封鎖

- 手動掃瞄：

  掃瞄 > 手動 > {展開 Messaging Security Agent} > 附件封鎖

- 預約掃瞄：

  掃瞄 > 預約 > {展開 Messaging Security Agent} > 附件封鎖

步驟

1. 從「目標」標籤，視需要更新下列項目：
   - 所有附件：代理程式可以封鎖所有含有附件的電子郵件。不過，這種類型的掃瞄會耗用大量處理資源。選取不要封鎖的附件類型或名稱可以改善這種類型的掃瞄。
     - 要排除的附件類型
     - 不掃瞄的附件名稱
   - 特定附件：選取這種掃瞄類型時，代理程式只會掃瞄包含您所確認之附件的電子郵件。這種類型的掃瞄具有高度排除性，適合用來偵測其附件可能感染安全威脅的電子郵件。如果您指定的附件名稱或類型數量不多，這種掃瞄執行起來會非常快速。

- 附件類型：代理程式是透過檢查檔案標頭（而不是檔案名稱）來確認實際的檔案類型。
- 附件名稱：依預設，代理程式是透過檢查檔案標頭（而不是檔案名稱）來確認實際的檔案類型。將「附件封鎖」設定為掃瞄特定名稱時，代理程式會根據名稱偵測附件類型。

- 封鎖 ZIP 檔案內的附件類型或名稱

2. 按一下「處理行動」標籤，設定 Messaging Security Agent 偵測到附件時所執行的處理行動。Messaging Security Agent 可以執行下列處理行動（如需說明，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁）：
   - 以文字/檔案取代
   - 隔離整個郵件
   - 隔離郵件部分
   - 刪除整封郵件
3. 選取「通知收件者」，設定 Messaging Security Agent 通知含有附件之電子郵件的預定收件者。

   選取「不通知外部收件者」，只傳送通知給內部郵件收件者。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。
4. 選取「通知寄件人」，設定 Messaging Security Agent 通知含有附件之電子郵件的寄件人。

   選取不通知外部寄件人，只傳送通知給內部郵件寄件人。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。
5. 按一下加號 (+) 圖示以展開「取代設定」子區段。
   a. 在「取代檔案名稱」欄位中，輸入當觸發使用「以文字/檔案取代」處理行動的規則時，「附件封鎖」將用來取代電子郵件的檔案的名稱，或接受預設值。
   b. 在「取代文字」欄位中輸入或貼上取代文字內容，供「附件封鎖」在電子郵件觸發處理行動為「以文字/檔案取代」的規則時使用，或接受預設文字。

6. 按一下「儲存」。

網頁信譽評等

網頁信譽評等可防止使用者存取具有潛在安全威脅的 Web 上或嵌入電子郵件中的 URL。網頁信譽評等會根據趨勢科技網頁信譽評等伺服器檢查 URL 的信譽，然後將信譽與電腦上實施的特定網頁信譽評等策略關聯。根據所使用的策略：

- Security Agent 將封鎖或允許對網站的存取。
- Messaging Security Agent（僅限 Advanced 版）將隔離、刪除或標記包含惡意 URL 的電子郵件，或允許傳送郵件（如果 URL 是安全的）。

網頁信譽評等可針對相關偵測，為管理員提供電子郵件通知，並對使用者提供線上通知。

在 Security Agent 中，根據用戶端的所在位置（在辦公室中/辦公室以外的地方），設定不同的安全層級。

如果「網頁信譽評等」封鎖了您認為安全無虞的 URL，請將該 URL 新增至核可的 URL 清單中。

秘訣

為了節省網路頻寬，趨勢科技建議您將企業內部網站新增至網頁信譽評等核可的 URL 清單。

信譽評分

URL 的「信譽評分」會決定其是否為網路安全威脅。趨勢科技則使用專有度量來計算分數。

如果 URL 的分數在定義的門檻值內，趨勢科技會將此 URL 視為 Web 安全威脅；如果分數超過該門檻值，則會將此 URL 視為安全的。

Security Agent 有三種安全層級，可決定允許還是封鎖對 URL 的存取。

- 高：封鎖下列網頁：
  - 危險：經驗證為詐騙網頁或已知的威脅來源
  - 非常可疑：懷疑可能是詐騙網頁或可能的威脅來源
  - 可疑：與垃圾郵件相關或可能遭到破壞
  - 未測試的：雖然趨勢科技會主動測試網頁以確保安全，但使用者仍可能會在造訪新的或較不熱門的網站時遇到未測試的網頁。封鎖對於未測試網頁的存取，可以提高安全，但也會讓人無法存取某些安全的網頁。
- 中：封鎖下列網頁：
  - 危險：經驗證為詐騙網頁或已知的威脅來源
  - 非常可疑：懷疑可能是詐騙網頁或可能的威脅來源
- 低：封鎖下列網頁：
  - 危險：經驗證為詐騙網頁或已知的威脅來源

設定 Messaging Security Agent 的網頁信譽評等

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「網頁信譽評等」。

   隨即顯示新畫面。
5. 視需要更新下列項目：
   - 啟動網頁信譽評等

- 安全層級：「高」、「中」或「低」
- 核可的 URL
  - 要核可的 URL：請以分號 (;) 分隔多個 URL。按一下「新增」。

    注意

    核可 URL 包含核可其所有子網域。

    請小心使用萬用字元，這可能會允許大批 URL。
  - 核可的 URL 清單：不會封鎖此清單中的 URL。

6. 按一下「處理行動」標籤，選取網頁信譽評等策略遭到觸發時，Messaging Security Agent 要執行的處理行動（如需說明，請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁）：
   - 以文字/檔案取代

     注意

     您無法取代「寄件人」、「收件人」、「副本」或「主旨」欄位中的文字。
   - 將郵件隔離到使用者的垃圾郵件資料夾
   - 刪除整封郵件
   - 加上標記並傳送
7. 選取「針對尚未由趨勢科技評估的 URL 採取處理行動」，將未分類的 URL 視為可疑。針對包含未分類 URL 的墊子郵件，將會執行和上一步所指定一樣的處理行動。
8. 選取「通知收件者」，設定「網頁信譽評等」對特定電子郵件採取處理行動時，Messaging Security Agent 通知預定收件者。

   由於各種原因，封鎖包含惡意 URL 的郵件時，您可能不想通知外部郵件收件者。選取「不通知外部收件者」，只傳送通知給內部郵件收件者。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

9. 選取通知寄件人，設定 Messaging Security Agent 在「網頁信譽評等」對特定電子郵件執行處理行動時，通知預定寄件人。

   由於各種原因，封鎖包含惡意 URL 的郵件時，您可能不想通知外部郵件寄件人。選取不通知外部寄件人，只傳送通知給內部郵件寄件人。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

10. 按一下「儲存」。

行動安全防護

行動安全防護設定可防止未經授權的裝置存取和下載 Microsoft Exchange Server 的資訊。系統管理員指出允許存取 Microsoft Exchange Server 的裝置，然後指出這些裝置的使用者是否可下載或更新其電子郵件、行事曆、聯絡人或工作。

系統管理員也可以將安全策略套用至裝置。這些策略控制密碼長度和複雜度、在裝置閒置一段時間後是否應將其鎖定、裝置是否需要使用加密，以及在一系列失敗的登入嘗試後是否應清除裝置資料。

行動安全防護支援

表 6-5. 行動裝置支援

作業系統	IIS 版本	裝置資料安全防護策略		存取控制		
		EXCHANGE 2007（或更高版本）64 位元	EXCHANGE 2003 32 位元	EXCHANGE 2010（和更高版本）64 位元	EXCHANGE 2007 64 位元	EXCHANGE 2003 32 位元
• Windows 2008（64 位元） • SBS 2008（64 位元）	7 +	是	不相容	是	否	不相容
Windows 2003（64 位元）	6.0	是	不相容	否	否	不相容
• Windows 2003（32 位元） • SBS 2003（32 位元）	6.0	不相容	否	不相容	不相容	否

表 6-6. 行動裝置作業系統支援

行動作業系統	OS 版本
iOS	3.0 - 6.1 (4.3 - 7.0)
Android	2.2 - 4.2
WM/WP (Windows)	7.0 - 8.0
BB (BlackBerry)	7.0 - 10.1

設定裝置存取控制

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「行動安全防護 > 裝置存取控制」。

   隨即顯示新畫面。
5. 選取「啟動裝置存取控制」。
6. 按一下「新增」。
7. 輸入策略名稱，以及有關策略的說明。
8. 識別裝置擁有者，以選取允許/封鎖哪些裝置存取 Microsoft Exchange Server：
   - 任何人
   - 指定裝置擁有者
9. 如果已選取「指定裝置擁有者」：

a. 輸入裝置擁有者的姓名，然後按一下「搜尋」，在 Microsoft Exchange Server 的全域通訊清單中尋找裝置擁有者。

b. 選取裝置擁有者，然後按一下「新增」。

10. 從「類型」下拉式清單中選取裝置的作業系統（如果已知）。

11. 選取「指定版本號碼範圍」並指明允許該作業系統的哪些版本（如果已知）。

12. 指定 Messaging Security Agent 應允許還是封鎖存取裝置擁有者的郵件、行事曆、聯絡人或工作。

13. 按一下「儲存」。

取消暫停的裝置清除

步驟

1. 移至「裝置」。

2. 選取 Messaging Security Agent。

3. 按一下「設定策略」。

   隨即顯示新畫面。

4. 按一下「行動安全防護 > 裝置清除」。

   隨即顯示新畫面。

5. 在裝置清除表格中找到裝置，然後按一下「取消清除」。

6. 按一下「確定」。

手動清除裝置

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「行動安全防護 > 裝置清除」。

   隨即顯示新畫面。
5. 按一下「選取裝置」。

   隨即顯示新畫面。
6. 輸入裝置擁有者的姓名，然後按一下「搜尋」尋找其裝置。
7. 如果可清除裝置，請選取該裝置，然後按一下「清除」。

   注意

   如果裝置狀態在搜尋後為「清除成功」或「清除已暫停」，則無法選取該裝置。

設定安全策略

Worry-Free Business Security 使用 Microsoft Exchange 預設策略做為預設策略。預設策略會顯示在安全策略清單中。

Worry-Free Business Security 不會保留使用 Microsoft Exchange 管理主控台或 Exchange Cmdlet 新增的非預設策略。

趨勢科技建議管理員從 Worry-Free Business Security 管理主控台或 Microsoft Exchange 管理安全策略。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「行動安全防護 > 安全策略」。

   隨即顯示新畫面。
5. 按一下「新增」。
6. 輸入策略名稱，以及有關策略的說明。
7. 輸入裝置擁有者的姓名，然後按一下「搜尋」，在 Microsoft Exchange Server 的全域通訊清單中尋找裝置擁有者。
8. 選取裝置擁有者，然後按一下「新增」。
9. 選取要套用至裝置的安全條件：
   - 最小密碼長度：如需有關行動裝置密碼的指導方針，請參閱密碼複雜度需求 第 6-51 頁。
   - 所需字元集的最小數量：如需有關行動裝置密碼的指導方針，請參閱密碼複雜度需求 第 6-51 頁。
   - 在閒置後鎖定裝置
   - 需要在裝置上加密：行動裝置必須支援加密。
   - 登入失敗後清除裝置
10. 按一下「儲存」。

密碼複雜度需求

針對不同裝置類型和作業系統有不同的密碼複雜度需求。

下表列出了在發行 Worry-Free Business Security 9.0 SP3 時所測試裝置的各個複雜度「選項」的行為。

注意

密碼複雜度的功能取決於裝置類型和作業系統版本。如果特定密碼不符合複雜度需求，大多數裝置會向使用者提供訊息，指示該裝置的特定需求。

表 6-7. Android 裝置

複雜度層級	複雜度需求	
	ANDROID 4	ANDROID 2
選項 1	以下類型字元的組合： • 至少一個大寫 (A-Z) 或小寫 (a-z) 字元 • 至少一個數字 (0-9) 或特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	英數字元
選項 2	以下類型字元的組合： • 至少一個大寫 (A-Z) 或小寫 (a-z) 字元 • 至少兩個數字 (0-9) 或特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	以下類型字元的組合： • 英數字元 • 至少兩個數字 (0-9) 或特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 3	以下類型字元的組合： • 至少一個大寫 (A-Z) 或小寫 (a-z) 字元 • 至少三個數字 (0-9) 或特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	以下類型字元的組合： • 英數字元 • 至少三個數字 (0-9) 或特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

複雜度層級	複雜度需求	
	ANDROID 4	ANDROID 2
選項 4	以下類型字元的組合： • 至少一個大寫 (A-Z) 或小寫 (a-z) 字元 • 至少四個數字 (0-9) 或特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	以下類型字元的組合： • 英數字元 • 至少四個數字 (0-9) 或特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

表 6-8. iOS 裝置

複雜度層級	複雜度需求
選項 1	以下類型字元的組合： • 英數字元 • 至少一個特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 2	以下類型字元的組合： • 英數字元 • 至少兩個特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 3	以下類型字元的組合： • 英數字元 • 至少三個特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 4	以下類型字元的組合： • 英數字元 • 至少四個特殊字元 (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

表 6-9. Windows Phone 裝置

複雜度層級	複雜度需求	
	WINDOWS PHONE 8	WINDOWS PHONE 7
選項 1	以下至少一種類型的字元： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下至少兩種類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 2	以下至少兩種類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下至少兩種類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 3	以下至少三種類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下至少三種類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 4	以下所有類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	以下所有類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

表 6-10. BlackBerry 裝置

複雜度層級	複雜度需求
選項 1	至少一個大寫 (A-Z) 或小寫 (a-z) 字元
選項 2	以下至少兩種類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 3	以下至少三種類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
選項 4	以下所有類型字元的組合： • 大寫字元 (A-Z) • 小寫字元 (a-z) • 數字字元 (0-9) • 特殊字元 (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Messaging Security Agent 的隔離功能

當 Messaging Security Agent 在電子郵件中偵測到安全威脅、垃圾郵件、限制的附件和（或）限制的內容，代理程式即會將該郵件移至隔離資料夾。此處理程序可做為刪除郵件/附件的替代項目，並防止使用者開啟中毒的郵件和散播安全威脅。

Message Security Agent 上的預設隔離資料夾為：

```
<Messaging Security Agent 安裝資料夾>\storage\quarantine
```

為了進一步增強安全，會將隔離檔案加密。如果要開啟加密的檔案，可使用 Restore Encrypted Virus and Spyware (VSEncode.exe) 工具。請參閱還原加密檔案 第 14-17 頁。

系統管理員可以查詢隔離資料庫，取得有關被隔離的郵件的資訊。

使用「隔離」：

- 減少重要郵件遭到永久刪除的機會（遭到嚴格的過濾程式誤判時）
- 檢視觸發內容過濾的郵件以判斷違反策略的嚴重性
- 保留員工可能不當使用公司郵件系統的證據

注意

請勿將「隔離資料夾」與終端使用者的「垃圾郵件資料夾」混為一談。隔離資料夾是一種檔案式的資料夾。每當 Messaging Security Agent 隔離電子郵件時，會將隔離的郵件傳送到隔離資料夾。使用者的垃圾郵件資料夾位於每位使用者信箱的「資訊儲存區」中。終端使用者的垃圾郵件資料夾只接受由垃圾郵件防護隔離至使用者垃圾郵件資料夾所產生的電子郵件，並不會隔離因內容過濾、防毒/間諜程式防護或附件封鎖策略而產生的處理行動。

查詢隔離目錄

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「隔離 > 查詢」。

   隨即顯示新畫面。
5. 視需要更新下列項目：

- 日期/時間範圍
- 隔離原因
  - 所有原因
  - 指定的類型：從「病毒掃瞄」、「垃圾郵件防護」、「內容過濾」、「附件封鎖」和（或）「無法掃瞄的郵件部分」進行選取。
- 重新傳送狀態
  - 未曾重新傳送
  - 至少重新傳送過一次
  - 以上皆是
- 進階條件
  - 寄件人：來自特定寄件人的郵件。必要時請使用萬用字元。
  - 收件者：來自特定收件人的郵件。必要時請使用萬用字元。
  - 主旨：含特定主旨的郵件。必要時請使用萬用字元。
  - 排序依據：設定結果頁面的排序條件。
  - 顯示：每頁顯示的結果數。

6. 按一下「搜尋」。請參閱檢視查詢結果和採取處理行動 第 6-57 頁。

檢視查詢結果和採取處理行動

「隔離查詢結果」畫面會顯示郵件的下列相關資訊：

- 掃瞄時間
- 寄件人
- 收件者

- 主旨
- 原因：隔離電子郵件的原因。
- 檔案名稱：電子郵件中封鎖的檔案名稱。
- 隔離路徑：電子郵件的隔離位置。管理員可使用 VSEncoder.exe 解密檔案（請參閱還原加密檔案 第 14-17 頁），並重新命名為 `.eml` 以便檢視。

  警告!

  檢視中毒檔案可能會散播病毒。

- 重新傳送狀態

步驟

1. 如果覺得郵件不安全，即可刪除郵件。

   警告!

   隔離資料夾包含具有高度感染風險的電子郵件。處理來自隔離資料夾的電子郵件時請務必小心，以免無意間感染了用戶端。

2. 如果您覺得郵件安全，即可選取該郵件並按一下重新傳送圖示 ( )。

   注意

   如果重新傳送原先使用 Microsoft Outlook 傳送的被隔離郵件，則收件人可能會收到數封相同的郵件。這可能是因為「病毒掃瞄」引擎會將每一封它掃瞄過數個區段的郵件加以去除。

3. 如果您無法重新傳送郵件，可能是 Microsoft Exchange Server 的系統管理員帳號不存在。

   a. 使用「Windows 登錄編輯程式」，開啟伺服器的下列登錄項目：

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
      Exchange\CurrentVersion
      ```

b. 按照下列方式編輯項目：

警告!

編輯登錄的方式如果不正確，將可能嚴重損害您的系統。進行登錄變更之前，您應該備份電腦上所有寶貴的資料。

- `ResendMailbox {管理員信箱}`

  例如：`admin@example.com`

- `ResendMailboxDomain {管理員的網域}`

  例如：`example.com`

- `ResendMailSender {管理員的電子郵件帳號}`

  例如：`admin`

c. 關閉「登錄編輯程式」。

維護隔離目錄

使用此功能，手動或自動刪除隔離的郵件。此功能可以刪除所有郵件、已重新傳送的郵件和尚未重新傳送的郵件。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。

4. 按一下「隔離 > 維護」。

   隨即顯示新畫面。

5. 視需要更新下列項目：
   - 啟動自動維護：僅適用於自動維護。
   - 要刪除的檔案
     - 所有隔離的檔案
     - 未曾重新傳送的隔離檔案
     - 至少重新傳送過一次的隔離檔案
   - 處理行動：郵件應儲存的天數。例如，如果日期為 11 月 21 日，當您在「刪除超過此天數的選取檔案」欄位中輸入 `10` 時，Messaging Security Agent 會在自動執行刪除時，刪除所有早於 11 月 11 日的檔案。
6. 按一下「儲存」。

設定隔離目錄

設定 Microsoft Exchange Server 上的隔離目錄。將不會掃瞄隔離目錄。

注意

隔離目錄以檔案為基礎，不會位於「資訊儲存區」中。

Messaging Security Agent 會根據您所設定的處理行動來隔離電子郵件。以下為隔離目錄：

- 防毒：隔離含有病毒/惡意程式、間諜程式/可能的資安威脅程式、蠕蟲、特洛伊木馬程式和其他惡意安全威脅的電子郵件。
- 垃圾郵件防護：隔離垃圾郵件和網路釣魚電子郵件。
- 附件封鎖：隔離包含限制附件的電子郵件。
- 內容過濾：隔離包含限制內容的電子郵件。

依預設，所有目錄均擁有相同路徑（<Messaging Security Agent 安裝資料夾>\storage\quarantine）。您可以變更個別或所有目錄的路徑。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「隔離 > 目錄」。

   隨即顯示新畫面。
5. 設定以下隔離目錄的路徑：
   - 防毒
   - 垃圾郵件防護
   - 內容過濾
   - 附件封鎖
6. 按一下「儲存」。

Messaging Security Agent 的通知設定

Worry-Free Business Security 可使用電子郵件的形式傳送通知，以發出各種警訊。

您可以使用自訂內部電子郵件定義，將通知設定為僅套用至內部電子郵件。如果貴公司有兩個以上的網域，而您想將來自這兩個網域的電子郵件視為內部電子郵件，這會非常有用。例如：example.com 和 example.net。

選取「不通知外部收件者」核取方塊（在「防毒」、「內容過濾」與「附件封鎖」的「通知」設定下方）後，「內部電子郵件定義」清單上的收件者會收到通知郵件。請勿將「內部電子郵件定義」清單和「核可的寄件人」清單混淆。

為了避免所有包含外部網域地址的郵件被歸類為垃圾郵件，請將外部電子郵件信箱加入「垃圾郵件防護」的核可的寄件人清單中。

關於自訂內部墊子郵件定義

Messaging Security Agent 將電子郵件傳輸分成兩種網路類別：內部和外部。代理程式會查詢 Microsoft Exchange Server，以瞭解內部地址和外部地址的定義方式。所有的內部地址均共用一個通用網域，且所有外部地址均不屬於該網域。

例如，如果內部網域地址是「@trend_1.com」，Messaging Security Agent 便會將「abc@trend_1.com」和「xyz@trend_1.com」之類的地址歸類為內部地址。代理程式會將所有其他地址（如「abc@trend_2.com」和「jondoe@123.com」）都歸類為外部地址。

您只能將一個網域定義為 Messaging Security Agent 的內部地址。如果您使用 Microsoft Exchange 系統管理員變更您在伺服器上的主要地址，Messaging Security Agent 並不會將此新地址識別為內部地址，因為 Messaging Security Agent 無法偵測到收件人策略已有所變更。

例如，貴公司有兩個網域地址：@example_1.com 和 @example2.com。您將 @example_1.com 設為主要地址。Messaging Security Agent 會將具有主要地址的電子郵件視為內部郵件（即 abc@example_1.com 或 xyz@example_1.com 為內部地址）。稍後，您用 Microsoft Exchange 系統管理員將主要地址變更為 @example_2.com。這意味著 Microsoft Exchange 現在會將 abc@example_2.com 和 xyz@example_2.com 這類地址視為內部地址。

設定 Messaging Security Agent 的通知設定

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。

3. 按一下「設定策略」。

   隨即顯示新畫面。

4. 按一下「作業 > 通知設定」。

   隨即顯示新畫面。

5. 視需要更新下列項目：

   - 電子郵件信箱：代表 Worry-Free Business Security 的信箱將傳送通知訊息。
   - 內部電子郵件定義
     - 預設：Worry-Free Business Security 會將來自相同網域的電子郵件視為「內部電子郵件」。
     - 自訂：指定要視為內部電子郵件的個別電子郵件信箱或網域。

6. 按一下「儲存」。

設定垃圾郵件維護

「垃圾郵件維護」畫面可讓您設定終端使用者隔離 (EUQ) 或伺服器端隔離的設定。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。

4. 按一下「作業 > 垃圾郵件維護」。

   隨即顯示新畫面。

5. 按一下「啟動終端使用者隔離工具」。

   當您啟動該工具時，各個用戶端收件匣的伺服器端都會建立一個隔離資料夾，而終端使用者的 Outlook 資料夾樹狀結構中會出現一個「垃圾郵件」資料夾。在啟動 EUQ 並建立「垃圾郵件」資料夾後，EUQ 即可將垃圾郵件過濾到使用者的「垃圾郵件」資料夾中。如需詳細資訊，請參閱管理終端使用者隔離 第 6-65 頁。

   秘訣

   如果您選取此選項，趨勢科技建議您關閉代理程式上的「趨勢科技垃圾郵件防護工具列」選項，以提升用戶端的效能。

   取消選取「啟動終端使用者隔離工具」，將 Microsoft Exchange Server 上所有信箱的終端使用者隔離工具關閉。當關閉 EUQ 工具時，使用者的「垃圾郵件」資料夾仍會保留下來，但偵測為垃圾郵件的郵件將不會移到「垃圾郵件」資料夾中。

6. 按一下「建立垃圾郵件資料夾並刪除垃圾郵件」將會立即在新建立的郵件用戶端以及已將「垃圾郵件」資料夾刪除的現有郵件用戶端上建立「垃圾郵件」資料夾。對於其他現有的郵件用戶端，則會刪除超過「用戶端垃圾郵件資料夾設定」欄位中指定天數的垃圾郵件。

7. 在「刪除超過 {number} 天的垃圾郵件」中，修改 Messaging Security Agent 將保留垃圾郵件的時間長度。預設值是 14 天，最大的時間限制為 30 天。

8. 若要關閉特定使用者的「終端使用者隔離」工具，請執行下列作業：

   a. 在「終端使用者隔離工具例外清單」下，輸入要關閉其 EUQ 的終端使用者的電子郵件信箱。

   b. 按一下「新增」。

      終端使用者的電子郵件信箱就會新增到 EUQ 已關閉的信箱清單中。

      若要從該清單中移除終端使用者並且恢復 EUQ 服務，請從該清單中選取該終端使用者的電子郵件信箱，然後按一下「刪除」。

9. 按一下「儲存」。

管理終端使用者隔離

安裝期間，Messaging Security Agent 會新增資料夾 `Spam Mail` 至每個終端使用者的伺服器端信箱。當垃圾郵件送達時，系統會根據 Messaging Security Agent 預先定義的垃圾郵件過濾規則，將這些郵件隔離到此資料夾中。終端使用者可以檢視此垃圾郵件資料夾，以開啟、讀取或刪除可疑的電子郵件。請參閱設定垃圾郵件維護 第 6-63 頁。

另外，管理員可以在 Microsoft Exchange 上建立垃圾郵件資料夾。系統管理員建立信箱帳號時，不會立即在 Microsoft Exchange Server 中建立信箱項目，而是會在下列情形下建立：

- 終端使用者第一次登入他的信箱時
- 第一封電子郵件送達該信箱時

系統管理員必須先建立信箱項目，EUQ 才能建立垃圾郵件資料夾。

用戶端的垃圾郵件資料夾

終端使用者可以開啟隔離到垃圾郵件資料夾的電子郵件。當他們開啟其中一封郵件時，在實際的電子郵件中會出現兩個按鈕：「核可的寄件人」和「檢視核可的寄件人清單」。

- 終端使用者開啟「垃圾郵件」資料夾中的電子郵件，並按一下「核可的寄件人」後，該電子郵件的寄件人信箱會新增至終端使用者的「核可的寄件人」清單。
- 按一下「檢視核可的寄件人清單」會開啟另一個畫面，終端使用者可以在這個畫面中，依電子郵件信箱或網域來檢視和修改自己的核可的寄件人清單。

核可的寄件人

終端使用者在「垃圾郵件」資料夾中收到電子郵件，並按一下核可的寄件人後，Messaging Security Agent 會將郵件移到終端使用者的本機收件匣，並將寄件人的信箱加入終端使用者的個人「核可的寄件人清單」。Messaging Security Agent 會記錄事件。

Microsoft Exchange Server 收到終端使用者之「核可的寄件人」清單中的信箱寄來的郵件時，不論郵件的標頭或內容為何，它都會將郵件遞送至終端使用者的收件匣。

注意

Messaging Security Agent 也會提供管理員「核可的寄件人清單」和「封鎖的寄件人清單」。Messaging Security Agent 會先套用系統管理員的核可的寄件人和封鎖的寄件人，再考慮終端使用者的清單。

終端使用者垃圾郵件隔離內部管理功能

Messaging Security Agent 的管家功能預設每隔 24 小時於上午 2:30 執行下列工作：

- 自動刪除到期的垃圾郵件
- 如果垃圾郵件資料夾已刪除則重新建立
- 對新建立的郵件帳號建立垃圾郵件資料夾
- 維護電子郵件規則

管家功能是 Messaging Security Agent 的整合部分，不需要設定。

趨勢技術支援/偵錯工具

支援/偵錯工具可以協助您偵錯或僅報告 Messaging Security Agent 處理程序的狀態。當您遭遇未預期的困難時，您可以使用偵錯工具來建立偵錯工具報告，將它們傳送到趨勢科技客服部門以進行分析。

每個 Messaging Security Agent 都會將訊息插入到程式，然後在執行時將處理行動記錄到記錄檔中。您可以將這些記錄檔轉寄給趨勢科技的客服人員，協助偵錯您環境中的實際程式流程。

使用偵錯工具產生下列模組的記錄檔：

- Messaging Security Agent 主服務
- Messaging Security Agent 遠端組態伺服器
- Messaging Security Agent 系統監視程式
- 病毒掃瞄引擎 (VSAPI)

- 簡易郵件傳輸通訊協定 (SMTP)
- 通用閘道介面 (CGI)

依預設，MSA 會在下列目錄中保存記錄檔：

```
<Messaging Security Agent 安裝資料夾>\Debug
```

利用任何文字編輯器檢視輸出。

產生系統偵錯工具報告

產生偵錯工具報告，以協助趨勢科技客戶服務部門進行問題的疑難排解。

步驟

1. 移至「裝置」。
2. 選取 Messaging Security Agent。
3. 按一下「設定策略」。

   隨即顯示新畫面。
4. 按一下「作業 > 支援/偵錯工具」。

   隨即顯示新畫面。
5. 選取要監控的模組：
   - Messaging Security Agent 主服務
   - Messaging Security Agent 遠端組態伺服器
   - Messaging Security Agent 系統監視程式
   - 病毒掃瞄引擎 (VSAPI)（在 Exchange Server 2003、2007 或 2010 上）
   - 儲存等級掃瞄（在 Exchange Server 2013 上）
   - 簡易郵件傳輸通訊協定 (SMTP)（在 Exchange Server 2003 上）

- 傳輸服務（在 Exchange Server 2007、2010 或 2013 上）
- 通用閘道介面 (CGI)

6. 按一下「套用」。

   偵錯工具會開始收集選取模組的資料。

即時監控

「即時監控」會顯示有關所選 Microsoft Exchange Server 及其 Messaging Security Agent 的目前資訊。會顯示已掃瞄郵件及保護統計資料的相關資訊，包含找到的病毒和垃圾郵件數目、封鎖的附件和內容違規。也會檢查代理程式是否正常運作。

