Symantec™ Messaging Gateway 10.7.3 管理指南

由 Brightmail™ 提供

Symantec

Symantec™ Messaging Gateway 10.7 管理指南

文件版本：1.0

法律聲明

Copyright ©2019 Symantec Corporation. 版權所有 © 2019 賽門鐵克公司。All rights reserved. 保留所有權利。

Symantec、Symantec 標誌和 Checkmark 標誌均為賽門鐵克公司或其附屬公司在美國及其他國家/地區的商標或註冊商標。其他名稱可能為其個別所有者的商標。

本文件中所述產品的散佈受到授權許可協議的規範，限制其使用、複製、散佈及解譯/逆向工程。未事先獲得賽門鐵克公司及其授權者 (如果有) 的書面授權，本產品的任何部分均不得以任何方式、任何形式複製。

本文件完全依「現狀」提供，不做任何所有明示或暗示的條件、聲明及保證，其中包含在任何特定用途之適售性與適用性的暗示保證、任何特定用途或不侵害他人權益，除了此棄權聲明認定的不合法部分以外。賽門鐵克公司對與提供之效能相關的意外或必然損害，或這份說明文件的使用，不負任何責任。本文件所包含的資訊若有變更，恕不另行通知。

根據 FAR 12.212 定義，授權許可的軟體和文件係「商業電腦軟體」，並受 FAR 第 52.227-19 節「商業電腦軟體 - 限制權利」和 DFARS 第 227.7202 節「商業電腦軟體和商業電腦軟體文件」中的適用法規以及所有後續法規中定義的限制權利的管轄，無論是藉由 Symantec 作為前提或託管服務所傳送。美國政府僅可根據此協議條款對授權許可的軟體和文件進行任何使用、變更、複製發行、履行、顯示或披露。

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec 支援

所有支援服務均依照您的支援協議及當時有效的企業技術支援政策予以提供。

知識庫文章和 Symantec Connect

聯絡技術支援之前，您可以在我們的線上知識庫中找到可用的內容，包括疑難排解文章、操作說明文章、警示和產品手冊。在下列 URL 的搜尋方塊中，輸入您的產品名稱：

https://support.symantec.com

請透過以下 URL 存取我們的部落格和線上論壇，與其他客戶、合作夥伴和賽門鐵克員工就廣泛的主題進行互動：

https://www.symantec.com/connect

技術支援和企業客戶支援

Symantec 支援在全球範圍內維護支援中心，全年無休。技術支援的主要角色是回應有關產品特性和功能的特定查詢。企業客戶支援會協助解決非技術性問題，例如授權啟用、軟體版本升級、產品存取和續購。

如需 Symantec 支援條款、條件、政策及其他支援資訊，請參閱：

https://entced.symantec.com/default/ent/supportref

若要聯絡 Symantec 支援，請參閱：

https://support.symantec.com/en_US/contact-support.html

目錄

Symantec 支援 3

第 1 章 Symantec Messaging Gateway 簡介 22

關於 Symantec Messaging Gateway 22
Symantec Messaging Gateway功能 23
Symantec Messaging Gateway 的運作方式 25
關於預設政策與功能 26
哪裡可以獲得更多資訊 27

第 2 章 部署掃描程式 29

關於掃描程式 29
關於 Symantec Messaging Gateway 中的 IPv6 位址 30
設定掃描程式 31
新增掃描程式 32
驗證或變更掃描程式安裝設定 32
指定 DNS 伺服器位址 33
驗證或變更主機上的時間設定 33
指定代理伺服器設定 34
架構 IPv4 乙太網路設定及路由 35
架構 IPv6 乙太網路設定及路由 36
架構進階乙太網路設定 37
架構掃描程式電子郵件設定 38
關於掃描程式電子郵件設定 39
架構郵件流方向 40
變更掃描程式入埠郵件設定 41
變更掃描程式入埠郵件接收設定 42
架構掃描程式入埠電子郵件傳送設定 43
變更掃描程式離埠郵件設定 44
變更掃描程式離埠郵件接收設定 45
架構掃描程式離埠郵件傳送設定 46
架構錯誤郵件處理 48
架構 SMTP 進階設定 48
SMTP 進階入埠設定 49
SMTP 進階離埠設定 50
SMTP 進階傳送設定 52

傳送繫結的 SMTP 進階設定 54
SMTP 進階驗證設定 55
指定用於非閘道部署的內部郵件主機 57
內部郵件伺服器： 非閘道部署 58
修改掃描程式組態 59
啟用與停用掃描程式 59
停止和啟動掃描程式 60
刪除掃描程式 61
變更控管中心主機的 IP 位址 62
管理服務與 MTA 作業 62
服務與 MTA 作業 63
掃描程式服務 64
MTA 與郵件佇列行為 65

第 3 章 架構電子郵件設定值 67

架構電子郵件設定值 67
架構電子郵件網域 69
關於電子郵件網域 70
新增或編輯網域 71
匯入網域清單 74
刪除網域 75
關於電子郵件網域接受設定 76
架構反向 DNS 驗證 76
架構電子郵件別名和地址偽裝 77
關於別名與位址偽裝 78
新增或編輯別名 79
匯入別名 79
新增或編輯位址偽裝 81
匯入位址偽裝清單 82
忽略本機位址中的文字大小寫 83
指定 TLS 通訊的 SSL 限制 83
關於無效收件者 85
設定無效的收件者處理 86
關於電子郵件訊息流 87
電子郵件訊息流階段 87
架構電子郵件進行 SMTP 驗證 89
關於使用 SMTP 驗證 90
如何設定 SMTP 驗證 91
架構 SMTP 驗證郵件設定 93
使用 SMTP 驗證的最佳實務準則 96
指定地址驗證條件 96

第 4 章 設定電子郵件寄件者驗證 98

寄件者驗證的運作方式 98
針對入埠郵件設定寄件者驗證 99
寄件者驗證的內容過濾政策 102
啟用 DMARC 報告 105
針對離埠郵件設定寄件者驗證 105
為網域啟用 DKIM 簽署 106
新增網域金鑰 109
匯入網域金鑰 109

第 5 章 設定寄件者群組 111

啟用或停用允許的寄件者群組和攔截的寄件者群組 111
為允許的寄件者群組和攔截的寄件者群組選擇動作 112
管理寄件者群組成員 112
新增寄件者至管理員定義之寄件者群組和第三方寄件者群組 113
編輯允許的寄件者群組和攔截的寄件者群組成員 114
刪除允許的寄件者群組和攔截的寄件者群組成員 114
啟用或停用允許的寄件者群組和攔截的寄件者群組成員 114
匯入允許的寄件者組項目和攔截的寄件者群組項目 115
寄件者群組匯入檔案格式 116
匯出寄件者群組資訊 117
識別寄件者的支援方法 118

第 6 章 啟用信譽過濾 120

啟用信譽型過濾功能 120
管理閘道的電子郵件流量 121
關於連線時攔截與允許郵件 122
關於管理閘道的連線負載 124
架構連線類別 125
架構電子郵件病毒攻擊辨識 127
架構電子郵件地址搜尋攻擊辨識 128
關於使用寄件者群組攔截和允許郵件 130
關於使用快速通過來節省資源 133
架構快速通過 135
防衛退回攻擊 136
關於防衛退回攻擊 137
架構控管中心的退回攻擊防護 138
架構政策群組的「退回攻擊防護」 139
建立退回攻擊防護的垃圾郵件或不必要的電子郵件政策 140
研究 IP 位址信譽 140

第 7 章 設定憑證 145

關於憑證 145
使用憑證 146
新增自行簽署的憑證 148
新增認證中心簽署憑證的方法 148
修改憑證授權中心簽署憑證匯入檔案 149
新增 CA 或中繼憑證 150
檢視現有的 CA 憑證 151
要求憑證授權中心簽署的憑證 151
匯入憑證授權中心簽署的憑證 152
取代所有現有的 CA 憑證 153
備份 CA 憑證 153
變更憑證或網域金鑰名稱 153
匯入應用程式憑證 154
匯出應用程式憑證 155
處理應用程式憑證 156
憑證與網域金鑰的 PEM 格式需求 157
檢視 SMTP/TLS 或 HTTPS 憑證 158
匯出 TLS 與 HTTPS 憑證 158
刪除 SMTP/TLS 或 HTTPS 憑證 159
指派 MTA TLS 憑證給掃描程式 159
指派使用者介面 HTTPS 憑證給控管中心 160

第 8 章 架構政策群組 161

關於政策群組 161
建立政策群組及指派政策 162
產生政策群組 163
新增成員至政策群組 164
刪除政策群組中的成員 165
關於管理政策群組成員 165
匯入及匯出政策群組成員 165
研究使用者所屬的政策群組 166
編輯、刪除、啟用或停用政策群組 168
關於選取政策群組的過濾政策 168
為政策群組選取惡意軟體政策 169
為政策群組選取垃圾郵件政策和不必要的電子郵件政策 170
選取用於政策群組的內容過濾政策 172
啟用與停用政策群組的使用者設定 173
啟用政策群組的一般使用者設定的需求 174
根據語言允許或攔截電子郵件 174
設定政策群組優先度 175

第 9 章 偵測病毒、惡意軟體與惡意攻擊 176

關於偵測病毒、惡意軟體與惡意攻擊 176
偵測病毒與惡意攻擊的產品技術 177
關於「解除」 179
使用「解除」移除潛在惡意內容 180
潛在惡意內容詳細資料 181
關於擷取解除的內容 183
對付可疑附件所採取的動作 184
間諜程式或廣告程式判斷詳細資訊 184
偵測病毒、惡意軟體與惡意威脅 185
建立電子郵件惡意軟體政策 187
預設電子郵件惡意軟體政策 188
管理電子郵件惡意軟體政策 190
修改電子郵件惡意軟體政策 191
啟用或停用電子郵件惡意軟體政策 191
刪除電子郵件惡意軟體政策 192
複製電子郵件惡意軟體政策 192
使用清單來改善病毒掃描效能 193
將檔案類型排除在病毒掃描範圍之外 193
修改要從掃描範圍排除的檔案類型 194
啟用或停用要從掃描範圍排除的檔案類型清單 195
刪除要從掃描範圍排除的檔案類型清單 196
匯出要從掃描範圍排除的檔案類型清單 196
設定巢狀檔案的限制 196
保持病毒定義檔在最新狀態 197
關於更新病毒定義 198
檢視病毒定義的狀態 199
排程自動病毒定義更新 200
停用自動病毒定義更新 200
視需要起始病毒定義更新 201
指定要從哪個來源取得病毒定義 201
修改人工智慧敏感程度 202

第 10 章 隔離可疑的病毒 204

關於隔離可疑病毒 204
關於瀏覽可疑病毒隔離所 205
架構可疑病毒郵件設定 205
選擇可疑病毒郵件的語言編碼 206
指定每頁顯示的可疑病毒郵件數目 206
指定可疑病毒郵件保留在隔離所的時間 207
修改為可疑病毒隔離所分配的磁碟空間 207
處理可疑的病毒郵件 208

檢視隔離所中可疑的病毒郵件 209
排序隔離所中的可疑病毒郵件 209
刪除隔離所中的可疑病毒郵件 209
從隔離所釋放可疑病毒郵件 210
搜尋隔離的病毒郵件 210

第 11 章 過濾垃圾郵件 213

關於過濾垃圾郵件及不必要的郵件 213
預設垃圾郵件及不必要的電子郵件政策 214
架構垃圾郵件及不必要的電子郵件偵測 216
掃描以文字為基礎的附件 218
建立偵測垃圾郵件及不必要的電子郵件的政策 219
減少不必要的電子郵件過濾的誤報 220
啟用和停用垃圾郵件及不必要的電子郵件政策 221
修改垃圾郵件及不必要的電子郵件政策 222
複製垃圾郵件政策 223
刪除垃圾郵件政策 223
架構可疑垃圾郵件識別的臨界值 224
啟用或停用向賽門鐵克提報 URI 225
啟用或停用 URL 信譽過濾 225
關於針對客戶特定垃圾郵件規則提交郵件 226
如何建立規則，以及為何郵件可能不會產生自訂規則 228
設定客戶特定垃圾郵件提交 228
啟用或停用客戶特定垃圾郵件提交 230
佈建客戶特定垃圾郵件提交的提交者 ID 230
設定客戶特定垃圾郵件提交積極程度 232
指定誰能夠提交客戶特定規則的郵件 233
處理「提交者電子郵件地址」清單 234
透過控管中心提交郵件以建立客戶特定規則 236
正在刪除客戶特定垃圾郵件資料 237

第 12 章 隔離垃圾郵件 239

關於隔離垃圾郵件 239
使用垃圾郵件隔離所之前 240
隔離已傳送至未解析電子郵件地址的垃圾郵件 240
關於瀏覽垃圾郵件隔離所 241
架構垃圾郵件隔離所設定 241
架構一般使用者隔離所 242
選擇垃圾郵件的語言編碼 244
修改「垃圾郵件隔離所」臨界值 245
指定垃圾郵件保留在隔離所的時間 246
指定垃圾郵件隔離所的清除時間與頻率 247

指定要通知誤報郵件的對象 247
檢視垃圾郵件隔離所中的郵件 248
管理員和使用者之垃圾郵件隔離所的差異 249
檢視隔離所中的垃圾郵件與可疑垃圾郵件 250
檢視傳送至郵件管理員信箱的垃圾郵件和可疑垃圾郵件 251
處理垃圾郵件隔離所中的郵件 251
指定垃圾郵件隔離所之郵件清單頁面上顯示的項目數 252
依日期排序隔離所中的垃圾郵件和可疑郵件 253
搜尋隔離的垃圾郵件 253
檢視垃圾郵件標頭 255
從隔離所釋放誤報的郵件 256
刪除隔離所中的垃圾郵件 256
指定通知使用者其隔離所中有垃圾郵件的時間 257
針對客戶特定規則，從「垃圾郵件隔離所」提交郵件 258
架構「垃圾郵件隔離所」通知 258
關於架構使用者與散布清單通知摘要 259
如何處理寄給散布清單的垃圾郵件 260
修改垃圾郵件通知郵件摘要範本 261
啟用散布清單的通知摘要 263
選取通知摘要格式 263
垃圾郵件隔離所疑難排解 264
大型部署的垃圾郵件隔離所最佳實務準則 266

第 13 章 參與 Symantec Probe Network 268

關於 Symantec Probe Network 268
關於探查帳戶 269
關於建立探查帳戶 269
設定探查帳戶 270
啟用探查參與 272
從無效收件者電子郵件地址建立探查帳戶 272
手動建立探查帳戶 273
啟用探查帳戶 274
停用探查帳戶 274
刪除探查帳戶 275

第 14 章 過濾內容 276

關於內容過濾 276
檢視、編輯、新增和管理內容過濾政策 277
建立內容過濾政策 278
定義內容過濾政策的條件 280
內容過濾政策條件的考量 281
內容過濾條件比對條件 283

在內容過濾政策條件中使用規則運算式 284
將動作新增至內容過濾政策 285
政策動作及其功能 285
修改 URL 以抵禦威脅和未經授權的存取 291
套用內容過濾政策至政策群組 296
測試內容過濾政策的提示 297
管理套用多個內容過濾政策的方式 298
郵件稽核日誌如何協助微調及疑難排解內容過濾政策 300

第 15 章 使用內容過濾資源來過濾內容 301

關於內容過濾政策資源 301
在內容過濾政策中使用結構化資料 302
關於您的資料來源檔案 304
建立結構化資料的記錄 306
將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位 307
上載資料來源檔案 312
複寫記錄 313
修改記錄 314
刪除記錄 315
關於記錄檢視 315
建立記錄檢視 318
編輯記錄檢視 318
刪除記錄檢視 319
處理內容過濾違規通知 320
關於政策違規通知 321
建立政策違規通知 321
編輯政策違規通知 323
刪除政策違規通知 324
使用辭典 324
關於內容過濾辭典 325
在非純文字檔案附件中掃描內容過濾違規 328
從辭典匯出單字或詞組 328
停用和啟用辭典中預先定義的單字或詞組 329
建立使用者定義的辭典 329
將單字或詞組匯入辭典中 330
編輯辭典 331
從辭典中刪除使用者定義的單字或詞組 331
尋找辭典中的單字或詞組 332
刪除辭典 332
高階與自訂內容過濾辭典 333
使用樣式偵測政策違規 337

關於樣式 338
建立您自己的自訂樣式 339
編輯樣式 340
刪除樣式 341
建立和管理政策違規的註釋 341
使用清單偵測禁止的附件 342
關於附件清單 343
建立偵測檔案附件類型的清單 351
編輯附件清單 353
刪除附件清單 354
Perl 相容規則運算式 354
指定封存郵件的儲存位置 356

第 16 章 處理內容過濾事件 358

架構內容事件資料夾 358
關於內容事件資料夾 359
關於管理內容事件資料夾的大小 360
建立內容事件資料夾 361
編輯內容事件資料夾 364
刪除內容事件資料夾 364
排程內容事件資料夾清除程式 365
架構郵件提交選項，使其顯示於隔離事件資料夾中 365
監控及因應事件 366
關於監控及因應事件 368
建立事件通知 368
關於從電子郵件通知補救事件 370
檢視內容事件資料夾中的事件 371
一次對多個事件執行動作 372
內容事件動作 372
封存事件 374
監控垃圾郵件提交 374
匯出事件的歷史記錄 378
轉寄事件 378
刪除事件 379
針對客戶特定規則，從隔離所資料夾提交郵件 380
補救已隔離的事件 381
更新事件的狀態 382
變更事件的嚴重性層級 382
檢視事件的歷史記錄 383
檢視違反內容過濾政策的文字 384
升級現有內容對相符文字功能的影響 385
使用 Symantec Content Encryption 加密資料 385

準備好系統以進行內容加密 386
管理內容加密的主機與通訊埠資訊 387
佈建內容加密帳戶 387
架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料 388

第 17 章 使用 Symantec Content Analysis 進行威脅防禦掃描 390

關於威脅防禦掃描 390
準備 Symantec Content Analysis 以連線至 Symantec Messaging Gateway 391
將 Symantec Messaging Gateway 連線至 Content Analysis 硬體裝置 392
架構威脅防禦掃描設定 392
從威脅防禦掃描中排除檔案類型 394
預設和範例威脅防禦政策 395
用於「內嵌」模式的預設威脅防禦政策 395
用於「監控」模式的範例威脅防禦政策 396
用於安全預覽的範例威脅防禦政策 397
建立新的威脅防禦政策集 398
選取用於政策群組的威脅防禦政策 400
檢視 Content Analysis 佇列 401

第 18 章 利用 Symantec Network Prevent 402

關於將 Symantec Data Loss Prevention 與 Symantec Messaging Gateway 整合 403
將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合 403
關於 Data Loss Prevention Network Prevent 406
Data Loss Prevention Network Prevent 整合所需的通訊埠 407
Symantec Messaging Gateway 與 Data Loss Prevention Network Prevent 如何互動 408
常用的 Data Loss Prevention Network Prevent 動作 409
支援的 Data Loss Prevention Network Prevent 傳送模式 410
關於 Data Loss Prevention Network Prevent 的故障行為 410
如何解決備份至 Symantec Network Prevent 的傳送佇列 411
啟用或停用 Data Loss Prevention Network Prevent 的略過 412
如何在啟用 Symantec Network Prevent 略過時，建立政策來偵測未經掃描的電子郵件 413
關於 Data Loss Prevention Network Prevent 報告 414
關於 Data Loss Prevention Network Prevent 整合會對效能造成的影響 414

關於 Data Loss Prevention Network Prevent 喜好設定順序 415
疑難排解 Data Loss Prevention Network Prevent 整合：郵件退回 416
Data Loss Prevention Network Prevent 整合疑難排解：延遲的郵件 416
如何架構 Symantec Network Prevent 將電子郵件傳回給 Symantec Messaging Gateway 417
架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線 417
根據 Symantec Network Prevent 標頭標記建立事件 419
關於讓 Data Loss Prevention Network Prevent 伺服器離線以進行維護 420

第 19 章 架構目錄資料整合 423

關於使用目錄資料服務 423
架構目錄資料整合 425
建立資料來源 426
新增資料來源 426
啟用新資料來源的功能 428
關於資料來源和功能 429
建立收件者驗證資料來源 430
建立驗證資料來源 431
建立繞送資料來源 434
建立位址解析資料來源 436
關於將驗證功能與資料來源搭配使用 437
關於搭配使用繞送功能與資料來源 438
關於搭配使用位址解析功能與資料來源 439
關於透過資料來源使用收件者驗證功能 439
關於資料來源查詢 440
建立和測試自訂的收件者驗證查詢 443
建立及測試自訂驗證與隔離所位址解析查詢 444
建立和測試自訂繞送查詢 448
建立和測試自訂位址解析查詢 450

第 20 章 管理目錄資料整合 454

展開散布清單和保留收件者地址 454
關於展開散布清單和保留收件者地址 455
啟用資料來源的散布清單展開 456
保留資料來源的收件者地址 456
修改現有資料來源 457
關於修改現有資料來源 458
停用或啟用資料來源 459
刪除資料來源 460

編輯資料來源 460
編輯資料來源的 LDAP 伺服器組態 461
啟用或編輯驗證功能 463
啟用或編輯位址解析功能 469
啟用或編輯繞送功能 472
啟用或編輯收件者驗證功能 474
編輯資料來源的進階設定 477
設定目錄資料快取 480
關於目錄資料快取 481
啟用快取持續性 481
關於預先載入目錄資料快取 482
預先載入資料快取 482
架構資料來源進階設定 484
安全性最佳實務準則 487
擴充性最佳實務準則 488
改善使用目錄資料服務時的訊息和系統負載 490
LDAP 連線疑難排解 491

第 21 章 報告 492

報告總覽 492
選取要為報告追蹤的資料 493
保留、刪除和清除報告資料 493
指定報告匯出設定 494
建立、儲存、以電子郵件傳送和列印報告 495
複製、編輯、排程和刪除我的最愛報告 496
將報告排程為自動產生 497
報告類型 498
疑難排解報告產生問題 509
產生的報告配置與資料 510

第 22 章 監控 Symantec Messaging Gateway 的狀態 515

關於監控系統狀態 515
使用儀表板 516
威脅類別元件 518
監控主機電腦和服務狀態 520
檢視硬體的相關資訊 520
檢視您的硬體狀態 521
檢視軟體和服務的狀態 521
軟體和服務狀態定義 522
監控日誌資料 524
關於日誌 525
日誌類型 526

檢視日誌檔 528
檢視控管中心錯誤日誌 529
儲存日誌檔 530
管理日誌資料庫大小 531
架構記錄層級 533
手動刪除日誌檔 535
關於記錄磁碟空間警示 535
清除磁碟空間檢查清單 536
監控遠端伺服器上的日誌 538
將遠端記錄架構為 syslog 538
傳送至遠端 syslog 之掃描程式日誌的標準字首 539
遠端 syslog 之 boot.log、cron、郵件和安全元件的日誌格式 540
遠端 syslog 之管道、Brightmail 用戶端、Brightmail 引擎和 JLU 控制器的日誌格式 540
遠端 syslog 之郵件傳輸代理程式的日誌格式 542
遠端 syslog 之郵件稽核日誌的日誌格式 542
處理郵件稽核日誌和郵件佇列 543
啟用郵件稽核日誌 545
搜尋郵件稽核日誌中的郵件 545
匯出郵件稽核日誌資料 549
關於郵件佇列 550
檢視佇列的郵件 550
重新繞送傳送佇列中的郵件 551
刪除佇列的郵件 552
停止郵件流 553
清除郵件佇列 554
監控郵件佇列大小和數量 554
疑難排解郵件佇列 555
監控已排程工作 555
關於已排程工作 556
已排程工作類型 556

第 23 章 透過控制中心管理產品 559

管理管理員 559
關於使用 LDAP 來源新增及授權管理員 560
關於預設管理政策 562
關於管理員和一般使用者檢視 564
設定本機和 LDAP 管理員帳戶 564
編輯管理員 572
刪除管理員 573
架構控管中心 573
架構控管中心設定 575

關於同時存取控管中心 575
關於指定可存取控管中心的主機名稱 576
指定哪些主機可以存取控管中心 576
架構 SNMP 設定以監控網路裝置 577
架構控管中心接聽程式通訊埠 578
存取控管中心時略過安全警告 579
指定控管中心憑證 580
設定地區設定編碼與遞補語言編碼 580
將 8 位元 MIME 郵件轉換為 7 位元 MIME 581
自訂日期格式與時間格式 581
自訂控管中心內的使用者喜好設定 583
指定自訂使用者登入說明頁面 584
讓使用者略過控管中心登入憑證 584
架構一般使用者喜好設定資料的複寫 585
設定 SMTP 問候語與郵件管理員地址 586
設定警示 586
警示類型 587
架構警示 590
設定已排程工作失敗警示 595
架構警示和報告的控管中心 SMTP 設定 595
管理密碼 596
重設管理員密碼 597
強制強式密碼 597
密碼最佳實務準則 598
強式密碼條件 599
硬體裝置維護 599
重新啟動硬體裝置 600
將硬體裝置重設為出廠預設值 600
架構 UPS 設定 601
從不同網路組態還原硬體裝置 602
關於維護足夠的磁碟空間 603
關閉硬體裝置 604
關於 Symantec Messaging Gateway 和 Symantec Protection Center 604
將 Symantec Messaging Gateway 與 Symantec Protection Center 整合 605
Symantec Protection Center 如何使用 Symantec Messaging Gateway 資料來強化報告 605
管理備份 606
排程備份 606
編輯排程的備份 608
刪除排程的備份 609
執行隨選備份 609

從備份還原硬體裝置 611
關於備份日誌資料 613
保持產品在最新狀態 613
授權您的產品 614
檢視授權狀態 615
取得更換授權檔 615
更新 Symantec Messaging Gateway 軟體 616
使用診斷 620
關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解 621
從控管中心執行網路公用程式 622
指定要包含於診斷套件中的內容 622
產生和下載診斷套件 623
產生診斷套件並將套件傳輸至遠端位置 625
刪除診斷套件 626

第 24 章 透過指令行管理 Symantec Messaging Gateway 627

透過指令行管理 Symantec Messaging Gateway 627
指令行介面存取方法 630

附錄 A 指令行參考 632

agent-config 634
cat 636
cc-config 637
clear 640
db-backup 641
db-restore 645
delete 647
diagnostics 652
dns-control 656
fipsmode 658
grep 659
help 660
ifconfig 666
iostat 667
ip 668
ldapsearch 669
list 670
mallog 672
malquery 674
monitor 679

more 685
mta-control 686
netstat 692
nslookup 693
password 694
patch 695
ping 697
ping6 698
reboot 699
route 700
rpmdb 701
rsa-金鑰 702
service 703
show 706
shutdown 707
sshd-config 708
symdiag 711
tail 712
telnet 715
traceroute 716
traceroute6 717
update 718

附錄 B 郵件過濾選項 720

來自多個判斷的動作組合 720
依判斷類別判斷 724
判斷組合 727
肯定與否定內容過濾規則條件範例 729

附錄 C 內容過濾範本 732

考爾迪科特報告政策範本 734
加拿大社會保險號碼政策範本 735
競爭對手通訊政策範本 735
機密文件政策範本 735
信用卡號碼政策範本 736
客戶資料保護政策範本 736
1998 年資料保護法政策範本 737
防禦郵件系統 (DMS) GENSER 分類政策範本 737
設計文件政策範本 738
員工資料保護政策範本 738
加密的資料政策範本 739
歐盟資料保護指令政策範本 739

出口管理條例規定 (EAR) 政策範本 739
財務資訊政策範本 740
賭博政策範本 740
金融服務法案 (Gramm-Leach-Bliley) 政策範本 740
HIPAA 政策範本 741
1998 年人權法政策範本 742
違禁藥品政策範本 743
美國報稅號碼 (ITIN) 政策範本 743
國際武器運輸條例規定 (ITAR) 政策範本 743
媒體檔政策範本 743
合併與收購資料政策範本 744
NASD 規定 2711 與 NYSE 規定 351 和 472 政策範本 744
NASD 規定 3010 與 NYSE 規定 342 政策範本 744
電業的 NERC 安全指導原則政策範本 745
網路圖政策範本 745
網路安全政策範本 745
攻擊性語言政策範本 746
海外資產控制局 (OFAC) 政策範本 746
密碼檔政策範本 746
付款卡產業資料安全標準政策範本 747
PIPEDA 政策範本 747
價格資訊政策範本 748
專案資料政策範本 748
出版文件政策範本 748
種族主義語言政策範本 748
限制的檔案政策範本 749
限制的收件者政策範本 749
履歷表政策範本 749
沙賓法案 (Sarbanes-Oxley) 政策範本 749
SEC 公平揭露規定政策範本 750
色情語言政策範本 750
原始程式碼政策範本 751
州資料隱密性政策範本 752
SWIFT 代碼政策範本 752
英國駕照號碼政策範本 753
英國選民登記號碼政策範本 753
英國國家保險號碼政策範本 753
英國護照號碼政策範本 753
英國稅務 ID 號碼政策範本 754
美國智慧型控制標記 (CAPCO) 及 DCID 1/7 政策範本 754
美國社會安全號碼政策範本 754
暴力與武器政策範本 755

附錄 D 使用 Dell Remote Access Controller 756

關於 Dell Remote Access Controller (DRAC) 卡 756
使用 DRAC 強制重新啟動 Symantec Messaging Gateway 硬體裝置 758
從 DRAC 正常重新啟動 Symantec Messaging Gateway 硬體裝置 758
使用 DRAC 從遠端安裝及架構 Symantec Messaging Gateway 硬體裝置 759
使用 DRAC 從虛擬媒體安裝 Symantec Messaging Gateway 影像 760
使用 DRAC 檢視 Dell 伺服器診斷 760
使用 DRAC 刪除 Symantec Messaging Gateway 硬體裝置的日誌、組態資訊和資料 761
使用 DRAC 將 Symantec Messaging Gateway 硬體裝置還原至原始出廠組態 761

附錄 E 聯邦資訊處理標準 (FIPS) 法規遵循 763

關於 Symantec Messaging Gateway FIPS 140-2 第 1 級標準遵循 763
關於使用 FIPS 模式時的安裝或升級 764
關於控管中心的憑證信任 765
FIPS 模式最佳實務準則與考量 765
關於使用 FIPS 時，部分 Symantec Messaging Gateway 的功能限制 766
開啟或關閉 FIPS 模式 767

附錄 F 適用於管理員的智慧卡驗證 769

關於適用於管理員的智慧卡驗證 769
在有 Internet 存取的情況下，對控制中心設定智慧卡驗證 770
在無 Internet 存取的情況下，對控制中心設定智慧卡驗證 771
匯入 CA 憑證或憑證撤銷清單 772
檢視 CA 憑證或憑證撤銷清單 773
刪除 CA 憑證或憑證撤銷清單 773
編輯管理員帳戶以啟用智慧卡驗證 774
使用智慧卡登入控制中心 774

小辭彙 776

索引 785

1

Symantec Messaging Gateway 簡介

本章包含以下主題：

- 關於 Symantec Messaging Gateway
- Symantec Messaging Gateway功能
- Symantec Messaging Gateway 的運作方式
- 關於預設政策與功能
- 哪裡可以獲得更多資訊

關於 Symantec Messaging Gateway

Symantec Messaging Gateway 可為企業提供入埠和離埠通訊安全性、即時垃圾郵件和病毒防護、進階內容過濾、威脅偵測和沙箱，以及資料外洩防護。

Symantec Messaging Gateway 會執行下列操作來保護您的環境：

- 偵測垃圾郵件、阻絕服務攻擊和其他入埠電子郵件威脅。
- 提供離埠寄件者流量管制，可抵禦受到感染的內部使用者的離埠垃圾郵件攻擊。
- 利用全域寄件者信譽和本機寄件者信譽分析 (包括以擴充的 URL 信譽為基礎的過濾)，透過限制不必要的連線來攔截垃圾郵件、惡意軟體及網路釣魚訊息，進而減少電子郵件基礎架構成本。
- 依政策過濾電子郵件以移除不必要的內容、示範法規遵循，以及防止透過電子郵件遺失智慧財產權和資料。
- 使用賽門鐵克「解除」技術，可偵測並移除許多常見電子郵件附件 (包括 Microsoft Office 文件和 Adobe PDF) 中的潛在惡意內容。潛在惡意內容類型包括巨集、程序檔、Flash 影片，以及其他易受攻擊的內容。「解除」會解構附件、刪除易受攻擊的內容，然後重建文

件並保留其視覺逼真度。您可以選擇要「解除」的文件類型和潛在惡意內容類型。您還可以選擇是否封存未經修改的原始文件，以防管理員或一般使用者需要存取它們。

- 讓您可以選擇透過對來自特定網域的入埠郵件強制執行 TLS 加密，使與信任夥伴和寄件者的通訊更加安全。
- 向 Symantec Data Loss Prevention 提供 TLS 加密的傳送，可提高將 Symantec Data Loss Prevention 與 Symantec Messaging Gateway 整合之客戶的安全性。
- 集成與Symantec內容分析提供先進的威脅偵測和虛擬sandboxing。
- 針對無法掃描的郵件提供精細的政策與判斷，以便您根據郵件無法掃描的原因來採取不同的行動。報告著重於無法掃描的郵件，可讓您隔離及解譯關於無法掃描的郵件和附件的統計資訊。
- 在儘量不造成管理負擔的狀況下透視訊息趨勢和事件。

請參閱第 23 頁的「Symantec Messaging Gateway功能」。

請參閱第 27 頁的「哪裡可以獲得更多資訊」。

Symantec Messaging Gateway功能

Symantec Messaging Gateway 可為企業提供入埠和離埠通訊安全性、即時垃圾郵件和病毒防護、進階內容過濾、威脅偵測和沙箱，以及資料外洩防護。在 Symantec Messaging Gateway 控管中心內，您可以自訂功能以滿足貴公司和您使用者的需求。

- 在閘道攔截不必要的電子郵件
  Symantec Messaging Gateway 提供數項功能，可讓您攔截電子郵件，使其無法進入網路。攔截不必要的電子郵件可讓您降低感染病毒的風險。您也可以減少掃描郵件所需的資源。
  請參閱第 122 頁的「關於連線時攔截與允許郵件」。
- 透過政策群組管理使用者
  您可以根據電子郵件地址、網域名稱或 LDAP 群組來指定使用者的群組， 然後對特定政策群組套用過濾政策。Symantec Messaging Gateway 安裝時，會一併安裝包含所有使用者的預設政策群組。
  請參閱第 161 頁的「關於政策群組」。
- 偵測垃圾郵件、可疑垃圾郵件及不必要的電子郵件
  Symantec Messaging Gateway 可以使用高水準的精確性，偵測垃圾郵件、可疑垃圾郵件及不必要的電子郵件。您可以定義和管理政策以處理垃圾郵件和不必要的電子郵件，並針對可疑的垃圾郵件設定臨界值。您甚至可以讓來自特定網域的訊息全都略過防垃圾郵件掃描。
  請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。
  在審核垃圾郵件前，先將垃圾郵件訊息攔截於垃圾郵件隔離所。如果您設定為使用者可存取垃圾郵件隔離所，收件者就會收到被隔離訊息的通知，然後採取適當的行動。
  請參閱第 239 頁的「關於隔離垃圾郵件」。

若要協助改善垃圾郵件過濾的成效，您可以選擇參與賽門鐵克的探測網路。
請參閱第 269 頁的「關於探查帳戶」。

- 啟用 DMARC、DK|IM、SPF 及寄件者 ID 驗證，以偵測具有偽造電子郵件地址或偽造標頭資訊的郵件。
  請參閱第 98 頁的章 4。
- 偵測惡意軟體與其他惡意攻擊
  您可以建立政策並架構設定，以偵測惡意軟體與其他惡意攻擊。
  請參閱第 176 頁的「關於偵測病毒、惡意軟體與惡意攻擊」。
- 發送電子郵件到 Symantec Content Analysis 伺服器，以偵測進階威脅。
  請參閱第 390 頁的「關於威脅防禦掃描」。
- 過濾郵件以強制執行內容政策
  您可以建立過濾入埠和離埠郵件內容的政策。此類政策可用來監控和強制執行對公司與法規要求的遵循，以及防止資料遺失。
  請參閱第 276 頁的「關於內容過濾」。
- 對入埠郵件強制執行 TLS 加密，可使與信任夥伴和寄件者的通訊更加安全。
  請參閱第 83 頁的「指定 TLS 通訊的 SSL 限制」。
- 修改內送郵件的 URL，以在收件者按下連結時將要求傳送給 Symantec 威脅隔離或 ProxySG。
  請參閱第 291 頁的「修改 URL 以抵禦威脅和未經授權的存取」。
- 監控效能
  控管中心包含可顯示整體系統狀態的儀表板。它提供有關入埠和離埠郵件對系統構成之威脅類型的統計資料。統計資料包含寄給無效收件者的郵件資料，或來自不良信譽位址的郵件資料， 也包括已觸發病毒、垃圾郵件與內容過濾政策的郵件數量。
  請參閱第 515 頁的「關於監控系統狀態」。
  Symantec Messaging Gateway 包含 50 多份相關報告，可提供來自所有掃描程式的關於內容過濾、電子郵件、IP 連線、垃圾郵件及病毒的統計資料。您可以視需要建立報告，或將報告架構為每天、每週或每個月以電子郵件傳送。
- 將您的惡意軟體定義檔維持在最新狀態
  您可以使用 LiveUpdate 自動更新防護。LiveUpdate 執行時，會下載和安裝任何可用的定義檔。
  請參閱第 198 頁的「關於更新病毒定義」。
- 配置Symantec Messaging Gateway自動地發送警示和通知關於疫情、系統問題和政策違規。
  請參閱第 587 頁的「警示類型」。
- 監控設備，配置並且管理掃描程式，並且管理軟體更新
  請參閱第 577 頁的「架構 SNMP 設定以監控網路裝置」。
  請參閱第 39 頁的「關於掃描程式電子郵件設定」。

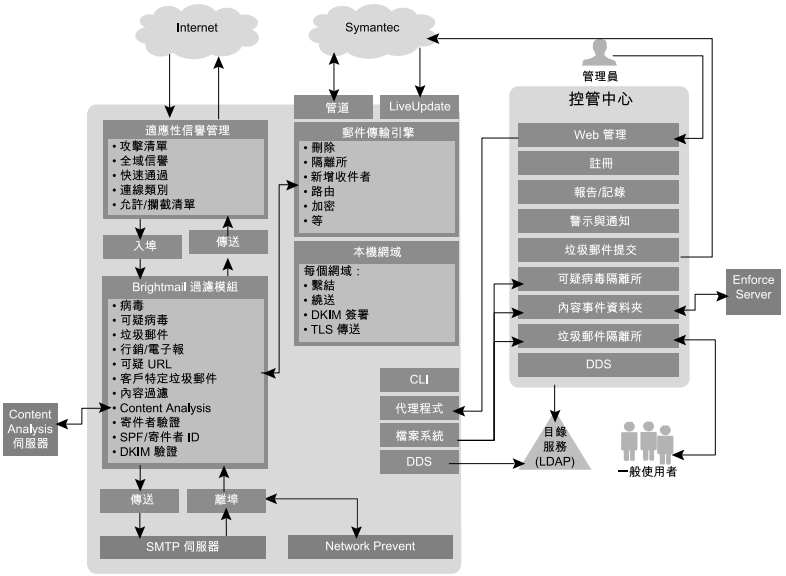
請參閱第 619 頁的「下載及安裝軟體更新」。

- 從指令行的架構Symantec Messaging Gateway。
  每部硬體裝置都具備一組指令，可讓您用來架構、最佳化和管理系統。若要存取這些指令，請透過 SSH、利用硬體裝置上的 VGA 或序列連線登入系統。

Symantec Messaging Gateway 的運作方式

圖 1-1 顯示 Symantec Messaging Gateway 如何處理電子郵件。此圖假設郵件會通過 Brightmail 過濾模組並傳送至郵件轉換引擎，而不會遭到拒絕。

圖 1-1 Symantec Messaging Gateway 架構



電子郵件訊息通過的路徑如下：

1. 郵件到達閘道時，全域信譽會判斷傳送 IP 是「允許的寄件者」還是「攔截的寄件者」，然後依據判斷結果，來接受或拒絕連線。
2. 「連線類別」會依據本機信譽，將傳送 IP 分類為 10 個類別的其中之一，並依據類別成員資格，來接受或延遲連線。
3. 在 MTA 接受郵件前，會先檢查網域位址與電子郵件地址。MTA 會判斷其是屬於「本機允許的寄件者網域」群組還是「本機攔截的寄件者網域」群組。如果屬於其中任一群組，則會對該郵件套用所架構的動作。適當的話，MTA 會將郵件移至入埠佇列中。
4. Brightmail 過濾模組會向目錄資料服務查詢，以增加郵件的散布清單，並判斷其所屬政策群組。

5. Brightmail 過濾模組會決定每個收件者的過濾政策。
6. 防毒過濾器會判定郵件是否受到感染。
7. 垃圾郵件過濾器會判斷郵件是垃圾郵件還是可疑垃圾郵件。
8. 不必要的郵件過濾器 (包括行銷電子報、重新導向 URL 和客戶特定垃圾郵件) 會判斷郵件是否為不必要的郵件。
9. 內容過濾政策過濾器會掃描郵件和附件是否含有限制的內容。
10. 威脅防禦政策將郵件傳送至 Symantec Content Analysis，以掃描郵件是否存在進階威脅，如果兩個系統已整合。
11. 郵件傳輸引擎會根據過濾結果和可架構的政策來執行動作，並依據所屬政策群阻，將它們套用至各個收件者的郵件。
12. 依據政策組態，可能將郵件保留在隔離所以供檢閱。您可以透過主控台或經由 Enforce Server 來補救內容事件資料夾中的郵件。
13. 接著郵件會插入至傳送佇列，等候由 MTA 進行傳送。

附註：Symantec Messaging Gateway 不會過濾任何不經過 SMTP 閘道的郵件。例如，不會過濾位於同一 Microsoft Exchange Server 上或 Exchange 組織內的信箱之間所傳送的郵件。

請參閱第 87 頁的「關於電子郵件訊息流」。

關於預設政策與功能

一旦安裝 Symantec Messaging Gateway，系統便立即可供使用。針對您的預設政策群組啟用一組政策以及一組功能。

政策群組是指您可為其指派過濾政策的使用者群組。Symantec Messaging Gateway 僅與包括所有使用者的預設政策群組一同安裝。會將每個垃圾郵件、惡意軟體或威脅防禦判斷的一個預設政策指派給預設群組。會提供垃圾郵件、惡意軟體和威脅防禦的其他範例政策供您使用。不會將這些其他政策指派給任何群組。

Symantec Messaging Gateway 不提供預設內容過濾政策。您可以使用預先定義的範本來建立內容過濾政策。

從**「管理」**>**「使用者」**>**「政策群組」**頁面，您可以建立其他政策群組，並為每個群組選擇一組政策。從**「垃圾郵件」**、**「惡意軟體」**、**「威脅防禦」**、**「內容」**和**「管理」**功能表，可建立其他過濾政策。您無法刪除預設政策群組或任一預設政策。

請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。

請參閱第 188 頁的「預設電子郵件惡意軟體政策」。

請參閱第 395 頁的「預設和範例威脅防禦政策」。

預設會啟用下列功能：

- 連線類別
- 允許的寄件者和攔截的寄件者群組
- 針對垃圾郵件、病毒以及其他威脅來過濾電子郵件
- 可疑垃圾郵件
- 將郵件保留在可疑病毒隔離所
- 郵件稽核日誌
- 選擇警示

安裝之後，依預設不會啟用下列功能：

- 垃圾郵件隔離所
- LDAP 目錄
- 快速通過
- 電子郵件地址搜尋攻擊防護
- 電子郵件病毒攻擊防護
- 退回攻擊防護
- 寄件者驗證，包括 SPF、寄件者 ID、DKIM
- SMTP 驗證
- TLS 加密
- 內容過濾
- 威脅防禦過濾
- 無效收件者處理
- 探查帳戶
- 為所有報告類型收集資料
- 所有警示類型

哪裡可以獲得更多資訊

下列資源提供與您的產品有關的詳細資訊。

文件

Symantec Messaging Gateway 文件集由下列手冊組成：

- *Symantec™ Messaging Gateway 10.6.3 管理指南*

- *Symantec™ Messaging Gateway 10.6 安裝指南*
- *Symantec™ Messaging Gateway 10.6 入門指南*
- *Symantec™ Messaging Gateway 10.6.3 指令行參考指南*
- *Symantec™ Messaging Gateway 10.6.3 版本說明*
- 「Symantec™ Messaging Gateway 10.6.3 軟體更新說明」

若要取得最新英文版本的 Symantec Messaging Gateway 文件，按下以下 URL，然後按下「文件」**連結**：

https://support.symantec.com/en_US/messaging-gateway.html

此網站提供有關 Symantec Messaging Gateway 的最佳實務準則、疑難排解資訊及其他資源。

產品說明系統

Symantec Messaging Gateway 內含完整的說明系統，其中包含概念性及程序性的資訊。

賽門鐵克網站

請造訪賽門鐵克網站，取得與您的產品有關的詳細資訊，如下所示：

- https://support.symantec.com/en_US/messaging-gateway.html
  提供您對技術支援知識庫、新聞群組、聯絡資訊、下載及郵寄清單訂閱的存取。
- https://licensing.symantec.com/acctmgmt/index.jsp
  提供有關註冊、常見問與答、如何回應錯誤訊息，以及如何聯絡「賽門鐵克授權管理」的相關資訊。
- www.symantec.com/zh/tw/business/index.jsp
  提供產品最新消息及更新。
- http://www.symantec.com/zh/tw/business/security_response/index.jsp
  提供您對病毒百科全書 (包含所有已知威脅、惡作劇程式的相關資訊，以及有關威脅之白皮書) 的存取。

2

部署掃描程式

本章包含以下主題：

- 關於掃描程式
- 設定掃描程式
- 新增掃描程式
- 驗證或變更掃描程式安裝設定
- 架構掃描程式電子郵件設定
- 架構 SMTP 進階設定
- 指定用於非閘道部署的內部郵件主機
- 修改掃描程式組態
- 啟用與停用掃描程式
- 停止和啟動掃描程式
- 刪除掃描程式
- 變更控管中心主機的 IP 位址
- 管理服務與 MTA 作業

關於掃描程式

掃描程式處理入埠和離埠郵件並繞送郵件，以進行傳送作業。掃描程式會從「賽門鐵克安全機制應變中心」下載病毒定義檔、垃圾郵件特徵，以及其他安全更新。掃描程式執行過濾、做出判斷，並依據適當的政策與設定，將動作套用到郵件。您可以架構掃描程式來限制連線數量，這有助於減少要掃描的郵件數量。

您可以執行下列任一工作來管理掃描程式：

- 新增掃描程式。
  請參閱第 32 頁的「新增掃描程式」。
- 修改掃描程式。
  請參閱第 59 頁的「修改掃描程式組態」。
- 啟用或停用掃描程式。
  請參閱第 59 頁的「啟用與停用掃描程式」。
- 停止和啟動掃描程式。
  請參閱第 60 頁的「停止和啟動掃描程式」。
- 刪除掃描程式。
  請參閱第 61 頁的「刪除掃描程式」。

您必須具備「完整的管理權限」或「管理設定」檢視權限，才能建立、修改、啟用、停用或刪除掃描程式。

關於 Symantec Messaging Gateway 中的 IPv6 位址

Symantec Messaging Gateway 可讓您使用 IPv6 位址來佈建部署中的任何主機。您必須至少先以一個 Symantec Messaging Gateway 可以用於控管中心和掃描程式間之通訊的主要 IPv4 位址來架構掃描程式。這個主要的 IPv4 位址是最初安裝硬體裝置時架構的。完成初始設定並架構好掃描程式或控管中心 (其中之一或兩者) 後，即可視需要執行 IPv6 位址。

如需詳細資訊，請參閱「Symantec Messaging Gateway 安裝指南」。

下列清單提供了您可以使用 IPv6 位址的實例：

- 啟用掃描程式及控管中心的 IPv6，並將 IPv6 位址新增至一或二個乙太網路介面。
  請參閱第 36 頁的「架構 IPv6 乙太網路設定及路由」。
- 新增 IPv6 位址和位址範圍以存取控管中心。
  請參閱第 576 頁的「關於指定可存取控管中心的主機名稱」。
- 如果啟用乙太網路介面的 IPv6，便可以將 IPv6 位址新增至 SMTP 組態。
  請參閱第 38 頁的「架構掃描程式電子郵件設定」。
- 如果啟用乙太網路介面的 IPv6，便可以將 IPv6 位址和位址範圍用於「內部郵件主機」。
  請參閱第 57 頁的「指定用於非閘道部署的內部郵件主機」。
- 在「允許的寄件者」清單和「攔截的寄件者」清單中使用 IPv6 位址。
  請參閱第 118 頁的「識別寄件者的支援方法」。
- 在執行信譽查閱時查詢 IPv6 位址。
  請參閱第 140 頁的「研究 IP 位址信譽」。
- 建立報告以傳回 IPv6 位址資訊或混合了 IPv4 和 IPv6 位址的資訊。
  請參閱第 495 頁的「建立、儲存、以電子郵件傳送和列印報告」。
- 檢視 IPv6 位址郵件稽核日誌。

請參閱第 545 頁的「搜尋郵件稽核日誌中的郵件」。

下列功能不支援 IPv6：

- 「連線類別」和「快速通過」會忽略 IPv6 位址並處理 IPv4 位址。
- 信譽檢查不會針對 IPv6 位址進行 DNS 式 IP 信譽檢查。
- 不支援 IPv6 位址的 SMTP 傳送。
- 不支援將 SMTP 驗證轉寄至 IPv6 驗證主機。
- LDAP、SNMP、DHA、NTP，以及病毒攻擊功能目前皆不使用 IPv6 位址。

設定掃描程式

表 2-1 架構掃描程式的程序

階段	動作	說明
階段 1	確認掃描程式組態。	安裝掃描程式軟體後，請檢閱您的組態。 請參閱第 33 頁的「指定 DNS 伺服器位址」。 請參閱第 33 頁的「驗證或變更主機上的時間設定」。 請參閱第 34 頁的「指定代理伺服器設定」。 請參閱第 35 頁的「架構 IPv4 乙太網路設定及路由」。
階段 2	架構掃描程式電子郵件接收設定及傳送設定。	架構掃描程式電子郵件設定。 請參閱第 40 頁的「架構郵件流方向」。 請參閱第 43 頁的「架構掃描程式入埠電子郵件傳送設定」。 請參閱第 46 頁的「架構掃描程式離埠郵件傳送設定」。 請參閱第 39 頁的「關於掃描程式電子郵件設定」。
階段 3	架構進階掃描程式 SMTP 設定。	架構進階掃描程式 SMTP 設定。 請參閱第 55 頁的「SMTP 進階驗證設定」。 請參閱第 49 頁的「SMTP 進階入埠設定」。 請參閱第 50 頁的「SMTP 進階離埠設定」。 請參閱第 52 頁的「SMTP 進階傳送設定」。 請參閱第 48 頁的「架構 SMTP 進階設定」。
階段 4	架構用於非閘道部署的內部郵件主機。	請參閱第 57 頁的「指定用於非閘道部署的內部郵件主機」。 請參閱第 58 頁的「內部郵件伺服器： 非閘道部署」。

新增掃描程式

您必須具有完整的管理權限或管理設定修改權限，才能新增掃描程式。新增掃描程式後，您可以檢查其狀態以確保能夠正常運作。

附註：如果已為您的訊息系統佈建內容加密，然後新增或變更掃描程式的 IP 位址，您必須通知您的賽門鐵克佈建代表。如需詳細資訊，請按下**「內容」>「設定」>「內容加密」**，然後按**「按下這裡」**以參閱「Symantec Content Encryption 佈建」頁面。

新增掃描程式

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 按下**「新增」**。

3 完成「新增掃描程式精靈」。

如需完成「新增掃描程式精靈」的相關資訊，請參閱「Symantec Messaging Gateway 安裝指南」。

驗證或變更掃描程式安裝設定

表 2-2 說明您可以驗證或變更的掃描程式安裝設定，以及您在安裝後可以自訂的其他設定。您可以視需要以任何順序執行這些工作。

表 2-2 掃描程式驗證安裝設定

工作	說明
指定 DNS 伺服器位址。	指定掃描程式所使用的 DNS 伺服器的 IP 位址，而且您可以在安裝之後變更 IP 位址。 請參閱第 33 頁的「指定 DNS 伺服器位址」。
驗證時間設定。	您可以指定主要、次要和第三級網路時間通訊協定 (NTP) 時間伺服器，也可以手動指定時間。 請參閱第 33 頁的「驗證或變更主機上的時間設定」。
指定代理伺服器設定。	如果您使用代理伺服器主機，則必須將代理伺服器資訊新增到您的掃描程式定義中。 請參閱第 34 頁的「指定代理伺服器設定」。
架構乙太網路設定及路由。	您可以自訂掃描程式的乙太網路設定，以符合網站的郵件流量需求。 請參閱第 35 頁的「架構 IPv4 乙太網路設定及路由」。

指定 DNS 伺服器位址

網域名稱系統 (DNS) 伺服器會將網域名稱轉譯為 IP 位址。指定掃描程式在安裝過程中所使用的 DNS 伺服器的 IP 位址，而且您可以在安裝之後變更 IP 位址。如果您的掃描程式會進行電子郵件掃描，則您指定的 DNS 伺服器將會用於傳送電子郵件。

附註：為了讓 DNS 伺服器正常運作，防火牆通訊埠 53 必須開啟。

您必須具有「完整的管理」權限或「管理設定」修改權限，才能新增或修改 DNS 伺服器設定。

指定 DNS 伺服器位址

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 按下您要修改 DNS 定義的主機名稱。
3. 在**「編輯主機組態」**頁面上，按下**「DNS/時間」**標籤。
4. 執行下列其中一項工作：

按下**「使用內部 DNS 伺服器」**。	若您需要覆寫預設 DNS 查詢通訊埠 53，請在**「查詢來源通訊埠」**欄位中輸入新的通訊埠號。
按下**「使用下列外部 DNS 伺服器」**，並輸入每個 DNS 伺服器的 IP 位址。	您最多可以指定三個外部 DNS 伺服器。 一開始，您指定的所有伺服器均擁有相同的優先度。Symantec Messaging Gateway 會查詢清單中的 DNS 伺服器、說明每個伺服器的來回行程時間 (RTT) 並開始偏好使用具有最低 RTT 值的 DNS 伺服器。如果該伺服器變慢或無回應，則系統會將 DNS 查詢繞送至清單中的下一個 RTT 最低的伺服器，以此類推。最後結果是主要 DNS 伺服器即是目前擁有最佳 RTT 效能的伺服器。 Symantec Messaging Gateway 僅支援 DNS 伺服器使用 IPv4 位址。不過，它支援這些 IPv4 DNS 伺服器使用 AAAA 記錄及 IPv6 反向 DNS 記錄。

若有需要，您也可以清除 DNS 伺服器或路由器的緩衝區。

5. 勾選**「套用上述設定至所有主機」**，將變更套用至所有主機。
6. 按下**「儲存」**。

請參閱第 29 頁的「關於掃描程式」。

驗證或變更主機上的時間設定

對於 Symantec Messaging Gateway 主機，您可以指定最多五個網路時間通訊協定 (NTP) 時間伺服器。賽門鐵克強烈建議您使用 NTP 時間伺服器，以管理您的主機上的時間設定。您也可以選擇手動設定時間。

您必須具有「完整的管理」權限或「管理設定」修改權限，才能架構時間設定。

架構時間設定

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 選取您要修改時間設定的主機名稱，然後按下**「編輯」**。

3 在**「編輯主機組態」**頁面上，按下**「DNS/時間」**標籤。

4 選取您要同步化時間的主機時區。

5 輸入 NTP 主機名稱或 IP 位址。

您可以指定最多五個 NTP 伺服器，也可以手動設定時間。

6 選用：按下**「套用上述設定至所有主機」**，將變更套用至所有主機。

7 按下**「儲存」**。

8 重新啟動電腦，讓時間變更生效。

指定代理伺服器設定

「管道」服務會在每個掃描程式上執行。透過管道，可以註冊您的授權、更新防垃圾郵件過濾器、下載新的病毒定義，以及執行軟體更新。如果您使用代理伺服器主機，則必須將代理伺服器資訊新增到您的掃描程式定義中。

代理伺服器錯誤將被記錄到警告記錄層級的 BrightmailLog.log。在架構代理存取之前，建議您使用指令 `cc-config cclog --level warnings` 來架構 BrightmailLog.log，以記錄警告層級的錯誤。如果代理伺服器主機在架構後無法運作，請檢查 BrightmailLog.log 中是否有錯誤。

表 2-3。

請參閱第 637 頁的cc-config。

表 2-3 可能的代理伺服器主機錯誤

問題	BrightmailLog.log 中的錯誤
代理伺服器主機需要使用者名稱和密碼，但兩者均未指定。	`IOException: Server returned HTTP response code: 407 for URL:`
為代理伺服器主機指定了錯誤的使用者名稱或密碼。	`ProtocolException: Server redirected too many times`
為代理伺服器主機指定了錯誤的位址和通訊埠。	會發生各種逾時錯誤

附註：LiveUpdate 使用您為掃描程式定義的代理伺服器，以從賽門鐵克下載病毒定義。如果您從 LAN 主機下載病毒定義，則只有在已定義代理伺服器時，LiveUpdate 才會使用代理伺服器。

請參閱第 201 頁的「指定要從哪個來源取得病毒定義」。

指定代理伺服器設定

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 在**「主機名稱」**下方，勾選您要為其指定代理伺服器的掃描程式名稱，然後按下**「編輯」**。
3. 在**「編輯主機組態」**頁面上，按下**「代理伺服器」**標籤。
4. 勾選**「使用代理伺服器」**。
5. 在**「代理伺服器主機名稱」**欄位中，輸入代理伺服器主機名稱。
6. 在**「代理伺服器主機通訊埠」**欄位中，輸入代理伺服器通訊埠號。
7. 視需要指定使用者名稱和密碼，以登入代理伺服器主機。
8. 按下**「儲存」**。

架構 IPv4 乙太網路設定及路由

掃描程式的 IPv4 位址乙太網路設定可以進行下列自訂，以符合網站郵件串流量需求：

- 架構掃描程式的乙太網路設定，並選擇啟用乙太網路介面來使用最多至 50 個的靜態路由。靜態路由能比動態路由更快將資料從一子網路導向至另一不同的子網路。如果位址變更，靜態路由也必須更新。
- 視需要新增或刪除乙太網路介面的虛擬 位址。
- 變更掃描程式的 IP 位址。

您必須具有「完整的管理」權限或「管理設定」修改權限，才能修改乙太網路設定。

若要架構 IPv4 位址乙太網路設定

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 在**「主機名稱」**下，勾選您要修改其乙太網路設定的掃描程式，然後按下**「編輯」**。
3. 在**「編輯主機組態」**頁面中，按下**「乙太網路」**標籤，然後按下**「IPv4」**標籤。
4. 視需要編輯乙太網路介面，輸入每一個乙太網路介面的 IP、網路遮罩、廣播及網路位址。

   視需要變更掃描程式或控管中心 IP 位址。您可以變更掃描程式或控管中心的 IP 位址。如果您變更控管中心的 IP 位址，之後請登入每個掃描程式的指令行介面。使用 `agent-config` 指令，重新允許從新的控管中心 IP 到掃描程式的安全連線。
5. 勾選**「啟用本介面」**可啟動第二個乙太網路介面。

   您可以指派第二個乙太網路介面來專責處理入埠或離埠流量。

6 視需要新增或刪除乙太網路介面的虛擬 IP 位址。

7 在「**繞送**」下的「**預設閘道**」欄位中，輸入預設閘道的 IP 位址。

預設閘道為必填。您必須以 IP 位址來表示它。

8 若要選擇定義靜態路由，請在「**靜態路由**」下方指定下列項目：

- 目的位址 - IP 位址、包含子網路遮罩的 IP 位址 (例如 128.113.1.0/255.255.255.0)，或 CIDR 標記法 (例如 192.30.250.00/18)
- 閘道位址 - IP 位址
- 介面—預設、乙太網路 1 或乙太網路 2

