



Symantec™ Endpoint Protection 14.3 RU10 安裝與管理指南

Updated: February 3, 2025

Table of Contents

版本說明	17
Symantec Endpoint Protection 14.3 RU10 的新功能？	17
Symantec Endpoint Protection 14.3 RU10 的已知問題	20
測試的虛擬安裝和虛擬化產品	22
Symantec Endpoint Protection 支援和培訓資源	23
如何提交功能要求或建立支援案例	23
什麼是 Symantec Endpoint Protection？	25
Symantec Endpoint Protection 功能	25
Symantec Endpoint Protection 架構元件	27
入門指南	30
Symantec Endpoint Protection 快速入門	34
安裝 Symantec Endpoint Protection Manager	42
架構 Symantec Endpoint Protection Manager 安裝	43
架構自訂 Symantec Endpoint Protection Manager 安裝	44
登入 Symantec Endpoint Protection Manager 主控台	47
啟用或匯入 Symantec Endpoint Protection 產品授權	50
購買 Symantec Endpoint Protection 授權	53
Symantec Endpoint Protection (SEP) 所需的外部 URL	53
使用儲存套件安裝 Symantec Endpoint Protection 用戶端	54
使用遠端推送安裝 Symantec Endpoint Protection 用戶端	55
使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端	57
安裝管理伺服器之後該做什麼？	58
Symantec Endpoint Protection 的通訊埠	59
安裝和解除安裝管理伺服器和用戶端	63
網路架構考量	63
關於選擇資料庫類型	63
關於基本管理伺服器設定	64
關於 SQL Server 架構設定	65
關於 SQL Server 資料庫驗證模式	67
國際化需求	69
將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2	69
了解 Symantec Endpoint Protection 和 FIPS 140-2 等級 1 遵從	72
支援 FIPS 140-2 等級 1 遵從的版本	73
FIPS 140-2 等級 1 遵從模式中不支援的功能和限制	74
針對 Symantec Endpoint Protection Manager 啟用或停用 FIPS 模式	74
安裝 SQL Server 資料庫憑證	75

關於 FIPS 遵從程式庫.....	78
關於已驗證模組.....	79
在 Symantec Endpoint Protection 上針對 FIPS 140-2 遵從問題進行疑難排解.....	80
管理 Symantec Endpoint Protection 用戶端安裝.....	80
準備 Windows 和 Mac 電腦進行遠端部署.....	81
選擇使用用戶端部署精靈安裝用戶端的方法.....	84
選擇要在用戶端上安裝哪些安全性功能.....	84
管理用戶端安裝套件.....	85
匯出用戶端安裝套件.....	86
將用戶端安裝套件匯入 Symantec Endpoint Protection Manager.....	87
Windows 用戶端安裝套件和內容更新大小.....	88
在 Symantec Endpoint Protection Manager 中建立自訂 Windows 用戶端安裝套件.....	88
關於 Windows 用戶端安裝設定.....	89
自訂用戶端安裝設定.....	89
移除現有第三方安全軟體.....	90
選擇使用用戶端安裝類型來下載雲端式還是本機式定義.....	91
Endpoint Protection/Endpoint Security 中的第三方安全軟體移除.....	92
Symantec Endpoint Security/Symantec Endpoint Protection 14.3 RU1 和更新版本中的第三方安全軟體移除.....	92
從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦.....	95
關於受管和非受管 (自我管理) 用戶端.....	96
檢查用戶端是受管用戶端還是非受管用戶端.....	97
如何取得非受管用戶端安裝套件.....	97
安裝非受管 Windows 用戶端.....	98
解除安裝 Symantec Endpoint Protection 用戶端.....	99
使用用戶端安裝設定來解除安裝 Symantec Endpoint Protection 用戶端 (14.3 RU9 和更早版本).....	101
解除安裝 Mac 的 Symantec Endpoint Protection 用戶端.....	101
刪除用戶端.....	102
升級和移轉到最新版本的 Symantec Endpoint Protection (SEP).....	103
Endpoint Protection 14.x 的升級最佳實務準則.....	104
Symantec Endpoint Protection 的升級資源.....	107
以 Microsoft Azure Code Signing (ACS) 支援升級 Windows 用戶端電腦至 14.3 RU8 及更新版本.....	108
最新版本 Symantec Endpoint Protection 支援和不支援的升級路徑.....	113
升級前增加 Symantec Endpoint Protection Manager 可用磁碟空間.....	114
升級管理伺服器.....	115
從內嵌資料庫升級到 Microsoft SQL Server Express 資料庫的最佳實務.....	115
在升級到 Microsoft SQL Server Express 之前，當資料庫已滿時減小資料庫大小.....	116
為 Microsoft SQL Server 資料庫啟用 FILESTREAM.....	117
在升級到 Microsoft SQL Server Express 之前，將資料庫大小減小到 10 GB 以下.....	118
挪出更多的可用磁碟空間以升級到預設 Microsoft SQL Server Express 資料庫.....	120
架構 Symantec Endpoint Protection Manager 與 Microsoft SQL Server 之間的加密通訊.....	121

Symantec Endpoint Protection Manager 偵測到已架構的電子郵件伺服器需要停用憑證驗證.....	135
解決 14.3 RU5 或更新版本安裝或升級後的 Microsoft SQL Server 資料庫連線錯誤.....	137
升級使用多個內嵌資料庫和管理伺服器的環境.....	144
在變更電腦的 IP 位址和主機名稱後重新架構 Symantec Endpoint Protection Manager	145
疑難排解伺服器名稱不符伺服器憑證時， Symantec Endpoint Protection Manager 會封鎖您登入或升級 (14.3 RU9 或更新版本).....	147
Symantec Endpoint Protection Manager 偵測到配置的複寫夥伴需要停用主機名稱驗證 (14.3 RU9 或更新版本).....	151
疑難排解：「##### IP #####」(14.3 RU8 或更新版本).....	154
停止及啟動管理伺服器服務.....	158
防止在升級期間複寫.....	159
還原複寫.....	160
選擇升級用戶端軟體的方法.....	160
使用自動升級來升級用戶端軟體.....	161
將自動升級設定套用至其他群組.....	163
使用用戶端升級政策升級用戶端軟體.....	164
將 Symantec Endpoint Protection 14.3 RU2+ 升級為支援的語言.....	166
在 Windows 用戶端上安裝 Endpoint Protection 用戶端修補程式.....	167
升級群組更新提供者.....	168
移轉至 SES 雲端主控台	169
移轉到 Symantec Endpoint Security 雲端主控台的好處.....	169
內部部署、混合或完全雲端管理選項.....	170
向雲端伺服器註冊 Symantec Endpoint Protection Manager 網域.....	172
以雲端伺服器 (14.3 RU3 或更新版本) 註冊 Symantec Endpoint Protection Manager	177
將 Symantec Endpoint Protection Manager 網域註冊到雲端伺服器後，我該如何管理用戶端和政策？.....	180
混合管理 Symantec Endpoint Protection Manager (SEPM) 如何與 Symantec Endpoint Security (SES) 雲端主控台互動.....	182
內部部署 SEPM 和雲端註冊的 SEPM 之間的功能差異.....	185
針對混合 Symantec Endpoint Protection Manager 、用戶端與雲端伺服器之間的通訊問題進行疑難排解.....	188
「進階安全性」頁面問題疑難排解.....	190
Symantec Endpoint Protection Manager 例外政策如何與 Symantec Endpoint Security (SES) 雲端主控台互動？.....	192
向雲端伺服器中的遠端複製夥伴註冊網站.....	194
在低頻寬環境中更新用戶端.....	196
從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端.....	198
從雲端伺服器取消註冊 Symantec Endpoint Protection Manager 網域.....	199
授權 Symantec Endpoint Protection	200
我的 Symantec Endpoint Protection 授權何時到期？.....	201
如何接收 Symantec Endpoint Protection 授權到期通知？.....	201
授權到期或過度部署後會發生的情況 (SEP 或 SES)。.....	202
刪除過時授權，以釋放更多授權.....	206

Symantec Endpoint Protection 授權涵蓋哪些方面？	207
備份和復原授權檔案 (.slf)	207
關於多年授權	208
Symantec Endpoint Protection 產品授權術語	208
授權非受管 Windows 用戶端	209
使用政策管理安全性	210
阻止惡意軟體和其他威脅的最佳實務	210
使用 Symantec Endpoint Protection 的勒索軟體緩和與防護	211
使用 Symantec Endpoint Protection 的勒索軟體防護	213
living-off-the land 技術勒索軟體防護的最新功能 (SES 和 SEP)	215
如何使用 Symantec Endpoint Protection 封鎖網站？	217
執行適用於所有政策的工作	218
安全性政策類型	220
在 Windows 用戶端上更新安全政策	221
建立自訂 Symantec Endpoint Protection Manager 政策	221
編輯政策	222
尋找政策的預設設定	222
在「政策」頁面中複製和貼上政策	223
在「用戶端」頁面上複製並貼上政策	223
指派政策給群組或位置	224
取代政策	224
匯出和匯入個別 Endpoint Protection 政策	225
關於共用和非共用政策	226
將共用政策轉換為非共用政策	227
從群組或位置解除指派政策	227
啟用應用程式探索	228
搜尋有關電腦執行之已探索應用程式的資訊	229
透過自適應防護攔截 Living Off the Land (LOTL) 攻擊	230
Symantec Endpoint Protection 與 Symantec Endpoint Security 之間的自適應防護功能比較	235
輕度註冊如何運作？	236
調適型防護如何收集感染狀況和事件計數？	236
行為規則	237
自適應防護政策 - 進階設定	238
從雲端而不是從 Symantec Endpoint Protection Manager 管理自適應防護	238
檢視 Symantec Endpoint Protection Manager 上的雲端分析資安事端 (14.3 RU8 和更新版本)	241
管理防火牆防護	243
防火牆的運作方式	243
關於 Symantec Endpoint Protection 防火牆	244
建立防火牆政策	244
從 Symantec Endpoint Protection Manager 管理防火牆規則	246

新增防火牆規則.....	247
關於防火牆伺服器規則和用戶端規則.....	247
防火牆處理防火牆規則和設定的順序.....	248
變更防火牆規則的順序.....	249
關於繼承的防火牆規則.....	250
新增繼承自父群組的防火牆規則.....	251
防火牆如何使用狀態式檢測.....	251
關於防火牆規則應用程式觸發條件.....	251
關於防火牆規則主機觸發條件.....	254
新增主機群組.....	256
關於防火牆規則網路服務觸發條件.....	256
新增網路服務至預設網路服務清單.....	256
關於防火牆規則網路配接卡觸發條件.....	257
將自訂網路配接卡新增到網路配接卡清單.....	258
複製 Symantec Endpoint Protection 防火牆規則.....	258
自訂防火牆規則.....	259
架構混合控制的防火牆設定.....	266
為網路服務啟用通訊而非新增規則.....	266
自動攔截連線至攻擊電腦.....	267
偵測潛在的攻擊和詐騙嘗試.....	268
防止對電腦的外部隱藏攻擊.....	268
關於 Mac 用戶端的防火牆設定.....	269
停用 Windows 防火牆.....	269
架構入侵預防.....	270
啟用入侵預防.....	278
整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站.....	278
使用 HKEY_CURRENT_USER 機碼安裝 Chrome 或 Edge 的 Endpoint Protection Browser 延伸.....	285
設定排除的電腦清單.....	288
針對入侵預防和記憶體攻擊緩和架構用戶端通知.....	289
關於賽門鐵克 IPS 特徵.....	289
為 IPS 特徵建立例外.....	290
關於自訂 IPS 特徵.....	291
管理自訂入侵預防特徵.....	291
建立自訂 IPS 特徵庫.....	292
將特徵新增至自訂 IPS 特徵庫.....	293
變更自訂 IPS 特徵的順序.....	294
定義自訂 IPS 特徵的變數.....	294
指派多個自訂 IPS 特徵庫至群組.....	295
測試自訂 IPS 特徵.....	295
使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊.....	295

Symantec Endpoint Protection 記憶體攻擊緩和技術.....	299
阻止和處理病毒和間諜軟體對用戶端電腦的攻擊.....	301
移除病毒和安全風險.....	302
識別受感染及有風險的電腦.....	303
檢查掃描動作及重新掃描識別出的電腦.....	303
Windows 用戶端如何從雲端接收定義檔.....	304
在用戶端電腦上管理掃描.....	306
關於掃描和即時防護的類型.....	307
關於自動防護的類型.....	308
關於病毒和安全風險.....	310
關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾.....	311
關於預設的病毒和間諜軟體防護政策掃描設定.....	313
Symantec Endpoint Protection 處理病毒和安全性風險偵測結果的方式.....	315
Symantec Endpoint Protection 如何在 Windows 8 電腦上處理偵測.....	316
設定在 Windows 電腦上執行的排程掃描.....	316
設定在 Mac 電腦上執行的排程掃描.....	317
設定在 Linux 電腦上執行的排程掃描.....	318
在用戶端電腦上執行隨選掃描.....	319
調整掃描以改善電腦效能.....	319
調整掃描以增強對用戶端電腦的防護.....	321
管理「下載鑑識」偵測.....	323
Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策.....	325
Symantec Endpoint Protection 如何使用進階機器學習？.....	325
Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？.....	327
管理 Windows 用戶端的隔離所.....	328
使用自訂 YARA 規則掃描 SEP 用戶端電腦.....	330
管理顯示在用戶端電腦上的病毒和間諜軟體通知.....	332
關於出現在 Windows 8 用戶端上的彈出式通知.....	333
啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知.....	334
管理提早啟動防惡意軟體 (ELAM) 偵測.....	334
調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項.....	335
架構站台使用私用 Insight 伺服器進行信譽查詢.....	336
將用戶端架構為使用 Symantec EDR 或私用伺服器進行信譽查詢和提交.....	336
自訂病毒和間諜軟體掃描.....	337
自訂在 Mac 電腦上執行的病毒和間諜軟體掃描.....	339
自訂在 Linux 電腦上執行的病毒和間諜軟體掃描.....	339
自訂 Windows 用戶端的自動防護.....	340
自訂 Mac 用戶端的自動防護.....	341
自訂 Linux 用戶端的自動防護.....	342
為 Windows 電腦上的電子郵件掃描自訂自動防護.....	343

為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描.....	344
為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描.....	344
為在 Linux 電腦上執行的用戶端自訂管理員定義掃描.....	345
隨機設定掃描以在 Windows 用戶端上的虛擬環境中改善電腦效能.....	346
修改全域掃描設定.....	346
在 Windows 電腦上修改日誌處理及通知設定.....	347
在 Linux 電腦上修改日誌處理設定.....	347
自訂下載鑑識設定.....	348
變更 Symantec Endpoint Protection 進行偵測時採取的動作.....	348
允許使用者在 Windows 電腦上暫停或停止掃描.....	350
架構 Windows 資訊安全中心通知以搭配 Symantec Endpoint Protection 用戶端使用.....	351
提交 Symantec Endpoint Protection 遙測資料以提高安全性.....	351
瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性.....	358
管理用戶端傳送給賽門鐵克的匿名或非匿名資料.....	359
Symantec Endpoint Protection 如何最大限度降低用戶端傳送資訊對網路頻寬的影響.....	360
指定用於用戶端傳送資訊和其他外部通訊的 Proxy 伺服器.....	360
管理行為分析 (SONAR).....	361
何謂 Symantec Endpoint Protection 中的行為分析 (SONAR) ?	362
處理和避免行為分析 (SONAR) 偵測誤報.....	363
調整用戶端電腦上的 SONAR 設定.....	364
監控行為分析 (SONAR) 偵測結果來查看是否有誤報.....	364
使用竄改防護保護 Symantec Endpoint Protection 程序和資源.....	365
應用程式控制、系統鎖定和裝置控制.....	366
設定應用程式控制.....	366
啟用和測試預設應用程式規則.....	367
應用程式控制與裝置控制政策的結構.....	368
將自訂規則新增至應用程式控制.....	368
新增應用程式控制規則時的最佳實務準則.....	370
選擇用於規則之條件的最佳實務準則.....	371
測試應用程式控制規則.....	372
設定系統鎖定.....	373
建立檔案指紋清單.....	376
在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單.....	378
匯入檔案指紋清單的最佳實務 (適用於 SEP 14.3 RU5 及更新版本).....	379
更新 Symantec Endpoint Protection Manager 中的檔案指紋清單.....	380
系統鎖定與 Symantec EDR 拒絕清單 (黑名單) 規則之間的互動.....	381
建立應用程式名稱清單以匯入系統鎖定架構中.....	381
自動更新系統鎖定的檔案指紋清單來允許或攔截.....	382
建立 index.ini 檔案以供自動更新用於系統鎖定的允許清單拒絕清單.....	383
針對系統鎖定啟用允許清單和拒絕清單的自動更新.....	384

針對檔案指紋清單憑證問題進行疑難排解.....	385
啟用系統鎖定前設定和測試系統鎖定架構.....	385
使用「裝置控制」和「應用程式控制」封鎖或允許裝置.....	386
新增「裝置控制」政策規則，以允許或封鎖用戶端電腦上的裝置.....	393
新增硬體裝置至硬體裝置清單中.....	394
使用 DevViewer 取得 Windows 電腦的裝置廠商或型號.....	394
Endpoint Protection 中的 Mac 裝置控制.....	395
使用 DeviceInfo 取得 Mac 裝置的裝置廠商、型號或序號.....	397
「應用程式控制」如何封鎖設備.....	397
將例外套用於 Symantec Endpoint Protection 中的掃描.....	398
針對哪種類型的掃描使用哪些 Windows 例外？.....	398
建立病毒和間諜軟體掃描的例外.....	399
從掃描中排除檔案或資料夾.....	401
從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險.....	403
從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名.....	403
建立應用程式例外.....	404
從 Windows 用戶端上的掃描中排除信任的 Web 網域.....	405
在 Windows 用戶端上建立竄改防護例外.....	405
針對會變更 DNS 或主機檔案的應用程式建立例外.....	406
在 Windows 用戶端上從掃描中排除憑證.....	406
限制使用者可在用戶端電腦上架構的例外類型.....	407
從日誌事件建立例外.....	407
使用 Web 和雲端存取防護控制網路存取.....	409
何謂 Web 和雲端存取防護？.....	411
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.....	415
在瀏覽器中測試 Web 和雲端存取防護 政策.....	417
架構 Web 和雲端存取防護的 WSS 代理程式攔截通知服務.....	418
將 Web 和雲端存取防護從 PAC 檔案重新導向方法移轉至通道方法.....	420
疑難排解 Web 和雲端存取防護.....	422
管理 Mac 用戶端的 Web 和雲端存取防護.....	425
Web 和雲端存取防護設定.....	426
測試 Symantec Endpoint Protection Manager 政策.....	428
測試病毒和間諜軟體防護政策.....	429
攔截程序在用戶端電腦上啟動.....	429
防止使用者寫入用戶端電腦上的登錄.....	430
防止使用者寫入特定檔案.....	430
新增和測試攔截 DLL 的規則.....	431
新增和測試終止程序的規則.....	432
測試預設 IPS 政策.....	432
管理用戶端伺服器連線.....	434

改善用戶端和伺服器效能.....	434
關於伺服器憑證.....	436
接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證.....	436
在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證.....	437
更新或還原伺服器憑證.....	439
檢查用戶端是否已連線至管理伺服器且受保護.....	440
Symantec Endpoint Protection 用戶端狀態圖示.....	441
使用政策序號檢查用戶端伺服器通訊.....	442
使用推送模式或提取模式更新用戶端上的政策和內容.....	442
用戶端電腦和管理伺服器的通訊方式？.....	444
在用戶端電腦上取代用戶端伺服器通訊檔案.....	445
使用 SylinkDrop 工具還原用戶端伺服器通訊設定.....	446
使用「通訊更新套件部署」還原用戶端伺服器通訊.....	447
手動匯出和匯入用戶端伺服器通訊檔案 (Sylink.xml).....	447
將用戶端伺服器通訊設定匯入 Linux 用戶端.....	448
IPv6 網路支援.....	449
設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊.....	449
尋找可用的通訊埠.....	450
針對用戶端通訊變更 Apache 的 HTTPS 通訊埠.....	450
啟用 HTTPS 用戶端伺服器通訊.....	451
管理群組、用戶端、管理員、密碼和網域.....	453
管理用戶端群組.....	453
如何設定群組結構.....	454
新增群組.....	454
以 Symantec Endpoint Protection Manager (SEPM) 來同步 Active Directory 群組.....	455
Active Directory 的組織單位是什麼？.....	460
將 Symantec Endpoint Protection Manager 連線至目錄伺服器.....	460
連線至遠端複製網站上的目錄伺服器.....	461
從目錄伺服器匯入組織單位.....	462
停用群組繼承.....	462
防止用戶端電腦被加入至群組.....	462
將用戶端電腦移至其他群組.....	463
管理用戶端電腦.....	464
檢視用戶端電腦的防護狀態.....	465
在用戶端電腦上啟用防護.....	466
搜尋未安裝用戶端軟體的用戶端.....	467
在 Symantec Endpoint Protection Manager 中搜尋用戶端電腦的資訊。.....	467
什麼是可對用戶端電腦執行的指令？.....	468
在用戶端電腦上從主控台執行指令.....	469
確保用戶端不會重新啟動.....	470

在使用者模式和電腦模式之間切換 Windows 用戶端.....	470
將用戶端架構為偵測非受管裝置.....	471
用密碼保護 Symantec Endpoint Protection 用戶端.....	472
防止使用者停用 Symantec Endpoint Protection 用戶端.....	474
允許使用者變更 Symantec Endpoint Protection 用戶端使用者介面的設定.....	475
收集使用者資訊.....	477
使用 AppleScript 程序檔檢查 Mac 用戶端.....	477
管理遠端用戶端.....	479
管理遠端用戶端的位置.....	480
啟動用戶端位置偵測.....	481
將位置新增到群組.....	482
變更預設位置.....	483
設定第一種狀況的位置偵測條件.....	483
設定第二種狀況的位置感應條件.....	484
架構位置的通訊設定.....	486
關於加強遠端用戶端的安全性政策.....	486
針對遠端用戶端之防火牆政策設定的最佳實務準則.....	487
關於開啟遠端用戶端的通知.....	487
關於從管理伺服器監控遠端用戶端.....	487
管理管理員帳戶和密碼.....	488
關於管理員帳戶和存取權限.....	489
新增管理員帳戶和設定存取權限.....	490
選擇管理員帳戶的驗證方法.....	491
搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID 驗證.....	492
使用 Symantec VIP 架構雙因素驗證.....	493
使用智慧卡架構驗證.....	494
測試管理員帳戶的目錄伺服器驗證.....	499
使用多因素驗證為 LDAP 伺服器架構 Okta (14.3 RU8 或更新版本).....	502
Symantec Endpoint Protection Manager 密碼遺失後重設.....	503
顯示「忘記了您的密碼？」連結，以便管理員可以重設遺失密碼.....	504
尋找 Symantec Endpoint Protection Manager 管理員電子郵件地址.....	504
Symantec Endpoint Protection Manager 的帳戶名稱和密碼要求.....	505
變更管理員帳戶或預設資料庫的密碼.....	506
架構全域密碼需求.....	507
使 Symantec Endpoint Protection Manager 登入密碼永久有效.....	508
在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息.....	508
在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊.....	509
允許或攔截存取遠端 Symantec Endpoint Protection Manager 主控台.....	509
在嘗試太多次登入後解除鎖定管理員帳戶.....	510
變更保持登入 Symantec Endpoint Protection Manager 主控台的逾時期間.....	511

關於網域.....	512
新增網域.....	513
切換至目前的網域.....	513
如何更新用戶端上的內容和定義檔.....	514
選擇派送方法以更新用戶端上的內容.....	515
選擇派送方法以根據平台來更新用戶端上的內容.....	519
將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager	519
確認 Symantec Endpoint Protection Manager 具有最新內容.....	521
關於 LiveUpdate 下載的內容類型.....	522
將用戶端架構為從內部 LiveUpdate 伺服器下載內容.....	526
架構用戶端從外部 LiveUpdate 伺服器下載內容.....	528
架構 Symantec Endpoint Protection Manager 連線到 Proxy 伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容.....	529
指定用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器.....	529
針對用戶端電腦架構 LiveUpdate 下載排程.....	530
架構使用者對 LiveUpdate 的控制能力.....	531
減少用戶端更新要求的網路超載.....	531
關於隨機進行同時內容下載.....	532
從預設管理伺服器或群組更新提供者隨機進行內容下載.....	532
減少因同步 SEP 用戶端 LiveUpdate 內容下載而造成的網路壅塞.....	533
將 Windows 用戶端更新架構為在用戶端電腦閒置時執行.....	533
將 Windows 用戶端更新架構為在定義檔太舊或電腦已中斷連線時執行.....	534
將用戶端架構為從 Symantec Endpoint Protection Manager 下載內容.....	534
在 Windows 用戶端上發布之前測試引擎更新.....	535
驗證用戶端電腦上所執行的引擎和定義檔.....	537
還原為舊版 Symantec Endpoint Protection 安全更新.....	538
使用群組更新提供者將內容散佈至用戶端.....	539
關於群組更新提供者的類型.....	539
將 Windows 用戶端架構為從群組更新提供者下載內容.....	541
搜尋作為群組更新提供者的用戶端.....	542
在您的網路中架構多種類型的群組更新提供者.....	542
使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容.....	543
使用第三方派送工具更新用戶端電腦.....	544
將 LiveUpdate 設定政策架構為允許將第三方內容派送至受管用戶端.....	545
準備非受管用戶端以從第三方派送工具接收更新.....	545
使用第三方派送工具派送內容.....	546
監控、報告和強制執行合規性.....	548
架構主機完整性.....	548
主機完整性的運作方式.....	549
關於主機完整性需求.....	550

將預先定義的需求新增至主機完整性政策.....	551
設定預先定義主機完整性需求的矯正.....	551
允許使用者延遲或取消主機完整性矯正.....	552
架構主機完整性檢查頻率的設定.....	553
允許主機完整性檢查在需求失敗時通過.....	553
架構主機完整性檢查的通知.....	553
針對失敗的主機完整性檢查建立隔離所政策.....	554
產生主機完整性檢查失敗的電腦清單.....	554
透過架構點對點驗證攔截遠端電腦.....	555
透過匯入範本建立主機完整性政策需求.....	556
撰寫自訂的需求指令碼.....	556
關於登錄條件.....	557
撰寫要在用戶端執行指令碼的自訂需求.....	558
撰寫要設定檔案時間戳記的自訂需求.....	559
編寫自訂需求以增加登錄 DWORD 值。.....	559
使用自訂需求程序檔建立測試主機完整性政策.....	560
監控 Symantec Endpoint Protection 用戶端.....	561
尋找未掃描電腦.....	563
尋找離線電腦.....	564
產生網路中安裝的 Symantec Endpoint Protection 版本的清單.....	564
執行有關用戶端部署狀態的報告.....	565
檢視風險.....	565
檢視攻擊目標和來源.....	565
檢視 Symantec Endpoint Protection 報告.....	566
檢視系統防護.....	566
架構報告偏好.....	566
從獨立式網頁瀏覽器登入報告.....	567
關於 Symantec Endpoint Protection Manager 報告類型.....	568
執行和自訂快速報告.....	574
使用過濾器建立自訂報告.....	574
新增並執行排程報告.....	575
列印和儲存報告副本.....	576
檢視日誌.....	576
關於 Symantec Endpoint Protection Manager 日誌類型.....	577
使用過濾儲存和刪除自訂日誌.....	578
檢視其他站台的日誌.....	579
將資料匯出至 Syslog 伺服器.....	579
將日誌資料匯出至文字檔.....	580
為外部日誌記錄架構容錯移轉伺服器.....	581
管理通知.....	581

通知的運作方式.....	582
有哪些類型的通知，何時傳送它們？.....	583
關於合作夥伴通知.....	585
建立管理伺服器與電子郵件伺服器之間的通訊.....	585
檢視和認可通知.....	585
儲存和刪除管理通知過濾器.....	586
設定管理員通知.....	586
從其他版本升級會如何影響通知條件.....	587
管理管理伺服器、網站和資料庫.....	589
關於 Symantec Endpoint Protection 伺服器的類型.....	589
匯出和匯入伺服器設定.....	589
管理 Symantec Endpoint Protection Manager 伺服器和第三方伺服器.....	590
維護資料庫.....	591
執行自動資料庫備份.....	593
排程自動資料庫維護工作.....	593
增加 Microsoft SQL Server 資料庫檔案大小.....	594
指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器.....	594
指定日誌大小以及在資料庫中保留日誌項目的時間長度.....	595
關於增加用於用戶端日誌資料的伺服器磁碟空間.....	595
從資料庫手動清除日誌資料.....	596
設定容錯移轉和負載平衡.....	596
關於容錯移轉和負載平衡.....	597
架構用於負載平衡的管理伺服器清單.....	599
安裝管理伺服器以進行容錯移轉或負載平衡.....	600
指派管理伺服器清單至群組和位置.....	600
取代管理伺服器清單.....	601
設定站台和複寫.....	601
什麼是站台以及複寫如何運作？.....	602
如何解決遠端複製期間網站之間的資料衝突.....	605
決定是否要設定多個網站和複寫.....	606
判斷需要的網站數量.....	607
如何安裝第二個站台用於遠端複製.....	608
變更遠端複製頻率和內容.....	609
立即遠端複製資料.....	610
刪除站台.....	610
Endpoint Protection 的災難復原最佳實務準則.....	610
備份資料庫和日誌.....	612
備份伺服器憑證.....	612
重新安裝或重新架構 Symantec Endpoint Protection Manager.....	613
產生新的伺服器憑證.....	614

還原資料庫.....	614
具 Symantec Endpoint Protection 的虛擬環境.....	616
關於共用智慧型掃描快取.....	616
關於虛擬映像例外工具.....	617
我必須怎麼做才能使用網路型共用智慧型掃描快取？.....	617
實作網路型共用智慧型掃描快取的系統需求.....	617
安裝和移除網路型共用智慧型掃描快取.....	618
啟用網路型共用智慧型掃描快取.....	619
自訂共用智慧型掃描快取設定.....	620
關於停止和啟動網路型共用智慧型掃描快取服務.....	622
檢視網路型共用智慧型掃描快取日誌事件.....	622
監控網路型共用智慧型掃描快取效能計數器.....	623
排除共用智慧型掃描快取問題.....	624
在基礎影像上使用虛擬映像例外工具.....	624
虛擬映像例外工具的系統需求.....	625
執行虛擬映像例外工具.....	625
架構 Symantec Endpoint Protection 以略過基礎影像檔掃描.....	625
在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection (NPVDIs).....	626
針對非持續 VDI (NPVDIs) 中的非持續訪客虛擬機器設定基礎影像.....	626
清除過時的非持續 (NPVDI) 用戶端以釋放授權.....	627
如何管理非持續虛擬桌面基礎架構 (NPVDI) 用戶端的授權計數.....	627
viptool.....	628
viptool.....	628
API.....	629
Symantec Endpoint Protection API 指令.....	629
Symantec Endpoint Protection 疑難排解.....	634
使用 SymDiag 進行 Windows 用戶端健康狀態疑難排解和檢查.....	635
於安裝或升級期間在 Microsoft Windows Server 2008 R2 上啟用 TLS 1.0 和 1.1.....	635
找出用戶端安裝的失敗點.....	637
Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解.....	638
在用戶端電腦上檢查與管理伺服器的連線.....	639
在用戶端上使用疑難排解檔案調查防護問題.....	639
啟用並檢視存取日誌，以檢查用戶端是否連線到管理伺服器.....	639
停止和啟動 Apache Web 伺服器.....	640
使用 ping 指令測試與管理伺服器的連線.....	640
使用瀏覽器測試與 Symantec Endpoint Protection Manager 用戶端上的 Symantec Endpoint Protection 的連線... 641	
檢查用戶端電腦上的除錯日誌.....	641
檢查管理伺服器上的收件匣日誌.....	641
Symantec Endpoint Protection Linux Agent 或 Symantec Single Agent for Linux 疑難排解.....	642

疑難排解 Symantec Endpoint Protection Manager 與主控台或預設資料庫之間的通訊問題.....	642
驗證管理伺服器與資料庫的連線.....	643
用戶端與伺服器通訊檔案.....	645
報告問題疑難排解.....	645
變更檢視報告和日誌的逾時參數.....	646
在停用回送位址時存取報告頁面.....	647
從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前應了解的事項.....	648
需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作.....	650
從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析.....	652
回應 Power Eraser 偵測.....	653
附錄.....	656
Symantec Endpoint Protection 功能 (依平台分類).....	656
Windows 用戶端的 Symantec Endpoint Protection 功能相依性.....	664
Symantec Endpoint Protection 隨附的工具.....	666
Symantec Endpoint Protection 和 Symantec Endpoint Security 中適用於 Windows 用戶端服務 smc 的指令.....	670
smc.exe 指令錯誤碼.....	675
使用第三方工具安裝 Windows 用戶端軟體.....	676
關於用戶端安裝功能和屬性.....	676
關於架構 MSI 指令字串.....	677
關於架構 Setaid.ini.....	677
Symantec Endpoint Protection 指令行用戶端安裝屬性.....	677
使用指令行安裝 Symantec Endpoint Protection 用戶端功能.....	678
Windows Installer 參數.....	679
Windows 資訊安全中心屬性.....	680
安裝 Windows 用戶端的指令行範例.....	681
使用 Microsoft SCCM/SMS 安裝 Windows 用戶端.....	681
使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端.....	682
建立 GPO 軟體派送.....	683
將電腦新增到組織單位以安裝軟體.....	684
複製 Sylink.xml 檔案以製作受管安裝套件.....	684
使用 Active Directory 群組原則物件解除安裝用戶端軟體.....	685
Amazon Web Services 的 Symantec™ Endpoint Protection 快速入門指南.....	685
Documentation Legal Notice.....	688

版本說明

取得有關 Symantec Endpoint Protection 的最新資訊。

Symantec Endpoint Protection 的新功能

Symantec Endpoint Protection 的每個版本皆會有[新功能](#)、[新修正](#)和[已知問題](#)更新。您還可以閱讀[封存檔案](#)，以獲取有關舊版本的資訊。

系統需求

瞭解工作站和伺服器的最新 Symantec Endpoint Security [系統要求](#)。

每個 Symantec Endpoint Protection 版本也都會具有其所支援的特定 [Linux 核心版本範圍](#)。

授權

下訂單之後，請務必[啟動](#) Symantec Endpoint Protection 授權。

您可以透過 [Broadcom 銷售](#)或您的[客戶經理](#)或您所在地區或國家的 [Broadcom 授權合作夥伴或經銷商](#)購買新產品和授權、續訂過期授權以及訂閱服務。

您或您的合作夥伴必須提供以下資訊：

- 目前網站 ID
- 前一訂單中使用的電子郵件地址
- 帳戶 ID

如需詳細瞭解更多授權相關資訊，請參閱[授權 Symantec Endpoint Protection](#)

若要取得該軟體試用版，請參閱 [Broadcom 試用軟體和概念證明示範](#)。

技術支援

如需技術支援，請參閱[如何提交功能要求或建立支援案例](#)或 [Symantec Endpoint Protection 支持和培訓資源](#)。

語言

在 2022 年，Symantec Endpoint Protection 文件已停止翻譯為捷克文、德文、義大利文、韓文、波蘭文或俄文。若要取得最新主題，請按一下頁面頂端的下拉式箭頭。文件仍然翻譯為法文、日文、巴西葡萄牙文、西班牙文和中文 (簡體和繁體)。

勒索軟體防護的新功能

Symantec Endpoint Protection (SEP) 包括[勒索軟體防護](#)增強功能，可讓用戶端電腦防禦 living-off-the-land (LOTL) 工具，以及惡意軟體市場中可用的檔案、網路工具和其他一般攻擊工具。

Symantec Endpoint Protection 14.3 RU10 的新功能？

本節描述此版本中的新功能。

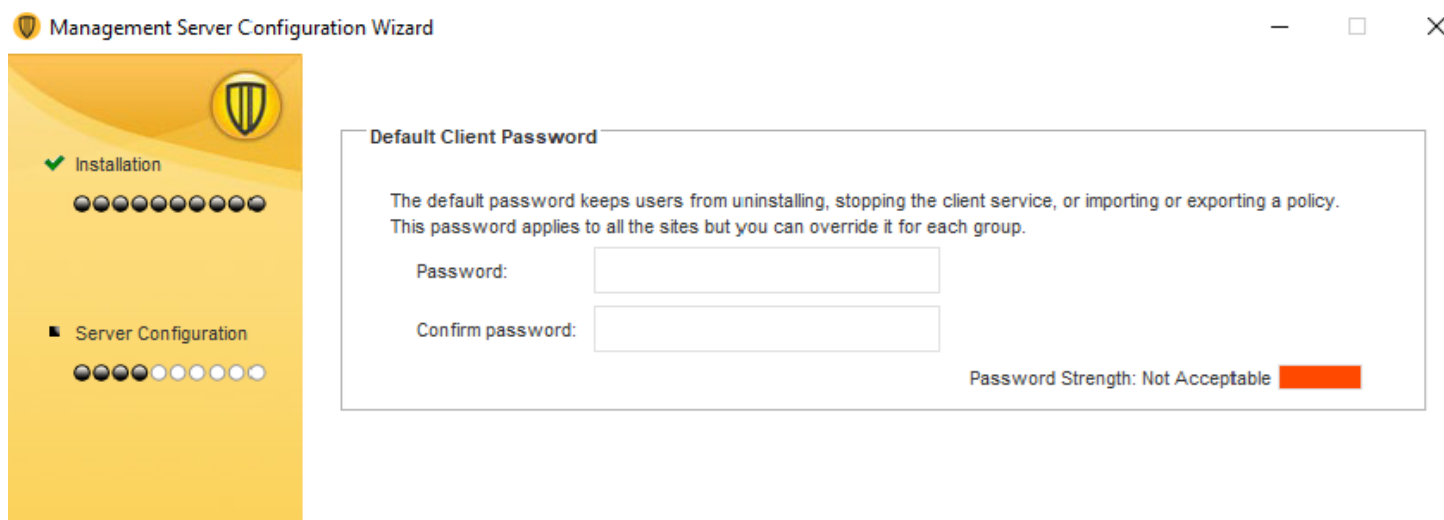
防護功能

- 您現在可以在內部部署 Symantec Endpoint Protection Manager 中完全架構和管理自適應防護政策，而不是僅能在雲端中。調適型防護使用豐富的行為分析引擎以及全球威脅遙測和專業知識來保護您的組織免於受到鎖定攻擊。您可以使用

「進階安全性」頁面上的熱圖來檢視感染狀況行為和相關聯的 MITRE 技術。您接著可以使用自適應防護政策來自動攔截不受信任的行為或手動允許信任的行為。

[透過自適應防護攔截 Living Off the Land \(LOTL\) 攻擊](#)

- 為了更好地防止攻擊者停止或移除 Symantec Endpoint Protection 用戶端，您需要設定網站層級的預設用戶端密碼。用戶端使用者必須鍵入密碼，才能執行下列工作：
 - 使用 `smc - stop` 命令來停止用戶端服務。
 - 手動或使用 CleanWipe 工具來解除安裝用戶端。
- [下載 CleanWipe 移除工具來解除安裝 Endpoint Protection](#)
- 匯入或匯出政策。
 - 使用 Sylink.xml 檔案來匯入用戶端通訊設定檔案。
- 您可以在管理伺服器安裝或升級期間設定預設用戶端密碼。



[安裝後架構 Symantec Endpoint Protection Manager](#)

- 安裝之後，您可以在群組層級變更密碼。在舊版本中，這些功能是「用戶端」>「政策」標籤>「密碼」對話方塊中的選用核取方塊。



Client Password Settings for My Company



☒ Use the default client password

☐ Use a group client password

Password:

Confirm password:

☐ Require a password to open the client user interface

☒ Require a password to run CleanWipe on the client

☒ Require a password to uninstall the client

☒ Require a password to stop the client service

☒ Require a password to import or export a policy and import client communication settings

OK

Cancel

Help

– 為了進一步防止在沒有密碼的情況下無意中修改或解除安裝用戶端，已移除下列選項。

- 「用戶端部署精靈」中的「密碼防護」選項。

存取此選項的方式是按一下「用戶端」頁面 > 「安裝用戶端」 > 「通訊更新套件部署」 > 「針對在 **Windows** 上執行的 **Symantec Endpoint Protection** 用戶端建立套件」 > 「密碼防護」選項。

如需在使用通訊檔案匯入用戶端安裝套件時使用密碼的相關資訊，請參閱[使用「通訊更新套件部署」還原用戶端伺服器通訊](#)。

- 「管理」頁面 > 「安裝套件」 > 「用戶端安裝設定」 > 「基本設定」標籤上的「移除無法解除安裝的現有 **Symantec Endpoint Protection** 用戶端軟體」選項。

如需解除安裝 Symantec Endpoint Protection 用戶端的其他方法的相關資訊，請參閱[解除安裝 Symantec Endpoint Protection 用戶端](#)。

- SONAR 日誌已重新命名為「SONAR：行為分析」日誌。

Symantec Endpoint Protection Manager

- 已新增 Windows Server 2025 的支援。
- 已捨棄 Windows Server 2012 和 Windows Server 2012 R2 的支援。

用戶端和平臺更新

Symantec Endpoint Protection Client for Mac

Symantec Endpoint Protection Client for Mac 沒有規劃版本。

Symantec Single Agent for Linux

Symantec Single Agent for Linux 沒有規劃版本。

Symantec Endpoint Security 雲端主控台

從雲端主控台管理的用戶端電腦獲得類似的功能和防護。

- 若要進一步瞭解 Symantec Endpoint Security 授權提供的雲端式功能，請參閱：[Symantec Endpoint Security 的新功能](#)
- 若要移轉至雲端主控台，請參閱：[移轉至雲端主控台](#)

最新版本的雲端主控台針對 Symantec Endpoint Protection 用戶端提供下列增強功能：

SymantecAI 聊天機器人具有全新外觀，並針對準確性進行調整。

說明文件

新主題包括：

- 如需您必須新增至支援案例的資訊的詳細資訊，請參閱[如何提交功能要求或建立支援案例](#)。
- 如需此版本中修正的相關資訊，請參閱 [Symantec Endpoint Protection 14.3 RU10 的新修正和元件版本](#)。

若要檢視資料庫綱要，請聯絡技術支援。

Symantec Endpoint Protection 14.3 RU10 的已知問題

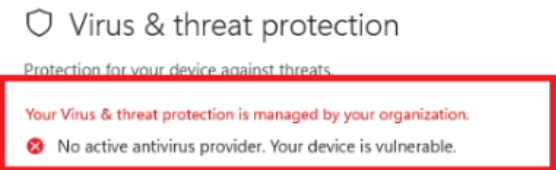
本主題列出 Symantec Endpoint Protection 最新版的已知問題和因應措施。

如需所有 Symantec Endpoint Protection 版本的相關資訊，請參閱：

- [Symantec Endpoint Protection 和 Endpoint Security 的版本、系統需求、發行日期、附註和修正](#)
- [所有 Symantec Endpoint Protection \(SEP\) 14.x 版本的已知問題和因應措施](#)
- [所有 Symantec Endpoint Protection \(SEP\) 14.x 版本的新功能](#)

下表列出目前版本的已知問題。

Table 1: 14.3 版 RU10

說明	因應措施
Symantec Endpoint Security (SES) 雲端和混合管理的 Symantec Endpoint Protection Manager (SEPM) 調適型防護熱圖顯示下列差異： - 在 SES 雲端熱圖上，如果在前 90 天內觸發行為，則非零感染狀況期限將從「學習」變更為 90 天。零感染行為保持為「學習」。 - 在 SEPM 熱圖上，如果觸發感染狀況行為，則除非過了 90 天之後，否則零感染狀況和非零感染狀況期限都會保持為「學習」。此外，感染狀況期限顯示如下： - 從 ≥ 90 且 < 180 天，感染狀況期限會顯示 90 天的事件。 - 從 ≥ 180 且 < 365 天，感染狀況期限會顯示 180 天的事件。 - 從 ≥ 365 天，感染狀況期限會顯示 365 天的事件。 而雲端熱圖顯示觸發行為時的非零感染狀況期限。 混合 Symantec Endpoint Protection Manager 熱圖檢視比 SES 雲端熱圖檢視更為保守。 [CDM-138308]	未來的修正規劃讓 SES 雲端與混合管理的 SEPM 之間的遙測收集相符。
Microsoft Windows Server 2025 中的 Windows 資訊安全中心無法將已安裝的 Symantec Endpoint Protection 用戶端辨識為防毒提供者，並且會顯示下列訊息： #####  [SEP-87042]	Microsoft 目前沒有修正。Broadcom 正在調查是否有解決問題的因應措施。不過，Symantec Endpoint Protection 用戶端仍然會保護用戶端電腦。
目前產品語言版本 (PVL) 通常會包括 LiveUpdate Administrator (LUA) 所需的所有內容。不過，在 14.3 RU10 中： - 某些內容使用現有的 14.3 RU9 PVL 來取得內容。 - 某些內容使用新的 14.3 RU10 PVL 來取得內容。 如果您將 LUA 架構成僅下載 14.3 RU10 內容，則用戶端無法取得所需的所有內容。 [CRE-20350]	您必須架構 LiveUpdate Administrator 來下載 14.3 RU9 和 14.3 RU10 內容，以充分更新 14.3 RU10 用戶端。 將 Symantec 產品新增至產品清單
在「系統 > 伺服器活動」日誌中，您會看到下列錯誤訊息：##### ###: TLS ##### 此問題的發生原因是託管 SEPM 資料庫的 SQL Server 已安裝 Symantec Endpoint Protection 14.3 RU6 到 14.3 RU9，而且 IPS 政策中已套用「頻外掃描」。 下列情況會發生此問題： - IPS 政策中已啟用頻外掃描，而且 IPS 正在處理大量流量。 - 您已在雲端伺服器中註冊 SEPM 網域，並升級至 14.3 RU10 SEPM，然後將 SEP 用戶端升級至 14.3 RU9。 - 您已從 14.3 RU6 到 14.3 RU9 SEPM 升級至 14.3 RU10。 [INFODEVSEP-203]	停用 IPS 政策中的頻外掃描。 請參閱架構入侵預防
如果您已在 14.0 MP1 和更舊版本的 Symantec Endpoint Protection Manager (SEPM) 中設定用戶端密碼防護，然後升級至 14.3 RU5 或更新版本的 SEPM，則該密碼沒有作用。如果您升級至 14.3 RU10 SEPM，則預設用戶端密碼會覆寫 14.0 MP1 和更舊版本的密碼。用戶端使用者會看到下列訊息：##### #### 此問題是 14.3 RU5 中進行的安全性增強所造成。 [INFODEVSEP-198]	用戶端使用者必須使用您在 Symantec Endpoint Protection Manager 14.3 RU10 中所設定的預設用戶端密碼。

說明	因應措施
14.3 RU4 和更舊版本中發生下列用戶端密碼問題： - 您在「用戶端密碼設定」對話方塊中設定密碼，然後按一下「確定」來儲存密碼。 - 您在未變更密碼的情況下重新開啟密碼對話方塊，然後按一下「確定」來儲存密碼。 密碼變更為未知值。  [INFODEVSEP-198]	此問題已在 14.3 RU10 中修正。
您無法使用 PowerShell 來解除安裝您使用 Symantec Endpoint Protection Manager 14.3 RU10 所管理的任何用戶端版本。 請參閱使用指令提示解除安裝 Endpoint Protection 用戶端。 [INFODEVSEP-229]	如果您使用預設用戶端密碼或群組層級密碼，則可以解除安裝用戶端。
在 Symantec Endpoint Protection Windows 用戶端「狀態」頁面上，您可能會看到下列訊息：Web ##### 按一下「說明 > 疑難排解 > Web 和雲端存取防護」頁面。如果您看到下列錯誤訊息：###80010907，升級至此版本時，Web 和雲端存取防護政策已經損壞。 INFODEVSEP-196	- 撤銷該用戶端使用者的 Web 和雲端存取防護政策。 - 刪除 C:\ProgramData\Symantec WSS Agent 資料夾。 - 將 Web 和雲端存取防護政策重新指派給用戶端使用者。 SEP Web 和雲端存取防護的運作不正常 錯誤：80010907

[Symantec Endpoint Protection 14.3 RU10 的新修正和元件版本](#)

[Symantec Endpoint Protection 支援和培訓資源](#)

測試的虛擬安裝和虛擬化產品

您可以在虛擬環境中執行的受測試作業系統上安裝 Symantec Endpoint Protection。請在客體作業系統 (而非主機) 上安裝 Symantec Endpoint Protection。

Symantec 已在 Symantec Endpoint Protection Manager 測試下列虛擬化產品，以及適用於 Windows 和 Linux 的 Symantec Endpoint Protection 用戶端軟體：

- Microsoft Azure
- Amazon Web Service (AWS) EC2
- Amazon 工作區
- Citrix Studio 版本 2009.0.0 (14.3 RU2)
- Citrix XenServer 5.6 或更新版本
- Microsoft Virtual Server 2005
- Microsoft Windows Server

- 2008 Hyper-V
- 2008 R2 Hyper-V
- 2012 Hyper-V
- 2012 R2 Hyper-V
- 2016 Hyper-V (14.2 MP1)
- 2019 Hyper-V Core Edition (14.2 MP1)
- Nutanix AOS 5.15 (LTS) (14.3 RU2)
- Oracle Cloud Infrastructure (OCI)
- Virtual Box (由 Oracle 提供)

NOTE

Symantec Endpoint Protection Manager 和用戶端 Symantec Endpoint Protection 不直接與虛擬化平台 (如 [VMware ESX](#)) 互動。該互動在作業系統和 Hypervisor 之間完成。請確認 Symantec Endpoint Protection Manager、用戶端和所選虛擬化平台都能在支援的作業系統上執行。

Symantec Endpoint Protection 包含多個可在虛擬環境中改善效能的功能。

針對 Virtual Image Exception 工具所支援的產品，請參閱[虛擬映像例外工具的系統需求](#)。

Symantec Endpoint Protection 支援和培訓資源

了解各種可供使用的 Symantec Endpoint Protection 資源，例如支援服務、講師指導培訓和社群論壇。

資源	連結
Broadcom 支援	Broadcom 支援 建立案例並查詢知識庫文章、下載和試用軟體、權利和授權資訊、Security Advisory 以及公告和法律聲明。 Broadcom 試用軟體和概念證明示範 。
訓練	• 教育訓練服務 存取訓練課程、線上產品說明庫等。 • 講師指導培訓 歡迎參閱目錄，了解最新的 Broadcom Enterprise Security 群組課程。
Symantec Connect 社群論壇	Endpoint Protection 論壇 加入最新的產品討論，閱讀問答清單等。
更多文件	相關文件 • 從 Broadcom Symantec Security Tech Docs Portal 下載線上 Endpoint Protection 文件。 • 若要尋找 Symantec Endpoint Protection Manager 資料庫綱要，請聯絡支援部門。 對於其他語言，請按一下「語言」下拉式功能表。
威脅資訊和更新	Symantec Protection Center 參閱最新的 Symantec 防護公告、報告產品安全性漏洞、檢查病毒定義檔、安全更新和更多內容。

如何提交功能要求或建立支援案例

若要提交功能要求或建立 Symantec Endpoint Protection (SEP) 或 Symantec Endpoint Security (SES) 支援案例，請參閱：

- [開啟支援案例](#)。
- 聯繫您的 [Broadcom 合作夥伴](#)。如果您不認識您的客戶經理，請參閱合作夥伴清單。
- 撥打您所在國家 / 地區的 [熱線](#)。

確認您的支援 ID 或聯絡 ID 有效。

當您開啟案例時，請新增下列資訊：

- 清楚的問題說明。
- 任何錯誤訊息的完整文字。
- 擷取問題的螢幕截圖。
- 來自 Symantec Endpoint Protection 用戶端的 SymDiag 和/或具有用戶端的「所有資料」的 Symantec Endpoint Protection Manager。
- 問題的開始時間。

什麼是 Symantec Endpoint Protection ?

瞭解 Symantec Endpoint Protection 架構和元件。

Symantec Endpoint Protection 是用戶端伺服器解決方案，可保護網路中的筆記型電腦、桌上型電腦和伺服器免於惡意軟體、風險和漏洞的危害。Symantec Endpoint Protection 結合了病毒防護和進階威脅防護，能主動保護用戶端電腦的安全，使其不受病毒、病蟲、特洛伊木馬程式和廣告軟體等已知和未知威脅的攻擊。Symantec Endpoint Protection 甚至能防止可躲避傳統安全措施的最複雜攻擊，如 Rootkit、零時差攻擊和變種的間諜軟體。

Symantec Endpoint Protection 具備低維護和高效能的優點，能透過網路通訊自動保護實體系統與虛擬系統使其免遭攻擊。Symantec Endpoint Protection 提供有效率且易於部署和使用的管理解決方案。

更多資訊

- [Symantec Endpoint Protection 14 型錄](#)
- [Symantec Endpoint Protection 技術如何保護您的電腦](#)
- [Symantec Endpoint Protection 架構元件](#)

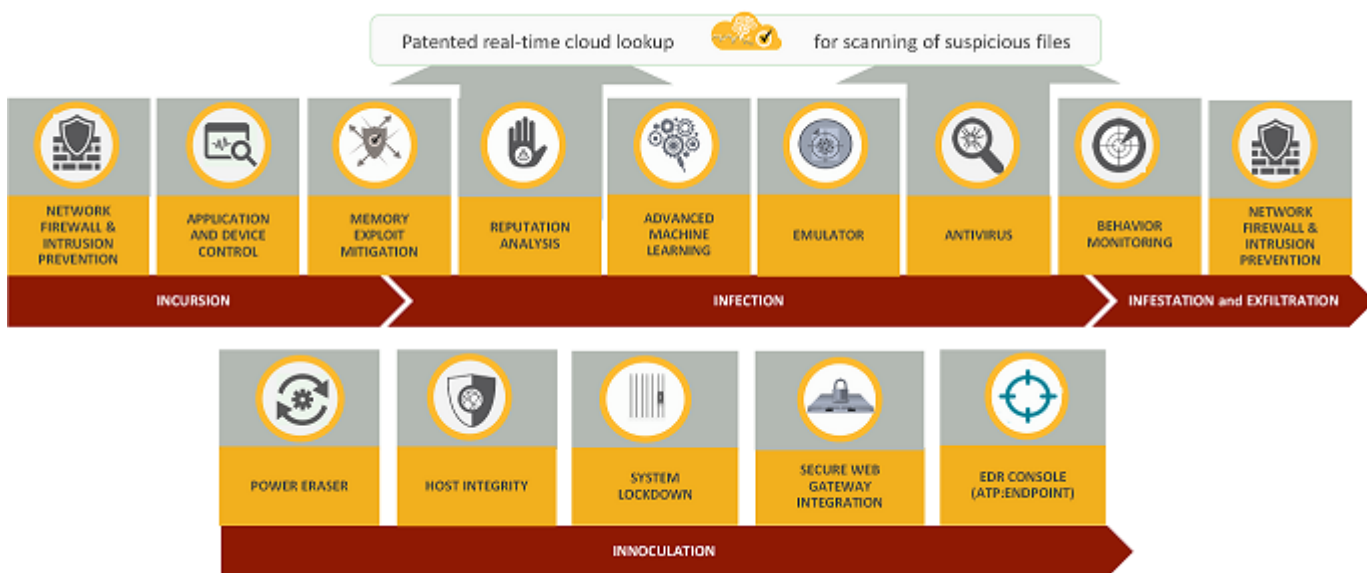
Symantec Endpoint Protection 功能

Symantec Endpoint Protection (SEP) 使用下列核心功能來防禦已知和未知威脅。

Symantec Endpoint Protection 使用分層方式進行防禦。全面方式可在攻擊之前、期間和之後保護網路。Symantec Endpoint Protection 藉由提供工具，在任何攻擊入侵之前增加您的安全態勢，降低您的風險暴露程度。

如需詳細瞭解 Symantec Endpoint Protection 型錄，請參閱：[Symantec Endpoint Protection 14](#)

若要取得網路中電腦的完整防護，請一律啟用所有防護。



如需詳細資訊，請參閱：

[Symantec Endpoint Protection 技術可防範哪些類型的攻擊？](#)

Symantec Endpoint Protection 使用以下整體安全方式，透過下列階段跨越整個攻擊鏈保護您的環境：入侵、感染、侵擾和外滲，以及矯正和感染。

第 1 階段：入侵

在入侵階段期間，駭客通常會使用目標攻擊 (例如社交詐騙、零時差弱點、SQL 插入、鎖定惡意軟體或其他方式) 中斷組織網路。

Symantec Endpoint Protection 會在攻擊進入系統之前使用以下技術防範攻擊：

- 入侵預防/防火牆 (網路威脅防護)：分析所有內送流量和外寄流量並提供瀏覽器防護，以便此類威脅在電腦上執行之前予以攔截。以規則為基礎的防火牆和瀏覽器防護可防範網頁式攻擊。請參閱：
 - [管理入侵預防](#)
 - [管理防火牆防護](#)
- 應用程式控制：控制檔案存取和登錄存取，以及允許程序如何執行。請參閱：
 - [關於應用程式控制、系統鎖定和裝置控制](#)
 - [設定應用程式控制](#)
- 裝置控制：限制存取以選取硬體，並控制哪些類型的裝置可以上傳或下載資訊。請參閱：[管理裝置控制](#)
- 記憶體攻擊緩和：處理廠商未修正之常用軟體中的零時差攻擊行為，例如 Heap Spray、SEHOP 覆寫和 Java 攻擊。請參閱：[使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊](#)

第 2 階段：感染

在目標式攻擊中，駭客通常會使用社交詐騙、零時差弱點、SQL 插入、鎖定惡意軟體或其他方式中斷組織網路。

Symantec Endpoint Protection 會使用下列技術，在攻擊感染您的系統之前偵測和防禦這些攻擊：

- 記憶體攻擊緩和：偵測惡意軟體。
- 檔案信譽分析 (Insight)：以使用 Symantec Global Intelligence Network 的人工智慧為基礎。此進階分析可以從使用者、網站和檔案檢查數以億計的相關聯連結，以識別和抵禦快速變化的惡意軟體。分析重要屬性 (例如檔案下載的原始點)，賽門鐵克即可在某個檔案抵達用戶端電腦之前，準確地識別該檔案是良好還是無效檔案，並指派信譽分數。請參閱：[管理「下載鑑識」偵測](#)
- 進階機器學習：分析 Global Intelligence Network 中所包含的上萬億良好檔案和無效檔案的範例。進階機器學習是一項無需簽名的技術，可在執行前攔截新惡意軟體變體。請參閱：[Symantec Endpoint Protection 如何使用進階機器學習？](#)
- 高速模擬：使用變種自訂封包程式偵測隱藏的惡意軟體。掃描程式在導致威脅出現的輕量型虛擬機器中執行每個檔案 (以毫秒為單位)，從而改進偵測率和效能。請參閱：[Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？](#)
- 惡意軟體防護：使用以特徵為基礎的防毒和檔案啟發式技術來尋找和根除系統上的惡意軟體，以防範病毒、病蟲、特洛伊木馬程式、間諜程式、Bot 傀儡程式、廣告軟體和 Rootkit。請參閱：
 - [在用戶端電腦上管理掃描](#)
 - [關於掃描和即時防護的類型](#)
- 行為分析：使用機器學習提供零時差防護，透過在執行時即時監控將近 1,400 個檔案行為來判斷檔案風險，以阻止新威脅和未知威脅。請參閱：[管理 SONAR](#)
- 調適型防護：使用行為分析引擎以及全球威脅遙測和專業知識，以透過管理信任的應用程式所執行的潛在風險行為來減少攻擊面。請參閱：[透過自適應防護攔截 Living Off the Land \(LOTL\) 攻擊](#)

第 3 階段：侵擾和外滲

資料外滲是對電腦中的資料進行未經授權的傳輸。一旦入侵者控制這些目標系統，便可能會竊取智慧財產或其他機密資料。攻擊者會使用擷取的資訊進行分析，然後進一步侵入或詐騙。

- 入侵預防/防火牆：攔截透過網路傳遞的威脅。
- 行為分析：協助停止感染散佈。

第 4 階段：矯正和感染

Symantec Endpoint Protection 包含單一主控台和代理程式，可針對作業系統、平台和任意規模的企業提供防護。

- **Power Eraser**：可遠端觸發的主動工具，用於解決進階持續性威脅和矯正頑固的惡意軟體。請參閱：
[從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項](#)
- **主機完整性**：透過強制執行政策、偵測未經授權的變更以及執行損毀評估，確保端點受到保護且符合標準。然後，主機完整性會隔離不符合需求的受管系統。請參閱：
[主機完整性的運作方式](#)
- **系統鎖定**：允許應用程式 (已知良好) 執行，或攔截應用程式 (已知無效) 使其無法執行。不論哪種模式，系統鎖定都會使用總和檢查碼和檔案位置參數，以驗證應用程式通過核准或未經核准。系統鎖定對於只需執行單一應用程式的資訊站很有用。請參閱：
[設定系統鎖定](#)
- **Cloud Secure Web Gateway 整合**：使用可程式化 REST API 以便可與 Secure Web Gateway 進行整合，來協助快速阻止用戶端電腦中的感染散佈。
- **EDR 主控台整合**。Symantec Endpoint Protection 與 Symantec EDR 整合，旨在透過排列攻擊的優先順序來更快地偵測、回應和攔截目標式攻擊和進階持續性威脅。EDR (Endpoint Detection and Response) 功能會內建到 Symantec Endpoint Protection，這樣就不需要部署其他代理程式。請參閱：
[設定系統鎖定](#)

Symantec Endpoint Protection 技術可防範哪些類型的攻擊？

下表顯示哪些類型的 Symantec Endpoint Protection 技術可防範哪些類型的攻擊。

Table 2: 每種 Symantec Endpoint Protection 技術可防範哪些類型的攻擊？

攻擊	進階機器學習	啟發式	入侵預防	網路保護	政策鎖定
零時差	√	√	√		√
社交詐騙	√	√	√	√	√
勒索軟體	√	√		√	√
鎖定攻擊	√	√	√		√
進階持續性威脅	√	√	√		
偷渡式下載		√	√		

Symantec Endpoint Protection 架構元件

Symantec Endpoint Protection 架構使用三個功能群組的元件。部分元件屬於多個群組，因為這些元件是多功能的。



Table 3: 主要元件

元件	說明
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager 是管理伺服器，用於為連線至貴公司網路的用戶端電腦管理事件、政策和用戶端註冊。 Symantec Endpoint Protection Manager 包含下列子元件： - 管理伺服器軟體用於提供連入及連出用戶端電腦和主控台的安全通訊。 - 主控台是管理伺服器的介面。主控台軟體會協調並管理安全性政策、用戶端電腦、報告、日誌、角色和存取、管理功能以及安全性。您也可以安裝遠端主控台，並從具有網路連線的任何電腦，使用它來登入管理伺服器。 - 資料庫隨 Symantec Endpoint Protection Manager 一起安裝，用於儲存安全性政策和事件。您也可以安裝 Microsoft SQL Server 資料庫，以改用自動安裝的 Microsoft SQL Server Express (自 14.3 RU1 起) 或內嵌資料庫 (14.3 MP1 及更舊版本)。對於具有 5000 部以上電腦的較大型組織，建議使用 SQL Server。Symantec Endpoint Protection Manager 會與本機或遠端 Microsoft SQL Server 資料庫通訊。 如需詳細資訊，請參閱： 安裝 Symantec Endpoint Protection Manager
Symantec Endpoint Protection 用戶端	Symantec Endpoint Protection 用戶端會提供解決方案的安全防護部分。用戶端會從 Symantec Endpoint Protection Manager 下載政策，有時為內容，並且在 Windows、Mac 和 Linux 上執行。

Symantec Endpoint Protection 可讓用戶端從管理伺服器、群組更新提供者、內部 LiveUpdate 伺服器或 Internet 下載內容。

Table 4: 選用元件及其功能

元件	說明
LiveUpdate 管理員	LiveUpdate Administrator 可從內部 LiveUpdate 伺服器下載定義檔、特徵和其他內容，並將更新派送至用戶端電腦。您可以在大型網路中使用內部 LiveUpdate 伺服器，以減輕 Symantec Endpoint Protection Manager 負載。如果您的組織執行多個賽門鐵克產品且這些產品也使用 LiveUpdate 更新用戶端電腦，則您也應使用內部 LiveUpdate 伺服器。 如需詳細資訊，請參閱： • 下載 LiveUpdate Administrator (LUA) • 選擇派送方法以更新用戶端上的內容 • 將用戶端架構為從內部 LiveUpdate 伺服器下載內容
群組更新提供者 (GUP)	群組更新提供者有助於在組織內部派送內容，對於位於頻寬最低的遠端位置的群組特別有用。有許多用戶端的組織可能希望對 Windows 用戶端使用「群組更新提供者」(GUP)。GUP 會減輕管理伺服器的負載，而且比內部 LiveUpdate 伺服器容易設定。請參閱： 使用群組更新提供者將內容散佈至用戶端
Symantec Endpoint Security (SES)	Symantec Endpoint Security 是您用來從雲端管理用戶端電腦的雲端平台。Symantec Endpoint Security 是內部部署 Symantec Endpoint Protection 的完整雲端受管版本。您可以從下列任一選項管理電腦： • Symantec Endpoint Protection Manager (僅限內部部署) • 從 Symantec Endpoint Protection Manager 和 Symantec Endpoint Security (混合式：內部部署和雲端)。請參閱： 在 Symantec Endpoint Protection Manager 主控台的雲端主控台中註冊網域 • Symantec Endpoint Security (僅限雲端)。請參閱： 直接從 SEP 內部部署選項移至完全雲端受管選項 內部部署、混合或完全雲端管理選項

Symantec Endpoint Protection 也隨附多項工具，可協助您提升安全性和管理產品。如需詳細資訊，請參閱：

- [Symantec Endpoint Protection 隨附的工具具有哪些？](#)
- [Symantec Endpoint Protection 技術如何保護您的電腦](#)

入門指南

立即啟動並執行 Symantec Endpoint Protection (SEP)。

評估安全性需求，並判斷預設設定是否提供了所需的效能和安全性平衡。有一些效能增強作業可以於安裝 Symantec Endpoint Protection Manager 後立即進行。

立即執行下列工作以安裝和保護網路中的電腦：

- [步驟 1：規劃安裝結構](#)
- [步驟 2：進行準備並安裝 Symantec Endpoint Protection Manager](#)
- [步驟 3：啟用產品授權](#)
- [步驟 4：新增群組、政策和位置](#)
- [步驟 5：變更通訊設定以增加效能](#)
- [步驟 6：決定用戶端部署方法](#)
- [步驟 7：準備用戶端進行安裝](#)
- [步驟 8：部署並安裝用戶端軟體](#)
- [步驟 9：檢查電腦是否列於預期的群組中，以及用戶端是否可與管理伺服器進行通訊](#)

如需詳細資訊，請參閱：

[安裝管理伺服器之後該做什麼？](#)

步驟 1：規劃安裝結構

安裝產品之前，請考量網路的規模和地理分佈位置，以決定安裝架構。

為了確保維持良好的網路和資料庫效能，您需要評估數個因素。這些因素包括需要防護的電腦數量、是否有任何電腦透過廣域網路連線，或排程內容更新的頻率。

- 如果網路規模很小、位於一個地理位置，而且少於 500 個用戶端，就只需要安裝一個 Symantec Endpoint Protection Manager。
- 如果您的網路非常龐大，則可安裝更多具有額外資料庫的站台，並將其架構為使用複寫來共用資料。若要提供額外的備援，您可以安裝額外的站台，以支援容錯移轉或負載平衡。容錯移轉和負載平衡只能搭配 Microsoft SQL Server 資料庫使用。
- 如果您的網路分散在不同地點，則可能需要針對負載平衡和頻寬分配目的，安裝額外的管理伺服器。

為了協助您規劃中型和大型安裝，請參閱：

[Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書](#)

如需詳細資訊，請參閱：

- [網路架構考量](#)
- [設定站台和複寫](#)
- [設定容錯移轉和負載平衡](#)

步驟 2：進行準備並安裝 Symantec Endpoint Protection Manager

1. 確定要安裝管理伺服器的電腦符合最低系統需求。請參閱：
[所有 Endpoint Protection 版本的版本說明、新修正和系統需求](#)
2. 若要安裝 Symantec Endpoint Protection Manager，您必須使用可授予本機管理員存取權的帳戶來登入。
3. 決定是使用預設的 Microsoft SQL Server Express 資料庫還是 Microsoft SQL Server 資料庫。

如果使用 Microsoft SQL Server 資料庫，安裝將會要求執行額外的步驟。這些步驟包括但不限於，架構或建立資料庫實例，將該實例架構為使用混合模式或 Windows 驗證模式。另外，還需要提供資料庫伺服器管理憑證，才能建立資料庫和資料庫使用者。這些會專門與管理伺服器搭配使用。請參閱：

- [關於 SQL Server 組態設定](#)
- [設定容錯移轉和負載平衡](#)

4. 您首先要安裝 Symantec Endpoint Protection Manager。安裝之後，您需要使用「管理伺服器組態精靈」立即架構安裝。

在架構管理伺服器時，決定以下項目：

- 用於登入管理主控台的密碼
- 可接收重要通知和報告的電子郵件地址
- 加密密碼，根據安裝期間您所選取的選項可能需要使用這個密碼

如需詳細資訊，請參閱：

- [安裝 Symantec Endpoint Protection Manager](#)
- [關於基本管理伺服器設定](#)
- [架構 Symantec Endpoint Protection Manager 安裝](#)

步驟 3：啟用產品授權

產品安裝後的 60 日之內購買並啟用授權。請參閱：

- [啟用或匯入 Symantec Endpoint Protection 產品授權](#)
- [授權 Symantec Endpoint Protection](#)
- [Symantec Endpoint Protection 產品授權術語](#)

步驟 4：新增群組、政策和位置

1. 群組可用來組織用戶端電腦，並將不同的安全層級套用到每個群組。您可以使用預設群組、匯入群組 (如果網路使用 Active Directory 或 LDAP 伺服器) 或新增群組。

如果新增群組，您可以使用下列群組結構作為基礎：

- 桌上型電腦
- 筆記型電腦
- 伺服器

如需詳細資訊，請參閱：

- [從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦](#)
- [如何設定群組結構](#)
- [新增群組](#)

2. 您可以使用位置，根據特定準則將不同的政策和設定套用到電腦。例如，您可以根據電腦位於公司網路內部或外部，為電腦套用不同的安全政策。一般而言，與防火牆內部的電腦相比，從防火牆外部連線至網路的電腦需要更佳的安全性。此位置讓位於辦公室外的行動電腦從賽門鐵克的 LiveUpdate 伺服器自動更新其定義檔。

如需詳細資訊，請參閱：

- [Symantec Endpoint Protection 位置偵測最佳實務](#)
- [將位置新增到群組](#)

3. 針對要使用不同政策或設定的群組或位置停用繼承。

依據預設，群組會從預設的父群組 **My Company** 繼承政策和設定。如果您想要指派不同的政策給子群組，或想要新增位置，您必須先停用繼承。然後就可以變更子群組的政策，或新增位置。

NOTE

Symantec Endpoint Protection Manager 政策繼承不會套用到從雲端接收到的政策。雲端政策會遵循在雲端中定義的繼承。

如需詳細資訊，請參閱：

停用群組繼承

- 針對每種類型的政策，您可以接受預設政策，或建立並修改新政策來套用到每個新群組或位置。您必須將需求新增至預設主機完整性政策，才能使主機完整性檢查對用戶端電腦起作用。

步驟 5：變更通訊設定以增加效能

您可以在每個群組中修改下列用戶端伺服器通訊設定，以改善網路效能：

- 使用提取模式取代推送模式，控制用戶端於何時使用網路資源下載政策和內容更新。
- 增加活動訊號的間隔。如果每部伺服器服務的用戶端數目少於 100，可將活動訊號間隔時間增加為 15-30 分鐘。如果為 100 至 1,000 個用戶端，請將活動訊號間隔時間增加為 30-60 分鐘。更大的環境可能需要更長的活動訊號間隔時間。賽門鐵克建議您將「讓用戶端立即上傳重大事件」保留勾選狀態。
- 將下載隨機設定增加為活動訊號間隔時間的一到三倍。

如需詳細資訊，請參閱：

- [從預設管理伺服器或群組更新提供者隨機進行內容下載](#)
- [使用推送模式或提取模式更新用戶端上的政策和內容](#)

步驟 6：決定用戶端部署方法

決定最適合用來在您環境中的電腦上安裝用戶端軟體的用戶端部署方法。請參閱：

選擇使用用戶端部署精靈安裝用戶端的方法

- 針對 Linux 用戶端，您可以使用「儲存套件」或「網路連結與電子郵件」，但不能使用「遠端推送」。
- 針對 Windows 和 Mac 用戶端，如果您使用「遠端推送」，可能需要執行下列工作：
 - 確認擁有遠端用戶端電腦的管理員存取權限。修改任何現有的防火牆設定 (包括通訊埠和通訊協定) 以允許在 Symantec Endpoint Protection Manager 與用戶端電腦之間進行遠端部署。請參閱：[Symantec Endpoint Protection 的通訊埠](#)
 - 您必須使用可授予本機管理員存取權的帳戶來登入。
如果用戶端電腦是 Active Directory 網域的一部分，您必須使用可授予用戶端電腦本機管理員存取權的帳戶登入裝載 Symantec Endpoint Protection Manager 的電腦。針對不是 Active Directory 網域一部分的每個用戶端電腦，您都應該有管理員憑證可供使用。請參閱：[準備 Windows 和 Mac 電腦進行遠端部署](#)

如需詳細資訊，請參閱：

準備用戶端安裝

步驟 7：準備用戶端進行安裝

- 確定要安裝用戶端軟體的電腦符合最低系統需求。您也應將用戶端安裝在裝載 Symantec Endpoint Protection Manager 的電腦上。請參閱：
[請參閱：所有 Endpoint Protection 版本的版本說明、新修正和系統需求](#)
- 從 Windows 電腦手動解除安裝 Symantec Endpoint Protection 用戶端安裝程式無法解除安裝的任何第三方安全軟體程式。
如需此功能所移除產品的清單，請參閱：
[架構用戶端套件來解除安裝現有安全軟體](#)
[Symantec Endpoint Protection 的第三方安全軟體移除支援](#)
您必須從 Linux 電腦或 Mac 電腦移除任何現有的安全軟體。
某些程式可能具有特殊的解除安裝常式，或者可能需要停用自我防護元件。請參閱第三方軟體的說明文件。

步驟 8：部署並安裝用戶端軟體

1. 針對 Windows 用戶端，執行下列工作：

- 建立自訂用戶端安裝功能集，決定要在用戶端電腦上安裝的元件。您也可以使用其中一個預設用戶端安裝功能集。請參閱：

[從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦](#)

若是工作站的用戶端安裝套件，請勾選環境中郵件伺服器所適用的電子郵件掃描程式防護選項。例如，如果您使用 Microsoft Exchange 郵件伺服器，則勾選「**Microsoft Outlook** 掃描程式」。

- 更新自訂用戶端安裝設定，決定用戶端電腦上的安裝選項。這些選項包括目標安裝資料夾、解除安裝第三方安全軟體和重新啟動行為。您也可以使用預設用戶端安裝設定。請參閱：

[選擇要在用戶端上安裝哪些安全性功能](#)

2. 使用「用戶端部署精靈」，建立用戶端安裝套件，其中包含從可用選項所進行的選擇，然後將它部署到用戶端電腦。您只能透過用戶端部署精靈部署至 Mac 或 Windows 電腦。請參閱：

- [使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端](#)
- [使用遠端推送安裝 Symantec Endpoint Protection 用戶端](#)
- [使用儲存套件安裝 Symantec Endpoint Protection 用戶端](#)
- [匯出用戶端安裝套件](#)

賽門鐵克建議您不要在安裝 Symantec Endpoint Protection 的同時執行第三方安裝。任何進行網路層級或系統層級變更的第三方案式安裝都可能會在安裝 Symantec Endpoint Protection 時導致不理想的結果。如可能，請在安裝 Symantec Endpoint Protection 之前重新啟動用戶端電腦。

步驟 9：檢查電腦是否列於預期的群組中，以及用戶端是否可與管理伺服器進行通訊

在管理主控台中，於「用戶端」>「用戶端」頁面上：

1. 將檢視變更為「用戶端狀態」，確認每個群組中的用戶端電腦可與管理伺服器進行通訊。

請查看以下各欄中的資訊：

- 連線至管理伺服器的用戶端會於「名稱」欄中顯示綠點。請參閱：

[檢查用戶端是否已連線至管理伺服器且受保護](#)

- 「上次狀態變更時間」欄中會顯示每個用戶端上次與管理伺服器進行通訊的時間。
- 「需要重新啟動」欄中會顯示用戶端電腦是否需要重新啟動才能受到保護。請參閱：

[從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)

- 「政策序號」欄中會顯示最新的政策序號。政策可能不會在一到兩個活動訊號時間範圍內進行更新。如果政策未立即更新，您可以在用戶端上手動更新政策。請參閱：
 - [使用政策序號檢查用戶端伺服器通訊](#)
 - [更新用戶端政策](#)

2. 變更為「防護技術」檢視，並確認「防毒狀態」和「竄改防護狀態」(含)之間欄的狀態設定為「開啟」。請參閱：

[檢視用戶端電腦的防護狀態](#)

3. 在用戶端上，檢查用戶端是否已連線至伺服器，並檢查政策序號是否為最新序號。請參閱：

- [在用戶端電腦上檢查與管理伺服器的連線](#)
- [檢查用戶端是否已連線至管理伺服器且受保護](#)
- [Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

從 Symantec Endpoint Security 雲端管理用戶端

您可以選擇從 Symantec Endpoint Protection Manager 和 Symantec Endpoint Security 雲端管理您的裝置。您可以在安裝完成後隨時將 Symantec Endpoint Protection Manager 網域註冊至雲端伺服器。

請參閱：[移轉至 SES 雲端主控台](#)

附錄：其他資源和指南

- [Symantec Endpoint Protection 的產品指南和手冊](#)
- [Symantec Endpoint Protection 的最佳實務](#)
- [Symantec Endpoint Protection 所使用的通訊埠](#)
- [Symantec Endpoint Protection \(SEP\) 和 Symantec Endpoint Protection \(SES\) 所需的外部 URL](#)
- [在安裝或架構期間發生錯誤：「...服務需要使用者權限」或「...無法讀取使用者權限」](#)

Symantec Endpoint Protection 快速入門

本指南可協助您下載、安裝及架構 Symantec Endpoint Protection，專用於 500 個或更少用戶端的預設、首次受管用戶端的安裝。

如需升級的相關資訊，請參閱[升級和移轉到最新版本的 Symantec Endpoint Protection \(SEP\)](#)。

- [安裝前：檢查系統需求](#)
- [步驟 1：下載 Symantec Endpoint Protection 安裝檔案](#)
- [步驟 2：安裝 Symantec Endpoint Protection Manager](#)
- [步驟 3：登入 Symantec Endpoint Protection Manager](#)
- [步驟 4：啟用授權](#)
- [步驟 5：新增群組](#)
- [步驟 6：檢閱和架構預設政策](#)
- [步驟 7：安裝 Symantec Endpoint Protection 用戶端](#)
- [步驟 8：驗證用戶端是否與管理伺服器通訊](#)
- [步驟 9：檢查是否已安裝最新定義檔](#)

安裝前：檢查系統需求

安裝 Symantec Endpoint Protection Manager 或 Symantec Endpoint Protection 用戶端之前，請執行以下步驟：

1. [下載 SymDiag](#)，並執行安裝前檢查，以確保您的電腦符合系統需求。
2. [檢閱 Symantec Endpoint Protection 的版本說明和系統需求](#)。

步驟 1：下載 Symantec Endpoint Protection 安裝檔案

您可以使用 Broadcom 支援入口網站來擷取授權金鑰和下載軟體。

1. 登入 [Broadcom 支援入口網站](#)。
2. 在左側面板上，按一下「我的權利」，然後使用您的序號、網站 ID、合約編號或客戶 ID 來搜尋授權。
3. 展開「我的網站 > Broadcom」，然後選取您的授權：「**Endpoint Security Complete**」或「**Endpoint Security Enterprise**」。
4. 按一下「下載」圖示。

My Entitlements

My Entitlements

PLA Entitlements

☐ PLA Products ☒ Active

Q BXXXXXXXXXX



Search

Site Name

Site ID

My Sites



Broadcom

XXXXXX

Get User List



Endpoint Security Complete

Entitlement Details

Product Details

Serial Number

Status

PLA Details



Contract Details

Downloads

Licenses

Cases

BXXXXXXXXXX

Active



5. 系統會將您重新導向至另一個頁面，您可以在其中再次選取產品名稱，然後按一下您想要下載的版本號碼。

取消核取「僅英文」，以其他語言來顯示軟體。

6. 在「產品版本」頁面上，從可用的下載選項中進行選擇，然後按一下「下載」圖示。

Endpoint Security Complete 14.3.9

Product Download H

Primary Downloads

Search

14.3.9

RU9

English

Download Selected

☒ Expand

Symantec Endpoint Protection 14.3 RU9 -
International English

Release
14.3.9

Release Level Info RU9

Packlist ID 521443

Copy

File Name

Last Updated

SHA2

MD5

Download

Tokens

Symantec_Endpoint_Prot
ection_14.3.0-
RU9_All_Clients_EN.zip
(255.51 MB)

Jun 24, 2024
08.45AM

4dba4eb83994e1087171b5d1bce6
bf50a64d484bec9422e36407283c6
e5137c0

f9ffd502b31cb58eaaacc2903a47b5
50



Generate



Symantec_Endpoint_Prot
ection_14.3.0-
RU9_Full_Installation_EN
.exe
(1.38 GB)

Jun 24, 2024
08.51AM

50c07873ff1e81a407d4fa7551c4c5
19d286c8d742f392a85d12aee00ca
07cc5

19044445a43424db823c4bf06d3d
a644



Generate

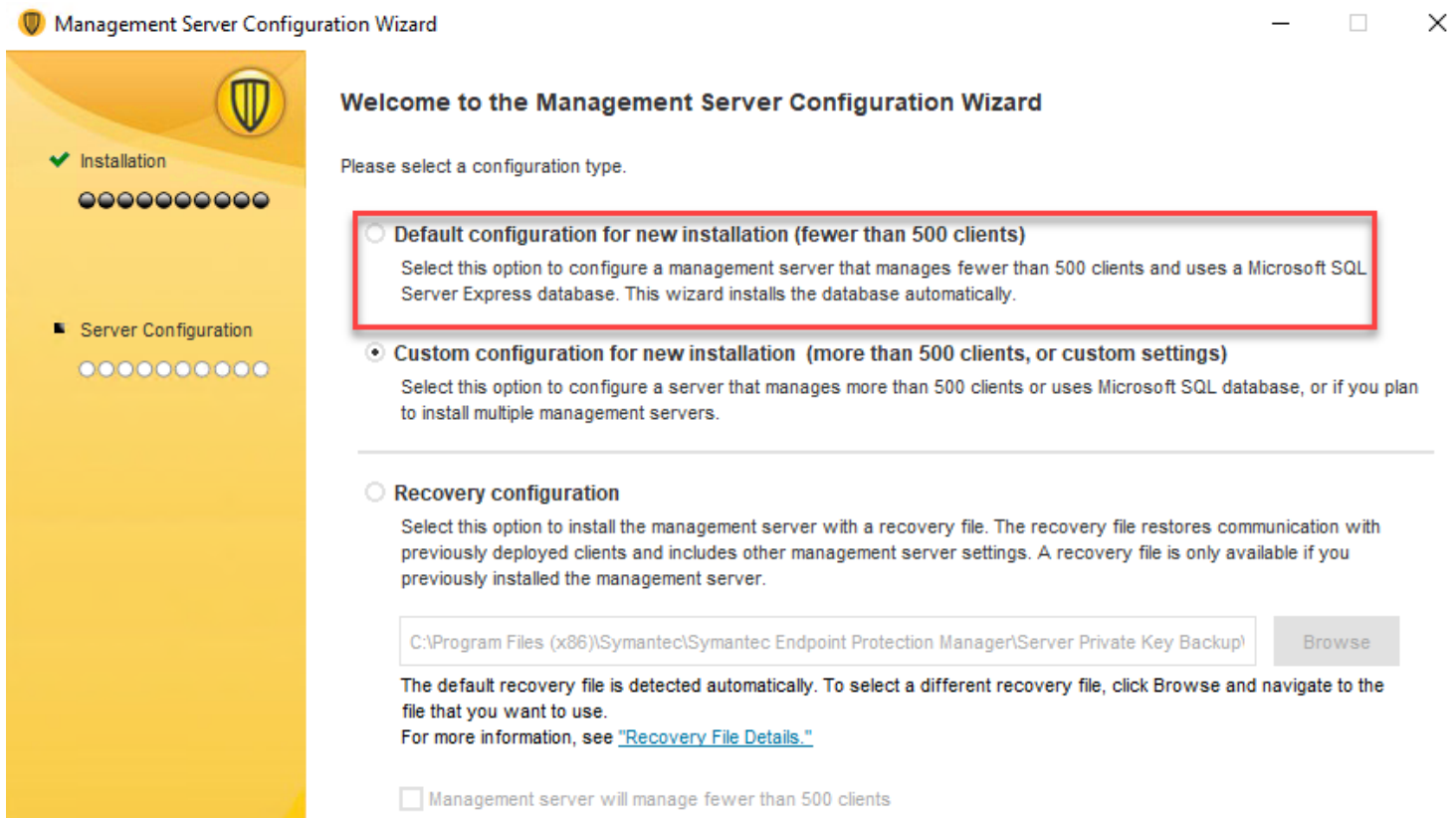


更多資訊

- 如需更多指示，請參閱 [Symantec 快速入門](#)，並向下捲動至頁面底部。
- 如需下載 Symantec 產品的詳細資訊，請參閱 [下載最新版本的 Symantec 軟體](#)。
- 如果您無法透過 Broadcom 支援入口網站找到或下載 Symantec 軟體，則請參閱 [客戶服務中心](#) 或 [銷售](#)。

步驟 2：安裝 Symantec Endpoint Protection Manager

1. 在已下載 Symantec Endpoint Protection 安裝檔案的資料夾中，連按兩下此檔案以解壓縮所有檔案。如果您看到開啟檔案 - 安全性警告提示，請按下「執行」。
安裝檔案包括 Tools 目錄。
請參閱 [Symantec Endpoint Protection 隨附的工具](#)。
2. 連按兩下 Setup.exe，然後按一下「安裝 Symantec Endpoint Protection Manager」。
3. 接受授權許可協議中的條款以及預設提示，然後按一下「安裝」。
4. 在「歡迎使用管理伺服器組態精靈」面板上，按一下「新安裝的預設架構 (少於 500 個用戶端)」，然後按「下一步」。
針對自訂安裝 (例如使用 SQL Server 資料庫)，按一下「新安裝的自訂架構」。
請參閱 [使用自訂架構安裝 Symantec Endpoint Protection Manager](#)。



5. 填寫必要欄位以建立下列項目，然後按「下一步」。
 - a. 系統管理員帳戶。將 admin 保留為使用者名稱。
 - b. Symantec Endpoint Protection Manager 對其傳送通知的電子郵件地址。
 - c. 郵件伺服器資訊。按一下「傳送測試電子郵件」。您必須將郵件伺服器架構為從管理伺服器接收通知及密碼重設電子郵件。如果您現在不要進行設定，則請按一下「否」，稍後進行設定。請參閱 [伺服器屬性：電子郵件伺服器](#)。

Management Server Configuration Wizard

Create a system administrator account. The password will be required to log on to the management console.

Company name: symc

User name: admin

Password: *

Confirm password: *

Password Strength: Weak

The password selected here is used for both the administrator password and the database password. If you change the administrator password after installation, the database password will not change.

Email address: * first.name@broadcom.com

Email Address Not Validated

You did not choose to send a test email to validate the specified email address. Do you want to send a test email?

Yes No

can later change these settings by

Port number: 25

Sender email address:

User name:

- 從 14.3 RU10 開始，在「預設用戶端密碼」面板上，鍵入用戶端使用者必須用來停止或解除安裝用戶端軟體的密碼。如果您之後忘記密碼，則可以在群組層級修改密碼，或重新架構管理伺服器。
請參閱[使用密碼保護 Symantec Endpoint Protection 用戶端](#)。
- 選擇性地檢查下列選項，然後按「下一步」：
 - 合作夥伴資訊 (如果其適用於您的授權狀況)。
 - 將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報 (建議)。
- 如果您看到下列訊息，則除非您必須執行 Windows 更新，否則請按一下「繼續」。

Error



The Microsoft SQL Server Express database installation may not be able to continue. Check that the Windows updates are current and that the Windows update service is running.

If you are running the latest update, click **Continue** to complete the installation.

If you are not running the latest update, click **Cancel**, save your work, run the latest update, restart your computer, and then continue the Symantec Endpoint Protection installation.

Continue

Cancel

此步驟可能需要時間才能完成。

- 在「已完成架構」面板上，按下「完成」以啟動 Symantec Endpoint Protection Manager。

步驟 3：登入 Symantec Endpoint Protection Manager

- 在 Symantec Endpoint Protection Manager 登入畫面上，鍵入您在上一個步驟中所建立的使用者名稱 (預設為 admin) 和密碼，然後按一下「登入」。

「開始使用」畫面會出現，並顯示多個常見工作連結。例如，您可以啟用授權或部署 Symantec Endpoint Protection 用戶端。

若要隨時開啟此畫面，請按一下 Symantec Endpoint Protection Manager 右上角的「說明」>「開始使用」頁面。

步驟 4：啟用授權

您必須啟用授權才能接收內容和追蹤授權使用情況。

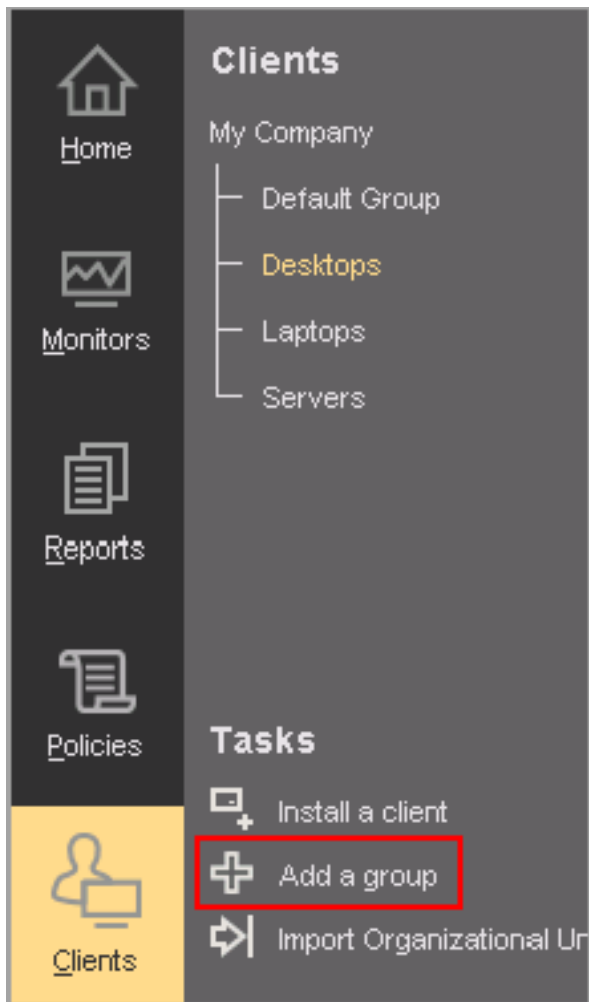
1. 在 Symantec Endpoint Protection Manager 中，按一下左側窗格中的「管理」>「授權」。
2. 在「工作」下方，按下「啟用授權」。
3. 使用訂單履行電子郵件包含的序號或 .SLF 授權檔，按照提示來安裝授權。

請參閱[啟用或匯入 Symantec Endpoint Protection 產品授權](#)。

步驟 5：新增群組

根據預設，當您安裝用戶端時，用戶端會安裝在預設「我的公司」群組中。您應該為桌上型電腦、膝上型電腦和伺服器建立單獨的群組，以針對每個群組套用自訂防護。

1. 在 Symantec Endpoint Protection Manager 中，按一下「用戶端」。
2. 在「用戶端」下方，按一下「我的公司」群組。
3. 在「工作」下方，按一下「新增群組」。



4. 在「新增 **My Company** 的群組」對話方塊中，輸入群組名稱和說明，然後按下「確定」。

然後，您可以進一步架構群組設定，例如政策繼承。

請參閱[新增群組](#)。

步驟 6：檢閱和架構預設政策

檢閱用來保護環境中裝置的政策。每種政策類型都會有一個預設政策，而 Symantec 會架構該政策以提供最佳防護和效能。

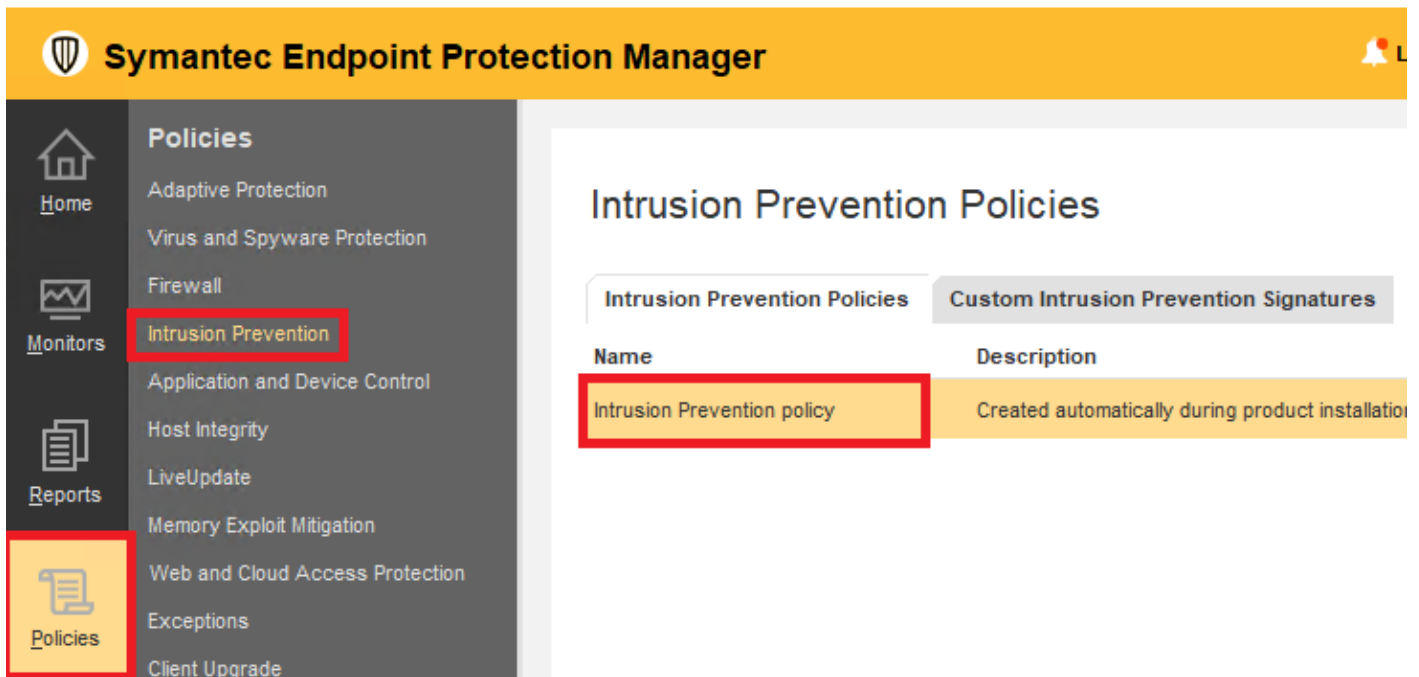
請參閱[安全性政策類型](#)。

您可以在安裝和部署 Symantec Endpoint Protection 安裝套件之前或之後執行此步驟。

檢閱和架構預設政策

1. 在 Symantec Endpoint Protection Manager 中，按一下「政策」>「<政策類型>」，然後開啟預設政策。

 Symantec Endpoint Protection Manager

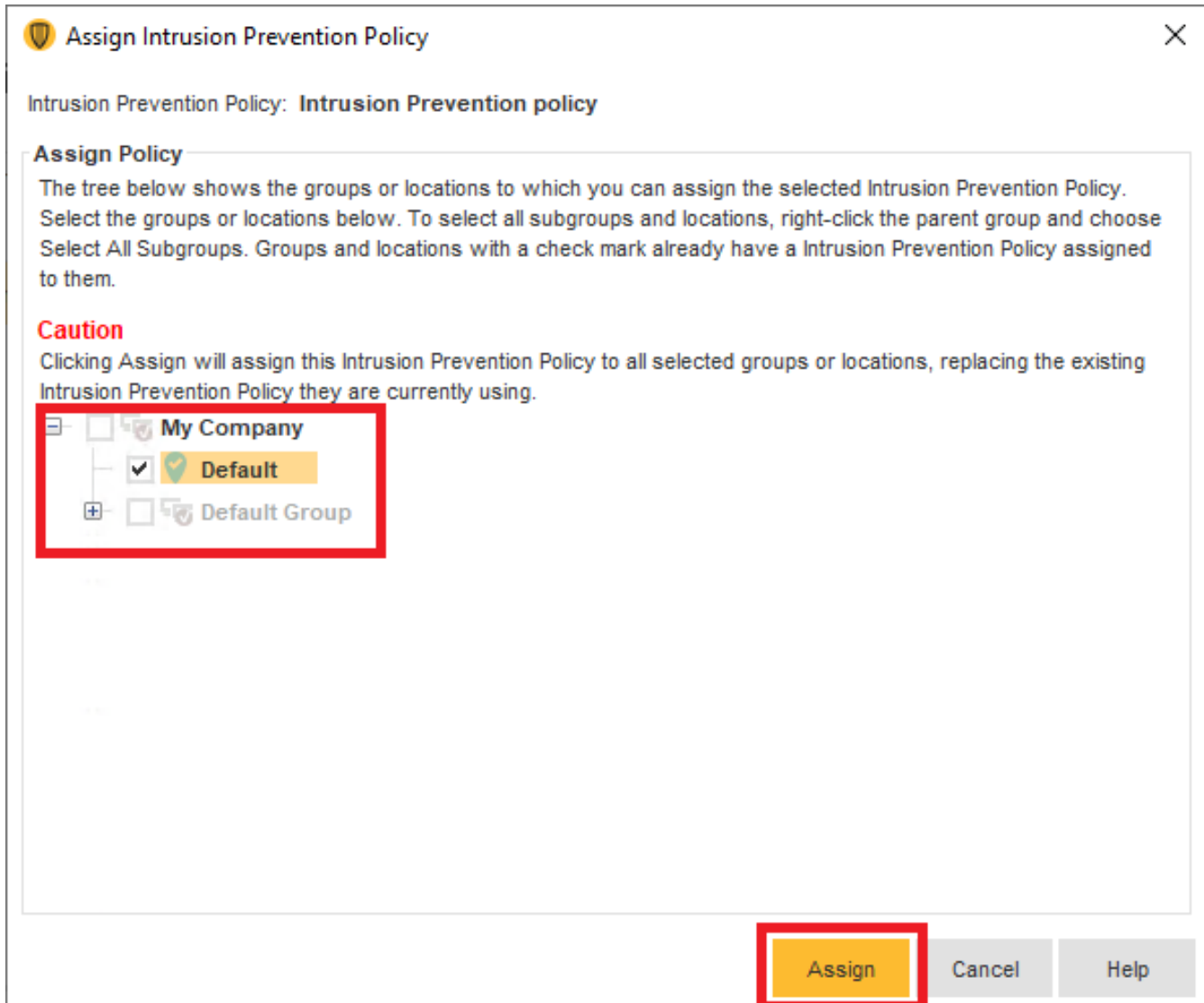


Intrusion Prevention Policies	
Name	Description
Intrusion Prevention policy	Created automatically during product installation

2. 在您進行變更之後，請按一下「確定」。

3. 您必須將政策指派給群組，才能提供防護。大多數政策預設會套用至「我的公司」群組。如果您新增群組，則必須將政策指派給該群組。

4. 若要將政策套用至不同群組或更多群組，請以滑鼠右鍵按一下政策，然後按一下「指派」，並選取一或多個群組，然後再按一下「指派」。



更多資訊

- [建立自訂 Symantec Endpoint Protection Manager 政策](#)
- [指派政策給群組或位置](#)

步驟 7：安裝 Symantec Endpoint Protection 用戶端

使用 Symantec Endpoint Protection Manager 安裝用戶端之前，請檢查以下項目：

- 確保能夠透過網路存取電腦。
- 確保您具有要部署到的電腦的管理員憑證。

安裝 Symantec Endpoint Protection 用戶端

1. 在 Symantec Endpoint Protection Manager 中，按一下「用戶端」>「用戶端」。
如果您稍早已建立群組，則請選取該群組，而不是「我的公司」。
2. 在「工作」下方，按下「安裝用戶端」。
3. 在「用戶端部署精靈」中，按一下「新套件部署」，然後按「下一步」。

4. 在「安裝套件」下拉式清單中，選取與用戶端電腦作業系統相符的作業系統。

– 對於 Windows：

在「安裝功能集」下拉式清單中，保留用戶端完整防護的預設設定。

 Client Deployment Wizard

×

Select Group and Install Feature Sets



Install Packages:

Windows - Symantec Endpoint Protection version 14.3 RU8 - English

Version:

14.3.10158.8000

This selection includes:

WIN64BIT: Windows - Symantec Endpoint Protection version 14.3 RU8 - English (11/8/24)

Group:

My Company\Default Group

Browse...

Install Feature Sets:

Full Protection for Clients

Full Protection for Clients

Full Protection for Servers

Basic Protection for Servers

Protection for Active Directory

Install Settings:

Options...

Content Options:

☐ Include virus definitions in the client installation package.

Uncheck this option to create a smaller client installation package that does not include virus definitions but does include all other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definitions.

在「安裝設定」下拉式清單中，保留 **Windows** 的預設標準用戶端安裝設定的預設設定。

用戶端安裝可能不需要重新啟動。若要變更重新啟動設定，您必須先新增自訂「安裝設定」套件。新增用戶端套件之後，按一下「選項」以選取自訂套件。請參閱：

[在 Symantec Endpoint Protection Manager 中建立自訂用戶端安裝套件](#)

除非處於特定情況，否則您可能不需要重新啟動 Windows 電腦。請參閱[從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)。

– 對於 Linux：

按「下一步」。Linux 套件會被限制為使用「網路連結與電子郵件」或「儲存套件」部署方法。請參閱：

[安裝 Symantec Endpoint Protection Linux Agent](#) 或 [Symantec Single Agent for Linux](#)

– 對於 Mac：

保留「升級設定」的預設設定，然後按「下一步」。

5. 選擇將用戶端安裝套件部署至您電腦的最佳方法。

– [透過儲存套件安裝 Symantec Endpoint Protection 用戶端](#)

– [透過遠端推送安裝 Symantec Endpoint Protection 用戶端](#)

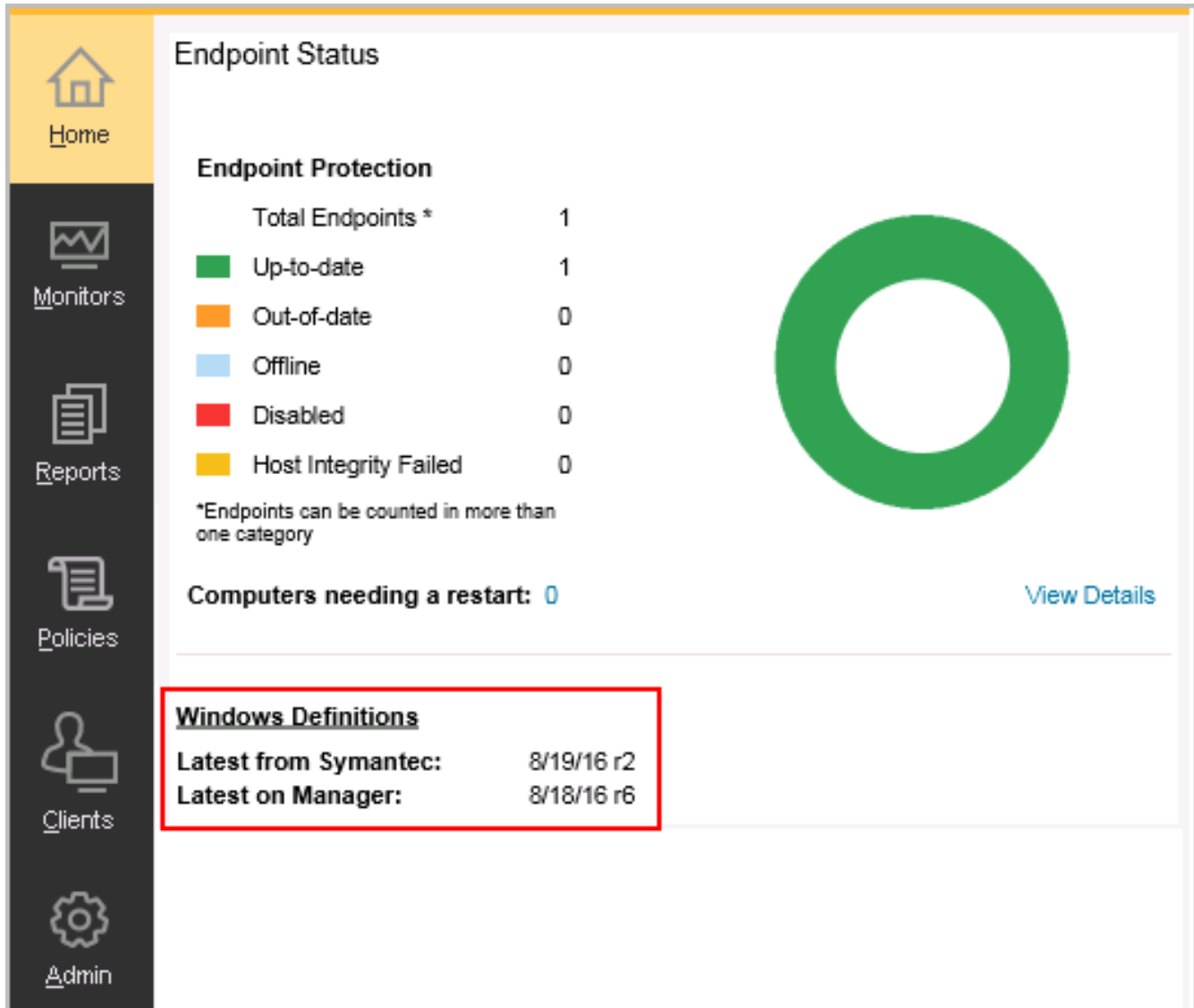
步驟 8：驗證用戶端是否與管理伺服器通訊

若要確認用戶端已成功安裝，請檢查您在「用戶端」窗格中新增的用戶端群組中是否包含此用戶端。請參閱：

[檢查用戶端是否已連線至管理伺服器且受保護](#)

步驟 9：檢查是否已安裝最新定義檔

1. 在 Symantec Endpoint Protection Manager 的左窗格中，按一下「首頁」。
2. 在「端點狀態」方塊中的「**Windows** 定義檔」下方，比較「管理程式最新定義檔」以及「**Symantec** 最新定義檔」的日期。



3. 如果日期不相符，請按一下「說明」>「入門指南」頁面，按一下「立即執行 **LiveUpdate**」，然後按一下「下載」。

安裝 Symantec Endpoint Protection Manager

安裝管理伺服器及主控台時，您需要執行數項工作。在安裝精靈中，每個已完成的任務旁將顯示綠色核取記號。

如需最新系統需求，請參閱：

[所有 Endpoint Protection 版本的版本說明、新修正和系統需求](#)

另外，Symantec Endpoint Protection Manager 安裝和組態會檢查所需權限的安全政策，以讓虛擬服務帳戶正確執行。Symantec Endpoint Protection Manager 會自動變更本機安全政策，並警示您對網域安全政策進行必要的變更。您也可以安裝之前變更安全政策。請參閱：

NOTE

Symantec Endpoint Protection Manager 需要系統登錄的完整存取權才能進行安裝和一般作業。

NOTE

如果在 IPv6 網路中安裝 Symantec Endpoint Protection Manager 14.2，您還必須針對 Java 提供 IPv4 堆疊，即使 IPv4 已停用。如果已解除安裝 IPv4 堆疊，Java 將無法運作，並且 Symantec Endpoint Protection Manager 安裝失敗。

安裝 Symantec Endpoint Protection Manager

1. 若已下載產品，請將完整的安裝檔案擷取至實體磁碟，例如：硬碟。從實體磁碟執行 **Setup.exe**。
安裝作業應能自動啟動。若未啟動，請開啟安裝檔案，然後連按兩下 **Setup.exe**。
2. 在「**Symantec Endpoint Protection 安裝程式**」對話方塊上，依序按下「安裝 **Symantec Endpoint Protection**」和「安裝 **Symantec Endpoint Protection Manager**」。
3. 檢閱安裝事件的順序，然後按「下一步」開始。
4. 在「授權許可協議」畫面中，按下「我接受授權許可協議中的條款」，再按「下一步」。
5. 在「目的資料夾」畫面中，接受預設目的資料夾或指定其他的目的資料夾，再按「下一步」。
6. 按下「安裝」。

Symantec Endpoint Protection Manager 管理伺服器 and 主控台的安裝程序即開始。安裝完成後，按「下一步」。

7. 初始安裝完成後，您便可以架構伺服器和資料庫。按「下一步」。
如果管理伺服器執行 Windows Server 2008 R2，則您可能會看到重新啟用 TLS 1.1 的訊息。您必須先重新啟用 TLS，再前往下一個步驟。請參閱：[於安裝或升級期間在 Microsoft Windows Server 2008 R2 上啟用 TLS 1.0 和 1.1](#)
「管理伺服器組態精靈」隨即啟動。請參閱：
 - [安裝後架構 Symantec Endpoint Protection Manager](#)
 - [使用自訂組態安裝 Symantec Endpoint Protection Manager](#)

更多資訊

[第一次在 Symantec Endpoint Protection Manager 上啟動並執行](#)

架構 Symantec Endpoint Protection Manager 安裝

管理伺服器組態精靈會在安裝 Symantec Endpoint Protection Manager 後自動啟動。根據您的需求架構管理伺服器。

安裝之後，您也可以從「開始 > 所有程式 > **Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager 工具**」隨時啟動「管理伺服器架構精靈」。請參閱：

[安裝 Symantec Endpoint Protection Manager](#)

若要架構 Symantec Endpoint Protection Manager 安裝

1. 選取「新安裝的預設架構 (少於 500 個用戶端)」後，請按「下一步」。
預設架構會自動安裝預設資料庫 Microsoft SQL Server Express (14.3 RU1 和更新版本)。14.3 版 MPx 和更舊版本會將內嵌資料庫安裝為預設資料庫。
2. 輸入您的公司名稱、預設管理員 `admin` 的密碼，以及電子郵件地址。
或者，您可以新增詳細資料以使用指定的郵件伺服器。

3. 可選擇性地按下「傳送測試電子郵件」。

Symantec Endpoint Protection Manager 會將密碼復原資訊和其他重要通知傳送至此電子郵件帳戶。請先確定您接收到電子郵件訊息，再繼續進行架構。

4. 一旦確認您收到測試電子郵件，請按「下一步」。

若為 14.3 MPx 及更舊版本，指示是否要在安裝過程中執行 LiveUpdate。按「下一步」。自 14.3 RU1 起，LiveUpdate 會作為全新安裝的一部分自動執行。

5. 從 14.3 RU10 開始，在「預設用戶端密碼」頁面上，建立一般使用者必須鍵入以停止或解除安裝用戶端軟體的密碼，然後按「下一步」。

6. 您也可以新增選擇性「夥伴資訊」，然後按「下一步」。

如果夥伴管理您的賽門鐵克授權，則請填寫此欄位。

7. 指示是否希望賽門鐵克接收匿名資料，然後按「下一步」開始建立資料庫。

您可能會看到一則訊息，指出可能無法繼續安裝 Microsoft Server Express。如果您的電腦具有最新 Microsoft 更新，則請按一下「繼續」。

建立資料庫可能需要幾分鐘時間。

8. 資料庫建立完成後，請按一下「完成」以完成 Symantec Endpoint Protection Manager 架構。

如果您將「啟動 **Symantec Endpoint Protection Manager**」保留勾選狀態，則會出現 Symantec Endpoint Protection Manager 主控台登錄畫面。在您登入之後，可以開始部署用戶端。請參閱：

[登入 Symantec Endpoint Protection Manager 主控台](#)

您可以在安裝 Symantec Endpoint Protection Manager 所在伺服器的下列位置尋找組態摘要：

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

架構自訂 Symantec Endpoint Protection Manager 安裝

如果您想要將 Symantec Endpoint Protection Manager 與 Microsoft SQL Server 資料庫一起安裝，或想要安裝多個網站，則應該選擇「管理伺服器架構精靈」中的「自訂架構」。當您選取此選項時，更多設定會變成可用。

NOTE

若要提供與資料庫的連線，必須在執行 Symantec Endpoint Protection Manager 的伺服器上安裝 SQL Server 用戶端工具。

如需詳細資訊，請參閱：

[關於 SQL Server 組態設定](#)

使用自訂組態安裝 **Symantec Endpoint Protection Manager**

1. [安裝 Symantec Endpoint Protection Manager](#)

2. 在「管理伺服器組態精靈」中，按下「新安裝的自訂組態」，然後按「下一步」。

針對較少數量的電腦，按一下「新安裝的預設架構 (少於 500 個用戶端)」。請參閱：

[安裝後架構 Symantec Endpoint Protection Manager](#)

3. 按下「安裝我的第一個網站」，然後按「下一步」。

下列選項適用於進階安裝，且不適用於 Symantec Endpoint Protection Manager 的首次安裝。

- 如需安裝額外的管理伺服器到現有站台，請參閱：

[設定容錯移轉和負載平衡](#)

- 若需「安裝其他網站」，請參閱：

-
- [設定站台和複寫](#)
 - [如何安裝第二個站台用於遠端複製](#)
 - [遠端複製的運作方式](#)

4. 在此畫面上，您可以自訂下列設定，然後按「下一步」：

- 站台名稱
- 埠號
在您變更預設 Symantec Endpoint Protection Manager 連接埠架構之前，應該聯絡網路管理員。
- Symantec Endpoint Protection Manager 伺服器儲存資料夾的位置
如果 Symantec Endpoint Protection Manager 安裝所在的磁碟機上沒有足夠的可用空間，請將伺服器儲存資料夾重新定位到替代磁碟機。

5. 在資料庫選取畫面上，按下「**Microsoft SQL Server 資料庫**」，然後按「下一步」。

- 如果為 5,000 個或更少之用戶端的自訂組態選取「預設 **Microsoft SQL Server Express 資料庫**」，請移至步驟 9。不過，此程序的其餘部分假設您選取 Microsoft SQL Server 資料庫。
- 請洽詢 SQL 資料庫管理員以確認是否應該啟用自動資料庫維護任務。
- 賽門鐵克建議您在單獨的實體伺服器上主控 SQL Server 和 Symantec Endpoint Protection Manager。
- 如需所支援 Microsoft SQL Server 版本的相關資訊，請參閱：
[Symantec Endpoint Protection 和 Endpoint Security 的版本、系統需求、發行日期、附註和修正](#)

6. 按下「建立新的資料庫」，然後按「下一步」。

NOTE

使用現有資料庫視為進階安裝選項，通常不適用於新安裝。

7. 在「步驟一：驗證資料庫伺服器」畫面上，填寫 Symantec Endpoint Protection Manager 連線之 SQL Server 的詳細資料，然後按下「連線至資料庫」。

如果資料庫連線成功，則「步驟二：建立新資料庫」區段會變為可用。

8. 在「步驟二：建立新資料庫」下方，填寫用於建立資料庫的詳細資料，然後按「下一步」。

如需有關「驗證資料庫伺服器」或「建立資料庫」的問題，請聯絡 SQL Server 資料庫管理員。

如果想要在 FIPS 140-2 遵從模式下使用 SQL Server，您必須在啟動 SQL Server 之前啟用 FIPS。如果您看到下列訊息，並且想要啟用 FIPS 模式，請按一下「是」以啟用選項，確保管理伺服器執行憑證驗證。

Authentication type: SQL Server Authentication

Database server: XX.XX.XXX.XX

SQL server port: 1433

SQL Server client folder: C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn Browse...

Step Two: Existing Database Parameters

Database name: sem5

Database user name: sem5

Database password:

Warning



Symantec Endpoint Protection Manager (SEPM) uses TLS to connect to the SQL Server database. However, SQL Server may use a temporary self-signed certificate which the SEPM Windows server does not trust; therefore, the SEPM relies on SQL Server IP address or hostname to trust its source other than the certificate. This may expose you to potential SQL Server spoofing.

You can make one of the following choices:

1. You must ensure that Windows trusts this certificate. Therefore, you must provide the certificate on the server computer by importing it into Windows. See [Ensuring that Windows trusts the SQL Server's certificate..](#) Then, click **Yes** to continue the management server configuration.
2. Click **No** to let the Symantec Endpoint Protection Manager use the server IP address or hostname to trust its source rather than the certificate. Only choose this option if both the Symantec Endpoint Protection Manager and SQL Server database are on a secured network.

Yes

No

9. 輸入公司名稱、預設管理員 admin 的密碼，以及電子郵件地址。

或者，您可以新增詳細資料以使用指定的郵件伺服器。

10. 按一下「傳送測試電子郵件」。一旦確認您收到測試電子郵件，請按「下一步」。

Symantec Endpoint Protection Manager 會將密碼復原資訊和其他重要通知傳送至此電子郵件帳戶。在您接收到電子郵件之後，請繼續進行此架構。

11. 在「用戶端密碼」面板上，新增下列密碼，然後按「下一步」。

- 「用戶端通訊密碼」保護用戶端與 Symantec Endpoint Protection Manager 之間的通訊，並儲存在 Symantec Endpoint Protection Manager 復原檔案中。
- 「預設用戶端密碼」用來防止停止或解除安裝用戶端服務或是匯入政策 (14.3 RU10 和更新版本)。您可以稍後在群組層級變更密碼。

如需密碼需求的相關資訊，請參閱[建立用戶端密碼](#)

12. 指示是否要在安裝過程中執行 LiveUpdate。如果在新安裝的過程中執行 LiveUpdate，內容會更方便於供您部署的用戶端使用。按「下一步」

如果夥伴管理您的賽門鐵克授權，則您也可以新增選擇性「夥伴資訊」。

13. 指示是否希望賽門鐵克接收匿名資料，然後按「下一步」開始建立資料庫。

14. 建立和初始化資料庫後 (可能需要幾分鐘的時間)，按下「完成」。

如果您將「啟動 **Symantec Endpoint Protection Manager**」保留勾選狀態，則會出現 Symantec Endpoint Protection Manager 主控台登錄畫面。在您登入之後，可以開始部署用戶端。

請參閱[登入 Symantec Endpoint Protection Manager 主控台](#)。

您可以在安裝 Symantec Endpoint Protection Manager 所在伺服器的下列位置尋找組態摘要：

```
ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc  
\SEPMConfigurationSummaryInfo.txt
```

如需詳細資訊，請參閱：

[關於選擇資料庫類型](#)

登入 Symantec Endpoint Protection Manager 主控台

您可以在安裝 Symantec Endpoint Protection Manager 之後登入 Symantec Endpoint Protection Manager 主控台。有兩種方式可以登入主控台：

1. 透過本機，從安裝管理伺服器的電腦。

您也可以從連線至管理伺服器的獨立式網頁瀏覽器，存取報告功能。請參閱：

[從獨立式網頁瀏覽器登入報告](#)

2. 透過遠端，從符合遠端主控台之系統需求並且可網路連線至管理伺服器的任何電腦。您可以登入遠端 Web 主控台或遠端 Java 主控台。請參閱：

[遠端登入 Symantec Endpoint Protection Manager](#)

基於安全性，主控台最遲會在一小時後將您登出。您可以縮短該時間。請參閱：

[變更保持登入 Symantec Endpoint Protection Manager 主控台的逾時期間](#)

本機登入 Java 主控台

本機登入 Java 主控台

1. 移到「開始 > 程式 > **Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**」。

2. 在 **Symantec Endpoint Protection Manager** 登入對話方塊中，輸入您在安裝期間所架構的使用者名稱 (預設為 admin) 和密碼。

可選擇勾選「記住我的使用者名稱」和「記住我的密碼」(如果有的話) 中的一項或兩項。請參閱：

[顯示「忘記了您的密碼？」連結，以便管理員可以重設遺失密碼](#)

— 若要使用 PIV 卡或 CAC 登入，請按下「選項」，然後勾選「登入智慧卡」(14.2 或更新版本)。在「登入/PIN」訊息中，輸入您的 PIN 號碼。請參閱：

架構 Symantec Endpoint Protection Manager 以驗證使用智慧卡登入的管理員

- 若要使用雙因素驗證登入，請輸入密碼，後面緊接 Token。如果省略 Token，則登入嘗試會失敗。如果您使用 Symantec VIP 智慧型手機應用程式，請輸入密碼，然後在按下「登入」後核准應用程式上的要求。如果您未在 2 分鐘內核准要求，則登入嘗試會失敗。請參閱：

使用 Symantec VIP 架構雙因素驗證

如果主控台有一個以上的網域，請按下「選項」，然後輸入網域名稱。請參閱：[新增網域](#)

3. 按下「登入」。

遠端登入 Web 主控台

若要遠端登入，您必須知道已安裝管理伺服器電腦的 IP 位址或主機名稱。此外，請確保網頁瀏覽器的 Internet 選項允許您檢視來自要登入的伺服器的內容，並且支援網頁瀏覽器。如需受支援網頁瀏覽器的清單，請參閱：

所有 Endpoint Protection 版本的版本說明、新修正和系統需求

尋找 IP 位址或主機名稱

1. 在本機登入。
2. 在「我的最愛報告」下的「首頁」上，按一下「依防護技術顯示風險分佈」。
3. 在「依防護技術顯示風險分佈」對話方塊的底部，尋找文字：您可以使用以下內容來啟動 Symantec Endpoint Protection Manager：

`http://<server_ip>:9090/symantec.html`

遠端登入時，可以執行與管理員本機登入時相同的工作。在主控台檢視哪些內容及執行哪些作業取決於您所屬的管理員類型。小型組織中的大多數管理員會以系統管理員身分登入。您可以使用管理權限架構主控台圖示或「開始」功能表項目以啟動。

使用管理員權限啟動 Java 主控台 (僅限 14.x 版本)

1. 對 Windows 桌面上的 **Symantec Endpoint Protection Manager Console** 圖示按滑鼠右鍵，或對「開始」功能表上的 **Symantec Endpoint Protection Manager Console** 項目按滑鼠右鍵。
2. 按一下「屬性」>「進階」>「以管理員身分執行」或是「其他」>「以管理員身分執行」。

對於 Windows Server 2016，請使用管理伺服器安裝所在電腦的主機名稱。

NOTE

如果您安裝的遠端 Java 主控台上使用的是該產品的先前版本，必須在升級至更新版本後重新安裝主控台。如果您執行 32 位元版本的 Windows，則無法登入 Symantec Endpoint Protection Manager 厚遠端主控台 (14.3 和更新版本)。Oracle Java SE Runtime Environment 不再支援 32 位元版本的 Microsoft Windows。遠端 Web 主控台會改而使用 JRE 版本 11。

登入 Web 主控台

1. 開啟支援的網頁瀏覽器，然後在位址方塊中輸入下列位址：

`http://<server_ip>:9090/`

其中 <server_ip> 是管理伺服器的主機名稱或 IP 位址。

IP 位址包括 IPv4 和 IPv6 (14.2 及更新版本)。必須用方括弧括住 IPv6 位址。例如：`http://[<server_ip>]:9090/`



2. 在「Symantec Endpoint Protection Manager 主控台 Web 存取」頁面，按下所需的主控台類型。
 - 如果按下「**Symantec Endpoint Protection Manager Web 主控台**」，將會載入一個安全的網頁，讓您可以從遠端登入而不使用 Java Runtime Environment (JRE)。
 - 如果按下「**Symantec Endpoint Protection Manager 主控台**」，您登入時使用的電腦必須已安裝 JRE 才能執行 Java 用戶端。如果沒有，您必須下載並安裝該程式。請按照提示安裝 JRE，並按照提供的任何其他指示操作。另一個選項不是遠端管理解決方案。您可按下「**Symantec Endpoint Protection Manager 憑證**」，系統會提示您下載管理主控台的憑證檔案。然後，您可以視需要將此檔案匯入網頁瀏覽器。
3. 如果出現主機名稱訊息，請按下「是」。

此訊息表示您指定的遠端主控台 URL 與 Symantec Endpoint Protection Manager 憑證名稱不符。如果您登入並指定 IP 位址，而不是指定管理伺服器的電腦名稱，就會發生此問題。

如果出現網頁安全憑證警告，請按下「繼續瀏覽此網站 (不建議)」，然後新增自我簽署憑證。
4. 遵照提示來完成登入程序。

如果這是在安裝後第一次登入，請使用帳戶名稱 `admin`。

根據登入方法，您可能需要提供其他資訊。例如，如果主控台有多個網域，請按下「選項」，並提供所要登入之網域的名稱。
5. 如果您使用的是 Java 型主控台，您可以選擇儲存使用者名稱和密碼。按下「登入」。

您可能會在遠端主控台啟動時，收到一或多個安全性警告訊息。如果確實如此，請按下「是」、「執行」、「啟動」，或同等功能的選項，然後繼續操作直到主控台出現。

根據需要接受 Symantec Endpoint Protection Manager 主控台要求的自我簽章憑證。

[接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證](#)

更多資訊

[授予或攔截對遠端 Symantec Endpoint Protection Manager 主控台的存取](#)

在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息

啟用或匯入 Symantec Endpoint Protection 產品授權

您可以使用「授權啟用精靈」工作流程執行下列工作：

- 啟用新的付費授權。
- 將試用授權轉換為付費授權。
- 續購授權。
- 啟用其他已付費授權，以回應過度部署狀態。

您可以使用從偏好的經銷商收到的檔案或序號匯入並啟用授權：請參閱：

合作夥伴定位器

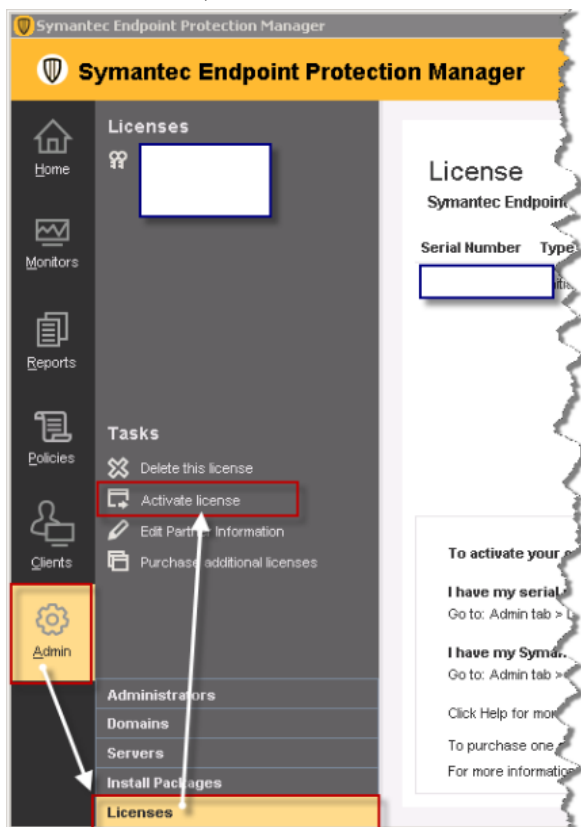
您可以透過下列方式啟動「授權啟用精靈」：

- 安裝產品之後出現的「入門」畫面。
您還可以透過「說明 > 開始使用頁面」存取「開始使用」畫面。
- Symantec Endpoint Protection Manager 主控台的「管理員」頁面。

如果從「入門指南」畫面啟用或匯入授權，您可以跳至步驟 3。

啟用或匯入 Symantec Endpoint Protection 產品授權

1. 在 Symantec Endpoint Protection Manager 中，按下「管理員 > 授權」。
2. 在「工作」下方，按下「啟用授權」。



3. 按下「啟用新授權」，然後按「下一步」。如果您沒看到此面板，請繼續下一個步驟。

License Activation Wizard

License Activation

This wizard is used to activate or renew your Symantec product license. What would you like to do?

☒ Activate a new license

☐ Renew an existing license

These procedures assume you have already purchased a product license and...

4. 在「授權啟用」面板上，選取符合您的情況的選項，再按「下一步」。

License Activation Wizard

License Activation

License activation requires that you enter a license serial number or select a license serial number or Symantec license file in an email after you purchase your product

☒ I have a serial number

☐ I have a Symantec License file (.slf) [? What's this?](#)

These procedures assume you have already purchased a product license and... available. If you do not have a license serial number or license file, contact your partner.

下表描述每個選項：

選項	說明
我有序號	當您或您的偏好經銷商已購買授權時，您可能會收到授權序號。如果您有授權序號，請選取此選項。如果您有序號，請選擇「我有賽門鐵克授權檔」。

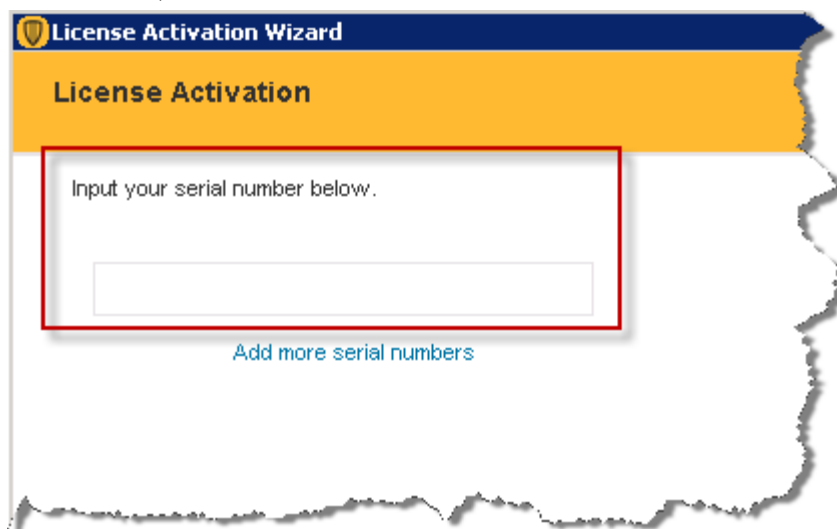
我有賽門鐵克授權檔 (.slf)	在大多數情況下，在您完成購買程序之後，很快就會收到 Broadcom 用電子郵件傳送給您的賽門鐵克授權檔 (.slf 檔)。這個檔案會以 .zip 檔的形式隨通知電子郵件一併送達。如果您已收到 .slf 檔，請選取此選項。 Note: 您必須先從 .zip 檔解壓縮 .slf 檔，才能用它來啟用產品授權。 Warning! .slf 檔包含您的授權專屬的資訊。為避免損壞授權檔，請不要修改其內容。您可以複製該檔案作為記錄。

5. 根據您在上一個步驟中選取的選項，執行下列其中一項工作：

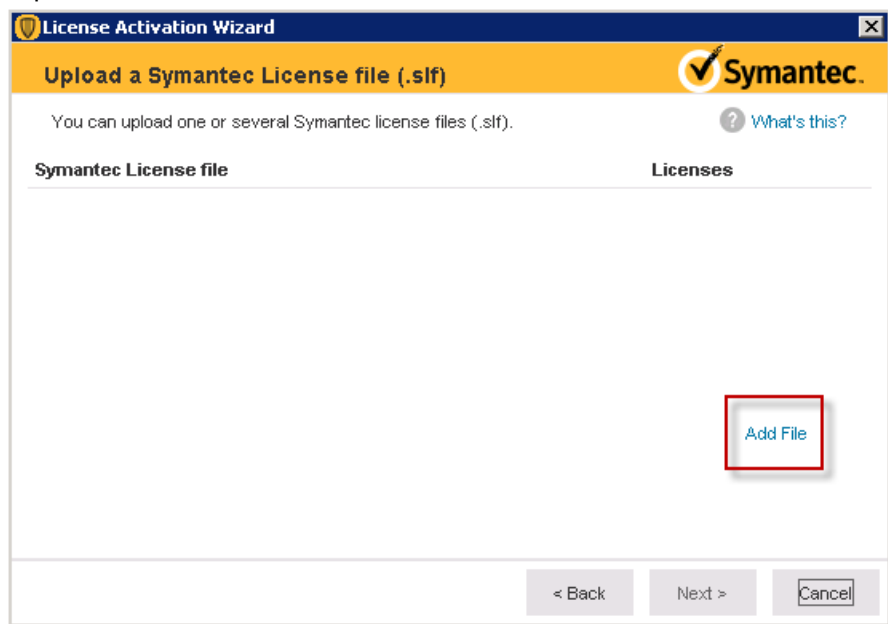
- 如果您選取「我有序號」，請輸入序號，然後按下「提交」。檢閱您新增的授權相關資訊，然後按「下一步」。

NOTE

若要使用序號啟用授權，您必須擁有作用中 Internet 連線並可連線至賽門鐵克授權伺服器。如果連線成功，將載入賽門鐵克首頁。



- 如果您選取「我有賽門鐵克授權檔 (.slf)」，請按下「新增檔案」。瀏覽並選取您從隨附於賽門鐵克通知電子郵件之 .zip 檔解壓縮的 .slf 檔。按下「開啟」，再按「下一步」。



6. 輸入有關技術聯絡人和主要聯絡人的資訊，以及有關公司的資訊。按下認可披露聲明，然後按下「提交」。
如果您在購買授權時提供這項資訊，此面板就不會顯示。

7. 按下「完成」。

更多資訊

- [購買 Symantec Endpoint Protection 授權](#)
- [授權 Symantec Endpoint Protection](#)

購買 Symantec Endpoint Protection 授權

若有下列情形，表示您需要購買授權：

- 您的試用授權已到期。Symantec Endpoint Protection 附有試用版授權，該授權允許您在您的環境中安裝及評估產品。
- 您目前的授權已到期。
- 您目前的授權已過度部署。過度部署表示您部署的用戶端已超過目前授權允許的數目。

根據購買授權的方式，您將透過電子郵件收到產品授權序號或 Symantec 授權檔。授權檔使用 .slf 副檔名。透過電子郵件接收授權檔時，該檔案將以 .zip 檔案的形式附加到電子郵件。您必須從 .zip 檔案解壓縮 .slf 檔案。

購買或續購授權

1. 連絡您偏好的經銷商。請參閱：

[尋找合作夥伴或代理商](#)

將授權檔儲存到可從 Symantec Endpoint Protection Manager 主控台進行存取的電腦。許多使用者將授權儲存在裝載 Symantec Endpoint Protection Manager 的電腦上。為了安全起見，許多使用者也將授權複本儲存到不同的電腦或抽取式儲存媒體上。

WARNING

為了避免授權檔損毀，請不要以任何方式開啟或改變檔案內容。不過，您可以根據需要複製和儲存授權。

更多資訊

[Symantec Endpoint Protection 產品授權需求](#)

[我需要多少個 Symantec Endpoint Protection 授權？](#)

[授權 Symantec Endpoint Protection](#)

Symantec Endpoint Protection (SEP) 所需的外部 URL

Symantec Endpoint Protection 會與特定 URL 通訊以執行多種功能，例如驗證授權、提交可疑檔案的範例，以及與內部部署 Symantec Endpoint Protection Manager 或雲端主控台通訊。如果在環境中使用一個或多個代理，將必要的流量重新導向到賽門鐵克伺服器，則您必須允許這些 URL。請參閱：

[Symantec Endpoint Protection \(SEP\) 和 Symantec Endpoint Protection \(SES\) 所需的外部 URL](#)

所需的 **Broadcom** URL

您應允許防火牆的以下 URL 存取 Broadcom 登入頁面和入口網站、下載軟體、存取文件以及建立支援案例。這些 URL 使用埠 80。

Table 5: Broadcom URL

用途	URL
針對所有 Okta 代理程式和一般使用者連線至 Okta。	• http://login.okta.com
下載 Broadcom 軟體、支援文件和其他檔案所需的 URL。	• http://api-broadcomcms-software • http://broadcomcms-software • http://broadcom.com • http://www.broadcom.com/ • http://downloads.broadcom.com • http://support.broadcom.com • http://images.sw.broadcom.com • http://secure.sw.broadcom.com
Volken 案例管理入口網站讓使用者可以為 CA、Carbon Black、Mainframe 軟體、Symantec、Tanzu 和 VMware 等產品建立和管理 Broadcom 支援案例。	• http://api-csm.wolkenservicedesk.com • http://wolkenservicedesk.com • http://wmaster.wolkenservicedesk.com • http://cdn.wolkenservicedesk.com • http://brcmsemiconductor-csm.wolkenservicedesk.com

使用儲存套件安裝 Symantec Endpoint Protection 用戶端

如果您擁有較少數目的用戶端，請使用儲存套件方法在用戶端上部署和安裝安裝套件。

儲存套件會建立安裝套件，讓您可以手動安裝、使用第三方部署軟體安裝或使用登入程序檔安裝。

「儲存套件」包含下列工作：

- 選擇架構，然後建立用戶端安裝套件。
- 將安裝套件儲存到執行 Symantec Endpoint Protection Manager 之電腦的資料夾中。
針對 Windows，安裝套件可以是 32 位元 (14.3 RU5 和更舊版本) 或 64 位元作業系統。安裝套件由一個 setup.exe 檔案或一組包含 setup.exe 檔案的多個檔案所組成。對電腦使用者而言，單一 setup.exe 檔案通常較容易使用。

NOTE

Mac 和 Linux 用戶端安裝套件會自動匯出 .zip 封存檔案格式。若要正確保留檔案權限，您應使用原生封存程式展開封存檔案，如 Mac「#####」或 ditto 指令。在這些作業系統上，您不能使用 Mac 的 unzip 指令、第三方應用程式或任何 Windows 應用程式來展開檔案

使用儲存套件安裝 Symantec Endpoint Protection 用戶端

1. 在主控台中，啟動「用戶端部署精靈」。
2. 在「用戶端部署精靈」中，執行下列其中一項工作：
 - 按下「新套件部署」，再按「下一步」。「儲存套件」僅安裝新的安裝套件。
 - 如果您想要在已安裝 Symantec Endpoint Protection 用戶端的電腦上更新 Windows 或 Mac 用戶端通訊設定，請按下「通訊更新套件部署」。按照畫面上的指示進行，然後移至步驟 4。
3. 從可用選項 (隨安裝套件類型而異) 中選擇，再按「下一步」。

NOTE

若要移除 Windows 用戶端上的現有安全軟體，您必須先架構自訂「用戶端安裝設定」，再啟動「用戶端部署精靈」。請參閱：

[架構用戶端套件來解除安裝現有安全軟體](#)

如需詳細資訊，請參閱：

關於 Windows 用戶端安裝設定

4. 按下「儲存套件」，再按「下一步」。
5. 按下「瀏覽」並指定要接收套件的資料夾。

如果是「通訊更新套件部署」或是 Mac 和 Linux 套件，請移至步驟 7。

如果是新的 Windows 套件，請勾選「單一 .exe 檔案 (預設)」或「獨立檔案 (.MSI 必需)」。

NOTE

除非您需要獨立檔案供第三方部署程式使用，否則使用「單一 .exe 檔案」。

6. 按「下一步」。
7. 檢閱設定摘要，然後按「下一步」，再按下「完成」。
8. 將匯出的套件提供給電腦使用者。

使用下列方式將匯出的套件提供給使用者：電子郵件、將套件儲存於安全的共用網路位置，或使用第三方案式。

9. 確認使用者下載並安裝用戶端軟體，以及確認用戶端的安裝狀態。

Mac 用戶端在安裝完成時會自動提示重新啟動。不需要重新啟動 Windows (自 14.3 RU4 起) 和 Linux 用戶端。請參閱：

- [執行有關用戶端部署狀態的報告](#)

更多資訊

- [從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)
- [選擇要在用戶端上安裝哪些安全性功能](#)
- [選擇使用用戶端部署精靈安裝用戶端的方法](#)
- [準備用戶端安裝](#)

使用遠端推送安裝 Symantec Endpoint Protection 用戶端

「遠端推送」會將用戶端軟體推送至依 IP 位址或電腦名稱指定的電腦。套件一旦複製到目標電腦之後，套件就會自動安裝。電腦使用者不需要開始安裝或具有管理員權限。

「遠端推送」包含下列工作：

- 選取現有的用戶端安裝套件、建立新的安裝套件，或建立套件以更新通訊設定。
- 如果是新的安裝套件，請架構並建立安裝套件。
- 指定您網路上要從 Symantec Endpoint Protection Manager 接收套件的電腦。

「遠端推送」會找出使用您提供之 IP 號碼或範圍的特定電腦，或是透過瀏覽網路，找出所有可見的電腦。

NOTE

若要将用戶端安裝套件推送到「瀏覽網路」標籤中的 Mac 用戶端，您必須在 Symantec Endpoint Protection Manager 伺服器上安裝 Bonjour 服務。請參閱下列文章：

[部署 Endpoint Protection for Mac 用戶端時發生錯誤：「無法瀏覽網路。遺失 Bonjour 服務。」](#)

[下載 Bonjour for Windows 列印服務](#)

Bonjour 服務不支援 IPv6 網路。僅啟用 IPv6 網路的 Mac 無法顯示在「瀏覽網路」中。

自 14.2 版起支援 IPv6 網路。

- Symantec Endpoint Protection Manager 將用戶端軟體推送到指定的電腦。
套件成功複製到目標電腦後，安裝會在電腦上自動開始。

NOTE

您無法使用「遠端推送」安裝 Linux 用戶端。

使用遠端推送安裝 **Symantec Endpoint Protection** 用戶端

1. 在主控台中，啟動「用戶端部署精靈」。

按一下「說明 > 「開始使用」頁面」，然後在「所需工作」下方按一下「在您的電腦上安裝用戶端軟體」。

2. 在「用戶端部署精靈」中，執行下列其中一項工作：

- 按下「新套件部署」以建立新的安裝套件，然後按「下一步」。
- 按下「現有套件部署」以使用先前建立的套件，然後按下「瀏覽」找出要安裝的套件。
「用戶端部署精靈」會上傳套件，並將您導向至「電腦選取」面板 (步驟 5)。
- 在「通訊更新套件部署」下方，選擇是否要更新已安裝 Symantec Endpoint Protection 用戶端之電腦上的 Windows 或 Mac 用戶端通訊設定。按照畫面上的指示進行，然後移至步驟 4。
使用此選項可將非受管用戶端轉換成受管型用戶端。

如需詳細資訊，請參閱：

[使用「通訊更新套件部署」還原用戶端伺服器通訊](#)

3. 若是新套件，請在「選取群組並安裝功能集」面板中，從可用選項 (隨安裝套件類型而異) 中進行選取。按「下一步」。

NOTE

若要解除安裝 Windows 用戶端上的現有安全軟體，您必須先架構自訂「用戶端安裝設定」，再啟動「用戶端部署精靈」。您也可以使用已架構為啟用此功能的現有用戶端安裝套件。請參閱：

[架構用戶端套件來解除安裝現有安全軟體](#)

如需詳細資訊，請參閱：

[關於 Windows 用戶端安裝設定](#)

4. 按下「遠端推送」，然後按「下一步」。
5. 在「電腦選取」面板中，使用下列其中一種方法找出要接收軟體的電腦：
 - 若要瀏覽網路尋找電腦，按下「瀏覽網路」。
 - 若要依據 IP 位址或電腦名稱尋找電腦，按下「搜尋網路」，再按下「尋找電腦」。

您可以設定逾時值，以限制伺服器套用至搜尋的時間長度。

6. 按下 >>，將電腦新增至清單，若精靈提示驗證網域或工作群組，請相應執行。

遠端推送安裝需要較高的權限。如果用戶端電腦是 Active Directory 網域的一部分，您應使用網域管理員帳戶。

7. 按「下一步」，然後按「傳送」，將用戶端軟體推送至選取的電腦。

「部署摘要」面板指示成功部署後，安裝作業便會自動在用戶端電腦上開始。

安裝作業可能需要數分鐘的時間。

8. 按「下一步」，然後按下「完成」。
9. 在「用戶端」頁面上確認所安裝用戶端的狀態。

NOTE

將用戶端安裝套件遠端安裝至 Mac 用戶端後，必須在用戶端電腦上確認已授權核心延伸。Symantec Endpoint Protection 需要核心延伸授權才能完全運作，如果需要授權，「遠端推送」不會提示您授權。在 Mac 上，勾選「安全性與隱私權」系統喜好設定，然後按下「允許」。

更多資訊

-
- 執行有關用戶端部署狀態的報告
 - 從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦
 - 準備用戶端安裝
 - 準備 Windows 和 Mac 電腦進行遠端部署
 - 選擇要在用戶端上安裝哪些安全性功能
 - 選擇使用用戶端部署精靈安裝用戶端的方法

使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端

「網路連結與電子郵件」選項會建立安裝套件和安裝套件的 URL。使用者以電子郵件的形式收到用於下載套件及安裝 Symantec Endpoint Protection 用戶端的 URL。使用者必須擁有管理員權限才能安裝套件。

網路連結與電子郵件包含下列工作：

- 選取、架構並建立用戶端安裝套件。
從針對 Windows、Mac 和 Linux 用戶端安裝套件的架構顯示的選項中選擇。所有用戶端安裝套件儲存於執行 Symantec Endpoint Protection Manager 的電腦內。
- 從 Symantec Endpoint Protection Manager 寄出電子郵件給電腦使用者，通知他們可以下載用戶端安裝套件。
提供要接收電子郵件訊息的使用者清單，該訊息包含下載和安裝用戶端安裝套件的指示。使用者可依照指示安裝用戶端軟體。

NOTE

Mac 和 Linux 用戶端安裝套件會自動匯出 .zip 封存檔案格式。若要正確保留檔案權限，您應使用原生封存程式展開封存檔案，如 Mac「#####」或 ditto 指令。在這些作業系統上，您不能使用 Mac 的 unzip 指令、第三方應用程式或任何 Windows 應用程式來展開檔案。

在使用「網路連結與電子郵件」之前，請確保正確架構管理伺服器到郵件伺服器之間的連線。請參閱：

[建立管理伺服器與電子郵件伺服器之間的通訊](#)

使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端

1. 在主控台中，啟動「用戶端部署精靈」。
按一下「說明 > 「開始使用」頁面」，然後在「所需工作」下方按一下「在您的電腦上安裝用戶端軟體」。
2. 在「用戶端部署精靈」中，按一下「新套件部署」，然後按「下一步」。網路連結和電子郵件僅傳送新的安裝套件。
3. 從可用選項 (隨安裝套件類型而異) 中選擇，再按「下一步」。

NOTE

若要移除 Windows 用戶端上的現有安全軟體，您必須先架構自訂「用戶端安裝設定」，再啟動「用戶端部署精靈」。請參閱：

[架構用戶端套件來解除安裝現有安全軟體](#)

如需詳細資訊，請參閱：

[關於 Windows 用戶端安裝設定](#)

4. 按下「網路連結與電子郵件」，然後按「下一步」。
5. 在「電子郵件收件者和訊息」面板中，指定電子郵件收件者和主旨。

若指定多位電子郵件收件者，請利用逗號分隔各電子郵件地址。管理主控台系統管理員會自動接收郵件的複本。

您可以接受預設的電子郵件主旨和本文，也可以編輯文字。您也可以複製 URL 並將其貼到內部網路網頁等方便的線上安全位置。

6. 若要建立套件和透過電子郵件傳遞連結，請依序按「下一步」和「完成」。
7. 確認電腦使用者已收到電子郵件訊息並安裝用戶端軟體。
Mac 用戶端在安裝完成時會自動提示重新啟動。不需要重新啟動 Windows (自 14.3 RU4 起) 和 Linux 用戶端。請參閱：

更多資訊

- [執行有關用戶端部署狀態的報告](#)
- [從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)
- [選擇要在用戶端上安裝哪些安全性功能](#)
- [選擇使用用戶端部署精靈安裝用戶端的方法](#)
- [準備用戶端安裝](#)

安裝管理伺服器之後該做什麼？

下表顯示安裝與架構產品後應執行以評估用戶端電腦是否具有正確防護等級的工作。繼續定期執行這些工作 (每週或每月)。

Table 6: 安裝後要執行的工作

動作	說明
修改病毒和間諜軟體防護政策	變更下列預設掃描設定： • 如果您建立伺服器群組，請將排程掃描時間變更為大多數使用者離線的某個時間。請參閱：設定在 Windows 電腦上執行的排程掃描 • 在自動防護中啟用風險追蹤程式。請參閱： 如需詳細資訊，請參閱文章：什麼是風險追蹤程式？ 風險追蹤程式具有以下前提條件： — 已啟用「網路威脅防護」。請參閱： 在用戶端電腦上從主控台執行指令 — 已啟用 Windows 檔案及印表機共用。 如需詳細資訊，請參閱： 自訂 Windows 用戶端的自動防護
修改遠端電腦群組和伺服器群組的防火牆政策	• 確認異地理位置的以下預設防火牆規則已啟用，增進遠端電腦的安全性： — 攔截外部電腦共用本機檔案 — 攔截遠端管理 • 確認下列防火牆規則已啟用，減弱伺服器群組的安全性：「允許本機電腦共用本機檔案」。此防火牆規則會確保僅允許本機流量。 如需詳細資訊，請參閱： • 自訂防火牆規則 • 管理遠端用戶端的位置

動作	說明
將應用程式和檔案排除在掃描範圍之外	您可以將用戶端架構為不掃描特定資料夾和檔案，以增強效能。 例如，用戶端會在每次排程掃描執行時掃描郵件伺服器目錄。您應該從掃描範圍內排除郵件伺服器程式檔和目錄。 如需詳細資訊，請參閱文章： 關於 Microsoft Exchange 伺服器和賽門鐵克產品的檔案和資料夾自動排除 您可以排除已知會於接受掃描時造成問題的資料夾和檔案，以提升效能。例如，Symantec Endpoint Protection 不應掃描專屬 Microsoft SQL Server 檔案。您應該新增例外，防止掃描包含 SQL Server 資料庫檔案的資料夾。這些例外可改善效能，並且避免發生損毀，或在 SQL Server 必須使用檔案時檔案遭到鎖定。 如需詳細資訊，請參閱知識庫文章： 如何使用集中式例外排除 MS SQL 檔案和資料夾 此外，應從掃描中排除誤報。 您也可以依副檔名排除 Windows 電腦上「自動防護」掃描的檔案。請參閱： • 建立病毒和間諜軟體掃描的例外 • 自訂 Windows 用戶端的自動防護 • 自訂 Mac 用戶端的自動防護
在排程掃描後執行快速報告和排程報告	執行快速報告和排程報告，以檢視用戶端電腦是否具有正確的安全性層級。請參閱： • 關於 Symantec Endpoint Protection Manager 報告類型 • 執行和自訂快速報告 • 如何執行排程報告
請檢查確認排程掃描已成功且用戶端依預期執行	檢視監控器、日誌和用戶端電腦的狀態，確認每個群組都具有正確的防護等級。請參閱： 監控 Symantec Endpoint Protection 用戶端
評估內容儲存和用戶端通訊頻寬需求	Symantec Endpoint Protection Manager 只會儲存最新完整版本加上增量差異。這種方式意味著用戶端幾乎都是下載差異，而非完整套件。只有在用戶端過時已久 (超過三個月) 的少數情況下，才需要完整下載最新的內容。請參閱： 如何更新用戶端上的內容和定義檔 如果您的環境必須精確地控制網路頻寬，您也可以調節用戶端通訊。如需詳細資訊，請參閱文章： Symantec Endpoint Protection 的用戶端通訊頻寬控制 如需計算儲存和頻寬需求的詳細資訊，請參閱： Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書
針對單一風險爆發以及偵測到新風險的疫情架構通知	針對「單一風險事件」建立通知，並針對「風險爆發」修改通知。 針對這些通知，賽門鐵克建議您執行下列動作： 1. 將「風險嚴重性」變更為「類別 1 (極低以上)」，以避免接收有關追蹤 Cookie 的電子郵件。 2. 將「調節器」設定保持為「自動」。 通知對於維護安全的環境而言非常重要，而且可以節省您的時間。請參閱： • 設定管理員通知 • 管理通知

更多資訊

- [第一次在 Symantec Endpoint Protection 上啟動並執行](#)
- [Symantec Endpoint Protection 對保護企業環境安全的最佳實務建議](#)

Symantec Endpoint Protection 的通訊埠

如果執行 Symantec Endpoint Protection Manager (SEPM) 和 Symantec Endpoint Protection (SEP) 用戶端的電腦也執行第三方防火牆軟體或硬體，您必須開啟特定通訊埠。這些通訊埠用於遠端部署以及管理伺服器 and 用戶端之間的通訊。如需有關開啟通訊埠或允許應用程式使用通訊埠的指示，請參閱防火牆產品說明文件。

依據預設，Symantec Endpoint Protection 的防火牆元件已經允許這些通訊埠上的流量。

WARNING

在 14.3 RU1 和更舊版本中，依據預設，初始安裝時會停用 Symantec Endpoint Protection 用戶端的防火牆，直到電腦重新啟動為止。為確保受到防火牆防護，請讓用戶端上的 Windows 防火牆保持啟用，直到軟體安裝完成且用戶端重新啟動為止。Symantec Endpoint Protection 用戶端防火牆會在電腦重新啟動時自動停用 Windows 防火牆。

Table 7: 用戶端和伺服器安裝與通訊用通訊埠

通訊埠	通訊協定	用於	接聽程序	版本
22	TCP	從 SEPM 推送部署到 Mac 電腦 - 由 SEPM (clientremote.exe) 起始 - 無法架構	launchd	全部
139, 445 137, 138	TCP UDP	從 SEPM 推送部署到 Windows 電腦 - 由 SEPM (clientremote.exe) 起始 - 無法架構 另也使用 TCP 暫時通訊埠。	svchost.exe :	全部
443	TCP	SEPM (HTTPS) 與 SEP 用戶端之間的通訊 - 由 SEP 用戶端起始 - 可架構 用戶端也使用 TCP 暫時通訊埠。	httpd.exe (Apache)	全部
443	TCP	SEPM 與雲端伺服器之間的通訊 如需新增至雲端主控台之代理略過清單的網域相關資訊，請參閱： 代理錯誤訊息顯示在 Endpoint Protection Manager 的「雲端」標籤 > 「疑難排解」中	prunsvr.exe	全部
443	HTTPS	SEP 漫遊用戶端與 Symantec Endpoint Security 雲端伺服器之間的通訊 與 SEPM 進行間歇性通訊的受管用戶端會將其重大事件直接上傳至雲端主控台。SEPM 必須向雲端主控台註冊。請參閱： 從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端	無	14.2 及更新版本
514	UDP	將資料轉送到 Syslog 伺服器 (選用) - Syslog 伺服器至 SEPM 的離埠流量 - Syslog 伺服器的入埠流量 - 可架構 來往 SEPM 的流量會使用 UDP 暫時通訊埠。	SemSvc.exe	
1100	TCP	主控端物件登錄 指示 AjaxSwing 在哪個通訊埠上執行 RMI 登錄。 - 由 AjaxSwing 起始 - 無法架構	SemSvc.exe	全部
1433	TCP	遠端 SQL Server 資料庫與 SEPM 之間的通訊 - 由 SEPM 起始 - 可架構 SEPM 也會使用 TCP 暫時通訊埠。	sqlserver.exe	全部

通訊埠	通訊協定	用於	接聽程序	版本
2638	TCP	自動安裝的資料庫與 SEPM 之間的通訊 - 由 SEPM 起始 - 可架構	- sqlserver.exe (SQL Server Express 資料庫；14.3 RU1 及更新版本) - dbsrv16.exe (內嵌資料庫；14.3 MP1 及更舊版本)	全部
2967	TCP	群組更新提供者 (GUP) Web 快取代理功能 - 由 SEP 用戶端起始 - 可架構	ccSvcHst.exe	全部
2968	TCP	Web 和雲端存取防護 用戶端驗證 - 由 SEP 用戶端起始 - 可架構	ccSvcHst.exe	14.2 及更新版本
8014	TCP	SEPM (HTTPS) 與 SEP 用戶端之間的通訊 - 由 SEP 用戶端起始 - 可架構 用戶端也使用 TCP 暫時通訊埠。	httpd.exe (Apache)	全部
8081 8082	HTTP HTTPS	SEPM 與 Content Analysis 伺服器硬體裝置或 Malware Analysis 硬體裝置之間的通訊	SEPM	僅限 14.2.x 版。已在 14.3 中棄用。
8443	TCP	伺服器通訊 (HTTPS)。所有登入資訊和管理通訊都是使用此安全通訊埠。 - 由 Java 型遠端主控台或網頁式遠端主控台起始，或是由複寫夥伴起始 - 可架構 SEPM 會接聽此通訊埠。	SemSvc.exe	全部
8445	TCP	由遠端報告主控台使用。 - 由報告主控台起始 - 可架構	httpd.exe (Apache)	全部
8446	TCP	Web 服務 遠端管理應用程式使用此通訊埠透過 HTTPS 傳送 Web 服務流量。 - 由遠端監控與管理 (RMM) 和 EDR 起始 - 可架構 - 用於 Java 遠端主控台	semapisrv.exe	全部
8447	TCP	程序啟動程式 此虛擬服務帳戶會啟動任何需要較高權限的 SEPM 程序，如此其他服務就不需要具有這些程序。僅遵守 localhost 的要求。 - 由 SEPM (SemSvc.exe) 起始 - 可架構	semlaunchsrv.exe	全部
8765	TCP	伺服器控制 由 SEPM for Tomcat Web 服務用於關機。 - 由 SEPM 起始 - 可架構	SemSvc.exe	全部

通訊埠	通訊協定	用於	接聽程序	版本
9090	TCP	Web 主控台通訊 此通訊埠僅用於遠端管理主控台與 SEPM 之間的初始 HTTP 通訊。此初始通訊包括安裝，僅顯示登入畫面。 • 由遠端 Web 主控台起始 • 可架構 另也使用 TCP 暫時通訊埠。	SemSvc.exe	全部

- Windows Vista 及更新版本包含預設已啟用的防火牆。若啟用防火牆，則可能無法遠端安裝或部署用戶端軟體。如果您在將用戶端部署到執行這些作業系統的電腦上時遇到問題，請架構其防火牆以允許所需流量。
- 如果決定在部署後使用 Windows 防火牆，您必須架構它以允許檔案和印表機共用 (通訊埠 445)。

如需架構 Windows 防火牆設定的詳細資訊，請參閱 Windows 說明文件。

更多資訊

- [關於基本管理伺服器設定](#)
- [準備 Windows 和 Mac 電腦進行遠端部署](#)

安裝和解除安裝管理伺服器 and 用戶端

計畫安裝 Symantec Endpoint Protection Manager 和用戶端。

在安裝 Symantec Endpoint Protection Manager 之前，您可能需要考慮以下問題：

- 網路中的用戶端數目。
- 您想要使用哪一個資料庫，預設 Microsoft SQL Server Express 資料庫還是 Microsoft SQL Server。
- 是否設定多個網站。
- 是否設定容錯移轉伺服器。

在安裝 Symantec Endpoint Protection 用戶端之前，您可能需要考慮以下問題：

- 要安裝哪些功能。
- 要使用哪一種部署方法。

網路架構考量

您可以針對測試用途而安裝 Symantec Endpoint Protection，無需考量您的公司網路架構。您可以安裝 Symantec Endpoint Protection Manager 和數個用戶端，並熟悉其特點與功能。

當您準備好安裝正式用戶端時，您應根據您的組織架構和運算需求來規劃您的部署。

規劃部署時應考量下列要素：

- Symantec Endpoint Protection Manager
管理員使用 Symantec Endpoint Protection Manager 管理安全性政策和用戶端電腦。針對已安裝 Symantec Endpoint Protection Manager 的電腦，您可能要考量到安全性與可用性。
- 遠端主控台
管理員可以使用執行主控台軟體的遠端電腦來存取 Symantec Endpoint Protection Manager。管理員不在辦公室時可使用遠端電腦。您應確保遠端電腦符合遠端主控台需求。
- 本機及遠端電腦
遠端電腦的網路連線可能較慢。您可能要使用有別於在本機電腦進行安裝的安裝方法。
- 如筆記型電腦等可攜式電腦
可攜式電腦可能不會定期與網路連線。您可能會想確認可攜式電腦具有啟用 LiveUpdate 排程的 LiveUpdate 政策。未定期登入的可攜式電腦不會取得其他政策更新。
- 位於安全區域中的電腦
位於安全區域的電腦可能需要與位於非安全區域的電腦不同的安全性設定。

確認您計畫安裝用戶端的電腦。賽門鐵克建議您在所有未受防護的電腦上安裝用戶端軟體，包括執行 Symantec Endpoint Protection Manager 的電腦。

更多資訊

[第一次在 Symantec Endpoint Protection 上啟動並執行](#)

關於選擇資料庫類型

Symantec Endpoint Protection Manager 會使用資料庫來儲存用戶端及設定的相關資訊。進行架構程序時，會建立資料庫。您必須先決定要使用的資料庫，再安裝管理伺服器。使用資料庫的管理伺服器架構完畢之前無法使用主控台。

Table 8: Symantec Endpoint Protection Manager 使用的資料庫

資料庫類型	說明
Microsoft SQL Server Express (預設；14.3 RU1 和更新版本) 內嵌資料庫 (預設；14.3 MP1 和更新版本)	預設資料庫會自動與 Symantec Endpoint Protection Manager 一起安裝，且不需要組態。預設資料庫最多支援 5,000 個用戶端。 您還可以個別安裝 SQL Server Express，這確實需要一些組態。 如需詳細資訊，請參閱： 關於基本管理伺服器設定
Microsoft SQL Server	如果選擇使用此選項，您必須在安裝 Symantec Endpoint Protection Manager 之前先安裝 SQL Server 和 SQL Server Native Client。為取得最佳相容性，請安裝與 SQL Server 版本等同的 SQL Server Native Client 版本。 您可考慮購買並安裝 SQL Server，原因如下： - 必須支援 5,000 個以上用戶端。每個使用 SQL Server 的管理伺服器最多都可支援 18,000 個用戶端。如果您的組織有更多用戶端，則可安裝另一台管理伺服器。 - 需支援容錯移轉和負載平衡。 - 您需要將其他的管理伺服器設為網站夥伴。請參閱： 判斷需要的網站數量 如果您建立的是 SQL Server 資料庫，則必須先在本機或遠端伺服器上安裝 SQL Server 實例。然後，您必須架構它，以便與管理伺服器進行通訊。請參閱： 關於 SQL Server 組態設定

關於基本管理伺服器設定

當您安裝 Symantec Endpoint Protection Manager 時，下列值表示預設設定。

只有使用自訂組態安裝 Symantec Endpoint Protection Manager 時，才能架構部分下列值。

如需詳細資訊，請參閱：

- [安裝 Symantec Endpoint Protection Manager](#)
- [Symantec Endpoint Protection 的通訊埠](#)
- [Symantec Endpoint Protection Manager 的帳戶名稱和密碼要求](#)

Table 9: 基本伺服器設定

設定	預設	說明
站台名稱	我的站台 (預設值) 站台##### (自訂)	出現在 Symantec Endpoint Protection Manager 中的站台名稱。網站名稱是用來架構所有功能並且在 Symantec Endpoint Protection Manager 內執行這些功能的最高層級容器。
伺服器名稱	#####	執行 Symantec Endpoint Protection Manager 的電腦名稱。
伺服器儲存資料夾	SEPM_Install\data	Symantec Endpoint Protection Manager 放置資料檔案 (包括備份、遠端複製日誌和其他檔案) 的目錄。如果不存在，安裝程式會建立這個目錄。 SEPM_Install 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。
加密密碼	無	此密碼會加密 Symantec Endpoint Protection Manager 和用戶端之間的通訊。 如果您選擇預設組態，則系統會自動為您產生加密密碼。您可以從摘要畫面將這項資訊列印或複製到剪貼簿。 如果您選擇自訂組態，可以讓系統自動產生隨機密碼，或是建立自己的密碼。密碼可為 8-32 (14.3 RU5 及更高版本) 或 6-32 (14.3 RU4 及更早版本) 個英數字元。 記下這個密碼並妥善保管。建立資料庫之後，您無法變更或還原密碼。如果您沒有可還原的備份資料庫，也必須輸入這個密碼，才能夠進行災難復原。請參閱： Endpoint Protection 的災難復原最佳實務

設定	預設	說明
使用者名稱	admin	第一次登入 Symantec Endpoint Protection Manager 主控台時所使用的預設使用者名稱。這個值不可架構。
密碼	無	伺服器架構期間為管理員帳戶指定的密碼。 您需要原始管理員密碼才能在稍後重新架構管理伺服器。記下這個密碼並妥善保管。
電子郵件地址	無	系統通知會傳送到指定的電子郵件地址。

關於 SQL Server 架構設定

如果您安裝 Symantec Endpoint Protection Manager 搭配 SQL Server 資料庫使用，SQL Server 有特定的架構需求。

建立資料庫之前，Symantec 建議您另外安裝符合 Symantec 安裝及架構需求的 SQL Server 實例。您可在現有實例內安裝資料庫，但必須正確架構此實例，否則資料庫安裝會失敗。例如，如果選取區分大小寫的 SQL 定序，安裝會失敗。

WARNING

若要確保遠端 SQL Server 通訊的最高安全，請將兩台伺服器置於同一安全子網路中。

Table 10: 必要的 SQL Server 組態設定

架構設定	安裝需求
實例名稱	不要使用預設實例名稱。請建立如 SEPM 的名稱。 根據預設，安裝 Symantec Endpoint Protection Manager 時，會在 SQL Server 實例中建立名為 Sem5 的資料庫。預設名稱雖然受到支援，但如果您在同一電腦上安裝多個實例，就可能會造成混淆。
驗證架構	「混合」模式或「Windows 驗證」模式。請參閱： 關於 SQL Server 資料庫驗證模式
sa 密碼	設定「混合模式」驗證時，請設定此密碼。
啟用的通訊協定	TCP/IP
TCP/IP 的 IP 位址	啟用 IP1 和 IP2
IP1、IP2 及 IPALL 的 TCP/IP 埠號	將「TCP 動態通訊埠」留白，並指定 TCP 埠號。通常，預設通訊埠為 1433。請在建立資料庫時指定此埠號。 Symantec Endpoint Protection Manager 資料庫不支援動態通訊埠。
遠端連線	必須啟用。此外必須指定 TCP/IP 通訊協定。

如果您的資料庫位於遠端伺服器上，則也必須在執行 Symantec Endpoint Protection Manager 的電腦上安裝 SQL Server 用戶端元件。SQL Server 用戶端元件包含 BCP.EXE。SQL Server 用戶端元件的版本號碼應與您使用的 SQL Server 的版本號碼相同。如需安裝指示，請參閱 SQL Server 說明文件。

在安裝的 Symantec Endpoint Protection Manager 資料庫組態階段，您需要選取和輸入各種資料庫值。請瞭解您必須做的決定，以便能正確架構資料庫。

下表顯示了您可能需要在開始安裝程序之前瞭解的設定。

Table 11: SQL Server 資料庫設定

設定	預設	說明
伺服器名稱	#####	執行 Symantec Endpoint Protection Manager 的電腦名稱。
伺服器儲存資料夾	SEPM_Install\data	Symantec Endpoint Protection Manager 用來存放資料檔的資料夾，其中包括備份檔案、複寫檔案及其他 Symantec Endpoint Protection Manager 檔案。如果此資料夾不存在，安裝程式會自行建立。 SEPM_Install 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。
加密密碼	無	加密 Symantec Endpoint Protection Manager 和用戶端之間通訊的密碼。密碼可為 8-32 (14.3 RU5 及更高版本) 或 6-32 (14.3 RU4 及更早版本) 個英數字元，且是必需的。 記下這個密碼並妥善保管。建立資料庫之後，您無法變更或還原密碼。如果您沒有可還原的備份資料庫，也必須輸入這個密碼，才能夠進行災難復原。請參閱： Endpoint Protection 的災難復原最佳實務
資料庫伺服器	#####	已安裝 SQL Server 之電腦的名稱以及選擇性實例的名稱。如果資料庫伺服器是與未命名的預設執行個體一同安裝，請輸入####或該主機的 IP ##。如果資料庫伺服器是與已命名的執行個體一同安裝，請輸入###\instance_name 或 IP ##\instance_name。 如果使用####，只對正確架構的 DNS 有效。 如果是安裝於遠端資料庫伺服器，必須先在執行 Symantec Endpoint Protection Manager 的電腦安裝 SQL Server 用戶端元件。
SQL Server 通訊埠	1433	用來與 SQL Server 傳送和接收流量的通訊埠。 不支援使用通訊埠 0。通訊埠 0 會指定隨機交涉的通訊埠。
資料庫名稱	sem5	已建立的資料庫名稱。
資料庫使用者名稱	sem5	已建立的資料庫使用者帳戶名稱。使用者帳戶是標準角色，有讀取及寫入存取權限。名稱可以是英數字元值和特殊字元 ~ # % _ + = : . 的組合。不允許使用特殊字元 ` ! @ ' \$ ^ & * () - { } [] " \ / < ; > , ?。 也不允許使用下列名稱： • sysadmin • server admin • setupadmin • securityadmin • processadmin • dbcreator • diskadmin • bulkadmin
資料庫密碼	無	與資料庫使用者帳戶相關聯的密碼。名稱可以是英數字元值和特殊字元 ~ # % _ + = : . / 的組合。不允許使用特殊字元 ! @ * () { } [] ; , ?。

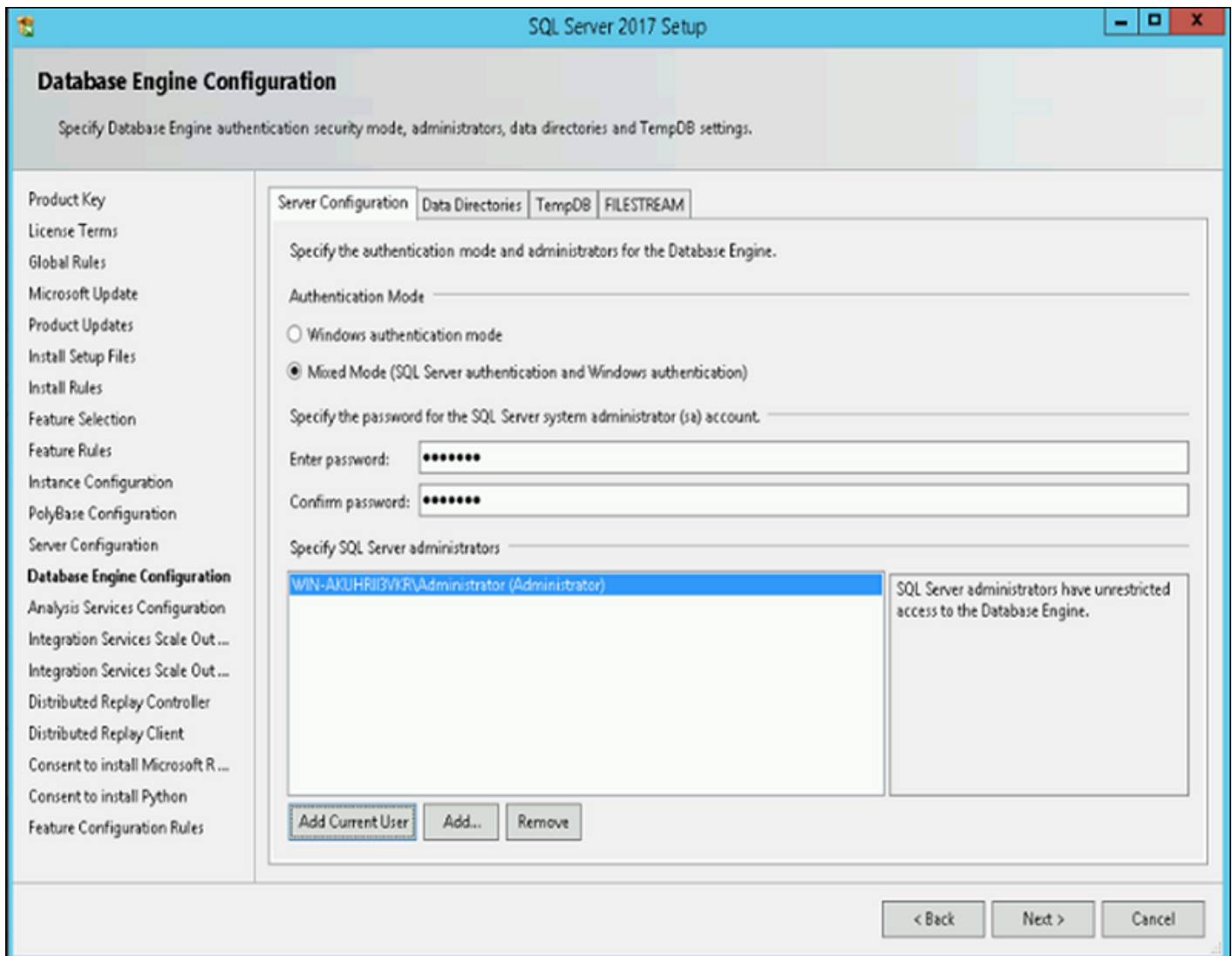
設定	預設	說明
SQL Server Native Client 資料夾	SQL Server 2008 : Install directory\100\Tools\Binn SQL Server 2012 : Install directory\110\Tools\Binn SQL Server 2014/2016/2017/2019 : Install directory\Client SDK\ODBC\110\Tools\Binn	包含 bcp.exe 的本機 SQL Native Client 目錄位置。所顯示的安裝路徑表示 Microsoft SQL Server 的預設路徑。Install directory Install directory 表示 Microsoft SQL Server 的安裝磁碟機和目錄。若要安裝 SQL Server Native Client，請參閱適用於 SQL Server 版本的 Microsoft TechNet 頁面： 安裝 SQL Server Native Client
伺服器使用者名稱	無	資料庫伺服器管理員帳戶的名稱，通常是 sa。
伺服器密碼	無	與資料庫伺服器管理員帳戶相關的密碼，通常是 sa。
資料庫儲存資料夾	SQL Server 2008 : Install directory\MSSQL10.MSSQLSERVER\MSSQL\Data SQL Server 2008 R2 : Install directory\MSSQL10_50.MSSQLSERVER\MSSQL\Data SQL Server 2012 : Install directory\MSSQL11.MSSQLSERVER\MSSQL\Data SQL Server 2014 : Install directory\MSSQL12.MSSQLSERVER\MSSQL\Data SQL Server 2016 : Install directory\MSSQL13.MSSQLSERVER\MSSQL\Data SQL Server 2017 : Install directory\MSSQL14.MSSQLSERVER\MSSQL\Data SQL Server 2019 : Install directory\MSSQL15.MSSQLSERVER\MSSQL\Data	SQL Server 資料資料夾的位置。如果您安裝至遠端伺服器，則磁碟區識別項必須符合遠端伺服器識別項。所顯示的安裝路徑表示 Microsoft SQL Server 的預設路徑。 - 如果是安裝至 SQL Server 2008 的具名實例，則會在 MSSQL10 後面附加實例名稱。例如 \MSSQL10.實例名稱\MSSQL\Data - 如果是安裝至 SQL Server 2008 R2 的具名實例，則會在 MSSQL10_50 後面附加實例名稱。例如 \MSSQL10_50.實例名稱\MSSQL\Data - 如果是安裝至 SQL Server 2012 的具名實例，則會在 MSSQL11 後面附加實例名稱。例如 \MSSQL11.實例名稱\MSSQL\Data - 如果是安裝至 SQL Server 2014 的具名實例，則會在 MSSQL12 後面附加實例名稱。例如 \MSSQL12.實例名稱\MSSQL\Data - 如果是安裝至 SQL Server 2016 的具名實例，則會在 MSSQL13 後面附加實例名稱。例如 \MSSQL13.實例名稱\MSSQL\Data - 如果是安裝至 SQL Server 2017 上的具名實例，則會在 MSSQL14 後面附加實例名稱。例如 \MSSQL14.實例名稱\MSSQL\Data - 如果是安裝至 SQL Server 2019 上的具名實例，則會在 MSSQL15 後面附加實例名稱。例如 \MSSQL15.實例名稱\MSSQL\Data 如需詳細資訊，請參閱： 預設和具名 SQL Server 實例的檔案位置 Note: 如果輸入的是正確的資料庫伺服器實例名稱，按下「預設值」就會顯示正確的安裝資料夾。如果按下「預設值」後未出現正確的安裝資料夾，則表示資料庫建立失敗。

更多資訊

[安裝 Symantec Endpoint Protection Manager](#)

關於 SQL Server 資料庫驗證模式

根據您的 SQL Server 資料庫安裝方式，Symantec Endpoint Protection Manager 支援兩種驗證模式：



- 混合模式
混合模式驗證會同時啟用 Windows 驗證和 SQL Server 驗證。您一律可以使用 Windows 驗證，無法停用。架構 SQL Server 使用混合模式時，就可設定 Symantec Endpoint Protection Manager 使用 Windows 驗證或 SQL Server 驗證。
- **Windows 驗證模式**
Windows 驗證模式會啟用 Windows 驗證並停用 SQL Server 驗證。您必須使用 Windows 驗證模式來設定 Symantec Endpoint Protection Manager。
使用「Windows 驗證」模式的遠端資料庫連線需注意下列需求：
 - 若是 Active Directory 環境中的部署，Symantec Endpoint Protection Manager 及 SQL Server 必須位於相同的 Windows 網域。
 - 若是「工作群組」環境中的部署，本機電腦及遠端電腦的 Windows 帳戶認證必須相同。
 - Windows 密碼必須滿足以下 Symantec Endpoint Protection Manager 要求。
 - Windows 密碼不得超過 79 個字元，且支援以下字元：`\_+`-=[] { } | ; ' : " , . / < > ~ ! @ # \$ % ^ & * () \ ? 。如果設定 Symantec Endpoint Protection Manager，則不可使用以下字元：/ " < > 。
 - 較舊版本不支援以下字元：% 和 + (14.3 RU1 和更舊版本)、& (14.3 RU1 和更舊版本)。
 - SEPM 會阻擋您貼上含不受支援字元的 Windows 密碼。

請參閱：[關於 SQL Server 組態設定](#)

國際化需求

在非英文或混合語言環境中安裝 Symantec Endpoint Protection Manager 時，有某些特定限制。

Table 12: 國際化需求

元件	需求
電腦名稱、伺服器名稱及工作群組名稱	支援非英文字元時的限制如下： - 若主機或使用者使用雙位元字元集或高 ASCII 字元集，可能無法進行網路稽核。 - 在 Symantec Endpoint Protection Manager 主控台或用戶端使用者介面上，可能無法正常顯示雙位元字元集名稱或高 ASCII 字元集名稱。 - 較長的雙位元字元集或高 ASCII 字元集主機名稱長度不能超過 NetBIOS 的限制。如果主機名稱長度超過 NetBIOS 的限制，則 Symantec Endpoint Protection Manager 主控台不會出現「首頁」、「監視器」和「報告」頁面。
英文字元	下列情形必須使用英文字元： - 將用戶端套件部署至遠端電腦。 - 在「管理伺服器組態精靈」中定義伺服器儲存資料夾。 - 定義 Symantec Endpoint Protection Manager 的安裝路徑。 - 定義部署用戶端至遠端電腦時的憑證。 - 定義群組名稱。 您可以為包含非英文字元的群組名稱建立用戶端套件。但是，若群組名稱包含非英文字元，您可能無法使用「推動部署精靈」部署用戶端套件。 - 將非英文字元推送至用戶端電腦。 用戶端使用者介面可能無法正常顯示伺服器端產生的某些非英文字元。例如，以非雙位元組字元集命名的用戶端電腦，無法正常顯示雙位元組字元集位置的名稱。
「使用者資訊」用戶端電腦對話方塊	安裝匯出的套件後，在「使用者資訊」用戶端電腦對話方塊中提供回應時，請勿使用雙位元字元或高 ASCII 字元。請參閱： 收集使用者資訊
授權啟用精靈	請勿在下列欄位中使用雙位元組字元： - 名 - 姓 - 公司名稱 - 城市 - 州/省
翻譯的語言	在 14.3 RU1 MP1 和更舊版本中，Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection Windows 用戶端已從英文翻譯成下列語言：中文、捷克文、法文、德文、義大利文、日文、韓文、波蘭文、巴西葡萄牙文、俄文和西班牙文。 - 在 14.3 RU2 中，Symantec Endpoint Protection 只翻譯成 4 種語言：法文、日文、巴西葡萄牙文和西班牙文。 - 在 14.3 RU4 中，Symantec Endpoint Protection 已新增簡體中文和繁體中文支援。 - 在 14.3 RU5 中，Symantec Endpoint Protection 已新增捷克文、波蘭文和俄文支援。 將 Symantec Endpoint Protection Manager 14.3 RU2+ 升級為支援的語言

將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2

設定您的網路來部署 Symantec Endpoint Protection 以遵從 FIPS 140-2。

聯邦資訊處理標準 (FIPS) 是由美國聯邦政府開發的公告標準，用於確保非軍事政府機構和承包商使用的電腦遵從安全標準。FIPS 140-2 標準涉及安全需求，因為它們與加密模組相關。

詳細瞭解 [fips 140-2 遵從性](#) 以及 [fips 140-2 遵從性不支援的功能](#)。

開始之前

在您第一次安裝 Symantec Endpoint Protection 之前，請確保您的 Symantec Endpoint Protection 版本 [支援 FIPS 遵從](#)。

重要附註

- 如果您將已在 FIPS 模式下的管理伺服器升級到支援的 Symantec Endpoint Protection 版本，則該管理伺服器仍處於 FIPS 模式下。
 - 如果先前版本未遵從 FIPS，請啟用 FIPS 模式。
 - 如果先前版本使用的是 HTTP 而不是 HTTPS 通訊，請參閱：[啟用 HTTPS 用戶端伺服器通訊](#)
- 如果您有一個站台具有多部管理伺服器，或有多個彼此複寫的站台，請在每部管理伺服器上啟用 FIPS 模式。
- 如果您的站台處於 FIPS 模式，並且您必須從災難中復原，請首先[停用 FIPS 模式](#)。在執行還原指令之後，請重新啟用 FIPS 模式。
- 在修復 Symantec Endpoint Protection Manager 安裝之後，必須重新啟用 FIPS 模式。
- 在執行管理伺服器組態精靈之前，必須停用 FIPS 模式。在執行精靈之後，請重新啟用 FIPS 模式。
- 如果您匯入新的伺服器憑證，則必須使用至少 2048 位元金鑰組。否則，您將看到##### 訊息，且無法匯入憑證。
- 對於 SQL Server 資料庫連線，RU7 具有更嚴格的需求。如果升級視窗顯示啟用 FIPS 模式失敗的訊息，請檢查 `FIPSMODE.log` 以修正問題。否則，Symantec Endpoint Protection Manager 主控台可能不會啟動。
請參閱：[在 Symantec Endpoint Protection 上針對 FIPS 140-2 遵從問題進行疑難排解](#)

步驟 1：安裝 Symantec Endpoint Protection Manager (SEPM)

第一次安裝 Symantec Endpoint Protection Manager 時，預設它不會遵從 FIPS。在啟用 FIPS 模式之前安裝 SEPM 以避免發生憑證問題。FIPS 程式庫部署指令碼會檢查 Symantec Endpoint Protection Manager 服務是否已安裝，然後再部署 FIPS 程式庫以防止此問題。

NOTE

FIPS 模式只能與 Microsoft SQL Server 資料庫一起運作，而不能與預設 Microsoft SQL Server Express 資料庫一起運作。

使用管理伺服器組態精靈架構 Microsoft SQL Server 資料庫時，您可能會在資料庫驗證和建立畫面上看到下列訊息。選取選項 1 以執行憑證驗證。

The image shows two overlapping windows from the Symantec Endpoint Protection Manager (SEPM) configuration interface.

The top window is titled "Step Two: Existing Database Parameters" and contains the following fields:

- Authentication type: SQL Server Authentication
- Database server: XX.XX.XXX.XX
- SQL server port: 1433
- SQL Server client folder: C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn (with a "Browse" button)

The bottom window is a "Warning" dialog box with a yellow shield icon. It contains the following text:

Symantec Endpoint Protection Manager (SEPM) uses TLS to connect to the SQL Server database. However, SQL Server may use a temporary self-signed certificate which the SEPM Windows server does not trust; therefore, the SEPM relies on SQL Server IP address or hostname to trust its source other than the certificate. This may expose you to potential SQL Server spoofing.

You can make one of the following choices:

1. You must ensure that Windows trusts this certificate. Therefore, you must provide the certificate on the server computer by importing it into Windows. See [Ensuring that Windows trusts the SQL Server's certificate](#). Then, click **Yes** to continue the management server configuration.
2. Click **No** to let the Symantec Endpoint Protection Manager use the server IP address or hostname to trust its source rather than the certificate. Only choose this option if both the Symantec Endpoint Protection Manager and SQL Server database are on a secured network.

At the bottom of the dialog are "Yes" and "No" buttons.

步驟2：在 **Symantec Endpoint Protection Manager** 上啟用 **FIPS** 遵從

在您第一次安裝 SEPM 之後，請執行 FIPSMODE-Enable.bat [啟用 FIPS 模式](#)。Symantec 提供此指令碼檔案來安裝啟用 FIPS 模式的程式庫和可執行檔。

如需詳細瞭解指令碼的功能，請參閱：[關於 FIPS 遵從程式庫](#)

步驟3：在 **Symantec Endpoint Protection** 用戶端上啟用 **FIPS** 模式

在 Windows 或 Windows Server 作業系統中啟用 FIPS 模式時，應用程式只會使用遵從 FIPS 140-2 等級 1 的加密演算法。您可以啟用 FIPS 模式，方法為在本機安全政策中或作為群組政策的一部分啟用特定安全設定，或編輯 Windows 登錄機碼。

1. 執行下列其中一個步驟：

- 若要使用群組政策設定，請開啟群組政策編輯器、瀏覽到 Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options，然後啟用「系統加密：使用 **FIPS** 遵從演算法進行加密、雜湊和簽署」設定。
- 若要使用 Windows 登錄，請前往 HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled，並將 **Enabled** 設為 1。

2. 如果 Symantec Endpoint Protection 用戶端已在執行，請重新啟動用戶端電腦，讓此設定生效。

如需在 Windows 上啟用 FIPS 模式的詳細資訊，請參閱「啟用 FIPS 安全政策」，位於：[FIPS 140-2 驗證](#)

步驟4：在 **Microsoft SQL Server** 上啟用 **FIPS** 遵從

使用下列步驟，針對所有用戶端強制執行加密通訊。

- 在 SQL Server 電腦上**啟用 FIPS 模式**。在啟動 SQL Server 之前，請先啟用 FIPS 模式，因為 SQL Server 會在啟動時讀取 FIPS 設定。
- 在 SQL Server 組態管理員中架構加密通訊：
 - a. 在 SQL Server 組態管理員中，展開「**SQL Server 網路組態**」、在「<MSSQLSERVER> 的通訊協定」上按一下滑鼠右鍵，然後選取「內容」。
 - b. 在「旗標」標籤的「強制加密」方塊中，選取「是」，然後選取「確定」。
 - c. 重新啟動 SQL Server 服務。
- 安裝 SQL Server 憑證。
請參閱：[安裝 SQL Server 資料庫憑證](#)

了解 **Symantec Endpoint Protection** 和 **FIPS 140-2 等級 1** 遵從

您在 FIPS 140-2 等級 1 遵從架構中部署 Symantec Endpoint Protection，以保護用戶端至管理伺服器、管理伺服器至管理伺服器，以及遠端系統管理通訊。

Symantec Endpoint Protection Manager 透過 Apache Web 服務器託管用戶端至管理伺服器通訊。對於 Symantec Endpoint Protection 14.3 或更新版本安裝，Apache 伺服器預設會在通訊埠 443 上接聽加密的 HTTPS 連線。HTTPS 連接可確保通訊經過加密並透過安全通道傳送。

根據預設，TLS 會保護用戶端至伺服器通訊和用戶端至主控台通訊。若要保護 SQL Server 資料庫通訊，請使用加密。

IMPORTANT

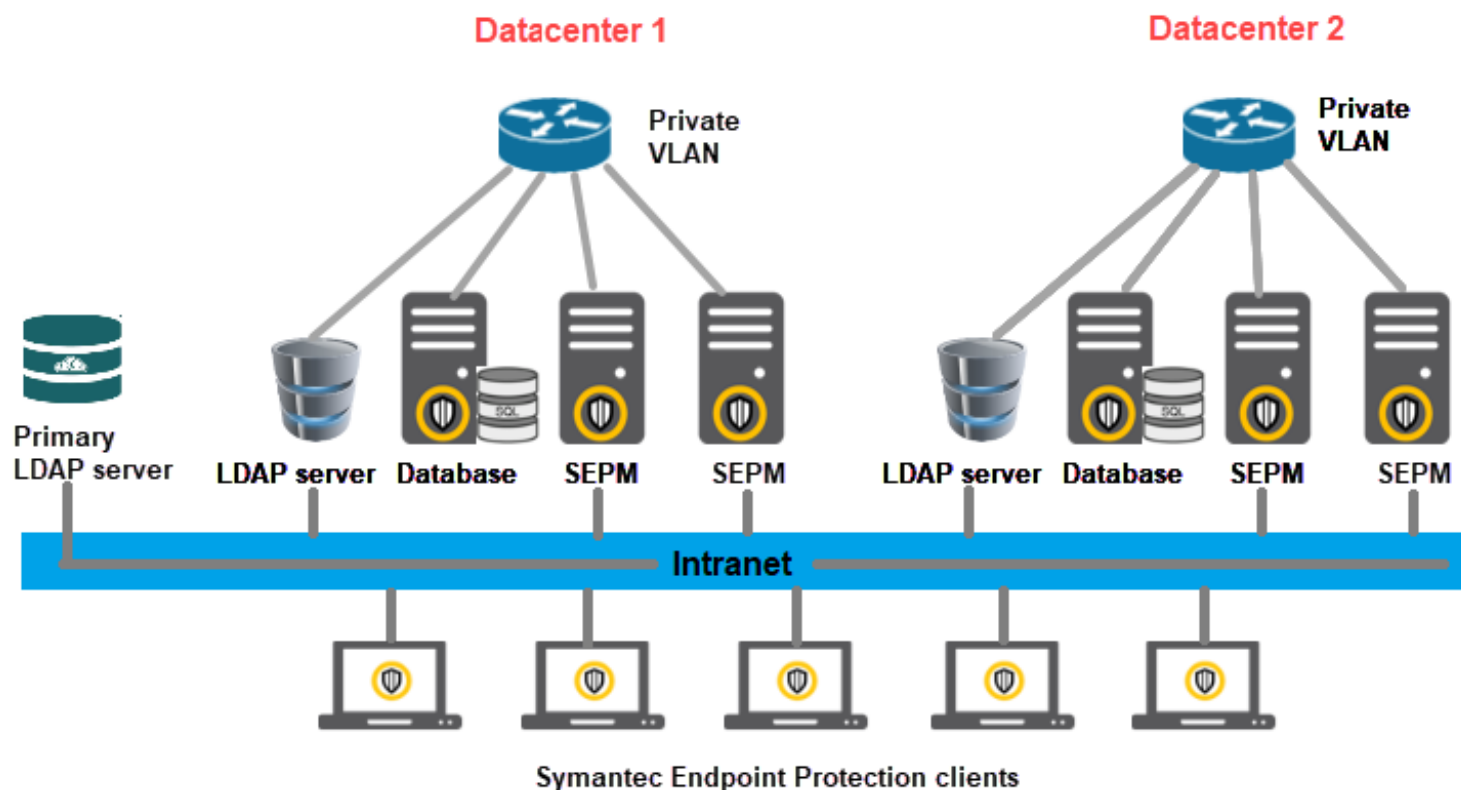
本文件中提供的資訊適用於 Symantec Endpoint Protection 14.3 RU7 和更新版本的 Windows 用戶端，這些用戶端會使用內部部署。雖然您可以將 Symantec Endpoint Protection Mac 用戶端和 Linux 用戶端連線至您的 FIPS 模式伺服器網路，但是這些用戶端目前不支援 FIPS 驗證的用戶端 TLS 加密模組。

請參閱：[FIPS 140-2 等級 1 遵從模式中不支援的功能和限制](#)

Symantec 會對您的網路環境做出下列假設：

- 您使用 Microsoft 網域控制器提供來自網域控制器憑證授權中心的憑證。
- 您已將憑證授權中心架構為企業憑證授權中心，此授權中心可在線上滿足網域中伺服器的憑證要求。

下圖說明搭配多個資料中心和 Symantec Endpoint Protection Manager 站台的大規模部署。私有 VLAN 網路可保護資料中心內的資料庫通訊。FIPS 驗證的模組可保護 Symantec Endpoint Protection 用戶端的通訊，以及內部網路上站台之間的通訊。



更多資訊

如需如何將 Symantec Endpoint Protection 部署為遵從 FIPS 140-2 的相關資訊	將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2
如需支援 FIPS 模式的 Symantec Endpoint Protection 版本的相關資訊	支援 FIPS 140-2 等級 1 遵從的版本
如需 FIPS 遵從的說明，以及在哪個 Windows 作業系統中使用哪些加密模組的清單	FIPS 140 驗證

支援 FIPS 140-2 等級 1 遵從的版本

了解 Symantec Endpoint Protection 14.x 的哪些版本支援 FIPS 140-2 等級 1 遵從

Table 13: Symantec Endpoint Protection 14.x 和 FIPS 140-2 等級 1 遵從

支援 FIPS 模式的 14.x 版本	未針對 FIPS 模式驗證的 14. x 版本
14.2 和更舊版本 14.3 RU7 和更新版本	14.3 到 14.3 RU6

下列資訊適用於安裝或升級到任何支援的 Symantec Endpoint Protection 版本：

- 您可以從任何不支援的 Symantec Endpoint Protection 版本升級到支援的 Symantec Endpoint Protection 版本，以取得 FIPS 140-2 等級 1 合規性。
- Symantec Endpoint Protection 14.3 會使用部署指令碼搭配支援 FIPS 140-2 等級 1 遵從的程式庫。Apache 提供有關通訊埠 8445 的 Symantec Endpoint Protection 報告。如果通訊埠 8445 使用中，則您應該變更報告網站，以在移轉過程中使用不同的通訊埠。

更多資訊

[針對 Symantec Endpoint Protection Manager 啟用或停用 FIPS 模式](#)

FIPS 140-2 等級 1 遵從模式中不支援的功能和限制

找出 140-2 等級 1 遵從模式中不支援的 Symantec Endpoint Protection (SEP) 功能。

從 14.3 RU7 起，下列功能不適用於處於 FIPS 模式的 Symantec Endpoint Protection 部署：

- Mac 和 Linux 用戶端。雖然您可以將 Mac 用戶端和 Linux 用戶端連線至您的 FIPS 遵從伺服器網路，但是這些用戶端目前不支援 FIPS 驗證的用戶端 TLS 加密模組。
- 智慧卡驗證。
- 未加密且不安全的 Syslog 通訊。
- 任意版本的內部部署 Symantec EDR 硬體裝置。Symantec 計畫從 Symantec Endpoint Protection 14.3 RU8 和 EDR 4.8 開始支援 FIPS 模式。

尚未分析或測試某些 Symantec Endpoint Protection 功能是否可在 Symantec Endpoint Protection FIPS 相容的部署中使用。作為最佳實務，請不要在 FIPS 保護的環境中使用下列 Symantec Endpoint Protection 功能：

- 群組更新提供者
- 隔離伺服器
- 使用 Symantec VIP 進行雙因素驗證

FIPS 部署具有下列限制：

- 對於遠端管理，Symantec 建議您使用 Web 主控台或一個使用 RDP 的連線，在伺服器上本機存取主控台。
- 由於 TLS 加諸在效能的負載增加，因此 Symantec 建議您使 Symantec Endpoint Protection Manager 管理有限數目的用戶端。

更多資訊

[將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2](#)

針對 Symantec Endpoint Protection Manager 啟用或停用 FIPS 模式

了解如何使用 Symantec 提供的指令碼，為 Symantec Endpoint Protection Manager 部署、啟用、停用和重新套用 FIPS 遵從模式。

您可以連按兩下指令碼以檢查目前 FIPS 狀態 (開啟或關閉)。您還可以使用 `FIPSMode.vbs` 指令碼的 `-reapply` 旗標，在升級或進行其他變更之後修復 FIPS 模式。

在使用啟用或停用 `FIPSMode` 指令之前，請登出並關閉本機 Symantec Endpoint Protection Manager 主控台，這是 Java 型主控台。如果您未登出，則在啟用或停用過程中必須取代的某些檔案將遭鎖定，因而無法取代。指令碼會提示您關閉任何剩餘的主控台程序，然後才能繼續。

NOTE

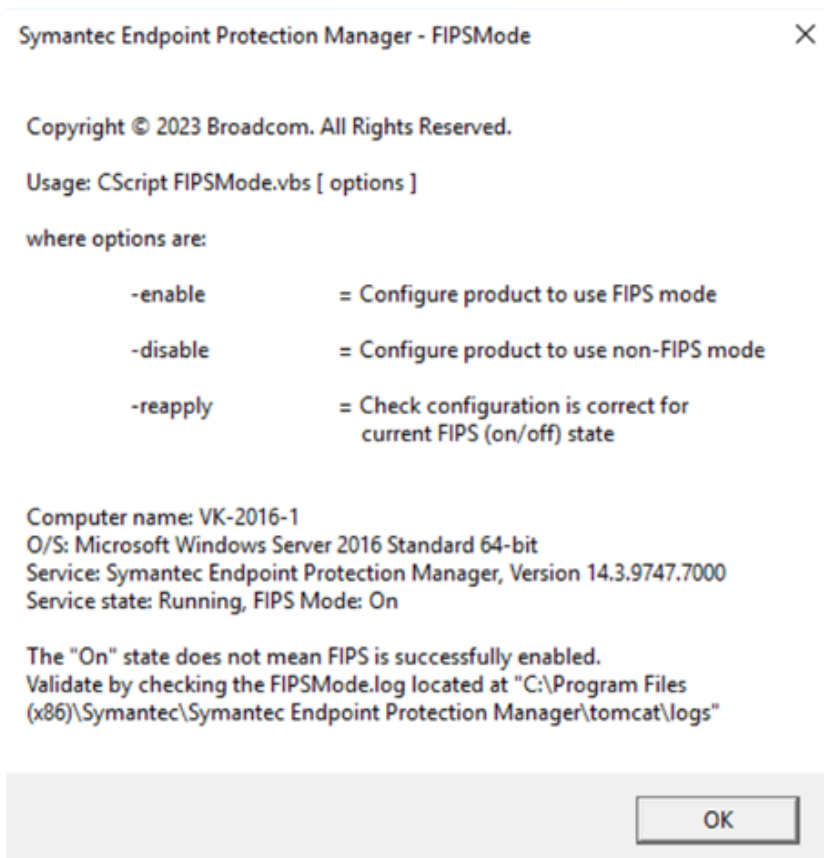
在執行管理伺服器組態精靈之前，必須停用 FIPS 模式，然後在完成時重新啟用 FIPS 模式。

NOTE

您可以不限次數地重複這些操作，這不會造成不良後果。

啟用 FIPS 遵從程式庫

1. 將資料夾變更為 `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin` 資料夾。
2. 連按兩下 `FIPSMode-Enable.bat` 檔案。



停用 FIPS 遵從程式庫

1. 將資料夾變更為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin 資料夾。
2. 連按兩下 FIPSMODE-Disable.bat 檔案。

檢查 FIPS 模式是否已啟用

若要驗證 FIPSMODE-Enable.bat 檔案是否已成功啟用 FIPS 模式，請檢查日誌。

1. 前往 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\logs 資料夾。
2. 開啟 FIPSMODE.log。
3. 尋找項目：FIPSMODE.vbs #####。

更多資訊

- [關於 FIPS 遵從程式庫](#)
- [將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2](#)

安裝 SQL Server 資料庫憑證

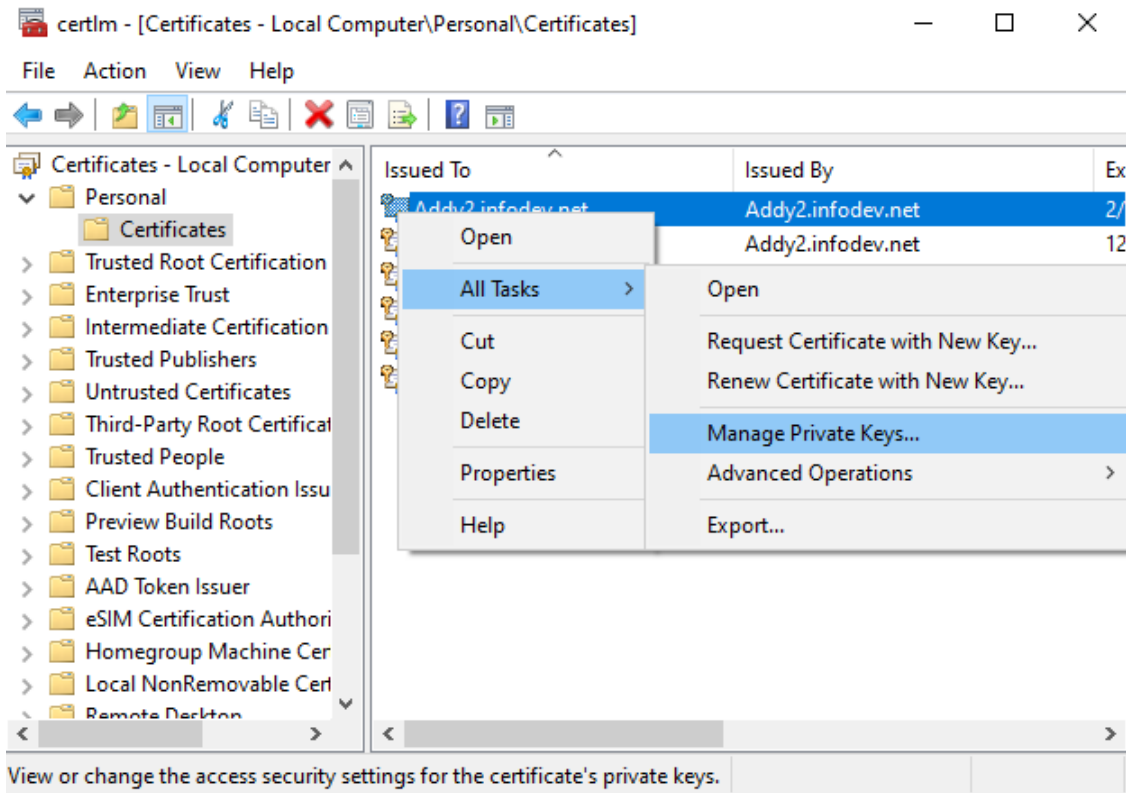
若要強制 Symantec Endpoint Protection 用戶端遵從 FIPS 140-2，您必須在 SQL Server 資料庫與用戶端之間架構加密通訊。遵循步驟來安裝 SQL Server 資料庫憑證。

在安裝 SQL Server 憑證之前，請確保可在安裝 SQL Server 的電腦上使用 .pfx 或 .pem 憑證。

步驟 1：檢查這些憑證是否可用

使用 Microsoft Management Console (MMC) 將 Microsoft SQL Server 登入使用者新增到私密金鑰權限清單。

1. 使用「執行」> `certlm.msc` 指令開啟憑證管理員。
2. 在「憑證 - 本機電腦」下，選取「個人」>「憑證」。
3. 在「核發對象」清單中，於憑證上按一下滑鼠右鍵，然後按一下「所有工作」>「管理私密金鑰」。



4. 在「私密金鑰的權限」對話方塊中，按一下「新增」，將 SQL Server 登入使用者新增至權限清單。
5. 在「輸入要選取的物件名稱」清單中，貼上 SQL Server 登入使用者名稱。
若要取得登入使用者名稱，請執行下列動作：
 - a. 前往 Windows「控制台」>「系統管理工具」>「服務」應用程式。
 - b. 按兩下 SQL Server 服務。
 - c. 在「內容」對話方塊中，按一下「登入」標籤，然後在「此帳戶」文字欄位中，複製服務名稱 (例如 NT Service\MSSQL\$SEM5)。
6. 在「選取使用者或群組」對話方塊中，於「輸入要選取的物件名稱」欄位中貼上服務名稱。

Select Users or Groups

Select this object type:
Users, Groups, or Built-in security principals

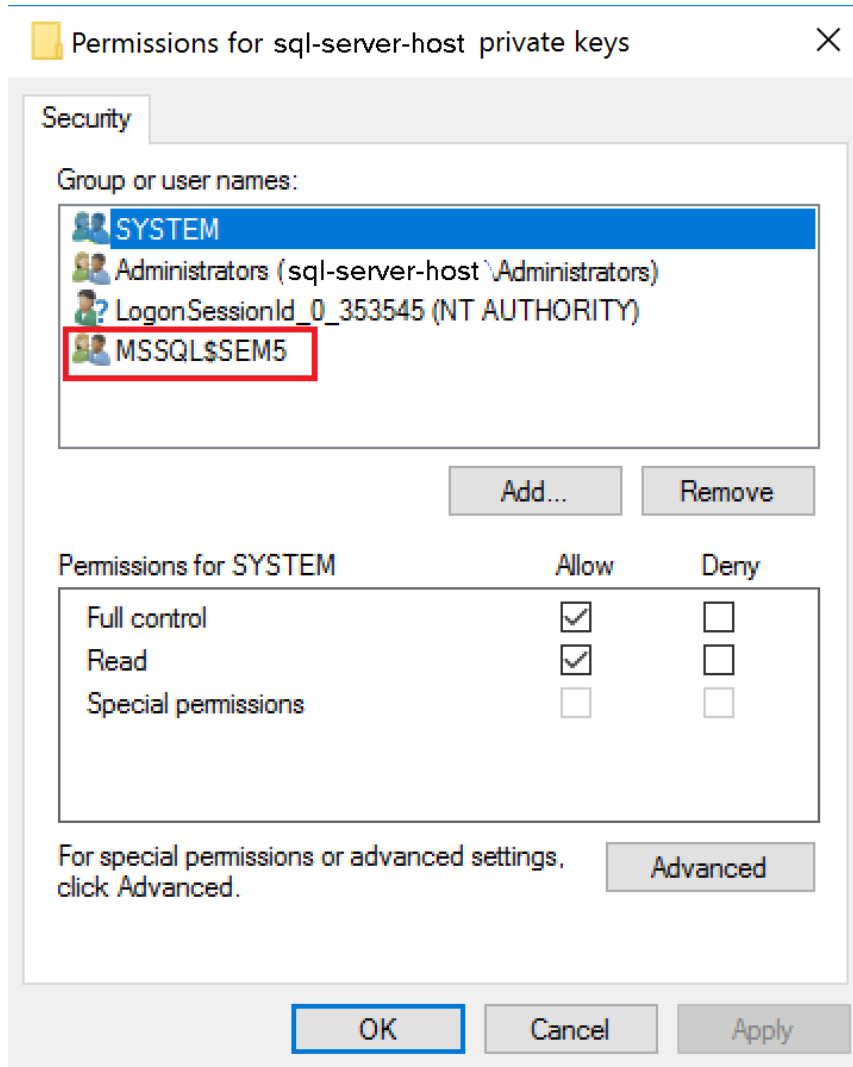
From this location:
Infodev.net

Enter the object names to select (examples):
NT Service\MSSQL\$SEM5

Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

您可以按一下「檢查名稱」，將使用者名解析為完整存在名稱；但這會自動發生。

7. 按下「確定」。



8. 按一下「確定」>「確定」。

步驟 2：使用 **SQL Server** 組態管理員匯入和安裝 **SSL/TLS** 憑證 (.pfx 或 .pem)

使用「主旨備用名稱」欄位，以便符合下列任一欄位：主機名稱、DNS 名稱和 IP 位址。

1. 在 SQL Server 組態管理員的主控台窗格中，展開「**SQL Server 網路組態**」。
2. 在「<實例名稱> 的通訊協定」上按一下滑鼠右鍵，然後選取「內容」。
3. 在「憑證」標籤上，從「憑證」下拉式功能表中選取憑證，然後按一下「確定」。

重新啟動 SQL Server 服務。

更多資訊

[將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2](#)

關於 **FIPS** 遵從程式庫

了解 Symantec 提供用於安裝 FIPS 遵從程式庫的指令碼。

此指令碼會採取下列動作：

- 停止 Symantec Endpoint Protection Manager 服務和 Symantec Endpoint Protection Manager Webserver 服務。
- 安裝 FIPS 遵從 Java 和 Apache 程式庫和可執行檔。
- 更新 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\jre\lib\security 資料夾中的 java.security 檔案，以安裝 JCE 提供者程式庫。
- 在 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf\ssl\ssl.conf 檔案中啟用 FIPSMODE 選項。
- 指定在 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tomcat\etc\conf.properties 檔案中使用 FIPS 模式。
- 新增下列一行，將偽亂數產生器演算法架構為 java.security 檔案的安全版本：
com.rsa.crypto.default.random=HMACDRBG256
- 安裝 OpenSSL FIPS 提供者 (fips.dll) 並呼叫 openssl fipsinstall 指令。此指令會呼叫必要的 FIPS 自我測試程序，並依照 OpenSSL FIPS 提供者安全政策文件的要求建立 fipsmodule.my.cnf 組態檔。
- 重新啟動 Symantec Endpoint Protection Manager 服務和 Symantec Endpoint Protection Manager Webserver 服務。

從版本 14.3 RU7 起，SEP 將 Bouncy Castle 用於 JAVA 安全通訊端擴展 (JSSE) 和加密提供程式。

更多資訊

- [針對 Symantec Endpoint Protection Manager 啟用或停用 FIPS 模式](#)
- 如需 FIPS 憑證和安全政策資訊，請參閱：[加密模組驗證程式](#)

關於已驗證模組

了解 Symantec Endpoint Protection 使用哪些已驗證模組來保護通訊。

Table 14: Symantec Endpoint Protection 如何保護通訊：模組和受保護元件

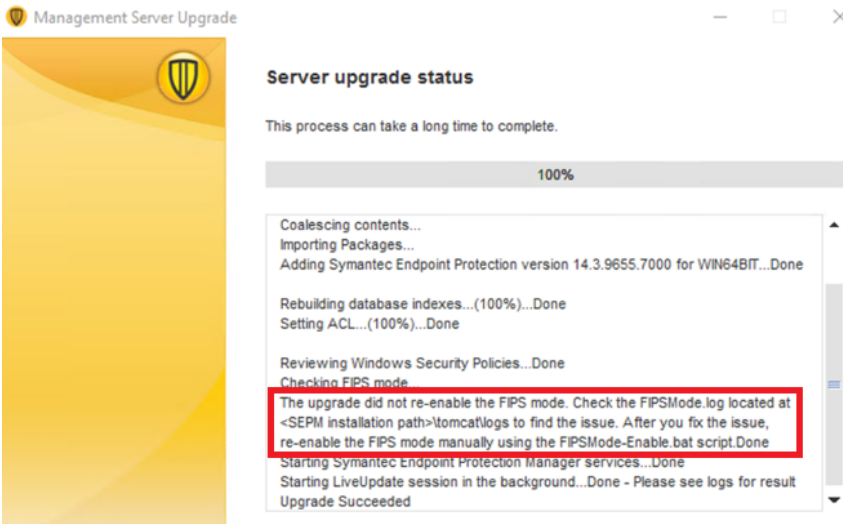
NIST CMVP 模組憑證編號和說明	受保護元件
Microsoft Windows FIPS 驗證的加密模組： • 加密基本程式庫 (bcryptprimitives.dll、ncryptsslp.dll) • 增強式 DSS 和 Diffie-Hellman 加密提供者 (dssenh.dll) (僅限 Windows 8 & Server 2012) • 增強式加密提供者 (rsaenh.dll) (僅限 Windows 8/Server 2012) 如需 Microsoft Windows 模組的最新 FIPS 驗證和憑證的相關資訊，請參閱： FIPS 140-2 驗證 。	• Symantec Endpoint Protection 用戶端與 Symantec Endpoint Protection Manager 的 TLS 連線 (透過 Windows Schannel) • Windows 遠端桌面連線 • 與 Microsoft SQL Server 的通訊
OpenSSL FIPS Provider (OpenSSL 3) 請參閱： 憑證編號 4282	Symantec Endpoint Protection Manager Apache 伺服器 TLS 連線
Bouncy Castle FIPS Java API 請參閱： 憑證編號 3514	• Symantec Endpoint Protection Manager Tomcat 伺服器 TLS 連線 (透過 Java JCE) • Symantec Endpoint Protection Manager Java 主控台 TLS 連線 (透過 Java JCE)

更多資訊

[關於 FIPS 遵從程式庫](#)

在 Symantec Endpoint Protection 上針對 FIPS 140-2 遵從問題進行疑難排解

Table 15: 針對 FIPS 140-2 遵從問題進行疑難排解

問題	解決方案
如果從 Windows Server 2019 升級到 Windows Server 2022，並嘗試在啟用 FIPS 的情況下登入 14.3 RU8 或更新版本的 SEPM，則可能會看到以下錯誤：#####0x10010000	找到託管 SEPM 資料庫的 SQL Server 使用的憑證。將此憑證匯入 Windows 受信任的根憑證授權單位。 升級作業系統之後無法登入已啟用 FIPS 的 14.3 RU8 SEPM
14.3 RU7 具有較早 SEPM 版本所沒有的限制。因此，在升級時您可能會遇到問題。 如果看到下列訊息，則未成功啟用 FIPS 模式。管理主控台可能無法啟動。 	1. 檢查 FIPSMODE.log 以查看問題的原因。修正問題。 如需詳細資訊，請在下列位置參閱「檢查 FIPS 模式是否已啟用」： 針對 Symantec Endpoint Protection Manager 啟用或停用 FIPS 模式 2. 重新執行 FIPSMODE-Enable.bat 以重新啟用 FIPS 模式。 如果您未修正此問題，請執行 FIPSMODE-Disable.bat 以確保 FIPS 模式已停用。SEPM 正常運作，但不能處於 FIPS 模式下。
在升級 Symantec Endpoint Protection Manager 之後，您可能不確定 FIPS 模式是否仍已啟用。	檢查 FIPSMODE.log 檔案。

將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2

管理 Symantec Endpoint Protection 用戶端安裝

您必須在每個想要保護的電腦上安裝 Symantec Endpoint Protection 用戶端，無論該電腦為實體電腦還是虛擬電腦。

Table 16: 用戶端電腦安裝工作

動作	說明
步驟 1：識別用戶端電腦	確認您要安裝用戶端軟體的電腦。檢查所有電腦是否執行支援的作業系統。 Note: 賽門鐵克建議您也在裝載 Symantec Endpoint Protection Manager 的電腦上安裝用戶端。 如需最新系統需求，請參閱： 所有 Endpoint Protection 版本的版本說明、新修正和系統需求
步驟 2：識別電腦群組 (選擇性)	確認要用戶端歸屬的電腦群組。例如，您可以根據電腦類型來將用戶端分組，以遵從公司組織或所需的安全層級。您可以在安裝用戶端軟體之前或之後建立這些群組。 您也可以匯入現有群組結構，如 Active Directory 結構。請參閱： • 管理用戶端群組 • 從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦
步驟 3：準備用戶端電腦進行部署和安裝	如果使用者沒有其電腦的管理權限，則您應該使用「遠端推送」遠端安裝用戶端軟體。「遠端推送」安裝會要求您輸入具有電腦本機管理權限的憑證。請參閱： 使用遠端推送安裝 Symantec Endpoint Protection 用戶端 準備電腦進行遠端用戶端部署以及在安裝之後成功與 Symantec Endpoint Protection Manager 進行通訊。請參閱： 準備 Windows 和 Mac 電腦進行遠端部署
步驟 4：確定功能並部署用戶端軟體	您可以使用其中一種可用方式來部署用戶端軟體。您也可以匯出自訂用戶端套件以便稍後部署，或者使用第三方工具進行部署。 Note: 賽門鐵克建議您不要在安裝 Symantec Endpoint Protection 的同時執行第三方安裝。任何進行網路層級或系統層級變更的第三方程式安裝都可能會在安裝 Symantec Endpoint Protection 時導致不理想的結果。如可能，請在安裝 Symantec Endpoint Protection 之前重新啟動用戶端電腦。 如需詳細資訊，請參閱： • 選擇使用用戶端部署精靈安裝用戶端的方法 • 匯出用戶端安裝套件 • 使用第三方工具安裝 Windows 用戶端軟體 • 您可以決定要在用戶端電腦上安裝哪些功能。匯出或部署安裝套件之前，請先架構自訂用戶端功能集與安裝設定。安裝設定包含安裝資料夾以及重新啟動設定。您也可以使用預設的用戶端功能集與安裝設定。請參閱： — 選擇要在用戶端上安裝哪些安全性功能 — 關於 Windows 用戶端安裝設定 • 針對 Windows 用戶端，當您架構用戶端安裝設定時，可以選擇自動解除安裝現有的第三方安全軟體。請參閱： 架構用戶端套件來解除安裝現有安全軟體
步驟 5：驗證安裝狀態	確認成功安裝用戶端，且用戶端可與 Symantec Endpoint Protection Manager 進行通訊。請參閱： • Symantec Endpoint Protection 用戶端狀態圖示

安裝完成後，您可以採取其他步驟來保護非受管電腦的安全，以及最佳化 Symantec Endpoint Protection 安裝的效能。

- [從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)

準備 Windows 和 Mac 電腦進行遠端部署

在從 Symantec Endpoint Protection 部署 Symantec Endpoint Protection Manager 之前，您必須採取一些步驟來準備電腦，才能確保遠端安裝成功。這些步驟僅與遠端安裝有關。您之後可以回復這些變更，但您必須再次套用它們，才能執行其他遠端安裝。

NOTE

您無法從 Symantec Endpoint Protection 將 Symantec Endpoint Protection Manager 用戶端遠端部署至 Linux 電腦。

Table 17: 準備所有電腦進行遠端部署的工作

工作	詳細資訊
具有用戶端電腦的管理員權限	如果用戶端電腦是 Active Directory 網域的一部分，則您應該使用網域管理員帳戶憑證進行遠端推送安裝。否則，請為要在其中部署的每個電腦提供管理員憑證。
修改防火牆設定	修改防火牆設定以允許 Symantec Endpoint Protection 元件之間進行通訊。請參閱： Symantec Endpoint Protection 的通訊埠
移除現有第三方安全軟體	解除安裝目前正在使用的所有第三方安全軟體。對於 Windows 電腦，Symantec Endpoint Protection 包括一種工具，可協助自動解除安裝選取的第三方安全軟體。您必須分別移除此工具無法移除的任何安全軟體。 Note: 某些程式可能具有特殊的解除安裝常式，或者可能需要停用自我防護元件。請參閱第三方軟體的說明文件。 您可以在部署之前架構此工具，解除安裝程序在 Symantec Endpoint Protection 安裝之前進行。請參閱： 架構用戶端套件來解除安裝現有安全軟體
解除安裝無法正常解除安裝的 Symantec Endpoint Protection 用戶端	您可以解除安裝適用於 Windows 的現有 Symantec Endpoint Protection 用戶端安裝。只有在現有 Symantec Endpoint Protection 安裝無法正常解除安裝時，才應使用此選項。請勿將此選項作為標準部署的一部分使用。 您可以在部署之前架構此工具，解除安裝程序在 Symantec Endpoint Protection 安裝之前進行。請參閱： 架構用戶端套件來解除安裝現有安全軟體
解除安裝不支援的或消費性賽門鐵克安全軟體	解除安裝所有不支援的賽門鐵克安全軟體，如 Symantec AntiVirus 或 Symantec Client Security。不支援直接從這些產品進行移轉。 您也必須移除所有消費者品牌的賽門鐵克安全產品，如 Norton Internet Security。 如需移除的相關資訊，請參閱賽門鐵克軟體的說明文件。 如需詳細資訊，請參閱： 支援升級到最新版本的 Symantec Endpoint Protection 14.x 的路徑

Table 18: 準備 Windows 用戶端進行遠端部署的工作

作業系統	工作
準備 Windows Vista、Windows 7 或 Windows Server 2008/2008 R2 電腦	Windows 的「使用者帳戶控制」會攔截本機管理員帳戶遠端存取遠端管理共用，如 C\$ 和 Admin\$。如果停用登錄機碼 LocalAccountTokenFilterPolicy，則不需要在遠端部署期間於用戶端電腦上完全停用「使用者帳戶控制」。 若要停用 UAC 遠端限制，請參閱： Windows Vista 中使用者帳戶控制和遠端限制的說明 Windows Vista 中使用者帳戶控制和遠端限制的說明 請執行下列工作： • 停用「共用精靈」。 「共用精靈」可防範更進階的共用選項在遠端推送期間運作。 • 使用「網路和共用中心」啟用網路搜尋。 網路搜尋可讓您瀏覽網路。您無需它即可搜尋網路。 • 啟用內建管理員帳戶並指派密碼至此帳戶。 本機管理員帳戶擁有空白密碼時，遠端推送會失敗。 如果 Windows 用戶端電腦是 Active Directory 網域的一部分，請使用具備本機管理員權限的網域管理員帳戶憑證來進行遠端推送。 • 驗證您推送安裝的帳戶擁有管理員權限。 • 啟用並啟動遠端登錄服務。 • 停用或移除 Windows Defender。 請查詢作業系統的文件，以取得如何成功完成這些工作的相關指示。
準備 Windows 8/8.1 或更新版本，或者 Windows Server 2012/2012 R2 或更新版本的電腦	在您部署前，請執行下列工作： • 停用登錄機碼 LocalAccountTokenFilterPolicy。 若要停用 UAC 遠端限制，請參閱： Windows Vista 中使用者帳戶控制和遠端限制的說明 Windows Vista 中使用者帳戶控制和遠端限制的說明 • 啟用並啟動遠端登錄服務。 • 停用或移除 Windows Defender。

Table 19: 準備 Mac 用戶端進行遠端部署的工作

作業系統	工作
準備任何支援作業系統上的 Mac 電腦	在部署前，請在 Mac 電腦上執行下列工作： • 按下「系統喜好設定 > 共用 > 遠端登入」，並且允許所有使用者進行存取，或僅允許特定使用者存取，如管理員。 • 如果使用 Mac 防火牆，請停用隱藏模式。啟用隱藏模式之後，遠端推送安裝將無法透過「搜尋網路」搜尋用戶端。 若要在 Mac 上停用隱藏模式，請參閱下列文章，並選取您的 Mac 作業系統版本。請參閱： 使用隱藏模式讓 Mac 更安全 • 確保防火牆不會攔截安全 Shell (SSH) 使用的通訊埠。依據預設，此通訊埠為 TCP 通訊埠 22。此通訊埠允許進行遠端登入的必要通訊。 • Bonjour 服務不支援 IPv6 網路。若要確保「瀏覽網路」或「搜尋網路」顯示這些 Mac，請確定同時啟用了 IPv4 網路。 自 14.2 版起支援 IPv6 網路。

更多資訊

- [Symantec Endpoint Protection 的通訊埠](#)
- [使用遠端推送安裝 Symantec Endpoint Protection 用戶端](#)
- [準備用戶端安裝](#)

選擇使用用戶端部署精靈安裝用戶端的方法

安裝 Symantec Endpoint Protection Manager 後，請使用用戶端部署精靈安裝 Symantec Endpoint Protection 用戶端。

Table 20: 用戶端安裝方法

選項	說明
儲存套件	此安裝選項會建立一個可執行安裝套件，供您儲存到管理伺服器，再派送至用戶端電腦。然後，使用者會安裝用戶端軟體，因此這些使用者必須對其電腦具有本機管理員權限。 您可以使用此選項安裝 Windows、Mac 和 Linux 用戶端。請參閱： 使用儲存套件安裝 Symantec Endpoint Protection 用戶端
遠端推送	遠端推送安裝可將用戶端軟體推送至您指定的電腦。用戶端電腦將自動開始安裝。遠端推送安裝不需要使用者對其電腦具有本機管理員權限。 您可以使用此選項安裝 Windows 和 Mac 用戶端。請參閱： • 使用遠端推送安裝 Symantec Endpoint Protection 用戶端 • 準備 Windows 和 Mac 電腦進行遠端部署
網路連結與電子郵件	使用者會收到其中包含下載及安裝用戶端軟體的連結的電子郵件訊息。然後，使用者會安裝用戶端軟體，因此這些使用者必須對其電腦具有本機管理員權限。 您可以使用此選項安裝 Windows、Mac 和 Linux 用戶端。請參閱： 使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端

執行「用戶端部署精靈」之前，應檢閱安裝選項，或對其進行自訂，然後選取安裝期間的選項。安裝選項包括要安裝的防護技術、安裝目的地資料夾以及重新啟動行為。請參閱：

- [選擇要在用戶端上安裝哪些安全性功能](#)
- [關於 Windows 用戶端安裝設定](#)
- [準備用戶端安裝](#)

選擇要在用戶端上安裝哪些安全性功能

使用「用戶端部署精靈」部署 Windows 用戶端安裝套件時，必須選擇功能集。功能集指定在用戶端上安裝哪些防護功能。您可以選取預設功能集，也可以自訂功能集。依據電腦的角色以及電腦需要的安全層級或效能層級，決定要安裝哪些功能集。

安裝之後，您應該保持所有功能的啟用狀態。

Table 21: 用戶端安裝功能集 (Windows)

功能集	說明
用戶端完整防護	建議用於工作站、桌上型電腦和筆記型電腦。 包含所有防護功能、完整下載防護和郵件通訊協定防護。適用於筆記型電腦、工作站和桌上型電腦。 如果可能，請使用完整防護以獲得最大的安全性。
伺服器完整防護	建議用於伺服器。 包括電子郵件掃描程式防護以外的所有防護功能。適用於需要最高網路安全性的任何伺服器，包括 Symantec Endpoint Protection Manager 伺服器。
伺服器基本防護	建議用於高處理量伺服器。 包含病毒和間諜軟體防護以及基本下載防護。「入侵預防」可能會導致高傳輸量伺服器發生效能問題，因此，此選項適用於任何需要最高網路效能的伺服器。

Mac 用戶端安裝套件會安裝「病毒和間諜軟體防護」以及「入侵預防」。您無法為 Mac 用戶端安裝套件自訂功能。

Linux 用戶端安裝套件僅會安裝「病毒和間諜軟體防護」。

暗網中可以使用哪些功能？

暗網中的用戶端電腦無法使用任何需要網路存取的功能。這些功能包括：

- 可疑行為偵測 (BPE)。行為分析 (SONAR) 會以信譽免責判定，所以不會發生這些偵測。
- 主動啟發式防毒偵測，其需要檔案信譽以判定免責。
- 下載鑑識和任何純雲端特徵，因為無法執行信譽查詢。
- 瀏覽器延伸
- Web 和雲端存取防護

下列功能會在暗網中執行：

- IPS，在內部網路上執行。
- 防火牆
- 記憶體攻擊緩和
- 應用程式控制
- 裝置控制
- LiveUpdate - 設定外部 LiveUpdate 管理員以手動將該內容帶到您選擇的 HTTPS 伺服器。

自訂安裝功能集

如果您想要安裝一部分的防護功能，則請建立自訂功能集。不過，賽門鐵克建議您安裝所有功能。

您無法自訂 Mac 或 Linux 用戶端安裝套件的功能。

建立自訂用戶端安裝功能集

1. 在主控台中，按下「管理員」>「安裝套件」。
2. 按下「用戶端安裝功能集」>「新增用戶端安裝功能集」。
3. 在「新增用戶端安裝功能集」對話方塊中，輸入名稱和說明，然後勾選要安裝在用戶端上的防護功能。
4. 按一下「確定」。

管理用戶端安裝套件

若要使用 Symantec Endpoint Protection Manager 管理用戶端，您必須匯出受管用戶端安裝套件，然後將套件檔案安裝到用戶端電腦上。您可以使用 Symantec Endpoint Protection Manager 或協力廠商部署工具來部署用戶端。

賽門鐵克有時會提供更新版的安裝檔案套件，一般是在發行新產品版本時。您可以使用「自動升級」功能，在群組中的所有受管 Windows 與 Mac 用戶端上自動更新用戶端軟體。您不需要使用安裝部署工具重新部署軟體。

Table 22: 用戶端安裝套件相關工作

工作	說明
架構用戶端安裝套件	您可以選擇特定的用戶端防護技術進行安裝，也可指定安裝程序與一般使用者的互動方式。請參閱： 選擇要在用戶端上安裝哪些安全性功能 關於 Windows 用戶端安裝設定
匯出用戶端安裝套件	您可以為受管用戶端或非受管用戶端匯出套件。 您可以將這些套件匯出成單一可執行檔或是目錄中的一系列檔案。您選擇的方法取決於您的部署方法，以及您是否要升級群組中的用戶端軟體。一般而言，如果您使用 Active Directory 群組原則物件，則不選擇匯出至單一執行檔。請參閱： 匯出用戶端安裝套件 如何取得非受管用戶端安裝套件 安裝非受管 Windows 用戶端
匯入用戶端安裝套件更新	您可以將用戶端安裝套件新增到資料庫，以使這些套件可從 Symantec Endpoint Protection Manager 進行散佈。您可以選擇性地在此程序期間匯出套件，以便將套件部署至沒有用戶端軟體的電腦。請參閱： 將用戶端安裝套件匯入 Symantec Endpoint Protection Manager
在一或多個群組中升級 Windows 和 Mac 用戶端	您可以將匯出的套件一次安裝至一台電腦，也可以同時將匯出的檔案部署至多部電腦。 賽門鐵克提供用戶端安裝套件的更新時，您必須先將這些更新新增至 Symantec Endpoint Protection Manager，並且使這些更新可供匯出。但您不需要使用用戶端部署工具重新安裝這些更新。使用最新軟體更新 Windows 和 Mac 用戶端的最簡單方式是使用「自動升級」。您應該先更新測試電腦數量較少的群組。請參閱： 使用自動升級來升級用戶端軟體 如果您允許用戶端執行 LiveUpdate，而且「LiveUpdate 設定」政策允許更新，則您也可以使用 LiveUpdate 更新用戶端。
刪除用戶端安裝套件	您可以刪除舊的用戶端安裝套件來節省磁碟空間。但是，自動升級有時會使用較舊的用戶端安裝套件來建置升級套件。升級套件可使用用戶端執行較小的下載。

更多資訊

[準備用戶端安裝](#)

匯出用戶端安裝套件

如果您需要在使用「用戶端部署精靈」中的「儲存套件」時不可用的那些選項，您可能需要匯出用戶端安裝套件。例如，您可能需要使用自訂政策建立非受管用戶端。您也可能僅需要適用於 Windows 的 32 位元 (14.3 RU5 或更早版本) 或 64 位元安裝套件，或者需要適用於 Linux 的 `DPKG` 或 `RPM` 安裝套件。

匯出用戶端安裝套件後，即可對其進行部署。「用戶端部署精靈」中的「遠端推送」可以部署您匯出的 Windows 和 Mac 套件。或者，您可以將匯出的套件直接安裝到用戶端，或使用第三方程式來部署套件。

您可以為受管用戶端或非受管用戶端建立安裝套件。這兩種類型的套件都包含您指定的功能、政策和設定。如果您建立受管用戶端的套件，則可使用 Symantec Endpoint Protection Manager 主控台管理這些用戶端。如果您建立非受管用戶端的套件，則無法從主控台管理這些用戶端。您隨時可以透過「用戶端部署精靈」的「通訊更新套件部署」，將非受管 Windows 或 Mac 用戶端轉換成受管用戶端。

NOTE

如果從遠端主控台匯出用戶端安裝套件，就會在執行遠端主控台的電腦建立套件。此外，如果您使用多個網域，則必須匯出各個網域的套件，否則這些套件不會顯示在適當的網域群組中。

匯出用戶端安裝套件

-
1. 在主控台中，按下「管理員」，再按下「安裝套件」。
 2. 在「安裝套件」下方，按下「用戶端安裝套件」。
 3. 在「用戶端安裝套件」窗格的「套件名稱」下方，於要匯出的套件上按下滑鼠右鍵，然後按下「匯出」。
 4. 按下「瀏覽」導覽至要包含匯出之套件的資料夾，選取它，然後按下「確定」。

NOTE

「匯出套件」不支援包含雙位元組或高 ASCII 字元的目錄，並會阻止選取這些目錄。

5. 根據個人安裝需求設定其他選項。這些選項因匯出的安裝套件類型和平台而有所不同。

若需此對話方塊中匯出選項的詳細資料，請按下「說明」。

如需詳細資訊，請參閱：

[匯出套件設定](#)

6. 按下「確定」。

更多資訊

- [將用戶端安裝套件匯入 Symantec Endpoint Protection Manager](#)
- [選擇要在用戶端上安裝哪些安全性功能](#)
- [使用「通訊更新套件部署」還原用戶端伺服器通訊](#)

將用戶端安裝套件匯入 Symantec Endpoint Protection Manager

如果您使用已從舊版還原的資料庫升級至更新版本的 Symantec Endpoint Protection Manager，則可能需要將用戶端安裝套件匯入至 Symantec Endpoint Protection Manager。資料庫包括舊版用戶端安裝套件，並且您需要匯入更新的套件。

您應始終保持 Symantec Endpoint Protection Manager 版本與用戶端版本相同或更新。

NOTE

您可以直接匯入 .exe 或 .zip 檔案套件等執行檔套件，但不建議這麼做。 .info 檔案包含描述套件以及確保透過差異更新正確移轉至 Symantec Endpoint Protection 用戶端之未來版次的資訊。另一方面，Symantec Endpoint Protection Manager Web 主控台不會匯入 .info 檔案格式。在 Web 主控台中，您只能在諸如 .zip 或 .exe 檔案格式的單一檔案中匯入或匯出套件。

將用戶端安裝套件匯入 Symantec Endpoint Protection Manager

1. 將匯入的安裝套件複製到執行 Symantec Endpoint Protection Manager 之電腦上的某個目錄中。

用戶端安裝套件包含兩個檔案。一個檔案命名為 product_name.dat，另一個檔命名為 product_name.info。這些檔案會在安裝或升級 Symantec Endpoint Protection Manager 期間自動匯入。您也可以從安裝檔案的 SEPM/Packages 資料夾中取得這些套件。

2. 在主控台中，按下「管理員」>「安裝套件」。
3. 在「工作」下方，按下「新增用戶端安裝套件」。
4. 在「新增用戶端安裝套件」對話方塊中，輸入套件的名稱和敘述。
5. 按下「瀏覽」。
6. 在「選取資料夾」對話方塊中，尋找並選擇 product_name.info 檔，用於在步驟 1 中複製的新套件，然後按一下「選取」。
7. 出現「成功完成」提示時，按下「關閉」。

若要匯出安裝檔案並用於部署，請按下「匯出這個套件」，然後完成此程序。請參閱：

匯出用戶端安裝套件

成功匯入套件後，可在「系統」>「管理日誌」中看到「套件已建立」事件。將使用類似「已透過 Symantec Endpoint Protection Manager 成功匯入 SEP 14.3 RU2 64 位元套件。此套件現在可供部署。」的文字描述該事件。

Windows 用戶端安裝套件和內容更新大小

用戶端安裝套件、產品修補程式以及內容更新也儲存於 Symantec Endpoint Protection 資料庫並影響儲存需求。產品修補程式包含用戶端套件的資訊，以及每一種語言或地區設定的資訊。請注意，修補程式也會建立新的、完整的用戶端版次。

下表顯示用戶端安裝套件的大小 (若已啟用最大的用戶端記錄和防護層級技術)。

Table 23: Windows 用戶端安裝套件大小

用戶端類型/定義檔類型	*隨病毒定義檔一起安裝？	64 位元套件 (MB)	32 位元套件 (MB)
Standard 和 Embedded CoreDefs-3**	是	188	175
	否	93	81
暗網 CoreDefs-1.5	是	288	276
	否	93	80

如需詳細資訊，請參閱：

選擇使用用戶端安裝類型來下載雲端式還是本機式定義

對於這些套件，您可以設定更大的活動訊號。這些大小不包括封包層級防火牆日誌，這些日誌不建議在生產環境中使用。如果用戶端記錄已停用，且沒有新政策或內容可從管理伺服器下載，則用戶端安裝套件較小。在這種情況下，您可以設定較小的活動訊號。

*如果您的網路具有低頻寬，請在沒有病毒定義檔的情況下安裝用戶端套件。只要用戶端連線至管理伺服器，就可接收完整的病毒定義檔集。

所有用戶端安裝套件皆包含所有功能，例如病毒和間諜軟體、防火牆、IPS、SONAR、系統鎖定、應用程式控制、主機完整性內容等。用戶端類型之間的差異在於病毒和間諜軟體定義檔的大小。

內容更新只需要資料庫與檔案系統中較小的儲存空間。管理伺服器現在僅能儲存一個完整內容版本，外加增量差量，而不能儲存多個完整版本。完整內容更新需要 ~470 MB。

NOTE

您可以使用 LiveUpdate 伺服器、管理伺服器或群組更新提供者，採用與其他內容相同的方式將用戶端修補程式下載到用戶端。請參閱：

[在 Windows 用戶端上安裝 Endpoint Protection 用戶端修補程式](#)

在 Symantec Endpoint Protection Manager 中建立自訂 Windows 用戶端安裝套件

您可以透過架構用戶端安裝設定和用戶端功能集，針對 Symantec Endpoint Protection for Windows 自訂用戶端安裝套件。除此之外，此自訂操作可讓您架構安裝路徑、重新啟動行為，以及安裝套件是否解除安裝第三方安全性產品。

NOTE

用戶端安裝設定和用戶端安裝功能集組態僅適用於 Windows 安裝套件。您可以透過「管理 > 安裝套件 > 用戶端安裝套件」匯出 Macintosh 或 Linux 安裝套件，但組態選項有所差異。

Table 24: 建立自訂 Windows 用戶端安裝套件的工作

工作	詳細資訊
建立新的自訂用戶端安裝設定組態	使用「用戶端安裝套件」可定義安裝行為。 如果您要移除用戶端電腦上的現有安全軟體，請在此進行架構。 如需詳細資訊，請參閱： 自訂用戶端安裝設定 架構用戶端套件來解除安裝現有安全軟體
建立新的自訂功能集	「用戶端安裝功能集」定義在用戶端電腦上安裝的防護技術。請參閱： 選擇要在用戶端上安裝哪些安全性功能
建立新的自訂安裝套件	匯出用戶端安裝套件時，請從建立的自訂設定中進行選取。您也可以選擇儲存套件的位置，以及該套件為單一檔案 (.EXE) 還是包含多個檔案的資料夾。 也可以搭配「用戶端部署精靈」使用自訂安裝設定和自訂功能集。 如需詳細資訊，請參閱： 匯出用戶端安裝套件 使用遠端推送安裝 Symantec Endpoint Protection 用戶端

更多資訊

[準備用戶端安裝](#)

關於 Windows 用戶端安裝設定

用戶端部署精靈會提示您指定 Windows 用戶端的用戶端安裝設定。用戶端安裝設定定義安裝程序本身的選項。您可以定義目標安裝資料夾、是否停用安裝記錄以及重新啟動設定等選項。

您可以選擇預設用戶端安裝設定，或在「管理 > 安裝套件 > 用戶端安裝設定」下新增自訂「用戶端安裝設定」。上下文說明可提供關於可架構設定的詳細資料。

您應該針對遠端部署使用無訊息安裝，以最大程度減少使用者干擾。使用無訊息部署時，必須重新啟動加裝到 Symantec Endpoint Protection 的應用程式，如 Microsoft Outlook。

如果使用自動安裝（「僅顯示進度列」），則 Windows 可能會向使用者顯示一或多個彈出式視窗。但是，即使使用者沒有注意到這些視窗，安裝應該也不會失敗。

您不應針對遠端部署使用互動安裝。除非使用者與此安裝類型進行互動，否則安裝會失敗。同一作業系統上的安全性功能（如 Windows 階段作業 0 隔離）可能會造成不顯示互動安裝精靈。您應該僅針對本機安裝使用互動安裝類型。這些建議適用於 32 和 64 位元作業系統。

更多資訊

- [自訂用戶端安裝設定](#)
- [選擇要在用戶端上安裝哪些安全性功能](#)

自訂用戶端安裝設定

您可以變更可套用至用戶端安裝套件以及用於自動升級的安裝設定。

例如，如果您想要將用戶端安裝至自訂安裝資料夾，或是重設用戶端伺服器通訊設定，您可以建立自訂的用戶端安裝設定。然後可以在匯出或部署套件時套用此自訂設定，或是設定自動升級。

自訂用戶端安裝設定

1. 在主控台中，按下「管理員 > 安裝套件 > 用戶端安裝設定」。

2. 在「工作」下方，按一下「新增用戶端安裝設定」。

無法修改預設的用戶端安裝設定檔。

3. 選擇該設定檔適用的作業系統。

4. 輸入名稱和說明。

5. 從以下標籤上的可用選項中進行選擇：

- Windows：「基本設定」和「重新啟動設定」
 - Mac：「重新啟動設定」和「升級設定」
- Mac 用戶端重新啟動和升級設定僅適用自動升級

6. 按下「確定」。

執行「用戶端部署精靈」或架構自動升級時，選取您從「安裝設定」旁的下拉式功能表建立的設定。

更多資訊

- [關於 Windows 用戶端安裝設定](#)
- [架構用戶端套件來解除安裝現有安全軟體](#)

移除現有第三方安全軟體

您可以先架構和部署新的安裝套件來解除安裝第三方安全軟體，再安裝 Symantec Endpoint Protection 用戶端。解除安裝現有的安全軟體可以讓 Symantec Endpoint Protection 用戶端的執行更有效率。若要檢視用戶端套件會移除哪些第三方軟體，請參閱：

若要檢視用戶端套件會移除哪些第三方軟體，請參閱：[Endpoint Protection/Endpoint Security 中的第三方安全軟體移除](#)

您可以建立或修改自訂用戶端安裝設定架構，來啟用安全軟體移除功能。然後，在部署期間選取這個自訂架構。

某些程式可能具有特殊的解除安裝常式，或者可能需要停用自我防護元件。請參閱第三方軟體的說明文件。

您無法利用 Mac 或 Linux 用戶端套件移除第三方安全軟體。您必須先解除安裝第三方安全軟體，然後才能部署 Symantec Endpoint Protection 用戶端套件。

NOTE

對版本 14.2 之第三方安全軟體移除的變更，表示您無法為更早版本的安裝套件啟用此功能。例如，如果您從 Symantec Endpoint Protection Manager 14.2 版建立並從中部署 14.0.1 版用戶端套件，則無法為其啟用第三方安全軟體移除。

NOTE

在 14.3 RU9 和更舊版本中，您可以移除無法透過標準方法 (例如 Windows 控制台) 解除安裝的現有 Symantec Endpoint Protection 用戶端。此功能會以用戶端安裝設定中的獨立選項出現。在 14.3 RU10 中，基於安全性考量，已移除此功能。例如，

只有使用以下程序建立的套件才能移除現有安全軟體。

架構用戶端套件來解除安裝現有安全軟體

1. 在主控台的「管理員」頁面上，按一下「安裝套件」，然後按一下「用戶端安裝設定」。

2. 在「工作」下方，按一下「新增用戶端安裝設定」。

NOTE

如果您之前已建立自訂用戶端安裝設定架構，則可以在「工作」下方進行修改，然後按一下「編輯用戶端安裝設定」。修改現有的自動架構並不會修改之前匯出的安裝套件。

3. 在「基本設定」標籤上，按一下「自動解除安裝現有的第三方安全軟體」。

在 14.3 RU9 和更舊版本中，您可以使用「移除無法解除安裝的現有 Symantec Endpoint Protection 用戶端軟體」選項來移除損毀版本的 Symantec Endpoint Protection 用戶端。請參閱：

