



Symantec Endpoint Protection Windows 用戶端指南

Updated: November 2022

Table of Contents

如何使用 Symantec Endpoint Protection 保護 Windows 電腦？.....	7
關於 用來保護電腦的技術.....	9
使用 LiveUpdate 更新定義檔.....	9
警示和通知的類型.....	11
關於掃描結果.....	11
回應病毒或風險偵測.....	12
回應詢問您要允許或攔截嘗試下載的檔案的下載鑑識訊息.....	13
回應詢問您是允許還是攔截應用程式的訊息.....	14
回應過期的授權訊息.....	14
回應訊息以更新用戶端軟體.....	15
管理電腦上的掃描.....	16
立即掃描用戶端電腦.....	18
暫停和延緩掃描.....	18
在用戶端上排程使用者定義的掃描.....	19
排程執行隨選或開機掃描.....	21
管理電腦上的下載鑑識偵測.....	21
自訂下載鑑識設定.....	23
自訂病毒和間諜軟體掃描設定.....	23
架構在偵測到惡意軟體與安全風險時採取的動作.....	24
關於排除掃描項目.....	26
排除掃描項目.....	27
管理電腦上的隔離檔案.....	28
啟用自動防護.....	29
瞭解向賽門鐵克傳送資訊可改善電腦防護功能.....	30
關於用戶端和 Windows 資訊安全中心.....	30
管理行為分析 (SONAR).....	31
防止對行為分析 (SONAR) 的誤報偵測.....	32
透過主機完整性掃描檢查電腦安全性遵從.....	32
矯正您的電腦以通過主機完整性檢查.....	33
啟用竄改防護.....	33
病毒和間諜軟體掃描的運作方式.....	34
關於病毒與安全風險.....	34
關於掃描類型.....	36
關於自動防護的類型.....	37
掃描如何回應偵測到的病毒或風險.....	38
如何使用 Symantec Insight 進行檔案相關決策.....	39

管理防火牆防護.....	41
防火牆的運作方式.....	41
在 Windows 用戶端上管理防火牆規則.....	42
用戶端上防火牆規則的元素.....	42
Symantec Endpoint Protection 用戶端程序防火牆規則的順序是什麼？.....	43
在用戶端上新增防火牆規則.....	44
在用戶端上匯入或匯出防火牆規則.....	45
啟用防火牆設定.....	45
在已安裝 用戶端的情況下啟用網路檔案和印表機共用.....	46
允許或攔截應用程式存取網路.....	48
允許或攔截已在用戶端上執行的應用程式.....	48
當螢幕保護程式處於作用中狀態或防火牆未執行時攔截流量.....	49
入侵預防的運作方式.....	51
在 Windows 用戶端上架構入侵預防.....	51
防止攻擊易受攻擊的應用程式.....	52
使用 Web 和雲端存取防護允許或攔截惡意網站.....	54
何謂 Web 和雲端存取防護？.....	54
驗證 Web 和雲端存取防護通道方法是否已在 Windows 用戶端上啟用和連接.....	54
管理 Windows 用戶端.....	58
管理 Windows 用戶端.....	59
瞭解 Symantec Endpoint Protection 用戶端狀態頁面.....	60
隱藏和顯示 用戶端上的通知區域圖示.....	60
關於受管用戶端和非受管用戶端.....	61
檢查用戶端是受管用戶端還是非受管用戶端.....	62
針對 防護問題進行疑難排解.....	63
在用戶端電腦上啟用防護.....	63
關於 Windows 用戶端的日誌.....	64
檢視日誌.....	65
啟用封包日誌.....	65
對話方塊說明.....	66
病毒和間諜軟體防護.....	66
病毒和間諜軟體防護設定：自動防護.....	66
病毒和間諜軟體防護設定：Outlook 自動防護.....	67
病毒和間諜軟體防護設定：下載智慧型掃描.....	67
病毒和間諜軟體防護設定：全域設定.....	68
掃描通知選項.....	69
下載智慧型掃描動作.....	70
下載鑑識通知選項.....	71
提早啟動防惡意軟體.....	71

自動防護進階選項.....	72
磁片設定.....	73
進階掃描選項.....	74
網路掃描設定.....	75
選取的副檔名.....	75
插入警告.....	76
傳送電子郵件至 收件者：訊息.....	76
傳送電子郵件給其他人：其他人.....	77
傳送電子郵件至 收件者：電子郵件伺服器.....	77
掃描動作.....	78
建立新掃描.....	79
建立新掃描 - 選取資料夾和檔案.....	80
建立新掃描 - 掃描選項.....	80
建立新掃描 - 掃描名稱.....	80
建立新掃描 - 排程.....	81
建立新掃描 - 掃描的項目.....	82
建立新掃描 - 掃描的時間.....	82
掃描調整選項.....	82
掃描類型 或 Symantec Endpoint Protection 偵測結果.....	83
Outlook 防護的進階選項.....	84
掃描通知選項.....	84
通知選項.....	85
主動型威脅防護.....	85
行為分析.....	86
系統變更偵測.....	86
採取動作.....	87
防網路和主機侵入.....	87
網路活動.....	87
檢視應用程式設定.....	88
架構應用程式設定.....	89
防網路和主機刺探利用：防火牆.....	90
防網路和主機侵入：通知.....	92
防網路和主機侵入設定：Microsoft Windows 網路.....	93
架構防火牆規則.....	93
新增或編輯防火牆規則：一般.....	93
新增或編輯防火牆規則：主機.....	94
新增或編輯防火牆規則：通訊埠和通訊協定.....	94
新增或編輯防火牆規則：應用程式.....	95
新增或編輯防火牆規則：排程.....	96
檢視防火牆規則.....	96

防網路和主機刺探利用設定：入侵預防.....	97
記憶體攻擊緩和.....	97
Web 和雲端存取防護.....	97
Web 和雲端存取防護設定.....	97
例外.....	98
例外：使用者定義的例外.....	98
已知安全風險例外.....	99
安全風險副檔名例外.....	100
信任的 Web 網域例外.....	100
隔離所.....	100
檢視隔離所.....	101
清除選項：隔離項目.....	101
清除選項：備份項目.....	101
清除選項：修復項目.....	102
用戶端管理.....	102
用戶端管理設定：一般.....	102
Proxy 伺服器設定.....	103
重新開機選項.....	103
用戶端管理設定：竄改防護.....	104
用戶端管理設定：LiveUpdate.....	105
用戶端管理設定：LiveUpdate Proxy 伺服器設定：HTTP.....	105
用戶端管理設定：LiveUpdate Proxy 伺服器設定：FTP.....	106
用戶端管理設定：傳送.....	106
疑難排解.....	107
疑難排解：管理/雲端管理.....	107
疑難排解：混合管理.....	108
疑難排解：版本.....	108
疑難排解：除錯日誌.....	108
用戶端管理除錯日誌設定.....	109
疑難排解：Windows 帳戶.....	109
Symantec Endpoint Protection 除錯日誌設定.....	109
疑難排解：電腦.....	110
疑難排解：安裝設定.....	110
疑難排解：用戶端升級.....	110
疑難排解：伺服器連線狀態或通用雲端連線狀態.....	110
疑難排解：訂購授權狀態.....	111
疑難排解：應用程式強化.....	112
疑難排解：EDR 連線狀態.....	112
疑難排解：Web 和雲端存取防護.....	113
日誌.....	113

疑難排解：日誌.....	113
病毒和間諜軟體防護日誌：掃描日誌.....	114
病毒和間諜軟體防護日誌：風險日誌.....	115
病毒和間諜軟體防護日誌：系統日誌.....	116
主動型威脅防護日誌：威脅日誌.....	116
主動型威脅防護日誌：系統日誌.....	117
強化日誌.....	118
過濾系統日誌.....	119
用戶端管理日誌：系統日誌.....	119
用戶端管理日誌：安全日誌.....	119
竄改防護日誌.....	121
防網路和主機侵入設定：日誌.....	121
用戶端管理日誌：控制日誌.....	122
防網路和主機侵入日誌：流量日誌.....	123
防網路和主機侵入日誌：封包日誌.....	125
回溯檢查資訊.....	126

如何使用 Symantec Endpoint Protection 保護 Windows 電腦？

Windows 適用的 Symantec Endpoint Protection 用戶端指南

用戶端的預設設定可保護您的電腦免受多種安全威脅的入侵。用戶端會自動處理威脅，或是讓您選擇如何處理威脅。

您可以檢查電腦是否受感染，此外，如果想讓電腦更安全或達到更佳效能，可以執行一些額外的的工作。

NOTE

在受管用戶端上，如果您的管理員已將某些選項架構為不可使用，則這些選項不會出現。在未受管用戶端上，大部分選項都會出現。

Table 1: 關於如何保護電腦的常見問題

問題	說明
如何得知我的電腦受到保護？	用戶端會顯示您電腦的防護狀態。 安裝所有防護功能並進行更新，您的電腦便受到最嚴密的保護。 如何判定用戶端電腦是否已使用「狀態」頁面圖示進行防護 Symantec Endpoint Protection 用戶端狀態圖示
如何判斷我的電腦是否已受到感染？	如果您的電腦受到感染，可能會看到下列任一類型的訊息： - 自動防護掃描偵測或手動掃描偵測。 這些訊息描述威脅以及對威脅所採取的動作。您可以選擇其中一個選項來處理威脅。 回應病毒或風險偵測 關於掃描結果 暫停和延緩掃描 「下載鑑識」偵測。 這些訊息描述「下載智慧型掃描」在您嘗試下載時偵測到的惡意和未經證明的檔案。 回應詢問您要允許或攔截嘗試下載的檔案的下載鑑識訊息 警示和通知的類型
如果我的電腦已受到感染，如何清除病毒？	如果您看到掃描視窗，表示您的管理員已經設定電腦對感染採取的動作。您或許可以選擇一個動作。如果您知道某個檔案受到感染，請按下「清除」或「隔離」。 若是排程掃描和「自動防護」，請確定主要動作設為「清除風險」，且次要動作設為「隔離風險」或「刪除」。 回應病毒或風險偵測 病毒和間諜軟體掃描的運作方式 架構在偵測到惡意軟體與安全風險時採取的動作

問題	說明
如何提高電腦的安全性？	根據預設，受管用戶端電腦會受到最大程度的防護。您的管理員可能修改了某些設定，以改善用戶端的效能。 如果您的管理員讓您修改自己電腦的防護設定，便可執行下列工作： - 排程定期完整掃描，通常是一天一次或一週一次。 在用戶端上排程使用者定義的掃描 - 安裝病毒和間諜軟體掃描、自動防護、SONAR、防火牆、入侵預防、記憶體攻擊緩和及下載鑑識，並隨時保持啟用且最新的狀態。 在用戶端電腦上啟用防護 啟用自動防護 防止攻擊易受攻擊的應用程式 在非受管用戶端上，您可以執行下列工作： - 使用 LiveUpdate 下載並安裝正確的病毒定義檔和安全內容。 安全機制應變中心會每天發佈病毒定義檔多次，並定期或視需要發佈其他安全內容。根據預設，用戶端排程為每四小時執行 LiveUpdate 一次。您也可以隨時啟動 LiveUpdate。 使用 LiveUpdate 更新用戶端內容 - 在啟用所有掃描增強功能的情況下，對電腦執行完整掃描。 依預設，您的電腦每週執行一次全面掃描。但您也可以隨時執行掃描。 在用戶端上排程使用者定義的掃描 立即掃描用戶端電腦
如果掃描導致工作速度變慢，要如何修改掃描設定？	如果掃描讓電腦的速度變慢，請調整下列設定： - 建立在營業時間後或您不使用電腦時執行的排程完整掃描。 在用戶端上排程使用者定義的掃描 - 排除您已知為安全的應用程式和檔案。 排除掃描項目 - 關閉掃描壓縮檔，或減少要在壓縮檔內展開已壓縮檔案的層數。 自訂病毒和間諜軟體掃描設定 - 針對使用者定義的掃描停用掃描增強功能選項。 在用戶端上排程使用者定義的掃描 Note: 如果您的管理員已鎖定這些設定，您可能無法變更這些設定。
如果防火牆阻止我瀏覽網際網路，該怎麼做？	根據預設，防火牆不會攔截網際網路存取。如果您無法存取網際網路，請聯絡管理員。管理員可能攔截了對特定網站的存取，或是不允許您的電腦存取特定瀏覽器。您不一定有權限修改防火牆規則。 在未受管用戶端上，您可以修改防火牆規則。不過，除非您瞭解防火牆規則攔截的流量是否為惡意，否則不應該變更或新增防火牆規則。 在您修改防火牆規則之前，請先釐清下列問題： - 存取網際網路的 Web 應用程式是否合法？ - Web 應用程式存取的遠端通訊埠是否正確？HTTP 流量對於 Web 應用程式而言是合法的流量，且 HTTP 流量使用通訊埠 TCP 80 和 443。您可能無法信任來自其他通訊埠的流量。 - 應用程式存取的網站 IP 位址是否正確或合法？ 在用戶端上新增防火牆規則
通知區域中出現訊息時要採取什麼動作？	讀取工具列上通知區域中的訊息。 通知會告訴您下列其中一件事： - 您的電腦可能遭受攻擊，且用戶端已處理威脅。 回應病毒或風險偵測 回應詢問您是允許還是攔截應用程式的訊息 - 您的電腦自動收到新的安全性政策。 根據威脅的類型而定，您還可以查看其中一個日誌檔中的詳細資訊。 檢視日誌

[檢查用戶端是受管用戶端還是非受管用戶端](#)

關於 用來保護電腦的技術

Windows 適用的 Symantec Endpoint Protection 用戶端指南

用戶端結合了多層防護，可主動保護電腦，不受已知和未知的威脅及網路攻擊入侵。

Table 2: 防護類型

防護層	說明
病毒和間諜軟體防護	「病毒和間諜軟體防護」可對抗種類繁多的威脅，包括間諜軟體、病蟲、特洛伊木馬程式、Rootkit 和廣告軟體。「檔案系統自動防護」會持續檢查所有電腦檔案是否有病毒和安全風險。「Microsoft Outlook 自動防護」會掃描內送和外寄的 Outlook 電子郵件訊息。 管理電腦上的掃描
主動型威脅防護	主動型威脅技術包括行為分析 (SONAR)，此工具針對零時差攻擊提供即時防護。行為分析甚至可以在傳統的特徵型定義檔偵測到威脅之前，阻止進攻。行為分析使用啟發式和檔案信譽資料做出有關應用程式或檔案的決策。 管理行為分析 (SONAR)
防網路和主機侵入	此防護包括防火牆、入侵預防系統和記憶體攻擊緩和。 - 以規則為基礎的防火牆可防止未經授權的使用者存取您的電腦。 - 入侵預防系統會自動偵測和攔截網路攻擊。 - 記憶體攻擊緩和會阻止對您的 Windows 電腦上常用應用程式的攻擊。 管理防火牆防護 架構入侵預防 防止攻擊易受攻擊的應用程式
Web 和雲端存取防護	「Web 和雲端存取防護」會將網路流量從 Symantec Endpoint Protection 用戶端重新導向至 Symantec Web Security Service，以根據管理員所設定的規則來允許或攔截流量。 何謂 Web 和雲端存取防護？

您的管理員負責控制管理伺服器將哪些類型的防護下載到您的用戶端電腦。用戶端也會將病毒定義檔、IPS 定義檔和產品更新下載到您的電腦。如果您在旅途中攜帶可攜式電腦，則可直接從 LiveUpdate 取得病毒定義檔和產品更新。

[使用 LiveUpdate 更新用戶端內容](#)

使用 LiveUpdate 更新定義檔

Windows 適用的 Symantec Endpoint Protection 用戶端指南

賽門鐵克的產品需要擁有最新的資訊，才能保護您的電腦免受最新的病毒侵入。這些資訊是透過賽門鐵克的 LiveUpdate 提供。

內容更新檔利用最新的威脅防護技術，使賽門鐵克產品保持在最新狀態。您收到的內容更新視您安裝在電腦上的防護而定。例如，LiveUpdate 會下載病毒和間諜軟體防護的病毒定義檔，以及「網路威脅防護」的 IPS 定義檔。

從 14 開始，用戶端也可以存取雲端中的完整內容集。在連線至雲端的標準或內嵌式/VDI 用戶端上執行的掃描可取得雲端中的完整定義檔集。

[Windows 用戶端如何從雲端接收定義檔](#)

LiveUpdate 也可以在需要時，提供已安裝用戶端的改進功能。這些改進的建立通常是用來延伸作業系統或硬體的相容性調整效能問題或是修正產品錯誤。只要經過架構，這些更新可以透過管理伺服器提供給受管用戶端。

LiveUpdate 會從賽門鐵克 Internet 網站擷取新的內容檔，然後取代舊的內容檔。受管用戶端電腦通常都是從其管理伺服器接收內容更新。受管或非受管用戶端電腦均可以直接從 LiveUpdate 伺服器接收此內容。您的電腦收到更新的方式取決於您的電腦是受管電腦還是非受管電腦，以及管理員架構更新的方式。

Table 3: 更新電腦內容的方式

工作	說明
依排程更新內容	依預設，LiveUpdate 會在排程間隔自動執行。您也可以修改排程，以便 LiveUpdate 在排程間隔自動執行。您可以排程 LiveUpdate 在您未使用電腦的期間執行。 在受管用戶端上，您只能將 LiveUpdate 架構為依排程執行，或是修改已由管理員啟用的現有排程。如果顯示掛鎖圖示而且選項顯示為灰色，則表示您無法按排程更新內容或修改現有排程。在非受管用戶端上，您可以停用或變更 LiveUpdate 排程。 使用 LiveUpdate 依排程更新內容
立即更新內容	根據您的安全性設定，您可以立即執行 LiveUpdate。在下列情況下，您應手動執行 LiveUpdate： • 用戶端軟體是最近安裝的。 • 自上次掃描以來經過了一段長時間。 • 您懷疑有病毒或其他惡意軟體問題。 Note: 僅當管理員將設定架構為允許受管用戶端手動執行 LiveUpdate 時，受管用戶端才能這麼做。 使用 LiveUpdate 立即更新內容

若要使用 **LiveUpdate** 依排程更新內容：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「用戶端管理」旁邊，按下「架構設定」。
3. 在「用戶端管理設定」對話方塊中，按下 **LiveUpdate**。
4. 在 **LiveUpdate** 標籤上，勾選「啟用自動更新」。
5. 在「頻率和時間」群組方塊中，視需要修改更新的頻率。
6. 選擇性地啟用和架構隨機化選項和閒置偵測設定。
這些選項可改善 LiveUpdate 更新用戶端所需的時間量。
7. 按下「確定」。

若要使用 **LiveUpdate** 立即更新內容：

在用戶端的側邊看板中，按下 **LiveUpdate**。

LiveUpdate 會連線至賽門鐵克伺服器，並檢查可用的更新，然後自動下載和安裝這些更新。

警示和通知的類型

Windows 適用的 Symantec Endpoint Protection 用戶端指南

用戶端會在背景執行，防護您的電腦，使您安全無虞，不受惡意活動的威脅。有時候，用戶端必須通知您偵測到的活動，或者提示您提供回應。

Table 4: 警示和通知的類型

警示	說明
掃描結果對話方塊	如果掃描偵測到病毒或安全性風險，會顯示掃描結果或包含感染詳細資料的「Symantec Endpoint Protection 偵測結果」對話方塊。對話方塊也會顯示掃描處理風險時所採取的動作。除了檢視活動和關閉對話方塊，您一般不需要採取任何進一步的動作。然而，若有必要，您也可以採取進一步的行動。 如果仍在進行掃描，對話方塊可能會顯示一個名稱，例如，「已於日期時間開始的掃描名稱」。如果掃描完成，對話方塊可能會顯示「Symantec Endpoint Protection 偵測結果」之類的名稱。 關於掃描結果
其他訊息對話方塊	在下列情況，您會看見彈出式訊息： - 用戶端自動更新用戶端軟體。 回應訊息以更新用戶端軟體 - 用戶端詢問您要允許或攔截應用程式。 回應詢問您是允許還是攔截應用程式的訊息 - 用戶端的試用授權已過期。 回應過期的授權訊息
通知區圖示訊息	在下列情況，通知區圖示中會出現通知： - 用戶端攔截應用程式： Traffic has been blocked from this application: Application name 如果用戶端架構為攔截全部流量，則這些通知會頻繁出現，並且通常不要求您執行任何動作。如果您的用戶端被架構為允許全部流量，這些通知將不會出現。 回應詢問您是允許還是攔截應用程式的訊息 - 用戶端終止應用程式： Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected. Symantec Endpoint Protection 將終止 <應用程式名稱> 應用程式 防止攻擊易受攻擊的應用程式 - 用戶端偵測到危害電腦的網路攻擊： Traffic from IP address 192.168.0.3 is blocked from 2/14/2010 15:37:58 to 2/14/2010 15:47:58. Port Scan attack is logged. 除了讀取訊息外，您不需要執行其他動作。 - 安全性遵從檢查失敗。系統可能會攔截出入電腦的流量： ##### 矯正您的電腦以通過主機完整性檢查

[用戶端狀態圖示](#)

關於掃描結果

Windows 適用的 Symantec Endpoint Protection 用戶端指南

若是受管用戶端，您的管理員通常會架構每週至少執行一次完整掃描。若是非受管用戶端，當您開啟電腦時，就會執行自動產生的「作用中掃描」。「自動防護」預設會持續在您的電腦上執行。

掃描執行時，會出現掃描對話方塊，以報告進度並顯示掃描結果。掃描完成時，結果會顯示在清單中。若用戶端未偵測到任何病毒或安全風險，清單將維持空白，且狀態為「已完成」。

如果用戶端在掃描期間偵測到風險，掃描結果對話方塊會顯示含有下列資訊的結果：

- 病毒或安全風險的名稱
- 受感染檔案的名稱
- 用戶端對風險所執行的動作

如果用戶端偵測到病毒或安全風險，您可能需要對受感染的檔案採取動作。

NOTE

針對受管用戶端，管理員可能會選擇隱藏掃描結果對話方塊。如果用戶端未受管理，您可以顯示或隱藏此對話方塊。

如果您或管理員架構用戶端軟體顯示掃描結果對話方塊，則可以暫停、重新啟動或停止掃描。

回應病毒或風險偵測

Windows 適用的 Symantec Endpoint Protection 用戶端指南

管理員定義掃描、使用者定義掃描或「自動防護」執行時，您可能會看到掃描結果對話方塊。您可以利用掃描結果對話方塊，立即對受影響的檔案採取動作。例如，您可能會決定將已清除病毒的檔案刪除，因為您想要以原始檔案取代該檔案。

如果 需要終止程序或應用程式，或需要停止服務，「立即移除風險」選項便會啟用。對話方塊中的風險要求您採取動作時，您可能無法關閉對話方塊。

您可能需要對風險採取動作，但可以選擇稍後再執行動作。您可以稍後透過下列方式使用「隔離所」、「風險日誌」或「掃描日誌」對檔案執行動作：

- 您可以開啟「風險日誌」，在風險上按下滑鼠右鍵，然後執行動作。
- 您可以執行掃描來偵測風險，然後重新開啟結果對話方塊。

在對話方塊中的風險上按下滑鼠右鍵，再選取動作，也可以執行動作。您可以執行的動作取決於先前針對掃描偵測出的特定風險類型所架構的動作。

若要在掃描結果對話方塊中回應病毒或風險偵測：

1. 在掃描結果對話方塊中，選取要對其採取動作的檔案。
2. 用滑鼠右鍵按下選擇項目，再選取下列其中一個選項：

清理	移除檔案中的病毒。此選項僅適用於病毒。
排除	將檔案排除在再次掃描的範圍以外。
永久刪除	刪除受感染的檔案，並嘗試移除或修復感染所造成的任何副作用。對於安全風險，請審慎使用此動作。某些情況下，如果刪除安全風險，可能會造成應用程式無法運作。
復原採取的動作	復原採取的動作。
移到隔離所	將受到感染的檔案置入「隔離所」內。若是安全風險，用戶端也會嘗試移除或修復感染所造成的副作用。在某些情況下，如果用戶端隔離安全風險，可能會造成應用程式無法運作。
屬性	顯示有關病毒或安全風險的資訊。

在某些情況下，可能會無法使用動作。

3. 在對話方塊中，按下「關閉」。

如果列出的風險要求您執行動作，您可能無法關閉對話方塊。例如，用戶端可能需要終止程序或應用程式，也可能需要停止服務。

如果需要採取動作，會顯示下列其中一個通知：

- 需要移除風險
在風險需要終止程序時出現。如果您選擇移除風險，就會回到結果對話方塊。如果也需要重新啟動，對話方塊中的風險列會指出需要重新啟動。
- 需要重新啟動
在風險需要重新啟動時出現。
如果需要重新啟動，移除或修復會在您重新啟動電腦後才完成。
- 需要移除風險並重新啟動
在風險需要終止程序且另一個風險需要重新啟動時出現。

4. 如果「立即移除風險」對話方塊顯示，請按下下列選項之一：

- 立即移除風險 (建議)
用戶端移除風險。移除風險可能需要重新啟動。對話方塊中的資訊會指明是否需要重新啟動。
- 不要移除風險
該結果對話方塊會提醒您是否仍需採取動作。不過，在您重新啟動電腦後，「立即移除風險」對話方塊會顯示。

5. 如果結果對話方塊在步驟 3 中未關閉，請按下「關閉」。

回應詢問您要允許或攔截嘗試下載的檔案的下載鑑識訊息

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「下載鑑識」通知顯示的資訊是關於在您嘗試下載時偵測到的惡意檔案和未經證明的檔案。

NOTE

如果針對未證明檔案的動作為「提示」時，則無論您是否啟用通知，都將收到偵測訊息。

您或您的管理員可以變更「下載鑑識」對惡意檔案的敏感程度。變更靈敏度等級可能會變更您收到的通知數目。

「下載鑑識」使用賽門鐵克的智慧型掃描技術，該技術會根據數百萬使用者構成的全球社群評估檔案並決定檔案分級。

「下載智慧型掃描」通知會顯示以下與偵測到的檔案相關的資訊：

- 檔案信譽
檔案信譽表示檔案的信任度。惡意檔案不受信任。未證明的檔案可能受信任，也可能不受信任。
- 檔案在社群中的常用程度
檔案的普及率非常重要。不常使用的檔案較可能是威脅。
- 檔案新舊程度
檔案愈新，賽門鐵克掌握的檔案相關資訊愈少。

此資訊可協助您決定要允許還是攔截檔案。

若要回應要求您允許或攔截您嘗試下載之檔案的「下載鑑識」偵測：

在「下載智慧型掃描」偵測訊息中，執行下列動作之一：

- 按下「從電腦中移除此檔案」。
「下載鑑識」會將此檔案移至「隔離所」。只會針對未證明的檔案顯示此選項。
- 按下「允許此檔案」。
您可能會看到權限對話方塊，詢問您是否確定要允許使用此檔案。

如果您選擇允許使用未被隔離的未證明檔案，則此檔案會自動執行。如果您選擇允許使用隔離的檔案，則此檔案不會自動執行。您可以從 Internet 暫存資料夾執行此檔案。

通常，資料夾位置是：

- Windows 7：磁碟機:\Users\使用者名稱\AppData\Local\Microsoft\Windows\Temporary Internet Files
- Windows 8/8.1：磁碟機:\Users\使用者名稱\AppData\Local\Microsoft\Windows\INetCache

若為非受管用戶端，如果您允許使用某個檔案，用戶端會在此電腦上自動為此檔案建立例外。若為受管型用戶端，如果管理員可讓您建立例外，用戶端會在此電腦上自動為此檔案建立例外。

回應詢問您是允許還是攔截應用程式的訊息

Windows 適用的 Symantec Endpoint Protection 用戶端指南

當電腦上的應用程式嘗試存取網路時，用戶端可能會詢問您要允許或攔截應用程式。您可以選擇攔截您認為不安全的應用程式，防止其存取網路。

此類型的通知顯示原因有：

- 應用程式要求存取您的網路連線。
- 存取您網路連線的應用程式已升級。
- 您的管理員升級了用戶端軟體。

您可能會看見下列訊息，通知您有應用程式嘗試存取您的電腦：

```
IEEXPLORE.EXE is attempting to access the network.  
Do you want to allow this program to access the network?
```

回應要求您允許或攔截應用程式的訊息：

1. 另一個選擇是，如果希望下次應用程式嘗試存取網路時不顯示此訊息，請在對話方塊中按下「記住我的答案，請勿再針對這項應用程式詢問我」。
2. 執行下列其中一項動作：
 - 若要允許應用程式存取網路，請按下「是」。
 - 若要阻止應用程式存取網路，請按下「否」。

在非受管電腦和部分受管電腦上，您也可以透過「狀態」頁面變更對應用程式採取的動作。在「防網路和主機侵入」旁，按下「選項」，然後按下「檢視網路活動」，或按下「檢視應用程式設定」。

[允許或攔截已在用戶端上執行的應用程式](#)

回應過期的授權訊息

Windows 適用的 Symantec Endpoint Protection 用戶端指南

用戶端會使用授權來更新掃描的病毒定義檔以及更新用戶端軟體。用戶端可使用試用授權或已付費授權。如果試用授權已到期，用戶端就不會再更新任何內容。

Table 5: 授權類型

授權類型	說明
試用授權	如果試用授權過期，用戶端的「狀態」窗格最上方會變成紅色，並顯示下列訊息： Trial License has expired. Click Details for more information. 當您按下「詳細資料」時，會出現訊息，指出內容下載於特定日期終止，並要求聯絡您的管理員以購買付費授權。「狀態」窗格也可能會顯示一些指出內容已過期的文字。 您也可以透過用戶端介面檢視授權到期日。按下「說明 > 關於」。
已付費授權	如果已付費授權過期，您應該不會在用戶端的「狀態」窗格中看到任何與過期狀態相關的訊息。已付費授權到期日不會顯示在「說明 > 關於」下。 內容會持續更新，例如病毒和間諜軟體定義檔。

不論是哪種授權，您都必須聯絡管理員來更新或續購授權。

警示和通知的類型

檢視日誌

回應訊息以更新用戶端軟體

Windows 適用的 Symantec Endpoint Protection 用戶端指南

如果有用戶端軟體更新可供下載，您可能會看到下列通知：

```
has detected that  
a newer version of the software is available from  
the .  
Do you wish to download it now?
```

用戶端軟體更新也可能會在背景中以無訊息方式安裝。安裝完成時，可能會出現訊息，通知您必須重新啟動電腦。

回應更新通知：

- 執行下列其中一項動作：
 - 若要立刻下載軟體，請按下「立即下載」。
 - 若要在指定時間後被提醒，請按下「稍後提醒我」。
- 如果更新軟體的安裝程序開始後顯示一則訊息，請按下「確定」。
- 如果出現訊息通知您升級已完成，請按照螢幕上的指示重新啟動。當您重新啟動電腦後，安裝即完成。

管理電腦上的掃描

Windows 適用的 Symantec Endpoint Protection 用戶端指南

根據預設，用戶端會每天執行作用中掃描。在受管用戶端上，如果管理員允許使用這些設定，您就可以自行架構掃描。非受管用戶端包含停用的預設作用中掃描，不過您可以管理自己的掃描。

掃描會存取在雲端設定的完整定義檔。

[Windows 用戶端如何從雲端接收定義檔](#)

Table 6: 管理掃描

工作	說明
了解掃描的運作模式	檢視掃描類型以及病毒和安全性風險的類型。 病毒和間諜軟體掃描的運作方式
更新病毒定義檔	確定電腦安裝了最新的病毒定義檔。 使用 LiveUpdate 更新用戶端內容
檢查自動防護是否啟用	「自動防護」預設為啟用。「自動防護」應隨時保持在啟用狀態。如果停用「自動防護」，您還會停用「下載鑑識」並會阻止 SONAR 進行啟發式偵測 (14.3 RU4 或更早版本)。 啟用自動防護
掃描電腦	定期掃描電腦是否有病毒和安全性風險。檢查上次掃描日期，確定掃描定期執行。 立即掃描用戶端電腦 在用戶端上排程使用者定義的掃描 掃描執行時，您會看到掃描結果對話方塊。可以使用該掃描結果對話方塊，對掃描偵測到的項目執行一些動作。 回應病毒或風險偵測 您可以暫停您開始的掃描。在受管用戶端上，管理員可以決定您能否暫停由管理員啟動的掃描。 暫停和延緩掃描 在受管用戶端上，管理員可能會從管理主控台起始 Power Eraser 掃描。Power Eraser 是一種強大的掃描，可以偵測嚴重的威脅，並且有時需要重新啟動才能完成。管理員可手動處理用於偵測的矯正。 您無法直接從用戶端執行 Power Eraser，但是，Power Eraser 可做為 SymDiag 支援工具的一部分使用。如果直接在用戶端上下載 SymDiag 工具並執行 Power Eraser 掃描，則不會將日誌傳送到管理主控台。管理員從管理主控台執行 Power Eraser 時，您應該確認沒有使用 SymDiag 工具在本機執行 Power Eraser；否則，可能會對電腦效能產生不良影響。
調整掃描以提高電腦效能	依預設，Symantec Endpoint Protection 會在提供高安全性等級的同時，將對電腦效能的影響降至最低。您也可以自訂設定，以進一步提高電腦效能。 對於排程掃描和隨選掃描，可以變更下列選項： • 掃描調整 將掃描調整設定為「最佳應用程式效能」。 • 壓縮檔 變更掃描壓縮檔的層數。 • 可復原掃描 可以指定掃描執行的最大時間。掃描會在電腦閒置時復原。 • 隨機掃描 可以指定掃描在指定時間間隔內隨機設定開始時間。 此外，您可能還需要停用啟動掃描，或變更排程掃描的排程。 自訂病毒和間諜軟體掃描設定 在用戶端上排程使用者定義的掃描

工作	說明
調整掃描以增強電腦的防護	在大多數情況下，預設掃描設定即可為電腦提供足夠的保護。在某些情況下，您可能希望增強防護。如果增強防護，則可能會影響電腦效能。 對於排程掃描和隨選掃描，可以變更下列選項： - 掃描效能 將掃描調整設定為「最佳掃描效能」。 - 掃描動作 變更偵測到病毒時執行的矯正動作 - 掃描持續時間 根據預設，排程掃描將執行到指定時間間隔到期為止，然後在用戶端電腦閒置時復原執行。您可以將掃描持續時間設定為「到掃描完成」。 - 提高 Bloodhound 防護的層級。 Bloodhound 會找到並隔離檔案的邏輯區域以偵測類似病毒的行為。您可以將偵測層級從「自動」變更為「主動」來增強對電腦的防護。不過，「主動」設定可能會產生更多的誤報結果。 自訂病毒和間諜軟體掃描設定
調整掃描以減少誤報	將安全檔案或程序排除在掃描的範圍以外。 排除掃描項目
將有關偵測的資訊傳送至 Symantec	依據預設，用戶端電腦會將有關偵測的資訊傳送到賽門鐵克安全機制應變中心。您可以關閉傳送，或選擇要傳送哪些種類的資訊。 賽門鐵克建議您永遠啟用傳送功能。此資訊有助於賽門鐵克處理威脅。 瞭解向賽門鐵克提交資訊可改善電腦防護功能
管理隔離的檔案	Symantec Endpoint Protection 會隔離受感染的檔案，並將它們移動到不會感染電腦上其他檔案的位置。如果已隔離檔案無法修復，則用戶端最終會將其移除。您也可以對此檔案採取其他動作。 管理電腦上的隔離檔案

下表顯示可修改的其他掃描設定，以便能夠提高防護、改善效能或減少誤報情形。

Table 7: 掃描設定

工作	說明
修改「自動防護」設定以提高電腦效能或增強防護	對於「自動防護」，您可能需要變更下列選項： - 檔案快取 請確保檔案快取處於啟用狀態（預設為啟用）。啟用檔案快取時，「自動防護」會記住其掃描的未感染檔案，不會重新掃描。 - 網路設定 如果啟用遠端電腦上的「自動防護」，請務必啟用「只在執行檔案時」。 - 此外，也可以指定「自動防護」信任遠端電腦上的檔案，並使用網路快取。 「自動防護」預設會在檔案從您的電腦寫入遠端電腦時，對其進行掃描。「自動防護」也會在檔案從遠端電腦寫入您的電腦時，對其進行掃描。 網路快取會儲存「自動防護」掃描來自遠端電腦的檔案記錄。如果使用網路快取，「自動防護」就不會重複掃描相同的檔案。 自訂病毒和間諜軟體掃描設定
管理下載鑑識偵測	「下載智慧型掃描」會檢查您嘗試透過網頁瀏覽器、文字訊息用戶端以及其他入口網站下載的檔案。「下載鑑識」會使用收集檔案信譽相關資訊的「賽門鐵克智慧型掃描」所提供的資訊。「下載智慧型掃描」會使用檔案的信譽等級來允許或攔截檔案，或提示使用者對檔案採取動作。 管理電腦上的下載鑑識偵測
管理行為分析 (SONAR)	您可以調整行為分析的設定。 管理行為分析 (SONAR)

立即掃描用戶端電腦

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以隨時手動掃描病毒和安全風險。如果最近安裝了用戶端或收到病毒或安全風險，應該立即掃描電腦。

可以選取從單一檔案、USB 磁碟機，甚至整個電腦進行掃描。隨選掃描包括「作用中掃描」與「完整掃描」。您也可以建立隨選執行的自訂掃描。

您可以透過下列其中一種方式立即掃描電腦：

- 從「掃描威脅」頁面立即掃描 Windows 電腦
- 從「狀態」頁面立即掃描 Windows 電腦
- 從 Windows 立即掃描電腦

若要從「掃描威脅」頁面立即掃描 **Windows** 電腦：

1. 在用戶端的側邊列中，按下「掃描威脅」。
隨即會開始掃描。
除非您的管理員停用掃描進度選項，否則您可以檢視掃描進度。若要檢視掃描進度，請按下目前掃描顯示的訊息連結：「掃描 進行中」。
如需各對話方塊上選項的詳細資訊，請按下「說明」。
您也可以暫停或取消掃描。
 - 按下「執行作用中掃描」以掃描最常感染的區域。
 - 按下「執行完整掃描」以掃描整個電腦。
 - 按一下「執行主機完整性掃描」以檢查是否遵從安全性政策。

NOTE

「執行主機完整性掃描」僅在用戶端已啟用主機完整性政策的情況下顯示。

- 在掃描清單中，在任何掃描上按下滑鼠右鍵，然後按下「立即掃描」。

若要從「狀態」頁面立即掃描 **Windows** 電腦：

1. 在用戶端「狀態」頁面的「病毒和間諜軟體防護」旁，按下「選項 > 執行作用中掃描」。

若要從 **Windows** 立即掃描電腦：

1. 在「我的電腦」或「Windows 檔案總管」視窗中，在需要掃描的檔案、資料夾或磁碟機按下滑鼠右鍵，然後按下「掃描病毒」。

32 位元和 64 位元作業系統支援此功能。

[關於掃描結果](#)