9 按下「**新增**」新增靜態路由。

您可以對每一乙太網路介面最多新增 50 個靜態路由。

10 按下「**儲存**」。

您可以將進階連線設定套用至所有位址。

請參閱第 37 頁的「架構進階乙太網路設定」。

您也可以架構您的乙太網路設定 IPv6 位址。

請參閱第 36 頁的「架構 IPv6 乙太網路設定及路由」。

架構 IPv6 乙太網路設定及路由

您可以自訂掃描程式及控管中心乙太網路設定以符合您的架構需求，其方法如下：

- 架構掃描程式的乙太網路設定，並選擇啟用乙太網路介面來使用最多至 50 個的靜態路由。靜態路由能比動態路由更快將資料從一子網路導向至另一不同的子網路。如果位址變更，靜態路由也必須更新。
- 變更掃描程式的 IPv4 位址，或建立 IPv6 位址。

您必須具有「完整的管理」權限或「管理設定」修改權限，才能修改乙太網路設定。您可以為乙太網路介面指派一或多個 IPv6 位址。

若要架構 IPv6 乙太網路設定及路由

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 在「**主機名稱**」下，勾選您要修改其乙太網路設定的掃描程式，然後按下「**編輯**」。

3 在「**編輯主機組態**」頁面中，按下「**乙太網路**」標籤，然後按下「**IPv6**」標籤。

4 勾選「**啟用 IPv6**」以啟用主機的 IPv6。

當您啟用 IPv6 時，必須架構至少一個 IPv6 位址和 IPv6 預設閘道。

5 視需要編輯乙太網路介面，提供每一個乙太網路介面的 IP 位址和字首。

您可以用任何標準 IPv6 格式指定個別的 IPv6 位址。位址會以縮寫格式儲存及顯示。位址範圍是以 CIDR 標記法表示，其組成包含位址部分和字首。

6 為其中一個或兩個介面提供 IP 位址**「字首」**。

IPv6 位址的字首值限制為 64 以下的整數值。

7 在**「繞送」**下的**「預設閘道」**欄位中，輸入預設閘道的 IP 位址。

預設閘道為必填。您必須以任何接受的 IPv6 格式指出其 IP 位址。

8 若要選擇定義靜態路由，請在**「靜態路由」**下方指定下列項目：

目的位址	您可以將標準 IPv6 格式使用於單一主機、範圍 CIDR 表示法，或是子網路遮罩。
閘道位址	IPv6 位址.
介面	預設、乙太網路 1 或乙太網路 2。

9 按下**「新增」**新增靜態路由。

您可以對每一乙太網路介面最多新增 50 個靜態路由。

10 按下**「儲存」**。

您可以將進階連線設定套用至所有位址。

請參閱第 37 頁的「架構進階乙太網路設定」。

架構進階乙太網路設定

使用下列程序，將進階連線資訊套用至所有已架構的 IPv4 和 IPv6 乙太網路設定和路由。

若要架構進階乙太網路設定

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 按下**「進階」**標籤以架構新乙太網路介面的設定。

3 為每個乙太網路介面勾選**「自動協議」**，或選取連線的速度，並指定連線的半雙工或全雙工操作。

4 如果您想要從閘道 CPU 將 TCP 分段卸載到乙太網路卡，請勾選**「分段」**。

請參閱第 35 頁的「架構 IPv4 乙太網路設定及路由」。

請參閱第 36 頁的「架構 IPv6 乙太網路設定及路由」。

架構掃描程式電子郵件設定

表 2-4說明可執行哪些工作來架構及修改掃描程式的入埠電子郵件設定和離埠電子郵件設定。您可以視需要以任何順序執行這些工作。

表 2-4 掃描程式電子郵件設定

工作	說明
在執行任何工作之前，請確定您已瞭解掃描程式電子郵件設定。	使用掃描程式電子郵件設定可以控制入埠和離埠郵件流的各種不同層面。您可以限制 Symantec Messaging Gateway 接受來自哪些 IP 位址的電子郵件， 也可以控制 Symantec Messaging Gateway 將過濾的電子郵件傳送至何處。 您可以透過架構個別的入埠與離埠掃描程式，來減少任何一個掃描程式所過濾的電子郵件數量。即使您只使用一個掃描程式來過濾入埠電子郵件與離埠電子郵件，也可以架構各種 SMTP 設定來控制郵件流。 請參閱第 39 頁的「關於掃描程式電子郵件設定」。
指定郵件流方向。	您可以指定是否要掃描程式過濾入埠電子郵件、離埠電子郵件或兩者。 請參閱第 40 頁的「架構郵件流方向」。
修改入埠郵件設定。	您可以變更掃描程式用來接受入埠郵件連線的 IP 位址或通訊埠號，或者新增 IPv6 位址。您也可以指定掃描程式是否接受入埠 TLS 加密的連線。 請參閱第 41 頁的「變更掃描程式入埠郵件設定」。
修改入埠郵件接收設定。	您可以將入埠連線限制為僅掃描程式用來過濾電子郵件的 IPv4 位址或 IPv6 位址，以節省掃描程式資源。透過僅允許來自特定 IP 位址與網域的連線，您就可以將所有其他入埠用戶端排除在連線時傳送郵件的範圍之外。 請參閱第 42 頁的「變更掃描程式入埠郵件接收設定」。
修改入埠電子郵件傳送設定。	掃描程式過濾入埠電子郵件之後，MTA 會將過濾的電子郵件轉遞到郵件伺服器中，以傳送給收件者。當您僅針對入埠或入埠與離埠組合掃描程式架構電子郵件傳送時，可以指定繞送已過濾入埠郵件的預設本機或非本機主機。 請參閱第 43 頁的「架構掃描程式入埠電子郵件傳送設定」。
修改離埠郵件設定。	您可以變更掃描程式用來接受離埠郵件連線的 IP 位址或通訊埠號，或者新增 IPv6 位址。您也可以指定掃描程式是否接受離埠 TLS 加密的連線。 請參閱第 44 頁的「變更掃描程式離埠郵件設定」。
修改離埠郵件接收設定。	您可以架構掃描程式，使其接受來自不限數量的郵件伺服器的離埠連線。透過僅允許來自特定 IPv4 位址或 IPv6 位址與網域的連線，您就可以將所有其他主機排除在連線時傳送郵件的範圍之外。 請參閱第 45 頁的「變更掃描程式離埠郵件接收設定」。

工作	說明
修改離埠郵件傳送設定。	離埠掃描程式會將過濾的電子郵件轉遞到本機或非本機的郵件伺服器，以傳送給收件者。針對僅離埠掃描程式或入埠與離埠組合的掃描程式架構電子郵件傳送時，請同時為本機和非本機郵件主機 (已過濾的離埠郵件在其中轉遞) 指定 IPv4 位址和通訊埠號。 請參閱第 46 頁的「架構掃描程式離埠郵件傳送設定」。
指定您要 Symantec Messaging Gateway 如何處理攔截的郵件。	Symantec Messaging Gateway 的攔截郵件處理功能可讓您指定系統掃描可能有格式錯誤之郵件的次數，然後再相應地將此郵件歸類。Symantec Messaging Gateway 接著就會將其放入攔截的郵件佇列。 請參閱第 48 頁的「架構錯誤郵件處理」。

關於掃描程式電子郵件設定

使用掃描程式電子郵件設定可以控制入埠和離埠郵件流的各種不同層面。您可以限制 Symantec Messaging Gateway 接受來自哪些 IP 位址的電子郵件， 也可以控制 Symantec Messaging Gateway 將過濾的電子郵件傳送至何處。

您可以透過架構個別的入埠與離埠掃描程式，來減少任何一個掃描程式所過濾的電子郵件數量。即使您只使用一個掃描程式來過濾入埠與離埠電子郵件，也可以架構各種 SMTP 設定來控制郵件流。

附註：個別的掃描程式電子郵件設定不應該與垃圾郵件或是病毒掃描設定混淆，因為該設定會控制所有掃描程式的垃圾郵件與病毒掃描活動。

在網站安裝期間，請至少架構一個結合的入埠與離埠掃描程式。此掃描程式可位於執行控管中心的同一台電腦上，也可位於其他電腦。您可以改為架構個別的入埠與離埠掃描程式，以便在不同的主機上執行，或是稍後新增專用的掃描程式。

附註：如果入埠和離埠電子郵件使用相同的 IP 位址和通訊埠，則掃描程式會使用離埠郵件接收設定來確定郵件為入埠還是離埠。掃描程式會先檢查離埠郵件接收設定。如果不接受郵件，掃描程式接下來會檢查入埠郵件接收設定。

請參閱第 45 頁的「變更掃描程式離埠郵件接收設定」。

「新增掃描程式精靈」將引導您完成架構掃描程式電子郵件設定的程序。這些初始電子郵件設定包括：

- 掃描程式角色 - 入埠電子郵件、離埠電子郵件或是入埠和離埠電子郵件。
- 郵件過濾 - 掃描程式 IP 位址與通訊埠號。
- 郵件接收 - 掃描程式接受要過濾之電子郵件的來源 IP 位址。

- 郵件傳送 - 轉遞過濾之電子郵件的目標郵件伺服器，以及是否要啟用「MX 查詢」。

請參閱第 32 頁的「新增掃描程式」。

將掃描程式新增至部署並加以測試之後，您可以透過下列方式進一步修改其設定：

- 變更掃描程式角色
  請參閱第 40 頁的「架構郵件流方向」。
- 修改掃描程式的入埠電子郵件設定
  請參閱第 41 頁的「變更掃描程式入埠郵件設定」。
  請參閱第 42 頁的「變更掃描程式入埠郵件接收設定」。
  請參閱第 43 頁的「架構掃描程式入埠電子郵件傳送設定」。
- 修改掃描程式的離埠電子郵件設定
  請參閱第 44 頁的「變更掃描程式離埠郵件設定」。
  請參閱第 45 頁的「變更掃描程式離埠郵件接收設定」。
  請參閱第 46 頁的「架構掃描程式離埠郵件傳送設定」。
- 架構進階 SMTP 設定
  請參閱第 48 頁的「架構 SMTP 進階設定」。

此外，「連線類別」會根據在每個掃描程式中所收集和實作的本機信譽資料，來延遲某些連線。

請參閱第 124 頁的「關於管理閘道的連線負載」。

架構郵件流方向

您可以架構掃描程式以過濾入埠電子郵件、離埠電子郵件，或者入埠與離埠電子郵件。

架構掃描程式的郵件流方向

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 在**「主機組態」**頁面上，按下要定義之掃描程式旁的方塊，然後按下**「編輯」**。
3. 在**「編輯主機組態」**頁面上，按下 **SMTP** 標籤。
4. 在**「主機名稱」**欄位中，視需要修改掃描程式的名稱，以透過其角色加以識別。
5. 在**「主機定義」**欄位中，修改掃描程式的定義，以反映其新角色。
6. 選取描述此掃描程式角色的選項。
   - 僅入埠郵件過濾 – 架構入埠 SMTP 掃描程式設定。
   - 僅離埠郵件過濾 – 架構離埠 SMTP 掃描程式設定。
   - 入埠和離埠郵件過濾 - 同時架構入埠與離埠 SMTP 掃描程式設定。

   請參閱第 39 頁的「關於掃描程式電子郵件設定」。

7 如果要將這些設定套用至所有掃描程式，請勾選位於頁面最下方的**「套用上述設定至所有主機」**。

8 按下**「儲存」**儲存您的變更。

在**「新增政策群組」**或**「編輯政策群組」**頁面上，您還必須針對每種過濾類型和郵件流方向啟用掃描。然後，您可以選擇要針對已啟用的郵件流方向套用的政策。Symantec Messaging Gateway 包含惡意軟體、威脅防禦、垃圾郵件及不想要的電子郵件的預設政策。這些預設政策會在安裝期間自動啟用並指派給所有使用者的**預設**政策群組。每個政策均包含可套用政策的郵件流方向。

您可以透過建立新政策群組來覆寫預設政策。

請參閱第 188 頁的「預設電子郵件惡意軟體政策」。

請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。

內容過濾沒有預設政策。郵件流方向已包含在 Symantec Messaging Gateway 提供的內容過濾範本內。

請參閱第 276 頁的「關於內容過濾」。

變更掃描程式入埠郵件設定

您可以變更掃描程式用來接受入埠郵件連線的 IP 位址或通訊埠號。您也可以指定掃描程式是否接受入埠 TLS 加密的連線。

變更掃描程式入埠郵件設定

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 在**「主機名稱」**下，勾選您要修改其設定之入埠掃描程式，然後按下**「編輯」**。

3 在**「編輯主機組態」**頁面上，按下 **SMTP** 標籤。

4 在**「入埠郵件 IP 位址」**下拉式功能表中選取您要接收入埠郵件的位址，然後在**「通訊埠」**文字方塊中輸入通訊埠號碼。

只有已針對此掃描程式的網路介面卡而架構的 IP 位址 (包括虛擬 IP 位址)，才會出現在下拉式功能表中。

5 如果啟用了 IPv6，則您可以在**「選用入埠郵件 IPv6 位址」**下拉式功能表中選取您要接收入埠郵件的 IPv6 位址，然後在**「通訊埠」**文字方塊中提供通訊埠號碼。

只有針對此掃描程式的網路介面卡架構的那些 IPv6 位址會顯示在下拉式功能表中。您可以用任何標準 IPv6 格式指定個別的 IPv6 位址。位址會以縮寫格式儲存及顯示。

6 如果您要主機使用 TLS 加密來接受連線，請勾選**「接受 TLS 加密」**。

如果您不勾選此選項，則 Symantec Messaging Gateway 不會在 SMTP 階段作業期間公告 TLS 加密的支援。

- 您必須先架構 MTA TLS 憑證並將其指派給此掃描程式，此掃描程式才能透過連線接受 TLS 加密的電子郵件。

請參閱第 159 頁的「指派 MTA TLS 憑證給掃描程式」。

- 「**通訊協定**」>**SMTP**>「**設定**」>**SMTP** 標籤上的「**SSL 限制**」設定會影響 Symantec Messaging Gateway 公告和支援的 TLS 版本。
  請參閱第 83 頁的「指定 TLS 通訊的 SSL 限制」。

7 從下拉式功能表中選取憑證名稱，以驗證掃描程式是否為可透過 TLS 加密的連線傳送給用戶端的信任來源。

請參閱第 145 頁的「關於憑證」。

8 如果要掃描程式先要求來自寄件者的 TLS 加密憑證再接受 TLS 加密的連線，請勾選「**要求用戶端憑證**」。

9 按下「**儲存**」以僅為此部主機儲存設定。

變更掃描程式入埠郵件接收設定

您可以將入埠連線限制為僅掃描程式用來過濾電子郵件的 IP 位址，以節省掃描程式資源。透過僅允許來自特定 IP 位址與網域的連線，您就可以將所有其他入埠用戶端排除在連線時傳送郵件的範圍之外。

警告：如果僅接受來自選取主機的郵件，且掃描程式沒有位於閘道，則必須新增所有的上游郵件伺服器。請在「**編輯主機組態頁面的 SMTP** 和「**內部郵件主機**」這兩個標籤上，新增上游郵件伺服器的 IPv4 和 IPv6 位址、CIDR 區塊或網路遮罩。Symantec Messaging Gateway 會拒絕來自未指定上游伺服器的電子郵件。

請參閱第 57 頁的「指定用於非閘道部署的內部郵件主機」。

變更掃描程式入埠郵件接收設定

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 在「**主機名稱**」下，勾選您要修改其設定的入埠掃描程式名稱，然後按下「**編輯**」。

3 在「**編輯主機組態**」頁面上，按下 **SMTP** 標籤。

4 選取下列其中一個選項：

接受來自所有 IP 位址的入埠郵件連線	如果您要掃描程式接受來自所有入埠郵件之寄件者的連線，請選取此選項。 繼續執行步驟 6。
僅接受來自以下 IP 位址的入埠郵件連線	如果您要掃描程式僅接受來自您在「**入埠郵件接收 IP 位址**」清單中勾選之位址的連線，請選取此選項。 接著在清單中勾選您要此掃描程式接受入埠郵件的來源 IP 位址。 繼續進行到下一步。

5 您也可以在「**入埠郵件接收**」下方，執行下列任何一項工作：

手動新增 IP 位址	按下「**新增**」，然後輸入您要過濾入埠電子郵件之來源本機網域的主機名稱、IPv4 位址或 IPv6 位址。 您可以用任何標準 IPv6 格式指定個別的 IPv6 位址。IPv6 位址會以縮寫格式儲存及顯示。範圍是以 CIDR 標記法表示，其組成包含位址部分和字首。
編輯 IP 位址	勾選您要變更設定之電子郵件用戶端的主機名稱或 IP 位址，接著按下「**編輯**」，然後進行所需的變更。
刪除一或多個 IP 位址	勾選您不再想要接受入埠連線的來源位址或網域，然後按下「**刪除**」，將它們從清單中刪除。 若要刪除所有現有的位址或網域，請按下「**全部刪除**」。
匯入 IP 位址	按下「**匯入**」，接著瀏覽至檔案位置，然後按下「**匯入**」。 您可以匯入以逗號、分號、空格和定位字元作為分隔字元的檔案。
匯出 IP 位址	按下「**匯出**」，然後指定匯出檔案的名稱及儲存該檔案的位置。

6 按下「**儲存**」或勾選「**套用上述設定至所有掃描程式**」，然後按下「**儲存**」。

架構掃描程式入埠電子郵件傳送設定

掃描程式過濾入埠電子郵件之後，MTA 會將過濾的電子郵件轉遞到郵件伺服器中，以傳送給收件者。當您僅針對入埠或入埠與離埠組合掃描程式架構電子郵件傳送時，可以指定應該繞送已過濾入埠郵件的預設本機或非本機主機。

您可以指定不限數目的本機或非本機郵件伺服器來傳送入埠郵件。如果您接受目的為其他網域的郵件，則多重下游郵件伺服器就能夠改善已過濾入埠電子郵件的負載散布與容錯。您必須指派喜好設定號碼給各個郵件主機，以指定預設轉遞 (靜態路由) 傳送入埠電子郵件的順序。掃描程式會嘗試先將電子郵件傳送到號碼較小的郵件主機。如果只架構一個郵件伺服器，則其喜好設定預設為 1。若要進行負載平衡，請為每部伺服器指定相同的喜好設定編號。

此外，您還可以將郵件伺服器指派給掃描程式用來接受入埠電子郵件的各個網域。每個郵件伺服器都可以托管多個本機網域。

請參閱第 70 頁的「關於電子郵件網域」。

您可以啟用使用主機名稱指定的任何郵件主機的 MX 查詢。然後，MX 查詢會決定要使用哪部伺服器，來傳送目的為本機網域收件者的電子郵件。

架構掃描程式入埠電子郵件傳送設定

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 在「**主機名稱**」下，勾選您要新增或編輯本機郵件伺服器的掃描程式，然後按下「**編輯**」。

3 在「**編輯主機組態**」頁面上，按下 **SMTP** 標籤。

4 在「**入埠本機郵件傳送**」下，勾選您要變更傳送資訊的本機主機，然後按下「**編輯**」。

或者，按下「**新增**」以新增關於本機郵件主機的傳送資訊。

您可以架構不限數目的本機郵件主機的入埠郵件傳送。

5 請在出現的文字方塊中輸入或修改 IP 位址與通訊埠號或主機名稱。

6 如果您要本機郵件主機使用 MX 查詢，以決定要使用哪個 IP 位址來傳送給電子郵件收件者，請勾選「**MX 查詢**」。

如果指定了一個主機名稱，就只能勾選「MX 查詢」。

7 如果您指定了多個主機，請在「**喜好設定**」欄位中輸入號碼。系統會嘗試先對號碼較小的伺服器進行連線。

8 如果掃描程式角色為「**入埠和離埠郵件過濾**」，請按下「**儲存**」來儲存設定，或勾選「**套用上述設定至所有主機**」，然後按下「**儲存**」。略過此程序的其餘部分。

9 如果掃描程式角色為「**僅入埠郵件過濾**」，請在「**入埠非本機郵件傳送**」下，按下其中一個選擇鈕：

- 「**為非本機郵件使用 MX 查詢**」可以在收件者網域上透過 MX 查詢，讓 Symantec Messaging Gateway 繞送非本機收件者的郵件。
- 「**轉遞非本機郵件至**」可指定郵件主機來傳送非本機郵件。

10 按下「**新增**」可以新增非本機郵件主機的主機名稱或 IP 位址和通訊埠號。

您可以架構不限數目的非本機郵件主機的入埠郵件傳送。

您可以勾選所要的非本機主機並按下「**編輯**」，然後在出現的文字方塊中修改 IP 位址和通訊埠號。

11 如果您要本機郵件主機使用 MX 查詢，以決定要使用哪個 IP 位址來傳送給電子郵件收件者，請勾選「**MX 查詢**」。

如果指定了一個主機名稱，就只能勾選「MX 查詢」。

12 如果您指定了多個主機，請在「**喜好設定**」欄位中輸入號碼。系統會嘗試先對號碼較小的伺服器進行連線。

13 按下「**儲存**」以儲存僅限入埠之掃描程式的傳送設定，或勾選「**套用上述設定至所有主機**」，然後按下「**儲存**」。

變更掃描程式離埠郵件設定

您可以變更掃描程式用來接受離埠郵件連線的 IP 位址或通訊埠號。您也可以指定掃描程式是否接受離埠 TLS 加密的連線。

變更掃描程式離埠郵件設定

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 在**「主機名稱」**下，按下您要修改其設定的離埠或入埠和離埠掃描程式的名稱，然後按下**「編輯」**。

3 在**「編輯主機組態」**頁面上，按下 **SMTP** 標籤。

4 在**「離埠郵件 IP 位址」**和**「通訊埠」**中，輸入要接收離埠郵件的 IP 位址和通訊埠號碼。

5 在**「選用離埠郵件 IPv6 位址」**和**「通訊埠」**中，選取要接收離埠郵件的選用 IPv6 位址並提供通訊埠號碼。

您可以用任何標準 IPv6 格式指定個別的 IPv6 位址。IPv6 位址會以縮寫格式儲存及顯示。

6 如果您要主機接受 TLS 加密的離埠連線，請勾選**「接受 TLS 加密」**。

- 您必須先架構 MTA TLS 憑證並將其指派給此掃描程式，才能接受 TLS 加密的離埠郵件進行過濾。
  請參閱第 159 頁的「指派 MTA TLS 憑證給掃描程式」。
- **「通訊協定」> SMTP >「設定」> SMTP** 標籤上的**「SSL 限制」**設定會影響 Symantec Messaging Gateway 接受的 TLS 版本。
  請參閱第 83 頁的「指定 TLS 通訊的 SSL 限制」。

7 從**「憑證」**下拉式功能表中選取憑證，以驗證掃描程式是否為可透過 TLS 加密的連線傳送給用戶端的信任來源。

請參閱第 145 頁的「關於憑證」。

8 按下**「儲存」**或勾選**「套用上述設定至所有主機」**，然後按下**「儲存」**。

變更掃描程式離埠郵件接收設定

您可以架構掃描程式，使其接受來自不限數量的郵件伺服器的離埠連線。透過僅允許來自特定 IP 位址與網域的連線，您就可以將所有其他主機排除在連線時傳送郵件的範圍之外。

附註：如果入埠和離埠電子郵件使用相同的 IP 位址和通訊埠，則掃描程式會使用離埠郵件接收設定來確定郵件為入埠還是離埠。掃描程式會先檢查離埠郵件接收設定。如果不接受郵件，掃描程式接下來會檢查入埠郵件接收設定。

請參閱第 44 頁的「變更掃描程式離埠郵件設定」。

變更掃描程式的離埠郵件接收設定

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 在**「主機名稱」**下，勾選您要修改其設定之離埠或是入埠與離埠掃描程式，然後按下**「編輯」**。

3 在「**編輯主機組態**」頁面上，按下 **SMTP** 標籤。

4 在「**離埠郵件接收**」下方，執行下列任何一項工作：

手動新增 IP 位址	按下「**新增**」，然後輸入您要過濾離埠電子郵件之來源本機網域的主機名稱、IPv4 位址或 IPv6 位址。 您可以使用 CIDR 標記法來輸入 IP 位址範圍。個別的 IPv6 位址會以任何標準 IPv6 格式指定，並以縮寫格式儲存及顯示。
編輯 IP 位址	勾選您要變更設定之電子郵件用戶端的主機名稱或 IP 位址，接著按下「**編輯**」，然後進行所需的變更。
刪除一或多個 IP 位址	勾選您不再用來接受離埠連線的來源位址或網域，然後按下「**刪除**」，將它們從清單中刪除。 若要刪除所有現有的位址或網域，請按下「**全部刪除**」。
匯入 IP 位址	按下「**匯入**」，接著瀏覽至檔案位置，然後按下「**匯入**」。 您可以匯入以逗號、分號、空格和定位字元作為分隔字元的檔案。
匯出 IP 位址	按下「**匯出**」，然後指定匯出檔案的名稱及儲存該檔案的位置。

5 按下「**儲存**」或勾選「**套用上述設定至所有掃描程式**」，然後按下「**儲存**」。

架構掃描程式離埠郵件傳送設定

離埠掃描程式會將過濾的電子郵件轉遞到本機或非本機的郵件伺服器，以傳送給收件者。僅針對離埠或入埠和離埠組合的掃描程式架構電子郵件傳送時，請同時為本機和非本機郵件主機 (已過濾的離埠郵件應在其中轉遞的主機) 提供 IP 位址和通訊埠號。

您可以指定多個郵件伺服器，將離埠電子郵件轉遞到 Internet 或網路中的下一個路由點。建議每個掃描程式最多有 3 個郵件伺服器。

架構掃描程式離埠郵件傳送設定

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 在「**主機組態**」頁面中的「**主機名稱**」下，勾選您要修改其設定的掃描程式名稱，然後按下「**編輯**」。

3 在「**編輯主機組態**」頁面上，按下 **SMTP** 標籤。

4 在「**郵件過濾**」下，選取「**僅離埠郵件過濾**」或「**入埠和離埠郵件過濾**」。

請參閱第 40 頁的「架構郵件流方向」。

5 按下「**離埠**」標籤。

如果您選擇「**入埠和離埠郵件過濾**」，請跳至步驟 10。

如果您選擇「**僅離埠郵件過濾**」，請移至下一步以架構「**離埠本機郵件傳送**」設定。

6 在**「將本機網域郵件轉遞至下列主機」**下，勾選本機主機，然後按下**「編輯」**。

或者，您可以按下**「新增」**以新增關於本機電子郵件主機的傳送資訊，或按下**「刪除」**以刪除主機。

7 在主機表格中，編輯郵件伺服器的**「主機」**(主機名稱或 IP 位址) 或**「通訊埠」**(號碼)，以便將過濾的離埠郵件傳送到這個郵件伺服器。

8 如果要啟用本主機的 MX 查詢，請勾選**「MX 查詢」**。

如果指定了一個主機名稱，就只能使用「MX 查詢」。

9 如果清單中有多個主機，請在**「喜好設定」**欄位中輸入每個主機的號碼。

- 將首先嘗試連線到喜好設定數字最小的主機。如果該主機不可用 (例如，所有連線均在使用中或存在硬體故障)，Symantec Messaging Gateway 將切換至下一個喜好設定數字最小的主機，但會在該主機變為可用時立即返回喜好設定數字較小的主機。
- 如果您將喜好設定值 1 指派給兩個主機，Symantec Messaging Gateway 會隨機挑選其中一個主機。如果該主機變為不可用，Symantec Messaging Gateway 將連線至喜好設定為 1 的另一個主機。如果該主機變為不可用，Symantec Messaging Gateway 將嘗試與第一個主機重新連線。僅當喜好設定為 1 的兩個主機都無法使用時，才會使用下一個喜好設定值最高的主機。

10 在**「離埠非本機郵件傳送」**下，按下列其中一個選項：

- **「為非本機網域郵件使用 MX 查詢」**可以在收件者網域上透過 MX 查詢，讓 Symantec Messaging Gateway 繞送非本機收件者的郵件。
  如果您選擇此選項，請跳至步驟 15。
- **「將非本機網域郵件轉遞至下列主機」**可指定郵件主機進行離埠電子郵件的非本機傳送。

11 在**「主機」**清單中，勾選要變更傳送資訊的非本機主機，然後按下**「編輯」**。

12 在主機表格中，編輯郵件伺服器的**「主機」**(主機名稱或 IP 位址) 或**「通訊埠」**(號碼)，以便將過濾的離埠郵件傳送到這個郵件伺服器。

或者，您可以按下**「新增」**以新增關於本機電子郵件主機的傳送資訊，或按下**「刪除」**以刪除主機。

13 如果要啟用本主機的 MX 查詢，請勾選**「MX 查詢」**。

如果指定了一個主機名稱，就只能使用「MX 查詢」。

14 如果清單中有多個主機，請在**「喜好設定」**欄位中輸入每個主機的號碼。如需喜好設定值的運作方式的說明，請參閱步驟 9。

15 按下**「儲存」**以儲存傳送設定，或勾選**「套用上述設定至所有掃描程式」**，然後按下**「儲存」**。

架構錯誤郵件處理

格式錯誤的電子郵件訊息造成 Brightmail 引擎失敗的情況很罕見。萬一發生此情況，Symantec Messaging Gateway 會將失敗時正在處理的少數郵件加以隔離，並逐一重新掃描這些郵件，直到找出造成失敗的郵件 (會造成 Brightmail 引擎再次失敗)。Brightmail 引擎會從這些失敗快速復原。郵件串流量不會中斷，也不會明顯延遲。偵測到錯誤郵件時，會傳送警示。

利用 Symantec Messaging Gateway 的錯誤郵件處理功能，您可以指定系統在將郵件分類為格式錯誤郵件並置於錯誤郵件佇列之前，掃描可能格式錯誤之郵件的次數。

附註：每次重試 (每次系統掃描格式錯誤的郵件時)，Brightmail 引擎都會失敗。設定此值時請特別小心。

然後，您可以使用 `mta-control` 指令行選項，存取及管理錯誤郵件佇列中的郵件。

確認郵件格式錯誤之後，在使用 `mta-control` 指令時您有如下幾個選項：

- 列出錯誤郵件佇列中的電子郵件
- 檢視或匯出郵件到指定 URL 或畫面
- 從錯誤郵件佇列中刪除郵件
- 略過 Brightmail 引擎並將郵件傳送給它的原始收件者
- 透過電子郵件將此郵件傳送給系統管理員
- 透過 Brightmail 引擎重新傳送郵件

請參閱第 627 頁的「透過指令行管理 Symantec Messaging Gateway」。

架構錯誤郵件處理

1. 按下**「通訊協定」> SMTP >「設定」**，然後按下**「內容掃描」**標籤。
2. 勾選**「啟用錯誤郵件處理」**。
3. 在 **「將郵件分類為錯誤之前的重試次數」** 欄位中輸入數值。
4. 按下**「儲存」**。

架構 SMTP 進階設定

指定 **MTA 主機名稱**可讓您定義 SMTP 對話初始期間的 HELO 橫幅。**MTA 主機名稱**也會出現在 Received 標頭中。這個主機名稱並不會連線到掃描程式的作業系統層級主機名稱。如果在**「編輯主機」**頁面上變更主機名稱，則 **MTA 主機名稱**不會變更。

架構 SMTP 進階設定

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 按下要架構且加上底線的主機名稱。

3 按下 **SMTP** 標籤。

4 捲動至頁面底部，然後按下**「進階設定」**。

5 進行所需的組態變更。

6 按下**「繼續」**。

7 在**「主機組態」**頁面上，按下**「儲存」**。

請參閱第 49 頁的「SMTP 進階入埠設定」。

請參閱第 50 頁的「SMTP 進階離埠設定」。

請參閱第 52 頁的「SMTP 進階傳送設定」。

請參閱第 54 頁的「傳送繫結的 SMTP 進階設定」。

請參閱第 55 頁的「SMTP 進階驗證設定」。

SMTP 進階入埠設定

表 2-5 描述您可以架構的入埠 SMTP 設定，以進一步定義掃描程式 SMTP 連線。

表 2-5 SMTP 進階設定 - 入埠組態

項目	說明
最大連線數目	設定最大的同時入埠連線數量。預設值為 2,000 個連線。
來自單一 IPv4 位址或 IPv6 範圍的連線數上限	設定可以來自單一 IPv4 位址或 IPv6 範圍的最大同時入埠連線數量。如果已啟用「連線類別」，則每個「連線類別」的設定都會覆寫 IPv4 寄件者的這個設定。 預設值為 20 個連線。
來自單一 IPv6 範圍的連線數上限的 IPv6 CIDR 字首	說明使用 IPv6 範圍時要使用的 CIDR 字首。 字首值必須是 0 到 128 之間的整數。預設值為 64。
來自單一 IP 位址的連線數上限	設定可以來自單一 IP 位址的最大同時入埠連線數量。預設值為 20。如果已啟用「連線類別」，則每個「連線類別」的設定都會覆寫此設定。
每封郵件的收件者數上限	設定郵件的最大收件者數量。預設值為 1,024 位收件者。
每個階段作業的郵件數量上限	指出單一階段作業所允許的電子郵件訊息數量上限。 如果您是從舊版升級，預設值為 0， 若為初次安裝，則預設值為 100。 如果已啟用「連線類別」，則會停用此欄位，且每個「連線類別」的設定都會覆寫此設定。

項目	說明
郵件大小上限 (以位元組為單位)	設定郵件在被拒絕之前的大小上限。預設值為 10,485,760 個位元組。
入埠佇列中的郵件數目上限	設定臨界值的上限。當達到或超過此臨界值時，將傳送警示 (若警示已啟用) 並延遲連線。預設值為 5,000 封郵件。
入埠佇列被佔滿時延遲新連線	當入埠佇列中的郵件數目超過上限時，會延遲郵件，並發出 SMTP 4xx 錯誤。如果取消勾選，只要資源允許，就會接受郵件。 請參閱第 555 頁的「疑難排解郵件佇列」。
在入埠郵件插入 RECEIVED 標頭	於入埠 SMTP 處理期間在郵件中置入 RECEIVED 標頭。
啟用反向 DNS 查詢	勾選時，可讓系統對 SMTP 用戶端的 IP 位址執行反向 DNS 查詢，將 IP 位址解析為名稱。預設為勾選。取消勾選時，將不會對入埠郵件執行反向 DNS 查詢。 **附註：**如果您在**「通訊協定」>SMTP >「設定」>SMTP** 標籤的**「DNS 驗證」**下啟用了全域反向 DNS 設定，將會覆寫此本機設定。 請參閱第 76 頁的「架構反向 DNS 驗證」。
階段作業逾時	此設定可控制 MTA 等候連線 MTA 之要求或回應的時間。如果超過此限制，硬體裝置即會中斷連線。

請參閱第 29 頁的「關於掃描程式」。

SMTP 進階離埠設定

表 2-6 描述您可以用來進一步定義 SMTP 組態的進階離埠 SMTP 設定。

表 2-6 SMTP 進階設定 - 離埠組態

項目	說明
最大連線數目	設定最大的同時離埠連線數量。預設值為 2,000 個連線。
來自單一 IPv4 位址或 IPv6 範圍的連線數上限	設定可以來自單一 IPv4 位址或 IPv6 範圍的最大同時離埠連線數量。 預設值為 20 個連線。
來自單一 IPv6 範圍的連線數上限的 IPv6 CIDR 字首	說明使用 IPv6 範圍時要使用的 CIDR 字首。 字首值必須是 0 到 128 之間的整數。預設值為 128。
來自單一 IP 位址的連線數上限	設定可以來自單一 IP 位址的最大同時離埠連線數量。預設值為 20 個連線。

項目	說明
郵件大小上限 (以位元組為單位)	設定郵件在被拒絕之前允許的最大大小。預設值為 10,485,760 個位元組。
每封郵件的收件者數上限	指出允許接收郵件的最大收件者數量。預設值為 1,024 位收件者。
每個階段作業的郵件數量上限	指出單一階段作業所允許的電子郵件訊息數量上限。 如果您是從舊版升級，預設值為 0， 若為初次安裝，則預設值為 100。
沒有網域的寄件者位址的預設網域	設定當郵件中找不到網域時所用的預設網域。
離埠佇列中的郵件數目上限	設定臨界值的上限。當達到或超過此臨界值時，將傳送警示 (若警示已啟用) 並延遲連線。預設值為 5,000 封郵件。
特定時間範圍內每個寄件者的離埠收件者數目上限	設定指定時間範圍內 (每分鐘或每小時)，寄件者最多可傳送郵件給多少個收件者。 預設值為 0。值 0 表示單一階段作業所允許的電子郵件訊息數量不限。
離埠佇列被佔滿時延遲新連線	當離埠佇列中的郵件數目超過上限時，會延遲郵件，並發出 SMTP 4xx 錯誤。如果取消勾選，只要資源允許，就會接受郵件。
插入 RECEIVED 標頭	勾選時，可於離埠 SMTP 處理期間在郵件中置入 RECEIVED 標頭。取消勾選時，則不會在離埠 SMTP 處理期間插入 RECEIVED 標頭。如果同時勾選此選項與**「刪除已存在的 RECEIVED 標頭」**，則郵件進入傳送佇列時仍會保留離埠 SMTP RECEIVED 標頭。
刪除已存在的 RECEIVED 標頭	勾選時，會移除離埠郵件的所有 RECEIVED 標頭。當標頭被移除時，就可能會因為其他 MTA 的設定而導致發生郵件來回傳送的情形。取消勾選時，訊息中的 RECEIVED 標頭在離埠處理期間仍會保留。同時勾選**「插入 RECEIVED 標頭」**與**「刪除已存在的 RECEIVED 標頭」**時，離埠 SMTP 處理的 RECEIVED 標頭仍會保留在郵件中。 **警告：**啟用此設定會降低您診斷郵件流問題的能力。

項目	說明
啟用反向 DNS 查詢	勾選時，可讓系統對 SMTP 用戶端的 IP 位址執行反向 DNS 查詢，將 IP 位址解析為名稱。預設為勾選。取消勾選時，將不會對離埠郵件執行反向 DNS 查詢。 **附註：**如果您在**「通訊協定」> SMTP >「設定」> SMTP** 標籤的**「DNS 驗證」**下啟用了全域反向 DNS 設定，將會覆寫此本機設定。 請參閱第 76 頁的「架構反向 DNS 驗證」。
階段作業逾時	此設定可控制 MTA 等候連線 MTA 之要求或回應的時間。如果超過此限制，硬體裝置即會中斷連線。

請參閱第 29 頁的「關於掃描程式」。

SMTP 進階傳送設定

表 2-7 描述您網站 SMTP 傳送組態郵件設定。

表 2-7 SMTP 進階設定 - 傳送組態

項目	說明
外部連線數上限	設定最大的同時外部連線數量。預設值為 100 個連線。
單一 IP 位址的外部連線數上限	設定可以來自單一 IP 位址的最大同時連線數量。預設值為 50 個連線。
所有內部郵件伺服器的連線數上限	設定可連到所有已定義之內部郵件伺服器的最大連線數量。預設值為 100 個內部郵件伺服器連線。
每個單一內部郵件伺服器的連線數上限	設定可連到一部內部郵件伺服器的最大連線數量。預設值為 50 個連線。
傳送佇列中的郵件數目上限	設定臨界值的上限。當達到或超過此臨界值時，將傳送警示 (若警示已啟用) 或延遲連線。預設值為 150,000 封郵件。
傳送佇列中每個郵件的收件者數目上限	指定批次傳送給多個收件者時，在傳送佇列中每個郵件所允許的收件者數目。如果郵件的收件者數目超過此值，則會分割郵件，直到每個郵件的收件者清單不再超過限制為止。 您可以輸入 1 到 1024 之間的值。預設值為 100。
連線的外寄郵件數上限	設定 MTA 透過單一連線可以傳送的郵件數的上限臨界值。設定為 0 會停用此限制。預設設定是 0。
傳送佇列被佔滿時延遲新連線	當傳送佇列中的郵件數目到達或超過上限時，會延遲郵件，並發出 SMTP 4xx 錯誤。如果取消勾選，只要資源允許，就會接受郵件。

項目	說明
最小重試間隔	設定 SMTP 伺服器在重新嘗試傳送郵件之前要等待的最小時間間隔。預設值為 15 分鐘。
最大重試間隔	設定 SMTP 伺服器在重新嘗試傳送郵件之前要等待的最大時間間隔。預設值為 7 小時。 請勿將此值設定為小於**「最小重試間隔」**的值。
已傳送郵件逾時時間	設定未傳送的郵件要在經過多久之後逾時並從佇列中被拒絕。預設值為 5 天。
退回郵件逾時時間	設定退回佇列中刪除郵件的逾時期間。在無法架構 LDAP 設定的環境中，這項設定會相當實用。預設值為 1 天。
通知前佇列中的郵件延遲時間	設定郵件在寄出未傳送通知之前在郵件佇列中等待的時間。預設值為 4 個小時。
嘗試對所有的郵件進行 TLS 加密	指示 MTA 嘗試對所有傳送的郵件進行 TLS 加密。 **附註：**如果您在**「通訊協定」> SMTP >「設定」> SMTP** 標籤上啟用「SSL 限制」，SMG 會嘗試僅使用支援的 TLS 通訊協定加密。 請參閱第 83 頁的「指定 TLS 通訊的 SSL 限制」。
提供 TLS 用戶端憑證	指示 MTA 提供為每一個 TLS 連線提供用戶端憑證。
連線逾時	等候連線系統呼叫回傳所需的時間長度 (以秒為單位)。預設值為 30 秒。
EHLO/HELO 逾時	等候 `EHLO` 或 `HELO` 指令回應所需的時間長度 (以秒為單位)。預設值為 5 分鐘。
MAIL FROM 逾時	等候 `MAIL FROM` 指令回應所需的時間長度 (以秒為單位)。預設值為 5 分鐘。
RCPT TO 逾時	等候 `RCPT TO` 指令回應所需的時間長度 (以秒為單位)。預設值為 5 分鐘。
DATA 逾時	在 CRLF.CRLF 終止 DATA 階段後，等待回應所需的時間長度 (以秒為單位)。此逾時相對較長，因為它是唯一涉及重要網路傳輸的傳輸階段。預設值為 10 分鐘。
RSET 逾時	等候 `RSET` 指令回應所需的時間長度。`RSET` 指令用於重設其中交易僅部分成功之 SMTP 階段作業的狀態。它允許當遠端伺服器短暫或永久回應失敗時，在成功完成傳送上一封郵件之前，立即先傳送單一 SMTP 階段作業中的所有後續郵件。預設值為 10 分鐘。
閒置逾時	當該網域目前沒有可傳送的郵件時，保持開啟閒置連線的時間長度 (以秒為單位)。預設值為 5 秒。

請參閱第 29 頁的「關於掃描程式」。

傳送繫結的 SMTP 進階設定

表 2-8 描述傳送繫結可用的設定。傳送繫結可讓您指定用來傳送郵件的 IP 位址。

您也可以針對非本機郵件設定網域特定的傳送繫結。對於每個本機網域，此功能可讓您定義一或多個 IP 位址 (透過其傳送來自該網域的郵件)。

表 2-9 描述了非本機郵件之每個網域傳送繫結的可用設定。

表 2-8 SMTP 進階設定 - 傳送繫結

項目	說明
本機郵件	設定本機傳送郵件的 IP 位址。 下拉式功能表為此掃描程式提供了 IP 位址的清單，您可從中選擇：入埠接聽程式 IP 位址、離埠接聽程式 IP 位址、所有虛擬位址或「自動」。如果您選擇「自動」，則 Symantec Messaging Gateway 會自動根據目前的流量來選擇最佳的路由。
非本機郵件	設定傳送非本機郵件的 IP 位址。 下拉式功能表為此掃描程式提供了 IP 位址的清單，您可從中選擇：入埠接聽程式 IP 位址、離埠接聽程式 IP 位址、所有虛擬位址或「自動」。如果您選擇「自動」，則 Symantec Messaging Gateway 會自動根據目前的流量來選擇最佳的路由。
作用中繞送的郵件	設定傳送郵件給非靜態路由的 IP 位址。 下拉式功能表為此掃描程式提供了 IP 位址的清單，您可從中選擇：入埠接聽程式 IP 位址、離埠接聽程式 IP 位址、所有虛擬位址或「自動」。如果您選擇「自動」，則 Symantec Messaging Gateway 會自動根據目前的流量來選擇最佳的路由。 **附註：**如果您使用多個 IP 位址，且已將系統佈建為進行內容加密，則必須將**「動態繞送的郵件」**設定為「自動」。 請參閱第 387 頁的「管理內容加密的主機與通訊埠資訊」。
目標為控管中心的郵件	設定 IP 位址，用於將郵件傳送到控管中心，以儲存到垃圾郵件隔離所、可疑病毒隔離所或內容事件資料夾。 下拉式功能表為此掃描程式提供了 IP 位址的清單，您可從中選擇：入埠接聽程式 IP 位址、離埠接聽程式 IP 位址、所有虛擬位址或「自動」。如果您選擇「自動」，則 Symantec Messaging Gateway 會自動根據目前的流量來選擇最佳的路由。

表 2-9 SMTP 進階設定 - 每一網域的非本機 SMTP 傳送繫結

項目	說明
網域	此清單包含已針對此掃描程式定義的所有本機或非本機網域。若要選取多個網域，請按住 Ctrl。
IP 位址	此清單包含此掃描程式上可用的所有 IP 位址。 若要選取多個 IP 位址，請按住 Ctrl。
新增	按下此項目可將選取的網域與 IP 位址組合新增至「網域/IP 位址」清單。透過選取多個網域或 IP 位址，您只要按一下便可新增多個列。
刪除	勾選「網域/IP 位址」清單中某列旁的方塊，然後按下**「刪除」**即可刪除該列。
全部刪除	按下此項目可刪除「網域/IP 位址」清單中的所有列，包括所有目前未顯示的列。
每頁的項目數	設定每頁顯示的項目數。
顯示	選取要顯示的項目範圍。
	移至項目的開頭。
	移至項目的上一頁。
	移至項目的下一頁。
	瀏覽至最後一頁的成員或第 51 頁 (如果超過 50 頁)。
網域/IP 位址清單	此清單中的每一列皆僅顯示一個網域和一個 IP 位址。您可以使用「新增」按鈕同時新增多個列。每個列皆會定義來自單一網域之非本機郵件的傳送繫結。

SMTP 進階驗證設定

表 2-10 說明您可用來進一步定義 SMTP 組態的進階驗證 SMTP 設定。

表 2-10 SMTP 進階設定 - SMTP 驗證組態

項目	說明
最大連線數目	設定最大的同時 SMTP 驗證連線數量。預設值為 2,000 個連線。

項目	說明
來自單一 IPv4 位址或 IPv6 範圍的連線數上限	設定可以來自單一 IPv4 位址或 IPv6 範圍的最大同時 SMTP 驗證連線數量。 預設值為 20 個連線。
來自單一 IPv6 範圍的連線數上限的 IPv6 CIDR 字首	說明使用 IPv6 範圍時要使用的 CIDR 字首。 字首值必須是 0 到 128 之間的整數。預設值為 64。
來自單一 IP 位址的連線數上限	設定可以來自單一 IP 位址的最大同時 SMTP 驗證連線數量。預設值為 20 個連線。
郵件大小上限 (以位元組為單位)	設定郵件在被拒絕之前允許的最大大小。預設值為 10,485,760 個位元組。
每封郵件的收件者數上限	指出允許接收郵件的最大收件者數量。預設值為 1,024 位收件者。
每個階段作業的郵件數量上限	指出單一階段作業所允許的電子郵件訊息數量上限。 預設值為 100。
插入 RECEIVED 標頭	勾選時，會在離埠處理使用 SMTP 驗證傳送的郵件期間，在郵件中置入 RECEIVED 標頭。取消勾選時，則不會在離埠 SMTP 處理期間插入 RECEIVED 標頭。如果同時勾選此選項與**「刪除已存在的 RECEIVED 標頭」**，則郵件進入傳送佇列時仍會保留離埠 SMTP RECEIVED 標頭。
刪除 RECEIVED 標頭	勾選時，會移除使用 SMTP 驗證傳送之離埠郵件的所有 RECEIVED 標頭。當標頭被移除時，就可能會因為其他 MTA 的設定而導致發生郵件來回傳送的情形。取消勾選時，訊息中的 RECEIVED 標頭在離埠處理期間仍會保留。同時勾選**「插入 RECEIVED 標頭」**與**「刪除已存在的 RECEIVED 標頭」**時，離埠 SMTP 處理的 RECEIVED 標頭仍會保留在郵件中。 **警告：**啟用此設定會讓您無法診斷郵件流問題。
啟用反向 DNS 查詢	勾選時，可讓系統對 SMTP 用戶端的 IP 位址執行反向 DNS 查詢，將 IP 位址解析為名稱。預設為勾選。取消勾選時，將不會針對使用 SMTP 驗證傳送的離埠郵件執行反向 DNS 查詢。 **附註：**如果您在**「通訊協定」> SMTP >「設定」> SMTP** 標籤的**「DNS 驗證」**下啟用了全域反向 DNS 設定，將會覆寫此本機設定。 請參閱第 76 頁的「架構反向 DNS 驗證」。
啟用選用的 SASL 一般支援	Symantec Messaging Gateway 預設會使用 SASL 登入驗證。您也可以選擇啟用 SASL 一般驗證。 如需詳細資訊，請參閱下列 RFC： 4954 4616

項目	說明
階段作業逾時	此設定可控制 MTA 等候連線 MTA 之要求或回應的時間。如果超過此限制，硬體裝置即會中斷連線。預設值為 30 秒。

附註：SMTP 驗證接聽程式會使用離埠郵件佇列，並沿用離埠接聽程式的某些行為。

請參閱第 29 頁的「關於掃描程式」。

指定用於非閘道部署的內部郵件主機

內部郵件主機是指郵件傳輸代理程式 (MTA)，它們會將電子郵件從 Internet 傳送至掃描程式。如果您的掃描程式位於 Internet 閘道，則不需要指定內部郵件主機。然而，如果您的網路已架構為在掃描程式的上游位置有一或多個 MTA，用於處理入埠郵件流，則您必須將這些 MTA 的 IPv4 位址或 IPv6 位址指定為內部郵件主機。您可以指定 IPv6 位址作為位址或範圍。

若網路具有的 MTA 是在 Symantec Messaging Gateway 的上游，則基於下列理由，必須將這些 MTA 指定為內部郵件主機：

- 從上游 MTA 到掃描程式的電子郵件，有可能包含某些垃圾郵件。掃描程式會將所有外部電子郵件都看成來自閘道 MTA 的 IP 位址。如果已啟用「連線類別」，這可能會導致所有從 Internet 送達的電子郵件發生延遲。
- 掃描程式將無法判定寄件者的 IP 位址。符合 IP 位址 (例如「本機攔截的寄件者 IP」) 的寄件者群組，將不會正確運作。

除了可以新增的內部郵件主機之外，Symantec Messaging Gateway 還會顯示內部主機清單中的一系列 IP 位址範圍。

請遵循這些程序，新增或刪除永遠允許掃描程式從其中接收郵件的內部郵件主機。

新增內部郵件主機至允許的主機清單

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 勾選您要架構的掃描程式。
3. 按下**「編輯」**。
4. 按下**「內部郵件主機」**標籤。
5. 指定內部郵件主機的 IP 位址。

   您可以指定 IPv4 位址或 IPv6 位址。

   個別的 IPv6 位址可以用任何標準 IPv6 格式指定，並以縮寫格式儲存及顯示。範圍是以 CIDR 標記法表示，其組成包含位址部分和字首。

6 按下「**新增**」。

7 按下「**儲存**」儲存資訊。

刪除內部郵件主機

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 勾選所需架構的掃描程式。

3 按下「**編輯**」。

4 按下「**內部郵件主機**」標籤。

5 選取內部郵件主機。

6 按下「**刪除**」。

當您刪除任何預設的內部郵件主機時，將會顯示警告訊息。

7 按下「**儲存**」儲存資訊。

請參閱第 58 頁的「內部郵件伺服器： 非閘道部署」。

內部郵件伺服器： 非閘道部署

將 Symantec Messaging Gateway 部署在閘道後，它會取得內送郵件的實際或對等 IP 連線，然後與允許的寄件者群組和攔截的寄件者群組中的項目進行比對。若掃描程式部署在網路中的其他位置，例如在非內部郵件主機的閘道 MTA 的下游，Symantec Messaging Gateway 可能會將閘道伺服器的 IP 位址視為垃圾郵件的來源。您應該依據入埠郵件流，精確識別 Symantec Messaging Gateway 硬體裝置上游的所有內部郵件主機。

請參閱第 57 頁的「指定用於非閘道部署的內部郵件主機」。

除了可以新增的內部郵件主機之外，Symantec Messaging Gateway 還包括內部主機清單中的一系列 IP 位址範圍，如下所示：

- 0.0.0.0/255.0.0.0
- 10.0.0.0/255.0.0.0
- 127.0.0.0/255.0.0.0
- 169.254.0.0/255.255.0.0
- 172.16.0.0/255.240.0.0
- 192.168.0.0/255.255.0.0
- ::/128
- ::1/128
- fe80 ::/10
- fc00::/7

Symantec Messaging Gateway 在下列判斷中會排除內部郵件主機的 IP 位址：

- 本機允許的寄件者 IP
- 允許的第三方寄件者
- 本機攔截的寄件者 IP
- 攔截的第三方寄件者
- 電子郵件地址搜尋攻擊
- 賽門鐵克全域攔截的寄件者
- 賽門鐵克全域允許的寄件者
- 連線類別
- 電子郵件病毒攻擊
- 快速通過

修改掃描程式組態

您可以隨時修改掃描程式的組態。例如，您可以中斷郵件串流通或啟動不同的元件與服務。

您必須具有「完整的管理」權限或「管理設定」修改權限，才能修改掃描程式設定。

修改掃描程式組態

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 按下您要編輯之掃描程式的連結名稱。

3 針對主機或其所包含的元件與服務進行變更。

附註：如果您要為訊息系統佈建內容加密且稍後新增或變更掃描程式的 IP 位址，則必須通知您的賽門鐵克佈建代表。如需詳細資訊，請按下**「內容」>「設定」>「內容加密」**，然後再按**「按下這裡」**連結，以參閱「Symantec Content Encryption 佈建」頁面。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

請參閱第 32 頁的「新增掃描程式」。

請參閱第 39 頁的「關於掃描程式電子郵件設定」。

啟用與停用掃描程式

您可以停用或啟用掃描程式，或刪除掃描程式。當您停用掃描程式時，會停止掃描程式與控管中心之間的電子郵件、統計資料、日誌與組態資訊的流量。 掃描程式會停止處理郵件。 掃描

程式不傳送也不接收郵件。控管中心會停止將「垃圾郵件隔離所」郵件繞送給掃描程式。「郵件稽核日誌」查詢會忽略掃描程式。

停用或啟用掃描程式

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

此頁面會列出您的掃描程式。「已啟用」欄中出現黑色破折號表示掃描程式已停用。「已啟用」欄中出現綠色的勾號則表示掃描程式已啟用。

2 勾選您要變更的掃描程式。

3 按下**「啟用」**以啟用掃描程式，或按下**「停用」**以停用掃描程式。

停止和啟動掃描程式

您有時可能會想要停止掃描程式。例如，您可能會想要暫時停止郵件串流量，以疑難排解問題。在您解決問題之後，就可以重新啟動掃描程式。或者，您可能會想要停止掃描程式，以刪除該掃描程式。否則，您可能會遺失掃描程式電子郵件佇列中的電子郵件訊息。您必須具有「完整的管理」權限或「管理設定」修改權限，才能停止和啟動掃描程式。

賽門鐵克建議您先停止掃描程式，再刪除該掃描程式。掃描程式在停止時不會處理郵件。

附註：您無法停止正在執行控管中心的主機。

如果您想要永久停止或移除掃描程式，則可以刪除該掃描程式。

請參閱第 61 頁的「刪除掃描程式」。

附註：停止掃描程式的最佳程序可能會根據系統參數和郵件流特性而不同。您可以設計停止掃描程式的專屬程序，其設計視每個設定之影響而定。

請參閱第 65 頁的「MTA 與郵件佇列行為」。

請參閱第 63 頁的「服務與 MTA 作業」。

停止掃描程式

1 在控管中心內，按下**「管理」>「主機」>「組態」**。

2 按下想要停止的掃描程式。

3 按下**「不接受內送郵件」**。

4 按下**「儲存」**。

5 按下**「狀態」> SMTP >「郵件佇列」**。

6 在**「主機」**下拉式清單中，選擇掃描程式。

7 在「**佇列**」下拉式清單中，選擇佇列。

8 在「**清單**」下拉式清單中，按下「**全部**」。

或者，若要加快在數量較多的掃描程式上的處理速度，請改為按下「**最長可有 10 個位於佇列中**」。

9 按下「**顯示已過濾**」。

10 按下「**全部重新傳送**」。

11 針對其他佇列，重複步驟 7 - 10。

12 清空佇列中的郵件。

若要檢查郵件佇列狀態，請針對每個佇列重複步驟 7 - 9。

13 按下「**管理**」>「**主機**」>「**組態**」。

14 按下想要停止的掃描程式。

15 勾選 **MTA**，然後按下「**停止**」。

16 按下「**儲存**」儲存變更，並回到「**主機組態**」頁面。

17 勾選想要停止之掃描程式旁邊的方塊，然後按下「**停用**」。

「掃描程式」清單會進行更新，反映出您的變更。

啟動掃描程式

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 若要啟用目前為停用狀態的掃描程式，請勾選掃描程式旁邊的方塊，然後按下「**啟用**」。

您可以勾選多個方塊。

「掃描程式」清單會進行更新，反映出您的變更。

刪除掃描程式

當您刪除掃描程式時，會將掃描程式的服務從控管中心永久移除。賽門鐵克建議您先停止掃描程式，再刪除該掃描程式。否則，您可以釋放掃描程式電子郵件佇列中的電子郵件訊息。您可以刪除正在執行控管中心的主機。您必須具備「完整管理」權限或「管理設定」修改權限，才能刪除掃描程式。

刪除掃描程式之後，您就無法擷取或存取其組態設定。如果您不確定是否要刪除掃描程式，可先停止掃描程式。停止掃描程式時，該程式仍會存在，但不會再掃描郵件。

刪除掃描程式

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 勾選要刪除之掃描程式旁的方塊。

3 按下「**刪除**」。

請參閱第 60 頁的「停止和啟動掃描程式」。

請參閱第 59 頁的「啟用與停用掃描程式」。

變更控管中心主機的 IP 位址

如果您必須變更託管控管中心的硬體裝置 IP 位址，您必須先使用控管中心來變更控管中心主機的 IP 位址，然後從每一個掃描程式指令行介面執行 `agentconfig` 指令，以重新允許從新的控管中心主機 IP 到該掃描程式的連線。

請參閱第 35 頁的「架構 IPv4 乙太網路設定及路由」。

請參閱第 634 頁的agent-config。

管理服務與 MTA 作業

從**「服務」**標籤中，您可以使用下列程序來管理個別的掃描程式服務及 MTA 作業。

啟動和停止服務

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 按下要停止或啟動服務的掃描程式名稱。
3. 勾選要啟動或停止的服務。
4. 按下**「停止」**可停止執行中的服務，按下**「啟動」**可啟動已停止的服務。

管理掃描程式的 MTA 作業

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 按下要變更的掃描程式名稱。
3. 在這個頁面的「MTA 作業」部分上，執行下列其中一項動作：

   若要暫停郵件傳送，請按下**「暫停郵件掃描和傳送」**。入埠和離埠郵件會放在佇列中，供未來掃描及傳送。

   若要拒絕傳入的郵件，請勾選**「不接受內送郵件」**。會掃描及傳送目前在郵件佇列中的所有郵件，但會拒絕所有新的郵件。

   若要還原正常運作，請按下**「照常接受和傳送郵件」**。
4. 按下**「儲存」**儲存您的變更。

請參閱第 65 頁的「MTA 與郵件佇列行為」。

請參閱第 63 頁的「服務與 MTA 作業」。

請參閱第 64 頁的「掃描程式服務」。

服務與 MTA 作業

表 2-11 列出各種設定，您可以使用這些設定來啟動或停止服務、檢視服務狀態及架構 MTA 作業。

表 2-11 「編輯主機組態」頁面 -「服務」標籤

項目	說明
啟動/停止	勾選「掃描程式服務」下服務名稱旁的方塊並按下「啟動」或「停止」，可讓您啟動或停止一或多個服務。 停止 MTA 服務將會停止入埠、離埠和傳送接聽程式。若要分別或依序停止一或多個接聽程式，請在**「狀態」> SMTP >「郵件佇列」**頁面上停止對應的郵件佇列。 **附註：**如果使用 SMTP 驗證，Symantec Messaging Gateway 會將其他的接聽程式用於驗證。此接聽程式由離埠接聽程式控制項來控制。如果停止離埠接聽程式，則驗證接聽程式也會停止。 請參閱第 65 頁的「MTA 與郵件佇列行為」。 **附註：**如果您停止了被架構為用於接收警示之主機上的 Brightmail 引擎或 MTA，但希望能繼續收到警示，請在**「管理」>「設定」>「控管中心」**頁面中的**「SMTP 主機」**下方，指定一個運作中的 MTA IP 位址。
掃描程式服務	列出可供所選取主機使用的掃描程式服務。包括： ■ **管道** ■ **LiveUpdate** ■ **Brightmail 引擎** ■ **MTA** ■ **目錄資料服務** 檢查您要對這個主機啟動或停止的服務名稱。勾選**「掃描程式服務」**以選取全部的服務。
狀態	指出特定服務在**「執行中」**(黑色)或**「已停止」**(紅色)。如果服務在過去 24 小時內曾經當機，則狀態底下會顯示紅色底線。將滑鼠放在紅色底線上，就可以檢視過去 24 小時內發生的當機次數。