[使用用戶端安裝設定來解除安裝 Symantec Endpoint Protection 用戶端 \(14.3 RU9 和更早版本\)](#)

4. 按一下「確定」>「確定」。

您也可以修改此組態的其他選項。如需這些選項的詳細資訊，請按一下「說明」。

部署用戶端套件來移除現有安全軟體

1. 在主控台的「首頁」頁面上，啟動「用戶端部署精靈」。
2. 按一下「說明 > 「開始使用」頁面」，然後在「所需工作」下方按一下「在您的電腦上安裝用戶端軟體」。
3. 在「用戶端部署精靈」中，按一下「新套件部署」，然後按「下一步」。
您可以使用「現有套件部署」部署您先前建立的安裝套件。但是，您必須早已使用自訂用戶端安裝設定架構匯出這些套件，如上述程序所述。
4. 在「選取群組並安裝功能集」中，選取 Windows 安裝套件。在「安裝設定」下拉式清單中，選取您在上述程序中所建立或修改的自訂用戶端安裝設定架構。按「下一步」。
5. 按一下您要使用的部署方法，然後按「下一步」繼續進行並完成您選擇的部署方法。

更多資訊

- [選擇使用用戶端部署精靈安裝用戶端的方法](#)
- [關於 Windows 用戶端安裝設定](#)
- [準備用戶端安裝](#)

選擇使用用戶端安裝類型來下載雲端式還是本機式定義

當您指定 Windows 用戶端安裝套件時，必須選擇從雲端還是本機下載定義。啟用雲端的選項包括標準用戶端和內嵌式/VDI 用戶端。Symantec Endpoint Protection 還包括適用於未連線至雲端之用戶端的暗網安裝。

NOTE

如果您稍後想要在用戶端安裝之後變更 Windows 用戶端安裝類型「標準用戶端」、「內嵌式或 VDI」或「暗網」，則必須先解除安裝現有用戶端軟體、重新架構這些設定，然後重新安裝新的用戶端套件。

Table 25: 用戶端的下載選項

標準用戶端	暗網用戶端	內嵌/VDI 用戶端
• 使用雲端中的病毒和間諜軟體定義檔。 • 僅在磁碟上安裝最新的病毒和間諜軟體定義檔。 標準用戶端在磁碟方面比舊版標準或暗網 Windows 用戶端小大約 80% 到 90%。 • 使用差量而非完整安裝處理「自動升級」。	• 無法使用雲端中的定義檔。 • 適用於具有間歇性雲端存取權或無雲端存取權的用戶端。 • 安裝一組完整的病毒和間諜軟體定義檔。 • 類似於舊版標準大小用戶端；如果已連線至雲端，則針對下載鑑識和行為分析 (SONAR) 使用信譽查詢。 • 使用差量而非完整安裝處理「自動升級」。	• 使用雲端中的病毒和間諜軟體定義檔。 • 僅安裝最新的病毒和間諜軟體定義檔。 用戶端在磁碟方面比暗網 Windows 用戶端小大約 80% 到 90%。 • 與標準用戶端相較，內嵌式/VDI 用戶端包含更多大小最佳化： — 在安裝完成之後，安裝快取不會儲存。此變更表示您無法透過「控制台」來移除或修改安裝，除非您先將安裝套件複製到用戶端電腦。 — 與標準用戶端相較，內嵌式用戶端會在更多的資料夾上利用 NTFS 壓縮。 • 使用完整安裝套件處理「自動升級」；無法使用差量。

更多資訊

- [選擇使用用戶端部署精靈安裝用戶端的方法](#)
- [匯出用戶端安裝套件](#)

Endpoint Protection/Endpoint Security 中的第三方安全軟體移除

下表列出了 Symantec Endpoint Protection 用戶端安裝套件可以移除的第三方安全產品。「用戶端安裝設定」對話方塊中的「自動解除安裝現有的第三方安全軟體」會移除這些產品。

Table 26: 「用戶端安裝精靈」移除的第三方安全產品清單

版本	更多資訊
14.3 RU1 和更新版本	Endpoint Protection 14.3 RU1 和更新版本中的第三方安全軟體移除
14.3 MP1	在 14.3 MP1，已從 Symantec Endpoint Protection Manager 移除「自動移除現有的協力廠商安全軟體」選項。請改用位於 Symantec Endpoint Protection 下載資料夾之 Tools/TPAR 資料夾中的 TPAR 工具。 讀我檔案位於： 關於 Symantec Endpoint Protection 中的第三方安全軟體移除功能 如果您有 14.3 MP1 Symantec Endpoint Protection Manager，並且需要為 14.0 到 14.3 用戶端建立安裝套件，則可以顯示並使用「自動解除安裝現有的第三方安全軟體」選項，方法是將 scm.uninstall.thirdparty.security.software.enabled=true 新增至 conf.properties 檔案，然後重新啟動管理伺服器服務。
14.0 到 14.3	Endpoint Protection 14 中的第三方安全軟體移除

更多資訊

- [移除現有第三方安全軟體](#)
- [使用用戶端安裝設定來解除安裝 Symantec Endpoint Protection 用戶端 \(14.3 RU9 和更早版本\)](#)

Symantec Endpoint Security/Symantec Endpoint Protection 14.3 RU1 和更新版本中的第三方安全軟體移除

下表列出了 Symantec Endpoint Protection (SEP)/Symantec Endpoint Security (SES) 可在用戶端安裝套件安裝之前移除的第三方產品和產品版本。用戶端安裝套件會移除產品的任何版本。

Table 27: 14.3 RU2 和更新版本用戶端安裝精靈所移除的第三方安全產品清單

設定	說明
Avast	AntiVirus
AVG	AVG Internet Security Business Edition 2013
ESET	ESET Smart Security
Kaspersky	Kaspersky AntiVirus Kaspersky Endpoint Security Kaspersky Internet Security Kaspersky Security Center Network Agent
McAfee	McAfee Scan Enterprise

Table 28: 「14.3 RU1 用戶端安裝精靈」所移除的第三方安全產品清單

設定	說明
Avast	AntiVirus
AVG	AVG Protection
ESET	ESET Endpoint Antivirus / ESET Endpoint Security ESET Remote Administrator Agent
F-Secure	F-Secure Anti-Spyware F-Secure Anti-Spyware Scanner F-Secure Anti-Virus Client Security Installer F-Secure Automatic Update Agent F-Secure Backweb F-Secure Browsing Protection F-Secure CustomizationSetup F-Secure DAAS2 F-Secure Device Control F-Secure Diagnostics F-Secure E-mail Scanning F-Secure FWES F-Secure GateKeeper Interface F-Secure Gemini F-Secure GUI F-Secure Help F-Secure HIPS F-Secure Internet Shield F-Secure Localization API F-Secure Management Agent F-Secure Management Extensions F-Secure NAC Support F-Secure NAP Support F-Secure NIF F-Secure Offload Scanning Agent F-Secure ORSP Client F-Secure Policy Manager Support F-Secure Protocol Scanner F-Secure Safe Banking Popup F-Secure Sidegrade Support F-Secure Software Updater F-Secure System File Update F-Secure TNB F-Secure Uninstall F-Secure Anti-Virus
Kaspersky	Kaspersky Endpoint Security Kaspersky AES Encryption Module Kaspersky Anti-Virus for Windows Servers Kaspersky Security for Windows Servers Kaspersky Anti-Virus for Windows Workstations Kaspersky PURE Kaspersky Small Office Security Kaspersky AntiVirus / Kaspersky Internet Security Kaspersky Endpoint Security 8 for Windows Console Plug-in Kaspersky Anti-Virus SOS Kaspersky Security Center Network Agent

設定	說明
McAfee	McAfee Endpoint Security Web Control McAfee Endpoint Security Firewall McAfee Endpoint Security Threat Prevention McAfee Endpoint Security Platform McAfee Desktop Firewall McAfee VirusScan Enterprise McAfee Firewall Protection Service McAfee Virus and Spyware Protection Service McAfee Browser Protection Service McAfee SiteAdvisor Enterprise McAfee Agent McAfee Product Improvement Program McAfee Host Intrusion Prevention
Sophos	Sophos Endpoint Agent Sophos Patch Agent Sophos Network Threat Protection Sophos System Protection Sophos Client Firewall Sophos Anti-Virus Sophos Exploit Prevention Sophos Remote Management System Sophos AutoUpdate Sophos Endpoint Defense
Trend Micro	Trend Micro OfficeScan Agent

有了 14.3 MP1 和更新版本的 Symantec Endpoint Protection Manager (SEPM)，您再也無法建立安裝套件，使用「用戶端安裝設定」對話方塊中的「自動移除現有的協力廠商安全軟體」選項。改用 TPAR。不過，如果您有 14.3 MP1 SEPM，並且正要為比 14.3 MP1 舊的 SEP 用戶端建立安裝套件，則可以使用此功能，但必須將 **scm.uninstall.thirdparty.security.software.enabled=true** 新增至 conf.properties，然後重新啟動管理伺服器服務。此動作會取消隱藏核取方塊。該選項僅適用於 14.0 到 14.3 版的用戶端，因為它們仍包含用戶端功能。

從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦

在 Symantec Endpoint Protection 中，您可能需要在安裝或升級之後重新啟動用戶端電腦。

下表說明每種用戶端類型的重新啟動選項。

用戶端類型	說明
Windows	在安裝之後，預設會自動重新啟動 Windows 用戶端電腦。不過，用戶端使用者可以延遲到第二天預先排定的時間。 在您安裝用戶端軟體之後，不需要重新啟動 Windows 電腦，但具有下列例外： • 已安裝防火牆 (14.3 RU1 和更舊版本)。 • 已安裝應用程式與裝置控制 (所有 14.x 版本) (14.3 RU4 和更早版本) 在升級用戶端之前執行的程序不會強制執行應用程式控制。 • 已安裝或解除安裝應用程式強化 (14.3 RU3 和更舊版本)。 在您升級用戶端軟體之後，不需要重新啟動 Windows 電腦，但具有下列例外： • 您可以從 14.3 RU2 和更舊版本的用戶端進行升級。 • 您可以安裝或解除安裝應用程式強化。或者，您可以從具有應用程式強化的 14.3 RU3 和更舊版本的用戶端進行升級。請從 Symantec Endpoint Security (SES) 雲端主控台管理應用程式強化和用戶端。 • Symantec Endpoint Protection 用戶端與下列代理程式安裝在同一部電腦上： — 獨立式 Symantec Data Center Security — 獨立式 Symantec Critical System Protection — Symantec Data Loss Prevention (15.5 - 15.8) • 先前從相同版本的升級嘗試失敗。例如，如果您嘗試從 14.3 RU2 升級到目前版本失敗。 匯出或部署安裝套件之前，您可以架構 Windows 用戶端安裝設定，以自訂安裝後重新啟動。您可以在某個群組上架構重新啟動選項，以控制在風險矯正或新用戶端下載後，用戶端電腦重新啟動的方式。 • 您也可以從管理伺服器執行重新啟動指令，隨時重新啟動 Windows 用戶端電腦。 什麼是可對用戶端電腦執行的指令？ 在用戶端電腦上從主控台執行指令 • 您可以將 Windows 用戶端電腦排程為在使用者方便的時間重新啟動。 • 您可以強制立即重新啟動或讓使用者延遲重新啟動。
Mac	Mac 用戶端電腦會提示安裝後重新啟動。如果您推送用戶端套件，而且使用者未登入 Mac 電腦，則安裝完成之後，會自動發生硬式重新啟動。您無法自訂此設定。 您也可以從管理伺服器執行重新啟動指令，隨時重新啟動 Mac 用戶端電腦。 將重新啟動指令傳送給 Mac 用戶端電腦時，始終會執行硬式重新啟動。
Linux	安裝後，Linux 用戶端電腦不需要重新啟動，也不會自動重新啟動。 您無法使用管理伺服器中的重新啟動指令來重新啟動 Linux 用戶端。

在 Windows 用戶端電腦上架構重新啟動選項

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面上選取群組，再按下「政策」。
3. 在「政策」標籤上，按下「一般設定」。
4. 在「一般設定」對話方塊的「重新啟動設定」標籤上，選取重新啟動方式和排程。
某些重新啟動選項僅適用於 Windows 用戶端。如需詳細資訊，請參閱前後文相關說明。
您也可以新增重新啟動前出現在用戶端電腦上的通知。預設訊息會告訴使用者安全風險矯正或新內容下載需要重新啟動。
5. 按一下「確定」。

重新啟動所選用戶端電腦

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」標籤中，選取群組。

3. 在「用戶端」標籤上，選取用戶端，在「對電腦執行指令」上按下滑鼠右鍵，然後按下「重新啟動用戶端電腦」。
 4. 按下「是」，指定您需要的重新啟動選項，然後按下「確定」。
- 某些重新啟動選項僅適用於 Windows 用戶端。如需詳細資訊，請參閱前後文相關說明。

重新啟動所選群組中的用戶端電腦

1. 在主控台中，按一下「用戶端」。
 2. 在「用戶端」頁面的「用戶端」標籤上選取群組，按下「對群組執行指令」，然後按下「重新啟動用戶端電腦」。
 3. 按下「是」，指定您需要的重新啟動選項，然後按下「確定」。
- 某些重新啟動選項僅適用於 Windows 用戶端。如需詳細資訊，請參閱前後文相關說明。

更多資訊

- [關於 Windows 用戶端安裝設定](#)
- [準備用戶端安裝](#)

關於受管和非受管 (自我管理) 用戶端

您可以將用戶端軟體安裝為受管用戶端或非受管用戶端。

在大多數情況下，您應該安裝受管用戶端。安裝非受管用戶端，以便使用者對電腦具有更多控制，例如測試電腦，或如果電腦主要為離站均可。請確認非受管用戶端使用者具有適當程度的知識，可以架構不同於預設設定的任何安全性設定。

NOTE

您可以稍後將非受管用戶端轉換成受管用戶端，方法為取代用戶端電腦上的用戶端伺服器通訊檔案。請參閱：[在用戶端電腦上取代用戶端伺服器通訊檔案](#)

Table 29: 受管與非受管用戶端之間的差別

受管用戶端	非受管用戶端
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，而管理伺服器會將設定下載到用戶端。若管理員變更防護。	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。
使用者不具必要的用戶端架構權限。所有設定均會鎖定或無法使用，但我們可以檢視用戶端在電腦上所執行動作的相關資訊。	用戶端使用者具有架構用戶端和所有設定的權限。
管理員負責管理用戶端，但用戶端使用者可以變更部分用戶端設定和執行某些工作。例如，用戶端使用者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。	用戶端使用者可以執行所有管理工作。
管理員負責管理用戶端，但我們可以變更所有用戶端設定和執行所有防護工作。	用戶端使用者會管理非受管用戶端。
受管用戶端可以透過 Symantec Endpoint Protection Manager、GUP、Internet 和 LiveUpdate 取得內容更新。	非受管用戶端則會透過 Internet 和 LiveUpdate 取得內容更新。用戶端使用者必須個別在每個用戶端上更新內容。

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	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。

更多資訊

- [檢查用戶端是受管用戶端還是非受管用戶端](#)
- [如何取得非受管用戶端安裝套件](#)
- [安裝非受管 Windows 用戶端](#)

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。

關於受管和非受管 (自我管理) 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」。

如何取得非受管用戶端安裝套件

您可以透過以下其中一種方式取得非受管 Symantec Endpoint Protection 用戶端安裝套件：

- 從 [Broadcom 支援入口網站](#) 下載獨立式用戶端安裝程式。
- 從 [Broadcom 支援入口網站](#) 複製完整安裝檔案內的資料夾。
- 使用預設政策和設定或使用自訂政策和設定，從 Symantec Endpoint Protection Manager 匯出非受管用戶端。

NOTE

如需下載軟體的指南，請參閱：

[下載最新版本的 Symantec Endpoint Protection](#)

下載獨立式用戶端安裝程式

1. 登入 [Broadcom 支援入口網站](#)。
2. 下載以下檔案：
Symantec_Endpoint_Protection_version_All_Clients_lang.zip

其中 version 是版本號碼，而 lang 是語言，例如 EN 表示英文。

3. 將檔案的內容解壓縮至您的硬碟機。
4. 根據要在其上安裝用戶端的作業系統，執行以下其中一個動作：
 - 若為 Windows：將 32 位 (14.3 RU5 或更早版本) 或 64 位 .exe 檔案複製至目標電腦。
 - 若為 Mac：將 Mac 用戶端 .zip 檔案複製到目標電腦。
 - 若為 Linux：將 Linux 用戶端 .zip 檔案複製到目標電腦。

NOTE

Symantec Agent 或 Symantec Endpoint Protection for Linux 14.3 RU1 和更新版本無法以非受管用戶端身分執行。

從完整安裝檔案複製資料夾

1. 登入 [Broadcom 支援入口網站](#)。
2. 下載以下檔案：
Symantec_Endpoint_Protection_version_Full_Installation_lang.exe
其中 version 是版本號碼，而 lang 是語言。
3. 連按兩下檔案以解壓縮其內容。
4. 執行下列其中一個動作：
 - 對於 14.2 版 MP1a (14.2.1023.0100) 或更新版本，檔案會解壓縮至 C:\Users\username\AppData\Local\Temp\7zXXXXXXXXXX，其中 XXXXXXXXXX 表示字母和數字組成的隨機字串。瀏覽到該資料夾。請不要關閉安裝功能表。
 - 對於早於 14.2 MP1a (14.2.1023.0100) 的版本，輸入或瀏覽到要解壓縮至其中的資料夾，然後按下「解壓縮」。解壓縮完成後，瀏覽至該資料夾。
5. 根據要在其上安裝用戶端的作業系統，執行以下其中一個動作：
 - 若為 Windows：將資料夾 **SEP** (32 位元) 或 **SEPx64** (64 位元) 複製到目標電腦。
 - 若為 Mac：將資料夾 **SEP_MAC** 複製到目標電腦。
 - 若為 Linux：將資料夾 **SEP_LINUX** 複製到目標電腦。

從 **Symantec Endpoint Protection Manager** 匯出非受管用戶端

1. 登入 Symantec Endpoint Protection Manager。
2. 執行下列其中一個動作：
 - 使用預設政策和設定，從 Symantec Endpoint Protection Manager 匯出非受管用戶端。請參閱：
[匯出用戶端安裝套件](#)
 - 使用自訂政策和設定，從 Symantec Endpoint Protection Manager 匯出非受管用戶端。如需建議，請參閱：
[非受管用戶端安裝套件的建議政策和設定](#)
您無法使用群組政策匯出非受管 Mac 用戶端。
然後，您可以為 Windows、Mac 或 Linux 安裝非受管用戶端。
如果檔案是 .zip 檔，您必須先解壓縮所有內容，然後進行安裝。

更多資訊

- [安裝非受管 Windows 用戶端](#)
- [關於受管和非受管用戶端](#)

安裝非受管 Windows 用戶端

非受管 (或自我管理) 用戶端通常會允許使用者透過用戶端使用者介面對 Symantec Endpoint Protection 設定擁有較多的控制。一般來說，您會將非受管 Symantec Endpoint Protection 用戶端直接安裝在 Windows 電腦上，而安裝需要使用者輸入才能完成。請參閱：

- [關於受管和非受管用戶端](#)
- [如何取得非受管用戶端安裝套件](#)

NOTE

將受管 Windows 用戶端安裝套件直接安裝至用戶端電腦上時，安裝步驟是類似的。只有「互動式」安裝需要使用者輸入。安裝未受管 Windows 用戶端時，用戶端安裝設定選項「只顯示進度列」和「無訊息」不需要使用者輸入。

NOTE

使用自訂政策架構的非受管用戶端套件，於安裝期間可能不會顯示描述的部分面板。如果您沒有看到程序步驟描述的某個安裝面板，請跳到下一個步驟。

安裝非受管 Windows 用戶端

1. 執行 Setup.exe 或 Symantec_Endpoint_Protection_<versionnumber>_Win64-bit_Client_<language>.exe，然後按一下「下一步」。
2. 在「授權許可協議」畫面中，按下「我同意」，再按「下一步」。
3. 在「安裝類型」面板上，按下列其中一個選項，然後按「下一步」：
按下包含最常用選項的「典型」。
按一下「自訂」以架構安裝。
 - 在「安裝類型」面板上，您可以選擇要從雲端還是在本機下載定義 (暗網)。
 - 在「自訂安裝」面板上，選擇要在電腦上安裝的功能。功能上的紅色 X 表示未安裝。如需更多詳細資訊，請參閱：[選擇要在用戶端上安裝哪些安全性功能](#)
4. 如果安裝精靈顯示提示，請按下「啟用自動防護」和「執行 LiveUpdate」，再按「下一步」。
5. 在「檔案信譽資料傳送」和「資料收集」面板上，如果您不想為賽門鐵克提供匿名資料，請取消勾選方塊，然後按一下「安裝」。
如果沒有已付費授權，則即使您讓方塊保持勾選，非受管用戶端還是不會傳送資料。
6. 在「精靈完成」畫面上，按下「完成」。

更多資訊

- [準備用戶端安裝](#)
- [關於 Windows 用戶端安裝設定](#)

解除安裝 Symantec Endpoint Protection 用戶端

- [解除安裝 Windows 用戶端](#)
- [刪除特定用戶端元件](#)
- [正在解除安裝 Symantec Endpoint Protect Manager \(SEPM\)](#)
- [傳統解除安裝方法失敗時該怎麼辦](#)
- [解除安裝 Linux Agent](#)
- [解除安裝 Mac 用戶端](#)

解除安裝 Windows 用戶端

解除安裝單一用戶端或一小群用戶端	使用 標準 Windows 解除安裝方法 程式和功能。 在 14.3 RU9 和更早版本中，您可以 部署自訂用戶端安裝套件 ，而此套件可移除 Symantec Endpoint Protection 用戶端。
解除安裝大型用戶端群組，包括遠端解除安裝大型用戶端群組。	無法實際存取每個用戶端時，還有許多方法可以自動執行該過程。其中包括： • 使用 Active Directory 群組原則物件解除安裝用戶端軟體 • 使用指令提示解除安裝 Endpoint Protection 用戶端

解除安裝用戶端不會從 Symantec Endpoint Protection Manager 將其移除。您也必須從 Symantec Endpoint Protection Manager 刪除用戶端，或設定時段以刪除在指定時間內未連線的用戶端。請參閱：

刪除用戶端

清除過時的非持續 (NPVDI) 用戶端以釋放授權

如果 Symantec Endpoint Protection 用戶端軟體使用可攔截硬體裝置的裝置控制政策，則政策會在您解除安裝軟體之後攔截裝置。如果您未在解除安裝之前停用裝置控制政策，則請使用「Windows 裝置管理員」來取消對裝置的攔截。

刪除特定的 Symantec Endpoint Protection 用戶端元件

從單個或未受管用戶端中刪除元件	您可以使用「新增或刪除程式」或「程式和功能」來刪除或新增防護元件，而無需重新安裝用戶端。請參閱： 新增或移除現有 Endpoint Protection 用戶端的功能 。
從一大組用戶端中刪除元件	使用 Symantec Endpoint Protection Manager 用戶端安裝功能集選項可以修改整組安裝功能。請參閱： 新增或移除現有 Endpoint Protection 用戶端的功能 。

解除安裝 Symantec Endpoint Protection Manager

解除安裝 Symantec Endpoint Protection Manager 相當簡單，應可以在每個管理伺服器進行。下表列出與此過程相關的主題。

執行災難復原並備份 Symantec Endpoint Protection Manager	在解除安裝 Symantec Endpoint Protection Manager 之前，應先進行備份，以便在重新安裝時輕鬆重新連接現有用戶端並使用之前配置的政策。 有關準備進行災難復原的資訊，請參閱 Endpoint Protection 的災難復原最佳實務準則備份資料庫和日誌
解除安裝 Symantec Endpoint Protection Manager	使用 標準 Windows 解除安裝方法 。 若要解除安裝 Symantec Endpoint Protection Manager，您可以使用 Windows「控制台」來解除安裝、修復或變更應用程式，通常是使用「程式和功能」。 移除 Symantec Endpoint Protection Manager 時也會移除伺服器主控台。在移除過程中，您可以選擇移除資料庫和資料庫備份檔案。
將現有用戶端重新連接到新的或重新安裝的 Symantec Endpoint Protection Manager	如果您需要解除安裝並重新安裝 Symantec Endpoint Protection Manager，而未提前執行災難復原，請將現有的 Symantec Endpoint Protection 用戶端重新連接到新的管理伺服器安裝。

傳統解除安裝方法失敗時該怎麼辦

有時，解除安裝 Symantec Endpoint Protection Manager 的建議方法和首選方法會失敗或無法按預期執行。	CleanWipe 實用工具只適用於從 Windows 控制面板安裝 Symantec Endpoint Protection 失敗的情況。請參閱： 下載 CleanWipe 移除工具來解除安裝 Endpoint Protection 。
您也可以手動刪除 Windows 用戶端，這是最後的手段。	請參閱： 手動解除安裝 Windows 上的 Endpoint Protection 用戶端

解除安裝 Linux Agent

執行指令碼以解除安裝任意大小的代理程式群組。	請參閱： 解除安裝 Symantec Endpoint Protection Linux Agent 或 Symantec Single Agent for Linux

解除安裝 Mac 用戶端

單一用戶端或一小群用戶端	請參閱： 解除安裝 Mac 用戶端
一大群用戶端	請參閱： 行動裝置管理 (MDM)

傳統方法失敗時該怎麼辦	RemoveSymantecMacFiles 實用工具會刪除與 Mac 用戶端安裝相關的所有檔案和資料夾。有關使用的更多資訊和說明，請參閱「 使用 RemoveSymantecMacFiles 刪除適用於 Mac OS 的 Symantec 軟體 」的文件。 RemoveSymantecMacFiles/SymantecRemovalTool 從 Mac 中刪除所有 Symantec 產品。

使用用戶端安裝設定來解除安裝 Symantec Endpoint Protection 用戶端 (14.3 RU9 和更早版本)

NOTE

Symantec Endpoint Protection Manager 14.3 RU10 已移除「移除無法解除安裝的現有 **Symantec Endpoint Protection** 用戶端軟體」選項。相反地，用戶端使用者必須輸入預設用戶端密碼或群組層級密碼，才能解除安裝用戶端。預設用戶端密碼是您在安裝或升級管理伺服器時所新增的密碼。如需建立群組層級密碼的相關資訊，請參閱[用密碼保護 Symantec Endpoint Protection 用戶端](#)。

在 14.3 RU9 和更舊版本中，您可以在 Symantec Endpoint Protection 安裝開始之前，解除安裝用戶端電腦上的現有用戶端安裝。此功能可與 CleanWipe 公用程式相比，因此，不應該針對所有部署啟用此功能。相反地，您應該僅使用此功能來移除已損毀或未正常運作的 Symantec Endpoint Protection 用戶端安裝。

使用「移除無法移除的現有 **Symantec Endpoint Protection** 用戶端軟體」功能之前，請注意此重要資訊：

- 此功能會移除所有 Symantec Endpoint Protection 版本，直到並包含您建立的安裝套件版本。
- 此功能無法解除安裝高於隨附安裝套件的 Symantec Endpoint Protection 版本。例如，您無法在規劃的回復期間使用此功能。
- 如果您部署的錯誤套件類型已啟用此功能，則不會執行移除。例如，如果您將 32 位元套件部署到 64 位元電腦，則無法安裝。因此，它不會移除現有的 Symantec Endpoint Protection 安裝。
- 您無法將此功能用於直接使用 .MSI 檔案的安裝，例如透過 GPO 部署。
- 此功能不適用於手動升級或自動升級。您僅能使用此功能與全新安裝搭配。
- 此功能不會移除 Symantec Endpoint Protection Manager。
- 如果其他賽門鐵克產品皆未使用此功能，此選項僅會移除 Windows LiveUpdate。
- 在用戶端電腦上，此功能會以無訊息方式執行，且不顯示狀態畫面或使用介面。
- 此選項會強制安裝類型為 [無訊息]。

若要使用用戶端安裝套件來解除安裝 Windows 用戶端，請參閱下列步驟：

1. 在主控台的「管理員」頁面上，按一下「安裝套件」，然後按一下「用戶端安裝設定」。
2. 在「工作」下方，按一下「新增用戶端安裝設定」。
如果您之前已建立自訂用戶端安裝設定架構，則可以在「工作」下方進行修改，然後按一下「編輯用戶端安裝設定」。修改現有的自動架構並不會修改之前匯出的安裝套件。
3. 在「基本設定」標籤上，勾選「移除無法解除安裝的現有 **Symantec Endpoint Protection** 用戶端軟體」。
4. 閱讀訊息，然後按下「確定」。
5. 按一下「確定」。

更多資訊

- [下載 CleanWipe 移除工具來解除安裝 Endpoint Protection](#)
- [架構用戶端套件來解除安裝現有安全軟體](#)
- [Endpoint Protection/Endpoint Security 中的第三方安全軟體移除](#)

解除安裝 Mac 的 Symantec Endpoint Protection 用戶端

用戶端使用者可以透過功能表列上的用戶端圖示來解除安裝 Mac 的 Symantec Endpoint Protection 用戶端。解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端需要管理使用者認證。

NOTE

在 Mac 用戶端解除安裝之後，會提示用戶端使用者重新啟動用戶端電腦以完成解除安裝。請確定使用者已儲存任何未完成的工作，並已關閉所有已開啟的應用程式，再將它們重新啟動。

解除安裝 Symantec Endpoint Protection for Mac 用戶端

1. 在 Mac 用戶端電腦上，開啟 Symantec Endpoint Protection 用戶端，然後按下「**Symantec Endpoint Protection** > 「解除安裝 **Symantec Endpoint Protection**」。
2. 再次按下「解除安裝」開始解除安裝作業。
3. 若要安裝解除安裝 Symantec Endpoint Protection 用戶端所需的協助程式工具，請輸入 Mac 的管理使用者名稱和密碼，然後按一下「安裝協助程式」。
4. 在「**Symantec Endpoint Protection** 嘗試修改系統副檔名」對話方塊中，輸入 Mac 的管理使用者名稱和密碼，然後按一下「確定」。

可能還會提示您輸入密碼以解除安裝用戶端。此密碼可能與 Mac 的管理密碼不同。

解除安裝完成之後，您可以按一下「立即重新啟動」。

如果解除安裝失敗，您可能必須使用其他解除安裝方法。請參閱：

[解除安裝 Symantec Endpoint Protection 用戶端](#)

刪除用戶端

刪除用戶端電腦時，您也必須解除安裝用戶端軟體。

如果您未同時解除安裝用戶端，管理伺服器將會繼續將內容更新下載到用戶端電腦。您也可以設定時段以刪除在指定時間內未連線的用戶端。請參閱：

[解除安裝 Symantec Endpoint Protection 用戶端](#)

[清除過時的非持續 \(NPVDI\) 用戶端以釋放授權](#)

刪除用戶端

1. 在主控台的「用戶端」頁面上，選取用戶端所在的群組。
2. 以滑鼠右鍵按一下用戶端，並按一下「刪除」，然後按一下「是」。

升級和移轉到最新版本的 Symantec Endpoint Protection (SEP)

更新到最新版本的 Symantec Endpoint Protection Manager 和用戶端。

使用此主題以升級到 SEP 的最新版本，並利用新功能。本資訊特別針對在已安裝相容產品版本的環境中升級軟體。

進行升級之前，請先檢閱下列資訊：

- [所有 Endpoint Protection 版本的版本說明、新修正和系統需求](#)
- [已知問題與因應措施](#)
- [Symantec Endpoint Protection 14.x 所有版本的新功能](#)
- [最新版本 Symantec Endpoint Protection 14.x 支援和不支援的升級路徑](#)

Table 31: 升級 Symantec Endpoint Protection 的程序

工作	說明
步驟 1：從「Broadcom 下載中心」下載最新版本	如需連結和資訊，請參閱： 下載最新版本的賽門鐵克軟體 在您升級 Symantec Endpoint Protection Manager (SEPM) 和 Symantec Endpoint Protection 用戶端之前，請確定遵循下列最佳實務準則，以在升級期間最大限度地保護您的網路： • 賽門鐵克建議您不要在升級 Symantec Endpoint Protection 的同時執行第三方安裝。在升級 Symantec Endpoint Protection 時，安裝進行網路或系統級更改的第三方軟體可能會導致不良結果。 • 如果可能，請在安裝或升級 Symantec Endpoint Protection 之前重新啟動用戶端電腦。 • 賽門鐵克建議您將整個網路升級至目前 Symantec Endpoint Protection 版本，而不是管理多個版本。 如需詳細資訊，請參閱： Endpoint Protection 14.x 的升級最佳實務準則
步驟 2：備份資料庫並準備災難復原	備份 Symantec Endpoint Protection Manager 用於確保用戶端資料完整性的資料庫、日誌和復原檔案。這些步驟因版本而異。請參閱： Endpoint Protection 的災難復原最佳實務
步驟 3：停止 Symantec Endpoint Protection Manager 服務 (14.3 RU8 或更舊版本)	如果是 14.3 RU8 或更舊版本，您必須先在所有網站手動停止管理伺服器服務，才可以安裝更新版本。管理伺服器服務停止在 SEPM 上運行的 Syslog 服務或類似服務，這些服務可能會鎖定 SEPM 檔案或資料夾並導致升級失敗。升級後，管理伺服器會自動啟動服務。 Note: 自 14.3 RU9 起，請勿停止網站中第一台伺服器的 SEPM 服務，否則升級作業會失敗。 Note: 如果管理伺服器是透過其他管理伺服器進行複寫，則請確定您升級 SEPM 以及停止管理伺服器服務期間未進行複寫。請參閱： Note: 防止在升級期間複寫
步驟 4：升級 Symantec Endpoint Protection Manager 軟體	在網路中的所有網站上安裝 Symantec Endpoint Protection Manager 的新版本取代現有版本。這會自動偵測現有版本，並且在升級時儲存所有的設定。請參閱： • 升級管理伺服器 • 安裝 Symantec Endpoint Protection Manager 如果您已在升級之前透過 SES 雲端伺服器 (混合管理) 註冊 Symantec Endpoint Protection Manager，則網域在升級程序期間會保持已註冊狀態。您也可以在此升級之後註冊任何網域。請參閱： 在 Symantec Endpoint Protection Manager 的雲端主控台中註冊網域

工作	說明
步驟 5：升級 Symantec 用戶端軟體	在安裝新版本之前，無需解除安裝以前的用戶端。超額安裝程序儲存用戶端設定，然後將用戶端升級到最新版本。您應該先更新測試電腦數量較少的群組，然後再更新整個生產網路。 如果您使用用戶端作為群組更新提供者，則必須先將它們升級。請參閱： 升級群組更新提供者 請檢閱下列各主題中的適用步驟： • 準備用戶端安裝 • 準備 Windows 和 Mac 電腦進行遠端部署 然後從升級用戶端的可用方法之一中選擇： • 自動升級：自動升級是群組更新 Windows 和 Mac 用戶端軟體最簡單的方法。您可以手動或透過使用「使用套件升級用戶端」精靈將用戶端套件指派給管理伺服器中的群組。您不需要執行進一步動作即可完成升級程序。請參閱： 使用自動升級來升級用戶端軟體 自動升級不支援 Symantec Agent for Linux 14.3 RU1。 • 安裝檔案：從 Broadcom 下載中心 下載用戶端安裝檔案。 如需連結和資訊，請參閱： 下載最新版本的賽門鐵克軟體 • 用戶端部署精靈：在管理伺服器中執行「用戶端部署」精靈。此精靈會引導您建立用戶端套件，而用戶端套件可以透過網路連結和電子郵件或遠端推送進行部署，或是儲存以供稍後執行本機安裝之用。您也可以使用第三方工具進行部署。請參閱： 選擇使用用戶端部署精靈安裝用戶端的方法

Endpoint Protection 14.x 的升級最佳實務準則

升級時，請遵循建議的最佳實務，並瞭解任何潛在問題和風險。

下列資源可協助您規劃和執行對目前 Symantec Endpoint Protection 版本 (SEP) 的最佳升級：

- [升級至最新版本的好處](#)
- [最新版本的重要資訊](#)
- [開始前必知事宜](#)
- [最佳實務準則](#)
- [常見問題 \(FAQ\)](#)

升級至最新版本的好處

若要取得最新的安全性功能、作業系統支援和客戶修正，請升級至最新版本。如需每個版本所具備功能的相關資訊，請參閱：

[Symantec Endpoint Protection \(SEP\) 14.x 所有版本的新功能](#)

最新版本的重要資訊

Table 32: 最新版本的重要資訊

系統需求和版本說明	請在升級前仔細檢閱下列資訊： Symantec Endpoint Protection 和 Endpoint Security 的版本、系統需求、發行日期、附註和修正 升級之前，請使用 Symantec Diagnostic Tool 來判斷電腦是否符合最低系統需求。請參閱： 下載 SymDiag 以偵測產品問題 如果您打算升級作業系統，請確定先將 Symantec Endpoint Protection 升級到支援該作業系統的版本。升級作業系統時保留不受支援的 Symantec Endpoint Protection 版本會導致非預期的結果。
支援和不支援的升級路徑	確定目前安裝的版本可以移轉或升級至新版本。檢閱下列資訊： • 最新版本 Symantec Endpoint Protection 支援和不支援的升級路徑
安裝和升級的重要資訊	• 當您從 Symantec Endpoint Protection Manager 內嵌資料庫升級到預設 Microsoft SQL Server Express 資料庫 (14.3 RU1 和更新版本) 時，可能會出現下列錯誤：##### 若要解決此問題，請參閱：將 SEPM 內嵌資料庫升級到 14.3 RU1 時，請參閱錯誤「指定的密碼不符合強式密碼需求」 • 14.3 RU1 MP1 或更舊版本的 Symantec Endpoint Protection Manager 無法管理 Symantec Endpoint Protection 14.3 RU2 用戶端。 • 對於升級至 14.3 RU1 或更新版本，預設 Microsoft SQL Server Express 資料庫會取代內嵌資料庫。最大資料庫大小為 10 GB。 • 對於升級至 14.2 或更新版本，如果已變更某些預設名稱，則防火牆政策無法納入 IPv6 的變更。預設名稱包括預設政策的名稱和預設規則名稱。如果無法在升級期間更新規則，則不會出現 IPv6 選項。您在升級後建立的任何新政策或規則不受影響。 如有可能，請將任何變更的名稱還原回預設名稱。否則，請確保您新增至預設政策的任何自訂規則不會以任何方式攔截 IPv6 通訊。請確保針對您新增的任何新政策或規則相同。 這些動作可預防任何 IPv6 通訊問題。 • 如果網路僅使用 IPv6 通訊，則無法將舊版 Symantec Endpoint Protection 用戶端升級至 14.2 版或更新版本。在此環境中，舊版用戶端是早於 14.2 版的 Symantec Endpoint Protection 用戶端。這些更早版本用戶端不支援 IPv6 通訊，因此升級可能會導致 Symantec Endpoint Protection Manager 通訊問題。 將環境移至純 IPv6 網路之前，先將用戶端升級至 14.2 版或更新版本。或者，解除安裝舊版，然後將新的 14.2 或更新版本套件部署到這些用戶端電腦。 • 如果 Symantec Endpoint Protection 使用 SQL Server 資料庫並且您的環境僅使用 TLS 1.2，請確保 SQL Server 支援 TLS 1.2。您可能需要修正 SQL Server。請參閱： Microsoft SQL Server 支援 TLS 1.2 此建議適用於 SQL Server 2008、2012 和 2014。 • 新的 Symantec Endpoint Protection Manager 安裝可在用戶端與管理主控台之間進行安全通訊。升級會維護目前的通訊組態。

開始前必知事宜

下表列出您應該在升級之前執行的建議例行維護工作。維護可能包括磁碟錯誤檢查、硬碟的磁碟重組，或其他例行健全狀況檢查。

Table 33: 建議的日常維護工作

磁碟空間不足	確保管理伺服器有足夠的磁碟空間來執行升級。為確保成功升級 Symantec Endpoint Protection Manager，可用空間應該至少是資料庫大小的三倍。請參閱系統需求以瞭解安裝 Symantec Endpoint Protection 用戶端所需的可用空間。請參閱： 升級前增加 Symantec Endpoint Protection Manager 可用磁碟空間。
代理伺服器	確保已對任何週邊防火牆或代理進行適當的排除，以確保與所有賽門鐵克伺服器成功通訊。請參閱： Symantec Endpoint Protection (SEP) 所需的外部 URL

掃描排除	在您部署用戶端升級前，可能需要建立其他掃描排除。請參閱： • 哪些掃描排除應套用到所有 Windows 叢集伺服器節點？ • 關於 Microsoft Exchange 伺服器和賽門鐵克產品的檔案和資料夾自動排除 • 虛擬化的最佳實務準則 • 從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險
升級的步驟	如需升級 Symantec Endpoint Protection 的一般資訊，請參閱： 升級和移轉到最新版本的 Symantec Endpoint Protection (SEP)
升級不受支援的語言	從不受支援的語言升級 SEPM 時，SEPM 會自動升級為英文 (14.3 RU2 和更新版本)。 如果您要升級為其他支援的語言 (例如，從義大利文到法文)，則請在升級之前參閱： 將 Symantec Endpoint Protection Manager 14.3 RU2+ 升級為支援的語言 若要在 Windows 用戶端上升級不受支援的語言，請參閱： 使用自動升級來升級用戶端軟體 Symantec Endpoint Protection Manager (SEPM) 和用戶端翻譯成下列語言： • 在 14.3 RU2 和更新版本中：英文、巴西葡萄牙文、法文、日文和西班牙文。 • 在 14.3 RU4 和更新版本中：簡體中文和繁體中文。 • 在 14.3 RU5 和更新版本中：捷克文、波蘭文和俄文。

最佳實務準則

Table 34: 最佳實務準則

在升級前備份	最佳實務準則是，始終在升級前備份 Symantec Endpoint Protection Manager 資料庫。請參閱： 備份資料庫和日誌
自動升級	使用「使用套件升級用戶端」精靈來升級現有 Windows 和 Mac 用戶端。 由於可能的頻寬使用量，您可能想要排程在營業時間後執行自動升級。您可以在 Web 伺服器上暫存用戶端套件，然後執行「使用套件升級用戶端」。也有部署升級套件的替代方法，例如透過「用戶端部署精靈」。請參閱： 使用自動升級來升級用戶端軟體
Symantec Endpoint Protection Manager 的全新安裝	您可以使用通訊更新套件將現有用戶端連線至新安裝的 Symantec Endpoint Protection Manager。例如，如果您解除委任現有伺服器，然後改為將 Symantec Endpoint Protection Manager 安裝到新伺服器。建立重設用戶端-伺服器通訊設定的新用戶端安裝設定，然後以與用戶端相同的方式部署「通訊更新套件」：「說明 > 「開始使用」頁面 > 在您的電腦上安裝用戶端軟體」。 您也可以使用用戶端安裝設定重設 Mac 電腦的用戶端-伺服器通訊設定。 用戶端連線後，您可以使用自動升級來升級用戶端。請參閱： 關於 Windows 用戶端安裝設定
虛擬化	Symantec Endpoint Protection 用戶端可用於保護支援作業系統的虛擬實例。 可以在支援作業系統的虛擬實例上安裝和管理 Symantec Endpoint Protection Manager。Symantec Endpoint Protection 包括虛擬用戶端的其他管理選項，例如「共用智慧型掃描快取」和用於清除離線非持續 GVM 的獨立組態選項。請參閱： Symantec Endpoint Protection 中虛擬化的最佳實務準則
災難復原準備	在您開始升級前，請確保已使用災難復原準備技術備份目前的 Symantec Endpoint Protection Manager 安裝。如果升級失敗，您可以快速還原 Symantec Endpoint Protection Manager 的功能。 若要在失敗後復原安裝，由於資料庫綱要和其他變更，您必須使用先前使用的確切版本重新安裝。請參閱： 請參閱 Endpoint Protection 的災難復原最佳實務準則：

常見問題 (FAQ)

問：我從何處取得 Symantec Endpoint Protection 的最新版本？

答：從「Broadcom 支援入口網站」。請參閱下列頁面以取得指南：

[下載最新版本的賽門鐵克軟體](#)

聯絡技術支援，以取得其他協助：

[Symantec Endpoint Security](#)

問：如何啟用我的授權？

答：登入 Symantec Endpoint Protection Manager 後，按一下「所需工作」下的「說明」>「入門指南」頁面。

問：升級方法是什麼？使用各種方法的時機是什麼？

答：有許多方法可用來升級用戶端。其次，決定哪個方法最適用於這種情況。每種情況是不同的，因此賽門鐵克為完成此目標提供了許多不同的方法：

- 自動升級：手動或透過使用「使用套件升級用戶端」精靈將用戶端套件指派給管理主控台中的群組。
- 從安裝檔案或安裝媒體進行本機安裝。
- 從管理主控台執行用戶端部署精靈。用戶端部署精靈引導您建立用戶端套件。然後您可以選擇透過電子郵件將 Web 連結傳送給使用者或透過遠端推送進行部署。您也可以儲存本機安裝的套件或使用第三方部署工具。

在開始前，請確保用戶端電腦已準備好接收升級套件。請參閱：

[管理 Symantec Endpoint Protection 用戶端安裝](#)

問：建議的移轉順序是什麼？在環境中我首先升級什麼？

答：建議的升級順序如下：

1. Symantec Endpoint Protection Managers
2. 群組更新提供者
3. 剩餘的用戶端 (根據需要)

問：如何產生環境中所安裝的 **Symantec Endpoint Protection** 版本清單？

答：使用「報告」可產生此清單。請參閱：

[產生網路中安裝的 Symantec Endpoint Protection 版本的清單](#)

問：若我的 **Symantec Endpoint Protection** 版本已達到「服務終止」(EOS) 會怎樣？

答：若您的 Symantec Endpoint Protection 版本不再受到支援，您應該升級到更新版本。如需有關哪些版本已達到 EOS 的資訊，請參閱：[產品生命週期 - 網路安全軟體](#)

Symantec Endpoint Protection 的升級資源

Table 35: 升級資源

項目	資源
用戶端安裝套件設定和功能	您可以透過各種不同的設定和防護功能架構用戶端安裝套件。請參閱： • Symantec Endpoint Protection 功能 (依平台分類) • 關於 Windows 用戶端安裝設定 • 選擇要在用戶端上安裝哪些安全性功能
功能和政策敘述	如需詳細資訊，請參閱： • Symantec Endpoint Protection 技術如何保護您的電腦 • 安全政策類型
功能相依性	如需詳細資訊，請參閱： Windows 用戶端的 Symantec Endpoint Protection 功能相依性
管理產品授權	Symantec Endpoint Protection 是根據保護站台中電腦所需的用戶端數目進行授權。請參閱： Symantec Endpoint Protection 產品授權需求

項目	資源
其他資源	請參閱下列文章： - Endpoint Protection 14.x 的升級最佳實務準則 - 下載最新版本的賽門鐵克軟體 - 所有 Endpoint Protection 版本的版本說明、新修正和系統需求

更多資訊

[升級至新版本](#)

以 Microsoft Azure Code Signing (ACS) 支援升級 Windows 用戶端電腦至 14.3 RU8 及更新版本

了解 Symantec 採用 Microsoft Azure Code Signing 的原因，以及對 14.3 RU8 及更新版本升級或安裝有何影響。

升級或安裝 Symantec Endpoint Protection 14.3 RU8 時，用戶端使用者可能會看到以下錯誤訊息：Symantec Endpoint Protection ##### Azure Code Signing ##### Windows #####

此訊息的出現原因為 Symantec Endpoint Protection 安裝程式偵測到電腦未執行支援 Microsoft Azure Code Signing 的 Microsoft Windows 版本。Symantec Endpoint Protection 用戶端將攔截 14.3 RU8 及更新版本的用戶端安裝，直到電腦安裝 ACS 支援。

什麼是 Microsoft Azure Code Signing，Symantec 為什麼採用？

Microsoft 協助開發人員使用其工具集，透過 Azure Code Signing 安全地建置和派送應用程式。ACS 會建立應用程式發行者的身分，以及自發行以來未經修改的完整性。

Microsoft 要求安全廠商使用 ACS 來簽署二進位檔。用戶端電腦作業系統上必須有 ACS 支援，才能順利執行 Symantec Endpoint Protection 用戶端。Symantec Endpoint Protection 用戶端 14.3 RU8 具有使用 Microsoft Azure Code Signing 基礎架構簽署的二進位檔。Symantec Endpoint Protection 在安裝或升級之前，請檢查作業系統是否已支援 ACS。若尚無支援，則需[安裝 ACS 支援](#)或升級至 Windows 10 21H2 或更新版本。

NOTE

升級至 14.3 RU8 或更新版本之前，14.3 RU7 和更舊版本的用戶端電腦不會受影響。

更多資訊：

- [Azure Code Signing，促進開發人員和消費者的信任](#)
- [KB5022661 - Windows 對 Azure Code Signing 程式的支援](#)

在用戶端電腦上安裝 ACS 支援

Microsoft 自動包括對 Windows 10 21H2 的 ACS 支援，但不包括對 Windows 10 21H1 及更早版本的支援。

在 Symantec Endpoint Protection 用戶端電腦上安裝 ACS 支援

- 檢查哪些用戶端電腦執行 Windows 10 21H1 或更早版本。
- 執行下列其中一項工作：
 - 升級用戶端電腦，以執行包括 ACS 支援的 Windows 10 21H2 或更新版本。
 - 為每台用戶端電腦執行的[作業系統手動安裝](#) Microsoft 安全更新。
- 重試 Symantec Endpoint Protection 用戶端升級。

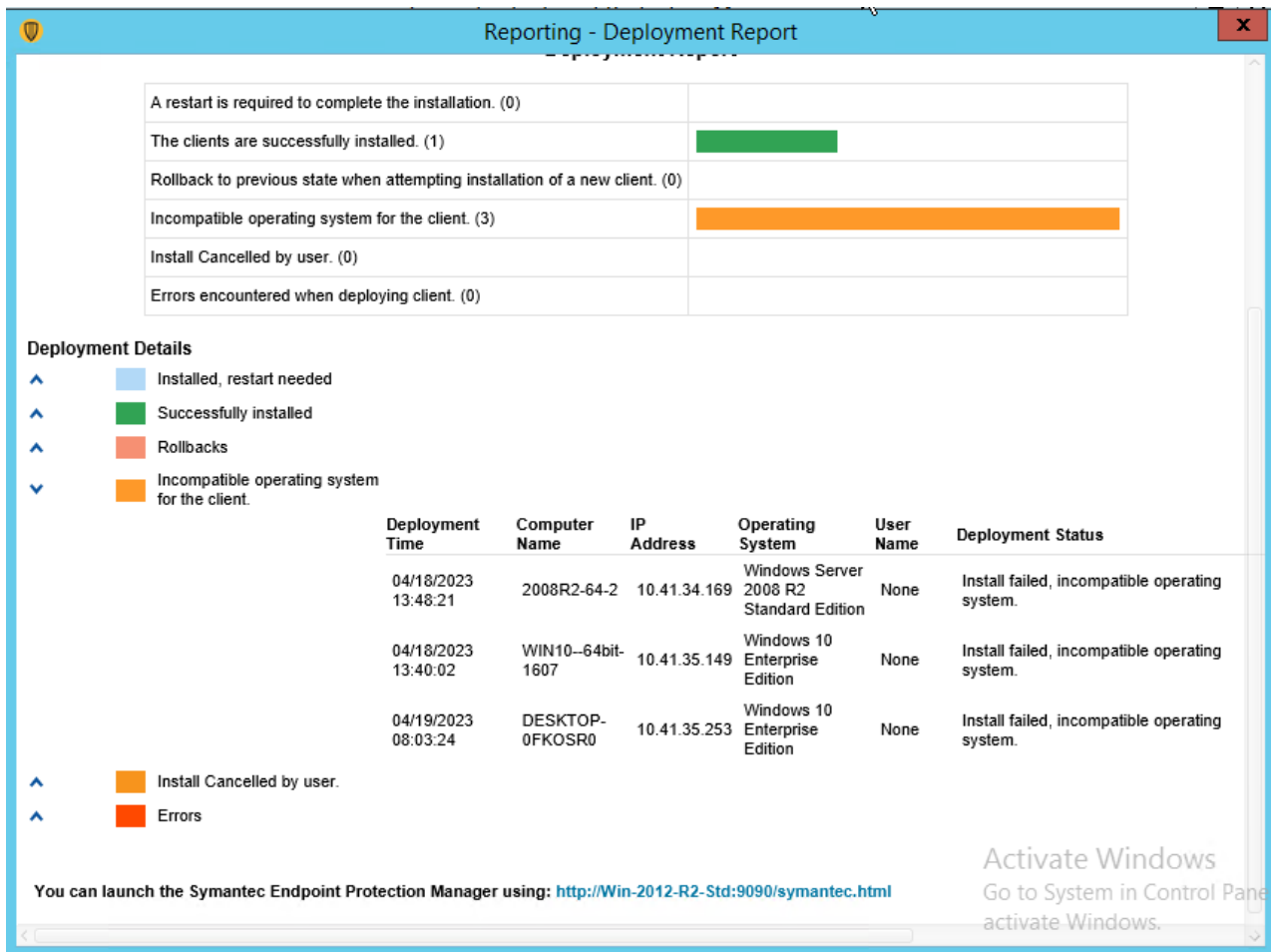
檢查支援和不支援 ACS 的用戶端電腦

您可以在內部部署 Symantec Endpoint Protection Manager (SEPM) 或 Symantec Endpoint Security (SES) 雲端主控台上找到哪些用戶端電腦已經安裝 ACS 支援。

在 Symantec Endpoint Protection Manager 中：

使用以下任何方法。

- 在主控台中，建立部署狀態的快速報告。在「部署狀態」欄，尋找具以下狀態的用戶端：#####



如需詳細資訊，請參閱：[執行有關用戶端部署狀態的報告](#)

- 在「電腦狀態」日誌中，在「作業系統」欄中尋找以下狀態的項目：#####

Symantec Endpoint Protection Manager

Summary Logs Command Status

Computer Status Logs

<< Back

Export Details

Command: Scan

Computer	IP Address
WIN-7-x64	10.41.34.167
DESKTOP-0FKOSR0	10.41.35.253
2008R2-64-2	10.41.34.169
WIN10--64bit-1607	10.41.35.149

Reporting - Detailed Computer Information

Threat Defense for Active Directory status: Not reporting status

Threat Defense for Active Directory message:

Web and Cloud Access Protection Status: Disabled

Web and Cloud Access Protection Message:

IPS Out-of-band Scanning Status: Not installed

Restart required: Yes

Restart reason:

Deployment status: Install failed, incompatible operating system.

Deployment message: Symantec Endpoint Protection can only be installed on systems with Azure Code Signing support. Please install the latest Windows Quality Rollup package.

Deployment previous version:

Deployment target version: 14.3.21772.8000

Deployment running version:

Time deployed: 04/18/2023 13:48:21

Install type: Standard

Infected: No

Worst detection: No detections

Attribute Extension:

Last virus time: Never

Last scan time: Never

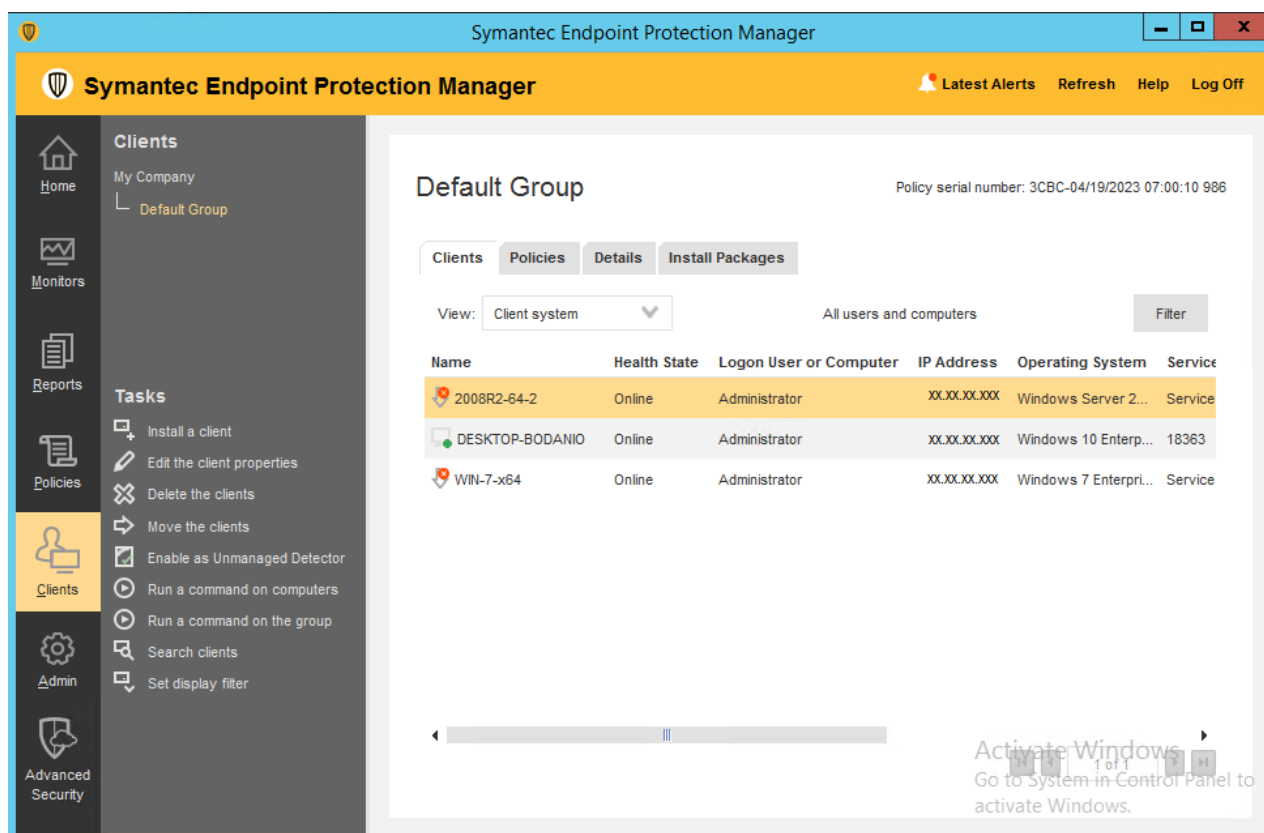
Time of last full LiveUpdate session: Never

Endpoint Detection and Response Status: No status reported

Entries 1 to 4 of 4

如需詳細資訊，請參閱：[執行和自訂快速報告](#)

- 在主控台中，按下「用戶端」>「用戶端」。在「名稱」欄中，尋找具代表安裝失敗紅色圖示的用戶端。



如需詳細資訊，請參閱：[檢查用戶端是否已連線至管理伺服器且受保護](#)

在 **Symantec Endpoint Security** 雲端主控台中：

- 在雲端主控台中的「裝置」頁面 > 「裝置群組」標籤上，選取「活動記錄」標籤。在「說明」欄中，尋找具有下列狀態的任何裝置：

```

- #####
- LiveUpdate #####
- #### LiveUpdate # Symantec Endpoint Protection WIN64 ###

```

在 **Symantec Endpoint Protection** 用戶端中：

- 在 Symantec Endpoint Protection 用戶端系統日誌中，尋找下列錯誤訊息：
Symantec Endpoint Protection ##### Azure Code Signing ##### Windows ###
###

支援 ACS 的 Windows 作業系統

Microsoft 對執行 Symantec Endpoint Protection 用戶端的多數 Windows 作業系統皆有安全更新。

下表所列作業系統版本開始，皆有提供對 Azure Code Signing 的支援。選擇 **KB 數** 並下載網路中每個受影響用戶端電腦的安全更新，以順利 Symantec Endpoint Protection 安裝或升級用戶端 14.3 RU8 和更新版本。

NOTE

如果您的作業系統未列在下表中，請聯絡 Microsoft。

Table 36: 具有原生 ACS 支援或更新的 Windows 作業系統

作業系統	KB 數
Windows Server 2022	5005619
Windows Server 2019	5005625
Windows Server 2016	5022661
Windows Server 2012 R2	5006729
Windows 11 22H2 ARM Windows 11 22H2 Windows 11 21H2 Windows 11 21H1	不需要；ACS 支援原生於作業系統。
Windows 10 22H2 Windows 10 21H2	不需要；ACS 支援原生於作業系統。
Windows 10 21H1 Windows 10 20H2 Windows 10 2004	5005611
Windows 10 1909	5005624
Windows 8.1	5006714

NOTE

Microsoft 不針對 Windows 7/Windows 8/Windows Embedded 提供 ACS 更新。從 2023 年 9 月 26 日開始，Symantec 內容更新不再使用 SHA-1 憑證簽署，這會影響 Windows Vista/Windows 7/Windows Server 2008/Windows 2008 R2。日

如需更多詳細資訊，請參閱：[Windows Vista、7、Server 2008 和 2008 R2 的 Endpoint Protection 內容傳送變更](#)

手動安裝 ACS 的 Microsoft 安全更新

若用戶端電腦未設定為自動安裝安全更新，則您必須手動安裝 Microsoft 服務堆疊更新，然後再安裝包括 ACS 支援的 Microsoft 安全更新。

NOTE

用戶端電腦也必須具安裝在憑證存放區 (受信任的根 CA 清單) 的 [Microsoft 身分驗證根憑證授權單位 2020](#) 憑證授權單位。若電腦可以存取網路且啟用 Windows 更新，則應自動下載此憑證授權單位。

步驟 1：安裝 Microsoft 服務堆疊更新

用戶端使用者安裝 Windows 安全更新後，可能會看到一則訊息，說明該更新不適用於他們的作業系統。若未安裝正確的 Windows 服務堆疊更新，就會出現此訊息。若 C:\Windows\SoftwareDistribution\Download 資料夾的內容過大，也會顯示此訊息。

若看到此訊息，則您必須先安裝最新的 Microsoft 服務堆疊更新，才能安裝 ACS 安全更新。

如需詳細了解服務堆疊更新，請參閱：

- [服務堆疊更新](#)
- [Windows 更新疑難排解](#)

步驟 2：安裝 Microsoft 安全更新

1. 從 Microsoft KB 安全更新頁面中，下載與每台用戶端電腦的作業系統相關聯的安全更新。
如需詳細資訊，請參閱：

2. 安裝此安全更新。

最新版本 Symantec Endpoint Protection 支援和不支援的升級路徑

通常，對於低於最新版本的 Symantec Endpoint Protection 版本，清單上位於它之前的每個版本都受支援。不過，您應該參考特定版本的版本說明進行確認。請參閱：

[發佈 Endpoint Security 及所有 Endpoint Protection 版本的版本、附註、新修正及系統需求](#)

另請參閱：[Endpoint Protection 14.x 的升級最佳實務準則](#)

Symantec Endpoint Protection Windows 用戶端

下列版本的 Symantec Endpoint Protection Windows 用戶端版本可以直接升級至目前版本：

- 14.x、14.2.x 和 14.3.x 的所有版本

Symantec Endpoint Protection Mac 用戶端

下列版本的 Symantec Endpoint Protection Windows 用戶端版本可以直接升級至目前版本：

- 14.x、14.2.x 和 14.3.x 的所有版本 (尚未發行 14.3 RU7)。
適用於 Mac 的 Symantec Endpoint Protection 用戶端未針對 14.0.1 MP2 進行更新。

Symantec Single Agent for Linux

NOTE

自 14.3 版 RU1 起，Linux 用戶端安裝程式會偵測並解除安裝舊版 Linux 用戶端，然後執行新用戶端的全新安裝。不會保留舊組態。

下列適用於 Linux 的 Symantec Endpoint Protection 用戶端版本可以直接升級至目前版本：

- 14.x、14.2.x 和 14.3.x 的所有版本 (尚未發行 14.3.7)。

在 14.3 RU1 中，適用於 Linux 的 Symantec Endpoint Protection 用戶端已改名為 Symantec Single Agent for Linux。

如果您有版次號碼，但不確定如何轉換為發行版本，請參閱：

[關於 Endpoint Protection 發行類型和版本](#)

不支援的升級路徑

您無法從所有賽門鐵克產品移轉到 Symantec Endpoint Protection。您必須先移除下列產品，然後再安裝 Symantec Endpoint Protection 用戶端。

- 降級路徑不受支援。例如，若要從 Symantec Endpoint Protection 14.3 RU8 移轉至 14.3 RU7，則必須首先解除安裝 Symantec Endpoint Protection 14.3 RU8。
- 14.3 RU6 及更新版本不支援 32 位元作業系統。將電腦升級到 64 位元作業系統或安裝 32 位元作業系統的 14.3 RU5。
- 14.0.x 已捨棄對 Windows XP、Server 2003，以及基於 Windows XP 的任何 Windows Embedded 作業系統的支援。Symantec Endpoint Protection Manager 14.2 RU1 可以管理這些電腦作為舊版 12.1.x 用戶端，儘管 12.1.x 用戶端是 EOL。對於這些用戶端，您可能想要使用仍然支援這些舊版作業系統的賽門鐵克產品，如 Data Center Security (DCS)。
- 所有賽門鐵克諾頓產品
- Symantec Endpoint Protection for Windows XP Embedded 5.1

Symantec Endpoint Security 雲端主控台的支援路徑

針對混合管理：

- *Symantec Endpoint Protection Manager*：Symantec 建議使用最新版本，但最低 14.3 MP1 (14.3.1169.0010)。
- *Symantec Endpoint Protection* 用戶端：14.3 MP1 (14.3.1169.0010) 或更新版本。用戶端執行於 Windows Server 2008 R2 或更新版本，而非執行於 Windows Server 2008 RTM/SP1/SP2。

請參閱：[移轉至 SES 雲端主控台](#)

升級前增加 Symantec Endpoint Protection Manager 可用磁碟空間

Symantec Endpoint Protection Manager 安裝需要最低可用磁碟空間量。請確定任何目前版本伺服器或新硬體符合最低硬體需求。不過，升級時可能需要額外的可用磁碟空間才能建立暫存檔。

進行架構變更之前對資料庫進行備份。請參閱：

[備份資料庫和日誌](#)

Table 37: 增加管理伺服器上磁碟空間的工作

工作	說明
變更 LiveUpdate 設定以降低空間需求	1. 移至「管理員 > 伺服器」，並在「本機網站」上按下滑鼠右鍵。選取「編輯網站屬性」。 2. 在 LiveUpdate 標籤上，減少要保留的內容修訂數量。對於升級，您可以將設定減少為 10。讓 Symantec Endpoint Protection Manager 有時間清除額外的修訂。不過，減少修訂數量可能會觸發從登入的用戶端下載完整更新。這些完整更新要求增加可能會對電腦效能產生負面的影響。 Note: 升級完成後不需要將修訂設定恢復為先前的值。Symantec Endpoint Protection Manager 儲存與管理內容的方式有所改善，與舊版本相比，耗用的磁碟空間更少，同時可容納的修訂更多。 如需詳細資訊，請參閱： • 如何更新用戶端上的內容和定義檔 • 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager
確定從 Symantec Endpoint Protection Manager 資料庫刪除未使用的病毒定義檔	1. 移至「管理員 > 伺服器」，在資料庫伺服器上按下滑鼠右鍵，然後選取「編輯資料庫屬性」。資料庫名稱為 SQLEXPRESSSYM (14.3 RU1 及更晚) 或 localhost (14.3 MPx 及更舊版本)。對於 Microsoft SQL Server 資料庫，資料庫伺服器名稱會根據資料庫位置有所不同。 2. 在「日誌設定」標籤上的「風險日誌設定」下，確定已勾選「刪除未使用的病毒定義檔」。
重新定位或移除共存的程式和檔案	• 如果其他程式與 Symantec Endpoint Protection Manager 安裝於同一台電腦，請考慮將它們重新定位至其他伺服器。您可以移除未使用的程式。 • 如果佔用儲存較多的程式與 Symantec Endpoint Protection Manager 安裝於同一台電腦，請考慮使一台專用電腦僅支援 Symantec Endpoint Protection Manager。 • 移除任何暫存 Symantec Endpoint Protection Manager 檔案。 Note: 移除程式和檔案之後，對硬碟進行磁碟重組。
使用外部資料庫	如果 Symantec Endpoint Protection 資料庫與 Symantec Endpoint Protection Manager 位於同一台電腦，請考慮在另一台電腦上安裝 Microsoft SQL Server 資料庫。會節省大量的磁碟空間，而且大多數情況下可提高效能。請參閱： 關於選擇資料庫類型

NOTE

升級之前，請確定用戶端電腦也有足夠的磁碟空間。檢查系統需求，並視需要移除不需要的程式和檔案，然後對用戶端電腦硬碟進行磁碟重組。請參閱：

[Symantec Endpoint Protection Manager 上的磁碟空間不足](#)

升級管理伺服器

升級任何用戶端前，必須先升級所有管理伺服器。

在支援負載平衡、容錯移轉或複寫的環境中升級管理伺服器時，必須按照特定順序準備和升級管理伺服器。

WARNING

您必須按照適用於您的安裝類型的方案操作，否則升級可能會失敗。

Table 38: 升級工作

工作	說明
升級和架構管理伺服器	步驟 1：檢閱系統需求和支援的升級路徑、升級管理伺服器，然後使用「管理伺服器組態精靈」進行架構。 Symantec Endpoint Protection Manager 升級適用下列幾點： - 不再支援 Windows Server 2008、所有桌上型電腦作業系統和 32 位元作業系統。 - 檢查是否支援您的 SQL Server 版本。 Symantec Endpoint Protection (SEP) 14.3 RU10 的系統需求 支援升級到最新版本的 Symantec Endpoint Protection 14.x 的路徑 - 升級後，您不需要重新啟動管理伺服器電腦，但是這麼做時可提升效能。 步驟 2：安裝和架構 Symantec Endpoint Protection Manager 安裝 Symantec Endpoint Protection Manager 架構 Symantec Endpoint Protection Manager 安裝 Note: 您可能需要編輯網域安全性政策，以允許虛擬服務帳戶在 Windows 7 / Server 2008 R2 或更新版本上正確執行。請參閱：在安裝或架構期間發生錯誤：「...服務需要使用者權限」或「...無法讀取使用者權限」
登入管理伺服器	出現 Symantec Endpoint Protection Manager 登入畫面時，您可以使用您的登入認證登入主控台。請參閱： 登入 Symantec Endpoint Protection Manager 主控台

更多資訊

- [設定容錯移轉和負載平衡](#)
- [設定站台和複寫](#)

從內嵌資料庫升級到 Microsoft SQL Server Express 資料庫的最佳實務

在 14.3 RU1 中，與 Symantec Endpoint Protection Manager (SEPM) 一起安裝的預設資料庫已從內嵌資料庫變更為 Microsoft SQL Server Express 2017 資料庫。第一次使用「管理伺服器組態精靈」中的預設組態升級或安裝管理伺服器時，SQL Server Express 資料庫會自動進行安裝並取代內嵌資料庫。

升級到版本 14.3 RU1 或更新版本時，管理伺服器電腦必須滿足某些需求，否則管理伺服器升級無法繼續。如果遇到這些問題，「管理伺服器組態精靈」會通知您，並為您提供修復它們的機會。

升級前必知事宜

升級前，請檢查您在安裝前可能需要修正的以下問題。

Table 39: 在升級之前修正問題

問題	說明
資料庫大小不足	對於資料檔案和日誌資料，SQL Server Express 資料庫具有 10 GB 的容量上限。Symantec Endpoint Protection Manager 會在安裝開始前備份內嵌資料庫。如果該備份大於 10 GB，升級無法繼續。在開始升級之前或升級期間，您必須減少資料量。當資料庫太大時，「管理伺服器組態」精靈會通知您。 如果在開始安裝之前資料庫超過 10 GB，請執行以下工作： 在升級到 Microsoft SQL Server Express 之前，當資料庫已滿時減小資料庫大小 Microsoft SQL Server Express 資料庫和 Microsoft SQL Server 資料庫兩者都會使用稱為 FILESTREAM 的功能，來減少資料庫大小。如果在升級期間發現資料庫太大或即將過大，您可以執行以下動作： 為 Microsoft SQL Server 資料庫啟用 FILESTREAM Note: 如果您使用 SQL Server 資料庫，請定期檢查資料庫大小，以確保資料庫未達到其大小的上限。請參閱： 增加 Microsoft SQL Server 資料庫檔案大小
磁碟空間不足	確保管理伺服器電腦上至少有 10 GB 的可用磁碟空間來執行升級。請參閱： 挪出更多的可用磁碟空間以升級到預設 Microsoft SQL Server Express 資料庫
Symantec Endpoint Protection Manager 未與資料庫通訊	Symantec Endpoint Protection Manager 會使用憑證驗證 Symantec Endpoint Protection (SEPM) 與 Microsoft SQL Server Express 或 SQL Server 資料庫之間的通訊。您必須產生憑證並將其匯入至 Symantec Endpoint Protection Manager 電腦，SEPM 才能連接到 SQL Server 資料庫。如果憑證不存在、過期或即將到期，則 SEPM 和資料庫之間的連線會失敗。請參閱： 架構 Symantec Endpoint Protection Manager 與 Microsoft SQL Server 之間的加密通訊 若要檢查管理伺服器是否連接到資料庫，請參閱： 驗證管理伺服器與資料庫的連線
疑難排解升級到 Microsoft SQL Server Express 的問題	升級時可能發生以下其中一個問題： - Windows 更新過期或 Windows 更新服務未執行。若要疑難排解此問題，請取消 SEPM 安裝、執行最新更新或重新啟動 Windows 更新服務、重新啟動電腦，然後繼續 Symantec Endpoint Protection Manager 安裝。 - SQL Server Express 資料庫未安裝。若要疑難排解，請檢閱資料庫日誌。請參閱： 疑難排解 Endpoint Protection Manager 的預設 SQL Server Express 資料庫的安裝問題 - Symantec Endpoint Protection Manager 與資料庫之間沒有連線。請參閱： 驗證管理伺服器與資料庫的連線 疑難排解 Symantec Endpoint Protection Manager 與主控台或預設資料庫之間的通訊問題 - 您可以變更在其上執行 Symantec Endpoint Protection Manager 之電腦的 IP 位址和主機名稱。請參閱： 在變更電腦的 IP 位址和主機名稱後重新架構 Symantec Endpoint Protection Manager

更多資訊

[備份資料庫和日誌](#)

在升級到 Microsoft SQL Server Express 之前，當資料庫已滿時減小資料庫大小

預設的 Microsoft SQL Server Express 資料庫對資料檔案和日誌資料的大小限制為 10 GB。當您從大於 10 GB 的內嵌資料庫進行升級，並在升級到 Microsoft SQL Server Express 的過程中時，升級程序無法繼續。

如果「管理伺服器架構精靈」偵測到資料庫太大，您可能會看到以下訊息：

```
SQL Server Express ##### 10 GB #####
```

當預設資料庫太大時，請暫停升級並執行以下步驟：

步驟 1：減少收集日誌的天數

在下列檔案中，減少天數：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\etc\conf.properties

- scm.sqlexpress.migration.otherlog.days=7
- scm.sqlexpress.migration.learnedapps.days=0
- scm.sqlexpress.migration.clientserveractivity.days=3
- scm.sqlexpress.migration.traffic.days=7
- scm.sqlexpress.migration.packet.days=7
- scm.sqlexpress.migration.security.days=7

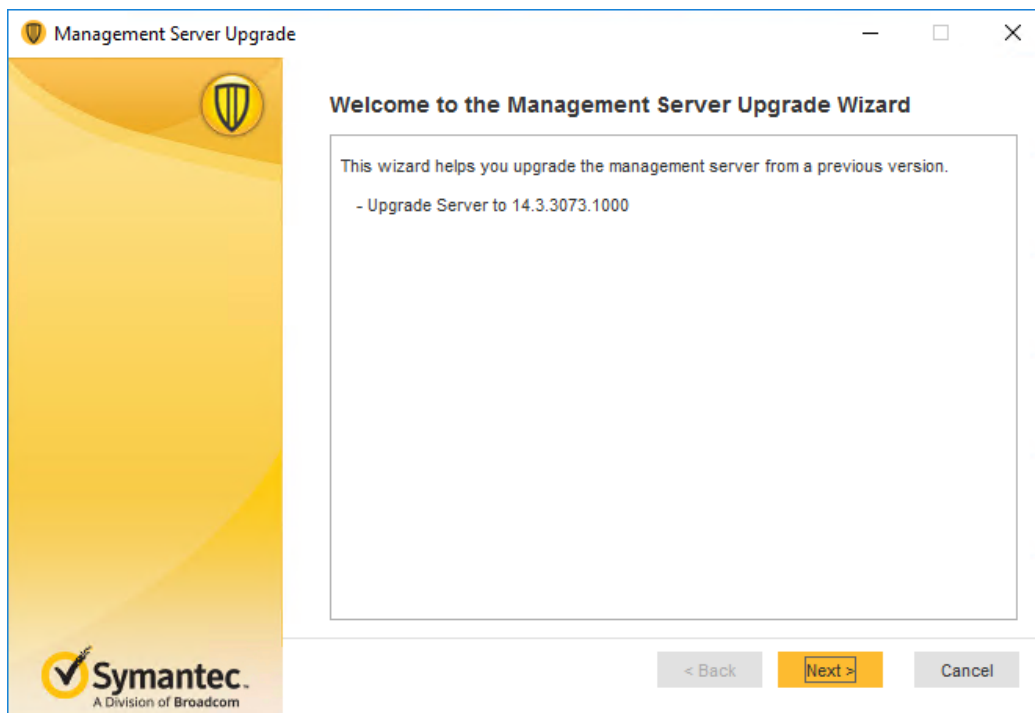
這會減少移轉到 SQL Server Express 資料庫的資料量。

NOTE

scm.sqlexpress.migration.clientserveractivity.days 已預設為 7，以將資料庫保持為較小的狀態。

步驟 2：重新啟動「管理伺服器升級精靈」

連按兩下 ..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat



NOTE

如果您在進行這些變更之前已啟動「資料庫備份和還原」對話方塊，請連按兩下 ..\Symantec\Symantec Endpoint Protection Manager\bin\dbtools.bat 來重新啟動它

更多資訊

在升級到 Microsoft SQL Server Express 之前，將資料庫大小減小到 10 GB 以下

為 Microsoft SQL Server 資料庫啟用 FILESTREAM

本主題說明如何為 Microsoft SQL Server 資料庫啟用 FILESTREAM。

Microsoft SQL Server 資料庫使用名為 FILESTREAM 的功能，來減小資料庫大小並提高資料庫效能。

- Microsoft SQL Server Express 資料庫具有 10 GB 的空間限制，並且需要啟用 FILESTREAM。如果您安裝自己的 SQL Server Express 實例，則必須啟用 FILESTREAM。
- 如果您從內嵌資料庫 (14.3 MP1 和更舊版本) 升級至 14.3 RU1 和更新版本，則不需要啟用 FILESTREAM；升級精靈或組態精靈會自動啟用 FILESTREAM。
- Microsoft SQL Server 資料庫不需要啟用 FILESTREAM，但建議使用它來改善效能。對於本機 SQL Server 資料庫，「管理伺服器升級和安裝精靈」可以為您啟用 FILESTREAM。對於遠端 Microsoft SQL Server 資料庫，您可以在安裝 SQL Server 資料庫的電腦上手動啟用 FILESTREAM。

如果您執行升級精靈或組態精靈，並出現下列訊息，則請按一下「是」，並啟用 FILESTREAM。

```
### Microsoft SQL Server ##### FILESTREAM ###
```

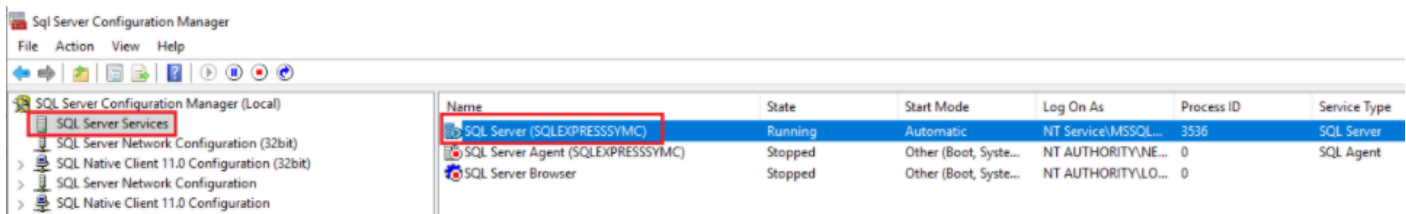
NOTE

如果您要繼續升級或安裝，而且目前不想要啟用 FILESTREAM 功能，則請按一下「否」。

如果您正在升級，則會關閉「管理伺服器升級精靈」。啟用 FILESTREAM 之後，您必須重新啟動升級精靈以繼續進行管理伺服器升級。在 Symantec Endpoint Protection Manager 電腦上，按一下：..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat。

手動啟用 FILESTREAM

1. 在「開始」功能表上，展開 **Microsoft SQL Server**，然後按一下「**SQL Server 組態管理員**」。
2. 在服務的「**SQL Server 組態管理員**」清單中，選擇「**SQL Server 服務**」，然後找到要在其上啟用 FILESTREAM 的 SQL Server 實例。



3. 在該實例上按下滑鼠右鍵，再按下「內容」。
4. 在「**SQL Server 屬性**」對話方塊中，按下 **FILESTREAM** 標籤。
5. 選取「啟用 FILESTREAM 進行 Transact-SQL 存取」，然後按下「啟用 FILESTREAM 進行檔案 I/O 串流存取」核取方塊。
6. 按下「套用」>「確定」。
7. 透過選取 SQL Server 的實例並按下「重新啟動」，重新啟動 SQL Server 資料庫服務。

更多資訊

[FILESTREAM \(SQL Server\)](#)

在升級到 Microsoft SQL Server Express 之前，將資料庫大小減小到 10 GB 以下

預設的 Microsoft SQL Server Express 資料庫對資料檔案和日誌資料的大小限制為 10 GB。資料檔案包括安裝套件、病毒定義檔、政策、警示和已探索的應用程式等項目。從大於 10 GB 的內嵌資料庫 (14.3 MP1 及更舊版本) 進行升級時，升級到 SQL Server Express 的程序無法繼續。如果「管理伺服器組態精靈」偵測到資料庫太大，您可能會看到以下訊息：

The backup exceeds the allowed SQL Server Express 10 GB limit. You must first reconfigure the management server to import less data. Then run the restore again.

The estimated data in the embedded database exceeds the Microsoft SQL Server Express limit of 10 GB. To continue the upgrade, the wizard must first reduce the amount of data to less than 10 GB.

首先必須使用下列其中一個工作，減少現有內嵌資料庫中的空間：

- 按下「繼續」，以便「管理伺服器組態精靈」在升級程序開始時減少資料庫大小。
- 使用下列步驟，取消「管理伺服器組態精靈」、自行減少資料庫大小，然後重新啟動精靈。

手動減少可用的資料庫大小

1. 移除 Symantec Endpoint Protection Manager 不使用的任何複寫夥伴。

如需詳細資訊，請參閱：

[刪除站台](#)

2. 減少日誌和已探索之應用程式資料的大小。

如需詳細資訊，請參閱：

[指定日誌大小以及在資料庫中保留日誌項目的時間長度](#)

Database Properties for karin-2012\SQLEXPRESS\SYMCMC

General Log Settings Backup Settings

Specify the size of logs maintained in the database for the site.

Management Server Log Settings

System Administrative Log Limit:	10000	entries	Expires after:	60	days
System Client-Server Activity Log Limit:	10000	entries	Expires after:	60	days
Audit Log Limit:	10000	entries	Expires after:	60	days
System Server Activity Log Limit:	10000	entries	Expires after:	60	days

Client Log Settings

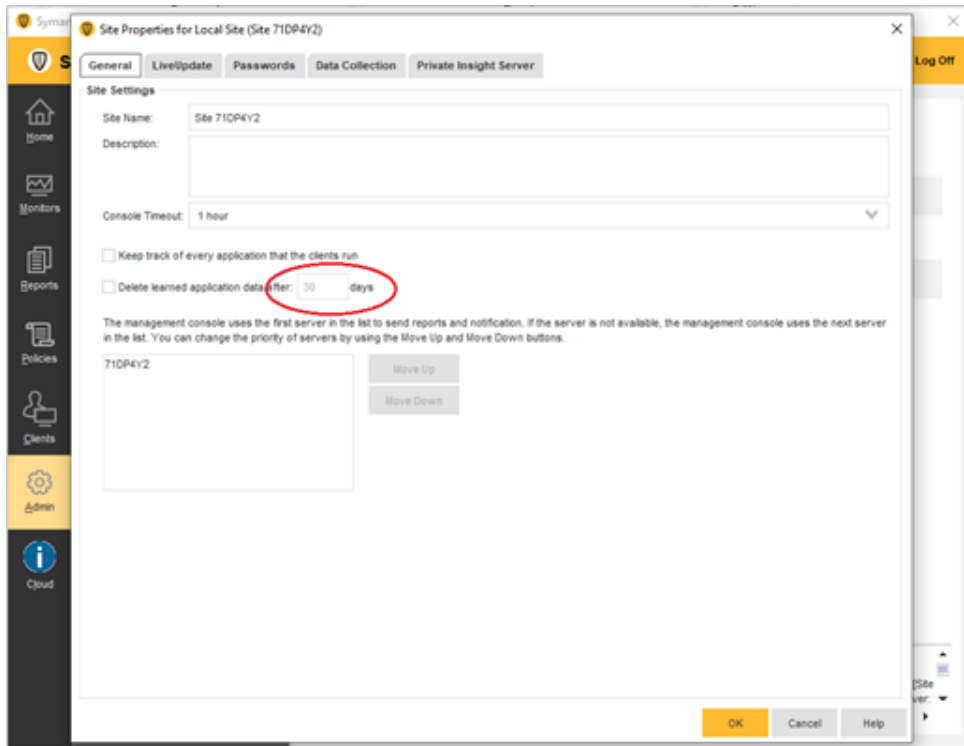
Client Activity Log Limit:	10000	entries	Expires after:	60	days
Security Log Limit:	10000	entries	Expires after:	60	days
Traffic Log Limit:	50000	entries	Expires after:	60	days
Packet Log Limit:	10000	entries	Expires after:	60	days
Control Log Limit:	20000	entries	Expires after:	60	days

Risk Log Settings

Delete risk events after:	60	days	Compress risk events after:	7	days
Delete acknowledged notifications after:	30	days	Delete unacknowledged notifications after:	30	days
Delete scan events after:	30	days	Delete commands after:	30	days

☒ Delete unused virus definitions ☒ Delete EICAR events

OK Cancel Help



3. 變更資料庫維護排程的預設設定。

- a. 停止管理伺服器。
- b. 在 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties 檔案中，減少下列項目的秒數。
`scm.timer.objectsweep=1800`
`scm.timer.objectsweep.delay=60`

NOTE

如果這些項目不在檔案中，則請新增它們。此步驟會增加資料庫將不需要的資料標示為已刪除的頻率。

如需詳細資訊，請參閱：

[Symantec Endpoint Protection Manager：如何排程「資料庫維護」？](#)

- c. 重新啟動管理伺服器並等待幾個小時或更長時間。請參閱：

[停止及啟動管理伺服器服務](#)

4. 排程所有合作夥伴之間的複寫至少發生一次。賽門鐵克建議您更頻繁地進行複寫。

如需詳細資訊，請參閱：

[將新站台以複寫夥伴的方式安裝到現有站台](#)

5. 在每次排程的複寫後等待幾個小時，然後再重新啟動升級。
6. 重新執行資料庫備份，然後嘗試將其還原。

挪出更多的可用磁碟空間以升級到預設 Microsoft SQL Server Express 資料庫

如果 Symantec Endpoint Protection Manager (SEPM) 電腦沒有至少 10 GB 的可用磁碟空間升級到 Microsoft SQL Server Express 資料庫，您可能會看到以下訊息：

```
The upgrade wizard cannot upgrade your embedded database to a Microsoft
SQL Server Express database. Either the destination drive does not
```

have enough available disk space, or the certificate is expired or will expire within 10 days. Make sure there is at least x of free disk space and that the certificate is current to continue.

除非挪出至少 10 GB 的可用磁碟空間，否則無法繼續升級程序。

NOTE

若憑證已到期或將在 10 天內到期，則 SEPM 會攔截升級。

增加磁碟空間

1. 移除未使用的檔案和暫存檔案。

Windows 暫存檔案位於：

- C:\Windows\Temp
- C:\Users\<username>\AppData\Local\Temp

如需詳細資訊，請參閱：

[Windows 10 中的磁碟清理](#)

2. 清空「資源回收筒」。
3. 如果前面的步驟沒有減少足夠的磁碟空間，請移除更多 SEPM 檔案。

- a. 使用 Run 指令停止管理伺服器服務：net stop semsrv

如需詳細資訊，請參閱：

[停止及啟動管理伺服器服務](#)

- b. 將以下 SEPM 檔案移到其他磁碟機：

- ..\Symantec\Symantec Endpoint Protection Manager\Inetpub\ClientPackages
- ..\Symantec\Symantec Endpoint Protection Manager\Inetpub\content
- ..\Symantec\Symantec Endpoint Protection Manager\data\backup
- ..\Symantec\Symantec Endpoint Protection Manager\data\inbox

- c. 重新啟動管理伺服器服務。

4. 變更資料庫備份設定。

- 確保「要保留的資料庫備份數目」選項設定為 1，這是預設值。
- 將「備份日誌」保持為未勾選狀態。

如需詳細資訊，請參閱：

[執行自動資料庫備份](#)

5. 將 Symantec Endpoint Protection Manager 未使用的檔案移到另一個磁碟機。

如果憑證過期，請參閱：

[架構 Symantec Endpoint Protection Manager 與 Microsoft SQL Server 之間的加密通訊](#)

架構 Symantec Endpoint Protection Manager 與 Microsoft SQL Server 之間的加密通訊

Symantec Endpoint Protection Manager 會使用憑證驗證 Symantec Endpoint Protection (SEPM) 與 Microsoft SQL Server Express 或 SQL Server 資料庫之間的通訊。您必須產生憑證並將其匯入至 Symantec Endpoint Protection Manager 電腦，SEPM 才能連接到 SQL Server 資料庫。如果憑證不存在、過期或即將到期，則 SEPM 和資料庫之間的連線會失敗。

如果尚未匯入憑證，可以安裝或升級管理伺服器 and SQL Server 資料庫。不過，管理伺服器組態精靈會偵測憑證是否過期還是在未來 30 天內到期。SEPM 每天會傳送通知，直到 30 天結束，提醒管理員匯入憑證。您可能會看到以下訊息：

```
### 30 ###Symantec Endpoint Protection Manager ##### Microsoft SQL Server ##### SQL
Server #####
```

NOTE

只有在 SEPM 和 SQL Server 共用相同的即將到期憑證時，您才需要使用下列步驟來更新 SEPM 憑證。

步驟 1：產生自我簽署憑證

如果您的組織還沒有憑證授權單位 (CA) 簽署的憑證，則您必須產生一個。具有正式 PKI 政策和程序的組織應該遵循其內部程序，以取得每個 Symantec Endpoint Protection Manager 的 CA 簽署的憑證。產生預設自我簽署 Symantec Endpoint Protection Manager (SEPM) 憑證並將其取代為 CA 簽署的憑證。

請參閱[使用簽署的憑證搭配 Endpoint Protection Manager](#) 的「產生憑證簽署要求」小節。

步驟 2：加構 SQL Server 的永久憑證

您必須為 SQL Server 資料庫引擎的實例啟用加密連線，並且必須使用 SQL Server Configuration Manager 來指定憑證。請參閱「架構伺服器」一節：

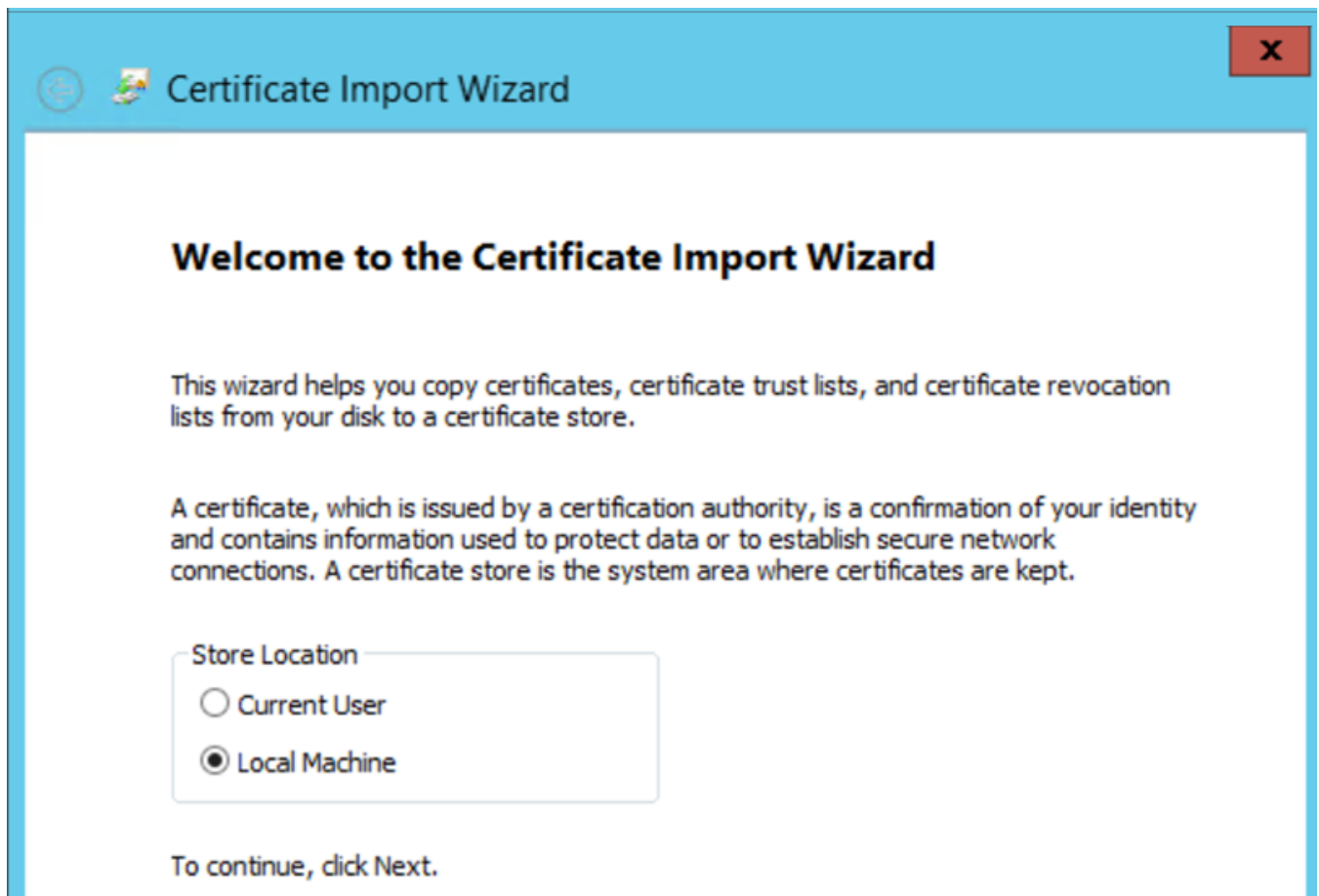
[啟用資料庫引擎的加密連線](#)

步驟 3：將 SQL Server 憑證匯入至 Symantec Endpoint Protection Manager 電腦上的 Windows

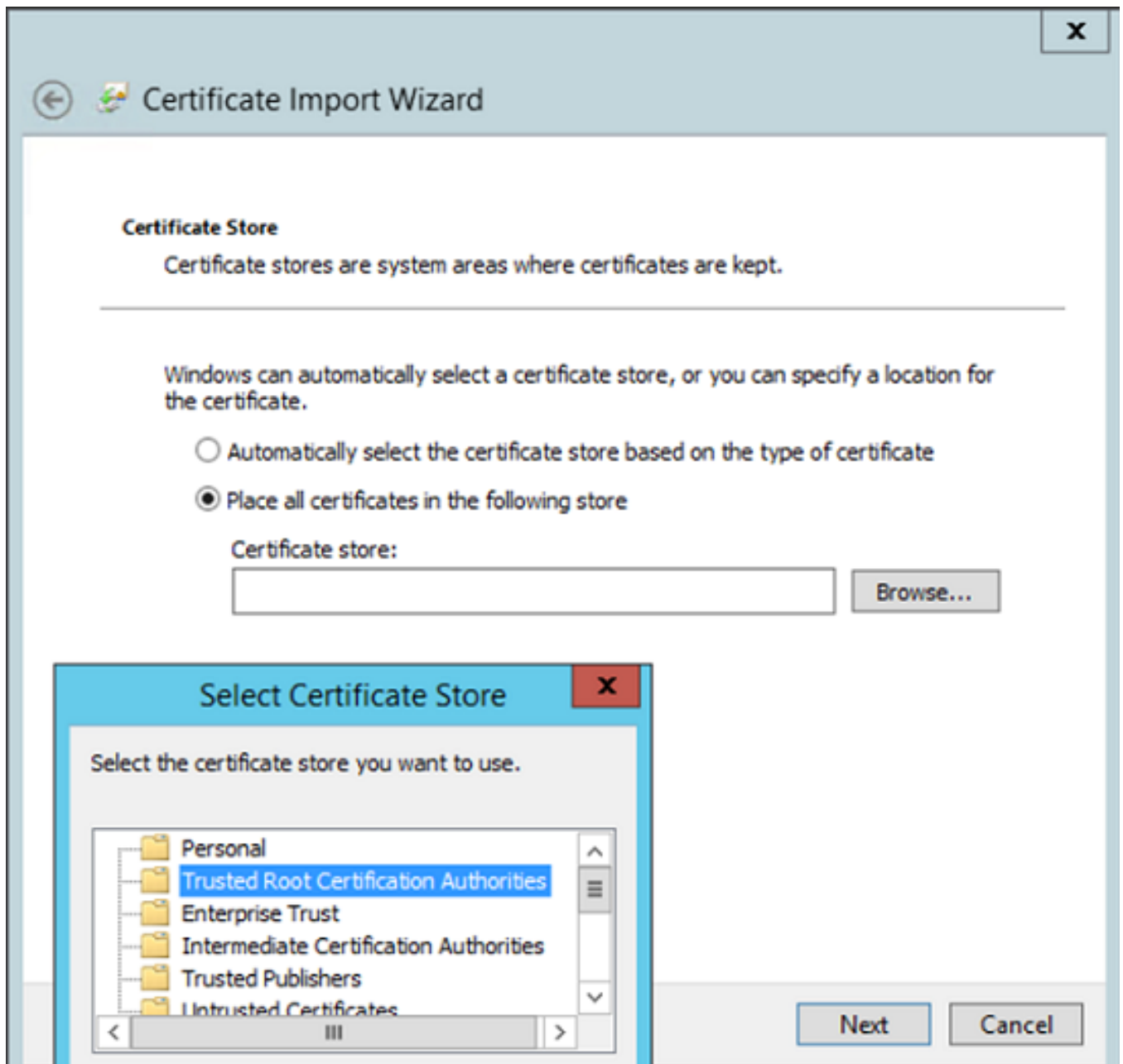
管理伺服器電腦必須已佈建 SQL Server 公用憑證。若要在管理伺服器電腦上佈建憑證，請將其匯入至 Windows。管理伺服器電腦必須設定為信任憑證的根授權。

將 SQL Server 憑證匯入至 Symantec Endpoint Protection Manager 電腦上的 Windows

1. 在管理伺服器電腦上，從「開始」功能表中選取「執行」，然後輸入 `certmgr.msc`。
2. 在憑證管理員中，選取「受信任的根憑證授權中心」，然後按一下「所有工作 > 匯入」。
這些步驟可能有所不同，取決於 Windows Server 版本。
3. 在「歡迎使用憑證匯入精靈」中，於憑證上按一下滑鼠右鍵，然後按一下「安裝憑證」。
4. 在「憑證匯入精靈」中，按照憑證匯入步驟執行。
 - 按一下「本機電腦」，然後按「下一步」。



- 按一下「將所有憑證放入以下的存放區」、按一下「瀏覽」，然後在「選取憑證存放區」對話方塊中，按一下「受信任的根憑證授權中心」。



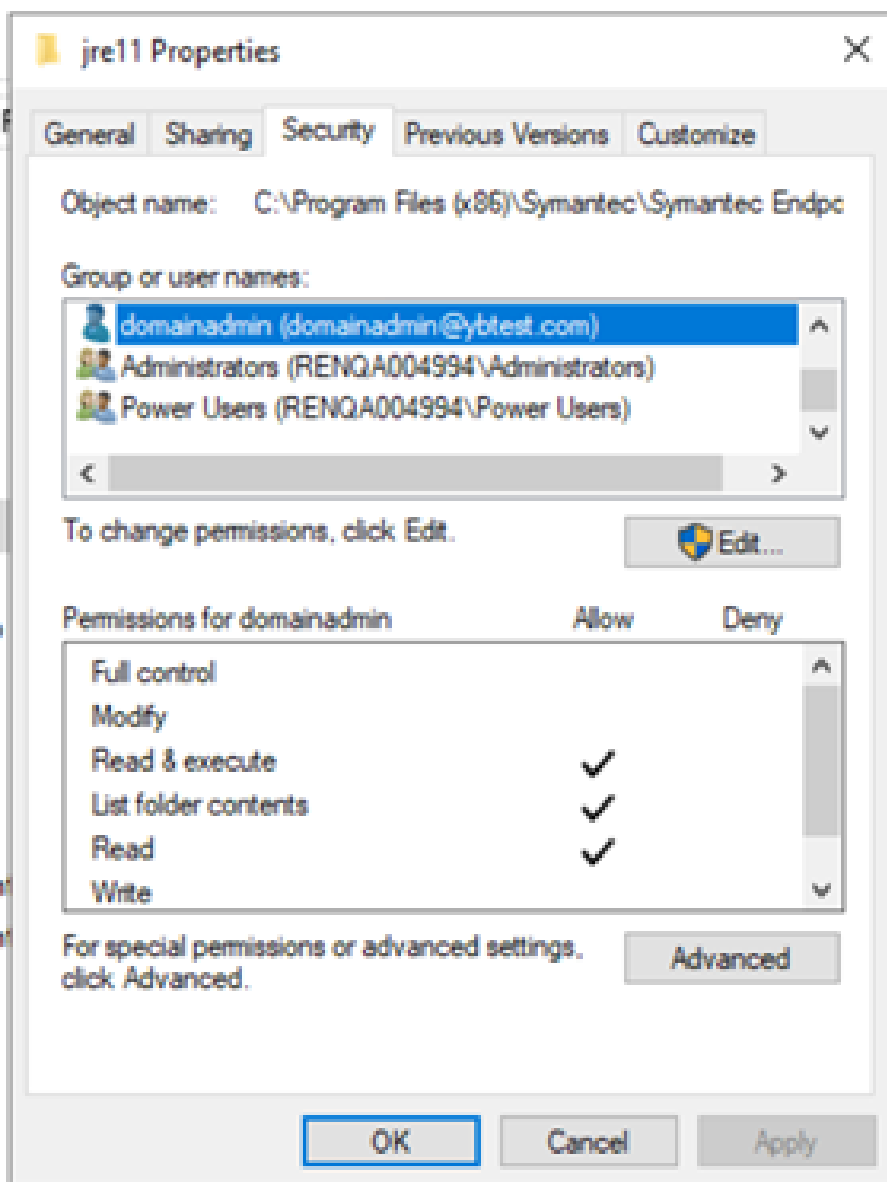
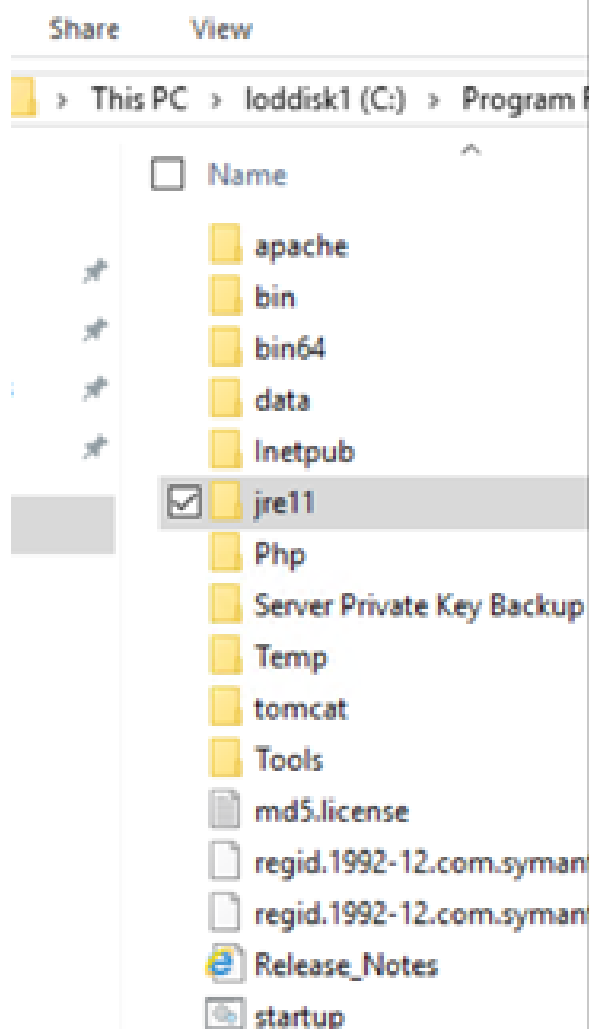
5. 按下「確定」，再按「下一步」。

步驟 4：架構 jre11 資料夾的權限

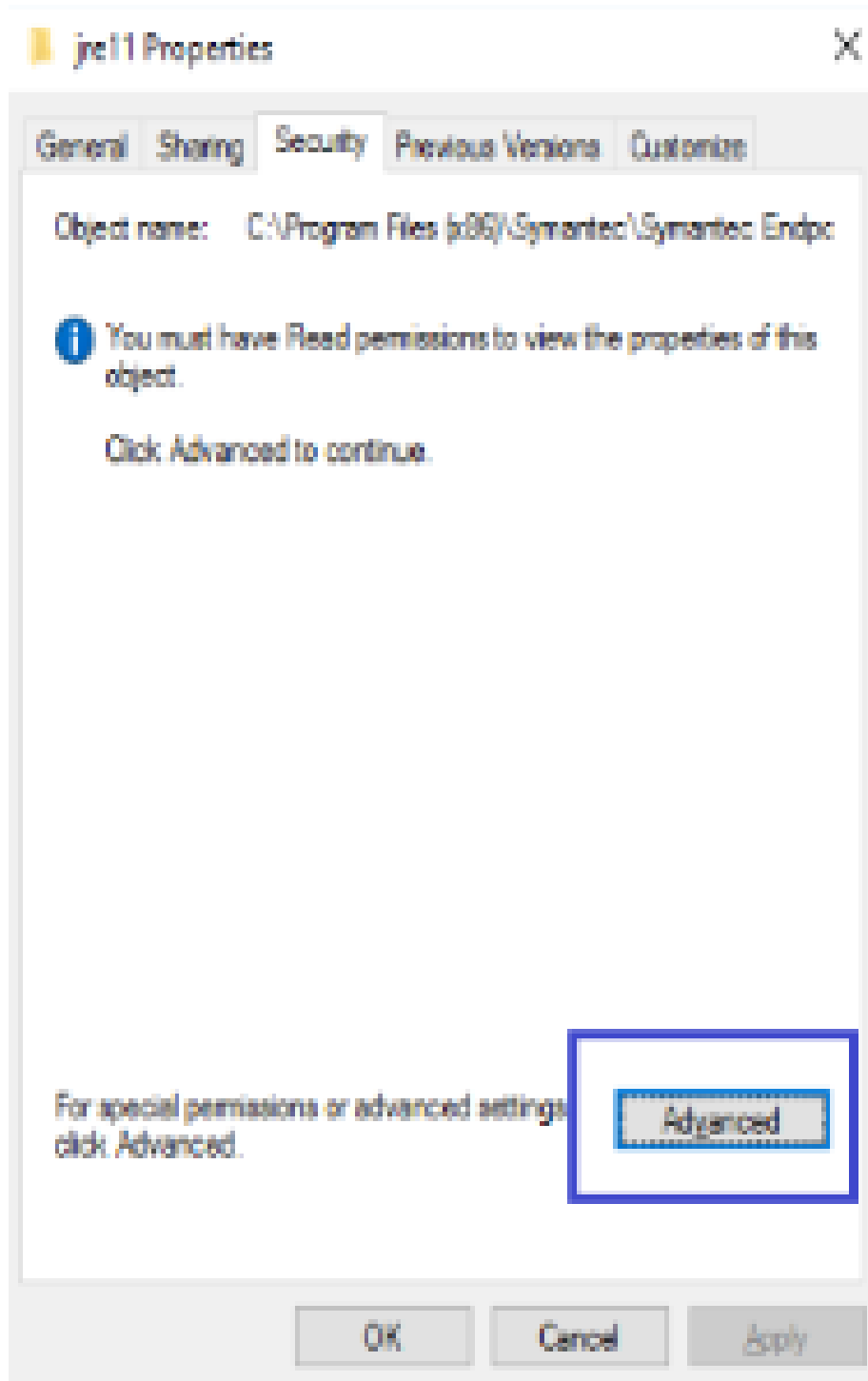
NOTE

如果搭配使用網域管理員與 Windows 驗證來架構您的 SQL Server，則網域管理員需要具有 Symantec Endpoint Protection Manager 伺服器上 jre11 資料夾的「讀取和執行」、「列出資料夾內容」和「讀取」權限。

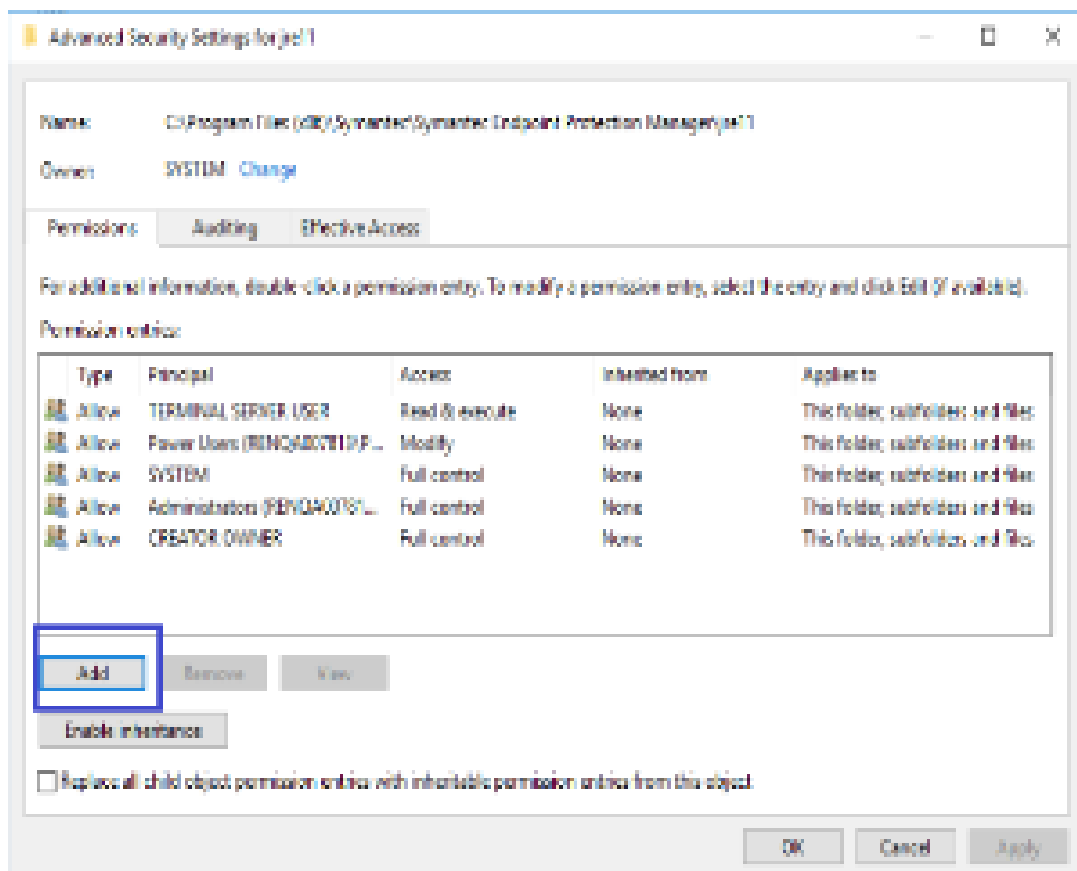
1. 在 Symantec Endpoint Protection Manager 伺服器上，移至 `...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager` 資料夾，並以滑鼠右鍵按一下 jre11 資料夾，然後按一下「屬性」。



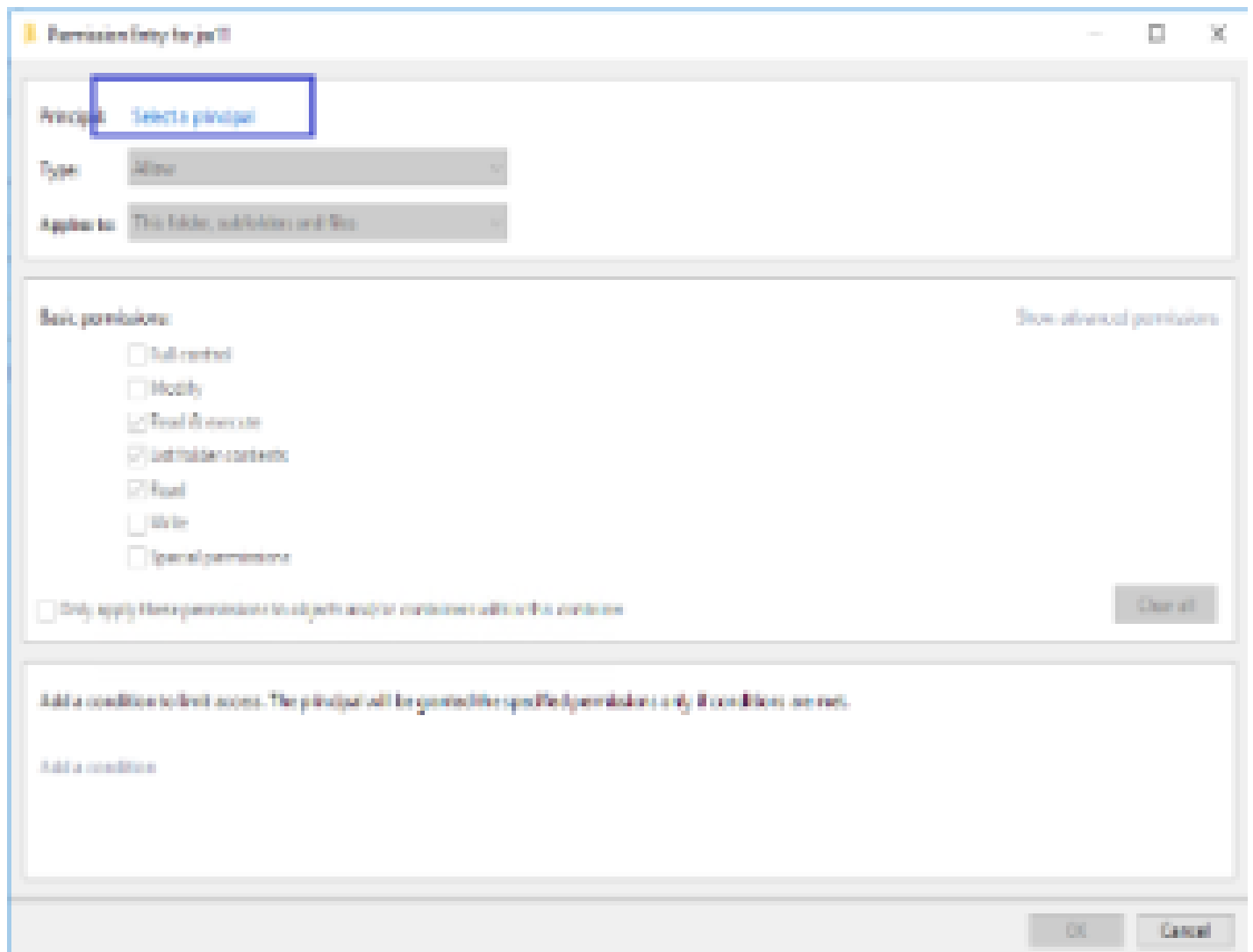
2. 在檔案屬性視窗的「安全性」標籤上，按一下「進階」。



3. 在「進階安全設定」視窗的「權限」標籤上，按一下「新增」。



4. 在「權限項目」視窗中，按一下「選取主體」。



5. 在「選取使用者、電腦、服務帳戶或群組」視窗中，新增 **domainadmin** 使用者，然後按一下「確定」。

Select User, Computer, Service Account, or Group

Select this object type:

User, Group, or Built-in security principal

Object Types...

From this location:

sep.com

Locations...

Enter the object name to select (examples):

domainadmin (domainadmin@sep.com)

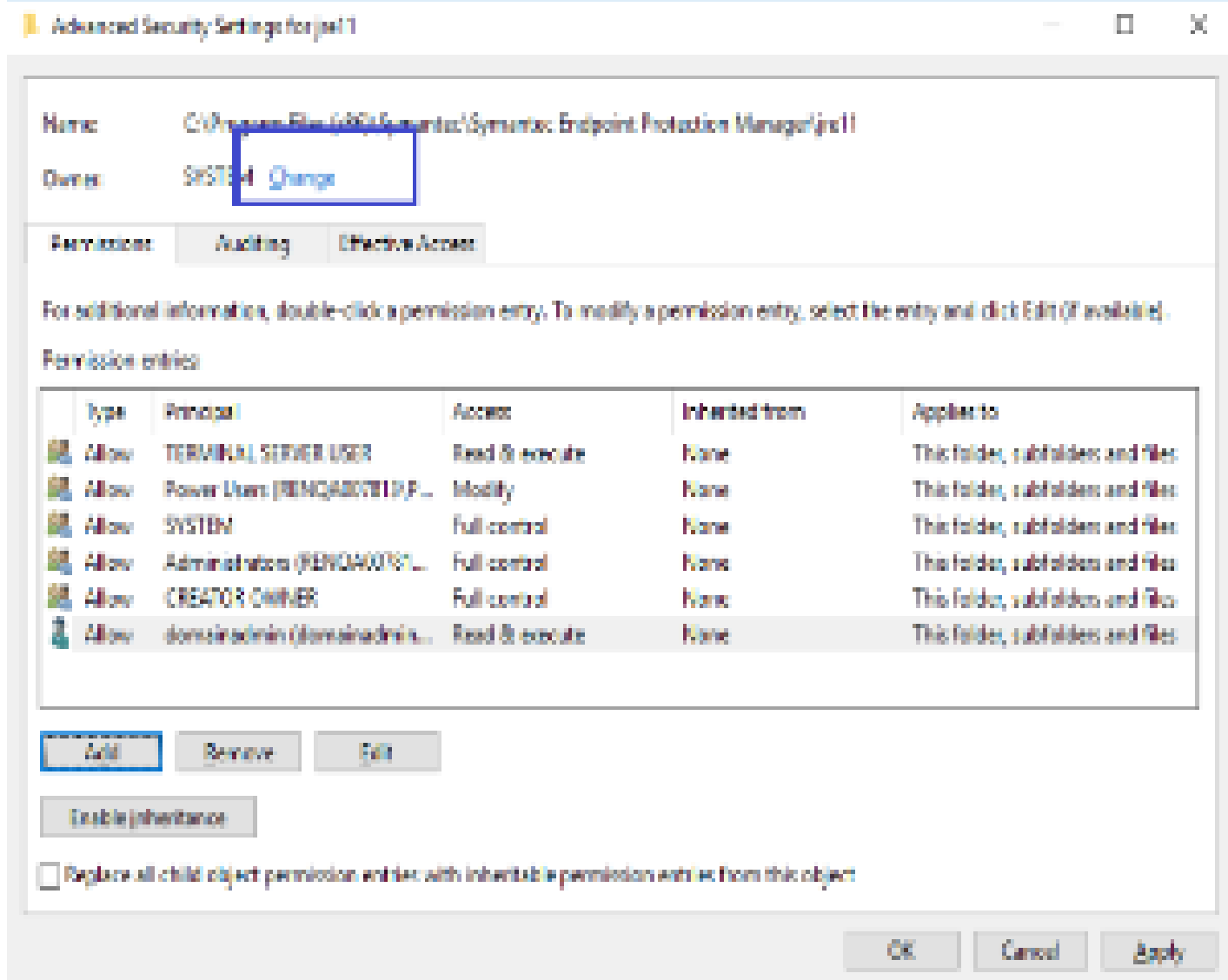
Check Names

Advanced...

OK

Cancel

6. 在「權限項目」視窗中，按一下「確定」。
7. 在「進階安全設定」視窗的「權限」標籤上，選取 **domainadmin**，然後，按一下「變更」。



8. 在「選取使用者、電腦、服務帳戶或群組」視窗中，再次新增 **domainadmin** 使用者，然後按一下「確定」。

Select User, Computer, Service Account, or Group

Select this object type:

User, Group, or Built-in security principal

Object Types...

From this location:

sep.com

Locations...

Enter the object name to select (examples):

domainadmin (domainadmin@sep.com)

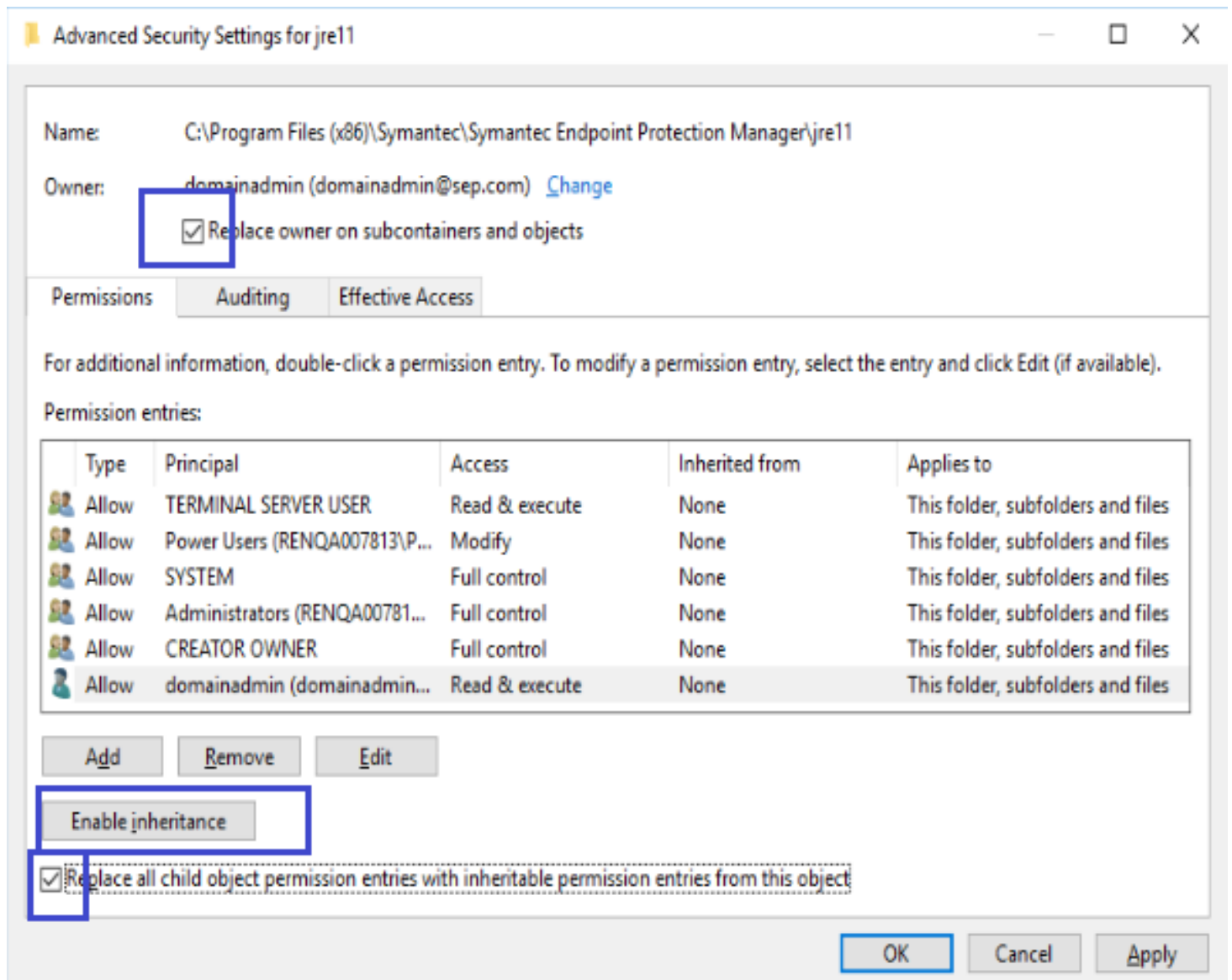
Check Names

Advanced...

OK

Cancel

9. 在「進階安全設定」視窗中，勾選「取代子配置區和物件擁有者」，並勾選「將所有子物件權限項目取代為此物件的可繼承權限項目」，再按一下「啟用繼承」，然後按一下「套用」。



10. 按下「是」或「確定」以確認。

11. 在檔案屬性視窗中，確定 **domainadmin** 使用者現在具有所有所需權限，然後按一下「確定」。

步驟 5：開啟「管理伺服器架構精靈」並使用「Windows 驗證」選項完成「伺服器架構」。

- 若要開啟精靈，請移至 \...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin 資料夾，然後連按兩下 sca.bat 檔案。

Management Server Configuration Wizard

Installation

Server Configuration

Step One: Database Server Authentication

This step must be completed first.

Authentication type: Windows Authentication

Database server: renqa007813.sep.com

SQL server port: 1433

Windows user name: sep/domainadmin

Windows user password: *****

SQL Server client folder: C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\

Browse...

Connect to database

(required)

Step Two: New Database Creation

Database name: sem5

Database data folder: C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQLDATA

< Back

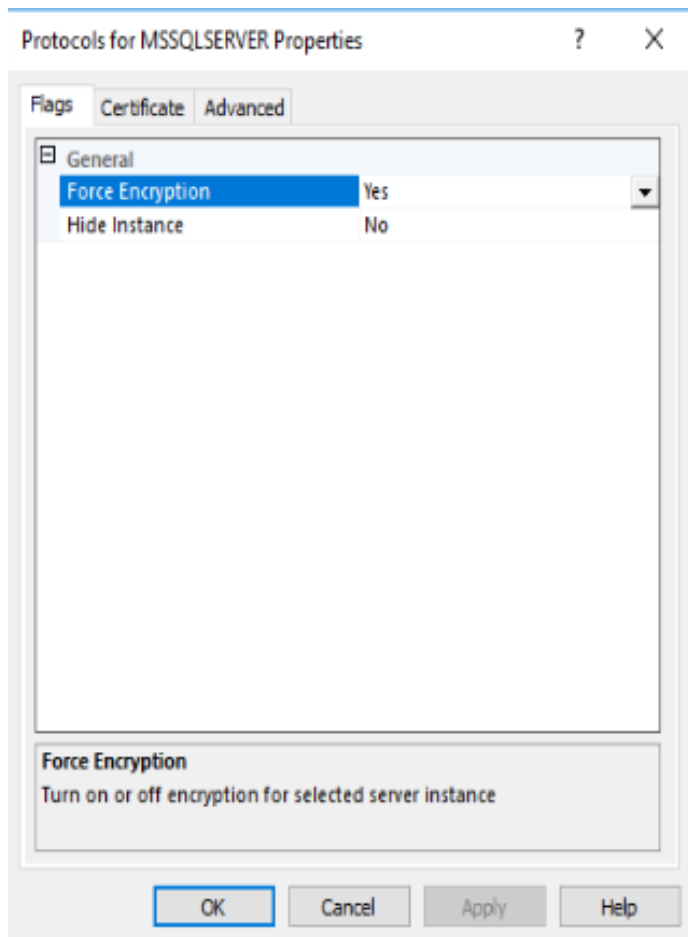
Next >

Cancel

Symantec
A Division of Broadcom

步驟 6：檢查是否加密通訊以及是否使用 **SQL Server** 憑證通訊

1. 在管理伺服器上，開啟下列檔案：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\conf\Catalina\localhost\root.xml，並確定 **encrypt=true** 和 **trustServerCertificate=false**。
2. 在 SQL Server 上，開啟「**MSSQLSERVER** 屬性的通訊協定」，並檢查是否「強制加密=是」。



3. 在 SQL Server 上，執行下列查詢，檢查是否加密 Symantec Endpoint Protection Manager 與 SQL Server 之間的連線：

```
SELECT session_id, connect_time, net_transport, encrypt_option, auth_scheme, client_net_address FROM  
sys.dm_exec_connections
```

檢查是否 **encrypt_option=TRUE**。

SQLQuery1.sql - RE...Administrator (53)) * X

```
SELECT session_id, net_transport, encrypt_option, auth_scheme, client_net_address FROM sys.dm_exec_connections
```

100 %

Results Messages

	session_id	net_transport	encrypt_option	auth_scheme	client_net_address
1	51	Shared memory	TRUE	NTLM	<local machine>
2	52	TCP	TRUE	SQL	10.32.168.100
3	53	Shared memory	TRUE	NTLM	<local machine>
4	54	Shared memory	TRUE	NTLM	<local machine>
5	55	TCP	TRUE	SQL	10.32.168.100
6	58	TCP	TRUE	SQL	10.32.168.100
7	57	TCP	TRUE	SQL	10.32.168.100
8	59	TCP	TRUE	SQL	10.32.168.100
9	60	TCP	TRUE	SQL	10.32.168.100

Symantec Endpoint Protection Manager 偵測到已架構的電子郵件伺服器需要停用憑證驗證

Symantec Endpoint Protection Manager (SEPM)，您可能會在管理伺服器升級精靈的最後一個畫面上看到下列訊息：

- Symantec Endpoint Protection Manager #####

如果您從 14.3 RU3 或更舊版本升級到 14.3 RU4 或更新版本，則可能會出現此訊息。
- Symantec Endpoint Protection Manager #####

如果您從 14.3 RU5 或更早版本升級到 14.3 RU6 或更新版本，則可能會出現此訊息。

如果 Symantec Endpoint Protection Manager 先前已停用憑證驗證以與電子郵件或目錄伺服器進行通訊，則會出現這些訊息。在升級過程中，Symantec Endpoint Protection Manager 會偵測到您架構的電子郵件伺服器憑證或目錄伺服器憑證無法驗證。但是，賽門鐵克建議您啟用伺服器憑證的驗證，以便與電子郵件伺服器或目錄伺服器的連線更加安全。

步驟 1：(選用) 建立 **Active Directory** 的個人 **CA** 根憑證

若您尚無 Active Directory 的個人 CA 根憑證，請執行下列步驟來建立一個。

若下列步驟與您所看到的不相符，請洽詢供應商，例如 Microsoft。

如要建立並匯出伺服器憑證

1. 在 Active Directory 網域伺服器上以網域管理員身分登入。
2. 按一下「開始 > 控制台 > 系統管理工具 > 憑證授權單位」，開啟 CA Microsoft Management Console (MMC)。
3. 以滑鼠右鍵按一下 CA 電腦，並選取「**CA** 屬性」。
4. 在「一般」功能表上，按一下「檢視憑證」。
5. 選取「詳細資料」檢視畫面，並按一下視窗右下角的「複製到檔案」。
6. 使用「憑證匯出」精靈，將 CA 憑證儲存於檔案中。

步驟 2：將伺服器憑證安裝至 **Symantec Endpoint Protection Manager** 電腦上的 **Windows**

接著匯入使用 DER、PEM 或 PFX 副檔名的電子郵件伺服器或目錄伺服器憑證。

如要將伺服器憑證匯入管理伺服器電腦上的 **Windows**

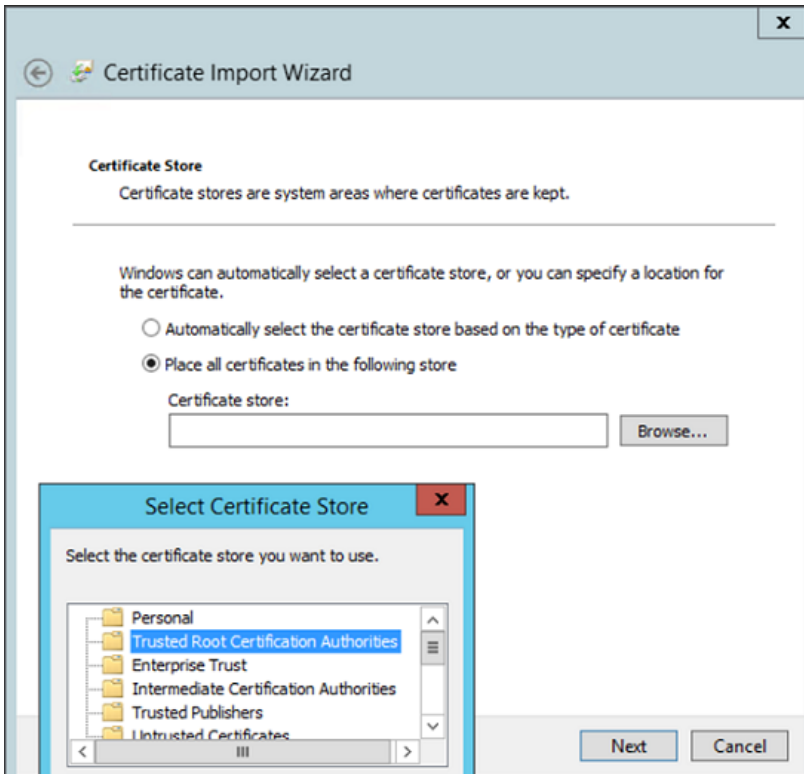
1. 將伺服器憑證匯出至安裝 Symantec Endpoint Protection Manager 的 Windows 電腦。
2. 以滑鼠右鍵按一下該憑證，然後按一下「安裝憑證」。



3. 在「憑證匯入精靈」對話方塊的「儲存位置」下方，選取「本機電腦」，然後按一下「下一步」。



4. 選取「將所有憑證放入以下的存放區」，按一下「瀏覽」，然後在「選取憑證存放區」對話方塊中，按一下「受信任的根憑證授權中心」。



5. 按下「確定」，再按「下一步」。

步驟 3：啟用伺服器憑證驗證

您必須啟用憑證驗證，SEPM 才能連線到電子郵件伺服器或目錄伺服器。啟用憑證驗證後，SEPM 會檢查憑證是否有效。

啟用電子郵件伺服器憑證驗證

1. 在主控台上，使用以下命令停止並重新啟動管理伺服器服務：

```
net stop semsrv, net stop semapisrv, net start semsrv, net start semapisrv
```

停止及啟動管理伺服器服務

2. 按一下「管理員 > 伺服器」，以滑鼠右鍵按一下管理伺服器，並按一下「編輯伺服器屬性」。
請參閱：[建立管理伺服器與電子郵件伺服器之間的通訊](#)
3. 在「電子郵件伺服器」標籤上，取消勾選「停用電子郵件伺服器憑證的驗證」選項，然後按一下「確認」。

若要啟用目錄伺服器憑證驗證

1. 在主控台上，使用以下命令停止並重新啟動管理伺服器服務：

```
net stop semsrv, net stop semapisrv, net start semsrv, net start semapisrv
```

2. 按一下「管理員 > 伺服器」，以滑鼠右鍵按一下管理伺服器，並按一下「編輯伺服器屬性」。
3. 在「目錄伺服器」標籤上，選擇伺服器，然後按一下「編輯」。
4. 取消勾選「停用電子郵件伺服器憑證的驗證」選項，然後按一下「確認」。
如果出現驗證或 Symantec Endpoint Protection Manager 無法連線到目錄伺服器的警告，請檢查憑證並再次驗證直到警告訊息消失。

NOTE

如果管理員架構為使用目錄伺服器驗證，則重複點按警告可能會影響 Symantec Endpoint Protection Manager 管理員登入並可能將管理員鎖住。

[在嘗試太多次登入後解除鎖定管理員帳戶](#)

[選擇管理員帳戶的驗證方法](#)

如需新增目錄伺服器的資訊，請參閱：

[連線至遠端複製網站上的目錄伺服器](#)

解決 14.3 RU5 或更新版本安裝或升級後的 Microsoft SQL Server 資料庫連線錯誤

您可能需要變更資料庫擁有者帳戶權限，或重新建立報告資料庫帳戶，以解決在您安裝或升級至 Symantec Endpoint Protection Manager (SEPM) 14.3 RU5 或更新版本時出現的錯誤。

於安裝或升級後，您可能會看到下列錯誤：

```
The Symantec Endpoint Protection Manager reporting account does not connect to the Microsoft SQL Server database. You must recreate or modify the reporting account in SQL Server Management Studio. Then run the Management Server Configuration Wizard again.
```

此錯誤的發生很可能是因為目前的「資料庫擁有者帳戶」並無 [#####] 權限，但也可能因為下列原因而發生：

- 您的密碼可能不相符。「報告帳戶」使用與「資料庫擁有者帳戶」相同的密碼。若重設「資料庫擁有者帳戶」的密碼，則必須重設「報告帳戶」以使用相同的密碼。若為新的安裝，「SEPM 管理伺服器組態精靈」將使用「資料庫擁有者帳戶」和「報告帳戶」建立 SEPM 資料庫。例如，若資料庫名為 sem5，而「資料庫擁有者帳戶」為 sem5，則「報告帳戶」為 REPORTER_sem5sem5 (格式為 "REPORTER_ < DatabaseName > < DBOwnerAccount >")。
- 「報告帳戶登入」和「使用者」已損壞或彼此不相符。

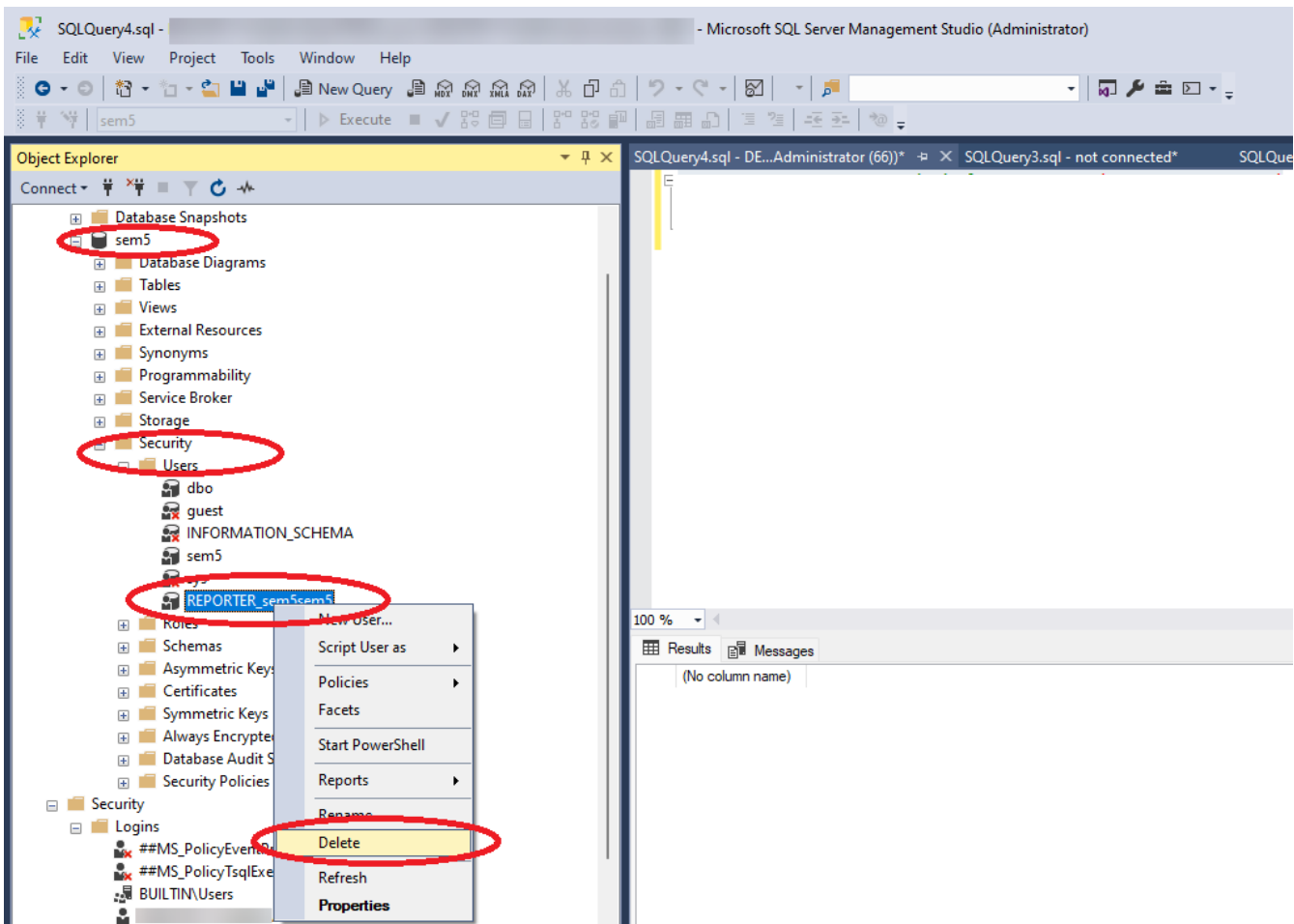
解決方案

如要解決此錯誤，請嘗試下列任一解決方案：

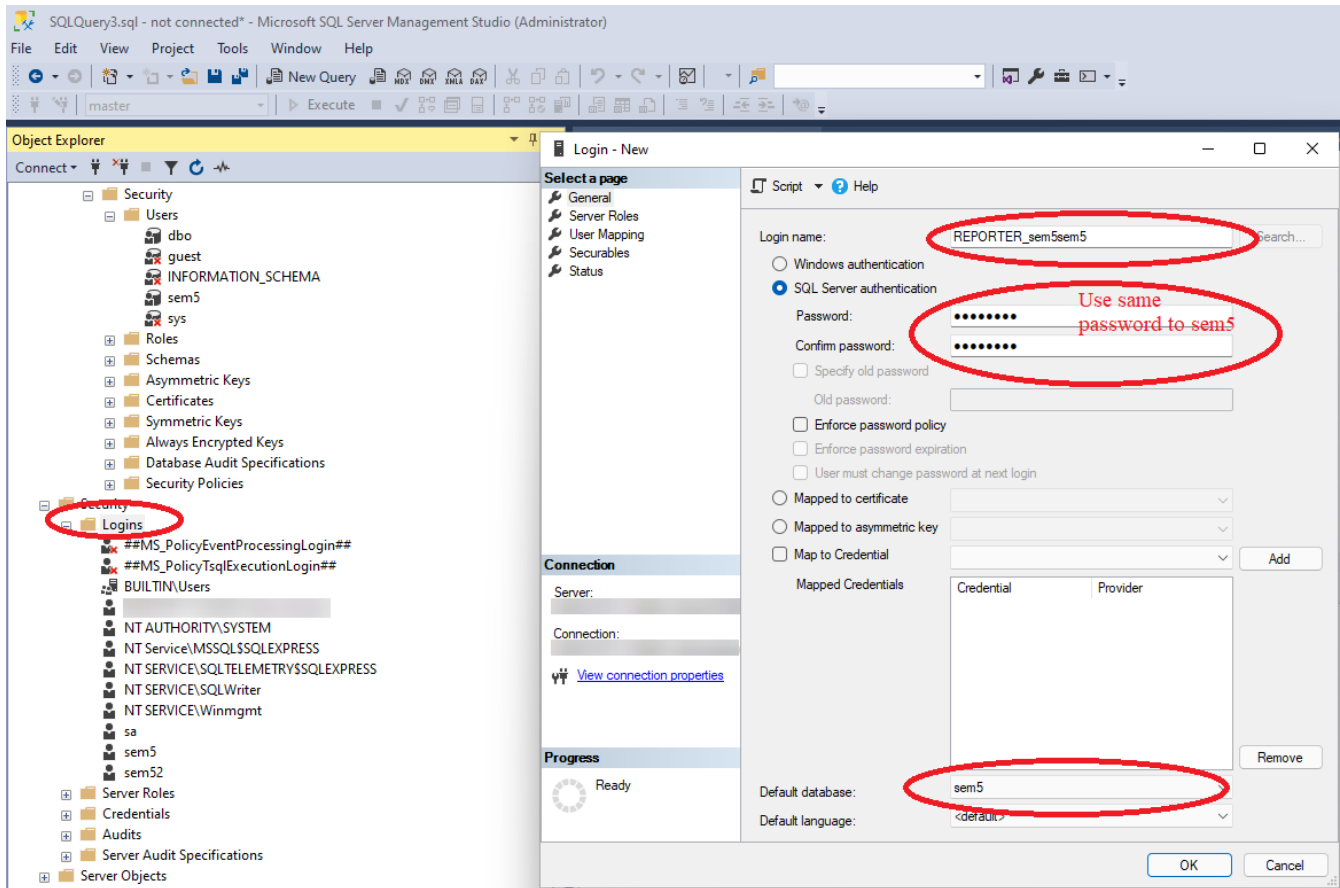
- 將 [#####] 權限授予「資料庫擁有者帳戶」，然後按兩下 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat 來重新設定或重新執行升級，以完成執行「管理伺服器組態精靈」。
- 若不想將此權限授予「資料庫擁有者帳戶」，可在 Microsoft SQL Server Management Studio 上重新建立報告資料庫帳戶。

如要在 Microsoft SQL Server Management Studio 上重新建立報告資料庫帳戶

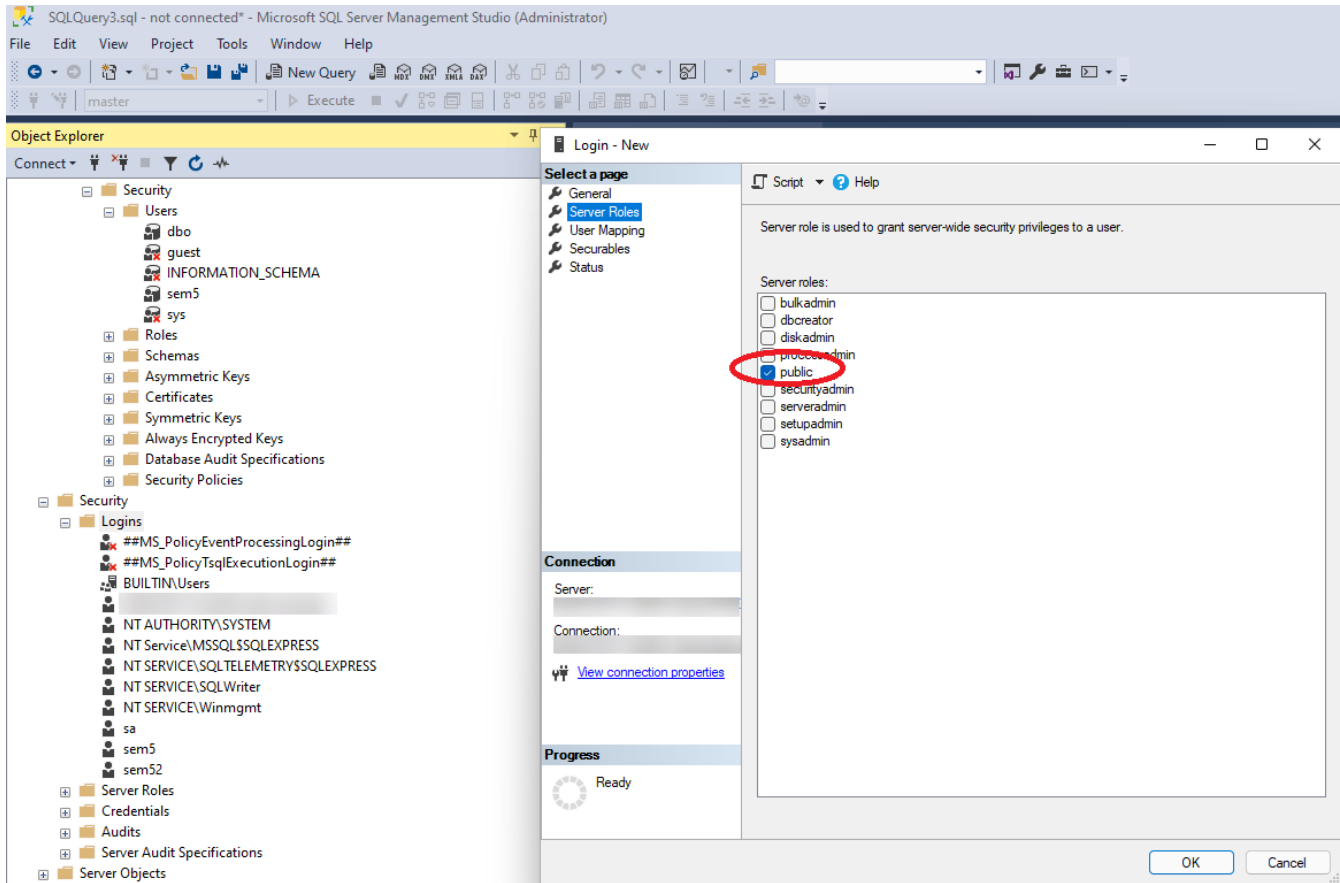
1. 在 Microsoft SQL Server 電腦上，開啟 Microsoft SQL Server Management Studio。
2. 刪除「報告帳戶」使用者帳戶 (若存在)。
 - a. 於 Object Explorer 中，選取 Symantec Endpoint Protection Manager 資料庫 (依預設為 **sem5**)。
 - b. 展開「安全性 > 使用者」，然後以滑鼠右鍵按一下「**REPORTER_ < DatabaseName > < DBOwnerAccount >**」。
 - c. 按一下「刪除」。



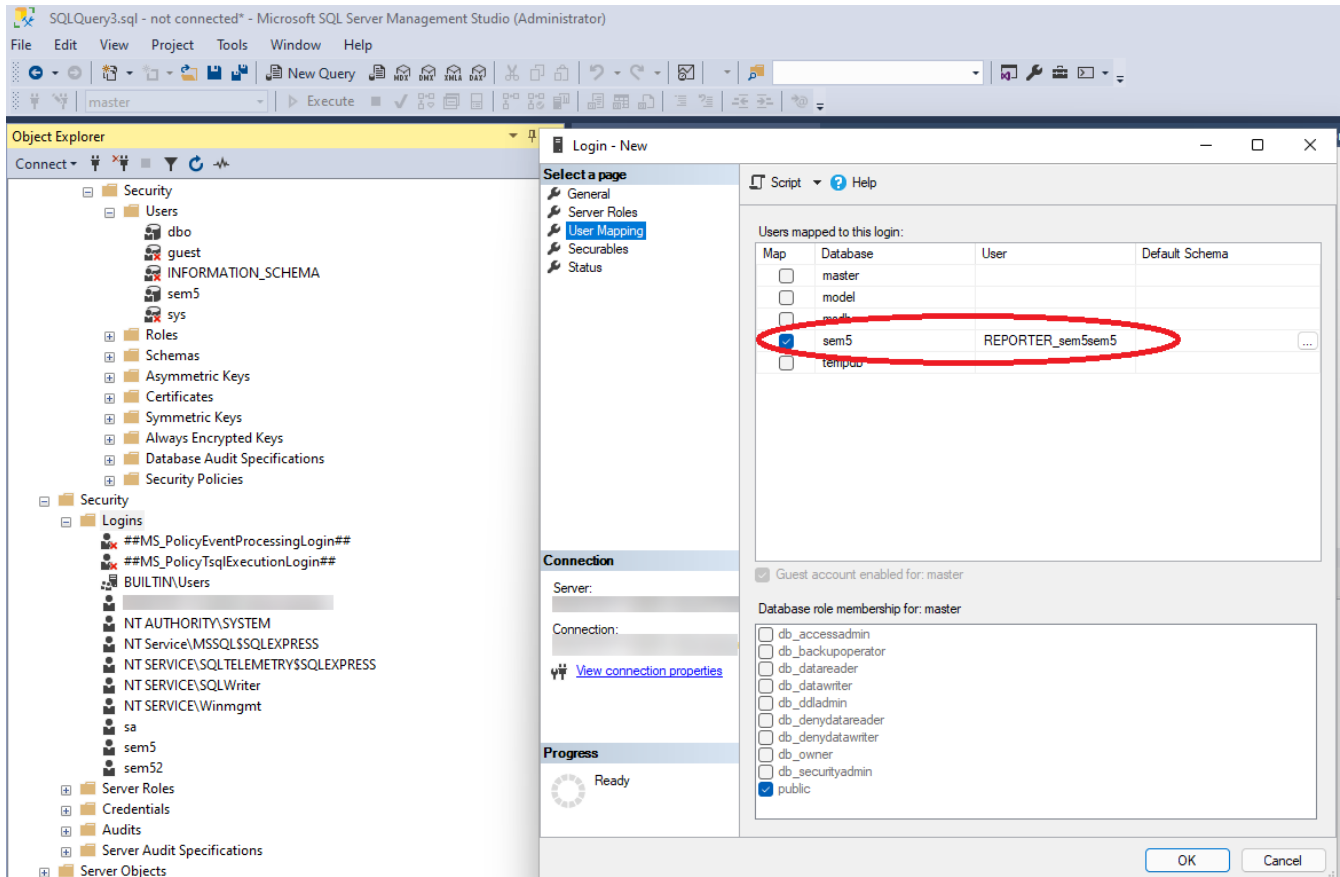
3. 修改或重新建立「報告帳戶」的登入。
 - a. 展開「安全性 > 登入」，然後選取您的資料庫。
 - b. 在「登入 > 一般」頁面中，選取您的登入名稱。
 - c. 於「**SQL Server 驗證**」下，鍵入「資料庫擁有者帳戶」的密碼。
若您的「資料庫擁有者帳戶」使用 Windows 驗證，請鍵入並確認您的 Windows 帳戶密碼。
 - d. 選取預設資料庫作為資料庫。



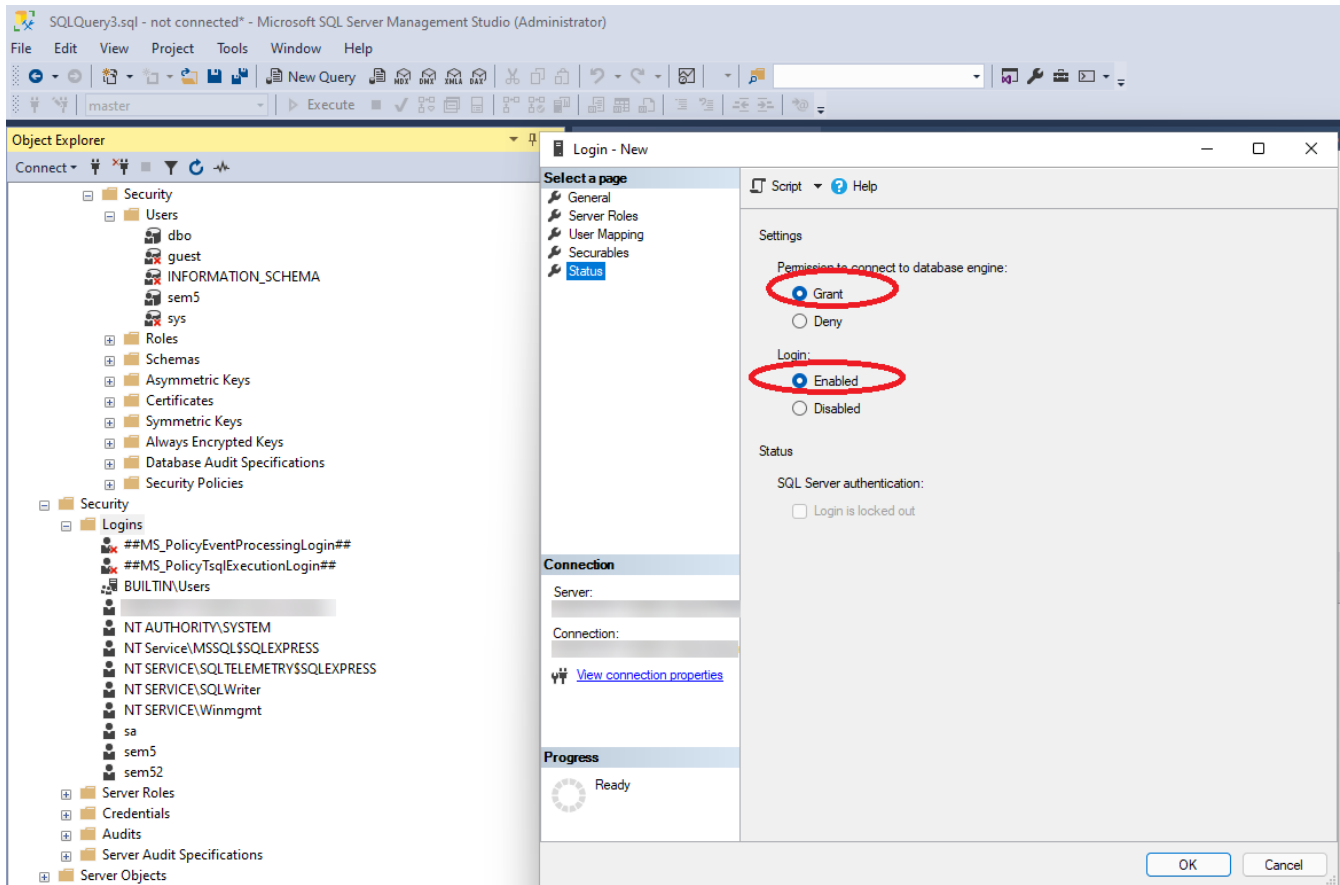
4. 在「伺服器角色」頁面中，選取「公共伺服器」角色。



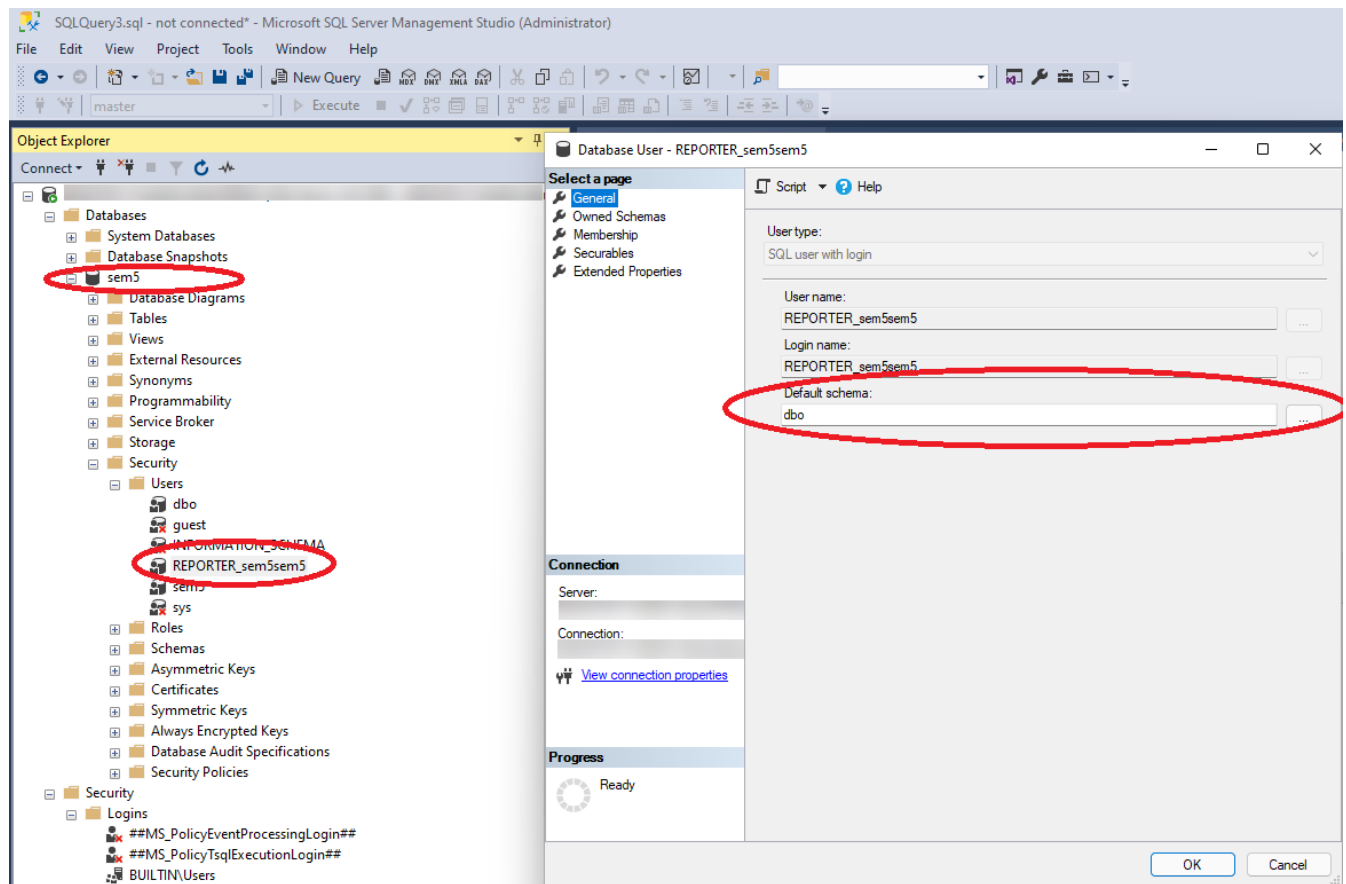
5. 在「使用者對應」頁面上，將登入帳戶對應至您的資料庫。



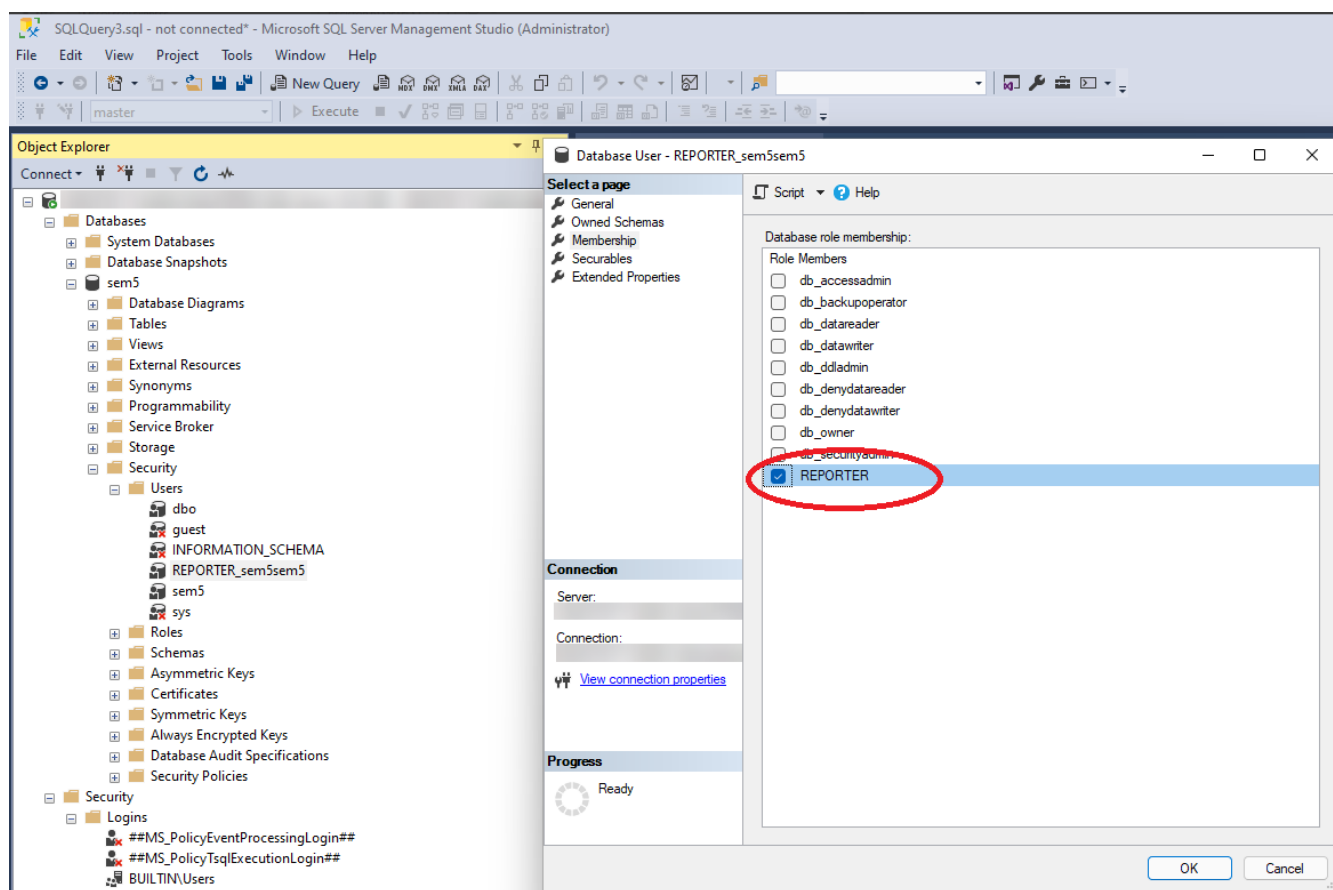
6. 在「狀態」頁面上，執行下列作業：
- 設定授予的授權。
 - 將登入帳戶設定為「已啟用」。
 - 按一下「確定」。



7. 重新設定或重新執行升級。連按兩下 `upgrade.bat`，完成重新執行「管理伺服器組態精靈」。
8. (選用) 完成後，您可驗證您的變更。請執行下列動作：
 - a. 在「一般」索引標籤上，驗證「報告帳戶」使用者是否使用正確的「預設」綱要。



- b. 在「成員資格」頁面上，驗證「報告帳戶」使用者是否具有角色 **REPORTER**。



主控台現在應可正確地顯示主頁。

升級使用多個內嵌資料庫和管理伺服器的環境

使用多個內嵌資料庫和管理伺服器的環境具有以下含義：

- 管理伺服器不會針對 Symantec Endpoint Protection 使用容錯移轉或負載平衡，因為內嵌資料庫不支援容錯移轉或負載平衡的伺服器。
- 管理伺服器是 Symantec Endpoint Protection 複寫夥伴。

所有的站台都有一台最先安裝管理伺服器的電腦。您必須先升級此管理伺服器，因為它包含加密金鑰或加密密碼等重要的站台資訊。然後再升級針對複寫所安裝的其他管理伺服器。

NOTE

自 14.3 RU1 起，Microsoft SQL Server Express 資料庫取代了內嵌資料庫。SQL Server Express 支援容錯移轉和負載平衡。

升級使用多個內嵌資料庫和管理伺服器的環境

1. 驗證並登入安裝第一個 Symantec Endpoint Protection Manager 所在的電腦。

請勿登入 Symantec Endpoint Protection Manager。如果您使用複寫，則無需首先將其停用。如果產品版本不符，則 Symantec Endpoint Protection 不允許複寫。

2. 升級管理伺服器。
3. 逐一升級所有其他的管理伺服器。

在變更電腦的 IP 位址和主機名稱後重新架構 Symantec Endpoint Protection Manager

Symantec Endpoint Protection 用戶端使用 Symantec Endpoint Protection Manager (SEPM) 電腦的主機名稱和 IP 位址以與 SEPM 通訊。如果您變更電腦的主機名稱和 IP 位址，則用戶端不會自動維護通訊。此外，因為資料庫伺服器名稱變更，並且其先前具有舊電腦名稱和 IP 位址的憑證無效，所以 SEPM 無法連線至資料庫。

因為 SEPM 電腦的 IP 位址和主機名稱與憑證的 IP 位址和主機名稱不同，所以 SEPM Web 主控台會顯示憑證錯誤。請參閱：

[疑難排解：「您的伺服器憑證無效，因為電腦主機名稱或 IP 位址已變更」\(14.3 RU8 或更新版本\)](#)

NOTE

SEPM 和 SEP 用戶端只透過 HTTPS 而非透過 HTTP 通訊時，您可以執行這些工作。

重新架構 Symantec Endpoint Protection Manager 並產生 SQL Server Express 或 SQL Server 資料庫的憑證

重新架構 Symantec Endpoint Protection Manager 並產生 SQL Server Express 或 SQL Server 資料庫的憑證

1. 在 Symantec Endpoint Protection Manager 中，更新管理伺服器清單以同時使用目前和新的主機名稱和 IP 位址，並確保將其指派給所有用戶端。
更新過的清單允許 SEP 用戶端在主機名稱和 IP 位址變更之後繼續與 SEPM 通訊。請參閱：
[指派管理伺服器清單至群組和位置](#)
2. 在「用戶端」>「政策」標籤上，按一下「一般」>「安全設定」標籤，然後清除「使用數位憑證進行驗證，以啟用管理伺服器與用戶端之間的安全連線」。停用安全通訊讓用戶端仍然可以與 SEPM 通訊，而不需要驗證與 SEPM 的通訊。
請參閱：
[在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證](#)
3. 在「用戶端」>「用戶端」標籤上，檢查用戶端是否仍然連線至管理伺服器。
4. 變更 SEPM 電腦 IP 位址。
5. 變更 SEPM 電腦主機名稱，然後重新啟動 SEPM 電腦。

NOTE

您可以只重新命名電腦主機名稱，而不需要重新命名 IP 位址。

6. 執行下列指令來停止 SEPM 服務：`net stop semsrv`、`net stop semapisrv` 和 `net stop semwebsrv`。請參閱：
[停止及啟動管理伺服器服務](#)

7. 開啟以下檔案：

```
<SEPM_Install>\tomcat\conf\Catalina\localhost\root.xml  
<SEPM_Install>\tomcat\instances\sepm-api\conf\Catalina_WS\localhost\jdbc.properties
```

其中 **<SEPM_Install>** 是 Symantec Endpoint Protection Manager 安裝目錄

- a. 變更：

```
jdbc:sqlserver://<sepm_old_computer_name>:2638  
至：  
jdbc:sqlserver://<sepm_new_computer_name>:2638
```

NOTE

如果使用的通訊埠編號不是 2638，則請繼續使用其他編號。

- b. 變更：

```
trustServerCertificate = false
```

至：

trustServerCertificate = true

8. 在目錄位置 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSSQLServer\Client\ConnectTo，變更：

值名稱：<old_sql_express_db_instance>\<sql_express_instance_name>

值資料：DBMSSOCN,<old_server name>\<sql_express_instance_name>,2638

至：

值名稱：<new_sql_express_db_instance>\<sql_express_instance_name>

值資料：DBMSSOCN,<new_server name>\<sql_express_instance_name>,2638

例如：

值名稱：WIN-newserver\SQLEXPRESSSYMCO

值資料：DBMSSOCN,WIN-newserver.xxx.labs.abc.net\SQLEXPRESSSYMCO,2638

9. 執行下列指令來重新啟動 Symantec Endpoint Protection Manager 服務：net start semsrv、net start semapisrv 和 net start semwebsrv。

10. 登入 Symantec Endpoint Protection Manager。

— 如果出現「#####」訊息，則請更新憑證並登入 (14.3 RU8 或更新版本)。

如需瞭解如何解決此問題，請參閱：[疑難排解：「您的伺服器憑證無效，因為電腦主機名稱或 IP 位址已變更」\(14.3 RU8 或更新版本\)](#)

— 如果出現「#####」訊息，則請按一下「確定」，並繼續登錄 (14.3 RU7 或更舊版本)。

11. 產生新的 SEPM 伺服器憑證。

此步驟會讓 SEPM 到 SEP 用戶端憑證資訊與新的電腦名稱和 IP 位址相符。請參閱：

[產生新的伺服器憑證](#)

12. 登出 SEPM 主控台。

13. 執行下列其中一個步驟：

Microsoft SQL Server Express 資料庫	1. 重新架構 SEPM。請參閱： 重新安裝或重新架構 Symantec Endpoint Protection Manager 2. 登入 SEPM。
Microsoft SQL Server 資料庫	1. 重新架構 SEPM。會出現 TLS 訊息。 2. 產生並匯入新的 SQL TLS 憑證。完成架構。 3. 登入 SEPM。 如果 SQL Server 資料庫與 SEPM 位於相同的電腦上，則請參閱： 在變更電腦的主機名稱後將 Microsoft SQL Server 資料庫重新架構為用戶端
內嵌資料庫	登入 SEPM。

14. 按一下「使用數位憑證進行驗證，以啟用管理伺服器與用戶端之間的安全連線」。

15. 檢查用戶端是否仍然連線至 SEPM。

在變更電腦的主機名稱後將 **Microsoft SQL Server** 資料庫重新架構為用戶端

如果將 Microsoft SQL Server 用作與 SEPM 相同的電腦上的資料庫伺服器，則在變更電腦的主機名稱後，用於 ODBC 連線的伺服器名稱也會變更。您必須更新用於 ODBC 連線的伺服器名稱。您只能變更 SEPM 的電腦名稱，而非 IP 位址。

變更 ODBC 連線所使用的伺服器名稱

1. 在 Symantec Endpoint Protection Manager 電腦上，按一下「開始」>「執行」。
2. 在「名稱」欄位中，輸入 odbccp32.cpl (32 位元) 或 odbcad32.exe (64 位元)，然後按一下「確定」。
3. 在「ODBC 資料來源管理員」對話方塊中，按一下「系統 DSN」標籤。
4. 按一下 **SymantecEndpointSecurityDSN** 作為「系統 DSN」，然後按一下「架構」。
5. 輸入伺服器名稱的正確連線目的 (如反斜線 \)，然後按「下一步」。

-
6. 如果您使用 Windows 驗證，則請選取「使用整合式 **Windows** 驗證」。如果使用 SQL Server 驗證，請選擇「使用輸入的登入 ID 和密碼進行 **SQL Server** 驗證」，然後輸入您的登入 ID 和密碼。按一下「連接到 **SQL Server** 以取得其他設定選項的預設設定」，然後按「下一步」。
 7. 選取「將預設資料庫變更為」，並選取 **sem5**，然後按「下一步」。
 8. 按下「完成」。
 9. 在 ODBC Microsoft SQL Server 對話方塊上，按一下「測試資料來源」。
如果您看到#####! 訊息，則 ODBC 連線測試已完成。

疑難排解伺服器名稱不符伺服器憑證時，Symantec Endpoint Protection Manager 會封鎖您登入或升級 (14.3 RU9 或更新版本)

從 14.3 RU9 開始，Symantec Endpoint Protection Manager 安裝和升級會要求管理伺服器名稱也必須符合伺服器憑證中列出的其中一個主旨備用名稱 (SAN)。此外，伺服器名稱必須使用有效的主機名稱、完全合格網域名稱 (FQDN) 或 IP 位址。

如果管理伺服器名稱和 SAN 不相符，請執行以下任一步驟。

- 重新命名管理伺服器。
- 更新憑證，因為管理伺服器名稱正確，但伺服器憑證不正確。請參閱：
[更新或還原伺服器憑證](#)

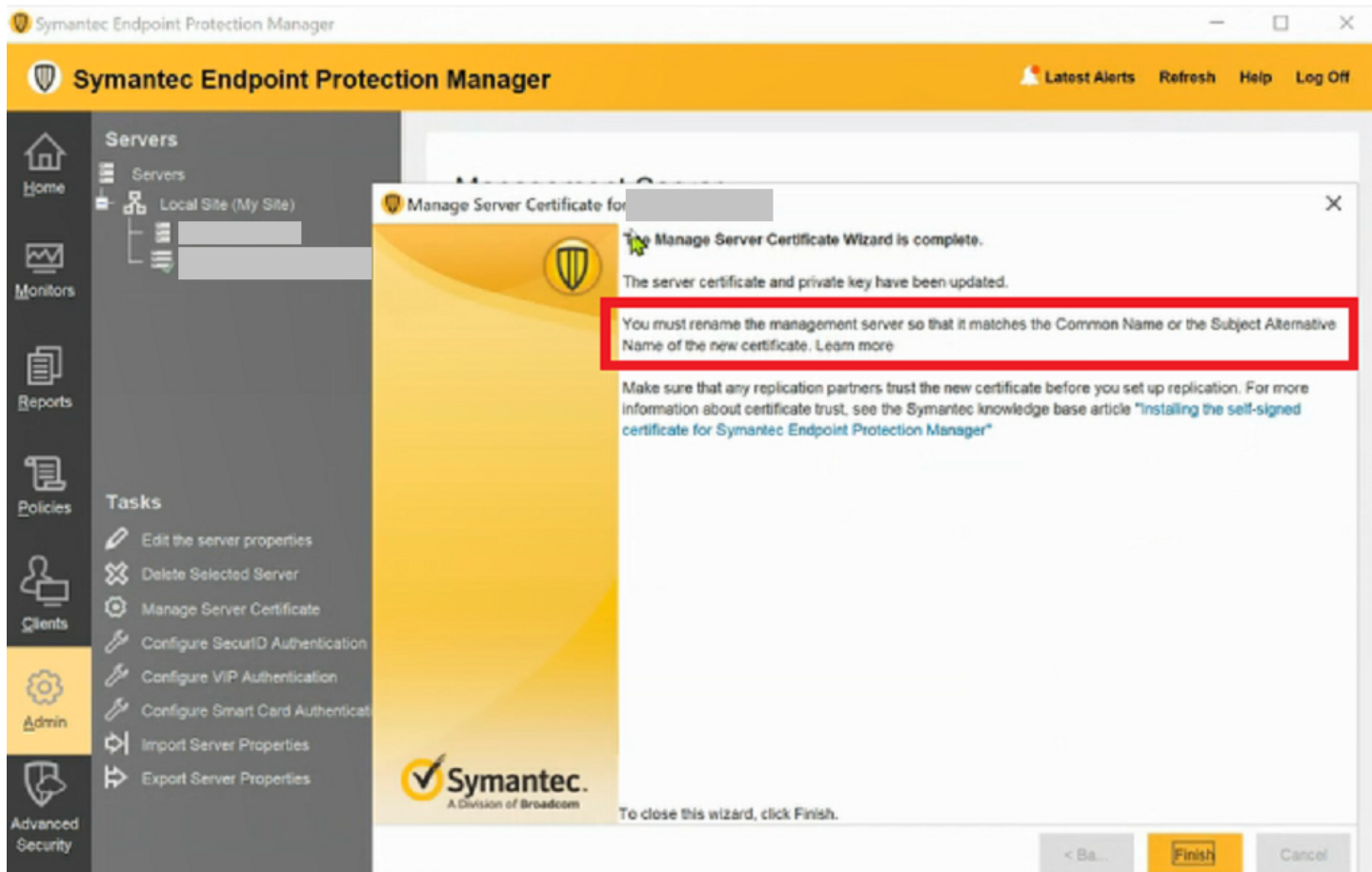
條件

此錯誤發生在以下情況：

情況 1：

匯入帶有一個或多個與當前管理伺服器名稱不相符的 SAN 的新憑證。匯入憑證後，在「管理伺服器憑證」精靈中會看到以下訊息：

#####



情況 2：

當您升級時，可能會看到下列訊息：

- ##### Symantec Endpoint Protection Manager #####
 – ##### IP ##### (SAN) #####
 – ##### Symantec Endpoint Protection Manager #####
- ##### IP #####
 ##

此訊息在以下情況會出現：

- 您從 14.3 RU8 和更舊版本的管理伺服器中匯入新的伺服器憑證，但未重新命名管理伺服器以符合所匯入憑證中的伺服器名稱。
- 從憑證的內容重新命名管理伺服器，然後開始升級。

原因

此錯誤的發生原因如下：

- 管理伺服器名稱不是解析 Symantec Endpoint Protection Manager 電腦 IP 位址的 DNS 名稱。
- DNS 名稱不是管理伺服器憑證 SAN 清單的一部分。

在這兩種情況下，當前管理伺服器名稱都不滿足 14.3 RU9 中的新要求。

解決方案

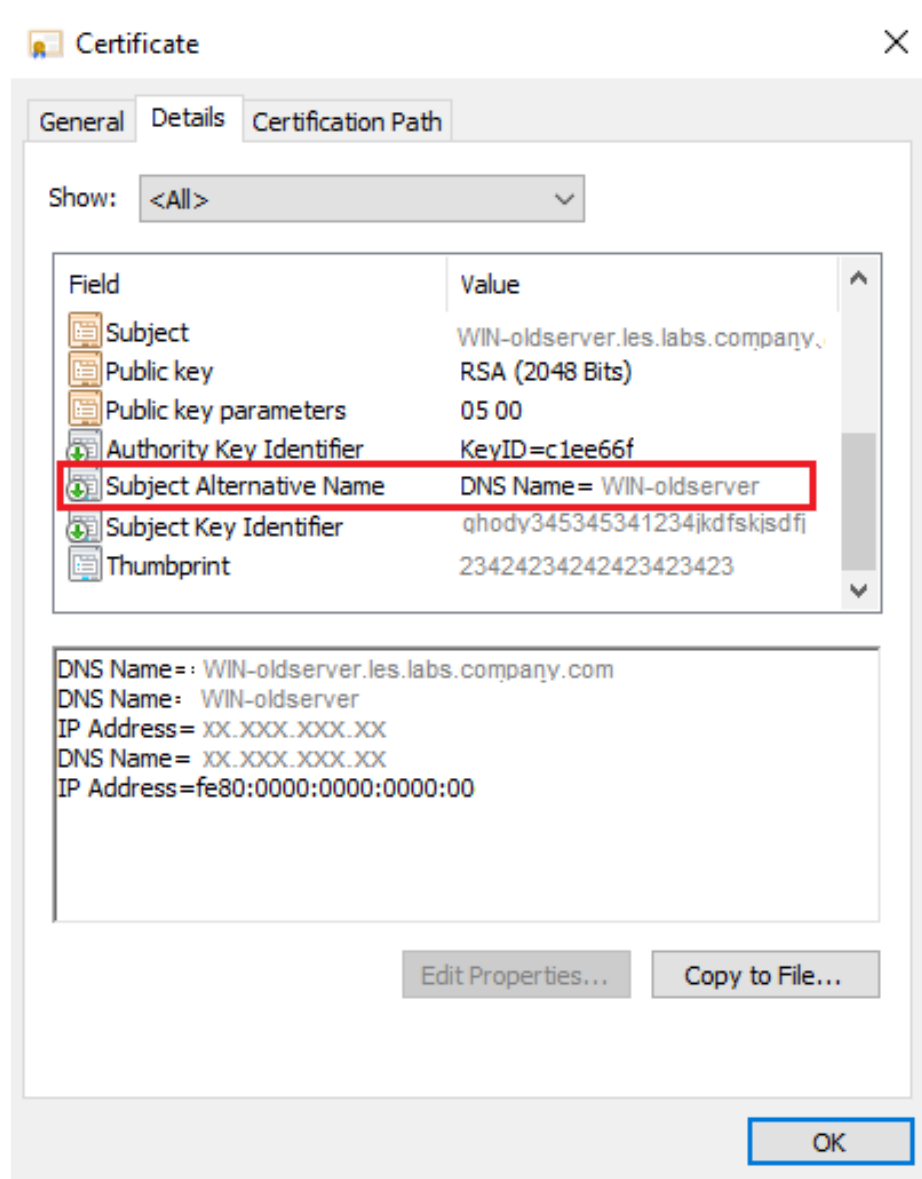
請在管理伺服器配置精靈中更改伺服器名稱，使憑證和管理伺服器中的伺服器名稱相符。

NOTE

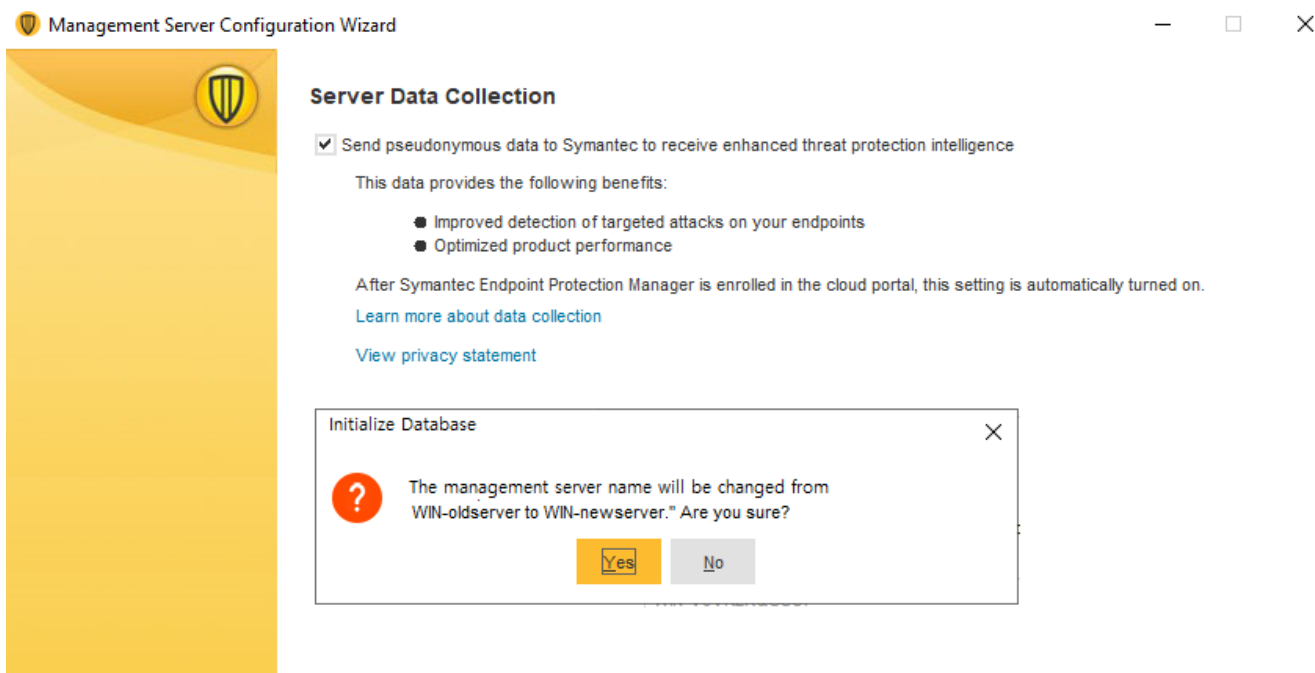
如果不執行此任務，則無法升級到 14.3 RU9 或更新版本。

重新配置管理伺服器名稱以符合伺服器憑證中的 **SAN**

1. 按一下「開始 > 所有程式 > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager 工具 > 管理伺服器架構精靈」。
2. 清除「使用還原檔案還原與之前已部署用戶端的通訊」選項，再按「下一步」。
復原檔案包括匯入新憑證之前的原始憑證檔。如果不清除此選項，則會覆寫匯入的憑證。
3. 在「指定網站名稱」面板中，將「伺服器名稱」更改為匯入的伺服器憑證中的相同名稱。
若要在憑證中尋找伺服器名稱，請執行以下步驟：
 1. 按兩下 <SEPM_Install>\apache\conf\ssl\server.crt 檔。
 2. 在「憑證」對話方塊 > 「詳細資訊」標籤上，複製「主旨備用名稱」或「IP 位址」欄的值。



4. 按「下一步」。
5. 保留每個面板中的剩餘預設值。
如果正確變更伺服器名稱，則在「伺服器資料收集」面板上將顯示以下訊息：



按下「是」。

6. 精靈完成資料庫更新之後，請再次嘗試升級。

如果正確完成了這些步驟，則不應看到封鎖升級的訊息。

如果無法登入，則管理伺服器名稱仍然與憑證中的名稱不相符。

其他問題

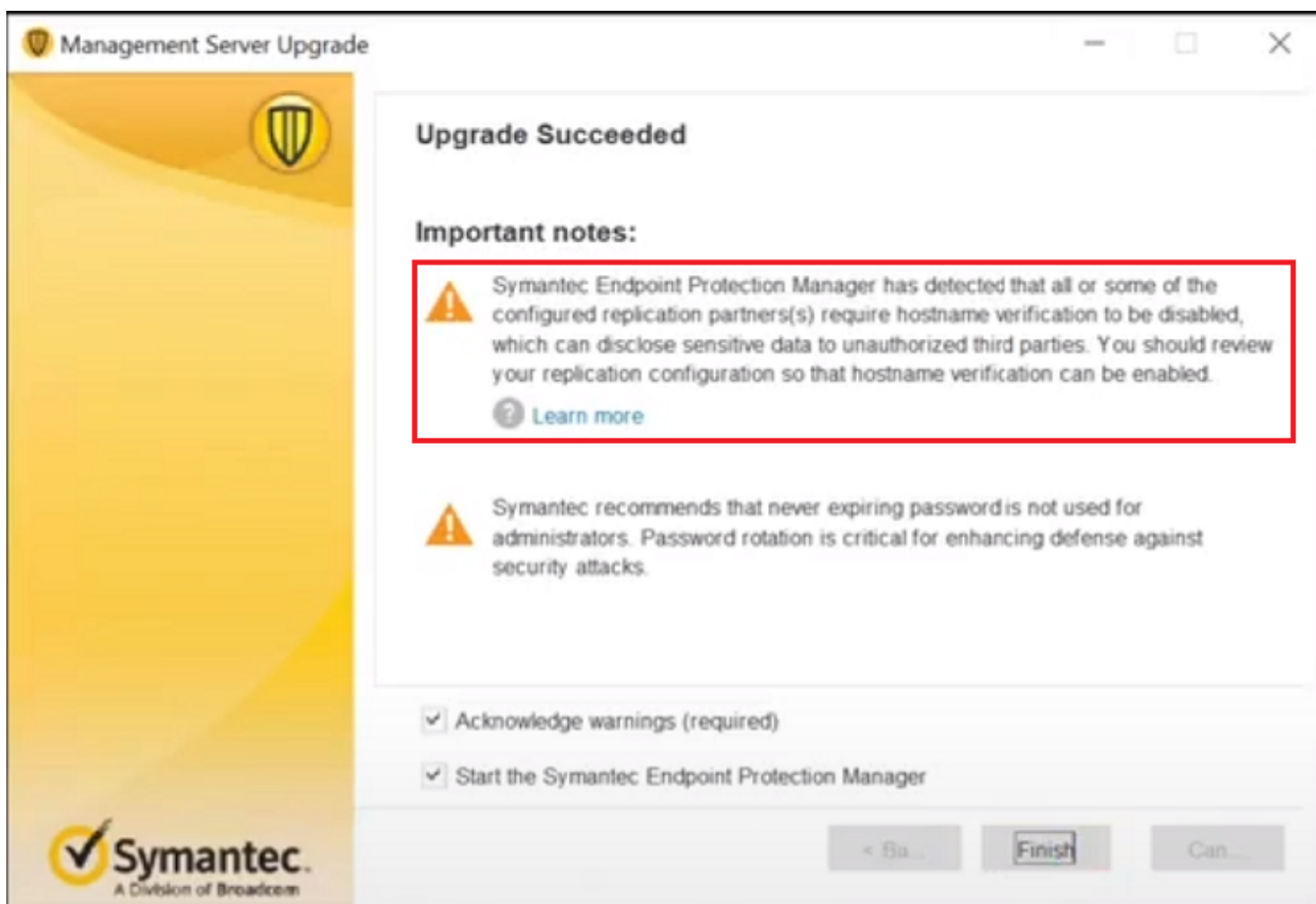
如果使用自簽署憑證而不是公開簽署憑證，請確保 SEPM 電腦信任該憑證。請參閱：

[接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證](#)

Symantec Endpoint Protection Manager 偵測到配置的複寫夥伴需要停用主機名稱驗證 (14.3 RU9 或更新版本)

升級至 Symantec Endpoint Protection Manager (SEPM) 14.3 RU9 或更新版本之後，您可能會在管理伺服器升級精靈的最後一個畫面上看到下列訊息。

```
Symantec Endpoint Protection Manager #####  
#####
```



發生下列其中一種情況時，會出現此訊息：

- 您已從 14.3 RU8 或更舊版本升級到 14.3 RU9 或更新版本。
- 本機管理伺服器指定的複寫合作夥伴主機名稱或 IP 位址與合作夥伴管理伺服器憑證中的一個或多個主旨備用名稱 (SAN) 不相符。

在升級期間，Symantec Endpoint Protection Manager 偵測到無法驗證您設定的複寫合作夥伴憑證主機名稱。因此，為了保持與複寫合作夥伴的連接，SEPM 會停用驗證。

但是，您應重新啟用複寫合作夥伴伺服器主機名稱的驗證，以讓與複寫合作夥伴的連接更加安全。

重新啟用合作夥伴伺服器主機名稱的驗證和更新

若要重新啟用驗證，請執行以下任務：

- 重新啟用管理伺服器驗證複寫合作夥伴伺服器主機名稱的要求。
- 確保複寫合作夥伴伺服器和本機管理伺服器使用相同的主機名稱。在複寫伺服器管理伺服器清單中變更複寫夥伴主機名稱。編輯該清單，使主機名稱或 IP 位址與各個複寫合作夥伴伺服器的憑證相符。

重新啟用合作夥伴伺服器主機名稱的驗證和更新

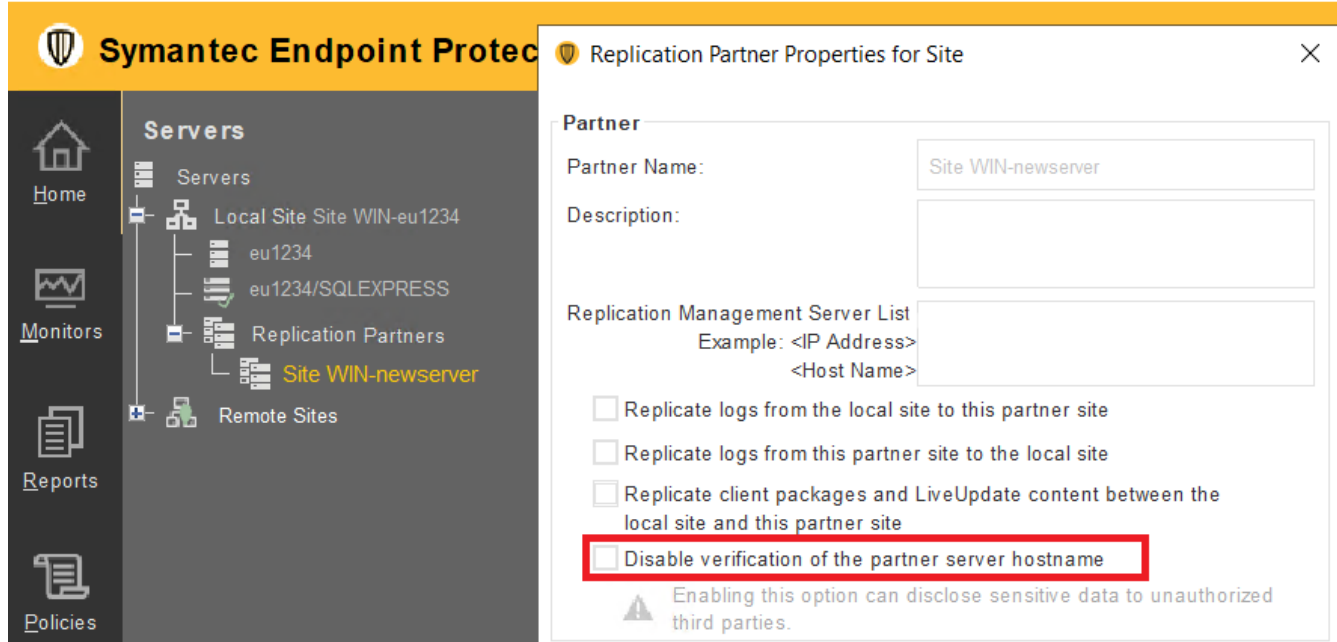
1. 按「管理」>「伺服器」>「複寫合作夥伴」。
(非必要)：若要驗證複寫是否正確執行，請右鍵按下複寫合作夥伴網站，然後按「立即複寫」。

請等待狀態框顯示以下訊息：##### sitename #####

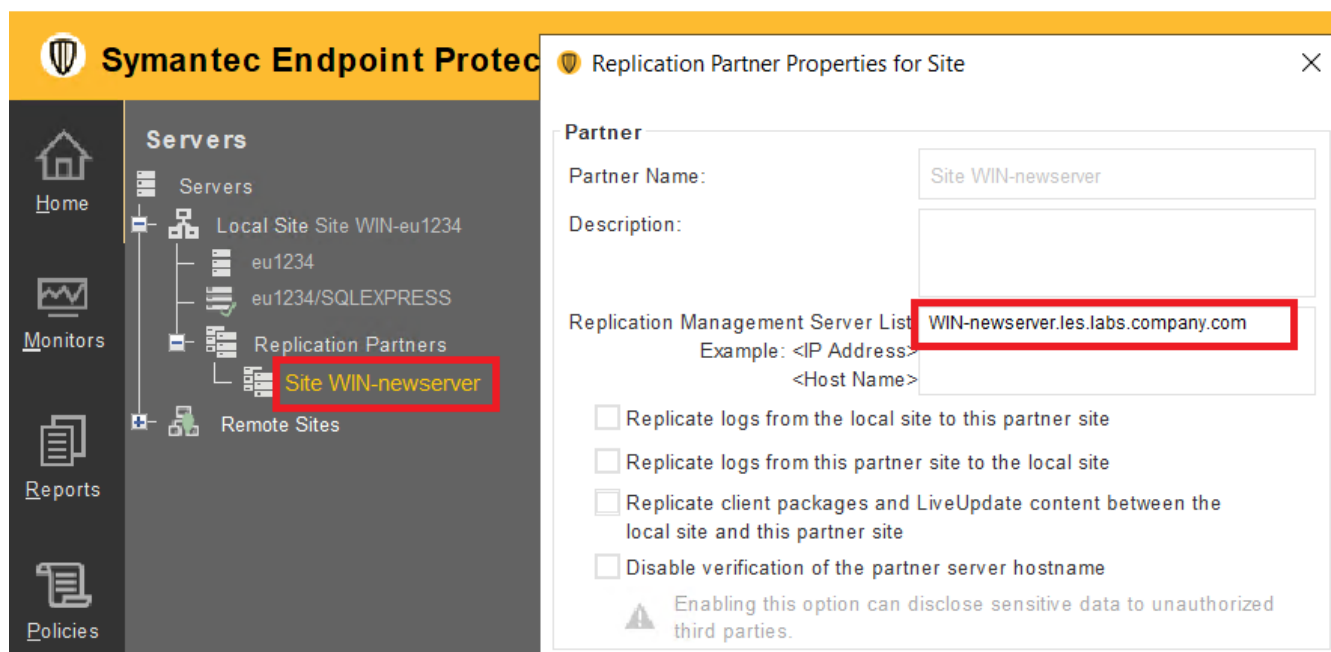
[立即遠端複製資料](#)

- 右鍵按下複寫合作夥伴網站，按「編輯複寫合作夥伴屬性」，清除「停用合作夥伴伺服器主機名稱驗證」選項。此步驟將重新啟用對複寫合作夥伴伺服器主機名稱的驗證。

 Symantec Endpoint Protection Manager



- 在複寫合作夥伴伺服器上，查看憑證中的 SAN，並確定哪個主機名稱是該複寫合作夥伴伺服器的正確主機名稱。可能有多個 SAN。有關如何查找 SAN 的資訊，請參閱：
[疑難排解：「您的伺服器憑證無效，因為電腦主機名稱或 IP 位址已變更」\(14.3 RU8 或更新版本\)](#)
- 在本機管理伺服器上，按「管理」>「伺服器」>「複寫合作夥伴」。
- 右鍵按下複寫合作夥伴網站，然後按下「編輯複寫合作夥伴屬性」。
- 在「網站 <主機名> 的複寫合作夥伴屬性」標籤上，將步驟 3 的複寫伺服器主機名稱貼到「複寫管理伺服器清單主機名稱欄位」。



7. 按一下「確定」。
8. (非必要)：若要驗證複寫是否正確執行，請右鍵按下複寫合作夥伴網站，然後按「立即複寫」>「是」>「確認」。
9. (非必要)：右鍵按一下複寫網站並按「檢查憑證」來驗證複寫伺服器是否信任憑證。
您應該會看到以下訊息：#####
10. 對所有剩餘的複寫合作夥伴重複這些步驟。

如需詳細瞭解您可能需要執行的其他憑證驗證，請參閱：[Symantec Endpoint Protection Manager 偵測到已架構的電子郵件伺服器需要停用憑證驗證](#)

疑難排解：「##### IP #####」(14.3 RU8 或更新版本)

登入到 Symantec Endpoint Protection Manager 時，您可能會看到以下錯誤訊息。

下表顯示該訊息以及解決問題的方式。

版本	訊息文本和解決方案
14.3 RU9 和更新版本	##### - ##### 因為您或管理員在登入時 (通常在遠端主控台) 收到信任憑證的提示時拒絕了該憑證，所以會出現此錯誤。此問題很少發生在預設信任伺服器憑證的本機主控台。 請參閱：接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證 - ##### IP ##### IP ##### Symantec Endpoint Protection Manager# 若您變更管理伺服器電腦的主機名稱或 IP 位址，而未更新憑證的主機名稱或 IP 位址，即會發生此錯誤。 當管理伺服器主機名稱 / IP 位址發生變更，或者新匯入的憑證具有不同的主機名稱 / IP 位址時，也可能發生這種情況。 請參閱：疑難排解伺服器名稱不符伺服器憑證時，Symantec Endpoint Protection Manager 會封鎖您登入或升級 (14.3 RU9 或更新版本) 在 14.3 RU8 和更新版本中，Symantec Endpoint Protection Manager 將驗證電腦主機名稱或 IP 位址是否與憑證所列內容相符。若新的主機名稱或 IP 位址不相符，Symantec Endpoint Protection Manager 會攔截您的登入。
14.3 RU8	##### IP ##### IP ##### Symantec Endpoint Protection Manager# 若您變更管理伺服器電腦的主機名稱或 IP 位址，而未更新憑證的主機名稱或 IP 位址，即會發生此錯誤。 請參閱：疑難排解伺服器名稱不符伺服器憑證時，Symantec Endpoint Protection Manager 會封鎖您登入或升級 (14.3 RU9 或更新版本)
14.3 RU7 及更舊版本	##### 您登入 Symantec Endpoint Protection Manager 時必須接受自簽署憑證。

NOTE

Symantec Endpoint Protection 用戶端會繼續與管理伺服器通訊。

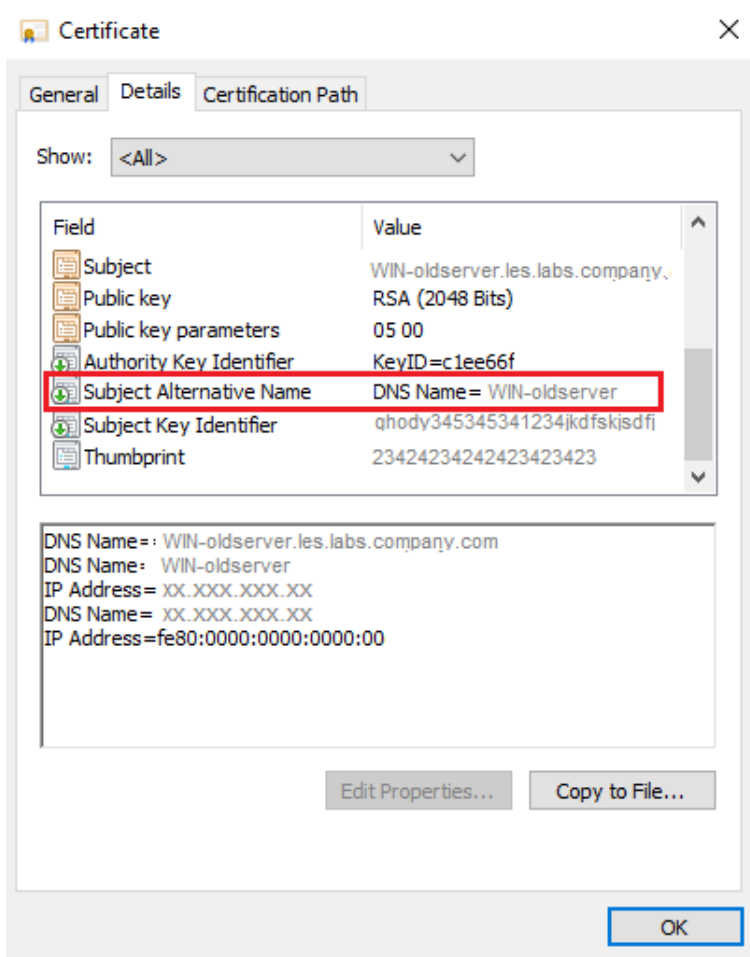
如果來自管理伺服器的主機名稱或 IP 位址與憑證不相符，請使用以下任務，暫時登入到管理伺服器。

NOTE

遵循此過程後，請確認已產生伺服器憑證，然後更新管理伺服器名稱。

變更電腦 IP 位址或主機名稱後登入管理伺服器

1. 變更主機名稱或 IP 位址後，請重新開啟管理伺服器電腦並按兩下 <SEPM_Install>\apache\conf\ssl\server.crt 憑證檔案。
2. 在「憑證」對話方塊 > 「詳細資訊」標籤上，複製「主旨備用名稱 (主機名稱)」或「IP 位址」欄的值。



3. 開啟 `C:\Windows\System32\drivers\etc\hosts` 檔案，新增 `127.0.0.1 <yourHostNameFromServer.crt>`，然後儲存該檔案。

其中 `<yourHostNameFromServer.crt>` 是前一步驟 `<SEPM_INSTALL>\apache\conf\ssl\server.crt` 檔案的原始主機名稱。在上一範例中，原始主機名為 `WIN-oldserver`。

↑ > This PC > Local Disk (C:) > Windows > System32 > drivers > etc

```
*hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
127.0.0.1 WIN-oldserver
```

4. 在 Symantec Endpoint Protection Manager 登入螢幕上，將新的伺服器主機名稱或 IP 位址變更為先前的管理伺服器主機名稱或 IP 位址，然後登入。

例如，如果原始主機名為 WIN-oldserver，新主機名為 WIN-newserver，請使用 WIN-oldserver 登入。

5. 產生伺服器憑證。請參閱：

[產生新的伺服器憑證](#)

請確保用戶端在您重新命名或變更 IP 位址後可以保持連線。

6. 更新憑證後，請使用新的主機名稱或 IP 位址登入到 Symantec Endpoint Protection Manager。

7. 從 14.3 RU9 開始，請重新配置 Symantec Endpoint Protection Manager 以使用新的 SEPM 主機名稱。

如果您在「伺服器 > 本機網站 > 管理伺服器」狀態螢幕上看到以下錯誤：No subject alternative DNS name matching <hostname>，請重新配置 Symantec Endpoint Protection Manager。

例如，您可以將 SEPM 從 WIN-oldserver 重新命名為 WIN-newserver。

[在變更電腦的 IP 位址和主機名稱後重新架構 Symantec Endpoint Protection Manager](#)

排除管理伺服器主機名變更時出現的問題

問題	解決方案
重新設定管理伺服器以使伺服器名稱與伺服器憑證中的名稱相符之後，您可能會看到以下錯誤：##### (SSL) ##### 如果出現以下情況，則會發生此錯誤： - 管理伺服器使用預設 SQL Express 資料庫。 - 您匯入了僅限第三方完全合格網域名稱 (FQDN) 的憑證。 出現此問題的原因是 Apache Tomcat 沒連接到 SQL Express 資料庫。	執行步驟 6 到 8： 重新架構 Symantec Endpoint Protection Manager 並產生 SQL Server Express 或 SQL Server 資料庫的憑證
如果 Symantec Endpoint Protection Manager 具有複寫合作夥伴，複寫可能會失敗。scm-server-0.log 會顯示以下任一錯誤。 ##### 或： HREAD 28 ### javax.net.ssl.SSLHandshakeException##### ### IP ## xx.xx.xx.xx.xx #####	請參閱： - 使用工具來解決此問題：將 Endpoint Protection Manger 升級到 14.3 RU8 之後，複寫失敗 將 Endpoint Protection Manager 升級到 14.3 RU8 之後，登入失敗以及意外的伺服器錯誤 - 對於憑證僅對 FQDN 有效的情况：使用僅限 FQDN 的憑證時，將 SEPM 升級到 Ru8 後出現複寫錯誤
管理伺服器無法產生報告並顯示以下錯誤： com.sygate.scm.server.task.SecurityAlertNotifyTask javax.net.ssl.SSLHandshakeException: ##### <servername> ##### DNS ###	請參閱： 排定報告在將 Endpoint Protection Manager 升級到 14.3 RU8 後停止執行

停止及啟動管理伺服器服務

在升級之前，您必須手動停止您網站中每部管理伺服器上的 Symantec Endpoint Protection Manager 服務。升級之後，服務會自動啟動。

WARNING

若不在伺服器升級前停止 Symantec Endpoint Protection Manager 服務，則有使現有 Symantec Endpoint Protection 資料庫損毀的風險。

NOTE

如果您停止管理伺服器服務，用戶端就無法再與之連線。如果用戶端需要與管理伺服器通訊以連線到網路，則在重新啟動此服務之後，才能允許這些用戶端存取。

例如，用戶端必須與管理伺服器通訊，才能通過「主機完整性」檢查。

如需詳細資訊，請參閱：

[升級至新版本](#)

透過控制面板停止和啟動管理伺服器服務

- 若要停止 Symantec Endpoint Protection Manager 服務，請按下「開始」>「設定」>「控制台」>「系統管理工具」>「服務」。
- 在「服務」視窗的「名稱」下方，捲動然後按下滑鼠右鍵：
Symantec Endpoint Protection Manager
Symantec Endpoint Protection ManagerAPI 服務
Symantec Endpoint Protection ManagerWebserver
- 按下「停止」。
- 關閉「服務」視窗。

WARNING

關閉「服務」視窗，否則升級會失敗。

5. 為所有 Symantec Endpoint Protection Manager 的安裝重複此程序。

NOTE

若要啟動 Symantec Endpoint Protection Manager 服務，請再次遵循此程序，但按下「啟動」。

透過指令停止和啟動管理伺服器服務

1. 若要從指令提示 (cmd) 停止 Symantec Endpoint Protection Manager 服務，請輸入：

```
net stop semsrv
net stop semapisrv
net stop semwebsrv
```

2. 若要從指令提示啟動 Symantec Endpoint Protection Manager 服務，請輸入：

```
net start semsrv
net start semapisrv
net start semwebsrv
```

防止在升級期間複寫

您應該確定任何管理伺服器上未進行複寫，而管理伺服器會以複寫夥伴形式架構為所升級的管理伺服器。如果遠端複製夥伴在升級期間啟動遠端複製，可能會產生無法預期的結果。

若要防止在升級期間複寫，請執行下列其中一個工作：

- 重新排程在升級期間以外的時間進行複寫。賽門鐵克建議使用此方法，因為它較為簡單。
- 在升級之前暫時中止複寫，並在複寫結束之後予以還原。

重新排程複寫

修改排程的優點是其他站台不會進行複寫，而是會在升級用戶端之前繼續服務用戶端。升級完成之後，站台可以強制執行一次性複寫來測試複寫，並將排程變更回先前設定的排程和頻率。

按照下列最佳實務準則來修改排程：

- 記錄現有排程和設定。
- 變更排程，防止在升級時段期間進行複寫，方法是排程它在未來或不同的日期執行。
- 強制複寫，讓所有複寫夥伴或站台選取排程。

如需詳細資訊，請參閱：

[變更遠端複製頻率和內容](#)

中止和還原複寫

您必須登入 Symantec Endpoint Protection Manager 並在至少兩個站台中止遠端複製。

WARNING

中止複寫與永久刪除複寫夥伴關係不同。如果您刪除關係，然後重新安裝管理伺服器，則管理伺服器會執行完整遠端複製而非增量遠端複製。請參閱：[刪除網站](#)

中止和還原複寫

1. 在主控台中，按一下「管理員 > 伺服器」。
2. 在「本機站台」>「伺服器」下方，展開「複寫夥伴」並選取管理伺服器。
3. 以滑鼠右鍵按一下管理伺服器，然後按一下「刪除複寫夥伴」。

-
4. 按下「是」。
 5. 在遠端複製資料的所有網站中重複此程序。
 6. 還原複寫，並重新啟動管理伺服器服務。請參閱：
[還原複寫](#)

更多資訊

- [Endpoint Protection 14 的升級最佳實務準則](#)
- [升級至新版本](#)

還原複寫

升級具有遠端複製關係的所有管理伺服器之後，重新新增遠端複製夥伴。還必須重新新增已架構用於容錯移轉和負載平衡的管理伺服器。

僅在最先升級管理伺服器的電腦上重新新增遠端複製夥伴。此外，升級的管理伺服器先前必須是相同站台陣列中的遠端複製夥伴。

重新新增遠端複製夥伴後，Symantec Endpoint Protection Manager 會使資料庫保持一致。不過，某些變更可能相互衝突。請參閱：

[如何解決遠端複製期間網站之間的資料衝突](#)

如果您擁有兩個單獨的非遠端複製網站，亦可使用此選項將其中一個網站轉換為透過其他網站遠端複製的網站。

還原複寫

1. 在主控台上，按一下「管理員 > 伺服器」。
2. 在「伺服器」下方，展開「本機網站」，然後在「工作」下方，按一下「新增複寫夥伴」。
3. 在「歡迎使用」面板中，按「下一步」。
4. 在「遠端據點資訊」面板中，輸入第二個管理伺服器的 IP 位址或主機名稱、系統管理員的登入資訊，然後按「下一步」。
依預設，系統管理員的使用者名稱為 `admin`。
5. 設定複寫排程，然後按「下一步」。
6. 檢查要複寫的項目，然後按「下一步」。
用戶端套件遠端複製會使用大量的流量和硬碟空間。
如果您按一下「是」，則管理伺服器會在兩個複寫夥伴之間執行完整資料複寫。
7. 當出現一則訊息詢問是否已還原夥伴網站上的資料庫時，請按下列其中一個選項：
 - 按一下「否」僅複寫自此夥伴關係停用之後變更的資料。賽門鐵克建議您選取此選項，尤其是在您的網路具有低頻寬的情況下。
 - 按一下「是」在兩個複寫夥伴之間執行完整資料複寫。
8. 按下「完成」。
9. 為所有以此電腦遠端複製資料的電腦重複這個程序。
確定在重新啟動複寫之後重新啟動管理伺服器服務。

更多資訊

- [Endpoint Protection 14 的升級最佳實務準則](#)
- [升級至新版本](#)

選擇升級用戶端軟體的方法

您可以利用多種方式來升級用戶端。您應採用的方法視環境和目標而定。例如，您可能擁有大量用戶端或群組，或者執行不同用戶端版本的電腦。

某些方法可能耗時達 30 分鐘。因此，您可以在大多數使用者未登入其電腦時，升級用戶端軟體。

Table 40: 升級用戶端軟體的方法

方法	使用時機	何時不使用
自動升級 (建議較小的環境使用)	- 當您擁有的用戶端數目較少時，例如 5,000 個或更少的用戶端。 - 當您需要將升級排程為在升級不中斷使用者工作的情況下執行時。 - 當您使用 Symantec Endpoint Protection Manager (而非第三方應用程式) 部署用戶端安裝套件時。 - 當您需要升級 Windows 或 Mac 用戶端，但不升級 Linux 用戶端時。 - 當您想要採用簡單的升級方法時。 如需詳細資訊，請參閱： 使用自動升級來升級用戶端軟體	- 當您擁有大量用戶端時。此方法不夠靈活。 - 當您擁有大量群組時，因為在精靈中個別按下每個群組相當耗時。 - 當您設定複雜的升級排程 (需要較高精細度) 時。 - 當您需要升級 Linux 用戶端時。請參閱： 如何將 Symantec Endpoint Protection Linux 用戶端部署為已複製磁碟機影像的一部分
匯出用戶端安裝套件 (建議較大的環境使用)	- 當您手動 (而非使用 Symantec Endpoint Protection Manager) 部署用戶端安裝套件時。 - 當您使用現有第三方部署應用程式 (而非使用 Symantec Endpoint Protection Manager) 部署用戶端安裝套件時。若要使用此方法，您應已安裝此基礎架構。 - 當您需要升級 Windows 用戶端、Mac 用戶端及 Linux 用戶端時。 如需詳細資訊，請參閱： 匯出用戶端安裝套件 使用第三方工具安裝 Windows 用戶端軟體	當您通常使用 Symantec Endpoint Protection Manager 更新用戶端時。
用戶端部署精靈	- 當您擁有的用戶端數目較少時，例如 250 個以下用戶端。 - 當您使用 Symantec Endpoint Protection Manager (而非第三方應用程式) 部署用戶端時。 - 當您想要採用較簡單的升級方法時。 使用「新套件部署」。請參閱： 使用遠端推送安裝 Symantec Endpoint Protection 用戶端	當您擁有大型網路環境時，因為此方法不夠靈活。
從 Broadcom 下載管理 頁面下載用戶端安裝檔。	- 當您想要在少數特定情況下一次升級數個用戶端時。例如： - 如果某個問題在數個安裝有舊版用戶端的電腦上出現，更新版本修正了該問題。 - 如果您要升級較少數目的用戶端，但不想升級管理伺服器。 - 當您需要升級 Windows、Mac 及 Linux 用戶端時。 - 當您必須直接在電腦上部署或使用第三方部署應用程式 (而非使用 Symantec Endpoint Protection Manager) 部署用戶端時。 您可以從「下載管理」頁面下載獨立的所有用戶端安裝檔。若要這麼做，請執行下列動作： - 前往：Symantec 入門指南 - 選取「內部部署安全產品」。 如需詳細資訊，請參閱： 安裝非受管 Windows 用戶端	如果您升級具有現有受管用戶端之電腦上的用戶端，這些受管用戶端會保持受管狀態。但是，如果您部署至不含現有用戶端的新電腦，此方法會僅安裝非受管用戶端。您必須稍後將用戶端轉換為受管用戶端，才能連線至管理伺服器。請參閱： 如何在用戶端電腦上取代用戶端伺服器通訊檔案？ 手動匯出用戶端伺服器通訊檔案 (Sylink.xml)

更多資訊

[升級至新版本](#)

使用自動升級來升級用戶端軟體

概述

自動升級可讓您自動升級群組中 Windows 或 Mac 用戶端上的 Symantec Endpoint Protection 用戶端軟體。

Windows 標準用戶端可使用自動升級接收 Symantec Endpoint Protection Manager 建立的增量升級套件。此套件比完整安裝套件小。內嵌的 Windows 或是 VDI 用戶端始終接收完整安裝套件。這些用戶端不會在安裝程式快取中保留安裝程式複本。Mac 用戶端始終接收完整安裝套件。

自動升級最佳實務

使用下列最佳實務來使用自動升級：

- 嘗試在產品網路中升級大量用戶端之前，先測試自動升級程序。如果沒有測試網路，您可以在正式網路中建立一個測試群組。針對這類測試，您可以將幾個非至關重要的用戶端新增至測試群組，然後使用「自動升級」來升級這些用戶端。
- 若要減少尖峰時間的頻寬，請在「使用套件升級用戶端」精靈中，排程在營業時間後執行「自動升級」，尤其是針對含縮減大小用戶端的用戶端群組。針對廣域網路，您應該也設定遠端用戶端，以從遠端 Web 伺服器接收升級套件。
- 自 14.3 RU2 起，LiveUpdate 會下載具有重要修正或安全修正的用戶端安裝套件，讓您可以在不變更用戶端版本的情況下進行安裝。例如，如果您已安裝 14.3 RU2 版次 4870，而且 14.3 RU2 版次 5200 變為可用，則可以使用自動升級精靈來安裝版次 5200。您不需要升級管理伺服器，而只需要升級用戶端。在每次升級之後，您必須重新啟動 14.3 RU2 和更舊版本的用戶端。對於 14.3 RU3 和更新版本，請參閱：

[從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)

- 在 14.3 RU2 和 14.3 RU3 中，Symantec Endpoint Protection 用戶端和 Symantec Endpoint Protection Manager 只翻譯成下列語言：英文、法文、西班牙文、葡萄牙文和日文。在 14.3 RU4 中，SEP 已新增簡體中文和繁體中文。如果您使用其中一種支援的語言，則不需要採取任何動作；您可以照常升級。如果先前的用戶端語言無法使用，則您可以將用戶端語言自動升級為英文。如果您選擇非英文語言，則不會升級語言不受支援的用戶端。預設會關閉此選項。若要啟用此選項，請按一下「用戶端」頁面 > 「安裝套件」頁面，然後按一下「新增用戶端安裝套件」> 「如果無法使用不支援的語言，則請升級至英文」。此選項僅適用於 Windows 用戶端。

[將 Symantec Endpoint Protection 14.3 RU2+ 升級為支援的語言](#)

- 因為自動升級最初包含在具有 Symantec Endpoint Protection 14 的 Mac 用戶端中，所以您無法從 14 版之前的版本使用自動升級進行升級。
- 升級 Symantec Endpoint Protection Manager 後，在主控台中至少執行一次 LiveUpdate，然後使用自動升級來升級用戶端。

[確認 Symantec Endpoint Protection Manager 具有最新內容](#)

- 只有在符合下列條件時，自動升級才會在用戶端電腦上安裝應用程式強化功能 (14.2 和更新版本)：
 - 當您執行「使用套件升級用戶端」時，必須啟用「更新時保留現有用戶端功能」。此設定預設為啟用。
 - 用戶端電腦無法安裝 Symantec Data Center Security 代理程式。
 - 病毒和間諜軟體防護功能目前已安裝，並選取進行升級。
- 如果您稍後想要在用戶端安裝之後變更 Windows 用戶端安裝類型「標準用戶端」、「內嵌式或 VDI」或「暗網」，則必須先解除安裝現有用戶端軟體、重新架構這些設定，然後重新安裝新的用戶端套件。您無法使用自動升級來變更此設定。

使用自動升級來升級用戶端軟體

- 在主控台中，按下「管理員」> 「安裝套件」。
- 在「工作」下方，按下「使用套件升級用戶端」。
- 在「升級用戶端精靈」面板中，按「下一步」，選取適當的用戶端安裝套件，然後按「下一步」。
- 選取包含您要升級之用戶端電腦的群組，然後按「下一步」。
- 從下列選項中選取用戶端應從何處下載套件：
 - 若要從 Symantec Endpoint Protection Manager 伺服器進行下載，請按下「從管理伺服器下載」。
 - 若要從位於需要更新之電腦本機的 Web 伺服器進行下載，請按下「從下列 URL (http 或 https) 下載」。在提供的欄位中輸入用戶端安裝套件的 URL。
- 按下「升級設定」以指定升級選項。
- 在「一般」標籤的「用戶端設定」下，從下列選項 (視用戶端作業系統而定) 中選擇：
 - 對於 Windows：

-
- 在「選取此套件的版本」中，選擇版次 (自 14.3 RU2 起)。
 - 請使用下拉式功能表選取「更新時保留現有用戶端功能」和「安裝設定」選項。如果取消選取「更新時保留現有用戶端功能」，您可以選擇在升級時新增或移除功能。
- 對於 Mac，請使用下拉式功能表選取「安裝設定」的選項。
 - 對於 Windows，「內容選取」可讓您在安裝套件中包含內容。如果包含內容，套件雖然較大但用戶端在安裝後就能立即擁有最新內容。如果不包含內容，套件雖然較小但用戶端必須在安裝後取得內容更新。
- 您也可以新增選擇性升級排程。如果未設定排程，自動升級程序會在精靈完成後開始。
8. 在「通知」標籤上，自訂使用者通知設定。
您可以自訂升級時用戶端電腦上顯示的訊息。您也可以允許使用者延後升級。
 9. 按下「確定」，再按「下一步」。
 10. 在「升級用戶端精靈完成」面板中，按下「完成」。

確認用戶端軟體的版本號碼

1. 升級完成後，您可以透過下列其中一種方式檢查版本以確認升級是否成功：
 - 在主控台中，按下「用戶端 > 用戶端」，選取適當的群組，並將檢視變更為「用戶端狀態」。
 - 在 Windows 用戶端上，於 Symantec Endpoint Protection 用戶端介面中按下「說明」>「關於」。
 - 在 Mac 用戶端上，開啟 Symantec Endpoint Protection 用戶端介面。在功能表列中，按一下「**Symantec Endpoint Protection > 關於 Symantec Endpoint Protection**」。

依據預設，用戶端會在安裝後重新啟動。對於 14.3 RU2 和更舊版本的用戶端，必須在升級之後重新啟動電腦。您可以在群組的一般設定中架構重新啟動選項，以控制群組中的用戶端在自動升級後的重新啟動方式。您也可以從管理伺服器執行重新啟動指令，隨時重新啟動用戶端。

[從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)

[將升級設定套用至其他群組](#)

架構用戶端升級政策 (選擇性)

自 14.3 RU3 起，您可以在不同的時間，針對測量的遞送升級安全群組中的一小部分用戶端。您可以使用用戶端升級政策和下列位置條件，將目標設為這些子群組：主機名稱、使用者名稱、群組名稱、檔案是否存在或作業系統。例如，使用者離線時，您可以在夜間升級 Windows 8 電腦。

用戶端升級政策提供更細化的排程設定，而這些設定會覆寫自動升級精靈中的升級排程設定。此政策會保留所有其他自動升級精靈設定。您可以將用戶端升級政策套用至已套用自動升級精靈的相同群組。

[使用用戶端升級政策升級用戶端軟體](#)

將自動升級設定套用至其他群組

您可以將現有自動升級用戶端安裝套件的升級設定從一個群組複製到另一個群組。如果複製升級設定，則無須為每個群組個別建立套件設定。

此選項會複製下列用戶端安裝套件設定：

- 用戶端功能集
- 「更新時保留現有用戶端功能」已啟用還是已停用
- 用戶端安裝設定
- 內容選取
- 下載來源
- 升級排程
- 「通知」標籤中的設定和訊息文字

在自動升級期間，Windows 設定會套用至 Windows 用戶端，Mac 設定會套用至 Mac 用戶端。這些設定也會套用至任何加入群組的新用戶端。

如果將已複製設定套用至已指派給目標群組的套件，則已複製設定會覆寫目標群組的現有設定。如果目標群組沒有指派套件，則此選項會使用已複製設定新增用戶端安裝套件。

套用升級設定到其他群組

1. 在主控台中，執行下列其中一項工作：

- 按下「用戶端」>「安裝套件」、選取群組，然後在「工作」下，按下「套用目前的部署設定到其他群組」。
- 按下「用戶端」，在群組上按下滑鼠右鍵，然後按下「複製部署設定」。

2. 在「複製部署設定」對話方塊中，按下新群組、按下「確定」，然後按下「是」。

更多資訊

使用自動升級來升級用戶端軟體

使用用戶端升級政策升級用戶端軟體

您可以將升級套件派送和安裝至用戶端群組內一小部分的用戶端 (14.3 RU2 用戶端和更新版本)。用戶端升級政策可讓您排程在多個日期和時間進行升級。此交錯升級可讓您在預先決定的時間發行軟體，並協助您在將其遞送給所有用戶端之前測試升級。

使用位置，指定用戶端必須符合才能使用新排程進行升級的條件。例如，使用者離線時，您可以在週末升級 Windows 10 電腦。

何時使用用戶端升級政策？

用戶端升級政策提供自動升級精靈以外的更進階排程選項。此政策在已架構自動升級的群組上執行。

下表說明單獨使用自動升級精靈與其他用戶端升級政策的差異。

Table 41: 自動升級精靈與用戶端升級政策

僅自動升級精靈	用戶端升級政策
對於 Windows 用戶端 14.3 版 RU2 MP1 和更舊版本。這些用戶端會忽略用戶端升級政策設定，以及從自動升級精靈中的「一般」標籤 > 「升級排程」設定來取得其排程設定。 您可以在用戶端之 config.xml 檔案的預設位置找到升級排程設定：C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\。	對於 Windows 用戶端 14.3 RU2 和更新版本的用戶端。這些用戶端會忽略自動升級精靈排程設定；所有其他自動升級設定都適用。
指定升級的開始和結束時間，以及可派送下載套件的天數。	指定： • 升級的開始和結束時間。 • 可派送下載套件的天數。 • 要在星期幾升級。 • 升級可延遲的天數。 • 如果在派送時段錯過升級，則可以重試升級。
請不要使用位置偵測	可讓您使用下列位置偵測條件來升級一小部分的用戶端：主機名稱、使用者或群組名稱、指定的檔案或作業系統。 位置偵測為低頻寬環境中的用戶端提供更好的選擇。
升級 Windows 和 Mac 用戶端，而不是 Linux 用戶端。	升級 Windows 用戶端，而不是 Mac 或 Linux 用戶端。
從 Symantec Endpoint Protection Manager、群組更新提供者或 LiveUpdate，下載並安裝完整用戶端安裝套件。	從 Symantec Endpoint Protection Manager 或群組更新提供者而非 LiveUpdate，下載並安裝完整用戶端安裝套件。
從 LiveUpdate 下載任何用戶端產品更新或用戶端修補程式，包括生產 LiveUpdate 或 LiveUpdate Administrator。	不要從 LiveUpdate 下載任何用戶端產品更新或用戶端修補程式。用戶端修補程式會使用「LiveUpdate 設定」政策中的排程。

下載並安裝 Symantec Endpoint Security 雲端主控台所管理的 Symantec Agent 套件。	不要下載並安裝 Symantec Endpoint Security 雲端主控台所管理的 Symantec Agent 套件。

架構用戶端升級政策

步驟 1：使用自動升級精靈將用戶端安裝套件指派給群組

架構用戶端安裝套件，並將其指派給用戶端群組。您可以接受預設「升級排程」設定。

[使用自動升級來升級用戶端軟體](#)

步驟 2：為群組建立多個位置

設定位置偵測，以讓用戶端切換到指示用戶端升級的位置。

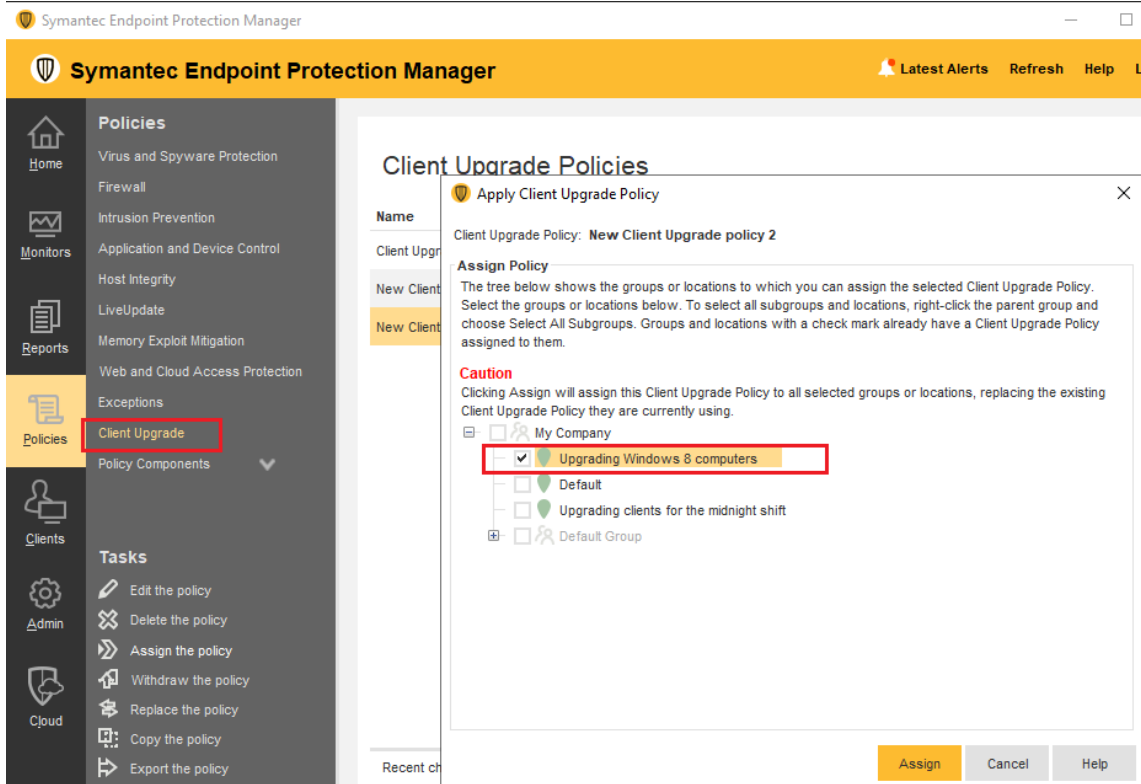
1. 在主控台中，按一下「用戶端」>「政策」，然後選取群組。
2. 在「政策」標籤上，按一下「管理位置」，然後使用下列任何準則來新增位置：主機名稱、使用者名稱、群組名稱、檔案存在或作業系統。

[將位置新增到群組](#)

[指定位置條件](#)

步驟 3：建立用戶端升級政策並將它指派給位置

1. 在主控台中，按一下「政策」>「用戶端升級」，以建立用戶端升級政策。
2. 在「概觀」窗格中，按一下「啟用此政策」。
如果您未啟用用戶端升級政策，則用戶端會使用您在步驟 1 所新增之用戶端安裝套件中的「升級排程」選項。
3. 在「排程」窗格中，指定下列建議的選項：
 - 從...升級至
 - 允許升級這些選項設定管理伺服器檢查新用戶端升級套件並將其下載到用戶端的頻率。
4. 按一下「確定」，並將政策指派至您在步驟 2 所建立的其中一個位置。



管理伺服器將 policy.xml 檔案下載至用戶端之後，用戶端會切換位置。

用戶端會根據您在用戶端升級政策中指定的排程來進行升級。

將 Symantec Endpoint Protection 14.3 RU2+ 升級為支援的語言

如果您從不受支援的語言升級用戶端或 SEPM，則可以升級為支援的語言或英文。

在 14.3 RU1 和更舊版本中，Symantec Endpoint Protection Manager (SEPM) 和用戶端已支援 12 種語言。在以後的版本中，語言支援變更如下：

- 在 14.3 RU2 中，語言支援已減少為英文、巴西葡萄牙文、法文、日文和西班牙文。
- 在 14.3 RU4 中，SEP 已新增簡體中文和繁體中文。
- 在 14.3 RU5 中，SEP 已新增捷克文、波蘭文和俄文。

將 Symantec Endpoint Protection Manager 從支援的語言升級為不受支援的語言

升級具有不受支援 Symantec Endpoint Protection Manager 語言的 SEPM 時，會將 SEPM 自動升級為英文。不過，您可以將 SEPM 升級為英文以外的受支援語言（例如，從義大利文到法文）。

SEPM 使用兩個元件來顯示語言：資源檔案和系統地區設定。若要以英文之外的一種受支援語言顯示 SEPM，SEPM 必須同時具有相同語言的資源檔案和系統格式地區設定。如果資源檔案和系統地區設定不符合受支援的語言，則會以英文安裝 SEPM。

NOTE

賽門鐵克建議您在升級管理伺服器之前遵循此步驟。

將系統格式地區設定設定為目標移轉語言

1. 按一下「開始」->「控制台」->「時鐘和地區」->「地區」->「格式」標籤 (Windows 10 和 Windows Server 2019)。此步驟會根據 SEPM 執行的 Windows 版本而變更。

2. 在「格式」下拉式清單中，選擇目標語言，然後按一下「確定」。

您可以為目標語言選擇任何格式。例如，如果您要升級為法文，則選擇法文 (阿爾及利亞) 還是法文 (比利時) 並沒有差別。

將用戶端從不受支援的語言升級為受支援的語言

若要將語言不受支援的用戶端自動升級為英文，請在自動升級精靈中勾選「如果不支援用戶端語言，請將 14.3+ 用戶端升級至英文」選項。如果您未勾選此選項，則不會自動升級語言不受支援的用戶端。只有 Symantec Endpoint Protection Manager 英文版才提供此選項。

Mac：必須手動或使用桌面管理工具，將 Mac 用戶端從不受支援的語言升級為受支援的語言。

Linux：Linux 只會保留翻譯成日文。

NOTE

如果您自動將語言不受支援的用戶端升級為英文，則用戶端會繼續使用英文顯示定義的日期設定 (14.3 RU1 和更新版本)。若要解決此問題，請解除安裝舊版用戶端，並手動安裝新的用戶端安裝套件。此外，應該修正自動升級的用戶端。[SEP-72481]

如需詳細資訊，請參閱：

[使用自動升級來升級用戶端軟體](#)

在 Windows 用戶端上安裝 Endpoint Protection 用戶端修補程式

什麼是用戶端修補程式以及運作方式為何？

用戶端修補程式是 Symantec Endpoint Protection Windows 用戶端的軟體修補程式，可更正用戶端程式碼中存在的產品缺陷或功能問題。Symantec 提供用戶端修補程式來修正問題，並將其上載到 14.3 RU2 (版本號碼 14.3.4615.2000) 或更新版本中的 LiveUpdate 伺服器。用戶端修補程式就像任何其他類型的內容 (如 IPS 特徵或病毒和間諜軟體定義檔) 一樣。

Symantec 提供用戶端修補程式來修正問題，並將其上載到 14.3 RU2 (版次號碼 14.3.4615.2000) 或更新版本中的 LiveUpdate 伺服器。然後，可使用 LiveUpdate 伺服器、管理伺服器或群組更新提供者 (GUP)，採用與其他內容相同的方式將修補程式下載到用戶端。請參閱：

[選擇派送方法以更新用戶端上的內容](#)

NOTE

用戶端修補程式與維護修補程式 (MP) 或發行更新 (RU) 不同。用戶端修補程式只處理用戶端缺陷，並透過 LiveUpdate 進行傳送。維護修補程式可提供其他更新或功能 (例如，為新的作業系統提供支援)，並透過 Broadcom「[下載管理](#)」頁面以完整安裝下載形式傳送。在 14.3 RU2 和更新版本中，用戶端修補程式的內容會與產品更新的内容相同。不過，產品更新包含在完整用戶端安裝套件中，而用戶端修補程式只包括 Delta 檔案。請參閱：

[關於 Endpoint Protection 發行類型和版本](#)

另請參閱：

[使用自動升級來升級用戶端軟體](#)

用戶端修補程式如何使用語言？

用戶端修補程式的語言必須與管理伺服器語言相符。例如，管理法文 (支援) 和德文 (不支援) 用戶端的法文版管理伺服器只提供法文版用戶端的用戶端修補程式。在 14.3 RU2 或更新版本中，您必須讓 AutoUpgrade 在德文版用戶端上安裝英文版安裝套件和英文版用戶端修補程式。如需如何將用戶端從不支援語言升級到所支援語言的詳細資訊，請參閱：

[將 Symantec Endpoint Protection 14.3 RU2+ 升級為支援的語言](#)

在 Windows 電腦上安裝用戶端修補程式

LiveUpdate 預設會將用戶端修補程式下載到 Symantec Endpoint Protection Manager。不過，在受管用戶端或未受管用戶端上，不會自動下載和安裝用戶端修補程式。不論您使用 Symantec Endpoint Protection Manager、LiveUpdate 還是群組更新提供者，在受管用戶端上，您都必須選取要安裝的用戶端修補程式。

用戶端下載並安裝用戶端修補程式之後，會立即執行修補程式 (14.3 RU2 和更新版本)。對於 14.3 RU1 和更舊版本，除非重新啟動用戶端，否則會繼續執行未經修補的舊版用戶端。用戶端一般使用者必須重新啟動電腦，或者您必須從管理伺服器執行重新啟動指令。管理伺服器會向您傳送一個通知，指示哪些用戶端需要重新啟動。請參閱：

[從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)

NOTE

與用戶端安裝套件一樣，您無法回復用戶端修補程式。您必須從舊版本解除安裝用戶端安裝套件，並將其重新安裝。

在 Windows 用戶端上安裝用戶端修補程式

1. 在主控台中，確認已將 LiveUpdate 架構為將用戶端修補程式下載至管理伺服器。
在「要下載的內容類型」對話方塊中，確保已勾選「用戶端修補程式」。請參閱：
[將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)
2. 若要執行報告以找出用戶端電腦上安裝哪些版本，請執行「防護內容版本」報告。請參閱：
[產生網路中安裝的 Symantec Endpoint Protection 版本的清單](#)
3. 確認已將 LiveUpdate 設定政策架構為下載修正程式至用戶端。
在 LiveUpdate 設定政策中，於「**Windows** 設定」下方，按下「進階設定」。確定已勾選「下載用戶端修補程式」。

NOTE

確定已勾選「可用時從 **LiveUpdate** 伺服器下載 **Delta** 內容」。此選項會合併目前發行中含該內容的用戶端修補程式與新的修補程式，然後僅下載差異或 Delta。用戶端的頻寬太低時，請使用此選項。

4. 重新啟動用戶端電腦。請參閱：
[在用戶端電腦上從主控台執行指令](#)

升級群組更新提供者

使用此程序升級屬於「群組更新提供者」的用戶端。

升級群組更新提供者用戶端

1. 將 Symantec Endpoint Protection Manager 伺服器升級為新版軟體。
2. 將屬於「群組更新提供者」的用戶端升級為新版用戶端軟體。
3. 將其餘的用戶端更新為新版用戶端軟體。

更多資訊

- [使用群組更新提供者將內容散佈至用戶端](#)
- [升級至新版本](#)

移轉至 SES 雲端主控台

了解如何將用戶端電腦的管理從內部部署 Symantec Endpoint Protection Manager (SEPM) 移轉至 Symantec Endpoint Security (SES) 雲端式主控台。

內部部署功能和雲端功能如何比較？

移轉至 Symantec Endpoint Security 有許多好處。

探索 SES 必須提供的高層級比較功能。

如需詳細比較的資料，請參閱：[內部部署 Symantec Endpoint Protection 與 Symantec Endpoint Security Complete 之間的功能比較](#)

開始之前

選擇最適合貴組織並受您產品類型和授權支援的[管理選項](#)。

檢閱此[重要資訊](#)並確保您的環境符合[先決條件](#)。

[關於從 Symantec Endpoint Protection \(SEP\) 移至 Symantec Endpoint Security \(SES\) 的常見問題](#)

SES 授權是否適用於 SEP？

Symantec Endpoint Security 授權適用於所有三個管理選項。與 Symantec Endpoint Security Enterprise (SESE) 授權相比，Symantec Endpoint Security Complete (SESC) 授權能提供您更多防護技術。

如何移至 SES

請依循移轉至您選擇之管理選項的工作流程。

移轉選項	更多資訊
內部部署至混合	- 賽門鐵克建議您先測試使用混合管理選項的雲端主控台。您將預設 SEPM 網域註冊至雲端。 向雲端伺服器註冊 Symantec Endpoint Protection Manager 網域 以雲端伺服器 (14.3 RU3 或更新版本) 註冊 Symantec Endpoint Protection Manager
混合至雲端	經過一段測試期之後，從混合模式全面移轉至完全原生的雲端選項。 從混合管理的 Symantec Endpoint Protection Manager (SEPM) 選項移至完全受管雲端選項
內部部署至雲端	或者，直接從內部部署移至完全雲端管理。此方法更為簡單，並提供比混合方法更多的保護。 從內部部署 Symantec Endpoint Protection Manager (SEPM) 選項直接移至完全雲端管理選項

當移動完成時

如果您是首次使用 Symantec Endpoint Security，請參閱：[開始使用 Symantec Endpoint Security](#)

移轉到 Symantec Endpoint Security 雲端主控台的好處

從內部部署解決方案移轉到雲端解決方案有很多好處。

移轉至雲端的好處

無論您選擇哪種管理選項 (混合管理或完全雲端管理)，您都會從 Symantec Endpoint Security (SES) 雲端主控台管理組織中的用戶端時獲得以下好處：

-
- 沒有管理伺服器 and 資料庫的安裝和管理成本或開銷。
 - 能夠跨單一管理主控台對多個賽門鐵克企業產品進行共用管理。
 - 對來自多個賽門鐵克產品的威脅、政策和事件的統一可見度，可將資安事端回應時間從幾天縮短到幾分鐘。
 - 改善用於管理和可見度的主控台。
 - 每月更新的動態平台。
 - 用戶端自動升級。

混合管理選項的好處

賽門鐵克建議您先測試雲端主控台，然後再完全移轉至雲端主控台。

透過混合管理選項，您可以從 Symantec Endpoint Security 中管理用戶端和一些政策。您可以從 Symantec Endpoint Protection Manager 管理其他政策。此混合管理選項可提供內部部署 Symantec Endpoint Protection Manager 無法提供的一些附加安全功能。

若要使用混合管理，您可以在 SES 雲端伺服器中註冊每個 Symantec Endpoint Protection Manager 網域。

下列清單是在註冊 Symantec Endpoint Protection Manager 網域時取得的功能的高階摘要：

- 使用端點偵測和回應來偵測和公開可疑網路活動。
- 具有中央允許清單和拒絕清單的整合式誤報管理
- 用於管理進階功能的現代雲端主控台

更多資訊

[在內部部署管理、混合管理或雲端管理選項之間進行選擇](#)

完全雲端管理選項的優點

Symantec Endpoint Security 具有 Symantec Endpoint Protection Manager 內部部署主控台所沒有的功能：

- 端點偵測和回應 (EDR)
- 調適型防護 (14.3 RU9 和更早版本)
- 應用程式控制
- 針對 Active Directory 的威脅防禦
- 防惡意軟體
- 行動威脅防禦和安全連線

NOTE

您可以透過 Symantec Endpoint Security Complete 訂購授權而不是 Symantec Endpoint Security Enterprise 訂購授權來獲得最多功能。

更多資訊：

- [Symantec Endpoint Protection 部署類型支援的 Symantec Endpoint Security 功能](#)
- [什麼是 Symantec Endpoint Security？](#)
- [Symantec Endpoint Security Complete](#)

內部部署、混合或完全雲端管理選項

您只能從內部部署 Symantec Endpoint Protection Manager (SEPM)、Symantec Endpoint Security (SES) 雲端主控台或兩者的組合 (混合管理) 管理代理程式。

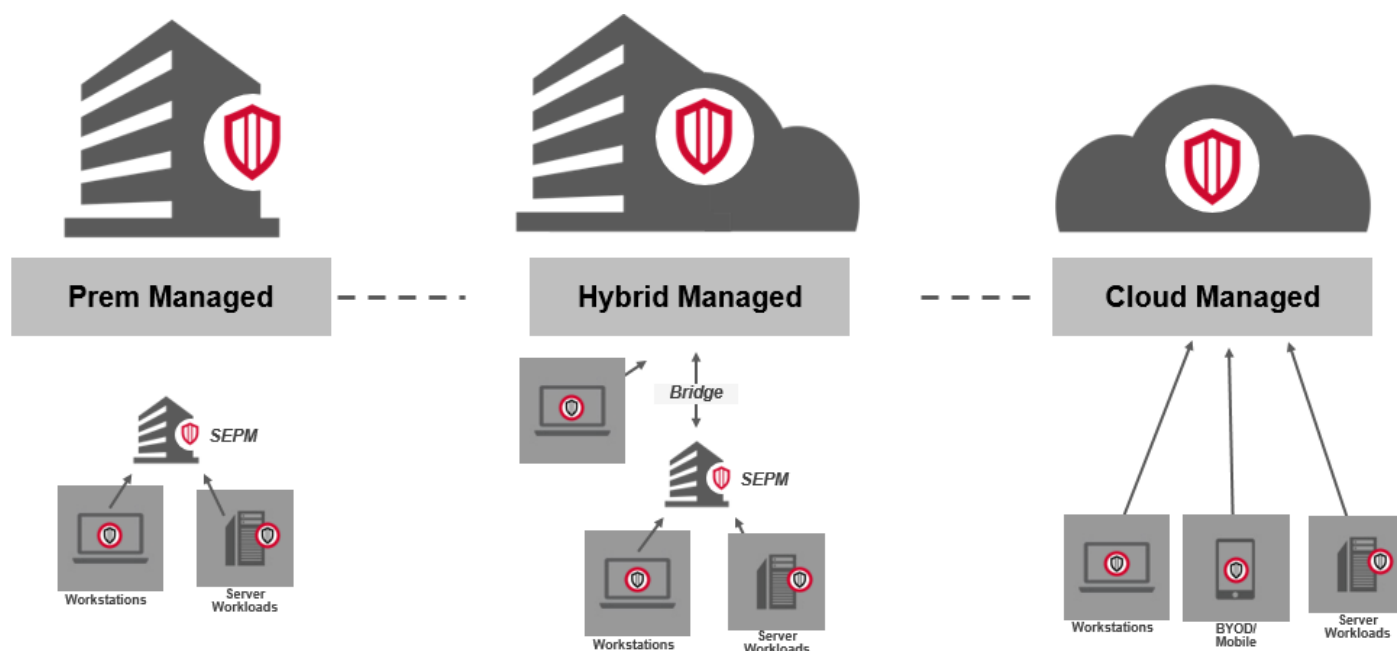


Table 42: 每個管理選擇之間的差別

	內部部署	混合	原生雲端
授權	Symantec Endpoint Protection 或 Symantec Endpoint Security (Enterprise 或 Complete)	Symantec Endpoint Protection 或 Symantec Endpoint Security (Enterprise 或 Complete)	Symantec Endpoint Security (Enterprise 或 Complete)
主控台	Symantec Endpoint Protection Manager 您不會將 SEPM 網域註冊到雲端伺服器。	- 內部部署: Symantec Endpoint Protection Manager。登入 SEPM。 - 雲端: Symantec Endpoint Security。登入您的 Symantec Security 雲端帳戶。 您在雲端中註冊 SEPM 網域。 - 將 Symantec Endpoint Protection Manager 網域註冊到雲端主控台	Symantec Endpoint Security (SES) 您不會在雲端中註冊 SEPM 網域。登入您的 Symantec Security 雲端帳戶。 從內部部署 Symantec Endpoint Protection Manager (SEPM) 選項直接移至完全雲端管理選項 Endpoint Security 入門指南
*用戶端軟體	Symantec Endpoint Protection 用戶端 從 Symantec Endpoint Protection Manager 部署用戶端安裝套件。	Symantec Endpoint Protection 用戶端 *Symantec Endpoint Protection 用戶端與 Symantec Agent 相同。 若為成功的混合部署，請使用最新版的 SEPM 以及 14.3 MP1 或更高版本用戶端。您可從 SES 管理代理程式和一些政策。您可從 SEPM 管理較早版本的用戶端。	Symantec Endpoint Protection 用戶端，但在 SES 雲端伺服器中稱為 Symantec Agent。 您會完全從雲端管理用戶端，這會繞過與內部部署 SEPM 的通訊。

何時可以使用此種方法？	- 您的網路包括遠端位置，例如石油鑽井平台或海上環境。 - 您的工作位在網路受到嚴格限制的政府環境中。 - 您在暗網中有很多用戶端。 - 您需要與內部部署管理伺服器相同的功能。但是 Symantec Endpoint Protection 持續新增功能。	- 您想從 14.3 MP1 或更高版本升級至 Symantec Endpoint Security，但想要緩慢地移動至完全雲端管理的主控台。 - 您想要更多的靈活性，並可於稍後完全移動至雲端。 - 您有用戶端位於使用 Symantec Endpoint Security 不支援作業系統的裝置上。	- 您不想要花費安裝和管理管理伺服器與資料庫的成本或開銷。 - 您有多個賽門鐵克企業產品，希望透過單一管理主控台共用管理功能。 - 您希望統一檢視多個賽門鐵克產品報告的威脅、政策和資安事端，進而將資安事端回應時間從幾天縮短到幾分鐘。 - Symantec Endpoint Security 具有 Symantec Endpoint Protection 內部部署所沒有的其他功能。請參閱： 快速參考 SES 中的 Symantec Endpoint Protection 受管與 Symantec Endpoint Security 受管功能

NOTE

*若是由 Symantec Endpoint Protection Manager 而非 SES 進行管理，則用戶端功能會稍有不同。Symantec Endpoint Protection Manager 在用戶端上控制較多選項，而 Symantec Endpoint Security 控制較少的選項。Symantec Endpoint Protection Manager 為使用者提供了較多的配置選項，而雲端受管用戶端提供的選項較少。但是，賽門鐵克在每月重新整理的 Symantec Endpoint Security 中增加了新功能。

更多資訊

- [管理選項](#)
- [內部部署 Symantec Endpoint Protection 14.x 和 Symantec Endpoint Security Complete 之間的比較](#)

向雲端伺服器註冊 Symantec Endpoint Protection Manager 網域

若要註冊混合管理，您必須先註冊 Symantec Endpoint Protection Manager (SEPM) 網域。混合管理可讓您從 Symantec Endpoint Security (SES) 雲端檢視與管理用戶端和政策。

此程序使用「進階安全性」頁面 > 「設定」，以在 Symantec Endpoint Security 雲端中註冊管理伺服器。

- 如果您具有 Symantec Endpoint Security Enterprise 訂閱、如果輕度註冊失敗，或者您有 14.3 RU2 或更早版本的管理伺服器，則必須使用此程序。
- 如果您具有 Symantec Endpoint Security Complete 訂閱以及 Symantec Endpoint Protection Manager (SEPM) 14.3 RU3 版或更新版本，則可以使用下列方法。此方法可協助您建立 Symantec Security Cloud 帳戶。

[以雲端伺服器 \(14.3 RU3 或更新版本\) 註冊 Symantec Endpoint Protection Manager](#)

NOTE

您最多可以新增 70 個生產網域。如果您使用多個賽門鐵克產品，則跨產品的網域總數不能超過 150。

當您升級時，Symantec Endpoint Protection Manager 會保留註冊狀態。

開始註冊之前

您的環境必須滿足以下需求，才能支援以雲端伺服器註冊網域：

- Symantec Endpoint Security Complete 或 Symantec Endpoint Security Enterprise 的付費訂閱。

NOTE

若要在 14.3 RU3 和更新版本上從雲端管理調適型防護，您必須具有 Symantec Endpoint Security Complete 訂閱。

- [Symantec Security Cloud 帳戶](#)

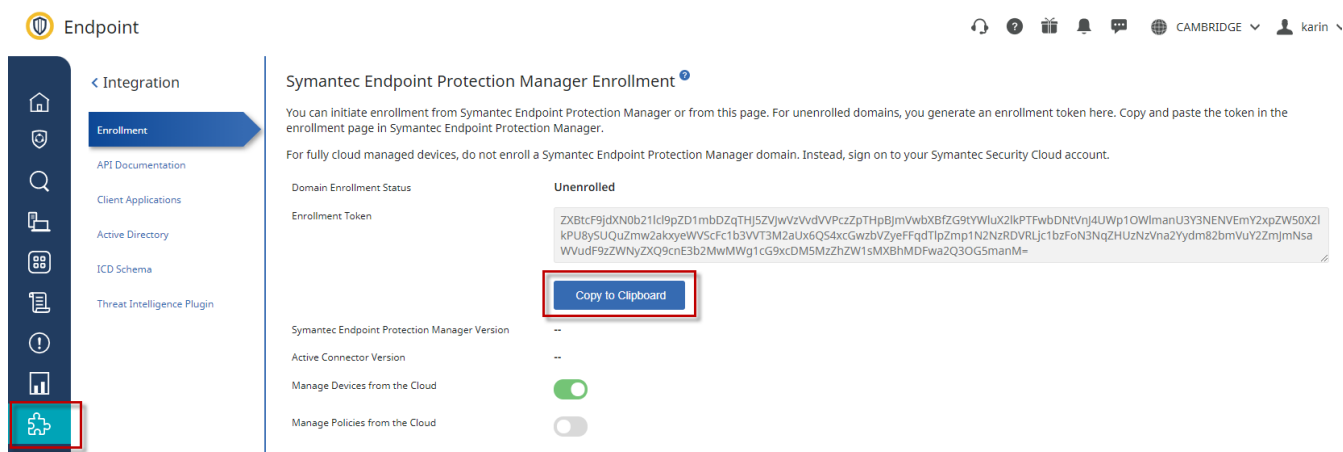
您可以在從 Symantec Endpoint Protection Manager 啟動網域註冊時設定此登入帳戶。也可以使用現有的帳戶登入。如果您沒有登入憑證，請與您的帳戶團隊經理聯繫。

- 管理員對 Symantec Endpoint Protection Manager 的存取。
- Symantec Endpoint Protection 14.3 MP1 (14.3.1169.0169) 或更新版本用戶端

您可以使用舊版用戶端將 Symantec Endpoint Protection Manager 網域註冊到雲端伺服器，但這些舊版用戶端無法利用僅限雲端政策。

步驟 1：從 **Symantec Endpoint Security** 取得註冊 Token

1. 在雲端主控台中，登入 [Symantec Security Cloud 帳戶](#)。
2. 前往「整合」>「註冊」。
3. 從此頁面中，選取「複製到剪貼簿」以複製註冊 Token。



步驟 2：開始註冊

14.3 RU3 版和更新版本：

1. 在 Symantec Endpoint Protection Manager 中，按一下「進階設定」>「設定」。
您可能需要捲動到「進階安全性」(14.3 RU10) 或「進階防護」(14.3 RU9 和更早版本) 頁面的底端。
2. 在「設定」文字方塊中，貼上您在步驟 1 取得的註冊 Token，然後按一下「註冊 **Symantec Endpoint Protection Manager**」。
例如 (14.3 RU10)：

Settings

Data Retrieval

You can decide whether or not the management server retrieves and refreshes this data.