使用「即時監控」

步驟

1. 如果要從 Web 主控台存取「即時監控」：
   a. 移至「裝置」。
   b. 選取 Messaging Security Agent。
   c. 按一下「設定策略」。

      隨即顯示新畫面。

   d. 按一下畫面右上方的「即時監控」連結。
2. 若要從 Windows「開始」功能表存取「即時監控」，按一下「所有程式 > Trend Micro Messaging Security Agent > 即時監控」。
3. 按一下「重設」，將保護統計資料重設為零。

4. 按一下「清除內容」，清除已掃瞄郵件的舊資訊。

新增免責聲明至出站的電子郵件

您只能對出站的電子郵件新增免責聲明訊息。

步驟

1. 建立文字檔案並且新增免責聲明至此檔案。
2. 修改登錄中的下列機碼：
   - 第一個機碼：

     路徑：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     機碼：`EnableDisclaimer`

     類型：`REG_DWORD`

     資料值：`0 - 關閉、1 - 啟動`
   - 第二個機碼：

     路徑：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     機碼：`DisclaimerSource`

     類型：`REG_SZ`

     值：免責聲明內容檔案的完整路徑。

     例如，`C:\Data\Disclaimer.txt`

注意

依預設，Worry-Free Business Security 會偵測出站郵件是傳送至內部網域還是外部網域，並且在傳送至外部網域的每封郵件中新增免責聲明。使用者可以覆寫預設設定，並且新增免責聲明至每封出站郵件，除了下列登錄機碼中包含的網域：

- 第三個機碼：

  路徑：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

  機碼：`InternalDomains`

  類型：`REG_SZ`

  值：輸入要排除的網域名稱。使用分號 (;) 分隔多個項目。

  例如：`domain1.org;domain2.org`

注意

這裡的網域名稱是 Exchange Server 的 DNS 名稱。

第 7 章

管理掃瞄

本章說明如何對 Security Agent 和 Messaging Security Agent（僅限 Advanced 版）執行掃瞄，以保護您的網路和用戶端不受威脅的侵擾。

關於掃瞄

掃瞄期間，趨勢科技掃瞄引擎會結合病毒碼檔案執行初級偵測，採用的程序稱為「病毒碼比對」。由於每種安全威脅均包含獨有的特徵，或是包含能夠將其與任何其他程式碼區分開來的描述字元所組成的字串，因此可在病毒碼檔案中擷取該程式碼的內隱小片段。然後，引擎會將每個已掃瞄檔案的特定部分與病毒碼檔案中的病毒碼做比較，以尋找相符項。

如果掃瞄引擎偵測到包含安全威脅的檔案，則會執行清除、隔離、刪除或以文字/檔案取代等處理行動（僅限 Advanced 版）。您可以在設定掃瞄工作時自訂這些處理行動。

Worry-Free Business Security 提供三種類型的掃瞄。雖然每種掃瞄都有不同的目的和用途，但是設定方式大致上都相同。

- 即時掃瞄。如需詳細資訊，請參閱即時掃瞄 第 7-2 頁。
- 手動掃瞄。如需詳細資訊，請參閱手動掃瞄 第 7-3 頁。
- 預約掃瞄。如需詳細資訊，請參閱預約掃瞄 第 7-5 頁。

執行掃瞄時，Security Agent 會使用兩種掃瞄方法中的任意一種：

- 雲端截毒掃瞄
- 標準掃瞄

如需詳細資訊，請參閱掃瞄方法 第 5-3 頁。

即時掃瞄

「即時掃瞄」會一直持續進行。

每當開啟、下載、複製或修改檔案時，Security Agent 中的「即時掃瞄」即會掃瞄檔案是否含有安全威脅。如需有關設定「即時掃瞄」的詳細資訊，請參閱設定 Security Agent 即時掃瞄 第 5-6 頁。

就電子郵件而言，Messaging Security Agent（僅限 Advanced 版）中的「即時掃瞄」會掃瞄所有收到的郵件、SMTP 郵件、張貼於公共資料夾的文件，以及

從其他 Microsoft Exchange Server 複製的檔案，藉此防護所有已知的病毒進入點。如需有關設定「即時掃瞄」的詳細資訊，請參閱設定 Messaging Security Agent 的「即時掃瞄」 第 6-5 頁。

手動掃瞄

會依要求執行「手動掃瞄」。

Security Agent 上的手動掃瞄可消除對檔案的安全威脅和消滅任何舊有的中毒檔案，盡可能降低重複中毒的可能性。

Messaging Security Agent（僅限 Advanced 版）上的手動掃瞄會掃瞄 Microsoft Exchange Server 的「資訊儲存區」中的所有檔案。

執行掃瞄所需的時間，取決於用戶端的硬體資源與要掃瞄的檔案數目。對於執行中的手動掃瞄，如果是從 Web 主控台遠端執行，Security Server 管理員可停止掃瞄。而如果是直接在用戶端上執行，則使用者可停止掃瞄。

秘訣

趨勢科技建議您在安全威脅爆發之後執行「手動掃瞄」。

執行手動掃瞄

此程序說明 Security Server 管理員可以如何從 Web 主控台對 Security Agent 和 Messaging Security Agent（僅限 Advanced 版）執行手動掃瞄。

注意

手動掃瞄也可以直接從用戶端執行，只需在 Windows 工具列的 Security Agent 圖示上按一下右鍵，然後按一下「立即掃瞄」即可。無法直接在 Microsoft Exchange Server 上執行手動掃瞄。

步驟

1. 瀏覽至「掃瞄 > 手動掃瞄」。
2. （選用）自訂掃瞄設定，然後再執行手動掃瞄。

說明與注意事項	建議掃瞄設定
若要自訂 Security Agent 的掃瞄設定，按一下桌上型電腦或伺服器群組。 請參閱 Security Agent 的掃瞄目標和處理行動 第 7-8 頁。 注意 使用者從用戶端執行手動掃瞄時，也會使用 Security Agent 的掃瞄設定。但是，如果您授與使用者自行設定掃瞄設定的權限，則掃瞄時將會使用使用者設定的設定。	目標 • 所有可掃瞄的檔案：包括所有可掃瞄的檔案。無法掃瞄的檔案為受密碼保護的檔案、加密檔案、或超過使用者定義的掃瞄限制範圍的檔案。 • 壓縮檔掃瞄層數上限 1：會掃瞄至壓縮檔的第 1 個壓縮層。對於預設的伺服器群組，預設值是「關閉」；對於預設的桌上型電腦群組，預設值是「開啟」。
	例外 • 不掃瞄趨勢科技產品的安裝目錄
	進階設定 • 修改間諜程式/可能的資安威脅程式例外清單（僅適用於間諜程式防護）

說明與注意事項	建議掃瞄設定
若要自訂 Messaging Security Agent 的掃瞄設定，展開代理程式並按一下以下項目： • 防毒：按一下此選項，可讓代理程式掃瞄病毒和其他惡意程式。請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁。 • 內容過濾：按一下此選項，可讓代理程式掃瞄電子郵件中是否有禁止的內容。請參閱管理內容過濾規則 第 6-14 頁。 • 附件封鎖：按一下此選項，可讓代理程式掃瞄電子郵件附件是否違規。請參閱設定附件封鎖 第 6-41 頁。	• 代理程式會掃瞄所有可掃瞄的檔案。掃瞄時包括電子郵件的內文。 • 代理程式偵測到含有病毒或其他惡意程式的檔案時，就會清除該檔案。如果無法清除檔案，就會以文字或檔案取代。 • 代理程式偵測到有特洛伊木馬程式或蠕蟲的檔案時，會以文字或檔案取代特洛伊木馬程式或蠕蟲。 • 代理程式偵測到含有封裝程式的檔案時，會以文字或檔案取代封裝程式。 • 代理程式不會清除中毒的壓縮檔。如此可以縮短即時掃瞄所花費的時間。

3. 選取要掃瞄的群組或 Messaging Security Agent。
4. 按一下「立即掃瞄」。

   Security Server 會傳送通知至代理程式以執行手動掃瞄。隨即出現的「掃瞄通知結果」畫面會顯示收到通知和未收到通知的代理程式數量。
5. 如果要停止進行中的掃瞄，按一下「停止掃瞄」。

   Security Server 會傳送另一封通知至代理程式以停止手動掃瞄。隨即出現的「停止掃瞄通知結果」畫面會顯示收到通知和未收到通知的代理程式數量。如果 Security Agent 在掃瞄開始後離線，或發生網路中斷，則可能無法收到通知。

預約掃瞄

預約掃瞄類似手動掃瞄，但會依設定的時間和頻率來掃瞄所有檔案和電子郵件（僅限 Advanced 版）。使用預約掃瞄可針對用戶端自動進行例行掃瞄，並提高安全威脅管理效率。

秘訣

在離峰時段執行預約掃瞄，可將對使用者和網路造成的任何可能中斷降到最低。

設定預約掃瞄

趨勢科技建議您不要將預約掃瞄和預約更新安排在相同的時間執行。如此可能會造成預約掃瞄提前中止。同樣地，如果您在執行預約掃瞄時啟動手動掃瞄，預約掃瞄會停止，但會根據其預約再次執行。

步驟

1. 瀏覽至「掃瞄 > 預約掃瞄」。
2. 按一下「預約」標籤。
   a. 設定掃瞄頻率（每日一次、每週一次或每月一次）和開始時間。每個群組或 Messaging Security Agent 可以有其自己的預約。

      注意

      對於每月一次的預約掃瞄，如果您選取 31、30 或 29 日，但該月沒有該日期，則該月將不會執行掃瞄。

   b. （選用）選取「預約掃瞄完成後將用戶端關機」。
   c. 按一下「儲存」。
3. 按一下「設定」標籤，然後進行任何所需的預約掃瞄設定。

說明與注意事項	建議掃瞄設定
若要自訂 Security Agent 的掃瞄設定，按一下桌上型電腦或伺服器群組。請參閱 Security Agent 的掃瞄目標和處理行動 第 7-8 頁。 注意 如果您授與使用者設定其自己的掃瞄設定的權限，則會在掃瞄期間使用使用者設定的設定。	目標 • 所有可掃瞄的檔案：包括所有可掃瞄的檔案。無法掃瞄的檔案為受密碼保護的檔案、加密檔案、或超過使用者定義的掃瞄限制範圍的檔案。 • 壓縮檔掃瞄層數上限 2：會掃瞄至壓縮檔的第 2 個壓縮層。 例外 • 不掃瞄趨勢科技產品的安裝目錄 進階設定 • 修改間諜程式/可能的資安威脅程式例外清單（僅適用於間諜程式防護）
若要自訂 Messaging Security Agent 的掃瞄設定，展開代理程式並按一下以下項目： • 防毒：按一下此選項，可讓代理程式掃瞄病毒和其他惡意程式。請參閱 Messaging Security Agent 的掃瞄目標和處理行動 第 7-14 頁。 • 內容過濾：按一下此選項，可讓代理程式掃瞄電子郵件中是否有禁止的內容。請參閱管理內容過濾規則 第 6-14 頁。 • 附件封鎖：按一下此選項，可讓代理程式掃瞄電子郵件附件是否違規。請參閱設定附件封鎖 第 6-41 頁。	• 代理程式會在每個星期日上午 5:00 開始執行掃瞄。 • 自訂此排程在您用戶端的離峰時間執行。代理程式會掃瞄所有可掃瞄的檔案。掃瞄時包括電子郵件的內文。 • 代理程式偵測到含有病毒或其他惡意程式的檔案時，就會清除該檔案。如果無法清除檔案，就會以文字或檔案取代。 • 當代理程式偵測到含有特洛伊木馬程式或蠕蟲的檔案時，就會以文字/檔案取代特洛伊木馬程式或蠕蟲。 • 當代理程式偵測到含有封裝程式的檔案時，就會文字/檔案取代封裝程式。 • 代理程式不會清除中毒的壓縮檔。

4. 選取將套用預約掃瞄設定的群組或 Messaging Security Agent。

注意

若要關閉預約掃瞄，請取消選取該群組或 Messaging Security Agent 的核取方塊。

5. 按一下「儲存」。

Security Agent 的掃瞄目標和處理行動

為每種掃瞄類型（手動掃瞄、預約掃瞄和即時掃瞄）設定以下設定：

「目標」標籤

選取方法：

- 所有可掃瞄的檔案：包括所有可掃瞄的檔案。無法掃瞄的檔案為受密碼保護的檔案、加密檔案、或超過使用者定義的掃瞄限制範圍的檔案。

注意

此選項提供了可能的最高安全性。但是，掃瞄每個檔案是一件即費時又耗資源的事，而且在某些情況下可能會太過累贅。因此，您可以限制代理程式在掃瞄中包含的檔案數量。

- 「智慧型掃瞄」使用「真實檔案類型」辨識：根據真實檔案類型掃瞄檔案。請參閱智慧型掃瞄 第 D-2 頁。
- 掃瞄具有下列副檔名的檔案：根據副檔名手動指定要掃瞄的檔案。請使用逗號分隔多個項目。

選取掃瞄觸發：

- 讀取：讀取檔案內容時掃瞄檔案；開啟、執行、複製或移動檔案時會讀取檔案。
- 寫入：寫入檔案內容時掃瞄檔案；修改、儲存、下載檔案或從其他位置複製檔案時會寫入檔案的內容。
- 讀取或寫入

掃瞄例外

可進行的設定包括：

- 啟動或關閉例外
- 不掃瞄趨勢科技產品目錄
- 不掃瞄其他目錄

  也不會掃瞄所有指定目錄路徑下的子目錄
- 不掃瞄檔案名稱或具有完整路徑的檔案名稱
- 不掃瞄副檔名

  副檔名中不得包含萬用字元（例如 *）

注意

（僅限 Advanced 版）如果用戶端上正在執行 Microsoft Exchange Server，趨勢科技建議您不掃瞄所有 Microsoft Exchange Server 資料夾。如果不要對 Microsoft Exchange Server 資料夾執行全域掃瞄，請移至「管理 > 全域設定 > 桌上型電腦/伺服器 {標籤} > 一般掃瞄設定」，然後選取「安裝在 Microsoft Exchange Server 上時，不掃瞄 Microsoft Exchange Server 的資料夾」。

進階設定

掃瞄類型	選項
即時掃瞄	掃瞄 POP3 郵件：依預設，「郵件掃瞄」只會掃瞄收件匣和垃圾郵件資料夾中，透過通訊埠 110 傳送的新郵件。不支援安全 POP3 (SSL-POP3)。 • Microsoft Outlook 2007、2010 或 2013 • Mozilla Thunderbird 1.5 或更新版本 「郵件掃瞄」無法偵測 IMAP 郵件中的安全威脅。使用 Messaging Security Agent（僅限 Advanced 版）偵測 IMAP 郵件中的安全威脅和垃圾郵件。
即時掃瞄和手動掃瞄	掃瞄網路上的網路磁碟機和共享資料夾：選取此選項可掃瞄實際位於其他電腦上、但對應至本機電腦的目錄。

掃瞄類型	選項
即時掃瞄	在系統關機時掃瞄軟碟機
即時掃瞄	啟動 IntelliTrap：IntelliTrap 可以偵測到壓縮檔中是否含有 Bot 之類的惡意程式碼。請參閱 IntelliTrap 第 D-2 頁。
即時掃瞄	隔離在記憶體中偵測到的惡意程式變體：如果「即時掃瞄」和「行為監控」已啟動並且選取此選項，則會掃瞄執行中的處理程序記憶體是否有封裝惡意程式。會隔離「行為監控」已偵測到的所有封裝惡意程式。
即時掃瞄、手動掃瞄和預約掃瞄	壓縮檔掃瞄層數上限 __：壓縮檔每壓縮一次就多一層。如果中毒檔案已壓縮數層，則必須掃瞄指定的層數才能偵測到感染。不過，掃瞄數層需要更多時間和資源。
即時掃瞄、手動掃瞄和預約掃瞄	修改間諜程式/可能的資安威脅程式例外清單：您無法從代理程式主控台設定此設定。
手動掃瞄、預約掃瞄	CPU 使用率/掃瞄速度：Security Agent 可以在掃瞄一個檔案之後、掃瞄下一個檔案之前暫停。 您可以選取下列選項： • 高：掃瞄之間不暫停 • 中：如果 CPU 耗用大於 50% 便在檔案掃瞄間暫停；如果小於 50% 則不暫停 • 低：如果 CPU 耗用大於 20% 便在檔案掃瞄間暫停；如果小於 20% 則不暫停
手動掃瞄、預約掃瞄	執行進階清除：Security Agent 會停止詐欺安全軟體（亦稱為 FakeAV）的活動。代理程式也使用進階清除規則來主動偵測並中止出現 FakeAV 行為的應用程式。 **注意** 提供主動式安全防護的同時，進階清除也會導致大量誤報。

間諜程式/可能的資安威脅程式例外清單

趨勢科技將某些應用程式歸類為間諜程式/可能的資安威脅程式，並非因為它們會對其所在的系統造成損害，而是因為有可能會讓用戶端或網路遭受惡意程式或駭客的攻擊。

Worry-Free Business Security 包含一份具有潛在風險的應用程式清單，依預設會阻止這些應用程式在用戶端上執行。

如果用戶端需要執行的應用程式已被趨勢科技歸類為間諜程式/可能的資安威脅程式，您就必須將該應用程式的名稱新增到「間諜程式/可能的資安威脅程式例外清單」中。

「處理行動」標籤

下列是 Security Agent 可針對病毒/惡意程式執行的處理行動：

表 7-1. 病毒/惡意程式中毒處理行動

處理行動	說明
刪除	刪除中毒檔案。
隔離	重新命名中毒檔案，再將這些檔案移至用戶端上的暫存隔離目錄。 然後，Security Agent 會將已隔離的檔案傳送到指定的隔離目錄（依預設位於 Security Server 上）。 Security Agent 會加密傳送到此目錄的隔離檔案。 如果您需要恢復任何已隔離的檔案，請使用 VSEncrypt 工具。
清除	先清除中毒檔案，才允許完整存取該檔案。 如果檔案無法清除，則 Security Agent 會執行第二個處理行動，第二個處理行動可能是下列其中一種：隔離、刪除、重新命名與暫不處理 系統可對所有類型的惡意程式（但不包括可能的病毒/惡意程式）執行此處理行動。 注意 有些檔案無法清除。如需詳細資訊，請參閱無法清除病毒的檔案 第 D-23 頁。
重新命名	將中毒檔案的副檔名變更為 "vir"。使用者一開始無法開啟重新命名的檔案，但是如果使檔案與特定的應用程式產生關聯，就可以開啟該檔案。 開啟重新命名的中毒檔案時，可能會執行病毒/惡意程式。

處理行動	說明
暫不處理	僅在手動掃瞄和預約掃瞄期間執行。Security Agent 無法在即時掃瞄過程中使用此中毒處理行動，因為在偵測到嘗試開啟或執行中毒檔案時，若未執行任何處理行動，則會允許執行病毒/惡意程式。「即時掃瞄」過程中可以使用其他所有的中毒處理行動。
拒絕存取	僅在即時掃瞄期間執行。當 Security Agent 偵測到嘗試開啟或執行中毒檔案的行為時，會立即阻止該作業。 使用者可以手動刪除中毒的檔案。

Security Agent 執行的中毒處理行動視偵測到間諜程式/可能的資安威脅程式的掃瞄類型而定。您可以為每種病毒/惡意程式類型設定特定的處理行動，但只能為所有間諜程式/可能的資安威脅程式類型設定一個處理行動。例如，當 Security Agent 在手動掃瞄（掃瞄類型）過程中偵測到任何類型的間諜程式/可能的資安威脅程式時，便會清除（處理行動）受影響的系統資源。

下列是 Security Agent 可針對間諜程式/可能的資安威脅程式執行的處理行動：

表 7-2. 間諜程式/可能的資安威脅程式中毒處理行動

處理行動	說明
清除	結束程序，或刪除登錄、檔案、Cookie 和捷徑。
暫不處理	不對偵測到的間諜程式/可能的資安威脅程式元件執行任何處理行動，但是在記錄檔中記錄偵測到的間諜程式/可能的資安威脅程式。此處理行動只能在手動掃瞄和預約掃瞄期間執行。在「即時掃瞄」期間，處理行動為「拒絕存取」。 如果偵測到的間諜程式/可能的資安威脅程式包含在例外清單中，Security Agent 將不會執行任何處理行動。
拒絕存取	拒絕存取（複製、開啟）偵測到的間諜程式/可能的資安威脅程式元件。此處理行動只能在「即時掃瞄」期間執行。在手動掃瞄和預約掃瞄期間，處理行動為「暫不處理」。

主動式處理行動

不同類型的病毒/惡意程式需要不同的中毒處理行動。自訂中毒處理行動需要有病毒/惡意程式的知識，並且可能會是冗長而乏味的工作。Security Agent 使用「主動式處理行動」來因應這些問題。

「主動式處理行動」是一套預先設定的中毒處理行動，可以處理病毒/惡意程式。如果您不熟悉中毒處理行動，或是不確定何種中毒處理行動適合那一種特定的病毒/惡意程式，趨勢科技建議您使用「主動式處理行動」。

使用「主動式處理行動」具有以下優點：

- 「主動式處理行動」會使用趨勢科技建議的中毒處理行動。您不需要耗費時間來設定中毒處理行動。
- 病毒撰寫者會不斷變更病毒/惡意程式攻擊端點的方式。更新「主動式處理行動」設定以抵禦最新威脅和最新的病毒/惡意程式攻擊方法。

下表說明「主動式處理行動」處理每種類型病毒/惡意程式的方式：

表 7-3. 趨勢科技建議的病毒/惡意程式中毒處理行動

病毒/惡意程式類型	即時掃瞄		手動掃瞄/預約掃瞄	
	第一個中毒處理行動	第二個中毒處理行動	第一個中毒處理行動	第二個中毒處理行動
惡作劇程式	隔離	刪除	隔離	刪除
特洛伊木馬程式/蠕蟲	隔離	刪除	隔離	刪除
封裝程式	隔離	無	隔離	無
可能的病毒/惡意程式	暫不處理	無	暫不處理或使用者設定的處理行動	無
病毒	清除	隔離	清除	隔離
測試病毒	拒絕存取	無	無	無
其他惡意程式	清除	隔離	清除	隔離

注意

- 有些檔案無法清除。如需詳細資訊，請參閱無法清除病毒的檔案 第 D-23 頁。
- 進行間諜程式/可能的資安威脅程式掃瞄時，無法使用主動式處理行動。
- 當提供新的病毒碼檔案時，這些設定的預設值可能會變更。

進階設定

掃瞄類型	選項
即時掃瞄、預約掃瞄	偵測到病毒/間諜程式時，在桌上型電腦或伺服器上顯示警告訊息
即時掃瞄、預約掃瞄	偵測到可能的病毒/間諜程式時，在桌上型電腦或伺服器上顯示警告訊息
手動掃瞄、即時掃瞄和預約掃瞄	偵測到可能的病毒/惡意程式時，執行清除：僅在您選擇「主動式處理行動」並自訂了可能的病毒/惡意程式的處理行動時，才可用。

Messaging Security Agent 的掃瞄目標和處理行動

為每種掃瞄類型（手動掃瞄、預約掃瞄和即時掃瞄）設定以下設定：

「目標」標籤

- 掃瞄目標
- 其他安全威脅掃瞄設定
- 掃瞄例外

「處理行動」標籤

- 中毒處理行動/主動式處理行動

- 通知
- 進階設定

掃瞄目標

選取掃瞄目標：

- 所有附件檔案：僅排除加密或受密碼保護的檔案。

  注意

  此選項提供了可能的最高安全性。但是，掃瞄每個檔案是一件即費時又耗資源的事，而且在某些情況下可能會太過累贅。因此，您可以限制代理程式在掃瞄中包含的檔案數量。

- 智慧型掃瞄：根據真實檔案類型掃瞄檔案。請參閱智慧型掃瞄 第 D-2 頁。
- 特定檔案類型：Worry-Free Business Security 會掃瞄屬於所選類型且具有所選副檔名的檔案。請以半形分號 (;) 分隔多個項目。

選取其他選項：

- 啟動 IntelliTrap：IntelliTrap 可以偵測到壓縮檔中是否含有 Bot 之類的惡意程式碼。請參閱 IntelliTrap 第 D-2 頁。
- 掃瞄郵件內文：掃瞄包含內嵌安全威脅的電子郵件內文。

其他安全威脅掃瞄設定

選取代理程式應該掃瞄的其他安全威脅。如需有關這些安全威脅的詳細資訊，請參閱瞭解安全威脅 第 1-7 頁。

選取其他選項：

- 在清除前備份中毒檔案：Worry-Free Business Security 會在清除之前製作安全威脅的備份。會加密備份檔案，並將其儲存在用戶端的下列目錄：

  `<Messaging Security Agent 安裝資料夾>\storage\backup`

  您可以在「進階選項」區段中的「備份設定」子區段中變更目錄。

  若要解密檔案，請參閱還原加密檔案 第 14-17 頁。

- 不清除中毒的壓縮檔以達最佳化效能

掃瞄例外

在「目標」標籤下，移至「例外」區段，並從以下條件中選取代理程式在不掃瞄電子郵件時將使用的條件：

- 郵件內文大小超過：Messaging Security Agent 只會掃瞄郵件內文大小小於或等於指定數字的電子郵件。
- 附件大小超過：Messaging Security Agent 只會掃瞄附件檔案大小小於或等於指定數字的電子郵件。

秘訣

趨勢科技建議您使用 30 MB 的限制。

- 解壓縮檔數目超過：壓縮檔內的解壓縮檔數量如果超過此數字，Messaging Security Agent 就只會掃瞄此選項所設定的檔案數上限。
- 解壓縮檔大小超過：Messaging Security Agent 只會掃瞄解壓縮後小於或等於此大小的壓縮檔。
- 壓縮的層數超過：Messaging Security Agent 只會掃瞄壓縮層小於或等於指定上限的壓縮檔。例如，如果您設定的限制為 5 個壓縮層，則 Messaging Security Agent 將只會掃瞄前 5 層壓縮檔，而不會掃瞄壓縮到第 6 層或更深入的檔案。
- 解壓縮檔的大小是壓縮檔的 x 倍：Messaging Security Agent 只會掃瞄解壓縮檔和壓縮檔大小的比例小於此數字的壓縮檔。此功能可避免 Messaging Security Agent 掃瞄可能導致拒絕服務 (DoS) 攻擊的壓縮檔。當非必要的工作耗用大量郵件伺服器的資源時，就會發生 DoS 攻擊。避免讓 Messaging Security Agent 掃瞄過大的壓縮檔，有助於防止此問題發生。

  例如：在下表中，x 值的輸入值為 100。

檔案大小 （未壓縮）	檔案大小 （未壓縮）	結果
500 KB	10 KB（比例為 50:1）	已掃瞄
1,000 KB	10 KB（比例為 100:1）	已掃瞄
1,001 KB	10 KB（比例超過 100:1）	未掃瞄 *
2000 KB	10 KB（比例為 200:1）	未掃瞄 *

* Messaging Security Agent 會執行您對不掃瞄的檔案所設定的處理行動。

中毒處理行動

管理員可以將 Messaging Security Agent 設定成依據病毒/惡意程式、特洛伊木馬程式和蠕蟲所呈現的安全威脅類型，採取不同的處理行動。如果您使用自訂中毒處理行動，即可針對每種安全威脅類型設定中毒處理行動。

表 7-4. Messaging Security Agent 自訂的處理行動

處理行動	說明
清除	從中毒的郵件內文和附件移除惡意程式碼。其餘的電子郵件文字、任何未中毒的檔案，以及清除後的檔案仍然會傳送給目標收件人。趨勢科技建議您對病毒/惡意程式執行預設中毒處理行動清除。 Messaging Security Agent 在某些情況下無法清除檔案。 在手動掃瞄或預約掃瞄期間，Messaging Security Agent 會更新「資訊儲存區」，並以已清除的檔案取代原有檔案。
以文字/檔案取代	刪除中毒/過濾的內容，並以文字或檔案加以取代。電子郵件會傳送給目標收件人，但是文字取代部分會告知收件人，原始內容已中毒而且已被取代。 對於內容過濾和 Data Loss Prevention，您只能取代內文或附件欄位中的文字（無法取代「寄件人」、「收件人」、「副件」或「主旨」欄位中的文字）。
隔離整個郵件	（僅限即時掃瞄）僅將中毒內容移至隔離目錄進行隔離，收件者會收到不含此內容的郵件。 對於內容過濾、Data Loss Prevention 和附件封鎖，會將整個郵件移至隔離目錄。

處理行動	說明
隔離郵件部分	（僅限即時掃瞄）僅將中毒或過濾的內容移至隔離目錄進行隔離，收件者會收到不含此內容的郵件。
刪除整封郵件	（僅限即時掃瞄）刪除整封電子郵件。原來的收件人不會收到該郵件。
通過	在病毒記錄檔中記錄惡意檔案的病毒感染，但是不執行任何中毒處理行動。已排除、加密或以密碼保護的檔案會直接傳遞給收件者，而不會更新記錄檔。 對於內容過濾，會原封不動地傳送郵件。
封存	將郵件移至封存目錄，並將郵件傳送給原始收件人。
將郵件隔離到伺服器端的垃圾郵件資料夾	將整封郵件傳送至 Security Server 進行隔離。
將郵件隔離到使用者的垃圾郵件資料夾	將整封郵件傳送至使用者的垃圾郵件資料夾進行隔離。該資料夾位於伺服器的「資訊儲存區」中。
加上標記並傳送	在電子郵件的標頭資訊中加上標籤，將其識別為垃圾郵件，然後再傳送給預定收件者。

除了這些處理行動外，您還可以設定以下處理行動：

- 啟動用於大量郵件行為的處理行動：針對安全威脅的大量郵件行為類型，從「清除」、「以文字/檔案取代」、「刪除整封郵件」、「暫不處理」或「隔離郵件部分」進行選取。
- 清除不成功時執行此動作：針對無法完成的清除嘗試，設定次要的處理行動。從「以文字/檔案取代」、「刪除整封郵件」、「暫不處理」或「隔離郵件部分」中選取。