項目	說明
MTA 作業	使用選擇鈕，決定主機如何處理郵件。選項有： ■ **照常接受和傳送郵件** - 依據已定義的政 來 理郵件。 ■ **暫停郵件掃描和傳送** - 接受入埠和離埠郵件；將郵件保留在佇列中，之後再掃描及傳送。如果您要在等待新病毒定義的同時暫停內送郵件，這個選項會很有幫助。 ■ **不接受內送郵件** - 拒絕內送郵件；郵件佇列中郵件的掃描及傳送會繼續進行。當您需要清空佇列，以便移除使用中的主機時，這個選項會很有幫助。拒絕郵件時，會傳送 `service not available` (450) 錯誤訊息給 SMTP 伺服器。一旦選取這個選項，系統會處理所有先前收到的郵件，但不會接受新的郵件。 請參閱第 65 頁的「MTA 與郵件佇列行為」。

掃描程式服務

使用**「服務」**標籤可架構掃描程式執行下列任何工作：

- 使用**「編輯主機組態」**頁面的**「服務」**標籤，可啟用或停用掃描程式的下列服務。每一部主機可執行幾項服務，並利用這些服務來與 Internet 及您網路上的其他伺服器進行通訊。

管道	透過安全 HTTPS 檔案傳輸，從賽門鐵克安全機制應變中心擷取全新和更新的電子郵件過濾器。「管道」會驗證過濾器，並警示 Brightmail 引擎有過濾器的存在。「管道」還管理可供賽門鐵克安全機制應變中心及 Symantec Messaging Gateway 用來編譯報告的統計資料。
LiveUpdate	從賽門鐵克安全機制應變中心自動下載病毒定義至掃描程式。此資訊是供掃描程式的 Brightmail 引擎使用，以識別已知的安全威脅。
Brightmail 引擎	掃描電子郵件、附件及檔案傳輸是否存在病毒和垃圾郵件，並根據您架構的過濾器政策進行內容過濾。
MTA	郵件傳輸代理程式會將入埠和離埠郵件繞送到 Brightmail 引擎進行處理，並將已過濾的郵件傳送到其內部目的地或 Internet。
目錄資料服務	使用目錄資料服務可以將儲存在輕量型目錄存取通訊協定 (LDAP) 目錄中的資訊，用於 Symantec Messaging Gateway 中的功能。

附註：如果您在一個已架構來接收警示的主機上停止了 Brightmail 引擎或 MTA 服務，則必須指定另一個主機來繼續接收警示。為避免中斷警示，在停止這些服務的任何一項之前，請修改控管中心的**「設定」**頁面 (**「管理」>「設定」>「控管中心」**) 上的**「SMTP 主機」與「通訊埠」**欄位。

請參閱第 62 頁的「管理服務與 MTA 作業」。

- 啟用、停用或暫停內送郵件掃描
  啟用掃描程式正常接受及傳送郵件是預設行為。不過，如果您必須使掃描程式離線，當您指派 MTA 作業給其他掃描程式時，可以分階段限制 MTA 作業。
  請參閱第 63 頁的「服務與 MTA 作業」。
  請參閱第 65 頁的「MTA 與郵件佇列行為」。

MTA 與郵件佇列行為

每個掃描程式都包含一個 MTA 與對應的郵件佇列： 入埠、離埠和傳送佇列。每個郵件佇列均由對應的接聽程式管理： 入埠、離埠和傳送佇列。在控管中心內，您可以對 MTA 和郵件佇列執行各種動作。

附註：如果使用 SMTP 驗證，Symantec Messaging Gateway 會將其他的接聽程式用於驗證。此接聽程式由離埠接聽程式控制項來控制。如果停止離埠接聽程式，則驗證接聽程式也會停止。

表 2-12 說明當您在**「管理」>「主機」>「組態」/「編輯」**頁面的**「服務」**標籤上執行特定動作時，新郵件與佇列中之郵件的預期行為。

表 2-12　在「編輯主機組態」頁面的「服務」標籤上管理 MTA 和郵件佇列

執行的動作	新郵件	佇列中的郵件	郵件傳送
按下**MTA**，然後按下**「停止」**。	不會被接受。不執行 MTA。外部 MTA 會將此視為 SMTP 4xx 錯誤。	不會被掃描、不會被傳送。	停止。
按下**「暫停郵件掃描和傳送」**。 **附註：**此動作相當於發出 `mta-control pause-mode pause-scan` 指令。	會被接受。	不會被掃描、不會被傳送。累積在入埠和離埠郵件佇列中。	停止。
按下**「不接受內送郵件」**。 **附註：**此動作相當於發出 `mta-control pause-mode pause-accept` 指令。	遭到拒絕，並發出 SMTP `service not available` (450) 錯誤訊息。	會被掃描和傳送。	繼續。

表 2-13 說明當您在**「狀態」> SMTP >「郵件佇列」**頁面上執行特定動作時，新郵件與佇列中之郵件的預期行為。

附註：表 2-13 中的每個動作只會影響一個郵件佇列。例如，停止入埠郵件佇列不會影響離埠或傳送郵件佇列。

表 2-13 在「郵件佇列」頁面上管理 MTA 和郵件佇列

執行的動作	新郵件	佇列中的郵件	郵件傳送
顯示郵件佇列，按下**「全部重新傳送」**。	會被接受。	重試任何由於傳送問題而延遲的郵件。	繼續。
顯示郵件佇列，按下**「全部刪除」**。	會被接受。	已刪除。	繼續。
顯示入埠郵件佇列，按下**「停止」**。	不會被接受。外部 MTA 會將此視為 SMTP 4xx 錯誤。	不會被掃描。	繼續。
顯示離埠郵件佇列，按下**「停止」**。	不會被接受。外部 MTA 會將此視為 SMTP 4xx 錯誤。	不會被掃描。	繼續。
顯示傳送郵件佇列，按下**「停止」**。	會被接受。	進行掃描，不進行傳送。累積在傳送郵件佇列中。	停止。

請參閱第 63 頁的「服務與 MTA 作業」。
請參閱第 64 頁的「掃描程式服務」。
請參閱第 604 頁的「關閉硬體裝置」。
請參閱第 550 頁的「關於郵件佇列」。

3

架構電子郵件設定值

本章包含以下主題：

- 架構電子郵件設定值
- 架構電子郵件網域
- 架構電子郵件別名和地址偽裝
- 指定 TLS 通訊的 SSL 限制
- 關於無效收件者
- 關於電子郵件訊息流
- 架構電子郵件進行 SMTP 驗證
- 指定地址驗證條件

架構電子郵件設定值

表 3-1 說明設定掃描程式的電子郵件設定的程序。

表 3-1 架構掃描程式電子郵件設定的程序

步驟	動作	說明
階段 1	設定網域。	瞭解電子郵件網域的運作方式。 確定適合您的網域組態。 請參閱第 70 頁的「關於電子郵件網域」。 請參閱第 71 頁的「新增或編輯網域」。 匯入網域的現有清單。 請參閱第 74 頁的「匯入網域清單」。 指定網域接受設定。 請參閱第 76 頁的「關於電子郵件網域接受設定」。
階段 2	架構電子郵件別名和地址偽裝。	瞭解別名和地址偽裝的運作方式。 請參閱第 78 頁的「關於別名與位址偽裝」。 對應每個別名的來源電子郵件地址及目的地。 請參閱第 79 頁的「新增或編輯別名」。 請參閱第 80 頁的「別名位址」。 匯入別名的現有清單。 請參閱第 79 頁的「匯入別名」。 新增、編輯和匯入地址偽裝。 請參閱第 81 頁的「新增或編輯位址偽裝」。 請參閱第 82 頁的「匯入位址偽裝清單」。
階段 3	架構無效收件者電子郵件處理。	IR 處理選項視您要啟用的功能而有所不同。請先確定需求，然後再指定 IR 處理。 請參閱第 85 頁的「關於無效收件者」。 指定希望系統如何處理無效受件者電子郵件。 請參閱第 86 頁的「設定無效的收件者處理」。
階段 4	瞭解 SMTP (簡易郵件傳輸通訊協定) 郵件流階段。	請參閱第 87 頁的「關於電子郵件訊息流」。 將郵件流階段用作指導方針，以建立和維護掃描程式電子郵件組態。 請參閱第 87 頁的「電子郵件訊息流階段」。

架構電子郵件網域

掃描程式的郵件處理需要根據您的電子郵件需求進行初始設定。例如，您可以指出接受入埠郵件的網域。

表 3-2說明在確定適當的網域組態後，可執行哪些工作來設定電子郵件網域。您可以視需要以任何順序執行這些工作。

表 3-2 使用電子郵件網域

工作	說明
深入瞭解電子郵件網域如何協助您做出使用這些網域的良好決策。	您必須將要 Symantec Messaging Gateway 接受入埠電子郵件的任何網域定義為本機網域。Symantec Messaging Gateway 僅接受要傳送至本機網域的入埠電子郵件。但是，送出電子郵件的網域可以是本機網域或非本機網域。 定義多個網域時，您可以將不同的路由與傳送選項指派給各個網域 (包括 TLS 加密)，以保護本機或非本機網域傳送的安全。為非本機網域架構 TLS 加密選項，您就可以保護由外部伺服器傳送之連線的安全。 請參閱第 70 頁的「關於電子郵件網域」。
新增或修改網域。	您必須將要 Symantec Messaging Gateway 接受入埠電子郵件的任何網域定義為本機網域。Symantec Messaging Gateway 僅接受要傳送至本機網域的入埠電子郵件。但是，送出電子郵件的網域可以是本機網域或非本機網域。 定義多個網域時，您可以將不同的路由與傳送選項指派給各個網域 (包括 TLS 加密)，以保護本機或非本機網域傳送的安全。為非本機網域架構 TLS 加密選項，您就可以保護由外部伺服器傳送之連線的安全。 架構個別的本機和非本機網域可提供您不同的繞送和傳送選項。 請參閱第 71 頁的「新增或編輯網域」。
匯入網域清單。	網域定義和電子郵件地址的清單，可從 ASCII 檔案 (類似 Sendmail mailertable) 中匯入。您可以納入選擇性路由資訊，讓預設本機目的主機可包含在定義內。 請參閱第 74 頁的「匯入網域清單」。
刪除不想再向其傳送電子郵件的網域。	刪除本機網域，表示 MTA 不再接受目的為該網域的入埠電子郵件訊息。刪除非本機網域，表示針對該網域架構的任何繞送或 TLS 選項都不再運作。 請參閱第 75 頁的「刪除網域」。
深入瞭解電子郵件網域接受設定。	在網站安裝期間，請至少指定一個本機網域供 Symantec Messaging Gateway 接受入埠電子郵件之用。您還需定義單一郵件主機，讓入埠掃描程式將要寄給本機網域的電子郵件繞送到此郵件主機。在網站安裝期間新增的任何網域都預設為本機網域，而且會將此靜態路由用作其預設轉遞，以傳送入埠電子郵件。 請參閱第 76 頁的「關於電子郵件網域接受設定」。

工作	說明
使用反向 DNS 作為另一種寄件者驗證形式。	反向 DNS 查詢會根據 IP 位址尋找網域名稱。由於反向 DNS 查詢可讓任何人檢視連線來源，因此許多攔截的寄件者並沒有反向 DNS 記錄，或是有虛假的反向 DNS 記錄。 請參閱第 76 頁的「架構反向 DNS 驗證」。

關於電子郵件網域

當入埠郵件到達掃描程式時，Symantec Messaging Gateway 會先驗證該郵件是否要傳送至有效的本機網域，然後再接受其進入適當的郵件佇列中。

您必須將要 Symantec Messaging Gateway 接受入埠電子郵件的任何網域定義為本機網域。Symantec Messaging Gateway 僅接受要傳送至本機網域的入埠電子郵件。但是，送出電子郵件的網域可以是本機網域或非本機網域。

定義多個網域時，您可以將不同的路由與傳送選項指派給各個網域 (包括 TLS 加密)，以保護本機或非本機網域傳送的安全。為非本機網域架構 TLS 加密選項，您就可以保護由外部伺服器傳送之連線的安全。

您也可以啟用本機或非本機網域的 DKIM 簽署，如此一來，從該網域傳送的每個郵件將會包含一個 DKIM 簽章，以透過接收 MTA 啟用 DKIM 驗證。

您也可以新增非本機網域。指定非本機網域，主要用來透過建立的連線，將離埠電子郵件繞送到外部伺服器，以進行非本機傳送。您也可以定義非本機網域的傳送選項。

Symantec Messaging Gateway 的多種功能都會使用網域的指定項目。

您可以新增或編輯網域，以執行下列動作：

- 為各個網域建立不同的電子郵件接受設定。
  請參閱第 76 頁的「關於電子郵件網域接受設定」。
- 為各個網域定義不同的傳送選項。
  您可以使用不限數目的預設轉遞，將已定址的入埠電子郵件繞送至不同的本機網域。
  您可以指定目錄資料繞送來源，以傳送目的為指定之非本機網域的電子郵件。
  傳送目的為非本機網域的電子郵件時，可使用 MX 查詢和 TLS 加密選項。
  請參閱第 71 頁的「新增或編輯網域」。
- 架構「收件者驗證」，根據您的 LDAP 目錄驗證內送電子郵件的收件者。
  請參閱第 85 頁的「關於無效收件者」。

附註：如果您打算從無效收件者電子郵件地址設定探查帳戶，您必須針對計畫使用探查帳戶的網域，勾選「啟用收件者驗證」。

請參閱第 272 頁的「從無效收件者電子郵件地址建立探查帳戶」。

- 架構靜態路由，可以將入埠或離埠電子郵件繞送到指定的郵件伺服器，以進行內部傳送。
  請參閱第 71 頁的「新增或編輯網域」。
- 架構非本機郵件的網域特有傳送繫結。這會讓您定義來自網域的郵件從哪一個或哪些 IP 位址傳送。
  請參閱第 54 頁的「傳送繫結的 SMTP 進階設定」。

您可以將網域清單匯入，稍後再個別編輯。

請參閱第 74 頁的「匯入網域清單」。

網域通常是指收件者電子郵件地址 @ 符號之後的部分。例如，anywhere.com 是 someone@anywhere.com 的網域。網域可以包含子網域。例如，somewhere.anywhere.com 是 anywhere.com 的子網域。或者，您可以將單一電子郵件地址指定為網域。

如果要將所有子網域包括在某個網域內，請在此網域前面輸入一個英文句點。例如，如果要將所有子網域包括在 example.com 內，請輸入 **.example.com**。但是，在網域前面輸入一個英文句點會忽略網域本身。例如，若要接受目的為 example.com 和 example.com 之所有子網域的電子郵件，您必須同時指定 **example.com** 和 **.example.com**。

如果您僅要將某些子網域包括在內，則必須分別指定各個子網域。例如，您必須同時將 **elsewhere.anywhere.com** 和 **somewhere.anywhere.com** 指定為單獨的網域，才能接受目的為 **overthere.anywhere.com** 除外之任一子網域的電子郵件。

附註：網域可以是完整網域名稱 (FQDN)、子網域，或 RFC5321 遵循的電子郵件地址。這些精細程度可讓您以最大程度地控制哪些位址是可接受的，以及要如何繞送目的為這些位址的電子郵件。

新增或編輯網域

本機網域是指 Symantec Messaging Gateway 接受入埠郵件的網域和電子郵件地址。在新增或編輯本機網域時，您可以針對從網域接受的郵件根據 MX 查詢、指定的主機或目錄資料來指定繞送行為，並啟用或停用收件者驗證。您也可以匯入本機網域的清單。

附註：如果已為您的訊息系統佈建內容加密，並新增網域或變更網域的位址，您必須通知您的賽門鐵克佈建代表。如需詳細資訊，請參閱「Symantec Content Encryption 佈建」頁面。按下**「內容」>「設定」>「內容加密」**，然後按下**「按下這裡」**。您還可能需要取代您的憑證或憑證組以納入網域。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

架構個別的本機和非本機網域可提供您不同的繞送和傳送選項。例如：

- 您可以使用不限數目的預設轉遞，將已定址的入埠電子郵件繞送至不同的本機網域。
- 您可以使用非本機預設轉遞來繞送傳送至非本機網域的離埠郵件，以便透過附屬公司或企業夥伴的外部郵件主機進行傳送。

- 您可以將目的為指定之非本機網域的離埠電子郵件，繞送至您專為機密通訊所保留的內部郵件伺服器。

非本機網域通常用來將離埠郵件繞送至您定期用來交換電子郵件的外部郵件主機。您也可以將目的為非本機網域的離埠電子郵件繞送至內部郵件主機。因為目的為非本機網域的電子郵件會先進行政策違規掃描，所以新增非本機網域可以為您提供選項，以安全地與企業夥伴或您自己組織的人員 (其網路位於獨立的防火牆之後) 交換郵件。

您可以架構新增的任何非本機網域，以執行下列動作：

- 將目的為非本機網域的離埠電子郵件靜態地繞送至任一郵件主機 (不限數量)，以進行非本機傳送。
  您可以選擇性地在任何定義靜態路由之非本機網域上啟用「MX 查詢」。賽門鐵克建議您啟用「MX 查詢」，以傳送至多部郵件主機。
- 針對指定的網域啟用 TLS 加密選項。

附註：透過編輯「網域」清單中的網域名稱來匯入網域之後，您可以為網域啟用繞送。

您也可以查詢繞送資料來源，以繞送目的為位於遠端網域之收件者的離埠電子郵件。

在網站安裝期間，您可以指定硬體裝置會接受其郵件的一或多個本機網域。您在網站安裝期間指定的任何網域預設都會是本機網域。當電子郵件要傳送至本機網域時，Symantec Messaging Gateway 只會接受來自寄件者 IP 的連線。進行處理之後，掃描程式會轉遞任何未違反政策條件的電子郵件，或對主控本機網域的郵件伺服器設定限制，以便將郵件傳送給收件者。

作為預設轉遞的郵件主機可主控多個本機網域。如果只針對本機網域指定一個郵件主機，則該主機會作為預設轉遞，負責傳送所有入埠郵件。您可以將不限數目的其他目的伺服器指定為預設轉遞，負責傳送目的為本機網域的入埠電子郵件。

在**「通訊協定」> SMTP >「網域」**頁面上，您可以：

- 新增您要 Symantec Messaging Gateway 接受入埠電子郵件的更多本機網域。
- 新增探查帳戶網域。
  如果您打算從未使用或無效的收件者電子郵件地址建立探查帳戶，則必須將探查帳戶網域新增至您的本機網域清單中。
  如果您打算從無效的收件者電子郵地址建立探查帳戶，您還必須為該網域啟用「收件者驗證」。
  請參閱第 270 頁的「設定探查帳戶」。
- 將目的為本機網域的入埠郵件限制為有效的收件者。
  Symantec Messaging Gateway 會先針對 LDAP 目錄資料檢查要傳送到指定本機網域之電子郵件的收件者，然後才會允許寄件者 IP 連線至入埠電子郵件介面的掃描程式。您必須架構適當的資料來源，啟用收件者驗證功能，並啟用「無效的收件者處理」以拒絕或棄置目的為無效收件者的入埠電子郵件。
- 針對個別網域定義不同的傳送選項。

新增或編輯網域

1 在控管中心內，按下**「通訊協定」> SMTP >「網域」**。

2 在「網域」頁面中，按下**「新增」**或按下您要編輯設定的網域名稱。

3 在**「接受入埠郵件的網域或電子郵件地址」**中，輸入本機網域、子網域或電子郵件地址，或編輯網域名稱。

在網域前放置英文句點 (.) 可讓 Symantec Messaging Gateway 接受所有子網域。

4 如果您要新增或編輯非本機網域，請取消選取**「本機網域」**核取方塊。

5 如果您希望使用 TLS 加密從該網域傳送郵件，請選取**「如果未使用 TLS 進行傳送，則拒絕來自此網域的郵件」**。

「通訊協定」> SMTP >「設定」> SMTP 標籤上的**「SSL 限制」**設定會影響 SMG 可用來加密來自此網域之郵件的 TLS 版本。

請參閱第 83 頁的「指定 TLS 通訊的 SSL 限制」。

6 如果您要拒絕或棄置無效的收件者，或如果您是探查帳戶參與者，請勾選**「啟用此網域的收件者驗證」**。

您無法啟用電子郵件地址或非本機網域的收件者驗證。

如果您要接受或拒絕無效的收件者電子郵件，則需要進一步的組態設定。

請參閱第 86 頁的「設定無效的收件者處理」。

7 若要定義此網域的傳送選項，請按下**「傳送」**標籤。

8 如果您要透過 MX 查詢繞送目的為此網域的郵件、透過主機型繞送或依目錄資料繞送目的為特定目的伺服器的郵件，請勾選**「選擇性地繞送此網域或電子郵件地址」**。

如果您不勾選此選項，會將郵件繞送至您在「編輯主機組態」頁面之 SMTP 標籤的「入埠本機郵件傳送」下架構的預設轉遞。

9 選擇下列其中一個選項：

- 按下**「MX 查詢」**可以將郵件繞送到使用 MX 查詢由收件者地址指定的主機。
  如果您指定完整網域名稱或電子郵件地址，則會在指定的網域，針對傳送給該網域收件者的郵件執行 MX 查詢。如果您指定子網域上層，則會根據收件者地址的完整網域名稱，針對傳送給指定上層網域之任一子網域中收件者的郵件執行 MX 查詢。
- 按下**「目的主機」**以指定一部或多部特定主機來繞送郵件，然後按下**「新增」**來新增每部主機。可以選擇為目的為此網域的郵件輸入要繞送至的通訊埠。您可以勾選**「MX 查詢」**為目的主機啟用 MX 查詢。如果您是使用 IP 位址指定主機，則無法使用 MX 查詢。輸入 1 到 100 之間的數字，在「喜好設定」下，指出應使用主機的順序。會先使用號碼較小的主機。
  請參閱第 46 頁的「架構掃描程式離埠郵件傳送設定」。
- 按下**「目錄資料來源」**，使用目錄型繞送來繞送郵件，以進行傳送解析。從其中的下拉式清單中，選擇 LDAP 繞送來源。

您必須對繞送定義 LDAP 目錄資料來源才能使用此選項。
請參閱第 426 頁的「建立資料來源」。
請參閱第 434 頁的「建立繞送資料來源」。

10 若要使用 TLS 加密將電子郵件傳送至非本機主機，請按下**「選用的傳送加密」**，然後按下最能描述此網域之 TLS 加密基礎的選擇鈕。

11 若要啟用此網域的 DKIM 簽署，請使用 DomainKeys Identified Mail 區段。

請參閱第 106 頁的「為網域啟用 DKIM 簽署」。

12 按下**「儲存」**，將網域、子網域或電子郵件地址新增至清單中，或確認編輯的內容。

匯入網域清單

網域定義和電子郵件地址的清單，可從 ASCII 檔案 (類似 Sendmail `mailertable`) 中匯入。作為定義的一部分，您可以將選擇性繞送資訊包括在預設本機目的主機。

匯入後，每個網域都在**「網域」**頁面的清單中出現。然後您可以視需要編輯任何網域。例如，如果您想要網域使用 TLS 加密或網域金鑰簽署，或者如果您想要將網域作為非本機網域使用，在匯入網域清單後您必須對其進行編輯。

附註：如果您要為訊息系統佈建內容加密且稍後新增網域，您必須通知您的賽門鐵克佈建代表。如需詳細資訊，請按下**「內容」>「設定」>「內容加密」**，然後按**「按下這裡」**，以參閱「Symantec Content Encryption 佈建」頁面。您可能也需要更新您的憑證以涵蓋新網域。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

附註：透過編輯「網域」清單中的網域名稱來匯入網域之後，您可以為網域新增目錄型路由。

請參閱第 71 頁的「新增或編輯網域」。

您也可以啟用匯入網域的收件者驗證。若要這麼做，您必須啟用「收件者驗證處理」，並架構用於收件者驗證的資料來源。

請參閱第 86 頁的「設定無效的收件者處理」。

請參閱第 430 頁的「建立收件者驗證資料來源」。

在匯入的檔案中，將各個網域定義個別放在一行中。網域定義包含下列以 Tab 分隔的屬性：

網域名稱	可以是完整的網域名稱、子網域名稱或電子郵件地址。若要在網域內包含所有子網域，請在網域名稱開頭加上英文句點。

目的地	包含目的地類型和目的主機名稱。僅支援目的地類型 (Mailer) 為 SMTP 或 ESMTP 的定義，而不支援 %backreferences。匯入後，ESMTP 目的地類型就會偽裝為 SMTP。當主機名稱以括號括住時 - smtp:[destination.domain.com] - 目的主機就不會執行 MX 查詢。
驗證	指出是否已針對網域啟用收件者驗證。這一欄中的 VALIDATE_RCPTS 值會啟用收件者驗證。其他任何值或沒有值則不會啟用收件者驗證。收件者驗證只能針對網域啟用。它無法針對電子郵件地址啟用。

匯入檔案的範例如下：

```
local1@domain.com  smtp:local1.com
local2@domain.com  smtp:local2.com:20
local3@domain.com  smtp:[local3.com]:30
local4@domain.com  smtp:[local4.com]
.local5.com        smtp:[192.168.248.105]
local6.com         smtp:[192.168.248.106]:60 VALIDATE_RCPTS
```

匯入本機網域的清單

1. 在控管中心內，按下**「通訊協定」> SMTP >「網域」**。
2. 按下**「匯入」**。
3. 在**「指定匯入檔案」**文字方塊中輸入檔名路徑，或瀏覽至含有網域定義清單的檔案。
4. 按下**「匯入」**。

   如果匯入檔案中的項目不符合必要的檔案格式，會出現含連結的錯誤訊息。按下連結，以下載含有未處理項目的檔案。

刪除網域

您可以刪除不想再傳送電子郵件的網域。刪除本機網域，表示 MTA 不再接受目的為該網域的入埠電子郵件訊息。刪除非本機網域，表示針對該網域架構的任何繞送或 TLS 選項都不再運作。

附註：如果刪除本機網域，任何與該網域關聯的探查帳戶將不再有效。請在刪除網域之前，先檢查作用中的探查帳戶。

請參閱第 71 頁的「新增或編輯網域」。

請參閱第 274 頁的「停用探查帳戶」。

刪除一個或多個網域

1 在控管中心內，按下**「通訊協定」> SMTP >「網域」**。

2 從「網域」清單中選取一個或多個網域，或按下**「全部刪除」**來刪除所有列出的網域。

3 按下**「刪除」**，只刪除所選取的網域。

關於電子郵件網域接受設定

在網站安裝期間，請至少指定一個本機網域供 Symantec Messaging Gateway 接受入埠電子郵件之用。您還需定義單一郵件主機，讓入埠掃描程式將要寄給本機網域的電子郵件繞送到此郵件主機。在網站安裝期間新增的任何網域都預設為本機網域，而且會將此靜態路由用作其預設轉遞，以傳送入埠電子郵件。

網站安裝完成之後，您就可以進一步架構入埠電子郵件網域接受，以執行下列動作：

- 拒絕或棄置目的為位於指定本機網域之無效收件者的電子郵件。
  請參閱第 85 頁的「關於無效收件者」。
- 偵測針對某網域導向的電子郵件地址搜尋攻擊。
  請參閱第 128 頁的「架構電子郵件地址搜尋攻擊辨識」。

您必須針對任何您要 Symantec Messaging Gateway 驗證收件者或偵測電子郵件地址搜尋攻擊的網域啟用收件者驗證。

透過架構 LDAP 收件者驗證設定檔，並依照各個網域啟用收件者驗證，您就可以將網域架構為驗證本機網域內的收件者地址。如果本機網域的收件者驗證已啟用，則 Symantec Messaging Gateway 會檢查資料來源，以確定電子郵件地址是否存在於 LDAP 目錄中。如果不符合，則會依照您網站對於處理無效收件者的設定，拒絕或棄置任何嘗試的連線。

請參閱第 86 頁的「設定無效的收件者處理」。

Symantec Messaging Gateway 會接受來自內部郵件主機的所有電子郵件。

請參閱第 45 頁的「變更掃描程式離埠郵件接收設定」。

架構反向 DNS 驗證

您可以使用反向 DNS 作為另一種寄件者驗證形式。反向 DNS 查詢會根據 IP 位址尋找網域名稱。由於反向 DNS 查詢可讓任何人檢視連線來源，因此許多攔截的寄件者並沒有反向 DNS 記錄，或是有虛假的反向 DNS 記錄。

請參閱第 69 頁的「架構電子郵件網域」。

架構反向 DNS 驗證

1 在控管中心內，按下**「通訊協定」> SMTP >「設定」**。

2 在 **SMTP** 標籤的**「DNS 驗證」**下，勾選下列任一選項：

- 拒絕連線 IP 位址不存在反向 DNS 記錄的連線

- 拒絕連線 IP 位址存在反向 DNS 記錄、但結果網域的 A 記錄或 AAAA 記錄與連線 IP 位址不相符的連線
- 拒絕網域提供於 HELO 和 EHLO、在 DNS 中不含 A 記錄、AAAA 記錄和 MX 記錄的連線
- 拒絕網域提供於 MAIL FROM 位址、在 DNS 中不含 A 記錄、AAAA 記錄和 MX 記錄的郵件

3 您也可以為您勾選的任何選項編輯「**拒絕郵件**」文字。

4 按下「**儲存**」。

架構電子郵件別名和地址偽裝

您可以架構電子郵件地址別名 (亦稱為散布清單) 及電子郵件地址偽裝。

表 3-3 說明可以對入埠郵件、離埠郵件或兩者如何執行地址偽裝。您可以視需要以任何順序執行這些工作。

表 3-3 電子郵件別名與位址偽裝

工作	說明
深入瞭解別名和位址偽裝。	別名會將電子郵件地址轉譯為一或多個目的位址。Windows 使用者可能都已瞭解「散布清單」這個概念。在輸入冗長的收件者清單時，您可以新增別名作為方便的捷徑。別名也可以將位址從一個最上層網域轉譯為另一個最上層網域。 位址偽裝是一種可以指定替代值給電子郵件地址或網域名稱，讓它們隱藏於電子郵件閘道背後的方法。 請參閱第 78 頁的「關於別名與位址偽裝」。
新增別名或修改現有別名。	針對您輸入的每個別名，指定一個 (且僅一個) 來源電子郵件地址或網域。 請參閱第 79 頁的「新增或編輯別名」。
匯入別名檔案。	別名可從文字檔案中匯入。 請參閱第 79 頁的「匯入別名」。
檢視別名來源和目的位址的範例。	您可以針對輸入為來源電子郵件地址的每個別名，輸入多個目的電子郵件地址。但是，對於輸入為來源網域的每個別名，則只能輸入單一目的網域。別名來源位址必須具有本機網域。目的網域可以是本機網域或非本機網域。 請參閱第 80 頁的「別名位址」。
新增位址偽裝或修改現有位址偽裝。	Symantec Messaging Gateway 可讓您針對入埠郵件及/或離埠郵件執行位址偽裝。 請參閱第 81 頁的「新增或編輯位址偽裝 」。

工作	說明
匯入位址偽裝檔案。	除了建立新的偽裝項目之外，您也可以從類似 Sendmail virtusertable 的文字檔案中匯入偽裝的項目。 請參閱第 82 頁的「匯入位址偽裝清單」。
將 Symantec Messaging Gateway 架構為忽略文字的大小寫。	啟用此選項時，MTA 會忽略位址偽裝、別名和探查帳戶中位址之本機部分的文字大小寫。 請參閱第 83 頁的「忽略本機位址中的文字大小寫」。

關於別名與位址偽裝

別名會將電子郵件地址轉譯為一或多個目的位址。Windows 使用者可能都已瞭解「散布清單」這個概念。在輸入冗長的收件者清單時，您可以新增別名作為方便的捷徑。別名也可以將位址從一個最上層網域轉譯為另一個最上層網域。 例如，您可以建立別名來源網域，以將 *example.com* 轉譯為目標網域 *example-internetsecurity.com*。然後，Symantec Messaging Gateway 會將傳送目的為 *someone@example.com* 的所有電子郵件傳送至 *someone@example-internetsecurity.com*。

位址偽裝是一種可以指定替代值給電子郵件地址或網域名稱，讓它們隱藏於電子郵件閘道背後的方法。 Symantec Messaging Gateway 可讓您針對入埠郵件及/或離埠郵件執行位址偽裝。位址偽裝通常用來隱藏內部郵件主機的名稱，讓外寄郵件看似來自不同於實際主機的網域。

離埠位址偽裝會變更郵件中顯示的寄件者。入埠位址偽裝會變更郵件中顯示的收件者。

只有對 Symantec Messaging Gateway 所處理的入埠或內部郵件才會進行別名翻譯。閘道允許電子郵件連線至入埠掃描程式之後，便會判斷 SMTP 信封 `To:` 欄位中的位址是否為別名，並在連線階段作業期間，將其轉譯為任何目的位址。轉換後的位址接著會寫回 SMTP 信封 `To:`，而後掃描程式便會過濾郵件。郵件內容中的 `To:` 和 `Cc:` 標頭會被忽略，且保持不變。

附註：如果您運用探查帳戶搭配別名和位址偽裝，則可能會遺失其中一個或其他帳戶。請遵循建立探查帳戶的指導方針。

請參閱第 269 頁的「關於建立探查帳戶」。

入埠位址偽裝優先於別名轉譯。如果相同的原始電子郵件地址或網域同時存在於位址偽裝清單和別名清單中，則傳送至來源網域的郵件便會繞送至偽裝的位址或網域。 Symantec Messaging Gateway 不會將郵件繞送至別名位址或網域。

除了位址偽裝套用至收件者位址的位置，您必須將別名的來源網域新增至本機網域清單 (Symantec Messaging Gateway 會接受來自此清單中網域的入埠電子郵件)。

請參閱第 71 頁的「新增或編輯網域」。

別名轉譯不適用於繞送至 Internet 的離埠郵件。

請參閱第 79 頁的「新增或編輯別名」。

請參閱第 81 頁的「新增或編輯位址偽裝 」。

新增或編輯別名

別名會將電子郵件地址轉譯為一或多個目的位址。針對您輸入的每個別名，指定一個 (且僅一個) 來源電子郵件地址或網域。對於每個目的位址，您可以輸入單一電子郵件地址，或多個電子郵件地址，並以逗號、分號或空格隔開。

請參閱第 78 頁的「關於別名與位址偽裝」。

請參閱第 80 頁的「別名位址」。

新增別名

1. 在控管中心內，按下**「通訊協定」> SMTP >「別名」**。
2. 按下**「新增」**。
3. 在**「新增別名」**頁面的**「別名網域或電子郵件地址」**方塊中，輸入別名。
4. 在**「此別名的網域或電子郵件地址」**方塊中，輸入網域或一或多個目的地電子郵件地址。

   您可以指定多個電子郵件地址或單一網域。
5. 按下**「儲存」**。

編輯別名

1. 在控管中心內，按下**「通訊協定」> SMTP >「別名」**。
2. 按下別名。
3. 在**「編輯別名」**頁面上，視需要修改**「別名網域或電子郵件地址」**方塊中的文字。
4. 視需要修改**「此別名的網域或電子郵件地址」**方塊中的文字。
5. 按下**「儲存」**。

匯入別名

別名可從文字檔案中匯入。 文字檔案中各個位址都必須以一或多個空格或 Tab 予以分隔，或以空格和 Tab 的組合予以分隔。 逗號或分號不是有效的分隔符號。 在匯入檔案中，每一行都必須包含別名位址，後面再接著一或多個目的位址。

匯入檔案的範例如下：

```
oak@example.com quercus@symantec-internetsecurity.com
ops@example.com tla@example.com bmi@example.com
blockads.com noadsorspam.com
```

匯入別名

1 在控管中心內，按下**「通訊協定」> SMTP >「別名」**。

2 按下**「匯入」**。

3 在**「指定匯入檔案」**文字方塊中，輸入或瀏覽到包含別名清單的檔名。

4 按下**「匯入」**。

如果匯入檔案中的項目未正確指定、與要求的檔案格式不符或重複，則會顯示錯誤訊息。您可以按下連結，下載包含未處理項目的檔案。

請參閱第 78 頁的「關於別名與位址偽裝」。

請參閱第 80 頁的「別名位址」。

按下**「取消」**，以忽略未處理的項目，並返回「別名」主頁面，以檢視有效的匯入項目。

別名位址

您可以針對輸入為來源電子郵件地址的每個別名，輸入多個目的電子郵件地址。但是，對於輸入為來源網域的每個別名，則只能輸入單一目的網域。別名來源位址必須具有本機網域。目的網域可以是本機網域或非本機網域。

別名來源範例	目的範例
anyone@example.com	somebody@example.com
anybody@example.com	someone@elsewhere.com
help@example.com	anybody@example.com、anyone@example.com、someone@example.com、somebody@example.com
example.com	elsewhere.com

附註：除了位址偽裝套用至收件者位址的位置，您必須將別名的來源網域新增至本機網域清單 (Symantec Messaging Gateway 會接受來自此清單中網域的入埠電子郵件)。

請參閱第 71 頁的「新增或編輯網域」。

別名是遞迴的。也就是說，在目的電子郵件地址清單中指定的別名，會擴大至別名清單中定義之別名，最多可達 1000 個位址。

在下面的範例中，由於 it@example.com 包含 ops@example.com，因此要寄到 it@example.com 的郵件會傳送至 it@example.com 和 ops@example.com 兩個目的位址。

別名	目的位址
it@example.com	alro@example.com、oak@example.com、ops@example.com

別名	目的位址
ops@example.com	tla@example.com、bmi@example.com、map@example.com

您新增的別名與已儲存的別名不得重複。您不能為網域建立電子郵件地址別名。也不能為電子郵件地址建立網域別名。您只能為一或多個其他電子郵件地址建立電子郵件地址別名。同樣，也只能為一或多個其他網域建立網域別名。

下面顯示的兩個別名都無效。

別名	目的位址
it@example.com	alro@example.com、symantec.com
example.com	sample@symantec.com

新增或編輯位址偽裝

位址偽裝是一種可以指定替代值給電子郵件地址或網域名稱，讓它們隱藏於電子郵件閘道背後的方法。

請參閱第 78 頁的「關於別名與位址偽裝」。

警告：如果您偽裝探查位址或網域，探查帳戶將變成無效。確定沒有與您偽裝的帳戶相關聯的探查帳戶。請參閱第 269 頁的「關於建立探查帳戶」。

請遵循下列步驟，新增或編輯偽裝的項目。

新增偽裝的項目

1. 在控管中心內，按下**「通訊協定」> SMTP >「位址偽裝」**。
2. 按下**「新增」**。
3. 在**「要偽裝的原始位址或網域」**方塊中，指定要偽裝的位址或網域。網域名稱不區分大小寫。
4. 在**「新增位址或網域」**方塊中，指定位址或網域名稱的新名稱。
5. 從**「套用至」**下拉式清單中，指定要套用此偽裝名稱的郵件：**「離埠郵件」**、**「入埠郵件」**或**「入埠和離埠郵件」**。
6. 按下**「儲存」**。

編輯偽裝的項目

1. 在控管中心內，按下**「通訊協定」> SMTP >「位址偽裝」**。
2. 按下您要修改的偽裝位址或網域。

3 在「**編輯偽裝項目**」頁面中，視需要修改偽裝的項目。

4 按下「**儲存**」。

匯入位址偽裝清單

除了建立新的偽裝項目之外，您還可以從類似 Sendmail `virtusertable` 的文字檔案中匯入偽裝項目。在匯入的檔案中，將各個偽裝位址定義個別放在一行中。 檔案中各個位址都必須以一或多個空格或 Tab 予以分隔，或以空格和 Tab 的組合予以分隔。 逗號或分號不是有效的分隔符號。

附註：您不可匯入含有擴充的 ASCII 或非 ASCII 字元的檔案，只能匯入以 US-ASCII 格式編碼的檔案。

偽裝的位址定義包含以下項目：

原始項目	指定要進行偽裝的原始電子郵件地址或網域名稱。
替代項目	指定替代的電子郵件地址或網域名稱。
套用至	指示要套用偽裝的方向。 可供選擇的有： ■ 入埠郵件 ■ 離埠郵件 ■ 入埠和離埠郵件

匯入檔案的範例如下：

```
orig1@domain.com  new1@domain.com  inbound
orig2@domain.com  new2@domain.com  outbound
orig3@domain.com  new3@domain.com  inbound/outbound
orig4@domain.com  new4.com         inbound
orig5@domain.com  new5.com         outbound
orig6@domain.com  new6.com         inbound/outbound
orig7.com         new7@domain.com  inbound
orig8.com         new8@domain.com  outbound
orig9.com         new9@domain.com  inbound/outbound
```

匯入偽裝項目的清單

1 在控管中心內，按下「**通訊協定**」**> SMTP >**「**位址偽裝**」。

2 按下「**匯入**」。

3 在「**指定匯入檔案**」文字方塊中，輸入或瀏覽至含有偽裝項目清單的檔名。

4 按下「**匯入**」。

如果匯入檔案中的項目未正確指定、與要求的檔案格式不符或重複，則會顯示錯誤訊息。您可以按下連結，下載包含未處理項目的檔案。按下「**取消**」返回「位址偽裝」頁面，檢閱有效的匯入項目。

忽略本機位址中的文字大小寫

啟用此選項時，MTA 會忽略位址偽裝、別名和探查帳戶中位址之本機部分的文字大小寫。

忽略本機位址中的文字大小寫

1 在控管中心內，按下「**通訊協定**」**> SMTP >**「**設定**」。

2 在 **SMTP** 標籤上的「**位址處理**」上，勾選「**忽略「位址偽裝」、「別名」和「網域」中本機位址部分文字的大小寫**」。

3 按下「**儲存**」。

請參閱第 77 頁的「架構電子郵件別名和地址偽裝」。

指定 TLS 通訊的 SSL 限制

在 Symantec Messaging Gateway 版本 10.6.5 及更新版本中，您可以防止使用舊版 TLS 或 SSLv3 的加密 SMTP 通訊。某些組織無法傳送或接受使用 SSLv3 或舊版 TLS 進行加密通訊的郵件。此設定可讓 SMG 視需要遵守更高的 TLS 標準。

啟用 SSL 限制

1 按下「**通訊協定**」**> SMTP >**「**設定**」。

2 在 **SMTP** 標籤上的「**SSL 限制**」面板中，選取「**在所有 SMTP TLS 對話中停用對 *<version>* 和舊版通訊協定的支援**」。

3 從下拉式功能表中，選取您要停用的最新版本。例如：

- 選取 **SSLv3** 以停用 SSLv3，並限制與 TLS 版本 1.0 或更新版本的通訊。SSLv3 具有嚴重漏洞，且某些組織不接受舊版 TLS。
- 若要允許使用 TLS 版本 1.1 或更新版本的加密通訊，並針對 TLS 1.0 或更舊版本停用支援，請選取 **TLSv1.0**。

4 按下「**儲存**」。

下表說明「**SSL 限制**」設定如何影響不同的 SMG 功能。此表還提供可讓您針對每個功能選擇設定的路徑。

表 3-4 SSL 限制如何影響主機、網域和 DLP 連線的加密設定

功能	控管中心位置
選取的掃描程式主機接受 TLS 加密連線用於入埠郵件。	**「管理」>「主機」>「組態」>「新增或編輯主機」> SMTP >「入埠」>「接受 TLS 加密」** 請參閱第 41 頁的「變更掃描程式入埠郵件設定」。 請參閱第 386 頁的「準備好系統以進行內容加密」。
如果遠端 MTA 提供加密，則選取的掃描程式主機會嘗試使用 TLS 加密傳送所有郵件。	**「管理」>「主機」>「組態」>「新增或編輯主機」> SMTP >「進階設定」>「傳送」標籤 >「嘗試針對傳送的所有郵件進行 TLS 加密」** 請參閱第 52 頁的「SMTP 進階傳送設定」。
選取的掃描程式主機接受 TLS 加密連線用於離埠郵件。	**「管理」>「主機」>「組態」>「新增或編輯主機」> SMTP >「離埠」>「接受 TLS 加密」** 請參閱第 44 頁的「變更掃描程式離埠郵件設定」。 請參閱第 386 頁的「準備好系統以進行內容加密」。
選取的掃描程式主機接受來自驗證和遠端連線以使用 MTA 傳送郵件之使用者的 TLS 連線。 **「管理」>「主機」>「組態」>「新增或編輯主機」> SMTP >「驗證」>「接受 TLS 加密」**可讓您選擇是否需要 TLS 加密。 ■ 如果您啟用此選項，而寄件者無法使用 SMG 支援的 TLS 版本進行通訊，則會退回該郵件。 ■ 如果您停用此選項，而寄件者無法使用 SMG 支援的 TLS 版本進行通訊，SMG 會接受未加密的連線 (不建議)。	**「管理」>「主機」>「組態」>「新增或編輯主機」> SMTP >「驗證」>「接受 TLS 加密」** 請參閱第 96 頁的「使用 SMTP 驗證的最佳實務準則」。 請參閱第 93 頁的「架構 SMTP 驗證郵件設定」。
掃描程式主機嘗試或需要 TLS 加密用於傳送到所選網域的郵件。 ■ 如果您需要 TLS 加密，而傳送伺服器無法使用 SMG 支援的 TLS 版本進行通訊，則郵件會排入傳送佇列，並且最終可能會退回。 ■ 如果您選取**「嘗試 TLS 加密」**，而傳送伺服器無法使用 SMG 支援的 TLS 版本進行通訊，則 SMG 將傳送未加密的郵件。	**「通訊協定」> SMTP >「網域」>「新增或編輯網域」>「傳送」>「TLS 加密設定」>「選用的傳送加密」**設定 請參閱第 71 頁的「新增或編輯網域」。
掃描程式主機需要 TLS 加密用於從該網域接收的郵件。	**「通訊協定」> SMTP >「網域」>「新增或編輯網域」>「接受」>「如果未使用 TLS 進行傳送，則拒絕來自此網域的郵件」** 請參閱第 71 頁的「新增或編輯網域」。

功能	控管中心位置
SMG 嘗試或需要 TLS 加密用於與 Data Loss Prevention Network Prevent 交換的郵件。	「內容」>「設定」>「**DLP 連線**」>「過濾」>「**TLS 加密設定**」>「**選用的傳送加密**」設定 請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。

關於無效收件者

依據預設，當要傳送至您網域的電子郵件送達時，若其要送達的收件者不是有效的使用者，則 Symantec Messaging Gateway 會將該郵件傳送至內部郵件伺服器。內部郵件伺服器可能會接受郵件並產生退回郵件，或者內部郵件伺服器可能會拒絕郵件。合法寄件者收到退回郵件時，可以用正確的位址重新傳送原有的郵件。然而，具有無效收件者的郵件也可能導因於垃圾郵件寄發者的電子郵件地址搜尋攻擊。

附註：在「電子郵件地址搜尋攻擊」頁面中，**「移除未解析的收件者」**動作只會在發生電子郵件地址搜尋攻擊時移除未解析的收件者。您可以將此動作與無效的收件者處理設定結合，或分別啟用這兩項設定。

請參閱第 128 頁的「架構電子郵件地址搜尋攻擊辨識」。

您可以將 Symantec Messaging Gateway 架構為接受、拒絕或棄置任何傳送給無效收件者的郵件，如下所述：

- 如果選擇接受所有收件者，則 Symantec Messaging Gateway 會接受所有郵件，不論收件者是否有效，皆是如此。不過，如果內部郵件伺服器拒絕收件者，則 Symantec Messaging Gateway 會傳送退回郵件。如果已將內部郵件伺服器架構為傳送退回郵件，則它也會傳送退回郵件。
- 如果選擇拒絕無效收件者，則 Symantec Messaging Gateway 會拒絕要傳送至 LDAP 目錄中不存在之電子郵件地址的任何郵件。傳送的 MTA 可能會產生退回郵件給寄件者。您必須針對收件者驗證架構資料來源。初始 SMTP 交談若發生 5xx SMTP 錯誤，就會拒絕收件者。
  請參閱第 439 頁的「關於透過資料來源使用收件者驗證功能」。
- 如果選擇棄置無效收件者，則 Symantec Messaging Gateway 會從郵件串流中棄置要傳送至 LDAP 目錄中不存在之電子郵件地址的任何郵件。退回郵件不會退回給寄件者。您必須針對收件者驗證架構資料來源。
- 若選擇拒絕或棄置無效收件者，Symantec Messaging Gateway 會將您的選擇套用至您架構要啟用收件者驗證的每個本機網域。如果您未啟用任何本機網域的收件者驗證，則不會棄置或拒絕任何郵件。
  請參閱第 71 頁的「新增或編輯網域」。

警告：棄置無效收件者的郵件是一種極端的措施。啟動此功能可能會阻礙診斷您電子郵件組態中的嚴重問題。請僅在您確定電子郵件系統穩定之後，才啟用此功能。此外，在啟用這項功能時，意外寫錯位址的郵件也會遭到棄置，而且不會傳送退回郵件。您可以改為拒絕無效收件者，而使傳送的 MTA 產生退回郵件 (若已架構)。

請參閱第 86 頁的「設定無效的收件者處理」。

設定無效的收件者處理

您可以設定無效的收件者處理以接受所有收件者，也可以棄置或拒絕無效的收件者。如果您選擇棄置或拒絕無效的收件者，您必須根據網域啟用無效的收件者驗證。

您必須在選擇拒絕或棄置無效的收件者之前，架構用於收件者驗證的目錄資料來源。

附註：如果您選擇**「拒絕」**或**「棄置」**無效的收件者郵件，您必須啟用該網域的收件者驗證。

請參閱第 71 頁的「新增或編輯網域」。

警告：棄置無效收件者的郵件是一種極端的措施。啟動此功能可能會阻礙診斷您電子郵件組態中的嚴重問題。 請僅在您確定電子郵件系統穩定之後，再啟用此功能。 此外，在啟動這項功能時，意外寫錯位址的郵件也會遭到棄置，而且不會寄出退回郵件。 您可以改為拒絕無效收件者，而使傳送的 MTA 產生退回郵件 (若已架構)。

設定無效的收件者處理

1 在控管中心內，按下**「通訊協定」> SMTP >「無效收件者」**。

2 執行下列其中一個步驟：

- 按下**「接受所有收件者」**可接受所有郵件而不管收件者是否有效。 如果內部郵件伺服器架構為傳送退回郵件或拒絕無效收件者，則會傳送退回郵件。
- 按下**「拒絕無效收件者」**可拒絕要傳送至 LDAP 目錄中不存在之使用者名稱的任何郵件。傳送的 MTA 可能會產生退回郵件給寄件者 (若已架構)。您必須架構用於收件者驗證的目錄資料來源以拒絕無效的收件者。 初始 SMTP 交談若發生 5xx SMTP 錯誤，就會拒絕收件者。
- 按下**「棄置無效收件者」**可從郵件串流棄置要傳送至 LDAP 目錄中不存在之使用者名稱的任何郵件。退回郵件不會退回給寄件者。您必須針對收件者驗證架構 LDAP 來源以使用此設定。
  此設定與使用**「電子郵件地址搜尋攻擊」**頁面指定的動作無關，但也可以搭配該動作一起使用。

3 按下**「儲存」**。

請參閱第 426 頁的「新增資料來源」。

關於電子郵件訊息流

確切瞭解電子郵件訊息在處理流程中都會發生哪些情況，可協助您以最佳方式架構系統，並協助您疑難排解發生的任何問題。Symantec Messaging Gateway 可讓您管理 SMTP (簡易郵件傳輸通訊協定)。本主題提供 SMTP 的郵件流總覽。

電子郵件政策和 SMTP 設定可以套用到這兩種入埠和離埠郵件流。某些政策和設定 (例如「Brightmail 適應性信譽管理」所涵蓋的政策和設定) 可解決只有入埠郵件流會發生的問題。另一方面，內容過濾政策可解決資料遺失預防與法規遵循問題，這些問題特別容易對離埠郵件流產生影響。

警告：Symantec Messaging Gateway 可讓您架構各種 MTA 組態參數，來管理您的電子郵件訊息流。如果您將郵件轉遞到其他 MTA，則這些 MTA 的某些設定可能會與 Symantec Messaging Gateway 設定衝突。例如，您將郵件大小上限架構為 10 MB，而您的本機轉遞 MTA 上限為 1 MB。這類衝突會造成難以診斷的錯誤。

請參閱第 122 頁的「關於連線時攔截與允許郵件」。

請參閱第 276 頁的「關於內容過濾」。

請參閱第 87 頁的「電子郵件訊息流階段」。

附註：您可以變更 Symantec Messaging Gateway 對可能有格式錯誤之郵件的掃描次數。

請參閱第 48 頁的「架構錯誤郵件處理」。

電子郵件訊息流階段

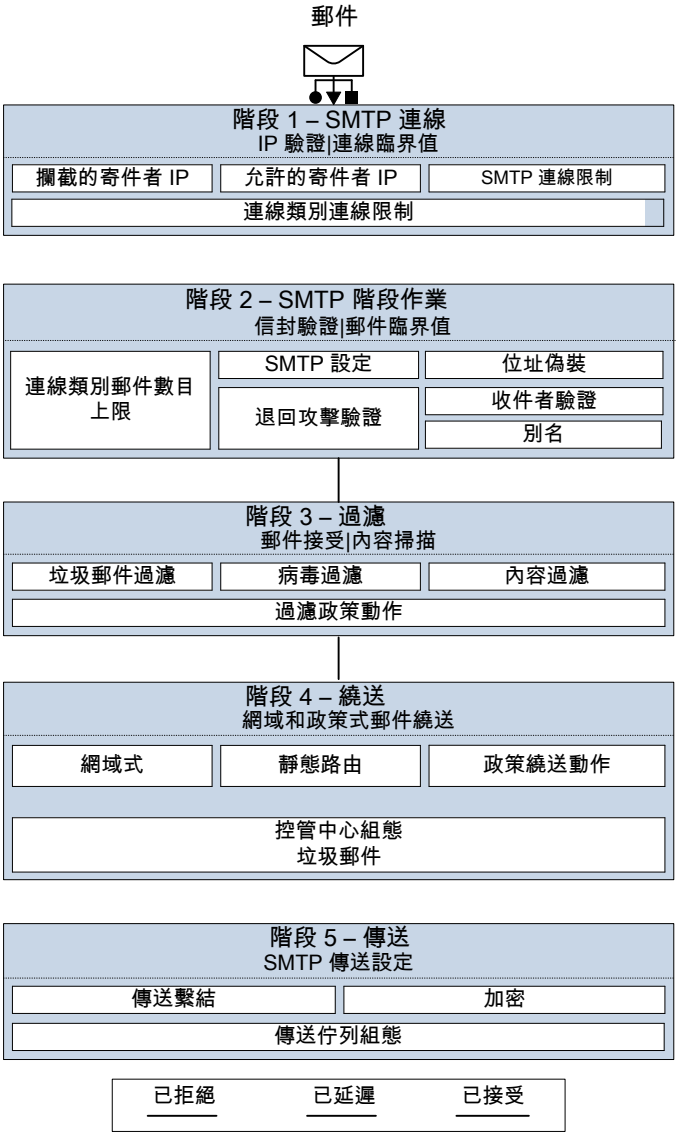
Symantec Messaging Gateway 使用下列階段處理電子郵件訊息：

- 階段 1 - SMTP 連線：在連線階段期間，除非特定政策或設定需要拒絕或延遲，否則 Symantec Messaging Gateway 會接受合法寄件者的連線。所有在此階段期間採取的動作都是單獨以 IP 位址為基礎。 Symantec Messaging Gateway 拒絕來自掃描程式 SMTP 設定不允許之任何 IP 位址的連線嘗試。 針對出現在 IP 式攔截寄件者群組中之 IP 位址的入埠連線，除非為群組架構不同的動作，否則 Symantec Messaging Gateway 會拒絕 SMTP 連線。某些連線會根據「連線類別」限制予以延遲。
  請參閱第 41 頁的「變更掃描程式入埠郵件設定」。
  請參閱第 124 頁的「關於管理閘道的連線負載」。
- 階段 2 - SMTP 階段作業：在 SMTP 階段作業期間，Symantec Messaging Gateway 會根據郵件信封來接受、拒絕或延遲郵件。它還會檢查「連線類別」設定和 SMTP 設定，以判定接受郵件是否超出架構的限制。
  請參閱第 42 頁的「變更掃描程式入埠郵件接收設定」。

- 階段 3 - 郵件過濾：掃描程式接受郵件之後，Symantec Messaging Gateway 會評估郵件內容並進行判斷。而評估郵件內容的根據是適用政策和設定 (必要時會包括內容過濾政策)。而且會根據判斷套用架構的動作。
  請參閱第 25 頁的「Symantec Messaging Gateway 的運作方式」。
- 階段 4 - 郵件繞送：Symantec Messaging Gateway 會將尚未隔離或保留以供檢閱的郵件繞送給郵件主機。路由是透過「網域傳送」設定和掃描程式的「本機郵件傳送」和「非本機郵件傳送」設定所決定。
  請參閱第 70 頁的「關於電子郵件網域」。
- 階段 5 - 郵件傳送：Symantec Messaging Gateway 會強制限制內部郵件伺服器的連線數目。如果架構了位址繫結設定以指定用來傳送電子郵件的 IP 位址，則 Symantec Messaging Gateway 會使用指定的 IP 位址。
  請參閱第 43 頁的「架構掃描程式入埠電子郵件傳送設定」。

圖 3-1 說明入埠郵件流。

圖 3-1 入埠郵件流



架構電子郵件進行 SMTP 驗證

SMTP 驗證會讓 MTA 驗證電子郵件用戶端，然後才讓您允許其傳送郵件。

表 3-5列出可幫助您架構 SMTP 驗證的工作。您可以視需要以任何順序執行這些工作。

表 3-5 SMTP 驗證

工作	說明
瞭解 Symantec Messaging Gateway SMTP 驗證。	您可以使用 SMTP 驗證，以允許遠端使用者透過 Symantec Messaging Gateway 傳送電子郵件。SMTP 驗證通常用來允許已授權使用者轉遞郵件。SMTP 驗證是 ESMTP 通訊協定的延伸服務。 本主題還列出 SMTP 驗證所需的支援 MUA 和 MTA 。此外，還說明您可用來驗證使用者憑證的方法。 請參閱第 90 頁的「關於使用 SMTP 驗證」。
設定 SMTP 驗證。	本主題說明設定 SMTP 驗證的程序。 請參閱第 91 頁的「如何設定 SMTP 驗證」。
架構適當的郵件設定。	您可以設定 SMTP 驗證，以便讓遠端連線的使用者可以從 Symantec Messaging Gateway 傳送郵件。 請參閱第 93 頁的「架構 SMTP 驗證郵件設定」。
檢閱 Symantec Messaging Gateway SMTP 驗證的最佳實務準則。	本主題提供賽門鐵克的建議，以幫助確保您的 SMTP 驗證正確運作。 請參閱第 96 頁的「使用 SMTP 驗證的最佳實務準則」。

關於使用 SMTP 驗證

您可以使用 SMTP 驗證，以允許遠端使用者透過 Symantec Messaging Gateway 傳送電子郵件。SMTP 驗證通常用來允許已授權使用者轉遞郵件。

SMTP 驗證是 ESMTP 通訊協定的延伸服務。如需有關 SMTP 驗證的詳細資訊，請參閱 RFC 4954：https://www.ietf.org/rfc/rfc4954.txt

許多電子郵件用戶端 (也稱為郵件使用者代理程式 (MUA)) 均支援 SMTP 驗證。支援的用戶端可讓使用者提供適當的憑證以啟用 SMTP 驗證。

Symantec Messaging Gateway 已針對下列 MUA 版本進行 SMTP 驗證的測試：

- Outlook 2013 (2013 年 3 月)
- Outlook 2010
- Outlook 2007
- Windows 7 上的 Windows Live Mail 2012
- Foxmail (中文版) v7 091 版
- Mail.app