Adaptive Protection

☒

ON

Cloud Analytics

☒

ON

Enrollment Token

To enroll the Symantec Endpoint Protection domain, enter the enrollment token below. You obtain the token from the Symantec Endpoint Security cloud. [Learn More](#)

ENROLLMENT TOKEN*

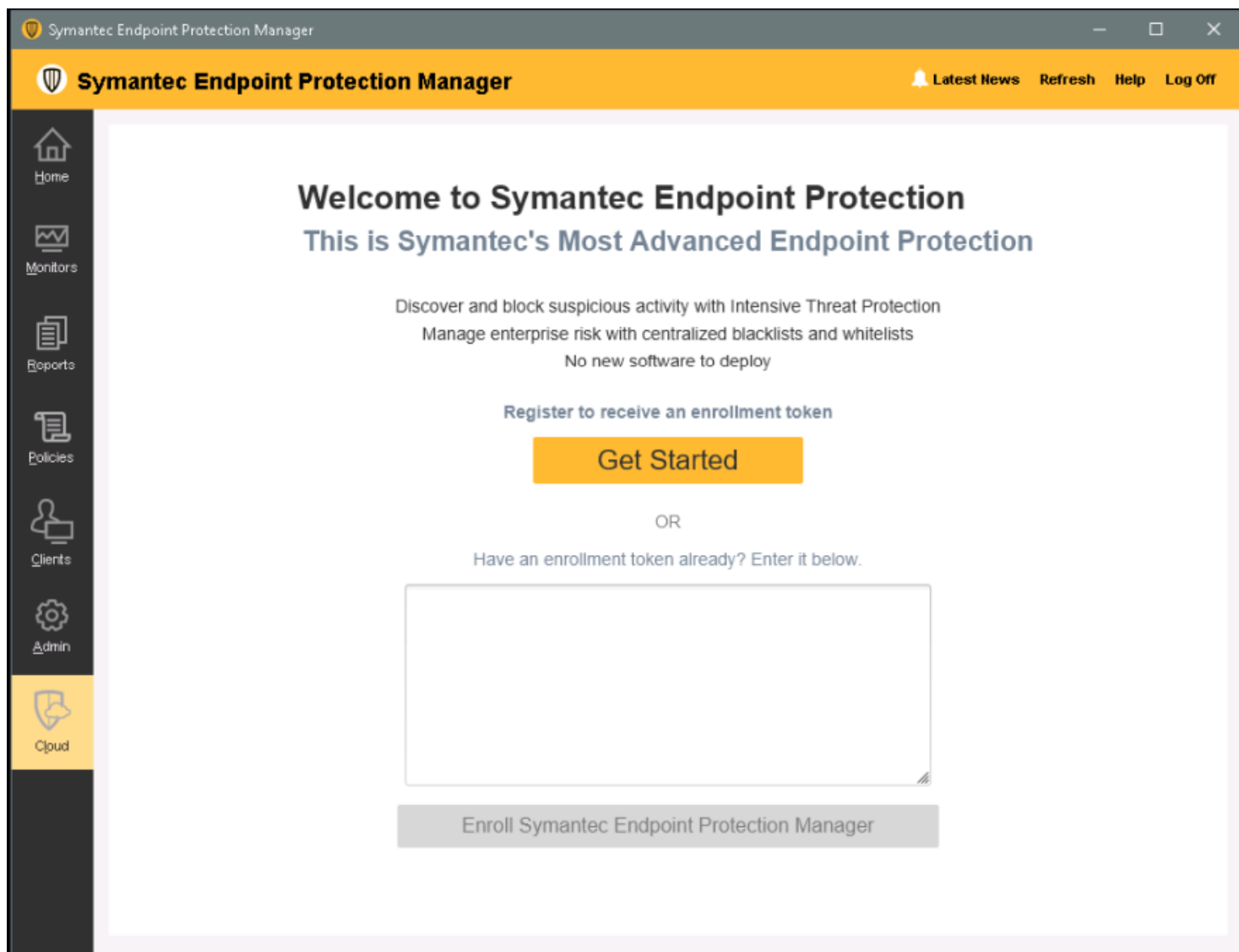
Enroll Symantec Endpoint Protection Manager

您可以使用下列方式來驗證雲端註冊是否成功：

- 在「註冊資訊」下方，將「註冊狀態」設定為「已註冊」。
- 關閉「設定」對話方塊。在「設定」選項旁邊，「未連線」變成「已連線」。

14.2 RU1 到 14.3 RU1 版：

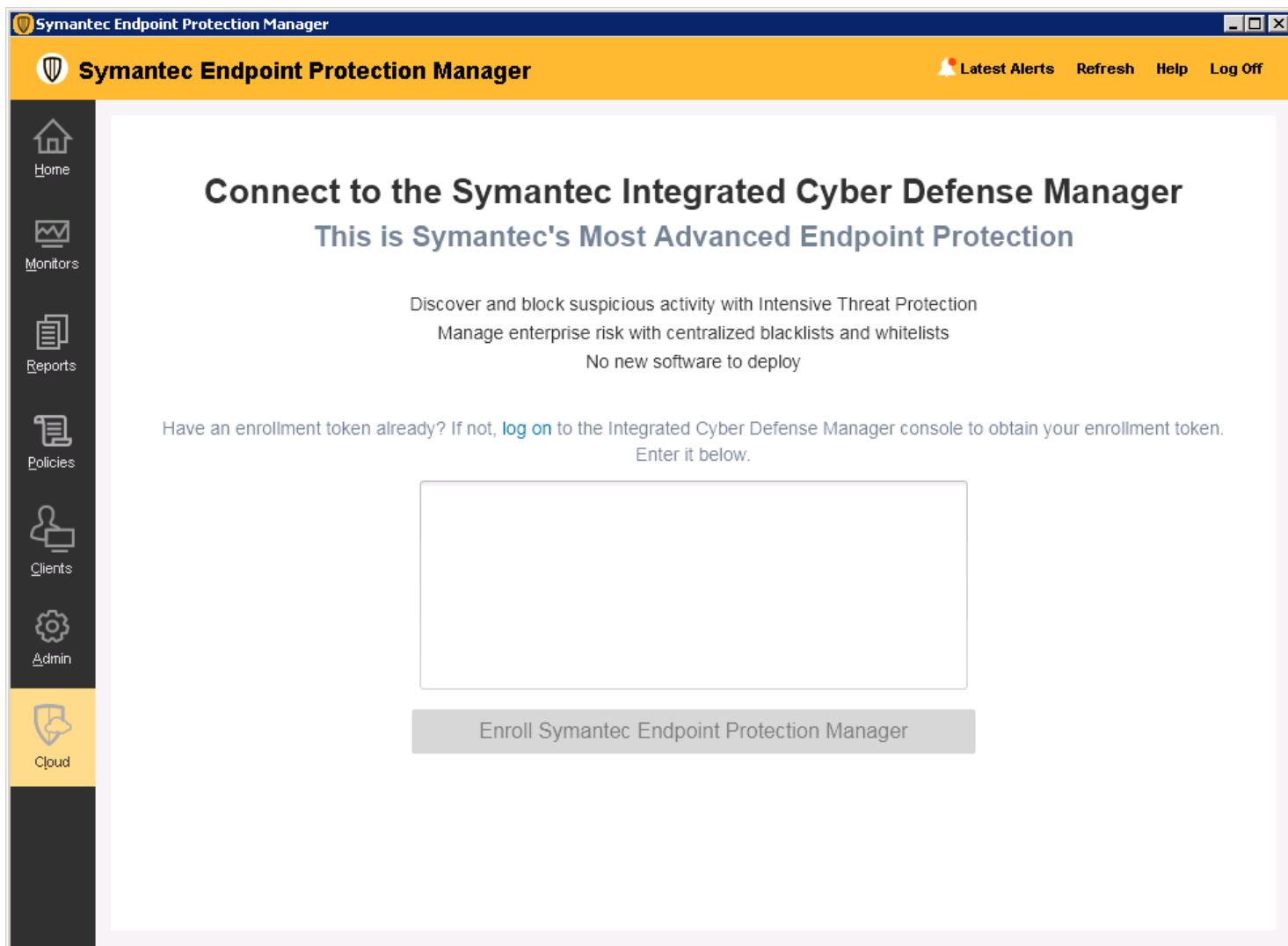
1. 在 Symantec Endpoint Protection Manager 中，前往「首頁」，然後選取「立即註冊」或前往「雲端」頁面。
「開始使用」按鈕將帶您進入 Symantec Security Cloud 登入頁面。



2. 在文字方塊中，貼上您在步驟 1 取得的註冊 Token，然後按一下「註冊 **Symantec Endpoint Protection Manager**」。
註冊 SEPM 之後，您會取得一則確認訊息。

14.2 RU1 到 14.3 RU2 版：

1. 按一下「雲端」頁面。



2. 在文字方塊中，貼上您在步驟 1 取得的註冊 Token，然後按一下「註冊 **Symantec Endpoint Protection Manager**」。

步驟 3：註冊之後，登入雲端主控台

註冊之後，請先登入 [Symantec Security Cloud 帳戶](#)。您的所有用戶端電腦都會在 Symantec Endpoint Security 雲端中顯示為裝置。依據預設，Symantec Endpoint Protection Manager 會管理拓樸。若要從雲端管理裝置和政策，您必須在雲端主控台上切換管理控制。

請參閱[向雲端伺服器註冊 Symantec Endpoint Protection Manager 網域之後如何管理用戶端和政策？](#)

WARNING

每當您對裝置群組結構進行變更時，均會延遲數分鐘，變更才會在 Symantec Endpoint Protection Manager 中顯示。反之亦然。此行為類似於 Symantec Endpoint Protection Manager 遠端複製運作的方式。在延遲期間，您不應該嘗試進行其他拓樸變更。變更可能不會生效。

更多資訊

[Symantec Endpoint Security 入門指南](#)

[向雲端主控台註冊 Symantec Endpoint Protection Manager 網域後發生的情況](#)

以雲端伺服器 (14.3 RU3 或更新版本) 註冊 Symantec Endpoint Protection Manager

若要註冊混合管理，您必須先註冊 Symantec Endpoint Protection Manager (SEPM) 網域。混合管理可讓您從 Symantec Endpoint Security (SES) 雲端檢視與管理用戶端和政策。

此程序使用「進階安全性」頁面 > 「在混合雲端中註冊」或「啟用調適型防護」按鈕，以在 Symantec Endpoint Security 雲端中註冊管理伺服器。您看到的按鈕取決於所使用的 SEPM 版本。

- 如果您具有 Symantec Endpoint Security Complete (SESC) 訂閱以及 14.3 RU3 或更新版本的管理伺服器和用戶端，則請使用此程序。
- 如果您具有 Symantec Endpoint Security Enterprise 訂閱、如果使用 SESC 訂閱進行輕度註冊失敗，或者，如果您執行 14.3 RU2 和更早版本的管理伺服器，則請參閱：[將 Symantec Endpoint Protection Manager 網域註冊到雲端伺服器](#)。

精靈會為您建立 Symantec Security Cloud 帳戶。如果您已有 Symantec Security Cloud 帳戶，則仍然可以使用這些步驟來註冊網域。精靈不會建立第二個 Symantec Security Cloud 帳戶。

步驟 1：開始註冊

NOTE

在您將 Symantec Endpoint Protection Manager 網域註冊到雲端之前，應該安裝最新版本的 Symantec Endpoint Protection Manager。您必須擁有管理員存取權。

1. 在 Symantec Endpoint Protection Manager 中，按一下「進階安全性」頁面。
最多需要 3 到 4 天，才會出現自適應防護行為應用程式熱圖。在此期間，Symantec Endpoint Protection Manager 會與 Endpoint Security 雲端伺服器通訊，並從中收集資料。
 - 從 14.3 RU10 開始，您可以使用 Symantec Endpoint Protection Manager 自適應防護政策來管理調適型防護。如果您願意，則可以在雲端中管理調適型防護。
如需兩個控制台中調適型防護之間差異的相關資訊，請參閱[Symantec Endpoint Protection 與 Symantec Endpoint Security 之間的自適應防護功能比較](#)。
 - 在 14.3 RU3 到 14.3 RU9 中，如果您想要檢視熱圖，則必須將 SEPM 網域註冊到雲端。您可以立即註冊 SEPM 網域，或等待以查看填入的熱圖。針對舊版本，「雲端」頁面會變更為「進階安全性」頁面。
2. 在「進階安全性」頁面上，執行下列其中一個任務：
 - a. 從 14.3 RU10 開始，按一下「在混合雲端中註冊」。

Symantec Endpoint Protection Manager

Home Monitors Reports Policies Clients

Advanced Security

Enroll in Hybrid Cloud

Advanced Security contains Adaptive Protection, which lets you allow behaviors that you deem as safe, or block the behaviors that are not. Use the heat map below to view prevalence behavior and automatically block untrusted behaviors.

Go to the Adaptive Protection policy to configure, enforce, and manage these behaviors. [Learn more](#)

If you prefer to manage your protection and your clients from the cloud, you can enroll in hybrid management. Either click **Enroll in Hybrid Cloud** or click **Settings**. [Learn more](#)

Adaptive Protection

Behavioral Activity Prevalence

0 Zero	0 Low	0 Medium	0 High	0 Learning

Data is updated periodically.

- b. 針對 14.3 到 14.3 RU9，按一下「啟用自適應防護」。
3. 同意法律協議，然後按一下「註冊」。
4. 在「雲端註冊」畫面中，輸入您的名字、姓氏和有效的電子郵件地址，而您可以從中接收具有 PIN 號碼的電子郵件訊息，然後按「下一步」。

NOTE

此精靈會驗證此地址是正確地址，而且您是該電子郵件地址的擁有者。您應該使用用來管理 Symantec Endpoint Protection Manager 以及想要用於 Symantec Security Cloud 帳戶的相同電子郵件地址。

此步驟也會自動為您註冊 SEPM 網域。

Cloud Enrollment

Verify Your Email Address

This Symantec Endpoint Protection Manager is enrolled in the cloud console. You must verify the email address you want to use to set up and access your Symantec Security Cloud account. You can use the Symantec Endpoint Protection Manager email address below, or change it. Click **Next** to receive a PIN number that verifies the email address.

If you already have a Symantec Security Cloud account, click **Cancel** and sign on at: [Symantec Security Cloud](#)

FIRST NAME*	LAST NAME*
John	Smith

WORK EMAIL ADDRESS*

jsmith@broadcom.com

Cancel Next

您會接收到具有上一步中所指定電子郵件地址的電子郵件訊息，其中包含一個 6 位 PIN 號碼。PIN 號碼的有效時間是 15 分鐘。

Lorem Ipsum <sepm_server@companyX.com>



Tue 5/04/2021 10:05 AM

To: You:



Your verification PIN is:

320152

ALERT! DO NOT share this code with anyone. We will never ask you for this code. Verification PIN: 320152 (expires in 3 minutes)

You are receiving this message because you signed up for this alert. Sign on to Symantec Endpoint Protection Manager to modify your notification settings.

Important Information:

If you did not initiate this request, contact your system administrator immediately.



Copyright © 2005-2021 Broadcom. All Rights Reserved.

5. 將 6 位 PIN 號碼貼入「輸入 PIN 以進行確認」畫面，然後按一下「驗證」。

 Cloud Enrollment ×

Enter the PIN to confirm



Symantec sent a PIN to the email address "jsmith@broadcom.com" for validation. Enter the 6-digit PIN below.

PIN

Didn't receive the PIN? Make sure that you entered the correct work email address. Click **Back** to [Re-enter](#) your email address.

[Resend PIN](#)

Back

Verify

6. 在驗證 PIN 號碼而且您取得確認訊息之後，請按一下「關閉」。
7. 若要驗證註冊，請捲動至「進階設定」畫面的右下角，然後執行下列任一任務：
 - a. 在「設定」旁邊，「未連線」變成「已連線」。



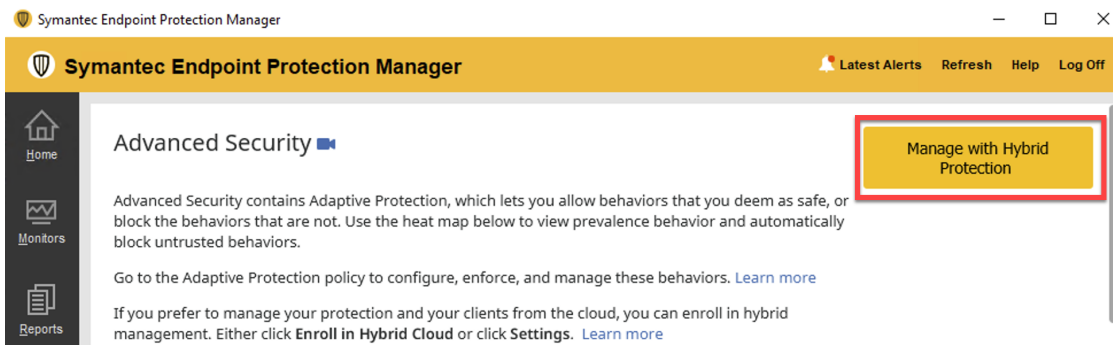
- b. 按一下「設定」。在「註冊資訊」下方，將「註冊狀態」設定為「已註冊」。

如需疑難排解註冊問題，請參閱：[「進階安全性」頁面問題疑難排解](#)

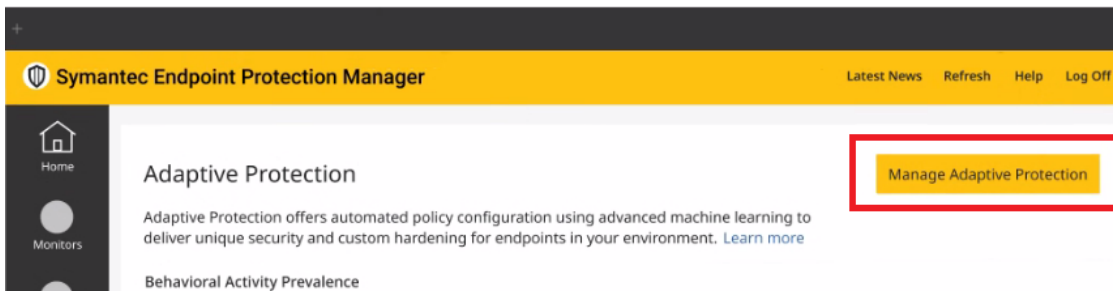
步驟 2：登入 Symantec Security Cloud 帳戶並建立密碼

註冊 SEPM 網域之後，您必須登入 Symantec Security Cloud 帳戶，而且必須建立密碼。註冊和雲端帳戶建立不會自動為您建立密碼。

1. 執行下列其中一個步驟：
 - 從 14.3 RU10 開始，按一下「使用混合防護進行管理」。



- 針對 14.3 RU9 和更早版本，請按一下「管理調適型防護」。



2. Symantec Security Cloud 登入頁面即會出現。

[登入 Symantec Security Cloud 帳戶](#)

[Symantec Endpoint Security 入門指南](#)

將 Symantec Endpoint Protection Manager 網域註冊到雲端伺服器後，我該如何管理用戶端和政策？

在 Symantec Endpoint Protection Manager (SEPM) 網域註冊之後，Symantec Endpoint Protection Manager 資料會同步到 Symantec Endpoint Security (SES) 雲端伺服器。資料包括雲端伺服器支援的用戶端階層和政策。同步時間不是立即的。

裝置與政策同步之後，您可以從 Symantec Endpoint Protection Manager 或 Symantec Endpoint Security 雲端主控台管理它們。這稱為混合式管理。

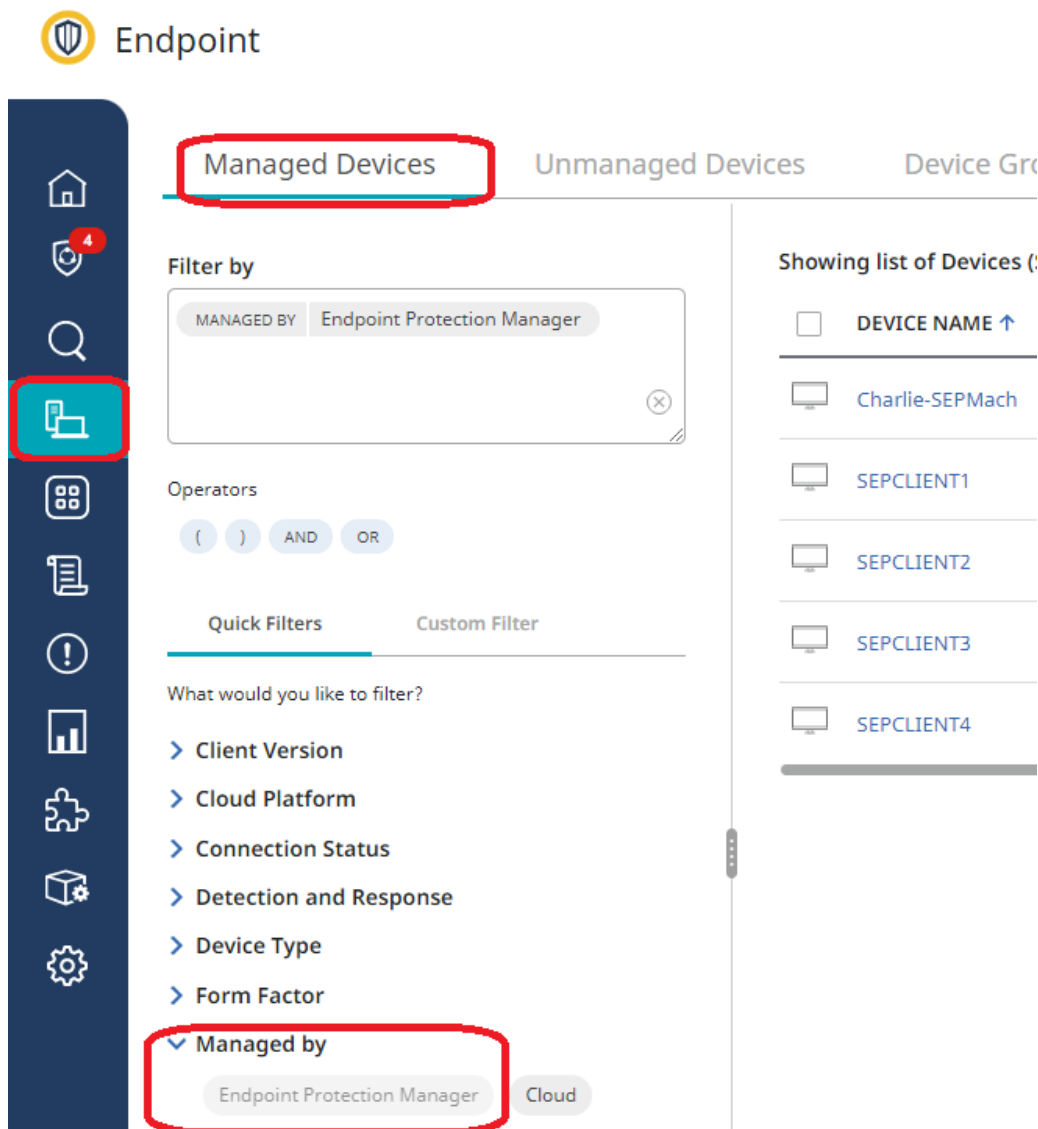
Symantec Endpoint Protection Manager 用戶端在雲端主控台中稱為 Symantec Agent。

步驟 1：從雲端主控台管理裝置

同步後，Symantec Endpoint Protection Manager 用戶端電腦和用戶端群組會自動作為裝置出現在 SES 雲端主控台上。

檢視從 **Symantec Endpoint Protection Manager** 同步的裝置

1. 於雲端主控台中「裝置」頁面上，執行下列其中一個任務：
 - 在「受管裝置」索引標籤上的「管理者」下拉功能表中，選取 **Endpoint Protection Manager** 依預設，裝置顯示於平面清單，而非「受管裝置」頁面上的群組中。



- 在「裝置群組」標籤上，前往「我的公司」群組。

預設情況下，您可以在 Symantec Endpoint Protection Manager 中管理裝置的組織。您可以只在雲端主控台中管理裝置，或是只在 Symantec Endpoint Protection Manager 管理裝置，但不能同時使用兩者。

NOTE

若希望 Active Directory 或其他第三方目錄工具來管理裝置組織，請保持「從雲端管理裝置」關閉。

每當您對裝置群組結構進行變更時，則需數分鐘後，變更才會顯示於 Symantec Endpoint Protection Manager 中。反之亦然。此行為類似於 Symantec Endpoint Protection Manager 遠端複製運作的方式。在延遲期間，您不應該嘗試進行其他拓模變更。變更可能不會生效。

從雲端主控台管理裝置

1. 在雲端主控台中，移至「整合 > 註冊」。
預設會停用此設定。
2. 開啟「從雲端管理裝置」。

步驟 2：從雲端主控台管理政策

政策會自動顯示在雲端主控台內的「政策」頁面上。您不需要從 Symantec Endpoint Protection Manager 匯出政策然後在雲端匯入，除非您希望從 SES 完全管理您的環境。

此設定適用於通常在 Symantec Endpoint Protection Manager 上的下列橋接政策：例外政策和記憶體攻擊緩和 (MEM) 政策。此設定會讓 SEPM 無法向下同步這些政策，以及在 SEPM 中建立新的政策。

網域註冊後，雲端伺服器一律會控制您從 SES 管理的受支援政策。

您可繼續使用 Symantec Endpoint Protection Manager 來管理其他政策。這些政策會向下推送至 Symantec Endpoint Protection Manager，而其會將政策派送至用戶端。

從雲端主控台管理政策

1. 在雲端主控台中，移至「整合 > 註冊」。
預設會停用此設定
2. 開啟「從雲端管理政策」。

步驟 3：尋找雲端伺服器偵測到的威脅

在雲端主控台上，「首頁」和「搜尋到的項目」頁面提供有關環境中偵測的更全面資訊。使用「首頁」頁面檢查政策設定的結果，並調整政策設定 (如有需要)。

混合管理 Symantec Endpoint Protection Manager (SEPM) 如何與 Symantec Endpoint Security (SES) 雲端主控台互動

Symantec Endpoint Protection Manager 與雲端伺服器之間的通訊與註冊

本節列出了透過雲端伺服器註冊 SEPM 網域時可能發生的一些預期行為。

- 如果 Symantec Endpoint Protection Manager 連接器無法取得雲端伺服器的存取 Token，它會每小時重試一次。
- 透過 Symantec Endpoint Protection Manager 連線的用戶端可能不會立即在雲端伺服器中顯示正確的線上狀態。在線上狀態變更後，可能需要 5-10 分鐘才能看到目前狀態的準確反映。請參閱：
[檢查用戶端是否已連線至管理伺服器且受保護](#)
- 管理伺服器與 Google Cloud Platform (GCP) 伺服器的系統時間相差必須在 10 分鐘以內。否則，註冊會失敗，並且您會看到以下錯誤訊息：

```
##### Symantec Endpoint Protection Manager #####
```

若要解決時間不相符問題，請將 Symantec Endpoint Protection Manager 伺服器與網路時間通訊協定 (NTP) 同步。請參閱下列各項以取得詳細資訊：

[NTP：網路時間通訊協定](#)

- 您可以使用以下日誌來疑難排解失敗的註冊：BRIDGE_INSTALL.log、catalinaWs.out、Cloud-0.log、scm-server-0.log 和 semapisrv_access_log.date.log。所有這些檔案皆位於 Symantec Endpoint Protection Manager 安裝資料夾內的 \tomcat\logs 中。

授權、安裝、升級、資料庫

- 您必須購買 Symantec Endpoint Security 授權才能使用或註冊雲端伺服器。
- 無法從雲端主控台升級管理伺服器。
- 無法從雲端備份或還原資料庫或 Symantec Endpoint Protection Manager 設定。
- 若要釋放授權，Symantec Endpoint Protection Manager 資料庫會根據所指定的天數刪除未連線至網域的用戶端。在雲端伺服器中，30 天後會自動刪除這些用戶端，且無法架構此間隔。首先會刪除 Symantec Endpoint Protection Manager 資料庫中的用戶端，然後刪除雲端伺服器中的用戶端。請參閱：
[從資料庫清除過時的用戶端以使更多授權可用](#)

網域註冊和取消註冊

註冊網域時：

- 會同步化事件、政策、用戶端和用戶端群組。
- 雲端支援的政策功能不適用於 Symantec Endpoint Protection Manager 中的組態。
- 雲端政策設定優先。

如有必要，可以取消註冊預設網域。例如，您可能有連線問題，或者您可能決定不希望雲端主控台管理政策。您可以在 Symantec Endpoint Protection Manager 上的註冊頁面或是雲端主控台內的「端點 > 整合 > 註冊」中取消註冊。

取消註冊過程將刪除雲端中未註冊網域的用戶端群組和用戶端。任何關聯的政策都保留在雲端主控台中以及相關事件中。請參閱：

- [向雲端伺服器註冊 Symantec Endpoint Protection Manager 網域](#)
- [將 Symantec Endpoint Protection Manager 網域註冊至雲端主控台中 \(14.3 RU3 或更新版本\)](#)
- [取消註冊 Symantec Endpoint Protection Manager 網域](#)

網站和複寫

- 對於每個網站，可在雲端主控台中針對每個網站註冊一個 Symantec Endpoint Protection Manager 網域。即使網域位於不同的站台，也無法註冊多個網域。如果您使用相同的雲端主控台帳戶，也無法註冊單獨的 Symantec Endpoint Protection Manager 網域。
- 對於具有兩個 Symantec Endpoint Protection Manager (共用 SQL Server 資料庫且架構進行容錯移轉) 的網站，您可以從其中一個管理伺服器註冊一個網域。在每個管理伺服器與雲端主控台之間通訊的橋接器服務一次在一個管理伺服器上執行。該服務首先在具有較高伺服器優先順序的管理伺服器上執行。如果第一個橋接器服務當機，則會改為執行第二個管理伺服器的服務。一次只能從雲端主控台管理一個網域。雲端主控台與每個管理伺服器之間的同步會同時發生。

下表顯示當您註冊 Symantec Endpoint Protection Manager 網域時雲端主控台所支援的網站架構。

Table 43: 雲端主控台支援的網站組態

站台組態	在雲端主控台上受支援
一個網站、一台電腦上的一個 Symantec Endpoint Protection Manager，僅搭配同一電腦上的資料庫	是
一個站台、一台電腦上的一個 Symantec Endpoint Protection Manager，搭配第二台電腦上的 Microsoft SQL Server 資料庫	是
一個站台、多個 Symantec Endpoint Protection Manager	是
多個網站、每個網站上的一個 Symantec Endpoint Protection Manager，搭配遠端複製*	是 (14.2 RU1 及更新版本)
多個網站、每個網站上的多個 Symantec Endpoint Protection Manager，搭配遠端複製*	是 (14.2 RU1 及更新版本)

* 僅支援遠端複製夥伴關係中一個網站上的一個 Symantec Endpoint Protection Manager 向雲端進行註冊。

如需詳細資訊，請參閱：[向雲端伺服器中的遠端複製夥伴註冊網站](#)

群組、用戶端、位置

- 如果您在雲端主控台中重新命名「我的公司」，Symantec Endpoint Protection Manager 中的群組名稱不會變更。
- 雲端管理功能需要受管用戶端。無法管理非受管用戶端，或將使用雲端功能的政策套用至非受管用戶端。如果將使用雲端功能的政策套用至非受管用戶端，該政策會預設為對等的舊 Symantec Endpoint Protection 選項。
- 14 版 MP2 和更舊版本的用戶端電腦會顯示在雲端主控台中，但不支援任何新的雲端式功能。
- 如果雲端主控台中的「從雲端管理裝置」選項處於開啟狀態，則雲端主控台會管理裝置。如果處於關閉狀態，則 Symantec Endpoint Protection Manager 會管理裝置。
如果搭配使用 Active Directory 與 Symantec Endpoint Protection Manager 來管理群組和用戶端，則 Symantec Endpoint Protection Manager 會自動管理裝置。在這種情況下，您無法將「從雲端管理裝置」切換到雲端主控台。此設定會將裝置組織的控制僅返回到 Symantec Endpoint Protection Manager。它不影響任何群組的政策防護。您可以繼續從雲端主控台管理進階政策功能。
- 每當您對裝置群組結構進行變更時，均會延遲數分鐘，變更才會在 Symantec Endpoint Protection Manager 中顯示。反之亦然。此行為類似於 Symantec Endpoint Protection Manager 遠端複製運作的方式。在延遲期間，您不應該嘗試進行其他拓撲變更。
- 如果在雲端主控台中新增包含以下任何特殊字元的群組或政策：*?<>|:”，這些字元會在 Symantec Endpoint Protection Manager 中轉換為破折號。例如，如果您在 Symantec Endpoint Protection Manager 上命名群組 Europe***，則此群組會標示為 Europe---。
- 雲端主控台支援 14.3 及更新版本代理程式的位置感知，稱為政策目標。對於較早版本的代理程式，如果 Symantec Endpoint Protection Manager 群組具有多個位置且每個位置使用不同的政策（共用或非共用），則只有預設位置的政策將會同步並套用至雲端主控台上對等的群組。在雲端主控台重新與 Symantec Endpoint Protection Manager 同步之後，雲端主控台中該群組的政策將作為共用政策套用至 Symantec Endpoint Protection Manager 上對等群組中的所有位置。此程序將同時套用到 Symantec Endpoint Protection Manager 中的記憶體攻擊緩和政策和例外政策。
- 雲端主控台不支援透過 IPv6 的連線。透過 IPv6 網路註冊 Symantec Endpoint Protection Manager，導致以下錯誤：
Token #####
Symantec Endpoint Protection Manager #####

政策

- 您可從雲端管理政策。
仍必須直接從 Symantec Endpoint Protection Manager 管理低於 14 之用戶端的政策設定。但是存在例外。如果從雲端套用例外政策，且用戶端支援例外類型，則例外會套用至用戶端（無論版本為何）。記憶體攻擊緩和政策會套用至所有 14 版用戶端及更新版本。
- 在病毒和間諜軟體防護政策中，當網域在雲端主控台中註冊時，部分選項旁會顯示雲端圖示。當密集型防護政策生效時，該政策覆寫這些選項。
- 在 Symantec Endpoint Protection Manager 中，於雲端主控台中建立和指派的第一個預設雲端政策會附加一個 v 和數字 (#)，如下所示：## MEM ## v1。如果取消註冊並重新註冊 Symantec Endpoint Protection Manager 網域，則會在政策名稱後面附加額外的 v#。例如，## MEM ## v1 可能會變為## MEM ## v1 v1 或## MEM ## v1 v3。
- 在 Symantec Endpoint Protection Manager，某些雲端政策顯示在「用戶端」>「政策」標籤的清單中。雲端圖示表示政策源自雲端。

Table 44: 雲端圖示

圖示	說明
	此群組不會從其雲端主控台中的父系繼承政策。政策會直接套用至群組。
	此群組會從其雲端主控台中的父系繼承政策。

某些雲端主控台政策是新政策，有些是現有政策的雲端版本。用戶端版本決定用戶端會支援哪些政策。如果您將政策套用至不支援此政策的用戶端，該用戶端會忽略此政策。無論政策源自雲端主控台還是 Symantec Endpoint Protection

Manager，都會發生此行為。Symantec Endpoint Protection Manager 中的使用者介面表示雲端主控台控制的選項或整個政策。

- 混合管理的雲端主控台目前支援 Windows 用戶端的 Symantec Endpoint Protection Manager 政策，但不支援 Mac 或 Linux 用戶端的。您仍必須完全從雲端或完全從 Symantec Endpoint Protection Manager 管理 Mac 和 Linux 用戶端。請參閱：

[內部部署 SEPM 和雲端註冊的 SEPM 之間的功能差異](#)

政策繼承

來自雲端的政策不會遵循 Symantec Endpoint Protection Manager 的政策繼承組態。相反地，它們會遵循在雲端中定義的繼承規則。

子裝置群組會繼承父系裝置群組的政策。但是，您可以將政策直接應用於子群組或子裝置。不必關閉繼承。請參閱：

[內部部署 SEPM 和雲端註冊的 SEPM 之間的功能差異](#)

內部部署 SEPM 和雲端註冊的 SEPM 之間的功能差異

註冊 Symantec Endpoint Protection Manager 網域後，您便可以在 Symantec Endpoint Security (SES) 雲端主控台和 Symantec Endpoint Protection Manager (SEPM) 中管理政策。

Table 45: 功能參考

Symantec Endpoint Protection Manager	Symantec Endpoint Security
首頁	首頁 • 提供引導式首次使用者體驗，幫助您熟悉 SES 雲端功能。 • 包括一個關鍵效能指示器 (KPI) 欄以及互動式小工具 (圖表)，並包含向下切入的詳細資訊。 • 顯示可疑檔案偵測的詳細可見度。
用戶端、用戶端群組 依預設，從 Symantec Endpoint Protection Manager 管理。	裝置、裝置群組 若要從雲端管理群組，請選取「整合 > 註冊 > 從雲端管理裝置」選項。此選項僅影響群組建立或刪除以及裝置移動或刪除。該功能的運作方式與 Active Directory 和 Symantec Endpoint Protection Manager 的運作方式類似。 當網域的管理裝置選項 (從雲端管理裝置) 已啟用時，您必須使用雲端主控台來組織用戶端和用戶端群組。 如果您使用 Symantec Endpoint Protection Manager、Active Directory，或使用第三方 API 來管理裝置，則應該停用此選項。 您可以在雲端主控台中查看您的裝置和裝置群組。當網域以雲端伺服器註冊且裝置管理選項處於啟用狀態時，您無法在 Symantec Endpoint Protection Manager 中建立群組。啟用裝置管理選項後，會在雲端中管理群組結構。 如需詳細瞭解「從雲端管理裝置」選項的運作方式，請參閱： Symantec Endpoint Protection Manager 註冊設定
沒有對應的組態。	政策群組
政策繼承 在 Symantec Endpoint Protection Manager 中，如果您想要直接將政策套用至子群組，則必須停用政策繼承。 Note: 如果您取消註冊網域，從雲端直接套用至子群組的任何 MEM 政策都會套用至子群組及其位置，而不論 Symantec Endpoint Protection Manager 繼承設定為何。	政策繼承 在雲端主控台中，政策繼承永遠為啟用狀態。不過，您始終可以直接將政策套用至子群組，以覆寫父系政策。

Symantec Endpoint Protection Manager	Symantec Endpoint Security
監控和報告頁面	「資安事端和警示」頁面 您可以篩選資安事端和警示。兩種檢視都提供包含增強詳細資訊的向下切入。 觸發特定警示時，預設警示規則會通知管理員。角色管理提供了定義哪些管理員會收到相關事件警示的方法。 您可以在「資安事端和警示 > 警示規則」標籤檢視和編輯預先定義的警示規則。 資安事端可協助您快速分析事件，以決定如何在環境中調整政策。您可以在「資安事端和警示 > 資安事端」標籤上檢視資安事端
管理員角色 - 系統管理員 - 管理員 (基於網域) - 限制的管理員 (基於政策) 雲端主控台管理員和 Symantec Endpoint Protection Manager 管理員未以任何形式連結。	管理員角色 - 超級管理員 - 網域管理員 - 限制的管理員 - 安全分析人員 - 檢視者 雲端主控台中的預設管理者角色
主控台逾時 預設為 1 小時。您可以變更逾時。	主控台逾時 您無法變更此逾時期間。逾時為 2 小時。
活動訊號選項	無法使用。 所有政策變更會即時發生。

下表顯示哪些政策適用於雲端中註冊的 Symantec Endpoint Protection Manager，以及支援每個策略的最低用戶端版本。

Table 46: 政策功能參考

Symantec Endpoint Protection Manager	Symantec Endpoint Security
開箱即用政策 其他政策將繼續在 Symantec Endpoint Protection Manager 中進行管理： - 防火牆政策 - 裝置控制 - 入侵預防政策 - LiveUpdate 政策 - 主機完整性政策 - 除 Bloodhound、SONAR 啟發式、下載鑑識和掃描動作以外的病毒和間諜軟體防護政策選項。 - 應用程式與裝置控制 - 系統鎖定	依預設，從 Symantec Endpoint Protection Manager 管理。 若要從雲端管理下列政策，請選取「整合 > 註冊 > 從雲端管理裝置」選項： - 密集型防護政策 - 系統政策 (僅限低頻寬選項) - 允許清單政策 - 拒絕清單政策 - MEM 政策 如需詳細瞭解「從雲端管理政策」選項的運作方式，請參閱： Symantec Endpoint Protection Manager 註冊設定 完全雲端管理的 Symantec Endpoint Security 可管理 Symantec Endpoint Protection 未管理的其他政策。請參閱： 內部部署產品與 SES 的功能比較
病毒和間諜軟體防護政策中的下載鑑識、Bloodhound 和行為分析 (SONAR) 設定 以雲端伺服器註冊網域時，以下設定不適用於 Symantec Endpoint Protection 用戶端： - 病毒和間諜軟體防護政策偵測動作 - Bloodhound 設定 - 下載鑑識靈敏度滑動軸 - 下載鑑識感染狀況、首次出現和內部網路選項 - SONAR 啟發式偵測和 SONAR 可疑行為設定 如果您取消註冊網域，這些設定仍將用於用戶端。 Note: 預設的「密集型防護」攔截層級較「病毒和間諜軟體防護」政策中的最主動 Bloodhound 設定不主動。如果您目前的政策將 Bloodhound 指定在其最高層級，則可能需要增加密集型防護層級。	密集型防護政策 網域註冊後自動套用於 Windows 用戶端 針對 Windows 用戶端取代病毒和間諜軟體防護政策中的一些設定。 這些用戶端使用密集型防護政策取代其病毒和間諜軟體防護政策中的某些現有設定： - Bloodhound - SONAR 啟發式 - 下載鑑識選項 - 掃描動作 不過，用戶端仍會使用其病毒和間諜軟體防護政策中的其他選項。
例外政策 在 Symantec Endpoint Protection Manager 中，有一個例外政策，其中包含對許多不同項目的排除以及應用程式的排除。雲端伺服器允許清單和拒絕清單政策會以個別政策出現在 Symantec Endpoint Protection Manager 中。 雲端伺服器中的專案將顯示在「例外」政策 > 「例外」清單中。 網域註冊後，只能為雲端伺服器中不支援的類型建立例外。	允許清單政策 即使將網域取消註冊，您在雲端中建立的任何允許清單政策仍會出現在 Symantec Endpoint Protection Manager 中。 雲端主控台包括允許或攔截之項目的中央清單，因此您可以在同一個位置檢視所有這些項目。 在 14.3 RU1 中，許可清單政策已重新命名為允許清單政策。
例外政策 來自雲端主控台的拒絕清單政策不會掃描例外。但是，來自雲端主控台的拒絕清單項目會出現在「例外」清單中。	拒絕清單政策 即使將網域取消註冊，您在雲端中建立的任何拒絕清單政策仍會出現在 Symantec Endpoint Protection Manager 中。 您可以在雲端伺服器或 Symantec Endpoint Protection Manager 中配置例外。雲端伺服器當前不支援完整範圍的例外。 Note: 「拒絕清單」政策是一種應用程式控制類型，其使用 Symantec Endpoint Protection Manager 中的行為分析 (SONAR) 來強制執行其規則。它不會使用 Symantec Endpoint Protection Manager 中的應用程式控制驅動程式。 在 14.3 RU1 中，黑名單政策已重新命名為拒絕清單政策。

Symantec Endpoint Protection Manager	Symantec Endpoint Security
沒有對應的選項。 Symantec Endpoint Protection Manager 會顯示低頻寬狀態。您可以在「外部通訊」>「雲端設定」中查看是否已啟用低頻寬選項。 Symantec Endpoint Protection Manager 還會管理低頻寬運作所需的 LiveUpdate AML 內容。	系統政策 (低頻寬選項) 系統政策是雲端中在 Symantec Endpoint Protection Manager 中沒有對應組態的新政策。但是，「低頻寬」選項要求在 Symantec Endpoint Protection Manager 上提供低頻寬進階機器學習 (AML) LiveUpdate 內容，此政策才會有效。 預設值為關閉。
記憶體攻擊緩和 (MEM) 政策 註冊網域時，必須使用雲端伺服器配置此政策。	攻擊緩和 (MEM) 政策 適用於自訂應用程式的 14.2 RU1 和更新版本。您必須已啟用應用程式隔離。用戶端必須安裝應用程式強化。 政策選項可與 Symantec Endpoint Protection Manager 中的選項相比。

針對混合 Symantec Endpoint Protection Manager、用戶端與雲端伺服器之間的通訊問題進行疑難排解

閱讀在混合環境中 Symantec Endpoint Protection Manager (SEPM) 與 Symantec Endpoint Security (SES) 雲端伺服器之間可能的通訊問題。

內部部署 Symantec Endpoint Protection Manager 如何與雲端伺服器進行通訊？

作為內部部署 SEPM 註冊程序的一部分，SEPM 會使用連接器連線到雲端伺服器。SEPM 會自動安裝連接器和上傳程式服務，但是這些服務僅能在註冊至雲端的 SEPM 上作用中。連接器使用 Google Cloud Platform (GCP) 將群組和事件資料上傳至雲端。

註冊的站台和雲端伺服器同步之後，SEPM 會：

- 為所有位於此站台的用戶端上傳群組、裝置和日誌事件。內部部署 SEPM 群組結構是 SEPM 傳送至雲端伺服器的其中一個第一段資料。同步的用戶端會置於雲端中重複的「我的公司」群組中。
- 將報告事件與雲端伺服器同步。
- 從雲端伺服器接收政策、日誌與指令，並立即將資料傳遞至與此網站進行通訊的用戶端。

如果一個站台具有多部管理伺服器，則第一個註冊的 SEPM (SEPM A) 會上傳群組資料。如果 SEPM A 無法與雲端伺服器通訊，則 SEPM B 會開始上載群組資料。SEPM B 是以管理伺服器清單為基礎。

針對通訊問題進行疑難排解

問題	解決方案
在管理伺服器升級期間，橋接器服務會停止，並且無法與雲端同步。	確保站中的所有管理伺服器皆可存取所需的 URL。作為最佳實務，允許下列服務進行連線。請參閱： Endpoint Protection (SEP) 和 Endpoint Protection (SES) 所需的外部 URL - 賽門鐵克雲端 API 閘道 - 雲端通知服務 (SPOC) - 雲端儲存服務 - SSL/TLS 憑證： http://crl3.digicert.com/DigiCertGlobalCAG2.crl http://crl4.digicert.com/DigiCertGlobalCAG2.crl http://ocsp.digicert.com
Symantec Endpoint Protection Manager 與雲端伺服器之間的同步會延遲。 為了驗證延遲，畫面將顯示 semapisrv_log 的以下項目： [HubSyncCheckTask] ERROR c.s.s.s.m.c.cloud.sepm.hubSyncCheckTask - hub agent [ASSET_UPLOAD] delayed by [64] hours	此錯誤發生在以下情況： - Symantec Endpoint Protection Manager 僅在一天中偶爾或短時間內連接到網路。 - 您的環境使用存取所需 URL 需要的代理設定。如果您的環境使用代理設定，則它可能適用於已登入使用者，而非執行 Symantec Endpoint Protection Manager 的系統使用者。因此 Symantec Endpoint Protection Manager 無法連線。 若要解決此問題，請執行下列動作： - 請檢查防火牆和 / 或代理設定是否封鎖來自 Symantec Endpoint Protection Manager 的存取。 - 請確認 Symantec Endpoint Protection Manager 可以連接到以下 URL：http://crl3.digicert.com/、http://crl4.digicert.com/ 和 http://ocsp.digicert.com/ 整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站 - 請確認您的代理設定適用於 SYSTEM 帳戶。
您想要使用通知來告知您管理伺服器是否與雲端同步。	如果 Symantec Endpoint Protection 橋接器服務和上載程式服務停止，則用戶端和群組結構不會與雲端同步。在 14.3 RU6 或更新版本中，「系統日誌 > 伺服器活動」日誌類型會顯示一個事件，詳述 SEPM 是否已成功註冊至雲端伺服器。 此外，SEPM 還會驗證與雲端服務 (14.3 RU6 和更新版本) 適當連線所需的數個 URL。 當雲端伺服器在至少 7 天未收到來自 SEPM 連接器的任何資料時，SES 會向您顯示以下報示規則： SEPM 橋接器服務中沒有最近活動
Symantec Endpoint Protection Manager 升級之後，SEPM 未連線到雲端伺服器。 在 SES 雲端日誌中，您會看到以下 403 錯誤： #####403 #####403#####	如果您從雲端伺服器取消註冊 SEPM，則會發生此錯誤，這有時會導致雲端伺服器不同步。雲端伺服器可能會錯誤地告知 SEPM 仍已註冊。 若要解決此問題，請重新註冊 SEPM 網域。 - 在 SEPM 主控台中，按一下「進階安全性」頁面底部的「設定」選項。 - 複製並貼上您從雲端主控台「整合 > 註冊」頁面取得的註冊 Token。 - 按一下「註冊 Symantec Endpoint Protection Manager」，然後確認您是否想要註冊。然後，SEPM 會偵測到雲端伺服器未同步。
SEPM 會在雲端中註冊，但有同步問題。	從 RU7 起，伺服器活動日誌類型會顯示 SEPM 和雲端伺服器是否成功同步。這些訊息包括下列狀況： <i>Symantec Endpoint Protection Manager</i> 無法與雲端同步。 <i>Symantec Endpoint Protection Manager</i> 與雲端的同步狀態不明。 <i>Symantec Endpoint Protection Manager</i> 未與雲端同步。
在註冊並與雲端同步之後，您已將用戶端新增至 SEPM，但用戶端並未移至雲端。	每當您變更裝置群組結構時，均會延遲數分鐘，變更才會在 SEPM 中出現。反之亦然。每當您變更裝置群組結構時，均會延遲數分鐘，變更才會在 SEPM 中出現。 在延遲期間，您不應該嘗試進行其他拓撲變更。變更可能不會生效。

更多資訊

- 如需針對 SEPM 中註冊問題進行疑難排解的詳細資訊，請參閱：[「進階安全性」頁面問題疑難排解](#)
- [向雲端主控台中的遠端複製夥伴註冊網站](#)
- [將 Symantec Endpoint Protection Manager 網域註冊到雲端主控台後，會發生什麼情況？](#)

「進階安全性」頁面問題疑難排解

瞭解如何疑難排解您嘗試在「進階安全性」頁面上啟動自適應防護時的問題。

這些問題適用於 Symantec Endpoint Protection 14.3 RU3 和更新版本。

啟動自適應防護

當您嘗試將 Symantec Endpoint Protection Manager 網域註冊到雲端並在「進階安全性」頁面上啟動自適應防護時，可能會看到下列訊息：#####Symantec Endpoint Protection Manager #####

下表顯示可能的原因和解決方案。

原因	解決方案
授權： • 您使用的授權過時。 • 您可能具有僅限內部部署 Symantec Endpoint Protection 授權。您需要 Symantec Endpoint Security Enterprise 或 Symantec Endpoint Security Complete 授權，才能以雲端伺服器註冊。	請聯絡合作夥伴或代理商以續購授權，或是將其升級到新的 Symantec Endpoint Security Complete 或 Symantec Endpoint Security Enterprise 訂閱。 更多資訊： 購買和續購 Symantec Endpoint Security 中的訂閱 Symantec Endpoint Security 的授權常見問答集
管理伺服器未從用戶端收集遙測： 1. 您可能會取得部分用戶端的提交，但不能從所有群組中的所有用戶端進行。 2. 用戶端可能未與所有賽門鐵克元件通訊。 3. 如果您在環境中使用一或多個 Proxy 以將必要的流量重新定向至賽門鐵克伺服器，則請確定您的網路防火牆允許賽門鐵克用來執行多個功能的 URL。	1. 請確定您已為所有群組 (而不是群組內的一部分用戶端) 啟用用戶端提交。請參閱：管理用戶端傳送給賽門鐵克的匿名或非匿名資料 2. 請確定已開啟下列通訊埠：TCP 139、445、443；HTTPS 443。請參閱：Symantec Endpoint Protection 的通訊埠 3. 如果您使用 Proxy，則請允許下列 URL： Symantec Endpoint Protection (SEP) 所需的外部 URL
Symantec Security Cloud 帳戶問題： 1. 您還沒有 Symantec Security Cloud 帳戶。 2. 您組織中的某個人已經有 Symantec Security Cloud 帳戶。第一次購買時，會自動建立新的租用戶。您不應該建立多個租用戶。租用戶的資訊根據合作夥伴針對合約提交給 Broadcom 的電子郵件。	1. 您必須手動建立 Symantec Security Cloud 帳戶。若要登入 Symantec Security Cloud，請從 Web 瀏覽器前往下列 URL： securitycloud.symantec.com 請參閱：登入 Symantec Security Cloud 帳戶 2. 如需現有帳戶的說明，請使用下列其中一種方法來開啟 Global Customer Care (GCA) 案例： • 提交 Customer Care 網頁表單： https://ca-broadcom.wolkenservicedesk.com/web-form • 使用 BOT，與 Customer Care 代表聊天： https://support.broadcom.com/security • 透過 Support Online 帳戶來記錄案例： http://support.broadcom.com • 撥打： • 北美：1-800-225-5224。 • 其他區域：https://support.broadcom.com/contact-support.html

選取「啟用調適型分析」選項後，「進階安全性」頁面隨即顯示 403 錯誤。	此錯誤的發生原因如下： 雲端伺服器無法授權 SEPM，因此無法在雲端伺服器上佈建租用戶。若您僅有 Symantec Endpoint Security Enterprise 授權，則此錯誤很少發生。 若要解決此問題，請執行下列動作： 1. 請選取「進階安全性」頁面底部的「設定」選項來註冊 SEPM 網域。 2. 複製並貼上您從雲端主控台「整合 > 註冊」頁面取得的註冊 Token。 3. 按一下「註冊 Symantec Endpoint Protection Manager」，然後確認您是否想要註冊。

如果您仍然無法解決問題，則請聯絡 Broadcom 支援，請參閱：[Symantec Enterprise Security](#)

註冊問題

下表顯示您嘗試註冊 SEPM 網域時可能出現的一些問題和解決方案。

問題	說明
出現「未建立 Symantec Security Cloud 帳戶」訊息。 	發生下列其中一種情況時，會出現此訊息： • 已註冊不同的 Symantec Endpoint Protection Manager 網域。您一次可以將一個網域註冊到雲端伺服器。若要註冊您想要的網域，請先取消註冊不想要的網域。然後重新註冊想要的網域。若要取消註冊網域，請關閉「設定」頁面上的「註冊狀態」切換。 • 此精靈未建立 Symantec Security Cloud 帳戶，因為您已有具有「驗證電子郵件地址」畫面中所指定地址的帳戶。要解決此問題，請直接登入到您的 Symantec Security Cloud。不過，此精靈已為您註冊 SEPM 網域。
<pre>### Token ##### Symantec Endpoint Protection ##### ## ##### ##### Symantec Endpoint Protection ##### #####</pre>	Symantec Endpoint Protection Manager 偵測到您已使用相同的 Token 將網域註冊到雲端伺服器。您不應將多個 SEPM 安裝註冊到一個 SES 網域中，否則來自多個網域的資料會合併在一起。 • 按一下「取消」會停止註冊並取得不同的註冊 Token。 • 如果您要從註冊之前所建立的備份中復原，請按一下「繼續」。
我想要使用與剛剛使用之 Symantec Security Cloud 帳戶不同的電子郵件地址來建立帳戶。	如果您已使用此精靈建立帳戶，則無法再次使用此精靈。相反地，請登入 Symantec Security Cloud 帳戶以存取 SES，並建立系統管理員帳戶。如需詳細資訊，請參閱：建立管理員帳戶 如果組織中的某個人已經建立帳戶，則您可能無法登入。
熱圖中的資料自我上次看到後尚未變更。	自適應防護行為熱圖資料每 24 個小時重新整理一次。因為熱圖沒有時間戳記，所以您應該每天檢查一次資料。

已知問題

錯誤	解決方案
當您按一下「進階安全性」頁面時，可能會看到下列錯誤訊息：#####	若您使用 Symantec Endpoint Security Enterprise 授權啟用自適應防護，則會出現此問題。您必須從合作夥伴或代理商購買 Symantec Endpoint Security Complete 授權。
當您按一下「進階安全性」頁面時，可能會看到下列錯誤訊息：sym-ui-sep-shared.errors.ERROR	若要解決此問題，請依序嘗試下列任務。在每個任務之後，請等待自適應防護熱圖出現。 1. 在右上角，按一下「重新整理」。 2. 導覽至另一個頁面，然後返回「進階安全性」頁面。 3. 登出並關閉 SEPM，然後重新啟動 SEPM。按一下「進階安全性」頁面。

請參閱：[針對混合 Symantec Endpoint Protection Manager、用戶端與雲端伺服器之間的通訊問題進行疑難排解](#)

Symantec Endpoint Protection Manager 例外政策如何與 Symantec Endpoint Security (SES) 雲端主控台互動？

例外政策如何在雲端主控台上運作？

雲端主控台並非支援 Symantec Endpoint Protection Manager 支援的所有例外。在雲端伺服器中註冊 Symantec Endpoint Protection Manager (SEPM) 網域之後，會根據例外類型將雲端主控台中原始 Symantec Endpoint Protection Manager 例外政策分為兩種政策類型，稱為「拒絕清單政策」和「允許清單政策」。

雲端政策不支援的例外仍保留在 Symantec Endpoint Protection Manager 例外政策中。在雲端伺服器和 Symantec Endpoint Protection Manager 同步之後，會將雲端式政策重新匯入 Symantec Endpoint Protection Manager 中。

例如，假設在 Symantec Endpoint Protection Manager 中建立稱為「SEPM 例外政策」的政策。此政策包含「應用程式」例外、「信任的 Web 網域」例外和「要監控的應用程式」例外。在雲端伺服器中註冊之後，「SEPM 例外政策」中的雲端式例外會分為兩種政策。這些政策稱為「匯入的 SEPM 例外政策 (BL)」和「匯入的 SEPM 例外政策 (WL)」。「拒絕清單」政策僅透過「應用程式」例外建立，而「允許清單」政策則透過「應用程式」例外和「網域」例外建立。原始的 Symantec Endpoint Protection Manager「SEPM 例外政策」會保留「要監控的應用程式」例外。在雲端伺服器與 Symantec Endpoint Protection Manager 同步之後，Symantec Endpoint Protection Manager 會顯示指派給同一個群組的三個政策：SEPM 例外政策、匯入的 SEPM 例外政策 (DL) v1 和匯入的 SEPM 例外政策 (AL) v1

在雲端主控台中，黑名單政策已重新命名為拒絕清單政策。白名單政策已重命名為允許清單政策。

如需詳細資訊，請參閱：

[建立病毒和間諜軟體掃描的例外](#)

此外，雲端主控台的允許清單和拒絕清單政策並非支援 Symantec Endpoint Protection Manager 例外政策支援的所有動作。雲端主控台之允許清單政策中的「應用程式」例外僅支援「忽略」動作。雲端主控台之拒絕清單政策中的「應用程式」例外僅支援「隔離」動作。如果在 Symantec Endpoint Protection Manager 例外政策中新增「應用程式」例外，然後在雲端伺服器中註冊 Symantec Endpoint Protection Manager，則雲端伺服器政策中的動作會自動變更。對於允許清單政策，「只記錄」動作會轉換為「忽略」動作。「終止」和「移除」動作會轉換為「隔離」動作。將這些政策重新匯入 Symantec Endpoint Protection Manager 中之後，管理伺服器會保留雲端主控台政策中的動作。

如需詳細資訊，請參閱：

[在 Windows 用戶端上監控應用程式以建立應用程式的例外](#)

雲端主控台支援和不支援哪些例外？

在 Windows 用戶端上，雲端主控台支援以下例外：

拒絕清單政策：

- 雜湊 (SHA-256)

允許清單政策：

- 憑證
- 檔案名稱
- 網域
- 雜湊
- 檔案路徑
- 副檔名
- IPS 主機

在雲端伺服器中註冊 Symantec Endpoint Protection Manager 之後，Symantec Endpoint Protection Manager 例外政策中的 Windows 例外會轉換為以下政策類型和例外類型：

Table 47: SEPM Windows 例外及其轉換為雲端式例外的方式

Symantec Endpoint Protection Manager 例外政策	拒絕清單政策	允許清單政策
應用程式	雜湊 (僅限 SHA-256)	雜湊 (僅限 SHA-256)
憑證	不適用	憑證
檔案 > 安全風險/SONAR	不適用	檔案名稱
資料夾 > 安全風險/SONAR	不適用	路徑
信任的 Web 網域	不適用	網域

以下 Windows 例外將保留在 Symantec Endpoint Protection Manager 例外政策中，但在雲端主控台中不受支援：

- 要監控的應用程式
- 副檔名
- 檔案 - 應用程式控制
- 資料夾 - 應用程式控制
- 已知風險
- 竄改防護例外
- DNS 或主機檔案變更例外

雲端伺服器不支援 Linux 用戶端例外或 Mac 用戶端例外。所有 Linux 例外項目和 Mac 例外項目均保留在 Symantec Endpoint Protection Manager 例外政策中。

NOTE

您也可以使用從 Symantec Endpoint Protection Manager 匯出之總和檢查碼的 .csv 檔案，將例外直接新增至雲端主控台。此檔案指紋清單包含位於電腦上指定路徑中之每個執行檔或 DLL 的路徑、檔案名稱以及對應的總和檢查碼。請參閱：

[以 checksum.exe 建立檔案指紋清單](#)

如需詳細資訊，請參閱：

[針對哪種類型的掃描使用哪些 Windows 例外？](#)

使用者可在 **Windows** 用戶端上新增的例外

Symantec Endpoint Protection Manager 例外政策允許您讓 Windows 用戶端上的使用者新增例外 (稱為用戶端限制)。

如果 Symantec Endpoint Protection Manager 在雲端伺服器中註冊，則 Symantec Endpoint Protection Manager 不會顯示以下用戶端限制：

- 應用程式例外
- 檔案例外
- 資料夾例外 > 安全風險例外/SONAR 例外
- 信任的 Web 網域例外
- 憑證例外

NOTE

此外，在雲端式例外政策所控制的 Windows 用戶端上，這些例外不會顯示在用戶端使用者介面中。

無論是否已註冊 Symantec Endpoint Protection Manager，Symantec Endpoint Protection Manager 都不會顯示以下用戶端限制。

- DNS 或主機檔案變更例外
- 副檔名例外
- 已知風險例外

如需詳細資訊，請參閱：

[限制使用者可在用戶端電腦上架構的例外類型](#)

註冊例外政策以及將其與雲端伺服器同步的問題

- 只有在原始 Symantec Endpoint Protection Manager 例外政策包含拒絕清單政策和允許清單政策支援的例外時，才會自動在雲端主控台中建立拒絕清單政策或允許清單政策。否則，雲端主控台會忽略例外政策。
- 註冊之後，只有已指派的 Symantec Endpoint Protection Manager 例外政策會與雲端伺服器同步，然後這些政策將重新匯入 Symantec Endpoint Protection Manager 中。未指派的政策與非雲端式例外政策一起保留在 Symantec Endpoint Protection Manager 中。此外，如果已指派的 Symantec Endpoint Protection Manager 例外政策沒有拒絕清單例外或允許清單例外，則會針對該群組在雲端主控台中建立對應的空白拒絕清單政策和/或空白允許清單政策。
- 註冊之後，您可以在 Symantec Endpoint Protection Manager 中建立和指派非雲端式例外政策。但是，這些政策必須僅包含以 Symantec Endpoint Protection Manager 為基礎的例外，而非雲端式例外。如果您建立和指派雲端型拒絕清單政策或允許清單政策，這些政策會自動同步並匯入到 Symantec Endpoint Protection Manager 中。
- 取消註冊網域之後，在雲端主控台中建立的例外政策仍會保留在 Symantec Endpoint Protection Manager 中。但是，這些雲端式政策會從 Symantec Endpoint Protection Manager 中的群組取消指派。您可以合併、重新指派或刪除這些政策（如果您不再需要這些政策）。
- 如果將 Symantec Endpoint Protection Manager 例外政策匯入雲端主控台且該政策具有應用程式例外，則這些例外會在政策匯入後遺失。您必須手動將應用程式例外重新新增至雲端主控台的拒絕清單和允許清單政策。雲端主控台會保留其他類型的例外，例如憑證例外。

向雲端伺服器中的遠端複製夥伴註冊網站

如何在雲端伺服器中註冊網站？

在 14.3 MP1 (14.3.1169.0100) 版和更新版本，可在雲端伺服器中註冊的一個網站，與不在雲端伺服器中註冊的其他網站之間設定遠端複製。您可以註冊一個網站作為主要網站。所有其他網站可以直接與主要網站進行遠端複製，或彼此進行遠端複製。例如，如果網站 A 為主要網站，將網站 A 註冊到雲端伺服器。可以架構網站 B 和網站 C 與網站 A 進行遠端複製。也可以架構網站 B 與網站 A 進行遠端複製，並架構網站 C 與網站 B 進行遠端複製。

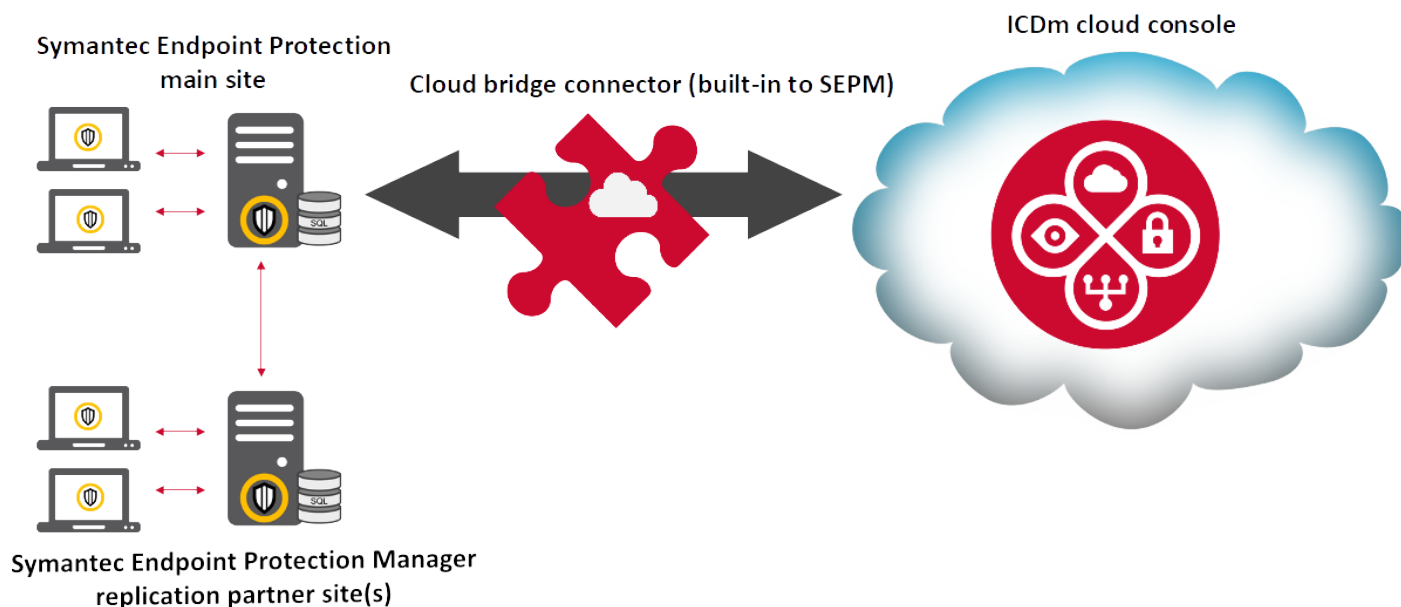


Table 48: 註冊多個遠端複製網站的程序

工作	說明
步驟 1：遠端複製兩個網站，然後在雲端伺服器中註冊。	註冊主要網站之前請遠端複製所有政策、群組和日誌事件，以避免任何資料庫衝突。您也可以先在雲端中註冊主要網站後，新增遠端複製夥伴。 主要網站可以有許多夥伴網站。請參閱： • 立即遠端複製資料 • 什麼是站台以及複寫如何運作？
步驟 2：註冊主要網站。	選擇並註冊一個網站作為主要網站，以執行註冊和任何進一步的動作，例如建立政策。 對於具有多個管理伺服器的網站，您只需要註冊其中一個管理伺服器。任何其他管理伺服器均會自動註冊。 不要在雲端伺服器中註冊第二個網站或夥伴網站
步驟 3：等待執行同步。	在註冊的主要網站和雲端伺服器同步後，會在主要網站上發生下列事件： • Bridge 服務會自動安裝在所有管理伺服器上。不過，Bridge 服務僅對會用於在雲端伺服器中註冊的管理伺服器有效。 • 主要網站會同步報告事件與雲端伺服器。 • 主要網站針對未連線到此網站的所有用戶端上傳群組、裝置、政策、日誌事件、用戶端套件，以及定義檔。 • 主要網站從雲端伺服器接收政策、日誌與指令，並立即將資料傳遞至與此網站進行通訊的用戶端。 如需詳細資訊，請參閱： 將 Symantec Endpoint Protection Manager 網域註冊到雲端伺服器後，我該如何管理用戶端和政策？
步驟 4：遠端複製主要網站及任何夥伴網站。	排程遠端複製，以便這兩個網站具有相同的註冊資料。執行遠端複製後，夥伴網站上會發生下列事件： • 夥伴網站會根據與主要網站的遠端複製排程，從雲端伺服器接收內容。然後，連線到夥伴網站的用戶端會收到此資料。 • 夥伴網站會從主要網站取得註冊詳細資料。這些詳細資料會顯示在 Symantec Endpoint Protection Manager 進階安全性頁面 > 設定 > 疑難排解。 • 夥伴網站的管理伺服器不會安裝 Bridge 服務。因此，夥伴網站不會直接與雲端伺服器同步。 如需詳細資訊，請參閱： 如何安裝第二個網站用於遠端複製

工作	說明
步驟 5：(選擇性) 將群組和裝置的控制切換至雲端伺服器。	依據預設，當您註冊未遠端複製的 Symantec Endpoint Protection Manager 網域時，雲端伺服器會管理用戶端群組結構。依據預設，當您註冊已遠端複製的網站時，Symantec Endpoint Protection Manager 會管理群組結構。 - 如果 Symantec Endpoint Protection Manager 為主要網站，您可以在主要網站上新增群組和政策，然後便會在夥伴網站上進行遠端複製。 - 如果將雲端伺服器設為主要網站，請先執行與夥伴網站的遠端複製。此遠端複製可確保您在夥伴網站上新增的群組和政策同步到雲端伺服器。 若要將控制切換到雲端伺服器，請在 Symantec Endpoint Security 雲端主控台的「整合 > 註冊」中進行註冊後，啟用「從雲端管理裝置」選項。

您無法針對遠端複製的夥伴執行容錯移轉或負載平衡。

請參閱：[設定容錯移轉和負載平衡](#)

NOTE

如果您在主要網站與雲端伺服器同步後，將新用戶端新增到複寫夥伴網站，則這些用戶端將顯示在雲端的「預設」群組中。反之，請先等待複寫網站與主要網站同步，且主要網站與雲端伺服器同步，再將更多用戶端新增到新群組。

在雲端伺服器中註冊的網站之間移除與還原遠端複製

如果您移除主要網站和夥伴網站之間的夥伴關係，會一併移除與雲端伺服器的夥伴關係。

若要還原與主要網站的夥伴關係，請使用「新增現有遠端複製夥伴」精靈。

您也可以直接在雲端伺服器中註冊夥伴網站，以作為個別網站。在此情況下，您必須建立不同的 Symantec Security Cloud 帳戶。若要還原與主要網站的夥伴關係，您必須取消註冊夥伴網站。然後，在主要網站上，使用「管理伺服器組態精靈」重新架構夥伴關係。

NOTE

作為最佳實務準則，將夥伴網站保留為個別網站，且請勿嘗試還原與主要網站的遠端複製。

如需詳細資訊，請參閱：

- 在升級前後停用遠端複製和還原遠端複製
- 重新安裝或重新架構 Symantec Endpoint Protection Manager

疑難排解雲端伺服器中的網站遠端複製

取得主要網站註冊和遠端複製的相關資訊：

- 尋找遠端複製事件。
在主要網站上，開啟「系統日誌」>「管理」日誌類型，並尋找「遠端複製事件」事件類型。請參閱：[檢視日誌](#)
- 從 Symantec Endpoint Protection Manager 進階安全性 > 設定頁面上檢視合作夥伴網站的註冊狀態：
在夥伴網站上，「註冊狀態」顯示為「已註冊」。
「連線狀態」等其他欄位則顯示「無」。
若要顯示註冊資訊，請參閱「疑難排解」。

[混合管理 Symantec Endpoint Protection Manager \(SEPM\) 如何與 Symantec Endpoint Security \(SES\) 雲端主控台互動](#)

在低頻寬環境中更新用戶端

何謂低頻寬模式？

低頻寬模式是至少符合下列其中一個準則的這些環境的選項：

- 需要較不頻繁的病毒和間諜軟體、行為分析 (SONAR) 和 IPS 內容更新
- 對雲端伺服器的連線能力較低

低頻寬用戶端較不常接收更新。賽門鐵克每週會更新低頻寬內容一次。在低頻寬模式下，您可以使用主動模式政策更好地調整端點上的安全性。請參閱：

[Symantec Endpoint Protection 如何使用進階機器學習？](#)

您必須在雲端伺服器中註冊，才能使用低頻寬政策。低頻寬預設為關閉。

- 在雲端主控台中，於「預設系統政策 (14)」中啟用低頻寬模式。
- 確定 LiveUpdate 下載低頻寬內容。
- 建立取得低頻寬內容的用戶端群組。

啟用低頻寬模式之後，您可以在「預設」檢視和「防護技術」檢視的「用戶端」標籤中查看其狀態。您也可以根據低頻寬內容派送產生報告。

從雲端啟用低頻寬模式

請在 Symantec Endpoint Security (SES) 雲端主控台的系統政策中，啟用或停用低頻寬模式。

1. 在 SES 雲端主控台中，前往「政策」>「預設系統政策 (14)」。
2. 開啟「在低頻寬模式下執行」。
3. 按下「儲存政策」。

下載低頻寬內容至 Symantec Endpoint Protection Manager (SEPM)

依據預設會下載和啟用進階機器學習內容。您可以使用以下程序來驗證已啟用它們。

下載低頻寬內容至 Symantec Endpoint Protection Manager

1. 在 Symantec Endpoint Protection Manager 主控台中，按下「管理員 > 本機網站 > 編輯網站屬性」。
2. 按下以選取 **LiveUpdate** 標籤，然後按下「要下載的內容類型」旁的「變更選定內容」。
3. 確定已勾選「進階機器學習」旁的方塊。
4. 按下「確定 > 確定」儲存變更。

在 LiveUpdate 內容政策中包含低頻寬內容

在 Symantec Endpoint Protection Manager 主控台中，前往「政策 > LiveUpdate」，然後編輯指派給群組 (包含啟用低頻寬的用戶端) 的政策。

1. 按下「LiveUpdate 內容」，然後連按兩下「LiveUpdate 內容政策」。
2. 在「Windows 設定」下方，按下「安全性定義檔」。
3. 在雲端主控台中，按下「裝置」，然後在「我的公司」下新增子群組。
4. 確保已勾選「進階機器學習」方塊。
5. 按下「確定」儲存變更。

針對低頻寬用戶端建立群組

1. 在雲端主控台中，按下「裝置」，然後在「我的公司」下新增子群組。
如果您無法新增子群組，請在雲端主控台 (「設定 > Symantec Endpoint Protection Manager 註冊」) 中啟用「管理裝置」。否則，請在 Symantec Endpoint Protection Manager 中新增群組。如果您使用 Active Directory 同步，請透過 Active Directory 新增群組。
2. 將「系統政策」套用至您先前架構為使用低頻寬的群組。在裝置群組上，按下「套用政策」，新增系統政策，然後按下「提交」。
3. 在 Symantec Endpoint Protection Manager 主控台中，確保您先前架構的 LiveUpdate 內容政策已套用至您建立的群組。您在 Symantec Endpoint Protection Manager 中啟用或停用的政策繼承僅會套用到 Symantec Endpoint Protection Manager 政策，而不會套用到雲端式裝置政策。

您可能必須預留一些時間供群組從雲端伺服器同步。

在於低頻寬模式下執行的用戶端上執行報告

您可執行報告以列出接收低頻寬內容的用戶端。

1. 在 Symantec Endpoint Protection Manager 主控台中，按下「報告 > 快速報告」，然後進行下列選擇：
 - 報告類型：「電腦狀態」
 - 選取報告：「低頻寬內容派送」
2. 選取時間範圍：「更多選項的其他設定」。
3. 按下「建立報告」。

從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端

漫遊 Symantec Endpoint Protection 用戶端是偶爾連線至管理伺服器的用戶端。漫遊用戶端會在風險較高的其他位置存取 Internet，例如機場、旅館或其他公司。Symantec Endpoint Protection Manager 可使用位置偵測對這些用戶端電腦提供網路內和網路外防護。

如果漫遊用戶端無法連線至管理伺服器，用戶端會自動將嚴重事件傳送至雲端主控台。漫遊用戶端重新連線至管理伺服器後，會傳送管理伺服器上任何新的重大事件。此外，不會再將此用戶端視為漫遊用戶端。

使用嚴重事件清單作為加強 Symantec Endpoint Protection Manager 安全政策的方式。例如，假設當 Employee1 位於特定旅館時，Employee1 的用戶端會遭受更多的阻斷服務攻擊。因此，您可以建立該旅館的位置，並在防火牆政策中啟用阻斷服務偵測。

如需詳細資訊，請參閱：

- [雲端入口網站顯示的嚴重事件有哪些？](#)
- [關於從管理伺服器監控遠端用戶端](#)
- [Endpoint Protection 的位置偵測最佳實務](#)

尋找漫遊用戶端和嚴重事件

若要找出漫遊的用戶端，請尋找下列項目：

- 裝置是否直接連線到雲端主控台而非管理伺服器。
- Symantec Endpoint Protection Manager 位置偵測政策中所定義的位置
- 用戶端的外部 IP 位址。

尋找漫遊用戶端和嚴重事件

1. 在雲端主控台中，前往「資安事端和警示」。
2. 在「安全事件」標籤上的「連線類型」下方，按下「雲端」以顯示用戶端傳送至雲端主控台的事件。

若要顯示管理伺服器傳送的事件，請按下 **Symantec Endpoint Protection Manager**。

3. 在「嚴重性」下方，按下「嚴重」。

雲端主控台僅過濾和顯示漫遊用戶端偵測到的嚴重安全事件。

4. 若要尋找位置和外部 IP 位址，請選取該裝置並尋找裝置位置項目。

雲端主控台顯示的嚴重事件有哪些？

漫遊用戶端將下列安全事件上傳到雲端主控台：

-
- 通訊埠掃描事件
 - Mac 詐騙
 - 阻斷服務
 - 卡納里群島
 - IP
 - 記憶體攻擊緩和
 - 主機完整性遵從

漫遊用戶端將下列安全事件上傳到雲端主控台：

- 防毒
- 行為分析 (SONAR)

從雲端伺服器取消註冊 Symantec Endpoint Protection Manager 網域

取消註冊過程將刪除雲端中未註冊網域的用戶端群組和用戶端。任何關聯的政策都保留在雲端主控台中以及相關事件中。從 Symantec Endpoint Security (SES) 雲端伺服器取消註冊 Symantec Endpoint Protection Manager 網域後，您無法再：

- 從雲端主控台管理裝置。
- 查看裝置上的檔案和應用程式。
- 將雲端特定的政策套用到裝置和裝置群組以保護它們。

在取消註冊過程中，雲端主控台上會顯示一條通知，您無法：

- 執行與裝置管理關聯的任何功能，例如創建群組、刪除群組或在群組之間移動裝置。
- 執行與政策管理關聯的任何功能，例如將政策套用到裝置或裝置群組。
- 註冊新網域，直到當前網域取消註冊。

NOTE

若要取消註冊網域，您需要 **Endpoint** 主控台超級管理員角色。請參閱：

[建立管理員帳戶](#)

取消註冊後，您會繼續在雲端主控台中看到警報、事件和政策。

取消註冊 **Symantec Endpoint Protection Manager** 網域

1. 在 Symantec Endpoint Security 雲端主控台上，前往「整合」。
2. 在 [註冊] 標籤上，選中 [網域註冊狀態] > [已註冊] 核取方塊，然後選擇 [取消註冊]。
3. 在「取消註冊網域」視窗中，輸入「####」以確認執行「取消註冊並刪除」動作。
4. 選取「取消註冊網域」以從雲端主控台取消註冊 Symantec Endpoint Protection Manager 並移除所有發現的裝置和檔案資訊。

NOTE

通常取消註冊需要兩個小時才能完成。

更多資訊

[將 Symantec Endpoint Protection Manager 網域註冊到雲端伺服器](#)

[將 Symantec Endpoint Protection Manager 網域註冊至雲端伺服器中 \(14.3 RU3 或更新版本\)](#)

授權 Symantec Endpoint Protection

購買或續購授權並於授權到期時進行檢查。

Symantec Endpoint Protection (SEP) 需要付費授權才能接收安全性內容更新、產品更新和版本，以及存取技術支援。安裝 Symantec Endpoint Protection Manager 後，您有 60 天的時間來購買足夠的授權基座，以便涵蓋部署的所有用戶端。

Table 49: 如何授權 Symantec Endpoint Protection

工作	說明
步驟 1：購買授權	若要購買新授權，請聯繫您 偏好的經銷商 。 如需更多詳細資訊，請前往 Symantec 入門指南 並向下滾動到內部部署安全產品。 若有下列情形，表示您必須購買授權： • 您是新客戶。 • 您的試用授權已到期。 • 您購買的授權已到期。 • 部署的用戶端比授權允許的要多 (過度部署)。 請參閱： Symantec Endpoint Protection 授權涵蓋哪些方面？
步驟 2：從 Broadcom 入口網站下載授權檔案	前往 Broadcom 入口網站 ，並下載授權檔案 (.slf) 到 Symantec Endpoint Protection Manager 電腦。 授權將不再透過電子郵件寄給您。
步驟 3：啟用所購買的授權	您需要使用該序號啟用安裝。 • 使用系統管理員帳戶 (如預設帳戶 ###) 登入 Symantec Endpoint Protection Manager。 • 前往「管理員」>「授權」頁面，匯入並 啟動 您的 Symantec Endpoint Protection 產品授權檔案。

Symantec Enterprise Broadcom 部門的重要客戶資訊

您可以執行下列工作來管理授權。

Table 50: 授權工作

工作	說明
擷取序號	如果您擁有 Symantec 的現有授權，並且必須擷取您的序號，請參閱： 下載 Broadcom 授權和產品的「我的授權常見問題」
續購授權	連絡您 偏好的經銷商 。請參閱： 購買或續購 Broadcom 產品的授權和訂閱
了解您的授權何時到期以及您是否過度部署	檢查已匯入主控台的各項授權的狀態，以瞭解是否必須續購授權或購買更多授權。 您可以將現有授權套用到產品升級。請參閱： 我的 Symantec Endpoint Protection 授權何時到期？ 授權到期或過度部署後會發生的情況 (SEP 或 SES)。
管理虛擬機器上的授權	如果是虛擬用戶端，管理伺服器僅計算線上非持續用戶端的授權。如果您擁有的使用者數目超過您擁有的用戶端數目，請使虛擬用戶端成為非持續用戶端。請參閱： 如何管理非持續虛擬桌面基礎架構 (NPVDI) 用戶端的授權計數
備份您的授權檔	備份您的授權檔，以便在資料庫或電腦硬碟損壞的情形下，仍能保有授權檔。請參閱： 備份和復原授權檔案 (.slf)
復原授權檔案	如果您不小心刪除了授權檔，可以進行還原。請參閱： 備份和復原授權檔案 (.slf)

工作	說明
授權到期時發送通知	預設情況下，Symantec Endpoint Protection 向管理員發送預配置的通知，通知有關到期授權和其他授權的問題。請參閱： 如何接收 Symantec Endpoint Protection 授權到期通知？
檢查產品授權需求	瞭解所要保護電腦的授權需求。授權可讓您將 Symantec Endpoint Protection 用戶端安裝在特定數量的電腦上。請參閱： Symantec Endpoint Protection 授權涵蓋哪些方面？ Symantec Endpoint Protection 產品授權術語 關於多年授權

我的 Symantec Endpoint Protection 授權何時到期？

您可以查看管理伺服器是使用試用版授權，還是已付費授權。對於已匯入主控台的所有已付費授權，您也可以取得下列相關授權資訊：

- 授權序號、基座總個數、到期日
- 有效基座個數
- 已部署的基座個數
- 已過期的基座個數
- 已過度部署的用戶端個數

試用版授權狀態僅提供與到期日期相關的有限資訊。

檢查 Symantec Endpoint Protection Manager 授權何時到期

- 若要檢查您是否擁有付費授權或試用授權，請在主控台中執行以下工作之一：
 - 按下「管理員」>「授權」。
 - 按下「首頁」>「授權詳細資料」。
- 若要檢查授權到期日期，請在主控台中按下「管理員」>「授權」。

更多資訊

- [使用情況資料 \(遙測\)](#)
- [授權 Symantec Endpoint Protection](#)
- [啟用或匯入 Symantec Endpoint Protection 產品授權](#)

如何接收 Symantec Endpoint Protection 授權到期通知？

若您看到訊息：Symantec Endpoint Protection Manager (SEPM) 說明 `Symantec ##### 30 #####`，即代表您的付費授權即將到期，必須續購。

依預設，系統管理員會在下列授權事件發生時收到通知：

內部部署	• 已付費授權到期：此通知會警示管理員和合作夥伴 (選用性) 已付費授權將在 30 天後到期或即將到期。您無段。 • 過度部署：此通知會警示管理員和合作夥伴 (選擇性) 有關過度部署的已付費授權。 • 試用授權到期：已過期或將在 60、30 和 7 天後到期的試用授權。 有關其他類型的通知，請參閱：有哪些類型的通知，何時傳送它們？
雲端主控台	• 您的授權即將到期或已過期。 • 裝置會回報無效或缺少的授權。 使用警示規則

架構授權通知

1. 「監視器」頁面 > 「通知」標籤上，按一下「通知條件」，然後點選通知類型。
2. 在「通知條件」窗格中，任選通知並按一下「編輯」：
 - 試用授權到期
 - 已付費授權問題
 - 過度部署問題若要新增合作夥伴的電子郵件地址，請將其新增至「傳送電子郵件給」文字欄位中。
3. 根據需要修改任何欄位，然後按一下「確定」。

刪除授權通知

若您不想顯示到期通知，請將其刪除。若有需要，您之後仍可以新增通知。

1. 在「通知條件」頁面中，選取該通知並按一下「刪除」。

更多資訊

- [SEP 授權到期後會有什麼改變？](#)
- [設定管理員通知](#)

授權到期或過度部署後會發生的情況 (SEP 或 SES)。

本主題涵蓋過期或不合規的 Symantec Endpoint Protection (SEP) 或 Symantec Endpoint Security (SES) 授權的影響。

您可購買下列授權：

- **Symantec Endpoint Protection** 授權，此包括僅對內部部署 Symantec Endpoint Protection 的存取權限，且無權存取 Symantec Endpoint Security (SES) 雲端主控台。
- **Symantec Endpoint Security** 授權，此包括對雲端主控台和內部部署 Symantec Endpoint Protection Manager (SEPM) 的存取。SES 授權提供全面的雲端主控台管理和混合管理，此可任您於雲端中註冊 Symantec Endpoint Protection Manager 網域。您可購買 Symantec Endpoint Security Enterprise (SESE) 授權或 Symantec Endpoint Security Complete (SESC) 授權，後者提供更多功能。
請參閱：[Symantec Endpoint Security 功能](#)

該授權的行為依您使用的是內部部署 SEP 或雲端主控台的授權而定。

授權的作用為何？

Symantec 授權具有下列功能。

- 規定合規性。
- 決定產品類型。產品類型啟用了您可用的某些功能，如 Symantec Endpoint Security Enterprise (SESE) 與 Symantec Endpoint Security Complete (SESC) 的比較。
- 從 Symantec 取得用戶端驗證 Token (CAT)。該 CAT 可讓用戶端搭配利用 Symantec 伺服器對自身進行驗證。例如，用戶端會連接至信譽伺服器以下載鑑識。

如何取得授權？

Symantec Endpoint Protection

內部部署 SEP 授權是個軟體授權產品，並使用授權檔。首次從合作夥伴處購買授權時，您會收到產品授權序號或 Symantec 授權檔案 (.SLF)。可以通過電子郵件或從安全網站下載許可檔。透過電子郵件接收授權檔時，該檔案將以 .ZIP 檔案的形式附加至電子郵件。您從 .ZIP 檔案中解壓縮 .SLF 檔案。將授權檔儲存至可從 Symantec Endpoint Protection Manager 主控台進行存取的電腦。儲存兩者：

- 在裝載 SEPM 之電腦上的授權。
- 為了安全起見，將授權複本儲存至不同的電腦或抽取式儲存媒體上。

NOTE

有時，您可能僅有授權序號。此序號可用來啟動 Symantec 產品授權並下載產品軟體。Symantec Endpoint Protection 授權適用於 Symantec Endpoint Protection 用戶端。例如，在具有 50 個端點的網路中，授權必須至少提供給 50 個基座個數。Symantec Endpoint Protection Manager 的實例不需要授權。

Symantec Endpoint Security

您必須購買 Symantec Endpoint Security Enterprise 或 Symantec Endpoint Security Complete 訂閱來取得雲端的存取權。這些訂閱是混合的，這表示一旦佈建了訂單，便會自動將 SES Enterprise 或 SES Complete 訂閱套用至雲端主控台。您無須啟動訂閱。購買 SES Enterprise 或 SES Complete 後，訂閱將在雲端中自動啟動。然後請登入 <https://securitycloud.symantec.com/> 以部署用戶端軟體。

內部部署 SEP 隨附於 SES Enterprise 或 SES Complete 訂閱中。

如要取得授權碼，請參閱：[下載或續訂 Broadcom、CA，和 Symantec 產品的授權碼](#)

如要續訂或購買更多的 SES 使用者個數，請參閱：[購買或續訂 Symantec Endpoint Security 中的訂閱](#)

已過度部署或過期授權的結果

當授權不合規時，Symantec 產品將進入軟性強制執行模式。軟性強制執行意指：

- 管理主控台會繼續下載內容。
- 使用者介面變更且日誌通知啟動。

在 SEP 中，若限制的管理員並無群組權限和功能權限，則其無法看到報告資料，也不會收到通知。若限制的管理員具有群組權限和報告權限，其會收到即將到期或已過度部署之授權的通知。

硬性強制執行意指內容更新停止。

若您的付費授權為已過度部署或已過期，則會發生下列情況。

管理	授權類型	授權狀態	行為
內部部署 Symantec Endpoint Protection	試用	已過度部署	已允許
		已過期	LiveUpdate 內容已停用。
	已付費	已過度部署	已允許 • 用戶端不再將樣本和資料提交給 Symantec Insight，但用戶端確實可以接收內容更新。 • 用戶端繼續向 Insight 提交信譽資料。 • Symantec Endpoint Protection Manager 將生成通知，提醒管理員不遵從。
		已過期	已允許 • 用戶端不再將樣本和資料提交給 Symantec Insight，但用戶端確實可以接收內容更新。 • Symantec Endpoint Protection Manager 會產生提醒管理員不合規的警示。 SEPM 表示授權的到期時間。SEPM 還會在授權到期日期前約 60 天顯示即將到期的警告。指定於 .SLF 檔案中之到期前的天數。
Symantec Endpoint Security 雲端主控台	試用	已過度部署	不會在超出試用限制 25 的裝置上啟動保護功能。
		已過期	LiveUpdate 內容*和保護功能均遭停用。
	已付費	已過度部署	已允許

		已過期	- 無法存取雲端控制台之前，您有 30 天時間可以續購授權，否則 Symantec 將移除租用戶並清除資料。如果您在 30 天內續購授權，則在原始 30 天結束後，您將獲得另外 30 天時間。 - 雲端管理的 SEP 用戶端會下載內容，直至租用戶授權到期為止。 - 在 30 天內，您將透過電子郵件、登入時的彈出式通知或雲端控制台的橫幅收到通知。

*停用 LiveUpdate 內容時，會在 Windows 10 RS3 + 上自動停用防惡意軟體即時掃描。

- 即使允許該行為，您仍然不合規。
- 匯入 SEPM 之雲端授權的行為方式與內部部署 SEP 授權相同。
- 混合管理模式的 SEP 用戶端會遵循基本功能的內部部署 SEP 授權和僅限雲端功能的雲端 SES 授權。例如，混合管理模式的試用授權僅允許 25 部裝置執行密集型防護、應用程式控制等。當內部部署授權在 SEPM 上過期時，SEPM 將會停止繼續內容下載。對於 SEP 14.3 RU4 客戶端，密集型防護和應用程式控制會繼續在這 25 部裝置上執行。但是，雲端主控台會顯示授權已過期，且不合規。對於 SEP 14.3 RU3 及更早版本的用戶端，不再套用密集型防護和應用程式控制。

計數已過度部署或過期的授權

Symantec 會計數每個受管裝置的授權。裝置是指單一實體或虛擬桌上型電腦、筆記型電腦、精簡型用戶端、工作站、行動裝置、伺服器或其他虛擬作業系統環境，在其上安裝、執行軟體的單一實例或其部分，或執行服務。

NOTE

伺服器需要 SES Complete 或 SES Enterprise 授權。

於 SES 中，授權會一政策而非裝置進行計數。

找出過度部署和過期授權的數量

Symantec Endpoint Protection :

1. 在主控台中，按一下「報告 > 快速報告」。
2. 在「快速報告」標籤上，選取「電腦狀態 > Symantec Endpoint Protection 授權狀態」，然後按一下「建立報告」。

Symantec Endpoint Protection

Symantec Endpoint Protection Licensing Status

Report generated on: 11/18/2021 02:40:01

Print

Save

Close

Description: This report contains licensing status, expiration dates and deployment status.

Deployment Summary

Total Purchased (100)	
Seats Used (2)	
Seats Available (98)	
Expired (0)	
Overdeployed (0)	

[View License Details](#)

License Details

Product	Seats Used	Seats Available	Expired	Over Deployed
Symantec Endpoint Protection	2	98	0	0

Client Details

Client Type	Windows	Mac	Linux
Symantec Endpoint Protection	2	0	0

Symantec Endpoint Security :

請參閱：[檢查 Symantec 產品訂閱的狀態](#)我如何收到有關我的授權過度部署或過期的通知？如需詳細資訊，請參閱：[如何接收 Symantec Endpoint Protection 授權到期通知？](#)

授權行為

內部部署 SEP 和 SES 雲端主控台會使用下列類型的授權來進行合規性。

授權類型	說明	內部部署	雲端主控台
試用授權	- 試用授權可讓您評估該產品。 - 提供 SEP 和 SES 兩者硬性強制執行	- SEP 授權有效期為 60 天。 - 不受限制的裝置。 - 下載該軟體時，授權包含於 SEPM 中，並在您架構 SEPM 時進行啟動。	- SES 授權有效期為 30 天。 - 最多 25 部裝置。 - 對於 14.3 RU4 或更新版本的用戶端，硬性強制執行會暫時中止。
已付費授權	您可從 Broadcom 授權入口網站上當地就近的經銷商取得並管理付費授權。用來授權非受管用戶端。	透過「管理員 > 授權」索引標籤匯入 SEPM 主控台。	Broadcom 授權團隊將授權新增至雲端租用戶。如要檢視授權，請移至「設定 > 訂閱」索引標籤。

授權沒有寬限期。

SEP 和 SES 不使用升級許可或 overdeployed 許可。若從 SEP 轉換至 SES Enterprise 或 SES Complete，請購買新的授權，但保留相同的授權檔。

疑難排解

您可回收不再使用的授權使用者個數。

SEP：

您可啟用 SEPM，移除在過去 24 小時內未登入的用戶端，從而使這些授權的使用者個數可用。若已安裝用戶端的數量大於授權使用者個數計數，則此過程無法解決問題。在該種狀況下，您必須購買更多的使用者個數。

如需有關如何回收未使用的授權資訊，請參閱：

- [從資料庫清除過時的用戶端以使更多授權可用](#)
- [Symantec Endpoint Protection Manager 正顯示用戶端的過度部署](#)

SES：

[從 Symantec Endpoint Security 中清除離線裝置以釋出更多可用的授權](#)

刪除過時授權，以釋放更多授權

Symantec Endpoint Protection Manager 可能會因為過時的用戶端，而錯誤地顯示過度部署的授權狀態。這些是受保護環境中不再與 Symantec Endpoint Protection Manager 進行通訊之用戶端的資料庫項目。用戶端可能會因為許多原因而呈現過時，例如當您升級作業系統、解除委任電腦，或變更硬體架構時。

如果授權報告顯示授權的基座數大於已知的部署基座數，則應該清除過時用戶端的資料庫。過時的用戶端不利於產品授權，因此一旦建立過時用戶端，立即將其清除是很重要的。根據預設，每隔 30 天會進行一次清除。您可以縮短清除週期的間隔，以更快清除過時的用戶端。請在清除週期完成後重設間隔以符合長期需求。

在非持續虛擬桌面基礎架構 (VDI) 中，您可以設定一段單獨的時間用於清除非持續用戶端。此設定會清除您所設定期間內未連線的離線用戶端。非持續離線的用戶端不會影響授權計數。

NOTE

如果您不小心在其他網站或位置安裝授權，請遵循此任務。

從資料庫刪除用戶端

1. 在主控台的「管理員」頁面上，按下「網域」，在網域上按下滑鼠右鍵，然後按下「編輯網域屬性」。
2. 在「一般」標籤上，將「刪除指定的時間內未連線的用戶端」設定從預設值 **30** 變更為 **1**。
您不需要因授權用途而設定清除非持續用戶端的選項。離線的非持續用戶端不會計算在授權總數內。
3. 按一下「確定」。
4. 請在經過 24 小時之後，將設定復原為 30 天，或其他符合所需的間隔。

更多資訊

- [清除過時的非持續 VDI 用戶端以釋放授權](#)
- [授權 Symantec Endpoint Protection](#)

Symantec Endpoint Protection 授權涵蓋哪些方面？

Symantec Endpoint Protection 的授權數會根據下列規則強制執行：

Table 51: 授權強制執行規則

適用範圍	規則
授權期限	授權期限是指從啟用的日期時間開始，到授權期限的最後一天的午夜結束。 如果您有多個站台，則授權的到期日為地處最西邊的 Symantec Endpoint Protection Manager 資料庫的日期和時間。
Symantec Endpoint Protection 元件	Symantec Endpoint Protection 授權適用於 Symantec Endpoint Protection 用戶端。例如，在具有 50 部電腦的網路中，授權必須至少提供給 50 個基座個數。Symantec Endpoint Protection Manager 實例不需要授權。 Symantec Endpoint Protection Manager 不要求用戶端具有存取管理伺服器的授權。連線到管理伺服器的未授權用戶端都會獲得一個授權。您必須確保已購買足夠的授權基座，以便涵蓋每部用戶端電腦。
站台和網域	Symantec Endpoint Protection 產品授權適用於整個安裝。無論安裝所包含的複製站台或網域數目為多少。例如，具有 100 個基座個數的授權涵蓋兩個站台的安裝，其中每個站台各有 50 個基座個數。 如果您並未實作複製，您可以部署相同的 .slf 檔案至多部 Symantec Endpoint Protection 管理伺服器。向管理伺服器報告的用戶端數量不得超過授權基座總數。
平台	授權基座會套用於任何平台上執行的用戶端，不論平台為 Windows、Mac 還是 Linux。
產品和版本	授權基座一視同仁適用於多個產品版本。

如需授權存取第三方伺服器軟體 (例如 Microsoft SQL Server) 的用戶端的相關資訊，請連絡軟體廠商。

更多資訊

- [授權 Symantec Endpoint Protection](#)
- [清除過時的非持續 VDI 用戶端以釋放授權](#)

備份和復原授權檔案 (.slf)

您應該備份授權檔案，以備資料庫或主控台電腦的硬碟損壞時使用。

將授權檔儲存到可從 Symantec Endpoint Protection Manager 主控台進行存取的電腦。許多使用者將授權儲存在裝載 Symantec Endpoint Protection Manager 的電腦上。為了安全起見，許多使用者也將授權複本儲存到不同的電腦或抽取式儲存媒體上。

若要備份您的授權檔

1. 從您儲存檔案的目錄中將 **.slf** 授權檔複製到您選取的另一台電腦。

若要復原您的授權檔

- 執行下列其中一項工作：
 - a. 在 Symantec Endpoint Protection Manager 主控台的「管理」頁面中，按下「授權」，然後在「工作」下方按下「還原刪除的授權」。在「授權還原」面板中，勾選要還原之已刪除授權旁的方塊，然後按下「提交」。
 - b. 從以下預設位置擷取授權檔案：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\inetpub\license。使用授權啟動精靈匯入授權檔案時，Symantec Endpoint Protection Manager 會在此資料夾放入授權檔案的複本。
 - c. 前往 [Symantec Endpoint Security](#) 網站，然後按一下「我的授權」。如需詳細資訊，請參閱：
[賽門鐵克至 Broadcom 轉換指南 - 我的授權](#)

更多資訊

[授權 Symantec Endpoint Protection](#)

關於多年授權

購買多年授權時，會根據授權有效的年數，收到等數的一組授權檔案。例如，三年授權會包含三個獨立授權檔。啟用多年授權時，會在同一個啟用階段作業中匯入所有的授權檔。Symantec Endpoint Protection Manager 會將獨立授權檔合併成一個啟用的授權，這個授權會在購買期限內有效。

未提供建議時，您可以啟用低於全數的授權檔。此時，Symantec Endpoint Protection Manager 會合併檔案，並套用最後到期之授權檔的持續期間。例如，僅啟用前兩個授權檔的三年授權，表示持續時間僅兩年。之後再啟用第三個檔案時，Symantec Endpoint Protection Manager 會精準報告授權的完整持續期間為三年。任何情況下，基座個數都會與所購買的基座個數一致。

當 Symantec Endpoint Protection Manager 合併檔案時，會刪除持續期間最短的檔案，並保留持續期間最長的檔案來進行內部授權保留功能。如果您認為某個授權遭到 Symantec Endpoint Protection Manager 不當刪除，請還原並重新啟用刪除的授權。

您可以查看與使用中授權相關聯且持續期間較短的授權序號。在「管理員」頁面上，按一下「授權」，然後按一下啟用的授權。相關聯的授權會出現在「相關授權」欄中。

更多資訊

[授權 Symantec Endpoint Protection](#)

Symantec Endpoint Protection 產品授權術語

您必須購買可涵蓋每個已部署用戶端的授權。一份授權可涵蓋所有用戶端，不論平台和版本為何。

下列術語適用於賽門鐵克產品授權：

Table 52: 產品授權術語

術語	說明
序號	授權中有一個序號，可以獨特的方式辨識您的授權，並使授權與您的公司相關聯。此序號可用來啟用 Symantec Endpoint Protection 授權。
已部署	「已部署」表示受 Symantec Endpoint Protection 用戶端軟體保護的端點電腦。例如，「我們具有 50 個已部署基座」表示有 50 個端點安裝了用戶端軟體。
啟用	您可以啟用 Symantec Endpoint Protection 產品授權，以便對所有程式功能進行不受限制的存取。您可以使用「授權啟用精靈」完成啟用過程。請參閱： 啟用或匯入 Symantec Endpoint Protection 產品授權
基座	一個基座是由 Symantec Endpoint Protection 用戶端軟體保護的一台端點電腦。授權須購買，僅對特定個數的基座有效。「有效基座個數」表示在所有的有效授權中指定的基座總數。

術語	說明
試用授權	試用授權表示具有完整功能的 Symantec Endpoint Protection，可在免費試用期內運作。如果要在試用期後繼續使用 Symantec Endpoint Protection，必須為您的安裝軟體購買並啟用授權。您不需要解除安裝軟體，即可將試用版軟體轉換為授權安裝。 您必須從銷售帳戶代表取得試用授權。 試用期是指自初始安裝 Symantec Endpoint Protection Manager 起 60 天內的時間。
已過度部署	授權已過度部署是指已部署用戶端的數量超過授權基座個數的數量。

瞭解授權需求，是規劃 Symantec Endpoint Protection 安裝以及安裝後管理產品授權的一部分。

更多資訊

[授權 Symantec Endpoint Protection](#)

授權非受管 Windows 用戶端

非受管用戶端不需要手動安裝授權檔，並且不會將其算入付費授權的總基座數。但是，若要從非受管 Windows 用戶端傳送信譽資料，您必須在該非受管用戶端上安裝已付費授權。非受管 Mac 用戶端和 Linux 用戶端不會提交信譽資料。

授權非受管 Windows 用戶端

1. 找到您目前的賽門鐵克授權檔 (.slf) 並建立該檔案的複本。

請使用您在 Symantec Endpoint Protection Manager 上用於啟用授權的相同檔案。

2. 在用戶端電腦，將複製的授權檔置於 Symantec Endpoint Protection 用戶端收件匣 (預設位置) 中：

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\

根據預設，收件匣所在的資料夾會處於隱藏狀態，因此請使用「資料夾選項」顯示隱藏的檔案和資料夾。

如果授權檔無效或授權安裝失敗，授權會出現在稱為 Invalid 的新資料夾中。如果授權檔有效，則系統會在處理該檔案後自動將其從收件匣移除。

3. 若要確認是否正確套用授權，請檢查收件匣資料夾中不存在任何檔案。

4. 確認 .slf 檔案位於下列資料夾 (預設位置) 中：

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config

您也可以將 .slf 檔案納入第三方部署套件中。

使用政策管理安全性

使用政策管理用戶端電腦上的安全性。

可以使用不同類型的安全性政策來管理網路安全性。預設政策會在安裝期間自動建立。可以使用預設政策,也可以自訂政策以符合特定環境的需要。

阻止惡意軟體和其他威脅的最佳實務

威脅態勢已改變,且網路犯罪猖獗。公司無法僅只是依靠桌面防毒技術來保護自己。

必須進行

請遵循以下步驟改善桌面防護,並使用 Symantec Endpoint Protection (SEP) 阻止惡意體。

- 使用 **IPS (入侵預防系統)**: 現今的威脅是網頁式威脅。Symantec Endpoint Protection 中的 IPS 可在威脅滲透機器之前阻止威脅。IPS 可阻止漏洞侵入、下載驅動攻擊和假冒的防毒安裝。
- 改善預設的 **Symantec Endpoint Protection** 設定: 透過改善其預設設定,充分利用 Symantec Endpoint Protection 產品。僅需變更一些設定即可大大提升您的安全性。
- 保持瀏覽器外掛程式的修正: 攻擊已移至瀏覽器。攻擊者不使用 Microsoft Internet Explorer 或 Adobe Reader/Acrobat/Flash 漏洞進入系統至關重要。當修正程式可用時,請使用每個供應商的自動更新或軟體分佈工具安裝修正程式。
- 攔截 **P2P** 用法: 散佈惡意軟體的最簡單方法是將之隱藏於點對點 (P2P) 網絡上共用的檔案中。建立並執行非 P2P 政策,包括在家中使用公司機器。在閘道和/或桌上型電腦強制執行政策。 [詳細瞭解如何使用 Symantec Endpoint Protection 在桌上型電腦上攔截 P2P](#)
- 關閉 **AutoRun**: 防止 Conficker/Downadup 和其他網路型病蟲從 USB 金鑰和網路磁碟機跳出,無須變更「開啟共用」上的公司政策。

應該進行

- 在 **Adobe Reader** 中開啟增強型安全性: 透過強化 Adobe Reader 來保護您的機器免受隱藏於 PDF 檔案中的攻擊。 [詳細瞭解如何使用 Reader 中可用的增強型安全性設定](#)。
- 限制使用網路共用 (對應磁碟機): 病蟲喜歡透過網路磁碟機進行散佈。除非有強烈的業務需求,否則關閉對應磁碟機。如有可能,請將權限限制為唯讀而非讀寫。
- 檢閱郵件安全和閘道攔截有效性: 使用有效的郵件和 Web 安全掃描,在威脅進入桌上型電腦之前將其攔截。檢查您是否備有經常更新的郵件安全解決方案,以檢測郵件閘道中最新的錯誤寄件者 IP、垃圾郵件和惡意軟體威脅。考慮實作 Web 安全解決方案,可保護您的組織免受 Web 2.0 威脅,包括惡意 URL 和惡意軟體。
- 檢閱您的安全內容派送排程: 防毒特徵每天發佈多次,而 IPS 內容每週大致發佈一次或依需要發佈。如有可能,請利用這些更新或至少更新經常遭感染的機器。
- 檢閱您的安全內容派送排程: 管理員有時僅使用傳統的特徵型病毒和間諜程式元件來部署 SEP。其他選用元件 (網路威脅防護、入侵預防系統、應用程式和裝置控制、主動型威脅防護) 大大增強了 SEP 抵禦現今複雜威脅的能力。「鑑識」技術對於尚無病毒特徵的最新威脅特別有效。除非有令人信服的理由,否則應將這些其他元件的每一個部署至整個組織中。請參閱: [新增或移除現有 Endpoint Protection 用戶端的功能](#)

可以執行

- 實作應用程式控制規則以攔截特定威脅: 「應用程式與裝置控制」是個強大的工具,可用來停止特定檔案、攔截點對點 (P2P) 網路使用或保護關鍵檔案與登錄項目。
- 教育使用者: 大多數的惡意軟體攻擊會使用社交工程。教育可以非常有效地使其停止。您的使用者不需要是安全專家。今天,只要記住四件事便可使其受到保護。

-
- 進行搜尋時僅按一下受信任來源，尤其是關注度高的主題。
 - 切勿從託管視訊或與該應用程式無關的網站更新媒體播放器、轉碼器或 Flash 軟體。
 - 請勿在商用機器上使用 P2P 應用程式，而在家用機器上要謹慎。
 - 請勿點按垃圾郵件中的連結或附件。
 - 教育您自己: Symantec 提供[多種資源](#)，讓您瞭解最新的安全威脅。
 - [P2P 攔截](#)
 - [SEO 中毒](#)

使用 Symantec Endpoint Protection 的勒索軟體緩和與防護

何謂勒索軟體？

勒索軟體是一種惡意程式類別，可加密文件，使其無法使用，但保留電腦的其餘部分可供存取。勒索軟體攻擊者會嘗試迫使受害者透過明確註明的付款方式支付贖金，之後可能會讓受害者存取其資料。

目標勒索軟體比原始勒索軟體攻擊更為複雜，並且不只涉及初始感染。攻擊者已使用下列範圍的派送方法來發現多種勒索受害者組織的方式：

- 網路釣魚：傳送給員工的電子郵件已偽裝為工作相關信件。
- 惡意廣告：影響媒體網站以提供惡意廣告，內含稱為 SocGholish 且偽裝為軟體更新的 JavaScript 型架構。
- 漏洞剌探利用：攻擊在公開伺服器上執行的易受攻擊軟體。
- 輔助感染：利用預先存在的殭屍網路，以作為受害者網路的穩固基礎。
- 不安全的服務：透過不安全的 RDP 服務攻擊組織，利用的方式是洩露或弱認證。

使用 Symantec Endpoint Protection 防禦勒索軟體

預設會啟用 Symantec Endpoint Protection 中可防禦勒索軟體的大部分功能。如需可保護環境之功能的詳細資訊，請參閱：

[使用 Symantec Endpoint Protection 的勒索軟體防護](#)

[使用 Symantec Endpoint Security 防禦勒索軟體](#)

[烏克蘭：磁碟擦除攻擊先於俄羅斯入侵](#)

緩和勒索軟體的最佳實務準則

[強化環境以抵禦勒索軟體](#)

除了啟用 SEP 防護之外，若要避免勒索軟體感染，請遵循其他步驟。

Table 53: 避免勒索軟體的步驟

步驟	動作
1. 保護本機環境	1. 確保您擁有最新版本的 PowerShell，並且已啟用記錄功能。 2. 限制對 RDP 服務的存取。僅允許來自特定已知 IP 位址的 RDP，並確保您正在使用多重驗證。使用「檔案伺服器資源管理員 (FSRM)」，鎖定在需要使用者寫入存取權的檔案共用上寫入已知勒索程式延伸的功能。 3. 建立計畫以考量外部方的通知。若要確保正確地通知到必要組織 (例如 FBI 或其他法律執行機構/機關)，請務必制定驗證計畫。 4. 建立「跳袋」，其中具有所有重大管理資訊的硬複本和已封存的軟複本。若要防範危害此重大資訊可用性，請將它儲存至跳袋，其中具有問題疑難排解所需的硬體和軟體。加密網路檔案時，將此資訊儲存至網路並沒有幫助。實作正確的管理帳戶使用情況稽核和控制。您也可以實作管理工作的一次性認證，協助防止竊取和使用管理認證。 5. 建立管理工具使用情況的設定檔。攻擊者使用其中多種工具，在透過網路水平移動時不被偵測到。如果使用者帳戶具有以 admin 身分在少量系統上使用 PsInfo/PsExec 執行的記錄，則可能很好，但在所有系統上執行 PsInfo/PsExec 的服務帳戶都是可疑的。
2. 保護電子郵件系統	1. 啟用雙重驗證 (2FA)，防止在網路釣魚攻擊期間危害認證。 2. 強化電子郵件系統周圍的安全架構，最大限度地減少到達一般使用者收件匣的垃圾郵件數量，並確保您遵循電子郵件系統的最佳實務準則，包括對網路釣魚攻擊使用 SPF 和其他防禦方法。
3. 進行備份	定期備份用戶端和伺服器上的檔案。您可以在電腦離線時備份檔案，或是使用網路電腦和伺服器無法寫入的系統。如果您沒有專用的備份軟體，也可以將重要檔案複製到抽取式媒體。然後退出並拔掉抽取式媒體；不要讓抽取式媒體持續插著。 1. 對備份複本實作異地儲存。安排至少有四週異地儲存每週完整和每日增量備份。 2. 實作現場離線備份。確保您的備份未連線至網路，以防止勒索軟體將它們進行加密。最好在系統關閉網路時進行移除，以防止任何潛在的威脅散佈。 3. 確認並測試伺服器層級備份解決方案。這應該已是災難復原程序的一部分。 4. 保護備份和備份資料庫的檔案層級權限。請不要加密備份。 5. 測試還原功能。確保還原功能支援業務需求。 用密碼和存取控制限制保護對應網路磁碟機，來鎖定這些磁碟機。對網路磁碟機上的檔案，使用唯讀存取權，除非絕對需要擁有這些檔案的寫入存取權。限制使用者權限可限制威脅可以加密哪些檔案。

如果您取得勒索軟體，應該什麼做？

目前沒有勒索軟體移除工具。沒有任何安全性產品可以解密勒索軟體所加密的檔案。萬一您的用戶端電腦感染到勒索軟體，且您的資料遭到加密，請遵循以下步驟：

1. 不要支付贖金。
如果您支付贖金：
 - 這不能保證攻擊者會提供解除鎖定電腦或解密檔案的方法。
 - 攻擊者會使用贖金來資助對其他使用者的其他攻擊。
2. 在勒索軟體可以攻擊受感染電腦可以存取的網路磁碟機之前，先將受感染的電腦隔離。
3. 使用 **Symantec Endpoint Protection Manager** 或 **SES** 更新病毒定義，並掃描用戶端電腦。
新定義可能會偵測並矯正勒索軟體。只要管理用戶端並將其連線至管理伺服器或雲端主控台，Symantec Endpoint Protection Manager 就會自動將病毒定義下載至用戶端。
 - 在 Symantec Endpoint Protection Manager 中，按下「用戶端」，在群組上按下滑鼠右鍵，然後按下「對群組執行指令」>「更新內容和掃描」。
 - 在 Symantec Endpoint Security 中，執行「立即掃描」指令。請參閱：
[在用戶端裝置上執行指令](#)
4. 使用全新安裝重新安裝。
如果從備份還原加密檔案，則可以取得所還原的資料，但可能會在攻擊過程安裝其他惡意程式。
5. 將惡意軟體提交至賽門鐵克安全機制應變中心。

如果您可以識別惡意的電子郵件或可執行檔，請將其提交至賽門鐵克安全機制應變中心。這些樣本可以讓賽門鐵克建立新特徵，以及改進防禦勒索軟體的功能。請參閱：

[賽門鐵克行家秘訣：成功提交！](#)

使用 Symantec Endpoint Protection 的勒索軟體防護

目標性勒索軟體攻擊可以細分為以下幾個主要階段：

- 初始危害
- 權限升級和認證竊取
- 水平擴散
- 備份加密和刪除

最佳防禦是攔截多種類型的攻擊，並知道大多數網路犯罪團隊用來識別安全優先順序的攻擊鏈結。不過，無法使用移除工具將勒索軟體解密。

在 Symantec Endpoint Protection Manager 上，部署並啟用下列功能。預設會啟用部分功能。

Table 54: Symantec Endpoint Protection Manager 功能

步驟	動作
步驟 1：啟用檔案型防護 賽門鐵克會隔離下列類型的檔案： Ransom.Maze、Ransom.Sodinokibi 和 Backdoor.Cobalt	啟用「病毒和間諜軟體防護」政策 (預設予以啟用)。請參閱： 阻止和處理病毒和間諜軟體對用戶端電腦的攻擊
步驟 2：啟用行為分析 (SONAR) Symantec Endpoint Protection 的行為式防護功能是另一個防禦惡意軟體的重要功能。SONAR 可防止 CryptoLocker 之類的勒索軟體變體的雙重可執行檔名稱執行。	在「病毒和間諜軟體防護」政策中，按下 SONAR > 「啟用 SONAR 」。此選項預設為啟用。請參閱： 管理行為分析 (SONAR)
步驟 3：修改下載 Insight Symantec Insight 可防止勒索軟體變體，方法是隔離賽門鐵克客戶群已知為惡意的檔案，或是尚未證明為安全或惡意的檔案。	「下載鑑識」是預設「病毒和間諜軟體 - 高度安全」政策的一部分。 1. 在主控台中，開啟目標「病毒和間諜軟體防護」政策，然後按一下「下載防護」。 如果新增政策，則請選取「病毒和間諜軟體防護政策 - 高度安全」政策。 2. 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」。 3. 檢查以下預設選項： — 使用者數量不超過: 5 個的檔案 — 使用者已知不超過: 2 天的檔案 低的預設值會迫使用戶端將尚未由超過五個使用者向賽門鐵克報告的任何檔案，或是將不足 2 天的任何檔案視為未證明的檔案。如果未證明的檔案符合這些準則，「下載鑑識」會將這些檔案偵測為惡意檔案。 4. 請確定勾選「自動信任從信任的 Internet 或內部網路網站下載的任何檔案」。 5. 在「動作」標籤的「惡意檔案」下方，使第一個動作保持為「隔離風險」，第二個動作則保持為「略過」。 6. 在「未證明的檔案」下方，按下「隔離風險」。 7. 按下「確定」。

步驟	動作
步驟 4：啟用入侵預防系統 (IPS) - IPS 會攔截光靠傳統病毒定義檔無法阻止的某些威脅。IPS 是最佳防禦工具，可以防止從 Internet 不知不覺地下載軟體時所發生的偷渡式下載。攻擊者通常使用侵入套件，透過偷渡式下載進行 CryptoLocker 之類的網頁式攻擊。 - 在某些情況下，IPS 可以中斷 command-and-control (C&C) 通訊來攔截檔案加密。C&C 伺服器是攻擊者或網路罪犯所控制的電腦，用來將指令傳送給惡意程式所破壞的系統，並從目標網路接收所竊取的資料。 「URL 信譽」根據網頁的信譽分數來防止 Web 威脅。「啟用 URL 信譽」選項會攔截信譽分數低於特定臨界值的網頁。(14.3 RU1 and later).	如需詳細資訊，請參閱： 啟用網路入侵預防或瀏覽器入侵預防 預設會啟用 URL 信譽。
步驟 5：攔截 PDF 檔案和程序檔	在「例外」政策中，按下「Windows 例外」>「檔案存取」。
步驟 6：下載修補程式 下載適用於 Web 應用程式架構的最新修正程式，以及網頁瀏覽器外掛程式。	請執行下列動作： - 使用「應用程式與裝置控制」，防止在「使用者設定檔」目錄 (如 Local 和 LocalLow) 中執行應用程式。勒索軟體應用程式會將自己安裝至 Local\Temp\Low 以外的多個目錄。請參閱： 加強防毒安全性以防止勒索軟體衍生 (Trojan.Cryptolocker 家族等) 感染 - 使用「端點偵測回應 (EDR)」識別具有勒索軟體行為的檔案： - 停用透過電子郵件傳輸之 MS Office 檔案的巨集程序檔。 - 以滑鼠右鍵按一下偵測到的端點，然後選取「隔離」。若要從主控台隔離和重新加入端點，您在 Symantec Endpoint Protection Manager 中必須具有指派給「主機完整性」政策的「隔離所防火牆」政策。請參閱： 關於主機完整性和隔離所防火牆政策
步驟 7：啟用 Web 和雲端存取防護 和 Symantec Cloud Secure Web Gateway (Cloud SWG) 使用 Web 和雲端存取防護 和安全連線設定，以便不論在公司網路、家中還是外出，端點都可以與 Cloud SWG 整合。Web 和雲端存取防護會自動將用戶端上的網際網路流量重新導向至 Cloud SWG，其中根據 Cloud SWG 政策允許或攔截流量。	如需詳細資訊，請參閱： 使用 Web 和雲端存取防護控制網路存取
步驟 8：啟用記憶體攻擊緩和 防範未修正軟體 (例如 JBoss 或 Apache Web 伺服器) 中攻擊者可利用的已知漏洞。	如需詳細資訊，請參閱： 使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊
步驟 9：啟用 AMSI 和無檔案掃描 第三方應用程式開發人員可以保護其客戶免受動態程序檔式的惡意軟體和非傳統網路攻擊途徑的影響。第三方應用程式呼叫 Windows AMSI 介面請求掃描使用者提供的程序檔，該程序檔路由到 Symantec Endpoint Protection 用戶端。用戶端以一個判斷來回應，以指示程序檔行為是否為惡意。如果行為不是惡意的，則程序檔執行將繼續。如果程序檔的行為是惡意的，則應用程式不會運行它。在用戶端上，「偵測結果」對話方塊顯示狀態為「拒絕存取」。第三方程序檔的範例包括 Windows PowerShell、JavaScript 和 VBScript。必須啟用「自動防護」。此功能適用於 Windows 10 和更新版本的電腦。 14.3 和更新版本。	預設為啟用。請參閱： 反惡意軟體掃描介面 (AMSI) 如何幫助您抵禦惡意軟體 防惡意軟體掃描介面 (AMSI)

步驟	動作
步驟 10：啟用端點偵測和回應 (EDR) EDR 專注於行為而不是檔案，而且可以加強魚叉式網路釣魚的防禦和 living-off-the-land 工具的使用。例如，如果 Word 通常不會在客戶環境中啟動 PowerShell，則這應該進入「攔截」模式。EDR 的 UI 可讓客戶輕鬆地瞭解常見且應該允許的行為、可見但仍應該發出警示的行為，以及不常見且應該攔截的行為。您也可以被動地處理缺口，作為調查和回應資安事端警示的一部分。資安事端警示將會顯示所有已觀測為缺口的行為，並提供功能讓這立即從資安事端詳細資料頁面進入攔截模式。	如需詳細資訊，請參閱： 將用戶端群組架構為使用私用伺服器進行信譽查詢和提交
步驟 11：啟用稽核 使用稽核工具，在有機會散佈勒索軟體之前，協助您瞭解公司網路內外部的端點。	使用要針對誤報進行測試的記憶體攻擊緩和。請參閱： 使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊
步驟 12：設定非受管偵測程式 需要有非受管偵測程式，才能考量可能沒有保護的端點。	如需詳細資訊，請參閱： 將用戶端架構為偵測非受管裝置

更多資訊

[使用 Symantec Endpoint Protection 移除與防範勒索軟體](#)

living-off-the land 技術勒索軟體防護的最新功能 (SES 和 SEP)

Symantec Endpoint Protection (SEP) 和 Symantec Endpoint Security (SES) 包含一些增強功能，可保護用戶端電腦免受 living-off-the-land (LotL) 工具及惡意軟體市場的檔案、網路工具和其他一般攻擊工具的危害。

Living-off-the-land 策略—攻擊者利用目標系統上已存在的原生工具和服務，這些方法已被目標攻擊組和常見的網路犯罪集團所使用。

以下技術將防止目標性勒索軟體威脅。

14.3 RU9

- 已更新對以下勒索軟體威脅的保護：
Akira、Albatat、Babuk、BiBi wiper、Black Basta、Blackcat、BlackHunt、BlackSuit、DoNex、Freeworld、Hunter International、Inc、Knight、Kuiper、Lockbit、Medusa、Mimic、Qilin、Phobos、Phoenix、Stop、Trigona、Tuga 勒索軟體系列以及勒索軟體攻擊中使用的各種工具。
- 改進了各種預勒索軟體和外滲工具 (包括 impacket、MegaSync、FileZilla 和 WinSCP) 的端點網路防護。

14.3 RU8

- 已更新針對以下勒索軟體威脅的保護：
Akira、Bianlin、Blackbyte、Blackcat、BlackBasta、Crosslock、Hardbit、Hsharada、IceFire、Lockbit、Magniber、Moneybird 以及勒索軟體攻擊中使用的各種工具。
- 已更新針對以下惡意軟體的保護：
Qakbot、AgentTesla、Gopuram、Icedid、Malicious Chrome WebExtensions、VipersoftX、Xworm。
- 已改善攻擊群組矯正 (AGR) 功能以支援更多程序終止。AGR 會識別偵測到的攻擊中所有元件，並確保移除攻擊中的每個程序和執行緒。
- 已增強針對 MSI 惡意軟體的掃描流程。
- 已增強對 IcedID 所使用 VBA 下載器的模擬支援。
- 已發佈針對 PDF 惡意軟體的新偵測框架。
- 已改善 OneNote 剖析器以擷取其他檔案類型。

14.3 RU7

- Hardbit、IceFire、Lockbit、Magniber、Moneymessage、Noberus、Nokoyawa、Royal 和各種前勒索軟體工具。

14.3 RU6

網路保護技術

- 對勒索軟體系列 (如 Conti、Avoslocker 和 Hive) 的改良網路保護。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的前勒索軟體工具。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的初始存取和水平擴散技術。

檔案檢測技術

- 對 LNK 威脅的改良模擬和分析。
- 對 HTML 威脅 (如 Qakbot 和 Gamaredon) 的改良模擬和分析。
- 改良的模擬和分析，避免在前勒索軟體活動中使用的 BAT 指令碼。
- 對前勒索軟體活動的改良 PowerShell 模擬。
- 對 VBA 擷取和 VBE/JSE 解碼的改良引擎功能。
- 已啟用非 PE 雲端查詢，進而提升非 PE 威脅的效力。

行為防護

- 對重新命名 LotLBins 的改良分析。
- 改良的 BASH 記憶體掃描效能和效力 (勒索軟體、Cobalt Strike)。
- 對 Bumblebee 等威脅的改良執行緒插入防護。
- 對巨大檔案威脅的改良 BPE 涵蓋範圍。
- AEP 和 JESE 掃描流程增強功能，以處理利用 svg 屬性來放置酬載的 Qakbot。
- 改良的一般勒索軟體 BPE 偵測，以減少大迴圈、多執行緒和免責問題。

14.3 RU5

網路保護技術

- 對勒索軟體系列 (如 Conti、Avoslocker 和 Hive) 的改良網路保護。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的前勒索軟體工具。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的初始存取和水平擴散技術。

行為防護

- 改良的一般勒索軟體 BPE 偵測，以減少大迴圈、多執行緒和免責問題。

14.3 RU4

網路保護技術

- 對勒索軟體系列 (如 Conti、Avoslocker 和 Hive) 的改良網路保護。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的前勒索軟體工具。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的初始存取和水平擴散技術。

檔案檢測技術

- 使用分析的強大保護，克服惡意軟體參與者濫用紅隊工具。
- 多建立了兩個指令行 subscanners (wbadmin.exe 和 wevtutil.exe) 以改進前勒索軟體活動偵測。
- 針對 Macro 檔案電腦病毒改良的修復功能。
- 針對 PowerPoint 威脅改良的 Macro 擷取支援。

行為防護

-
- 針對基於 Python 勒索軟體改良的靜態和行為偵測。
 - 為勒索軟體系列 (如 Conti) 啟用 DLL 格式的 BASH 記憶體掃描。Conti 勒索軟體將加密的 DLL 載入記憶體並執行。
 - 建立四個新的指令行 subscanners 和多個新偵測，改進駭客工具和 LOLBins 的前勒索軟體活動檢測。LOLBins 是一種複雜的威脅，需要進階工具才能偵測到。
 - 針對 Emotet 垃圾郵件活動改良的分數分析和 AMSI 偵測。
 - 增強的記憶體掃描使用 SONAR 行為政策強制執行 (BPE) 來處理 Cobalt Strike 使用的程序注入技術。

14.3 RU3

網路保護技術

- 檢測在目標勒索軟體攻擊中使用的可疑程序鏈。
- 遙測增強功能，可在勒索軟體或前勒索軟體工具影響新的用戶端電腦時發出警告。
- 防止 Cobalt Strike 的侵入後動作和水平擴散。
- 防止高普及率惡意軟體，如 IcedID。

檔案檢測技術

- 透過防惡意軟體掃描介面 (AMSI) 對 Office Open XML (OOXML)、Windows Management Instrumentation (WMI)、dotnet 和 XLM 進行加密的保護。
- Microsoft PowerShell 模擬啟發式改進，使用 AMSI 停用技術來檢測惡意軟體。
- 強化指令行啟發式技術，可防禦勒索軟體和 Cobalt Strike 駭客攻擊工具。
- 新增 PE 模擬器後繼掃描支援，利用垃圾迴圈和反模擬來改進惡意軟體的檢測。
- Visual Basic (VB) 和 dotnet 模擬器增強功能，可防止惡意軟體，如 Mass Logger、FormBook 和 Agent Tesla。
- 實施 Microsoft Office Scanner，檢測 VBA stompng 和非 PE 放置器，如 Hancitor。
- 包括常見解析器，用於支援 Microsoft Publisher 和 Microsoft Access 檔的 VBA 提取和模擬。
- 增強 AMSI 和指令碼模擬字符串掃描，識別和矯正 LotL 惡意軟體，如 IsErlk。

行為防護

- 最小化對 Isass.exe 的讀取存取權限，增強憑證盜竊保護。
- 在可信任程序上觸發勒索軟體檢測時，鎖定檔案寫入存取，藉此增強勒索軟體保護。
- 增強對父程序詐騙技術的程序跟蹤。
- 將主執行緒的進入點位址與從磁片檔解析的進入點位址進行比較，對程序空白技術進行檢測。
- 檢測已停用的程序建立。
- 複雜勒索軟體的行為檢測，如 Ryuk、REvil/Sodinokibi、Conti、Darkside、Burglar 和 Lorenz。
- 一般勒索軟體預加密行為檢測，和使用檔案重新命名事件新屬性的後加密檢測。
- 對 Cobalt Strike 侵入後動作和水平擴散的行為檢測，以及針對 Cobalt Strike 信號的記憶體檢測。
- 在程序控制代碼開啟時使用 SetThreadContext 函數和權限標誌，對 DLL 重新整理和程序注入技術進行的行為檢測。
- 對 Microsoft Office Excel 和 Microsoft Office PowerPoint 威脅的行為檢測。
- Symantec Endpoint Detection and Response (SEDR) 可視性，可將一些 BPE 檢測結果為進階攻擊技術 (AAT)。
- LoLBins 上的新 ACM 事件。

如何使用 Symantec Endpoint Protection 封鎖網站？

SEP 提供多元功能來封鎖惡意、包含過多廣告或不適合工作場所的網站。

以下功能大多能封鎖整個網站，而不只是特定 URL。URL 是用於存取網路上特定資源的位址。

• Web 和雲端存取防護

Web 和雲端存取防護是一個重新導向元件，可以將網路流量 (包括網站) 傳送到 Symantec Cloud SWG。在 Cloud SWG 上，您可以設定管理和控制流量的政策。這些流量政策會封鎖不適合工作場合或包含已知惡意內容的網站類別。您也可以將唯一的 URL 新增到 Cloud SWG 允許清單和封鎖清單，進一步覆寫 Symantec 指派的類別。

您必須設定 Web 和雲端存取防護政策以及 Cloud SWG 政策。

更多資訊

如需深入瞭解如何定義政策，請參閱「[Cloud SWG 政策](#)」

如需瞭解如何更新 Cloud SWG 允許和封鎖清單，請參閱「[定義要在自訂 Cloud SWG 政策中使用的物件清單](#)」

[建立自訂 Cloud SWG 內容篩選規則](#)

如需深入瞭解 Web 和雲端存取防護政策，請參閱：

SEP：使用 [Web 和雲端存取防護控制網路存取](#)

SES：[Web 和雲端存取防護入門](#)以及 [Web 和雲端存取防護常見問題](#)

- 瀏覽器入侵預防

Google Chrome 和 Microsoft Edge 的 IPS 瀏覽器副檔名會在執行時攔截瀏覽器中執行的 VBScript、JavaScript 和 ActiveX 呼叫，檢查這些呼叫的參數，偵測是否有漏洞。然後，瀏覽器 IPS 引擎會偵測本來對其他偵測方法 (包括 CIDS 引擎) 隱藏或混淆的侵入代碼。客戶端會進一步將使用者重新導向至封鎖存取該 URL 的預設登陸頁面。

根據預設，瀏覽器入侵預防為啟用狀態。

[整合瀏覽器延伸和 Symantec Endpoint Protection \(SEP\)，防止惡意網站](#)

- URL 信譽

URL 信譽可識別來自網域和 URL 的威脅，這些網域和 URL 可以託管惡意程式、詐騙、網路釣魚和垃圾郵件等惡意內容。URL 信譽會禁止存取識別為惡意內容之已知來源的網址。

預設會啟用 URL 信譽。

SEP：[管理入侵預防](#)

SES：[在 Symantec Endpoint Security 中管理入侵預防](#)

- IPS 特徵

IPS 特徵會檢視進出網站的流量，而非檢視網站本身。

根據預設，系統會安裝 IPS 特徵。

SEP：[Symantec IPS 特徵說明](#)

- 防火牆規則

您可以新增防火牆規則，以封鎖進出特定 DNS 名稱 (如 <https://www.maliciouscompany.com>) 而非特定 URL 的流量。此方式不會封鎖透過 HTTP/HTTPS 代理存取的網站。

如需瞭解如何透過防火牆封鎖網站，請參閱「[如何使用 Symantec Endpoint Protection \(SEP\) 用戶端網路威脅防護 \(NTP\) 元件封鎖特定網站](#)」

執行適用於所有政策的工作

安全性政策定義防護技術如何保護電腦免受已知和不明威脅的侵擾。

您可以採用多種方法管理您的 Symantec Endpoint Protection 安全性政策。例如，您可以自行建立安全性政策，然後依據特定需求加以自訂。您可以鎖定和解除鎖定某些設定，以便使用者無法在用戶端電腦上變更這些設定。

Table 55: 適用所有政策的工作

工作	說明
新增政策	若不欲使用預設政策，可新增政策。 您可以新增共用政策或非共用政策。 Note: 如果您在「政策」頁面中新增或編輯共用政策，還必須得將這些政策指派到群組或位置。否則這些政策不會生效。 如需詳細資訊，請參閱： • 安全政策類型 • 關於共用和非共用政策 • 新增政策
鎖定和解除鎖定政策設定	您可以允許或防止用戶端使用者架構部分政策設定和用戶端使用者介面設定。請參閱： 防止使用者在用戶端電腦上停用防護
編輯政策	如果您希望變更現有政策中的設定，則可以對其進行編輯。您可以透過修改電腦的安全性政策來提高或降低電腦的防護程度。除非變更群組指派，否則不必重新指派經過修改的政策。請參閱： 編輯政策
指派政策	若要使用政策，必須將政策指派給一個或多個群組或位置。請參閱： 指派政策給群組或位置
測試政策	賽門鐵克建議您在生產環境中運用新政策之前，一律先測試新政策。
更新用戶端政策	可依據可用頻寬，架構用戶端使用推送模式或提取模式作為政策更新方法。請參閱： 使用推送模式或提取模式更新用戶端上的政策和內容
取代政策	可使用一個共用政策取代另一個共用政策。您可以取代所有位置或某一位置的共用政策。請參閱： 取代政策
複製和貼上政策	您可能想要複製目前的政策作為新政策的基礎使用，而非新增新政策。 您可以在「政策」頁面或「用戶端」頁面上的「政策」標籤上複製和貼上政策。 Note: 還可以使用「用戶端」頁面上的「政策」標籤，複製群組中的所有政策，將其貼到其他群組中。 如需詳細資訊，請參閱： • 在「用戶端」頁面上複製並貼上政策 • 在「政策」頁面中複製和貼上政策
將共用政策轉換為非共用政策	您可以複製共用政策的內容，然後從該內容建立非共用政策。請參閱： 關於共用和非共用政策 您可以透過使用複本，變更某個位置中的共用政策內容，而不影響所有其他位置。此複本會覆寫現有非共用政策。 當共用政策不再套用至所有群組或所有位置時，您可將此政策轉換為非共用政策。完成轉換時，轉換後具有新名稱的政策會出現在「位置限定的政策與設定」下方。請參閱： 將共用政策轉換為非共用政策
匯出和匯入政策	若要在不同站台或管理伺服器使用現有政策，可匯出該政策。之後可以匯入此政策，並將其應用於群組或特定位置。請參閱： 匯出和匯入個別 Endpoint Protection 政策
撤銷政策	如果刪除某政策，Symantec Endpoint Protection Manager 將從資料庫中移除該政策。如果您不想刪除某政策，但也不想再使用它，可以撤銷政策。 您可以撤銷「病毒和間諜軟體防護政策」和「LiveUpdate 設定政策」以外的任何類型的政策。請參閱： 從群組或位置解除指派政策
刪除政策	如果政策已指派至一個或多個群組和位置，則無法刪除政策，除非從所有群組和位置取消指派該政策。您也可以將政策取代為另一個政策
檢查用戶端是否具有最新的政策	您可以檢查用戶端是否具有最新政策。如果不是，您可以在用戶端上手動更新政策。請參閱： • 使用政策序號檢查用戶端伺服器通訊 • 更新用戶端政策

安全性政策類型

可以使用多種不同類型的安全性政策來管理網路安全性。多數類型的政策會在安裝期間自動建立。可以使用預設政策,也可以自訂政策以符合特定環境的需要。

Table 56: 安全性政策類型

政策類型	說明
病毒和間諜軟體防護政策	「病毒和間諜軟體防護政策」提供下列防護： - 透過使用特徵偵測,移除和修復病毒和安全性風險的負面影響。 - 透過使用「下載智慧型掃描」中的信譽資料,偵測使用者所嘗試下載檔案中的威脅。 - 透過使用行為分析 (SONAR) 啟發式技術和信譽資料,偵測顯示可疑行為的應用程式。 「病毒和間諜軟體防護政策」透過其行為分析技術尋找行為異常情況。 Note: 「下載智慧型掃描」和行為分析技術僅可用於 Windows 用戶端。 如需詳細資訊,請參閱： 在用戶端電腦上管理掃描
防火牆政策	「防火牆政策」提供下列防護： - 攔截未授權的使用者存取連線至 Internet 的電腦和網路。 - 偵測駭客攻擊。 - 清除不需要的網路流量來源。 Note: 防火牆政策僅能套用於 Windows 用戶端。 如需詳細資訊,請參閱： 管理防火牆防護
入侵預防政策	入侵預防政策自動偵測並攔截網路攻擊和瀏覽器上的攻擊,以及保護應用程式免受弱點攻擊。請參閱： 管理入侵預防
應用程式與裝置控制	應用程式與裝置控制政策保護系統資源免受應用程式使用並管理可連線到電腦的週邊裝置。請參閱： 設定應用程式控制 應用程式控制政策僅適用於 Windows 用戶端。裝置控制政策適用於 Windows 和 Mac 電腦。
主機完整性	主機完整性政策提供定義、強制執行和還原用戶端電腦的安全性的功能,以保護企業網路和資料的安全。使用此政策驗證存取網路的用戶端是否執行防毒軟體、修正程式和定義的其他應用程式準則。請參閱： 設定主機完整性
LiveUpdate 政策	「LiveUpdate 內容政策」和「LiveUpdate 設定政策」包含決定用戶端電腦如何以及何時從 LiveUpdate 下載內容更新的設定。可以定義用戶端所聯絡的電腦,以檢查更新和排程用戶端電腦檢查更新的時間和方法。請參閱： 如何更新用戶端上的內容和定義檔
記憶體攻擊緩和	記憶體攻擊緩和和政策會使用 DLL 劫取、HeapSpray 緩和與 Java 侵入預防這類緩和技術,停止對軟體的已知和未知弱點進行攻擊嘗試。請參閱： 使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊

政策類型	說明
Web 和雲端存取防護	Web 和雲端存取防護 會將網路流量傳送到 Symantec Cloud Secure Web Gateway (Cloud SWG)。Cloud SWG 解決方案保護使用者和組織的方式為，對應用程式和網站進行分類，然後根據政策允許或拒絕存取它們。 Symantec Web Security Service 已在 2022 年重新命名為 Symantec Cloud Secure Web Gateway。 請參閱： 使用 Web 和雲端存取防護控制網路存取
例外	「例外政策」提供從病毒和間諜軟體掃描偵測以及行為分析偵測中排除應用程式和程序的能力。 您還可以從應用程式控制中排除應用程式。請參閱： 管理 Symantec Endpoint Protection 中的例外

更多資訊

[執行適用於所有政策的工作](#)

在 Windows 用戶端上更新安全政策

如果您認為沒有最新的政策，可手動更新 Symantec Endpoint Protection 用戶端電腦上的政策。

- 如果政策設定阻止您開啟使用者介面或通知區域圖示，您可能無法手動更新政策。在 Symantec Endpoint Protection Manager 中，沒有任何指令可用於手動提示用戶端更新政策。
- 用戶端會根據提取模式或推送模式的更新方法檢查政策更新。
- 如果用戶端未收到更新，則可能是通訊出現問題。檢查政策序號，以查證您的受管用戶端電腦是否可與管理伺服器通訊。

更新用戶端政策

1. 在 Windows 工作列中，於通知區域中的 Symantec Endpoint Protection 圖示上按下滑鼠右鍵，然後按「更新政策」。
2. 在用戶端中，按「說明 > 疑難排解 > 管理」，然後按「更新」。

從其他用戶端匯出和匯入用戶端政策

如果用戶端未連接到 Symantec Endpoint Protection Manager，則您應從已連接的其他用戶端匯出 policy.xml 檔，然後匯入政策。

1. 在連接到管理伺服器的用戶端中，按「說明 > 疑難排解 > 管理」。
2. 在「管理」面板中的「政策設定檔」下，按「匯出」，然後將 policy.xml 儲存到可以從第二個用戶端存取的位置。
3. 在第二個用戶端上，按一下「說明 > 疑難排解 > 管理」，並鍵入密碼，然後按一下「匯入」。從第一個用戶端找到政策並按照提示進行操作。
從 14.3 RU10 開始，您必須鍵入密碼。在舊版本中，密碼是選用性項目。您將會在第一次安裝或升級管理伺服器時設定密碼。

建立自訂 Symantec Endpoint Protection Manager 政策

建立您自己的自訂 Symantec Endpoint Protection Manager 政策。

Symantec Endpoint Protection Manager 針對各種類型的防護隨附有預設政策。但您可以建立自己的自訂政策。而且您可以為各類型的政策建立多個版本。

賽門鐵克建議您在生產環境中使用新政策之前，一律先測試新政策。

建立自訂政策

-
1. 在主控台中，按下「政策」。
 2. 在「政策」頁面中，選取政策類型，再按下新增新政策的連結。
 3. 修改政策設定以提升或降低防護。
 4. 按下「確定」儲存政策。
 5. 可選擇將新政策指派至群組。

您可以在建立政策期間或建立政策之後，將新政策指派至群組。新政策將取代相同防護類型的目前指派政策。請參閱：
[指派政策給群組或位置](#)

更多資訊

[執行適用於所有政策的工作](#)

編輯政策

您可以在「用戶端」頁面及「政策」頁面的「政策」標籤上編輯共用和非共用政策。

位置與群組可以共用相同的政策。您必須先完成編輯，才能指派共用政策。請參閱：

[指派政策給群組或位置](#)

在「政策」頁面上編輯政策 (選項 1)

1. 若要在「政策」頁面編輯政策，請在主控台中按一下「政策」。
2. 在「政策」頁面的「政策」下方，按下政策類型。
3. 在「政策類型 政策」窗格中，按一下要編輯的特定政策。
4. 在「工作」下方，按下「編輯政策」。
5. 必要時，在「政策類型 政策概述」窗格中，編輯政策的名稱和說明。
6. 若要編輯政策，請針對政策按一下任一個「政策類型 政策」頁面。

在「用戶端」頁面上編輯政策 (選項 2)

1. 若要在「用戶端」頁面編輯政策，請在主控台中按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方，選取要為其編輯政策的群組。
3. 在「政策」標籤中，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
您必須停用此群組的繼承。如果沒有取消核取繼承，就無法編輯政策。
4. 在「位置限定的政策與設定」下方，捲動尋找要編輯其中政策的位置名稱。
5. 找出要編輯的位置限定政策。
6. 在選取的政策右側，按下「工作」，然後按下「編輯政策」。
7. 執行下列其中一項工作：
 - 若要編輯非共用政策，請進行下一步驟。
 - 若要編輯共用政策，請在「編輯政策」對話方塊中，按下「編輯共用」以編輯所有位置中的該政策。
8. 對於要編輯的政策類型，您可以按下連結。

尋找政策的預設設定

如果您已變更政策的設定，則可以將政策還原為其預設設定。您可以新增 <政策類型>> 政策，其自動包括預設設定。請參閱：

[建立自訂 Symantec Endpoint Protection Manager 政策](#)

在「政策」頁面中複製和貼上政策

可以在“策略”页面中复制和粘贴策略。例如,您可能想要稍微編輯政策設定以套用於其他群組。

在「政策」頁面中複製政策

1. 在主控台中, 按下「政策」。
2. 在「政策」頁面的「政策」下方, 按一下要複製的政策類型。
3. 在「政策類型 政策」窗格中, 按一下要複製的特定政策。
4. 在「政策」頁面的「工作」下方, 按一下「複製政策」。
5. 如果您不想再收到關於此程序的通知, 請在「複製政策」對話方塊中勾選「不要再顯示此訊息」。
若要重新顯示「不要再顯示此訊息」核取方塊, 請按一下「管理」>「管理員」, 並選取管理員帳戶, 然後按一下「重設複製政策提醒」。
6. 按下「確定」。

在「政策」頁面中貼上政策

1. 在主控台中, 按下「政策」。
2. 在「政策」頁面的「政策」下方, 按一下要貼上的政策類型。
3. 在「政策類型 政策」窗格中, 按一下要貼上的特定政策。
4. 在「政策」頁面的「工作」下方, 按一下「貼上政策」。

更多資訊

- [在「用戶端」頁面上複製並貼上政策](#)
- [執行適用於所有政策的工作](#)

在「用戶端」頁面上複製並貼上政策

您可以複製並貼上政策而不必新增政策。您可以在「用戶端」頁面上複製共用或非共用政策。

在「用戶端」頁面中複製政策

1. 在主控台中, 按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方, 選取要為其複製政策的群組。
3. 在「政策」標籤的「位置限定的政策與設定」下方, 捲動尋找要複製其中政策的位置名稱。
4. 找出您在該位置中要複製的特定政策。
5. 在政策的右側, 按一下「工作」, 然後按一下「複製」。
6. 按下「確定」。

在「用戶端」頁面上貼上政策

1. 在主控台中, 按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方, 選取要為其貼上政策的群組。
3. 在「政策」標籤上, 取消勾選「從父群組」群組名稱" 繼承政策和設定」。
您必須停用此群組的繼承。如果沒有取消核取繼承, 就無法貼上政策。
4. 在「位置限定的政策與設定」下方, 捲動尋找要貼上其政策的位置名稱。
5. 找出您在該位置中要貼上的特定政策。
6. 在政策的右側, 按一下「工作」, 然後按一下「貼上」。
7. 當畫面出現覆寫現有政策的提示時, 請按一下「是」。

更多資訊

- [在「政策」頁面中複製和貼上政策](#)
- [執行適用於所有政策的工作](#)

指派政策給群組或位置

您可以透過群組將政策指派到用戶端電腦。每一群組的每一防護類型任何時間皆必須指派一個且僅一個政策。通常，您可為執行不同平台的用戶端建立單獨的群組。如果將執行不同平台的用戶端置於同一群組，則每個用戶端平台會忽略未套用的任何設定。

未指派的政策不會下載到群組和位置中的用戶端電腦。如果您在新增政策時沒有指派政策，可以稍後再指派給群組和位置。您也可以重新指派政策給不同的群組或位置。

政策指派至電腦群組的情形如下：

- 初始安裝時，賽門鐵克預設的安全政策會指派至 **My Company** 父群組。
- **My Company** 父群組內的安全政策會自動指派至每一新增的子群組。依據預設，新建的子群組會從 **My Company** 繼承。
新群組一律會繼承自其直屬父群組。如果您建立子群組階層，那麼每一個群組都會從其直屬父群組繼承，而不是從頂層父群組繼承。
- 您可利用指派其他同類型政策的方式，取代群組內的政策。您可取代已指派至 **My Company** 父群組或任何子群組的政策。

這些圖示顯示了下列資訊：

Table 57: 政策圖示

圖示	說明
	未指派政策的群組。
	已指派政策的群組。文字為粗體。
	未指派政策的位置。
	已指派政策的位置。文字為粗體。
	繼承自父群組且未指派政策的位置。
	繼承自父群組且已指派政策的位置

指派政策給群組或位置

1. 在主控台中，按下「政策」> 政策類型。
2. 在「政策」頁面上，選取政策，然後按下「指派政策」。
3. 在「指派政策」對話方塊中，選取群組或位置，然後按下「指派」。
4. 按下「確定」以確認。

更多資訊

[從群組或位置解除指派政策](#)

取代政策

您可能需要以其他共用政策取代某個共用政策。您可以在所有位置或為個別位置取代共用政策。

當您取代所有位置的政策時，管理伺服器只會針對有該政策的位置取代政策。例如，假設 Sales 群組在其四個位置的其中三個使用「業務」政策。如果要用「行銷」政策取代「業務」政策，就只有這三個位置會收到「行銷」政策。

您可能需要某一組用戶端使用相同的設定，不論各用戶端的位置在哪裡。在這種狀況下，您可以使用共用政策取代非共用政策。使用共用政策分別為每個位置取代非共用政策。

取代所有位置的共用政策

1. 在主控台中，按下「政策」。
2. 在「政策」頁面的「政策」下方，按下要取代的政策類型。
3. 在「政策類型 政策」窗格中，按一下政策。
4. 在「政策」頁面的「工作」下方，按下「取代政策」。
5. 在「取代 政策類型 政策」對話方塊的「新 政策類型 政策」清單方塊中，選取要取代舊政策的共用政策。
6. 選取要取代現有政策的群組和位置。
7. 按下「取代」。
8. 當取代群組和位置政策的確認提示顯示時，按下「是」。

取代某個位置的共用政策或非共用政策

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面中的「用戶端」下，選取要為其取代政策的群組。
3. 在「政策」標籤中，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
您必須停用此群組的繼承。如果沒有取消核取繼承，就無法取代政策。
4. 在「位置限定的政策與設定」下，捲動尋找包含政策的位置。
5. 在要取代的政策旁邊，按下「工作」，然後按下「取代政策」。
6. 在「取代政策」對話方塊中的「新政策」清單方塊內，選取取代政策。
7. 按下「確定」。

更多資訊

[執行適用於所有政策的工作](#)

匯出和匯入個別 Endpoint Protection 政策

可以匯出和匯入政策而不是重新建立政策。所有與政策關聯的設定都會自動匯出。

可能需要針對下列原因匯出政策：

- 從舊版管理伺服器更新為新版管理伺服器。需要使用先前自訂的政策更新新的管理伺服器。
- 需要匯出政策以在另一個網站中使用。

一次匯出和匯入一個政策。匯出檔案後，將它匯入並套用至群組，或只套用至位置。可以在「用戶端」頁面中為特定位置匯出共用或非共用政策。

從「政策」頁面匯出單一政策

1. 在主控台中，按下「政策」。
2. 在「政策」頁面的「政策」下方，按下要匯出的政策類型。
3. 在「政策類型 政策」窗格中，按一下要匯出的特定政策。
4. 在「政策」頁面中的「工作」下方，按下「匯出政策」。
5. 在「匯出政策」對話方塊中，尋找要匯出政策檔案的資料夾，然後按下「匯出」。

從「用戶端」頁面匯出共用或非共用政策

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，選取要針對其匯出政策的群組。

3. 在「政策」標籤中，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
您必須停用此群組的繼承。如果沒有取消勾選繼承，就無法匯出政策。
4. 在「位置限定的政策與設定」下方，捲動尋找要匯出其中政策的位置名稱。
5. 找出要匯出的位置限定政策。
6. 在政策的右邊按下「工作」，然後按下「匯出政策」。
7. 在「匯出政策」對話方塊中，瀏覽到您要將政策匯出至哪一個資料夾。
8. 在「匯出政策」對話方塊中，按下「匯出」。

匯入單一政策

1. 在主控台中，按下「政策」。
2. 在「政策」頁面的「政策」下方，按下您要匯入的政策類型。
3. 在「政策類型 政策」窗格中，按一下要匯入的政策。
4. 在「政策」頁面的「工作」下方，按下「匯入政策類型 政策」。
5. 在「匯入政策」對話方塊中，瀏覽至要匯入的政策檔案，然後按下「匯入」。

更多資訊

[執行適用於所有政策的工作](#)

關於共用和非共用政策

政策可以是共用政策或非共用政策。如果將政策套用於多個群組或位置，則該政策為共用政策。如果您建立共用政策，則可以在所有使用政策的群組和位置輕鬆編輯和取代政策。您可以在 My Company 群組層級或較低層級套用共用政策，而子群組能夠繼承政策。您可以擁有多個共用政策。

如果對於特定的群組或位置，需要一個特定政策，則可建立一個唯一政策。您可以將此唯一、非共用政策指派到一個特定群組或位置。在每個位置，每種政策類型僅能有一個政策。

例如，下面是一些可能的狀況：

- 財務部門中的一個使用者群組在辦公室和在家裡時，需要使用不同的位置連線到企業網路。對於該群組，您可能需要將具有各自的規則集和設定的不同防火牆政策套用於每個位置。
- 您的遠端使用者通常會使用 DSL 及 ISDN，因此他們可能需要 VPN 連線。其他遠端使用者需要使用撥號來連線至企業網路。但是，銷售及行銷群組還需要使用無線連線。針對這些群組連接至企業網路時所處的位置，每個群組可能需要有自己的防火牆政策。
- 對於在大多數員工工作站上安裝的非驗證應用程式，您需要實作限制性政策以保護企業網路免受攻擊。您的 IT 群組可能需要存取其他應用程式。因此相較於一般員工，IT 群組的安全性政策限制可能要少些。在這種狀況下，您可以為 IT 群組建立不同的防火牆政策。

您通常會在 [政策] 頁面的 [政策] 標籤上新增群組和位置共用的任何政策。不過，如果增加的政策不是群組之間共用的政策，而只套用到特定位置，請在 [用戶端] 頁面中新增。如果決定要在 [用戶端] 頁面中新增政策，可以使用下列任何方法增加新政策：

- 新增政策。請參閱：
[新增政策](#)
- 複製現有政策以此為基礎建立新政策。請參閱：
 - 在「政策」頁面中複製和貼上政策
 - 在「用戶端」頁面上複製並貼上政策
- 匯入以前從其他站台匯出的政策。請參閱：
[匯出和匯入個別 Endpoint Protection 政策](#)

更多資訊

- [執行適用於所有政策的工作](#)
- [將共用政策轉換為非共用政策](#)

將共用政策轉換為非共用政策

您可以複製共用政策的內容，然後從該內容建立非共用政策。您可以透過使用複本，變更某個位置中的共用政策內容，而不影響所有其他位置。複本會覆寫現有的共用政策。

完成轉換時，轉換後具有新名稱的政策會出現在「位置限定的政策與設定」下方。不過，除非將非共用政策從「用戶端」頁面 > 「政策」標籤複製到「政策」頁面，否則它不會出現在政策類型的「政策」頁面中。

如需詳細資訊，請參閱：

- [關於共用和非共用政策](#)
- [在「用戶端」頁面上複製並貼上政策](#)
- [在「政策」頁面中複製和貼上政策](#)

將共用政策轉換為非共用政策

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方，選取您要為其轉換政策的群組。
3. 在與上一步驟所選群組關聯的窗格中，按一下「政策」。
4. 在「政策」標籤上，取消勾選「從父群組 **group_name** 繼承政策和設定」。
您必須停用此群組的繼承。如果沒有取消核取繼承，就無法取代政策。
5. 在「位置限定的政策與設定」下方，捲動尋找位置名稱以及要轉換的特定政策。
6. 在特定政策旁，按一下「工作」，然後按一下「轉換為非共用政策」。
7. 在「概述」對話方塊中，編輯政策的名稱與說明。
8. 根據需要修改其他政策設定。
9. 按下「確定」。

更多資訊

[執行適用於所有政策的工作](#)

從群組或位置解除指派政策

如果要永久刪除某個政策或儲存政策以便日後使用，則可能需要從群組或位置解除指派該政策。

例如，某個特定群組可能在您採用新政策後發生問題。如果您想將政策保留在資料庫中，則可以將政策撤銷而不是刪除。撤銷政策時，政策會自動從您將政策指定至的群組和位置中撤銷。使用政策的位置數量會顯示在「政策」頁面的「政策類型政策」窗格中。

NOTE

刪除政策前，必須從所有群組和位置撤銷政策或取代政策。

您可以從某個位置或群組中的「政策」頁內撤銷下列政策以外的所有政策：

- 病毒和間諜軟體防護
- **LiveUpdate** 設定

僅能以其他「病毒和間諜軟體防護」政策或「**LiveUpdate** 政策」來取代它們。請參閱：

- [取代政策](#)
- [指派政策給群組或位置](#)

在「政策」頁面中解除指派共用政策

1. 在主控台中，按一下「政策」。

-
2. 在「政策」頁面的「政策」下方，按下您要撤銷的政策類型。
 3. 在「政策類型 政策」窗格中，按一下要撤銷的特定政策。
 4. 在「政策」頁面的「工作」下方，按下「撤銷政策」。
 5. 在「撤銷政策」對話方塊中，勾選您要從其中撤銷政策的群組和位置。
 6. 按下「撤銷」。
 7. 當自群組和位置撤銷政策的確認提示顯示時，按下「是」。

在「用戶端」頁面中解除指派共用或非共用政策

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方，選取您要為其撤銷政策的群組。
3. 在「政策」標籤中，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
您必須停用此群組的繼承。如果沒有取消核取繼承，就無法撤銷政策。
4. 在「位置限定的政策與設定」下方，捲動尋找您要為其撤銷政策的位置名稱。
5. 找出要從該位置撤銷的政策。
6. 按下「工作」，然後按下「撤銷政策」。
7. 在「撤銷政策」對話方塊中，按下「是」。

更多資訊

[執行適用於所有政策的工作](#)

啟用應用程式探索

您可能想要監控和收集在您環境中執行於每部電腦上之應用程式和服務的相關資訊。

您使用這些資訊以新增至下列政策和功能：

- 防火牆政策
- 應用程式與裝置控制政策
- 行為分析
- 主機完整性政策
- 網路應用程式監控
- 檔案指紋清單

您會將用戶端架構為收集資訊，接著將清單傳送至管理伺服器。用戶端越多，暫時儲存的應用程式和資料種類就會越多。此資料可能會對已經資源不足的管理伺服器產生 CPU 或記憶體問題。作為最佳實務，請先在一個用戶端子集上執行應用程式學習。

NOTE

在某些國家/地區，依據當地法律，在某些狀況下可能不允許使用所學習的應用程式工具。例如，您可能想要收集一份員工從其公司筆記型電腦登入您辦公室網路及從其家中登入時所存取的應用程式清單。在您使用此工具之前，請確認您可在當地法令管轄範圍內使用該工具。若不允許，請停用應用程式學習。

NOTE

Mac 和 Linux 用戶端不支援已探索的應用程式。

步驟 1：啟用網站的應用程式學習

如要啟用網站的應用程式學習

1. 在主控台中，按一下「管理員」>「伺服器」。
2. 於「檢視伺服器」下，執行下列其中一項動作：
 - a. 按一下「本機網站 (網站 <網站名稱>)」。
 - b. 展開「遠端網站」，接著按一下「網站 <網站名稱>」。

3. 於「工作」之下，按一下「編輯網站屬性」。
4. 在「一般」標籤中，勾選「保持追蹤用戶端所執行的每個應用程式」。
5. 如要最小化學習到應用程式資料佔用的資料庫空間，請勾選「在 x 天後刪除已學習的應用程式」。如果您在更新管理伺服器資料庫時遇到問題，賽門鐵克建議您輸入 7。
6. 按下「確定」。

步驟 2：將已學習的應用程式傳送至某個位置或群組的管理伺服器

在你啟用網站以從用戶端收集已學習應用程式的清單後，您可讓用戶端依群組或依位置將清單傳送至伺服器。

NOTE

用戶端必須安裝「網路威脅防護」元件，才可使此功能發揮作用。

如要將已學習的應用程式傳送至某群組的管理伺服器

1. 在主控台中，按一下「用戶端」、選取一個群組，然後按下「政策」。
2. 在「政策」標籤上，按下「通訊設定」。
3. 在「通訊設定」對話方塊中，勾選「探索在用戶端電腦執行的應用程式」，然後按下「確定」。

傳送探索到的應用程式至某一位置的管理伺服器

1. 在主控台中，按一下「用戶端」、選取一個群組，然後按下「政策」。
2. 在「政策」上，選取位置，然後展開「位置限定的設定」。
3. 在「通訊設定」右邊，按下「工作」，然後取消勾選「使用群組通訊設定」並按下「編輯設定」。
勾選此設定能讓您建立一個位置設定，而不是群組設定。
4. 在「位置名稱 的通訊設定」對話方塊中，勾選「探索在用戶端電腦執行的應用程式」，然後按一下「確定」。

更多資訊：

- 如要允許變更應用程式總和檢查碼，您必須啟用「網路應用程式監控」。請參閱：[攔截可能受到攻擊的網路應用程式](#)
- 群組或位置中的每個用戶端執行應用程式時，您可以設定將通知傳送至您的電子郵件地址。請參閱：[設定管理員通知](#)
- [建立應用程式例外](#)

搜尋有關電腦執行之已探索應用程式的資訊

當管理伺服器收到來自用戶端的已探索應用程式清單之後，您可以執行查詢以尋找有關這些應用程式的詳細資料。例如，您可以尋找所有使用未經授權應用程式的用戶端電腦。然後您可以建立防火牆規則，來攔截用戶端電腦上的應用程式。或者，您可能想要升級所有用戶端電腦，以使用最新版的 Microsoft Word。您可以使用來自任何政策類型的「搜尋應用程式」工作。

NOTE

Mac 用戶端不會監控應用程式和服務。

您可以使用下列方式搜尋應用程式：

- 根據應用程式。
您可以將搜尋範圍限制為特定應用程式或應用程式詳細資料，例如名稱、檔案指紋、路徑、大小、版本或最後修改時間。
- 根據用戶端或用戶端電腦。
您可以搜尋特定使用者或特定用戶端電腦執行的應用程式。例如，您可以根據電腦的 IP 位址進行搜尋。

您也可以直接在防火牆政策內搜尋要新增到防火牆規則的應用程式名稱。請參閱：

[定義應用程式的相關資訊](#)

NOTE

啟用可記錄用戶端執行之各種應用程式的功能前，不會收集「搜尋」方塊中的資訊。您可以移至每個群組或位置的「用戶端」頁面的「通訊設定」對話方塊來啟用此功能。

搜尋有關電腦執行的應用程式資訊

1. 在主控台中，按下「政策」。
2. 在「政策」頁面的「工作」下方，按下「搜尋應用程式」。
3. 在「搜尋應用程式」對話方塊的「搜尋應用程式於」欄位右側，按下「瀏覽」。
4. 在「選取群組或位置」對話方塊中，選取您要檢視應用程式的用戶端群組，然後按下「確定」。

您一次只能指定一個群組。

5. 請確定勾選「搜尋子群組」。
6. 執行下列其中一項動作：
 - 若要根據使用者或電腦資訊進行搜尋，請按下「依據用戶端/電腦資訊」。
 - 若要根據應用程式進行搜尋，請按下「依據應用程式」。
7. 按下「搜尋欄位」下的空白儲存格，然後從清單中選取搜尋條件。

「搜尋欄位」儲存格會顯示所選選項的條件。如需這些條件的詳細資料，請按下「說明」。
8. 按下「比較運算子」下的空白儲存格，然後選取其中一個運算子。
9. 按下「值」下的空白儲存格，然後選取或輸入值。

「值」儲存格可能會從下拉式清單提供格式或值，視您在「搜尋欄位」儲存格中選取的條件而定。
10. 若要加入其他搜尋條件，請按下第二列，然後在「搜尋欄位」、「比較運算子」和「值」儲存格中輸入資訊。

如果您輸入多列的搜尋條件，則查詢會嘗試符合所有條件。
11. 按下「搜尋」。
12. 在「查詢結果」表格中，執行下列任一動作：
 - 按下捲動箭頭，可檢視更多列和欄。
 - 按下「上一頁」和「下一頁」，可查看資訊的其他畫面。
 - 選取某列，然後按下「檢視詳細資料」，可查看有關應用程式的其他資訊。

除非您將結果匯出至檔案，否則不會儲存結果。
13. 若要移除查詢結果，請按下「清除全部」。
14. 按下「關閉」。

更多資訊

- [執行適用於所有政策的工作](#)

透過自適應防護攔截 Living Off the Land (LOTL) 攻擊

從 143 RU10 開始，您可以在內部部署 Symantec Endpoint Protection Manager 上架構、管理和強制執行行為。若要管理自適應防護，請執行下列步驟：

-
- [開始之前](#)
 - [步驟 1：完成自適應防護需求](#)
 - [步驟 2：等待自適應防護了解您環境中的行為](#)
 - [步驟 3：攔截所有零普及率的應用程式行為](#)
 - [步驟 4：決定允許或拒絕哪些應用程式行為 \(進階\)](#)
 - [步驟 5：減少誤報數目 \(選用\)](#)

[開始之前](#)

選擇您想要用來管理自適應防護的管理選項：

- 具有無輕度註冊的 Symantec Endpoint Protection 或 Symantec Endpoint Security Enterprise (SESE) 授權的內部部署。
您在沒有熱圖或任何感染狀況資料的情況下管理自適應防護政策。
- 具有含輕度註冊的 Symantec Endpoint Security 完整 (SESC) 授權的內部部署。
您在具有熱圖的情況下管理自適應防護政策，並從遙測資料中取得感染狀況。
- 混合管理，即內部部署與雲端管理的組合。您在 Symantec Endpoint Security 雲端中註冊 Symantec Endpoint Protection Manager 網域。
如需從雲端管理自適應防護的相關資訊，請參閱[從雲端而不是從 Symantec Endpoint Protection Manager 管理自適應防護](#)。

如需每個管理層級可取得哪些自適應防護功能的相關資訊，請參閱[Symantec Endpoint Protection 與 Symantec Endpoint Security 之間的自適應防護功能比較](#)。

如需不同管理選項的說明，請參閱[內部部署、混合或完全雲端管理選項](#)。

[步驟 1：完成自適應防護需求](#)

若要從 Symantec Endpoint Protection Manager 管理自適應防護，您必須符合下列需求：

- Symantec Endpoint Security Complete 授權。
Symantec Endpoint Security Complete 授權啟動稱為[輕度註冊](#)的程序。輕度註冊會與 Symantec Endpoint Security 雲端伺服器進行通訊，而不需要在雲端中完全註冊。此通訊提供可修改行為規則的熱圖和感染狀況資料。
如果您使用 Symantec Endpoint Protection 或 Symantec Endpoint Security Enterprise 授權，則不會取得輕度註冊。不過，您仍然可以在沒有快速調整功能或熱圖的情況下使用自適應防護政策來管理行為。
- Symantec Endpoint Protection Manager 14.3 RU10。
- Symantec Endpoint Protection Windows 用戶端 14.3 RU10。
Linux 或 Mac 電腦不支援自適應防護。
- 針對所有用戶端群組啟用資料收集 (遙測)。當您安裝管理伺服器時，預設會啟用遙測。
若要啟用遙測，請參閱[管理用戶端傳送給賽門鐵克的匿名或非匿名資料](#)。
- 您的公司防火牆或 Proxy 必須允許下列 URL：<https://ent-shasta-rrs.symantec.com>。如果防火牆攔截此 URL，則自適應防護不會取得遙測。
如需防火牆必須允許的所有 URL 的相關資訊，請參閱 [Symantec Endpoint Protection \(SEP\) 和 Symantec Endpoint Security \(SES\) 所需的外部 URL](#)。
- 風險日誌應該保留 14 天以上的資料。
事件計數所使用的資料量與風險日誌所保留的資料量一樣多。天數可能會受限於資料庫大小。
如需增加資料保留期間的相關資訊，請參閱[指定日誌大小以及在資料庫中保留日誌項目的時間長度](#)。
- 已啟用行為分析 (SONAR)。
- 系統管理員或網域管理員帳戶。
- LiveUpdate 正在執行。
透過 Live Update 定期將行為清單新增至自適應防護政策。

步驟 2：等待自適應防護了解您環境中的行為

在您安裝或升級 Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端之後，必須等待管理伺服器收集您環境中所執行應用程式的足夠資料。

- 如果您是第一次安裝，則請等待 90 天。除非過了 90 天，否則應用程式行為的感染狀況會將狀態顯示為「學習」。
- 如果您進行升級，則請使用最佳判斷來決定合適時間，以準確反映您的正常商務活動。例如：
 - 如果您在不到 90 天前升級至 14.3 RU10，則會看到「學習」狀態。請至少等待 90 天。
 - 如果您已在 90 到 180 天前安裝 14.3 RU9 或更早版本，然後升級至 14.3 RU10，則會在過了 180 天之後看到 90 天的資料。然後，您會看到 180 天的資料。您有足夠的資料來做出決策。
 - 如果您已在一年多前安裝 14.3 RU9 或更早版本，然後升級至 14.3 RU10，則會看到長達一年的資料。您有足夠的資料來做出決策。
 - 如果您之前已停用遙測，則不會取得感染狀況資料。您必須啟用遙測，然後等待 90 天，自適應防護才會了解您的行為。

如需如何收集和分析資料的相關資訊，請參閱[用戶端如何偵測行為並將其傳送至自適應防護？](#)

步驟 3：攔截所有零普及率的應用程式行為

經過足夠長的時間後，感染狀況資料會同時出現在自適應防護政策和「進階安全性」頁面熱圖中。一開始，所有應用程式行為都設定為動作為「監控」的「探索」。

降低感染狀況行為指標的潛在攻擊面。在自適應防護政策中，零感染狀況行為會出現為藍色陰影。您應該攔截所有零感染狀況行為以減少攻擊面。在您的環境中，沒有零感染狀況的應用程式行為，因此您可以放心地將其攔截，而不會影響您的使用者。「行為規則」頁面顯示感染狀況，而非風險。您要尋找您認為在環境中合法的特定行為實例。

NOTE

在下列情況下，使用事件計數資料來決定是否攔截行為：您具有 Symantec Endpoint Protection 或 SES Enterprise 授權、輕度註冊失敗，或您的環境處於暗網中。

1. 在主控台中，按一下「政策 > 自適應防護」。
2. 在「行為規則」頁面上，按一下「快速調整」，然後按一下「是」。
然後，將所有零感染狀況事件標上「拒絕」(攔截)動作。

Behavior Rules

Potentially Risky Behaviors

Configure how Adaptive Protection handles unusual or risky behavior by trusted applications.

Quick Tune

Applications: All Behaviors: All Prevalence: All MITRE Technique: All Action: All

Events: Last 30 Days Events on any computer

Displaying 496 behavior(s) out of 496 total behaviors.

Application Behavior	MITRE Technique	Prevalence	Event Count	Action
CMSTP launching	T1218.003	Zero	0	☐ Allow ☒ Monitor ☐ Deny
Csvde launching	T1087.002	Learning	0	☐ Allow ☒ Monitor ☐ Deny
Curl launching	T1046	Zero	0	☐ Allow ☒ Monitor ☐ Deny
eHorus remote access tool launching		Zero	0	☐ Allow ☒ Monitor ☐ Deny
Esentutl downloading a file		Zero	0	☐ Allow ☒ Monitor ☐ Deny
Excel launching Msbuild tools		Zero	0	☐ Allow ☒ Monitor ☐ Deny
Expand downloading a file	T1105	Zero	0	☐ Allow ☒ Monitor ☐ Deny
Extrac32 downloading a file	T1105	Zero	0	☐ Allow ☒ Monitor ☐ Deny
Findstr downloading a file	T1105	Zero	0	☐ Allow ☒ Monitor ☐ Deny
GPresult launching	T11013 T1033	High	0	☐ Allow ☒ Monitor ☐ Deny
lcacls launching	T1222.001 T1083	High	0	☐ Allow ☒ Monitor ☐ Deny

Confirm

Quick Tune will set 451 zero prevalence behavior(s) to deny. Do you wish to continue?

Yes No

請確定將政策套用至適當的用戶端群組。

- 在「進階設定」頁面上，您可以新增用戶端使用者在攔截應用程式時收到的自訂通知。
- 若要儲存政策，請按一下「確定」。

在有新資料可用時，定期檢查零感染狀況行為。

如需自適應防護政策中設定的詳細資訊，請參閱[自適應防護政策設定](#)。

如需信任的應用程式和行為清單的相關資訊，請參閱[信任的應用程式參考](#)。

步驟 4：決定允許或拒絕哪些應用程式行為 (進階)

您在自適應防護政策中攔截零感染狀況行為之後，就不需要執行更多動作。不過，在下列情況下，您可能會想要變更其他感染狀況行為活動的行為動作：

- 您認為攔截特定行為十分危險，即使政策將其顯示為零感染狀況也是一樣。在該情況下，您可以將行為的動作從「拒絕」變更為「允許」或「監控」。
- 如果行為是低感染狀況 (但不是零感染狀況)，而且您認為該行為仍然不應該在您的環境中發生。您可以手動將行為移至「拒絕」，風險自負。在此情況下，您應該新增應用程式例外以消除風險。

如需建立例外的詳細資訊，請參閱：

[步驟 5：減少誤報數目 \(選用\)](#)

[建立應用程式例外](#)。

如果您擔心違反，則請更積極地拒絕行為。如果您擔心用戶端使用者收到許多有關已攔截應用程式的通知，則請不要積極地拒絕行為。

若要手動允許或攔截行為，請遵循下列步驟：

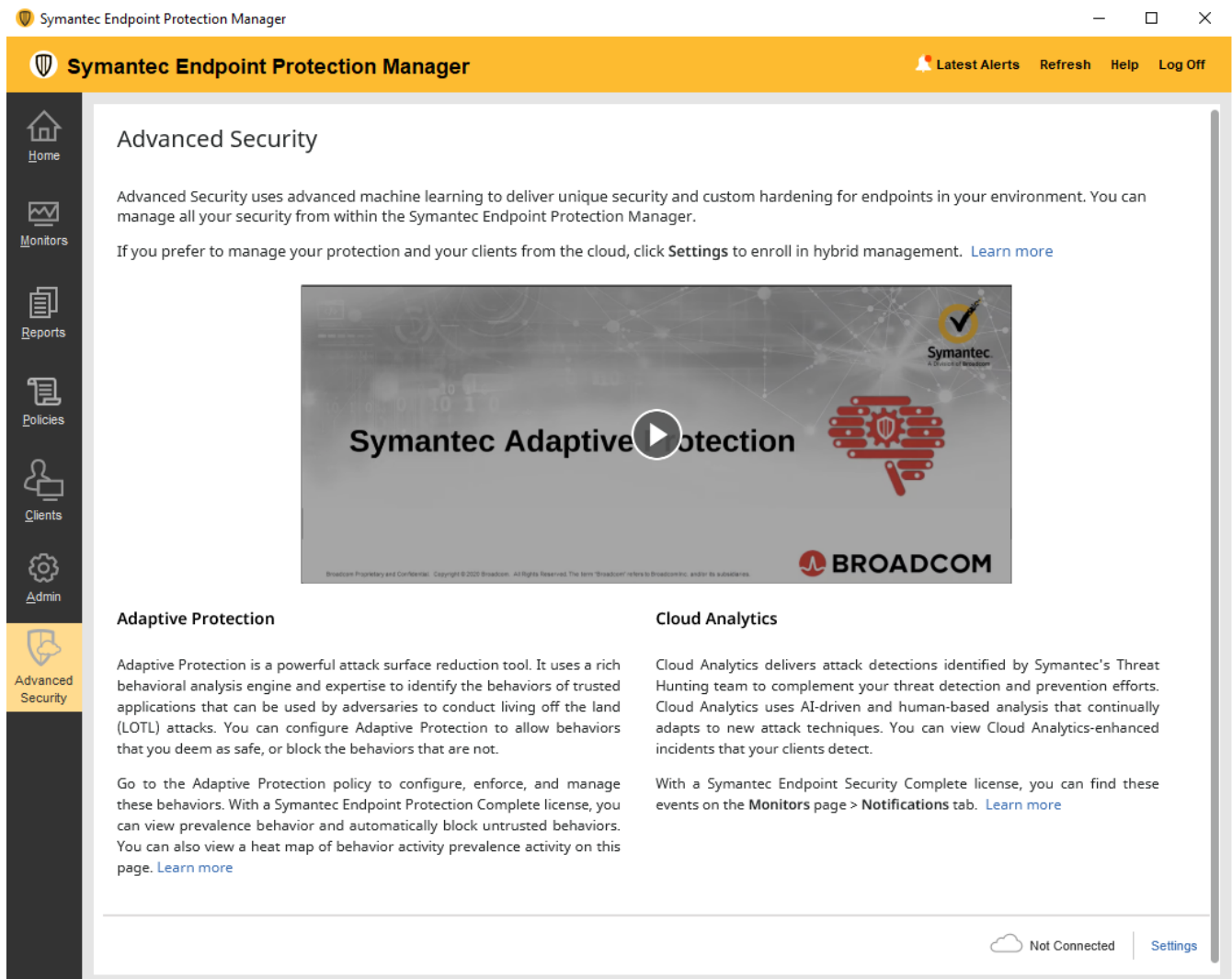
- 開啟自適應防護政策，然後按一下「行為規則」。
- 按一下「感染狀況」下拉式清單，然後選取「零」或「低」以查看您想要的感染狀況類別。
- 選取每個行為應用程式規則，然後按一下所需的全域動作。
- 按下「確定」儲存政策。

使用熱圖來評估感染狀況 (選用；僅限 SESC 授權)

熱圖和自適應防護政策都使用色彩編碼來顯示您環境中信任的應用程式行為的感染狀況。熱圖顯示您環境中行為的三維檢視，而自適應防護政策顯示二維檢視。不過，您只能變更政策中行為的動作。

NOTE

在您啟用 Symantec Endpoint Security Complete 授權後的 24 小時內，「進階安全性」頁面會顯示熱圖小工具。如果您因下列情況而看不到熱圖：您具有 Symantec Endpoint Protection 授權或 Symantec Endpoint Enterprise 授權，或是輕度註冊失敗。請參閱「[進階安全性](#)」頁面問題疑難排解。



步驟 5：減少誤報數目 (選用)

在您修改自適應防護政策中的行為規則之後，請檢查日誌以監控所有行為活動。如果自適應防護攔截許多行為，則可能指出已嘗試惡意活動，或者只是限制過強的規則攔截您合法使用的應用程式。您接著可以決定是否執行下列動作：

- 將動作變更為「監控」。
將規則設定為「監控」動作時，日誌可讓您更深入地瞭解環境中的行為，而不會在用戶端上實際將其攔截。
- 將應用程式例外新增至例外政策。
如果您新增讓行為感染狀況降為零的合法軟體例外，則可以手動拒絕應用程式行為。

請參閱[建立應用程式例外](#)。

- 不會採取任何動作。

若要檢視日誌，請執行下列步驟：

1. 在「監視器」頁面上，按一下「日誌 > SONAR：行為分析」。
2. 按一下「其他設定」>「事件類型」>選取「自適應防護」，然後按一下「檢視日誌」。

您也可以將誤報提交給賽門鐵克安全機制應變中心團隊。請參閱對 [Symantec](#) 和 [Carbon Black](#) 產品使用 [SymSubmit](#)。

Symantec Endpoint Protection 與 Symantec Endpoint Security 之間的自適應防護功能比較

下表顯示從下列項目管理用戶端時的自適應防護功能差異：內部部署 Symantec Endpoint Protection Manager、具有輕度註冊的 Symantec Endpoint Protection Manager 或混合管理 (在雲端中註冊 Symantec Endpoint Protection Manager)。

內部部署和輕度註冊選項使用 Symantec Endpoint Protection Manager 自適應防護政策。混合管理使用 Symantec Endpoint Security 雲端伺服器中的自適應防護政策。

	內部部署	具有輕度註冊的內部部署	混合/SES
熱圖普及率和事件計數 提供根據參與者和目標的行為感染狀況二維視覺化。此雙重維度檢視可更深入地了解如何在環境中傳播行為。 調適型防護如何收集感染狀況和事件計數？	是*	是*	是
快速調整 攔截所有零感染狀況行為。您有機會在攔截發生之前將其核准。	是	否	是
自動調整 自動識別並拒絕特定行為，以協助減少攻擊面。	否	否	是
威脅態勢鑑識 顯示全域威脅態勢中的最近攻擊，以及應用程式行為可能發生的攻擊鏈。	否	否	是
遙測指示器 顯示警示列或圖示以反白顯示遙測問題，以及指向疑難排解步驟或診斷工具的連結。	否	否	是
大量變更 可讓您選取多個行為，並且一次予以套用。	否	否	是
政策建議 提供建議，而建議是根據賽門鐵克對您環境內行為的歷史分析。這些見解使用遙測資料和威脅情報來判斷可以安全攔截的內容。	否	否	是
政策管理 可讓您選取要套用熱圖的政策。熱圖資料是從使用此政策的所有電腦所收集。	是	否	是
例外管理 可讓您修改現有規則以允許在客戶環境中觀察到的特定合法行為，同時仍然強制攔截相同行為的一般實例。	否	否	是

*在 Symantec Endpoint Protection Manager 中，切換顯示 30、60 或 90 天，而不是 90、180 或 365 天。

輕度註冊提供在 Symantec Endpoint Protection Manager 中管理自適應防護的最佳結果。輕度註冊會將 Symantec Endpoint Protection Manager 所管理的電腦中的遙測資料與 Symantec 後端遙測資料庫中的資料進行比對。管理伺服器必須提交遙測，自適應防護才能取得感染狀況。

如果您註冊到雲端，則雲端中的自適應防護政策會覆寫您在 Symantec Endpoint Protection Manager 中所新增的政策。

更多資訊

請參閱 [輕度註冊如何運作？](#)：

如需從雲端管理自適應防護的相關資訊，請參閱[從雲端而不是從 Symantec Endpoint Protection Manager 管理自適應防護](#)。

如需不同管理選項的說明，請參閱[內部部署、混合或完全雲端管理選項](#)。

輕度註冊如何運作？

輕度註冊是在 LiveUpdate 第一次將調適型防護內容下載至 Symantec Endpoint Protection Manager 時發生的背景程序。輕度註冊的目的是讓 Symantec Endpoint Protection Manager 建立一種與 Symantec Endpoint Security 雲端伺服器通訊以及接收資料的方法。輕度註冊還會將您的 Symantec Endpoint Security Complete 授權與您公司中的資料比對。

輕度註冊的工作方式如下：

- LiveUpdate 會將內容下載到 Symantec Endpoint Protection Manager，這會啟動向雲端伺服器的註冊工作。此註冊工作：
 - 驗證 Symantec Endpoint Security Complete 授權。
 - 檢查 Symantec Endpoint Protection Manager 網域中的用戶端群組是否已啟用遙測。如果大部分用戶端裝置硬體金鑰 (MID) 相符，則適當的 API 會向雲端伺服器傳回回應，指出您的組織符合註冊條件。
- 雲端伺服器授權註冊。
 - 如果註冊失敗，則「進階安全性」頁面會顯示 401 錯誤。如果已註冊 SEPM 網域，則您會看到 403 錯誤。請參閱[「進階安全性」頁面問題疑難排解](#)。

調適型防護如何收集感染狀況和事件計數？

使用 Symantec Endpoint Protection Manager 中的調適型防護，透過攔截信任的應用程式所執行的潛在風險行為來攔截 Living Off the Land (LOTL) 攻擊。

用戶端將一個應用程式行為複本傳送至 Symantec 後端遙測資料庫，並將第二個複本傳送至 Symantec Endpoint Protection Manager。分析進入遙測資料庫的複本以及所有用戶端電腦上執行的所有行為。這些行為會將具有感染狀況值的事件傳回給管理伺服器。進入管理伺服器的複本會顯示事件計數值。

感染狀況

感染狀況代表用戶端於一段時間內在其上辨識到單一行為的電腦數目。例如，在過去 180 天，Microsoft Word 可能已在 20 個用戶端上啟動 cmd.exe。

若要取得感染狀況，您必須啟用遙測，並且必須已成功進行輕度註冊。啟用遙測之後，在 90 天的學習後，您會看到感染狀況期限為零、低、中或高。只要啟用遙測，遙測資料庫就會從安裝管理伺服器的那天開始收集資料。例如：

- 如果您已在 2023 年 4 月安裝 SEPM 14.3 RU7，然後在 2025 年 2 月升級至 SEPM 14.3 RU10，則會在 2023 年 4 月開始收集感染狀況資料。
- 如果您已在 14.3 RU7 中停用遙測，然後在 2025 年 2 月於啟用遙測的情況下升級至 14.3 RU10，則會在 2025 年 2 月開始收集資料。
- 如果您在 2025 年 3 月將用戶端升級至 14.3 RU10，則會在 2025 年 2 月開始收集資料。

如果停用遙測，則您看到的每個行為都會顯示「未提供」感染狀況。如果您擁有 SESE 授權，則不會取得感染狀況。相反地，您必須根據事件計數來做出決定。

NOTE

除非感染狀況無法使用，否則請一律使用感染狀況資料，而不是事件計數。

如需啟用遙測的相關資訊，請參閱[提交 Symantec Endpoint Protection 遙測資料以提高安全性](#)

事件計數

如果沒有感染狀況資料，則請使用事件計數。您必須等待合理的時間，才能取得足夠的資料。

事件計數是任何用戶端偵測到單一行為的次數。例如，一或多個用戶端可能已偵測到 Microsoft Word 在過去 30 天已啟動 cmd.exe 200 次。Microsoft Word 事件的事件計數可能各在 20 個用戶端上發生 10 次，或僅在 1 個用戶端上發生 200 次。

當您同時安裝或升級 14.3 RU10 管理伺服器 and 14.3 RU10 用戶端時，事件計數即開始。例如，如果您已在 2025 年 2 月升級至 SEPM 14.3 RU10，然後在 2025 年 3 月升級用戶端，則會在 3 月開始收集資料。您無法從 14.3 RU9 和更早版本的用戶端取得任何事件計數資料。您也必須增加用戶端上的風險記錄保留資料的天數。風險日誌預設會將資料保留 14 天。例如，在上例中，如果您在 2025 年 2 月 1 日和 2 月 28 日安裝用戶端，則事件計數會包括 2 月 14 日至 28 日的資料，而不是更早的資料。

若要增加保留風險日誌項目的天數，請參閱[指定日誌大小以及在資料庫中保留日誌項目的時間長度](#)。

行為規則

使用此標籤以允許和攔截應用程式行為，以及攔截潛在 Living Off the Land (LOTL) 攻擊。您可以允許您信任的行為，並攔截您不信任的行為。

設定	說明
快速調整	一次攔截清單中的所有零感染狀況項目。在您拒絕零感染狀況行為之後，除非清單中出現更多零感染狀況行為，否則「快速調整」按鈕會無法使用。
應用程式	列出用戶端電腦上執行的潛在應用程式。
行為	列出應用程式可能執行的行為。行為可能有風險，也可能沒有風險。 此表格將應用程式與行為組合在一起。例如，Microsoft Excel launching sc.exe 是安全行為，而 PowerShell launching Msbuild tools 可能不是安全行為。
普及率	顯示在某段時間內偵測到應用程式行為的用戶端電腦數目。 - 分析 Symantec Endpoint Protection Manager 已連線至雲端，但尚未收到熱圖資料。最後，行為規則會顯示感染狀況資料。 - 學習：自適應防護仍然從用戶端電腦收集資料。如果您第一次安裝管理伺服器，則從用戶端收集資訊最多需要 90 天。 - 未提供：Symantec Endpoint Protection Manager 因下列其中一個原因而未連線至雲端： - 已停用資料收集 (遙測)。 提交 Symantec Endpoint Protection 遙測資料以提高安全性 - 組織中的防火牆攔截遙測伺服器：https://ent-shasta-mr-clean.symantec.com - 輕度註冊未運作。相反地，您必須使用沒有感染狀況資料的自適應防護政策，或將管理伺服器從僅限內部部署管理轉換為混合管理。 感染狀況資料無法使用時，請使用「事件計數」欄來決定是否變更針對行為的動作。 - 零：感染狀況為零表示您的環境尚未偵測到應用程式行為。將行為設定為「拒絕」，即可放心地攔截這些應用程式行為。 - 低：極少的電腦偵測到此應用程式行為。 - 中：少數電腦偵測到此應用程式行為。 - 高：80% 的電腦偵測到此應用程式行為。 感染狀況期限是根據 Symantec Endpoint Protection Manager 網域期限。 Note: 在您升級至 14.3 RU10 之後，感染狀況期限一開始會顯示為 90 天。在 1 到 2 天之後，根據網域期限，感染狀況期限會恢復為「學習」、「90 天」、「180 天」或「365+ 天」。 調適型防護如何收集感染狀況和事件計數？
Mitre 技術	顯示指向 MITRE ATT&CK® 網站的連結，而此網站描述與應用程式行為相關聯的技術。MITRE ATT&CK 資料庫是描述可疑行為的業界標準。如需詳細資訊，請參閱 Enterprise 的 MITRE ATT&CK® 矩陣 。

設定	說明
動作	列出政策動作，而政策動作套用至與應用程式行為配對相符的任何行為活動。 - 允許：政策允許此應用程式行為。使用「允許」以停止記錄您信任之行為的事件。 - 監控：政策允許和記錄此應用程式行為。如果您還不確定要允許還是攔截，則請使用此動作。 - 拒絕：這個政策攔截和記錄此應用程式行為。 所有應用程式行為預設都會設定為「監控」。選取任何動作以變更設定。
事件	列出已在過去 30、60 或 90 天收集的應用程式行為事件。使用「事件」下拉式清單，以顯示自上次允許或攔截行為以來所出現的事件。 事件是根據下列準則： - 所有電腦上的事件：此行為規則在過去 N 天所觸發的事件總數，不論涉及的電腦數目有多少。例如，規則可能已在一部電腦上共觸發 100 個事件，或在兩部電腦上各觸發 50 個事件。此選項可能指出有較少數目的電腦大量使用行為規則。 - 不同電腦上的事件：過去 N 天出現此行為的電腦數目。例如，100 個事件的計數顯示有 100 部電腦出現該行為。
事件計數	顯示所有用戶端發現單一行為的次數。例如，假設 Microsoft Word launched cmd.exe 事件在過去 30 天發生 200 次。Microsoft Word 事件可能各在 20 個用戶端上發生 10 次，或僅在 1 個用戶端上發生 200 次。 只有在感染狀況資料無法使用時 (例如，您的環境處於暗網時)，才使用事件計數資料。此外，您必須等待足夠的時間，讓管理伺服器收集足夠的資訊。 基於下列原因，感染狀況期限不是 0 時，您可能會看到事件計數 0： - 事件計數是根據「事件」下拉式清單中的已過濾期間。如果感染狀況大於所出現的天數，則偶數計數為 0。 - 感染狀況是根據 SEPM 網域中任何用戶端電腦的遙測。如果提交遙測的用戶端已移至另一個網域或不再存在，則不會將這些用戶端計入事件計數。

自適應防護政策 - 進階設定

使用此標籤以設定調適型防護的預設記錄動作，以及針對用戶端使用者編寫自訂訊息。

設定	說明
在用戶端電腦上顯示通知訊息：	當自適應防護政策封鎖行為時，用戶端電腦上會顯示標準訊息。標準訊息的範例可能是： <pre>#####PowerShell</pre> 您可以在「行為規則」頁面上指定要封鎖的應用程式行為。 設為「拒絕」的行為越多，這些通知的顯示頻率就越高。如果將應用程式行為設為「允許」或「監控」，則不會顯示這些通知。
監控所有規則	不論「行為規則」頁面上所設定的動作為何，都將所有行為的動作設定為「監控」。暫時使用此選項以進行疑難排解。

從雲端而不是從 Symantec Endpoint Protection Manager 管理自適應防護

瞭解如何在 Symantec Endpoint Protection Manager (SEPM) (14.3 RU3 和更新版本) 中啟用自適應防護熱圖。

在 14.3 RU3 和更新版本中，您可以使用內部部署 Symantec Endpoint Protection Manager 來檢視 [自適應防護熱圖](#)。然後，您前往 Symantec Endpoint Security (SES) 雲端以管理自適應防護政策。

從 14.3 RU10 開始，您可以從 SEPM 完全管理自適應防護。

請參閱 [透過自適應防護攔截 Living Off the Land \(LOTL\) 攻擊](#)。

如需每個管理層級可取得哪些自適應防護功能的相關資訊，請參閱 [Symantec Endpoint Protection 與 Symantec Endpoint Security 之間的自適應防護功能比較](#)。

什麼是自適應防護？

若要瞭解自適應防護，請參閱：

[使用自適應防護](#)

[Symantec 自適應防護如何在安全性防禦中標記新章節](#)

視訊：[Symantec Endpoint Security Complete \(具備自適應防護\)](#)

自適應防護需求

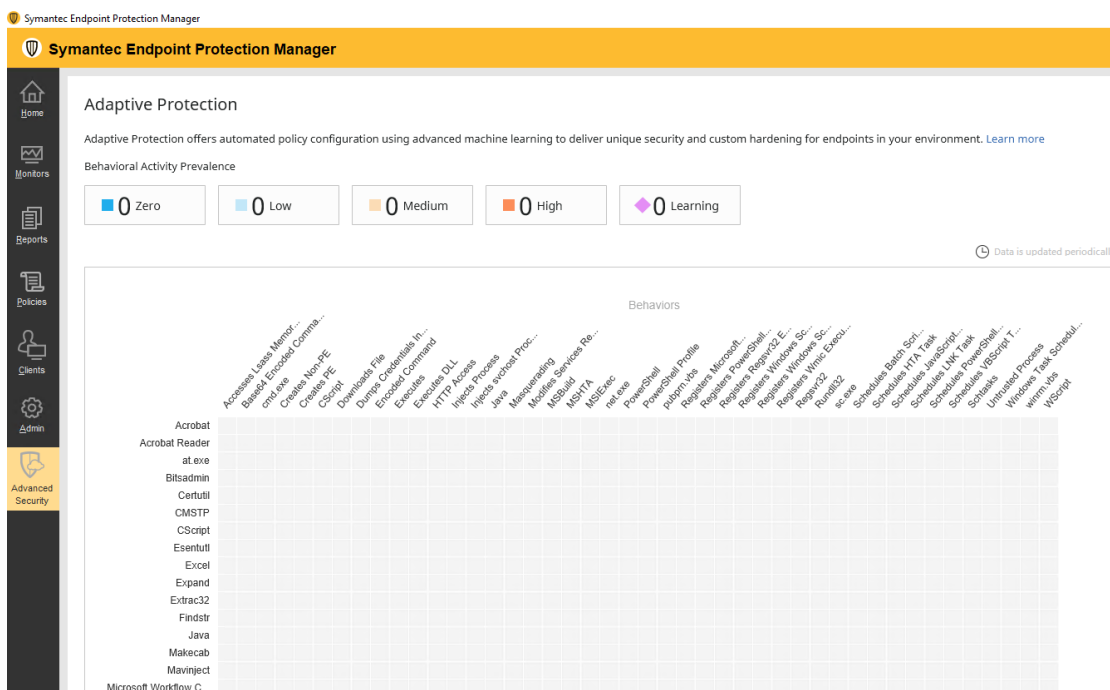
若要從雲端檢視或管理自適應防護，您必須具有：

- Symantec Endpoint Security Complete 授權。
若要檢視自適應防護熱圖或接收雲端分析通知，管理伺服器必須首先向雲端伺服器完成輕度註冊。
請參閱 [輕度註冊如何運作？](#)：
- 14.3 RU3 版或更新版本的 Windows 用戶端。
- 最新版本的 Symantec Endpoint Protection Manager。
- 為用戶端群組啟用遙測。
在 Symantec Endpoint Protection Manager 中，確定已啟用「將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報」選項。請參閱：
[管理用戶端傳送給賽門鐵克的匿名或非匿名資料](#)

若要[管理自適應防護](#)，您必須向 Symantec Endpoint Security 雲端伺服器[註冊](#)管理伺服器網域 (稱為混合管理)。

瞭解自適應防護熱圖

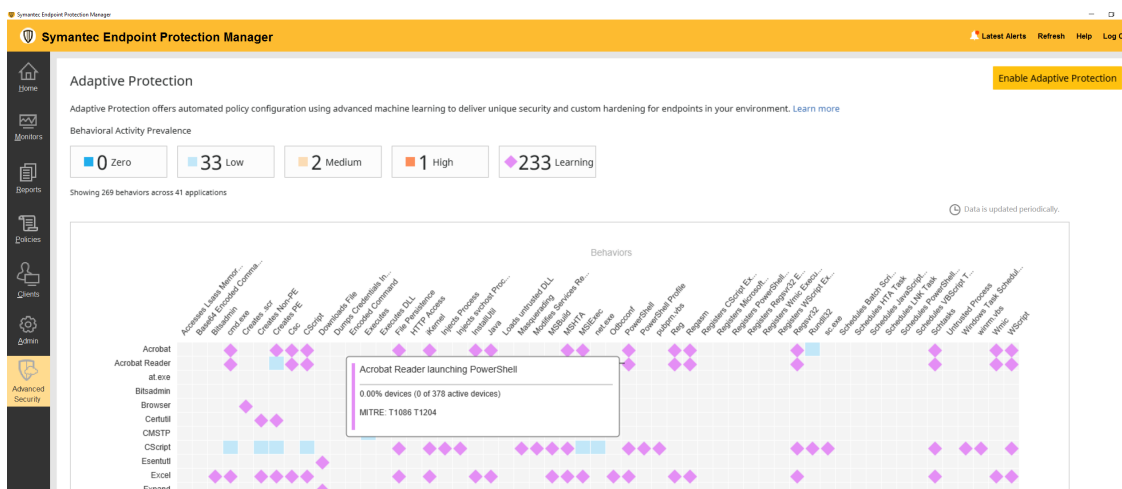
在啟用 Symantec Endpoint Security Complete 授權的 24 小時內，「進階安全性」頁面會取代「雲端」頁面。「自適應防護」頁面最多顯示 3 或 4 天的空熱圖，直到 Symantec 足夠瞭解您環境中的行為為止，而且 SEPM 會與雲端伺服器進行通訊。



NOTE

如果您具有 Symantec Endpoint Security Enterprise 訂閱，則會持續看到「雲端」頁面。

「自適應防護」頁面顯示熱圖 Widget，而此 Widget 使用色彩編碼來顯示您環境中受信任應用程式行為的感染狀況。熱圖資料收集自使用特定自適應防護政策的所有裝置。熱圖中的資料根據過去 90 天從裝置收集到的遙測。



熱圖中的下列圖示顯示應用程式行為配對的感染狀況。

- 零感染狀況
此應用程式行為不盛行。裝置未受到政策動作變更的影響。
- 低感染狀況
此應用程式行為不盛行。少數裝置受到政策動作變更的影響。
- 中感染狀況
此應用程式行為比較盛行。部分裝置受到政策動作變更的影響。
- 高感染狀況
此應用程式行為非常盛行。如果您變更此應用程式行為的政策動作，則最多會影響 80% 的裝置。
- 探索
自適應防護仍在瞭解此應用程式行為，沒有足夠的目前資料來指派感染狀況值。如果有最多 5% 的裝置是新的，則也可能發生此情況。例如，您的組織可能會頻繁地將筆記型電腦取代為新影像。自適應防護會在觀察應用程式行為 90 天之後指派感染狀況。

一開始，所有應用程式行為都設定為動作為「監控」的「探索」。

在雲端中管理自適應防護政策

如果您想要調整您環境的自適應防護，則必須將管理從僅內部部署管理切換到混合管理。混合管理可讓您從內部部署 Symantec Endpoint Protection Manager 或 SES 雲端主控台管理用戶端。不過，您可以從雲端主控台而非 Symantec Endpoint Protection Manager 來管理自適應防護政策。對於混合管理，請在雲端伺服器中註冊 Symantec Endpoint Protection Manager 網域。

步驟	說明
步驟 1：在雲端伺服器中註冊 Symantec Endpoint Protection Manager 網域。	• 針對 14.3 RU3 和更新版本以及具有 Symantec Endpoint Security Complete 授權： 以雲端伺服器 (14.3 RU3 或更新版本) 註冊 Symantec Endpoint Protection Manager • 對於 14.3 RU2 和更舊版本或具有 Symantec Endpoint Security Enterprise 授權，登入 Symantec Security Cloud、取得記號，並將記號貼入 Symantec Endpoint Protection Manager。 請參閱：向雲端伺服器註冊 Symantec Endpoint Protection Manager 網域

步驟 2：在雲端主控台中，建立自適應防護政策。	在 Symantec Endpoint Security 雲端主控台中，建立自適應防護政策，並將政策套用到 Symantec Endpoint Protection Manager 受管裝置。 如需如何在雲端主控台中使用自適應防護功能的詳細資訊，請參閱： 使用自適應防護

NOTE

如果您從雲端主控台中管理自適應防護，但不想要重新整理 Symantec Endpoint Protection Manager 中的應用程式行為熱圖，則請前往「設定」，並關閉「自適應防護」。

檢視 Symantec Endpoint Protection Manager 上的雲端分析資安事端 (14.3 RU8 和更新版本)

Symantec Endpoint Protection 可使用雲端式雲端分析服務收集的資料，增強您的資安事端偵測。

什麼是雲端分析？

雲端分析提供滲透後違規偵測功能。這些功能可協助您搜尋目前在環境中發生的複雜、有針對性和人為驅動的攻擊，並採取行動。雲端分析著重於搜尋其他部署安全產品可能會遺漏的攻擊。

雲端分析服務結合 Symantec Threat Hunter 團隊的研究，在他們攻擊您的環境之前，發現已知和未知攻擊。分析不斷發展以跟上新的攻擊模式。賽門鐵克在程序和檔案層級分析來自已知遭到入侵電腦的資料，並評估在入侵和網路活動時使用的標準工具。此遙測會饋送到學習模型中，以訓練鎖定攻擊的行為方式。當賽門鐵克發現類似的可疑行為時，會將資安事端直接傳送到 Symantec Endpoint Protection Manager。通知會顯示對攻擊者、技術、受影響電腦的詳細分析以及矯正指南。

雲端分析是與 Symantec EDR 提供的鎖定攻擊分析相同的技術。

NOTE

雲端分析是自適應防護的一部分。

檢視雲端分析通知

當雲端分析服務偵測到資安事端時，該資安事端會透過 Symantec Endpoint Security 雲端伺服器傳遞，並在 Symantec Endpoint Protection Manager 中的資安事端顯示事件的通知。

請參閱：[瞭解資安事端、事件和實體](#)

雲端分析服務會根據新資訊持續重新評估以前可能看過的事件。雲端可以判定以前可疑的活動不再可疑。例如，您可能會看到以下事件：### - ##### DGA ##。

您可能會看到每個資安事端平均有 10-15 個事件。管理伺服器通常不會顯示 Symantec Endpoint Protection 用戶端攔截之行為的事件。

若要接收這些通知，您必須遵循與[自適應防護熱圖](#)相同的需求。使用 Symantec Endpoint Security Complete 授權登入 Symantec Endpoint Protection Manager 之後，將會開始[輕度註冊](#)。輕度註冊最多可能需要 24 小時。Symantec Endpoint Protection Manager 接著會顯示雲端分析服務偵測到的資安事端。

NOTE

您不需要向雲端伺服器完全註冊 Symantec Endpoint Protection Manager。

檢視雲端分析事件

1. 在主控台中，按兩下「監控」頁面 > 「通知」。
2. 在「通知」標籤上，按一下「進階設定」，然後按一下「通知名稱」下拉式清單。
3. 在「選取通知名稱」對話方塊中，選取「雲端分析違規偵測」，然後按一下「確定」。

Symantec Endpoint Protection Manager

Latest Alerts Refresh Help Log Off

Summary Logs Command Status Notifications

Notifications

Tell me more... Auto-refresh: Every 30 seconds

Last updated: 08/08/2023 08:38:45

Notification Conditions

Acknowledge all notifications in this filtered list

Details

Ack	Report	Time	Created By	Subject	Message
		08/07/2023 22:34:05	admin	LOW: TAA EICAR	Targeted Attack Analytics test
		08/07/2023 21:40:08	admin	HIGH: Suspected Breach	BITS Jobs; PowerShell; Security Account Manager
		08/07/2023 21:37:05	admin	MEDIUM: DGA Beacons	Domain Generation Algorithm usage detected
		08/07/2023 21:37:05	admin	Updated - Not Suspicious: DGA Beacons	Symantec has determined that this incident is not suspicious activity.
		08/07/2023 21:34:32	admin	Updated - Not Suspicious: TAA EICAR 2	Symantec has determined that this incident is not suspicious activity.
		08/07/2023 21:34:32	admin	LOW: TAA EICAR 2	Suspicious Behavior adversary: DemoActor; Credential Dumping (SAM); Data Compressed

檢視雲端分析傳送

您可以檢視 Symantec Endpoint Protection Manager 傳送給賽門鐵克安全機制應變中心團隊進行檢閱的資安事端。此外，您可以使用該報告來調查特定用戶端電腦的活動。您不需架構用戶端對事件採取的動作。

1. 在主控台中，按一下「監控」>「日誌」。
2. 在「日誌」標籤上，選取「系統」日誌類型，然後按一下「用戶端活動」。
3. 按下「檢視日誌」。

關閉雲端分析通知

如果您不想檢視雲端分析的通知，您可以從 Symantec Endpoint Protection Manager > 「監視器」> 「通知」標籤關閉通知。

NOTE

Symantec 建議您開啟雲端分析資料重新整理功能。

停用雲端分析通知

- 停止所有 Symantec Endpoint Protection Manager 服務：
 - Symantec Endpoint Protection Manager
 - Symantec Endpoint Protection Manager API ##
 - Symantec Endpoint Protection Manager Webserver
- 停止及啟動管理伺服器服務
- 停止和啟動 Apache Web 伺服器
- 前往：<SEPM_Install>tomcat\etc

其中 *SEPM_Install* 表示 Symantec Endpoint Protection Manager 的安裝資料夾。

- 請開啟 `conf.properties` 檔案，在最後新增以下新行，然後儲存檔案：`scm.targeted.attack.analytics.feature.enabled=false`
- 重新啟動所有 Symantec Endpoint Protection Manager 服務。

重新整理雲端分析資料

根據預設，Symantec Endpoint Protection Manager 每 24 到 48 小時會重新整理雲端分析資料。如果您的環境頻寬較低，則可能需要停用重新整理資料的功能。只有在您向雲端伺服器[完全註冊](#) Symantec Endpoint Protection Manager 時，才能啟用或停用此選項。

啟用或停用雲端分析資料重新整理

- 在 Symantec Endpoint Protection Manager 中，移至「進階安全性」>「設定」，然後關閉「啟用雲端分析」。

管理防火牆防護

防火牆允許您在防火牆政策中指定的進出網路流量。Symantec Endpoint Protection 防火牆政策包含規則與防護設定，大部分可由您啟用或停用，以及架構。

Table 58: 管理防火牆防護的選擇性工作

工作	說明
讀取防火牆防護的相關資訊	在架構防火牆防護之前，您應當先熟悉一下防火牆。請參閱： • 防火牆的運作方式 • 關於 Symantec Endpoint Protection 防火牆
修改現有預設防火牆政策或建立新政策	您可以修改預設政策，也可以建立新政策。請參閱： 建立防火牆政策
建立及自訂防火牆規則	防火牆規則是控制防火牆保護用戶端電腦免受惡意攻擊的方式的政策元件。預設防火牆政策包含預設防火牆規則。建立新政策後，Symantec Endpoint Protection 將提供預設防火牆規則。但是，您可以修改預設規則，也可以建立新規則。請參閱： • 新增防火牆規則 • 自訂防火牆規則
啟用防火牆防護設定	在防火牆完成特定作業後，控制權就會移交給數個元件。每個元件都是設計來執行不同類型的封包分析。請參閱： • 為網路服務啟用通訊而非新增規則 • 自動攔截連線至攻擊電腦 • 防止對電腦的外部隱藏攻擊 • 停用 Windows 防火牆 • 透過架構點對點驗證攔截遠端電腦
監控防火牆防護	定期監控電腦上的防火牆防護狀態。請參閱： 監控 Symantec Endpoint Protection 用戶端

更多資訊

- [在用戶端電腦上從主控台執行指令](#)
- [架構混合控制的防火牆設定](#)

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。

關於 Symantec Endpoint Protection 防火牆

Symantec Endpoint Protection 防火牆會使用防火牆政策和規則來允許或攔截網路流量。Symantec Endpoint Protection 包含預設的防火牆政策，提供辦公室環境所需的預設防火牆規則和防火牆設定。辦公室環境通常受到企業防火牆、邊界封包篩選器或防毒伺服器的保護。因此辦公室環境比起使用有限邊界保護的大多數家用環境，通常要更安全。

防火牆規則可控制用戶端如何保護用戶端電腦，不受惡意入埠流量及惡意離埠流量的攻擊。防火牆自動根據這些規則檢查所有入埠及離埠的封包。然後，防火牆根據規則中指定的資訊允許或攔截封包。當一台電腦嘗試與另一台電腦連線時，防火牆會將連線類型與其防火牆規則清單進行比較。防火牆也會對所有網路流量使用狀態式檢測。

當您首次安裝主控台時，它會自動將預設防火牆政策加入每個群組。

每當您新增位置時，主控台會自動將防火牆政策複製到預設位置。

您可以決定使用者與用戶端互動的程度，即允許或禁止其架構防火牆規則和防火牆設定。只有在用戶端將新的網路連線和可能的問題通知使用者時，使用者才能與用戶端互動。您也可以為他們授予對使用者介面的完全存取權。

您可以使用預設防火牆設定安裝用戶端。在大多數情況下，您無須變更設定。不過，如果您對網路有深入的瞭解，可以對用戶端防火牆做許多變更，自行調整用戶端電腦的防護功能。

自 14.2 版起，Mac 用戶端僅提供適用於受管用戶端的防火牆。僅當管理員已允許用戶端控制時，使用者才能啟用或停用防火牆。由於它會在不同於 Mac 作業系統防火牆的網路層運作，因此可以同時啟用和並行執行。

更多資訊

- [關於 Mac 用戶端的防火牆設定](#)
- [管理防火牆防護](#)
- [防火牆的運作方式](#)
- [防火牆如何使用狀態式檢測](#)
- [安全政策類型](#)

建立防火牆政策

Symantec Endpoint Protection 包含預設的防火牆政策，提供辦公室環境所需的預設防火牆規則和預設防火牆設定。辦公室環境通常受到企業防火牆、邊界封包篩選器或防毒伺服器的保護。因此辦公室環境比起使用有限邊界保護的大多數家用環境，通常要更安全。

當您首次安裝主控台時，它會自動將預設防火牆政策加入每個群組。

NOTE

變更預設防火牆政策的名稱可能會導致升級未更新政策。這一點同樣適用於預設防火牆政策中的預設規則。

每當您新增位置時，主控台會自動將防火牆政策複製到預設位置。如果預設的防護並不適合，您可以自訂每個位置的防火牆政策，例如主站台或客戶站台。如果您不想使用預設防火牆政策，可以進行編輯或以其他共用政策加以取代。

下表說明可執行以架構新防火牆政策的工作。您首先必須增加防火牆政策，但之後其餘的工作是選擇性的，您可以按任何順序完成這些工作。

Table 59: 如何建立防火牆政策

工作	說明
新增防火牆規則	防火牆規則是政策元件，會控制防火牆防護用戶端電腦不受惡意連入流量和應用程式侵襲的方式。防火牆會自動根據這些規則檢查所有連入封包及連出封包。防火牆會根據規則中指定的資訊允許或攔截封包。您可以修改預設規則、建立新的規則或停用預設規則。 建立新的防火牆政策時，Symantec Endpoint Protection 會提供預設啟用的預設防火牆規則。 如需詳細資訊，請參閱： 新增防火牆規則
啟用和自訂告知使用者所存取的應用程式已受到攔截的通知	您可以向使用者傳送已攔截其要存取的應用程式的通知。 依預設會停用這些設定。 如需詳細資訊，請參閱： 通知使用者已攔截存取應用程式
啟用自動防火牆規則	您可以啟用自動允許特定網路服務之間進行通訊的選項。使用這些選項，就不需建立明確允許這些服務的規則。您也可以啟用流量設定，偵測和攔截透過 NetBIOS 與 Token Ring 進行通訊的流量。 依預設，只會啟用流量通訊協定。 如需詳細資訊，請參閱： 為網路服務啟用通訊而非新增規則 如果 Symantec Endpoint Protection 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。用戶端會啟動主動回應，此功能會自動攔截特定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。 此選項預設為停用。 如需詳細資訊，請參閱： 自動攔截連線至攻擊電腦
架構防護和隱藏設定	您可啟用設定，偵測並記錄可能在用戶端上進行的攻擊，並攔截詐騙行動。您可啟用防止外部攻擊偵測用戶端相關資訊的設定。 如需詳細資訊，請參閱： 防止對電腦的外部隱藏攻擊 依預設會停用所有防護選項和隱藏選項。
將 Symantec Endpoint Protection 防火牆與 Windows 防火牆整合	您可以指定 Symantec Endpoint Protection 停用 Windows 防火牆的條件。解除安裝 Symantec Endpoint Protection 後，Symantec Endpoint Protection 會將 Windows 防火牆設定還原為安裝 Symantec Endpoint Protection 之前的狀態。 預設設定為僅停用 Windows 防火牆一次，並停用 Windows 防火牆停用訊息。 如需詳細資訊，請參閱： 停用 Windows 防火牆
架構點對點驗證	您可以使用點對點驗證，允許遠端用戶端電腦 (對等者) 連線至同一企業網路內的其他用戶端電腦 (驗證者)。驗證者會暫時攔截遠端電腦的入埠 TCP 和 UDP 流量，直到遠端電腦通過主機完整性檢查。 此選項預設為停用。 如需詳細資訊，請參閱： 透過架構點對點驗證攔截遠端電腦

啟用防火牆防護時，政策會允許所有入埠 IP 網路流量和所有離埠 IP 網路流量，但以下情況例外：

- 預設的防火牆防護會攔截與所有遠端系統的入埠與離埠 IPv6 流量。

NOTE

IPv6 是用於網際網路的網路層通訊協定。如果您在執行 Microsoft Vista 的電腦上安裝用戶端，則「規則」清單會包含攔截 IPv6 乙太網路通訊協定類型的數種預設規則。如果移除這些預設規則，就必須建立攔截 IPv6 的規則。

- 預設的防火牆防護會限制一些經常用於進行攻擊之通訊協定 (例如 Windows 檔案共用) 的入埠連線。允許內部網路連線，但會攔截外部網路。

管理防火牆防護

針對遠端用戶端之防火牆政策設定的最佳實務準則

從 Symantec Endpoint Protection Manager 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。

Symantec Endpoint Protection 會與包含預設規則的預設防火牆政策一併安裝。建立新的防火牆政策時，Symantec Endpoint Protection 會提供預設防火牆規則。如果您的管理員允許，或者您的用戶端未受管理，則可以修改任何預設規則，或建立新的防火牆規則。

政策中必須至少有一個規則。不過，您可以視需要使用任意數量的規則。您可以視需要啟用或停用規則。例如，您可能需要停用某個規則以執行疑難排解，並在完成後再次啟用該規則。

下表說明管理防火牆規則所需瞭解的相關內容。

Table 60: 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。 請查閱：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。 當您瞭解這些觸發條件以及如何能充分加以善用後，就可以自訂防火牆規則來保護您的用戶端和伺服器。
新增防火牆規則	您可以執行下列工作來管理防火牆規則： - 使用幾種方法，透過主控台新增防火牆規則。 有一種方法可讓您增加具有預設設定的空白規則。另一種方法則會提供精靈，在建立新規則的過程中給您指導。 - 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。 - 複製並貼上防火牆規則。 您可以複製與要建立之規則類似的現有規則，以節省建立新防火牆規則的時間。然後，您可以修改複製的規則以配合您的需要。
自訂防火牆規則	建立新規則後 (或者，如果您要自訂預設規則)，您可以修改任何防火牆規則條件。

新增防火牆規則

您可以使用下列任一種方法建立新的防火牆規則：

空白的規則	空白規則會允許所有流量。請參閱： 新增新的空白防火牆規則
「新增防火牆規則」精靈	如果您使用「新增防火牆規則」精靈新增規則，請務必架構該規則。此精靈不會架構具有多個準則的新規則。請參閱： 使用精靈新增防火牆規則

您應該盡可能在規則中同時指定入埠和離埠流量。您無須建立 HTTP 等流量的入埠規則。Symantec Endpoint Protection 用戶端會針對 TCP 流量使用狀態式檢測。因此，不需要規則來篩選用戶端啟始的傳回流量。

當您建立新的防火牆規則時，它會自動啟用。如果您要允許存取特定的電腦或應用程式，可以停用某項防火牆規則。所有繼承政策都會停用該規則。

若為共用政策，則所有位置也都會停用該規則；若為位置特定政策，則只有一個位置會停用該規則。

NOTE

規則必須啟用，防火牆才能處理這些規則。

新增新的空白防火牆規則

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
3. 在「規則」標籤的「規則」清單下，按下「新增空白規則」。
4. 或者，您也可以視需要變更防火牆規則準則。
5. 架構完此規則後，請按一下「確定」。

使用精靈新增防火牆規則

1. 在主控台中，開啟某個防火牆政策。
 2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
 3. 在每個畫面上填寫選項，然後按「下一步」。
 4. 按下「完成」。
- 或者，您也可以視需要變更防火牆規則準則。

更多資訊

- [自訂防火牆規則](#)
- [防火牆如何使用狀態式檢測](#)

關於防火牆伺服器規則和用戶端規則

規則可分為伺服器規則或用戶端規則。伺服器規則是您在 Symantec Endpoint Protection Manager 建立並下載至 Symantec Endpoint Protection 用戶端的規則。用戶端規則是使用者在用戶端上建立的規則。

Mac 用戶端上的所有規則都是伺服器規則。Mac 使用者沒有為 Mac 用戶端建立用戶端規則的選項。

自 14.2 版起，Mac 用戶端引入防火牆。

下表說明以下兩者之間的關係：用戶端的使用者控制等級和使用者與防火牆規則的互動。

Table 61: 使用者控制等級和規則狀態

使用者控制等級	使用者互動
伺服器控制	Windows 用戶端接收到伺服器規則，但使用者無法檢視這些規則。使用者無法建立用戶端規則。 Mac 用戶端不允許使用者啟用或停用防火牆。
混合控制	Windows 用戶端接收到伺服器規則。使用者可以建立用戶端規則，這些規則會與伺服器規則以及用戶端安全設定合併。 Mac 用戶端允許或不允許使用者啟用或停用防火牆。此取決於精細設定設定為伺服器控制或用戶端控制。
用戶端控制	用戶端不接收伺服器規則。使用者可以建立用戶端規則。Symantec Endpoint Protection Manager 管理員無法檢視用戶端規則。 Mac 用戶端允許使用者啟用或停用防火牆。

如需詳細資訊，請參閱：

[防止使用者在用戶端電腦上停用防護](#)

下表列出防火牆對伺服器規則、用戶端規則和用戶端設定的處理順序。

Table 62: 伺服器規則和用戶端規則的處理優先順序

優先順序	規則類型或設定
第一	高優先順序的伺服器規則 ([規則] 清單中藍線以上的規則)
秒	用戶端規則
第三	低優先順序的伺服器規則 ([規則] 清單中藍線以下的規則) 在用戶端，藍線以下的伺服器規則會在用戶端規則之後處理。
第四	用戶端安全設定
第五	用戶端應用程式專用的設定

在用戶端，使用者可以修改用戶端規則或安全設定，但使用者無法修改伺服器規則。

WARNING

如果用戶端為混合控制，使用者可以建立允許所有流量的用戶端規則。此規則會覆寫藍線以下所有的伺服器規則。

更多資訊

- [管理防火牆規則](#)
- [變更防火牆規則的順序](#)
- [防止使用者在用戶端電腦上停用防護](#)

防火牆處理防火牆規則和設定的順序

防火牆規則會在規則清單中，從最高到最低優先順序，依序排列。如果第一項規則未指定如何處理封包，防火牆就會檢查第二項規則。

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。

下表顯示了對防火牆規則進行排序的最佳做法。

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。

在 Symantec Endpoint Protection Manager 中，規則清單中有條藍色分隔線。在下列情況中，分隔線會設定各項規則的優先順序：

- 子群組繼承父群組的規則。
- Windows 用戶端設定為混合控制。防火牆同時處理伺服器規則和用戶端規則。

下表顯示防火牆對規則、防火牆設定和入侵預防設定的處理順序。

Table 63: 處理順序

優先順序	設定
1	自訂 IPS 特徵
2	IPS 設定和防護以及隱藏設定，通訊埠掃描除外
3	內建規則
4	防火牆規則
5	通訊埠掃描檢查
6	透過 LiveUpdate 下載的 IPS 特徵

變更防火牆規則的順序

防火牆會由上而下處理防火牆規則清單。您可以變更防火牆規則的順序，以決定防火牆處理防火牆規則的方式。

如果 Symantec Endpoint Protection 用戶端使用位置切換，則當您變更防火牆規則順序時，該變更只會影響目前位置的順序。

NOTE

為加強防護效果，請將最嚴格的規則放在最前面，最寬鬆的規則放在最後面。

如需詳細資訊，請參閱：

[關於防火牆規則、防火牆設定和入侵預防處理順序](#)

變更管理伺服器中的防火牆規則順序

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面上，按下「規則」，再選取要移動的規則。
3. 執行下列其中一項工作：
 - 若要將所選規則調整到上一則規則之前處理，請按下「上移」。
 - 若要將所選規則調整到下一則規則之後處理，請按下「下移」。
4. 按一下「確定」。

變更用戶端中的防火牆規則順序

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，選取您要移動的規則。
- 4. 執行下列其中一項動作：
 - 若要讓防火牆處理上一則規則之前處理此規則，請按向上箭頭。
 - 若要讓防火牆處理下一則規則之後處理此規則，請按向下箭頭。
- 5. 當您移動規則完畢時，按下「確定」。

更多資訊

管理防火牆規則

關於繼承的防火牆規則

子群組的政策可以僅繼承父群組中啟用的防火牆規則。當您已繼承規則時，可以停用這些規則，但無法加以修改。當新規則新增至父群組的政策時，新規則會自動新增至繼承政策。

繼承的規則顯示在「規則」清單中時，會加上斜體陰影。在藍字那行上面，繼承的規則會新增到您以 Symantec Endpoint Protection Manager 管理員身分所建立的規則上面。在藍字那行下面，繼承的規則會新增到您所建立的規則下面。

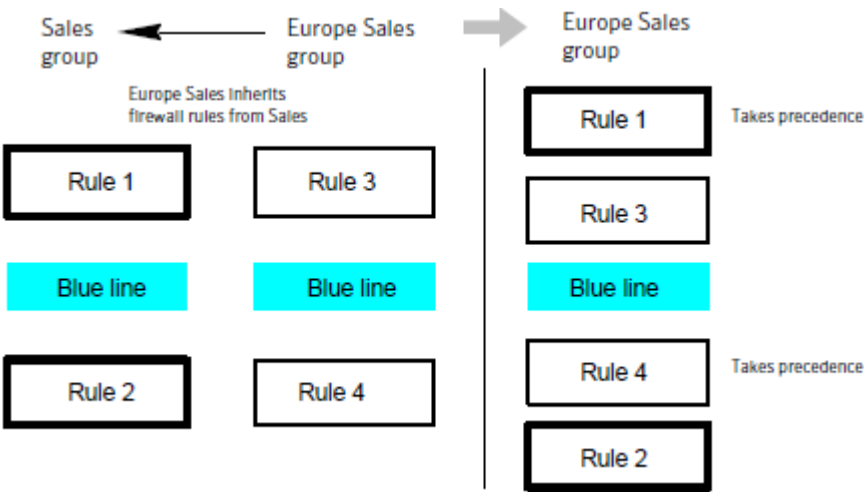
防火牆政策也會繼承預設規則，因此子群組的防火牆政策可能有兩組的預設規則。您可能會想要刪除其中一組預設規則。

若要移除繼承的規則，請移除繼承，而不是刪除這些規則。您必須移除所有繼承的規則，而不是選取的規則。

防火牆處理「規則」清單中繼承的防火牆規則，其方式如下：

在藍色分隔線之上	政策繼承的規則優先順序高於您建立的規則。
在藍色分隔線之下	您建立的規則優先順序高於政策繼承的規則。

下圖顯示當子群組從父群組繼承規則時，「規則」清單如何排列規則順序。此例中，「銷售」群組是父群組。「歐洲銷售」群組從「銷售」群組繼承。



更多資訊

- [管理防火牆規則](#)
- [新增繼承自父群組的防火牆規則](#)

新增繼承自父群組的防火牆規則

您可以藉由從父群組繼承規則，將防火牆規則新增至防火牆政策。若要從父群組繼承規則，子群組的政策必須不是共用政策。

NOTE

如果群組的所有政策都繼承自父群組，則無法使用此選項。

新增繼承自父群組的防火牆規則

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
在 14.2 之前版本中，沒有「**Mac** 設定」的選項。
3. 在 [規則] 標籤上，勾選 [從父群組繼承防火牆規則]。
若要移除繼承的規則，請取消勾選 [從父群組繼承防火牆規則]。
4. 按下「確定」。

更多資訊

- [編輯政策](#)
- [關於繼承的防火牆規則](#)
- [管理防火牆規則](#)

防火牆如何使用狀態式檢測

防火牆防護會使用狀態式檢測追蹤目前連線。狀態式檢測可追蹤來源及目的 IP 位址、通訊埠、應用程式以及其他連線資訊。用戶端檢查防火牆規則之前，會先根據連線資訊決定流量。

例如，如果防火牆規則允許電腦連線至 Web 伺服器，防火牆便會記錄連線資訊。當伺服器回覆時，防火牆預測會產生從 Web 伺服器到電腦的回應。便會允許 Web 伺服器流量傳送到發起流量的電腦，而不會檢查規則資料庫。在防火牆將連線記錄之前，規則必須允許最初的離埠流量。

使用狀態式檢測就不必再建立新規則。對於單向起始的流量，您無須建立允許雙向流量的規則。單向起始的用戶端流量包括 Telnet (通訊埠 23)、HTTP (通訊埠 80) 及 HTTPS (通訊埠 443)。用戶端電腦會發起此離埠流量，您可以為這些通訊協定建立允許離埠流量的規則。狀態式檢測會自動允許回應出埠流量的傳回流量。由於防火牆在本質上是狀態式的，因此您只需建立起始連線的規則，無需建立特定封包的特性。所有屬於允許連線的封包隱含允許作為同一連線不可缺少的部分。

狀態式檢測支援指引 TCP 流量的所有規則。

狀態式檢測不支援篩選 ICMP 流量的規則。對於 ICMP 流量，您必須建立允許雙向流量的規則。例如，若要讓用戶端使用 Ping 指令並接收回覆，您必須建立允許雙向 ICMP 流量的規則。

您可以定期清除維護連線資訊的狀態表。例如，當防火牆政策更新已處理或 Symantec Endpoint Protection 服務已重新啟動時，便會清除它。

關於防火牆規則應用程式觸發條件

如果應用程式是您在允許流量的規則中定義的唯一觸發條件，則防火牆會允許該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。

以應用程式為基礎的規則可能不太容易進行疑難排解，因為應用程式可能使用有多種通訊協定。例如，如果防火牆先處理允許 Internet Explorer 的規則，再處理攔截 FTP 的規則，使用者仍可以與 FTP 通訊。使用者可以在瀏覽器輸入使用 FTP 的 URL，例如 ftp://ftp.symantec.com。

例如，假設您允許 Internet Explorer，而且未定義其他任何觸發條件。則電腦使用者可以存取使用 HTTP、HTTPS、FTP、Gopher，以及網頁瀏覽器所支援之其他通訊協定的遠端站台。您可以定義其他觸發條件，描述允許進行通訊的網路通訊協定和主機。

請不要使用應用程式規則來控制網路層級的流量。例如，如果使用者使用其他網頁瀏覽器，攔截或限制使用 Internet Explorer 的規則就沒有作用。其他網頁瀏覽器所產生的流量還是會與 Internet Explorer 規則以外的所有其他規則比對。規則架構為攔截傳送和接收流量的應用程式時，以應用程式為基礎的規則才比較適用。

更多資訊

- [定義應用程式的相關資訊](#)
- [通知使用者已攔截存取應用程式](#)
- [管理防火牆規則](#)
- [攔截可能受到攻擊的網路應用程式](#)

定義應用程式的相關資訊

您可以定義用戶端執行的應用程式的相關資訊，並將此資訊加入到防火牆規則中。

您可以使用下列方式定義應用程式：

- 手動輸入資訊。請參閱：
[手動定義應用程式的相關資訊](#)
- 在探索到的應用程式清單中搜尋應用程式。
探索到的應用程式清單中的應用程式是您網路中用戶端電腦執行的應用程式。請參閱：
[從探索到的應用程式清單搜尋應用程式](#)

手動定義應用程式的相關資訊

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」下方，按下「規則」。
在 14.2 之前版本中，在「防火牆政策」頁面上，按下「規則」。
3. 在「規則」標籤的「規則」清單中，用滑鼠右鍵按下要變更規則的「應用程式」欄位，再按下「編輯」。
4. 在「應用程式清單」對話方塊中，按下「新增」。
5. 在「新增應用程式」對話方塊中，輸入下列一或多個欄位：
 - 檔案名稱，可包含檔案路徑
 - 檔案敘述
此欄位僅作為顯示之用。無法作為比對條件使用。
 - 檔案大小 (位元組)
 - 應用程式上次變更的日期
 - 檔案指紋