[暫停和延緩掃描](#)

[排程執行隨選或開機掃描](#)

[使用 LiveUpdate 更新用戶端內容](#)

暫停和延緩掃描

Windows 適用的 Symantec Endpoint Protection 用戶端指南

暫停功能可讓您在掃描期間隨時停止掃描，並在稍後繼續進行掃描。您可以暫停您起始的任何掃描。

網路管理員可以決定，您是否可以暫停管理員啟動的掃描。如果無法使用「暫停掃描」選項，表示管理員已停用暫停功能。如果您的管理員已啟用「延緩」功能，則您可以將管理員排定的掃描延後一段設好的間隔時間後執行。

掃描繼續時，會從掃描停止處開始。

NOTE

如果您在用戶端掃描壓縮檔時暫停掃描，用戶端可能要幾分鐘才能回應暫停要求。

管理電腦上的掃描

若要暫停您所啟動的掃描：

1. 掃描執行時，請在掃描對話方塊中，按下「暫停掃描」。
掃描會停在目前的階段，而且掃描對話方塊會一直保持開啟，直到重新啟動掃描為止。
2. 在掃描對話方塊中按下「繼續掃描」，繼續進行掃描。

若要暫停或延緩管理員啟動的掃描：

1. 管理員啟動的掃描執行時，請在掃描對話方塊中按下「暫停掃描」。
2. 在「排程掃描暫停」對話方塊中，進行下列任一動作：
 - 若要暫停掃描，請按下「暫停」。
 - 若要延緩掃描，請按下「延緩 1 小時」或「延緩 3 小時」。
您的管理員會指定您可以延緩掃描的時間長度。暫停的時間到達限制時，便會從頭開始重新掃描。您的管理員會指定在停用此功能之前，您可以延緩排程掃描的次數。
 - 若要繼續掃描不暫停，請按下「繼續」。

在用戶端上排程使用者定義的掃描

Windows 適用的 Symantec Endpoint Protection 用戶端指南

用戶端上的排程掃描是威脅與安全風險防護的一項重要組成部分。您應該排程至少每週掃描一次，才能確保電腦不受病毒和安全風險威脅。建立新掃描時，掃描會出現在「掃描威脅」窗格的掃描清單中。

NOTE

如果管理員已建立排程掃描，該掃描就會出現在「掃描威脅」窗格的掃描清單中。

電腦必須開啟，而且必須載入「Symantec Endpoint Protection 服務」，才能進行排程掃描。「Symantec Endpoint Protection 服務」預設會在開啟電腦時載入。

對於管理型用戶端，管理員可能會覆寫這些設定。

立即掃描用戶端電腦

管理電腦上的掃描

設定排程掃描時，請注意下列重點：

使用者定義的掃描不會要求使用者登入	如果定義掃描的使用者未登入，仍然會執行掃描。您可以指定用戶端在使用者登出後不執行掃描。
多個同時掃描會接續執行	如果您在同一台電腦上排程執行多重掃描，且掃描的開始時間都相同，則掃描會接續執行。一個掃描作業完成後，再開始另一個。例如，您可能在電腦上排定三種不同的掃描於下午 1:00 執行。每次掃描都會掃描不同的磁碟機。一個掃描掃描磁碟機 C，另一個掃描磁碟機 D，第三個掃描磁碟機 E。在這個範例中，較好的解決方式是，建立一個排程掃描，來掃描磁碟機 C、D 和 E。
錯過的排程掃描可能不會執行	如果您的電腦由於某種原因錯過排程掃描，預設會嘗試執行掃描，直到啟動為止，或直到指定時間間隔到期為止。如果無法在重試間隔內啟動錯過的掃描，就不會再執行該掃描。

排程掃描時間可能偏離	如果最後一次執行的掃描由於掃描持續時間或錯過排程掃描設定而發生在不同的時間，可能不會使用排程的時間。例如，您可以將每週掃描架構為在每星期日午夜執行且重試間隔為一天。如果電腦錯過此掃描並於星期一早上 6 點啟動，則會在早上 6 點執行掃描。下一次掃描會在從星期一早上 6 點算起的一週後執行，而非在下一個星期日的午夜執行。 如果您並未在星期二早上 6 點 (晚了兩天，且超過重試間隔) 之前重新啟動電腦，就不會重試掃描。它會等到下一個星期日的午夜再嘗試執行掃描。 不論是何種情況，如果您隨機設定掃描開始時間，您可能會變更掃描的最後一次執行時間。
------------	--

您也可以建立隨選掃描或開機掃描。

排程執行隨選或開機掃描

若要排程使用者定義掃描：

1. 在用戶端的側邊列中，按下「掃描威脅」。
2. 按下「建立新掃描」。
3. 在「建立新掃描 - 掃描的項目」對話方塊中，選取下列其中一種掃描進行排程：

作用中掃描	掃描電腦中最常受病毒和安全風險感染的區域。 您應該每天執行一次作用中掃描。
完整掃描	掃描整部電腦是否有病毒和安全風險。 您可能需要一週或一個月執行一次完整掃描。完整掃描可能會影響電腦效能。
自訂掃描	掃描電腦上所選取區域是否有病毒和安全風險。

4. 按「下一步」。
5. 如果選取「自訂掃描」，請勾選適當的核取方塊，指定要掃描的位置，然後按「下一步」。

符號的敘述如下：

☐	未選取檔案、磁碟機或資料夾。如果該項目是磁碟機或資料夾，其中的資料夾或檔案亦未被選取。
☒	已選取個別檔案或資料夾。
☒	已選取個別資料夾或磁碟機。亦會選取該資料夾或磁碟機內的所有項目。
☐	未選取個別資料夾或磁碟機，但已選取資料夾或磁碟機內的一個或多個項目。

6. 在「建立新掃描 - 掃描選項」對話方塊中，您可以修改下列任一選項：

檔案類型	變更用戶端要掃描的檔案副檔名。預設設定為掃描所有檔案。
動作	變更發現病毒及安全風險時應採取的第一個和第二個動作。
通知	編寫發現病毒或安全風險時要顯示的訊息。您也可以架構進行矯正動作前要不要收到通知。
進階	變更其他掃描功能，例如顯示掃描結果對話方塊。
掃描增強功能	變用戶端會掃描的電腦元件。這些選項可用與否，視您在步驟 3 所選取的而定。

-
7. 按「下一步」。
 8. 在「建立新掃描 - 掃描的時間」對話方塊按下「在指定時間」，然後按下「下一步」。
 9. 在「建立新掃描 - 排程」對話方塊的「掃描排程」下方，指定掃描頻率和掃描時間，然後按「下一步」。
 10. 在「掃描持續時間」下，您可以指定必須完成掃描的時間長度。您也可以隨機設定掃描開始時間。
 11. 在「錯過掃描排程」下方，可以指定可重試掃描的間隔。
 12. 在「建立新掃描 - 掃描名稱」對話方塊中，輸入掃描的名稱和說明。
例如，將掃描作業稱為：星期五早上
 13. 按下「完成」。

排程執行隨選或開機掃描

除排程掃描之外，您可以在開機或登入電腦時額外進行自動掃描。通常開機掃描只著重在重要、高風險的資料夾，例如 Windows 資料夾和儲存 Microsoft Word 與 Excel 範本的資料夾。

如果要定期掃描同一組檔案或資料夾，您可以針對這些項目建立隨選掃描。不論何時，您都可以快速確認指定的檔案與資料夾並未受到病毒及安全風險感染。隨選掃描必須以手動方式執行。

如果您建立的開機掃描不只一個，則掃描動作會按照您當初建立的順序依次執行。管理員可能已架構用戶端，因此您無法建立開機掃描。

立即掃描用戶端電腦

若要排程執行隨選或開機掃描：

1. 在用戶端的側邊列中，按下「掃描威脅」。
2. 按下「建立新掃描」。
3. 指定排程掃描的掃描內容和任何掃描選項。

在用戶端上排程使用者定義的掃描

4. 在「建立新掃描 - 掃描的時間」對話方塊中，進行下列其中一個動作：
 - 按下「啟動時」。
 - 按下「隨選」。
5. 按「下一步」。
6. 在「建立新掃描 - 掃描名稱」對話方塊中，輸入掃描的名稱和說明。

例如，將掃描作業稱為：MyScan1

7. 按下「完成」。

管理電腦上的下載鑑識偵測

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「自動防護」包含「下載鑑識」，該功能可檢查您試圖透過網頁瀏覽器、文字訊息用戶端以及其他入口網站下載的檔案。必須先啟用「自動防護」，「下載鑑識」才能運作。

支援的入口網站包含 Internet Explorer、Firefox、Microsoft Outlook、Outlook Express、Windows Live Messenger 和 Yahoo Messenger。

NOTE

在「風險日誌」中，「下載鑑識」偵測的風險詳細資料只顯示嘗試下載的第一個入口網站應用程式。例如，您可以使用 Internet Explorer 嘗試下載「下載智慧型掃描」偵測的檔案。如果您接著使用 Firefox 嘗試下載該檔案，則風險詳細資料中的「下載者」欄位會將 Internet Explorer 顯示為入口網站。

NOTE

「自動防護」還可以掃描使用者以電子郵件附件接收的檔案。

Table 8: 管理電腦上的下載鑑識偵測

工作	說明
了解「下載鑑識」如何使用信譽資料做出關於檔案的決策	「下載鑑識」根據有關檔案信譽的相關證據，決定下載的檔案是否存在風險。「下載鑑識」只會使用信譽資訊進行有關下載檔案的決策。它不會使用特徵或啟發式技術進行決策。如果「下載鑑識」允許檔案，則「自動防護」或行為分析 (SONAR) 將在使用者開啟或執行該檔案時掃描該檔案。 Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策
確定已啟用智慧型掃描查詢	「下載鑑識」需要使用信譽資料進行檔案相關決策。如果停用智慧型掃描查詢，則「下載鑑識」可以執行，但無法進行偵測。依預設，「智慧型掃描查詢」已啟用。 瞭解向賽門鐵克提交資訊可改善電腦防護功能
回應下載鑑識偵測	當「下載鑑識」執行偵測時，您可能會看到相關通知。對於受管用戶端，您的管理員可以選擇停用「下載鑑識」偵測通知。 啟用通知後，系統將在「下載鑑識」偵測到惡意檔案或未證明的檔案時顯示相關訊息。對於未證明的檔案，您必須選擇是否允許該檔案。 回應詢問您要允許或攔截嘗試下載的檔案的下載鑑識訊息
為特定檔案或 Web 網域建立例外	您可以為下載的應用程式建立例外。您也可以為您認為受信任的特定 Web 網域建立例外。 依預設，「下載智慧型掃描」不會檢查使用者從信任的 Internet 或內部網路網站下載的任何檔案。信任的網站在「Windows 控制台 > 信任的 Internet 網站 > 安全性」標籤上架構。啟用「自動信任從內部網路網站下載的任何檔案」選項後，用戶端將允許使用者從信任的網站下載的任何檔案。 「下載鑑識」只會辨識您或管理員明確架構的受信任網站。 排除掃描項目
自訂下載鑑識設定	您可能因以下原因需要自訂「下載鑑識」設定： • 增加或減少「下載鑑識」偵測的數目。 您可以調整惡意檔案靈敏度滑動軸，以增加或減少偵測數目。靈敏度等級愈低，「下載鑑識」偵測到的惡意檔案愈少，偵測到的未證明的檔案愈多。誤報偵測也愈少。 靈敏度等級愈高，「下載智慧型掃描」偵測到的惡意檔案愈多，偵測到的未證明的檔案愈少。誤報偵測也愈多。 • 變更偵測到惡意檔案或未證明的檔案時採取的動作。 您可以變更「下載鑑識」處理惡意檔案或未證明檔案的方式。您可能會想變更對未證明的檔案採取的動作，以避免收到相關偵測通知。 • 取得有關「下載智慧型掃描」偵測的警示。 如果「下載鑑識」偵測到其視為惡意的檔案，在相應動作設為「隔離」的情況下，它會在用戶端電腦上顯示訊息。您可以復原隔離動作。 如果「下載鑑識」偵測到其視為未證明的檔案，它會在用戶端電腦上顯示訊息。只有在您將未證明檔案的動作設為「提示」或「隔離」的情況下，此訊息才會出現。如果將動作設為「提示」，則可以允許或攔截此檔案。如果將動作設為「隔離」，則可以復原隔離動作。 您可以關閉使用者通知，如此您不用在「下載鑑識」偵測到視為未證明的檔案時進行選擇。如果您保持啟用通知，可將未證明檔案的動作設為「忽略」，以一律允許這些偵測，且不會通知您。 當啟用通知時，惡意檔案靈敏度的設定會影響您收到的通知數量。如果您提高靈敏度，則會增加使用者通知的數目，因為偵測的總數會增加。 自訂下載鑑識設定

工作	說明
控制要將哪些信譽偵測相關資訊傳送給賽門鐵克	根據預設，所有受管用戶端都會將有關信譽偵測的資訊傳送給賽門鐵克。 賽門鐵克建議您持續為信譽偵測啟用傳送功能。此資訊有助於賽門鐵克處理威脅。 瞭解向賽門鐵克提交資訊可改善電腦防護功能

自訂下載鑑識設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可能需要自訂「下載智慧型掃描」設定，以降低用戶端電腦上的偵測誤報率。您可以變更「下載智慧型掃描」對於描述惡意檔案特徵的檔案信譽資料的敏感程度。您也可以變更「下載智慧型掃描」進行偵測時顯示在用戶端電腦上的通知。

NOTE

必須先啟用「自動防護」，「下載智慧型掃描」才能運作。如果停用「自動防護」，則即使「下載智慧型掃描」已啟用，「下載智慧型掃描」也無法運作。

若要自訂下載鑑識設定：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「病毒和間諜軟體防護」旁，按下「架構設定」。
3. 在「下載鑑識」標籤上，確定勾選「啟用下載鑑識以根據檔案信譽偵測下載檔案中的潛在風險」。
如果停用「自動防護」，則即使「下載智慧型掃描」已啟用，也無法運作。
4. 移動滑動軸以變更惡意檔案靈敏度。

NOTE

如果僅安裝了基本病毒和間諜軟體防護，則惡意檔案靈敏度將自動設定為等級 1，並且無法變更設定。

如果設定為更高等級，則「下載智慧型掃描」會將較多的檔案偵測為惡意檔案，並將較少的檔案偵測為未證明的檔案。不過，設定等級愈高，傳回的誤報就越多。

5. 您可以勾選或取消勾選下列選項，用做檢查未證明檔案的附加條件：
 - 使用者數量不超過 **x** 個的檔案，其中 **x** 預設為 5。您可以從下拉式清單中選取其他值。
 - 使用者已知不超過 **x** 天的檔案，其中 **x** 預設為 2。您可以輸入任何值
如果未證明的檔案符合此條件，下載鑑識會將這些檔案偵測為惡意檔案。
6. 確定已勾選「自動信任從內部網路網站下載的任何檔案」。
7. 按下「動作」。
8. 在「惡意檔案」下方，指定第一個動作和第二個動作。
9. 在「未證明的檔案」下方，指定動作。
10. 按下「確定」。
11. 按下「通知」，然後指定是否應在「下載智慧型掃描」執行偵測時顯示通知。
您可以自訂顯示的警告訊息文字。
12. 按下「確定」。

自訂病毒和間諜軟體掃描設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

預設會提供電腦所需的病毒和安全風險防護。如果使用非受管用戶端，您可能需要架構某些掃描設定。

您可以自訂使用者定義的掃描、全域掃描設定，以及自動防護。

- [執行使用者定義的掃描](#)
- [變更全域掃描設定](#)
- [自訂自動防護](#)

若要執行使用者定義的掃描：

1. 在用戶端的側邊列中，按下「掃描威脅」。
2. 在「掃描威脅」頁面中，用滑鼠右鍵按下掃描，然後按「編輯」。
3. 在「掃描選項」標籤上，執行下列任一工作：
 - 若要指定減少掃描的檔案類型，請按下「選取的副檔名」，然後按下「副檔名」。

NOTE

使用者定義的掃描一律會掃描配置區檔案，除非您在「進階掃描選項」下方為排程掃描停用壓縮檔案選項，或為配置區副檔名建立例外。

- 若要指定用戶端對受感染的檔案採取的第一個動作和第二個動作，請按下「動作」。
- 若要指定通知選項，請按下「通知」。
- 若要架構壓縮檔案、備份和調整的進階選項，請按下「進階」。

您可以變更調整選項，以提高用戶端電腦的效能。

如需各對話方塊上選項的詳細資訊，請按下「說明」。

4. 按下「確定」。

若要變更全域掃描設定：

1. 在用戶端的側邊看板中，按下「變更設定」，然後按下「病毒和間諜軟體防護」旁的「架構設定」。
2. 在「全域設定」標籤上，在「掃描選項」下方變更智慧型掃描或 Bloodhound 啟發式病毒偵測的設定。
3. 若要檢視或建立掃描例外，請按下「檢視清單」。檢視或建立例外後，按下「關閉」。
4. 在「日誌保留」或「網際網路瀏覽器防護」下方，進列所需的所有變更。
5. 按下「確定」。

若要自訂自動防護：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「病毒和間諜軟體防護」旁，按下「架構設定」。
3. 在任何「自動防護」標籤上，執行下列工作：
 - 若要指定減少掃描的檔案類型，請按下「選取的」，再按下「副檔名」。
 - 若要指定用戶端對受感染的檔案採取的第一個動作和第二個動作，請按下「動作」。
 - 若要指定通知選項，請按下「通知」。

如需各對話方塊上選項的詳細資訊，請按下「說明」。

4. 在「自動防護」標籤上，按下「進階」。

您可以變更檔案快取的選項以及「風險追蹤程式」和備份的選項。您可能需要變更這些選項以提高電腦效能。

5. 按下「網路」以變更在遠端電腦上信任檔案的設定和設定網路快取的設定。
6. 按下「確定」。

架構在偵測到惡意軟體與安全風險時採取的動作

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構您希望 用戶端在偵測到惡意軟體或安全風險時採取的動作。您可以架構兩個動作，如果第一個動作失敗，就執行第二個動作。

NOTE

若您的電腦由管理員所管理，且這些選項顯示一個鎖定圖示，您就無法變更這些選項，因為已被您的管理員鎖定。

對任何類型的掃描，架構動作的方式都相同。每種掃描都有其自己的動作架構。您可以針對不同的掃描，架構不同的動作。

NOTE

您可以單獨針對「下載智慧型掃描」與行為分析 (SONAR) 架構動作。

[自訂病毒和間諜軟體掃描設定](#)

[自訂下載鑑識設定](#)

[防止對行為分析 \(SONAR\) 的誤報偵測](#)

架構在偵測到惡意軟體與安全風險時採取的動作：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 按下「病毒和間諜軟體防護」旁邊的「架構設定」，然後在任何「自動防護」標籤上，按下「動作」。
3. 按下「動作」。
4. 在「掃描動作」對話方塊中，選取「惡意軟體」或「安全風險」類別。

您還可以選取子類別。依據預設，每個子類別都會自動架構為使用為整個類別所設定的動作。

類別會隨著賽門鐵克取得有關風險的新資訊而隨時動態變更。

5. 若要僅針對子類別架構動作，請執行下列其中一項動作：
 - 勾選「覆寫針對惡意軟體架構的動作」，然後僅針對該子類別設定動作。

NOTE

一個類別下方可能有單一子類別，視賽門鐵克目前對風險進行分類的方式而定。例如，在「惡意軟體」下方，可能有稱為「病毒」的單一子類別。

- 勾選「覆寫針對安全風險架構的動作」，然後僅針對該子類別設定動作。
6. 針對類別或子類別，選取下列選項中的第一個和第二個動作：

清除風險	移除受感染檔案中的病毒。此設定是對「惡意軟體」類別執行的第一個預設動作。 Note: 此設定僅適用於作為「惡意軟體」類別的第一個動作。此動作不會套用到安全風險。 對病毒執行的第一個動作應一律使用此設定。如果用戶端成功清除檔案中的病毒，您就不需要採取任何其他動作。您的電腦將免於偵測到病毒的困擾，而且病毒不再容易散播到電腦的其他區域。 然而，在某些情況下，清除病毒後的檔案可能會無法使用。因為病毒可能已造成過多的損害。某些受感染的檔案無法清除。 Note: 不會清除 Windows 8 樣式應用程式和檔案中所偵測到的惡意軟體。會改為刪除此偵測到的項目。
隔離風險	將受感染的檔案從其原始位置移到「隔離所」。放到「隔離所」後的受感染檔案無法散佈病毒。 • 若是惡意軟體，此動作會將受感染的檔案從其原始位置移到「隔離所」。此設定是對惡意軟體執行的第二個預設動作。 • 若是安全風險，此動作會將受感染的檔案從其原始位置移到「隔離所」，並嘗試移除或修復任何副作用。此設定是對安全風險執行的第一個預設動作。 「隔離所」包含所有已執行動作的記錄。您可以使電腦回到用戶端移除風險之前的狀態。 Note: 不會隔離 Windows 8 樣式應用程式和檔案中所偵測到的惡意軟體。會改為刪除此偵測到的項目。

刪除風險	從電腦硬碟上刪除受感染的檔案。如果用戶端無法刪除檔案，「通知」對話方塊會顯示已採取之動作的相關資訊。此項資訊也會顯示在事件日誌中。 此設定是對安全風險執行的第二個預設動作。 只有在您有未受病毒或安全風險感染的備份複本可以取代此檔案時，才能使用此動作。用戶端會永久刪除風險。受感染的檔案無法從資源回收筒復原。 Note: 當您架構對安全風險執行的動作時，請審慎使用此動作。某些情況下，刪除安全風險可能造成應用程式喪失功能。
略過 (只記錄)	維持檔案不變，並在風險記錄中置入項目，以記錄該風險。使用此選項來手動控制用戶端處理惡意軟體或安全風險的方法。 Note: 惡意軟體可能會擴散到電腦的其他部分或網路上的其他電腦，直到您採取進一步的動作。 當您執行大規模的自動掃描 (如排程掃描) 時，請勿選取此動作。若要檢視掃描結果，之後再採取其他動作，則可能需要使用此動作。其他動作可能是將檔案移到「隔離所」。 您的管理員可能會送出自訂訊息，說明應該如何回應。

- 針對您想要設定特定動作的每個類別，重複上述步驟，然後按下「確定」。
- 如果您選取安全風險類別，則可以針對該安全風險類別的一個或多個特定實例選取自訂動作。您可以排除掃描某個安全風險。例如，您可能想要排除某個廣告軟體，因為您工作時會用到它。
- 按下「確定」。

關於排除掃描項目

Windows 適用的 Symantec Endpoint Protection 用戶端指南

例外是您要從掃描中排除的檔案和其他項目。如果您已掃描電腦，知道有些檔案安全無虞，即可加以排除。在某些情況下，例外可減少掃描時間並提升系統效能。通常您不必建立例外。

對於受管用戶端，您的管理員可能已經建立掃描例外。如果建立的例外與管理員定義的例外發生衝突，會優先採用管理員定義的例外。管理員還可以防止您架構任何或所有類型的例外。

Table 9: 例外類型

例外類型	說明
檔案	適用於排程掃描和手動掃描、自動防護、行為分析 (SONAR) 和應用程式控制。掃描會忽略您選取的檔案。
資料夾	適用於排程掃描和手動掃描、自動防護、行為分析和應用程式控制。掃描會忽略您選取的資料夾。
已知風險	適用於排程掃描和手動掃描、自動防護和行為分析。掃描會忽略您選取的所有已知風險。
副檔名	適用於排程掃描和手動掃描以及自動防護。掃描會忽略帶有指定副檔名的全部檔案。
Web 網域	適用於下載鑑識。 「下載智慧型掃描」會忽略指定的信任 Web 網域。
應用程式	適用於排程掃描和手動掃描、自動防護、行為分析和下載鑑識。掃描會忽略、記錄、隔離或終止您在此指定的應用程式。
DNS 或主機檔案變更	適用於行為分析 (SONAR)。 當特定應用程式嘗試變更 DNS 設定或變更主機檔案時，掃描會忽略、記錄或攔截應用程式，並且提示使用者。

NOTE

如果電子郵件應用程式將所有電子郵件儲存在單一檔案中，則您應該建立檔案例外，才不會掃描收件匣檔案。依預設，掃描會隔離病毒。如果掃描在收件匣檔案中偵測到病毒，掃描將隔離整個收件匣。如果掃描隔離收件匣，您就無法存取電子郵件。

排除掃描項目

排除掃描項目

您可以將已知為安全的應用程式和檔案項目排除在掃描範圍之外。您也可以排除某些項目以改善電腦的效能。

對於受管用戶端，您的管理員可能已經建立掃描例外。如果建立的例外與管理員定義的例外發生衝突，會優先採用管理員定義的例外。

您可以將項目排除在安全風險掃描之外、將資料夾排除在行為分析 (SONAR) 掃描之外，以及將應用程式排除在所有掃描之外。

NOTE

在 Windows Server 2008 的 Server Core 安裝上，對話方塊的外觀可能會與這些步驟中說明的對話方塊不同。

若要從安全風險掃描中排除項目：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「例外」旁，按下「架構設定」。
3. 在「例外」對話方塊的「使用者定義例外」下方，按下「新增 > 安全風險例外」。
4. 選取下列任一例外類型：
 - 已知風險
 - 檔案
 - 資料夾
 - 副檔名
 - Web 網域
5. 執行下列其中一項動作：
 - 對於已知風險，勾選您要從掃描中排除的安全風險。
若要記錄偵測到或忽略安全風險時的事件，請勾選「偵測到安全風險時記錄」。
 - 對於檔案或資料夾，選取您要排除的檔案或資料夾，或輸入檔案或資料夾名稱。
選取掃描類型（「全部掃描」、「自動防護」或「排程和隨選」），然後按下「確定」。
如果您執行的應用程式將許多暫存檔案寫入資料夾，則可能需要從自動防護中排除該資料夾。自動防護會在檔案寫入時加以掃描，因此您可以透過將例外限制為排程和隨選掃描來提升電腦效能。
您可能需要從排程和隨選掃描中排除不常使用的資料夾或是包含封存檔案或封裝檔案的資料夾。例如，排程或隨選掃描不常使用的深度封存檔案可能會降低電腦效能。只有在存取任何檔案或寫入任何檔案到資料夾時，自動防護才會透過掃描來保護資料夾。
 - 對於副檔名，輸入您要排除的副檔名。
文字方塊中只能輸入一個副檔名。若輸入多個副檔名，用戶端會將該輸入項目視為一個副檔名。
 - 對於網域，輸入您要從下載智慧型掃描和 SONAR 偵測中排除的網域名稱或 IP 位址。您可以指定 URL，但是例外狀況僅使用 URL 的網域名稱部分。如果指定了 URL，則您可以使用 HTTP 或 HTTPS (不區分大小寫) 預先擱置 URL，但是例外狀況適用於兩者，即 HTTP 和 HTTPS。此例外允許您從網域中的任何位置下載檔案。
針對「下載鑑識」，允許使用萬用字元，但不支援無法路由的 IP 位址範圍。例如，「下載鑑識」無法將 10.*.* 識別為信任網站。此外，「下載鑑識」不支援「網際網路選項」>「安全性」>「自動偵測內部網路」選項所搜尋到的網站。
6. 按下「確定」。

若要從行為分析 (SONAR) 中排除資料夾：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「例外」旁，按下「架構設定」。
3. 在「例外」對話方塊的「使用者定義例外」下方，按下「新增 > SONAR 例外 > 資料夾」。
4. 選取您要排除的資料夾，勾選或取消勾選「包括子資料夾」，然後按下「確定」。
5. 按下「關閉」。

若要排除會變更 DNS 或主機檔案的應用程式：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「例外」旁，按下「架構設定」。
3. 在「例外」對話方塊的「使用者定義例外」下方，按下「DNS 或主機檔案變更例外」>「應用程式」。
4. 選取您要排除的應用程式，然後按下「確定」。

若要變更所有掃描處理應用程式的方式：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「例外」旁，按下「架構設定」。
3. 在「例外」對話方塊的「使用者定義例外」下方，按下「新增 > 應用程式例外」。
4. 選取應用程式的檔名。
5. 在「動作」下拉式方塊中，選取「忽略」、「只記錄」、「隔離」、「終止」或「移除」。
6. 按下「確定」。
7. 按下「關閉」。

管理電腦上的隔離檔案

Windows 適用的 Symantec Endpoint Protection 用戶端指南

關於隔離的檔案

依預設，會嘗試在偵測到受感染的檔案時清除檔案中的病毒。如果無法清除此檔案，則掃描作業會將此檔案放置在電腦上的隔離所中。當用戶端將受感染的檔案移到隔離所時，它會加密該檔案。由於檔案已加密，因此您無法存取隔離的檔案。隔離所中的檔案無法感染電腦或網路中其他電腦上的檔案。但是，隔離動作不會清除風險。風險會停留在電腦上，直到用戶端清除風險或刪除檔案為止。

以新的病毒定義檔更新電腦之後，用戶端會自動重新掃描隔離所。最新的定義可能會清除或修復先前隔離的檔案。

- 大多數病毒都可以隔離。開機病毒存在於電腦的開機磁區或分割表中，因此這些項目無法移至隔離所。有時候，用戶端會偵測到不明病毒，無法以目前的病毒定義檔集加以排除。
- 對於安全風險，掃描作業會將受感染的檔案移至隔離所，並修復安全風險的任何副作用。
- 「下載智慧型掃描」和行為分析 (SONAR) 也可以隔離檔案。

掃描如何回應偵測到的病毒或風險

管理隔離所中的檔案

由於隔離所會處理您電腦上受感染的檔案，您可以將這些檔案保留在隔離所中。但是，有一些動作您可能需要對隔離所中的檔案執行。例如，如果檔案錯誤遭到隔離，可以從隔離所還原該檔案。或者，如果您需要節省電腦空間，可以減少隔離所自動刪除其內容前的時間。

若要管理隔離所中的檔案：

1. 在用戶端的側邊列中，按下「檢視隔離所」。
2. 在「檢視隔離所」視窗中，選取隔離項目清單中的檔案。
3. 按下以下其中一個選項，並按照畫面上的指示操作。

[檢視隔離所](#)

[管理電腦上的掃描](#)

啟用自動防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

對於檔案和程序、Internet 電子郵件和電子郵件群組軟體應用程式，您應該使自動防護保持啟用狀態。有任何類型的「自動防護」停用時，病毒和間諜軟體狀態在「狀態」頁面上會以紅色出現。

若為受管用戶端，管理員可能會鎖定「自動防護」，因此您無法自行停用。另外，管理員也可能會指定您可以暫時停用「自動防護」，但指定的時間一過，「自動防護」就會自動再次開啟。

NOTE

如果您停用「自動防護」，則會同時停用「下載智慧型掃描」，即使「下載智慧型掃描」已啟用也是如此。在 14.3 或更早版本中，行為分析 (SONAR) 也無法偵測啟發式威脅；不過，行為分析會繼續偵測主機檔案及系統變更。

WARNING

賽門鐵克建議，如果需要排除用戶端電腦上的「自動防護」問題，請暫時停用這個功能。

若要針對檔案系統啟用自動防護：

1. 在用戶端的「狀態」頁面上，「病毒和間諜軟體防護」旁進行下列任一動作：
 - 按下「選項 > 啟用病毒和間諜軟體防護」。
 - 按下「選項 > 停用所有病毒和間諜軟體防護功能」。

若要針對電子郵件啟用自動防護：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「病毒和間諜軟體防護」旁，按下「架構設定」。
3. 執行下列其中一項動作：
 - 在「**Outlook** 自動防護」標籤上，勾選「啟用 **Microsoft Outlook** 自動防護」。
「Microsoft Outlook 自動防護」會自動安裝在執行 Outlook 的電腦上。
 - 對於低於 14.2 RU1 的版本，請在「**Internet** 電子郵件自動防護」標籤上，勾選「啟用 **Internet** 電子郵件自動防護」。
伺服器作業系統不支援「Internet 電子郵件自動防護」。
 - 對於低於 14.2 RU1 的版本，請在「**Notes** 自動防護」標籤上，勾選「啟用 **Lotus Notes** 自動防護」。
4. 按下「確定」。

[關於自動防護的類型](#)

[如何判定用戶端電腦是否已使用「狀態」頁面圖示進行防護](#)

瞭解向賽門鐵克傳送資訊可改善電腦防護功能

Windows 適用的 Symantec Endpoint Protection 用戶端指南

依據預設，用戶端會定期向賽門鐵克傳送匿名偵測、網路及組態資訊。賽門鐵克使用此資訊保護您的用戶端電腦，使其免受新威脅、目標威脅和變種威脅的危害。您傳送的任何資料都可提升賽門鐵克回應威脅的能力。賽門鐵克建議您傳送盡可能多的資訊。

賽門鐵克會竭盡所能匿名化用戶端傳送的任何資訊。

用戶端向賽門鐵克傳送匿名資訊可為您提供下列好處：

- 增強網路安全性
- 最佳化產品效能

不過，在某些情況下，您可能想要阻止用戶端傳送某些資訊。您可以僅停用網路資訊傳送，而非停用所有類型的用戶端傳送資訊。

NOTE

賽門鐵克建議您始終保持用戶端傳送資訊為啟用狀態。停用傳送可能會妨礙對組織中獨佔使用之應用程式誤報偵測的快速解析。如果沒有組織中惡意軟體的相關資訊，產品和賽門鐵克對威脅的回應可能需要更長時間。

Symantec 遙測收集的資料可能包括不可直接識別的匿名元素。Symantec 既不需要也不會設法使用遙測資料來識別任何個別使用者。

修改向賽門鐵克傳送資訊

1. 選取「變更設定」>「用戶端管理」。
2. 在「提交」標籤上，勾選「將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報」。此選項可讓 傳送在您電腦中發現的威脅之相關資訊，以及網路和組態的相關資訊。
賽門鐵克建議您保持此選項的啟用狀態。
3. 如果想選擇要傳送的資訊類型，請選取「更多選項」。
4. 按下「確定」。

您也可以將檔案從隔離所手動傳送至賽門鐵克。

[管理電腦上的隔離檔案](#)

如需隱私權的詳細資訊，請參閱下列文件：

[隱私權聲明](#)

關於用戶端和 Windows 資訊安全中心

Windows 適用的 Symantec Endpoint Protection 用戶端指南

如果您在 Windows XP (已安裝 Service Pack 2 或 Service Pack 3) 上使用 Windows 資訊安全中心 (WSC)，則可以在 WSC 中查看 的狀態。

下表顯示 WSC 中的防護狀態報告。

Table 10: WSC 防護狀態報告

賽門鐵克產品狀況	防護狀態
尚未安裝	找不到 (紅色)
已安裝，並啟用全面防護	開啟 (綠色)

賽門鐵克產品狀況	防護狀態
已安裝，但病毒和安全風險定義不是最新的	過期 (紅色)
已安裝，但未啟用檔案系統的「自動防護」。	關閉 (紅色)
已安裝，但未啟用檔案系統的「自動防護」，而且病毒和安全風險定義不是最新的	關閉 (紅色)
已安裝，但 ccSvcHst 已手動關閉	關閉 (紅色)

下表顯示 WSC 中報告的 防火牆狀態。

Table 11: WSC 防火牆狀態報告

賽門鐵克產品狀況	防火牆狀態
未安裝 Symantec Firewall	找不到 (紅色)
已安裝並啟用 Symantec Firewall	開啟 (綠色)
已安裝 Symantec Firewall，但未啟用	關閉 (紅色)
尚未安裝或啟動 Symantec Firewall，但有安裝並啟動第三方的防火牆	開啟 (綠色)

NOTE

在 中，預設會停用「Windows 防火牆」。

如果啟用一個以上的防火牆，WSC 會報告已安裝並啟用多個防火牆。

管理行為分析 (SONAR)

Windows 適用的 Symantec Endpoint Protection 用戶端指南

在 14.3 RU5 中，SONAR 已重命名為行為分析。

行為分析這種即時防護可在電腦上執行應用程式時偵測潛在惡意的行為。行為分析使用啟發式技術及信譽資料來偵測新出現和不明威脅。行為分析提供「零時差」防護，因為它會在傳統病毒和間諜軟體偵測定義檔建立前偵測惡意行為，從而解決威脅。

您可以將行為分析作為「主動型威脅防護」的一部分進行管理。在受管用戶端上，管理員可能會鎖定部分設定。

只要啟用「主動威脅防護」，預設就會啟用行為分析。

請參閱：[在用戶端電腦上啟用防護](#)

Table 12: 管理行為分析

步驟	說明
步驟 1：確定已啟用智慧型掃描查詢 (14.3 RU4 和更早版本)	除了啟發式之外，行為分析還會使用信譽資料進行偵測。如果停用智慧型掃描查詢 (信譽查詢)，行為分析將只採用啟發式技術進行偵測。誤報率可能會增加，且行為分析提供的防護會受到限制。 自訂下載鑑識設定
步驟 2：防止誤報偵測	您也可以變更對行為分析偵測到的某些威脅類型的偵測動作。您可能希望變更偵測動作以減少偵測誤報率。 防止對行為分析 (SONAR) 的誤報偵測

步驟	說明
步驟 3：為已知安全的應用程式建立例外	行為分析可能會將您想要在電腦上執行的非惡意檔案或應用程式偵測為惡意檔案或應用程式。而且，在某些情況下，當行為分析將程式碼插入應用程式中進行檢查時，應用程式可能變得不穩定或無法執行。 您可以從下列位置新增檔案、資料夾或應用程式的 SONAR 例外： 「系統變更偵測」標籤。 「例外 > 變更設定」頁面上的 SONAR 例外。 排除掃描項目 「隔離」。
步驟 4：將有關行為分析偵測的相關資訊提交給「賽門鐵克安全機制應變中心」(選用)	賽門鐵克建議您將有關偵測的資訊傳送至「賽門鐵克安全機制應變中心」。此資訊有助於賽門鐵克處理威脅。遞送預設為啟用。 瞭解向賽門鐵克提交資訊可改善電腦防護功能

防止對行為分析 (SONAR) 的誤報偵測

Windows 適用的 Symantec Endpoint Protection 用戶端指南

若要減少誤報偵測率，您可以在監控偵測時暫時將偵測動作變更為「只記錄」。

NOTE

在受管用戶端上，管理員可能會鎖定這些設定。

防止對行為分析的誤報偵測

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「主動型威脅防護」旁，按下「架構設定」。
3. 在「行為分析」標籤或「系統變更偵測」標籤上，將高風險或低風險偵測的動作短時間變更為「只記錄」。
4. 按下「確定」。