Symantec Messaging Gateway 提供兩種方法來驗證提供給 SMTP 驗證的使用者憑證。您可以使用 LDAP 驗證來源，也可以將 MUA 提供的憑證轉寄至其他 SMTP 伺服器以進行驗證。

Symantec Messaging Gateway 透過將簡單繫結用於支援的所有 LDAP 目錄類型，支援透過 LDAP 進行 SMTP 驗證。對於透過使用密碼取回之 LDAP 所進行的 SMTP 驗證，所有支援的目錄類型 (Active Directory、Active Directory 通用類別目錄及 Domino 除外) 都受到支援。

附註：Symantec Messaging Gateway 會搜尋所有驗證目錄資料來源，以尋找嘗試驗證的使用者。如果使用者存在於多個驗證目錄資料來源中，SMTP 驗證將失敗。

請參閱第 429 頁的「關於資料來源和功能」。

對於透過 SMTP 轉寄至 SMTP 伺服器的 SMTP 驗證，已針對托管下列 MTA 版本的伺服器對 Symantec Messaging Gateway 進行測試：

- Exchange
- Domino
- Sendmail

警告：如果未使用適當的安全防護進行正確架構，則使用 SMTP 驗證可能會讓您的系統面臨嚴重的安全威脅。架構 SMTP 驗證時，請確保採取適當的步驟來保護您的使用者、系統及資料。

請參閱第 96 頁的「使用 SMTP 驗證的最佳實務準則」。

若要使用 SMTP 驗證，請執行設定程序。 請參閱第 91 頁的「如何設定 SMTP 驗證」。

如何設定 SMTP 驗證

表 3-6說明設定電子郵件進行 SMTP 驗證的程序。

表 3-6 設定電子郵件進行 SMTP 驗證

步驟	動作	說明
步驟 1 必要	選擇驗證來源。	您可以使用 LDAP 伺服器或 SMTP 伺服器作為驗證來源。 如果選擇 LDAP 伺服器，則必須擁有或建立目錄資料來源以進行驗證。如需詳細資訊，請參閱步驟 5 中的連結。 如果您選擇 SMTP 轉寄，則必須提供支援 SMTP 驗證之 SMTP 伺服器的詳細資料。此伺服器不得為其他 Symantec Messaging Gateway 硬體裝置。如需詳細資訊，請略過步驟 2 並參閱步驟 3 中的連結。 **附註：**使用 SMTP 轉寄可能會對郵件處理效能造成不良影響。

步驟	動作	說明
步驟 2 如果您選擇LDAP，則為必要	選擇您的驗證方法。	您可以使用簡單繫結或密碼取回以驗證使用者密碼。 如果未建立自訂 LDAP 查詢，則 Symantec Messaging Gateway 預設會使用簡單繫結。如果要使用密碼取回，則必須建立自訂 LDAP 查詢。 請參閱第444頁的「建立及測試自訂驗證與隔離所位址解析查詢」。 Symantec Messaging Gateway 透過將簡單繫結用於支援的所有 LDAP 目錄類型，支援透過 LDAP 進行 SMTP 驗證。對於透過使用密碼取回之 LDAP 所進行的 SMTP 驗證，所有支援的目錄類型 (Active Directory、Active Directory 通用類別目錄及 Domino 除外) 都受到支援。
步驟 3 必要	架構 SMTP 驗證郵件設定.	啟用驗證並提供重要的驗證詳細資料，包含是透過 LDAP 還是透過 SMTP 轉寄來驗證用戶端憑證。 用於 SMTP 驗證的 IP 位址/通訊埠組合，必須與您的入埠和離埠 IP 位址/通訊埠組合不同。 請參閱第 93 頁的「架構 SMTP 驗證郵件設定」。
步驟 4 選用	架構進階 SMTP 驗證設定.	設定 SMTP 驗證的最大值及其他進階組態參數。 請參閱第 48 頁的「架構 SMTP 進階設定」。 請參閱第 55 頁的「SMTP 進階驗證設定」。
步驟 5 選用	架構 LDAP 驗證.	透過 LDAP 進行 SMTP 驗證時，此為必要動作。 如果尚未建立資料來源，請建立資料來源並啟用SMTP驗證。 請參閱第 426 頁的「新增資料來源」。 請參閱第 428 頁的「啟用新資料來源的功能」。 請參閱第 431 頁的「建立驗證資料來源」。 如果已建立資料來源，請啟用 SMTP 驗證。 請參閱第 463 頁的「啟用或編輯驗證功能」。
步驟 6 必要	為一般使用者提供指示或架構 MUA.	將 MUA 架構為連線至驗證接聽程式通訊埠。驗證接聽程式的預設通訊埠為通訊埠 587。如果您在步驟 3 中變更了此通訊埠，請使用變更後的值。
步驟 7 選用	架構 SMTP 驗證警示.	架構警示，以便在 SMTP 驗證登入失敗時通知管理員。 請參閱第 590 頁的「架構警示」。

架構 SMTP 驗證郵件設定

您可以設定 SMTP 驗證，以便讓遠端連線的使用者可以從 Symantec Messaging Gateway 傳送郵件。

您也可以架構 SMTP 驗證登入失敗的警示。

請參閱第 590 頁的「架構警示」。

架構 SMTP 驗證郵件設定

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 勾選想要修改其設定的掃描程式，然後按下**「編輯」**。
3. 在**「編輯主機組態」**頁面上，按下 **SMTP** 標籤。
4. 若要檢視「驗證郵件設定」標籤，請啟用**「僅離埠郵件過濾」**或**「入埠和離埠郵件過濾」**。
5. 按下**「驗證」**標籤。
6. 在**「驗證郵件設定」**下，按下**「啟用驗證」**。
7. 在**「驗證郵件 IP 位址」**下拉式功能表中，選取您要驗證使用者的 IP 位址。

   提供的選擇項目是所選掃描程式上提供的乙太網路介面及虛擬介面。
8. 保留指派的預設通訊埠 587，或在**「通訊埠」**欄位中輸入新的通訊埠。

   此處指派的通訊埠是您架構電子郵件用戶端進行存取的通訊埠，或指示使用者在自己的電子郵件用戶端中架構的通訊埠。

   用於 SMTP 驗證的 IP 位址/通訊埠組合，必須與您的入埠和離埠 IP 位址/通訊埠組合不同。

   如需詳細資訊，請參閱下列 RFC：

   4954
9. 或者，從**「選用驗證郵件 IPv6 位址」**下拉式清單選取 IPv6 位址。

   您可以選取所選掃描程式上已架構用於乙太網路介面的任何 IPv6 位址。

   保留指派的預設通訊埠 587，或在**「通訊埠」**欄位中輸入新的通訊埠。

   此處指派的通訊埠是您架構電子郵件用戶端進行存取的通訊埠，或指示使用者在自己的電子郵件用戶端中架構的通訊埠。

   用於 SMTP 驗證的 IP 位址/通訊埠組合，必須與您的入埠和離埠 IP 位址/通訊埠組合不同。
10. 如果您要主機使用 TLS 加密來接受連線，請勾選**「接受 TLS 加密」**。

    如果您不勾選此選項，則 Symantec Messaging Gateway 不會在 SMTP 階段作業期間公告 TLS 加密的支援。

- 您必須先架構 MTA TLS 憑證並將其指派給此掃描程式，才能接受 TLS 加密的離埠郵件進行過濾。
  請參閱第 159 頁的「指派 MTA TLS 憑證給掃描程式」。
- **「通訊協定」>SMTP>「設定」>SMTP** 標籤上的**「SSL 限制」**設定會影響 Symantec Messaging Gateway 接受的 TLS 版本。
  請參閱第 83 頁的「指定 TLS 通訊的 SSL 限制」。

11 從下拉式功能表中選取憑證名稱，以驗證掃描程式是否為可透過 TLS 加密的連線傳送給用戶端的信任來源。

請參閱第 145 頁的「關於憑證」。

12 如果要掃描程式先要求來自寄件者的 TLS 加密憑證再接受 TLS 加密的連線，請勾選**「要求用戶端憑證」**。

13 勾選**「需要 TLS 加密」**以僅允許 TLS 加密的連線。

警告：賽門鐵克強烈建議您在啟用 SMTP 驗證時，要求使用 TLS 加密。

請參閱第 96 頁的「使用 SMTP 驗證的最佳實務準則」。

---

14 在**「驗證來源」**下，按下**「LDAP 伺服器」**或**「SMTP 轉寄」**。

如果您選擇**「LDAP 伺服器」**，則必須具有為驗證而定義的目錄資料來源。

請參閱第 90 頁的「關於使用 SMTP 驗證」。

如果您選擇了**「LDAP 伺服器」**，請略過下一步。

如果您選擇了**「SMTP 轉寄」**，則必須具有執行支援 SMTP 驗證之 MTA 的主機。

15 如果您選擇了**「SMTP 轉寄」**，請指定下列項目： SMTP 伺服器、主機、通訊埠，以及您要使用的 TLS 服務。

- 在**「主機」**欄位中指定 IP 位址或主機名稱，並指定**「通訊埠」**。
- (可選) 對於**「繫結」**，您可以選擇**「自動」**，也可以選擇特定 IP 位址。Symantec Messaging Gateway 會將郵件從您選擇的 IP 位址傳送至 SMTP 伺服器。
- 在 **TLS** 下，選取下列其中一個項目：

不嘗試 TLS 加密	對於與 SMTP 伺服器進行未加密通訊，請選取此選項。
嘗試 TLS 加密	選取此選項可以嘗試進行 TLS 加密的通訊。如果 SMTP 伺服器不支援 TLS，則不會對通訊進行解密。
需要 TLS 加密但不驗證憑證	如果 SMTP 伺服器不支援 TLS，則選取此選項可以中斷通訊，而不驗證 SMTP 伺服器憑證。

需要 TLS 加密且驗證憑證	如果 SMTP 伺服器不支援 TLS，或是無法成功驗證 SMTP 伺服器憑證，則選取此選項可以中斷通訊。

- (可選) 如果您使用 TLS，請勾選**「提供 TLS 用戶端憑證」**並選擇要使用的憑證。

警告：賽門鐵克強烈建議您在使用 SMTP 轉寄時，要求使用 TLS 加密。

警告：請勿將其他 Symantec Messaging Gateway 硬體裝置指定為進行 SMTP 轉寄的 SMTP 伺服器。

請參閱第 96 頁的「使用 SMTP 驗證的最佳實務準則」。

16 在**「驗證郵件連線」**下，選取下列其中一個選項：

接受通過驗證的所有郵件連線 (來自任意 IP 位址)	如果透過 SMTP 驗證進行連線的使用者經常出差，請選取此選項。 跳至 18。
僅接受來自以下 IP 位址，且通過驗證的郵件連線	如果使用者固定從相同 IP 位址連線，請選取此選項。此選項可提高安全性。 然後，在清單中，勾選您要此掃描程式接受來自哪些 IP 位址的已驗證郵件。 繼續進行到下一步。

17 可選擇執行下列其中一個工作：

手動新增 IP 位址	按下「**新增**」，然後輸入您要接受來自哪個本機網域之主機名稱或 IP 位址的已驗證郵件連線。您可以使用 CIDR 格式來輸入 IP 位址範圍。
編輯 IP 位址	勾選您要變更設定之電子郵件用戶端的主機名稱或 IP 位址，接著按下「**編輯**」，然後進行所需的變更。
刪除一或多個 IP 位址	勾選您不再接受已驗證郵件連線的來源位址或網域，然後按下「**刪除**」，將其從清單中刪除。 若要刪除所有現有的位址或網域，請按下「**全部刪除**」。
匯入 IP 位址	按下「**匯入**」，接著瀏覽至檔案位置，然後按下「**匯入**」。 您可以匯入以逗號、分號、空格和定位字元作為分隔字元的檔案。
匯出 IP 位址	按下「**匯出**」，然後指定匯出檔案的名稱及儲存該檔案的位置。

18 按下「**儲存**」或勾選「**套用上述設定至所有掃描程式**」，然後按下「**儲存**」。

使用 SMTP 驗證的最佳實務準則

您可以使用 SMTP 驗證來允許遠端使用者使用 MTA 傳送電子郵件。如果未採取適當的步驟來確保通訊安全無虞，則使用 SMTP 驗證可能會提高安全風險。

賽門鐵克強烈建議您在使用 SMTP 驗證時，實作下列最佳實務準則：

- 要求對 SMTP 驗證使用 TLS 加密。
  請參閱第 93 頁的「架構 SMTP 驗證郵件設定」。
- 如果您使用 SMTP 轉寄功能，請要求對 SMTP 轉寄使用 TLS 加密。
- 請勿嘗試將其他 Symantec Messaging Gateway 硬體裝置用作 SMTP 轉寄的 SMTP 伺服器。SMTP 轉寄僅透過 IPv4 位址執行。
- 架構 SMTP 驗證郵件設定時，請勿選擇接受來自所有 IP 位址的已驗證郵件連線，相反的，請指定 IPv4 和/或 IPv6 位址清單。此最佳實務準則可能並非適用於所有組織。
- 架構並啟用可抵禦垃圾郵件的離埠過濾政策。
  請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。
- 架構 SMTP 驗證登入失敗的警示。
  請參閱第 590 頁的「架構警示」。

指定地址驗證條件

您可以指定一個必須驗證電子郵件地址的條件。尤其是，您可以指定允許在地址中使用的字元。

指定地址驗證條件

1 在控管中心內，按下**「通訊協定」> SMTP >「設定」**。

2 在 **SMTP** 標籤上的**「地址驗證」**下選取您要執行的條件，如下：

允許電子郵件地址包含百分比字元

允許電子郵件地址包含百分比符號。

這選項對於允許此符號作為電子郵件地址一部分的舊式系統非常有用。

允許電子郵件地址以破折號為開頭

讓地址以減號作為第一個字元。

當您選取此選項時，Symantec Messaging Gateway 接受任何地址開頭為「-」字元的電子郵件。若取消勾選，Symantec Messaging Gateway 會拒絕以「-」字元開頭而傳送至任何收件者位址的電子郵件。

允許在電子郵件地址中使用 8 個位元的字元

允許電子郵件地址包含 8 位元字元。

請參閱第 581 頁的「將 8 位元 MIME 郵件轉換為 7 位元 MIME」。

移除收件者驗證目錄查詢中的子位址

提供在收件者驗證中對子位址的支援。

子位址由電子郵件地址的本機部分 (@ 之前的部分)，緊接在加號或減號之後的附加文字所組成。若選取此選項，則 Symantec Messaging Gateway 會在完成 LDAP 收件者驗證查詢之前移除電子郵件地址的 *+詳細資訊*或 *-詳細資訊*部分。

附註：如果您在電子郵件地址中使用加號或減號，但並非用於子位址，則啟用此功能會導致收件者驗證發生錯誤。

請參閱第 430 頁的「建立收件者驗證資料來源」。

3 按下**「儲存」**。

4

設定電子郵件寄件者驗證

本章包含以下主題：

- 寄件者驗證的運作方式
- 針對入埠郵件設定寄件者驗證
- 針對離埠郵件設定寄件者驗證
- 為網域啟用 DKIM 簽署

寄件者驗證的運作方式

垃圾郵件作者通常會嘗試偽造郵件伺服器名稱、傳送網域或電子郵件訊息中的其他中繼資料，以避開偵測。SMG 提供多個用於偵測這些偽造的寄件者驗證選項。您可以在**「垃圾郵件」>「設定」>「寄件者驗證」**頁面上啟用下列任何選項：

- **SPF**：根據發布的 DNS 記錄檢查信封寄件者的網域。
- **寄件者 ID**：根據發布的 DNS 記錄檢查郵件標頭「寄件者」地址的網域。寄件者 ID 不及 SPF 有效，因為與信封寄件者相較，「寄件者」地址更容易偽造。
- **DKIM**：使用私密網域金鑰來簽署網域的外寄郵件標頭及郵件內文。寄件者將符合的公開金鑰新增至網域的 DNS 記錄。接收郵件的郵件伺服器會使用公開金鑰，來比較原始特徵和電子郵件標頭與內文中接收的特徵。如果特徵相符，該郵件會通過 DKIM 驗證。
- **DMARC**：使用 SPF 和 DKIM 來驗證電子郵件訊息，但新增可供寄件者和收件者共用結果相關資訊的機制。傳送電子郵件訊息的網域可以在其 DNS TXT 記錄中發布 DMARC 政策。收件者可以根據寄件者已發布的政策來檢查 SPF 和 DKIM 驗證的結果。然後，收件者可以使用已發布的政策，來決定如何處理任何不相符的郵件。

附註：如果您並未在閘道中部署 SMG，DMARC 和 DKIM 結果會很有用，但 SPF 沒有任何結果。如果連線內部 IP 位址，SMG 不會執行 SPF 驗證。

DMARC 允許寄件者要求有關不相符的郵件的報告，並提供讓收件者提供報告的機制。這些報告可讓雙方注意具詐騙性的網域。

附註：Symantec Email Fraud Protection 是一種雲端服務，可協助客戶實作 DMARC 標準，以防止攻擊者詐騙其網域名稱。Email Fraud Protection 提供作為 Symantec Messaging Gateway 的附加程式。購買服務的客戶會將其 DMARC、SPF 和 DKIM 記錄指向 Email Fraud Protection 平台，以即時回應驗證要求，並確保使用客戶網域名稱所傳送的電子郵件已獲得授權。如需 Email Fraud Protection 運作方式的相關資訊，請參閱服務的線上說明，網址為：https://help.symantec.com/home/FRAUD_PRO?locale=EN_US。

您可以選擇對傳送到所有網域的入埠郵件執行寄件者驗證。此設定可提供最高安全性，但需要更多處理。作為替代方案，您可以建立要進行特殊處理的網域清單。然後，您可以選擇從寄件者驗證中排除列出的網域，或僅在列出的網域上執行寄件者驗證。

當您啟用驗證方法時，SMG 會在其掃描的每個入埠郵件中插入驗證結果標頭。此標頭包含該方法的掃描結果。結果以每個通訊協定的已發布標準為基礎。

寄件者驗證結果也會出現在郵件稽核日誌中。例如：

```
DKIM|permfail (body hash did not verify)|newsletters.stream|dkim
```

若要處理寄件者驗證失敗的郵件，SMG 會針對最常見的 DKIM、DMARC、寄件者 ID 和 SPF 判斷提供預設內容過濾政策。這些政策預設為啟用，您可以自訂這些政策來滿足您組織的需求。然而，您必須先將內容過濾政策指派給政策群組，SMG 才能使用這些政策來處理郵件。

當寄件者驗證結果觸發內容過濾政策時，郵件稽核日誌會記錄判斷。日誌項目包含觸發政策的違規，以及 Symantec Messaging Gateway 對郵件執行的動作。例如：

```
VERDICT|hthistle@yourcompany.net|content_521|default|senderid validation
softfail: modify subject line with "[senderid
softfail]"|header|authentication-results|senderid=softfail
```

請參閱第 99 頁的「針對入埠郵件設定寄件者驗證」。

請參閱第 105 頁的「針對離埠郵件設定寄件者驗證」。

針對入埠郵件設定寄件者驗證

入埠寄件者驗證會偵測垃圾郵件作者何時嘗試偽造郵件伺服器名稱、傳送網域或您的使用者收到的電子郵件訊息中的其他中繼資料。SMG 會提供 SPF、寄件者 ID、DKIM 及 DMARC 寄件者驗證選項，以提供全面的垃圾郵件偵測。

附註：Symantec Email Fraud Protection 是一種雲端服務，可協助客戶實作 DMARC 標準，以防止攻擊者詐騙其網域名稱。Email Fraud Protection 提供作為 Symantec Messaging Gateway 的附加程式。購買服務的客戶會將其 DMARC、SPF 和 DKIM 記錄指向 Email Fraud Protection 平台，以即時回應驗證要求，並確保使用客戶網域名稱所傳送的電子郵件已獲得授權。如需 Email Fraud Protection 運作方式的相關資訊，請參閱服務的線上說明，網址為：https://help.symantec.com/home/FRAUD_PRO?locale=EN_US。

設定入埠寄件者驗證

1 設定您要用於垃圾郵件偵測的寄件者驗證方法。

表 4-1 摘要說明如何針對入埠郵件設定 SPF、寄件者 ID、DKIM 及 DMARC 驗證。可以在**「垃圾郵件」>「設定」>「寄件者驗證」**頁面上啟用您想要 SMG 使用的每個驗證方法。然後，可以指派相關的內容過濾政策給政策群組。這些內容過濾政策位於**「內容」>「政策」>「電子郵件」>「電子郵件內容過濾政策」**頁面。

當郵件未通過寄件者驗證時，SMG 會根據符合驗證方法和失敗條件的政策來處理郵件。

請參閱第 102 頁的「寄件者驗證的內容過濾政策」。

2 選取要測試的外部網域。

寄件者驗證會使用重要處理資源，但 SMG 驗證來自全部網域的入埠郵件時這樣可最有效地防範垃圾郵件。您選取**「網域驗證」**設定時，需決定如何在垃圾郵件防護與您的特定安裝效能之間取得平衡。

請參閱第 101 頁的"選取用於寄件者驗證的網域"。

表 4-1 入埠寄件者驗證設定指示

寄件者驗證方法	入埠實作步驟
SPF	1 在**「垃圾郵件」>「設定」>「寄件者驗證」**頁面上，於**「驗證類型」**面板中啟用 **SPF**。 2 在**「內容」>「政策」>「電子郵件」>「電子郵件內容過濾政策」**頁面上，將政策群組指派至相關的內容過濾政策，以處理無法通過 SPF 驗證的郵件。
寄件者 ID	1 在**「垃圾郵件」>「設定」>「寄件者驗證」**頁面上，於**「驗證類型」**面板中啟用**「寄件者 ID」**。 您啟用「寄件者 ID」時，SMG 也啟用 SPF，因為當 SMG 使用 DNS 驗證寄件者 ID 時，程序也會提供 SPF 驗證。 2 在**「內容」>「政策」>「電子郵件」>「電子郵件內容過濾政策」**頁面上，將政策群組指派至相關的內容過濾政策，以處理無法通過「寄件者 ID」驗證的郵件。

寄件者驗證方法	入埠實作步驟
DKIM	1 在「**垃圾郵件**」>「**設定**」>「**寄件者驗證**」頁面上，於「**驗證類型**」面板中啟用 **DKIM**。 2 您也可以將「DKIM 簽章驗證數上限」變更為任何介於 1 和 20 (含) 之間的數字。 單一郵件超過「**DKIM 簽章驗證數上限**」時，Symantec Messaging Gateway 便會停止該郵件的 DKIM 驗證。會忽略其他簽章。 如果任何 DKIM 簽章通過，則郵件會通過 DKIM 驗證。 如果達到「**DKIM 簽章驗證數上限**」時沒有簽章通過，則郵件未通過 DKIM 驗證。 3 在「**內容**」>「**政策**」>「**電子郵件**」>「**電子郵件內容過濾政策**」頁面上，將政策群組指派至相關的內容過濾政策，以處理無法通過 DKIM 驗證的郵件。
DMARC	1 在「**垃圾郵件**」>「**設定**」>「**寄件者驗證**」頁面上，於「**驗證類型**」面板中啟用 **DMARC**。 2 在「**DMARC 報告設定**」面板上，選取 DMARC 報告選項。 請參閱第 105 頁的「啟用 DMARC 報告」。 3 在「**內容**」>「**政策**」>「**電子郵件**」>「**電子郵件內容過濾政策**」頁面上，將政策群組指派至相關的內容過濾政策，以處理無法通過 DMARC 驗證的郵件。

選取用於寄件者驗證的網域

賽門鐵克建議您在所有寄件者網域上執行寄件者驗證。但是，「**網域驗證**」設定可讓您建立傳送網域清單，然後選擇要從寄件者驗證包含或排除網域。當 SMG 收到郵件時，它會對照清單檢查信封寄件者的網域，以決定是否要執行您啟用的寄件者驗證檢查。

選取要驗證的寄件者網域

1 在「**網域驗證**」面板中：

- 選取「**驗證所有網域**」，以對來自所有網域的入埠郵件執行寄件者驗證。然後，按下「**儲存**」。
  「**驗證所有網域**」提供最有效率的垃圾郵件防護，但會最大程度影響效能。
- 選取「**只驗證下列網域**」，以對來自所列網域的入埠郵件執行寄件者驗證。然後，移至步驟 2，建立網域清單。
  此選項對效能影響程度最小，但會提供最低效的垃圾郵件防護。
- 選取「**驗證除下列網域以外的所有網域**」，從寄件者驗證中排除列出的網域。然後，移至步驟 2，建立網域清單。
  當您選取此選項時，SMG 不會測試任何顯示來自這些網域的入埠郵件。您可以使用此選項防止 SMG 測試已知安全的傳送網域，這樣可提升效能。

2 建立網域清單，以驗證或從驗證排除網域。SMG 提供預設網域清單。

- 若要新增網域至清單，請按下**「新增」**。在文字欄位中輸入網域名稱，然後按下**「儲存」**。

  附註：Symantec Messaging Gateway 會對您新增的網域執行精確相符性檢查。例如，如果您新增最上層網域，SMG 不會自動符合子網域。必須明確地新增也要相符的每個子網域。不能使用萬用字元。

- 若要編輯網域的拼字，請選取網域，然後按下**「編輯」**。進行變更，然後按下**「儲存」**。
- 若要從清單中刪除網域，請選取網域，然後按下**「刪除」**。

3 按下**「儲存」**。

寄件者驗證的內容過濾政策

從版本 10.6.5 開始，Symantec Messaging Gateway 會使用內容過濾政策來處理寄件者驗證失敗的郵件。下表說明**「內容」>「政策」>「電子郵件」>「電子郵件內容過濾政策」**頁面上的寄件者驗證的預設內容過濾政策。這些政策預設為啟用，並且僅套用至入埠郵件。

可以根據您在**「垃圾郵件」>「設定」>「寄件者驗證」**頁面上啟用的驗證選項來指派這些政策。您必須將這些政策指派給政策群組，然後 SMG 才能使用這些政策來處理寄件者驗證失敗的郵件。若要根據不同的失敗條件處理郵件，SMG 會針對每個驗證方法提供多個內容過濾政策。此表包含何時指派每個政策的建議

附註：Symantec Email Fraud Protection 是一種雲端服務，可協助客戶實作 DMARC 標準，以防止攻擊者詐騙其網域名稱。Email Fraud Protection 提供作為 Symantec Messaging Gateway 的附加程式。購買服務的客戶會將其 DMARC、SPF 和 DKIM 記錄指向 Email Fraud Protection 平台，以即時回應驗證要求，並確保使用客戶網域名稱所傳送的電子郵件已獲得授權。如需 Email Fraud Protection 運作方式的相關資訊，請參閱服務的線上說明，網址為：https://help.symantec.com/home/FRAUD_PRO?locale=EN_US。

表 4-2 寄件者驗證的預設政策

政策名稱	觸發政策的預設條件	預設動作	建議
寄件者驗證：DMARC、SPF，寄件者 ID 失敗：刪除	郵件標頭包含下列其中一個項目： ■ 驗證結果：DMARC = 失敗：拒絕 ■ 驗證結果：SPF = 失敗**以及**驗證結果：DMARC = 無 ■ 驗證結果：SENDERID = 失敗**以及**驗證結果：DMARC = 無	刪除郵件	如果您已啟用 DMARC 寄件者驗證，請將此政策指派給您的政策群組。此政策處理如下郵件： ■ DMARC 驗證失敗，並且寄件者的已發布政策為拒絕這些郵件 (p-reject)。 ■ SPF 驗證失敗，並且寄件者的已發布政策為無 (p=none)。 ■ 寄件者 ID 驗證失敗，並且寄件者的已發布政策為無 (p=none)。 依據預設，此政策的**「後續內容過濾處理」**設定為**「僅提供事件和通知動作」**，因為預設動作為刪除郵件。 如果您變更政策動作或將政策移至清單中的其他位置，請務必評估**「後續內容過濾處理」**的效果。在預設設定中，SMG 僅針對位於清單底端的政策執行資安事端和通知動作。
寄件者驗證：DMARC 失敗：隔離	郵件標頭包含： 驗證結果：DMARC = 失敗：隔離	將郵件保留在垃圾郵件隔離所	如果您啟用 DMARC 寄件者驗證，請將此政策指派給您的政策群組。此政策會處理 DMARC 驗證失敗的郵件，並且寄件者的已發布政策為隔離這些郵件 (p-quarantine)。
寄件者驗證：DKIM 失敗：使用「[DKIM 失敗]」修改主旨行	郵件標頭包含： 驗證結果：DKIM = 失敗	在郵件主旨行前面加上「[DKIM 失敗]」	如果您啟用 DKIM 寄件者驗證，但不啟用 DMARC，請將此政策指派給您的政策群組。 如果您啟用 DMARC，並將 DMARC 政策指派給您的政策群組，則不需要指派此政策。DKIM 失敗觸發 DMARC 失敗。

政策名稱	觸發政策的預設條件	預設動作	建議
寄件者驗證：SPF，寄件者 ID 失敗：使用「[寄件者驗證失敗]」修改主旨行	郵件標頭包含下列其中一個項目： ■ 驗證結果：SPF = 失敗 ■ 驗證結果：SENDERID = 失敗	在主旨行前面加上「[寄件者驗證失敗]」	如果您啟用 SPF 或寄件者 ID 驗證，但不啟用 DMARC，請將此政策指派給您的政策群組。 如果您啟用 DMARC，並將 DMARC 政策指派給您的政策群組，則不需要指派此政策。SPF 或寄件者 ID 失敗觸發 DMARC 失敗。
寄件者驗證：SPF Softfail：使用「[SPF Softfail]」修改主旨行	郵件標頭包含： 驗證結果：SPF = Softfail	在郵件主旨行前面加上「[SPF Softfail]」	如果您啟用 SPF 驗證，但不啟用 DMARC，請將此政策指派給您的政策群組。 如果您啟用 DMARC，並將 DMARC 政策指派給您的政策群組，則不需要指派此政策。
寄件者驗證：寄件者 ID Softfail：使用「[寄件者 ID Softfail]」修改主旨行	郵件標頭包含： 驗證結果：SENDERID = Softfail	在郵件主旨行前面加上「[寄件者 ID Softfail]」	如果您啟用寄件者 ID 驗證，但不啟用 DMARC，請將此政策指派給您的政策群組。 如果您啟用 DMARC，並將 DMARC 政策指派給您的政策群組，則不需要指派此政策。
寄件者驗證：驗證錯誤：使用「[寄件者驗證驗證錯誤]」修改主旨行	郵件標頭包含下列其中一個項目： ■ 驗證結果：SPF = Temperror ■ 驗證結果：SPF = Permerror ■ 驗證結果：DKIM = Temperror ■ 驗證結果：SENDERID = Temperror ■ 驗證結果：SENDERID = Permerror	在主旨行前面加上「[寄件者驗證驗證錯誤]」	啟用任何寄件者驗證選項時，將此政策指派給您的群組。 當 SMG 遇到 DMARC、SPF、DKIM 或寄件者 ID 的暫時性錯誤條件時，此政策會處理郵件。例如，驗證檢查期間發生 DNS 逾時會觸發 *Temperror* 條件。 此政策還會處理因永久錯誤導致的驗證失敗。例如，具有無效結構的 DNS 記錄會觸發 *Permerror* 條件。

啟用 DMARC 報告

當您在**「垃圾郵件」>「設定」>「寄件者驗證」**頁面上針對入埠郵件設定 DMARC 寄件者驗證時，也可以啟用 DMARC 失敗報告。SMG 會以電子郵件形式將失敗報告傳送給郵件未通過 DMARC 驗證之寄件者的網域。

啟用 DMARC 報告

1 在 SMG 控管中心，選取**「垃圾郵件」>「設定」>「寄件者驗證」**。

2 在**「寄件者驗證」**頁面上，啟用**「以網域為基礎的郵件驗證、報告和符合性(DMARC)」**。

您也可以限制想讓 SMG 檢查其郵件的外部網域，或允許 SMG 針對所有網域執行寄件者驗證。

請參閱第 99 頁的「針對入埠郵件設定寄件者驗證」。

3 在**「DMARC 報告設定」**面板中，選取**「啟用失敗報告」**。

4 在**「寄件者地址」**欄位中，輸入傳送失敗報告的電子郵件地址。**「寄件者地址」**必須是電子郵件系統上的有效地址。

SMG 僅向提供其 DMARC DNS 記錄中的電子郵件地址的網域傳送失敗報告。如果失敗報告無法傳送至提供地址的網域，您的寄件者地址信箱會收到退回的郵件。

- 如果您要監控何時無法傳送失敗報告，請輸入管理員地址作為寄件者地址。
- 如果您不想監控這些傳送失敗，請輸入不受監控的電子郵件帳戶的地址。

SMG 不會保留所傳送的失敗報告的複本。

5 按下**「儲存」**。

寄件者網域的 DMARC DNS 記錄必須要求蒐證報告並提供電子郵件地址，才能接收這些失敗報告。

請參閱 Anatomy of a DMARC resource record in the DNS (「DNS 中的 DMARC 資源記錄的解析」)，網址為：https://dmarc.org/overview

如需有關 DMARC 失敗報告的詳細資訊，請造訪：https://tools.ietf.org/html/rfc7489#section-7.3

針對離埠郵件設定寄件者驗證

離埠寄件者驗證可協助組織外部的郵件伺服器，在收到具有偽造電子郵件地址或標頭資訊 (來自您的網域) 的郵件時進行偵測。

離埠郵件的寄件者驗證需要對 SMG 作業範圍之外的 DNS 記錄進行變更。下表的離埠設定說明針對離埠郵件設定寄件者驗證所需執行的動作。

表 4-3 寄件者驗證的離埠步驟

寄件者驗證方法	離埠實作步驟 (可讓收件者偵測您網域中的詐騙性電子郵件)
SPF	建立 DNS 記錄以提供網域擁有權證明。如果需要指示，請參閱 Internet 上的資源，例如 http://www.openspf.org/SPF_Record_Syntax。
寄件者 ID	建立 DNS 記錄以提供網域擁有權證明。如需相關指示，請參閱 Internet 上的資源。
DKIM	1 在**「管理」>「設定」>「憑證」>「網域金鑰」**標籤上，新增或匯入網域金鑰。 請參閱第 109 頁的「新增網域金鑰」。 2 在**「通訊協定」>「網域」>「新增或編輯網域」>「傳送」**標籤上，啟用**「DKIM 簽署」**。 請參閱第 106 頁的「為網域啟用 DKIM 簽署」。 3 此外，在**「通訊協定」>「網域」>「新增或編輯網域」>「傳送」**標籤上，按下**「產生」**以產生 DKIM DNS 文字記錄。此作業會提供正確的 DNS TXT 記錄內容和語法。 4 手動將產生的 DKIM DNS 文字記錄複製到網域的 DNS 記錄中。
DMARC	1 如上所述，針對網域啟用 DKIM 簽署。 2 將 DMARC 資源記錄新增至網域的 DNS 記錄。 如需詳細資訊，包括 DMARC 資源記錄語法，請造訪 https://dmarc.org/resources/specification/。也可以在 dmarc.org 常見問答集「What steps should I follow to implement DMARC on my corporate email domain? (若要在我的公司電子郵件網域中實作 DMARC，應遵循什麼步驟？)」中找到實作 DMARC 的一般程序 **附註：**Symantec Email Fraud Protection 是一種雲端服務，可協助客戶實作 DMARC 標準，以防止攻擊者詐騙其網域名稱。Email Fraud Protection 提供作為 Symantec Messaging Gateway 的附加程式。購買服務的客戶會將其 DMARC、SPF 和 DKIM 記錄指向 Email Fraud Protection 平台，以即時回應驗證要求，並確保使用客戶網域名稱所傳送的電子郵件已獲得授權。如需 Email Fraud Protection 運作方式的相關資訊，請參閱服務的線上說明，網址為：https://help.symantec.com/home/FRAUD_PRO?locale=EN_US。 **附註：**

為網域啟用 DKIM 簽署

您可以使用現有的網域金鑰，為所有來自特定網域的離埠郵件啟用 DKIM 簽署。

附註：雖然 DKIM 標準允許多個簽章，但 Symantec Messaging Gateway 只能新增一個 DKIM 簽章至離埠郵件。

為網域啟用 DKIM 簽署

1 在控管中心內，於**「管理」>「設定」>「憑證」>「網域金鑰」**標籤上，確保已為 DKIM 簽署新增或匯入網域金鑰。

請參閱第 109 頁的「新增網域金鑰」。

2 按下**「通訊協定」> SMTP >「網域」**。

3 按下您要新增 DKIM 簽署之網域加上底線的名稱。

4 在**「編輯網域」**頁面上，按下**「傳送」**標籤。

5 在 **DomainKeys Identified Mail** 面板中，按下**「啟用來自此網域之郵件的 DKIM 簽署」**。

6 在**「基底網域」**欄位中，輸入要用作DKIM 簽章一部分的網域名稱，格式為：**example.com**

附註：如果您也啟用離埠郵件的DMARC，在此處輸入的基底網域會影響您在DMARC記錄中指定的 DKIM 對齊方式。如需如何建立 DMARC 記錄的相關指示，請造訪 https://dmarc.org/overview/。

7 在**「選取器」**方塊中，輸入接收 MTA 可使用的選取器字串，該字串可用來執行 DNS 查詢以擷取公開金鑰。

該選取器會識別 SMG 用來簽署從此網域傳送的郵件的金鑰。輸入含有最多 63 個小寫英數字元的字串 (a-z 或 0-9)。

若需使用選取器的詳細資訊，請參閱 RFC 4871 第 3.1 節。

https://tools.ietf.org/html/rfc4871#section-3.1

8 從**「簽署金鑰」**下拉式清單中，選擇您要用來簽署來自此網域之郵件的網域金鑰。

9 在**「簽章有效期限」**方塊中，輸入介於 1 和 9999 (含) 之間的整數，然後按下**「小時」**或**「天」**。

預設值為 30 天。

10 如果您要進一步自訂 DKIM 簽署，請按下**「顯示進階」**並完成下列選用欄位：

識別

一種電子郵件地址 (包含或不包含 @ 前面的部分)，包括基底網域或基底網域的子網域。例如，如果基底網域為 example.com，則可接受的身分字串包括：

- @example.com
- user@example.com
- @new.example.com
- user@old.example.com

覆寫預設已簽署的標頭

勾選此方塊，使用您自己設計的標頭取代預設已簽署的標頭。然後，輸入一或多個標頭 (以冒號隔開)。

您可以在任何標頭的後面添加下列其中一個字元：

- ? - 簽署標頭的單一副本。不要強制使用不存在的標頭 (如果標頭不存在)。
- * - 簽署標頭的所有現有副本。強制使用不存在的標頭 (如果標頭不存在)。
- + - 簽署標頭的所有現有副本。不要強制使用不存在的標頭 (如果標頭不存在)。
- [無字元] - 簽署標頭的單一副本。強制使用不存在的標頭 (如果標頭不存在)。

範例：

```
Received+:X-Example*:From:Subject?:Received
```

無論您是否覆寫預設的已簽署標頭，Symantec Messaging Gateway 都會包含 From: 標頭。

標頭

您可以選擇用來準備郵件標頭簽章的方法。

- **套用「寬鬆」演算法**會根據標頭的呈現方式 (包含空格更動等細微變更) 來建立簽章。如果標頭在轉換期間發生細微修改，則在許多情況下，寬鬆規範化仍會產生相符的簽章。
- **套用「簡單」演算法**將簽章以精確的標頭內容為基礎，包括間距等詳細資料。

郵件標頭的預設值為**套用「寬鬆」演算法**。

內文

您可以選擇 SMG 用來準備郵件內文簽章的方法。

- **套用「寬鬆」演算法**會根據郵件內文的呈現方式 (包含空格更動等細微變更) 來建立簽章。如果郵件內文在轉換期間發生細微變動，則在許多情況下，寬鬆規範化仍會產生相符的簽章。
- **套用「簡單」演算法**將簽章以精確的郵件內文內容為基礎，包括間距等詳細資料。

郵件內文的預設值為**套用「簡單」演算法**。

如需規範化的詳細資訊，請參閱 RFC 4871 第 3.4 節。

RFC 4871，第 3.4 節

11 按下**「產生」**建立 DKIM DNS 文字記錄。此文字記錄使用您在先前步驟中指定的基底網域、選取器和簽署金鑰詳細資料。

12 按下**「儲存」**。

13 手動將公開金鑰新增至您的 DNS 記錄。

MTA 執行 DKIM 驗證時，接收 MTA 會存取 DNS 項目以擷取您的公開金鑰。

您可以使用 Linux 功能 `dig` 來確認是否已正確架構 DNS。

請參閱第 105 頁的「針對離埠郵件設定寄件者驗證」。

新增網域金鑰

SMG 掃描程式使用網域金鑰來對離埠郵件執行 DKIM 簽署。新增網域金鑰時，SMG 會產生一個 RSA 金鑰組，其中包括公開金鑰和私密金鑰。當您從**「通訊協定」>SMTP>「網域」>「新增或編輯網域」>「傳送」**標籤啟用網域的 DKIM 簽署時，選取網域金鑰。

SMG 使用私密金鑰建立簽章，它將新增至每封離埠郵件的標頭和內文。收件者郵件伺服器使用公開金鑰來驗證郵件。

新增網域金鑰

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「網域金鑰」**標籤。
3. 按下**「新增」**。
4. 在**「網域金鑰名稱」**欄位中，輸入此網域金鑰的唯一名稱。
5. 在**「金鑰長度」**下拉式清單中，選擇 RSA 金鑰的長度 (位元)。

   預設金鑰長度為 1024 個位元。

   許多 DNS 伺服器將 DNS 記錄的長度限制在 256 個字元。長度超過 256 個字元的記錄可能會載入失敗，或者遭 DNS 伺服器截斷。若要避免發生此問題，請使用長度為 1024 個位元的 DKIM 金鑰。若要使用 1536 或 2048 位元的金鑰，請將 DNS 項目分割成多行，每行長度皆少於 256 個字元。
6. 按下**「建立」**。

如果您要使用自己的私密金鑰建立 DKIM 簽章，可以將它匯入為網域金鑰，而非新增網域金鑰。

請參閱第 109 頁的「匯入網域金鑰」。

請參閱第 106 頁的「為網域啟用 DKIM 簽署」。

匯入網域金鑰

如果您有要用來簽署離埠郵件的 RSA 私密金鑰，可以將其匯入為網域金鑰並選取它進行 DKIM 簽署。您匯入的網域金鑰必須是 PEM 格式的私密金鑰，並儲存在文字檔案中。

請參閱第 157 頁的「憑證與網域金鑰的 PEM 格式需求」。

如果網域金鑰不是 PEM 格式或無法被 OpenSSL 接受，則 Symantec Messaging Gateway 會嘗試轉換網域金鑰來修正問題。如果嘗試失敗，或金鑰或檔案不符合其他需求，匯入會失敗。

匯入網域金鑰

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「網域金鑰」**標籤。

3 按下「**匯入**」。

4 按下「**檔案名稱**」欄位旁的「**瀏覽**」，然後選取含有您要新增之網域金鑰的文字檔案。

5 在「**網域金鑰名稱**」欄位中，輸入此網域金鑰的唯一名稱。

6 按下「**匯入**」。

您在「**通訊協定**」**> SMTP >**「**網域**」**>**「**新增或編輯網域**」**>**「**傳送**」標籤上啟用 DKIM 簽署時，現在可以選取匯入的金鑰。SMG 會建立相符的公開金鑰。

請參閱第 106 頁的「為網域啟用 DKIM 簽署」。

請參閱第 109 頁的「新增網域金鑰」。

5

設定寄件者群組

本章包含以下主題：

- 啟用或停用允許的寄件者群組和攔截的寄件者群組
- 為允許的寄件者群組和攔截的寄件者群組選擇動作
- 管理寄件者群組成員
- 匯出寄件者群組資訊
- 識別寄件者的支援方法

啟用或停用允許的寄件者群組和攔截的寄件者群組

使用下列程序來啟用或停用寄件者群組。當停用寄件者群組時，Symantec Messaging Gateway 不會在信譽掃描期間使用該群組。

啟用或停用允許的寄件者群組和攔截的寄件者群組

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**或**「信譽」>「政策」>「允許的寄件者」**。

   「已啟用」欄中黑色的連字號表示目前已停用該項目。「已啟用」欄中綠色的核取記號表示目前已啟用該項目。
2. 勾選或取消勾選您要啟用或停用之群組旁邊的方塊。
3. 按下**「啟用」**或**「停用」**。

請參閱第 114 頁的「啟用或停用允許的寄件者群組和攔截的寄件者群組成員」。

請參閱第 114 頁的「編輯允許的寄件者群組和攔截的寄件者群組成員」。

為允許的寄件者群組和攔截的寄件者群組選擇動作

所有寄件者群組都有其預設動作。而您可以為任一寄件者群組選擇其他的動作。下列程序不適用於快速通過。

為允許的寄件者群組或攔截的寄件者群組選擇動作

1. 在控管中心內，按下「**信譽**」>「**政策**」>「**攔截的寄件者**」或「**信譽**」>「**政策**」>「**允許的寄件者**」。
2. 按下其中一個攔截的寄件者群組或允許的寄件者群組。
3. 在「**動作**」下，按下「**新增**」。
4. 在「**架構動作**」頁面上，按下下拉式清單，然後選擇您要新增的動作。
5. 按下「**新增動作**」。
6. 若要新增更多動作，請重複步驟 3 至 5。

   Symantec Messaging Gateway 會阻止您合併相互矛盾的動作。例如，如果出現「**延遲 SMTP 連線**」動作，則會因為無法對延遲的連線採取其他動作，而無法新增另一個動作。如果您想要新增不同的動作，請先勾選「**延遲 SMTP 連線**」旁邊的方塊，再按下「**刪除**」。

   請參閱第 285 頁的「政策動作及其功能」。
7. 若要刪除動作，請在動作清單中勾選一個動作，然後按下「**刪除**」。
8. 按下「**儲存**」。

管理寄件者群組成員

表 5-1說明您可管理寄件者群組成員的方式。您可以視需要以任何順序執行這些工作。

附註：下列主題不適用於「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、「電子郵件地址搜尋攻擊」、「電子郵件病毒攻擊」或「快速通過」。

表 5-1 管理寄件者群組成員

工作	說明
新增寄件者至群組。	若要防範不需要的郵件傳送至收件匣，可將特定的電子郵件地址、網域和連線新增至「攔截的寄件者群組」。若要確保來自特定電子郵件地址、網域和連線的郵件不被視為垃圾郵件，您可以將這些郵件新增至「允許的寄件者群組」。 請參閱第 113 頁的「新增寄件者至管理員定義之寄件者群組和第三方寄件者群組」。

工作	說明
編輯現有允許的寄件者群組成員和攔截的寄件者群組成員。	遵循這些步驟來變更寄件者資訊。 請參閱第 114 頁的「編輯允許的寄件者群組和攔截的寄件者群組成員」。
刪除允許的寄件者群組成員和攔截的寄件者群組成員。	您可以刪除不再需要的允許的寄件者群組成員或攔截的寄件者群組成員。 請參閱第 114 頁的「刪除允許的寄件者群組和攔截的寄件者群組成員」。
啟用或停用允許的寄件者群組成員和攔截的寄件者群組成員。	基於疑難排解或測試目的，您可能需要定期停用再重新啟用寄件者群組成員。 請參閱第 114 頁的「啟用或停用允許的寄件者群組和攔截的寄件者群組成員」。
匯入允許的寄件者群組檔案和攔截的寄件者群組檔案。	您可以將 LDIF 格式的文字檔匯入允許的寄件者群組和攔截的寄件者群組中。 請參閱第 115 頁的「匯入允許的寄件者組項目和攔截的寄件者群組項目」。

新增寄件者至管理員定義之寄件者群組和第三方寄件者群組

若要防範不需要的郵件傳送至收件匣，可將特定的電子郵件地址、網域和連線新增至「攔截的寄件者群組」。若要確保來自特定電子郵件地址、網域和連線的郵件不被視為垃圾郵件，您可以將這些郵件新增至「允許的寄件者群組」。您無法新增寄件者至「賽門鐵克全域允許的寄件者」或「賽門鐵克全域攔截的寄件者」群組。此程序不適用於直接電子郵件地址搜尋攻擊、電子郵件病毒攻擊或「快速通過」。

新增寄件者至管理員定義之寄件者群組和第三方寄件者群組

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**或**「信譽」>「政策」>「允許的寄件者」**。
2. 勾選允許或是攔截的寄件者群組，然後按下**「編輯」**。
3. 在**「本機允許的寄件者網域」**或**「本機攔截的寄件者網域」**頁面上，按下**「新增」**。
4. 在**「新增寄件者群組成員」**頁面上，輸入寄件者清單的適當資訊，將清單新增到目前的寄件者群組中。

   請參閱第 118 頁的「識別寄件者的支援方法」。
5. 按下**「儲存」**。
6. 在**「本機允許的寄件者網域」**或**「本機攔截的寄件者網域」**頁面上，視需要修改要對來自此寄件者群組之寄件者的郵件採取的預設動作。
7. 按下**「儲存」**。

編輯允許的寄件者群組和攔截的寄件者群組成員

遵循這些步驟來變更寄件者資訊。此程序不適用於「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、電子郵件地址搜尋攻擊、電子郵件病毒攻擊或「快速通過」。

請參閱第 114 頁的「啟用或停用允許的寄件者群組和攔截的寄件者群組成員」。

請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。

編輯允許的寄件者群組和攔截的寄件者群組成員

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**或**「信譽」>「政策」>「允許的寄件者」**。
2. 從寄件者群組清單中勾選寄件者群組，然後按下**「編輯」**。
3. 若要修改寄件者的資訊，請勾選您要修改其資訊的寄件者，然後按下**「編輯」**。

   您也可以按下加上底線的寄件者名稱，自動跳至對應的編輯頁面。
4. 在**「編輯寄件者群組成員」**頁面中，進行任何變更，然後按下**「儲存」**。
5. 按下**「儲存」**來提交變更。

刪除允許的寄件者群組和攔截的寄件者群組成員

遵循下列步驟，刪除寄件者。此程序不適用於「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、電子郵件地址搜尋攻擊、電子郵件病毒攻擊或「快速通過」。

從允許的寄件者群組和攔截的寄件者群組中刪除寄件者

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**或**「信譽」>「政策」>「允許的寄件者」**。
2. 按下其中一個攔截的寄件者群組或允許的寄件者群組。
3. 在「成員」清單中，勾選要從清單中移除之寄件者旁邊的方塊，然後按下**「刪除」**。
4. 按下**「儲存」**。

請參閱第 114 頁的「編輯允許的寄件者群組和攔截的寄件者群組成員」。

請參閱第 117 頁的「匯出寄件者群組資訊」。

請參閱第 114 頁的「啟用或停用允許的寄件者群組和攔截的寄件者群組成員」。

啟用或停用允許的寄件者群組和攔截的寄件者群組成員

在將新的寄件者新增到寄件者群組時，Symantec Messaging Gateway 會自動啟用過濾器，並且在評估內送郵件時使用。基於疑難排解或測試目的，您可能需要定期停用再重新啟用寄件者群組成員。 Symantec Messaging Gateway 會以處理其他任何郵件一樣的方式來處理已停用的寄件者所寄送的郵件。此程序不適用於「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、電子郵件地址搜尋攻擊、電子郵件病毒攻擊或「快速通過」。

啟用或停用允許的寄件者群組和攔截的寄件者群組成員

1 在控管中心內，按下**「信譽」>「政策」>「允許的寄件者」**或**「信譽」>「政策」>「攔截的寄件者」**。

2 按下其中一個允許的寄件者群組或攔截的寄件者群組。

「已啟用」欄中出現黑色破折號表示項目已停用。**「已啟用」**欄中綠色的核取記號表示目前已啟用該項目。

3 在該寄件者群組頁面上的**「成員」**清單中，執行下列其中一項工作：

- 若要恢復寄件者群組中目前已停用的成員，請勾選寄件者資訊旁邊的方塊，然後按下**「啟用」**。
- 若要停用寄件者群組中目前已啟用的成員，請勾選寄件者資訊旁邊的方塊，然後按下**「停用」**。

4 按下**「儲存」**。

請參閱第 111 頁的「啟用或停用允許的寄件者群組和攔截的寄件者群組」。

請參閱第 114 頁的「編輯允許的寄件者群組和攔截的寄件者群組成員」。

匯入允許的寄件者組項目和攔截的寄件者群組項目

使用下列程序將 LDIF 格式的文字檔匯入「允許的寄件者」群組和「攔截的寄件者」群組中。此程序不適用於「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、電子郵件地址搜尋攻擊、電子郵件病毒攻擊或「快速通過」。

對於可匯入寄件者群組中的項目數量，請注意下列限制：

- 可儲存的寄件者總數上限是 650,000 (含允許的寄件者和攔截的寄件者)。
- 匯入寄件者時，各個檔案的行數上限為 500,000。若要新增更多寄件者，請將寄件者分散至多個檔案，然後分別匯入各個檔案。
- 如果超過這些限制，不會顯示任何警告。寄件者的資料會在不顯示任何訊息的狀況下予以捨棄。

匯入允許的寄件者群組項目和攔截的寄件者群組項目

1 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**或**「信譽」>「政策」>「允許的寄件者」**。

2 勾選其中一個攔截的寄件者群組或允許的寄件者群組，然後按下**「編輯」**。

您可以在一次匯入動作中匯入所有「允許的寄件者」群組或所有「攔截的寄件者」群組內的項目 (不論開啟哪個群組)。不過，您無法匯入「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、「電子郵件地址搜尋攻擊」、「電子郵件病毒攻擊」或「快速通過」的項目。

3 按下**「匯入」**。

4 在「**匯入**」對話方塊中，指定或瀏覽至文字檔的位置，檔案中含有您要匯入的寄件者資訊。

寄件者資訊的格式必須正確。

請參閱第 116 頁的「寄件者群組匯入檔案格式」。

5 按下「**匯入**」。

Symantec Messaging Gateway 會將所匯入清單中的資料與現有的寄件者資訊合併。

6 按下「**儲存**」。

寄件者群組匯入檔案格式

針對寄件者群組匯入寄件者資訊時，請使用本節的規格。您無法匯入「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、「電子郵件地址搜尋攻擊」、「電子郵件病毒攻擊」或「快速通過」的寄件者項目。

請參閱第 115 頁的「匯入允許的寄件者組項目和攔截的寄件者群組項目」。

匯入的檔案應該是行導向，而且使用的格式要與輕量型目錄交換格式 (LDIF) 類似，而該格式具有下列限制及特性：

- 檔案必須要有必要的 LDIF 標頭。請不要變更前三個未註解行的下列值：

```
dn: cn=mailwall, ou=bmi
objectclass: top
objectclass: bmiBlackWhiteList
```

- 在標頭的後面，每一行都必須剛好包含一個屬性，以及一個對應的樣式。
- 不允許有空白行或空格。
- 會略過開頭為 # 的行。
- 以冒號、破折號樣式 (:-) 終止的項目會被停用；以冒號、加號樣式 (:+) 終止的項目則會啟用；未具有上述任一終止符號的項目也會被啟用。

若要填入清單，請指定後面接有樣式的屬性。在下列範例中，屬性及樣式清單是接在 LDIF 標頭後面。請參閱下面的屬性代碼說明。

```
## Permit List
#
dn: cn=mailwall, ou=bmi
objectclass: top
objectclass: bmiBlackWhiteList
AC: 65.86.37.45/255.255.255.0
AS: grandma@example.com
RC: 20.45.32.78/255.255.255.255
RS: spammer@example.com
```

```
BL: sbl.spamhaus.org
# Example notations for disabled and enabled entries follow
RS: rejectedspammer@example.com:-
RS: rejectedspammer2@example.com:+
```

下列表格會列出屬性及值的語法。

屬性	說明	範例

AC:	允許的連線或網路。請指定數值 IP 位址、數值 IP 位址及網路遮罩，或 Classless Inter-Domain Routing (CIDR) IP 位址。	`AC: 76.86.37.45`
		`AC: 76.86.37.45/255.255.255.0`
		`AC: 76.86.37.00/18`

RC:	拒絕或攔截的連線或網路。請指定數值 IP 位址、數值 IP 位址及網路遮罩，或 CIDR IP 位址。	`RC: 76.86.37.45`
		`RC: 76.86.37.45/255.255.255.0`
		`RC: 76.86.37.00/18`

AS:	允許的寄件者。請使用數字字母及特殊字元－不含加號 (+)，指定電子郵件地址或網域。	`AS: example.com`
		`AS: spammer@example.org`
		`AS: john?????@example.com`

RS:	拒絕或攔截的寄件者。請使用數字字母及特殊字元－不含加號 (+)，指定電子郵件地址或網域。	`RS: example.com`
		`RS: spammer@example.org`
		`RS: john?????@example.com`

BL:	攔截的第三方寄件者清單。請使用清單提供者指定的區域名稱。	`BL: sbl.spamhaus.org`
WL:	允許的第三方寄件者清單。請使用清單提供者指定的區域名稱。	`WL: allowed.example.com`

匯出寄件者群組資訊

偶爾可能要匯出寄件者群組中儲存的資料以用於另一個應用程式。請使用下列程序將寄件者群組項目匯出到文字檔。此程序不適用於「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、電子郵件地址搜尋攻擊、電子郵件病毒攻擊或「快速通過」。

請參閱第 115 頁的「匯入允許的寄件者組項目和攔截的寄件者群組項目」。

將寄件者群組資訊匯出到文字檔

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**或**「信譽」>「政策」>「允許的寄件者」**。
2. 按下其中一個攔截的寄件者群組或允許的寄件者群組。

   所有「允許的寄件者」群組或所有「攔截的寄件者」群組的項目都會匯出 (不論開啟哪個群組)。不過，您無法匯出「賽門鐵克全域允許的寄件者」、「賽門鐵克全域攔截的寄件者」、「電子郵件地址搜尋攻擊」、「電子郵件病毒攻擊」或「快速通過」的項目。
3. 按下**「匯出」**。

   瀏覽器會提示您從目前位置開啟檔案，或儲存到磁碟。

識別寄件者的支援方法

下列方法可用來辨識允許的寄件者群組和攔截的寄件者群組的寄件者：

IP 式

指定 IP 連線。

Symantec Messaging Gateway 會檢查啟動連線之郵件伺服器的 IP 位址，以驗證其位於允許的寄件者群組還是攔截的寄件者群組中。您可以指定 IPv4 位址或 IPv6 位址。

不支援萬用字元。

您可以使用標準 IPv4 格式或 IPv6 格式 (適用於單一主機)，或是 CIDR 標記法 (適用於位址範圍)。您可以使用網路遮罩指定位址範圍，但不能使用定義若干組非連續 IP 位址 (例如 69.84.35.0/255.0.255.0) 的子網路遮罩。

第三方服務

提供第三方寄件者服務的查詢網域。Symantec Messaging Gateway 可針對您訂閱的第三方 DNS 清單 (例如 list.example.org) 檢查郵件來源。

附註：使用前，請確認第三方清單的品質。賽門鐵克無法解析因使用第三方清單所導致的誤報。

網域式

指定寄件者位址或網域名稱。

Symantec Messaging Gateway 會依據清單中的特徵，檢查內送郵件的下列特徵：

- SMTP 信封中的 MAIL FROM: 位址。指定符合位址 localpart@domain 值的樣式。
- `From`：郵件標頭中的位址。指定符合 FROM: 標頭中 localpart@domain 值的樣式。

可指定網域名稱中的萬用字元，除非本機部分在前面。例如，支援 localpart@example.com 和 localpart*@example.com，但是不支援 localpart@*.example.com。

表 5-2 提供在您將成員新增到寄件者群組時，如果選擇依據位址或網域名稱辨識寄件者，可用來建立項目的範例。

表 5-2 範例

範例	相符項範例
example.com	chang@example.com, marta@example.com, john@bank.example.com
*.example.com	server1.example.com、server2.example.com
example*.com	example1.com、example2.com
malcolm@example.net	malcolm@example.net
sara*@example.org	sara@example.org, sarahjane@example.org
jo??@example.org	john@example.org, josh@example.org

6

啟用信譽過濾

本章包含以下主題：

- 啟用信譽型過濾功能
- 管理閘道的電子郵件流量
- 架構電子郵件病毒攻擊辨識
- 架構電子郵件地址搜尋攻擊辨識
- 關於使用寄件者群組攔截和允許郵件
- 關於使用快速通過來節省資源
- 防衛退回攻擊
- 研究 IP 位址信譽