NOTE

必須啟用「網路應用程式監控」才能依檔案大小、上次修改日期或檔案指紋定義防火牆規則。如果停用「網路應用程式監控」，規則處理會忽略「檔案名稱」以外的所有欄位。

6. 按下「確定」新增應用程式條件。
7. 按下「確定」儲存應用程式清單。

從探索到的應用程式清單搜尋應用程式

1. 在「防火牆政策」頁面上，按下「規則」。
2. 在「規則」標籤選取規則，用滑鼠右鍵按下「應用程式」欄位，再按下「編輯」。
3. 在「應用程式清單」對話方塊中，按下「新增自」。

-
- 在「搜尋應用程式」對話方塊中搜尋應用程式。
 - 在「查詢結果」表下，若要新增應用程式到「應用程式」清單，請選取應用程式，按下「新增」，再按下「確定」。
 - 按下「關閉」。
 - 按下「確定」。

更多資訊

- [管理防火牆規則](#)
- [編輯政策](#)
- [關於防火牆規則應用程式觸發條件](#)

攔截可能受到攻擊的網路應用程式

網路應用程式監控會將應用程式的行為記錄在安全日誌中。如果應用程式的內容修改太過頻繁，應用程式可能是受到特洛伊木馬程式攻擊，用戶端電腦就處於不安全的狀態。如果應用程式的內容修改並非經常性，則可能已安裝修正程式，而用戶端電腦處於安全狀態。您可以使用這些資訊建立防火牆規則來允許或攔截應用程式。

您可以架構用戶端偵測和監控用戶端電腦上執行的任何網路應用程式。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。

如果您懷疑應用程式受到了特洛伊木馬程式攻擊，可以使用網路應用程式監控架構用戶端攔截應用程式。您也可以架構用戶端詢問使用者是允許還是攔截應用程式。

應用程式內容變更的原因如下：

- 應用程式受到特洛伊木馬程式攻擊。
- 應用程式已更新為新版本或使用更新程式進行了更新。

您可以將應用程式新增到清單，設定用戶端不監控它們。您可以將認為不會受到特洛伊木馬程式攻擊，但經常會有自動修正程式更新的應用程式排除在監控之外。

您也可以將詢問使用者允許或攔截網路應用程式的通知數減至最少。

攔截可能受到攻擊的網路應用程式

- 在主控台中，按一下「用戶端」。
- 在「用戶端」下方選取群組後，再按下「政策」。
- 在「政策」標籤的「與位置無關的政策與設定」下方，按下「網路應用程式監控」。
- 在「用於 群組名稱 的網路應用程式監控」對話方塊中，按一下「啟用網路應用程式監控」。
- 在「偵測到應用程式變更時」下拉式清單中，選取防火牆要對用戶端上執行的應用程式採取的動作：

詢問	詢問使用者是允許還是攔截應用程式。
攔截流量	攔截應用程式使其無法執行。
允許並記錄日誌	允許應用程式執行，並將資訊記錄在安全日誌中。 防火牆只會對修改過的應用程式採取此動作。

6. 如果選取「詢問」，請按下「其他文字」。
7. 在「其他文字」對話方塊中，鍵入要出現在標準訊息下方的文字，再按下「確定」。
8. 若要將應用程式排除在監控之外，請在「未受監控的應用程式清單」下方，執行下列其中一個工作：

手動定義應用程式	按下「新增」、填寫一個或多個欄位，然後按下「確定」。
從已知的應用程式清單定義應用程式	按下「新增自」。 探索到的應用程式清單會監控網路和非網路應用程式。您只能從探索到的應用程式清單選取網路應用程式。將應用程式加入到「未受監控的應用程式清單」之後，您可以啟用、停用、編輯或刪除它們。

9. 勾選應用程式旁邊的方塊可以啟用應用程式；取消選中此方塊可停用應用程式。
10. 按下「確定」。

更多資訊

- [管理防火牆規則](#)
- [通知使用者已攔截存取應用程式](#)
- [啟用應用程式探索](#)

通知使用者已攔截存取應用程式

您可以向使用者傳送已攔截其要存取的應用程式的通知。此通知會顯示在使用者電腦上。

NOTE

啟用太多通知不僅會使使用者感到不知所措，還會向這些使用者傳送警示。啟用通知時請務必小心。

通知使用者已攔截存取應用程式

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面上，按下「規則」。
3. 在「通知」標籤上，勾選「用戶端攔截應用程式時在電腦上顯示通知」，並選擇性地新增自訂訊息。
4. 按下「確定」。

更多資訊

- [管理防火牆規則](#)
- [針對入侵預防和記憶體攻擊緩和架構用戶端通知](#)
- [設定管理員通知](#)

關於防火牆規則主機觸發條件

定義主機觸發條件時，您須指定位於所述網路連線兩端的主機。

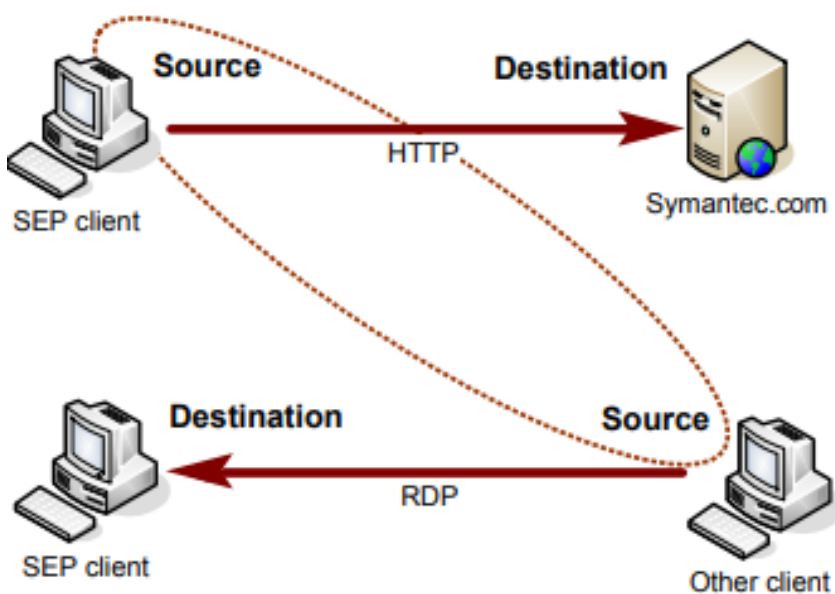
一般表示主機之間關係的方式，是將主機稱為網路連線的來源或目標。

您可以使用下列其中一種方式定義主機關係：

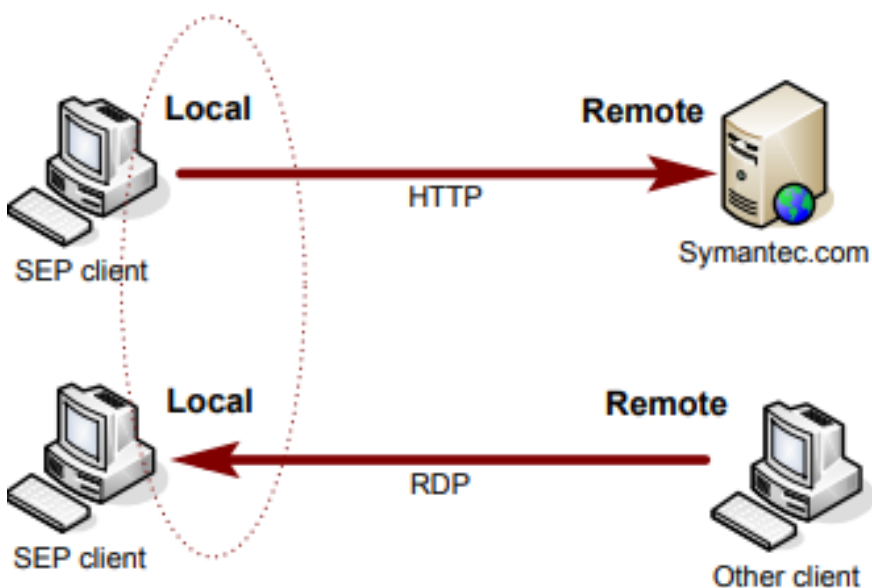
來源和目的	主機是來源還是目的取決於流量的方向。有時候可能本機用戶端電腦是來源，而有時候則可能遠端電腦是來源。來源與目的關係較常用於網路型防火牆。
本機及遠端	本機主機一定是本機用戶端電腦，而遠端主機則一定是位於網路其他位置的遠端電腦。這種主機關係的表示方式與流量方向無關。 本機與遠端關係較常用於主機型防火牆，而且比較容易查看流量。

您可以定義多個來源主機和多個目的主機。

下圖會以流量方向來說明來源關係和目的的關係。



下圖會以流量方向來說明本機主機與遠端主機的關係。



關係可使用下列陳述類型評估：

在連線 (來源和目的之間) 任一端定義的主機	OR 陳述式
選取的主機	AND 陳述式

例如，假設有個規則定義了單一本地主機和多個遠端主機。當防火牆檢查封包時，本地主機必須符合相關的 IP 位址。不過，位址的另一端則可符合任何遠端主機。例如，您可以定義規則以允許本機主機與 Yahoo.com 或 Google.com 之間的 HTTP 通訊。單一規則與兩個規則相同。

更多資訊

-
- [新增主機群組](#)
 - [攔截來往於特定伺服器的流量](#)
 - [管理防火牆規則](#)

新增主機群組

主機群組是 DNS 網域名稱、DNS 主機名稱、IP 位址、IP 範圍、MAC 位址或子網路的集合，在同一個名稱之下組成一個群組。主機群組的目的是為了不必重複輸入主機位址和名稱。例如，您可以將多個 IP 位址一次一個新增到防火牆規則中。或者，可以將多個 IP 位址新增到一個主機群組，然後將群組新增到防火牆規則。

當您加入主機群組時，必須說明群組的使用位置。如果您稍後決定刪除主機群組，必須先從參照此群組的所有防火牆規則中移除主機群組。

新增主機群組時，主機群組會出現在「主機」清單最下方。您可以從防火牆規則的「主機」欄位中存取「主機」清單。

新增主機群組

1. 在主控台中，按下「政策」。
2. 展開「政策元件」，然後按下「主機群組」。
3. 在「工作」下，按下「新增主機群組」。
4. 在「主機群組」對話方塊中輸入名稱，然後按下「新增」。
5. 在「主機」對話方塊的「類型」下拉式清單中，選取主機。
6. 輸入每種主機類型的適當資訊。
7. 按下「確定」。
8. 視需要新增其他主機。
9. 按下「確定」。

更多資訊

[關於防火牆規則主機觸發條件](#)

關於防火牆規則網路服務觸發條件

網路服務可讓網路電腦傳送和接收郵件、共用檔案以及列印。網路服務會使用一或多個通訊協定或通訊埠，藉此傳送特定類型的流量。例如，HTTP 服務會透過 TCP 通訊協定使用通訊埠 80 和 443。您可以建立允許或攔截網路服務的防火牆規則。網路服務觸發條件會根據所述的網路流量，識別產生作用的一項或多項網路通訊協定。

定義 TCP 型或 UDP 型服務觸發時，您可以指明所描述網路連線兩端的通訊埠。一般將通訊埠稱為網路連線的來源或目的。

更多資訊

- [新增網路服務至預設網路服務清單](#)
- [允許用戶端瀏覽網路中的檔案和印表機](#)
- [管理防火牆規則](#)

新增網路服務至預設網路服務清單

網路服務可讓網路電腦傳送和接收郵件、共用檔案以及列印。您可以建立允許或攔截網路服務的防火牆規則。

使用網路服務清單，就無須在建立攔截或允許網路服務的防火牆規則時還要重複輸入通訊協定和通訊埠。建立防火牆規則時，您可以從預設的常用網路服務清單中選取網路服務。您也可以將網路服務新增到預設清單。不過，您需要瞭解服務所使用的通訊協定類型和通訊埠。

NOTE

IPv4 和 IPv6 是兩種用於網際網路的網路層通訊協定。如果您在執行 Windows Vista 的電腦上安裝用戶端，則「規則」清單會包含攔截 IPv6 乙太網路通訊協定類型的數種預設規則。如果移除這些預設規則，就必須建立攔截 IPv6 的規則。

NOTE

您可以透過防火牆規則新增自訂網路服務。不過，該網路服務不會加入預設清單。您無法從任何其他規則存取自訂網路服務。

新增網路服務至預設網路服務清單

1. 在主控台中，按下「政策」。
2. 展開「政策元件」，然後按下「網路服務」。
3. 在「工作」下，按下「新增網路服務」。
4. 在「網路服務」對話方塊中，鍵入服務的名稱，再按下「新增」。
5. 從「通訊協定」下拉式清單選取通訊協定。

其他選項會根據您所選的通訊協定變更。

6. 在相應的欄位中輸入，然後按下「確定」。
7. 視需要新增一或多個其他通訊協定。
8. 按下「確定」。

更多資訊

- [管理防火牆規則](#)
- [關於防火牆規則網路服務觸發條件](#)
- [控制網路電腦是否可以共用郵件、檔案和列印](#)
- [允許用戶端瀏覽網路中的檔案和印表機](#)

關於防火牆規則網路配接卡觸發條件

您可以定義防火牆規則，攔截或允許通過 (傳輸或接收) 網路配接卡到的流量。

當您定義特定類型的配接卡時，請將配接卡的使用方式列入考量。例如，如果規則允許乙太網路配接卡的離埠 HTTP 流量，則已安裝的所有同類型配接卡都會允許 HTTP 通過。唯一的例外是同時指定了本地主機位址。用戶端電腦可能會使用多 NIC 的伺服器和工作站來橋接兩個以上的網路區段。若要控制特定配接卡的相關流量，就必須使用每個區段的位址配置，而不是配接卡本身。

網路配接卡清單可讓使用者無須為防火牆規則重新輸入配接卡類型。建立防火牆規則時，您可以從常用網路配接卡的預設清單選取網路配接卡。您也可以將網路配接器新增到預設清單。

您可以從所有防火牆政策和規則共用的預設清單選取網路配接卡。「政策元件」清單的預設清單包含最常見的配接卡。

NOTE

您可以透過防火牆規則新增自訂網路配接卡。但是，該網路配接卡不會加入預設清單。您無法從任何其他規則存取自訂網路配接卡。

更多資訊

-
- [管理防火牆規則](#)
 - [將自訂網路配接卡新增到網路配接卡清單](#)
 - [控制通過網路配接卡的流量](#)

將自訂網路配接卡新增到網路配接卡清單

您可以對每個網路配接卡分別套用不同的防火牆規則。例如，您可能會想要在辦公室攔截經由 VPN 的流量，但不會想在家裡這麼做。

您可以從所有防火牆政策和規則共用的預設清單選取網路配接卡。「政策元件」清單的預設清單包含最常見的配接卡。使用預設清單，您就無須為每個建立的規則重新輸入每個網路配接卡。

使用網路配接卡清單，就無須為防火牆規則重新輸入配接卡。建立防火牆規則時，您可以從預設的常用網路配接卡清單中選取網路配接卡。您也可以將網路配接器新增到預設清單。

NOTE

您可以透過防火牆規則新增自訂網路配接卡。但是，該網路配接卡不會加入預設清單。您無法從任何其他規則存取自訂網路配接卡。

將自訂網路配接卡新增到網路配接卡清單

1. 在主控台中，按下「政策 > 政策元件 > 網路配接卡」。
2. 在「工作」下，按下「新增網路配接卡」。
3. 在「網路配接卡」對話方塊的「配接卡類型」下拉式清單中，選取配接卡。
4. 在「配接卡名稱」欄位中，選擇性地輸入敘述。
5. 在「配接卡識別」文字方塊中，輸入配接卡品牌名稱，須區分大小寫。

若要找出配接卡的品牌名稱，可開啟用戶端的指令行，並輸入下列文字：

```
ipconfig/all
```

6. 按下「確定」。

更多資訊

- [管理防火牆規則](#)
- [關於防火牆規則網路配接卡觸發條件](#)
- [控制通過網路配接卡的流量](#)

複製 Symantec Endpoint Protection 防火牆規則

快速建立 SEP 防火牆規則。從政策匯出防火牆規則，然後將該規則匯入至不同的政策。您也可以匯出包含要重複使用之設定的現有防火牆規則，以節省規則建立時間。然後將該規則匯入至政策，並對其進行修改。

將規則匯出至 .dat 檔案。當您準備好匯入規則時，請確定您有權存取 .dat 檔案。規則會以其出現在父政策中的順序新增，以藍線為準。在您匯入規則之後，可以變更處理順序。

匯出防火牆規則

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
在 14.2 之前版本中，沒有「**Mac** 設定」的選項。
3. 在「規則」清單中，選取要匯出的規則，並按一下滑鼠右鍵，然後按一下「匯出」。
4. 在「匯出政策」對話方塊中，找出目錄來儲存 .dat 檔案，然後輸入檔案名稱，再按下「匯出」。

匯入防火牆規則

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
在 14.2 之前版本中，沒有「**Mac** 設定」的選項。
3. 用滑鼠右鍵按下「規則」清單，再按下「匯入」。
4. 在「匯入政策」對話方塊中，找出包含想要匯入防火牆規則的 .dat 檔案，再按下「匯入」。
5. 在「輸入」對話方塊中，輸入政策的新名稱，再按下「確定」。
6. 按下「確定」。

更多資訊

- [新增防火牆規則](#)
- [自訂防火牆規則](#)
- [關於防火牆規則、防火牆設定和入侵預防處理順序](#)

自訂防火牆規則

建立新的防火牆政策時，該政策會包括多個預設規則。您可以根據需要修改一個或多個規則元件。

Table 64: 防火牆規則的元件

動作	動作參數會指定防火牆成功比對到規則時所採取的動作。如果有規則符合並被選取來回應接收的封包，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，則會讓規則指定的流量存取網路。如果防火牆攔截流量，則會攔截規則指定的流量，不讓流量存取網路。 動作如下： • 允許 防火牆允許網路連線。 • 攔截 防火牆攔截網路連線。 Note: Mac 用戶端防火牆會監控封包，但不會記錄封包。 Note: 自 14.2 起，此附註才適用。
觸發條件	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真，防火牆即不會套用規則。您可以結合各項觸發條件的定義，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。 觸發條件如下： • 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，防火牆將允許此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。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。請參閱： 關於防火牆規則應用程式觸發條件 • 主機 在定義主機觸發條件時，您可以指定位於所述網路連線兩端的主機。 一般表示主機之間關係的方式，是將主機稱為網路連線的來源或目標。請參閱： 關於防火牆規則主機觸發條件 • 網路服務 網路服務觸發條件會識別對所述流量而言非常重要的一個或多個網路通訊協定。 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。請參閱： 關於防火牆規則網路服務觸發條件 • 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。請參閱： 關於防火牆規則網路配接卡觸發條件
條件	規則條件包含規則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。您可以定義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。條件參數是選用項目，如果未經定義，則不會有任何作用。防火牆不會評估非作用中的規則。
通知	「日誌」設定用於指定流量事件符合針對這項規則設定的條件時，伺服器是建立日誌項目還是傳送電子郵件。 「嚴重性」設定用於指定違規的嚴重性等級。

自訂防火牆規則

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
在 14.2 之前版本中，沒有「**Mac** 設定」的選項。
3. 在「規則」標籤的「規則」清單中，在「已啟用」欄位中，確定已勾選此方塊啟用此規則。取消勾選此方塊將停用此規則。
Symantec Endpoint Protection 僅處理您啟用的規則。根據預設，會啟用所有規則。

-
4. 連按兩下「名稱」欄位,然後鍵入防火牆規則的唯一名稱。
 5. 在「動作」欄位上按下滑鼠右鍵,選取在觸發規則時要 Symantec Endpoint Protection 執行的動作。
 6. 在「應用程式」欄位中,定義應用程式。請參閱：
[定義應用程式的相關資訊](#)
 7. 在「主機」欄位中,指定主機觸發條件。請參閱：
[攔截來往於特定伺服器的流量](#)
 8. 除指定主機觸發條件外,您還可以指定允許存取本機子網路的流量。請參閱：
[僅允許本機子網路的特定流量](#)
 9. 在「服務」欄位中,指定網路服務觸發條件。請參閱：
[控制網路電腦是否可以共用郵件、檔案和列印](#)
 10. 在「日誌」欄位中,指定在違反此防火牆規則時,您希望 Symantec Endpoint Protection 傳送電子郵件給您的時間。請參閱：
[設定違反防火牆規則通知](#)
 11. 在「嚴重性」欄位上按下滑鼠右鍵,並選取違規的嚴重性等級。
 12. 在「配接卡」欄中,指定規則的配接卡觸發條件。請參閱：
[控制通過網路配接卡的流量](#)
 13. 在「時間」欄中,指定此規則處於使用中狀態的時段。
 14. 在「螢幕保護程式」欄位上按下滑鼠右鍵,並指定用戶端電腦的螢幕保護程式必須處於哪一種狀態時,規則才會啟用。
「建立於」欄位無法編輯。如果共用政策,則會顯示「共用」一詞。如果未共用政策,此欄位將顯示指派了此非共用政策的群組的名稱。
 15. 在「敘述」欄位上按下滑鼠右鍵,按下「編輯」,輸入規則的敘述(可選),然後按下「確定」。
 16. 架構完此規則後,請按一下「確定」。

更多資訊

- [新增防火牆規則](#)
- [管理防火牆規則](#)

攔截來往於特定伺服器的流量

若要攔截來往於特定伺服器的流量,請以 IP 位址攔截流量,而不要以網域名稱或主機名稱來攔截流量。否則,使用者還是可以存取與主機名稱對等的 IP 位址。

攔截來往於特定伺服器的流量

1. 在主控台中,開啟某個防火牆政策。
2. 在「防火牆政策」頁面上,按下「規則」。
3. 在「規則」標籤的「規則」清單中,選取要編輯的規則,在「主機」欄位按下滑鼠右鍵,然後按下「編輯」。
4. 在「主機清單」對話方塊中,執行下列其中一個動作：
 - 按下「來源/目的」。
 - 按下「本機/遠端」。

5. 執行下列其中一項工作：

從「類型」下拉式清單中選取主機類型	執行下列所有工作： - 在「來源及目的或本機及遠端」表中，按下「新增」。 - 在「主機」對話方塊中，從「類型」下拉式清單中選取主機類型，然後輸入各主機類型的相應資訊。 - 按下「確定」。 您建立的主機將自動啟用。
選取主機群組	在「主機清單」對話方塊中，執行下列其中一個動作： - 按下「來源/目的」。 - 按下「本機/遠端」。 然後在「主機清單」對話方塊中，對要新增到此規則的任何主機群組勾選「已啟用」欄中的方塊。

6. 視需要新增其他主機。

7. 按下「確定」回到「規則」清單。

更多資訊

- [新增防火牆規則](#)
- [自訂防火牆規則](#)
- [新增主機群組](#)

僅允許本機子網路的特定流量

您可以建立防火牆規則，來僅允許本機子網路的特定流量。此防火牆規則會永遠套用至本機子網路 IP 位址，而不管該位址為何。因此，即使您變更本機子網路 IP 位址，您也從不必為新位址修改此規則。

例如，您可以建立此規則以僅允許本機子網路通訊埠 80 的流量，而不管本機子網路 IP 位址為何。

僅允許本機子網路的特定流量

- 在主控台中，開啟某個防火牆政策。
 - 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
- 在 14.2 之前版本中，沒有「**Mac** 設定」的選項。
- 在「規則」標籤的「防火牆規則」表格中，尋找您要編輯的規則。
 - 連按兩下您要建立本機子網路流量條件之規則的「主機」欄。
 - 在此規則套用的主機類型（「本機」或「遠端」）下，按下「新增」。
 - 按下「地址類型」下拉式清單並選取下列其中一項：
 - Windows：「本機子網路」
 - Mac：「子網路」
 - 按下「確定」，然後再次按下「確定」關閉「主機清單」對話方塊。

更多資訊

[自訂防火牆規則](#)

控制網路電腦是否可以共用郵件、檔案和列印

網路服務可讓網路電腦傳送和接收郵件、共用檔案以及列印。您可以建立允許或攔截網路服務的防火牆規則。

您可以透過防火牆規則新增自訂網路服務。不過，該網路服務不會加入預設清單。您無法從任何其他規則存取自訂服務。

控制網路電腦是否可以共用郵件、檔案和列印

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
在 14.2 之前版本中，沒有「**Mac** 設定」的選項。
3. 在「規則」標籤的「規則」清單中，選取要編輯的規則，並以滑鼠右鍵按一下「服務」欄位，然後按一下「編輯」。
4. 在「服務清單」對話方塊中，對要觸發規則的每項服務，勾選其旁邊的方塊。
5. 若只要為選取的規則新增其他服務，請按一下「新增」。
6. 在「通訊協定」對話方塊中，從「通訊協定」下拉式清單選取通訊協定。
7. 填入適當的欄位。
8. 按下「確定」。
9. 按下「確定」。
10. 按下「確定」。

更多資訊

- [新增防火牆規則](#)
- [自訂防火牆規則](#)
- [關於防火牆規則網路服務觸發條件](#)
- [新增網路服務至預設網路服務清單](#)

允許用戶端瀏覽網路中的檔案和印表機

您可以讓用戶端在區域網路上提供其檔案共用，或瀏覽區域網路上的共用檔案和印表機。為防止網路型攻擊，您可能不需要啟用網路檔案和印表機共用。

您可以新增防火牆規則來啟用網路檔案和列印共用。防火牆規則允許存取通訊埠來瀏覽和共用檔案及印表機。您可以先建立一個防火牆規則，讓用戶端可以提供其檔案共用。接著再建立第二個防火牆規則，讓用戶端可以瀏覽其他檔案和印表機。

根據您為用戶端指定的控制類型，此設定會以不同方式執行，如下所示：

用戶端控制或混合控制	Windows 用戶端上的使用者可以在「防網路和主機侵入」中架構這些設定，以自動啟用設定。 Mac 用戶端上的使用者只能啟用或停用防火牆。
混合控制	指定這種類型流量的伺服器防火牆規則可以在 Windows 上覆寫這些設定。 在 Mac 上，所有防火牆規則均為伺服器防火牆規則。
伺服器控制	這些設定在用戶端上無法使用。

允許 **Windows** 用戶端瀏覽網路中的檔案和印表機 (選項 1)

1. 在主控台上，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」下方，按一下「規則」。
3. 在「規則」標籤的「規則」清單中，選取要編輯的規則，並以滑鼠右鍵按一下「服務」欄位，然後按一下「編輯」。
4. 在「服務清單」對話方塊中，按下「新增」。
5. 在「通訊協定」對話方塊的「通訊協定」下拉式清單中，按下 **TCP**，再按下「本機/遠端」。
6. 執行下列其中一項工作：

允許用戶端瀏覽網路中的檔案和印表機	在「遠端通訊埠」下拉式清單中，輸入 88, 135, 139, 445。
讓其他電腦瀏覽用戶端上的檔案	在「本機通訊埠」下拉式清單中，輸入 88, 135, 139, 445。

7. 按下「確定」。
8. 在「服務清單」對話方塊中，按下「新增」。
9. 在「通訊協定」對話方塊的「通訊協定」下拉式清單中，按下 **UDP**。
10. 執行下列其中一項工作：

允許用戶端瀏覽網路中的檔案和印表機	在「本機通訊埠」下拉式清單中，輸入 137, 138。 在「遠端通訊埠」下拉式清單中，輸入 88。
讓其他電腦瀏覽用戶端上的檔案	在「本機通訊埠」下拉式清單中，輸入 88, 137, 138。

11. 按下「確定」。
12. 在「服務清單」對話方塊中，確保兩項服務均啟用，然後按下「確定」。
13. 在「規則」標籤上，確保將「動作」欄位設定為「允許」。
14. 架構完此政策後，按下「確定」。

允許 **Mac** 用戶端瀏覽網路中的檔案和印表機 (選項 2)

1. 在主控台中，開啟某個防火牆政策。

NOTE

自 14.2 版起，提供 Mac 防火牆。

2. 在「防火牆政策」頁面的「**Mac** 設定」下方，按下「規則」。
3. 在「規則」標籤的「規則」清單中，選取要編輯的規則，並以滑鼠右鍵按一下「服務」欄位，然後按一下「編輯」。
4. 在「服務清單」對話方塊中，按下「新增」。
5. 在「通訊協定」對話方塊的「通訊協定」下拉式清單中，按下 **TCP**，再按下「本機/遠端」。
6. 若要讓其他電腦能夠瀏覽用戶端上的檔案，請在「本機通訊埠」下拉式清單中輸入 139 和 445。
預設會啟用從 Mac 瀏覽網路的外寄要求。
7. 按下「確定」。
8. 在「服務清單」對話方塊中，確保新服務已啟用，然後按下「確定」。
9. 在「規則」標籤上，確保將「動作」欄位設定為「允許」。
10. 架構完此政策後，按下「確定」。

可透過 Bonjour 服務在 Mac 上執行印表機搜尋，該服務預設為開啟。您不需要架構 Bonjour 服務的自訂規則。

可透過 Bonjour 服務在 Mac 上執行印表機搜尋，該服務預設為開啟。您不需要架構 Bonjour 服務的自訂規則。

更多資訊

- [新增防火牆規則](#)
- [自訂防火牆規則](#)

設定違反防火牆規則通知

您可以架構 Symantec Endpoint Protection 在每次防火牆偵測到違反規則、攻擊或事件時，寄發電子郵件訊息給您。例如，您可能想在用戶端攔截來自某個特定 IP 位址的流量時收到通知。

為防火牆違規設定通知

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「規則」。
在 14.2 之前版本中，沒有「**Mac** 設定」的選項。

3. 在「規則」標籤中選取規則，然後在「日誌」欄位上按下滑鼠右鍵，再執行下列其中一或多項工作：

觸發防火牆規則時傳送電子郵件訊息	勾選「傳送電子郵件警示」。
觸發防火牆規則時產生日誌事件	若為 Windows 規則，同時勾選「寫入至流量日誌」和「寫入至封包日誌」。 若為 Mac 規則，請勾選「寫入至流量日誌」。

4. 架構完此政策後，按下「確定」。

5. 架構安全性警示。

6. 架構郵件伺服器。

7. 按下「確定」。

更多資訊

- [新增防火牆規則](#)
- [自訂防火牆規則](#)
- [設定管理員通知](#)

控制通過網路配接卡的流量

如果您定義了網路配接卡觸發條件，則規則只會與指定配接卡轉送或接收的流量有關。

您可以透過防火牆規則新增自訂網路配接卡。不過，該配接卡不會加入共用清單。您無法從任何其他規則存取自訂配接卡。

控制通過網路配接卡的流量

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」下方，按一下「規則」。
3. 在「規則」標籤的「規則」清單中，選取要編輯的規則，並以滑鼠右鍵按一下「配接卡」欄，然後按一下「更多配接卡」。
4. 在「網路配接卡」對話方塊中，執行下列其中一個動作：

觸發任何配接卡的規則 (即使未列出)	按一下「套用規則到所有配接卡」然後跳至步驟 7。
觸發選取配接卡的規則	按一下「套用規則到下列配接卡」。 然後，對要觸發規則的每個配接卡勾選其旁邊的方塊。

5. 若要只為選取的規則新增自訂配接卡，請執行下列工作：

- 按一下「新增」。
- 在「網路配接卡」對話方塊中，選取配接卡類型，然後在「配接卡識別」文字欄位中輸入配接卡的品牌名稱。

6. 按下「確定」。

7. 按下「確定」。

8. 按下「確定」。

更多資訊

- [新增防火牆規則](#)
- [自訂防火牆規則](#)
- [關於防火牆規則網路配接卡觸發條件](#)

架構混合控制的防火牆設定

您可以架構用戶端，讓使用者不能控制、完全控制或有限控制其可架構的防火牆設定。

在 Mac 防火牆中，無論用戶端使用者介面設定為何，使用者都無法建立防火牆規則或變更設定。選項未曾顯示在用戶端使用者介面中。

伺服器控制	在 Windows 中，使用者無法建立任何防火牆規則或啟用防火牆設定。 在 Mac 中，使用者無法啟用或停用防火牆。
用戶端控制	在 Windows 中，使用者可以建立防火牆規則和啟用所有防火牆設定。 在 Mac 中，使用者可以啟用和停用防火牆。
混合控制	在 Windows 中，使用者可以建立防火牆規則。您可以決定使用者能夠啟用哪些防火牆設定。 在 Mac 中，您可以決定使用者是否可以啟用或停用防火牆。

NOTE

自 14.2 版起，防火牆才適用於 Mac 用戶端。

架構混合控制的防火牆設定

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，選取具有您要修改之使用者控制層級的群組。
3. 在「政策」標籤的「位置限定的政策與設定」下，展開某位置下方的「位置限定的設定」。
4. 在「用戶端使用者介面控制設定」的右側，按一下「工作 > 編輯設定」。
5. 在「控制模式設定」對話方塊中，按一下「混合控制」，然後按一下「自訂」。
6. 在「用戶端/伺服器控制設定」標籤的「防火牆政策」類別下方，執行下列其中一項工作：
 - 若要讓使用者可以架構用戶端設定，請按一下「用戶端」。
 - 若要架構用戶端設定，請按一下「伺服器」。
7. 按下「確定」。
8. 按下「確定」。
9. 針對您要設定為「伺服器」的每個防火牆設定，在「防火牆」政策中啟用或停用該設定。

更多資訊

- [管理防火牆防護](#)
- [為網路服務啟用通訊而非新增規則](#)

為網路服務啟用通訊而非新增規則

您可以啟用自動允許特定網路服務之間進行通訊的選項，這樣您就不必定義明確允許這些服務的規則。您也可以啟用流量設定，偵測和攔截透過 NetBIOS 與 Token Ring 進行通訊的流量。

您可允許已架構使用 DHCP、DNS 和 WINS 流量的網路連線進行離埠要求和入埠回應。

這些過濾會允許 DHCP、DNS 或 WINS 用戶端接收來自伺服器的 IP 位址。此外，也可防護用戶端在下列情況下不受來自網路的攻擊：

如果用戶端傳送要求至伺服器	用戶端會等待五秒後再允許入埠回應。
如果用戶端沒有傳送要求至伺服器	所有過濾均不允許封包。

啟用這些選項時，Symantec Endpoint Protection 會在有要求發出時允許封包；它不會攔截封包。您必須建立防火牆規則來攔截封包。

NOTE

若要在混合控制中架構這些設定，您還必須在「用戶端使用者介面混合控制設定」對話方塊中啟用這些設定。

為網路服務啟用通訊而非新增規則

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的「**Windows** 設定」或「**Mac** 設定」下方，按下「內建規則」。
在 14.2 之前版本中，這些設定僅適用於 Windows。
3. 勾選要啟用的選項。
4. 按下「確定」。
5. 如果系統顯示提示，請將政策指派至某個位置。

更多資訊

- [建立防火牆政策](#)
- [編輯政策](#)
- [防止使用者在用戶端電腦上停用防護](#)

自動攔截連線至攻擊電腦

如果 Symantec Endpoint Protection 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。用戶端會啟動主動回應，此功能會自動攔截特定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。

攻擊者的 IP 位址會記錄在「安全日誌」中。您可以取消特定 IP 位址或取消全部的主動回應來取消攔擊攻擊。

如果您將用戶端設定為混合控制，則可以指定用戶端上是否提供該設定供使用者啟用。如果未提供該設定，就必須在「用戶端使用者介面混合控制設定」對話方塊中啟用它。

更新的 IPS 特徵、更新的服務阻斷特徵、通訊埠掃描以及 MAC 詐騙也會觸發主動回應。

自動攔截連線至攻擊電腦

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面的左窗格中，按下列其中一個選項：
 - 在「**Windows** 設定」下方：「防護與隱藏」
 - 在「**Mac** 設定」下方：「防護」
自 14.2 版起，才開始提供 Mac 設定。
3. 在「防護設定」下方，勾選「自動攔截攻擊者的 IP 位址」。
4. 在「攔截 IP 位址的秒數...秒」文字方塊中，指定攔截可能攻擊者的秒數。
您可以輸入 1 到 999,999 的值。
5. 按下「確定」。

更多資訊

- [建立防火牆政策](#)
- [架構混合控制的防火牆設定](#)
- [編輯政策](#)

偵測潛在的攻擊和詐騙嘗試

您可以啟用各種設定讓 Symantec Endpoint Protection 偵測和記錄用戶端上的潛在攻擊並攔截詐騙嘗試。這些選項全部預設為停用。

Table 65: 您可以啟用的設定

設定	說明
啟用通訊埠掃描偵測	啟用此設定時，Symantec Endpoint Protection 會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，Symantec Endpoint Protection 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。
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。
啟用防 MAC 詐騙	啟用此設定時，如果對該特定主機提出要求，則 Symantec Endpoint Protection 會允許下列連入流量和連出流量： - 位址解析通訊協定 (ARP) (IPv4) - 芳鄰搜尋通訊協定 (NDP) (IPv6) 自 14.2 版起受支援。 系統會攔截所有其他非預期的流量，並在安全日誌中產生項目。

NOTE

若要在混合控制中架構這些設定，您還必須在「用戶端使用者介面混合控制設定」對話方塊中啟用這些設定。

偵測潛在的攻擊和詐騙嘗試

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面上，按下列其中一項：
 - 在「**Windows** 設定」下方：「防護與隱藏」
 - 在「**Mac** 設定」下方：「防護」自 14.2 版起，才開始提供 Mac 設定。
3. 在「防護設定」下方，勾選您要啟用的任何選項。
4. 按下「確定」。
5. 如果系統顯示提示，請將政策指派至某個位置。

更多資訊

- [建立防火牆政策](#)
- [防止使用者在用戶端電腦上停用防護](#)
- [編輯政策](#)

防止對電腦的外部隱藏攻擊

您可啟用防止外部攻擊偵測用戶端相關資訊的設定。依預設會停用這些設定。

NOTE

若要在混合控制中架構這些設定，您還必須在「用戶端使用者介面混合控制設定」對話方塊中啟用這些設定。

NOTE

這些隱藏設定不適用於 Mac 防火牆。

防止對電腦的外部隱藏攻擊

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面中，按下「防護與隱藏」。
3. 在「隱藏設定」下方，勾選您要啟用的任何選項。
4. 按下「確定」。
5. 如果系統顯示提示，請將政策指派至某個位置。

更多資訊

- [建立防火牆政策](#)
- [防止使用者在用戶端電腦上停用防護](#)
- [編輯政策](#)

關於 Mac 用戶端的防火牆設定

包含在適用於 Mac 的 Symantec Endpoint Protection 用戶端中的防火牆設定如下：

- 防火牆智慧型規則
- 自訂防火牆規則

只有 Symantec Endpoint Protection Manager 管理員能架構這些設定。防火牆僅適用於受管用戶端。

自 14.2 版起，防火牆隨附於適用於 Mac 的 Symantec Endpoint Protection 用戶端。

Table 66: 防火牆設定

設定類型	說明
防火牆智慧型規則	防火牆智慧型規則提供防護來防止常見的攻擊類型。這些規則也會在 Mac 對特定的通訊協定提出初始要求時，允許該通訊協定上的流量。 防護設定包括： • 通訊埠掃描偵測 • 服務阻斷偵測 • 防 MAC 詐騙 • 自動攔截攻擊者的 IP 位址 流量通訊協定包括： • 智慧型 DHCP • 智慧型 DNS 適用於 Mac 的 Symantec Endpoint Protection 防火牆未與作業系統的內建防火牆整合，而是會並行執行。作業系統防火牆會在應用層進行檢查，而 Symantec Endpoint Protection 防火牆則在較低層級 (網路和傳輸) 進行檢查。 適用於 Mac 的 Symantec Endpoint Protection 防火牆不提供點對點攔截規則，但是您可以透過自訂防火牆規則建立部分這類規則。
自訂防火牆規則	自訂防火牆規則可讓管理員建立涉及各種網路流量屬性的規則。

更多資訊

[管理防火牆防護](#)

停用 Windows 防火牆

您可以指定 Symantec Endpoint Protection 停用 Windows 防火牆的條件。發生下列情況時，Symantec Endpoint Protection 會將 Windows 防火牆設定還原為安裝 Symantec Endpoint Protection 之前的狀態：

-
- Symantec Endpoint Protection 已移除。
 - Symantec Endpoint Protection 防火牆已停用。

NOTE

Symantec Endpoint Protection 不會修改任何現有的 Windows 防火牆政策規則或排除項目。

一般而言，如果停用 Windows 防火牆，Windows 使用者會在其電腦重新啟動時收到通知。依據預設，Symantec Endpoint Protection 會停用此通知，以避免在停用 Windows 防火牆時向使用者傳送警示。然而如有需要，可以啟用通知。

停用 Windows 防火牆

1. 在主控台中，按下「政策」。
2. 在「政策」下方，按下「防火牆」。
3. 執行下列其中一項工作：
 - 建立新的防火牆政策。
 - 在「防火牆政策」清單中，連按兩下要修改的防火牆政策。
4. 在「防火牆政策」下方，按下「**Windows 整合**」。
5. 在「停用 **Windows** 防火牆」下拉式清單中，指定您希望何時停用 Windows 防火牆。

預設設定為「僅停用一次」。

如需關於選項的詳細資訊，請按下「說明」。請參閱：

[Windows 整合](#)

6. 在「**Windows** 防火牆停用訊息」下拉式清單中，指定您是否希望在啟動時停用會說明已停用防火牆的 Windows 訊息。
預設設定為「停用」，表示使用者不會在電腦啟動時收到說明已停用 Windows 防火牆的訊息。
7. 按下「確定」。

更多資訊

- [建立防火牆政策](#)
- [安全政策類型](#)

架構入侵預防

使用入侵預防系統 (IPS) 保護您的端點免受勒索軟體和惡意軟體的侵害。IPS 是 Windows 和 Mac 用戶端上防火牆後面之惡意程式的第一層防禦。

什麼是入侵預防且其用途為何？

入侵預防：

- 在攻擊進入組織網路之前，攔截超過 70% 的攻擊。即使在惡意軟體進入您的組織之後，IPS 還是可在侵擾和外滲階段偵測到惡意程式。在此階段期間，IPS 會在威脅通過網路時予以攔截。
- 使用 URL 信譽偵測勒索程式攻擊，從而防止 Web 威脅。
- 是指任何其他安全性公司都未使用的獨一無二的防護。

在酬載到達端點之前，IPS 會攔截網路層的惡意軟體，因為它會掃描入埠和離埠網路流量。IPS 可以：

- 辨識並瞭解各種網路通訊協定，並為每種類型提供自訂防護。
- 使用型樣比對來識別未知和已知威脅。
- 使用賽門鐵克的 Insight Intelligence，攔截已知惡意 URL 和 IP 位址的 command-and-control (C&C) 通訊。

在 Endpoint Security 上，IPS 使用超過 400 的稽核特徵。稽核特徵是沒有預設動作的特徵。

NOTE

賽門鐵克建議您在伺服器及桌上型電腦上安裝用戶端軟體。此外，賽門鐵克還會建議您將伺服器端點移到相同的群組。

如需特徵的詳細資訊，請參閱：

[關於賽門鐵克 IPS 特徵](#)

步驟 1：啟用入侵預防

預設會啟用 IPS，因此您的電腦一律會受到保護。

NOTE

賽門鐵克建議您一律保持 IPS 的啟用狀態。

根據預設，也會啟用下列 IPS 功能：

功能	說明
瀏覽器防護 (Windows 瀏覽器入侵預防)	IPS Web 瀏覽器特徵可允許和攔截入埠和離埠瀏覽器流量。根據預設，系統會安裝 Google Chrome 瀏覽器延伸 (14.3 RU2 和更新版本) 和 Microsoft InTune 延伸 (14.3 RU8 和更新版本)。 整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站
網路入侵預防	網路 IPS 特徵可防禦網路攻擊。
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 信譽可攔截識別為已知惡意內容來源之網址的存取。來自已造訪 URL 的資訊會傳送給賽門鐵克以擷取信譽等級。 Endpoint Security / Endpoint Protection URL 信譽功能錯誤偵測 URL，進而導致誤報。 Note: 如果客戶端將 URL 錯誤偵測為託管惡意內容，請將該 URL 提交為誤報案例。請參閱： Note: URL 信譽誤報程序

對於已在其上安裝用戶端軟體的伺服器，請在「入侵預防」政策中啟用下列設定：

路徑外掃描	套用多執行緒掃描以改善效能。
針對伺服器使用特徵子集	套用可防止伺服器上最常見已知威脅的特徵。

Endpoint Protection 效能調整設定：

Server Performance Tuning

Server performance tuning helps to improve the performance of intrusion prevention on server operating systems.

☐ Out-of-band scanning

Note: This option may have compatibility issues with other Windows Filtering Platform (WFP) drivers.

Therefore, if you enable this option, apply the policy to a test server to test it before you apply it to all production servers.

☐ Use signature subset for servers

Endpoint Security 效能調整設定：

Use signature subset for servers



Out-of-band scanning



如需調整設定的詳細資訊，請參閱：

- [啟用入侵預防](#)
- [URL 信譽常見問答集](#)
- [整合瀏覽器延伸和 Symantec Endpoint Protection \(SEP\)，防止惡意網站](#)

步驟 2：使用 URL 信譽攔截勒索程式 (14.3 RU2 和更新版本)

IPS 是最佳防禦工具，可以防止從 Internet 不知不覺地下載軟體時所發生的偷渡式下載。攻擊者通常使用侵入套件，透過偷渡式下載進行 CryptoLocker 之類的網頁式攻擊。

在某些情況下，IPS 可以中斷 command-and-control (C&C) 通訊來攔截檔案加密。C&C 伺服器是攻擊者或網路罪犯所控制的電腦，用來將指令傳送給惡意程式所破壞的系統，以從目標網路接收所竊取的資料。

對於 14.3 RU2 和更新版本的用戶端，URL 信譽會攔截這些偷渡式下載，以及啟用 URL 信譽。

Endpoint Protection URL 信譽設定：

Prevention Policy

tion

ettings

gs

Intrusion Prevention

Intrusion Prevention
Network Intrusion Prevention automatically detects and blocks network attacks and blocks browser attacks.

☒ Enable Network Intrusion Prevention

☒ Enable excluded hosts

☒ Enable Browser Intrusion Prevention for Windows

☐ Log detections but do not block

☒ Enable URL reputation

Endpoint Security URL 信譽設定：

Advanced Settings

Intrusion Prevention



Also supports

Browser Protection [Show Advanced](#)



Enable URL reputation



Server Performance Tuning [Show Advanced](#)

如需 URL 信譽設定的詳細資訊，請參閱：

[使用 Symantec Endpoint Protection 的勒索軟體防護](#)

步驟 3：(選用) 新增自訂 IPS 特徵

若要識別特定入侵並減少特徵導致誤報的可能性，您可以撰寫自己的自訂網路入侵預防特徵。您在自訂特徵中新增的資訊愈多，特徵就愈有效。

NOTE

自訂 IPS 特徵只適用於 Symantec Endpoint Protection。它們很快就可以在 Symantec Endpoint Security 中使用。

Intrusion Prevention Manager Latest Alerts Refresh Help

Intrusion Prevention Policies

Intrusion Prevention Policies Custom Intrusion Prevention Signatures

Name	Description	Group and Location Use Count

Custom Intrusion Prevention Signatures

Name: New Custom Intrusion Prevention Signatures

Description: You can follow this sample to create your own custom Intrusion Prevention signatures.

Signatures Variables

Signature Groups

- NetBIOS Group

Group Name: NetBIOS Group

Description: This is an example of a NetBIOS signature group.

☒ Enable this group

Signatures for this Group

Enabled	Name	Content	Applications	Action	Track
☒	NetBIOS DoS R...	rule tcp, dest=...	*	Block	Log

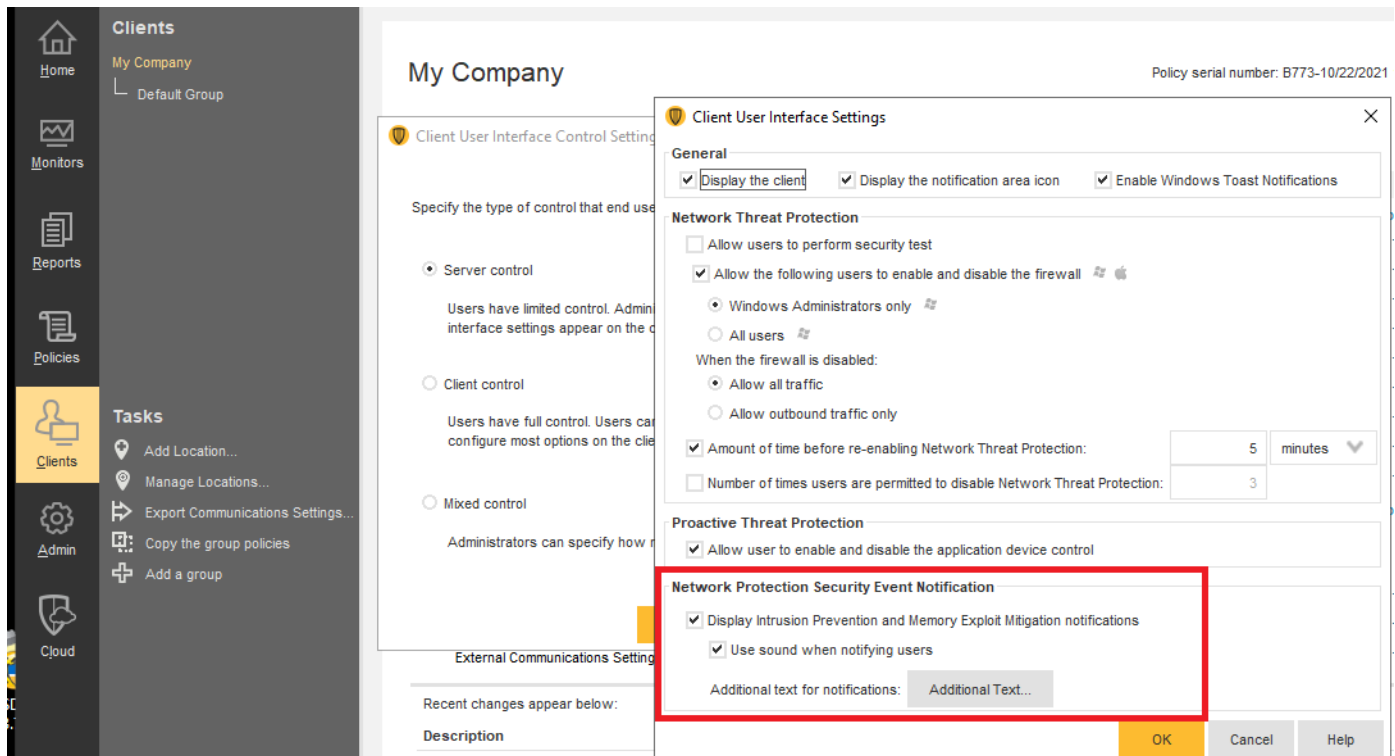
如需詳細資訊，請參閱：

- [管理自訂入侵預防特徵](#)
- [關於自訂 IPS 特徵](#)

步驟 4：(選用) 為用戶端使用者架構在 IPS 偵測到可疑活動時的自訂通知

IPS 在用戶端上偵測到可疑活動時，會向用戶端使用者傳送通知。您可以保留預設通知文字，或將它取代為自訂訊息。

Endpoint Protection 通知設定：



如需通知設定的詳細資訊，請參閱：

[針對入侵預防和記憶體攻擊緩和架構用戶端通知](#)

Endpoint Security 通知設定：

User Notification Settings

Notifications are only sent for enabled signatures.

Show notification on the device [Hide Advanced](#)

Also supports



Show a custom notification on the device

步驟 5：(選用) 執行 IPS 偵測的報告

若要更好地瞭解您組織的 IPS 偵測和網路安全性狀況，請執行下列報告：

- 在 Symantec Endpoint Protection 中，執行「防網路和主機侵入」報告。
- 在 Symantec Endpoint Security 中，執行「入侵預防」報告。

Endpoint Protection 報告設定：

[Home](#)[Monitors](#)[Reports](#)[Policies](#)[Clients](#)[Admin](#)[Cloud](#)[Quick Reports](#)[Scheduled Reports](#)

Network and Host Exploit Mitigation Reports

What type of report would you like to see?

Report type: Network and Host Exploit Mitigation

Select a report: Full Report

Use a saved filter: Default

What filter settings would you like to use?

Time range: Past 24 hours

[Additional Settings >>](#)

Reports to Include

Reports to Include

Specify the reports you want to include:

- ☒ Top Types of Attack
- ☒ Top Targets Attacked by Group
- ☒ Top Targets Attacked by Subnet
- ☒ Top Targets Attacked by Client
- ☒ Top Sources of Attack
- ☒ Top Traffic Notifications by Group (Traffic)
- ☒ Top Traffic Notifications by Group (Packets)
- ☒ Top Traffic Notifications by Subnet (Traffic)
- ☒ Top Traffic Notifications by IPv6 Subnet (Traffic)
- ☒ Top Traffic Notifications by Subnet (Packets)
- ☒ Top Traffic Notifications by IPv6 Subnet (Packets)

如需報告的詳細資訊，請參閱：

[執行和自訂快速報告](#)

Endpoint Security 報告設定：

IPS 特徵會偵測或許為惡意程式的威脅。如果您認為特徵未與您環境中可能存在的惡意活動相關聯，並且是誤報，則可以建立例外，防止 IPS 使用該特徵。

1. 新增例外。
您可以將 IPS 對任何檔案採取的動作從「攔截」變更為「允許」，以減少誤報數目。

- 新增例外**
- a. 對瀏覽器入侵預防特徵啟用只記錄模式，以記錄它在未影響用戶端使用者的情況下所攔截的流量。
 - b. 使用 Symantec Endpoint Protection Manager 中的「防網路和主機侵入」攻擊日誌，在「入侵預防」政策中建立例外，以忽略特定瀏覽器特徵。
 - c. 停用只記錄模式。

建立病毒和間諜軟體掃描的例外

2. 建立自訂 IPS 特徵。
請遵循步驟 3：(選用) 新增自訂 IPS 特徵中所列的步驟。

自訂 IPS 特徵只適用於 Symantec Endpoint Protection。它們很快就可以在 Symantec Endpoint Security 中使用。

3. 根據特定電腦的 IP 位址予以排除，讓 IPS 引擎不掃描這些電腦。
例如，您可能還要排除一些電腦，允許 Internet 服務供應商掃描您網路中的通訊埠，以確保遵從其服務合約。或者，您可以將內部網路的某些電腦設定為進行測試。

276

Intrusion Prevention

Intrusion Prevention

Network Intrusion Prevention automatically detects and blocks network attacks and blocks browser attacks.



☒ Enable Network Intrusion Prevention



☒ Enable excluded hosts

Excluded Hosts...



Excluded Hosts

Host List

Hosts to exclude from Intrusion Prevention:

Enabled Group Name

如需已排除主機設定的詳細資訊，請參閱：

[設定排除的電腦清單](#)

Endpoint Security 主機排除設定 (在「允許清單」中)：

Intrusion Prevention Host Exclusion

List of excluded hosts

[+ Add](#)

HOST TYPE

HOST SPECIFICATION

No IPS hosts added.

如需主機排除設定的詳細資訊，請參閱：

[新增允許清單政策掃描例外](#)

- 如果您認為 URL 信譽觸發已知的良好 URL，則請將 URL 提交給賽門鐵克安全團隊。

請遵循下列「支援」文章中的步驟：

[URL 信譽誤報程序](#)

Endpoint Protection 例外設定：



Intrusion Prevention Policy

Intrusion Prevention Policy

Overview

Intrusion Prevention

Windows Settings

Exceptions

Mac Settings

Exceptions

Exceptions

Intrusion
Select s

ID



Add Intrusion Prevention Exceptions

Intrusion Prevention Exceptions

Select the signatures that need settings that are different from the default settings.

Show category:

All

Show severity

ID	Signature Name	Severity	Categories
20632	System Infected: BD BackOrifice 2000 UD...	High	Intrusion Preven
20119	System Infected: BD NetBus Activity	High	Intrusion Preven
20042	Attack: DDOS Mstream HandlerAgent Com...	High	Server Signature
20068	OS Attack: SMB Request Buffer Overflow ...	Medium	Server Signature

Endpoint Security 例外設定：

Search Signatures



Showing list of Signatures



Enable



Log



Disable



Remove



Add



SIGNA...

PLATF...

SIGNATURE NAME

SEVER...

CATEGORY

STATUS

啟用入侵預防

入侵預防預設為啟用。通常情況下，除非進行疑難排解，否則不應停用入侵預防。

您可以對瀏覽器入侵預防啟用只記錄模式，以記錄它在未影響用戶端使用者的情況下所攔截的流量。您可以隨後使用 Symantec Endpoint Protection Manager 中的「防網路和主機侵入」攻擊日誌，在「入侵預防」政策中建立例外，以忽略特定的瀏覽器特徵。然後，您會停用只記錄模式。

NOTE

若要讓這些設定可供用戶端使用者啟用或停用，請在「用戶端使用者介面混合控制設定」對話方塊中架構這些設定。

啟用入侵預防

1. 在主控台中，開啟某個入侵預防政策。
2. 在政策頁面上，按下「入侵預防」。
3. 確定勾選下列選項：
 - 啟用網路入侵預防
您還可以從網路入侵預防中排除特定電腦。請參閱：
[設定排除的電腦清單](#)
 - 啟用 **Windows** 瀏覽器入侵預防
取消選取此選項也讓您解除安裝 Google Chrome 瀏覽器延伸 (14.3 RU5 或更新版本) 和 Microsoft Edge 瀏覽器延伸 (14.3 RU8 或更新版本)。
4. 按一下「確定」。

更多資訊

- [為 IPS 特徵建立例外](#)
- [管理入侵預防](#)
- [架構混合控制的防火牆設定](#)

整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站

什麼是 SEP 瀏覽器延伸？

瀏覽器延伸是將功能和特性新增至 Web 瀏覽器的外掛程式。SEP 瀏覽器延伸會監控進出 Web 瀏覽器的 HTTP 和 HTTPS 流量，並在用戶端確定 URL 是惡意 URL 時攔截該流量。如果 Web 瀏覽器偵測到 URL 是惡意的，則用戶端會將使用者重新導向到[預設登陸頁面](#)。

Symantec Endpoint Protection 為以下瀏覽器提供瀏覽器防護：

- 版本 14.3 RU8 和更新版本會安裝 Microsoft Edge 延伸。
- 版本 14.3 RU2 和更新版本會安裝 Google Chrome 延伸。
- Mozilla Firefox 和 Microsoft Internet Explorer 不使用瀏覽器延伸。相反地，SEP 會根據用戶端使用的用戶端入侵偵測系統 (CIDS) 引擎版本來支援這些瀏覽器。

SEP 瀏覽器延伸如何運作？

SEP 瀏覽器延伸會使用下列技術來識別和保護惡意 URL：

- 瀏覽器入侵防禦 (亦稱為「瀏覽器防護」) 會將 IPS Web 瀏覽器特徵套用至 Windows 用戶端上的入埠和離埠瀏覽器流量。請參閱：
[預期的瀏覽器入侵防禦行為](#)
- **URL** 信譽可識別來自網域和 URL 的威脅，這些網域和 URL 可以託管惡意程式、詐騙、網路釣魚和垃圾郵件這類惡意內容。URL 信譽接著會攔截識別為惡意內容之已知來源的網址存取權。請參閱：
[SEP URL 信譽常見問答集](#)

安裝 Chrome 或 Edge 瀏覽器延伸之後，LiveUpdate 會下載名為 WebExt 的 IPS 子功能。瀏覽器延伸使用 WebExt 定義和 IPS 特徵。

WebExt 定義包括下列元件：

- **WebFilter**：使用延伸引擎 WebPulse，以根據網域和類別來檢測 URL。WebPulse 使用鑑識和信譽查詢。
- 掃描程式：使用 IPS 特徵來報告偵測的掃描檔案。

與核心 IPS 的其中一個差異在於 IPS 看不到 HTTPS 流量，而瀏覽器延伸可以看得到。

步驟 1：安裝 SEP 瀏覽器延伸之前

安裝 SEP 瀏覽器延伸之前，請完成以下步驟：

1. 確認用戶端安裝套件包括「進階下載防護」和「入侵預防」元件。瀏覽器延伸取決於 IPS。請參閱：
[選擇要在用戶端上安裝哪些安全性功能](#)
2. 確認已啟用 Live Update 瀏覽器延伸內容。
LiveUpdate 預設會自動安裝這些定義。此內容的啟用是按一下「管理」>「伺服器」>「編輯網站屬性」>「**LiveUpdate**」標籤>「要下載的內容類型」>「瀏覽器延伸」。請參閱：
[將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)
3. 選擇您要直接從 Symantec Endpoint Protection Manager 安裝 SEP 瀏覽器延伸，或使用第三方管理控制台。
請參閱：[步驟 2：選擇安裝 SEP 瀏覽器延伸的方法](#)
4. (選擇性) 若要降低誤報次數，請建立例外以允許 Web 網域，讓用戶端永遠不會攔截它們。在「例外」政策中，新增 Windows「信任的 **Web** 網域」例外。請參閱：
[信任的 Web 網域例外](#)

步驟 2：選擇安裝 SEP 瀏覽器延伸的方法

下表說明可以在 Google Chrome 或 Microsoft Edge 上安裝 SEP 瀏覽器延伸的方法。

NOTE

當您使用以下方式設定政策時，HKEY_LOCAL_MACHINE 會優先於雲端使用者政策，而此政策優先於 HKEY_CURRENT_USER。

Table 67: 安裝 SEP 瀏覽器延伸的方法

方法	使用時機	如何設定
Symantec Endpoint Protection 用戶端安裝程式 (預設)	您希望將 SEP 瀏覽器延伸直接安裝到 Web 瀏覽器上。	- 啟動瀏覽器防護。請參閱： 步驟 3：在「入侵預防」政策中啟用瀏覽器防護 SEP 用戶端會修改本機群組原則 (GPO) 以強制執行瀏覽器延伸並新增以下機碼至登錄檔： Chrome：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForceList Edge：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForceList
第三方管理工具 (14.3 RU9 和更新版本)	您不希望 SEP 瀏覽器延伸覆寫其 Web 瀏覽器上的用戶端使用者政策，否則用戶端使用者看不到任何其他延伸。	- 將 SEP 瀏覽器延伸安裝到 Web 瀏覽器上。最常用的方法包括： Chrome：Chrome 瀏覽器雲端管理 請參閱：設定 Chrome 瀏覽器雲端管理 Edge：Microsoft Intune 請參閱：在 Microsoft Intune 中設定 Microsoft Edge 政策 - 在 SEPM 入侵預防政策中同時選擇「啟用瀏覽器入侵預防」和「啟用延伸的第三方管理」選項。 請參閱：步驟 3：在「入侵預防」政策中啟用瀏覽器防護
	您的組織使用 Active Directory 網域。	- 啟動瀏覽器防護。 您無需啟用啟用延伸的第三方管理。 步驟 3：在「入侵預防」政策中啟用瀏覽器防護 - 配置 AD 群組政策物件政策以安裝和管理您的瀏覽器延伸。 您必須將 SEP 瀏覽器延伸新增到延伸清單中。SEP 接著會從 Google Web Store 下載任一延伸。請參閱： 使用 Active Directory 群組原則物件安裝 Chrome 或 Edge 的 Endpoint Protection 瀏覽器延伸 Note: 您在 AD GPO 政策中所架構的項目，其優先順序高於任何安裝方法。如果您先安裝 SEP 用戶端，則 AD GPO 政策會覆寫 SEP 用戶端登錄值。如果您先使用 AD GPO 政策，並且稍後安裝 SEP 用戶端，則用戶端會跳過寫入至登錄，因為它使用 Google Web Store URL。
在以下位置將政策新增至登錄檔：HKEY_CURRENT_USER	您不希望 SEP 瀏覽器延伸覆寫用戶端使用者政策，也不希望使用第三方管理工具安裝和管理瀏覽器延伸。	- 啟動瀏覽器防護。請參閱： 步驟 3：在「入侵預防」政策中啟用瀏覽器防護 - 將機碼新增至登錄檔 HKEY_CURRENT_USER。請參閱： 使用 HKEY_CURRENT_USER 機碼安裝 Chrome 或 Edge 的 Endpoint Protection Browser 延伸

如果您升級瀏覽器，則延伸會保持已安裝狀態。

步驟 3：在「入侵預防」政策中啟用瀏覽器防護

請透過「入侵預防」政策啟用 SEP 瀏覽器延伸，並直接從 Symantec Endpoint Protection Manager 安裝瀏覽器延伸。

NOTE

在 14.3 RU9 或更新版本中，您可以使用第三方管理工具 (而非 Symantec Endpoint Protection Manager) 安裝瀏覽器延伸。如果您使用第三方管理工具，請先安裝瀏覽器延伸，然後按照以下步驟操作。

在「入侵預防」政策中啟用瀏覽器防護

1. 開啟「入侵預防」政策。
2. 在「入侵預防」頁面上，確定勾選下列選項：
 - 啟用 **Windows** 瀏覽器入侵預防
 - 啟用 **URL** 信譽「啟用延伸的第三方管理」選項預設為清除。

若要從第三方管理工具而非 Symantec Endpoint Protection Manager 安裝延伸，請選擇此選項。此選項會移除 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForceList。

如需詳細瞭解這些設定，請參閱：[入侵預防設定](#)

3. 按一下「確定」。

更多資訊

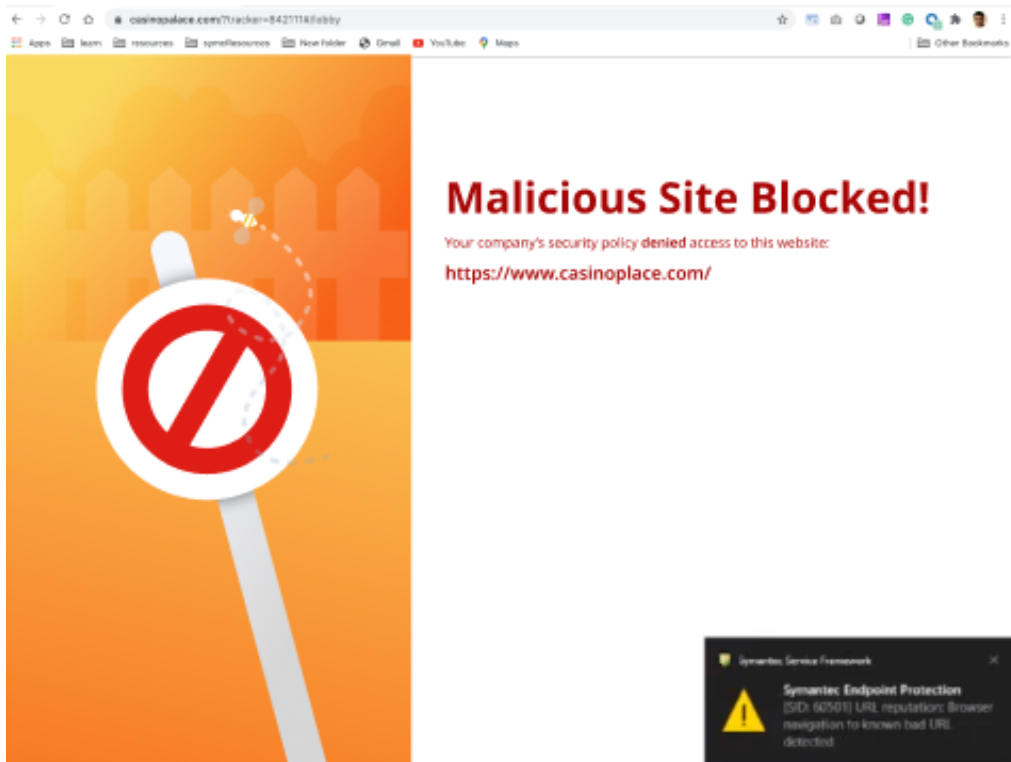
若要驗證是否已正確安裝並啟用瀏覽器延伸，請參閱：[驗證是否已安裝或啟用瀏覽器延伸](#)

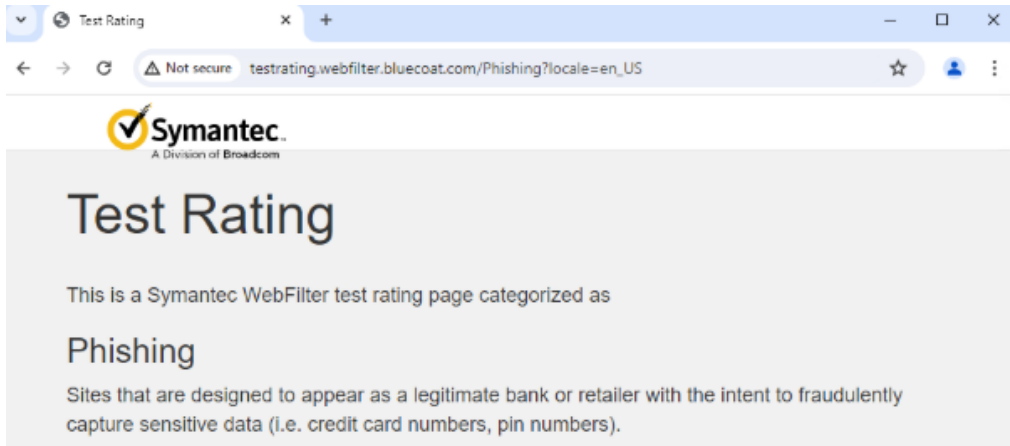
如需詳細瞭解雲端主控台的設定，請參閱：[在 Symantec Endpoint Security 中管理入侵預防](#)

步驟 4：測試 SEP 瀏覽器延伸

1. 將下列任何 URL 貼入支援的 Web 瀏覽器，以查看瀏覽器是否將其攔截。瀏覽器可能會嘗試數次。
 - http://testrating.webfilter.bluecoat.com/Malicious%20Sources/Malnets?locale=en_US
 - http://testrating.webfilter.bluecoat.com/Malicious%20Outbound%20Data/Botnets?locale=en_US
 - http://testrating.webfilter.bluecoat.com/Phishing?locale=en_US
 - <http://www.fakebook.com>

如果 Symantec Endpoint Protection 偵測到惡意 URL，根據您如何設定瀏覽器延伸安裝，您可能會看到以下任一畫面。





2. 檢查用戶端安全日誌，查看是否已記錄偵測。請參閱：

[驗證瀏覽器攻擊偵測的安全日誌](#)

(非必要) 驗證瀏覽器延伸已安裝或啟用

作為疑難排解步驟，您可以驗證瀏覽器延伸是否安裝在用戶端電腦和 Web 瀏覽器上。您也可以驗證瀏覽器延伸是否在 SEPM 和用戶端電腦上都已啟用。

驗證用戶端電腦上瀏覽器延伸的安裝狀態

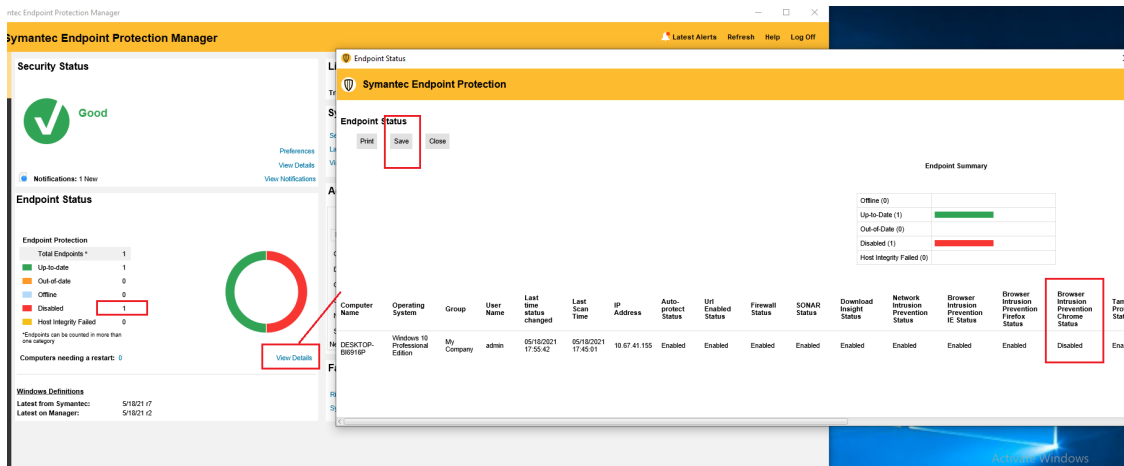
- 在登錄檔查看以下項目：
 - **Chrome**：
 - HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.broadcom.webextbridge
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist (如果啟用延伸的第三方管理選項已清除 [14.3 RU9 或更新版本])
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Symantec\Symantec Endpoint Protection\{965393C7-9C7B-4B0A-BB01-CD0BC8425DEB}\Common Client\PathExpansionMap > WebExtDefs\20210721.023
 - **Edge**：
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Edge\NativeMessagingHosts\com.broadcom.webextbridge
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist (如果啟用延伸的第三方管理選項已清除 [14.3 RU9 或更新版本])
- 檢查 WebExt 資料夾和 updates.xml 檔案是否存在：
C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.4345.2000.105\Data\Definitions\WebExt\20210221.007\updates.xml
- 在 Symantec Endpoint Protection Manager 檢查是否已啟用瀏覽器延伸引擎和定義：
按一下「說明」>「疑難排解」>「版本」>「瀏覽器延伸引擎」和「瀏覽器延伸」。

驗證 Web 瀏覽器上瀏覽器延伸的安裝狀態

- 在 Web 瀏覽器上執行以下步驟：
 - **Chrome**：在 Chrome Web 瀏覽器中，按一下垂直省略符號 > 「設定」> 「延伸」> 「Symantec Endpoint Protection」> 「詳細資料」。尋找版本號碼。
 - **Edge**：在 Microsoft Edge Web 瀏覽器中，按一下垂直省略符號 > 「延伸」> 「Symantec 延伸」。

驗證瀏覽器延伸已啟用

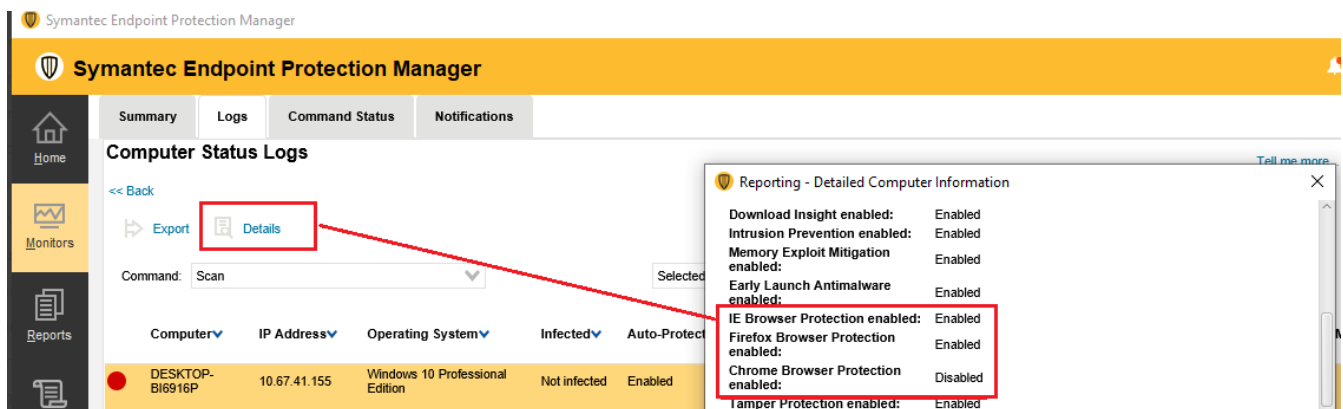
1. 在 Symantec Endpoint Protection 用戶端上，前往以下位置：
 - 每次啟用、停用、安裝或解除安裝瀏覽器延伸或是從瀏覽器移除瀏覽器延伸時，用戶端系統日誌都會顯示事件。
 - 「說明」>「疑難排解」>「版本」>「瀏覽器延伸引擎」和「瀏覽器例外」。
2. 在 Symantec Endpoint Protection Manager，前往以下位置：
 - 「用戶端」頁面 > 「用戶端」標籤 > 「防護技術」檢視會顯示啟用還是停用瀏覽器延伸。
 - 在「首頁」頁面的「端點狀態」下方，選取具有「已停用」狀態的用戶端，然後按一下「詳細資料」。在報告中，檢視已啟用或停用的瀏覽器延伸。按一下「儲存」，以使用 HTML 格式儲存報告。



NOTE

該報告顯示 Chrome 和 Edge 延伸的單一狀態。如果僅安裝一個延伸或出現故障，則狀態將顯示為啟用或故障。

- 在「首頁」頁面的「我的最愛報告」下方，「Symantec Endpoint Protection 每週狀態」報告會顯示已開啟或關閉延伸的用戶端。
- 在「報告」>「快速報告」>「電腦狀態」報告類型 > 「防護內容版本」報告上，按一下「建立報告」。按一下「安全狀態摘要」報告，以查看哪些用戶端具有已停用或未正常運作的瀏覽器延伸或是更新過的瀏覽器延伸定義。
- 「監視器 > 日誌」頁面上，電腦狀態日誌會顯示「Chrome 瀏覽器防護已啟用」欄。按一下「詳細資料」，以取得「瀏覽器延伸定義」的修訂編號。使用此資訊，確定將瀏覽器延伸內容下載到用戶端。



(非必要) 檢視瀏覽器攻擊偵測的安全日誌

若要查看特定的瀏覽器攻擊偵測，請查看 Symantec Endpoint Protection 安全日誌。例如，請參閱以下條目或通知：

-
- Symantec Endpoint Protection [SID: 60501] ##### URL # URL #####<path>
 - ##### PlugX ##### 2 ###<path>
 - [SID: 29565] Web ##### Webpulse #####<path>

瀏覽器延伸常見問答集

問：Windows 用戶端上的瀏覽器防護支援哪些瀏覽器版本？

- Microsoft Edge：最新版本和之前的兩個版本。
- Google Chrome：最新版本和之前的兩個版本。

如需詳細瞭解哪些瀏覽器版本受到支援，請參閱：[Endpoint Protection 中瀏覽器入侵預防支援的瀏覽器](#)

問：瀏覽器延伸是否使用定義？

瀏覽器攻擊偵測需要 Symantec LiveUpdate 所下載的瀏覽器延伸定義、SymPlatform 定義和 IPS 定義。請參閱：

[關於 LiveUpdate 下載的內容類型](#)

問：哪些 IPS 特徵用於 URL 信譽偵測？

- SID 60501 偵測用於瀏覽器型偵測。
- SID 29565 偵測是從非瀏覽器來源觸發。

問：如何停用或解除安裝 Chrome 或 Edge 瀏覽器延伸？

您應該一律保持瀏覽器延伸的已安裝和已啟用狀態來進行防護。不過，如果您必須對瀏覽器問題進行疑難排解，則可以停用或解除安裝瀏覽器延伸。

您可以透過在入侵預防政策中取消勾選「啟用 Windows 瀏覽器入侵預防」來停用瀏覽器延伸。停用此選項會卸載安裝在用戶端電腦上的 Chrome 瀏覽器延伸或 Microsoft Edge 延伸。重新啟用這些選項即會重新載入該延伸。重新載入該延伸可能需要一些時間。

WebFilter 和掃描程式這類 WebExt 功能已予以停用，但保持已安裝狀態。如果您停用 WebExt 功能的任何部分，則會停用整個功能的防護。

您可以使用下列方法來解除安裝 Chrome 或 Edge 瀏覽器延伸：

- 停用 IPS 政策，以從所有瀏覽器解除安裝延伸。
- 從 AD GPO 政策中移除 Google Chrome 或 Microsoft Edge 項目，以解除安裝瀏覽器延伸。在 14.3 RU9 或更新版本中，如果延伸是由第三方管理工具安裝，請將其卸載。
- 解除安裝 SEP 用戶端。
- 在沒有「入侵預防」元件的情況下重新安裝 SEP 用戶端。
- 執行 CleanWipe。CleanWipe 會解除安裝 Symantec Endpoint Protection 用戶端和任一瀏覽器延伸。

疑難排解和已知問題

您可以執行 Symantec Diagnostic Tool (SymDiag) 來收集以下瀏覽器延伸相關資訊：

- .SDBZ 檔案。SymDiag 會取得您電腦的快照，並在一個副檔名為 .SDBZ 的檔案中記錄資料。
- WPP 日誌中的非預期偵測相關資訊。

若要啟動 SymDiag，請在用戶端按一下「說明」>「下載 Symantec Diagnostic Tool」。請參閱：

如需詳細瞭解如何疑難排解瀏覽器延伸問題，請參閱：

[透過 SymDiag 收集支援案例的資料](#)

已知問題

- 下表顯示安裝時遇到以及可能使用瀏覽器延伸的最常見問題。若要允許非託管用戶端存取整個網站，請將被封鎖的網域新增到受信任主機清單中。請參閱：

關於排除掃描項目

- 如果非託管客戶端偵測到惡意 URL，Edge 延伸將封鎖整個網站。Chrome 延伸僅會封鎖惡意 URL。
- 如果您使用第三方開發人員工具並封鎖原生訊息，則 SEP 瀏覽器延伸將顯示其已安裝但無法運作。若要解決此問題，請將以下機碼新增到登錄檔：

```
HKEY_CURRENT_USER\Software\Policies\Google\Chrome\NativeMessagingAllowlist 1 =  
'com.broadcom.webextbridge'
```

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Edge\NativeMessagingAllowlist 1 =  
'com.broadcom.webextbridge'
```

更多資訊

Chrome：[NativeMessagingBlocklist](#)

Edge：[Microsoft Policies - NativeMessagingBlocklist](#)

[CRE-17244]

- Symantec Endpoint Protection Manager 安裝 Chrome 和 Edge 瀏覽器的延伸時會追蹤每個端點上的成功和失敗。如果啟用「啟用延伸的第三方管理」選項，且您使用第三方工具安裝延伸，Symantec Endpoint Protection Manager 可能無法偵測到安裝是否失敗。反之，延伸會錯誤顯示其已成功安裝。此問題將在未來的版本中解決。[INFODEVSEP-74]
- 如果已啟用 Chrome Incognito 模式（預設予以停用），則用戶端不會攔截惡意 URL。若要在 Google Chrome Web 瀏覽器中停用此模式，請按一下垂直省略符號 > 「設定」> 「延伸」> 「Symantec Endpoint Protection」> 「詳細資料」，並關閉「在 Incognito 中允許」。
- 如果您使用 IPv4 或 IPv6 位址來新增信任的 Web 網域例外 URL，則 Chrome 延伸無法辨識該位址。
- 當您停止用戶端服務時，Chrome 瀏覽器延伸仍然會執行，但用戶端不會在安全性日誌中產生事件。
- Symantec Endpoint Protection 用戶端啟動時，會執行 Web 延伸。不過，用戶端未針對允許或攔截的 URL 產生任何通知或日誌時，會有較短的時段。[MI-4947]

使用 HKEY_CURRENT_USER 機碼安裝 Chrome 或 Edge 的 Endpoint Protection Browser 延伸

在入侵防護政策中停用「在 Symantec Endpoint Protection Manager 之外安裝和管理瀏覽器延伸」選項時，您可以向 HKEY_CURRENT_USER 登錄檔新增一個機碼，來安裝 SEP 瀏覽器延伸。

請使用此方法安裝 SEP 瀏覽器延伸，以讓用戶端使用者可以安裝其他瀏覽器延伸。如果您沒有第三方管理工具（如 Chrome 瀏覽器雲端管理），則可以使用此方法。

使用 HKCU 機碼安裝 Chrome 或 Edge 的 Endpoint Protection Browser 延伸

1. 在用戶端電腦上的 Google Chrome 瀏覽器中，輸入 `chrome://policy`。
在「chrome://policy」頁面上，將顯示以下值：政策名稱 `ExtensionInstallForcelist`、其值（`pamolibmfekbnkdmfabpjbfbffbec`）、來源欄位設為「平台」，應用於欄位設為「機器」。

← → Chrome chrome://policy

Policies

Filter policies by name

Reload policies More actions Show policies with no value set

Status

Google Update

Version: 124.0.6359.0

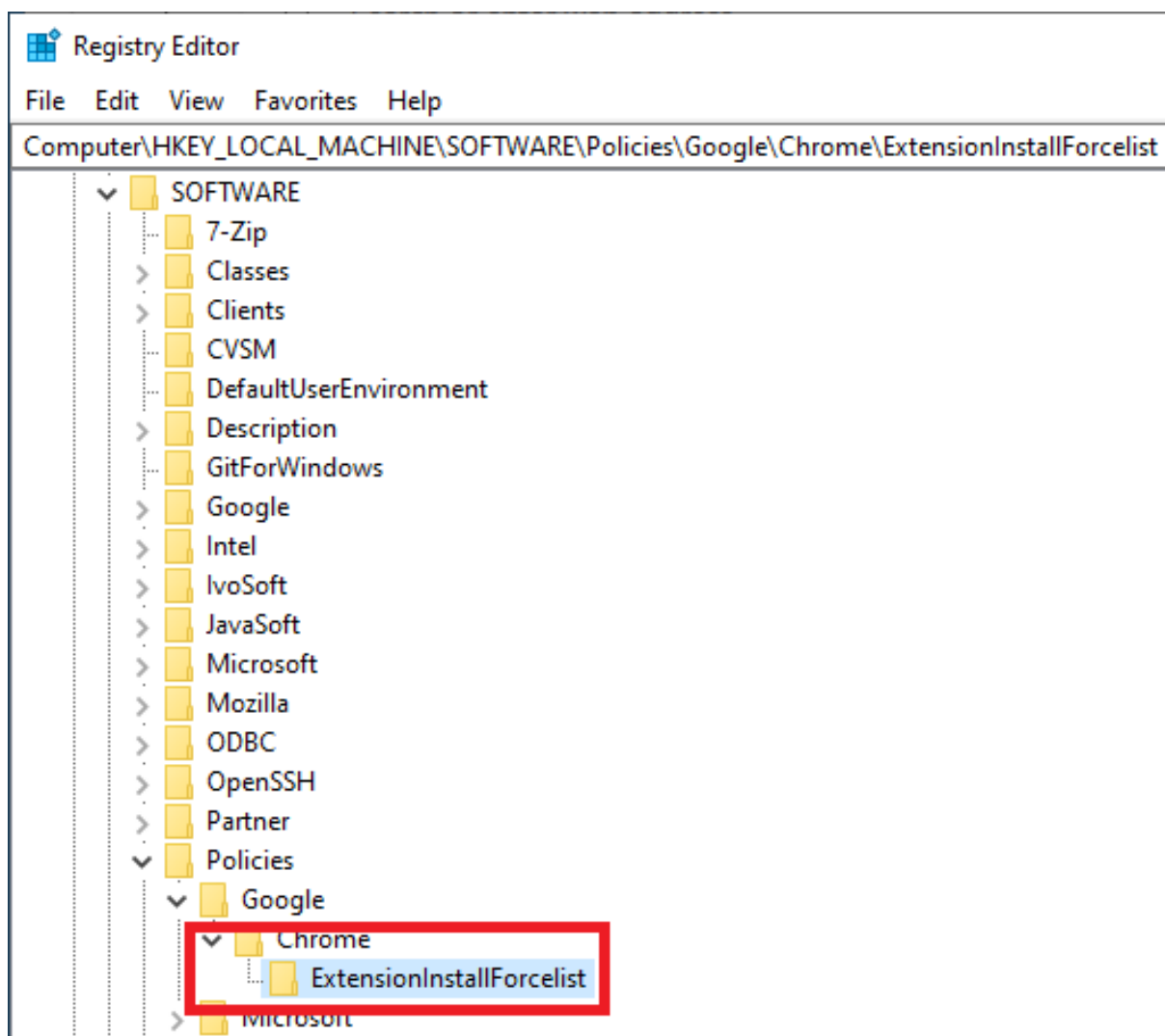
Enrollment domain: Broadcom.net

Last policy timestamp: 2 hours ago

Chrome Policies

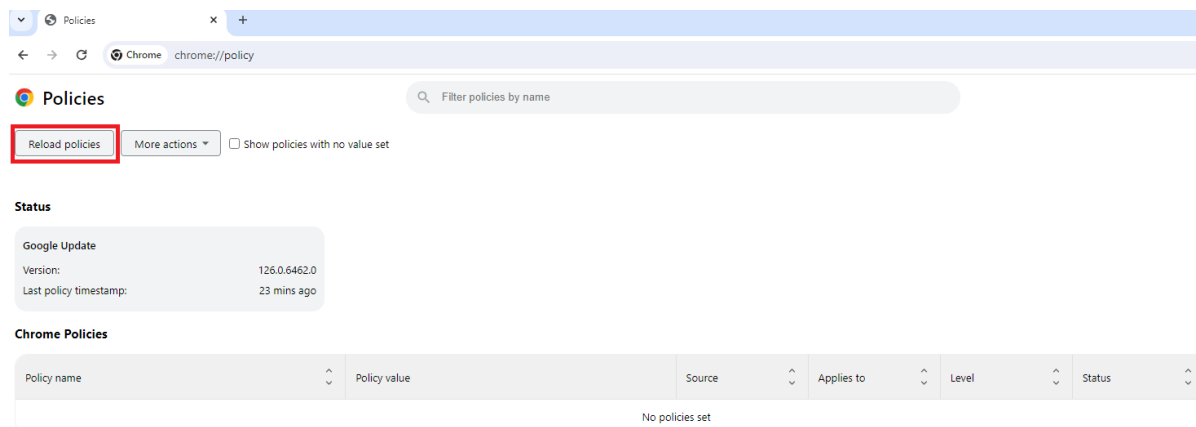
Policy name	Policy value	Source	Applies to	Level	Status
ExtensionInstallForcelist	["miinejh1lmkpdosimnoncd1liejpdk;https://clients2.google.com/..."]	Platform	Machine	Mandatory	OK

2. 在登錄檔刪除 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist。

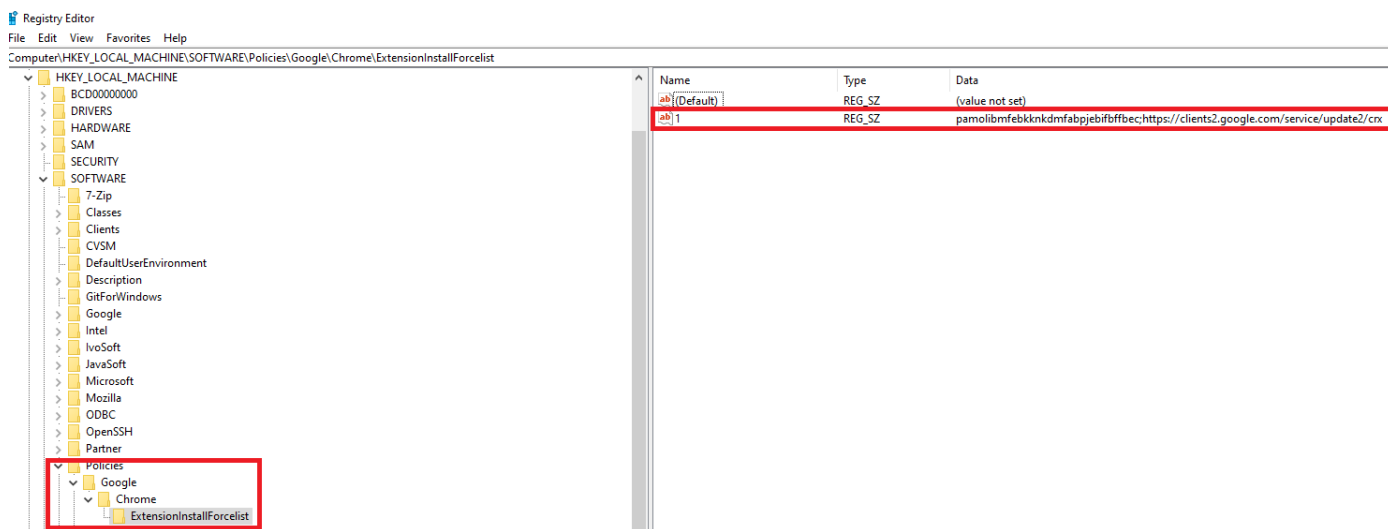


3. 在 chrome://policy 頁面，按一下「重新載入政策」。

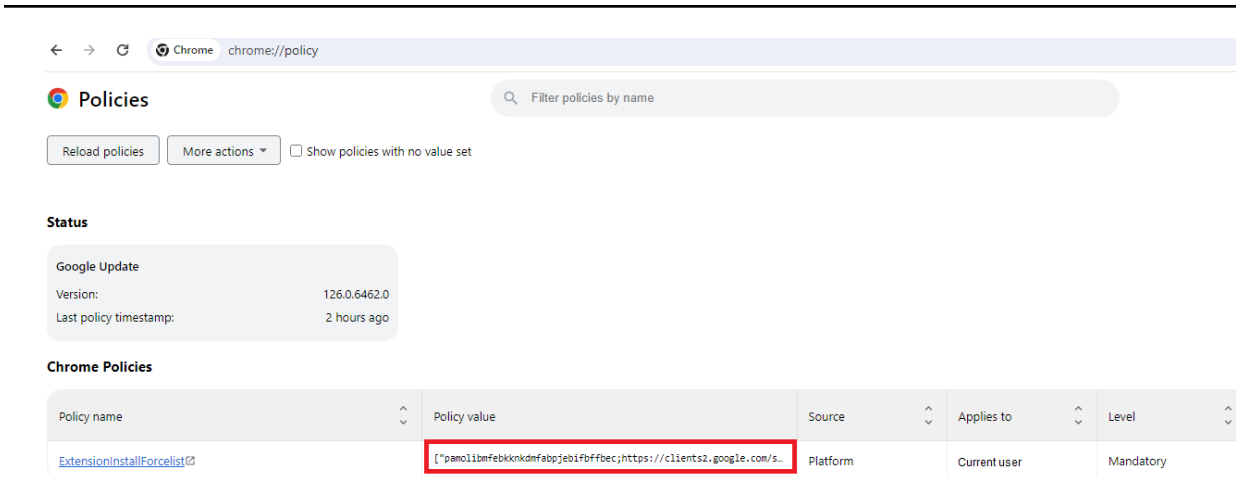
ExtensionInstallForcelist 政策即消失。



4. 透過以下值建立以下登錄機碼 HKEY_CURRENT_USER\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist :
- 字串值 = 1
 - 值資料 = pamolibmfebkkndmfabpjbefibfbfbec;https://clients2.google.com/service/update2/crx



5. 在 chrome://policy 頁面，按一下「重新載入政策」。
- ExtensionInstallForcelist 政策以下列值重新顯示：來源欄位設為「平台」，應用於欄位設為「目前使用者」。



更多資訊

有關設定瀏覽器延伸的資訊，請參閱：[整合瀏覽器延伸和 Symantec Endpoint Protection \(SEP\)，防止惡意網站](#)

如需詳細瞭解雲端主控台的設定，請參閱：[在 Symantec Endpoint Security 中管理入侵預防](#)

設定排除的電腦清單

網路入侵防護和防火牆支援排除的主機。

您可以設定電腦清單，針對這些電腦，用戶端不會比對攻擊特徵，或是檢查是否有通訊埠掃描或受到阻絕服務攻擊。網路入侵預防和點對點驗證允許來自排除的主機清單中主機的任何來源流量。不過，網路入侵預防和點對點驗證會繼續評估送往清單中主機的任何目的地流量。此清單會套用至入埠和離埠流量，但僅適用於流量的來源。此清單也僅適用於遠端 IP 位址。

例如，您可能還要排除一些電腦，允許 Internet 服務供應商掃描您網路中的通訊埠，以確保遵從其服務合約。或者，您可以將內部網路的某些電腦設為測試用途。

NOTE

您也可以設定電腦清單，在 IPS 特徵未偵測到攻擊時允許這些電腦的所有入埠流量和離埠流量。在此情況下，您可以建立允許所有主機的防火牆規則。

設定排除的電腦清單

1. 在主控台中，開啟某個入侵預防政策。
2. 在政策頁面上，按下「入侵預防」。
3. 勾選「啟用排除的主機」（若尚未勾選），再按下「排除的主機」。
4. 在「排除的主機」對話方塊中，勾選您要從網路入侵防護中排除的所有主機群組旁邊的「已啟用」。請參閱：[攔截來往於特定伺服器的流量](#)
5. 若要新增您要排除的主機，請按下「新增」。
6. 在「主機」對話方塊的下拉式清單中，選取下列其中一種主機類型：
 - IP 位址
 - IP 位址範圍
 - 子網路
7. 針對所選取的主機類型，輸入與其關聯的適當資訊。

如需這些選項的詳細資訊，請按一下「說明」。

-
8. 按下「確定」。
 9. 重複步驟 5，然後按一下「確定」，將其他裝置和電腦新增至排除的電腦清單。
 10. 若要編輯或刪除任何排除的主機，請選取某一行，再按下「編輯」或「刪除」。
 11. 按下「確定」。
 12. 架構完此政策後，按下「確定」。

針對入侵預防和記憶體攻擊緩和架構用戶端通知

根據預設，當用戶端偵測到入侵防護事件和記憶體攻擊緩和時，用戶端電腦上會顯示通知。這些通知啟用時，通知會顯示標準訊息。針對 IPS 通知，您可以在標準訊息中加入自訂的文字。

針對入侵預防和記憶體攻擊緩和架構用戶端通知

1. 在主控台中，按一下「用戶端」，然後在「用戶端」下方選取群組。
2. 在「政策」標籤的「位置限定的政策與設定」下，展開某位置下方的「位置限定的設定」。
3. 在「用戶端使用者介面控制設定」右側，按一下「工作」，然後按一下「編輯設定」。
4. 在「**group name** 的用戶端使用者介面控制設定」對話方塊中，按一下「伺服器控制」或「混合控制」。
5. 在「混合控制」或「伺服器控制」旁邊，按一下「自訂」。

如果您按一下「混合控制」，請在「用戶端/伺服器控制設定」標籤的「顯示/隱藏入侵防護通知」旁邊按一下「伺服器」。然後按一下「用戶端使用者介面設定」標籤。

6. 在「用戶端使用者介面設定」對話方塊或標籤中，按一下「顯示入侵預防和記憶體攻擊緩和通知」。
7. 若要在通知出現時啟用音效，請按一下「通知使用者時使用音效」。
8. 按下「確定」。
9. 按下「確定」。

更多資訊

- [管理入侵預防](#)
- [使用記憶體攻擊緩和政策強化 Windows 用戶端防範記憶體竄改攻擊](#)
- [設定管理員通知](#)

關於賽門鐵克 IPS 特徵

根據預設，會在用戶端上安裝賽門鐵克入侵預防特徵。

入侵預防使用賽門鐵克特徵來監控各個封包或封包串流。對於封包串流，入侵預防能記住以前封包的型樣或部分型樣清單。然後，會將此資訊應用於後續的封包檢查。

Symantec 特徵會下載至用戶端作為 LiveUpdate 內容的一部分。對於 Mac 電腦，存在一些內建到軟體的其他網路入侵預防特徵。

NOTE

Symantec 會根據其研究或公開資訊建立特徵。

在 Windows 電腦上，LiveUpdate 內容還包括瀏覽器入侵預防的特徵。

網路入侵預防特徵	網路特徵會比對可導致應用程式當機或利用用戶端電腦上作業系統漏洞的攻擊型樣。您可以變更賽門鐵克網路特徵攔截或允許通訊。您也可以變更 Symantec Endpoint Protection 是否應在安全日誌中記錄根據特徵的偵測。
瀏覽器防護特徵 (僅限 Windows) (瀏覽器入侵預防)	瀏覽器特徵會比對支援瀏覽器上的攻擊型樣 (例如，可導致瀏覽器當機的程序檔)。您無法自訂瀏覽器特徵的動作或日誌設定，但可以排除瀏覽器特徵。您可以將瀏覽器防護架構為記錄瀏覽器偵測但不攔截它們。此動作可協助您識別可能需要排除的那些瀏覽器特徵。在建立特徵排除之後，請停用只記錄模式。

賽門鐵克安全機制應變中心團隊提供攻擊特徵。根據預設，會在用戶端上安裝入侵預防引擎和相應的特徵集。特徵是您在用戶端上更新的部分內容。

更多資訊

- 如需攻擊特徵的 Symantec 資料庫，請參閱：[攻擊特徵](#)
- 如需 Microsoft 漏洞的 Symantec IPS 特徵相關資訊，請參閱：[Symantec 端點對 Microsoft 每月安全公告的回應](#)
- 如需 Mac 用戶端的內建 IP 特徵相關資訊，請參閱：[Symantec Endpoint Protection IPS for Mac 的內建特徵](#)
- [為 IPS 特徵建立例外](#)

為 IPS 特徵建立例外

您可以使用例外變更賽門鐵克 IPS 特徵的行為。

對於 Windows 和 Mac 電腦，您可以變更 IPS 辨識網路特徵時用戶端所採取的動作。您也可以變用戶端是否將事件記錄至「安全日誌」。

對於 Windows 電腦，您無法變更賽門鐵克瀏覽器特徵的行為；與網路特徵不同，瀏覽器特徵不允許自訂動作和記錄設定。然而，您可以建立瀏覽器特徵的例外，以便用戶端略過該特徵。

NOTE

當您新增瀏覽器特徵例外時，Symantec Endpoint Protection Manager 會將該特徵包含到例外清單中，並自動將動作設定為「允許」，將日誌設定設為「不記錄」。您無法自訂動作或日誌設定。

如需詳細資訊，請參閱：

[管理入侵預防](#)

NOTE

若要變更您建立或匯入之自訂 IPS 特徵，您可以直接編輯該特徵。自訂特徵僅支援在 Windows 電腦上使用。

建立 IPS 特徵例外

1. 在主控台中，開啟某個入侵預防政策。
2. 在「**Windows** 設定」或「**Mac** 設定」下方，按下「例外」，然後按下「新增」。

NOTE

特徵清單會以管理主控台下載的最近 LiveUpdate 內容填入。對於 Windows 電腦，如果管理伺服器尚未下載內容，則此清單顯示為空白。對於 Mac 電腦，此清單一律至少包含內建特徵，這些特徵已自動安裝在 Mac 用戶端上。

3. 在「新增入侵預防例外」對話方塊中，執行下列動作以過濾特徵：
 - (僅限 Windows) 若只要顯示特定類別的特徵，請從「顯示類別」下拉式清單中選取選項。如果您選取「瀏覽器防護」，特徵動作選項會自動變更為「允許」和「不記錄」。
 - (Windows 和 Mac) 若要顯示按特定嚴重性分類的特徵，請從「顯示嚴重性」下拉式清單中選取選項。

-
4. 選取一個或多個特徵。
若要為所有特徵設定相同行為，請按下「全選」。
 5. 按「下一步」。
 6. 在「特徵動作」對話方塊中，設定下列選項，然後按下「確定」。
 - 將「動作」設定為「攔截」或「允許」。
 - 將「記錄」設定為「記錄流量」或「不記錄流量」。

NOTE

這些選項只適用於網路特徵。如果是瀏覽器特徵，請按下「確定」。

如果您要將特徵的行為轉化成原始行為，請在「例外」清單中選取此特徵，然後按下「刪除」。

7. 按下「確定」儲存政策變更。

更多資訊

[管理 Symantec Endpoint Protection 中的例外](#)

關於自訂 IPS 特徵

您可以建立自己的 IPS 網路特徵。這些特徵以封包為基礎。

與賽門鐵克特徵不同的是，自訂特徵只會掃描單一封包酬載。但是，自訂特徵可偵測到 TCP/IP 堆疊中速度比賽門鐵克特徵快的攻擊。

封包式特徵會檢查單一封包是否符合規則。規則根據各種準則（如通訊埠、通訊協定、來源或目的 IP、TCP 旗標號碼或應用程式）而制定。例如，自訂特徵可監控收到的資訊封包中是否有 GET / cgi-bin/phf? 中的字串 phf，該字串表示 CGI 程式攻擊。每個封包都要經過評估，看是否具有該特定型樣。如果流量的封包符合規則，則用戶端會允許或攔截該封包。

您可以指定 Symantec Endpoint Protection 是否在封包日誌中記錄根據自訂特徵的偵測。

NOTE

您必須安裝並啟用防火牆，才能使用自訂 IPS 特徵。請參閱：

[選擇要在用戶端上安裝哪些安全性功能](#)

自訂特徵僅支援在 Windows 電腦上使用。請參閱：

[管理自訂入侵預防特徵](#)

管理自訂入侵預防特徵

您可以自行撰寫網路入侵預防特徵來識別特定入侵，並減少特徵導致誤報的可能性。您在自訂特徵加入的資訊愈多，特徵就愈有效。

WARNING

在制訂入侵預防特徵之前，您應該熟悉 TCP、UDP 或 ICMP 通訊協定。格式不正確的特徵可能會損毀自訂特徵庫及用戶端的完整性。

NOTE

您必須安裝並啟用防火牆，才能使用自訂 IPS 特徵。請參閱：

[選擇要在用戶端上安裝哪些安全性功能](#)

Table 68: 管理自訂入侵預防特徵

工作	說明
建立含有特徵群組的自訂特徵庫	若要包含自訂特徵,必須建立自訂特徵庫。建立自訂特徵庫時,可以使用特徵群組,以便更輕鬆地管理特徵。必須將至少一個特徵群組新增至自訂特徵庫,才能新增特徵。請參閱： 關於自訂 IPS 特徵 建立自訂 IPS 特徵庫
將自訂 IPS 特徵新增至自訂特徵庫	您可以將自訂 IPS 特徵新增至自訂特徵庫中的特徵群組。請參閱： 將特徵新增至自訂 IPS 特徵庫
將特徵庫指派給用戶端群組	您可以將自訂特徵庫指派給用戶端群組而不是某個位置。請參閱： 指派多個自訂 IPS 特徵庫至群組
變更特徵的順序	入侵預防會使用第一個規則比對。Symantec Endpoint Protection 會按特徵在特徵清單中列出的順序檢查特徵。 例如,如果您新增一個特徵群組來攔截目的通訊埠 80 的雙向 TCP 流量,可以新增以下特徵： - 攔截通訊埠 80 的所有流量。 - 允許通訊埠 80 的所有流量。 如果「攔截所有流量」特徵列出在前面,「允許所有流量」特徵永遠不會套用。如果「允許所有流量」特徵列出在前面,「攔截所有流量」特徵永遠不會套用,且會永遠允許所有 HTTP 流量。 Note: 防火牆規則會優先於入侵預防特徵。 如需詳細資訊,請參閱： 變更自訂 IPS 特徵的順序
複製並貼上特徵	您可以在群組之間和特徵庫之間複製和貼上特徵。
定義特徵的變數	新增自訂特徵時,可以使用變數來代表特徵中的可變資料。如果資料變更,您可以編輯變數,無須編輯整個特徵庫中的特徵。請參閱： 定義自訂 IPS 特徵的變數
測試自訂特徵	您應該測試自訂入侵預防特徵以確保它們可以正常運作。請參閱： 測試自訂 IPS 特徵

建立自訂 IPS 特徵庫

您可以建立自訂 IPS 特徵庫以包含您的自訂 IPS 特徵。請參閱：

[管理自訂入侵預防特徵](#)

建立自訂 IPS 特徵庫

1. 在主控台中的「政策」頁面上,在「政策」下按下「入侵預防」。
2. 按下「自訂入侵預防」標籤。
3. 在「工作」下,按下「新增自訂入侵預防特徵」。
4. 在「自訂入侵預防特徵」對話方塊中,鍵入特徵庫的名稱和 (選擇性) 敘述。
NetBIOS Group 是特徵群組範例,其中有一個特徵範例。您可以編輯現有群組或新增群組。
5. 若要增加新群組,請在「特徵」標籤的「特徵群組」清單下,按下「新增」。
6. 在「入侵預防特徵群組」對話方塊中,鍵入群組名稱和 (選擇性) 敘述,然後按下「確定」。

群組預設為啟用。如果啟用特徵群組,該群組內的所有特徵會自動啟用。若要保留群組供參考但要停用它,請取消勾選「啟用這個群組」。

7. 新增自訂特徵。請參閱：

[將特徵新增至自訂 IPS 特徵庫](#)

將特徵新增至自訂 IPS 特徵庫

您可以將自訂入侵預防特徵新增至新的或現有自訂 IPS 特徵庫。請參閱：

管理自訂入侵預防特徵

新增自訂特徵

1. 建立自訂 IPS 特徵庫。請參閱：

建立自訂 IPS 特徵庫

2. 在「特徵」標籤的「此群組的特徵」下,按下「新增」。
3. 在「新增特徵」對話方塊中,輸入特徵的名稱和選用敘述。
4. 在「嚴重性」下拉式清單中,選取嚴重性等級。
符合特徵條件的事件將會記錄為此嚴重性等級。
5. 在「方向」下拉式清單中,指定要特徵檢查的流量方向。
6. 在「內容」欄位中,鍵入特徵的語法。

例如,某些常見通訊協定的特徵使用下列語法：

HTTP	<pre>rule tcp, dest=(80,443), saddr=\$LOCALHOST, msg="MP3 GET in HTTP detected", regexcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 ."</pre>
FTP	<pre>rule tcp, dest=(21), tcp_flag&ack, saddr=\$LOCALHOST, msg="MP3 GET in FTP detected", regexcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"</pre>

如需語法的詳細資訊,請按下「說明」。請參閱：

自訂入侵預防特徵的語法

7. 如果您要應用程式觸發特徵,請按下「新增」。
8. 在「新增應用程式」對話方塊中,輸入應用程式的檔案名稱和選用敘述。
例如,若要新增應用程式 Internet Explorer,請將檔案名稱鍵入為 `iexplore` 或 `iexplore.exe`。如果不指定檔案名稱,任何應用程式都可以觸發特徵。
9. 按下「確定」。
新增的應用程式預設為啟用。如果要停用應用程式稍後再啟用,請取消勾選「已啟用」欄的核取方塊。
10. 在「動作」群組方塊中,選取特徵偵測到事件時用戶端要採取的動作:

攔截	識別並攔截事件或攻擊,並且記錄在安全日誌中
允許	識別並允許事件或攻擊,並且記錄在安全日誌中

11. 若要將事件或攻擊記錄在封包日誌中,請勾選「寫入至封包日誌」。
12. 按下「確定」。

新增的特徵預設為啟用。如果要停用特徵稍後再啟用,請取消勾選「已啟用」欄的核取方塊。

13. 您可以新增其他特徵。完成之後,按下「確定」。
14. 如果系統提示您,請指派自訂 IPS 特徵給群組。

您也可以將多個自訂 IPS 程式庫指派給群組。請參閱：

變更自訂 IPS 特徵的順序

自訂特徵的 IPS 引擎會按照特徵清單中的特徵列示順序來檢查特徵。每個封包只會觸發一個特徵。當入埠或離埠流量封包有符合的特徵時，IPS 引擎就會停止檢查其他特徵。如此，IPS 引擎才能以正確的順序執行特徵。您可以在特徵清單中變更特徵的順序。如果有多個相符的特徵，請將優先順序較高的特徵移至頂端。

例如，如果您新增一個特徵群組來攔截目的通訊埠 80 的雙向 TCP 流量，可以新增以下特徵：

- 攔截通訊埠 80 的所有流量。
- 允許通訊埠 80 的所有流量。

如果「攔截所有流量」特徵列出在前面，「允許所有流量」特徵永遠不會套用。如果「允許所有流量」特徵列出在前面，「攔截所有流量」特徵永遠不會套用，且會永遠允許所有 HTTP 流量。

NOTE

防火牆規則會優先於入侵預防特徵。

如需詳細資訊，請參閱：

管理自訂入侵預防特徵

變更自訂 IPS 特徵的順序

1. 開啟自訂 IPS 特徵庫。
2. 在「特徵」標籤的「此群組的特徵」表格中，選取要移動的特徵，然後執行下列其中一個動作：
 - 若要先處理此特徵再處理其上面的特徵，請按下「上移」。
 - 若要在處理此特徵前先處理其下面的特徵，請按下「下移」。
3. 架構完此特徵庫後，請按下「確定」。

定義自訂 IPS 特徵的變數

新增自訂 IPS 特徵時，可以使用變數來代表特徵中的可變資料。如果資料變更，您可以編輯變數，無須編輯整個特徵庫中的特徵。請參閱：

管理自訂入侵預防特徵

您必須先定義特徵的變數，然後才能使用。自訂特徵庫中所定義的變數，可以用於該特徵庫中的任何特徵。

建立內容時，您可以複製並貼上現有範例變數，然後繼續編輯。

定義自訂 IPS 特徵的變數

1. 建立自訂 IPS 特徵庫。
[建立自訂 IPS 特徵庫](#)
2. 在「自訂入侵預防特徵」對話方塊中，按下「變數」標籤。
3. 按一下「新增」。
4. 在「新增變數」對話方塊中，鍵入變數的名稱和選擇性敘述。
5. 新增變數值的內容字串，最多 255 個字元。
輸入變數內容字串時，應遵從的語法與輸入特徵內容值使用的語法相同。
[自訂入侵預防特徵的語法](#)
6. 按下「確定」。
變數新增至表格後，您就可以將該變數用於此自訂特徵庫中的任何特徵。

在自訂 IPS 特徵中使用變數

1. 在「特徵」標籤上，新增或編輯特徵。
2. 在「新增特徵」或「編輯特徵」對話方塊中，於「內容」欄位鍵入變數名稱，前面加上貨幣符號 (\$)。
例如，若要建立名為 HTTP 的變數，用來指定 HTTP 連接埠，請鍵入：
\$HTTP
3. 按下「確定」。
4. 架構完此特徵庫後，請按下「確定」。

指派多個自訂 IPS 特徵庫至群組

建立自訂 IPS 特徵庫之後，您可將它指派給群組而非個別位置。您可以稍後再將其他自訂 IPS 程式庫指派給群組。請參閱：

管理自訂入侵預防特徵

指派多個自訂 IPS 特徵庫至群組

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，選取要將自訂特徵指派到的群組。
3. 在「政策」標籤的「與位置無關的政策與設定」下方，按下「自訂入侵預防」。
4. 在「用於 **group name** 的自訂入侵預防」對話方塊中，針對要指派至該群組的每個自訂 IPS 程式庫，勾選「已啟用」欄中的核取方塊。
5. 按下「確定」。

測試自訂 IPS 特徵

在建立自訂 IPS 特徵後，應測試它們以確保可正常發揮作用。

Table 69: 測試自訂 IPS 特徵

步驟	說明
步驟 1：確保用戶端使用目前政策	用戶端下次收到政策時，該用戶端會套用新的自訂特徵。請參閱： 更新用戶端政策
步驟 2：測試用戶端上的特徵內容	應該測試您要在用戶端電腦上攔截的流量。 例如，如果您的自訂 IPS 特徵應攔截 MP3 檔案，則嘗試將某些 MP3 檔案下載到用戶端電腦。如果在多次嘗試後，下載未執行或逾時，則表示自訂 IPS 特徵成功。 可以按下「說明」，瞭解有關可在自訂 IPS 特徵中使用的語法詳細資訊。請參閱： 自訂入侵預防特徵的語法
步驟 3：檢視 Symantec Endpoint Protection Manager 中攔截的事件	可以在防網路和主機侵入攻擊日誌中檢視事件。在自訂 IPS 特徵中指定的訊息會出現在此日誌中。 請參閱： 監控 Symantec Endpoint Protection 用戶端

更多資訊

管理自訂入侵預防特徵

使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊

如需詳細資訊，請參考下列各節：

-
- [記憶體攻擊緩和如何保護應用程式？](#)
 - [侵入防護的類型](#)
 - [記憶體攻擊緩和的需求](#)
 - [修正和防止誤報](#)
 - [尋找記憶體攻擊緩和事件的日誌和報告](#)
 - [稽核已終止應用程式的防護](#)

記憶體攻擊緩和如何保護應用程式？

Symantec Endpoint Protection 包括記憶體攻擊緩和，其使用多種緩和技術來停止對軟體中已知和未知弱點的攻擊嘗試。例如，當用戶端使用者執行 Internet Explorer 之類應用程式時，侵入可能改為啟動包含惡意程式碼的其他應用程式。

為了阻止侵入，記憶體攻擊緩和會將 DLL 插入至受保護的應用程式。在記憶體攻擊緩和偵測到侵入嘗試之後，它會攔截侵入或終止侵入所威脅的應用程式。Symantec Endpoint Protection 會對用戶端電腦上的使用者顯示有關偵測的通知，並且在用戶端的安全日誌中記錄事件。

例如，用戶端使用者可能會看見以下通知：

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

記憶體攻擊緩和會繼續攔截侵入或終止應用程式，直到用戶端電腦執行已修正弱點的軟體版本為止。

侵入防護的類型

記憶體攻擊緩和使用多種類型的緩和技術來處理侵入，端視該類型的應用程式最適合的技術為何。例如，StackPvt 和 RopHeap 技術會攔截攻擊 Internet Explorer 的侵入。請參閱：

[Symantec Endpoint Protection 記憶體攻擊緩和技術](#)

NOTE

如果您已在電腦上啟用 Microsoft App-V 功能，記憶體攻擊緩和不會保護 App-V 所保護的 Microsoft Office 程序。

記憶體攻擊緩和的需求

只有在已安裝入侵預防的情況下，才能使用記憶體攻擊緩和。記憶體攻擊緩和有自己的一組獨立特徵，這些特徵會隨入侵預防定義檔一起下載。不過，您可以獨立地啟用或停用入侵預防和記憶體攻擊緩和。

此外，您必須至少執行 LiveUpdate 一次，應用程式清單才會出現在記憶體攻擊緩和和政策中。根據預設，出現在政策中的所有應用程式均啟用防護。請參閱：

[確認 Symantec Endpoint Protection Manager 具有最新內容](#)

修正和防止誤報

記憶體攻擊緩和偶爾會意外終止用戶端電腦上的應用程式。如果您判斷應用程式的行為是合法並且未被侵入，偵測即為誤報。針對誤報，您應該停用防護，直到賽門鐵克安全機制應變中心變更記憶體攻擊緩和的行為為止。

下表顯示處理誤報偵測的步驟。

Table 70: 尋找和修正誤報的步驟

工作	
步驟 1：找出用戶端電腦上非預期終止的應用程式。	您可以使用下列方式找出用戶端電腦上終止的應用程式： - 用戶端電腦上的使用者通知您某個應用程式未執行。 - 開啟記憶體攻擊緩和日誌或報告，其中列出哪項緩和技術終止了用戶端電腦上的應用程式。 Note: 由於侵入的本質，有時緩和技術不會產生日誌。 如需詳細資訊，請參閱： 尋找記憶體攻擊緩和事件的日誌和報告
步驟 2：停用防護並稽核終止應用程式的技術。	先將防護停用在最低層級，使得其他處理程序保持受到保護。請勿關閉記憶體攻擊緩和，以允許應用程式執行，直到您已嘗試所有其他方法為止。 在以下每個子工作之後，前往步驟 3。 - 首先，稽核緩和技術所終止的特定應用程式的防護。 例如，如果 Mozilla Firefox 已終止，您會停用 SEHOP 技術或 HeapSpray 技術。由於侵入的本質，有時緩和技術不會建立日誌事件，因此，您無法確定哪項緩和技術終止了應用程式。在此情況下，您應該停用保護該應用程式的每項技術，一次一項，直到您找出造成終止的技術為何。 - 稽核單一緩和技術保護的所有應用程式的防護。 - 稽核所有應用程式的防護，而不論技術為何。此選項類似於停用記憶體攻擊緩和，除了管理伺服器會為偵測收集日誌事件。 如需詳細資訊，請參閱： 稽核已終止應用程式之緩和技術的防護
步驟 3：更新用戶端電腦上的政策並重新執行應用程式。	- 如果應用程式正確執行，該緩和技術的偵測即為誤報。 - 如果應用程式未以您預期的方式執行，該偵測即為檢出。 - 如果應用程式仍終止，請在層級限制的層級上稽核。例如，稽核不同的緩和技術或技術保護的所有應用程式。 如需詳細資訊，請參閱： 在 Windows 用戶端上更新安全政策
步驟 4：報告誤報並為檢出重新啟用防護。	針對誤報偵測： - 將偵測是誤報一事通知賽門鐵克團隊。請參閱： 塞門鐵克行家秘訣：成功提交！ - 透過將每項技術的動作設定為「否」，針對終止的應用程式保持停用防護。 - 在安全機制應變解決問題之後，透過將技術的動作變更為「是」重新啟用防護。 針對檢出偵測： - 透過將該緩和技術規則的動作變更回「是」重新啟用防護。 - 檢查是否有受感染應用程式的修補版本或較新的發行版可修正目前的弱點。安裝修補的應用程式之後，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該應用程式。

尋找記憶體攻擊緩和事件的日誌和報告

您必須檢視日誌並執行快速報告，以尋找記憶體攻擊緩和終止的應用程式。

尋找記憶體攻擊緩和事件的日誌和報告

1. 在主控台中，執行下列其中一個動作：

- 針對日誌，按下「監視器」>「日誌」>「防網路和主機侵入」日誌類型>「記憶體攻擊緩和」日誌內容>「檢視日誌」。

尋找「記憶體攻擊緩和已攔截事件」事件類型。「事件類型」欄會列出緩和技術，而「動作」欄則列出「應用程式名稱」欄中的應用程式是否已遭攔截。例如，下列日誌事件表示 Stack Pivot 攻擊：

Attack: Return Oriented Programming Changes Stack Pointer

- 針對快速報告，按下「報告」>「快速報告」>「防網路和主機侵入」報告類型>「記憶體攻擊緩和偵測」報告>「建立報告」。

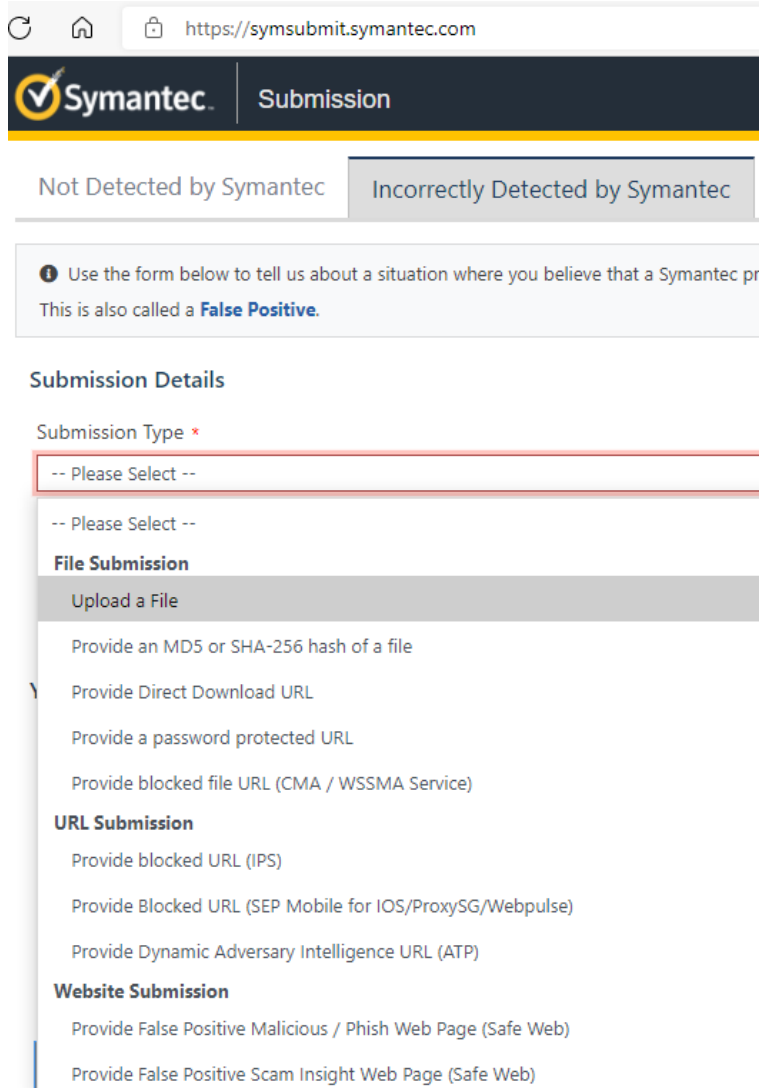
尋找攔截的記憶體攻擊緩和偵測。

稽核已終止應用程式的防護

對誤報進行測試時，請變更記憶體攻擊緩和行為，使其可稽核偵測，但也讓應用程式執行。不過，記憶體攻擊緩和不會保護應用程式。

稽核已終止應用程式的防護

1. 在主控台中，按下「政策」>「記憶體攻擊緩和」>「記憶體攻擊緩和」。
2. 在「緩和技術」標籤上，於「選擇緩和技術」旁，選取終止應用程式的技術，例如 **StackPvt**。
3. 在「受保護」欄下方，選取終止的應用程式，然後將「預設值 (是)」變更為「只記錄」。
在驗證該偵測真的是誤報之後，將動作變更為「否」。「只記錄」和「否」兩者會允許可能的侵入，但也會讓應用程式執行。
部分應用程式有會攔截侵入的多項緩和技術，因此請個別對每項技術執行此步驟。
4. (選擇性) 執行下列其中一個步驟，然後按下「確定」：
 - 如果您不確定哪項技術終止了應用程式，請按下「為此技術的所有應用程式選擇防護動作」。此選項會覆寫每項技術的設定。
 - 如果您同時具有 14.0.1 用戶端和舊版 14 MPx 用戶端，而您只想要測試 14.0.1 用戶端，請按下「將所有技術的防護動作設為只記錄」。
5. (選擇性) 如果要測試應用程式而不論技術為何，請在「應用程式規則」標籤上，於「受保護」欄中，取消勾選終止的應用程式，然後按下「確定」。
針對舊版 14 MPx 用戶端，您僅可以使用此選項。升級至 14.0.1 版用戶端之後，重新啟用防護並執行較精細的調整。開啟「電腦狀態」日誌來尋找哪個用戶端執行哪個產品版本。
6. 在主控台中，按下「政策」>「記憶體攻擊緩和」。
7. 取消勾選「啟用記憶體攻擊緩和」。
8. 按下「確定」。
9. 在 Symantec Endpoint Protection Manager 中，請確保已啟用 Symantec Insight。Insight 預設為啟用。請參閱：
[自訂下載鑑識設定](#)
10. 在用戶端電腦上下載並執行 SymDiag 工具。請參閱：
[下載 SymDiag 以偵測產品問題](#)
11. 在 SymDiag 工具的「首頁」上，按下「收集支援資料」，並針對「除錯記錄」>「進階」選項，將「WPP 除錯」>「追蹤層級」設為「詳細資訊」。請參閱：
[SymDiag 中 Endpoint Protection 用戶端的進階除錯日誌選項](#)
12. 重現誤報偵測。
13. 日誌收集完成後，開啟新案例或使用這個新資訊更新現有案例，以提交 .sdbz 檔案。提交至：
[使用 SymDiag 所收集的資料建立或更新支援案例](#)
14. 將偵測到的應用程式提交至 [SymSubmit 網站](#)。如需如何提交誤報或誤否定的指示。請參閱：
[塞門鐵克行家秘訣：成功提交！](#)



- 對於「其他詳細資料」文字方塊，輸入偵測發生時間和產品。例如，輸入 **B2 Symantec Endpoint Protection 14.x** 產品，然後按一下 **C5 - IPS** 事件。
- 提供前一個步驟中的技術支援案例編號、觸發 MEM 偵測的應用程式，以及有關應用程式版本號碼的詳細資料。例如，您可能會新增：「"Blocked Attack: Return Oriented Programming API Invocation attack against C:\Program Files\VideoLAN\VLC\vlc.exe"，而 vlc.exe 的版本為 2.2.0-git-20131212-0038。這不是最新的可用版本，卻是我們的組織需要使用的版本。」

15. 在用戶端電腦上，壓縮位於以下位置的提交資料夾的複本：`%PROGRAMDATA%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK`。

將此資料夾提交至技術支援，並通知他們您在前一個步驟中開啟的誤報提交的追蹤號碼。技術支援可確保所有必要的日誌和材料完整保留且與誤報調查相關聯。

Symantec Endpoint Protection 記憶體攻擊緩和技術

記憶體攻擊緩和 (MEM) 會停止對 Windows 用戶端電腦上軟體的已知和未知弱點進行攻擊嘗試。MEM 使用以下緩和技術類型來阻止這些攻擊：

- **SEHOP** (結構式例外處理覆寫防護) (14)

「記憶體攻擊緩和」可針對 RealPlayer 媒體播放器等應用程式提供結構式例外處理覆寫防護。侵入攻擊可利用覆寫例外處理常式函式，控制軟體的執行流程朝攻擊者的 Shell 程式碼進行。例外處理常式函式位址儲存在堆疊記憶體中，當存在堆疊緩衝溢位時，可輕易遭覆寫。Windows 作業系統包含 SEHOP，但部分 Windows Vista 作業系統預設停用 SEHOP。即使 Windows 中的 SEHOP 關閉，「記憶體攻擊緩和」仍能提供防護。SEHOP 攻擊僅出現在 32 位元用戶端上。

- **Java Security Manager**

「記憶體攻擊緩和」會攔截嘗試停用 Windows Security Manager 的 Java Applet。有些漏洞攻擊會利用 Java Applet 關閉 Security Manager 來允許 Java 程式碼執行特許動作。

- **StackPvt (StackPivot)**

Stack Pivot 技術可偵測到呼叫堆疊位址是否已變更。此事件指示刺探利用已將堆疊指標 (ESP) 暫存器變更為指向刺探利用的虛假或精心製作的呼叫堆疊記憶體。虛假記憶體包含 ROP 攻擊鏈結。

- **ForceDEP (強制資料執行預防)**

刺探利用攻擊通常將其惡意的可執行程式碼 (稱為 Shell 程式碼) 插入堆疊記憶體 (使用緩衝區溢位) 或堆積記憶體 (使用堆積填充)。刺探利用隨後便劫取朝這些位置進行的執行流程。為了避免此攻擊，Windows XP SP2 及更新版本包含資料執行預防 (DEP)，此系統層級防護會將這些記憶體位置標記為非可執行檔。但是，問題在於此功能可透過 `SetProcessDEPPolicy()` API 呼叫關閉。此外，對於使用 DEP 防護的程序，應該透過 `/NXCOMPAT` 參數進行編譯。ForceDEP 技術可防止 DEP 關閉，即使是在未使用該參數編譯的這些程式上亦是如此。

- **ForceASLR (強制位址空間配置隨機化)**

對於要修改或損壞作業系統的刺探利用，則需要呼叫系統 API，例如 `URLDownloadToFile` 和 `CreateProcess`。在早期 Windows XP 及更早版本中，`Kernel32.dll` 等系統 DLL 始終載入至固定的可預測記憶體位置。因此，硬式編碼的位址輕鬆地呼叫 API。此外，在引入 DEP 之後，刺探利用已發明備用方法來執行稱為 Return Oriented Programming (ROP) 的程式碼。將使用程序中所載入的各個 DLL 中的現有可執行檔程式碼位元組組合來建構 Shell 程式碼，而不是在堆疊或堆積記憶體中寫入和執行 Shell 程式碼。為了防止此程序，Windows Vista 及更新版本引入了 ASLR。此功能會隨機化在記憶體中載入 DLL 的位址，使硬式編碼位址使用無效。但是，對於要在隨機記憶體中載入的 DLL，應使用 `/DYNAMICBASE` 參數進行編譯。一些舊 DLL 仍未使用此參數進行編譯，刺探利用便可利用這些內容。ForceASLR 使 ASLR 成為這些 DLL 上的必要項。

- **堆積填充**

當攻擊者嘗試將其攻擊程式碼放置在預先決定的記憶體位置時，就會發生堆積填充攻擊。堆積填充技術會保留常用的記憶體位置，以防止攻擊者使用這些位置。堆積填充攻擊屬於緩衝區攻擊類型，出現在舊版網頁瀏覽器和應用程式中。

- **EnhASLR (增強位址空間配置隨機化) (14.0.1)**

EnhASLR 技術會在程序中配置隨機記憶體區域。記憶體配置變得不易預測，這樣有助於避免堆積填充。EnhASLR 還會針對 ASLR 和 DLL 重定位增加 Entropy。

- **NullProt (空白頁面防護) (14.0.1)**

NULL (0x00000000) 是可供刺探利用使用的有效記憶體位址。NullProt 技術會重新配置此記憶體位置以避免使用的可能性。

- **DllLoad (14.0.1)**

阻止程序從共用資料夾載入 DLL。一些刺探利用會使用此向量從其惡意伺服器直接執行 DLL，例如 `\\malicious.com\\malware.dll`。請注意，DllLoad 技術不會阻止 DLL 透過本機網路 (例如本機主機、連結本機和私人 IP 位址) 進行遠端載入。在檢查載入路徑與實際載入時間之間，使用主機名稱針對遠端路徑查詢 DNS 伺服器的結果可能會有所不同。

下列緩和技術可防範 Return Oriented Programming (ROP) 攻擊：

- **StackNX (14.0.1)**

StackNX 技術可防止對記憶體防護 API (例如 `VirtualProtect`) 的呼叫將屬於堆疊的記憶體位址標記為可執行檔。

- **RopCall (14.0.1)**

確保系統重要 API 從呼叫指令，而非現有 RET 指令或跳轉指令進行呼叫。

- **RopHeap (14.0.1)**

拒絕對堆積的記憶體防護 API 呼叫，該呼叫之後會使用返回指令執行。

- **RopFlow**

呼叫系統重要 API 時，RopFlow 技術會針對呼叫堆疊中的返回位址執行來執行模擬。RopFlow 會檢查 RET 指示是否指向其他重要 API 或指向未正確標記為可執行檔的記憶體。任一事件皆指示發生 ROP 攻擊。RopFlow 將會模擬允許的指示數目上限來避免效能影響。

記憶體攻擊緩和事件已記錄到用戶端上的安全日誌以及 Symantec Endpoint Protection Manager 上的記憶體攻擊緩和日誌中。除了事件 ID 使用範圍為 61000-61999 的特徵 ID 外，這些事件與 IPS 事件類似。

NOTE

如果您已在用戶端電腦上安裝或啟用下列應用程式，則 MEM 不會保護這些應用程式所保護的程序：

Windows Enhanced Mitigation Experience Toolkit (EMET)

Microsoft Application Virtualization (App-V) 功能

更多資訊

[使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊](#)

阻止和處理病毒和間諜軟體對用戶端電腦的攻擊

您可以遵循一些重要準則來阻止和處理病毒和間諜軟體對用戶端電腦的攻擊。

Table 71: 保護電腦免受病毒和間諜軟體攻擊

工作	說明
確定電腦已安裝 Symantec Endpoint Protection	網路中的所有電腦和所有伺服器應該已安裝 Symantec Endpoint Protection。確定 Symantec Endpoint Protection 執行正常。請參閱： 檢視用戶端電腦的防護狀態
使定義檔保持最新	確定用戶端電腦已安裝最新的定義檔。 您可以在「用戶端」標籤上檢查定義檔日期。您可執行指令以更新過期的定義檔。 您還可以執行電腦狀態報告以檢查最新的定義檔日期。請參閱： 如何更新用戶端上的內容和定義檔
執行定期掃描	依預設，「自動防護」和行為分析 (SONAR) 執行於用戶端電腦上。預設排程作用中掃描也會在用戶端電腦上執行。 您可以根據需求執行掃描。您可以自訂掃描設定。請參閱： 在用戶端電腦上執行隨選掃描 您可能希望建立和自訂排程掃描。 一般而言，您最好每週執行一次完整排程掃描，並且每天執行一次作用中掃描。依預設，Symantec Endpoint Protection 會產生在下午 12:30 執行的作用中掃描。在非受管電腦上，Symantec Endpoint Protection 還包含已停用的預設開機掃描。 請確定網路中的電腦每天執行一次作用中掃描。如果懷疑網路中有非作用中威脅，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。請參閱： • 設定在 Windows 電腦上執行的排程掃描 • 設定在 Mac 電腦上執行的排程掃描 • 設定在 Linux 電腦上執行的排程掃描
讓用戶端立即上傳重大事件	請確定用戶端 (僅限 Windows) 可以略過活動訊號間隔並立即將重大事件傳送至管理伺服器。重大事件包括任何發現的風險 (cookie 除外) 及任何入侵事件。您可以在「用戶端 > 政策 > 通訊設定」中找到該選項。此選項預設為啟用。 當相關通知的調節器期間設定為「無」時，管理員通知可以立即警示您。請參閱： 設定管理員通知

工作	說明
檢查或修改掃描設定以提昇防護	根據預設，病毒和間諜軟體掃描會偵測、移除和修復病毒和安全風險的負面影響。預設掃描設定可在最佳化用戶端電腦效能的同時，仍然提供高階的防護。但是，您可以提高防護等級。例如，您可能希望提升 Bloodhound 啟發式防護。您可能還希望啟用對網路磁碟機的掃描。請參閱： 調整掃描以增強對用戶端電腦的防護
允許用戶端將有關偵測的資訊傳送給賽門鐵克	用戶端可將有關偵測的資訊傳送給賽門鐵克。所傳送的資訊有助於賽門鐵克處理威脅。請參閱： 瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性
執行入侵預防	賽門鐵克建議您在用戶端電腦上執行入侵預防以及病毒和間諜軟體防護。請參閱： 管理入侵預防
根據需要對感染進行矯正	執行掃描後，用戶端電腦可能仍然存在感染。例如，新威脅可能沒有特徵，或者 Symantec Endpoint Protection 無法完全移除該威脅。在某些情況下，用戶端電腦需要重新啟動，以便 Symantec Endpoint Protection 完成清除程序。請參閱： 移除病毒和安全風險

移除病毒和安全風險

作為對電腦上的病毒和間諜軟體攻擊進行處理的一部分，您可對風險進行矯正。

您可以使用主控台中的報告和監控功能來確定哪些電腦已受感染，並檢視矯正結果。

Table 72: 移除病毒和安全風險

步驟	說明
步驟 1：辨識受感染和有風險的電腦	您可以從 Symantec Endpoint Protection Manager 取得有關受感染和有風險的電腦的資訊。在首頁上，檢查「病毒和風險活動摘要」中「新感染」和「仍受感染」的計數。「新感染」的計數為「仍受感染」的計數的子集。「新感染」的計數顯示您在摘要中指定的間隔期間受感染和有風險的電腦的數目。 Note: 沒有將未矯正的行為分析 (SONAR) 偵測計為「仍受感染」。它們在摘要中為「可疑」計數的一部分。 如果後續掃描將電腦偵測為受感染，則這些電腦會被視為仍受感染。例如，排程掃描可能會部分清除某個檔案。「自動防護」隨後會將該檔案偵測為風險。 當新定義檔到達時或一旦用戶端電腦閒置，就會重新掃描被視為「仍受感染」的檔案。請參閱： 識別受感染及有風險的電腦
步驟 2：更新定義檔和重新掃描	您應確保用戶端使用最新的定義檔。 對於在 Windows 電腦上執行的舊版用戶端，還應確保排程和隨選掃描使用「智慧型掃描查詢」功能。排程和隨選掃描始終使用智慧型掃描查詢。 您可在「受感染和處於風險的電腦」報告中檢查定義檔日期。可從風險日誌中執行「更新內容並掃描」指令。 如果首頁上的「病毒和風險活動摘要」顯示「仍受感染」和「新感染」計數為零，則已經清除了所有風險。請參閱： 如何更新用戶端上的內容和定義檔
步驟 3：檢查掃描動作和重新掃描	可將掃描架構為略過風險。您可能希望編輯病毒和間諜軟體防護政策並變更針對風險類別的動作。下次掃描執行時，Symantec Endpoint Protection 會套用新動作。 您可在「動作」標籤上針對特定掃描類型 (管理員定義或隨選掃描，或自動防護) 設定動作。您還可以針對「下載鑑識」和行為分析變更偵測動作。請參閱： 檢查掃描動作及重新掃描識別出的電腦

步驟	說明
步驟 4：重新啟動電腦以完成矯正作業 (如有必要)	電腦由於需要重新啟動，才能完成病毒或安全風險的矯正作業，故而可能仍處於風險之中或受感染。 您可以檢視風險日誌以確定是否有任何電腦需要重新啟動。 您可從電腦狀態日誌執行指令以重新啟動電腦。請參閱： 在用戶端電腦上從主控台執行指令
步驟 5：調查和清除殘留的風險	如果仍殘留有任何風險，您應做進一步的調查。 您也可以檢視「賽門鐵克安全機制應變中心」網頁，取得病毒和安全風險的最新資訊。請參閱： http://securityresponse.symantec.com 在用戶端電腦上，您還可以從掃描結果對話方塊中存取「安全機制應變中心」網站。 您也可以從 Symantec Endpoint Protection Manager 執行 Power Eraser 以分析和矯正困難的永久性威脅。Power Eraser 是一項應在一台電腦上執行的主動分析，而只有當電腦不穩定或嚴重感染時，才應在少量電腦上執行。請參閱： 從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項 賽門鐵克技術支援還會提供 Threat Expert 工具。該工具可快速提供對威脅的詳細分析。您還可以執行載入點分析工具，該工具可幫助您對問題進行疑難排解。請直接在用戶端電腦上執行這些工具。請參閱： 使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解
步驟 6：檢查電腦狀態日誌	檢視電腦狀態日誌以確保已矯正風險或已將風險從用戶端電腦中移除。請參閱： 檢視日誌

更多資訊

- [網路上的病毒移除和疑難排解](#)
- [阻止和處理病毒和間諜軟體對用戶端電腦的攻擊](#)
- [監控 Symantec Endpoint Protection 用戶端](#)

識別受感染及有風險的電腦

您可以使用 Symantec Endpoint Protection Manager 首頁和風險報告來識別受感染及有風險的電腦。

識別受感染和有風險的電腦

1. 在主控台中，按下「首頁」並檢視「病毒和風險活動摘要」。

如果您是系統管理員，就會看到站台中「新感染」和「仍受感染」的電腦數。如果您是網域管理員，可看到網域中「新感染」和「仍受感染」的電腦數。

「仍受感染」是「新感染」的子集合，「仍受感染」的數目會隨著您刪除網路中的風險而降低。如果後續掃描將電腦報告為「受感染」，則電腦仍會處於受感染狀態。例如，Symantec Endpoint Protection 可能只能部分清除電腦中的風險，因此「自動防護」仍會偵測到該風險。

2. 在主控台中，按下「報告」。
3. 在「報告類型」清單方塊中，按下「風險」。
4. 在「選取報告」清單方塊中，按下「受感染和處於風險的電腦」。
5. 按下「建立報告」，然後留意顯示的受感染及有風險的電腦清單。

更多資訊

[移除病毒和安全風險](#)

檢查掃描動作及重新掃描識別出的電腦

如果您的任何電腦已受感染以及有感染風險，則應找出這些電腦仍處於感染和風險狀態的原因。檢查針對受感染和有風險電腦上每個風險所採取的動作。架構及採取的動作有可能是「略過」。如果動作是「略過」，您應該清除電腦中的風險、將電

腦從網路中移除，或接受風險。若是 Windows 用戶端，您可能想要編輯「病毒和間諜軟體防護」政策並變更掃描動作。請參閱：

移除病毒和安全風險

識別需要變更的動作及重新掃描識別出的電腦

1. 在主控台中，按下「監視器」。
2. 在「日誌」標籤中，選取「風險日誌」，然後按下「檢視日誌」。

從「風險日誌事件」欄中，您可以查看發生的事件以及採取的動作。從「風險名稱」欄中，您可以查看仍在作用中風險的名稱。從「網域群組使用者」欄中，您可以查看電腦屬於哪一個群組。

如果用戶端因為掃描採取「略過」動作而存在風險，您可能需要變更群組的病毒和間諜軟體防護政策。在「電腦」欄中，您可以查看仍處於風險之中的電腦名稱。請參閱：

變更 Symantec Endpoint Protection 進行偵測時採取的動作

如果您的政策架構為使用推送模式，則在下次活動訊號時，該政策就會被推送至群組中的用戶端。請參閱：

使用推送模式或提取模式更新用戶端上的政策和內容

3. 按「上一步」。
4. 在「日誌」標籤中，選取「電腦狀態日誌」，然後按下「檢視日誌」。
5. 如果您變更了動作並推送了新政策，請選取需要使用新設定重新掃描的電腦。
6. 在「指令」清單方塊中，選取「掃描」，然後按下「開始」以重新掃描電腦。

您可以從「指令狀態」標籤，監控「掃描」指令的狀態。

Windows 用戶端如何從雲端接收定義檔

Symantec Endpoint Protection 標準和內嵌式/VDI 用戶端利用雲端中的定義檔提供即時防護。舊版提供了一些具有各種功能的雲端防護，例如下載鑑識。現在，所有病毒和間諜軟體功能使用雲端來評估檔案。雲端內容包括整組病毒和間諜軟體定義檔，以及賽門鐵克具有的有關檔案和潛在威脅的最新資訊。

NOTE

僅 Windows 用戶端支援 Intelligent Threat Cloud Service。

用戶端支援啟用雲端的內容

啟用雲端的內容包括提供充分防護的一組減小大小的定義檔。當用戶端需要新的定義檔時，用戶端會下載或查詢在雲端的定義檔，以取得更好的效能和速度。

Windows 用戶端：用戶端類型 (縮減大小的定義) 必須支援啟用雲端的內容。您可以在「說明 > 疑難排解 > 安裝設定」中查看用戶端類型。

標準用戶端和內嵌/VDI 用戶端支援啟用雲端的內容。

所有掃描會自動使用雲端查詢

雲端查詢包括查詢 Symantec Insight 的檔案信譽資訊以及雲端中的定義檔檢查。

- 排程和隨選掃描會自動執行雲端查詢。
- 自動防護還會自動執行雲端查詢。現在，自動防護在使用者模式而非核心模式下執行，可減少記憶體使用量，並提供更好的效能。

除了定義檔在磁碟上佔用較少的使用量，智慧型威脅雲端服務還可減少 15% 的掃描時間。

用戶端會自動將檔案信譽查詢的相關資訊傳送至賽門鐵克。

雲端查詢如何在網路中運作

Symantec Endpoint Protection 會將雲端查詢直接傳送至雲端。

如果您要使用代理伺服器，可在用戶端的瀏覽器「網際網路選項」中指定 HTTPS 代理。或者，您可以使用 Symantec Endpoint Protection Manager 主控台在「政策 > 外部通訊」中為用戶端指定 HTTPS 代理。

Symantec Endpoint Protection Manager 如何向您警示雲端查詢錯誤

如果用戶端嘗試雲端查詢 3 天但未成功，則 Symantec Endpoint Protection Manager 預設會將電子郵件通知傳送給系統管理員。也可以在「監視器 > 日誌 > 系統日誌 > 用戶端活動」中檢視警示。通知條件類型為「檔案信譽偵測」。

什麼是入口網站檔案？

當下載鑑識檢查使用者從支援入口網站下載的檔案時，會將該檔案標示為入口網站檔案。排程和隨選掃描、自動防護和下載鑑識使用為下載鑑識設定的靈敏度等級評估入口網站檔案的信譽。

NOTE

必須啟用下載鑑識，將檔案標示為入口網站檔案。

支援的入口網站包含 Internet Explorer、Firefox、Microsoft Outlook、Outlook Express、Google Chrome、Windows Live Messenger 和 Yahoo Messenger。入口網站清單 (或自動防護入口網站清單) 是 LiveUpdate 下載到管理伺服器或用戶端的病毒和間諜軟體防護內容的一部分。

掃描和下載鑑識一律使用賽門鐵克設定的預設內部靈敏度等級來評估非入口網站檔案。內部預設值僅偵測大多數惡意檔案。

作用中雲端查詢範例

Intelligent Threat Cloud Service 保護用戶端的方式範例：

- 用戶端使用者執行 Internet Explorer 並嘗試下載檔案。下載鑑識使用雲端中的 Symantec Insight 提供之靈敏度等級和信譽資訊，判斷檔案是否無害。
- 下載鑑識判斷檔案的信譽是否可接受，允許下載檔案，並將該檔案標示為入口網站檔案。
- 之後，賽門鐵克從其廣泛的 Global Intelligence Network 取得有關檔案的詳細資訊。賽門鐵克判斷該檔案可能有害，並更新 Insight 信譽資料庫。賽門鐵克可能會在雲端的定義檔中提供檔案的最新特徵。
- 如果使用者開啟檔案或執行掃描，自動防護或掃描會從雲端取得有關檔案的最新資訊。透過最新檔案信譽和下載鑑識敏感程度或透過最新檔案特徵，自動防護或掃描現在可以偵測檔案為具有潛在惡意。

必要設定和建議設定

依據預設，Symantec Endpoint Protection 會使用雲端。如果您停用其中任何選項，便會限制或停用雲端防護。

- 自動防護
必須啟用「自動防護」。「自動防護」預設為啟用。
- 下載鑑識
必須啟用「下載鑑識」，以便它可以檢查檔案下載，並將檔案下載標示為入口網站檔案以供日後掃描。如果您停用「下載鑑識」，所有檔案下載都將視為非入口網站檔案。掃描僅偵測大多數惡意的非入口網站檔案。
- 智慧型掃描查詢
必須啟用「智慧型掃描查詢」。智慧型掃描查詢選項可控制信譽查詢以及雲端定義查詢。此選項預設為啟用。

WARNING

如果停用智慧型掃描查詢，雲端防護將會完全停用。

- 遞送

賽門鐵克建議您與賽門鐵克共用資訊。與賽門鐵克共用的資料可提升偵測功能的效能。可能會攻擊您電腦的潛在惡意軟體的相關資訊可協助改善安全性領域並加快解決威脅的速度。賽門鐵克會竭盡所能讓資料匿名，以防止傳輸個人識別資訊。請參閱：

[瞭解向賽門鐵克提交資訊可改善電腦防護功能](#)

在用戶端電腦上管理掃描

某些掃描會預設執行，但您可能希望變更設定或設定自己的排程掃描。您還可以自訂掃描，並變更這些掃描在您的用戶端電腦上提供的防護程度。

NOTE

從 14 版開始，掃描會存取在雲端設定的完整定義檔。請參閱：

[Windows 用戶端如何從雲端接收定義檔](#)

Table 73: 在用戶端電腦上修改掃描

工作	說明
檢視掃描類型和預設設定	檢查您的掃描設定。您可以檢視預設值，然後決定是否要進行變更。請參閱： 關於掃描和即時防護的類型 關於預設的病毒和間諜軟體防護政策掃描設定
建立排程掃描和執行隨選掃描	您可以使用排程掃描與隨選掃描，增強自動防護所提供的防護。自動防護會在您讀寫檔案時，提供防護。排程掃描與隨選掃描則可以掃描用戶端電腦儲存的所有檔案。也可以防護用戶端電腦的記憶體、載入點，及其他重要位置。 排程掃描設定可以儲存為範本。架構多個政策時，使用掃描範本可節省時間。您可使用存為範本的任何掃描，做為不同政策中新掃描的基礎。 Note: 對於受管理用戶端，Symantec Endpoint Protection 提供預設排程掃描，掃描用戶端電腦中所有的檔案、資料夾及位置。 如需詳細資訊，請參閱： 設定在 Windows 電腦上執行的排程掃描 設定在 Mac 電腦上執行的排程掃描 設定在 Linux 電腦上執行的排程掃描 在用戶端電腦上執行隨選掃描
為您的環境自訂掃描設定	您可以自訂「自動防護」設定及管理員定義掃描中的選項。您可能希望變更掃描設定以處理偵測誤報、最佳化電腦或掃描效能，或變更掃描動作或通知。 對於排程掃描，您還可以針對未執行掃描、隨機化掃描及是否要掃描網路磁碟機來設定選項。 如需詳細資訊，請參閱： 自訂在 Windows 電腦上執行的病毒和間諜軟體掃描 自訂在 Mac 電腦上執行的病毒和間諜軟體掃描 自訂在 Linux 電腦上執行的病毒和間諜軟體掃描
調整掃描以提高用戶端電腦效能	根據預設，Symantec Endpoint Protection 會在提供高安全性等級的同時，將對用戶端電腦效能的影響降至最低。但是，您可以變更某些設定，進一步最佳化電腦效能。最佳化在虛擬環境中很重要。 Note: 透過調整設定來最佳化用戶端電腦效能，或許會降低用戶端電腦的一些安全性。 如需詳細資訊，請參閱： 調整掃描以改善電腦效能
調整掃描以提高對用戶端電腦的防護	預設掃描設定可在最佳化用戶端電腦效能的同時，仍然提供高階的防護。但是，您可以提高防護等級。請參閱： 調整掃描以增強對用戶端電腦的防護

工作	說明
管理下載鑑識偵測	「下載智慧型掃描」會檢查使用者嘗試透過網頁瀏覽器、文字訊息用戶端及其他入口網站下載的檔案。 「下載智慧型掃描」使用來自「賽門鐵克智慧型掃描」的信譽資訊進行檔案相關決策。請參閱： 管理「下載鑑識」偵測
管理行為分析 (SONAR)	行為分析是用戶端電腦上主動型威脅防護的一部分。但是，行為分析設定是病毒和間諜軟體防護政策的一部分。請參閱： 管理 SONAR
架構掃描的例外	您可以為已知是安全的檔案和應用程式建立例外。 Symantec Endpoint Protection 還會自動排除某些檔案和資料夾。 如需詳細資訊，請參閱： 管理 Symantec Endpoint Protection 中的例外 關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾
管理隔離所中的檔案	您可以監控和刪除用戶端電腦上已隔離的檔案。 還可以指定隔離所的設定。請參閱： 管理 Windows 用戶端的隔離所
允許用戶端將有關偵測的資訊傳送給賽門鐵克	根據預設，用戶端會將有關偵測的資訊傳送給賽門鐵克。您可以關閉遞送或選擇用戶端遞送的資訊類型。 賽門鐵克建議您始終允許用戶端傳送資訊。此資訊有助於賽門鐵克處理威脅。請參閱： 瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性
管理顯示在用戶端電腦上的病毒和間諜軟體通知	您可以決定是否要在用戶端電腦上顯示病毒和間諜軟體事件的通知。請參閱： 管理顯示在用戶端電腦上的病毒和間諜軟體通知

關於掃描和即時防護的類型

Symantec Endpoint Protection 包含不同類型的掃描和即時防護，用於偵測不同類型的病毒、威脅和風險。

NOTE

掃描會存取在雲端設定的完整定義檔。請參閱：

[Windows 用戶端如何從雲端接收定義檔](#)

依預設，Symantec Endpoint Protection 會在每天下午 12:30 執行作用中掃描。Symantec Endpoint Protection 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，Symantec Endpoint Protection 還包含已停用的預設開機掃描。

NOTE

當用戶端電腦關機或處於休眠或睡眠模式時，電腦可能會錯過排程的掃描。當電腦開機或喚醒時，預設會在指定的間隔時間內重試掃描。如果間隔時間已經結束，Symantec Endpoint Protection 則不會執行掃描，而會等到下次的排程時間再執行。您可以修改錯過排程掃描的設定。

請確定網路中的電腦每天執行一次作用中掃描。如果懷疑網路中有非作用中威脅，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。請參閱：

[在用戶端電腦上管理掃描](#)

Table 74: 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。Mac 用戶端和 Linux 用戶端僅支援對檔案系統的「自動防護」。 在連線至雲端的標準和內嵌式/VDI 用戶端上，自動防護會自動查詢雲端的最新定義檔。 如需詳細資訊，請參閱： 自訂 Linux 用戶端的自動防護
下載鑑識 (僅限 Windows 用戶端)	「下載智慧型掃描」會透過以下方法提升「自動防護」掃描的安全性：當使用者嘗試從瀏覽器及其他入口網站下載檔案時檢查這些檔案。它會使用來自「賽門鐵克智慧型掃描」的信譽資訊來允許或攔截下載嘗試。 「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」。 如需詳細資訊，請參閱： Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策
管理員定義掃描	管理員定義的掃描會透過檢查用戶端電腦上的全部檔案和程序來偵測病毒及安全風險。管理員定義的掃描還可檢查記憶體及載入點。 可用的管理員定義的掃描類型如下： 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、休眠或睡眠狀態，除非電腦已架構為重試錯過的掃描，否則不會執行此掃描。當電腦啟動或喚醒時，Symantec Endpoint Protection 會重試掃描，直到掃描開始或重試間隔到期為止。 您可以針對 Windows 用戶端排程作用中掃描、完整掃描或自訂掃描。您只能對 Mac 用戶端或 Linux 用戶端排程自訂掃描。 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目錄。 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。 Note: 開機掃描和觸發掃描僅可用於 Windows 用戶端。 隨選掃描 隨選掃描是指，您在 Symantec Endpoint Protection Manager 中選取掃描指令時立即執行的掃描。 您可以從 [用戶端] 標籤或日誌中選取該指令。 如果 Windows 適用的 Symantec Endpoint Protection 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。 掃描可能會記錄比政策為此掃描期間所定義更高靈敏度等級的偵測。 如需詳細資訊，請參閱： 設定在 Windows 電腦上執行的排程掃描 設定在 Mac 電腦上執行的排程掃描
行為分析 (SONAR) (僅限 Windows 用戶端)	行為分析提供防範零時差攻擊的即時防護。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。 與主動型威脅掃描相同，行為分析也會偵測鍵盤記錄程式、間諜軟體以及任何其他可能具有惡意或具有潛在惡意的應用程式。請參閱： 何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？
提早啟動防惡意軟體 (ELAM) (僅限 Windows 用戶端)	與 Windows 提早啟動防惡意軟體驅動程式搭配使用。在 Windows 8 或更新版本以及 Windows Server 2012 或更新版本中受支援。 提早啟動防惡意軟體會在網路中的電腦啟動時，以及第三方驅動程式初始化之前，為電腦提供防護。請參閱： 管理提早啟動防惡意軟體 (ELAM) 偵測

關於自動防護的類型

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。

預設會啟用所有類型的自動防護。如果您使用伺服器型電子郵件掃描解決方案，例如 Symantec Mail Security，就可能不需要啟用電子郵件自動防護。

Mac 用戶端和 Linux 用戶端不支援電子郵件自動防護掃描。

Table 75: 自動防護的類型

自動防護的類型	說明
自動防護	從用戶端電腦讀取檔案或將檔案寫入用戶端電腦時，進行連續掃描。 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。 對於不執行電子郵件自動防護的那些用戶端，啟用自動防護後，用戶端電腦仍會受到保護。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性風險。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。 Note: 在 14.2 RU2 和更新版本中，您可以設定檔案系統自動防護，以自動掃描電腦使用者插入的 USB 磁碟機。請參閱：Symantec Endpoint Protection 會掃描 USB 快閃磁碟機嗎？
Microsoft Outlook 自動防護 (僅限 Windows 用戶端)	下載內送的 Microsoft Outlook 電子郵件附件，並在使用者閱讀訊息並開啟附件時，掃描是否存在病毒和安全風險。 Outlook 自動防護外掛程式支援 Microsoft Outlook 98 到 Outlook 2019 和 Outlook 365 的 MAPI 或 Internet 通訊協定。Outlook 自動防護支援 32 位元和 64 位元系統。 Note: 若 Microsoft Outlook 2016 與 SEP 搭配安裝，您可能需要停用 Outlook 自動防護外掛程式，或安裝較新版本的 Microsoft Outlook。請參閱： Note: Outlook 2016 在使用 Endpoint Protection 增益集時當機 在安裝期間，如果套件中已納入「Microsoft Outlook 自動防護」，且電腦上已經安裝 Microsoft Outlook，則 Symantec Endpoint Protection 會安裝此防護。 如果使用者透過慢速連線下載大型附件，會影響電子郵件效能。如果您確定文件是安全的，則可以建立例外。 如需詳細資訊，請參閱： 從掃描中排除檔案或資料夾 Note: 請不要在 Microsoft Exchange Server 上安裝 Microsoft Outlook 自動防護。您應改為安裝 Symantec Mail Security for Microsoft Exchange。
Internet 電子郵件自動防護 (僅限 Windows 用戶端) (可用於用戶端第 14.2 和更舊版本)。	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 (僅限 Windows 用戶端) 此功能僅適用於低於 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。 在安裝期間，如果套件中已納入「Lotus Notes 自動防護」，且電腦上已經安裝 Lotus Notes，則 Symantec Endpoint Protection 會安裝該防護。

更多資訊

- [關於掃描和即時防護的類型](#)
- [為 Windows 電腦上的電子郵件掃描自訂自動防護](#)

關於病毒和安全風險

Symantec Endpoint Protection 可以掃描病毒和安全風險。病毒和安全風險可透過電子郵件或時傳訊程式感染。通常使用者會因為接受軟體程式的「使用者授權許可協議」，而在不知情的狀況下載風險。

許多病毒和安全風險都以偷渡式下載安裝到電腦。這類下載通常發生於使用者瀏覽惡意網站或受感染的網站時，而應用程式的下載程式會透過電腦上的合法漏洞進行安裝。

您可以變更 Symantec Endpoint Protection 在偵測到病毒或安全風險時要執行的動作。對於 Windows 用戶端，安全風險類別是動態的，會隨時間變化，因為賽門鐵克會收集有關風險的資訊。請參閱：

[變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)

您可以在「賽門鐵克安全機制應變中心」網站上檢視有關特定病毒和安全風險的資訊。

Table 76: 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。Bot 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	提供任何廣告內容的程式。
Cookie	Web 伺服器出於識別電腦或使用者的目的傳送給網頁瀏覽器的訊息。
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。
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，告知必須移除的任何假病毒感染。
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。
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	是一種單機的程式，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。

關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾

當 Symantec Endpoint Protection 偵測到特定第三方應用程式和某些 Symantec 產品存在時，它會自動為這些檔案和資料夾建立排除項目。用戶端會從所有掃描中排除這些檔案和資料夾。

NOTE

用戶端不會將系統暫存資料夾排除在掃描範圍外，因為這樣做會產生明顯的電腦安全弱點。

若要提高掃描效能或減少誤報偵測，您可以將檔案或資料夾例外新增到「例外」政策以排除檔案。您也可以指定要包含在特定掃描中的副檔名或資料夾。

WARNING

從掃描中排除的檔案或資料夾不會受到保護，因此可能受到病毒和安全風險的威脅。

您可以檢視用戶端自動建立的排除項目。

請查看 Windows 登錄的以下位置：

- 在 32 位元的電腦：HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions
- 在 64 位元的電腦 (14.3 RU4 或更舊版本)：HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions。
- 在 64 位元的電腦 (14.3 RU5 或更舊版本)：HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions

WARNING

請勿直接編輯此登錄機碼。

Table 77: 檔案與資料夾排除

檔案	說明
Microsoft Exchange	用戶端軟體會為下列版本的 Microsoft Exchange Server 自動建立檔案和資料夾的掃描排除項目： - Exchange 5.5 - Exchange 6.0 - Exchange 2000 - Exchange 2003 - Exchange 2007 - Exchange 2007 SP1 - Exchange 2010 - Exchange 2013 - Exchange 2016 - Exchange 2019 對於 Exchange 2007，請參閱使用者文件，瞭解防毒軟體的相容性。在少數情況下，可能需要為某些 Exchange 2007 資料夾手動建立掃描排除項目。例如，在叢集的環境中，您可能需要建立一些排除項目。 用戶端軟體會定期檢查 Microsoft Exchange 檔案和資料夾位置是否有變更。如果您在已安裝用戶端軟體的電腦上安裝 Microsoft Exchange，則用戶端檢查變更狀況時，會建立排除項目。用戶端會排除相應的檔案和資料夾；如果單一檔案移出排除的資料夾，該檔案仍然會在排除範圍內。
Microsoft Forefront	用戶端會自動為以下 Microsoft Forefront 產品建立檔案和資料夾排除項目： - Forefront Server Security for Exchange - Forefront Server Security for SharePoint - Forefront Threat Management Gateway 檢查 Microsoft 網站中建議排除項目的清單。 如需詳細資訊，請參閱下列文章： 為 Microsoft Forefront 架構 Symantec Endpoint Protection 排除項目
Active Directory 網域控制器	用戶端會自動為 Active Directory 網域控制器資料庫、日誌和工作檔案建立檔案和資料夾排除項目。用戶端會監控安裝在用戶端電腦上的應用程式。如果軟體偵測到用戶端電腦上有 Active Directory，便會自動建立排除項目。
賽門鐵克產品	在偵測到某些賽門鐵克產品時，用戶端會自動建立適當的檔案和資料夾掃描排除項目。 用戶端會為下列賽門鐵克產品建立排除項目： - Symantec Mail Security 4.0、4.5、4.6、5.0、6.0 for Microsoft Exchange - Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange - Norton AntiVirus 2.x for Microsoft Exchange - Symantec Endpoint Protection Manager 預設資料庫 (Microsoft SQL Server Express 或內嵌) 和日誌
Veritas 產品	在偵測到某些 Veritas 產品時，用戶端會自動建立適當的檔案和資料夾掃描排除項目： - Veritas Backup Exec - Veritas NetBackup - Veritas System Recovery 支援自動排除以 8.x 結束的 Veritas Netbackup。
選取的副檔名和 Microsoft 資料夾	對於各種類型的管理員定義掃描或自動防護，您可以按照副檔名選取要包含的檔案。對於管理員定義掃描，您也可以按照資料夾選取要包含的檔案。例如，您可以指定排程掃描只掃描某些副檔名，而「自動防護」掃描所有副檔名。 對於執行檔和 Microsoft Office 檔案，即使病毒變更檔案的副檔名，自動防護也可以確定檔案的類型。Symantec Endpoint Protection 預設會掃描所有的副檔名和資料夾。您取消選取的任何副檔名或資料夾，都會從該特定掃描中排除。 Symantec 不建議您從掃描中排除任何副檔名。然而，如果您決定按副檔名排除檔案和任何 Microsoft 資料夾，則應考慮網路所需的防護程度。您還應考慮用戶端電腦完成掃描所需的時間和資源量。 Note: 您從檔案系統「自動防護」掃描中排除的任何副檔名，也會從「下載鑑識」中排除。如果您正在執行「下載鑑識」，則應將常用程式和文件的副檔名包含在要掃描的副檔名清單中。您也應務必掃描 .msi 檔案。

檔案	說明
檔案與資料夾排除	您可使用例外政策，為您希望 Symantec Endpoint Protection 從所有病毒和間諜軟體掃描中排除的檔案或資料夾建立例外。 Note: 預設情況下，用戶端電腦上的使用者也可以建立檔案和資料夾例外。 例如，您可能需要為電子郵件應用程式收件匣建立檔案排除項目。 如果在隨選掃描或排程掃描過程中，用戶端在收件匣檔案中偵測到病毒，則用戶端會隔離整個收件匣。您也可以建立例外以排除收件匣檔案。然而，如果用戶端在使用者開啟電子郵件時偵測到病毒，則用戶端仍會隔離或刪除該郵件。
受信任檔案	病毒和間諜軟體掃描使用 Insight，它可讓掃描略過受信任檔案。您可以為要略過的檔案選擇信任層級，也可以停用該選項。如果您停用該選項，可能會增加掃描時間。 自動防護也可以略過由受信任程序 (例如 Windows 搜尋) 存取的檔案。

更多資訊

[從掃描中排除檔案或資料夾](#)

關於預設的病毒和間諜軟體防護政策掃描設定

Symantec Endpoint Protection Manager 包括三種預設政策：

- 病毒和間諜軟體防護平衡政策
- 病毒和間諜軟體防護高安全性政策
高安全性政策是所有預先架構的政策中最嚴格的。您必須注意，它可能會影響其他應用程式的效能。
- 病毒和間諜軟體防護高效能政策
與高安全性政策相比，高效能政策可提供更佳的效能，但不提供相同的防護措施。該政策主要依靠「自動防護」來掃描具有所選取檔案副檔名的檔案，以偵測威脅。

基本病毒和間諜軟體防護政策完善地兼顧了安全性與效能。

Table 78: 病毒和間諜軟體防護平衡政策掃描設定

設定	說明
檔案系統的自動防護	已啟用 「下載鑑識」惡意檔案靈敏度設定為等級 5。 「下載鑑識」對於未證明的檔案採取的動作為「忽略」。 「自動防護」包含下列設定： • 對所有檔案進行病毒和安全風險掃描。 • 攔截安裝安全風險。 • 清除受病毒感染的檔案。先備份檔案再修復。隔離無法清除的檔案。 • 隔離有安全風險的檔案。記錄無法隔離的檔案。 • 檢查所有磁片是否有開機病毒。記錄開機病毒。 • 通知電腦使用者病毒和安全風險的相關資訊。
電子郵件的自動防護	已啟用 其他類型的「自動防護」包含下列設定： • 掃描所有檔案，其中包括壓縮檔內的檔案。 • 清除受病毒感染的檔案。隔離無法清除的檔案。 • 隔離有安全風險的檔案。記錄無法隔離的檔案。 • 將有關偵測到的病毒和安全風險的訊息傳送給電腦使用者。

設定	說明
行為分析 (SONAR)	已啟用 - 高風險的啟發式偵測已被隔離 - 記錄任何低風險的啟發式偵測 - 主動模式已停用 「偵測到時顯示警示」已啟用 - 系統變更偵測動作設定為「忽略」。 - 可疑行為偵測會攔截高風險威脅並忽略低風險威脅。
管理員定義掃描	排程掃描包含下列預設設定： - 每天下午 12:30 執行一次作用中掃描。該掃描為隨機進行。 - 掃描所有檔案和資料夾，包括壓縮檔內的檔案。 - 掃描記憶體、常見感染位置，以及已知的病毒和安全風險位置。 - 清除受病毒感染的檔案。先備份檔案再修復。隔離無法清除的檔案。 - 隔離有安全風險的檔案。記錄無法隔離的檔案。 - 在三天內重試未執行的掃描。 隨選掃描政策提供了下列防護： - 掃描所有檔案和資料夾，包括壓縮檔內的檔案。 - 掃描記憶體及常見的感染位置。 - 清除受病毒感染的檔案。先備份檔案再修復。隔離無法清除的檔案。 - 隔離有安全風險的檔案。記錄無法隔離的檔案。

預設的病毒和間諜軟體高安全性政策提供高階安全性，並且包含病毒和間諜軟體防護政策中的許多設定。此政策要求執行更多的掃描。

Table 79: 病毒和間諜軟體防護高安全性政策設定

設定	說明
檔案系統和電子郵件的自動防護	與病毒和間諜軟體防護平衡政策相同 「自動防護」還會檢查遠端電腦上的檔案。
行為分析 (SONAR)	與病毒和間諜軟體防護平衡政策相同，但有下列差異： 攔截任何系統變更事件。
全域設定	Bloodhound 設定為「主動」。 Note: 「主動」選項可能會產生更多的誤報結果。僅建議進階使用者使用此選項。

預設的病毒和間諜軟體防護高效能政策提供高階效能。該政策包含病毒和間諜軟體防護政策中的許多設定。此政策提供的安全性低一些。

Table 80: 病毒和間諜軟體防護高效能政策設定

設定	說明
檔案系統的自動防護	與病毒和間諜軟體防護平衡政策相同，但有下列差異： 「下載鑑識」惡意檔案靈敏度設定為等級 1。
Microsoft Outlook 自動防護 Internet 電子郵件自動防護* Lotus Notes 自動防護* * 僅適用於低於 14.2 RU1 的用戶端版本	已停用

設定	說明
行為分析 (SONAR)	與病毒和間諜軟體防護平衡政策相同，但有下列差異： - 忽略任何系統變更事件。 - 忽略任何行為政策強制執行事件。
管理員定義掃描	與病毒和間諜軟體防護平衡政策相同。

Symantec Endpoint Protection 處理病毒和安全性風險偵測結果的方式

Symantec Endpoint Protection 會使用預設動作處理對病毒和安全性風險的偵測結果。您可以變更部分預設值。

Table 81: Symantec Endpoint Protection 處理病毒和安全風險偵測結果的方式

偵測	說明
病毒	依預設，Symantec Endpoint Protection 用戶端會先嘗試清除感染病毒的檔案。 如果用戶端軟體無法清除檔案，就會執行下列動作： - 將檔案移動至受感染電腦上的隔離所 - 拒絕對檔案的任何存取動作 - 記錄事件
安全風險	依預設，用戶端會將任何受到安全性風險感染的檔案移至受感染電腦上的隔離所。用戶端也會嘗試移除或修復風險的副作用。 如果安全風險無法被隔離和修復，則第二個預設動作將記錄風險。 依預設，隔離所包含用戶端所有已執行動作的記錄。您可以使電腦回到用戶端嘗試移除和修復作業之前所存在的狀態。

會將行為分析 (SONAR) 執行的偵測視為可疑事件。您可在行為分析組態中，為這些偵測結果架構動作。請參閱：

[管理 SONAR](#)

NOTE

有風險的 Cookie 一律刪除，除非您指定想要記錄 Cookie。您只能針對 Cookie 指定一個動作：「刪除」或「略過 (只記錄)」。

作業系統	說明
Windows	您可以變更 Symantec Endpoint Protection 發現安全風險時採取的第一和第二動作。您可以針對排程掃描、隨選掃描或自動防護掃描使用不同的動作。 安全風險偵測類型清單是動態的，會隨著 Symantec 發現新的類別而有所改變。當新的定義檔到達時，會將新的類別下載到主控台或用戶端電腦。
Linux	Linux 用戶端會採取以下預設動作： - 惡意軟體：清除並隔離風險 - 安全風險：隔離並記錄風險。 在 14.3 RU1 及更新版本中，您無法設定偵測的動作。
Mac	您可以指定 Symantec Endpoint Protection 是否要修復其發現的受感染檔案。也可以指定 Symantec Endpoint Protection 是否要將無法修復的受感染檔案移至隔離所。您可以針對排程掃描、隨選掃描或自動防護掃描使用不同的動作。

如需詳細資訊，請參閱：

[管理 Windows 用戶端的隔離所](#)

Symantec Endpoint Protection 如何在 Windows 8 電腦上處理偵測

Symantec Endpoint Protection 會同時保護 Windows 8 樣式使用者介面以及 Windows 8 桌面。不過，與 Windows 8 樣式應用程式和檔案相關的偵測動作運作方式與其他偵測動作的運作方式不同。

在 Windows 8 樣式使用者介面上裝載的應用程式，會在與作業系統中的其他程序隔開的配置區內實作。Symantec Endpoint Protection 不會清除也不會隔離影響 Windows 8 樣式應用程式或檔案的任何偵測。對於牽涉到這些應用程式和檔案的所有偵測，Symantec Endpoint Protection 只會刪除或記錄偵測。

對於與 Windows 8 樣式應用程式和檔案不相關的任何偵測，Symantec Endpoint Protection 可以隔離並修復偵測，並且如同它通常在任何其他 Windows 作業系統上一樣進行操作。

在「病毒和間諜軟體防護」政策中設定動作時，以及執行報告時，您應該注意其差異。請參閱：

- [關於出現在 Windows 8 用戶端上的彈出式通知](#)
- [Symantec Endpoint Protection 處理病毒和安全性風險偵測結果的方式](#)

設定在 Windows 電腦上執行的排程掃描

您可以在設定病毒和間諜軟體防護政策時架構排程掃描。

當您為安全網路中的 Windows 電腦設定排程掃描時，請考慮下列重點：

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，Symantec Endpoint Protection 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 Symantec Endpoint Protection 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，Symantec Endpoint Protection 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，Symantec Endpoint Protection 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。

NOTE

Windows 設定包含的一些選項不適用於在其他作業系統上執行的用戶端。

若需程序中使用選項的詳細資訊，您可以按下「敘述」。

設定在 Windows 電腦上執行的排程掃描

-
1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
 2. 在「**Windows** 設定」下方，按一下「管理員定義掃描」。
 3. 在「掃描」標籤的「已排程的掃描」下方，按一下「新增」。
 4. 在「新增排程掃描」對話方塊中，按下「建立新的排程掃描」。
 5. 按下「確定」。
 6. 在「新增排程掃描」對話方塊的「掃描詳細資料」標籤中，輸入此排程掃描的名稱和說明。
 7. 按下「作用中掃描」、「完整掃描」或「自訂掃描」。
 8. 如果您選取「自訂」，就可以在「掃描」下指定要掃描的資料夾。
 9. 在「檔案類型」下，按下「掃描所有檔案」或「只掃描選取的副檔名」。

NOTE

除非您停用「進階掃描選項」下的「掃描壓縮檔內的檔案」選項，或為配置區副檔名建立特定例外，否則排程掃描一律會掃描配置區檔案。

10. 在「勾選以下項目以加強掃描」下，勾選或取消勾選「記憶體」、「常見感染位置」或「已知病毒和安全風險位置」。
11. 在「排程」標籤的「掃描排程」下方，設定應該執行掃描的頻率和時間。
「錯過掃描排程」下的重試設定，會根據您選取「每日」、「每週」或「每月」自動變更。
12. 在「錯過掃描排程」下，您可以停用相應選項，以執行錯過的掃描，也可以變更重試時間間隔。
您也可以指定掃描暫停之前的最長掃描持續時間。您也可以隨機產生掃描開始時間。
13. 若要將此掃描儲存為範本，請勾選「另存複本為排程掃描範本」。
14. 按下「確定」。

更多資訊

- [在用戶端電腦上管理掃描](#)
- [為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描](#)
- [從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名](#)

設定在 **Mac** 電腦上執行的排程掃描

您可以在設定病毒和間諜軟體防護政策時架構排程掃描。請參閱：

- [在用戶端電腦上管理掃描](#)
- [為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描](#)

NOTE

Mac 設定並未包含執行於 Windows 之用戶端適用的所有選項。

設定在 **Mac** 電腦上執行的排程掃描

-
1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
 2. 在「**Mac** 設定」下方，按下「管理員定義掃描」。
 3. 在「掃描」標籤的「已排程的掃描」下方，按一下「新增」。
 4. 在「新增排程掃描」對話方塊中，按下「建立新的排程掃描」，然後按下「確定」。
 5. 在「新增排程掃描」對話方塊的「掃描詳細資料」標籤中，鍵入掃描的名稱和敘述。
 6. 在「掃描磁碟機和資料夾」下，指定要掃描的項目。
 7. 在「排程」標籤的「掃描排程」下方，設定應該執行掃描的頻率和時間。

NOTE

Symantec 不建議一天多次執行排程掃描。增加掃描頻率或設定多個排程掃描可能會導致效能問題。

8. 若要將此掃描儲存為範本，請勾選「另存複本為排程掃描範本」。
9. 按下「確定」。

設定在 Linux 電腦上執行的排程掃描

您可以在設定病毒和間諜軟體防護政策時架構排程掃描。

設定在 **Linux** 電腦上執行的排程掃描

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Linux** 設定」下，按下「管理員定義掃描」。
3. 在「掃描」標籤的「已排程的掃描」下方，按一下「新增」。
4. 在「新增排程掃描」對話方塊中，按下「新增排程掃描」。
5. 在「新增排程掃描」對話方塊的「掃描詳細資料」標籤中，輸入此排程掃描的名稱和說明。
6. 在「資料夾類型」下，按下「掃描所有資料夾」，或指定要掃描的資料夾。
7. 在「檔案類型」下，按下「掃描所有檔案」或「只掃描選取的副檔名」。

自 14.3 RU1 起，不提供「只掃描選取的副檔名」選項。

NOTE

除非您停用「掃描壓縮檔內的檔案」選項，或為配置區副檔名建立特定例外，否則排程掃描一律會掃描配置區檔案。

8. 在「其他選項」下方，勾選或取消勾選「掃描安全風險」。
9. 在「排程」標籤的「掃描排程」下方，設定應該執行掃描的頻率和時間。

「錯過掃描排程」下的重試設定，會根據您選取「每日」、「每週」或「每月」自動變更。

10. 14.3 RU1 和更新版本：在「錯過掃描排程」下，您可以停用相應選項，以執行錯過的掃描，也可以變更重試時間間隔。
11. 若要將此掃描儲存為範本，請勾選「另存複本為排程掃描範本」。
12. 按一下「確定」。

更多資訊

[在用戶端電腦上管理掃描](#)

在用戶端電腦上執行隨選掃描

您可以從管理主控台遠端為用戶端電腦執行手動或隨選掃描。您的策略可能包括執行隨選掃描，以防止和處理用戶端電腦上的病毒和間諜軟體攻擊。

依預設，作用中掃描會在您更新定義檔之後自動執行。您可以將隨選掃描架構為完整掃描或自訂掃描，然後執行該隨選掃描，進行更廣泛的掃描。

隨選掃描的設定很類似排程掃描的設定。

- 對於 Windows 用戶端電腦，您可以執行作用中掃描、完整掃描或自訂隨選掃描。
- 對於 Mac 用戶端電腦，您可以執行作用中或完整隨選掃描。
- 對於 Linux 用戶端電腦，您可以執行完整隨選掃描。

自訂掃描會使用病毒和間諜軟體防護政策中為隨選掃描架構的設定。

NOTE

如果您在執行隨選掃描的用戶端電腦上發出重新啟動的指令，掃描會停止，且用戶端電腦將重新啟動。掃描並不會重新啟動。

您可以從電腦狀態日誌或從主控台中的「用戶端」標籤執行隨選掃描。

您可以從「電腦狀態」日誌，取消所有正在進行的掃描以及放入所選用戶端佇列中的掃描。如果您確認了指令，表格會重新整理，然後您會看見取消的指令新增到指令狀態表格中。

在用戶端電腦上執行隨選掃描

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，在要掃描的群組或用戶端上按下滑鼠右鍵。
3. 執行下列其中一項動作：
 - 按下「對群組執行指令 > 掃描」。
 - 按下「對電腦執行指令 > 掃描」。

按下「更新內容和掃描」以更新定義檔，然後一步執行掃描。

4. 對於 Windows 用戶端，請選取「作用中掃描」、「完整掃描」或「自訂掃描」，然後按下「確定」。

更多資訊

- [在用戶端電腦上管理掃描](#)
- [阻止和處理病毒和間諜軟體對用戶端電腦的攻擊](#)
- [在用戶端電腦上從主控台執行指令](#)
- [什麼是可對用戶端電腦執行的指令？](#)

調整掃描以改善電腦效能

依據預設，系統會執行病毒和間諜軟體掃描，以將對用戶端電腦資源的影響降至最低。您可以變更某些掃描設定，以進一步最佳化效能。此處建議的多項工作，對於在虛擬機器 (VM) 上的來賓作業系統中執行 Symantec Endpoint Protection 的環境裡非常有用。

Table 82: 調整掃描以改善 Windows 電腦的電腦效能

工作	說明
修改排程掃描和隨選掃描的調整和壓縮檔案選項	您可以調整排程和隨選掃描的下列選項： - 變更調整選項 您可以將掃描調整變更為「最佳應用程式效能」。當您利用此設定架構掃描時，掃描可以啟動，但僅會在用戶端電腦閒置時執行。如果將作用中掃描架構為在收到新定義檔時執行，當使用者正在使用電腦時，掃描可能長達 15 分鐘無法執行。 - 變更要掃描壓縮檔的層數 預設層數為 3。您可以將層數變更為 1 或 2，以縮短掃描時間。 如需詳細資訊，請參閱： 為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描
使用可繼續的掃描	對於網路中具有大型磁碟區的電腦，可將排程掃描架構為可繼續的掃描。 掃描持續時間選項會提供執行掃描的指定期間。如果掃描在指定持續時間結束前未完成，則該掃描會在下個排程掃描期間繼續。該掃描會在其停止的地方繼續，直到完成整個磁碟區的掃描為止。通常，您可以使用伺服器上的掃描持續時間選項。 Note: 如果您懷疑電腦受到感染，請勿使用可繼續的掃描。您應執行會掃描整個電腦的完整掃描。如果掃描可在指定時間間隔之前完成，也不應使用可繼續的掃描。 如需詳細資訊，請參閱： 設定在 Windows 電腦上執行的排程掃描
調整自動防護設定	您可以針對檔案系統的自動防護掃描，調整一些可能改善用戶端電腦效能的設定。 您可以設定下列選項： - 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 如果遠端電腦的自動防護掃描已啟用，則務必啟用「只在執行檔案時」。 如需詳細資訊，請參閱： 自訂 Windows 用戶端的自動防護
允許所有掃描略過受信任檔案	病毒和間諜軟體掃描包含稱為「智慧型掃描」的選項，該選項會略過受信任的檔案。預設會啟用「智慧型掃描」選項。 您可以變更掃描略過之檔案類型的信任層級： - 賽門鐵克和社群信任的檔案 此層級會略過賽門鐵克和賽門鐵克社群信任的檔案。 - 賽門鐵克信任的檔案 此層級僅會略過賽門鐵克信任的檔案。 如需詳細資訊，請參閱： 修改 Windows 用戶端的全域掃描設定
隨機設定排程掃描	在部署了多部虛擬機器 (VM) 的虛擬環境中，同時進行掃描會造成資源問題。例如，單一伺服器可執行 100 部或更多的 VM。在這些 VM 上同時進行掃描，會耗盡伺服器上的資源。 您可以隨機設定掃描，以限制對伺服器的影響。請參閱： 隨機設定掃描以在 Windows 用戶端上的虛擬環境中改善電腦效能
在虛擬環境中使用共用智慧型掃描快取	使用共用智慧型掃描快取就無需重新掃描 Symantec Endpoint Protection 已確認未感染病毒的檔案。 您可以使用共用智慧型掃描快取在用戶端電腦上進行排程和手動掃描。共用智慧型掃描快取是安裝在伺服器或虛擬環境中的個別應用程式。請參閱： 啟用網路型共用智慧型掃描快取
停用提早啟動防惡意軟體 (ELAM) 偵測	Symantec Endpoint Protection ELAM 會與 Windows ELAM 搭配，共同提供對惡意啟動驅動程式的防護。請參閱： 管理提早啟動防惡意軟體 (ELAM) 偵測

Table 83: 調整掃描以改善 Mac 電腦的電腦效能

工作	說明
啟用閒置狀態掃描	適用於在 Mac 電腦上執行之用戶端的排程掃描。 此選項會將排程掃描架構為僅在電腦處於閒置狀態時執行。請參閱： 為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描
修改壓縮檔設定	適用於自動防護和隨選掃描。 您可以啟用或停用該選項，但無法指定要掃描的壓縮檔層數。請參閱： 自訂 Mac 用戶端的自動防護

Table 84: 調整掃描以改善 Linux 電腦的電腦效能

工作	說明
依資料夾類型掃描	預設為掃描所有資料夾類型。您可以指定任一資料夾： Root 、 Home 、 Bin 、 Usr 、 Etc 和 Opt 。如果您知道某個資料夾是安全的，可以在清單中將其取消勾選。
依檔案類型掃描	預設為掃描所有檔案。如果您知道某種特定副檔名是安全的，可以在清單中將其取消勾選。
掃描壓縮檔內的檔案	您可以在壓縮檔內展開最多三層目錄結構。您可以將層數變更為 1 或 2，以縮短掃描時間。
掃描安全風險	可讓您選擇是否掃描安全風險。安全風險可透過 LiveUpdate 進行更新。掃描安全風險會讓掃描速度變慢，但會提升安全性。預設為掃描安全風險。若要改善電腦效能，請取消勾選此選項。

更多資訊

[在用戶端電腦上管理掃描](#)

調整掃描以增強對用戶端電腦的防護

預設情況下，Symantec Endpoint Protection 可提供高層級的安全防護。您可以進一步增強這道防護。

在 Windows 電腦上執行的用戶端與在 Mac 和 Linux 電腦上執行的用戶端的設定不同。

NOTE

如果您增強對用戶端電腦的防護，則可能會影響電腦的效能。

Table 85: 調整掃描以增強對 Windows 電腦的防護

工作	說明
鎖定掃描設定	預設情況下，某些設定處於鎖定狀態；您也可以鎖定其他設定，這樣使用者就無法變更其電腦上的防護。
修改管理員定義掃描的設定	您應該檢查或修改下列選項： - 掃描效能 將掃描調整設定為「最佳掃描效能」。不過，此設定可能會影響用戶端電腦的效能。即使在電腦不是處於閒置狀態時，掃描也會執行。 - 排程掃描持續時間 預設情況下，排程掃描會執行直到指定的時間間隔到期為止，然後在用戶端電腦閒置時繼續執行。您可以將掃描持續時間設定為「到掃描完成」。 Warning! 請確定已啟用智慧型掃描查詢。如果停用智慧型掃描查詢，雲端防護將會完全停用。排程掃描和隨選掃描永遠使用雲端來評估入口網站檔案。自動防護也使用雲端來評估入口網站檔案。 如需詳細資訊，請參閱： 為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描 Windows 用戶端如何從雲端接收定義檔
指定更嚴格的掃描偵測動作	為偵測指定「隔離」、「刪除」或「終止」動作。 Note: 對安全風險偵測使用「刪除」或「終止」動作時，請小心。這些動作可能會導致一些合法應用程式喪失功能。 如需詳細資訊，請參閱： 變更 Symantec Endpoint Protection 進行偵測時採取的動作
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。請參閱： 修改 Windows 用戶端的全域掃描設定
調整自動防護設定	您可以變更下列選項： - 檔案快取 您可以停用檔案快取，以便讓「自動防護」重新掃描無毒檔案。 - 網路設定 預設情況下，網路磁碟機上的檔案只有在處於執行狀態時才會進行掃描。 如需詳細資訊，請參閱： 自訂 Windows 用戶端的自動防護

Table 86: 調整掃描以增強對 Mac 和 Linux 電腦的防護

工作	說明
修改掃描的壓縮檔選項	預設設定是掃描壓縮檔中 3 層深的檔案。若要增強防護，請保留 3 層深，或變更為 3 (若為較深的層級)。請參閱： 為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描 為在 Linux 電腦上執行的用戶端自訂管理員定義掃描
鎖定自動防護設定	預設情況下，某些設定處於鎖定狀態；您也可以鎖定其他設定，這樣使用者就無法變更其電腦上的防護。在 Mac 用戶端和 Linux 用戶端上，您可以按下「啟用自動防護」，然後按下鎖定圖示來鎖定設定。請參閱： 自訂 Mac 用戶端的自動防護 自訂 Linux 用戶端的自動防護

工作	說明
指定更嚴格的掃描偵測動作	針對偵測指定「隔離」或「刪除」(僅限 Linux) 動作。 自 14.3 RU1 起，為 Linux 用戶端架構偵測動作已棄用。 Note: 對安全風險偵測使用「刪除」動作時，請小心。這些動作可能會導致一些合法應用程式喪失功能。 如需詳細資訊，請參閱： 變更 Symantec Endpoint Protection 進行偵測時採取的動作

管理「下載鑑識」偵測

「自動防護」包含一項名為「下載鑑識」的功能，該功能可檢查使用者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。

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

「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。只有 Windows 電腦上執行的用戶端支援「下載智慧型掃描」。

NOTE

如果您針對用戶端電腦上的電子郵件安裝「自動防護」，則「自動防護」也會掃描使用者以電子郵件附件形式收到的檔案。

如需詳細資訊，請參閱：

[在用戶端電腦上管理掃描](#)

Table 87: 管理「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」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) 將於使用者開啟或執行該檔案時掃描該檔案。請參閱： Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策
檢視下載風險分布報告以檢視「下載鑑識」偵測	您可以使用下載風險分布報告，檢視「下載智慧型掃描」在您的用戶端電腦上偵測到的檔案。您可以依照 URL、Web 網域或應用程式排序報告。您也可以查看使用者是否已選擇允許某個偵測到的檔案。 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。例如，使用者可以使用 Internet Explorer 嘗試下載「下載鑑識」偵測的檔案。如果使用者接著使用 Firefox 嘗試下載該檔案，則風險詳細資料會將 Internet Explorer 顯示為入口網站。 顯示在報告中的使用者允許檔案可能表示偵測誤報。 您也可以指定在使用者允許進行任何新下載時，接收電子郵件通知。請參閱： 設定管理員通知 使用者可以透過回應顯示的偵測通知允許下載檔案。 Symantec Endpoint Protection Manager 會產生並透過電子郵件傳送每週報告，其中包括提供給管理員的報告。您必須在安裝過程中為管理員指定電子郵件地址，或在管理員屬性中架構。您也可以從主控台的「報告」標籤中產生報告。請參閱： 執行和自訂快速報告

工作	說明
為特定檔案或 Web 網域建立例外	您可以為使用者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。請參閱： • 建立應用程式例外 • 從 Windows 用戶端上的掃描中排除信任的 Web 網域 Note: 如果用戶端電腦使用帶驗證功能的代理，您必須為 Symantec URL 指定信任的 Web 網域例外。這些例外可讓您的用戶端電腦與「賽門鐵克智慧型掃描」和其他重要的賽門鐵克網站進行通訊。 如需建議例外的相關資訊，請參閱下列文章： • 如何測試智慧型掃描與賽門鐵克授權伺服器連線能力 • 允許 Symantec Endpoint Protection 連線至賽門鐵克信譽和授權伺服器所需的代理伺服器排除項 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 > 網路網路選項 > 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。如果已啟用「自動信任從內部網路網站下載的任何檔案」選項，則 Symantec Endpoint Protection 會允許使用者從任何清單中的網站下載的任何檔案。 Symantec Endpoint Protection 會在使用者登入時及每四個小時檢查「網路網路選項」信任網站清單的更新。 Note: 「下載智慧型掃描」只辨識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」不支援由「網路網路選項 > 安全性 > 自動偵測內部網路」選項搜尋到的網站。
確定已啟用智慧型掃描查詢	「下載智慧型掃描」需要使用來自賽門鐵克「智慧型掃描」的信譽資料進行關於檔案的決策。如果您停用「智慧型掃描查詢」，則「下載鑑識」會執行，但只會偵測信譽最差的檔案。依預設，「智慧型掃描查詢」已啟用。請參閱： 自訂下載鑑識設定
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。指定的動作不僅會影響偵測結果，也會影響使用者是否可與偵測結果進行互動。 例如，您可將針對未證明檔案採取的動作變更為「忽略」。然後，「下載智慧型掃描」會一律允許未證明的檔案，而不會向使用者發出警示。 • 針對「下載鑑識」偵測結果向使用者發出警示。 當啟用通知時，惡意檔案靈敏度的設定會影響使用者收到的通知數量。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。 您可以關閉通知，讓使用者在「下載智慧型掃描」進行偵測時無法進行動作。如果您將通知保持啟用狀態，則可將針對未證明檔案進行的動作設為「忽略」，一律允許這些偵測，且不通知使用者。 不論通知設定為何，當「下載鑑識」偵測到未證明的檔案且動作為「提示」時，使用者就可以允許或攔截檔案。如果使用者允許該檔案，則該檔案會自動執行。 當啟用通知且「下載智慧型掃描」隔離某個檔案時，使用者可以復原隔離動作並允許使用檔案。 Note: 如果使用者允許使用隔離的檔案，則此檔案不會自動執行。使用者可以從 Temporary Internet Files 資料夾執行此檔案。通常，資料夾位置為下列其中之一： — Windows 8 及更新版本：磁碟機:\Users\使用者名稱\AppData\Local\Microsoft\Windows\INetCache — Windows Vista / 7：磁碟機:\Users\使用者名稱\AppData\Local\Microsoft\Windows\Temporary Internet Files 如需詳細資訊，請參閱： 自訂下載鑑識設定

工作	說明
允許用戶端將有關信譽偵測的資訊傳送給賽門鐵克	依預設，用戶端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。請參閱： 管理用戶端傳送給賽門鐵克的匿名或非匿名資料

Symantec Endpoint Protection 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。Symantec Endpoint Protection 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

Symantec Endpoint Protection 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。

Symantec Endpoint Protection 如何使用進階機器學習？

如需詳細資訊，請參考下列各主題：

- [進階機器學習如何運作？](#)
- [AML 如何與雲端搭配運作？](#)
- [如何架構 AML？](#)
- [疑難排解進階機器學習](#)

進階機器學習如何運作？

進階機器學習 (AML) 引擎會透過學習程序判斷檔案是良好還是無效檔案。賽門鐵克安全機制應變中心會訓練該引擎來辨識惡意屬性，以及定義 AML 引擎用來進行偵測的規則。賽門鐵克會在實驗室環境中使用下列程序訓練和測試 AML 引擎：

- LiveUpdate 會下載 AML 模型至用戶端，並執行數日。
- AML 引擎會學習用戶端執行的應用程式，並使用用戶端的遙測資料侵入。每個用戶端電腦均屬於會將模型的相關資訊傳回賽門鐵克的 Global Intelligence Network 的一部分。
- 賽門鐵克會根據賽門鐵克從用戶端的遙測資料所探索的資訊來調整 AML 模型。
- 賽門鐵克會修改 AML 模型來攔截侵入通常攻擊的應用程式。

AML 屬於靜態資料掃描程式 (SDS) 引擎的一部分。SDS 引擎包括模擬器、Intelligent Threat Cloud Service (ITCS) 和 CoreDef-3 定義檔引擎。

Symantec Endpoint Protection 在下載鑑識、行為分析 (SONAR) 以及病毒和間諜軟體掃描中使用進階機器學習，這些均使用智慧型掃描查詢來偵測威脅。

AML 如何與雲端搭配運作？

賽門鐵克利用 Intelligent Threat Cloud Service (ITCS) 來確認 AML 在用戶端電腦上進行的偵測正確。有時在 AML 向 ITCS 查詢之後，可能會撤銷原判。雖然 AML 引擎不需要 Symantec Insight，但此回饋會使賽門鐵克能夠訓練 AML 演算法，以減少誤報和增加檢出。當電腦在線上時，Symantec Endpoint Protection 可以阻止平均 99% 的威脅。請參閱：

- [Windows 用戶端如何從雲端接收定義檔](#)
- [Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？](#)

如何架構 AML？

您無法架構進階機器學習。依據預設，LiveUpdate 會下載 AML 定義檔。不過，您需要確定已啟用以下技術。

Table 88: 確保 AML 保護用戶端電腦的步驟

工作	說明
步驟 1：確定已啟用雲端查詢可用性	AML 對 Symantec Insight 進行的查詢稱為信譽查詢、雲端查詢或智慧型掃描查詢。如果智慧型掃描查詢已啟用，針對行為分析 (SONAR) 和病毒與間諜軟體掃描的 AML 偵測會具有較少的誤報。若要驗證已啟用智慧型掃描查詢，請參閱： Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策 此外，請確定已啟用用戶端傳送資訊。此資訊有助於賽門鐵克衡量和改善偵測技術的有效性。請參閱： 瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性
步驟 2：確定已啟用 Bloodhound 偵測	將 Bloodhound 偵測層級設定為自動或主動。請參閱： 修改 Windows 用戶端的全域掃描設定 當 AML 引擎遇到某些高度風險檔案時，用戶端會自動進入更主動的掃描。 進入主動掃描模式時： • 隨即會重新啟動掃描。 • 用戶端上會出現以下通知： <pre>#####</pre> 在主動模式中，您可能需要進一步管理誤報。

工作	說明
步驟 3：確定 LiveUpdate 下載高密度定義檔 (選用)	LiveUpdate 一律會下載 AML 內容。 LiveUpdate 會下載一個主動的定義檔集，可搭配您自雲端取得的低頻寬政策使用。您可以停用 AML 內容，使其不再透過 LiveUpdate 下載。 從 LiveUpdate 至 Symantec Endpoint Protection Manager，請參閱： 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager 從 Symantec Endpoint Protection Manager 至 Windows 用戶端，請參閱： 還原為舊版 Symantec Endpoint Protection 安全更新 關於 LiveUpdate 下載的內容類型
步驟 4：處理誤報	使用「例外」政策管理誤報。請參閱： 建立病毒和間諜軟體掃描的例外 處理和避免 SONAR 偵測誤報 當 Symantec Endpoint Protection 刪除您認為是安全的檔案時的最佳實務

疑難排解進階機器學習

進階機器學習偵測的日誌和報告與其他 SDS 引擎相同。若要查看具有最新威脅的報告，請針對「網路中偵測到的新風險」執行風險報告。

您可針對 AML 偵測執行排程報告。在「報告」頁面上，按下「排程報告」>「新增」>「電腦狀態」>「進階機器學習 (靜態) 內容派送」。Symantec Endpoint Protection Manager 網域必須在雲端主控台中註冊，才能顯示此報告。

如需詳細資訊，請參閱：

- [如何執行排程報告](#)
- [檢視日誌](#)

Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？

Symantec Endpoint Protection 使用功能強大的模擬器，來防範來自自訂封包程式惡意軟體的攻擊。針對自動防護和病毒掃描，這個模擬器可將掃描效能和有效性較舊版至少提升 10%。此防躲避技術可解決包裝的惡意軟體迷惑技術，並能偵測自訂封包程式中隱藏的惡意軟體。

什麼是自訂封包程式？

許多惡意軟體程式利用「封包程式」，或是用來壓縮和加密檔案進行傳輸的軟體程式。然後，當這些檔案到達使用者的電腦時，即會在記憶體中執行。

雖然封包程式本身並非惡意軟體，但攻擊者會使用它們來隱藏惡意軟體並混淆程式碼的實際意圖。一旦將惡意軟體解除封包，它會執行並啟動其惡意酬載，經常會略過防火牆、閘道和惡意軟體防護。攻擊者已從使用商業封包程式 (例如 UPX、PECompact、ASProtect 和 Themida) 轉變為建立自訂封包程式。自訂封包程式使用專屬的演算法來略過標準的偵測技術。

許多新出現的自訂封包程式為變種。它們使用防偵測策略，其中程式碼本身經常變更，但惡意軟體的目的和功能仍保持不變。自訂封包程式也使用聰明的方式來將程式碼插入目標程序並變更其執行流程，經常能擺脫解除封包程式常式。它們當中的一部分為運算密集型，會呼叫特殊 API 使得難以解除封裝。

自訂封包程式變得愈來愈老練，可隱藏攻擊，發現時多半為時已晚。

Symantec Endpoint Protection 模擬器如何防範自訂封包程式？

Symantec Endpoint Protection 中的高速模擬器會欺騙惡意軟體，讓其認為它是在一般電腦上執行。模擬器實則會在用戶端電腦上的輕量虛擬沙箱中將自訂封裝檔案解除封裝並觸發。然後，惡意軟體會將其酬載開啟至滿載，造成威脅在遏制的環境中顯現。包含了防毒引擎和啟發式引擎的靜態資料掃描程式會對該酬載採取行動。沙箱是暫時的，會在處理完威脅之後消失。

模擬器需要模擬作業系統、API 和處理器指示的複雜技術。它會同時管理虛擬記憶體並執行各種啟發式和偵測技術來檢查酬載。對乾淨的檔案平均需要 3.5 毫秒，而對惡意軟體則需要 300 毫秒，大約是用戶端使用者在桌面上按下檔案所需的相同時間。模擬器可以快速偵測威脅，對效能和產能的影響程度最低，因此用戶端使用者不會被中斷。此外，模擬器會使用最低的磁碟空間量和虛擬環境中最多 16 MB 的記憶體。

模擬器可以與其他防護技術搭配使用，其中包括進階機器學習、記憶體攻擊緩和、行為監控和信譽分析。有時會有多個引擎加入，協同回應以預防、偵測和矯正攻擊。

模擬器不使用 Internet。不過，根據模擬器從自訂封包程式解壓縮的惡意軟體，靜態資料掃描程式內的引擎可能需要 Internet。請參閱：

[Symantec Endpoint Protection 如何使用進階機器學習？](#)

如何架構模擬器？

模擬器內建在 Symantec Endpoint Protection 軟體中，因此您不需要架構它。賽門鐵克會定期新增或變更模擬器內容以取得新威脅，並每季發行內容更新至模擬器引擎。依據預設，LiveUpdate 會自動下載此內容與病毒和間諜軟體定義檔。請參閱：

[將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)

Symantec Endpoint Protection Manager 不會包括模擬器所進行偵測的個別日誌。您可以改為在風險日誌和掃描日誌中尋找任何偵測。請參閱：

[檢視日誌](#)

管理 Windows 用戶端的隔離所

您可以將隔離所設定當成病毒疫情策略的重要部分進行管理。

當病毒和間諜軟體掃描或行為分析 (SONAR) 偵測到威脅時，Symantec Endpoint Protection 會將可疑的檔案放到受感染電腦的本機隔離所。用戶端可以對檔案進行修復、修復並還原或刪除。

用戶端偵測到風險並隔離檔案時，用戶端會通知管理伺服器。您可以讓管理伺服器自動要求和擷取隔離的檔案。管理伺服器會上載並儲存資料庫中的風險範例、顯示其事件詳細資料，以及可讓您對其進行下載以進行進一步分析。您可能想要將檔提交給內部惡意程式或安全團隊以進行反向工程，或提交給其他沙箱以進行分析。如果您認為原判是誤報，則請連絡 Broadcom 支援以記錄案例。

NOTE

自 14.3 RU2 起，您無法再使用中央隔離所伺服器。而是用戶端會將隔離的檔案提交給 Symantec Endpoint Protection Manager。

將隔離的檔案上載到管理伺服器

管理伺服器預設不會從用戶端擷取隔離的檔案。您必須啟用此設定。

上載隔離的檔案

1. 在主控台中，按一下「管理」>「網域」>「編輯網站屬性」。
2. 在「一般」標籤上，按一下「從用戶端上載隔離的檔案」，然後按一下「確定」。

下載用戶端所隔離並上載到管理伺服器的檔案

1. 在主控台中，按一下「監控器」>「日誌」，然後選取「風險」日誌類型。
2. 開啟日誌，並選取隔離的檔案，然後在「動作」下拉式清單中按一下「下載用戶端所隔離的檔案」。

架構隔離所設定

您可以針對隔離處理用戶端上檔案的方式來修改下列選項：

- 新的定義檔到達用戶端時，會發生什麼情況：

新的定義檔到達時，用戶端預設會重新掃描隔離所中的項目，並以無訊息方式自動修復和還原項目。如果您已在隔離所中建立某個檔案或應用程式的例外，則 Symantec Endpoint Protection 會在新的定義檔到達後還原該檔案。

- 儲存所隔離項目的位置：

隔離所預設會將備份、修復和隔離的檔案儲存在預設資料夾中。檔案超過指定的期限或儲存它們的目錄達到特定大小時，隔離所清除功能會自動刪除隔離所中的檔案。它會在 30 天後自動刪除檔案。

如果您不想要使用用戶端電腦上的預設隔離所目錄 (%ProgramData%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Quarantine) 來儲存隔離的檔案，則可以指定不同的本機目錄。您可以使用路徑擴展，方法是在輸入路徑時使用百分比符號。例如，您可以輸入 %COMMON_APPDATA%。如此便不允許使用相對路徑。

架構隔離所設定

1. 在「病毒和間諜軟體防護」政策中，按一下「**Windows 設定**」>「隔離所」。
2. 在「一般」標籤上，架構「當新的病毒定義檔到達時」和「本機隔離所選項」下方的選項。
指定如何處理隔離的項目以及儲存所隔離檔案的本機資料夾。請參閱：

[隔離所：一般](#)

3. 按下「確定」。

刪除隔離所中的檔案

隔離所會在指定的天數後自動刪除已修復的檔案、備份檔案和隔離的檔案。您可以架構隔離所在儲存檔案的資料夾達到指定大小時或特定天數之後刪除檔案。

您應該定期檢查用戶端電腦的隔離所，以避免累積大量檔案。當網路上出現新病毒疫情 (爆發) 時，檢查隔離的檔案。

請將發生不明感染的檔案保留在隔離所。用戶端在收到新的定義檔時會重新掃描隔離所中的項目，而且可能會刪除或修復檔案。

如果有保留檔案備份，或已從受信任的來源取得檔案複本，則可以刪除隔離的檔案。您可以在受感染的電腦上直接刪除隔離的檔案，或使用 Symantec Endpoint Protection 主控台中的「風險日誌」進行刪除。

NOTE

如果 Symantec Endpoint Protection 偵測到壓縮檔案中的風險，壓縮檔案會整個遭到隔離。然而，「風險」日誌包含壓縮檔案中每個檔案的單獨項目。為成功刪除壓縮檔中的所有風險，您必須選取壓縮檔中的所有檔案。

將用戶端架構為自動刪除檔案

1. 在「病毒和間諜軟體防護」政策中，按一下「**Windows 設定**」>「隔離所」。
2. 在「清理」標籤上，勾選或取消勾選啟用或停用它們的選項，然後架構時間間隔和大小上限。請參閱：
[隔離：清除](#)
3. 按下「確定」。

從風險日誌中刪除檔案

1. 在主控台中，按下「監視器」。
2. 在「日誌」標籤的「日誌類型」清單方塊中，選取「風險」日誌，然後按下「檢視日誌」。
3. 執行下列其中一項動作：
 - 在日誌中選取一個檔案被隔離的項目。
 - 選取壓縮檔案中所有的檔案項目。
您必須讓壓縮檔案中的所有項目顯示於日誌檢視中。您可以使用「其他設定」下的「限制」選項，增加檢視的項目數。
4. 從「動作」清單方塊中，選取「從隔離所刪除」。
5. 按下「開始」。
6. 在顯示的對話方塊中，按一下「刪除」，然後按一下「確定」。

使用自訂 YARA 規則掃描 SEP 用戶端電腦

在 14.3 RU4 和更新版本中，Symantec Endpoint Protection (SEP) 和 Symantec Endpoint Security (SES) 提供 YARA 掃描程式來偵測惡意程式。

使用此文件來建立自訂 YARA 規則。會在隨選掃描、作用中掃描和排定的掃描期間套用您編寫的 YARA 規則。

NOTE

YARA 規則未與自動防護或 Linux 代理程式搭配運作。

關於 YARA

步驟 1：建置和編譯自訂 YARA 規則

若要編譯和部署自訂 YARA 規則，請使用下列 YARA 分佈：<https://github.com/VirusTotal/yara/releases/tag/v4.2.1>

- 14.3 RU4 和 14.3 RU5 需要 YARA 編譯器 4.2.1。
- 您使用其他版本的編譯器編譯的 YARA 規則不受套用。
- YARA 規則可以使用 PE、ELF、Math、Hash 和 Time 模組。包含不支援模組的 YARA 規則集不能使用。

如需詳細資訊，請參閱：

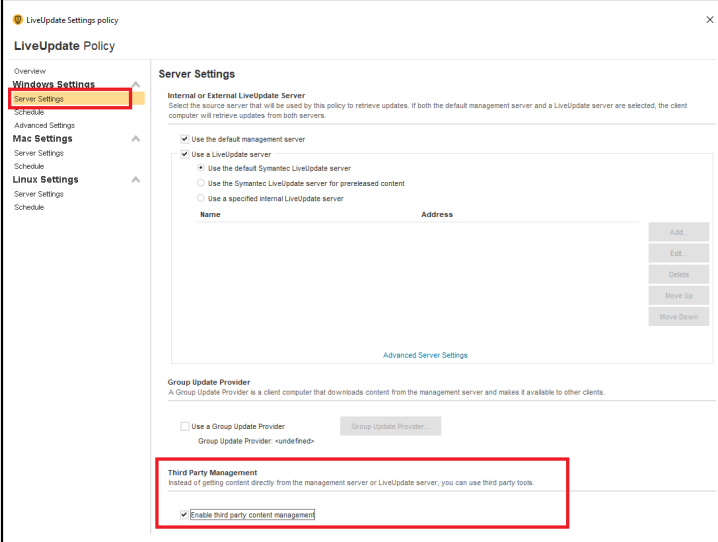
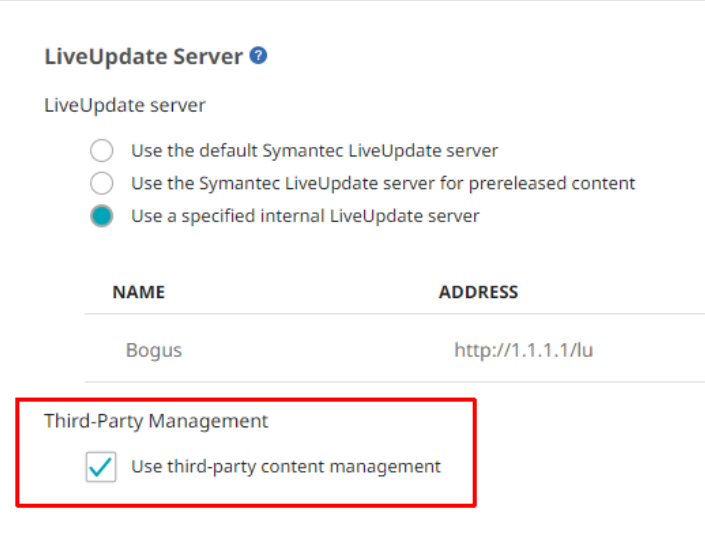
- 如何編寫自訂 YARA 規則：[YARA 規則指南：學習此惡意軟體研究工具](#)
- YARA 文件和更新：<http://virustotal.github.io/yara/>

步驟 2：在 SEP 和 SES 中啟用第三方管理

在 Symantec Endpoint Protection Manager 或 Symantec Endpoint Security 管理主控台中，啟用此設定，讓第三方分佈工具更新受管用戶端。

啟用受管用戶端的第三方管理

1. 執行下列其中一項工作：

九月	SES
在 LiveUpdate 政策中，選取「伺服器設定 > 啟用第三方內容管理」。 將 LiveUpdate 設定政策架構為允許將第三方內容派送至受管用戶端	在系統政策中，於「LiveUpdate 伺服器」下方選取「使用第三方內容管理」 LiveUpdate 伺服器設定
	

步驟三：將已編譯的 .yara 檔複製至用戶端

在您編寫自訂 YARA 規則並將其編譯成 .yara 檔案之後，請將 .yara 檔案複製至 SEP 用戶端上的 inbox 資料夾。

將已編譯的 .yara 檔案複製至用戶端

1. 將 .yara 檔案複製至 C:\ProgramData\Symantec\Symantec Endpoint Protection\Current Version\inbox。
例如：C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8262.5000\inbox
.yara 檔案會自動移至下列位置，而 SDS 定義引擎會在其中執行它：C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8262.5000\Data\Definitions\SDSDefs

NOTE

如果出現名為 Invalid 的資料夾，而其中包含您的 .yara 檔案，則您可能未在上一步正確地啟用第三方管理。如果 .yara 檔案消失，則您可以在 C:\ProgramData\Symantec\Symantec Endpoint Protection\Current Version\Definitions 和 AdvMLDefs 或 SDSDefs 中找到它。

步驟四：執行可評估自訂 YARA 規則的掃描

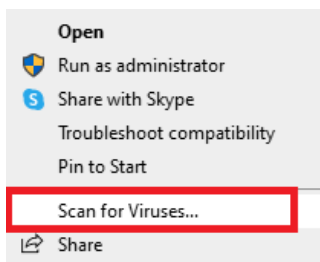
執行掃描時，會在掃描中使用提供的 YARA 規則。如果掃描在惡意軟體範例中的規則與型樣之間找到相符項目，則用戶端會記錄可指定規則名稱和中繼資料的事件。

NOTE

用戶端只會記錄事件，並不會採取其他動作。

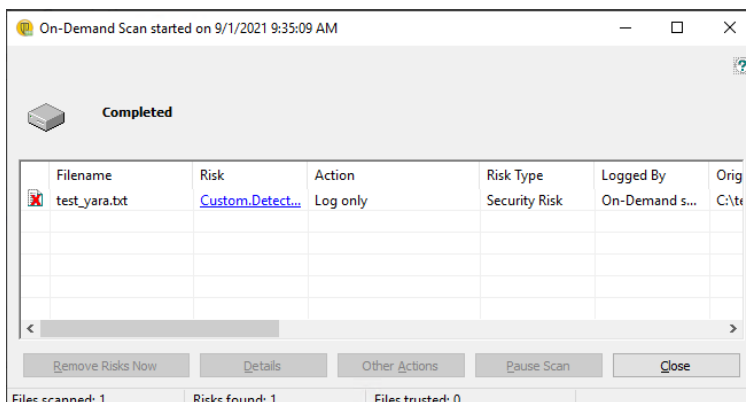
執行可評估自訂 YARA 規則的隨選掃描

1. 將您要用來測試自訂規則功能的惡意軟體測試檔案下載至用戶端電腦。
2. 在測試檔案上按一下滑鼠右鍵，然後選取「掃描病毒...」。



即會出現隨選掃描的結果。偵測到並使用 YARA 規則判定為威脅的檔案會標示為 Custom.Detection 風險。

例如：

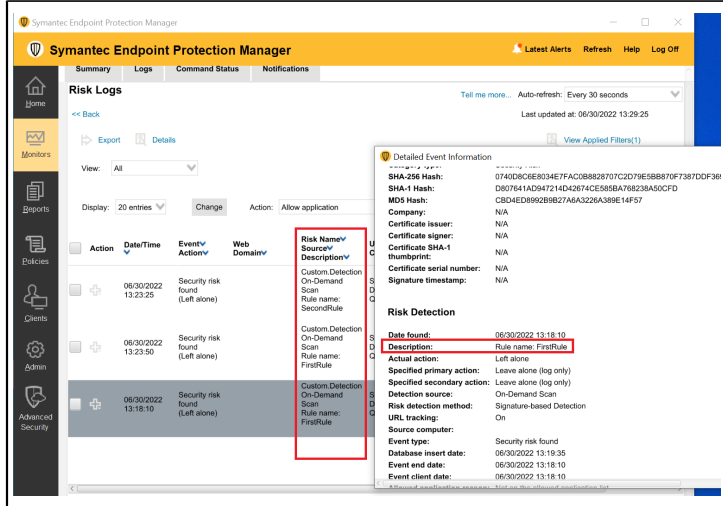
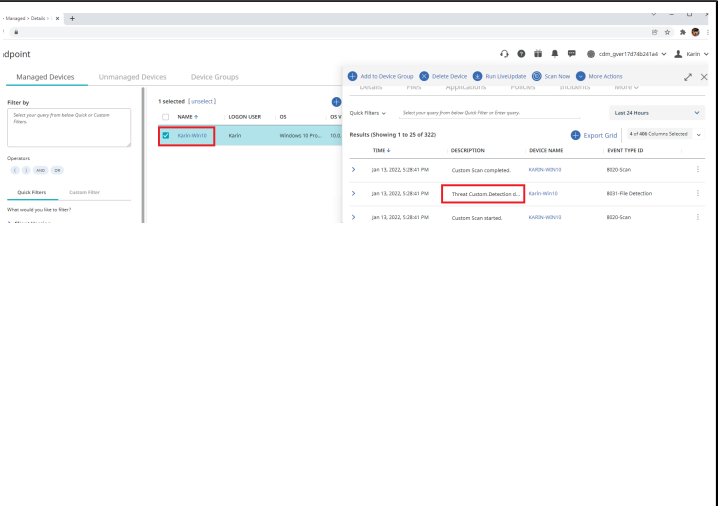


步驟五：檢視 YARA 規則偵測的日誌

完成掃描之後，用戶端會將偵測的相關資訊上傳至管理主控台。您可以檢視特定偵測事件的詳細資訊。

檢視 YARA 規則偵測的日誌

1. 執行下列其中一項工作：

九月	ES
在「監視器」頁面 > 「日誌」標籤上，選取「風險」日誌類型，然後選取「檢視日誌」。	在「裝置」頁面上，選取裝置，然後開啟「活動記錄」標籤。
	

取代已部署的 YARA 規則集 (可選)

若要刪除或取代已部署的 YARA 規則集，請部署新的規則集。您也可以建立永不回傳判定的「虛擬」規則集。例如：