主動式處理行動

下表說明「主動式處理行動」處理每種類型病毒/惡意程式的方式：

表 7-5. 趨勢科技建議的病毒/惡意程式中毒處理行動

病毒/惡意程式類型	即時掃瞄		手動掃瞄/預約掃瞄	
	第一個中毒處理行動	第二個中毒處理行動	第一個中毒處理行動	第二個中毒處理行動
病毒	清除	刪除整封郵件	清除	以文字/檔案取代
特洛伊木馬程式/蠕蟲	以文字/檔案取代	無	以文字/檔案取代	無
封裝程式	隔離郵件部分	無	隔離郵件部分	無
其他惡意程式碼	清除	刪除整封郵件	清除	以文字/檔案取代
其他安全威脅	隔離郵件部分	無	以文字/檔案取代	無
大量郵件行為	刪除整封郵件	無	以文字/檔案取代	無

中毒處理行動通知

選取「通知收件者」，以將 Messaging Security Agent 設定為，在針對特定電子郵件採取處理行動時通知預定收件者。由於各種原因，封鎖包含機密資訊的郵件時，您可能不想通知外部郵件收件者。選取「不通知外部收件者」，只傳送通知給內部郵件收件者。從「作業 > 通知設定 > 內部郵件定義」，定義內部信箱。

您也可以對欺詐寄件者的外部收件者關閉通知傳送。

進階設定（中毒處理行動）

設定	詳細資訊

巨集	巨集病毒是針對特定應用程式的病毒，會使隨附於應用程式的巨集公用程式中毒。進階巨集掃瞄會使用自動邏輯分析掃瞄來偵測巨集病毒，或者清除偵測到的所有巨集程式碼。自動邏輯分析掃瞄是一種評估式的偵測病毒方法，使用病毒碼辨識和規則技術來搜尋惡意的巨集程式碼。這個方法在偵測還不具備已知病毒特徵的未發現病毒和安全威脅方面十分卓越。
	
	Messaging Security Agent 會依您設定的處理行動，對惡意巨集程式碼採取處理行動。
	
	• 自動邏輯分析等級
	  • 「等級 1」會使用最嚴格的條件，但所偵測到的巨集程式碼最少。
	  • 「等級 4」會偵測到最多巨集程式碼，但會使用最寬鬆的條件，而誤將安全的巨集程式碼識別為惡意巨集程式碼。
	
	秘訣
	趨勢科技建議的自動邏輯分析掃瞄等級為 2。這個等級的未知巨集病毒偵測等級較高，掃瞄速度較快，而且只用必要的規則檢查巨集病毒字串。「等級 2」在安全巨集程式碼中錯誤識別出惡意程式碼的機率也較低。
	
	• 刪除進階巨集掃瞄偵測到的所有巨集：清除在掃瞄的檔案中偵測到的所有巨集程式碼

無法掃瞄的郵件部分	針對加密和（或）受密碼保護的檔案，設定處理行動和通知條件。對於處理行動，可從「以文字/檔案取代」、「隔離整個郵件」、「刪除整封郵件」、「暫不處理」或「隔離郵件部分」中進行選取。
排除的郵件部分	針對不掃瞄的郵件部分，設定處理行動和通知條件。對於處理行動，可從「以文字/檔案取代」、「隔離整個郵件」、「刪除整封郵件」、「暫不處理」或「隔離郵件部分」中進行選取。
備份設定	在代理程式清除中毒檔案之前儲存中毒檔案備份的位置。
取代設定	設定取代文字的文字和檔案。如果處理行動是「以文字/檔案取代」，Worry-Free Business Security 會以此文字字串和檔案取代安全威脅。

第 8 章

管理更新

本章說明 Worry-Free Business Security 元件和更新程序。

更新總覽

所有元件更新都是由趨勢科技主動式更新伺服器提供。如果有可用的更新，Security Server 會下載更新的元件，然後將它們分發到 Security Agent 和 Messaging Security Agent（僅限 Advanced 版）。

如果 Security Server 管理大量 Security Agent，更新可能會耗用大量的伺服器電腦資源，進而影響伺服器的穩定性和效能。為了解決這個問題，Worry-Free Business Security 提供了更新代理程式功能，以讓特定 Security Agent 分擔將更新分發到其他 Security Agent 的工作。

下表說明 Security Server 和代理程式的元件更新選項，以及使用各選項的建議時機：

表 8-1. 更新選項

更新順序	說明	建議
1. 主動式更新伺服器或自訂更新來源 2. Security Server 3. 代理程式	趨勢科技 Security Server 會從主動式更新伺服器或自訂更新來源接收更新的元件，並將這些元件直接部署到代理程式（Security Agent 和 Messaging Security Agent）。	如果 Security Server 與代理程式之間沒有低頻寬的區段，請使用這個方法。
1. 主動式更新伺服器或自訂更新來源 2. Security Server 3. Update Agent、Messaging Security Agent、沒有更新代理程式的 Security Agent 4. 所有其他 Security Agent	趨勢科技 Security Server 會從主動式更新伺服器或自訂更新來源接收更新的元件，並將這些元件直接部署到下列各項： • 更新代理程式 • Messaging Security Agent • 沒有更新代理程式的 Security Agent 然後，更新代理程式會將這些元件部署到其各自的 Security Agent。如果這些 Security Agent 無法進行更新，它們將直接從 Security Server 進行更新。	如果 Security Server 與 Security Agent 之間有低頻寬的區段，請使用這個方法來平衡網路上的傳輸負載。

更新順序	說明	建議
1. 主動式更新伺服器 2. Security Agent	無法從任何來源進行更新的 Security Agent 會直接從主動式更新伺服器進行更新。 注意 Messaging Security Agent 絕對不會直接從主動式更新伺服器進行更新。如果所有來源均無法使用，則 Messaging Security Agent 會結束更新處理程序。	此機制只能在別無他法時使用，而且必須先進行下列動作： 在「更新權限」下啟動「將趨勢科技主動式更新用作次要更新來源」

可更新的元件

Worry-Free Business Security 會使用元件，以保護用戶端免受最新安全威脅的攻擊。請透過執行手動或預約更新，使這些元件保持在最新狀態。

您可以透過執行下列操作來檢視元件清單：

- 移至「更新 > 手動」。
- 移至「即時狀態」，然後按一下「代理程式狀態」Widget 上的「檢查元件狀態」。

下表列出 Security Server 從主動式更新伺服器下載的元件：

表 8-2. 通訊元件（僅限 Advanced 版）

元件	分發到	說明
Messaging Security Agent 垃圾郵件防護病毒碼	Messaging Security Agent	垃圾郵件防護病毒碼可辨識電子郵件和電子郵件附件中的最新垃圾郵件。
Messaging Security Agent 垃圾郵件防護引擎（32/64 位元）	Messaging Security Agent	垃圾郵件防護引擎可偵測到電子郵件和電子郵件附件中的垃圾郵件。

元件	分發到	說明
Messaging Security Agent 掃瞄引擎（32/64 位元）	Messaging Security Agent	掃瞄引擎可偵測到電子郵件和電子郵件附件中的 Internet 蠕蟲、大量寄件程式、特洛伊木馬程式、網路釣魚網站、間諜程式、網路弱點攻擊和病毒。
Messaging Security Agent URL 過濾引擎（32/64 位元）	Messaging Security Agent	URL 過濾引擎可促進 Worry-Free Business Security 和趨勢科技 URL 過濾服務之間的通訊。URL 過濾服務是一個對 URL 進行分級並向 Worry-Free Business Security 提供分級資訊的系統。

表 8-3. 防毒和雲端截毒掃瞄

元件	分發到	說明
病毒碼	使用標準掃瞄的 Security Agent	「病毒碼」所含的資訊，可協助 Security Agent 識別最新的病毒/惡意程式和混合式安全威脅攻擊。趨勢科技會每週建立數次新版的「病毒碼」並發行，而在發現特別具有破壞力的病毒/惡意程式時會立即建立並發行。
IntelliTrap 病毒碼	Security Agent	IntelliTrap 病毒碼用於偵測包裝成為可執行檔的即時壓縮檔的檔案。 如需詳細資訊，請參閱 IntelliTrap 第 D-2 頁。
IntelliTrap 例外病毒碼	Security Agent	IntelliTrap 例外病毒碼包含「許可的」壓縮檔清單。

元件	分發到	說明
病毒掃瞄引擎（32/64 位元）	Security Agent	所有趨勢科技產品的核心都是掃瞄引擎，其最初的開發目的是偵測早期的檔案型病毒。現在的掃瞄引擎則非常成熟，而且可以偵測不同類型的病毒和惡意程式。掃瞄引擎也可以偵測開發用於研究目的的受控制病毒。 引擎和病毒碼檔案不會掃瞄每個檔案的每個位元組，而會一起合作來辨識下列項目： • 病毒程式碼的獨有特徵 • 檔案內病毒所在的確切位置
雲端截毒掃瞄病毒碼	未分發到 Security Agent。此病毒碼會保留在 Security Server 伺服器中，而且會在收到來自 Security Agent 的掃瞄查詢時，用來回應這些查詢。	使用雲端截毒掃瞄模式時，Security Agent 會使用兩個共同運作的小型病毒碼，提供與標準惡意程式防護病毒碼和間諜程式防護病毒碼相同的防護。 雲端截毒掃瞄病毒碼包含大多數病毒碼定義。本機雲端病毒碼包含雲端截毒掃瞄病毒碼中未包含的所有其他病毒碼定義。 Security Agent 使用本機雲端病毒碼掃瞄安全威脅。如果 Security Agent 在掃瞄期間無法判斷檔案的風險，就會傳送掃瞄查詢到掃瞄伺服器（由 Security Server 代管的服務），以確認風險。掃瞄伺服器會使用雲端截毒掃瞄病毒碼驗證該風險。Security Agent 會「快取」由掃瞄伺服器提供的掃瞄查詢結果，以提升掃瞄效能。
本機雲端病毒碼	使用雲端截毒掃瞄的 Security Agent	
損害清除及復原範本	Security Agent	「損害清除及復原範本」由損害清除及復原引擎用於辨識特洛伊木馬程式檔案和處理程序，以便引擎可將它們清除。
損害清除及復原引擎（32/64 位元）	Security Agent	「損害清除及復原引擎」可掃瞄並移除特洛伊木馬程式和特洛伊木馬程式處理程序。

元件	分發到	說明
記憶體檢測病毒碼	Security Agent	此技術提供針對多構式病毒和變體病毒的增強型病毒掃瞄，並模擬檔案執行來加強病毒碼式掃瞄。接著會在受控制的環境中分析結果以取得有關惡意企圖的證據，卻不會對系統效能造成明顯影響。
關聯式智慧引擎（32/64 位元）	Security Agent	關聯式智慧引擎會監控不常見的檔案所執行的程序、擷取其中的行為特徵，由關聯式智慧查詢處理程式傳送給 Machine Learning 引擎進行分析。
關聯式智慧型病毒碼	Security Agent	關聯式智慧型病毒碼包含「核可的」行為清單，其中所列行為與任何已知的安全威脅無關。
關聯式智慧查詢處理程式（32/64 位元）	Security Agent	關聯式智慧查詢處理程式會處理關聯式智慧引擎所識別的行為，然後將報告傳送給 Machine Learning 引擎。
進階威脅掃描引擎（32/64 位元）	Security Agent	進階威脅掃描引擎會從不常見的檔案中擷取檔案特徵，然後將該資訊傳送給 Machine Learning 引擎。
進階安全威脅關聯病毒碼	Security Agent	進階安全威脅關聯病毒碼包含一份檔案特徵清單，其中所列檔案特徵與任何已知的安全威脅無關。
Early Boot Cleanup 驅動程式（32/64 位元）	Security Agent	趨勢科技 Early Boot Cleanup 驅動程式會在作業系統驅動程式載入之前載入，以偵測和封鎖開機型 Rootkit。載入 Security Agent 之後，Early Boot Cleanup 驅動程式會調用「損害清除及復原服務」來清除 Rootkit。

表 8-4. 間諜程式防護

元件	分發到	說明
間諜程式/可能的資安威脅程式掃瞄引擎 v.6（32/64 位元）	Security Agent	間諜程式/可能的資安威脅程式掃瞄引擎會掃瞄間諜程式/可能的資安威脅程式，並對其執行適當的中毒處理行動。

元件	分發到	說明
間諜程式/可能的資安威脅程式病毒碼第 6 版	Security Agent	間諜程式/可能的資安威脅程式病毒碼可識別檔案和程式中的間諜程式/可能的資安威脅程式、記憶體中的模組、Windows 登錄和 URL 捷徑。
間諜程式/可能的資安威脅程式病毒碼	Security Agent	

表 8-5. 網路病毒

元件	分發到	說明
一般防火牆病毒碼	Security Agent	與病毒碼相同，一般防火牆病毒碼可協助用戶端識別病毒特徵（表明存在網路病毒的獨特位元和位元組病毒碼）。

表 8-6. 行為監控和周邊設備存取控管

元件	分發到	說明
行為監控偵測病毒碼（32/64 位元）	Security Agent	此病毒碼包含用於偵測可疑安全威脅行為的規則。
行為監控核心驅動程式（32/64 位元）	Security Agent	此核心模式驅動程式可監控系統事件，並將它們傳遞到「行為監控核心服務」以便進行策略實施。
行為監控核心服務（32/64 位元）	Security Agent	此使用者模式服務具有下列功能： • 提供 Rootkit 偵測 • 規範對於外部裝置的存取 • 保護檔案、登錄機碼和服務
行為監控配置特徵碼	Security Agent	「行為監控驅動程式」使用此特徵碼來識別正常系統事件，並將它們從策略實施排除。
損害還原病毒碼	Security Agent	損害還原病毒碼包含用來監控可疑安全威脅行為的策略。
數位簽章特徵碼	Security Agent	此特徵碼包含有效數位簽章清單，「行為監控核心服務」使用這些數位簽章來判斷負責系統事件的程式是否安全。

元件	分發到	說明
策略實施特徵碼	Security Agent	「行為監控核心服務」會根據此病毒碼中的策略來檢查系統事件。
記憶體掃瞄觸發病毒碼（32/64 位元）	Security Agent	記憶體掃瞄觸發服務偵測到記憶體中的處理程序解除封裝時，會執行其他掃瞄引擎。
程式檢測監控病毒碼	Security Agent	程式檢測監控病毒碼會監控和儲存用來行為監控的檢測點。
安全威脅追蹤病毒碼（32/64 位元）	Security Agent	安全威脅追蹤病毒碼會識別無檔案型態惡意程式攻擊。

表 8-7. 瀏覽器攻擊

元件	分發到	說明
瀏覽器弱點攻擊防護特徵碼	Security Agent	此病毒碼可識別最新網頁瀏覽器攻擊，並防止攻擊者利用這些攻擊對網頁瀏覽器造成危害。
程式檔分析器統一病毒碼	Security Agent	此病毒碼分析網頁中的程式檔並識別惡意程式檔。

表 8-8. Machine Learning

元件	分發到	說明
Machine Learning 本機檔案模型	Security Agent	當端點中斷與 Internet 的連線時，Machine Learning 本機檔案模型會識別可攜式可執行檔安全威脅。

HotFix、Patch 和 Service Pack

在產品正式發行之後，趨勢科技通常會開發下列項目來解決問題，以增強產品的效能或增加新功能：

- 重要修補程式 第 D-2 頁
- Hot Fix 第 D-2 頁

- 修補程式 第 D-8 頁
- Service Pack 第 D-22 頁

您的廠商或支援提供者會在這些項目可供使用時聯絡您。如需有關新的 Hot Fix、修補程式和 Service Pack 發行的資訊，請造訪趨勢科技網站：

http://www.trendmicro.com/download/zh-tw/

所有發行都有 Readme 檔，其中包含安裝、部署和組態設定資訊。請詳細閱讀 Readme 檔再執行安裝。

Security Server 更新

自動更新

Security Server 會自動執行下列更新：

- 安裝 Security Server 之後，它會立即從趨勢科技主動式更新伺服器進行更新。
- 每當 Security Server 啟動時，它都會更新元件。
- 依預設，預約更新會每小時執行一次（可以從 Web 主控台變更更新頻率）。

手動更新

如果更新比較緊急，您可以從 Web 主控台執行手動更新。

伺服器更新提醒和秘訣

- 進行更新之後，Security Server 會自動將元件更新分發到代理程式。如需有關分發到代理程式之元件的詳細資訊，請參閱可更新的元件 第 8-3 頁。
- 純 IPv6 Security Server 無法執行下列工作：
  - 直接從趨勢科技主動式更新伺服器或純 IPv4 自訂更新來源取得更新。
  - 將更新直接分發到純 IPv4 代理程式。

同樣地，純 IPv4 Security Server 也無法直接從純 IPv6 自訂更新來源取得更新，或將更新分發到純 IPv6 代理程式。

在這些情況下，如果要允許 Security Server 取得並分發更新，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

- 如果使用 Proxy 伺服器連線到 Internet，請在「管理 > 全域設定 > Proxy」標籤中，設定正確的 Proxy 伺服器設定以順利下載更新。

元件複製

趨勢科技會定期發行病毒碼檔案，讓您將用戶端防護保持在最新狀態。由於會定期提供病毒碼檔案更新，因此 Security Server 使用稱為「元件複製」的機制，讓您能夠更快下載病毒碼檔案。

當趨勢科技主動式更新伺服器上有最新版的完整病毒碼檔案可供下載時，也會同時提供漸增式病毒碼。漸增式病毒碼為完整病毒碼檔案的小型版本，僅提供最新版和之前完整病毒碼檔案版本之間的差異。例如，如果最新版為 175，則漸增式病毒碼 v_173.175 會包含 175 版中擁有，但 173 版中找不到的簽章（病毒碼號碼會以 2 為遞增單位發行，因此 173 版即為前一個完整病毒碼版本）。漸增式病毒碼 v_171.175 則包含 175 版中擁有，但 171 中找不到的簽章。

為了減少下載最新病毒碼時產生的網路流量，Security Server 會執行元件複製，使用這種元件更新方式時，伺服器僅會下載漸增式病毒碼。若要利用元件複製功能，請務必定期更新 Security Server。否則，伺服器將被強制下載完整的病毒碼檔案。

元件複製適用於下列元件：

- 病毒碼
- 本機雲端病毒碼
- 損害清除及復原範本
- IntelliTrap 例外病毒碼
- 間諜程式病毒碼

設定 Security Server 更新來源

開始之前

依預設，Security Server 會從趨勢科技主動式更新伺服器取得更新。如果 Security Server 無法直接連線至主動式更新伺服器，可指定自訂更新來源。

- 如果來源是「趨勢科技主動式更新伺服器」，請確定 Security Server 有 Internet 連線；如果使用 Proxy 伺服器，請測試是否可以使用 Proxy 伺服器設定建立 Internet 連線。如需詳細資訊，請參閱進行 Internet Proxy 伺服器設定 第 11-2 頁。
- 如果來源是自訂更新來源（「包含目前檔案複本的 Intranet 位置」或「替代的更新來源」），請設定此更新來源的適當環境和更新資源。此外，請確定 Security Server 與此更新來源之間的連線正常。如果需要設定更新來源的協助，請聯絡您的經銷商。
- 純 IPv6 Security Server 無法直接從趨勢科技主動式更新伺服器或任何純 IPv4 自訂更新來源進行更新。同樣地，純 IPv4 Security Server 也無法直接從純 IPv6 自訂更新來源進行更新。如果要允許 Security Server 連線至更新來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

步驟

1. 瀏覽至「更新 > 來源」。
2. 在「伺服器」標籤上，選取更新來源。
   - 趨勢科技主動式更新伺服器
   - 包含目前檔案複本的 Intranet 位置：輸入來源的通用命名慣例 (UNC) 路徑（例如 `\\Web\ActiveUpdate`）。此外，請指定 Security Server 將用於連線至此來源的登入認證（使用者名稱和密碼）。
   - 替代的更新來源：輸入此來源的 URL。請確定目標 HTTP 虛擬目錄（Web 共享）可供 Security Server 使用。
3. 按一下「儲存」。

手動更新 Security Server

安裝或升級 Security Server 之後，在病毒爆發時，需要手動更新 OfficeScan 伺服器元件。

步驟

1. 手動更新的啟動方式分為兩種：
   - 移至「更新 > 手動」。
   - 移至「即時狀態」，然後按一下「代理程式狀態」Widget 上的「檢查元件狀態」。

   「手動更新」畫面隨即顯示。
2. 選取要更新的元件。

   如需有關元件的詳細資訊，請參閱可更新的元件 第 8-3 頁。
3. 按一下「立即更新」。

   接著會顯示一個新畫面，顯示更新狀態。如果更新成功，Security Server 會將更新元件自動分發至代理程式。

為 Security Server 設定預約更新

設定 Security Server 定期檢查其更新來源並自動下載任何可用的更新檔。使用預約更新是確保安全威脅防護永遠保持最新狀態的簡單又有效的方法。

趨勢科技會在病毒/惡意程式爆發期間迅速更新病毒碼檔案（每週發出更新的次數可能不只一次）。掃瞄引擎與其他元件也會定期更新。趨勢科技建議您每天更新元件，並於病毒/惡意程式爆發時增加更新次數，以協助確保代理程式擁有最新的元件。

重要

避免將掃瞄和更新排定在同一個時間執行。如此可能會造成預約掃瞄無預期地中止。

步驟

1. 瀏覽至「更新 > 預約」。
2. 選取要更新的元件。

   如需有關元件的詳細資訊，請參閱可更新的元件 第 8-3 頁。
3. 按一下「預約」標籤，然後指定更新預約。
   - 標準掃瞄更新包括除雲端病毒碼和本機雲端病毒碼之外的所有元件。選擇每日、每週還是每月更新一次，然後為「更新持續時間為」指定一個值，以表示 Security Server 將在其間執行更新的時數。Security Server 會在此期間內的任何指定時間進行更新。

     注意

     對於每月一次的預約更新（不建議），如果您選取 31、30 或 29 日，但該月沒有該日期，則該月將不會執行更新。
   - 雲端截毒掃瞄更新僅包括雲端病毒碼和本機雲端病毒碼。如果您沒有任何代理程式使用雲端截毒掃瞄，則可略過此項目。
4. 按一下「儲存」。

還原元件

「還原」的意思是恢復到舊版「病毒碼」、「本機雲端病毒碼」和「病毒掃瞄引擎」。如果這些元件無法正常運作，請將它們還原成之前版本。Security Server 會保留目前和之前版本的「病毒掃瞄引擎」，以及最新三個版本的「病毒碼」和「本機雲端病毒碼」。

注意

只能還原上述元件。

Worry-Free Business Security 會針對執行 32 位元和 64 位元平台的代理程式使用不同的掃瞄引擎。您必須個別還原這些掃瞄引擎。所有掃瞄引擎類型的還原程序都相同。

步驟

1. 瀏覽至更新 > 還原。
2. 按一下特定元件的同步化，通知代理程式將其元件版本與伺服器上的版本進行同步。
3. 按一下特定元件的還原，在 Security Server 和代理程式上還原該元件。

Security Agent 和 Messaging Security Agent 更新

自動更新

Security Agent 和 Messaging Security Agent（僅限 Advanced 版）會自動執行下列更新：

- 安裝後，代理程式立即從 Security Server 進行更新。
- 每次 Security Server 完成更新時，會將更新自動發送至代理程式。
- 每次更新代理程式完成更新時，會將更新自動發送至各個 Security Agent。
- 依預設，預約更新執行頻率如下：
  - 在辦公室中 Security Agent 每隔 8 小時一次
  - 辦公室以外的地方 Security Agent 每隔 2 小時一次

- 依預設，Messaging Security Agent 會每隔 24 小時，在上午 12:00 執行一次預約更新。

執行手動更新

Security Agent 會自動從 Security Server 接收更新。

如果您已有一段時間未連線辦公室網路，或是迫切需要取得最新安全威脅防護（例如，在病毒爆發之後），您也可以手動進行更新。

如果您使用 Proxy 伺服器來連線 Internet，請確定您有正確的 Proxy 伺服器設定。

步驟

1. 開啟主畫面，然後請點選「更新」。

   注意

   您也可以在 Windows 工具列的 Security Agent 圖示上請點選右鍵，然後選取「立即更新」來執行手動更新。

2. 完成更新時，請點選「關閉」。

代理程式更新提醒和秘訣

- Security Agent 從 Security Server、更新代理程式或趨勢科技主動式更新伺服器進行更新。

  Messaging Security Agent 僅從 Security Server 進行更新。

  如需更新程序的詳細資訊，請參閱更新總覽 第 8-2 頁。

- 純 IPv6 代理程式無法直接從純 IPv4 Security Server/更新代理程式和趨勢科技主動式更新伺服器取得更新。

同樣地，純 IPv4 代理程式無法直接從純 IPv6 Security Server/更新代理程式取得更新。

此時，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate），代理程式才能取得更新。

- 如需代理程式所更新元件的詳細資訊，請參閱可更新的元件 第 8-3 頁。
- 代理程式從 Security Servere 更新時，除了元件，還會收到更新的組態設定檔。代理程式需要組態設定檔才能套用新設定。每一次您經由 Web 主控台修改代理程式設定時，組態設定檔都會變更。

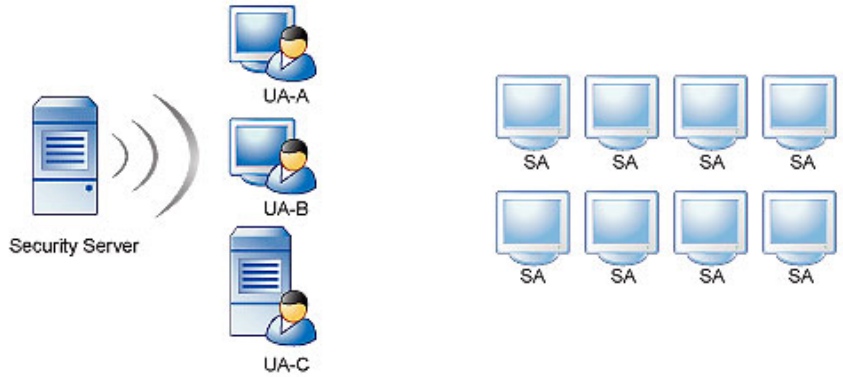
更新代理程式

更新代理程式即為 Security Agent，可從 Security Server 或主動式更新伺服器接收更新的元件，然後將元件部署到其他 Security Agent。

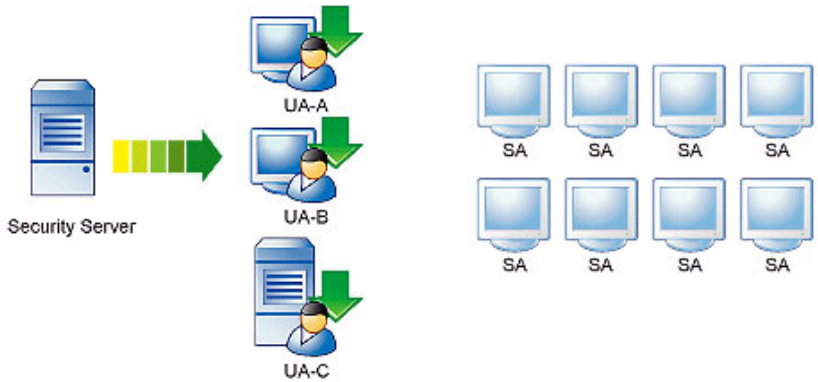
如果您認定用戶端和趨勢科技 Security Server 之間的網段為「低頻寬」或「高流量」，則可將 Security Agent 指定為更新代理程式。更新代理程式讓所有的 Security Agent 免於存取 Security Server 以取得元件更新，從而得以減少耗用的網路頻寬。如果您的網路是依照位置分段，而且各區段之間的網路連結經常發生高傳輸負載，則趨勢科技建議您在每個區段上至少讓一部 Security Agent 作為更新代理程式。

更新代理程式的更新過程可描述如下：

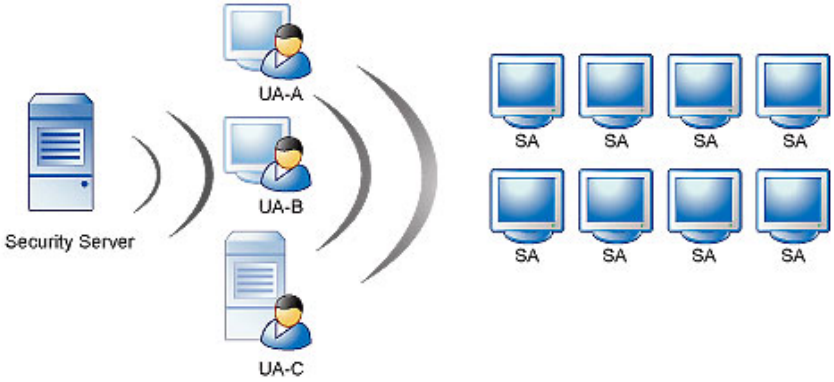
1. Security Server 會通知「更新代理程式」已發佈新的更新。



2. 更新代理程式會從 Security Server 下載更新的元件。

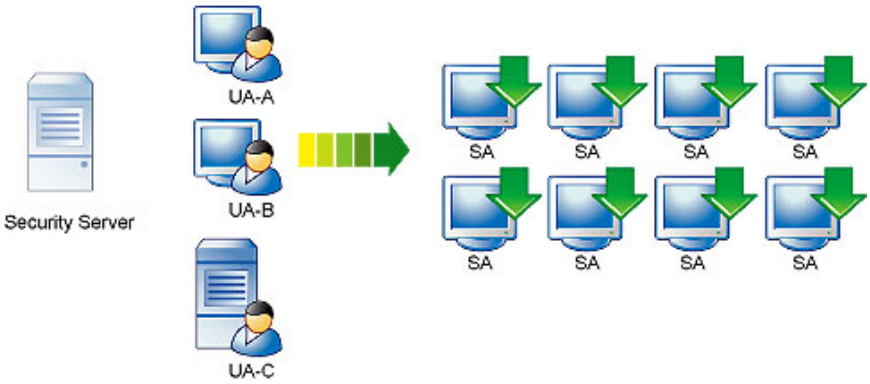


3. 接著，Security Server 會通知 Security Agent 已有可用的更新元件。



4. 每個 Security Agent 會載入一份更新代理程式順序表，以判斷其適用的更新來源。更新代理程式在更新代理程式順序表中的順序，最初取決於其在 Web 主控台上新增為替代更新來源的順序。每個 Security Agent 會從表中的第一個項目開始查起，一次查詢一個項目，直到辨識出其更新來源為止。