啟用信譽型過濾功能

表 6-1 說明設定信譽型過濾的程序。

表 6-1　　設定信譽型過濾功能的程序

階段	動作	說明
階段 1	瞭解 Symantec Messaging Gateway 的攔截功能與技術。	請參閱第 122 頁的「關於連線時攔截與允許郵件」。 請參閱第 124 頁的「關於管理閘道的連線負載」。
階段 2	自訂郵件流參數。	架構連線類別以自訂郵件流的參數。 請參閱第 125 頁的「架構連線類別」。 請參閱第 126 頁的「連線類別預設設定」。

階段	動作	說明
階段 3	設定電子郵件病毒攻擊識別，並指定要採取的動作。	架構系統以辨識和攔截違規者。 請參閱第 127 頁的「架構電子郵件病毒攻擊辨識」。 請參閱第 128 頁的「架構電子郵件地址搜尋攻擊辨識」。 針對攔截的寄件者電子郵件指定過濾規則。 請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。 使用其他工具進行 IP 分析，以確認寄件者歷史記錄。 請參閱第 140 頁的「研究 IP 位址信譽」。
階段 4	保護系統資源。	瞭解快速通過如何防止珍貴的系統資源流失。 請參閱第 133 頁的「關於使用快速通過來節省資源」。 架構系統以辨識和快速追蹤合法寄件者，減少處理能力耗費。 請參閱第 135 頁的「架構快速通過」。
階段 5	設定退回攻擊防護。	瞭解退回攻擊以及不可傳送的收件者 (NDR) 郵件。 請參閱第 137 頁的「關於防衛退回攻擊」。 在您的控管中心提供退回攻擊防護種子值。 請參閱第 138 頁的「架構控管中心的退回攻擊防護」。 判斷並架構要讓系統套用「退回攻擊防護」的群組。 請參閱第 139 頁的「架構政策群組的「退回攻擊防護」」。 指派政策 (系統會提供預設政策) 至群組，以決定要針對未通過「退回攻擊防護」驗證之 NDR 所採取的動作。 請參閱第 140 頁的「建立退回攻擊防護的垃圾郵件或不必要的電子郵件政策」。

管理閘道的電子郵件流量

您可以在控管中心架構可用的工具，啟用專屬技術來大幅減少內送垃圾郵件，讓垃圾郵件無法襲擊您的網路。

表 6-2列出有關這些技術以及如何與閘道整合的主題。

表 6-2 管理閘道的流量

主題	說明
請參閱第 122 頁的「關於連線時攔截與允許郵件」。	Symantec Messaging Gateway 具有 Brightmail 適應性信譽管理 (Brightmail ARM) 功能。Brightmail ARM 包括設計用來減少不必要的內送電子郵件串流量、使您的網路免受攻擊，以及最佳化處理資源的使用等功能。Brightmail ARM 包括許多技術，能夠僅依據內送 IP 位址來拒絕或延遲內送連線嘗試。
請參閱第 124 頁的「關於管理閘道的連線負載」。	您可以管理連線負載，並區別已知垃圾郵件寄件者的連線與合法寄件者的連線，藉此降低處理成本。連線類別功能可根據自動收集的本機信譽資料，動態管理連線負載。
請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。	根據寄件者的網域、IP 位址或電子郵件地址過濾電子郵件，可以減少垃圾郵件和惡意軟體。
請參閱第 125 頁的「架構連線類別」。 請參閱第 140 頁的「研究 IP 位址信譽」。	這些主題說明如何架構啟用這些技術的工具。

關於連線時攔截與允許郵件

掃描電子郵件是否為垃圾郵件、惡意軟體以及其內容過濾都是十分耗費資源的工作。任何必須在經過閘道時進行處理的電子郵件，都會加重郵件基礎架構、資源容量與系統效能的負擔。Symantec Messaging Gateway 具有 Brightmail 適應性信譽管理 (Brightmail ARM) 功能。Brightmail ARM 包括設計用來減少不必要的內送電子郵件串流量、使您的網路免受攻擊，以及最佳化處理資源的使用等功能。

Brightmail ARM 包括許多技術，能夠僅依據內送 IP 位址來拒絕或延遲內送連線嘗試。為了完成這項工作，Brightmail ARM 使用動態、自我學習的本機信譽資料、全域信譽資料，以及管理員定義之攔截的寄件者政策與允許的寄件者政策。

Brightmail ARM 會依據您郵件串流中的郵件上所轉譯之允許與攔截的判斷，來產生本機信譽資料。Brightmail ARM 會運用 Brightmail IQ 服務的各種全球資料收集能力來建置全域信譽資料。Brightmail IQ 服務包括「探查網路」(賽門鐵克用來在整個 Internet 中收集垃圾郵件的數百萬個誘捕電子郵件)，以及 Global Intelligence Network。Global Intelligence Network 包括威脅偵測，及遍佈全世界由賽門鐵克安全機制應變中心所管理的安全機制應變中心。

Brightmail ARM 使用下列多種技術來達成 5 項目標：

- 在閘道即去除大部分的垃圾郵件訊息，進而減少內送電子郵件數。
- 在閘道即停止病毒、惡意軟體及電子郵件地址搜尋攻擊。
- 允許來自擁有極佳本機信譽之寄件者的郵件，以略過垃圾郵件掃描。
- 為極佳寄件者提供不中斷的連線能力，不管任何時候垃圾郵件或攻擊數量的多寡。

- 限制不合法寄件者的連線能力，保護您免於受到阻絕服務攻擊。

Symantec Messaging Gateway 能夠節省、保護並最佳化您的實體資產、郵件流及重要資料。Brightmail ARM 是入埠防護程序的第一個階段。透過檢查內送 IP 位址 (某些情況下也會檢查郵件信封)，Brightmail ARM 能夠採取預防性動作。透過拒絕或延遲不需要的連線，Brightmail ARM 能夠將寶貴的過濾循環還原給掃描程式。

Brightmail ARM 運用下列功能與技術來達成這些目標。

表 6-3

功能	說明
連線類別	「連線類別」可以為您極佳的寄件者提供極佳的連線能力，並將漸差的連線能力提供給所有其他寄件者。「連線類別」能夠確保極差寄件者無法降低極佳寄件者的連線體驗。 「連線類別」會依據本機信譽，自動將每個內送寄件者 IP 放置到 10 個類別的其中一個類別中。系統會根據每個 IP 已傳送至掃描程式的合法郵件與垃圾郵件數量來決定類別成員資格，而且會經常更新。 新的 IP 會指派給「預設」類別。「允許的寄件者」群組中的寄件者永遠都使用極佳類別 (類別 1)。「攔截的寄件者」群組中的寄件者永遠都使用極差類別 (類別 9)。 請參閱第 124 頁的「關於管理閘道的連線負載」。 請參閱第 125 頁的「架構連線類別」。
電子郵件病毒攻擊防護	如果 Symantec Messaging Gateway 從某個 IP 位址偵測到指定數目的受感染郵件，則電子郵件病毒攻擊防護就會延遲進一步的連線。或者，您可以選擇其他動作。 請參閱第 127 頁的「架構電子郵件病毒攻擊辨識」。
電子郵件地址搜尋攻擊防護	如果 Symantec Messaging Gateway 從某個 IP 位址偵測到指定數目與百分比的無效收件者，則電子郵件地址搜尋攻擊防護就會延遲進一步的連線。或者，您可以選擇其他動作。 請參閱第 128 頁的「架構電子郵件地址搜尋攻擊辨識」。
攔截的寄件者政策	您可以將寄件者新增到管理員定義的群組，並使用「賽門鐵克全域攔截的寄件者」攔截來自攔截之寄件者的電子郵件，或選擇其他動作。 請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。
允許的寄件者政策	您可以將寄件者新增到管理員定義的群組，並使用「賽門鐵克全域允許的寄件者」正常傳送來自允許之寄件者的電子郵件，或選擇其他動作。 請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。

功能	說明
快速通過	「快速通過」功能會讓具有極佳本機信譽的寄件者豁免在垃圾郵件掃描之外，藉以節省資源。Symantec Messaging Gateway 會自動收集本機寄件者信譽資料，以支援快速通過判斷，並定期重新評估寄件者授予的通行證。Symantec Messaging Gateway 只會根據將各個寄件者的郵件判定為垃圾郵件的數量，來授予和撤銷通行證。您可以將特定寄件者排除在接收過通過權之外。 請參閱第 133 頁的「關於使用快速通過來節省資源」。 請參閱第 135 頁的「架構快速通過」。

關於管理閘道的連線負載

現今多數網路中，大多數的電子郵件流量是垃圾郵件。您可以管理連線負載，並區別已知垃圾郵件寄件者的連線與合法寄件者的連線，藉此降低處理成本。連線類別功能可根據自動收集的本機信譽資料，動態管理連線負載。連線類別功能具有自動學習能力。為回應本機信譽的最新變更，「連線類別」會即時更新其連線負載管理。

附註：為了「連線類別」資料收集目的，不會將不必要的郵件計為垃圾郵件。

垃圾郵件寄發者經常會利用由受到感染的用戶端機器構成的大量網路 (稱為傀儡網路) 來進行攻擊。這樣他們就不需要透過單一 IP 位址來傳送大量郵件，因而可避免特定位址被列入全球黑名單。「連線類別」能有效防堵傀儡網路送出的垃圾郵件和大量垃圾郵件，彌補了賽門鐵克全域清單、第三方清單以及管理員定義之清單的不足。

「連線類別」可透過降低本機信譽不佳之寄件者所使用的系統資源，保護您的合法郵件流不受阻絕服務攻擊。啟用「連線類別」之後，垃圾郵件寄發者所能使用的連線數會變少。因此，系統就有較多的資源可處理合法寄件者送來的郵件。

附註：若要使用連線類別功能，您必須在閘道上部署 Symantec Messaging Gateway 硬體裝置。

「連線類別」的運作方式是根據 IP 位址所傳送的垃圾郵件數目，將每個連線 IP 位址指派至十種類別的其中一種。「連線類別」會將新的 IP 位址指派至預設類別。「連線類別」會以即時方式不斷獲取有關寄件者信譽的更多資訊，並定期變更寄件者的類別

「連線類別」可允許極佳寄件者 (類別 1) 的大多數連線。當寄件者從最佳類別移至最差類別 (類別 9) 時，該寄件者可使用的網路資源便會變少。對於「類別 9」，「連線類別」會延遲大多數連線。

「賽門鐵克全域允許的寄件者」、「本機允許的寄件者 IP」和「允許的第三方寄件者」群組中的寄件者總是會被指派至最佳類別 (類別 1)。「賽門鐵克全域攔截的寄件者」、「本機攔截的寄件者 IP」和「攔截的第三方寄件者」群組中的寄件者總是會被指派至最差類別 (類別 9)。

Symantec Messaging Gateway 分別為您系統中的每個掃描程式確定類別成員資格。相同的寄送 IP 在某個掃描程式上可能屬於類別 3，而在另一個掃描程式上可能屬於類別 4。根據每個 IP 位址所傳送的垃圾郵件數目而定，類別可能會經常變更，以動態反映最新的本機每一掃描程式的信譽。

寄件者使用您系統與網路資源時的受限程度，與該寄件者向您組織傳送垃圾郵件的信譽直接相關。系統會將沒有不良記錄的寄件者放在最佳類別，並允許比有不良記錄的寄件者更頻繁的連線。相反地，信譽不佳的 IP 位址可以減少發送垃圾郵件，多寄合法郵件，以逐漸改善其類別。

「連線類別」會依據信譽資料庫中收集的資料，判斷從指定 IP 傳送的郵件可能為垃圾郵件的機率。隨著硬體裝置收集的資料愈來愈多，可能性判斷的結果也會愈來愈精準。

Symantec Messaging Gateway 根據「連線類別」所採取的唯一動作是延遲某些 SMTP 連線。連線延遲也稱為「委婉拒絕」或「450 SMTP 錯誤」。「連線類別」會在入埠郵件流的連線階段和 SMTP 階段作業階段延遲連線。

請參閱第 87 頁的「關於電子郵件訊息流」。

必須等到硬體裝置所記錄的資料足夠做出準確的預測之後，Symantec Messaging Gateway 才會根據「連線類別」採取動作。安裝掃描程式之後，連線類別一開始會處在學習模式。必須在收到 50,000 封郵件，並將從這些郵件收集的統計資料新增到資料庫之後，學習模式才會結束。之後，如果「連線類別」是啟用狀態，則會開始進行連線管理。如果您有多個掃描程式，新安裝的掃描程式開始會處於學習模式，而您的其他掃描程式可能已經在管理連線負載。

附註：如果停用「連線類別」，掃描程式仍會繼續記錄寄件者的信譽資訊。這表示您可以暫時停用這項功能，但在這段期間不會漏失任何寄件者資料。

您可以編輯每個類別的連線參數。

請參閱第 125 頁的「架構連線類別」。

您可以查詢 IP 信譽的狀態。

請參閱第 140 頁的「研究 IP 位址信譽」。

架構連線類別

使用「連線類別」可確保信譽最佳之寄件者的連線能力不會受到信譽不佳寄件者的影響。「連線類別」會自動為內送 IP 位址分配一個類別 (共 10 個類別)。 Symantec Messaging Gateway 會自動收集本機信譽資料以通知類別。系統會為最佳類別中的寄件者指派最佳的連線參數，因為他們甚少 (或未曾) 傳送垃圾郵件。而最差類別中的寄件者則只能使用最差的連線參數。新 IP 位址一開始會被放在預設類別。

安裝之後，在系統收到50,000封郵件之前，「連線類別」都是處於學習模式。在學習模式中，系統不會根據郵件的連線類別延遲任何郵件。

「連線類別」可在沒有任何組態時運作。不過，您還是可以架構「連線類別」來自訂郵件流量的參數。使用本節中的程序可啟用、停用或架構「連線類別」。

架構連線類別

1 在控管中心內，按下**「信譽」**>**「政策」**>**「連線類別」**。

2 在**「連線類別」**頁面上，勾選**「啟用連線類別」**。

若要停用**「連線類別」**，請取消勾選該方塊。

3 若要架構「連線類別」參數，請按下**「編輯」**。

表格中的欄位會變成可編輯，而且**「編輯」**按鈕會變成**「載入預設值」**按鈕。

請參閱第 126 頁的「連線類別預設設定」。

4 若要變更每個類別的連線數目上限，請在**「連線數目上限」**列中的 10 個欄位鍵入新值。

每個值代表配置給該類別的可用連線總數的百分比。10 個值的總和必須等於 100%。在每個欄位中，您可以輸入 0.1 到 99.1 之間的值 (包含 0.1 和 99.1)。當您編輯欄位時，左邊之**「連線數目上限」**標籤下會以紅字顯示您輸入之值的總和。

5 若要變更以個別 IP 位址為基礎的允許連線數目，請在**「每個 IP 的連線數目上限」**欄位輸入新值。

6 若要變更每個連線的允許郵件數目，請在**「每個連線的郵件」**欄位輸入新值。

7 若要變更允許 IP 重新連線之前的延遲時間 (秒)，請在**「重新連線逾時」**欄位輸入新值。

8 若要變更針對每個類別延遲的連線百分比，請在**「延遲的郵件」**欄位輸入新值。

此列上的每個值代表由該類別之寄件者 IP 位址傳送的郵件中，有多少百分比的郵件會被系統延遲處理。您可以鍵入 0 到 100 之間的整數 (包含 0 和 100)。這些值的總和不需要等於 100%。

9 若要放棄變更並還原為預設值，請按下**「載入預設值」**。

10 若要提交變更，請按下**「儲存」**。

連線類別預設設定

表 6-4 顯示每個連線類別的預設值。零值表示沒有限制。

表 6-4 每個連線類別的預設值

連線類別	連線數目上限 (總和必須是 100%)	每個 IP 的連線數目上限	每個連線的郵件	重新連線逾時	延遲的郵件
預設類別	10.0%	1	1	10 秒	10%

連線類別	連線數目上限(總和必須是 100%)	每個 IP 的連線數目上限	每個連線的郵件	重新連線逾時	延遲的郵件
類別 9 (極差)	0.2%	1	1	60 秒	95%
類別 8	0.4%	1	1	30 秒	80%
類別 7	1.0%	1	1	30 秒	60%
類別 6	5.0%	1	1	15 秒	30%
類別 5	10.0%	1	5	5 秒	10%
類別 4	10.0%	25	10	2 秒	5%
類別 3	10.0%	50	20	1 秒	0%
類別 2	19.0%	100	40	1 秒	0%
類別 1 (極佳)	34.4%	200	0	0 秒	0%

請參閱第 124 頁的「關於管理閘道的連線負載」。

架構電子郵件病毒攻擊辨識

在電子郵件病毒攻擊中，會從某特定 IP 位址接收到指定數量的受感染電子郵件訊息。預設會延遲來自違規寄件者的所有連線。

請按照以下程序所述，設定電子郵件病毒攻擊辨識。電子郵件病毒攻擊辨識預設為停用，必須啟用才能加以啟動。

啟用或停用電子郵件病毒攻擊辨識

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**。
2. 若要在此頁面啟用或停用電子郵件病毒攻擊辨識，請勾選**「電子郵件病毒攻擊」**，再按下**「啟用」**或**「停用」**。

   或是繼續進行下一個步驟。
3. 按下**「電子郵件病毒攻擊」**。
4. 勾選**「啟用電子郵件病毒攻擊偵測」**來啟用電子郵件病毒攻擊辨識，或是取消勾選**「啟用電子郵件病毒攻擊偵測」**來停用電子郵件病毒攻擊辨識。

架構電子郵件病毒攻擊辨識

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**。
2. 按下**「電子郵件病毒攻擊」**。

3 接受預設值，或修改「電子郵件病毒攻擊組態」下方的值：

病毒郵件百分比下限	來自單一伺服器的病毒郵件的百分比，必須超過這個百分比才會觸發指定的動作。同時也必須超過數量下限。
病毒郵件數目下限	來自單一伺服器的病毒郵件數量，必須超過這個數量才會觸發指定的動作。同時也必須超過百分比下限。
條件限定時間視窗	在這段時間內，必須超過病毒郵件的指定百分比和數量，才會觸發指定動作。
處罰席時間	在這段時間內，Symantec Messaging Gateway 會對來自傳送 SMTP 連線的所有郵件執行指定動作。

4 在**「動作」**下，您可以：

- 接受預設的「延遲 SMTP 連線」的建議動作，並附上「稍後再試」訊息。
- 編輯動作以輸入新訊息，然後按下**「更新動作」**。
- 或是從**「如果發生電子郵件病毒攻擊」**下方的下拉式清單中選取另一個動作。

其他動作可提供其他選項讓您架構。例如，若您選擇**「封存郵件」**動作，則**「電子郵件病毒攻擊」**頁面會顯示**「選擇性封存標籤」**文字方塊及**「編碼」**下拉式清單。

5 按下**「新增動作」**，將該動作新增至 Symantec Messaging Gateway 辨識病毒攻擊後要採取動作的清單。

Symantec Messaging Gateway 會阻止您合併相互矛盾的動作。例如，您無法將某個動作加入預設動作，是因為無法對延遲的連線採取其他動作。如果您想要新增不同的動作，請先勾選**「延遲 SMTP 連線」**旁邊的方塊，再按下**「刪除」**。

請參閱第 285 頁的「政策動作及其功能」。

6 若要變更現有動作的設定，請勾選動作旁邊的方塊，然後按下**「編輯」**。

這樣會出現該動作的所有可用選項。架構選項之後，請按下**「更新動作」**。

7 按下**「儲存」**。

架構電子郵件地址搜尋攻擊辨識

垃圾郵件寄發者採用電子郵件地址搜尋攻擊，在目標網站搜尋有效的電子郵件地址。電子郵件地址搜尋攻擊的進行方式，是將大量的可能電子郵件地址傳送至網站。未防護的郵件伺服器會拒絕任何傳送到無效位址的郵件。此行為會讓垃圾郵件寄發者根據原始清單檢查遭拒絕的郵件，進而得知哪些是有效的電子郵件地址。

啟用電子郵件地址搜尋攻擊辨識之後，就會預設延遲來自違規寄件者的任何連線。擱置連線會使可能的攻擊的進度變慢，並阻止垃圾郵件寄發者保持連線。

按照以下程序所述，設定電子郵件地址搜尋攻擊辨識。電子郵件地址搜尋攻擊辨識預設為停用。您必須啟用電子郵件地址搜尋攻擊辨識，才能加以啟動。

附註： 啟用電子郵件地址搜尋攻擊辨識之前，您必須執行下列動作：

- 設定本機網域。 Symantec Messaging Gateway 只會針對您指定的網域接受入埠郵件。
  請參閱第 71 頁的「新增或編輯網域」。
- 啟用「無效的收件者處理」，架構成拒絕無效收件者。
  請參閱第 86 頁的「設定無效的收件者處理」。

啟用或停用電子郵件地址搜尋攻擊辨識

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**。
2. 若要在此頁面啟用或停用電子郵件地址搜尋攻擊辨識，請勾選**「電子郵件地址搜尋攻擊」**，再按下**「啟用」**或**「停用」**。

   或是繼續進行下一個步驟。
3. 按下**「電子郵件地址搜尋攻擊」**。
4. 勾選**「啟用 DHA 偵測」**以啟用電子郵件地址搜尋攻擊辨識，或取消勾選**「啟用 DHA 偵測」**以停用電子郵件地址搜尋攻擊辨識。
5. 按下**「儲存」**。

架構電子郵件地址搜尋攻擊辨識

1. 在控管中心內，按下**「信譽」>「政策」>「攔截的寄件者」**。
2. 按下**「電子郵件地址搜尋攻擊」**。
3. 接受預設值，或修改「電子郵件地址搜尋攻擊組態」下方的值：

錯誤收件者百分比下限	來自單一伺服器的錯誤收件者郵件的百分比，必須超過這個百分比才會觸發指定的動作。同時也必須超過數量下限。攔截的收件者郵件是指傳送到不存在於本機網域位址的郵件。
錯誤收件者數目下限	來自單一伺服器的錯誤收件者郵件的數量，必須超過這個數量才會觸發指定的動作。同時也必須超過百分比下限。
條件限定時間視窗	在這段時間內，必須超過錯誤收件者郵件的指定百分比和數量，才會觸發指定動作。
處罰席時間	在這段時間內，Symantec Messaging Gateway 會對來自傳送 SMTP 連線的所有郵件執行指定動作。

4. 在**「動作」**下，您可以：
   - 接受預設的「延遲 SMTP 連線」的建議動作，並附上「稍後再試」訊息。

- 編輯動作以輸入新訊息，然後按下**「更新動作」**。
- 或者，從如果發生**「電子郵件地址搜尋攻擊」**下方的下拉式清單中選取另一個動作。

其他動作可提供其他選項讓您架構。例如，如果您選擇**「封存郵件」**動作，則**「電子郵件地址搜尋攻擊」**頁面會顯示**「選擇性封存標籤」**文字欄位及**「編碼」**下拉式清單。

5 按下**「新增動作」**，將該動作新增至 Symantec Messaging Gateway 辨識電子郵件地址搜尋攻擊後所採取動作的清單。

Symantec Messaging Gateway 會阻止您合併相互矛盾的動作。例如，您無法將某個動作加入預設動作，是因為無法對延遲的連線採取其他動作。如果您想要新增不同的動作，請先勾選**「延遲 SMTP 連線」**旁邊的方塊，再按下**「刪除」**。

請參閱第 285 頁的「政策動作及其功能」。

6 若要變更現有動作的設定，請勾選動作名稱旁邊的方塊，然後按下**「編輯」**。

這樣會出現該動作的所有可用選項。架構選項之後，請按下**「更新動作」**。

7 按下**「儲存」**。

關於使用寄件者群組攔截和允許郵件

依據寄件者的網域、IP 位址或電子郵件地址過濾郵件，可為管理員和一般使用者提供減少垃圾郵件與惡意軟體的有效方式。

附註：本節將說明適用於您的組織伺服器層級之管理員定義群組和全域寄件者群組。若要讓一般使用者維護個人的寄件者清單，請前往「管理」>「使用者」>「群組」，啟用個人的「允許的寄件者清單」和「攔截的寄件者清單」。

請參閱第 173 頁的「啟用與停用政策群組的使用者設定」。

Symantec Messaging Gateway 可讓您利用下列方式自訂垃圾郵件偵測：

定義允許的寄件者	Symantec Messaging Gateway 會將來自「本機允許的寄件者網域」和「本機允許的寄件者 IP」群組中之位址或連線的郵件視為合法郵件。允許的寄件者群組可降低信任的寄件者所傳送郵件被視為垃圾郵件或過濾掉的小小風險。系統預設會以正常方式傳送來自這些寄件者的郵件。
定義攔截的寄件者	Symantec Messaging Gateway 支援對來自「本機攔截的寄件者網域」和「本機攔截的寄件者 IP」群組中之寄件者或連線的郵件採取許多動作。系統預設會刪除來自「本機攔截的寄件者網域」群組中之寄件者的郵件。系統預設會拒絕來自「本機攔截的寄件者 IP」和「攔截的第三方寄件者」群組中之寄件者的 SMTP 連線。但是，您可以選擇其他動作。

使用全域寄件者群組

Symantec Messaging Gateway 預設是架構為使用「賽門鐵克全域允許的寄件者」和「賽門鐵克全域攔截的寄件者」。賽門鐵克監控幾十萬個電子郵件來源，以判定從這些 IP 位址寄出的電子郵件中有多少是合法郵件，有多少是垃圾郵件。

「賽門鐵克全域允許的寄件者」是由根據賽門鐵克收集之信譽資料判定為合法之寄件者的 IP 位址所組成。「賽門鐵克全域攔截的寄件者」是由傳送大量垃圾郵件至賽門鐵克保護之郵件伺服器的 IP 位址所組成。

這兩個群組都會持續地編譯、更新，以及納入您站台上的 Symantec Messaging Gateway 過濾程序。這些清單不需要另外組態。您可以選擇停用任一清單。

系統預設會以正常方式傳送來自「賽門鐵克全域允許的寄件者」群組之寄件者的郵件。系統預設會拒絕來自「賽門鐵克全域攔截的寄件者」群組之寄件者的 SMTP 連線。但是，您可以選擇其他動作。

加入其他人管理的清單

第三方所編譯和管理的需要或不需要 IP 位址的清單。這些清單是使用 DNS 查詢進行查詢。您可以將第三方寄件者清單新增至「攔截的第三方寄件者」或「允許的第三方寄件者」群組。

系統預設會拒絕來自這些群組之攔截寄件者的 SMTP 連線，並以正常方式傳送來自這些群組之允許的寄件者的郵件。但是，您可以選擇其他動作。

附註：使用第三方清單前，請務必確認該清單的品質。賽門鐵克無法解決第三方清單所引起的誤報。

表 6-5 說明為何需要維護組織之允許寄件者的清單或攔截的寄件者清單，並提供可讓管理員用來比對寄件者的樣式範例。

表 6-5 允許的寄件者群組和攔截的寄件者群組之使用案例

問題	解決方案	樣式範例
一般使用者的同事寄送的郵件有時候會被標示為垃圾郵件。	如果針對一般使用者啟用允許的寄件者清單和攔截的寄件者清單，則該使用者可以將同事的電子郵件地址新增到其「允許的寄件者」清單。若要為一般使用者啟用此功能，請移至**「管理」>「使用者」>「政策群組」**，編輯包含一般使用者的政策群組，再按下**「一般使用者」**標籤。接著，該使用者便可以將 colleague@trustedco.com 新增到其「允許的寄件者」清單。 請參閱第 173 頁的「啟用與停用政策群組的使用者設定」。	colleague@trustedco.com
郵寄清單中需要的電子報有時候被標示為垃圾郵件。	新增 newsletter.com 至「本機允許的寄件者網域」群組。 請參閱第 113 頁的「新增寄件者至管理員定義之寄件者群組和第三方寄件者群組」。	latest@newsletter.com

問題	解決方案	樣式範例
個人將不必要的電子郵件寄送至組織中的人員。	新增 Joe.unwanted@getmail.com 至「本機攔截的寄件者網域」群組。 請參閱第 113 頁的「新增寄件者至管理員定義之寄件者群組和第三方寄件者群組」。	Joe.unwanted@getmail.com
來自特定範圍之 IP 位址的許多人將未經請求的郵件寄送至組織中的人員。	分析所接收之標頭以判斷寄件者的網路和 IP 位址之後，新增 218.187.0.0/255.255.0.0 至「本機攔截的寄件者 IP」群組。 請參閱第 113 頁的「新增寄件者至管理員定義之寄件者群組和第三方寄件者群組」。 請參閱第 118 頁的「識別寄件者的支援方法」。	218.187.0.0/255.255.0.0

在評估網域名稱是否相符時，Symantec Messaging Gateway 會自動擴充指定的網域，以包括子網域。例如，Symantec Messaging Gateway 會擴充 example.com 以包括 biz.example.com 及 jenny@foo.example.com，以確保正確允許或攔截任何可能的子網域。

請參閱第 118 頁的「識別寄件者的支援方法」。

允許的寄件者群組和攔截的寄件者群組中不能有完全相同的項目。如果其中一個群組中已存在某個項目，在您嘗試將相同的項目新增至另一個群組時，就會看見錯誤訊息。如果想要讓一個群組中的項目出現在另一個群組中，請先從目前所在的群組中刪除項目，再將項目新增到另一個群組中。

整併協力廠商清單會增加額外的過濾程序步驟。例如，類似一般的 DNS 查詢，將依據協力廠商資料庫中維護的 DNS 清單，檢查每一個內送郵件的傳送端郵件伺服器的 IP 位址。如果傳送郵件伺服器出現在清單中，則會將郵件標示為垃圾郵件。如果您的郵件相當多，則透過第三方資料庫執行內送郵件時，可能會因為必要的 DNS 查詢程序而影響效能。賽門鐵克建議您使用「賽門鐵克全域允許的寄件者」和「賽門鐵克全域攔截的寄件者」群組，而不要啟用第三方清單。

將 Symantec Messaging Gateway 部署在閘道後，它會取得內送郵件的實際或對等 IP 連線，然後與允許的寄件者群組和攔截的寄件者群組中的項目進行比對。若掃描程式部署在網路中的其他位置，例如在非內部郵件主機的閘道 MTA 的下游，Symantec Messaging Gateway 可能會將閘道伺服器的 IP 位址視為垃圾郵件的來源。您應該精確識別來自 Symantec Messaging Gateway 硬體裝置之入埠郵件流上游的所有內部郵件主機。

請參閱第 57 頁的「指定用於非閘道部署的內部郵件主機」。

除了可以新增的內部郵件主機之外，Symantec Messaging Gateway 還包括內部主機清單中的一系列 IP 位址範圍，如下所示：

- 0.0.0.0/255.0.0.0
- 10.0.0.0/255.0.0.0
- 127.0.0.0/255.0.0.0

- 169.254.0.0/255.255.0.0
- 172.16.0.0/255.240.0.0
- 192.168.0.0/255.255.0.0

Symantec Messaging Gateway 在下列判斷中會排除內部郵件主機的 IP 位址：

- 本機允許的寄件者 IP
- 本機允許的第三方寄件者
- 本機攔截的寄件者 IP
- 本機攔截的第三方寄件者
- 電子郵件地址搜尋攻擊
- 賽門鐵克全域攔截的寄件者
- 賽門鐵克全域允許的寄件者
- 連線類別
- 電子郵件病毒攻擊
- 快速通過

關於使用快速通過來節省資源

掃描電子郵件是否為垃圾郵件和不必要的郵件是一個十分耗費資源的程序。「快速通過」可讓具有不傳送垃圾郵件之示範記錄的寄件者，暫時豁免於垃圾郵件掃描之外，藉而節省資源。如果某個郵件來源已傳送指定數目的連續合法郵件 (預設為 15 封)，則會將「通過權」授予給該郵件來源。

附註：為了「快速通過」資料收集目的，會將不必要的郵件計為垃圾郵件。

一旦來源收到通行證，套用至來自該來源之郵件的防垃圾郵件處理量就會隨時間減少。隨著來自該來源的合法電子郵件越來越多，允許略過防垃圾郵件過濾的郵件數也會相應地增加。這樣會減少來自合法來源之郵件所需的處理時間，也會減少偵測垃圾郵件所需的效能。快速通過功能的設計，是以最不會減少效能的成本來提供顯著增加的效能。

如果持有通過權的郵件來源後續傳送了已取樣的垃圾郵件，則該通過權就會立即從所有 /24 範圍之違規 IP 位址的 IP 位址中撤銷。Symantec Messaging Gateway 會對來自該範圍之來源的所有郵件執行完整的防垃圾郵件分析。不過，透過再次符合所有架構的條件，該來源會保留接收其他通行證的資格。

「快速通過」會使用資料庫來儲存並分類郵件來源 IP 位址。資料庫包含下列表格：

「快速通過」試用表	包含已經過評估可能包含在「快速通過」表格中的項目。根據對 IP 位址之合法郵件的成功測試，系統會做出判斷，是否將該 IP 位址從試用表移至通過表。所有來自「快速通過」試用表之 IP 位址的郵件都會進行掃描，以確定是否為垃圾郵件和不必要的郵件。
「快速通過」表格	包含依據來自該 IP 位址的指定數目郵件中沒有任何垃圾郵件，已由「快速通過」授予通行證的項目。

您可以架構下列任一設定：

「快速通過」資料庫的大小	預設大小為 250,000 個 IP 位址；您可以將此變更為 1,000 到 1,000,000 (含) 之間的任何整數。25% 的資料庫保留供「快速通過」表格使用。剩餘的 75% 保留供「快速通過」試用表使用。
「快速通過」試用表的成長速率	指定當不明 IP 位址在傳送合法郵件時，該 IP 位址新增至「快速通過」試用表的可能性。您可以指定任何從 1/1 可能性到 1/100 可能性 (含) 的任何 (整數) 可能性。僅輸入分數中的分母來表示可能性。預設值為 3，表示 1/3 或三分之一的可能性。請注意，該數字只是可能性，而非必然值。例如，如果設定為 1/3，則可能會出現未新增連續 5 個不同的不明 IP，或新增 2 個同一列 IP 等情況。
「快速通過」表格的成長速率	指定在將「快速通過」試用表中的 IP 位址新增到「快速通過」表格之前所需的連續合法郵件數目。您可以指定介於 1 和 1,000 (含) 之間的任何整數 (不含逗號)。預設設定是 15。
將通行證發給某個 IP 位址之後，對郵件進行垃圾郵件掃描的初始可能性	隨著 IP 位址繼續傳送合法郵件，此取樣率會隨之降低。您可以指定介於 2 和 50 (含) 之間的整數。僅指定分數中的分母來表示可能性。預設值為 5，表示 1/5 或五分之一的可能性。
無法授予通行證的 IP 位址清單	您可以新增個別 IP 位址，或匯入 IP 位址清單，來建立此清單。

任一表格達到架構的限制時，「快速通過」就會放棄最近使用的項目，才能為下一個項目挪出空間。

請注意，「快速通過」只會將寄件者豁免在垃圾郵件掃描之外。系統會對來自擁有通過權之寄件者的郵件進行病毒與內容過濾。但是，因為這些郵件都不會進行垃圾郵件掃描，所以它們無法接收到「可疑垃圾郵件」或「垃圾郵件」判斷。

隸屬於「本機允許的寄件者 IP」或「賽門鐵克全域允許的寄件者」寄件者群組之寄件者不會收到通行證。不過，這些寄件者已經排除在垃圾郵件掃描之外。

「快速通過」資料庫只會將垃圾郵件、可疑垃圾郵件和不必要的郵件判斷列入考慮。病毒判斷、內容過濾判斷、寄件者驗證判斷，以及寄件者群組判斷都不會影響通過權的授予或撤銷。

請參閱第 135 頁的「架構快速通過」。

架構快速通過

Symantec Messaging Gateway 會自動在每個 IP 位址傳送之垃圾郵件及不必要的郵件的層級收集資料，並使用此資料來授予或撤銷郵件的通行證。 當 Symantec Messaging Gateway 對寄件者授予通行證後，仍會少量取樣掃描該寄件者傳送的電子郵件，以確定是否為垃圾郵件及不必要的郵件。 如果 Symantec Messaging Gateway 發現垃圾郵件或不必要的郵件，它會立即撤銷該寄件者之郵件的通行證。

「快速通過」功能預設不啟用。啟用「快速通過」可大幅節省處理資源。不需要設定自訂組態即可開始使用「快速通過」，但您可視需要予以自訂。

請參閱第 133 頁的「關於使用快速通過來節省資源」。

啟用或停用快速通過

1. 在控管中心內，按下**「信譽」>「政策」>「允許的寄件者」**。
2. 按下**「快速通過」**。
3. 勾選**「啟用快速通過」**來啟用「快速通過」，或取消勾選**「啟用快速通過」**來停用「快速通過」。

架構快速通過

1. 在控管中心內，按下**「信譽」>「政策」>「允許的寄件者」**。
2. 按下**「快速通過」**。
3. 按下**「顯示進階」**。
4. 在**「資料庫中追蹤的寄送 IP 數目上限」**欄位中，輸入介於 1,000 到 1,000,000 之間的整數以變更資料庫大小。

   不要鍵入逗號。 資料庫包含兩個表格。「快速通過」試用表包含要評估是否讓其郵件通過的寄送 IP 位址，而且限制為資料庫大小上限的 75%。「快速通過」表包含目前具有通過授權的寄送 IP，而且限制為資料庫大小上限的 25%。

   預設值為 250,000。
5. 在**「將新 IP 新增到快速通過試用表的可能性」**欄位中，輸入介於 1 到 100 之間的整數，以變更「快速通過」試用表的成長速率。

   較小的值會產生較頻繁的取樣。 例如，值 1 表示傳送合法郵件的每個新 IP 都會新增至該表格。 值 5 表示不在「快速通過」試用表中的新寄送 IP 有 20% (1/5 或五分之一) 的機率會新增至該表格。 所有來自「快速通過」試用表之 IP 位址的郵件都會進行掃描，以確定是否為垃圾郵件和不必要的郵件。 如果收到垃圾郵件或不必要的郵件，寄送 IP 位址的整個 /24 範圍都會從「快速通過」試用表和「快速通過」表格移除。

   預設值為 3，表示三分之一的可能性。

6 在**「授予通行證前所需的合法郵件數目下限」**欄位中，輸入介於 1 到 1,000 之間的整數，以變更「快速通過」表格的成長速率。

不要鍵入逗號。當 IP 進入「快速通過」試用表之後，此值表示系統將該 IP 移至「快速通過」表格之前，必須從該 IP 接收的合法郵件數目。若收到任何垃圾郵件，將會導致該 IP 位址的整個 /24 範圍從兩個表格中移除。

預設值為 15。

7 在**「發行通行證後的初始郵件取樣率」**欄位中，輸入 2 到 50 之間 (包含 2 與 50) 的整數，以變更針對目前行為受到檢查且具有通行證之 IP 位址的速率。

較小的值會產生較頻繁的取樣。例如，值 2 表示對於剛取得通行證的 IP 位址，系統會掃描該 IP 傳送之郵件的一半郵件 (每 2 封就掃描 1 封) 是否為垃圾郵件及不必要的郵件。值 25 表示每收到 25 封就會掃描其中 1 封郵件。後續從 IP 位址接收其他合法郵件時，系統會調整初始取樣率，以降低取樣的郵件數目。取樣率不能低於初始取樣率的五分之一。例如，8 的初始取樣率會隨著處理其他合法郵件而逐漸降低，直到取樣率變成每 40 封檢查 1 封。

預設值為 5，表示五分之一的可能性。

排除不授與快速通過的 IP

1 在控管中心內，按下**「信譽」**>**「政策」**>**「允許的寄件者」**。

2 按下**「快速通過」**。

3 按下**「顯示進階」**。

4 在**「快速通過排除」**下的**「IP 位址」**欄位中，鍵入要予以排除而不想為其授與通行證的 IP 位址。

您可以鍵入多個 IP 位址，每個 IP 位址之間必須以逗號分隔。您可以使用 CIDR 標記法鍵入完整的 IP 位址或多個 IP 位址。不支援萬用字元。如果指定主機名稱，會損失「快速通過」的部分效能優勢，因為 Symantec Messaging Gateway 接著需要查詢每封所取樣郵件之 IP 的主機名稱，以確保其不符合您已指定要排除的主機名稱。

5 按下**「匯入」**以匯入 IP 位址清單。

要匯入的檔案必須是純文字格式，而且每行只能包含一個項目。

6 勾選 IP 位址旁邊的方塊，然後按下**「刪除」**，以從清單中刪除項目。

7 按下**「全部刪除」**可刪除清單目前頁面的所有項目。

8 按下**「匯出」**可將目前儲存之已排除 IP 的清單匯出到文字檔。

防衛退回攻擊

您可以啟用 Symantec Messaging Gateway 的退回攻擊防護技術，來移除不可傳送的收件者 (NDR) 郵件，這類郵件通常是垃圾郵件寄發者使用重新導向技術的結果。

表 6-6說明實作退回攻擊防護的程序。

表 6-6 退回攻擊防護

步驟	工作	說明
步驟 1	深入瞭解退回攻擊以及 Symantec Messaging Gateway 如何能協助您防範這類攻擊。	垃圾郵件寄發者可以在傳送垃圾郵件時採取退回攻擊手段，以利用初始收件者的良好信譽、敗壞初始收件者的IP信譽，或針對目標伺服器發動阻絕服務攻擊。 請參閱第 137 頁的「關於防衛退回攻擊」。
步驟 2	架構控管中心設定以執行退回攻擊防護。	您必須在控管中心架構種子值。種子值會用來計算標籤，該標籤將附加到外寄郵件，並在郵件遭退回時用來驗證該郵件。 請參閱第 138 頁的「架構控管中心的退回攻擊防護」。
步驟 3	架構政策群組以使用退回攻擊防護。	在「控管中心設定」頁面中架構「退回攻擊防護」之後，您必須啟用系統應套用驗證的政策群組，並指派「退回攻擊防護」政策。 請參閱第 139 頁的「架構政策群組的「退回攻擊防護」」。
步驟 4	建立防止退回攻擊的政策。	最後，您必須針對政策群組啟用退回攻擊防護。指派垃圾郵件政策或不必要的郵件政策，此類政策描述了在郵件無法通過退回攻擊驗證時，您要 Symantec Messaging Gateway 採取的動作。 請參閱第 140 頁的「建立退回攻擊防護的垃圾郵件或不必要的電子郵件政策」。

關於防衛退回攻擊

當垃圾郵件寄發者透過使用某個電子郵件伺服器將垃圾郵件退回至其他伺服器上的位址，以隱藏郵件來源時，就會發生退回攻擊。為發動此類型攻擊，垃圾郵件寄發者會將目標位址插入郵件信封的 Mail From 值，然後將這些郵件傳送到另一個位址。

如果初始收件者發現郵件無法傳送，該郵件伺服器就會將偽造的 Mail From 值辨識成原始寄件者，然後將郵件傳回或「退回」該目標。如果目標系統將退回郵件的伺服器辨識為合法寄件者，就會將郵件視為合法的未傳遞回報 (NDR) 郵件。

垃圾郵件寄發者可以在傳送垃圾郵件時採取退回攻擊手段，以利用初始收件者的良好信譽、敗壞初始收件者的 IP 信譽，或針對目標伺服器發動阻絕服務攻擊。

將系統架構為採用退回攻擊防護之後，Symantec Messaging Gateway 會計算出唯一的標籤，該標籤會使用提供的種子值以及當天的日期。您的掃描程式會將此標籤附加到您定義之政策群組中的使用者所傳送的離埠郵件。

附註：為了成功處理，您必須同時確保透過硬體裝置繞送所有適用的離埠郵件。

如果郵件因無法傳送而被傳回，信封的回覆位址將包含此標籤。

如果系統接收的是無法傳送之傳回郵件，系統就會比對入埠郵件的收件者與政策群組組態，以查看使用者的政策群組是否架構成採用退回攻擊防護。如果已架構該政策群組，則系統會計算新的標籤 (其中包含種子值與當時日期)，然後使用新的標籤驗證電子郵件中的標籤。

入埠 NDR 上的有效標籤將包含下列項目：

- 正確的標籤格式
- 符合新計算的標籤種子值之種子值
- 計算新標籤當週的日期

Symantec Messaging Gateway 將會根據此評估執行下列動作：

- 如果系統判斷標籤有效，則會從信封刪除標籤，然後轉寄該郵件以根據您的郵件過濾組態進行過濾與傳送。
- 如果沒有標籤或標籤內容不符合計算用來驗證的標籤，則系統會改寫位址並去除標籤資訊，然後根據您的退回攻擊防護政策組態進行管理。系統會記錄錯誤，並將此郵件列入郵件統計資料作為具有「單一威脅」的郵件。此郵件也會包含在您的系統垃圾郵件統計資料中作為「退回威脅」。
  在您的政策組態中，如果您不是為無法通過驗證的郵件指定「拒絕」動作，則該郵件可能會產生更多威脅，接著會計入您的統計資料中作為「多個威脅」。
- 如果系統因為無法識別的格式而無法執行驗證，則不會刪除該標籤，而且會將該標籤保留為位址的一部分。接著，系統會根據您在垃圾郵件政策組態中定義的動作針對此郵件採取動作。

附註：超於 50k 的退回郵件會被截斷。遭截斷之郵件中的附件可能無法讀取。

請參閱第 136 頁的「防衛退回攻擊」。

架構控管中心的退回攻擊防護

您必須在控管中心架構「退回攻擊防護」，方法是提供可用來計算標籤的種子值，而該標籤將附加到外寄郵件，並在郵件遭退回時用來驗證該郵件。

請參閱第 137 頁的「關於防衛退回攻擊」。

建立種子值，以在建立外寄郵件的驗證標籤時使用

1 在控管中心內，選取**「管理」>「設定」>「控管中心」**。

2 按下**「憑證」**標籤。

3 在**「控管中心憑證」**下，輸入**「退回攻擊防護種子」**。

這個種子值應該包含八個英數字元。

4 按下**「儲存」**。

警告：如果您利用不同的控管中心來執行不同掃描程式上的入埠與離埠郵件，請使用相同的種子值，為每個控管中心重複步驟 1 到 3。這樣可確保所有入埠與離埠伺服器都會針對驗證計算相同的標籤。

附註：為能順利處理，您必須確保透過硬體裝置繞送所有適用的離埠郵件。

現在，您必須啟用政策群組的「退回攻擊防護」，並指派垃圾郵件政策，該政策描述在郵件無法通過退回攻擊驗證時將採取的動作。如果您未啟用至少一個政策群組的「退回攻擊防護」，則「退回攻擊防護」將停用，且不會保護您的系統抵禦退回攻擊。

請參閱第 139 頁的「架構政策群組的「退回攻擊防護」」。

提供了預設垃圾郵件政策，稱為「無法通過退回攻擊驗證：拒絕郵件」。您可以依原狀使用此政策、加以編輯，或是建立您自己的政策。

請參閱第 140 頁的「建立退回攻擊防護的垃圾郵件或不必要的電子郵件政策」。

架構政策群組的「退回攻擊防護」

在「控管中心設定」頁面中架構「退回攻擊防護」之後，您必須啟用系統應套用驗證的政策群組，並指派「退回攻擊防護」政策。

請參閱第 137 頁的「關於防衛退回攻擊」。

架構政策群組的「退回攻擊防護」

1 在控管中心內，選取**「管理」>「使用者」>「政策群組」**。

2 選取要編輯的政策群組，或建立新的政策群組，然後選取該政策群組的**「垃圾郵件」**標籤。

3 在**「電子郵件」**下，勾選**「啟用此政策群組的退回攻擊防護」**。

4 在**「退回攻擊防護政策」**中，選取想要套用至退回之郵件的政策。

此政策必須包含「如果郵件無法通過退回攻擊驗證」條件，而且採取的動作應該會讓退回位址標籤驗證失敗。Symantec Messaging Gateway 會提供一個預設政策：「無法通過退回攻擊驗證: 拒絕郵件」。此預設政策的架構是要拒絕無法通過標籤驗證的郵件。

您也可以編輯此政策，或建立新的政策。

請參閱第 140 頁的「建立退回攻擊防護的垃圾郵件或不必要的電子郵件政策」。

5 按下**「儲存」**。

為能順利處理，您必須確保透過硬體裝置繞送所有適用的離埠郵件。

建立退回攻擊防護的垃圾郵件或不必要的電子郵件政策

若要啟用「退回攻擊防護」，您必須啟用「退回攻擊防護」的政策群組，並指派垃圾郵件政策或不必要的電子郵件政策，此類政策描述了在郵件無法通過退回攻擊驗證時將採取的動作。

請參閱第 137 頁的「關於防衛退回攻擊」。

Symantec Messaging Gateway 提供預設的退回政策，名為「無法通過退回攻擊驗證： 拒絕郵件」。這個預設的政策提供一個動作，也就是拒絕未通過標籤驗證的所有郵件。您可以編輯此政策以變更要採取的動作，或視需要建立新的政策。

建立退回攻擊防護條件的垃圾郵件或不必要的電子郵件條件政策

1 在控管中心內，按下**「垃圾郵件」>「政策」>「電子郵件」**。

2 按下**「新增」**以建立新政策。

3 輸入新政策的名稱，並在**「如果符合下列條件:」**中，選取「如果郵件無法通過退回攻擊驗證」。

「套用至」欄位會自動設為「入埠郵件」並停用。您只能針對此條件架構入埠政策。離埠政策是固定的，無法修改。

4 選取退回郵件無法通過驗證時應該套用的動作。系統提供「拒絕未通過退回攻擊驗證的郵件」動作，或者您也可以視需要選取任何其他動作。

請務必考慮現有的垃圾郵件政策，以及這樣做會對整體電子郵件組態造成什麼影響。

5 在**「套用至下列政策群組」**下，選取要套用此政策的政策群組。

6 按下**「儲存」**。

研究 IP 位址信譽

使用**「IP 信譽查閱」**頁面可以研究特定 IPv4 或 IPv6 位址的歷史和目前的統計資訊。您可以檢視目前含有該 IP 位址的寄件者群組 (如果有)、將 IP 位址新增到「本機允許的寄件者 IP」或「本機攔截的寄件者 IP」寄件者群組，或清除該 IP 位址目前的寄件者政策。清除寄件者政策

時，Symantec Messaging Gateway 會移除「本機允許的寄件者 IP」或「本機攔截的寄件者 IP」群組中的 IP 位址。

您也可以重設 IP 位址的本機信譽 (而清除用來管理該 IP 位址連線的資料)。頁面會顯示指定的 IP 位址從上次重設垃圾郵件信譽以來所收集到的資料。

IP 信譽功能可以在流量穿過您組織閘道但尚未進入網路前，進行轉譯判斷。這個功能的最大優點是，它可以在流量尚未進入您的網路並使用資源時，就拒絕或延遲信譽不佳的連線。當 Symantec Messaging Gateway 部署在網路邊緣時，此功能的效果最好。不過，如果 Symantec Messaging Gateway 是部署在您網路內的轉遞站後面或其他位置，仍可以依據收到的標頭內容進行判斷。

附註：除非您已架構 Symantec Messaging Gateway 持續儲存歷史資料，否則此頁面上無法提供歷史資料。您可以在**「管理」>「設定」>「報告」**頁面上進行架構。勾選**「報告資料儲存」**下的**「寄件者 IP 連線」**，然後按下**「儲存」**。

檢查 IP 位址的目前與歷史資訊

1. 在控管中心內，按下**「信譽」>「信譽工具」>「IP 信譽查閱」**。
2. 指定您要查詢的 IPv4 位址或 IPv6 位址。

   您可以用任何標準 IPv6 格式指定個別的 IPv6 位址。
3. 按下**「尋找」**。

隨即顯示您所指定之 IP 位址的下列資訊：

表 6-7 信譽狀態

項目	說明
新增至本機允許的寄件者 IP	按下以將此 IP 位址加入您的「本機允許的寄件者 IP」群組。預設會允許來自「本機允許的寄件者 IP」之 IP 位址的連線，且郵件會略過垃圾郵件過濾。
新增至本機攔截的寄件者 IP	按下以將此 IP 位址加入您的「本機攔截的寄件者 IP」群組。預設會拒絕來自「本機攔截的寄件者 IP」之 IP 位址的連線。
清除寄件者政策	按下以從「本機攔截的寄件者 IP」或「本機允許的寄件者 IP」群組中，移除此 IP 位址。
不良信譽 - 全域攔截的寄件者	如果此 IP 位址位於「賽門鐵克全域攔截的寄件者」群組，則會出現綠色核取符號。如果不是，則會出現黑色破折號。如果停用「攔截的寄件者」頁面上的「賽門鐵克全域攔截的寄件者」群組，此欄就會變成灰色。

項目	說明
要求移除	此連結只有當IP位址位於「賽門鐵克全域攔截的寄件者」群組時才會出現。按下連結以要求賽門鐵克將此IP位址從「賽門鐵克全域攔截的寄件者」中移除。
不良信譽 - 本機攔截的寄件者 IP	如果此IP位址位於「本機攔截的寄件者IP」群組，則會出現綠色核取符號。如果不是，則會出現黑色破折號。如果停用「攔截的寄件者」頁面上的「本機攔截的寄件者 IP」群組，此欄就會變成灰色。
良好信譽 - 全域允許的寄件者	如果此IP位址位於「賽門鐵克全域允許的寄件者」群組，則會出現綠色核取符號。如果不是，則會出現黑色破折號。如果停用「允許的寄件者」頁面上的「賽門鐵克全域允許的寄件者」群組，此欄就會變成灰色。
良好信譽 - 本機允許的寄件者 IP	如果此IP位址位於「本機允許的寄件者IP」群組，則會出現綠色核取符號。如果不是，則會出現黑色破折號。如果停用「允許的寄件者」頁面上的「本機允許的寄件者 IP」群組，此欄就會變成灰色。

附註：IP 位址可以位於「本機允許的寄件者 IP」群組或「本機攔截的寄件者 IP」群組，但不能同時屬於這兩個群組。因此，如果 IP 位址目前位於其中一個群組，則新增按鈕就會變成灰色。您可以按下其他群組的這個按鈕，將該 IP 位址從某一個群組切換到另一個群組。

表 6-8 本機狀態

項目	說明
重設狀態	按下並確認此動作後，Symantec Messaging Gateway 便會「忘記」此寄件者之前的所有信譽資料。此動作會清除**「目前的動作」**、**「郵件數」**及**「垃圾郵件百分比」**欄。不過，如果寄件者屬於「本機允許的寄件者 IP」、「本機攔截的寄件者 IP」或「快速通過」等寄件者群組中之任何一個群組，則寄件者仍會保留在這些群組中。若要將寄件者從這些寄件者群組的任何一個當中移除，請按下**「清除寄件者政策」**。按下**「重設狀態」**也會將寄件者移到預設的「連線類別」類別。 請參閱第 124 頁的「關於管理閘道的連線負載」。
掃描程式	已偵測到來自此IP位址之流量的掃描程式。安裝中的每一個掃描程式都會有自己的線路。

項目	說明
目前的動作	這一行會顯示依據「IP 信譽」資料庫中的資訊，對此 IP 位址的連線所採取的動作。 可針對來自指定 IP 位址的連線指派下列其中一個動作： ■ 拒絕：此 IP 位址位於「攔截的寄件者」群組，而且該群組的動作是拒絕 SMTP 連線。 ■ 延遲：此 IP 位址位於「攔截的寄件者」群組，而且該群組的動作是延遲 SMTP 連線。 ■ 過濾時略過： 此 IP 位址位於「允許的寄件者」群組，該群組的動作是照常傳送。雖然 Symantec Messaging Gateway 不會過濾來自此 IP 位址的郵件是否有垃圾郵件，但仍會針對這些郵件進行所有其他的過濾，包含防毒過濾。 ■ 部分過濾： 此 IP 位址已由快速通過功能授予通過權。在大多數情況下，Symantec Messaging Gateway 不會過濾來自此 IP 位址的郵件以確定是否有垃圾郵件。不過，Symantec Messaging Gateway 還是會過濾取樣的郵件，以確定是否有垃圾郵件。所有的郵件都會受到所有其他的過濾，包括防毒過濾。 ■ 正常過濾：此 IP 沒有負面的本機或全域信譽，且已由「快速通過」功能授予通過權。
郵件數	來自此 IP 位址的郵件數量。會出現下列四個值之一： ■ 無 (這是預設值) ■ 低 ■ 中 ■ 高
垃圾郵件百分比	來自此 IP 的郵件中，被識別為垃圾郵件的郵件所佔之百分比
連線類別	指派給這個掃描程式之此 IP 位址的連線類別 (1-9 或預設)。IP 位址若屬於較高 (較差) 的類別，則來自該 IP 位址的連線被「連線類別」延遲的比例較高。IPv6 位址的連線類別始終為「1」。
快速通過	如果此 IP 位址目前已由此掃描程式上的「快速通過」功能授予通過權，則此欄中會出現綠色勾號。如果不是，則會出現黑色破折號。不支援 IPv6 位址。
電子郵件地址搜尋攻擊	如果此 IP 位址依據您在**「信譽」>「攔截的寄件者」>「電子郵件地址搜尋攻擊」**中的設定而受到「電子郵件地址搜尋攻擊」的限制，則會出現綠色勾號。如果不是，則會出現黑色破折號。不支援 IPv6 位址。
病毒攻擊	如果這個 IP 位址依據您在**「信譽」>「攔截的寄件者」>「電子郵件病毒攻擊」**中的設定而受到「病毒攻擊」的限制，就會出現綠色勾號。如果不是，則會出現黑色破折號。不支援 IPv6 位址。
上封郵件	上次從這個 IP 位址偵測到流量的時間。

表 6-9 本機連線記錄

項目	說明
時間範圍	選擇「本機連線記錄」表格中顯示資料的時間範圍。您可以選擇「過去 1 小時內」、「過去 1 天內」或「過去 1 週內」。
已嘗試	此 IP 位址在指定的時間範圍內所嘗試的連線數。
已接受	此 IP 位址在指定的時間範圍內所接受的連線數。
已拒絕	此 IP 位址在指定的時間範圍內所拒絕的連線數。
已延遲	此 IP 位址在指定的時間範圍內所延遲的連線數。

檢查網域、電子郵件地址或 IP 位址的寄件者群組成員資格

1 在控管中心內，按下**「信譽」>「信譽工具」>「尋找寄件者」**。

2 輸入網域、電子郵件地址或 IP 位址。

3 按下**「尋找寄件者」**。

如果寄件者屬於下列任一群組，則會出現群組名稱：

- 本機攔截的寄件者網域
- 本機攔截的寄件者 IP
- 攔截的第三方寄件者
- 本機允許的寄件者網域
- 本機允許的寄件者 IP
- 允許的第三方寄件者

7

設定憑證

本章包含以下主題：

- 關於憑證
- 使用憑證
- 憑證與網域金鑰的 PEM 格式需求
- 檢視 SMTP/TLS 或 HTTPS 憑證
- 匯出 TLS 與 HTTPS 憑證
- 刪除 SMTP/TLS 或 HTTPS 憑證
- 指派 MTA TLS 憑證給掃描程式
- 指派使用者介面 HTTPS 憑證給控管中心

關於憑證

憑證會保護及驗證用戶端與伺服器 IP 位址或網域之間的通訊。您可以產生自行簽署的憑證，也可以匯入由憑證授權中心 (CA) 授予的已簽署憑證。

請注意這些憑證類型之間的差異：

- 憑證授權中心尚未簽署自行簽署的憑證。
- 根憑證授權中心憑證 (根 CA 憑證) 是識別特定憑證授權中心的憑證。
- 中繼憑證授權中心憑證 (中繼 CA 憑證) 可識別另一個對憑證具有責任的相關方，且可能需要此憑證為憑證簽章提供完整的驗證鏈結。
- 憑證授權中心已簽署憑證授權中心簽署的憑證。為了確保憑證授權中心簽署的憑證可被接受為有效憑證，請確定簽署憑證之憑證授權中心的 CA 憑證顯示在**「憑證設定」**頁面**「憑證授權中心」**標籤的**「CA 憑證」**清單中。

若要成功使用 CA 憑證來進行 HTTPS 驗證，必須有從用戶端憑證到 CA 憑證的完整「路徑」或「鏈結」。此外，協議中的雙方參與者也必須能夠辨識簽署權限。Symantec Messaging Gateway 已預先安裝最常見憑證授權中心廠商的根 CA 憑證。**「憑證設定」**頁面上的**「憑證授權中心」**標籤會列出預先安裝的 CA 憑證。您可以新增額外的根憑證或中繼 CA 憑證。部分憑證發照者需要並提供中繼 CA 憑證，以為其所發行的憑證取得更佳的安全性。