```
rule empty
{
    condition:
        false
}
```

已知問題

- 針對編譯的規則集，檔案大小上限為 4 MB。
- 無法正確載入包含不受支援模組匯入的 YARA 規則集。
- 其他 YARA 規則會增加掃描時間。賽門鐵克具有內建防護功能，僅允許使用 Yara 引擎掃描單一檔案一秒。這可避免因過大或複雜的規則集，導致效能大幅降低。
- 若您套用 YARA 規則集，然後在雲端主控台將用戶端從 14.3 RU4 升級到 14.3 RU5，則「防惡意軟體政策 > 政策名稱」欄位中的 YARA 規則集檔案名稱會遺失，並替換為自訂 YARA。若要解決此問題，請將 YARA 規則集重新套用到升級後的 14.3 RU5 用戶端。

管理顯示在用戶端電腦上的病毒和間諜軟體通知

您可以決定是否要在用戶端電腦上顯示病毒和間諜軟體事件的通知。您可以自訂有關偵測結果的訊息。請參閱：

[在用戶端電腦上管理掃描](#)

Table 89: 管理顯示在用戶端電腦上的病毒和間諜軟體通知的工作

工作	說明
自訂掃描偵測訊息	對於 Windows 和 Linux 用戶端電腦，您可以為以下掃描類型架構偵測訊息： - 所有自動防護類型 - 排程掃描和隨選掃描 對於排程掃描，您可以為每個掃描架構個別的訊息。 Note: 如果某個程序持續將相同的安全性風險下載到用戶端電腦，則經過三次偵測之後，自動防護會自動停止傳送通知。自動防護也會停止記錄事件。不過，在某些情況下，自動防護不會停止傳送通知和記錄事件。當偵測對應的動作為「略過 (只記錄)」時，自動防護會繼續傳送通知和記錄事件。 對於 Mac 用戶端電腦，您可以架構套用至所有排程掃描、隨選掃描和自動防護偵測的偵測訊息。這些通知訊息會出現在 macOS 通知中心。無法為 Mac 自訂訊息。 如需詳細資訊，請參閱： 為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描 為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描 為在 Linux 電腦上執行的用戶端自訂管理員定義掃描
變更關於下載鑑識偵測的使用者通知設定	僅適用於 Windows 用戶端電腦。 您可以變更使用者收到的「下載智慧型掃描」偵測相關通知。請參閱：管理「下載鑑識」偵測
變更關於行為分析 (SONAR) 偵測的使用者通知設定	僅適用於 Windows 用戶端電腦。 您可以變更使用者收到的偵測相關通知。請參閱：管理 SONAR
選擇是否顯示自動防護結果對話方塊	僅適用於 Windows 用戶端電腦。 僅適用於檔案系統的自動防護。請參閱：為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描
設定自動防護電子郵件通知	僅適用於 Windows 用戶端電腦。 當自動防護電子郵件掃描發現風險時，自動防護可傳送電子郵件通知，向電子郵件寄件者及您指定的任何其他電子郵件地址發出警示。您也可以電子郵件中插入警告。 對於 Internet 電子郵件自動防護，您也可以指定當自動防護掃描電子郵件時，顯示有關掃描進度的通知。「Internet 電子郵件自動防護」僅適用於低於 14.2 RU1 的用戶端版本。請參閱：為 Windows 電腦上的電子郵件掃描自訂自動防護
允許使用者查看掃描進度及啟動或停止掃描	僅適用於 Windows 用戶端電腦。 您可以架構是否顯示掃描進度對話方塊。您可以架構是否允許使用者暫停或延遲掃描。 如果您允許使用者檢視掃描進度，用戶端使用者介面的主頁上會顯示掃描進度對話方塊連結。另外也會顯示重新排程下一個排程掃描的連結。請參閱：允許使用者在 Windows 電腦上檢視掃描進度並與掃描互動
架構警告、錯誤和提示	僅適用於 Windows 用戶端電腦。 您可以啟用或停用幾種顯示在用戶端電腦上有關病毒和間諜軟體防護事件的警示類型。請參閱：在 Windows 電腦上修改日誌處理及通知設定
啟用或停用 Windows 8 樣式使用者介面上的彈出式通知	適用於 Windows 8 上執行的用戶端。 您可以啟用或停用出現在 Windows 8 樣式使用者介面中，用於偵測和其他重要事件的彈出式通知。請參閱：啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知

關於出現在 Windows 8 用戶端上的彈出式通知

在 Windows 8 電腦上，用於惡意軟體偵測及其他重要 Symantec Endpoint Protection 事件的彈出式通知會出現在 Windows 8 樣式使用者介面和 Windows 8 桌面上。不論使用者目前檢視的是哪一個介面，通知都會警示使用者 Windows 8 樣式使用者介面或 Windows 8 桌面上發生的事件。

您可以在用戶端電腦上啟用或停用彈出式通知。

NOTE

Windows 8 組態也包含顯示或隱藏通知的設定。只有在將 Windows 8 架構為顯示 Symantec Endpoint Protection 彈出式通知時，才會出現這些通知。在 Windows 8 樣式使用者介面上，「設定」窗格或「變更電腦設定」選項可讓您顯示或隱藏應用程式通知。如需詳細資訊，請參閱 Windows 8 使用者說明文件。

如果使用者在 Windows 8 樣式使用者介面上按下某個通知，則 Windows 8 桌面便會出現。如果使用者按下 Windows 8 桌面上的通知，通知將會消失。針對惡意軟體或安全風險偵測，使用者可以在 Windows 8 桌面上，於「偵測結果」對話方塊中檢視偵測相關資訊。

當 Symantec Endpoint Protection 通知 Windows 8 偵測到影響 Windows 8 樣式應用程式的惡意軟體或安全風險時，在應用程式磚上會出現一個警示圖示。當使用者按下這個磚時，Windows 應用程式商店便會出現，讓使用者可以重新下載該應用程式。

更多資訊

- [啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知](#)
- [Symantec Endpoint Protection 如何在 Windows 8 電腦上處理偵測](#)

啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知

依據預設，彈出式通知會出現在 Windows 8 樣式使用者介面與 Windows 8 桌面上，用於惡意軟體偵測及其他重要 Symantec Endpoint Protection 事件。

使用者可以檢視 Windows 桌面，以查看產生通知之事件的詳細資料。使用者可能需要採取動作，例如重新下載應用程式。不過，在某些情況下，您可能想要向使用者隱藏這些彈出式通知。您可以在 Symantec Endpoint Protection 架構中啟用或停用此類型的通知。

NOTE

Windows 8 組態也包含顯示或隱藏通知的設定。只有在將 Windows 8 架構為顯示 Symantec Endpoint Protection 通知時，才會出現這些通知。在 Windows 8 樣式使用者介面上，「設定」窗格或「變更電腦設定」選項可讓您顯示或隱藏應用程式通知。如需詳細資訊，請參閱 Windows 8 使用者說明文件。

啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 通知

1. 在主控台的「用戶端」標籤中，於「政策」標籤的「位置限定的設定」下方，按下「用戶端使用者介面控制設定」旁的「伺服器控制」。
2. 在「伺服器控制」旁，按下「自訂」。
3. 在「用戶端使用者介面設定」對話方塊中，勾選或取消勾選「一般」下的「啟用 Windows Toast 通知」。
4. 按下「確定」。

更多資訊

[關於出現在 Windows 8 用戶端上的彈出式通知](#)

管理提早啟動防惡意軟體 (ELAM) 偵測

提早啟動防惡意軟體 (ELAM) 會在電腦啟動時，以及第三方驅動程式初始化之前，為您網路中的電腦提供防護。可以當作驅動程式或 Rootkit 載入的惡意軟體，可能會在作業系統完全載入且 Symantec Endpoint Protection 啟動前攻擊系統。Rootkit 有時候可能會躲避病毒和間諜軟體掃描。提早啟動防惡意軟體會在系統啟動時偵測這些 Rootkit 和惡意驅動程式。

NOTE

Microsoft Windows 8 或更新版本和 Windows Server 2012 或更新版本支援 ELAM。

Symantec Endpoint Protection 提供的 ELAM 驅動程式可搭配 Windows ELAM 驅動程式使用，以提供防護。您必須啟用 Windows ELAM 驅動程式，Symantec ELAM 驅動程式才會起作用。

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。

Table 90: 管理 ELAM 偵測

工作	說明
檢視用戶端電腦的 ELAM 狀態	您可以在「電腦狀態」日誌中檢視 Symantec Endpoint Protection ELAM 是否已啟用。請參閱： 檢視日誌
檢視 ELAM 偵測	您可以在「風險日誌」中檢視提早啟動防惡意軟體偵測。 當 Symantec Endpoint Protection ELAM 架構為報告偵測到 Windows 未知的惡意驅動程式或惡意的重要驅動程式時，Symantec Endpoint Protection 會將偵測結果記錄為「只記錄」。依預設，Windows ELAM 允許載入未知的驅動程式。
啟用或停用 ELAM	您可能需要停用 Symantec Endpoint Protection ELAM，以協助改善電腦效能。請參閱： • 調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項 • 調整掃描以改善電腦效能
如果您得到誤報，請調整 ELAM 偵測設定	Symantec Endpoint Protection ELAM 設定提供的選項可將惡意驅動程式或惡意的重要驅動程式視為不明。惡意的重要驅動程式就是被識別為惡意軟體但卻是啟動電腦所必需的驅動程式。如果得到可攔截重要驅動程式的誤報偵測，您可以選取覆寫選項。如果您攔截重要驅動程式，則可能會使用戶端電腦無法啟動。 Note: ELAM 不支援個別驅動程式的特定例外。覆寫選項可全域套用到 ELAM 偵測。 如需詳細資訊，請參閱： 調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項
對 Symantec Endpoint Protection 無法矯正的 ELAM 偵測執行 Power Eraser	在某些情況下，ELAM 偵測需要 Power Eraser。在這類情況下，日誌中會顯示一則訊息，建議您執行 Power Eraser。您可以從主控台執行 Power Eraser。Power Eraser 也是賽門鐵克說明工具的一部分。您應在 Rootkit 模式下執行 Power Eraser。請參閱： • 從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析 • 使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解

調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項

Symantec Endpoint Protection 提供的 ELAM 驅動程式會搭配 Microsoft ELAM 驅動程式使用，以便在電腦啟動時，為您網路中的電腦提供防護。Microsoft Windows 8 或更新版本和 Windows Server 2012 或更新版本支援這些設定。

Symantec Endpoint Protection ELAM 驅動程式是一種特殊類型的驅動程式，該驅動程式會先初始化並檢測其他啟動驅動程式是否包含惡意程式碼。當驅動程式偵測到啟動驅動程式時，它會判斷該驅動程式是良好、惡意還是未知。Symantec Endpoint Protection 驅動程式接著將資訊傳遞給 Windows，以決定允許還是攔截偵測到的驅動程式。

您無法為個別的 ELAM 偵測建立例外；但是，您可以建立全域例外，將所有的惡意驅動程式記錄為未知。依預設，允許載入未知的驅動程式。

對於需要矯正的某些 ELAM 偵測，您可能需要執行 Power Eraser。Power Eraser 是賽門鐵克說明工具的一部分。

NOTE

「自動防護」會掃描載入的所有驅動程式。

調整 Symantec Endpoint Protection ELAM 選項

1. 在 Symantec Endpoint Protection Manager 主控台的「政策」標籤上，開啟「病毒和間諜軟體防護」政策。
2. 在「防護技術」下，選取「提早啟動防惡意軟體驅動程式」。
3. 勾選或取消勾選「啟用賽門鐵克提早啟動防惡意軟體」。

您必須啟用 Windows ELAM 驅動程式，才能啟用這個選項。您可以使用 Windows 群組原則編輯器或登錄檔編輯器來檢視及修改 Windows ELAM 設定。如需詳細資訊，請參閱 Windows 說明文件。

4. 如果您要僅記錄偵測，請在「偵測設定」下，選取「將偵測記錄為不明，以便 Windows 允許載入驅動程式」。
5. 按下「確定」。

管理提早啟動防惡意軟體 (ELAM) 偵測

使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解

架構站台使用私用 Insight 伺服器進行信譽查詢

如果您已購買並安裝 Symantec Insight for Private Clouds，則私用 Insight 伺服器設定可讓您將用戶端信譽查詢指向內部網路伺服器。Symantec Insight for Private Clouds 通常安裝在缺乏網際網路連線的網路中。私用 Insight 伺服器會儲存賽門鐵克智慧型掃描之信譽資料庫的複本。Symantec Endpoint Protection 信譽查詢由私用 Insight 伺服器處理，而不是由 Symantec Insight 伺服器進行處理。

私用伺服器會透過加密的安全連線來下載 Symantec Insight 資料。您可以手動更新 Insight 資料，也可以使用第三方工具來自動檢查更新及下載資料。您所使用的更新方法，取決於您的網路，以及執行 Symantec Insight for Private Clouds 所在伺服器的類型。

當您使用私用 Insight 伺服器時，賽門鐵克既不會接收也不會傳送任何有關檔案信譽的查詢。

NOTE

此工作不適用於內部部署的 Symantec EDR 伺服器。請參閱：

[將用戶端架構為使用 Symantec EDR 或私用伺服器進行信譽查詢和提交](#)

架構站台使用私用 Insight 伺服器進行信譽查詢

1. 在主控台的「管理員」頁面上，選取「伺服器」。
2. 選取站台，然後在「工作」下方選取「編輯站台屬性」。
3. 在「私用 Insight 伺服器」標籤中，確認已勾選「啟用私用 Insight 伺服器」。

您也必須輸入「名稱」、「伺服器 URL」和「通訊埠」。

NOTE

如果您將現有伺服器 URL 變更為無效的 URL，用戶端會使用先前有效的私用 Insight 伺服器 URL。如果您先前從未架構過伺服器 URL，而現在輸入的 URL 無效，用戶端會使用預設的 Symantec Insight 伺服器。

在下次活動訊號出現時，您的用戶端會開始使用指定的私用伺服器來進行信譽查詢。

更多資訊

- [Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策](#)
- [將用戶端群組架構為使用私用伺服器進行信譽查詢和提交](#)

將用戶端架構為使用 Symantec EDR 或私用伺服器進行信譽查詢和提交

您可以將用戶端信譽查詢 (智慧型掃描查詢) 從群組導向至私用內部網路伺服器。私用伺服器可以是 Symantec EDR 硬體裝置或是您購買並在您的網路中分開安裝的 Symantec Insight for Private Clouds 伺服器。

以下是用於群組的私用伺服器選項：

- Symantec EDR

Symantec EDR 伺服器會收集用戶端偵測的相關資料並提供蒐證分析。當您使用 Symantec EDR 伺服器時，Symantec Endpoint Protection 會將所有信用查詢 (查詢) 和大部分的用戶端傳送資訊類型傳送到 Symantec EDR。然後，Symantec EDR 將查詢或傳送資訊傳送至賽門鐵克。請注意，Symantec EDR 會接收防毒、行為分析 (SONAR) 和 IPS 傳送資訊，但是它不會接收檔案信譽傳送資訊。Symantec Endpoint Protection 一律將檔案信譽傳送資訊直接傳送至賽門鐵克。

- Symantec Insight for Private Clouds

此選項會將信譽查詢從群組中的用戶端重新導向至私用 Insight 伺服器。私用 Insight 伺服器會儲存賽門鐵克的智慧型掃描信譽資料庫的複本。私用 Insight 伺服器會處理信譽查詢，而不是由 Symantec Insight 伺服器進行處理。當您使用私用 Insight 伺服器時，用戶端會繼續將關於偵測的傳送傳送至賽門鐵克。您通常會在暗網中使用私用 Insight 伺服器，暗網是指與 Internet 中斷連線的網路。在該情況下，賽門鐵克無法接收任何用戶端傳送。

如需詳細資訊，請參閱：

[瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性](#)

您也可以將私用伺服器架構複製到其他用戶端群組。

您可以指定多台私用伺服器以負載平衡網路流量。您也可以指定多組伺服器來管理容錯移轉。

當您選擇啟用 EDR 伺服器時，EDR 連線狀態會顯示在用戶端使用者介面以及管理主控台日誌和報告中。若要與 EDR 伺服器通訊，Symantec Endpoint Protection 用戶端必須至少執行病毒和間諜軟體防護。

將用戶端架構為使用 **Symantec EDR** 或私用伺服器

1. 在主控台中，移至「用戶端」，然後選取應使用私用伺服器清單的群組。
2. 在「政策」標籤上，按一下「外部通訊設定」。
3. 在「私有雲端」標籤上，按一下「啟用私用伺服器以管理我的資料」。
4. 根據您使用的伺服器類型，按一下「使用 **Symantec EDR** 伺服器進行智慧型掃描查詢和提交」或「使用私用 **Insight** 伺服器進行智慧型掃描查詢」。

您不應該在優先順序清單中混合伺服器類型。

5. 如果您希望用戶端使用賽門鐵克伺服器進行信譽查詢以及用戶端防毒和行為分析 (SONAR) 傳送，請按一下「當私用伺服器不可用時，使用賽門鐵克伺服器」。

用戶端一律將檔案信譽傳送傳送至賽門鐵克。

6. 在「私用伺服器」下方，按一下「新增 > 新伺服器」。
7. 在「新增私用伺服器」對話方塊中，選取通訊協定，然後輸入 URL 的主機名稱。
8. 指定伺服器的埠號。
9. 若要新增優先順序群組，請按一下「新增 > 新群組」。
10. (選用) 若要將設定套用至其他用戶端群組，請按一下「複製設定」。選取群組和位置，然後按一下「確定」。

自訂病毒和間諜軟體掃描

您可以為在環境的裝置上執行的管理員定義掃描 (排程掃描和隨選掃描) 自訂選項。您也可以為「自動防護」自訂選項。

Table 91: 自訂 Windows 電腦上的病毒和間諜軟體掃描

工作	說明
自訂「自動防護」設定	您可以採用多種方法自訂「自動防護」，包括進行下列設定的架構： 「自動防護」掃描的檔案類型 「自動防護」進行偵測時所採取的動作 「自動防護」偵測的使用者通知 您還可以針對檔案系統的「自動防護」掃描，啟用「掃描結果」對話方塊。請參閱： 自訂 Windows 用戶端的自動防護 為 Windows 電腦上的電子郵件掃描自訂自動防護
自訂管理員定義的掃描	您可以為排程掃描和隨選掃描自訂以下類型的選項。 - 壓縮檔 - 調整選項 - 進階排程選項 - 有關偵測的使用者通知 如需詳細資訊，請參閱： 為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描 您也可以自訂掃描動作。
調整 ELAM 設定	如果您認為 ELAM 影響電腦的效能，可能會想要啟用或停用 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 偵測。或者，如果出現太多誤報 ELAM 偵測結果，您也可以覆寫預設偵測設定。請參閱： 管理提早啟動防惡意軟體 (ELAM) 偵測
調整「下載鑑識」設定	您可能需要調整惡意檔案靈敏度，以增加或減少偵測的數目。您也可以修改偵測的動作和偵測的使用者通知。請參閱： 自訂下載鑑識設定
自訂掃描動作	您可以變更 Symantec Endpoint Protection 進行偵測時採取的動作。請參閱： 變更 Symantec Endpoint Protection 進行偵測時採取的動作
自訂全域掃描設定	您可能需要自訂全域掃描設定，以增加或減少用戶端電腦上的防護程度。請參閱： 修改全域掃描設定 全域掃描選項
自訂「病毒和間諜軟體防護」的其他選項	您可以指定用戶端傳送至 Symantec Endpoint Protection Manager 的風險事件類型。請參閱： 在 Windows 電腦上修改日誌處理及通知設定

Table 92: 自訂 Mac 電腦上的病毒和間諜軟體掃描

工作	說明
自訂自動防護	您可以為 Mac 電腦上執行的用戶端自訂「自動防護」設定。請參閱： 自訂 Mac 用戶端的自動防護
自訂管理員定義的掃描	您可以自訂一般設定和通知，以及掃描優先順序。 您也可以啟用在定義檔過時的情況下警示使用者的警告。請參閱： 為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描
自訂全域掃描選項	您可以指定希望自動防護、排程掃描和手動掃描來掃描的檔案或資料夾。請參閱： 修改全域掃描設定 Mac 全域掃描選項

Table 93: 自訂 Linux 電腦上的病毒和間諜軟體掃描

工作	說明
自訂「自動防護」設定	您可以採用多種方法自訂「自動防護」，包括進行下列設定的架構： 「自動防護」掃描的檔案類型 「自動防護」進行偵測時所採取的動作 自 14.3 RU1 起，為 Linux 用戶端架構偵測動作已棄用。 「自動防護」偵測的使用者通知 您還可以針對檔案系統的「自動防護」掃描，啟用或停用「掃描結果」對話方塊。請參閱： 自訂 Linux 用戶端的自動防護
自訂管理員定義的掃描	您可以為排程掃描和隨選掃描自訂以下類型的選項。 - 檔案和資料夾類型 - 壓縮檔 - 安全風險 - 排程選項 - 偵測動作 自 14.3 RU1 起，為 Linux 用戶端架構偵測動作已棄用。 - 使用者通知
自訂掃描動作 (自 14.3 RU1 起已棄用)	您可以變更 Symantec Endpoint Protection 進行偵測時採取的動作。請參閱： 變更 Symantec Endpoint Protection 進行偵測時採取的動作
自訂全域掃描選項 (自 14.3 RU3 起可用)	您可以自訂設定，而這些設定套用至所有在 Linux 用戶端上執行的病毒和間諜程式掃描。請參閱： 修改全域掃描設定 Linux 全域掃描選項
自訂「病毒和間諜軟體防護」的其他選項 (自 14.3 RU1 起已棄用)	您可以指定用戶端傳送至 Symantec Endpoint Protection Manager 的風險事件類型。請參閱： 在 Linux 電腦上修改日誌處理設定

更多資訊

[在用戶端電腦上管理掃描](#)

自訂在 Mac 電腦上執行的病毒和間諜軟體掃描

您可以為 Mac 電腦上執行的管理員定義掃描 (排程掃描和隨選掃描) 自訂選項。您也可以為「自動防護」自訂選項。

Table 94: 自訂 Mac 電腦上的病毒和間諜軟體掃描

工作	說明
自訂自動防護	您可以為 Mac 電腦上執行的用戶端自訂「自動防護」設定。請參閱： 自訂 Mac 用戶端的自動防護
自訂管理員定義的掃描	您可以自訂一般設定和通知，以及掃描優先順序。 您也可以啟用在定義檔過時的情況下警示使用者的警告。請參閱： 為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描
自訂全域掃描選項	您可以指定希望自動防護、排程掃描和手動掃描來掃描的檔案或資料夾。請參閱： 修改全域掃描設定

自訂在 Linux 電腦上執行的病毒和間諜軟體掃描

您可以為 Linux 電腦上執行的管理員定義掃描 (排程掃描和隨選掃描) 自訂選項。您也可以為「自動防護」自訂選項。

Table 95: 自訂 Linux 電腦上的病毒和間諜軟體掃描

工作	說明
自訂「自動防護」設定	您可以採用多種方法自訂「自動防護」，包括進行下列設定的架構： 「自動防護」掃描的檔案類型 「自動防護」進行偵測時所採取的動作 自 14.3 RU1 起，為 Linux 用戶端架構偵測動作已棄用。 「自動防護」偵測的使用者通知 您還可以針對檔案系統的「自動防護」掃描，啟用或停用「掃描結果」對話方塊。請參閱： 自訂 Linux 用戶端的自動防護
自訂管理員定義的掃描	您可以為排程掃描和隨選掃描自訂以下類型的選項。 - 檔案和資料夾類型 - 壓縮檔 - 安全風險 - 排程選項 - 偵測動作 自 14.3 RU1 起，為 Linux 用戶端架構偵測動作已棄用。 - 使用者通知
自訂掃描動作 (自 14.3 RU1 起已棄用)	您可以變更 Symantec Endpoint Protection 進行偵測時採取的動作。請參閱： 變更 Symantec Endpoint Protection 進行偵測時採取的動作
自訂全域掃描選項 (自 14.3 RU3 起可用)	您可以為在 Linux 用戶端上執行的掃描自訂全域設定。請參閱： 修改全域掃描設定
自訂「病毒和間諜軟體防護」的其他選項 (自 14.3 RU1 起已棄用)	您可以指定用戶端傳送至 Symantec Endpoint Protection Manager 的風險事件類型。請參閱： 在 Linux 電腦上修改日誌處理設定

自訂 Windows 用戶端的自動防護

您可能需要自訂 Windows 用戶端的自動防護設定。

架構 **Windows** 用戶端的自動防護

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Windows** 設定」下的「防護技術」下方，按下「自動防護」。
3. 在「掃描詳細資料」標籤上，確保已勾選「啟用自動防護」。

WARNING

如果您停用「自動防護」，即使「下載智慧型掃描」已啟用，仍將無法運作。

4. 在「掃描中」的「檔案類型」下方，選取下列其中一個選項：
 - 掃描所有檔案
此選項是預設值，也是最安全的選項。
 - 只掃描選取的副檔名
您可以選取此選項以改善掃描效能，然而，這樣可能會降低對電腦的防護。

-
5. 在「其他選項」下方，勾選或取消勾選「掃描安全風險」。
 6. 按下「進階掃描與監控」，變更為觸發自動防護掃描之動作的選項，以及自動防護處理磁片掃描的方式。
 7. 按下「確定」。
 8. 在「網路設定」下方，勾選或取消勾選「掃描遠端電腦上的檔案」，以啟用或停用網路檔案的自動防護掃描。
依預設，自動防護只會在執行檔案時掃描遠端電腦上的檔案。
您可能需要停用網路掃描，以改善掃描和電腦效能。
 9. 當啟用了遠端電腦上的檔案掃描時，請按下「網路設定」以修改網路掃描選項。
 10. 在「網路設定」對話方塊中，執行下列任何動作：
 - 啟用或停用「自動防護」信任執行「自動防護」之遠端電腦上的檔案。
 - 架構「自動防護」掃描的網路快取選項。
 11. 按下「確定」。
 12. 在「動作」標籤上，設定任一選項。請參閱：
[變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
您也可以為自動防護設定矯正選項。
 13. 在「通知」標籤上，設定任何通知選項。請參閱：
[管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)
 14. 在「進階」標籤上，設定下列任何選項：
 - 開機和關機
 - 重新載入選項
 15. 在「其他選項」下方，按下「檔案快取」或「風險追蹤程式」。
 16. 架構檔案快取或風險追蹤程式設定，然後按下「確定」。
 17. 架構完此政策後，按下「確定」。

更多資訊

- [自訂在 Windows 電腦上執行的病毒和間諜軟體掃描](#)
- [在用戶端電腦上管理掃描](#)

自訂 Mac 用戶端的自動防護

您可能需要為在 Mac 電腦上執行的用戶端自訂自動防護設定。

自訂 Mac 用戶端的自動防護

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「Mac 設定」下方的「防護技術」下，按下「自動防護及 SONAR」。
3. 在「掃描詳細資料」標籤的上方，按下鎖定圖示以鎖定或解除鎖定所有設定。
4. 勾選或取消勾選下列任何選項：
 - 啟用自動防護
 - 自動修復受感染的檔案
 - 無法修復的隔離所檔案
 - 掃描壓縮檔

-
5. 在「一般掃描詳細資料」下方，指定「自動防護」掃描的檔案。

NOTE

若要從掃描中排除檔案，您必須選取「掃描除指定資料夾外的所有位置」，然後增加例外政策以指定要排除的檔案。請參閱：

[從掃描中排除檔案或資料夾](#)

6. 在「掃描掛載磁碟詳細資料」下方，勾選或取消勾選任何可用選項。
7. 在「可疑行為偵測」下方，勾選或取消勾選啟用「可疑行為偵測」。
自版本 14.3 RU1 起提供此選項。
8. 在「通知」標籤上，設定任一通知選項，然後按下「確定」。

更多資訊

- [自訂在 Mac 電腦上執行的病毒和間諜軟體掃描](#)
- [變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
- [管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)

自訂 Linux 用戶端的自動防護

您可能需要為在 Linux 電腦上執行的用戶端自訂自動防護設定。

NOTE

自 14.3 RU1 起，為 Linux 用戶端在「動作」標籤、「通知」標籤和「進階」標籤 (步驟 9、10 和 11) 上架構選項已棄用。

自訂 Linux 用戶端的自動防護

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「Linux 設定」下方的「防護技術」下，按下「自動防護」。
3. 在「掃描詳細資料」標籤上，勾選或取消勾選「啟用自動防護」。
4. 在「掃描中」的「檔案類型」下方，按下列其中一個選項：
 - 掃描所有檔案
此選項是預設值，也是最安全的選項。
 - 只掃描選取的副檔名
您可以選取此選項以改善掃描效能，然而，這樣可能會降低對電腦的防護。
(自 14.3 RU1 時不提供)
5. 在「其他選項」下方，勾選或取消勾選「掃描安全風險」。
6. 按下「進階掃描與監控」，變更為觸發自動防護掃描之動作的選項，以及自動防護處理壓縮檔掃描的方式。
7. 按下「確定」。
8. 在「網路設定」下方，勾選或取消勾選「掃描遠端電腦上的檔案」，以啟用或停用網路檔案的自動防護掃描。
依預設，自動防護只會在執行檔案時掃描遠端電腦上的檔案。
您可能需要停用網路掃描，以改善掃描和電腦效能。
9. 在「動作」標籤上，設定任一選項。請參閱：
[變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
您也可以為自動防護設定矯正選項。

-
10. 在「通知」標籤上，設定任何通知選項。請參閱：
[管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)
 11. 在「進階」標籤上，勾選或取消勾選「啟用快取」。
設定快取大小，或接受預設值。
 12. 按下「確定」。

更多資訊

- [自訂在 Linux 電腦上執行的病毒和間諜軟體掃描](#)
- [變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
- [管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)

為 Windows 電腦上的電子郵件掃描自訂自動防護

您可以為 Windows 電腦上的電子郵件掃描自訂自動防護。

為 **Windows** 電腦上的電子郵件掃描自訂自動防護

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Windows** 設定」下方，選取下列其中一個選項：
 - **Microsoft Outlook** 自動防護
 - **Internet** 電子郵件自動防護*
 - **Lotus Notes** 自動防護*

* 僅適用於低於 14.2 RU1 的用戶端版本。
3. 在「掃描詳細資料」標籤上，勾選或取消勾選「啟用 **Internet** 電子郵件自動防護」。
4. 在「掃描中」的「檔案類型」下方，選取下列其中一個選項：
 - 掃描所有檔案
此選項是預設值，也是最安全的選項。
 - 只掃描選取的副檔名
您可以選取此選項以改善掃描效能，然而，這樣可能會降低對電腦的防護。
5. 勾選或取消勾選「掃描壓縮檔內的檔案」。
6. 在「動作」標籤上，設定任一選項。請參閱：
[變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
7. 在「通知」標籤上的「通知」下方，勾選或取消勾選「在受感染的電腦上顯示通知訊息」。您也可以自訂這個訊息。
8. 在「電子郵件通知」下方，勾選或取消勾選下列任何選項：
 - 插入警告至電子郵件訊息
 - 傳送電子郵件給寄件者
 - 傳送電子郵件給其他人

您可以自訂訊息文字，並加上一項警告。對於 Internet 電子郵件自動防護，您也必須指定郵件伺服器。
9. 對於 Internet 電子郵件自動防護，在「進階」標籤上的「加密連線」下方，啟用或停用加密的 POP3 或 SMTP 連線。
10. 在「大量郵件病蟲啟發式掃描」下方，勾選或取消勾選「離埠病蟲啟發式掃描」。
11. 架構完此政策後，按下「確定」。

更多資訊

-
- [自訂在 Windows 電腦上執行的病毒和間諜軟體掃描](#)
 - [管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)

為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描

您可能需要為在 Windows 電腦上執行的用戶端自訂排程掃描或隨選掃描。您可以設定壓縮檔的掃描選項，並最佳化對電腦的掃描或掃描效能。

為在 **Windows** 電腦上執行的用戶端自訂管理員定義的掃描

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Windows** 設定」下方，按下「管理員定義掃描」。
3. 執行下列其中一項動作：
 - 在「排程掃描」下，選取要自訂的排程掃描，或建立新的排程掃描。
 - 在「管理員隨選掃描」下方，按下「編輯」。
4. 在「掃描詳細資料」標籤上，選取「進階掃描選項」：
 - 在「壓縮檔」標籤上，您可以減少要掃描的壓縮檔的層數。如果減少層數，則有可能會提高用戶端電腦的效能。
 - 在「調整」標籤上，變更最佳用戶端電腦效能或最佳掃描效能的調整層級。

按下「確定」，以儲存變更。

5. 僅針對排程掃描，在「排程」標籤上，設定下列任何選項：
 - 掃描持續時間
您可以設定掃描在暫停並等待用戶端電腦閒置多長時間後開始執行。您也可以隨機產生掃描開始時間。
 - 錯過掃描排程
您可以為錯過的掃描指定重試時間間隔。
6. 在「動作」標籤上，變更任何偵測動作。請參閱：
[變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
7. 在「通知」標籤上，啟用或停用掃描執行偵測時在用戶端電腦上顯示的通知。請參閱：
[管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)
8. 按下「確定」。

更多資訊

- [自訂在 Windows 電腦上執行的病毒和間諜軟體掃描](#)
- [設定在 Windows 電腦上執行的排程掃描](#)

為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描

您可以分別自訂排程掃描和隨選掃描。其中有部分選項不同。

自訂在 **Mac** 電腦執行的排程掃描

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Mac** 設定」下方，選擇「管理員定義掃描」。
3. 在「排程掃描」下，選取要自訂的排程掃描，或建立新的排程掃描。
若需新掃描，可以手動建立新掃描，或者從範本建立排程掃描。
4. 在「掃描詳細資料」標籤的「掃描磁碟機和資料夾」下方，選取您要掃描的項目。
5. 您也可以啟用或停用閒置狀態掃描。啟用此選項可改善電腦效能，停用此選項則可改善掃描效能。
6. 按下「確定」。
編輯此政策中包含的任何其他掃描的掃描詳細資料。

-
7. 在「通知」標籤上，啟用或停用與掃描偵測相關的通知訊息。此設定會套用到您在此政策中包含的所有排程掃描。
 8. 在「一般設定」標籤上，設定下列任何選項：

- 掃描選項
- 動作
- 警示

這些選項會套用到您在此政策中包含的所有排程掃描。

9. 按下「確定」。

自訂在 Mac 電腦上執行的隨選掃描

1. 在「病毒和間諜軟體防護政策」頁面的「**Mac** 設定」下方，選取「管理員定義掃描」。
2. 在「管理員隨選掃描」下方，按下「編輯」。
3. 在「掃描詳細資料」標籤的「掃描磁碟機和資料夾」下方，選取您要掃描的項目。
您也可以為掃描偵測指定動作，並啟用或停用壓縮檔的掃描。
4. 在「通知」標籤上，啟用或停用偵測的通知。
您也可以指定顯示在用戶端上的訊息。
5. 按下「確定」。

更多資訊

- [自訂在 Mac 電腦上執行的病毒和間諜軟體掃描](#)
- [設定在 Mac 電腦上執行的排程掃描](#)
- [變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
- [管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)

為在 Linux 電腦上執行的用戶端自訂管理員定義掃描

您可能需要為在 Linux 電腦上執行的用戶端自訂排程掃描或隨選掃描。您可以設定壓縮檔的掃描選項，並最佳化對電腦的掃描或掃描效能。

為在 Linux 電腦上執行的用戶端自訂管理員定義掃描

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「Linux 設定」下方，按下「管理員定義的掃描」。
3. 執行下列其中一項動作：
 - 在「排程掃描」下，選取要自訂的排程掃描，或建立新的排程掃描。
 - 在「管理員隨選掃描」下方，按下「編輯」。
4. 在「掃描詳細資料」標籤上，勾選「掃描所有資料夾」，或指定您要掃描的特定資料夾。
5. 按下「掃描所有檔案」或「只掃描選取的副檔名」，並指定您要掃描的副檔名。
自 14.3 RU1 起，不提供「只掃描選取的副檔名」選項。
6. 如果選擇了「掃描壓縮檔內的檔案」，您可以減少要掃描的壓縮檔的層數。如果減少層數，則有可能會提高用戶端電腦的效能。
7. 勾選或取消勾選「掃描安全風險」。
8. 僅針對排程掃描，在「排程」標籤上，設定下列任何選項：
 - 掃描排程
您可以設定掃描的執行頻率：每日、每週或每月。
 - 錯過掃描排程

您可以為錯過的掃描指定重試時間間隔。

9. 在「動作」標籤上，變更任何偵測動作。請參閱：

[變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)

自 14.3 RU1 起，為 Linux 用戶端架構偵測動作已棄用。

10. 在「通知」標籤上，啟用或停用掃描執行偵測時在用戶端電腦上顯示的通知。請參閱：

[管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)

11. 按下「確定」。

更多資訊

- [自訂在 Linux 電腦上執行的病毒和間諜軟體掃描](#)
- [設定在 Linux 電腦上執行的排程掃描](#)
- [變更 Symantec Endpoint Protection 進行偵測時採取的動作](#)
- [管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)

隨機設定掃描以在 Windows 用戶端上的虛擬環境中改善電腦效能

您可以隨機設定排程掃描，以改善 Windows 用戶端電腦的效能。隨機設定在虛擬化環境中很重要。

例如，您可以將掃描排程在晚上 8:00 執行。如果您選取 4 小時的時間間隔，則用戶端電腦上的掃描會於晚上 8:00 至凌晨 12:00 之間的某個隨機時間開始。

隨機設定掃描以在虛擬化環境中改善電腦效能

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Windows** 設定」下方，按一下「管理員定義掃描」。
3. 建立新的排程掃描，或選取要編輯的現有排程掃描。
4. 在「新增排程掃描」或「編輯排程掃描」對話方塊中，按下「排程」標籤。
5. 在「掃描排程」下方，選取掃描應執行的頻率。
6. 在「掃描持續時間」下方，勾選「最多掃描」並選取小時數。小時數會控制隨機設定掃描的時間間隔。
7. 確認啟用了「在此期間隨機設定掃描開始時間 (建議在 VM 中)」。
8. 按下「確定」。
9. 確認將政策套用到包含執行虛擬機器之電腦的群組。

更多資訊

- [調整掃描以改善電腦效能](#)
- [設定在 Windows 電腦上執行的排程掃描](#)

修改全域掃描設定

您可以自訂設定，而這些設定套用到所有在用戶端電腦上執行的病毒和間諜程式掃描。您可能需要修改這些選項，以增進用戶端電腦的安全性。

NOTE

如果修改這些選項以增進對用戶端電腦的防護，可能會影響用戶端電腦的效能。

如需詳細資訊，請參閱：

- [在用戶端電腦上管理掃描](#)
- [自訂病毒和間諜軟體掃描](#)

修改全域掃描設定

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Windows** 設定」、「**Mac** 設定」或「**Linux** 設定」下方，按一下「全域掃描選項」。
3. 架構下列任何作業系統的選項：

Windows	如需詳細資訊，請參閱： 全域掃描選項
Mac	如需詳細資訊，請參閱： Mac 全域掃描選項
Linux	(自 14.3 RU3 起) 如需詳細資訊，請參閱： Linux 全域掃描選項

4. 按下「確定」。

在 Windows 電腦上修改日誌處理及通知設定

每項病毒和間諜軟體防護政策包含的選項，都可以套用到 Windows 用戶端電腦上執行的所有病毒和間諜軟體掃描。

您可以設定下列選項：

- 指定預設的 URL，讓 Symantec Endpoint Protection 在修復變更了瀏覽器首頁的安全風險時使用該網址。
- 指定風險日誌處理選項。
- 定義檔過期或遺失時警告使用者。
- 將虛擬影像排除在自動防護或管理員定義掃描的範圍之外。

在 Windows 電腦上修改日誌處理及通知設定

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Windows** 設定」下方，按一下「其他」。
指定「**Internet** 瀏覽器防護」的選項。
3. 在「日誌處理」標籤上，設定事件過濾、日誌存留和日誌彙總的選項。
4. 在「通知」標籤上，架構全域通知。請參閱：
[自訂在 Windows 電腦上執行的病毒和間諜軟體掃描](#)
5. 按下「確定」。

更多資訊

[管理顯示在用戶端電腦上的病毒和間諜軟體通知](#)

在 Linux 電腦上修改日誌處理設定

每項病毒和間諜軟體防護政策包含的日誌處理設定，都可以套用到 Linux 用戶端電腦上執行的所有病毒和間諜軟體掃描。

自 14.3 RU1 起，修改 Linux 用戶端的日誌處理設定已棄用。

Linux 電腦上的日誌處理設定

-
1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
 2. 在「Linux 設定」下方，按下「其他」。
 3. 在「日誌處理」標籤上，設定事件過濾、日誌存留和日誌彙總的選項。

更多資訊

[檢視日誌](#)

自訂下載鑑識設定

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。請參閱：

- [自訂在 Windows 電腦上執行的病毒和間諜軟體掃描](#)
- [管理「下載鑑識」偵測](#)

自訂下載智慧型掃描設定

1. 在主控台中，開啟「病毒和間諜軟體防護」政策，然後選擇「下載防護」。
2. 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。

3. 將惡意檔案靈敏度的滑桿移至適當層級。

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。

4. 檢查下列選項，用作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
- 使用者已知不超過 **x** 天的檔案

如果未證明的檔案符合這些準則，「下載鑑識」會將這些檔案偵測為惡意檔案。

5. 請確定勾選「自動信任從信任的 **Internet** 或內部網路網站下載的任何檔案」。
6. 在「動作」標籤的「惡意檔案」下方，指定第一個動作和第二個動作。
7. 在「未證明的檔案」下方，指定動作。
8. 在「通知」標籤上，指定當「下載鑑識」進行偵測時，是否在用戶端電腦上顯示訊息。

您也可以自訂當使用者允許「下載智慧型掃描」偵測到的檔案時，顯示之警告訊息的文字。

9. 按下「確定」。

變更 Symantec Endpoint Protection 進行偵測時採取的動作

您可以架構掃描進行偵測時應採取的一或多個動作。每個掃描均有本身的動作集，例如「清除」、「隔離」、「刪除」或「略過 (只記錄)」。

在 Windows 用戶端和 Linux 用戶端上，每個偵測類別均可架構第一個和第二個動作；以便於在第一個動作無法進行時，能進行第二個動作。

自 14.3 RU1 起，為 Linux 用戶端架構偵測動作已棄用。

依預設，Symantec Endpoint Protection 會嘗試清除感染病毒的檔案。如果 Symantec Endpoint Protection 無法清除檔案，則會執行下列動作：

-
- 將檔案移至受感染電腦上的隔離所，並拒絕對該檔案的任何存取。
 - 記錄事件。

依預設，Symantec Endpoint Protection 會將任何受到安全性風險感染的檔案移至隔離所。

如果您將動作設定為只記錄，則依預設當使用者建立或儲存受感染的檔案時，Symantec Endpoint Protection 會刪除這些檔案。

在 Windows 電腦上，您也可以為檔案系統的管理員掃描、隨選掃描和自動防護掃描架構矯正動作。

您可以鎖定動作，讓使用者無法在使用此政策的用戶端電腦上變更動作。

WARNING

對於安全風險，請小心使用刪除動作。在某些情形下，刪除安全風險會導致應用程式無法運作。如果您架構用戶端刪除受到安全風險影響的檔案，將無法還原檔案。

若要備份受到安全風險影響的檔案，請改用隔離動作。

變更當 Symantec Endpoint Protection 在 Windows 用戶端上進行偵測時採取的動作

1. 在「病毒和間諜軟體防護政策」中的「**Windows** 設定」下，選取掃描 (任何自動防護掃描、管理員掃描或隨選掃描)。
2. 在「動作」標籤的「偵測」下方，選取惡意軟體或安全風險類型。

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。

NOTE

在 Windows 用戶端上，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。

3. 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，可能名為「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。
4. 在「動作目的」下方，選取用戶端軟體在偵測到該病毒或安全風險類別時，所要採取的第一個與第二個動作。

對於安全風險，請小心使用刪除動作。在某些情形下，刪除安全風險會導致應用程式無法運作。
 5. 針對每個您想設定動作的 (病毒與安全風險) 類別重複上述步驟。
 6. 架構完此政策後，按下「確定」。

變更當 Symantec Endpoint Protection 在 Linux 用戶端上進行偵測時採取的動作

1. 在「病毒和間諜軟體防護政策」的「**Linux** 設定」下，選取「全域掃描選項」。
2. 使用核取方塊「記載偵測，但不對威脅採取任何行動。」
3. 架構完此政策後，按下「確定」。

變更當 Symantec Endpoint Protection 在 Mac 用戶端上進行偵測時採取的動作

1. 在「病毒和間諜軟體防護」政策中的「**Mac** 設定」下方，選取「管理員定義掃描」。
2. 執行下列其中一項動作：
 - 對於排程掃描，請選取「一般設定」標籤。
 - 對於隨選掃描，請在「掃描」標籤上的「管理員隨選掃描」下方，按下「編輯」。
3. 在「動作」下方，選取以下任何一個選項：
 - 自動修復受感染的檔案
 - 無法修復的隔離所檔案

4. 對於隨選掃描，請按下「確定」。
5. 架構完此政策後，按下「確定」。

更多資訊

- [檢查掃描動作及重新掃描識別出的電腦](#)
- [移除病毒和安全風險](#)

允許使用者在 Windows 電腦上暫停或停止掃描

您可以架構是否在 Windows 用戶端電腦上顯示掃描進度對話方塊。如果您允許此對話方塊顯示在用戶端電腦上，使用者就能暫停或延後管理員定義掃描。

掃描進度對話方塊會顯示目前執行中掃描的進度。

此外：

- 掃描執行時，將顯示「掃描進行中」訊息連結。
使用者可以按下此連結來顯示掃描進度。
- 另外也會顯示重新排程下一個排程掃描的連結。

您可以允許使用者執行下列掃描動作：

暫停	使用者暫停掃描時，「掃描結果」對話方塊仍保持開啟，等候使用者繼續或放棄掃描。如果電腦關機，暫停的掃描就無法繼續執行。
延緩	使用者延緩排程掃描時，可以選擇將掃描延緩一小時或三小時。您可以架構延緩的次數。使用者延緩掃描後，「掃描結果」對話方塊就會關閉；它會在延緩期間結束後再次出現，並繼續掃描。
停止	使用者停止掃描時，掃描通常會立即停止。如果使用者停止掃描的同時，用戶端軟體正在掃描壓縮檔，則掃描不會馬上停止。在這種情況下，在壓縮檔一掃描完畢後就會停止掃描。停止的掃描則不會重新啟動。

暫停的掃描在經過一段指定的時間間隔後會自動重新啟動。

NOTE

使用者可以停止 Power Eraser 分析，但無法暫停或延緩該分析。

若需程序中使用選項的詳細資訊，您可以按下「敘述」。

允許使用者在 Windows 電腦上暫停或停止

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「Windows 設定」下方，按一下「管理員定義掃描」。
3. 在「進階」標籤的「掃描進度選項」下，按下「顯示掃描進度」或「顯示偵測到風險時的掃描進度」。
4. 若要在掃描完成後自動關閉掃描進度指標，請勾選「完成時關閉掃描進度視窗」。
5. 勾選「允許使用者停止掃描」。
6. 按下「暫停選項」。
7. 在「掃描暫停選項」對話方塊中，執行下列任一動作：
 - 若要限制使用者可以暫停掃描的時間，請勾選「限制掃描暫停的時間」，然後輸入分鐘數。範圍是 3 至 180。
 - 若要限制使用者可以延後 (或延緩) 掃描的次數，請在「延緩的次數上限」方塊中，輸入 1 至 8 之間的數字。
 - 根據預設，使用者可將掃描動作延後一個小時。若要變更此限制為 3 小時，請勾選「允許使用者延緩掃描 3 小時」。
8. 按下「確定」。

更多資訊

架構 Windows 資訊安全中心通知以搭配 Symantec Endpoint Protection 用戶端使用

您可以在用戶端電腦上設定 Windows 安全中心設定。

架構 Windows 資訊安全中心以搭配 Symantec Endpoint Protection 用戶端使用

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「Windows 設定」下方，按一下「其他」。
3. 在「其他」標籤上，指定 Windows 資訊安全中心的選項。

如需詳細瞭解這些設定，請參閱：[其他](#)

4. 按一下「確定」。

提交 Symantec Endpoint Protection 遙測資料以提高安全性

如需詳細資訊，請參考下列各主題：

- [簡介](#)
- [用途](#)
- [啟用遙測收集](#)
- [遙測常見問答集](#)
- [效能、大小和部署](#)

簡介

遙測亦稱為傳送或資料收集，會收集資訊以改善網路的安全狀況及產品體驗。遙測會廣泛收集下列類型的資訊：

- 系統環境，包括硬體和軟體詳細資料
- 產品錯誤與相關事件
- 產品組態的有效性

收集的資料會傳送至賽門鐵克。

NOTE

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。

用途

賽門鐵克會使用這些資訊分析並改善客戶的產品體驗。

- Broadcom 支援使用遙測。
- 賽門鐵克會使用遙測洞察威脅環境，並將其用作 Risk Insight 程式的一部分。

啟用遙測收集

賽門鐵克同時從管理伺服器 and Symantec Endpoint Protection 用戶端收集遙測資料。

然而，為因應網路頻寬問題或用戶端傳出資料的相關限制，您可能需要停用遙測傳送。您可以檢查用戶端活動日誌，來檢視傳送活動及監控頻寬使用量。

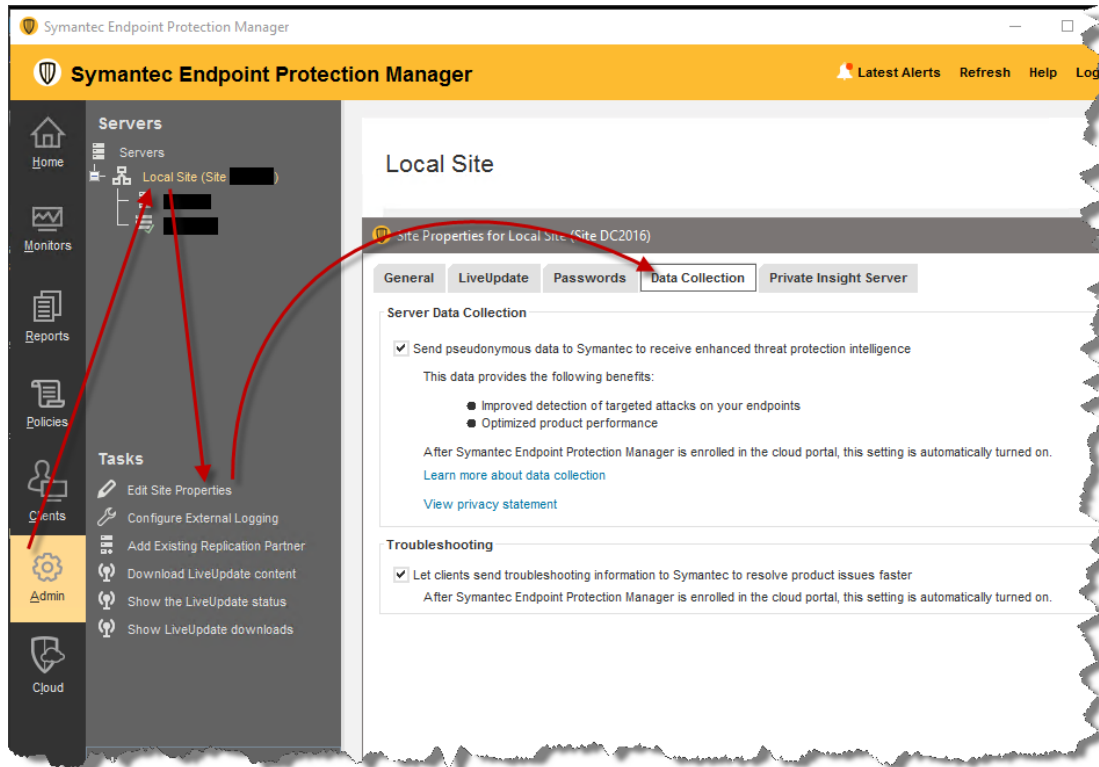
啟用或停用管理伺服器遙測收集

針對伺服器資料收集啟用或停用「將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報」選項。

1. 在管理主控台中，前往「管理」>「伺服器」>「本機網站」>「網站屬性」>「資料收集」並變更選項。

NOTE

在 Symantec Endpoint Protection Manager 安裝期間，您也可以停用伺服器資料收集選項，但不建議這麼做。



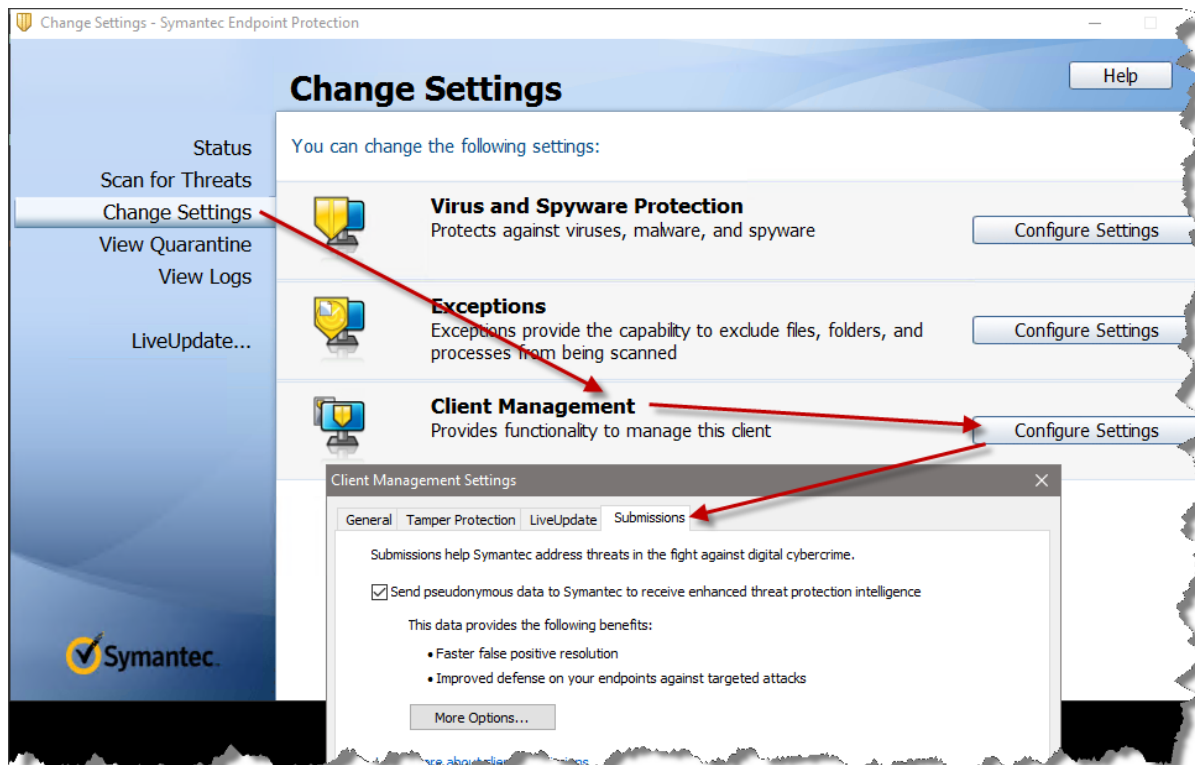
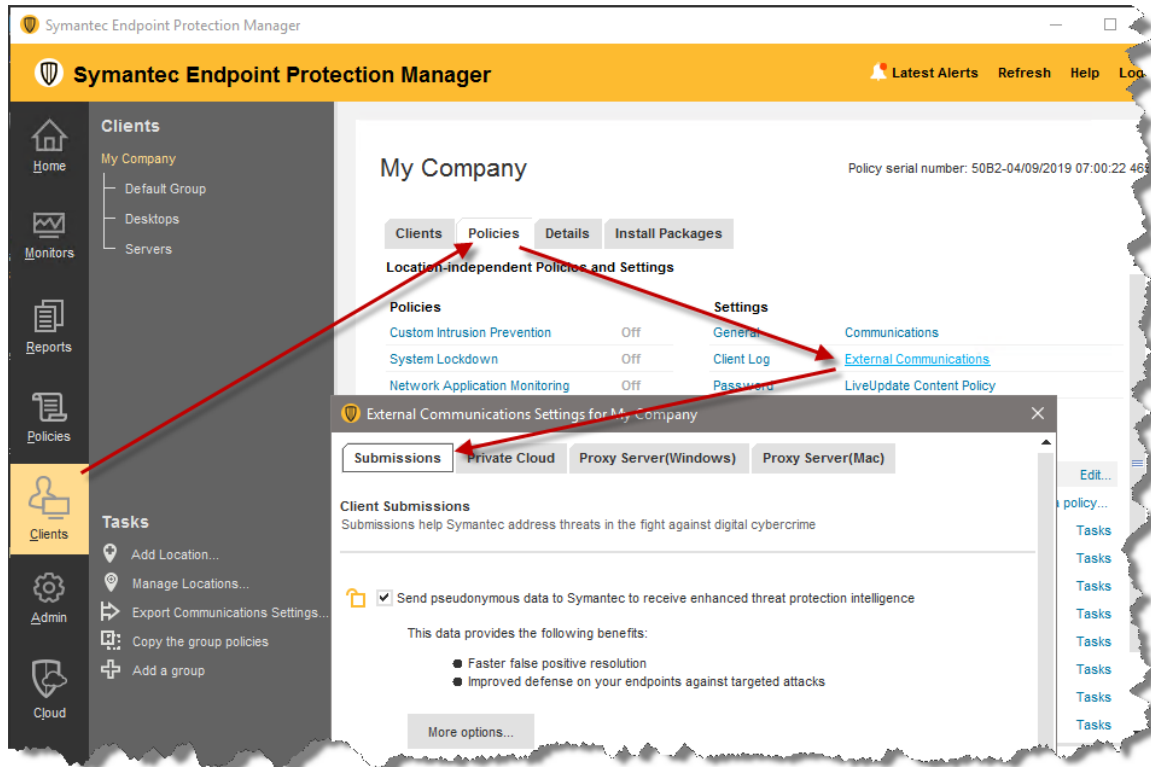
啟用或停用用戶端遙測傳送

針對用戶端提交啟用或停用「將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報」選項。您可以在管理主控台中的群組層級變更選項，或針對用戶端使用者介面中的單一用戶端變更選項。

企業中的每個用戶端都屬於某個群組。每個群組有其自己的政策。在某些情況下，群組會架構為繼承其父群組的政策。由於用戶端傳送為群組範圍的設定，因此請確保根據需要將設定套用到所有群組。

賽門鐵克建議您傳送威脅資訊，以協助賽門鐵克提供最佳威脅防護。

1. 在管理主控台中，前往「用戶端」>「政策」標籤。在「設定」窗格中，選取「外部通訊設定」>「傳送」。
在用戶端使用者介面中，前往「變更設定」>「用戶端管理」>「架構設定」>「傳送」。



2. 如果停用傳送並鎖定設定，使用者將無法架構群組中的用戶端傳送資訊。如果啟用該選項，請選取傳送類型並鎖定設定，使用者將無法停用傳送。如果不鎖定設定，則使用者可以變更組態，包括「更多選項」中的傳送類型。

Symantec Endpoint Protection 會收集何種類型的資訊？

如需詳細資訊，請參閱：

[隱私權和資料防護](#)

下表說明了 Symantec Endpoint Protection 收集的資訊類型。

Table 96: 有關 Symantec Endpoint Protection 收集之資訊類型的更多詳細資料

類型	更多詳細資料
軟體組態、產品詳細資料和安裝狀態	包括有關病毒和間諜軟體防護政策的資訊： • Bloodhound 設定 Bloodhound 為啟用還是停用，以及層級為自動還是主動。(「病毒和間諜軟體防護」政策 > 「全域掃描選項」) • 下載鑑識設定 下載鑑識為啟用還是停用，以及何謂下載鑑識設定，包括靈敏度等級和感染狀況臨界值。(「病毒和間諜軟體防護」政策 > 「下載防護」) • 自動防護設定 為惡意軟體或安全風險架構何種覆寫。(「病毒和間諜軟體防護」政策 > 「自動防護」) 包括具有最大用戶端數目的前 20 個群組的相關資訊。對於每個群組，會選取第一個位置 (通常為預設位置) 來傳送資訊。 通常，資訊包括： • 用戶端模式：用戶端是使用伺服器控制、用戶端控制、混合模式，還是找不到任何資料 • 推送/提取模式：用戶端是從伺服器取得還是要求政策 • 應用程式探索開啟或關閉 • 活動訊號間隔 (以分鐘為單位) • 重大事件上傳開啟或關閉 • 下載隨機化開啟或關閉；隨機化時段 (以分鐘為單位) • 用戶端是使用上次使用的群組設定還是上次使用的群組模式 • 用戶端是否傳送偵測傳送以及偵測類型為何，例如防毒偵測或檔案信譽。 • 是否已在用戶端上啟用主機完整性 • 網域數目。 • 所有網域中的群組總數，會以近似值的形式顯示，例如 <1500。超過 3,000 會以 >1=3000 的形式傳送 • 所有網域之間群組的最大深度 • 用戶端總數的計數 • 電腦模式下的用戶端數目 • 使用者模式下的用戶端數目 • 組織單位 (OU) 群組中的用戶端數目
授權狀態、授權權利資訊、授權 ID 與授權使用量	不適用
裝置名稱、類型、作業系統版本、語言、位置、瀏覽器類型與版本、IP 位址和 ID	不適用
裝置硬體、軟體和應用程式清查	伺服器資料庫會傳送有關用戶端硬體的彙整資訊。資訊包括 Symantec Endpoint Protection 安裝磁碟上的 CPU、RAM 和可用磁碟空間。

類型	更多詳細資料
應用程式與資料庫存取組態、政策需求和政策遵循狀態，以及應用程式例外和工作流程失敗日誌	包括系統管理日誌項目的規則數目。還會傳送下列資料庫日誌的日誌項目數目以及距離日誌項目到期所剩餘的天數： - 系統管理日誌 - 用戶端伺服器活動日誌 - 稽核日誌 - 系統伺服器活動日誌 包括任何伺服器遠端複製失敗事件，例如遠端複製失敗或資料庫版本不相符。
與可能的威脅相關聯的資訊包括：用戶端安全事件資訊、IP 位址、使用者 ID、路徑、裝置資訊 (例如裝置名稱和狀態)、下載的檔案、檔案動作	不適用
檔案與應用程式信譽包括檔案下載、動作與執行應用程式資訊及惡意軟體傳送	檔案信譽資料是依據檔案信譽偵測到的檔案相關資訊。 這些傳送將匯入 Symantec Insight 信譽資料庫，並協助保護您的電腦防範新興風險。 資訊包括檔案雜湊、用戶端 IP 雜湊、用於下載檔案的 IP 位址、檔案大小和檔案的信譽分數。
應用程式例外和工作流程失敗日誌	不適用
架構服務或任何其他後續服務呼叫期間所提供的個人資訊	不適用
授權資訊，例如名稱、版本、語言和授權權利資料	不適用
SEP 中包含的防護技術使用狀況	包括具有最大用戶端數目的前 20 個群組的相關資訊。對於每個群組，會選取第一個位置 (通常為預設位置) 來傳送資訊。 資訊包括： - 已啟用或停用特定防護技術的用戶端數目。 - 由已啟用防護技術進行的第一個和第二個偵測動作的數量和類型 (如隔離、僅記錄、清除等)。 Symantec Endpoint Protection Manager 會傳送其資料庫中每種類型的共用政策的數目，該數目等於預設政策數目與自訂政策數目之和。資訊包括： - 網域數目 - 下列每個共用政策的數目： - 病毒和間諜軟體防護政策 - 防火牆政策 - 入侵預防政策 - 應用程式與裝置控制政策 - LiveUpdate 政策 - 主機完整性政策 - 自訂入侵預防特徵的數目

類型	更多詳細資料
說明 SEP 組態的資訊，例如作業系統資訊、伺服器硬體和軟體組態細節、CPU 名稱、記憶體大小、軟體版本及已安裝套件的功能	包括伺服器資訊，例如： • 複寫夥伴數目 • 是否已複寫日誌資料 • 是否已複寫內容資料 包括 Linux 作業系統類型與核心版本，以及使用此組態的用戶端數目的計數。 包括 Symantec Endpoint Protection Manager 資料庫中有關 Symantec Endpoint Protection 用戶端運作狀態的彙整資訊，包含下列計數： • 用戶端總數 • 縮減大小用戶端 • 標準大小用戶端 • 啟用 EWF 的用戶端 • 啟用 FBWF 的用戶端 • 啟用 UWF 的用戶端 • Microsoft Hypervisor 用戶端 • VMware Hypervisor 用戶端 • Citrix Hypervisor 用戶端 • 不明 Hypervisor 用戶端 傳送 LiveUpdate 修訂版的大概數目，例如 <30。
潛在安全風險、被識別為惡意軟體 (可能包含個人資訊) 的可攜式可執行檔和包含可執行內容的檔案的相關資訊，包括此類檔案在安裝時所執行之動作的相關資訊	包括下列資訊： • 防毒偵測 (僅限 Windows 和 Mac) 有關病毒和間諜軟體掃描偵測的資訊。用戶端傳送的資訊類型包括檔案雜湊、用戶端 IP 雜湊、防毒特徵、攻擊者 URL 等。 • 防毒進階啟發式偵測 (僅限 Windows) 由 Bloodhound 及其他病毒和間諜軟體掃描啟發式技術偵測到的潛在威脅的相關資訊。這些偵測為無訊息偵測，不會顯示在風險日誌中。有關這些偵測的資訊用於進行統計分析。 • 行為分析 (SONAR) 偵測 (僅限 Windows) 行為分析偵測到的威脅的相關資訊，此包括系統變更事件和受信任應用程式出現的可疑行為。 還包括程序資料，例如： • 行為分析啟發式偵測 (僅限 Windows) 為無訊息偵測，不會顯示在「風險日誌」中。此資訊用於進行統計分析。用戶端傳送的資訊類型通常包括如下所示的偵測屬性： — 隱藏的程序 — 小型印記程序 — 按鍵輸入記錄或螢幕擷取行為 — 停用安全性產品行為 — 偵測日期和時間戳記
網路活動的相關資訊，包括存取的 URL 和網路連線的相關彙整資訊 (例如，有關網路連線的主機名稱、IP 位址和統計資訊)	包括下列資訊： • 網路偵測事件 (僅限 Windows 和 Mac) 由 IPS 引擎 (入侵預防) 執行之偵測的相關資訊。用戶端傳送的資訊包括用戶端 IP 雜湊、攻擊者 URL、偵測時間戳記、攻擊者 IP 位址、IPS 特徵等。 • 瀏覽器偵測事件 (僅限 Windows) 所有在瀏覽器網址列中輸入、按下或連線以進行下載的 URL。 用戶端也會傳送有關下列內容的中繼資料： — 每個網路連線，包括 IP 位址、通訊埠號、主機名稱、應用程式起始連線、通訊協定、連線時間、每個連線的位元組數目。 — 裝置之間的所有檔案傳輸活動，包括裝置識別、傳輸時間、通訊協定、檔案屬性 (類型、名稱、路徑、大小) 及內容的 SHA-256。

類型	更多詳細資料
SEP 安裝和運作的相關狀態資訊，只有在 SEP 於安裝或發生錯誤時所使用的檔案或資料夾名稱包含個人資訊時，狀態資訊才可能包含此類資訊，此資訊使賽門鐵克得以確認是否成功安裝 SEP，以及 SEP 是否發生錯誤	不適用
匿名的一般、統計與狀態資訊	不適用

我如何知道 **Symantec Endpoint Protection** 用戶端正在進行遙測傳送？

檢查用戶端活動日誌來檢視傳送事件。如果該日誌不包含目前的傳送事件，請檢查下列項目：

- 確保用戶端傳送已啟用。
- 如果您使用代理伺服器，請檢查代理例外。請參閱：
[我可否為用戶端傳送指定代理伺服器？](#)
- 檢查賽門鐵克伺服器的連線。
- 檢查以確保用戶端具有目前的 LiveUpdate 內容。
Symantec Endpoint Protection 會使用傳送控制資料 (SCD) 檔案。賽門鐵克會發布 SCD 檔案，並將其包含在 LiveUpdate 套件中。每項賽門鐵克產品都有各自的 SCD 檔案。SCD 檔案會控制下列設定：
 - 一天之中用戶端可傳送的次數
 - 用戶端軟體重試傳送時等候的時間長度
 - 傳送失敗後重試的次數
 - 賽門鐵克安全機制應變中心接收傳送內容的 IP 位址

如果 SCD 檔案過時，則用戶端會停止傳送。如果用戶端電腦已有 7 天未擷取 LiveUpdate 內容，則賽門鐵克會認為該 SCD 檔案過時。用戶端會在 14 天後停止傳送。

如果用戶端停止傳送，則用戶端軟體不會收集傳送資訊，也不會在稍後傳送它。用戶端再次開始傳送時，只會傳送在傳送重新開始之後發生的事件資訊。

我可否退出遙測傳送？

您可以退出。您可以在用戶端和伺服器使用者介面中修改伺服器資料收集或用戶端傳送選項。但是，賽門鐵克建議您啟用盡可能多的遙測，以改善網路安全性。

效能、大小和部署

遙測會耗用多少頻寬？

Symantec Endpoint Protection 會調節用戶端電腦傳送，將對您網路的影響降至最低。Symantec Endpoint Protection 會以下列方式調節傳送：

- 用戶端電腦只會在電腦閒置時傳送範例。閒置傳送有助於在整個網路中隨機設定傳送流量。
- 用戶端電腦只會傳送唯一檔案的範例。如果賽門鐵克已經看見此檔案，用戶端電腦就不會傳送資訊。

NOTE

這些傳送的資料大小是非常微不足道的。例如，防毒傳送一般不會超過 4 KB，且類似的 IPS 傳送大小約為 32 KB。

我可否為用戶端傳送指定代理伺服器？

您可以架構 Symantec Endpoint Protection Manager 使用代理伺服器傳送資訊，以及進行 Windows 用戶端使用的其他外部通訊。如果用戶端電腦使用需驗證的 Proxy，您可能需要在 Proxy 伺服器組態中為 Symantec URL 指定例外。這些例外可讓您的用戶端電腦與「賽門鐵克智慧型掃描」和其他重要的賽門鐵克網站進行通訊。

如需有關代理的更多詳細資料，請參閱：

指定用於用戶端傳送資訊和其他外部通訊的代理伺服器

如需瞭解更多有關 Symantec URL 例外的資訊，請參閱：

[允許 SEP 和 SES 連接到賽門鐵克伺服器的 URL](#)

瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性

依據預設，Symantec Endpoint Protection 用戶端和 Symantec Endpoint Protection Manager 會向賽門鐵克提交某些類型的匿名資訊。用戶端也可以向賽門鐵克傳送非匿名資料以進行自訂分析。您可以控制自己的用戶端或 Symantec Endpoint Protection Manager 是否傳送資訊。

伺服器資料和用戶端傳送資訊對於改善網路安全都極為重要。

如需詳細資訊，請參考下列各主題：

- [何謂伺服器資料收集？](#)
- [何謂匿名用戶端提交？](#)
- [何謂非匿名用戶端提交？](#)
- [隱私權考量](#)
- [頻寬使用量考量](#)

何謂伺服器資料收集？

伺服器資料是可協助賽門鐵克衡量和改善偵測技術效能之資訊的一部分。

Symantec Endpoint Protection Manager 會向賽門鐵克提交下列類型的匿名資訊：

- 授權資訊，其中包括名稱、版本、語言及授權權利資料
- Symantec Endpoint Protection 防護功能的使用情況
- Symantec Endpoint Protection 組態的相關資訊。資訊包括作業系統資訊、伺服器硬體和軟體組態、CPU 大小、記憶體大小，以及已安裝套件的軟體版本和功能

您可以在安裝期間變更伺服器傳送資訊設定，也可以在主控台中變更伺服器「網站屬性 > 資料收集」標籤上的設定。

NOTE

賽門鐵克始終建議您保持伺服器資料收集為啟用狀態。

何謂匿名用戶端提交？

Symantec Endpoint Protection 用戶端會自動向賽門鐵克安全機制應變中心提交有關偵測、網路及組態的匿名資訊。賽門鐵克使用這些匿名資訊來應付新的威脅與不斷變化的威脅，以及改善產品效能。匿名資料不會直接用於識別特定使用者。

用戶端傳送的偵測資訊包括防毒偵測、入侵預防、行為分析 (SONAR) 及檔案信譽偵測相關資訊。

NOTE

Mac 用戶端傳送資訊不包括行為分析或檔案信譽傳送資訊。Linux 用戶端不支援任何用戶端傳送。

用戶端傳送給賽門鐵克的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。例如，您的公司政策可能不允許用戶端電腦向外部實體傳送任何網路資訊。您可以停用單一類型的傳送 (例如網路資訊的傳送)，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。

如需詳細資訊，請參閱：

- [管理用戶端傳送給賽門鐵克的匿名或非匿名資料](#)
- [Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策](#)

何謂非匿名用戶端提交？

您可以選擇向賽門鐵克提交非匿名用戶端資訊。這種類型的資訊有利於進一步瞭解安全性挑戰，可協助賽門鐵克提供建議的自訂解決方案。

- 您應該只有在參與賽門鐵克贊助的計畫 (可提供自訂分析) 時，才使用此選項。
- 此選項預設為停用。

如需詳細資訊，請參閱：

[管理用戶端傳送給賽門鐵克的匿名或非匿名資料](#)

隱私權考量

賽門鐵克會竭盡所能匿名化用戶端提交資料。

- 僅會傳送可疑的可執行檔。
- 將使用者名稱從路徑名稱中移除。
- 電腦和企業均由唯一的匿名化值識別。
- IP 位址在用於識別地理位置後即會捨棄。

如需隱私權的詳細資訊，請參閱下列文件：

[隱私權聲明](#)

頻寬使用量考量

Symantec Endpoint Protection 會最大限度降低用戶端傳送資訊對網路頻寬的影響。

您可以檢查用戶端活動日誌，來檢視用戶端電腦所傳送的資訊類型，以及監控頻寬使用量。請參閱：

- [Symantec Endpoint Protection 如何最大限度降低用戶端傳送資訊對網路頻寬的影響](#)
- [檢視日誌](#)

管理用戶端傳送給賽門鐵克的匿名或非匿名資料

Symantec Endpoint Protection 可以透過將偵測相關資訊提交給賽門鐵克，為電腦提供保護。賽門鐵克會使用該資訊來應付新的與不斷變化的威脅。您傳送的任何資料都有助於賽門鐵克提高回應威脅以及為電腦自訂防護的能力。賽門鐵克建議您選擇傳送盡可能多的偵測資訊。請參閱：

[瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性](#)

用戶端電腦會匿名提交偵測相關資訊。您可以指定用戶端應傳送哪些類型的偵測資訊。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。

NOTE

Mac 用戶端傳送資訊不包括行為分析 (SONAR) 或檔案信譽傳送資訊。Linux 用戶端不支援任何用戶端傳送。

變更用戶端傳送資訊設定

1. 在主控台中，選取「用戶端」，然後按下「政策」標籤。
2. 在「設定」窗格中，按下「外部通訊設定」。
3. 選取「用戶端傳送資訊」標籤。
4. 啟用或停用「將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報」選項。
5. 如果想要啟用或停用特定傳送類型 (例如檔案信譽)，請選取「更多選項」。
6. 如果您參與了賽門鐵克贊助的自訂分析計畫，請選取「將可識別用戶端的資料傳送給賽門鐵克進行自訂分析」。

WARNING

此選項會將非匿名資訊傳送給賽門鐵克。只有在您參與賽門鐵克贊助的計畫並且想要與賽門鐵克共用可識別用戶端的資料時，才使用此選項。

7. 選取「確定」。

NOTE

在 Mac 用戶端上，您也可以停用 IPS 連線偵測傳送。請參閱下列文章：

[如何在 Symantec Endpoint Protection for Mac 用戶端上停用 IPS 資料傳送](#)

Symantec Endpoint Protection 如何最大限度降低用戶端傳送資訊對網路頻寬的影響

Symantec Endpoint Protection 會調節用戶端電腦傳送，將對您網路的影響降至最低。Symantec Endpoint Protection 會以下列方式調節傳送：

- 用戶端電腦只會在電腦閒置時傳送範例。閒置傳送有助於在整個網路中隨機設定傳送流量。
- 用戶端電腦只會傳送唯一檔案的範例。如果賽門鐵克已經看見此檔案，用戶端電腦就不會傳送資訊。
- Symantec Endpoint Protection 會使用傳送控制資料 (SCD) 檔案。賽門鐵克會發布 SCD 檔案，並將其包含在 LiveUpdate 套件中。每項賽門鐵克產品都有各自的 SCD 檔案。

SCD 檔案會控制下列設定：

- 一天之中用戶端可傳送的次數
- 用戶端軟體重試傳送時等候的時間長度
- 傳送失敗後重試的次數
- 「賽門鐵克安全機制應變中心」擷取傳送內容的 IP 位址

如果 SCD 檔案過時，則用戶端會停止傳送。如果用戶端電腦已有 7 天未擷取 LiveUpdate，則賽門鐵克會認為該 SCD 檔案過時。用戶端會在 14 天後停止傳送。

如果用戶端停止傳送，則用戶端軟體不會收集傳送資訊，也不會在稍後傳送它。用戶端再次開始傳送時，只會傳送在傳送重新開始之後發生的事件資訊。

更多資訊

[瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性](#)

指定用於用戶端傳送資訊和其他外部通訊的 Proxy 伺服器

您可以架構 Symantec Endpoint Protection Manager 使用 Proxy 伺服器傳送資訊，以及進行 Windows 用戶端使用的其他外部通訊。

NOTE

如果用戶端電腦使用需驗證的 Proxy，您可能需要在 Proxy 伺服器組態中為 Symantec URL 指定例外。這些例外可讓您的用戶端電腦與「賽門鐵克智慧型掃描」和其他重要的賽門鐵克網站進行通訊。

如果您使用下列代理組態選項，則需要在代理伺服器設定中包含 Symantec URL 的例外：

- 您使用需驗證的代理伺服器。
- 您要在「外部通訊Symantec Endpoint Protection Manager」對話方塊中選取「使用用戶端瀏覽器指定的代理伺服器」選項。
- 您要在瀏覽器的「網際網路選項」中使用自動偵測或自動設定。

如果您不使用自動偵測或自動設定，就不需要在代理伺服器設定中為 Symantec URL 指定例外。您應該在「外部通訊」對話方塊中選取「使用自訂代理設定」，然後指定驗證設定。

指定用於用戶端傳送資訊和其他外部通訊的代理伺服器

1. 在主控台的「用戶端」頁面上，選取群組並按下「政策」。
2. 在「設定」或「位置限定的設定」下方，按下「外部通訊」。
3. 在「代理伺服器 (Windows)」標籤的「HTTPS 代理架構」下方，選取「使用自訂代理設定」。
4. 輸入用戶端使用之代理伺服器的相關資訊。如需這些選項的詳細資訊，請參閱線上說明。
5. 按下「確定」。

如需建議例外的相關資訊，請參閱下列文章：

- [如何測試智慧型掃描與賽門鐵克授權伺服器的連線能力](#)
- [允許 Symantec Endpoint Protection 連線至賽門鐵克信譽和授權伺服器所需的代理伺服器排除項](#)

更多資訊

- [瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性](#)
- [建立病毒和間諜軟體掃描的例外](#)

管理行為分析 (SONAR)

行為分析是用戶端電腦上主動型威脅防護的一部分，也是 Symantec Endpoint Protection Manager 中病毒和間諜軟體防護政策的一部分。

Table 97: 管理行為分析

工作	說明
瞭解 SONAR 運作方式	瞭解行為分析偵測未知威脅的方式。此資訊可協助您決定如何在安全網路中使用行為分析。請參閱： 何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？
檢查 SONAR 是否已啟用	行為分析可與某些其他 Symantec Endpoint Protection 功能交互運作。行為分析需要自動防護。您可以使用「用戶端」標籤檢查用戶端電腦上是否已啟用「主動型威脅防護」。請參閱： 調整用戶端電腦上的 SONAR 設定
檢查行為分析的預設設定	行為分析設定是病毒和間諜軟體防護政策的一部分。請參閱： 關於預設的病毒和間諜軟體防護政策掃描設定
確定已啟用智慧型掃描查詢	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，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 SONAR 提供的防護會受到限制。請在「提交」對話方塊中啟用或停用「智慧型掃描查詢」。請參閱： 瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性
監控行為分析事件以檢查是否有偵測誤報	您可使用行為分析日誌監控事件。 您還可以檢視「SONAR 偵測結果」報告 (在「風險報告」下) 以檢視偵測相關資訊。請參閱： • 監控 SONAR 偵測結果來查看是否有誤報 • 監控 Symantec Endpoint Protection 用戶端

工作	說明
調整行為分析設定	您可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。 您還可能希望針對高風險或低風險啟發式偵測啟用或停用通知。請參閱： 調整用戶端電腦上的 SONAR 設定 處理和避免 SONAR 偵測誤報
防止行為分析偵測已知安全的應用程式	SONAR 可能會偵測您希望在用戶端電腦上執行的檔案或應用程式。可以使用「例外」政策為要允許的特定檔案、資料夾或應用程式指定例外。對於 SONAR 隔離的項目，您可以為 SONAR 日誌中隔離的項目建立例外。 您還可能希望設定 SONAR 動作以記錄和允許偵測。您可以使用應用程式探索，以便 Symantec Endpoint Protection 了解用戶端電腦上的合法應用程式。在 14.3 RU4 和更早版本中，在 Symantec Endpoint Protection 瞭解您於網路中使用的應用程式後，您可將 SONAR 動作變更為「隔離」。 Note: 如果您將高風險偵測對應的動作設定為「只記錄」，則可能會為您的用戶端電腦帶來潛在威脅。 如需詳細資訊，請參閱： 處理和避免 SONAR 偵測誤報
阻止行為分析檢查某些應用程式	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。可以針對應用程式建立檔案、資料夾或應用程式例外。請參閱： 建立病毒和間諜軟體掃描的例外
管理行為分析偵測變更 DNS 或主機檔案的應用程式的方式	您可全域調整 SONAR 處理 DNS 或主機檔案變更偵測的方式。可以使用「例外」政策來架構特定應用程式的例外。請參閱： 調整用戶端電腦上的 SONAR 設定 針對會變更 DNS 或主機檔案的應用程式建立例外
允許用戶端將有關行為分析偵測的資訊傳送給賽門鐵克	賽門鐵克建議您在用戶端電腦上啟用傳送。用戶端送出的偵測相關資訊有助於賽門鐵克解決威脅。此資訊有助於賽門鐵克建立更好的啟發式技術，進而產生較低的偵測誤報率。請參閱： 瞭解伺服器資料收集 and 用戶端提交及其對網路安全的重要性

何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？

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。

行為分析可為您的用戶端電腦提供額外的防護等級，並能與您現有的病毒和間諜軟體防護、入侵預防、記憶體攻擊緩和以及防火牆防護相輔相成。

行為分析使用啟發式系統，該系統會運用賽門鐵克的線上智慧型網路，並且對用戶端電腦進行主動型本機監視，以偵測新出現的威脅。行為分析也會偵測您應監視之用戶端電腦上的變更或行為。

NOTE

「自動防護」也會使用稱為 Bloodhound 的啟發式掃描來偵測檔案中是否有可疑行為。

行為分析會將一些程式碼插入以 Windows 使用者模式執行的應用程式中，以監控這些應用程式是否有可疑的活動。在某些情況下，插入程式碼可能會影響應用程式效能，或導致執行應用程式時出現問題。您可以建立例外，將檔案、資料夾或應用程式排除在這類監控的範圍之外。

行為分析不會偵測應用程式類型，但會偵測程序的行為模式。行為分析只會在應用程式有惡意行為時才會採取動作，不論應用程式類型為何。例如，如果某個特洛伊木馬程式或按鍵記錄器沒有惡意行為，則行為分析不會加以偵測。

SONAR 會偵測以下項目：

啟發式威脅	行為分析會使用啟發式技術判斷不明檔案是否有可疑行為，以及可能會產生較高風險或較低風險。它也會使用信譽資料，判斷威脅會產生較高風險或較低風險。
系統變更	行為分析會偵測嘗試修改用戶端電腦上之 DNS 設定或主機檔案的應用程式或檔案。
呈現不良行為的受信任應用程式	某些沒有問題的受信任檔案可能會伴隨可疑行為。行為分析會將這些檔案偵測為可疑行為事件。例如，常見的文件共用應用程式可能會建立可執行檔。

如果您停用自動防護，會限制行為分析偵測高風險和低風險檔案的能力。如果您停用智慧型掃描查詢 (信譽查詢)，則也會限制行為分析的偵測功能。

更多資訊

- [管理 SONAR](#)
- [管理 Symantec Endpoint Protection 中的例外](#)

處理和避免行為分析 (SONAR) 偵測誤報

對於某些內部自訂應用程式，行為分析可能會做出偵測誤報。此外，如果您停用「智慧型掃描查詢」，則來自行為分析的誤報數目會增加。請參閱：

[瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性](#)

一般而言，您可以變更行為分析設定以減輕偵測誤報率。您也可以為行為分析偵測為誤報的特定檔案或特定應用程式建立例外。

WARNING

如果您將高風險偵測對應的動作設定為「只記錄」，則可能會為您的用戶端電腦帶來潛在威脅。

Table 98: 處理 SONAR 誤報

工作	說明
記錄 SONAR 高風險啟發式偵測與使用應用程式探索	您可能需要在一段短時間內將高風險啟發式偵測對應的偵測動作設為「記錄」。同時，請讓應用程式探索執行相同的一段時間。Symantec Endpoint Protection 會探索您在網路上執行的合法程序。然而，這麼做可能無法隔離某些真正的偵測結果。請參閱： 啟用應用程式探索 在該段時間之後，您應將偵測動作重新設為「隔離」。 Note: 如果您針對低風險啟發式偵測使用主動模式，會增加偵測誤報的可能性。依預設會停用主動模式。 如需詳細資訊，請參閱： 調整用戶端電腦上的 SONAR 設定
為 SONAR 建立例外以允許安全應用程式	您可以使用下列方式，為 SONAR 建立例外： • 使用 SONAR 日誌為已偵測到且隔離的應用程式建立例外 您可以從 SONAR 日誌為偵測誤報建立例外。如果項目已隔離，Symantec Endpoint Protection 會在隔離所中重新掃描該項目後還原項目。用戶端收到更新的定義檔之後，會重新掃描隔離所中的項目。請參閱： 從日誌事件建立例外 • 使用例外政策為特定檔案名稱、資料夾名稱或應用程式指定例外。 您可以從 SONAR 偵測中排除整個資料夾。您可能需要排除自訂應用程式所在的資料夾。請參閱： 建立病毒和間諜軟體掃描的例外

調整用戶端電腦上的 SONAR 設定

若要降低偵測誤報率，您可能需要變更 SONAR 動作。若要變更顯示在您用戶端電腦上的偵測通知數目，您可能也需要變更 SONAR 動作。

NOTE

當此網域在雲端主控台中註冊時，部分選項旁會顯示雲端圖示。當密集型防護政策生效時，該政策覆寫這些選項。

調整用戶端電腦上的 SONAR 設定

1. 在「病毒和間諜軟體防護」政策中，選取 **SONAR**。
2. 在 14.3 RU4 或更早版本，確認已勾選「啟用 **SONAR**」。
3. 在 14.3 RU4 或更早版本，在「掃描詳細資料」下，變更高或低風險啟發式威脅對應的動作。

您可以為低風險偵測啟用主動模式。此設定會增加 SONAR 對低風險偵測的靈敏度。它可能會增加偵測誤報率。

4. 您也可以選擇變更顯示在用戶端電腦上的通知相關設定。
5. 在「系統變更事件」下，變更「偵測到 **DNS** 變更」或「偵測到主機檔案變更」對應的動作。

NOTE

「提示」動作可能導致用戶端電腦上出現許多通知。「忽略」之外的任何動作都可能會導致主控台上有許多日誌事件，並傳送電子郵件通知給管理員。

WARNING

如果將動作設定為「攔截」，則可能會攔截用戶端電腦上重要的應用程式。

例如，如果將「偵測到 **DNS** 變更」對應的動作設定為「攔截」，可能會發生攔截 VPN 用戶端的情形。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。您可以使用 DNS 或主機檔案變更例外，允許特定應用程式進行 DNS 或主機檔案變更。

如需詳細資訊，請參閱：

[針對會變更 DNS 或主機檔案的應用程式建立例外](#)

6. 在「可疑行為偵測」下，您可以變更高或低風險偵測對應的動作。
7. 按下「確定」。

更多資訊

- [管理 SONAR](#)
- [建立病毒和間諜軟體掃描的例外](#)

監控行為分析 (SONAR) 偵測結果來查看是否有誤報

用戶端會收集行為分析偵測結果，並且上傳到管理伺服器。結果會儲存在「SONAR：行為分析」日誌中。

若要判斷哪些程序合法而哪些程序具有安全風險，請參閱日誌的以下各欄：

事件	事件類型與用戶端針對程序採取的動作，例如清除事件或記錄事件。請檢視下列事件類型： • 可能為合法性最低的程序會列為「發現潛在風險」事件。 • 可能為安全風險的程序會列為「發現安全風險」事件。
應用程式	程序名稱。
應用程式類型	行為分析掃描偵測到的惡意軟體類型。
檔案/路徑	程序啟動時所在路徑的名稱。

從「事件」欄可馬上看出偵測的程序是否為安全風險或合法性最低的程序。然而，發現的潛在風險不一定是合法程序，而發現的安全風險也不一定是惡意程序。因此，您需要檢視「應用程式類型」和「檔案/路徑」等欄，以瞭解相關資訊。例如，您可能認得第三方合法應用程式的應用程式名稱。

監控 **SONAR** 偵測結果來查看是否有誤報

1. 在主控台中，按下「監控器 > 日誌」。
2. 在「日誌」標籤的「日誌類型」下拉式清單中，按一下「SONAR：行為分析」。
3. 從「時間範圍」清單方塊中，選取一個最接近上次變更掃描設定時間的時間。
4. 按下「其他設定」。
5. 在「事件類型」下拉式清單中，選取下列其中一個日誌事件：
 - 若要檢視所有偵測的程序，確定已選取「全部」。
 - 若要檢視已評估為安全風險的程序，請按下「發現安全風險」。
 - 若要檢視已評估且已記錄為潛在風險的程序，請按下「發現潛在風險」。
6. 按下「檢視日誌」。
7. 在辨識合法應用程式和安全風險之後，請在例外政策中為其建立例外。

您可以直接從「SONAR：行為分析日誌」窗格建立例外。

更多資訊

[從日誌事件建立例外](#)

使用竄改防護保護 Symantec Endpoint Protection 程序和資源

竄改和/或停用安全性軟體是當今威脅環境中許多鎖定攻擊所採用的技術。竄改防護是一項關鍵技術，透過任何更改或停用嘗試來保護 Symantec Endpoint Protection 程序和資源。竄改防護會攔截對 Symantec Endpoint Protection 登錄設定和檔案的修改，並防止竄改 Windows 用戶端上的執行中程序。

如果您使用可偵測並防禦不當廣告軟體和間諜軟體的任何第三方安全風險掃描程式，這些掃描程式一般會影響賽門鐵克資源。如果您在執行這類掃描程式的同時，將「竄改防護」設定為記錄竄改事件，「竄改防護」會產生大量的日誌項目。如果您決定記錄「竄改防護」事件，請使用日誌過濾來管理事件的數量。

您可以架構用戶端，以攔截或記錄嘗試修改賽門鐵克資源的動作。您可以為「竄改防護」偵測的應用程式建立例外。

竄改防護設定會針對選取的群組進行架構。

啟用或停用竄改防護

1. 在主控台中，按一下「用戶端」。
2. 在「政策」標籤的「設定」下，按下「一般設定」。
3. 在「竄改防護」標籤上，勾選或取消勾選「防護賽門鐵克安全軟體不受竄改或關閉」。
4. 在「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」下的清單方塊中，選取下列其中一個記錄動作。
5. 按下「確定」。

更多資訊

[在 Windows 用戶端上建立竄改防護例外](#)

應用程式控制、系統鎖定和裝置控制

若要監控和控制用戶端電腦上的應用程式行為，可以使用應用程式控制和系統鎖定。應用程式控制會在已定義的應用程式嘗試存取用戶端電腦系統資源時，加以允許或攔截。系統鎖定則只會允許已核准的應用程式在用戶端電腦上執行。若要管理存取用戶端電腦的硬體裝置，可以使用裝置控制。

WARNING

應用程式控制和系統鎖定是進階安全功能，僅應由具經驗的管理員進行架構。

應用程式控制、系統鎖定和裝置控制可用來完成下列工作。

應用程式控制	- 防止惡意軟體佔據應用程式。 - 限制可執行的應用程式。 - 防止使用者變更組態檔。 - 保護特定的登錄機碼。 - 保護特定資料夾，例如 \WINDOWS\system。 可使用「應用程式控制」和「裝置控制」政策架構應用程式控制和裝置控制。請參閱： 設定應用程式控制
系統鎖定	- 控制用戶端電腦上的應用程式。 - 攔截嘗試執行或將自己載入現有應用程式的幾乎所有的特洛伊木馬程式、間諜軟體或惡意軟體。 系統鎖定能確保系統維持在已知且受信任的狀態。 Note: 如果未審慎實作系統鎖定，則可能會導致網路發生嚴重問題。賽門鐵克建議您在特定階段實作系統鎖定。 可在「用戶端」頁面上的「政策」標籤中架構系統鎖定。請參閱： 設定系統鎖定
裝置控制	- 攔截或允許不同類型的裝置附加到用戶端電腦，例如 USB、紅外線和 FireWire 裝置。 - 攔截或允許序列埠和平行埠。 如需詳細資訊，請參閱： 管理裝置控制

Mac 電腦支援裝置控制。

設定應用程式控制

應用程式控制會在已定義的應用程式嘗試存取用戶端電腦系統資源時，加以允許或攔截。您可以允許或攔截對特定登錄機碼、檔案和資料夾的存取。您也可以定義哪些應用程式可以執行、哪些應用程式不能透過異常程序終止，以及哪些應用程式可以呼叫 DLL。

使用下列步驟可在一組用戶端電腦上設定應用程式控制。

Table 99: 設定應用程式控制

步驟	說明
開啟政策並啟用預設應用程式控制規則集	「應用程式控制」政策包含預先定義的規則集，而這些規則集預設會停用。您可以啟用任何需要的規則集，然後將政策套用至群組。預先定義的規則集是在生產模式而非測試模式下進行架構。但是，您應該將設定變更為測試模式，然後在測試網路中測試這些規則，之後才將這些規則套用至生產網路。請參閱： 啟用和測試預設應用程式規則
新增其他應用程式控制規則 (選擇性)	如果預設規則集不符合您的需求，請新增規則集與規則。此工作通常只應由進階管理員執行。請參閱： 將自訂規則新增至應用程式控制

步驟	說明
針對應用程式新增例外	應用程式控制會在部分應用程式中插入程式碼來對其進行檢查，如此可能會讓電腦上執行的應用程式變慢。如有必要，您可以從應用程式控制中排除部分應用程式。可使用例外政策針對應用程式控制新增檔案例外或資料夾例外。請參閱： 從掃描中排除檔案或資料夾
檢視應用程式控制日誌	如果您要測試新的政策或是對問題進行疑難排解，則應該監控此日誌中的應用程式控制事件。在測試模式和生產模式中，應用程式控制事件均是記錄在 Symantec Endpoint Protection Manager 的應用程式控制日誌中。在用戶端電腦上，應用程式控制和裝置控制事件會顯示在「控制」日誌中。 一項應用程式控制動作可能會顯示有重複或多個日誌項目。例如，explorer.exe 在嘗試複製檔案時，會設定檔案存取遮罩的寫入位元和刪除位元。Symantec Endpoint Protection 會記錄該事件。如果複製動作因應用程式控制規則攔截這個動作而失敗，explorer.exe 會嘗試僅使用存取遮罩中的刪除位元來複製檔案。Symantec Endpoint Protection 會針對該複製嘗試記錄另外一個事件。請參閱： 檢視日誌
阻止或允許使用者啟用或停用應用程式控制 (選擇性)	在極少數情況下，應用程式控制可能會干擾用戶端電腦上執行的某些安全應用程式。您可能要允許使用者停用此選項以對問題進行疑難排解。在混合模式或用戶端模式下，使用「用戶端使用者介面設定」對話方塊中的「允許使用者啟用和停用應用程式裝置控制」設定。請參閱： 防止使用者在用戶端電腦上停用防護

您也可以使用系統鎖定，在用戶端電腦上允許核准的應用程式或是攔截未核准的應用程式。請參閱：

[設定系統鎖定](#)

啟用和測試預設應用程式規則

應用程式控制包括由一或多個規則組成的預設規則集。預設應用程式控制規則集會隨 Symantec Endpoint Protection Manager 一起安裝。預設規則集在安裝時是停用的。要在應用程式控制政策中使用預設規則集，您必須啟用它們並將政策套用至用戶端群組。

如需常見預先定義規則的說明，請參閱：

[強化 Symantec Endpoint Protection \(SEP\)：使用應用程式與裝置控制政策來增加安全性](#)

在下列工作中，您可以啟用和測試「攔截向 **USB** 磁碟機寫入內容」規則集。

啟用預設應用程式規則集

1. 在主控台中，按下「政策」>「應用程式與裝置控制」，然後在「工作」下方，按下「新增應用程式控制政策」。
2. 在「概述」窗格中，輸入政策的名稱和說明。
3. 按下「應用程式控制」。
4. 在「應用程式控制」窗格中，勾選您要實作的每個規則集旁的「已啟用」核取方塊。
例如，在「攔截向 **USB** 磁碟機寫入內容」規則集旁，勾選「已啟用」欄中的核取方塊。
5. 要檢閱規則集的規則，請選取規則，按下「編輯」，然後按下「確定」。
[將自訂規則新增至應用程式控制](#)
6. 將「生產」變更為「測試 (只記錄)」。
7. 指派政策給群組，然後按下「確定」。

測試攔截向 **USB** 磁碟機寫入內容規則集

1. 在用戶端電腦上，連接 USB 磁碟機。
2. 開啟「Windows 檔案總管」，然後連按兩下 USB 磁碟機。
3. 以滑鼠右鍵按下視窗，然後按下「新增」>「資料夾」。
如果應用程式控制已生效，就會出現「無法建立資料夾」錯誤訊息。

更多資訊

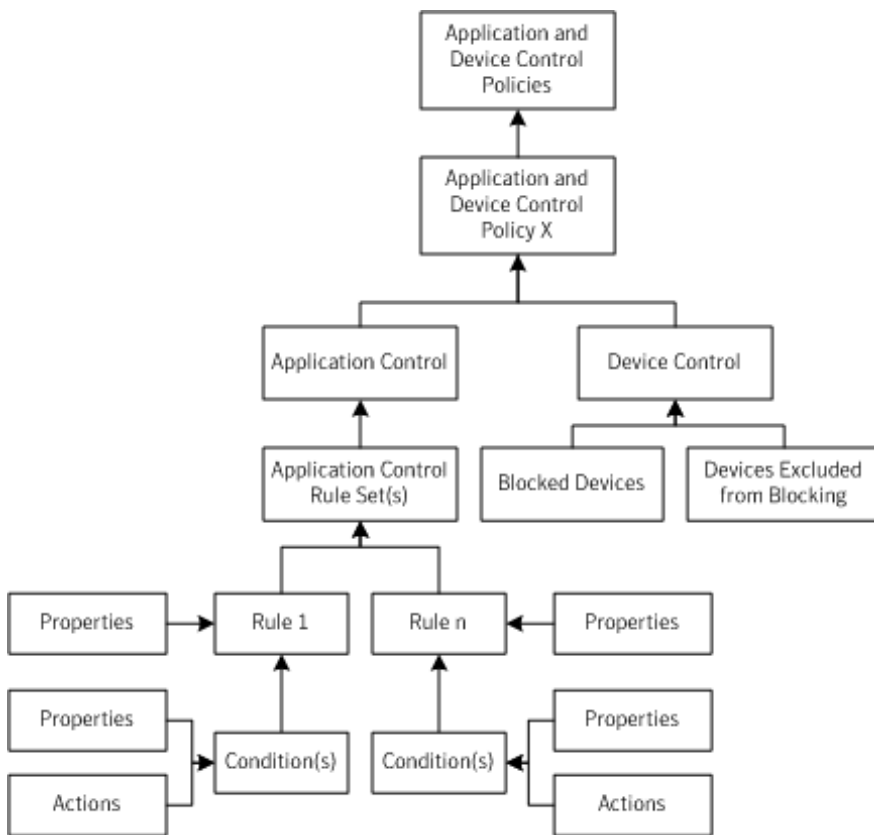
- [關於應用程式控制、系統鎖定和裝置控制](#)
- [關於應用程式控制與裝置控制政策的結構](#)

應用程式控制與裝置控制政策的結構

「應用程式與裝置控制」政策分兩個部分：

- 「應用程式控制」包含一或多個規則集。每個規則集都包含一或多個規則。您可以架構各項規則的屬性、條件和動作：
 - 「規則」定義您要監控的應用程式。
 - 「條件」監控規則中定義之應用程式的指定操作。條件也包含觀察到指定操作時要採取的動作。
 - 新增規則和條件時，您需要指定條件的特定「屬性」以及符合條件時要採取的動作。每種條件類型包含的屬性皆不同。
- 裝置控制包含攔截的裝置清單及不攔截的裝置清單。您可以新增至這兩份清單，並管理其中的內容。

下圖說明應用程式和裝置控制元件，以及兩者之間的關係。



更多資訊

- [關於應用程式控制、系統鎖定和裝置控制](#)
- [設定應用程式控制](#)
- [將自訂規則新增至應用程式控制](#)
- [管理裝置控制](#)

將自訂規則新增至應用程式控制

如果預設規則集不符合您的需求，請新增規則集與規則。您可以修改隨政策安裝的預先定義的規則集。

- 規則集是一個配置區，其中包含一或多個允許或攔截動作的規則。
- 規則集中的規則則定義一或多個程序或應用程式。您也可以排除不要監控的程序。
- 每個規則包含要套用至特定程序的條件和動作。對於各項條件，您可以架構符合條件時要採取的動作。您可以架構規則只套用於某些應用程式，也可以架構規則排除動作套用於其他應用程式。

關於應用程式控制與裝置控制政策的結構

使用下列步驟來自行新增應用程式規則：

- [步驟 1：將自訂規則集和規則新增至應用程式控制政策 \(選用\)](#)
- [步驟 2：為規則定義應用程式或程序 \(選用\)](#)
- [步驟 3：將條件和動作新增至規則 \(選用\)](#)
- 步驟 4：在將規則套用至生產網路前先測試規則。請參閱：
[測試應用程式控制規則](#)

步驟 1：將自訂規則集和規則新增至應用程式控制政策 (選擇性)

最佳實務準則是建立一個規則集，並在其中納入所有允許、攔截和監控指定工作的動作。另一方面，如果您有多個工作，則應該建立多個規則集。例如，如果您想要攔截所有嘗試寫入抽取式磁碟機的動作，並且想要攔截對特定應用程式進行篡改的應用程式，則應該建立兩個規則集。您可以按需新增及啟用任何數目的規則集與規則。

例如，BitTorrent 是一項用於點對點檔案共用的通訊協定，其本身並不安全。BitTorrent 會散佈電影、遊戲、音樂和其他檔案。BitTorrent 可謂散佈威脅最簡單的方法之一。惡意軟體會隱藏在透過點對點網路來共用的檔案內。您可以使用應用程式控制來攔截對 BitTorrent 通訊協定的存取。您也可以使用點對點驗證和入侵預防。請參閱：

[透過架構點對點驗證攔截遠端電腦](#)

架構規則及其條件時，請考慮順序問題，以免發生無法預期的結果。此工作通常只應由進階管理員執行。請參閱：

[新增應用程式控制規則時的最佳實務準則](#)

將自訂規則集和規則新增至應用程式控制政策

1. 開啟應用程式控制政策。請參閱：
[啟用和測試預設應用程式規則](#)
2. 在「應用程式控制」面板的預設規則集清單下方，按下「新增」。
若要修改預先定義的規則集，請將其選取，然後按下「編輯」。例如，若要監控存取 BitTorrent 通訊協定的應用程式，請選取「攔截從抽取式磁碟機執行程式 [AC2]」。
3. 在「新增應用程式控制規則集」對話方塊中，為規則集輸入名稱和敘述。
4. 在「規則」下方，選取「規則 1」，然後在「屬性」標籤上，為規則輸入有意義的名稱和敘述。
若要新增其他規則，請按下「新增」>「新增規則」。

步驟 2：為規則定義應用程式或程序 (選用)

每項規則均必須包含至少一個要在用戶端電腦上監控的應用程式或程序。您還可以從規則中排除特定應用程式。

為規則定義應用程式或程序

1. 選取規則後，在「屬性」標籤的「套用此規則至下列程序」旁邊，按下「新增」。
2. 在「新增程序定義」對話方塊中，輸入應用程式名稱或程序名稱，例如 `bittorrent.exe`。
如果您想將這項規則套用至某組應用程式以外的其他所有應用程式，請在這個步驟中定義代表全部之意的萬用字元 (*)。然後，在「請勿套用此規則至下列程序」旁邊，列出需要當作例外的應用程式。
3. 按下「確定」。
「啟用此規則」核取方塊預設為啟用狀態。如果取消核取此選項，則不會套用規則。

步驟 3：將條件和動作新增至規則 (選用)

條件可控制嘗試在用戶端電腦上執行的應用程式或程序的行為。每種條件類型均有專屬的屬性來指定條件要尋找的情況。

每個條件均各自設有當條件成立時，要對程序採取的特定動作。動作（「終止程序」動作除外）一律會套用至您為「規則」（而非「條件」）定義的程序。

WARNING

「終止程序」動作會終止呼叫者程序或是提出要求的應用程式。呼叫者程序是您在規則中（而非在條件中）定義的程序。對目標程序執行的其他動作則在條件中定義。

Table 100: 依條件採取的動作

條件	說明
登錄存取嘗試	允許或攔截對用戶端電腦上登錄設定的存取
檔案和資料夾存取嘗試	允許或攔截對用戶端電腦上所定義檔案或資料夾的存取
啟動程序嘗試	允許或攔截在用戶端電腦上啟動程序的動作。
終止程序嘗試	允許或攔截在用戶端電腦上終止程序的動作。例如，您可能需要攔截將特定應用程式停止的動作。 Warning! 「終止程序嘗試」條件會參考目標程序。如果您對 Symantec Endpoint Protection 或其他重要程序使用「終止程序嘗試」條件，然後使用「終止程序」動作來刪除嘗試刪除 Symantec Endpoint Protection 的程序。
載入 DLL 嘗試	允許或攔截在用戶端電腦載入 DLL 的動作。

將條件和動作新增至規則

- 在「規則」下，選取您新增的規則，按下「新增」>「新增條件」，然後選擇條件。請參閱：
[選擇用於規則之條件的最佳實務準則](#)
例如，按下「啟動程序嘗試」，即可新增要在用戶端電腦存取 BitTorrent 通訊協定時套用的條件。
- 在「屬性」標籤上，選取應該或不應該啟動的程序：
 - 指定要啟動的程序：
在「套用至下列實體」旁邊，按一下「新增」。
 - 排除不要啟動的程序：
在「請勿套用至下列程序」旁邊，按一下「新增」。
- 在「新增實體定義」對話方塊中，輸入程序名稱、DLL 或登錄機碼。
例如，若要新增 BitTorrent，請輸入其檔案路徑和可執行檔，例如：C:\Users\UserName\AppData\Roaming\BitTorrent
若要將條件套用至特定資料夾中的所有程序，最佳實務準則是使用 folder_name* 或 folder_name**。一個星號即包括指名資料夾中全部的檔案和資料夾。使用 folder_name 可包含指名資料夾中各個檔案和資料夾，以及各個子資料夾中各個檔案和資料夾。
- 按下「確定」。
- 在條件的「動作」標籤上，選取要採取的動作。
例如，若要在 Textpad 嘗試啟動 Firefox 時加以攔截，請按下「攔截存取」。
- 核取「啟用記錄」和「通知使用者」，然後新增要向用戶端電腦使用者顯示的訊息。
例如，輸入 Textpad tries to launch Firefox。
- 按下「確定」。
此時會顯示新規則集，並會針對測試模式架構此規則集。您應該先測試新規則集，再將其套用至用戶端電腦。

新增應用程式控制規則時的最佳實務準則

您應該審慎規劃自訂應用程式控制規則。建立應用程式控制規則時，請記住以下最佳實務準則。

Table 101: 應用程式控制規則的最佳實務準則

最佳實務準則	說明	範例
考慮規則順序	應用程式控制規則的運作方式類似於大多數網路型防火牆規則，兩者都是使用第一個規則相符的功能。如果滿足多個條件時，第一個規則會是套用的唯一規則，除非為此規則架構的動作為「繼續處理其他規則」。	您希望防止所有使用者在 USB 磁碟機上移動、複製和建立檔案。 您具有一個現有規則，該規則具有一個條件允許寫入存取名為 Test.doc 的檔案。您可以將第二個條件新增至這個現有規則集，以攔截所有 USB 磁碟機。在這種情況下，使用者仍可以建立和修改 USB 磁碟上的 Test.doc 檔案。在規則集中，「允許存取」Test.doc 的條件會在「攔截存取」USB 磁碟機的條件之前。當滿足清單中「攔截存取」USB 磁碟機的條件前面的條件時，便不會處理這個條件。
使用正確的動作	「終止程序嘗試」條件會允許或攔截應用程式在用戶端電腦上終止呼叫程序的動作。 此條件不會允許或攔截使用者採用平常的方法停止應用程式，例如按下「檔案」功能表中的「結束」。	Process Explorer 是一項工具，可顯示已開啟或載入的 DLL 程序，以及程序使用哪些資源。 您可能希望在 Process Explorer 嘗試終止特定應用程式時終止 Process Explorer。 使用「終止程序嘗試」條件和「終止程序」動作建立此類型的規則。您可以將此條件套用至 Process Explorer 應用程式。您可以將此規則套用至您不希望 Process Explorer 終止的一個或多個應用程式。
每個目標使用一個規則集	建立一個規則集，並在其中納入所有允許、攔截或監控特定工作的動作。	您希望攔截嘗試寫入所有的卸除式磁碟機，並且希望攔截應用程式篡改特定應用程式。 若要實現這些目標，應該建立兩個不同的規則集，而不是建立單一規則集。
謹慎使用「終止程序」動作	當呼叫程序滿足所架構的條件時，「終止程序」動作會刪除該程序。 只有進階管理員才可使用「終止程序」動作。通常，您應該改用「攔截存取」動作。	您希望在任何程序啟動 Winword.exe 時隨時終止 Winword.exe。 您可以建立一個規則並使用「啟動程序嘗試」條件和「終止程序」動作架構此規則。您將條件套用於 Winword.exe，並且將規則套用於全部的程序。 您可能希望此規則終止 Winword.exe，但此規則未執行這個動作。如果您嘗試從「Windows 檔案總管」啟動 Winword.exe，包含此組態的規則會終止 Explorer.exe，而非 Winword.exe。如果使用者直接啟動 Winword.exe，則仍可執行該程式。請改用「攔截存取」動作來攔截目標程序，或 Winword.exe。
在將規則投入生產環境之前先測試規則	規則集的「測試 (只記錄)」選項僅會記錄動作，而不會將動作套用至用戶端電腦。在將規則切換回生產模式之前，請先以測試模式執行規則達某段可接受的時間長度。在此期間，可檢閱應用程式控制日誌，並確認規則是否會按計劃運作。	測試選項將會減少因未考量規則的所有可能性而引起的潛在意外。請參閱： 測試應用程式控制規則

更多資訊

- [將自訂規則新增至應用程式控制](#)
- [選擇用於規則之條件的最佳實務準則](#)

選擇用於規則之條件的最佳實務準則

您可以新增自訂應用程式控制規則和條件，以防止使用者開啟應用程式、寫入檔案或共用檔案。您可以查看預設規則集，來幫助決定如何設定規則。例如，您可以編輯「攔阻應用程式執行」規則集，以檢視如何使用「啟動程序嘗試」條件。請參閱：

[將自訂規則新增至應用程式控制](#)

Table 102: 用於規則的一般條件

規則	條件
防止使用者開啟應用程式	當應用程式滿足下列條件之一時，您可以攔截它： • 啟動程序嘗試 例如，若要防止使用者傳輸 FTP 檔案，您可以新增規則來攔截使用者從指令提示啟動 FTP 用戶端。 • 載入 DLL 嘗試 例如，如果您新增在用戶端電腦上攔截 Msvcr7.dll 的規則，則使用者將無法開啟 Microsoft WordPad。此規則還會攔截使用 DLL 的任何其他應用程式。
防止使用者寫入特定檔案	您可能想要允許使用者開啟某個檔案，但不能修改檔案。例如，檔案可能包含員工應檢視但不該編輯的財務資料。 您可以建立規則，將檔案的唯讀存取權限授予使用者。例如，您可以新增規則，來允許您在記事本中開啟文字檔案而不允許您編輯此檔案。 針對此類型的規則使用「檔案和資料夾存取嘗試」條件。
在 Windows 電腦上攔截檔案共用	您可以在 Windows 電腦上停用本機檔案和列印共用。 包括下列條件： • 登錄存取嘗試 新增所有相關的 Windows 安全性和共用登錄機碼。 • 啟動程序嘗試 指定伺服器服務程序 (svchost.exe)。 • 載入 DLL 嘗試 指定「安全性」和「共用」標籤的 DLL (rshx32.dll、ntshrui.dll)。 • 載入 DLL 嘗試 指定伺服器服務 DLL (srvsvc.dll)。 您可以將各個條件的動作設定為「攔截存取」。 您還可以使用防火牆規則來阻止或允許用戶端電腦共用檔案。請參閱： 允許用戶端瀏覽網路中的檔案和印表機
防止使用者執行對等應用程式	您可以防止使用者在其電腦上執行點對點應用程式。 您可以建立具有「啟動程序嘗試」條件的自訂規則。在此條件中，您必須指定所有要攔截的點對點應用程式，例如 LimeWire.exe 或 *.torrent。您可以將條件的動作設定為「拒絕存取」。 使用「入侵預防」政策攔截來自點對點應用程式的網路流量。使用防火牆政策攔截傳送和接收點對點應用程式流量的通訊埠。請參閱： • 管理入侵預防 • 建立防火牆政策
攔截嘗試寫入 DVD 光碟機	目前，應用程式控制不具有可直接攔截 CD/DVD 寫入的預設規則。相反地，您可以使用「新增條件」和「檔案和資料夾存取嘗試」條件建立攔截寫入 CD 或 DVD 磁碟機之特定 DLL 的規則。 您還應建立設定 Windows 登錄機碼的「主機完整性」政策，以攔截嘗試寫入 DVD 光碟機。請參閱： • 設定主機完整性 • 如何在 Windows 7 中攔截 CD/DVD 寫入

測試應用程式控制規則

新增應用程式控制規則後，您應該在自己的網路中測試這些規則。「應用程式控制」政策中使用的規則集若發生架構錯誤，可能會使電腦或伺服器無法運作。用戶端電腦可能會失敗，或者與 Symantec Endpoint Protection Manager 之間的通訊可能會遭到攔截。測試好規則後，即可將其套用至您的生產網路。

步驟 1：將規則集設定為測試模式

您可以將模式設定為測試模式來測試規則集。測試模式會建立一個日誌項目，用以指示何時套用規則集中的規則（實際上並不會套用這些規則）。

預設規則預設會使用生產模式。自訂規則預設會使用測試模式。您應該同時測試預設和自訂規則集。

您可能希望個別測試規則集中的規則。您可以在規則集中啟用或停用規則來測試各個規則。

將規則集變更為測試模式

1. 在主控台中開啟「應用程式與裝置控制」政策。
2. 在「應用程式控制政策」下方，按下「應用程式控制」。
3. 在「應用程式控制規則集」清單中，針對規則集按下「測試/正式」欄中的下拉式箭頭，然後按下「測試 (只記錄)」。

如需詳細資訊，請參閱：

[設定應用程式控制](#)

步驟 2：將「應用程式與裝置控制」政策套用至測試網路中的電腦

如果您建立了新的「應用程式與裝置控制」政策，請將此政策套用至測試網路中的用戶端。請參閱：

[指派政策給群組或位置](#)

步驟 3：監控應用程式控制日誌

規則集在測試模式下執行一段時間後，可檢查日誌是否有任何錯誤。在測試模式和生產模式中，應用程式控制事件均是記錄在 Symantec Endpoint Protection Manager 的應用程式控制日誌中。在用戶端電腦上，應用程式控制和裝置控制事件會顯示在「控制」日誌中。

一項應用程式控制動作可能會顯示有重複或多個日誌項目。例如，explorer.exe 在嘗試複製檔案時，會設定檔案存取遮罩的寫入位元和刪除位元。Symantec Endpoint Protection 會記錄該事件。如果複製動作因應用程式控制規則攔截這個動作而失敗，explorer.exe 會嘗試僅使用存取遮罩中的刪除位元來複製檔案。Symantec Endpoint Protection 會針對該複製嘗試記錄另外一個事件。請參閱：

[檢視日誌](#)

步驟 4：將規則集變更回生產模式

如果規則如預期般執行，可將規則集模式變更回生產模式。

設定系統鎖定

系統鎖定透過使用允許清單或拒絕清單，來控制允許執行於用戶端電腦上的應用程式。

- 允許清單 (許可清單) 包括所有已核准的應用程式。用戶端會攔截所有其他應用程式。
- 拒絕清單 (黑名單) 包括所有未核准的應用程式。用戶端允許所有其他應用程式。

您應產生一份用戶端執行之所有應用程式的清單。例如，您的網路可能包括 Windows 8.1 32 位元及 64 位元用戶端，以及 Windows 10 64 位元用戶端。您可以為每個用戶端影像建立檔案指紋清單。

您可透過產生檔案指紋或特定應用程式檔案名稱的清單來建立允許清單或拒絕清單：

- 檔案指紋清單包括檔案指紋和電腦路徑位置。使用檔案指紋清單比使用應用程式名稱更安全，因為駭客可以重新命名應用程式名稱。
- 檔案名稱清單包括檔案路徑和應用程式名稱，例如 C:\Program Files\Notepad++。檔案名稱清單更易於維護。若您允許經常更新某個知名應用程式，則無需不斷更新檔案指紋清單。

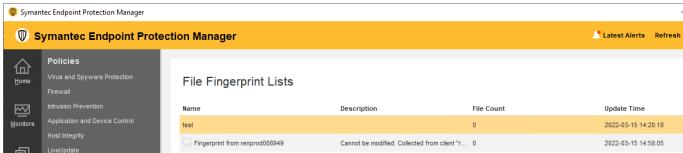
NOTE

- 您需要針對網路中的每個群組或位置設定系統鎖定。
- 系統鎖定允許的所有應用程式受 Symantec Endpoint Protection 中的其他保護功能支配。
- 您可以使用「應用程式控制」政策而不使用系統鎖定來控制特定的應用程式，也可以既使用「應用程式與裝置控制」政策又使用系統鎖定。

系統鎖定步驟

NOTE

必須安裝並啟用應用程式控制元件，系統鎖定才能運作。

動作	說明
步驟 1：建立檔案指紋清單或檔案名稱清單。	方法 1：建立檔案指紋清單 您可以使用下列其中一種方法來建立檔案指紋清單： - 與用戶端軟體一起安裝的 checksum.exe 公用程式。 checksum.exe 公用程式收集指定路徑中應用程式的所有指紋。此方法適用於建立拒絕清單。 「收集檔案指紋清單」指令。 此指令會收集檔案指紋清單，此包括目標用戶端群組或個別用戶端電腦上的每個應用程式。此方法適用於建立允許清單。您無法修改指令產生的檔案指紋清單。 若使用此方法，請略過步驟 2，並移至步驟 3。 - 協力廠商指令碼工具，如 PowerShell 或 Python，或文字編輯器。 checksum.exe 公用程式 (自 14.3 RU5 起) 和「收集檔案指紋清單」指令 (自 14.3 RU5 起) 建立一個具舊版 MD5 和更安全之 SHA-256 檔案指紋的清單。 如需詳細資訊，請參閱： 建立檔案指紋清單 Note: 如果您在網路中執行 Symantec EDR，您可能會從 Symantec EDR 看到檔案指紋清單。如需詳細資訊，請參閱： Note: 系統鎖定與 Symantec EDR 拒絕清單 (黑名單) 規則之間的互動
	方法 2：建立檔案名稱清單 或者，您可將個別應用程式名稱新增至檔案名稱清單中，以允許或將其攔截。 您可使用任何文字編輯器來建立包含檔案名稱的文字檔。與檔案指紋清單不同，您可將這些檔案名稱直接匯入系統鎖定架構。匯入檔案名稱後，應用程式會以個別項目顯示於系統鎖定架構中。若您直接新增檔案名稱，則將獲得用來監控應用程式的一組擴充屬性。 若使用此方法，請略過步驟 2，並移至步驟 3。 Note: 當以拒絕模式啟用系統鎖定时，擁有大量的指定應用程式可能會影響用戶端電腦效能。 如需詳細資訊，請參閱： 建立應用程式名稱清單以匯入系統鎖定架構中
步驟 2：將檔案指紋清單匯入 Symantec Endpoint Protection Manager (僅使用 checksum.exe 或協力廠商指紋產生工具)。	若於步驟 1 中使用 checksum.exe 或協力廠商指紋產生公用程式產生檔案指紋清單，請將清單新增至「政策 > 政策元件 > 檔案指紋清單」。  如需詳細資訊，請參閱： 在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單 Note: 若使用「收集檔案指紋清單」命令，將會自動新增清單。

動作	說明
步驟 3：允許或攔截檔案指紋清單或檔案名稱清單。	依預設，系統鎖定將遭停用並允許所有應用程式。所有應用程式皆會加以記錄，但不會遭到攔截。 如要允許或攔截應用程式 - 於「系統鎖定」對話方塊中，按一下「僅記錄未核准的應用程式」。 - 按一下「允許模式」或「拒絕模式」。 - 於允許模式中 (預設值)，檔案指紋為已核准的應用程式。當在允許模式下啟用系統鎖定时，會攔截不在核准的應用程式清單上的所有應用程式。 - 在拒絕模式下，檔案指紋是未核准的應用程式。當在拒絕模式下啟用系統鎖定时，會攔截在未核准的應用程式清單上的所有應用程式。 - 將檔案指紋清單和/或個別應用程式新增至系統鎖定架構。 您可匯入應用程式名稱清單，無須於系統鎖定架構中逐一輸入名稱。 - 在允許模式下，應用程式是已核准的應用程式。 - 在拒絕模式下，應用程式是未核准的應用程式。 - 按一下「確定」，可在一段時間內執行測試。 如需詳細資訊，請參閱： 啟用系統鎖定前設定和測試系統鎖定架構
步驟 4：檢視未核准的應用程式，並視需要修改系統鎖定架構。	執行一段時間的測試後，可以檢查未核准的應用程式清單。可以在「系統鎖定」對話方塊中檢查狀態，以檢視未核准的應用程式清單。 記錄的事件也會出現在「應用程式控制」日誌中。 您可決定是否新增更多應用程式至檔案指紋清單或應用程式清單中。啟用系統鎖定之前，也可以視需要新增或移除檔案指紋清單或應用程式。 如需詳細資訊，請參閱： 啟用系統鎖定前設定和測試系統鎖定架構
步驟 5：啟用系統鎖定。	如要啟用系統鎖定 - 於「系統鎖定」對話方塊中，按一下「啟用系統鎖定」。 - 按下「確定」。 Note: 確定在啟用系統鎖定之前，已測試您的架構。如果攔截了必要的應用程式，用戶端電腦可能無法重新啟動。

選用的測試步驟

動作	說明
步驟 1：更新系統鎖定的檔案指紋清單。	您可能會隨時間變更網路中執行的應用程式。您可依需要更新檔案指紋清單或移除清單。您可以下列方式更新檔案指紋清單： - 請手動附加、取代或合併您匯入的檔案指紋清單。 您無法將檔案指紋清單附加至您使用「收集檔案指紋清單」指令產生的指紋清單。您可以使用指令產生的清單附加匯入的清單。在該情況下，如果您重新執行指紋指令，則必須重新建立附加的清單。 如需詳細資訊，請參閱： 手動更新 Symantec Endpoint Protection Manager 中的檔案指紋清單 在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單 - 自動更新您匯入的現有檔案指紋清單。 也可以自動更新您匯入的應用程式或應用程式名稱清單。 如需詳細資訊，請參閱：自動更新系統鎖定的檔案指紋清單來允許或攔截 - 重新執行「收集檔案指紋清單」指令以自動更新指令產生的指紋清單。 如需詳細資訊，請參閱：建立檔案指紋清單 當您重新執行此指令時，新清單會自動取代現有清單。 Note: 在將用戶端電腦新增到網路中後，您可能想要重新測試整個系統鎖定架構。您可將新的用戶端移至獨立群組或測試網路，然後停用系統鎖定。或者，您可以保持系統鎖定啟用，並在只記錄模式下執行架構。也可如步驟 2 中的說明，測試個別檔案指紋或應用程式。
步驟 2：當系統鎖定啟用後，在新增或移除選取項目之前對其進行測試。	當系統鎖定啟用後，在系統鎖定架構中新增或移除個別檔案指紋、應用程式名稱清單或特定應用程式前，可以對它們進行測試。 若您有不再使用的檔案指紋清單，請考慮將其移除。 Note: 從系統鎖定新增或移除檔案指紋清單或特定應用程式時，請小心。從系統鎖定新增或移除項目可能有風險。可能會攔截用戶端電腦上的重要應用程式。 - 測試選取項目。 使用「移除前測試」選項，將特定的檔案指紋清單或特定應用程式記錄為未核准。 執行此測試時，會啟用系統鎖定，但不攔截所選取的任何應用程式，或選取的檔案指紋清單中的任何應用程式。而是系統鎖定將應用程式記錄為未核准。 - 檢查「應用程式控制」日誌。 日誌項目會出現在「應用程式控制」日誌中。若該日誌不包含測試的應用程式項目，則可確定用戶端未使用這些應用程式。

更多資訊

[設定應用程式控制](#)

建立檔案指紋清單

您可使用「收集檔案指紋清單」指令或 checksum.exe 公用程式來建立檔案指紋清單。

檔案指紋清單包含位於電腦上指定路徑中每個執行檔或 DLL 的下列項目：

- 路徑
- 檔案名稱
- 相應的指紋

然後，將檔案指紋清單匯入 Symantec Endpoint Protection Manager，以用於您的系統鎖定組態中。

如需詳細資訊，請參閱：

- 在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單
- 設定系統鎖定
- 匯入檔案指紋清單的最佳實務 (適用於 SEP 14.3 RU5 及更新版本)

您還可使用第三方指令碼工具來建立檔案指紋清單。

Table 103: 檔案指紋範例輸出

指紋類型	範例
MD5 14.3 RU4 和更早版本	bbe80313cf12098d3fc4d8a42e9dbb33 c:\Windows\System32\notepad.exe
MD5 和 SHA-256 14.3 RU5 和更新版本	bbe80313cf12098d3fc4d8a42e9dbb33, deb5b0067e4af84bb0 7fa3d84631cee94787fb3be7cda11c0016992f54ab4dda c:\Windows\System32\notepad.exe

NOTE

SEPM 14.3 RU5 及更高版本可於 14.3 RU4 用戶端上收集 MD5 和 SHA-256 檔案指紋。

使用「收集檔案指紋清單」指令

您無法修改指令產生的檔案指紋清單。

SEPM 14.3 RU5 或更新版本的「收集檔案指紋清單」指令會建立一個同時包括舊版 MD5 及更安全 SHA-256 檔案指紋的清單。

Mac 和 Linux 用戶端電腦不會處理此指令。

NOTE

該指令不會生成相應的目錄路徑和檔名。

如要使用「收集檔案指紋清單」指令建立檔案指紋清單

1. 在「用戶端」頁面上，以滑鼠右鍵按一下群組或個別用戶端，然後選取「收集檔案指紋清單」。
執行此指令時，檔案指紋清單會自動匯入「政策 > 政策元件 > 檔案指紋清單」中。

如需詳細資訊，請參閱：

[在用戶端電腦上從主控台執行指令](#)

使用 **checksum.exe** 公用程式

與 Symantec Endpoint Protection 用戶端電腦一起安裝的 checksum.exe 公用程式。

- 14.3 RU5 和較新的 checksum.exe 公用程式會建立一個同時包括舊版 MD5 及 SHA-256 檔案指紋的清單。您可以使用或不使用 `csv` 切換執行此命令。
- 14.3 RU4 和更早的 checksum.exe 公用程式會建立一個包括 MD5 及具有 `csv` 切換之 SHA-256 檔案指紋的清單。
- 14.3 RU4 和更早的 checksum.exe 公用程式會建立一個包括 MD5 檔案指紋及不具 `csv` 切換之檔案名稱的清單。

NOTE

SEPM 14.3 RU5 及更高版本可於 14.3 RU4 用戶端上收集 MD5 和 SHA-256 檔案指紋。

如要利用 **checksum.exe** 公用程式建立檔案指紋清單

1. 在包含要建立其檔案指紋清單之影像的電腦上，開啟命令提示視窗。
電腦必須已安裝了 Symantec Endpoint Protection 用戶端軟體。
2. 瀏覽至用戶端安裝資料夾，其中包含 checksum.exe 檔案。一般而言，檔案位於以下資料夾中：
在 32 位元電腦上：C:\Program Files\Symantec\Symantec Endpoint Protection\

在 64 位元電腦上 (14.3 RU4 和更舊版本) : C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\

在 64 位元電腦上 (14.3 RU5 和更新版本) : C:\Program Files\Symantec\Symantec Endpoint Protection\

3. 鍵入下列其中一個指令：

- checksum.exe <outputfile.txt> <path>
- checksum.exe <outputfile.txt> -csv <path> (具有 csv 切換)

其中：

- <outputfile.txt> 為產生之文字檔案的名稱，其中包含指定磁碟機上所有應用程式的指紋。
- <path> 為您要在其中收集指紋資訊之電腦上的檔案路徑。
- csv 切換不區分大小寫。

NOTE

若要針對 C 磁碟機上的所有檔案執行 checksum.exe 公用程式，必須在 <path> 的末尾新增正斜線。否則，該指令僅在 checksum.exe 所在資料夾中執行。

輸出檔案中的每一行格式可為下列其中一項：

```
fingerprint_of_the_file full_pathname_of_the_exe_or_DLL  
fingerprint_of_the_file -CSV full_pathname_of_the_exe_or_DLL
```

4. 以空格分隔指紋值和完整路徑名稱。

checksum.exe 的語法範例

下列是您可用來建立 C 磁碟機上所有檔案之指紋清單的語法範例：

```
checksum.exe cdrive.txt -csv c:/
```

此指令會建立稱為 cdrive.txt 的檔案。該檔案包含所有可執行檔和 DLL (在執行所在之電腦的 C 磁碟機上找到) 的指紋和檔案路徑。

NOTE

如果路徑包含空格或如果您使用批次檔，請用引號 (") 括住路徑。例如："C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" cdrive.txt -csv c:/

下列是您可以用來在用戶端電腦上建立資料夾指紋的語法範例：

```
checksum.exe blocklist.txt -csv c:\Files
```

此指令會建立稱為 blocklist.txt 的檔案。該檔案包含於「##」資料夾中找到的任何可執行檔和 DLL 的指紋和檔案路徑。

NOTE

如果路徑包含空格或如果您使用批次檔，請用引號 (") 括住路徑。例如："C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" blocklist.txt -csv "c:\Files with a space"

在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單

使用 checksum.exe 公用程式或第三方指紋產生工具建立檔案指紋清單時，必須手動匯入這些清單。還可以合併檔案指紋清單。

Symantec Endpoint Protection Manager 主控台必須提供檔案指紋清單，以便將這些清單新增到系統鎖定架構。

如需詳細資訊，請參閱：

[以 checksum.exe 建立檔案指紋清單](#)

[匯入檔案指紋清單的最佳實務 \(適用於 SEP 14.3 RU5 及更新版本\)](#)

您使用收集檔案指紋清單指令建立的檔案指紋清單會自動在「政策元件」頁面中提供使用。您不需匯入它們。您無法修改使用「收集檔案指紋清單」指令建立的檔案指紋清單。不過，您可以將指令產生的檔案指紋清單與另一個檔案指紋清單合併。若您再次執行此指令以重新產生清單，則必須再次手動合併清單。

匯入或合併檔案指紋清單

1. 在主控台中，按下「政策」。
2. 在「政策」下方，展開「政策元件」，然後按下「檔案指紋清單」。
3. 在「工作」下方，按一下「新增檔案指紋清單」，然後按一下「下一步」。
4. 於「新增檔案指紋清單」對話方塊中，按一下「下一步」。
5. 在「新檔案指紋清單的相關資訊」面板中，鍵入新清單的名稱和說明，然後按一下「下一步」。
6. 在「建立檔案指紋清單」面板中，選取下列選項之一，然後按一下「下一步」：
 - 透過匯入指紋檔案建立檔案指紋
指定所建立的檔案指紋的路徑。您可以瀏覽尋找該檔案。
 - 透過合併多個現有檔案指紋建立檔案指紋
選取您要合併的指紋清單。

NOTE

只有在您已匯入多個檔案指紋清單時，才可使用此選項。

7. 按照畫面上的指示進行操作。
匯入或合併的指紋清單會顯示於「政策 > 政策元件 > 檔案指紋清單」之下。

匯入檔案指紋清單的最佳實務 (適用於 SEP 14.3 RU5 及更新版本)

將 Symantec Endpoint Protection Manager (SEPM) 升級至 14.3 RU5 及更高版本時，Symantec 建議您重新產生並重新匯入已指派給系統鎖定組態的所有現有檔案指紋清單。

從 14.3 RU5 開始，checksum.exe 公用程式和「收集檔案指紋清單」指令皆會產生一個 CSV 文字檔案，其同時包括經密碼編譯更為安全的 SHA-256 指紋和舊版 MD5 指紋。您仍可使用僅包含 MD5 值的檔案指紋清單，但其並不安全。使用 SHA-256 格式可消除指紋衝突攻擊的風險。您還可僅使用 SHA-256 值的檔案指紋清單，但無法將該清單部署至 14.3 RU3 及更早版本的用戶端。

CSV 檔案的每一列皆會將應用程式對應至 MD5 檔案指紋和相應的 SHA-256 指紋。可能會有缺少 SHA-256 檔案值或 MD5 值的情況，此稱為部分對應。當應用程式不再存在於舊電腦上時，可能會發生此部分對應。若指紋檔案清單具有部分對應，「政策元件 > 檔案指紋清單」頁面隨即顯示下列訊息：

```
The imported file fingerprint list contains at least one entry that uses  
the legacy MD5 fingerprint type without a mapping to a more secure SHA-256  
fingerprint type. Symantec recommends that you reimport a new .CSV file that  
contains both MD5 and SHA-256 file fingerprints.
```

如要解決此問題，請使用支援 SHA-256 格式的較新用戶端重新產生檔案指紋清單，或手動新增缺少的檔案指紋。若找不到缺少的檔案指紋：

- 對於缺少的 MD5 指紋，14.3 RU4 和較早的用戶端將會略過該應用程式。14.3 RU5 和更高版本的用戶端會使用 SHA-256 指紋。
- 對於缺少的 SHA-256 指紋，14.3 RU5 及更高版本的用戶端會使用 MD5 指紋，但安全性較低。

NOTE

SEPM 14.3 RU5 及更高版本可於 14.3 RU4 用戶端上收集 MD5 和 SHA-256 檔案指紋。

重新產生每個群組的檔案指紋清單後，您必須重新匯入該清單並重新測試系統鎖定組態。

Table 104: 檔案指紋範例輸出

指紋類型	範例
MD5 14.3 RU4 和更早版本	bbe80313cf12098d3fc4d8a42e9dbb33 c:\Windows\System32\notepad.exe
MD5 和 SHA-256 14.3 RU5 和更新版本	bbe80313cf12098d3fc4d8a42e9dbb33, deb5b0067e4af84bb0 7fa3d84631cee94787fb3be7cda11c0016992f54ab4dda c:\Windows\System32\notepad.exe

如需詳細資訊，請參閱：

[在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單](#)

[設定系統鎖定](#)

更新 Symantec Endpoint Protection Manager 中的檔案指紋清單

在執行系統鎖定一段時間之後，您可能會想要更新檔案指紋清單。您可以附加、取代或移除已匯入的現有檔案指紋清單中的項目。您無法直接編輯 Symantec Endpoint Protection Manager 中任何現有的檔案指紋清單。

若您要將指紋清單合併到不同名稱的新清單，請使用「新增檔案指紋精靈」。

如果您使用收集檔案指紋清單指令建立指紋清單，則不可附加、取代或移除項目。不過，您可以將指令產生的清單附加至匯入的清單。如果您重新執行此指令，則必須再次手動更新指紋清單。

您無法修改 Symantec EDR 傳送至 Symantec Endpoint Protection Manager 的任何檔案指紋清單。請參閱：

- [在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單](#)
- [設定系統鎖定](#)
- [匯入檔案指紋清單的最佳實務 \(適用於 SEP 14.3 RU5 及更新版本\)](#)

更新 Symantec Endpoint Protection Manager 中的檔案指紋清單

1. 在主控台中，按下「政策」。
2. 在「政策」下方，展開「政策元件」，然後按下「檔案指紋清單」。
3. 在「檔案指紋清單」窗格中，選取要編輯的指紋清單。
4. 按下「編輯」。
5. 在「編輯檔案指紋精靈」中，按「下一步」。
6. 執行下列其中一個動作：
 - 按一下「附加一個指紋至此檔案指紋清單」，新增檔案至現有的檔案。
 - 按一下「附加其他檔案指紋清單至此檔案指紋清單」，以合併您已匯入的檔案指紋清單。
 - 按一下「將此指紋清單取代為指紋清單檔案」。
 - 按一下「移除已出現於指紋檔案中的所有指紋」。
7. 執行下列其中一項工作：
 - 按下「瀏覽」找出檔案，或輸入您要附加、取代或移除之檔案指紋清單的完整路徑。
 - 選取您要合併的檔案指紋。

8. 按「下一步」>「關閉」>「完成」。

系統鎖定與 Symantec EDR 拒絕清單 (黑名單) 規則之間的互動

如果您的網路包括 Symantec EDR，您可能會在 Symantec EDR 的系統鎖定組態中看到攔截的應用程式。

Symantec EDR 拒絕清單以下列方式與系統鎖定組態互動：

- Symantec Endpoint Protection Manager 從 Symantec EDR 接收黑名單規則時，Symantec Endpoint Protection Manager 會為所有網域和群組以黑名單模式啟用系統鎖定。
- 拒絕清單規則顯示於系統鎖定組態中的 Symantec Endpoint Protection Manager 檔案指紋清單內。您無法從 Symantec EDR 修改檔案指紋清單。
- 如果您架構了具有以允許模式啟用之系統鎖定的用戶端群組，設定將予以保留且 Symantec Endpoint Protection Manager 不會使用 Symantec EDR 拒絕清單規則。
- 如果您停用系統鎖定並刪除 Symantec EDR 拒絕清單，Symantec Endpoint Protection Manager 會自動重新啟用系統鎖定並套用拒絕清單。
- 如果您停用系統鎖定但不刪除 Symantec EDR 拒絕清單，在您重新啟用系統鎖定之前，其將保留為停用狀態。

NOTE

Symantec EDR 會直接將允許清單規則傳送至 Symantec Endpoint Protection 用戶端。Symantec EDR 不會將允許清單檔案指紋傳送至 Symantec Endpoint Protection Manager。

更多資訊

- [設定系統鎖定](#)
- [將用戶端群組架構為使用私用伺服器進行信譽查詢和提交](#)

建立應用程式名稱清單以匯入系統鎖定架構中

您可將應用程式名稱清單匯入系統鎖定架構。您可能想要匯入應用程式名稱清單，而不是將應用程式名稱逐一新增至系統鎖定架構。

根據預設，合併應用程式名稱清單中最多可包含 512 個應用程式。您可以在 conf.properties 檔案中變更該數目上限。

您可以使用任何文字編輯器，建立應用程式名稱清單檔案。

檔案中的每一行可包含用空格分隔的下列項目：

- 檔案名稱
如果使用路徑名稱，則必須放在引號內。
- 測試模式
值應為 1 或 Y (表示啟用)，或者 0 或 N (表示停用)。如果欄位保留空白，表示停用測試模式。如果要指定比對模式，您必須包含值。
- 比對模式 (萬用字元或規則運算式)
值應為 1 或 Y (表示規則運算式比對)，或者 0 或 N (表示萬用字元比對)。如果欄位保留空白，就會使用萬用字元比對。

NOTE

測試模式欄位會啟用或停用清單中每個應用程式的「增加前測試」或「移除前測試」選項。當您使用「僅記錄應用程式」選項來測試整個系統鎖定架構時，會忽略測試模式欄位。

每一行都應使用下列語法：

```
filename test_mode matching_mode
```

例如：

```
aa.exe
```

```
bb.exe 0 1
cc.exe 1
dd.exe 1 0
"c:\program files\ee.exe" 0 0
```

將此清單匯入系統鎖定時，個別應用程式會出現在系統鎖定架構中，且具有下列設定：

Table 105: 比對模式設定的範例

應用程式名稱	「增加前測試」 或「移除前測試」	比對模式
aa.exe	已停用	萬用字元
bb.exe	已停用	規則運算式
cc.exe	已啟用	萬用字元
dd.exe	已啟用	萬用字元
c:\program files\ee.exe	已停用	萬用字元

更多資訊

[設定系統鎖定](#)

自動更新系統鎖定的檔案指紋清單來允許或攔截

Symantec Endpoint Protection Manager 可以自動更新您匯入、合併或附加的現有檔案指紋清單和應用程式名稱清單。當您在同一台電腦上重新執行此指令時，會自動更新您從「收集檔案指紋清單」指令所產生的檔案指紋清單。

NOTE

從 14.3 RU5 開始，checksum.exe 公用程式和「收集檔案指紋清單」指令皆會產生一個 CSV 文字檔案，其同時包括經密碼編譯更為安全的 SHA-256 指紋和舊版 MD5 指紋。請參閱：

[匯入檔案指紋清單的最佳實務 \(適用於 SEP 14.3 RU5 及更新版本\)](#)

您也可以手動更新現有檔案指紋。

Table 106: 更新系統鎖定的許可清單 (白名單) 和拒絕清單 (黑名單)

步驟	說明
步驟 1：建立已更新的檔案指紋清單或應用程式名稱清單並壓縮檔案	您可以使用 checksum.exe 公用程式或任何第三方公用程式來建立已更新的檔案指紋清單。您可以使用任何文字編輯器來更新應用程式名稱清單。這些清單的名稱必須與 Symantec Endpoint Protection Manager 中現存的名稱相同。請參閱： 以 checksum.exe 建立檔案指紋清單 無法直接更新您從「收集檔案指紋清單」指令所產生的指紋清單。您可以將指令產生的清單與另一個清單合併，或是在匯入的清單上附加指令產生的清單。 自動更新功能需要檔案指紋和應用程式名稱清單的壓縮檔案 (zip 檔案)。您可以在 Windows 或任何壓縮公用程式中使用檔案壓縮功能來壓縮檔案。
步驟 2：建立 index.ini 檔案	index.ini 檔案指定 Symantec Endpoint Protection Manager 應更新哪一個檔案指紋清單和應用程式名稱清單。 您可以使用任何文字編輯器來建立 index.ini 檔案，然後將該檔案複製到指定的 URL。請參閱： 建立 index.ini 檔案以供自動更新用於系統鎖定的允許清單拒絕清單

步驟	說明
步驟 3：使壓縮檔案和 index.ini 可供 Symantec Endpoint Protection Manager 使用	Symantec Endpoint Protection Manager 使用 UNC、FTP 或 HTTP/HTTPS，在指定的 URL 擷取 index.ini 檔案和 zip 檔案。Symantec Endpoint Protection Manager 使用 index.ini 檔案中的指示來更新指定的檔案。當您啟用自動更新時，Symantec Endpoint Protection Manager 會根據您設定的排程定期檢查此 URL 是否有已更新的檔案。 對於 UNC，僅支援 JCFIS 共用。不支援 DFS 共用。 Note: 如果無法使用 UNC、FTP 或 HTTP/HTTPS，您可以將 index.ini 和更新的檔案指紋及應用程式名稱檔案直接複製到下列資料夾：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\WhitelistBlacklist\content。這些檔案應解壓縮。如果 Symantec Endpoint Protection Manager 無法使用 UNC、FTP 或 HTTP/HTTPS 來更新檔案，便會檢查此資料夾。
步驟 4：在管理主控台中啟用自動許可清單和拒絕清單更新	您必須在 Symantec Endpoint Protection Manager 主控台中啟用自動更新現有的許可清單或拒絕清單。 您可使用 Symantec Endpoint Protection Manager 中的「檔案指紋更新」對話方塊，啟用更新功能及指定排程和 URL 資訊。請參閱： 針對系統鎖定啟用允許清單和拒絕清單的自動更新
步驟 5：檢查許可清單或拒絕清單的自動更新狀態	您可以在主控台中檢查狀態，以確定 Symantec Endpoint Protection Manager 完成更新。在主控台中，執行下列其中一個動作： - 在「管理員」標籤上，選取站台。類似下列內容的訊息隨即出現：更新修訂版本 20200528 R016 說明的允許和拒絕清單成功。 - 在「監視器」標籤上，檢視「系統日誌：伺服器活動」。事件類型通常會顯示成類似於「檔案指紋更新」。 - 在「政策」標籤的「政策元件」下方，檢查檔案指紋清單敘述。說明會顯示成類似於修訂：20200528 R016 說明。

更多資訊

- [手動更新 Symantec Endpoint Protection Manager 中的檔案指紋清單](#)
- [設定系統鎖定](#)

建立 index.ini 檔案以供自動更新用於系統鎖定的允許清單拒絕清單

自動更新功能需要 index.ini 檔案。您可以使用任何文字編輯器建立此檔案。

NOTE

如果您在文字檔案中使用非英文字元，您應使用沒有位元組順序標記 (Byte Order Mark, BOM) 字元的 UTF-8 來編輯和儲存此檔案。

index.ini 檔案可指定下列項目：

- 包含已更新檔案指紋清單和應用程式名稱清單之壓縮檔案的版本和名稱。
- 您要更新之檔案指紋清單和應用程式名稱清單的名稱。
- 使用應用程式名稱清單的用戶端群組名稱。

現有的檔案指紋清單或群組必須已經存在於 Symantec Endpoint Protection Manager 中。群組必須啟用系統鎖定。檔案指紋清單和應用程式名稱清單必須可從指定的壓縮檔案取得。

您必須使用下列語法建構 index.ini 檔案：

```
[Revision]
Revision=YYYYMMDD RXXX
SourceFile=zip file name
Description=optional description
```

```
[FingerprintList - domain name or Default]
existing fingerprint list="updated list" REPLACE/APPEND/REMOVE
```

```
[ApplicationNameList - domain name or Default]
existing group path="updated list" REPLACE/APPEND/REMOVE
```

例如，您可以在 index.ini 檔案中使用下面幾行：

```
[Revision]
Revision=20111014 R001
SourceFile=20110901 R001.zip
Description=NewUpdates

[FingerprintList - Default]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - Default]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE

[FingerprintList - DomainABC]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - DomainABC]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE
```

更多資訊

- [自動更新系統鎖定的檔案指紋清單來允許或攔截](#)
- [建立應用程式名稱清單以匯入系統鎖定架構中](#)

針對系統鎖定啟用允許清單和拒絕清單的自動更新

您可以將 Symantec Endpoint Protection Manager 架構為自動更新用於系統鎖定的允許清單 (白名單) 和拒絕清單 (黑名單)。

若要自動更新使用「收集檔案指紋清單」指令產生的檔案指紋清單，首先執行該指令。

針對系統鎖定啟用允許清單和拒絕清單的自動更新

1. 在主控台的「管理員」標籤上，按下「伺服器」。
2. 用滑鼠右鍵按下相關伺服器，然後選取「編輯伺服器屬性」。
3. 在「伺服器屬性」對話方塊中，選取「檔案指紋更新」標籤。
4. 在「檔案指紋更新」標籤上，勾選「自動更新允許或拒絕清單」。
5. 輸入 index.ini 和壓縮檔案所在位置的 URL。

如果想要使用 UNC 或 FTP，您也必須為 index.ini 和內容指定使用者名稱和密碼。

6. 在「排程」下方，您可以指定 Symantec Endpoint Protection Manager 應該嘗試更新清單的頻率。
7. 按下「確定」。

更多資訊

[自動更新系統鎖定的檔案指紋清單來允許或攔截](#)

針對檔案指紋清單憑證問題進行疑難排解

條件

如果在升級 Symantec Endpoint Protection Manager 時看到下列訊息，則升級會遭封鎖，直到您解決了自動更新檔案指紋清單的問題。

#####

原因/矯正

當自動上傳並裝載 index.ini 檔案的伺服器 URL 傳送一個使用 HTTPS 通訊協定的憑證時，此問題便會發生。HTTPS 憑證可能具有下列任一問題。

原因	矯正
憑證過期。	更新過期的憑證。
憑證是自我簽署的。	檢查 SEPM 電腦是否信任憑證。
所架構 URL 的主機名稱不符合主旨備用名稱 (SAN) 屬性中的任何主機名稱。	SAN 屬性可讓您指定要由 SSL 憑證保護的主機名稱。 例如，如果使用 https://mycorp.com 作為伺服器 URL，則在用戶端驗證此憑證時，它會檢查 mycorp.com 主機名稱是否位於 SAN 中。 如果您使用 https://192.128.100.100 作為伺服器 URL，且伺服器傳送未在 SAN 屬性中包括 192.128.100.100 的憑證，則連線會失敗。 因此，請執行下列其中一項工作： • 確保所架構伺服器 URL 的主機名稱 (IP 位址、DNS 名稱等) 是 SAN 屬性。通常可以使用多個主機名稱連線一部伺服器。 • 針對此伺服器核發在 SAN 中列出主機名稱的憑證。

啟用系統鎖定前設定和測試系統鎖定架構

一般來說，需要在測試模式下執行一周或足夠時間的系統鎖定，以讓用戶端執行其典型的應用程式。在確定系統鎖定設定不會對使用者造成問題後，可以啟用系統鎖定。

在測試模式下執行系統鎖定时，系統鎖定處於停用。系統鎖定不會攔截任何應用程式。而是記錄但不攔截未核准的應用程式，以便您可以在啟用系統鎖定前檢閱清單。可以檢閱「控制」日誌中的日誌項目。也可以在「系統鎖定」對話方塊中檢閱未核准的應用程式。

NOTE

也可以建立防火牆規則，以允許用戶端上已核准的應用程式。

啟用系統鎖定前設定和測試系統鎖定架構

1. 在主控台中，按下「用戶端」，然後在「用戶端」下方找到要設定系統鎖定的群組。
2. 在「政策」標籤上，按下「系統鎖定」。
3. 按下「記錄未核准的應用程式」，以便在測試模式下執行系統鎖定。
此選項會記錄用戶端目前正在執行的未核准的應用程式。
4. 選取「允許模式」或「拒絕模式」。
這些選項是從 14.3 RU1 中的「許可清單模式」或「黑名單模式」變更而來的。
5. 在「應用程式檔案清單」的「檔案指紋清單」下，新增或移除檔案指紋清單。
若要新增清單，該清單必須在 Symantec Endpoint Protection Manager 中可供使用。請參閱：
[在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單](#)
6. 若要新增應用程式名稱清單，請在「應用程式檔案清單」的「檔案名稱」下，按下「匯入」。
指定要匯入的應用程式名稱清單，然後按下「匯入」。清單中的應用程式以個別項目的形式出現在系統鎖定架構中。
應用程式名稱清單必須是指定檔案名稱、測試模式和比對模式的文字檔案。請參閱：
[建立應用程式名稱清單以匯入系統鎖定架構中](#)

7. 若要新增個別應用程式，請在「應用程式檔案清單」的「檔案名稱」下，按下「新增」。
8. 在「新增檔案定義」對話方塊中，指定檔案 (.exe 或 .dll) 的完整路徑名稱。
可以使用標準字串或規則運算式語法來指定名稱。名稱可以包括萬用字元 (* 代表任意字元，? 代表單一字元)。名稱也可以包括環境變數，例如 %ProgramFiles% 代表程式檔案目錄的位置，而 %windir% 代表 Windows 安裝目錄的位置。
9. 預設會保持選取「使用萬用字元比對 (支援 * 和 ?)」，如果檔案名稱使用了規則運算式，則按下「使用規則運算式比對」。
10. 如果您只想在該檔案在特定磁碟機類型上執行時允許它，請按下「僅比對下列磁碟機類型內的檔案」。
取消選取不要包含的磁碟機類型。根據預設會選取所有磁碟機類型。
11. 如果您希望依照裝置 ID 類型進行比對，請選取「僅比對下列裝置 ID 類型的檔案」，然後按下「選取」。
12. 在清單中按下需要的裝置，然後按下「確定」。
13. 按下「確定」開始測試。

一段時間後，便可以檢視未核准的應用程式清單。如果重新開啟「用於 群組名稱 的系統鎖定」對話方塊，可以查看測試的執行時間。

檢視測試已記錄但沒有攔截的未核准的應用程式

1. 在「用於 群組名稱 的系統鎖定」對話方塊中，按一下「檢視未核准的應用程式」。
2. 在「未核准的應用程式」對話方塊中，檢視應用程式。
這個清單包含應用程式執行的時間、電腦的主機名稱、用戶端的使用者名稱，以及執行檔檔名等資訊。
3. 決定要處理未核准應用程式的方式。
若是允許模式，則可以將要允許的應用程式名稱新增至核准的應用程式清單。若是拒絕模式，則可以移除要允許的應用程式的名稱。
4. 如果變更了檔案指紋清單或個別應用程式，並且想要重新執行測試，請在「未核准的應用程式」對話方塊中，按下「重設測試」。否則，按下「關閉」。
5. 完成測試後，便可以啟用系統鎖定。

更多資訊

設定系統鎖定

使用「裝置控制」和「應用程式控制」封鎖或允許裝置

本主題介紹如何使用 Symantec Endpoint Protection 裝置控制政策和應用程式控制政策，允許或封鎖用戶端電腦上的硬體裝置。

- [裝置控制的運作方式](#)
- [裝置類別和 GUID \(類別 ID\) 和裝置 ID](#)
- [透過 Symantec DevViewer 尋找 GUID 和裝置 ID](#)
- [將 GUID 和裝置 ID 新增至規則的最佳做法](#)
- [裝置控制中自動允許的 Windows 裝置](#)
- [裝置控制中自動排除的 Windows 裝置](#)
- [設定裝置控制政策](#)

另請參閱：「[應用程式控制](#)」如何封鎖設備

裝置控制的運作方式

Symantec Endpoint Protection 透過裝置控制政策規則封鎖和允許硬體裝置。

- 封鎖裝置的裝置控制在 Windows 裝置管理員上停用該裝置。已停用的裝置無法在 Symantec Endpoint Protection 用戶端電腦上的運作。

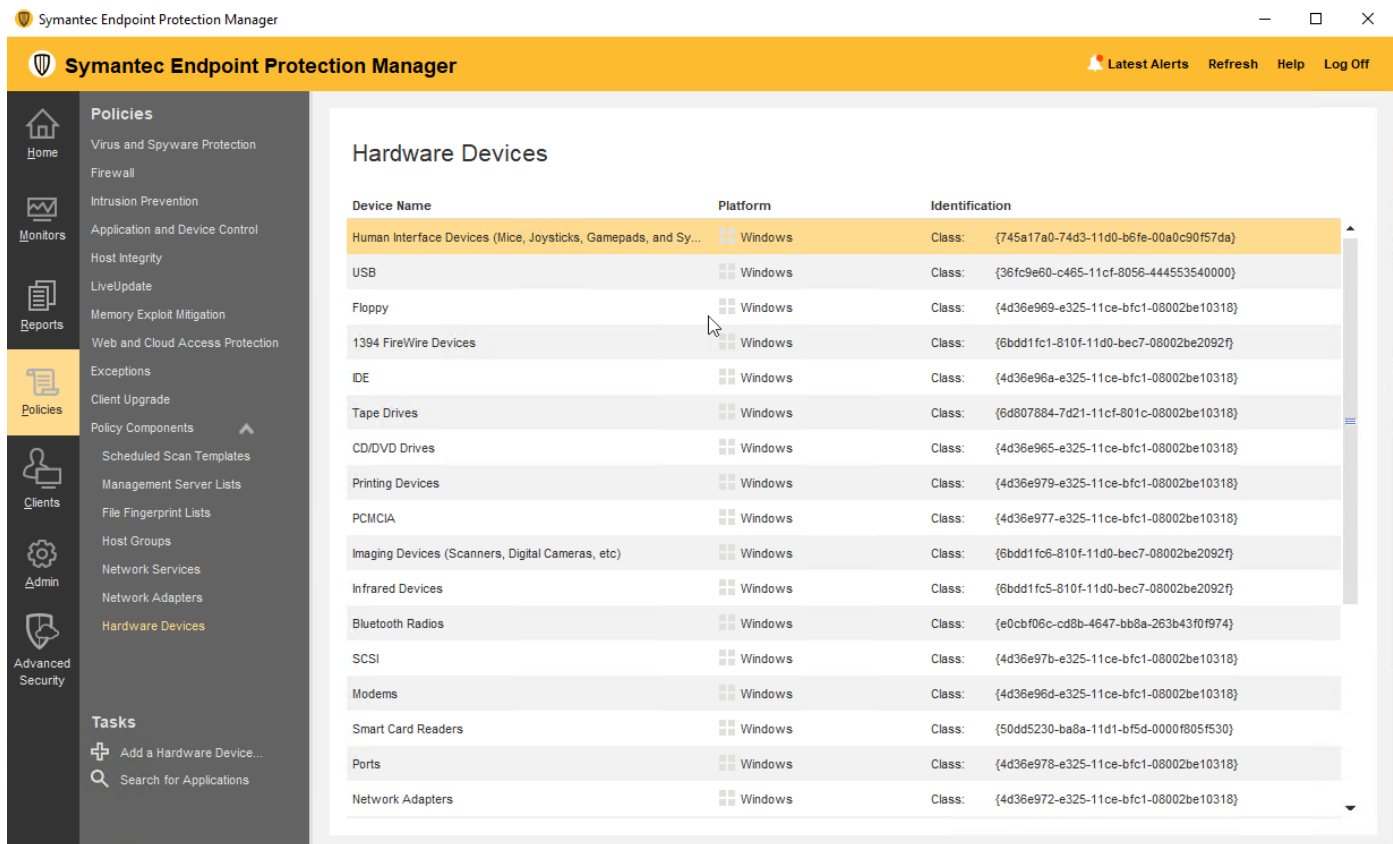
NOTE

當裝置控制透過裝置 ID 封鎖用戶端使用者 (如 Android、iPhone 和其他可攜式裝置) 時，用戶端使用者無法為裝置充電。

- 允許裝置的裝置控制在用戶端電腦上啟用裝置。

裝置控制透過 GUID (類別 ID) 或裝置 ID 來標識要封鎖或允許的硬體裝置。

Symantec Endpoint Protection Manager 在「硬體裝置」清單中包含一個內建 GUID 清單和一些裝置 ID。您可以新增更多在用戶端電腦上執行的 GUID (針對裝置類別) 和裝置 ID (針對單一裝置)。



The screenshot shows the Symantec Endpoint Protection Manager web interface. The left sidebar contains navigation links for Home, Monitors, Reports, Policies, Clients, Admin, and Advanced Security. The Policies section is expanded, showing various protection settings. The main content area displays the 'Hardware Devices' list, which includes columns for Device Name, Platform, and Identification. The list contains various hardware categories like Human Interface Devices, USB, Floppy, 1394 FireWire Devices, IDE, Tape Drives, CD/DVD Drives, Printing Devices, PCMCIA, Imaging Devices, Infrared Devices, Bluetooth Radios, SCSI, Modems, Smart Card Readers, Ports, and Network Adapters. Each entry shows its platform (all are Windows) and its class GUID.

Device Name	Platform	Identification
Human Interface Devices (Mice, Joysticks, Gamepads, and Sy...	Windows	Class: {745a17a0-74d3-11d0-b6fe-00a0c90f57da}
USB	Windows	Class: {36fc9e60-c465-11cf-8056-444553540000}
Floppy	Windows	Class: {4d36e969-e325-11ce-bfc1-08002be10318}
1394 FireWire Devices	Windows	Class: {6bdd1fc1-810f-11d0-bec7-08002be2092f}
IDE	Windows	Class: {4d36e96a-e325-11ce-bfc1-08002be10318}
Tape Drives	Windows	Class: {6d807884-7d21-11cf-801c-08002be10318}
CD/DVD Drives	Windows	Class: {4d36e965-e325-11ce-bfc1-08002be10318}
Printing Devices	Windows	Class: {4d36e979-e325-11ce-bfc1-08002be10318}
PCMCIA	Windows	Class: {4d36e977-e325-11ce-bfc1-08002be10318}
Imaging Devices (Scanners, Digital Cameras, etc)	Windows	Class: {6bdd1fc6-810f-11d0-bec7-08002be2092f}
Infrared Devices	Windows	Class: {6bdd1fc5-810f-11d0-bec7-08002be2092f}
Bluetooth Radios	Windows	Class: {e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
SCSI	Windows	Class: {4d36e97b-e325-11ce-bfc1-08002be10318}
Modems	Windows	Class: {4d36e96d-e325-11ce-bfc1-08002be10318}
Smart Card Readers	Windows	Class: {50dd5230-ba8a-11d1-bf5d-0000f805f530}
Ports	Windows	Class: {4d36e978-e325-11ce-bfc1-08002be10318}
Network Adapters	Windows	Class: {4d36e972-e325-11ce-bfc1-08002be10318}

然後將這些裝置 ID 新增到封鎖或允許 (排除) 這些受支援裝置的裝置控制政策。

Application and Device Control Policy

Overview

Application Control

Windows Settings

Device Control

Mac Settings

Device Control

Windows Device Control

Hardware Device Control Lists

Devices a client computer is blocked from accessing, such as USB drives, Bluetooth devices, printers, and serial and parallel ports.

Blocked Devices

Use this pane to manage the list of devices to which you want to block access.

Device Name	Identification
USB Hub	Device: USB\VID_0BDA&PID_5413\B&857A6CF&0&3

Add...

Delete

Devices Excluded From Blocking

Use this pane to manage the list of devices to which you want to allow access.

Device Name	Identification
Infrared Devices	Class: {6bdd1fc5-810f-11d0-bec7-08002be2092f}

將政策套用至用戶端群組之後，裝置控制將監控用戶端電腦發出的裝置變更訊息。每次出現訊息時 (例如，當用戶端使用者插入 USB 裝置)，SEP 都會計算電腦上的所有裝置。SEP 會根據適用於與該裝置關聯的裝置類別清單規則檢查每台裝置。

根據規則條件類型，Symantec Endpoint Protection 用戶端會以兩種不同方式檢查 GUID 或裝置 ID：

- 如果裝置控制政策指定 GUID，Symantec Endpoint Protection 用戶端將執行直接字串比較。
- 如果裝置控制政策指定裝置 ID，Symantec Endpoint Protection 用戶端將執行規則運算式比對。如果條件相符，SEP 將根據規則動作啟用或停用裝置。啟用或停用裝置的動作類似於使用者在 Windows 裝置管理員中執行相同動作的方式。

裝置類別和 GUID (類別 ID)

Windows 會將硬體裝置分類到裝置階層中，每個階層可以有相同分類的裝置，稱為裝置類別。Windows 會為每個裝置類別分配一個裝置 GUID，這是一個不重複的標識符。

例如：

- 磁碟機 - {4d36e967-e325-11ce-bfc1-08002be10318}
- 儲存磁碟區 - {71a27cdd-812a-11d0-bec7-08002be2092f}
- USB 裝置 - {36FC9E60-C465-11CF-8056-444553540000}

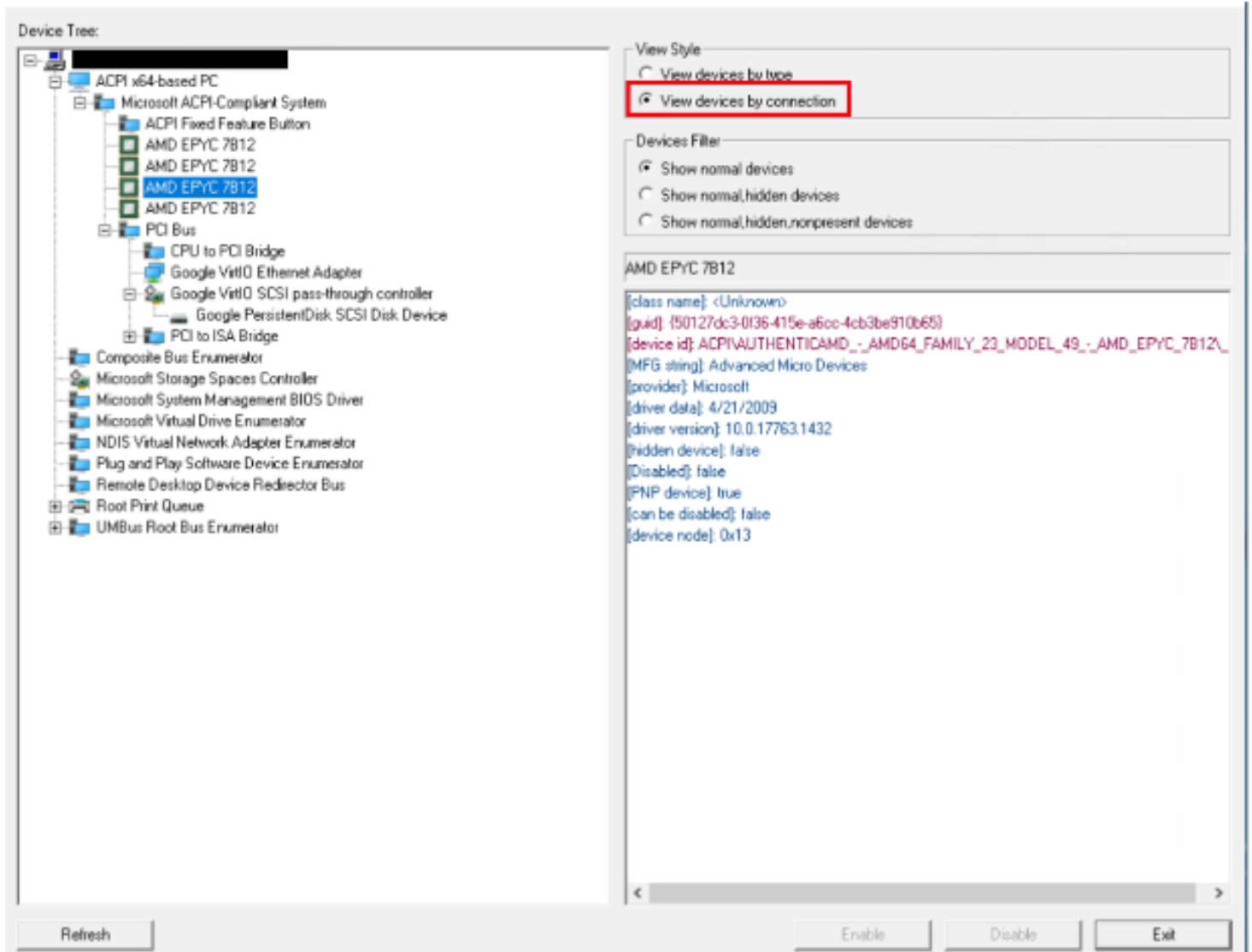
如需詳細瞭解類別 ID 清單，請參閱：[供應商可用的系統定義的裝置設定類別](#)

瞭解邏輯裝置類別

Windows 裝置階層包括應用於多種裝置的邏輯裝置類別。這些裝置類別可以包括多個不同類型的實體裝置類別，如 USB 裝置類別。多種類別可能導致套用於特定實體裝置的政策規則意外重複。

邏輯裝置類別的另一個範例是儲存磁碟區，它不對應特定的實體裝置類型。實體硬碟 / USB 磁碟 / 其他儲存裝置連接到系統並分配分區 (邏輯磁碟機代號) 之後，Windows 會建立磁碟區裝置類別。

以下 Symantec DevViewer 圖片顯示不同裝置之間的關係。在本範例中，DevViewer 會顯示 SanDisk Cruzer 裝置階層，其中既有系統建立的 USB 大容量磁碟機，也有一般儲存磁碟區裝置類別。將顯示從「按連接查看裝置」切換到「按類型查看裝置」時，這些磁碟和磁碟區裝置會顯示在「磁碟機」和「儲存磁碟區」下。



瞭解裝置階層和邏輯裝置可協助您設定裝置控制政策，確保政策按照預期執行。例如，封鎖磁碟機的規則會封鎖所有實體磁碟，包括內部和外部 USB 磁碟。同理，封鎖儲存磁碟區的規則不論基礎儲存的類型，會封鎖所有邏輯分區。

當裝置控制封鎖 Windows 裝置階層中任何父節點上的裝置時，即會阻止子節點上的所有裝置。如果父節點允許該裝置，則子節點上所有裝置也受允許。

裝置 ID

裝置 ID (在 Windows 中也稱為裝置執行個體 ID) 是 Windows 為每個裝置提供的特定 ID。裝置 ID 通常包含一個類型字串前綴 (如 `IDE\CDROM`)，後跟描述特定裝置模型的字串。例如，裝置 ID 的兩個常見格式包括：

- `<class>\<type>&<vendor>&<model>&<revision>\<serial number>`
- `<class>\<type><vendor><model><revision>\<serial number>`

透過 Symantec DevViewer 尋找 GUID 和裝置 ID

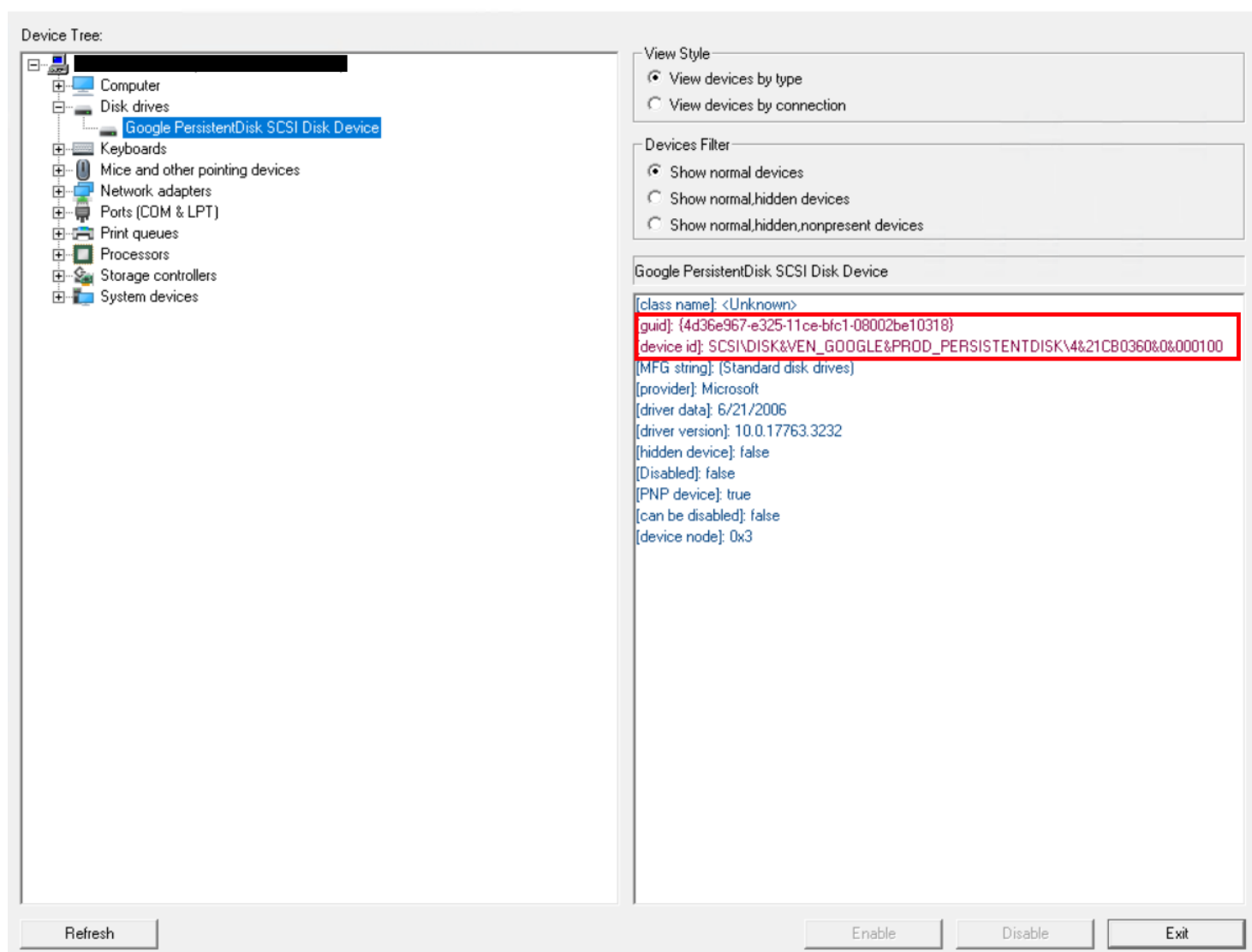
您可以使用 Symantec DevViewer 或 Windows 裝置管理員查看 Windows 裝置階層。這兩個工具都顯示連接到每台用戶端電腦的實際硬體裝置。

您可以使用任一工具查找和複製裝置的 GUID 或裝置 ID，然後貼到裝置控制政策中。

但 Symantec 建議您使用 DevViewer，因為使用者介面的目的是更直接地顯示所有必要裝置屬性。

DevViewer 會按照類型或連接顯示裝置。

下圖顯示 DevViewer 介面。在裝置屬性視窗中，請複製類別 ID [guid] 或裝置 ID [device id] 欄位，並貼到裝置控制政策中。裝置控制政策會使用這些屬性來定義與用戶端相符的 Symantec Endpoint Protection 規則。



[更多資訊](#)

如需詳細瞭解 DevViewer 下載資訊，請參閱：[使用 DevViewer 查找 Endpoint Protection / Endpoint Security 中裝置封鎖的硬體裝置 ID](#)

將 GUID 和裝置 ID 新增至裝置控制規則的最佳做法

請使用以下資訊，將規則新增到裝置控制政策：

- **GUID** (裝置類別 ID) 會啟用或停用整個裝置類別。例如，如果在封鎖規則中指定了 USB 類別 GUID，則所有 USB 裝置連接到 USB 通訊埠時都會被停用。此裝置類別在階層中執行，因為會封鎖不同類型的實體裝置 (如相機、滑鼠和儲存裝置)。SEP 裝置控制可以決定套用於每個實體裝置的裝置類別 GUID 清單。
- **裝置 ID** 會根據規則動作啟用或停用特定裝置。例如，如果在封鎖規則中新增 **ID\CDROM***，則將裝置控制政策套用於群組時，會停用直接連接到主機板的所有 CD/DVD 磁碟機。

通常 Symantec 會建議您使用裝置 ID 而非 GUID，因為裝置 ID：

- 更加明確。
- 可以更有效封鎖或允許裝置，因為裝置 ID 是串聯特定裝置相關資料清單而生的。裝置 ID 通常採用更容易讀取的格式。
- 最不可能出現意外的裝置控制政策規則行為，因為這些規則與特定實體裝置的關聯度最高。

裝置 ID 中的萬用字元

將裝置 ID 新增到硬體裝置清單時，Symantec 支援 * 和 ? 萬用字元。

- 使用 * 表示零個或多個任意字元。
- 使用 ? 表示任意值的單一字元。

下表說明如何在裝置控制政策中針對裝置 ID 使用萬用字元。

Table 107: 如何在裝置 ID 中使用萬用字元

裝置類型	萬用字元
任何 USB 儲存裝置	USBSTOR*
任何 USB 磁碟	USBSTOR\DISK*
任何 USB SanDisk 磁碟	USBSTOR\DISK&VEN_SANDISK*
任何 USB SanDisk Micro Cruzer 磁碟	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO*
特定 SanDisk 裝置	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033 \0002071406&0

NOTE

將萬用字元新增到裝置控制政策時，SEP 不支援 GUID 中的萬用字元。

裝置控制中自動允許的 Windows 裝置

為了防止政策配置導致硬體無法使用，並節省手動新增裝置類別的時間，SEPM 包括內建一般已知類別 ID 的清單。如果建立規則來封鎖這些裝置，則 Symantec Endpoint Protection 用戶端將忽略該規則並允許這些裝置。

例如：

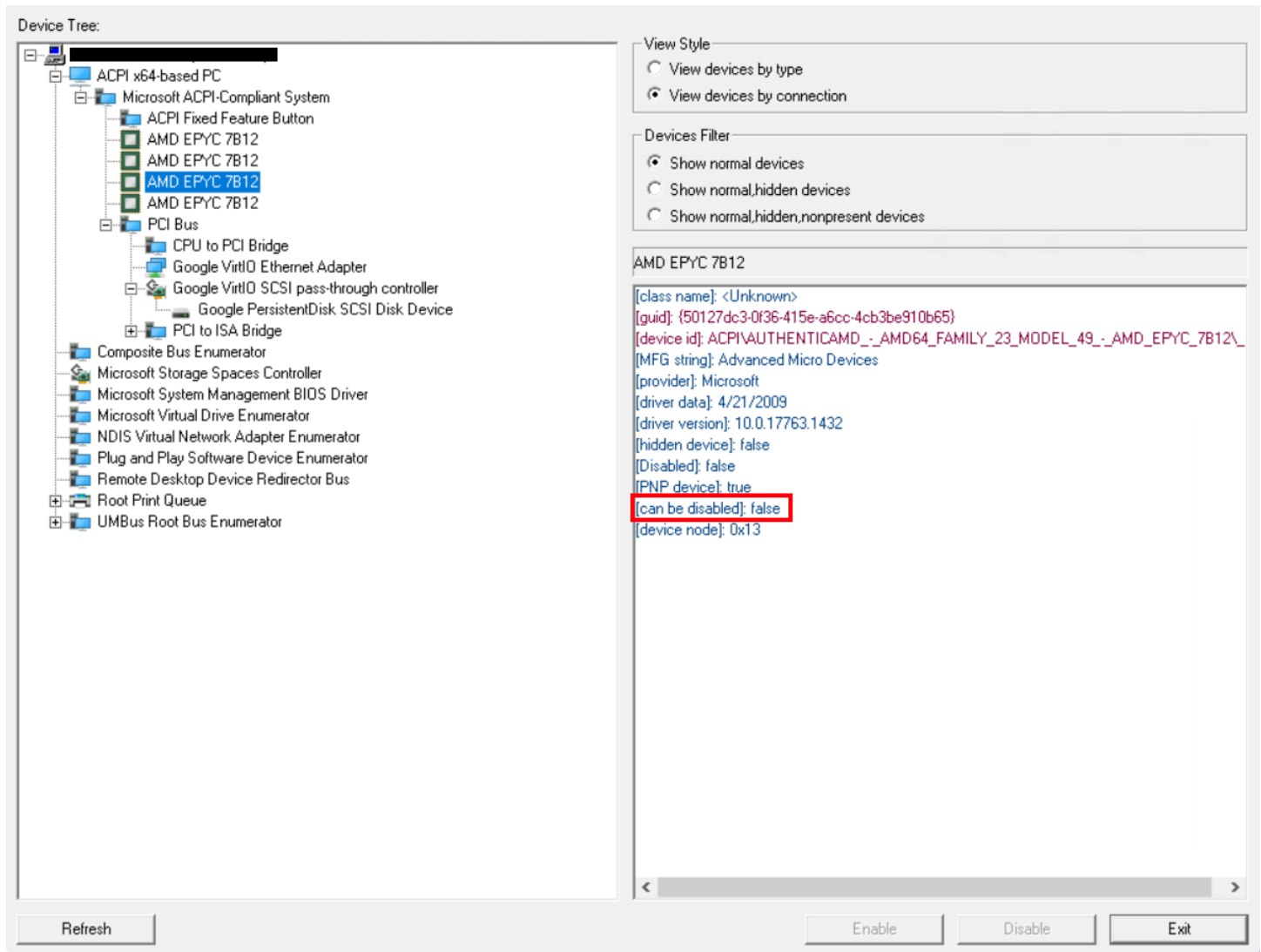
- **USB/PCMCIA/FireWire (1394) 控制器：**
封鎖這些裝置可能導致意外行為，因為控制器和任何連接的裝置都會受到影響。建立針對控制器支援的裝置和裝置類別的政策。
- **包含系統 OS 或頁面檔案的磁碟和磁碟區：**
封鎖這些裝置可能導致不可復原的系統錯誤 (BSOD)。SEP 不會停用這些裝置，但您可以使用裝置控制政策封鎖其他磁碟和磁碟區。

裝置控制中自動排除的 Windows 裝置

建立允許裝置的規則時，您可以排除該裝置以免遭封鎖。在以下情況，您必須允許部分裝置：

- 部分 Windows 系統關鍵裝置永遠無法停用。例如，Windows 不允許裝置控制停用 CPU 裝置。
- 您需要封鎖一個裝置之外的所有裝置，例如 USB 儲存裝置。不論實際的裝置類別項目是什麼，排除都優先於封鎖。

下圖顯示 DevViewer 屬性視窗中的 [Can be disabled]: false 欄位。Symantec Endpoint Protection 用戶端在停用裝置之前確認此狀態為 true。用戶端不能在狀態為 false 的裝置上執行。



若要允許裝置，請將其新增到裝置控制政策的「從封鎖排除的裝置」部分。

設定裝置控制政策

請使用 DevViewer 尋找 GUID 和裝置 ID，然後將 GUID 和裝置 ID 複製貼上到裝置控制政策的「硬體裝置」清單。

設定裝置控制政策

1. 在用戶端電腦[下載](#)並開啟 DevViewer。
2. 針對要封鎖或允許的每個裝置或裝置類別，請從 DevViewer [複製 GUID 或裝置 ID](#)。
3. 將 GUID 和裝置 ID 新增到「Symantec Endpoint Protection Manager 硬體裝置」清單。

請參閱：[新增硬體裝置至硬體裝置清單中](#)

4. 將 GUID 和裝置 ID 新增到裝置控制政策。

請參閱：[新增「裝置控制」政策規則，以允許或封鎖用戶端電腦上的裝置](#)

如需詳細瞭解如何從 Mac 取得 GUID 和裝置 ID，請參閱：[使用 DeviceInfo 取得 Mac 裝置的裝置廠商、型號或序號](#)

新增「裝置控制」政策規則，以允許或封鎖用戶端電腦上的裝置

您可以使用「應用程式與裝置控制」政策來架構裝置控制。開始之前，將您需要的任何裝置新增至「硬體裝置」清單。請參閱：

[新增硬體裝置至硬體裝置清單中](#)

為 Windows 用戶端新增裝置控制規則

1. 在主控台中開啟「應用程式與裝置控制」政策。
2. 按下「裝置控制」。
3. 執行下列其中一項工作：
 - 如果要封鎖裝置，請在「封鎖的裝置」下，按下「新增」。
 - 如果要允許裝置，請在「不封鎖的裝置」下，按下「新增」。
4. 在「裝置選取」視窗中，選取一個或多個裝置，然後按下「確認」。
如有必要，請確定是否攔截特定的通訊埠，就會排除裝置。

NOTE

通常，絕不應該攔截鍵盤。

5. 如果您希望通知使用者，請勾選「當裝置被攔截時通知使用者」。
6. 按一下「確定」。

為 Mac 用戶端新增裝置控制規則

1. 在主控台中開啟「應用程式與裝置控制」政策。
2. 在「Mac 設定」下方，按下「裝置控制」。
3. 在「攔截的裝置」下，按下「新增」。
4. 在「裝置選取」視窗中，從清單中選取裝置。您一次僅可以新增一個裝置。
若視窗底部的欄位可用，請填寫。如果您將這些欄位保留為空白，此類型的所有裝置都將被攔截。
您也可使用規則運算式來定義裝置廠商、裝置型號或序號。如需詳細資訊，請參閱「Mac 裝置控制」視窗中的說明。
若要從 Mac 的連線裝置取得序號、型號或廠商名稱，請使用安裝檔案中的 DeviceInfo 工具。您可在 Tools/
DeviceInfo 下找到此工具及其指示。
5. 按下「確定」。
6. 在「不攔截的裝置」下，按下「新增」。
7. 在「裝置選取」視窗中，從清單中選取裝置，定義已排除的裝置，然後按下「確定」。
8. 如果您希望通知使用者，請勾選「當裝置被攔截時通知使用者」。
9. 按下「確定」。

更多資訊

- [Mac 裝置控制](#)
- [管理裝置控制](#)
- [關於應用程式控制、系統鎖定和裝置控制](#)

新增硬體裝置至硬體裝置清單中

在取得硬體裝置的 GUID 或裝置 ID 後，您可以將硬體裝置新增至預設「硬體裝置」清單。您接著可以從「應用程式與裝置控制」政策的裝置控制部分存取此預設清單。

如需詳細瞭解 GUID 和裝置 ID，請參閱：[使用「裝置控制」和「應用程式控制」封鎖或允許裝置](#)

新增硬體裝置至硬體裝置清單中

1. 在主控台中，按下「政策」。
2. 在「政策」下方，展開「政策元件」，然後按下「硬體裝置」。
3. 在「工作」下方，按下「新增硬體裝置」。
4. 輸入要新增裝置的名稱。
類別 ID 和裝置 ID 依慣例會用大括號 ({}) 括住。您可能需要將大括號取代為萬用字元 ?。
5. 選取 [類別 ID] 或 [裝置 ID]，然後貼上從「Windows 裝置管理員」或 DevViewer 工具複製的 ID。
6. 您可以使用萬用字元來定義一組裝置 ID。例如，您可以使用下列字串：*IDE\DVDROM*。

如需詳細資訊，請參閱：

[使用 DevViewer 取得 Windows 電腦的裝置廠商或型號](#)

7. 按下「確定」。

使用 DevViewer 取得 Windows 電腦的裝置廠商或型號

您可以使用 Symantec DevViewer 工具或 Microsoft Windows 裝置管理員取得類別 ID (GUID) 或裝置 ID。

取得裝置 ID 後，您可在「裝置控制」政策中使用萬用字元進行修改，標示為非專屬的裝置群組。

使用 Symantec DevViewer 工具取得類別 ID 或裝置 ID

1. 將 DevViewer 從下列位置的「附件」區段下載到用戶端電腦：
[使用 DevViewer 在 Endpoint Protection 中尋找進行裝置攔截的硬體裝置 ID](#)
2. 在用戶端電腦上，執行 DevViewer.exe。
3. 展開裝置樹狀結構，然後找到需要裝置 ID 或 GUID 的裝置。
例如，展開「磁碟機」，然後選取該類別中的裝置。
4. 在右窗格中，在 [guid] (或 [## ID]) 上按下滑鼠右鍵，然後按下「複製 GUID」或「複製裝置 ID」。
5. 按下「結束」。
6. 在管理伺服器上，將 GUID 或裝置 ID 貼到「政策元件 > 硬體裝置」清單中。

從 Microsoft Windows 裝置管理員取得裝置 ID

1. 在控制面板中，搜尋「裝置管理員」。
2. 在「裝置管理員」對話方塊中，展開裝置類別，然後按一下「屬性」。
3. 在該裝置的「屬性」對話方塊中，從「詳細資訊」標籤選取「類別 GUID」或「硬體 ID」。
4. 複製字串。
5. 按一下「確定」。

更多資訊

- [使用「裝置控制」和「應用程式控制」封鎖或允許裝置](#)
- [新增「裝置控制」政策規則，以允許或封鎖用戶端電腦上的裝置](#)
- [新增硬體裝置至硬體裝置清單中](#)

Endpoint Protection 中的 Mac 裝置控制

您可以針對各類型的政策建立硬體裝置控制清單。此清單包含攔截的裝置清單及不攔截的裝置清單。

硬體裝置控制出現在檔案系統層級。因此，使用者可能仍然能夠在遭攔截裝置或唯讀裝置上使用 Disk Utility 或 Terminal 指令執行磁碟區層級工作。這些工作包括消除、退出或建立遭攔截裝置的光碟影像。

此清單不會顯示所有允許的裝置。此清單只顯示「攔截的裝置」清單例外的裝置。

您應先測試您在小型測試群組上所建立的所有裝置控制條件，然後再將政策套用至所有 Mac 用戶端。測試可確保裝置控制政策能如預期般攔截裝置及不攔截裝置。

NOTE

當依廠商或裝置 ID 攔截時，請注意。賽門鐵克建議您不要選取在尋找程式中可能顯示的非儲存裝置作為要攔截的裝置。

您可以使用「伺服器控制」或「混合控制」模式架構用戶端使用者介面控制設定，以防止使用者啟用或停用裝置控制。

如需詳細資訊，請參閱：

防止使用者在用戶端電腦上停用防護

廠商、型號和序號欄位不區分大小寫。對於每個指定的裝置，如果您將廠商、型號或序號欄位保留為空白，則政策會攔截任何符合裝置類型的裝置。如果您確實為這些欄位指定了值，請為每個欄位僅鍵入一個值 (例如，供應商欄位中的一個供應商名稱、模型欄位中的一個模型編號以及編號欄位中的一個序號)。

裝置控制規則條件的優先權高於最具體的準則。例如，完整文字字串的優先權最高，具有萬用字元的部分文字字串較低，僅有萬用字元的字串最低。欄位空白類似於萬用字元搜尋，其所佔權數少於完整文字字串或部分文字字串。同樣地，序號的優先權高於型號名稱，而型號名稱的優先權高於廠商名稱。廠商名稱的完整字串文字的優先權高於序號的部分字串文字。

Mac 裝置控制條件的權數如下所列 (從最高權數至最低權數)：

- 完整字串文字，序號
- 完整字串文字，型號名稱
- 完整字串文字，廠商名稱
- 具有萬用字元的部分字串文字，序號
- 具有萬用字元的部分字串文字，型號名稱
- 具有萬用字元的部分字串文字，廠商名稱
- 僅萬用字元，序號
- 僅萬用字元，型號名稱
- 僅萬用字元，廠商名稱
- 空白欄位 (尚未定義)

若要從 Mac 的連線裝置取得序號、型號或廠商名稱，請使用安裝檔案中的 DeviceInfo 工具。您可在 Tools/DeviceInfo 下找到此工具及其指示。

下表列出可供 Mac 裝置使用的裝置攔截選項。

Table 108: Mac 裝置攔截選項

群組或選項	說明
裝置名稱	已攔截或不攔截的裝置名稱。您可以從此清單新增或刪除裝置。 Mac 支援的裝置類型為： - Thunderbolt 裝置 - CD/DVD 磁碟機 - USB 裝置 - FireWire 裝置 - 安全數位 (SD) 卡
裝置廠商	已攔截或不攔截之裝置的供應商。 您可以依特定供應商名稱來攔截或不攔截所有裝置類型 (Thunderbolt 除外)。 您可以使用規則運算式來定義供應商名稱。請參閱： 用於攔截 Mac 之裝置的規則運算式
裝置型號	已攔截或不攔截之裝置的型號。 您可以依特定型號來攔截或不攔截所有裝置類型。 您可以使用規則運算式來定義型號名稱。請參閱： 用於攔截 Mac 之裝置的規則運算式
序號	已攔截或不攔截之裝置的序號。 您只能攔截或不攔截 Thunderbolt 和 USB 裝置的特定序號。 您可以使用規則運算式來定義序號。請參閱： 用於攔截 Mac 之裝置的規則運算式
記錄偵測到的裝置	每當「裝置控制」偵測到裝置時，即新增項目至裝置控制日誌。此選項預設為啟用。
當裝置被攔截或取消攔截時通知使用者	當攔截的裝置連線或啟動時，傳送通知至用戶端電腦。此選項預設為停用。

下表說明您可用來定義裝置控制準則的規則運算式。

Table 109: 用於攔截 Mac 之裝置的規則運算式

選項	說明
. (點)	比對新行以外的任何字元。 例如，So*.* 會比對 "So"、"Soo"、"Sooo"、"Sobar"、"Sooxxx"。
\ (反斜線)	比對隨後的字元。 反斜線會逸出所有其他中繼字元及本身。在字集中使用反斜線時，它會被視為一般字元。 如果是二進位比對，請使用 \x。例如，\xA0 會比對二進位 a0 十六進位值。
[set]、[^Set] (字集)	比對字集中的一個字元。 如果字集中的第一個字元是 carat (^)，則字集會嘗試比對不在字集中的任何字元。特殊字元右括號 () 和連字號 (-) 若作為字集中的第一個字元，並無特殊意義。 字集也可以比對一個範圍或多個字元。例如，S-E 會指定 S 到 E (含) 的一組字元。 例如，[a-z] 會比對任何字母字元，而 [^]-] 則會比對除]、\ 和 - 以外的任何字元。
* (星形或星號)	任何結尾為星號 (*) 的舊規則運算式形式都會比對該形式的零或多個相符項目。 例如，Soo* 會比對 "Soo\","Soo\\"、"Soo\\" 和 "Soo\\12"。
+ (加號)	任何結尾為加號 (+) 的舊規則運算式形式都會比對該形式的一或多個相符項目。 例如，Soo\+ 會比對 "Soo\","Soo\\" 和 "Soo\\"，但是它不比對 "Soo\\12"。

使用 DeviceInfo 取得 Mac 裝置的裝置廠商、型號或序號

您可以使用 DeviceInfo 工具在 Mac 用戶端上取得特定裝置的裝置廠商、型號或序號，以便在「裝置控制」政策中使用。

NOTE

此工具僅適用於識別掛載裝置的此資訊。此工具無法辨識非掛載裝置。

使用 DeviceInfo 取得 Mac 裝置的裝置廠商、型號或序號

1. 在安裝檔案中，找到 \Tools\DeviceInfo 資料夾，然後將該資料夾複製到 Mac 用戶端電腦的桌面上。
2. 在 Mac 用戶端電腦上，確保您要取得其資訊的裝置已連線，然後開啟終端應用程式。
3. 若要導航至工具資料夾，請輸入下列命令：

```
cd ~/Desktop/DeviceInfo/
```

4. 若要取得裝置資訊，請輸入下列命令：

```
./DeviceInfo
```

5. 記錄結果中的相關資訊，以便用於 Mac 裝置控制政策。

「應用程式控制」如何封鎖設備

「應用程式控制」會封鎖或允許裝置上的讀取、寫入或執行指令，更精準地封鎖設備。「應用程式控制」也會控制哪些應用程式可以使用。

例如，政策可以封鎖從 USB 磁碟機執行的任何程式，這些程式可能會變更登錄檔或修改主機上的檔案。

透過「應用程式控制」，您可以使用裝置 ID，但不能使用 GUID。

您可以在以下規則條件中使用裝置 ID：

- 應用程式規則程序
- 啟動程序嘗試
- 終止程序嘗試
- 檔案和資料夾存取嘗試
- 載入 DLL 嘗試

「應用程式控制」只會封鎖裝置階層中最後一個節點裝置，除非最後一個節點是一般磁碟區或儲存磁碟區。在這兩種情況下，作為最後一個節點之父節點的裝置會被封鎖。

「應用程式控制」支援的大多數裝置 ID 都為以下類型之一：

裝置類型	範例
USBSTOR	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0
FCD	FDC\GENERIC_FLOPPY_DRIVE\4&371082C9&0&0
DE	IDE\DISKHTS541060G9SA00_____MB3IC60H\4&14AA9DA8&0&0.0.0
SCSI	SCSI\DISK&VEN_WDC_WD50&PROD_00KS-00MNB0&REV_700\4&1291CDED&0&000

NOTE

「應用程式控制」只能阻止 Windows 視為磁碟機且具有與之關聯的磁碟機代號的裝置。沒有新增磁碟機代碼的裝置 (例如：iPhone 或 iPad) 必須透過「設備控制」封鎖。請參閱：

[在 Symantec Endpoint Protection Manager 中封鎖 USB 裝置 \(不包括滑鼠和鍵盤\)。](#)

如需詳細瞭解 GUID 和裝置 ID，請參閱：[使用「裝置控制」和「應用程式控制」封鎖或允許裝置](#)

將例外套用於 Symantec Endpoint Protection 中的掃描

您可以在 Symantec Endpoint Protection 主控台中管理 Symantec Endpoint Protection Manager 的例外。

Table 110: 管理例外

工作	說明
了解例外	使用例外可將項目排除在用戶端電腦上的掃描範圍之外。
檢視 Symantec Endpoint Protection 自動排除掃描的檔案和資料夾類型	Symantec Endpoint Protection 會針對某些第三方應用程式和賽門鐵克的某些產品自動建立例外或排除項。 您也可以架構個別的掃描，以便僅掃描特定副檔名並略過任何其他副檔名。請參閱： 關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾
建立掃描例外	可以直接在「例外」政策中新增例外，也可以從「監視器」頁面上的日誌事件新增例外。請參閱： 建立病毒和間諜軟體掃描的例外 從日誌事件建立例外
限制使用者可在用戶端電腦上架構的例外類型 (僅限 Windows)	根據預設，用戶端電腦上的使用者具有有限的例外架構權限。您可以進一步限制使用者，以免其針對病毒和間諜軟體掃描或行為分析建立例外。 使用者永遠無法強制執行應用程式偵測，也永遠沒有建立「竄改防護」例外的權限。 用戶端使用者建立的例外 (稱為使用者定義例外)，不會上傳至管理伺服器。 使用者也無法建立應用程式控制的檔案例外。請參閱： 限制使用者可在用戶端電腦上架構的例外類型
查看日誌，是否有可能要為其建立例外的偵測。	在 Symantec Endpoint Protection 執行偵測後，您可以從日誌事件建立偵測的例外。 例如，您可能希望針對掃描會偵測，但使用者要求下載的檔案建立例外。請參閱： 從日誌事件建立例外
建立入侵預防特徵的例外	您可以指定入侵預防的例外。 您還可以針對入侵預防設定排除主機清單。 入侵預防例外會在「入侵預防」政策中架構。請參閱： 為 IPS 特徵建立例外

針對哪種類型的掃描使用哪些 Windows 例外？

下表列出針對哪些類型的掃描使用例外政策中的哪些例外類型。

Table 111: 例外名稱

Symantec Endpoint Protection Manager	用戶端限制 (位於 Symantec Endpoint Protection Manager)*	Windows 用戶端	例外適用功能
應用程式	應用程式例外	應用程式例外	- 自動防護 - 手動掃描 - 排程掃描 - 下載鑑識 - 行為分析
要監控的應用程式	無法使用	無法使用	應用程式控制
憑證	無法使用	無法使用	- 自動防護 - 手動掃描 - 排程掃描 - 下載鑑識 - 行為分析

Symantec Endpoint Protection Manager	用戶端限制 (位於 Symantec Endpoint Protection Manager)*	Windows 用戶端	例外適用功能
DNS 或主機檔案變更	DNS 或主機檔案變更例外	DNS 或主機檔案變更例外 > 應用程式	行為分析
副檔名	副檔名例外	安全風險例外 > 副檔名	- 自動防護 - 手動掃描 - 排程掃描
檔案	檔案例外	安全風險例外 > 檔案	- 自動防護 - 手動掃描 - 排程掃描 - 行為分析 - 應用程式控制
檔案存取權	檔案存取權		應用程式控制
資料夾	資料夾例外： - 安全風險例外 - SONAR 例外	安全風險例外 > 資料夾 SONAR 例外	- 自動防護 - 手動掃描 - 排程掃描 - 行為分析 - 應用程式控制
已知風險	已知的風險例外	安全風險例外 > 已知風險	- 自動防護 - 手動掃描 - 排程掃描 - 行為分析
信任的 Web 網域	信任的 Web 網域例外	安全風險例外 > Web 網域	下載鑑識
竄改防護例外	無法使用	無法使用	竄改防護所保護的應用程式

*用戶端限制是可以在用戶端上顯示或隱藏以供用戶端使用者新增的例外。在雲端主控台中新增的例外無法在 Symantec Endpoint Protection Manager 中的用戶端上啟用或停用。

請參閱：[限制使用者可在用戶端電腦上架構的例外類型](#)

建立病毒和間諜軟體掃描的例外

可為 Symantec Endpoint Protection 建立不同類型的例外。

您建立的任何例外會優先於使用者可能定義的任何例外。在用戶端電腦上，使用者無法檢視您建立的例外。使用者僅能檢視自己建立的例外。

病毒和間諜軟體掃描的例外也適用於「下載鑑識」。

Table 112: 為 Symantec Endpoint Protection 建立例外

工作	說明
從病毒和間諜軟體掃描中排除檔案	在 Windows 和 Mac 用戶端上支援。 從 Windows 用戶端上的病毒和間諜軟體掃描、行為分析或應用程式控制，依名稱排除檔案。 如需詳細資訊，請參閱： 從掃描中排除檔案或資料夾
從病毒和間諜軟體掃描中排除資料夾	在 Windows、Mac 和 Linux 用戶端上受支援。 從病毒和間諜軟體掃描、行為分析或 Windows 用戶端上的所有掃描中排除資料夾。 在 Windows 和 Linux 用戶端上，您可以選擇將病毒和間諜軟體掃描的例外限制為自動防護或是排程和隨選掃描。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。 如需詳細資訊，請參閱： 從掃描中排除檔案或資料夾
從病毒和間諜軟體掃描中排除已知風險	在 Windows 用戶端上支援。 從病毒和間諜軟體掃描中排除已知風險。掃描會忽略此風險，但是您可以架構例外以便掃描記錄偵測。任何情況下，用戶端軟體都不會在偵測到指定的風險時通知使用者。 如果使用者針對架構為忽略的已知風險架構自訂動作，則 Symantec Endpoint Protection 會忽略自訂動作。 安全風險例外不適用於行為分析。 如需詳細資訊，請參閱： 從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險
從病毒和間諜軟體掃描中排除檔案副檔名	在 Windows 和 Linux 用戶端上支援。 從病毒和間諜軟體掃描中排除任何含指定副檔名的檔案。 副檔名例外不適用於行為分析或 Power Eraser。 如需詳細資訊，請參閱： 從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名
監控應用程式以為應用程式建立例外	在 Windows 用戶端上支援。 使用「要監控的應用程式」例外來監控特定的應用程式。當 Symantec Endpoint Protection 探索到應用程式時，便可以建立例外以指定 Symantec Endpoint Protection 處理應用程式的方式。 如果停用應用程式探索，「要監控的應用程式」例外會針對指定的應用程式強制執行應用程式探索。 如需詳細資訊，請參閱： 建立應用程式例外
指定病毒和間諜軟體掃描如何處理受監控的應用程式	在 Windows 用戶端上支援。 使用應用程式例外以指定套用到受監控的應用程式的 Symantec Endpoint Protection 動作。動作類型決定 Symantec Endpoint Protection 是否在偵測到應用程式或在應用程式執行時套用動作。Symantec Endpoint Protection 在應用程式啟動或執行時，對應用程式套用「終止」、「隔離」或「移除」動作。它在偵測到應用程式時會套用「只記錄」或「忽略」動作。 與檔案名稱例外不同，應用程式例外是一種雜湊型的例外。不同的檔案可以具有相同的名稱，但檔案雜湊會獨特地標識應用程式。 此應用程式例外是 SHA-2 雜湊的例外。 在 Symantec Endpoint Protection 探索到應用程式後，可以為其建立例外的應用程式會出現在「例外」對話方塊中。可以要求 Symantec Endpoint Protection 監控特定的應用程式以進行探索。 如需詳細資訊，請參閱： • 建立應用程式例外 • 啟用應用程式探索

工作	說明
從病毒和間諜軟體掃描中排除 Web 網域	在 Windows 用戶端上支援。 「下載鑑識」會掃描使用者試圖從網站及其他入口網站下載的檔案。「下載智慧型掃描」會作為病毒和間諜軟體掃描的一部分執行。您可以為已知安全性的特定 Web 網域架構例外。您必須啟用「下載智慧型掃描」，例外才會生效。 Note: 如果用戶端電腦使用帶驗證功能的代理，您必須為 Symantec URL 指定信任的 Web 網域例外。這些例外可讓您的用戶端電腦與「賽門鐵克智慧型掃描」和其他重要的賽門鐵克網站進行通訊。 請參閱下列文章： • 如何測試智慧型掃描與賽門鐵克授權伺服器的連線能力 • 允許 Symantec Endpoint Protection 連線至賽門鐵克信譽和授權伺服器所需的代理伺服器排除項 如需詳細資訊，請參閱： 從 Windows 用戶端上的掃描中排除信任的 Web 網域
為竄改防護建立檔案例外	在 Windows 用戶端上支援。 竄改防護可保護用戶端電腦不受竄改賽門鐵克程序和內部物件之程序的攻擊。當竄改防護偵測到一個可能會修改賽門鐵克架構設定或 Windows 登錄值的程序時，就會攔截該程序。一些第三方應用程式會無意地嘗試修改賽門鐵克程序或設定。可能需要允許安全應用程式修改賽門鐵克設定。您可能想要停止用戶端電腦上特定登錄區或特定檔案的竄改防護。 在某些情況下，「竄改防護」可能會攔截螢幕閱讀器或部份其他輔助技術應用程式。可以建立檔案例外，讓應用程式可在用戶端電腦上執行。「竄改防護」不支援資料夾例外。 如需詳細資訊，請參閱： 在 Windows 用戶端上建立竄改防護例外
允許應用程式變更 DNS 或主機檔案	在 Windows 用戶端上支援。 可以建立應用程式例外以變更 DNS 或主機檔案。行為分析通常會防止 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。 如需詳細資訊，請參閱： 針對會變更 DNS 或主機檔案的應用程式建立例外
排除憑證	在 Windows 用戶端上支援。 您可以排除掃描某個憑證。排除憑證可避免其被標示為可疑。例如，下載鑑識掃描可能會將內部工具上的自我簽署憑證標示為可疑。 如需詳細資訊，請參閱： 在 Windows 用戶端上從掃描中排除憑證

更多資訊

- [管理 Symantec Endpoint Protection 中的例外](#)
- [從日誌事件建立例外](#)

從掃描中排除檔案或資料夾

您可以分別為檔案或資料夾新增例外。如果您想建立多個檔案的例外，請重複此程序。

您可以在 Windows 和 Mac 用戶端上架構檔案或資料夾例外，以及在 Linux 用戶端上架構檔案例外。

在 Windows 用戶端上從掃描中排除檔案

1. 在「例外政策」頁面上，按下「例外」。
2. 在「例外」下方，按下「新增 > Windows 例外 > 檔案」。
3. 在「前置變數」下拉式方塊中，選取常用資料夾。
 選取 [NONE] 以輸入絕對路徑與檔案名稱。
 選擇前置字元時，可在不同的 Windows 作業系統使用例外。
4. 在「檔案」文字方塊中，輸入檔案名稱。

若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[NONE]**，請鍵入完整的路徑名稱。

NOTE

路徑必須使用反斜線來表示。

NOTE

Windows 用戶端不支援在例外中使用 UNC 路徑。自動防護會忽略這些例外。隨選掃描、排程掃描和其他防護技術無法可靠地排除這些位置。相反地，您應該將 UNC 位置對應至 Windows 中的磁碟機，而且應該建立對應的磁碟機代號例外，以獲得最佳效能和可靠性。

5. 在「指定將排除此檔案的掃描類型」下方，選取掃描類型（「安全風險」、「**SONAR** 或「應用程式控制」）。您必須選取至少一種類型。
6. 若是安全風險掃描，請在「指定安全風險掃描的類型」下方，選取「自動防護」、「排程和隨選」或「全部掃描」。請參閱說明，以取得為何要將例外限制為特定類型的安全風險掃描的相關資訊。
7. 按下「確定」。

在 **Windows** 用戶端上從掃描中排除資料夾

1. 在「例外政策」頁面上，按下「例外」。
2. 在「例外」下方，按下「新增 > **Windows** 例外 > 資料夾」。
3. 在「前置變數」下拉式方塊中，選取常用資料夾。
選取 **[NONE]** 以輸入絕對路徑與檔案名稱。
選擇前置字元時，可在不同的 Windows 作業系統使用例外。
4. 在「資料夾」文字方塊中，輸入資料夾名稱。
若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[NONE]**，請鍵入完整的路徑名稱。

NOTE

路徑必須使用反斜線來表示。

5. 在「指定排除此資料夾的掃描類型」下方，選取掃描類型（「安全風險」、「**SONAR**」、「應用程式控制」或「全部」）。您必須選取至少一種類型。
6. 若是安全風險掃描，請在「指定安全風險掃描的類型」下方，選取「自動防護」、「排程和隨選」或「全部掃描」。請參閱說明，以取得為何要將例外限制為特定類型的安全風險掃描的相關資訊。
7. 按下「確定」。

從 **Mac** 用戶端上的掃描中排除檔案或資料夾

1. 在「例外政策」頁面上，按下「例外」。
2. 在「例外」下方，按下「新增 > **Mac** 例外 > 檔案或資料夾的安全風險例外」。
3. 在「檔案或資料夾的安全風險例外」下方的「前置變數」下拉式方塊中選擇一般資料夾。
選取 **[NONE]** 以輸入絕對路徑與檔案名稱。
4. 在「檔案或資料夾」文字方塊中，鍵入檔案或資料夾的名稱。
若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[NONE]**，請鍵入完整的路徑名稱。

NOTE

資料夾路徑必須用正斜線表示。

5. 按下「確定」。

從 **Linux** 用戶端上的掃描中排除資料夾

1. 在「例外政策」頁面上，按下「例外」。
2. 在「例外」下方，按下「新增 > **Linux** 例外」。
3. 按下「資料夾」。
4. 在「新增資料夾例外」對話方塊中，您可以選擇前置變數，鍵入資料夾名稱，以及是否要包含子資料夾。
自 14.3 RU1 起，Symantec Agent for Linux 不支援「同時排除子資料夾」選項，並且掃描時一律會排除所有子目錄。
若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[NONE]**，請鍵入完整的路徑名稱。

NOTE

資料夾路徑必須用正斜線表示。

5. 指定安全風險掃描的類型。選取「自動防護」、「排程和隨選」或「全部掃描」，然後按下「確定」。

更多資訊

- [建立病毒和間諜軟體掃描的例外](#)
- [從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名](#)

從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險

用戶端軟體偵測到的安全風險會顯示在「已知安全風險例外」對話方塊中。

已知安全風險清單包含有關風險嚴重性的資訊。

從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險

1. 在「例外政策」頁面上，按下「例外」。
2. 在「例外」下方，按下「新增 > Windows 例外 > 已知風險」。
3. 在「新增已知安全風險例外」對話方塊中，選取要從病毒和間諜軟體掃描中排除的一或多個安全風險。
4. 如果您想要記錄該偵測事件，勾選「偵測到安全風險時記錄」。

如果您未勾選此選項，用戶端會在偵測到選取風險時忽略該風險。用戶端也因此不會記錄該偵測事件。

5. 按下「確定」。
6. 架構完此政策後，按下「確定」。

更多資訊

[建立病毒和間諜軟體掃描的例外](#)

從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名

您可以新增多個副檔名至例外。在您建立例外之後，您無法為相同的政策建立其他副檔名例外。您必須編輯現有的例外。

您一次僅可以新增一個副檔名。如果您在「新增」文字方塊中輸入多個副檔名，政策會將這些項目視作一個副檔名進行處理。

如需詳細資訊，請參閱：

[建立病毒和間諜軟體掃描的例外](#)

從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名

1. 在「例外政策」頁面上，按下「例外」。
2. 在「例外」下方，按下「新增 > Windows 例外 > 副檔名」或「新增 > Linux 例外 > 副檔名」。
3. 在文字方塊中，輸入要排除的副檔名，然後按下「新增」。
4. 在「指定安全風險掃描的類型」下，選取「自動防護」、「排程和隨選」或「全部掃描」。
5. 將任何其他副檔名新增至例外。
6. 按下「確定」。

更多資訊

[從掃描中排除檔案或資料夾](#)

建立應用程式例外

您可防止 Symantec Endpoint Protection (SEP) 用戶端掃描或偵測您認為安全的應用程式。

您可監控特定的應用程式，以便為 Symantec Endpoint Protection 處理應用程式的方式建立例外。在 Symantec Endpoint Protection 了解該應用程式且管理主控台接收事件後，該應用程式隨即顯示於「應用程式例外」對話方塊的應用程式清單中。如果網路中的用戶端電腦尚未探索到任何應用程式，則應用程式清單顯示空白。

應用程式清單包括監控的應用程式以及使用者下載的檔案。當 Symantec Endpoint Protection 偵測到應用程式或應用程式執行時，Symantec Endpoint Protection 便會套用該動作。

應用程式也會出現在「**DNS** 和主機檔案變更例外」的清單中。

強制用戶端了解應用程式

您可以下列方式啟用應用程式學習：

1. 若您知道要學習的應用程式名稱，請架構 SEP 用戶端以監控該應用程式並學習其指紋。
若您停用應用程式學習，則要監控的應用程式例外會強制對指定的應用程式進行應用程式學習。
請參閱：[要監控的應用程式](#)
2. 若您不知道應用程式的名稱，且想要監控用戶端上的所有應用程式，則可架構 SEP 用戶端監控所有應用程式並學習其指紋。暫時對一小部分的用戶端執行應用程式學習。否則，此清單會快速地變大。
請參閱：[啟用應用程式探索](#)

如要建立應用程式例外

1. 在「例外政策」頁面上，按下「例外」。
2. 按下「新增 > **Windows** 例外 > 應用程式」。
3. 於「檢視」下拉式清單中，選取「全部」、「受監控的應用程式」，或「使用者允許的應用程式」。
4. 選取要為其建立例外的應用程式。
5. 於「指定要對此應用程式採取的動作」下拉式方塊中，選取「忽略」或「僅限記錄」。
 - 「忽略」和「僅限記錄」動作排除了應用程式的偵測，並允許其執行。
 - 當應用程式啟動時，會套用「終止」、「隔離」和「移除」動作。對不良或惡意的應用程式使用這些動作。
6. 按一下「確定」。

該應用程式還會出現在相關日誌中，並且可以從日誌中建立例外。

如要使用檔案指紋 (SHA256 雜湊) 來建立應用程式例外

若您知道應用程式的指紋 (SHA256 雜湊)，請直接輸入或啟用應用程式監控，以讓 SEP 用戶端了解用戶端電腦上的應用程式，接著從學習清單中建立例外。

1. 在「例外政策」頁面上，按下「例外」。
2. 按下「新增 > **Windows** 例外 > 應用程式」。
3. 按一下「依指紋新增應用程式」。
4. 請輸入應用程式指紋及應用程式名稱 (選用)。
5. 於「指定要對此應用程式採取的動作」中，選取「忽略」或「僅限記錄」。
6. 按一下「確定」。

更多資訊

- 如要找出用戶端電腦執行的應用程式，請參閱：[搜尋有關電腦執行之已探索應用程式的資訊](#)
- 於 14.3 RU3 和更新版本中，應用程式例外僅於 Windows 中受到支援。若您想在其他作業系統 (如 macOS 和 Linux) 中支援應用程式例外，請傳送一個[增強功能要求](#)。
- 「自動防護」程序排除並未於「例外政策」中進行架構。如要架構「自動防護」程序排除，請參閱：[防止 SEP 掃描受信任程序存取的檔案](#)。

從 Windows 用戶端上的掃描中排除信任的 Web 網域

您可從病毒和間諜軟體掃描和從行為分析中排除 Web 網域。排除信任的 Web 網域時，始終會允許使用者從該網域內的任何位置下載的任何檔案。不過，自動防護和其他定義的掃描仍會掃描該檔案。

依據預設，「下載鑑識」會排除出現在「Internet 信任的網站」清單上的網站，該清單位於「Internet Explorer > 工具 > 網際網路選項 > 安全性」。您可以從「病毒和間諜軟體防護」政策的「下載鑑識」設定中架構此設定。

如果停用「下載鑑識」或「自動防護」，則也會停用信任的 Web 網域例外。

NOTE

架構例外時請務必小心。您建立的每個例外都會降低電腦的安全性設定檔。考慮傳送任何可疑的誤報進行檢查，而不是開啟永久的掃描排除。一律使用 Symantec Endpoint Protection 提供的多層防護。請參閱：

[報告可疑的錯誤的偵測 \(誤報\)](#)

支援的 Web 網域例外

建立 Web 網域例外時，請遵循以下準則：

- 指定信任的 Web 網域例外時，您必須以 URL 或 IP 位址形式輸入單一網域。一次只能指定一個網域。
- 不支援通訊埠號。
- 指定 URL 時，例外只會使用 URL 的網域名稱部分。您可以在 URL 之前附加 HTTP 或 HTTPS (不區分大小寫)，但是例外會套用至這兩個通訊協定。
- 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。如果使用者透過其 URL 瀏覽到某個位置，Symantec Endpoint Protection 會將主機名稱解析成 IP 位址並套用例外。您只能在 IP 位址之前附加 HTTP (不區分大小寫)。
- 下載鑑識和行為分析均會排除該網域，而不論使用者是否透過 HTTP 或 HTTPS 瀏覽至網域。
- 針對 FTP 位置，您必須指定 IP 位址。不支援 FTP URL。
- 支援將萬用字元 * 與信任的 Web 網域的例外搭配使用。
- 「入侵防禦」政策中的 URL 信譽允許任何您指定為「信任的 Web 網域例外」的網站。

從 Windows 用戶端上的掃描中排除信任的 Web 網域

1. 在「例外政策」頁面上，按下「新增 > Windows 例外 > 信任的 Web 網域」。
2. 在「新增信任的 Web 網域例外」對話方塊中，輸入要排除的網域名稱或 IP 位址。
3. 按下「確定」。
4. 重複此程序可新增更多 Web 網域例外。

更多資訊

[建立病毒和間諜軟體掃描的例外](#)

在 Windows 用戶端上建立竄改防護例外

可以為「竄改防護」建立檔案例外。如果竄改防護會對您用戶端電腦上的已知安全性應用程式造成干擾，則您可能希望建立竄改防護例外。例如，「竄改防護」可能會攔截像螢幕閱讀器這類的輔助技術應用程式。

您需要知道與輔助技術應用程式相關聯的檔案名稱。然後您就可以建立例外，允許應用程式執行。

NOTE

「竄改防護」不支援資料夾例外。

14.2 RU1 及更新版本包括對 [User Profile] 和 [System] 前置變數的支援。

在 Windows 用戶端上建立竄改防護例外

-
1. 在「例外政策」頁面上，按下「例外」。
 2. 按下「新增 > Windows 例外 > 竄改防護例外」。
 3. 在「新增竄改防護例外」對話方塊的「前置變數」下拉式方塊中選擇一般資料夾。
選擇前置字元時，可在不同的 Windows 作業系統使用例外。
若您想輸入絕對路徑與檔案名稱，請選擇 **[NONE]**。
 4. 在「檔案」文字方塊中，輸入檔案名稱。
若您選擇一個前置字元，路徑應與前置字元有關。若您將前置字元選為 **[NONE]**，請鍵入完整的路徑名稱。
必須指定檔案名稱。「竄改防護」不支援資料夾例外。如果輸入資料夾名稱，「竄改防護」不會排除具有該名稱的資料夾中的所有檔案。它只會排除具有該指定名稱的檔案。
 5. 按下「確定」。

更多資訊

[建立病毒和間諜軟體掃描的例外](#)

針對會變更 DNS 或主機檔案的應用程式建立例外

您可以針對會變更 DNS 或主機檔案的特定應用程式建立例外。SONAR 可能會防止 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。

您可以監控特定應用程式，以便建立 DNS 或主機檔案變更例外。在 Symantec Endpoint Protection 探索到應用程式且管理主控台接收事件時，該應用程式會顯示在應用程式清單中。如果網路中的用戶端電腦尚未探索到任何應用程式，則應用程式清單顯示空白。

請使用 SONAR 設定來控制 SONAR 全域偵測 DNS 或主機檔案變更的方式。

針對會變更 DNS 或主機檔案的應用程式建立例外

1. 在「例外政策」頁面上，按下「例外」。
2. 按下「新增 > Windows 例外 > DNS 或主機檔案變更例外」。
3. 選取要為其建立例外的應用程式。
4. 在「動作」下拉式方塊中，選取「忽略」、「只記錄」、「提示」或「攔截」。
當掃描偵測到應用程式對 DNS 或主機檔案進行變更時，就會套用動作。
5. 按下「確定」。

更多資訊

- [建立病毒和間諜軟體掃描的例外](#)
- [建立應用程式例外](#)
- [調整用戶端電腦上的 SONAR 設定](#)

在 Windows 用戶端上從掃描中排除憑證

您可以個別為憑證新增例外，以防止將憑證所簽署的檔案掃描和偵測為可疑檔案。例如，公司內部開發的工具會使用自我簽署憑證。從掃描排除此憑證可防止自動防護、下載鑑識、SONAR 或其他掃描將其簽署的檔案偵測為可疑檔案。

憑證排除僅支援 X.509 和 base64 憑證類型。當您新增憑證例外時，將需要 DER 或 base64 編碼檔案 (.cer) 中的公用憑證的複本。

以下產品不支援憑證排除：

-
- 記憶體攻擊緩和
 - 主動型威脅防護系統變更事件
 - 竄改防護
 - 壓縮檔案內憑證簽署的檔案

無需在用戶端電腦上的憑證儲存區中安裝排除的憑證，排除即可運作。如果憑證例外和拒絕清單規則之間發生衝突，則會優先採用拒絕清單規則。

您只能透過 Symantec Endpoint Protection Manager 政策，而不能透過 Symantec Endpoint Protection 用戶端介面設定，新增憑證例外。

NOTE

如果已從雲端主控台取消註冊 Symantec Endpoint Protection Manager，則只能在其中新增憑證例外。如果已註冊 Symantec Endpoint Protection Manager，請使用雲端主控台來新增或管理憑證例外。

在 **Windows** 用戶端上從掃描中排除憑證

1. 在「例外政策」頁面上，按下「例外」。
2. 在「例外」下方，按下「新增 > **Windows** 例外 > 憑證」。

如果已在雲端主控台中註冊 Symantec Endpoint Protection Manager，這個選項不會出現。請改為在雲端主控台中新增憑證例外。

3. 在「憑證檔案」下方，按下「瀏覽」來瀏覽至您要排除的憑證，然後按下「確定」。
4. 確認「憑證資訊」下方的值對您要排除的憑證來說是正確的，然後按下「確定」。

若要針對多個憑證建立例外，請重複此程序。

更多資訊

[建立病毒和間諜軟體掃描的例外](#)

限制使用者可在用戶端電腦上架構的例外類型

您可讓用戶端電腦上的使用者為掃描建立例外，稱為使用者定義例外。依預設，允許使用者架構例外。若使用者在您關閉此功能之前已建立了例外，則例外仍然存在。

無論限制設定為何，用戶端電腦上使用者都無法建立竄改防護例外。

使用者也無法建立應用程式控制的檔案例外。

NOTE

用戶端使用者建立的例外 (稱為使用者定義例外)，不會上傳至管理伺服器。

限制使用者可在用戶端電腦上架構的例外類型

1. 請在「例外政策」頁面上，按下「用戶端限制」。
2. 在「用戶端限制」下，取消勾選任何您不希望使用者在用戶端電腦上架構的例外。
3. 架構完此政策後，按下「確定」。

更多資訊

[管理 Symantec Endpoint Protection 中的例外](#)

從日誌事件建立例外

您可以針對病毒和間諜軟體掃描、行為分析、應用程式控制和「竄改防護」從日誌事件中建立例外。

NOTE

無法針對提早啟動防惡意軟體偵測從日誌事件建立例外。

如果是 Linux 代理程式，您可以為資料夾和副檔名建立例外，但不能為檔案建立例外。

Table 113: 例外和日誌類型

例外類型	日誌類型
檔案	風險日誌
資料夾	風險日誌 SONAR：行為分析日誌
已知風險	風險日誌
副檔名	風險日誌
應用程式	風險日誌 SONAR：行為分析日誌
信任的 Web 網域	風險日誌 SONAR：行為分析日誌
竄改防護	應用程式控制日誌
DNS 或主機檔案變更	SONAR：行為分析日誌

Symantec Endpoint Protection 必須已偵測到您要為其建立例外的項目。當使用日誌事件建立例外時，您可指定應包含例外的例外政策。

從日誌事件建立例外

1. 在「監視器」標籤上，按下「日誌」標籤。
2. SONAR：行為分析日誌或應用程式和裝置控制日誌。
3. 如果選取了「應用程式與裝置控制」，請從「日誌內容」清單中選取「應用程式控制」。
4. 按下「檢視日誌」。
5. 在「時間範圍」旁，選取過濾日誌的時間間隔。

6. 選取要為其建立例外的一個或多個項目。

7. 在「動作」旁，選取要建立的例外類型。

對於所選取的項目，您選取的例外類型必須有效。

8. 按下「套用」或「開始」。
9. 在對話方塊中，移除任何您不想包含在例外中的項目。
10. 對於安全風險，如果要記錄偵測，請勾選「偵測到安全風險時記錄 Symantec Endpoint Protection」。
11. 選取所有應使用例外的例外政策。
12. 按一下「確定」。

更多資訊

- [監控 Symantec Endpoint Protection 用戶端](#)
- [管理 Symantec Endpoint Protection 中的例外](#)
- [建立病毒和間諜軟體掃描的例外](#)

使用 **Web** 和雲端存取防護控制網路存取

Web 和雲端存取防護政策會將 Symantec Cloud Secure Web Gateway (Cloud SWG) 功能整合至 Symantec Endpoint Protection。Web 和雲端存取防護政策會自動將用戶端上的所有網際網路流量重新導向至 Cloud SWG，其中根據 Cloud SWG 政策允許或攔截流量。

若要在 Symantec Endpoint Protection Manager (SEPM) 中使用此功能，您必須擁有有效的 Cloud SWG 訂閱。請聯絡您的帳戶代表以取得訂購授權。

您應該針對 Cloud SWG 政策利用應用程式執行徹底測試。

NOTE

Symantec Web Security Service (WSS) 已在 2022 年重新命名為 Symantec Cloud Secure Web Gateway (Cloud SWG)。

使用通道方法架構 **Web** 和雲端存取防護

在 14.3 RU8 及更新版本中，通道方法是與 Cloud SWG 整合的唯一方法。通道方法僅能執行於 Windows 用戶端。

Table 114: 架構通道方法

步驟	說明
步驟 1：為 Symantec Endpoint Protection Manager (SEPM) 中之通道方法架構 Web 和雲端存取防護政策。	1. 在 SEPM 中，於 Web 和雲端存取防護政策中，請確保將重新導向方法設定為通道。請參閱下列主題中的「步驟 3 - 在 SEP Manager 中架構 Web 和雲端存取防護 - 通道模式」：SEP Web 和雲端存取防護 - 通道模式。 2. 選擇「識別流量」選項 (14.3 RU5 及更新版本)。 下圖顯示決策樹狀結構，可協助您選擇要使用的流量識別方法。 <pre> graph TD A{Is this a true multi-user windows environment (Windows 10 multi-session, VDI)?} -- Yes --> B([Use the Based on the running process option]) A -- No --> C{Is a tunnel required prior to console user availability (RDP, Azure AD forgot password)?} C -- Yes --> D{Do you authenticate your users to WSS using SAML?} C -- No --> E([Use the Based on the console user option]) D -- Yes --> F([Use the Using WSS SAML authentication option]) D -- No --> G([Use the Based on the running process option]) </pre> 如需每種流量識別方法的說明，請參閱： Web 和雲端存取防護設定 a. (選用) 若要在 Symantec Endpoint Protection 用戶端上使用 SAML 驗證方法，請先在 Cloud SWG 入口網站上啟用 SAML 驗證。請參閱： • 關於 SAML 驗證和 Cloud SWG • WSS 代理程式的 SAML 支援 3. 產生並貼上您從 Cloud SWG 取得的整合 Token。 透過瀏覽至「連線 > WSS 代理程式」，可從 Cloud SWG 入口網站取得 Token。 Agent Token: ###X#XXXXXX###XX#### 4. 將政策保持解除鎖定狀態。 5. 將「Web 和雲端存取防護」政策指派給測試群組。
步驟 2：檢查是否已在用戶端上啟用「Web 和雲端存取防護」政策。	測試 SEP 用戶端時，請確保已啟用 Web 和雲端存取防護政策，並連線至 Cloud SWG。 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
步驟 3：架構並測試 Cloud SWG 政策。	若要測試 Web 和雲端存取防護，請先在實驗室環境中設定或修改 Cloud SWG 政策。然後，針對 Cloud SWG 政策執行各種測試方案，這通常涉及將用戶端的合規性與 Cloud SWG 政策進行比較。
步驟 4：鎖定 Web 和雲端存取防護政策。	您確定 Cloud SWG 政策在 Symantec Endpoint Protection 用戶端上依期望的方式運作後，鎖定該政策。然後，將會保護用戶端電腦，使用者無法從 Cloud SWG 中斷用戶端的連線。 若要鎖定「Web 和雲端存取防護」，請鎖定 SEPM「Web 和雲端存取防護」政策中的掛鎖。

NOTE

於 14.3 RU4 中，預設的流量識別方法是基於執行中程序。於 14.3 RU5 及更新版本中，預設的識別方法是基於主控台使用者。若您升級至 14.3 RU5 或更新版本，且「Web 和雲端存取防護」政策已套用至用戶端群組，則流量識別方法將會基於執行中程序保持不變。

如要使用「主機完整性」政策範本在用戶端電腦上安裝 WebView2 應用程式，或將獨立 WSS 代理程式遷移至包含「Web 和雲端存取防護」的 SEP 用戶端，請參閱：[疑難排解 Web 和雲端存取防護](#)

使用 PAC 檔案方法架構 Web 和雲端存取防護 (14.0.1 MP1 至 14.3 RU7)

NOTE

14.3 RU8 中的 PAC 檔案方法已移除。若要在 Windows 用戶端上使用 Web 和雲端存取防護，您必須使用通道方法。針對 Mac 用戶端，您須使用 Symantec Endpoint Protection Manager 或 Mac 用戶端版本 14.3 RU4 到 14.3 RU7。請參閱：

[將 Web 和雲端存取防護從 PAC 檔案重新導向方法移轉至通道方法](#)

Cloud SWG 管理員從 Cloud SWG 入口網站提供代理自動架構 (PAC) 檔案 URL 或整合 Token。然後，您可以使用 PAC 檔案或整合 Token 更新 Web 和雲端存取防護 政策，並將「Web 和雲端存取防護」政策指派給群組。請參閱：

[SEP Web 和雲端存取防護 - 明確模式](#)

使用「攔截通知服務」攔截內容時傳送通知 (選用)

若您的 Cloud SWG 帳戶與 CloudSOC 整合，則您可以使用攔截通知服務 (BNS)。當 CloudSOC gatelet (CASB/DLP) 政策攔截內容時，BNS 會對 SEP 用戶端提供路徑外通知。

[WSS 代理程式攔截通知服務](#)

報告

- Web 和雲端存取防護 政策的組態變更會出現在 Symantec Endpoint Protection Manager 稽核日誌中。
- 通道方法的事件會顯示於用戶端的「Web 和雲端存取防護」日誌中。這些事件會上傳到 Symantec Endpoint Protection Manager 系統日誌。

檢視用戶端上的 Web 和雲端存取防護日誌

1. 在用戶端電腦「狀態」頁面上，於「Web 和雲端存取防護」旁邊，按一下「選項」>「檢視日誌」。

更多資訊：

- [何謂 Web 和雲端存取防護？](#)
- [使用 SEP Web 和雲端存取防護整合 SEP 與 Cloud SWG \(以前稱為 WSS\)](#)

何謂 Web 和雲端存取防護？

Web 和雲端存取防護 保護用戶端電腦避開不安全的 URL，方法為將網路流量重新導向到 Symantec Cloud Secure Web Gateway (Cloud SWG)，其中 Cloud SWG 政策允許或攔截 Symantec Endpoint Protection (SEP) 用戶端上的流量。與 Cloud SWG 的整合可確保員工無法存取惡意網站或遵守您已定義的 Web 使用政策。

[Web 和雲端存取防護運作方式](#)

Cloud SWG 管理員會於 Cloud SWG 入口網站產生整合 Token。請新增 整合 Token 至 Symantec Endpoint Protection Manager Web 和雲端存取防護 政策，然後將此整合推送至 SEP 用戶端。當用戶端使用者登入其電腦時，SEP 用戶端會啟動與 Cloud SWG 的安全連線 (使用階段作業金鑰和預先共用金鑰 (PSK))。然後，SEP 用戶端會將「斷言」提供給 Cloud SWG。斷言包含使用者身分和有關電腦的其他資訊，如作業系統版本。這種「無縫識別」意味著使用者在透過網頁驗證入口網站存取網際網路時不必再次登入。此程序允許將每個使用者政策套用至流量，並將有風險的用戶端內容提供給 Cloud SWG，以進行記錄和報告。

Symantec Endpoint Protection 用戶端會以下列其中一種方式來處理所有支援的流量：

-
- 將它重新導向至 Cloud SWG 伺服器。
 - 攔截它。
 - 允許它繼續前往目的地。

重新導向方法

Web 和雲端存取防護政策在用戶端和 Cloud SWG 之間提供以下重新導向方法。下表描述每種方法的好處，以及它們的運作方式。

Table 115: 重新導向方法

方法	使用時機	運作方式
通道 (預設) (14.3 RU1 和更新版本)	通道方法會將 Cloud SWG 技術內嵌並部署至 Symantec Endpoint Protection，如此即可擷取非代理應用程式。此方法： - 依據 Cloud SWG 管理員如何架構 Web 和雲端存取防護通道模式的行為，重新導向連接埠 80、443、8080 和 8443 上的 http 和 https 通訊協定。 請參閱： 設定 WSS 代理程式網路和安全選項 - 重新導向任何應用程式，而不只是網頁瀏覽器。您還可以選擇僅重新導向網頁流量。 - 對於頻繁變更網路的漫遊使用者來說，更為強大。 - 透過加密流量，在用戶端電腦與資料中心之間提供更好的安全性。 - 為與 Cloud SWG 的主要連線方法。 - 在 64 位元 Intel 裝置上執行。 - 在 Windows 10 64 位元版本 1803 和更新版本 (14.3 RU4 和更新版本) 以及 Windows 10 19H2 和更新版本 (14.3 RU5 和更新版本) 上執行。 - 不支援 Windows 10 長期服務通道 (LTSC)。Microsoft 想要將 LTSC 只用於專業化系統。	此方法會從非代理感知應用程式擷取流量，而與單獨使用的 PAC 檔案重新導向相較，可讓 Token 進行更精細等級的安全管理。Cloud SWG 整合 Token 會轉送更多的標頭資料以識別起始流量的使用者，從而允許每個使用者的流量規則。 透過通道方法重新導向的流量取決於 Cloud SWG 政策的設定方式。例如，政策規則只能指定網頁流量，或指定所有通訊埠和通訊協定。通道方法還取決於您的 Cloud SWG 授權。 依預設，通道方法會安裝憑證，因為它是加密的通道。 如需 SEP 用戶端用來識別流量之不同方式的詳細資訊，請參閱「通道方法選項」： Web 和雲端存取防護設定
PAC 檔案 (14.0.1 MP1 至 14.3 RU7)	PAC 檔案方法： - 比通道方法快。 - 在所有支援的 Windows 作業系統上執行。 - 在 Mac 電腦上執行 (14.3 RU4 到 14.3 RU7) - 僅重新導向網頁流量。 - 不加密流量。	Cloud SWG 管理員可在 Cloud SWG 入口網站中架構 PAC 檔案，以取得 PAC 檔案 URL。PAC 檔案可自動將網頁流量重新導向到 Cloud SWG，並為網頁瀏覽器提供安全代理設定。PAC 檔案方法允許通訊埠 80 和 443 流量 (網頁流量) 重新導向以進行檢測。不過，它無法重新導向 80/443 以外的流量，或來自不遵守代理之應用程式的流量。只有網頁流量重新導向到 WSS 代理程式。 每次使用者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 Cloud SWG 傳送所有網頁瀏覽器流量，如 PAC 檔案所定義。根據 PAC 檔案定義的規則，會以下列其中一種方式處理所有支援的瀏覽器流量： - 如果沒有 Cloud SWG 整合 Token，所有網頁瀏覽器流量都會造訪 Cloud SWG 的 PAC 檔案 URL。所有使用者都遵守 Cloud SWG 的相同流量規則。 - 透過 Cloud SWG 整合 Token，所有網頁瀏覽器流量都會造訪 Cloud SWG 之本機快取的 PAC 檔案。Cloud SWG 可以判斷流量來自哪一個使用者，然後根據實際狀況導向網頁流量。

需求和限制

Table 116: 技術需求和限制

需求	說明
支援的瀏覽器	<i>Windows :</i> - Microsoft Internet Explorer 9 - 11 - Mozilla Firefox - Google Chrome - Microsoft Edge <i>Mac : (14.3 RU4 到 14.3 RU7)</i> - Mac 支援 Apple Safari、Google Chrome 和 Mozilla Firefox。 14.2 RU1 或更新版本中支援 Firefox 65 版及更新版本。
限制	- Cloud SWG 是在 IPv4 上提供，而不是在 IPv6 上提供。 - 如果在端點上安裝「Web 和雲端存取防護」功能，則無法安裝獨立式 Symantec WSS 代理程式。同樣地，若安裝 WSS 代理程式，則不會安裝「Web 和雲端存取防護」功能。不過，您可以使用下列其中一種方法，從現有端點移除「Web 和雲端存取防護」，而不需要解除安裝整個用戶端： - 在 Symantec Endpoint Protection Manager (SEPM) 中，建立未包括「Web 和雲端存取防護」的「用戶端安裝功能集」，然後將它套用至端點。請參閱： 新增或移除現有 Endpoint Protection 用戶端的功能 - 下列指令行選項使用用戶端安裝檔案來移除「Web 和雲端存取防護」：<code>setup.exe /s /v "REMOVE=NTR /qn"</code> 通道方法有以下限制： - 在 Windows 10 64 位元版本 1803 和更新版本 (每半年服務通道) 或 Windows 11 上執行。此方法不支援任何其他 Windows 作業系統或 Mac 用戶端。 - 不支援長期服務通道 (LTSC)。Microsoft 想要將 LTSC 只用於專業化系統。 - Symantec Endpoint Protection 用戶端的出埠流量會在用戶端防火牆或 URL 信譽規則對其進行評估之前重新導向到 WSS 代理程式。反之，會根據 WSS 代理程式防火牆和 URL 規則評估該流量。例如，如果 SEP 用戶端防火牆規則攔截了 google.com，而 WSS 代理程式規則允許 google.com，則該用戶端允許使用者存取 google.com。仍然由 Symantec Endpoint Protection 防火牆處理至用戶端的入埠本地流量。 - 如果用戶端電腦使用通道方法連線至 WSS 代理程式並裝載虛擬機器，則每個訪客使用者都必須安裝 Cloud SWG 入口網站中提供的 SSL 憑證。 - 不會重新導向本機網路 (如主目錄或 Active Directory 驗證) 的流量。 - 它與 Microsoft DirectAccess VPN 不相容。

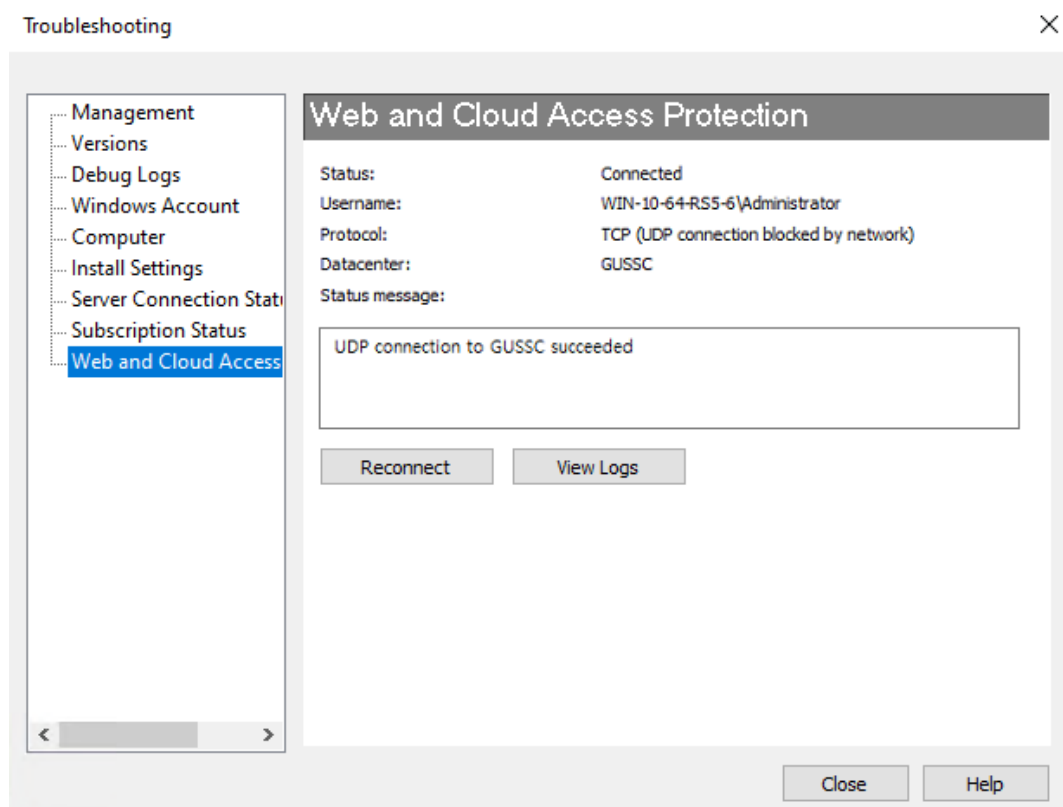
版本變更

- 在 14.3 RU8 中，PAC 檔案方法已移除。因為 Mac 用戶端不使用通道方法，Web 和雲端存取防護僅支援 14.3 RU1 到 14.3 RU7 Mac 用戶端。
- 在 14.3 RU6 之後，Symantec Web Security Service 已重新命名為 Symantec Cloud Secure Web Gateway (Cloud SWG)。
- 在 14.3 RU5 中，通道方法支援兩種其他方式來識別從 SEP 用戶端到 WSS 的流量。
- 在 14.3 RU4 中，通道方法包括支援 Windows 11 和已啟用 HVCI 的 Windows 64 位元裝置。
- 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」。
- 在 14.3 RU1 中，已新增稱為通道方法的新連線方法。
- 在 14.3 RU1 中，「WSS 流量重新導向」已重新命名為「網路流量重新導向」。
- 在 14.2 中，已新增支援，允許利用 WSS 進行加強的用戶端驗證，根據傳送網頁流量的使用者，對網頁流量進行更精細的控制。
- 在 14.2 RU2 中，已新增對 Mac 電腦的支援。
- 在 14.0.1 MP1 到 14.2 RU1 中，WSS 流量重新導向僅適用於 Windows 電腦。

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

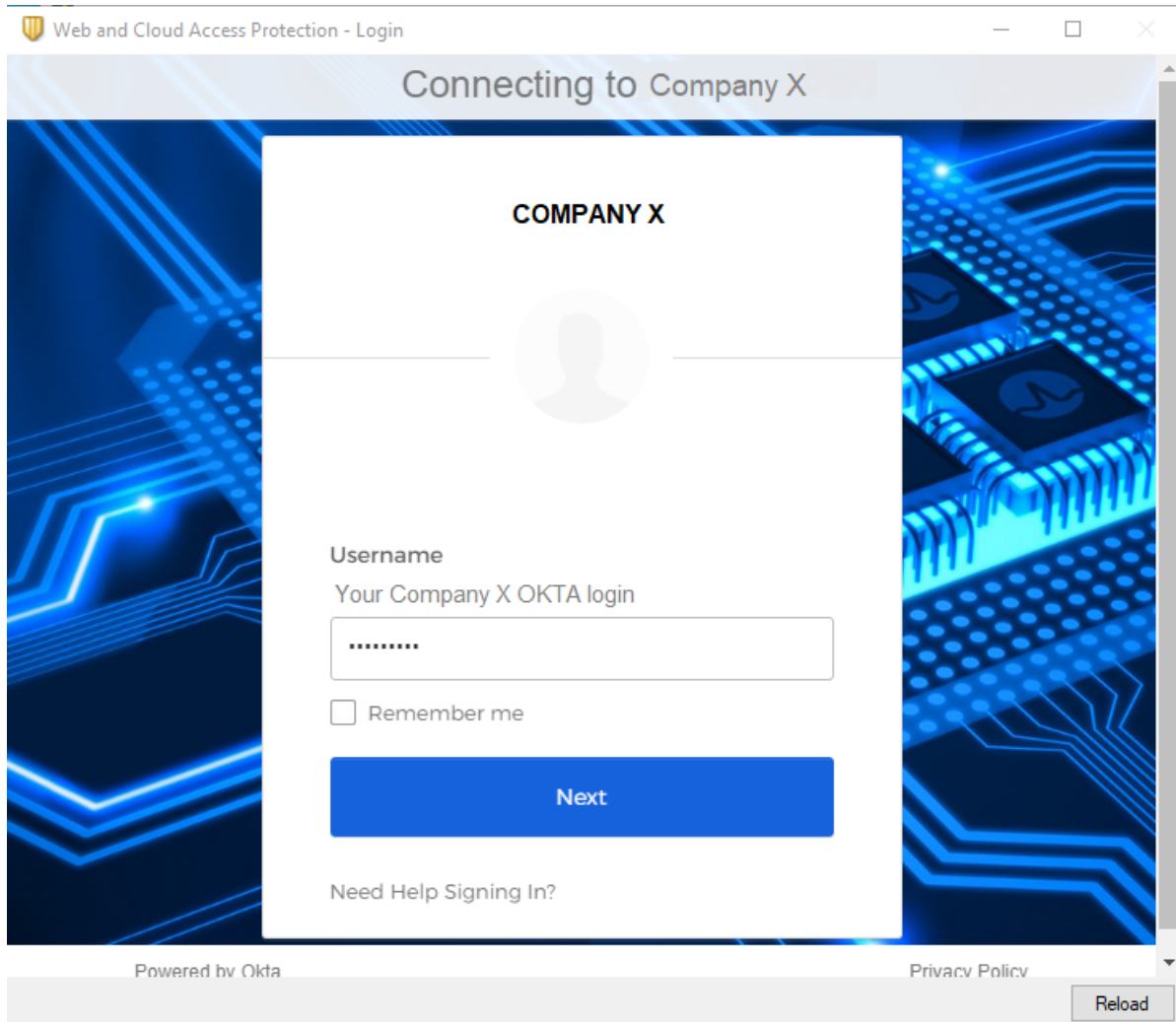
1. 在 Symantec Endpoint Protection (SEP) 用戶端上，按一下「說明」>「疑難排解」>「Web 和雲端存取防護」。如果「狀態」欄位顯示「已連線」，則會啟用 Web 和雲端存取防護，並將其並連線至 Cloud SWG。



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 Cloud SWG 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。

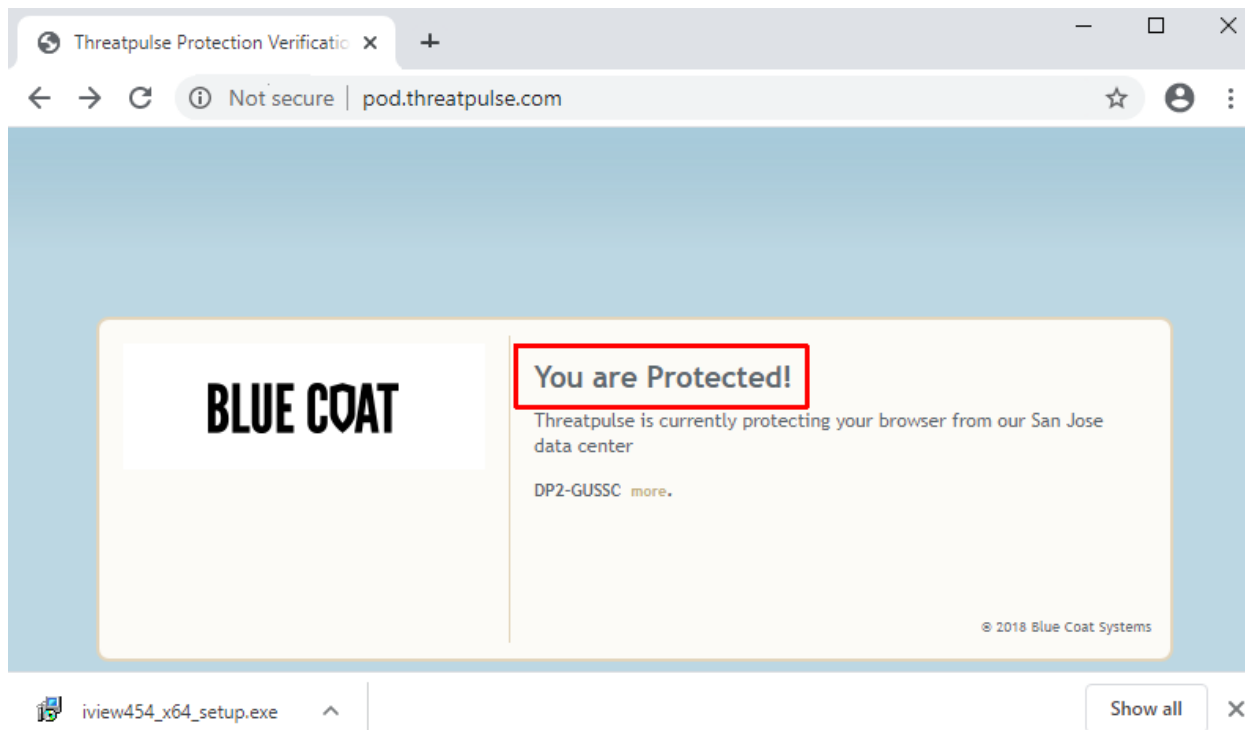


NOTE

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 Web 和雲端存取防護，則用戶端使用者應該會看到下列訊息。



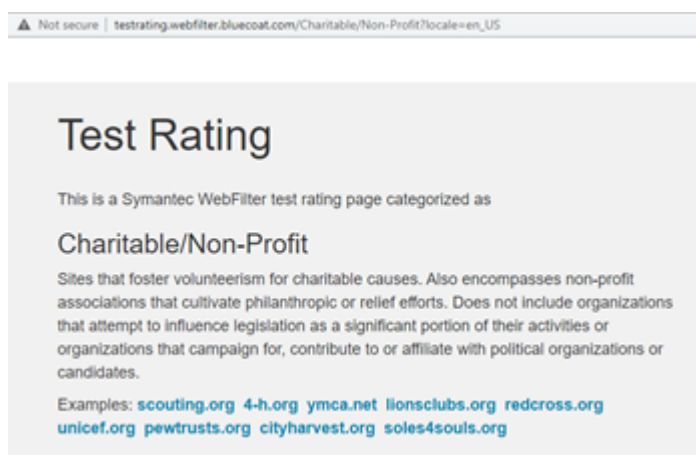
在瀏覽器中測試 Web 和雲端存取防護 政策

造訪測試網站

Cloud SWG 解決方案保護組織的方式為，對應用程式和網站進行分類，然後根據 Cloud SWG 政策允許或拒絕用戶端使用者。測試這些政策通常十分困難，因為需要用戶端使用者嘗試造訪可能危險的網站，如分類為具有已知惡意程式的網站。為了讓測試更為安全，Symantec 已經建置每個類別都有個別連結的網站。用戶端使用者可以按一下連結來模擬該類別的造訪，而不會產生風險。

造訪測試網站

1. 在用戶端電腦上，開啟瀏覽器視窗，並前往 <http://sitereview.symantec.com>
2. 按一下「類別」，然後選取「測試頁面」。
3. 按一下與 Cloud SWG 政策允許和拒絕的網站所對應的個別連結。驗證代理程式是否符合 Cloud SWG 類別政策。例如，允許的網站可能顯示如下：



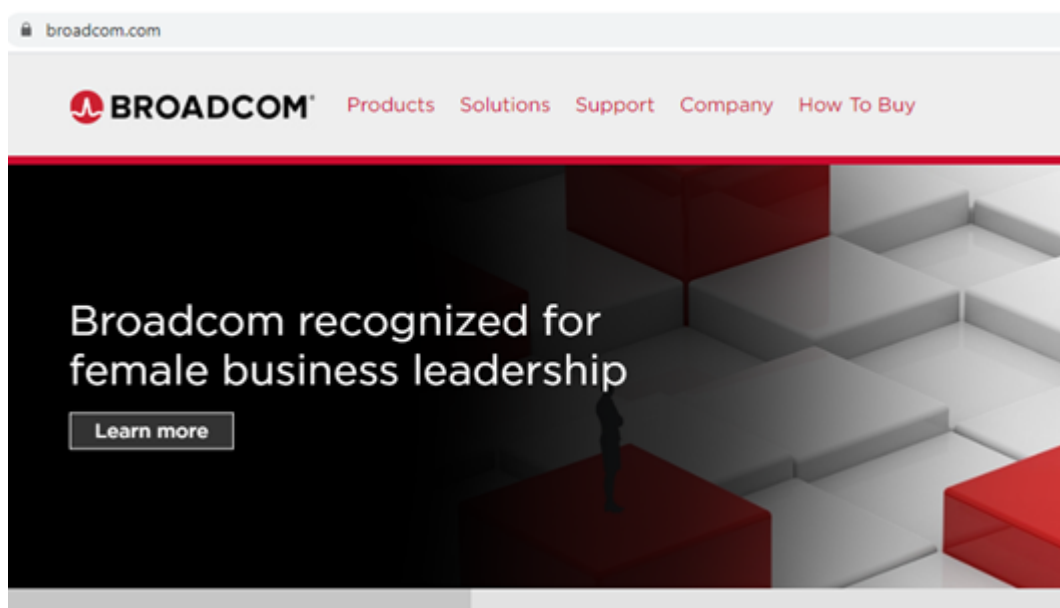
4. 按一下「威脅風險」，然後選取「測試頁面」。
這些連結會依 1-10 的遞增模擬風險來進行排序。
5. 按一下每個連結，以驗證用戶端是否符合 Cloud SWG 風險政策。

造訪政策允許的網站

此範例示範造訪 Cloud SWG 政策所允許網站的用戶端使用者。流量會重新導向至 Cloud SWG、進行檢查，並傳遞至網站。

造訪政策允許的網站

1. 前往 <http://www.broadcom.com>
2. 驗證用戶端電腦是否開啟該網站。



使用 Cloud SWG 政策測試通道方法

您可以使用 Cloud SWG 管理員在 Cloud SWG 主控台中設定的政策來測試整合式 Web 和雲端存取防護 解決方案。您可能需要與 Cloud SWG 管理員合作，取得可用來測試每個方案的網站清單，因為每個組織的政策都不同。

架構 Web 和雲端存取防護的 WSS 代理程式攔截通知服務

當內容遭到 Symantec CloudSOC gatelet (CASB/DLP) 政策攔截時，WSS 代理程式攔截通知服務 (BNS) 會對 Symantec Endpoint Protection 用戶端提供路徑外通知。

技術需求

此功能適用於已部署的 Symantec Endpoint Protection 用戶端，其透過與 CloudSOC 整合的 Cloud SWG 帳戶進行連線。

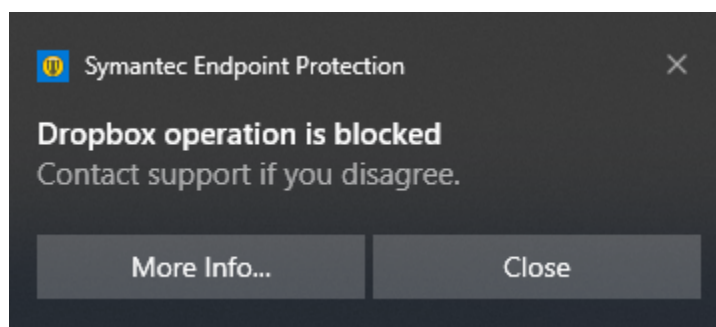
關於 Cloud SWG 與 CloudSOC 整合

「攔截通知服務」是如何運作的？

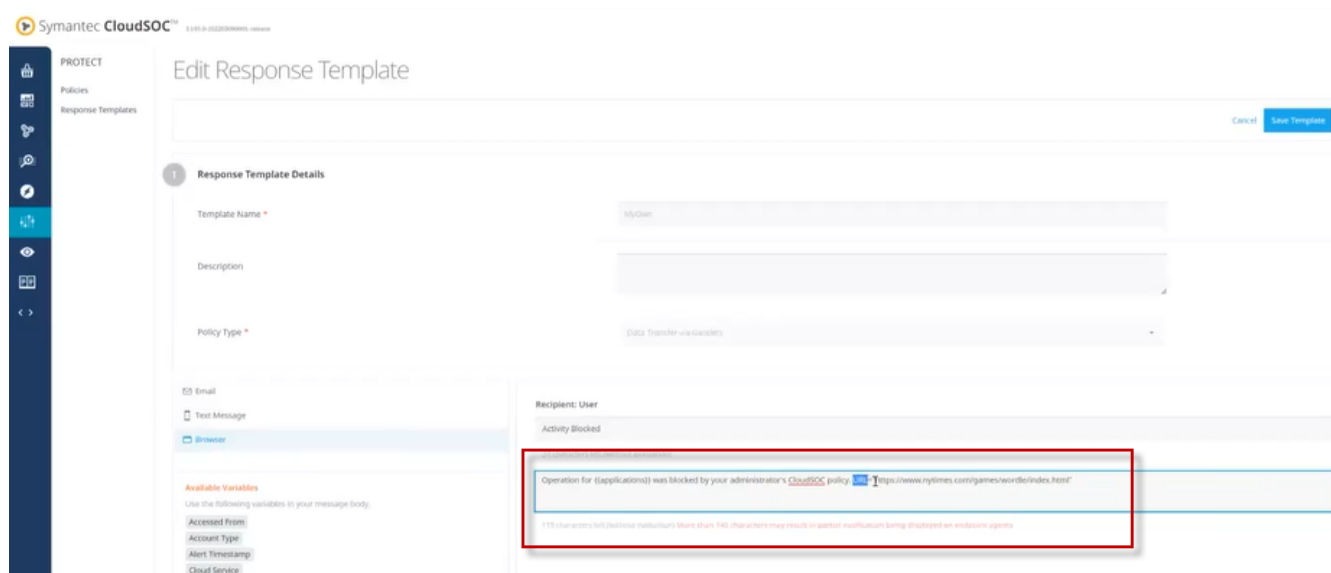
WSS 代理程式 BNS 會顯示一則依 Symantec CloudSOC 管理員所建立之政策規則的彈出式訊息。例如，CloudSOC 政策可能會攔截檔案下載，並啟用與 Dropbox 之間的檔案上傳。

Symantec Endpoint Protection 用戶端會建立使用者通道並連線至 WSS 代理程式 BNS。訊息會透過該連線傳遞至用戶端。用戶端會使用 Windows 作業系統 (Windows 上的「行動作業中心」) 所提供的通知機制。

用戶端使用者嘗試從 Dropbox 下載檔案時，會看到下列類型的訊息：



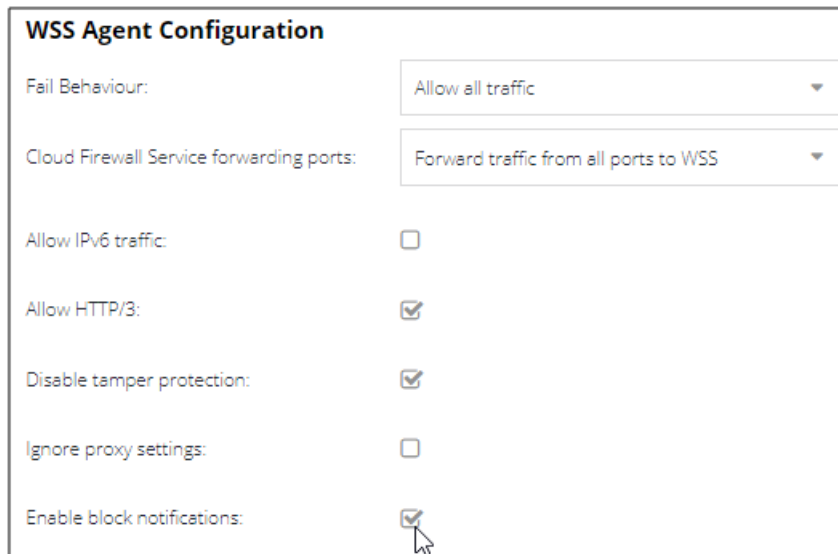
若 CloudSOC 管理員於政策中新增 URL 和訊息，則「更多資訊」選項隨即顯示。



當用戶端使用者瀏覽至 WSS 代理程式攔截或允許存取的網頁時，則不會使用 BNS 來顯示訊息。

架構攔截通知服務

1. 在 Cloud SWG 入口網站中，移至「連線 > **WSS** 代理程式」。
2. 按一下「啟用攔截通知」。



WSS Agent Configuration

Fail Behaviour: Allow all traffic

Cloud Firewall Service forwarding ports: Forward traffic from all ports to WSS

Allow IPv6 traffic: ☐

Allow HTTP/3: ☒

Disable tamper protection: ☒

Ignore proxy settings: ☐

Enable block notifications: ☒

當這些元素到位時，BNS 就會發揮作用。不需要其他組態。

最佳實務準則

若 Symantec Endpoint Protection 用戶端看似已連線且可運作，但未收到通知，請檢查 **Symantec WSS** 代理程式應用程式傳送通知的設定。

已知問題

- 當有很多檔案要與 OneDrive 同步時，便會出現 BNS 連續彈出式視窗。
解決方法 - 防止 OneDrive 程序在 Windows 登入時自動啟動：OneDrive「設定 > 一般」，並清除「登入 **Windows** 時自動啟動 **OneDrive**」選項。

將 **Web** 和雲端存取防護從 **PAC** 檔案重新導向方法移轉至通道方法

自 14.3 RU8 起，Web 和雲端存取防護政策不再提供 Windows 或 Mac 用戶端與 Symantec Cloud Secure Web Gateway (Cloud SWG) 之間的 PAC 檔案重新導向方法。您必須使用通道重新導向方法。

下表顯示透過架構 PAC 檔案重新導向方法，升級到 14.3 RU8 或更新版本時可能遇到的情況，以及如何解決這些問題。

範例	顯示內容	因應措施
如果從版本 14.3 RU1 到 14.3 RU7 升級至 14.3 RU8 或更新版本，且啟用 Web 和雲端存取防護並架構 PAC 檔案方法，Symantec Endpoint Protection Manager 將攔截升級。	啟動 Symantec Endpoint Protection Manager 安裝精靈並按一下「下一步」之後，將顯示以下訊息： <pre>#### PAC ##### Symantec Endpoint Protection Manager ##### Web ##### #####</pre>	- 取消安裝精靈。 - 返回至 Symantec Endpoint Protection Manager，停用 Web 和雲端存取防護政策，或針對通道方法架構這些政策。無論您在升級前或後重新架構通道方法，都必須從 Cloud SWG 取得新的整合 Token。 Note: 針對 Symantec Endpoint Protection Manager 14.3 RU1 之前的版本，您只能停用 Web 和雲端存取防護。 若要停用 Web 和雲端存取防護，請開啟該政策並取消選取「啟用 Web 和雲端存取防護」。 - 重新啟用安裝精靈。 附註： - Symantec 建議您在升級後停用這些政策並建立新政策。 14.3 RU1 之前的 SEP 用戶端版本不支援通道方法。因此，將 Symantec Endpoint Protection Manager 升級到 14.3 RU8 或更新版本後，Web 和雲端存取防護政策便無法在 14.3 及更舊版本的用戶端上運行。在升級 Symantec Endpoint Protection Manager 之前或之後，您必須將用戶端升級到更新版本。
如果從版本 14.3 RU1 到 14.3 RU7 升級至 14.3 RU8 或更新版本，且停用 Web 和雲端存取防護並架構 PAC 檔案方法，Symantec Endpoint Protection Manager 將允許升級並轉換政策至通道方法。	管理伺服器升級精靈成功升級 Symantec Endpoint Protection Manager。升級成功窗格會通知您政策已移轉，如下所示： <pre>Symantec Endpoint Protection Manager ##### Web ##### ### PAC ##### Symantec Endpoint Protection Manager #####</pre>	- 從 Cloud SWG 取得新的整合 Token。 - 將其貼到移轉的 Web 和雲端存取防護政策。 PAC 檔案重新導向方法 Token 不會移轉。
您在啟用 Web 和雲端存取防護且架構 PAC 檔案方法的情況下，執行了從 14.3 RU1 到 14.3 RU7 的資料庫備份。接著，您在 Symantec Endpoint Protection Manager 14.3 RU8 或更新版本中還原了資料庫備份。	啟動還原過程後，您會看到以下訊息： <pre>Symantec Endpoint Protection Manager ##### Web ##### ##### PAC ##### #####Symantec Endpoint Protection Manager ##### #####</pre>	還原資料庫之後，您必須為通道方法重新架構 Web 和雲端存取防護。 - 從 Cloud SWG 取得新的整合 Token。 - 將其貼到移轉的 Web 和雲端存取防護政策。
您已將 Web 和雲端存取防護 .dat 檔案從 Symantec Endpoint Protection Manager 14.3 MP1 匯出至 14.3 RU7，並要將其匯入 Symantec Endpoint Protection Manager 14.3 RU8 或更新版本。	Symantec Endpoint Protection Manager 不允許您匯入架構 PAC 檔案方法的舊政策。即便停用 Web 和雲端存取防護，Symantec Endpoint Protection Manager 仍不允許匯入。 您會看到以下訊息： <pre>##### PAC ##### #####</pre>	請建立使用通道方法和新整合 Token 的新政策。

範例	顯示內容	因應措施
若將 SEP 用戶端升級至 14.3 RU8 或更新版本，用戶端使用者的功能保持不變。	用戶端使用者看不到 PAC 檔案重新導向方法。	用戶端使用者仍然只能在 Symantec Endpoint Protection 管理員允許之下，啟用或停用 Web 和雲端存取防護。這與早期版本相同。

附註：

- 在 14.3 RU7 及更早版本中，Symantec Endpoint Protection Manager 僅支援 Mac 用戶端的 PAC 檔案重新導向方法。未來版本中將新增對通道方法的 Mac 支援。若要繼續支援 Mac 用戶端上的 Web 和雲端存取防護，請不要升級到 Symantec Endpoint Protection Manager 14.3 RU8。
- 在 2023 年 10 月 1 日以前，SES 雲端伺服器支援 PAC 檔案重新導向方法。

更多資訊

[SEP/SES「PAC 檔案模式」流量重新導向器生命週期](#)

[SEP 代理在 PAC 檔案模式下產生的部分交易不會受到記錄](#)

疑難排解 Web 和雲端存取防護

您可使用 Symantec Endpoint Protection (SEP) Web 和雲端存取防護對常見問題進行疑難排解。

- [重新連線至 Cloud SWG](#)
- [匯入主機完整性範本以解除安裝 WSS 代理程式，並執行 Microsoft WebView2 執行時間應用程式](#)

若要使用 SymDiag 收集除錯資料以解決將流量路由到 Cloud SWG 的 Symantec Endpoint Protection 用戶端的問題，請參閱：

[使用 SymDiag 為 SEP 用戶端收集 Cloud SWG 除錯資料](#)

下表顯示啟用 Web 和雲端存取防護時在 SEP 用戶端上發生的問題。

Table 117: Web 和雲端存取防護問題

問題	重新導向方法	解決方法
如果您停用 Symantec Endpoint Protection 通知區域圖示 (系統匣圖示)，則 WSS 通道模式不適用於 SAML 驗證。	通道	讓通知區域圖示保持啟用。請參閱： 在管理伺服器： 用戶端使用者介面混合控制設定：用戶端/伺服器控制設定 在用戶端： 顯示或隱藏 Symantec Endpoint Protection 用戶端上的通知區域圖示 在雲端控制台： 隱藏 Symantec Endpoint Protection 用戶端通知區域圖示 (自 14.3 RU9)
啟用 WSS 通道後，在 Symantec Endpoint Protection 防火牆有機會檢查流量之前，連出流量會通過通道。連入流量仍會受到檢查。	通道	無。
若您使用 PAC 檔案重新導向方法，並升級至 SEPM 14.3 RU8 或更新版本，該升級會遭攔截。	PAC 檔案	SEPM 14.3 RU8 的 PAC 檔案方法已移除。請參閱： 將 Web 和雲端存取防護從 PAC 檔案重新導向方法移轉至通道方法

問題	重新導向方法	解決方法
啟用 SAML 驗證後，某些用戶端使用者會看到下列其中一個錯誤： - 用戶端「狀態」頁面會顯示下列錯誤：Web ##### # WebView2 ##### WebView2 ##### 「SAML 登入」視窗會顯示 404 狀態錯誤或逾時錯誤。	通道	當用戶端執行 Windows 10 且未安裝 Microsoft Edge WebView2 執行時間應用程式時，會出現此問題。 如要解決該問題： - 請確保用戶端電腦執行 14.3 RU5 或更新版本。 - 手動或使用主機完整性範本作為管理員下載並安裝 Microsoft Edge WebView2 執行時間應用程式。請參閱：匯入主機完整性範本以解除安裝 WSS 代理程式，並執行 Microsoft WebView2 執行時間應用程式 用戶端在大約10分鐘後會偵測 WebView2 應用程式安裝。若該選項可用，用戶端使用者還可按一下「Web 和雲端存取防護設定 > 啟用 Web 和雲端存取防護」。 依預設，WebView2 執行時間應用程式隨 Windows 11 安裝。 請參閱：啟用 SAML 驗證時，WSS 代理程式使用者無法登入
「SAML 登入」視窗 (Web 和雲端存取防護 - 登入) 凍結。	通道	有時，msedgewebview2 程序可能會當機，此將導致 SAML 登入畫面凍結。 如要解決此問題，請依順序執行下列步驟： - 在「Web 和雲端存取防護 - 登入」視窗中，按一下「重新載入」。 - 在「用戶端 狀態」頁面上的「Web 和雲端存取防護」旁，按一下「選項 > 重新連線」。 - 從用戶端登出，然後登入。 - 重新啟動用戶端電腦。
當啟用 SAML 驗證但 SAML 登入視窗顯示為空白或不斷重新出現且消失時。	通道	在用戶端上，按一下「重新連線」選項。
啟用 SAML 驗證且 Symantec Endpoint Protection 用戶端無法存取 Internet 時，將不會顯示 SAML 登入視窗 (Web 和雲端存取防護 - 登入)。	通道	在用戶端上，請依順序執行下列步驟： - 按一下「重新連線」選項，以連線至 Cloud SWG 並重新初始化 SAML 驗證。 - 重新啟動用戶端。
啟用 SAML 驗證後，「 Web 和雲端存取防護 - 登入」視窗將遭到凍結或為空白。用戶端使用者無法輸入其憑據。	通道	在用戶端電腦上，請執行下列步驟： - 在「Web 和雲端存取防護 - 登入」視窗中，按一下「重新載入」。 - 在 SEP 用戶端上，按一下「重新連線」選項。
利用 SAML 驗證，用戶端使用者在嘗試存取 HTTPS 網站時看到中斷的連線。	PAC 檔案	如要解決此問題，請先手動存取 HTTP 網站，如 HTTP://www.bbc.co.uk ；然後回到原始的 HTTPS 網站 https://www.bbc.co.uk 。
網頁會重新導向至 Cloud SWG，但顯示缺少憑據的錯誤。	PAC 檔案	如果您於 Web 和雲端存取防護政策中提供了無效的 Cloud SWG Token，則可能會發生此問題。 若要解決此問題，請檢查您是否已為 Cloud SWG 整合提供了正確的 Token。
無法下載 PAC 檔案。	PAC 檔案	若您提供了錯誤的 PAC 檔案 URL，或您的瀏覽器正阻止檔案下載，則可能會出現此問題。 如要解決此問題，請檢查您在「Web 和雲端存取防護」政策中使用的 PAC 檔案 URL，並驗證問題是否適用於所有瀏覽器。
Symantec Endpoint Protection 用戶端顯示下列中一個錯誤： - 即使在用戶端使用者成功登入之後，Web 和雲端存取防護 SAML 登入頁面仍會重複彈出。 「狀態」頁面顯示：Web ##### - 用戶端「關於」>「疑難排解」>「Web 和雲端存取防護」頁面會在「狀態」欄位中顯示下列錯誤：80010908	通道	導致此問題的原因是，Windows 主機對 Cloud SWG 產生未回應的 TLS 1.0 要求。 即使在 WSS 代理程式使用者登入之後，這些使用者仍會使 SAML 視窗重複彈出

重新連線至 Cloud SWG

Web 和雲端存取防護 應該持續連線至 Cloud SWG。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線至 Cloud SWG。

Table 118: 重新連線至 Cloud SWG 的方法

方法	說明
若 Symantec Endpoint Protection 用戶端偵測到連線中斷。	1. 在用戶端上，按一下「狀態」頁面。 2. 在頁面頂端，如果 Web 和雲端存取防護 已啟用、已連線且正常運作，則條紋為綠色。如果防護已啟用或中斷連線，則條紋為黃色或紅色。 3. 若要重新連線至 Cloud SWG，用戶端使用者應該按一下「修正」按鈕。 
如果用戶端未偵測到連線已中斷。	1. 在用戶端上，按一下「狀態」頁面。 2. 在「Web 和雲端存取防護」旁，按一下「選項 > 重新連線」。「狀態」欄位應顯示「已連接」。若非如此，請按下「重新連接」。

匯入主機完整性範本以解除安裝 WSS 代理程式，並執行 Microsoft WebView2 執行時間應用程式

為了節省時間，您可匯入在用戶端電腦上依據您設定的排程，執行下列任務的主機完整性指令碼：

- 請從用戶端電腦上解除安裝 Symantec WSS 代理程式，然後安裝 Web 和雲端存取防護功能。
- 在用戶端電腦上安裝 Microsoft Edge WebView2 執行時間應用程式。

Table 119: 主機完整性範本

範本	說明
• 將獨立的 WSS 代理程式 (未解除安裝 Token) 遷移至 Symantec Endpoint Protection 用戶端 • 將獨立的 WSS 代理程式 (解除安裝 Token) 遷移至 Symantec Endpoint Protection 用戶端	• 如果已在 Cloud SWG 入口網站上設了解除安裝 Token，請修改「使用解除安裝 Token」指令碼，來使用您公司使用的 Token。 • 確保這些腳本不在同一組上同時運行。請為每個指令檔建立一個各自的政策。 • 每天執行一次主機完整性檢查，而非每隔2分鐘一次。每天一次就夠了。在「進階設定」頁面上，修改「每 x 分鐘檢查主機完整性」選項。請參閱：進階設定
安裝 Microsoft Edge WebView2 執行時間以進行 SAML 驗證	• Microsoft Edge WebView2 執行時間應用程式在使用 SAML 驗證的 14.3 RU5 及更新版本的用戶端上是必要的。您可將「主機完整性」政策指派給 14.3 RU4 和較早的用戶端，而不會產生任何後果。 • 您必須在執行 Windows 10 (但非 Windows 11) 之用戶端電腦上安裝 Microsoft Edge WebView2 執行時間應用程式。

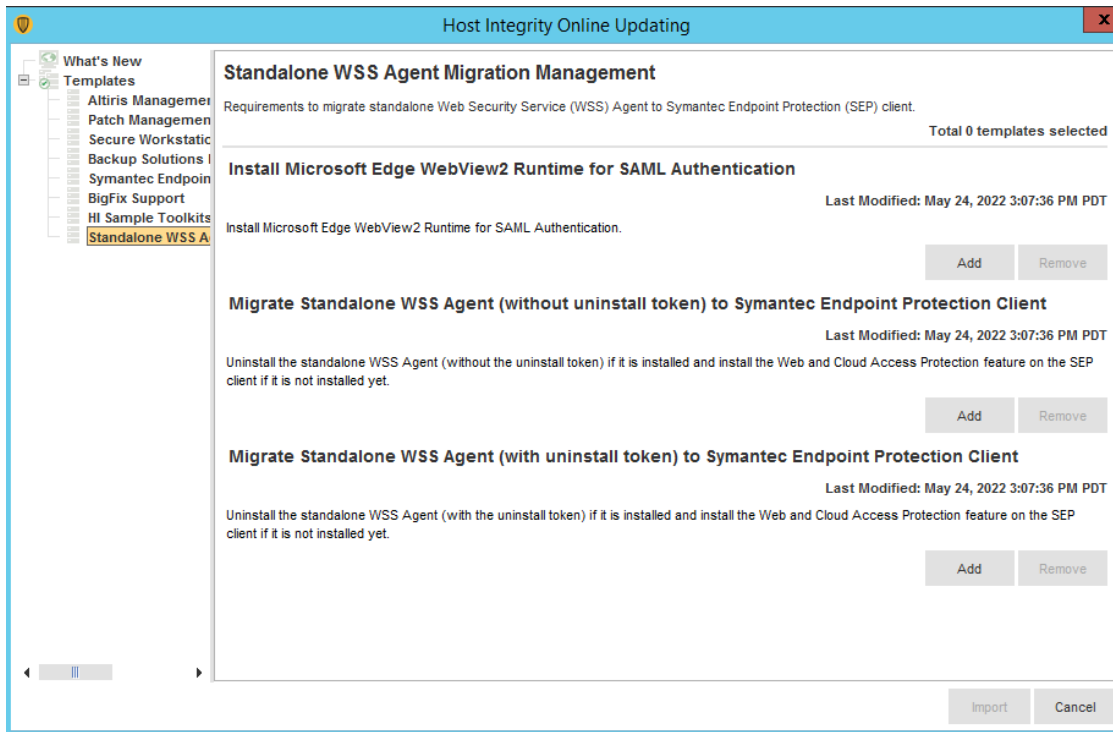
附註：

- 請先閱讀每個指令碼，以了解其功能。請確保先使用適合貴組織和環境的附加檢查對其進行測試。
- 若指令碼失敗，請監控用戶端電腦，然後進行疑難排解。
- 於雲端主控台中，請確保勾選了「即使這項要求失敗，也允許主機完整性檢查通過」選項。您不希望該裝置遭到失敗的遷移或其他要求隔離，也不會受到影響。您可以檢查報告，找出未通過主機完整性檢查但標記為通過的裝置，然後對其進行疑難排解。

[允許主機完整性檢查在需求失敗時通過](#)

在 **Symantec Endpoint Protection Manager** 中匯入 **Cloud SWG** 的主機完整性範本

1. 於 Symantec Endpoint Protection Manager 主控台中，開啟「主機完整性」政策，然後按一下「要求 > 新增」。
2. 於「新增要求」對話方塊中，按一下「使用現有範本」，然後按一下「確定」。
3. 於「主機完整性線上更新」對話方塊中，「範本」下，選取「獨立 WSS 代理程式遷移管理」。



4. 在您要新增的每個範本旁，按一下「新增 > 匯入」，然後按一下「確定」。

[透過匯入範本建立主機完整性政策需求](#)

管理 Mac 用戶端的 Web 和雲端存取防護

關於 Web 和雲端存取防護

Web 和雲端存取防護透過將網路流量重新導向至 Symantec Cloud Secure Web Gateway (Cloud SWG)，保護電腦免受不安全的 Web 內容影響。您的組織建立政策以允許或攔截 Web 流量。與 Cloud SWG 整合可確保您遵守由公司設定的類別和內容政策，並攔截存取惡意網站。

Web 和雲端存取防護運作方式

Web 和雲端存取防護政策在用戶端和 Cloud SWG 之間提供以下重新導向方法：

- 通道 (若您從 Symantec Endpoint Security 雲端主控台而非從 Symantec Endpoint Protection Manager 管理通道，則此方式可用。)

所有流量都傳送到 Cloud SWG 以進行檢測。

- PAC 檔 (已從 14.3 RU8 移除)

套用 PAC 檔案規則時，只有通訊埠 80 和 443 上的 Web 流量會重新導向至 Cloud SWG。

NOTE

您的管理員設定流量重新導向的方法。

NOTE

系統可能會提示您輸入網路認證。

造訪網站

根據您組織的政策，顯示或攔截 Web 內容。被攔截的網頁會在您的瀏覽器中顯示為「拒絕存取」的通知頁面。

開啟或關閉 Web 和雲端存取防護

管理員可能會要求您停用 Web 和雲端存取防護以進行疑難排解。

NOTE

管理員可能會設定政策來預防您停用此功能。

若要開啟或關閉 Web 和雲端存取防護

1. 在 Mac 用戶端中，按下「進階」>「Web 和雲端存取防護」。
2. 按下「Web 和雲端存取防護」。
3. 切換「Web 和雲端存取防護」選項。

驗證 Web 和雲端存取防護流量重新導向

若要協助進行疑難排解，您可以測試 Mac 用戶端是否將流量重新導向至 Cloud SWG。

若要驗證 Web 和雲端存取防護流量重新導向

1. 開啟瀏覽器
2. 前往 <https://pod.threatpulse.com>

如果您的流量被重新導向，則瀏覽器會顯示訊息「您已受到保護！」

Web 和雲端存取防護設定

Web 和雲端存取防護可讓 Windows 和 Mac 用戶端電腦防禦網路流量，方法為將其重新導向至 Symantec Cloud Secure Web Gateway (Cloud SWG)，其中 Cloud SWG 允許或攔截流量。Cloud SWG 會根據管理員在 Cloud SWG 中架構的政策允許或攔截流量。

NOTE

若要在 Symantec Endpoint Protection Manager 內使用此功能，您必須擁有有效的 Cloud SWG 訂閱。請聯絡您的帳戶代表以取得訂購授權。

Table 120: Web 和雲端存取防護 設定

選項	說明
啟用 Web 和雲端存取防護	啟用或停用 Symantec Endpoint Protection 用戶端上的 Web 和雲端存取防護 功能。您必須勾選此選項，才能在用戶端上啟用它。 如果您對 PAC 檔案方法停用此選項，仍可以啟用「在用戶端上安裝 Symantec Web Security Service 根憑證，以便保護加密流量」選項。
重新導向方法 (14.0.1 MP1 至 14.3 RU7)	- 通道方法會依據您架構 WSS 代理程式行為的方式自動將所有 Internet 流量 (連接埠 80、443、8080 和 8443) 重新導向至 Cloud SWG。 設定代理程式網路和安全選項 您應該針對 Cloud SWG 政策利用應用程式執行徹底測試。 - PAC 檔案方法會重新導向僅 Web 流量 (通訊埠 80 和 443)。14.3 RU8 中的 PAC 檔案方法已移除。 如需重新導向方法之間差異的相關資訊，請參閱： 何謂 Web 和雲端存取防護？

下表顯示 Cloud SWG 用來識別來自 SEP 用戶端流量的不同方法。在 Cloud SWG 中架構這些設定，然後於 SEP 用戶端中選擇該方法。

Table 121: 通道方法選項

選項	說明	優點	缺點
識別流量	基於主控台使用者： - 單一通道。 14.3 RU5 和更新版本用戶端的預設值。 - 於 14.3 RU5 及更新版本上受支援。	- 確保將所有流量皆識別為登入至裝置的 SAML 使用者。 - 即使未使用 SAML 驗證，也適用於所有狀況。 - 若主控台使用者因登入、登出或快速使用者切換而產生變化，則流量識別方法也會隨之切換。	- 不適用於透過遠端桌面協議 (RDP) 連線存取的端點。 - 於用戶端使用者登入後，才會建立 VPN 通道。若您使用 Microsoft Azure Active Directory 租用戶並對其進行架構，以限制對僅源自 SEP 用戶端流量的存取，則 Azure AD 忘記密碼將不起作用。
	使用 WSS SAML 驗證： - 單一通道。 - 於 14.3 RU5 及更新版本上受支援。	- 確保將所有流量皆識別為指派的使用者，無論登入裝置的本機使用者為何。 - 適用於透過 RDP 連線存取的端點。 - 於用戶端使用者登入之前建立 VPN 通道。	要求在使用之前設定 Cloud SWG 的 SAML 驗證。
	基於執行中的程序： - 多個通道。 - 預設為 14.3 RU4。 - 於 14.3 RU1 及更新版本上受支援。	- 確保將流量識別為最初在裝置上傳送流量的使用者。 - 適用於透過 RDP 連線存取的端點。 - 於使用者登入之前建立 VPN 通道。	- 將一些攔截和重新插入流量的安全應用程式識別為重新插入流量的程序使用者，而非原始使用者。 - 連線可能需要更長時間，因為其在用戶端處理來自新使用者流量時隨需要加以建立。 - 非互動式使用者的重新連線或中斷會造成所有目前建立的通道重新連線。 - 未來需要單一通道的「Web 和雲端存取防護」增強功能無法使用。
網路整合 Token	Cloud SWG 管理員會從 Cloud SWG 入口網站產生隨機的整合 Token。		

Table 122: PAC 檔案方法選項 (14.0.1 MP1 到 14.3 RU7)

選項	說明
代理自動架構 (PAC) 檔案 URL	指示代理自動架構檔案的 URL，如 Cloud SWG 管理員所定義。 只能在 Symantec Endpoint Protection Manager 中架構或編輯此 URL。
流量攔截通訊埠	指示正由本機代理服務使用的通訊埠。 對於 14.2 RU1 以前的版本，此選項僅適用於 Windows 電腦。
網路整合 Token	Symantec Endpoint Protection 用戶端使用此 Token，將使用者 ID 和用戶端內容資訊安全地轉送到 Cloud SWG。本機代理服務要求 Token 剖析每個使用者規則的標頭資訊，以允許或攔截該 Web 流量。 此選項可允許 PAC 檔案的本機快取。 對於 14.2 RU1 以前的版本，此選項僅適用於 Windows 電腦。
網路防護無法使用時允許直接流量	如果使用 Cloud SWG 雲端代理 (proxySG) 時使用者驗證失敗，請使用此選項為使用者授與 Web 存取權。如果管理員設定了 PAC 檔案，而不是 Cloud SWG 漫遊使用者，則會發生這種情況。 - 如果勾選了此選項，而且用戶端使用者無法驗證，則用戶端無法開啟。 - 如果未勾選此選項，而且用戶端使用者無法驗證，則用戶端無法關閉。 在驗證使用者之前，Web 和雲端存取防護 不會保護他們。Cloud SWG 嘗試在背景每 5 分鐘驗證使用者。然後，Cloud SWG 會要求在 Cloud SWG 漫遊網頁驗證入口網站中手動驗證使用者。 在進行有效的驗證嘗試之前，會忽略此設定。 此選項適用於用戶端 14.2 RU2 MP1 及更新版本。
啟用 LPS 自訂 PAC 檔案	將用戶端上的 LPS 伺服器託管的預設 PAC 檔替換為自訂 PAC 檔。自訂 PAC 檔解決了與第三方應用程式的相容性問題，這些應用程式不能用於在回送配接卡上接聽的本地代理伺服器。您應透過 Cloud SWG 入口網站進行所有其他架構的略過和篩選。 此選項適用於用戶端 14.3 及更新版本。 Warning! 如果您錯誤地架構自訂 PAC 檔案選項，則可能會阻止用戶端使用者和應用程式存取 Internet。 Note: 自訂 PAC 檔案的效果可能不會立即生效。您可能需要重新啟動用戶端。
在用戶端上安裝 Symantec Web Security Service 根憑證，以便保護加密流量	在 Symantec Endpoint Protection 用戶端上安裝適當的根憑證來保護加密流量。 「啟用 Web 和雲端存取防護」選項停用時，您可啟用此選項，此可讓您安裝根憑證，即使未選取 PAC 檔案選項也是一樣。

測試 Symantec Endpoint Protection Manager 政策

您可能需要先評估 Symantec Endpoint Protection 或測試政策，然後才能將它們下載到用戶端電腦。您可以使用 Symantec Endpoint Protection Manager 政策來測試下列功能，以確保產品能在用戶端電腦上正確運作。

Table 123: 您可以測試的功能

功能	請參閱本主題
病毒和間諜軟體防護	若要測試預設病毒和間諜軟體防護政策，請從以下位置下載 EICAR 測試病毒： 反惡意程式 TESTFILE 然後，請參閱： 測試病毒和間諜軟體防護政策
行為分析	下載 Socar.exe 測試檔以確認 SONAR 運作是否正常
Insight	如何測試智慧型掃描與賽門鐵克授權伺服器的連線能力

功能	請參閱本主題
入侵預防	測試預設 IPS 政策
應用程式控制	攔截程序在用戶端電腦上啟動 防止使用者寫入用戶端電腦上的登錄 防止使用者寫入特定檔案 新增和測試攔截 DLL 的規則 新增和測試終止程序的規則

測試病毒和間諜軟體防護政策

若要測試並檢查病毒和間諜軟體防護政策是否起作用，您可以使用測試病毒檔 eicar.com。EICAR 測試病毒是歐洲電腦防毒研究協會 (European Institute for Computer Antivirus Research, EICAR) 所開發的文字檔，其提供了簡單且安全的方式來測試大多數的防毒軟體。您可以使用它來確認用戶端防毒部分的運作情況。

測試病毒和間諜軟體防護政策

1. 在用戶端電腦上，從 EICAR 網站下載防毒測試檔，網址如下：

[下載防惡意軟體 Testfile](#)

2. 執行 EICAR 測試檔。

系統會顯示通知，表示發現風險。

3. 在 Symantec Endpoint Protection Manager 的「監視器」頁面上，按下「日誌」。
4. 在「日誌」標籤的「日誌類型」下拉式清單中，按下「風險」，再按下「檢視日誌」。
5. 在「風險日誌」頁面上，會出現「發現病毒事件」。

攔截程序在用戶端電腦上啟動

FTP 用戶端是將檔案從伺服器傳輸至用戶端電腦的常見方式。若要防止使用者傳輸檔案，您可以新增規則來攔截使用者從命令提示字元啟動 FTP 用戶端。

新增攔截程序在用戶端電腦上啟動的規則

1. 開啟應用程式控制政策，並在「應用程式控制」窗格中按一下「新增」。
 2. 在「應用程式控制規則集」對話方塊的「規則」清單中選取規則，然後在「屬性」標籤的「規則名稱」文字方塊中輸入 `ftp_blocked_from_cmd`。
 3. 在「套用此規則至下列程序」右側，按下「新增」。
 4. 在「新增程序定義」對話方塊的「要比對的程序名稱」下方，輸入 `cmd.exe`，然後按下「確定」。
 5. 在「應用程式控制規則集」對話方塊的「規則」清單下方，按下「新增條件 > 啟動程序嘗試」。
 6. 在「屬性」標籤的「敘述」文字方塊中，輸入 `no ftp from cmd`。
 7. 在「套用此規則至下列程序」右側，按下「新增」。
 8. 在「新增程序定義」對話方塊的「要比對的程序名稱」下方，輸入 `ftp.exe`，然後按下「確定」。
 9. 在「應用程式控制規則集」對話方塊的「動作」標籤上，按下「攔截存取」、「啟用記錄」和「通知使用者」。
 10. 在「通知使用者」下方，輸入 `ftp is blocked if launched from the cmd`。
 11. 按下「確定」兩次，然後將政策指派給群組。
- 測試規則。

測試攔截程序在用戶端電腦上啟動的規則

1. 在用戶端電腦上，開啟命令提示字元。
 2. 在命令提示字元視窗中，輸入 `ftp`，然後按 **Enter** 鍵。
- 由於已指定規則，FTP 用戶端不會開啟。

防止使用者寫入用戶端電腦上的登錄

您可以保護特定的登錄機碼，防止使用者存取或修改登錄中的任何登錄機碼或值。您可以允許使用者檢視登錄機碼，但不能重新命名或修改登錄機碼。

若要測試此功能，請執行下列動作：

- 新增測試登錄機碼。
- 新增可以讀取但無法寫入登錄機碼的規則。
- 嘗試將新值加入到登錄機碼。

新增測試登錄機碼

1. 在用戶端電腦上，開啟指令行並輸入 `regedit`，以開啟登錄檔編輯器。
2. 在登錄檔編輯器中，展開 `HKEY_LOCAL_MACHINE\Software`，然後建立名為 `test` 的新登錄機碼。

防止使用者寫入用戶端電腦上的登錄

1. 開啟應用程式控制政策，並在「應用程式控制」窗格中按一下「新增」。
2. 在「應用程式控制規則集」的「規則」清單下方，按下「新增 > 新增規則」。
3. 在「屬性」標籤的「規則名稱」文字方塊中，輸入 `HKLM_write_not_allowed_from_regedit`。
4. 在「套用此規則至下列程序」右側，按下「新增」。
5. 在「新增程序定義」對話方塊的「要比對的程序名稱」下方，輸入 `regedit.exe`，然後按下「確定」。
6. 在「應用程式控制規則集」對話方塊的「規則」清單下方，按下「新增 > 新增條件 > 登錄存取嘗試」。
7. 在「屬性」標籤的「敘述」文字方塊中，輸入 `registry access`。
8. 在「套用此規則至下列程序」右側，按下「新增」。
9. 在「新增登錄機碼定義」對話方塊的「登錄機碼」文字方塊中，輸入 `HKEY_LOCAL_MACHINE\software\test`，然後按下「確定」。
10. 在「應用程式控制規則集」對話方塊的「動作」標籤上，按下「讀取嘗試」群組方塊中的「允許存取」、「啟用記錄」和「通知使用者」。
11. 在「通知使用者」下方，輸入「####」。
12. 在「建立、刪除或寫入嘗試」群組方塊中，按下「攔截存取」、「啟用記錄」和「通知使用者」。
13. 在「通知使用者」下方，輸入 `writing is blocked`。
14. 按下「確定」兩次，然後將政策指派給群組。
測試規則。

測試攔截寫入登錄的規則

1. 套用政策之後，在用戶端電腦的登錄檔編輯器中，展開 `HKEY_LOCAL_MACHINE\Software`。
2. 按下先前建立名為 `test` 的登錄機碼。
3. 用滑鼠右鍵按下測試機碼，然後按下「新增」，再按下「字串值」。
您應無法將新值加入到測試登錄機碼。

防止使用者寫入特定檔案

您可能會想要使用者可以檢視但無法修改檔案。例如，檔案可能包含員工應檢視但不該編輯的財務資料。

您可以建立應用程式和裝置控制規則，將檔案的唯讀存取權限授予使用者。例如，您可以新增規則，來允許您在記事本中開啟文字檔案而不允許您編輯此檔案。

新增防止使用者寫入特定檔案的規則

1. 開啟應用程式控制政策，並在「應用程式控制」窗格中按一下「新增」。
2. 在「應用程式控制規則集」的「規則」清單下方，按下「新增」>「新增規則」。

3. 在「屬性」標籤的「規則名稱」文字方塊中，輸入 `1.txt in c read allowed write terminate`。
4. 在「套用此規則至下列程序」右側，按下「新增」。
5. 在「新增程序定義」對話方塊的「要比對的程序名稱」下方，輸入 `notepad.exe`，然後按下「確定」。
6. 在「應用程式控制規則集」對話方塊的「規則」清單下方，按下「新增 > 新增條件 > 檔案和資料夾存取嘗試」。
7. 在「屬性」標籤的「敘述」文字方塊中，輸入 `file access launched`。
8. 在「套用此規則至下列程序」右側，按下「新增」。
9. 在「新增檔案或資料夾定義」對話方塊中，將 `c:\1.txt` 輸入「要比對的檔案或資料夾名稱」群組方塊的文字方塊中，然後按一下「確定」。
10. 在「應用程式控制規則集」對話方塊的「動作」標籤上，選取「讀取嘗試」群組方塊中的「允許存取」，然後勾選「啟用記錄」和「通知使用者」。
11. 在「通知使用者」下方，輸入「####」。
12. 在「建立、刪除或寫入嘗試」群組方塊中，按下「攔截存取」、「啟用記錄」和「通知使用者」。
13. 在「通知使用者」下方，輸入 `writing to block Notepad`。
14. 按兩次「確定」，然後將政策指派給用戶端電腦群組。
測試規則。

測試防止使用者寫入特定檔案的規則

1. 在用戶端電腦上，開啟「檔案總管」，找到 `c:\` 磁碟機，然後按下「檔案 > 新增 > 文字文件」。
如果您使用「記事本」建立檔案，檔案會是唯讀檔案。
2. 將檔案重新命名為 `1.txt`。
確定檔案儲存到 `c:\` 資料夾。
3. 在「記事本」中開啟 `c:\1.txt` 檔案。
您可以開啟檔案但無法編輯它。

新增和測試攔截 DLL 的規則

您可能會想防止使用者開啟特定應用程式。攔截使用者開啟應用程式的方法之一，就是攔截應用程式執行所需的 DLL。若要攔截 DLL，您可以建立攔截 DLL 載入的規則。當使用者嘗試開啟應用程式時，即無法開啟應用程式。

例如，`Msvcrt.dll` 檔案包含用來執行如 Microsoft WordPad 等多項 Windows 應用程式的程式碼。如果您新增規則來攔截用戶端電腦上的 `Msvcrt.dll`，就無法開啟 Microsoft WordPad。

NOTE

以「重視安全性」為前提撰寫的某些應用程式可能會將 DLL 植入解讀為惡意動作。請採取因應措施來攔截植入或移除 DLL。

若要新增攔截 DLL 的規則，請開啟應用程式控制政策

1. 開啟應用程式控制政策，並在「應用程式控制」窗格中按一下「新增」。
2. 在「應用程式控制規則集」的「規則」清單下方，按下「新增」>「新增規則」。
3. 在「屬性」標籤的「規則名稱」文字方塊中，輸入「##### Microsoft Wordpad」。
4. 在「套用此規則至下列程序」右側，按下「新增」。
5. 在「新增程序定義」對話方塊的「要比對的程序名稱」下方，輸入 `C:\Program Files\Windows NT\Accessories\wordpad.exe`，然後按下「確定」。
6. 在「應用程式控制規則集」對話方塊的「規則」清單下方，按下「新增」>「新增條件」>「載入 DLL 嘗試」。
7. 在「屬性」標籤的「敘述」文字方塊中，輸入「### DLL」。
8. 在「套用至下列 DLL」右側，按下「新增」。
9. 在「新增 DLL 定義」對話方塊中，將 `MSVCRT.dll` 輸入「##### DLL ##」群組方塊的文字方塊中，然後按下「確定」。
10. 在「應用程式控制規則集」對話方塊的「動作」標籤上，按下「攔截存取」、「啟用記錄」和「通知使用者」。
11. 在「通知使用者」下方，輸入「##### WordPad」。

-
- 按兩次「確定」，然後將政策指派給用戶端電腦群組。
測試規則。

測試攔截 DLL 的規則

- 在用戶端電腦上，嘗試開啟 Microsoft WordPad。

新增和測試終止程序的規則

Process Explorer 是一項工具，可顯示已開啟或載入的 DLL 程序，以及程序使用哪些資源。您也可以使用 Process Explorer 終止程序。您可以新增一項規則：如果使用者使用 Process Explorer 嘗試終止「小算盤」應用程式，即終止 Process Explorer。

新增終止程序的規則

- 開啟應用程式控制政策，並在「應用程式控制」窗格中按一下「新增」。
- 在「應用程式控制規則集」的「規則」清單下方，按下「新增」>「新增規則」。
- 在「屬性」標籤的「規則名稱」文字方塊中，輸入## Process Explorer #### calc.exe#### Process Explorer。
- 在「套用此規則至下列程序」右側，按下「新增」。
- 在「新增程序定義」對話方塊的「要比對的程序名稱」下方，輸入 procexp.exe，然後按下「確定」。
- 在「屬性」標籤的「敘述」文字方塊中，輸入### DLL。
- 在「套用此規則至下列程序」右側，按下「新增」。
- 在「新增程序定義」對話方塊中，將 **calc.exe** 輸入「#####」群組方塊的文字方塊中，然後按下「確定」。
- 在「應用程式控制規則集」對話方塊的「動作」標籤上，按下「終止程序」、「啟用記錄」和「通知使用者」。
- 在「通知使用者」下方，輸入##### procexp ## calc#procexp #####。
- 按下「確定」兩次，然後將政策指派給群組。
測試規則。

測試終止程序的規則

- 在用戶端電腦上，從下列網址下載並執行免費版本的 Process Explorer：
[Process Explorer](#)
- 在 Windows 中開啟「小算盤」。
- 開啟 Process Explorer。
- 在 **Process Explorer** 視窗中，用滑鼠右鍵按下 calc.exe 程序，然後按下 **Kill Process**。
Process Explorer 即會終止。

測試預設 IPS 政策

若要測試預設 IPS 政策，您必須先觸發用戶端電腦上的事件。

測試預設 IPS 政策

- 重新命名可執行檔 (.exe) 為 jpeg (.jpg)。
- 將 .jpg 檔案上傳到 Web 伺服器\站台。
- 在用戶端電腦上，使用網頁瀏覽器開啟重新命名的可執行檔。

NOTE

若要開啟重新命名的可執行檔，您必須使用 IP 位址存取 Web 伺服器\站台。例如，您可以輸入：
http://Web ### IP ##/#####.jpg

4. 如果用戶端上的 IPS 政策運作正常，會發生下列事件：

- 您應無法開啟 .jpg 檔案。
- 通知區域圖示中的訊息指出用戶端已攔截 .jpg 檔案。
- 您可以開啟安全日誌並尋找指出用戶端已攔截 .jpg 檔案的日誌項目。

管理用戶端伺服器連線

請確定管理伺服器將內容提供給用戶端。

安裝用戶端後，管理伺服器會自動連線到用戶端電腦。

Table 124: 管理伺服器和用戶端之間的連線管理工作

動作	說明
檢查用戶端是否連線至管理伺服器	您可以在用戶端與管理主控台中檢查用戶端狀態圖示。狀態圖示會顯示用戶端和伺服器之間是否通訊。請參閱： 檢查用戶端是否已連線至管理伺服器且受保護 電腦可能已安裝用戶端軟體，但沒有正確的通訊檔案。請參閱： 用戶端電腦和管理伺服器的通訊方式？ 如何在用戶端電腦上取代用戶端伺服器通訊檔案？
檢查用戶端是否取得政策更新	檢查用戶端和管理主控台的政策序號，確認用戶端電腦是否取得最新的政策更新。如果用戶端能夠與伺服器進行通訊，並且接收定期的政策更新，則政策序號應該相符。您可以執行手動政策更新，然後比對政策序號。請參閱： 使用政策序號檢查用戶端伺服器通訊 更新用戶端政策
變更用來下載政策與內容至用戶端的方式	您可以將管理伺服器架構為推送政策至用戶端，或由用戶端提取管理伺服器的政策。請參閱： 使用推送模式或提取模式更新用戶端上的政策和內容
決定是否使用預設的管理伺服器清單	您可以針對容錯移轉和負載平衡使用其他管理伺服器清單。管理伺服器清單可提供用戶端可連線至多個管理伺服器的清單資訊。請參閱： 架構用於負載平衡的管理伺服器清單
架構位置的通訊設定	您可以針對位置和群組分別架構通訊設定。請參閱： 架構位置的通訊設定
排除管理伺服器連線問題	若管理伺服器與用戶端無法連線，您可以解決兩者連線的問題。請參閱： Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解

如需詳細資訊，請參閱下列文章：

[關於 Symantec Endpoint Protection 所使用的通訊埠](#)

改善用戶端和伺服器效能

Symantec Endpoint Protection Manager 包含各種功能，可用於提升用戶端效能和伺服器效能，同時仍維持高度安全性。

Table 125: 可改善伺服器 and 用戶端效能的工作

工作	說明
變更用戶端伺服器通訊設定	使用提取模式取代推送模式，控制管理伺服器下載政策和內容更新至用戶端電腦的頻率。在提取模式中，管理伺服器可支持更多用戶端。 增加活動訊號間隔，降低用戶端和伺服器間的通訊頻率。如果每部伺服器服務的用戶端數目少於 100，可將活動訊號間隔時間增加為 15-30 分鐘。如果為 100 至 1,000 個用戶端，請將活動訊號間隔時間增加為 30-60 分鐘。更大的網路可能需要更長的活動訊號間隔時間。將下載隨機設定增加為活動訊號間隔時間的一到三倍。請參閱： 使用推送模式或提取模式更新用戶端上的政策和內容 如需設定活動訊號間隔的詳細資訊，請參閱下列白皮書： Symantec Endpoint 規模設定及擴充性最佳實務
隨機選擇並減少內容更新次數	內容更新的大小和頻率各有不同，實際取決於內容類型和可用性。您可以使用下列方式，減少下載及匯入完整內容更新集的影響： - 將用戶端負載分散到多部管理伺服器。請參閱： 架構用於負載平衡的管理伺服器清單 - 使用其他方式來派送內容，如「群組更新提供者」或第三方派送工具。 「群組更新提供者」可將伺服器的處理負載轉移到下載內容的用戶端，協助您保留頻寬。請參閱： 使用群組更新提供者將內容散佈至用戶端 使用第三方派送工具更新用戶端電腦 - 隨機選擇 LiveUpdate 下載內容到用戶端電腦的時間。請參閱： 從 LiveUpdate 伺服器隨機進行內容下載 從預設管理伺服器或群組更新提供者隨機進行內容下載 - 在使用者不主動使用用戶端電腦時下載內容更新。請參閱： 將 Windows 用戶端更新架構為在用戶端電腦閒置時執行
調整掃描以改善電腦效能	您可以變更某些掃描設定，在不降低防護能力的情況下，改善電腦效能。 例如，您可以將掃描架構為忽略信任的檔案或在電腦閒置時執行。請參閱： 調整掃描以改善電腦效能 自訂 Windows 用戶端的自動防護 進階掃描與監控
減少資料庫用戶端日誌量	您可以架構記錄選項，以最佳化儲存需求並符合公司控制保留記錄資料的政策。 資料庫會接收持續產生的項目，並將項目儲存到日誌檔案中。您必須管理儲存在資料庫中的資料，以確保儲存的資料不會耗盡所有可用的磁碟空間。資料過多時，會造成執行資料庫的電腦當機。 您可以執行下列工作，來減少日誌資料量： - 只將部分用戶端日誌上傳至伺服器，以及變更上傳用戶端日誌的頻率。請參閱： 指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器 - 指定用戶端電腦在資料庫中可保留的日誌項目數，以及可保留多久的時間。請參閱： 指定日誌大小以及在資料庫中保留日誌項目的時間長度 - 過濾掉重要性較低的風險事件和系統事件，減少轉送到伺服器的資料。請參閱： 在 Windows 電腦上修改日誌處理及通知設定 - 減少各管理伺服器所管理的用戶端數目。請參閱： 架構用於負載平衡的管理伺服器清單 安裝 Symantec Endpoint Protection Manager - 減少活動訊號頻率，這會控制用戶端日誌多久上傳一次到伺服器。請參閱： 使用推送模式或提取模式更新用戶端上的政策和內容 - 在將日誌資料寫入資料庫之前，增加儲存日誌資料之目錄的硬碟空間。請參閱： 關於增加用於用戶端日誌資料的伺服器磁碟空間
執行資料庫維護工作	為提高用戶端與伺服器間的通訊速度，您應該排程定期的資料庫維護工作。請參閱： 排程自動資料庫維護工作

關於伺服器憑證

憑證是用於驗證和加密敏感資料的產業標準。若要防止傳送通過網路中路由器的資訊，應該對資料進行加密。

為了與用戶端通訊，管理伺服器會使用伺服器憑證。為了讓管理伺服器利用伺服器憑證識別並驗證自己，Symantec Endpoint Protection Manager 預設會加密資料。不過，某些情況下，您必須停用伺服器與用戶端之間的加密。請參閱：

[在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證](#)

基於安全起見，您可能也會想要備份憑證。如果管理伺服器損壞，或是您忘記了密鑰儲存密碼，便可以輕易的擷取該密碼。請參閱：

- [備份伺服器憑證](#)
- [更新或還原伺服器憑證](#)
- [產生新的伺服器憑證](#)

管理伺服器支援下列的憑證類型：

- JKS 金鑰儲存檔案 (.jks) (預設)
Java 工具 keytool.exe 會產生密鑰儲存檔案。Java Cryptography Extension (.jceks) 格式需要有特定版本的 Java Runtime Environment (JRE)。管理伺服器僅支援使用與管理伺服器上 Java Development Kit 相同版本所產生的 .jceks 密鑰儲存檔案。
這個金鑰儲存檔案必須包含憑證及私密金鑰。密鑰儲存密碼必須與金鑰密碼相同。您可以在以下檔案中找到密碼：
SEPM_Install\Server Private Key Backup\recovery_timestamp.zip
SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。
- PKCS12 金鑰儲存檔案 (.pfx 或 .p12)
- 憑證和私密金鑰檔案 (.der 或 .pem 格式)
賽門鐵克支援 .der 或 .pem 格式的未加密憑證及私密金鑰，不支援 Pkcs8 加密的私密金鑰。

NOTE

當 Symantec Endpoint Protection 用戶端連接至管理伺服器且您看到以下 cURL 錯誤：##### 。這可能是憑證 / PKI 問題造成的，例如以 [CRL 強制檢查的錯誤架構 AIA/CDP 副檔名](#)。

接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證

當您安裝 Symantec Endpoint Protection Manager 時，呈現於瀏覽器中的網頁自我簽署憑證會包含在安裝裡。當您第一次從遠端主控台存取這些網頁時，您必須接受自我簽署憑證，才能顯示管理伺服器網頁。

Warning - Security

×

Server Certificate is not present in your trusted store.
Do you want to trust the certificate?

Certificate Info:

Version:

3

Subject:

Issuer:

MGMT CA

Serial No:

Valid From:

23. februar 2023

Valid To:

22. februar 2025

Signature Algorithm:

SHA512withRSA

Public Key Algorithm:

RSA

Fingerprint:

D8EE

Subject Alternative Names:

Other Name: : 0000 - 30 2b 06 0a
DNS Name: :

More Details..

Accept

Accept Always

Reject

Help

會為每位使用者單獨儲存憑證。每個管理員帳戶都必須為每個連線到管理伺服器的遠端位置接受憑證。

接受憑證

- 按一下「接受」或「一律接受」。

根據預設，本機主控台會信任管理伺服器的憑證。但是在遠端管理主控台上，每次 Symantec Endpoint Protection Manager 登入嘗試都可能會持續顯示該訊息。

NOTE

如果拒絕該憑證，您可能會在登入 Symantec Endpoint Protection Manager 時看到一則錯誤訊息。這個情況通常是因為複寫夥伴的管理員不接受憑證。

部分事件 (如主機名稱與憑證通用名稱 (CN) 不相符) 會導致 Java 密鑰儲存 (預設位於 \tomcat\etc) 中的憑證不受信任。該提示應允許您將憑證新增到 Java 密鑰儲存，但是檔案存取問題可以避免發生此情況。請參閱 Windows (%temp%) 使用者暫存目錄的 scm-ui log 以瞭解詳情。

如需瞭解如何將安全憑證新增至 Web 瀏覽器，您需要先將管理員的憑證安裝為受信任的根 CA。請參閱：

[使用 Web 瀏覽器來檢視 Endpoint Protection 管理員主控台時發生憑證錯誤](#)

更多資訊

[登入 Symantec Endpoint Protection Manager 主控台](#)

在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證

Symantec Endpoint Protection Manager 使用憑證來驗證其與 Symantec Endpoint Protection 用戶端之間的通訊。該憑證亦會數位簽署用戶端從中下載的政策檔案和安裝套件。用戶端將在管理伺服器清單中儲存憑證的快取複本。如果憑證損毀或無效，用戶端就無法與伺服器通訊。

如果您停用安全通訊，則用戶端仍然可與伺服器進行通訊，但不會驗證來自管理伺服器的通訊。更新憑證且用戶端登入並接收到該憑證之後，再次啟用安全通訊。

如果管理伺服器確實中斷了與用戶端的通訊，請使用通訊更新套件還原遺棄用戶端。

[使用「通訊更新套件部署」還原用戶端伺服器通訊](#)

[使用 SylinkDrop 工具還原用戶端伺服器通訊設定](#)

在單一管理伺服器上更新伺服器憑證

在網站的單一管理伺服器上更新伺服器憑證

1. 在主控台中，按一下「政策」>「政策元件」>「管理伺服器清單」。
 2. 在「工作」下方，按下「複製清單」，然後按下「貼上清單」。
 3. 右鍵按下清單的副本，按「分配」，選擇與原始清單相同的群組，然後按「分配」。
 4. 按一下「用戶端 > 政策 > 一般」。
 5. 針對所有群組，在「安全性設定」標籤中，取消勾選「使用數位憑證進行驗證，以啟用管理伺服器與用戶端之間的安全通訊」，然後按一下「確定」。
- 即使您通常不會使用 HTTPS，也必須執行此步驟。

NOTE

請確定您同樣針對未繼承父群組的群組架構此設定。

6. 請等待至少 24 小時或更長時間，然後再繼續下一步。
建議等待一週，盡量讓更多用戶端從管理伺服器下載新的通訊詳細資料。如果過早更新憑證會孤立客戶端，您必須使用通訊更新套件手動重新連接它們。
7. 更新伺服器憑證。
[更新或還原伺服器憑證](#)
8. 按一下「確定」。
若要重新啟用原始設定，請等待至少 24 小時，然後重新勾選「使用數位憑證進行驗證，以啟用管理伺服器與用戶端之間的安全通訊」，並將原始管理伺服器清單重新指派回您的群組。

在多個管理伺服器上更新伺服器憑證

在具有多個管理伺服器的站台上更新憑證以及使用容錯移轉或負載平衡時，該憑證會在管理伺服器清單中進行更新。在執行容錯移轉或負載平衡程序期間，用戶端接收到更新的管理伺服器清單和新憑證。

WARNING

由於通訊模組發生變更，僅用戶端版本 14.2/14.2.1 無法使用此方法來更新伺服器憑證。若要避免中斷與這些用戶端的通訊，請針對這些用戶端版本 (甚至針對多重管理伺服器網站) 使用單一管理伺服器網站程序。

更新多個管理伺服器站台上的伺服器憑證

1. 在主控台中，請確保您的用戶端已架構為負載平衡或容錯移轉到至少一個其他 Symantec Endpoint Protection Manager。

[設定容錯移轉和負載平衡](#)

如果您無法啟用負載平衡或容錯移轉，請使用單一管理伺服器網站程序，以先後停用並重新啟用安全通訊。

WARNING

由於通訊模組發生變更，僅用戶端版本 14.2/14.2.1 無法使用此方法來更新伺服器憑證。若要避免中斷與這些用戶端的通訊，請針對這些用戶端版本 (甚至針對多重管理伺服器網站) 使用單一管理伺服器網站程序。

2. 更新 Symantec Endpoint Protection Manager 上的伺服器憑證。
[更新或還原伺服器憑證](#)
3. 等待至少三個活動訊號週期，然後在網站上更新下一個 Symantec Endpoint Protection Manager 上的伺服器憑證。
4. 重複步驟 2 和 3，直到網站上的每個 Symantec Endpoint Protection Manager 都具有新憑證為止。

NOTE

由於外出或正在休假的使用者的裝置處於離線狀態，因此可能無法接收這些更新。許多機構會執行容錯移轉方法 30 天或以上，以盡可能擷取多個外出用戶端。您可能想要使用舊憑證讓一個 Symantec Endpoint Protection Manager 持續執行 90 天，以確保這些使用者不會被孤立。

有關更多詳細資訊，請參閱：[伺服器憑證說明](#)

更新或還原伺服器憑證

伺服器憑證會對伺服器與用戶端間的檔案進行加密和解密。用戶端會利用加密金鑰，連線至伺服器、下載檔案，然後對金鑰進行解密，以驗證其可信度。如果您變更伺服器上的憑證，而沒有手動更新用戶端，則伺服器與用戶端間的加密連線將會中斷。此問題稱為遺棄用戶端。

NOTE

當嘗試使用「管理伺服器憑證精靈」更新 Symantec Endpoint Protection Manager (SEPM) 憑證時，您可能會看到下列錯誤：「#####。」SEPM 可能在處理檔案時遇到錯誤，或憑證無效。請參閱：[在 Endpoint Protection Manager 憑證更新期間發生錯誤「無效的私密金鑰檔案 \[0x840b0000\]」](#)

我何時該更新伺服器憑證？

下列情況下，您必須更新伺服器憑證：

- 不使用還原檔案的情況下，重新安裝 Symantec Endpoint Protection Manager。更新憑證以還原用戶端已使用的先前憑證。請參閱：[安裝 Symantec Endpoint Protection Manager](#)
- 將某一部管理伺服器取代為另一部管理伺服器，並且使用相同的 IP 位址和伺服器名稱。
- 在災難復原之後，套用了錯誤的伺服器憑證 (.JKS)。
- 購買了不同的憑證，想要使用該憑證來取代預設的 .JKS 憑證。請參閱：[關於伺服器憑證](#)

匯入伺服器憑證之前

在步驟 6 中匯入新憑證之前，您必須：

- 中斷遠端複製關係 (非必要)。如果要更新的管理伺服器會透過其他管理伺服器進行遠端複製，請中斷遠端複製關係。請參閱：[在升級前後停用遠端複製和還原遠端複製](#)
- 停用伺服器憑證驗證。當您停用驗證時，用戶端會在伺服器更新伺服器憑證時保持連線。
[在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證](#)
根據下列因素而定，部署更新政策的程序可能需要一週或更長的時間：
 - 連線到管理伺服器的用戶端數目。大型安裝可能需要數天才能完成此程序，因為受管電腦必須上線才能接收新政策。
 - 某些使用者可能正在休假，而其電腦為離線狀態。
- 確認新憑證有效。
- 確認新憑證中的伺服器名稱與現有憑證所列的主旨備用名稱 (SAN) 相符。
如果伺服器名稱是無效的主機名稱、完全合格網域名稱 (FQDN) 或 IP 位址，或者如果它與伺服器憑證中列出的主旨備用名稱 (SAN) 之一不相符，則必須重新命名伺服器或更新伺服器憑證。
[疑難排解：「您的伺服器憑證無效，因為電腦主機名稱或 IP 位址已變更」\(14.3 RU8 或更新版本\)](#)

更新伺服器憑證

更新或還原伺服器憑證

- 在主控台中，按下「管理員」，再按「伺服器」。

2. 在「伺服器」的「本機網站」下方，按下您要更新伺服器憑證的管理伺服器。
3. 在「工作」下方，按一下「管理伺服器憑證」，然後按「下一步」。
4. 在「管理伺服器憑證」面板中，按下「更新伺服器憑證」，然後按「下一步」。
5. 當您看到以下訊息：#####，請選擇以下任一選項：
 - 如果需要完成以下任務，請按「否」>「取消」。
 - 暫時停用伺服器驗證。
 - 確認新憑證中的伺服器名稱與現有憑證相符。
[疑難排解：「您的伺服器憑證無效，因為電腦主機名稱或 IP 位址已變更」\(14.3 RU8 或更新版本\)](#)
完成這些任務之後，請重新啟動該過程。
 - 如果您已完成這些任務，請按「是」。
6. 在「更新伺服器憑證」面板中，選擇您要匯入的憑證類型，然後按「下一步」。
7. 針對每種憑證類型，按照面板上的指示操作，然後按下「完成」。
備份伺服器憑證位於 <SEPM_Install>\Server Private Key Backup\recovery_timestamp.zip。
您可以在相同的 .zip 檔案內的 settings.properties 檔案中，找到金鑰儲存檔案的密碼。密碼出現在 keystore.password= 行。
SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。
8. 重新啟動下列服務以使用新的憑證：
 - Symantec Endpoint Protection Manager 服務
 - Symantec Endpoint Protection Manager Webserver 服務。
 - Symantec Endpoint Protection Manager API 服務
 - [停止及啟動管理伺服器服務](#)
 - [停止和啟動 Apache Web 伺服器](#)
9. 重新啟動伺服器憑證驗證。
10. (選擇性)。如果在環境中使用複寫，請還原複寫關係。

更多資訊：

[疑難排解伺服器名稱不符伺服器憑證時，Symantec Endpoint Protection Manager 會封鎖您登入或升級 \(14.3 RU9 或更新版本\)](#)

[Symantec Endpoint Protection Manager 偵測到配置的複寫夥伴需要停用主機名稱驗證 \(14.3 RU9 或更新版本\)](#)

檢查用戶端是否已連線至管理伺服器且受保護

在您安裝用戶端後，請檢查用戶端是否為線上狀態且已連線至 Symantec Endpoint Protection Manager。您可以在主控台和用戶端上檢查連線狀態。

檢查 **Symantec Endpoint Protection** 用戶端上的用戶端管理伺服器連線

1. 在用戶端電腦上，執行下列其中一項工作：
 - 電腦工作列中的用戶端保護盾帶有綠點：
 - 開啟用戶端並查看「狀態」畫面，其指出「您的電腦已受到防護」並顯示綠色核取記：
 - 開啟用戶端並按下「說明」>「疑難排解」。

如需詳細資訊，請參閱：[Symantec Endpoint Protection 用戶端狀態圖示](#)

在 **Symantec Endpoint Protection Manager** 中檢查用戶端管理伺服器連線

1. 在主控台中，按下「用戶端」，然後選取目標群組。

2. 在「用戶端」標籤上，已連線的用戶端在「名稱」欄中會顯示帶有綠點的圖示，並顯示「線上」運作狀態：

NOTE

透過 Symantec Endpoint Protection Manager 連線的用戶端可能不會立即在雲端主控台中顯示正確的線上狀態。在線上狀態變更後，可能需要 5-10 分鐘才能看到目前狀態的準確反映。

Table 126: 管理主控台中的用戶端狀態圖示，位於「用戶端」>「用戶端」標籤>「名稱」欄

圖示	說明
	用戶端軟體安裝失敗。
	- 用戶端能夠與 Symantec Endpoint Protection Manager 進行通訊。運作狀態為「線上」。 - 用戶端處於電腦模式。
	- 用戶端無法與 Symantec Endpoint Protection Manager 進行通訊。運作狀態為「離線」。 - 用戶端處於電腦模式。 - 可能已使用主控台新增用戶端，但可能尚未安裝任何 Symantec 用戶端軟體。
	- 用戶端能夠與 Symantec Endpoint Protection Manager 進行通訊。 - 用戶端處於電腦模式。 - 用戶端為非受管偵測程式。
	- 用戶端無法與 Symantec Endpoint Protection Manager 進行通訊。 - 用戶端處於電腦模式。 - 用戶端為非受管偵測程式。
	- 用戶端能夠與 Symantec Endpoint Protection Manager 進行通訊。 - 用戶端處於使用者模式。
	- 用戶端無法與 Symantec Endpoint Protection Manager 進行通訊。 - 用戶端處於使用者模式。 - 可能已使用主控台新增用戶端，但可能尚未安裝任何 Symantec 用戶端軟體。
	- 用戶端能夠與另一站台上的 Symantec Endpoint Protection Manager 進行通訊。 - 用戶端處於電腦模式。
	- 用戶端能夠與另一站台上的 Symantec Endpoint Protection Manager 進行通訊。 - 用戶端處於電腦模式。 - 用戶端為非受管偵測程式。
	- 用戶端能夠與另一站台上的 Symantec Endpoint Protection Manager 進行通訊。 - 用戶端處於使用者模式。

更多資訊

[檢視用戶端電腦的防護狀態](#)

Symantec Endpoint Protection 用戶端狀態圖示

您可以檢查用戶端上的通知區圖示，判斷用戶端是否連線至管理伺服器以及獲得適當保護。通知區域圖示有時又稱為系統匣圖示。

該圖示位於用戶端電腦桌面的右下角。您還可以滑鼠右鍵按下此圖示，顯示常用指令。

NOTE

在受管用戶端上，如果管理員已架構為不能使用，則通知區域圖示不會出現。

[允許使用者變更 Symantec Endpoint Protection 用戶端使用者介面的設定](#)

Table 127: 用戶端狀態圖示

圖示	說明
	用戶端執行時未發生問題。該用戶端可能離線或為非受管用戶端。非受管用戶端並未連線到管理伺服器。
	用戶端執行時未發生問題。該用戶端已連線到伺服器，並與其通訊。安全性政策的所有元件都可防護電腦。
	用戶端發生次要問題。例如，病毒定義檔可能過期。
	用戶端未執行、發生了重大問題、具有過期的授權，或至少有一個防護技術停用。

更多資訊

- [顯示或隱藏 Symantec Endpoint Protection 用戶端上的通知區域圖示](#)
- [瞭解 Symantec Endpoint Protection 用戶端狀態頁面](#)

使用政策序號檢查用戶端伺服器通訊

若要檢查伺服器和用戶端是否通訊，請檢查主控台和用戶端上的政策序號。如果用戶端與管理伺服器進行通訊，並且接收定期的政策更新，則序號應該相符。

如果政策序號不符，您可以嘗試在用戶端電腦上手動更新政策，並且檢查疑難排解日誌。請參閱：

- [更新用戶端政策](#)
- [使用推送模式或提取模式更新用戶端上的政策和內容](#)

檢視主控台中的政策序號

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，選取相關群組。

NOTE

政策序號與政策日期還會顯示在「詳細資料」標籤上的詳細資料清單的底部。

檢視用戶端電腦上的政策序號

1. 在用戶端電腦上的用戶端中，按下「說明 > 疑難排解」。
2. 在「管理」標籤上，找到政策序號。
此序號應與用戶端電腦所在群組的主控台上的序號相符合。

更多資訊

[執行適用於所有政策的工作](#)

使用推送模式或提取模式更新用戶端上的政策和內容

什麼是提取模式和推送模式？

當您在管理伺服器上架構政策時，必須將已更新的政策下載至用戶端電腦。您可以在主控台中將用戶端電腦架構為使用以下任一更新方法：

提取模式	用戶端電腦會根據活動訊號設定的頻率，定期連線至管理伺服器。用戶端電腦會在用戶端連線時檢查管理伺服器的狀態。
推送模式	用戶端電腦會與管理伺服器建立持續的 HTTPS 連線。只要管理伺服器狀態變更，就會立刻通知用戶端電腦。

無論使用哪一種模式，用戶端電腦都會根據管理伺服器狀態的變更來採取相對應的動作。由於必須持續連線的關係，推送模式需要較大的網路頻寬。架構為使用提取模式的用戶端電腦需要較小的頻寬。

活動訊號通訊協定定義用戶端電腦上傳資料的頻率，例如上傳日誌項目和下載政策等。用戶端啟動後會立刻出現首次活動訊號。依照您所設定的活動訊號頻率會出現下次活動訊號。

活動訊號頻率是決定 Symantec Endpoint Protection Manager 可支援多少個用戶端的重要因素。如果您將活動訊號頻率設為 30 分鐘 (含) 以下，那麼 Symantec Endpoint Protection Manager 可支援的用戶端總數就會受限制。如果部署的用戶端數為 1,000 或更多，賽門鐵克建議盡可能地將活動訊號頻率設定為最長時間。賽門鐵克建議您使用仍符合公司安全性需求的最長時間間隔。例如，如果您想要每天更新政策並收集日誌，則可能會將活動訊號頻率設定為 24 小時。評估您網路環境所需的正確組態、硬體及網路架構。

NOTE

您也可以可以在用戶端電腦上手動更新政策。

更多資訊：

- [使用政策序號檢查用戶端伺服器通訊](#)
- [Symantec Endpoint Protection 的通訊埠](#)

架構群組或位置的推送模式或提取模式

可以指定是 Symantec Endpoint Protection Manager 將政策下推至用戶端，還是用戶端從 Symantec Endpoint Protection Manager 提取政策。預設設定為推送模式。若選取提取模式，則依據預設，用戶端每隔五分鐘就會連線到管理伺服器，但可以變更此預設活動訊號間隔。

可以設定群組或位置的模式。

架構群組的推送或提取模式

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，選取您要為其指定推送或提取政策的群組。
3. 按下「政策」。
4. 取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
5. 在「與位置無關的政策與設定」窗格的「設定」下方，按下「通訊設定」。
6. 在「群組名稱 的通訊設定」對話方塊中，確認已勾選「下載」下方的「從管理伺服器下載政策和內容」。
7. 執行下列其中一項工作：
 - 按一下「推送模式」。
 - 按一下「提取模式」，然後在「活動訊號間隔時間」下方，設定分鐘數或小時數。
8. 按一下「確定」。

為位置指定推送模式或提取模式

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，選取您要為其指定推送或提取政策的群組。
3. 按下「政策」。
4. 取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
5. 在「位置限定的政策與設定」下方，針對要修改的位置找出「位置限定的政策」，然後展開「位置限定的設定」。
6. 在「位置限定的設定」下方，按下「通訊設定」右側的「工作」，然後取消勾選「使用群組通訊設定」。
7. 在「通訊設定」的右側，按下「本機 - 推送」或 (「本機 - 提取」)。
8. 執行下列其中一項工作：
 - 按一下「推送模式」。
 - 按一下「提取模式」，然後在「活動訊號間隔時間」下方，設定分鐘數或小時數。
9. 按一下「確定」。

用戶端電腦和管理伺服器的通訊方式？

Symantec Endpoint Protection Manager 使用通訊檔 Sylink.xml 連線至用戶端。Sylink.xml 檔案含有通訊設定，例如，管理伺服器的 IP 位址和活動訊號間隔。在您安裝用戶端套件到用戶端電腦後，用戶端和伺服器會自動通訊。

Sylink 檔案會在活動訊號期間執行大多數功能。活動訊號是用戶端電腦將日誌上傳到管理伺服器，並下載政策和指令的頻率。

Sylink 檔案包含：

- 所有管理伺服器的公開憑證。
- KCS 或加密金鑰。
- 每個用戶端所屬的網域 ID。

NOTE

請勿編輯 Sylink 檔案。如果您變更設定，管理伺服器會在用戶端下次連線至管理伺服器時覆寫大部分設定。

如需詳細資訊，請參閱：

[使用推送模式或提取模式更新用戶端上的政策和內容](#)

疑難排解 Sylink 通訊

在版本 14.2 中，通訊模組已升級，並包含新的日誌檔。您可以使用此資訊來疑難排解 Symantec Endpoint Protection Manager 與用戶端之間的通訊問題。

14.2 通訊模組適用於所有用戶端類型 (包括 Windows、Mac 和 Linux)，並且已改進 IPv6 支援。

NOTE

自 14.2 版起，通訊模組僅遵守系統代理資訊。

檢視通訊模組的日誌檔

1. 在 Windows 用戶端上的下列資料夾中：

`C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data`

您可以檢視下列檔案：

– 對於用戶端註冊：

- `RegistrationInfo.xml`
用戶端提交至 Symantec Endpoint Protection Manager 的用戶端註冊中繼資料。
- `Registration.xml`
Symantec Endpoint Protection Manager 傳回用戶端的用戶端註冊中繼資料。
- `State.xml`
包含內部設定，例如管理伺服器 IP 位址。

– 對於通訊模組日誌：

`\Logs\cve.log` 和 `\Logs\cve-actions.log`

您可以使用這些日誌來疑難排解 Symantec Endpoint Protection Manager 與用戶端之間的通訊。如果系統要求，請將這些日誌傳送至技術支援。

– 對於 **Opstate** 狀態：

顯示在 `\Pending` 和 `\Sent` 資料夾中的日誌中

架構通訊模組日誌

1. 開啟 Windows 登錄編輯程式，並按一下「開始 > 執行」，再輸入 `regedit`，然後按一下「確定」。

2. 若要啟用 `cve.log` 或 `cve-actions.log`，請開啟下列 Windows 登錄機碼：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink  
REG_DWORD: CVELogLevel
```