[管理行為分析 \(SONAR\)](#)

透過主機完整性掃描檢查電腦安全性遵從

Windows 適用的 Symantec Endpoint Protection 用戶端指南

主機完整性掃描可確認在電腦連線至網路之前該電腦是否符合某些安全性需求。例如，主機完整性檢查可以確認作業系統是否有最新的安全修正程式。如果您的電腦不符合安全性需求，則用戶端會矯正您的電腦，以確保其可以通過主機完整性檢查。若要矯正，檢查會自動下載並安裝必要的軟體。您的管理員可能會傳送讓您矯正電腦的訊息。

主機完整性檢查將在您啟動電腦時執行，並且會在網路連線結束之前一直執行。您也可以手動執行主機完整性檢查。

即使特定需求未能通過，您的管理員也可以將主機完整性檢查架構為通過。您可以在用戶端安全日誌中檢視主機完整性檢查的結果。

透過主機完整性掃描檢查電腦安全性遵從：

1. 在用戶端的側邊列中，按下「掃描威脅」。
2. 在「掃描威脅」對話方塊中，按下「執行主機完整性掃描」。
3. 按下「確定」。

如果遵從失敗阻止了您對網路的存取，則應該在更新電腦以符合遵從需求時重新獲得存取權。

掃描結果將會出現在安全日誌中。

矯正您的電腦以通過主機完整性檢查

Windows 適用的 Symantec Endpoint Protection 用戶端指南

如果用戶端未能符合主機完整性政策需求，則用戶端會以下列其中一種方式回應：

- 用戶端會自動下載軟體更新。
- 用戶端會提示您下載所需的軟體更新。

矯正電腦：

在對話方塊中，執行下列其中一個動作：

- 若要檢視電腦不符合的安全性需求，請按下「詳細資料」。
- 若要立即安裝軟體，請按下「立即還原」。
在開始安裝之後，您可能無法選擇取消安裝。
- 若要延後進行軟體安裝，請按「稍後提醒我」，然後在下拉式清單中選擇時間間隔。
管理員能夠架構您延後安裝的次數上限。

啟用竄改防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「竄改防護」為伺服器及用戶端上執行的賽門鐵克應用程式提供即時防護。可防止威脅和安全風險竄改賽門鐵克資源。您可以啟用或停用「竄改防護」。您也可以架構「竄改防護」在偵測到意圖竄改電腦上的賽門鐵克資源時，所要採取的動作。

根據預設，「竄改防護」已設定為「攔截且不記錄」。

NOTE

若為受管用戶端，管理員可能會鎖定「竄改防護」設定。

啟用竄改防護：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「用戶端管理」旁，按下「架構設定」。
3. 在「竄改防護」標籤上，確保已勾選「防護賽門鐵克安全軟體不受竄改或關閉」。
4. 在「應用程式嘗試竄改或關閉賽門鐵克安全軟體時要執行的動作」清單方塊中，按下「只記錄」、「攔截且不記錄」或「攔截並記錄」。
5. 按下「確定」。

病毒和間諜軟體掃描的運作方式

Windows 適用的 Symantec Endpoint Protection 用戶端指南

病毒和間諜軟體掃描身分並處理或清除電腦上的病毒和安全風險。掃描會使用下列程序排除病毒或風險：

- 掃描引擎會在電腦上的檔案和其他元件中，搜尋病毒、特洛伊木馬程式、病蟲和其他威脅 (例如安全風險)。每種威脅都有可辨識的型樣，就是所謂的特徵。用戶端會使用包含大量已知特徵資訊的定義檔。掃描引擎會將每個檔案或元件與定義檔進行比較。如果掃描引擎發現符合的特徵，表示該檔案已受到感染或帶有惡意。
- 掃描引擎使用定義檔來判斷威脅所屬的種類。掃描引擎會對威脅採取矯正動作。掃描引擎會清除、刪除或隔離被偵測為威脅的項目。掃描引擎也會修復威脅所造成的任何副作用。它所採取的動作，取決於偵測到的威脅類型。

[掃描如何回應偵測到的病毒或風險](#)

- 在連線至雲端的標準或內嵌式/VDI 用戶端上，掃描會存取雲端中的完整定義檔集。

[Windows 用戶端如何從雲端接收定義檔](#)

NOTE

不會隔離，也不會清除 Windows 8 樣式應用程式中所偵測到的任何風險。會刪除該風險。

下表說明用戶端會在您電腦上掃描的元件。

Table 13: 用戶端掃描的電腦元件

元件	說明
選取的檔案	用戶端會根據您選取的掃描類型或管理員排程的掃描類型，來掃描個別檔案。您也可以在 Windows 中掃描個別檔案或資料夾。針對大部分的掃描類型，您可以選取要掃描的檔案。
電腦記憶體	用戶端會掃描電腦的記憶體。任何檔案病毒、開機磁區病毒或巨集病毒都可能常駐在記憶體中。常駐在記憶體中的病毒已自行複製到電腦的記憶體中。病毒可以隱藏在記憶體中，直到發生觸發事件為止。然後，病毒會散佈到硬碟機中。掃描無法清除存在於記憶體中的病毒。然而，出現提示時，您可以重新啟動電腦，以移除記憶體中的病毒。
開機磁區	用戶端會檢查電腦的開機磁區是否有開機病毒。將對兩個項目進行檢查：分割區表與主要開機記錄。
卸除式媒體	利用卸除式媒體 (例如 USB 磁碟機) 傳播，是某些威脅的常見傳播方式。用戶端不會在您插入卸除式媒體時自動掃描該媒體，但您可以在 Windows 中透過對媒體按下滑鼠右鍵來對其進行掃描。

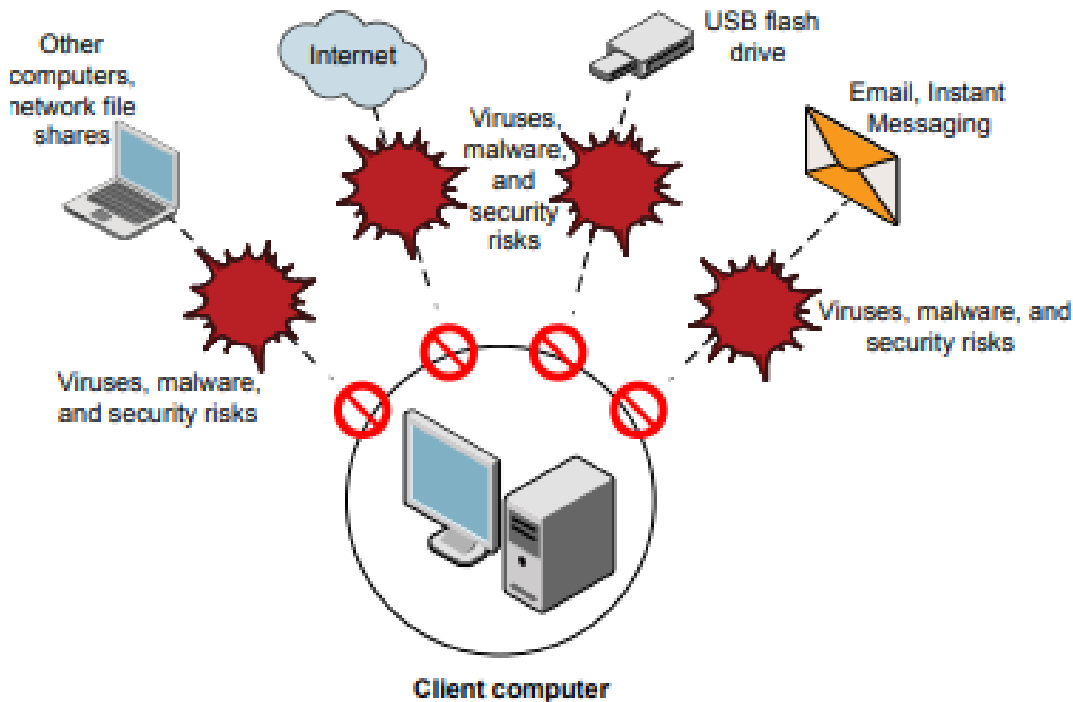
關於病毒與安全風險

Windows 適用的 Symantec Endpoint Protection 用戶端指南

可以掃描病毒和安全風險。安全風險包含間諜軟體、廣告軟體、Rootkit 和可使電腦或網路處於風險之中的其他檔案。

病毒和安全風險可透過電子郵件或時傳訊程式感染。您可能會在接受軟體程式的使用者授權許可協議時，不知不覺地下載風險。

許多病毒和安全風險都以「偷渡式下載」安裝到電腦。這些下載通常在您訪問惡意網站或受感染網站時出現。應用程式的下載程式透過您電腦上的合法漏洞進行安裝。



下表列出可能攻擊電腦的病毒和風險類型。

Table 14: 病毒和安全風險

風險	說明
病毒	執行時將本身附加在其他電腦程式或檔案的程式或檔案。當受感染的程式執行時，附加的病毒程式會啟動，並將自己附加到其他程式和檔案中。 病毒類別中包含下列威脅類型： - 惡意 Internet Bot 在 Internet 上執行自動化工作的程式。Bots 可用來自動化對電腦的攻擊，或從網站收集資訊。 - 病蟲 複製時不會感染其他程式的程式。有些病蟲透過在磁碟間自我複製來進行傳播，而另外一些病蟲在記憶體中進行複製，從而降低電腦效能。 - 特洛伊木馬程式 將自己隱藏在諸如遊戲或公用程式之類的無害程式中的程式。 - 混合型威脅 將病毒、病蟲、特洛伊木馬程式和程式碼與伺服器 and Internet 弱點混合，以便起始、傳送和散佈攻擊的威脅。混合型威脅利用多種方法和技術迅速傳播，並導致大範圍的破壞。 - Rootkit 藏匿在電腦作業系統中的程式。
廣告軟體	提供廣告內容的程式。
Cookie	Web 伺服器傳送到網頁瀏覽器來用於識別電腦或使用者的訊息。
撥接工具	這類程式通常會利用電腦，在沒有使用者許可或不知情的狀況下，透過 Internet 撥號到 900 號碼或是 FTP 網站。通常，撥接這些號碼，會產生費用。
駭客工具	駭客所使用的程式，可以未經授權存取使用者的電腦。例如，有一種駭客工具叫做按鍵記錄器，它可以追蹤與記錄個別的按鍵，並傳回這個資訊給駭客。然後駭客就可以執行通訊埠掃描或是漏洞掃描。駭客工具也可以用來建立病毒。

風險	說明
惡作劇程式	這種程式企圖以幽默或嚇人的方式，來改變或中斷電腦的作業。例如，玩笑程式會在使用者試圖刪除項目時，使資源回收筒遠離滑鼠。
誤導應用程式	故意誤報電腦安全性狀態的應用程式。這些應用程式通常偽裝成安全性通知，告知必須移除假病毒感染。
家長防護網程式	監控或限制電腦使用的程式。這些程式在執行時不會被偵測到，並且通常會將監控資訊傳輸到其他電腦。
勒索軟體	一種惡意軟體類別，會破壞文件並使其無法使用，但電腦使用者仍可存取電腦。
遠端存取程式	這種程式允許由其他電腦透過 Internet 存取，因此它們可以得到資訊，或是攻擊或改變使用者的電腦。
安全評定工具	用於收集資訊以便取得對電腦的未經授權的存取的程式。
間諜軟體	單機程式，可以秘密地監控系統活動，並偵測密碼以及其他機密的資訊，再將它轉遞回另一台電腦。
追蹤軟體	單機或附加的應用程式，可追蹤使用者在 Internet 上的路徑，並將資訊傳送到控制者或駭客系統。

您可以在[賽門鐵克資訊安全中心](#)檢視有關特定風險的資訊。

賽門鐵克安全機制應變中心網站提供關於威脅和安全風險的最新資訊。該網站也提供大量的參考資訊，例如，關於病毒與安全風險的白皮書和詳細資訊。

掃描如何回應偵測到的病毒或風險

關於掃描類型

Windows 適用的 Symantec Endpoint Protection 用戶端指南

包含不同的掃描類型，用於防範不同類型的病毒、威脅和風險。

依預設，會在每天下午 12:30 執行作用中掃描。也會在新的定義到達用戶端電腦時執行作用中掃描。在非受管電腦上，還包含已停用的預設開機掃描。

NOTE

掃描會存取在雲端設定的完整定義檔。

Windows 用戶端如何從雲端接收定義檔

在非受管電腦上，您應確保每天在電腦上執行一次作用中掃描。如果您懷疑電腦上有非作用中威脅，您最好排程每週或每月執行一次完整掃描。完整掃描會消耗更多的電腦資源，而且可能會影響電腦效能。

Table 15: 掃描類型

掃描類型	說明
自動防護	「自動防護」會持續檢查寫入電腦或從電腦讀取的檔案和電子郵件資料。「自動防護」會自動處理或清除偵測到的病毒和安全風險。 「自動防護」還會保護您可能傳送或接收的某些電子郵件。 在連線至雲端的標準和內嵌式/VDI 用戶端上，自動防護也會使用雲端定義檔。 關於自動防護的類型
下載鑑識	「下載智慧型掃描」透過以下方法提昇自動防護的安全性：當使用者嘗試從瀏覽器及其他入口網站下載檔案時檢查檔案。 「下載智慧型掃描」會使用「賽門鐵克智慧型掃描」所提供的資訊。「賽門鐵克智慧型掃描」從社群數百萬使用者收集資訊來判斷檔案的安全信譽。「下載智慧型掃描」會使用檔案的信譽等級來允許或攔截檔案，或提示使用者對檔案採取動作。 「下載智慧型掃描」包含在「自動防護」中因此需要啟用「自動防護」。如果停用「自動防護」但啟用「下載鑑識」，則「下載鑑識」無法運作。 Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策

掃描類型	說明
管理員掃描和使用者定義的掃描	對於受管用戶端，管理員可建立排程掃描或執行隨選掃描。在非受管用戶端或掃描設定已解除鎖定的受管用戶端上，您可以建立和執行自己的掃描。 管理員掃描或使用者定義的掃描偵測病毒和安全性風險的方法為檢查用戶端電腦上的全部檔案和程序。這些掃描類型也可以檢驗記憶體和載入點。 在連線至雲端的標準和內嵌式/VDI 用戶端上，這些掃描會使用雲端定義檔。 系統提供以下類型的管理員掃描或使用者定義掃描： • 排程掃描 排程掃描會於指定時間在用戶端電腦上執行。任何排程時間相同的掃描都會按順序執行。若於排程掃描期間電腦為關閉狀態，除非電腦已架構為重試未執行的掃描，否則不會執行此掃描。您可以排程作用中掃描、完整掃描或自訂掃描。 排程掃描設定可以儲存為範本。您可使用另存為範本的任何掃描作為不同掃描的基礎。架構多個政策時，使用掃描範本可節省時間。根據預設，政策中會包含排程掃描範本。預設排程掃描會掃描所有的檔案和資料夾。 • 開機掃描和觸發掃描 開機掃描於使用者登入電腦時執行。觸發掃描於新的病毒定義檔下載至電腦時執行。 • 隨選掃描 隨選掃描是由您手動啟動的掃描。您可以透過 [掃描威脅] 頁面執行隨選掃描。 如果用戶端偵測到大量的病毒、間諜軟體或高風險威脅，則進入主動掃描模式。掃描將重新啟動並使用智慧型掃描查詢。 病毒和間諜軟體掃描的運作方式
行為分析 (SONAR)	行為分析甚至可以在傳統特徵型定義檔可解決威脅之前，阻止攻擊。行為分析使用啟發式技術及檔案信譽資料來偵測新出現和不明威脅。

關於自動防護的類型

Windows 適用的 Symantec Endpoint Protection 用戶端指南

自動防護會掃描檔案及某些類型的電子郵件和電子郵件附件。

「自動防護」只適用於支援的電子郵件用戶端，它不會保護郵件伺服器。

NOTE

如果在開啟電子郵件時偵測到病毒，該電子郵件可能要花數秒鐘才能開啟，讓「自動防護」完成掃描。

Table 16: 自動防護的類型

自動防護的類型	說明
檔案系統自動防護	在從電腦讀取檔案或將檔案寫入電腦時，持續掃描檔案。 預設會為檔案系統啟用自動防護。自動防護在電腦啟動時載入。此項防護將檢測所有檔案中是否存在病毒及安全風險，並攔截安全風險的安裝。可選擇掃描檔案副檔名、掃描遠端電腦上的檔案，以及掃描磁片上的開機病毒。可選擇先備份檔案，再嘗試修復檔案、終止程序及停止服務。 您可以架構「自動防護」只掃描選取的副檔名。當自動防護掃描選取的副檔名時，即使病毒變更了檔案的副檔名，自動防護也能判斷檔案的類型。 自動防護會掃描所有檔案，甚至包括電子郵件附件。如果您未針對電子郵件啟用自動防護，用戶端電腦仍會在啟用檔案系統自動防護時受到保護。大多數電子郵件應用程式會在使用者啟動電子郵件附件時，將附件儲存到暫存資料夾。自動防護會在檔案寫入暫存資料夾時掃描檔案，並偵測是否存在任何病毒或安全風險。如果使用者嘗試將受感染的附件儲存到本機磁碟機或網路磁碟機，「自動防護」也會偵測病毒。
Microsoft Outlook 自動防護	下載內送的 Microsoft Outlook 電子郵件附件，並在您讀取郵件並開啟附件時掃描是否有病毒和安全風險。 Microsoft Outlook 自動防護支援 Microsoft Outlook 98 到 Outlook 2016 的 MAPI 或 Internet 通訊協定。Microsoft Outlook 自動防護支援 32 位元和 64 位元系統。 安裝期間，如果您的管理員將 Microsoft Outlook 自動防護包含在套件中，而且電腦上已安裝 Microsoft Outlook，會安裝 Microsoft Outlook 自動防護。 如果您透過慢速連線下載大型附件，會影響電子郵件效能。如果您經常收到大型附件，您可能會想要停用這項功能。 Note: 請不要在 Microsoft Exchange Server 上安裝 Microsoft Outlook 自動防護。
Internet 電子郵件自動防護 (僅適用於低於 14.2 RU1 的用戶端版本。)	掃描入埠 Internet 電子郵件內文和電子郵件附件是否存在病毒和安全風險；此外，也執行離埠電子郵件啟發式掃描。 依據預設，「Internet 電子郵件自動防護」支援透過 POP3 與 SMTP 連線的加密密碼及電子郵件。 「Internet 電子郵件自動防護」支援 32 位元或 64 位元系統。如果您使用 POP3 或 SMTP 搭配安全通訊端層 (SSL)，則用戶端會偵測安全連線，但不會掃描加密的郵件。 Note: 基於效能考量，伺服器作業系統不支援 POP3 的「Internet 電子郵件自動防護」。 電子郵件掃描不支援 IMAP、AOL 或 HTTP 式的電子郵件，例如 Hotmail 或 Yahoo! Mail。
Lotus Notes 自動防護 (僅適用於低於 14.2 RU1 的用戶端版本。)	掃描內送的 Lotus Notes 電子郵件附件是否存在病毒和安全風險。 Lotus Notes 自動防護支援 Lotus Notes 7.x 或更新版本。 安裝期間，如果您的管理員將 Lotus Notes 自動防護包含在套件中，而且電腦上已安裝 Lotus Notes，會安裝 Lotus Notes 自動防護。

掃描如何回應偵測到的病毒或風險

Windows 適用的 Symantec Endpoint Protection 用戶端指南

病毒和安全風險感染檔案時，用戶端會以不同的方式回應威脅類型。對於各類威脅，用戶端都會使用第一個動作，如果第一個動作失敗，則會使用第二個動作。

Table 17: 用戶端如何回應病毒和安全風險

威脅類型	動作
病毒	根據預設，當用戶端偵測到病毒時會採取下列動作： - 用戶端會先嘗試從受感染的檔案清除病毒。 - 如果用戶端清除檔案，用戶端即完全將風險從您的電腦移除。 - 如果用戶端無法清除檔案，就會記錄這個失敗，並將受感染的檔案移到「隔離所」。 管理電腦上的隔離檔案 Note: 不會隔離在 Windows 8 樣式應用程式和檔案中偵測到的病毒。會刪除這個病毒。
安全風險	根據預設，當用戶端偵測到安全風險時會採取下列動作： - 用戶端會隔離受感染的檔案。 - 用戶端會嘗試移除或修復安全風險所造成的任何變更。 - 如果用戶端無法隔離安全風險，就會記錄該風險，並讓它保持原狀。 在某些情況下，您可能在不知情的情況下，不小心安裝了包含安全風險的應用程式，如廣告軟體和間諜軟體。當偵測到此類安全風險時，用戶端會採取下列動作： - 如果隔離風險的動作不會對電腦造成傷害或讓電腦處於不穩定的狀態，用戶端會立即這麼做。 - 否則，用戶端會先等候應用程式安裝完成，然後才隔離風險，接著再修復風險所造成的影響。 Note: 不會隔離在 Windows 8 樣式應用程式和檔案中偵測到的安全風險。會刪除該風險。

對於各掃描類型，您可以變更用戶端處理病毒和安全風險方式的設定。對於各類別的風險和個別安全風險，您可以設定不同的動作。

如何使用 Symantec Insight 進行檔案相關決策

賽門鐵克會從其全球數百萬使用者的社群及全球情報網收集有關檔案的資訊。收集的資訊可透過 Symantec Insight 供雲端中的賽門鐵克產品使用。Symantec Insight 可提供檔案信譽資料庫以及最新的病毒和間諜軟體定義檔。

賽門鐵克產品會利用 Insight 保護用戶端電腦，使其免受新威脅、目標威脅和變種威脅的危害。該資料有時也稱為雲端資料，因為它並非置於用戶端電腦。必須要求或查詢 Insight 以取得資訊。查詢稱為信譽查詢、雲端查詢或智慧型掃描查詢。

Insight 信譽分級

Symantec Insight 可判斷每個檔案的風險等級或安全性分級。分級亦稱為檔案的信譽。

Insight 可透過檢查檔案的下列特性及其內容，判斷檔案的安全性等級：

- 檔案來源
- 檔案新舊程度
- 檔案在社群中的常用程度
- 其他安全性衡量標準，例如檔案可能與惡意軟體關聯的程度

智慧型掃描查詢

中的掃描功能會利用智慧型掃描來進行檔案和應用程式的相關決策。病毒和間諜軟體防護包含一項名為「下載智慧型掃描」的功能。下載鑑識需要信譽資訊來進行偵測。行為分析 (SONAR) 也會使用信譽資訊進行偵測。

若要變更智慧型掃描查詢設定

- 在「用戶端」標籤上，前往「政策 > 設定 > 外部通訊 > 用戶端傳送」。

若要變更 Windows 用戶端上的智慧型掃描查詢設定

- 移至「變更設定 > 用戶端管理 > 傳送」。

在標準和內嵌式/VDI 用戶端上，智慧型掃描查詢選項還會允許自動防護與排程掃描和手動掃描查詢檔案信譽資訊以及雲端中的定義檔。賽門鐵克建議您將此選項保持啟用。

WARNING

下載鑑識、行為分析 (SONAR) 以及病毒和間諜軟體掃描會使用智慧型掃描查詢來偵測威脅。賽門鐵克建議您始終允許智慧型掃描查詢。停用查詢會停用「下載鑑識」，並影響 SONAR 啟發式掃描 (僅限 14.3 RU4 和更早版本) 以及病毒和間諜軟體掃描的功能。

檔案信譽傳送

依據預設，用戶端電腦會將信譽偵測的相關資訊傳送到賽門鐵克安全機制應變中心進行分析。此資訊有助於調整智慧型掃描的信譽資料庫以及雲端中的最新定義檔。傳送資訊的用戶端愈多，信譽資料庫就會變得愈有用。

賽門鐵克建議您持續為信譽偵測啟用用戶端傳送資訊功能。

管理防火牆防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

根據預設，用戶端會提供電腦所需的適當防火牆防護等級。不過，您的管理員可能變更了某些預設防火牆規則和設定。如果您的管理員授予了您修改防火牆防護的權限，您就可以修改防火牆規則或防火牆設定。

下表說明您可以執行以保護電腦的防火牆工作。所有這些工作都是選擇性的工作，並且可以任何順序執行。

Table 18: 管理防火牆防護

工作	說明
讀取防火牆的運作方式	瞭解防火牆如何保護電腦不受網路攻擊威脅。 防火牆的運作方式
新增及自訂防火牆規則	您可以新增防火牆規則或編輯現有的防火牆規則。例如，您可以攔截不想在電腦上執行的應用程式，例如廣告軟體應用程式。 管理防火牆規則 您也可以架構防火牆規則來允許或防止應用程式存取網路。 允許或攔截已在用戶端上執行的應用程式
架構防火牆設定	除建立防火牆規則外，您還可以啟用及架構防火牆設定，以進一步增強防火牆防護。 啟用防火牆設定
檢視防火牆日誌	您可以定期檢查電腦上的防火牆防護狀態，以確定以下事項： • 您所建立的防火牆規則是否正常運作。 • 用戶端是否攔截任何網路攻擊。 • 用戶端是否攔截您希望執行的任何應用程式。 您可以使用「流量日誌」和「封包日誌」來檢查防火牆防護狀態。根據預設，「封包日誌」在受管用戶端上為停用。 關於日誌 啟用封包日誌
允許或攔截應用程式和某些類型的流量	為了額外的安全性，您可以在下列情況下攔截網路流量以防存取您的電腦。 • 當電腦的螢幕保護程式開啟時，您可以攔截流量。 • 當防火牆沒有執行時，您可以攔截流量。 • 您可以在任何時候攔截全部流量。 當螢幕保護程式處於作用中狀態或防火牆未執行時攔截流量 • 您可以自動地允許或攔截網路存取，也可以由電腦上所執行的應用程式來要求您這麼做。您也可以架構 允許或攔截應用程式存取網路 允許或攔截已在用戶端上執行的應用程式
啟動或停用防火牆。	您可以暫時停用「網路威脅防護」以進行疑難排解。例如，您可能需要停用防火牆以便能夠開啟某個應用程式。 在用戶端電腦上啟用防護

防火牆的運作方式

防火牆可防止任何未經授權的使用者存取您組織中連線至 Internet 的電腦和網路。

此外，防火牆會執行下列任務：

- 監控您的電腦與 Internet 上其他電腦之間的通訊
- 建立防護措施，允許或攔截他人企圖存取您電腦上的資訊
- 警告您來自其他電腦的連線嘗試
- 警告您電腦上的應用程式嘗試連線到其他電腦

防火牆檢視 Internet 上載送的資料封包。封包是不連續的資料單位，屬於兩台電腦間資訊流的一部分。封包會在目的地重組起來，成為不中斷的資料流。

套件包含顯示下列關於資料的資訊：

- 來源電腦
- 指定收件者
- 封包資料的處理方式
- 接收封包的通訊埠

通訊埠是一種通道，會將來自 Internet 上的資料流分隔開來。電腦上執行的應用程式會接聽通訊埠。應用程式會接受傳送到通訊埠的資料。

網路攻擊即是利用易受攻擊的應用程式中的弱點。攻擊者會利用這些弱點，將包含惡意程式碼的封包傳送到通訊埠。當易受攻擊的應用程式接聽通訊埠時，惡意程式碼就能讓攻擊者存取電腦。

在 Windows 用戶端上管理防火牆規則

防火牆規則會控制防火牆如何防護您的電腦不受惡意的連入流量和應用程式侵襲。防火牆會針對您啟用的規則，檢查所有連入和連出封包。它會根據您在防火牆規則中指定的條件，允許或攔截封包。

NOTE

用戶端包含預設防火牆規則，可保護您的電腦。不過，如果您的管理員允許，或者您的用戶端未受管理，則可以為其他防護修改防火牆規則。

下表說明管理防火牆規則所需瞭解的相關內容。

Table 19: 管理防火牆規則

工作	說明
瞭解防火牆規則如何運作以及構成防火牆規則的內容	在修改防火牆規則之前，您應該瞭解防火牆規則如何運作： • 如何排序規則，以確保先評估限制最嚴格的規則，最後評估最一般的規則。 請參閱：關於防火牆規則、防火牆設定和入侵預防處理順序 • 用戶端使用狀態式檢測，以追蹤網路連線的狀態。 請參閱：防火牆如何使用狀態式檢測 • 組成防火牆規則的防火牆元件。 請查閱：用戶端上的防火牆規則元素
新增防火牆規則	您可以： • 將您自己的規則新增至 預設安裝的規則。 請參閱：在用戶端上新增防火牆規則 • 變更任何防火牆規則準則來自訂規則。 • 從其他防火牆政策匯出和匯入防火牆規則。 請參閱：在用戶端匯出或匯入防火牆規則 • 複製並貼上防火牆規則。

用戶端上防火牆規則的元素

Windows 適用的 Symantec Endpoint Protection 用戶端指南

當一台電腦嘗試連線到另一台電腦時，防火牆會將連線類型與防火牆規則進行比較。您可以使用應用程式、主機及通訊協定這類觸發條件，來定義防火牆規則。例如，一條可辨別與目的位址有關之通訊協定的規則。當防火牆評估規則時，全部觸發條件都必須為真，才會出現完全符合的狀況。若目前封包有任何觸發條件為假，防火牆就不會套用該項規則。

一旦封包觸發防火牆規則，防火牆便不會再進一步評估防火牆規則。如果封包未觸發任何規則，防火牆會自動攔劫封包，且不記錄該事件。

防火牆規則描述允許或攔截網路連線的條件。例如，某項規則可能允許每日上午 9 時至下午 5 時之間，在 IP 位址 192.58.74.0 和遠端通訊埠 80 之間進行的網路通訊。

下表說明用於定義防火牆規則的準則。

Table 20: 防火牆規則準則

條件	說明
觸發條件	• 應用程式 如果應用程式是您在允許流量規則中定義的唯一觸發條件，則防火牆會允許應用程式執行任何網路作業。應用程式才是發揮作用的值，而不是應用程式執行的網路作業。例如，假設您允許 Internet Explorer，而且未定義其他任何觸發條件。則使用者可以存取使用 HTTP、HTTPS、FTP、Gopher 及網頁瀏覽器所支援其他任何通訊協定的遠端站台。您可以定義其他觸發條件，說明允許進行通訊的特定網路通訊協定和主機。 • 主機 本機主機一定是本機用戶端電腦，而遠端主機一定是位在網路其他位置的遠端電腦。這種主機關係的表示方式與流量方向無關。在定義主機觸發條件時，您可以指定位於所述網路連線遠端的主機。 • 通訊協定 通訊協定觸發條件會根據所述的流量，識別產生作用的一項或多項網路通訊協定。 本機主機電腦一定擁有本機通訊埠，而遠端電腦一定擁有遠端通訊埠。這項通訊埠關係的說明與流量方向無關。 • 網路配接卡 如果您定義網路配接卡觸發條件，規則只會與使用指定配接卡類型傳輸或接收的流量有關。您可以指定任何配接卡，也可以指定目前與用戶端電腦關聯的配接卡。 您可以結合各項觸發準則，形成更複雜的規則，例如根據特定目的位址，識別特定通訊協定。當防火牆評估規則時，全部觸發條件都必須為真，才會出現完全符合的狀況。對於目前封包而言，如果其中有任一個觸發條件不是 True，防火牆即不會套用規則。
條件	• 排程和螢幕保護程式狀態 條件參數不會描述網路連線的任何內容。條件參數會決定規則的作用中狀態。條件參數是選用項目，如果未經定義，則不會有任何作用。您可以設定排程或識別螢幕保護程式的狀態，決定將規則視為作用中或非作用中的狀況。防火牆接收封包時，防火牆不會評估非作用中規則。
動作	• 允許或攔截，記錄或不記錄 動作參數會指定防火牆成功比對到規則時所採取的動作。如果規則是指對接收的封包選取的規則，則防火牆會執行全部動作。防火牆可以允許或攔截封包，也可以記錄或不記錄封包。 如果防火牆允許流量通過，規則指定的流量便可存取網路。 如果防火牆攔截流量，規則指定的流量則無法存取網路。

Symantec Endpoint Protection 用戶端程序防火牆規則的順序是什麼？

這項程序會持續進行，直到防火牆找到符合的規則為止。防火牆找到符合的規則後，就會採取該規則指定的動作，而不會再檢查優先順序較低的後續規則。例如，若第一項規則指定攔截所有流量，而下一項規則允許所有流量，則用戶端會攔截所有流量。

您可以根據限制的嚴格性將規則排序。先評估限制最嚴格的規則，最後評估最普通的規則。例如，攔截流量的規則應該排在規則清單前幾位，清單中優先順序較低的規則可能會允許流量。

建立規則資料庫的最佳方法，包括下列規則順序：

第一	攔截所有流量的規則。
第二	允許所有流量的規則。
第三	允許或攔截特定電腦的規則。
第四	允許或攔截特定應用程式、網路服務，以及通訊埠的規則。

Table 21: 處理順序

優先順序	設定
第一	自訂 IPS 特徵
秒	入侵預防設定、流量設定及隱藏設定
第三	內建規則
第四	防火牆規則
第五	通訊埠掃描檢查
第六	透過 LiveUpdate 下載的 IPS 特徵

在用戶端上新增防火牆規則

Windows 適用的 Symantec Endpoint Protection 用戶端指南

在用戶端上新增或變更防火牆規則時，您必須決定規則有何功能。例如，您可能想要允許來自特定來源的全部流量，或攔截來自某個網站的 UDP 封包。

建立防火牆規則時，將自動啟用規則。

NOTE

您可以在非受管用戶端或受管用戶端 (若管理員授予對受管用戶端的用戶端控制權) 上新增或變更防火牆規則。

若要新增防火牆規則：

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項」>「架構防火牆規則」。
3. 在「架構防火牆規則」對話方塊中，按下「新增」以開啟空白規則。

NOTE

對於受管用戶端，此動作會啟動規則建立精靈。以下步驟說明了架構空白規則。

4. 在空白規則的「一般」標籤上輸入規則的名稱，然後按下「攔截此流量」或「允許此流量」。
5. 若要定義規則的觸發條件，請按下各個標籤並視需要進行架構。
 - 一般
 - 主機
 - 通訊埠和通訊協定
 - 應用程式
 - 排程

例如，您可能要選取此規則套用到的網路配接器、此規則套用到的主機、規則處於作用中或非作用中狀態的時段，或記錄封包流量。

NOTE

寫入封包日誌時請務必小心，因為可能會記錄大量資料。

用戶端上防火牆規則的元素

6. 按下「確定」。
規則會自動啟用。您必須啟用規則，好讓防火牆處理這些規則。
7. 若要變更規則順序，請按下向上或向下箭頭。
8. 按下「確定」。

在用戶端上匯入或匯出防火牆規則

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以和另一個用戶端共用規則，即可不必重新建立規則。您可以從另一部電腦匯出規則，然後匯入至您的電腦。匯入規則時，這些規則會新增至防火牆規則清單的末端。即使匯入的規則與現有規則完全相同，匯入的規則也不會覆寫現有規則。

匯出的規則和匯入的規則會儲存在 .sar 檔案中。

在用戶端上匯出防火牆規則

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項」>「架構防火牆規則」。
3. 在「架構防火牆規則」對話方塊中，選取想要匯出的規則。
4. 在規則上按滑鼠右鍵，然後按下「匯出選取的規則」。
5. 在「匯出」對話方塊中，輸入檔案名稱，然後按下「儲存」。
6. 按下「確定」。

在用戶端上匯入防火牆規則

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項」>「架構防火牆規則」。
3. 在「架構防火牆規則」對話方塊中，在防火牆規則清單上按下滑鼠右鍵，然後按下「匯入規則」。
4. 在「匯入」對話方塊中，找出包含想要匯入規則的 .sar 格式檔案。
5. 按下「開啟」。
6. 按下「確定」。

啟用防火牆設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以啟用用戶端的防火牆設定來防護電腦，避免特定類型的網路攻擊。某些設定會取代您需要另外新增的防火牆規則。

NOTE

管理員不一定會允許您架構部分設定。

下表說明您可架構的防火牆設定類型以進一步自訂防火牆防護。

Table 22: 防火牆設定

類別	說明
重要網路服務的內建規則	提供了內建規則，供某些重要網路服務進行一般交換。有了內建規則，您無須建立明確允許這些服務的防火牆規則。處理期間，這些內建規則會在防火牆規則之前評估，如此符合作用中內建規則的封包即獲得允許。您可以定義 DHCP、DNS 和 WINS 服務的內建規則。
流量和隱藏網頁瀏覽	您可以啟用各種流量設定和隱藏網頁瀏覽設定，保護用戶端不受特定類型的網路攻擊。您可以啟用流量設定，偵測和攔截透過驅動程式、NetBIOS 和 Token Ring 進行通訊的流量。您可以架構設定，以偵測使用較隱形攻擊的流量。您也可以控制不符合任何防火牆規則的 IP 流量行為。
網路檔案和印表機共用	您可以允許用戶端在區域網路上共用本身的檔案或瀏覽共用的檔案與印表機。若要防範網路攻擊，您可以停用網路檔案與印表機共用。 在已安裝 用戶端的情況下啟用網路檔案和印表機共用
攻擊偵測和攔截	當 用戶端偵測到網路攻擊，會自動攔截連線以保護用戶端電腦的安全。然後，用戶端會在一段時間內自動攔截所有進出攻擊電腦 IP 位址的全部流量。 單一位置會攔截攻擊電腦的 IP 位址。
入埠流量控制	您可以架構電腦在下列情況下攔截入埠流量以及離埠流量： - 當您電腦的螢幕保護程式啟動時。 - 當防火牆停止執行時。 - 當您在任何時候想要攔截所有入埠及離埠流量時。 當螢幕保護程式處於作用中狀態或防火牆未執行時攔截流量

啟用防火牆設定：

1. 在用戶端中，按下「變更設定」。
2. 在「防網路和主機侵入」旁，按下「架構設定」。
3. 在「防火牆」標籤上，勾選要啟用的設定。
如需關於設定的詳細資訊，請按下「說明」。
4. 按下「確定」。

在已安裝 用戶端的情況下啟用網路檔案和印表機共用

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以允許用戶端在區域網路上共用本身的檔案或瀏覽共用的檔案與印表機。若要防範網路攻擊，您可以停用網路檔案與印表機共用。

Table 23: 啟用網路檔案與列印共用的方式

工作	說明
在「Microsoft Windows 網路」標籤上自動啟用網路檔案與印表機共用設定。	如果有防火牆規則攔截此流量，防火牆規則的優先順序將高於此設定。 自動啟用網路檔案和印表機共用與瀏覽
藉由新增防火牆規則，手動啟用網路檔案與印表機共用。	如果您需要更高的彈性 (相較於設定所提供者)，則可以新增防火牆規則。例如，當您建立規則時，可以指定特定主機而非所有主機。防火牆規則允許存取通訊埠來瀏覽和共用檔案及印表機。 您可以建立一套防火牆規則，讓用戶端得以共用其檔案。然後建立第二套防火牆規則，讓用戶端得以瀏覽其他檔案與印表機。 手動啟用網路檔案和印表機共用與瀏覽 手動允許其他電腦瀏覽用戶端電腦上的檔案