對於使用 CA 憑證進行的 SMTP/TLS 驗證，即使從用戶端憑證至 CA 憑證的路徑或鏈並不完整，Symantec Messaging Gateway 也允許您使用憑證。

請在新增憑證之後，將其指派給控管中心，以保護網頁式通訊的安全，或指派給掃描程式 MTA，以支援 TLS 加密。

MTA TLS 憑證	每個掃描程式中的入埠、離埠和驗證郵件程序都會使用指派給它們的 TLS 憑證，以接受要進行掃描的郵件及傳送 TLS 加密的郵件。 請參閱第 159 頁的「指派 MTA TLS 憑證給掃描程式」。
使用者介面 HTTPS 憑證	控管中心會使用 HTTPS 憑證來確保網頁瀏覽器的通訊安全無虞。 請參閱第 160 頁的「指派使用者介面 HTTPS 憑證給控管中心」。

附註：在購買或產生憑證時，必須能夠指定是準備將它用於 SMTP/TLS 還是 HTTPS。憑證授權中心除了憑證本身，可能還需要您匯入中繼 CA 憑證。請確定已安裝從憑證授權中心獲得的憑證與所有中繼憑證。

您可以使用下列其中一種方式，將 CA 簽署的憑證新增到可用憑證清單中：

- 完成**「新增憑證」**頁面，以產生自行簽署的憑證。自行簽署的憑證可立即用於控管中心和掃描程式 MTA 在接受 TLS 加密時的 HTTPS 憑證。
- 將您在**「新增憑證」**頁面中產生的憑證簽署要求傳送到憑證授權中心，以新增憑證授權中心簽署的憑證。當您從憑證授權中心收到憑證時，請將其儲存在本機上並匯入至控管中心，以將它新增至可用憑證清單。
- 匯入先前從 Symantec Messaging Gateway 硬體裝置匯出的憑證授權中心簽署的憑證。
- 使用僅有效期限不同的新憑證更新現有憑證授權中心簽署的憑證。
- 新增憑證授權中心簽署的憑證，而不必在控管中心產生憑證簽署要求。您必須先修改憑證。憑證必須使用 PEM 格式。

請參閱第 146 頁的「使用憑證」。

使用憑證

您可以透過控管中心設定憑證。

表 7-1 說明您可使用憑證執行的工作。您可以視需要以任何順序執行這些工作。

表 7-1 使用憑證

工作	說明
新增自行簽署的憑證。	自行簽署的憑證可用於 HTTPS 通訊或 SMTP/TLS。有些郵件伺服器可能無法辨識用於 SMTP/TLS 的自行簽署憑證。很多郵件伺服器都要求使用憑證授權中心簽署的憑證。 請參閱第 148 頁的「新增自行簽署的憑證」。
決定您要使用哪一種方式來新增憑證授權中心簽署的憑證。	本主題說明您可使用哪些方法來新增憑證授權中心簽署的憑證。 請參閱第 148 頁的「新增認證中心簽署憑證的方法」。
透過匯入方式新增憑證授權中心簽署的憑證。	您可以新增憑證授權中心簽署的憑證，而不必在控管中心產生憑證簽署要求。 請參閱第 149 頁的「修改憑證授權中心簽署憑證匯入檔案」。
新增自己的 CA 或中繼憑證。	Symantec Messaging Gateway 已預先安裝許多常見憑證授權中心廠商的 CA 憑證。如果憑證授權中心為您簽署了 SMTP/TLS 或 HTTPS 憑證，但控管中心內尚不存在該憑證授權中心的 CA 憑證，則請新增 CA 憑證。 若憑證需要中繼 CA 憑證，也會新增 CA 憑證。當您新增 CA 憑證時，須完成憑證鏈結，以允許驗證憑證授權中心簽署的憑證。 請參閱第 150 頁的「新增 CA 或中繼憑證」。
請查看包含您所有 CA 憑證的詳細目錄。	您可以檢視目前安裝的 CA 憑證清單。 請參閱第 151 頁的「檢視現有的 CA 憑證」。
要求憑證授權中心簽署的憑證。	對於 SMTP/TLS 通訊而言，憑證授權中心簽署的憑證可能比自行簽署的憑證更有效，並且還可以用於 HTTPS 通訊。控管中心的**「憑證授權中心」**標籤上列有一些可用的 CA，但也支援其他 CA。 請參閱第 151 頁的「要求憑證授權中心簽署的憑證」。
將憑證授權中心簽署的憑證匯入控管中心。	您從憑證授權中心 (CA) 收到憑證時，必須將其匯入，以在控管中心內使用。除了此憑證之外，CA 可能也寄送中繼 CA 憑證給您，必須將其在控管中心加以安裝。 請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。
在不同的 Symantec Messaging Gateway 硬體裝置上匯出要匯入的憑證或儲存成備份。	您不需要匯入前修改憑證匯入檔案。 請參閱第 158 頁的「匯出 TLS 與 HTTPS 憑證」。
使用另一組 CA 憑證取代控管中心所有現有的 CA 憑證。	所有現有的 CA 憑證均將移除，並以所指定之檔案中的 CA 憑證加以更換。 請參閱第 153 頁的「取代所有現有的 CA 憑證」。

工作	說明
備份 CA 憑證。	您可以備份安裝於控管中心的 CA 憑證。 請參閱第 153 頁的「備份 CA 憑證」。
變更憑證或網域金鑰名稱。	您無法修改憑證的任何其他部分。若要變更憑證的其他部分，您必須建立新的憑證。 請參閱第 153 頁的「變更憑證或網域金鑰名稱」。
匯入、匯出和使用應用程式憑證。	您可以視需要匯入和匯出應用程式憑證，也可以編輯、檢視和刪除這些憑證。 請參閱第 154 頁的「匯入應用程式憑證」。 請參閱第 155 頁的「匯出應用程式憑證」。 請參閱第 156 頁的「處理應用程式憑證」。

新增自行簽署的憑證

自行簽署的憑證可用於 HTTPS 通訊或 SMTP/TLS。 某些電子郵件伺服器可能無法辨識用於 SMTP/TLS 的自行簽署的憑證。 很多電子郵件伺服器都要求使用憑證授權中心簽署的憑證。 自行簽署的憑證不建議用於 SMTP/TLS。

新增自行簽署的憑證

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「TLS 和 HTTPS 憑證」**標籤。
3. 按下**「新增」**。
4. 在**「憑證名稱」**方塊中，輸入此憑證的名稱。
5. 在**「憑證類型」**下拉式清單中，選擇**「自行簽署的」**。
6. 完成頁面上的其餘資訊。
7. 按下**「建立」**。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

請參閱第 145 頁的「關於憑證」。

新增認證中心簽署憑證的方法

表 7-2 描述可用來新增憑證授權中心簽署憑證的方法。

表 7-2 新增憑證授權中心簽署憑證的方法

方法	程序
將您在「**新增憑證**」頁面中產生的憑證簽署要求傳送到憑證授權中心。當您從憑證授權中心收到憑證時，請將其儲存在本機上並匯入至控管中心，以將它新增至可用憑證清單。	請參閱第 151 頁的「要求憑證授權中心簽署的憑證」。
從 Symantec Messaging Gateway 硬體裝置匯出憑證授權中心簽署的憑證或自行簽署的憑證，然後匯入該憑證。	請參閱第 148 頁的「新增自行簽署的憑證」。 請參閱第 158 頁的「匯出 TLS 與 HTTPS 憑證」。 請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。
使用僅有效期限不同的新憑證更新現有 TLS & HTTPS 憑證授權中心簽署的憑證。若要執行此作業，請將更新過的憑證匯入控管中心，並保持原憑證不動。	請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。
新增憑證授權中心簽署的憑證，而不必在控管中心產生憑證簽署要求。您必須先修改匯入檔案。憑證必須使用 PEM 格式。	請參閱第 149 頁的「修改憑證授權中心簽署憑證匯入檔案」。 請參閱第 157 頁的「憑證與網域金鑰的 PEM 格式需求」。

為了確保憑證授權中心簽署的憑證可被接受為有效憑證，請確定簽署憑證之憑證授權中心的 CA 憑證顯示在「**憑證設定**」頁面「**憑證授權中心**」標籤的「**CA 憑證**」清單中。

請參閱第 150 頁的「新增 CA 或中繼憑證」。

在新增憑證之後，您可以將其指派給控管中心，以保護網頁式通訊的安全，或指派給掃描程式 MTA，以支援 TLS 加密。

請參閱第 160 頁的「指派使用者介面 HTTPS 憑證給控管中心」。

請參閱第 159 頁的「指派 MTA TLS 憑證給掃描程式」。

若 TLS 和 HTTP 憑證需要中繼憑證授權中心憑證，也會需要新增憑證授權中心憑證。當您新增憑證授權中心簽署的憑證時，須完成憑證鏈結，才允許驗證新憑證。您架構的所有掃描程式都可存取控管中心的憑證授權中心簽署的憑證，以進行 SMTP/TLS 和 HTTPS 驗證。

請參閱第 145 頁的「關於憑證」。

修改憑證授權中心簽署憑證匯入檔案

您可以新增憑證授權中心簽署的憑證，而不必在控管中心產生憑證簽署要求。如果尚未從 Symantec Messaging Gateway 硬體裝置匯出憑證，則必須先修改憑證匯入檔案。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

請參閱第 145 頁的「關於憑證」。

若要修改憑證匯入檔案，請從用於產生憑證簽署要求的金鑰中，移除密語。接著，先後將憑證和修改過的金鑰結合至一個新檔案。將結合的檔案儲存在本機，並將其匯入到控管中心，以新增至可用憑證清單。憑證必須使用 PEM 格式。

修改「憑證授權中心」簽署憑證匯入檔案

1 從用於產生憑證簽署要求的金鑰中，刪除密語。

您可以使用下列指令：

```
# openssl rsa -in key.pem -out key-nopass.pem
```

其中 *key.pem* 是金鑰的輸入檔案名稱，而 *key-nopass.pem* 則是沒有密語之金鑰的輸出檔案名稱。

2 建立新的文字檔。

3 將憑證複製到新檔案。

4 在憑證下方，複製沒有密語的公開金鑰到新檔案。

5 將新檔案儲存在本機。

6 將檔案匯入控管中心。

請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。

新增 CA 或中繼憑證

Symantec Messaging Gateway 已預先安裝許多常見憑證授權中心廠商的 CA 憑證。如果憑證授權中心為您簽署了 SMTP/TLS 或 HTTPS 憑證，但控管中心內尚不存在該憑證授權中心的 CA 憑證，則請新增 CA 憑證。

若憑證需要中繼 CA 憑證，也會新增 CA 憑證。當您新增 CA 憑證時，須完成憑證鏈結，以允許驗證憑證授權中心簽署的憑證。

請參閱第 145 頁的「關於憑證」。

請確定您具有 CA 憑證再繼續進行。當您從憑證授權中心收到憑證時，可能會隨附 CA 憑證。您也可以從憑證授權中心網站下載 CA 憑證。內含 CA 憑證的檔案必須為 PEM 格式。

請參閱第 157 頁的「憑證與網域金鑰的 PEM 格式需求」。

新增 CA 或中繼憑證

1 在控管中心內，按下**「管理」>「設定」>「憑證」**。

2 按下**「憑證授權中心」**標籤。

3 按下**「更新」**。

4 在「更新 CA 憑證」頁面上，按下**「瀏覽」**。

5 尋找並選取包含 CA 或中繼憑證的檔案。

6 按下「**更新**」。

頁面頂端會出現一則狀態訊息，指出成功或失敗。

檢視現有的 CA 憑證

您可以檢視目前安裝的 CA 憑證清單。

請參閱第 145 頁的「關於憑證」。

檢視現有的 CA 憑證

1 在控管中心內，按下「**管理**」>「**設定**」>「**憑證**」。

2 按下「**憑證授權中心**」標籤。

此時會出現目前安裝的 CA 憑證。

要求憑證授權中心簽署的憑證

對於 SMTP/TLS 通訊而言，憑證授權中心簽署的憑證可能比自行簽署的憑證還要有效用，並且還可以用於 HTTPS 通訊。請先決定要購買憑證的 CA，再繼續進行。控管中心的「**憑證授權中心**」標籤上列有一些可用的 CA，但也支援其他 CA。

針對一般名稱，請使用網域名稱或安裝憑證所在之電腦的完整網域名稱。某些 CA 可能不支援使用 IP 位址 (而非網域名稱) 作為一般名稱所建立的憑證。請與 CA 確認。

請參閱第 151 頁的「檢視現有的 CA 憑證」。

請參閱第 145 頁的「關於憑證」。

每一個 CA 都各自有一組要求及發出憑證的程序。如需詳細資料，請洽詢您的 CA 並遵循您的安裝所適用的指示。

附註：如果您有憑證授權中心簽署的憑證，即使沒有傳送憑證簽署要求，依然可以新增該憑證。不過，如果您尚未在控管中心產生新憑證簽署要求，或尚未從 Symantec Messaging Gateway 硬體裝置匯出憑證，則必須先修改憑證。

請參閱第 149 頁的「修改憑證授權中心簽署憑證匯入檔案」。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

要求憑證授權中心簽署的憑證

1 在控管中心內，按下「**管理**」>「**設定**」>「**憑證**」。

2 按下「**TLS 和 HTTPS 憑證**」標籤。

3 按下「**新增**」。

4 在「**憑證名稱**」方塊中，輸入這個憑證的名稱。

5 在「**憑證類型**」下拉式清單中，按下「**憑證中心簽署的**」。

6 視需要，在頁面的其餘部分填入資訊。

7 按下「**建立**」。

8 複製出現的文字區塊，並將它貼到文字檔中加以儲存。

將產生的文字儲存為文字檔。您稍後可以將文字檔的資訊複製並貼到 CA 要求表單上。

9 使用 CA 所要求的方式，將憑證授權中心簽署要求 (CSR) 傳送至 CA。

匯入憑證授權中心簽署的憑證

您從憑證授權中心 (CA) 收到憑證時，必須將其匯入，以在控管中心內使用。除了此憑證之外，CA 可能也寄送中繼 CA 憑證給您，必須將其在控管中心加以安裝。

附註：您不能匯入數位簽章演算法 (DSA) 簽署的憑證。

您也可以更新僅有效期限不同的現有 TLS 和 HTTPS 憑證授權中心簽署的憑證。請依照以下程序，在保持原憑證不變的同時，匯入更新過的憑證。

附註：如果您有憑證授權中心簽署的憑證，即使尚未產生憑證簽署要求，也可以匯入該憑證。不過，如果您尚未在控管中心產生新憑證簽署要求，或尚未從 Symantec Messaging Gateway 硬體裝置匯出憑證，則必須先修改憑證。

請參閱第 149 頁的「修改憑證授權中心簽署憑證匯入檔案」。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

請參閱第 145 頁的「關於憑證」。

匯入憑證授權中心簽署的憑證

1 在您收到 CA 的憑證檔案後，請將該檔案儲存到可從控管中心存取的位置。

在某些情況下，可能需要儲存多個檔案，具體視憑證授權中心的需求而定。

2 在控管中心內，按下「**管理**」>「**設定**」>「**憑證**」。

3 按下「**TLS 和 HTTPS 憑證**」標籤。

4 按下「**匯入**」。

5 在「**匯入憑證**」頁面上，輸入憑證的完整路徑和檔案名稱，或按下「**瀏覽**」並選擇檔案。

6 按下「**匯入**」。

取代所有現有的 CA 憑證

您可以使用另一組 CA 憑證取代控管中心所有現有的 CA 憑證。所有現有的 CA 憑證均將移除，並以所指定之檔案中的 CA 憑證加以更換。

請確定您具有 CA 憑證再繼續進行。內含 CA 憑證的檔案必須為 PEM 格式。

請參閱第 157 頁的「憑證與網域金鑰的 PEM 格式需求」。

請參閱第 145 頁的「關於憑證」。

取代所有現有的 CA 憑證

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「憑證授權中心」**標籤。
3. 按下**「還原」**。
4. 在**「還原 CA 憑證」**頁面上，按下**「瀏覽」**，然後找出含有 CA 憑證的檔案。
5. 按下**「還原」**。

   頁面頂端會出現一則狀態訊息，指出成功或失敗。

備份 CA 憑證

您可以備份安裝於控管中心的 CA 憑證。

請參閱第 145 頁的「關於憑證」。

備份 CA 憑證

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「憑證授權中心」**標籤。
3. 按下**「備份」**。
4. 在瀏覽器的**「檔案下載」**對話方塊中，按下**「儲存」**，然後指定儲存檔案的位置。

   檔案可以儲存到預設瀏覽器的下載目錄或您指定的位置。

變更憑證或網域金鑰名稱

您可以變更憑證或網域金鑰名稱，但是不能修改憑證的其他任何部分。若要變更憑證的其他部分，您必須建立新的憑證。

請參閱第 148 頁的「新增自行簽署的憑證」。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

請參閱第 109 頁的「新增網域金鑰」。

變更自行簽署或憑證授權中心簽署的憑證名稱

1 按下「**管理**」>「**設定**」>「**憑證**」。

2 按下「**TLS 和 HTTPS 憑證**」標籤。

3 勾選您要修改之憑證旁的方塊。

4 按下「**編輯**」。

5 在「**編輯憑證**」頁面的「**憑證名稱**」欄位中，輸入憑證的新名稱。

憑證名稱的長度上限為 255 個 US-ASCII 字元。

6 按下「**儲存**」。

變更網域金鑰名稱

1 按下「**管理**」>「**設定**」>「**憑證**」。

2 按下「**網域金鑰**」標籤。

3 勾選您要修改之網域金鑰旁的方塊。

4 按下「**編輯**」。

5 在「**編輯網域金鑰**」頁面的「**網域金鑰名稱**」欄位中，輸入憑證的新名稱。

6 按下「**儲存**」。

匯入應用程式憑證

將應用程式憑證匯入 Symantec Messaging Gateway 後，Symantec Messaging Gateway 便能驗證來自信任的用戶端應用程式的連線。

例如，假設您想要在 Symantec Messaging Gateway 和 Data Loss Prevention Enforce 之間同步資料。您必須先從 Enforce Sever 取得憑證。接著，您必須在 Symantec Messaging Gateway 中匯入憑證。然後，Symantec Messaging Gateway 便會獲得驗證 Enforce Server 的允許以執行同步化。

請參閱第 403 頁的「將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合」。

附註：數位簽章演算法 (DSA) 簽署了不支援的憑證。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

請參閱第 145 頁的「關於憑證」。

您必須具有「完整的管理權限」或「管理設定」修改權限，才能匯入應用程式憑證。

若要匯入應用程式憑證

1. 在您收到應用程式憑證檔案後，請將該檔案儲存到可從控管中心存取的位置。
2. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
3. 按下**「應用程式」**標籤。
4. 按下**「匯入」**。
5. 在**「匯入應用程式憑證」**頁面的**「管理員」**欄位中，選擇對所有內容事件資料夾擁有修改權限的管理員。

   附註：未來於應用程式介面中使用此憑證進行的所有動作，在日誌中都將記入此管理員名下。

6. 在**「憑證名稱」**欄位中，輸入此憑證的描述性名稱。
7. 在**「檔案名稱」**欄位中，輸入憑證的完整路徑和檔案名稱，或按下**「瀏覽」**並選擇檔案。
8. 按下**「匯入」**。

匯出應用程式憑證

您可以從 Symantec Messaging Gateway 匯出應用程式憑證。將此憑證匯入應用程式時，應用程式便能向 Symantec Messaging Gateway 進行驗證。

警告：匯出應用程式憑證可能產生嚴重的安全風險。匯出檔案含有伺服器驗證所需的一切資料。

作為最佳實務準則，您也可能想要匯出憑證作為備份，或以備災難復原之需。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

請參閱第 154 頁的「匯入應用程式憑證」。

您必須具有「完整的管理權限」或「管理設定」修改權限，才能匯出應用程式憑證。

若要匯出應用程式憑證

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「應用程式」**標籤。
3. 勾選您要匯出之憑證旁的方塊。
4. 按下**「匯出」**。
5. 將檔案儲存到安全位置。

處理應用程式憑證

除了匯入和匯出應用程式憑證的功能之外，您也可以執行下列工作：

編輯　修改憑證名稱和管理員。

您可能會想要修改憑證名稱，以與相似的憑證進行區別。

刪除　讓您刪除一或多個指定的憑證。

您可能會想要刪除不需要的憑證，以保持憑證清單易於管理。

警告：一旦刪除憑證，便只能從完整備份或自訂組態備份將其擷取回來。

請參閱第 611 頁的「從備份還原硬體裝置」。

檢視　讓您檢視指定的憑證。

您可以檢視憑證詳細資料以驗證其有效性。

附註：如果您擁有 Symantec Protection Center 憑證，則只能檢視此憑證的詳細資料。無法編輯、匯出或刪除該憑證。

您必須具有「完整的管理權限」或「管理設定」修改權限，才能處理應用程式憑證。

若要處理應用程式憑證

1. 按下**「管理」>「設定」>「憑證」**。
2. 按下**「應用程式」**標籤。
3. 勾選您要處理之憑證旁的方塊。
4. 執行下列其中一項工作：

按下**「編輯」**。	按下下拉式功能表以變更管理員或修改憑證名稱，然後按下**「儲存」**。
按下**「刪除」**。	在確認對話方塊中，按下**「刪除」**。
按下**「檢視」**。	檢視憑證詳細資料後，請按**「確定」**以返回應用程式憑證清單。

5. 按下**「儲存」**。

請參閱第 154 頁的「匯入應用程式憑證」。

請參閱第 155 頁的「匯出應用程式憑證」。

憑證與網域金鑰的 PEM 格式需求

在您新增憑證 (不論為自行產生或憑證授權中心簽署) 以及匯入網域金鑰時，請確定憑證或網域金鑰符合下列需求：

- 憑證或網域金鑰必須以 PEM 格式儲存在檔案中，且憑證或網域金鑰必須以 Base64 編碼文字包含在下列標記之間：
  憑證必須在 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 之間。
  PKCS#8 網域金鑰必須在 `-----BEGIN PUBLIC KEY-----` 和 `-----END PUBLIC KEY-----` 之間。
  OpenSSL 網域金鑰必須在 `-----BEGIN RSA PRIVATE KEY-----` 和 `-----END RSA PRIVATE KEY-----` 之間。
  將會忽略不在開頭標記與結尾標記之間的文字。
  憑證和網域金鑰的格式皆相同，只有開始標記和結束標記不同。
  Base64 文字僅可包含大寫與小寫羅馬英文字母 (A–Z、a–z)、數字 (0–9)，以及「+」和「/」符號。
- 檔案必須編碼為 US-ASCII 或 UTF。檔案不得包含擴充 ASCII 或非 ASCII 字元。
- 新增或更換 CA 憑證 (「更新」或「還原」) 時，一個檔案可包含多個憑證。
- 含有憑證或網域金鑰的檔案副檔名沒有特別限制。通常，憑證會使用 .txt 或 .crt 副檔名，而網域金鑰通常使用 .key 副檔名。
- 您必須從用於存取控管中心的瀏覽器來存取內含憑證或網域金鑰的檔案。

下列是範例 PEM 格式的 CA 憑證：

```
Text before Begin Certificate is ignored.
-----BEGIN CERTIFICATE-----
MIICPTCCAaYCEQDNun9W8N/kvFT+IqyzcqpVMA0GCSqGSIb3DQEBAgUAMF8xCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE3MDUGA1UECxMuQ2xh
c3MgMSBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw05
NjAxMjkwMDAwMDBaFw0yODA4MDEyMzU5NTlaMF8xCzAJBgNVBAYTAlVTMRcwFQYD
VQQKEw5WZXJpU2lnbiwgSW5jLjE3MDUGA1UECxMuQ2xhc3MgMSBQdWJsaWMgUHJp
bWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA5Rm/baNWYS2ZSHH2Z965jeu3noaACpEO+jglr0aIguVzqKCbJF0N
H8xlbgyw0FaEGIeaBpsQoXPftFg5a27B9hXVqKg/qhIGjTGsf7A01480Z4gJzRQR
4k5FVmkfeAKA2txHkSm7NsljXMXg1y2He6G3MrB7MLoqLzGq7qNn2tsCAwEAATAN
BgkqhkiG9w0BAQIFAAOBgQBMP7iLxmjf7kMzDl3ppssHhE16M/+SG/Q2rdiVIjZo
EWx8QszznC7EBz8UsA9P/5CSdvnivErpj82ggAr3xSnxgiJduLHdgSOjeyUVRjB5
FvjqBUuUfx3CHMjjt/QQQDwTw18fU+hI5Ia0e6E1sHslurjTjqs/OJ0ANACY89Fx
lA==
-----END CERTIFICATE-----
Text after End Certificate is ignored.
```

新增網域金鑰時，Symantec Messaging Gateway 會依據符合 PEM 格式需求的方式產生網域金鑰。

請參閱第 150 頁的「新增 CA 或中繼憑證」。

請參閱第 148 頁的「新增自行簽署的憑證」。

請參閱第 109 頁的「匯入網域金鑰」。

請參閱第 109 頁的「新增網域金鑰」。

檢視 SMTP/TLS 或 HTTPS 憑證

您可以檢視任何 SMTP/TLS 或 HTTPS 憑證。

請參閱第 151 頁的「檢視現有的 CA 憑證」。

檢視 SMTP/TLS 或 HTTPS 憑證

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「TLS 和 HTTPS 憑證」**標籤。
3. 勾選您要檢視之憑證旁的方塊。
4. 按下**「檢視」**。

匯出 TLS 與 HTTPS 憑證

您可以從 Symantec Messaging Gateway 硬體裝置匯出任何憑證，然後再匯入該憑證。您也可能想要匯出憑證作為備份，或以備災難復原之需。

警告：匯出憑證可能產生嚴重的安全風險。匯出檔案含有伺服器驗證所需的一切資料。

附註：您不能匯出憑證簽署要求。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。

匯出 TLS 與 HTTPS 憑證

1. 在控管中心內，按下**「管理」>「設定」>「憑證」**。
2. 按下**「TLS 和 HTTPS 憑證」**標籤。
3. 按下您要匯出之單一憑證旁的核取方塊。

4 按下「**匯出**」。

5 將檔案儲存到安全位置。

刪除 SMTP/TLS 或 HTTPS 憑證

您可以檢視或刪除憑證。您無法刪除正用於 SMTP/TLS 或 HTTPS 驗證的憑證。

請參閱第 158 頁的「檢視 SMTP/TLS 或 HTTPS 憑證」。

刪除 SMTP/TLS 或 HTTPS 憑證

1 按下「**管理**」>「**設定**」>「**憑證**」。

2 按下「**TLS 和 HTTPS 憑證**」標籤。

3 勾選要刪除之憑證旁邊的方塊。

4 按下「**刪除**」。

此時會顯示確認視窗。

指派 MTA TLS 憑證給掃描程式

您可以將 MTA TLS 憑證指派給掃描程式。如果您希望掃描程式傳送或接受 TLS 加密郵件以掃描入埠或離埠郵件，或是進行驗證，則需要執行此工作。

請參閱第 145 頁的「關於憑證」。

您也可以將憑證指派給 SMTP 驗證。

請參閱第 93 頁的「架構 SMTP 驗證郵件設定」。

您可以使用自行簽署的憑證或憑證授權中心簽署的憑證。可能還需要安裝中繼或根 CA 憑證，才能確保憑證鏈結可進行驗證。對於 SMTP/TLS 驗證，Symantec Messaging Gateway 允許您使用憑證授權中心簽署的憑證，即使從用戶端憑證至憑證授權中心簽署之憑證的路徑或鏈並不完整，也是如此。

請參閱第 148 頁的「新增認證中心簽署憑證的方法」。

指派 MTA TLS 憑證給掃描程式

1 在控管中心內，按下「**管理**」>「**主機**」>「**組態**」。

2 勾選所需主機旁的方塊，然後按下「**編輯**」。

3 按下 **SMTP** 標籤。

4 如果您要讓這個掃描程式掃描入埠或離埠 TLS 加密電子郵件，請在「**入埠郵件設定**」、「**離埠郵件設定**」或「**驗證郵件設定**」下方，勾選「**接受 TLS 加密**」。

5 在相鄰的下拉式清單中，選擇適用於入埠、離埠或驗證郵件流的 MTA TLS 憑證。

您可以同時指派相同的憑證給入埠、離埠及驗證 TLS 加密電子郵件過濾。

6 如果您想要入埠或驗證連線用戶端出具 TLS 憑證以供驗證，請勾選**「要求用戶端憑證」**。

未成功驗證的用戶端將無法傳送郵件到硬體裝置。

此步驟不適用於離埠郵件流。

您可能需要安裝中繼憑證授權中心簽署的憑證或 CA 憑證，才可驗證連線用戶端的 TLS 憑證。

7 您可以勾選**「需要 TLS 加密」**(僅適用於驗證)。

不使用 TLS 加密的用戶端將無法進行驗證。

8 按下**「儲存」**。

指派使用者介面 HTTPS 憑證給控管中心

您可以指派使用者介面 HTTPS 憑證給控管中心。您可以使用自行簽署的憑證或憑證授權中心簽署的憑證。若使用憑證中心簽署的憑證，則可能需要安裝中繼或根 CA 憑證，才能確保憑證鏈結可進行驗證。

請參閱第 145 頁的「關於憑證」。

請參閱第 150 頁的「新增 CA 或中繼憑證」。

指派使用者介面 HTTPS 憑證給控管中心

1 在控管中心內，按下**「管理」>「設定」>「控管中心」**。

2 按下**「憑證」**標籤。

3 按下**「使用者介面 HTTPS 憑證」**下拉式清單並選取憑證。

4 按下**「儲存」**。

8

架構政策群組

本章包含以下主題：

- 關於政策群組
- 建立政策群組及指派政策
- 關於管理政策群組成員
- 編輯、刪除、啟用或停用政策群組
- 關於選取政策群組的過濾政策
- 啟用與停用政策群組的使用者設定
- 根據語言允許或攔截電子郵件
- 設定政策群組優先度

關於政策群組

政策群組為一組使用者。您可以將垃圾郵件、惡意軟體、威脅防禦和內容過濾政策套用至政策群組。您也可以啟用管理政策、啟用一般使用者隔離所或一般使用者設定權限，或設定政策群組之入埠郵件的語言限制。

當郵件符合政策條件時，根據所屬政策群阻，SMG 針對每個寄件者或收件者所採取的動作會有所不同。對於入埠郵件，SMG 根據收件者的政策群組中的過濾政策處理每個收件者的郵件。對於離埠郵件，寄件者的政策群組會決定如何處理郵件。

依據預設，Symantec Messaging Gateway 將垃圾郵件、惡意軟體和威脅防禦的預設過濾政策指派給您建立的政策群組。內容過濾沒有預設政策，因此沒有內容過濾政策指派給新的政策群組。建立您自己的過濾器政策後，您可以編輯政策群組以指派新政策。

如果某個收件者或寄件者屬於多個政策群組，則只會套用至具有最高群組優先度的群組。群組在**「管理」>「使用者」>「政策群組」**頁面上的清單中出現的位置越靠前，群組的優先度就越高。

「預設」政策群組包括所有使用者。此政策群組始終為清單中的最後一個群組，以確保您指派給自訂政策群組的政策正常運作。您無法變更**「預設」**政策群組的位置。

從**「管理」>「使用者」>「政策群組」**頁面，您可以：

- 設定政策群組優先度，它可確定套用至每個郵件的政策。
- 編輯所屬政策群阻和動作。
- 啟用和停用政策群組。
- 刪除政策群組。
- 檢視個別使用者的政策群組資訊。

請參閱第 162 頁的「建立政策群組及指派政策」。

建立政策群組及指派政策

表 8-1 說明建立政策群組以及將政策指派給那些群組的程序。

表 8-1 建立政策群組及指派政策的程序

步驟	動作	說明
步驟 1	建立政策群組和新增成員.	建立政策群組. 請參閱第 163 頁的「產生政策群組」。 新增成員至政策群組. 請參閱第 164 頁的「新增成員至政策群組」。
步驟 2	將電子郵件訊息**「病毒政策」**指派給政策群組。	賽門鐵克會預先安裝電子郵件病毒政策，可供您指派給政策群組。 請參閱第 169 頁的「為政策群組選取惡意軟體政策」。 請參閱第 188 頁的「預設電子郵件惡意軟體政策」。 請參閱第 187 頁的「建立電子郵件惡意軟體政策」。

步驟	動作	說明
步驟 3	將電子郵件訊息**「垃圾郵件政策」**指派給政策群組。	賽門鐵克會預先安裝垃圾郵件政策，可供您指派給政策群組。 請參閱第 170 頁的「為政策群組選取垃圾郵件政策和不必要的電子郵件政策」。 請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。 如果您要為政策群組指派自訂垃圾郵件政策，必須先建立這些政策，然後返回此步驟並套用這些政策。 請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。
步驟 4	為政策群組指派內容過濾政策.	沒有任何預設內容過濾政策。您必須使用預先定義的範本來設定這些政策。 請參閱指派內容過濾政策的程序主題。 請參閱第 278 頁的「建立內容過濾政策」。

產生政策群組

「政策群組」頁面會列出每個政策群組。預設政策群組始終為清單中的最後一個群組。預設政策群組包含所有使用者與所有網域。雖然您可以新增或修改預設政策群組的動作，但無法新增成員至預設政策群組。您無法刪除、停用或變更預設政策群組的優先度。

附註：如果您已啟用探查參與，則**「探查帳戶」**政策群組會出現在政策群組清單中。只要此清單不包含已存在的自訂政策群組，**「探查帳戶」**政策群組就是清單中的第一個群組。您可以變更**「探查帳戶」**政策群組的優先權。當您編輯**「探查帳戶」**政策群組時，會顯示**「探查帳戶」**頁面。

建立政策群組

1. 在控管中心內，按下**「管理」**>**「使用者」**>**「政策群組」**。
2. 在**「政策群組」**頁面上，按下**「新增」**。
3. 在**「政策群組名稱」**欄位中，輸入識別此群組的名稱。
4. 按下**「儲存」**。

   建立政策群組後，您可以新增成員。

   請參閱第 164 頁的「新增成員至政策群組」。

新增成員至政策群組

您可以根據電子郵件地址、網域名稱或LDAP群組，將成員指派給政策群組，以便套用政策。建立自己的政策群組並新增成員之後，您就可以選取要讓群組擁有的政策。

附註：沒有任何編輯按鈕可供編輯政策群組成員。請使用新增/移除方法，來變更成員名稱。例如，如果您要更正成員名稱中的錯字，您必須先刪除該成員，然後再次新增該成員。

如果您使用儲存在LDAP目錄中的散布清單或群組作為政策群組成員資格的一部分，並且對目錄的結構進行變更，造成任何 LDAP 群組的辨別名稱 (DN)、散布清單或屬於這些 LDAP 實體之成員的使用者也因此產生變更，則請執行下列動作，以確保一致地套用了政策群組。

- 如果政策群組成員為 LDAP DN，請更新政策群組中的 DN (如果有變更)。
- 清除目錄資料來源上的快取，已架構該資料來源對這些 LDAP 群組、散布清單及其使用者成員執行位址解析。即使您依據政策群組中的電子郵件地址參照 LDAP 散布清單，也應該執行此步驟。
  請參閱第 481 頁的「關於目錄資料快取」。

新增成員至政策群組

1. 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。
2. 按下您要編輯的政策群組。
3. 確定已顯示**「成員」**標籤，然後按下**「新增」**。
4. 使用下列其中一種方法來指定成員：
   - 在方塊中輸入電子郵件地址、網域名稱，或輸入兩者。如要指定多個項目，請以逗號、分號或空格分隔各個項目。若要將特殊網域的所有收件者新增為成員，請使用以下任意格式輸入網域：

     ```
     domain.com
     *@domain.com
     ```

     SMG 會將星號 (*) 和問號 (?)解譯為文字。
   - 在提供的欄位中，輸入群組的 LDAP 識別名稱，例如：cn=some ldap group,dc=domain,dc=com。
     只要進行的任何修改會變更以此方式新增的直接成員識別名稱字串，就必須在政策群組中手動更新修改。為了保護郵件流的運作方式，您應該在修改群組之前，先將新的識別名稱字串成員資格新增至政策，並在修改完成後，移除舊的識別名稱字串。
   - 勾選一或多個 LDAP 群組旁的方塊。
     此頁所列之 LDAP 群組，是從您的 LDAP 伺服器載入的。若要使用 LDAP 群組清單，至少必須啟用一個位址解析功能，並且必須架構群組清單查詢。
     請參閱第 439 頁的「關於搭配使用位址解析功能與資料來源」。

5 按下「**新增成員**」以增加新成員。

6 按下「編輯政策群組」頁面上的「**儲存**」。

刪除政策群組中的成員

新增或移除政策群組成員時，會重建任何位址解析度來源的成員資格。如果群組很大，則可能需要一些時間，所做的變更才能反映在系統中。

刪除政策群組成員

1 在控管中心內，按下「**管理**」>「**使用者**」>「**政策群組**」。

2 按下您要編輯的政策群組。

3 在「編輯政策群組」頁面的「**成員**」標籤中，勾選一個以上電子郵件位址、網域或 LDAP 群組旁的方塊，然後按下「**刪除**」。

4 按下「**儲存**」。

關於管理政策群組成員

您可以使用控管中心的工具管理所屬政策群阻。您可以手動新增成員 (在政策群組建立過程中)；也可以從外部檔案匯入成員。

請參閱第 164 頁的「新增成員至政策群組」。

請參閱第 165 頁的「匯入及匯出政策群組成員」。

若要尋找某成員所屬的全部政策群組，可使用控管中心所提供的研究選項。

請參閱第 166 頁的「研究使用者所屬的政策群組」。

沒有任何用於編輯政策群組成員的編輯選項。請使用新增/移除方法，來變更成員名稱。例如，如果您要更正成員名稱中的錯字，您必須先刪除該成員，然後再次新增該成員至群組。

匯入及匯出政策群組成員

您可以從檔案匯入政策群組成員，也可以將群組成員匯出至檔案。

附註：您無法匯入或匯出由辨別名稱描述的 LDAP 群組成員。

從檔案匯入政策群組成員

1 在控管中心內，按下「**管理**」>「**使用者**」>「**政策群組**」。

2 按下要編輯之政策群組的加上底線的名稱。

3 在「編輯政策群組」頁面的「**成員**」標籤上，按下「**匯入**」。

4 輸入適當的路徑與檔案名稱 (或按下「**瀏覽**」找到硬碟中的檔案)，然後按下「**匯入**」。

以換行的方式在純文字檔案中分隔各個網域或電子郵件地址。以下為範例檔案：

```
ruth@example.com
rosa@example.com
ben*@example.com
example.net
*.org
```

範例檔案中的電子郵件地址的行為如下：

- ruth@example.com 和 rosa@example.com 符合完全精確的電子郵件地址。
- ben*@example.com 符合 ben@example.com 和 benjamin@example.com 等等。
- example.net 符合 example.net 中的所有電子郵件地址。
- *.org 符合所有以 .org 結尾的網域中所有電子郵件地址。

5 按下**「儲存」**。

將政策群組成員匯出至檔案

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 按下要編輯之政策群組的加上底線的名稱。

3 在「編輯政策群組」頁面的「成員」標籤上，按下**「匯出」**。

4 請視需要完成作業系統的儲存檔案對話方塊作業。

研究使用者所屬的政策群組

您可以識別已指派使用者的所有政策群組。

表 8-2 提供了 SMG 根據您所輸入之準則比對政策成員的方式的範例。

表 8-2 所屬政策群阻搜尋條件

條件	範例
網域名稱	您可以使用下列任一方式輸入網域名稱： ■ symantecexample.com SMG 會尋找具有電子郵件網域 symantecexample.com 或任何子網域 (如 norton.symantecexample.com 和 sep.norton.symantecexample.com) 的成員。 ■ *symantecexample.com SMG 會尋找具有電子郵件網域 symantecexample.com 或任何子網域 (如 norton.symantecexample.com 和 sep.norton.symantecexample.com) 的成員。 ■ *.symantecexample.com SMG 會尋找電子郵件網域為 symantecexample.com 的任何子網域 (如 norton.symantecexample.com 和 sep.norton.symantecexample.com) 的成員。但是並不會尋找「symantecexample.com」。 ■ .symantecexampl*.com SMG 會尋找 symantecexample.com 和 symantecexamplo.com。 如果您在 網域中輸入問號 (?)，則 SMG 便會將其視為該位置的萬用字元。例如，如果您輸入 symante?，則 SMG 會尋找 symantec.com 和 symantem.com。
電子郵件地址	如果您輸入 sep.1@symantecexample.com，則 SMG 會尋找符合 sep.1@symantecexample.com 和 sep11@symantecexample.com 的成員。
LDAP 網域名稱	如果您輸入如「dc=symantec.mail?tail」或「dc=com」的成員網域名稱，則此群組中的任何使用者皆會顯示為符合搜尋條件。 SMG 會將 LDAP 網域名稱中的句號 (.) 或問號 (?) 等中繼字元視為常值字元。

研究使用者所屬的政策群組

1 執行下列其中一個步驟：

- 在控管中心內，依序按下**「管理」>「使用者」>「政策群組」**，然後按下群組名稱，並按下**「尋找使用者」**。
- 在控管中心內，按下**「管理」>「使用者」>「尋找使用者」**。

2 在**「電子郵件地址」**方塊中，輸入使用者的電子郵件地址。

3 按下**「尋找使用者」**。

控管中心會以政策群組優先度列出指定的使用者所存在的啟用政策群組。

請參閱第 161 頁的「關於政策群組」。

請參閱第 163 頁的「產生政策群組」。

請參閱第 164 頁的「新增成員至政策群組」。

編輯、刪除、啟用或停用政策群組

以下章節說明政策群組的一般管理工作。

編輯現有的政策群組

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 按下政策名稱或勾選政策群組旁邊的方塊，然後按下**「編輯」**。

按照您在建立時所進行的步驟，針對此政策群組新增或刪除成員或變更過濾動作。

請參閱第 163 頁的「產生政策群組」。

啟用政策群組

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 勾選政策群組旁邊的方塊，然後按下**「啟用」**。

停用政策群組

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 勾選政策群組旁邊的方塊，然後按下**「停用」**。

附註：您無法停用或刪除預設政策群組。

刪除政策群組

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 在「政策群組」頁面中，勾選政策群組旁邊的方塊，然後按下**「刪除」**。

關於選取政策群組的過濾政策

依據預設，會為所建立的政策群組指派垃圾郵件、惡意軟體及內容過濾的預設過濾政策。

以下說明如何將自訂過濾器政策指派給政策群組 (可視需要，依任何順序執行這些工作)：

- 選取政策群組的電子郵件惡意軟體政策。
  請參閱第 169 頁的「為政策群組選取惡意軟體政策」。
  使用可用惡意軟體政策的索引，可協助您自訂政策群組。
  請參閱第 170 頁的「惡意軟體類別及預設動作」。
- 選取政策群組的垃圾郵件政策。
  請參閱第 170 頁的「為政策群組選取垃圾郵件政策和不必要的電子郵件政策」。
- 選取政策群組的內容過濾政策。
  請參閱第 172 頁的「選取用於政策群組的內容過濾政策」。

若要讓 SMG 能夠過濾政策，政策必須至少指派給一個政策群組，且政策必須啟用。

為政策群組選取惡意軟體政策

您可以為每個政策群組指定惡意軟體政策。SMG 隨附預設啟用的預先架構之惡意軟體政策。為政策群組選取惡意軟體政策時，從這些預先載入的政策中選取。

請參閱第 188 頁的「預設電子郵件惡意軟體政策」。

然而，您也可以建立自訂的惡意軟體政策，並將它們套用到您的政策群組中。或者，您可以修改預設惡意軟體政策，以進行微調或擴大或縮小其範圍。

請參閱第 187 頁的「建立電子郵件惡意軟體政策」。

請參閱第 191 頁的「修改電子郵件惡意軟體政策」。

附註：根據預設，系統會清除包含惡意軟體的郵件和附件，也會刪除包含大量郵寄病蟲的入埠郵件和離埠郵件。無法掃描的郵件也會刪除。如果您擔心遺失重要的郵件，可以變更無法掃描之郵件的預設設定。您可以將不同的動作套用至因不同原因而無法掃描的郵件。

為政策群組選取惡意軟體政策

1. 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。
2. 在**「政策群組」**頁面中，按下您要為其選取惡意軟體政策的群組。
3. 按下**「惡意軟體」**標籤。
4. 您可以選擇性地按下任何政策旁的**「檢視」**，檢視該政策的詳細資料。
5. 如有需要，請在**「電子郵件」**下，勾選**「啟用此政策群組的入埠電子郵件病毒掃描」**，然後從下列各個下拉式清單中選取需要的政策：
   - **入埠防毒政策**
   - **入埠大量郵寄病蟲政策**
   - **入埠加密附件政策**
   - **入埠解除政策**
   - **入埠可疑附件政策**
   - **入埠間諜程式/廣告程式政策**
   - **因超出限制政策而無法掃描的入埠檔案**
   - **因其他政策而無法掃描的入埠檔案**
   - **因解除政策而無法掃描的入埠檔案**
6. 如有需要，請在**「電子郵件」**下，勾選**「啟用此政策群組的離埠電子郵件病毒掃描」**，然後從下列各個下拉式清單中選取需要的政策：
   - **離埠防毒政策**

- **離埠大量郵寄病蟲政策**
- **離埠加密附件政策**
- **離埠解除政策**
- **離埠可疑附件政策**
- **離埠間諜程式/廣告程式政策**
- **因超出限制政策而無法掃描的離埠檔案**
- **因其他政策而無法掃描的離埠檔案**
- **因解除政策而無法掃描的離埠檔案**

7 按下「**儲存**」。

惡意軟體類別及預設動作

表 8-3描述 SMG 惡意軟體類別的預設動作。

請參閱第 169 頁的「為政策群組選取惡意軟體政策」。

請參閱第 188 頁的「預設電子郵件惡意軟體政策」。

表 8-3 病毒類別及預設動作

類別	預設電子郵件動作
病毒	清除郵件。
大量郵件病蟲	刪除郵件。
無法掃描的郵件	刪除郵件。
加密的附件	在 Subject: 標頭前面添加 `[WARNING ENCRYPTED ATTACHMENT NOT VIRUS SCANNED]`。
間諜程式或廣告程式	在 Subject: 標頭前面添加 `[SPYWARE OR ADWARE INFECTED]`。
可疑附件	入埠訊息： 刪除和延遲可疑病毒隔離所中的郵件。 離埠訊息： 將郵件保留在可疑病毒隔離所。
潛在惡意內容 (解除)	入埠郵件：移除潛在惡意內容 離埠郵件：正常傳送

為政策群組選取垃圾郵件政策和不必要的電子郵件政策

垃圾郵件政策及不必要的電子郵件政策，會決定針對符合下列任一條件的入埠電子郵件和離埠電子郵件採取的動作：

- 如果電子郵件是垃圾郵件
  SMG 根據特徵比對、過濾器和啟發式分析所得的分數，識別為垃圾郵件的郵件。
- 如果電子郵件是不必要的郵件

  不必要的郵件包括：

  - 可疑垃圾郵件
    SMG 根據特徵比對和啟發式分析所得的分數，識別為可能是垃圾郵件的郵件。
  - 客戶特定垃圾郵件
    SMG 根據客戶特定規則集，識別為垃圾郵件的郵件。
  - 行銷郵件
    內含使用者可能已要求的商業性或籌款訊息的郵件。
  - 電子報
    定期(通常是每週或每月)發送包含特定主題內容的郵件，使用者可能已要求接收此類郵件。
  - 內含重新導向 URL 的電子郵件
    重新導向 URL 包括免費的托管網站、URL 縮短服務以及 URL 重新導向服務，這些可能會遭到不當使用以傳送垃圾郵件或惡意軟體酬載。

SMG 安裝時，會一併安裝預先架構的預設垃圾郵件政策與不想要的電子郵件政策，您可以將這些政策套用至政策群組。

請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。

附註：您也可以套用自訂的垃圾電子郵件政策與不必要的電子郵件政策。您必須先建立這些政策，然後選擇功能表中才能提供這些政策。

請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。

為政策群組選取垃圾郵件和不必要的電子郵件政策

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 在**「政策群組」**頁面上，按下您要為其選取垃圾郵件政策或不必要的電子郵件政策的政策群組。

3 按下**「垃圾郵件」**標籤。

4 您可以選擇性地按下任何政策旁的**「檢視」**，檢視該政策的詳細資料。

5 若要啟用入埠垃圾郵件掃描，請勾選**「對此政策群組啟用入埠垃圾郵件及不必要的電子郵件掃描」**，然後從下拉式清單中選取所需要的政策。

6 針對**「對此政策群組啟用入埠垃圾郵件及不想要的電子郵件掃描」**下方的每個項目，按下項目旁邊的下拉式清單，然後選取動作。按下**「檢視」**以檢視政策的詳細資料。

必須啟用客戶特定垃圾郵件提交功能，客戶特定垃圾郵件過濾政策才會顯示在下拉式清單中。

7 若要啟用離埠垃圾郵件掃描，請勾選**「對此政策群組啟用離埠垃圾郵件及不必要的電子郵件掃描」**，然後從下拉式清單中選取所需要的政策。

離埠郵件並沒有預先架構的不必要的電子郵件政策。除非您為不必要的電子郵件建立政策，否則下拉式清單中不會顯示任何政策。

8 針對**「對此政策群組啟用離埠垃圾郵件及不想要的電子郵件掃描」**下方的每個項目，按下項目旁邊的下拉式清單，然後選取動作。按下**「檢視」**以檢視政策的詳細資料。

必須啟用客戶特定垃圾郵件提交功能，客戶特定垃圾郵件過濾政策才會顯示在下拉式清單中。

9 您也可以勾選**「啟用此政策群組的退回攻擊防護」**，然後從**「退回攻擊防護政策」**下拉式清單中選取需要的政策。

SMG 會提供一個預設政策：「無法通過退回攻擊驗證: 拒絕郵件」。您也可以編輯此政策，或建立新的政策。新政策必須包含**「如果郵件無法通過退回攻擊驗證」**條件，而且採取的動作應該會讓退回位址標籤驗證失敗。

10 按下**「儲存」**。

您無法從**「編輯政策群組」**頁面變更垃圾郵件政策詳細資料。

選取用於政策群組的內容過濾政策

讓適當的內容過濾政策與群組產生關聯，就可以檢查郵件的附件類型、關鍵字或比對規則運算式。依據郵件內容，您可以新增註釋、傳送通知，也可以複製郵件給某個電子郵件地址。您也可以使用內容過濾政策來檢查法規或組織政策的內容過濾情形。

附註：因為沒有預設的內容過濾政策，所以**「編輯政策群組」**頁面的下拉式清單一開始是空白的。在您選取用於政策群組的內容過濾政策之前，您必須至少建立一個內容過濾政策。

請參閱第 278 頁的「建立內容過濾政策」。

選取用於政策群組的內容過濾政策

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 在**「政策群組」**頁面上，按下您要為其選取內容過濾政策的政策群組。

3 按下**「內容過濾」**標籤。

4 勾選**「啟用此政策群組的入埠內容過濾」**。

5 從「**內容過濾政策**」下拉式清單中，選取所需的政策。

您必須先將政策套用至「**編輯電子郵件內容過濾政策**」頁面上的群組，才能讓政策出現在下拉式清單中。

您可以依喜好按下「**檢視**」以查看內容過濾政策的摘要，然後按下「**確定**」以返回「**編輯政策群組**」頁面。從下拉式清單新增內容過濾政策時，該政策會顯示在底端清單中，在下拉式清單中則無法使用。

6 按下「**新增**」。

7 您可以依喜好從「**內容過濾政策**」下拉式清單中新增額外政策。

8 若要架構群組的離埠內容過濾政策，請勾選「**啟用此政策群組的離埠內容過濾**」，並再次執行步驟 5 至步驟 7。

9 按下「**儲存**」。

您無法從「**編輯政策群組**」頁面變更內容政策的詳細資料 (如條件與動作)。雖然您可以在這個頁面上將現有的政策新增至清單中，但您無法從這個頁面新增內容過濾政策。

啟用與停用政策群組的使用者設定

一般使用者設定可確定政策群組中的一般使用者是否可以登入控管中心，來執行下列任一工作：

- 架構個人的「允許的寄件者」和「攔截的寄件者」清單。
- 攔截或允許使用指定語言的電子郵件。

附註：必須為位址解析架構資料來源，才能啟用此頁面，並且需要驗證和位址解析資料來源，系統才能執行您的設定。

請參閱第 429 頁的「關於資料來源和功能」。

請參閱第 174 頁的「啟用政策群組的一般使用者設定的需求」。

若要登入，使用者可在瀏覽器內存取與控管中心管理員相同的 URL： https://<hostname>。一般使用者的登入帳號與密碼，與其 LDAP 的登入帳號與密碼相同。

如需支援瀏覽器的相關資訊，請參閱「SMG 安裝指南」。

附註：對於「允許的寄件者」和「攔截的寄件者」清單，一般使用者在這兩種清單中的項目總和上限為 200。

附註：雖然 SMG 用以識別郵件語言的語言識別技術具有高精確率，但還是可能發生語言識別錯誤。請注意，識別出使用禁用語言的郵件將會被刪除。

選取政策群組的一般使用者設定

1. 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。
2. 在「政策群組」頁面中，按下要為其選取一般使用者政策的群組。
3. 按下**「一般使用者」**標籤。
4. 勾選**「啟用此政策群組的一般使用者設定」**。
5. 必要時，可勾選**「建立個人之允許的寄件者清單和攔截的寄件者清單」**。
6. 若有需要，可勾選**「指定語言設定」**。
7. 按下**「儲存」**。

啟用政策群組的一般使用者設定的需求

一般使用者架構個人「允許的寄件者」和「攔截的寄件者」清單，並攔截或允許指定語言的電子郵件之前，必須符合下列需求：

- 至少啟用一個資料來源以進行驗證。
- 至少啟用一個資料來源以進行位址解析。
- 必須設定一般使用者喜好設定複寫頻率。
- 必須在**「編輯政策群組」**頁面上的**「一般使用者」**標籤中，啟用指定政策群組的一般使用者喜好設定。
- 政策群組的成員只能是LDAP使用者，不可為本機定義的使用者(亦即手動輸入的電子郵件地址)。

請參閱第 242 頁的「架構一般使用者隔離所」。

根據語言允許或攔截電子郵件

使用 SMG 提供的語言識別技術，可針對群組攔截或允許以指定語言編寫的郵件。例如，您可以選擇僅允許英文與西班牙文的郵件，或是攔截英文與西班牙文的郵件並允許所有其他語言的郵件。

請參閱第 163 頁的「產生政策群組」。

請參閱第 164 頁的「新增成員至政策群組」。

依據語言，允許或攔截群組的電子郵件

1. 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。
2. 在「政策群組」頁面中，按下您要為其選取語言政策的群組。
3. 按下**「語言」**標籤。
4. 按下所需的設定。

5 如果選擇**「只接收下列語言的郵件」**或**「不接收下列語言的郵件」**，請勾選每種所需語言的核取方塊。

可用的語言設定如下：中文、荷蘭文、英文、法文、德文、義大利文、日文、韓文、葡萄牙文、俄文和西班牙文。

6 按下**「儲存」**。

雖然 SMG 用以識別郵件語言的語言識別技術具有高精確率，但還是可能發生語言識別錯誤。請注意，被識別出使用禁用語言撰寫的郵件將會被刪除。

設定政策群組優先度

「政策群組」頁面會依特定順序列出政策群組。位於清單中較高位置的政策群組具有較高的優先度。如果使用者是多個群組的成員，則確定如何處理該使用者的郵件時，會套用優先度較高的政策群組。

預設政策群組始終為清單中的最後一個群組。您無法變更預設政策群組的優先度。如果您已啟用探查參與，則**「探查帳戶」**政策群組會出現在政策群組清單中。

設定政策群組優先度

1 在控管中心內，按下**「管理」>「使用者」>「政策群組」**。

2 按下您要移動的群組，然後將其向上或向下拖曳至您要的位置。

請參閱第 272 頁的「啟用探查參與」。

請參閱第 161 頁的「關於政策群組」。

9

偵測病毒、惡意軟體與惡意攻擊

本章包含以下主題：

- 關於偵測病毒、惡意軟體與惡意攻擊
- 關於「解除」
- 對付可疑附件所採取的動作
- 間諜程式或廣告程式判斷詳細資訊
- 偵測病毒、惡意軟體與惡意威脅
- 建立電子郵件惡意軟體政策
- 管理電子郵件惡意軟體政策
- 使用清單來改善病毒掃描效能
- 設定巢狀檔案的限制
- 保持病毒定義檔在最新狀態
- 修改人工智慧敏感程度

關於偵測病毒、惡意軟體與惡意攻擊

病毒和其他類型的惡意攻擊可導致郵件伺服器當機、網路停機時間，以及危害和破壞公司資料。Symantec Messaging Gateway 惡意軟體掃描會在電子郵件流中提供病毒和惡意威脅偵測。

建立惡意軟體政策以保護伺服器免於下列類型的攻擊：

病毒	Symantec Messaging Gateway 會在所有的主要檔案類型 (例如 Microsoft Word 檔案，包括壓縮檔案格式) 中，偵測病毒、病蟲以及特洛伊木馬程式。 請參閱第 177 頁的「偵測病毒與惡意攻擊的產品技術」。
大量郵件病蟲	Symantec Messaging Gateway 會偵測電子郵件是否為大量郵件病蟲或病毒。它會自動刪除受感染的電子郵件訊息和任何附件。
可疑附件	Symantec Messaging Gateway 會偵測顯示有病毒跡象的電子郵件。它也會偵測包含可疑新郵件流樣式的郵件，此樣式的郵件流包括電子郵件訊息附件。
加密的附件	受感染的檔案可能會被刻意加密。如果沒有適當的解密工具，就無法對加密的檔案進行解密和掃描。您可以架構要讓 Symantec Messaging Gateway 處理加密配置區檔案的方式。
潛在惡意內容	Symantec Messaging Gateway 的「解除」技術會偵測並移除電子郵件附件 (包括 Microsoft Office 文件和 Adobe PDF) 中的潛在惡意內容。您可以架構要解除的文件和內容類型。您可以解除巨集、JavaScript、Flash 和其他易受攻擊的內容。
廣告程式和間諜程式	Symantec Messaging Gateway 會偵測執行下列任何動作的安全風險： ■ 對電腦系統提供未授權的存取 ■ 透過記錄按鍵的方式竊取身分或進行詐騙 ■ 擷取電子郵件流量 ■ 搜尋個人資訊，例如密碼與登入識別 ■ 呈現某種類型的干擾或妨礙 請參閱第 184 頁的「間諜程式或廣告程式判斷詳細資訊」。

- Symantec Messaging Gateway 必須能夠分解並掃描配置區檔案，以偵測病毒。您可以指定配置區檔案的大小上限與掃描深度層級，以減少接觸 zip 炸彈或阻絕服務攻擊的機會。
  請參閱第 196 頁的「設定巢狀檔案的限制」。
- 當 Symantec Messaging Gateway 掃描郵件並偵測惡意軟體政策違規時，會執行您在該政策中指定的判斷。
  請參閱第 187 頁的「建立電子郵件惡意軟體政策」。
  請參閱第 169 頁的「為政策群組選取惡意軟體政策」。
- 您必須擁有有效的防毒授權，才能執行防毒掃描功能以及取得更新的病毒定義檔。
  請參閱第 614 頁的「授權您的產品」。

為獲得額外防護，您可以將 Symantec Messaging Gateway 與 Symantec Content Analysis 整合以掃描檔案和附件中是否存在進階威脅。