5. 接著，Security Agent 會從所指定的更新代理程式下載更新的元件。如果指定的更新代理程式因故而無法使用，Security Agent 將嘗試從 Security Server 下載更新的元件。



設定更新代理程式

步驟

1. 瀏覽至「更新 > 來源」。
2. 按一下「更新代理程式」標籤。
3. 執行下列工作：

工作	步驟
將 Security Agent 指定為更新代理程式	a. 在「指定更新代理程式」區段中，按一下「新增」。 接著會開啟一個新畫面。 b. 從清單方塊中，選取一個或多個代理程式做為更新代理程式。 c. 按一下「儲存」。 畫面隨即關閉。 d. 如果您希望更新代理程式永遠從 Security Server（而不是其他更新代理程式）下載更新的元件，請返回「指定更新代理程式」區段，並選取「更新代理程式一律只直接從 Security Server 進行更新」。

工作	步驟
將 Security Agent 設定為從更新代理程式進行更新	a. 在「替代的更新來源」區段中，選取「啟動 Security Agent 和更新代理程式的替代更新來源」。 注意 關閉此選項可阻止 Security Agent 從更新代理程式進行更新，從而有效地將其更新來源切換回 Security Server。 b. 按一下「新增」。 接著會開啟一個新畫面。 c. 輸入將從更新代理程式進行更新之 Security Agent 的 IP 位址。 • 輸入 IPv4 位址範圍。 若要指定單一 Security Agent，請在「起始範圍」和「結束範圍」欄位中輸入 Security Agent 的 IP 位址。 • 對於 IPv6，請輸入 IP 字首和長度。 d. 從下拉式清單中選取更新代理程式。 如果沒有可用的下拉式清單，表示尚未設定任何更新代理程式。 e. 按一下「儲存」。 畫面隨即關閉。 f. 視需要定義更多 IP 範圍。如果已定義多個 IP 範圍，您可以使用「重新排列順序」選項，設定 IP 範圍優先順序。當 Security Server 通知 Security Agent 已有可用的更新時，Security Agent 會掃瞄 IP 範圍清單以辨識其正確的更新來源。Security Agent 會從清單中的第一個項目開始向下掃瞄，直到辨識出其正確的更新來源為止。 秘訣 可為相同 IP 範圍定義多個更新代理程式做為容錯移轉措施。這樣做意味著：如果 Security Agent 無法從某更新代理程式進行更新，則會嘗試其他更新代理程式。若要如此，請至少建立兩 (2) 個 IP 範圍相同的項目，並為每個項目指定不同的更新代理程式。

工作	步驟
移除更新代理程式	若要移除某更新代理程式並取消指定已為其指定的所有 Security Agent，請移至「指定更新代理程式」區段，並選取該更新代理程式的電腦名稱所對應的核取方塊，然後按一下「移除」。 此動作不會移除「替代的更新來源」區段中的 Security Agent IP 位址範圍，而只會導致「孤立的」Security Agent 將其更新來源切換回 Security Server。如果您有其他更新代理程式，可以將其指定給該孤立的 Security Agent。
取消 Security Agent 的更新代理程式指定	如果不再希望 Security Agent 屬於從某更新代理程式進行更新的 IP 位址範圍，請移至「替代的更新來源」區段，並選取該 Security Agent 的 IP 位址範圍所對應的核取方塊，然後按一下「移除」。

4. 按一下「儲存」。

第 9 章

使用即時狀態

即時狀態

Worry-Free Business Security 提供用作快速視覺參考的 Widget，用於協助管理 Security Agent。

「即時狀態」畫面會在開啟 Worry-Free Business Security Web 主控台或在主功能表中按一下「即時狀態」時顯示。

表 9-1. 即時狀態 Widget

WIDGET	說明
處理行動中心	此 Widget 顯示需要管理員採取處理行動解決問題的事件。
歷來的安全威脅偵測	此 Widget 概述網路中偵測到威脅的端點以及特定時間範圍內影響網路的威脅類型。
勒索軟體摘要	此 Widget 概述指定時間範圍內所有嘗試過的勒索軟體攻擊。
使用授權狀態	此 Widget 概述您的使用授權的授權使用情況和到期狀態。
Exchange Server 摘要	此 Widget 提供 Messaging Security Agent 連線狀態以及 Exchange Server 上偵測到的安全威脅散佈情況的總覽。
代理程式狀態	此 Widget 概述網絡中 Security Agent 的連線和更新狀態。

在「即時狀態」畫面中，資訊的重新整理速率會依區段而有所不同。一般而言，重新整理速率介於 1 到 10 分鐘之間。如果要手動重新整理畫面資訊，請按一下瀏覽器的「重新整理」按鈕。

處理行動中心

此 Widget 顯示需要管理員採取處理行動解決問題的事件。

有些事件隨附有建議的處理行動按鈕。按一下這些按鈕可嘗試解決這些問題，也可按一下事件檢視更多詳細資訊。

表 9-2. 處理行動中心事件

事件	建議
防毒 - 尚未解決的安全威脅	使用 Trend Micro HouseCall 工具執行掃瞄。
防毒 — 端點上的即時掃瞄已關閉	在所有裝置上啟動即時掃瞄，以持續受到保護。
防毒 — Exchange Server 上的即時掃瞄已關閉	在所有 Exchange Server 上啟動即時掃瞄，以持續受到保護。
間諜程式防護 - 需要重新啟動裝置的偵測數	重新啟動裝置，以完全移除偵測到的安全威脅。
使用授權相關事件	移至「管理 > 產品使用授權」來檢查使用授權狀態。
資源短缺 — 剩餘的磁碟空間少於 %threshold%	執行 Disk Cleaner 工具來刪除未使用的備份檔、記錄檔和病毒碼檔案。 如需詳細資訊，請參閱節省磁碟空間 第 14-13 頁。
主動式雲端截毒技術服務 — 服務無法使用	在 Worry-Free Business Security 主控台上檢查雲端截毒伺服器狀態，並確保該伺服器處於正常運作中。
更新 — 在病毒碼發行 1 小時過後至少有一個過期的 Messaging Security Agent	請確保已在 Security Server 上啟動 Messaging Security Agent 的預約更新，且 Messaging Security Agent 可連線到 Internet。
更新 — 部署率於病毒碼發行 1 小時過後低於 %threshold%	請檢查 Security Agent 的 Internet 連線，然後再次更新 Security Agent。
更新 — 已超過 %threshold% 天未更新 Security Server 元件	請確保已在 Security Server 上啟動元件的預約更新，且 Security Server 可連線到 Internet。
更新 — 已超過 %threshold% 小時未更新雲端病毒碼	請確保已在 Security Server 上啟動雲端病毒碼的預約更新，且 Security Server 可連線到 Internet。

防毒：尚未解決的安全威脅

您可以按一下處理行動中心中的「防毒 - 尚未解決的安全威脅：%N%」事件，檢視此資訊。每當發生即時掃瞄、手動掃瞄或預約掃瞄時，Worry-Free Business Security 都會產生或更新此記錄資訊。

- 按一下「下載工具」以下載趨勢科技 HouseCall 工具，並使用此工具在受影響的裝置上執行掃瞄。
- 按一下「從處理行動中心消除」以重新導向至「即時狀態」畫面，然後從處理行動中心移除通知事件。與此畫面上的事件相關的記錄檔仍透過記錄查詢提供。
- 按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	上次清除或移除病毒或惡意程式不成功的日期和時間
裝置名稱	受影響的裝置的名稱
病毒/惡意程式名稱	偵測到的病毒或惡意程式的名稱 按一下連結之後將被重新導向到「趨勢科技安全威脅百科全書」，您可以在該處找到有關安全威脅的詳細說明，包括手動清除此特定安全威脅對系統造成之攻擊的指示。
檔案名稱	病毒或惡意程式損毀的檔案的名稱
路徑	中毒檔案的位置
掃瞄類型	用於偵測病毒或惡意程式的掃瞄類型
中毒處理行動	Worry-Free Business Security 為回應病毒或惡意程式偵測而採取的中毒處理行動

防毒：端點上的即時掃瞄已關閉

透過在處理行動中心按一下「防毒 — 端點上的即時掃瞄已關閉：%N%」事件，即可檢視此資訊。

- 按一下「啟動即時掃瞄」，以在所有裝置上啟動掃瞄。
- 按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
裝置名稱	已關閉即時掃瞄的裝置名稱
群組名稱	裝置所屬群組的名稱

防毒：Exchange Server 上的即時掃瞄已關閉

透過在處理行動中心按一下「防毒 — Exchange Server 上的即時掃瞄已關閉：%N%」事件，即可檢視此資訊。

- 按一下「啟動即時掃瞄」，以在所有 Exchange Server 上啟動掃瞄。
- 按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
Exchange Server 名稱	已關閉即時掃瞄的 Exchange Server 名稱

間諜程式防護：需要重新啟動裝置的偵測

您可以按一下處理行動中心中的「間諜程式防護 - 需要重新啟動裝置的偵測：%N%」事件，檢視此記錄檔資訊。

- 按一下「從處理行動中心消除」以重新導向至「即時狀態」畫面，然後從處理行動中心移除通知事件。與此畫面上的事件相關的記錄檔仍透過記錄查詢提供。
- 按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 將間諜程式或可能的資安威脅程式偵測資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	受影響的裝置的名稱
間諜程式/可能的資安威脅程式名稱	偵測到的間諜程式/可能的資安威脅程式名稱 按一下連結之後將被重新導向到「趨勢科技安全威脅百科全書」，您可以在該處找到有關安全威脅的詳細說明，包括手動清除此特定安全威脅對系統造成之攻擊的指示。
掃瞄類型	用於偵測間諜程式或可能的資安威脅程式的掃瞄類型

資源短缺 — 剩餘的磁碟空間

透過在處理行動中心按一下「資源短缺 — 剩餘的磁碟空間少於 %threshold %」事件，即可檢視此資訊。

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
伺服器名稱	磁碟空間不足的伺服器名稱
群組名稱	伺服器所屬群組的名稱

更新：已過期的代理程式

在處理行動中心按一下「更新：部署率於病毒碼發行 1 小時過後低於 %threshold%」事件，即可檢視此資訊。此畫面上列出的 Security Agent 需要進行引擎或病毒碼更新。

- 按一下「立即更新」以通知過期的 Security Agent 來更新至最新元件。
- 按一下「檢查元件狀態」來開啟「手動更新」畫面。
- 按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
裝置名稱	需要進行元件更新的裝置名稱
群組名稱	裝置所屬群組的名稱
掃瞄方法	• 雲端截毒掃瞄 • 標準掃瞄

更新 — 已過期的 Messaging Security Agent

透過在處理行動中心按一下「更新 — 在病毒碼發行 1 小時過後至少有一個過期的 Messaging Security Agent」事件，即可檢視此資訊。

- 按一下「立即更新」以通知過期的 Messaging Security Agent 來更新至最新元件。
- 按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
Exchange Server 名稱	需要進行元件更新的 Exchange Server 名稱

歷來的安全威脅偵測

此 Widget 概述網路中偵測到威脅的端點以及特定時間範圍內影響網路的威脅類型。

- 按一下 或 可在不同檢視之間切換。
- 按一下「已知安全威脅」、「未知安全威脅」或「策略違規」標籤，可檢視特定安全威脅的偵測資訊。

檢視	說明
圖形 ( )	• 按一下圖形下方的威脅類型名稱，以顯示/隱藏圖形上的偵測資訊。 • 將游標懸停在任一特殊日期的節點上，以檢視顯示的威脅類型的偵測總數。按一下某個節點以重新導向至清單中反白顯示的威脅類型的記錄檔畫面。
表格 ( )	• 按一下偵測計數，以開啟記錄檔畫面，其中列出了偵測詳細資訊。

安全威脅偵測：病毒/惡意程式

您可以在「歷來的安全威脅偵測」Widget 上的「已知安全威脅」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「病毒/惡意程式」偵測計數
- 圖形檢視中的任何「病毒/惡意程式」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 向 Worry-Free Business Security 報告病毒或惡意程式偵測資訊的日期和時間
裝置名稱	受影響的裝置的名稱
病毒/惡意程式名稱	偵測到的病毒或惡意程式的名稱 按一下連結之後將被重新導向到「趨勢科技安全威脅百科全書」，您可以在該處找到有關安全威脅的詳細說明，包括手動清除此特定安全威脅對系統造成之攻擊的指示。
檔案名稱	病毒或惡意程式損毀的檔案的名稱
路徑	中毒檔案的位置
掃瞄類型	用於偵測病毒或惡意程式的掃瞄類型

欄	說明
中毒處理行動	Worry-Free Business Security 為回應病毒或惡意程式偵測而採取的中毒處理行動

安全威脅偵測：間諜程式/可能的資安威脅程式

您可以在「歷來的安全威脅偵測」Widget 上的「已知安全威脅」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「間諜程式/可能的資安威脅程式」偵測計數
- 圖形檢視中的任何「間諜程式/可能的資安威脅程式」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 將間諜程式或可能的資安威脅程式偵測資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	受影響的裝置的名稱 按一下名稱，以查看該裝置上偵測到的個別間諜程式或可能的資安威脅程式清單。
間諜程式/可能的資安威脅程式名稱	偵測到的間諜程式/可能的資安威脅程式名稱
掃瞄類型	用於偵測間諜程式或可能的資安威脅程式的掃瞄類型
中毒處理行動	Worry-Free Business Security 為回應間諜程式或可能的資安威脅程式偵測而採取的中毒處理行動

安全威脅偵測：網頁信譽評等

您可以在「歷來的安全威脅偵測」Widget 上的「已知安全威脅」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「網頁信譽評等」偵測計數

- 圖形檢視中的任何「網頁信譽評等」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 將 URL 違規資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	嘗試存取受限制 URL 的裝置的名稱
URL	受限制的 URL
風險等級	TrendLabs 根據感染方式的簡易度和潛在損害指定的分級。

安全威脅偵測：網路病毒

您可以在「歷來的安全威脅偵測」Widget 上的「已知安全威脅」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「網路病毒」偵測計數
- 圖形檢視中的任何「網路病毒」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 向 Worry-Free Business Security 報告網路病毒偵測資訊的日期和時間
裝置名稱	受影響的裝置的名稱
攻擊者的 IP	攻擊者的 IP 位址
受害者的 IP	受害者的 IP 位址
封包方向	封包的方向
網路病毒名稱	偵測的網路病毒名稱

欄	說明
總數	每個網路病毒在每次偵測到時均會計算一次。

安全威脅偵測：行為監控

您可以在「歷來的安全威脅偵測」Widget 上的「未知安全威脅」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「行為監控」偵測計數
- 圖形檢視中的任何「行為監控」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

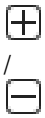
欄	說明
日期/時間	Security Agent 將行為監控違規資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	觸發策略違規的裝置的名稱
安全威脅	安全威脅的類型
主旨	作業的主旨
事件類型	相關的系統事件
目標	作業的目標
作業	由使用者執行的觸發違規的作業
結果	Worry-Free Business Security 為回應行為監控違規而採取的中毒處理行動

安全威脅偵測：Machine Learning

您可以在「歷來的安全威脅偵測」Widget 上的「未知安全威脅」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「Machine Learning」偵測計數
- 圖形檢視中的任何「Machine Learning」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
	按一下圖示，以展開或關閉資料表列下方的記錄詳細資訊。
日期/時間	Security Agent 將偵測資訊回報給 Worry-Free Business Security 日期和時間
裝置名稱	受影響的裝置的名稱
群組名稱	裝置所屬群組的名稱
未知安全威脅	可能的安全威脅名稱
安全威脅可能性	指出檔案/程序符合惡意程式模型的程度
檔案名稱	執行程序的檔案物件或程式名稱 重要 此偵測所偵測到的檔案名稱可能與其他端點上所偵測到的檔案名稱不同。Machine Learning 是依檔案雜湊值將偵測項目彼此關聯，而非依特定檔案名稱。
路徑	執行程序的檔案物件路徑或程式路徑
感染管道	安全威脅的來源通道
中毒處理行動	Worry-Free Business Security 為了回應偵測而採取的處理行動

安全威脅偵測：Machine Learning 詳細資訊

在「安全威脅偵測：Machine Learning」記錄檔畫面上按一下第一欄中的任何
圖示，即可檢視此資訊。

記錄詳細資訊區段包含兩個標籤：

- 未知安全威脅：提供 Machine Learning 分析的結果
- 檔案名稱：針對此特定偵測記錄檔，提供與檔案內容和憑證資訊相關的一般詳細資料

秘訣

請按一下「新增到例外清單」，以快速將受影響檔案的檔案雜湊值新增到全域的 Machine Learning 例外清單。在「全域設定」畫面上，檢視完整的例外清單。

如需詳細資訊，請參閱設定例外清單設定 第 11-12 頁。

下表說明「未知安全威脅」標籤上提供的資訊。

表 9-3. 未知安全威脅標籤詳細資訊

項目	說明
安全威脅可能性	指出檔案/程序符合惡意程式模型的程度
可能的安全威脅類型	指出 Machine Learning 在將分析結果與其他已知的安全威脅相比較後，所發現檔案中最可能包含的安全威脅類型
安全威脅識別碼	列出檔案/程序中所使用、可能指示出現了所偵測安全威脅類型的 API 函數。 **重要** 判斷安全威脅類型時，API 函數識別是唯一一個考量因素。Machine Learning 會使用其他許多檔案特徵與分析方法，來計算安全威脅可能性和可能的安全威脅類型。

項目	說明
偵測類型	觸發偵測的物件類型（「檔案」或「程序」）
類似的已知安全威脅	列出已知會展現出與此偵測類似之檔案/程序特徵的安全威脅類型

安全威脅偵測：URL 過濾

您可以在「歷來的安全威脅偵測」Widget 上的「策略違規」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「URL 過濾」偵測計數
- 圖形檢視中的任何「URL 過濾」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 將 URL 違規資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	嘗試存取受限制 URL 的裝置的名稱
URL	受限制的 URL

安全威脅偵測：周邊設備存取控管

您可以在「歷來的安全威脅偵測」Widget 上的「策略違規」標籤上，按一下以下其中一個連結來檢視此資訊：

- 表格檢視中的「周邊設備存取控管」偵測計數
- 圖形檢視中的任何「周邊設備存取控管」節點

按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 向 Worry-Free Business Security 報告周邊設備存取控管違規資訊的日期和時間
裝置名稱	觸發策略違規的裝置的名稱
類型	儲存裝置的類型
權限	為儲存裝置設定的權限
主旨	作業的主旨
物件	作業的物件
作業	作業已完成

勒索軟體摘要

此 Widget 概述指定時間範圍內所有嘗試過的勒索軟體攻擊。

預設檢視顯示所有勒索軟體偵測的摘要，並根據感染通道進一步對嘗試進行分類。

- 在預設檢視上按一下勒索軟體偵測計數，以開啟「勒索軟體摘要」記錄檔畫面，其中列出了勒索軟體偵測詳細資訊。
- 使用下拉式清單可在不同檢視之間切換。

按一下 可在圖表中顯示偵測資訊。

- 將游標懸停在任一特殊日期的節點上，以檢視顯示的偵測類別的偵測總數。按一下某個節點以重新導向至「勒索軟體摘要」記錄檔畫面，其中列出了該特定日期的勒索軟體偵測詳細資訊。

勒索軟體摘要記錄

透過在「勒索軟體摘要」Widget 中的圖形或偵測計數上按一下節點，即可檢視此資訊。

- 使用「感染管道」和「期間」清單調整視圖。
- 按一下「匯出」以將記錄事件儲存為 CSV 檔案。

欄	說明
日期/時間	Security Agent 將勒索軟體偵測資訊向 Worry-Free Business Security 回報的日期和時間
安全威脅	勒索軟體類型 • 病毒/惡意程式名稱：顯示已知勒索軟體檔案的偵測名稱 • 未經授權的檔案加密：Worry-Free Business Security 偵測到可疑程式加密了檔案時即顯示 • <URL>：Worry-Free Business Security 偵測到與勒索軟體相關的已知 URL 時即顯示
Source	偵測到安全威脅的掃瞄類型
路徑/URL	• 勒索軟體的檔案路徑 • 感染勒索軟體的 URL
中毒處理行動	Worry-Free Business Security 為回應勒索軟體偵測而採取的中毒處理行動
裝置名稱	受影響的裝置的名稱
感染管道	勒索軟體偵測的管道
詳細資訊	按一下「檢視」以查看記錄檔詳細資訊。

勒索軟體：行為監控記錄詳細資訊

您可以按一下「勒索軟體摘要」記錄檔畫面上「詳細資訊」欄中的「檢視」連結，檢視此資訊。

列	說明
日期/時間	Security Agent 將行為監控違規資訊向 Worry-Free Business Security 回報的日期和時間

列	說明
裝置名稱	觸發策略違規的裝置的名稱
安全威脅	安全威脅的類型
主旨	作業的主旨
事件類型	相關的系統事件
目標	作業的目標
作業	由使用者執行的觸發違規的作業
結果	Worry-Free Business Security 為回應行為監控違規而採取的中毒處理行動

勒索軟體：URL 過濾記錄檔詳細資訊

您可以按一下「勒索軟體摘要」記錄檔畫面上「詳細資訊」欄中的「檢視」連結，檢視此資訊。

列	說明
日期/時間	Security Agent 將 URL 違規資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	嘗試存取受限制 URL 的裝置的名稱
URL	受限制的 URL
URL 類別	受限制的 URL 的類別
中毒處理行動	Worry-Free Business Security 為回應 URL 違規而採取的中毒處理行動

勒索軟體：病毒記錄檔詳細資訊

您可以按一下「勒索軟體摘要」記錄檔畫面上「詳細資訊」欄中的「檢視」連結，檢視此資訊。

列	說明
日期/時間	Security Agent 將勒索軟體偵測資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	受影響的裝置的名稱
病毒/惡意程式名稱	偵測到的勒索軟體的名稱 按一下連結之後將被重新導向到「趨勢科技安全威脅百科全書」，您可以在該處找到有關安全威脅的詳細說明，包括手動清除此特定安全威脅對系統造成之攻擊的指示。
檔案名稱	勒索軟體損毀的檔案的名稱
路徑	中毒檔案的位置
感染管道	勒索軟體藉以存取端點的媒體
掃瞄類型	用於偵測勒索軟體的掃瞄類型
中毒處理行動	Worry-Free Business Security 為回應勒索軟體偵測而採取的中毒處理行動

勒索軟體：網頁信譽評等記錄檔詳細資訊

您可以按一下「勒索軟體摘要」記錄檔畫面上「詳細資訊」欄中的「檢視」連結，檢視此資訊。

列	說明
日期/時間	Security Agent 將 URL 違規資訊向 Worry-Free Business Security 回報的日期和時間
裝置名稱	嘗試存取受限制 URL 的裝置的名稱
URL	受限制的 URL
風險等級	TrendLabs 根據感染方式的簡易度和潛在損害指定的分級。
中毒處理行動	Worry-Free Business Security 為回應 URL 違規而採取的中毒處理行動

使用授權狀態

此 Widget 概述您的使用授權的授權使用情況和到期狀態。

Exchange Server 摘要

此 Widget 提供 Messaging Security Agent 連線狀態以及 Exchange Server 上偵測到的安全威脅散佈情況的總覽。

按一下安全層級，為 Messaging Security Agent 設定垃圾郵件偵測等級。

欄	說明
Server	Exchange Server 的名稱
事件	電子郵件垃圾郵件的類型
比率	等於偵測數目除以已掃瞄的郵件數目

代理程式狀態

此 Widget 概述網絡中 Security Agent 的連線和更新狀態。

- 按一下狀態旁的計數，以重新導向至「裝置」畫面，此畫面會列出該特定狀態的裝置詳細資訊。
- 按一下「新增裝置，以重新導向至「新增裝置」畫面，您可以在此畫面中將 Security Agent 安裝到更多裝置上。

  如需詳細資訊，請參閱安裝代理程式 第 3-1 頁。
- 按一下「檢查元件狀態」，以重新導向至「手動更新」畫面，您可以在此畫面中檢視最新元件資訊。

  如需詳細資訊，請參閱可更新的元件 第 8-3 頁。

第 10 章

管理通知

本章說明如何使用不同的通知選項。

使用通知

若要將管理員監控 Worry-Free Business Security 所需的時間量降至最低，並確保管理員可透過電子郵件提前收到警告，掌握即將到來的疫情爆發狀況，請將伺服器設定為網路上一發生異常的事件時即傳送通知。

依預設，「通知」畫面中列出的所有事件均會被選取，並觸發伺服器傳送通知給管理員。

表 10-1. 需要採取處理行動通知

事件類型	說明
安全威脅事件	
防毒 - 尚未解決的安全威脅	對病毒/惡意程式採取的中毒處理行動失敗。 偵測計數不包括下列掃瞄中毒處理行動：暫不處理潛在的安全威脅
防毒 — 端點上的即時掃瞄已關閉	端點上的即時掃瞄已關閉。
防毒 — Exchange Server 上的即時掃瞄已關閉	Exchange Server 上的即時掃瞄已關閉。
間諜程式防護 - 需要重新啟動裝置的偵測數	偵測到有間諜程式/可能的資安威脅程式的端點需要重新啟動，才能完全移除安全威脅。
系統事件	
更新 — 已過期的代理程式	過期的 Security Agent 需要元件更新。
更新 — 已過期的 Messaging Security Agent	過期的 Messaging Security Agent 需要元件更新。
更新 — 已過期的雲端病毒碼	過期的雲端病毒碼需要病毒碼更新。
更新 — 已過期的 Security Server 元件	過期的 Security Server 需要元件更新。
主動式雲端截毒技術服務 — 服務無法使用	設定為使用雲端截毒掃瞄的 Security Agent 無法連線至主動式雲端截毒技術服務，或者無法使用此服務。

事件類型	說明
資源短缺 — 剩餘的磁碟空間	部分伺服器上的剩餘磁碟空間量低於指定的百分比。
使用授權事件	
使用授權 — 已到期	使用授權已到期。
使用授權 — 將在 60 天內到期	使用授權即將到期。
使用授權 — 授權數目的使用率大於 110%	授權數目的使用率大於 110%。
使用授權 — 授權數目的使用率大於 100%	授權數目的使用率大於 100%。

表 10-2. 警告通知

事件類型	說明
安全威脅事件	
防毒 — 端點上偵測到的病毒超過：	端點上偵測到的病毒/惡意程式安全威脅在指定時間範圍內超過指定的數目。
防毒 — Exchange Server 上偵測到的病毒超過：	Exchange Server 上偵測到的病毒/惡意程式安全威脅在指定時間範圍內超過指定的數目。
間諜程式防護 — 偵測到的間諜程式/可能的資安威脅程式超過：	端點上偵測到的間諜程式/可能的資安威脅程式安全威脅在指定時間範圍內超過指定的數目。
垃圾郵件防護 — 在已接收的所有郵件中偵測到的垃圾郵件超過：	在已接收的所有郵件中偵測到的垃圾郵件超過指定的百分比。
網頁信譽評等 — URL 違規超過：	URL 違規在指定時間範圍內超過指定的數目。
URL 過濾 — URL 違規超過：	URL 違規在指定時間範圍內超過指定的數目。
Machine Learning — 偵測到的未知安全威脅超過：	偵測到的未知安全威脅在指定時間範圍內超過指定的數目。
行為監控 — 行為監控違規超過：	行為監控違規在指定時間範圍內超過指定的數目。

事件類型	說明
網路病毒 — 偵測到的網路病毒超過：	偵測到的網路病毒在指定時間範圍內超過指定的數目。
周邊設備存取控管 — 周邊設備存取控管違規超過：	周邊設備存取控管違規在指定時間範圍內超過指定的數目。

設定通知事件

Worry-Free Business Security 提供三種方法來傳送通知：

- SNMP 通知
- Windows 事件記錄檔
- 電子郵件通知

步驟

1. 移至「管理 > 通知」。
2. 若要接收 SNMP 通知，請設定「SNMP 通知的收件人」區段。

   簡易網路管理通訊協定 (SNMP) 是網路管理所使用的通訊協定。如果要檢視 SNMP Trap 的資料，請使用 Management Information Base 瀏覽器。

   a. 選取「啟動 SNMP 通知」。

   b. 指定 SNMP Trap 的 IP 位址。

   c. 指定 SNMP 社群字串。
3. 若要接收 Windows 事件記錄檔通知，請在「記錄」下選取「寫入 Windows 事件記錄檔。
4. 若要接收電子郵件通知，請指定寄件人和收件者。

秘訣

以半形分號 (;) 分隔多個項目。

5. 按一下「需要採取處理行動或「警告」標籤。
6. 在「電子郵件通知」欄中選取您要接收其相關通知的事件類型所對應的核取方塊。
7. 如果在「警訊門檻值」欄中可用，請指定觸發通知的每個時間範圍內偵測或違規的數目。
8. 若要自訂每個事件通知的主旨行與郵件內文，請按一下「類型」欄中的通知連結。

   如需有關自訂通知的詳細資訊，請參閱 Token 變數 第 10-5 頁。
9. 按一下「儲存」。

Token 變數

可使用 Token 變數自訂事件通知的主旨行和郵件內文。

為了避免來自外部網域地址的郵件被歸類為垃圾郵件，請將外部電子郵件信箱加入「垃圾郵件防護」的「核可的寄件人」清單中。

下列 Token 代表在桌上型電腦/伺服器以及 Microsoft Exchange Server 上偵測到的安全威脅事件。

TOKEN	說明	警訊類型
%COUNT	插入偵測數目	警告事件：所有
$CSM_SERVERNAME	插入 Security Server 的名稱	全部
%DATE	插入使用授權的剩餘天數	使用授權 — 已到期 使用授權 — 將在 60 天內到期