自動啟用網路檔案和印表機共用與瀏覽：

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項」>「變更設定」。
3. 在「**Microsoft Windows** 網路」標籤上，按下以下其中一個設定：
 - 若要瀏覽網路上的其他電腦和印表機，請按下「瀏覽網路上的檔案和印表機」。
 - 若要讓其他電腦瀏覽您的電腦上的檔案，請按下「與網路上的其他人共用我的檔案和印表機」。
4. 按下「確定」。

手動啟用網路檔案和印表機共用與瀏覽：

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項」>「變更設定」>「架構防火牆規則」。

NOTE

僅當您的管理員使此設定可用或者您正在執行非受管用戶端時，才可查看此設定。

3. 在「架構防火牆規則」對話方塊中，按下「新增」。
4. 在「一般」標籤上輸入規則名稱，並按下「允許此流量」。
5. 在「通訊埠和通訊協定」標籤的「通訊協定」下拉式清單中，按下 **TCP**。
6. 在「遠端通訊埠」下拉式清單中，輸入以下內容：
88, 135, 139, 445
7. 按下「確定」。
8. 在「架構防火牆規則」對話方塊中，按下「新增」。
9. 在「一般」標籤上輸入規則名稱，並按下「允許此流量」。
10. 在「通訊埠和通訊協定」標籤的「通訊協定」下拉式清單中，按下 **UDP**。
11. 在「遠端通訊埠」下拉式清單中，輸入以下內容：
88
12. 在「本機通訊埠」下拉式清單中，輸入以下內容：
137, 138
13. 按下「確定」。

手動讓其他電腦瀏覽用戶端電腦上的檔案：

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「架構設定」。
3. 在「架構防火牆規則」對話方塊中，按下「新增」。
4. 在「一般」標籤上輸入規則名稱，並按下「允許此流量」。
5. 在「通訊埠和通訊協定」標籤的「通訊協定」下拉式清單中，按下 **TCP**。
6. 在「本機通訊埠」下拉式清單中，輸入以下內容：
88, 135, 139, 445
7. 按下「確定」。
8. 在「架構防火牆規則」對話方塊中，按下「新增」。
9. 在「一般」標籤上輸入規則名稱，並按下「允許此流量」。
10. 在「通訊埠和通訊協定」標籤的「通訊協定」下拉式清單中，按下 **UDP**。
11. 在「本機通訊埠」下拉式清單中，輸入以下內容：
88, 137, 138

12. 按下「確定」。

允許或攔截應用程式存取網路

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以將 架構為允許或攔截應用程式，或架構為先詢問您要允許應用程式還是攔截應用程式。此動作會建立防火牆規則，該規則指定電腦上的執行中應用程式是否可以存取網路。這些規則稱為以應用程式為基礎的防火牆規則。例如，您可以攔截 Internet Explorer 從您的電腦存取任何網站。

Table 24: 應用程式存取用戶端或網路時，防火牆採取的動作

動作	說明
允許	允許入埠流量存取用戶端電腦，以及允許離埠流量存取網路。 如果用戶端接收流量，圖示的左下角會顯示一個小藍點。如果用戶端傳送流量，小藍點會顯示在圖示的右下角。
攔截	阻止入埠流量及離埠流量存取網路或網際網路連線。
詢問	詢問您下次嘗試執行應用程式時，是否要應用程式存取網路。
終止	停止程序。

允許或攔截應用程式存取網路：

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項」>「檢視網路活動」。
3. 在「網路活動」對話方塊中的執行應用程式或服務上按下滑鼠右鍵，然後選取您希望用戶端對該應用程式採取的動作。
如果您按下「允許」、「攔截」或「詢問」，則僅針對該應用程式建立防火牆規則。

[允許或攔截已在用戶端上執行的應用程式](#)

4. 按下「關閉」。

允許或攔截已在用戶端上執行的應用程式

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以針對已在用戶端電腦上執行之應用程式的允許或攔截時間和方式架構條件。例如，您可以指定某個電玩遊戲應用程式只能在特定時段存取網路。應用程式型防火牆規則也稱為應用程式設定。

[允許或攔截應用程式存取網路](#)

NOTE

如果防火牆規則和以應用程式為基礎的防火牆規則發生衝突，則會優先採用防火牆規則。例如，可攔截凌晨 1:00 至上午 8:00 之間所有流量的防火牆規則，會覆寫可允許 iexplore.exe 隨時執行的應用程式規則。

允許或攔截已在用戶端上執行的應用程式：

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項 > 檢視應用程式設定」。
3. 在「檢視應用程式設定」對話方塊中，您可以透過在應用程式上按下滑鼠右鍵，然後按下「允許」、「詢問」或「攔截」來變更動作。
4. 若要變更應用程式型規則的其他選項，請按下「架構」。
5. 在「架構應用程式設定」對話方塊中，架構此應用程式的限制或例外。

如果動作已在步驟 3 中設定為「允許」，則您架構的所有設定都是此規則的限制。如果您按下「攔截」，則您架構的設定就是此規則的例外。

若需這些設定的詳細資訊，請按下「說明」。

6. 按下「確定」，接受組態變更。
7. 若要移除您對應用程式加諸的規則，請按下應用程式名稱，然後按下「移除」。在移除限制時，也會消除用戶端針對應用程式採取的動作。當應用程式或服務嘗試再度連線至網路時，系統會再次詢問您是要允許或攔截應用程式。
若要移除所有應用程式型防火牆規則，請按下「全部移除」。
8. 按下「確定」，關閉「檢視應用程式設定」對話方塊。

當螢幕保護程式處於作用中狀態或防火牆未執行時攔截流量

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構您的電腦在下列情況下攔截入埠流量以及離埠流量：

當您電腦的螢幕保護程式啟動時	您可以架構讓電腦在啟動螢幕保護程式時，攔截「網路上的芳鄰」的所有入埠及離埠流量。一旦關閉螢幕保護程式時，您的電腦就會返回先前指派的安全層級。 在螢幕保護程式啟動時攔截流量
當防火牆停止執行時	在電腦啟動後，防火牆服務啟動前，或在防火牆服務停止、電腦關閉之後的這段時間，電腦皆不受保護。這段時間是安全上的漏洞，可能會允許未經授權的通訊。 在防火牆停止執行時攔截流量
當您想要隨時攔截所有入埠及離埠流量時	您可能會在破壞性病毒攻擊您的網路或子網路時攔截所有流量。在一般情況下您不會攔截所有流量。 Note: 管理員可能已經架構不提供這個選項。您無法攔截非受管用戶端上的通訊。 在任何時候攔截全部流量

停用「網路威脅防護」後即可允許全部流量。

在用戶端電腦上啟用防護

在螢幕保護程式啟動時攔截流量：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「防網路和主機侵入」旁，按下「架構設定」。
3. 在「Microsoft Windows 網路」標籤上，按下「執行螢幕保護程式時，攔截 Microsoft Windows 網路流量」。
4. 按下「確定」。

在防火牆未執行時攔截流量：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「防網路和主機侵入」旁，按下「架構設定」。
3. 在「防火牆」標籤的「流量設定」下，按下「在防火牆啟動之前及防火牆停止之後攔截所有流量」。
如果您停用「允許初始 DHCP 和 NetBIOS 流量」，啟用網路連線的初始流量會遭到攔截。

4. 按下「確定」。

在任何時候攔截全部流量：

1. 在用戶端的側邊列中，按下「狀態」。
2. 在「防網路和主機侵入」旁，按下「選項」>「檢視網路活動」。
3. 按下「工具」>「攔截全部流量」。
4. 若要確認，請按下「是」。
5. 若要返回用戶端先前使用的防火牆設定，請取消勾選「工具」>「攔截全部流量」。

[啟用防火牆設定](#)

入侵預防的運作方式

入侵預防會自動偵測和攔截網路攻擊。在 Windows 電腦上，入侵預防還會偵測和攔截對於受支援瀏覽器的瀏覽器攻擊。入侵預防是繼防火牆之後用於保護用戶端電腦的另一層防護。入侵預防有時亦稱為入侵預防系統 (IPS)。

入侵預防會截取網路層中的資料。它使用特徵掃描封包或封包串流。透過尋找與網路攻擊或瀏覽器攻擊對應的模式，入侵預防可以個別掃描各個封包。入侵預防會偵測作業系統元件和應用程序層的攻擊。

根據預設，也會啟用下列 IPS 功能：

Table 25: IPS 功能

類型	說明
網路入侵預防	網路入侵預防使用特徵來識別用戶端電腦上的攻擊。對於已知攻擊，入侵預防會自動捨棄與特徵符合的封包。
瀏覽器入侵預防 (僅限 Windows)	瀏覽器入侵預防會監控對瀏覽器的攻擊，包括 Internet Explorer、Firefox 和 Chrome。Firefox 可能會停用 Symantec Endpoint Protection 外掛程式，但可以重新開啟它。 入侵預防使用攻擊特徵和啟發式方法來識別對瀏覽器的攻擊。 對於某些瀏覽器攻擊，入侵預防會要求用戶端終止瀏覽器。用戶端電腦上會顯示通知。 如需瀏覽器入侵防禦所保護瀏覽器的最新資訊，請參閱： 瀏覽器入侵防禦支援的瀏覽器版本
URL 信譽	URL 信譽偵測可識別來自網域和 URL 的威脅，這些網域和 URL 可以託管惡意軟體、詐騙、網路釣魚和垃圾郵件等這類惡意內容。URL 信譽會禁止存取識別為惡意內容之已知來源的網址。來自已造訪 URL 的資訊會傳送到 Broadcom 以擷取信譽等級。

請參閱：[架構入侵預防](#)

在 Windows 用戶端上架構入侵預防

Windows 適用的 Symantec Endpoint Protection 用戶端指南

依據預設，入侵預防會在您的電腦上執行。入侵預防會截取網路層中的資料。它使用特徵掃描封包或封包串流。透過尋找與網路攻擊或瀏覽器攻擊對應的模式，入侵預防可以個別掃描各個封包。入侵預防是繼防火牆之後用於保護用戶端電腦的另一層防護。入侵預防有時亦稱為入侵預防系統 (IPS)。

NOTE

入侵預防和防火牆是網路威脅防護的一部分。「網路威脅防護」和「記憶體攻擊緩和」是「防網路和主機侵入」的一部分。

若要管理入侵預防：

1. 確定已下載最新的 IPS 特徵。
依預設，會將最新特徵下載到用戶端。不過，您可能會想要立即手動下載特徵。
[使用 LiveUpdate 更新用戶端內容](#)
2. 將入侵預防保持啟用狀態。
您應該將入侵預防隨時保持在啟用狀態。會在安全日誌中記錄入侵嘗試和事件。如果管理員進行相應架構，也可以將入侵事件記錄在封包日誌中。
[檢視日誌](#)
[啟用封包日誌](#)
3. 如果您認為偵測為誤報，請通知您的管理員。

請勿將非預期的事件視為誤報。

[回應 Symantec Endpoint Protection 中可疑 IPS 誤報的最佳實務](#)

NOTE

管理員可能已經架構不提供這些選項。

啟用入侵預防

入侵預防包含兩種類型：

- 網路入侵預防
網路入侵預防使用特徵來識別用戶端電腦上的攻擊。對於已知攻擊，入侵預防會自動捨棄與特徵符合的封包。
- 瀏覽器入侵預防
瀏覽器入侵預防會監控 Internet Explorer 和 Firefox 上的攻擊。所有其他瀏覽器均不支援瀏覽器入侵預防。如需瀏覽器入侵預防所保護瀏覽器的最新資訊，請參閱：[瀏覽器入侵預防支援的瀏覽器版本](#)。

您也可以啟用或停用當用戶端偵測到網路攻擊時的通知。

若要啟用入侵預防：

1. 在用戶端的側邊列中，按下「變更設定」。
2. 在「防網路和主機侵入」旁，按下「架構設定」。
3. 在「入侵預防」標籤上，確定勾選下列選項：
 - 啟用網路入侵預防
 - 啟用瀏覽器入侵預防

您也可以將瀏覽器入侵預防架構為只記錄偵測但不攔截它們。您應該只暫時使用此組態，因為它會降低電腦的防護。例如，當您對遭攔截的流量進行疑難排解時，您會架構只記錄模式。在檢閱安全日誌以識別及排除攔截流量的特徵之後，請停用只記錄模式。
4. (選擇性) 若要啟用入侵防護通知，請確保「通知」標籤上的「顯示入侵預防和記憶體攻擊緩和通知」通知。
5. 按下「確定」。

防止攻擊易受攻擊的應用程式

Windows 適用的 Symantec Endpoint Protection 用戶端指南

記憶體攻擊緩和 (MEM) 會阻止對 Windows 電腦上所執行常用應用程式的攻擊。當用戶端偵測到侵入嘗試時，會顯示下列其中一則或兩則訊息。

- Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected
用戶端會攔截侵入，而不終止應用程式。
- Symantec Endpoint Protection will terminate your application
用戶端會終止應用程式，使其無法執行。

如果應用程式保持終止，請執行以下步驟：

1. 通知您的管理員。
2. 判斷實際侵入攻擊了應用程式，還是偵測為誤報。
 - 如果侵入攻擊了應用程式，請檢查是否存在修正版本或更新版本的受感染應用程式可修正目前弱點。當您或您的管理員安裝修正應用程式後，請在用戶端電腦上重新執行該應用程式以查看記憶體攻擊緩和是否仍會終止應用程式。
 - 如果偵測為誤報，請暫時停用記憶體攻擊緩和。請向管理員或 [賽門鐵克安全機制應變中心](#) 通知錯誤偵測。使記憶體攻擊緩和處於停用狀態，直到賽門鐵克解決問題為止。然後，重新啟用記憶體攻擊緩和。

判斷偵測是否為誤報：

1. 在安全日誌中，確認記憶體攻擊緩和確實已終止應用程式。

例如，您可能會看到下列事件：Attack: Blocked Structured Exception Handler Overwrite attack against C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe

[檢視日誌](#)

2. 停用記憶體攻擊緩和。
3. 重新執行應用程式。
 - 如果應用程式正常執行，則偵測為誤報。
 - 如果應用程式行為異常，例如開啟另一個應用程式，則偵測為檢出。

在受管用戶端上，您的管理員可能會防止您停用記憶體攻擊緩和。

停用並重新啟用記憶體攻擊緩和：

1. 在「防網路和主機侵入」旁的「狀態」頁面上，按下「選項」。
2. 在下拉式功能表中，執行下列其中一項工作：
 - 按下「停用記憶體攻擊緩和」或「啟用記憶體攻擊緩和」。
 - 按下「變更設定 > 記憶體攻擊緩和」標籤，然後勾選或取消勾選「啟用記憶體攻擊緩和」。

使用 Web 和雲端存取防護允許或攔截惡意網站

Windows 適用的 Symantec Endpoint Protection 用戶端指南

Web 和雲端存取防護 (WCAP) 透過將應用程式和網站進行分類，然後根據 WSS 政策允許或拒絕存取，來保護您的電腦。只有在管理員解除鎖定此設定或您正在執行未受管用戶端時，您才能啟用或停用 Web 和雲端存取防護。如果您因 WSS 政策架構錯誤而無法存取網頁，則您可能需要停用此功能。否則，請保持啟用 WCAP。

您無法架構 Web 和雲端存取防護；您只能啟用或停用它。

1. 在用戶端中，按下 **Web** 和雲端存取防護旁邊的「選項 > 變更設定」。
2. 勾選或取消勾選 啟用 **Web** 和雲端存取防護，然後按下「確定」。

若要檢查 Web 和雲端存取防護是否正在執行並已連線，請參閱：[驗證 Web 和雲端存取防護通道方法是否已在 Windows 用戶端上啟用和連接](#)

何謂 Web 和雲端存取防護？

Windows 適用的 Symantec Endpoint Protection 用戶端指南

Web 和雲端存取防護會將網路流量從 Symantec Endpoint Protection 用戶端重新導向至 Symantec Web Security Service，以根據 WSS 管理員所設定的政策規則來允許或攔截流量。與 Symantec Web Security Service 的安全連線可讓用戶端對所有網路通訊執行內容篩選和威脅防護。

NOTE

在 14.3 RU2 中，「網路流量重新導向」已重新命名為「Web 和雲端存取防護」。

Web 和雲端存取防護如何運作？

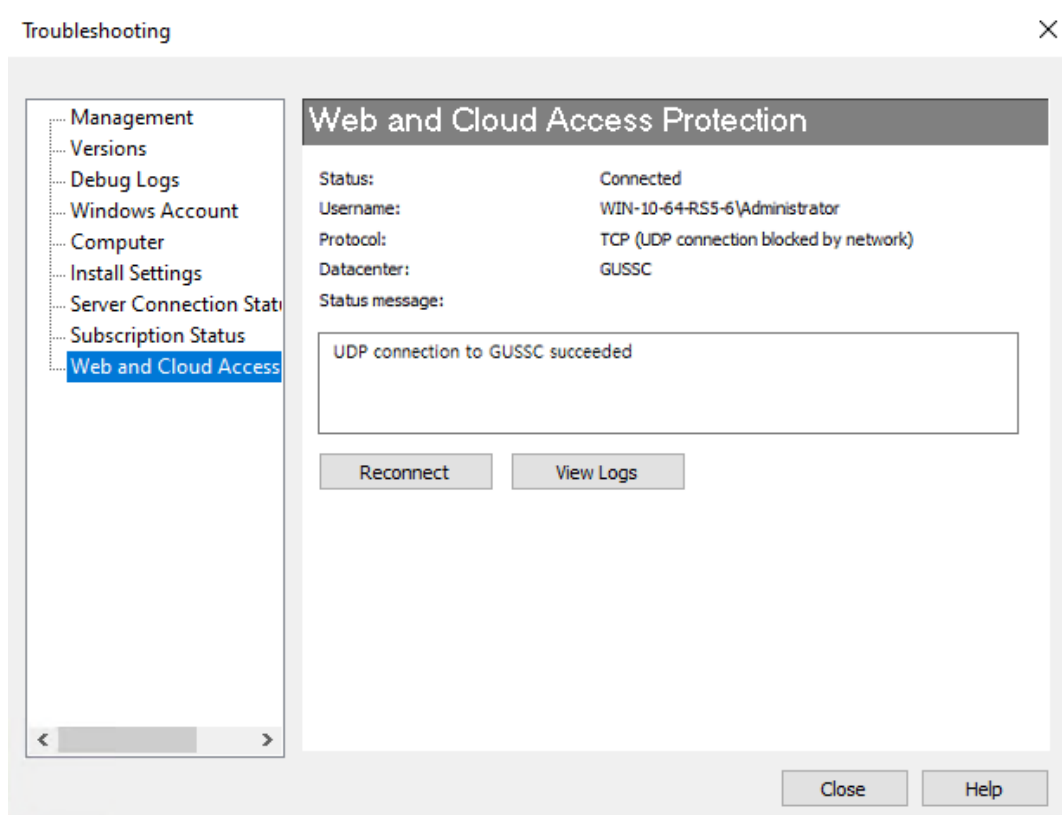
Web 和雲端存取防護使用下列重新導向方法：

- **PAC** 檔案方法只會透過代理自動架構 (PAC) 檔案將 Web 流量重新導向至 WSS。WSS 為網頁瀏覽器提供安全代理架構。只有網頁流量重新導向到 WSS。每次您使用網頁瀏覽器存取網站時，瀏覽器都會透過最近的雲端託管 WSS 傳送所有網頁瀏覽器流量，如 PAC 檔案所定義。根據預先定義的架構，Symantec WSS 代理可以允許或攔截流量。
- 通道方法透過 VPN 將所有網路流量重新導向至 WSS，以進行流量檢查。Symantec Endpoint Protection 用戶端在安裝之後，就會立即連線至 VPN，以透過 Symantec WSS 代理重新導向所有網路流量。VPN 架構為一律開啟，並且會在因電腦重新開機、睡眠或休眠而斷線時自動重新連線。此方法適用於只在 Windows 10 和更新版本的 64 位元 Intel 裝置上執行的 14.3 RU1 和更新版本的用戶端。

驗證 Web 和雲端存取防護通道方法是否已在 Windows 用戶端上啟用和連接

若要驗證 **Web** 和雲端存取防護 通道方法是否已在 **Windows** 用戶端上啟用和連接

1. 在 Symantec Endpoint Protection (SEP) 用戶端上，按一下「說明」>「疑難排解」>「**Web** 和雲端存取防護」。如果「狀態」欄位顯示「已連線」，則會啟用並連線 Web 和雲端存取防護。



如果此面板未出現，則已在用戶端上停用通道方法。

- 若您已在 WSS 入口網站上啟用了 SAML 驗證，則 SEP 用戶端會顯示一個「**Web** 和雲端存取防護 - 登入」視窗，其中包含貴公司身份供應商 (IdP) 頁面，用戶端使用者會在其中輸入其公司憑證。身份供應商 (IdP) 是儲存和管理數位身分的服務。

下列視窗是用戶端使用者所看到內容的範例。視窗的模糊部分對於使用者輸入其憑證的每個公司都是唯一的。若登入視窗凍結或空白，則用戶端使用者應按一下「重新載入」按鈕。

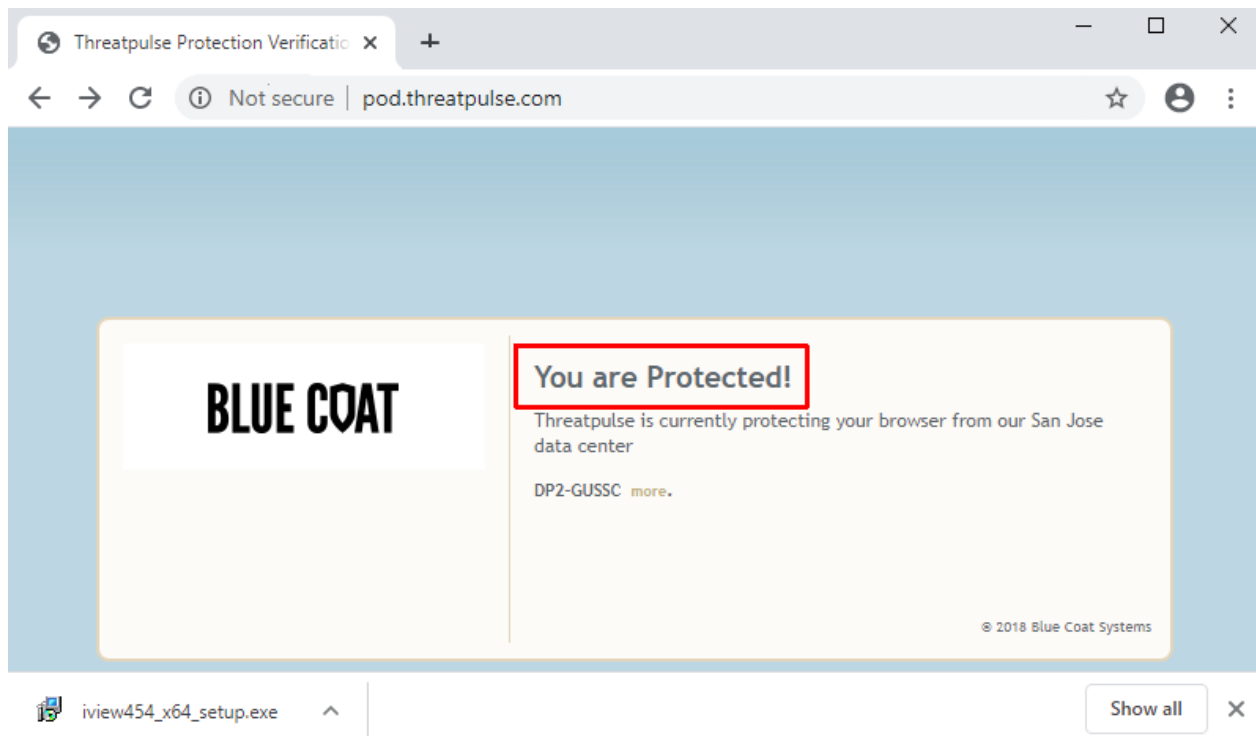


NOTE

若要正確執行 SAML 驗證方法，您必須以系統管理員身分下載並安裝 Microsoft Edge WebView2 Runtime2。下載 [Microsoft Edge Webview2 執行時間](#) 應用程式，然後以滑鼠右鍵按一下應用程式，然後按一下「以系統管理員身分執行」。若為 Windows 11 用戶端，依預設安裝 WebView2 執行時間應用程式。

如要使用主機完整性政策範本來安裝 WebView2 應用程式，請參閱：[疑難排解 Web 和雲端存取防護](#)

2. 在用戶端上，瀏覽到以下測試 URL：pod.threatpulse.com。
如果啟用，則用戶端使用者應該會看到下列訊息。



管理 Windows 用戶端

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您的電腦預設會受到防護，應該不需要架構用戶端。不過，您可能會因為下列原因而想要修改防護情況：

- 您的電腦執行的是非受管用戶端。
安裝非受管用戶端之後，只有您可以控制電腦的防護。非受管用戶端預設會受到防護，但您可能需要修改電腦的防護設定。
[關於受管用戶端和非受管用戶端](#)
[檢查用戶端是受管用戶端還是非受管用戶端](#)
- 您想啟用或停用一或多項防護技術。
[在用戶端電腦上啟用防護](#)
- 您想確認是否有最新的病毒定義檔和安全性內容。
- 您聽說最近出現新病毒或安全威脅，想要執行掃描。

Table 26: 架構用戶端的工作

步驟	說明
回應警示或通知	回應出現並要求您輸入資訊的訊息。例如，掃描可能偵測到病毒或安全風險，並且會顯示掃描結果，要求您對偵測到的病毒或安全風險採取動作。 警示和通知的類型
檢查防護狀態	定期檢查「狀態」頁面，確定所有類型的防護均啟用。 在用戶端電腦上啟用防護 用戶端狀態圖示
更新病毒定義檔及安全性內容	檢查電腦是否具有最新的病毒定義檔及安全性內容。 • 檢查是否有最新的防護更新。您可以在用戶端的「狀態」頁面，於每種防護類型底下檢查這些定義檔的日期和編號。 • 取得最新的防護更新。 使用 LiveUpdate 更新用戶端內容 在管理員允許的情況下，您可以在受管用戶端上執行這些工作。
掃描電腦	執行掃描來檢查電腦或電子郵件應用程式是否有任何病毒。用戶端預設會在您開啟它時掃描電腦，但您可以隨時掃描電腦。 立即掃描用戶端電腦
調整防護設定	在大多數情況下，預設設定即能為電腦提供足夠的防護。如有需要，您可以減少或加強下列類型的防護： • 排定額外的掃描 管理電腦上的掃描 • 新增防火牆規則 (僅適用於非受管用戶端) 管理防火牆防護
執行合規檢查	檢查電腦是否符合公司的安全政策。 透過主機完整性掃描檢查電腦安全性遵從
檢視日誌中的偵測或攻擊記錄	查看日誌來確認用戶端是否偵測到病毒或網路攻擊。 檢視日誌
更新安全性政策 (僅適用於受管用戶端)	檢查用戶端是否從管理伺服器收到最新的安全性政策。安全性政策包含適用於用戶端的最新防護技術設定。 用戶端狀態圖示 安全性政策會自動更新。然而，若要確保擁有最新政策，您可以手動加以更新。 更新用戶端政策

管理 Windows 用戶端

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您的電腦預設會受到防護，應該不需要架構用戶端。不過，您可能會因為下列原因而想要修改防護情況：

- 您的電腦執行的是非受管用戶端。
安裝非受管用戶端之後，只有您可以控制電腦的防護。非受管用戶端預設會受到防護，但您可能需要修改電腦的防護設定。
[關於受管用戶端和非受管用戶端](#)
[檢查用戶端是受管用戶端還是非受管用戶端](#)
- 您想啟用或停用一或多項防護技術。
[在用戶端電腦上啟用防護](#)
- 您想確認是否有最新的病毒定義檔和安全性內容。
- 您聽說最近出現新病毒或安全威脅，想要執行掃描。

Table 27: 架構用戶端的工作

步驟	說明
回應警示或通知	回應出現並要求您輸入資訊的訊息。例如，掃描可能偵測到病毒或安全風險，並且會顯示掃描結果，要求您對偵測到的病毒或安全風險採取動作。 警示和通知的類型
檢查防護狀態	定期檢查「狀態」頁面，確定所有類型的防護均啟用。 在用戶端電腦上啟用防護 用戶端狀態圖示
更新病毒定義檔及安全性內容	檢查電腦是否具有最新的病毒定義檔及安全性內容。 • 檢查是否有最新的防護更新。您可以在用戶端的「狀態」頁面，於每種防護類型底下檢查這些定義檔的日期和編號。 • 取得最新的防護更新。 使用 LiveUpdate 更新用戶端內容 在管理員允許的情況下，您可以在受管用戶端上執行這些工作。
掃描電腦	執行掃描來檢查電腦或電子郵件應用程式是否有任何病毒。用戶端預設會在您開啟它時掃描電腦，但您可以隨時掃描電腦。 立即掃描用戶端電腦
調整防護設定	在大多數情況下，預設設定即能為電腦提供足夠的防護。如有需要，您可以減少或加強下列類型的防護： • 排定額外的掃描 管理電腦上的掃描 • 新增防火牆規則 (僅適用於非受管用戶端) 管理防火牆防護
執行合規檢查	檢查電腦是否符合公司的安全政策。 透過主機完整性掃描檢查電腦安全性遵從
檢視日誌中的偵測或攻擊記錄	查看日誌來確認用戶端是否偵測到病毒或網路攻擊。 檢視日誌
更新安全性政策 (僅適用於受管用戶端)	檢查用戶端是否從管理伺服器收到最新的安全性政策。安全性政策包含適用於用戶端的最新防護技術設定。 用戶端狀態圖示 安全性政策會自動更新。然而，若要確保擁有最新政策，您可以手動加以更新。 更新用戶端政策

瞭解 Symantec Endpoint Protection 用戶端狀態頁面

Windows 適用的 Symantec Endpoint Protection 用戶端指南

開啟 用戶端時，「狀態」頁面最上方會顯示各種警示圖示來表示電腦的防護狀態。如果您必須採取進一步的動作，則與圖示一起顯示的文字會提供更多資訊。

Table 28: 狀態頁面圖示

圖示	說明
	顯示每種防護均啟用。
	警告您用戶端電腦上的病毒定義檔或安全性內容已過期。若要接收最新的病毒定義檔或安全性內容，您可以在管理員允許的情況下立即執行 LiveUpdate。 此狀態可能也指示 需要重新啟動。 具有作用中主機完整性政策的 用戶端電腦也可能具有下列問題： - 用戶端電腦未通過「主機完整性」安全性合規檢查。若要找出通過檢查所需的項目，請查看「用戶端管理安全」日誌。 - 用戶端電腦無法下載主機完整性內容。 使用 LiveUpdate 更新用戶端內容
	顯示一或多項防護停用，或用戶端的授權已過期。若要啟用防護，請按下「修正」或「全部修正」。 在用戶端電腦上啟用防護

請參閱：[用戶端狀態圖示](#)

隱藏和顯示 用戶端上的通知區域圖示

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以視需要隱藏 通知區域圖示 (亦稱為系統匣圖示)。例如，如果在 Windows 工作列上需要更多空間時，可以將它隱藏。

[用戶端狀態圖示](#)

若要隱藏或顯示用戶端上的通知區域圖示：

NOTE

在受管用戶端上，如果您的管理員限制使用此功能，您便無法隱藏通知區域圖示。

1. 在用戶端中，按下「變更設定」。
2. 在「變更設定」頁面上，按下「用戶端管理」旁的「架構設定」。
3. 在「用戶端管理設定」對話方塊「一般」標籤下的「顯示選項」中，取消勾選或勾選「在通知區域中顯示賽門鐵克安全性圖示」。
4. 按下「確定」。

若要隱藏或顯示群組中所有用戶端上的通知區域圖示：

NOTE

您必須以管理員身分登入，才能執行這些步驟。這些設定會隱藏或顯示通知區域圖示，並防止使用者進行變更。

1. 按下「用戶端」。
2. 按下您要隱藏或顯示通知區域圖示的群組，然後按下「政策 > 位置限定的設定」。
3. 在「用戶端使用者介面控制設定」旁，按下「工作 > 編輯設定」。
4. 在「伺服器控制」旁，按下「自訂」。
5. 在「一般」下方，按下以啟用或停用「顯示通知區域圖示」選項，然後按下「確定」。
6. 按下「確定」。

NOTE

如果群組已架構為使用「混合控制」，請依照先前程序執行，然後按下「混合控制 > 自訂」。在「顯示/隱藏通知區域圖示」旁，按下「伺服器」。

關於受管用戶端和非受管用戶端

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您的管理員可以將用戶端安裝成受管用戶端 (由管理員管理的版本) 或非受管用戶端 (單機版)。

Table 29: 受管用戶端與非受管用戶端之間的差別

用戶端類型	說明
受管用戶端	受管用戶端會與網路中的管理伺服器通訊。管理員會架構防護和預設設定。管理伺服器會通知用戶端，並且用戶端會下載設定。根據管理伺服器的通訊設定，如果管理員對防護進行變更，則用戶端將立即下載此變更。 管理員可利用下列方式變更您與用戶端互動的程度： • 管理員完全管理用戶端。您不需要架構用戶端。所有設定均會鎖定或無法使用，但您可以檢視用戶端在電腦上所執行動作的相關資訊。 • 管理員負責管理用戶端，但您可以變更部分用戶端設定和執行某些工作。例如，您可以執行自己的掃描，以及手動擷取用戶端更新和防護更新。 • 管理員負責管理用戶端，但您可以變更所有用戶端設定和執行所有防護工作。 用戶端設定和設定值的可用性會定期變更。例如，如果管理員更新控制用戶端防護的政策，則設定可能會變更。
非受管用戶端	非受管用戶端不會與管理伺服器通訊，管理員也不會管理該用戶端。 非受管用戶端可能是下列類型之一： • 未連接至網路的單機型電腦，例如家用電腦或筆記型電腦。該電腦會使用預設選項設定或管理員預設的設定來安裝用戶端。 • 連線至公司網路之前即符合安全性需求的遠端電腦。然而，非受管用戶端不支援主機完整性。 用戶端在初次安裝時即具有預設設定。在安裝用戶端之後，您可以變更所有用戶端設定以及執行所有防護工作。

下表說明受管用戶端與非受管用戶端使用者介面之間的差別。

Table 30: 受管用戶端與非受管用戶端在功能區上的差別

功能區	集中受管用戶端	非受管用戶端
病毒和間諜軟體防護	用戶端會顯示上鎖的掛鎖圖示，而且無法架構的選項會變成灰色。	用戶端既不會顯示上鎖的掛鎖，也不會顯示未上鎖的掛鎖。
主動型威脅防護	用戶端會顯示上鎖的掛鎖圖示，而且無法架構的選項會變成灰色。	用戶端既不會顯示上鎖的掛鎖，也不會顯示未上鎖的掛鎖。
用戶端管理和防網路和主機侵入設定	管理員控制的設定不會出現。	所有設定均會出現。

檢查用戶端是受管用戶端還是非受管用戶端

Windows 適用的 Symantec Endpoint Protection 用戶端指南

若要檢查您擁有多少控制權來架構用戶端上的防護，首先必須檢查用戶端是受管或未受管用戶端。在非受管用戶端上，可架構的設定比受管用戶端多。

關於受管用戶端和非受管用戶端

若要檢查用戶端是受管用戶端還是非受管用戶端：

1. 在「狀態」頁面上，按下「說明 > 疑難排解」。
2. 在「疑難排解」對話方塊中按下「管理」。
3. 在「管理」面板的「一般資訊」之下，查看「伺服器」旁的下列資訊：
 - 如果用戶端為受管用戶端，「伺服器」欄位會顯示管理伺服器的位址或「離線」文字。
位址可能是 IP 位址、DNS 名稱或 NetBIOS 名稱。例如，DNS 名稱可能是 SEPMServer1。如果用戶端為受管用戶端，但目前未連線至管理伺服器，此欄位會顯示「離線」。
 - 如果用戶端為非受管用戶端，「伺服器」欄位會顯示「自我管理」。
4. 按下「關閉」。

針對 防護問題進行疑難排解

您應一律啟用 防護技術。

WARNING

如果您暫時停用防護，請重新啟用防護以確保電腦仍然受到保護。

您還可以執行 Symantec Diagnostic Tool 來幫助解決問題。請參閱：[使用 SymDiag 進行 Windows 用戶端健康狀態疑難排解和檢查](#)

下表列出了啟用防護時可能遇到的問題。首先向您的系統管理員諮詢可能發生問題的原因和解決方案。

防護類型	
自動防護	安裝應用程式時出現問題。 自動防護可能會導致以下問題： • 自動防護可能會阻止您開啟文件。例如，如果開啟包含巨集的 Microsoft Word， • 「自動防護」會警告您有疑似病毒活動，但是您知道此活動並非病毒所造成的。 • 「自動防護」可能干擾 Windows 驅動程式更換。 • 「自動防護」可能會減緩用戶端電腦的速度。 如果自動防護導致應用程式出現問題，則最好建立一個例外而不是停用防護，即使 啟用自動防護 排除掃描項目
主動型威脅防護	您可能會因為下列原因停用「主動型威脅防護」： • 出現太多誤認為是威脅的警告。 • 用戶端電腦的速度可能會減緩。
防網路和主機侵入	「防網路和主機侵入」可能會導致以下問題： • 您安裝了可能導致防火牆加以攔截的應用程式。 • 防火牆規則或防火牆設定，因管理員的疏失攔截了某應用程式。 • 防火牆或入侵預防系統會導致與網路連接相關的問題。 • • 您會無法開啟應用程式。 • 應用程式意外終止。 防止攻擊易受攻擊的應用程式 如果不確定「防網路和主機侵入」是否會導致發生問題，則可能需要停用所有防護 在受管用戶端上，您的管理員可能會完全鎖定「防網路和主機侵入」，這樣您就無 • 用戶端允許所有流量或只允許所有離埠流量。 • 停用防護的時間長度。 • 在重新啟動用戶端之前，可以停用防護的次數。 在用戶端電腦上啟用防護
竄改防護	通常，您應當保持啟用「竄改防護」。 若是您得到許多誤報偵測，可考慮暫時停用「竄改防護」。例如，有些第三方應用 啟用竄改防護