請參閱第 390 頁的「關於威脅防禦掃描」。

偵測病毒與惡意攻擊的產品技術

表 9-1 說明 Symantec Messaging Gateway 用來偵測病毒、惡意攻擊和潛在惡意內容的技術。

表 9-1 偵測病毒與惡意攻擊的技術

技術	說明
防毒引擎	防毒引擎透過多執行緒掃描系統，提供快速又可靠的病毒防護。它會掃描內送與外寄電子郵件串流量。它會識別並清除包含病毒與相關惡意可執行檔的郵件。它也會嘗試修復電子郵件附件內的病毒。 防毒引擎本身無法修改。
人工智慧技術	此產品會使用靜態和動態人工智慧技術來偵測疑似病毒的行為，以識別不明的病毒。您可以將人工智慧敏感設定調整為以較積極或較不積極的方式識別病毒。 請參閱第 202 頁的「修改人工智慧敏感程度」。
病毒定義	病毒定義每小時提供一次，以防止遭到最新、快速散播的威脅。 Symantec LiveUpdate 是硬體裝置用來接收最新病毒定義檔的程序。硬體裝置預設會下載取得經認證的病毒定義檔。 您可以架構要取得更新定義的方式和時間。 請參閱第 198 頁的「關於更新病毒定義」。
防毒政策	您可以建立政策來偵測病毒或惡意攻擊。 建立政策時，您可以指定違反政策時 Symantec Messaging Gateway 要採取的動作。例如，您可以清除受感染的附件，但會刪除整個間諜程式附件。 您可以視需要建立許多防毒政策。 請參閱第 187 頁的「建立電子郵件惡意軟體政策」。
初始偵測	此功能會在防毒定義可用之前，先利用賽門鐵克的電子郵件威脅檢視與啟發式分析，來識別可疑的附件。包含可疑附件的郵件可能會移至「可疑病毒隔離所」。Symantec Messaging Gateway 會依照您指定的時間長度 (最多 24 小時)，將此郵件保留在隔離所中。之後，它會釋放郵件以再次使用更新的病毒定義進行掃描。 您可以建立包含判斷的病毒政策，以隔離可疑的郵件附件。您也可以架構附件保留在「可疑病毒隔離所」中的時間長度。 請參閱第 204 頁的「關於隔離可疑病毒」。
解除	「解除」會掃描電子郵件附件中的 Microsoft Office 和 PDF 文件是否包含潛在惡意內容 (PMC)。潛在惡意內容包括巨集、Flash 影片，以及其他易受攻擊的內容。「解除」會對其中包含潛在惡意內容 (PMC) 的附件進行解構、移除 PMC，然後重建並傳送已經安全的附件。您可以選擇嘗試要移除或重建的文件類型和 PMC 類型。您也可以封存原始未更改的文件，以便稍後進行擷取。 請參閱第 179 頁的「關於「解除」」。

技術	說明
威脅防禦	威脅防禦將 Symantec Messaging Gateway 與 Symantec Content Analysis 整合以偵測進階威脅。然後，Symantec Messaging Gateway 會將威脅防禦政策套用到電子郵件訊息。 請參閱第 390 頁的「關於威脅防禦掃描」。 當您在**「惡意軟體」>「設定」>「電子郵件掃描設定」>「解除」**標籤上為內容類型啟用「解除」時，威脅防禦政策也可以解除附件。

關於「解除」

Symantec Messaging Gateway 的解除技術可從電子郵件附件找到和移除潛在惡意內容 (PMC)。您可以同時掃描入埠郵件和離埠郵件，以偵測可能包含 PMC 的 Microsoft Office 和 Adobe PDF 附件。PMC 類型包括巨集、程序檔、Flash 內容，以及其他易受攻擊的內容。

附註：解除無法決定其偵測和移除的內容是否是惡意的。它反而會偵測指定文件類型範圍中的指定內容類型是否有潛在被利用的可能，然後移除它們。

啟用「解除」之後，它會偵測附加文件中是否存在 PMC，解構附件，移除 PMC，然後重建文件。您可以選擇要嘗試移除的文件和 PMC 類型。您還可以選擇封存原始文件以供日後擷取。

解除是作為 Symantec Messaging Gateway 初始偵測功能的延伸功能來實作。它會擴充賽門鐵克分解程式的功能來：

- 以遞迴方式從配置區文件類型解壓縮內嵌物件。
- 過濾掉可能有害的內容 (巨集、程序檔、可執行檔、無法辨識的內容、未參照的物件)。
- 將可能有害的物件取代為無害或重建版本。
- 重建配置區文件，然後重新附加到電子郵件。

「解除」不支援掃描加密或受密碼保護的附件，也不支援掃描使用非支援格式 (例如 RAR) 壓縮的附件。如果支援的配置區文件巢狀於其他支援的文件內，解除會解構文件，直到其處理最後一份巢狀文件或達到配置區限制為止。接著，「解除」會從支援的類型移除 PMC，然後重建並重新附加文件。

請參閱第 196 頁的「設定巢狀檔案的限制」。

附註：移除 PMC 和重建文件可能會影響視覺逼真度和功能。重建文件中的文字格式或影像的外觀可能有所不同。如果原始文件包含像是以巨集實作的文字輸入欄位元素，功能可能無法運作。如果您選擇從郵件移除內嵌檔案和附件，則內容可能會遺失。解除也可能會影響 Symantec Messaging Gateway 的整體傳輸速度，如果選擇掃描所有支援的附件和 PMC 類型，其影響尤為顯著。

若要啟用解除，您可以啟用設定以指定要解除的內容類型。然後，您可以建立使用解除的惡意軟體或威脅防禦政策，並將政策套用至政策群組。您也可以選擇可讓您略過解除的內容過濾動作。

請參閱第 180 頁的「使用「解除」移除潛在惡意內容」。

使用「解除」移除潛在惡意內容

不同於多數其他電子郵件惡意軟體政策，**「解除: 解除附件」**政策動作預設不會啟動，儘管它已啟用。若要啟用它，請執行下列操作：

- 架構電子郵件掃描設定以指定要偵測的配置區文件和 PMC 類型。
- 架構一個電子郵件惡意軟體政策，用於偵測配置區文件中是否存在指定的 PMC 類型並包含解除 PMC 的動作。
- 將此政策套用至一或多個政策群組。

您也可以對移除 PMC 的郵件加上註釋，標示主旨行，以及封存原始郵件以供日後擷取。任何可新增至其他惡意軟體政策的動作也可新增至**「解除: 解除附件」**政策。

附註：您也可以將威脅防禦政策架構為使用解除。

請參閱第 398 頁的「建立新的威脅防禦政策集」。

表 9-2 說明您執行以偵測及移除潛在惡意內容的工作。您可以任何順序執行這些工作。

表 9-2 解除潛在惡意內容

工作	說明
架構電子郵件掃描設定以指定要移除的文件和 PMC 類型。	在**「惡意軟體」**頁面上，選取**「電子郵件掃描設定」**，然後選取**「解除」**標籤。指定要偵測哪些文件類型，以及指定要解除每個文件類型內的哪些潛在惡意內容類型。 如果您發現 PDF 附件受到「解除」的負面影響，也可以啟用**「前置處理不合格的 PDF」**。 請參閱第 181 頁的「潛在惡意內容詳細資料」。獲取有關文件和 PMC 類型的詳細資料。

工作	說明
選取預設值或建立新的「解除」政策。	Symantec Messaging Gateway 隨附一個預先架構且會啟用的預設「解除」政策，但是不會套用於任何使用者群組。您可以依原狀使用此預設政策，也可以修改它來建立您自己的自訂政策。您也可以選擇將 PMC 偵測功能新增至其他現有的政策。 使用預設 PMC 政策： 在**「電子郵件惡意軟體政策」**頁面上，選取**「解除: 解除附件」**政策。在**「動作」**區域中，選取**「解除附件」**，然後按下**「儲存」**。 請參閱第 188 頁的「預設電子郵件惡意軟體政策」。 請參閱第 187 頁的「建立電子郵件惡意軟體政策」。
將解除政策套用至政策群組。	您可以使用下列兩種方式之一，將解除政策套用至政策群組： ■ 在**「電子郵件惡意軟體政策」**頁面上，選取**「解除: 解除附件」**政策。在**「套用至下列政策群組」**區域中，選取所需的政策群組，然後按下**「儲存」**。 ■ 在**「管理」**標籤中的**「使用者」**下，選取**「政策群組」**。從清單中選取政策群組，然後按下**「惡意軟體」**標籤。為惡意軟體掃描啟用**「解除: 解除附件」**政策，然後按下**「儲存」**。請注意，解除預設會套用至入埠掃描，但是您也可以選擇解除離埠附件。
指定解除政策的其他動作。	任何可新增至其他惡意軟體政策的動作也可新增至解除政策。例如，您可以對移除 PMC 的郵件加上註釋，隔離具有 PMC 的郵件，以及封存原始郵件以供日後擷取。 請參閱第 183 頁的「關於擷取解除的內容」。
監控報告。	查看報告以追蹤 PMC 偵測和政策。報告也可以指出您組織接收到的潛在威脅數量。此資訊可以協助您微調威脅偵測設定。

潛在惡意內容詳細資料

Symantec Messaging Gateway 可以偵測數種常見電子郵件附件類型 (Word、Excel、PowerPoint、PDF) 中的潛在惡意內容。表 9-3 列出和描述每種類型的 PMC，以及說明從配置區文件移除 PMC 的後果。

表 9-3 潛在惡意內容配置區和內容類型詳細資料

類別	說明
內嵌檔案和附件 支援的檔案類型：Office 2003、Office 2007 和更新版本，以及 PDF	偵測內嵌或附加於另一個檔案或文件中的惡意軟體，其複雜程度高於直接內含在電子郵件中的惡意軟體。「解除」可讓您以遞迴方式重建或移除內嵌的檔案和附件，不僅僅從郵件本身，也會從郵件的附加文件重建或移除。每個開啟之附加或內嵌的文件都會被掃描是否有附加或內嵌的物件，直到達到**「SMTP 通訊協定設定」**頁面上**「配置區限制」**區域中指定的限制。只要檔案類型受支援，就會重建附加的檔案或內嵌檔案。否則，就會移除。某些通常不是惡意的檔案類型 (例如影像檔) 會予以忽略，而不是重建或移除。 **移除的後果:** 移除內嵌或附加的檔案可能導致內容遺失。您可以封存要移除其中內嵌檔案和附件的郵件，以便稍後可以復原內容。 附加的文件有時包含用於開啟文件中其他內嵌文件的圖示。如果在「解除」掃描設定中停用內嵌文件類型，則「解除」會保留圖示，並將停用的文件類型的內容取代為一段說明內容是故意移除的文字。按下圖示時，會顯示此文字。 如果您發現 PDF 附件變得無法讀取，請在**「惡意軟體」>「掃描設定」>「解除」**標籤上啟用**「前置處理不合格的 PDF」**。此功能會識別並嘗試修復不符合已發佈 PDF 標準的 PDF 文件結構。這項前置處理作業有助於「解除」在掃描後適當重新建構這些 PDF。
Flash 支援的檔案類型：Office 2003、Office 2007 和更新版本，以及 PDF	Flash 內容 (特別是未經修正的 Flash Player) 是網頁和文件中常見的惡意軟體傳播媒介。 **移除的後果:** Flash 內容會從附件中移除並取代為具有黑色外框的白色矩形。
巨集 支援的檔案類型：Office 2003 及 Office 2007 和更新版本	巨集用於在文件中提供額外功能。通常一開啟文件就會執行巨集，因此常被利用作為惡意軟體的傳播媒介。 **移除的後果:** 遺失巨集型功能，包括自訂增益集、對話方塊，以及資料解壓縮程序。
3D 元件 支援的檔案類型：PDF	PDF 格式支援包含使用通用 3D 檔案格式的 3D 內容。選取此選項時，解除會刪除所有 3D 元件。 **移除的後果:** 遺失 3D 預覽之類的功能。

類別	說明
字型 支援的檔案類型： PDF	內嵌在 PDF 檔案中的字型可被利用作為惡意軟體的傳播媒介。選取此選項時，解除會刪除內嵌的字型。 **移除的後果:** 如果端點上沒有可用的替代字型，可能會改變視覺逼真度。管理員可選擇將已知的安全替換字型散佈到他們組織的端點，以減少解除之附件的視覺逼真度問題。
結尾資訊 支援的檔案類型： PDF	PDF 檔案是由標頭、本文、交互參照表和結尾所組成。結尾包含根物件和交互參照表的相關資訊。只要在結尾中加入其他物件，就可以將結尾用於惡意用途。 **移除的後果:** 無。不會遺失功能或逼真度。
JavaScript 支援的檔案類型： PDF	PDF 中的 JavaScript 最常用於變更文件內容以回應某些事件。例如，JavaScript 可用於在列印文件前隱藏文件的某個部分，還可用於在文件開啟時預先填入表單欄位。JavaScript 也可用於限制 Acrobat Reader 的動作 (例如，驗證在 PDF 表單欄位中輸入的資料)，還可用於在文件中引入惡意程式碼。 **移除的後果:** 遺失 JavaScript 提供的功能。
啟動 支援的檔案類型： PDF	「啟動」功能是可讓您從 PDF 內部啟動可執行檔的 PDF 功能 (預設為啟用)。惡意軟體建立者利用此功能已有一段時間。選取此選項時，會停用「啟動」功能。 **移除的後果:** PDF 無法再啟動其他程序或應用程式。依賴於啟動其他文件或程序的增益集、範本和工具都無法再正常運作。
XFA (及其 Javascript) 支援的檔案類型： PDF	XFA (XML 表單架構) 是一組專用的 XML 規格，用於增強網頁表單的處理能力。選取此選項時，「解除」會同時移除與其關聯的 XFA 和 JavaScript。 **移除的後果:** 遺失 XFA 提供的功能。表單的視覺配置通常不受影響，但其互動功能可能會遺失。
全螢幕 支援的檔案類型： PDF	PDF 文件的全螢幕模式可用於惡意模擬 GUI 或 Internet 網站，以誘騙使用者輸入敏感的資訊。為了防止這類不當用途，解除會阻止 PDF 附件使用全螢幕功能。 **移除的後果:** 遺失用於合法及潛在惡意用途的全螢幕功能。

關於擷取解除的內容

使用「解除」從電子郵件附件移除潛在惡意內容 (PMC)，可能會影響重建文件的視覺逼真度和功能。例如，如果將內嵌字型移除並取代為系統字型，文件的外觀可能有所變化。如果原始文件包含以巨集實作的元素 (例如，文字輸入表單)，功能可能無法運作。解除附件之後，輸入欄

位可能仍然存在於重建文件中，但不會再提供輸入驗證或視覺回應。同樣，移除 JavaScript 之後，由 JavaScript 控制的滑鼠動作或鍵盤輸入將不再起作用。

移除 PMC 還可能導致整份文件中的功能都無法運作，甚至遺失內容。例如，如果您解除 Microsoft Office 文件中的所有巨集，則使用巨集的 Excel 試算表將無法再正常運作。同樣的，如果您選擇從電子郵件重建內嵌檔案和附件，則「解除」不支援的附加或內嵌內容將會被捨棄。

將所有郵件連同附件一起封存，是保留原始內容及其所有功能的唯一方法。若要封存郵件，首先您要指定儲存封存檔的位置。然後指定「封存郵件」作為解除政策的動作。在**「編輯電子郵件惡意軟體政策」**頁面上的**「動作」**區域中，按下**「新增」**，然後從**「架構動作」**下拉式清單中選取「封存郵件」。

對付可疑附件所採取的動作

建立政策並選擇「如果郵件包含可疑附件」條件時，會有兩個額外選項可以使用，如下所示：

將郵件保留在可疑病毒隔離所	選取此選項來隔離郵件和所有附件。
刪除和延遲可疑病毒隔離所中的郵件	選取此選項來刪除可疑附件並隔離郵件。選取此選項時，就無法擷取可疑附件。

上述兩個動作都會將郵件移至隔離所。郵件會在經過所指定的時間長度之後進行重新掃描。不過，此時會使用可用的最新定義檔來掃描郵件。

請參閱第 204 頁的「關於隔離可疑病毒」。

請參閱第 187 頁的「建立電子郵件惡意軟體政策」。

間諜程式或廣告程式判斷詳細資訊

Symantec Messaging Gateway 可偵測安全風險。

安全風險是指執行下列其中一項動作的程式：

- 對電腦系統提供未授權的存取
- 危害資料完整性、隱私權、機密性或安全性
- 呈現某種類型的干擾或妨礙

Symantec Messaging Gateway 會針對偵測到的所有安全風險套用間諜程式或廣告程式判斷。

請參閱第 176 頁的「關於偵測病毒、惡意軟體與惡意攻擊」。

表 9-4 列出 Symantec Messaging Gateway 偵測到的安全風險類別。

表 9-4 包含在間諜程式或廣告程式判斷中的安全風險類別

類別	說明
廣告程式	透過 Internet 收集個人資訊，並在使用者不知情的狀況下，轉遞回遠端電腦的獨立式或附加程式。 廣告程式可能會監控為廣告目的之瀏覽習慣， 也會傳送廣告內容。
駭客工具	用以取得未授權之使用者電腦存取權限的程式。 例如，按鍵側錄程式會追蹤並記錄各個按鍵，並將此資訊傳送至遠端電腦。遠端使用者可執行通訊埠掃描或漏洞掃描。駭客工具也可用來製造病毒。
撥號工具	在未經使用者許可或察覺的狀況下，使用電腦透過 Internet 撥號至 900 號碼台或 FTP 網站的程式。這些程式通常會有費用產生。
惡作劇程式	更改或打斷電腦運作，刻意製造幽默效果或造成困擾的程式。 例如，惡作劇程式可能會在使用者嘗試點選資源回收筒時，刻意讓滑鼠點不到該圖示。
遠端存取程式	讓遠端使用者透過 Internet 取得對某電腦的存取權，以取得資訊、攻擊或更改主機電腦的程式。
間諜程式	可以秘密監控系統活動的獨立式程式。這些程式能夠偵測密碼及其他機密資訊，然後將資訊轉遞回遠端電腦。

偵測病毒、惡意軟體與惡意威脅

表 9-5 說明您可執行以偵測病毒與惡意威脅的工作。您可以任何順序執行任一或所有工作。

表 9-5 偵測病毒、惡意軟體與惡意威脅

工作	說明
電子郵件病毒攻擊識別。	在電子郵件病毒攻擊中，會從某特定 IP 位址接收到指定數量的受感染電子郵件訊息。預設會延遲來自違規寄件者的所有連線。電子郵件病毒攻擊識別預設為停用，必須啟用才能加以啟動。 請參閱第 127 頁的「架構電子郵件病毒攻擊辨識」。
建立並啟用電子郵件惡意軟體政策。	Symantec Messaging Gateway 隨附預先架構的惡意軟體政策，這些政策會自動啟用。您可以修改這些政策並建立總覽政策。 請參閱第 188 頁的「預設電子郵件惡意軟體政策」。 請參閱第 187 頁的「建立電子郵件惡意軟體政策」。

工作	說明
設定人工智慧敏感程度。	Symantec Messaging Gateway 包含靜態和動態人工智慧技術。此技術會掃描是否存在異常行為 (例如自我複寫)，從而找到可能受感染的郵件內文與附件。 預設設定是「中」。不過，您可以修改此設定或關閉偵測。人工智慧掃描需要您在惡意軟體偵測率和誤報之間做出取捨。較低的人工智慧敏感程度可能會遺漏掉更多的惡意軟體，但會產生較少的誤報。較高的人工智慧敏感程度可能會捕捉到更多惡意軟體，但導致出現更多的誤報偵測。 請參閱第 202 頁的「修改人工智慧敏感程度」。
指定可以略過防毒掃描的檔案類型。	您可以指定能夠略過防毒掃描的檔案類型。例如，某些檔案類型通常不會包含病毒，例如 .mpg 檔案。您確定不包含病毒的檔案類型都可以略過病毒掃描，以節省系統資源。 Symantec Messaging Gateway 會提供檔案類型類別的預設清單。不過您必須建立「排除掃描清單」，再選取您要納入的類別，然後啟用清單。您也可以從「排除掃描清單」中新增或移除檔案類型。 請參閱第 193 頁的「將檔案類型排除在病毒掃描範圍之外」。
架構「可疑病毒隔離所」。	您可以建立病毒政策，以將可疑的郵件附件隔離在「可疑病毒隔離所」中。 賽門鐵克提供下列「可疑病毒隔離所」設定的預設值；不過，您可以視需要變更這些設定： ■ 郵件保留在隔離所中的時間上限 預設設定為 6 小時。 ■ 隔離所可用的磁碟空間 預設設定為 10 GB。 請參閱第 204 頁的「關於隔離可疑病毒」。
啟用定義更新。	LiveUpdate 預設為啟用。白金級定義更新排程為星期一到星期五每 10 分鐘出現一次。不過，您可以修改要取得更新的時間和方式。 請參閱第 198 頁的「關於更新病毒定義」。
架構疫情通知警示。	設定警示通知，可讓您瞭解是否發生下列任一與病毒相關的事件： ■ 已偵測到疫情 ■ 惡意軟體過濾的時間早於您指定的期間 ■ 取得新的惡意軟體過濾 ■ 防毒授權已過期 請參閱第 590 頁的「架構警示」。
監控報告。	監控報告可以判斷病毒偵測和政策的有效程度。報告也可以指出您組織接收到的威脅數量。此資訊可以協助您微調防毒偵測與威脅偵測設定。

建立電子郵件惡意軟體政策

Symantec Messaging Gateway 安裝時，會一併安裝數個預先架構的惡意軟體政策，依預設會啟用這些政策。除了這些政策之外，您還可以建立自己的自訂政策。內容過濾、垃圾郵件與惡意軟體政策名稱必須是唯一的。例如，如果您的內容過濾政策名為 XYZ，則垃圾郵件政策或惡意軟體政策名稱不能是 XYZ。電子郵件惡意軟體政策預設會在建立之後啟用。

請參閱第 188 頁的「預設電子郵件惡意軟體政策」。

建立電子郵件惡意軟體政策

1. 在控管中心內，按下**「惡意軟體」>「政策」>「電子郵件」**。
2. 按下**「新增」**。
3. 在**「政策名稱」**方塊中，輸入惡意軟體政策的名稱。
4. 在**「條件」**下，按下**「套用至」**下拉式清單，然後選擇應套用惡意軟體政策的郵件類型：
   - 入埠郵件
   - 離埠郵件
   - 入埠和離埠郵件
     此選項可在您架構政策群組時，於**「惡意軟體」**標籤上指定此惡意軟體政策可用的位置。
     例如，假設您選擇**「入埠郵件」**與**「如果郵件含有大量郵件病蟲」**條件。當您架構政策群組時，只能在**「入埠大量郵件病蟲政策」**清單中找到此惡意軟體政策。
5. 按下**「如果符合下列條件」**下拉式清單，來選取一個條件。
6. 在**「動作」**下，按下**「新增」**。

   在**「架構動作」**頁面上，按下拉式清單，然後選取動作。

   某些動作需要在該動作下面的欄位中指定其他資訊。

   例如，假設您選取**「轉寄郵件的副本」**動作。您可以在出現的方塊中，輸入要轉寄該郵件的收件者電子郵件地址。

   請參閱第 285 頁的「政策動作及其功能」。

   請參閱第 169 頁的「為政策群組選取惡意軟體政策」。
7. 按下**「新增動作」**。

   您可以視需要新增多個動作，但動作不可互相衝突。
8. 在**「政策群組」**下，勾選應套用此政策的一或多個群組。
9. 按下**「儲存」**。

預設電子郵件惡意軟體政策

Symantec Messaging Gateway 安裝時會一併安裝預先架構的惡意軟體政策。預設會啟用這些政策，您可以將這些政策套用至政策群組。您可以停用或修改政策動作，以及套用政策的政策群組。對於標示為預設的預先架構病毒政策，您無法修改其政策名稱、政策所套用的郵件類型以及必須符合的條件。

請參閱第 187 頁的「建立電子郵件惡意軟體政策」。

請參閱第 169 頁的「為政策群組選取惡意軟體政策」。

表 9-6 預設電子郵件惡意軟體政策

政策名稱	套用至下列郵件	如果符合下列條件	動作	套用至下列政策群組	預設狀態
病毒：清除郵件 (預設)	入埠和離埠郵件	郵件包含病毒	清除郵件	預設群組	預設啟用
病蟲：刪除郵件 (預設)	入埠和離埠郵件	郵件包含大量郵件病蟲	刪除郵件	預設群組	預設啟用
因解除而無法掃描：正常傳送	入埠和離埠郵件	無法掃描郵件是否存在潛在惡意內容	正常傳送郵件	無	預設啟用
因任何原因而無法掃描是否存在惡意軟體和內容過濾：刪除郵件 (預設)	入埠和離埠郵件	無法掃描郵件是否存在惡意軟體和內容過濾	刪除郵件	預設群組	預設啟用
加密的附件：使用「[警告 - 未掃描加密的附件是否包含病毒]」修改郵件主旨行	入埠和離埠郵件	郵件包含加密附件	在主旨行前面加上「[警告 - 未掃描加密的附件是否包含病毒]」	預設群組	預設啟用
病毒：刪除郵件	入埠和離埠郵件	郵件包含病毒	刪除郵件	無	預設啟用
病毒：使用「[已感染病毒]」修改郵件主旨行	入埠和離埠郵件	郵件包含病毒	在主旨行前面加上「[已感染病毒]」	無	預設啟用
病毒：正常傳送	入埠和離埠郵件	郵件包含病毒	正常傳送郵件	無	預設啟用
病蟲：清除郵件	入埠和離埠郵件	郵件包含大量郵件病蟲	清除郵件	無	預設啟用

政策名稱	套用至下列郵件	如果符合下列條件	動作	套用至下列政策群組	預設狀態
病蟲：使用「[已感染病蟲]」修改郵件主旨行	入埠和離埠郵件	郵件包含大量郵件病蟲	在主旨行前面加上「[已感染病蟲]」	無	預設啟用
病蟲：正常傳送	入埠和離埠郵件	郵件包含大量郵件病蟲	正常傳送郵件	無	預設啟用
因任何原因而無法掃描是否存在惡意軟體和內容過濾：使用「[警告-未掃描是否包含病毒]」修改郵件主旨行	入埠和離埠郵件	無法掃描郵件是否存在惡意軟體和內容過濾	在主旨行前面加上「[警告 - 未掃描是否包含病毒]」	無	預設啟用
因任何原因而無法掃描是否存在惡意軟體和內容過濾：正常傳送	入埠和離埠郵件	無法掃描郵件是否存在惡意軟體和內容過濾	正常傳送郵件	無	預設啟用
解除：解除附件	預設為僅入埠，但是您也可以選擇將其套用至離埠郵件。	其附件含潛在惡意內容的郵件，且您在**「惡意軟體」>「掃描設定」>「電子郵件掃描設定」>「解除」**標籤上選取要移除的配置區文件和解除內容類型。	對附件進行解構、移除潛在惡意內容、重建附件，然後正常傳送	無	預設為啟用，但是只有在「解除」標籤上選取文件和解除內容類型且此政策套用於群組時，才會套用。
威脅：使用「[已感染間諜程式或廣告程式]」修改郵件主旨行(預設)	入埠和離埠郵件	郵件包含間諜程式或廣告程式 請參閱第 184 頁的「間諜程式或廣告程式判斷詳細資訊」。	在主旨行前面加上「[已感染間諜程式或廣告程式]」	預設群組	預設啟用

政策名稱	套用至下列郵件	如果符合下列條件	動作	套用至下列政策群組	預設狀態
入埠可疑病毒：刪除附件並將郵件保留在可疑病毒隔離所 (預設)	入埠郵件	郵件包含可疑附件	刪除和延遲可疑病毒隔離所中的郵件，並加上「已刪除您郵件的某個部分，因為它們是可疑病毒。」	預設群組	預設啟用
離埠可疑病毒：將郵件保留在可疑病毒隔離所 (預設)	離埠郵件	郵件包含可疑附件	將郵件保留在可疑病毒隔離所	預設群組	預設啟用

管理電子郵件惡意軟體政策

表 9-7 說明您可管理電子郵件惡意軟體政策的方式。您可以視需要以任何順序執行這些工作。

表 9-7 管理電子郵件惡意軟體政策

工作	說明
修改電子郵件惡意軟體政策。	您可以視需要修改電子郵件惡意軟體政策。您可以修改預設電子郵件惡意軟體政策或自己的自訂政策。 請參閱第 191 頁的「修改電子郵件惡意軟體政策」。
啟用或停用電子郵件惡意軟體政策。	您必須啟用政策，Symantec Messaging Gateway 才能用它來評估電子郵件。當您建立新政策時，預設會自動啟用它。Symantec Messaging Gateway 預先安裝的政策預設也會自動啟用。 請參閱第 191 頁的「啟用或停用電子郵件惡意軟體政策」。
刪除電子郵件惡意軟體政策。	如果您不再需要某項惡意軟體政策，可將其刪除。刪除後，該政策將永久移除，且無法還原。 如果您不確定是否要永久刪除某項政策，可考慮將其停用。 請參閱第 192 頁的「刪除電子郵件惡意軟體政策」。
複製電子郵件惡意軟體政策。	您可能需要建立與現有政策類似的新政策。您無需從頭開始建立政策，只需將其複製，然後視需要修改新建立的政策即可。 請參閱第 192 頁的「複製電子郵件惡意軟體政策」。

修改電子郵件惡意軟體政策

您可以修改預設和自訂電子郵件惡意軟體政策，以進行微調或擴大或縮小其範圍。

表 9-8說明您可以修改的預設電子郵件惡意軟體政策和自訂電子郵件惡意軟體政策設定。

表 9-8　　可修改的電子郵件惡意軟體政策設定

設定值	可於預設政策修改	可於自訂政策修改
政策名稱	否	是
套用至	否	否
如果符合下列條件	否	否
執行下列動作	是	是
套用至下列群組	是	是

修改電子郵件惡意軟體政策

1. 在控管中心內，按下**「惡意軟體」>「政策」>「電子郵件」**。
2. 勾選要修改之政策旁的方塊，然後按下**「編輯」**。
3. 進行所需的修改。
4. 按下**「儲存」**。

啟用或停用電子郵件惡意軟體政策

預設會啟用預設的電子郵件惡意軟體政策。當您建立新的電子郵件惡意軟體政策時，預設會啟用該政策。您可以停用不想讓 Symantec Messaging Gateway 在掃描電子郵件時使用的任何政策。

您可以停用惡意軟體政策，以疑難排解電子郵件惡意軟體掃描問題。您也可以建立自訂電子郵件惡意軟體政策以因應疫情，並在疫情結束時將其停用。您可以在發生另一個疫情時開啟該政策。

您也可以停用不再使用但還不想刪除的政策。

啟用或停用電子郵件惡意軟體政策

1. 在控管中心內，按下「**惡意軟體**」>「**政策**」>「**電子郵件**」。
2. 勾選您要啟用或停用之政策旁的方塊。
3. 按下下列其中一個選項：

啟用	啟用政策時，「**已啟用**」欄會顯示綠色勾號。
停用	停用政策時，「**已啟用**」欄會顯示水平線。

請參閱第 192 頁的「刪除電子郵件惡意軟體政策」。

刪除電子郵件惡意軟體政策

您可以刪除不再需要的電子郵件惡意軟體政策。但是，刪除政策之後即無法回復。如果不確定是否要永久刪除政策，您可以改為將它停用。

請參閱第 191 頁的「啟用或停用電子郵件惡意軟體政策」。

刪除電子郵件惡意軟體政策

1. 在控管中心內，按下「**惡意軟體**」>「**政策**」>「**電子郵件**」。
2. 勾選您要刪除之政策旁的方塊。
3. 按下「**刪除**」。
4. 按下確認對話方塊中的「**確定**」。

複製電子郵件惡意軟體政策

有些時候您可能會建立複雜的電子郵件惡意軟體政策，而且想要據以建立只包含少數修改的類似政策。Symantec Messaging Gateway 可讓您複製電子郵件惡意軟體政策。

當您複製電子郵件惡意軟體政策時，新政策的名稱不能與任何現有政策相同。例如，如果您的內容過濾政策名為 XYZ，則垃圾郵件政策或惡意軟體政策名稱不能是 XYZ。電子郵件惡意軟體政策預設會在建立之後啟用。

複製電子郵件惡意軟體政策

1. 在控管中心內，按下「**惡意軟體**」>「**政策**」>「**電子郵件**」。
2. 勾選您要複製之政策旁的方塊。
3. 按下「**複製**」。
4. 在「**新增電子郵件惡意軟體政策**」頁面上，鍵入新的政策名稱。
5. 進行您所需的任何其他變更。
6. 按下「**儲存**」。

使用清單來改善病毒掃描效能

您可以建立要從病毒掃描排除的檔案類型清單。您可以修改隨產品一起安裝的預設清單，以建立自訂清單。

表 9-9說明您可對註釋執行的動作。您可以視需要以任何順序執行這些工作。

表 9-9 管理病毒掃描清單

工作	說明
建立包含能夠略過防毒掃描的檔案類型之清單。多重清單可協助您分類檔案類型。	病毒與惡意威脅通常包含在可執行檔類型中。您可以讓不包含可執行檔的檔案類型略過掃描，以改善掃描效能。 請參閱第 193 頁的「將檔案類型排除在病毒掃描範圍之外」。
微調惡意軟體掃描政策時，修改要從掃描範圍排除的檔案類型。	例如，您可能發現某些惡意可執行檔被修改為看起來無害的檔案類型。因此，您想要從排除掃描檔案清單中移除可能會被利用的檔案類型。 請參閱第 194 頁的「修改要從掃描範圍排除的檔案類型」。
視需要啟用或停用清單。	您可以有多個要從掃描範圍排除的檔案類型清單。但是，除非啟用某清單，否則系統不會略過該清單中的檔案類型而不予掃描是否有病毒。建立清單之後，預設會啟用該清單。停用不想讓 Symantec Messaging Gateway 在掃描電子郵件時使用的任何清單。 您可以停用清單，以疑難排解電子郵件病毒掃描問題。您也可以建立自訂清單以因應疫情，並在疫情結束時將其停用。您可以在發生另一個疫情時重新啟用該清單。您也可以停用不再使用但不想刪除的清單。 請參閱第 195 頁的「啟用或停用要從掃描範圍排除的檔案類型清單」。
刪除要從掃描範圍排除、不再需要的檔案類型清單。	刪除清單後，便無法回復該清單的內容。 請參閱第 196 頁的「刪除要從掃描範圍排除的檔案類型清單」。
將要從掃描範圍排除的檔案類型清單匯出至文字檔。	在下列情況中，您可能想要匯出檔案類型： ■ 您想要有一份檔案類型清單，以便分送給組織中需要知道系統會略過哪些檔案類型不予掃描的人員。 ■ 您想要在複製、修改或刪除清單之前封存檔案類型清單副本。 請參閱第 196 頁的「匯出要從掃描範圍排除的檔案類型清單」。

將檔案類型排除在病毒掃描範圍之外

Symantec Messaging Gateway 可讓您建立要從病毒掃描中排除的檔案類型清單。您可以建立單一清單，也可以建立多個清單，以協助您分類檔案類型。

為了協助您建立自己的清單，Symantec Messaging Gateway 會提供分組類似檔案類型的檔案類別。您可以選擇檔案類別中的每個檔案類型，也可以選取要從病毒掃描中排除的個別檔案類型。此外，還可以選取**「所有檔案類別」**以建立 SMG 提供的每個檔案類別的清單。

從威脅防禦掃描中排除檔案類型

1 在控管中心內，按下「**惡意軟體**」>「**設定**」>「**電子郵件掃描設定**」。

2 在「**排除掃描**」標籤上，按下「**新增**」。

3 在「**排除掃描清單名稱**」方塊中，輸入清單的名稱。

4 在「**檔案類別**」清單中，選取您要從掃描中排除的檔案類別。

- 若要選取多個類別，請按住 **Ctrl** 鍵並同時按下檔案類別的名稱。
- 若要選取「**檔案類別**」清單中的每個檔案類別，請按下「**所有檔案類別**」。

5 「**檔案類型**」清單會顯示與所選檔案類別相關聯的所有檔案類型。

- 若要從病毒掃描中排除「**檔案類型**」清單中的每個檔案類型，請按下「**新增檔案類別**」。
- 若要從排除清單中移除檔案類型，請在按住 **Ctrl** 鍵的同時取消選取檔案類型。然後，按下「**新增檔案類別**」以新增其餘的所選檔案類型。

6 按下「**儲存**」。

檔案類型的名稱隨即出現在「**說明**」清單中。

當您建立新清單時，預設會啟用它。如果您希望 SMG 在掃描期間使用排除掃描清單，則必須啟用該清單。如果某封郵件包含符合已排除檔案類型的附件，SMG 將不會對該檔案執行病毒掃描。在「**惡意軟體**」>「**設定**」>「**電子郵件掃描設定**」>「**排除掃描**」標籤上，可以編輯、刪除、停用、啟用或匯出排除掃描清單。

修改要從掃描範圍排除的檔案類型

微調掃描政策時，您可以修改要從掃描範圍排除的檔案類型。例如，您可能發現某些惡意可執行檔被修改為看起來無害的檔案類型。因此，您想要從排除掃描檔案清單中移除可能會被利用的檔案類型。

請參閱第 193 頁的「將檔案類型排除在病毒掃描範圍之外」。

修改要從掃描範圍排除的檔案類型

1 在控管中心內，按下「**惡意軟體**」>「**設定**」>「**電子郵件掃描設定**」。

2 按下「**排除掃描**」標籤。

3 勾選您要修改之「**排除掃描清單**」旁的方塊。

4 按下「**編輯**」。

5 執行下列其中一個工作：

新增檔案類型至該清單	在**「檔案類別」**清單中，選取您要從掃描中排除的檔案類別。 若要選取多個類別，請按住 **Ctrl** 鍵並同時按下檔案類別的名稱。 按下您要從中排除特定檔案類型的檔案類別。然後從**「檔案類型」**清單中選取檔案類型。 按住 **Ctrl** 可以選取多個檔案類型。 按下**「新增檔案類型」**。
從該清單中移除檔案類型	在**「說明」**之下，勾選您要刪除之檔案類型旁的方塊，再按**「刪除」**。

6 按下**「儲存」**。

請參閱第 195 頁的「啟用或停用要從掃描範圍排除的檔案類型清單」。

啟用或停用要從掃描範圍排除的檔案類型清單

您可以有多個要從掃描範圍排除的檔案類型清單。但是，除非啟用某清單，否則系統不會略過該清單中的檔案類型而不予掃描是否有病毒。建立清單之後，預設會啟用該清單。停用不想讓 Symantec Messaging Gateway 在掃描電子郵件時使用的任何清單。

您可以停用清單，以疑難排解電子郵件病毒掃描問題。您也可以建立自訂清單以因應疫情，並在疫情結束時將其停用。您可以在發生另一個疫情時重新啟用該清單。

您也可以停用不再使用但還不想刪除的清單。

啟用或停用要從掃描範圍排除的檔案類型清單

1 在控管中心內，按下**「惡意軟體」>「設定」>「電子郵件掃描設定」**。

2 按下**「排除掃描」**標籤。

3 勾選您要啟用或停用之政策旁的方塊。

4 選取下列其中一個選項：

啟用	啟用政策時，**「已啟用」**欄會顯示綠色勾號。
停用	停用政策時，**「已啟用」**欄會顯示水平線。

請參閱第 196 頁的「刪除要從掃描範圍排除的檔案類型清單」。

刪除要從掃描範圍排除的檔案類型清單

您可以刪除要從掃描範圍排除、不再需要的檔案類型清單。但是，刪除清單後，便無法回復該清單的內容。如果不確定是否要永久刪除清單，您可以改為將它停用。刪除清單之前，您可以先將它匯出以保留該清單作為記錄。

請參閱第 195 頁的「啟用或停用要從掃描範圍排除的檔案類型清單」。

刪除要從掃描範圍排除的檔案類型清單

1. 在控管中心內，按下**「惡意軟體」>「設定」>「電子郵件掃描設定」**。
2. 按下**「排除掃描」**標籤。
3. 勾選您要刪除之清單旁的方塊。
4. 按下**「刪除」**。
5. 按下確認對話方塊中的**「刪除」**。

匯出要從掃描範圍排除的檔案類型清單

您可以將要從掃描範圍排除的檔案類型清單匯出至文字檔。

在下列情況中，您可能想要匯出檔案類型：

- 您想要有一份檔案類型清單，以便分送給組織中需要知道系統會略過哪些檔案類型不予掃描的人員。
- 您想要在複製、修改或刪除清單之前封存檔案類型清單副本。

匯出要從掃描範圍排除的檔案類型清單

1. 在控管中心內，按下**「惡意軟體」>「設定」>「電子郵件掃描設定」**。
2. 按下**「排除掃描」**標籤。
3. 勾選包含您要匯出之檔案類型之清單旁的方塊。
4. 按下**「匯出」**。
5. 在確認對話方塊中，指定您要開啟檔案或儲存檔案。

設定巢狀檔案的限制

Symantec Messaging Gateway 處理某些壓縮檔案時，這些檔案可能會不斷擴大，直到耗盡系統記憶體為止。這一類的配置區檔案通常稱為「zip 炸彈」。 Symantec Messaging Gateway 可以自動挑出並刪除大型附件，以因應此類情形。它假設這類檔案可能是 zip 炸彈，且不該任由它耗盡系統資源。對檔案採取動作只是因為大小有問題，而不是因為可能含有病毒或其他違規的跡象。

您可以指定此大小臨界值，以及 Symantec Messaging Gateway 在記憶體中處理的最大解壓縮層級，也可以指定掃描配置區的時間限制。 如果達到架構的限制，Symantec Messaging Gateway 會執行您針對**「無法掃描是否存在惡意軟體和內容過濾」**類別所指定的動作。

下表說明在哪個臨界值時，無法使用您架構的各個選項來掃描配置區：

配置區掃描深度上限	如果配置區檔案 (例如 .zip 檔案或電子郵件訊息) 中的巢狀深度超過指定的數字。 請勿將此值設定過高。否則您可能容易遭受阻絕服務或 zip 炸彈 (包含許多層級的巢狀檔案) 的攻擊。
開啟配置區的時間上限	在掃描配置區附件 (例如 .zip 檔案) 時經過的指定時間。 使用此設定可偵測出未超過其他配置區設定的配置區，但仍包含配置區巢狀、大量檔案、大型檔案或這些檔案的組合。
開啟時個別檔案大小上限	配置區的任何個別元件在解壓縮時超出指定的大小。
開啟時累積檔案大小上限	配置區中所有檔案的總計大小在解壓縮時超出指定的大小。

設定巢狀檔案的限制

1. 在控管中心內，按下**「通訊協定」> SMTP >「設定」**，然後按下**「內容掃描」**標籤。
2. 在**「配置區限制」**下方的**「配置區掃描深度上限」**方塊中，輸入配置區深度的上限。
3. 在**「開啟配置區的時間上限」**方塊中輸入值，然後按下下拉式功能表指定**「秒」**、**「分鐘」**或**「小時」**。
4. 在**「開啟時個別檔案大小上限」**方塊中輸入檔案大小上限，然後按下下拉式功能表選取 **KB**、**MB** 或 **GB**。
5. 在**「開啟時累積檔案大小上限」**方塊中輸入累積的檔案大小上限，然後按下下拉式功能表選取 **KB**、**MB** 或 **GB**。
6. 按下**「儲存」**。

保持病毒定義檔在最新狀態

表 9-10說明您可保持病毒定義在最新狀態的所有方式。您可以視需要以任何順序執行這些工作。

表 9-10 維持最新病毒定義的方式

工作	說明
深入瞭解應維持最新定義的原因以及 Symantec Messaging Gateway 更新定義的方式。	Symantec Messaging Gateway 會根據最新資訊來偵測病毒和威脅。發生問題的最常見原因之一是病毒定義並非最新的。賽門鐵克會定期提供更新的病毒定義，其中含有關於所有新發現之病毒和威脅的必要資訊。定期更新該資訊可以獲得最完整的安全保護，並保護組織中的電腦免於受到感染，以及因疫情而造成停機。 請參閱第 198 頁的「關於更新病毒定義」。
監控您的定義更新狀態。	LiveUpdate 狀態提供下列詳細資料： ■ 上次 LiveUpdate 嘗試 ■ 上次病毒定義 LiveUpdate 狀態 ■ 病毒定義版本 (修訂) ■ 目前病毒定義名單 請參閱第 199 頁的「檢視病毒定義的狀態」。
排程自動更新，以確保您持續受到保護。	排程自動病毒定義更新之後，可確保您能從賽門鐵克取得可用的最新病毒定義。您可以指定 Symantec Messaging Gateway 嘗試取得病毒定義的頻率。 請參閱第 200 頁的「排程自動病毒定義更新」。
視需要停用自動更新。	您可以停用自動更新。停用自動更新之後，您必須執行隨選更新才能取得新的病毒定義。 請參閱第 200 頁的「停用自動病毒定義更新」。
需要立即取得最新的定義時，執行隨選定義更新。	您可以隨時起始 LiveUpdate，即使您已排程自動更新。 請參閱第 201 頁的「視需要起始病毒定義更新」。
指定要從中取得定義更新的來源位置。	您可以指定要從以下哪個來源取得病毒定義： ■ 賽門鐵克網站 ■ LAN 主機 請參閱第 201 頁的「指定要從哪個來源取得病毒定義」。

關於更新病毒定義

Symantec Messaging Gateway 會根據最新資訊來偵測病毒和威脅。發生問題的最常見原因之一是病毒定義並非最新的。賽門鐵克會定期提供更新的病毒定義，其中含有關於所有新發現之病毒和威脅的必要資訊。定期更新該資訊可以獲得最完整的安全保護，並保護組織中的電腦免於受到感染，以及因疫情而造成停機。

Symantec Messaging Gateway 每 10 分鐘會輪詢一次賽門鐵克伺服器，查看是否有更新可用。如有，即會在**「狀態」**頁面上顯示該資訊。但是，系統只會根據您指定的排程下載更新。或者，您也可以手動下載定義檔更新。

表 9-11 列出從賽門鐵克取得更新之病毒定義的方法。

表 9-11 從賽門鐵克取得更新之病毒定義的方法

方法	說明
LiveUpdate	您可以使用 LiveUpdate 自動更新防護。當 LiveUpdate 執行時，它會下載並安裝可用的定義檔。 您可以將 LiveUpdate 設定為定期執行，或在需要時手動執行。預設會啟用 LiveUpdate，它會在週一到週五之間每隔 10 分鐘更新定義檔。 請參閱第 200 頁的「排程自動病毒定義更新」。 請參閱第 201 頁的「視需要起始病毒定義更新」。
快速回應	LiveUpdate 快速回應更新現已過時，而且不再受到支援。現在會以更頻繁的排程自動更新。

您可以選取要從哪個來源取得病毒定義。如果您的組織有多個硬體裝置，您可以從內部伺服器取得定義檔。 接著，您可以將定義散發給所有 Symantec Messaging Gateway 硬體裝置。這種架構可讓您限制存取 Symantec LiveUpdate 的 Internet 流量。在此情景中，您必須視需要指定 LAN 主機和代理伺服器的資訊。

請參閱第 201 頁的「指定要從哪個來源取得病毒定義」。

您必須具有有效的內容授權，才能安裝定義檔。內容授權是由賽門鐵克公司授予給您，可用來將賽門鐵克公司的軟體更新為最新的相關內容 (如新的定義檔)。當您沒有內容授權或授權到期時，產品就不會接收到最新的定義檔。您的環境將容易遭受攻擊。

請參閱第 614 頁的「授權您的產品」。

檢視病毒定義的狀態

Symantec Messaging Gateway 提供病毒定義狀態的詳細資料。

LiveUpdate 狀態提供下列詳細資料：

上次 LiveUpdate 嘗試	Symantec Messaging Gateway 上次嘗試病毒定義更新的星期幾、日期和時間。
上次病毒定義 LiveUpdate 狀態	上次嘗試的病毒定義更新是否成功。
病毒定義版本 (修訂)	目前病毒定義的版本。
目前病毒定義名單	包含在此更新中的病毒定義清單。

檢視病毒定義的狀態

- 在控管中心內，按下**「惡意軟體」>「電子郵件掃描設定」> LiveUpdate**。

  LiveUpdate 狀態會出現在**「LiveUpdate 設定」**標籤下。

排程自動病毒定義更新

排程自動病毒定義更新之後，可確保您能從賽門鐵克取得可用的最新病毒定義。您可以指定 Symantec Messaging Gateway 嘗試取得病毒定義的頻率。

您只能透過 LiveUpdate 來排程自動更新。

請參閱第 201 頁的「指定要從哪個來源取得病毒定義」。

請參閱第 200 頁的「停用自動病毒定義更新」。

排程自動病毒定義檔更新

1. 在控管中心內，按下**「惡意軟體」>「電子郵件掃描設定」> LiveUpdate**。
2. 在**「LiveUpdate 排程」**下，按下**「根據下列排程啟用自動更新」**。
3. 勾選適當的方塊，以指定一週某幾天的哪個時間啟動 LiveUpdate。(建議：將每個方塊保持為已勾選。)
4. 使用**「第一次嘗試」**控制項，以指定希望 LiveUpdate 初次嘗試開始的時間。
5. 選擇**「頻率」**設定，以指定 LiveUpdate 在初次執行之後的執行頻率。

   預設值為每 10 分鐘一次。
6. 選擇 LiveUpdate 病毒定義檔的來源：
   - 如果您選擇**「從賽門鐵克網站下載經認證的病毒定義檔」**，Symantec Messaging Gateway 將直接從 Internet 下載病毒定義檔。此為預設設定。
   - 如果您的組織已經在您的網路上安裝 LiveUpdate Administrator 伺服器，您可以選擇**「從 LAN 主機下載病毒定義」**。

     如果 LiveUpdate Administrator 需要驗證，請輸入 Symantec Messaging Gateway 必須提供的**「LAN 主機位址」**、**「使用者名稱」**和**「密碼」**。

     如果您也希望使用代理伺服器來與 LiveUpdate Administrator 進行通訊，請勾選**「使用代理伺服器」**，然後輸入與代理伺服器通訊所需的**「代理伺服器主機」**和**「代理伺服器通訊埠」**資訊。如果代理伺服器需要驗證，請輸入 Symantec Messaging Gateway 必須提供的**「使用者名稱」**和**「密碼」**。
7. 您可以輸入 3 分鐘到 60 分鐘之間的值。預設值為 20 分鐘。
8. 按下**「儲存」**。

停用自動病毒定義更新

您可以停用自動更新。停用自動更新之後，您必須執行隨選更新才能取得新的病毒定義。

警告：停用自動更新之後，您的環境比較容易遭受病毒和惡意程式攻擊。自動病毒定義更新可確保您的網路隨時都能有最新的防護，可以防禦各種威脅。

停用自動病毒定義更新

1 在控管中心內，按下「**惡意軟體**」>「**電子郵件掃描設定**」> **LiveUpdate**。

2 按下「**停用自動更新**」。

3 按下「**儲存**」。

視需要起始病毒定義更新

您可以隨時起始 LiveUpdate，即使您已排程自動更新。

視需要起始病毒定義更新

1 按下「**惡意軟體**」>「**電子郵件掃描設定**」> **LiveUpdate**。

2 按下「**立即 LiveUpdate**」。

請參閱第 199 頁的「檢視病毒定義的狀態」。

請參閱第 201 頁的「指定要從哪個來源取得病毒定義」。

指定要從哪個來源取得病毒定義

您可以指定要從以下哪個來源取得病毒定義：

賽門鐵克網站	直接從 Symantec LiveUpdate 伺服器下載病毒定義。 此選項為預設設定。
LAN 主機	如果您的組織有多個硬體裝置，您可以從內部伺服器取得定義檔。接著，您可以將定義散發給所有 Symantec Messaging Gateway 硬體裝置。這種架構可讓您限制存取 Symantec LiveUpdate 的 Internet 流量。在此情景中，您必須視需要指定 LAN 主機和代理伺服器的資訊。

請參閱第 200 頁的「排程自動病毒定義更新」。

請參閱第 201 頁的「視需要起始病毒定義更新」。

從 Symantec LiveUpdate 伺服器取得病毒定義更新

1 在控管中心內，按下「**惡意軟體**」>「**電子郵件掃描設定**」> **LiveUpdate**。

2 在「**來源**」下，選取「**從賽門鐵克網站下載經認證的病毒定義**」。

LiveUpdate 會使用您在「**管理**」>「**主機**」>「**組態**」>「**編輯**」頁面之「**代理伺服器**」標籤定義的代理伺服器。

3 按下「**儲存**」。

從 LAN 主機取得病毒定義更新

1. 在控管中心內，按下**「惡意軟體」>「電子郵件掃描設定」> LiveUpdate**。
2. 在**「來源」**之下，按下**「從 LAN 主機下載病毒定義」**。

   如果從 LAN 主機下載病毒定義，LiveUpdate 會使用代理伺服器 (若您已在**「使用代理伺服器」**下指定代理伺服器)。

   若需設定 LAN 主機的相關資訊，請參閱「LiveUpdate 管理指南」。
3. 在**「位址」**欄位中，鍵入 LAN 主機的位址。

   請使用 URL，不要使用主機名稱。
4. 在**「使用者名稱」**欄位和**「密碼」**欄位中，鍵入使用者名稱和密碼 (如果需要使用者名稱和密碼才能存取該 LAN 主機)。
5. 如果使用代理伺服器，請勾選**「使用代理伺服器」**。
6. 在**「代理伺服器主機」**主機欄位中，鍵入有效的主機名稱。
7. 在**「代理伺服器通訊埠」**欄位中，鍵入有效的通訊埠號。
8. 在**「使用者名稱」**欄位和**「密碼」**欄位中，鍵入使用者名稱和密碼 (如果需要使用者名稱和密碼才能存取該代理伺服器主機)。
9. 按下**「儲存」**。

修改人工智慧敏感程度

依據預設，Messaging Gateway 會攔截使用靜態和動態人工智慧，以及病毒定義檔的惡意內容。敏感程度決定了系統使用人工智慧偵測惡意軟體和掃描不存在任何已知定義檔的威脅的方式。除了掃描已知威脅 (靜態) 之外，Messaging Gateway 還會使用人工智慧技術來掃描異常行為 (動態)，從而找到可能受感染的郵件內文與附件。

人工智慧掃描需要您在惡意軟體偵測率和誤報之間做出取捨。較低的人工智慧敏感程度可能會遺漏掉更多的惡意軟體，但會產生較少的誤報。較高的人工智慧敏感程度可能會捕捉到更多惡意軟體，但導致出現更多的誤報偵測。對於可接受高誤報率的環境，請選擇**「高偵測敏感度」**以增加對惡意內容的攔截。若要最大限度地減少誤報，請選擇**「低偵測敏感度」**，以最低的誤報成本提供最佳的惡意內容攔截。

修改敏感程度

1. 按下**「惡意軟體」>「設定」>「電子郵件掃描設定」**。
2. 按下**「一般」**標籤。
3. 在**「Bloodhound 層級」**下，按下您要的層級。

   預設設定為「中等偵測敏感度」。
4. 按下**「儲存」**。

請參閱第 185 頁的「偵測病毒、惡意軟體與惡意威脅」。

10

隔離可疑的病毒

本章包含以下主題：

- 關於隔離可疑病毒
- 關於瀏覽可疑病毒隔離所
- 架構可疑病毒郵件設定
- 處理可疑的病毒郵件

關於隔離可疑病毒

當 Symantec Messaging Gateway 掃描到含有可疑附件的郵件時，會將該郵件放入可疑病毒隔離所。

若要使用可疑病毒隔離所，您的惡意軟體政策必須對可疑附件使用下列其中一個動作：

- 將郵件保留在可疑病毒隔離所
- 刪除和延遲可疑病毒隔離所中的郵件

在發生下列其中一種狀況之前，郵件會一直保留在可疑病毒隔離所中：

郵件保留在隔離所中已達一段特定時間。	您可以指定將含有可疑附件的郵件保留在隔離所中的時間長度。預設值為 6 小時。 將郵件保留在隔離所中，可讓賽門鐵克有時間發布更新的病毒定義，藉此重新掃描郵件。當使用更新的定義重新掃描郵件時，郵件將會接收安全還是受感染的判斷。 **附註：**注意：如果您修改了預設值，請確保給予 Symantec Messaging Gateway 足夠時間來下載最新的防毒定義。 請參閱第 207 頁的「指定可疑病毒郵件保留在隔離所的時間」。

您可以從可疑病毒隔離所手動釋放或刪除郵件。	請參閱第 209 頁的「刪除隔離所中的可疑病毒郵件」。 請參閱第 210 頁的「從隔離所釋放可疑病毒郵件」。
已超出可疑病毒隔離所的大小上限。	如果隔離所超出大小上限，將會自動刪除隔離所中的郵件，以釋放空間來容納新郵件。 您可以指定上限限制。 請參閱第 207 頁的「修改為可疑病毒隔離所分配的磁碟空間」。
已評估現有政策，並已藉此採取動作。	Symantec Messaging Gateway 會評估您的政策，然後執行您針對含有可疑附件之郵件所指定的動作。 請參閱第 184 頁的「對付可疑附件所採取的動作」。

關於瀏覽可疑病毒隔離所

下列瀏覽圖示可協助您瀏覽「可疑病毒郵件隔離所」頁面上的郵件：

移至郵件開頭。

瀏覽至最後一頁郵件，如果總共超過 50 頁，則會瀏覽至 50 頁後。

移至上一頁郵件。

移至下一頁郵件。

最多可選擇目前郵件頁面之前或之後的 500 頁。

當您瀏覽至不同郵件頁面時，並不會保留原始頁面中的核取方塊狀態。例如，假設您在第一頁上選取三封郵件，然後移到下一頁。當您返回第一頁時，會清除所有郵件的核取方塊。

請參閱第 209 頁的「檢視隔離所中可疑的病毒郵件」。

請參閱第 206 頁的「指定每頁顯示的可疑病毒郵件數目」。

請參閱第 209 頁的「排序隔離所中的可疑病毒郵件」。

請參閱第 210 頁的「搜尋隔離的病毒郵件」。

架構可疑病毒郵件設定

表 10-1說明您可架構可疑病毒郵件設定的所有方式。您可以視需要以任何順序執行這些工作。

表 10-1 病毒郵件設定

工作	說明
必要時選擇語言編碼。	在大多數情況下，「自動偵測」設定可以正確地判斷「可疑病毒隔離所」中之郵件的語言編碼。不過，對於某些郵件，控管中心可能無法判斷其正確語言編碼。如果郵件呈現亂碼，請選取最可能符合該郵件所使用的語言編碼。 請參閱第 206 頁的「選擇可疑病毒郵件的語言編碼」。
自訂隔離所檢視。	您可以指定每頁要顯示的已隔離郵件項目數。 請參閱第 206 頁的「指定每頁顯示的可疑病毒郵件數目」。
排程 Symantec Messaging Gateway 應自動釋放「可疑病毒隔離所」中之郵件的時間。	您可以選擇郵件保留在「可疑病毒隔離所」中的最長時間。郵件會在您指定的期間之後自動從「可疑病毒隔離所」中釋放，並以更新的病毒定義重新掃描。 請參閱第 207 頁的「指定可疑病毒郵件保留在隔離所的時間」。
若要最佳化您的系統資源，可以指定隔離所使用的最大磁碟空間。	您可以指定「可疑病毒隔離所」使用的磁碟空間容量。 請參閱第 207 頁的「修改為可疑病毒隔離所分配的磁碟空間」。

選擇可疑病毒郵件的語言編碼

在大多數情況下，「自動偵測」設定可以正確地判斷「可疑病毒隔離所」中之郵件的語言編碼。不過，對於某些郵件，控管中心可能無法判斷其正確語言編碼。如果郵件呈現亂碼，請選取最可能符合該郵件所使用的語言編碼。

請參閱第 209 頁的「檢視隔離所中可疑的病毒郵件」。

請參閱第 205 頁的「關於瀏覽可疑病毒隔離所」。

只有具有「完整管理」權限或「管理隔離所」之修改權限的管理員可以選擇隔離所中之郵件的語言編碼。

選擇可疑病毒郵件的語言編碼

1. 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。
2. 按下您要檢視之郵件的主旨行。
3. 在「郵件詳細資料」頁面上，從下拉式清單中選取語言編碼。