TOKEN	說明	警訊類型
%DATE_TIME	插入事件的時間和日期	防毒 - 尚未解決的安全威脅 防毒 — 端點上的即時掃瞄已關閉 防毒 — Exchange Server 上的即時掃瞄已關閉 間諜程式防護 - 需要重新啟動裝置的偵測數 更新 — 已過期的代理程式 更新 — 已過期的 Messaging Security Agent 更新 — 已過期的 Security Server 元件 主動式雲端截毒技術服務 — 服務無法使用 資源短缺 — 剩餘的磁碟空間

TOKEN	說明	警訊類型
%DEVICE_COUNT	插入受影響的裝置數目	防毒 - 尚未解決的安全威脅 防毒 — 端點上的即時掃瞄已關閉 防毒 — Exchange Server 上的即時掃瞄已關閉 間諜程式防護 - 需要重新啟動裝置的偵測數 更新 — 已過期的代理程式 更新 — 已過期的 Messaging Security Agent 資源短缺 — 剩餘的磁碟空間 除下列項目之外的所有警告事件： 垃圾郵件防護 — 在已接收的所有郵件中偵測到的垃圾郵件超過：
%FROM	插入事件的開始時間和日期	除下列項目之外的所有警告事件： 垃圾郵件防護 — 在已接收的所有郵件中偵測到的垃圾郵件超過：

TOKEN	說明	警訊類型
%NUMBER	列出事件數目	防毒 - 尚未解決的安全威脅 防毒 — 端點上的即時掃瞄已關閉 防毒 — Exchange Server 上的即時掃瞄已關閉 間諜程式防護 - 需要重新啟動裝置的偵測數 除下列項目之外的所有警告事件： 垃圾郵件防護 — 在已接收的所有郵件中偵測到的垃圾郵件超過：
%SEAT_IN_USE_COUNT	插入正在使用的桌上型電腦/伺服器授權數目	使用授權 - 授權數目的使用率大於 110% 使用授權 - 授權數目的使用率大於 100%
%SEAT_PURCHASED_COUNT	插入使用授權提供的桌上型電腦/伺服器授權數目	使用授權 - 授權數目的使用率大於 110% 使用授權 - 授權數目的使用率大於 100%

TOKEN	說明	警訊類型
%THRESHOLD%	提供事件的門檻值	更新 — 已過期的代理程式 更新 — 已過期的雲端病毒碼 更新 — 已過期的 Security Server 元件 主動式雲端截毒技術服務 — 服務無法使用 資源短缺 — 剩餘的磁碟空間 使用授權 — 授權數目的使用率大於 110% 使用授權 — 授權數目的使用率大於 100% 警告事件：所有
%TO	插入事件的結束時間和日期	除下列項目之外的所有警告事件： 垃圾郵件防護 — 在已接收的所有郵件中偵測到的垃圾郵件超過：

```
主旨：[Security Server - <$CSM_SERVERNAME>] [需要
採取處理行動] 防毒 — 尚未解決的安全威脅：%NUMBER
訊息：Trend Micro Worry-Free Business Security 通知
* 防毒 — 尚未解決的安全威脅：%NUMBER
* 報告時間：%DATE_TIME
* 受影響的裝置：%DEVICE_COUNT
* 建議：
  使用 Trend Micro HouseCall 工具執行掃瞄。
```

```
主旨：[Security Server - 伺服器 A] [需要採取處理行動]
防毒 — 尚未解決的安全威脅：5
訊息：Trend Micro Worry-Free Business Security 通知
* 防毒 — 尚未解決的安全威脅：5
* 報告時間：2018 年 2 月 14 日
* 受影響的裝置：2
```

```
* 建議：
  使用 Trend Micro HouseCall 工具執行掃瞄。
```

第 11 章

管理全域設定

本章討論 Security Server 的代理程式和系統設定的全域設定。

全域設定

您可以從 Web 主控台設定 Security Server 和 Security Agent 的全域設定。

標籤	說明
Proxy	如果您的網路使用 Proxy 伺服器與 Internet 連線，請指定下列服務的 Proxy 伺服器設定： • 元件更新與使用授權通知 • 網頁信譽評等、行為監控與雲端截毒掃瞄 如需詳細資訊，請參閱進行 Internet Proxy 伺服器設定 第 11-2 頁。
SMTP	SMTP 伺服器設定會套用至 Security Server 所產生的所有通知和報告。 如需詳細資訊，請參閱進行 SMTP 伺服器設定 第 11-4 頁。
桌上型電腦/伺服器	這些安全設定會套用至所有 Security Agent。 如需詳細資訊，請參閱進行桌上型電腦/伺服器設定 第 11-4 頁。
系統	系統設定可讓您自動移除離線代理程式、檢查代理程式的連線和維護隔離資料夾。 如需詳細資訊，請參閱進行系統設定 第 11-8 頁。
例外	例外清單可讓您覆寫網頁信譽評等、URL 過濾和 Machine Learning 中定義的策略設定。 如需詳細資訊，請參閱設定例外清單設定 第 11-12 頁。

進行 Internet Proxy 伺服器設定

如果 Security Server 和代理程式使用 Proxy 伺服器與 Internet 連線，請指定 Proxy 伺服器設定以便使用下列功能和趨勢科技服務：

- Security Server：元件更新與使用授權維護
- Security Agent：網頁信譽評等、URL 過濾、行為監控、Smart Feedback 及雲端截毒掃瞄
- Messaging Security Agent（僅限 Advanced 版）網頁信譽評等和垃圾郵件防護

步驟

1. 移至「管理 > 全域設定」。
2. 從「Proxy」標籤，視需要更新下列項目：
   - Security Server Proxy

     注意

     Messaging Security Agent 對使用 Security Server Proxy 設定。

     - 為更新檔和使用授權通知使用 Proxy 伺服器
     - 使用 SOCKS 4/5 Proxy 通訊協定
     - 地址：IPv4/IPv6 位址或主機名稱
     - 通訊埠
     - Proxy 伺服器驗證
       - 使用者名稱
       - 密碼
   - Security Agent Proxy
     - 使用為更新 Proxy 指定的認證

       注意

       Security Agent 使用 Internet Explorer Proxy 伺服器和通訊埠來連線至 Internet。如果用戶端上的 Internet Explorer 和 Security Server 共用相同的驗證憑證，請選取此選項。

- 使用者名稱
- 密碼

3. 按一下「儲存」。

進行 SMTP 伺服器設定

SMTP 伺服器設定會套用至 Worry-Free Business Security 所產生的所有通知和報告。

步驟

1. 移至「管理 > 全域設定」。
2. 按一下「SMTP」標籤，並視需要更新下列項目：
   - SMTP 伺服器：SMTP 伺服器的 IPv4/IPv6 位址或名稱。
   - 通訊埠
   - 啟動 SMTP 伺服器驗證
     - 使用者名稱
     - 密碼
3. 若要驗證設定是否正確，請按一下「傳送測試電子郵件」。如果未成功傳送，請修改設定或檢查 SMTP 伺服器的狀態。
4. 按一下「儲存」。

進行桌上型電腦/伺服器設定

「桌上型電腦/伺服器」選項與 Worry-Free Business Security 的全域設定有關。個別群組的設定會覆寫這些設定。如果您尚未對群組設定特定選項，則會

使用「桌上型電腦/伺服器」選項。例如，如果特定群組沒有核准的 URL，則在此畫面上核准的所有 URL 都適用於該群組。

步驟

1. 移至「管理 > 全域設定」。
2. 按一下「桌上型電腦/伺服器」標籤，視需要更新下列項目：

設定	說明

位置偵測	「位置偵測」可讓管理員根據用戶端與網路的連線方式，對安全設定進行控管。
	「位置偵測」可控制「在辦公室中/辦公室以外的地方」連線設定。
	Security Agent 可根據 Web 主控台設定的閘道資訊，自動識別出用戶端的位置，然後控制使用者所能存取的網站。其限制會隨使用者的位置發生變更：
	• 啟動位置偵測：這些設定會影響防火牆、網頁信譽評等和預約更新頻率的「在辦公室中/辦公室以外的地方」連線設定。
	• 閘道資訊：從遠端連線至網路（使用 VPN）並啟動「位置偵測」後，此清單中的用戶端和連線會使用「內部連線」設定。
	  • 閘道 IP 位址
	  • MAC 位址：新增 MAC 位址可將連線的權限限定於已設定裝置，藉以大幅提升安全性。
	按一下對應的刪除圖示 (x) 即可刪除項目。

服務台通知	「服務台通知」會在 Security Agent 上顯示通知，以告知使用者聯絡人的資訊以取得協助。視需要更新下列項目： • 服務台標籤 • 服務台電子郵件信箱 • 其他資訊：當使用者將滑鼠放在標籤上時就會快顯此資訊

設定	說明
一般掃瞄設定	• 關閉雲端截毒掃瞄服務：將所有 Security Agent 切換為「標準掃瞄」模式。您必須在此處再次啟動雲端截毒掃瞄，才能加以使用。若要切換一或多個 Security Agent 群組，請瀏覽至「裝置 > {群組} > 設定策略 > 掃瞄方法」。 注意 如需有關切換 Security Agent 掃瞄方法的指導方針，請參閱設定掃瞄方法 第 5-4 頁。 • 啟動延遲掃瞄檔案作業：啟動此設定可暫時增進系統效能。 警告! 啟動延遲掃瞄可能會造成安全威脅。 • 排除陰影複製區段：「陰影複製服務」或「磁碟區快照服務」會取得特定磁碟區中，檔案或資料夾的手動或自動備份副本或快照。 • 排除 Security Server 資料庫資料夾：僅在「即時掃瞄」期間防止安裝於 Security Server 的代理程式對其本身的資料庫進行掃瞄。 依預設，WFBS 不會掃瞄自身的資料庫。趨勢科技建議您保留此項選擇，防止掃瞄時可能會發生的資料庫損毀。 • 在 Microsoft Exchange Server 安裝時不包括 Microsoft Exchange Server 資料夾：防止安裝於 Microsoft Exchange Server 的代理程式掃瞄 Microsoft Exchange 的資料夾。 • 排除 Microsoft 網域控制器資料夾：防止安裝於網域控制器的代理程式掃瞄網域控制器的資料夾。這些資料夾儲存使用者資訊、使用者名稱、密碼和其他重要資訊。

設定	說明
病毒掃瞄設定	• 設定大型壓縮檔的掃瞄設定：指定解壓縮檔的最大大小，以及代理程式應掃瞄的壓縮檔中的檔案數目。 • 清除壓縮檔：代理程式會嘗試清除壓縮檔內的中毒檔案。 • 最多掃瞄 { } 個 OLE 層：代理程式會掃瞄指定的「物件連結與嵌入」(OLE) 層數。OLE 可讓您使用一個應用程式來建立物件，然後在另一個應用程式中連結或嵌入這些物件。例如：內嵌於 .doc 檔案中的 .xls 檔案。 • 將「手動掃瞄」新增到用戶端的 Windows 捷徑功能表：將「使用 Security Agent 來掃瞄」連結新增至內容感應式功能表。如此一來，使用者即可用滑鼠右鍵按一下檔案或資料夾（在桌面上或「Windows 檔案總管」中）並手動掃瞄檔案或資料夾。
間諜程式/可能的資安威脅程式掃瞄設定	• 掃瞄 Cookie：Security Agent 會掃瞄 Cookie。 • 將 Cookie 偵測新增至間諜程式記錄檔：將偵測到的間諜程式 Cookie 新增至間諜程式記錄檔。
防火牆設定	選取「關閉防火牆並解除安裝驅動程式」核取方塊，以解除安裝 Worry-Free Business Security 用戶端防火牆並移除與防火牆關聯的驅動程式。 注意 關閉防火牆之後，除非重新啟動防火牆，否則相關設定將無法再使用。
HTTPS Web 威脅防護	啟動此功能，以在 Chrome、Firefox 和 Microsoft Edge 上根據網頁信譽評等和 URL 過濾設定檢查 HTTPS URL。 注意 此功能不需要其他瀏覽器附加元件。 依預設，Worry-Free Business Security 會使用瀏覽器附加元件來檢查 Internet Explorer 的 HTTPS URL。
警訊設定	如果病毒碼檔案在 { } 天後未更新，則會在 Windows 工作列上顯示警訊圖示：如果病毒碼檔案在特定天數後仍未更新，則會在用戶端上顯示警訊圖示。

設定	說明
Security Agent 解除安裝密碼	• 允許用戶端使用者不需密碼即可解除安裝 Security Agent。 • 要求用戶端使用者使用密碼才能解除安裝 Security Agent。
Security Agent 程式結束和解除鎖定密碼	• 允許用戶端使用者不需要使用密碼，就可以結束並解除鎖定他們電腦上的 Security Agent。 • 要求用戶端使用者輸入密碼才能結束並解除鎖定 Security Agent。 注意 解除鎖定 Security Agent 可讓使用者覆寫在「裝置 > {群組} > 設定策略 > 代理程式權限」下進行的所有設定。
偏好的 IP 位址	只有雙堆疊 Security Server 可使用此設定，而且此設定只會由雙堆疊代理程式套用。 安裝或升級代理程式之後，代理程式會使用 IP 位址向 Security Server 註冊。 請從下列選項選擇： • 先使用 IPv4 位址，然後再使用 IPv6 位址：代理程式會先使用其 IPv4 位址。如果代理程式無法使用其 IPv4 位址來註冊，則會使用其 IPv6 位址。如果無法使用這兩種位址來註冊，代理程式會使用此選項的 IP 位址優先順序來重試。 • 先使用 IPv6 位址，然後再使用 IPv4 位址：代理程式會先使用其 IPv6 位址。如果代理程式無法使用其 IPv6 位址來註冊，則會使用其 IPv4 位址。如果無法使用這兩種位址來註冊，代理程式會使用此選項的 IP 位址優先順序來重試。

3. 按一下「儲存」。

進行系統設定

「全域設定」畫面的「系統」區段包含用來自動移除離線代理程式、檢查代理程式連線和維護隔離資料夾的選項。

步驟

1. 移至「管理 > 全域設定」。
2. 按一下「系統」標籤，並視需要更新下列項目：

設定	說明
移除離線的 Security Agent	當您使用用戶端上的 Security Agent 解除安裝程式，以從用戶端移除代理程式時，程式會自動通知 Security Server。當 Security Server 收到這項通知時，便會將該用戶端圖示自安全群組樹狀結構中移除，藉以表示該用戶端不復存在。 然而，如果使用其他方法移除 Security Agent（例如，重新格式化電腦的硬碟或手動刪除用戶端檔案），Security Server 就不會得知 Security Agent 已經移除，而會將它顯示為離線。如果使用者長期卸載或關閉代理程式，Security Server 也會將 Security Agent 顯示為離線。 如果要讓「安全群組樹狀結構」只顯示連線的用戶端，您可以將 Security Server 設定成自動移除「安全群組樹狀結構」中的離線 Security Agent。 • 啟動自動移除離線的 Security Agent：自動移除在指定的天數內未與 Security Server 聯絡的用戶端。 • 在離線 {} 天後自動移除 Security Agent：允許用戶端離線的天數，若超過此限便從 Web 主控台移除用戶端。

設定	說明

代理程式連線驗證	Worry-Free Business Security 會在「安全群組樹狀結構」中使用圖示來表示用戶端連線狀態。但是，某些狀況可能會造成「安全群組樹狀結構」無法正確顯示代理程式連線狀態。例如，如果用戶端的網路線被意外拔掉，代理程式將無法通知趨勢科技 Security Server 其正處於離線狀態。此代理程式在「安全群組樹狀結構」中仍然會顯示為線上狀態。
	
	您可以手動驗證代理程式與伺服器之間的連線，或從 Web 主控台預約該驗證。
	
	注意
	「連線驗證」不允許選取特定的群組或代理程式。它會驗證向 Security Server 註冊的所有代理程式的連線。
	
	• 啟動預約驗證：啟動對代理程式與伺服器之間連線的預約驗證。
	  • 每小時一次
	  • 每日一次
	  • 每週一次，於
	  • 開始時間：驗證的開始時間。
	• 立即驗證：立即測試連線能力。

設定	說明
隔離維護	依預設，Security Agent 會將隔離的中毒檔案傳送至 Security Server 中的下列目錄： `<Security Server 安裝資料夾>\PCCSRV\Virus` 如果您需要變更目錄（例如，如果磁碟空間不足），請在「隔離目錄」欄位中輸入絕對路徑（例如 `D:\Quarantined Files`）。如果進行此操作，請同時對「裝置 > {群組} > 設定策略 > 隔離」套用相同變更，否則代理程式會繼續將檔案傳送至 `<Security Server 安裝資料夾>\PCCSRV\Virus`。 此外，請設定下列維護設定： • 隔離資料夾的大小：隔離資料夾的大小（以 MB 為單位）。 • 單一檔案大小上限：儲存在隔離資料夾中的單一檔案的大小上限（以 MB 為單位）。 • 刪除所有隔離檔案：刪除隔離資料夾中的所有檔案。如果資料夾已滿但又上傳新檔案，則不會儲存新的檔案。 如果您不希望代理程式將隔離檔案傳送至 Security Server，請在「裝置 > {群組} > 設定策略 > 隔離」中設定新目錄，並忽略所有維護設定。如需指示，請參閱隔離目錄 第 5-15 頁。
Security Agent 安裝	Security Agent 安裝目錄：在安裝期間，系統會提示您輸入 Security Agent 安裝目錄，該目錄是安裝程式安裝每個 Security Agent 的位置。 如果需要，請輸入絕對路徑來變更目錄。僅會將以後的代理程式安裝到此目錄；現有代理程式將保持其目前的目錄。 請使用下列其中一個變數設定用安裝路徑： • `$BOOTDISK`：開機磁碟的磁碟機代號 • `$WINDIR`：安裝 Windows 的資料夾 • `$ProgramFiles`：程式資料夾

3. 按一下「儲存」。

設定例外清單設定

步驟

1. 移至「管理 > 全域設定」。
2. 按一下「例外」標籤，並視需要設定下列項目：

區段	說明
網頁信譽評等和 URL 過濾	• 核可的 URL 清單：排除在網頁信譽評等和 URL 過濾驗證範圍外的網站（及其子網域）。 **注意** 例外清單優先於封鎖的清單。當 URL 與例外清單中的項目相符時，即使該 URL 位於封鎖的清單中，代理程式也一律允許存取 URL。 特定群組自訂的核可/封鎖的 URL 會覆寫全域例外設定。 • 封鎖的 URL 清單：在 URL 過濾時一律封鎖的網站（及其子網域）。 • 處理程序例外清單：從網頁信譽評等和 URL 過濾驗證排除的處理程序。鍵入組織認為值得信任的重要處理程序。 **秘訣** 更新處理程序例外清單且伺服器將更新的清單部署至代理程式時，用戶端電腦上的所有作用中 HTTP 連線（透過通訊埠 80、81 或 8080）將會中斷連線數秒。請考慮在離峰時間更新處理程序例外清單。 • IP 例外清單：排除在網頁信譽評等和 URL 過濾驗證範圍外的 IP 位址（例如：192.168.0.1）。輸入貴公司認為可靠的重要 IP 位址。 • 將網頁信譽評等和 URL 過濾記錄檔傳送至 Security Server

區段	說明
Machine Learning 例外清單	設定全域的 Machine Learning 檔案例外，以防止所有 Security Agent 將某個檔案偵測為惡意檔案。輸入要從掃瞄中排除的檔案 SHA-1 雜湊值。（選擇性）提供附註來解釋當成例外的原因，或是說明與雜湊值相關聯的檔案名稱。

3. 按一下「儲存」。

第 12 章

使用記錄檔和報告

本章說明如何使用記錄檔和報告來監控系統以及分析防護能力。

記錄檔

Worry-Free Business Security 會保留關於病毒/惡意程式和間諜程式/可能的資安威脅程式感染、事件以及更新的詳細記錄檔。您可以使用這些記錄評估您組織的防護策略、識別中毒風險較高的用戶端，以及確認已成功部署更新。

注意

請使用試算表應用程式（例如：Microsoft Excel）來檢視 CSV 記錄檔。

Worry-Free Business Security 會維護下列類別的記錄檔：

- Web 主控台事件記錄檔
- 桌上型電腦/伺服器記錄檔
- Microsoft Exchange Server 記錄檔（僅限 Advanced 版）

表 12-1. 記錄檔類型和內容

類型（產生記錄檔項目的項目）	內容（取得內容的記錄檔類型）
管理主控台事件	• 手動掃瞄 (從 Web 主控台啟動) • 更新（Security Server 更新） • 主控台事件

類型（產生記錄檔項目的項目）	內容（取得內容的記錄檔類型）

桌上型電腦/伺服器	• 病毒記錄檔
	  • 手動掃瞄
	  • 即時掃瞄
	  • 預約掃瞄
	• 間諜程式/可能的資安威脅程式記錄檔
	  • 手動掃瞄
	  • 即時掃瞄
	  • 預約掃瞄
	• Machine Learning 記錄
	• 網頁信譽評等記錄檔
	• URL 過濾記錄檔
	• 行為監控記錄檔
	• 更新記錄檔
	• 網路病毒記錄檔
	• 事件記錄檔
	• 周邊設備存取控管記錄
	• 更新部署記錄
	• 勒索軟體記錄檔
	  • 防毒
	  • 行為監控
	  • 網頁信譽評等
	  • URL 過濾
	  • Machine Learning

類型（產生記錄檔項目的項目）	內容（取得內容的記錄檔類型）
Exchange Server（僅限 Advanced 版）	• 病毒記錄檔 • 附件封鎖記錄檔 • 內容過濾/資料遺失防範記錄檔 • 更新記錄檔 • 備份記錄檔 • 封存記錄檔 • 掃瞄事件記錄 • 無法掃瞄的郵件部分記錄檔 • 網頁信譽評等記錄檔 • 行動事件記錄檔

使用記錄查詢

執行記錄查詢可以從記錄檔資料庫取得資訊。您可以使用「記錄查詢」畫面來設定和執行查詢。查詢結果可以匯出至 .CSV 檔案，也可以將其列印出來。

Messaging Security Agent（僅限 Advanced 版）每五分鐘會將其記錄檔傳送到 Security Server（不論記錄檔是何時產生的）。

步驟

1. 瀏覽至「報告 > 記錄查詢」。
2. 視需要更新下列選項：
   - 時間範圍
     - 預先設定的範圍
     - 指定範圍：將查詢限定於特定日期。

- 類型：請參閱記錄檔 第 12-2 頁，以檢視每一種記錄檔類型的內容。
  - 管理主控台事件
  - 桌上型電腦/伺服器
  - Exchange Server（僅限 Advanced 版）
- 內容：可用的選項視記錄檔的類型而定。

3. 按一下「顯示記錄檔」。
4. 如果要將記錄檔儲存為逗號分隔值 (CSV) 資料檔案，請按一下「匯出」。使用試算表應用程式檢視 CSV 檔案。

報告

您可以手動產生綜合報告，也可以設定 Security Server 以產生預約報告。

您可以列印報告，或透過電子郵件將報告傳送給管理員或其他個人。

報告中提供的資料受產生報告時 Security Server 上提供的記錄檔數量影響。在新增記錄檔以及刪除現有記錄檔時，記錄檔數量會發生變更。在「報告 > 維護」中，您可以手動刪除記錄檔或設定記錄檔刪除預約。

使用綜合報告

步驟

1. 瀏覽至「報告 > 綜合報告」。
2. 執行下列工作：

工作	步驟
產生報告	a. 按一下「新增」。 隨即顯示新畫面。 b. 設定下列項目： • 報告名稱 • 時間範圍：將報告限定於特定日期。 • 內容：若要選取所有安全威脅，請選取「全選」核取方塊。如果要選取個別的安全威脅，請按一下對應的核取方塊。按一下加號 (+) 圖示以展開選項。 • 傳送報告至 • 收件者：輸入收件者的電子郵件信箱，並以分號 (;) 進行分隔。 • 格式：選擇 PDF 或 HTML 報告連結。如果選擇 PDF，PDF 將附加到電子郵件中。 c. 按一下「新增」。
檢視報告	在「報告名稱」欄下，按一下報告的連結。第一個連結將開啟 PDF 報告，第二個連結將開啟 HTML 報告。 報告中提供的資料受產生報告時 Security Server 上提供的記錄檔數量影響。在新增記錄檔以及刪除現有記錄檔時，記錄檔數量會發生變更。在「報告 > 維護」中，您可以手動刪除記錄檔或設定記錄檔刪除預約。 如需有關報告內容的詳細資訊，請參閱解譯報告 第 12-9 頁。
刪除報告	a. 選取包含報告連結的列。 b. 按一下「刪除」。 **注意** 若要自動刪除報告，請瀏覽至「報告 > 維護 > 報告」標籤，然後設定 Worry-Free Business Security 將保留的最大綜合報告數目。預設為 10 個綜合報告。超過該數目時，Security Server 便會從保留時間最久的報告開始刪除報告。

使用預約報告

步驟

1. 瀏覽至「報告 > 預約報告」。
2. 執行下列工作：

工作	步驟
建立預約報告範本	a. 按一下「新增」。 隨即顯示新畫面。 b. 設定下列項目： • 報告範本名稱 • 預約：每日一次、每週一次、每月一次以及產生報告的時間 對於每月一次的報告，如果您選取 31、30 或 29 日，但該月沒有該日期，WFBS 將不會產生該月的報告。 • 內容：若要選取所有安全威脅，請選取「全選」核取方塊。如果要選取個別的安全威脅，請按一下對應的核取方塊。按一下加號 (+) 圖示以展開選項。 • 傳送報告至 • 收件者：輸入收件者的電子郵件信箱，並以分號 (;) 進行分隔。 • 格式：選擇 PDF 或 HTML 報告連結。如果選擇 PDF，PDF 將附加到電子郵件中。 c. 按一下「新增」。

工作	步驟
檢視預約報告	a. 在包含從中產生預約報告之範本的列中，按一下「報告記錄」。 接著會開啟一個新畫面。 b. 在「檢視」欄下，按一下報告的連結。第一個連結將開啟 PDF 報告，第二個連結將開啟 HTML 報告。 報告中提供的資料受產生報告時 Security Server 上提供的記錄檔數量影響。在新增記錄檔以及刪除現有記錄檔時，記錄檔數量會發生變更。在「報告 > 維護」中，您可以手動刪除記錄檔或設定記錄檔刪除預約。 如需有關報告內容的詳細資訊，請參閱解譯報告 第 12-9 頁。
範本維護工作	
編輯範本設定	按一下範本，然後在顯示的新畫面中編輯設定。 在儲存變更後產生的報告將使用新設定。
啟動/關閉範本	按一下「已啟動」欄下的圖示。 如果您想暫時停止產生預約報告，並在再次需要報告時將其啟動，請關閉範本。
刪除範本	選取範本，並按一下「刪除」。 刪除範本時，不會刪除從範本產生的預約報告，但 Web 主控台中將不再提供這些報告的連結。您可以直接從 Security Server 電腦存取這些報告。僅當您手動刪除電腦中的報告，或在 Security Server 根據「報告 > 維護 > 報告」標籤中的預約報告自動刪除設定，自動刪除報告時，才會刪除報告。 若要自動刪除範本，請瀏覽至「報告 > 維護 > 報告」標籤，然後設定 Worry-Free Business Security 將保留的最大範本數目。預設為 10 個範本。超過該數目時，Security Server 便會從保留時間最久的範本開始刪除範本。
報告維護工作	

工作	步驟
傳送預約報告的連結	透過電子郵件傳送預約報告（使用 PDF 格式）的連結。收件者只需按一下電子郵件中的連結即可存取 PDF 檔案。請確保收件者可以連線至 Security Server 電腦，否則，檔案將不會顯示。 **注意** 僅會在電子郵件中提供 PDF 檔案的連結，而不會附加實際的 PDF 檔案。 a. 在包含從中產生預約報告之範本的列中，按一下「報告記錄」。 接著會開啟一個新畫面。 b. 選取報告，然後按一下「傳送」。 會開啟預設電子郵件用戶端，其中含有包含報告連結的新電子郵件。
刪除預約報告	a. 在包含從中產生預約報告之範本的列中，按一下「報告記錄」。 接著會開啟一個新畫面。 b. 選取報告，然後按一下「刪除」。 **注意** 若要自動刪除報告，請瀏覽至「報告 > 維護 > 報告」標籤，然後設定 Worry-Free Business Security 將在每個範本中保留的最大預約報告數目。預設為 10 個預約報告。超過該數目時，Security Server 便會從保留時間最久的報告開始刪除報告。

解譯報告

Worry-Free Business Security 報告包含下列資訊。顯示的資訊可能會隨所選的選項而不同。

表 12-2. 報告的內容

報告項目	說明
防毒	桌上型電腦/伺服器病毒摘要 病毒報告會顯示掃瞄引擎偵測到的病毒/惡意程式數目和類型，以及所採取的中毒處理行動的詳細資訊。報告也會列出排行榜病毒/惡意程式名稱。按一下病毒/惡意程式的名稱，會開啟新的 Web 瀏覽器頁面，然後將它重新導向「趨勢科技病毒百科全書」，以便瞭解更多該病毒/惡意程式的資訊。
	偵測到最多病毒的前 5 部桌上型電腦/伺服器 顯示報告病毒/惡意程式偵測的前 5 部桌上型電腦或伺服器。在同一個用戶端上經常觀察到病毒/惡意程式事件可能代表該用戶端存在高度的安全威脅，可能需要進一步的調查
間諜程式防護	桌上型電腦/伺服器間諜程式/可能的資安威脅程式摘要 間諜程式/可能的資安威脅程式報告會顯示在用戶端上偵測到的間諜程式/可能的資安威脅程式威脅的詳細資訊，包括偵測數目及 WFBS 所執行的處理行動。報告中包含圓形圖，顯示每一項間諜程式防護中毒處理行動的已執行百分比。
	偵測到最多間諜程式/可能的資安威脅程式的前 5 部桌上型電腦/伺服器 報告中也顯示偵測到的前 5 種間諜程式/可能的資安威脅程式威脅，以及偵測到含有最多間諜程式/可能的資安威脅程式的前 5 部桌上型電腦/伺服器。如需瞭解偵測到的間諜程式/可能的資安威脅程式威脅的進一步資訊，請按一下間諜程式/可能的資安威脅程式名稱。如此將會開啟新的網路瀏覽器網頁，顯示趨勢科技網站上該間諜程式/可能的資安威脅程式相關的資訊。
垃圾郵件防護摘要（僅限 Advanced 版）	垃圾郵件摘要 垃圾郵件防護報告會顯示，在掃瞄的訊息總數量中，所偵測到的垃圾郵件和釣魚網站的數目的資訊。它會列出垃圾郵件誤判。
Machine Learning	前 5 名違反 Machine Learning 策略的程式
	前 10 部違反 Machine Learning 策略的電腦
網頁信譽評等	前 10 部違反網頁信譽評等策略的電腦