使用下列任一值：

- 1 = 除錯
- 2 = 告知
- 3 = 警告
- 4 = 錯誤
- 5 = 嚴重

如果登錄機碼不存在或不具有有效值，則預設值為 4。安裝預設值也是 4。

例如，您可以輸入：

- 32 位元：[HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink]
"CVELogLevel"=dword:00000001
- 64 位元 (14.3 RU4 或更早版本)：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection
- 64 位元 (14.3 RU5 或更高版本)：[HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] "CVELogLevel"=dword:00000001

3. 若要控制這些日誌的大小，請使用下列登錄值：

[HKEY_LOCAL_MACHINE\SOFTWARE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] REG_DWORD: CVELogSizeDB

預設大小為 250 MB。

更多資訊

- [如何在 Endpoint Protection 14.2 中啟用通訊模組記錄](#)
- [如何針對 Endpoint Protection 用戶端啟用 Sylink 除錯 \(14.1 及更早版本\)](#)

在用戶端電腦上取代用戶端伺服器通訊檔案

何時應在用戶端電腦上取代用戶端伺服器通訊檔案？

通常您不需要取代 Sylink.xml 檔案。不過，您應在下列情況下取代用戶端電腦上的現有 Sylink.xml 檔案：

- 用戶端和管理伺服器無法通訊如需瞭解如何檢查通訊，請參閱：
[在用戶端電腦上檢查與管理伺服器的連線](#)
- 您想要將非受管用戶端轉換成受管用戶端。如果使用者從安裝檔案安裝用戶端，該用戶端即為非受管用戶端，不會與管理伺服器進行通訊。請參閱：
[關於受管和非受管用戶端](#)
[如何將適用於 Macintosh 用戶端的非受管 Symantec Endpoint Protection 轉換為受管](#)
您也可以再在電腦上重新安裝用戶端軟體成為受管電腦。
- 您必須重新連接先前遺棄的用戶端。例如，如果安裝在管理伺服器上的硬碟損毀，您必須重新安裝管理伺服器。更新 Sylink 檔案時，遺棄用戶端會與管理伺服器重新建立通訊。
如需瞭解遺棄用戶端，請參閱：[在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證](#)

在用戶端電腦上取代用戶端伺服器通訊檔案的方式

NOTE

從 14.3 RU10 開始，您必須使用預設用戶端密碼或群組層級密碼，才能將 Sylink.xml 檔案匯入至用戶端。

若要在用戶端電腦上取代用戶端伺服器通訊檔案 (Sylink.xml)，您可以使用以下任一方法：

- 在用戶端電腦上重新部署用戶端安裝套件。如果在大型環境中手動匯入 Sylink.xml 是實際無法進行的作業，且要求管理存取權時，請使用這個方法。請參閱：
[使用「通訊更新套件部署」還原用戶端伺服器通訊](#)
- 寫入執行 SylinkDrop 工具的指令碼。

針對多個用戶端使用 SylinkDrop，或如果您使用軟體管理工具下載用戶端軟體到電腦。軟體管理工具的優點是，只要一般使用者開啟用戶端電腦，它就會下載 Sylink.xml 檔案。相較之下，用戶端安裝套件只會在用戶端電腦連線至管理伺服器時，才會下載新的 Sylink.xml 檔案。請參閱：

[使用 SylinkDrop 工具還原用戶端伺服器通訊設定](#)

- 使用「匯出通訊設定」命令以將 Sylink.xml 檔案匯出至用戶端電腦，然後手動在用戶端電腦上將其匯入。如果您想要使用軟體管理工具，您應使用此方法。利用軟體管理工具，只要使用者啟動電腦，工作就會佇列並完成。使用其他方法時，用戶端電腦將必須連線。請參閱：

[手動匯出用戶端伺服器通訊檔案 \(Sylink.xml\)](#)

- 使用「匯出通訊設定」指令以將 Sylink.xml 檔案匯出至用戶端電腦，然後使用下列指令以手動在用戶端電腦上將其匯入：`smc -importsylink -p <password> <sylinkpath>` 請參閱：

[手動匯出用戶端伺服器通訊檔案 \(Sylink.xml\)](#)

不論您使用哪種方式，用戶端都會立即連線至管理伺服器。管理伺服器會將用戶端放置於通訊檔案中指定的群組。用戶端會以群組的政策和設定進行更新。用戶端與管理伺服器進行通訊之後，用戶端電腦工作列將顯示帶有綠點的通知區域圖示。請參閱：

[檢查用戶端是否已連線至管理伺服器且受保護](#)

更多資訊

- [用戶端與伺服器通訊檔案](#)
- [用戶端電腦和管理伺服器的通訊方式？](#)

使用 SylinkDrop 工具還原用戶端伺服器通訊設定

Sylink.xml 檔案包含用戶端與 Symantec Endpoint Protection Manager 伺服器之間的通訊設定。如果用戶端失去與管理伺服器之間的通訊，則必須使用新的 Sylink.xml 檔案來取代舊的 Sylink.xml 檔案。SylinkDrop 工具會自動使用新的 Sylink.xml 檔案來取代 Windows 用戶端電腦上的 Sylink.xml 檔案。

如需瞭解替換用戶端電腦的其他方法，請參閱：[在用戶端電腦上取代用戶端伺服器通訊檔案](#)

替換現有 Sylink 檔案時，該檔案也可以執行以下任務：

- 將用戶端移轉/移動至新的網域或管理伺服器。
- 將無法在管理伺服器上修正的通訊損壞還原至用戶端。
- 將用戶端從一台伺服器移至另一台非遠端複製夥伴的伺服器。
- 將用戶端從一個網域移至另一個網域。
- 將非受管用戶端轉換為受管用戶端。

在管理伺服器上，您可以在 `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools\SylinkDrop` 找到 SylinkDrop 工具。

您可以遠端執行工具，或是先儲存該工具，然後再於用戶端電腦執行該工具。在 14.3 RU4 及更舊版本中，SylinkDrop 工具安裝在用戶端電腦上。

使用 SylinkDrop 工具還原用戶端伺服器通訊設定

1. 在管理主控台中，將連線至管理伺服器的群組通訊檔案匯出至您要用戶端電腦進行連線的伺服器。通訊檔案為 Sylink.xml 檔案。請參閱：
[手動匯出用戶端伺服器通訊檔案 \(Sylink.xml\)](#)
2. 將 Sylink.xml 檔案複製到用戶端電腦。
您可以將檔案儲存到網路位置、透過電子郵件傳送給用戶端電腦的使用者，或是複製到卸除式媒體。
3. 開啟 SylinkDrop 工具，然後按「流覽」找出您在步驟 2 中部署至用戶端電腦的 .xml 檔案。
4. 按下「更新 Sylink」。
5. 在 14.3 RU10 和更高版本中，於「密碼」對話方塊中輸入用戶端密碼，然後按一下「確定」。
6. 您看見確認對話方塊時，請按下「確定」。

7. 在 **Sylink Drop** 對話方塊中，按下「結束」。

使用「通訊更新套件部署」還原用戶端伺服器通訊

如果用戶端伺服器通訊中斷，則您可以部署通訊更新套件，透過取代用戶端電腦上的 Sylink.xml 檔案來快速還原通訊。

請將此方法用於許多電腦、您實際上無法輕易存取的電腦或需要管理存取權的電腦。

若要使用通訊更新套件來還原用戶端伺服器通訊，請遵循下列步驟：

- 在主控台中，按一下「用戶端」，並選取群組，然後按一下「安裝用戶端」。
- 在「用戶端部署精靈」的「通訊更新套件部署」下方，按一下「針對在 **Windows/Mac** 上執行的 **Symantec Endpoint Protection** 用戶端建立套件」，然後按「下一步」。
- 選取您想要套用政策的群組，然後按「下一步」。
在僅適用於 Windows 用戶端的 Symantec Endpoint Protection Manager 14.3 RU9 和更早版本中，您可以選擇性地設定密碼防護。

NOTE

從 14.3 RU10 開始，安裝或升級管理伺服器時會自動設定密碼防護。您無法選擇停用密碼防護。

- 選擇下列其中一種部署方法，然後按「下一步」：
 - 按下「遠端推送」並移至下列程序中的「電腦選取」步驟。請參閱：
[使用遠端推送安裝 Symantec Endpoint Protection 用戶端](#)
 - 按一下「儲存套件」，然後前往下列程序中的「瀏覽」步驟。請參閱：
[使用儲存套件安裝 Symantec Endpoint Protection 用戶端](#)
- 下載和解壓縮通訊更新套件以及用戶端使用者執行 SylinkDrop 工具之後，請確認電腦與 Symantec Endpoint Protection Manager 成功通訊。

[使用 SylinkDrop 工具還原用戶端伺服器通訊設定](#)

手動匯出和匯入用戶端伺服器通訊檔案 (Sylink.xml)

如果 Windows 用戶端與管理伺服器之間的通訊中斷，您應在用戶端電腦上取代 Sylink.xml 檔案才能還原通訊。您可以根據群組從 Symantec Endpoint Protection Manager 手動匯出 Sylink.xml 檔案。

如需詳細瞭解您應取代通訊檔案的情況，請參閱：[在用戶端電腦上取代用戶端伺服器通訊檔案](#)

匯出 Sylink.xml 檔案

手動匯出用戶端伺服器通訊檔案 (Sylink.xml)

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，選取要使用戶端在其中出現的群組。
3. 在群組上按下滑鼠右鍵，然後按下「匯出通訊設定」。
4. 在「匯出 群組名稱 的通訊設定」對話方塊中，按一下「瀏覽」。
5. 在「選取匯出檔案」對話方塊中，找出要將 .xml 檔案匯出至的資料夾，然後按下「確定」。
6. 在「偏好政策模式」中，確定已核取「電腦模式」。
7. 按下「匯出」，然後按下「確定」。

匯入 Sylink.xml 檔案

從 Symantec Endpoint Protection Manager 匯出 sylink 檔案之後，請將其匯入用戶端電腦。

NOTE

從 14.3 RU10 開始，需要密碼才能匯入 Sylink.xml 檔案。請與 Symantec Endpoint Protection Manager 管理員聯繫。密碼可以是預設用戶端密碼或群組層級密碼。

您可以使用以下任一方法匯入 sylink.xml 檔案。

使用 **import sylink** 指令匯入用戶端伺服器通訊檔案

1. 在您已複製 Sylink.xml 檔案的用戶端電腦上，開啟指令行，然後鍵入：或 `smc -importsylink -p <password> <sylinkpath>`，其中 `<password>` 是密碼。

NOTE

如果使用 SylinkDrop 工具的密碼包括 " (雙引號)，則用戶端使用者必須將 " 取代為 \ "。

例如，如果密碼為 1234"，則：

`SylinkDrop -silent -p 1234" sylink.xml` 失敗。

`SylinkDrop -silent -p 1234\" sylink.xml` 成功。

使用用戶端疑難排解功能表匯入用戶端伺服器通訊檔案

1. 在您已複製 Sylink.xml 檔案的用戶端電腦上，開啟用戶端。
2. 在右上角，按下「說明」，再按下「疑難排解」。
3. 在「疑難排解」對話方塊的「通訊管理」下「管理」窗格中，按下「匯入」。
4. 在「密碼」對話方塊中，鍵入預設用戶端密碼或群組層級密碼 (如果是由 Symantec Endpoint Protection Manager 14.3 RU10 或更新版本所管理)。
5. 在「匯入群組註冊設定」對話方塊中，找出 `<group name>_sylink.xml` 檔案，然後按一下「開啟」。
6. 按下「關閉」，關閉「疑難排解」對話方塊。

匯入通訊檔案後，用戶端與管理伺服器進行通訊時，電腦工作列將顯示帶有綠點的通知區域圖示。綠點表示用戶端與管理伺服器互相通訊中。

如需密碼需求以及設定群組層級密碼的相關資訊，請參閱[用密碼保護 Symantec Endpoint Protection 用戶端](#)。

將用戶端伺服器通訊設定匯入 Linux 用戶端

(適用於 14.3 MP1 及更舊版本)

為 Linux 用戶端安裝非受管 Symantec Endpoint Protection 後，您可將其轉換為受管用戶端，以便利用 Symantec Endpoint Protection Manager 集中管理用戶端的政策和狀態。受管用戶端會與 Symantec Endpoint Protection Manager 通訊，並向其報告狀態和其他資訊。

您也可以使用此程序，將先前遺棄的用戶端重新與 Symantec Endpoint Protection Manager 連線。

NOTE

您必須具有進階使用者權限才能執行此程序。必要時，此程序會使用 `sudo` 來提高權限。

文字 `path-to-sav` 代表 `sav` 指令的路徑。預設路徑為 `/opt/Symantec/symantec_antivirus/`。

將用戶端伺服器通訊設定檔案匯入 Linux 用戶端

1. 您或 Symantec Endpoint Protection Manager 管理員必須先從 Symantec Endpoint Protection Manager 匯出通訊設定檔案，然後再將檔案複製到 Linux 電腦上。確認檔案名稱是 `sylink.xml`。

[手動匯出用戶端伺服器通訊檔案 \(Sylink.xml\)](#)

2. 在 Linux 電腦上，開啟終端機視窗，然後輸入下列指令：

```
sudo path-to-sav/sav manage -i path-to-sylink/sylink.xml
```

其中 `path-to-sylink` 代表您要將 `sylink.xml` 複製到的路徑。

例如，如果您將檔案複製到使用者設定檔的桌面，請輸入：

```
sudo path-to-sav/sav manage -i ~/Desktop/sylink.xml
```

3. 傳回「確定」即表示匯入成功。若要進一步驗證受管狀態，請輸入下列指令，它會顯示成功匯入的政策序號：

```
path-to-sav/sav manage -p
```

如需詳細資訊，請參閱：

[安裝適用於 Linux 的 Symantec Endpoint Protection 用戶端](#)

NOTE

自 Linux 用戶端 14.3 RU2 起，您可以使用 **sav** 指令來匯入 *sylink.xml* 檔案。請參閱：

[執行 Linux 用戶端指令行工具 \(sav\)](#)。

IPv6 網路支援

在 14.2 版中，已新增此支援。

IPv6 是對 Internet 通訊協定的修訂，是 IPv4 的後續協定。這兩種類型的位址為已連線到 Internet 的裝置進行通訊提供了所需的唯一數字 IP 位址。IPv4 位址為 32 位元，而 IPv6 位址為 128 位元。因此，IPv6 允許更多位址可供使用者和裝置在 Internet 上進行通訊。

IPv6 位址一般使用十六進位字串來表示。例如，`fd32:32a4:d0cf:a0c4:0000:8a2e:0370:7334`，也可以表示為 `fd32:32a4:d0cf:a0c4::8a2e:0370:7334`。當您輸入以通訊埠編號結尾的 IPv6 位址時，必須以方括弧括住 IPv6 位址。括弧會防止通訊埠號被解釋為 IPv6 位址的一部分。例如：`http://[fd32:32a4:d0cf:a0c4::8a2e:0370:7334]:9090`。

Symantec Endpoint Protection 14.2 透過下列方式支援 IPv6：

- 管理伺服器與 Windows、Mac 和 Linux 用戶端之間的通訊。
- 主控台和管理伺服器之間的通訊，例如從本機或遠端登入 Symantec Endpoint Protection Manager。請參閱：[登入 Symantec Endpoint Protection Manager 主控台](#)
- 管理伺服器和執行 LiveUpdate Administrator 的內部 LiveUpdate 伺服器之間的通訊。請參閱：[將用戶端架構為從內部 LiveUpdate 伺服器下載內容](#)
- Windows LiveUpdate 到管理伺服器。
- 管理伺服器或用戶端與服務或功能 (例如 LiveUpdate Engine (LUE) 和信譽查詢) 之間的通訊。
- 位置偵測中具有以 IPv6 為基礎之準則的位置定義。

此外，許多其他政策現在可讓您輸入 IPv6 位址作為定義準則 (除了 IPv4 以外)，例如自訂 IPS 特徵或明確 GUP。

下列項目不支援 IPv6：

- 使用 Symantec VIP 進行雙因素驗證 (2FA)。請參閱：[使用 Symantec VIP 架構雙因素驗證](#)
- 註冊和連線至雲端主控台。

設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊

Symantec Endpoint Protection Manager 會使用 Apache Web 伺服器與用戶端通訊，並提供報告服務。對於 Symantec Endpoint Protection 的新安裝，依預設啟用 HTTPS 通訊。HTTPS 是使用憑證簽署和加密資料的安全通訊協定，可確保通訊的機密性和完整性。

如果您已從 12.1.x 版直接升級，或 HTTPS 通訊已停用，則應該啟用 HTTPS。

Table 128: 架構與用戶端的 HTTPS 通訊

步驟	說明
步驟 1：檢查預設 HTTPS 通訊埠是否可用	依據預設，HTTPS 流量會使用通訊埠 443。在某些網路中，通訊埠 443 可能已繫結至其他應用程式或服務。在啟用 HTTPS 通訊之前，您必須檢查預設通訊埠是否可用。請參閱： 尋找可用的通訊埠
步驟 2：視需要變更預設 HTTPS 通訊埠	如果通訊埠 443 無法使用，請從通訊埠範圍的上限部分 (49152-65535)，選擇未使用的通訊埠。將管理伺服器架構為使用新通訊埠。更新管理伺服器清單以反映新通訊埠。請參閱： • 針對用戶端通訊變更 Apache 的 HTTPS 通訊埠 • 架構用於負載平衡的管理伺服器清單
步驟 3：啟用與用戶端的 HTTPS 通訊	編輯 Apache httpd.conf 檔案，以允許與用戶端的 HTTPS 通訊。測試連線，然後將用戶端切換為 HTTPS 通訊。請參閱： 啟用 HTTPS 用戶端伺服器通訊

尋找可用的通訊埠

某些 Symantec Endpoint Protection Manager 架構會要求變更指定的預設通訊埠，以防止與其他應用程式或服務發生衝突。指派新的通訊埠之前，您必須先檢查並確認其他應用程式或服務未使用新的通訊埠。

開啟指令提示並輸入下列區分大小寫的指令：

```
netstat -an | find ":port" | find "LISTENING"
```

其中 port 代表要檢查可用性的埠號。例如，若要查看通訊埠 443 是否可用，請輸入：

```
netstat -an | find ":443" | find "LISTENING"
```

如果 netstat 指令傳回結果，您必須找到未使用的通訊埠。您會使用相同的指令，但請以您選擇的通訊埠取代 port。如果此指令未產生任何結果，便可自由地使用該通訊埠。

更多資訊

- [針對用戶端通訊變更 Apache 的 HTTPS 通訊埠](#)
- [設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊](#)

針對用戶端通訊變更 Apache 的 HTTPS 通訊埠

Apache 的預設 HTTPS 通訊埠為通訊埠 443。如果託管 Symantec Endpoint Protection Manager 的系統也託管其他 HTTPS 服務，則可能已指派通訊埠 443。您應針對新安裝使用其他通訊埠，以盡量減少與已使用預設通訊埠 443 之任何應用程式之間的衝突。如果您想讓用戶端使用預設通訊埠來與 Symantec Endpoint Protection Manager 進行通訊，應該先驗證該通訊埠是否可用。

NOTE

如果在部署用戶端軟體後自訂 HTTPS 埠號，則用戶端將失去與管理伺服器的通訊。從包含新連線資訊的伺服器執行下一次用戶端更新之後，將會重新建立通訊。也可以使用通訊更新套件。請參閱[使用「通訊更新套件部署」還原用戶端伺服器通訊](#)。

完成此程序之後，啟用 HTTPS 用戶端伺服器通訊。

針對用戶端通訊變更 Apache 的 HTTPS 通訊埠

1. 在文字編輯器中，開啟下列檔案：

```
SEPM_Install\apache\conf\ssl\sslForClients.conf
```

SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。

NOTE

封閉資料夾 SEPM_Install\apache\conf\ssl\ 可能是唯讀的。在該情況下，您可能需要在資料夾內容中取消勾選「唯讀」。

2. 編輯下列行並以新的埠號取代預設的 443：

```
Listen 443  
  
<VirtualHost_default_: 443>
```

3. 儲存檔案，然後關閉文字編輯器。

更多資訊

- [啟用 HTTPS 用戶端伺服器通訊](#)
- [設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊](#)

啟用 HTTPS 用戶端伺服器通訊

編輯 httpd.conf 檔案，以使用 HTTPS 通訊協定啟用 Symantec Endpoint Protection Manager 伺服器與用戶端之間的安全通訊。

如果您需要為安全通訊使用替代通訊埠，必須先在 Symantec Endpoint Protection Manager 中變更通訊埠指派。

對於 Symantec Endpoint Protection 的新安裝，根據預設會啟用 HTTPS 用戶端伺服器通訊。

為 Apache Web 伺服器啟用 HTTPS

1. 在文字編輯器中，開啟下列檔案：

```
SEPM_Install\apache\conf\httpd.conf
```

SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。

2. 尋找下列文字字串並移除井字號 (#)：

```
#Include conf/ssl/sslForClients.conf
```

3. 儲存並關閉檔案。

4. 重新啟動 **Symantec Endpoint Protection Manager Webserver** 服務。

停止並重新啟動 Symantec Endpoint Protection Manager Webserver 服務亦會停止和重新啟動 Symantec Endpoint Protection Manager 服務。

[停止和啟動 Apache Web 伺服器](#)

確認 HTTPS 正常運作

1. 在網頁瀏覽器中輸入下列 URL：

```
https://SEPMServer:port/secars/secars.dll?hello,secars
```

其中 SEPMServer 是 Symantec Endpoint Protection Manager 的伺服器主機名稱，而 port 是 HTTPS 埠號。依據預設，HTTPS 流量會使用通訊埠 443。

2. 如果瀏覽器顯示「確定」一詞，表示 HTTPS 連線成功。

如果顯示頁面錯誤，請重複前面的步驟，並檢查所有字串的格式是否正確。請同時檢查輸入的 URL 是否正確無誤。

如果您沒有使用憑證授權中心簽署的憑證以及私密金鑰組更新管理伺服器，網頁瀏覽器會顯示憑證不受信任的警告。當您從 URL 存取網站（與管理伺服器憑證上的主旨名稱不同）時，會顯示相同的警告，此為預期行為。

將用戶端切換為使用 HTTPS 以與 Symantec Endpoint Protection Manager 進行通訊

1. 在 Symantec Endpoint Protection Manager 主控台的「政策」標籤中，按下「政策元件 > 管理伺服器清單」。

-
2. 連按兩下您的用戶端群組和位置使用的管理伺服器清單。如果您只有預設的管理伺服器清單，請複製該清單，然後連按兩下新的清單加以編輯。

也可以按下「工作」下方的「新增管理伺服器清單」。在「管理伺服器」下方的「新增 > 新伺服器」中新增伺服器資訊。您可以為伺服器 IP 位址和伺服器名稱分別新增一個「新伺服器」項目。

[在「政策」頁面中複製和貼上政策](#)

3. 按下「使用 **HTTPS** 通訊協定」。

只有當您先前已使用認證中心簽章的憑證以及私密金鑰組更新管理伺服器時，才應按下「使用 **HTTPS** 通訊協定時驗證憑證」。

[更新或還原伺服器憑證](#)

NOTE

如果已在 `sslForClients.conf` 檔案中使用自訂 HTTPS 通訊埠編號，請從管理伺服器清單編輯伺服器。按下「自訂 **HTTPS** 通訊埠」，然後編輯該通訊埠，使其與先前使用的號碼相符。

按下「確定」儲存自訂通訊埠。

4. 按下「確定」儲存管理伺服器清單。
5. 如果您已編輯預設管理伺服器清單的複本，請在複本上按下滑鼠右鍵，然後按下「指派」，將其指派給每個群組和位置。

[指派管理伺服器清單至群組和位置](#)

當用戶端接收到更新的管理伺服器清單時，用戶端會切換為使用 HTTPS 與 Symantec Endpoint Protection Manager 進行通訊。

NOTE

請等待至少 24 小時，以完成變更。建議等待一週，盡量讓更多用戶端從管理伺服器下載新的通訊詳細資料。由於外出或正在休假的使用者的裝置處於離線狀態，因此可能無法接收這些更新。許多機構會執行容錯移轉方法 30 天或以上，以盡可能擷取多個外出用戶端。

確認用戶端與管理伺服器的通訊

1. 在 Symantec Endpoint Protection 用戶端上，按下「說明 > 疑難排解 > 伺服器連線狀態」。
2. 在「上次嘗試連線」和「上次成功連線」下方，確認用於 HTTPS 通訊之伺服器位址和埠號的顯示。
3. 按下「立即連線」以強制立即連線 (視需要)。

更多資訊

- [針對用戶端通訊變更 Apache 的 HTTPS 通訊埠](#)
- [設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊](#)

管理群組、用戶端、管理員、密碼和網域

瞭解如何新增及管理群組、用戶端、管理員、密碼和網域。

本節介紹如何管理用戶端電腦、用戶端、管理員、密碼和網域。

管理用戶端群組

在 Symantec Endpoint Protection Manager 中，群組用作執行用戶端軟體的端點的配置區。這些端點可以是電腦或使用者。您可以將具有類似安全需求的用戶端分門別類為群組，以便於管理網絡安全性。

Symantec Endpoint Protection Manager 包含下列預設群組：

- **My Company** 群組為頂層或父群組，其中包含子群組的平面樹狀結構。
- **Default Group** 是 **My Company** 的子群組。除非用戶端屬於預先定義的群組，否則以 Symantec Endpoint Protection Manager 率先登錄時，會先指定到 **Default Group**。您無法在 **Default Group** 下建立子群組。

NOTE

您無法在 Symantec Endpoint Protection Manager 或雲端主控台重新命名或刪除「我的公司」或「預設群組」。

Table 129: 群組管理動作

工作	說明
新增群組	如需詳細資訊，請參閱： 如何設定群組結構 新增群組
匯入現有群組	若您的組織已有現成的群組結構，可匯入該群組作為組織單位。 Note: 您無法以管理 Symantec Endpoint Protection Manager 中建立的群組的相同方式來管理匯入的組織單位。 如需詳細資訊，請參閱： 從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦
停用子群組繼承	根據預設，子群組會從父群組繼承相同的安全性設定。您可以停用繼承。請參閱： 停用群組繼承
在群組內建立位置	您可以設定代理程式，在用戶端實體位置變更時，自動切換成另一安全性政策；請參閱： 管理遠端用戶端的位置 某些安全設定屬於群組特定，而某些設定屬於位置特定。您可以自訂位置特定的任何設定。請參閱： 架構位置的通訊設定
管理群組的安全性政策	您可以根據各群組的需要建立安全性政策。然後，您可以將不同的政策指派到不同的群組或位置。請參閱： • 新增政策 • 指派政策給群組或位置 • 執行適用於所有政策的工作
執行群組維護	您可以移動群組以方便管理，並在群組之間移動用戶端。您還可以攔截用戶端，使其無法新增到特定群組。請參閱： • 將用戶端電腦移至其他群組 • 防止用戶端電腦被加入至群組

如何設定群組結構

您可以建立多個群組和子群組，以符合公司的組織結構和安全性。亦可根據功能、角色、地理位置或單項準則組合等群組結構進行。

Table 130: 群組建立準則

準則	說明
函數	您可以根據欲管理的電腦類型建立群組，例如筆記型電腦、桌上型電腦以及伺服器。或者也可以根據使用類型建立多個群組。例如，您可以為出差使用的用戶端電腦建立遠端群組，以及為辦公室內的用戶端電腦建立本機群組。
角色	您可以根據各部門角色建立群組，例如銷售、工程、財務以及行銷等部門。
地理位置	您可以根據辦公室、城市、州、地區或國家等電腦所處位置建立群組。
組合	您可以根據準則組合建立群組。例如可以合併功能與角色兩者。 您可以根據角色新增父群組，然後根據功能新增子群組，如下所示： - 銷售，底下設有筆記型電腦、桌上型電腦和伺服器的子群組。 - 工程，底下設有筆記型電腦、桌上型電腦和伺服器的子群組。

在您將用戶端電腦組成群組之後，可以將適量的安全性套用到該群組。

例如，假設公司有電話行銷和會計部門。這些部門分別在紐約、倫敦和法蘭克福分公司都有職員。這兩個部門的所有電腦都指派給相同的群組，因此可以從相同來源接收病毒及安全風險定義檔更新。但是，IT 報告指出電話銷售部門比會計部門更容易受到風險的威脅。因此，系統管理員建立了獨立的電話行銷和會計群組。電話行銷用戶端會共用嚴格限制使用者與病毒和安全風險防護互動方式的架構設定。

如需詳細資訊，請參閱：

- [建立群組結構的最佳實務準則](#)
- [執行適用於所有政策的工作](#)
- [管理用戶端群組](#)

新增群組

您可以在定義組織的群組結構之後，新增群組。

群組敘述最多可包含 1024 個字元。群組名稱可包含除下列字元之外的任何字元："/ \ * ? < > | : 群組敘述不會受到限制。

NOTE

您無法在 Default Group 中新增群組。

如需詳細資訊，請參閱：

[如何設定群組結構](#)

新增群組

-
1. 在主控台中，按一下「用戶端」。
 2. 在 [用戶端] 下方，選取要新增子群組的群組。
 3. 在「用戶端」標籤的「工作」下方，按下「新增群組」。
 4. 在「新增 群組名稱 的群組」對話方塊中，輸入群組名稱和說明。
 5. 按下「確定」。

以 **Symantec Endpoint Protection Manager (SEPM)** 來同步 **Active Directory** 群組

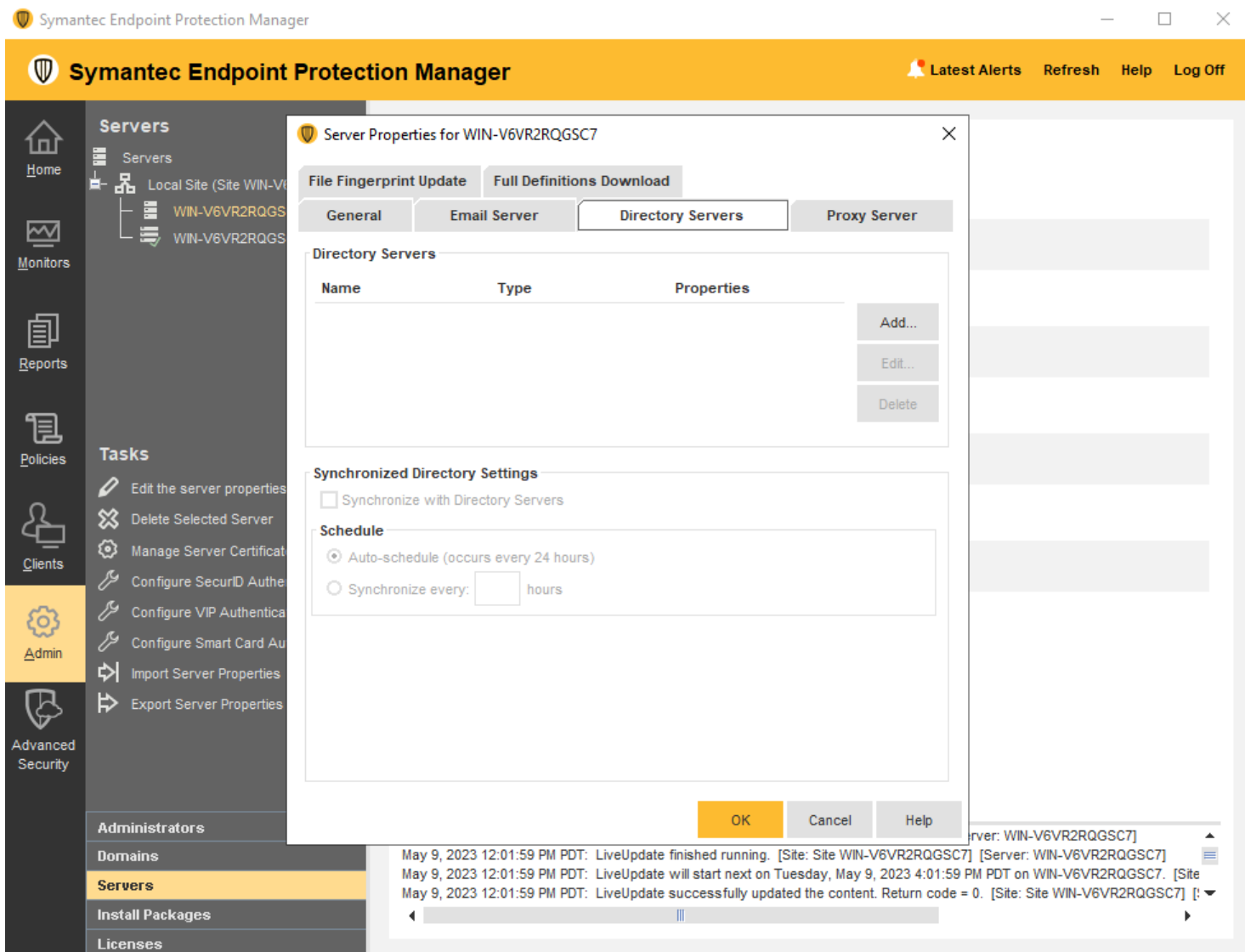
如果您的公司使用 Active Directory (AD) 或 LDAP 伺服器管理群組，您可以將群組結構匯入 Symantec Endpoint Protection Manager。然後，您可以從管理主控台管理群組和電腦。

NOTE

請勿以超過一個 Symantec Endpoint Protection Manager (SEPM) 來同步 Active Directory 群組。

步驟 1：以 **Symantec Endpoint Protection Manager (SEPM) 來整合 **Active Directory****

1. 在主控台中，按一下「管理員」>「伺服器」。
2. 在「伺服器」>「本機網站」下方，以滑鼠右鍵按一下管理伺服器，並按一下「編輯伺服器屬性」。
3. 在「伺服器屬性」對話方塊的「目錄伺服器」標籤上，按一下「新增」。



4. 在「新增目錄伺服器」對話方塊中，輸入目錄伺服器的網域名稱。
5. 按一下「**Active Directory**」。
輸入網域使用者或專用服務帳戶的使用者名稱和密碼。
新增 LDAP 伺服器時，若 LDAP 伺服器的通訊埠編號必須與預設值不同，則變更埠號。
6. 在「伺服器 IP 位址或名稱」欄位中，輸入您的公司 IP 位址或網域名稱。例如，針對電子郵件地址 abc@mycompany.com，新增網域名稱：mycompany.com。
7. 按一下「確定」。
若未成功驗證憑證，請檢查「使用安全連線」並按一下「確定」。
「使用安全連線」使用 LDAP 636 並提供加密連線。

File Fingerprint Update

Full Definitions Download

General

Email Server

Directory Servers

Proxy Server

Directory

Name

DDC2016

Synchron

☒ Synch

Schedule

☒ Auto

☐ Sync

✕ Add Directory Server

General

Replication Servers

Name:

DC2016

Server Type:

☒ Active Directory

☐ LDAP

Server IP Address or Name:

mycompany.com

LDAP Port:

636

LDAP BaseDN:

User Name:

abc

Password:

.....

☒ Use Secure Connection

☐ Disable verification of the directory server certificate



Enabling this option can disclose sensitive data to unauthorized third parties.

OK

Cancel

Help

OK

Cancel

Help

- 在「目錄伺服器」標籤上，勾選「與目錄伺服器同步處理」，然後設定同步處理排程。

Server Properties for WIN-V6VR2RQGSC7

File Fingerprint Update

Full Definitions Download

General

Email Server

Directory Servers

Proxy Server

Directory Servers

Name	Type	Properties	
DDC2016	Active Directory	Server:DC2016, User:do...	Add... Edit... Delete

Synchronized Directory Settings

☒ Synchronize with Directory Servers

Schedule

☒ Auto-schedule (occurs every 24 hours)

☐ Synchronize every: hours

OK

Cancel

Help

9. 按一下「確定」。

步驟 2：匯入 **Active Directory** 組織單位

您可以將組織單位匯入成 **My Company** 群組或您所建立群組的子群組，但不能是 **Default Group** 的子群組。您不能建立群組作為組織單位的子群組。您不能將組織單位置於多個 Symantec Endpoint Protection Manager 群組中。

NOTE

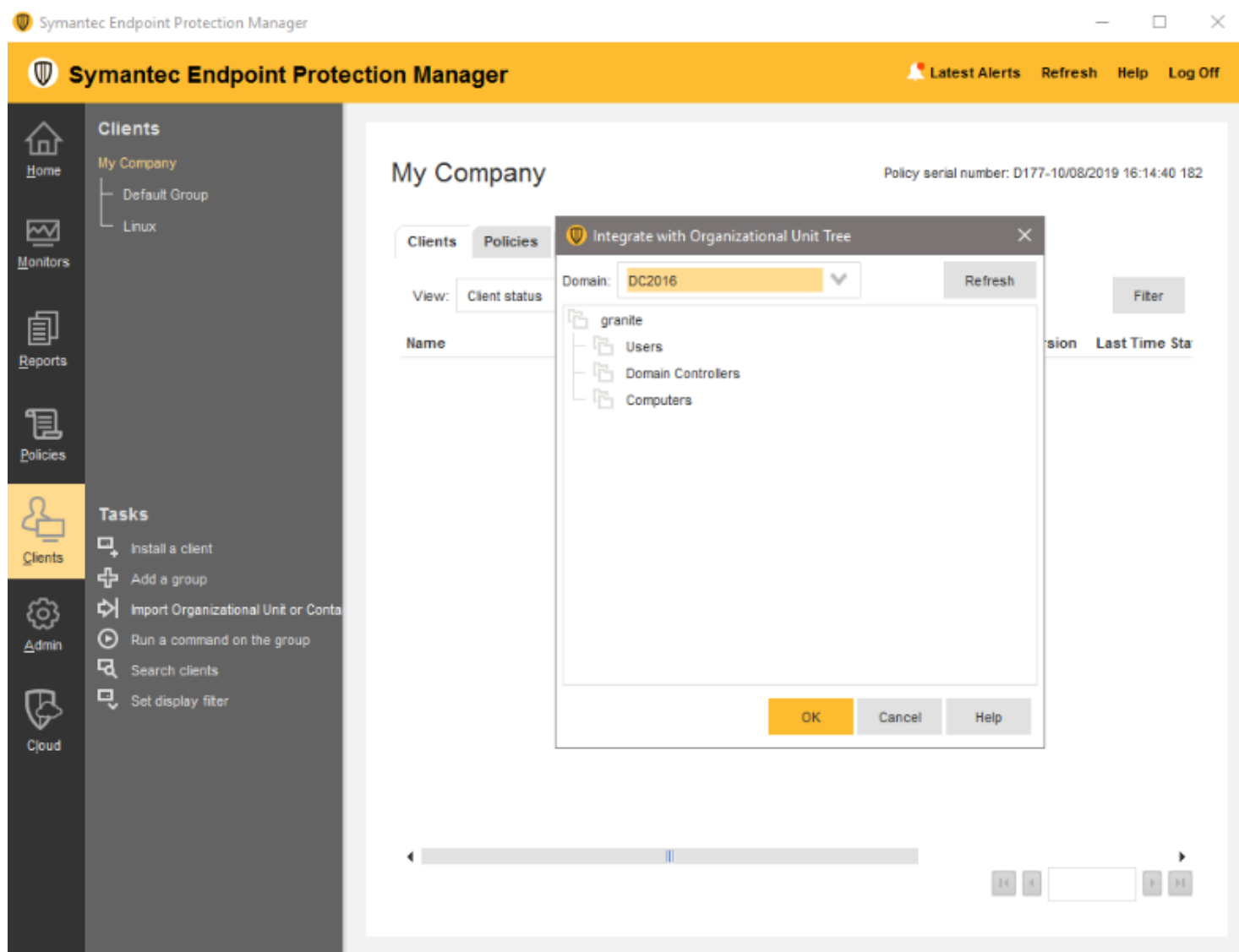
將組織單位匯入 Symantec Endpoint Protection Manager 之前，您必須先轉換電腦名稱或使用者名稱前面的一些特殊字元。您可以在目錄伺服器中執行這項工作。您必須轉換特殊字元，以讓管理伺服器匯入這些帳戶。

轉換下列特殊字元：

- 出現在項目開頭的空格或井字號字元 (#)。
- 出現在項目結尾的空格字元。
- 逗號 (,)、加號 (+)、雙引號 (")、小於或大於符號 (< 或 >)、等號 (=)、分號 (;)、反斜線 (\)。

若要允許匯入包含這些字元的名稱，您必須在每個字元前面加上反斜線字元 (\)。

1. 在「用戶端」頁面 > 「用戶端」標籤上，選取您要新增 Active Directory 組織單位的目的地群組。
2. 在「工作」下方，按下「匯入組織單位或配置區」。
3. 在「網域」下拉式清單中，選取您上一步驟所建立的網域名稱。
4. 按一下「確定」。



5. 選擇要與管理伺服器整合的適當 OU，然後按一下「確定」。

請參閱：[Active Directory 的組織單位是什麼？](#)

疑難排解同步問題

有關 AD 同步的問題，請參閱以下日誌。

- 32-bit: C:\Program Files\Symantec\Symantec Endpoint Protection Manager\Tomcat\logs\ADSI\Task-0.log
- 64-bit: C:\Program Files(x86)\Symantec\Symantec Endpoint Protection Manager\Tomcat\logs\ADSI\Task-0.log

搜尋「錯誤碼」以及接續幾行內容，以了解問題根源。

Active Directory 的組織單位是什麼？

Microsoft Active Directory 和 LDAP 伺服器使用組織單位來管理電腦和使用者的帳戶。您可以將組織單位及其帳戶資料匯入 Symantec Endpoint Protection Manager，然後在管理主控台中管理該帳戶資料。由於 Symantec Endpoint Protection Manager 會將組織單位視為群組，因此您接著可以將安全性政策指派給組織單位群組。

您也可以藉由複製帳戶的方式，將帳戶從組織單位移入 Symantec Endpoint Protection Manager 群組。如此一來，Symantec Endpoint Protection Manager 群組和組織單位便存在相同的帳戶。由於 Symantec Endpoint Protection Manager 群組的優先順序高於組織單位，因此複製的帳戶會採用 Symantec Endpoint Protection Manager 群組的政策。

如果您從目錄伺服器刪除已複製到 Symantec Endpoint Protection Manager 群組的帳戶，該帳戶名稱仍會留在 Symantec Endpoint Protection Manager 群組中。您必須從管理伺服器手動移除該帳戶。

如果您需要修改組織單位中的帳戶資料，請在目錄伺服器上，而不是在 Symantec Endpoint Protection Manager 中執行這項工作。例如，您可以從管理伺服器刪除組織單位，此舉並不會永久刪除目錄伺服器中的該組織單位。您必須將 Symantec Endpoint Protection Manager 與 Active Directory 伺服器進行同步處理，這些變更才能自動更新於 Symantec Endpoint Protection Manager。設定連線至目錄伺服器時，可以啟用同步處理。

NOTE

同步處理僅適用於 Active Directory 伺服器。Symantec Endpoint Protection 不支援與 LDAP 伺服器進行同步處理。

您也可以將選取的使用者匯入 Symantec Endpoint Protection Manager 群組，而不是匯入整個組織單位。

更多資訊

- [將 Symantec Endpoint Protection Manager 連線至目錄伺服器](#)
- [從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦](#)
- [從目錄伺服器匯入組織單位](#)

將 Symantec Endpoint Protection Manager 連線至目錄伺服器

您必須先將 Symantec Endpoint Protection Manager 連線至公司的目錄伺服器，然後才能匯入包含電腦帳戶或使用者的帳戶的組織單位。

您無法修改管理伺服器中組織單位內的帳戶，只能在目錄伺服器中修改這些帳戶。不過，您可以同步處理 Active Directory 伺服器與管理伺服器間的帳戶資料。您在 Active Directory 伺服器上所做的任何變更，均會在 Symantec Endpoint Protection Manager 中自動更新。您在 Active Directory 伺服器上所做的任何變更，不會立即出現在先前匯入至管理伺服器的組織單位中。延遲的時間視同步處理頻率而定。在您架構連線時，請啟用同步處理，並設定同步處理頻率。

如果您從 Symantec Endpoint Protection Manager 中刪除目錄伺服器連線，則必須先刪除與該連線關聯的任何已匯入組織單位。然後，您便可以同步處理伺服器間的資料。

NOTE

同步處理僅適用於 Active Directory 伺服器。Symantec Endpoint Protection 不支援與 LDAP 伺服器進行同步處理。

將 Symantec Endpoint Protection Manager 連線至目錄伺服器

1. 在主控台中，按下「管理員」>「伺服器」。
2. 在“服务器”和“本地站点”下，选择管理服务器。
3. 在「工作」下方，按一下「編輯伺服器屬性」。
4. 在「伺服器屬性」對話方塊的「目錄伺服器」標籤上，按一下「新增」。
5. 在「新增目錄伺服器」對話方塊中，輸入目錄伺服器的名稱。
6. 勾選 **Active Directory** 或 **LDAP**，然後輸入 IP 位址、主機名稱或網域名稱。

新增 LDAP 伺服器時，若 LDAP 伺服器的通訊埠編號必須與預設值不同，則變更埠號。

7. 如果想要使用加密連線，請勾選「使用安全連線」。
8. 按下「確定」。
9. 在「目錄伺服器」標籤上，勾選「與目錄伺服器同步處理」，然後在「排程」下方設定同步處理排程。
10. 按下「確定」。

更多資訊

[從目錄伺服器匯入組織單位](#)

連線至遠端複製網站上的目錄伺服器

如果某站台使用複寫 Active Directory 或 LDAP 伺服器，則可以將 Symantec Endpoint Protection Manager 連線至主要目錄伺服器和複寫伺服器。如果主要目錄伺服器連線中斷，管理伺服器仍會與遠端複製目錄伺服器保持連線。

然後，Symantec Endpoint Protection Manager 可以驗證管理員帳戶，並同步本機站台與複寫站台的所有 Active Directory 伺服器上的組織單位。請參閱：

[設定站台和複寫](#)

NOTE

同步處理僅適用於 Active Directory 伺服器。Symantec Endpoint Protection 不支援與 LDAP 伺服器進行同步處理。

連線至複寫站台上的目錄伺服器

1. 在主控台中，按下「管理員」>「伺服器」。
2. 在「伺服器」下方，選取管理伺服器。
3. 在「工作」下方，按一下「編輯伺服器屬性」。
4. 在「伺服器屬性」對話方塊的「目錄伺服器」標籤上，按一下「新增」。
5. 在「新增目錄伺服器」對話方塊的「複寫伺服器」標籤上，按一下「新增」。
6. 在「新增複寫伺服器」對話方塊中，輸入目錄伺服器的 IP 位址、主機名稱或網域名稱，然後按一下「確定」。
7. 按下「確定」。
8. 按下「確定」。

更多資訊

[將 Symantec Endpoint Protection Manager 連線至目錄伺服器](#)

從目錄伺服器匯入組織單位

當您從 Active Directory 或 LDAP 伺服器匯入電腦帳戶或使用者帳戶時，會作為組織單位匯入這些帳戶。您接著便可以將安全性政策套用到該組織單位。您也可以將這些帳戶複製到現有的 Symantec Endpoint Protection Manager 群組。

您可以將組織單位匯入成 **My Company** 群組或您所建立群組的子群組，但不能是 **Default Group** 的子群組。您不能建立群組作為組織單位的子群組。您不能將組織單位置於多個 Symantec Endpoint Protection Manager 群組中。

如果您不想將組織單位或容器內的所有帳戶新增至 Symantec Endpoint Protection Manager，仍然必須將其匯入。一旦匯入完成，可將要管理的帳戶複製到現有用戶端群組。

NOTE

將組織單位匯入 Symantec Endpoint Protection Manager 之前，您必須先轉換電腦名稱或使用者名稱前面的一些特殊字元。您可以在目錄伺服器中執行這項工作。如果不轉換特殊字元，管理伺服器就不會匯入這些帳戶。

您必須轉換下列特殊字元：

- 出現在項目開頭的空格或井字號字元 (#)。
- 出現在項目結尾的空格字元。
- 逗號 (,)、加號 (+)、雙引號 (")、小於或大於符號 (< 或 >)、等號 (=)、分號 (;)、反斜線 (\)。

若要允許匯入包含這些字元的名稱，您必須在每個字元前面加上反斜線字元 (\)。

從目錄伺服器匯入組織單位

1. 將 Symantec Endpoint Protection Manager 連線至目錄伺服器。請參閱：
[以 Symantec Endpoint Protection Manager \(SEPM\) 來同步 Active Directory 群組](#)
2. 在主控台中按下「用戶端」，然後在「用戶端」下方，選取要新增組織單位的群組。
3. 在「工作」下方，按下「匯入組織單位或配置區」。
4. 在「網域」下拉式清單中，選擇您在步驟 1 中建立的目錄伺服器名稱。
5. 選取網域或子群組。
6. 按一下「確定」。

Active Directory 的組織單位是什麼？

停用群組繼承

在群組結構中，子群組起初會自動從其父群組繼承位置、政策及設定。依據預設，每個群組會啟用繼承。您可以停用繼承，如此就能為子群組架構獨立的安全性設定。如果您在執行變更後又啟用繼承，則會覆寫子群組設定中的所有變更。

來自雲端的政策不會遵循 Symantec Endpoint Protection Manager 政策繼承組態。相反地，它們會遵循在雲端中定義的繼承規則。請參閱：

管理用戶端群組

停用群組繼承

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方，選取要停用或啟用繼承的群組。
您可以選擇頂層群組 My Company 以外的任何群組。
3. 在「群組名稱」窗格的「政策」標籤上，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。

防止用戶端電腦被加入至群組

您可以設定已定義群組成員資格的用戶端安裝套件。如果您在套件中定義了群組，則用戶端電腦會自動新增至相關群組。第一次新增用戶端時，會連線至管理伺服器。請參閱：

管理用戶端安裝套件

如果您不希望用戶端在連線至網路時自動新增到特定群組，可以攔截用戶端。您可以攔截新用戶端新增至用戶端安裝套件中指派給使用者的群組。在此情況下，該用戶端會新增至預設群組。您可以手動將電腦移到攔截的群組。

攔截用戶端電腦加入至群組

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，在群組上按下滑鼠右鍵，再按下「屬性」。
3. 在「詳細資訊」標籤的「工作」下方，按下「編輯群組屬性」。
4. 在「群組名稱 的群組屬性」對話方塊中，按下「攔截新用戶端」。
5. 按下「確定」。

更多資訊

將用戶端電腦移至其他群組

將用戶端電腦移至其他群組

若您的用戶端電腦位於不正確的群組內，則可將其移至其他群組內。

您可以使用以下方法：

- 「用戶端」頁面上的「移動」指令。
- 重新部署用戶端安裝套件。
請參閱：[使用「通訊更新套件部署」還原用戶端伺服器通訊](#)
- REST API 指令 (/api/v1/computers)。
請參閱：<https://apidocs.securitycloud.symantec.com/#/doc?id=computers>

透過「移動」指令將用戶端電腦移至其他群組

1. 在主控台中，按一下「用戶端」>「用戶端」，然後選取群組。
2. 在「用戶端」標籤中選取的群組內，選取電腦，然後在「移動」上按下滑鼠右鍵。

使用 Shift 鍵或 Ctrl 鍵可選取多台電腦。

3. 在「移動用戶端」對話方塊中，選取新的群組。
4. 按一下「確定」。

管理用戶端電腦

Table 131: 管理用戶端電腦的工作

工作	說明
檢查電腦上是否安裝了用戶端軟體	- 您可以在各群組中顯示尚未安裝用戶端軟體的電腦。請參閱： 搜尋未安裝用戶端軟體的用戶端 - 您可以架構用戶端電腦以偵測未安裝用戶端軟體的其他裝置。部分這些裝置可能是未受保護的電腦。然後，您可以將用戶端軟體安裝到這些電腦上。請參閱： 將用戶端架構為偵測非受管裝置 - 您可以將用戶端新增至群組，稍後再安裝用戶端軟體。 如需詳細資訊，請參閱： 選擇使用用戶端部署精靈安裝用戶端的方法
檢查用戶端是否連線至管理伺服器	您可以在管理主控台和用戶端中檢查用戶端狀態圖示。狀態圖示會顯示用戶端和伺服器之間是否通訊。請參閱： 檢查用戶端是否已連線至管理伺服器且受保護 Symantec Endpoint Protection 用戶端狀態圖示 電腦可能已安裝用戶端軟體，但本身是非受管用戶端。您無法管理未受管用戶端。請改為將未受管用戶端轉換成受管用戶端。請參閱： 用戶端電腦和管理伺服器的通訊方式？
架構用戶端與伺服器之間的連線	安裝用戶端軟體後，用戶端電腦會在下一次活動訊號時自動連線至管理伺服器。您可以變更伺服器與用戶端電腦進行通訊的方式。請參閱： 管理用戶端伺服器連線 您可以疑難排解任何連線問題。請參閱： 疑難排解 Symantec Endpoint Protection Manager 與主控台或資料庫之間的通訊問題
檢查用戶端電腦是否擁有正確的防護等級	- 您可以檢視用戶端電腦上各項防護技術的狀態。請參閱： 檢視用戶端電腦的防護狀態 檢查用戶端是否已連線至管理伺服器且受保護 - 您可以執行報告或檢視日誌，看是否必須提高防護等級或改善效能。例如，掃描可能導致誤報。您也可以識別需要防護的用戶端電腦。請參閱： 監控 Symantec Endpoint Protection 用戶端 - 您可以根據用戶端軟體或用戶端電腦的特定屬性來修改防護。請參閱： 搜尋用戶端電腦相關資訊

工作	說明
調整用戶端電腦的防護功能	如果您認為用戶端未擁有正確的防護等級，可以調整防護設定。 - 您可以根據報告和日誌的結果，來增減各種類型的防護功能。請參閱： 安全政策類型 Symantec Endpoint Protection 技術如何保護您的電腦 - 您可以要求在用戶端上使用密碼。請參閱：用密碼保護 Symantec Endpoint Protection 用戶端
在群組之間移動端點來修改防護 (選擇性)	若要變更某用戶端電腦的防護等級，您可以將它移到提供較多或較少防護的群組。請參閱：將用戶端電腦移至其他群組 當您部署用戶端安裝套件時，會指定用戶端要歸屬於哪個群組。您可以將用戶端移至其他群組。如果用戶端遭到刪除或中斷連線，然後又重新加入且重新連線，則用戶端會回到原始群組。 若要讓用戶端留在最後歸屬的群組中，請架構重新連線喜好設定。您可以在「通訊設定」對話方塊的「用戶端」>「政策」標籤上架構這些設定。請參閱：<group_name> 的通訊設定
決定使用者是否可以控制電腦防護 (選擇性)	您可以指定使用者對用戶端電腦上的防護功能具有何種控制。 - 對於病毒和間諜軟體防護、主動型威脅防護以及記憶體攻擊緩和，您可以在政策內鎖定或解除鎖定核取方塊，以指定使用者是否能夠變更個別設定。 - 針對防火牆政策和 IPS 政策，以及部分用戶端使用者介面設定，您可以更廣泛地變更使用者控制等級。請參閱：防止使用者在用戶端電腦上停用防護 - 如果使用者需要用戶端的完整控制權限，您可以安裝非受管用戶端。請參閱：用戶端電腦和管理伺服器的通訊方式？
從解除委任的電腦移除 Symantec Endpoint Protection 用戶端軟體 (選擇性)	如果您已解除委任用戶端電腦，並且想要將授權用於其他電腦，則可以解除安裝 Symantec Endpoint Protection 用戶端軟體。對於未連線的受管用戶端，Symantec Endpoint Protection Manager 預設會在 30 天後從資料庫刪除用戶端。 您可以變更時段，在該時段之後，Symantec Endpoint Protection Manager 即會從資料庫中刪除用戶端。刪除用戶端後，您也會省下資料庫的空間。請參閱： 解除安裝 Symantec Endpoint Protection 用戶端 解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端 解除安裝適用於 Linux 的 Symantec Endpoint Protection 用戶端 從資料庫清除過時的用戶端以使更多授權可用

檢視用戶端電腦的防護狀態

您可以檢視網路中用戶端與電腦的即時操作狀態和防護狀態的相關資訊，例如：

- 未安裝用戶端的受管用戶端電腦清單。

您可以檢視電腦名稱、網域名稱，以及登入使用者名稱。

- 已啟用和已停用的防護。
- 擁有最新政策和定義檔的用戶端電腦。
- 群組的政策序號和用戶端的版本號碼。
- 有關用戶端電腦網路元件的資訊，例如電腦使用的網路卡 MAC 位址。
- 有關用戶端電腦的系統資訊，例如，可用磁碟空間量和作業系統版本號碼。

瞭解特定用戶端的狀態後，即可解決用戶端電腦的任何安全問題。您可以透過對群組執行指令來解決多種問題。例如，您可以更新內容或啟用「自動防護」。

NOTE

如果您管理任何執行舊版 Symantec Endpoint Protection 的用戶端，某些較新的防護技術可能會列為「未報告」。這是預期狀況。這並不表示您需要對這些用戶端採取動作。

如需詳細資訊，請參閱：

- [檢查用戶端是否已連線至管理伺服器且受保護](#)
- [在用戶端電腦上從主控台執行指令](#)
- [搜尋未安裝用戶端軟體的用戶端](#)

檢視用戶端電腦的防護狀態

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下，找出需要相關資訊的用戶端所在群組。
3. 在「用戶端」標籤上，按下「檢視」下拉式清單。然後選取類別。

您可以在右下角的文字方塊中輸入頁碼，直接移至特定的頁面。

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。

[Symantec Endpoint Protection 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」。

搜尋未安裝用戶端軟體的用戶端

您可根據下列準則搜尋群組中的用戶端：

- 已安裝用戶端軟體。
- 在 Windows、Mac 或 Linux 電腦上執行用戶端
- Windows 用戶端處於電腦模式或使用者模式。
- 在虛擬桌面基礎架構中，用戶端處於非持續且離線狀態。

如需詳細資訊，請參閱：

- [檢視用戶端電腦的防護狀態](#)
- [檢查用戶端是否已連線至管理伺服器且受保護](#)

搜尋用戶端

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」窗格中，選擇要搜尋的群組。
3. 在「用戶端」標籤的「工作」下方，按下「設定顯示過濾器」。
4. 在「設定顯示過濾器」對話方塊中，勾選「已建立但尚未安裝用戶端軟體的新使用者或電腦」。
5. 按下「確定」。

在 Symantec Endpoint Protection Manager 中搜尋用戶端電腦的資訊。

您可以搜尋用戶端、用戶端電腦和使用者的資訊，以便在充分掌握資訊的狀況下，決定網路的安全。

例如，您可以找出 Sales 群組的哪些電腦執行最新的作業系統。您可以找出 Finance 群組的哪些用戶端電腦需要安裝最新的病毒定義檔。

NOTE

若要搜尋大多數關於使用者的資訊，您必須在用戶端軟體安裝期間，或此後收集使用者資訊。這項使用者資訊也會顯示在用戶端「編輯屬性」對話方塊的「一般」標籤和「使用者資訊」標籤上。

如需詳細資訊，請參閱：

[收集使用者資訊](#)

在 Symantec Endpoint Protection Manager 中搜尋用戶端電腦的資訊

1. 在主控台中，按一下「用戶端」。
2. 在「工作」下方，按下「搜尋用戶端」。
3. 在「搜尋用戶端」對話方塊的「尋找」下拉式清單中，按下「電腦」或「使用者」。
4. 按下「瀏覽」可選取預設群組以外的其他群組。按下以選取群組，然後按下「確定」。
5. 在「搜尋條件」下方，按下「搜尋欄位」顯示下拉式清單，然後選取搜尋條件。

若要尋找內嵌式用戶端，您可以搜尋使用中的寫入過濾器類型。按下「加強型寫入過濾器」、「檔案型寫入過濾器」或「統一寫入過濾器」，搜尋它們是已安裝、已啟用還是兩者皆是。您也可以搜尋縮減大小用戶端。按下「安裝類型」以搜尋「縮減大小」的值。

6. 按下「比較運算子」下拉式清單，然後選取比較運算子。

您可以在搜尋條件中使用標準的布林運算子。如需關於選項的詳細資訊，請按下「說明」。

7. 在「值」儲存格中，輸入搜尋字串。

8. 按下「搜尋」。

您可以將結果匯出至文字檔。

9. 按下「關閉」。

您可以將查詢中包含的資料匯出至文字檔。請參閱：

[檢視用戶端電腦的防護狀態](#)

什麼是可對用戶端電腦執行的指令？

您可以從主控台，對個別用戶端或整個群組執行遠端指令。

若要查看任何指令的結果，請按下「監視器」頁面 > 「日誌」 > 「指令狀態」。您也可以從「類型」下拉式清單執行某些指令。

系統管理員和網域管理員可自動執行這些指令。對於限制的管理員，可個別啟用或停用每個指令的存取權限。請參閱：

- [新增管理員帳戶和設定存取權限](#)
- [在用戶端電腦上從主控台執行指令](#)

Table 132: 可對用戶端電腦執行的指令

指令	說明
分析 (已在 14.3 中移除)	在舊版中，「分析」指令會顯示您從雲端主控台提交至 Content Analysis 系統 (CAS) 以進行分析的所有要求的進度。
取消有害證據掃描	開始或取消您在第三方遠端監控與管理上使用的掃描。
掃描	在用戶端電腦上執行隨選掃描。 如果您執行掃描指令，並選擇「自訂」掃描，掃描會使用您在「管理員定義掃描」頁面上架構的指令掃描設定。指令使用的是「病毒和間諜軟體防護」政策 (套用於選取的用戶端電腦) 的設定。請參閱： 在用戶端電腦上執行隨選掃描 Note: 您只能在 Mac 用戶端電腦上執行自訂掃描。
更新內容	在用戶端電腦初始化 LiveUpdate 階段作業，以更新用戶端的內容。用戶端會從 Symantec LiveUpdate 接收最新的內容。請參閱： 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager
更新內容和掃描	初始化 LiveUpdate 階段作業，以更新內容，然後在用戶端電腦執行隨選掃描。
啟動 Power Eraser 分析	在選取的電腦上執行 Power Eraser 分析。一般來說，您應當僅在一台或少數幾台電腦上執行 Power Eraser。應當僅在電腦呈現不穩定狀態或持續發生問題時執行 Power Eraser。Power Eraser 和其他掃描不同，並不會自動矯正任何潛在威脅。您必須檢閱日誌中的偵測結果，並指定要移除或略過的風險。 Note: Mac 和 Linux 用戶端電腦不會處理此指令。 如需詳細資訊，請參閱： 從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析

指令	說明
重新啟動用戶端電腦	重新啟動用戶端電腦。 如果使用者登入至用戶端，根據管理員為該用戶端所架構的重新啟動選項，使用者會看見警告。您可以在「一般設定」頁面上架構用戶端的重新啟動選項。 Note: 重新啟動選項僅適用於 Windows 用戶端電腦。Mac 用戶端電腦始終執行硬式重新啟動。Linux 用戶端電腦會忽略此指令。 如需詳細資訊，請參閱： 從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦 Note: 您可以確保 Windows 用戶端不會重新啟動。您可以在用戶端新增登錄機碼，使其即使管理員發出重新啟動指令也不會重新啟動。請參閱： Note: 確保用戶端不會重新啟動
啟用自動防護	為用戶端電腦上的檔案系統啟用「自動防護」。 預設會為檔案系統啟用「自動防護」。賽門鐵克建議您始終保持自動防護為啟用狀態。您可以鎖定此設定，讓用戶端電腦上的使用者無法停用「自動防護」。請參閱： • 自訂 Windows 用戶端的自動防護 • 自訂 Mac 用戶端的自動防護 如果電子郵件的自動防護已停用，可在病毒和間諜軟體防護政策中加以啟用。
「啟用網路威脅防護」和「停用網路威脅防護」	啟用或停用用戶端電腦上的防火牆和啟用入侵預防。 Note: Linux 用戶端電腦不會處理此指令。 如需詳細資訊，請參閱： 管理防火牆防護
「啟用下載鑑識」和「停用下載鑑識」	啟用或停用用戶端電腦上的「下載鑑識」。 Note: Mac 和 Linux 用戶端電腦不會處理此指令。 如需詳細資訊，請參閱： 管理「下載鑑識」偵測
從隔離所刪除	從隔離所刪除所有檔案。此指令僅出現在「風險」日誌 > 「動作」下拉式清單中。請參閱： 如何從 Symantec Endpoint Protection Manager 刪除隔離項目
收集檔案指紋清單	從所選用戶端產生無法編輯的檔案指紋清單。收集的指紋清單會顯示在「政策元件」>「檔案指紋清單」下方的「政策」標籤上。通常，您可以在單一電腦或小型電腦群組上執行此指令。如果選取多台電腦，則指令會收集每台電腦的個別清單。 • 14.3 RU5 和更新版本會建立一個同時包括更安全 SHA-256 和 MD5 檔案指紋的清單。 • 14.3 RU4 及較早版本僅利用 MD5 檔案指紋建立清單。 Note: Mac 和 Linux 用戶端電腦不會處理此指令。

更多資訊

[Symantec Endpoint Protection 功能 \(依平台分類\)](#)

在用戶端電腦上從主控台執行指令

您可以隨時在用戶端電腦上手動執行指令，例如，啟動掃描或取消掃描。在受管用戶端上，從管理伺服器執行的指令會覆寫使用者執行的指令。指令在用戶端電腦上的處理順序，根據指令的不同而有所差異。無論在何處啟動指令，處理指令的方式一樣。請參閱：

[什麼是可對用戶端電腦執行的指令？](#)

您從下列位置執行這些指令：

-
- 「用戶端」頁面。
 - 「電腦狀態」日誌。您僅可以從「電腦狀態」日誌執行「取消全部掃描」和「啟動 **Power Eraser** 分析」指令。
 - 「風險」日誌。您僅可以從「風險」日誌執行「從隔離所刪除」指令。請參閱：
[如何從 Symantec Endpoint Protection Manager 刪除隔離項目](#)

開始掃描後，您也可以立即將其取消。

在用戶端電腦上從「用戶端」頁面執行指令

1. 在主控台中，按一下「用戶端」。
2. 對群組或電腦執行下列其中一項動作：
 - 在左側窗格中，以滑鼠右鍵按一下群組，然後按一下「對群組執行指令 > 指令」
 - 按一下「用戶端」標籤，以滑鼠右鍵按一下電腦，然後按一下「對電腦執行指令 > 指令」
3. 在出現的訊息中，按下「是」。

從電腦狀態日誌執行指令

1. 按下「監視器」>「日誌」>「電腦狀態」日誌類型，然後按下「檢視日誌」。
2. 從「指令」清單方塊中選取指令，並選取電腦，然後按下「啟動」。

NOTE

透過從指令清單按下「取消全部掃描」，即可以取消進行中的排程掃描或您開始的掃描。

檢視指令結果

1. 按下「監視器」。
2. 在「指令狀態」標籤上，從清單中選取一個指令，然後按下「詳細資訊」。

NOTE

您也可透過按下掃描指令「指令」欄中的「取消掃描」圖示，來取消進行中掃描。

確保用戶端不會重新啟動

您可以使用以下程序，來確保任何 Symantec Endpoint Protection 用戶端電腦不會重新啟動。例如，您可能想要在執行 Symantec Endpoint Protection 用戶端的伺服器上設定此值。設定此登錄機碼可確保當管理員從主控台於自己所屬的群組上發出「重新啟動電腦」指令時，伺服器不會重新啟動。

確保用戶端不會重新啟動

1. 在用戶端電腦中開啟登錄編輯程式。
2. 瀏覽至 HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC。
3. 將下面這一行新增至登錄：

```
DisableRebootCommand REG_DWORD 1
```

在使用者模式和電腦模式之間切換 Windows 用戶端

您可依照將政策套用至群組中用戶端的方式，將 Windows 用戶端新增為使用者模式或電腦模式。將使用者或電腦新增至群組後，系統會採用先前指派至該群組的政策。

新增用戶端時，預設為使用優先於使用者模式的電腦模式。賽門鐵克建議您使用電腦模式。Linux 用戶端和 Mac 用戶端僅以電腦模式安裝。

Table 133: 使用者模式與電腦模式

模式	說明
電腦模式	用戶端電腦會從電腦所屬的群組取得政策。不論哪個使用者登入電腦，用戶端都會以相同的政策防護電腦。政策會以電腦所在的群組為準。電腦模式為預設設定。多數組織多數於電腦模式架構用戶端。您可能會想要依照網路環境架構幾個擁有特殊要求的使用者用戶端。 若電腦名稱已位於其他群組中，您無法將使用者模式切換為電腦模式。切換至電腦模式時，會從群組中刪除用戶端的使用者名稱，並將用戶端的電腦名稱新增至該群組。 加入於電腦模式的用戶端可啟用為非受管偵測程式，並且用於偵測未經授權的裝置。請參閱： 將用戶端架構為偵測非受管裝置
使用者模式	用戶端電腦會從使用者所屬的群組取得政策。政策會根據登入用戶端的使用者而變更。政策會以使用者為準。 如果您將現有群組結構從 Microsoft Active Directory 或 LDAP 目錄伺服器匯入 Symantec Endpoint Protection Manager 以按使用者編排用戶端，則使用使用者模式。 如果使用者登入名稱與電腦名稱已存於任何群組中，您無法將電腦模式切換為使用者模式。切換至使用者模式時，會從群組中刪除用戶端的電腦名稱。然後，將用戶端的使用者名稱新增至群組。請參閱： 從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦

當您部署用戶端安裝套件時，會指定用戶端要歸屬於哪個群組。您稍後可以將用戶端指定為使用者模式或電腦模式。若用戶端稍後被刪除或失去連線，然後又將其重新新增和重新連線，用戶端將回到原群組。不過，您可以架構用戶端留在其上次移至使用者模式或電腦模式時所在的群組。例如，新的使用者可能登入架構為使用者模式的用戶端。用戶端接著會留在先前使用者所在的群組。

您可以按下「用戶端」>「政策」，再按下「通訊設定」，來架構這些設定。請參閱：

[<group_name> 的通訊設定](#)

在使用者模式和電腦模式之間切換 **Windows** 用戶端

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方，選取包含使用者或電腦的群組。
3. 在「用戶端」標籤上，在表格中的電腦或使用者名稱上按下滑鼠右鍵，然後選取「切換至電腦模式」或「切換至使用者模式」。

此模式是屬於切換設定，因此始終會切換顯示其中一種模式。表格中的資訊會隨新設定而變更。

將用戶端架構為偵測非受管裝置

未授權裝置能夠以多種方式連線至網路，例如，會議室的實體存取或非授權無線網路存取點。若要在各個端點強制執行政策，您必須能夠迅速偵測出網路中是否有新的裝置出現。您必須判斷這些裝置是否安全。您可以啟用任何用戶端作為非受管偵測程式，以偵測不明裝置。不明裝置是未執行 Symantec Endpoint Protection 用戶端軟體的非受管裝置。如果非受管裝置是電腦，您可以在該電腦上安裝 Symantec Endpoint Protection 用戶端軟體。

裝置啟動時，作業系統會將下列流量傳送至網路，以告知其他電腦有裝置出現：

- 位址解析通訊協定 (ARP) 流量 (ICMPv4)
 - 芳鄰搜尋通訊協定 (NDP) 流量 (ICMPv6)
- 自 14.2 起支援 ICMPv6。

啟用成為非受管偵測程式的用戶端會收集此封包資訊，然後傳送至管理伺服器。管理伺服器會在封包中搜尋裝置的 MAC 位址和 IP 位址。伺服器會將這些位址與伺服器資料庫中的現有 MAC 位址與 IP 位址清單相互比對。如果伺服器找不到相符的位址，伺服器會記錄該裝置為新裝置。然後您可以決定該裝置是否安全。由於用戶端只傳輸資訊，因此不會使用額外的資源。

您可以架構非受管偵測程式忽略某些裝置，例如印表機。您也可以設定電子郵件通知，以便在非受管偵測程式偵測出不明裝置時通知您。

若要架構用戶端成為非受管偵測程式，必須執行下列動作：

-
- 啟用網路威脅防護。請參閱：
[在用戶端電腦上從主控台執行指令](#)
 - 將用戶端切換為電腦模式。請參閱：
[在使用者模式和電腦模式之間切換 Windows 用戶端](#)
 - 任何時間都在執行不間斷的電腦上安裝用戶端。

自 14.3 RU1 起，將 Linux 用戶端啟用為非受管偵測程式已棄用。

架構非受管偵測程式

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下，選取包含要啟用為非受管偵測程式的用戶端的群組。
3. 在「用戶端」標籤上，在要啟用成為非受管偵測程式的用戶端上按下滑鼠右鍵，然後按下「啟用為非受管偵測程式」。
4. 若要指定一個或多個裝置由非受管偵測程式排除在偵測之外，請按下「架構非受管偵測程式」。
5. 在「用戶端名稱 發生非受管偵測程式例外」對話方塊中，按一下「新增」。
6. 在「新增非受管偵測程式例外」對話方塊中，按下下列其中一個選項：
 - 「排除偵測 IP 位址範圍」，然後輸入多個裝置的 IP 位址範圍。
 - 「排除偵測 MAC 位址」，然後輸入裝置的 MAC 位址。
7. 按一下「確定」>「確定」。
8. 若要顯示用戶端偵測到的未授權裝置清單，請按一下「首頁」。
9. 在「首頁」頁面的「安全狀態」區段中，按下「更多詳細資料」。
10. 在「安全狀態詳細資料」對話方塊中，捲動至「不明裝置失敗」表格。
11. 關閉對話方塊。

查看是否正在偵測非受管用戶端

1. 移至「主頁」頁面，然後按一下「安全狀態」區域中的「檢視詳細資料」。
2. 「安全狀態詳細資料」視窗出現時，按一下「不明裝置失敗」。
「偵測到的不明裝置總數」顯示非受管裝置數目。除了電腦之外，這還包括存取點、路由器、交換器和其他裝置。
3. 若要過濾無關裝置，請移至「用戶端」頁面，然後以滑鼠右鍵按一下非受管偵測程式。
4. 按一下「架構非受管偵測程式」，然後新增要過濾的裝置的 IP 或 Mac 位址。

用密碼保護 Symantec Endpoint Protection 用戶端

您在使用者每次執行特定任務時都要求在用戶端電腦上啟用密碼保護，以提高勒索軟體攻擊的安全性。勒索軟體攻擊可以停止或解除安裝用戶端服務，然後啟動攻擊。

您可以使用密碼保護的用戶端任務

您可以針對下列動作設定用戶端密碼：

- 使用 `smc - stop` 命令來停止用戶端服務。
- 使用 CleanWipe 手動或自動解除安裝用戶端。
- 匯入或匯出政策檔案。
- 匯入用戶端通訊設定檔案 (Sylink.xml)。
- 顯示用戶端使用者介面 (針對所有版本都是選用項目)。

針對 Symantec Endpoint Protection Manager 14.3 RU9 和更早版本，針對這些動作設定密碼是選用項目。從 14.3 RU4 到 14.3 RU9，會出現一則訊息，提醒您至少啟用其中一個密碼選項。

從 14.3 RU10 開始，需要密碼才能執行這些任務。您建立此預設用戶端密碼，而此密碼會在您安裝或升級 Symantec Endpoint Protection Manager 時套用至所有網站。您可以 [修改每個群組的密碼](#)來自訂此密碼。

- 如果用戶端位於尚未自訂密碼的群組中，則請使用預設用戶端密碼。
- 如果用戶端位於已自訂密碼的群組中，則請使用自訂的密碼。

如何使用密碼保護用戶端？

- 在 14.3 RU9 和更早版本中，您可以在安裝管理伺服器之後建立群組密碼。
- 從 14.3 RU10 開始，您需要在安裝或升級管理伺服器時建立預設用戶端密碼。此預設用戶端密碼適用於所有網站和所有群組。安裝之後，您可以[修改每個群組的密碼](#)來自訂此密碼。
請參閱[架構 Symantec Endpoint Protection Manager 安裝](#)。

建立群組密碼

若要為每個群組建立唯一密碼，請遵循下列步驟：

1. 在主控台中，按一下「用戶端」>「用戶端」，然後選取您想要設定密碼防護的群組。
2. 在「政策」標籤上，按一下「密碼」。
舊版 Symantec Endpoint Protection 可能具有一些措辭不同的選項。
如需此對話方塊中設定的詳細資訊，請參閱：[用戶端密碼設定](#)
3. 在「用戶端密碼設定」對話方塊 (從 14.3 RU10 開始) 中，執行下列動作：
 - 保留「使用預設用戶端密碼」，以使用您在安裝管理伺服器期間所建立的密碼。
此預設密碼適用於所有網站。您無法復原預設密碼，但可以重新架構管理伺服器或使用群組層級密碼進行變更。
 - 選取「使用群組用戶端密碼」，以僅建立此群組的密碼。群組密碼會覆寫預設密碼。
4. 在「密碼」和「確認密碼」文字方塊中，鍵入相同密碼。
 - 如果方塊顯示為灰色，此群組會從父群組繼承政策。您必須先編輯父群組中的密碼設定，或停用此群組的繼承，才能繼續。
請參閱[停用群組繼承](#)
 - 在 14.3 RU9 和更舊版本中，如果您看到「將密碼設定套用至非繼承的子群組」核取方塊，則此群組是其他用戶端群組的父群組。若要修改不會從父系繼承其設定的任何子群組的密碼防護設定，請勾選此選項。
 - 如果您看到密碼強度薄弱的訊息，則請考慮增加您密碼的強度。不過，您仍然可以儲存密碼。
5. 勾選您想要將密碼設為用戶端使用者必要項目的核取方塊。
6. 按一下「確定」。

密碼需求

如需密碼需求的相關資訊，請參閱[建立用戶端密碼](#)。

如何復原忘記的用戶端密碼？

如果您忘記預設用戶端密碼，則可以使用下列方式予以復原：

- 針對 14.3 RU9 和更早版本，請變更群組的密碼。
- 從 14.3 RU10 開始，請使用下列其中一種方法：
 - 變更每個群組的密碼。套用至群組的密碼會覆寫預設用戶端密碼。如果您想要每個群組都具有唯一密碼，則也可以使用此選項。
 - 只要用戶端連線至管理伺服器，就重新架構管理伺服器。
 - 解除安裝管理伺服器，然後將其重新安裝。

匯出受密碼保護的用戶端安裝套件

在 Symantec Endpoint Protection Manager 14.3 RU9 和更早版本中，您可以匯出在受密碼保護和非密碼保護的 Windows 用戶端以及不受密碼保護的 Mac 用戶端上執行的通訊更新套件。

從 14.3 RU10 開始，您可以匯出只在受密碼保護的 Windows 用戶端以及不受密碼保護的 Mac 用戶端上執行的通訊更新套件。在您將匯出的 Windows 套件複製至目標機器並執行 SylinkDrop 工具之後，必須提供密碼。

[使用「通訊更新套件部署」還原用戶端伺服器通訊](#)

使用 SylLinkDrop 工具還原用戶端伺服器通訊設定

在 14.3 RU10 中，已從通訊更新套件部署中移除「密碼防護」選項。

防止使用者停用 Symantec Endpoint Protection 用戶端

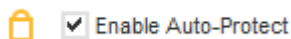
以 Symantec Endpoint Protection Manager 管理員身分，透過設定使用者控制等級或鎖定政策選項，防止使用者停用用戶端電腦上的防護。您使用的方法取決於政策類型以及在 Symantec Endpoint Protection Manager 中引入該政策的時間。例如，防火牆政策 (版本 11) 使用控制等級，而病毒和間諜軟體防護政策 (政策 12.1.x) 則使用鎖定。

NOTE

當您建立新政策時，所有設定皆會依預設解除鎖定。用戶端使用者可以變更設定，此無安全性問題。因此，賽門鐵克建議您防止使用者停用防護，並變更設定。如果需要解決用戶端電腦上的問題，或允許小型內部開發人員群組測試內部開發的應用程式，則您可能希望允許用戶端使用者停用防護。

步驟 1：使用掛鎖鎖定政策設定

您可以點選掛鎖，鎖定和解除鎖定部分政策設定。用戶端使用者無法變更已鎖定的設定。可鎖定的設定旁會顯示掛鎖圖示。您可以鎖定和解除鎖定病毒和間諜軟體防護設定、竄改防護設定、傳送設定和入侵預防設定。



使用掛鎖鎖定政策

1. 在主控台中，按一下「用戶端」。
2. 按下要限制的用戶端群組，然後按下「政策」標籤。
3. 展開「位置特定政策」，然後在政策旁邊按一下「任務 > 編輯政策 > 編輯共用」。
4. 請在每個政策中鎖定掛鎖以進行以下設定。

政策	政策
病毒和間諜軟體防護	在「Windows 設定」下，鎖定： • 自動防護 > 啟用自動防護 • 下載防護 > 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 • SONAR > 啟用 SONAR (14.3 RU4 和更舊版本) • SONAR > 啟用可疑的偵測行為 (14.3 RU4 和更舊版本) • 提早啟動防惡意軟體驅動程式 > 啟用 Symantec 提早啟動防惡意軟體 • Internet 電子郵件自動防護 > 啟用 Internet 電子郵件自動防護 (14.2 和更舊版本) • Microsoft Outlook 自動防護 > 啟用 Microsoft Outlook 自動防護 • Lotus Notes 自動防護 > 啟用 Lotus Notes 自動防護 (14.2 和更舊版本) 在「全域掃描選項」下鎖定： • 針對以下項目啟用 Insight • 啟用 Bloodhound 啟發式病毒偵測
入侵預防	在「入侵防禦」下鎖定： - 啟用網路入侵預防 - 啟用瀏覽器入侵預防 - 啟用 URL 信譽
記憶體攻擊緩和	記憶體攻擊緩和 > 啟用記憶體攻擊緩和
Web 和雲端存取防護	在「Web 和雲端存取防護」下，鎖定「啟用 Web 和雲端存取防護」

步驟 2：使用使用者控制等級鎖定政策設定

若要鎖定防火牆以及應用程式和裝置控制政策，請將使用者控制等級從用戶端控制變更為伺服器控制。

NOTE

如果您不想針對所有群組變更政策，請在要進行變更的群組上停用政策繼承。如果編輯共用政策，即使政策繼承已停用，編輯後的政策也會套用至已套用共用政策的每個群組。

鎖定防火牆以及應用程式和裝置控制政策

1. 在主控台中，按一下「用戶端」。
2. 按下要限制的用戶端群組，然後按下「政策」標籤。
3. 展開「位置限定的設定」。
4. 在「用戶端使用者介面控制設定」的右側，按一下「工作 > 編輯設定」。
5. 按下「伺服器控制」或「混合控制」，然後按下「自訂」。
6. 在「用戶端使用者介面設定」對話框 (伺服器控制) 或標籤 (混合控制) 上，取消選取：
 - a. 允許下列使用者啟用和停用防火牆
 - b. 允許使用者啟用和停用應用程式裝置控制。
7. 按一下「確定」>「確定」。

如需詳細瞭解使用者控制等級，請參閱：[允許使用者變更 Symantec Endpoint Protection 用戶端使用者介面的設定](#)

步驟 3：更新用戶端政策

進行這些變更後，群組中的用戶端會根據群組的通訊設定接收更新的政策：

- 如果群組處於推送模式，Symantec Endpoint Protection Manager 會提示用戶端花幾秒的時間登入。
- 如果群組處於提取模式，用戶端會在下次排程的活動訊號時登入。

NOTE

如果您希望它們在下次活動訊號之前實現，可以從 Symantec Endpoint Protection 用戶端更新政策，提示用戶端登入並更新其政策。請參閱：

[更新用戶端政策](#)

用戶端更新政策之後，當用戶端使用者在 Symantec Endpoint Protection 通知區域圖示上按下滑鼠右鍵時，「停用 Symantec Endpoint Protection」會顯示為灰色。

NOTE

如果「停用 Symantec Endpoint Protection」選項未顯示為灰色，請確認您已鎖定該群組的所有政策設定。

允許使用者變更 Symantec Endpoint Protection 用戶端使用者介面的設定

使用者可以在用戶端使用者介面上變更哪些設定？

在受管用戶端上，您可以為使用者開放許多防護設定，讓他們可以在用戶端上進行設定。例如，您可以允許用戶端使用者在掃描發現偵測時新增防火牆規則或指定動作。

請允許用戶端使用者使用以下方式變更部分設定 (具體取決於政策類型或設定)：

- 鎖定和解鎖掛鎖 (SEPM 版本 12.1.x 及更新版本)：除「防火牆」和「應用程式和裝置控制」政策之外的所有其他政策。Symantec Endpoint Protection Manager 中任何有掛鎖的設定都是您可以允許或封鎖用戶端使用者變更的設定。
- 使用者控制等級：「防火牆」政策和「應用程式和裝置控制」政策以及用戶端使用者介面設定，如顯示用戶端盾牌圖示。

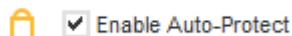
使用使用者控制等級來提供對特定功能的用戶端使用者控制。

如需詳細瞭解您可以在用戶端上啟用或封鎖的設定，請參閱：[用戶端使用者介面混合控制設定：用戶端/伺服器控制設定](#)和 [用戶端使用者介面設定](#)

使用者無法存取所有用戶端功能。

以掛鎖鎖定用戶端設定

您可以點選掛鎖，鎖定和解除鎖定部分政策設定。用戶端使用者無法變更已鎖定的設定。可鎖定的設定旁會顯示掛鎖圖示。除了「防火牆」和「應用程式和裝置控制」的設定以外，您可以鎖定和解除鎖定大多數政策設定。您可以透過使用者控制等級來配置這些設定。



使用者控制等級說明

如果您執行下列任一項工作，則可以架構用戶端上的使用者介面設定：

- 將用戶端使用者控制等級設定為伺服器控制。
- 將用戶端使用者控制等級設定為混合控制，並將「用戶端/伺服器控制設定」標籤上的父系功能設定為「伺服器」。
例如，您可以將「顯示/隱藏通知區域圖示」選項設定為「用戶端」。通知區域圖示會出現在用戶端上，而使用者可以選擇顯示或隱藏圖示。如果您將「顯示/隱藏通知區域圖示」選項設定為「伺服器」，則可以選擇是否要在用戶端上顯示通知區域圖示。

NOTE

這些設定大部分僅適用於 Windows 用戶端。您只能在伺服器控制中架構 Mac 用戶端上的幾個選項。

使用者控制等級也會決定用戶端使用者介面不顯示項目、顯示部分功能集或顯示完整的使用者介面。

如果您將用戶端設定為「混合控制」或「伺服器控制」，但未鎖定選項，則使用者可變更設定。這些變更會保留在原位，直到 Symantec Endpoint Protection Manager 出現下次活動訊號。鎖定各種政策中的政策選項可確保用戶端使用者無法對設定進行變更，即使處於「用戶端控制」也是如此。

部分受管設定具有相依性。例如，使用者可能有權限架構防火牆規則，但無法存取用戶端使用者介面。由於使用者無法存取「架構防火牆規則」對話方塊，也就無法建立規則。

NOTE

無論「位置限定的設定」組態為何，非管理員的 Windows 使用者群組均無法變更 Symantec Endpoint Protection 用戶端使用者介面中的設定。即使在您設定這些選項之後，Windows 10 管理員仍可透過通知區域圖示停用產品。但是，他們無法透過用戶端使用者介面停用個別防護技術。

當伺服器套用隔離所政策時，在「用戶端控制」或「混合控制」中執行的用戶端會切換成「伺服器控制」。

更多資訊

如需詳細瞭解三種使用者控制等級的差別，請參閱：[用戶端使用者介面控制設定](#)

如需詳細瞭解您可以啟用的設定，請參閱：[用戶端使用者介面混合控制設定：用戶端/伺服器控制設定](#) 和 [用戶端使用者介面設定](#)

透過使用者控制等級來鎖定和解除鎖定設定

鎖定和解除鎖定設定

1. 在「用戶端」頁面上，選取包含您希望受影響的用戶端的群組。
2. 在「政策」標籤上，展開「位置限定的設定」。
3. 在「用戶端使用者介面控制設定」右側，按一下「工作」，然後按一下「編輯設定」。
4. 選擇「伺服器控制」或「混合控制」，然後按一下「自訂」(如果尚未設定這些選項)。
如果您選擇「用戶端控制」，請按「確定」。用戶端使用者可以設定「用戶端使用者介面」對話框的任何設定。
 - 如果您選擇「伺服器控制」，系統將開啟「用戶端使用者介面設定」對話框。
在「用戶端使用者介面設定」標籤上，勾選選項的核取方塊，這樣就能在用戶端上使用選項。
 - 如果您選擇「混合控制」，系統將開啟「用戶端使用者介面混合控制設定」對話框。執行下列其中一項動作：

- 如此一來您就可以僅從管理伺服器進行設定，並按「伺服器」鎖定選項。
您對「伺服器」設定的任何病毒及間諜軟體防護設定，會覆寫用戶端上的設定。
- 因此用戶端使用者可以按「用戶端」，在用戶端解鎖選項上進行設定。預設會針對所有設定選取用戶端，但不包含病毒及間諜軟體設定。

針對一些已設定為「伺服器」的選項，請按下「用戶端使用者介面設定」標籤設定這些選項。例如，若要啟用防火牆設定，請在「防火牆」政策中架構設定。

如需瞭解在主控台何處架構其餘設定為「伺服器」的選項，請按下「說明」。

[為網路服務啟用通訊而非新增規則](#)

[啟用網路入侵預防或瀏覽器入侵預防](#)

[架構混合控制的防火牆設定](#)

5. 按一下「確定」>「確定」。

收集使用者資訊

在進行用戶端軟體安裝程序或政策更新時，您可以提示用戶端電腦的使用者輸入自己的相關資訊。您可以收集有關員工的資訊，包括行動電話號碼、工作職稱和電子郵件地址等。收集此資訊之後，您必須手動維護和更新資訊。

當管理伺服器偵測到哪些用戶端電腦有問題 (例如感染或超出定義) 時，此資訊非常有用。然後，您可以找到電腦的位置以及使用它的使用者。

NOTE

用戶端電腦上第一次出現啟用訊息後，如果使用者已回應所需的資訊，訊息則不會再次出現。即使使用者編輯任何欄位，或停用並再次啟用訊息，用戶端也不會顯示新訊息。然而，使用者可以隨時編輯資訊，而且管理伺服器也可擷取該資訊。

如需詳細資訊，請參閱：

[管理用戶端安裝套件](#)

收集使用者資訊

1. 在主控台中，按下「管理員」，再按下「安裝套件」。
2. 在「安裝套件」窗格，按下「用戶端安裝套件」。
3. 在「工作」下方，按下「設定使用者資訊收集」。
4. 在「設定使用者資訊收集」對話方塊中，勾選「收集使用者資訊」。
5. 在「彈出式訊息」文字方塊中，輸入您想要使用者在收到提示資訊時閱讀的訊息。
6. 如果您想要讓使用者能延後收集使用者資訊，請勾選「啟用稍後提醒我」，然後以分鐘為單位設定時間。
7. 在「選取要顯示來讓使用者輸入的欄位」下，選擇要收集的資訊類型，然後按下「新增」。

按 Shift 鍵或 Ctrl 鍵可同時選擇一個或多個欄位。

8. 在「非必填」欄位中，在您要定義為使用者選填的欄位旁勾選核取方塊。
9. 按下「確定」。

使用 AppleScript 程序檔檢查 Mac 用戶端

(適用於 14.3 RU2 和更新版本)

AppleScript 與 Symantec Endpoint Protection for Mac 用戶端的整合可讓您建立和執行 AppleScript 程序檔，以查詢或控制 Mac 用戶端。

用於查詢 Mac 用戶端的預先定義程序檔無法使用。您可以根據需求彈性地建立程序檔。

您可以在程序檔編輯器中建立並執行程序檔，也可以從指令行執行程序檔。使用 Mac 功能，您也可以排程在指定的時間自動執行程序檔。

在程序檔編輯器中建立和執行 **AppleScript** 程序檔：

1. 在 Mac 裝置上，開啟程序檔編輯器，並建立您要在 Mac 裝置上執行的程序檔。
您可以使用下面提供的程序檔範例。
2. 若要測試程序檔，請按一下工具列上的「執行」。
3. 以最符合您需求的格式儲存程序檔。

從指令行執行 **AppleScript** 程序檔：

1. 在 Mac 裝置上，開啟「終端機」視窗。
2. 執行您要的程序檔。

Table 134: Mac 用戶端的 AppleScript 程序檔範例

動作	程序檔範例
取得上次掃描時間	要在程序檔編輯器中執行的程序檔： tell application "Symantec Endpoint Protection" get last scan time end tell 從指令行執行的程序檔： osascript -e 'tell app "Symantec Endpoint Protection" to get last scan time'
取得產品版本	要在程序檔編輯器中執行的程序檔： tell application "Symantec Endpoint Protection" get version end tell 從指令行執行的程序檔： osascript -e 'tell app "Symantec Endpoint Protection" to get version'
取得內容版本	要在程序檔編輯器中執行的程序檔： tell application "Symantec Endpoint Protection" get definition information end tell 從指令行執行的程序檔： osascript -e 'tell app "Symantec Endpoint Protection" to get definition information'
執行 LiveUpdate	要在程序檔編輯器中執行的程序檔： tell application "Symantec Endpoint Protection" activate tell main window to run LiveUpdate end tell 從指令行執行的程序檔： osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to run LiveUpdate' -e 'end tell'

動作	程序檔範例
執行快速掃描	要在程序檔編輯器中執行的程序檔： <pre>tell application "Symantec Endpoint Protection" activate tell main window to quick scan end tell</pre> 從指令行執行的程序檔： <pre>osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to quick scan' -e 'end tell'</pre>
執行 FullScan	要在程序檔編輯器中執行的程序檔： <pre>tell application "Symantec Endpoint Protection" activate tell main window to full scan disks end tell</pre> 從指令行執行的程序檔： <pre>osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to full scan disks' {"/"}' -e 'end tell'</pre>
執行 FileScan	要在程序檔編輯器中執行的程序檔： <pre>tell application "Symantec Endpoint Protection" activate tell main window to full scan files {"/tmp"} end tell</pre> 從指令行執行的程序檔： <pre>osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to scan files' {"/tmp"}' -e 'end tell'</pre>

管理遠端用戶端

您的網路可能會包含一些從不同位置連線到網路的用戶端。管理這些用戶端的方式，可能與管理僅從網路內部連線之用戶端的方式不同。您可能需要管理一些始終透過 VPN 遠端連線的用戶端，或由於員工出差而從多個位置進行連線的用戶端。您可能需要為一些不在管理控制範圍內的電腦管理安全性。例如，您可能會提供客戶、承包商、供應商或業務夥伴有限的網路存取權限。部分員工可能會使用自己的個人電腦連線到您的網路，因此，您可能需要以不同的方式管理這些用戶端。

在所有上述情況下，您都必須應付更大的安全性風險。連線或用戶端電腦的安全性可能會比較低，而且您對部分用戶端的控制權可能會較少。為了將這些風險對整體網路安全性的影響降至最低，您應評估各個用戶端對網路的不同類型遠端存取權限。然後，您就可以根據評估套用更嚴格的安全性政策。

若要基於安全性風險的差異以不同方式管理連線到網路的用戶端，您可以使用 Symantec Endpoint Protection 的位置感測功能。

您需要根據用戶端的位置，為可能對網路造成較大風險的用戶端套用不同的政策。Symantec Endpoint Protection 中的位置會定義成用戶端電腦用於連線到網路的連線類型。位置也可以包含有關連線位於公司網路內部或外部的資訊。

您可以為用戶端群組定義位置。然後為每個位置指派不同的政策。部分安全性設定可以指派給整個群組，不論位置為何。而部分設定則會視位置而有所不同。

Table 135: 管理遠端用戶端

工作	說明
根據安全性風險評估設定群組	如需詳細資訊，請參閱： 管理用戶端群組
設定遠端用戶端群組的位置	如需詳細資訊，請參閱： 管理遠端用戶端的位置
架構各位置的通訊設定	如需詳細資訊，請參閱： 架構位置的通訊設定
加強安全性政策	如需詳細資訊，請參閱： 關於加強遠端用戶端的安全政策
開啟用戶端通知	如需詳細資訊，請參閱： 關於開啟遠端用戶端的通知
自訂用戶端日誌管理設定	自訂遠端用戶端的日誌設定，特別是如果用戶端離線多天。若要減少頻寬和管理伺服器負載，請進行下列變更： - 將用戶端設定為不上傳其日誌到管理伺服器。 - 將用戶端設定為僅上傳用戶端安全日誌。 - 將過濾日誌事件設定為僅上傳指定事件。 建議要上傳的事件包括定義更新，否則會對修復故障有副作用。 - 延長日誌的存留時間。 較長的存留時間可以讓您檢閱更多的病毒和間諜軟體事件資料。
監視遠端用戶端	如需詳細資訊，請參閱： 關於從管理伺服器監控遠端用戶端 從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端

管理遠端用戶端的位置

設定需要管理的群組後，請新增位置。如果您的安全策略有此需求，則每個群組可以有不同的位置。您可在 Symantec Endpoint Protection Manager 主控台中設定依照位置觸發自動政策切換的條件。位置偵測功能會根據用戶端符合的位置條件，自動將您指定的安全性政策套用到用戶端。

位置條件可依據數個準則。這些準則包含 IP 位址、網路連線類型，以及用戶端電腦是否可以連線到管理伺服器。您可以根據指定的準則，允許或攔截用戶端連線。

位置可以套用到您為其建立的群組，也可套用到從該群組繼承的任何子群組。因此最好能夠在 My Company 群組層級建立任何用戶端都可以使用的位置。然後，在子群組層級上為特定的群組建立位置。

如果您建立的群組和位置的數目較少，安全性政策和設定的管理會比較簡單。不過，由於網路的複雜性和其安全性需求，可能需要更多的群組和位置。視您所需要的不同安全設定、日誌相關設定、通訊設定和政策數目而定，會決定您建立多少群組和位置。

您想為遠端用戶端自訂的部分組態選項是與位置無關的。這些選項可以從父群組繼承，也可以獨立設定。如果您建立單一組來包含所有遠端用戶端，則對群組中的用戶端來說，與位置無關的設定都是相同的。

下列設定與位置無關：

- 自訂入侵預防特徵
- 系統鎖定設定
- 網路應用程式監控設定
- LiveUpdate 內容政策設定
- 用戶端日誌設定
- 用戶端伺服器通訊設定
- 一般安全性相關設定，包括位置感應和竄改防護

若要自訂上述任何與位置無關的設定，例如處理用戶端日誌的方式，就需要建立不同的群組。

某些設定會視位置而定。

基於最佳實務，請勿允許使用者關閉下列防護：

- 自動防護
- 行為分析
- 竄改防護
- 您所建立的防火牆規則

Table 136: 可執行的位置感應工作

工作	說明
規劃位置	您應該衡量環境中所需的各種安全性政策類型，藉此決定應使用的位置。然後，即可判斷定義每個位置所要使用的準則。最好同時規劃群組和位置。請參閱： 管理用戶端群組 以下範例可能對您很有用： • 設定第一種狀況的位置偵測條件 • 設定第二種狀況的位置偵測條件
啟用位置偵測	若要根據用戶端的連線位置來控制指派給用戶端的政策，您可以啟用位置感測。請參閱： 啟動用戶端位置偵測
新增位置	可新增群組位置。請參閱： 將位置新增到群組
指派預設位置	所有群組都必須有個預設位置。安裝主控台後，僅有一個名為「預設值」的位置。建立新群組後，預設位置永為「預設值」。稍後新增其他位置之後，您可以變更預設位置。 如果發生下列情形之一，會使用預設位置： • 多個位置中有一個符合位置準則，且上一個位置不符合位置準則。 • 您正在使用位置偵測，而所有位置都不符合準則。 • 位置在政策中已重新命名或變更。用戶端接收新政策時會復原為預設位置。 如需詳細資訊，請參閱： 變更預設位置
架構各位置的通訊設定	您也可以根據位置，架構管理伺服器與用戶端之間的通訊設定。請參閱： 架構位置的通訊設定

更多資訊

- [管理遠端用戶端](#)
- [Symantec Endpoint Protection 位置偵測最佳實務](#)

啟動用戶端位置偵測

如果要根據用戶端的連線位置來指定用戶端政策，您可啟動用戶端位置感測。

勾選「記住上次的位置」後，當用戶端連線至網路時，將從上次使用的位置指定政策。如果啟用位置偵測，用戶端會在幾秒後自動切換至適當的政策。與特定位置關聯的政策會判斷用戶端的網路連線。如果停用了位置偵測，即使用戶端是在伺服器控制中，用戶端仍可手動切換至任意位置。如果啟用隔離所位置，用戶端可能會在幾秒後切換至隔離所政策。

如果取消勾選「記住上次的位置」後，當用戶端連線至網路時，將從預設位置指定政策。用戶端無法連接到最後使用的位置。如果啟用位置偵測，用戶端會在幾秒後自動切換至適當的政策。與特定位置關聯的政策會判斷用戶端的網路連線。如果停用了位置偵測，即使用戶端是在伺服器控制中，使用者仍可手動切換至任意位置。如果啟用隔離所位置，用戶端可能會在幾秒後切換至隔離所政策。

啟動用戶端位置感測

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方，選取要實作自動位置切換的群組。
3. 在「政策」標籤中，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
4. 在「與位置無關的政策和設定」下方，按下「一般設定」。
5. 在「一般設定」對話方塊之「一般設定」標籤的「位置設定」下方，勾選「記住上次的位置」。

此選項預設為啟用。用戶端一開始會指派給與用戶端最後連線至網路的位置相關聯的政策。

6. 勾選「啟用位置偵測」。

依據預設，會啟用位置偵測。用戶端會自動指派給使用者嘗試連接至網路位置相關聯的政策。

7. 按下「確定」。

更多資訊

[將位置新增到群組](#)

將位置新增到群組

將位置新增到群組時，您可以指定觸發該群組中的用戶端切換到該位置的條件。您也必須將適當的政策和設定套用到各位置，位置感應才會有效。

將位置新增到群組

1. 在主控台中，按一下「用戶端」。
 2. 在「用戶端」頁面的「用戶端」下，選取要新增一個或多個位置的群組。
 3. 在「政策」標籤中，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
- 您只能針對未繼承父群組政策的群組新增位置。
- 您也可以按下「新增位置」來執行「新增位置」精靈。
4. 在「用戶端」頁面的「工作」下方，按下「管理位置」。
 5. 在「管理位置」對話方塊的「位置」下方，按下「新增」。
 6. 在「新增位置」對話方塊中，輸入新位置的名稱和敘述，然後按下「確定」。
 7. 在「切換至這個位置的狀況」方塊的右側，按下「新增」。
 8. 在「類型」清單中選取條件，然後選取該條件所適用的定義。

若用戶端電腦符合指定的準則，便會切換到該位置。

-
9. 按下「確定」。
 10. 若要新增更多條件，請按下「新增」，然後選取「含 **AND** 關係的準則」或「含 **OR** 關係的準則」。
 11. 按下「確定」。

更多資訊

[關於加強遠端用戶端的安全政策](#)

變更預設位置

首次安裝 Symantec Endpoint Protection Manager 時，只有名為「預設值」的單一位置存在。這時，所有群組的預設位置都是「預設值」。每個群組都必須有個預設位置。建立新群組時，Symantec Endpoint Protection Manager 主控台會自動將其預設位置設為「預設值」。

新增其他位置後，您便可指定其他位置作為某群組的預設位置。您或許偏好指定如家裡 (Home) 或出差 (Road) 的位置為預設位置。

如果發生下列情形之一，會使用群組的預設位置：

- 多個位置中有一個符合位置準則，且上一個位置不符合位置準則。
- 您正在使用位置偵測，而所有位置都不符合準則。
- 位置在政策中已重新命名或變更。用戶端接收新政策時會復原為預設位置。

變更預設位置

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面的「用戶端」下方，按下要指派不同預設位置的群組。
3. 在「政策」標籤中，取消勾選「從父群組 "群組名稱" 繼承政策和設定」。
4. 在「工作」下方，按下「管理位置」。
5. 在「管理位置」對話方塊的「位置」下，選取要作為預設位置的位置。
6. 在「敘述」下，勾選「如果發生衝突則設定此位置為預設位置」。

在為群組指派另一個位置前，預設位置通常會是預設位置。

7. 按下「確定」。

更多資訊

[管理遠端用戶端的位置](#)

設定第一種狀況的位置偵測條件

如果您使用遠端用戶端，在最單純的狀況下，通常是使用 My Company 群組與三個位置。這是第一種狀況。

若要管理這種狀況下的用戶端安全性，您可以在 My Company 群組之下建立下列位置以便使用：

- 登入辦公室的辦公室用戶端。
- 從遠端透過 VPN 登入公司網路的遠端用戶端。
- 從遠端未透過 VPN 登入 Internet 的遠端用戶端。

由於沒有 VPN 連線的遠端位置最不安全，因此會有最安全的政策。最佳實務準則是，請一律將這個位置設為預設位置。

NOTE

如果您關閉 My Company 群組繼承，然後新增群組，則新增的群組不會繼承您針對 My Company 群組設定的位置。

下列建議是第一種狀況的最佳實務做法。

針對位在辦公室中的用戶端設定辦公室位置

1. 在「用戶端」頁面上，選取要新增位置的群組。
2. 在「政策」標籤的「工作」下方，按下「新增位置」。
3. 在「新增位置精靈」中，按「下一步」。
4. 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「下一步」。
5. 在清單方塊中，按下清單中的「用戶端可以連線到管理伺服器」，然後按「下一步」。
6. 按下「完成」，然後按下「確定」。
7. 在「工作」下方，按下「管理位置」，然後選取您建立的位置。
8. 按下「新增」，再按下「含 **AND** 關係的準則」。
9. 在「指定位置條件」對話方塊的「類型」清單中，按下「網路連線類型」。
10. 按下「如果用戶端電腦不使用下方指定的網路連線類型」。
11. 在底部清單方塊中，選取您組織使用的 VPN 用戶端名稱，然後按下「確定」。
12. 按下「確定」結束「管理位置」對話方塊。

針對透過 VPN 登入的用戶端設定遠端位置

1. 在「用戶端」頁面上，選取要新增位置的群組。
2. 在「政策」標籤的「工作」下方，按下「新增位置」。
3. 在「新增位置精靈」中，按「下一步」。
4. 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「下一步」。
5. 在清單方塊中，按下「網路連線類型」。
6. 在「連線類型」清單方塊中，選取您的組織使用的 VPN 用戶端名稱，然後按「下一步」。
7. 按下「完成」。
8. 按下「確定」。

為未透過 VPN 登入的用戶端設定遠端位置

1. 在「用戶端」頁面上，選取要新增位置的群組。
2. 在「政策」標籤的「工作」下方，按下「新增位置」。
3. 在「新增位置精靈」中，按「下一步」。
4. 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「下一步」。
5. 在清單方塊中，保留「無特定條件」，然後按「下一步」。
使用這些設定之後，此位置的政策會最為嚴格且安全，可作為預設的位置政策。
6. 按下「完成」，然後按下「確定」。

更多資訊

- [設定第二種狀況的位置偵測條件](#)
- [管理遠端用戶端](#)

設定第二種狀況的位置感應條件

在第二種狀況中，您可以使用第一種狀況中指定的兩個遠端位置，以及兩個辦公室位置，這樣總共有四個位置。

您會新增下列辦公室位置：

- 透過乙太網路連線登入的辦公室用戶端。
- 透過無線連線登入的辦公室用戶端。

這可簡化管理程式，使所有的用戶端處於預設的伺服器控制模式。如果要對使用者進行與不可進行的細部控制，有經驗的管理員可使用混合控制。一般使用者可控制混合控制設定的某些安全性設定，但必要時，您可以覆寫使用者所做的變更。「用戶端控制」讓使用者控制更多項目，但是也相對提高網路安全風險。

賽門鐵克建議您只在下列狀況使用用戶端控制：

- 使用者必須相當瞭解電腦安全性。
- 絕對必要時。

NOTE

辦公室中的某些用戶端使用乙太網路連線，某些用戶端使用無線連線。因此，程序的最後一項條件設為無線連線。這項條件可供您建立乙太網路位置防火牆政策規則，以在同時使用兩種連線時，攔截所有的無線連線流量。

針對透過乙太網路登入的用戶端設定辦公室位置

1. 在「用戶端」頁面上，選取要新增位置的群組。
2. 在「工作」下方，按下「新增位置」。
3. 在「新增位置精靈」中，按「下一步」。
4. 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「下一步」。
5. 在清單方塊中，選取「用戶端可以連線到管理伺服器」，然後按「下一步」。
6. 按下「完成」。
7. 按下「確定」。
8. 在「工作」下方，按下「管理位置」，然後選取您建立的位置。
9. 在「切換至這個位置的狀況」旁，按下「新增」，然後選取「含 **AND** 關係的準則」。
10. 在「指定位置條件」對話方塊的「類型」清單中，按下「網路連線類型」。
11. 按下「如果用戶端電腦不使用下方指定的網路連線類型」。
12. 在底部清單方塊中，選取您組織使用的 VPN 用戶端名稱，然後按下「確定」。
13. 按下「新增」，再按下「含 **AND** 關係的準則」。
14. 在「指定位置條件」對話方塊的「類型」清單中，按下「網路連線類型」。
15. 按下「如果用戶端電腦使用下方指定的網路連線類型」。
16. 在底部清單方塊中，選取「乙太網路」，然後按下「確定」。
17. 按下「確定」結束「管理位置」對話方塊。

針對透過無線連線登入的用戶端設定辦公室位置

1. 在「用戶端」頁面上，選取要新增位置的群組。
2. 在「工作」下方，按下「新增位置」。
3. 在「新增位置精靈」中，按「下一步」。
4. 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「下一步」。
5. 在清單方塊中，按下「用戶端可以連線到管理伺服器」，然後按「下一步」。
6. 按下「完成」。
7. 按下「確定」。
8. 在「工作」下方，按下「管理位置」，然後選取已建立的位置。
9. 在「切換至這個位置的狀況」旁按下「新增」，然後按下「含 **AND** 關係的準則」。
10. 在「指定位置條件」對話方塊的「類型」清單中，按下「網路連線類型」。
11. 按下「如果用戶端電腦不使用下方指定的網路連線類型」。
12. 在底部清單方塊中，選取您組織使用的 VPN 用戶端名稱，然後按下「確定」。
13. 按下「新增」，再按下「含 **AND** 關係的準則」。
14. 在「指定位置條件」對話方塊的「類型」清單中，按下「網路連線類型」。
15. 按下「如果用戶端電腦不使用下方指定的網路連線類型」。
16. 在底部清單方塊中，按下「乙太網路」，然後按下「確定」。
17. 按下「新增」，再按下「含 **AND** 關係的準則」。
18. 在「指定位置條件」對話方塊的「類型」清單中，按下「網路連線類型」。
19. 按下「如果用戶端電腦使用下方指定的網路連線類型」。
20. 在底部清單方塊中，按下「無線」，然後按下「確定」。

21. 按下「確定」結束「管理位置」對話方塊。

更多資訊

- [設定第一種狀況的位置偵測條件](#)
- [管理遠端用戶端](#)

架構位置的通訊設定

預設情況下，您可以在群組層級架構管理伺服器與用戶端之間的通訊設定。但是，您也可以為群組中的各個位置架構這些設定。例如，對於用戶端電腦透過 VPN 進行連線的位置，您可以使用個別的管理伺服器。若要將同時連線至管理伺服器的用戶端數目降至最低，您可以針對各個位置指定不同的活動訊號。

您可以針對位置架構下列通訊設定：

- 用戶端執行所用的控制模式。
- 用戶端使用的管理伺服器清單。
- 用戶端執行所用的下載模式。
- 是否要收集在用戶端上執行的全部應用程式的清單，並將此清單傳送到管理伺服器。
- 用戶端進行下載的活動訊號間隔時間。
- 管理伺服器是否會隨機從預設管理伺服器或群組更新提供者下載內容。

NOTE

這些設定中只有一部分可以針對 Mac 用戶端進行架構。

架構位置的通訊設定

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」頁面上，選取群組。
3. 在「政策」標籤的「位置限定的政策與設定」下，展開某位置下方的「位置限定的設定」。
4. 在「通訊設定」右邊，按下「工作」，然後取消勾選「使用群組通訊設定」。
5. 再按一下「工作」，然後按一下「編輯設定」。
6. 在「位置名稱 的通訊設定」對話方塊中，僅修改指定位置的設定。
7. 按下「確定」。

更多資訊

- [使用推送模式或提取模式更新用戶端上的政策和內容](#)
- [管理遠端用戶端的位置](#)
- [管理用戶端群組](#)

關於加強遠端用戶端的安全性政策

當您管理遠端使用者時，基本上會採取下列其中一種方式：

- 保留預設政策，以免妨礙遠端使用者使用電腦。
- 加強預設安全性政策，以進一步保護網路，即使這會限制遠端使用者可執行的動作。

在大多數情況下，最佳實務是加強遠端用戶端的安全性政策。

您可以建立共用或非共用政策，然後將政策指派給群組或位置。共用政策是套用到任何群組和位置的政策，而且可以繼承。非共用政策則是套用到群組中特定位置的政策。一般來說，最佳實務是建立共用政策，因為這可以方便變更多個群組和位置的政策。但是，當您需要建立特定位置專屬的政策，就需要建立非共用政策，或將政策轉換為非共用政策。

更多資訊

針對遠端用戶端之防火牆政策設定的最佳實務準則

下表描述一些情景和最佳實務建議。

Table 137: 防火牆政策最佳實務

範例	建議
使用者不使用 VPN 進行登入的遠端位置	- 將最嚴格的安全政策指派給不使用 VPN 進行遠端登入的用戶端。 - 啟用 NetBIOS 防護。 Note: 對於遠端用戶端透過 VPN 登入公司網路的位置，請勿啟用 NetBIOS 防護。此規則僅適用於遠端使用者連線到網際網路的狀況，不適用於連線到公司網路的狀況。 - 為提升安全性，攔截 NetBIOS 通訊埠 135、139 及 445 上的所有本機 TCP 流量。
使用者透過 VPN 登入的遠端位置	- 維持各項攔截所有配接卡上流量的規則。請勿變更這些規則。 - 維持各項允許所有配接卡上 VPN 流量的規則。請勿變更此規則。 - 對於各項使用「允許」動作的規則，請將「配接卡」欄的「全部配接卡」變更為您使用的 VPN 配接卡名稱。 - 啟用攔截其他所有流量的規則。 Note: 如果要避免透過 VPN 分割通道，您需要進行所有上述變更。
使用者透過乙太網路或無線連線登入的辦公室位置	使用您的預設防火牆政策。對於無線連線，請確定已啟用允許無線 EAPOL 的規則。802.1x 會使用 LAN 延伸驗證通訊協定 (EAPOL) 進行連線驗證。

更多資訊

- [建立防火牆政策](#)
- [為網路服務啟用通訊而非新增規則](#)

關於開啟遠端用戶端的通知

對於未透過 VPN 登入的遠端用戶端，最好在下列狀況開啟用戶端通知：

- 入侵偵測
您可以使用特定位置的伺服器開啟這些通知，也可以在「用戶端使用者介面控制設定」中選取「混合控制」。您可以在「用戶端使用者介面設定」標籤上自訂此設定。
- 病毒和安全風險
您可以在「病毒和間諜軟體防護」政策開啟這些通知。

當您開啟這些通知，出現安全性問題時，會通知遠端使用者。

更多資訊

關於從管理伺服器監控遠端用戶端

通知和日誌是維護安全環境所不可或缺的。一般來說，監控遠端用戶端的方式應與監控其他用戶端的方式相同。您應隨時檢查防護是否為最新，而且網路目前未受到攻擊。如果網路遭受攻擊，那麼需要找出是誰發出攻擊以及攻擊的方式。

首頁的喜好設定會決定 Symantec Endpoint Protection Manager 顯示資料的期間。根據預設，首頁上的資料僅表示過去 12 小時內連線的用戶端。如果有許多用戶端經常離線，最佳的監控方式是查看日誌和報告。在日誌和報告中，您可以過濾資料，只包含離線用戶端。

即使您限制了行動用戶端可以上傳的部分用戶端日誌資料，還是可以檢查下列顯示畫面。

Table 138: 監控遠端用戶端安全性的顯示畫面

顯示	說明
首頁 > 端點狀態	顯示內容是否最新，或檢視是否有任何防護已關閉。 您可以檢查下列狀態條件： - 內容日期和版本號碼 - 用戶端連線 - 已啟用和已停用的防護 您可以按下「詳細資料」，檢視各用戶端的狀態。
首頁 > 安全性狀態	顯示系統安全性概觀。檢視「病毒和風險活動摘要」，查看網路是否受到攻擊。 您可以按下「詳細資料」，檢視各安全防護技術的狀態。
首頁 > 病毒和風險活動摘要	顯示偵測到的病毒和風險活動，以及採取的動作，如已清除、已攔截或已隔離。
「監視器」>「摘要類型」>「網路威脅防護」	顯示攻擊類型和來源的相關資訊。

更多資訊

- [管理遠端用戶端](#)
- [從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端](#)

管理管理員帳戶和密碼

您可以使用管理員帳戶管理 Symantec Endpoint Protection Manager 資料中心。管理員可登入 Symantec Endpoint Protection Manager 來變更政策設定、管理群組、執行報告、安裝用戶端軟體以及執行其他管理工作。

預設帳戶是系統管理員帳戶，可供存取所有功能。您也可以針對需要執行一部分工作的管理員，新增有較多限制的管理員帳戶。

針對小公司，您可能只需要一個管理員和一個網域。如果大公司擁有多個站台和 Windows 網域，則很可能需要多個管理員，某些管理員比其他人擁有更多的存取權。您可能也需要在 Symantec Endpoint Protection Manager 中新增多個網域。

您可以在「管理員」頁面上管理網域和管理員帳戶及其密碼。

Table 139: 帳戶管理

工作	說明
決定是否新增多個網域	決定是否新增網域。請參閱： 關於網域 新增網域 切換至目前的網域
新增管理員帳戶	針對需要存取 Symantec Endpoint Protection Manager 主控台的管理員新增帳戶。 - 新增所需的帳戶類型和存取權限層級。請參閱： 關於管理員帳戶和存取權限 新增管理員帳戶和設定存取權限 - 選擇在管理員登入 Symantec Endpoint Protection Manager 時進行驗證的方法 (選擇性)。根據預設，Symantec Endpoint Protection Manager 資料庫會驗證管理員的憑證。請參閱：選擇管理員帳戶的驗證方法

工作	說明
解除鎖定或鎖定管理員帳戶	根據預設，在使用者嘗試使用管理員帳戶登入 Symantec Endpoint Protection Manager 太多次後，Symantec Endpoint Protection Manager 會鎖定管理員。您可以架構這些設定，增加鎖定管理員的嘗試次數或時間。如果管理員的帳戶遭到鎖定，則必須等待指定的時間，然後再次登入。鎖定時間間隔內，您無法解除鎖定帳戶。請參閱： 在嘗試太多次登入後解除鎖定管理員的帳戶
變更並重設遺失密碼	- 變更您的帳戶密碼或其他管理員的帳戶密碼。請參閱： 變更管理員帳戶或預設資料庫的密碼 - 使用出現在管理伺服器登入畫面上的「忘記了您的密碼？」連結重設遺失密碼。管理員會收到包含用於啟用暫時密碼的連結的電子郵件。請參閱： 重設忘記的 Symantec Endpoint Protection Manager 密碼 顯示「忘記了您的密碼？」連結，以便管理員可以重設遺失密碼 - 允許管理員在管理伺服器登入畫面上儲存他們的使用者名稱和密碼。請參閱： 在登入畫面上顯示「記住我的使用者名稱」核取方塊 - 強制管理員的登入密碼在一定天數後到期。請參閱： 在登入畫面上顯示「記住我的使用者名稱」核取方塊
為 Symantec Endpoint Protection Manager 架構登入選項	您可以為每種管理員類型架構下列登入選項： - 顯示管理員要在登入前閱讀的訊息。請參閱： 在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息 - 允許或攔截管理主控台的登入存取，以限制某些管理員是否能夠從遠端登入。請參閱： 授予或攔截對遠端 Symantec Endpoint Protection Manager 主控台的存取 - 變更管理員可保持登入管理伺服器的期限。請參閱： 變更保持登入 Symantec Endpoint Protection Manager 主控台的逾時期間 如需詳細資訊，請參閱： 登入 Symantec Endpoint Protection Manager 主控台

關於管理員帳戶和存取權限

安裝 Symantec Endpoint Protection Manager 時，會建立一個名為 `admin` 的預設系統管理員帳戶。該系統管理員帳戶可讓管理員存取 Symantec Endpoint Protection Manager 中的所有功能。

您可以新增其他系統管理員帳戶、網域管理員帳戶與限制的管理員帳戶，協助您管理安全性。網域管理員與限制的管理員可存取 Symantec Endpoint Protection Manager 的部分功能。

您可根據公司需要的角色類型與存取權選擇所需的帳戶。例如，大公司可能會使用下列角色類型：

- 安裝管理伺服器 and 用戶端安裝套件的管理員。安裝產品後，負責接管作業的管理員。這些管理員很可能是系統管理員。
- 作業管理員，維護伺服器、資料庫，和安裝修正程式。如果您具有單一網域，作業管理員可以是獲得完全授權來管理站台的網域管理員。
- 防毒管理員，在用戶端上建立和管理「病毒和間諜軟體防護」政策和 LiveUpdate 政策。此管理員很可能是限制的管理員。
- 桌面管理員，負責用戶端安全和為用戶端建立、維護「防火牆」政策和「入侵預防」政策。此管理員很可能是網域管理員。
- 服務台管理員，建立報告，和擁有政策唯讀存取權。防毒管理員和桌面管理員會讀取服務台管理員傳送的報告。服務台管理員很可能是獲得報告權限和政策權限的限制的管理員。

Table 140: 管理員角色和責任

管理員角色	責任
系統管理員	系統管理員可以登入 Symantec Endpoint Protection Manager 主控台，且擁有對所有功能與工作的完整不受限制的存取權。 系統管理員可以建立並管理其他系統管理員帳戶、網域管理員帳戶與限制的管理員帳戶。 系統管理員可以執行下列工作： • 管理所有網域。 • 管理授權。 • 檢視和管理所有主控台設定。 • 管理資料庫和管理伺服器。
管理員	管理員是可檢視並管理單一網域的網域管理員。網域管理員具有與系統管理員一樣的權限，但僅限單一網域。依預設，網域管理員具有管理網域 (而非站台) 的完整系統管理員權限。您必須明確地授予單一網域內的站台權限。雖然網域管理員無法修改自己的站台權限，但可以修改其他管理員與限制的管理員的站台權限。 網域管理員可以執行下列工作： • 建立和管理單一網域內的管理員帳戶和限制的管理員帳戶。 網域管理員無法修改自己的站台權限。此功能必須由系統管理員執行。 • 執行報告、管理站台及重設密碼。 • 無法管理授權。只有系統管理員可以管理授權。 如需詳細資訊，請參閱： 關於網域
限制的管理員	限制的管理員可以有限的存取權登入 Symantec Endpoint Protection Manager 主控台。根據預設，限制的管理員沒有存取權。系統管理員角色必須明確地授予可讓限制的管理員執行工作的存取權。 當您限制存取權限時，部分管理伺服器使用者介面無法供限制的管理員使用。例如： • 不具報告權限的限制管理員無法檢視「首頁」、「監視器」或「報告」頁面。 • 不具政策權限的限制管理員無法檢視或修改政策。此外，他們也不能套用、取代或撤銷政策。

更多資訊

- [新增管理員帳戶和設定存取權限](#)
- [管理管理員帳戶](#)

新增管理員帳戶和設定存取權限

系統管理員可以新增其他系統管理員、管理員或限制的管理員。網域內的管理員可以新增存取權限與自己相當或較不受限制的其他管理員。管理員可以新增限制的管理員並架構其存取權限。

新增管理員帳戶

1. 在主控台中，按下「管理員」>「管理員」。
2. 在「工作」下，按下「新增管理員」。
3. 在「新增管理員」對話方塊的「一般」標籤中，輸入使用者名稱和電子郵件地址。
4. 在「存取權限」標籤上，指定管理員帳戶的類型。

如果您新增限制的管理員帳戶，也必須指定管理員的存取權限。未被授予任何存取權限的限制管理員帳戶是在停用狀態下建立的，且限制的管理員無法登入管理伺服器。請參閱：

[關於管理員帳戶和存取權限](#)

5. 在「驗證」標籤的「**Symantec Endpoint Protection Manager 驗證**」下，輸入管理員用來登入的密碼。

當管理員登入 Symantec Endpoint Protection Manager 時，Symantec Endpoint Protection Manager 會使用資料庫驗證使用者名稱與密碼是否正確。請參閱：

選擇管理員帳戶的驗證方法

6. 按下「確定」。

選擇管理員帳戶的驗證方法

您可以從管理伺服器在登入前，用來檢查管理員憑證的多個驗證方法中進行選擇。

若為第三方驗證方法，Symantec Endpoint Protection Manager 在資料庫中會有管理員帳戶的相關項目，但由第三方伺服器來驗證使用者名稱與密碼。

Table 141: 驗證方法

類型	使用時機
Symantec Endpoint Protection Manager 驗證 (預設)	透過儲存在 Symantec Endpoint Protection Manager 資料庫中的管理員使用者名稱和密碼，來驗證管理員。當管理員登入管理伺服器時，管理伺服器會使用資料庫驗證使用者名稱與密碼是否正確。您可以顯示「密碼永久有效」選項，這樣一來管理員的帳戶將不會過期。請參閱： 使 Symantec Endpoint Protection Manager 登入密碼永久有效
雙因素驗證	使用智慧型手機上的 Symantec VIP 驗證來驗證管理員。管理員在登入時除了提供密碼，還必須提供一次性的唯一驗證碼。為了讓此選項可供使用，您必須先新增適當的 PKCS 金鑰儲存區檔案和金鑰儲存區的密碼。請參閱： 使用 Symantec VIP 架構雙因素驗證
RSA SecurID 驗證	使用 RSA SecurID Token (而非軟體 RSA Token)、RSA SecurID 卡或 RSA 鍵台卡 (而非 RSA 智慧卡)，驗證管理員。若要驗證使用 RSA SecurID 機制的管理員，請先安裝 RSA Authentication Manager 伺服器，並啟用 RSA SecurID 加密驗證。請參閱： 搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID 驗證
目錄伺服器驗證	使用 LDAP 伺服器或 Microsoft Active Directory 伺服器驗證管理員。若要使用 Active Directory 或 LDAP 目錄伺服器驗證管理員，您需要在目錄伺服器上設定帳戶。您還必須建立目錄伺服器與 Symantec Endpoint Protection Manager 之間的連線。如果您沒有建立連線，便無法從 Active Directory 伺服器匯入使用者，也無法與它們進行同步處理。 Note: 同步處理僅適用於 Active Directory 伺服器。不支援與 LDAP 伺服器進行同步處理。 如需詳細資訊，請參閱： • 將 Symantec Endpoint Protection Manager 連線至目錄伺服器 • 檢查目錄伺服器驗證
智慧卡驗證	驗證在美國聯邦機構以平民或軍事人員身分工作且必須使用 PIV 卡或 CAC 登入的管理員。請參閱： 架構 Symantec Endpoint Protection Manager 以驗證使用智慧卡登入的管理員

選擇管理員帳戶的驗證方法

1. 新增管理員帳戶。請參閱：

[新增管理員帳戶和設定存取權限](#)

2. 在「驗證」標籤上，如果您不想使用「Symantec Endpoint Protection Manager 驗證」(預設)，則選取驗證方法。

3. 按下「確定」。

4. 在「確認變更」對話方塊中，輸入您用來登入 Symantec Endpoint Protection Manager 的密碼，然後按下「確定」。

在切換驗證方法時，必須輸入管理員帳戶的密碼。

搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID 驗證

NOTE

在 IPv6 環境中，您必須在 Symantec Endpoint Protection Manager 伺服器上安裝並啟用 IPv4 堆疊以使用 RSA SecurID 驗證。

(自 14.2 版起支援 IPv6 網路。)

架構 RSA SecurID 驗證 Symantec Endpoint Protection Manager 管理員

如果您要使用 RSA SecurID 驗證使用 Symantec Endpoint Protection Manager 的管理員，必須先架構與 RSA Authentication Manager 伺服器的連線來啟用加密的驗證。

架構 RSA SecurID 驗證 Symantec Endpoint Protection Manager 管理員

1. 必要時，安裝 RSA Authentication Manager 伺服器。使用 RSA Authentication Manager 8.1。
2. 在 Symantec Endpoint Protection Manager 伺服器上安裝並正確架構 RSA Authentication Agent 以連接到 RSA 伺服器。使用 RSA Authentication Agent 7.x。
3. 確認 Symantec Endpoint Protection Manager 伺服器註冊為 RSA Authentication Manager 伺服器上的有效主機。
4. 確定可以在網路上存取 RSA Authentication Manager 伺服器上的 `sdconf.rec` 檔案。
5. 將同步化的 SecurID 卡或密鑰卡指派給管理伺服器帳戶；在 RSA Authentication Manager 伺服器上啟用登入名稱。
6. 確保管理員有可使用的 RSA PIN 或密碼。
賽門鐵克支援下列的 RSA 登入類型：
 - RSA SecurID Token (非軟體 RSA Token)
 - RSA SecurID 卡
 - RSA 鍵台卡 (非 RSA 智慧卡)若要以 RSA SecurID 登入管理伺服器，管理員需有登入名稱、Token (硬體) 和 PIN。

安裝 RSA Authentication Agent 並將 Symantec Endpoint Protection Manager 伺服器架構為使用 RSA SecurID 驗證

若要搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID，您必須在 Symantec Endpoint Protection Manager 伺服器上安裝 RSA Authentication Agent，並將其架構為 SecurID 驗證用戶端。

安裝 RSA Authentication Agent

1. 在 Symantec Endpoint Protection Manager 伺服器上安裝 RSA Authentication Agent 的軟體。您可以從 RSA Authentication Agent 安裝檔案執行 Windows .msi 檔案來安裝軟體。
2. 將 `sdconf.rec` 檔案從 RSA Authentication 伺服器複製到 Symantec Endpoint Protection Manager 伺服器。
若為舊版 RSA Authentication Agent，請複製 `nodesecret.rec`、`sdconf.rec` 和 `agent_nsload.exe`。

架構 Symantec Endpoint Protection Manager 伺服器使用 RSA SecurID 驗證

1. 登入 Symantec Endpoint Protection Manager 主控台，然後按下「管理員 > 伺服器」。
2. 在「伺服器」下方的「本機網站」下，按下管理伺服器。
3. 在「工作」下方，按下「架構 SecurID 驗證」。
4. 在「歡迎使用架構 SecurID 驗證精靈」畫面中，按「下一步」。
5. 在「架構 SecurID 驗證精靈」的「資格」畫面中，閱讀先決條件，並確認符合所有要求。
6. 按「下一步」。
7. 在「架構 SecurID 驗證精靈」的「上傳 RSA 檔案」畫面中，瀏覽尋找 `sdconf.rec` 檔案所在的資料夾。
您也可以鍵入路徑名稱。
8. 按「下一步」，然後按下「測試」來測試您的架構。
9. 在「測試架構」對話方塊中，鍵入 SecurID 的使用者名稱和密碼，然後按下「測試」。
現在已成功驗證。

新增使用 RSA SecurID 驗證的 Symantec Endpoint Protection Manager 管理員

在您完成先前的程序之後，可以新增 Symantec Endpoint Protection Manager 管理員。

新增使用 RSA SecurID 驗證的 Symantec Endpoint Protection Manager 管理員

1. 新增管理員帳戶。請參閱：
[新增管理員帳戶和設定存取權限](#)
2. 在「驗證」標籤上，按下「RSA SecurID 驗證」。
如果無法使用此選項，請參閱架構準則。請參閱：
[架構 RSA SecurID 驗證 Symantec Endpoint Protection Manager 管理員](#)
3. 按下「確定」。
您也可以將現有管理員帳戶變更為使用 RSA SecurID 驗證，不過並不建議採取這種做法，尤其是預設管理員帳戶 admin。如果您在編輯現有使用者時提供了無效的資訊，則會較難復原該使用者。
不過，如果要修改現有管理員帳戶，請在「確認變更」對話方塊中，輸入您用來登入 Symantec Endpoint Protection Manager 的密碼，然後按下「確定」。
在切換驗證方法時，必須輸入管理員帳戶的密碼。請參閱：
[選擇管理員帳戶的驗證方法](#)

使用 Symantec VIP 架構雙因素驗證

如果您的環境中使用 Symantec VIP 雙因素驗證，您可以將 Symantec Endpoint Protection Manager 管理員架構為向其進行驗證。

雙因素驗證可為登入程序的安全增添多一層保護。如果啟用雙因素驗證，您在登入時除了提供密碼，還必須提供唯一的一次性驗證碼。您可以透過語音、文字或使用免費的 Symantec VIP Access 應用程式收到此驗證碼。建議您使用此應用程式，因為它最安全且方便易用。如需 Symantec VIP 的快速總覽，請參閱：

[Symantec VIP：讓所有人輕鬆進行企業級驗證](#)

您可以針對使用 Symantec Endpoint Protection Manager 驗證的每一個個別管理員管理個別的雙因素驗證設定。使用 RSA SecurID 或目錄驗證進行驗證的管理員無法使用雙因素驗證。

NOTE

透過 IPv6 或在啟用 FIPS 的環境中，不支援雙因素驗證。

架構 Symantec Endpoint Protection Manager 以使用 Symantec VIP 進行雙因素驗證

1. 在主控台中，按一下「管理員 > 伺服器」，然後按一下本機伺服器名稱。
2. 在「工作」下方，按一下「架構 VIP 驗證」。
3. 瀏覽至 PKCS 金鑰儲存區檔案加以選取，並輸入金鑰儲存區的密碼，然後按一下「確定」。
憑證會自動傳播至同一網站中的其他 Symantec Endpoint Protection Manager 主控台，而不需要遠端複製。您不需要手動將憑證新增到網站上的每個 Symantec Endpoint Protection Manager。
若要將憑證傳播至其他網站上的 Symantec Endpoint Protection Manager，這些網站必須是遠端複製夥伴。

架構管理員以使用 Symantec VIP 進行雙因素驗證

1. 請確認 Symantec Endpoint Protection Manager 管理員在 Symantec VIP Manager 上具有包括大小寫在內，完全相符的對應使用者名稱。這兩個使用者名稱的密碼不一定要相符。
請參閱 Symantec VIP Manager 說明文件，以瞭解如何架構使用者名稱。請參閱：
[Symantec VIP Access Manager 3.0 管理指南](#)
2. 在主控台中，按下「管理員」>「伺服器」>「管理員」。
3. 選取現有的管理員，然後按一下「編輯管理員」。
您也可以新增管理員以進行架構。

4. 在「驗證」標籤上，按一下「使用 **VIP** 啟用雙因素驗證」。

使用智慧卡架構驗證

在版本 14.2 或更新版本，在美國聯邦機構工作的管理員可以使用智慧卡登入 Symantec Endpoint Protection Manager (SEPM)。

若要設定智慧卡驗證，管理員必須執行下列步驟：

- [步驟1：將根憑證和中間憑證匯入至 Symantec Endpoint Protection Manager](#)
- [步驟2：匯入憑證撤銷清單 \(CRL\) \(暗網必需\)](#)
- [步驟3：新增管理員帳戶並註冊智慧卡](#)
- [步驟4：使用智慧卡登入 Symantec Endpoint Protection Manager](#)

關於智慧卡

美國聯邦機構需要使用智慧卡驗證來符合 [Homeland Security Presidential Directive 12](#) 需求。美國聯邦智慧卡包含將聯邦機構和資訊系統存取權授予持卡人的必要資料。此存取權可確保所有適用的聯邦應用程式享有適當的安全層級。

讀卡機通常內建在鍵盤和筆記型電腦中，但是也支援外部 USB 讀取器。請與製造商聯繫，以取得任何適用的驅動程式需求。

Symantec Endpoint Protection Manager 會驗證使用下列類型智慧卡的管理員：

- 個人身分驗證 (PIV) 卡，例如 IDEMIA 和 Gemalto (適用於平民)
- 通用存取卡 (CAC) (適用於軍事人員)

Symantec Endpoint Protection Manager 不支援 FIPS 模式中的智慧卡或使用 RSASSA-PSS 簽署的智慧卡。Symantec 會針對 NIST 提供的智慧卡範例套件測試每個版本。

步驟1：將根憑證和中間憑證匯入至 Symantec Endpoint Protection Manager

您必須匯入根憑證及/或要用於信任根的中間憑證。此步驟建立用於驗證智慧卡登入的根憑證。您可以匯入多個根憑證和中間憑證。

所有根檔案和中間檔案都必須存在於 Symantec Endpoint Protection Manager 電腦上，並且中間憑證應與根憑證位於同一鏈中。否則，管理員無法登入。

將根憑證和中間憑證匯入至 Symantec Endpoint Protection Manager

1. 在主控台中，按一下「管理員 > 伺服器」，然後選取本機管理伺服器名稱。
2. 在「工作」下方，按一下「架構智慧卡驗證」。
3. 在「指定根憑證及 (或) 中間憑證檔案的路徑」文字方塊中，瀏覽至一或多個憑證檔案，然後按一下「確定」。
選取您需要建立信任的所有憑證檔案。若要選取多個檔案，請按下 **Ctrl**。
4. 按下「確定」。
5. 重新啟動 Symantec Endpoint Protection Manager 服務。請參閱：
[停止及啟動管理伺服器服務](#)

步驟2：匯入憑證撤銷清單 (CRL)，並執行撤銷檢查 (選用；暗網必需)

如果管理伺服器沒有 Internet 存取權，您必須將其架構為改成檢查管理伺服器電腦上的 CRL 檔案。如果未執行此檢查，管理員仍可登入，但管理伺服器無法檢查 CRL 檔案，可能會導致安全問題。

將憑證撤銷清單 (CRL) 匯入至管理伺服器

1. 在主控台中，按一下「管理員 > 伺服器」，然後選取本機管理伺服器名稱。
2. 在「工作」下方，按一下「架構智慧卡驗證」。
3. 在「指定憑證撤銷清單的路徑」文字方塊中，瀏覽至一個或多個 .crl 或 .pem 檔案，然後按一下「確定」。

選取需要檢查是否撤銷的所有憑證檔案。若要選取多個檔案，請按下 **Ctrl**。

4. 按下「確定」。

略過憑證驗證

由於在暗網中登入的管理員無法存取網路，因此您必須允許這些管理員無論使用哪種憑證都可以連線。若要允許連線，請略過憑證驗證。

1. 在管理伺服器上，開啟下列檔案：<Symantec Endpoint Protection Manager installation path>\tomcat\etc\conf.properties
2. 在 conf.properties 檔案中，新增 smartcard.cert.revocation.ocsp.crl.dp.enabled=false 並儲存檔案。
3. 重新啟動管理伺服器服務。請參閱：
[停止及啟動管理伺服器服務](#)

步驟 3：新增管理員帳戶並註冊智慧卡

此步驟會匯入管理員憑證，而此憑證會與 SEPM 登入上的智慧卡進行比對。

- 智慧卡驗證需要用來驗證 PIV 認證的憑證和金鑰組：
 - 是由授權實體發出的。
 - 尚未過期。
 - 尚未撤銷且與您在步驟 1 中匯入的憑證位於同一鏈中。
- PIV 憑證還會識別管理員就是核發憑證的同一人。

此步驟也會確保管理員必須輸入使用者名稱、插入卡，然後輸入智慧卡 PIN 來登入 Symantec Endpoint Protection Manager。管理員不需要輸入 Symantec Endpoint Protection Manager 密碼。

不支援透過 IPv6 進行智慧卡驗證。

NOTE

對於使用智慧卡登入 Symantec Endpoint Protection Manager 的每個管理員，請遵循此步驟。

新增管理員帳戶並註冊智慧卡

1. 在主控台中，按下「管理員」>「伺服器」>「管理員」。
2. 新增管理員，或編輯現有管理員。請參閱：
[新增管理員帳戶和設定存取權限](#)
3. 在「驗證」標籤上，按一下「啟用智慧卡驗證」。
4. 瀏覽至該管理員的 PIV 卡或 CAC 的驗證憑證檔案，然後按一下「確定」。
5. 在「確認變更」對話方塊中，輸入管理員密碼，然後按一下「確定」。

步驟 4：使用智慧卡登入 Symantec Endpoint Protection Manager

Java 主控台和 Web 主控台支援智慧卡驗證。RMM 主控台和 REST API 不支援智慧卡驗證。

在您登入之前，請將卡插入至智慧卡讀卡機。在您登入之前或登入之後輸入 PIN，取決於您使用的主控台。

當智慧卡管理員登入和使用管理伺服器時，必須始終將智慧卡插入讀取裝置。

NOTE

如果您在虛擬機器上執行 SEPM，Symantec 建議使用 Windows 遠端桌面。如果您使用 VMware ESXI，請使用 VMware 遠端主控台。

登入 Symantec Endpoint Protection Manager Java 主控台

若要使用 Gemalto IDPrime 智慧卡登入 Java 主控台，您必須安裝 Thales SafeNet 驅動程式。

1. 登入 Symantec Endpoint Protection Manager Java 主控台。請參閱：
[登入 Symantec Endpoint Protection Manager 主控台](#)
2. 在 Symantec Endpoint Protection Manager 登入畫面出現之後，按一下「選項 >>」、勾選「使用智慧卡登入」、輸入您的使用者名稱，然後按一下「登入」。
3. 輸入智慧卡 PIN 號碼，然後按一下「確定」。



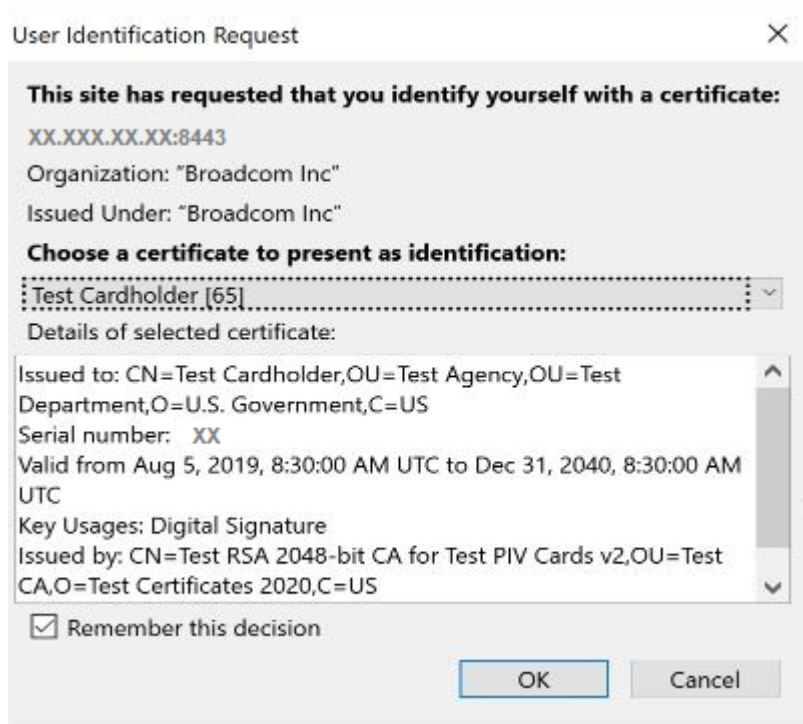
Symantec Endpoint Protection Manager 主控台即會出現。

若要登入 **Symantec Endpoint Protection Manager Web** 主控台

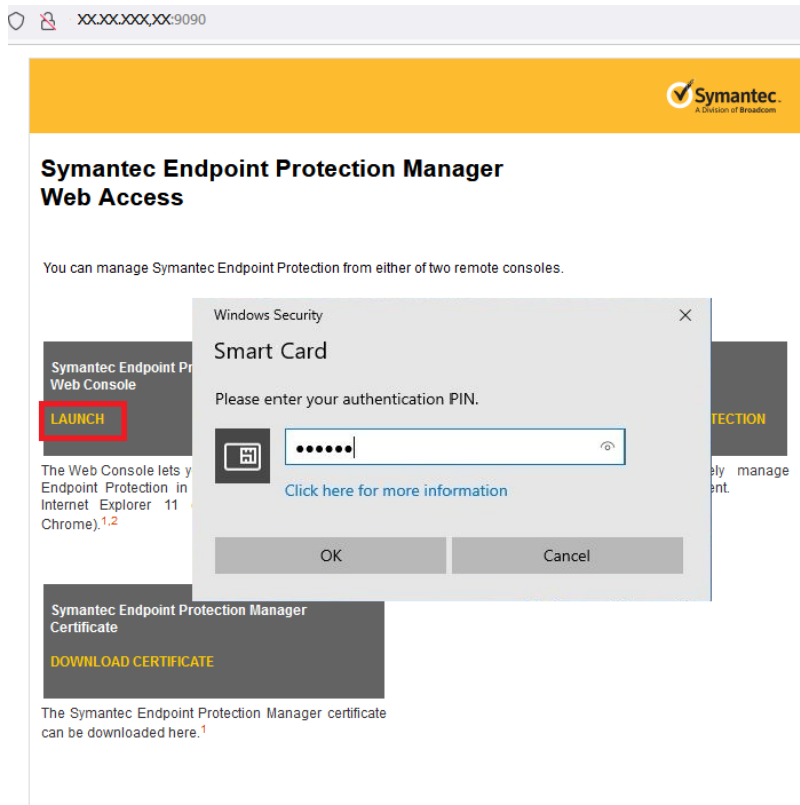
Symantec 建議下列最佳實務：

- 若要使用 Web 主控台，您可能需要安裝適用於組織使用的智慧卡製造商的驅動程式。
 - 確定中間憑證或分葉憑證未過期。當瀏覽器提示您在此工作中選取憑證時，過期的憑證不會出現在清單中。SEPM Web 主控台不會出現，因此您無法登入。
 - 大部分現式瀏覽器支援智慧卡登入。
 - 基於安全原因，在管理員從讀卡機中取出智慧卡之後，管理員應立即登出 Web 主控台。
1. 開啟支援的網頁瀏覽器，然後在位址方塊中輸入下列位址：
`http://<SEPMServer>:9090/`
其中 <SEPMServer> 是管理伺服器的主機名稱或 IP 位址。
 2. 在 **Symantec Endpoint Protection Manager Web** 主控台下，按一下「啟動」。

如果在您登入主控台之後出現下列其中一則彈出式訊息，請確保您選取了正確的智慧卡憑證 (分葉憑證) 來信任。否則，Web 主控台不會出現。
每種類型的 Web 瀏覽器都會顯示不同的彈出式訊息。



3. 在「**Windows 安全智慧卡**」登入畫面中，輸入您的 PIN 號碼，然後按一下「確定」。



4. 在 **Symantec Endpoint Protection Manager** 登入畫面中，按一下「選項 >>」、勾選「使用智慧卡登入」、輸入您的使用者名稱，然後按一下「登入」。
- 網域管理員必須在登入時新增特定網域，即使其為預設網域也一樣。

您可能會看到：

- 另一則選取正確中間憑證的訊息。選取以前選取的相同憑證。
 - 智慧卡登入畫面可能再次出現。輸入 PIN 號碼。
- Symantec Endpoint Protection Manager 主控台即會出現。

針對多部管理伺服器和多個站台使用智慧卡

如果您有多部管理伺服器或在您的環境中執行複寫，請架構一次智慧卡驗證。智慧卡的複寫遵循與政策相同的程序。

在單一站台內的多部管理伺服器之間共用憑證

1. 在站台中的一部管理伺服器上架構智慧卡驗證。
等待 5 分鐘，直到共用資料庫的其他管理伺服器更新為止。
2. 重新啟動所有管理伺服器。

跨多個站台在多部管理伺服器之間共用憑證

1. 在一個站台中的一部管理伺服器上架構智慧卡驗證。
2. 在所有站台之間複寫資料。
等待 5 分鐘，直到來自遠端站台的其他管理伺服器更新為止。
3. 重新啟動所有站台上的所有管理伺服器。

確認每部管理伺服器已成功複寫憑證

1. 前往「監視器 > 日誌」。
2. 在「日誌類型」下拉式清單中，選取「系統 > 伺服器活動」，然後按一下「檢視日誌」。
3. 在「事件類型」欄中，尋找「遠端檔案下載成功」。

還原智慧卡架構

如果您錯誤地架構了智慧卡驗證，則可以將目前智慧卡架構重設回預設行為。

還原預設智慧卡架構

1. 停止 Symantec Endpoint Protection Manager 服務。
2. 開啟下列檔案：<SEPM installation directory>\apache\conf\ssl\smartCard.pem 和 <SEPM installation directory>\apache\conf\ssl\CRL.pem
3. 移除這些檔案中第一個項目以外的所有憑證項目，然後儲存檔案。
4. 重新啟動 Symantec Endpoint Protection Manager 服務。
SEPM 應該回到其預設狀態，即不新增任何中間或根憑證，也不架構任何 CRL。

測試管理員帳戶的目錄伺服器驗證

您可以檢查 Active Directory 或 LDAP 伺服器是否驗證您所建立的管理員帳戶的使用者名稱和密碼。此次檢查會評估您新增的使用者名稱和密碼是否正確，以及目錄伺服器上是否存在此帳戶名稱。

您在 Symantec Endpoint Protection Manager 中會與您在目錄伺服器中一樣，為管理員帳戶使用相同的使用者名稱和密碼。當管理員登入管理伺服器時，目錄伺服器會驗證管理員的使用者名稱和密碼。管理伺服器會使用您所新增的目錄伺服器組態，搜尋目錄伺服器上的帳戶。

您也可以檢查 Active Directory 或 LDAP 伺服器是否會驗證沒有使用者名稱和密碼的管理員帳戶。沒有使用者名稱或密碼的帳戶是匿名存取。您應該使用匿名存取建立一個管理員帳戶，讓管理員永遠不會因為目錄伺服器上的密碼變更而遭到鎖定。

NOTE

在 Windows 2003 Active Directory 伺服器中，預設會停用匿名驗證。因此，如果您將沒有使用者名稱的目錄伺服器新增至管理員帳戶，然後按下「檢查帳戶」，就會顯示「帳戶驗證失敗」錯誤訊息。若要解決這個問題，請建

立兩個目錄伺服器項目，一個用於測試，另一個用於匿名存取。管理員仍然可以使用有效的使用者名稱和密碼登入管理伺服器。

步驟 1：新增多個目錄伺服器連線

若要讓測試更容易進行匿名存取，請至少新增兩個目錄伺服器項目。使用其中一個項目測試驗證，另一個項目測試匿名存取。這些項目全部都使用具有不同組態的相同目錄伺服器。

根據預設，除非移到不同的組織單位，否則多數使用者位於 CN=Users。LDAP 目錄伺服器中的使用者是以 CN=Users、DC=<sampldomain>、DC=local 所建立。若要找出使用者在 LDAP 中的位置，請使用 ADSIEdit。

使用下列資訊設定此範例的目錄伺服器：

- CN=John Smith
- OU=test
- DC=<sampldomain>
- DC=local

此範例會使用預設的 Active Directory LDAP (389)，但也可以使用安全 LDAP (636)。

新增多個目錄伺服器連線

1. 若要新增目錄伺服器連線以檢查 Active Directory 和 LDAP 伺服器身分驗證，請在主控台上按一下「管理員」>「伺服器」，選取預設伺服器，然後按一下「編輯伺服器屬性」。
2. 在「目錄伺服器」標籤上，按下「新增」。
3. 在「一般」標籤上，新增下列目錄伺服器組態，然後按下「確定」。

目錄 1	• 名稱：<sampldomain> Active Directory • 伺服器類型：Active Directory • 伺服器 IP 位址或名稱：server01.<sampldomain>.local • 使用者名稱：<sampldomain>\administrator • 密碼：<directory server password>
目錄 2	• 名稱：<sampldomain> LDAP with User Name • 伺服器類型：LDAP • 伺服器 IP 位址或名稱：server01.<sampldomain>.local • LDAP 通訊埠：389 • LDAP BaseDN：DC=<sampldomain>, DC=local • 使用者名稱：<sampldomain>\administrator • 密碼：<directory server password>
目錄 3	• 名稱：<sampldomain> LDAP without User Name • 伺服器類型：LDAP • 伺服器 IP 位址或名稱：server01.<sampldomain>.local • LDAP 通訊埠：389 • LDAP BaseDN：<empty> 當您使用匿名存取時，請將此欄位留空。 • 使用者名稱：<empty> • 密碼：<empty> 按下「確定」之後，會出現一個警告。但是目錄伺服器是有效的。 當您嘗試新增沒有使用者名稱和密碼的 BaseDN 時，會出現警告。

步驟 2：新增多個管理員帳戶

您要新增多個系統管理員帳戶。匿名存取的帳戶沒有使用者名稱或密碼。

新增多個管理員帳戶

- 若要使用目錄伺服器項目新增管理員帳戶，請按一下主控台上的「管理員」>「管理員」，並在「一般」標籤上新增先前步驟中的管理員帳戶。請參閱：
 - [新增管理員帳戶和設定存取權限](#)
 - [選擇管理員帳戶的驗證方法](#)
- 在您新增每個管理員帳戶並按下「檢查帳戶」選項之後，您會看到一則訊息。在某些情況下，這個訊息似乎會使帳戶資訊無效。但是，管理員仍然可以登入 Symantec Endpoint Protection Manager。
- 在「一般」標籤上，輸入下列資訊：

管理員 1	- 名稱：<sampldomain> LDAP without User Name - 伺服器類型：LDAP - 伺服器 IP 位址或名稱：server01.<sampldomain>.local LDAP 通訊埠：389 LDAP BaseDN：<empty> 當您使用匿名存取時，請將此欄位留空。 - 使用者名稱：<empty> - 密碼：<empty> 按下「確定」之後，會出現一個警告。但是目錄伺服器是有效的。 當您嘗試新增沒有使用者名稱和密碼的 BaseDN 時，會出現警告。
管理員 2	- 使用者名稱：john - 全名：John Smith - 電子郵件地址：john@<sampldomain>.local - 在「存取權」標籤上，按下「系統管理員」。 - 在「驗證」標籤上，按下「目錄驗證」。 - 在「目錄伺服器」下拉式清單中，選取 <sampldomain> LDAP with User Name。 - 在「帳戶名稱」欄位中，輸入 john。 - 按下「檢查帳戶」。 - 系統管理員 john 無法使用目錄驗證，登入 Symantec Endpoint Protection Manager。
管理員 3	- 使用者名稱：john - 全名：John Smith - 電子郵件地址：john@<sampldomain>.local - 在「存取權」標籤上，按下「系統管理員」。 - 在「驗證」標籤上，按下「目錄驗證」。 - 在「目錄伺服器」下拉式清單中，選取 <sampldomain> LDAP with User Name。 - 在「帳戶名稱」欄位中，輸入 John Smith。 - 按下「檢查帳戶」。 - 系統管理員 john 可以登入 Symantec Endpoint Protection Manager 進行目錄驗證。
管理員 4	- 使用者名稱：john - 全名：John Smith - 電子郵件地址：john@<sampldomain>.local - 在「存取權」標籤上，按下「系統管理員」。 - 在「驗證」標籤上，按下「目錄驗證」。 - 在「目錄伺服器」下拉式清單中，選取 <sampldomain> LDAP without User Name。 - 在「帳戶名稱」欄位中，輸入 John Smith。 - 按下「檢查帳戶」。 - 帳戶驗證失敗，但是系統管理員 John Smith 可以登入 Symantec Endpoint Protection Manager。

更多資訊

[以 Symantec Endpoint Protection Manager \(SEPM\) 來同步 Active Directory 群組](#)

使用多因素驗證為 LDAP 伺服器架構 Okta (14.3 RU8 或更新版本)

如果您的組織已使用 Okta 整合進行安全存取，則可以使用 Okta 來驗證管理員帳戶，而不是使用 Symantec VIP。多因素驗證可為登入程序的安全增添多一層保護。管理員登入時，他們必須認可通知或提供唯一的一次性記號。

如需 Symantec VIP 的概觀，請參閱：[使用 Symantec VIP 架構雙因素驗證](#)

步驟 1：在 Symantec Endpoint Protection Manager 中架構 LDAP 連線

首先，設定 Symantec Endpoint Protection Manager 與貴公司 Okta 伺服器之間的 LDAP 連線，並使用自動推送通知。

在 Symantec Endpoint Protection Manager 中架構 LDAP 連線

1. 在主控台中，新增管理員帳戶。
[新增管理員帳戶和設定存取權限](#)
2. 在「驗證」標籤上，選取「目錄驗證」>「目錄伺服器」。
3. 在「目錄伺服器」對話方塊中，按一下「新增」。
4. 在「新增目錄伺服器」對話方塊 > 「一般」標籤中，新增以下項目：
 - 「名稱」：<optionalname>
 - 伺服器類型：LDAP
 - 伺服器類型位址或名稱：yourcompany.ldap.okta.com
 - 「LDAP 通訊埠」：636
 - 「LDAP BaseDN」：ou=users,dc=<yourcompany>,dc=okta,dc=<top-leveldomain>。例
如：ou=users,dc=mycompany,dc=okta,dc=com
 - 「使用者名稱」：uid=<user@yourcompany.domain>,dc=<LDAP 伺服器名稱>,dc=<頂層網域名稱>。例
如：uid=kg123456@mycompany.com,dc=mycompany,dc=okta,dc=com
 - 「密碼」：Okta 的管理員密碼。
5. 按一下「確定」>「確定」。
6. 在「驗證」標籤的「目錄驗證」底下，新增下列資訊：
 - 「目錄伺服器」：<optionalname>
 - 「帳戶名稱」：例如：uid=kg123456@mycompany.com,dc=mycompany,dc=okta,dc=com
7. 按下「確定」。

步驟 2：使用 Okta Verify 登入 Symantec Endpoint Protection Manager

登入 Symantec Endpoint Protection Manager 取決於您的 Okta 管理員如何架構 Okta Verify。Symantec Endpoint Protection Manager 管理員可以登入：

- 自動，沒有任何通知。
- 藉由新增密碼以認可推送通知或新增多因素密碼。

更多資訊：

- [架構 Okta 登入政策](#)
- [透過 LDAP 介面使用多因素驗證](#)

使用 Okta Verify 自動推送來登入 Symantec Endpoint Protection Manager 主控台

1. 在 Symantec Endpoint Protection Manager 登入畫面 > 「密碼」欄位中，管理員輸入他們的一般使用者密碼，然後按一下「確定」。
2. 推播通知出現時，管理員需要批准推播。
LDAP 驗證完成，Symantec Endpoint Protection Manager 隨即開啟。

使用 Okta Verify 來登入 Symantec Endpoint Protection Manager 主控台 (沒有自動推送)

針對此登入架構，Okta 管理員需要管理員認可推送通知或新增多因素記號。

1. 在 Symantec Endpoint Protection Manager 登入畫面 > 「密碼」欄位中，管理員輸入：以下其中一個選項，然後按一下「確定」。
 - a. 針對推送通知：<password>,push
 - b. 針對記號：<password,MFAtoken>例如，管理員輸入：password,123456，其中密碼是管理員使用者密碼，123456 是 Okta Verify 密碼。

Symantec Endpoint Protection Manager 密碼遺失後重設

如果您有系統管理員帳戶，您可以重設自己的密碼並允許其他管理員重設他們自己的密碼。

要重設遺失的密碼，請確定啟用了以下項目：

- 管理員可以重設自己的密碼。請參閱：
[顯示「忘記了您的密碼？」連結，以便管理員可以重設遺失密碼](#)
- 「忘記了您的密碼？」連結已設為出現在管理伺服器登入畫面上。依據預設，會出現此連結。請參閱：
[在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊](#)
- 必須架構郵件伺服器，以便郵件伺服器傳送通知。
若要對 Symantec Endpoint Protection Manager 電子郵件失敗進行疑難排解，請參閱：
 - [錯誤：在 Endpoint Protection Manager 中傳送的測試電子郵件「無法傳送測試電子郵件」](#)
 - [正確設定電子郵件設定之後，Endpoint Protection Manager 密碼還原失敗](#)
 - [建立管理伺服器與電子郵件伺服器之間的通訊](#)

將此方法用於透過使用 Symantec Management Server 驗證進行驗證，而不是透過 RSA SecurID 驗證或目錄驗證進行驗證的管理員帳戶。

NOTE

在 14.2 和更新版本中，密碼必須包含至少 8 個字元且少於 16 個字元。密碼必須包含至少一個小寫字母 [a-z]、一個大寫字母 [A-Z]、一個數字字元 [0-9]，以及一個特殊字元 ["/\[]:;|=, + * ? < >]。

在 14.3 RU5 和更新版本中，密碼必須包含至少八個字元且少於 1024 個字元。您可使用其他字元和一個空格。您可將管理伺服器設定為需要唯一密碼。

[架構全域密碼需求](#)

如需詳細資訊，請參閱：

[選擇管理員帳戶的驗證方法](#)

如果您不知道收件者的電子郵件地址，請參閱：[尋找 Symantec Endpoint Protection Manager 管理員電子郵件地址](#)

重設忘記的 Symantec Endpoint Protection Manager 密碼

1. 在管理伺服器電腦上，按下「開始」>「所有程式」> **Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**。

依據預設，「忘記了您的密碼？」連結會出現在管理伺服器登入畫面上。

2. 在「登入」畫面上，按下「忘記了您的密碼？」。
3. 在「忘記了密碼」對話方塊中，輸入要重設密碼的帳戶的使用者名稱。

對於網域管理員和限制的管理員，輸入帳戶的網域名稱。如果未設定網域，請保留網域欄位空白。

4. 按下「暫時密碼」。

管理員會收到包含用於啟用暫時密碼的連結的電子郵件。管理員每分鐘只能向管理主控台要求暫時密碼一次。由於安全原因，管理伺服器不會驗證輸入資訊。

5. 管理員必須在登入後立即變更暫時密碼。

若要驗證管理員是否順利重設密碼，請檢查管理員收到的電子郵件訊息。請參閱：

[變更管理員帳戶或預設資料庫的密碼](#)

無法重設密碼時

如果您無法使用「忘記了您的密碼？」功能來復原管理員密碼，Symantec 也無法協助恢復您的密碼。您必須在不使用資料庫備份的情況下重新架構 Symantec Endpoint Protection Manager 和資料庫。此程序會覆寫先前的管理伺服器 and 資料庫設定，並可讓您重新建立新的密碼。因此，設定管理伺服器和稽核管理員帳戶資訊時正確架構電子郵件設定很重要。請參閱：

- [還原資料庫](#)
- [重新安裝或重新架構 Symantec Endpoint Protection Manager。](#)

顯示「忘記了您的密碼？」連結，以便管理員可以重設遺失密碼

如果您有系統管理員帳戶，您可以讓其他管理員重設其忘記的密碼。在 Symantec Endpoint Protection Manager 登入畫面上啟用「忘記了您的密碼？」連結，以便管理員可要求暫時密碼。

允許管理員重設忘記的密碼

1. 在主控台中，按下「管理員」。
2. 在「管理員」頁面中，按下「伺服器」。
3. 在「伺服器」下方，選取本機網站。
您只能針對本機網站控制此設定。
4. 按下「編輯網站屬性」。
5. 在「密碼」標籤上，勾選「允許管理員重設密碼」。
6. 按下「確定」。

更多資訊

- [重設忘記的 Symantec Endpoint Protection Manager 密碼](#)
- [在登入畫面上顯示「記住我的使用者名稱」核取方塊](#)

尋找 Symantec Endpoint Protection Manager 管理員電子郵件地址

您可能因為忘記安裝 Symantec Endpoint Protection 時設定的電子郵件地址，而無法登入 Symantec Endpoint Protection Manager。

尋找 Symantec Endpoint Protection Manager 管理員電子郵件地址

1. 在管理伺服器上，移至 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc。
2. 在「記事本」中，開啟 mailConfig.properties 檔案。
3. 尋找下列項目：adminMailRecipients= <name@broadcom.com>，其中 name@broadcom.com 是貴組織中收件者的電子郵件地址。
4. 執行下列其中一項工作：
 - 如果您看到電子郵件地址，請檢查此收件者電子郵件地址的電子郵件收件匣，並驗證他們是否取得 Symantec Endpoint Protection 的通知。
 - 如果您未看到特定電子郵件地址，則重設 Symantec Endpoint Protection Manager 管理員密碼，或在沒有資料庫備份的情況下重新架構 Symantec Endpoint Protection Manager 和資料庫。此程序會覆寫先前的管理伺服器和資料庫設定，並可讓您重新建立新的密碼。

[Symantec Endpoint Protection Manager 密碼遺失後重設](#)

[重新安裝或重新架構 Symantec Endpoint Protection Manager](#)

Symantec Endpoint Protection Manager 的帳戶名稱和密碼要求

依您所要求之不同帳戶名稱和密碼允許的長度和字元要求，來管理 Symantec Endpoint Protection Manager (SEPM)。強制執行下列需求。

Table 142: Symantec Endpoint Protection Manager 帳戶名稱和密碼要求

元件	需求
Symantec Endpoint Protection Manager 管理員帳戶	- 使用者名稱： - 不可超過 20 個字元。 - 不允許使用下列字元："/ \ [] : ; = , + * ? < > - 密碼： - 若使用 SQL Server 資料庫進行安裝，則允許所有字元。但是，您可使用不超過 256 個字元，且不可少於 6 個字元。 - 如果使用預設資料庫安裝： - 於 14.3 RU5 或更新版本中，密碼可以包含 8 個字元到 1024 個字元。此外，您還可設定是否需要字母和數字、唯一密碼和密碼重複使用限制。您可使用空格。如需詳細資訊，請參閱： 架構全域密碼需求 - 於 14.3 RU4 或更早版本中，密碼可包含 6 到 30 個字元。您不可使用空格，且不允許使用下列字元：\ " ; 管理員帳戶和具有預設資料庫的 SEPM 使用相同的使用者名稱和密碼。具有 SQL Server 資料庫組態的 Symantec Endpoint Protection Manager 有個別的需求。
SQL Server 驗證	SQL Server 管理員名稱 (DBA 使用者)： - 不可為空白。 - 您可以使用小寫字母和大寫字母、數字和下列特殊字元：& _ # \$ - 不可使用其他特殊字元。 - SEPM 中的預設值為 sa (適用於 SQL Server 的預設內建管理員帳戶)。您可指定具有伺服器管理員存取權限的任何帳戶。 SQL Server 管理員密碼 (DBA 密碼)： - 允許 128 個字元以下 (針對 Windows 驗證方法允許 79 個字元)。 - 允許所有字元，包括高 ASCII 或雙位元組字元，以及下列基於 Symantec Endpoint Protection Manager 版本和驗證方法的限制： - 早於 14.2 RU1：SQL 驗證或 Windows 驗證不允許使用下列字元：" [] { } () , ; ? * ! @ ; 14.2 RU1 和更新版本：如果是第一次安裝 SEPM，Windows 驗證允許但 SQLServer 驗證不允許以下字元：" [] { } () , ; ? * ! @ ;。 - 如果設定 SEPM，則不可使用以下字元：/ " < > 。 - 有關設定 DBA 密碼的建議，請參閱 Microsoft 文件。 - 此密碼是在您的 SQL Server 電腦上設定的。 - 您並未在 SEPM 上將其建立；僅進行提供。 具 Windows 驗證的 SQL Server 資料庫管理員： - 使用資料庫伺服器現有的 Windows 使用者名稱和密碼。 - Windows 驗證密碼不可使用下列字元：< > / " SQL Server SEP 資料庫名稱： - 不可為空白。 - 僅可使用下列字元：大小寫字母、數字和特殊字元 & _ # \$ - 不可使用其他特殊字元。 - Symantec Endpoint Protection 資料庫的預設值為 sem5 (與資料庫使用者名稱相同的值)。

元件	需求
具預設資料庫的 SEPM (SQL Server Express 或內嵌)	- 資料庫使用者名稱 (使用者)： - 不可超過 128 個字元；不可為空白。 - 僅可使用下列字元：大小寫字母、數字和特殊字元：~ # % _ + = : . - 不可使用下列特殊字元：` ! @ ' \$ ^ & * () - { } [] " \ / < ; > , ? - Symantec Endpoint Protection 資料庫使用者名稱的預設值為 sem5。 SEPM 資料庫使用者密碼 (密碼)： - 不可超過 128 個字元；不可為空白。 - 僅可使用大小寫字母、數字和下列特殊字元：~ # % _ + = : . / - 不可使用下列特殊字元：! @ * () { } [] ; , ?
加密密碼	「管理伺服器組態精靈」可以為您產生此密碼。 - 若選擇設定自己的密碼，其可包含 8 個字元到 1024 個字元 (14.3 RU5 或更新版本) 或 6 到 32 個字元 (14.3 RU4 和更早版本)。允許使用所有字元。
Symantec Endpoint Protection Manager 群組名稱	- 群組名稱最多可包含 990 個字元。 - 群組名稱的完整路徑最多可包含 1000 個字元。 - 不可使用下列字元：" / \ * ? < > : &
Symantec Endpoint Protection Manager 網域名稱	- 網域名稱長度不可超過 256 個字元，且不可為空白。 - 不可使用下列字元：" / \ [] : ; = , + * ? < >
Symantec Endpoint Protection Manager 網站名稱	- 網站名稱長度不可超過 60 個字元，且不可為空白。 - 允許使用所有字元。

變更管理員帳戶或預設資料庫的密碼

變更管理員帳戶的密碼

如果密碼已忘記、遺失或遭受破壞，您需要變更您的帳戶或其他管理員帳戶的密碼。

變更密碼時適用下列規則：

- 系統管理員可以變更所有管理員的密碼。
- 網域管理員可以變更同一個網域中其他網域管理員和限制的管理員的密碼。
- 限制的管理員只能變更自己的密碼。

如果變更密碼是為了解決管理員帳戶鎖定問題，管理員仍必須等到鎖定期結束。

NOTE

在 14.2 或更新版本中，密碼必須包含 8 個字元至 16 個字元。它必須包含至少一個小寫字母 [a-z]、一個大寫字母 [A-Z]、一個數字字元 [0-9]，以及一個特殊字元 ["/\ [] : ; | = , + * ? < >] @。

在 14.3 RU5 中，密碼必須包含 8 個字元至 1024 個字元。此外，您還可設定是否需要字母和數字、唯一密碼和密碼重複使用限制。請參閱：

[架構全域密碼需求](#)

如需詳細資訊，請參閱：

[在嘗試太多次登入後解除鎖定管理員的帳戶](#)

變更管理員帳戶的密碼

- 在主控台中，按下「管理員」>「管理員」。
- 在「管理員」下方，選取管理員帳戶，再按下「變更密碼」。
按 F1，查看密碼限制。
- 輸入您的密碼和管理員的新密碼。

4. 按下「變更」。請參閱：
 - [重設忘記的 Symantec Endpoint Protection Manager](#)
 - [顯示「忘記了您的密碼？」連結](#)，以便管理員可以重設遺失密碼

變更預設資料庫密碼

架構管理伺服器並選取預設資料庫 (Microsoft SQL Server Express 或內嵌資料庫 (14.3 MPx 和更新版本)) 時，輸入的預設管理員帳戶 `admin` 密碼也會成為資料庫密碼。如果您變更預設管理員的密碼，資料庫密碼並不會自動變更。透過重新執行「管理伺服器組態精靈」並重新配置 Symantec Endpoint Protection Manager，您可以變更資料庫密碼。

若要變更預設資料庫密碼

1. 在 Windows 的「開始」功能表上，瀏覽到 **Symantec Endpoint Protection Manager** > 「管理伺服器組態精靈」。
2. 按下「重新架構管理伺服器」，然後按「下一步」>「下一步」。請參閱：[重新安裝或重新架構 Symantec Endpoint Protection Manager 密碼](#)
3. 按一下下列其中一個選項，然後按一下「變更資料庫管理員密碼」並輸入新密碼。
 - 按一下「預設 **SQL Server Express** 資料庫」(14.3 RU1 和更新版本)。
 - 按一下「預設 內嵌資料庫」(14.3 MPx 和更新版本)。
4. 遵循每個面板的指示來完成架構。

架構全域密碼需求

在 14.3 RU5 和更新版本中，Symantec Endpoint Protection Manager (SEPM) 可讓系統管理員為管理員建立複雜密碼，以保護電腦免受暴力攻擊。您可以設定密碼需求，以滿足貴組織的密碼政策準則。這些設定會覆寫預設的 SEPM 密碼需求。如果您想要繼續使用預設 SEPM 密碼需求，則請停用此對話方塊中的選項。

這些密碼需求適用於所有網域和所有類型的管理員 (系統、網域和受限制)。

檢閱下列資訊：

- 預設 Microsoft SQL Express 資料庫或 Microsoft SQL Server 資料庫的管理員帳戶具有個別的密碼需求。
- 複雜程度還必須符合 Microsoft SQL Express 密碼需求，且應與目前的 SEPM 需求相同或更複雜。
- 首次在「管理伺服器組態精靈」中架構管理伺服器時，可選取預設安裝或自訂安裝。若您選取預設安裝，則輸入的密碼與加密密碼相同。如果此時變更管理員密碼，則加密密碼就不會變更。
- 從 14.3 RU4 或更新版本升級時，現有密碼仍然有效。但是，下次架構密碼時，必須符合這些更嚴格的需求。
- 在 14.3 RU5 和更新版本中，密碼強度層級更為嚴格。例如，在 RU4 和更新版本中視為「##」，在 RU5 中則視為「#」。

如需瞭解密碼要求，請參閱：

[Symantec Endpoint Protection Manager 的帳戶名稱和密碼要求](#)

若要建立管理員的密碼

1. 在主控台中，按下「管理員」>「管理員」。
2. 按一下「架構密碼需求」，然後視需要變更預設值。

選項	14.3 RU5 和更新版本預設值	14.3 RU4 及更新版本的預設值
大寫字母 [A-Z]、小寫字母 [a-z] 和數字 [0-9]	已啟用	已啟用 - 無法停用
特殊字元	~ ` # \$ % - _ + = : . ' ^ & / \ < > [] { } 和空格。	相同。 建立管理員使用者 <code>REST API</code> 不支援空格或 " ; \ 特殊字元。(14.3 RU5 和更新版本)。
字元數下限	8	8
字元數上限	1024	16
限制密碼重複使用	已啟用	無限制

管理員可以重複使用密碼前的唯一密碼數	6	無限制
管理員可以重複使用密碼前的最大天數	90	無限制

3. 按一下「確定」。

更多資訊

[新增管理員帳戶和設定存取權限](#)

[變更管理員帳戶或預設資料庫的密碼](#)

如需用戶端密碼需求的相關資訊，請參閱[用密碼保護 Symantec Endpoint Protection 用戶端](#)

使 Symantec Endpoint Protection Manager 登入密碼永久有效

如果您使用 Symantec Endpoint Protection Manager 驗證，則密碼的預設選項設定為在 60 天後到期。

您可以顯示選項，供管理員使用永久有效的密碼。此選項預設為停用以增加安全性，因此您必須先啟用它。啟用此選項後，選項會出現在管理員帳戶的「驗證」標籤上。

使 Symantec Endpoint Protection Manager 登入密碼永久有效

1. 在主控台中，按下「管理員」。
2. 在「管理員」頁面中，按下「網域」。
3. 在「網域」下，選取允許管理員儲存登入憑證的網域。
4. 按下「編輯網域屬性」。
5. 在「密碼」標籤上，按下「允許管理員使用永不到期密碼」。
6. 按下「確定」。
7. 按下「管理員」>「管理員」，然後開啟管理員帳戶。
8. 在「驗證」標籤上，按下「密碼永久有效」，然後按下「確定」。

更多資訊

- [重設忘記的 Symantec Endpoint Protection Manager 密碼](#)
- [在嘗試太多次登入後解除鎖定管理員的帳戶](#)

在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息

您可以建立和顯示所有管理員登入主控台之前會看到的自訂訊息。最主要的用途是向即將登入專屬電腦的管理員顯示法律聲明。

在管理員鍵入其使用者名稱和密碼並按下「登入」後，會在主控台中顯示此訊息。管理員閱讀訊息後，他們可以同意聲明的內容並按下「確定」，即可登入成為管理員。如果管理員按下「取消」，則會取消登入程序，而管理員會回到登入視窗。

如果管理員從連線至管理伺服器的獨立網頁瀏覽器執行報告功能，此訊息也會出現。

在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息

1. 在主控台中，依序按下「管理員」和「網域」。
2. 選取要為其新增登入橫幅的網域。
3. 在「工作」下方，按下「編輯網域屬性」。
4. 在「登入橫幅」標籤上，勾選「當管理員登入 Symantec Endpoint Protection Manager 時，顯示法律聲明」。
5. 輸入橫幅標題和文字。

如需詳細資訊，按下「說明」。

-
6. 按下「確定」。

更多資訊

新增管理員帳戶和設定存取權限

在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊

系統管理員可啟用「記住我的使用者名稱」和「記住我的密碼」核取方塊，使其出現在其他管理員帳戶的 Symantec Endpoint Protection Manager 登入畫面上。管理員的使用者名稱和密碼會預先填入登入畫面。

在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊

1. 在主控台中，按下「管理員」。
2. 在「管理員」頁面中，按下「網域」。
3. 在「網域」下，選取允許管理員儲存登入憑證的網域。
4. 按下「編輯網域屬性」。
5. 在「密碼」標籤上，勾選「允許使用者在登入時儲存憑證」。
6. 按下「確定」。

更多資訊

重設忘記的 Symantec Endpoint Protection Manager 密碼

允許或攔截存取遠端 Symantec Endpoint Protection Manager 主控台

根據預設，會授予對所有主控台的存取。管理員可以從本機或遠端網路中的任何一台電腦登入主要主控台。

您可以透過拒絕對某些電腦的存取，保護管理主控台不進行遠端連線。

您最好授予或拒絕以下類型的使用者或電腦進行的存取：

- 您應該拒絕 Internet 上任何人進行存取。否則，主控台會面臨 Internet 攻擊的風險。
- 如果受限管理員使用非其管理之網路上的主控台，您應該拒絕他們存取。
- 您應該授予系統管理員和 IT 管理員存取權。
- 您應該授予實驗室電腦 (例如用於測試的電腦) 存取。

除了全域授予或拒絕存取之外，您也可以使用 IP 位址指定例外。如果授予存取所有遠端主控台，管理伺服器會拒絕存取例外項目。相反地，如果您拒絕存取所有遠端主控台，那麼將會自動授予存取例外項目。當您建立例外時，指定的電腦必須具有靜態 IP 位址。您也可以指定子網路遮罩，針對電腦群組建立例外。例如，您可能想要在您管理的所有區域中授予存取。不過，您可能會想要拒絕位於公共區域之主控台的存取。

授予或拒絕遠端主控台的存取

1. 在主控台中，按下「管理員」，再按「伺服器」。
2. 在「伺服器」下方，選取您要變更遠端主控台存取權限的伺服器。
3. 在「工作」下方，按一下「編輯伺服器屬性」。
4. 在「一般」標籤上，按下「授予存取」或「拒絕存取」。
5. 如果您要指定電腦 IP 位址，將其設為此主控台存取權限的例外，請按下「新增」。

您新增的電腦成為例外項目。如果您按下「授予存取」，您指定的電腦會被拒絕存取。如果您按下「拒絕存取」，您指定的電腦會被授予存取。您可以針對單一電腦或電腦群組建立例外。

6. 在「拒絕主控台存取」對話方塊中，按下列其中一個選項：
 - 單一電腦

針對單一電腦，輸入 IP 位址。

- 電腦群組

對於多台電腦，輸入群組的 IP 位址及子網路遮罩。

7. 按下「確定」。

此時電腦會出現在例外清單中。會顯示每個 IP 位址與遮罩的權限狀態。

如果您將「授予存取」變更為「拒絕存取」，或將「拒絕存取」變更為「授予存取」，所有例外也會一併變更。如果您曾經建立拒絕存取的例外，此時會變更為允許存取。

8. 按下「編輯全部」，變更顯示在例外清單上電腦的 IP 位址或主機名稱。

「IP 位址編輯器」隨即出現。「IP 位址編輯器」是一種文字編輯器，可讓您編輯 IP 位址和子網路遮罩。

9. 按下「確定」。

10. 完成新增例外至清單或完成編輯清單後，請按下「確定」。

更多資訊

- [新增管理員帳戶和設定存取權限](#)
- [登入 Symantec Endpoint Protection Manager 主控台](#)

在嘗試太多次登入後解除鎖定管理員帳戶

Symantec Endpoint Protection Manager 會在管理員多次嘗試登入失敗後，鎖定管理員一段時間。依預設，管理伺服器會在嘗試失敗 5 次之後鎖定管理員達 15 分鐘的時間。

您可能想鎖定管理員帳戶，來攔截使用隨機使用者名稱和密碼登入管理伺服器的惡意攻擊。

為提高安全性，第一次鎖定之後，每額外鎖定 1 次都會將鎖定間隔加倍。Symantec Endpoint Protection Manager 在成功登入後或第一次鎖定後的 24 小時之後，會恢復原始的鎖定時間間隔。例如，如果原始鎖定時間間隔為 15 分鐘，第二次鎖定會觸發 30 分鐘的鎖定時間間隔。第三次鎖定則會觸發 60 分鐘的鎖定時間間隔。如果第一次鎖定發生於星期四下午 2 點，則 24 小時期間會結束於星期五下午 2 點，且 Symantec Endpoint Protection Manager 會將鎖定間隔重設為 15 分鐘。

禁止鎖定管理員帳戶

您可以停用管理員帳戶的鎖定，即使此動作不會解除帳戶鎖定。您也可以變更登入嘗試失敗次數和鎖定帳戶前允許的等待時間。密碼變更不會重設或影響到鎖定時間間隔。

禁止鎖定管理員帳戶

1. 在主控台中，按下「管理員」>「管理員」。
2. 在「管理員」下，選取遭到鎖定的管理員帳戶。
3. 在「工作」下，按下「編輯管理員」。
4. 在「一般」標籤上，取消勾選「達到指定的登入失敗次數後鎖定帳戶」。