在用戶端電腦上啟用防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您應將電腦上所有類型的防護始終保持啟用狀態，尤其是「自動防護」。

在用戶端上，任何防護停用時：

- 「狀態」頁面最上方的狀態列會是紅色的。
- 用戶端圖示會出現常見的禁止符號，即中間有斜線的紅圈。用戶端圖示會在 Windows 桌面右下角的工作列中顯示為完整的盾牌。在某些架構中，圖示不會出現。

用戶端狀態圖示

若為受管用戶端，管理員可以隨時啟用或停用防護技術。如果您停用某個防護，管理員稍後可以再次啟用該防護。管理員也可以鎖定某個防護，讓您無法停用它

從狀態頁面啟用防護技術	在用戶端「狀態」頁面最上方，按下「修正」或「全部修正」。
從工作列啟用防護技術	在 Windows 桌上型電腦的通知區域中，以滑鼠右鍵按一下用戶端圖示，然後按一下「啟用 Symantec Endpoint Protection 」。
從用戶端內部啟用防護技術	在用戶端的「狀態」頁面上，按一下防護類型旁邊的「選項」>「啟用 <防護類型>」。
啟用防火牆	1. 在用戶端「狀態」頁面最上方的「防網路和主機侵入」旁邊，按下「選項」>「變更設定」。 2. 在「防火牆」標籤上，勾選「啟用防火牆」。 3. 按下「確定」。

關於 Windows 用戶端的日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

日誌包含了用戶端架構變更、安全性相關活動及錯誤的相關資訊，這些記錄稱為事件。

安全性相關活動包括病毒偵測、電腦狀態，以及進出電腦流量的相關資訊。如果您使用的是受管用戶端，其日誌可以定期上傳至管理伺服器。管理員可以使用日誌的資料，來分析網路的整體安全性狀態。

日誌很重要，可以追蹤電腦活動，以及電腦與其他電腦和網路互動的情形。您可以使用日誌中的資訊來追蹤電腦上病毒、安全風險及攻擊方面的趨勢。

如需日誌的詳細資訊，可按下 F1，檢視該日誌的說明。

Table 31: 用戶端日誌

日誌	說明
控制日誌	包含應用程式存取的 Windows 登錄機碼、檔案和 DLL，以及您電腦所執行應用程式的相關資訊。
除錯日誌	包含用於疑難排解之用戶端、掃描及防火牆的相關資訊。管理員可能會要求您啟用或架構日誌，然後匯出。
Web 和雲端存取防護日誌	包含 Symantec Web Security Service (WSS) (若已啟動) 的診斷資訊。
封包日誌	包含透過電腦通訊埠進出的資料封包相關資訊。 封包日誌預設為停用。在受管用戶端上，除非管理員允許，否則您無法啟用封包日誌。若為非受管用戶端，則您可以啟用封包日誌。 啟用封包日誌
風險日誌	包含已感染電腦之病毒及安全風險 (如廣告軟體和間諜軟體) 的相關項目。安全風險包含可連至賽門鐵克安全機制應變中心網頁的連結，該網頁可提供其他資訊。
掃描日誌	包含某段時間內，已在您電腦上執行的掃描相關項目。
安全日誌	包含可能對您的電腦產生威脅的活動之相關資訊。例如，可能會顯示有關服務阻斷攻擊、通訊埠掃描及可執行檔變更等活動的資訊。 安全日誌也會顯示主機完整性檢查的結果。

日誌	說明
系統日誌	- 病毒和間諜軟體防護：包含電腦上與病毒及安全風險相關的系統活動資訊。這項資訊包含架構變更、錯誤及定義檔資訊。 - 主動型威脅防護：包含電腦上與行為分析 (SONAR) 相關的系統活動資訊。 - 用戶端管理：包含電腦上發生之一切作業變更的相關資訊。 變更可能包含下列活動： - 服務啟動或停止 - 電腦偵測網路應用程式 - 已架構軟體
竄改防護日誌	包含嘗試竄改您電腦上賽門鐵克應用程式的事件相關項目。這些項目包含「竄改防護」偵測到或偵測到並阻擋的嘗試事件相關資訊。
威脅日誌	包含行為分析 (SONAR) 在電腦上執行應用程式時偵測到潛在惡意行為的威脅相關資訊。SONAR 會偵測任何可疑行為的檔案。行為分析也會偵測系統變更。
流量日誌	包含防火牆流量和入侵預防攻擊的相關事件，日誌包含電腦透過網路進行之連線的相關資訊。 在啟用風險追蹤程式的情況下，防網路和主機侵入日誌有助於回溯檢查威脅活動的來源，並排除可能的網路攻擊。這些日誌可讓您瞭解您的電腦何時遭到攔截而無法連至網路，並可協助您判斷存取遭攔截的原因。 如需詳細資訊，請參閱什麼是風險追蹤程式？

檢視日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以檢視電腦上的日誌，查看已發生事件的詳細資料。

若要檢視日誌：

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 按下「檢視日誌」按鈕，並在下拉式功能表中選擇您要檢視的日誌。

根據您的安裝，一些防護技術可能不會顯示。

啟用封包日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

除了封包日誌以外，所有防網路和主機侵入日誌及用戶端管理日誌都預設為啟用。若為非受管用戶端，您可以啟用和停用封包日誌。

若為受管用戶端，管理員可能會讓您啟用或停用封包日誌。

關於日誌

若要啟用封包日誌：

1. 在用戶端之「狀態」頁面的「防網路和主機侵入」旁，按下「選項」，再按下「變更設定」。
2. 按下「日誌」。
3. 勾選「啟用封包日誌」。
4. 按下「確定」。

對話方塊說明

對話方塊上設定的參考資訊。

使用本節瀏覽 Symantec Endpoint Protection Windows 用戶端對話方塊的所有說明主題。

病毒和間諜軟體防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

本節包括「變更設定 > 病毒和間諜軟體防護」頁面之對話方塊的說明。

病毒和間諜軟體防護設定：自動防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「自動防護」可即時防護您電腦上的檔案。每當您存取、複製、儲存、移動、開啟或關閉檔案時，「自動防護」都會加以掃描，以確保沒有存在病毒或安全風險。「自動防護」是保護資料不受到感染的有效方式。

在受管用戶端上，管理員可能會鎖定部分設定。

NOTE

若要將檔案或資料夾排除在掃描範圍之外，請使用例外。

Table 32: 自動防護檔案系統選項

選項	說明
啟用檔案系統自動防護	您可以啟用或停用檔案防護的「自動防護」功能。 如果您停用「自動防護」，則也會變更下列防護： 「下載鑑識」即使已啟用，也無法運作。 - 行為分析 (SONAR) 未偵測到啟發式威脅，並顯示未正常運作 (14.3 RU4 或更早版本)。但是，系統變更或主機檔案變更的偵測會繼續執行。
檔案類型	指定「自動防護」應掃描所有檔案類型，或是只掃描所選取的副檔名。 Note: 「下載智慧型掃描」也會使用這些設定。 檔案類型包括下列選項： - 所有類型：不分類型，掃描電腦上的所有檔案。 - 已選取：若只要掃描特定副檔名的檔案，請選取此選項。 - 副檔名：指定掃描範圍內只應包含特定副檔名。如果程式及文件所使用的副檔名不在清單中，您可以將它們加入。僅掃描您指定的副檔名。不會掃描副檔名不在清單中的檔案。 如果要從掃描中排除檔案或資料夾，您可以建立例外。例外會套用到所有執行的掃描。 - 檢查檔案內容來判斷檔案類型：掃描特定的可架構副檔名群組，包含可執行的程式碼和所有的 .exe 與 .doc 檔。用戶端會讀取每個檔案的標頭來判斷其檔案類型。即使病毒變更了 .exe 和 .doc 檔案的副檔名，它仍可掃描這些檔案。
動作	架構「自動防護」偵測到病毒和安全風險時要採取的動作。
通知	指定「自動防護」在偵測到病毒或安全風險時是否應顯示訊息。同時指定訊息的內容。
進階	設定進階掃描選項 (例如開機及備份選項)，以及檔案快取和「風險追蹤程式」選項。

選項	說明
選項	選項包括下列： - 掃描安全風險 您可以停用此選項，讓「自動防護」停止掃描安全風險。 - 掃描遠端電腦上的檔案 對遠端電腦上的檔案啟用或停用「自動防護」掃描。預設情況下，只有在檔案執行時，「自動防護」才會掃描這些檔案。 - 只在執行檔案時 停用此選項可對遠端電腦上的全部檔案執行「自動防護」。不過，如果停用此選項，可能會影響客戶端電腦的效能。

病毒和間諜軟體防護設定：Outlook 自動防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「自動防護」可以掃描 Microsoft Outlook 電子郵件的附件。

在受管用戶端上，管理員可能會鎖定部分設定。

Table 33: Microsoft Outlook 的自動防護選項

選項	說明
啟用 Microsoft Outlook 自動防護	啟用或停用 Microsoft Outlook 電子郵件附件的「自動防護」。
檔案類型	指定「自動防護」應掃描所有檔案類型，或是只掃描所選取的副檔名。 檔案類型包括下列選項： - 所有類型：不分類型，掃描電腦上的所有檔案。 - 已選取：若只要掃描特定副檔名的檔案，請選取此選項。 - 副檔名：指定掃描範圍內只應包含特定副檔名。如果程式及文件所使用的副檔名不在清單中，您可以將它們加入。僅掃描您指定的副檔名。不會掃描副檔名不在清單中的檔案。
動作	架構「自動防護」偵測到病毒和安全風險時要採取的動作。
通知	指定「自動防護」在偵測到病毒或安全風險時是否應顯示訊息。同時指定訊息的內容。
進階	設定進階掃描選項，例如壓縮及連線設定等。
電子郵件訊息	您可以架構下列類型的電子郵件訊息： - 插入警告至電子郵件訊息：在受感染的郵件中加入電子郵件警告。您可以變更預設文字。 - 傳送電子郵件給寄件者：通知受感染郵件的寄件者。您可以變更訊息的預設文字。 - 傳送電子郵件給其他人：通知受感染郵件的任何指定電子郵件地址。您可以變更訊息的預設文字。

病毒和間諜軟體防護設定：下載智慧型掃描

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以啟用或停用「下載鑑識」，並變更「下載鑑識」對潛在惡意檔案的敏感程度。使用這些設定可控制誤報偵測率。

在受管用戶端上，管理員可能會鎖定部分設定。

Table 34: 下載鑑識設定

選項	說明
啟用下載智慧型掃描根據檔案信譽偵測潛在風險	啟用或停用「下載鑑識」。當您嘗試透過瀏覽器或簡訊用戶端下載檔案時，「下載智慧型掃描」會偵測惡意檔案或可能具有惡意的檔案。 Note: 「下載鑑識」需要使用「自動防護」。如果停用「自動防護」但啟用「下載智慧型掃描」，則「下載智慧型掃描」無法運作。在狀態頁面上，狀態詳細資料指示「下載鑑識」未正常運作。
指定下載防護等級	設定「下載鑑識」偵測惡意檔案的靈敏度。您可能想要調整滑桿以變更總偵測數和偵測誤報數。 Note: 如果您或管理員只安裝了基本病毒和間諜軟體防護，「下載鑑識」將一律採用靈敏度等級 1。您無法變更設定。 「下載鑑識」根據有關檔案信譽的相關證據，決定下載的檔案是否存在風險。賽門鐵克會收集檔案的相關資訊以確定其信譽，並提供這些資訊給「下載智慧型掃描」。滑桿指示從最可能是惡意檔案到最不可能是惡意檔案的信譽範圍。 您可以調整此滑桿，以變更將檔案視為惡意檔案或未證明的檔案的信譽等級。 設定的靈敏度等級越高，「下載鑑識」偵測到的惡意檔案越多，並且視為未證明的檔案越少。等級越高，「下載鑑識」傳回的偵測誤報越多。僅允許具有最佳信譽的檔案。 靈敏度等級越低，「下載智慧型掃描」偵測到的惡意檔案越少，傳回的偵測誤報越少，但是，視為未證明的檔案則會變多。 Note: 移動滑桿以檢視各等級的敘述。各等級的敘述提供了相應等級允許或攔截檔案的方式及其潛在誤報率的相關資訊。 按一下「動作」以設定「下載智慧型掃描」對惡意檔案或未證明檔案執行的作業。
同時根據賽門鐵克社群中的使用情況偵測惡意檔案	為信譽高於所架構靈敏度設定的已下載檔案設定附加需求。如果檔案滿足附加需求，系統會將其視為未證明、但已偵測為惡意檔案。 使用附加需求，「下載鑑識」可以將賽門鐵克社群中的檔案使用量考慮在內。越少使用者的檔案越可能有害。同時，在賽門鐵克社群中最近出現的檔案也越可能有害。 可用選項如下： • 少於以下數目的檔案 指定使用檔案的最高使用者人數。用戶端會偵測使用者人數少於指定使用者人數的所有已下載檔案。 • 使用者已知少於以下數目的檔案 指定檔案在賽門鐵克社群內已知的最大天數。用戶端會偵測賽門鐵克已知時間短於指定天數的任何已下載檔案。
自動信任從內部網路網站下載的任何檔案	預設情況下，「下載智慧型掃描」不會檢查您從受信任的 Internet 或內部網路網站下載的任何檔案。您可以在 Windows「控制台 > 網際網路選項 > 安全性」標籤上，架構信任的網站和信任的本機內部網路網站。 啟用此選項後，將允許使用者從其中一個受信任網站下載的任何檔案。檔案下載後，如有必要，可由其他防護功能對該檔案進行偵測並執行動作。 會在使用者登入時及每四個小時檢查「網際網路選項」信任網站清單的更新。當您在停用「自動信任從內部網路網站下載的任何檔案」後又重新啟用時，它也會檢查清單的更新。 此外，您也可以針對特定 Web 網域建立例外。 「下載鑑識」只識別明確架構的信任網站。允許使用萬用字元，但不支援無法路由的 IP 位址範圍。例如，「下載鑑識」不會將 10.*.* 識別為信任網站。此外，「下載鑑識」不支援「網際網路選項」>「安全性」>「自動偵測內部網路」選項所搜尋到的網站，

病毒和間諜軟體防護設定：全域設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構用戶端的全域病毒和間諜軟體選項。

在受管用戶端上，管理員可能會鎖定部分設定。

Table 35: 全域設定

選項	說明
掃描選項	您可以架構要套用於手動掃描和「自動防護」的下列選項： - 針對以下項目啟用 Insight 使用智慧型掃描功能，掃描可以略過經過數位簽章的檔案和受信任檔案。您可以架構智慧型掃描在使用信譽資料略過檔案時，所使用的信任層級。如果選取「賽門鐵克和社群信任的檔案」，掃描會略過較多的檔案 (較不安全)。如果選取「賽門鐵克信任的檔案」，掃描會略過較少的檔案 (較安全)。 當掃描略過檔案時，掃描效能可能會有改善。 - 啟用 Bloodhound 啟發式病毒偵測 Bloodhound 會隔離並找出檔案的邏輯區域，偵測出大多數未知病毒。此外，用戶端會監控您電腦上的活動，查看是否有病毒經常執行的行為，來偵測未知的病毒。偵測到可疑的活動時，用戶端會防止這個動作繼續進行。 您可以設定 Bloodhound 的靈敏度等級。 「自動」是預設等級，使用進階啟發式進行偵測。如果啟用了偵測傳送，此等級還會使用一些實驗啟發式。 「主動」可提高自動「Bloodhound 偵測」的靈敏度。如果選取此層級很可能會看到更多的誤報偵測。此選項僅建議進階使用者使用。 - 例外 按一下「檢視清單」，即可檢視您為掃描建立的所有例外。
日誌存留	指定用戶端日誌中的項目在經過多久的時間之後刪除 這個選項不會影響任何傳送至管理主控台的日誌事件。請使用此參數來減少您電腦上的日誌大小。
網際網路瀏覽器防護	指定當安全風險劫取您電腦的首頁時，要用來作為首頁的 URL 用戶端會在修復風險時使用此 URL。

掃描通知選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構「自動防護」或使用者定義掃描的通知及矯正選項。

若是受管用戶端，您的管理員可能會鎖定部分設定。

NOTE

矯正選項僅適用於檔案系統的自動防護掃描。

Table 36: 通知及矯正選項

選項	說明
偵測選項	可用選項如下： - 在偵測出風險時顯示通知訊息 啟用或停用當「自動防護」或使用者定義的掃描發現病毒或安全風險時，在受感染電腦上顯示通知。您可以修改要顯示在通知中的資訊類型。您可以使用預設的文字，也可以刪除文字並輸入自己的文字。如果在文字方塊中按下滑鼠右鍵，則您可以將變數欄位插入至通知文字中。在通知內文，相關文字會自動取代變數欄位。 訊息變數顯示預設訊息變數以及您可以新增的變數。 - 顯示自動防護結果對話方塊 啟用或停用在受感染的電腦上顯示結果。此選項僅適用於檔案系統的「自動防護」。
矯正選項	這些選項僅適用於檔案系統的自動防護。用戶端可能需要終止程序或停止服務，才能移除或修復風險。 可用選項如下： - 自動終止程序 如果您啟用這個選項，用戶端會自動終止程序。如果您停用這個選項，會在對程序採取動作之前先提示您。 - 自動停止服務 如果您啟用這個選項，用戶端會自動停止服務。如果您停用這個選項，用戶端會在對服務採取動作之前先提示您。 Note: 必須重新啟動時，一定會通知您。然後您便可以儲存資料並關閉開啟的應用程式，或選擇不要重新啟動。

Table 37: 訊息變數

欄位	說明
記錄者	偵測病毒或安全風險的掃描類型。
事件	事件的類型，例如「發現風險」。
安全風險名稱	發現的病毒或安全風險名稱。
路徑及檔名	感染病毒或安全風險之檔案的完整路徑及名稱。
位置	病毒或安全風險所在的電腦磁碟機。
電腦	病毒或安全風險所在的電腦名稱。
使用者	出現病毒或安全風險時登入的使用者名稱。
已執行的操作	回應偵測到病毒或安全風險後所採取的動作。此動作可為架構的第一或第二個動作。
發現日期	發現病毒或安全風險的日期。
狀態	檔案的狀態：「受感染」、「未受感染」或「已刪除」。
檔案名稱	受病毒或安全風險感染的檔案名稱。
儲存裝置名稱	應用程式的受感染區域，例如，「檔案系統自動防護」。
動作說明	偵測到病毒或安全風險後所採取回應動作的完整敘述。

下載智慧型掃描動作

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以指定「下載智慧型掃描」對偵測到惡意檔案和未證明的檔案的回應方式。您可以調整靈敏度滑桿，變更「下載智慧型掃描」用於判斷檔案為惡意或未證明檔案的檔案信譽層級。

在受管用戶端上，管理員可能會鎖定部分設定。

Table 38: 下載智慧型掃描動作

選項	說明
惡意檔案	根據防護等級滑桿設定，架構「下載智慧型掃描」對偵測到的項目執行的動作。您可以架構第一個要採取的動作，以及第一個動作失敗時所要採取的第二個動作。 「如果第一個動作失敗」的可用選項是根據「第一個動作」目前選項。 您可以指定下列動作： • 隔離風險：嘗試在偵測到檔案時，將檔案移到用戶端電腦上的「隔離所」。如果通知已啟用，您可以選擇允許這個檔案。如果選擇允許這個檔案，則您可以執行 Internet 暫存資料夾中的檔案。在將某個檔案移至「隔離所」之後，您將無法執行這個檔案。不過，您可以對「隔離所」中的檔案執行其他動作。 • 「刪除風險」：嘗試刪除檔案。檔案會永久刪除，且無法復原。 如果「下載智慧型掃描」無法刪除這個檔案，所採取動作動作的詳細資訊會顯示在系統日誌中。 • 略過 (只記錄)：允許存取檔案並記錄事件。
未證明的檔案	架構「下載智慧型掃描」在偵測到未證明的檔案時採取的動作。 對未證明的檔案採取的動作與對惡意檔案採取的動作相同 (「隔離風險」、「刪除風險」、「略過 (只記錄)」)，同時還有下列兩個其他可行動作： • 提示 提示使用者允許或攔截已下載檔案。 • 略過 允許用戶端電腦上的檔案。

下載鑑識通知選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構「下載防護」的通知選項。通知包括有關偵測到的安全風險的資訊。

在受管用戶端上，管理員可能會鎖定此設定。

Table 39: 下載智慧型掃描通知選項

選項	說明
在受感染的電腦上顯示通知訊息	啟用或停用當「下載智慧型掃描」進行偵測時在受感染電腦上顯示通知訊息。 啟用此選項時，可以修改當您允許「下載智慧型掃描」偵測到的檔案時所顯示的預設訊息。

提早啟動防惡意軟體

Windows 適用的 Symantec Endpoint Protection 用戶端指南

提供的提早啟動防惡意軟體 (ELAM) 驅動程式可搭配 Microsoft ELAM 驅動程式使用，以便在電腦啟動時以及第三方驅動程式初始化之前，保護您網路中的電腦。Microsoft Windows 8 和 Windows Server 2012 支援這些設定。

Table 40: 提早啟動防惡意軟體選項

選項	說明
啟用賽門鐵克提早啟動防惡意軟體檢查	啟用 提早啟動防惡意軟體 (ELAM) 驅動程式。 如果啟用此選項，只有在啟用 Windows ELAM 驅動程式時，這些設定才會生效。
偵測到潛在的惡意驅動程式	您可以選擇下列任一選項： - 將偵測記錄為不明，以便 Windows 允許載入驅動程式 這個「只記錄」選項會架構 提早啟動防惡意軟體驅動程式，以便將惡意驅動程式或惡意的重要驅動程式報告為 Windows 未知的驅動程式。會將偵測結果記錄為惡意驅動程式或惡意的重要驅動程式，然後 Windows 會針對未知的驅動程式執行其政策中的動作。依據預設，Windows 允許載入未知的驅動程式。如果得到攔截重要驅動程式的誤報偵測，您可以選取這個選項。 - 使用預設 Windows 動作進行偵測 您可以使用 Windows 群組原則編輯器檢視及修改 Windows ELAM 設定。如需詳細資訊，請參閱 Windows 說明文件。

自動防護進階選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構檔案系統「自動防護」掃描的進階選項。

在受管用戶端上，管理員可能會鎖定部分設定。

Table 41: 檔案系統自動防護的進階選項

選項	說明
需要自動防護重新載入的變更	指定應該重新載入「自動防護」的時間 可用選項如下： - 等候電腦重新啟動 在電腦重新啟動時，停止並重新載入「自動防護」。 - 停止並重新載入「自動防護」 立即停止並重新載入「自動防護」。
掃描檔案的時機	可用選項如下： - 存取或修改檔案時掃描 在寫入、開啟、移動、複製或執行檔案時進行掃描。您可以使用此選項進行更完整的檔案系統防護。「自動防護」會在所有類型的作業期間掃描檔案，因此這個選項可能會影響效能。 - 修改檔案時掃描 在寫入、修改或複製檔案時進行掃描。使用此選項，效能會稍微快一點。 - 備份檔案時掃描 在進行備份時，如果有另一個程序嘗試在備份期間寫入檔案，就會掃描該檔案。備份程序在備份期間只會讀取檔案，因此備份程序本身不會起始掃描。 如果停用此選項，則自動防護在備份期間不會掃描任何檔案。不過，無論此設定為何，自動防護都會掃描從備份還原的檔案。 - 當信任的程序存取檔案時，不掃描檔案 略過由「Windows 搜尋」索引器及其他安全程序存取的檔案。

選項	說明
其他選項	可用選項如下： - 一律刪除新建立的受感染檔案 啟用此選項可刪除受感染的新檔案，無論其針對風險類型所架構的動作為何。此設定不會套用至包含病毒之現有檔案的「自動防護」偵測項目。除非所架構的動作為「刪除」，否則自動防護不會刪除已存在於用戶端電腦上的受感染檔案。 - 一律刪除新建立的受感染安全風險 此選項僅於啟用 [一律刪除新建立的受感染檔案] 時可用。啟用此選項可刪除包含安全風險的新建立檔案，無論其針對風險類型所架構的動作為何。此設定不會套用至任何包含安全風險之現有檔案的「自動防護」偵測項目。除非所架構的動作為「刪除」，否則自動防護不會刪除已存在於用戶端電腦上的任何安全風險。
檔案快取	可用選項如下： - 啟用檔案快取 檔案快取會減少自動防護記憶體的使用量，並且有助於提升自動防護掃描的效能。您可能會想停用檔案快取，以針對問題進行疑難排解。 - 載入新的定義檔時重新掃描快取 當新的定義到達用戶端電腦時，重新掃描檔案快取。您可以停用此選項來提高電腦效能。
風險追蹤程式	可用選項如下： - 啟用風險追蹤程式 啟用或停用識別攻擊 IP 位址。風險追蹤程式會識別 IP 位址，但不會將其攔截。 - 解析來源電腦 IP 位址 如果啟用此選項，「自動防護」只會尋找並記錄電腦的 NetBIOS 名稱。「自動防護」也會報告傳送時登入電腦的使用者。 - 輪詢網路階段作業間隔 啟用或停用輪詢網路階段作業。
自動啟用	指定是否要在特定的分鐘數之後重新啟用「自動防護」 可用選項如下： 「自動防護」停用時，多久之後啟用： 如果停用了「自動防護」，在指定的分鐘數之後再啟用。如果您偶爾想要停用「自動防護」，此選項很有用。時間範圍的有效值為 3 分鐘到 60 分鐘。
備份選項	可用選項如下： 先備份檔案再嘗試修復 為了資料安全起見，嘗試修復檔案前，應先啟用此選項。原始受病毒感染的檔案會加密，然後複製到「隔離所」資料夾。您可以使用這個未修復的備份檔案，讓檔案回到原始受感染的狀態。 Note: 取消勾選此選項時請小心，因為這表示在嘗試修復之前，不會備份含有病毒的檔案。 此設定僅適用於已受病毒感染的檔案。無論此設定為何，用戶端一律會備份其隔離與修復的檔案。
其他進階選項	以下是可用的命令選項： - 磁片：架構掃描磁片的選項。 - 網路：架構網路掃描設定。

磁片設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

首次存取磁片時，您可以監控磁片上是否有開機記錄型病毒。最安全的設定是清除受感染磁片上的病毒。

在受管用戶端上，管理員可能會鎖定這些設定。

Table 42: 檢查磁片的設定

選項	說明
磁片設定	可用選項如下： - 存取磁片時，檢查磁片是否有開機病毒：在存取磁片的資料時，啟用或停用磁片掃描。 - 找到開機病毒時：當自動防護發現開機型病毒時，選取清除開機記錄的病毒，或是將其略過。如果按一下「略過 (只記錄)」，則偵測到病毒時會傳送警示，但不會採取任何動作。
電腦關機設定	可用選項如下： 電腦關機時檢查磁片：在電腦關機時，啟用或停用掃描磁片。

進階掃描選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用這些選項自訂您的掃描設定。

Table 43: 進階掃描選項

進階選項	定義
壓縮檔選項	您可以設定下列選項： - 掃描壓縮檔內的檔案 啟用配置區 (如 Files.zip) 及配置區內容 (即個別壓縮的檔案) 掃描。 會在隨選、電子郵件及排程掃描時掃描壓縮檔。啟用此選項，並且使用「副檔名」對話方塊僅包含指定的副檔名時，即使未指定配置區副檔名，也會繼續掃描配置區檔案及其內容。您可以停用「掃描壓縮檔內的檔案」選項，或為特定配置區副檔名建立例外，使掃描作業不會掃描這些副檔名。 因為處理負荷過大，所以在 Windows 電腦上，「自動防護」不會掃描壓縮檔中的檔案。不過，當檔案從壓縮檔中解壓縮之後，「自動防護」就會掃描這些檔案。 Note: 您無法在掃描壓縮檔期間停止掃描。如果您選擇停止掃描，用戶端只有在完成掃描壓縮檔後，才會停止掃描。 - 壓縮檔中有壓縮檔時要展開的層次數目 指定支援的內部掃描層次數。
備份選項	嘗試修復檔案前自動備份檔案。
對話選項	指定掃描進度對話方塊是否會出現。您還可以指定是否要在掃描結束時關閉掃描進度對話方塊。選取「顯示掃描進度」或「顯示偵測到風險時的掃描進度」後，將顯示下列選項目： - 掃描執行時，將顯示「掃描進行中」訊息連結。 您可以按下此連結以便顯示掃描進度。 - 另外也會顯示重新排程下一個排程掃描的連結。
調整選項	平衡掃描效能最佳化，及其對其他應用程式的影響。 您可以選取下列任一選項： - 最佳掃描效能 最佳化掃描的效能。掃描完成需要較少的時間，但在掃描期間內，電腦上的其他應用程式可能會執行緩慢。對於具有四個或以上 CPU 的電腦，使用此選項可獲得最佳整體效能。 - 平衡效能 在掃描效能與其他應用程式效能之間取得平衡。在掃描效能與掃描期間執行的其他應用程式效能之間取得平衡。 - 最佳應用程式效能 最佳化電腦上執行的其他應用程式效能。掃描完成需要較長的時間，但在掃描期間電腦中其他應用程式的執行效能可能會較好。設定此選項後，掃描可以啟動，但只有在用戶端電腦處於閒置狀態時執行。 如果將「作用中掃描」架構為在收到新定義時執行，且如果使用者正在使用用戶端電腦，掃描最多可延後 15 分鐘。

進階選項	定義
儲存體移轉選項	指定「階層式儲存管理」(HSM) 以及離線備份系統維護之檔案的選項。 Note: 請洽詢您的 HSM 或備份廠商，協助您選取最適當的設定。

網路掃描設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構網路磁碟機的「自動防護」掃描選項。

在受管用戶端上，管理員可能會鎖定這些設定。

Table 44: 網路掃描設定

選項	說明
信任執行「自動防護」的遠端電腦檔案	防止「自動防護」在啟用網路掃描的情況下對可讀取的檔案執行重複掃描。 如果此選項啟用於兩個用戶端，每個用戶端會檢查另一個用戶端的「自動防護」設定是否與自己一樣安全。然後用戶端會信任彼此的「自動防護」掃描，並不會重新掃描任何檔案。 例如，當用戶端 A 存取用戶端 B 上一個網路磁碟機中的檔案，用戶端 A 的「自動防護」會檢查用戶端 B 的「自動防護」設定。如果用戶端 B 的「自動防護」可以信任，則用戶端 A 的「自動防護」就不會掃描檔案。如果用戶端 B 的「自動防護」無法被信任，則用戶端 A 的「自動防護」就會掃描檔案。 但是，當您讀取遠端電腦上的檔案時，「自動防護」可能不會掃描這些檔案。「自動防護」預設會嘗試信任「自動防護」的遠端版本。如果兩台電腦都啟用信任選項，則本機「自動防護」會檢查遠端電腦的「自動防護」設定。如果遠端「自動防護」設定提供的安全等級高於或等於本機設定時，本機「自動防護」就會信任遠端「自動防護」。當本機「自動防護」信任遠端「自動防護」時，本機「自動防護」不會掃描從遠端電腦讀取的檔案。因為，本機電腦相信，遠端「自動防護」已掃描過檔案。 如果您想要允許重複掃描，則停用此設定。 Note: 此功能僅適用於讀取存取。當用戶端 A 要求從用戶端 B 寫入權限，則無論此設定如何，用戶端 A 的「自動防護」會掃描檔案。 本機的「自動防護」一律都會掃描從遠端電腦複製的檔案。
網路快取	此選項可避免「自動防護」重複掃描相同的檔案，並可提升系統效能。您可以設定「自動防護」掃描並記住的檔案 (項目) 數目；也可以設定檔案從快取中移除之前的逾時。在逾時過期後，如果用戶端從網路伺服器要求網路檔案，「自動防護」會再次掃描這些檔案。

選取的副檔名

Windows 適用的 Symantec Endpoint Protection 用戶端指南

架構掃描只掃描選取的副檔名時，您可以將副檔名新增至清單，或從清單移除副檔名。

排程掃描和手動掃描一律會掃描配置區副檔名，例如.zip，無論選取要掃描的副檔名為何。您可以停用「進階掃描選項」對話方塊中的「掃描壓縮檔內的檔案」選項，以停用掃描配置區副檔名。

Table 45: 副檔名選項

選項	說明
使用預設值	將副檔名清單還原為預設狀態 會移除所有您新增的副檔名，而所有您移除的預設副檔名都會新增回去。
要新增一般副檔名類型的項目	可用選項如下： - 程式：選取常用程式的所有副檔名。 - 文件：選取常用文件的所有副檔名。

插入警告

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以將警告插入到附件受感染的電子郵件訊息本文中。此警告會指出用戶端在原始訊息中偵測到病毒。另外也會提供關於感染的資訊，包括用戶端採取的動作。

您可以使用此對話方塊自訂警告。您可以使用預設警告設定，或可以刪除文字，然後自行輸入所需的文字。如果用滑鼠右鍵按下文字方塊，可以將變數欄位插入警告。出現在警告時，相關的文字會自動取代變數欄位。

Table 46: 警告文字方塊

選項	說明
將原始訊息的主旨變更為	啟用或停用修改受感染檔案附件相關的訊息主旨。
訊息本文	指定訊息本文所要包含的文字。
感染資訊	指定電子郵件訊息應包含哪些感染資訊： 感染資訊也可以針對每一個受感染檔案列出： • 附件檔名稱 • 安全風險的名稱 • 採取動作 (例如清除、移至隔離所、刪除或略過) • 檔案狀態 (受感染或未受感染) 電子郵件變數欄位 顯示可新增至訊息的變數。

Table 47: 電子郵件變數欄位

欄位	說明
原始附件名稱	內含病毒或安全風險之附件的名稱。
安全風險名稱	發現的病毒或安全風險名稱。
已執行的操作	回應偵測到病毒或安全風險後所採取的動作。此動作可為架構的第一或第二個動作。
狀態	檔案的狀態：「受感染」、「未受感染」或「已刪除」。
檔案名稱	受病毒或安全風險感染的檔案名稱。
路徑及檔名	感染病毒或安全風險之檔案的完整路徑及名稱。
電腦	病毒或安全風險所在的電腦名稱。
使用者	出現病毒或安全風險時登入的使用者名稱。
發現日期	發現病毒或安全風險的日期。
電子郵件寄件者	已傳送附件受感染之電子郵件的電子郵件地址。
電子郵件收件者清單	附件受感染之電子郵件所寄送的地址清單。
儲存裝置名稱	應用程式受影響的區域。例如「自動防護」或「Microsoft Outlook 自動防護」。
電子郵件主旨	原始訊息的主旨。

傳送電子郵件至 收件者：訊息

Windows 適用的 Symantec Endpoint Protection 用戶端指南

若使用支援的電子郵件軟體，您可以自動傳送訊息給受感染電子郵件訊息的寄件者。此訊息會指出，用戶端在原始訊息偵測到病毒。另外也會提供關於感染的資訊，包括用戶端採取的動作。

您可以使用此對話方塊自訂訊息主旨及其內容。您可以使用預設訊息，或可以刪除文字，然後自行輸入所需的文字。如果用滑鼠右鍵按下文字方塊，可以將變數欄位插入訊息。出現在訊息時，相關的文字會自動取代變數欄位。

NOTE

並非所有變數欄位都可供每個文字方塊使用。

Table 48: 電子郵件訊息文字方塊

選項	說明
主旨	受感染訊息的主旨，並覆寫原始主旨。
訊息本文	此訊息的內容，會出現在訊息的最上方。
感染資訊	針對各受感染檔案列出下列資訊： • 附件檔名稱 • 安全風險的名稱 • 採取動作 (例如清除、移至隔離所、刪除或略過) • 檔案狀態 (受感染或未受感染)

Table 49: 電子郵件變數欄位

欄位	說明
原始附件名稱	內含病毒或安全風險之附件的名稱。
安全風險名稱	發現的病毒或安全風險名稱。
已執行的操作	回應偵測到病毒或安全風險後所採取的動作。此動作可為架構的第一或第二個動作。
狀態	檔案的狀態：「受感染」、「未受感染」或「已刪除」。
檔案名稱	受病毒或安全風險感染的檔案名稱。
路徑及檔名	感染病毒或安全風險之檔案的完整路徑及名稱。
電腦	病毒或安全風險所在的電腦名稱。
使用者	出現病毒或安全風險時登入的使用者名稱。
發現日期	發現病毒或安全風險的日期。
電子郵件寄件者	已傳送附件受感染之電子郵件的電子郵件地址。
電子郵件收件者清單	附件受感染之電子郵件所寄送的地址清單。
儲存裝置名稱	應用程式受影響的區域。例如「自動防護」或「Microsoft Outlook 自動防護」。
電子郵件主旨	原始訊息的主旨。

傳送電子郵件給其他人：其他人

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以自動通知其他人有關病毒或安全風險的感染情形。

輸入應收到病毒或安全風險通知之個人的電子郵件地址。用戶端會將關於病毒感染資訊的電子郵件訊息傳送到清單中的地址。按下「新增」加入電子郵件地址，或選取您想要移除的電子郵件地址，接著按下「移除」。

傳送電子郵件至 收件者：電子郵件伺服器

Windows 適用的 Symantec Endpoint Protection 用戶端指南

若要通知使用 Internet 電子郵件傳送受感染訊息的寄件者，您必須指定要用來傳送訊息的郵件伺服器。

Table 50: 電子郵件伺服器選項

選項	說明
郵件伺服器	郵件伺服器的名稱
郵件通訊埠	用來傳送訊息的郵件通訊埠
使用者名稱	存取郵件伺服器與傳送訊息所需的使用者名稱
密碼	郵件伺服器所需的密碼
回復路徑	郵件伺服器的回復路徑資訊。回復路徑通常不需要，但郵件伺服器可能需要它。您可以插入產生訊息的電腦的 DNS 名稱。