報告項目	說明
URL 類別	前 5 項已違反的 URL 類別策略 列出違反策略的最常存取的網站類別。
	前 10 部違反 URL 類別策略的電腦
行為監控	前 5 名違反行為監控策略的程式
	前 10 部違反行為監控策略的電腦
周邊設備存取控管	前 10 部違反周邊設備存取控管策略的電腦
內容過濾摘要（僅限 Advanced 版）	內容過濾摘要 內容過濾報告會顯示 Messaging Security Agent 所過濾的訊息總數的資訊。
	前 10 名違規的內容過濾規則 前 10 名違規的內容過濾規則清單。請使用此報告結果來微調您的過濾規則。
網路病毒	前 10 名偵測到的網路病毒 列出一般防火牆驅動程式最常偵測到的 10 種網路病毒。 按一下病毒的名稱，會開啟新的 Web 瀏覽器頁面，然後將它重新導向「趨勢科技病毒百科全書」，以便瞭解更多該病毒的資訊。
	前 10 部最常遭受攻擊的電腦 列出您的網路上最常回報病毒事件的電腦。

執行報告和記錄檔維護工作

步驟

1. 瀏覽至「報告 > 維護」。
2. 執行下列工作：

工作	步驟
設定報告和範本上限	您可以限制綜合報告、預約報告（根據範本）和 Security Server 上可用範本的數量。超過上限時，Security Server 便會從保留日期最久的報告/範本開始刪除。 a. 按一下「報告」標籤。 b. 輸入要保留的綜合報告、預約報告和報告範本數量上限。
設定自動刪除記錄檔	a. 按一下「自動刪除記錄檔」標籤。 b. 選取記錄檔類型，並指定記錄檔的保留時間上限。超過此值的記錄檔將會刪除。
手動刪除記錄檔	a. 按一下「手動刪除記錄檔」標籤。 b. 針對各個記錄檔類型，輸入記錄檔的保留時間上限。超過此值的記錄檔將會刪除。若要刪除所有記錄檔，輸入 `0`。 c. 按一下「刪除」。

3. 按一下「儲存」。

第 13 章

執行管理工作

本章說明如何執行其他管理工作，例如：檢視產品使用授權、使用「Plug-in Manager」和解除安裝 Security Server。

變更 Web 主控台密碼

趨勢科技建議您對 Web 主控台使用強式密碼。強式密碼的長度至少有八個字元，包含一或多個大寫字母 (A-Z)、一或多個小寫字母 (a-z)、一或多個數字 (0-9)，以及一或多個特殊字元或標點符號 (!@#$%^&,.:;?)。強式密碼絕對不可以和使用者的登入名稱相同，也不得包含登入名稱。強式密碼中不能加入使用者的姓名、生日，或是任何可以輕易與使用者產生聯想的項目。

步驟

1. 瀏覽至「管理 > 密碼」。
2. 視需要更新下列選項：
   - 舊密碼
   - 新密碼
   - 確認密碼：重新輸入新密碼以便確認。
3. 按一下「儲存」。

使用 Plug-in Manager

Plug-in Manager 會在 Security Server 和 Security Agent 的外掛程式推出後，立刻在 Web 主控台中同時顯示這些程式。您就可以從 Web 主控台安裝並管理這些程式，包含將用戶端外掛程式佈署到代理程式。從「管理 > 嵌入程式」下載和安裝 Plug-in Manager。安裝後，您可以檢查是否有可用的外掛程式。如需詳細資訊，請參閱 Plug-in Manager 和嵌入程式的文件。

管理產品使用授權

您可以透過「產品使用授權」畫面來續約、升級或檢視產品使用授權的詳細資料。

「產品使用授權」畫面會顯示有關您的使用授權的詳細資訊。根據您在安裝期間所選擇的選項，您可能會有完整授權的版本或試用版。不論是哪種情況，您的使用授權都可讓您享有維護合約。當您的維護合約到期時，網路上的用戶端所受到的保護將極為有限。使用「產品使用授權」畫面來判斷使用授權到期日，確保您能在使用授權到期前進行續約。

注意

趨勢科技對各種元件的授權會因地區而異。安裝之後，您會看到允許您使用的授權碼/啟動碼元件摘要。請與廠商或經銷商驗證您擁有哪些元件的使用授權。

使用授權續約

您可以透過購買維護續約，來續約或升級到完整授權版本的 Worry-Free Business Security。完整授權版本需要啟動碼。

產品使用授權的續約方式分為兩種：

- 在主控台上，瀏覽至「即時狀態」畫面，並按照畫面上的指示進行。這些指示會在使用授權到期的 60 天前和 30 天後顯示。
- 請洽詢趨勢科技的銷售人員或公司經銷商，以便續約使用授權合約。

  經銷商可以在 Security Server 上的檔案中留下其聯絡資訊。在以下位置查看此檔案：

  ```
  {Security Server 安裝資料夾}\PCCSRV\Private\contact_info.ini
  ```

  注意

  {Security Server 安裝資料夾} 通常是 C:\Program Files\Trend Micro\Security Server。

  趨勢科技的銷售人員會使用趨勢科技的「產品註冊」更新您的註冊資訊。

  Security Server 會輪詢「產品註冊」伺服器，並從「產品註冊」伺服器接收新的到期日。進行使用授權的續約程序時，您不需要手動輸入新的「啟動碼」。

啟動新授權

您的使用授權類型取決於 Worry-Free Business Security 啟動碼。

表 13-1. 依使用授權類型設定的啟動碼

使用授權類型	啟動碼
Worry-Free Business SecurityStandard 完整授權版本	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
Worry-Free Business SecurityAdvanced 完整授權版本	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

注意

如果您有關於啟動碼的問題，請查詢下列網址的趨勢科技支援網站：

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

請透過在「產品使用授權」畫面中輸入新的「啟動碼」，來變更您的使用授權類型。

1. 瀏覽至「管理 > 產品使用授權」。
2. 按一下輸入新的啟動碼。
3. 並輸入新的「啟動碼」。
4. 按一下啟動。

設定產品更新設定

將 Worry-Free Business Security 設定為自動執行產品更新。

步驟

1. 移至「管理 > 產品更新」。

   「設定」標籤隨即出現。

2. 在「更新設定」下，選取「啟動產品更新下載」。

3. 指定在新更新套件可用時要採取的處理行動。
   - 下載：根據設定的預約時程自動將更新套件下載到下載資料夾。
   - 下載並安裝：根據設定的預約時程自動下載並安裝更新套件。
4. 指定採取處理行動的時間。

注意

安裝程序可能需要一些時間才能完成，並會重新啟動 Security Server。請選擇對其他作業影響最小的時間來安裝更新套件。

5. 按一下「儲存」。

設定產品更新通知

Worry-Free Business Security 可以在有新版本、Service Pack 或修補程式可用時，通知使用者有產品更新。您可以設定下列產品更新通知類型：

- Security Agent：在端點上的通知區域附近顯示通知
- 電子郵件

步驟

1. 移至「管理 > 產品更新」。
2. 按一下「通知」。
3. 若要從 Security Agent 接收通知，請設定「Security Agent 通知」區段。
   a. 按一下「新增」。
   b. 從清單中選取 Security Agent。
   c. 按一下「儲存」。
4. 若要接收產品更新的電子郵件通知，請在「電子郵件通知」區段中指定收件者。

注意

若要接收電子郵件通知，您必須在「管理 > 全域設定」中設定「SMTP」標籤。

5. 按一下「儲存」。

參與 Smart Feedback 系統程式

如需 Smart Feedback 的詳細資訊，請參閱 Smart Feedback 第 1-5 頁。

步驟

1. 瀏覽至「管理 > 主動式雲端截毒技術」。
2. 按一下「啟動 Trend Micro Smart Feedback」。
3. 如果要傳送用戶端電腦中有關檔案潛在安全威脅的資訊，請選取「啟動可疑程式檔案的回饋」核取方塊。

注意

傳送給 Smart Feedback 的檔案未含任何使用者資料，僅提交做威脅分析之用。

4. 如果要協助趨勢科技瞭解您的組織，請選取「產業」類型。
5. 按一下「儲存」。

變更代理程式的介面語言

依預設，該代理程式介面所用的語言將對應於在用戶端作業系統上設定的地區設定。使用者可從代理程式介面變更語言。

儲存及還原程式設定

您可以儲存 Security Server 資料庫和重要組態設定檔的副本，以還原 Security Server。如果發生問題而需要重新安裝 Security Server，或是要還原成先前的組態設定，即可執行此作業。

步驟

1. 停止 Trend Micro Security Server Master Servic。
2. 將資料夾中的下列檔案和資料夾手動複製到其他位置：

   警告!
   請勿使用備份工具或應用程式來進行這項工作。

   `<Security Server 安裝路徑>\PCCSRV`

   - `Ofcscan.ini`：包含全域設定。
   - `ous.ini`:包含防毒元件部署的更新來源表格。
   - `Private` 資料夾：包含防火牆和更新來源設定。

- `Pccnt\Common\OfcPfw.dat`:包含防火牆設定。
- `Download\OfcPfw.dat`:包含防火牆部署設定。
- `log` 資料夾：包含系統事件和驗證連線記錄檔。
- `Virus` 資料夾：WFBS 隔離中毒檔案的資料夾。
- `HTTDB` 資料夾：包含 WFBS 資料庫。

3. 解除安裝 Security Server。請參閱解除安裝 Security Server 第 13-9 頁。
4. 執行初次安裝。請參閱 Worry-Free Business Security 的《安裝和升級手冊》。
5. 在主安裝程式結束後，請停止目標電腦上的 Trend Micro Security Server Master Service。
6. 從備份檔案更新病毒碼版本：
   a. 從新伺服器取得目前的病毒碼版本。

      ```
      <Security Server 安裝路徑>\PCCSRV\Private\component.ini.
      [6101]

      ComponentName=Virus pattern

      Version=xxxxxx 0 0
      ```

   b. 更新備份檔案中的病毒碼版本：

      ```
      \Private\component.ini
      ```

      注意

      如果您變更 Security Server 安裝路徑，則必須更新備份檔案 `ofcscan.ini` 和 `\private\ofcserver.ini` 中的路徑資訊。

7. 使用您建立的備份，覆寫目標電腦上的 Worry-Free Business Security 資料庫和相關的檔案與資料夾（在 `PCCSRV` 資料夾中）。
8. 重新啟動 Trend Micro Security Server Master Service。

解除安裝 Security Server

解除安裝 Security Server 也會解除安裝 Scan Server。

Worry-Free Business Security 可使用解除安裝程式，從您的電腦安全地移除趨勢科技 Security Server。在移除 Security Server 之前，先從所有用戶端移除代理程式。

解除安裝趨勢科技 Security Server 並不會解除安裝代理程式。在解除安裝趨勢科技 Security Server 之前，管理員必須先解除安裝所有代理程式或將這些代理程式移動到其他 Security Server。請參閱移除代理程式 第 3-33 頁。

步驟

1. 在用來安裝伺服器的電腦上，按一下「開始 > 控制台 > 新增或移除程式」。
2. 按一下「趨勢科技 Security Server」，然後按一下「變更/移除」。

   會出現確認畫面。
3. 按一下「下一步」。

   「主解除安裝程式」（伺服器解除安裝程式）會提示您輸入系統管理員密碼。
4. 在文字方塊中輸入管理員密碼，然後按一下「確定」。

   「主解除安裝程式」會開始移除伺服器檔案。在解除安裝 Security Server 之後，隨即出現確認訊息。
5. 按一下「確定」以關閉解除安裝程式。

第 14 章

使用管理工具

本章說明如何使用管理和用戶端工具以及快捷工具列。

工具類型

Worry-Free Business Security 提供了一組可協助您輕鬆完成各項工作（包括伺服器組態設定和用戶端管理）的工具。

注意

您無法從 Web 主控台啟動管理工具和用戶端工具。您可以從 Web 主控台下載快捷工具列。

如需有關使用這些工具的詳細資訊，請參閱下面的相關章節。

這些工具可分為三大類：

- 管理工具
  - Login Script Setup (`SetupUsr.exe`)：自動安裝 Security Agent。請參閱使用 Login Script Setup 安裝 第 3-10 頁。
  - Vulnerability Scanner (`TMVS.exe`)：尋找網路上未受保護的電腦。請參閱使用 Vulnerability Scanner 進行安裝 第 3-17 頁。
  - Remote Manager Agent：讓經銷商能夠透過集中式 Web 主控台管理 Worry-Free Business Security。請參閱安裝 Trend Micro Remote Manager Agent（Customer Licensing Portal 使用者） 第 14-4 頁。
  - Trend Micro Disk Cleaner：刪除不必要的 Worry-Free Business Security 備份檔案、記錄檔和未使用的病毒碼檔案。請參閱節省磁碟空間 第 14-13 頁。
  - Scan Server Database Mover：將 Scan Server 資料庫安全移動至其他磁碟機。請參閱移動 Scan Server 資料庫 第 14-16 頁。
- 用戶端工具
  - Client Packager (`ClnPack.exe`)：建立包含 Security Agent 和元件的自動解壓縮檔。請參閱以 Client Packager 進行安裝 第 3-11 頁。

- 恢復加密的病毒和間諜程式 (VSEncode.exe)：開啟由 Worry-Free Business Security 加密的中毒檔案。請參閱還原加密檔案 第 14-17 頁。
- Client Mover 工具 (IpXfer.exe)：可以將代理程式從一部 Security Server 移轉到另一部 Security Server。請參閱移動代理程式 第 4-10 頁。
- 重新產生 Security Agent ClientID (WFBS_WIN_All_ReGenID.exe)：根據代理程式是處於複製的電腦還是虛擬機器，使用 ReGenID 公用程式重新產生 Security Agent ClientID。請參閱使用 ReGenID 工具 第 14-21 頁。

- 快捷工具列：可讓管理員從支援的 Windows 作業系統的主控台即時檢視安全和系統資訊。這與「即時狀態」畫面上顯示的高層級資訊相同。請參閱管理 SBS 及 EBS 快捷工具列 第 14-21 頁。

注意

舊版 Worry-Free Business Security 中提供的某些工具在這一版中並未提供。如果您需要這些工具，請聯絡趨勢科技客戶服務部門。

Trend Micro Remote Manager Agent

Trend Micro Remote Manager Agent 可讓經銷商或合作夥伴使用 Trend Micro Remote Manager 管理 Worry-Free Business Security。您可以在 Security Server 安裝完成之後將 Remote Manager Agent 安裝到該 Security Server 上，也可以稍後安裝 Remote Manager Agent。

安裝需求：

- Remote Manager Agent 全域唯一識別碼 (GUID)
- 作用中 Internet 連線
- 50MB 可用磁碟空間

請遵循下列其中一個項目中的程序：

- 安裝 Trend Micro Remote Manager Agent（Customer Licensing Portal 使用者） 第 14-4 頁
- 安裝 Trend Micro Remote Manager Agent（Licensing Management Platform 使用者） 第 14-6 頁

安裝 Trend Micro Remote Manager Agent（Customer Licensing Portal 使用者）

步驟

1. 取得 Remote Manager Agent GUID。
   a. 在 Remote Manager Web 主控台上，移至「客戶」。
   b. 在「公司」欄，按一下某位客戶。
   c. 在「產品」標籤上，選取「Worry-Free Business Security」產品。
   d. 複製該 GUID。
2. 移到 Security Server 並且瀏覽至下列安裝資料夾：`PCCSRV\Admin\Utility\RmAgent`，然後啟動應用程式 `TMRMAgentforWFBS.exe`。

   例如：`C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   注意
   如果您從「Security Server Setup」畫面啟動安裝，請略過此步驟。
3. 在 Trend Micro Remote Manager Agent 安裝精靈中，閱讀授權合約。如果您同意其中的條款，請選取「我接受合約中的條款」，然後按一下「下一步」。
4. 按一下「是」，確認您是認證的合作夥伴。
5. 選取「我已經有 Trend Micro Remote Manager 帳號且我想要安裝代理程式」，然後按一下「下一步」。

6. 確定您的狀況。

狀況	步驟
新客戶	a. 選取「與新的客戶進行關聯」。 b. 按一下「下一步」。輸入客戶資訊。 注意 如果該客戶已存在於 TMRM 主控台且您使用上述選項與新的客戶進行關聯，這會導致 TMRM 網路樹狀結構中顯示兩個具有相同名稱的重複客戶。如果要避免此問題，請使用下列方法。
現有客戶	a. 選取「此產品已存在於 Remote Manager」。 注意 WFBS 必須已新增至 TMRM 主控台。如需相關指示，請參閱您的 TMRM 說明文件。 b. 輸入 GUID。

7. 按一下「下一步」。
8. 選取「地區」和「通訊協定」，然後輸入 Proxy 資訊（如果需要）。
9. 按一下「下一步」。

   會出現「安裝位置」畫面。
10. 如果要使用預設位置，請按一下「下一步」。
11. 按一下「完成」。

    如果安裝成功且設定正確，Remote Manager Agent 應該會自動註冊至 Trend Micro Remote Manager 伺服器。Remote Manager Agent 應該會在 Remote Manager Web 主控台上顯示為「線上」。

安裝 Trend Micro Remote Manager Agent（Licensing Management Platform 使用者）

步驟

1. 取得 Worry-Free Business Security 啟動碼。
   a. 在 Remote Manager Web 主控台上，移至「客戶」。
   b. 在「公司」欄，按一下某位客戶。
   c. 在「產品」標籤上，選取「Worry-Free Business Security」產品。
   d. 複製該啟動碼。
2. 更新 Worry-Free Business Security 使用授權資訊。
   a. 在 Worry-Free Business Security Web 主控台上，移至「管理 > 產品使用授權」。
   b. 在「使用授權資訊」下，按一下「輸入新的啟動碼」。
   c. 在「新的啟動碼」欄位中貼上啟動碼。
   d. 按一下啟動。
   e. 按一下「重新整理使用授權資訊」。
3. 移到 Security Server 並且瀏覽至下列安裝資料夾：`PCCSRV\Admin\Utility\RmAgent`，然後啟動應用程式 `TMRMAgentforWFBS.exe`。

   例如：`C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   注意
   如果您從「Security Server Setup」畫面啟動安裝，請略過此步驟。
4. 選取「我已經有 Trend Micro Remote Manager 帳號且我想要安裝代理程式」，然後按一下「下一步」。

5. 選取「與現有 Licensing Management Platform 使用授權建立關聯」，然後按一下「下一步」。
6. 指定 Remote Manager 帳號認證，然後按一下「下一步」。
7. 如果需要，請指定 Proxy 伺服器資訊，然後按一下「下一步」。
8. 如果需要，請指定安裝資料夾，然後按一下「下一步」。
9. 按一下「完成」。

   如果安裝成功且設定正確，Remote Manager Agent 應該會自動註冊至 Trend Micro Remote Manager 伺服器。Remote Manager Agent 應該會在 Remote Manager Web 主控台上顯示為「線上」。

從受管理伺服器管理代理程式

本節包含關於如何從受管理伺服器管理代理程式的資訊。

代理程式狀態訊息

在受管理伺服器上，Agent 會顯示以下其中一個系統匣圖示：

表 14-1. 系統匣圖示

圖示	說明
	綠色圖示表示此 Agent 已連線到 Remote Manager 通訊伺服器。Agent 正在正常運作。
	紅色圖示表示此 Agent 未連線到 Remote Manager 通訊伺服器，或此 Agent 的版本與伺服器不相符，需要進行更新。
	帶紅色箭頭的圖示表示此 Agent 已從 Remote Manager 登出。
	帶有紅色「X」的圖示表示 Agent 已關閉。

在受管理伺服器上變更 Agent GUID

如果您在安裝 Remote Manager Agent 期間輸入了錯誤的全域唯一識別碼 (GUID)，請刪除該 Agent，然後使用正確的 GUID 重新進行安裝。如果無法執行上述程序，您可以執行以下作業：

步驟

1. 移至 `C:\Program Files\Trend Micro\TMRMAgentForWFBS`。
2. 使用文字編輯器開啟 `AgentSysConfig.xml` 檔案。
3. 在 `<AgentGUID>` 和 `</AgentGUID>` 參數之間找到 GUID。
4. 編輯 GUID 並儲存該檔案。
5. 使用文字編輯器開啟相同資料夾中的 `csmSysConfig.xml` 檔案。
6. 在 `<ProductGUID>` 和 `</ProductGUID>` 參數之間找到 GUID。
7. 編輯 GUID 並儲存該檔案。
8. 在工作列的 Remote Manager Agent 圖示上按一下滑鼠右鍵，然後按一下「重新啟動服務」。

使用 Agent Configuration Tool

使用 Agent Configuration Tool，可對 Remote Manager Agent 組態設定進行變更。

移至「開始 > 程式集 > Trend Micro Remote Manager Agent > Agent Configuration Tool」，或在系統匣圖示上按一下滑鼠右鍵，然後按一下「設定」。

如需詳細資訊，請參閱 Agent 設定 第 14-9 頁。

Agent 設定

Agent 設定功能表

若要設定 Agent，請以滑鼠右鍵按一下系統匣圖示，以開啟以下功能表：

圖 14-1. Agent Configuration Tool 快顯功能表

其中顯示以下項目：

- 設定：開啟 Agent 設定畫面。
- 選取語言：除了其他可能的語言外，永遠會顯示「英文」語言。
- 服務：「開始」、「停止」和「重新啟用」。
- 結束：結束工具不會停止 Remote Manager 服務。這僅會關閉設定工具，並從工作列中移除該圖示。隨時可以重新啟用該工具。

設定工具主要對話方塊

以滑鼠右鍵按一下系統匣圖示，然後在 Agent 設定功能表上按一下「設定」，以開啟 Agent Configuration Tool 的「一般」標籤。

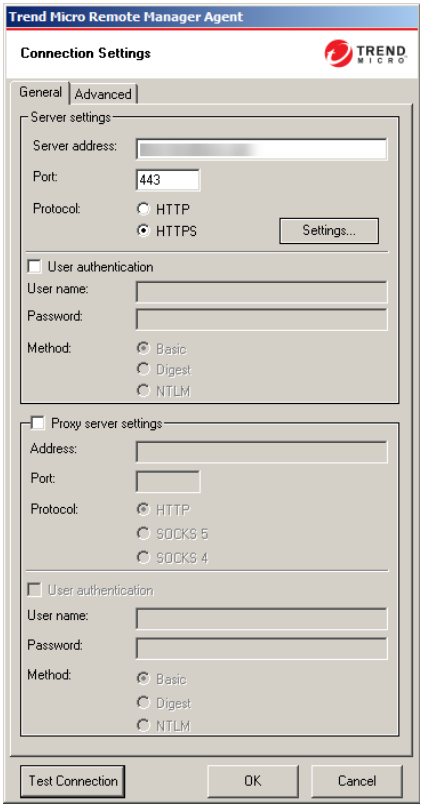


圖 14-2. Agent Configuration Tool 的「一般」功能表

Agent 設定畫面的以下區段只是此工具目前相關的區段。

- 伺服器設定：設定以下內容來設定伺服器通訊：
  - 伺服器位址：Remote Manager 通訊伺服器的完整網域名稱 (FQDN)。FQDN 在各地區有所不同。如果需要變更伺服器位址資訊，請洽詢您的支援代表。

- 通訊埠：Remote Manager 伺服器用來與 Agent 通訊的通訊埠。採用 HTTP 時應為 80，採用 HTTPS 時應為 443。
- 通訊協定：伺服器與 Agent 通訊時所使用的通訊協定。

重要

趨勢科技不建議變更「伺服器位址」或「通訊埠」資訊，除非是您的支援供應商要求您這樣做。

- Proxy 伺服器設定：如果使用者的網路需要 Proxy 來與 Remote Manager 伺服器通訊，可透過按一下「Proxy 伺服器設定」複選框來啟動此區域。
  - 位址：Proxy 伺服器的 IP 位址
  - 通訊埠：通訊埠或 Proxy 伺服器
  - 通訊協定
- 「測試連線」按鈕：「測試連線」按鈕用於測試 Agent 與 Remote Manager 伺服器之間的通訊。使用此功能可測試與通訊伺服器的基本連線是否正常運作。如果測試失敗（工具無法連線至伺服器時，會顯示快顯對話方塊），則可能有基本問題。例如，通訊伺服器的位址和通訊埠有問題，或 Proxy 伺服器的位址和通訊埠有問題。

備份和還原代理程式設定

如果您需要解除安裝 Agent，並在三日內使用相同的 GUID 重新安裝 Agent，請保留 Agent 設定以避免資料有任何重疊。若要執行此作業，請手動備份設定檔案，然後在解除安裝 Agent 後使用備份檔案取代新檔案。

備份設定

步驟

1. 在受管理伺服器上，以滑鼠右鍵按一下 Agent 系統匣圖示，然後按一下「停止服務」，以停止 Agent 服務。

2. 從安裝資料夾複製所有 .xml、.dat 和 .ini 檔案：C:\Program Files \Trend Micro\TMRMAgentForWFBS 或 C:\Program Files (x86)\Trend Micro\TMRMAgentForWFBS。
   - .xml 檔案
     - csmSysConfig.xml
     - csmLocalConfig.xml
     - csmLogDef.xml
     - AgentWorkConfig.xml
     - AgentSysConfig.xml
     - AgentStatus.xml
     - AgentLocalConfig.xml
   - .dat 檔案
     - MSA.dat
     - logBuf.dat
     - group.dat
     - CSA.dat
     - CriticalVA.dat
   - .ini 檔案
     - csmStatusData.ini
3. 從 \Cache 資料夾複製所有檔案。
4. 重新啟用 Agent 服務。

還原設定

步驟

1. 從本機移除 Agent。

   注意

   在本機移除 Agent 時，Agent 會從 Remote Manager 取消註冊，這樣會自動刪除與 Agent 關聯的所有資料。若要防止取消註冊 Agent，請先修改 Agent 介面上的伺服器位址值，然後再移除 Agent。

2. 重新安裝 Agent。確保您使用同一 GUID，其可從 `agentSysConfig.xml` 取得。
3. 在受管理伺服器上，以滑鼠右鍵按一下 Agent 系統匣圖示，然後按一下「停止服務」，以停止 Agent 服務。
4. 使用備份檔案取代設定檔按。
5. 在 Agent 系統匣圖示上按一下右鍵，然後按一下「啟用服務」，以重新啟用服務。

節省磁碟空間

執行 Disk Cleaner 來節省 Security Server 和用戶端上的磁碟空間。

在 Security Server 上執行 Disk Cleaner

開始之前

為了節省磁碟空間，Disk Cleaner Tool (`TMDiskCleaner.exe`) 會識別及刪除下列目錄中未使用的備份、記錄檔及病毒碼檔案：

- `{Security Agent}\AU_Data\AU_Temp\*`

- {Security Agent}\Reserve
- {Security Server}\PCCSRV\TEMP* (隱藏檔案除外)
- {Security Server}\PCCSRV\Web\Service\AU_Data\AU_Temp*
- {Security Server}\PCCSRV\wss*.log
- {Security Server}\PCCSRV\wss\AU_Data\AU_Temp*
- {Security Server}\PCCSRV\Backup*
- {Security Server}\PCCSRV\Virus* (刪除超過兩週的隔離檔案，NOTVIRUS 檔案除外)
- {Security Server}\PCCSRV\ssaptpn.xxx (僅保留最新的病毒碼)
- {Security Server}\PCCSRV\lpt$vpn.xxx (僅保留最新的病毒碼)
- {Security Server}\PCCSRV\icrc$oth.xxx (僅保留最新的病毒碼)
- {Security Server}\DBBackup* (僅保留最新的兩個子資料夾)
- {Messaging Security Agent}\AU_Data\AU_Temp*
- {Messaging Security Agent}\Debug*
- {Messaging Security Agent}\engine\vsapi\latest\pattern*

步驟

1. 在 Security Server 上，移到下列目錄：

   {伺服器安裝資料夾}\PCCSRV\Admin\Utility\

2. 按兩下 TMDiskCleaner.exe。

   隨即顯示 Trend Micro Worry-Free Business Security Disk Cleaner。

   注意

   無法恢復檔案。

3. 按一下「刪除檔案」以掃瞄及刪除未使用的備份、記錄及病毒碼檔案。

使用命令列介面在 Security Server 上執行 Disk Cleaner

步驟

1. 在 Security Server 上，開啟「命令提示字元」視窗。
2. 在命令提示字元執行下列命令：

   ```
   TMDiskCleaner.exe [/hide] [/log] [/allowundo]
   ```

   - `/hide`:以背景處理程序執行工具。
   - `/log`:將作業的記錄儲存至位於目前資料夾中的 DiskClean.log。

     注意

     唯有在使用 `/hide` 時才能使用 `/log`。

   - `/allowundo`:將檔案移至「資源回收筒」，並不會永久刪除檔案。
3. 若要時常執行 Disk Cleaner Tool，請使用 Windows「排定的工作」設定新工作。如需詳細資訊，請參閱 Windows 文件。

節省用戶端上的磁碟空間

步驟

- 在具有 Security Agent 的桌上型電腦/伺服器上：
  - 清除隔離檔案
  - 清除記錄檔

  - 執行 Windows Disk Cleanup Utility
- 在具有 Messaging Security Agent 的 Microsoft Exchange Server 上：
  - 清除隔離檔案
  - 清除記錄檔
  - 執行 Windows Disk Cleanup Utility
  - 清除封存記錄
  - 清除備份檔案
  - 檢查 Microsoft Exchange 資料庫或交易記錄檔的大小

移動 Scan Server 資料庫

如果安裝了 Scan Server 的磁碟機空間不足，請使用 Scan Server Database Mover Tool 將 Scan Server 資料庫安全移動至其他磁碟機。

請確保 Security Server 電腦具有多個磁碟機，並且新磁碟機有至少 3GB 可用磁碟空間。不可使用網路磁碟機。請勿手動移動資料庫或使用其他工具。

步驟

1. 在 Security Server 電腦上，瀏覽至 `<Security Server 安裝資料夾>\PCCSRV\Admin\Utility`。
2. 啟動 `ScanServerDBMover.exe`。
3. 按一下變更。
4. 按一下瀏覽，然後瀏覽至其他磁碟機上的目標目錄。
5. 按一下確定，在資料庫移動後，按一下完成。

還原加密檔案

為了防止開啟中毒檔案，Worry-Free Business Security 會在下列情況下加密檔案：

- 隔離檔案前
- 在清除檔案前加以備份時

Worry-Free Business Security 提供的一個工具可在您需要從檔案中擷取資訊時，將檔案解密，然後恢復檔案。Worry-Free Business Security 可以解密及恢復下列檔案：

表 14-2. Worry-Free Business Security 可以解密及恢復的檔案

檔案	說明
用戶端上的隔離檔案	這些檔案位於以下目錄中： • <Security Agent 安裝資料夾>\SUSPECT\Backup 或 <Security Agent 安裝資料夾>\quarantine（任一可用目錄）。 • <Messaging Security Agent 安裝資料夾>\storage\quarantine 這些檔案會上傳至指定的隔離目錄（通常是 Security Server 上的目錄）。
指定隔離目錄中的隔離檔案	依預設，此目錄位於 Security Server 電腦上（<Security Server 安裝資料夾>\PCCSRV\Virus）。若要變更目錄，請瀏覽至「管理 > 全域設定 > 系統」標籤，然後移至「隔離維護」區段。
備份的加密檔案	這些是代理程式可清除之中毒檔案的備份。這些檔案位於以下資料夾中： • <Security Agent 安裝資料夾>\Backup。 • <Messaging Security Agent 安裝資料夾>\storage\backup 若要恢復這些檔案，使用者必須將其移至用戶端上的隔離資料夾中。

警告!