解鎖管理員帳戶

管理員可以透過以下任一方式解鎖帳戶：

- 使用重置帳戶鎖定選項。
- 等待指定時間。

使用重置帳戶鎖定選項

1. 在主控台中，按下「管理員」>「管理員」。
2. 在「管理員」下方，選取管理員帳戶，再按下「重置帳戶鎖定」。
即會顯示訊息「##### <##>」。

更多資訊

- [重設忘記的 Symantec Endpoint Protection Manager 密碼](#)
- [變更管理員帳戶或預設資料庫的密碼](#)
- [使 Symantec Endpoint Protection Manager 登入密碼永久有效](#)

變更保持登入 Symantec Endpoint Protection Manager 主控台的逾時期間

為了防止未經授權的使用者登入 Symantec Endpoint Protection Manager，主控台會在您在 Java 主控台閒置 1 小時和在 Web 主控台閒置 10 分鐘後自動將您登出。您可以縮短或延長此逾時期間。

變更 Java 主控台的逾時期間

您可以變更每個網站的遠端 Java 主控台的逾時期間。

若要變更 Java 主控台的逾時期間

1. 在管理伺服器上，按「管理」>「伺服器」。
2. 按下「本機站台」或遠端站台，並且按下「編輯站台屬性」。
3. 在「一般」標籤上，按下「主控台逾時」下拉式清單，然後選取其中一個可用選項作為時間長度。
4. 按一下「確定」。

變更 Web 主控台的逾時期間

Web 主控台會在 10 分鐘之後逾時。若要變更 Web 主控台的預設逾時值，您可以編輯設定檔案。如果延長逾時值可能會造成管理伺服器的效能降低。

若要在設定檔案內變更 Web 主控台的預設逾時期間

1. 在管理伺服器上，於文字編輯器中開啟以下檔案：
`Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties`
2. 如果尚不存在，請新增下列一行：
`scm.web.timeout.minutes=<timeout_value>`
<timeout_value> 為無活動的分鐘數，在此時間之後，主控台即會登出。最大值為 60 (以分鐘為單位)。如果將該值設為 0，則系統會套用預設值。預設逾時為 10 分鐘。將該值設為 0 等於未將該值新增到設定檔案。如果出現這行，您可以變更逾時值。負值則會停用逾時期間。
3. 儲存並關閉檔案。
4. 重新啟動 Symantec Endpoint Protection Manager 服務。

[停止及啟動管理伺服器服務](#)

若要調整虛擬記憶體設定

如果遠端管理員在嘗試登入遠端主控台時遇到重試頁面，則您必須調整虛擬記憶體設定。如果延長虛擬記憶體值會造成管理伺服器的效能降低。

1. 在管理伺服器上，於文字編輯器中開啟以下檔案：
`### > Symantec > Symantec Endpoint Protection Manager > tomcat > etc > conf.properties`
2. 將下列一行新增到 `conf.properties` 檔案，然後儲存該檔案：
`scm.web.ui.required.virtualmem_mb=<virtual memory value>`
<virtual memory value> 是系統所需的記憶體值 (以 MB 為單位)。若要停用虛擬記憶體限制，請將該值設為 0。預設值為 500 MB。
3. 重新啟動管理伺服器。

重新啟動管理伺服器時，您設定的值或預設值將寫入 `catalina.err`。

若要變更 Web 瀏覽器的逾時期間

如果 Web 瀏覽器設為比 Web 主控台更快逾時，則您必須延長 Web 瀏覽器的值。

- 如果是 Internet Explorer，請遵循 Microsoft 文章中的指示來變更登錄機碼 `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings`：
[如何變更 Internet Explorer 中的預設 Keep-Alive 逾時值](#)
- Google Chrome 沒有可針對網路逾時期間架構的設定。
- 如果是 Mozilla Firefox，請在位址欄中輸入以下文字：`about:config`。將值 (秒) 變更為您需要的值。預設值為 115。

關於網域

安裝管理伺服器時，Symantec Endpoint Protection Manager 主控台中有一個稱為 Default 的網域。網域是從 Symantec Endpoint Protection Manager 基礎架構分離出的資料的邏輯分隔。網域是主控台內的結構性配置區，可用來編排群組、用戶端、電腦和政策的階層。您可以設定額外的網域，以管理網路資源。

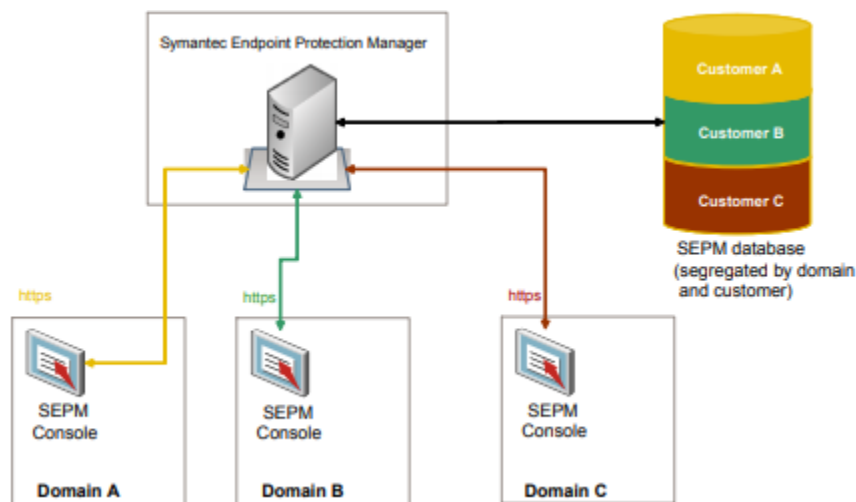
網域的主要目的在於，受管服務提供者可以建置可為多個客戶提供服務的單一 Symantec Endpoint Protection Manager 基礎架構。

NOTE

Symantec Endpoint Protection Manager 中的網域不同於 Windows 網域或其他網路網域。

新增的每個網域都將共用相同的管理伺服器和資料庫，並提供其他主控台實例。各個網域的全部資料都會完全分隔。這種分隔可避免某個網域的管理員檢視其他網域的資料。您可以新增管理員帳戶，以便各個網域有各自的管理員。這些管理員只能檢視及管理其自己的網域內容。

如果您的公司規模相當大，在許多地區都有營業處，您可能需要能夠集中檢視管理資訊。您可以委派管理權限、實際分隔安全資料，或設定編排使用者、電腦和政策的較大彈性。如果您是受管服務提供者 (MSP)，可能需要管理多家獨立的公司，以及「Internet 服務供應商」。為滿足這些需求，您可以建立多個網域。例如，針對各個國家、地區或公司，您可以建立個別的網域。



新增網域時，網域中空無內容。您必須將該網域設定為目前的網域。然後將管理員、群組、用戶端、電腦和政策新增至此網域。

您可以將政策從一個網域複製到另一個網域。若要在網域間複製政策，您可以從來源網域匯出政策，然後將此政策匯入目的地網域。

您也可以將用戶端從一個網域移動到另一個網域。若要在網域之間移動某用戶端，舊網域的管理員必須從用戶端群組中刪除該用戶端。然後就可以將用戶端上的「通訊設定」檔案取代為新網域中的檔案。

如果您不再需要某個網域，則可以將其停用。當嘗試停用網域時，確定未將它設定為目前網域。

更多資訊

- [新增網域](#)
- [切換至目前的網域](#)

新增網域

您可以建立網域來編排組織中群組、用戶端、電腦和政策的階層。例如，您可能想新增網域來依部門組織使用者。

NOTE

您可以使用網域 ID 來進行災難復原。如果組織內的管理伺服器皆已故障，則您必須使用與舊伺服器相同的 ID 來重建管理伺服器。您可以從任何用戶端的 sylink.xml 檔案取得舊的網域 ID。

新增網域

1. 在主控台中，按下「管理員」。
2. 在「管理員」頁面中，按下「網域」。
3. 在工作下，按下「新增網域」。
4. 在「新增網域」對話方塊中，輸入網域名稱，並選擇性地輸入公司名稱和聯絡資訊。
5. 如果您要新增網域 ID，請按下「進階」，然後在文字方塊中輸入值。
6. 按下「確定」。

更多資訊

[關於網域](#)

切換至目前的網域

預設網域名為 **Default**，且設定為目前網域。在 Symantec Endpoint Protection Manager 主控台中新增網域時，網域中空無內容。若要為新網域新增群組、用戶端、政策和管理員，必須首先將其設定為目前網域。將網域指定為目前網域後，標題中的網域名稱後將顯示文字「目前網域」。如果您有多個網域，必須捲動「網域」清單以顯示目前網域是哪一個。

如果您以系統管理員的身分登入主控台，不論何者為目前網域，您都會看見全部的網域。然而，您只會看見目前網域中建立的管理員和限制的管理員。如果您以管理員或限制的管理員等身分登入主控台，只會看見您可存取的網域。

如果移除目前的網域，管理伺服器會將您登出。只能移除不是目前網域，且不是唯一網域的網域。

切換至目前的網域

1. 在主控台中，按下「管理員」。
2. 在「管理員」頁面中，按下「網域」。
3. 在「網域」下，按下要設為目前網域的網域。
4. 在「工作」下，按下「管理網域」。
5. 在「管理員網域」對話方塊中，若要進行確認，按下「是」。
6. 按下「確定」。

更多資訊

- [關於網域](#)
- [新增網域](#)

如何更新用戶端上的內容和定義檔

更新內容包括病毒定義檔、入侵預防特徵和主機完整性範本等。

依據預設，Symantec Endpoint Protection Manager 從公用 Symantec LiveUpdate 伺服器下載內容更新。Symantec Endpoint Protection 用戶端接著會從 Symantec Endpoint Protection Manager 下載這些更新。該內容包括病毒定義檔、入侵預防特徵和主機完整性範本等。

NOTE

如果要在 Symantec Endpoint Protection Manager 無法存取網路或 LiveUpdate 管理員 (LUA) 伺服器時更新內容，您可以使用 .jdb 檔案下載並安裝已驗證的定義。請確認您下載並套用正確的 .jdb 檔案。例如，14.3 RU6 定義可以套用於從 14.3 RU0 到 14.3 RU6 的所有用戶端，但 14.3 RU7 定義僅適用於 14.3 RU7 用戶端。

您可以建立使用 .jdb 檔案名稱格式的自動指令碼，儘管 Symantec 可能會更改檔案格式。請勿建立從 .jdb 內部解壓縮和複製檔案名稱的自動化指令碼。

[下載 .jdb 檔案以更新 Endpoint Protection Manager 的定義檔](#)

Table 143: 更新 Symantec Endpoint Protection 用戶端上的內容的步驟

工作	說明
請確保管理伺服器具有來自 LiveUpdate 的最新內容 (建議使用)	依據預設，在 Symantec Endpoint Protection Manager 安裝過程中，LiveUpdate 會執行。遇到下列情況時，您可能需要手動執行 LiveUpdate： - 在安裝期間略過了 LiveUpdate。 - 您必須執行 LiveUpdate 才能下載主機完整性範本和入侵預防特徵。 - 您想要在下一個排程更新之前執行 LiveUpdate。 如需詳細資訊，請參閱： 確認 Symantec Endpoint Protection Manager 具有最新內容 此外，如果您使用遠端複製，則可以在本機站台與夥伴站台之間遠端複製內容和政策。請參閱： 如何安裝第二個網站用於遠端複製
變更用戶端電腦取得更新的方式 (選擇性)	根據預設，Windows 用戶端電腦將從管理伺服器取得內容更新。其他傳送方法包括群組更新提供者、內部 LiveUpdate 伺服器或第三方工具派送。您可能需要變更傳送方法以支援不同的用戶端平台、大量的用戶端或網路限制。請參閱： 選擇派送方法以更新用戶端上的內容 選擇派送方法以根據平台來更新用戶端上的內容
變更管理伺服器的 LiveUpdate 設定 (選擇性)	您可以自訂 LiveUpdate 階段作業的頻率、下載的防護元件等。請參閱： 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager
減少網路超載 (建議使用)	如果管理伺服器收到太多來自用戶端的關於完整定義套件的並行要求，網路可能會超載。您可以降低這些超載的風險，並阻止用戶端下載完整定義。請參閱： 減少用戶端更新要求的網路超載
改善效能 (建議使用)	為了協助降低下載對網路頻寬的影響，可以隨機下載內容，這樣，所有用戶端就不會同時取得更新。請參閱： 關於隨機化同時內容下載 從預設管理伺服器或群組更新提供者隨機進行內容下載 從 LiveUpdate 伺服器隨機進行內容下載 為了緩解下載對用戶端電腦效能的影響，您可以讓用戶端電腦在閒置時下載內容更新。請參閱： 將 Windows 用戶端更新架構為在用戶端電腦閒置時執行

工作	說明
讓您的端點使用者管理他們自己的更新 (選擇性)	根據預設，用戶端電腦上的使用者可以隨時執行 LiveUpdate。您可以決定給予使用者對其內容更新的控制範圍。請參閱： 架構使用者對 LiveUpdate 的控制能力 您也可以用戶端電腦上使用智慧型更新小幫手 (Intelligent Updater) 來更新定義檔。請參閱： 使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容
在賽門鐵克發布測試引擎更新之前測試更新 (選擇性)	賽門鐵克將每季發布引擎更新。在使用特定的 Symantec LiveUpdate 伺服器發布引擎更新之前，您可以先下載這些更新。然後，在引擎內容遞送到生產環境之前，可以測試內容。請參閱： 在 Windows 用戶端上發布之前測試引擎更新

更多資訊

[準備非受管用戶端以從第三方派送工具接收更新](#)

如需詳細瞭解 LiveUpdate 錯誤代碼，請參閱：[LiveUpdate 錯誤代碼 \(Endpoint Protection/Endpoint Security\)](#)

選擇派送方法以更新用戶端上的內容

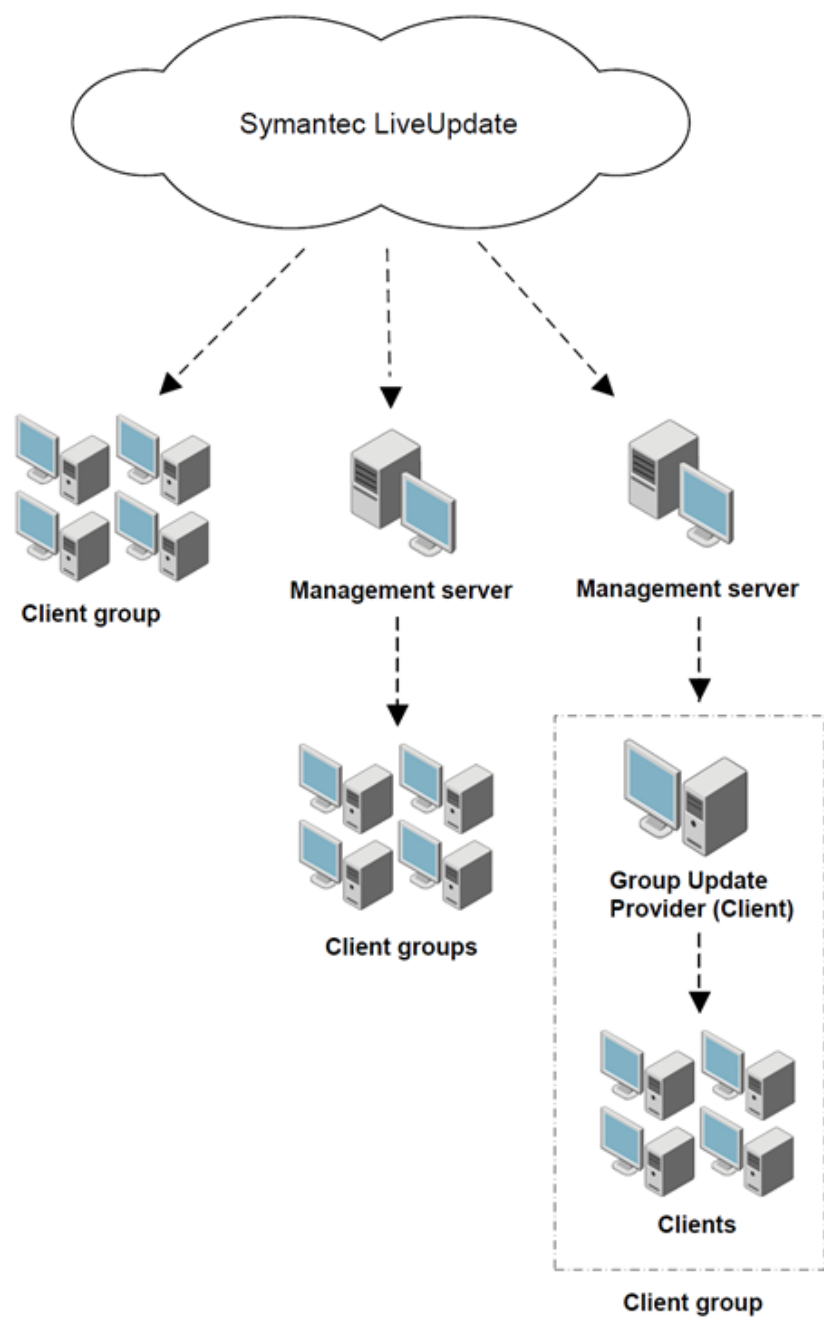
您可能需要變更用戶端的預設更新方法，視用戶端平台、網路組態、用戶端數目或是您公司的安全政策和存取政策而定。

Table 144: 內容派送方法及使用時機

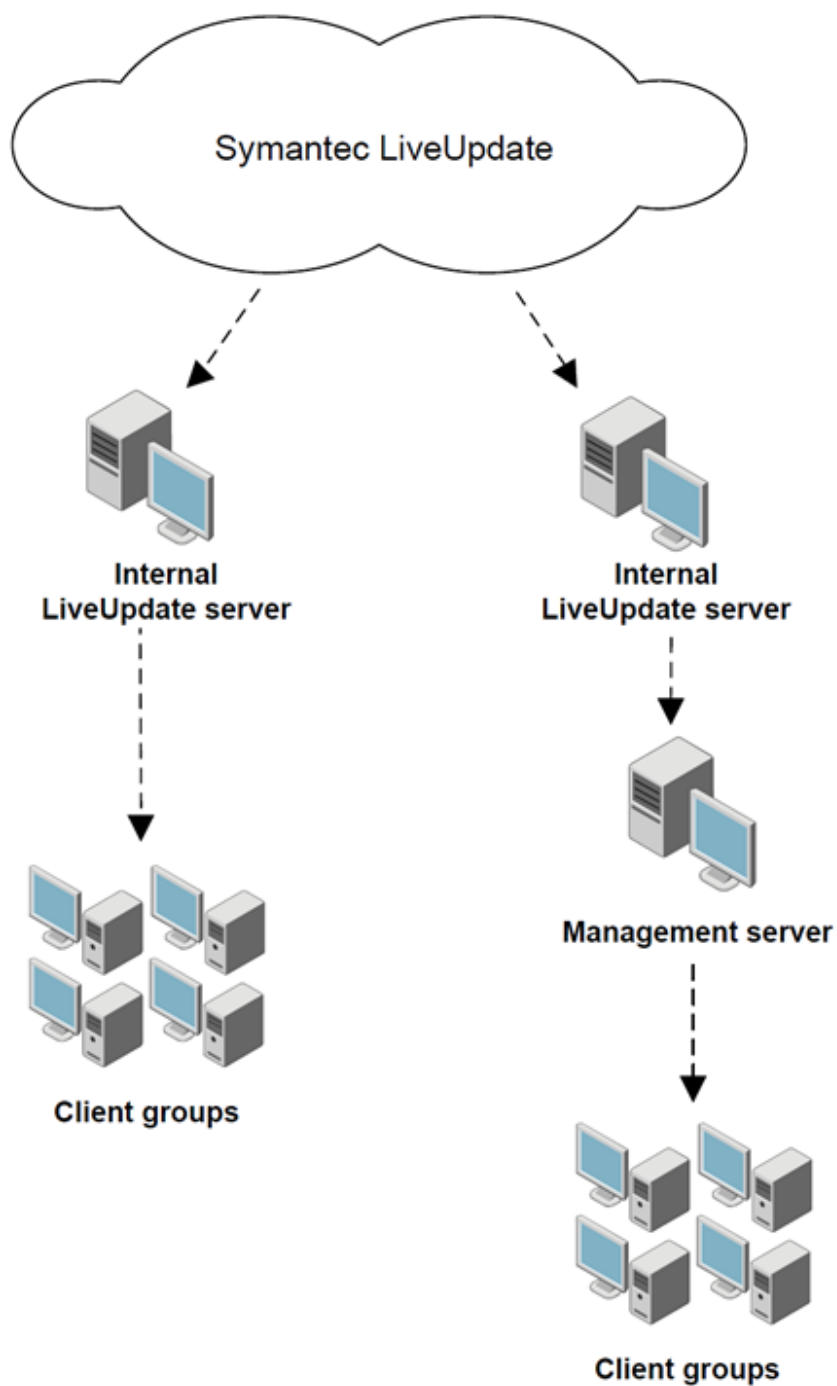
方法	說明	使用時機
Symantec Endpoint Protection Manager 至用戶端電腦 (預設值) (Windows、Mac、Linux)	預設管理伺服器會自動更新所管理的用戶端電腦。請勿定義從管理伺服器到用戶端之更新的排程。用戶端根據通訊模式和活動記錄頻率從管理伺服器下載內容。請參閱： 將用戶端架構為從 Symantec Endpoint Protection Manager 下載內容 • 使用推送模式或提取模式更新用戶端上的政策和內容	賽門鐵克建議您使用此方法，除非網路限制或是您的政策需要替代方法。 如果您有大量用戶端或頻寬問題，可以搭配使用此方法和「群組更新提供者」。 要讓 Mac 或 Linux 電腦從管理伺服器接收內容更新，則必須架構 Apache Web 伺服器。請參閱： 使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容
「群組更新提供者」至用戶端電腦 (僅限 Windows 用戶端)	「群組更新提供者」是從管理伺服器接收更新的用戶端電腦。然後，「群組更新提供者」會將更新轉送到群組中的其他用戶端電腦。「群組更新提供者」可以更新多個群組。 「群組更新提供者」可以派送除用戶端軟體更新之外的所有類型的 LiveUpdate 內容。「群組更新提供者」也無法用於更新政策。	「群組更新提供者」可讓您減輕管理伺服器的負載，而且比內部 LiveUpdate 伺服器更容易架構。 對於位於最小頻寬的遠端位置的群組，請使用「群組更新提供者」。請參閱： • 使用群組更新提供者將內容散佈至用戶端 • 決定是否要設定多個網站和遠端複製

方法	說明	使用時機
內部 LiveUpdate 伺服器至用戶端電腦 (Windows、Mac、Linux)	用戶端電腦可以直接從內部 LiveUpdate 伺服器下載更新。內部 LiveUpdate 伺服器從 Symantec LiveUpdate 伺服器接收其更新。 如有必要，您可以設定幾個內部 LiveUpdate 伺服器，並將此清單散佈到用戶端電腦。 您可以將下載排程從 LiveUpdate 伺服器變更為管理伺服器。請參閱： 針對用戶端電腦架構 LiveUpdate 下載排程 如需設定內部 LiveUpdate 伺服器的詳細資訊，請參閱 <i>LiveUpdate Administrator User's Guide</i>，網址為： 下載 LiveUpdate Administrator	內部 LiveUpdate 伺服器可讓您減輕大型網路中管理伺服器的負載。在較小型網路中，請考量「群組更新提供者」是否能夠滿足組織的需要。 請考慮在下列情況下使用內部 LiveUpdate 伺服器： • 如果管理大型網路 (超過 10,000 個用戶端) • 如果管理不應連線至外部 LiveUpdate 伺服器的 Mac 或 Linux 用戶端 • 如果您組織部署的多項賽門鐵克產品也使用 LiveUpdate 派送內容到用戶端電腦 Note: 您不應該將管理伺服器與內部 LiveUpdate 伺服器安裝在同一個實體硬體或虛擬機器上。安裝在同一台電腦上可能導致重大的伺服器效能問題。 如需詳細資訊，請參閱： • 同一台電腦上的 LiveUpdate Administrator 2.x 和 Symantec Endpoint Protection Manager • 將用戶端架構為從內部 LiveUpdate 伺服器下載內容
外部 Symantec LiveUpdate 伺服器透過 Internet 與用戶端電腦連線 (Windows、Mac、Linux)	用戶端電腦可以直接從 Symantec LiveUpdate 伺服器接收更新。	如果您需要排程用戶端更新內容的時間或者 Symantec Endpoint Protection Manager 與用戶端之間的可用頻寬受限，則可以使用外部 Symantec LiveUpdate 伺服器。 Symantec Endpoint Protection Manager 和排程更新預設會啟用。使用預設設定時，用戶端一律從管理伺服器取得更新，除非管理伺服器在較長時間內無回應。 Note: 請勿將大量的受管理網路用戶端架構為從外部 Symantec LiveUpdate 伺服器提取更新。此組態會耗用不必要的頻寬。 如需詳細資訊，請參閱： 架構用戶端從外部 LiveUpdate 伺服器下載內容
第三方工具派送 (僅限 Windows 用戶端)	Microsoft SMS 等第三方工具可將特定的更新檔案派送至用戶端。	此方法可讓您在派送更新檔案之前先行測試。如果您備有第三方工具派送基礎架構，則可能也適用。請參閱： 使用第三方派送工具派送內容
智慧型更新程式 (僅限 Windows 用戶端)	智慧型更新程式檔案包含可用於手動更新用戶端的病毒和安全風險內容以及入侵預防內容。 您可以從賽門鐵克網站下載智慧型更新小幫手 (Intelligent Updater) 自動解壓縮檔案。	如果 LiveUpdate 無法使用，可以使用智慧型更新小幫手 (Intelligent Updater) 檔案。請參閱： 使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容 若要更新其他種類的內容，您必須設定和架構管理伺服器以下載和預備更新檔案。請參閱： 使用第三方派送工具更新用戶端電腦

下表顯示較小型網路的派送架構範例。



下表顯示較大型網路的派送架構範例。



更多資訊

- [選擇派送方法以根據平台來更新用戶端上的內容](#)
- [如何更新用戶端上的內容和定義檔](#)
- [將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)

選擇派送方法以根據平台來更新用戶端上的內容

可用於將病毒定義檔和其他內容派送到用戶端電腦的方法視用戶端平台而定。

Table 145: 根據 Windows、Mac 和 Linux 用戶端的內容派送方法

平台	方法
Windows	依據預設，Windows 用戶端會從管理伺服器取得內容。 Windows 用戶端也可以從下列來源取得更新： • LiveUpdate 伺服器 (外部或內部)。請參閱： – 將用戶端架構為從內部 LiveUpdate 伺服器下載內容 – 架構用戶端從外部 LiveUpdate 伺服器下載內容 • 外部 LiveUpdate 伺服器 (僅限測試)。請參閱：在 Windows 用戶端上發布之前測試引擎更新 • 群組更新提供者。請參閱：使用群組更新提供者將內容散佈至用戶端 • 第三方派送工具。請參閱：使用第三方派送工具派送內容 • 智慧型更新小幫手。請參閱：使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容 如需詳細資訊，請參閱：選擇派送方法以更新用戶端上的內容 對於 Windows 用戶端，您也可以自訂下列設定： • 用戶端接收的內容類型 • 用戶端是否能從多個來源取得定義檔 • 如果管理伺服器只能提供完整定義檔套件，則用戶端是否能從 LiveUpdate 取得較小的套件 (增量) 完整定義檔套件非常龐大。下載過多完整套件可能會使您的網路超載。增量通常小很多，對網路頻寬的影響也很少。請參閱：減少用戶端更新要求的網路超載
Mac 或 Linux	• LiveUpdate 伺服器 (外部或內部) • 架構為反向代理的 Apache Web 伺服器。請參閱：使 Mac 或 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容

更多資訊

- [將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)
- [關於 LiveUpdate 下載的內容類型](#)
- [如何更新用戶端上的內容和定義檔](#)

將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager

架構管理伺服器下載 LiveUpdate 內容時，必須做幾個決定。將內容下載至 Symantec Endpoint Protection Manager 時，可以下載站台上所有管理伺服器的內容。

關於下載內容的決定

Table 146: 關於內容下載的決定

決定	說明
LiveUpdate 伺服器應該提供什麼內容給站台？	您可以指定外部 Symantec LiveUpdate 伺服器 (建議) 也可以指定先前已安裝和架構的一台或多台內部 LiveUpdate 伺服器。 您不應該將 Symantec Endpoint Protection Manager 與內部 LiveUpdate 伺服器安裝在同一個實體硬體或虛擬機器上。安裝在同一台電腦上可能導致重大的伺服器效能問題。 如果您決定使用一台或多台內部 LiveUpdate 伺服器,則可能要將賽門鐵克公共 LiveUpdate 伺服器新增為最後一個項目。如果您的用戶端無法連線清單上的任何伺服器,它們仍可從 Symantec LiveUpdate 伺服器進行更新。 若要繼續使用內部 LiveUpdate 伺服器,您應升級至最新版 LiveUpdate Administrator。請參閱： • 下載 LiveUpdate Administrator • 架構用戶端從外部 LiveUpdate 伺服器下載內容 • 將用戶端架構為從內部 LiveUpdate 伺服器下載內容 • 選擇派送方法以更新用戶端上的內容
站台要儲存多少內容修訂？	管理伺服器僅儲存最近的完整內容套件,以及您在此處所指定數目的修訂的增量差異。這種方法可減少在伺服器上儲存多個內容修訂所需的磁碟空間。 您在安裝 Symantec Endpoint Protection Manager 期間選取的用戶端數目將定義伺服器儲存的修訂數目。 對於每個 LiveUpdate 內容類型,預設值如下： • 如果您不勾選「管理伺服器將管理少於 500 個用戶端」, Symantec Endpoint Protection Manager 將儲存 21 個修訂。 • 如果您勾選「管理伺服器將管理少於 500 個用戶端」, Symantec Endpoint Protection Manager 將儲存 90 個修訂。 在升級期間的大部分實例中,安裝會增加修訂數目以符合這些新預設值。如果您在升級之前擁有的修訂數目少於新的最小預設值 (根據上述準則),則會發生這種增加的情況。請參閱： 還原為舊版 Symantec Endpoint Protection 安全更新
站台檢查 LiveUpdate 內容更新的頻率為何？	讓 Symantec Endpoint Protection Manager 每四小時執行一次 LiveUpdate 的預設排程是最佳實務準則。
我將下載哪些作業系統的內容？	LiveUpdate 僅下載適用於指定作業系統的內容。
可下載至站台和用戶端的內容類型有哪些？	請確定站台可下載用戶端 LiveUpdate 內容政策中指定的所有內容更新。請參閱： • 關於 LiveUpdate 下載的內容類型 • 還原為舊版 Symantec Endpoint Protection 安全更新
應該為產品更新下載哪些語言？	這個設定僅套用於產品更新；會自動下載所有語言的內容更新。
應該為定義檔下載哪些內容大小？	標準和內嵌/VDI 用戶端使用啟用雲端的縮減大小定義檔集 (僅限最新)。這些用戶端上的掃描會自動使用在雲端的延伸定義檔集。 暗網用戶端會下載整個定義檔集。 Warning! 管理伺服器必須為您網路中的用戶端類型下載正確內容。如果管理伺服器不下載已安裝用戶端所需的內容,用戶端將無法從管理伺服器取得更新。
應在發布引擎更新之前測試這些更新？	若為大型組織,您應該先測試新引擎更新和定義檔,然後將其遞送到所有用戶端電腦。您想要以最少的中斷次數和停機時間測試新引擎更新。請參閱： 在 Windows 用戶端上發布之前測試引擎更新

將 **LiveUpdate** 伺服器中的內容下載至 **Symantec Endpoint Protection Manager**

將內容下載至管理伺服器時,可以針對站台內所有管理伺服器進行下載。

架構站台以下載內容

1. 在主控台中，按一下「管理員」>「伺服器」。
 2. 在「伺服器」下方，於「本機網站」上按下滑鼠右鍵，然後按下「編輯網站屬性」。
 3. 在 **LiveUpdate** 標籤上，從下列可用選項中進行選擇。
 4. 在「**LiveUpdate** 來源伺服器」下方，按下「編輯來源伺服器」，然後檢查目前用於更新管理伺服器的 LiveUpdate 伺服器。此伺服器預設為 Symantec LiveUpdate 伺服器。然後執行下列其中一個動作：
 - 若要使用現有的 LiveUpdate 來源伺服器，按下「確定」。
 - 若要使用內部 LiveUpdate 伺服器，請按下「使用指定的內部 **LiveUpdate** 伺服器」，然後按下「新增」。如果已選取「使用指定的內部 **LiveUpdate** 伺服器」，請在「新增 **LiveUpdate** 伺服器」對話方塊中填寫可識別 LiveUpdate 伺服器的資訊，然後按下「確定」。
- 出於容錯移轉目的，您可以新增多台伺服器。如果一個伺服器離線，其他伺服器會提供支援。您還可以將賽門鐵克公共 LiveUpdate 伺服器新增為清單中的最後一台伺服器。如果新增公共伺服器，請使用 URL <http://liveupdate.symantecliveupdate.com>。

NOTE

如果使用 UNC 伺服器，則 LiveUpdate 會要求您在使用者名稱中使用網域或工作群組。

如果電腦是在網域中，請使用格式 domain_name\user_name。

如果電腦是在工作群組中，請使用格式 computer_name\user_name。

- 在「**LiveUpdate** 伺服器」對話方塊中，按下「確定」。
5. 在「用於下載的磁碟空間管理」下方，輸入要保留的 LiveUpdate 內容修訂號碼。
 6. 在「下載排程」群組方塊中，按下「編輯排程」，設定伺服器應檢查更新頻率的選項。按下「確定」。
 7. 在「要下載的平台」下方，按下「變更平台」，然後檢查平台清單。取消核取您不想將內容下載到哪些平台。
 8. 在「要下載的內容類型」下方，檢查已下載的更新類型清單。

若要新增或刪除更新類型，請按下「變更選定內容」、修改清單，然後按下「確定」。

此清單應與包含在用戶端電腦的 LiveUpdate 內容政策中的內容類型清單相符合。
 9. 在「要為用戶端類型下載的內容」下方，決定要為標準和內嵌式/VDI 用戶端還是暗網用戶端下載和儲存內容。

WARNING

您必須為網路中的用戶端類型下載內容。如果沒有下載已安裝的用戶端所需的內容，則用戶端無法從管理伺服器取得更新。

- 若要修改設定，請按下「變更選定內容」，修改選定內容，然後按下「確定」。
10. 在「要下載的語言」下方，檢查已下載更新類型的語言清單。

若要新增或刪除語言，按下「變更選定內容」，修改清單，然後按下「確定」。
 11. 按下「確定」以儲存您的選定內容並關閉視窗。

更多資訊

[如何更新用戶端上的內容和定義檔](#)

確認 Symantec Endpoint Protection Manager 具有最新內容

LiveUpdate 會按排程將定義檔和其他內容下載至 Symantec Endpoint Protection Manager。但是，如果 Symantec Endpoint Protection Manager 沒有最新版本，您可以隨時下載內容。然後 Symantec Endpoint Protection Manager 會透過預設的 LiveUpdate 政策提供此內容給用戶端電腦。

確認 Symantec Endpoint Protection Manager 具有最新內容

-
1. 在主控台上，按下「首頁」。
 2. 在「端點狀態」群組方塊中的「**Windows 定義檔**」下，比較「管理程式最新定義檔」以及「**Symantec 最新定義檔**」的日期。
 3. 如果日期不相符，請按下「管理員」>「伺服器」>「本機站台 (我的站台)」。
 4. 在「工作」下方，按下「下載 **LiveUpdate** 內容」>「下載」。

如果您無法透過 LiveUpdate 更新 Symantec Endpoint Protection Manager 上的內容，則可以從賽門鐵克安全機制應變中心下載 .jdb 檔案。Symantec Endpoint Protection Manager 會處理這些檔案的內容，並使其可供用戶端下載。請參閱：

[下載 .jdb 檔案以更新 Endpoint Protection Manager 的定義檔](#)

將內容從 **LiveUpdate** 下載至 時檢查 **Symantec Endpoint Protection Manager**

您可以確定內容在 LiveUpdate 中的 Symantec Endpoint Protection Manager 上的最近更新日期和時間。

檢查從 **LiveUpdate** 下載到 **Symantec Endpoint Protection Manager** 的內容

1. 在主控台中，按下「管理員」。
2. 在「管理員」頁面的「工作」下，按下「伺服器」，然後選取相應站台。
3. 執行下列其中一項工作：
 - 若要檢查下載狀態，請按下「顯示 **LiveUpdate** 狀態」。
 - 若要檢查 Symantec Endpoint Protection Manager 所使用的目前內容版本，請按下「顯示 **LiveUpdate** 狀態」。
4. 按下「關閉」。

更多資訊

- [疑難排解 Endpoint Protection Manager 的 LiveUpdate 和定義檔問題](#)
- [將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)

關於 **LiveUpdate** 下載的內容類型

依據預設，Symantec Endpoint Protection Manager 會從公用 Symantec LiveUpdate 伺服器下載所有類型的內容。然後，LiveUpdate 內容政策會從 Symantec Endpoint Protection Manager 將所有類型的內容下載至 Windows 和 Mac 用戶端。

如果您從網站排除某個內容類型，但從 LiveUpdate 內容政策移除此內容，則此內容不會傳送至用戶端。通常，不需要排除 Symantec Endpoint Protection Manager 下載的內容。如果不確定是否需要，請不要排除某個類型的內容。

請參閱：[還原至舊版 Symantec Endpoint Protection 安全更新](#)

LiveUpdate 不會下載已更新的政策。指派新政策給群組或編輯現有政策時，Symantec Endpoint Protection Manager 會將政策更新至用戶端。

Table 147: 可從 LiveUpdate 下載到 Symantec Endpoint Protection Manager 的內容類型

內容類型	說明
用戶端產品更新	包含 Windows 用戶端安全性漏洞的軟體改進和重要修正。例如，攻擊者可能會略過 Symantec Endpoint Protection 防護功能。 LiveUpdate 會將產品更新下載為 RUx 發行之間的完整用戶端安裝套件。每個套件的版次號碼都會相同，但具有更新過的建立號碼。例如，第一個用戶端安裝套件可能會標示為 14.3.4555.2000，第二個則標示為 14.3.5228.1000。啟用此選項時，最新的過渡期套件會出現在「版本選取項目」下拉式清單中的下列位置： - 自動升級精靈：在「管理」頁面 > 「安裝套件」頁面 > 用戶端安裝套件 > 使用套件升級用戶端 > 「升級設定」選項 > 「一般」標籤。自動升級精靈只會顯示最新的版本。 - 新套件：在「用戶端」頁面 > 「安裝套件」標籤 > 新增用戶端安裝套件 > 「一般」標籤。 此選項不會升級本身為新版本且具有主要功能的用戶端安裝套件，如 14.3 RU2 到 14.3 RU3。您仍然必須使用自動升級或是透過 Broadcom「下載管理」頁面手動下載和安裝完整用戶端安裝套件，才能進行升級。 若要更新 Mac 和 Linux 用戶端，您必須使用「用戶端部署精靈」中的「網路連結與電子郵件」和「儲存套件」選項。 在 14.3 RU1 MP1 和更舊版本中，如果未使用此選項，則請將此設定保持取消勾選狀態。請參閱： 升級至新版本 使用自動升級來升級用戶端軟體
用戶端修補程式	包括與產品更新相同的用戶端軟體改進和安全修正，但是這些修補程式是作為增量差異檔案 (.dax) 進行下載，而非完整用戶端安裝套件。 若要將內容下載至用戶端，請前往「LiveUpdate 設定」政策 > 「其他設定」標籤，然後勾選「下載用戶端修補程式」。此選項可讓您將來自 LiveUpdate、管理伺服器或群組更新提供者的用戶端修補程式更新到用戶端。 此選項重新命名自 14.3 RU2 中的「用戶端安全修補程式」。
病毒和間諜軟體定義檔	x86 及 x64 平台分別有適用的病毒定義套件。此內容類型也包括自動防護入口網站清單以及 Power Eraser 定義檔。
SONAR 啟發式特徵	防範零時差攻擊的威脅。
入侵預防特徵	防範網路威脅和主機漏洞。支援入侵預防、偵測引擎和記憶體攻擊緩和。
主機完整性內容	包括預先定義需求的範本，這些範本會強制在用戶端電腦上執行更新的修正程式與安全措施。LiveUpdate 會針對執行 Windows 作業系統和 Mac 作業系統的電腦下載範本。請參閱： 從範本新增自訂需求
傳送控制特徵	控制傳送至賽門鐵克安全機制應變中心的流程。
信譽設定	包含對用於防護的信譽資料的更新。
延伸檔案屬性和特徵	用於使更新憑證和下載鑑識更加受到資料驅動。這些資料驅動的下載有助於賽門鐵克使用定義檔式更新來更新信任的特徵清單。
端點偵測和回應	Endpoint Detection and Response (EDR) 元件的更新，用於偵測和調查可疑活動及主機與端點上的問題。EDR 會提供此蒐證資訊給各種產品元件，包括提交和 EDR 伺服器。已在第 14 版中新增。請參閱： 適用於 14 RU1 和更新用戶端的 Endpoint Detection and Response 引擎更新
通用網路傳輸程式庫和組態	整個產品用以接收網路傳輸和遙測的定義檔。這些定義檔是信譽查詢以及提交和與 EDR 通訊所必需的定義檔。此類別中的定義檔包括 SEPM STIC 和 SEPC STIC，分別用於 Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端。
進階機器學習	定義檔供使用低頻寬政策的用戶端用於病毒和間諜軟體掃描。對具有慢速 Internet 連線網路的標準用戶端和內嵌用戶端使用低頻寬模式。在低頻寬模式中，LiveUpdate 會每週下載一次定義檔或以更不頻繁的頻率下載。若要使用低頻寬模式，您必須註冊使用雲端並啟用「低頻寬」政策。暗網用戶端無法使用低頻寬模式。 如果您不在雲端主控台中註冊管理伺服器，或不要使用低頻寬政策，請停用此選項以節省部分頻寬和 Symantec Endpoint Protection Manager 上的磁碟空間。請參閱： 在低頻寬環境中更新用戶端
Web 和雲端存取防護	來自 Symantec Cloud Secure Web Gateway (Cloud SWG) 的定義。Web 和雲端存取防護會使用 Cloud SWG 伺服器，為您的網頁瀏覽器提供安全的代理設定。

內容類型	說明
SymPlatform 定義 (SEF)	Symantec Endpoint Foundation (SEF) 是一個框架，會透過 LiveUpdate 將未來的防護技術作為內容提供。SEF 使您能夠將新功能下載到用戶端，而無需升級它們。 包括 URL 信譽 (14.3 RU1 或更新版本) 和自動防護 (14.3 RU3 或更新版本) 的定義。
應用程式控制內容	應用程式控制引擎用於應用程式控制政策的定義檔。此選項應隨時保持在啟用狀態。 此內容僅在 14.2 及更新版本的用戶端上執行。在舊版 Windows 用戶端中，您必須先將它們升級至 14.2。
政策指令處理常式	政策指令處理常式引擎使用的內容。
Endpoint Threat Defense for AD 資料	Active Directory 防禦引擎使用的內容。新增於 14.2 RU1。
瀏覽器延伸	用戶端用來攔截 Google Chrome 上惡意網站之 IPS 引擎的內容。已在 14.3 RU2 中新增。
受攻擊面縮小	用於混合管理用戶端之應用程式強化的整合元件。包括應用程式控制、自適應隔離和應用程式探索。新增於 14.3 RU5 中。

如需詳細資訊，請參閱：

[適用於 Endpoint Protection 14 的 LiveUpdate Administrator 內容選項](#)

無法在 LiveUpdate 內容政策中停用下列內容類型，其中包括「延伸檔案屬性和特徵」、「端點偵測和回應」、「通用網路傳輸程式庫和組態」。

Table 148: 功能及其需要的更新內容

安裝非受管用戶端時	更新時，您必須下載這些類型的內容
病毒和間諜軟體防護	• 病毒和間諜軟體定義檔 • SONAR 定義檔 在「站台屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 • 集中式信譽設定 在「站台屬性」中架構下載的內容類型時，這個內容類型稱為「信譽設定」。 • 撤銷資料 (依據預設下載，無法從 Symantec Endpoint Protection Manager 架構) • 賽門鐵克許可清單 (賽門鐵克白名單) • 傳送控制特徵 • 自動防護入口網站清單 • Power Eraser 定義檔 • 延伸檔案屬性和特徵 • 端點偵測和回應 • 通用網路傳輸程式庫和組態 • 進階機器學習
「病毒和間諜軟體防護」>「下載防護」	• 病毒和間諜軟體定義檔 • SONAR 定義檔 在「站台屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 • 集中式信譽設定 • 撤銷資料 • 賽門鐵克許可清單 (賽門鐵克白名單) • 入侵預防特徵 選取這個下載選項時，同時包含入侵預防特徵和入侵預防引擎的更新。 • 傳送控制特徵 • 自動防護入口網站清單 • Power Eraser 定義檔 • 延伸檔案屬性和特徵 • 端點偵測和回應 • 通用網路傳輸程式庫和組態 • 進階機器學習
「病毒和間諜軟體防護」>「Outlook 掃描程式」	• 病毒和間諜軟體定義檔 • SONAR 定義檔 在「站台屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 • 集中式信譽設定 • 撤銷資料 • 賽門鐵克許可清單 (賽門鐵克白名單) • 傳送控制特徵 • 自動防護入口網站清單 • Power Eraser 定義檔 • 延伸檔案屬性和特徵 • 端點偵測和回應 • 通用網路傳輸程式庫和組態 • 進階機器學習

安裝非受管用戶端時	更新時，您必須下載這些類型的內容
「病毒和間諜軟體防護」>「Notes 掃描程式」	• 病毒和間諜軟體定義檔 • SONAR 定義檔 在「站台屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 • 集中式信譽設定 • 撤銷資料 • 賽門鐵克許可清單 (賽門鐵克白名單) • 傳送控制特徵 • 自動防護入口網站清單 • Power Eraser 定義檔 • 延伸檔案屬性和特徵 • 端點偵測和回應 • 通用網路傳輸程式庫和組態 • 進階機器學習
「主動型威脅防護」> SONAR	SONAR 定義檔 傳送控制特徵 延伸檔案屬性和特徵 進階機器學習
「主動型威脅防護」>「應用程式控制」	傳送控制特徵 延伸檔案屬性和特徵 應用程式控制內容
Web 和雲端存取防護政策	Web 和雲端存取防護
「防網路和主機侵入」>「入侵預防」	• 入侵預防特徵 選取這個下載選項時，同時包含入侵預防特徵和入侵預防引擎的更新。 • 傳送控制特徵 • 延伸檔案屬性和特徵 • 瀏覽器延伸 (自 14.3 RU2 開始)
「防網路和主機侵入」>「防火牆」	傳送控制特徵 延伸檔案屬性和特徵
主機完整性	主機完整性內容 傳送控制特徵 延伸檔案屬性和特徵

更多資訊

- [將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)
- [如何更新用戶端上的內容和定義檔](#)
- [選擇派送方法以更新用戶端上的內容](#)

將用戶端架構為從內部 LiveUpdate 伺服器下載內容

依據預設，Windows 用戶端將從管理伺服器取得其更新。

NOTE

對於 Mac 和 Linux 用戶端，您需要架構管理伺服器字作為反向代理，或者需要使用 LiveUpdate Administrator。

[使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容](#)

如果您管理大量的用戶端，您可能希望對 Windows 用戶端使用「群組更新提供者」(GUP)。GUP 會減輕管理伺服器的負載而且比內部 LiveUpdate 伺服器容易設定。請參閱：

[使用群組更新提供者將內容散佈至用戶端](#)

如果您不想使用預設管理伺服器或「群組更新提供者」進行用戶端更新,則可以:

- 設定內部 LiveUpdate 伺服器。
- 使用位於網路外部的 Symantec LiveUpdate 伺服器。

若要使用內部 LiveUpdate 伺服器,您必須執行下列工作:

- 安裝內部 LiveUpdate 伺服器。
如需使用內部 LiveUpdate 伺服器的詳細資訊,請參閱「*LiveUpdate 管理指南*」。

NOTE

Symantec Endpoint Protection Manager 不再包括 LiveUpdate Administrator 1.x 舊版支援。若要繼續使用內部 LiveUpdate 伺服器,您應升級至最新版 LiveUpdate Administrator。對 LiveUpdate Administrator 2.x 和更新版本的支援始終處於啟用狀態。

- 使用 LiveUpdate 設定政策將您的用戶端架構為使用該內部 LiveUpdate 伺服器。

NOTE

您可以為連線至內部 LiveUpdate 伺服器以檢查更新的用戶端指定 Proxy 設定。代理設定僅適用於更新,不適用於用戶端使用的其他外部通訊類型。您必須另外為其他類型的用戶端外部通訊架構代理。請參閱:

[指定用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器](#)

將 **Windows** 用戶端架構為使用內部 **LiveUpdate** 伺服器:

1. 在「政策」下方,按一下 **LiveUpdate**。
2. 在「**LiveUpdate** 設定」標籤上,開啟您要編輯的政策。
3. 在「**Windows** 設定」下方,按一下「伺服器設定」。
4. 在「伺服器設定」窗格中,勾選「使用 **LiveUpdate** 伺服器」。
5. 按一下「使用指定的內部 **LiveUpdate** 伺服器」,然後按一下「新增」。
6. 在「新增 **LiveUpdate** 伺服器」對話方塊中,輸入識別所要使用的伺服器並與之通訊所需的資訊。

對於 **URL**:

- 您可以使用 HTTP 或 HTTPS 方法。輸入伺服器的 URL。例如:網域名稱: <http://myliveupdateserver.com>
 - IPv4 位址: <http://192.168.133.11:7070/clu-prod>
 - IPv6 位址: [http://\[fd00:fe32::b008\]:7070/clu-prod](http://[fd00:fe32::b008]:7070/clu-prod)

NOTE

14.3 RU1 已移除對 FTP 方法或 UNC 方法的支援。在更舊版本中:

- 如果您使用的是 FTP 方法,請輸入伺服器的 FTP 位址。例如: <ftp://myliveupdateserver.com>
- 如果您使用的是 LAN 方法,請輸入伺服器的 UNC 路徑名稱。例如: <\\myliveupdateserver\LUDepot>

7. 如果需要,請輸入伺服器的使用者名稱和密碼,然後按一下「確定」。

NOTE

如果您使用 UNC 伺服器,則 LiveUpdate 會要求除使用者名稱之外,還要使用網域或工作群組。如果電腦是網域的一部分,請使用格式 `domain_name\user_name`。如果電腦是工作群組的一部分,請使用格式 `computer_name\user_name`。

8. 在「**LiveUpdate** 政策」下方,按一下「排程」透過 LiveUpdate 為更新設定排程,然後按一下「確定」。請參閱:
[針對用戶端電腦架構 LiveUpdate 下載排程](#)
9. 選擇性地按一下「進階設定」。
決定要保留還是變更預設的使用者設定、產品更新設定和非標準標頭設定。一般來說,您不希望讓使用者修改更新設定。但是,如果用戶端太多而無法支援,您不妨讓使用者手動啟動 LiveUpdate 階段作業。請參閱:
[架構使用者對 LiveUpdate 的控制能力](#)
10. 按一下「確定」。

將 **Mac** 用戶端或 **Linux** 用戶端架構為使用內部 **LiveUpdate** 伺服器:

1. 在「政策」頁面上,按一下 **LiveUpdate**。

-
2. 在「**LiveUpdate 設定**」標籤上，開啟政策。
 3. 在「**Mac 設定**」或「**Linux 設定**」下方，按一下「伺服器設定」。
 4. 按一下「使用指定的內部 **LiveUpdate** 伺服器」，然後按一下「新增」。
 5. 在「新增 **LiveUpdate** 伺服器」對話方塊中，輸入識別所要使用的伺服器並與之通訊所需的資訊。

對於 **URL**：

- 您可以使用 HTTP 或 HTTPS 方法。輸入伺服器的 URL。例如：網域名稱：http://myliveupdateserver.com
 - IPv4 位址：http://192.168.133.11:7070/clu-prod
 - IPv6 位址：http://[fd00:fe32::b008]:7070/clu-prod

NOTE

14.3 RU1 已移除對 FTP 方法或 UNC 方法的支援。

6. 如果需要，請輸入伺服器的使用者名稱和密碼，然後按一下「確定」。
7. 如果您的伺服器使用 FTP，則請按一下「進階伺服器設定」，並按一下伺服器使用的 FTP 模式（「主動」或「被動」），然後按一下「確定」。
8. 若要修改排程，請按一下「排程」。
9. 按一下「確定」。

更多資訊

- [從 LiveUpdate 伺服器隨機進行內容下載](#)
- [將 Windows 用戶端更新架構為在用戶端電腦閒置時執行](#)
- [選擇派送方法以更新用戶端上的內容](#)

架構用戶端從外部 **LiveUpdate** 伺服器下載內容

依預設，Symantec Endpoint Protection Manager 會為 Windows 用戶端提供更新。為了協助降低 Windows 用戶端更新的網路負載，您還應讓用戶端從 LiveUpdate 伺服器取得更新。Linux 和 Mac 用戶端必須從 LiveUpdate 伺服器取得更新，或者您可以將 Apache Web 伺服器設為反向代理來從管理伺服器下載更新。請參閱：

- [選擇派送方法以更新用戶端上的內容](#)
- [使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容](#)

NOTE

您可能需要建立代理伺服器與 Symantec Endpoint Protection Manager 之間的通訊，以便它可以連線至賽門鐵克訂購授權服務。代理伺服器可以在您的站台和外部 Symantec LiveUpdate 伺服器之間提供多一層的保護。請參閱：

[架構 Symantec Endpoint Protection Manager 連線到代理伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容](#)

架構用戶端從外部 **LiveUpdate** 伺服器下載內容

1. 在主控台中，開啟 LiveUpdate 政策，然後按下「編輯」。
2. 在「**Windows 設定**」、「**Mac 設定**」或「**Linux 設定**」下方，按一下「伺服器設定」。
3. 按一下「使用預設 **Symantec LiveUpdate** 伺服器」，或指定另一台 LiveUpdate 伺服器。如有需要，請指定 Proxy 架構。
4. 按一下「確定」。

更多資訊

[如何更新用戶端上的內容和定義檔](#)

架構 Symantec Endpoint Protection Manager 連線到 Proxy 伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容

您可以將 Symantec Endpoint Protection Manager 架構為通過代理伺服器以連線至 Internet。Proxy 伺服器可以增加一層安全性，原因是只有 Proxy 伺服器直接連線到 Internet。

架構 Symantec Endpoint Protection Manager 連線到代理伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容

1. 在主控台中，按下「管理員」，再按「伺服器」。
2. 在「伺服器」下，選取您要將 Proxy 伺服器連接至的管理伺服器。
3. 在「工作」下方，按一下「編輯伺服器屬性」。
4. 在「Proxy 伺服器」標籤的「HTTP Proxy 設定」或「FTP Proxy 設定」下，為「Proxy 使用」選取「使用自訂 Proxy 設定」。
5. 鍵入 Proxy 設定。
如需這些設定的詳細資訊，請按一下「說明」。
6. 按下「確定」。

更多資訊

[指定用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器](#)

指定用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器

您可以指定用戶端用來與內部 LiveUpdate 伺服器通訊的 Proxy 伺服器。Proxy 設定不會影響群組更新提供者的任何設定。

NOTE

其他用戶端通訊的 Proxy 設定則需另行架構。

指定 Windows 電腦或 Linux 電腦用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的 Proxy 伺服器

1. 在主控台中，按下「政策」。
2. 在「政策」下方，按下 **LiveUpdate**，然後按下「LiveUpdate 設定」標籤。
3. 在所需的政策上按下滑鼠右鍵，再選取「編輯」。
4. 在「Windows 設定」下或「Linux 設定」下，按下「伺服器設定」。
5. 在「LiveUpdate Proxy 架構」下方，按下「架構 Proxy 選項」。
6. 執行下列其中一個動作：
 - 對於 Windows 用戶端，在「HTTP 或 HTTPS」標籤上，選取所需的選項。還可以指定 FTP 的 Proxy 設定。
 - 對於 Linux 用戶端，在 HTTP 標籤上，選取所需的選項。如需這些選項的詳細資訊，請參閱線上說明。
7. 按下對話方塊中的「確定」。
8. 按下「確定」。

指定 Mac 電腦用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器

1. 在主控台中，按下「用戶端 > 政策」。
2. 在「與位置無關的政策與設定」下方的「設定」下，按下「外部通訊設定」。
3. 在「代理伺服器 (Mac)」標籤上，選取所需的選項。
4. 按下「確定」。

更多資訊

[如何更新用戶端上的內容和定義檔](#)

針對用戶端電腦架構 LiveUpdate 下載排程

LiveUpdate 用戶端排程設定在「LiveUpdate 設定」政策中進行定義。這些設定會套用至 LiveUpdate 階段作業，以從 Symantec LiveUpdate 伺服器或內部 LiveUpdate 伺服器取得最新的更新。請參閱：

- [架構用戶端從外部 LiveUpdate 伺服器下載內容](#)
- [將用戶端架構為從內部 LiveUpdate 伺服器下載內容](#)

若要儲存頻寬，您可以讓您的用戶端只在符合下列任一條件時執行排定的 LiveUpdate 階段作業：

- 用戶端電腦上的病毒和間諜軟體定義檔已超過 2 天。
- 用戶端電腦與 Symantec Endpoint Protection Manager 中斷連線已超過 8 小時。

NOTE

若要確保任何不常與您的網路連線的用戶端電腦取得最新的更新，請讓這些電腦從 Symantec LiveUpdate 伺服器取得更新。這些伺服器是公用的，因此用戶端不根據與您的網路連線來取得更新。

架構 LiveUpdate 下載至 Windows 用戶端電腦的排程

1. 按一下「政策」，然後按一下 **LiveUpdate**。
2. 在「**LiveUpdate 設定**」標籤上，以滑鼠右鍵按一下所需的政策，然後按一下「編輯」。
3. 在「**Windows 設定**」下方，按一下「排程」。
4. 確認已勾選「啟用 **LiveUpdate** 排程」。此選項預設為啟用。

NOTE

您不應取消勾選此方塊。如果您停用「**LiveUpdate** 排程」，用戶端不會取得最新更新。

5. 指定頻率。
如果選取「每日」，請同時設定要執行的時間。如果選取「每週」，請同時設定要在星期幾和哪個時間執行。
6. 如果選取「連續」之外的任何頻率，請指定「重試時段」。
「重試時段」是當排程的 LiveUpdate 因故失敗時，用戶端電腦嘗試執行 LiveUpdate 的小時數或天數。
7. 請視需要設定任何其他選項。如果定義檔已過期，或是用戶端最近未連線至管理伺服器，賽門鐵克建議您保留執行 LiveUpdate 的預設值。
8. 按一下「確定」。
[從 LiveUpdate 伺服器隨機進行內容下載](#)

架構 LiveUpdate 下載至 Mac 用戶端電腦的排程

1. 按一下「政策」，然後按一下 **LiveUpdate**。
2. 在「**LiveUpdate 設定政策**」標籤上，以滑鼠右鍵按一下所要的政策，然後按一下「編輯」。
3. 在「**Mac 設定**」下方，按一下「排程」。
4. 指定頻率。
如果選取「每日」，請同時設定要執行的時間。如果選取「每週」，請同時設定要在星期幾和哪個時間執行。
5. 完成後，請按一下「確定」。

架構 LiveUpdate 下載至 Linux 用戶端電腦的排程

1. 在「**LiveUpdate 設定政策**」標籤上，以滑鼠右鍵按一下所要的政策，然後按一下「編輯」。
2. 在「**Linux 設定**」下方，按一下「排程」。
3. 指定頻率。
如果選取「每日」，請同時設定要執行的時間。如果選取「每週」，請同時設定要在星期幾和哪個時間執行。

您也可以隨機進行內容下載。

4. 按一下「確定」。

更多資訊

[如何更新用戶端上的內容和定義檔](#)

架構使用者對 LiveUpdate 的控制能力

您可能想要讓出差的使用者可以使用 Internet 連線，直接從 Symantec LiveUpdate 伺服器取得更新。您也可以讓使用者修改您為內容下載設定的 LiveUpdate 排程。

NOTE

如果未受管用戶端具有在建立安裝套件時向其指派的 LiveUpdate 設定政策，則 SEPM 政策設定一律會優先於使用者的變更。若要安裝未受管用戶端，以優先採用使用者的變更，則請從安裝檔案安裝用戶端。

架構使用者對 LiveUpdate 的控制能力

1. 在主控台中，按下「政策」。
2. 在「政策」下方，按一下 **LiveUpdate**。
3. 在「**LiveUpdate** 設定」標籤上，以滑鼠右鍵按一下所需的政策，然後按一下「編輯」。
4. 在「**Windows** 設定」下方，按一下「進階設定」。
5. 在「使用者設定值」窗格下方，勾選「允許使用者手動啟動 **LiveUpdate**」。
6. 您也可以勾選「允許使用者修改 **LiveUpdate** 排程」。
7. 按下「確定」。

更多資訊

- [還原為舊版 Symantec Endpoint Protection 安全更新](#)
- [針對用戶端電腦架構 LiveUpdate 下載排程](#)

減少用戶端更新要求的網路超載

當有過多用戶端同時從管理伺服器或「群組更新提供者」要求一組完整的病毒和間諜軟體定義檔時，您必須針對這種重大但不常見的情況管理網路。如果管理伺服器發生錯誤或磁碟空間不足，以致用戶端上的下載和更新定義檔失敗，就可能發生這種情況。如果管理伺服器不下載定義檔套件，然後用戶端要求此特定差異，也可能會發生此情況。不論是哪種情況，用戶端接著都必須從管理伺服器或「群組更新提供者」要求包含一組完整定義檔的套件。

為了協助防止網路超載，管理伺服器提供下列功能：

- 當管理伺服器在指定期間內收到對一組完整定義檔提出的指定數目要求時，會發出通知。
您可以根據造成環境超載的原因，設定此通知的條件。若要架構通知，請新增「網路負載：病毒和間諜軟體完整定義檔的要求」通知條件。請參閱：
[設定管理員通知](#)
- 在管理伺服器只能提供一組完整定義檔的情況下，讓用戶端能夠從 LiveUpdate 伺服器取得病毒和間諜軟體定義檔的差異。在 LiveUpdate 設定政策中，按下「進階設定」>「從可用的 **LiveUpdate** 伺服器下載差異內容」。
此選項已重新命名自 14.3 RU2 中的「在可用時從 **LiveUpdate** 伺服器下載較小的用戶端安裝套件」。
- 攔截用戶端，使其無法從管理伺服器下載一組完整的病毒和間諜軟體定義檔。
如果您收到網路超載的通知，可以攔截任何從管理伺服器進一步下載完整套件的動作。但是，您無法停止任何已在進行中的下載作業。架構此選項，方法為按下「管理員」>「伺服器」> server_name >「編輯伺服器屬性」>「完整定義檔下載」>「防止用戶端下載完整定義檔套件」。請參閱：
[完整定義檔下載](#)

關於隨機進行同時內容下載

Symantec Endpoint Protection Manager 支援從預設管理伺服器或「群組更新提供者」，隨機將內容同時下載至您的用戶端。這也支援從 LiveUpdate 伺服器隨機將內容下載至您的用戶端。隨機化可減少尖峰網路流量，並且預設為啟動。

您可以啟用或停用隨機化功能。已啟用預設設定。您也可以架構隨機化視窗。管理伺服器會使用隨機化視窗錯開內容下載的時間。一般而言，您應該不需要變更預設的隨機化設定。

然而，在某些狀況下，可能需要提高隨機化視窗值。例如，在執行管理伺服器的相同實體電腦上，您可能在多個虛擬機器上執行 Symantec Endpoint Protection 用戶端。較高的隨機化值可以改善伺服器的效能，但是會延遲虛擬機器的內容更新。

當您有多部實體用戶端電腦連線至執行管理伺服器的單一伺服器時，也可能需要增加隨機化視窗。一般而言，用戶端與伺服器的比例愈高，可能需要設定愈多的隨機化視窗。較高的隨機化值可減少伺服器的尖峰負載，但是會延遲用戶端電腦的內容更新。

有較少用戶端且需要快速的內容傳送時，可以將隨機化視窗設定為較低的值。較低的隨機化值會增加伺服器的尖峰負載，但是可加速用戶端的內容傳送。

若是從預設管理伺服器或「群組更新提供者」進行下載，您可以在選取的群組的「通訊設定」對話方塊中架構隨機化設定。這些設定不是 LiveUpdate 設定政策的一部分。

如果是從 LiveUpdate 伺服器下載至用戶端，您可以將隨機化設定架構為 LiveUpdate 設定政策的一部分。

更多資訊

- [從預設管理伺服器或群組更新提供者隨機進行內容下載](#)
- [從 LiveUpdate 伺服器隨機進行內容下載](#)
- [將用戶端架構為從內部 LiveUpdate 伺服器下載內容](#)

從預設管理伺服器或群組更新提供者隨機進行內容下載

多個用戶端電腦嘗試同時從您的預設管理伺服器或「群組更新提供者」下載內容時，預設管理伺服器或「群組更新提供者」可能會遭遇效能下降。您可以在用戶端電腦所屬群組的通訊設定中設定隨機化時段。每台用戶端電腦會嘗試在該時段內的隨機時間下載內容。

NOTE

通訊設定不會控制用戶端電腦從 LiveUpdate 伺服器下載內容的隨機化設定。您可以在 LiveUpdate 設定政策中變更這些電腦的隨機化設定。請參閱：

[從 LiveUpdate 伺服器隨機進行內容下載](#)

從預設管理伺服器或群組更新提供者隨機進行內容下載

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」下方，按下您所要的群組。
3. 在「政策」標籤的「與位置無關的政策與設定」下方，按下「設定」下方的「通訊設定」。
4. 在「通訊設定」對話方塊的「下載隨機化」下方，勾選「啟用隨機化」。
5. 或者，可以變更隨機化時段持續時間。
6. 按下「確定」。

更多資訊

- [關於隨機化同時內容下載](#)
- [將用戶端架構為從內部 LiveUpdate 伺服器下載內容](#)

減少因同步 SEP 用戶端 LiveUpdate 內容下載而造成的網路壅塞

隨機化 SEP Windows 和 Linux 用戶端 LiveUpdate 內容下載的時間，以釋放網路資源。

多個 SEP Windows 和 Linux 用戶端同時執行下載時，LiveUpdate 內容下載可能會對您的網路造成負擔。架構用戶端電腦以在隨機時間排程 LiveUpdate 內容下載，以減少網路壓力。隨機化用戶端內容下載可確定用戶端在不同的時間執行 LiveUpdate 內容下載，以釋放網路資源。

NOTE

對於從預設管理伺服器或群組更新提供者下載內容的用戶端電腦 LiveUpdate 政策排程設定未控制隨機化。您可以在這些電腦所屬群組的「通訊設定」對話方塊中變更這些電腦的隨機化設定。請參閱：

[從預設管理伺服器或群組更新提供者隨機進行內容下載](#)

從 **LiveUpdate** 伺服器隨機進行內容下載

1. 按下「政策」。
2. 在「政策」下方，按一下 **LiveUpdate**。
3. 在「**LiveUpdate** 設定」標籤上，以滑鼠右鍵按一下要編輯的政策，然後按一下「編輯」。
4. 在「**Windows** 設定」、「**Mac** 設定」或「**Linux** 設定」下方，按下「排程」。
5. 在「下載隨機化選項」下方，勾選「隨機設定開始時間為 + 或 - (小時)」。

NOTE

如果您選取「每週」更新，則此設定以天為單位。

6. 或者，可以變更隨機開始時間的持續時間。
7. 按下「確定」。

更多資訊

- [關於隨機化同時內容下載](#)
- [將用戶端架構為從內部 LiveUpdate 伺服器下載內容](#)

將 Windows 用戶端更新架構為在用戶端電腦閒置時執行

為緩和 Windows 用戶端電腦效能問題，您可以架構內容下載在用戶端電腦閒置時執行。此設定預設為開啟。會以使用者、CPU 和磁碟動作等數個條件，判斷電腦何時處於閒置狀態。

如果已啟用「閒置偵測」，則應進行特定更新時，下列狀況可能會延遲工作階段：

- 使用者並未處於閒置狀態。
- 電腦使用電池電力。
- CPU 處於忙碌狀態。
- 磁碟輸入/輸出處於忙碌狀態。
- 沒有網路連線。

一小時後，該攔截設定會變為只有 CPU 忙碌、磁碟輸入/輸出忙碌，或沒有網路連線等狀況會延遲更新。當排程的更新逾期兩個小時後，不論閒置狀態為何，只要有網路連線，就會執行排程的 LiveUpdate。

將 **Windows** 用戶端更新架構為在用戶端電腦閒置時執行

-
1. 按一下「政策」。
 2. 在「政策」下方，按一下 **LiveUpdate**。
 3. 在「**LiveUpdate** 設定」標籤上，以滑鼠右鍵按一下要編輯的政策，然後按一下「編輯」。
 4. 在「**Windows** 設定」下方，按一下「排程」。
 5. 勾選「延遲排程的 LiveUpdate，直到電腦變成閒置為止。逾期階段作業將無條件執行」。
 6. 按下「確定」。

更多資訊

- [針對用戶端電腦架構 LiveUpdate 下載排程](#)
- [將 Windows 用戶端更新架構為在定義檔太舊或電腦已中斷連線時執行](#)

將 Windows 用戶端更新架構為在定義檔太舊或電腦已中斷連線時執行

您可以確保 Windows 用戶端在定義檔太舊或電腦於一段指定時間內中斷網路連線時進行更新。

NOTE

如果同時勾選兩個可用的選項，則用戶端電腦必須同時符合兩個條件。

架構 **Windows** 用戶端在定義檔太舊或電腦與管理程式中斷連線時進行更新

1. 按一下「政策」。
2. 在「政策」下方，按一下 **LiveUpdate**。
3. 在「**LiveUpdate** 設定」標籤上，以滑鼠右鍵按一下要編輯的政策，然後按一下「編輯」。
4. 在「**Windows** 設定」下方，按一下「排程」。
5. 勾選「只有在病毒和間諜軟體定義檔的時間早於以下時間時才執行 **LiveUpdate:**」，然後設定小時數或天數。
6. 勾選「只有在用戶端與 **Symantec Endpoint Protection Manager** 中斷的時間超過以下時間時才執行 **LiveUpdate:**」，然後設定分鐘數或小時數。
7. 按下「確定」。

更多資訊

- [針對用戶端電腦架構 LiveUpdate 下載排程](#)
- [將 Windows 用戶端更新架構為在用戶端電腦閒置時執行](#)

將用戶端架構為從 Symantec Endpoint Protection Manager 下載內容

將內容下載至用戶端的預設方法是使用管理伺服器。

請勿定義從管理伺服器到用戶端之更新的排程。用戶端根據通訊模式和活動記號頻率從管理伺服器下載內容。

將用戶端架構為從 **Symantec Endpoint Protection Manager** 下載內容

1. 在主控台中，開啟 LiveUpdate 政策，然後按下「編輯」。
2. 在「**Windows** 設定」下方，按一下「伺服器設定」。
3. 確保已勾選「使用預設管理伺服器」。
4. 按下「確定」。

更多資訊

在 Windows 用戶端上發布之前測試引擎更新

Symantec Endpoint Protection 包含多個執行其部分功能的引擎。這些引擎是二進位檔案 (.dll 或 .exe)，會隨安全性定義檔一起傳送。賽門鐵克會更新這些引擎的功能，以強化 Symantec Endpoint Protection 功能並回應新威脅。

雖然賽門鐵克每天更新病毒定義檔多次，但引擎內容按季更新。賽門鐵克使用 LiveUpdate 提供引擎更新。

賽門鐵克會提供特殊的伺服器，可讓您在將引擎內容遞送到生產環境之前下載並測試內容。賽門鐵克會在早期採用者伺服器 (EAS) 上發布這些更新。引擎更新會在引擎可供在公用 LiveUpdate 伺服器上進行一般發布之前的幾週內發布。

您可使用 EAS 下載引擎更新，在實驗室環境中加以嘗試，並告知賽門鐵克您遇到的任何衝突。此程序可讓賽門鐵克在一般發布之前修正這些衝突。

請使用下列程序來測試引擎更新。

- [步驟 1：建立一組測試電腦來接收內容](#)
- [步驟 2：將測試電腦架構為從早期採用者伺服器接收搶鮮版內容](#)
- [步驟 3：將測試和非測試電腦架構為特定引擎版本](#)
- [步驟 4：設定新引擎版本的通知 \(選擇性\)](#)
- [步驟 5：發布引擎內容後，監控測試電腦](#)

步驟 1：建立一組測試電腦來接收內容

最準確的引擎相容性測試是在實際執行工作的生產系統下進行的。透過使用下列準則選取一組用戶端電腦來接收 EAS 內容，以建立永久測試群組：

- 識別您環境內各種類型的重要系統。這些系統可能因硬體、軟體或功能而有所不同。例如，可在其他要測試的重要系統之間識別零售系統，例如金級桌面影像、銷售點系統和 Web 伺服器。
- 由於某些軟體衝突可能僅間歇性地出現，因此，請使用每種類型的多個系統。選擇已具備您通常使用且執行代表工作負載的已安裝軟體的生產系統。
- 架構用於接收較早版本內容的測試用戶端電腦，例如非測試的生產電腦。測試及非測試的兩個用戶端應安裝相同的 Symantec Endpoint Protection 功能並使用相同的政策。

如果您不希望將生產電腦用於透過 EAS 進行測試，您可以使用以實驗室為基礎的系統。在此情況下，您可能想要撰寫自動化，以在測試和模擬負載下運用系統功能。

對於用戶端電腦數量較少的客戶，您只需要一個 Symantec Endpoint Protection Manager 和一個 Windows 適用的 Symantec Endpoint Protection 用戶端。

步驟 2：將測試電腦架構為從早期採用者伺服器接收搶鮮版內容

針對測試群組，透過執行下列步驟，將 LiveUpdate 架構為從賽門鐵克早期採用者伺服器下載內容。

將站台架構為從賽門鐵克早期採用者 **LiveUpdate** 伺服器下載內容

1. 在主控台中，按一下「管理員」>「伺服器」。
2. 在「伺服器」下方，於「本機網站」上按下滑鼠右鍵，然後按下「編輯網站屬性」。
3. 在「LiveUpdate 來源伺服器」下，按下「編輯來源伺服器」。
4. 在「LiveUpdate 伺服器」對話方塊中，按下「使用 Symantec LiveUpdate 伺服器取得搶鮮版內容」，然後按下「確定」>「確定」。

將受管用戶端架構為使用搶鮮版賽門鐵克早期採用者 **LiveUpdate** 伺服器

1. 在主控台中，開啟新的 LiveUpdate 設定政策，然後按下「政策」> **LiveUpdate**。
2. 在「Windows 設定」下，按下「伺服器設定」>「使用 LiveUpdate 伺服器」>「使用 Symantec LiveUpdate 伺服器取得搶鮮版內容」。
3. 按下「確定」，然後將政策指派給測試群組。

只要您的 LiveUpdate 設定政策從 EAS 取得內容，測試用戶端就會繼續接收搶鮮版內容。

NOTE

對於非測試群組，始終對您通常使用的 LiveUpdate 伺服器架構 LiveUpdate 設定政策。在引擎可供一般發布之後，所有用戶端電腦會接收 LiveUpdate 內容，視您將用戶端電腦架構為接收此內容的方式而定。

如需詳細資訊，請參閱：

- [將用戶端架構為從內部 LiveUpdate 伺服器下載內容](#)
- [架構用戶端從外部 LiveUpdate 伺服器下載內容](#)

步驟 3：將測試和非測試電腦架構為特定引擎版本

架構多個 LiveUpdate 內容政策，以便：

- 測試群組會收到最新版本的安全性定義檔及引擎。此群組會下載所有未來的內容修訂以及其中的搶鮮版引擎。
- 非測試群組會收到現有的安全引擎版本。

您也可以鎖定引擎版本。藉由此選項，用戶端會繼續收到與特定引擎相關聯的最新安全性定義檔，而不是最新引擎版本。請參閱：

[還原為舊版 Symantec Endpoint Protection 安全更新](#)

對於通常具有搶鮮版內容的測試群組功能感到滿意之後，您可以手動選擇這些非測試群組的下一個引擎版本。

步驟 4：設定新引擎版本的通知 (選擇性)

若要取得 LiveUpdate 下載至 Symantec Endpoint Protection Manager 的計劃引擎版本的通知，請執行下列其中一項工作：

- 新增何時已將新內容下載至 Symantec Endpoint Protection Manager 的通知。新內容的通知包括新引擎版本以及安全定義檔。只有在依引擎版本指定內容修訂的一或多個 LiveUpdate 內容政策因可用引擎更新而鎖定時，您才會收到通知。若要檢視通知，請在「首頁」頁面的「安全狀態」窗格中，按下「檢視通知」。

NOTE

EAS 與定期 LiveUpdate 伺服器的更新頻率相同。如果您認為收到這些通知的頻率過高，請架構為不顯示通知。

如需詳細資訊，請參閱：

[設定管理員通知](#)

- 頂級支援客戶可以在這裡登入客戶訂閱入口網站。請參閱：
[頂級支援客戶如何註冊警示和通知](#)

步驟 5：發布引擎內容後，監控測試電腦

當賽門鐵克將引擎更新發布到 EAS 之後，開始監控架構為接收此內容的電腦。監控下列項目：

- 確認測試電腦執行搶鮮版引擎更新。請參閱：
[驗證用戶端電腦上所執行的引擎和定義檔](#)
- 開機時間、伺服器上的可用資源，及其他使用 Microsoft System Center Operations Manager 等工具的重要基礎架構。
- 在用戶端電腦上執行的應用程式，用於確保其如預期般繼續執行。
- Symantec Endpoint Protection 用戶端狀態，用於確保其仍會連線至管理伺服器且受到保護。請參閱：
[檢查用戶端是否已連線至管理伺服器且受保護](#)

此外，在修改政策後執行用戶端或執行掃描，以確保電腦如預期般運作。

如果您發現任何非預期行為，或懷疑引擎更新存在軟體衝突，請聯絡支援以取得協助。通常，如果賽門鐵克在開始進行分階段遞送之前確認存在軟體衝突，賽門鐵克會重新排程發布，並與您一起修正問題。然後，賽門鐵克會將更新的引擎重新發布至 EAS。

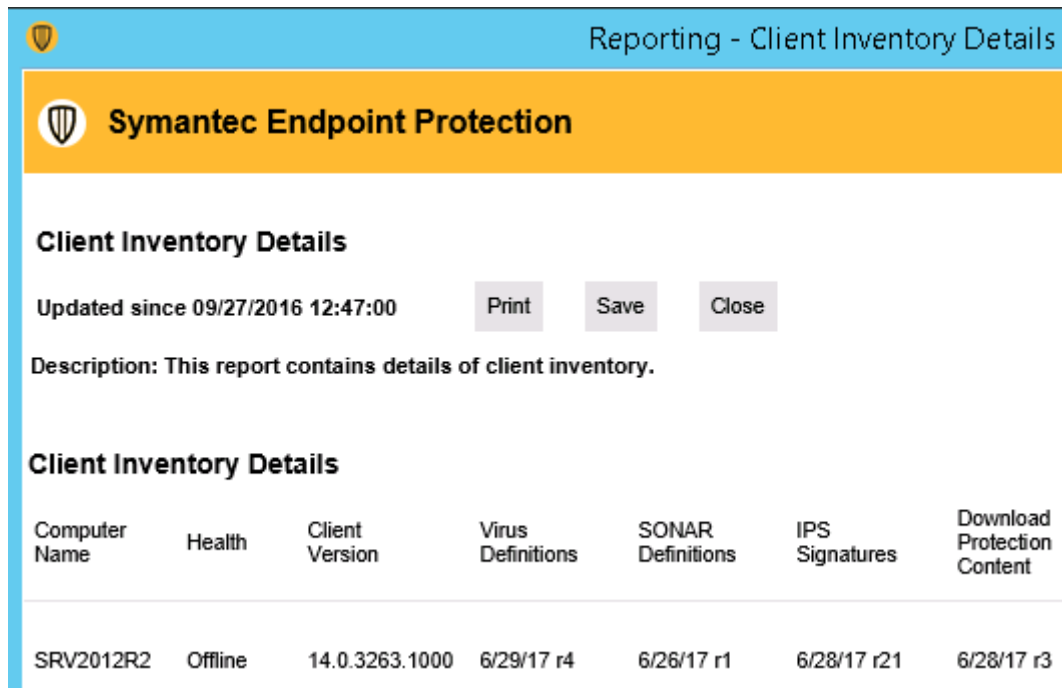
驗證用戶端電腦上所執行的引擎和定義檔

在管理伺服器 and 用戶端中，尋找用戶端執行的引擎和定義檔的版本號碼。比較包含更新引擎之內容的日期和修訂編號。您可以快速判定哪些用戶端具有新引擎，哪些用戶端仍需要更新。

確認用戶端執行的引擎版本

1. 在 Symantec Endpoint Protection Manager 主控台中，按一下「報告」>「快速報告」標籤。
2. 針對「報告類型」，選取「電腦狀態」，針對「選取報告」，按一下「用戶端清查詳細資料」。
3. 選取時間範圍，並按一下「儲存過濾器」以指定報告名稱，然後按一下「建立報告」。

此報告會顯示所有主要內容類型的定義檔日期和修訂編號。您可以視需要將此報告匯出至 .CSV 檔案。



Reporting - Client Inventory Details

Symantec Endpoint Protection

Client Inventory Details

Updated since 09/27/2016 12:47:00 [Print](#) [Save](#) [Close](#)

Description: This report contains details of client inventory.

Client Inventory Details

Computer Name	Health	Client Version	Virus Definitions	SONAR Definitions	IPS Signatures	Download Protection Content
SRV2012R2	Offline	14.0.3263.1000	6/29/17 r4	6/26/17 r1	6/28/17 r21	6/28/17 r3

4. 在用戶端上，按一下「說明」>「疑難排解」>「版本」。

您也可以使用下列方法，以確認 AV 引擎和 Eraser 引擎更新已成功套用至用戶端。請參閱：

- [如何從用戶端電腦檢查 AV 引擎、IPS 引擎和 Eraser 引擎的版本](#)
- [關於電腦狀態報告和日誌](#)

Symantec Endpoint Protection 執行的引擎有哪些？

安全機制應變中心小組會維護和更新 Endpoint Protection 引擎版本。

Symantec Endpoint Protection 會使用 Windows 用戶端上的下列引擎元件：

- **防毒引擎 (AVE)** (病毒和間諜軟體防護)
此唯一掃描引擎針對最新威脅提供以檔案為基礎的進階偵測。新版防毒引擎可能會變更 Symantec Endpoint Protection 使用的已分頁集區記憶體數量。引擎所使用的檔案由賽門鐵克簽署。
- **BASH 引擎 (SONAR)**
SONAR 的行為引擎，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。
- **CIDS** (用戶端入侵偵測系統) 引擎 (入侵預防系統、記憶體攻擊緩和)

CIDS 引擎與防範網路攻擊和瀏覽器攻擊的 IPS 定義檔搭配使用。對於瀏覽器入侵預防，支援是以用戶端使用的 CIDS 引擎版本為基礎。記憶體攻擊緩和 (自 14 版起) 技術也使用 CIDS 引擎。請參閱：

[Endpoint Protection 中瀏覽器入侵預防支援的瀏覽器](#)

- **Eraser 引擎** (病毒和間諜軟體防護)

Eraser 引擎可用於針對客戶系統上所找到的威脅提供修復和移除功能 (矯正)。Eraser 也會確認在啟動時執行的驅動程式和應用程式不是惡意的。請參閱：

[Eraser 更新及套用 Eraser 引擎更新後的應用程式測試的所有相關資訊](#)

- **靜態資料掃描程式 (SDS) 引擎**

此引擎及其定義檔支援模擬器、Intelligent Threat Cloud Service (ITCS)，以及進階機器學習 (AML) 的 CoreDef-3 定義檔引擎 (自 14 版起)。SDS 引擎會判斷指定的開機磁區、分割表、檔案或程序記憶體是否包含威脅。它會在特定條件下修復威脅。

還原為舊版 Symantec Endpoint Protection 安全更新

依據預設，從 LiveUpdate 伺服器下載至管理伺服器的最新版本內容會自動下載至 Windows 用戶端。LiveUpdate 內容政策會指定允許用戶端檢查和安裝的內容類型。

不過，在下列情況下，您可能需要下載舊版內容：

- 最新的定義檔集或引擎導致用戶端電腦上發生軟體衝突。
- 您需要時間在內容發布至生產之前測試控制群組上的新引擎。

NOTE

請謹慎使用此功能。取消勾選內容類型意味著用戶端上的此功能不會保持最新。這可能會將您的用戶端置於較大的風險中。

如果您將內容類型設定為「選取修訂版本」，然後將 Symantec Endpoint Protection 用戶端轉換為雲端管理用戶端，則不會更新用戶端上的內容。若要避免此問題，請確保在轉換用戶端之前將內容選項設定為「使用最新的可用群組更新提供者」。

還原為舊版 Symantec Endpoint Protection 安全更新

1. 在主控台中，按下「政策」> **LiveUpdate**，然後開啟 LiveUpdate 內容政策。
2. 在「**Windows 設定**」下方，按下「安全性定義檔」。
無法回復 Mac 用戶端或 Linux 用戶端的內容。
3. 若要將內容回復為特定版本，請按下下列其中一個選項：
 - 「選取修訂版本」>「編輯」，然後選取修訂編號。
此選項會將用戶端鎖定至一組特定的安全性定義檔。用戶端不會收到任何新的安全性定義檔。
 - 「選取引擎版本」>「編輯」，然後選取引擎版本。
此選項會將用戶端鎖定到一個特定引擎，但仍繼續派送與該引擎相關聯的最新安全性定義檔。如果您知道目前在環境中運作的引擎，而且您需要在發布前測試其他群組中的較新引擎，請選取引擎版本。或者，按下「使用最新的可用群組更新提供者」，讓用戶端持續收到該內容類型的最新引擎版本和定義檔。
4. 按下「確定」。
無須重新啟動用戶端電腦，即可更新內容。
5. 在您解決任何疑難排解問題之後，請在「**Windows 設定**」下方，針對每種內容類型按下「安全性定義檔」>「使用最新的可用群組更新提供者」。

更多資訊

- [在 Windows 用戶端上發布之前測試引擎更新](#)
- [將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager](#)

使用群組更新提供者將內容散佈至用戶端

群組更新提供者 (GUP) 係為一部可直接將內容更新派送給其他用戶端的用戶端電腦。

GUP 的優勢包括：

- 可透過將處理負載轉移到 GUP，以保留頻寬和管理伺服器資源。
- 可有效地將更新傳送至網路連線受限或緩慢的用戶端。
- 比內部 LiveUpdate 伺服器容易設定。

Table 149: 使用群組更新提供者的工作

步驟	說明
步驟 1：瞭解您可以架構的各種群組更新提供者類型之間的區別	您可以設定單一、多個或跨子網路群組更新提供者。您設定的群組更新提供者類型取決於您的網路及該網路上的用戶端。各「群組更新提供者」類型之間並不會互斥。您可以對每個政策架構一或多種類型的「群組更新提供者」。請參閱： • 關於群組更新提供者的類型 • 關於在您的網路中架構一種以上類型群組更新提供者的影響
步驟 2：確認用戶端的通訊	架構群組更新提供者前，請確認用戶端電腦可接收伺服器的內容更新。解決任何用戶端伺服器通訊問題。 您可以在「監視器」頁面的「日誌」標籤上檢視「系統日誌」中的用戶端伺服器活動。請參閱： Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解
步驟 3：在一個或多個「LiveUpdate 設定」政策中架構群組更新提供者	在「LiveUpdate 設定」政策中架構群組更新提供者。請參閱： 將用戶端架構為從群組更新提供者下載內容
步驟 4：將「LiveUpdate 設定」政策指派給群組	您可以指派「LiveUpdate 設定」政策給使用「群組更新提供者」的群組。您也必須指派政策給內含「群組更新提供者」的群組。 針對單一「群組更新提供者」，您需要為每個站台的每個群組指派一個「LiveUpdate 設定」政策。 針對多個「群組更新提供者」和明確的「群組更新提供者」清單，您需要跨子網路指派一個「LiveUpdate 設定」政策給多個群組。請參閱： 指派政策給群組或位置
步驟 5：確認用戶端已指定為群組更新提供者	若要檢視被指定為群組更新提供者的用戶端電腦，請執行下列其中一項工作： • 按下「用戶端」>「用戶端」標籤 > 在用戶端上按下滑鼠右鍵，然後按下「編輯屬性」。「群組更新提供者」欄位為 True 或 False。 • 搜尋作為「群組更新提供者」的用戶端。請參閱：搜尋作為群組更新提供者的用戶端

關於群組更新提供者的類型

您可以在「LiveUpdate 設定」政策中架構多種類型的群組更新提供者。您使用的群組更新提供者的類型取決於網路的設定方式。您可以對每個政策架構一或多種類型的群組更新提供者；這些類型並不互斥。

Table 150: 何時使用特定群組更新提供者類型

「群組更新提供者」類型	使用時機
單一	單一「群組更新提供者」係指可為一個或多個用戶端群組提供內容的專屬用戶端電腦。架構單一群組更新提供者會將單一用戶端變成群組更新提供者。單一群組更新提供者可以是任一群組中的某台用戶端電腦。 當您要對所有用戶端電腦使用相同的「群組更新提供者」時，使用單一「群組更新提供者」。 您可以使用單一「LiveUpdate 設定」政策，為單一群組更新提供者指定靜態 IP 位址或主機名稱。但是，如果用作單一群組更新提供者的用戶端變更位置，您必須變更政策中的 IP 位址。 如果您要在不同的群組中使用不同的單一「群組更新提供者」，則必須為每個群組建立個別的「LiveUpdate 設定」政策。
多個	多個群組更新提供者會使用一組規則或準則選出為本身所擁有子網路中用戶端群組提供服務的提供者。所有用戶端電腦位於相同的子網路中。 您可以指定用戶端電腦作為群組更新提供者所必須符合的準則。如果用戶端電腦符合準則，管理伺服器會將此用戶端新增至全域群組更新提供者清單。然後，管理伺服器會對網路中的所有用戶端提供全域清單。用戶端可查看清單並選擇位於本身所屬子網路內的「群組更新提供者」。 架構多個「群組更新提供者」會將多個用戶端變成「群組更新提供者」。 針對下列任一情況使用多個群組更新提供者： - 您擁有多個群組，而且想要在每個群組中使用不同的群組更新提供者。 您可以使用一項政策指定多個「群組更新提供者」的選擇規則。如果用戶端變更位置，您不需要更新「LiveUpdate 設定」政策。Symantec Endpoint Protection Manager 會結合各站台與網域的多個「群組更新提供者」。您網路中各群組的所有用戶端便可使用此份清單。 - 多個「群組更新提供者」亦具備容錯移轉機制的功能。使用多個「群組更新提供者」可確保在每個子網路中至少都有一個「群組更新提供者」可以使用。
明確清單	如果您希望用戶端能夠連線到位於用戶端本身所屬子網路以外的其他子網路上的「群組更新提供者」，請使用明確的「群組更新提供者」清單。變更位置的用戶端可以漫遊到清單上最近的群組更新提供者。 明確的群組更新提供者清單不會將用戶端變成群組更新提供者。 當您架構明確的清單時，可以指定 IP 位址在特定子網路的用戶端應使用特定群組更新提供者。用戶端可能有多個 IP 位址，管理伺服器在比對要使用的群組更新提供者時，會將用戶端的所有 IP 位址列入考量。因此，政策比對的 IP 位址不一定繫結至用戶端用來與「群組更新提供者」通訊的介面。 例如，假設用戶端有 IP 位址 A，用來與管理伺服器和群組更新提供者通訊。這一個用戶端也有 IP 位址 B，這個位址符合您在「LiveUpdate 設定」政策中針對此用戶端架構的「明確群組更新提供者」。這個用戶端可以選擇使用根據位址 B 的「群組更新提供者」，儘管該位址並不是它用來與「群組更新提供者」通訊的位址。

在「LiveUpdate 設定」政策中架構單一或多個「群組更新提供者」時，會執行下列功能：

- 指定具有此政策的哪些用戶端作為「群組更新提供者」。
- 指定具有此政策的用戶端應使用哪些群組更新提供者來進行內容更新。

架構明確的群組更新提供者清單時，就只會執行一項功能：

- 指定具有此政策的用戶端應使用哪些群組更新提供者來進行內容更新。
雖然它不會將用戶端變成「群組更新提供者」，不過您仍可以架構和套用僅包含一個明確提供者清單的政策。不過，您接著必須在 Symantec Endpoint Protection Manager 中的其他政策架構單一「群組更新提供者」或多個「群組更新提供者」。或者，您可以在其他政策中同時架構這兩種類型。

如果用戶端無法透過任何群組更新提供者取得其更新，則可能會選擇性地嘗試從 Symantec Endpoint Protection Manager 更新。

更多資訊

- 關於在您的網路中架構一種以上類型群組更新提供者的影響
- 使用群組更新提供者將內容散佈至用戶端
- 將用戶端架構為從群組更新提供者下載內容
- 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager

將 Windows 用戶端架構為從群組更新提供者下載內容

您可以使用「LiveUpdate 設定」政策，使 Windows 用戶端只從群組更新提供者取得更新，永遠不從管理伺服器取得更新。您可以設定單一、多個或跨子網路群組更新提供者。您設定的群組更新提供者類型取決於您的網路及該網路上的用戶端。請參閱：

關於群組更新提供者的類型

Mac 用戶端和 Linux 用戶端無法從群組更新提供者取得內容。

將 Windows 用戶端架構為從群組更新提供者下載內容

1. 若要將用戶端架構為從群組更新提供者下載內容，請按一下「政策」。
2. 在「政策」下方，按一下 **LiveUpdate**。
3. 在「**LiveUpdate** 設定」標籤上，以滑鼠右鍵按一下所需的政策，然後按一下「編輯」。
4. 在「**LiveUpdate** 設定政策」視窗的「**Windows** 設定」下，按一下「伺服器設定」。
5. 在「內部或外部 **LiveUpdate** 伺服器」下方，勾選「使用預設管理伺服器」。
6. 在「群組更新提供者」下，勾選「使用群組更新提供者」。
7. 按下「群組更新提供者」。
8. 執行下列其中一項工作：
 - 按照**架構單一群組更新提供者**中的步驟執行。
 - 按照**架構多個群組更新提供者**中的步驟執行。
 - 按照**若要架構明確群組更新提供者清單**中的步驟執行。
9. 在「群組更新提供者設定」下，架構控制群組更新提供者電腦下載與儲存內容方式的選項。如需內容下載的相關資訊，請按一下「說明」。
10. 按下「確定」。

架構單一群組更新提供者

1. 在「群組更新提供者」對話方塊中，勾選「單一群組更新提供者 IP 位址或主機名稱」，然後輸入用作單一群組更新提供者之用戶端電腦的 IP 位址或主機名稱。如需 IP 位址或主機名稱的相關資訊，請按一下「說明」。
2. 返回此程序架構「群組更新提供者」。

架構多個「群組更新提供者」

1. 在「群組更新提供者」對話方塊中，勾選「多個群組更新提供者」，然後按一下「架構群組更新提供者清單」。
2. 在「群組更新提供者清單」對話方塊中，選取樹狀結構節點「群組更新提供者」，然後按下「新增」以新增規則集。
3. 在「指定群組更新提供者的規則準則」對話方塊的「選取」下拉式清單中，選取下列選項目之一：
 - 電腦 IP 位址或主機名稱
 - 登錄機碼
 - 作業系統
4. 如果您已選取「電腦 IP 位址或主機名稱」或「登錄機碼」，則請按一下「新增」。
5. 輸入或選取 IP 位址或主機名稱、Windows 登錄機碼或作業系統資訊。如需架構規則的相關資訊，請按一下「說明」。
6. 按下「確定」，直到返回「群組更新提供者清單」對話方塊，您可以在此對話方塊中選擇新增更多規則集。
7. 按下「確定」。
8. 返回此程序架構「群組更新提供者」。

架構「群組更新提供者」明確清單

1. 在「群組更新提供者」對話方塊中，勾選「漫遊用戶端的明確群組更新提供者」，然後按一下「架構明確群組更新提供者清單」。
2. 按一下「新增」。

-
3. 在「新增明確群組更新提供者」對話方塊中，輸入要這些群組更新提供者對應至的用戶端網路。

按一下「指定用戶端網路遮罩」以一次新增多個用戶端網路。請參閱：

[新增明確群組更新提供者](#)

4. 根據 IP 位址、主機名稱或群組更新提供者的網路位址，選取要設定的對應類型。
針對選取的對應類型輸入必要的設定。
5. 按下「確定」。

更多資訊

- [選擇派送方法以更新用戶端上的內容](#)
- [使用群組更新提供者將內容散佈至用戶端](#)

搜尋作為群組更新提供者的用戶端

您可以先確認用戶端是否可作為「群組更新提供者」。在「用戶端」標籤進行搜尋即可檢視「群組更新提供者」清單。

NOTE

您也可查看用戶端屬性。屬性中包括一項說明用戶端是否可作為「群組更新提供者」的欄位。

搜尋作為「群組更新提供者」的用戶端

1. 在主控台中，按一下「用戶端」。
2. 在「用戶端」標籤上的「檢視」方塊中，選取「用戶端狀態」。
3. 在「工作」窗格中，按下「搜尋用戶端」。
4. 在「尋找」下拉式清單中，選取「電腦」。
5. 在「在群組中」方塊中指定群組名稱。
6. 在「搜尋條件」下方，按下「搜尋欄位」欄並選取「群組更新提供者」。
7. 在「搜尋條件」下方，按下「比較運算子」欄並選取 =。
8. 在「搜尋條件」下方，按下「值」欄並選取 **True**。

若需搜尋條件的相關資訊，請按下「說明」。

9. 按下「搜尋」。

更多資訊

[使用群組更新提供者將內容散佈至用戶端](#)

在您的網路中架構多種類型的群組更新提供者

如果您在政策中架構一或多個「群組更新提供者」，則 Symantec Endpoint Protection Manager 會撰寫已經登入的所有提供者的全域清單。此檔案預設為：

- 32 位元作業系統：C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml。
- 64 位元作業系統：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml

Symantec Endpoint Protection Manager 提供此全域清單給任何要求此清單的用戶端，因此用戶端可以決定自身應該使用的「群組更新提供者」。由於存在此程序，因此如果單一提供者滿足明確對應準則，政策僅架構了多個或明確「群組更新提供者」的用戶端也可以使用單一「群組更新提供者」。此現象可能發生，因為單一提供者是用戶端從其 Symantec Endpoint Protection Manager 取得的全域提供者清單的一部分。

因此，在 Symantec Endpoint Protection Manager 上任何政策中架構的所有「群組更新提供者」均有可能為用戶端使用。如果您將僅包含明確的「群組更新提供者」清單的政策套用到群組中的用戶端，則群組中的所有用戶端均會嘗試使用 Symantec Endpoint Protection Manager 全域「群組更新提供者」清單中滿足明確對應準則的「群組更新提供者」。

NOTE

Symantec Endpoint Protection 用戶端可能有多個 IP 位址。當 Symantec Endpoint Protection 符合某「群組更新提供者」時，會考量所有 IP 位址。因此，政策符合的 IP 位址不是永遠繫結至用戶端用於與 Symantec Endpoint Protection Manager 和「群組更新提供者」通訊的介面。

如果所有類型的「群組更新提供者」均在 Symantec Endpoint Protection Manager 上的政策中架構，則用戶端會嘗試連接到全域清單中的「群組更新提供者」，順序如下：

- 「多個群組更新提供者」清單中依序列出的提供者
- 「明確的群組更新提供者」清單中依序列出的提供者
- 架構為「單一群組更新提供者」的提供者

您可以架構以下類型的明確對應準則：

- IP 位址：子網路 A 中的用戶端應該使用 IP 位址為 x.x.x.x 的「群組更新提供者」。
- 主機名稱：子網路 A 中的用戶端應該使用主機名為 xxxxx 的「群組更新提供者」。
- 子網路網路位址：子網路 A 中的用戶端應該使用位於### B 中的任何「群組更新提供者」。

可將多個對應準則用於單一政策中明確的「群組更新提供者」清單。賽門鐵克建議您小心架構多個對應準則，避免發生意外結果。例如，如果您對明確對應架構不當，在無法取得更新時就可能中斷用戶端。

可以考量在單一政策中架構的以下多個明確對應準則，作為方案：

- 如果用戶端在子網路 10.1.2.0 中，請使用 IP 位址為 10.2.2.24 的「群組更新提供者」
- 如果用戶端在子網路 10.1.2.0 中，請使用 IP 位址為 10.2.2.25 的「群組更新提供者」
- 如果用戶端在子網路 10.1.2.0 中，請使用主機名為 SomeMachine 的「群組更新提供者」
- 如果用戶端在子網路 10.1.2.0 中，請使用子網路 10.5.12.0 上的任何「群組更新提供者」
- 如果用戶端在子網路 10.6.1.0 中，請使用子網路 10.10.10.0 上的任何「群組更新提供者」

有了這個明確的「群組更新提供者」政策，如果用戶端在子網路 10.1.2.0 中，前四個規則適用；第五個規則不適用。如果未指定任何對應給用戶端所在的子網路，例如 10.15.1.0，則沒有規則適用於該用戶端。用戶端的政策指出使用一個明確的「群組更新提供者」清單，但是根據這些規則，沒有用戶端可以使用的對應。如果您也禁止了該用戶端從 Symantec Endpoint Protection Manager 和 Symantec LiveUpdate 伺服器下載更新，則該用戶端沒有可用的更新方法。

更多資訊

- [關於群組更新提供者的類型](#)
- [將用戶端架構為從群組更新提供者下載內容](#)

使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容

賽門鐵克建議用戶端電腦使用 LiveUpdate 來更新 Symantec Endpoint Protection 用戶端上的內容。但是，如果您不想使用 LiveUpdate 或 LiveUpdate 無法使用，則可以使用智慧型更新小幫手 (Intelligent Updater) 檔案更新用戶端。Windows 適用的智慧型更新小幫手 (Intelligent Updater) .exe 檔案僅為更新用戶端設計。智慧型更新程式檔案並不包含 Symantec Endpoint Protection Manager 更新其受管用戶端所需的資訊。

Windows 適用的智慧型更新小幫手 (Intelligent Updater) 檔案是包含病毒和間諜軟體定義檔的自動執行檔案。其他智慧型更新小幫手 (Intelligent Updater) 檔案可供 SONAR 定義檔與入侵預防特徵使用。針對 Mac 和 Linux，您可以下載病毒和間諜軟體定義檔。

下載檔案後，您可以採用偏好的派送方法，將更新派送到用戶端。

NOTE

智慧型更新小幫手 (Intelligent Updater) 不提供任何其他類型內容的更新。例如，智慧型更新小幫手(Intelligent Updater) 不支援延伸檔案屬性和特徵、自動防護入口網站清單、Power Eraser 定義檔或縮減大小定義檔。

使用智慧型更新小幫手檔案更新 **Symantec Endpoint Protection** 用戶端上的內容

1. 若要使用網頁瀏覽器下載智慧更新程式檔，請移至以下頁面：

[病毒定義檔與安全性更新](#)

2. 從下拉式清單，選取其中一個可用的 Symantec Endpoint Protection 選項。

頁面會重新整理，以顯示可供該版本使用的內容。

3. 在防護類別中，按一下「下載」旁邊的「定義」。

4. 按下您要更新的用戶端版本的適當檔案名稱。

NOTE

針對 Linux 病毒定義檔，按下「**Unix 平台**」標籤。

5. 當系統提示您提供儲存檔案的位置時，請在硬碟上選取一個資料夾。

6. 使用偏好的派送方法將檔案派送至用戶端電腦。

7. 若要在用戶端電腦上安裝病毒定義和安全更新檔，請在用戶端電腦上找到派送至用戶端的智慧更新程式檔。

8. 執行下列其中一個動作：

- 若為 Windows：連按兩下 .exe 檔案，然後按照畫面上的指示操作。
- 若為 Mac：連按兩下 .zip 檔案，連按兩下 .pkg 檔案，然後按照畫面上的指示操作。
- 若為 Linux：驗證檔案具有可執行權限，驗證已安裝 uudecode 和 uncompress，然後使用進階使用者權限執行 .sh 檔案。請參閱下列各項以取得詳細資訊：

[如何使用智慧型更新小幫手 \(Intelligent Updater\) 定義檔更新 Linux 系統電腦](#)

更多資訊

[選擇派送方法以更新用戶端上的內容](#)

使用第三方派送工具更新用戶端電腦

某些大型企業依賴第三方派送工具 (例如 IBM Tivoli 或 Microsoft SMS) 將內容更新派送到用戶端電腦。Symantec Endpoint Protection 支援使用第三方派送工具，更新執行 Windows 作業系統的受管用戶端和非受管用戶端。Mac 和 Linux 用戶端僅能從內部或外部 LiveUpdate 伺服器收到內容更新。

在您準備使用第三方派送工具之前，必須安裝 Symantec Endpoint Protection Manager 以及要更新的用戶端電腦。

Table 151: 準備使用第三方派送工具進行更新前要執行的工作

工作	說明
將 Symantec Endpoint Protection Manager 架構為接收內容更新。	您可以將管理伺服器架構為自動或手動接收內容更新。請參閱： • 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager • 如何更新用戶端上的內容和定義檔
將群組的 LiveUpdate 設定政策架構為允許派送第三方內容更新。	如果要使用第三方派送工具更新受管用戶端，則您必須將群組的 LiveUpdate 設定政策架構為允許執行該作業。請參閱： 將 LiveUpdate 設定政策架構為允許將第三方內容派送至受管用戶端

工作	說明
為非受管用戶端進行準備，以透過第三方派送工具接收更新。	如果要使用第三方派送工具更新非受管用戶端，必須先在每個非受管用戶端上建立登錄機碼。請參閱： 準備非受管用戶端以從第三方派送工具接收更新
尋找、複製與派送內容。	每個 Symantec Endpoint Protection Manager 用戶端群組都有 index2.dax 檔案，該檔案位於執行 Symantec Endpoint Protection Manager 的電腦上。依據預設，這些檔案位於 SEPM_Install\data\outbox\agent 資料夾下的子資料夾中。若要更新用戶端，您需要使用 index2.dax 檔案。 SEPM_Install 的預設位置為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。請參閱： - 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager - 使用第三方派送工具派送內容

將 LiveUpdate 設定政策架構為允許將第三方內容派送至受管用戶端

如果要使用第三方派送工具更新受管用戶端，則您必須將用戶端群組的 LiveUpdate 設定政策架構為允許執行該作業。您可以選擇是否要停用讓用戶端使用者手動執行 LiveUpdate 的功能。

完成此程序時，群組之用戶端電腦的下列位置會顯示資料夾 (適用於 Vista 和更新版本的作業系統)：

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

使用 **LiveUpdate** 政策啟用派送第三方內容給受管用戶端的功能

1. 在主控台中，按下「政策」。
2. 在「政策」下方，按一下 **LiveUpdate**。
3. 在「**LiveUpdate** 設定」標籤的「工作」下方，按一下「新增 **LiveUpdate** 設定政策」。
4. 在「**LiveUpdate** 政策」視窗的「政策名稱」和「說明」文字方塊中，輸入名稱和說明。
5. 在「**Windows** 設定」下方，按一下「伺服器設定」。
6. 在「第三方管理」下方，勾選「啟用第三方內容管理」。
7. 取消勾選其他所有 LiveUpdate 來源選項。
8. 按下「確定」。
9. 在「指派政策」對話方塊中，按一下「是」。
您也可以取消此程序，稍後再指派政策。
10. 在「指派 **LiveUpdate** 政策」對話方塊中，選取一個或多個要指派此政策的群組，然後按一下「指派」。

更多資訊

[將用戶端架構為從內部 LiveUpdate 伺服器下載內容](#)

準備非受管用戶端以從第三方派送工具接收更新

如果您從安裝檔案安裝非受管用戶端，則無法立即使用第三方派送工具，向其派送 LiveUpdate 內容或政策更新。作為安全措施，根據預設，這些用戶端電腦既不信任也不處理第三方派送工具傳送給其的內容。

若要成功使用第三方派送工具傳送更新，您必須先在每個非受管用戶端上建立 Windows 登錄機碼。此機碼可讓您使用非受管用戶端上的收件匣資料夾，以便使用第三方派送工具來派送 LiveUpdate 內容和政策更新。

收件匣資料夾顯示在非受管用戶端的以下位置 (Vista 和更新版本的作業系統)：

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

登錄機碼一經建立，您便可以使用第三方派送工具，複製內容或政策更新到此資料夾。然後，Symantec Endpoint Protection 用戶端軟體便會信任並處理更新。

準備非受管用戶端以從第三方派送工具接收更新

1. 請在每台用戶端電腦上，使用 regedit.exe 或其他 Windows 登錄編輯工具新增下列 Windows 登錄機碼之一：

- 在 32 位元電腦上：HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState
- 在 64 位元電腦上 (14.3 RU4 或更早版本的用戶端)：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState
- 在 64 位元電腦上 (14.3 RU5 或更高版本的用戶端)：HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState

2. 將登錄機碼的值類型設定為 DWORD (32 位元) 或 QWORD (64 位元)，並將值設定為十六進位數字 80，如下所示：

```
0x00000080 (128)
```

3. 儲存登錄機碼，然後結束登錄編輯工具。

更多資訊

- [使用第三方派送工具更新用戶端電腦](#)
- [使用第三方派送工具派送內容](#)

使用第三方派送工具派送內容

若要使用第三方派送工具將內容派送到用戶端電腦，您需要使用 index2.dax 檔案。index2 檔案中與 LiveUpdate 相關的內容，包含一組稱為內容 Moniker 的 GUID 及其關聯的序號。每個內容 Moniker 對應一個特定的內容類型。index2 檔案中的每個序號都對應於特定內容類型的修訂。視已安裝的防護功能而定，您必須判斷需要哪些內容類型。請參閱：

[關於 LiveUpdate 下載的內容類型](#)

NOTE

內容 moniker 通常隨每個主要版本而異。有時，也可能變更次要版本的內容 Moniker。賽門鐵克通常不會變更版本更新或維護修正程式的 moniker。

您可以開啟 ContentInfo.txt 檔案來查看代號物件與其內容類型的相同映射內容。根據預設，ContentInfo.txt 檔案位於 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Inetpub\content\。

例如，您可能會看見以下項目：

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SEPC Virus Definitions  
Win32 14.3 RU3 - MicroDefsB.CurDefs - SymAllLanguages
```

每個 Symantec Endpoint Protection Manager 用戶端群組有其自己的 index2 檔案。每個用戶端群組的 index2 檔案都可在該群組的資料夾中找到。根據預設，用戶端群組的資料夾位於 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\。用戶端群組的資料夾名稱與群組政策序號相對應。您可以在「群組屬性」對話方塊中或「用戶端」頁面的「詳細資料」標籤上找到序號。每個群組政策序號的前四個十六進位值與該群組資料夾中的前四個十六進位值相符合。

受管用戶端使用的 index2.dax 檔案已加密。若要檢視該檔案的內容，請開啟同一資料夾中的可用 index2.xml 檔案。index2.xml 檔案提供了內容 Moniker 及其序 (版本) 號清單。例如，您可能會看見以下項目：

```
<File Checksum="D5ED508E8CF7A8A4450B0DBA39BCCB25" DeltaFlag="1"  
FullSize="625203112" LastModifiedTime="1425983765211" Moniker=  
"{535CB6A4-441F-4e8a-A897-804CD859100E}" Seq="150309034"/>
```

群組的 LiveUpdate 內容政策會指定特定版本的內容或最新內容。index2 檔案中的序號必須與對應於群組的 LiveUpdate 內容政策中的內容規範的序號相符合。例如，如果所有內容類型的政策均架構為「使用最新的可用群組更新提供者」，則每種類型的序號即為最新的可用內容。在此範例中，派送僅在 index2 檔案調出對應於最新內容修訂的序號 (修訂號) 時才執行。如果序號對應到任何其他改版編號，則此發布無效。

NOTE

您必須使用 Copy 指令將檔案放入用戶端的 \inbox 資料夾。使用 Move 指令不會觸發更新處理，而且更新會失敗。如果將內容壓縮至單一封存檔以供派送，不應該將它直接解壓縮至 \inbox 資料夾。

使用第三方派送工具將內容派送至用戶端

1. 在執行 Symantec Endpoint Protection Manager 的電腦上，建立工作資料夾 (如 \Work_Dir)。

2. 執行下列其中一項動作：

- 對於受管用戶端，請在主控台的「用戶端」標籤上，於要更新的群組上按下右鍵，然後按下「屬性」。
- 對於非受管用戶端，請在主控台的「用戶端」標籤上，右鍵按下「我的公司」，然後按下「屬性」。

3. 記下「政策序號」的前四位十六進位值，例如 7B86。

4. 導覽至以下資料夾：

```
SEPM_Install\data\outbox\agent
```

其中 SEPM_Install 表示 Symantec Endpoint Protection Manager 的安裝資料夾。預設安裝資料夾為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。

5. 找到包含與「政策序號」相符合的前四位十六進位值的資料夾。

6. 開啟該資料夾，然後將 index2.dax 檔案複製到您的工作資料夾。

7. 導覽至以下資料夾：

```
SEPM_Install\Inetpub\content
```

其中 SEPM_Install 表示 Symantec Endpoint Protection Manager 的安裝資料夾。預設安裝資料夾為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。

8. 開啟並讀取 ContentInfo.txt，搜尋每個 target moniker 資料夾包含的內容。

每個目錄的內容會採用下列格式：target moniker\sequence number\full.zip|full。

9. 將每個 \target moniker 資料夾的內容複製到您的工作資料夾 (如 \Work_Dir)。

10. 刪除每個 \target moniker 中的所有檔案和資料夾，只在您的工作資料夾中保留下列資料夾結構和檔案：

```
\\Work_Dir\target moniker\latest sequence number\full.zip
```

現在，您的工作資料夾包含要派送至用戶端的資料夾結構和檔案。

11. 使用第三方派送工具將工作資料夾的內容派送至每個用戶端的 \\Symantec Endpoint Protection\inbox\ 資料夾。

最後的結果須類似如下：

```
\\Symantec Endpoint Protection\inbox\index2.dax
```

```
\\Symantec Endpoint Protection\inbox\target moniker\latest sequence number\full.zip
```

然後，會刪除已成功處理的檔案。未能成功處理的檔案則會移至名為 Invalid 的子資料夾中。如果您在 inbox 資料夾下的 Invalid 資料夾中看到檔案，則必須重新處理這些檔案。

更多資訊

- [使用第三方派送工具更新用戶端電腦](#)
- [準備非受管用戶端以從第三方派送工具接收更新](#)

監控、報告和強制執行合規性

瞭解如何執行與讀取報告和日誌，以及設定主機完整性。

本節介紹如何：

- 設定主機完整性以確保用戶端電腦受到防護，並遵從公司的安全性政策。
- 使用日誌和報告來監控環境中的安全性。
- 管理通知。

架構主機完整性

使用主機完整性政策，可確保您網路中的 Windows 用戶端電腦符合組織的安全政策。

NOTE

Mac 用戶端或 Linux 代理程式不支援主機完整性。

下表列出您使用主機完整性政策設定安全合規性的步驟。

Table 152: 設定主機完整性政策的工作

步驟	說明
步驟 1：建立主機完整性政策，用於檢查用戶端電腦的需求並針對非遵從電腦強制執行矯正動作。	將需求新增至主機完整性政策 1. 在主控台中，開啟主機完整性政策，然後按一下「需求」。 新增您想要用戶端電腦檢查的需求。為每種類型的軟體 (如應用程式、檔案和修補程式) 建立單獨的需求。請參閱： — 將預先定義的需求新增至主機完整性政策 — 關於主機完整性需求 2. 在「新增需求」對話方塊中，針對非遵從用戶端電腦架構矯正動作。 矯正需要用戶端電腦安裝或要求用戶端使用者安裝所需的軟體。請參閱： 設定預先定義主機完整性需求的矯正 3. 在「需求」頁面上，使用「上移」和「下移」選項以設定檢查需求和嘗試矯正的順序。例如，應該以特定的順序完成更新，以便在使用者必須重新啟動用戶端電腦之前套用所有更新。
步驟 2：設定主機完整性檢查和通知的選項。	在「進階設定」頁面上： • 架構主機完整性檢查的執行頻率。請參閱： 架構主機完整性檢查頻率的設定 • 架構使用者是否可以取消矯正。請參閱： 允許使用者延遲或取消主機完整性矯正 • 設定當主機完整性檢查通過或失敗時顯示於用戶端電腦的通知。使用通知來告訴一般使用者下一步的動作。例如，使用者可能需要在用戶端電腦上下載並安裝新修正式。請參閱： 架構主機完整性檢查的通知
步驟 3：設定點對點強制執行 (選擇性)。	如果測試主機完整合規性的用戶端電腦與已遵從用戶端電腦位於同一網路，則您可以設定點對點強制執行。您主要是針對檔案共用使用點對點強制執行。請參閱： 透過架構點對點驗證攔截遠端電腦
步驟 4：針對非遵從電腦和未經矯正的電腦設定隔離所政策 (選擇性)。	如果用戶端電腦執行主機完整性檢查失敗並且未執行矯正，您可以使用隔離所政策隔離電腦。請參閱： 針對失敗的主機完整性檢查建立隔離所政策

[產生主機完整性檢查失敗的電腦清單](#)

主機完整性的運作方式

主機完整性可確保用戶端電腦受到防護並遵從公司的安全性政策。主機完整性政策可用於定義、強制執行和還原用戶端的安全性，以保護企業網路和資料的安全。

需求

若要讓「主機完整性」檢查執行，請確保：

- 您已在用戶端電腦上安裝「病毒、間諜軟體及基本下載防護」元件和「防火牆」元件。請參閱：[選擇要在用戶端上安裝哪些安全性功能](#)
- 用戶端電腦上已啟用「病毒和間諜軟體防護」元件和「網路威脅防護」元件。如果用戶端使用者停用這些功能中的任何一項，用戶端電腦會忽略「主機完整性」政策。

檢查元件是否已啟用

1. 在主控台中，新增「主機完整性」政策並新增防毒、防間諜軟體和防火牆需求。
2. 針對「必須安裝和執行的 <防毒> 應用程式」的每項需求，選取「Symantec Endpoint Protection」。
3. 勾選「如果尚未在用戶端執行防毒應用程式，請啟動」。

 Add Requirement ×

Name:

Client Type:

Antivirus application that must be installed and running

☐ Install antivirus if it has not been installed on the client

☐ Download the installation package

Download URL:

Execute the command (use %F% to specify the downloaded file if it is available):

☒ Start antivirus if it is not running on the client

Execute the command:

Antivirus Signature File Checking

☐ Specify the oldest age of the signature file:

☐ Check the signature file date

☒ Ensure signature file date is not equal to

☐ Ensure signature file date is equal to

October 20, 2023

October 20, 2023

主機完整性工作流程

Table 153: 在用戶端電腦上強制執行安全性遵從的程序

步驟	說明
步驟 1：用戶端電腦在本機執行主機完整性檢查。	管理伺服器會將主機完整性政策下載到所指派群組中的用戶端電腦。用戶端電腦會執行主機完整性檢查，它會將每台電腦的組態與您新增至主機完整性政策的要求進行比較。 主機完整性政策會檢查是否存在防毒軟體、修正程式、修補程式，以及其他安全性要求。例如，政策會檢查作業系統是否套用了最新的修正程式。請參閱： 架構主機完整性
步驟 2：通過或未通過主機完整性檢查	- 如果電腦符合政策的全部要求，表示通過主機完整性檢查。 - 如果電腦不符合政策的全部要求，表示未通過主機完整性檢查。您也可以設定政策以忽略不符合的需求，使檢查能夠通過。請參閱： 允許主機完整性檢查在需求失敗時通過 您也可以設定防火牆政策中設定點對點驗證，此驗證可授予或攔截對於已安裝用戶端之遠端電腦的入埠存取。請參閱： 透過架構點對點驗證攔截遠端電腦
步驟 3：非遵從電腦矯正失敗的主機完整性檢查 (選擇性)	- 如果主機完整性檢查失敗，您可以架構用戶端來加以矯正。若要矯正，用戶端會下載並安裝遺漏的軟體。您可以架構用戶端或一般使用者在預先定義的需求或自訂需求中進行矯正。接著，主機完整性會重新檢查用戶端電腦是否已安裝軟體。請參閱： 設定預先定義主機完整性需求的矯正 - 如果驗證矯正的主機完整性檢查仍然失敗，用戶端會套用隔離所政策。您可以使用隔離所政策將更嚴格的限制套用到失敗的電腦。請參閱： 針對失敗的主機完整性檢查建立隔離所政策 - 如果用戶端位於「隔離所」位置，主機完整性檢查會繼續執行並嘗試矯正。檢查頻率和矯正設定依架構主機完整性政策的方式而定。在用戶端經過矯正並通過主機完整性檢查之後，用戶端就會自動移出「隔離所」位置。 在某些情況下，您可能需要手動矯正用戶端電腦。
步驟 4：用戶端繼續監控合規性狀態	主機完整性檢查會主動監控每個用戶端的遵從狀態。一旦用戶端的遵從狀態變更，電腦的權限也會變更。 - 如果您變更主機完整性政策，它會在下一次出現活動訊號時下載至用戶端。用戶端接著會執行「主機完整性」檢查。 - 當主機完整性檢查正在進行時，如果用戶端切換至具有不同主機完整性政策的位置，則用戶端會停止此項檢查。此停止包括任何矯正嘗試。如果新的位置無法使用矯正伺服器連線，使用者可能會看見逾時訊息。檢查完成後，用戶端會捨棄結果。接著，用戶端會根據位置的新政策，立即執行新的「主機完整性」檢查。 您可以在遵從日誌中檢視主機完整性檢查的結果。請參閱： 檢視日誌

關於主機完整性需求

建立新主機完整性政策時，請決定要新增的需求類型。

每個需求都會指定下列項目：

- 檢查的條件
例如，需求將會檢查最新病毒定義檔集是否已經安裝在用戶端電腦上。
- 如果用戶端未能通過條件需求，用戶端應該採取什麼矯正動作
例如，矯正動作可以包括用戶端可下載並安裝缺少的病毒定義檔所在的 URL。

下表列出您可以使用的需求類型。

Table 154: 主機完整性政策的需求類型

類型	說明
預先定義的需求	使用預先定義的需求來檢查特定應用程式或檔案是否已經在用戶端上安裝並執行。預先定義的需求可以檢查以下任一類型的應用程式的狀態：防毒軟體、防間諜軟體、防火牆、修正程式或服務套件。例如，修正程式需求可檢查用戶端電腦是否執行特定的作業系統修正程式。 如果預先定義的需求沒有足夠的詳細資料，請新增自訂需求並撰寫指令碼。請參閱： 將預先定義的需求新增至主機完整性政策
範本中的自訂需求	範本為預先定義的自訂需求，是賽門鐵克為經常執行的工作所撰寫。例如，用戶端可以檢查是否已在過去 42 天內變更密碼。您也可以基於範本來撰寫自訂需求指令碼。 利用「主機完整性政策 LiveUpdate 服務」可以取得範本需求，您必須首先設定 LiveUpdate，以將主機完整性範本下載至管理伺服器。請參閱： • 從範本新增自訂需求 • 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager
自訂需求	如果預先定義的需求和範本均無法提供您需要的檢查種類，請使用自訂需求。自訂需求包括與預先定義的需求相同的欄位，但是會提供更多的彈性。例如，您可以包括不位於預先定義之防間諜軟體應用程式清單的防間諜軟體應用程式。 而在自訂需求中包括類似的應用程式，可大大簡化必要應用程式的管理。例如，Internet Explorer 和 Mozilla Firefox 之類的網際網路瀏覽器都可納入同一個需求中。請參閱： 撰寫自訂的需求指令碼

更多資訊

[設定主機完整性](#)

將預先定義的需求新增至主機完整性政策

主機完整性政策中預先定義的需求將檢查用戶端電腦是否執行以下任何類型的應用程式，例如：防毒軟體、防間諜軟體或防火牆。

您可決定特定應用程式，例如適用於 Windows 7 作業系統的特定修正程式。然後，您可以指定用戶端電腦取得修正程式的路徑。

將預先定義的需求新增至主機完整性政策

1. 在主控台中，開啟某個主機完整性政策。
2. 在「主機完整性政策」頁面上，按下「需求」>「新增」。
3. 在「新增需求」對話方塊中，按下「選取需求」下拉式清單，選取預先定義的需求，然後按下「確定」。
4. 架構此需求的設定和矯正選項，然後按下「確定」。請參閱：

[設定預先定義主機完整性需求的矯正](#)

更多資訊

- [從範本新增自訂需求](#)
- [撰寫自訂的需求指令碼](#)

設定預先定義主機完整性需求的矯正

如果用戶端「主機完整性」檢查顯示需求失敗，則您可以架構還原必要檔案的政策。此用戶端將透過下載、安裝或執行所需的應用程式來還原檔案，以符合需求。用戶端電腦接著便可通過主機完整性檢查。

您可以在新增預先定義需求的相同對話方塊中設定矯正。您不僅可以指定用戶端下載矯正檔案的路徑，也可以指定如何實作矯正程序。

您還可以讓使用者控制何時矯正其電腦。例如，重新啟動可能會讓使用者遺失工作，因此使用者可能想要將矯正延遲到當天結束時進行。

在下載、安裝或執行還原需求的指令之後，用戶端一律會重新測試需求。此外，用戶端還會記錄結果，即 `pass` 或 `fail`。

設定預先定義主機完整性需求的矯正

1. 在主控台中，開啟某個主機完整性政策並新增一個預先定義的需求。請參閱：

[將預先定義的需求新增至主機完整性政策](#)

2. 在「新增需求」對話方塊中，按下「如果尚未在用戶端安裝 <需求類型>，請安裝」。
3. 按下「下載安裝套件」。
4. 在「下載 URL」文字方塊中，輸入可將安裝檔案下載到用戶端電腦的 URL。請參閱：

[關於指定用於矯正的檔案位置和執行指令](#)

5. 在「執行指令」文字方塊中，執行下列其中一個工作：

- 如果您要讓用戶端使用者執行安裝，請將文字方塊保留空白。
- 如果您要安裝自動執行，請輸入 `%F%`。
`%F%` 變數代表最後下載的檔案。您可以使用可從「開始」>「執行」執行的任何指令。例如，若要安裝 Vista 的修正程式，請鍵入指令 `%Systemroot%\system32\wusa.exe /quiet /norestart %F%`。

6. 可以選擇性地設定延遲或取消矯正的選項，然後按下「確定」。請參閱：

[允許使用者延遲或取消主機完整性矯正](#)

7. 按下「確定」。

更多資訊

[允許主機完整性檢查在需求失敗時通過](#)

允許使用者延遲或取消主機完整性矯正

您可以允許使用者將矯正延遲到比較方便的時間。如果使用者針對某個需求在安裝軟體後必須重新啟動其電腦，則可能需要等待以後再重新啟動電腦。

如果使用者延遲矯正，則可能會發生以下任一事件：

- 用戶端會記錄該事件。「主機完整性」狀態會顯示為失敗，因為不符合需求。使用者隨時都可從用戶端手動執行新的「主機完整性」檢查。
- 用戶端執行另一次「主機完整性」檢查前，「主機完整性」檢查矯正訊息視窗都不會顯示。如果使用者選擇在 5 分鐘內提醒，但「主機完整性」檢查是每隔 30 分鐘執行一次，則訊息視窗會等到 30 分鐘後才顯示。為了避免造成使用者困惑，您可能需要將最短時間設定和「主機完整性」檢查頻率設定同步。
- 如果使用者在下次「主機完整性」檢查之前延遲矯正，則使用者的選擇會被覆寫。
- 如果使用者延遲矯正動作且用戶端接收到更新的策略，矯正可用的時間長度則會重設為新的最大值。

允許使用者延遲或取消主機完整性矯正

1. 在主控台中，開啟某個主機完整性政策並新增一個需求。請參閱：

[將預先定義的需求新增至主機完整性政策](#)

2. 在「新增需求」對話方塊中，設定矯正。請參閱：

[設定預先定義主機完整性需求的矯正](#)

3. 在需求的對話方塊中，執行下列其中一項工作，然後按下「確定」：

- 若要讓用戶端使用者延遲下載檔案，請勾選「指定下載失敗時要等待多久後再次嘗試下載」。
- 若要讓用戶端使用者取消矯正，請勾選「允許使用者取消下載主機完整性矯正」。

-
4. 按下「確定」。
 5. 按下「進階設定」。
 6. 在「進階設定」頁面的「矯正對話方塊選項」下方，架構取消矯正的選項。
 7. 若要在用戶端電腦上新增自訂訊息，請按下「設定其他文字」。
使用者按下「詳細資訊」時，此處鍵入的訊息會顯示在用戶端矯正視窗中。
 8. 按下「確定」。

架構主機完整性檢查頻率的設定

您可架構主機完整性檢查的執行方式，以及檢查結果的處理方式。

在您新增或更新主機完整性政策之後，它就會在出現下一次活動訊號時，下載至用戶端。然後，用戶端會執行主機完整性檢查。

如果使用者切換至具有不同政策的位置，而此時正在執行主機完整性檢查，則用戶端會停止此項檢查。如果政策有要求，則這個停止動作還包含矯正嘗試。如果新的位置無法使用矯正伺服器連線，使用者可能會看見逾時訊息。檢查完成後，用戶端會捨棄結果。接著，用戶端會根據位置的新政策，立即執行新的「主機完整性」檢查。

如果新位置使用相同的政策，則用戶端會保留所有的「主機完整性」計時器設定。唯有在政策設定有需要時，用戶端才會執行新的「主機完整性」檢查。

架構主機完整性檢查頻率的設定

1. 在主控台中，開啟「主機完整性」政策，然後按一下「進階設定」。
2. 在「進階設定」頁面的「主機完整性檢查選項」下方，設定「主機完整性」檢查頻率。
3. 按下「確定」。

更多資訊

- [將預先定義的需求新增至主機完整性政策](#)
- [允許主機完整性檢查在需求失敗時通過](#)

允許主機完整性檢查在需求失敗時通過

即使使用者的電腦未能通過主機完整性檢查，使用者也可能需要繼續工作。即使特定的需求失敗，您也可以讓主機完整性檢查通過。用戶端將記錄結果，但會忽略結果。

您可以針對特定的需求套用此設定。如果您要將這項設定套用至所有的需求，您必須分別在每項需求上啟用此設定，設定預設為停用。

允許主機完整性檢查在需求失敗時通過

1. 在主控台中，開啟某個主機完整性政策。
2. 新增預先定義的需求或自訂需求，然後按下「確定」。請參閱：
 - [將預先定義的需求新增至主機完整性政策](#)
 - [撰寫自訂的需求指令碼](#)
3. 在需求的對話方塊上，勾選「即使這項要求失敗，也允許主機完整性檢查通過」，然後按下「確定」。
4. 按下「確定」。

架構主機完整性檢查的通知

用戶端執行「主機完整性」檢查時，您可以架構發生下列狀況時出現的通知：

- 主機完整性檢查失敗時。
- 主機完整性檢查失敗後再次檢查通過時。

「主機完整性」檢查的結果會出現在用戶端的「安全日誌」中。這些資訊會上傳至管理伺服器「監控器」頁面的「遵從日誌」中。

用戶端的「安全日誌」包含多個窗格。如果您選取「主機完整性」檢查事件類型，左下方窗格會列出各個需求已通過還是未通過。右下方窗格會列出需求的條件。您可以架構用戶端，使資訊不出現在右下方窗格中。雖然進行疑難排解時可能需要這項資訊，但是您可能不希望使用者檢視這項資訊。例如，您可能寫入指定登錄值或檔案名稱的自訂需求。「安全日誌」仍會記錄詳細資訊。

您也可以啟用通知，使得使用者能夠選擇立即下載軟體，或延遲矯正。請參閱：

[允許使用者延遲或取消主機完整性矯正](#)

架構主機完整性檢查的通知

1. 在主控台中，開啟某個主機完整性政策。
2. 在「主機完整性」頁面上，按一下「進階設定」。
3. 在「進階設定」頁面的「通知」下方，若要顯示詳細的需求資訊，請勾選「顯示詳細的主機完整性記錄」。

用戶端的「安全日誌」右下方窗格會顯示「主機完整性」需求的完整資訊。

4. 勾選下列任何選項：
 - 主機完整性檢查失敗時顯示通知訊息。
 - 主機完整性檢查失敗後再次檢查通過時顯示通知訊息。
5. 若要新增自訂訊息，請按一下「設定其他文字」，並輸入最多 512 個字元的其他文字，然後按一下「確定」。
6. 架構完此政策後，請按一下「確定」。

針對失敗的主機完整性檢查建立隔離所政策

您對主機完整性檢查失敗的用戶端電腦使用隔離所政策，嘗試矯正，然後再次矯正失敗。用戶端電腦矯正失敗之後，會自動切換至隔離所位置，在其中對該電腦套用隔離所政策。請使用隔離所政策對失敗的電腦套用更嚴格的限制。您可以對隔離所政策使用任何類型的保護政策。例如，您可以套用會封鎖電腦對 Internet 之存取權的隔離所防火牆政策。

當用戶端電腦位於隔離所位置時，您可以架構主機完整性檢查來繼續執行並嘗試矯正電腦。您可能也需要手動矯正電腦。

針對失敗的主機完整性檢查建立隔離所政策

1. 在主控台中，按下「用戶端」，再按下「政策」標籤。
2. 在「政策」標籤中，按下「主機完整性檢查失敗時的隔離政策」旁的「新增政策」。
3. 在「新增隔離所政策」對話方塊中，選擇政策類型，然後按「下一步」。
4. 選擇是否使用現有政策、建立新政策或匯入政策檔，然後按「下一步」。
5. 執行下列其中一項工作：
 - 在「新增政策」對話方塊中選擇政策，然後按下「確定」。
 - 在「政策類型」對話方塊中架構政策，然後按下「確定」。
 - 在「匯入政策」對話方塊中，找到 .dat 檔案並按下「匯入」。

更多資訊

- [設定預先定義主機完整性需求的矯正](#)
- [關於主機完整性需求](#)

產生主機完整性檢查失敗的電腦清單

建立「主機完整性」政策以檢查是否通過需求之後，您要知道哪些用戶端的「主機完整性」檢查失敗。例如，您可能想要知道是否已安裝 Microsoft 修正程式。

檢視主機完整性檢查失敗之電腦的報告

1. 在主控台中，按一下「首頁」。
2. 在「端點狀態」底下，按一下「主機完整性失敗」。

此合規性日誌列出了指定時間範圍內的每個主機完整性失敗事件。使用該清單來判斷網路中的哪些裝置仍然需要安裝 Microsoft 修正程式。

產生主機完整性檢查失敗之電腦的清單

1. 在主控台中，按一下「監控」>「日誌」標籤。
2. 在「日誌類型」下拉式清單中，選取「合規性」。
3. 在「日誌內容」下拉式清單中，選取「用戶端主機完整性」。
4. 按下「其他設定」。
5. 調整「時間範圍」。
6. 在「事件類型」下拉式清單中，選取「主機完整性失敗」。
7. 按下「檢視日誌」。

透過架構點對點驗證攔截遠端電腦

您可以使用點對點驗證，允許遠端用戶端電腦（對等者）連線至同一企業網路內的其他用戶端電腦（驗證者）。驗證者會暫時攔截遠端電腦的入埠 TCP 和 UDP 流量，直到遠端電腦通過主機完整性檢查。當遠端電腦實際上在遠端時，您可以使用此強制執行技術。此技術利用 Symantec Endpoint Protection 防火牆的進階功能來增強共用檔案的存取。

主機完整性檢查會驗證遠端電腦的下列特性：

- 遠端電腦已安裝 Symantec Endpoint Protection。
- 遠端電腦已通過主機完整性檢查。

如果遠端電腦通過主機完整性檢查，則驗證者會允許來自遠端電腦的入埠連線。

如果遠端電腦未通過主機完整性檢查，則驗證者會繼續攔截遠端電腦。您可以指定要攔截遠端電腦多久時間，等過了這段時間，才能再次嘗試連線至驗證者。您也可以指定一律允許某些遠端電腦，即使它們無法通過主機完整性檢查。如果您沒有啟用遠端電腦的主機完整性政策，則遠端電腦會通過主機完整性檢查。

點對點驗證資訊會出現在防網路和主機侵入流量日誌中。

NOTE

點對點驗證適用於伺服器控制和混合控制，但不適用於用戶端控制。

透過架構點對點驗證攔截遠端電腦

1. 在主控台中，開啟某個防火牆政策。
2. 在「防火牆政策」頁面上，按一下「點對點驗證設定」。
3. 在「點對點驗證設定」頁面中，勾選「啟用點對點驗證」。
4. 架構頁面上所列的每個值。

如需這些選項的詳細資訊，請按一下「說明」。

5. 若要允許遠端電腦不經驗證就可連線到用戶端電腦，請勾選「從驗證範圍中排除主機」，然後按一下「排除的主機」。

用戶端電腦允許傳送至「主機」清單中所列電腦的流量。

6. 在「排除的主機」對話方塊中，按下「新增」，新增不必經過驗證的遠端電腦。
7. 在「主機」對話方塊中，定義主機的 IP 位址、IP 範圍或子網路，然後按下「確定」。
8. 在「排除的主機」對話方塊中，按下「確定」。
9. 按下「確定」。
10. 如果系統顯示提示，請將政策指派至某個群組。

更多資訊

- [建立防火牆政策](#)
- [設定主機完整性](#)
- [防止使用者在用戶端電腦上停用防護](#)

透過匯入範本建立主機完整性政策需求

使用 Symantec 提供的主機完整性政策需求範本建立 SEP 主機完整性政策需求。

您可以使用提供常用需求的預先定義範本，而非從頭開始建立自訂主機完整性政策需求。主機完整性政策需求定義 (1) SEP 應該檢查的條件，以及 (2) 要在條件失敗時採取的矯正。例如：主機完整性需求是檢查用戶端是否使用最新病毒定義檔。否則，矯正是將含 URL 的電子郵件傳送給用戶端，而使用者可以從此 URL 下載目前病毒定義檔。

若要取得主機完整性政策範本，請透過 LiveUpdate 將主機完整性內容下載至管理伺服器。主機完整性內容包含主機完整性政策需求範本。

NOTE

如果您下載主機完整性政策需求範本，而且存在具有相同名稱的需求，則 SEP 不會覆寫現有需求。相反地，新的需求會出現在「需求」表格上，而且名稱後面會附加數字 2。

透過匯入範本建立主機完整性政策需求

1. 在主控台中，開啟某個主機完整性政策。
2. 在「主機完整性政策」頁面上，按下「需求」>「新增」。
3. 於「新增要求」對話方塊中，按一下「使用現有範本」，然後按一下「確定」。
4. 在「主機完整性線上更新」對話方塊中，於「範本」之下，選取範本類別。
5. 在要新增的每個範本旁邊，按下「新增」。
6. 按下「匯入」。
7. 按下「確定」。

請參閱：

[關於主機完整性需求](#)

撰寫自訂的需求指令碼

自訂需求比預先定義的需求提供更多的彈性。例如，您可以新增預先定義應用程式清單中未納入的應用程式。

若要建立自訂需求，您可以將一或多個函數或 **IF..THEN** 陳述式新增至程序檔。執行指令碼時，「主機完整性」檢查會搜尋 **IF** 節點下列的條件。接著根據該條件，執行 **THEN** 節點下列的動作。最後傳回結果 (pass 或 fail)。

在要檢查的一個指令碼中新增許多不同條件時，這個設定會套用到整個自訂需求指令碼。這個選擇可能會影響您決定是要建立多個小型自訂需求，還是建立包含多個步驟的大型自訂需求。

撰寫自訂的需求指令碼

1. 在主控台中，開啟某個主機完整性政策。
2. 在「主機完整性政策」頁面上，按下「需求」>「新增」。
3. 在「新增需求」對話方塊中，按下「選取需求」下拉式清單，選取預先定義的需求，然後按下「確定」。
4. 在「自訂需求」對話方塊中，輸入需求的名稱。
需求名稱會顯示在用戶端電腦中。名稱會向使用者顯示需求通過與否，或提示使用者下載軟體。
5. 若要新增條件，請在「自訂的需求指令碼」下方，按下「新增」，然後按下 **IF..THEN**。

NOTE

如果您先新增函數或 **IF..THEN** 陳述式但沒有填寫欄位，則會顯示錯誤。如果您不想新增陳述式，請以滑鼠右鍵按一下陳述式，然後按一下「刪除」。

6. 在 **IF** 節點下反白顯示空白條件，然後在右窗格中選取條件。

「主機完整性」檢查會搜尋用戶端電腦上的條件。

7. 在「選取條件」下拉式清單下，指定其他必要的資訊。
8. 在「自訂的需求指令碼」下方，按下 **THEN**，然後按下「新增」。

THEN 陳述式提供條件為 True 時應採取的動作。

9. 按下以下任何選項：

- **IF..THEN**
使用巢狀 **IF..THEN** 陳述式，來定義檢查條件和條件評估為 True 時採取的動作。
- 函數
使用函數定義矯正動作，例如下載檔案。
- 返回
使用傳回陳述式，指定條件評估結果通過或失敗。各個自訂需求的末尾必須是通過或未通過的陳述式。
- 「註解」(選擇性)
使用註解，說明您新增的條件、函數或陳述式等功能。

10. 在右窗格中，定義已新增的條件。

若需這些選項的詳細資訊，請按下「說明」。

11. 若要新增更多的巢狀陳述式、條件或函數，請在「自訂的需求指令碼」下，在節點上按下滑鼠右鍵，然後按下「新增」。
12. 必要時，重複步驟 9 至 11。
13. 若不論結果如何，都要使「主機完整性」檢查通過，請勾選「即使這項要求失敗，也允許主機完整性檢查通過」。
14. 按下「確定」。

更多資訊

- [使用自訂需求程序檔建立測試主機完整性政策](#)
- [將預先定義的需求新增至主機完整性政策](#)

關於登錄條件

您可以指定哪些要檢查的 Windows 登錄設定，作為自訂需求的 **IF..THEN** 陳述式的一部分。此外，還可以指定變更登錄值的方法。只有 `HKEY_CLASSES_ROOT#HKEY_CURRENT_USER#HKEY_LOCAL_MACHINE#HKEY_USERS` 和 `HKEY_CURRENT_CONFIG` 是受支援的登錄設定。

指定登錄機碼時，務必留意下列考量：

- 機碼名稱不可超過 255 個字元。
- 如果登錄機碼末尾含有反斜線 (\)，則被視為登錄機碼。例如：HKEY_LOCAL_MACHINE\SOFTWARE\
- 如果登錄機碼末尾沒有反斜線，則被視為登錄名稱。例如：HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch

指定登錄值時，務必留意下列考量：

- 值名稱不可超過 255 個字元。
- 您可以檢查 DWORD (十進位)、二進位 (十六進位) 或字串形式的值。
- 若是 DWORD 值，您可以檢查值是否低於、等於、不等於或大於指定值。
- 若是字串值，您可以檢查值資料是否等於或包含特定字串。如果您要以區分大小寫的方式進行字串比較，請勾選 [符合大小寫] 核取方塊。
- 若是二進位值，您可以檢查值資料是否等於或包含特定片段的二進位資料。以十六進位元組來表示資料。如果您指定值「包含」，還可指定此資料的位移。如果位移保留空白，則會搜尋特定二進位資料的值。十六進位編輯方塊中允許的值為 0 到 9 以及 a 到 f。

以下是登錄值的範例：

DWORD	12345 (十進位)
二進位	31 AF BF 69 74 A3 69 (十六進位)
字串	ef4adf4a9d933b747361157b8ce7a22f

撰寫要在用戶端執行指令碼的自訂需求

在自訂主機完整性需求中，您可指定函數，讓用戶端執行指令碼。您可以使用程序檔命令語言 (如 JScript 或 VBScript) 來搭配 Microsoft Windows Script Host 執行。

撰寫要在用戶端執行指令碼的自訂需求

1. 在主控台中，開啟某個主機完整性政策。
2. 在「主機完整性政策」頁面上，按下「需求」>「新增」。
3. 在「新增需求」對話方塊中，按下「選取需求」下拉式清單，選取預先定義的需求，然後按下「確定」。請參閱：

撰寫自訂的需求指令碼

4. 在「自訂需求」對話方塊的「自訂的需求指令碼」下方，選取要新增功能的節點。
5. 按下「新增」，再按下「函數」。
6. 按下「公用程式: 執行指令碼」。
7. 輸入指令碼的檔案名稱，例如 `myscript.js`。
8. 輸入指令碼的內容。
9. 在「執行指令」文字欄位中，輸入用來執行指令碼的指令。

使用 %F 來指定指令碼檔案名稱。指令碼會在系統路徑位置執行。

10. 若要指定允許 **Execute** 指令完成的時間長度，請選取下列其中一個選項：

- 不等候
如此一來只要成功執行，動作就會傳回 true，而不會等到完成執行。
- 等候執行完成
- 輸入最長時間
輸入以秒為單位的時間。如果 `Execute` 指令未在指定時間內完成，便會終止檔案的執行。

11. 此外，如果不再需要檔案，您也可以取消勾選「在執行完成或終止之後，刪除暫存檔」。

如果選取「不等候」，則這個選項停用。

12. 此外，您也可以取消勾選「顯示新程序視窗」，表示不要看到視窗顯示執行指令碼的需求。

撰寫要設定檔案時間戳記的自訂需求

在自訂主機完整性需求中，您可以指定「設定時間戳記」函數，以建立 Windows 登錄設定來儲存目前的日期和時間。然後再使用「檢查時間戳記」條件，來檢查建立時間戳記後，是否已經超過了指定的時間長度。

例如，如果主機完整性檢查每 2 分鐘執行一次，您可以指定動作以較長的時間隔 (如一天) 執行。在此情況下，就會移除儲存的時間值。您可以設定指令碼執行如下：

- 當用戶端收到新的設定檔
- 當使用者手動執行主機完整性檢查

撰寫要設定檔案時間戳記的自訂需求

1. 在主控台中，開啟某個主機完整性政策。
2. 在「主機完整性政策」頁面上，按下「需求」>「新增」。
3. 在「新增需求」對話方塊中，按下「選取需求」下拉式清單，選取預先定義的需求，然後按下「確定」。

撰寫自訂的需求指令碼

4. 在「自訂需求」對話方塊的「自訂的需求指令碼」下方，選取要新增功能的節點。
5. 按下「新增」，再按下「函數」。
6. 按下「公用程式: 設定時間戳記」。
7. 針對儲存日期和時間資訊的登錄設定，鍵入名稱，最多 255 個字元。

例如，輸入 `Date and time of last file update:`

比較目前時間與儲存的時間值

1. 撰寫自訂需求指令碼。如需詳細資訊，請參閱：

撰寫自訂的需求指令碼

2. 在「自訂需求」對話方塊的「自訂的需求指令碼」下方，選取要新增條件的節點。
3. 按下「新增」，然後按下 **IF..THEN**。
4. 按下「公用程式: 檢查時間戳記」。
5. 鍵入您之前為所儲存時間登錄設定所輸入的名稱。
6. 指定以分鐘、小時、天或週為單位的時間長度。
如果超過指定的時間長度，或登錄設定值空白，則「設定時間戳記」函數會傳回 True 值。

編寫自訂需求以增加登錄 DWORD 值。

針對自訂需求，您可以增加 Windows 登錄 DWORD 值。如果機碼不存在，「增加登錄 DWORD 值」功能會建立該機碼。

編寫自訂需求以增加登錄 DWORD 值

1. 在主控台中，新增具有自訂需求指令碼的主機完整性政策。請參閱：

撰寫自訂的需求指令碼

2. 在「自訂需求」對話方塊的「自訂的需求指令碼」下方，選取要新增功能的節點。
3. 按下「新增」，再按下「函數」。
4. 按下「登錄: 增加登錄 DWORD 值」。
5. 在「登錄機碼」欄位中輸入要檢查的登錄機碼。
6. 在「值名稱」欄位中輸入要檢查的值名稱。
7. 按下「確定」。

使用自訂需求程序檔建立測試主機完整性政策

您為此測試建立的政策僅用於示範目的。政策會偵測作業系統的存在，且當偵測到時會產生 `fail` 事件。一般來說，`fail` 事件的產生通常是因為其他的原因。

請完成下列工作：

- 使用自訂需求指令碼新增主機完整性政策，該指令碼可檢查用戶端電腦上的作業系統。請參閱：
[使用自訂需求指令碼建立測試主機完整性政策](#)
- 測試已建立的主機完整性政策。請參閱：
[測試用戶端電腦上的主機完整性政策](#)

使用自訂需求指令碼建立測試主機完整性政策

1. 在主控台中，開啟某個主機完整性政策。
 2. 在「主機完整性政策」頁面上，按下「需求」>「新增」。
 3. 在「新增需求」對話方塊中，按下「選取需求」下拉式清單，選取預先定義的需求，然後按下「確定」。
 4. 在「名稱」方塊中，輸入自訂需求的名稱。
 5. 在「自訂需求」對話方塊的「自訂的需求指令碼」下的「在下方插入陳述式」上按下滑鼠右鍵，然後按下「新增 > IF.THEN」。
 6. 在右窗格的「選取條件」下拉式清單中，按下「公用程式: 作業系統是」。
 7. 在「作業系統」下，勾選用戶端電腦所執行且您可以測試的一或多個作業系統。
 8. 在「自訂的需求指令碼」下的「**THEN** //在此插入陳述式」上按下滑鼠右鍵，然後按下「新增 > 函數 > 公用程式: 顯示訊息對話方塊」。
 9. 在「訊息方塊的標題」欄位中，輸入要在訊息標題中顯示的名稱。
 10. 在「訊息方塊的文字」欄位中，輸入您想要訊息顯示的文字。
 11. 在左窗格的「自訂的需求指令碼」下方，按下「通過」。
 12. 在右窗格的「需求結果會傳回」下方，勾選「失敗」，然後按下「確定」。
 13. 按下「確定」。
 14. 在「主機完整性政策」對話方塊的左面板中，按下「指派政策」。
 15. 在「指派主機完整性政策」對話方塊中，選取要指派政策給哪些群組，然後按下「指派」。
- 在「指派主機完整性政策」對話方塊中，按下「是」，指派主機完整性政策的變更。

NOTE

一項主機完整性政策可以指派給多個群組，但一個群組只能具有一項主機完整性政策。您可以用不同的政策來取代現有政策。

-
16. 若要在用戶端電腦上測試主機完整性政策，請按一下「用戶端」>「用戶端」。
 17. 在「用戶端」下方，按下並反白顯示包含您套用主機完整性政策的用戶端電腦的群組。
 18. 在「工作」下方，按下「對群組執行指令 > 更新內容」，然後按下「確定」。
 19. 登入執行用戶端的電腦並注意出現的訊息方塊。

因為規則已觸發 `fail` 測試，所以訊息方塊會出現。測試後，停用或刪除測試政策。

更多資訊

- [撰寫自訂的需求指令碼](#)
- [編寫自訂需求以增加登錄 DWORD 值](#)
- [撰寫要在用戶端執行指令碼的自訂需求](#)

監控 Symantec Endpoint Protection 用戶端

Symantec Endpoint Protection 會收集網路安全性事件的相關資訊。您可以使用日誌和報告檢視這些事件，也可透過通知方式在發生事件時隨時通知您。

您可以使用報告和日誌來判定下列種類問題的答案：

- 哪些電腦已受感染？
- 哪些電腦需要掃描？
- 網路內偵測出哪些風險？

Table 155: 監控端點防護工作

工作	說明
檢閱網路的安全性狀態	下列清單說明了部分您可執行以監控用戶端電腦安全性狀態的工作。 - 檢視未安裝的用戶端數量。請參閱： 執行有關用戶端部署狀態的報告 - 檢視已離線的電腦數量。請參閱： 尋找離線電腦 - 取得已偵測病毒的計數以及其他安全性風險，並檢視各病毒與安全性風險的詳細資料。請參閱： 檢視風險 - 取得網路中未受保護電腦的計數，並檢視每部電腦的詳細資訊。請參閱： 檢視系統防護 - 檢視病毒和間諜軟體定義檔為最新的電腦數量。請參閱： 檢視系統防護 - 檢視用戶端電腦的即時作業狀態。請參閱： 檢視用戶端電腦的防護狀態 - 檢閱網路中執行的程序。請參閱： 監控 SONAR 偵測結果來查看是否有誤報 - 找出哪些電腦已指派至哪些群組。 - 檢視安裝在您網路中的用戶端和 Symantec Endpoint Protection 伺服器上的 Symantec Endpoint Protection Manager 軟體版本清單。請參閱： 產生網路中安裝的 Symantec Endpoint Protection 版本的清單 - 檢視用戶端電腦上的授權資訊，其中包括有效基座個數、已過度部署基座個數、已過期的基座個數，以及到期日。請參閱： 檢查 Symantec Endpoint Protection Manager 中的授權狀態 如需詳細資訊，請參閱： 檢視每日或每週狀態報告 首頁
找出需要保護的用戶端電腦	您可以執行下列工作，檢視或尋找哪些電腦需要額外進行防護： - 檢視已停用 Symantec Endpoint Protection 的電腦數量。請參閱： 檢視系統防護 - 檢視病毒和間諜軟體定義檔已過期的電腦數量。請參閱： 檢視系統防護 - 尋找最近未掃描的電腦。請參閱： 尋找未掃描電腦 - 檢視攻擊目標和來源。請參閱： 檢視攻擊目標和來源 - 檢視事件日誌。請參閱： 檢視日誌
防護您的用戶端電腦	您可以從主控台執行指令，保護用戶端電腦。請參閱： 在用戶端電腦上從主控台執行指令 例如，您可以消除用戶端電腦上的安全風險。請參閱： 檢查掃描動作及重新掃描識別出的電腦
架構通知，以便在發生安全性事件時發出警示。	您可以建立並架構在發生某些安全相關事件時啟動通知。例如，您可以設定用戶端電腦發生入侵嘗試時提出通知。請參閱： 設定管理員通知

工作	說明
為正在進行的監控建立自訂快速報告和排程報告	您可以建立和產生自訂的快速報告，也可以排程含有所要檢視資訊的自訂報告定期執行。請參閱： • 執行和自訂快速報告 • 如何執行排程報告 • 儲存自訂報告 • 架構報告偏好
將用戶端日誌使用的空間量減到最少	基於安全理由，您可能需要將日誌記錄保留一段較長的時間。然而，如果您有許多用戶端，可能會產生大量的用戶端日誌資料。 如果您的管理伺服器空間不夠，您可能需要減少日誌大小，並縮短資料庫保留日誌的時間。 您可以執行下列工作，來減少日誌資料量： • 只將部分用戶端日誌上傳至伺服器，以及變更上傳用戶端日誌的頻率。請參閱： 指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器 • 指定用戶端電腦在資料庫中可保留的日誌項目數，以及可保留多久的時間。請參閱： 指定日誌大小以及在資料庫中保留日誌項目的時間長度 • 過濾掉重要性較低的風險事件和系統事件，減少轉送到伺服器的資料。請參閱： 在 Windows 電腦上修改日誌處理及通知設定 • 減少各管理伺服器所管理的用戶端數目。 • 減少活動訊號頻率，這會控制用戶端日誌多久上傳一次到伺服器。請參閱： 使用推送模式或提取模式更新用戶端上的政策和內容 • 在將日誌資料插入資料庫之前，減少日誌資料所儲存目錄的空間。請參閱： 關於增加用於用戶端日誌資料的伺服器磁碟空間
將日誌資料匯出至集中位置	如果您要在集中的位置存放整個網路的所有日誌，日誌資料匯出會很有用。如果您要使用試算表等第三方程式組織或運用資料，也可以使用日誌資料匯出的方式。您也可能想在刪除日誌記錄之前，先匯出日誌的資料。 您可以將某些日誌中的資料匯出至逗號分隔文字檔。您可以將其他日誌的資料匯出至稱為傾印檔的 Tab 分隔文字檔，或匯出至 Syslog 伺服器。請參閱： • 將日誌資料匯出至文字檔 • 將資料匯出至 Syslog 伺服器 • 檢視其他網站的日誌
使用報告和日誌進行問題疑難排解	您可以使用報告針對部分問題進行疑難排解。請參閱： 報告問題疑難排解

NOTE

Symantec Endpoint Protection 會從管理伺服器上的事件日誌，提取報告中所顯示的事件。事件日誌包含用戶端電腦時區的時間戳記。當管理伺服器收到事件時，會將事件的時間戳記轉換成格林威治標準時間 (GMT)，再插入資料庫中。當您建立報告時，報告軟體會以您檢視報告所在電腦的當地時間，來顯示事件資訊。

尋找未掃描電腦

您可以列出需要掃描的電腦。請參閱：

[監控 Symantec Endpoint Protection 用戶端](#)

尋找未掃描電腦

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤上，指定下列資訊：

報告類型	選取「掃描」。
所選報告	選取「未掃描電腦」。

-
3. 按下「建立報告」。

尋找離線電腦

您可以列出離線的電腦。

用戶端離線的原因有幾個。您可以利用幾種方式來識別離線的電腦並針對這些問題採取補救措施。請參閱：

[Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

尋找離線電腦

1. 在主控台上，按下「首頁」。
2. 在「首頁」頁面的「端點狀態」窗格中，按代表離線電腦數量的連結。
3. 若需離線電腦的更多資訊，請按「檢視詳細資料」連結。

檢視電腦狀態日誌中的離線用戶端電腦

1. 在主控台中，按下「監視器」。
2. 在「日誌」標籤的「日誌類型」清單方塊中，按下「電腦狀態」。
3. 按下「其他設定」。
4. 在「線上狀態」清單方塊中，按下「離線」。
5. 按下「檢視日誌」。
依預設，在過去 24 小時離線的電腦清單會出現。此清單包括每部電腦的名稱、IP 位址以及上次登入其伺服器的時間。您可以調整時間範圍，顯示在您想要查看的任何時間範圍內離線的電腦。

產生網路中安裝的 Symantec Endpoint Protection 版本的清單

您可以從 Symantec Endpoint Protection Manager 執行快速報告，這個報告會提供網路中安裝的 Symantec Endpoint Protection 軟體版本的清單。當您想要從舊版的 Symantec Endpoint Protection 升級或移轉軟體時，此清單可能很實用。此清單包括本機和遠端電腦。

您可以使用 MHTML 網頁封存檔格式儲存此報告。請參閱：

[列印和儲存報告副本](#)

產生列出 Symantec Endpoint Protection 軟體版本的報告

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤的「報告類型」選取「電腦狀態」。
3. 在「選取報告」中，選取「Symantec Endpoint Protection 產品版本」。
4. 按下「建立報告」。

產生詳細的用戶端電腦清單，包括 Symantec Endpoint Protection 軟體版本

1. 在主控台中，按下「監視器」，然後按下「日誌」標籤。
2. 在「日誌類型」中，選取「電腦狀態」。
3. 視需要調整「時間範圍」，然後按下「檢視日誌」。
4. 捲動以尋找「版本」欄。按下標頭，以依版本號碼排序。
按下「檢視套用的過濾器」以調整日誌過濾。按下「匯出」以匯出清單。按下用戶端電腦，然後按下「詳細資料」以查看其詳細資料。

更多資訊

- [檢視日誌](#)
- [選擇升級用戶端軟體的方法](#)
- [Symantec Endpoint Protection 的升級資源](#)

執行有關用戶端部署狀態的報告

您可以執行多個有關您用戶端部署狀態的報告。例如，您可以查看成功或未成功安裝的用戶端數。您也可以查看哪些用戶端上安裝了何種防護技術，以及有關用戶端電腦的系統資訊。請參閱：

[監控 Symantec Endpoint Protection 用戶端](#)

檢視已部署用戶端的狀態

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤上，按下「電腦狀態」報告類型，然後按下其中一個報告：
 - 如需瞭解用戶端的部署狀態，請按下「部署報告」。
 - 如需瞭解用戶端的防護狀態，請按下「用戶端清查詳細資料」。
3. 按下「建立報告」。

檢視風險

產生報告，以取得關於網路風險的相關資訊。

[監控 Symantec Endpoint Protection 用戶端](#)

檢視風險

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤上，按一下「報告類型」下拉式清單，然後選取「風險」。
3. 按一下「所選報告」下拉式清單，然後選取您想要檢視之風險類型的報告。一些建議如下：

風險類型	「所選報告」選項
受感染的端點以及存在風險的端點	受感染和有風險的電腦
更好地瞭解未啟用某些功能的優勢和風險。此報告提供下列資訊： • 以特徵為基礎的病毒和間諜軟體偵測 • SONAR (行為分析) 偵測 • 「下載鑑識」偵測 • 入侵預防和瀏覽器防護偵測	依防護技術顯示風險分佈
新偵測到的風險	網路中偵測到的新風險
綜合風險報告，其中包括多份長期偵測到的風險相關報告。	綜合性風險報告

4. 按下「建立報告」。

檢視攻擊目標和來源

產生報告以取得攻擊目標和其來源的相關資訊。

檢視攻擊目標和來源

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤上，按一下「報告類型」下拉式清單，然後選取「防網路和主機侵入」。
3. 按一下「選取報告」下拉式清單，然後選取您想要產生的報告。一些建議如下：
 - 前幾名遭攻擊目標
 - 前幾名攻擊來源
 - 完整報告
 - 您可以按一下「產生」來選取您想要顯示在完整報告中的詳細資料。
4. 按下「建立報告」。

檢視 Symantec Endpoint Protection 報告

檢視每日或每週狀態報告，隨時瞭解 Symantec Endpoint Protection 發生事項的最新資訊。

「每日狀態報告」可提供下列資訊：

- 採取了已清除、可疑、已攔截、已隔離、已刪除、新感染和仍受感染動作的病毒偵測結果數。
- 病毒定義檔派送時間表
- 前 10 個風險和感染

「每週狀態報告」可提供下列資訊：

- 電腦狀態
- 病毒偵測
- 防護狀態快照
- 病毒定義檔派送時間表
- 依日期顯示風險分佈
- 前 10 個風險和感染

如需詳細資訊，請參閱：

[監控 Symantec Endpoint Protection 用戶端](#)

檢視每日狀態報告

1. 在主控台上，按下「首頁」。
2. 在「首頁」的「我的最愛報告」窗格中，按下「**Symantec Endpoint Protection 每日狀態**」或「**Symantec Endpoint Protection 每週狀態**」。

檢視系統防護

系統防護包含下列資訊：

- 病毒定義檔為最新的電腦數量。
- 病毒定義檔已過期的電腦數量。
- 已離線的電腦數量。
- 已停用的電腦數量。

如需詳細資訊，請參閱：

[監控 Symantec Endpoint Protection 用戶端](#)

檢視系統防護

1. 在主控台上，按下「首頁」。
系統防護顯示於「端點狀態」窗格中。
2. 在「端點狀態」窗格中，按下「檢視詳細資料」以檢視更多的系統防護資訊。

架構報告偏好

您可以架構下列報告偏好：

- 「主頁」和「監視器」頁面顯示選項
- 「安全狀態」臨界值
- 用於日誌和報告以及舊版日誌檔上傳的顯示選項

您設定的安全狀態臨界值，可決定何時將 Symantec Endpoint Protection Manager 的「主頁」的安全狀態訊息視為不良。臨界值是以百分比表示，設定將網路視為違反安全性政策的時機。

例如，您可以設定病毒定義過時的電腦數量百分比，以觸發不良安全性狀態。您也可以設定需要將定義檔視為過期的天數。Symantec Endpoint Protection 會按下列方式，在計算特徵或定義檔是否過期時，判斷哪些項目是最新的。其標準是最新的病毒定義和 IPS 特徵日期，這可以從執行主控台的管理伺服器取得。

如需可設定的喜好設定選項的相關資訊，您可以按一下「喜好設定」對話方塊各個標籤上的「說明」。

架構報告偏好

1. 在主控台的「主頁」上，按一下「喜好設定」。
2. 根據要設定的偏好類型，按下以下其中一個標籤：
 - 首頁和監視器
如需詳細資訊，請參閱：
[偏好：首頁和監視器頁面](#)
 - 安全狀態
如需詳細資訊，請參閱：
[偏好：安全狀態](#)
 - 日誌和報告
如需詳細資訊，請參閱：
[偏好：日誌和報告](#)
3. 設定要變更的選項值。
4. 按下「確定」。

從獨立式網頁瀏覽器登入報告

您可以從與您的管理伺服器連線的獨立式網頁瀏覽器，存取「首頁」、「監視器」和「報告」頁面。然而，使用獨立式瀏覽器時，所有其他主控台功能都無法使用。

報告頁面和日誌頁面通常會以安裝管理伺服器時所用的語言顯示。若要在使用遠端主控台或瀏覽器時顯示這些頁面，您必須在所使用的電腦上安裝適當的字型。

若要從網頁瀏覽器存取報告，您必須具備下列資訊：

- 管理伺服器的主機名稱。
- 管理伺服器的使用者名稱和密碼。

NOTE

針對支援正在使用的 Symantec Endpoint Protection 版本的最低瀏覽器版本檢查系統需求。不支援更低的網頁瀏覽器版本。請參閱：

[所有 Endpoint Protection 版本的版本說明、新修正和系統需求](#)

從獨立式網頁瀏覽器登入報告

1. 開啟網頁瀏覽器。
2. 按照以下格式，在位址文字方塊中輸入預設的報告 URL：

`https://SEPMServer:8445/reporting`

其中 SEPMServer 是管理伺服器的主機名稱或 IP 位址。

如需受支援網頁瀏覽器的清單，請參閱：

[所有 Endpoint Protection 版本的版本說明、新修正和系統需求](#)

IP 位址包括 IPv4 和 IPv6。必須用方括弧括住 IPv6 位址。例如：`https://[SEPMServer]:8445`

自 14.2 版起支援 IPv6。

NOTE

在瀏覽器中輸入 HTTPS 獨立式報告 URL 時，瀏覽器可能會顯示警告。出現警告是因為管理伺服器使用自我簽署憑證。若要解決這個問題，您可以在瀏覽器的信任憑證儲存區中安裝憑證。憑證僅支援主機名稱，所以請在 URL 中使用主機名稱。如果使用 localhost、IP 位址或完整網域名稱，警告還是會出現。

3. 當出現登入對話方塊時，請輸入您的使用者名稱和密碼，然後按下「登入」。

如果您使用超過一個網域，請在「網域」文字方塊中鍵入您的網域名稱。

關於 Symantec Endpoint Protection Manager 報告類型

以下是可用的報告類別：

- 快速報告，可視需要執行。
- 排程報告，根據您架構的排程自動執行。

報告包含從您的管理伺服器以及與這些伺服器通訊的用戶端電腦收集到的事件資料。您可以自訂報告來提供想要檢視的資訊。

快速報告是預先定義的報告，不過您可以自訂這些報告，並儲存用來建立自訂報告的篩選條件。您可以使用自訂過濾條件建立自訂排程報告。當您排程要執行的報告時，可以架構它以電子郵件傳送給一或多個收件者。

排程報告預設通常為執行。您可以針對尚未執行的任何排程報告變更此設定。您也可以刪除單一或所有排程報告。

Table 156: 可作為快速報告和排程報告的報告類型

報告類型	說明
稽核	顯示用戶端和位置目前使用之政策的相關資訊。此報告包含關於政策修改活動的資訊，如事件時間和類型、政策修改、網域、站台、管理員以及敘述。請參閱： 稽核日誌和快速報告
應用程式與裝置控制	顯示攔截某些類型行為之事件的相關資訊。這些報告包括應用程式安全性警示、攔截的目標及攔截的裝置等相關資訊。攔截的目標可能是 Windows 登錄機碼、DLL、檔案和程序。請參閱： 應用程式與裝置控制日誌和快速報告
合規性	顯示已通過或未通過主機完整性檢查之用戶端數量的相關資訊。
電腦狀態	顯示網路中電腦作業狀態 (例如哪些電腦關閉了安全功能) 的相關資訊。這類報告包括有關版本、尚未登入伺服器的用戶端、用戶端清查及線上狀態等的資訊。請參閱： 電腦狀態日誌和報告
防網路和主機侵入	顯示入侵預防、防火牆攻擊、防火牆流量和封包以及記憶體攻擊緩和的相關資訊。 「防網路和主機侵入」報告可以追蹤電腦活動，以及該電腦與其他電腦及網路的互動狀況。其記錄的資訊包括嘗試透過網路連線進出電腦的流量。記憶體攻擊緩和事件列出了終止應用程式或攔截攻擊以防止其攻擊應用程式的緩和技術。請參閱： 防網路和主機侵入日誌和快速報告
風險	顯示管理伺服器及其用戶端上風險事件的相關資訊。其包含有關行為分析 (SONAR) 掃描的資訊。請參閱： 風險日誌和快速報告 SONAR：行為分析日誌
掃描	顯示病毒和間諜軟體掃描活動的相關資訊。請參閱： 掃描日誌和快速報告

報告類型	說明
系統	顯示事件時間、事件類型、站台、網域、伺服器及嚴重性等級等的相關資訊。「系統」報告包含有助於疑難排解用戶端問題的資訊。請參閱： 系統日誌和快速報告

如果您的網路包含多個網域，多個報告可讓您檢視所有網域、單一或數個站台的資料。所有快速報告均預設為顯示適用於您選取要建立之報告的所有網域、群組、伺服器。請參閱：

- [執行和自訂快速報告](#)
- [如何執行排程報告](#)

下一節依照名稱及其一般內容來說明報告。您可以針對所有報告架構「基本設定」和「進階設定」，以精簡所要檢視的資料。您也可以命名並儲存自訂過濾器，以便日後執行相同的自訂報告。

Table 157: 稽核報告

報告名稱	說明
使用的政策	此報告顯示用戶端和位置目前所使用的政策。此項資訊包含網域名稱、群組名稱，以及套用於各個群組的政策序號。

Table 158: 應用程式與裝置控制報告

報告名稱	說明
含最多警示的前幾名群組	此報告由一個圓形圖與一些相對長條組成。它會顯示含應用程式控制日誌的群組，這些日誌已產生大量的安全警示。
前幾名被攔截目標	此報告由一個圓形圖與下列目標 (如果有) 組成： • 前幾名檔案 • 前幾名登錄機碼 • 前幾名程序 • 前幾名模組 (dll)
前幾名被攔截裝置	此報告由一個圓形圖組成，會顯示最常被攔截而不能存取網路的裝置。

Table 159: 合規性報告

報告名稱	說明
主機完整性狀態	此報告顯示通過或未通過電腦上所執行主機完整性檢查的用戶端。
按遵從失敗摘要的用戶端	此報告由一個長條圖組成，其中顯示： • 按控制失敗事件的類型 (例如防毒、防火牆或 VPN) 列出的唯一工作站計數 • 群組內的用戶端總數
遵從失敗詳細資料	此報告由一個表格組成，會按控制失敗顯示唯一電腦。它會顯示每個失敗中涉及的準則和規則，以及已部署的用戶端百分比和失敗的百分比。
按位置的非遵從用戶端	此報告由一個表格組成，會顯示合規性失敗事件。這些事件會按其位置顯示在群組中。此項資訊包括失敗的唯一電腦，以及失敗總計百分比和位置失敗百分比。

Table 160: 電腦狀態報告

報告名稱	說明
病毒定義檔派送	此報告顯示用於整個網路的唯一病毒定義檔版本，以及使用每種定義檔版本的電腦數量和百分比。
最近未更新的電腦	此報告顯示最近未更新的所有電腦清單。它也會顯示電腦的作業系統、IP 位址、使用者名稱和上次變更其狀態的時間。
Symantec Endpoint Protection 產品版本	此報告顯示網路中所有 Symantec Endpoint Protection 產品版本的版本號碼清單。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
入侵預防特徵分佈	此報告顯示用於整個網路的 IPS 特徵檔案版本。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
下載防護特徵分佈	此報告顯示用於整個網路的下載防護特徵檔案版本。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
SONAR 特徵分佈	此報告顯示用於整個網路的 SONAR 特徵檔案版本。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
用戶端清查	此報告由一個長條圖組成，會顯示每一項的電腦總數和百分比： - 作業系統 - 總記憶體 - 可用記憶體 - 總計磁碟空間 - 可用磁碟空間 - 處理器類型
遵從狀態分佈	此報告由一個圓形圖與一些相對長條組成，這些長條會按群組或按子網路顯示合規性通過和未通過情況。它會顯示合規的電腦數量和百分比。
用戶端線上狀態	此報告由一些圓形圖及對應於每個群組或每個子網路的相對長條組成。它會顯示線上的電腦百分比。線上具有下列意義： - 若是推送模式下的用戶端，線上代表用戶端目前已連線至伺服器 - 若是提取模式下的用戶端，線上代表用戶端在最後兩個用戶端活動訊號期間內，已連上伺服器 - 若是遠端據點中的用戶端，線上代表用戶端在上次遠端複製時處於線上狀態
有最新政策的用戶端	此報告由對應於每個群組或每個子網路的圓形圖組成。它會顯示套用最新政策的電腦數量和百分比。
依群組顯示用戶端數目	此報告由一個表格組成，會按群組列出主機資訊。它會顯示用戶端和使用者數量。如果您使用多個網域，此項資訊會按網域顯示。
安全狀態摘要	此報告會反映網路的一般安全狀態，並顯示有下列狀態的電腦數量和百分比： - 防毒引擎關閉 - 自動防護關閉 - 竊改防護關閉 - 需要重新啟動 - 主機完整性檢查失敗 - 網路威脅防護關閉
防護內容版本	此報告顯示用於整個網路的所有主動型防護內容版本。針對下列每種防護類型，會顯示一個圓形圖： - 分解程式版本 - Eraser 引擎版本 - SONAR 內容版本 - SONAR 引擎版本 - 商用應用程式清單版本 - 內容處理引擎版本 - 允許的應用程式清單版本 - 賽門鐵克安全機制應變中心已新增的內容類型

報告名稱	說明
Symantec Endpoint Protection 授權狀態	此報告包含試用授權到期的天數以及新增授權的指示。
用戶端清查詳細資料	此報告包含用戶端清查的詳細資料，例如電腦規格和特徵。
用戶端軟體首展 (快照) 僅限排程報告	此報告由一個表格組成，用於追蹤用戶端套件部署進度。快照資訊可讓您瞭解遞送的進度情況，以及尚未完全部署的用戶端數量。
某段時間內的用戶端線上/離線 (快照) 僅限排程報告	此報告由折線圖和表格組成，會顯示線上或離線的用戶端數量。針對每個前幾項目標顯示一個圖表。目標是群組或作業系統。
某段時間內有最新政策的用戶端 (快照) 僅限排程報告	此報告由一個折線圖組成，會顯示已套用最新政策的用戶端。對於每個前幾名用戶端顯示一個圖表。
某段時間內的非遵從用戶端 (快照) 僅限排程報告	此報告由一個折線圖組成，會顯示某段時間內未通過主機完整性檢查的用戶端百分比。對於每個前幾名用戶端顯示一個圖表。
病毒定義檔首展 (快照) 僅限排程報告	此報告會列出已遞送到用戶端的病毒定義檔套件版本。此項資訊有助於從主控台追蹤新病毒定義檔的部署進度。
部署報告	此報告摘要說明了用戶端安裝和部署的狀態。

Table 161: 防網路和主機侵入報告

報告名稱	說明
前幾名遭攻擊目標	包括攻擊數量和百分比、攻擊類型和嚴重性以及攻擊分佈等資訊。您可以使用群組、子網路、用戶端或通訊埠作為目標來檢視資訊。
前幾名攻擊來源	顯示對您網路發動攻擊的前幾部主機。它包括攻擊數量和百分比、攻擊類型和嚴重性及攻擊分佈等資訊。
前幾名攻擊類型	包括事件數量和百分比、群組和嚴重性以及按群組的事件類型和數量等資訊。
前幾名攔截的應用程式	顯示遭攔截而無法存取您網路的前幾個應用程式。它包括攻擊數量和百分比、群組和嚴重性及按群組的事件類型和數量等資訊。
某段時間內的攻擊	顯示所選時段內的攻擊。例如，如果時間範圍是上個月，則報告會顯示上個月每天的攻擊總數。它會包括攻擊的數量和百分比。您可以檢視所有電腦的攻擊情況，或是按前幾名作業系統、使用者、IP 位址、群組或攻擊類型進行檢視。
依嚴重性顯示安全性事件	顯示網路中按嚴重性分級之安全事件的總數和百分比。
某段時間內攔截的應用程式	顯示在您選取的時段內遭攔截而無法存取您網路的應用程式總數。它包括事件時間、攻擊數量和百分比。您可以顯示所有電腦的資訊，或是按群組、IP 位址、作業系統或使用者來顯示資訊。
某段時間內的流量通知	顯示某段時間內基於防火牆規則違規的通知數量。計入的規則就是您在「防火牆政策規則」清單的「記錄」欄位中已勾選「傳送電子郵件警示」選項的規則。您可以在此報告中，顯示所有電腦的資訊，或是按群組、IP 位址、作業系統或使用者來顯示資訊。
前幾名流量通知	列出群組或子網路，以及通知數量和百分比。它會顯示根據您架構為務必通知之防火牆規則違規情況所產生的通知數。計入的規則就是您在「防火牆政策規則」清單的「記錄」欄位中已勾選「傳送電子郵件警示」選項的規則。您可以檢視按前幾名群組或子網路分組的全部、流量日誌或封包日誌的資訊。
記憶體攻擊緩和偵測	顯示已攔截或允許的記憶體攻擊緩和類型的數量。
熱門 URL 偵測	列出 URL 信譽所攔截的 URL。
完整報告	列出單一報告中的前幾個「網路威脅防護」項目。

Table 162: 風險報告

報告名稱	說明
受感染和處於風險的電腦	此報告由兩個表格組成。其中一個表格會列出有病毒感染的電腦，而另一個表格會列出有尚未矯正之安全風險的電腦。
動作清單	此報告由一個表格組成，會顯示偵測到風險時可能採取的所有動作數量。可能的動作有「已清除」、「可疑」、「已攔截」、「已隔離」、「已刪除」、「擱置修復」、「已記錄商用或強制偵測」、「新感染」和「仍受感染」。此資訊也會顯示在 Symantec Endpoint Protection 首頁上。
風險偵測數目	此報告由一個圓形圖、一個風險表格以及一個相關相對長條組成。它會按網域、伺服器或電腦顯示風險偵測數量。如果您用的是舊版 Symantec AntiVirus 用戶端，則此報告會使用伺服器群組，而非網域。
網路中偵測到的新風險	此報告由一個表格和一個分佈圓形圖組成。針對每一個新風險，表格會提供下列資訊： - 風險名稱 - 風險類別或類型 - 第一次搜尋到的資料 - 組織中的第一次發生 - 最先偵測到它的掃描類型 - 發現它時它所在的網域 (舊版電腦上為伺服器群組) - 發現它的伺服器 (舊版電腦上的父系伺服器) - 發現它的群組 (舊版電腦上為父系伺服器) - 發現它的電腦，以及當時登入的使用者名稱 圓形圖會按目標選取類型顯示新風險分佈：網域 (舊版電腦上為伺服器群組)、群組、伺服器 (舊版電腦上為父系伺服器)、電腦或使用者名稱。
前幾名風險偵測交叉比對	此報告由一個 3D 長條圖組成，透過兩個變數將病毒和安全風險偵測進行交叉比對。您可以選取電腦、使用者名稱、網域、群組、伺服器或風險名稱，作為 x 和 y 軸變數。此報告會顯示每個座標軸變數的前五個實例。如果您已選取電腦為變數之一，而受感染的電腦少於 5 部，則圖中可能顯示未感染的電腦。 Note: 對於執行舊版 Symantec AntiVirus 的電腦，會使用伺服器群組和父系伺服器，而不是網域和伺服器。
下載風險分佈	此報告顯示下載鑑識所偵測到的檔案數量，並按敏感程度進行分組。會向找到的檔案提供詳細報告。您也可以執行報告之前，按 URL、Web 網域、應用程式和使用者允許的方式分組檔案。
風險分佈摘要	此報告由一個圓形圖和一個相關長條圖組成，會顯示所選目標類型中每個唯一項目的相對百分比。例如，如果選擇的目標是風險名稱，則圓形圖會顯示每個唯一風險的切片。每個風險名稱會顯示一個長條，詳細資料包括偵測數目及其佔偵測總數的百分比。
某段時間內的風險分佈	此報告由一個表格及一個相對長條組成，表格會顯示單位時間內偵測到病毒和安全風險數量。
依防護技術顯示風險分佈	此報告顯示每個防護技術的病毒和安全風險偵測數量。
SONAR 偵測結果	此報告由一個圓形圖和一些長條圖組成，會顯示下列資訊： - 標記為風險但您已經將其新增至網路中允許的例外的應用程式清單 - 已偵測到並確認為風險的應用程式清單 - 已偵測到但風險狀態仍待確認的應用程式清單 每份清單上，此報告都顯示公司名稱、應用程式雜湊及版本，以及涉及到的電腦。對於允許的應用程式，此報告還會顯示允許的來源。
SONAR 威脅分佈	以數個相對長條和一個摘要表格顯示偵測出的前幾名應用程式名稱。這些偵測包括「商用應用程式清單」和「強制偵測」清單上的應用程式。第一個摘要表格包含應用程式名稱以及偵測數目和百分比。
某段時間內的 SONAR 威脅偵測	此報告由一個折線圖組成，會顯示所選時間範圍內的主動型威脅偵測數目。它也包含具有相對長條的表格，會列出某段時間內偵測出的威脅總數。
前幾名風險的動作摘要	此報告會列出網路中發現的前幾名風險。對於每個風險，此報告都會顯示動作摘要長條，會顯示偵測到風險時所採取的每項動作百分比。動作包括「已隔離」、「已清除」、「已刪除」等。此報告也會顯示每一個特定動作為第一個架構的動作、第二個架構的動作、兩者皆非或不明的時間百分比。
通知數	此報告由一個圓形圖以及一個相關相對長條組成。圖表會顯示根據您架構為務必通知之防火牆規則違規情況所觸發的通知數。它會包括每個通知的類型和數量。

報告名稱	說明
某段時間內的通知數	此報告由一個折線圖組成，會顯示所選時間範圍內網路中的通知數。它也包含一個表格，會列出某段時間內的通知數和百分比。您可以過濾資料，使其按通知類型、確認狀態、建立者和通知名稱顯示。
每週爆發	此報告顯示指定時間範圍內每週偵測到病毒和安全風險的數目以及相對長條。時間範圍為一天時，會顯示過去一週的情況。
綜合性風險報告	此報告預設會包含所有的分佈報告和新風險報告。不過，您可以將其架構為僅包含特定的報告。此報告包括所有網域的資訊。
Symantec Endpoint Protection 每日狀態	此報告包含過去 24 小時內網路事件的病毒偵測情況、介入情況和定義狀態。
Symantec Endpoint Protection 每週狀態	此報告包含過去一週內端點電腦的授權狀態和病毒偵測統計資料。除非另有說明，資料反映的是累計值。

Table 163: 掃描報告

報告名稱	說明
掃描統計長條圖	此報告由一個長條圖組成，您可以在這裡選取掃描中的下列資訊的分佈方式： - 按掃描時間 (秒) - 按偵測到的風險數 - 按具有偵測的檔案數 - 按掃描的檔案數 - 按掃描時省略的檔案數 您也可以架構 Bin 寬度和長條圖中使用的 Bin 數目。Bin 寬度是用於選定群組的資料間隔。Bin 數目則會指定長條圖重複幾次資料間隔。 顯示的資訊包括項目數、最大值和最小值，以及平均值和標準誤差。 您可能會想要變更報告值，以使報告長條圖中產生大量的資訊。例如，您可能會想要考慮所檢視的網路規模和資訊量。
依上次掃描時間顯示電腦	此報告按上次掃描時間顯示安全網路內的電腦清單。它也包含 IP 位址和掃描時登入的使用者名稱。
未掃描電腦	此報告顯示安全網路中尚未掃描的電腦清單，並提供下列資訊： - IP 位址 - 上次掃描的時間 - 目前使用者或上次掃描時登入的使用者的名稱

Table 164: 系統報告

報告名稱	說明
產生錯誤的前幾名用戶端	此報告由一個圓形圖組成，會顯示每個警告狀況和錯誤狀況。圖表會按用戶端顯示相對錯誤數和相對警告數及百分比。
產生錯誤的前幾名伺服器	此報告由一個圓形圖組成，會顯示每個警告狀況和錯誤狀況。圖表會按伺服器顯示相對錯誤數和相對警告數及百分比。
某段時間內的資料庫複寫失敗	此報告由一個折線圖與一個相關表格組成，會列出所選時間範圍內的遠端複製失敗。
網站狀態報告	此報告會顯示所有網站運作狀態的即時摘要，以及本機網站上所有伺服器的相關資訊。
網路整合 Token 使用情況	此報告摘要說明使用 Web 和雲端存取防護 進行用戶端驗證的整合 Token 使用情況。

執行和自訂快速報告

快速報告係指預先定義的自訂報告。這些報告包含從您的管理伺服器以及與這些伺服器通訊的用戶端電腦收集到的事件資料。快速報告可根據您為報告架構的特定設定提供關於事件的資訊。您可以儲存報告設定，以便日後可執行相同的報告，並且可以列印和儲存報告。

快速報告屬於靜態報告，可根據您在報告中指定的時間範圍提供特定資訊。您也可以利用日誌即時監控各個事件。

執行快速報告

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤的「報告類型」清單方塊中，選取要執行的報告類型。
3. 在「選取報告」清單方塊中，選取要執行的報告名稱。
4. 按下「建立報告」。

自訂快速報告

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤的「報告類型」清單方塊中，選取要自訂的報告類型。
3. 在「選取報告」清單方塊中，選取要自訂的報告名稱。
4. 在「使用儲存的過濾」清單方塊中，選取要使用的儲存過濾架構，或使用預設過濾。
5. 在「您要使用什麼過濾設定？」的「時間範圍」清單方塊中，選取報告的時間範圍。
6. 如果您已選取「設定特定日期」，則使用「開始日期」和「結束日期」清單方塊。這些選項可設定您要檢視資訊的時間間隔。
產生電腦狀態報告後選取「設定特定日期」，您可指定檢視自日期和時間欄位指定時間後，尚未登記於伺服器的電腦的所有相關項目。
7. 如果您要架構報告的其他設定，請按下「其他設定」，並設定您想要的選項。
您可以按下「更多相關資訊」，以檢視上下文關聯說明的過濾選項敘述。

NOTE

過濾選項文字方塊，接受萬用字元，並可不區分大小寫搜尋相符項目。ASCII 星號字元是唯一可當做萬用字元使用的星號字元。

如果您日後要再次執行此報告，則可以儲存報告架構設定。

8. 按下「建立報告」。

更多資訊

- [儲存自訂報告](#)
- [列印和儲存報告副本](#)
- [如何執行排程報告](#)

使用過濾器建立自訂報告

您可以將自訂設定儲存為快速報告和排程報告的過濾條件，以便日後再次產生相同的報告。儲存設定時，設定會儲存到資料庫中。您提供給過濾的名稱會顯示在適用於該類型之日誌和報告的「使用儲存的過濾」清單方塊中。

NOTE

您儲存的過濾架構設定僅供您的使用者登入帳戶使用。其他具有報告權限的使用者無法存取您儲存的設定。

您可以刪除您所建立的任何報告架構。刪除架構後，您就無法再使用該過濾器。

NOTE

如果您刪除管理員，管理伺服器會自動儲存被刪除的管理員所建立的過濾器。過濾器的擁有權和報告名稱皆會變更。新報告名稱的格式為 `OriginalName('AdminName')`。例如，由管理員 JSmith 建立名為 `Monday_risk_reports` 的報告，會重新命名為 `Monday_risk_reports(JSmith)`。在較舊版本中，系統不會儲存已刪除的管理員所建立的任何自訂過濾器。

如需詳細資訊，請參閱：

關於管理員帳戶和存取權限

儲存自訂報告

1. 在主控台中，按下「報告」。
2. 在「快速報告」標籤中，從清單方塊選擇一項報告類型。
3. 變更報告的任何基本設定或其他設定。
4. 按一下「儲存過濾器」。
5. 在「過濾器名稱」文字方塊中，輸入此報告過濾的敘述性名稱。過濾器新增至「使用儲存的過濾」清單時，系統只會顯示該名稱的前 32 個字元。
6. 按一下「確定」。
7. 當出現確認對話方塊時，按一下「確定」。

在您儲存過濾之後，該過濾會顯示在適用於相關報告和日誌的「使用儲存的過濾」清單方塊中。

新增並執行排程報告

排程報告是指根據您所架構之排程自動執行的報告。排程報告會以電子郵件形式傳送給收件者，因此您必須加入至少一位收件者的電子郵件地址。執行報告之後，該報告會以 .mht 檔案附件形式由電子郵件傳送給您所架構的收件者。

排程報告中所顯示的資料每小時都會在資料庫中進行更新。當管理伺服器以電子郵件傳送排程報告時，報告中的資料是一小時內的新資料。

含某段時間內資料的其他報告會根據您針對用戶端日誌所架構的上傳間隔，在資料庫中進行更新。請參閱：

指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器

NOTE

如果您在站台中有多個伺服器共用資料庫，則只有第一個安裝的伺服器會執行針對該站台所排程的報告。此預設可以確保站台中的所有伺服器不會同時執行相同的排程掃描。若要指定不同的伺服器來執行排程報告，則可以在本機站台屬性中架構此選項。

若要新增並執行排程報告

1. 在主控台中，按下「報告」。
2. 在「排程報告」標籤上，按下「新增」。
3. 在「報告名稱」文字方塊中，鍵入描述性名稱，並選擇是否鍵入較長的敘述。

雖然您可以將 255 個以上字元的內容貼到「敘述」文字方塊中，但敘述中只會儲存 255 個字元。

-
4. 若您不要在下次之前執行此報告，可取消勾選「啟用此排程報告」核取方塊。
 5. 從清單方塊選取您要排程的報告類型。
 6. 從清單方塊選取您要排程的特定報告名稱。
 7. 從清單方塊選取您要使用之儲存的過濾名稱。
 8. 在「執行一次每隔」文字方塊中，選取您要以電子郵件形式傳送報告給收件者的時間間隔 (時數、天數、週數、月數)。然後輸入您選取的時間間隔值。例如，如果您要每隔一天傳送報告，請選取天數，然後輸入 2。
 9. 在「在以下時間後開始」文字方塊中，鍵入您要開始執行報告的日期，或者按下行事曆圖示，然後選取日期。然後從清單方塊選取小時和分鐘。
 10. 在「報告收件者」下方，鍵入電子郵件地址，多個地址則請以逗號分隔。
您必須設定郵件伺服器屬性，電子郵件通知才會生效。
 11. 按一下「確定」。

列印和儲存報告副本

儲存的檔案或印出的報告均提供報告資料庫中現有資料的快照，因此，您可以保有先前的記錄。如果稍後再以相同的過濾架構執行相同的報告，新報告會顯示不同的資料。

版本 16 刪除了「列印」和「儲存」按鈕。相反地，請從 Web 瀏覽器列印或儲存快速報告。您無法列印排程報告。

檢視日誌

您可以選取一組過濾設定，再根據這些設定從日誌產生要檢視的事件清單。

NOTE

檢視含大量資料的日誌，而收到資料庫錯誤時，您可能要變更資料庫逾時參數。

如果收到 CGI 或終止程序錯誤，您可能要變更其他逾時參數。

如需詳細資訊，請參閱：

[變更檢視報告和日誌的逾時參數](#)

報告和日誌始終會以安裝管理伺服器時所用的語言顯示。若要在使用遠端 Symantec Endpoint Protection Manager 主控台或瀏覽器時顯示這些項目，您必須在所使用的電腦上安裝適當的字型。請參閱：

- [關於 Symantec Endpoint Protection Manager 日誌類型](#)
- [使用過濾儲存和刪除自訂日誌](#)

檢視日誌

1. 在主控台中，按下「監視器」。
2. 在「日誌」標籤的「日誌類型」清單方塊中，選取您要檢視的日誌類型。
3. 對於某些類型的日誌，會顯示「日誌內容」清單方塊。如果顯示此方塊，請選取您要檢視的日誌內容。
4. 在「使用儲存的過濾」清單方塊中，選取儲存的過濾，或保留「預設」值。
5. 從「時間範圍」清單方塊選取時間，或保留預設值。如果您選取「設定特定日期」，請設定您要顯示哪個或哪些日期和時間之後的項目。
6. 按下「其他設定」，限制顯示的項目數。
您也可以針對所選的日誌類型，設定任何其他可用的「其他設定」。

NOTE

接受萬用字元和搜尋相符項目的篩選選項欄位不區分大小寫。ASCII 星號字元是唯一可當做萬用字元使用的星號字元。

7. 按下「檢視日誌」。

也可以按下「儲存過濾」儲存過濾組態，以便日後產生相同的日誌檢視。

關於 Symantec Endpoint Protection Manager 日誌類型

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記錄，這些記錄稱為事件。日誌會顯示這些事件以及所有相關的其他資訊。安全性相關活動包括病毒偵測、電腦狀態，以及進出用戶端電腦流量的相關資訊。

日誌很重要，可以追蹤每一用戶端電腦的活動，及其與其他電腦和網路互動的情形。可以使用這些資料分析網路的整體安全狀態，並修改用戶端電腦上的防護。您可以追蹤與病毒、安全風險和攻擊相關的趨勢。當多人共用一部電腦時，您可能可以識別引入風險的人員，並協助其採取更好的預防措施。

您可以在 [監視器] 頁面的 [日誌] 標籤上檢視日誌資料。

管理伺服器會定期將用戶端中的日誌資訊上傳到管理伺服器。您可以在日誌或報告中檢視這些資訊。由於報告是靜態的，其所包括的詳細資料沒有日誌裡那麼多，因此您可能傾向於使用日誌來監控網路。

除了使用日誌來監控網路，您還可以從各種日誌中採取以下動作：

- 在用戶端電腦上執行指令。請參閱：
[在用戶端電腦上從主控台執行指令](#)
- 新增多種類型的例外。請參閱：
[從日誌事件建立例外](#)
- 從 [隔離所] 刪除檔案。請參閱：
[管理 Windows 用戶端的隔離所](#)

下表說明您可檢視的不同類型內容，以及您可從各個日誌採取的動作。

Table 165: 日誌類型

日誌類型	內容和動作
稽核	「稽核」日誌包含政策修改活動的資訊。 提供的資訊包括事件時間和類型、修改的政策、相關網域、站台和使用者名稱，以及敘述。 此日誌沒有任何關聯的動作。 如需詳細資訊，請參閱： 稽核日誌和快速報告
應用程式與裝置控制	應用程式控制日誌和裝置控制日誌包含有關某類行為遭攔截的事件資訊。 下列應用程式與裝置控制日誌可供使用： • 應用程式控制，包含「竄改防護」資訊 • 裝置控制 提供的資訊包括事件發生的時間、採取的動作，以及相關的網域和電腦。此外，還包括相關的使用者、嚴重性、相關的規則、呼叫者程序以及目標。 您可以透過「應用程式控制」日誌建立應用程式控制或竄改防護例外。 如需詳細資訊，請參閱： • 建立應用程式例外 • 應用程式與裝置控制日誌和快速報告

日誌類型	內容和動作
合規性	遵從日誌包含用戶端「主機完整性」的相關資訊。 這些日誌沒有任何關聯的動作。 如需詳細資訊，請參閱： 合規性日誌和快速報告
電腦狀態	「電腦狀態」日誌包括網路用戶端電腦的即時作業狀態資訊。 提供的資訊包括電腦名稱、IP 位址、受感染狀態、防護技術、自動防護狀態、版本和定義檔日期。此外，也包括使用者、上次登入時間、政策、群組、網域，以及需要重新啟動狀態。 您可以從此日誌清除受感染電腦狀態。 Note: 此日誌包含同時從 Windows 用戶端和 Mac 用戶端收集的資訊。 如需詳細資訊，請參閱： 電腦狀態日誌和報告
防網路和主機侵入	防網路和主機侵入日誌包含入侵預防、防火牆與記憶體攻擊緩和的相關資訊。 這些日誌包含有關防火牆和入侵預防所受之攻擊的資訊。提供的資訊包括服務阻斷攻擊、通訊埠掃描，以及針對執行檔進行的變更。其中還包含有關通過防火牆的連線 (流量) 以及通過的資料封包的資訊。這些日誌也包含針對電腦進行的某些作業變更，例如偵測網路應用程式，以及架構軟體。 如需詳細資訊，請參閱： 防網路和主機侵入日誌和快速報告
SONAR：行為分析	行為分析 (先前稱為 SONAR) 日誌包含行為分析威脅掃描期間所偵測到威脅的相關資訊。這些是即時掃描，可以偵測在您的用戶端電腦上執行的潛在惡意應用程式。 資訊包括發生時間、事件實際動作、使用者名稱、網域、應用程式、應用程式類型、檔案和路徑等項目。 如需詳細資訊，請參閱： • SONAR：行為分析日誌 • 何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？
風險	「風險」日誌包含風險事件的資訊。其中提供的資訊包括事件時間、事件實際動作、使用者名稱、電腦和網域、風險名稱和來源、計數，以及檔案和路徑。 如需詳細資訊，請參閱： 風險日誌和快速報告
掃描	掃描日誌包含來自 Windows 用戶端和 Mac 用戶端的病毒和間諜軟體掃描活動相關資訊。 日誌提供的資訊包括開始掃描、電腦、IP 位址、狀態、持續時間、偵測、掃描、省略以及網域等項目。 這些日誌沒有任何關聯的動作。 如需詳細資訊，請參閱： 掃描日誌和快速報告
系統	系統日誌包含事件的相關資訊，例如服務何時啟動和停止。 這些日誌沒有任何關聯的動作。 如需詳細資訊，請參閱： 系統日誌和快速報告

使用過濾儲存和刪除自訂日誌

您可以使用「基本設定」和「其他設定」架構自訂過濾，來變更所要查看的資訊。您可以將自己的過濾設定儲存到資料庫，以便日後再次產生相同的檢視。儲存設定時，設定會儲存到資料庫中。您提供給過濾的名稱會顯示在適用於該類型之日誌和報告的「使用儲存的過濾」清單方塊中。

NOTE

如果您選取「過去 24 小時」作為報告過濾的時間範圍，則 24 小時的時間範圍會從您首次選取過濾時開始算起。如果您重新整理頁面，並不會重設 24 小時範圍的開始時間。如果您選取過濾，然後等待檢視日誌，那麼時間範圍會從您選取過濾時開始算起。而不是從您檢視日誌時開始算起。

如果您要確定過去 24 小時時間範圍是從現在起算，請選取不同的時間範圍，然後重新選取「過去 24 小時」。

使用過濾儲存自訂日誌

1. 在主視窗中，按下「監視器」。
2. 在「日誌」標籤的「日誌類型」清單方塊中，選取您要架構過濾的日誌檢視類型。
3. 對於某些類型的日誌，會顯示「日誌內容」清單方塊。如果顯示此方塊，請選取要架構過濾的日誌內容。
4. 在「使用儲存的過濾」清單方塊中，選取您要作為開始的過濾。例如，選取預設過濾。
5. 在「您要使用什麼過濾設定」下方，按下「其他設定」。
6. 變更任何設定。
7. 按一下「儲存過濾器」。
8. 在顯示對話方塊的「過濾名稱」方塊中，輸入要用於此日誌過濾架構的名稱。當儲存的過濾新增至過濾清單時，只會顯示該名稱的前 32 個字元。
9. 按下「確定」，新的過濾名稱便會新增至「使用儲存的過濾」清單方塊中。
10. 當出現確認對話方塊時，按一下「確定」。

刪除儲存的過濾

1. 在「使用儲存的過濾」清單方塊中，選取您要刪除的日誌過濾名稱。
2. 在「使用儲存的過濾」清單方塊旁，按下「刪除」圖示。
3. 當提示您確認要刪除過濾時，按下「是」。

檢視其他站台的日誌

如果您想要檢視其他站台的日誌，您必須從 Symantec Endpoint Protection Manager 主控台登入遠端站台的伺服器。如果您擁有遠端據點伺服器的帳戶，您可以執行遠端登入並檢視該網站的日誌。

如果您已架構複寫夥伴，您可以選擇將所有日誌從複寫夥伴複製到本機夥伴，反之亦然。如果您選擇遠端複製日誌，依據預設當您檢視任何日誌時，您會同時看見您網站與遠端複製網站的資訊。如果您想要看見單一網站，您必須過濾資料，將其限制在您想要檢視的位置。如果您選擇複寫日誌，請確定您有充足的磁碟空間可以儲存其他所有複寫夥伴的日誌。請參閱：

[如何安裝第二個網站用於遠端複製](#)

檢視其他網站的日誌

1. 開啟網頁瀏覽器。
2. 在位址文字方塊中輸入以下內容，如下所示：

```
http://SEPMServer:9090
```

其中 SEPMServer 是伺服器名稱或 IP 位址。

IP 位址可以是 IPv4 或 IPv6。必須用方括弧括住 IPv6 位址：http://[SEPMServer]:9090

主控台開始下載。您登入的電腦必須已安裝 Java Runtime Environment (JRE)。如果沒有，您會收到下載和安裝提示。遵照提示安裝 JRE。

3. 在主控台登入對話方塊中，輸入您的使用者名稱和密碼。
4. 如果「伺服器」文字方塊沒有自動填寫，如下所示，在其中輸入伺服器名稱或 IP 位址和通訊埠編號 8443：