掃描動作

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構當掃描偵測到惡意軟體或安全風險時執行的動作。

若是「自動防護」，您的管理員可能會在受管用戶端上鎖定某些設定。

Table 51: 掃描動作選項

偵測類型	動作選項
惡意軟體	您可以架構第一個要採取的動作，以及第一個動作失敗時所要採取的第二個動作。 Note: 根據預設，「自動防護」會自動刪除新建立或儲存的受感染檔案，不論您在這裡指定的動作選項為何。 Note: 您可以在「自動防護進階選項」中啟用或停用此選項。 適用於惡意軟體的動作包括： - 清除風險：嘗試修復受病毒感染的檔案（僅限第一個動作）。此動作對特洛伊木馬程式或病蟲沒有作用。 Note: 不會清除在 Windows 8 樣式應用程式中偵測到的任何惡意軟體。會改為刪除惡意軟體。 - 隔離風險：嘗試在偵測到受感染的檔案時，將它移到受感染電腦上的「隔離所」。當檔案移到「隔離所」之後，除非您將檔案移回原始位置，否則無法執行該檔案。 Note: 不會隔離在 Windows 8 樣式應用程式中偵測到的任何惡意軟體。會改為刪除惡意軟體。 - 刪除風險：嘗試永久刪除檔案。只有在您可以使用沒有病毒的備份複本取代受感染的檔案時，才使用此選項。當永久刪除檔案後，您就無法從「資源回收筒」復原該檔案。 如果掃描無法刪除檔案，所採取動作的詳細資訊會出現在「通知」對話方塊和用戶端「風險日誌」中。 - 略過（只記錄）：拒絕存取檔案、顯示通知，並記錄事件。使用此選項來手動控制掃描處理偵測結果的方式。您可以為「風險日誌」中的偵測結果指定動作。
安全風險	您可以架構的安全風險動作如下： - 為所有安全風險架構相同的動作。 - 為整個類別的安全風險架構相同的動作。 按一下類別，然後按一下「覆寫針對安全風險架構的動作」。 - 針對特定類別所設定的動作，架構個別安全風險例外。 Note: 依據預設，自動防護會自動刪除新建立或儲存的安全風險，不論您在這裡指定的動作選項為何。 Note: 您可以在「自動防護進階選項」中啟用或停用此選項。 您可以架構第一個要採取的動作，以及第一個動作失敗時所要採取的第二個動作。 用於安全風險的動作包括： - 隔離風險：一偵測到安全風險或安全風險完成安裝時，立即嘗試將任何安全風險移到電腦上的「隔離所」。會嘗試移除或修復風險造成的任何副作用。副作用包括額外的登錄機碼、修改過的登錄機碼值、.ini 或 .bat 檔新增內容，或主機檔中的額外項目。副作用還包括系統驅動程式中的錯誤或 rootkit 的作用。在將安全風險移至「隔離所」之後，您將無法執行它。不過，您可以對安全風險執行其他動作。在某些情況下，您可能需要重新啟動電腦來完成移除或修復的動作。 Note: 不會隔離在 Windows 8 樣式應用程式中偵測到的安全風險。會改為刪除安全風險。 - 刪除風險：嘗試永久刪除安全風險。只有在您可以使用乾淨的備份複本取代安全風險檔案時，才使用此選項。您無法復原永久刪除的檔案。 請謹慎使用此動作。刪除安全風險可能會導致應用程式失去功能。 如果用戶端無法刪除檔案，用戶端所採取動作的詳細資訊會出現在「通知」對話方塊和「風險日誌」中。 「略過（只記錄）」：略過該風險，但是會記錄這項偵測。使用此選項來手動控制用戶端處理安全風險的方法。您可以為「風險日誌」中的安全風險指定一個動作。 Note: 在某些情況下，您可能會在不知情的情況下，安裝了包含安全風險的應用程式，如廣告軟體和間諜軟體。如果賽門鐵克判斷攔截風險並不會對電腦造成傷害，則根據預設值，用戶端將會攔截風險。如果攔截動作可能導致電腦處於不穩定狀態，用戶端會先等待應用程式安裝完成。用戶端之後才會對安全風險執行架構的動作。

建立新掃描

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以為電腦建立新的自訂掃描，以在需要時、指定時間或開機時執行。

Table 52: 掃描啟動選項

啟動選項	說明
隨選	只隨選執行選取的掃描。
在指定時間	只在指定的日期和時間執行掃描。
啟動時	只在系統開機或有新使用者登入時才執行掃描。

Table 53: 掃描的項目選項

掃描選項	說明
作用中	掃描此電腦的記憶體及其他常見的感染位置是否有病毒和安全風險。
完整掃描	掃描整個電腦是否有病毒和安全風險。使用此掃描，可檢查開機磁區、載入記憶體的程式，以及所有檔案和資料夾。掃描網路磁碟機可能需要密碼。
自訂	只掃描指定的檔案和資料夾。

建立新掃描 - 選取資料夾和檔案

Windows 適用的 Symantec Endpoint Protection 用戶端指南

若為自訂掃描，請使用此視窗定義掃描的一或多個目標。您可以定義整台電腦、一個本機磁碟、一或多個資料夾，或個別檔案。

建立新掃描 - 掃描選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊選取掃描選項。

Table 54: 掃描選項

選項	說明
檔案類型	架構您要掃描所有檔案類型還是僅掃描選取的副檔名。
動作	架構遇到安全風險時的動作。
通知	架構受感染電腦的通知訊息選項和矯正選項。 使用「用戶端管理」設定，可啟用或停用顯示在 Windows 8 樣式使用者介面上的彈出式通知。
進階	設定進階掃描選項，如掃描壓縮檔案、備份選項、對話選項、調整選項以及儲存體移轉選項。
掃描增強功能	指定掃描選取的檔案和資料夾前，其他要搜尋病毒和安全風險的位置。

建立新掃描 - 掃描名稱

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此視窗啟用、命名及描述掃描。

Table 55: 一般掃描資訊

欄位名稱	說明
掃描名稱	將掃描名稱鍵入此欄位。
掃描敘述	在此欄位鍵入掃描敘述。
啟用掃描	勾選此核取方塊，使掃描在預定的時間執行。 Note: 隨選掃描沒有此核取方塊。

建立新掃描 - 排程

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以設定掃描時間、隨機設定掃描開始時間，以及指定錯過掃描時的重試間隔。

Table 56: 排程選項

選項	說明
啟用	啟用或停用掃描排程
掃描排程	指定掃描頻率。 「每日」可讓您選取每天執行掃描的時間。實際執行掃描的時間，則要根據最後一次的執行時間、掃描持續時間和錯過的排程掃描設定。 「每週」可讓您選取每週執行掃描的時間和星期幾。實際執行掃描的時間，則要根據最後一次的執行時間、掃描持續時間和錯過的排程掃描設定。 「每月」可讓您選取每月執行掃描的時間和日期。實際執行掃描的時間，則要根據最後一次的執行時間、掃描持續時間和錯過的排程掃描設定。 如果最後一次執行的掃描由於掃描持續時間或錯過排程掃描設定而發生在不同的時間，可能不會使用架構的時間。例如，您可以將每週掃描架構為在每星期日午夜執行且重試間隔為一天。如果電腦錯過此掃描並於星期一早上 6:00 啟動，則會在早上 6:00 執行掃描。下一次掃描會在從星期一早上 6:00 算起的一週後執行，而非在下一個星期日的午夜執行。 如果電腦並未在星期二早上 6 點 (超過重試間隔兩天) 之前啟動，電腦就不會重試掃描。該電腦會等到下一個星期日的午夜再嘗試執行掃描。 不論是何種情況，如果您隨機設定掃描開始時間，您可能會變更掃描的最後一次執行時間。您也可以啟用或停用「即使沒有任何使用者登入，也執行此掃描」。
掃描持續時間	指定掃描應該執行多久的時間。您可以指定下列任一選項： - 到掃描完成 建議在大多數情況下使用此設定，以便獲得最佳的掃描效能。 - 最多掃描 n 小時 此設定可讓您控制資源可能有限之環境中的掃描時間。如果掃描未在指定的時段之內完成，則掃描會在下一個排程時間繼續。對於隨機化掃描，掃描會在指定時間間隔內的某個隨機時間繼續。 例如，如果您架構掃描在下午 8:00 執行，並設定長達 4 小時的期間，則非隨機化掃描會在下午 8:00 開始或繼續執行。若是隨機化掃描，掃描會在下午 8:00 與午夜之間的任意所選時間點開始或繼續執行。 如果您將頻率設為「每日」，則最長掃描持續時間為 23 小時。如果您將頻率設為「每週」，則最長掃描持續時間為 167 小時。如果您將頻率設為「每月」，則最長掃描持續時間為 671 小時。 如果選擇限制掃描時間，您還可以指定「在此期間隨機設定掃描開始時間」。使用此設定可掃描虛擬機器。隨機掃描可將多個掃描在同一時間開始從而需要佔用主機電腦上大量資源的幾率降到最低。

選項	說明
錯過掃描排程	您可以指定未依排程開始之掃描的重試時間間隔。例如，掃描可能會因為電腦關機而錯過執行時間。當電腦啟動時，會重試掃描，直到掃描開始或重試間隔到期為止。 「重試掃描間隔時間」可指定可重試錯過之掃描的小時數或天數。 如果您將頻率設為「每日」，則最長重試間隔時間為 72 小時。如果您將頻率設為「每週」，則最長重試間隔時間為七天。如果您將頻率設為「每月」，則最長重試間隔為 11 天。預設值與最大值相同，但每週掃描除外，它的預設值為三天。 Note: 在非受管用戶端上，設為「每日」的掃描的預設重試間隔為 8 小時。您最好增加這個間隔時間，以確保錯過的掃描會在更長的時段內重試。

建立新掃描 - 掃描的項目

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以定義您要執行的掃描類型。

Table 57: 掃描類型

掃描類型	定義
作用中掃描	掃描電腦中的記憶體和其他常見的感染位置，檢查是否有病毒及安全風險。您應該每天執行一次作用中掃描。
完整掃描	掃描整個電腦，檢查是否有病毒及安全風險，如廣告軟體和間諜軟體。使用此掃描，可檢查開機磁區、載入記憶體的程式，以及所有檔案和資料夾。掃描網路磁碟機可能需要密碼。您可能需要一週或一個月執行一次完整掃描。完整掃描可能會影響電腦效能。
自訂掃描	僅掃描您指定的檔案和資料夾。

建立新掃描 - 掃描的時間

Windows 適用的 Symantec Endpoint Protection 用戶端指南

當您建立新的掃描時，可選擇執行掃描的時間。

Table 58: 掃描啟動選項

選項	定義
在指定時間	在指定日期和時間定期執行此掃描。
啟動時	當系統啟動或當新使用者登入時執行此掃描。管理員可能已經架構不提供這個選項。
隨選	掃描不會自動執行。只有在指示時才執行此掃描。

掃描調整選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此視窗選取掃描的效能等級。

Table 59: 效能等級

效能等級	定義
最佳掃描效能	最佳化用戶端電腦上執行之掃描的效能 如果您選擇滑桿頂端，則掃描所需的時間較少，但在掃描期間其他應用程式的執行速度可能會較慢。 對於具有四個或以上 CPU 的電腦，使用此選項可獲得最佳整體效能。
平衡效能	在掃描效能與其他應用程式效能之間取得平衡 選擇滑桿中間，在掃描效能與掃描期間執行的其他應用程式效能之間取得平衡。
最佳應用程式效能	最佳化電腦上執行之其他應用程式的效能 如果您選擇滑桿的下端，則掃描所需的時間較長，但在掃描期間電腦上其他應用程式的執行效能會更好。

掃描類型 或 Symantec Endpoint Protection 偵測結果

Windows 適用的 Symantec Endpoint Protection 用戶端指南

如果用戶端沒有在掃描檔案中偵測到任何病毒，進度列會顯示掃描完成。

如果用戶端掃描時偵測到病毒，則結果清單會顯示感染詳細資訊。

NOTE

如果 Windows 適用的 用戶端偵測到大量的病毒、間諜軟體或高風險威脅，則進入主動掃描模式。掃描將重新啟動並使用智慧型掃描查詢。

Table 60: 感染詳細資訊

選項	說明
圖示	表示某檔案或風險是否仍屬威脅的圖示。綠色勾號表示某風險或檔案不再是威脅。紅色「x」表示某風險或檔案仍屬威脅。
檔案名稱	受感染檔案的名稱。 Note: 執行用戶端的作業系統語言可能無法解譯病毒名稱中的某些字元。如果作業系統無法解譯字元，那些字元會在通知中顯示為問號。例如，某些 Unicode 病毒名稱可能含有全形字元。在執行用戶端的英文作業系統電腦上，這些字元會顯示為問號。
風險	偵測到之風險的名稱。 您可以按下風險名稱，顯示賽門鐵克安全機制應變中心網站上有關風險的更多詳細資訊。
動作	用戶端針對風險 (如果有) 所執行的動作。
風險類型	偵測到之風險的類別。
登錄者	偵測到風險的掃描類型。
原始位置	用戶端偵測到之風險的資料夾路徑。
電腦	用戶端偵測到之風險的電腦名稱。
使用者	用戶端偵測到風險時，作用中使用者的名稱。
狀態	偵測到檔案的狀態。
目前位置	仍留在電腦上之受感染檔案的資料夾路徑。
主要動作	針對偵測到之風險架構的第一個動作。
次要動作	針對偵測到之風險架構的第二個動作。
動作敘述	用戶端對所偵測之風險 (如果有) 採取的動作說明。
日期和時間	顯示用戶端偵測到風險的日期與時間。

偵測到病毒時，用戶端便會嘗試完成您指定的動作。如果動作失敗，用戶端會執行指定給該類型病毒和掃描的第二個動作。您可以在偵測到的風險名稱上按下滑鼠右鍵，顯示掃描後動作的清單。並非所有動作都適用每種風險類型。

Table 61: 動作

選項	說明
排除	確保將來的掃描會忽略該病毒或風險。
清理	移除受感染檔案中的病毒。 如果用戶端成功清除檔案中的病毒，您就不需要採取任何其他動作。您的電腦將免於病毒的困擾，而且病毒不再容易散播到電腦的其他區域。 當用戶端清除檔案時，會移除受感染檔案、開機磁區和分割區表中的病毒。此移除程序可消除病毒散播的能力。 在某些情況下，清除的檔案可能會無法使用。這是病毒感染的結果，而非清除動作的結果。 某些受感染的檔案無法清除。
永久刪除	從電腦硬碟上刪除受感染的檔案。 只有在您有未受病毒或安全風險感染的備份複本可以取代此檔案時，才能使用此動作。當檔案永久刪除後，您就無法從「資源回收筒」復原檔案。 Note: 當您架構對安全風險執行的動作時，請審慎使用此動作，因為在某些情況下，刪除安全風險可能會造成應用程式喪失功能。
復原採取的動作	復原用戶端針對偵測到之風險所執行的動作。 不是在所有情況下都可以復原。例如，用戶端無法復原已刪除的檔案。
移到隔離所	執行下列其中一個動作： - 若是病毒，將受感染的檔案從其原始位置移到「隔離所」。放到「隔離所」後的受感染檔案無法散佈病毒。 - 若是安全風險，會將受感染的檔案從其原始位置移到「隔離所」，並嘗試移除或修復任何副作用。隔離所包含了所有執行動作的記錄。此記錄可讓您將電腦回復至用戶端移除風險之前的狀態。
屬性	顯示偵測到之風險的更多詳細資訊。

Outlook 防護的進階選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊決定是否要掃描 Outlook 郵件附件中壓縮檔的內容。您還可以設定掃描壓縮檔內部的壓縮檔的深度。

掃描通知選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構 Outlook 電子郵件「自動防護」掃描的通知選項。您可以啟用或停用「自動防護」偵測出病毒或安全風險時顯示的訊息。

若是受管用戶端，您的管理員可能會鎖定這些設定。

Table 62: 通知選項

選項	說明
偵測選項	在偵測出風險時顯示通知訊息。 啟用或停用當「自動防護」或使用者定義的掃描發現病毒或安全風險時，在受感染電腦上顯示通知。 您可以修改訊息中顯示的資訊類型。您可以使用預設的文字，也可以刪除文字並輸入自己的文字。如果在文字方塊中按下滑鼠右鍵，則您可以將變數欄位插入至通知文字中。出現在訊息時，相關的文字會自動取代變數欄位。 訊息變數顯示預設訊息變數以及您可以新增的變數。

Table 63: 訊息變數

欄位	說明
記錄者	偵測病毒或安全風險的掃描類型。
事件	事件的類型，例如「發現風險」。
安全風險名稱	發現的病毒或安全風險名稱。
路徑及檔名	感染病毒或安全風險之檔案的完整路徑及名稱。
位置	病毒或安全風險所在的電腦磁碟機。
電腦	病毒或安全風險所在的電腦名稱。
使用者	出現病毒或安全風險時登入的使用者名稱。
已執行的操作	回應偵測到病毒或安全風險後所採取的動作。此動作可為架構的第一或第二個動作。
發現日期	發現病毒或安全風險的日期。
狀態	檔案的狀態：「受感染」、「未受感染」或「已刪除」。
檔案名稱	受病毒或安全風險感染的檔案名稱。
儲存裝置名稱	應用程式的受感染區域，例如，「Microsoft Outlook 自動防護」。
動作說明	偵測到病毒或安全風險後所採取回應動作的完整敘述。

通知選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此視窗選取通知和矯正選項。

Table 64: 通知選項

選項	說明
偵測選項	在受感染的電腦上顯示自訂訊息。
矯正選項	發現病毒時，自動終止程序或停止服務。

主動型威脅防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

本節包括「變更設定 > 主動型威脅防護」頁面上行為分析 (SONAR) 對話方塊的說明。

行為分析

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以變更行為分析處理某些偵測類型的方式。您可能要變更這些設定，以減少誤報偵測數量。

行為分析以前稱為 SONAR。

NOTE

如果已停用「自動防護」且已啟用行為分析，則狀態頁面中會顯示行為分析未正常運作錯誤。停用「自動防護」後，行為分析會喪失某些功能，但仍可偵測啟發式威脅。若需完整的行為分析防護，您應啟用「自動防護」。

選項	說明
高度危險偵測 低度危險偵測	架構行為分析偵測對啟發式威脅的動作。啟發式威脅分為較可能是惡意威脅 (高風險) 或較不可能是惡意威脅 (低風險)。 對於低風險偵測，可以停用所有動作。如此，行為分析只會偵測最可能是惡意的應用程式。 您可以設定下列動作： • 矯正 將與偵測有關聯的檔案移動或嘗試移動到受感染電腦上的本機隔離所。攔截檔案，並記錄事件。 • 記錄：允許檔案，並記錄事件。 • 忽略：允許檔案，但不記錄事件。
當偵測發現以下項目時	行為分析可以在進行偵測且動作為「隔離」或「移除」時發出警示。您可以選取下列通知： • 偵測到時顯示警示 • 終止程序前提示 • 停止服務前提示
掃描遠端電腦上的檔案	啟用或停用對網路磁碟機進行行為分析掃描。

系統變更偵測

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以架構行為分析 (SONAR) 在偵測到 DNS 變更或主機檔案變更時的反應方式。

NOTE

當某個實體嘗試開啟或存取主機檔案時，行為分析不執行任何動作。只有在某個實體 (如 Internet Explorer) 修改主機檔案時，行為分析才會執行動作。

Table 65: 系統變更偵測選項

選項	說明
偵測到 DNS 變更 偵測到主機檔案變更	您可以架構當應用程式嘗試變更用戶端電腦的 DNS 設定或主機檔案時，由行為分析執行下列動作： • 略過 忽略偵測。此為預設動作。此動作可能導致用戶端電腦上出現許多通知。 • 提示 提示使用者允許或攔截變更。此動作可能導致日誌檔變大。 • 只記錄 允許變更，但為相關事件建立日誌項目。 • 攔截 攔截變更。 Note: 如果將 DNS 變更的動作設定為「攔截」，則可能會攔截對重要應用程式 (如 VPN 用戶端) 的存取。如果將「偵測到主機檔案變更」對應的動作設為「攔截」，則可能會攔截需要存取主機檔案的應用程式。
檢視清單	按下即可檢視針對系統變更偵測的任何使用者定義例外。

採取動作

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此對話方塊，針對偵測到的風險執行需要的動作。嘗試針對「**Symantec Endpoint Protection** 偵測結果」對話方塊中出現的風險採取行動時，用戶端會判斷動作是否可行。如果動作可行，則風險會出現在「採取動作」對話方塊中。如果想要執行動作，必須按下對話方塊右上角的按鈕。按鈕標籤視需要動作而定，可能是以下其中之一：

- 開始復原
- 開始清除
- 開始刪除
- 隔離

如果某風險的動作沒有出現，則風險不會出現在對話方塊中。關閉對話方塊即可返回「**Symantec Endpoint Protection** 偵測結果」對話方塊。

防網路和主機侵入

Windows 適用的 Symantec Endpoint Protection 用戶端指南

本節包括「變更設定 > 防網路和主機刺探利用」頁面上防火牆、入侵預防系統和記憶體攻擊緩和之對話方塊的說明。

網路活動

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用「網路活動」對話方塊，可以檢視用戶端上執行及存取網路的應用程式和服務。

Table 66: 網路活動功能表指令或滑鼠右鍵選項

選項	說明
工具功能表指令	顯示下列功能表指令： 測試網路安全：顯示「賽門鐵克安全機制」網站，讓您掃描電腦是否有病毒和風險。 管理員可能已經將此功能表指令架構成不會出現。
檢視功能表指令	以多種格式在「執行中的應用程式」面板中顯示項目。您也可以顯示下列其他的應用程式相關資訊： - 應用程式詳細資料 顯示應用程式的相關資訊，例如路徑和版本號碼。 - 連線詳細資料 顯示應用程式網路連線的相關資訊。 您可以顯示下列其他的流量類型： - 顯示 Windows 服務 顯示或隱藏用戶端執行的 Windows 服務。 - 顯示廣播流量 顯示廣播流量。如果取消勾選「顯示廣播流量」，就會顯示單點傳播流量。廣播流量是在特定子網路傳送至每部電腦的網路流量，不會特別導向至您的電腦。單點傳播流量則會特別導向至您的電腦。
連入和連出圖	顯示入埠流量和離埠流量。
連入和連出流量記錄圖	顯示過去兩分鐘入埠流量和離埠流量的即時資料。 此顯示畫面包含允許和攔截的流量。綠色表示允許的流量，紅色則表示攔截的流量。
攻擊記錄圖	顯示對電腦發出的攻擊數。
執行中的應用程式面板	顯示目前存取網路的應用程式和服務清單。 Note: 以 Unicode 補充字元命名的應用程式檔案名稱，顯示為兩個問號。 在面板按下滑鼠右鍵，即可取得「檢視」功能表內的相同功能表指令。 在未受管理用戶端時，如果在清單內的應用程式上按下滑鼠右鍵，也可以在應用程式執行下列指令： - 允許 用戶端允許應用程式存取網路。 - 詢問 通知會詢問您，下次嘗試執行應用程式時，是否要應用程式存取網路。 - 攔截 用戶端會攔截應用程式，不允許存取網路。 - 終止 用戶端停止程序。 如果按下「允許」或「攔截」，該應用程式就會新增至「檢視應用程式設定」對話方塊中的清單。

檢視應用程式設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

應用程式清單會顯示已存取網路連線的應用程式和服務。如果用戶端要求使用者允許或攔截某應用程式，該應用程式就會出現在清單中。

如果在「網路活動」對話方塊中的應用程式按下滑鼠右鍵，再按下「允許」或「攔截」，也可以新增應用程式。

網路活動

您可以對應用程式設限，例如，指定應用程式使用的 IP 位址和通訊埠。您可透過將某個應用程式從清單中移除，來移除對該應用程式的限制。當該應用程式再次嘗試要連接到網路時，會出現訊息，詢問您要允許或攔截該應用程式。

NOTE

如果您對此清單中的應用程式所架構的防火牆規則和這些設定有衝突時，則會優先採用防火牆規則的設定。

Table 67: 應用程式限定設定

選項	說明
應用程式設定	顯示應用程式或服務的檔案名稱、版本號碼、動作，以及路徑。 您可以將用戶端架構為對應用程式採取下列任一動作： - 允許 提供應用程式對網路的完整存取權。 - 攔截 阻止應用程式存取電腦或網路。
架構	讓您對選取的應用程式架構其他設定。

架構應用程式設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以對電腦上執行的應用程式或服務架構設定。架構特定應用程式的設定與建立防火牆規則時相同。差別在於其使用的準則較簡單，且只會套用於一個應用程式。

NOTE

如果防火牆規則與這些設定有衝突，將會優先採用防火牆規則的設定。例如，您可能在這個對話方塊中允許 Internet Explorer，但防火牆規則設定為攔截 Internet Explorer。那麼，用戶端會攔截 Internet Explorer。

Table 68: 架構應用程式限定設定

選項	說明
應用程式名稱	顯示選取的應用程式或服務的名稱。
應用程式的信任 IP	指定應用程式可存取的 IP 位址或 IP 位址範圍。 您可以選擇 IPv4 或 IPv6 作為位址類型。 若要選取範圍，請依序輸入起始位址、連字號 (-)、結束位址。 例如，若為 IPv6，請輸入： FE80::2AA:FF:FE9A:4CA2-FE80::2AA:FF:FE9A:4CA9 Note: 如果「信任 IP」或通訊埠文字欄位留白，則會允許所有流量。
遠端伺服器通訊埠	指定可用於此應用程式的遠端 TCP 或 UDP 通訊埠或遠端通訊埠範圍。 用戶端會攔截所有不在清單中的通訊埠。
允許連出連線	允許應用程式存取網路。
本機通訊埠	指定可用於此應用程式的本機 TCP 或 UDP 通訊埠或本機通訊埠範圍。 用戶端會攔截所有不在清單中的通訊埠。
允許連入連線	允許應用程式執行於電腦上。
允許 ICMP 流量	允許離埠 ICMP 回應要求 (類型：8，代碼：0) 和入埠 ICMP 回應回覆 (類型：0，代碼：0)。
在啟用螢幕保護程式時允許	當用戶端電腦執行螢幕保護程式時，允許應用程式存取網路。

選項	說明
啟用排程	指定啟用或忽略對應用程式限制的期間。 • 下列週期期間 只在指定的期間內啟用規則。 • 排除下列期間 除了指定的期間，其他時間均啟用規則。 • 開始於 指定期間開始的月、日、小時和分鐘。 • 時間長度 指定期間持續的天數、時數和分鐘數。

防網路和主機刺探利用：防火牆

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此標籤可啟用防火牆設定。這些設定可幫助偵測透過網路流量所發動的攻擊，並保護用戶端不受攻擊。

Table 69: 防火牆設定

選項	說明
啟用防火牆	啟用或停用防火牆。如果停用防火牆，所有流量都會進出用戶端。不會啟用任何防火牆規則或防火牆設定。
內建規則	• 啟用智慧型 DHCP 僅允許離埠 DHCP 要求和入埠 DHCP 回覆。智慧型 DHCP 也會允許 DHCP 更新。 此外，若要使用 DHCP，您必須建立防火牆規則，允許遠端通訊埠 67 (bootps) 和 68 (bootpc) 上的 UDP 流量。 動態主機架構通訊協定 (DHCP) 是一種將動態 IP 位址指派給網路裝置的通訊協定。動態位址能讓裝置在每次連線到企業網路時可以有不同的 IP 位址。DHCP 同時支援靜態 IP 位址和動態 IP 位址。因為軟體會記錄 IP 位址，動態位址可以簡化網路管理作業。否則，每次新增電腦到企業網路時，管理員都必須手動指派唯一的 IP 位址。如果用戶端從某個子網路移至另一個子網路，DHCP 可對用戶端的 IP 組態進行適當的調整。 • 啟用智慧型 WINS 僅允許將離埠 WINS 要求送至指派 WINS 伺服器，以及接收來自指派 WINS 伺服器的對應入埠回覆。 如果電腦送出 WINS 要求，而對方在五秒內回應，便會允許兩者通訊。所有其他 WINS 封包都會捨棄。 此外，若要使用 WINS，您必須建立防火牆規則，允許遠端通訊埠 137 上的 UDP 封包。 WINS 提供分散式資料庫，會針對網路使用的電腦及群組，註冊及查詢 NetBIOS 名稱的動態對應。WINS 會將 NetBIOS 名稱對應到 IP 位址。在使用 NetBIOS over TCP/IP 的路由網路中，WINS 用於 NetBIOS 名稱解析。在舊版 Microsoft 作業系統中建立網路服務時，需要用到 NetBIOS 名稱。NetBIOS 命名通訊協定與 TCP/IP 之外的其他網路通訊協定相容，例如 NetBEUI 或 IPX/SPX。不過，WINS 是專為支援 NetBIOS over TCP/IP (簡稱 NetBT) 而設計。WINS 可簡化 TCP/IP 網路中的 NetBIOS 名稱空間管理。 • 啟用智慧型 DNS 僅允許將離埠 DNS 要求送至指派 DNS 伺服器，以及接收來自指派 DNS 伺服器的對應入埠回覆。 如果電腦送出 DNS 要求，而對方在五秒內回應，便會允許兩者通訊。所有其他 DNS 封包都會捨棄。 若要使用 DNS，您也可建立防火牆規則，允許遠端通訊埠 53 (網域) 上的 UDP 流量。

選項	說明
流量設定	啟用 NetBIOS 防護 攔截來自外部網路的 NetBIOS 流量。 您可使用 LAN 上共用的「網路上的芳鄰」檔案和印表機，保護電腦免受任何外部網路利用 NetBIOS 侵入。此選項會攔截並非由定義的 ICANN 內部範圍內之 IP 位址發出的 NetBIOS 封包。ICANN 內部範圍包括 10.x.x.x、172.16.x.x、192.168.x.x 和 169.254.x.x，但不包括 169.254.0.x 和 169.254.255.x 子網路。NetBIOS 封包包括 UDP 88、UDP 137、UDP 138、TCP 135、TCP 139、TCP 445 和 TCP 1026。 Note: 用戶端電腦連線至不同子網路上的 Microsoft Exchange Server 時，NetBIOS 防護可能會導致 Microsoft Outlook 發生問題。您可能想要將伺服器的 IP 位址新增到入侵預防排除的電腦清單。會在處理內建規則之前，先處理排除的電腦清單。 允許 Token Ring 流量 允許透過 Token Ring 配接卡連線的用戶端電腦存取網路，不論用戶端上的防火牆規則為何。如果停用此設定，任何透過 Token Ring 配接卡連線的電腦所送出的流量都無法存取企業網路。防火牆不會過濾 Token Ring 流量，不是允許所有 Token Ring 流量，就是攔截所有 Token Ring 流量。 啟用防 MAC 詐騙 只有在對特定主機發出 ARP (位址解析通訊協定) 要求時，才允許入埠及離埠的 ARP 流量。這會攔截所有其他非預期的 ARP 流量，並記錄在安全日誌中。 有些駭客使用 MAC 詐騙，試圖劫取兩台電腦之間的通訊階段作業。媒體存取控制 (MAC) 位址是用於識別電腦、伺服器、路由器等的硬體位址。當電腦 A 想要與電腦 B 通訊時，可能會傳送 ARP 封包到電腦 B。 防 MAC 詐騙會保護電腦，不讓其他電腦重設 MAC 位址表。如果電腦送出 ARP REQUEST 訊息，用戶端會在 10 秒內允許對應的 ARP RESPOND 訊息。用戶端會拒絕來路不明的 ARP RESPOND 訊息。 啟用網路應用程式監控 允許用戶端監控用戶端電腦上執行之網路應用程式的變更。 網路應用程式會傳送和接收流量。用戶端會偵測應用程式的內容是否變更。 在防火牆啟動之前及防火牆停止之後攔截所有流量 當防火牆因故沒有執行時，會攔截所有進出用戶端電腦的入埠流量和離埠流量。 下列是電腦未受到防護的時間： - 用戶端電腦開啟之後，到防火牆服務啟動之前的這段時間 - 防火牆服務停止及用戶端電腦停止之後 這段時間是安全上的小漏洞，可能會允許未經授權的通訊。此設定可防止未經授權的應用程式與其他電腦通訊。 Note: 停用「網路威脅防護」時，用戶端會忽略此設定。 允許初始 DHCP 和 NetBIOS 流量 允許啟用網路連線的初始流量。此流量包括允許用戶端取得 IP 位址的初始 DHCP 和 NetBIOS 流量。 啟用服務阻斷偵測 服務阻斷偵測是一種入侵偵測。啟用此設定時，用戶端會在偵測到已知特徵的模式時攔截流量，不論埠號或使用的 Internet 通訊協定類型為何。 啟用通訊埠掃描偵測 監控任何安全規則攔截的所有連入封包。如果規則短時間內在不同通訊埠上攔截到幾個不同的封包，會建立安全日誌項目。通訊埠掃描偵測不會攔截任何封包。您必須建立安全政策，以便在執行通訊埠掃描時攔截流量。

選項	說明
不相符的 IP 流量設定	控制不符合任何防火牆規則的內送 IP 流量與外寄 IP 流量。IP 流量包含通過 IP 網路和使用 TCP、UDP 和 ICMP 通訊協定的資料封包。應用程式、郵件交換、檔案傳輸、連線偵測程式和 Web 傳輸等，都是 IP 流量的類型。 您可以架構下列 IP 流量設定： • 允許 IP 流量 除非防火牆規則另外說明，否則會允許任何內送流量與外寄流量。例如，如果您新增攔截 VPN 流量的防火牆規則，則防火牆會允許除了 VPN 流量之外的所有其他流量。 • 僅允許應用程式流量 允許流量進出應用程式，並攔截與任何應用程式都無關的流量。例如，除非另設規則，否則防火牆會允許 Internet Explorer 但攔截 VPN 流量。 • 允許應用程式流量前提示 顯示訊息，詢問您要允許或攔截應用程式。例如，您可能會想選擇是否要攔截媒體檔案。或者，您可能會想隱藏來自於 NTOSKRNL.DLL 程序的廣播。NTOSKRNL.DLL 程序的存在可能表示有間諜程式，因為間諜程式經常會下載和安裝 NTOSKRNL.DLL 程序。
主動回應設定	自動攔截攻擊者 IP 位址的秒數 在一個可架構的秒數內自動攔截已知入侵者的 IP 位址。 如果偵測到網路攻擊，會自動攔截連線以保護用戶端電腦的安全。用戶端會啟動主動回應，此功能會自動攔截可架構期間內所有進出攻擊電腦的通訊。 單一位置會攔截攻擊電腦的 IP 位址。
隱藏設定	• 啟用 TCP 重新排序 防止入侵者假借或詐騙他人的 IP 位址。 駭客使用 IP 詐騙，劫取兩台電腦 (例如，電腦 A 和 B) 之間的通訊階段作業。駭客可能送出會造成電腦 A 通訊中斷的資料封包。然後駭客會假冒為電腦 A，與電腦 B 通訊並加以攻擊。為防護電腦，TCP 重新排序會隨機產生 TCP 序號。 啟用 TCP 重新排序時，作業系統指紋偽裝的效果最好。 Warning! 用戶端服務執行時，TCP 重新排序會變更 TCP 排序號碼。服務執行時和服務不執行時的序號是不同的。因此，當您停止或啟動防火牆服務時，網路連線會終止。TCP/IP 封包會使用一連串的階段作業號碼與其他電腦進行通訊。如果用戶端未執行，則用戶端電腦會使用 Windows 編號配置。如果用戶端已執行，且 TCP 重新排序已啟用，則用戶端會使用不同的編號配置。如果用戶端服務突然停止，編號配置會回復至 Window 編號配置，接著 Windows 會捨棄流量封包。此外，TCP 重新排序與某些 NIC 可能有相容性問題，會導致用戶端攔截所有入埠流量和離埠流量。 • 啟用作業系統指紋偽裝 防止偵測用戶端電腦的作業系統。用戶端會變更 TCP/IP 封包的 TTL 和識別值，以防止作業系統被識別出來。 Note: 啟用 TCP 重新排序時，作業系統指紋偽裝的效果最好。 Warning! TCP 重新排序與某些 NIC 可能有相容性問題，會導致用戶端攔截所有入埠流量和離埠流量。 • 啟用隱藏模式網頁瀏覽 偵測來自任何通訊埠上網頁瀏覽器的 HTTP 流量，並移除下列資訊：瀏覽器名稱和版本號碼、作業系統，以及參考網頁。這可防止網站得知電腦使用哪種作業系統和瀏覽器。但是，不會偵測 HTTPS (SSL) 流量。 Warning! 隱藏模式網頁瀏覽可能會導致一些網站無法正常運作。某些 Web 伺服器會建立以網頁瀏覽器資訊為基礎的網頁。由於此選項會移除瀏覽器資訊，因此某些網頁可能無法正常顯示，或者完全無法顯示。隱藏模式網頁瀏覽會從 HTTP 要求標頭移除名為 HTTP_USER_AGENT 的瀏覽器特徵，並以一般特徵取代。

防網路和主機侵入：通知

Windows 適用的 Symantec Endpoint Protection 用戶端指南

在下列情況下，此對話方塊可讓通知出現在通知區域圖示中：

- 每次 IPS 特徵偵測到入侵預防攻擊嘗試時。在顯示前一個通知之後，如果用戶端偵測出第二個攻擊，則您只會看見一個通知。
- 每次記憶體攻擊緩和攔截到侵入或終止應用程式使其無法執行時。例如，您可能會看見下列通知：
Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected
Symantec Endpoint Protection will terminate your application

在受管用戶端上，管理員可能會阻止您架構這些設定。

防網路和主機侵入設定：Microsoft Windows 網路

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此標籤，可指定網路配接卡和網路瀏覽權限。

Table 70: Microsoft Windows 網路選項

選項	說明
選取您要架構的配接卡	指定網路流量會通過的網路介面卡。
瀏覽網路上的檔案和印表機	讓您瀏覽網路上的其他電腦、裝置和印表機。 Note: 如果停用此選項，會無法從網路位置複製檔案。
與網路上的其他人共用我的檔案和印表機	允許您網路上的其他使用者瀏覽您電腦上的檔案和資料夾。
執行螢幕保護程式時，攔截 Microsoft Windows 網路流量	當您電腦的螢幕保護程式啟用時，自動攔截所有「網路上的芳鄰」流量。當您再次使用電腦，就會馬上恢復之前指派的防護等級。

架構防火牆規則

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊可新增、編輯、啟用、刪除及變更所建立的防火牆規則順序。

防火牆會根據這些規則自動檢查所有入埠流量和離埠流量，然後適當地允許或攔截流量。每個規則都會指定規則生效所需符合的條件，以及規則會產生的效用。這些條件包括指定應用程式、通訊埠和通訊協定、主機以及指定時段。

NOTE

如果某防火牆規則與您在「檢視應用程式清單」對話方塊中所架構的特定應用程式設定發生衝突，則會優先採用防火牆規則設定。例如，如果您在應用程式清單中允許 Internet Explorer，但防火牆規則中卻攔截此程式，則用戶端就會攔截 Internet Explorer。

新增或編輯防火牆規則：一般

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊，可設定規則名稱、規則動作、網路配接卡觸發程序，以及其他幾個一般選項。

Table 71: 一般防火牆規則選項

選項	說明
規則名稱	規則的名稱。 命名規則時，請務必具體。例如，使用「Block After 1 AM」的規則名稱相較於「Rule1」為佳。
攔截此流量	攔截規則所指定的流量，使其無法存取您的網路。
允許此流量	允許規則指定的流量存取您的網路。
套用此規則到以下網路配接卡	將規則套用至選取的網路配接卡。
套用此規則，當螢幕保護程式為	根據螢幕保護程式的狀態啟用規則： - 開啟 只有在螢幕保護程式啟動時啟用規則。 - 關閉 只有螢幕保護程式關閉，並且所有的條件都符合時，這項規則才會啟用。 - 開或關 規則不受螢幕保護程式影響。
將此流量記錄於「封包日誌」中	在封包日誌中記錄這項規則所影響的流量。 您無須啟用封包日誌，讓用戶端記錄流量。