恢復中毒檔案可能會將病毒/惡意程式散佈到其他檔案與用戶端。在恢復檔案前，請先隔離中毒用戶端，並將此用戶端上的重要檔案移至備份位置。

解密及恢復 Security Agent 上的檔案

步驟

1. 開啟命令提示字元，然後瀏覽至 <Security Agent 安裝資料夾>。
2. 輸入下列命令，以執行 VSEncode.exe：

   ```
   VSEncode.exe /u
   ```

   此參數會開啟一個畫面，其中顯示位於<Security Agent 安裝資料夾>\SUSPECT\Backup 下的檔案清單。

   系統管理員可從「間諜程式/可能的資安威脅程式」標籤恢復被歸類為間諜程式/可能的資安威脅程式的檔案。畫面會顯示在以下路徑找到的檔案清單：<Security Agent 安裝資料夾>\BackupAS。
3. 選取要恢復的檔案，然後按一下「恢復」。

   注意

   此工具一次只能恢復一個檔案。
4. 在開啟的畫面中，指定要將檔案恢復到哪個資料夾。
5. 按一下「確定」。

   注意

   在檔案恢復後，代理程式有可能重新掃瞄該檔案，並將其視為中毒檔案。為了防止該檔案遭到掃瞄，請將其新增至掃瞄例外清單中。

   請參閱 Security Agent 的掃瞄目標和處理行動 第 7-8 頁。

   檔案即會恢復到指定的資料夾。

6. 按一下「關閉」。

解密及恢復 Security Server、自訂隔離目錄或 Messaging Security Agent 上的檔案

步驟

1. 如果檔案位於 Security Server 電腦上，請開啟命令提示字元，然後瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\VSEncrypt。

   如果檔案位於 Messaging Security Agent 用戶端或自訂隔離目錄中，請瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility，然後將 VSEncrypt 資料夾複製到用戶端或自訂隔離目錄。

2. 建立文字檔，然後輸入要加密或解密的檔案的完整路徑。

   例如，如果要恢復 C:\My Documents\Reports 中的檔案，請在文字檔中輸入 C:\My Documents\Reports*.*。

   Security Server 電腦上的隔離檔案位於 <伺服器安裝資料夾>\PCCSRV\Virus 下。

3. 以 INI 或 TXT 副檔名儲存文字檔。例如，您可以在 C: 磁碟機上將其儲存為 ForEncryption.ini。

4. 開啟命令提示字元，然後瀏覽至 VSEncrypt 資料夾所在的目錄。

5. 輸入下列命令，以執行 VSEncode.exe：

   ```
   VSEncode.exe /d /i <INI 或 TXT 檔案的位置>
   ```

   說明：

   <INI 或 TXT 檔案的位置>就是您建立的 INI 或 TXT 檔案的路徑（例如：C:\ForEncryption.ini）。

6. 使用其他參數發出各種命令。

表 14-3. 恢復參數

參數	說明
無（沒有參數）	加密檔案
/d	解密檔案
/debug	建立偵錯記錄檔，並將其儲存至電腦。在用戶端上，會於 <代理程式安裝資料夾> 中建立偵錯記錄檔 VSEncrypt.log。
/o	覆寫已存在的加密或解密檔案
/f <檔案名稱>	加密或解密單一檔案
/nr	不恢復原始檔名
/v	顯示工具的相關資訊
/u	啟動工具的使用者介面
/r <目標資料夾>	用以恢復檔案的資料夾
/s <原始檔案名稱>	原始加密檔案的檔名

例如，輸入 VSEncode [/d] [/debug]，可以解密 Suspect 資料夾中的檔案，並建立偵錯記錄檔。當您解密或加密檔案時，Worry-Free Business Security 便會在相同資料夾中建立解密或加密檔案。在解密或加密檔案前，請確認檔案並未鎖定。

恢復傳輸中立封裝格式的電子郵件

傳輸中立封裝格式 (TNEF) 是 Microsoft Exchange/Outlook 所使用的郵件封裝格式。這種格式通常都封裝成名為 Winmail.dat 的電子郵件附件，Outlook Express 會自動隱藏此附件。

如需詳細資訊，請參閱 https://support.microsoft.com/en-us/help/290809/。

如果 Messaging Security Agent 封存這類電子郵件，而且檔案的副檔名已變更為 .EML，則 Outlook Express 將只會顯示電子郵件的內文。

使用 ReGenID 工具

每個 Security Agent 安裝都需要一個全域唯一識別碼 (GUID)，如此 Security Server 才能識別各個代理程式。重複的 GUID 通常出現在複製的用戶端或虛擬機器上。

如果兩個或更多個代理程式報告相同的 GUID，請執行 ReGenID 工具，以為每個用戶端產生唯一的 GUID。

步驟

1. 在 Security Server 上，移到下列目錄：`<Server 安裝資料夾>\PCCSRV\Admin\Utility`。
2. 將 `WFBS_WIN_All_ReGenID.exe` 複製到安裝 Security Agent 所在用戶端上的暫存資料夾。

   例如：`C:\temp`
3. 按兩下 `WFBS_WIN_All_ReGenID.exe`，然後按照畫面上的指示操作。

   該工具會停止 Security Agent 並移除用戶端 GUID。
4. 重新啟動 Security Agent。

   Security Agent 會產生新的用戶端 GUID。

管理 SBS 及 EBS 快捷工具列

Worry-Free Business Security 提供快捷工具列，可讓管理員從下列 Windows 作業系統的主控台即時檢視安全和代理程式狀態資訊：

- Windows Small Business Server (SBS) 2008
- Windows Essential Business Server (EBS) 2008
- Windows SBS 2011 Standard/Essentials

- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

手動安裝 SBS 及 EBS 快捷工具列

SBS 或 EBS 快捷工具列會在您將 Security Server 安裝到執行所支援作業系統的端點上時自動安裝。若要在執行這些所支援作業系統的其他端點上使用快捷工具列，您需要手動安裝快捷工具列。

步驟

1. 登入 Security Server Web 主控台。
2. 移至「管理 > 管理工具」。
3. 按一下「快捷工具列」。
4. 按一下對應的下載連結，取得安裝程式。
5. 將安裝程式複製到目標端點並啟動。

使用 SBS 或 EBS 快捷工具列

步驟

1. 開啟 SBS 或 EBS 主控台。
2. 在「安全性」標籤下，按一下「Trend Micro Worry-Free Business Security」，檢視狀態資訊。

附錄 A

Security Agent 圖示

本附錄說明顯示在用戶端上的不同 Security Agent 圖示。

檢查 Security Agent 狀態

下列影像顯示 Security Agent 主控台，其上的所有元件都是最新狀態且正常運作：

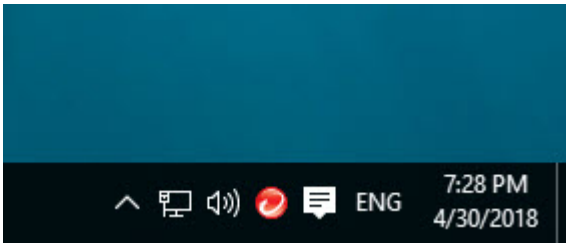
下表列出 Security Agent 主控台主要使用者介面上的圖示與其代表的意義：

表 A-1. Security Agent 主控台主要使用者介面圖示

圖示	狀態	說明和處理行動
	安全防護已啟動：您的電腦已受保護，且軟體是最新的	軟體是最新狀態且正常執行。不需要處理行動。
	重新啟動電腦：請重新啟動電腦以完成修復安全威脅	Security Agent 已發現安全威脅，但無法立即修復。 請重新啟動電腦以完成修復這些安全威脅。
	安全防護有風險：聯絡系統管理員	「即時掃瞄」遭到關閉，或其他原因造成電腦的安全防護有風險。 請啟動「即時掃瞄」。如果這樣不能解決問題，請聯絡客服部門。
	立即更新：您未接收更新的天數（數字）	病毒碼已超過 3 天。 請立即更新 Security Agent。
	雲端截毒掃瞄無法使用：檢查 Internet 連線	Security Agent 已超過 15 分鐘未存取「掃瞄伺服器」。 請確定您已連線至網路，以便使用最新病毒碼來掃瞄。
	重新啟動電腦：請重新啟動電腦以完成安裝更新	請重新啟動電腦以完成更新。
	正在更新程式：您的安全防護軟體正在更新	更新正進行中。結束前，請勿中斷網路連線。

檢視 Windows 工作列上的 Security Agent 圖示

Windows 工作列會顯示下列 Security Agent 圖示：



圖示	意義
	狀態為正常
	（動畫顯示）正在執行手動掃瞄或預約掃瞄。Security Agent 正在使用標準掃瞄或雲端截毒掃瞄。
	Security Agent 正在執行更新。
	需要執行處理行動： • 已關閉即時掃瞄 • 必須重新啟動，才能完全清除惡意程式 • 由於已更新引擎，必須重新啟動 • 必須重新啟動，才能還原勒索軟體加密的檔案 • 需要更新 **注意** 開啟 Security Agent 主畫面以查看需要執行的處理行動。

存取主控台浮動視窗

將滑鼠游標移到 Security Agent 主控台右下方的小圖示上時，Security Agent 主控台浮動視窗將會開啟。

下表列出主控台浮動視窗的圖示與其意義：

表 A-2. 主控台浮動視窗圖示

功能	圖示	意義
連線		已連線至 Security Server
		未連線至 Security Server，但即時掃瞄仍在執行。病毒碼檔案可能不是最新的。在 Windows 工作列上的用戶端圖示上請點選右鍵，然後請點選「立即更新」。
位置		在辦公室中（內部網路）
		辦公室以外的地方（外部網路）
即時掃瞄		開啟
		關閉
POP3 電子郵件掃瞄		開啟
		關閉

功能	圖示	意義
雲端截毒掃瞄		已連線至趨勢科技主動式雲端截毒技術
		無法連線至主動式雲端截毒技術；由於 Security Agent 無法傳送掃瞄查詢，防護會降低。 注意 請確認雲端截毒掃瞄服務 TMiCRCScanService 正在執行，並且 Security Agent 已連線至 Security Server。
		「雲端截毒掃瞄」已關閉。正在使用「標準掃瞄」
• 防火牆 • 網頁信譽評等 • URL 過濾 • 行為監控 • 周邊設備存取控管 • Machine Learning		開啟
		關閉

附錄 B

Worry-Free Business Security 中的 IPv6 支援

本附錄的適用對象是打算在支援 IPv6 定址的環境中部署 Worry-Free Business Security 的使用者。本附錄包含有關 Worry-Free Business Security 中 IPv6 支援範圍的資訊。

趨勢科技假設讀者熟悉 IPv6 概念及設定支援 IPv6 定址之網路的相關工作。

Worry-Free Business Security 和 Security Agent 的 IPv6 支援

自 8.0 版起，Worry-Free Business Security 支援 IPv6。先前的 Worry-Free Business Security 版本不支援 IPv6 定址。安裝或升級符合 IPv6 需求的 Security Server、Security Agent 和 Messaging Security Agent 之後，會自動啟動 IPv6 支援。

Security Server IPv6 需求

Security Server 的 IPv6 需求如下：

- 如果伺服器將管理 IPv4 和 IPv6 代理程式，則必須同時具有 IPv4 和 IPv6 位址，且必須由其主機名稱加以識別。如果伺服器是由其 IPv4 位址所識別，則純 IPv6 代理程式無法連線到該伺服器。如果純 IPv4 用戶端連線到由其 IPv6 位址所識別的伺服器，則會發生相同的問題。
- 如果伺服器將只會管理 IPv6 代理程式，則最低需求為一個 IPv6 位址。伺服器可由其主機名稱或 IPv6 位址加以識別。當伺服器由其主機名稱所識別時，會偏好使用其「完整合格的網域名稱 (FQDN)」。這是因為在純 IPv6 環境中，WINS 伺服器無法將主機名稱轉換為其對應的 IPv6 位址。
- 確認可以使用如「`ping`」或「`nslookup`」等命令擷取主機的 IPv6 或 IPv4 位址。
- 如果您正在純 IPv6 電腦上安裝 Security Server，請設定一個可在 IPv4 和 IPv6 位址之間進行轉換的雙堆疊 Proxy 伺服器（例如 DeleGate）。將 Proxy 伺服器置於 Security Server 與 Internet 之間，以便讓伺服器成功連線到趨勢科技代管的服務，例如：主動式更新伺服器、線上註冊網站和主動式雲端截毒技術。

Messaging Security Agent 需求

Messaging Security Agent（僅限 Advanced 版）必須安裝在雙堆疊或純 IPv6 Microsoft Exchange Server 上。

Messaging Security Agent 最好同時具有 IPv4 和 IPv6 位址，因為與它連線的一些實體僅支援 IPv4 定址。

單純 IPv6 伺服器的限制

下表列出 Security Server 僅具有 IPv6 位址時所存在的限制。

表 B-1. 單純 IPv6 伺服器的限制

項目	限制
代理程式管理	純 IPv6 伺服器無法執行以下操作： • 將代理程式部署到純 IPv4 用戶端。 • 管理純 IPv4 代理程式。
更新和集中式管理	純 IPv6 伺服器無法從純 IPv4 更新來源更新，例如： • 趨勢科技主動式更新伺服器 • 任何純 IPv4 自訂更新來源
產品註冊、啟動和續約	純 IPv6 伺服器無法連線到趨勢科技線上註冊伺服器註冊產品、取得使用授權和啟動/續約使用授權。
Proxy 伺服器連線	純 IPv6 伺服器無法透過純 IPv4 Proxy 伺服器進行連線。
嵌入程式解決方案	純 IPv6 伺服器會包含 Plug-in Manager，但無法將任何 Plug-in 解決方案部署到： • 純 IPv4 代理程式或純 IPv4 主機（因為無法直接連線） • 純 IPv6 代理程式或純 IPv6 主機（因為嵌入程式解決方案都不支援 IPv6）。

透過設定可在 IPv4 和 IPv6 位址之間進行轉換的雙堆疊 Proxy 伺服器（例如 DeleGate），可以克服上述大部分的限制。將 Proxy 伺服器置於 Security Server 以及它所連線或服務的實體之間。

純 IPv6 Security Agent 的限制

下表列出 Security Agent 僅具有 IPv6 位址時所存在的限制。

表 B-2. 純 IPv6 Security Agent 的限制

項目	限制
上層 Security Server	純 IPv4 Security Server 無法管理純 IPv6 代理程式。
更新	純 IPv6 Security Agent 無法從純 IPv4 更新來源更新，例如： • 趨勢科技主動式更新伺服器 • 純 IPv4 Security Server • 純 IPv4 更新代理程式 • 任何純 IPv4 自訂更新來源
掃瞄查詢和 Smart Feedback	純 IPv6 Security Agent 無法傳送查詢至趨勢科技主動式雲端截毒技術，也無法使用 Smart Feedback。
嵌入程式解決方案	純 IPv6 代理程式無法安裝嵌入程式解決方案，因為所有嵌入程式解決方案都不支援 IPv6。
Proxy 連線	純 IPv6 Security Agent 無法透過純 IPv4 Proxy 伺服器進行連線。

透過設定可在 IPv4 和 IPv6 位址之間進行轉換的雙堆疊 Proxy 伺服器（例如 DeleGate），可以克服上述大部分的限制。將 Proxy 伺服器置於 Security Agent 與它們連線的實體之間。

設定 IPv6 位址

透過 Web 主控台可設定 IPv6 位址或 IPv6 位址範圍。下面是一些組態設定準則。

- Worry-Free Business Security 接受標準的 IPv6 位址表示法。

  例如：

  ```
  2001:0db7:85a3:0000:0000:8a2e:0370:7334
  ```

```
2001:db7:85a3:0:0:8a2e:370:7334
```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- Worry-Free Business Security 也接受連結-本機 IPv6 位址，例如：

```
fe80::210:5aff:feaa:20a2
```

警告!

指定連結-本機 IPv6 位址時應謹慎小心，因為即使 Worry-Free Business Security 可以接受這類位址，但它可能在某些情況下無法如預期般運作。例如，如果更新來源位於其他網路區段且可由其連結-本機 IPv6 位址所辨識，Security Agent 就無法從該來源進行更新。

- IPv6 位址是 URL 的一部分時，請使用方括號 ([]) 將位址括起來。
- 對於 IPv6 位址範圍，通常需要輸入字首和字首長度。對於需要伺服器查詢 IP 位址的組態，會套用字首長度限制，以防止伺服器查詢大量 IP 位址時可能出現效能問題。例如，對於外部伺服器管理功能，字首長度只能介於 112（65,536 個 IP 位址）和 128（2 個 IP 位址）之間。
- 涉及 IPv6 位址或位址範圍的某些設定會部署到 Security Agent，但是 Security Agent 會暫不處理這些設定。例如，如果設定了主動雲端截毒技術來源清單，其中包括可由其 IPv6 位址辨識的主動雲端截毒技術伺服器，則純 IPv4 Security Agent 會略過該伺服器並連線到其他主動雲端截毒技術來源。

顯示 IP 位址的畫面

本主題將列舉 Web 主控台中顯示 IP 位址的位置。

- 安全群組樹狀結構

  每當用戶端樹狀結構顯示時，純 IPv6 代理程式的 IPv6 位址都會顯示在「IP 位址」欄下。對於雙堆疊代理程式，如果它們使用自己的 IPv6 位址向伺服器註冊，則會顯示它們的 IPv6 位址。

注意

雙堆疊代理程式向伺服器註冊時所用的 IP 位址，可以在「管理 > 全域設定 > 桌上型電腦/伺服器」標籤的「偏好的 IP 位址」區段中進行控制。

將代理程式設定匯出至檔案時，IPv6 位址也會顯示在匯出檔案中。

- 記錄檔

  雙堆疊代理程式和純 IPv6 代理程式的 IPv6 位址會顯示在記錄檔中。

附錄 C

技術支援

瞭解下列主題：

- 疑難排解資源 第 C-2 頁
- 聯絡趨勢科技 第 C-3 頁
- 將可疑內容傳送到趨勢科技 第 C-4 頁
- 其他資源 第 C-5 頁

疑難排解資源

聯絡技術支援之前，請考慮造訪下列趨勢科技線上資源。

使用支援入口網站

趨勢科技支援入口網站是全年無休的線上資源，包含有關常見和不常見問題的最新資訊。

步驟

1. 移至 https://success.trendmicro.com。
2. 從可用產品中進行選取，或請點選適當的按鈕來搜尋解決方案。
3. 使用「搜尋支援」方塊搜尋可用的解決方案。
4. 如果未找到解決方案，請點選「聯絡支援」，然後選取所需的支援類型。

秘訣

若要線上提交支援案例，請造訪下列 URL：

https://success.trendmicro.com/smb-new-request

趨勢科技支援工程師會在 24 小時或更短時間內調查案例並對其進行回應。

安全威脅百科全書

現今的大多數惡意程式都包含混合安全威脅（合併了兩種或更多種技術），以略過電腦安全通訊協定。趨勢科技會使用建立自訂防範策略的產品來抵禦此複雜惡意程式。安全威脅百科全書提供了多種混合性安全威脅的名稱和癥狀的完整清單，包括已知惡意程式、垃圾郵件、惡意 URL 和已知弱點。

移至 https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware 以瞭解更多資訊：

- 目前正在使用中或「擴散中」的惡意程式和惡意可攜式程式碼。
- 用於形成完整網頁攻擊過程的關聯安全威脅資訊頁面
- 有關目標攻擊和安全威脅的 Internet 安全威脅諮詢
- 網頁攻擊和線上趨勢資訊
- 每週惡意程式報告

聯絡趨勢科技

可以透過電話或電子郵件聯絡趨勢科技代表：

地址	趨勢科技股份有限公司 台北市敦化南路二段 198 號 8 樓
電話	(886) 2-23789666
網站	https://www.trendmicro.com
電子郵件信箱	http://www.trend.com.tw/corpmail/

- 全球客戶服務據點：

  https://www.trendmicro.com/us/about-us/contact/index.html

- 與台灣趨勢科技聯絡：

  http://www.trendmicro.tw/tw/about-us/contact/index.html

- 趨勢科技產品文件：

  https://docs.trendmicro.com

加速支援要求

為了提高解決問題的速度，現已提供下列資訊：

- 問題模擬的步驟
- 裝置或網路資訊
- 電腦品牌、型號以及連接的任何其他硬體或裝置
- 記憶體大小和可用硬碟空間
- 作業系統和 Service Pack 版本
- 安裝的用戶端版本
- 產品序號或啟動碼
- 安裝環境的詳細說明
- 已接收的任何錯誤訊息的確切文字

將可疑內容傳送到趨勢科技

有多個選項可供將可疑內容傳送到趨勢科技，以便進一步分析。

電子郵件信譽評等服務

查詢特定 IP 位址的信譽評等，並指定一個訊息轉移用戶端，以將其包含在全域核可清單中：

https://servicecentral.trendmicro.com/en-us/ers/

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

https://success.trendmicro.com/solution/1112106

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交到趨勢科技：

https://success.trendmicro.com/solution/1059565

記錄案例編號以供追蹤。

網頁信譽評等服務

查詢疑似網路釣魚網站的 URL 的安全分級和內容類型，或其他所謂「病媒」（間諜程式和惡意程式等 Internet 威脅的蓄意來源）：

https://global.sitesafety.trendmicro.com/

如果指定的分級不正確，請傳送重新分類要求到趨勢科技。

其他資源

除了解決方案和支援外，線上還提供許多其他實用資源，可讓您保持最新狀態、瞭解創新以及最新的安全趨勢。

下載專區

有時，趨勢科技可能會針對報告的已知問題發行修補程式，或是發行適用於特定產品或服務的升級。如果要瞭解是否有適用的修補程式，請移至：

https://www.trendmicro.com/download/

如果未套用修補程式（修補程式已過期），請開啟 Readme 檔以判斷其是否與您的環境相關。Readme 檔還包含安裝說明。

文件意見反應

趨勢科技始終力求改善其文件。如果您對本文件或趨勢科技的任何文件有任何疑問、意見或建議，請透過 docs@trendmicro.com 聯絡我們。

附錄 D

產品術語詞彙和概念

此附錄所包含的項目提供趨勢科技產品和技術的更多相關資訊。

重要修補程式

重要修補程式著重於安全問題，適合對所有客戶進行部署。Windows 重要修補程式包括安裝程式，而非 Windows Patch 一般則有安裝程式檔。

Hot Fix

Hotfix 是針對單一客戶回報的問題的因應措施或解決方案。HotFix 是針對特定問題，所以不會對所有客戶發行。Windows HotFix 包括安裝程式，而非 Windows HotFix 則不包括（通常您需要停止程式精靈、複製檔案以覆寫安裝中的對應檔案，然後重新啟動精靈）。

智慧型掃瞄

「智慧型掃瞄」是識別要掃瞄之檔案的方法。對於執行檔（例如：.exe），真實的檔案類型取決於檔案內容。針對非執行檔（例如 .txt），則根據檔案標頭判斷真實檔案型態。

使用「智慧型掃瞄」具有以下優點：

- 效能最佳化：由於智慧型掃瞄使用最少的系統資源，所以不會影響代理程式上的應用程式。
- 縮短掃瞄時間：由於「智慧型掃瞄」採用真實檔案型態辨識，只掃瞄容易受到感染的檔案，因此會比掃瞄所有檔案所花的掃瞄時間少很多。

IntelliTrap

IntelliTrap 是趨勢科技的自動邏輯分析技術，可用來發現使用與其他惡意程式特徵（例如：封裝程式）搭配的「即時壓縮」的安全威脅。這涵蓋病毒/惡意程式、蠕蟲、特洛伊木馬程式、後門程式和 Bot。病毒設計者經常會嘗試使用不

同的檔案壓縮格式來規避病毒/惡意程式過濾機制。IntelliTrap 是一種基於規則的病毒碼辨識即時掃瞄引擎技術，可針對目前最常見的 16 種壓縮類型中的任何一種格式，進行已知病毒/惡意程式的偵測與移除作業，最多能夠掃瞄壓縮層數達 17 層的檔案。

注意

IntelliTrap 與病毒掃瞄使用相同的掃瞄引擎。因此，IntelliTrap 將採用系統管理員針對病毒掃瞄所定義的檔案處理和掃瞄規則。

用戶端會將偵測到的 Bot 和其他惡意程式寫入 IntelliTrap 記錄檔。您可以匯出 IntelliTrap 記錄檔的內容，以將其納入報告中。

IntelliTrap 使用下列元件來檢查 Bot 及其他惡意程式：

- 病毒掃瞄引擎
- IntelliTrap 病毒碼
- IntelliTrap 例外病毒碼

入侵偵測系統

入侵偵測系統 (IDS) 有助於在指出端點上可能遭到攻擊的網路封包中識別病毒碼。

入侵偵測系統 (IDS) 有助於防止下列眾所周知的入侵行為：

入侵	說明
Too Big Fragment	一種「拒絕服務」攻擊，其中駭客會將過大的 TCP/UDP 封包導向目標端點。這會造成緩衝區溢位而凍結或重新啟動端點。
Ping of Death	一種「拒絕服務」攻擊，其中駭客會將過大的 ICMP/ICMPv6 封包導向目標端點。這會造成緩衝區溢位而凍結或重新啟動端點。
Conflicted ARP	一種攻擊類型，其中駭客會傳送具有相同來源和目標 IP 位址的「位址解析通訊協定」(ARP) 要求給目標端點。目標端點持續將 ARP 回應（其 MAC 位址）傳送給自己，使端點凍結或當機。

入侵	說明
SYN Flood	一種「拒絕服務」攻擊，其中程式會將多個 TCP 同步化 (SYN) 封包傳送到端點，造成端點持續傳送同步化確認 (SYN/ACK) 回應。這樣會耗盡端點記憶體，最後造成端點當機。
Overlapping Fragment	類似於 Teardrop 攻擊，這種「拒絕服務」攻擊會將重疊的 TCP 片段傳送到端點。這會覆寫第一個 TCP 片段中的標題資訊，且有可能通過防火牆。防火牆可能接著會允許包含惡意程式碼的後續片段通過而到達目標端點。
Teardrop	類似於重疊片段攻擊，這種「拒絕服務」攻擊與 IP 片段有關。位於第二或其後 IP 片段的混淆偏移值可能會造成接收端點上的作業系統在嘗試重組片段時當機。
Tiny Fragment Attack	一種攻擊類型，其中小型 TCP 片段會迫使第一項 TCP 封包標題資訊到下一個片段中。這樣會造成負責過濾流量的路由器忽略後續片段，而其中可能含有惡意資料。
Fragmented IGMP	一種「拒絕服務」攻擊，會將片段式 IGMP 封包傳送到目標端點，而此電腦無法正確處理 IGMP 封包。這樣會凍結或拖慢端點速度。
LAND Attack	一種攻擊類型，會將具有相同來源和目標位址的 IP 同步化 (SYN) 封包傳送給端點，造成端點將同步化確認 (SYN/ACK) 回應傳送給自己。這樣會凍結或拖慢端點速度。

關鍵字

在 Worry-Free Business Security 中，關鍵字包括下列各項，並可用於過濾郵件：

- 字組（guns、bombs 等）
- 數字（1、2、3 等）
- 特定字元（&、#、+ 等）
- 片語（blue fish、red phone、big house 等）
- 以邏輯運算子連接的字組或詞組 (apples .AND. oranges)