```
http://SEPMServer:8443
```

5. 按下「登入」。

將資料匯出至 Syslog 伺服器

為了增加資料庫中的空間，您可以架構管理伺服器將日誌資料傳送至 Syslog 伺服器。

將日誌資料匯出至 Syslog 伺服器時，您必須架構 Syslog 伺服器接收日誌。請參閱：

[將日誌資料匯出至文字檔](#)

將資料匯出至 Syslog 伺服器

1. 在主控台中，按下「管理員」。
2. 按下「伺服器」。
3. 按下您要匯出日誌資料的本機站台或遠端站台。
4. 按下「架構外部記錄」。
5. 在「一般」標籤上，從「更新頻率」清單方塊選取將日誌資料傳送至檔案的頻率。
6. 在「主要日誌伺服器」清單方塊中，選取要傳送日誌的管理伺服器。

如果您使用 SQL Server 並將多個管理伺服器連線到資料庫，請將其中一個伺服器指定為主要日誌伺服器。

7. 勾選「啟用日誌傳輸至 Syslog 伺服器」。
8. 提供下列資訊：
 - **Syslog 伺服器**
輸入您要接收日誌資料的 Syslog 伺服器的 IP 位址或網域名稱。
 - 目的通訊埠
選取要使用的通訊協定，並輸入 Syslog 伺服器用來接聽 Syslog 訊息的目的通訊埠。
 - 日誌設備
鍵入您要用於 Syslog 架構檔的日誌設備數目，或使用預設值。有效值的範圍介於 0 和 23 之間。
9. 在「日誌過濾」標籤上，勾選要匯出的日誌。
10. 按下「確定」。

將日誌資料匯出至文字檔

將日誌資料匯出到文字檔案時，預設檔案位於資料夾中。依據預設，該資料夾路徑為 C:\Program Files (x86)\Symantec \Symantec Endpoint Protection Manager\data/dump。項目會暫存在 .tmp 檔案中，直到所有記錄都傳送至文字檔為止。

NOTE

您無法使用匯出的日誌資料還原資料庫。

下表顯示日誌資料類型與所匯出日誌資料檔案名稱的對應。日誌名稱未逐一對應「監視器」頁面之「日誌」標籤上使用的日誌名稱。

Table 166: Symantec Endpoint Protection 的日誌文字檔名稱

日誌資料	文字檔名稱
伺服器管理	scm_admin.log
應用程式與裝置控制	agt_behavior.log
伺服器用戶端	scm_agent_act.log
伺服器政策	scm_policy.log
伺服器系統	scm_system.log
用戶端封包	agt_packet.log
用戶端主動型威脅	agt_proactive.log
用戶端風險	agt_risk.log
用戶端掃描	agt_scan.log
用戶端安全	agt_security.log
用戶端系統	agt_system.log

日誌資料	文字檔名稱
用戶端流量	agt_traffic.log

NOTE

匯出至文字檔時，匯出記錄的數目可能與您在「外部記錄」對話方塊中設定的數目不同。重新啟動管理伺服器時，會發生這種狀況。重新啟動管理伺服器後，日誌項目計數會重設為 0，而暫存日誌檔中可能已經有項目。在這種狀況下，重新啟動後各類型產生的第一個 *.log 檔案包含的項目會多於指定值。後續匯出的任何日誌檔則會包含正確數目的項目。

匯出日誌資料至文字檔案

1. 在主控台中，按下「管理員」。
2. 按下「伺服器」。
3. 按下要架構外部記錄的本機網站或遠端據點。
4. 按下「架構外部記錄」。
5. 在「一般」標籤上，選取將日誌資料傳送至檔案的頻率。
6. 在「主要日誌伺服器」清單方塊中，選取要傳送日誌的伺服器。

如果您是使用 Microsoft SQL，且有多個管理伺服器連接資料庫，只有一部伺服器需設為主要日誌伺服器。

7. 勾選「匯出日誌至傾印檔」。
8. 若有必要，勾選「限制傾印檔記錄」，並鍵入您要一次傳送至文字檔的項目數目。
9. 在「日誌過濾」標籤上，選取要傳送至文字檔的所有日誌。

如果您選取の日誌類型可選取嚴重性等級，您必須勾選要匯出的嚴重性等級。

10. 按下「確定」。

為外部日誌記錄架構容錯移轉伺服器

Symantec Endpoint Protection Manager 充當主要日誌伺服器，將日誌轉送到系統日誌伺服器。自 14.3 起，您可以設定第二個管理伺服器作為主要伺服器的容錯移轉伺服器。如果主要管理伺服器離線，第二個管理伺服器將接管日誌並轉發到系統日誌伺服器。當主要管理伺服器重新連線時，它將繼續轉送日誌。

若要為外部日誌記錄架構容錯移轉伺服器

1. 在主控台中，按下「管理員」>「伺服器」，選擇網站，然後按一下「架構外部日誌記錄」。
2. 在「一般」標籤上，在「主要日誌伺服器」下拉清單中，選擇要對其發送日誌的主要管理伺服器。
如果主要伺服器關閉，清單中的下一個管理伺服器將會接管工作。管理伺服器列在「管理員」>「伺服器」>「編輯網站屬性」>「一般」標籤的報告伺服器優先順序清單中。
3. 按下「確定」。

更多資訊

[安裝管理伺服器以進行容錯移轉和負載平衡](#)

管理通知

通知可警示管理員及電腦使用者潛在的安全問題。

當您在架構一些通報類型時，會包括預設值。這些指導方針會根據您環境的大小提供合理的設定值，但您還可能需要另行調整。必須經過測試和錯誤才能讓您在過多與過少通報之間找出最適合您環境的平衡點。將臨界值設為初始限值，然後試行幾天。幾天之後，您可以調整通知設定。

以病毒、安全風險和防火牆事件偵測為例，假設您網路中的電腦數目少於 100 台。此網路的合理設定方式是架構一個可在一分鐘內偵測兩個風險事件的通報。如果您有 100 到 1000 台電腦，合理的設定方式是在一分鐘內偵測五個風險事件。

您可以在「監視器」頁面中管理通知。您可以使用「首頁」頁面決定需要注意、但未認可的通知數量。

下表列出管理通知可執行的工作。

Table 167: 通知管理

工作	說明
瞭解通知	瞭解通知的運作方式。請參閱： 通知的運作方式
確認電子郵件伺服器已架構為啟用電子郵件通知	若要以電子郵件傳送通知，需要正確架構 Symantec Endpoint Protection Manager 和電子郵件伺服器。請參閱： 建立管理伺服器與電子郵件伺服器之間的通訊
檢閱預先架構的通知	檢閱 Symantec Endpoint Protection 提供的預先架構的通知。請參閱： 有哪些類型的通知，何時傳送它們？
檢視未認可的通知	檢視及回應未認可的通知。請參閱： 檢視和認可通知
架構新通知	您可以選擇建立通知，以提醒您及其他管理員相關的重要問題。請參閱： • 設定管理員通知 • 關於開啟遠端用戶端的通知
建立通知過濾	您可以選擇建立過濾，以擴大或限制所有已觸發通知的檢視範圍。請參閱： 儲存和刪除管理通知過濾器

通知的運作方式

通知針對潛在的安全性問題，向管理員和使用者發出警示。例如，通知可以針對過期授權或病毒感染，向管理員發出警示。

事件可觸發通知。出現新的安全風險、用戶端電腦發生硬體變更，或是試用授權過期，都有可能觸發通知。觸發通知後，系統可能會採取相應動作。動作可以將通知記錄在日誌中，也可以執行批次檔或可執行檔，亦或傳送電子郵件。

NOTE

使用電子郵件通知必須正確架構 Symantec Endpoint Protection Manager 與電子郵件伺服器之間的通訊。

您可以設定通知的節流器期間。節流器期間指定必須經過多久時間，才能檢查通知條件中的新資料。如果通知條件有節流器期間，僅在期間內首次出現觸發條件時才會發出通知。例如，假設發生大規模病毒攻擊，而您有架構好的通知條件，在病毒感染了網路中的五台電腦時即會傳送電子郵件。如果將該通知條件的節流器期間設定為 1 小時，伺服器在攻擊過程中每小時只會傳送一封通知電子郵件。

NOTE

如果您針對重要事件的相關通知，將「調節器」期間設定為「無」，則應該確保用戶端可以立即上載重要事件。「讓用戶端立即上傳重大事件」選項預設為啟用，並且是在「通訊設定」對話方塊中進行架構。

更多資訊

- [管理通知](#)
- [建立管理伺服器與電子郵件伺服器之間的通訊](#)
- [有哪些類型的通知，何時傳送它們？](#)
- [設定管理員通知](#)
- [檢視和認可通知](#)

有哪些類型的通知，何時傳送它們？

Symantec Endpoint Protection Manager 提供了針對管理員的通知。您可以自訂其中大部分通知，以符合您的特定需求。例如，您可以新增篩選器，將觸發條件僅限定為特定伺服器。或者，您也可以設定通知在觸發時採取特定動作。

根據預設，安裝 Symantec Endpoint Protection Manager 時會啟用其中的部分通知。預設啟用的通知架構為記錄到伺服器，並傳送電子郵件給系統管理員。

如需詳細資訊，請參閱：

- [管理通知](#)
- [從其他版本升級會如何影響通知條件](#)

Table 168: 預先架構的通知

通知	說明
驗證失敗	在定義的時段中可架構的登入失敗次數會觸發驗證失敗通知。您可以設定觸發通知必須發生的登入失敗次數及時段。
已變更用戶端清單	現有用戶端清單有所變更時，將觸發此通知。預設會啟用此通知條件。 用戶端清單變更可包括： • 新增用戶端 • 變更用戶端名稱 • 刪除用戶端 • 變更用戶端的硬體 • 變更用戶端的非受管偵測程式狀態 • 用戶端模式變更
用戶端安全性警示	在發生下列任一安全性事件時，即觸發此通知： • 遵從事件 • 防網路和主機侵入事件 • 流量事件 • 封包事件 • 裝置控制事件 • 應用程式控制事件 您可以修改此通知以指定判斷這些通知何時觸發的事件類型、嚴重性和頻率。其中的某些發生類型會要求您同時在關聯的政策中啟用記錄。 Note: 通知調節器期間指定無論在該期間發生多少事件，管理伺服器都將透過電子郵件/報告資料通知管理員的頻率。例如，如果調節器為 1 分鐘，且在該分鐘內 3 個用戶端上有 3 個事件，則管理伺服器會傳送一個通知。 Note: 新增或編輯通知條件 Note: 確保用戶端可以立即上傳重要事件。「讓用戶端立即上傳重大事件」選項預設為啟用，並且是在「通訊設定」對話方塊中進行架構。
下載防護內容過時	警示管理員有關過時的下載防護內容。您可以指定觸發通知的定義檔期限。
檔案信譽查詢警示	將檔案提交至賽門鐵克進行信譽檢查時警示管理員。行為分析 (SONAR) 和下載鑑識使用檔案信譽查詢，並自動將檔案提交給賽門鐵克。 「檔案信譽偵測」通知預設為啟用。
偵測到強制性應用程式	當偵測到商用應用程式清單上的應用程式或偵測到管理員所監控應用程式清單上的應用程式時，會觸發此通知。
IPS 特徵過時	警示管理員有關過時的 IPS 特徵。您可以指定觸發通知的定義檔期限。

通知	說明
授權問題	已付費授權到期 此通知會警示管理員和合作夥伴 (選擇性) 已付費授權到期或即將到期。 預設會啟用此通知。 過度部署 此通知會警示管理員和合作夥伴 (選擇性) 有關過度部署的已付費授權。 預設會啟用此通知。 試用授權到期 此通知警示管理員已過期的試用授權和 60、30 和 7 天內將到期的試用授權。 根據預設，如果有試用授權，則會啟用此通知。根據預設，如果您的授權應進行升級或已付款，則不會啟用此通知。
記憶體攻擊緩和偵測	偵測到對已知和未知弱點的攻擊嘗試時，會觸發此通知。
網路負載警示: 病毒和間諜軟體完整定義檔的要求	請求完整定義集的用戶端過多及存在潛在網路頻寬問題時警示管理員。 預設會啟用此通知。
新發現的應用程式	應用程式探索偵測到新的應用程式時，會觸發此通知。
偵測到新風險	每當病毒和間諜軟體掃描偵測到新風險時就會觸發此通知。
新軟體套件	當下載新軟體套件或發生下列情況時，會觸發此通知: • LiveUpdate 下載用戶端套件。 • 管理伺服器已升級。 • 主控台手動匯入用戶端套件。 • LiveUpdate 具有新的安全性定義檔或引擎內容。 您可以指定是僅根據新的安全定義檔，還是僅根據新的用戶端套件，或是同時根據兩者觸發通知。 預設會啟用此通知。
新使用者允許的下載	當用戶端電腦允許「下載智慧型掃描」所偵測到的應用程式時，會觸發此通知。管理員可以使用此資訊，協助評估應攔截還是允許應用程式。
建議使用 Power Eraser	定期掃描無法修復感染時警示管理員，以便管理員可使用 Power Eraser。 預設會啟用此通知。
風險爆發	此通知會警示管理員有關安全風險的爆發。您可以設定新風險的發生次數和類型，以及這些新風險必須發生在什麼時段才會觸發此通知。發生類型包括發生於任何電腦、發生於一台電腦或發生於多台電腦。 預設會啟用此通知條件。
伺服器健康狀態	伺服器健康狀態問題會觸發此通知。此通知會列出伺服器名稱、健康狀態、原因以及最後一次的上線或離線狀態。 預設會啟用此通知。
單一風險事件	在偵測到單一風險事件時會觸發此通知，並且提供關於風險的詳細資訊。詳細資料包括涉及的使用者和電腦，以及管理伺服器所採取的動作。 Note: 如果您只在「調節器」時段期間看到一個事件，則請檢查「監視器」>「風險」日誌或「SONAR：行為分析」日誌，以找出多部用戶端電腦上的偵測。調節器期間設計為若有多個偵測，僅立即警示管理員一次。
SONAR 定義檔過時	警示管理員有關過時的 SONAR 定義檔。您可以指定觸發通知的定義檔期限。
系統事件	當發生特定系統事件時，會觸發此通知，且通知中會提供偵測到的此類事件數目。系統事件包括管理伺服器活動、複寫失敗、備份和系統錯誤。
非受管電腦	當管理伺服器在網路上偵測到非受管電腦時，會觸發此通知。此通知提供有關各非受管電腦的 IP 位址、MAC 位址和作業系統等詳細資料。
升級授權到期	升級授權授予從舊版的 Symantec Endpoint Protection Manager 升級到目前版本。當此升級授權即將到期時，會觸發此通知。 此通知僅會在升級後出現。
病毒定義檔過時	警示管理員有關過時的病毒定義檔。您可以指定觸發通知的定義檔期限。 預設會啟用此通知。

關於合作夥伴通知

當管理伺服器偵測到用戶端的已付費授權即將到期或已到期時,它會傳送通知給系統管理員。同樣地,管理伺服器可以在偵測到授權過度部署時,也傳送通知給管理員。

但是,在上述兩種情況中,若要解決問題,都需要購買新授權或續購。在許多安裝中,伺服器管理員可能沒有進行此類購買的權限,而仰賴賽門鐵克合作夥伴執行此工作。

管理伺服器提供維護合作夥伴的聯絡人資訊的功能。此資訊可在安裝伺服器時提供。在主控台的「授權」窗格中進行安裝後,系統管理員還可以隨時提供或編輯合作夥伴資訊。

提供合作夥伴聯絡人資訊給管理伺服器時,與已付費授權相關的通知和過度部署授權通知都會自動傳送給管理員和合作夥伴。

[有哪些類型的通知,何時傳送它們?](#)

建立管理伺服器與電子郵件伺服器之間的通訊

要讓管理伺服器傳送自動電子郵件通知,您必須架構管理伺服器與電子郵件伺服器之間的連線。請參閱:

[管理通知](#)

建立管理伺服器與電子郵件伺服器之間的通訊

1. 在主控台中,按下「管理員」,再按「伺服器」。
2. 在「伺服器」下方,選取要與電子郵件伺服器建立連線的管理伺服器。
3. 在「工作」下方,按一下「編輯伺服器屬性」。
4. 在「伺服器屬性」對話方塊中,按下「電子郵件伺服器」標籤。
5. 輸入電子郵件伺服器設定。
6. 按下「確定」。

更多資訊

[在 Endpoint Protection Manager Console 中傳送測試電子郵件訊息失敗](#)

檢視和認可通知

您可以檢視未認可的通知或所有通知,可以認可未認可的通知,可以檢視目前在主控台中架構的所有通知條件。

「首頁」頁面上的「安全狀態」窗格會指出過去 24 小時內發生的未認可通知數。

如需詳細資訊,請參閱[管理通知](#)。

檢視最近未認可的通知	- 按一下「首頁」。 - 在「首頁」頁面的「安全狀態」窗格中，按下「檢視通報」。 此時「通知」標籤下會顯示最近未認可的通知清單。 (可選) 在通知清單的「報告」欄中，按下文件圖示 (如果有)。 通報報告將出現於不同的瀏覽器視窗內。如果沒有文件圖示，則會在通知清單的「訊息」欄中顯示所有通知資訊。
檢視所有通知	- 在主控台中，按下「監視器」，然後按下「通知」標籤。 (可選) 在「通知」標籤的「使用儲存的過濾」功能表中，選取儲存的過濾。 儲存和刪除管理通知過濾器 (可選) 在「通知」標籤的「時間範圍」功能表中，選取一個時間範圍。 - 在「通報」標籤上，按下「檢視通報」。
認可通知	- 檢視通知。 - 在「通知」標籤的通知清單中，按下「認可」欄中的紅色圖示以確認通知。
檢視所有已架構的通知條件	- 在主控台中，按下「監視器」。 - 在「監視器」頁面的「通知」標籤上，按下「通知條件」。 此時將顯示在主控台中架構的所有通知條件。您可以利用選取「顯示通知類型」功能表內的通知類型來過濾清單。

儲存和刪除管理通知過濾器

您可以使用過濾器在主控台中擴大或限制管理通知的檢視範圍。您可以儲存新過濾器，也可以刪除以前儲存的過濾器。

如需詳細資訊，請參閱：

- [檢視和認可通知](#)
- [管理通知](#)

您可以建立使用任意準則組合的已儲存過濾器。例如，您可以建立一個過濾器，以便僅顯示過去 24 小時內發佈的未認可風險爆發通知。

新增通知過濾器

- 在主控台中，按下「監視器」。
- 在「監視器」頁面上的「通知」標籤中，按下「其他設定」。
- 在「您要使用什麼過濾設定？」標題下，設定過濾器的條件。
- 按一下「儲存過濾器」。
- 在「通知」標籤的「過濾器名稱」方塊中，鍵入過濾器名稱，然後按下「確定」。

刪除儲存的過濾通知過濾器

- 在主控台中，按下「監視器」。
- 在「監視器」頁面上的「通知」標籤中，在「使用儲存的過濾」功能表上選擇過濾器。
- 在「使用儲存的過濾」功能表的右側，按下 **X** 圖示。
- 在「刪除過濾」對話方塊中，按下「是」。

設定管理員通知

您可以架構通知，以便在發生特定種類的事件時，向您和其他管理員發出警示。您還可以新增觸發通知的條件，以提醒您執行重要工作。例如，您可以新增通知條件，在授權到期或偵測到安全風險時通知您。

觸發通知後，可以執行特定動作，例如：

- 將通知記錄到資料庫。
- 傳送電子郵件給一個或多個人員。
- 執行批次檔案。

NOTE

若要傳送電子郵件通知，您必須將郵件伺服器架構為與管理伺服器通訊。

如需詳細資訊，請參閱：

建立管理伺服器與電子郵件伺服器之間的通訊

您可以從可用通知類型清單中選擇通知條件。

選擇通知類型後，如下所述進行架構：

指定過濾器。	並非所有通知類型都提供過濾器。如有提供，便可以使用過濾器來限制觸發通知的條件。例如，您可以將通知限制為僅在影響特定群組中的電腦時觸發。
指定設定。	所有通知類型都提供設定，但具體設置因類型而異。例如，風險通知可能會讓您指定觸發通知的掃描類型。
指定動作。	所有通知類型都提供可指定的動作。

NOTE

若您針對重要事件的相關通知，將「調節器」期間設定為「1 分鐘」，則應確保用戶端可立即上載重要事件。相關通知包括：「用戶端安全性警示」、「單一風險事件」、「偵測到新風險」與「風險爆發」。「讓用戶端立即上傳重大事件」選項預設為啟用，並且是在「通訊設定」對話方塊中進行架構。

設定管理員通知

1. 在主控台中，按下「監視器」。
2. 在「監視器」頁面的「通知」標籤上，按下「通知條件」。
3. 在「通知」標籤上，按下「新增」，然後按下通知類型。
4. 在「新增通知條件」對話方塊中，提供下列資訊：
 - 在「通知名稱」文字方塊中，輸入用於標示通知條件的名稱。
 - 在「您要使用何種過濾設定？」(如果有) 下，指定通知條件的過濾設定。
 - 在「您要此通知使用哪些設定？」下，指定觸發通知的條件。
 - 在「觸發此通知時應該採取什麼動作？」下，指定觸發通知時應採取的動作。
5. 按下「確定」。

更多資訊

- [管理通知](#)
- [檢視和認可通知](#)

從其他版本升級會如何影響通知條件

在新伺服器上安裝 Symantec Endpoint Protection 時，預設會啟用許多預先架構的通知條件。但是，從舊版升級 Symantec Endpoint Protection 將會影響預設啟用的通知條件，還會影響其預設設定。

根據預設，會在新安裝 Symantec Endpoint Protection 時啟用下列通知條件：

-
- 已變更用戶端清單
 - 新用戶端軟體
 - 過度部署問題
 - 已付費授權問題
 - 風險爆發
 - 伺服器健康狀態
 - 試用軟體授權到期
 - 病毒定義檔過時

當管理員從舊版升級軟體時,將保留舊版中的所有現有通知條件。但是,現有的「新軟體套件」通知條件將變為「新用戶端軟體」通知條件。「新用戶端軟體」條件具有「新軟體套件」條件所沒有的兩個設定:「用戶端套件」和「安全性定義檔」。升級軟體時,將針對在升級後保留的此類型通知條件啟用上述兩種設定。但是,「新用戶端軟體」通知是在升級後建立的條件,根據預設,此通知會啟用「用戶端套件」設定,並停用「安全性定義檔」設定。

NOTE

啟用「新用戶端軟體」通知條件中的「安全性定義檔」設定後,可能會導致傳送大量通知。當存在多個用戶端或存在經常排程的安全定義檔更新時,可能會發生此種情況。如果您不希望接收有關安全定義檔更新的頻繁通知,則可以編輯此通知條件以停用「安全性定義檔」設定。

數個通知條件可能具有舊版所沒有的新設定,即:「傳送電子郵件給系統管理員」。如果對於某個通知條件而言,此設定是新設定,則根據預設,會在升級後對此類型的任何現有條件停用此設定。

如果未在早期安裝中新增預設通知條件類型,則會在升級安裝中新增此通知條件。但是,升級程序無法判斷管理員在早期安裝中故意刪除的預設通知條件。因此,在升級安裝中每個預設通知條件會停用所有下列動作設定,只有一個例外:「傳送電子郵件給系統管理員」、「記錄通知」、「執行批次檔」和「傳送電子郵件給」。將上述四項動作全部停用後,將不會處理通知條件,即使條件本身存在也是如此。管理員可以編輯通知條件以啟用任何或所有上述設定。

請注意,「新用戶端軟體」通知條件是例外:根據預設,可以在升級過程中新增此通知條件時產生通知。與其他預設的通知條件不同的是,將針對此條件啟用「記錄通知」和「傳送電子郵件給系統管理員」動作設定。

如果軟體的舊版不支援授權,則會啟用「升級授權到期」通知條件。

某些通知條件類型在軟體的舊版中無法使用。根據預設,在升級軟體時,會啟用這些通知條件。請參閱:

[有哪些類型的通知,何時傳送它們?](#)

管理管理伺服器、網站和資料庫

瞭解用戶端伺服器通訊、執行災難復原以及架構複寫、網站和容錯移轉。

使用此節以：

- 架構管理伺服器與用戶端之間的連線。
- 架構管理伺服器和憑證。
- 管理資料庫。
- 設定容錯移轉和負載平衡
- 管理網站和複寫。
- 執行災難復原。

關於 Symantec Endpoint Protection 伺服器的類型

管理伺服器時，下列定義可能有助於理解：

- 站台
網站是由通常位於相同公司位置的一或多部管理伺服器以及一個資料庫所組成。您登入的網站為本機網站，可以直接進行修改。本機站台以外的所有其他站台都稱為遠端站台。使用遠端複製連線網站。請參閱：
[設定站台和複寫](#)
- 管理伺服器
已安裝 Symantec Endpoint Protection Manager 軟體的電腦。從管理伺服器可以建立政策並將其指派給不同的組織群組。您可以監控用戶端，檢視報告、日誌和警示，以及架構伺服器和管理員帳戶。單一站台的多個管理伺服器可提供容錯移轉和負載平衡功能。請參閱：
[設定容錯移轉和負載平衡](#)
- 資料庫伺服器
Symantec Endpoint Protection Manager 使用的資料庫。每個網站有一個資料庫，不是 Microsoft SQL Server Express 就是 Microsoft SQL Server。如果您使用的是 SQL Server 資料庫，資料庫可位於與管理伺服器相同或不同的電腦上。SQL Server Express 取代了 14.3 RU1 中的內嵌資料庫。請參閱：
[維護資料庫](#)
- 複寫夥伴
在兩個站台之間複寫資料而建立的關係。請參閱：
[設定站台和複寫](#)

匯出和匯入伺服器設定

伺服器屬性檔案包含 Symantec Endpoint Protection Manager 的伺服器設定。下列情況下，您可能需要匯出和匯入伺服器屬性檔案：

- 使用災難復原檔案來重新安裝 Symantec Endpoint Protection Manager。
災難復原檔案未包含伺服器設定。重新安裝 Symantec Endpoint Protection Manager 時，會遺失先前變更的任何預設伺服器設定。您可以使用匯出的伺服器屬性檔案來重新匯入變更後的伺服器設定。
請參閱：[Endpoint Protection 的災難復原最佳實務準則](#)
- 您可以先在測試環境中安裝 Symantec Endpoint Protection Manager，稍後再將管理伺服器安裝在生產環境中。您可以將匯出的伺服器屬性檔案匯入生產環境。

NOTE

當您將匯出的 domain.dat 檔案匯入相同資料庫時，網域 ID 會變更以防止發生衝突。

匯出伺服器設定

1. 在主控台中，按下「管理員」，再按「伺服器」。
2. 在「伺服器」下，展開「本機網站 (網站 **site_name**)」，然後選取您要匯出的管理伺服器。
3. 按下「匯出伺服器屬性」。
4. 選取儲存檔案的位置，並指定檔案名稱。
5. 按下「匯出」。

匯入伺服器設定

1. 按一下「管理員」，然後按一下「伺服器」。
2. 在「伺服器」下，展開「本機網站 (站台 **site_name**)」，然後選取您要匯入設定的管理伺服器。
3. 按下「匯入伺服器屬性」。
4. 選取您要匯入的檔案，然後按下「匯入」。
5. 按下「是」。

管理 Symantec Endpoint Protection Manager 伺服器和第三方伺服器

您可以架構 Symantec Endpoint Protection Manager 整合網路環境中許多不同的伺服器類型。

Table 169: 伺服器管理

工作	說明
瞭解有關伺服器的資訊	決定您需要設定的伺服器類型。請參閱： 關於 Symantec Endpoint Protection 伺服器的類型
設定伺服器通訊權限	可以允許或拒絕存取遠端主控台。根據單一電腦或一組電腦的 IP 位址新增例外，即可管理存取。請參閱： 授予或攔截對遠端 Symantec Endpoint Protection Manager 主控台的存取
修改伺服器設定	若要修改資料庫設定，或者在不同的電腦還原資料庫，則可以修改伺服器設定。請參閱： 重新安裝或重新架構 Symantec Endpoint Protection Manager
架構郵件伺服器	若要使用網路中的特定郵件伺服器，必須架構郵件伺服器。請參閱： 建立管理伺服器與電子郵件伺服器之間的通訊
管理目錄伺服器	您能夠以 Active Directory 整合 Symantec Endpoint Protection 並以 AD 群組進行同步。請參閱： 以 Symantec Endpoint Protection Manager (SEPM) 來同步 Active Directory 群組
如果您使用 Proxy 伺服器連線到 Symantec LiveUpdate 伺服器，請架構 Proxy 設定	若要設定 Symantec Endpoint Protection Manager 來透過 Proxy 伺服器連線到 Internet，您必須架構 Proxy 伺服器連線。請參閱： 架構 Symantec Endpoint Protection Manager 連線到代理伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容
匯入或匯出伺服器屬性	您可以將伺服器設定匯出至 xml 檔案，以及重新匯入相同的設定。請參閱： 匯出和匯入伺服器設定
管理伺服器憑證	Symantec Endpoint Protection Manager 伺服器使用伺服器憑證加密資料，供網路中的所有伺服器和用戶端之間進行通訊。伺服器用伺服器憑證識別及自行驗證。可能需要備份、更新或產生新的伺服器憑證。請參閱： • 關於伺服器憑證 • 更新或還原伺服器憑證 • 備份伺服器憑證 • 產生新的伺服器憑證
架構伺服器的 SecurID 驗證	如果選擇使用 RSA SecurID 驗證管理員帳戶，您也必須架構管理伺服器，才能與 RSA 伺服器通訊。請參閱： 搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID 驗證

工作	說明
使用 Symantec VIP 為 Symantec Endpoint Protection Manager 架構雙因素驗證	如果您在環境中使用 Symantec VIP 進行雙因素驗證，則可以為使用 Symantec Endpoint Protection Manager 驗證進行驗證的管理員啟用此功能。 在 14.2 版中，已新增此支援。 如需詳細資訊，請參閱： 使用 Symantec VIP 架構雙因素驗證
將伺服器移到不同的電腦	基於下列原因，您可能必須在電腦之間移動管理伺服器軟體： - 必須將管理伺服器從測試環境移到生產環境。 - 執行管理伺服器的電腦發生硬體故障。 您可以用下列方式移動管理伺服器軟體： - 在另一部電腦安裝管理伺服器並執行複製。請參閱： 如何安裝第二個網站用於遠端複製 - 使用復原檔案在另一部電腦安裝管理伺服器。請參閱： 重新安裝或重新架構 Symantec Endpoint Protection Manager
啟動和停止管理伺服器	管理伺服器會執行成為自動服務。升級或執行災難復原時，必須停止管理伺服器服務。請參閱： 停止及啟動管理伺服器服務

維護資料庫

Symantec Endpoint Protection (SEPM) 同時支援 Microsoft SQL Server Express 資料庫和 Microsoft SQL Server 資料庫。如果您有 5,000 個以上的用戶端，請使用 Microsoft SQL Server 資料庫。

Symantec Endpoint Protection Manager 會自動安裝 Microsoft SQL Server Express 資料庫。您也可以單獨安裝 SQL Server Express。該資料庫包含安全政策、架構設定、攻擊資料、日誌及報告等資訊。SQL Server Express 取代了 14.3 RU1 中的內嵌資料庫。

在安裝 Symantec Endpoint Protection Manager 後，管理伺服器可能會在數週或數月之後速度開始變慢。為改善管理伺服器的效能，您可能需要縮小資料庫儲存空間，並排程各種資料庫維護工作。

Table 170: 資料庫管理工作

工作	說明
排程定期的資料庫備份	您應該排程定期的資料庫備份，以防資料庫發生毀損。請參閱： 備份資料庫和日誌 排程自動資料庫備份 Endpoint Protection 的災難復原最佳實務 或者，您也可以選擇手動刪除資料庫中的資料，避免在備份發生之前自動刪除資料庫。請參閱： 從資料庫手動清除日誌資料
排程資料庫維護工作	您可以排程資料庫維護工作，以加速管理伺服器與資料庫之間的互動。您可以排程管理伺服器，使其立即執行下列維護工作，或在使用者不在用戶端電腦上時執行下列維護工作。 - 從交易日誌移除未使用的資料。 - 重建資料庫表索引，來改善資料庫的排序和搜尋功能。 如需詳細資訊，請參閱： 排程自動資料庫維護工作
定期檢查資料庫檔案大小	確定資料庫不會達到檔案大小的上限。Microsoft SQL Server Express 資料庫具有 10 GB 大小限制。如果您在安裝 SEPM 時安裝 SQL Server Express，則 SEPM 會在您接近限制時提出警告。請參閱： 增加 Microsoft SQL Server 資料庫檔案大小

工作	說明
計算所需的資料庫儲存空間	請計算所需的磁碟空間總量後，再決定如何減少儲存空間的大小。 資料庫儲存空間取決於以下因素： - 日誌大小和到期時間。 - 用戶端電腦數目。 - 每月病毒平均數目。 - 各日誌所需保留的事件數。 - 內容更新次數。 內容更新每次約需 300 MB。請參閱： 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager 還原為舊版 Symantec Endpoint Protection 安全更新 各語言所需保留的用戶端版本數目。 例如，如果您同時具備 32 位元用戶端和 64 位元用戶端，則需要兩倍的語言版本數目。 必須保留的備份數目。 備份檔案大約佔資料庫大小的 75%，然後再乘以保留的備份複本數。 如需如何計算所需硬碟空間的詳細資訊，請參閱下列 Symantec 白皮書： Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書
減少日誌資料量	資料庫會接收持續產生的項目，並將項目儲存到日誌檔案中。您必須管理儲存在資料庫中的資料，以確保儲存的資料不會耗盡所有可用的磁碟空間。資料過多時，會造成執行資料庫的電腦當機。 您可以執行下列工作，來減少日誌資料量： - 只將部分用戶端日誌上傳至伺服器，以及變更上傳用戶端日誌的頻率。請參閱： 指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器 - 指定用戶端電腦在資料庫中可保留的日誌項目數，以及可保留多久的時間。請參閱： 指定日誌大小以及在資料庫中保留日誌項目的時間長度 - 過濾掉重要性較低的風險事件和系統事件，減少轉送到伺服器的資料。請參閱： 在 Windows 電腦上修改日誌處理及通知設定 - 在將日誌資料插入資料庫之前，減少日誌資料所儲存目錄的空間。請參閱： 關於增加用於用戶端日誌資料的伺服器磁碟空間 - 減少各管理伺服器所管理的用戶端數目。請參閱： 架構用於負載平衡的管理伺服器清單 - 減少活動訊號頻率，這會控制用戶端日誌多久上傳一次到伺服器。請參閱： 使用推送模式或提取模式更新用戶端上的政策和內容
將日誌資料匯出至另一部伺服器	基於安全目的，您可能需要將大量的日誌記錄保留更久的時間。為了將用戶端日誌資料量保持在較低的水平，您可以將日誌資料匯出至另一部伺服器。 您可以架構多個管理伺服器以接收日誌資料，以防其中一台伺服器關閉。請參閱： 將資料匯出至 Syslog 伺服器 將日誌資料匯出至文字檔
建立僅包含所需防護的用戶端安裝套件	用戶端安裝的防護功能越多，用戶端資訊在資料庫中所佔用的空間越多。建立僅包含用戶端電腦所需適當防護等級的用戶端安裝套件。加入的群組越多，用戶端資訊在資料庫中所佔用的空間越多。請參閱： 選擇要在用戶端上安裝哪些安全性功能
使用「群組更新提供者」下載內容	如果您的頻寬低或是用戶端電腦超過 100 個，請使用「群組更新提供者」下載內容。例如，2,000 個用戶端使用一個「群組更新提供者」下載內容，就等同使用四到五部管理伺服器進行下載。請參閱： 使用群組更新提供者將內容散佈至用戶端 若要減少磁碟空間和資料庫大小，您可以減少保留在伺服器上的內容修訂數目。請參閱： 將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager
還原資料庫	要復原損毀的資料庫，您可以將資料庫還原到其最初安裝的電腦上。或者，您可以將資料庫安裝在其他電腦上。請參閱： 還原資料庫

資料庫中的資訊會儲存在也稱為資料庫綱要的表格中。您可能需要綱要寫入自訂報表的查詢。如需詳細資訊，請參閱：

更多資訊

[驗證與資料庫的連線](#)

執行自動資料庫備份

您可以排程在較少使用者登入網路時進行資料庫備份。

您也可以在任何時候備份資料庫。請參閱：

[備份資料庫和日誌](#)

執行自動資料庫備份

1. 在主控台中，按一下「管理員」>「伺服器」。
2. 在「伺服器」下方，按下「本機網站 (我的網站)」> **SQLEXPRESSSYMC**。
3. 在「工作」下方，按一下「編輯資料庫屬性」。
4. 在「資料庫屬性」對話方塊的「備份設定」標籤中，執行以下工作。
 - 在「備份伺服器」下拉式清單中，指定要儲存備份的管理伺服器。
 - 若您因安全目的或公司政策需要儲存日誌複本，請勾選「備份日誌」。
否則，請將此選項保持停用，因為日誌會用掉許多磁碟空間。
 - 若公司政策規定，請設定「保留的備份數量」。如果使用預設資料庫且資料庫太大，請保留低數量。
5. 確定勾選「排程備份」，並設定排程。
6. 按下「確定」。

排程自動資料庫維護工作

安裝管理伺服器之後，資料庫的空間會不斷地成長。管理伺服器會在數週或數月之後速度變慢。為減少資料庫大小，並改善資料庫的回應時間，管理伺服器會執行下列資料庫維護工作：

- 截斷交易日誌。
在資料庫內所發生的每項變更，交易日誌幾乎都會記錄下來。管理伺服器會從交易日誌移除未使用的資料。
- 重建索引。
管理伺服器會重組資料庫表索引，以縮短其花費在排序及搜尋資料庫的時間。

根據預設，管理伺服器會依排程執行這些工作。您可以立即執行維護工作，或調整排程，讓它在使用者不在電腦上時進行。

NOTE

您也可以使用 Microsoft SQL Server Management Studio 執行資料庫維護工作。不過，您應該使用 Symantec Endpoint Protection Manager 或 Management Studio 其中之一，而不是同時使用這兩個軟體來執行這些工作。

在需要時執行資料庫維護工作

1. 在主控台中，按下「管理員」，再按「伺服器」。
2. 在「伺服器」下方，按下代表資料庫的圖示。
3. 在「工作」下方，選取以下任何一個選項：
 - 立即截斷交易日誌
 - 立即重建索引
4. 按下「執行」。
5. 完成工作後，請按下「關閉」。

排程資料庫維護工作自動執行

1. 在主控台中，按下「管理員」，再按「伺服器」。
2. 在「伺服器」下方，按下代表資料庫的圖示。
3. 在「工作」下方，按一下「編輯資料庫屬性」。
4. 在「一般」標籤中，勾選下列其中一個選項，或兩個都勾選，然後按下「排程工作」並指定每項工作的排程。
 - 「截斷資料庫交易日誌」。此工作的預設排程是每 4 小時一次。
 - 「重建索引」。此工作的預設排程是每個星期日的 2:00。

WARNING

如果您使用 SQL Server Management Studio 執行這些工作，請取消勾選這些選項。

更多資訊

排程自動資料庫備份

增加 Microsoft SQL Server 資料庫檔案大小

如果您使用 SQL Server 資料庫，請定期檢查資料庫大小，以確保資料庫未達到其大小的上限。如果可以，請增加至 SQL Server 資料庫可容納的最大大小。請參閱：

排程自動資料庫維護工作

增加 Microsoft SQL Server 資料庫大小

1. 在 Microsoft SQL 伺服器電腦上，開啟 SQL Server Management Studio。
2. 在 Object Explorer 中，展開「資料庫」資料夾，在 **sem5** 上按下滑鼠右鍵，然後按下「屬性」。
3. 在「資料庫屬性」對話方塊中，選取「檔案」。
4. 在「資料庫檔案」下，選取 **sem5_log1**，然後捲動至右側來檢視「自動成長」欄。
5. 在「自動成長」欄中，按下 ... 按鈕。
6. 在「變更 **sem5_log1** 的自動成長」對話方塊中，按一下「不限制檔案成長」，然後按一下「確定」。
7. 按下「確定」。

指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器

公司政策可能要求您增加資料庫保留的日誌事件的時間與類型。您可以指定要保留的日誌項目數，以及每個項目保留在用戶端上的天數。

您可以架構是否將每種類型的用戶端日誌上傳到伺服器。還可以架構最大上傳大小。如果您選擇不上傳用戶端日誌，則無法執行下列工作：

- 您無法使用「監視器」頁面中的「日誌」標籤，從 Symantec Endpoint Protection Manager 主控台檢視用戶端日誌資料。
- 您無法在備份資料庫時備份用戶端日誌。
- 您無法將用戶端日誌資料匯出至檔案或集中式日誌伺服器。

NOTE

部分用戶端日誌設定是群組限定的，而部分是在病毒和間諜軟體防護政策中設定，可套用到位置。如果您要區分所有遠端用戶端日誌和辦公室用戶端設定，則必須使用群組 (而非位置) 來管理遠端用戶端。

如需詳細資訊，請參閱：

指定日誌大小以及在資料庫中保留日誌項目的時間長度

指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器

1. 在主控台上按下「用戶端」，然後選取群組。
2. 在「政策」標籤上，按下「用戶端日誌」。
3. 在「用戶端日誌設定 (針對 群組名稱 對話方塊中，設定檔案大小上限和保留日誌項目的天數。
4. 對任何想要用戶端轉送至伺服器的日誌勾選「上傳到管理伺服器」。
5. 若是「安全」日誌和「流量」日誌，設定調節器期間和調節器閒置期間。
6. 按下「確定」。

指定日誌大小以及在資料庫中保留日誌項目的時間長度

若要有助於控制硬碟空間，您可以減少資料庫保留的日誌項目數。您也可以架構項目保留的天數。

NOTE

「監視器」頁面中 Symantec Endpoint Protection Manager 主控台「日誌」標籤上的日誌資訊會以邏輯群組的形式呈現，方便您檢視。「網站屬性日誌設定」標籤上的日誌名稱會對應到日誌內容，而非對應到「監視器」頁面中「日誌」標籤上的日誌類型。

如需詳細資訊，請參閱：

指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器

指定日誌大小以及在資料庫中保留日誌項目的時間長度

1. 在主控台中，按下「管理員」。
2. 在「伺服器」下方，展開「本機網站」，然後按下資料庫。
3. 在「工作」下方，按一下「編輯資料庫屬性」。
4. 在「日誌設定」標籤上，為每個類型的日誌設定項目數目和保留日誌項目的天數。
5. 按下「確定」。

關於增加用於用戶端日誌資料的伺服器硬碟空間

若您架構將大量用戶端日誌資料頻繁上傳到伺服器，可能會導致伺服器硬碟空間不足問題。如果您必須上傳大量用戶端日誌資料，可能就需要調整某些預設值，以避免發生空間不足的問題。當您部署到用戶端時，請監控伺服器上日誌插入目錄的空間，並視需要調整這些值。

將日誌轉換成 .dat 檔案，然後寫入至資料庫的預設目錄位於下列預設位置：

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\log。

若要調整控制伺服器上可用空間的值，您必須在 Windows 登錄中變更這些值。需要變更的 Windows 登錄機碼位於伺服器上的：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Symantec\Symantec Endpoint Protection\SEPM

下表列出 Windows 登錄機碼和其預設值，並說明其作用為何。

Table 171: 包含日誌上傳設定的 Windows 登錄機碼

值名稱	說明
MaxInboxSpace	用於指定分配給目錄的空間，日誌檔案會在此目錄中轉換成 .dat 檔案，之後再儲存到資料庫。 預設值為 8 GB。
MinDataFreeSpace	用於指定此目錄應保留可用的最小空間。此機碼可確保使用同一個目錄的其他應用程式有足夠的空間可供執行，而不會對效能有不利的影響。 預設值為 200 MB。

值名稱	說明
IntervalOfInboxSpaceChecking	用於指定管理伺服器在檢查完收件匣中可供日誌資料使用的空間之前，應等待多長時間。 預設值為 30 秒。

更多資訊

[維護資料庫](#)

從資料庫手動清除日誌資料

如果您要在進行例行資料庫維護時手動掃除日誌，則可以在備份資料庫後執行掃除。

如果您允許自動掃除，而又不常進行資料庫備份，可能會遺失部分日誌資料。如果您定期在執行資料庫備份後執行手動日誌掃除，則可以確保維持所有日誌資料完整保留。如果您必須將日誌保留一段較長時間 (例如一年)，這個程序就很有用。您可以手動清除日誌，但此為選用程序，您並非一定要進行。請參閱：

- [備份資料庫和日誌](#)
- [指定日誌大小以及在資料庫中保留日誌項目的時間長度](#)

從資料庫手動清除日誌資料

1. 為避免備份前自動進行資料庫掃除，可將站台日誌大小增大至最大值。
2. 視需要執行備份。
3. 在安裝 Symantec Endpoint Protection Manager 的電腦上開啟網頁瀏覽器，並輸入下列 URL：
`https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs`
執行此工作後，所有類型日誌的項目都會儲存在備用的資料庫資料表中。原始資料表會保留到下一次掃除啟動為止。
4. 要清空所有項目，而僅保留最新項目，請執行第二次掃除。原始資料表也會給清除，然後會再次儲存項目。
5. 將「網站屬性」對話方塊「日誌設定」標籤上的設定改回您偏好的設定。

設定容錯移轉和負載平衡

用戶端電腦必須能夠隨時與管理伺服器保持連線，以下載安全性政策並接收日誌事件。您應該設定容錯移轉，在管理伺服器無法使用時保持與 Symantec Endpoint Protection Manager 的通訊。負載平衡用來透過使用管理伺服器清單在多台管理伺服器之間分配用戶端管理。

下表列出了您在設定容錯移轉和負載平衡時應執行的工作。

Table 172: 容錯移轉和負載平衡的設定程序

工作	說明
閱讀容錯移轉和負載平衡的相關資訊。	您應瞭解是否需要以及何時設定容錯移轉和負載平衡的管理伺服器。請參閱： 關於容錯移轉和負載平衡
安裝其他管理伺服器。	如需詳細資訊，請參閱： 安裝管理伺服器以進行容錯移轉或負載平衡 每部管理伺服器的用戶端數量取決於日誌大小等數個因素。 若要計算所需的管理伺服器數量，請參閱： Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書

工作	說明
將管理伺服器新增到管理伺服器清單。	若要設定負載平衡，您需要新增多個管理伺服器到管理伺服器清單中。您可以使用預設的管理伺服器清單，或將管理伺服器新增到新的管理伺服器清單中。管理伺服器清單包含可供用戶端連線的管理伺服器 IP 位址或主機名稱。請參閱： 架構用於負載平衡的管理伺服器清單
將自訂管理伺服器清單指派給群組。	在建立自訂管理伺服器清單後，您必須將該清單指派給群組。請參閱： 指派管理伺服器清單至群組和位置

如果管理伺服器離線，或發生用戶端與管理伺服器無法通訊的問題，您也應該解決該問題。請參閱：

[Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

更多資訊

[為外部日誌記錄架構容錯移轉伺服器](#)

[設定站台和複寫](#)

關於容錯移轉和負載平衡

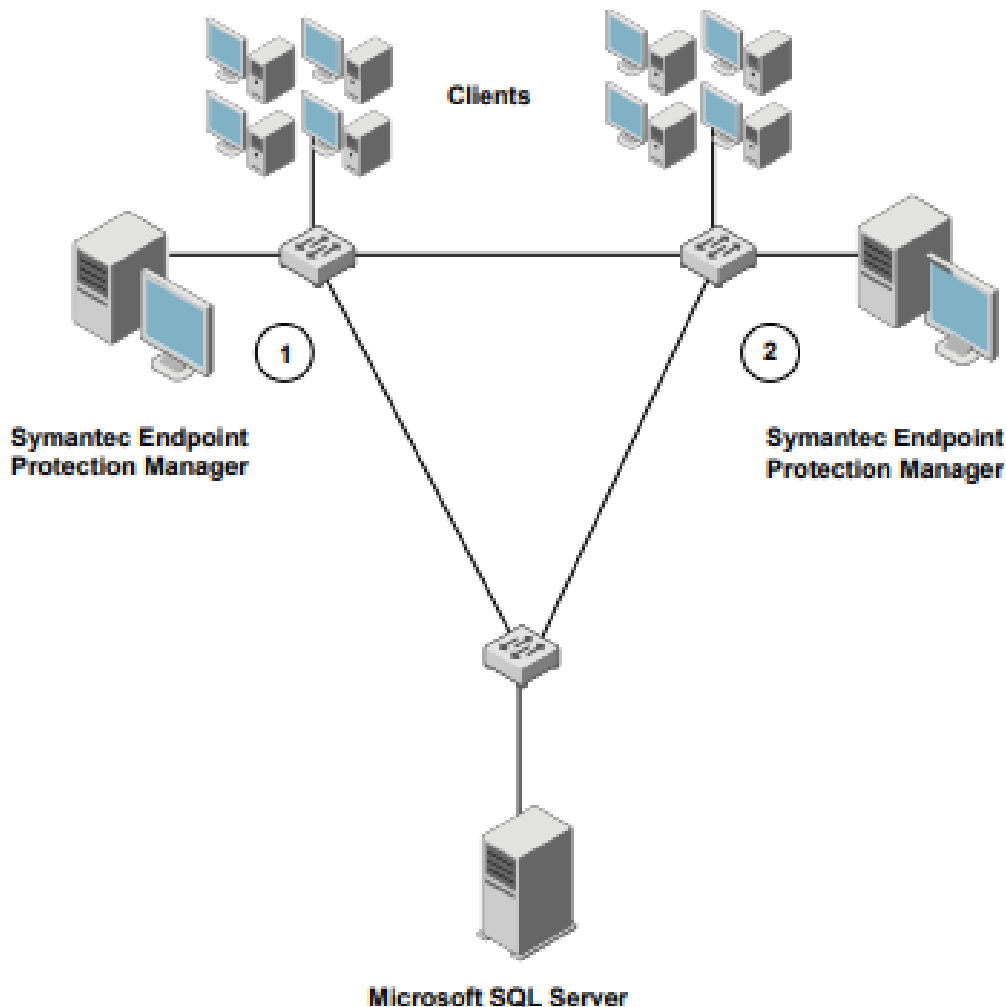
您可以安裝兩個以上的管理伺服器與一個資料庫進行通訊，並將其架構作為容錯移轉或負載平衡之用。主要伺服器故障時，容錯移轉會將工作負載重新導向備份管理伺服器。負載平衡會派送工作負載，以防止管理伺服器超載。

容錯移轉和負載平衡的運作方式為何？

若您安裝的管理伺服器數目超過處理用戶端所需的管理伺服器數目，即會發動容錯移轉，以防止個別管理伺服器失效。平衡負載透過指派至群組的管理伺服器優先順序清單觸發。您應該將至少兩個管理伺服器新增到網站，以在它們之間自動分配負載。

在自訂管理伺服器清單中，各個伺服器會被指派一個優先順序。新加入網路的用戶端會隨機選取最高優先順序的伺服器進行連線。如果嘗試的第一個伺服器無法使用，而清單中有其他最高優先順序的伺服器，則會隨機嘗試連線到其中一個伺服器。如果沒有任何最高優先順序的伺服器可供使用，則用戶端會嘗試連線到清單中其中一個次高優先順序的伺服器。這個隨機分配用戶端連線的方法會使各個管理伺服器分擔用戶端負載量。

下圖顯示不同子網路上的元件。管理伺服器與資料庫伺服器可位於相同的子網路中。伺服器標示為 1 及 2，代表容錯移轉架構。



在容錯移轉組態中，所有用戶端會在伺服器 1 中傳送和接收流量。如果伺服器 1 離線，所有用戶端會在伺服器 2 中傳送和接收流量，直到伺服器 1 重新上線。在說明圖中資料庫為遠端安裝，但資料庫也可以安裝於執行 Symantec Endpoint Protection Manager 的電腦中。

哪些 Symantec Endpoint Protection 元件會使用容錯移轉？

針對網站中多個 Symantec Endpoint Protection Manager，您可以在以下情況使用容錯移轉。

- 內容更新 執行 LiveUpdate 的所有元件也可以使用更新來源的優先順序清單。您的管理伺服器可以使用本機 LiveUpdate 伺服器，並在發生故障時移轉至其他實體位置的 LiveUpdate 伺服器。

NOTE

使用內部 LiveUpdate 伺服器、「群組更新提供者」和站台複寫時，不會提供負載平衡功能。請勿為了負載平衡而設定多個站台。

- 資料庫：若您使用 Microsoft SQL Server 資料庫或 Microsoft SQL Server Express 資料庫，便能設定容錯移轉和負載平衡。針對 14.3 MPx 或更早版本，您可以使用 Microsoft SQL Server 資料庫設定容錯移轉。您可以使用內嵌資料庫設定容錯移轉，但前提是您使用複寫。當您將複寫與內嵌資料庫搭配使用時，賽門鐵克建議您不要架構負載平衡，因為可能導致資料不一致和遺失。
- 報告：報告任務執行於單一管理伺服器。若伺服器關閉，semapisrv 服務會確認第二個管理伺服器是否有網路連線。若第二個管理伺服器有連線，則會發生容錯移轉。
- 混合管理：在 14.3 RU7 或更早版本中，您無法透過雲端伺服器設定容錯移轉。

在 14.3 RU8 中，若優先管理伺服器關閉，semapisrv 服務會確認第二個管理伺服器是否有網路連線。若第二個管理伺服器有連線，則會執行雲端連接器並嘗試連線至雲端伺服器。若連線檢查失敗，容錯移轉也會失敗，該程序將透過第三個管理伺服器重新開始。不論哪個管理伺服器連接到雲端，同一網域會一律在雲端伺服器中保持註冊狀態。

更多資訊

- [設定容錯移轉和負載平衡](#)
- [架構用於負載平衡的管理伺服器清單](#)
- [判斷需要的網站數量](#)
- [設定站台和複寫](#)

架構用於負載平衡的管理伺服器清單

架構容錯移轉和負載平衡時，預設會將相同的優先順序指派給管理伺服器。安裝後，如果要變更預設的優先順序，可以使用 Symantec Endpoint Protection Manager 主控台進行變更。只有在網站包含多個管理伺服器時，才能架構負載平衡。

管理伺服器清單中指派為優先順序 1 的伺服器之間，會發生負載平衡。如果多部伺服器指派為優先順序 1，用戶端會隨機選擇其中一部伺服器，並與此伺服器建立通訊。如果優先順序為 1 的所有伺服器都出現故障，則用戶端會連線至指派為優先順序 2 的伺服器。

同時提供負載平衡和漫遊功能：

- 啟用 DNS，並且在自訂管理伺服器清單中只放入網域名稱作為唯一項目。
- 啟用 Symantec Endpoint Protection 位置感測功能，並且為各個位置使用自訂管理伺服器清單。至少針對各個站台建立一個位置。
- 使用提供容錯移轉或負載平衡的硬體裝置。許多這類裝置也提供漫遊設定。

如需詳細資訊，請參閱：

[關於容錯移轉和負載平衡](#)

架構用於負載平衡的管理伺服器清單

1. 在主控台中，按下「政策」。
2. 展開「政策元件」，然後按一下「管理伺服器清單」。
3. 在「工作」下方，按一下「新增管理伺服器清單」。
4. 在「管理伺服器清單」對話方塊中，按一下「新增 > 新伺服器」。
5. 在「新增管理伺服器」對話方塊的「伺服器位址」方塊中，輸入管理伺服器的完整網域名稱或 IP 位址。
如果您鍵入的是 IP 位址，請確定該位址是靜態的，且所有用戶端都能解析該位址。
6. 按下「確定」。
7. 新增任何其他伺服器。
8. 若要架構另一個管理伺服器用於負載平衡，請按一下「新增 > 新優先順序」。
9. 若要變更用於負載平衡的伺服器的優先順序，請選定伺服器，然後按一下「向上移動」或「向下移動」。
10. 按下「確定」。

您接著必須將管理伺服器清單套用到群組。請參閱：

[指派管理伺服器清單至群組和位置](#)

安裝管理伺服器以進行容錯移轉或負載平衡

如果用戶端無法與 Symantec Endpoint Protection Manager 進行通訊，則會使用容錯移轉架構保持通訊。負載平衡則會用來分配管理伺服器之間的用戶端管理。您可以在「管理伺服器」清單中指派管理伺服器的優先順序，以架構容錯移轉和負載平衡。

只有原始 Symantec Endpoint Protection Manager 使用 Microsoft SQL Server 資料庫時，才支援容錯移轉和負載平衡安裝。在用於容錯移轉或負載平衡的電腦上，也必須安裝 SQL Server Native Client 檔案。

若要安裝管理伺服器以進行容錯移轉或負載平衡，請執行下列動作：

1. 安裝 Symantec Endpoint Protection Manager。請參閱：

[安裝 Symantec Endpoint Protection Manager](#)

2. 在「管理伺服器組態精靈」面板中，勾選「自訂組態」，然後按「下一步」。請參閱：

[安裝後架構 Symantec Endpoint Protection Manager](#)

3. 選取您要此伺服器管理的用戶端數目，然後按「下一步」。
4. 勾選「安裝額外的管理伺服器到現有網站」，然後按「下一步」。
5. 在「伺服器資訊」畫面中，接受或變更預設值，然後按「下一步」。
6. 在「**Microsoft SQL Server** 資訊」對話方塊中，按下有關安裝 SQL Server 用戶端工具之訊息中的「確定」。
7. 在下列文字方塊中輸入遠端伺服器值：

「步驟一」告知 Symantec Endpoint Protection Manager 可在何處尋找網路上的 SQL Server，其中包括主機名稱、實例名稱和通訊埠。

您也可以挑選驗證類型，包括 Windows 驗證或 SQL 驗證。

- 資料庫伺服器instance_name
SQL Server 通訊埠
資料庫名稱
「**SQL** 用戶端資料夾」(本機電腦上)

如果此文字方塊未自動填入正確路徑，則表示 Microsoft SQL Client Utility 未安裝或未正確安裝。

8. 「步驟二」告知 Symantec Endpoint Protection Manager 如何向 SQL Server 進行驗證，並包含資料庫名稱、資料庫使用者和資料庫使用者的密碼。

安裝該網站的第一個管理伺服器時，您應該已經備妥此資訊。

9. 按「下一步」。
10. 指定並確認 Symantec Endpoint Protection Manager admin 帳戶的密碼。
也可以選擇提供管理員的電子郵件地址。
11. 按「下一步」。
12. 出現警告時，請閱讀簡訊，然後按下「確定」。
13. 在「管理伺服器完成」面板中，按下「完成」。請參閱：

[為外部日誌記錄配置容錯移轉伺服器](#)

指派管理伺服器清單至群組和位置

新增政策之後，您必須將該政策指派給群組或(和)位置。您也可以使用管理伺服器群組，將用戶端的群組從某個管理伺服器移至另一個管理伺服器。

您必須先完成新增或編輯管理伺服器清單，才能指派清單。請參閱：

架構用於負載平衡的管理伺服器清單

指派管理伺服器清單至群組和位置

1. 在主控台中，按下「政策」。
2. 在「政策」頁面中，展開「政策元件」，然後按下「管理伺服器清單」。
3. 在「管理伺服器清單」窗格中，選取要指派的管理伺服器清單。
4. 在「工作」下方，按下「指派清單」。
5. 在「套用管理伺服器清單」對話方塊，勾選要套用管理伺服器清單的群組和位置。
6. 按下「指派」。
7. 按下「是」。

在用戶端頁面上指派管理伺服器清單至群組或位置

1. 在主控台中，按下「用戶端 > 政策」。
2. 在「政策」標籤中，選取群組，然後取消勾選「從父群組繼承政策和設定」。
只有在群組不再從父群組繼承任何政策和設定時，您才能針對該群組設定任何通訊設定。
3. 在「與位置無關的政策與設定」下方，按下「通訊設定」。
4. 在「**group name** 的通訊設定」對話方塊的「管理伺服器清單」下方，選取管理伺服器清單。
與管理伺服器通訊時，您選取的群組就會使用此管理伺服器清單。
5. 按下「確定」。

取代管理伺服器清單

針對負載平衡，請建立第二個管理伺服器清單，然後將其指派給原始群組或取代。例如，假設您有三份清單，分別為「預設的管理伺服器清單」、List2 以及 List3。您可以將「預設的管理伺服器清單」更換為 List3，但不得同時將 List2 更換為 List3。反之，您可以利用「指定清單」指令同時更換「預設的管理伺服器清單」與 List2。

請參閱：[指派管理伺服器清單至群組和位置](#)

以其他清單取代管理伺服器清單

1. 已建立第二個管理伺服器清單。
請參閱：[架構用於負載平衡的管理伺服器清單](#)
2. 在「政策」頁面上，按一下「政策元件」>「管理伺服器清單」。
3. 在「任務」下方，按一下「取代清單」。
4. 在「取代管理伺服器清單」對話方塊中，從「新的管理伺服器清單」下拉式清單選擇新清單，然後選擇要套用新清單的群組。
以粗體顯示的群組會顯示目前的管理伺服器清單。
您無法更換從父群組繼承的群組清單。繼承顯示下列文字的群組：**[繼承自父群組]**。
5. 按一下「取代」>「是」。

設定站台和複寫

一個站台包含一個資料庫、一或多個管理伺服器以及多個用戶端。依據預設，您將 Symantec Endpoint Protection 部署為單一站台。具有多個資料中心或多處實體位置的組織通常使用多個網站。

遠端複製組態用於備援。一個資料庫內的資料會複製或複寫至另一個資料庫上。一個資料庫發生故障時，您仍然可以管理及控制所有用戶端，因為另一個資料庫包含了用戶端資訊。請參閱：

[什麼是站台以及複寫如何運作？](#)

Table 173: 設定站台和複寫的程序

工作	說明
步驟 1：確認您是否需要新增另一個網站	設定多個網站和遠端複製之前，請確認是否必要。賽門鐵克建議您只在特定情況下設定多個站台，並且在每個站台陣列中新增最多五個站台。如果您新增額外的網站，請決定哪個網站設計用於您的組織。請參閱： 決定是否要設定多個網站和遠端複製 判斷需要的網站數量
步驟 2：在第一個站台上安裝 Symantec Endpoint Protection Manager	第一次安裝 Symantec Endpoint Protection 時，依據預設，您已安裝第一個站台或本機站台。請參閱： 安裝 Symantec Endpoint Protection Manager
步驟 3：在第二個網站上安裝 Symantec Endpoint Protection Manager	透過建立第二個管理伺服器來建立第二個站台。第二個站台歸類為遠端站台，管理伺服器稱為複寫夥伴。遠端複製會根據您在初始安裝期間新增第二個網站時的預設排程進行。新增遠端複製夥伴後，您可以變更遠端複製排程以及遠端複製的資料。請參閱： 如何安裝第二個網站用於遠端複製 兩個站台間的資料庫第一次複寫時，讓複寫完整完成。由於整個資料庫都要經過複寫，因此複寫可能需要比較長的時間。 您可能想要立即複寫資料，而不是等到排程資料庫進行複寫。您也可以將複寫排程變更為較早或較晚進行。 如果在一個網站上升級管理伺服器，則必須在所有網站上升級管理伺服器版本。請參閱： 立即遠端複製資料
步驟 4：檢查遠端複製事件的歷程記錄 (選擇性)	如果您需要檢查發生的遠端複製或針對遠端複製事件進行疑難排解，請查看系統日誌。在第二個管理伺服器中，檢視系統日誌。「管理」>「遠端複製事件」事件類型的過濾器。如需詳細資訊，請參閱： 檢視日誌

您還可以將管理伺服器重新架構為透過網路中目前存在的站台複寫資料。或者，如果您擁有兩個非遠端複製網站，可以將其中一個轉換為透過第二個網站遠端複製的網站。請參閱：

[重新安裝或重新架構 Symantec Endpoint Protection Manager](#)

請注意下列情況：

- 架構 Symantec Endpoint Protection 後，您應該備份包含所有架構變更的資料庫。請參閱：
[備份資料庫和日誌](#)
- 如果您停用某個遠端複製夥伴以升級至最新版的管理伺服器，則必須重新新增遠端複製夥伴。請參閱：
 - [在升級前後停用遠端複製和還原遠端複製](#)
 - [升級至新版本](#)

更多資訊

[連線至遠端複製網站上的目錄伺服器](#)

什麼是站台以及複寫如何運作？

如需詳細資訊，請參考下列各主題：

網站和遠端複製夥伴

網站是 Symantec Endpoint Protection Manager 資料庫，有一或多個 Symantec Endpoint Protection Manager 附加至該資料庫。複寫功能可以在不同站台的資料庫之間複製資料，以便讓兩個資料庫包含相同的資訊。如果其中一個資料庫發生故障，您可以使用第二個站台上的資料庫中的資訊來管理每個站台。

複寫夥伴是第二個站台或遠端站台內的個別管理伺服器。一個網站可視其需要有限數目的遠端複製夥伴。每個夥伴都會連線到主站台或本機站台，也就是您登入的站台。所有設定為夥伴的站台都可以視為位於相同站台陣列。

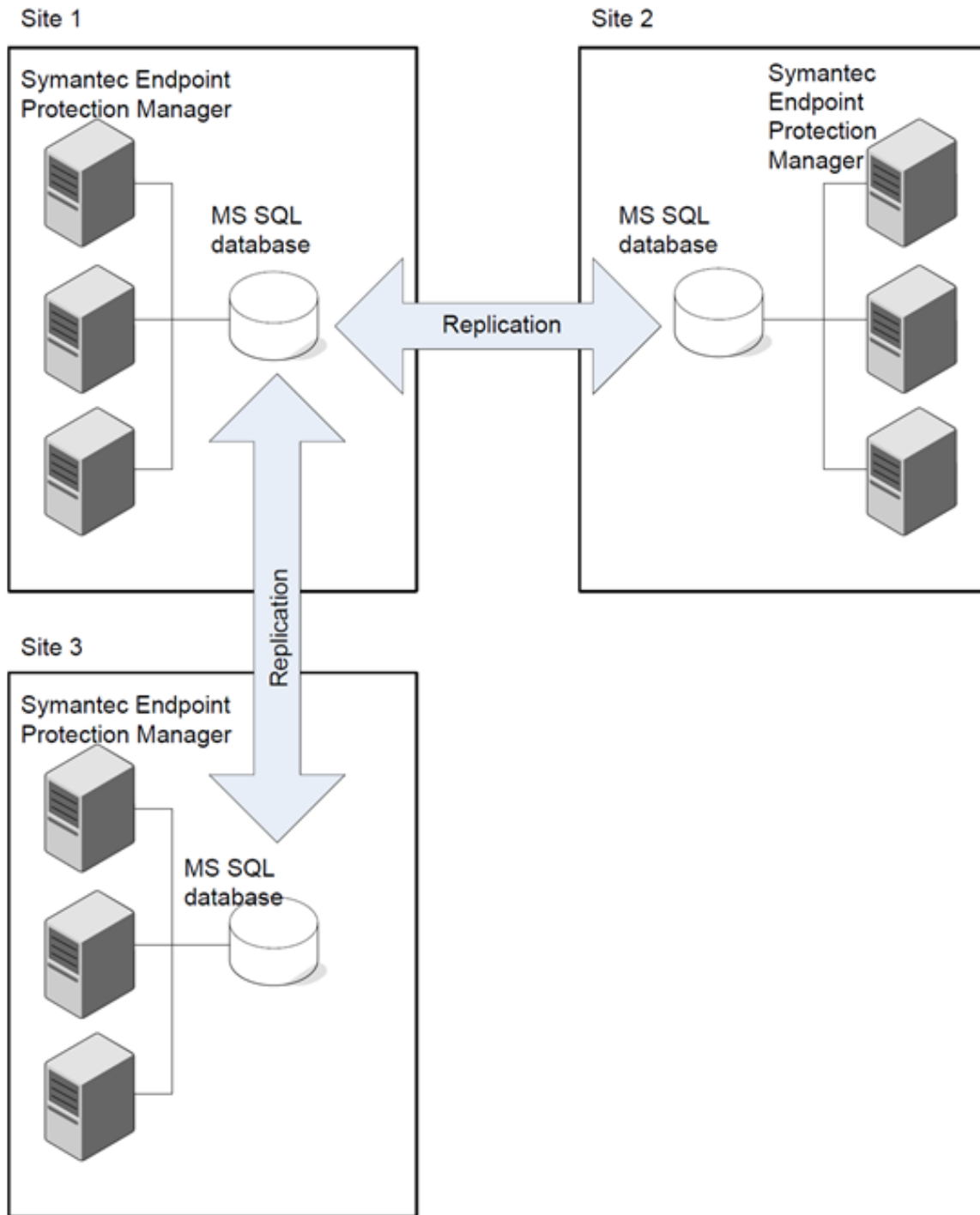
任何與您共同進行資料複寫的站台，都是複寫夥伴或站台夥伴。複寫夥伴和站台夥伴都會使用多部管理伺服器，但它們使用的資料庫以及通訊方式則不相同：

- 遠端複製合作夥伴可以使用預設資料庫 (14.3 RU1 中的 Microsoft SQL Server Express) 或 Microsoft SQL Server 資料庫。管理伺服器不會共用資料庫。所有的複寫夥伴會共用公共的授權碼。如果您使用的是 Microsoft SQL Server 資料庫，則可以連接共用一個資料庫的多個管理伺服器。只有其中一個管理伺服器需要設為遠端複製夥伴。
- 網站夥伴會共用單一 Microsoft SQL Server 資料庫。

遠端複製如何運作？

您在任何夥伴上執行的變更都會複製到所有其他夥伴上。例如，您可能會想要在主要辦公室設定一個網站 (網站 1) 和第二個網站 (網站 2)。站台 2 是站台 1 的夥伴。透過複寫排程，站台 1 和站台 2 上的資料庫會進行協調。如果在站台 1 進行了變更，在執行複寫之後，該變更會自動顯示在站台 2。如果在站台 2 進行了變更，在執行複寫之後，該變更會自動顯示在站台 1。您也可以安裝第三個站台 (站台 3)，它可從站台 1 或站台 2 複寫資料。

在複寫進行之後，站台 1 上的資料庫及站台 2 上的資料庫會彼此相同。只有伺服器的電腦識別資訊會不同。



如需複寫頻率的詳細資訊，請參閱下列文章：

[SEPM 複寫設定](#)

如需詳細資訊，請參閱：

- [決定是否要設定多個網站和遠端複製](#)
- [判斷需要的網站數量](#)
- [如何解決遠端複製期間網站之間的資料衝突](#)

判斷遠端複製伺服器的大小

遠端複製夥伴需要比單一管理伺服器安裝更大的資料庫。遠端複製伺服器的大小需求增加包括下列因素：

- 受管用戶端數目
- 資料庫中保留的用戶端安裝套件大小
- 保留的日誌檔數目
- 資料庫維護設定
- 日誌大小與到期時間範圍
- 定義檔更新大小
- 資料庫備份資訊需求

一般來說，複寫伺服器的硬碟需求應該是原始 Symantec Endpoint Protection Manager 用於初始複寫之硬碟空間的至少三倍。

更多資訊

- [如何安裝第二個網站用於遠端複製](#)
- [遠端複製考量和最佳實務準則](#)
- [Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書](#)

如何解決遠端複製期間網站之間的資料衝突

複寫會將資料傳輸或轉送到另一台管理伺服器。網站可以有多個遠端複製夥伴，而在其中一個夥伴上做出的任何變更都會遠端複製到所有網站。

會複製哪些資料？

複寫站台並不會互相覆寫，而是會比較每個網站的內容；如果某個網站有一套或一份其餘網站所沒有的內容，就會共用該內容。如果所有 LiveUpdate 內容和用戶端套件都相符，就不會交換任何內容。

複寫夥伴會複製下列資料：

- 政策和群組 (必要，雙向)
- LiveUpdate 內容和用戶端安裝套件 (如果您指定了這些選項) (選擇性，雙向)
- 日誌 (選擇性，雙向或單向)

如果在一個網站上升級管理伺服器，則必須在所有網站上升級管理伺服器版本。如果資料庫結構綱要版本不相符，就不會進行複寫。

說明管理伺服器如何在管理員變更站台陣列中站台上的設定時解決衝突。

Table 174: 管理伺服器解決站台間衝突的方式

衝突類型	範例	解決方法
兩項差異無法共存。	站台 1 和站台 2 的管理員都架構同一個防火牆政策設定。在站台 1 上，該設定為啟用。在網站 2 上，該設定為停用。	管理伺服器只會保留最近所做的變更。 例如，如果您先在站台 1 進行變更，然後在站台 2 進行變更，則會保留站台 2 的變更。
為兩個站台建立了相同的變數。	站台 1 和站台 2 的管理員都新增相同名稱的群組。	管理伺服器會保留這兩項變更，並在最近建立的變數後加上波浪號和數字 1 (~1)。 例如，兩個群組都命名為 Sales 時，最近命名的 Sales 群組會變成 Sales ~1。

衝突類型	範例	解決方法
資料可以合併，沒有衝突。	站台 1 的管理員新增了兩項防火牆政策，而站台 2 的管理員新增了五項防火牆政策。	管理伺服器會合併變更。 例如，管理伺服器會在雙方網站上顯示所有七項防火牆政策。

決定是否要設定多個網站和複寫

在您安裝第二個網站之前，應該決定多個網站和複寫是否為您網路的最好選擇。設定一個以上的網站可能會增加不必要的複雜性。多個站台可能會導致某些工作 (例如檢視用戶端日誌和報告) 更加困難。一般來說，您應只安裝一個站台。

設定多個站台和複寫的主要目的如下：

- 如果網路的 WAN 連結速度很慢。
多個網站會提供第二部管理伺服器，供位於多個地理區域的用戶端在本機上連線。例如，假設公司在德國和美國都設有幾個大型辦公室。如果德國和美國之間的連線速度很慢，則該公司應分別在德國和美國各建立一個站台。德國用戶端可以連線至德國網站，而美國用戶端可以連線至美國網站。這樣的分配方式可減少必須透過慢速 WAN 連結通訊的用戶端數目。
- 為了提供資料庫備援。
複寫可確保在其中一個資料中心損毀或遺去的情況下，其他資料中心有備份的資料庫。

用戶端數量

單一 SEPM 網站可以管理大約 250,000 個用戶端。如果您有足夠的資源 (五部管理伺服器且每部各服務 50,000 個用戶端，而且活動訊號間隔為 4 小時)，則應該使用第二個網站來容納用戶端數目超過 250,000 個的環境。

熱網站容錯移轉和法規遵從性

如果基於法規原因而必須符合特定服務層級協議，則建立次要 SEPM 網站並透過複寫來保持其更新是確保用戶端可以在 SEPM 網站完全失敗時存取管理伺服器的一種方式。

常見的複寫誤解

下列清單描述一些最常見的複寫誤解：

1. 複寫提供跨多個網站的實時報告功能。
2. 一個網站一個 SEPM。
3. 多個具有複寫的網站允許使用不同的控制網域。
4. SEPM 複寫可以架構成完全「單向」。
5. 跨慢速 WAN 連結進行複寫會比跨慢速 WAN 連結進行用戶端活動訊號更為可取。
6. 跨 WAN 進行複寫可降低用戶端到 SEPM 通訊的頻寬成本。
7. SEPM 複寫使用內建 Microsoft SQL Server 資料庫複寫技術。
8. SEPM 網站類似於 Active Directory 網站。

群組更新提供者

在某些情況下，您應使用群組更新提供者 (GUP)，而非多個站台和複寫。當您有許多用戶端或用戶端分散在多個地理位置時，請使用 GUP。

NOTE

您不應設定超過五個遠端複製的網站。

Table 175: 決定要使用一個以上的站台搭配複寫、使用 GUP，或是都不使用

問題	答	使用多個站台搭配複寫或使用 GUP
您是否有超過 45,000 個用戶端？	是。 您是否有多個位置，或連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度很慢？	是。 - 若 WAN 連結速度很慢，請考慮使用複寫。 - 若有多個位置，請考慮使用 GUP。
		否。您不需要遠端複製或 GUP。
	否。 您連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度是否很慢？	是。請考慮使用複寫。
		否。您不需要遠端複製或 GUP。
您的 WAN 連結速度是否很慢？	是。 您是否有多個位置，而每個位置都有超過 1,000 個用戶端？	是。請考慮使用複寫。
		否。請考慮使用 GUP。
	否。 您是否有多個位置，而每個位置都有超過 1,000 個用戶端？	是。請考慮使用複寫。
		否。您不需要遠端複製或 GUP。
您是否有多個位置，而每個位置都有超過 1,000 個用戶端？	是。 您連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度是否很慢？	是。請考慮使用 GUP。
		否。您不需要遠端複製或 GUP。
	否。 您連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度是否很慢？	是。請考慮使用 GUP。
		否。您不需要遠端複製或 GUP。

更多資訊

- [使用群組更新提供者將內容散佈至用戶端](#)
- [設定站台和複寫](#)
- [判斷需要的網站數量](#)

判斷需要的網站數量

大多數中小組織只需要單一站台集中管理網路安全性。由於每個網站只有一個資料庫，因此所有資料都在中央位置上。

甚至位於單一地理位置的大型組織，通常也只需要一個站台。但是對於過於複雜無法集中管理的組織，您應該使用具有多個網站的分散式管理架構。

對於下列任何因素，您都應該考慮使用多個站台：

- 大量用戶端。
- 地理位置數量，以及不同位置之間的通訊連結類型。
- 功能部門或管理群組數量。
- 資料中心數量。最佳實務準則是針對各個資料中心設定一個 Symantec Endpoint Protection 站台。
- 要更新內容的頻率。
- 需要保留的用戶端日誌資料量、保留資料的時間長度，以及應該儲存資料的位置。
- 多個具有幾千個用戶端的實體位置之間的 WAN 連結速度很慢。如果您設定具有自己的管理伺服器的第二個站台，可以將用戶端與伺服器之間透過該緩慢連結的流量減至最少。用戶端較少時，應該使用「群組更新提供者」。請參閱：
[使用群組更新提供者將內容散佈至用戶端](#)
- 任何其他獨特的企業管理和 IT 安全性管理考量事項。

請使用下列規模指引決定安裝網站的數量：

- 儘可能安裝較少的站台，最多不超過 20 個站台。複寫站台的數量應維持在五個以下。
- 最多將 10 個管理伺服器連線到一個資料庫。
- 將多達 18,000 個用戶端連線至管理伺服器。

新增站台後，您應該透過複寫功能在多個站台間複寫站台資訊。複寫是在資料庫之間共用資訊的程序，可確保內容一致。

Table 176: 多網站設計

網站設計	說明
已派送	每個站台都會針對群組和政策執行雙向複寫，但不會針對日誌和內容執行複寫。若要檢視站台報告，您可以使用主控台連線至遠端站台中的管理伺服器。 如果您不需要即時存取遠端據點資料，則可以使用此設計。
集中式記錄設計	所有日誌都從其他網站轉送到中央網站上。 如果您需要集中式報告，則使用此設計。
高可用性	每個站台都有多個管理伺服器安裝和資料庫叢集。 若要處理其他用戶端，您需要新增多個管理伺服器而不是新增多個網站。您可以使用管理伺服器清單，將用戶端電腦架構為在主要管理伺服器變成無法使用時自動切換到替換管理伺服器。 使用此設計可提供備援、容錯移轉和災難復原功能。 Note: 當您將遠端複製與內嵌資料庫 (14.3 MPx 及更舊版本) 搭配使用時，賽門鐵克建議您不要新增負載平衡，因為可能導致資料不一致和遺失。 如需詳細資訊，請參閱： 設定容錯移轉和負載平衡

如需是否設定複寫的詳細資訊，請參閱以下知識庫文章：

[何時將複寫與 Endpoint Protection Manager 搭配使用](#)

更多資訊

- [什麼是站台以及複寫如何運作？](#)
- [設定站台和複寫](#)
- [決定是否要設定多個網站和遠端複製](#)

如何安裝第二個站台用於遠端複製

安裝用於複寫的第二個站台的程序分兩個階段：

- 安裝第二個 Symantec Endpoint Protection Manager 和資料庫以透過已安裝的 Symantec Endpoint Protection Manager 和資料庫進行複寫。
- 登入第二個 Symantec Endpoint Protection Manager 並變更要遠端複製的排程和項目 (選擇性)。請參閱：
[變更遠端複製頻率和內容](#)

安裝第二個站台用於複寫

1. 安裝第二個 Symantec Endpoint Protection Manager。請參閱：
[安裝 Symantec Endpoint Protection Manager](#)
「管理伺服器組態精靈」會在安裝管理伺服器後自動啟動。
2. 在「管理伺服器組態精靈」中，按下「新安裝的自訂組態 (多於 500 個用戶端，或自訂設定)」，然後按「下一步」。
3. 按下「安裝其他網站」，然後按「下一步」。
4. 在下一個面板中，輸入以下資訊，然後按「下一步」：
 - 複寫伺服器
已安裝之管理伺服器的名稱或 IP 位址以及遠端複製此管理伺服器所使用的名稱或 IP 位址。
 - 「系統管理員名稱」和「密碼」。

依預設，系統管理員的使用者名稱為 `admin`。您必須使用系統管理員帳戶，而不是使用限制的管理員帳戶或網域管理員帳戶。

- 勾選「在本機網站和此夥伴網站之間遠端複製用戶端套件和 **LiveUpdate** 內容」(選擇性)。

如果您現在不勾選此選項，可以稍後勾選。

5. 如果出現有關接受憑證的警告訊息，請按下「是」。
6. 在「網站資訊」窗格中，接受或變更預設值，然後按「下一步」。
7. 在「資料庫選擇」窗格中，按下「預設 **SQL Server Express** 資料庫」或「**Microsoft SQL Server** 資料庫」，然後按「下一步」。

賽門鐵克建議您遠端複製的網站使用相同類型的資料庫，但這並非是必需的。對於 14.3 MPx 和更舊版本，預設資料庫是「預設內嵌式資料庫」。

根據選擇的資料庫完成安裝。

8. 在「執行 **LiveUpdate**」窗格中，按「下一步」。

或者，也可以新增夥伴資訊。

9. 或者，接受資料收集功能，然後按「下一步」。

隨即建立資料庫。此步驟需要一些時間。

Symantec Endpoint Protection Manager 隨即啟動。

如有必要，請變更排程。請參閱：

[變更遠端複製頻率和內容](#)

更多資訊

- [設定站台和複寫](#)
- [什麼是網站以及遠端複製如何運作？](#)
- [決定是否要設定多個網站和遠端複製](#)
- [防止在升級期間複寫](#)

變更遠端複製頻率和內容

依據預設，已排程為在安裝第二個站台和管理伺服器之後自動執行遠端複製。在安裝第二個管理伺服器的過程中，根據預設排程執行遠端複製。但是，您可能需要根據遠端複製所需時間來變更頻率。您可以在本機站台或新站台上變更頻率，但賽門鐵克建議您首先在新站台上架構遠端複製。下次當兩個站台遠端複製時，這些站台上的排程相同。較小 ID 號碼的站台會先起始排程複寫。無論哪個網站架構為新的遠端複製夥伴，都將始終由來自新網站所指向的本機網站的資料庫覆寫其資料庫。

兩個站台會自動共用群組和政策。可以根據可用磁碟空間量選擇是否遠端複製日誌、用戶端安裝套件或 LiveUpdate 內容。

遠端複製所需時間，取決於資料庫大小及網站間的網路連線。首先，測試一個遠端複製週期，查看其花費的時間。您應該根據該段時間來排程複寫，並確定管理伺服器複寫資料的時間不會重疊。用戶端套件和 LiveUpdate 內容可包含大量資料。用戶端套件中的資料最大可達 5 GB。用戶端安裝套件可能需要多達 500 MB 的磁碟空間。如果您計劃遠端複製日誌，務必確定您有充足的磁碟空間可以儲存所有遠端複製夥伴伺服器上的其他日誌。

在初次的完整資料庫遠端複製完成後，如果只遠端複製政策、用戶端和群組，而不遠端複製日誌，則後續的遠端複製規模會相當小。確保管理伺服器具有足夠的可用磁碟空間來根據頻率及內容進行遠端複製。

變更遠端複製頻率和排程

1. 在主控台中，按一下「管理員」>「伺服器」。
2. 在「伺服器」>「本機網站」下，展開「遠端複製夥伴」，然後選取您要遠端複製的網站。
3. 在「工作」下方，按下「編輯遠端複製夥伴屬性」。
4. 選擇您要複寫的內容。
5. 若要變更排程，請執行下列其中一項工作：
 - 勾選「自動遠端複製」讓管理伺服器選擇何時遠端複製資料。

此選項可在兩個站台之間約每 2 小時定期進行自動複寫。

- 勾選「按排程遠端複製」以設定自訂排程。

6. 按下「確定」。

更多資訊

[遠端複製考量和最佳實務準則](#)

立即遠端複製資料

複寫通常會在您設定其他站台時根據預設排程進行。您可能希望立即進行複寫。較小 ID 號碼的站台會先起始排程複寫。

如果在多部伺服器上使用了 Microsoft SQL Server 資料庫，則只能從該網站上的第一部伺服器開始遠端複製。

立即複寫資料

1. 在主控台中，按一下「管理員」>「伺服器」。
2. 在「伺服器」>「本機網站」下，展開「遠端複製夥伴」並選取網站。
3. 在「工作」下方，按下「立即遠端複製」。
4. 依序按下「是」和「確定」。

更多資訊

- [變更遠端複製頻率和內容](#)
- [設定站台和複寫](#)

刪除站台

在 Symantec Endpoint Protection Manager 中刪除遠端複製夥伴會中斷夥伴關係，但不會解除安裝管理伺服器軟體或刪除第二個站台。

如果移除遠端據點中的管理伺服器，您需要手動從所有網站中刪除它。將軟體從某個管理伺服器主控台中解除安裝，並不會使圖示從其他主控台上的「伺服器」窗格中消失。請參閱：

[在升級前後停用遠端複製和還原遠端複製](#)

刪除網站

1. 在主控台中，按下「管理員」>「伺服器」>「本機網站」，展開「遠端複製夥伴」，於遠端複製夥伴上按下滑鼠右鍵，然後按下「刪除遠端複製夥伴」。
2. 在「遠端據點」下的網站上按下滑鼠右鍵，然後按下「刪除遠端據點」。
3. 按下「是」。

更多資訊

[設定站台和複寫](#)

Endpoint Protection 的災難復原最佳實務準則

若要準備在發生硬體故障或資料庫損毀後復原，您應該備份安裝 Symantec Endpoint Protection Manager 後所收集的資訊。

如需詳細資訊，請參考下列各主題：

準備進行災難復原

請遵循下列步驟來準備。

Table 177: 準備災難復原時的重要工作

步驟	說明
步驟 1：備份資料庫	定期備份資料庫 (最好每週備份一次)。 依據預設，資料庫備份資料夾會儲存到以下預設位置： C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup 備份檔案稱為 date_timestamp.zip。 如需詳細資訊，請參閱： 備份資料庫和日誌
步驟 2：備份最近的災難復原檔案	嚴重損壞修復檔案包括加密密碼、密鑰儲存檔案網域 ID、憑證檔案、授權檔及通訊埠號。依據預設，此檔案位於以下目錄中： C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip 復原檔案僅儲存預設網域 ID。如果您有多個網域，則復原檔案不會儲存該資訊。如果需要執行災難復原，您必須再次新增網域。請參閱： 新增網域 如果您有多個 zip 檔，則僅備份最近的檔案。
步驟 3：更新或備份伺服器憑證 (選擇性)	如果將自我簽署憑證更新為不同的憑證類型，則管理伺服器會建立新的還原檔案。由於復原檔案具有時間戳記，因此您可以分辨出哪一個檔案是最新的檔案。請參閱： • 更新或還原伺服器憑證 • 備份伺服器憑證
步驟 4：將管理伺服器的 IP 位址和主機名稱儲存到文字檔 (選擇性)	如果您發生嚴重的硬體錯誤，必須使用原始管理伺服器的 IP 位址和主機名稱來重新安裝管理伺服器。 請將 IP 位址和主機名稱新增至文字檔，例如：Backup.txt。
步驟 5：在離站的安全位置儲存備份資料	將您在先前步驟中所備份的檔案複製到另一台電腦

執行災難復原

下表列出在發生硬體故障或資料庫損毀時復原 Symantec Endpoint Protection 環境的步驟。

在執行這些步驟之前，請確保您已建立備份和復原檔案。

Table 178: 執行嚴重損壞修復的程序

步驟	動作
步驟 1：使用災難復原檔案重新安裝 Symantec Endpoint Protection Manager。	藉由重新安裝管理伺服器，您可以復原初始安裝後儲存的檔案。請參閱： 重新安裝或重新架構 Symantec Endpoint Protection Manager 如果您在不同的電腦上重新安裝 Symantec Endpoint Protection Manager，而且沒有使用嚴重損壞修復檔案，則必須產生新的伺服器憑證。請參閱： 產生新的伺服器憑證
步驟 2：還原資料庫。	無論有沒有資料庫備份，您都可以還原資料庫。請參閱： 還原資料庫
步驟 3：重新啟用聯邦資訊處理標準 (FIPS) 140-2 法規遵循。(選擇性)	如果您使用遵從 FIPS 的 Symantec Endpoint Protection 版本並且啟用遵從 FIPS，那麼在復原 Symantec Endpoint Protection Manager 之後，您必須重新啟用遵從 FIPS。 此設定未儲存在災難復原檔案中。

更多資訊

-
- [備份您的授權檔](#)
 - [匯出和匯入伺服器設定](#)
 - [Endpoint Protection 的災難復原最佳實務](#)

備份資料庫和日誌

賽門鐵克建議您，至少每週備份一次資料庫。您應將備份檔案儲存於另一部電腦內。

依據預設，備份檔案儲存在下列資料夾中：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup。

備份會放入 .zip 檔案中。備份的資料庫檔案會預設命名為 date_timestamp.zip，此為備份發生的日期。

NOTE

避免將備份檔案儲存於產品安裝目錄內。否則移除產品時將一併移除備份檔案。

日誌資料不會備份，除非架構 Symantec Endpoint Protection Manager 來加以備份。如果不備份日誌，則備份期間只會儲存日誌架構選項。您可以使用備份還原資料庫，但資料庫的日誌在還原之後將不會有任何資料。

您可以保留多達 10 個版本的站台備份。如果選擇保留多個版本，請確定有足夠的磁碟空間可存放所有資料。

您可以在備份期間和備份之後，於「系統日誌」以及備份資料夾查看狀態。

您可以立即備份資料庫，也可以排程自動備份。

NOTE

Microsoft SQL Server Express 資料庫具有 10 GB 限制。若要備份資料庫，資料庫不得超過 10 GB，並且必須至少有 10 GB 的可用磁碟空間。

[從內嵌資料庫升級到 Microsoft SQL Server Express 資料庫的最佳實務](#)

如需詳細資訊，請參閱：

- [排程自動資料庫備份](#)
- [Endpoint Protection 的災難復原最佳實務](#)

備份資料庫和日誌

1. 在執行 Symantec Endpoint Protection Manager 的電腦上，於「開始」功能表上，按下「所有程式 > **Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager 工具 > 資料庫備份及還原**」。
2. 在「資料庫備份與還原」對話方塊中，按下「備份」。
3. 在「備份資料庫」對話方塊中，選擇性勾選「備份日誌」，然後按下「是」。
4. 按下「確定」。
5. 資料庫備份完畢後，按下「結束」。
6. 複製備份的資料庫檔案至另一部電腦。

從主控台內備份資料庫和日誌

1. 在主控台上，按一下「管理員 > 伺服器」。
2. 在「伺服器」下方，按一下「本端網站 (我的網站)」> **SQLEXPRESSSYMC** (自 14.3 RU1 起) 或 **localhost**。
3. 在「工作」下方，按下「立即備份資料庫」。
4. 在「備份資料庫」對話方塊中，選擇性勾選「備份日誌」，然後按下「是」。
5. 按下「確定」。
6. 按下「關閉」。

備份伺服器憑證

您應該備份私密金鑰與憑證，以便在管理伺服器上的電腦遭到毀損時使用。

初始安裝期間，會備份 JKS 密鑰儲存檔案。此外也會備份名為 `server_timestamp.xml` 的檔案。JKS 密鑰儲存檔案包含伺服器的私密和公開金鑰組以及自我簽章憑證。

備份伺服器憑證

1. 在主控台中，按下「管理員」，再按「伺服器」。
2. 在「伺服器」下方，按下要備份其伺服器憑證的管理伺服器。
3. 在「工作」下方，按一下「管理伺服器憑證」，然後按「下一步」。
4. 在「管理伺服器憑證」面板中，按下「備份伺服器憑證」，然後按「下一步」。
5. 在「備份伺服器憑證」面板中，按下「瀏覽」以指定備份資料夾，然後按下「開啟」。

NOTE

您可以將管理伺服器憑證備份至相同的資料夾。

6. 在「備份伺服器憑證」面板中，按「下一步」。
7. 按下「完成」。

更多資訊

- [關於伺服器憑證](#)
- [產生新的伺服器憑證](#)

重新安裝或重新架構 Symantec Endpoint Protection Manager

如果需要重新安裝或重新架構管理伺服器，您可以使用災難復原檔案匯入所有設定。您可以將軟體重新安裝在同一台電腦的同一個安裝目錄中。Symantec Endpoint Protection Manager 會在安裝時建立還原檔案。您也可以使用這個程序重新架構現有站台，或安裝其他用於複寫的站台。

另請參閱：

[Endpoint Protection 的災難復原最佳實務](#)

重新安裝管理伺服器

1. 解除安裝現有管理伺服器。
2. 從安裝檔案安裝伺服器。
[安裝 Symantec Endpoint Protection Manager](#)
3. 在「歡迎使用」面板中，確保勾選「使用還原檔案還原與之前已部署用戶端的通訊」選項，再按「下一步」。
依據預設，復原檔案位於：`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup`。復原檔案會將您的用戶端重新連線至 Symantec Endpoint Protection Manager。
4. 遵照每個面板的指示進行。預設設定適用於大多數情況。如果重新安裝的伺服器連線至現有資料庫，則要將資料庫設定變更為現有資料庫的設定。
必要時，也可還原資料庫。不過，如果 Symantec Endpoint Protection Manager 資料庫位於另一部電腦或未受影響，則不需要還原資料庫。

[還原資料庫](#)

重新架構管理伺服器

1. 按一下「開始 > 所有程式 > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager 工具 > 管理伺服器架構精靈」。
2. 選取下列其中一個選項：
 - 若要在現有的站台上重新架構管理伺服器，請按下「重新架構管理伺服器」。
 - 若要重新架構管理伺服器透過現有的網站遠端複製資料，請按下「重新架構管理伺服器透過不同網站遠端複製」。

此選項會將本機安裝的管理伺服器重新架構為建立新站台並透過網路中的其他現有站台複寫資料。此外，如果您擁有兩個非複寫站台，使用此選項可將其中一個轉換為透過第二個站台複寫的站台。

NOTE

如果保留「使用還原檔案還原與之前已部署用戶端的通訊」為勾選狀態，安裝會繼續。但是，會忽略還原檔案中的預設網域 ID，並使用複寫夥伴的網域 ID。完成重新組態之後，現有用戶端可能會因為網域 ID 發生變更而無法連線。

3. 遵照每個面板的指示進行。

更多資訊

[重新安裝或重新架構 Symantec Endpoint Protection Manager](#)

產生新的伺服器憑證

如果伺服器的 IP 位址或主機名稱發生變更，或私密金鑰遭受破壞，請為 Symantec Endpoint Protection Manager 產生新的伺服器憑證。

依據預設，用戶端伺服器通訊取決於伺服器憑證驗證。如果產生新的伺服器憑證，則此驗證失敗且通訊中斷。請參閱：

[在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證](#)

產生新的伺服器憑證

1. 在主控台中，按下「管理員」，再按「伺服器」。
2. 在「伺服器」下方，按下管理伺服器。
3. 在「工作」下方，按一下「管理伺服器憑證」，然後按「下一步」。
4. 在「管理伺服器憑證」面板中，按下「產生新的伺服器憑證」。確保已勾選「產生新的金鑰」，然後按「下一步」。

「產生新的金鑰」會產生具有新金鑰組 (公開和私密金鑰) 的新憑證。如果取消勾選此選項，新憑證會使用與之前相同的金鑰組，這樣一來會在金鑰組遭受破壞時降低 Symantec Endpoint Protection Manager 伺服器安全性設定檔。

5. 按下「是」，然後按「下一步」。
6. 您必須重新啟動下列服務以使用新的憑證：
 - Symantec Endpoint Protection Manager 服務
 - Symantec Endpoint Protection Manager Webserver 服務。
 - Symantec Endpoint Protection Manager API 服務

如需詳細資訊，請參閱：

- [停止及啟動管理伺服器服務](#)
- [停止和啟動 Apache Web 伺服器](#)

下次您登入 Symantec Endpoint Protection Manager 時，系統會要求您信任新的憑證。

更多資訊

- [接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證](#)
- [登入 Symantec Endpoint Protection Manager 主控台](#)

還原資料庫

如果資料庫損毀或需要執行嚴重損壞修復，您可以還原資料庫。若要還原資料庫，您必須先備份資料庫。請參閱：

[備份資料庫和日誌](#)

NOTE

您必須使用備份資料庫所用的相同 Symantec Endpoint Protection Manager 版本還原資料庫。您可以在本來安裝資料庫的同一部電腦或是不同的電腦上還原資料庫。

還原資料庫可能需要數分鐘的時間才能完成。

若要使用資料庫備份還原資料庫，請執行下列動作：

1. 停止管理伺服器服務。請參閱：
[停止及啟動管理伺服器服務](#)
2. 在「開始」功能表上，按下「所有程式 > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager 工具 > 資料庫備份及還原」。
3. 在「資料庫備份及還原」對話方塊中，按下「還原」。
4. 按下「是」確認還原資料庫。
5. 在「還原網站」對話方塊中，選取備份的資料庫檔案，然後按下「確定」。
6. 尋找備份資料庫時製作的備份資料庫檔案複本。備份的資料庫檔案會預設命名為 date_timestamp.zip。
7. 按下「確定」。
8. 按下「結束」。
9. 重新啟動管理伺服器服務。

若要不使用資料庫備份還原資料庫，請執行下列動作：

在下列情況下，您可能需要不使用資料庫備份還原資料庫：

- 您嘗試過並且無法重設管理員密碼。請參閱：
[重設忘記的 Symantec Endpoint Protection Manager 密碼](#)
 - 您未進行資料庫備份，而資料庫已損毀。
 - 您需要將資料庫還原為新資料庫，而無需重新安裝 SEPM。(跳到步驟3)
1. 備份政策檔。
您在重新安裝資料庫之後匯入了匯出的政策檔。
 2. 如果您有多個網域，請建立名為 SEPBackup.txt 的文字檔案，並新增任何網域 ID。(選擇性)
若要儲存管理伺服器資訊，請將管理伺服器的 IP 位址和主機名稱新增至該檔案。
 3. 停止管理伺服器服務。請參閱：
[停止及啟動管理伺服器服務](#)
 4. 使用「管理伺服器組態精靈」和復原檔案來重新架構管理伺服器。請參閱：
[重新安裝或重新架構 Symantec Endpoint Protection Manager](#)
 5. 在重新架構的 Symantec Endpoint Protection Manager 上，於以下檔案中：
SEPM_Install/tomcat/etc/conf.properties
預設 SEPM_Install 是 C:/Program files (x86)/Symantec/Symantec Endpoint Protection Manager。
變更：
`scm.agent.groupcreation=false` 為 `scm.agent.groupcreation=true`
此編輯可自動建立用戶端群組。否則，用戶端會在登入時重新出現在預設群組中。
用戶端可與 Symantec Endpoint Protection Manager 通訊，但只有在其下次登入後才會重新出現在主控台中。

具 Symantec Endpoint Protection 的虛擬環境

架構在虛擬機器上執行用戶端。

Symantec Endpoint Protection 針對虛擬基礎架構提供共用智慧型掃描快取和「虛擬映像例外」功能，可讓您啟用以改善效能。您需要執行一些額外的安裝和架構工作，才能啟用這些功能。

Table 179: 虛擬基礎架構功能及其用途

功能及用途	說明
使用共用智慧型掃描快取略過已知未受病毒感染的檔案，不進行掃描。	共用智慧型掃描快取會追蹤已知未受病毒感染的檔案。共用智慧型掃描快取可因為不需要重新掃描這些檔案，而減少掃描的負荷。 您可以設定下列類型的共用智慧型掃描快取： - 網路型共用智慧型掃描快取 使用任何類型虛擬基礎架構的虛擬用戶端都可以使用網路型共用智慧型掃描快取。以減少掃描的負荷。 如需詳細資訊，請參閱： 關於共用智慧型掃描快取 我必須怎麼做才能使用網路型共用智慧型掃描快取？
使用「虛擬映像例外」工具，用戶端就可以略過基礎影像檔，不進行掃描。	「虛擬映像例外」工具可讓您將基礎影像檔標記為「安全」，如此就可在掃描期間略過這些檔案，從而減少掃描的負荷。 虛擬映像例外工具僅在虛擬環境中執行。請參閱： 關於虛擬映像例外工具
架構非持續虛擬桌面基礎架構功能。	Symantec Endpoint Protection 用戶端有一項組態設定，會指出用戶端為非持續虛擬用戶端。您可以針對非持續虛擬桌面基礎架構中離線的 GVM 架構不同的老化期間。Symantec Endpoint Protection Manager 會移除離線時間超過指定時間的非持續 GVM 用戶端。請參閱： 在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection 清除過時的非持續 VDI 用戶端以釋放授權

Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 中的防護技術在虛擬基礎架構與實體基礎架構中運作的方式通常相同。您可以在虛擬基礎架構中，採用與實體基礎架構中相同的方式安裝、架構和使用 Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端。

關於共用智慧型掃描快取

使用共用智慧型掃描快取可改善虛擬基礎架構的效能。Symantec Endpoint Protection 用戶端認定未受感染的檔案會新增到快取中。使用相同病毒定義檔版本的後續掃描都可以忽略共用智慧型掃描快取中的檔案。共用智慧型掃描快取僅用於排程掃描和手動掃描。

網路型共用智慧型掃描快取會當作獨立於 Symantec Endpoint Protection 用戶端的 Web 服務執行。共用智慧型掃描快取使用一個投票系統。用戶端使用最新的內容掃描檔案並判斷該檔案未受感染之後，用戶端會傳送投票至快取。如果檔案受感染，則用戶端不會傳送投票。當檔案的投票計數大於或等於投票計數臨界值時，共用智慧型掃描快取就會將檔案視為未受感染。之後當另一個用戶端需要掃描相同的檔案時，該用戶端會先查詢共用智慧型掃描快取。如果檔案因目前的內容而標記為未受感染，則用戶端不會掃描該檔案。

當用戶端傳送投票至共用智慧型掃描快取時，快取會檢查用戶端用來掃描檔案的內容版本。如果用戶端沒有最新的內容，則共用智慧型掃描快取會忽略此投票。如果有可用的更新內容，則更新的內容會成為已知的最新內容，且共用智慧型掃描會將投票計數重設為 1。

為了使快取大小易於管理，共用智慧型掃描快取採用了一種刪減演算法。這個演算法會先移除最舊的快取項目，也就是時間戳記最舊的項目。此演算法可確保快取大小不會超過記憶體使用率臨界值。

更多資訊

- [我必須怎麼做才能使用網路型共用智慧型掃描快取？](#)
- [自訂共用智慧型掃描快取設定](#)
- [在虛擬基礎架構中使用 Symantec Endpoint Protection](#)

關於虛擬映像例外工具

「虛擬映像例外」工具可讓用戶端略過基礎影像檔的威脅掃描。此功能可降低磁碟 I/O 和 CPU 的資源負載。

Symantec Endpoint Protection 同時對受管型用戶端和非受管用戶端支援虛擬映像例外的使用。

NOTE

賽門鐵克不支援在實體環境中使用虛擬映像例外工具。

更多資訊

- [在基礎影像上使用虛擬影像例外工具](#)
- [在虛擬基礎架構中使用 Symantec Endpoint Protection](#)

我必須怎麼做才能使用網路型共用智慧型掃描快取？

您可以使用網路型共用智慧型掃描快取來改善掃描效能。

Table 180: 安裝及使用網路型共用智慧型掃描快取的工作

步驟	工作
步驟 1：安裝共用智慧型掃描快取。	• 實作網路型共用智慧型掃描快取的系統需求 • 安裝和解除安裝網路型共用智慧型掃描快取
步驟 2：在 Symantec Endpoint Protection Manager 的「病毒和間諜軟體」政策中，讓您的虛擬用戶端使用共用智慧型掃描快取。	啟用網路型共用智慧型掃描快取

安裝共用智慧型掃描快取之後，可以選擇性執行下列工作：

- 自訂共用智慧型掃描快取的任何服務、快取或日誌設定。請參閱：
[自訂共用智慧型掃描快取設定](#)
- 檢視日誌中的相關事件。請參閱：
[檢視網路型共用智慧型掃描快取日誌事件](#)
- 使用 Windows 效能管理員監控其效能。請參閱：
[監控網路型共用智慧型掃描快取效能計數器](#)

實作網路型共用智慧型掃描快取的系統需求

網路型共用智慧型掃描快取伺服器設計為在獨立式實體或虛擬機器上執行。不應將共用智慧型掃描快取安裝至執行其他資料庫應用程式或高可用性伺服器應用程式 (如 Symantec Endpoint Protection Manager 或 Microsoft SQL Server) 的電腦上。

下表說明虛擬基礎架構執行共用智慧型掃描快取所需的最低系統需求。

Table 181: 網路型共用智慧型掃描快取系統需求

需求	說明
軟體	- Windows Server 2008 及更新版本 - Windows Server 2012 和 Windows Server 2012 R2 - Windows Server 2016 (自 14.2 MP1 起) - Windows Server 2019 (自 14.2 MP1 起) .NET Framework 4
CPU	共用智慧型掃描快取必須安裝在專用伺服器或虛擬機器上。
記憶體	最小 2 GB
可用磁碟空間	最小 100 MB

更多資訊

- [關於共用智慧型掃描快取](#)
- [安裝和解除安裝網路型共用智慧型掃描快取](#)

安裝和移除網路型共用智慧型掃描快取

在您安裝網路型共用智慧型掃描快取之前，請確定已符合所有系統需求，並且以 Windows 管理員的身分登入。可以在獨立式實體或虛擬機器上安裝並執行共用智慧型掃描快取。

NOTE

您不應在安裝了共用智慧型掃描快取的伺服器的主機名稱中使用 DBCS 或高 ASCII 字元。您還應避免在用於存取的使用者名稱中使用 DBCS 或高 ASCII 字元。這些字元會導致共用智慧型掃描快取服務無法啟動。

如需詳細資訊，請參閱：

[實作網路型共用智慧型掃描快取的系統需求](#)

安裝網路型共用智慧型掃描快取

- 在 Symantec Endpoint Protection 安裝檔案上，瀏覽到 `Tools/Virtualization/SharedInsightCache` 資料夾。
- 連按兩下以下檔案，啟動安裝程式：

`SharedInsightCacheInstallation.msi`

NOTE

您可以改為輸入下列指令來啟動相同的安裝程式：

```
msiexec /i SharedInsightCacheInstallation.msi
```

- 在 **Shared Insight Cache Setup** 精靈窗格中，按下 **Next**。
- 仔細閱讀賽門鐵克軟體授權許可協議，勾選 **I accept the terms of the License Agreement**，然後按下 **Next**。
- 在 **Destination folder** 窗格中，執行下列工作之一：
 - 按下 **Next**，接受共用智慧型掃描快取的預設位置。
 - 按下 **Change**，瀏覽並選取不同的目的資料夾，按下 **OK**，然後按下 **Next**。

6. 在 **Shared Insight Cache Settings** 窗格中，指定以下共用智慧型掃描快取設定：

Cache Usage (% of Physical Memory)	快取的大小上限。 當快取超過此臨界值時，Shared Insight Cache 會刪減快取大小。
Listening Port	伺服器用來接聽的通訊埠。
Status Listening Port	伺服器用來溝通伺服器狀態資訊的通訊埠。

7. 按下「安裝」。

8. 當安裝完成時，按下「完成」。

如需詳細資訊，請參閱：

[自訂共用智慧型掃描快取設定](#)

移除共用智慧型掃描快取的作用與停止共用智慧型掃描快取服務的作用相同。如果不確定是否要永久移除 Shared Insight，可以改為停止快取服務。請參閱：

[關於停止和啟動網路型共用智慧型掃描快取服務](#)

NOTE

若要移除共用智慧型掃描快取，請使用適當的 Windows 控制台，例如「新增或移除程式」。您必須具有 Windows 管理員權限才能解除安裝共用智慧型掃描快取。

如果您解除安裝共用智慧型掃描快取，可能也想要停用 Symantec Endpoint Protection Manager 中的共用智慧型掃描快取。停用共用智慧型掃描快取可避免 Windows 事件日誌在每次用戶端無法聯絡快取時收到通知。

啟用網路型共用智慧型掃描快取

若要透過網路與 Symantec Endpoint Protection 用戶端進行通訊，共用智慧型掃描快取預設不會使用驗證，也不會使用 SSL。如果您將「共用智慧型掃描快取」設定變更為使用「具有 SSL 的基本驗證」或「沒有 SSL 的基本驗證」，則必須指定可存取共用智慧型掃描快取的使用者名稱和密碼。請參閱：

[自訂共用智慧型掃描快取設定](#)

啟用網路型共用智慧型掃描快取

1. 在 Symantec Endpoint Protection Manager 主控台中，開啟適當的「病毒和間諜軟體防護」政策，然後按下「其他」。
2. 在「共用智慧型掃描快取」標籤中，勾選「使用網路共用智慧型掃描快取」。
3. 如果在組態檔中啟用了 SSL 驗證，則按下「需要 **SSL**」。
4. 在「主機名稱」方塊中，輸入您安裝共用智慧型掃描快取所在主機的主機名稱。
5. 在「通訊埠」方塊中，輸入共用智慧型掃描快取的通訊埠號。
6. (選擇性) 如果您架構了共用智慧型掃描快取驗證：
 - 在「使用者名稱」方塊中，鍵入使用者名稱。
 - (選擇性) 按下「變更密碼」將預設密碼 (null) 變更為您為驗證建立的密碼。
如果不想使用密碼，請將這些欄位保留空白。
7. 按下「確定」。

更多資訊

[我必須怎麼做才能使用網路型共用智慧型掃描快取？](#)

自訂共用智慧型掃描快取設定

安裝共用智慧型掃描快取之後，您可以在組態檔中自訂其設定。

架構檔是遵循 .NET Framework 應用程式架構標準的 XML 檔案。如果有無效的架構 (例如有無效的 XML、錯誤的值類型或漏填了必填值)，則共用智慧型掃描快取不會啟動。

如需詳細資訊，請參閱：

[組態編輯器工具 \(SvcConfigEditor.exe\)](#)

下表描述您可以架構的選項。

Table 182: 共用智慧型掃描快取架構選項

選項和預設值	說明和註解
快取服務接聽通訊埠 預設值為 9005。	服務接聽的通訊埠。用戶端會使用接聽埠傳送檔案的掃描結果，以及提出要求來判斷用戶端是否應掃描檔案。 如果接聽埠的範圍不在 0 到 65535 之間，則服務不會啟動。 如果服務無法接聽指定的通訊埠，則它不會啟動。 <endpoint address="http://localhost:9005/1" 依據預設，共用智慧型掃描快取伺服器會接聽所有 IP 位址。若要為 HTTP 或 HTTPS 服務架構接聽 IP 位址，您必須使用 Netsh.exe。共用智慧型掃描快取伺服器會接聽您在這些工具所修改的「IP 接聽清單」中指定的 IP 位址。 Netsh.exe 包含在 Windows Server 2008 中。 如需詳細資訊，請參閱： 架構 HTTP 和 HTTPS
狀態服務接聽通訊埠 預設值為 9006。	伺服器用來溝通伺服器狀態資訊的通訊埠。狀態接聽埠在架構區段中指定的通訊埠上使用以 SOAP 為基礎的介面。此介面提供管理員據以查詢快取伺服器資訊和狀態的機制。 如果這個範圍不在 0 - 65535 之間，則服務不會啟動。 如果服務無法接聽指定的通訊埠，則它不會啟動。
投票計數 預設值為 1。	在共用智慧型掃描快取使用結果之前，必須驗證檔案是否未感染病毒的用戶端數目。 這個值必須小於或等於 15。如果大於 15，則伺服器將使用預設值。 <cache.configuration vote.count="1" />
刪減大小 預設值為 10。	當快取達到記憶體使用量限制時，要從快取移除的記憶體使用量百分比。 這個值必須介於 10 和 100 之間。如果這個值不在 10 和 100 之間，則伺服器將使用預設值。 Note: 賽門鐵克建議您保留預設的刪減大小。 <prune.size="10" />
記憶體用量 預設值為 50。	在共用智慧型掃描快取開始刪減快取前，快取大小的百分比。 必須大於或等於 10。 <mem.usage="50" />
日誌檔 預設值是 install_folder/ CacheServer.log	共用智慧型掃描快取日誌的檔案。 <filevalue="CacheServer.log" />

選項和預設值	說明和註解
日誌等級 預設值為 ERROR。	ALL DEBUG INFO WARN ERROR FATAL 關閉 值 OFF 表示共用智慧型掃描快取不記錄任何訊息。 <pre><level value="ERROR" /></pre> 如需詳細資訊，請參閱： 檢視網路型共用智慧型掃描快取日誌事件
日誌大小 預設值為 10000。	日誌的大小 (位元組)，超過這個大小之後，共用智慧型掃描快取會轉增日誌。 <pre><maximumFileSizevalue="10000" /></pre>
日誌備份 預設值為 1。	刪除最舊的日誌之前要保留的轉增日誌數目。 值 0 表示共用智慧型掃描快取不保留任何備份。負值表示共用智慧型掃描快取保留的備份數不受限制。 <pre><maxSizeRollBackupsvalue="1" /></pre>
啟用 SSL 啟用驗證	依據預設，共用智慧型掃描快取設定為不進行任何驗證，也沒有 SSL。您可以將它變更為「具有 SSL 的基本驗證」、「沒有 SSL 的驗證」，或「沒有 SSL 的基本驗證」。 <pre> <webHttpBinding> <bindingname="CacheServerBinding"> <!-- Uncomment the appropriate section to get the desired security. If enabling ssl modify the uri to use https. A cert will also have to be installed and registered for the ip/port. --> <!-- Basic authentication with SSL.--> <security mode="Transport"> <transport clientCredentialType="Basic"/> </security--> <!-- No authentication with SSL.--> <security mode="Transport"> <transport clientCredentialType="None"/> </security--> <!-- Basic authentication with no SSL.--> <security mode="TransportCredentialOnly"> <transport clientCredentialType="Basic"/> </security--> <!-- No authentication with no SSL. DEFAULT --> <securitymode="None"> <transportclientCredentialType="Basic"/> </security> </binding> </webHttpBinding> </pre> 如需詳細資訊，請參閱： 啟用網路型共用智慧型掃描快取

1. 瀏覽到以下檔案並將其開啟：

```
C:\Program Files (x86)\Symantec\Shared Insight Cache  
\SharedInsightCacheInstallation.exe.config
```

對於舊版安裝，此檔案路徑可能會有所不同。

2. 視需要進行修改。
3. 儲存變更並關閉檔案。
4. 重新啟動共用智慧型掃描快取服務。

您必須重新啟動共用智慧型掃描快取服務，日誌等級以外的所有架構設定才會生效。請參閱：

[關於停止和啟動網路型共用智慧型掃描快取服務](#)

更多資訊

[我必須怎麼做才能使用網路型共用智慧型掃描快取？](#)

關於停止和啟動網路型共用智慧型掃描快取服務

您可能需要暫時停止共用智慧型掃描快取服務才能排除問題。解決問題後，您可以重新啟動該服務。您可以從「服務控制管理員」啟動和停止服務。

移除共用智慧型掃描快取的作用與停止共用智慧型掃描快取服務的作用相同。如果不確定是否要永久移除 Shared Insight，可以改為停止快取服務。

您必須具有 Windows 管理員權限才能停止和啟動共用智慧型掃描快取服務。請參閱：

[排除共用智慧型掃描快取問題](#)

檢視網路型共用智慧型掃描快取日誌事件

您可以檢視共用智慧型掃描快取日誌檔，查看共用智慧型掃描快取建立的任何事件。日誌檔位於安裝資料夾中，名為 CacheServer.log。

共用智慧型掃描快取採用下列格式列印日誌：

```
[|] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message [-]%newline
```

例如：

```
[|] 4 | 12/15/2010 10:51:37 | INFO | CacheServerService.Service | Started service [-]
```

修改組態檔可指定要用於網路型共用智慧型掃描快取的日誌等級。

下表說明您可以設定的等級。

Table 183: 網路型共用智慧型掃描快取日誌等級

日誌等級	說明
關閉	OFF 表示不記錄任何事件。
FATAL	FATAL 訊息會要求您採取動作。這些訊息是一些會導致共用智慧型掃描快取停止的錯誤。 例如，某個 FATAL 訊息可能表示伺服器 IP 位址無法使用，這意味著共用智慧型掃描快取無法執行。
ERROR	ERROR 訊息會要求您採取動作，但相應程序會繼續執行。它們是導致 Shared Insight Cache 發生故障或無法工作的系統錯誤。 您也會接收到 FATAL 訊息的所有日誌項目。 此層級是預設的日誌記錄層級。

日誌等級	說明
WARN	WARN 訊息會指出可能不必要、但不會導致共用智慧型掃描快取失敗的共用智慧型掃描快取行為。您也會收到 FATAL 訊息和 ERROR 訊息的所有日誌項目。
INFO	INFO 訊息描述共用智慧型掃描快取的一般動作或提供其相關資訊。它們可能指出系統狀態，並有助於驗證行為或追蹤問題。不過，單獨使用時，其目的不在呈報可行動項目。 例如，某個資訊訊息可能指出快取刪減已完成。該訊息不提供問題的詳細資料。它只記錄行為。您也會收到 FATAL 訊息、ERROR 訊息及 WARN 訊息的所有日誌項目。
DEBUG ALL	DEBUG 和 ALL 日誌層級訊息產生相同的結果。這些日誌等級僅供支援人員排除共用智慧型掃描快取問題。您也會接收到所有其他日誌層級的所有日誌項目。

只有在需要排除共用智慧型掃描快取的問題時才升高日誌等級。如果升高日誌等級，會使日誌檔開始顯著變大。解決問題後，請恢復為預設的 ERROR 日誌等級。

移至下列位置：

Installation folder/CacheServer.log

更多資訊

[自訂共用智慧型掃描快取設定](#)

監控網路型共用智慧型掃描快取效能計數器

您可以在 Windows 效能監視器中檢視網路型共用智慧型掃描快取統計值。共用智慧型掃描快取服務必須正在執行才能檢視其效能計數器。

Table 184: 共用智慧型掃描快取統計值

統計值	說明
快取中的項目數	此數代表快取中目前的項目數。
快取中已投票為未感染病毒的項目數	此數代表快取中目前已投票為未感染病毒的項目數。
快取要求的數目	對共用智慧型掃描快取服務提出的快取要求數目。 此數目只包含收到 200 回應的有效要求數目。此計數器在服務重新啟動時不會繼續。
更新要求的數目	對服務提出的更新要求數目。 此數目只是收到 200 回應的有效要求。此計數器在服務重新啟動時不會繼續。

監控網路型共用智慧型掃描快取效能計數器

1. 在命令提示下，鍵入下列命令：

```
perfmon
```

2. 在「效能」視窗中的圖形上按下滑鼠右鍵。

3. 選取「新增計數器」。

4. 在「效能物件」下拉式清單中，選取「共用智慧型掃描快取」。

5. 選取要檢視的計數器，然後按下「新增」。

6. 按下「關閉」。

此時「效能」圖形中會顯示您選取的共用智慧型掃描快取計數器。

如需使用 Windows 效能監視器的詳細資訊，請參閱 Windows 說明文件。

更多資訊

- [排除共用智慧型掃描快取問題](#)
- [我必須怎麼做才能使用網路型共用智慧型掃描快取？](#)

排除共用智慧型掃描快取問題

下表提供如何對共用智慧型掃描快取問題進行疑難排解的建議。

Table 185: 共用智慧型掃描快取疑難排解

問題	說明/解決方法
快取結果出現問題	重新啟動服務。請參閱： 關於停止和啟動網路型共用智慧型掃描快取服務
共用智慧型掃描快取傳回「無結果」回應	共用智慧型掃描快取無法成功執行快取查詢時，會傳回「無結果」回應。如果用戶端要求快取查詢，則「無結果」表示必須對檔案進行掃描。 Note: 即使 Shared Insight Cache 無法成功執行快取更新，也會傳回「成功」回應。原因是因為更新失敗時，用戶端不需要執行其他動作。
懷疑 HTTP 流量出現問題	檢視 HTTP 流量錯誤日誌。HTTP 流量錯誤記錄在以下位置： %Windir%\System32\Logfiles\HTTPERR

更多資訊

- [檢視網路型共用智慧型掃描快取日誌事件](#)
- [監控網路型共用智慧型掃描快取效能計數器](#)

在基礎影像上使用虛擬影像例外工具

在您建置虛擬機器之前，可以在基礎影像上使用虛擬影像例外工具。虛擬影像例外工具可讓您的用戶端略過基礎影像檔威脅掃描，這會降低磁碟 I/O 的資源負載。它還會改善虛擬桌面基礎架構中的 CPU 掃描程序效能。

Symantec Endpoint Protection 支援針對受管用戶端和非受管用戶端使用虛擬影像例外工具。

NOTE

您無法在非虛擬環境中使用虛擬影像例外工具。

Table 186: 在基礎影像上使用虛擬影像例外工具的程序

步驟	動作
步驟 1	在基礎影像上，對所有檔案執行完整掃描，以確保檔案是乾淨的。 如果 Symantec Endpoint Protection 用戶端隔離受感染的檔案，您必須修復或刪除隔離的檔案，從隔離所移除它們。
步驟 2	確定用戶端的隔離所空白。
步驟 3	從指令行執行虛擬影像例外工具，以標示基礎影像檔。請參閱： • 執行虛擬影像例外工具 • vietool
步驟 4	在 Symantec Endpoint Protection Manager 中啟用該功能，以便在掃描執行時用戶端知道尋找並略過標示的檔案。請參閱： 架構 Symantec Endpoint Protection 以略過基礎影像檔掃描
步驟 5	從基礎影像移除虛擬影像例外工具。

虛擬影像例外工具支援本機固定式磁碟機。它可處理符合新技術檔案系統 (NTFS) 標準的 檔案。

[更多資訊](#)

[虛擬影像例外工具的系統需求](#)

虛擬映像例外工具的系統需求

Symantec 已在 Virtual Image Exception 工具上測試下列虛擬化產品：

- Citrix XenDesktop 平台
- Nutanix AOS 5.15 (LTS)
- Microsoft Hyper-V
- VMware ESX

用戶端必須安裝在其中一個支援的虛擬環境中。

WARNING

用戶端版本必須與虛擬影像例外工具版本相同。

[更多資訊](#)

如需管理伺服器 and 用戶端所支援的已測試虛擬化產品，請參閱[測試的虛擬安裝和虛擬化產品](#)。

[在基礎影像上使用虛擬影像例外工具](#)

執行虛擬影像例外工具

執行虛擬影像例外工具之前，請確保已符合所有系統需求。

WARNING

用戶端版本必須與虛擬影像例外工具版本相同。

如需詳細資訊，請參閱：

[虛擬影像例外工具的系統需求](#)

執行虛擬影像例外工具

1. 從安裝檔案的 Symantec Endpoint Protection 工具資料夾，將以下檔案下載到基礎影像：

```
/Virtualization/VirtualImageException/vietool.exe
```

2. 以管理權限開啟指令提示。
3. 用正確的引數執行虛擬影像例外工具。

例如，輸入：`vietool c: --generate`

[更多資訊](#)

[vietool](#)

架構 Symantec Endpoint Protection 以略過基礎影像檔掃描

您在基礎影像檔上執行虛擬影像例外工具之後，可以在 Symantec Endpoint Protection Manager 中啟用使用虛擬影像例外。啟用這個功能後，虛擬用戶端就會尋找工具所插入的屬性。然後 Symantec Endpoint Protection 會略過掃描包含該屬性的基礎影像檔。

您可以略過「自動防護」掃描或管理員定義掃描 (例如手動掃描或排程掃描) 中未變更的基礎影像檔，不進行掃描。

架構 Symantec Endpoint Protection 使用虛擬影像例外略過掃描基礎影像檔

1. 在主控台上，開啟適當的「病毒和間諜軟體防護」政策。
2. 在「進階選項」下方，按一下「其他」。
3. 在「虛擬影像」標籤上，勾選要啟用的選項。
4. 按下「確定」。

更多資訊

[在基礎影像上使用虛擬影像例外工具](#)

在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection (NPVDIs)

您可以在虛擬環境中架構 Symantec Endpoint Protection。

Table 187: 在非持續虛擬桌面基礎架構中若要使用 Symantec Endpoint Protection 需執行的工作

步驟	說明
步驟 1：設定基礎影像。	您可以在基礎影像中架構 Symantec Endpoint Protection 用戶端，以指出其為非持續虛擬用戶端。請參閱： 針對 VDI 中的非持續訪客虛擬機器設定基礎影像
步驟 2：在 Symantec Endpoint Protection Manager 中，架構離線非持續 VDI 用戶端的獨立清除間隔。	Symantec Endpoint Protection Manager 會移除離線超過指定時間的非持續 GVM 用戶端。這項功能可以簡化管理 Symantec Endpoint Protection Manager 中的 GVM。請參閱： 清除過時的非持續 VDI 用戶端以釋放授權

針對非持續 VDI (NPVDIs) 中的非持續訪客虛擬機器設定基礎影像

您可以設定基礎影像，以便更簡化使用 Symantec Endpoint Protection Manager 在非持續虛擬桌面基礎架構中管理 GVM 的方式。

Table 188: 針對非持續 GVM 設定基礎影像的工作

步驟	說明
步驟 1：將 Symantec Endpoint Protection 安裝在基礎影像上。	如需詳細資訊，請參閱： 選擇使用用戶端部署精靈安裝用戶端的方法
步驟 2：在管理伺服器中停用「竄改防護」，以便可以修改登錄。	如需詳細資訊，請參閱： 變更竄改防護設定
步驟 3：確保 Symantec Endpoint Protection Manager 會正確計算非持續虛擬用戶端的授權數目。	非持續用戶端的優點在於離線非持續用戶端不會計入已部署授權的數量。只有線上用戶端會計入。若將虛擬用戶端標示為非持續用戶端，您必須在基礎影像中建立登錄機碼。 如需詳細資訊，請參閱： 如何針對非持續 VDI 用戶端管理授權計數
步驟 4：在 Symantec Endpoint Protection Manager 中，重新啟用「竄改防護」。	如需詳細資訊，請參閱： 變更竄改防護設定

設定完基礎影像之後，可以在 Symantec Endpoint Protection Manager 中針對非持續用戶端架構獨立的清除間隔。請參閱：

[清除過時的非持續 VDI 用戶端以釋放授權](#)

清除過時的非持續 (NPVDI) 用戶端以釋放授權

長時間下來，過時用戶端可能會累積在 Symantec Endpoint Protection Manager 資料庫中。過時用戶端是指未連線至 Symantec Endpoint Protection Manager 達 30 天的用戶端。Symantec Endpoint Protection Manager 預設為每隔 30 天會清除過時用戶端。

如果您不想要等待同樣的天數來清除過時的非持續用戶端，可以為這些用戶端架構獨立的間隔。如果您沒有架構獨立的間隔，則離線非持續虛擬用戶端會按照清除過時實體用戶端的相同間隔進行清除。

線上非持續用戶端會計入已部署授權數量；離線非持續用戶端則不會。請參閱：

[如何針對非持續 VDI 用戶端管理授權計數](#)

您也可以在此「用戶端」頁面上，從檢視篩選離線非持續用戶端。

清除過時的非持續 VDI 用戶端以釋放授權

1. 在 Symantec Endpoint Protection Manager 主控台的「管理員」頁面上，按下「網域」。
2. 在「網域」樹狀結構中，按下所要的網域。
3. 在「工作」下方，按下「編輯網域屬性」。
4. 在「編輯網域屬性 > 一般」標籤中，勾選「刪除指定的時間內未連線的非持續 VDI 用戶端」核取方塊，然後將「天」的值變更為所要的數字。
「刪除指定的時間內未連線的用戶端」選項必須勾選，才能存取離線非持續 VDI 用戶端的選項。
5. 按下「確定」。

更多資訊

[在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection](#)

如何管理非持續虛擬桌面基礎架構 (NPVDI) 用戶端的授權計數

管理伺服器會針對實體電腦（無論電腦是處於線上還是離線狀態）上的用戶端計算每個授權。如果是虛擬用戶端，管理伺服器僅計算線上非持續用戶端的授權。不計算離線非持續用戶端。如果您擁有的使用者數目超過您擁有的用戶端數目，請使虛擬用戶端成為非持續用戶端。

若將虛擬用戶端標示為非持續用戶端，您必須在基礎影像中建立登錄機碼。

針對非持續 VDI 用戶端管理授權計數

1. 安裝 Symantec Endpoint Protection 用戶端並停用「竄改防護」之後，在基礎影像上開啟登錄編輯器。請參閱：
[變更竄改防護設定](#)
2. 瀏覽到以下其中一個登錄機碼：
 - 在 32 位元的電腦上：HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
 - 在 64 位元的電腦上 (14.3 RU4 或更舊版本)：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\
 - 在 64 位元的電腦上 (14.3 RU5 或更新版本)：HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
3. 建立一個名為 Virtualization 的新子機碼。
4. 在 Virtualization 子機碼中，建立名為 IsNPVDIClient 的 DWORD 類型機碼，然後為其指派值 1。

更多資訊

-
- 清除過時的非持續 VDI 用戶端以釋放授權
 - 針對 VDI 中的非持續訪客虛擬機器設定基礎影像

vietsol

vietsol

vietsol - 執行虛擬影像例外工具

簡介

```
vietsol.exe volume: --generate|clear|verify|hash [options ...]
```

說明

vietsol 指令透過新增屬性來標示所指定磁碟區上的基礎影像檔。

選項

--generate

對指定磁碟區上的所有檔案執行虛擬影像例外工具。不能將此選項與 --clear 搭配使用。

例如：vietsol c: --generate

--verify

確認已針對指定磁碟區上的所有檔案設定虛擬影像例外。不能將此選項與 --clear 搭配使用。

例如：vietsol c: --verify

--clear

移除指定磁碟區上的所有檔案的虛擬影像例外。

例如：vietsol.exe c: --clear

刪除特定檔案：vietsol.exe c:\Users\Administrator\target.file --clear

您可以使用完整路徑代替磁碟區識別元，清除單個檔案或資料夾內容的虛擬影像例外。每個指令行只允許有一個檔案名稱、資料夾名稱或磁碟區識別元。不能將此指令與 --generate、--verify 或 --hash 搭配使用。

執行 --clear 指令後，必須重新啟動用戶端。

--hash

針對指定磁碟區上的所有檔案產生雜湊值。

虛擬影像例外工具會使用雜湊將本機檔案排除在以後的掃描外。用戶端會分別計算檔案雜湊，以傳送到共用智慧型掃描快取來儲存掃描結果。不能將此選項與 --clear 搭配使用。

例如：vietsol.exe c: --generate --hash

--volume arg

指定該工具掃描的磁碟區。

使用 --clear 選項時，此選項可以是一個檔案。您必須指定磁碟區，磁碟區可以使用磁碟區旗標進行指定，也可以單獨進行指定。例如，使用旗標指定 vietsol.exe --volume c: --generate，或單獨指定 vietsol.exe c: --generate。

--verbose

將大量的程式執行資訊輸出到主控台。

--stop

在該工具遇到第一個錯誤時停止。否則，該工具會將錯誤資訊寫入主控台，然後繼續。

--help

顯示此說明訊息。

API

使用 API 與第三方產品整合。

您可以使用 API 將第三方安全性、報告或其他功能整合至 Symantec Endpoint Protection Manager。

Symantec Endpoint Protection API 指令

Symantec Endpoint Protection 提供一組 REST API，其適用於與各種第三方應用程式整合以執行作業。

Table 189: Symantec Endpoint Protection API

API 類別	連結
管理員	- 取得所有管理員使用者詳細資訊 - 建立管理員使用者 - 取得管理員使用者詳細資訊 - 更新管理員使用者 - 取得本機資料庫 - 取得伺服器 - 取得 TDAD 伺服器詳細資訊 - 更新 TDAD 伺服器詳細資訊 - 刪除 TDAD 伺服器詳細資訊 - 取得所有授權 - 新增新的授權 - 取得授權架構 - 取得權利 - 取得 SEPM 授權摘要 - 取得目前使用者 Token
黑名單	- 依名稱取得檔案指紋列印清單 - 新增黑名單 - 取得檔案指紋列印清單 - 更新黑名單 - 刪除黑名單
雲端	- 取得雲端註冊 - 啟用自動政策同步 - 取得註冊狀態 - 進行雲端註冊 - 取消雲端註冊 - 取得集線器狀態 - 已註冊

API 類別	連結
指令	• 作用中掃描 • 取得基準行指令 • 成為雲端管理 • EOC 指令 • 取得二進位檔案內容 • 取得二進位檔案詳細資訊 • 取得檔案命令 • 完整掃描 • 使 IRON 快取項目無效 • 套用授權覆寫 • 重設授權覆寫 • 隔離指令 • 更新內容指令 • 取得指令狀態詳細資訊 • 取消指令
電腦	• 取得電腦 • 移動用戶端 • 刪除用戶端 • 註冊 • 註冊狀態 • 刪除電腦
內容	• 取得 AV Def 最新資訊
網域	• 取得網域 • 新增網域 • 取得網域名稱 • 取得網域 • 更新網域已啟用狀態 • 更新網域 • 刪除網域
事件	• 發佈通知確認 • 取得關鍵事件資訊

API 類別	連結
群組	• 同步刪除群組 • 同步群組 • 不同步群組 • 取得群組雲端外部通訊設定 • 更新群組外部通訊 • 從群組撤銷設定 • 從群組取得政策 ID • 將政策指派給群組 • 從群組撤銷政策 • 從群組取得政策 ID • 將政策指派給群組 • 從群組撤銷政策 • 從我的公司取得群組詳細資訊 • 從 SAEP 群組 ID 取得群組詳細資訊 • 取得群組 • 取得群組詳細資訊 • 建立群組 • 刪除群組 • 修補群組 • 依群組 ID 取得電腦 • 取得群組外部通訊設定 • 放置群組外部通訊 • 修補群組外部通訊 • 取得群組的位置 ID • 取得群組位置外部通訊設定 • 放置群組位置外部通訊 • 修補群組位置外部通訊 • 取得位置的政策類型 • 取得類型的政策 ID • 取得隔離的政策類型 • 取得類型的隔離政策 ID • 取得群組設定 • 修補群組設定 • 取得位置 XML • 將政策指派至位置 • 取得指派給群組的政策 • 將政策指派給群組 • 將指紋指派至群組
群組更新提供者	• 取得 GUP 資料
身分	• 驗證使用者 • 登出
通知	• 發佈外部通知

API 類別	連結
政策	• 建立例外政策 • 取得例外政策 • 編輯例外政策 • 刪除例外政策 • 更新例外政策 • 取得防火牆政策 • 刪除防火牆政策 • 建立 HID 政策 • 取得 HID 政策 • 編輯 HID 政策 • 刪除 HID 政策 • 更新 HID 政策 • 取得 IPS 政策 • 建立授權政策 • 取得 LiveUpdate 政策 • 建立 MEM 政策 • 取得 MEM 政策 • 編輯 MEM 政策 • 刪除 MEM 政策 • 更新 MEM 政策 • 取得政策 XML • 取得政策摘要 • 取得具政策類型的政策摘要 • 建立 TDAD 政策 • 取得 TDAD 政策 • 編輯 TDAD 政策 • 刪除 TDAD 政策 • 更新 TDAD 政策 • 建立例外政策 • 取得例外政策 • 編輯例外政策 • 刪除例外政策 • 更新例外政策
複寫	• 網站是否具有複寫夥伴 • 立即複寫 • 取得複寫狀態
報告	• 驗證使用者
要求的檔案	• 取得 Sha256 的二進位檔案內容
統計資料	• 取得自動解析的攻擊計數 • 取得用戶端 Def 狀態 • 取得用戶端內容下載來源 • 取得被感染的用戶端 • 取得惡意軟體用戶端統計資料 • 取得用戶端連線離線計數統計資料 • 取得風險分佈統計資料 • 取得用戶端版本 • 取得威脅統計資料

API 類別	連結
針對 Active Directory 的威脅防禦	- 取得政策 - 發佈政策 - 放置政策 - 刪除政策 - 修補政策 - 取得政策 - 刪除政策
版本	取得版本

Symantec Endpoint Protection 疑難排解

瞭解如何對 Symantec Endpoint Protection 問題進行疑難排解。

下表顯示在安裝和使用 Symantec Endpoint Protection 時可能會遇到的最常見問題。

Table 190: 您可以解決的常見問題

工作	說明
解決安裝問題	您可以下載並執行 Symantec Diagnostic Tool (SymDiag) 來驗證電腦是否已做好安裝準備。此工具是透過管理伺服器 and 用戶端上的「說明」，由 Broadcom 支援網站提供。請參閱： • 使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解 • 找出安裝的失敗點
修復 Microsoft SQL Server 資料庫的問題	您可使用預設的 Microsoft SQL Server Express 資料庫或 Microsoft SQL Server 資料庫解決升級和安裝問題。 更多資訊： • 維護資料庫 • 升級前增加 Symantec Endpoint Protection Manager 可用磁碟空間 • 增加 Microsoft SQL Server 資料庫檔案大小 • 為 Microsoft SQL Server 資料庫啟用 FILESTREAM • 架構 Symantec Endpoint Protection Manager 與 Microsoft SQL Server 之間的加密通訊 • Symantec Endpoint Protection Manager 偵測到已架構的電子郵件伺服器需要停用憑證驗證 • 解決 14.3 RU5 或更新版本安裝或升級後的 Microsoft SQL Server 資料庫連線錯誤
處理病毒疫情 (爆發)	您可以防止威脅攻擊網路上的電腦。請參閱： • 阻止和處理病毒和間諜軟體對用戶端電腦的攻擊 • 移除病毒和安全風險 如果確實有威脅在攻擊用戶端電腦，您可以識別威脅並做出回應。請參閱： 網路上的病毒移除和疑難排解
內容更新問題疑難排解	如果 Symantec Endpoint Protection Manager 或用戶端未正確更新最新病毒定義檔，請參閱下列文章： 疑難排解 Endpoint Protection Manager 的 LiveUpdate 和定義檔問題 如需詳細資訊，請參閱： Symantec Endpoint Protection : LiveUpdate 疑難排解流程圖
解決通訊問題	Symantec Endpoint Protection 的所有元件之間的通訊通道都必須處於開啟狀態。這些通道包括下列項目：伺服器到用戶端、伺服器到資料庫以及伺服器和用戶端到內容傳送元件 (如 LiveUpdate) 之間的通道。請參閱： • Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解 • Symantec Endpoint Protection Manager 與主控台或資料庫之間的通訊問題疑難排解 • 群組更新提供者的最佳實務和疑難排解 • Symantec Endpoint Protection (SEP) 所需的外部 URL
執行災害復原	發生資料庫損毀或硬體故障時，如果您有資料庫備份檔案，則可以還原資料庫的最新快照。請參閱： Endpoint Protection 的災難復原最佳實務
報告問題疑難排解	您可以解決各種報告和日誌問題。請參閱： 報告問題疑難排解
疑難排解複寫問題	如需詳細資訊，請參閱： Symantec Endpoint Protection 的遠端複製疑難排解流程圖

更多資訊

使用 SymDiag 進行 Windows 用戶端健康狀態疑難排解和檢查

SymDiag 會評估 Symantec 產品的安全健康狀態、識別常見問題，以及收集資料和日誌以進行輔助疑難排解。

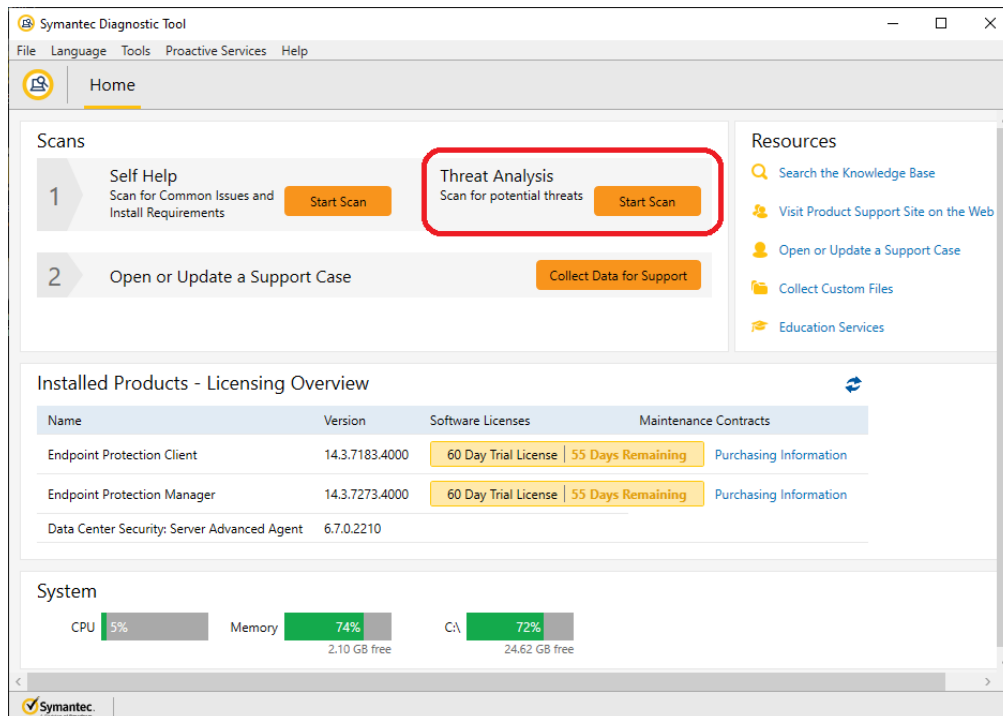
Symantec Diagnostic (SymDiag) 工具提供 Symantec 產品技術問題、零時差威脅分析、最佳作法建議和主動型服務的自助支援。

SymDiag：

- 迅速和準確地識別已知的問題。
- 工具在辨識問題之後，會將您重新導向到資源以讓您自行解決問題。
- 如果問題未解決，工具可讓您輕鬆將資料提交給技術支援以進行進一步診斷。

下載和使用 SymDiag 工具

1. 從下列網站下載工具：[下載 SymDiag 以偵測產品問題](#)
2. 按兩下 SymDiag.exe 圖示。
3. 在「Symantec Diagnostic Tool > 首頁」頁面上，執行下列其中一個工作：
 - 若要檢查您的安全性，請按下「威脅分析」下方的「開始掃描」。



- 對於其他自助和疑難排解問題，請按下「自助」下方的「開始掃描」。

於安裝或升級期間在 Microsoft Windows Server 2008 R2 上啟用 TLS 1.0 和 1.1

在 Microsoft Windows Server 2008 R2 上安裝或升級至 Symantec Endpoint Protection Manager (SEPM) 14.3 RU4 或更高版本期間，可能會看到下列訊息。

- Microsoft Windows Server 2008 R2 ##### Symantec Endpoint Protection Manager ####
TLS 1.1####TLS 1.1 ## TLS 1.2 ##### Windows 2012 R2

在您看到「管理伺服器架構精靈」(安裝) 或「管理伺服器升級精靈」(升級) 之前會顯示此訊息。

您必須修正此問題，因為 SEPM 使用 TLS (傳輸層安全性) 與用戶端和資料庫進行通訊。Microsoft Windows Server 2008 R2 使用 TLS 1.1，而其不如 TLS 1.2 安全。結束 Windows Server 2008 R2 支援時，Microsoft 已停用 TLS 1.0 和 1.1。

若要確保 SEPM 與用戶端和資料庫通訊，您必須執行下列其中一項任務：

- 升級為支援的 Microsoft Windows 版本 (建議)。
- 啟用 TLS 1.0 和 1.1。

NOTE

14.3 RU4 是在 Windows Server 2008 R2 上安裝或升級之 SEPM 的最後一個版本。賽門鐵克建議您升級為含 TLS 1.2 支援的較新 Windows 版本，以進行更安全的通訊。

在 Microsoft Windows Server 2008 R2 上啟用 TLS 1.0 和 1.1

WARNING

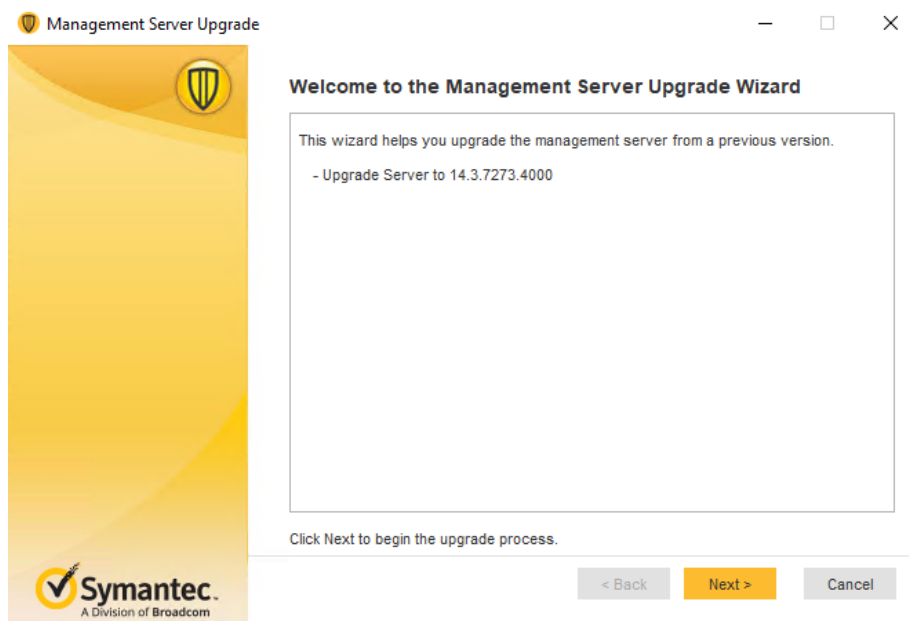
您必須先啟用 TLS 1.0 和 1.1，才會出現「管理伺服器架構精靈」(安裝) 或「管理伺服器升級精靈」(升級)，否則您會看到失敗訊息。

在您選取「下一步」按鈕之前，啟用 TLS：

- 若為第一次安裝：



- 若為升級：



如要於安裝或升級期間在 **Windows** 上啟用 **TLS 1.0** 和 **1.1**

1. 在管理伺服器電腦上，開啟 `<SEPM_Install>\jre11\conf\java.security` 檔案。
例如：`C:\Program Files\Symantec\Symantec Endpoint Protection Manager\jre11\conf\security\java.security`
2. 在 `java.security` 檔案中，搜尋下行：`jdk.tls.disabledAlgorithms`，其列出已停用的通訊協定 (包括 **TLSv1.0** 和 **TLSv1.1**)。

例如：

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA, \ DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \ include jdk.disabled.namedCurves
```

3. 從停用的通訊協定行中移除 **TLSv1.0** 和 **TLSv1.1**。

例如：

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, \ DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \ include jdk.disabled.namedCurves
```

如要於安裝或升級期間在 **Windows** 上啟用 **TLS 1.0** 和 **1.1**

若您未於安裝之後啟用 **TLS 1.0** 和 **1.1**，則請重新啟動安裝或升級精靈。

- 執行下列其中一項工作：
 - 若為第一次安裝，請按兩下 `Symantec\Symantec Endpoint Protection Manager\bin\sca.bat`，以重新啟動「管理伺服器架構精靈」。
 - 若為升級，請按兩下 `Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat`，以重新啟動「管理伺服器升級精靈」。

找出用戶端安裝的失敗點

Windows Installer 和「推送部署精靈」會建立日誌檔，這些日誌檔可用於確認安裝是否成功。日誌檔會列出成功安裝的元件，並提供安裝套件的各種詳細資訊。您可使用日誌檔來協助辨識會造成安裝失敗的元件或動作。如果您無法判斷安裝失敗的原因，就必須保留日誌檔。如果需要，請將這個檔案提供給賽門鐵克技術支援。

NOTE

每次執行安裝封裝時，日誌檔都會被覆寫。

識別用戶端安裝的失敗點

1. 使用文字編輯器，開啟安裝程式所產生的日誌檔。
2. 若要尋找失敗，請搜尋以下項目：

Value 3

在此項目所在那一行前面的動作，最有可能是造成失敗的動作。在這個項目後面出現的各行，是因安裝不成功而傳回的安裝元件。

更多資訊

[選擇使用用戶端部署精靈安裝用戶端的方法](#)

Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解

如果用戶端與伺服器之間的通訊出現問題，您應該先檢查確定網路沒有任何問題。您也應該檢查網路連線，若仍無法解決問題，才電洽「賽門鐵克技術支援」。

您可以透過多種方式，檢查用戶端與管理伺服器之間的通訊。

Table 191: 檢查管理伺服器與用戶端之間的連線

檢查的項目	解決方案
查看用戶端是否連線到管理伺服器	您可以下載並檢視用戶端上的疑難排解檔案，確認通訊設定。請參閱： • Symantec Endpoint Protection 用戶端狀態圖示 • 在用戶端電腦上檢查與管理伺服器的連線 • 在用戶端上使用疑難排解檔案調查防護問題
測試用戶端與管理伺服器之間的連線	您可以執行幾項工作來檢查用戶端與管理伺服器之間的連線。 • 請參閱：啟用並檢視存取日誌，以檢查用戶端是否連線到管理伺服器 • 從用戶端電腦測試與管理伺服器的連線。請參閱：使用 ping 指令測試與管理伺服器的連線 • 在用戶端電腦上使用網頁瀏覽器連線到管理伺服器。請參閱：使用瀏覽器測試與 Symantec Endpoint Protection 用戶端上的 Symantec Endpoint Protection Manager 的連線
檢查管理伺服器是否使用正確的伺服器憑證	如果您重新安裝了 Symantec Endpoint Protection Manager，請檢查是否已套用正確的伺服器憑證。如果管理伺服器使用不同的伺服器憑證，伺服器仍可下載內容，但用戶端會無法讀取內容。如果管理伺服器使用了錯誤的伺服器憑證，您必須加以更新。請參閱： • 更新或還原伺服器憑證 您可以透過檢查下列項目，驗證管理伺服器是否使用錯誤的伺服器憑證： • 用戶端沒有在工作列中顯示綠點，表示它未與管理伺服器通訊。請參閱：檢查用戶端是否已連線至管理伺服器且受保護 • 用戶端未從管理伺服器接收政策更新。 • 管理伺服器顯示它未與用戶端連線。請參閱：Symantec Endpoint Protection 用戶端狀態圖示

檢查的項目	解決方案
檢查網路是否有問題	您應該檢查下列項目，以確認網路沒有任何問題： • 可先測試用戶端與管理伺服器之間的連線。如果用戶端電腦無法測試與管理伺服器的連線，或者無法以 Telnet 連線到管理伺服器，您應該確認用戶端的 DNS 服務是否正常。 • 檢查用戶端的路由路徑。 • 檢查管理伺服器是否存在網路問題。 • 檢查 Symantec Endpoint Protection 防火牆 (或任何第三方防火牆) 是否造成任何網路問題。
檢查用戶端上的除錯日誌	您可以使用用戶端上的除錯日誌，判斷用戶端是否有通訊問題。請參閱： • 檢查用戶端電腦上的除錯日誌 • 檢查管理伺服器上的收件匣日誌
復原失去的用戶端通訊	用戶端若失去與管理伺服器之間的通訊，可使用工具復原通訊檔案。請參閱： 使用 SylinkDrop 工具還原用戶端伺服器通訊設定

如果 Symantec Endpoint Protection Manager 顯示記錄錯誤或 HTTP 錯誤碼，請參閱下列文章：

[Symantec Endpoint Protection Manager 通訊疑難排解](#)

在用戶端電腦上檢查與管理伺服器的連線

如果您具有受管用戶端，您可以檢查與管理伺服器的連線。如果您沒有連線到管理伺服器，您可以要求用戶端連線。請參閱：

[疑難排解 Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題](#)

在用戶端電腦上檢查與管理伺服器的連線

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「連線狀態」。
3. 在「連線狀態」窗格中，您可以看到最後嘗試的連線和最後成功的連線。
4. 若要重新建立與管理伺服器的連線，請按下「立即連線」。

在用戶端上使用疑難排解檔案調查防護問題

若要檢查用戶端問題，您可以查看用戶端電腦上的 Troubleshooting.txt 檔案。Troubleshooting.txt 檔案的資訊包括政策、病毒定義檔以及其他用戶端相關資料。

賽門鐵克技術支援可能會要求您以電子郵件方式寄送 Troubleshooting.txt 檔案。請參閱：

[Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

從用戶端匯出疑難排解檔案

1. 在用戶端電腦中開啟用戶端。
2. 在用戶端中按下「說明」>「疑難排解」。
3. 在「管理」窗格的「疑難排解資料」底下按「匯出」。
4. 在「另存新檔」對話方塊中，接受預設的疑難排解檔案名稱或輸入新的檔案名稱，然後再按下「儲存」。

您可以將檔案儲存在桌面或指定資料夾。

5. 利用文字編輯器，開啟 Troubleshooting.txt 查看內容。

啟用並檢視存取日誌，以檢查用戶端是否連線到管理伺服器

您可以檢視管理伺服器上的 Apache HTTP 伺服器存取日誌，檢查用戶端是否連線到管理伺服器。如果用戶端有連線，表示用戶端的連線問題可能不是網路方面的問題。網路問題包括防火牆攔截存取或網路之間無法連線。

您必須先啟用 Apache HTTP 伺服器存取日誌才能檢視日誌。

NOTE

請在檢視完畢後停用日誌，因為日誌會佔用不必要的 CPU 資源和硬碟空間。

如需詳細資訊，請參閱：

[Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

NOTE

SEPM_Install 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。

啟用 Apache HTTP 伺服器存取日誌

- 1. 在文字編輯器中，開啟檔案 SEPM_Install\apache\conf\httpd.conf。
- 2. 在 httpd.conf 檔案中，移除以下文字字串中的井字號 (#)，然後儲存檔案：
#CustomLog "logs/access.log" combined
- 3. 停止並重新啟動 Symantec Endpoint Protection Manager 服務和 Apache HTTP 伺服器。
[停止及啟動管理伺服器服務](#)
[停止和啟動 Apache Web 伺服器](#)

檢視 Apache HTTP 伺服器存取日誌

- 1. 在管理伺服器上，開啟檔案 SEPM_Install\apache\logs\access.log。
- 2. 尋找用戶端電腦的 IP 位址或主機名稱，這表示用戶端已連線到 Apache HTTP 伺服器。
- 3. 停用 Apache HTTP 伺服器存取日誌。

停止和啟動 Apache Web 伺服器

當您安裝 Symantec Endpoint Protection Manager 時，它會安裝 Apache Web 伺服器。Apache Web 伺服器會執行成為自動服務。您可能需要停止並重新啟動 Web 伺服器，才能啟用 Apache HTTP 伺服器存取日誌。請參閱：

[啟用並檢視存取日誌，以檢查用戶端是否連線到管理伺服器](#)

停止 Apache Web 伺服器	從指令提示處輸入： net stop semwebsrv
啟動 Apache Web 伺服器	從指令提示處輸入： net start semwebsrv

使用 ping 指令測試與管理伺服器的連線

您可以嘗試從用戶端電腦使用 ping 指令，測試管理伺服器的連線。請參閱：

[Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

使用 ping 指令測試與管理伺服器的連線

- 1. 在用戶端上，開啟命令提示字元。
- 2. 輸入 ping 指令。例如：

ping 名稱

其中 名稱 是管理伺服器的電腦名稱。您可以使用伺服器 IP 位址取代電腦名稱。在這兩種狀況下，指令應該都會傳回正確的伺服器 IP 位址。

如果 ping 指令未傳回正確位址，請確認用戶端的 DNS 服務並檢查其路由路徑。

使用瀏覽器測試與 Symantec Endpoint Protection Manager 用戶端上的 Symantec Endpoint Protection 的連線

您可以在用戶端電腦上使用網頁瀏覽器測試管理伺服器與用戶端之間的連線。此方法有助於判斷問題是出於連線或網路，還是用戶端本身。

您也可以使用下列方法檢查管理伺服器與用戶端電腦的之間連線：

- 查看 Symantec Endpoint Protection 用戶端狀態圖示是否顯示綠點。請參閱：
[Symantec Endpoint Protection 用戶端狀態圖示](#)
- 檢查 Symantec Endpoint Protection 用戶端的連線狀態。請參閱：
[在用戶端電腦上檢查與管理伺服器的連線](#)

使用瀏覽器測試與 Symantec Endpoint Protection 用戶端上的 Symantec Endpoint Protection Manager 的連線

1. 在用戶端電腦上開啟網頁瀏覽器，例如 Internet Explorer。
2. 在瀏覽器指令行中，鍵入下列指令：

```
http://SEPMServer:8014/secars/secars.dll?hello,secars
```

其中 SEPMServer 是管理伺服器的 DNS 名稱、NetBIOS 名稱或 IP 位址。

IP 位址包括 IPv4 和 IPv6。您必須用方括弧括住 IPv6 位址：`http://[SEPMServer]:##`

3. 當網頁出現時，尋找是否有下列其中一種結果：
 - 如果出現 **OK** 一字，表示用戶端電腦已連線到管理伺服器。請檢查用戶端本身是否有問題。
 - 如果未出現 **OK** 一字，表示用戶端電腦未連線到管理伺服器。請檢查用戶端的網路連線以及用戶端電腦上是否正在執行網路服務。確認用戶端的 DNS 服務並檢查其路由路徑。請參閱：
[Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

檢查用戶端電腦上的除錯日誌

您可以檢查用戶端上的除錯日誌。如果用戶端與管理伺服器之間的通訊出現問題，日誌會顯示連線問題的狀態訊息。請參閱：

[Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)

您可以使用下列方法檢查除錯日誌：

- 在用戶端的「說明及支援」功能表中，按下「疑難排解」對話方塊中的「編輯除錯日誌設定」，然後輸入日誌的名稱。您可以接著按下「檢視日誌」。
- 您可以使用 Windows 登錄在用戶端上開啟除錯功能。
您可以在下列位置找到 Windows 登錄機碼：
`HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on`

檢查管理伺服器上的收件匣日誌

您可以使用 Windows 登錄機碼，產生管理伺服器收件匣活動的日誌。修改 Windows 登錄機碼時，管理伺服器會產生日誌 (ersecreg.log 及 exsecars.log)。您可以檢視這些日誌，以解決用戶端與伺服器通訊的問題。請參閱：

- [Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解](#)
- [檢查用戶端電腦上的除錯日誌](#)

檢查管理伺服器上的收件匣日誌

1. 在管理伺服器的 `HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM` 下方，將 DebugLevel 值設為 3。

收件匣會出現在管理伺服器電腦的下列預設位置：`SEPM_Install\data\inbox\log`

SEPM_Install 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager#

2. 使用「記事本」開啟日誌。

Symantec Endpoint Protection Linux Agent 或 Symantec Single Agent for Linux 疑難排解

使用這些提示，對 Symantec Endpoint Protection Linux Agent 或 Symantec Single Agent for Linux 問題進行疑難排解。

NOTE

在本主題中，Symantec Single Agent for Linux 和 Symantec Endpoint Protection Linux Agent 稱為 Linux Agent。

下表顯示用於對 Linux Agent (自 14.3 RU1 起) 進行疑難排解的資源。

Table 192: 對 Symantec Linux Agent 進行疑難排解的資源

動作	說明
檢查代理程式的狀態。	若要檢查代理程式的版本和連線狀態，以及確認是否已載入模組以及是否精靈是否正在執行，請導覽至 /usr/lib/symantec，並執行下列指令： ./status.sh
檢查代理程式套件的版本。	導覽至 /usr/lib/symantec，並執行下列指令： ./version.sh
檢視日誌。	您可以在下列位置找到 Symantec Linux Agent 日誌： - AMD 日誌 - 提供掃描相關資訊。 /var/log/sdcssllog/amd.log - CAF 日誌 - 提供代理程式活動相關資訊，例如與伺服器、註冊、指令、事件、政策版本、內容版本等的通訊。 /var/log/sdcssl-caflog/cafagent.log - 代理程式日誌 - 提供代理程式活動的一些合併相關資訊 (掃描資訊、更新資訊)。 /var/log/sdcssllog/SISIDSEvents*.csv - CVE 日誌 - 提供 Symantec Endpoint Protection Manager 與代理程式間之通訊的相關資訊。 /var/log/sdcssl-caflog/cve.log
將日誌收集到一個 ZIP 檔案。	您可以使用 GetAgentInfo 程序檔將所有日誌檔都收集到一個 ZIP 檔案，而您可以將該檔傳送給客戶支援。 - 登入 Symantec Linux Agent 系統。 - 導覽至 /opt/Symantec/sdcsslagent/IPS/tools/。 - 以 root 身分執行 ./getagentinfo.sh。 - 將會在 /tmp/ 目錄中建立 ZIP 檔案。 檔案名稱將會類似 20201208_184935_0001_CU_mihsan-rhel8.zip -out <##> 可讓您變更所產生 ZIP 檔案的位置和名稱。

疑難排解 Symantec Endpoint Protection Manager 與主控台或預設資料庫之間的通訊問題

如果 Symantec Endpoint Protection Manager 主控台或預設資料庫發生連線問題，您可能會看到下列其中一種症狀：

- 管理伺服器服務 (semsrv) 停止。
- 管理伺服器服務未處於啟動狀態。
- 「首頁」、「監視器」和「報告」頁面顯示 HTTP 錯誤。
- 「首頁」、「監視器」和「報告」頁面空白。
- 「首頁」、「監視器」和「報告」頁面顯示持續載入中的進度列，而未顯示任何內容。

上述所有問題在 Windows 事件日誌中均會顯示 Java -1 錯誤。若要找出 Java -1 錯誤的確切原因，請查看 scm-server 日誌。scm-server 日誌預設位於下列位置：

SEPM_Install\tomcat\logs\scm-server-0.log

SEPM_Install 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager#

Table 193: 檢查與主控台或資料庫的連線

檢查的項目	說明
測試資料庫與管理伺服器之間的連線。	您可以檢查管理伺服器與資料庫之間的通訊是否正常。請參閱： 驗證與資料庫的連線
檢查管理伺服器的堆疊大小是否正確。	如果您無法登入管理伺服器的遠端主控台，則可能需要增加 Java 堆疊大小。您也可能會在 scm-server 日誌中看到記憶體不足的訊息。 如需預設堆疊大小的詳細資訊，請參閱： 決定安裝 Symantec Endpoint Protection Manager 期間所選取網路大小的預設設定
檢查管理伺服器是否未執行多個版本的 PHP。	您可以檢查管理伺服器是否執行多個使用不同版本 PHP 的軟體套件。PHP 會檢查全域架構檔 (php.ini)。如果有多個架構檔，您必須強制每個產品使用其本身的解譯器。當每個產品使用其正確版本的 PHP 時，管理伺服器就能恢復正常運作。
檢視系統需求。	您可以檢查用戶端和管理伺服器是否在符合最低或建議系統需求的情況下執行。 如需最新系統需求，請參閱： 所有 Endpoint Protection 版本的版本說明、新修正和系統需求

驗證管理伺服器與資料庫的連線

管理伺服器和資料庫可能無法正常進行通訊。請先檢查資料庫是否執行，然後測試伺服器與資料庫之間的連線。

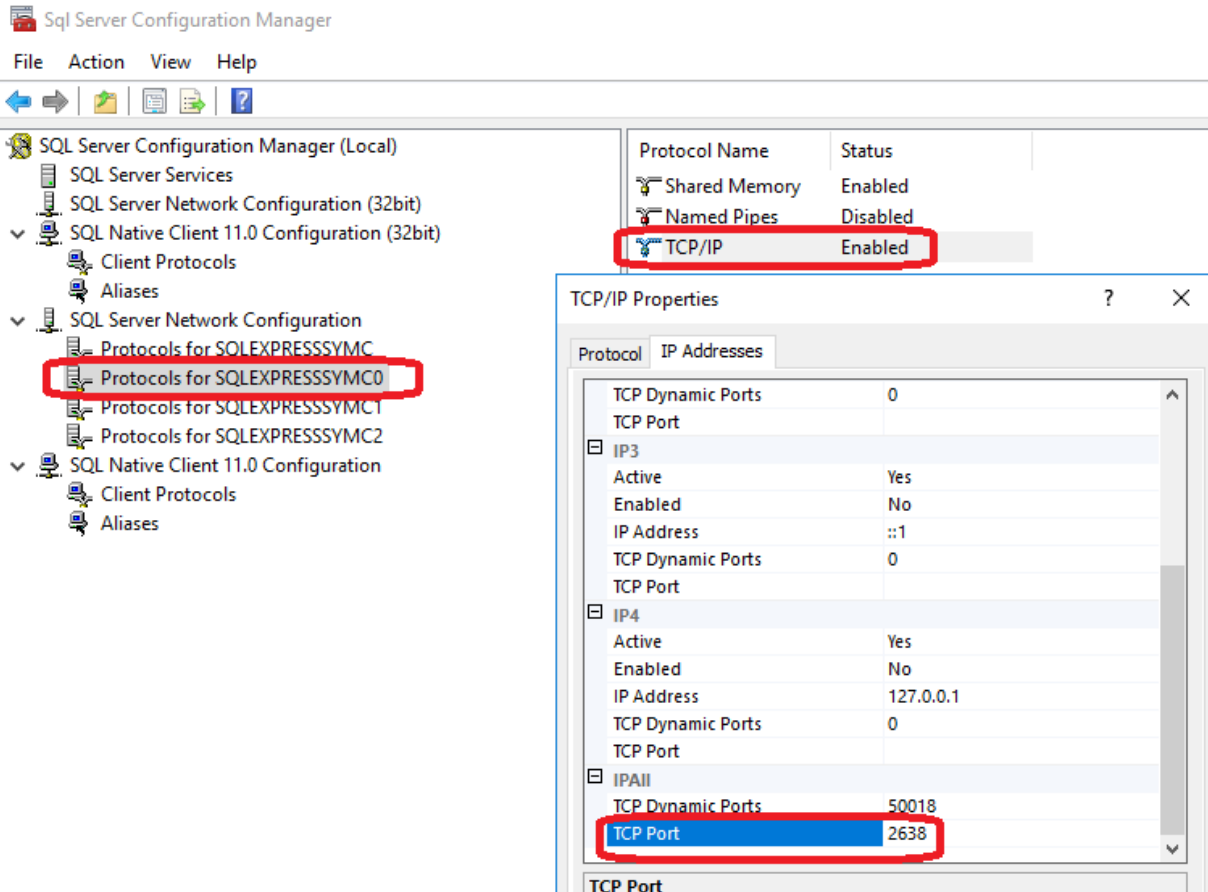
Table 194: 驗證資料庫連線

資料庫類型	執行這些步驟
Microsoft SQL Server Express 資料庫 (自 14.3 RU1 起)	• 驗證 SQL Server Express 服務是否執行，以及 sqlserver.exe 程序是否接聽 TCP 通訊埠 2638。 • 測試 ODBC 連線。
內嵌 Sybase 資料庫 (14.3 MP1 及更舊版本)	• 檢查 Symantec 內嵌資料庫服務是否執行，而且 dbsrv9.exe 程序是否接聽 TCP 通訊埠 2638。 • 測試 ODBC 連線。
遠端 Microsoft SQL Server 資料庫	• 檢查您在安裝和架構 Symantec Endpoint Protection Manager 時是否指定了具名實例。 • 檢查 SQL Server 是否執行而且正確架構。 • 檢查管理伺服器與 SQL 資料庫之間的網路連線是否正確。 • 測試 ODBC 連線。

驗證與 Microsoft SQL Server Express 資料庫的通訊

1. 在「開始」功能表上，展開 **Microsoft SQL Server 2017**，然後按下「**SQL Server 2017 組態管理員**」。

2. 在「**SQL Server 組態管理員**」對話方塊中，展開「**SQL Server 網路組態**」，然後選取「**SQLExpress 實例的通訊協定**」。
TCP/IP 欄位應設定為「已啟用」。
3. 在 TCP/IP 上按下滑鼠右鍵，再按下「內容」。
4. 在「IP 位址」標籤上，向下捲動到 IPAll 類別；「TCP 通訊埠」欄位預設會顯示通訊埠編號 2638。



檢查與內嵌資料庫的通訊

1. 在管理伺服器電腦上，按下「開始」>「控制台」>「系統管理工具」。
2. 在「系統管理工具」對話方塊中，連按兩下「資料來源 (ODBC)」。
3. 在「ODBC 資料來源管理員」對話方塊中，按下「系統 DSN」。
4. 在「系統 DSN」標籤上，連按兩下 **SymantecEndpointSecurityDSN**。
5. 在 ODBC 標籤上，確定「資料來源名稱」下拉式清單是 SymantecEndpointSecurityDSN，然後輸入選擇性說明。
6. 按下「登入」。
7. 在「登入」標籤的「使用者 ID」文字方塊中，輸入 dba。
8. 在「密碼」文字方塊中，輸入資料庫的密碼。
密碼是您在安裝管理伺服器時，為資料庫輸入的密碼。
9. 按下「資料庫」。
10. 在「資料庫」標籤的「伺服器名稱」文字方塊中，輸入：
\\servername\instancename
如果使用的是 Symantec Endpoint Protection Manager 英文版，請輸入預設值 sem5。否則，請將「伺服器名稱」文字方塊保留空白。
11. 在 ODBC 標籤上，按下「測試連線」並確認是否成功。

12. 按下「確定」。

13. 按下「確定」。

若要驗證與 **Microsoft SQL Server** 資料庫的通訊，請執行下列動作：

1. 在管理伺服器電腦上，按下「開始」>「控制台」>「系統管理工具」。
2. 在「系統管理工具」對話方塊中，連按兩下「資料來源 (ODBC)」。
3. 在「**ODBC 資料來源管理員**」對話方塊中，按下「系統 DSN」。
4. 在「系統 DSN」標籤上，連按兩下 **SymantecEndpointSecurityDSN**。
5. 在「伺服器」下拉式清單中，檢查是否已選取正確的伺服器和實例。
6. 按「下一步」。
7. 在「登入 ID」中，輸入 sa。
8. 在「密碼」文字方塊中，輸入資料庫的密碼。
密碼是您在安裝管理伺服器時，為資料庫輸入的密碼。
9. 按「下一步」，確定為預設資料庫選取 sem5。
10. 按「下一步」。
11. 按下「完成」。
12. 按下「測試資料來源」，然後查看結果是否如下：

#####!

用戶端與伺服器通訊檔案

用戶端與伺服器之間的通訊設定，以及其他用戶端設定，是儲存在用戶端電腦的檔案中。

Table 195: 用戶端檔案

檔案名稱	說明
SerDef.dat	依照位置儲存通訊設定的加密檔案。每當使用者變更位置時，用戶端就會讀取 SerDef.dat 檔案並套用新位置所對應之適當的通訊設定。
sylink.xml	儲存全域通訊設定。此檔案僅供內部使用，且不應加以編輯，其包含 Symantec Endpoint Protection Manager 的設定。如果您編輯此檔案，大部分設定會在下一次用戶端連線到管理伺服器時，遭到管理伺服器的設定所覆寫。
SerState.dat	儲存使用者介面相關資訊的加密檔案，這些資訊包括用戶端畫面大小、是否顯示防網路和主機侵入的用戶端主控台，以及是否顯示 Windows 服務等。用戶端啟動時，會讀取此檔案並傳回與其停止前相同的使用者介面狀態。

報告問題疑難排解

使用報告時，請務必注意下列資訊：

- 報告與日誌的時間戳記 (含用戶端掃描時間) 會以使用者的本地時間為準。報告資料庫所包含的事件則是以格林威治標準時間 (GMT) 為準。當您建立報告時，GMT 值會轉換成您檢視報告所在電腦的當地時間。
- 若受管型用戶端與管理伺服器的時區不同，而且您使用「設定特定日期」過濾選項，則可能會發生無法預期的結果，而且可能影響用戶端與管理伺服器的資料與時間準確性。
- 如果您在伺服器上變更時區，請登出主控台後重新登入，以便在日誌和報告中看到正確的時間。
- 在某些情況下，報告資料不會與安全產品中所出現的事件一一對應。發生不對應的情況是因為報告軟體會彙總安全性事件。
- 您可以將 SSL 與報告功能搭配使用，以增加安全性。SSL 可確保用戶端和伺服器之間的機密性和資料的完整性，並可在兩者之間進行驗證。請參閱文章：

在 Symantec Endpoint Protection Manager 與其用戶端之間啟用 SSL 通訊

- 報告中的風險類別資訊是從「賽門鐵克安全機制應變中心」網站取得的。在 Symantec Endpoint Protection Manager 主控台能擷取此項資訊之前，您產生的任何報告在風險類別欄位中都會顯示為「不明」。
- 您產生的報告可提供網路中受威脅電腦的精準狀況。這些報告基於日誌資料，而非 Windows 登錄資料。
- 如果在執行含大量資料的報告時，出現資料庫錯誤，您可能要變更資料庫逾時參數。請參閱：
[變更檢視報告和日誌的逾時參數](#)
- 如果收到 CGI 或終止程序錯誤，您可能要變更其他逾時參數。如需詳細資訊，請參閱下列文章：
[查詢大量資料時，SEPM Reporting 不回應或顯示逾時錯誤訊息。](#)
- 如果您在電腦上停用回送位址，則報告頁面不會顯示。請參閱：
[在停用回送位址時存取報告頁面](#)

變更檢視報告和日誌的逾時參數

如果檢視含有大量資料的報告或日誌時資料庫發生錯誤，您可以進行下列變更：

- 變更資料庫連線逾時時間
- 變更資料庫指令逾時時間

這些報告預設值如下：

- 連線逾時時間為 300 秒 (5 分鐘)
- 指令逾時時間為 300 秒 (5 分鐘)

若要變更 **Reporter.php** 和 **Reporter2.php** 中的資料庫逾時值

1. 瀏覽至 Symantec Endpoint Protection Manager 伺服器的下列預設資料夾：
`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php\Include\Resources`
2. 使用純文字編輯器 (例如「記事本」) 開啟 Reporter.php 和 Reporter2.php 檔案。
3. 找到 **\$CommandTimeout** 和 **\$ConnectionTimeout** 行，並增加值 (以秒為單位)。如果其中一行不存在，請建立它。例如，若要將逾時期間增加到 10 分鐘，請將此行變更為以下值：
`$CommandTimeout = 600;`
`$ConnectionTimeout = 600;`
在下列字元之前新增這些新行：?>
4. 儲存並關閉 Reporter.php 和 Reporter2.php 檔案。

NOTE

如果您指定零值，或使欄位留白，則會使用預設設定。

如果收到 CGI 或終止程序錯誤，您可能要變更下列參數：

- Php.ini 檔案中的 max_execution_time 參數
- httpd.conf 檔案中的 Apache 逾時參數 FcgidIOTimeout、FcgidBusyTimeout 和 FcgidIdleTimeout

變更 **Php.ini** 中的 **max_execution_time** 參數

1. 瀏覽至 Symantec Endpoint Protection Manager 伺服器的下列預設資料夾：
`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php`
2. 在 Php.ini 檔案按下滑鼠右鍵，再按下「屬性」。
3. 在「一般」標籤上，取消勾選「唯讀」。
4. 按下「確定」。
5. 以諸如「記事本」的純文字編輯器來開啟 Php.ini 檔案。

-
6. 找到 **max_execution_time** 項目並增加值 (以秒為單位)。例如，若要將逾時時間增加到 10 分鐘，請將此行變更為以下值：
`max_execution_time=600`
 7. 儲存並關閉 `Php.ini` 檔案。
 8. 在 `Php.ini` 檔案上按下滑鼠右鍵，再按下「內容」。
 9. 在「一般」標籤上，勾選「唯讀」。
 10. 按下「確定」。

變更 `httpd.conf` 中的 **Apache** 逾時參數

1. 瀏覽至 Symantec Endpoint Protection Manager 伺服器的下列預設資料夾：
`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf`
2. 以諸如「記事本」的純文字編輯器來開啟 `httpd.conf` 檔案。
3. 找到下面這幾行並增加值 (以秒為單位)：
 - `FcgidIOTimeout 1800`
 - `FcgidBusyTimeout 1800`
 - `FcgidIdleTimeout 1800`
4. 儲存並關閉 `httpd.conf` 檔案。

在停用回送位址時存取報告頁面

如果您在電腦上停用回送位址，則報告頁面不會顯示。如果您嘗試登入 Symantec Endpoint Protection Manager 主控台，或嘗試存取報告功能，您會看見下列錯誤訊息：

無法與報告元件進行通訊

「首頁」、「監視器」以及「報告」頁面空白；「政策」、「用戶端」以及「管理員」頁面的外觀和功能正常。

若要使「報告」元件在已停用回送位址時顯示，必須將文字 `localhost` 與電腦的 IP 位址相關聯。您可以編輯 Windows 主機檔案，使本機主機與 IP 位址相關聯。請參閱：

從獨立式網頁瀏覽器登入報告

在執行 **Windows** 的電腦上使本機主機與 **IP** 位址相關聯

1. 將目錄變更至主機檔案的位置。

主機檔案預設位於 `%SystemRoot%\system32\drivers\etc`

2. 使用編輯器開啟 `hosts` 檔案。

3. 將下列一行新增至主機檔案：

`IPAddress localhost #以登入報告功能`

在這裡將 `IPAddress` 取代為電腦的 IP 位址。您可以在井字符號 (#) 後加上任何需要的註解。例如，您可以鍵入下列一行：

`192.168.1.100 localhost # 此項目是我的主控台電腦的 IPv4 位址`

`2001:db8:85a3::8a2e:370:7334 localhost # 此項目是我的主控台電腦的 IPv6 位址`

自 14.2 版起支援 IPv6。

4. 儲存並關閉檔案。

從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前應了解的事項

Symantec Power Eraser 是免費的病毒移除工具，可從電腦中移除惡意軟體和威脅。Power Eraser 隨附於產品，無需安裝。

通常，當「風險」日誌顯示修復失敗且建議執行 Power Eraser 時，應執行 Power Eraser 分析。當電腦變得不穩定且似乎有無法移除的惡意軟體或病毒時，您可能也需要執行 Power Eraser。

Symantec Power Eraser 提供主動掃描和分析，以協助解決嚴重感染的 Windows 電腦的問題。由於 Power Eraser 分析是主動的，因此它有時會標記您可能需要的關鍵檔案。Power Eraser 產生的誤報數可能超過病毒和間諜軟體所掃描到的誤報數。

WARNING

您應只在緊急的狀況下才執行 Power Eraser，例如當電腦出現不穩定或存在持續性問題時。通常情況下，在單一電腦或一小組電腦上執行 Power Eraser。您不應同時執行其他應用程式。在某些情況下，定期掃描事件會警示您執行 Power Eraser 分析。

對於 Norton Power Eraser，請參閱：[下載並執行適用於 Windows 的 Norton Power Eraser 免費病毒和惡意軟體移除工具](#)

從 Symantec Endpoint Protection Manager 使用強力清除器與在本機使用 SymDiag 工具執行強力清除器的差異

您可以從 Windows 用戶端上的管理主控台遠端執行 Power Eraser。Symantec Endpoint Protection 不包括直接從用戶端啟動 Power Eraser 的選項。但是，用戶端電腦上的使用者可以下載 SymDiag 工具並從該工具執行強力清除器。

- 如果使用 SymDiag 工具，則強力清除器偵測到的項目不會出現在 Symantec Endpoint Protection Manager 日誌中。
- 當您從主控台執行強力清除器時，強力清除器不會檢查使用者特定載入點、註冊和資料夾，但是 SymDiag 工具卻會。

NOTE

請確保您不會同時從主控台執行強力清除器，又在本機使用 SymDiag 工具執行強力清除器。否則，可能會對電腦效能產生負面的影響。

Power Eraser 耗用大量的電腦資源。如果您在某台電腦上多次執行 Power Eraser，則 Power Eraser 檔案也會耗用該電腦上的大量空間。在每次分析期間，Power Eraser 都會將偵測資訊儲存在存放於 Symantec Endpoint Protection 應用程式資料夾中的檔案。用戶端清除日誌時會清除這些檔案。

Power Eraser 掃描和病毒及間諜軟體掃描之間的差異

Power Eraser 與定期掃描的差異體現在以下方面：

14.3 RU5 和更新版本	14.3 RU4 和更早版本
Power Eraser 掃描、病毒和間諜軟體掃描均執行作用中的掃描和完整掃描。 然而，Power Eraser 會使用更主動的「高密度偵測 (HID)」掃描，其採用進階機器學習 (AML) 技術。AML 引擎會透過學習程序判斷檔案是良好還是無效檔案。 AML 引擎可辨識惡意屬性，並定義 AML 引擎用來進行偵測的規則。	與完整病毒和間諜軟體掃描不同的是，Power Eraser 不會掃描電腦上的每個檔案。Power Eraser 會檢查載入點和載入點磁碟位置，以及執行中的程序和已安裝的服務。
Power Eraser 依據掃描閾值層級自動矯正偵測。 HID 掃描會使用閾值層級 (從 1 到 5)，其會觸發偵測動作，攔截 (層級 1 和 2) 或記錄 (層級 3 和 4)。 - 遭攔截的偵測為首先清除之遭定罪的檔案，且若不成功，則進行隔離 (病毒) 或先進行隔離 (安全風險)。 - 記錄的偵測為傳送至「掃描」日誌或「風險」日誌的可疑檔案。您必須檢閱任一日誌中的偵測清單，並從該日誌選取一個動作。	Power Eraser 不會自動矯正偵測。 Power Eraser 偵測不會自動傳送至「隔離」。 您必須檢閱掃描日誌或風險日誌中的偵測清單，且必須從該日誌選取動作。您可以選擇移除偵測或將偵測標示為安全 (略過)。您也可以還原 (復原) 已移除的偵測。
Power Eraser 優先於病毒和間諜軟體掃描。當您執行 Power Eraser 時，Symantec Endpoint Protection 會取消進行中的所有病毒和間諜軟體掃描。 若您在混合模式下管理 Symantec Endpoint Protection，Power Eraser 會在層級 2 或「密集型防護」政策層級 (以較高值為準) 攔截偵測。例如，若雲端主控台「密集型防護」政策攔截層級設定為 3，則 Power Eraser 將在 3 處攔截。	Power Eraser 優先於病毒和間諜軟體掃描。當您執行 Power Eraser 時，Symantec Endpoint Protection 會取消進行中的所有病毒和間諜軟體掃描。
僅處於 rootkit 模式之 14.3 RU4 或更早版本的用戶端電腦會重新啟動。	Power Eraser 可以在正常模式或 Rootkit 模式下執行。Rootkit 模式需要在掃描啟動之前重新啟動。此外，如果您選擇移除任何 Power Eraser 偵測，則必須重新啟動電腦才能完成矯正。
Power Eraser 僅執行於 Windows 用戶端上，而病毒和間諜軟體掃描則執行於 Windows、Mac 和 Linux 用戶端上	與 14.3 RU5 及更新版本相同。

必須執行 Power Eraser 時所執行的高階步驟概觀

從主控台執行 Power Eraser 時，請執行兩個高階步驟：

- 在一台電腦或一小組電腦上啟動 Power Eraser 分析。Power Eraser 可能會也可能不會依據用戶端版本自動矯正偵測。
- 使用風險日誌或掃描日誌檢閱 Power Eraser 偵測，並手動要求 Power Eraser 移除任何您判斷為威脅的偵測。您也可以認可您要忽略的偵測並略過。

瞭解如何從主控台執行 Power Eraser，及如何確保您正確架構主控台設定。請參閱：

[需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作](#)

影響 Power Eraser 之 Symantec Endpoint Protection Manager 政策設定的概觀

下列政策設定會影響 Power Eraser：

- 使用者互動的掃描設定
當您讓使用者取消任何病毒和間諜軟體掃描時，也就是讓他們取消任何 Power Eraser 分析。但是，使用者無法暫停或延緩 Power Eraser。請參閱：
[允許使用者在 Windows 電腦上檢視掃描進度並與掃描互動](#)
- 例外政策

Power Eraser 遵守下列病毒和間諜軟體例外：檔案、資料夾、已知風險、應用程式和信任的 Web 網域。Power Eraser 不遵守副檔名例外。請參閱：

[建立病毒和間諜軟體掃描的例外](#)

- 日誌保留設定

只要日誌中出現偵測，便可以對 Power Eraser 偵測採取動作。經過病毒和間諜軟體防護政策中指定的時間之後，日誌將遭清除。根據預設，有 14 天的日誌事件可用。您可以修改日誌保留設定，也可以在事件到期之後，執行另一個掃描並重新填入日誌。請參閱：

[在 Windows 電腦上修改日誌處理及通知設定](#)

- 重新啟動選項 (14.3 RU4 或更早的電腦)

當您選擇在 Rootkit 偵測模式下執行 Power Eraser 時，可以專門針對 Rootkit 分析架構重新啟動設定。管理員必須具有重新啟動權限。在選擇移除 Power Eraser 偵測之後，電腦會使用群組重新啟動設定。Power Eraser 不會使用 Rootkit 重新啟動設定來重新啟動和完成矯正。請參閱：

[從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦](#)

- 信譽查詢

Power Eraser 在掃描檔案並做出有關檔案的決策時，會使用雲端中的 Symantec Insight 伺服器。如果停用信譽查詢，或用用戶端電腦無法連線至 Insight 伺服器，則 Power Eraser 無法使用 Symantec Insight。若沒有 Symantec Insight，Power Eraser 所進行的偵測會變少，同時它進行的偵測較可能是誤報。如果已啟用「允許進行智慧型掃描查詢以偵測威脅」選項，會啟用信譽查詢。此選項預設為啟用。請參閱：

[Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策](#)

- 遞送

Symantec Endpoint Protection 在啟用「將匿名資料傳送給 Symantec，以獲得增強的威脅防護情報」選項時，對 Symantec 傳送有關 Power Eraser 偵測的相關資訊。此選項預設為啟用。請參閱：

[瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性](#)

更多資訊

[使用 Symantec Diagnostic Tool \(SymDiag\) 對電腦問題進行疑難排解](#)

需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作

WARNING

請謹慎使用 Power Eraser。該分析是積極的，但容易誤報。

如需詳細資訊，請參閱：

[從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項](#)

您僅可在 Windows 用戶端電腦上從 Symantec Endpoint Protection Manager 執行 Power Eraser。

Table 196: 需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作

工作	說明
確保您的用戶端具有 Internet 連線	您的用戶端電腦需要 Internet 存取，以便 Power Eraser 可以使用 Symantec Insight 信譽資料來做出有關潛在威脅的決策。 間歇或不存在的 Internet 存取表示 Power Eraser 無法使用 Symantec Insight。如果不使用 Symantec Insight，Power Eraser 進行偵測的次數會變少，且產生的偵測更容易是誤報。
設定限制的管理員權限以執行 Power Eraser	若要在用戶端電腦上執行 Power Eraser，限制的管理員必須具有下列指令存取權限： • Power Eraser 分析 • 重新啟動用戶端電腦 (執行具 Rootkit 偵測之 Power Eraser 的 14.3 RU4 和較早版本用戶端) 如需詳細資訊，請參閱： 新增管理員帳戶和設定存取權限
設定日誌存留政策	日誌存留設定將影響事件供您執行 Power Eraser 矯正和還原動作所花費的時間。如果您需要更多時間考慮上述動作，您可以修改日誌存留設定。或者，您可以再次執行 Power Eraser 以重新填入日誌。 日誌存留設定屬於病毒和間諜軟體防護政策中的其他選項。請參閱： 在 Windows 電腦上修改日誌處理及通知設定
從 Symantec Endpoint Protection Manager 執行 Power Eraser 分析	您可以從 Symantec Endpoint Protection Manager 中的幾個地方發出 Power Eraser 指令： • 「用戶端」頁面 • 電腦狀態日誌 • 風險日誌 Note: 用戶端電腦上的使用者無法在用戶端使用者介面上直接執行 Power Eraser。強力清除器可做為 SymDiag 工具的一部分使用。不過，如果用戶端使用者執行該工具，所產生的包括 Power Eraser 偵測的日誌不會傳送至 Symantec Endpoint Protection Manager。 如需詳細資訊，請參閱： 從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析 您可以在電腦狀態日誌中檢視指令的狀態。您可以篩選該日誌，以僅顯示 Power Eraser 指令，從而便於檢視。
在用戶端電腦上取消 Power Eraser 指令或動作	若要取消 Power Eraser 指令，請使用電腦狀態日誌。 Note: 若重新啟動提示出現於用戶端電腦上，則您無法取消 Power Eraser。重新啟動後，如果病毒和間諜軟體防護政策讓使用者取消掃描，則僅電腦使用者可以取消 Power Eraser。 如果取消 Power Eraser 指令，您也可以取消與所有 Power Eraser 分析相關聯的任何擱置中的動作，包括所有矯正或復原動作。 如需詳細資訊，請參閱： 在用戶端電腦上從主控台執行指令

工作	說明
從日誌中檢視 Power Eraser 偵測	您可以從 Symantec Endpoint Protection Manager 的下列日誌中檢視 Power Eraser 偵測： 「掃描」日誌 掃描日誌有一個可僅顯示 Power Eraser 結果的「掃描類型」篩選器。該檢視也表示掃描結果是否處於擱置中。您可以在篩選檢視中選取「偵測」，以顯示「Power Eraser 偵測」檢視。 - 風險日誌 風險日誌針對 Power Eraser 偵測提供類似的過濾器。不過，風險日誌不會顯示掃描結果是否處於擱置中。 - 電腦狀態日誌 電腦狀態日誌可能在「受感染」欄中包含報告圖示。事件詳細資料圖示將連結到一個報告，該報告顯示目前無法矯正的所有威脅。該報告包含只記錄偵測和未解析的偵測。該報告可能建議在相同電腦上執行 Power Eraser。 Power Eraser 圖示將連結到一個報告，該報告顯示需要管理員動作的電腦上的所有 Power Eraser 偵測。 這些圖示也會出現在「用戶端」頁面的「運作狀態」欄中。 如需詳細資訊，請參閱： 檢視日誌
檢查建議您在用戶端電腦上執行 Power Eraser 的通知	根據預設，管理員會在定期掃描無法修復感染時收到一條通知：建議使用 Power Eraser。您可在「監視器 > 通知 > 通知條件」頁面上檢查「建議使用 Power Eraser」通知。請參閱： 檢視和認可通知
在「指令狀態」頁面上檢視 Power Eraser 偵測	可以在「指令狀態」頁面上存取有關 Power Eraser 偵測的報告。 事件詳細資料圖示將出現在「完成狀態」欄中。該圖示將連結到一個報告，該報告顯示「啟動 Power Eraser 分析」指令和任何其他掃描指令所執行的偵測的相關資訊。 指令狀態詳細資料選項提供有關特定掃描的資訊。可按下事件詳細資料圖示，以取得有關特定用戶端電腦的資訊。請參閱： 在用戶端電腦上從主控台執行指令
從「用戶端」標籤中檢視 Power Eraser 偵測	您可以從「用戶端」頁面的「用戶端」標籤存取有關 Power Eraser 偵測的報告。 如果資訊可用，報告圖示將出現在「運作狀態」欄中。事件詳細資料圖示將連結到一個報告，該報告顯示目前無法矯正的所有威脅。該報告包含所有 Power Eraser 偵測。 Power Eraser 圖示將連結到一個報告，該報告顯示需要管理員動作的電腦上的所有 Power Eraser 偵測。 這些圖示也出現在電腦狀態日誌中。 如需詳細資訊，請參閱： 檢視用戶端電腦的防護狀態
從 Symantec Endpoint Protection Manager 中的掃描日誌或風險日誌矯正或還原 Power Eraser 偵測	在 14.3 RU5 和更新版本中，若威脅層級低於某一閾值，則 Power Eraser 會隔離偵測到的威脅。於下列狀況中，Power Eraser 不會自動矯正偵測。 - 若為 14.3 RU4 和較早版本的用戶端。 - 若為記錄為可疑且超出特定閾值的 14.3 RU5 偵測。 Power Eraser 分析是積極的，但可能會偵測到許多誤報。在您決定偵測是否需要矯正後，您必須手動啟動矯正。 也可以復原（還原）已隔離的 Power Eraser 偵測。 如需詳細資訊，請參閱： 回應 Power Eraser 偵測

從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析

您可以執行 Power Eraser 來分析和偵測單一電腦或一小組電腦上的持續性威脅。請參閱：

[從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項](#)

在 Power Eraser 偵測到潛在風險之後，您可以檢視風險並判斷哪些風險是威脅。在 14.3 RU4 和更早版本中，Power Eraser 不會自動矯正風險。您必須手動執行 Power Eraser 以矯正您判斷為威脅的風險。您也可以對特定威脅或其他防護功能偵測到的威脅執行 Power Eraser。Power Eraser 在與偵測關聯的電腦上執行。請參閱：

- 需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作
- 回應 Power Eraser 偵測

NOTE

執行 Power Eraser 且在 14.3 RU4 和更早版本的用戶端電腦上顯示重新啟動選項訊息時，管理員或使用者無法取消 Power Eraser。在重新啟動之後，如果病毒和間諜軟體防護政策讓使用者取消掃描，則使用者可以取消 Power Eraser。

如要從用戶端頁面啟動 **Power Eraser** 分析

1. 在「用戶端」頁面的「用戶端」標籤上，選取您要分析的電腦。
如果您選取多台電腦，可能會對網路的效能產生負面影響。
2. 在「工作」下方，按下「對電腦執行指令」，然後按下「啟動 **Power Eraser** 分析」。
3. 於「選擇 **Power Eraser** 類型」對話方塊中，選取要在其中執行掃描的模式。
 - 14.3 RU5 和更新版本：對於完整磁碟選項，您無需重新啟動電腦，除非 14.3 RU4 和較早版本的用戶端在該群組中。
 - 14.3 RU4 和更早版本：對於 rootkit 模式，您可設定重新啟動選項。您必須擁有管理員權限，才能設定重新啟動選項並執行 Rootkit 掃描。
4. 按下「確定」。
Power Eraser 即會在選取的電腦上執行。您可以在「監視器」頁面的「指令狀態」標籤上取消此指令。

如要從電腦狀態日誌啟動 **Power Eraser** 分析

1. 在主控台的側邊看板中，按下「監視器」，然後選取「日誌」標籤。
2. 在「日誌類型」清單方塊中，選取「電腦狀態」日誌，然後按下「檢視日誌」。
3. 選取要在其上執行 Power Eraser 的電腦，然後從「指令」下拉式方塊中選取「啟動 **Power Eraser** 分析」。
如果您選取多台電腦，可能會對網路的效能產生負面影響。
4. 按下「開始」。
5. 於「選擇 **Power Eraser** 類型」對話方塊中，選取掃描類型。
6. 按下「確定」。
Power Eraser 即會在選取的電腦上執行。您可以在「指令狀態」標籤上取消此指令。

如要從風險日誌啟動 **Power Eraser** 分析

1. 在主控台的側邊看板中，按下「監視器」，然後選取「日誌」標籤。
2. 在「日誌類型」清單方塊中，選取「風險」日誌，然後按一下「檢視日誌」。
3. 選取要對其執行 Power Eraser 的風險。在「事件動作」欄中，您可能會看到執行 Power Eraser 的警示。
您可以對日誌中的任何風險執行 Power Eraser。
4. 從「動作」下拉式清單或「動作」欄中，選取「啟動 **Power Eraser** 分析」。
5. 按下「開始」。
6. 於「選擇 **Power Eraser** 類型」對話方塊中，選取是否要 Power Eraser 執行下列其中一個選項：
 - 14.3 RU5 和更新版本：選取「常見感染位置」或「完整磁碟」。
 - 14.3 RU4 及更早版本：選取「無 rootkit 偵測」或「含 rootkit 偵測」。對於 rootkit 偵測，您可設定重新啟動選項。您必須擁有管理員權限，才能設定重新啟動選項並執行 Rootkit 掃描。
7. 按下「確定」。
Power Eraser 即會在受所選風險感染的電腦上執行。您可以在「指令狀態」標籤上取消此指令。

回應 **Power Eraser** 偵測

Power Eraser 以不同方式矯正偵測，視用戶端版本而定。

Table 197: Power Eraser 矯正

14.3 RU5 和更新版本	14.3 RU4 和更早版本
Power Eraser 會使用「高密度偵測」(HID) 掃描引擎，其會將威脅偵測為已確認的風險或確認的可疑風險。HID 掃描會立即處理這些風險。 - 病毒已清除，且若失敗，則會將其隔離。 - 安全風險已隔離，且若失敗，則會將其記錄為可疑檔案。 您可透過隔離可疑檔案以手工方式對其進行矯正。若您認為該檔案是誤報，則使用「忽略可疑檔案」動作建立例外。	Power Eraser 不會矯正任何偵測，以最小化誤報。相反的，在檢閱過偵測後，您必須針對日誌中偵測到的事件要求矯正，然後決定予以矯正還是忽略。如果您選擇矯正，Power Eraser 會移除與偵測關聯的檔案。但在日誌被清除之前，您可以還原已移除的檔案。

日誌保留政策決定 Power Eraser 事件的存留時間長度。依預設，事件會保留 14 天。

如需詳細資訊，請參閱：

- 需要從 [Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作](#)
- 從 [Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項](#)

回應 Power Eraser 偵測

- 確認 Power Eraser 分析已完成。
 - 電腦狀態日誌包含用於指示掃描已完成的圖示。
 - 掃描日誌會顯示 Power Eraser 是否已完成分析。
- 在風險日誌或「掃描日誌 > 檢視偵測」頁面中，選取要套用動作的一或多個偵測。
 - 在標示為「發現潛在風險 (擱置管理員動作)」的特定風險旁邊，按下「動作」欄中的加號圖示。
 - 選取標示為「發現潛在風險 (擱置管理員動作)」的多個風險，然後從「動作」下拉式功能表中選取動作。
- 選擇下列其中一個動作：

14.3 RU5 及更新版本：矯正可疑檔案 14.3 RU4 及更早版本：刪除 Power Eraser 偵測到的風險	將風險從電腦中移除以矯正該風險。Power Eraser 會儲存一份可供還原的安全備份檔案。
14.3 RU5 及更新版本：忽略可疑檔案 14.3 RU4 及更早版本：忽略 Power Eraser 偵測到的風險	確認您已檢閱偵測，但不想要矯正風險。 Note: 此動作只會在管理主控台日誌中將事件動作變更為「由管理員略過」。此認可不會更新用戶端上對應的事件動作。用戶端日誌檢視會繼續將事件動作顯示為「等待分析中」。

- 如果已從「動作」下拉式功能表中選取動作，請按下「套用」。

如果您選取了「忽略 **Power Eraser** 偵測到的風險」，偵測現在會顯示為「發現潛在風險 (略過)」。

您可選取下列動作之一，還原標示為「發現潛在風險 (已移除)」的已移除偵測：

- 14.3 RU5 及更新版本：從隔離還原
- 14.3 RU4 及更早版本：還原 **Power Eraser** 已刪除的風險

Table 198: Power Eraser 偵測狀態摘要

偵測狀態	說明
擱置管理員動作	Power Eraser 將風險偵測為潛在威脅。您應檢閱風險並決定 Power Eraser 是否應矯正風險，或認可該風險並予以忽略。
已還原	管理員已還原管理員要求 Power Eraser 矯正風險時所移動的所有檔案。
已隔離 (14.3 RU5)	Power Eraser 或管理員隔離了已確認的風險或已確認的可疑風險。
已刪除 (14.3 RU4 和更早版本)	管理員要求 Power Eraser 矯正並刪除風險。當 Power Eraser 刪除風險時，它會刪除與風險關聯的檔案，同時建立可供還原的安全備份複本。當日後判斷並非風險時，您可能會想要將已刪除的風險還原。在日誌事件被清除之前，您可以還原檔案。
由管理員略過	管理員要求 Power Eraser 略過風險。

附錄

取得用戶端功能比較、工具、指令行選項、第三方安裝工具的參考資訊。

本節包括用戶端功能比較、Symantec Endpoint Protection 中包含的工具、用戶端命令列選項、使用第三方工具的 Windows 安裝等。

Symantec Endpoint Protection 功能 (依平台分類)

如需詳細資訊，請參考下列各主題：

- [用戶端防護功能](#)
- [管理功能](#)
- [自動升級](#)
- [自適應防護政策](#)
- [病毒和間諜軟體防護政策](#)
- [入侵預防和記憶體攻擊緩和政策](#)
- [LiveUpdate 政策](#)
- [Web 和雲端存取防護 政策](#)
- [例外政策](#)
- [應用程式與裝置控制政策](#)

另請參閱：

- [如何選擇用戶端安裝類型](#)
- [Windows 用戶端的 Symantec Endpoint Protection 功能相依性](#)

用戶端防護功能

Table 199: 用戶端防護功能

用戶端功能	Windows	Mac	Linux
病毒和間諜軟體防護	是	是	是
防網路和主機侵入 • 網路威脅防護 (入侵預防和防火牆) • 記憶體攻擊緩和	是	• 防火牆 (自 14.2 起) • 入侵預防 適用於 Mac 的入侵預防不支援自訂特徵。	否
主動型威脅防護 • 應用程式與裝置控制 • 行為分析 (SONAR)	是	僅「裝置控制」	否
主機完整性	是	否	否
其他防護 • 系統鎖定 • 竄改防護	是	否	否

如需詳細資訊，請參閱：

- [關於應用程式控制、系統鎖定和裝置控制](#)
- [主機完整性的運作方式](#)

管理功能

Table 200: 管理功能

管理功能	Windows	Mac	Linux
從 Symantec Endpoint Protection Manager 遠端部署用戶端 - 網路連結與電子郵件 - 遠端推送 - 儲存套件	是	是	是 (僅限「網路連結與電子郵件」、「儲存套件」)
從管理伺服器在用戶端上執行指令	- 掃描 - 更新內容 - 更新內容和掃描 - 啟動 Power Eraser 分析 - 重新啟動用戶端電腦 - 啟用自動防護 - 啟用網路威脅防護 - 停用網路威脅防護 - 啟用下載鑑識 - 停用下載鑑識 - 收集檔案指紋清單 - 從隔離所刪除** - 取消全部掃描**	- 掃描 - 更新內容 - 更新內容和掃描 - 重新啟動用戶端電腦 (僅限硬式重新啟動) - 啟用自動防護 - 啟用/停用網路威脅防護	- 掃描 - 更新內容 - 更新內容和掃描 - 啟用自動防護
啟用探索到的應用程式和網路應用程式監控	是	否	否
建立位置和設定安全政策 (依位置套用)	是	是	否 您可以透過指令行來檢視用戶端的位置，但是用戶端不會根據特定的準則自動切換位置。
設定用戶端的重新啟動選項	是	否	否
快速報告和排程報告	- 稽核 - 應用程式與裝置控制 - 合規性 - 電腦狀態 - 欺詐 - 防網路和主機侵入 - 風險 - 掃描 - 系統	- 電腦狀態 - 防網路和主機侵入 - 風險 - 掃描	- 稽核 - 電腦狀態 - 風險 - 掃描 - 系統
針對用戶端電腦上維護的日誌設定大小和保留選項	- 系統 - 安全性和風險 - 安全性 - 流量 - 封包 - 控制	- 系統 - 安全性和風險 - 安全性	- 系統 - 安全性和風險
使用密碼保護用戶端	是	僅解除安裝用戶端	否
執行 SylinkDrop 工具以將用戶端移至其他管理伺服器	是	是	否

管理功能	Windows	Mac	Linux
使用「通訊更新套件部署」選項重新部署用戶端套件，以將用戶端移至其他管理伺服器	是	是	否
架構用戶端向賽門鐵克提交匿名安全資訊	是	是 傳送設定僅控制防毒偵測資訊。 您可以在用戶端上手動停用或啟用入侵預防傳送。請參閱： 如何在 Symantec Endpoint Protection for Mac 用戶端上停用 IPS 資料傳送	否
架構用戶端以安全提交匿名系統和使用資訊	是	否	否
管理管理伺服器與用戶端之間的外部通訊	是	僅限 LiveUpdate	否
管理用戶端通訊設定	- 管理伺服器清單 - 通訊模式 (推送或提取) - 設定活動訊號間隔時間 - 上傳探索到的應用程式 - 立即上傳重大事件 - 設定下載隨機化 - 設定重新連線喜好設定	- 管理伺服器清單 - 通訊模式 (推送或提取) - 設定活動訊號間隔時間 - 設定下載隨機化 - 設定重新連線喜好設定	- 管理伺服器清單 - 通訊模式 (推送或提取) - 設定活動訊號間隔時間
架構用戶端以使用私用伺服器 - 用於智慧型掃描查詢和提交的 Endpoint Detection and Response 伺服器 - 用於智慧型掃描查詢的私用 Insight 伺服器	是	否	否
使用「自動升級」來自動升級 Symantec Endpoint Protection 用戶端	是	是	否
自動移除現有的協力廠商安全軟體	是	否	否
自動移除有問題的 Symantec Endpoint Protection 用戶端	是	否	否
Symantec Endpoint Protection Manager 登入的驗證	- Symantec Endpoint Protection Manager 驗證 - 雙因素驗證 (14.2) - RSA SecurID 驗證 - 目錄驗證 - 智慧卡 (PIV/CAC) 驗證 (14.2)	不適用	不適用

**您只能在 Symantec Endpoint Protection Manager 中檢視日誌時執行這些指令。

如需詳細資訊，請參閱：

- [什麼是可对用戶端電腦執行的指令？](#)
- [需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作](#)
- [管理用戶端伺服器連線](#)
- [使用「通訊更新套件部署」還原用戶端伺服器通訊](#)

自動升級功能

Table 201: 自動升級功能

功能	Windows	Mac
增量套件	標準用戶端和暗網用戶端會接收 Symantec Endpoint Protection Manager 產生的增量升級套件。內嵌式用戶端則接收完整安裝套件來進行升級。	Mac 用戶端一律接收完整安裝套件，以進行升級。
組態選項	包括自訂安裝資料夾，以及解除安裝現有安全軟體的選項。	僅適用於重新啟動和升級。您無法自訂安裝資料夾。安裝記錄一律寫入 /tmp/sepinstall.log。
「用戶端安裝設定」中升級完成之後的重新啟動選項	包括不要重新啟動 Windows 用戶端電腦的選項。	請勿包括不要重新啟動的選項。升級完成後，Mac 用戶端電腦一律重新啟動。
「使用套件升級用戶端」精靈	您可以修改 Windows 用戶端上的功能集。	您無法修改 Mac 用戶端上的功能集。
從舊版升級	您可依據支援的升級路徑，從任何更早版本升級至 Symantec Endpoint Protection 的最新版本。	是，對於 14.x 和最新版本。

如需詳細資訊，請參閱：

- [使用自動升級來升級用戶端軟體](#)
- [支援升級到最新版本的 Symantec Endpoint Protection 14.x 的路徑](#)
- [如何選擇用戶端安裝類型](#)

自適應防護政策

調適型防護只會從 Windows 用戶端收集資料。

如需詳細資訊，請參閱：[透過自適應防護攔截 Living Off the Land \(LOTL\) 攻擊。](#)

病毒和間諜軟體防護政策

Table 202: 病毒和間諜軟體防護政策

政策設定	Windows	Mac	Linux
管理員定義掃描	- 排程掃描 (作用中、完整、自訂) - 隨選掃描 - 觸發掃描 - 開機掃描 - 重試錯過的排程掃描 - 隨機設定排程掃描	- 排程掃描 (自訂) - 隨選掃描 - 重試錯過的排程掃描	- 排程掃描 (自訂) - 隨選掃描 - 重試錯過的排程掃描 (14.3 RU1)
自動防護	- 啟用自動防護 - 掃描所有檔案 - 只掃描選取的副檔名 - 檢查檔案內容來判斷檔案類型 - 掃描安全風險 - 掃描遠端電腦上的檔案 - 存取、修改或備份檔案時掃描 - 掃描磁片是否存在開機病毒，含有選項可刪除開機病毒或僅記錄它 - 一律刪除新建立的受感染檔案或安全風險 - 保留檔案時間 - 針對掃描速度或應用程式速度調整掃描效能 - 包裝的惡意軟體的模擬器	- 啟用自動防護 - 自動修復受感染的檔案 - 無法修復的隔離所檔案 - 掃描壓縮檔 - 掃描所有檔案 - 僅掃描選取的資料夾 - 掃描除所選資料夾外的所有位置 - 掃描安全風險 在掛載的目前用戶端上掃描： - 資料磁碟 - 所有其他磁碟和裝置	- 啟用自動防護 - 掃描所有檔案 - 只掃描選取的副檔名 (已在 14.3 RU1 中移除) - 掃描抽取式媒體 - 掃描安全風險 - 掃描遠端電腦上的檔案 - 在存取或修改檔案時進行掃描 - 在壓縮檔內掃描
電子郵件掃描	- Microsoft Outlook 自動防護 - Internet 電子郵件自動防護 (14.2 RU1 中已移除) - Lotus Notes 自動防護 (14.2 RU1 中已移除)	否	否
要掃描的內容	- 其他位置 - 記憶體 - 選取的資料夾 - 選取的副檔名 - 儲存體移轉位置 - 壓縮檔內的檔案 - 安全風險	- 全部或選取的資料夾 - 硬碟和抽取式磁碟機 - 壓縮檔內的檔案	- 所有檔案 - 全部或選取的資料夾 - 選取的副檔名 - 壓縮檔內的檔案 - 安全風險
使用者定義的掃描 (用戶端)	- 作用中掃描 - 完整掃描 - 自訂掃描個別資料夾、檔案和副檔名	- 完整掃描 - 自訂掃描個別資料夾和檔案	- 完整掃描 - 自訂掃描個別資料夾和檔案
定義偵測的矯正動作	- 清除 (僅適用於惡意軟體) - 隔離 - 刪除 - 略過 (只記錄) 這些動作適用於賽門鐵克定期更新的惡意軟體和安全風險類別。	- 修復受感染的檔案 - 無法修復的隔離所檔案	(14.3 MP1 和更早版本) - 清除 (僅適用於惡意軟體) - 隔離 - 刪除 - 略過 (只記錄)

政策設定	Windows	Mac	Linux
設定掃描執行時要採取的動作	- 停止掃描 - 暫停掃描 - 延緩掃描 - 僅在電腦閒置時掃描	是 - 停止掃描 - 暫停掃描 - 開始前延緩掃描 - 僅在電腦閒置時掃描	否
下載鑑識	是	否	否
智慧型掃描查詢用於偵測威脅	是	否	否
Bloodhound	是	否	是
行為分析 (SONAR)	是	否 是	否
提早啟動防惡意軟體驅動程式	Windows 8 及更新版本，以及 Windows Server 2012 及更新版本	否	否
Power Eraser	是	否	否
Endpoint Detection and Response 啟用	是	否	否
共用智慧型掃描快取	是	否	否
虛擬影像例外	是	否	否

如需詳細資訊，請參閱：

- [阻止和處理病毒和間諜軟體對用戶端電腦的攻擊](#)
- [在虛擬基礎架構中使用 Symantec Endpoint Protection](#)

入侵預防和記憶體攻擊緩和政策

Table 203: 入侵預防政策

政策設定	Windows	Mac
入侵預防特徵的例外	是 Note: 「瀏覽器防護」特徵不支援自訂例外。	是
顯示或隱藏使用者通知	是	是
啟用或停用排除的主機	是	是
自訂 IPS 特徵	是	否
啟用或停用網路入侵預防	是	是
LiveUpdate 更新 IPS 內容	是	是
管理伺服器更新 IPS 內容	是	否 **
用戶端套件包含 IPS	是	是
網路入侵預防	是	是
瀏覽器入侵預防	是 只記錄模式	否
排除的主機 (網路入侵預防)	是	是

**您可以將隨 Symantec Endpoint Protection Manager 安裝的 Apache Web 伺服器設定為 LiveUpdate 內容的反向代理。

如需詳細資訊，請參閱：

- [使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容](#)
- [管理入侵預防](#)

Table 204: 記憶體攻擊緩和和政策

政策設定	Windows	Mac
記憶體攻擊緩和	是 • 微調誤報 • 自訂應用程式 (僅限雲端)	否

如需詳細資訊，請參閱：

[使用記憶體攻擊緩和和政策強化 Windows 用戶端防範記憶體竄改攻擊](#)

LiveUpdate 政策

Table 205: LiveUpdate 政策

政策設定	Windows	Mac	Linux
使用預設管理伺服器	是	否 **	否 **
使用 LiveUpdate 伺服器 (內部或外部)	是	是	是
使用群組更新提供者	是	否	否
啟用第三方內容管理	是	否	否
啟用/停用定義	是	是	否
減少大小定義	是	否	否
執行智慧型更新程式以更新內容	• 病毒和間諜軟體定義檔 • 行為分析 (SONAR) • IPS 定義	病毒和間諜軟體定義檔	病毒和間諜軟體定義檔
LiveUpdate 代理架構	是	是，但它不在 LiveUpdate 政策中架構。若要架構此設定，請按下「用戶端」>「政策」，然後按下「外部通訊設定」。	是
LiveUpdate 排程設定	• 頻率 • 重試時段 • 下載隨機化 • 電腦閒置時執行 • 用於略過 LiveUpdate 的選項	• 頻率 • 下載隨機化	• 頻率 • 重試時段 • 下載隨機化
用戶端安全修補程式	是	否	否
應用程式控制內容	是 (14.2)	否	否

** 您可以將隨 Symantec Endpoint Protection Manager 安裝的 Apache Web 伺服器設定為 LiveUpdate 內容的反向代理。

如需詳細資訊，請參閱：

- [使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容](#)
- [如何選擇用戶端安裝類型](#)
- [如何更新用戶端上的內容和定義檔](#)
- [使用智慧型更新小幫手 \(Intelligent Updater\) 檔案更新 Symantec Endpoint Protection 用戶端上的內容](#)

Web 和雲端存取防護 政策

政策設定	Windows	Mac	Linux
PAC 檔案方法 • 本機代理服務	是	是 (14.2 RU2 和更新版本)	否
通道方法 (14.3 RU1)	是，僅 Windows 10 64 位元和更高版本	否	否

如需詳細資訊，請參閱：

[使用 Web 和雲端存取防護控制網路存取](#)

例外政策

Table 206: 例外政策

政策設定	Windows	Mac	Linux
伺服器型例外	• 應用程式 • 要監控的應用程式 • 副檔名 • 檔案 • 資料夾 • 已知風險 • 信任的 Web 網域 • 竊改防護例外 • DNS 或主機檔案變更例外 • 憑證	• 檔案或資料夾的安全風險例外	• 資料夾 • 副檔名
用戶端限制 (控制一般使用者可以在用戶端電腦上新增哪些限制)	是	否	否

如需詳細資訊，請參閱：

[管理 Symantec Endpoint Protection 中的例外](#)

應用程式與裝置控制政策

應用程式控制僅會在 Windows 電腦上執行。

Table 207: 裝置控制政策

Windows	Mac
裝置控制僅依據類別 ID (GUID) 和裝置 ID 運作。	裝置控制在檔案系統層級上運作。磁碟區層級的工作 (例如，可透過指令行或磁碟公用程式執行的工作) 未受影響。
裝置控制在具有星形字元或星號 (*) 的類別 ID 或裝置 ID 上執行萬用字元比對。	裝置控制執行規則運算式 (regex) 比對，且限於執行下列特定作業： • . (點) • \ (反斜線) • [set], [^Set] (集) • * (星形字元或星號) • + (加號)
依預設，硬體裝置清單包括多種常見裝置類型。	您只能從五個裝置類型中進行選擇： • Thunderbolt • CD/DVD • USB • FireWire • 安全數位 (SD) 卡 您無法使用硬體裝置清單。
您可透過類別 ID 或裝置 ID 將其他自訂裝置新增到硬體裝置清單。	您無法新增其他自訂裝置。
要攔截 (或從攔截排除) 的裝置僅可從硬體裝置清單中取得。此清單包括預設常見裝置類型，也包括您可能已新增的自訂裝置。	要攔截 (或從攔截排除) 的裝置可從上述裝置類型中選取。廠商、型號和序號可保留為空白，或由規則運算式 (regex) 查詢定義。您可使用規則運算式來定義一系列類似裝置，例如不同廠商、型號、序號範圍等。
您可一次新增多個裝置類型。	您一次僅可以新增一個裝置類型。
要採取的行動是攔截，或從攔截排除 (允許)。	要採取的行動是攔截，或使用掛載權限從攔截排除 (允許)。下列掛載權限受支援： • 唯讀 • 讀取和寫入 • 讀取和執行 • 讀取、寫入和執行
您可以自訂裝置控制的用戶端通知。	您無法自訂裝置控制的用戶端通知。

如需詳細資訊，請參閱：

[管理裝置控制](#)

Windows 用戶端的 Symantec Endpoint Protection 功能相依性

部分政策功能需要同時啟用，才能提供對 Windows 用戶端電腦的完整防護。

WARNING

賽門鐵克建議您不要停用「智慧型掃描查詢」。

Table 208: 防護功能的相依性

功能	交互操作性指示
下載防護	下載防護功能為自動防護的一部分，可使 Symantec Endpoint Protection 能夠追蹤 URL。有幾種政策功能需要追蹤 URL。 如果您安裝的 Symantec Endpoint Protection 沒有下載防護功能，則「下載鑑識」的功能會有所限制。瀏覽器入侵預防需要下載防護功能。 「自動信任從內部網路網站下載的任何檔案」選項也需要下載防護功能。
下載鑑識	「下載鑑識」具有下列相依性： - 必須啟用「自動防護」 如果您停用「自動防護」，即使「下載智慧型掃描」已啟用，仍將無法運作。 - 必須啟用智慧型掃描查詢 賽門鐵克建議您讓「智慧型掃描查詢」選項保持啟用狀態。如果您停用該選項，會完全停用「下載鑑識」。 Note: 如果沒有安裝基本的「下載防護」，「下載鑑識」會在層級 1 的用戶端上執行。系統不會套用您在此政策中設定的任何層級。同樣地，使用者也無法調整靈敏度層級。 即使您停用「下載鑑識」，「自動信任從內部網路網站下載的任何檔案」選項仍會繼續運作。 如果您停用「下載鑑識」，則會停用入口網站偵測。這意味著自動防護以及排程掃描和隨選掃描會將所有檔案評估為非入口網站檔案，並使用由賽門鐵克決定的敏感程度。請參閱： 管理「下載鑑識」偵測
智慧型掃描查詢和雲端防護	「智慧型掃描查詢」會使用雲端中的 Symantec Insight 信譽資料庫，針對從支援的入口網站下載的檔案進行決策。 在標準和內嵌式/VDI 用戶端上執行自動防護、排程掃描和隨選掃描的過程中，「智慧型掃描查詢」功能會自動執行。標準和內嵌式/VDI 用戶端支援啟用雲端的内容。 如需詳細資訊，請參閱： Windows 用戶端如何從雲端接收定義檔 雲端掃描具有下列功能相依性： - 必須啟用「智慧型掃描查詢」。否則，雲端掃描和「智慧型掃描查詢」無法運作。 - 必須啟用「下載鑑識」，才能將檔案標示為入口網站檔案。 - 如果「下載鑑識」已停用，則雲端掃描和「智慧型掃描查詢」會繼續運作。它們所使用的靈敏度等級由賽門鐵克自動設定，僅用於偵測大多數惡意檔案。
SONAR	SONAR 具有下列相依性： - 必須安裝下載防護。 - 必須啟用「自動防護」。 如果已停用「自動防護」，則 SONAR 會失去部分偵測功能，並顯示未於用戶端上正常運作。然而，即使已停用「自動防護」，SONAR 仍然可以偵測啟發式威脅。 - 必須啟用「智慧型掃描查詢」。 如果沒有使用「智慧型掃描查詢」，則 SONAR 可以執行，但無法進行偵測。在極少見的情況下，SONAR 可以在沒有使用「智慧型掃描查詢」的情況下進行偵測。如果 Symantec Endpoint Protection 先前已快取了有關特定檔案的信譽資訊，則 SONAR 可能會使用快取的資訊。 如需詳細資訊，請參閱： 管理 SONAR
瀏覽器入侵預防	必須安裝下載防護。可啟用或停用「下載鑑識」。
信任的 Web 網域例外	只有在已安裝「下載防護」時才會套用例外。
自訂 IPS 特徵	使用防火牆。請參閱： 管理自訂入侵預防特徵

功能	交互操作性指示
Power Eraser	使用「智慧型掃描查詢」。 Power Eraser 使用信譽資訊檢查檔案。Power Eraser 具有無法修改的預設信譽靈敏度設定。如果您停用「允許進行智慧型掃描查詢以偵測威脅」選項，Power Eraser 就無法使用 Symantec Insight 提供的信譽資訊。在沒有「智慧型掃描」的情況下，Power Eraser 會減少偵測次數，而且偵測較可能產生誤報的情況。 Note: Power Eraser 會使用自己的信譽臨界值，這些臨界值無法在 Symantec Endpoint Protection Manager 中架構。Power Eraser 不使用「下載智慧型掃描」設定。 如需詳細資訊，請參閱： 從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項
記憶體攻擊緩和	必須安裝入侵預防。可啟用或停用入侵預防。

更多資訊

[選擇要在用戶端上安裝哪些安全性功能](#)

Symantec Endpoint Protection 隨附的工具

本文說明了 Symantec Endpoint Protection 隨附的工具以及這些工具的用途。

- [位於安裝檔案中的工具](#)
- [與 Symantec Endpoint Protection Manager 一起安裝的工具](#)
- [附加到知識庫 \(KB\) 文章的工具](#)

安裝檔案上的工具

下列工具和說明文件位於從 Broadcom「[下載管理](#)」頁面下載之完整 Symantec Endpoint Protection 安裝檔案的 /Tools 資料夾中：若要查看##資料夾，請使用 7-zip 等工具提取完整的 Symantec Endpoint Protection。

您可以在下列位置的工具 ZIP 檔案中找到這些工具的許多說明檔：

相關文件

ApacheReverseProxy

此工具可在 Symantec Endpoint Protection Manager 中設定 Apache Webserver，以允許 Mac 用戶端和 Linux 用戶端透過 Web 伺服器下載 LiveUpdate 內容。Apache Web 伺服器與 Symantec Endpoint Protection Manager 搭配運作，可在每次發佈新內容時，針對 Mac 和 Linux 用戶端本機下載和快取 LiveUpdate 內容。

此工具適用於用戶端數目較少的網路。

CleanWipe (14.3 RU9 和更早版本)

CleanWipe 會解除安裝 Symantec Endpoint Protection 產品。只有在嘗試 Windows 控制台等其他解除安裝方法失敗的情況下，才應使用 CleanWipe 作為最後方法。

請參閱[解除安裝 Symantec Endpoint Protection](#)

ContentDistributionMonitor (SEPMMonitor)

內容派送監控可協助監控群組更新提供者 (GUP) 健康狀態和狀態以及一般內容部署。此工具是直接接在 Symantec Endpoint Protection Manager (SEPM) 伺服器上執行的輕量型獨立式工具，而且應該傳回內容派送狀態的圖形化顯示。

欺詐 (14.3 RU8 和更早版本)

欺敵可用於偵測端點中使用「欺敵」的對抗活動。此方法的基礎假設為攻擊者已違反網路的主要防禦並在環境中執行偵察。攻擊者會尋找重要資產，例如網域控制器或資料庫憑證。

DeviceInfo

DeviceInfo 可獲取特定 Mac 裝置的裝置廠商、型號或序號。新增此資訊至「硬體裝置」清單。然後，可以將裝置 ID 新增至裝置控制政策，以允許或攔截用戶端電腦上的裝置。

更多資訊

- [使用 DeviceInfo 取得 Mac 裝置的裝置廠商、型號或序號](#)
- [Endpoint Protection 中的 Mac 裝置控制](#)
- [新增硬體裝置至硬體裝置清單中](#)
- [使用「裝置控制」和「應用程式控制」封鎖或允許裝置](#)

ITAnalytics

IT Analytics 軟體透過讓您建立自訂報告和自訂查詢，來擴充 Symantec Endpoint Protection 提供的內建報告功能。IT Analytics 提供 Symantec Endpoint Protection Manager 資料庫內所含資料的多維分析和圖形報告功能。此功能可讓您不需要具備資料庫或第三方報告工具的進階知識，就能夠自行瀏覽資料。

JAWS

JAWS 螢幕閱讀器程式和一組程序檔可讓您更易於讀取 Symantec Endpoint Protection 功能表和對話方塊。JAWS 是一項輔助技術，可遵循 Section 508 產品存取性。

不支援

- **MoveClient**

MoveClient 是 Visual Basic 程序檔，會根據用戶端的主機名稱、使用者名稱、IP 位址或作業系統，將用戶端從一個 Symantec Endpoint Protection Manager 群組移至另一個群組。MoveClient 也會在使用者模式與電腦模式之間切換用戶端。請參閱：

[在使用者模式和電腦模式之間切換 Windows 用戶端](#)

- **Qextract**

Qextract 可從用戶端的本機隔離所解壓縮和還原檔案。如果用戶端隔離了某個檔案，而您認為其為誤報，就可能需要此工具。

PushDeploymentWizard

可使用推動部署精靈將 Symantec Endpoint Protection 用戶端安裝套件部署至目標電腦。推動部署精靈與 Symantec Endpoint Protection Manager 中的用戶端部署精靈相同。通常，您可以使用它來部署至較小的電腦或遠端電腦群組。請參閱：

如需詳細資訊，請參閱：[Symantec Endpoint Protection 中的推動部署精靈概觀](#)

SplunkAuditPolicyDiff (14.3 MP1 和更新版本)

SplunkAuditPolicyDiff 是一個 Python 指令碼，可用來尋找 Splunk 中稽核日誌中 policy.xml 內容之間的差異。此指令碼列出對 Symantec Endpoint Protection Manager 政策所做的變更。此工具是根據 XMLDiff Python 模組。

SylinkDrop

在 14.3 RU5 和更新版本中，SylinkDrop 工具僅隨著 Symantec Endpoint Protection Manager 一起安裝。

SymDiag

SymDiag 是一款多產品診斷工具，可識別常見問題、收集支援協助式疑難排解所需的資料、提供其他客戶自助和支援資源的連結。SymDiag 也可以針對一些賽門鐵克產品以及 Threat Analysis Scan 提供授權和維護狀態，這有助於找到潛在的惡意軟體。

虛擬化

此虛擬化工具可改善虛擬桌面基礎架構 (VDI) 環境中所安裝用戶端的掃描效能。

- **SharedInsightCache**

共用智慧型掃描快取工具使用戶端不必掃描 Symantec Endpoint Protection 用戶端已判斷為未感染病毒的檔案，因而改善了虛擬化環境中的掃描效能。如果用戶端掃描檔案中是否存在威脅並判斷該檔案未感染病毒，則用戶端會將有關該檔案的資訊傳送至共用智慧型掃描快取。

之後，當另一個用戶端嘗試掃描同一個檔案時，該用戶端可以查詢共用智慧型掃描快取以判斷該檔案是否未感染病毒。如果該檔案未感染病毒，該用戶端不會掃描該特定檔案。如果該檔案感染了病毒，則用戶端會掃描該檔案中的病毒，並將相應結果傳送到共用智慧型掃描快取。

共用智慧型掃描快取是一種獨立於用戶端執行的 Web 服務。不過，必須架構 Symantec Endpoint Protection 以指定共用智慧型掃描快取的位置，以使用戶端能夠與其通訊。共用智慧型掃描快取透過 HTTP 或 HTTPS 與用戶端通訊。在掃描完成之前，會維持與用戶端的 HTTP 連線。請參閱：

[安裝和架構 SEP 共用智慧型掃描快取](#)

- **虛擬影像例外**

若要在 VDI 環境中提高效能和安全性，常見的做法是視需要使用基礎影像來建立虛擬機器階段作業。賽門鐵克虛擬映像例外工具可讓 Symantec Endpoint Protection 用戶端略過基礎影像檔案威脅掃描，這會降低磁碟 I/O 的資源負載。它還會改善 VDI 環境中的 CPU 掃描程序效能。請參閱：

[關於賽門鐵克虛擬影像例外工具](#)

WebServicesDocumentation

Symantec Endpoint Protection 包括一組 Web 服務形式的公用 API，可支援遠端監控和管理 (RMM) 應用程式。Web 服務提供有關用戶端和管理伺服器功能。對 Symantec Endpoint Protection Web 服務的所有呼叫都將透過 OAuth 進行驗證，並且僅允許授權的 Symantec Endpoint Protection 管理員存取。開發人員使用這些 API 將其公司的第三方網路安全解決方案與 Symantec Endpoint Protection 管理伺服器 and 用戶端進行整合。

支援遠端管理和遠端監控。遠端管理透過 Web 服務形式的公用 API 所提供，可讓您將協力廠商解決方案或自訂主控台與基本用戶端和管理伺服器功能整合。遠端監控透過公開支援的登錄機碼和 Windows 事件記錄所提供。

適用於遠端管理的 Web 服務可執行下列工作：

- 除了將授權狀態報告至 Windows 事件日誌外，還會依 Web 服務呼叫報告管理伺服器上的授權狀態和內容狀態。
- 將指令核發給用戶端，例如更新、更新並掃描，以及重新啟動。
- 管理傳送至用戶端的政策。可以從另一部管理伺服器匯入政策，也可以將政策指派至另一部管理伺服器上的群組或位置。

與 Symantec Endpoint Protection Manager 一起安裝的工具

下列工具將與 Symantec Endpoint Protection Manager 一起安裝到以下預設位置：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

CollectLog

CollectLog.cmd 將 Symantec Endpoint Protection Manager 日誌放置在壓縮的 .zip 檔案中。將該 .zip 檔案傳送給 Broadcom 支援或其他管理員以進行疑難排解。

ConfigSEPM

在部分安全或隔離的環境中，您必須停用從 Symantec Endpoint Protection Manager 到網際網路的所有連出連線。

請參閱：[如何從 Endpoint Protection Manager 停用所有連出網路連接](#)

資料庫驗證程式

可使用 dbvalidator.bat 來協助支援部門診斷 Symantec Endpoint Protection Manager 執行之資料庫所存在的問題。

LogUtils

scm-datacollector

由於難以使用具有更安全授權的虛擬服務帳戶 (VSA)，所以用於建立記憶體和執行緒傾印。

請參閱：[SEPM 對資料收集程式進行疑難排解](#)

SetSQLServerTLSEncryption

依據預設，Symantec Endpoint Protection Manager 透過加密通道與 Microsoft SQL Server 進行通訊。此工具可讓您停用或啟用管理伺服器與 Microsoft SQL Server 通訊之間的 TLS 加密。從 14 版開始，此工具可用於架構為使用 Microsoft SQL Server 資料庫的管理伺服器安裝。

SylinkDrop

Sylink.xml 檔案包含 Windows 用戶端與 Symantec Endpoint Protection Manager 之間的通訊設定。如果用戶端失去與 Symantec Endpoint Protection Manager 之間的通訊，請使用 SylinkDrop 工具自動將用戶端電腦上的現有 Sylink.xml 檔案取代為新的 Sylink.xml 檔案。

取代 Sylink.xml 檔案需執行下列工作：

- 將非受管用戶端轉換為受管用戶端。
- 將用戶端移轉/移動至新的網域或管理伺服器。
- 將無法在管理伺服器上修正的通訊損壞還原至用戶端。
- 將用戶端從一台伺服器移至另一台非遠端複製夥伴的伺服器。
- 將用戶端從一個網域移至另一個網域。

您也可以將此工具僅用於 Windows 用戶端；該工具位於 (64 位元) : C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

如需詳細資訊，請參閱：

[使用 SylinkDrop 工具還原用戶端伺服器通訊設定](#)

第三方移除工具 (TPAR)

移除用戶端電腦上的第三方安全軟體，以便您可以安裝 Symantec Endpoint Protection 用戶端。

請參閱：[Endpoint Protection/Endpoint Security 中的第三方安全軟體移除](#)

updatedbtime

請參閱：[SEPM LiveUpdate 在伺服器的時鐘意外移入未來後無法正常運作](#)

附加到知識庫 (KB) 文章的工具

從文章內部或附件部分的底部下載每個工具。

API 參考

Symantec Endpoint Protection Manager 包含一組連線至 Endpoint Detection and Response (EDR) 並從中執行 Symantec Endpoint Protection Manager 作業的 REST API。如果您無法存取 Symantec Endpoint Protection Manager，請使用 API。文件位於：

- Broadcom 入口網站。請參閱：
[Endpoint Security REST API 說明文件](#)
- 位於下列位址的 Symantec Endpoint Protection Manager 伺服器上，其中 SEPM-IP 是 Symantec Endpoint Protection Manager 伺服器的 IP 位址：
<https://SEPM-IP:8446/sepm/restapidocs.html>
IP 位址包括 IPv4 和 IPv6。您必須用方括弧括住 IPv6 位址：[http://\[SEPM-Server\]:#####](http://[SEPM-Server]:#####)

CleanWipe

若要下載最新版本的 CleanWipe，請參閱[下載 CleanWipe 移除工具來解除安裝 Endpoint Protection](#)

資料庫綱要

聯繫 Broadcom 技術支援，他們可以提供 Symantec Endpoint Protection Manager 綱要。

DeviceInfo

DevViewer 可獲取特定 Windows 裝置的裝置廠商、型號或序號。新增此資訊至 Symantec Endpoint Protection Manager 的「硬體裝置」清單。然後，可以將 GUID 或裝置 ID 新增至裝置控制政策，以允許或攔截用戶端電腦上的裝置。

從下列位置的「附件」區段下載 DevViewer：

[使用 DevViewer 在 Endpoint Protection 中尋找進行裝置攔截的硬體裝置 ID](#)

更多資訊

- [新增硬體裝置至硬體裝置清單中](#)
- [在 Endpoint Protection 中攔截或允許裝置](#)

LiveUpdate 管理員

Symantec LiveUpdate Administrator 是不同於 Symantec Endpoint Protection 的獨立式 Web 應用程式。LiveUpdate Administrator 會鏡像公用 LiveUpdate 伺服器的內容，然後在內部透過內建 Web 伺服器將該內容提供給賽門鐵克產品。

LiveUpdate Administrator 是 Symantec Endpoint Protection 的選擇性元件，更新 Symantec Endpoint Protection 用戶端時不需要 LiveUpdate Administrator。依據預設，Symantec Endpoint Protection Manager 使用 LiveUpdate 技術而非 LiveUpdate Administrator，以從 Symantec 公用 LiveUpdate 伺服器直接下載內容。

在某些情況下，您可能需要使用 LiveUpdate Administrator。例如，如果 Symantec Endpoint Protection Manager 無法下載內容，則請改用 LiveUpdate。您可以先安裝 LiveUpdate Administrator 伺服器，然後架構 Symantec Endpoint Protection Manager 以從 LiveUpdate 進行下載。請參閱：

[何時使用 LiveUpdate Administrator](#)

若要下載 LiveUpdate Administrator 和說明文件，請參閱：

- [下載 LiveUpdate Administrator \(LUA\)](#)
- [LiveUpdate Administrator 版本說明和修正附註](#)

Symantec Endpoint Protection 和 Symantec Endpoint Security 中適用於 Windows 用戶端服務 smc 的指令

您可以使用 smc (或 smc.exe) 指令行介面執行 Windows 用戶端服務。您可以在遠端執行用戶端的程序檔中使用 smc 指令。例如，您可能需要停止用戶端才能在多個用戶端上安裝應用程式。然後，您可以使用程序檔一次停止和重新啟動所有用戶端。

除了 smc -start 參數之外，用戶端服務必須執行，才能使用指令行參數。指令行參數不區分大小寫。對於某些參數，您可能需要密碼。用戶端不支援 UNC 路徑。

使用 smc 指令行介面執行 Windows 指令

1. 在用戶端電腦上，按下「開始 > 執行」，然後輸入 cmd。
2. 在命令提示視窗中，執行下列其中一項工作：

- 如果此參數不需要密碼，請輸入：

```
smc -<parameter>
```

其中 *parameter* 是參數。

- 如果此參數需要密碼，請輸入：

- `smc -p <password> -<parameter>`

例如：`smc -p 1234 -exportconfig c:\profile.xml`

NOTE

您必須在指令之前輸入 smc 服務的安裝路徑。例如，在安裝 Symantec Endpoint Protection 到預設位置的 64 位元 Windows 系統上，請輸入：

```
C:\Program Files\Symantec\Symantec Endpoint Protection\smc.exe
```

Table 209: smc 的參數

參數	說明	套用到
<code>smc -start ↑*</code>	啟動用戶端服務。 傳回 0、-1	所有支援的版本
<code>smc -stop↑↑*</code>	停止用戶端服務，並從記憶體卸載。 如果此指令受密碼保護，則在一般使用者輸入正確的密碼後一分鐘內停用用戶端。 傳回 0、-1	所有支援的版本
<code>smc -startgui</code> <code>smc -showgui</code> <code>smc -dismissgui</code>	將目前登入的使用者資訊傳送給 Symantec Endpoint Protection Manager。 顯示用戶端使用者介面。 關閉用戶端使用者介面。	所有支援的版本
<code>smc -cloudmanaged <path to Symantec_Agent_Setup.exe></code>	將雲端管理裝置移至另一個雲端網域或租用戶。 將用戶端電腦從 Symantec Endpoint Protection Manager 管理移至雲端主控台管理。 對於目的地雲端網域/租用戶，需要 <code>Symantec_Agent_Setup.exe</code> 安裝檔案。您可以從雲端主控台下載此檔案。請參閱： 使用 smc 在 SEP 和 SES 管理之間切換 Windows 用戶端，或變更裝置的租用戶或網域	14.2 RU1 的新功能
<code>smc -configure -proxy-mode <mode></code>	與註冊參數一起使用，讓用戶端可以使用所需的代理架構進行註冊。也可用於更正錯誤的代理選項。 可能的模式如下所示： system 、 manual 、 none 。 指定代理位址會自動切換至 手動模式。如果您輸入 manual ，但未指定 Proxy 主機，則會忽略此模式。 在 Symantec Endpoint Protection Manager 所管理的用戶端上不受支援 如需更多資訊，請參閱表格： 在指令提示中輸入的代理設定組合	14.3 RU1 的新功能
<code>smc -configure -proxy-address <host or IP></code>	允許您手動指定代理主機或代理位址。 如果將代理模式設定為手動，則為必要項目。	14.3 RU1 的新功能
<code>smc -configure -proxy-port <port number></code>	允許您手動指定代理通訊埠。 相同的通訊埠會用於 HTTP 和 HTTPS 連線。 如果未指定任何通訊埠，則會將通訊埠自動設定為 80 (對於 HTTP) 和 443 (對於 HTTPS)。	14.3 RU1 的新功能
<code>smc -configure -proxy-port-http <port number></code>	允許您手動指定 HTTP 連線的代理通訊埠。 覆寫預設 HTTP 通訊埠或已透過 <code>smc -configure -proxy-port</code> 指定的通訊埠。	14.3 RU1 的新功能
<code>smc -configure -proxy-port-https <port number></code>	允許您手動指定 HTTPS 連線的代理通訊埠。 覆寫預設 HTTPS 通訊埠或已透過 <code>smc -configure -proxy-port</code> 指定的通訊埠。	14.3 RU1 的新功能
<code>smc -configure -proxy-auth-mode basic</code>	可能的驗證模式如下： basic 、 ntlm 。 預設驗證模式為 basic 。	14.3 RU1 的新功能
<code>smc.exe -configure -proxy-user-name <name></code>	允許您手動指定代理使用者。 對於 ntlm ，您必須指定一個網域/使用者。	14.3 RU1 的新功能
<code>smc -configure -proxy-password <plain pwd></code>	允許您手動指定代理密碼。 最大長度為不含空值的 255 個字元。密碼區分大小寫。	14.3 RU1 的新功能
<code>smc -enable -ntp</code> <code>smc -disable -ntp ↑</code>	啟用/停用 Symantec Endpoint Protection 防火牆與入侵預防系統。	所有支援的版本 14.2 RU1 <code>-disable</code> 新功能的密碼需求

參數	說明	套用到
smc -enable -mem * smc -disable -mem *	啟用/停用 Symantec Endpoint Protection 記憶體攻擊緩和系統。	版本 14 MP1 的新功能
smc -enable -gem * smc -disable -gem *	啟用/停用 Symantec Endpoint Protection 記憶體攻擊緩和系統。	僅限 14 版
smc -dismissgui	關閉用戶端使用者介面。 用戶端仍會執行並繼續保護用戶端電腦。 傳回 0	所有支援的版本
smc -exportconfig ††*	將用戶端架構檔案匯出至 .xml 檔案。組態檔包括以下管理伺服器設定： • 政策 • 群組 • 安全性設定 • 使用者介面設定 您必須指定路徑名稱和檔案名稱。例如，您可以輸入以下指令： smc -exportconfig C:\My Documents\MyCompanyprofile.xml 傳回 0、-1、-5、-6	所有支援的版本
smc -exportlog	將日誌的全部內容匯出為 .txt 檔案。 若要匯出日誌，請使用下列語法： smc -exportlog log_type 0 -1 output_file 其中： log_type 如下： • 0 = 系統日誌 • 1 = 安全日誌 • 2 = 流量日誌 • 3 = 封包日誌 • 4 = 控制日誌 例如，您可以輸入下列語法： smc -exportlog 2 0 -1 c:\temp\TrafficLog 其中 0 是檔案的開頭，而 -1 是檔案的結尾。 您僅可以匯出「控制日誌」、「封包日誌」、「安全日誌」、「系統日誌」和「流量日誌」。 名稱 output_file 是您指派給匯出檔案的路徑名稱和檔案名稱。 傳回 0、-2、-5	所有支援的版本
smc -exportadvrule †*	將用戶端防火牆規則匯出為 .xml 檔案。 此指令僅用於未受管用戶端或控制模式用戶端的防火牆規則。如果是伺服器控制模式或混合模式的用戶端，請使用 -exportconfig。 您必須指定路徑名稱和檔案名稱。例如，您可以輸入以下指令： smc -exportadvrule C:\myrules.xml 傳回 0、-1、-5、-6 您無法直接從對應網路磁碟機匯入架構檔或防火牆規則檔案。 防止使用者停用 Symantec Endpoint Protection 用戶端	所有支援的版本
smc -image †	取消註冊 Symantec Agent (Symantec Endpoint Protection 用戶端)，並將它保持已取消註冊狀態。 與一般取消註冊的差異在於移除硬體金鑰和保存的硬體金鑰資訊。 使用需要密碼才能匯入或匯出政策以及匯入用戶端通訊設定密碼選項。 如果是 SES 雲端主控台管理的用戶端，執行 smc -image 指令亦會導致用戶端變成未受管狀態。如果如此，您將需要執行其他指令，以雲端伺服器重新註冊該用戶端。請參閱： 在用戶端裝置上安裝 Symantec Agent，不會自動進行註冊	14.3 RU1 (Symantec Endpoint Security) 的新功能 14.3 RU6 (Symantec Endpoint Protection) 的新功能

參數	說明	套用到
<code>smc -importadvrule† *</code>	將防火牆規則匯入用戶端。您匯入的規則會覆寫任何現有規則。您可以匯入下列項目： - 透過 <code>smc -exportadvrule</code> 匯出的 .xml 格式規則 - 透過用戶端使用者介面匯出的 .sar 格式規則 只有用戶端為非受管用戶端，或是受管用戶端處於用戶端控制模式或混合模式時，才能匯入防火牆規則。處於伺服器控制模式的受管型用戶端會忽略這些規則。 若要匯入防火牆規則，請匯入 .xml 或 .sar 檔案。例如，您可以輸入以下指令： <pre>smc -importadvrule C:\myrules.xml</pre> 匯入規則之後，系統日誌會新增項目。 傳回 0、-1、-5、-6 若要附加規則，而不是覆寫規則，請從用戶端使用者介面中使用「匯入規則」。 如需詳細資訊，請參閱： 防止和允許使用者變更用戶端的使用者介面 在用戶端上匯出或匯入防火牆規則	所有支援的版本
<code>smc -importconfig ‡†*</code>	以匯入的架構檔取代用戶端目前架構檔的內容，並更新用戶端的政策。用戶端必須執行才能匯入架構檔的內容。 您必須指定路徑名稱和檔案名稱。例如，您可以輸入以下指令： <pre>smc -importconfig C:\My Documents\MyCompanyprofile.xml.</pre> 傳回 0、3、-1、-5、-6	所有支援的版本
<code>smc -importsymlink <path to symlink.xml>††</code>	匯入用戶端通訊檔案 (symlink.xml)。	所有支援的版本
<code>smc -enable -wss</code> <code>smc -disable -wss</code>	啟用或停用 Web 和雲端存取防護。	版本 14.0.1 MP1 的新功能
<code>smc -enable -pcapsmc -disable -pcap</code>	啟用或停用 WSS 通道內封包擷取。	
<code>smc -enable -sepsmc -disable -sep</code>	啟用或停用網路威脅防護、防病毒、主動型威脅防護、MEM 和 WSS。	
<code>smc -report</code>	建立包含用戶端上發生之當機或邏輯錯誤的傾印檔案 (.dmp)。此檔案會自動傳送給賽門鐵克技術支援。請聯絡技術支援來尋求協助診斷錯誤。 您可以在以下位置找到傾印檔案： <pre>SEP_Install\Data\LocalDumps</pre> 其中 SEP_Install 是安裝資料夾。根據預設，此路徑為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\version.	版本 14 的新功能
<code>smc -restart†</code>	停止並立即啟動用戶端，其會執行與 <code>-stop</code> 跟 <code>-start</code> 相同的任務。該指令會在不重新開機電腦的情況下重啟用戶端。使用此指令作為疑難排解工具，來協助診斷未知問題。	14.3 RU3 的新功能
<code>smc -runhi</code>	執行主機完整性檢查。 傳回 0	所有支援的版本
<code>smc -sepmmanaged</code>	將用戶端管理從雲端主控台復原回先前管理它的 Symantec Endpoint Protection Manager。	14.2 RU1 的新功能
<code>smc -sepmmanaged <path to symlink.xml></code>	匯入用戶端通訊檔案 (symlink.xml)。 等同於 <code>-importsymlink</code> 但不需要密碼。	14.2 RU1 的新功能
<code>smc -showgui</code>	顯示用戶端使用者介面。 傳回 0	所有支援的版本

參數	說明	套用到
<code>smc -updateconfig</code> ‡	起始用戶端伺服器通訊，確保用戶端的架構檔案是最新的。 如果用戶端的架構檔案不是最新的，則 <code>updateconfig</code> 會下載最新的架構檔案，並覆寫現有架構檔案，也就是 <code>serdef.dat</code> 。 傳回 0	所有支援的版本

‡ 需要與密碼搭配使用的參數 (自 14.3 RU10 起)。當您安裝或升級 Symantec Endpoint Protection Manager 時，在網站層級設定預設用戶端密碼。您可以建立稍後會覆寫網站層級密碼的群組層級密碼。

請參閱：[用密碼保護 Symantec Endpoint Protection 用戶端](#)

† 如果設定密碼則為支援密碼的參數。您可以使用密碼保護 Symantec Endpoint Protection Manager 中的用戶端。

* 如果符合下列條件，則只有管理員群組的成員可以使用的參數：

- 用戶端執行 Windows /Vista 或 Windows Server 2008，且使用者為 Windows 管理員群組的成員。
如果用戶端執行 Windows Vista，且啟用「使用者帳戶控制」，使用者會自動成為群組「管理員」和「使用者」的成員。

不再支援 `smc -checkinstallation` 和 `smc -checkrunning`。

Table 210: 在指令提示中輸入的代理設定組合

proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	動作
系統	否	否	否	否	使用系統代理
系統	是	否	否	否	ERROR_INVALID_COMMAND_LINE (遺漏密碼)
系統	否	是	否	否	ERROR_INVALID_COMMAND_LINE (遺漏使用者)
系統	否	否	是	否	使用系統代理 (忽略伺服器)
系統	是	是	否	否	搭配使用系統代理與驗證
系統	是	是	是	否	搭配使用系統代理與驗證 (忽略伺服器)
系統	是	是	是	是	搭配使用系統代理與驗證 (忽略伺服器和通訊埠)
manual	否	否	否	否	ERROR_INVALID_COMMAND_LINE
manual	是	否	否	否	ERROR_INVALID_COMMAND_LINE
manual	否	是	否	否	ERROR_INVALID_COMMAND_LINE
manual	否	否	是	否	具有預設通訊埠的有效 "manual" (自訂) 代理
manual	是	是	否	否	ERROR_INVALID_COMMAND_LINE
manual	是	是	是	否	具有預設通訊埠的有效 "manual" (自訂) 代理
manual	是	是	是	是	有效的 "manual" (自訂) 代理
manual	是	否	是	yes 或 no	ERROR_INVALID_COMMAND_LINE (無密碼)
manual	否	是	是	yes 或 no	ERROR_INVALID_COMMAND_LINE (無使用者)

proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	動作
無	否	否	否	否	有效的 "none" 代理
無	是	否	否	否	有效的 "none" 代理
無	否	是	否	否	有效的 "none" 代理
無	否	否	是	否	有效的 "none" 代理
無	是	是	否	否	有效的 "none" 代理
無	是	是	是	否	有效的 "none" 代理
無	是	是	是	是	有效的 "none" 代理
否	否	否	否	否	無代理設定
否	是	否	否	否	無代理設定 (忽略使用者)
否	否	是	否	否	無代理設定 (忽略密碼)
否	否	否	是	否	具有預設通訊埠的有效 "manual" (自訂) 代理
否	是	是	否	否	無代理設定 (忽略額外選項)
否	是	是	是	否	具有預設通訊埠的有效 "manual" (自訂) 代理
否	是	是	是	是	有效的 "manual" (自訂) 代理

更多資訊

[指令錯誤碼](#)

smc.exe 指令錯誤碼

下表顯示 `smc.exe` 指令在必要參數無效或遺漏時傳回的錯誤碼。

Table 211: smc.exe 指令錯誤碼

錯誤碼	說明
0	指令成功。
-1	Windows 管理員群組或 Windows 進階使用者群組中，無此使用者。若用戶端執行 Windows Vista，則 Windows 管理員群組成員中無此使用者。
-2	無效的參數。 您鍵入的參數可能錯誤，或者在參數後方附加了不正確的參數。
-3	未安裝 <code>smc</code> 用戶端服務。
-4	並未執行 <code>smc</code> 用戶端服務。
-5	無效的輸入檔。 例如， <code>importconfig</code> 、 <code>exportconfig</code> 、 <code>updateconfig</code> 、 <code>importadv</code> 、 <code>exportadvrule</code> 和 <code>exportlog</code> 參數需要正確的路徑名稱與檔案名稱。
-6	輸入檔不存在。 例如， <code>importconfig</code> 、 <code>updateconfig</code> 和 <code>importadvrule</code> 參數需要正確的路徑名稱、架構檔名稱 (.xml) 或防火牆規則檔案名稱 (.sar)。

更多資訊

使用第三方工具安裝 Windows 用戶端軟體

您可以使用第三方工具安裝用戶端，而不使用隨管理伺服器一起安裝的工具。如果您使用的是大型網路，則可能使用這些選項來安裝賽門鐵克用戶端軟體比較有利。

您可以藉由使用各種不同的第三方產品安裝用戶端。這些產品包括 Microsoft Active Directory、Tivoli、Microsoft Systems Management Server (SMS) 和 Novell ZENworks。Symantec Endpoint Protection 支援 Novell ZENworks、Microsoft Active Directory 和 Microsoft SMS。

您也可以在使用 **Symantec Software Management Solution powered by Altiris** 管理的環境中部署 Symantec Endpoint Protection。您可以使用下列其中一項政策，從一個 Software Management Solution 套件部署 Symantec Endpoint Protection：

- 「受管軟體傳送」政策
- 「快速傳送」政策

如需詳細資訊，請參閱 Software Management Solution 套件產品說明，或者請參閱：

[Symantec Software Management Solution 產品登陸頁面](#)

Table 212: 安裝用戶端的第三方工具

工具	說明
Windows Installer 指令行工具	賽門鐵克用戶端軟體安裝套件屬於 Windows Installer (MSI) 檔案，您可以使用標準的 Windows Installer 選項來架構。您可以使用支援 MSI 部署的環境管理工具 (如 Active Directory 或 Tivoli)，在您的網路上安裝用戶端。您可以架構「Windows 資訊安全中心」與非受管用戶端互動的方式。請參閱： • 關於用戶端安裝功能和屬性 • 關於架構 MSI 指令字串 • 關於架構 Setaid.ini • Symantec Endpoint Protection 指令行用戶端功能 • Symantec Endpoint Protection 指令行用戶端安裝屬性 • Windows Installer 參數 • 安裝 Windows 用戶端的指令行範例 • Windows 資訊安全中心屬性
Microsoft SMS 2003	您可以使用 Microsoft Systems Management Server 安裝用戶端。請參閱： 使用 Microsoft SCCM/SMS 安裝 Windows 用戶端
Windows Active Directory	如果用戶端電腦是 Windows Active Directory 網域的成員，您就可以使用 Windows Active Directory 群組原則物件。用戶端電腦同樣必須使用支援的 Windows 作業系統。請參閱： • 使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端 • 使用 Active Directory 群組原則物件解除安裝用戶端軟體
虛擬化軟體	您可以在虛擬環境中安裝用戶端。請參閱： 支援的虛擬安裝和虛擬化產品

更多資訊

[匯出用戶端安裝套件](#)

關於用戶端安裝功能和屬性

安裝功能和屬性是出現在文字檔和指令行中的字串。在所有用戶端軟體安裝期間，都會處理一些文字檔和指令行。安裝功能會控制要安裝的元件。安裝屬性則控制安裝之後要啟用或停用哪些子元件。安裝功能和屬性僅適用於 Symantec Endpoint

Protection 用戶端軟體，也適用於 Windows 作業系統。安裝功能和屬性不適用於 Symantec Endpoint Protection Manager 安裝。

安裝功能和屬性的指定方式有兩種：作為 Setaid.ini 檔案中的資料行，和作為 Windows Installer (MSI) 指令中的值。MSI 指令可以於 Windows Installer 字串中指定，也可以於 Setaid.ini 中指定，以執行自訂部署。進行所有受管用戶端軟體的安裝時，一律會處理 Windows Installer 指令和 Setaid.ini。如果指定不同的值，則一律優先採用 Setaid.ini 中的值。

關於架構 MSI 指令字串

Symantec Endpoint Protection 安裝軟體使用 Windows Installer (MSI) 3.1 或更新的套件進行安裝和部署。如果您使用指令行部署套件，您可以自訂安裝。您可以使用標準的 Windows Installer 參數，以及賽門鐵克特定功能與內容。

使用 Windows Installer 需要更高的權限。如果您嘗試在沒有提高權限的情況下安裝，安裝可能會未預先通知而失敗。

如需 Symantec 安裝指令和參數的最新清單，請參閱文章：

[Symantec Endpoint Protection 的 MSI 指令行參考。](#)

NOTE

不支援 Windows Installer 廣告功能。Setaid.ini 指定的功能和屬性的優先順序高於 MSI 指定的功能和屬性。MSI 指令的功能和屬性名稱區分大小寫。請參閱：

[關於架構 Setaid.ini](#)

關於架構 Setaid.ini

Setaid.ini 會出現在所有安裝套件中，並且控制許多方面的安裝內容，例如要安裝哪些功能。Setaid.ini 一律優先於用於啟動安裝的 MSI 指令字串中可能出現的任何設定。Setaid.ini 與 setup.exe 出現在相同的目錄中。如果匯出至單一 .exe 檔案，則無法架構 Setaid.ini。但是，當您從主控台匯出 Symantec Endpoint Protection 用戶端安裝檔案時，會自動架構該檔案。

如需您可以架構的行和值的相關資訊，請參閱 [Endpoint Protection 的 MSI 命令行參考](#)。

NOTE

這些功能會縮排以顯示階層。不過，在 Setaid.ini 檔案中時不會縮排。Setaid.ini 中的功能名稱區分大小寫。

功能值設為 1，則會安裝此功能。功能值設為 0，則不安裝此功能。您必須指定並安裝父功能，才能順利安裝用戶端功能。

請注意下列 setaid.ini 設定，而這些設定對應至 MSI 屬性，以進行 Symantec Endpoint Protection 用戶端安裝：

- DestinationDirectory 對應至 PRODUCTINSTALLDIR
- KeepPreviousSetting 對應至 MIGRATESETTINGS
- AddProgramIntoStartMenu 對應至 ADDSTARTMENUICON

更多資訊

- [Symantec Endpoint Protection 指令行用戶端功能](#)
- [Symantec Endpoint Protection 指令行用戶端安裝屬性](#)
- [Windows Installer 參數](#)

Symantec Endpoint Protection 指令行用戶端安裝屬性

這些安裝屬性是搭配 MSI 指令行安裝使用的。

Table 213: Symantec Endpoint Protection 用戶端安裝屬性

屬性	說明
RUNLIVEUPDATE=val	決定安裝程序是否執行 LiveUpdate，其中 val 是以下其中一個值： 1: 安裝期間執行 LiveUpdate (預設)。 0: 安裝期間不執行 LiveUpdate。 依預設，群組中全部的 Symantec Endpoint Protection 用戶端都會收到所有內容和產品更新的最新版本。如果用戶端架構為從管理伺服器接收更新，則用戶端只會接收伺服器所下載的更新。如果 LiveUpdate 內容政策允許所有更新，但管理伺服器未下載所有更新，用戶端只會接收伺服器所下載的內容。
ENABLEAUTOPROTECT=val	決定安裝完成後是否啟用「檔案系統自動防護」，其中 val 是以下其中一個值： 1: 安裝後啟用「自動防護」(預設)。 0: 安裝後停用「自動防護」。
CACHE_INSTALLER=val	決定是否在用戶端上快取安裝檔案，其中 val 是以下其中一個值： 1: 快取安裝檔案 (預設)。 0: 不快取安裝檔案。
MIGRATESETTINGS=val	決定升級方案中保留設定的狀態，其中 val 是以下其中一個值： 0: 不保留設定或日誌。 1: 保留所有設定和日誌。 2: 僅保留 Sylink.xml 和日誌。
ADDSTARTMENUICON=val	決定是否將程式新增到「開始功能表」資料夾，其中 val 是以下其中一個值： 0: 不將程式新增到「開始功能表」資料夾。 1: 將程式新增到「開始功能表」資料夾 (預設)。

使用指令行安裝 Symantec Endpoint Protection 用戶端功能

您可以在 Setaid.ini 檔案和 MSI 指令中指定安裝的防護功能。功能多半都有父與子的關係。如果您需要安裝具有父系功能的子系功能，必須也安裝父系功能。例如，如果您指定安裝「防火牆」功能，但是未指定安裝 NTPMain，就不會安裝防火牆。

NOTE

除非在 Endpoint Security 雲端伺服器上註冊 Symantec Endpoint Protection Manager 網域且 Symantec Endpoint Protection Manager 收到 Symantec Enterprise Security Complete 授權，否則應用程式強化將停用。

Table 214: Symantec Endpoint Protection 用戶端功能

功能	說明	必選的父系功能
Core	安裝用於用戶端與 Symantec Endpoint Protection Manager 之間通訊的檔案。這是必要的功能。	無
ADDefense	安裝 Endpoint Threat Defense for Active Directory 元件。	Core
DCMain	安裝「應用程式控制與裝置控制」功能。	PTPMain
下載	安裝下載檔案的完整防護。包含「下載智慧型掃描」提供的完整功能性信譽掃描。	SAVMain
防火牆	安裝防火牆功能。	NTPMain
ITPMain	安裝「網路入侵預防和瀏覽器入侵預防」功能。	NTPMain
LANG1033	安裝英文資源。	Core
NotesSnapiin	安裝「Lotus Notes 自動防護」電子郵件功能。 僅適用於低於 14.2 RU1 的版本。	SAVMain

功能	說明	必選的父系功能
NTPMain	安裝「防網路和主機侵入」元件。	Core
NTR	安裝 Web 和雲端存取防護元件。	Core
OutlookSnapin	安裝「Microsoft Exchange 自動防護」電子郵件功能。	SAVMain
Pop3Smtplib	安裝 POP3 和 SMTP 郵件的防護。僅適用於 32 位元系統。 僅適用於 14.2 RU1 和更舊版本。	SAVMain
PTPMain	安裝「主動型威脅防護」元件。	Core
SAVMain	安裝病毒、間諜軟體和基本下載防護。子功能會安裝其他防護。	Core
TruScan	安裝「行為分析 (SONAR)」功能。	PTPMain

請參閱：[Endpoint Protection 的 MSI 指令行參考](#)

Windows Installer 參數

Symantec Endpoint Protection 用戶端安裝套件會使用標準的 Windows Installer 參數和一組用來進行指令行安裝及部署的延伸檔案。

如需使用標準 Windows Installer 參數的詳細資訊，請參閱 Windows Installer 說明文件。您也可以從指令行執行 msixec.exe，取得完整的參數清單。

Table 215: Windows Installer 參數

參數	說明
Sep.msi (32 位元) Sep64.msi (64 位元)	Symantec Endpoint Protection 用戶端的安裝檔案。如果檔案名稱包含空格，在與 /I 和 /x 一起使用時，請在檔案名稱兩邊加上引號。 需要
Msiexec	Windows Installer 執行檔。 需要
/I ".msi 檔案名稱"	安裝指定的檔案。如果檔名包含空格，請在檔名兩邊加上引號。如果檔案和您執行的 Msiexec 位於不同的目錄，請指定路徑名稱。如果路徑名稱包含空格，請在路徑名稱兩邊加上引號。例如，msiexec.exe /I "C:\path to\Sep.msi" 需要
/qn	無訊息安裝。
/x ".msi 檔案名稱"	解除安裝指定的元件。 非必填
/qb	顯示安裝進度的基本使用者介面安裝。 非必填
/!v logfilename	建立詳細日誌檔，其中 logfilename 是要建立的日誌檔名稱。 非必填
PRODUCTINSTALLDIR =路徑	在目標電腦上指定一個自訂路徑，其中 路徑 是指定的目標目錄。如果路徑包含空格，請在路徑兩邊加上引號。依預設： 32 位元電腦：C:\Program Files\Symantec\Symantec Endpoint Protection 64 位元電腦 (14.3 RU4 或更舊版本)：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection 64 位元電腦 (14.3 RU5 或更新版本)：C:\Program Files\Symantec\Symantec Endpoint Protection 非必填

參數	說明
SYMREBOOT=value	控制安裝完成後重新啟動電腦，其中 value 是一個有效引數。 有效引數如下： - Force：要求電腦重新啟動。解除安裝時需要。 - Suppress：大部分情況下都不重新啟動。 - ReallySuppress：安裝程序完全不重新啟動，甚至是無訊息安裝。 非必填 Note: 以無訊息模式解除安裝 Symantec Endpoint Protection 用戶端時，使用 ReallySuppress 防止重新啟動。
ADDLOCAL= feature	選取要安裝的自訂功能，其中 feature 是一個指定的元件或元件清單。如果沒有使用這個屬性，預設會安裝所有適用的功能，並且安裝只偵測電子郵件程式的自動防護電子郵件用戶端。 若要增加用戶端安裝的全部適當功能，請依照 ADDLOCAL=ALL 使用 ALL 指令。請參閱： Symantec Endpoint Protection 指令行用戶端功能 Note: 指定要安裝的新功能時，您必須在已安裝功能名稱中，加上要保留的。如果未指定需要保留的功能，Windows Installer 便會將功能移除。指定現有的功能，就不會覆寫已安裝的功能。若要解除安裝現有的功能，請使用 REMOVE 指令。 非必填
REMOVE=feature	解除安裝先前安裝的程式，或已安裝程式中的特定功能，其中 feature 是以下其中一項： - 功能從目標電腦解除安裝功能或功能清單。 - ALL：解除安裝程式及所有已安裝的功能。如果沒有指定某個功能，那麼預設是 ALL。 非必填

Windows 資訊安全中心屬性

Symantec Endpoint Protection 用戶端安裝期間，您可以自訂 Windows 資訊安全中心 (WSC) 屬性。這些屬性只適用於非受管用戶端。Symantec Endpoint Protection Manager 控制受管型用戶端的這些屬性。

NOTE

這些屬性僅適用於 Windows XP Service Pack 3。不適用於執行 Windows Vista 或 Windows 7 或更新版本的用戶端，WSCAVUPTODATE 屬性除外。

「Windows 資訊安全中心」已在 Windows 7 及 Windows 8 中分別重新命名為「行動作業中心」與「重要訊息中心」，在 Windows 10 中則為「安全性與維護」。

Table 216: Windows 資訊安全中心屬性

屬性	說明
WSCCONTROL=val	控制 WSC，其中 val 是以下其中一個值： 0: 不控制 (預設)。 1: 在第一次偵測到時，停用一次。 2: 永遠停用。 3: 若是停用，請還原。
WSCAVALERT=val	架構 WSC 的防毒警示，其中 val 是以下其中一個值： 0: 啟用。 1: 停用 (預設)。 2: 不控制。

屬性	說明
WSCFWALERT=val	架構 WSC 的防火牆警示，其中 val 是以下其中一個值： 0: 啟用。 1: 停用 (預設)。 2: 不控制。
WSCAVUPTODATE=val	架構防毒定義的 WSC 過期時間，其中 val 是以下其中一個值： 1 - 90: 天數 (預設為 30)。
DISABLEDEFENDER=val	決定安裝期間是否停用 Windows Defender，其中 val 是以下其中一個值： 1: 停用 Windows Defender (預設)。 0: 不停用 Windows Defender。

安裝 Windows 用戶端的指令行範例

Table 217: 指令行範例

工作	指令行
以無訊息模式，使用預設設定將所有 Symantec Endpoint Protection 用戶端元件安裝至目錄 C:\SFN。抑制電腦重新啟動，然後建立詳細的日誌檔。	<code>msiexec /I SEP.msi PRODUCTINSTALLDIR=C:\SFN SYMREBOOT=ReallySuppress /qn /l*v c:\temp\msi.log</code>
以無訊息模式安裝含「病毒和間諜軟體防護」以及入侵預防和防火牆的 Symantec Endpoint Protection 用戶端。強制電腦重新啟動，然後建立詳細日誌檔。	<code>msiexec /I SEP.msi ADDLOCAL=Core,SAVMain,OutlookSnapin, Pop3Smt,ITPMain,Firewall SYMREBOOT=Force /qn / l*v c:\temp\msi.log</code>

使用 Microsoft SCCM/SMS 安裝 Windows 用戶端

您可以使用 Microsoft System Center Configuration Manager (SCCM) 來安裝 Symantec 用戶端軟體。我們假定使用 SCCM 的系統管理員先前已使用 SCCM 安裝軟體。因此，我們假定您不需要使用 SCCM 安裝 Symantec 用戶端軟體的相關詳細資訊。

NOTE

此主題也適用於 Microsoft Systems Management Server (SMS)。

NOTE

本附註適用於 SMS 2.0 及更早版本：如果使用 SMS，需要在「宣告的程式監視器」中停用用戶端的「在工具列上顯示所有系統動作的狀態圖示」功能。在某些情況下，Setup.exe 也許需要更新「宣告的程式監視器」所使用的某個共用檔案。如果檔案在使用中，那麼安裝就會失敗。

賽門鐵克建議 SCCM/SMS 套件啟動 Setup.exe，而非直接啟動 MSI。此方法可啟用安裝程式記錄。使用 SCCM/SMS 中的自訂套件建立功能而非套件精靈功能建立自訂套件。

WARNING

您應該使用從 Symantec Endpoint Protection Manager 中匯出的受管用戶端安裝套件。如果您使用產品下載或安裝檔案的用戶端安裝套件，則可以部署非受管用戶端。以預設設定安裝非受管用戶端，且用戶端不會與管理伺服器進行通訊。請參閱：

[使用儲存套件安裝 Symantec Endpoint Protection 用戶端](#)

Table 218: 使用 Microsoft System Center Configuration Manager / Systems Management Server 安裝用戶端的程序

步驟	說明
步驟 1	從包含軟體和政策的 Symantec Endpoint Protection Manager 中匯出受管用戶端安裝套件，以便安裝到用戶端電腦。依預設，受管用戶端安裝套件包含名為 Sylink.xml 的檔案，該檔案可識別管理用戶端的伺服器。
步驟 2	建立來源目錄，並將 Symantec 用戶端安裝套件複製到該來源目錄。例如，您可以建立來源目錄並複製從 Symantec Endpoint Protection Manager 中匯出的 Setup.exe 檔案。
步驟 3	在 SCCM/SMS 中，建立自訂套件，命名套件，然後將來源目錄指明為套件的一部分。
步驟 4	架構套件的「程式」對話方塊，來指定啟動安裝程序的可執行檔，可能的話，也指定具有參數的 MSI。
步驟 5	使用「宣告」功能將軟體派送到特定「集合」。

如需使用 SCCM/SMS 的詳細資訊，請參閱適合您版本的 Microsoft 說明文件。

使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端

您可以使用 Windows Active Directory 群組原則物件來安裝 Windows 用戶端。此程序假設您已安裝此軟體，並且使用 Windows Active Directory 來安裝具有 Active Directory 群組原則物件的用戶端軟體。

Symantec 用戶端安裝使用標準 Windows Installer (MSI) 檔案。因此，您可以使用 MSI 屬性自訂用戶端安裝。請參閱：

[關於架構 MSI 指令字串](#)

您應該確認您的 DNS 伺服器設定正確無誤，然後再進行部署。設定必須正確無誤，因為 Active Directory 仰賴 DNS 伺服器進行電腦通訊。若要測試設定，您可以連線偵測 Windows Active Directory 電腦，然後反向連線偵測。請使用完整的網域名稱。僅使用電腦名稱將無法呼叫新的 DNS 搜尋。格式如下：

ping computename.fullyqualifieddomainname.com

WARNING

您應該使用從 Symantec Endpoint Protection Manager 中匯出的受管用戶端安裝套件。如果您使用產品下載或安裝檔案的用戶端安裝套件，則可以部署非受管用戶端。以預設設定安裝非受管用戶端，且用戶端不會與管理伺服器進行通訊。請參閱：

[使用儲存套件安裝 Symantec Endpoint Protection 用戶端](#)

Table 219: 使用 Active Directory 群組原則物件安裝用戶端軟體的步驟

步驟	動作
步驟 1	透過「獨立檔案 (.MSI 必需)」選項匯出受管用戶端安裝套件。請參閱： 使用儲存套件安裝 Symantec Endpoint Protection 用戶端
步驟 2	佈置安裝檔案的資料夾。例如，將受管用戶端安裝套件複製到您已在其上設定正確權限以允許存取的共用資料夾中。
步驟 3	建立 GPO 軟體派送。 您還應該在正式部署之前，在少數電腦上進行 GPO 安裝測試。如果您未正確架構 DNS，GPO 安裝可能要花一小時或更長時間。請參閱： 建立 GPO 軟體派送
步驟 4	將電腦新增到組織單位。請參閱： 將電腦新增到組織單位以安裝軟體

更多資訊

[使用 Active Directory 群組原則物件解除安裝用戶端軟體](#)

建立 GPO 軟體派送

如果您在環境中使用 Microsoft Active Directory，則您可以使用 GPO 部署 Symantec Endpoint Protection 用戶端套件至 Windows 電腦。您可建立軟體派送，然後架構軟體套件的 GPO 系統管理範本。

此程序假設您已安裝 Microsoft 的「群組原則管理主控台」，並加裝 Service Pack 1 或更新版本。Windows 介面可能會根據您使用的 Windows 版本而略微不同。

此程序也假設您在 Computers 群組或其他群組中有電腦需要安裝用戶端軟體。您可以選擇性地將這些電腦拖曳到建立的新群組。請參閱：

[使用 Active Directory 群組原則物件 \(GPO\) 安裝 Windows 用戶端](#)

建立 GPO 軟體散佈

1. 在 Windows 工作列上，按下「開始 > 所有程式 > 系統管理工具 > 群組原則管理」。
2. 在「**Active Directory 使用者和電腦**」視窗的主控台樹狀結構中，在網域上按下滑鼠右鍵，然後按下「**Active Directory 使用者和電腦**」。
3. 在「**Active Directory 使用者和電腦**」視窗中，選取合適網域下的目標組織單位 (OU)。您也可以建立新 OU 以供測試或其他用途。如需有關如何建立新 OU 的詳細資訊，請參閱 Microsoft 的 Active Directory 說明文件。
4. 在「群組原則管理」視窗的主控台樹狀結構中，在您剛選擇或建立的組織單位上按下滑鼠右鍵，然後按下「在這裡建立及連結 **GPO**」。
您可能需要重新整理網域，才能看到新建的 OU。
5. 在「新增 **GPO**」對話方塊的「名稱」方塊中，輸入 GPO 的名稱，然後按下「確定」。
6. 在右窗格您剛建立的 GPO 上按下滑鼠右鍵，然後按下「編輯」。
7. 在「群組政策物件編輯器」視窗的左窗格，展開「電腦設定」下方的「軟體設定」。
8. 在「軟體安裝」上按下滑鼠右鍵，再按「新增 > 套件」。
9. 在「開啟」對話方塊中，輸入指向並包含 MSI 套件的通用命名慣例 (UNC) 路徑。
使用以下範例所示的格式：
\\#####\SharedDir\Sep.msi
10. 按下「開啟」。
11. 在「部署軟體」對話方塊中，按下「已指派」，然後按下「確定」。
如果您選取「軟體安裝」，套件會出現在「群組政策物件編輯器」視窗的右窗格。

架構軟體套件的系統管理範本

1. 若要為套裝軟體架構管理範本，請在「群組政策物件編輯器」視窗的主控台樹狀結構中，顯示並啟用下列設定：
 - 「電腦組態」>「系統管理範本」>「系統」>「登入」>「永遠在電腦啟動及登入時等待網路啟動」
 - 「電腦組態」>「系統管理範本」>「系統」>「群組政策」>「軟體安裝政策處理」
 - 「使用者組態」>「系統管理範本」>「Windows 元件」>「Windows Installer」>「永遠以較高的權限安裝」

NOTE

如果您啟用了用戶端電腦上的使用者帳戶控制 (UAC)，您也必須啟用「電腦組態 > 系統管理範本 > Windows 元件 > Windows Installer > 永遠以較高的權限安裝」，來安裝具有 GPO 的 Symantec 用戶端軟體。設定這些選項，才能讓所有 Windows 使用者安裝賽門鐵克用戶端軟體。

2. 關閉「群組政策物件編輯器」視窗。
3. 在「群組原則管理」視窗的左窗格中，於剛編輯的 GPO 上按下滑鼠右鍵，然後按下「強制」。
4. 在右窗格的「安全性過濾」下方，按下「新增」。
5. 在對話方塊的「輸入要選取的物件名稱」下方，輸入「#####」，然後按下「確定」。

將電腦新增到組織單位以安裝軟體

您可以將電腦新增到由 GPO 安裝 Symantec Endpoint Protection 的組織單位。電腦重新啟動時，用戶端軟體安裝程序就會開始。使用者登入電腦時，用戶端軟體安裝程序即告完成。不過，群組政策更新並非即時，因此，需要時間來傳播此政策。下列程序包含您可以在用戶端電腦上執行的指令，以便依照需求更新政策。請參閱：

使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端

新增電腦到組織單位以安裝軟體

1. 在 Windows 工作列上，按下「開始 > 所有程式 > 系統管理工具 > **Active Directory** 使用者和電腦」。
2. 在「**Active Directory** 使用者和電腦」視窗的主控台樹狀結構中，找出一或多部電腦，將其新增到您針對 GPO 安裝所選擇的組織單位。
電腦會先出現在「電腦」組織單位中。
3. 將電腦拖放到為安裝而選擇或建立的組織單位中。
4. 關閉「**Active Directory** 使用者和電腦」視窗。

在用戶端電腦上隨選更新 GPO

1. 在用戶端電腦上，開啟命令提示字元。
2. 輸入 gpupdate，然後按 **Enter** 鍵。
完成時，「指令提示」視窗會顯示訊息，讓您知道已成功完成政策更新。如果顯示了錯誤訊息，請依照螢幕上的指示取得更多資訊。
3. 關閉「指令提示」視窗。

複製 Sylink.xml 檔案以製作受管安裝套件

安裝 Symantec Endpoint Protection Manager 時會為每一個用戶端群組建立 Sylink.xml 檔案。Symantec Endpoint Protection 用戶端會讀取這個檔案的內容，以瞭解哪一部管理伺服器管理用戶端。如果您從安裝檔案來安裝用戶端，則安裝的是非受管用戶端。不過，您可以在安裝之前將 Sylink.xml 檔複製到此資料夾，以安裝受管用戶端。

NOTE

從 Symantec Endpoint Protection Manager 主控台匯出的套件是受管套件，並且已經包括 Sylink.xml 檔案。若要匯出可以用「群組政策物件」部署的新受管套件，請使用用戶端部署精靈。按下「儲存套件」，然後在系統提示時勾選「獨立檔案 (.MSI 需要此項)」。

使用儲存套件安裝 Symantec Endpoint Protection 用戶端

將 **Sylink.xml** 檔案複製到產品安裝檔案以製作受管安裝套件

1. 在 Symantec Endpoint Protection Manager 中，從正確的用戶端群組匯出 Sylink.xml 檔並將它複製到電腦。

NOTE

匯出 Sylink.xml 檔之前，應該透過管理主控台建立至少一個新群組。如果未建立，用戶端會出現在預設群組中。

如需詳細資訊，請參閱：

- [新增群組](#)
 - [手動匯出用戶端伺服器通訊檔案 \(Sylink.xml\)](#)
2. 將安裝資料夾從您下載的安裝檔案複製至您用戶端電腦上的資料夾。資料夾 SEPx64 包含 64 位元用戶端。
您可以對先前匯出為個別檔案的非受管用戶端套件使用安裝資料夾。

3. 將 Sylink.xml 複製到安裝資料夾。在系統提示時取代現有的 Sylink.xml 檔。

使用 Active Directory 群組原則物件解除安裝用戶端軟體

您可以使用 Active Directory 解除安裝已安裝的用戶端軟體。

1. 在 Windows 工作列上，按下「開始 > 所有程式 > 系統管理工具 > 群組原則管理」。
您使用的 Windows 版本可能會在「開始」功能表中顯示「程式集」，而非「所有程式」。
2. 在「群組原則管理」視窗的主控台樹狀結構中，展開網域，展開「電腦設定」，展開「軟體設定」，在「軟體安裝」上按下滑鼠右鍵，然後按下「內容」。
3. 在「進階」標籤上，勾選「如果這個群組原則物件不再適用於管理領域，就解除這個應用程式安裝」，然後按下「確定」。
4. 在右窗格的軟體封裝上按下滑鼠右鍵，然後按下「移除」。
5. 在「移除軟體」對話方塊中，勾選「立刻移除使用者及電腦軟體」，然後按下「確定」。
6. 關閉「群組原則物件編輯器」視窗，然後關閉「群組原則管理」視窗。
重新啟動用戶端電腦時，就會解除安裝軟體。

[解除安裝 Symantec Endpoint Protection 用戶端](#)

Amazon Web Services 的 Symantec™ Endpoint Protection 快速入門指南

Amazon Web Services (AWS) 上的 Symantec Endpoint Protection Manager 使用說明和最佳實踐

當您首次登入 Amazon Web Services 上的 Symantec Endpoint Protection Manager Amazon Machine Image (AMI) 時，應該注意可能發生的問題。

Table 220: 可能的 Symantec Endpoint Protection Manager Amazon Machine Image (AMI) 問題

項目	說明
初始登入憑證	首次連線到實例時，Symantec Endpoint Protection Manager 將自動開啟，然後提示您更改密碼。
初始登入後 LiveUpdate	首次啟動 Symantec Endpoint Protection Manager LiveUpdate 時，下載的內容會比後續的 LiveUpdate 階段作業更多。因此，實例的回應速度會變慢，直到 LiveUpdate 完成。這是預期狀況，並且僅在初始啟動時發生。 LiveUpdate 在初始登入後五分鐘啟動 Symantec Endpoint Protection Manager。
用戶端不會立即顯示在 Symantec Endpoint Protection Manager	您可能會注意到，在實例上預先安裝的用戶端不會立即顯示在 Symantec Endpoint Protection Manager 中的 首頁選項卡上。這是預期狀況。Symantec Endpoint Protection Manager 活動訊號完成後，用戶端將顯示在首頁選項卡上。
更新管理員的電子郵件地址	您必須在 Symantec Endpoint Protection Manager 中更改管理員的預設電子郵件地址。依預設，電子郵件地址為 a@b.com。您可以在登入 Symantec Endpoint Protection Manager 的「管理員」窗格後，輕鬆地變更此電子郵件地址，其位置位於「管理員 > 編輯管理員」下方。 由於 Symantec Endpoint Protection Manager 的密碼復原需要有效的電子郵件地址，因此應在首次登入時執行此工作。
更新資料庫密碼	在版本 14 或更新版本中，您可以更改 Symantec Endpoint Protection Manager 的資料庫密碼。應在第一次登入時變更此密碼。請參閱： 變更管理員帳戶或內嵌資料庫的密碼

項目	說明
遠端推送部署 (選擇性)	Symantec Endpoint Protection Manager 推送部署使用 ICMP 連線偵測通訊協定查詢網路上實例的 IP 位址。您必須在用戶端實例候選項上明確添加 ICMP 回應要求入口規則，以使它們可以在 Symantec Endpoint Protection Manager 用戶端部署精靈中顯示。 若要成功地將用戶端套件從 Symantec Endpoint Protection Manager 部署到用戶端實例，必須在用戶端實例上啟用 TCP 通訊埠 445。有關詳細資訊，請參閱「安全性群組」章節。
安全性群組	下表演示了執行 Symantec Endpoint Protection 中 AMI 實例的建議安全性群組防火牆規則： 有關如何使用用戶端實例的資訊，請參閱： 適用於 Windows 的 Amazon EC2 安全性群組實例

Table 221: Symantec Endpoint Protection 實例的內送安全性群組設定

類型 / 通訊協定	套用到	埠號	來源	用途
自訂 TCP 規則 / TCP	Symantec Endpoint Protection Manager	8014 443*	0.0.0.0/0	用於 Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端之間的 HTTP 通訊。 * = 用於可選 HTTPS 組態。
自訂 TCP 規則 / TCP	Symantec Endpoint Protection Manager	8443	0.0.0.0/0	用於遠端管理主控台和 Symantec Endpoint Protection Manager 之間的 HTTPS 通訊。 所有登入資訊和管理通訊都是使用此安全通訊埠。
自訂 TCP 規則 / TCP	Symantec Endpoint Protection Manager	8444	0.0.0.0/0	由 Symantec Endpoint Protection Manager Web 服務使用。
自訂 TCP 規則 / TCP	Symantec Endpoint Protection Manager	8445	0.0.0.0/0	用於報告主控台的 HTTPS 通訊。
自訂 TCP 規則 / TCP	Symantec Endpoint Protection Manager	8765	0.0.0.0/0	用來關閉 Tomcat。
自訂 TCP 規則 / TCP	Symantec Endpoint Protection Manager	9090	0.0.0.0/0	用於遠端管理主控台和顯示登入畫面的 Symantec Endpoint Protection Manager 之間的初始登入通訊。
自訂 TCP 規則 / TCP	Symantec Endpoint Protection 用戶端	445	0.0.0.0/0	用於遠端部署來自 Symantec Endpoint Protection Manager 的安裝套件。
自訂 ICMP 規則 / 回應要求	Symantec Endpoint Protection 用戶端	不適用	0.0.0.0/0	由遠端推送用於查找網路上 Symantec Endpoint Protection 用戶端實例的 IP 位址。
RDP / TCP	Symantec Endpoint Protection Manager Symantec Endpoint Protection 用戶端	3389	0.0.0.0/0	用於遠端連線到實例。

Table 222: Symantec Endpoint Protection 實例的外寄安全性群組設定

類型 / 通訊協定	套用到	埠號	目的
全部流量 / 全部	Symantec Endpoint Protection Manager Symantec Endpoint Protection 用戶端	全部	0.0.0.0/0

在 Amazon Web Services 上使用 Symantec Endpoint Protection Manager 的要求

Amazon Web Services (AWS) 帳戶持有人可訂閱 Amazon Machine Image (AMI) 或 Amazon 的 Elastic Compute Cloud (EC2) 上的 Symantec Endpoint Protection Manager。

Table 223: 執行 Symantec Endpoint Protection Manager AMI 的先決條件、支援的平台和實例

需求	詳細資訊
先決條件	使用 Amazon EC2 的 Symantec Endpoint Protection Manager AMI 先決條件如下： - 您必須擁有 AWS Marketplace 帳戶。若要建立帳戶或存取現有帳戶，請移至： https://aws.amazon.com/marketplace - 如果使用「自帶授權 (BYOL)」選項，則必須具有有效的 Symantec Endpoint Protection 授權。若要檢閱您的授權狀態，請登入「Broadcom 支援入口網站」，然後前往： Broadcom 下載中心 或者，您可以聯絡支援，瞭解授權的非技術問題： Symantec 客戶支援
支援的平台和實例	Amazon EC2 (BYOL 和付費) 的 Symantec Endpoint Protection Manager AMI 包括以下產品的支援： - Symantec Endpoint Protection Manager，版本 14 MP1 或更新 - Windows Server 2012 R2 或更新 Symantec Endpoint Protection Manager AMI 支援 AWS Marketplace 上以下 Windows Server 2012 的 Amazon EC2 實例： 10 個用戶端層：m4.large (2 倍 CPU、8 GB RAM、EBS 磁片) 100 個用戶端層級：m4.xlarge (4x CPU，16 GB RAM，EBS 磁片) 250 個用戶端層級：m4.2xlarge (8x CPU、32 GB RAM、EBS 磁片) 500 個用戶端層級：c4.2xlarge (8x CPU、15 GB RAM、EBS 磁片)

其他參考

如需使用 Amazon EC2 和 Symantec Endpoint Protection AMI 的相關資訊，請參閱：

[AWS 入門指南](#)

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2025 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