新增或編輯防火牆規則：主機

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用主機選項，可指定觸發防火牆規則的流量來源。例如，您可能想要只允許 IP 範圍為 192.168.0.1 到 198.168.0.76 的電腦所傳出的流量。

Table 72: 主機選項

選項	說明
全部主機	任何 IP 位址、MAC 位址或子網路位址及子網路遮罩。
MAC 位址	可識別電腦、伺服器、路由器及其他網路裝置的唯一硬體位址。 12 個字元的 MAC 位址使用十六進位格式 xx-xx-xx-xx-xx-xx。xx 代表 0-9 及 A-F 或 a-f。
IP 位址	IP 位址或 IP 位址範圍。 多個 IP 位址及多個 IP 位址範圍，請用逗號 (,) 分隔。例如，10.0.0.1, 192.168.0.1-198.168.0.76。
子網路	指定關於子網路的下列資訊： - 子網路 IP 位址 子網路的 IP 位址。 - 子網路遮罩 位址的網路及節點部分。子網路遮罩格式為 nnn.nnn.nnn.nnn。例如，您可能使用 255.255.255.0。

新增或編輯防火牆規則：通訊埠和通訊協定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以定義觸發防火牆規則的網路服務。服務的基礎為其通訊協定、通訊埠及流量方向。

Table 73: 通訊埠和通訊協定選項

選項	說明
通訊協定	套用規則到下列任一通訊協定： • 所有IP通訊協定 套用到任何通訊埠的任何通訊協定，入埠和出埠流量都適用。 • TCP 封包過濾如使用 TCP 和 UDP 時，您便需要定義入埠和離埠流量的來源與目標通訊埠號碼。通訊埠號碼可識別透過 TCP 和 UDP 執行的應用程式。在用戶端中，您可以定義遠端通訊埠和本機通訊埠。本機和遠端通訊埠一般會用於設定主機架構的防火牆。 • UDP 對於 UDP 通訊，用戶端會分析第一個 UDP 資料包，並將對初始資料包所採取的動作，套用到目前程式工作階段的所有後續 UDP 資料包。相同電腦之間的入埠或離埠流量會被認為是 UDP 連線的一部分。如果您指定了 TCP 或 UDP 通訊協定，請架構本機通訊埠、遠端通訊埠和流量方向。 – 遠端通訊埠 與用戶端電腦通訊的電腦。 – 本機通訊埠 用戶端電腦。 當用戶端電腦連接到遠端桌面時，遠端通訊埠就是通訊埠 TCP 上的 3389。對於入埠流量和離埠流量而言，本機通訊埠則相同。 如果您沒有選取任何埠號，則所有通訊埠都會觸發規則。如果您輸入本機通訊埠的埠號，但是未輸入遠端通訊埠的埠號，則所輸入的特定本機通訊埠及所有遠端通訊埠都會觸發規則。 – 狀態 UDP 對於狀態 UDP 流量，當建立 UDP 連線時，即允許入埠 UDP 通訊，即使防火牆規則攔截它也是一樣。防火牆使用狀態式檢測來追蹤連線資訊。例如，如果有某個規則攔截特定應用程式的入埠 UDP 通訊，但您選擇允許離埠 UDP 資料包，則在目前的應用程式工作階段中，將允許所有入埠 UDP 通訊。對於無狀態 UDP，您必須建立允許入埠 UDP 通訊回應的防火牆規則。對於單向起始的流量，您無須建立允許雙向流量的規則。TCP 會自動包含狀態式檢測。 若應用程式關閉通訊埠，UDP 工作階段會在 40 秒後逾時。 • ICMP 控制報告流量通訊錯誤的訊息，例如回應應答。 • 特定IP通訊協定 介於 0 到 255 之間的任何類型和代碼。 • 乙太網路 乙太網路通訊協定是 IEEE 802.3 所涵蓋的 LAN 群組。
流量方向	指定網路流量相對於電腦的方向。 • 內送 流入電腦的流量。 • 外寄 流出電腦的流量。 • 兩者 流入和流出電腦的流量。

新增或編輯防火牆規則：應用程式

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以指定會觸發防火牆規則的應用程式。例如，如果您想要允許電腦開啟 Internet Explorer 並搜尋網頁，則可以將 iexplore.exe 新增到清單。您必須將可能要存取網路連線或需要定期執行的應用程式加入。

Table 74: 應用程式選項

選項	說明
僅顯示已選取的應用程式	僅顯示「檔案名稱」欄中已勾選的應用程式。這些應用程式會觸發規則。
應用程式	列出您要允許或攔截的應用程式或服務的檔案名稱、版本號碼，以及路徑和執行檔名稱。「檔案名稱」欄含有核取方塊。如果勾選選定應用程式相對應的核取方塊，則用戶端會允許或攔截應用程式。當取消勾選核取方塊時，防火牆規則會忽略應用程式。

新增或編輯防火牆規則：排程

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用排程選項，可架構啟用或停用規則的時間。例如，您可能想要在安裝新應用程式時停用規則。

Table 75: 排程選項

選項	說明
啟用排程	啟用排程功能。
下列期間	使規則在特定期間內啟用。
排除下列期間	使規則在特定期間之外的時間啟用。
開始於	指定排程開始的月、日、小時和分鐘。
時間長度	指定期間持續的天數、時數和分鐘數。 例如，您可能希望期間從上午 8 點開始到上午 10 點結束。在「開始於」群組方塊中，將「小時」欄位設定為 08 (表示上午 8 點)。在「時間長度」群組方塊中，將「小時」設定為 2。

檢視防火牆規則

Windows 適用的 Symantec Endpoint Protection 用戶端指南

伺服器規則是管理員為用戶端所架構的規則。用戶端規則是您在用戶端上建立的規則。防火牆會以特定順序處理伺服器規則、用戶端規則和用戶端設定。

您可以在同一處檢視伺服器規則、用戶端規則和用戶端設定。您可以修改或變用戶端規則或用戶端設定的順序，但伺服器規則就不行。對於伺服器規則，您只能檢視用戶端是否會攔截、允許或要求使用者允許或攔截指定的流量類型。

管理員必須設定此選項可用，您才能檢視這個對話方塊。

Table 76: 防火牆處理伺服器規則和用戶端規則的順序

優先順序	使用者類型
第一	管理員指派高優先順序的伺服器規則
秒	用戶端規則
第三	低優先順序的伺服器規則
第四	用戶端網路威脅防護設定
第五	用戶端應用程式專用的設定

防網路和主機刺探利用設定：入侵預防

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此標籤可架構入侵預防系統設定。這些設定可協助偵測和防護用戶端，以防範符合已知入侵模式的攻擊。

在受管用戶端上，管理員可能會鎖定這些設定。

Table 77: 入侵預防設定

選項	說明
啟用網路入侵預防	將網路 IPS 特徵和 IPS 特徵例外套用於用戶端的入埠和離埠流量。 網路攻擊會記錄在安全日誌中。您可以架構用戶端電腦偵測到攻擊時發出通知。 通常情況下，應總是啟用此選項。根據預設，會啟用這些選項。
啟用 URL 信譽	識別來自網域和 URL 的威脅，這些網域和 URL 可以託管惡意軟體、詐騙、網路釣魚和垃圾郵件等這類惡意內容。URL 信譽功能會攔截識別為惡意內容之已知來源的網址存取權。 在 14.3 RU1 中提供。
啟用瀏覽器入侵預防	將 IPS 網頁瀏覽器特徵套用至用戶端上的入埠和離埠瀏覽器流量。 啟用此選項時，用戶端會將瀏覽器特徵與瀏覽器的入埠和離埠流量進行比較。支援的瀏覽器包括 Internet Explorer 和 Firefox。不支援其他瀏覽器。如需特定瀏覽器版本的相關資訊，請參閱： Endpoint Protection 中瀏覽器入侵預防支援的瀏覽器版本 瀏覽器攻擊會記錄在安全日誌中。 對於某些瀏覽器攻擊，入侵預防會要求用戶端終止瀏覽器。用戶端電腦上會顯示通知。 通常情況下，應總是啟用此選項。此選項預設為啟用。
記錄偵測但不攔截	您可以使用此選項來記錄瀏覽器入侵預防在沒有攔截任何流量的情況下所進行的偵測。疑難排解 Web 連線問題時，此選項可能非常有用。 在一段短時間之後，您應停用只記錄模式，以為您的電腦提供最佳防護。

記憶體攻擊緩和

Windows 適用的 Symantec Endpoint Protection 用戶端指南

記憶體攻擊緩和會阻止對用戶端電腦上所執行的常用應用程式進行弱點攻擊。為阻止侵入，記憶體攻擊緩和有時需要終止應用程式。您的電腦上出現一則訊息，指示 已終止應用程式。

Symantec Endpoint Protection will terminate your application

如果您認為偵測遇到錯誤，請取消勾選「啟用記憶體攻擊緩和」並重新執行應用程式。向您的管理員報告錯誤偵測，然後重新啟用記憶體攻擊緩和防護。

在受管用戶端上，管理員可能會阻止您變更此設定。

Web 和雲端存取防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

本節包括「變更設定 > Web 和雲端存取防護」頁面上 Web 和雲端存取防護的說明。

Web 和雲端存取防護設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

Web 和雲端存取防護只會將網路流量或 Web 流量重新導向至 Symantec Web Security Service (WSS)。WSS 上的規則可允許或攔截用戶端上的流量。

選項	說明
啟用 Web 和雲端存取防護	啟用或停用用戶端上的 Web 和雲端存取防護。此選項只有在 Symantec Endpoint Protection 管理員將其設為可用時才能使用。不過，您無法架構重新導向方法。除非您或管理員需要對用戶端問題進行疑難排解，否則您應該將此防護保持啟用狀態。

例外

Windows 適用的 Symantec Endpoint Protection 用戶端指南

本節包括「變更設定 > 例外」頁面上掃描例外之對話方塊的說明。

例外：使用者定義的例外

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此標籤將檔案、資料夾、風險和程序排除，不接受掃描。例如，您不妨排除安全無虞的檔案。排除不接受掃描的檔案，可以提高掃描的效能。

Table 78: 例外選項

例外	定義
安全風險例外	從病毒和間諜軟體掃描中排除的已知風險、檔案、資料夾和副檔名。您也可以排除受信任的 Web 網域。
SONAR 例外	選取要從 SONAR 中排除的資料夾。如果要排除某個特定程序，請改為指定應用程式例外。
應用程式例外	指定要對其套用動作的應用程式。該動作會覆寫應用程式的預設掃描動作。例外適用於所有掃描。您可以指定下列任一動作： • 略過 將應用程式排除在日後掃描的偵測範圍外。此動作為預設動作。 • 只記錄 偵測到應用程式時，在「主動型威脅防護」威脅日誌中新增項目。 • 隔離 應用程式啟動時加以隔離。 • 終止 應用程式啟動時使其停止，但不會將其從電腦中移除。 • 移除 應用程式啟動時使其停止，並將其從電腦中移除。 Note: 當指定的應用程式執行時，會套用「隔離」、「終止」和「移除」動作。當偵測到應用程式時，會套用「忽略」和「只記錄」動作。

例外	定義
DNS 或主機檔案變更例外	針對應用程式建立例外以變更 DNS 或主機檔案。行為分析 (SONAR) 通常會防止 DNS 或主機檔案變更之類的系統變更。例如，您可能需要針對 VPN 應用程式建立例外。 Note: DNS 或主機檔案變更例外不會讓應用程式免於行為分析偵測。如果行為分析出現潛在的惡意行為，則一律會偵測到該應用程式。 您可以指定下列任一動作： • 略過 應用程式進行 DNS 或主機檔案變更時，將它排除在偵測範圍之外。 • 提示 提示使用者允許或攔截指定的應用程式進行 DNS 或主機檔案變更。 • 攔截 阻止應用程式進行 DNS 或主機檔案變更。 • 只記錄 當行為分析偵測到是由指定的應用程式進行 DNS 或主機檔案變更時，在掃描日誌中新增項目。 Note: 當應用程式嘗試變更主機檔案或修改 DNS 設定時，行為分析會套用指定的動作。如果應用程式只是開啟或存取主機檔案或是包含 DNS 設定的檔案，則行為分析不會套用動作。

已知安全風險例外

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊可選取病毒和間諜軟體掃描應排除的已知安全風險。分級愈高，代表風險越高。

Table 79: 安全風險例外選項

選項	說明
安全風險表	已知安全風險表中的欄顯示下列欄標題： • 安全風險 已知安全風險的名稱。如果您想要排除安全風險，勾選安全風險名稱旁的核取方塊。 • 風險類別 風險的類型，例如誤導型應用程式。 • 整體分級 安全風險嚴重性的一般性評估。此評估是以安全風險的隱私權等級、效能等級、隱密性等級和移除等級的組合為基礎。 • 隱私權影響分級 安全風險威脅您私人資訊的程度。 • 效能影響分級 安全風險影響您電腦效能的程度。 • 隱藏分級 安全風險嘗試隱藏以防止被偵測及移除的程度。 • 移除分級 移除安全風險的容易程度。 • 獨立程式 應用程式是否依賴安全風險才能正常運作。
偵測到安全風險時記錄	掃描偵測到已知安全風險時，會將偵測記錄於「風險日誌」。即使風險已排除在掃描的範圍以外，掃描還是會記錄偵測。

安全風險副檔名例外

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊可指定病毒和間諜軟體掃描應排除的檔案類型。您一次僅可以新增一個副檔名。副檔名中可以包含一個空格。

如果您想要新增多個副檔名，請輸入一個副檔名後再新增該副檔名。針對每個要新增的副檔名重複此步驟。請勿在「新增」文字方塊中輸入多個副檔名。若輸入多個副檔名，用戶端會將該輸入項目視為一個副檔名。

Table 80: 副檔名例外

選項	說明
新增	新增副檔名至副檔名清單加以排除，不接受掃描。 Note: 請勿鍵入前面的點 (.). 例如，鍵入 exe 而不是 .exe。
移除	從清單中移除副檔名。

信任的 Web 網域例外

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以將 Web 網域排除在「下載智慧型掃描」偵測和行為分析 (SONAR) 的範圍之外。如果排除某個 Web 網域，將一律允許使用從該 Web 網域下載的檔案。但是，任何允許的檔案都將由「自動防護」以及任何管理員或使用使用者定義的掃描進行掃描。

依預設，「下載智慧型掃描」不會檢查使用者從信任的 Internet 或內部網路網站下載的任何檔案。您可以在 Windows「控制台 > 網際網路選項 > 安全性」標籤上，架構信任的網站和信任的本機內部網路網站。您可以在「病毒和間諜軟體防護」設定中停用內部網站的「下載智慧型掃描」設定。

指定信任的 Web 網域例外時，您必須輸入單一網域或 IP 位址。一次只能指定一個網域。不支援通訊埠號。您必須指定 FTP 位置的 IP 位址。

您可以指定 URL，但是例外狀況僅使用 URL 的網域名稱部分。如果指定了 URL，則您可以使用 HTTP 或 HTTPS (不區分大小寫) 預先擱置 URL，但是例外狀況適用於兩者，即 HTTP 和 HTTPS。

例如，下列任一項目均會產生相同的例外狀況：

- test.domain.com
- test.domain.com/mydocs
- HTTP://test.domain.com/mydocs
- https://test.domain.com

無論您是透過 HTTP 還是 HTTPS 瀏覽到 test.domain，「下載智慧型掃描」和行為分析都會排除這個網域。如果您瀏覽到這個網域中的任何位置 (例如 mydocs)，便可從該位置下載檔案。

當您指定 IP 位址時，例外會同時套用至指定的 IP 位址及其對應的主機名稱。

例如，針對 FTP 位置，您必須指定 IP 位址。如果您透過 FTP 的 URL 來瀏覽到 FTP 位置，會將主機名稱解析為 IP 位址並套用例外。

隔離所

Windows 適用的 Symantec Endpoint Protection 用戶端指南

本節包括「檢視隔離所」頁面的說明。

檢視隔離所

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此視窗可管理隔離所中的檔案。

NOTE

您用戶端的作業系統語言可能無法轉譯風險名稱中的某些字元。如果作業系統無法解譯字元，那些字元會在通知中顯示為問號。例如，某些 Unicode 編碼的風險名稱可能包含全形字元。在執行用戶端的英文作業系統電腦上，這些字元會顯示為問號。

Table 81: 隔離選項

選項	定義
還原	將檔案還原至其原始位置，並將其從隔離所中移除。如果您認為某個檔案因誤報而被錯誤隔離，可以還原該檔案。有時候，清除的檔案並沒有可供還原的位置。例如，受感染的附件可能已從電子郵件中刪除而置於隔離所中。您必須釋放該檔案並指定一個位置。
刪除	從隔離所刪除檔案。依據預設，隔離所會在 30 天之後自動刪除檔案，但是管理員可以架構其他時段。
全部重新掃描	重新掃描隔離所內的檔案以判斷是否可以清除、修復和還原。在用戶端上更新定義檔後，用戶端也會重新掃描檔案
匯出	將檔案清單匯出至試算表或資料庫以進行分析。
新增	隔離檔案，以便在該檔案存在病毒或威脅時不會感染您的電腦。當掃描偵測到威脅時，用戶端可能無法在偵測發生時執行預先定義動作。這些預先定義動作可能包含清除檔案或隔離檔案。如果預設動作無法完成，用戶端會記錄事件。您可以透過 用戶端將檔案手動匯入「隔離所」。您也可以稍後再使用「風險日誌」或「掃描日誌」中的項目來隔離檔案。
送出	您可以將隔離所中可能感染的項目送至「賽門鐵克安全機制應變中心」進行分析，以確認其是否受到感染。賽門鐵克安全機制應變中心還會使用此資料防範新威脅或發展中的威脅。 如果管理員停用這些傳送類型，傳送選項將無法使用。
清除選項	在指定時間間隔或資料夾大小後，從隔離所移除項目。您也可以指定，在儲存項目的資料夾達到特定大小時，用戶端便移除項目。此架構可防止您因忘記從這些區域中手動移除檔案而造成檔案堆積。 Note: 您的管理員可以指定項目可藉以保留在「隔離所」中的參數。符合這些參數之後，項目便會自動從「隔離所」中刪除。

清除選項：隔離項目

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊，可排程 用戶端自動清除隔離的檔案。

Table 82: 隔離所清除選項

選項	說明
儲存的時間長度超過	在指定時間長度後刪除隔離項目。您可以調整用戶端刪除項目前需等待的天數、月數或年數。
資料夾總大小超過	當資料夾達到其定義的大小限制時，會自動刪除隔離項目。用戶端會刪除資料夾中最舊的檔案，直到資料夾大小符合限制。

清除選項：備份項目

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊排程 用戶端自動清除備份的檔案。

Table 83: 備份清除選項

選項	說明
儲存的時間長度超過	啟用此核取方塊，在指定時間長度後刪除備份項目。您可以調整用戶端刪除項目前需等待的天數、月數或年數。
資料夾總大小超過	啟用此核取方塊，自動清除備份的項目，讓資料夾保持於定義的大小限制內。當資料夾超過大小限制時，用戶端會刪除資料夾中最舊的檔案直到資料夾大小符合限制。

清除選項：修復項目

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊排程 用戶端自動清除修復的檔案。

Table 84: 修復清除選項

選項	說明
儲存的時間長度超過	啟用此核取方塊，在指定時間長度後刪除修復項目。您可以調整用戶端刪除項目前需等待的天數、月數或年數。
資料夾總大小超過	啟用此核取方塊，自動清除修復的項目，讓資料夾保持於定義的大小限制內。當資料夾超過大小限制時，用戶端會刪除資料夾中最舊的檔案直到資料夾大小符合限制。

用戶端管理

本節包括「變更設定 > 用戶端管理」頁面上「用戶端管理」對話方塊的說明。

用戶端管理設定：一般

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此標籤，顯示通報區域圖示、變更您的位置，以及更新使用者資訊。

Table 85: 一般選項

選項	說明
在通知區域中顯示賽門鐵克安全性圖示	顯示或隱藏在 Windows 通知區域中出現的產品圖示。 用戶端狀態圖示
重要警示使用 Windows Toast 通知	僅在執行 Windows 8 的用戶端電腦上出現。啟用或停用進行偵測和出現其他重大事件時在 Windows 8 樣式使用者介面顯示的彈出式通知。
架構 Proxy 選項	讓您設定要用於外部通訊的代理伺服器。如果使用代理伺服器，用戶端將更加安全，因為用戶端不與 Internet 直接通訊。
架構重新開機選項	讓您架構重新啟動電腦的排程。
位置選項	顯示可用位置的清單。 將位置變更為清單上的其他位置。但是，如果其他位置符合任何條件，則用戶端會立即自動切換至該位置。 僅適用於受管用戶端。
使用者資訊	如果管理員已啟用此選項，可讓您更新使用者資訊。 僅適用於受管用戶端。

選項	說明
啟用應用程式與裝置控制	您可以啟用或停用應用程式與裝置控制規則。應用程式控制透過控制用戶端電腦上的應用程式的行為，保護您的電腦。裝置控制保護您的電腦免受可能插入電腦的硬體裝置 (如 USB 裝置) 的危害。在極少數情況下，應用程式控制可能會干擾您執行的某些安全的應用程式，您可能需要暫時停用此選項。這個選項不會防止應用程式和裝置控制檢查程序和應用程式。這個選項只會啟用或停用您的管理員管理的政策規則。在受管電腦上，管理員可能會阻止您變更此選項。

Proxy 伺服器設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可能希望為外部通訊使用 Proxy 伺服器。如果您打算使用預設設定 (亦即為 Proxy 伺服器使用瀏覽器設定)，則不需要執行任何動作。例如，如果使用 Internet Explorer 作為預設網頁瀏覽器，則 Proxy 伺服器就可以使用「Windows 網際網路選項」。

NOTE

您在這裡架構的 Proxy 可用於除 LiveUpdate 之外的所有外部通訊。如果您希望將預設的 Windows 網際網路選項設定用作 LiveUpdate 的 Proxy 設定，則無需執行任何動作。如果希望為不使用預設值的 LiveUpdate 設定一個 Proxy，您必須透過 LiveUpdate 標籤架構它。

使用代理伺服器設定指示以下資訊：

- 不使用代理伺服器
您不希望使用 HTTP 或 HTTPS Proxy 伺服器。
- 使用用戶端瀏覽器指定的 **Proxy** 伺服器 (預設)
您希望為代理伺服器使用預設的 Windows 網際網路選項設定。
- 使用自訂 **Proxy** 設定
您希望自訂要使用的 Proxy 伺服器的 HTTP 或 HTTPS 設定。

Table 86: HTTP 和 HTTPS 代理設定

選項	說明
主機代理	如有需要，請輸入代理伺服器位址。
通訊埠	輸入伺服器上要使用的 HTTP 或 HTTPS 通訊埠。
需要驗證	如果 Proxy 伺服器需要使用者名稱和密碼，則應勾選此選項。
使用者名稱	輸入要用於 Proxy 伺服器的帳戶使用者名稱。
密碼	輸入要用於 Proxy 伺服器的帳戶密碼。
NT LAN Manager 驗證	透過 NT LAN Manager (NTLM) 輸入其他選擇性驗證。您必須在「使用者名稱」欄位中包含以下列格式的網域名稱： domain_name\user_name 網域名稱不能超過 14 個字元，並且使用者名稱不能超過 64 個字元。 Note: 如果您為系統代理選取驗證或選取「NT LAN Manager 驗證」，任何早於 14.2 RU1 的用戶端版本可能會中斷通訊。

重新開機選項

Windows 適用的 Symantec Endpoint Protection 用戶端指南

下表說明使用案例，協助您瞭解在不同情況下使用哪些選項。

Table 87: 重新開機選項

選項	說明
重新啟動電腦	- 立即 如果用戶端電腦必須立即重新啟動，請使用此選項。可能需要立即重新啟動的情況包含：惡意軟體矯正、排程緊急情況以及針對臨近威脅的主動型威脅防護。 - 目前 如果立即重新啟動會影響工作，或者可以安全地延遲重新啟動，則可使用此選項。請務必瞭解當目前存在動態威脅時，延遲重新啟動的意義。 - 隨機設定開始時間 使用此選項可避免與其他排程工作產生衝突。使用「隨機化時數」設定可控制此選項的行為。 - 隨機化時數 使用此控制可變更「隨機設定開始時間」選項的行為。您可以改變預設隨機化設定，範圍為 1 到 8 小時。
重新啟動類型	- 不要重新啟動 不建議使用。如果使用此選項，則需要由使用者重新啟動電腦。請確定瞭解使用此選項的影響，尤其是存在動態威脅時。 - 無提示 此選項通常與「在所示時間」選項一起使用，在使用者遠離電腦時禁止重新啟動提示。 - 倒數計時提示 使用此選項顯示提示，通知使用者已接近重新啟動時間。與「立即」和「在所示時間」設定一起使用時，此選項尤其實用。 - 提示並允許延緩最多 當用戶端電腦必須在指定時間內重新啟動時，可使用此選項。使用者可利用此選項儲存資料和結束程式，並確保電腦重新啟動。
重新啟動訊息	您可以指定訊息，以讓使用者知道必須重新啟動電腦。
其他選項	這些選項可控制用戶端電腦與重新啟動之時可能正在執行的其他程式相關時的行為。 這些選項僅適用於 Windows 用戶端。Mac 用戶端始終執行硬式重新啟動。 - 硬式重新啟動 無論用戶端電腦上正在進行任何其他活動，此選項均可強制用戶端電腦重新啟動。除非出現極端情形，否則大部分情況下均不使用此選項。 - 如果使用者未登入，立即重新啟動 送出重新啟動要求時，如果使用者未登入，此選項會強制立即重新啟動並覆寫其他擱置重新啟動動作。

用戶端管理設定：竄改防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「竄改防護」為伺服器及用戶端上執行的賽門鐵克應用程式提供即時防護。它可防護賽門鐵克程序及內部物件不受非賽門鐵克程序 (例如，病蟲、特洛伊木馬程式、病毒和安全風險) 攻擊。「竄改防護」可攔截或記錄嘗試修改賽門鐵克程序或同步賽門鐵克執行緒及程序的內部軟體物件的動作。

在受管用戶端上，管理員可能會鎖定這些設定。

Table 88: 竄改防護選項

選項	說明
防護賽門鐵克安全軟體不受竄改或關閉	啟用或停用「竄改防護」。
如果應用程式嘗試竄改或關閉賽門鐵克安全軟體，要執行的動作	指定「竄改防護」偵測到問題時，所要執行的動作。 選取下列任一動作： - 只記錄 此動作會記錄發生的未經授權活動，但會允許該活動繼續執行。 - 攔截且不記錄 此動作會攔截未經授權的活動，但不記錄發生的事件。 - 攔截並記錄 此動作會攔截未經授權的活動，並記錄發生的事件。

用戶端管理設定：LiveUpdate

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此對話方塊決定更新內容 (例如病毒定義及 IPS 特徵) 的時間和方式。

在受管用戶端上，唯有由管理員啟用，您才能排程執行 LiveUpdate。

Table 89: LiveUpdate 更新排程的選項

選項	說明
啟用自動更新	讓用戶端於排定間隔執行 LiveUpdate。
頻率和時間	表示用戶端下載防護更新和產品更新的頻率。 這些選項可用與否，視您選取的頻率而定： - 連續：無選項可用。 - 每：您可以選取更新之間相隔的時數。 - 每日：您可以選取每日更新開始的時間。 - 每週：您可以選取更新在星期幾及那一天的幾點開始。
重試時段	如果 LiveUpdate 失敗，您可以指定用戶端嘗試再次執行 LiveUpdate 的時間間隔。如果該時間間隔晚於下次排程的 LiveUpdate 下載，LiveUpdate 會等到下次排程時間再嘗試執行。 如果 LiveUpdate 成功，LiveUpdate 則不會於此處指定的時間間隔再次執行。
隨機化選項	可讓您將多個用戶端同時嘗試下載更新的影響降至最低。您可以架構用戶端隨機下載更新。您可以指定下載要在更新排程時間前後開始的時間範圍。時間範圍可以為數天或數小時，視您選取的頻率而定。
閒置偵測	延後排程更新，直到電腦處於閒置狀態為止。逾期工作最終將無條件執行。 如果停用此選項，則無論電腦繁忙程度如何，排程的 LiveUpdate 階段作業都將一律在排程時間執行。
Proxy 選項	讓您可以設定要用於 LiveUpdate 的自訂 Proxy 伺服器。

用戶端管理設定：LiveUpdate Proxy 伺服器設定：HTTP

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可能需要為 LiveUpdate 使用 Proxy 伺服器。如果您打算為 Proxy 伺服器使用 Windows 網際網路選項設定，則不需要執行任何動作。

使用代理伺服器設定指示以下資訊：

- 您希望停用 HTTP 或 HTTPS Proxy 伺服器的使用。
- 您希望為代理伺服器使用預設的 Windows 網際網路選項設定。
- 您希望自訂要使用的 Proxy 伺服器的設定。

Table 90: HTTP 或 HTTPS Proxy 設定

選項	說明
伺服器位址	如有需要，請輸入代理伺服器位址。
HTTP 通訊埠 HTTPS 通訊埠	根據使用的是 HTTP 通訊協定還是 HTTPS 通訊協定，在適當文字方塊中輸入要使用的通訊埠。
需要驗證	如果 Proxy 伺服器需要使用者名稱和密碼，則應勾選此選項。
基本驗證	此選項需要您輸入要用於代理伺服器之帳戶的使用者名稱和密碼。
NT LAN Manager 驗證	此選項需要您輸入要用於代理伺服器之帳戶的使用者名稱和密碼。您還必須輸入伺服器所在網域的名稱。

用戶端管理設定：LiveUpdate Proxy 伺服器設定：FTP

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可能需要為 LiveUpdate 使用 Proxy 伺服器。如果您打算為 Proxy 伺服器使用 Windows 網際網路選項設定，則不需要執行任何動作。

使用代理伺服器設定指示以下資訊：

- 您希望停用 FTP Proxy 伺服器的使用。
- 您希望為代理伺服器使用預設的 Windows 網際網路選項設定。
- 您希望自訂要使用的 Proxy 伺服器的設定。

Table 91: FTP Proxy 設定

選項	說明
FTP 主機 Proxy	輸入要用於 Proxy 伺服器的位址。
通訊埠	輸入要用於 Proxy 伺服器的通訊埠。

用戶端管理設定：傳送

Windows 適用的 Symantec Endpoint Protection 用戶端指南

依據預設，用戶端電腦會將匿名資訊傳送至賽門鐵克，以改善威脅防護並更快地阻止威脅。

如果您的組織是賽門鐵克贊助的自訂分析計畫的一部分，您傳送的資料會提高賽門鐵克回應威脅以及為電腦自訂防護的能力。

NOTE

賽門鐵克建議您允許傳送。

Table 92: 傳送選項

選項	說明
將匿名資料傳送至賽門鐵克，以獲得增強的威脅防護情報	會將 資訊傳送至賽門鐵克，其中包括偵測資訊以及網路和架構資訊。賽門鐵克會匿名處理用戶端提交資料，這樣就無法使用該資料來直接識別特定使用者。賽門鐵克可使用此資訊更快地解析誤報和應對惡意軟體攻擊，從而提高產品安全性。 賽門鐵克建議您保持此選項開啟。
更多選項	您可以啟用或停用特定傳送類型。這些類型包括檔案信譽資料、程序資料、網路資料和組態資料
允許智慧型掃描查詢以偵測威脅	允許 使用賽門鐵克的信譽資料庫進行威脅相關決策。信譽資料庫稱為 Symantec Insight。對資料庫的查詢稱為「智慧型掃描查詢」。 下載鑑識、病毒與間諜軟體掃描以及行為分析 (SONAR) 會使用智慧型掃描查詢來偵測威脅。賽門鐵克建議您盡可能允許智慧型掃描查詢。停用智慧型掃描查詢會停用「下載鑑識」，並可能會影響行為分析和病毒與間諜軟體掃描的功能。 但是，如果您不希望允許賽門鐵克查詢「賽門鐵克智慧型掃描」，則可以停用此選項。例如，您的公司可能要求您關閉與網路的外部通訊，使資料永遠不會離開電腦。 此選項預設為啟用。

疑難排解

本節包括「說明 > 疑難排解」面板的說明。

疑難排解：管理/雲端管理

Windows 適用的 Symantec Endpoint Protection 用戶端指南

此面板會顯示用戶端和用戶端防護的相關資訊。

NOTE

只有在管理員或賽門鐵克技術支援指示時，才使用此面板。

- 如果您的管理員從 管理此用戶端，則此面板稱為「管理」。
- 如果您的管理員從雲端管理此用戶端，則此面板稱為「雲端管理」。

如果在雲端主控台中註冊 Symantec Endpoint Protection Manager 網域，則也會顯示「混合管理」面板。

Table 93: 管理選項

選項	說明
一般資訊	- 伺服器：管理伺服器的 IP 位址或 DNS 名稱。如果伺服器已連線，IP 位址就會出現。如果用戶端已受管理，但是目前未連線伺服器，狀態會顯示為「離線」。如果用戶端是非受管用戶端，狀態則會顯示為「自我管理」。 關於受管用戶端和非受管用戶端 - 群組：用戶端所屬及提供其防護的群組。 - 上次連線時間：用戶端上次與管理伺服器進行通訊的日期和時間。 - 主機完整性狀態：如果您的用戶端已通過主機完整性檢查，用戶端會存取網路。如果您的用戶端未通過檢查，可能會要求您下載軟體，也可能會將您重新導向到其他網路。 - 位置偵測/位置：不同的位置可以指派有不同的安全政策。 - 政策序號：從管理伺服器下載的安全政策的序號。
通訊設定	讓您匯入通訊檔案 (.xml)。使用通訊檔案可以將受管用戶端轉換成非受管用戶端，或將非受管用戶端轉換成受管用戶端。您會從管理員收到通訊檔案。
政策設定檔	讓您更新、匯入或匯出政策檔案至用戶端。政策檔案包含了防護電腦的設定。

選項	說明
疑難排解資料	可讓您將用戶端和電腦的相關資訊，以文字檔的方式儲存。此檔案也包含一般政策資訊、定義檔版本號碼，以及其他資訊。您可以將此檔案，透過電子郵件傳送給管理員或賽門鐵克技術支援，以協助解決用戶端或電腦方面的問題。

Table 94: 雲端管理選項

選項	說明
一般資訊	- 雲端：雲端伺服器的位址。如果伺服器已連線，位址就會出現。 - 群組：用戶端所屬及提供其防護的群組。 - 位置偵測/位置：不同的位置可以指派有不同的安全政策。
政策	列出了套用至您的用戶端並提供防護的雲端式政策。此區段不會顯示以 為基礎的政策。

疑難排解：混合管理

Windows 適用的 Symantec Endpoint Protection 用戶端指南

已在 Symantec Endpoint Security 雲端主控台中註冊 Symantec Endpoint Protection Manager 網域時，會顯示此面板。此面板顯示用戶端接收自雲端的雲端式政策。

選項	說明
一般資訊	雲端伺服器位址。如果用戶端未連線至伺服器，則此欄位會顯示「未註冊」。
政策	列出套用至用戶端的雲端式政策。Symantec Endpoint Protection Manager 所控制的政策會顯示在「管理」面板上。
政策設定檔	從雲端主控台要求政策，並在用戶端上更新該政策。使用此選項可手動更新政策。

疑難排解：版本

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此面板，檢視用戶端防護引擎和防護定義檔案的版本號碼。

NOTE

只有在管理員或「賽門鐵克技術支援」指示時，才能使用此面板。

Table 95: 版本資訊

選項	說明
引擎	顯示安裝元件的版本號碼。
定義	顯示目前安裝的病毒定義檔和其他定義檔的類型、序號和上次檢查日期。

疑難排解：除錯日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此面板，架構和檢視除錯日誌的內容。管理員會使用日誌內的資訊，來記錄用戶端和電腦防護的相關資訊。

[用戶端管理除錯日誌設定](#)

NOTE

只有在管理員或「賽門鐵克技術支援」指示時，才能使用此面板。

用戶端管理除錯日誌設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此對話方塊架構除錯日誌，來收集用戶端下列區域的疑難排解相關資訊。

- 與伺服器的連線
- 防火牆事件
- 位置切換
- 主機完整性遵從

將此資訊傳送給管理員或「賽門鐵克技術支援」。日誌檔案的名稱就是稱為 `debug.log` 的文字檔。

WARNING

如果啟用此除錯日誌，日誌大小增加的速度可能很快。因此，只有在管理員或「賽門鐵克技術支援」指示時，才能指定設定。

Table 96: 用戶端管理除錯日誌設定

選項	說明
除錯開啟	啟用日誌會開始記錄資料。
除錯等級	記錄掃描事件。預設值為 0，疑難排解通常建議使用此值。
日誌等級	記錄防火牆事件。日誌記錄已攔截封包的相關資訊，其中包括已套用的規則，和傳送封包的應用程式。預設值為 0，會記錄所有可能的事件。
日誌檔大小 (KB)	增加或減少日誌檔大小。預設日誌大小為 256 KB。檔案大小不妨保持小一點，以節省電腦上的空間。

疑難排解：Windows 帳戶

您可以使用此面板檢視目前使用者的設定檔。

NOTE

只有在被賽門鐵克技術支援引導時才能使用此面板。

Table 97: Windows 帳戶

選項	說明
使用者	目前登入使用者的名稱、網域和 SID 資訊。
群組	使用者所屬 Active Directory 群組的名稱、網域和屬性清單。
使用權限	使用者可以執行之 Active Directory 權限或動作的名稱、顯示名稱和屬性清單。

Symantec Endpoint Protection 除錯日誌設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此對話方塊啟用用戶端，來收集掃描的疑難排解相關資訊。日誌檔案的名稱就是稱為 `vpdebug.log` 的文字檔。

WARNING

如果指定設定，日誌大小增加的速度可能很快。因此，只有在管理員或「賽門鐵克技術支援」指示時，才能指定設定。

疑難排解：電腦

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此面板檢視您電腦的架構資訊。

NOTE

只有在被 Broadcom 技術支援引導時才能使用此面板。

Table 98: 電腦資訊

選項	說明
作業系統	顯示用戶端作業系統的類型和版本。
電腦	列出用戶端電腦上的處理器總數以及各個處理器的製造商和類型。
記憶體	列出用戶端電腦上全部的以及可用的實體記憶體與虛擬記憶體。
磁碟機空間	列出用戶端電腦上的每個磁碟機及其相應的總磁碟機空間和可用磁碟機空間。