- 使用一般表示式的字組或詞組（.REG. a.*e 符合「ace」、「ate」和「advance」，但不包括「all」、「any」或「antivirus」）

Worry-Free Business Security 可以從文字 (.txt) 檔案匯入現有的關鍵字清單。匯入的關鍵字會出現在關鍵字清單中。

在關鍵字上使用運算子

運算子是結合多個關鍵字的命令。運算子可以擴大或縮小條件的結果範圍。以句號 (.) 將運算子括起來。例如：

`apples .AND. oranges 和 apples .NOT. oranges`

注意

運算子前後各緊接一個點。後面的點和關鍵字之間有一個空格。

表 D-1. 使用運算子

操作員	運作方式	範例
任何關鍵字	Messaging Security Agent 會搜尋符合文字的內容	輸入文字，並將它新增到關鍵字清單中
OR	Messaging Security Agent 會就 OR 所分隔的其中任何一個關鍵字進行搜尋 例如：apple OR orange。代理程式會搜尋 apple 或 orange。如果內容包含兩者中的任何一個，即表示符合。	在您要包含的所有字之間輸入「.OR.」 例如， 「apple .OR. orange」
AND	Messaging Security Agent 會就 AND 所分隔的所有關鍵字進行搜尋 例如：apple AND orange。代理程式會搜尋 apple 和 orange。如果內容沒有同時包含這兩個字，即表示不符。	在您要包含的所有字之間輸入「.AND.」 例如， 「apple .AND. orange」

操作員	運作方式	範例
NOT	Messaging Security Agent 會從搜尋中排除跟隨 NOT 之後的關鍵字。 例如，.NOT. juice，代理程式會搜尋沒有包含 juice 的內容。如果郵件含有「orange soda」，即表示符合，但是如果包含「orange juice」，則表示不符。	在您要排除的字前面輸入「`.NOT.`」 例如， 「.NOT. juice」
WILD	萬用字元符號用來替代文字的遺失部分。任何使用萬用字元以外部分所拼寫的字就是符合的項目。 注意 Messaging Security Agent 不支援在萬用字元命令「.WILD.」中使用「?」。	在您要包含的文字部分之前輸入「`.WILD.`」 例如，如果您想要比對所有包含「valu」的字，可輸入「`.WILD.valu`」。因此，Valumart、valucash 和 valubucks 這些字都符合。
REG	如果要指定一般表示式，請在比對模式之前加入 .REG. 運算子（例如，.REG. a.*e）。 請參閱一般表示式 第 D-8 頁。	在您要偵測的文字比對模式前面輸入「`.REG.`」。 例如，「.REG. a.*e」會符合：「ace」、「ate」及「advance」，但不包括「all」、「any」或「antivirus」

有效使用關鍵字

Messaging Security Agent 提供簡單又強大的功能，可以建立極精確的過濾。建立「內容過濾」規則時，請考慮以下因素：

- 依預設，Messaging Security Agent 會搜尋完全符合關鍵字的項目。使用一般表示式搜尋部分符合關鍵字的項目。請參閱一般表示式 第 D-8 頁。
- Messaging Security Agent 會對同行內的多個關鍵字、各佔一行的多個關鍵字，以及利用逗號/句號/連字號和其他標點符號分隔的多個關鍵字，採取不同的分析方式。如需有關使用不同行的多個關鍵字的詳細資訊，請參閱下表。

- 您也可以設定 Messaging Security Agent 搜尋實際關鍵字的同義字。

表 D-2. 如何使用關鍵字

情況	範例	相符/不符
同行的兩個字	guns bombs	相符： 「Click here to buy guns bombs and other weapons.」 不符： 「Click here to buy guns and bombs.」
以逗號分隔的兩個字	guns, bombs	相符： 「Click here to buy guns, bombs, and other weapons.」 不符： 「Click here to buy used guns, new bombs, and other weapons.」
不同行的多個字	guns bombs weapons and ammo	當您選擇「任何指定的關鍵字」時 相符： 「Guns for sale」 相符 2： 「Buy guns, bombs, and other weapons」 當您選擇「所有指定的關鍵字」時 相符： 「Buy guns bombs weapons and ammo」 不符： 「Buy guns bombs weapons ammunition.」 不符 2： 「Buy guns, bombs, weapons, and ammo」

情況	範例	相符/不符
同行相連的多個關鍵字	guns bombs weapons ammo	相符： 「Buy guns bombs weapons ammo」 不符： 「Buy ammunition for your guns and weapons and new bombs」

修補程式

修補程式是一組 Hot Fix 和安全修補程式，可解決多種程式問題。趨勢科技會定期提供修補程式。Windows Patch 包括安裝程式，而非 Windows Patch 一般則有安裝程式檔。

一般表示式

一般表示式可用來執行字串比對。下表列出一些常見的一般表示式範例以供參考。若要指定一般表示式，請在該比對模式之前加一個「.REG.」運算子。

線上有一些相關的網站和教學課程，可供您學習使用。PerlDoc 網站是其中一個這樣的網站，網址是：

http://www.perl.com/doc/manual/html/pod/perlre.html

警告!

一般表示式是強大的字串比對工具。因此，趨勢科技建議選擇使用一般表示式的系統管理員必須熟悉及慣用一般表示式語法。撰寫不當的一般表示式可能對效能造成嚴重的負面影響。趨勢科技建議您先從簡單的一般表示式開始著手，而不要使用複雜的語法。在引進新規則時，請先使用封存處理行動，並觀察 Messaging Security Agent 如何使用您的規則來管理郵件。當您有把握規則不會產生無法預期的結果時，才可以變更處理行動。

一般表示式範例

下表列出一些常見的一般表示式範例以供參考。若要指定一般表示式，請在該比對模式之前加一個「.REG.」運算子。

表 D-3. 計數與分組

項目	涵義	範例
.	點或句號字元代表新行字元以外的任何字元。	do. 的相符項目有 doe、dog、don、dos、dot 等。 d.r 的相符項目有 deer、door 等。
*	星號字元表示星號前面的項目有零個或多個實體。	do* 的相符項目有 d、do、doo、dooo、doooo 等。
+	加號字元表示前面的項目有一個或多個實體。	do+ 的相符項目有 do、doo、dooo、doooo 等，但不包括 d。
?	問號字元表示前面的項目有零個或一個實體。	do?g 的相符項目有 dg 或 dog，但不包括 doog、dooog 等。
( )	括弧字元會將置於其中的任何文字組成群組，以視為單一實體。	d(eer)+ 的相符項目有 deer、deereer、deereereer 等。+ 符號會套用至括弧內的子字串，因此一般表示式會尋找在 d 後跟隨一組或多組「eer」的項目。
[ ]	方括號字元表示一個字元集合或字元範圍。	d[aeiouy]+ 的相符項目有 da、de、di、do、du、dy、daa、dae、dai 等。+ 符號會套用至方括號內的字元集合，因此一般表示式會尋找其後跟隨一個或多個屬於集合 [aeioy] 中任何字元的 d。 d[A-Z] 的相符項目有 dA、dB、dC 等，一直類推到 dZ。方括號中的集合代表從 A 到 Z 之間所有大寫字母的範圍。
[^]	方括號內的插入號 (Carat) 字元會在邏輯上否定指定的集合或範圍，意即一般表示式將比對集合或範圍以外的任何字元。	d[^aeiouy] 的相符項目有 db、dc、dd、d9、d# 等，也就是其後跟隨任何除了母音字母以外單一字元的 d。

項目	涵義	範例
{ }	大括號字元設定前面項目的特定出現次數。大括號內的單一值表示只會比對那些多次。由逗號分隔的一對數字代表前面字元的一組有效計數。後面跟著逗號的單一數字表示沒有上限。	da{3} 的相符項目為 daaa，也就是其後跟隨 3 個且僅出現 3 次「a」的 d。da{2,4} 的相符項目為 daa、daaa、daaaa 和 daaaa（但不包括 daaaaa），也就是其後跟隨出現 2、3 或 4 次「a」的 d。da{4,} 的相符項目如 daaaa、daaaaa、daaaaaa 等，也就是其後跟隨出現 4 或更多次「a」的 d。

表 D-4. 字元類別（速記）

項目	涵義	範例
\d	任何數字字元，功能相當於 [0-9] 或 [[:digit:]]	\d 的相符項目有 1、12、123 等，但不包括 1b7；也就是一個或多個的任何數字字元。
\D	任何非數字字元，功能相當於 [^0-9] 或 [^[:digit:]]	\D 的相符項目有 a、ab、ab&，但不包括 1；也就是一個或多個除了 0、1、2、3、4、5、6、7、8 或 9 以外的任何字元。
\w	任何「字組」字元（即任何英數字元）的功能相當於 [_A-Za-z0-9] 或 [_[:alnum:]]	\w 的相符項目有 a、ab、a1，但不包括 !&；也就是一個或多個大寫或小寫字母或數字，但不包括標點符號或其他特殊字元。
\W	任何非英數字元，功能相當於 [^_A-Za-z0-9] 或 [^_[:alnum:]]	\W 的相符項目如 *、&，但不包括 ace 或 a1，也就是一個或多個除了大寫及小寫字母和數字以外的任何字元。
\s	任何空白字元，空格、新行、定位鍵 (Tab)、不中斷空格等字元，功能相當於 [[:space]]	vegetable\s 與在「vegetable」後跟隨任何空白字元的項目相符。因此字句如「I like a vegetable in my soup」將會觸發一般表示式，但是「I like vegetables in my soup」則不然。

項目	涵義	範例
\S	任何非空白字元，除了空格、新行、定位鍵 (Tab)、不中斷空格等字元，功能相當於 [^[:space]]	vegetable\S 與在「vegetable」後跟隨任何非空白字元的項目相符。因此字句如「I like vegetables in my soup」將會觸發一般表示式，但是「I like a vegetable in my soup」則不然。

表 D-5. 字元類別

項目	涵義	範例
[:alpha:]	任何英文字母字元	.REG.[[:alpha:]]的相符項目有 abc、def、xxx，但不包括 123 或 @#$。
[:digit:]	任何數字字元；功能相當於 \d	.REG.[[:digit:]]的相符項目有 1、12、123 等。
[:alnum:]	任何「字組」字元；也就是任何英數字元，功能相當於 \w	.REG.[[:alnum:]]的相符項目有 abc、123，但不包括 ~!@。
[:space:]	任何空白字元；空格、新行、定位鍵 (Tab)、不中斷空格等字元，功能相當於 \s	.REG.(vegetable)[[:space:]]與其後跟隨任何空白字元的「vegetable」相符。因此字句如「I like a vegetable in my soup」將會觸發一般表示式，但是「I like vegetables in my soup」則不然。
[:graph:]	除了空格、控制字元等以外的任何字元	.REG.[[:graph:]]的相符項目有 123、abc、xxx、><"，但不包括空格或控制字元。
[:print:]	任何字元（與 [:graph:] 類似）可包括空格字元	.REG.[[:print:]]的相符項目有 123、abc、xxx、><" 和空格字元。
[:cntrl:]	任何控制字元（例如：CTRL + C、CTRL + X）	.REG.[[:cntrl:]]的相符項目有 0x03、0x08，但不包括 abc、123、!@#。
[:blank:]	空格和定位字元	.REG.[[:blank:]]與空格和定位字元比對相符，但不包括 123、abc、!@#

項目	涵義	範例
[:punct:]	標點符號字元	.REG.[[:punct:]]的相符項目有 ; :? ! ~ @ # $ % & * ' " , 等，但不包括 123、abc
[:lower:]	任何小寫字母字元（注意：必須先啟動「啟動大小寫相符比對」，否則功能如同 [:alnum:]）	.REG.[[:lower:]]的相符項目有 abc、Def、sTress、Do 等，但不包括 ABC、DEF、STRESS、DO、123、!@#。
[:upper:]	任何大寫字母字元（注意：必須先啟動「啟動大小寫相符比對」，否則功能如同 [:alnum:]）	.REG.[[:upper:]]的相符項目有 ABC、DEF、STRESS、DO 等，但不包括 abc、Def、Stress、Do、123、!@#。
[:xdigit:]	十六進位數字 (0-9a-fA-F) 中允許的數字	.REG.[[:xdigit:]]的相符項目有 0a、7E、0f 等。

表 D-6. 比對模式錨點

項目	涵義	範例
^	表示字串的開頭。	^(notwithstanding) 與開頭為「notwithstanding」的任何文字區塊相符，因此字句如「notwithstanding the fact that I like vegetables in my soup」將會觸發一般表示式，但是「The fact that I like vegetables in my soup notwithstanding」則不然。
$	表示字串的結尾。	(notwithstanding)$ 與結尾為「notwithstanding」的任何文字區塊相符，因此字句如「notwithstanding the fact that I like vegetables in my soup」將不會觸發一般表示式，但是「The fact that I like vegetables in my soup notwithstanding」則會觸發。

表 D-7. 逸出序列和常值字串

項目	涵義	範例
\	用來比對某些在一般表示式中具有特別意義的字元（例如：「+」）。	(1) .REG.C\\C\+\+ 與「C\C++」相符。 (2) .REG.* 與 * 比對相符。 (3) .REG.\? 與 ? 比對相符。
\t	表示定位字元。	(stress)\t 與在子字串「stress」後緊接定位字元 (ASCII 0x09) 的任何文字區塊相符。
\n	表示新行字元。 **注意** 不同平台表示新行字元的方式會有差異。Windows 的新行是一對字元，即歸位字元後面接著換行字元。Unix 和 Linux 的新行只是換行字元，而 Macintosh 的新行則只是歸位字元。	(stress)\n\n 與在子字串「stress」後緊接兩個新行字元 (ASCII 0x0A) 的任何文字區塊相符。
\r	表示歸位字元。	(stress)\r 與在子字串「stress」後緊接一個歸位字元 (ASCII 0x0D) 的任何文字區塊相符。

項目	涵義	範例
\b	表示退格字元。 OR 代表邊界。	(stress)\b 與在子字串「stress」後緊接一個退格字元 (ASCII 0x08) 的任何文字區塊相符。 文字邊界 (\b) 會定義為兩個字元間的點，它的一邊有 \w，另一邊則有 \W（任何順序皆可），當字串的開頭與結尾符合 \W 時即會停止計算虛構的字元（在字元類別內，\b 表示退格字元，而非文字邊界）。 例如，下列的一般表示式會比對社會安全號碼：.REG.\b\d{3}-\d{2}-\d{4}\b
\xhh	表示具有指定十六進位碼（其中的 hh 代表任何兩位數十六進位值）的 ASCII 字元。	\x7E(\w){6} 與包含前有 ~（波浪號）字元再加上正好六個英數字元的「文字」的任何文字區塊相符。因此，字組「~ab12cd」、「~Pa3499」會相符，但「~oops」則不符。

一般表示式產生器

決定如何設定「資料遺失防範」的規則時，請考量一般表示式產生器只能根據下列規則和限制建立簡單的表示式：

- 只能使用英數字元作為變數。
- 所有其他字元（例如 [-] 和 [/] 等）只能作為常數。
- 變數範圍只能介於 A-Z 和 0-9 之間（例如：您無法將範圍限制為 A-D）。
- 此工具產生的一般表示式不區分大小寫。
- 此工具產生的一般表示式只能產生完全相符項目，無法產生部分相符項目（「如果不符合」）。
- 根據您的樣本建立的表示式只能比對字元與空格數與樣本完全相同的項目，此工具無法產生符合「一或多個」指定字元或字串的樣式。

複雜表示式語法

關鍵字表示式是由憑證構成，這是用來比對表示式與內容的最小單位。憑證可以是運算子、邏輯符號或運算元，例如：運算子在其上進行動作的引數或值。

運算子包括 .AND.、.OR.、.NOT.、.NEAR.、.OCCUR.、.WILD.、「.(.」及「.).」。運算元和運算子必須以空格分隔。運算元可能包含數個憑證。請參閱關鍵字 第 D-4 頁。

一般表示式的工作方式

下列範例說明「社會安全」內容過濾（此為其中一個預設過濾）如何運作：

[Format] .REG.\b\d{3}-\d{2}-\d{4}\b

上述表示式使用退格字元 \b，隨後是任意數字 \d，然後是表示位數的 {x}，最後是表示連字號的 -。此表示式與社會安全號碼相符。下表說明符合範例一般表示式的字串：

表 D-8. 與社會安全一般表示式相符的號碼

.REG.\b\d{3}-\d{2}-\d{4}\b	
333-22-4444	符合
333224444	不符
333 22 4444	不符
3333-22-4444	不符
333-22-44444	不符

如果將表示式修改成如下所示，

[Format] .REG.\b\d{3}\x20\d{2}\x20\d{4}\b

新的表示式會符合下列序號：

333 22 4444

掃瞄例外清單

Security Agent 掃瞄例外清單

此例外清單包含所有預設為不掃瞄的趨勢科技產品。

表 D-9. Security Agent 例外清單

產品名稱	安裝路徑位置
InterScan eManager 3.5x	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion ProgramDirectory=
ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11、5.1、5.11、5.12	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion ProgramDirectory=
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite Program Directory= C:\Program Files\Trend Micro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=

產品名稱	安裝路徑位置
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

產品名稱	安裝路徑位置
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder=

產品名稱	安裝路徑位置
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= 從 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir 取得 exclusion.txt 檔案路徑 移至 HomeDir 路徑（例如：C:\Program Files\Trend Micro\Messaging Security Agent\） 開啟 exclusion.txt C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

Messaging Security Agent（僅限 Advanced 版）掃瞄例外清單

依預設，當 Messaging Security Agent 安裝在 Microsoft Exchange Server（2000 或更新版本）上時，不會掃瞄 Microsoft Exchange 資料庫、Microsoft Exchange 記錄檔、虛擬伺服器資料夾或 M:\ 磁碟機。例外清單儲存於：

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
\CurrentVersion\Misc.

ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\

priv1.stm|C:\Program Files\Exchsrvr\mdbdata\

priv1.edb|C:\Program Files\Exchsrvr\mdbdata\

pub1.stm|C:\Program Files\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\
```

對於其他 Microsoft Exchange 建議資料夾，請手動將其新增至掃瞄例外清單。請參閱 http://support.microsoft.com/kb/245822/。

SBS 2003 例外

針對 SBS 2003，請手動新增下列項目：

Microsoft Exchange 例外	
Microsoft Exchange Server 資料庫	`C:\Program Files\Exchsrvr\MDBDATA`
Microsoft Exchange MTA 檔案	`C:\Program Files\Exchsrvr\Mtadata`
Microsoft Exchange Message 追蹤記錄檔	`C:\Program Files\Exchsrvr\server_name.log`
Microsoft Exchange SMTP Mailroot	`C:\Program Files\Exchsrvr\Mailroot`
Microsoft Exchange 工作檔案	`C:\Program Files\Exchsrvr\MDBDATA`
站台複寫服務	`C:\Program Files\Exchsrvr\srsdata` `C:\Program Files\Exchsrvr\conndata`
IIS 例外	

IIS 系統檔案	C:\WINDOWS\system32\inetsrv
IIS 壓縮資料夾	C:\WINDOWS\IIS Temporary Compressed Files
網域控制器例外	
Active Directory 資料庫檔案	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
NTFRS 資料庫檔案	C:\WINDOWS\ntfrs
Windows SharePoint 服務例外	
暫存 SharePoint 資料夾	C:\windows\temp\FrontPageTempDir
用戶端桌上型電腦例外資料夾	
Windows Update 儲存區	C:\WINDOWS\SoftwareDistribution\DataStore
其他例外	
抽取式儲存裝置資料庫（用於 SBS 備份）	C:\Windows\system32\NtmsData
SBS POP3 連接器失敗郵件	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail
SBS POP3 連接器內送郵件	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail
Windows Update 儲存區	C:\WINDOWS\SoftwareDistribution\DataStore
DHCP 資料庫儲存區	C:\WINDOWS\system32\dhcp
WINS 資料庫儲存區	C:\WINDOWS\system32\wins

Service Pack

Service Pack 是重要到足以成為產品升級的 HotFix、Patch 和功能加強的合併整合。Windows 和非 Windows Service Pack 都包括安裝程式和安裝程序檔。

Trojan Port（特洛伊木馬程式通訊埠）

特洛伊木馬程式通訊埠通常是特洛伊木馬程式連線到用戶端所使用的通訊埠。在病毒爆發期間，Worry-Free Business Security 會封鎖下列可能遭特洛伊木馬程式利用的通訊埠號碼。

表 D-10. 特洛伊木馬程式通訊埠

通訊埠號碼	特洛伊木馬程式	通訊埠號碼	特洛伊木馬程式
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver

通訊埠號碼	特洛伊木馬程式	通訊埠號碼	特洛伊木馬程式
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

無法清除病毒的檔案

「病毒掃瞄引擎」無法清除下列檔案：

表 D-11. 無法清除的檔案解決方案

無法清除的檔案	說明和解決方案
感染特洛伊木馬程式的檔案	特洛伊木馬程式是一種會執行無法預期或未經授權（惡意）動作的程式，例如：顯示訊息、刪除檔案、或將磁碟格式化。特洛伊木馬程式不會感染檔案，因此不需要清除。 解決方案：使用損害清除及復原引擎和損害清除及復原範本會移除特洛伊木馬程式。
感染蠕蟲的檔案	蠕蟲是一種自含程式（或一組程式集），可將本身的功能或程式碼的一部分散佈到其他用戶端系統。這種病毒通常透過網路連線或電子郵件的附件散播。由於蠕蟲是自含程式，因此無法清除。 解決方案：趨勢科技建議您刪除蠕蟲。
防寫的中毒檔案	解決方案：移除防寫，以允許清除檔案。

無法清除的檔案	說明和解決方案
密碼保護的檔案	受密碼保護的檔案，包括受密碼保護的壓縮檔或受密碼保護的 Microsoft Office 檔案。 解決方案：移除密碼保護，以允許清除檔案。
備份檔案	副檔名為 RB0~RB9 的檔案是中毒檔案的備份副本。清除程序會建立中毒檔案的備份，以防病毒/惡意程式在清除期間損害檔案。 解決方案：如果成功清除中毒檔案，您便不需要保留其備份複本。如果用戶端運作正常，就可以將備份檔案刪除。

資源回收筒內的中毒檔案	因為系統正在執行，所以系統可能不允許移除「資源回收筒」內的中毒檔案。
	
	解決方案：
	
	1. 在 MS-DOS 模式下重新啟動用戶端。
	2. 開啟命令提示字元。
	3. 輸入下列指令以刪除檔案：
	
	`cd \`
	
	`cd recycled`
	
	`del *.* /S`
	
	最後一個命令可刪除「資源回收筒」內的所有檔案。

Windows Temp 資料夾或 Internet Explorer 暫存資料夾內的中毒檔案	因為用戶端會使用 Windows Temp 資料夾或 Internet Explorer 暫存資料夾中的中毒檔案，所以系統不允許清除這些檔案。要清除的檔案可能是 Windows 作業所需的暫存檔。
	
	解決方案：
	
	1. 在 MS-DOS 模式下重新啟動用戶端。
	2. 如果中毒檔案位於 Windows Temp 資料夾中：
	
	a. 開啟命令提示字元並移至 Windows Temp 資料夾（預設位置為 `C:\Windows\Temp`）。
	
	b. 輸入下列指令以刪除檔案：
	
	`cd temp`
	
	`attrib -h`

無法清除的檔案	說明和解決方案

	`del *.* /S`
	最後一個指令可以刪除 Windows Temp 資料夾中的所有檔案。
	c. 在標準模式下重新啟動用戶端。
	3. 如果中毒檔案位於 Internet Explorer 暫存資料夾中：
	a. 開啟命令提示字元並移至 Internet Explorer Temp 資料夾（預設位於 `C:\Users\<您的使用者名稱>\AppData\Local\Microsoft\Windows\Temporary Internet Files`）。
	b. 輸入下列指令以刪除檔案：
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	最後一個指令會刪除 Internet Explorer 暫存資料夾中所有的檔案。
	c. 在標準模式下重新啟動用戶端。

使用不支援的壓縮格式壓縮的檔案。	解決方案：解壓縮檔案。
鎖住的檔案，或是目前正在執行的檔案。	解決方案：解除鎖定檔案或等候檔案執行完畢。
毀損的檔案。	解決方案：刪除檔案。

索引

A
ActiveX 惡意程式碼, 1-8
AutoPcc.exe, 3-6, 3-7, 3-10

C
Client Packager, 3-7, 3-11–3-13
　設定, 3-12
　部署, 3-14
COM 檔案感染型病毒, 1-8
Conflicted ARP, D-3

D
DHCP 設定, 3-20

E
Early Boot Cleanup 驅動程式, 8-6
EICAR 測試程式檔, 1-8
EXE 檔案感染型病毒, 1-8

F
Fragmented IGMP, D-4

H
HotFix, 8-8
HTML 病毒, 1-8

I
IntelliTrap 例外病毒碼, 8-4
IntelliTrap 病毒碼, 8-4
IPv6 支援, B-2
　限制, B-3, B-4
　顯示 IPv6 位址, B-5

J
JavaScript virus（JavaScript 病毒）, 1-8
Java 惡意程式碼, 1-8

L
LAND Attack, D-4
Login Script Setup, 3-6, 3-7, 3-10

O
Overlapping Fragment, D-4

P
Patch, 8-8
Ping of Death, D-3
Plug-in Manager, 3-4

R
Rootkit 偵測, 8-7

S
Security Agent 安裝
　從 Web 主控台, 3-14
Security Agent 安裝方法, 3-6
SYN Flood, D-4

T
Teardrop, D-4
Tiny Fragment Attack, D-4
Too Big Fragment, D-3

V
VBScript 病毒, 1-8
Vulnerability Scanner, 3-7, 3-17
　DHCP 設定, 3-20
　ping 設定, 3-27
　電腦說明擷取, 3-25

W
Web 主控台, 2-4
　需求, 2-4
　關於, 2-4

Web 安裝網頁, 3-6
WFBS
    文件, xii

一畫
一般防火牆病毒碼, 8-7

二畫
入侵偵測系統, D-3

四畫
中毒處理行動
    間諜程式/可能的資安威脅程式, 7-12
元件, 8-3
元件複製, 8-10
支援
    更快地解決問題, C-4
文件, xii
文件意見反應, C-6

五畫
主動式處理行動, 7-12
主動式雲端截毒技術, 1-3, 1-4
    主動式雲端截毒技術, 1-3
    網頁信譽評等服務, 1-4
    檔案信譽評等服務, 1-3
加密檔案, 14-17
可能的病毒/惡意程式, 1-7
外部裝置防護, 8-7
巨集病毒, 1-8
用戶端安裝
    Client Packager, 3-11
    Login Script Setup, 3-10
    使用 Vulnerability Scanner, 3-17

六畫
安全 Patch, 8-8
安全威脅, 1-9
    間諜程式/可能的資安威脅程式, 1-9
安全策略
    密碼複雜度
        需求, 6-51
安裝前的工作, 3-8, 3-15, 3-18
行為監控核心服務, 8-7
行為監控配置特徵碼, 8-7
行為監控偵測病毒碼, 8-7
行為監控驅動程式, 8-7

七畫
伺服器更新
    元件複製, 8-10
    手動更新, 8-12
    預約更新, 8-12
更新代理程式, 3-4
防火牆
    優點, 5-24

九畫
封裝程式, 1-8

十畫
特洛伊木馬程式, 1-8, 8-5
病毒/惡意程式, 1-7–1-9
    ActiveX 惡意程式碼, 1-8
    COM 和 EXE 檔案感染型病毒, 1-8
    Java 惡意程式碼, 1-8
    VBScript、JavaScript 或 HTML 病毒, 1-8
    可能的病毒/惡意程式, 1-7
    巨集病毒, 1-8
    封裝程式, 1-8
    特洛伊木馬程式, 1-8
    惡作劇程式, 1-7
    測試病毒, 1-8
    開機磁區病毒, 1-8

類型, 1-7–1-9
蠕蟲, 1-9
病毒百科全書, 1-7
病毒掃瞄引擎, 8-5
病毒碼, 8-4, 8-13

十一畫
密碼複雜度, 6-51
掃瞄方法, 3-12
掃瞄類型, 3-3

十二畫
惡作劇程式, 1-7
測試病毒, 1-8
程式, 8-3
程式檔分析器統一病毒碼, 8-8
程式檢測監控病毒碼, 8-8
策略實施特徵碼, 8-8
進階安全威脅關聯病毒碼, 8-6
進階威脅掃描引擎, 8-6
開機磁區病毒, 1-8
間諜程式/可能的資安威脅程式, 1-9
密碼破解應用程式, 1-9
惡作劇程式, 1-9
惡意撥號程式, 1-9
間諜程式, 1-9
遠端存取工具, 1-9
廣告軟體, 1-9
駭客工具, 1-9
間諜程式/可能的資安威脅程式病毒碼, 8-7
間諜程式/可能的資安威脅程式掃瞄
處理行動, 7-12
間諜程式/可能的資安威脅程式掃瞄引擎, 8-6
雲端截毒掃瞄, 5-4

十三畫
損害清除及復原引擎, 8-5
損害清除及復原服務, 3-3
損害清除及復原範本, 8-5
損害還原病毒碼, 8-7
新功能, 1-2
解除安裝
使用解除安裝程式, 3-36
隔離目錄, 5-15, 14-17

十四畫
漸增式病毒碼, 8-10
網頁信譽評等, 1-4, 3-3, 5-2
網路病毒, 5-24
遠端安裝, 3-6

十五畫
數位簽章特徵碼, 8-7
標準掃瞄, 5-4

十七畫
檔案信譽評等, 1-3

十八畫
瀏覽器弱點攻擊防護特徵碼, 8-8

十九畫
關聯式智慧引擎, 8-6
關聯式智慧型病毒碼, 8-6
關聯式智慧查詢處理程式, 8-6

二十畫
蠕蟲, 1-9

TREND MICRO™

趨勢科技股份有限公司

台北市敦化南路二段 198 號 8 樓

電話：(886) 2-23789666　傳真：(886) 2-23780993　info@trendmicro.com

www.trendmicro.com

Item Code: WFTM108706/190701