疑難排解：安裝設定

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊，檢查用戶端是否：

- 具有大小完整的定義檔或大小縮小的定義檔。縮減大小定義檔用於內嵌或虛擬用戶端。
- 用戶端上安裝的防護技術。

疑難排解：用戶端升級

Windows 適用的 Symantec Endpoint Protection 用戶端指南

此面板會顯示用戶端升級的相關資訊。

Table 99: 用戶端升級選項

選項	說明
發行通道	顯示用戶端取得其更新的發行通道。可能的值包括： • 上次發行通道：將上次發行版次推送至用戶端。 • 最新發行通道：將最新發行版次推送至用戶端。
目前的升級順序	顯示目前安裝的用戶端的 LiveUpdate 序號。此值也會顯示在「說明 > 關於」和「說明 > 疑難排解 > 版本」下。
選擇升級日期	當管理員定義升級日期範圍時，顯示下一次用戶端升級的日期。 LiveUpdate 上有可用升級之後，會從該範圍中選取日期來升級用戶端軟體。

疑難排解：伺服器連線狀態或通用雲端連線狀態

Windows 適用的 Symantec Endpoint Protection 用戶端指南

此面板會顯示用戶端與管理伺服器或用戶端與雲端伺服器之間的連線狀態。

NOTE

只有在被管理員或技術支援引導時才能使用此面板。

- 如果您的管理員從 管理此用戶端，此面板稱為「連線狀態」。
- 如果您的管理員從雲端管理此用戶端，此面板稱為「通用雲端連線狀態」。

如果用戶端與伺服器之間的通訊出現問題，您應該先檢查並確定網路沒有任何問題，然後呼叫技術支援。

基於下列任何原因，您可能需要檢查通訊：

- 用戶端未收到安全性政策更新。
- 用戶端似乎未能連線到伺服器。Windows 通知區的用戶端圖示沒有顯示綠點。
- 病毒定義檔長期未更新。
- 需要檢查用戶端是受管用戶端還是非受管用戶端。受管用戶端連線到伺服器，但可能會呈現離線狀態。非受管用戶端絕不會連線到伺服器。

Table 100: 連線狀態選項

選項	說明
狀態	顯示用戶端目前是否使用下列設定連線到伺服器： • 已連線：用戶端已連線到伺服器。 • 未連線：用戶端目前未連線到伺服器。
立即連線	嘗試連線到伺服器。使用此選項以測試用戶端是否連線。
上次嘗試連線	顯示用戶端上次嘗試連線到伺服器的日期和時間。例如，用戶端會在每次電腦重新啟動時重新連線到伺服器。
上次成功連線	顯示用戶端上次成功連線到伺服器的日期和時間。
伺服器名稱	顯示管理伺服器的 IP 位址或 DNS 名稱。
通訊埠編號	顯示伺服器用來連線到用戶端的埠號。Windows 防火牆可能會攔截該通訊埠編號。

如果用戶端未連線，您可以按下「錯誤詳細資料」瞭解原因。您也可以查看用戶端上次嘗試連線到伺服器的時間，以及用戶端上次成功連線的時間。此面板也會顯示伺服器的位址或 DNS 名稱，以及伺服器用來連線的通訊埠。

Table 101: 雲端主控台連線狀態選項

選項	說明
狀態	顯示用戶端目前是否根據下列狀態來連線到雲端伺服器： • 已連線：用戶端已連線到伺服器。 • 未連線：用戶端目前未連線到伺服器。
雲端已連線	顯示用戶端上次嘗試連線到雲端伺服器的日期和時間。例如，用戶端會在每次電腦重新啟動時重新連線到伺服器。
已連線的 SPOC	顯示用戶端上次嘗試連線到 SPOC 伺服器的日期和時間。
連線詳細資料	• 雲端 顯示雲端伺服器的 IP 位址或 DNS 名稱。 • SPOC：阻止用戶端執行特定活動 (例如檢查安全政策更新) 的雲端伺服器。雲端會告知 SPOC 阻止受管用戶端，以便他們簽入。
手動註冊	將 Symantec Endpoint Protection 用戶端 (在雲端中稱為 Symantec 代理程式) 連線至雲端伺服器。代理程式必須進行註冊，才能與雲端通訊，因此，請從雲端下載政策。如果您知道雲端主控台管理用戶端但未連線，則請使用此選項。

疑難排解：訂購授權狀態

Windows 適用的 Symantec Endpoint Protection 用戶端指南

此面板會顯示此用戶端上安裝的每個 產品的訂閱到期日。例如，
您可以訂閱一或三年。

疑難排解：應用程式強化

Windows 適用的 Symantec Endpoint Protection 用戶端指南

此面板會顯示應用程式強化功能是會保護您的用戶端裝置，還是僅進行監控。

您必須訂閱 Symantec Endpoint Security 並在雲端主控台中註冊，才會出現資訊。

Table 102: 應用程式強化選項

選項	說明
註冊狀態	指示用戶端是否已向雲端註冊。
預防模式	- 預防：主動攔截您的管理員定義之政策中所定義的行為。 - 監控：監控並記錄可能不利的動作。不執行任何動作。
傳遞模式	- 已啟用：應用程式強化將載入其驅動程式，但會略過政策和任何偵測。啟用此設定意味著應用程式強化會略過「預防模式」。 - 已停用：應用程式強化將載入其驅動程式、讀取政策，並根據「預防模式」的定義進行偵測。

疑難排解：EDR 連線狀態

Windows 適用的 Symantec Endpoint Protection 用戶端指南

顯示用戶端是否已連線至 Symantec Endpoint Detection and Response (EDR) 伺服器。僅當 政策指定 Symantec EDR 伺服器時可用。

Table 103: EDR 連線狀態選項

選項	說明
狀態	- 已連線：已啟用 EDR，而且用戶端已連線至 Symantec EDR 伺服器。會出現已連線 Symantec EDR 伺服器的名稱。 - 未驗證：Symantec EDR 已完成佈建用戶端進行註冊，並已將登入認證傳送至管理伺服器。Symantec EDR 正在等待用戶端進行驗證，以完成註冊程序。 - 未連線：已啟用 EDR，但用戶端未連線至內部部署 Symantec EDR 伺服器。 用戶端與 Symantec EDR 之間的連線不是永久性的。用戶端架構必須更新但未連線至伺服器時，用戶端狀態會從「已連線」移至「未連線」。在大部分情況下，架構包括 FDR 排定的提交。 更新 Symantec EDR 政策架構可能需要幾分鐘時間。 會出現「已嘗試伺服器」清單。「連線」選項可以使用。 - 已停用：已停用 EDR，而且用戶端未連線至 Symantec EDR 伺服器。
已嘗試連線 成功連線	當用戶端成功連線到 Symantec EDR 伺服器或用戶端嘗試連線到 Symantec EDR 伺服器時顯示時間。
已嘗試伺服器	當 EDR 連線狀態為「未連線」時顯示的 EDR 伺服器清單。 此用戶端的管理伺服器政策可確定 EDR 伺服器的優先順序。當用戶端未連線時，EDR 伺服器清單會在一開始比對管理伺服器政策中顯示的優先順序。 在您選取「連線」之後，用戶端會重新整理清單以顯示用戶端嘗試 Symantec EDR 伺服器的實際順序。 用戶端會從政策的第一個優先順序群組中隨機選擇一部伺服器，然後嘗試該群組中的所有其他伺服器。如果伺服器皆未連線，則用戶端會以相同的方式嘗試下一個優先順序群組。
上次連線嘗試	顯示上次手動嘗試連線或驗證的日期和時間。

選項	說明
目前正連線至伺服器	顯示用戶端正在嘗試連線的 Symantec EDR 伺服器。

疑難排解：Web 和雲端存取防護

Windows 適用的 Symantec Endpoint Protection 用戶端指南

選項	說明
狀態	顯示用戶端上的 Web 和雲端存取防護元件狀態： - 已啟用：已在電腦上安裝並啟用 Web 和雲端存取防護。 - 未安裝：未在電腦上安裝 Web 和雲端存取防護。 - 已按策略停用。已在電腦上安裝並啟用 Web 和雲端存取防護，但未啟用 Web 和雲端存取防護政策。 - 故障：Web 和雲端存取防護未正確執行。WSS 記號可能無效。 - 通道失敗：在使用「根據主控台使用者」流量識別方法時發生。WSS 代理程式無法與已登錄的使用者連線。 Web 和雲端存取防護需要 Symantec Web Security Services 的授權。
使用者名稱	狀態所套用至的使用者。
通訊協定	列出 Web 和雲端存取防護所使用的通訊協定。
Datacenter	列出重新導向網路流量並由其進行處理的目標 WSS Datacenter。
狀態訊息	提供 Web 和雲端存取防護元件狀態的資訊。
重新連線	Web 和雲端存取防護應該持續連線至 WSS。不過，在某些情況下，連線會中斷。Wi-Fi 可能關閉、網際網路連線停用或資料中心故障。無論是什麼原因導致中斷，當服務回復時，用戶端使用者必須重新連接到 WSS。如果用戶端未偵測到連線已中斷，則請按一下「重新連線」選項。如果用戶端偵測到連線已中斷，則請按下「狀態」頁面上的「修正」按鈕。
檢視日誌	顯示系統日誌中所記錄並上傳至 Symantec Endpoint Protection Manager 的 Web 和雲端存取防護診斷事件。

日誌

本節包括「檢視日誌」頁面上對話方塊的說明。

疑難排解：日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此面板可檢視各防護類型的日誌。您可以展開或濃縮各類日誌。

NOTE

如果您登入的是受管用戶端，部分日誌中的某些選項可能無法使用。是否能使用這些選項取決於您的管理員所允許的項目。

在任何日誌中，不適合特定項目的選項可能無法使用。

Table 104: 用戶端日誌及敘述

日誌	說明
掃描日誌	某段時間內在電腦上執行的掃描。
風險日誌	感染電腦的病毒和安全風險。安全風險包含可連至「賽門鐵克安全機制應變中心」網頁的連結，該網頁可提供其他資訊。
病毒和間諜軟體防護系統日誌	電腦上與病毒及安全風險相關系統活動的資訊。這項資訊包含架構變更、錯誤及定義檔資訊。
威脅日誌	行為分析 (SONAR) 在您電腦上偵測到的威脅。這些包含作為惡意用途的商用應用程式。範例為特洛伊木馬程式、病蟲或按鍵記錄器，或大量郵件病蟲、病毒及程序檔式威脅。
主動型威脅防護系統日誌	電腦上與行為分析相關的系統活動。
竄改防護日誌	嘗試竄改賽門鐵克應用程式的事件相關項目。這些項目包含「竄改防護」偵測到或偵測到並攔截的嘗試事件相關資訊。
流量日誌	您的電腦透過網路建立的連線。
封包日誌	進入或離開電腦通訊埠的資料封包。
控制日誌	電腦應用程式會存取或執行的登錄機碼、檔案和 DLL。
安全日誌	針對您的電腦且可能造成威脅的活動。服務阻斷攻擊、通訊埠掃描及執行檔變更等活動都是範例。
應用程式控制日誌	顯示環境中不需要和未經授權的應用程式以及用戶端所攔截的行為。如果系統管理員從雲端主控台管理應用程式強化政策，則會顯示此日誌。
用戶端管理系統日誌	發生在電腦上的作業變更。範例包括當服務啟動或停止、電腦偵測網路應用程式或架構軟體時的活動。

病毒和間諜軟體防護日誌：掃描日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「掃描日誌」會使用來自「事件日誌」的資料，提供已經在您電腦上執行掃描的完整狀況。這些資訊會顯示電腦的掃描頻率以及在電腦上執行的掃描類型。但不適當的動作或管理員不允許的動作是看不到的。

您可以使用此日誌查看掃描是否因某種原因停止或中斷。

您可以使用此資訊注意感染的趨勢，讓您可以有更好的偵測策略回應。例如，假設您在星期五工作時花很多時間在 Internet 上，您可能會注意到感染常發生在星期一早上。這時您就可以安排每星期一早上 8:00 執行完整掃描。

您可以在「掃描日誌」中執行下列工作：

- 檢視某段時間內，已在您電腦上發生的掃描清單。掃描會和這些掃描的其他相關資訊一起顯示。
- 將日誌中的資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。
- 在項目上按滑鼠右鍵，可檢視其屬性。

Table 105: 掃描日誌欄

欄名稱	說明
開始時間	掃描開始的日期和時間。
已完成	掃描結束的日期和時間。
登錄者	執行的掃描類型。例如，如果掃描是「開機掃描」，此欄就會顯示「開機」。
電腦	執行掃描的電腦。例如，如果您從本機電腦掃描網路磁碟機，此欄位就會包含本機電腦名稱。這不是磁碟機實際所在的電腦。
狀態	掃描的目前狀態，例如「掃描完成」、「掃描中」或「掃描中斷」。
檔案總數	已掃描的檔案總數。

欄名稱	說明
受感染	找到的感染或異常數。
信任	註明為受 Insight 信任的檔案數。

病毒和間諜軟體防護日誌：風險日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「風險日誌」會顯示清單，包含電腦所感染的病毒及安全風險和有關各個感染的其他資訊。第一欄中的狀態圖示會顯示風險是仍然存在於電腦上，還是已成功移除。如果病毒或安全風險仍然存在，會出現紅色的 x。如果病毒或安全風險已被移除，則會出現綠色勾選標記。

您可以在「風險日誌」中執行下列工作：

Table 106: 風險日誌選項

選項	說明
匯出	可讓您將日誌資料儲存為逗號分隔文字檔，然後匯入到其他應用程式，例如試算表。
清理	可讓您清除在掃描期間所發現風險的副作用。此動作會有效地將風險從電腦移除。
刪除	在可能的情況下，可讓您從電腦刪除風險。
復原	在可能的情況下，可讓您復原動作。
隔離	在可能的情況下，可讓您隔離發現的風險。

您也可以在某個項目上按下滑鼠右鍵檢視其詳細資料。

NOTE

「下載智慧型掃描」偵測的風險詳細資料只顯示嘗試下載的第一個入口網站應用程式。

Table 107: 風險日誌欄

欄名稱	說明
檔案名稱	所涉及的檔案名稱 (如果適用)。
風險	發現的病毒或安全風險名稱。
動作	針對病毒或安全風險所採取的動作。
風險類型	所發現威脅或安全風險的類型，例如病毒、廣告軟體、間諜軟體或撥接工具。
登錄者	負責記錄事件的掃描類型，例如「自動防護」或「開機」。
原始位置	發現病毒或安全風險的位置 (如果適用)。
電腦	記錄偵測到風險的電腦。例如，如果您使用本機電腦而「自動防護」發現遠端檔案有病毒，則「電腦」就會是您的本機電腦。
使用者	發現病毒或安全風險時登入電腦的使用者。
狀態	檔案目前的感染狀態。例如，狀態可能是受感染、已清除或已刪除。已隔離的檔案通常會有受感染的狀態，但它無法傷害您的電腦。
目前位置	目前的病毒或安全風險位置。例如，位置可能是「隔離所」。
主要動作	針對此病毒或安全風險或其類別所架構的第一個動作。
次要動作	針對此病毒或安全風險或其類別所架構的第二個動作。架構的第二個動作會在第一個動作失敗時採取。
動作敘述	針對病毒或安全風險所採取之動作的敘述。

欄名稱	說明
日期和時間	記錄病毒或安全風險的日期和時間。

病毒和間諜軟體防護日誌：系統日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「系統日誌」會每天記錄與電腦防護相關的病毒和安全風險活動。這些記錄稱為事件，包括架構變更、錯誤以及病毒和安全風險定義檔資訊，而且會一起顯示其他資訊。但不適當的動作或管理員不允許的動作是看不到的。

藉由使用「系統日誌」中的資訊，可讓您追蹤電腦上與病毒和安全風險相關的趨勢。如果有多人使用同一部電腦，您可以識別是誰帶來風險，協助其使用更完善的預防措施。

您可以在「系統日誌」中執行下列工作：

Table 108: 系統日誌選項

選項	說明
匯出	將資料儲存成逗點分隔 (.csv) 的檔案。
過濾器	可讓您過濾顯示畫面，只看到一或幾種事件。 您可以勾選要在日誌檢視顯示的事件類型。所有類型的事件仍會繼續寫入「系統日誌」。

您也可以用滑鼠右鍵按下某個項目檢視其屬性。

Table 109: 系統日誌的各欄

欄名稱	說明
事件	發生的事件。
登錄者	負責記錄事件的實體。例如，此實體可以是排程掃描或系統事件 (如載入新的病毒定義檔)。
電腦	發生事件的電腦。
使用者	報告這個事件的使用者帳戶。
說明	所發生事件的說明。
日期和時間	事件的記錄日期與時間。

主動型威脅防護日誌：威脅日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「威脅日誌」會列出主動型威脅掃描在電腦上已偵測且預防的威脅，另外還包含其他資訊。但不適當的動作或管理員不允許的動作是看不到的。

NOTE

可使用哪些動作選項取決於所選日誌項目所適用的動作。

您可以在「威脅日誌」中執行下列工作：

Table 110: 威脅日誌選項

選項	說明
匯出	將資料儲存成逗點分隔 (.csv) 的檔案。
終止	結束在電腦上找到的程式或程序。
還原	還原「隔離所」中已選取的威脅。 只有在您選取已隔離的威脅時，這個選項才有作用。
隔離	將選取的檔案移至「隔離所」。
新增至 DNS 或主機檔案變更例外	允許選取的應用程式進行 DNS 或主機檔案變更。 僅當您在嘗試進行 DNS 或主機檔案變更的偵測到的應用程式上按下滑鼠右鍵時，這個選項才會出現。

您也可以用滑鼠右鍵按下某個項目檢視其屬性。

Table 111: 威脅日誌欄

欄名稱	說明
檔案名稱	所涉及的檔案名稱 (如果適用)。
風險	已找到的威脅名稱。
動作	針對威脅採取的動作。
風險類型	已找到的威脅類型。
登錄者	負責記錄事件的掃描類型。
原始位置	找到威脅的位置 (如果有)。
電腦	發生威脅的電腦。
使用者	發現威脅時，登入電腦的使用者。
狀態	威脅目前的狀態。例如，目前狀態可能是已終止或已隔離。
目前位置	威脅目前的位置。例如，位置可能是「隔離所」。
主要動作	針對這個威脅所架構要採取的第一個動作。
次要動作	針對這個威脅所架構要採取的第二個動作。
動作敘述	針對威脅採取的動作敘述。
日期和時間	記錄威脅的日期和時間。

主動型威脅防護日誌：系統日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

在「系統日誌」中，您可以檢視與行為分析 (SONAR) 相關的系統事件。但不適當的動作或管理員不允許的動作是看不到的。

您可以在「主動型威脅防護系統日誌」中執行下列工作：

Table 112: 系統日誌選項

選項	說明
匯出	將資料儲存成逗點分隔 (.csv) 的檔案。
過濾器	過濾「系統日誌」資料。 當您選取此選項時，「過濾事件」對話方塊會出現。您可以選取想要在「系統日誌」中出現的項目。

您也可以滑鼠右鍵按下某個項目檢視其屬性。

Table 113: 系統日誌的各欄

欄名稱	說明
事件	所發生事件的說明。
登錄者	將 SONAR 顯示為 功能，該功能負責記錄事件。
電腦	起始或負責該事件的電腦。
使用者	在事件發生時登入至造成事件的電腦的使用者。
說明	針對威脅採取的動作敘述。
日期和時間	事件的記錄日期與時間。

強化日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

應用程式強化政策包括「應用程式控制」和「適配性隔離」，而系統管理員可以從雲端主控台對其進行管理。

使用應用程式控制日誌可尋找環境中不需要和未經授權的應用程式以及用戶端所攔截的行為。您的系統管理員會架構應用程式強化政策，以限制是否啟動應用程式以及它可以使用的系統資源。此政策使用可監控所指定檔案、資料夾和程序的規則和條件。

NOTE

應用程式控制和應用程式隔離事件使用相同的日誌。因此，「目前日誌檔大小」一律會相同。您可以分別檢視每個日誌，只篩選出事件。

欄	說明
日期和時間	事件的記錄日期與時間。
動作	顯示用戶端對嘗試執行的應用程式或程序所採取的下列其中一個動作。 - 已允許：執行應用程式或程序。用戶端不會記錄事件。 - 已攔截：未執行應用程式或程序，而且用戶端會記錄事件。 - 只記錄：在執行應用程式或程序時建立日誌事件。允許執行全部應用程式和程序。 應用程式控制政策處於監控模式時，可用的動作為「已攔截」或「只記錄」。已允許的應用程式不會記錄事件。
說明和活動	顯示用戶端在偵測到程序或檔案時對其採取的行為。如需這些事件的定義，請查看 ICDm 綱要 。在綱要中，尋找事件 ID，並選取它來尋找活動。例如，8027 是程序偵測事件 (安全事件)，可報告程序威脅或政策違規的偵測和解決方式。 8027：程序啟動 (應用程式控制) 22：政策覆寫 (應用程式控制)
規則名稱	規則名稱。如果規則名稱不存在，則此欄位空白。
登錄者	顯示已產生事件的賽門鐵克技術 (應用程式控制)。
呼叫程序 ID	觸發事件之呼叫程序的特徵。
呼叫程序	觸發事件之呼叫程序的路徑。例如，假設規則攔截程式寫入某個資料夾。如果您接著嘗試將文件儲存到該資料夾，則所記錄的事件會將 winword.exe 顯示為呼叫程序。
目標	很快就會提供。
指令行	執行中程序的指令引數或整個指令行。

過濾系統日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊，指定您想在病毒和安全風險的「系統日誌」中檢視的事件類型。其核取方塊沒有勾選的項目類型不會顯示在「系統日誌」中。此過濾器只控制日誌的顯示。所有事件類型會繼續寫入日誌。

用戶端管理日誌：系統日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「系統日誌」記錄所有的作業變更，例如服務開始時間和停止時間、偵測到網路應用程式、軟體組態修改以及軟體執行錯誤。「系統日誌」也會記錄與伺服器進行的通訊，包括連線及下載。「系統日誌」提供的所有資訊也會即時出現在訊息區中。「系統日誌」對用戶端的疑難排解特別有用。

您可以在「系統日誌」中執行下列工作：

- 檢視每當您的電腦連接至網路時的系統事件清單。
- 清除日誌中的所有項目。
- 將日誌中的資料匯出為 Tab 分隔文字檔案，以便在其他應用程式中使用。
- 根據時間範圍或嚴重性來過濾項目。

Table 114: 系統日誌的各欄

欄	說明
日期和時間	指出記錄事件的日期與時間。
嚴重性	指出下列嚴重性等級的資訊： • 錯誤 指出來源電腦發生問題。 • 警告 指出可能的問題。 • 資訊 提供涉及用戶端之事件的其他資訊，或提供與伺服器通訊相關的資訊。
摘要	描述事件。

用戶端管理日誌：安全日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「安全日誌」記錄可疑活動，例如通訊埠掃描、病毒攻擊，或阻斷服務攻擊。「安全日誌」是用戶端中最重要的日誌。

您可以在「安全日誌」中執行下列工作：

- 檢視與安全相關的事件。
- 清除日誌中的所有項目。
- 將日誌中的資料匯出為 Tab 分隔文字檔案，以便在其他應用程式中使用。
- 切換本機檢視和來源檢視。若要檢視來源通訊埠和主機及目的通訊埠和主機的欄，可以從「檢視」功能表選取「來源檢視」。
- 根據時間範圍或嚴重性來過濾項目。
- 回溯檢查用於嘗試攻擊的資料封包，以找出其來源。請注意，並非每個項目都可以回溯檢查。
- 讓用戶端停止攔截來自其他電腦的攻擊。

Table 115: 安全日誌欄

欄	說明
日期和時間	事件的記錄日期與時間。
事件類型	安全警示類型，例如服務阻斷攻擊、執行檔或病毒攻擊。
嚴重性	攻擊的嚴重性等級，包括下列選項： • 重要 • 主要 • 次要 • 資訊
方向	流量相對於用戶端電腦的傳遞方向： • 內送 攻擊大多數是入埠，因為是由另一台電腦所發起。 • 外寄 如特洛伊木馬程式的攻擊會視為離埠，因為這些攻擊已下載到您的電腦，已經存在。 • 不明 流量已被攔截或從作用中回應中斷，或因為應用程式執行檔已變更。
通訊協定	通訊協定的類型。例如，通訊協定可以是 UDP、TCP 或 ICMP。
遠端主機或來源主機	目前檢視中的主機，包括下列欄位： • 遠端主機 (本機檢視) 遠端電腦的 IP 位址。 • 來源主機 (來源檢視) 來源電腦的 IP 位址。
遠端通訊埠	TCP 埠號、UDP 埠號、遠端電腦的 ICMP 類型或程式碼。
遠端 MAC 或來源 MAC	目前檢視的 MAC 位址，包括下列欄位： • 遠端 MAC (本機檢視) 遠端電腦的 MAC 位址。如果位址在子網路以外，則是路由器的 MAC 位址。 • 來源 MAC (來源檢視) 來源電腦的 MAC 位址。
本機主機或目的主機	目前檢視中的主機，包括下列欄位： • 本機主機 (本機檢視) 本機電腦的 IP 位址 • 目的主機 (來源檢視) 目的電腦的 IP 位址。
本機通訊埠	TCP 埠號、UDP 埠號、或遠端電腦的 ICMP 類型或程式碼。
本機 MAC 或目的 MAC	目前檢視的 MAC 位址，包括下列欄位： • 本機 MAC (本機檢視) 本機電腦的 MAC 位址。 • 目的 MAC (來源檢視) 目的電腦的 MAC 位址。
應用程式	與攻擊關聯的應用程式名稱。
特徵 ID	攻擊觸發的入侵預防特徵的 ID。您可以使用此特徵 ID 在線上尋找特徵。
特徵子 ID	攻擊觸發的入侵預防特徵的子 ID。
特徵名稱	攻擊觸發的特徵名稱。
入侵 URL	與瀏覽器攻擊相關的 URL。
X-入侵-酬載 URL	攻擊將瀏覽器重新導向的目的地 URL。

欄	說明
使用者	傳送或接收流量的使用者或電腦。
使用者網域	用戶端登入的伺服器網域名稱。
位置	攻擊時有效的位址。 例如，位置可以是辦公室 (Office)、家用 (Home) 或 VPN。
發生次數	攻擊方法的發生次數。
開始時間	攻擊開始的時間。
結束時間	攻擊結束的時間。

竄改防護日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

您可以使用此日誌檢視關於「竄改防護」事件的資訊。當發生竄改嘗試時，您可以檢視此日誌，查看關於「竄改防護」偵測的詳細資料。

您可以在「竄改防護日誌」中執行下列工作：

- 檢視與「竄改防護」相關的事件清單。
- 將日誌中的資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。
- 在項目上按滑鼠右鍵，可檢視其屬性。

但不適當的動作或管理員不允許的動作是看不到的。

Table 116: 竄改防護日誌欄

選項	說明
電腦	發生竄改嘗試的電腦。
使用者	竄改嘗試時登入電腦的使用者名稱。
採取動作	「竄改防護」所採取的動作。
物件類型	所涉及的物件類型 (如果適用)。
事件	發生的事件。
參與者	發出攻擊的實體識別 (如果適用)。
目標	竄改嘗試的目標實體 (如果適用)。
目標程序	竄改嘗試的目標程序 (如果適用)。
日期和時間	記錄竄改嘗試的日期和時間。

防網路和主機侵入設定：日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此標籤可架構「控制日誌」、「封包日誌」、「用戶端管理安全日誌」和「流量日誌」。您可以設定日誌大小、指定每個日誌中項目的記錄天數，以及清除日誌。

Table 117: 日誌標籤選項

選項	說明
日誌檔大小上限	指定日誌檔的大小上限 (單位為 KB)。在到達大小上限之後，會移除最舊的項目，換成最新的項目。您可以設定介於 64 KB 到 15,000 KB (即 15 MB) 之間的大小。 Note: 建議盡量保持最小的日誌檔大小。
儲存每個日誌項目	指定項目從日誌中移除前的保留天數。
清除日誌	清除日誌中的所有項目。
啟用封包日誌	將封包資訊記錄到封包日誌。

用戶端管理日誌：控制日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「控制日誌」會記錄套用到用戶端的「應用程式與裝置控制」政策的結果。「應用程式與裝置控制」政策會防護登錄和特定檔案或目錄。也會控制程序、DLL 和應用程式的執行。

「控制日誌」會記錄應用程式行為專有的活動。這會記錄應用程式存取或執行的登錄機碼、檔案及 DLL。如果應用程式執行不被允許的活動，就會受到攔截。例如，提供網頁的 Web 伺服器不應該複製檔案到您的系統資料夾。

NOTE

控制日誌中一個事件可能會出現兩個日誌項目。例如，如果應用程式讀取並接著嘗試寫入檔案，則可能會出現兩個項目。如果應用程式寫入並接著嘗試刪除檔案，也會出現兩個項目。

Table 118: 控制日誌選項

欄	說明
日期和時間	記錄事件的日期和時間。
嚴重性等級	行為的嚴重性。
動作	不符合規則時，用戶端所採取的動作。 當系統程序嘗試在目標上執行作業時，用戶端會對應用程式或裝置採取下列其中一個動作： - 攔截 - 允許 - 繼續 觸發規則，但用戶端會忽略事件，只會記錄。 - 終止 用戶端終止程序。
測試模式	測試管理員可能會用到此資訊。
說明	用戶端行為敘述。
API	導致記錄此行為的 API 名稱。
規則名稱	導致記錄此行為的規則名稱。
IP 位址	應用程式或程序觸發此規則所使用的 IP 位址。
呼叫程序 ID	觸發記錄的應用程式或程序 ID。
呼叫程序	傳送錯誤的應用程式或程序名稱。
裝置實例 ID	用於 API 呼叫的參數。 參數會轉換成 STRING，並以空格字元隔開。
目標	程序或應用程式執行動作的目標。

欄	說明
檔案大小	應用程式或程序執行動作的檔案的大小。 檔案大小可能顯示為 0 位元組，而不是實際檔案大小。通常，當應用程式控制規則在程序建立或寫入檔案前觸發時，檔案大小會顯示為 0 個位元組。
使用者	電腦或使用者的名稱。
使用者網域	用戶端登入的伺服器網域名稱。
位置	應用程式已登入的位置名稱。

防網路和主機侵入日誌：流量日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用「流量日誌」來檢視防火牆事件的相關資訊，其中包括網路攻擊或入侵嘗試。日誌會顯示電腦連接至網路時的連入流量及連出流量清單。

下表顯示您可使用「流量日誌」功能表指令執行的工作。

Table 119: 流量日誌功能表指令

功能表	說明
檔案	可讓您執行下列工作： - 清除 移除日誌中的所有項目。 - 匯出 將日誌中的所有項目儲存為 Tab 分隔文字檔案，以便在其他應用程式中使用。 - 變更設定 (僅限非受管用戶端) 顯示可讓您修改「網路威脅防護設定」的對話方塊。 - 選項 (僅限受管用戶端) - 結束 關閉日誌。
編輯	可讓您執行下列工作： - 複製 將選取的日誌項目複製到剪貼簿。 - 全選 選取顯示的日誌項目。您可以將這些項目複製並貼到其他應用程式。
檢視	可讓您使用下列指令切換不同的日誌或不同的檢視： - 流量日誌或封包日誌 顯示其中一種日誌。 - 本機檢視和來源檢視 日誌中的直欄會根據您選擇的是本機檢視或來源檢視而改變。本機檢視會從本機通訊埠及遠端通訊埠的觀點來顯示內容。這種觀點較常用於主機型防火牆。來源檢視會從來源通訊埠及目的通訊埠的觀點來顯示內容。這種觀點較常用於網路型防火牆。 本機檢視和來源檢視顯示會同時出現在「本機檢視」和「來源檢視」的欄。
過濾器	顯示在指定天數內記錄或依嚴重性記錄的日誌項目。

功能表	說明
動作	可讓您執行下列工作： • 回溯檢查 找出資料封包的來源。您也許需要從用來進行攻擊的資料封包中找出來源主機。請注意，並非每個項目都可以回溯檢查。 • 停止主動回應 允許來自特定主機先前被用戶端封鎖的流量。 • 停止全部主動回應

若為受管用戶端，您可能無法存取所有的功能。不適合特定項目的動作都無法使用。

下表顯示會同時出現在本機檢視和來源檢視的表格欄。

Table 120: 本機檢視和來源檢視

欄	說明
日期和時間	事件的記錄日期與時間。
動作	用戶端對流量所採取的動作。用戶端會攔截或允許流量。
嚴重性	流量的嚴重性等級，範圍從 1 到 10。
方向	流量的方向，即連入或連出。
通訊協定	通訊協定的類型，即 UDP、TCP 或 ICMP。
遠端主機或來源主機	主控目前檢視的電腦，包括下列欄位： • 遠端主機 (本機檢視) 遠端電腦名稱。 • 來源主機 (來源檢視) 來源電腦名稱。
遠端 MAC 或來源 MAC	目前檢視的 MAC 位址，包括下列欄位： • 遠端 MAC (本機檢視) 遠端電腦的 MAC 位址。如果在子網路以外，則是路由器的 MAC 位址。 • 來源 MAC (來源檢視) 來源電腦的 MAC 位址。
遠端通訊埠或來源通訊埠	目前檢視中的通訊埠，包括下列欄位： • 遠端通訊埠 (本機檢視) 遠端電腦上的通訊埠和 ICMP 類型 (只出現在「本機檢視」)。 • 來源通訊埠 (來源檢視) 來源電腦上的通訊埠和 ICMP 類型 (只出現在「來源檢視」)。
本機主機或目的主機	目前檢視中的主機，包括下列欄位： • 本機主機 (本機檢視) 本機電腦的 IP 位址。 • 目的主機 (來源檢視) 目的電腦的 IP 位址。
本機 MAC 或目的 MAC	目前檢視的 MAC 位址，包括下列欄位： • 本機 MAC (本機檢視) 本機電腦的 MAC 位址。如果在子網路以外，則是路由器的 MAC 位址。 • 目的 MAC (來源檢視) 目的電腦的 MAC 位址。

欄	說明
本機通訊埠或目的通訊埠	目前檢視中的通訊埠，包括下列欄位： - 本機通訊埠 (本機檢視) 電腦上用於此封包的通訊埠。 - 目的通訊埠 (來源檢視) 目的電腦上用於此封包的通訊埠。
應用程式	與流量關聯的路徑和應用程式名稱。
使用者	使用者的登入名稱。
使用者網域	指出用戶端登入之伺服器網域的名稱。
位置	在流量期間有效的位置，例如辦公室 (Office)、家用 (Home)、VPN 等。
發生次數	流量在開始及結束時間期間傳送的封包數量。
開始時間	流量符合規則的開始時間。
結束時間	流量不再符合規則的時間。
規則	決定這個流量通過或攔截的規則。

如果防網路和主機侵入日誌和用戶端管理日誌中的項目有更多資訊可以提供時，這些資訊會顯示在下列位置：

- 「敘述」資訊會顯示在日誌檢視畫面的左下方窗格。
- 「資料」資訊會顯示在日誌檢視畫面的右下方窗格。

防網路和主機侵入日誌：封包日誌

Windows 適用的 Symantec Endpoint Protection 用戶端指南

「封包日誌」會擷取每個進出電腦通訊埠的資料封包。「封包日誌」會顯示入侵嘗試。

您可以在封包日誌中執行下列工作：

- 檢視每當您電腦連接至網路時的連入流量事件及連出流量事件清單。
- 清除日誌中的所有項目。
- 將資料匯出為 Tab 分隔文字檔案、網路監控格式或 NetXray 格式，以便在其他應用程式中使用。
- 切換本機檢視和來源檢視。若要檢視來源通訊埠和主機及目的通訊埠和主機的欄，可以從「檢視」功能表選取「來源檢視」。
- 選取時間範圍來過濾項目。
- 回溯檢查用於嘗試攻擊的資料封包，以找出其來源。請注意，並非每個項目都可以回溯檢查。

日誌檢視在左下方窗格中包含有關實際資料封包的資訊。右下角的窗格中顯示記錄的封包類型資料。

如果您或您的管理員停用了「封包日誌」，該日誌會停止記錄資訊。「封包日誌」預設為停用。

若為受管用戶端，您可能無法存取所有的功能。不適合特定項目的動作都無法使用。

Table 121: 封包日誌直欄

直欄或欄位	說明
日期和時間	記錄封包的日期與時間。
遠端主機或來源主機	主控目前檢視的電腦，包括下列欄位： - 遠端主機 (本機檢視) 遠端電腦名稱。 - 來源主機 (來源檢視) 來源電腦名稱。

直欄或欄位	說明
遠端通訊埠或來源通訊埠	目前檢視中的通訊埠，包括下列欄位： - 遠端通訊埠 (本機檢視) 遠端主機上收發封包的通訊埠。 - 來源通訊埠 (來源檢視) 來源主機上收發封包的通訊埠。
本機主機或目的主機	來源檢視中的 IP 位址，包括下列欄位： - 本地主機 (本機檢視) 本機電腦的 IP 位址。 - 目的主機 (來源檢視) 目的電腦的 IP 位址。
本機通訊埠或目的通訊埠	目前檢視中的通訊埠，包括下列欄位： - 本機通訊埠 (本機檢視) 電腦上用於此封包的通訊埠。 - 目的通訊埠 (來源檢視) 目的電腦上用於此封包的通訊埠。
方向	封包傳遞的方向： - 內送 - 外寄
動作	電腦採取的動作。 - 已攔截 - 已允許
應用程式	與封包關聯的應用程式名稱。
規則	有關套用到此封包的入侵預防規則或防火牆規則的資訊。

回溯檢查資訊

Windows 適用的 Symantec Endpoint Protection 用戶端指南

使用此對話方塊，可找出流量事件起始躍點之 IP 位址的相關詳細資訊。請注意，起始躍點的 IP 位址會列出流量連接所用之路由器的擁有者。不一定會列出真實的 IP 位址。

NOTE

您的網路架構可能會使回溯檢查功能無法正常運作。

Table 122: 回溯檢查欄位

選項	說明
躍點	躍點號碼 躍點是指資料封包從某台電腦傳到網路上另一台電腦所會經過的一個轉換點。路由器即是一個常見的轉換點。
IP 位址	流量會經過的每台電腦或路由器的 IP 位址。
名稱	發起流量事件的電腦。
時間 (ms)	尋找躍點 IP 位址所需的時間 (單位為毫秒)。
Who is >>	關於遠端 IP 位址的更詳細資訊，如組織名稱及聯絡資訊。