指定每頁顯示的可疑病毒郵件數目

您可以指定每頁要顯示的已隔離郵件項目數。

您必須具備「完整的管理權限」或管理隔離所檢視或修改權限，才能檢視「可疑病毒隔離所」中的郵件。

指定每頁顯示的可疑病毒郵件數目

1 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。

2 按下**「每一頁的項目數」**下拉式清單，然後選取數字。

請參閱第 209 頁的「檢視隔離所中可疑的病毒郵件」。

請參閱第 205 頁的「關於瀏覽可疑病毒隔離所」。

請參閱第 209 頁的「排序隔離所中的可疑病毒郵件」。

請參閱第 210 頁的「搜尋隔離的病毒郵件」。

指定可疑病毒郵件保留在隔離所的時間

您可以選擇郵件保留在「可疑病毒隔離所」中的最長時間，最久保留 24 小時。郵件會在您指定的期間之後自動從「可疑病毒隔離所」中釋放，並以更新的病毒定義重新掃描。

您可以從**「狀態」>「已排程工作」**頁面中，檢查已排程工作的狀態。

請參閱第 556 頁的「關於已排程工作」。

請參閱第 207 頁的「修改為可疑病毒隔離所分配的磁碟空間」。

您也可以手動從「可疑病毒隔離所」中刪除郵件。

請參閱第 209 頁的「刪除隔離所中的可疑病毒郵件」。

您必須有「完整的管理」權限或「修改」權限，才能變更「可疑病毒隔離所」設定。

指定可疑病毒郵件保留在隔離所的時間

1 在控管中心內，按下**「惡意軟體」>「設定」>「可疑病毒設定」**。

2 在**「郵件釋放」**下，按下**「自動釋放超過下列時間的郵件」**下拉式清單，然後選取要將郵件保留在隔離所的時數。

預設為 6 個小時。設定上限為 24 小時。

3 按下**「儲存」**。

修改為可疑病毒隔離所分配的磁碟空間

您可以指定「可疑病毒隔離所」使用的磁碟空間容量。預設磁碟空間為 10 GB。

只有具備完整的管理權限或管理設定修改權限的管理員，才能修改「可疑病毒隔離所」設定。

修改為可疑病毒隔離所分配的磁碟空間

1 按下**「惡意軟體」>「設定」>「可疑病毒設定」**。

2 勾選**「可疑病毒隔離所大小上限」**以啟用臨界值。

3 指定要為「可疑病毒隔離所」分配的磁碟空間。

預設值為 10 GB。

4 按下**「儲存」**。

請參閱第 207 頁的「指定可疑病毒郵件保留在隔離所的時間」。

請參閱第 209 頁的「刪除隔離所中的可疑病毒郵件」。

請參閱第 210 頁的「從隔離所釋放可疑病毒郵件」。

處理可疑的病毒郵件

表 10-2說明您可對「可疑病毒隔離所」中的郵件採取的動作。您可以視需要以任何順序執行這些工作。

表 10-2 處理可疑的病毒郵件

工作	說明
檢視隔離所中的郵件以判斷您應採取的動作。	您必須具備「完整的管理權限」或管理隔離所檢視或修改權限，才能檢視「可疑病毒隔離所」中的郵件。 請參閱第 209 頁的「檢視隔離所中可疑的病毒郵件」。
對隔離所中的郵件進行排序。	您可以依日期排序「可疑病毒隔離所」中的郵件，更輕鬆地將郵件分類或尋找特定郵件。預設會以日期順序 (遞減順序) 顯示郵件。最新的郵件會顯示在頁面的最上方。 請參閱第 209 頁的「排序隔離所中的可疑病毒郵件」。
搜尋特定郵件。	搜尋郵件的能力可讓您更輕鬆地找到您要檢視、刪除或是釋放的特定郵件。 請參閱第 210 頁的「搜尋隔離的病毒郵件」。 請參閱第 211 頁的「可疑病毒郵件搜尋標準和提示」。
完全從隔離所中刪除郵件。	您可以一次刪除「可疑病毒隔離所」中的一封郵件，或一次刪除數封郵件。刪除郵件之後，就無法再存取該郵件。 請參閱第 209 頁的「刪除隔離所中的可疑病毒郵件」。
將隔離所中的郵件釋放給目標收件者。	您可以將郵件從「可疑病毒隔離所」釋放，以便使用最新的病毒定義進行重新掃描。如果 Symantec Messaging Gateway 無法修復病毒，而您的政策是隔離可疑病毒，則 Symantec Messaging Gateway 會將郵件傳回隔離所。 您可以一次釋放一封郵件，也可以一次釋放所有郵件。您還可以設定自動釋放以及重新掃描可疑病毒郵件。 請參閱第 210 頁的「從隔離所釋放可疑病毒郵件」。 請參閱第 207 頁的「指定可疑病毒郵件保留在隔離所的時間」。

檢視隔離所中可疑的病毒郵件

您必須具備「完整的管理權限」或管理隔離所檢視或修改權限，才能檢視「可疑病毒隔離所」中的郵件。

檢視隔離所中可疑的病毒郵件

- 執行下列其中一個步驟：

如果您不在「可疑病毒郵件隔離所」頁面上	在控管中心內，按下**「病毒」>「隔離所」>「電子郵件可疑病毒」**。
如果您是在「可疑病毒郵件隔離所」頁面上，並想要查看新抵達的郵件	在**「病毒」>「隔離所」>「電子郵件可疑病毒」**頁面上，如果看不見**「全部顯示」**圖示，請按下**「顯示過濾器」**，然後按下**「全部顯示」**。

排序隔離所中的可疑病毒郵件

您可以依日期排序「可疑病毒隔離所」中的郵件，更輕鬆地將郵件分類或尋找特定郵件。預設會以日期順序 (遞減順序) 顯示郵件。最新的郵件會顯示在頁面的最上方。

您必須具備「完整的管理權限」或管理隔離所檢視或修改權限，才能檢視「可疑病毒隔離所」中的郵件。

排序隔離所中的可疑病毒郵件

1. 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。
2. 按下**「日期」**欄位標題，依照遞增或遞減順序排序。

請參閱第 209 頁的「檢視隔離所中可疑的病毒郵件」。

請參閱第 206 頁的「指定每頁顯示的可疑病毒郵件數目」。

請參閱第 205 頁的「關於瀏覽可疑病毒隔離所」。

請參閱第 210 頁的「搜尋隔離的病毒郵件」。

刪除隔離所中的可疑病毒郵件

您可以一次刪除「可疑病毒隔離所」中的一封郵件，或一次刪除數封郵件。刪除郵件之後，就無法再存取該郵件。只有具有「完整的管理」權限或「管理隔離所」之修改權限的管理員可以刪除隔離所中的郵件。

請參閱第 209 頁的「檢視隔離所中可疑的病毒郵件」。

您也可以使用清除公用程式來自動刪除「可疑病毒隔離所」中的郵件。這個公用程式讓您不需要手動刪除隔離所中的郵件，即可釋放空間。這個公用程式會根據您指定的排程清除郵件。

請參閱第 207 頁的「指定可疑病毒郵件保留在隔離所的時間」。

刪除隔離所中的個別郵件

1 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。

2 按下要刪除的每個郵件旁之核取方塊。

3 按下**「刪除」**。

刪除隔離所中的所有郵件

1 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。

2 按下**「全部刪除」**以刪除可疑病毒隔離所中的所有郵件，包括其他頁面中的郵件。

從隔離所釋放可疑病毒郵件

您可以將郵件從「可疑病毒隔離所」釋放，以便使用最新的病毒定義進行重新掃描。如果 Symantec Messaging Gateway 無法修復病毒，而且您的政策將隔離可疑病毒，則會將郵件傳回可疑病毒隔離所。

您可以一次釋放一封郵件，也可以一次釋放所有郵件。您還可以設定自動釋放以及重新掃描可疑病毒郵件。

請參閱第 207 頁的「指定可疑病毒郵件保留在隔離所的時間」。

若要釋放郵件，必須存取控管中心的 IP 位址。如果您有限制入埠或離埠 SMTP 存取權，請勾選「入埠郵件設定值及離埠郵件設定值」。

只有具有「完整的管理」權限或「管理隔離所」之修改權限的管理員可以從隔離所釋放郵件。

請參閱第 209 頁的「刪除隔離所中的可疑病毒郵件」。

請參閱第 39 頁的「關於掃描程式電子郵件設定」。

從隔離所釋放個別郵件

1 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。

2 勾選您要釋放之郵件旁的方塊。

3 按下**「釋放」**。

從隔離所釋放所有郵件

1 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。

2 按下**「全部釋放」**可釋放可疑病毒隔離所中的所有郵件，包括其他頁面中的郵件。

搜尋隔離的病毒郵件

您可以搜尋「可疑病毒隔離所」中的郵件。搜尋郵件的能力可讓您更輕鬆地找到您要檢視、刪除或是釋放的特定郵件。您必須具備「完整的管理權限」或管理隔離所檢視或修改權限，才能檢視「可疑病毒隔離所」中的郵件。

搜尋隔離的病毒郵件

1 在控管中心內，按下**「惡意軟體」>「隔離所」>「電子郵件可疑病毒」**。

2 在郵件清單頁面上，按下**「顯示過濾器」**。

3 執行下列任一項操作以進行搜尋：

搜尋郵件信封 To 收件者	在**「收件者」**方塊中輸入名稱或地址，搜尋郵件信封 `RCPT TO:` 標頭。 您可以搜尋顯示名稱、電子郵件地址的使用者名稱部分，或顯示名稱或電子郵件使用者名稱的任一部分。若在「收件者」方塊中輸入完整的電子郵件地址，則 Symantec Messaging Gateway 僅會搜尋 `user_name@example.com` 的使用者名稱部分。該搜尋會限制在信封 `To:` 中，其中所含資訊可能與郵件詳細資料頁面中所顯示標頭 `To:` 的資訊不同。
搜尋 From 標頭	在**「寄件者」**方塊中輸入名稱或地址，在所有郵件的 `From:` 標頭中搜尋特定寄件者。 您可以搜尋顯示名稱、電子郵件地址，或顯示名稱或電子郵件地址的任一部分。該搜尋會限制在顯示的郵件 `From:` 標頭中，在垃圾郵件中該部分通常是偽造的。顯示的郵件 `From:` 標頭可能含有郵件信封以外的其他資訊。
搜尋主旨標頭	在**「主旨」**方塊中輸入內容，以便在所有郵件的 `Subject:` 標頭中搜尋有關特定主題的郵件。
搜尋時間範圍	按下**「時間範圍」**下拉式清單，以顯示在您指定的時間範圍期間收到的所有郵件。

4 按下**「顯示已過濾」**。

請參閱第 209 頁的「檢視隔離所中可疑的病毒郵件」。

請參閱第 206 頁的「指定每頁顯示的可疑病毒郵件數目」。

請參閱第 205 頁的「關於瀏覽可疑病毒隔離所」。

請參閱第 209 頁的「排序隔離所中的可疑病毒郵件」。

可疑病毒郵件搜尋標準和提示

搜尋功能已經最佳化，以便搜尋數量龐大的郵件。不過，仍可能產生無法預期的搜尋結果。

請考慮下列秘訣和資訊，以協助您在「可疑病毒隔離所」中進行搜尋：

字符	字符會以子字串語義比對。以搜尋目標 <in> 搜尋主旨時，將找出「Lowest rate in 45 years」、「RE: re:Sublime Bulletin (verification)」、「Up to 85% off Ink Cartridges + no shipping!」以及「Re-finance at todays super low rate」。
多字詞搜尋	如果在多字詞搜尋中找到郵件內含有其中任何字，該郵件會視為符合。例如，搜尋 red carpet 時，會找到 red carpet、red wine 與 flying carpet。
區分大小寫	所有文字搜尋都是不分字母大小寫的。例如，假設您在 From 方塊中輸入 emerson。From 標頭中含有 emerson、Emerson 和 eMERSOn 的所有郵件都會出現在搜尋結果中。
完全相同的詞組	若要搜尋完全相同的詞，請在詞的前後加上雙引號 (" ")。
萬用字元	您可以使用 * (星號) 執行萬用字元搜尋。這個字元亦作為邏輯「和」字元使用。此外，您可以使用特殊字元進行搜尋，例如 &、! (驚嘆號)、$ (美元符號)，以及 # (井字號)。
單一字元	即使是單一字元也會視為子字串目標。
特殊字元	您可以使用特殊字元進行搜尋，例如 & (連線符號)、! (驚嘆號)、$ (美元符號)，以及 # (井字號)。
多重特性	如果您搜尋多重特性，則搜尋結果僅會列出同時符合所有特性的郵件。例如，假設您在 From 方塊中輸入 LPQTech，並在「主旨」方塊中輸入 Inkjet。只有在 `From:` 標頭中含有 LPQTech 且在 `Subject:` 標頭中含有 Inkjet 的郵件，才會出現在搜尋結果中。
偽造的標頭資訊	垃圾郵件寄發者通常會「欺騙」或偽造某些顯示的郵件標頭 (例如「寄件者」和「收件者」及看不見的信封資訊)。有時候他們會以實際的電子郵件地址或非相關人士或公司的網域偽造標頭資訊。
執行搜尋的時間	執行搜尋所需的時間，須視您使用的搜尋方塊數量與信箱中的郵件數量而定。在管理員信箱中搜尋會比在使用者信箱中搜尋花更長的時間。

請參閱第 210 頁的「搜尋隔離的病毒郵件」。

11

過濾垃圾郵件

本章包含以下主題：

- 關於過濾垃圾郵件及不必要的郵件
- 架構垃圾郵件及不必要的電子郵件偵測
- 掃描以文字為基礎的附件
- 建立偵測垃圾郵件及不必要的電子郵件的政策
- 減少不必要的電子郵件過濾的誤報
- 啟用和停用垃圾郵件及不必要的電子郵件政策
- 修改垃圾郵件及不必要的電子郵件政策
- 複製垃圾郵件政策
- 刪除垃圾郵件政策
- 架構可疑垃圾郵件識別的臨界值
- 啟用或停用向賽門鐵克提報 URI
- 啟用或停用 URL 信譽過濾
- 關於針對客戶特定垃圾郵件規則提交郵件

關於過濾垃圾郵件及不必要的郵件

Symantec Messaging Gateway 提供一組預設的垃圾郵件及不必要的電子郵件政策。若為全新安裝，不會將不必要的電子郵件政策指定給任何群組。如果是從舊版進行升級，會停用不必要的電子郵件政策，且不會將其指定給任何群組。您可以修改這些政策中的動作，也可以建立自己的政策。

請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。

您可以修改垃圾郵件、可疑垃圾郵件、行銷電子郵件、電子報和重新導向 URL 的政策設定。

表 11-1 說明不必要的電子郵件類別。

表 11-1 不必要的電子郵件類別

不必要的電子郵件類別	說明
行銷郵件	內含商業性或籌款訊息的電子郵件，使用者可能已要求接收。這些郵件通常不提供選擇退出功能。
電子報	已知定期 (通常每週或每月) 寄送，內含特定主題內容的電子郵件。使用者可能已要求接收這些出版品。通常會提供選擇退出功能。
重新導向 URL	重新導向 URL 包括免費的托管網站、URL 縮短服務以及 URL 重新導向服務，這些可能會遭到不當使用以傳送垃圾郵件或惡意軟體酬載。Symantec Messaging Gateway 可以過濾內含一或多個重新導向 URL 的電子郵件。

Symantec Messaging Gateway 支援與下列不必要的電子郵件判斷相關的誤報及漏報提交：

- 行銷郵件
- 電子報
- 重新導向 URL

您可以指定處理垃圾郵件、可疑垃圾郵件或不必要的電子郵件的方式。例如，您可以將可疑垃圾郵件傳送至「垃圾郵件隔離所」。您也可以在主旨行前面添加指定的文字，讓使用者知道郵件是可疑垃圾郵件。

附註：過濾不必要的電子郵件會一併過濾合法郵件。賽門鐵克建議由郵件主旨行標記或隔離等動作開始著手。

請參閱第 239 頁的「關於隔離垃圾郵件」。

請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。

請參閱第 224 頁的「架構可疑垃圾郵件識別的臨界值」。

預設垃圾郵件及不必要的電子郵件政策

Symantec Messaging Gateway 安裝時會一併安裝一組預設的垃圾郵件及不必要的電子郵件政策。預設的垃圾郵件政策會自動啟用並指定給預設政策群組。若為全新安裝，不會將不必要的電子郵件政策指定給任何群組。如果是從舊版進行升級，會停用不必要的電子郵件政策，且不會將其指定給任何群組。

如果您建立自訂垃圾郵件或不必要的電子郵件政策，並將其套用至預設政策群組，則該政策會覆寫預設政策。

表 11-2 預先架構的垃圾郵件政策

政策名稱	套用至下列郵件	如果符合下列條件	動作	套用至下列政策群組	預設狀態
垃圾郵件：使用「[垃圾郵件]」修改郵件主旨行 (預設)	入埠和離埠	如果郵件是垃圾郵件	在主旨行前面加上「[垃圾郵件]」	預設群組	已啟用
可疑垃圾郵件: 使用「[可疑垃圾郵件]」修改郵件主旨行(預設)	入埠和離埠	如果郵件是可疑垃圾郵件	在主旨行前面加上「[可疑垃圾郵件]」	預設群組	已啟用
垃圾郵件或可疑垃圾郵件: 刪除郵件	入埠和離埠	如果郵件是垃圾郵件或可疑垃圾郵件	刪除郵件	無	已啟用
垃圾郵件或可疑垃圾郵件: 隔離郵件	入埠和離埠	如果郵件是垃圾郵件或可疑垃圾郵件	將郵件保留在垃圾郵件隔離所	無	已啟用
垃圾郵件或可疑垃圾郵件：正常傳送	入埠和離埠	如果郵件是垃圾郵件或可疑垃圾郵件	正常傳送郵件	無	已啟用
垃圾郵件或可疑垃圾郵件：新增 X 標頭 此政策可供已移轉至 9.5 版的版本使用。 在 9.5 版或更新版本的全新安裝中，不提供此政策作為預先架構的政策。	入埠和離埠	如果郵件是垃圾郵件或可疑垃圾郵件	在垃圾郵件中新增 X 標頭	無	已啟用
客戶特定垃圾郵件：使用「[客戶特定垃圾郵件]」修改郵件主旨行	入埠	如果郵件是客戶特定垃圾郵件	在主旨行前面加上「[客戶特定垃圾郵件]」	無	已停用 您必須啟用客戶特定垃圾郵件提交功能，才能啟用或修改此政策。
客戶特定垃圾郵件：刪除郵件	入埠	如果郵件是客戶特定垃圾郵件	刪除郵件	無	已停用 您必須啟用客戶特定垃圾郵件提交功能，才能啟用或修改此政策。

政策名稱	套用至下列郵件	如果符合下列條件	動作	套用至下列政策群組	預設狀態
客戶特定垃圾郵件：隔離郵件	入埠	如果郵件是客戶特定垃圾郵件	隔離郵件	無	已停用 您必須啟用客戶特定垃圾郵件提交功能，才能啟用或修改此政策。
客戶特定垃圾郵件：正常傳送	入埠	如果郵件是客戶特定垃圾郵件	正常傳送郵件	無	已停用 您必須啟用客戶特定垃圾郵件提交功能，才能啟用或修改此政策。
無法通過退回攻擊驗證：拒絕郵件(預設)	僅入埠	如果郵件無法通過退回攻擊驗證	拒絕未通過退回攻擊驗證的郵件	預設群組	已啟用
行銷郵件: 使用 [Marketing Mail] 修改郵件主旨行	僅入埠	如果郵件是行銷電子郵件	在郵件主旨行前面加上 [Marketing Mail]	無	已啟用
電子報: 使用 [Newsletter] 修改郵件主旨行	僅入埠	如果郵件是電子報	在郵件主旨行前面加上 [Newsletter]	無	已啟用
重新導向 URL 內容: 使用 [Caution: Message contains Redirect URL content] 修改郵件主旨行	僅入埠	如果郵件包含重新導向 URL 內容	在郵件主旨行前面加上 [Caution: Message contains Redirect URL content]	無	已啟用

架構垃圾郵件及不必要的電子郵件偵測

表 11-3 說明您可以執行哪些工作，以偵測垃圾郵件及不必要的電子郵件並加強偵測能力。

表 11-3 架構垃圾郵件及不必要的電子郵件偵測

工作	說明
建立並啟用垃圾郵件及不必要的電子郵件政策。	Symantec Messaging Gateway 安裝時會一併安裝一組預設的垃圾郵件及不必要的電子郵件政策。 對於新安裝或升級，預設的垃圾郵件政策會自動啟用並指定給預設政策群組。 對於新安裝，會啟用預先架構之不必要的電子郵件政策，但不會將其指定給任何群組。如果是從舊版進行升級，會停用預先架構之不必要的電子郵件政策，且不會將其指定給任何群組。您可以修改這些政策或建立自訂的政策。 請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。 請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。 請參閱第 222 頁的「修改垃圾郵件及不必要的電子郵件政策」。 請參閱第 216 頁的「架構垃圾郵件及不必要的電子郵件偵測」。
設定可疑垃圾郵件層級。	Symantec Messaging Gateway 在評估郵件是否為垃圾郵件時，會計算每封郵件的垃圾郵件分數 (1 到 100)。這個分數是根據多種防垃圾郵件技術計算出的結果。 您可以定義介於 25 到 89 之間的分數，將這個分數範圍內的郵件視為「可疑垃圾郵件」。透過政策，您可以針對識別為可疑垃圾郵件的郵件與識別為垃圾郵件的郵件指定不同的動作。 賽門鐵克建議，除非您對網站的過濾樣式有所瞭解，否則請不要調整垃圾郵件臨界值。每週逐漸將臨界值設定往下調整 1 至 5 分，直到誤報次數減少到可接受的程度為止。 請參閱第 224 頁的「架構可疑垃圾郵件識別的臨界值」。
啟用能將資訊提供給賽門鐵克的功能，協助我們建立更好的垃圾郵件過濾器。	啟用下列功能可以協助賽門鐵克建立更好的垃圾郵件過濾器： ■ 統一資源識別元 (URI) 報告 啟用 URI 報告時，Symantec Messaging Gateway 會將報告傳送至賽門鐵克安全機制應變中心。 報告所包含的 URI 會出現在 Symantec Messaging Gateway 掃描垃圾郵件的訊息中。賽門鐵克會使用此資訊來開發全新、以 URI 為基礎的過濾器。 請參閱第 225 頁的「啟用或停用向賽門鐵克提報 URI」。 ■ 探查帳戶 您可以將未使用或無效的電子郵件地址轉寄至 Symantec Probe Network。賽門鐵克會利用這些電子郵件地址引誘垃圾郵件寄發者。接著，賽門鐵克會利用這些地址收到的垃圾郵件，建立更好的垃圾郵件過濾器。 請參閱第 272 頁的「啟用探查參與」。 請參閱第 272 頁的「從無效收件者電子郵件地址建立探查帳戶」。 請參閱第 274 頁的「啟用探查帳戶」。

工作	說明
架構垃圾郵件隔離所。	您可以將垃圾郵件、可疑垃圾郵件或不必要的電子郵件繞送至「垃圾郵件隔離所」。使用者可以存取「垃圾郵件隔離所」，來判斷是否為誤報的郵件。 如果郵件儲存在垃圾郵件隔離所中，但為合法郵件，使用者可將此類郵件釋放至他們的收件匣中。 使用者可以通知您發生誤報情況，讓您可以據此持續地調整垃圾郵件設定與垃圾郵件及不必要的電子郵件政策。您也可以將摘要通知設定為傳送至使用者的收件匣中。 請參閱第 240 頁的「使用垃圾郵件隔離所之前」。 請參閱第 242 頁的「架構一般使用者隔離所」。 請參閱第 247 頁的「指定要通知誤報郵件的對象」。 請參閱第 259 頁的「關於架構使用者與散布清單通知摘要」。 您可以架構臨界值來控制配置給「垃圾郵件隔離所」的空間。 請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。 請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。
監控報告。	監控報告可以判斷垃圾郵件政策的有效程度。報告也可以指出您組織收到的垃圾郵件數量。此資訊可以協助您微調垃圾郵件偵測設定。
以文字為基礎的附件掃描。	Symantec Messaging Gateway 可以掃描電子郵件中下列副檔名類型的附件是否為垃圾郵件： ■ .doc ■ .htm ■ .html ■ .rtf ■ .txt ■ .wps ■ .xml 根據預設，此選項會在新安裝時啟用，並且會在升級時停用。 啟用此選項可能會導致 Symantec Messaging Gateway 的效能變慢。停用此選項時，Symantec Messaging Gateway 將不會使用所有掃描技術來評估附件以尋找垃圾郵件。 請參閱第 218 頁的「掃描以文字為基礎的附件」。

請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。

掃描以文字為基礎的附件

Symantec Messaging Gateway 可以掃描電子郵件中下列副檔名類型的附件是否為垃圾郵件：

- .doc

- .htm
- .html
- .rtf
- .txt
- .wps
- .xml

掃描以文字為基礎的附件

1 在控管中心內，按下**「垃圾郵件」>「設定」>「掃描設定」**。

2 在**「以文字為基礎的附件掃描」**下，按下**「掃描以文字為基礎的附件」**。

根據預設，此選項會在新安裝時啟用，並且會在升級時停用。啟用此選項可能會導致 Symantec Messaging Gateway 的效能變慢。停用此選項時，Symantec Messaging Gateway 將不會使用所有掃描技術來評估附件以尋找垃圾郵件。

請參閱第 216 頁的「架構垃圾郵件及不必要的電子郵件偵測」。

建立偵測垃圾郵件及不必要的電子郵件的政策

您可以建立垃圾郵件政策，來決定要對特定垃圾郵件條件採取的動作。

Symantec Messaging Gateway 安裝時會一併安裝數個預先架構的政策。您可以直接使用這些政策、加以編輯以符合您的需求，或是建立您自己的自訂政策。

請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。

建立新的垃圾郵件政策後，預設會將其啟用。

建立偵測垃圾郵件及不必要的電子郵件的政策

1 在控管中心內，按下**「垃圾郵件」>「政策」>「電子郵件」**。

2 按下**「新增」**。

3 在**「垃圾郵件政策」**頁面的**「政策名稱」**方塊中，輸入垃圾郵件政策的名稱。

內容過濾、垃圾郵件與惡意軟體政策名稱必須是唯一的。例如，如果您有一個稱為 XYZ 的內容過濾政策，則垃圾郵件政策或惡意軟體政策就不能稱為 XYZ。

4 在**「條件」**下，按下**「套用至」**下拉式清單，然後選擇僅限入埠郵件、僅限離埠郵件或兩者的套用政策。

5 按下「**如果符合下列條件**」下拉式清單，然後選取下列其中一個選項：

如果郵件包含重新導向 URL 內容	如果郵件包含重新導向 URL 內容，則執行指定的動作。
如果郵件無法通過退回攻擊驗證	如果郵件是無法通過驗證的非傳送接收郵件，則執行指定的動作。此條件僅適用於入埠郵件。
如果郵件屬於行銷郵件	如果郵件是行銷電子郵件，則執行指定的動作。
如果郵件屬於電子報	如果郵件屬於電子報，則執行指定的動作。
如果郵件是客戶特定垃圾郵件	如果郵件根據客戶特定垃圾郵件規則被識別為垃圾郵件，則執行指定的動作。
如果郵件是垃圾郵件	如果郵件是垃圾郵件，則執行指定的動作。
如果郵件是垃圾郵件或可疑垃圾郵件	如果郵件是垃圾郵件或可疑垃圾郵件，則執行指定的動作。
如果郵件是可疑垃圾郵件	如果郵件可能是垃圾郵件，則執行指定的動作。可在「**垃圾郵件**」>「**設定**」>「**掃描設定**」頁面上調整可疑垃圾郵件等級。

6 在「**動作**」下，按下「**新增**」。

7 在「**架構動作**」頁面上，按下拉式清單，然後選取要對符合所指定垃圾郵件條件的郵件採取的動作。

某些動作需要指定其他資訊。

請參閱第 285 頁的「政策動作及其功能」。

8 在「**架構動作**」頁面上按下「**新增動作**」。

您可以視需要新增額外的動作。

9 在「**套用至下列群組**」下方，勾選應套用此政策的一或多個政策群組。

10 按下「**儲存**」。

減少不必要的電子郵件過濾的誤報

您必須微調設定，以減少誤報的事件。

表 11-4 描述了當使用者沒收到預期的電子郵件時如何微調設定。您可以視需要以任何順序執行這些工作。

表 11-4 減少誤報的方式

工作	說明
停用、啟用或重新啟用及修改過濾政策。	若要疑難排解誤報事件，請停用您認為可能造成問題的政策。您可以逐一停用再重新啟用政策，直到找出需要修改的政策。找到要修改的政策後，請編輯該政策，然後重新啟用。 請參閱第 168 頁的「編輯、刪除、啟用或停用政策群組」。
將過濾政策中指定的動作變更為較不嚴格的動作。	例如，您可以將郵件傳送到「垃圾郵件隔離所」或使用郵件主旨行標記，來取代刪除郵件動作。 請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。
變更使用過濾政策的政策群組。	另一個可能的解決方法是對使用者子集關閉過濾。 請參閱第 170 頁的「為政策群組選取垃圾郵件政策和不必要的電子郵件政策」。
將寄件者新增至「允許的第三方寄件者」群組。	如果您確定寄件者的信譽，您可以將寄件者新增到「允許的第三方寄件者」群組。此群組中寄件者的郵件會自動略過垃圾郵件過濾。 請參閱第 113 頁的「新增寄件者至管理員定義之寄件者群組和第三方寄件者群組」。
新增內容過濾政策。	政策應有條件可尋找被錯誤過濾掉的特定郵件。您可以指定**「略過垃圾郵件掃描」**動作。 請參閱第 278 頁的「建立內容過濾政策」。

啟用和停用垃圾郵件及不必要的電子郵件政策

預設會啟用新的垃圾郵件及不必要的電子郵件政策。對於新安裝或升級，預設的垃圾郵件政策會自動啟用並指定給預設政策群組。對於新安裝，會啟用預先架構之不必要的電子郵件政策，但不會將其指定給任何群組。如果是從舊版進行升級，會停用預先架構之不必要的電子郵件政策，且不會將其指定給任何群組。您可以停用不想讓 Symantec Messaging Gateway 在掃描電子郵件時使用的任何政策。

您可以停用垃圾郵件政策，以疑難排解防垃圾郵件掃描問題。例如，您可以停用不再使用但還不想刪除的政策。

不必要的電子郵件定義如下：

- 可疑垃圾郵件
- 行銷郵件
- 電子報
- 內含一或多個重新導向 URL 的電子郵件

啟用或停用垃圾郵件或不必要的電子郵件政策

1 在控管中心內，按下「**垃圾郵件**」>「**政策**」>「**電子郵件**」。

2 勾選您要啟用或停用之政策旁的方塊。

3 選取下列其中一個選項：

啟用	啟用政策時，「**已啟用**」欄會顯示綠色勾號。
停用	停用政策時，「**已啟用**」欄會顯示水平線。

請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。
請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。
請參閱第 222 頁的「修改垃圾郵件及不必要的電子郵件政策」。
請參閱第 223 頁的「複製垃圾郵件政策」。
請參閱第 223 頁的「刪除垃圾郵件政策」。

修改垃圾郵件及不必要的電子郵件政策

您可以修改垃圾郵件及不必要的電子郵件政策，以進行微調或是擴大或縮小其範圍。

表 11-5 說明您可以修改的預設垃圾郵件政策和自訂垃圾郵件政策設定。

表 11-5 可修改的垃圾郵件及不必要的電子郵件政策設定

設定值	可於預設政策修改	可於自訂政策修改
政策名稱	否	是
套用至	否	否
如果符合下列條件	否	否
執行下列動作	是	是
套用至下列政策群組	是	是

修改垃圾郵件及不必要的電子郵件政策

1 在控管中心內，按下「**垃圾郵件**」>「**政策**」>「**電子郵件**」。

2 勾選要修改之政策旁的方塊，然後按下「**編輯**」。

3 進行所需的修改。

4 按下「**儲存**」。

請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。

請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。

請參閱第 221 頁的「啟用和停用垃圾郵件及不必要的電子郵件政策」。

請參閱第 223 頁的「複製垃圾郵件政策」。

請參閱第 223 頁的「刪除垃圾郵件政策」。

複製垃圾郵件政策

有些時候您可能會建立複雜的垃圾郵件政策，而且想要據以建立只包含少數修改的類似政策。Symantec Messaging Gateway 可讓您複製垃圾郵件政策。

當您複製垃圾郵件政策時，新政策的名稱不能與任何現有政策相同。例如，如果您的內容過濾政策名為 XYZ，則垃圾郵件政策或惡意軟體政策名稱不能是 XYZ。垃圾郵件政策建立後，預設會將其啟用。

請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。

請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。

請參閱第 221 頁的「啟用和停用垃圾郵件及不必要的電子郵件政策」。

請參閱第 222 頁的「修改垃圾郵件及不必要的電子郵件政策」。

請參閱第 223 頁的「刪除垃圾郵件政策」。

複製垃圾郵件政策

1. 在控管中心內，按下**「垃圾郵件」>「政策」>「電子郵件」**。
2. 勾選您要複製之政策旁的方塊。
3. 按下**「複製」**。
4. 在**「垃圾郵件政策」**頁面上，鍵入新的政策名稱。
5. 進行您所需的任何其他變更。
6. 按下**「儲存」**。

刪除垃圾郵件政策

您可以刪除不需要的垃圾郵件政策。 但是，刪除政策之後即無法回復。 如果不確定是否要永久刪除政策，您可以改為將它停用。

請參閱第 221 頁的「啟用和停用垃圾郵件及不必要的電子郵件政策」。

請參閱第 223 頁的「複製垃圾郵件政策」。

請參閱第 222 頁的「修改垃圾郵件及不必要的電子郵件政策」。

刪除垃圾郵件政策

1 在控管中心內，按下**「垃圾郵件」>「政策」>「電子郵件」**。

2 勾選您要刪除之政策旁的方塊。

3 按下**「刪除」**。

4 按下確認對話方塊中的**「刪除」**。

架構可疑垃圾郵件識別的臨界值

Symantec Messaging Gateway 在評估郵件是否為垃圾郵件時，會計算每封郵件的垃圾郵件分數 (1 到 100)。這個分數是根據樣式比對與啟發式分析等技術來計算的。

Symantec Messaging Gateway 會將垃圾郵件分數分類如下：

90 - 100	如果電子郵件的分數介於 90 到 100 之間，則定義為垃圾郵件。賽門鐵克會決定哪些郵件是垃圾郵件。您無法調整這項判斷。
89 - 25 可疑垃圾郵件臨界值 預設為 75	您可以定義從 25 到 89 之間的分數範圍。分數介於這個範圍的郵件都視為「可疑垃圾郵件」。透過政策，您可以針對識別為可疑垃圾郵件的郵件與識別為垃圾郵件的郵件指定不同的動作。 例如，假設您架構可疑垃圾郵件的分數範圍介於 80 到 89。如果內送郵件得到的垃圾郵件分數為 83，則 Symantec Messaging Gateway 會將該郵件視為可疑垃圾郵件。它會套用針對可疑垃圾郵件所指定的動作，例如「修改郵件」(在主旨行加上標籤)。
低於可疑垃圾郵件臨界值	如果郵件的分數低於可疑垃圾郵件臨界值，則 Symantec Messaging Gateway 會將它視為非垃圾電子郵件。

賽門鐵克建議，除非您對網站的過濾樣式有所瞭解，否則請不要調整垃圾郵件臨界值。每週逐漸將臨界值設定往下調整 1 至 5 分，直到誤報次數減少到可接受的程度為止。有一種方法可測試垃圾郵件評分的效果，就是將垃圾郵件政策架構為將可疑垃圾郵件隔離在「垃圾郵件隔離所」中。然後，設定指定的信箱來接收誤報抱怨，並隨著變更垃圾郵件評分臨界值來監控其次數。

附註：賽門鐵克不會將收到可疑垃圾郵件判斷的合法郵件視為誤報，也不會檢閱收到可疑垃圾郵件判斷並提交給賽門鐵克安全機制應變中心的郵件。原因是賽門鐵克無法控制組織架構「可疑垃圾郵件」臨界值的方式。因此，賽門鐵克不會建立過濾器或根據可疑垃圾郵件判斷來修改過濾器。根據設定過低之可疑垃圾郵件臨界值而建立的過濾器，可能會影響所有賽門鐵克客戶的垃圾郵件效能。

請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。

架構可疑垃圾郵件識別的臨界值

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**掃描設定**」。

2 在「**要將郵件標示為可疑垃圾郵件?**」下方，按下「**是**」或「**否**」。

3 在「**選取介於 25 到 89 之間的可疑垃圾郵件臨界值**」下方，按下並拖曳滑動軸，以增加或減少可疑垃圾郵件的範圍下限。也可以在方塊中輸入數值。

4 按下「**儲存**」。

啟用或停用向賽門鐵克提報 URI

您可以協助賽門鐵克建立更好的垃圾郵件過濾，以依據統一資源識別元 (URI) 攔截郵件。啟用 URI 報告時，Symantec Messaging Gateway 會將報告傳送至賽門鐵克安全機制應變中心。報告所包含的 URI 會出現在 Symantec Messaging Gateway 掃描垃圾郵件的訊息中。賽門鐵克會使用此資訊來開發全新、以 URI 為基礎的過濾器。您可透過「管道」接收這些更新的過濾器。

請參閱第 64 頁的「掃描程式服務」。

URI 報告功能不會對產品效能產生顯著的影響。

啟用或停用向賽門鐵克提報 URI

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**掃描設定**」。

2 在「**統一資源識別元 (URI) 報告**」下，執行下列其中一項工作：

啟用 URI 報告	請勾選「**向賽門鐵克安全機制應變中心提報 URI**」。 新安裝預設會啟用此功能。
停用 URI 報告	取消勾選「**向賽門鐵克安全機制應變中心提報 URI**」。 此功能預設會在移轉安裝時停用。

3 按下「**儲存**」。

啟用或停用 URL 信譽過濾

當您啟用 URL 信譽過濾時，Symantec Messaging Gateway 會掃描電子郵件是否有 URL，並將 DNS 查詢傳送至賽門鐵克以執行信譽查閱。這項功能可將 URL 與大型的全球信譽資料集區比對，提升規則檢查 URL 型垃圾郵件的效果。

啟用或停用 URL 信譽過濾

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**掃描設定**」。

2 在「**啟用 URL 信譽過濾**」下，執行下列其中一項工作：

啟用 URL 信譽過濾	勾選「**啟用 URL 信譽過濾**」。 新安裝預設啟用「**URL 信譽過濾**」。 如果您已升級，且未在舊版的「**垃圾郵件**」>「**掃描設定**」頁面中停用「**統一資源識別元 (URI) 報告**」功能，預設會啟用「**URL 信譽過濾**」。
停用 URL 信譽過濾	取消勾選「**啟用 URL 信譽過濾**」。 如果您已升級，且在舊版中停用「**統一資源識別元 (URI) 報告**」，預設會停用「**啟用 URL 信譽過濾**」。

3 按下「**儲存**」。

請參閱第 225 頁的「啟用或停用向賽門鐵克提報 URI」。

關於針對客戶特定垃圾郵件規則提交郵件

您可以根據管理員與一般使用者提交的遺漏垃圾郵件及誤報郵件，取得特別針對您組織自訂的垃圾郵件規則。

此功能具有下列優點：

- 改善 Symantec Messaging Gateway 偵測垃圾郵件的能力，並協助管理員控管誤報事件。
- 更輕鬆地將遺漏的垃圾郵件或誤報郵件提交給賽門鐵克，以進行分析及建立規則集。
- 能夠看見提交狀態與規則集建立的狀況。

請參閱第 228 頁的「如何建立規則，以及為何郵件可能不會產生自訂規則」。

架構此功能後，管理員及一般使用者就可以將電子郵件當作遺漏的垃圾郵件或誤報提交給賽門鐵克。在數分鐘內，賽門鐵克便會建立自訂規則集。管道包含規則集，規則集之後會套用到每個已架構的掃描程式。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

如果您想要使用客戶特定的垃圾郵件提交功能，您必須取得提交者 ID。提交者 ID 可確保自訂規則僅供由指定控管中心管理的掃描程式使用。

請參閱第 230 頁的「佈建客戶特定垃圾郵件提交的提交者 ID」。

Symantec Messaging Gateway 可讓您指定誰能夠提交郵件以建立自訂規則。或者，您可以指定誰無法提交郵件。系統會提交受限制使用者的郵件，但不將其郵件視為自訂規則。受限制使用者的提交項目在報告中會顯示成「**已攔截**」。

請參閱第 233 頁的「指定誰能夠提交客戶特定規則的郵件」。

您可以建立垃圾郵件政策，其可根據自訂規則，在 Symantec Messaging Gateway 偵測郵件時，採取您指定的動作。例如，您可以建立垃圾郵件政策，政策的條件是**「如果郵件是客戶特定垃圾郵件」**，動作是**「建立隔離事件」**。此動作可讓您監控違反自訂規則的郵件，以監控規則的有效性並協助您疑難排解問題。

請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。

您可以在**「狀態」>「提交」>「提交詳細資料」**頁面上檢視垃圾郵件提交狀態。控管中心控制面板包含有關提交服務及您客戶特定規則的資訊。報告中也會包含垃圾郵件提交資料。

請參閱第 374 頁的「監控垃圾郵件提交」。

請參閱第 516 頁的「使用儀表板」。

請參閱第 498 頁的「報告類型」。

有實例可讓您停用此功能，並移除所有的客戶垃圾郵件提交資料。或者您可能要刪除所有現有的規則並開始新的規則。Symantec Messaging Gateway 可讓您刪除所有的客戶垃圾郵件提交資料。此資料包含提交者 ID、所有相關的規則、提交者清單中的電子郵件地址、報告資訊等等。刪除資料之後，就無法再擷取或還原該資料。

請參閱第 237 頁的「正在刪除客戶特定垃圾郵件資料」。

賽門鐵克會針對全域規則考慮所有提交為「垃圾郵件」或「不是垃圾郵件」的郵件，無論客戶特定的垃圾郵件提交規則是否為啟用。根據預設，客戶垃圾郵件提交功能為停用。啟用此功能後，所有已提交的郵件都會視為客戶特定規則產生。此外，誤報會造成規則刪除。如果您停用功能，提交的郵件仍都視為客戶特定規則產生或規則刪除。賽門鐵克會繼續建立新的規則，但不會部署新的規則。客戶特定垃圾郵件過濾政策會受到限制，以便將這些規則套用到郵件流量。如果您再次啟用此功能，則賽門鐵克所傳送的規則會從此功能初始停用時的先前狀態開始變更。客戶特定垃圾郵件過濾政策將啟用，且這些政策會套用最新的客戶特定規則。如果您刪除所有提交資料，所有提交的郵件僅視為全域規則產生或規則刪除。

因為 BodyHash 規則是以電子郵件的精準特徵為目標，所以 BodyHash 規則具有高度準確性。BodyHash 規則對於對抗垃圾郵件寄發者和其他攻擊者所用的簡短內容郵件及重複郵件特別有效。

BrightSig3 規則會隨著垃圾郵件寄發者所嘗試的動作而進行調整，以隨機排列並干擾惡意電子郵件。這些規則會以擁有與範例郵件相似之統計資訊的郵件為目標，對於對抗不同郵件間存在高度相似性的垃圾郵件攻擊特別有效。這些規則採用模糊邏輯演算法，來擊敗嘗試使用混淆和變化技術避開更多傳統特徵的垃圾郵件寄發者。

BodyHash 與 BrightSig3 規則的組合，提供抵禦使用簡短內容郵件的攻擊者，以及垃圾郵件寄發者使用不同混淆技術之攻擊的高效防護盾。這些技術代表賽門鐵克用來消滅全球電子郵件威脅載體之 20 種以上不同技術的其中兩種技術。客戶特定垃圾郵件規則的使用者擁有其他 BodyHash 和 BrightSig3 規則提供的增補防護。此外，這些規則也會特別以個別公司通常會遭遇到的威脅作為目標。

若要啟用、設定、修改或刪除垃圾郵件提交設定值，您必須具備「完整管理權限」或「管理垃圾郵件提交」的修改權限。

請參閱第 566 頁的「管理員權限」。

如何建立規則，以及為何郵件可能不會產生自訂規則

賽門鐵克會完成下列程序決定是否需要根據提交的郵件建立規則集：

1. 確認已啟用客戶特定垃圾郵件提交功能。

   請參閱第 230 頁的「啟用或停用客戶特定垃圾郵件提交」。

2. 確認郵件來自有效來源。

   請參閱第 230 頁的「佈建客戶特定垃圾郵件提交的提交者 ID」。

3. 確認提交郵件的人員位於**「允許」**清單中，或不在**「攔截」**清單中。

   請參閱第 233 頁的「指定誰能夠提交客戶特定規則的郵件」。

4. 決定郵件本身是否有效。

   賽門鐵克可能因為下列原因而將郵件視為無效，且不將其用於建立自訂規則集：

   - 不符合 RFC5322 的郵件皆視為無效。

     附註：儲存為 .msg 檔案的 Outlook 郵件與 RFC 不相容，因此不會被視為有效提交。

     您可以在控管中心內上載或貼上有效 RFC5322 郵件。
     如需有關 RFC5322 要求的更多資訊，請連線至 Internet 並移至下列 URL：
     https://tools.ietf.org/html/rfc5322

   - 有時，郵件在傳輸過程中遭到了修改，因此在送達賽門鐵克時已經失去了有效性。失去有效性的郵件不能用於建立自訂規則。有效性的喪失可能會因為各種原因而發生。

5. 判斷是否已存在全域規則。

   即使全域規則已經存在，賽門鐵克仍可以建立自訂規則以作為全域規則遭到刪除或停用時的預防措施。

6. 判斷是否達到積極程度。

   如果積極程度為「保守」，則必須有多個使用者提交相同的郵件才會考慮根據該郵件建立規則。

   請參閱第 232 頁的「設定客戶特定垃圾郵件提交積極程度」。

7. 如果符合所有上述條件，則賽門鐵克便會在提交垃圾郵件時建立新規則。如果提交了誤報郵件，則不會建立新規則，且賽門鐵克可能會刪除導致誤報的自訂規則。

設定客戶特定垃圾郵件提交

表 11-6 描述了為設定客戶特定的垃圾郵件提交功能所必須採取的步驟。您必須具備「完整管理權限」、「管理設定」或「管理垃圾郵件提交」修改權限，才能執行這些工作。

表 11-6 設定客戶特定垃圾郵件提交功能

步驟	工作	說明
步驟 1	啟用客戶特定垃圾郵件提交功能。	您必須啟用此功能，賽門鐵克才能建立自訂規則。 此功能預設為停用。 請參閱第 230 頁的「啟用或停用客戶特定垃圾郵件提交」。
步驟 2	取得提交者 ID 或指定現有的提交者 ID。	提交者 ID 可確保自訂規則集僅供由指定控管中心管理的掃描程式使用。 請參閱第 230 頁的「佈建客戶特定垃圾郵件提交的提交者 ID」。
步驟 3	指定提交積極程度。	您可以指定是否將所有提交的郵件都視為自訂規則。或者您可以指定一封郵件是否必須從不同的使用者提交多次後，才考慮該郵件。 請參閱第 232 頁的「設定客戶特定垃圾郵件提交積極程度」。
步驟 4	指定可以提交或無法提交自訂規則郵件的人員。	Symantec Messaging Gateway 可讓您指定誰能夠提交郵件以建立自訂規則。或者，您可以指定誰無法提交郵件。 請參閱第 233 頁的「指定誰能夠提交客戶特定規則的郵件」。
步驟 5	啟用使用客戶特定規則的政策。	您必須針對客戶特定規則啟用客戶特定政策，才能套用至內送郵件。 請參閱第 221 頁的「啟用和停用垃圾郵件及不必要的電子郵件政策」。 請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。
步驟 6 選用	架構**「這是垃圾郵件」**與**「這不是垃圾郵件」**選項在內容隔離事件資料夾中顯示。	如果您要讓管理員針對客戶特定規則從內容隔離事件資料夾提交郵件，您必須架構這些選項，使其在**「事件」**詳細頁面上顯示。 針對每個您要顯示郵件的內容隔離所事件資料夾啟用這些選項。 **附註：**資訊事件資料夾無法使用這個選項。 請參閱第 365 頁的「架構郵件提交選項，使其顯示於隔離事件資料夾中」。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

請參閱第 228 頁的「如何建立規則，以及為何郵件可能不會產生自訂規則」。

啟用或停用客戶特定垃圾郵件提交

啟用客戶特定垃圾郵件提交功能，以管理員與一般使用者識別為遺漏垃圾郵件或誤報的電子郵件為依據，來取得客戶特定垃圾郵件規則。即使此功能停用，郵件仍會提交給賽門鐵克，但是不會建立自訂規則。

在您啟用此功能後，請確定完成剩餘的步驟，以完整設定此功能。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

如果您在環境中不再利用客戶特定規則，您可以停用此功能。您也可以刪除所有相關的規則與資料。

請參閱第 237 頁的「正在刪除客戶特定垃圾郵件資料」。

您必須具備「完整管理權限」、「管理設定」或「管理垃圾郵件提交」修改權限，才能啟用或停用此功能。

啟用客戶特定垃圾郵件提交

1. 在控管中心內，按下**「垃圾郵件」>「設定」>「提交設定」**。
2. 在**「客戶特定垃圾郵件提交」**頁面上，勾選**「啟用客戶特定垃圾郵件提交」**。

   此功能預設為停用。
3. 請參閱隱私權政策協議，並勾選**「我同意此隱私權政策的條款」**。

   隱私權協議只會在您第一次啟用此功能時顯示。
4. 按下**「啟用客戶特定垃圾郵件提交」**。

   您必須先佈建您的提交者 ID，才能按下**「儲存」**。

   請參閱第 230 頁的「佈建客戶特定垃圾郵件提交的提交者 ID」。

停用客戶特定垃圾郵件提交

1. 在控管中心內，按下**「垃圾郵件」>「設定」>「提交設定」**。
2. 在**「客戶特定垃圾郵件提交」**頁面上，取消勾選**「啟用客戶特定垃圾郵件提交」**。
3. 按下**「儲存」**。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

佈建客戶特定垃圾郵件提交的提交者 ID

賽門鐵克要求每個提交自訂規則郵件的控管中心都需有提交者 ID。Symantec 會根據具有 ID 的「控管中心」所提交的郵件建立自訂規則。接著這些規則會套用到具有該提交者 ID 的「控管中心」所管理的任何掃描程式。

您可以讓每個控管中心擁有唯一的提交者 ID，或者讓多個控管中心共用提交者 ID。共用提交者 ID 的控管中心也會共用相同的自訂規則。

表 11-7會提供控管中心是否使用唯一的提交者 ID 或共用提交者 ID 的準則。

表 11-7　　提交者 ID 使用建議

情景	建議
單一控管中心 (標準組態)	取得並使用唯一提交者 ID。 請參閱第 232 頁的「佈建客戶特定垃圾郵件提交的新提交者 ID」。
您要共用規則的多個控管中心 (標準組態)	例如，假設有兩個控管中心。您要這兩個控管中心使用相同的自訂規則，無論是由哪個「控管中心」提交垃圾郵件來建立規則集。 取得一個控管中心的唯一提交者 ID。接著將該提交者 ID 套用到其他的控管中心。 請參閱第 232 頁的「指定客戶特定垃圾郵件提交的現有提交者 ID」。 賽門鐵克會根據從任何一個控管中心提交的所有郵件建立規則，並在所有控管中心之間套用相同的規則。
您要使用唯一規則的多個控管中心 (進階組態)	例如，假設有兩個控管中心。一個控管中心的組態及用途與另一個控管中心的大不相同。因此您要每個控管中心為自己的自訂規則提交自己的郵件。 取得每個控管中心的唯一提交者 ID。每個控管中心會根據從該控管中心提交的垃圾郵件接收自己的自訂規則集。

無論您是取得新的提交者 ID 或佈建現有的提交者 ID，管理員都會從賽門鐵克收到一封電子郵件，這封郵件確認作業並包含提交者 ID 號碼。賽門鐵克建議的最佳實務準則就是保留這封電子郵件作為參考。您必須啟用管理員的警示通知，才能收到這些電子郵件通知。

請參閱第 590 頁的「架構警示」。

當您刪除客戶特定垃圾郵件資料時，也會刪除提交者 ID。當您重設為出廠設定值時，也會遺失提交者 ID。當您執行完整備份或組態備份時，您會備份提交者 ID。當成功還原備份時，ID 便可供使用。

請參閱第 237 頁的「正在刪除客戶特定垃圾郵件資料」。

請參閱第 600 頁的「將硬體裝置重設為出廠預設值 」。

請參閱第 606 頁的「排程備份」。

請參閱第 609 頁的「執行隨選備份」。

請參閱第 641 頁的db-backup。

您必須具備「完整管理權限」、「管理垃圾郵件提交」或「管理設定」修改權限，才能執行這些工作。您也必須具備有效的授權才能取得新的提交者 ID。

佈建客戶特定垃圾郵件提交的新提交者 ID

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**提交設定**」。

2 在「**客戶特定垃圾郵件提交**」頁面上，按下「**立即註冊新的提交者 ID**」。

3 在「**註冊提交 ID**」對話方塊中，按下「**註冊**」。

4 在確認對話方塊中，按下「**關閉**」。

5 按下「**儲存**」。

指定客戶特定垃圾郵件提交的現有提交者 ID

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**提交設定**」。

2 在「**客戶特定垃圾郵件提交**」頁面上，按下「**輸入現有提交者 ID**」。

3 在「**多個控管中心**」對話方塊中，輸入現有的提交者 ID。

4 按下「**驗證提交者 ID**」。

5 在「**註冊提交 ID**」對話方塊中，按下「**註冊**」。

6 在確認對話方塊中，按下「**關閉**」。

7 按下「**儲存**」。

8 為每個您要共用自訂規則的控管中心重複此程序。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

設定客戶特定垃圾郵件提交積極程度

Symantec Messaging Gateway 會根據管理員與一般使用者提交的郵件建立自訂規則。根據預設，賽門鐵克只會針對管理員提交的郵件建立規則。此外，您可架構賽門鐵克為一般使用者提交的郵件建立規則。一般使用者提交的預設設定能夠進一步確定您未取得任何依據意外提交或錯誤提交的規則。但是，您可以指定使用一般使用者提交的所有郵件來建立自訂規則。

您必須具備「完整管理權限」、「管理垃圾郵件提交」或「管理設定」修改權限，才能修改此設定。

設定客戶特定垃圾郵件提交積極程度

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**提交設定**」。

2 在「**客戶特定垃圾郵件提交**」頁面上，「**提交積極程度**」下選取以下其中一個選項：

- **「保守」- 僅具有多重提交的郵件會取得規則**
  多個一般使用者必須提交相同的郵件，賽門鐵克才會針對新規則考慮這些郵件。
- **積極 - 每個提交都會取得規則**
  部分提交的郵件中發生的實例未產生新的規則集。
  請參閱第 228 頁的「如何建立規則，以及為何郵件可能不會產生自訂規則」。

預設設定是**「保守」**。

3 按下**「儲存」**。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

指定誰能夠提交客戶特定規則的郵件

Symantec Messaging Gateway 可讓您指定誰能夠提交郵件以建立自訂規則。或者，您可以指定誰無法提交自訂規則的郵件。系統會提交受限制使用者的郵件，但不將其郵件視為規則集建立。受限制使用者的提交項目在報告中會顯示成**「已攔截」**。

您可以使用以下其中一種方法將使用者新增至**「提交者電子郵件地址」**清單：

- 手動輸入。
  請以逗點分隔多個電子郵件地址。
- 匯入使用者清單。
  匯入的使用者清單必須是文字檔 (.txt)，其中有新行字元可分隔項目。

警告：當您匯入電子郵件地址時，所有現有的電子郵件地址會以匯入檔案 (非附加檔案) 中的電子郵件地址取代。

附註：不支援萬用字元，您必須輸入有效的電子郵件地址。

在**「提交者電子郵件地址」**清單中最多可以有 1,000 個電子郵件地址。Symantec Messaging Gateway 會驗證您的項目，確保您使用有效的電子郵件地址，而且沒有重複的項目。

您也可以視需要移除、匯出並檢視清單中的電子郵件地址。

請參閱第 234 頁的「處理「提交者電子郵件地址」清單」。

當您執行完整備份或組態備份時，會備份**「提交者電子郵件地址」**清單。賽門鐵克建議的最佳實務準則就是排程定期備份，確保您能擷取最新的**「提交者電子郵件地址」**清單。當您要進行變更以保留為備份時，也可以定期匯出**「提交者電子郵件地址」**清單。

請參閱第 606 頁的「排程備份」。

具有「完整的管理權限」、「管理垃圾郵件提交」修改權限或「管理設定」修改權限的管理員才能提交郵件以建立規則。管理員也必須具有上述其中一個權限，才能修改這些設定。

具有「有限的管理權限」(包括「管理垃圾郵件提交」修改權限和「管理隔離所/隔離事件」檢視或修改權限) 的管理員所提交的項目可用於建立客戶特定垃圾郵件規則。

只要佈建提交者 ID，啟用和停用客戶特定垃圾郵件提交功能對於提交和建立客戶特定規則將沒有任何影響。一旦佈建了提交者 ID，即使停用客戶特定垃圾郵件提交功能，系統仍會建立客戶特定垃圾郵件規則。

不過，必須在啟用客戶特定垃圾郵件提交功能之後，才能下載所建立的規則。

指定誰能夠提交客戶特定規則的郵件

1 在控管中心內，按下**「垃圾郵件」>「設定」>「提交設定」**。

2 在**「客戶特定垃圾郵件提交」**頁面上，按下**「提交者清單」**標籤。

3 選取選項以允許**「提交者電子郵件地址」**中的使用者提交垃圾郵件規則的郵件或攔截郵件。

預設值是**「允許 - 僅此清單上的管理員和電子郵件地址可以傳送郵件」**。

4 執行下列其中一項工作：

手動新增電子郵件地址	在**「手動新增電子郵件地址」**欄位中，輸入電子郵件地址並按下**「新增」**。
匯入電子郵件地址	執行下列所有工作： ■ 按下**「瀏覽」**。 ■ 找到並選取您要匯入的檔案。 ■ 按下**「匯入」**。 **警告：**當您匯入電子郵件地址時，所有現有的電子郵件地址會以匯入檔案 (非附加檔案) 中的電子郵件地址取代。

5 按下**「儲存」**。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

處理「提交者電子郵件地址」清單

下列內容描述**「垃圾郵件」>「提交設定」>「提交者清單」**標籤上之**「提交者電子郵件地址」**清單的功能。

刪除一或多個項目	您可以一次刪除一或多個項目。您也可以一次刪除清單內的所有項目。刪除項目之後，就無法再擷取該項目。 請參閱第 235 頁的「若要一次刪除一或多個項目」。

匯出項目	您可能想要從某一個控管中心上的**「提交者電子郵件地址」**匯出電子郵件地址，並將其匯入另一個控管中心。此功能去除了重新輸入所有電子郵件地址項目的必要性。 請參閱第235頁的「若要從「提交者電子郵件地址」清單匯出電子郵件地址」。
檢視項目	**「提交者電子郵件地址」**中最多可以有1,000個電子郵件地址。Symantec Messaging Gateway 提供了可以幫助您輕鬆瀏覽清單的圖示。 請參閱第 235 頁的「若要瀏覽「提交者電子郵件地址」清單」。

您必須擁有「完整的管理權限」、「管理垃圾郵件提交」或「管理設定」的修改權限，才能修改這些設定。

若要一次刪除一或多個項目

1 在控管中心內，按下**「垃圾郵件」>「設定」>「提交設定」**。

2 在**「客戶特定垃圾郵件提交」**頁面上，按下**「提交者清單」**標籤。

3 執行下列其中一項工作：

若要刪除一或多個電子郵件地址	執行下列其中一個工作： ■ 勾選要刪除之電子郵件地址旁的方塊，然後按下**「刪除」**。 ■ 若要選取**「提交者電子郵件地址」**清單中所有可見地址，請勾選**「提交者電子郵件地址」**旁的方塊，然後按下**「刪除」**。
若要刪除**「提交者電子郵件地址」**清單中的所有電子郵件地址。	按下**「全部刪除」**，並在確認對話方塊中按下**「確定」**。

4 按下**「儲存」**。

若要從「提交者電子郵件地址」清單匯出電子郵件地址

1 按下**「匯出」**。

2 遵循網頁瀏覽器對話方塊指示，指定匯出檔案的儲存位置。

若要瀏覽「提交者電子郵件地址」清單

◆ 執行下列其中一個工作：

若要指定每頁檢視的地址數量	按下**「每頁的項目數」**下拉式箭頭，並選取每頁要檢視的項目數量。 您可以在每頁上檢視 10、25、50 或 100 個項目。預設值為 25。
若要指定想要檢視的電子郵件地址頁數	按下**「顯示」**下拉式箭頭，然後選取頁數。

若要前往另一頁	選取下列其中一個瀏覽圖示： ■ 瀏覽至第一頁的提交者電子郵件地址。 ■ 瀏覽至上一頁的提交者電子郵件地址。 ■ 瀏覽至下一頁的提交者電子郵件地址。 ■ 瀏覽至最後一頁的提交者電子郵件地址。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

請參閱第 233 頁的「指定誰能夠提交客戶特定規則的郵件」。

透過控管中心提交郵件以建立客戶特定規則

除了從「垃圾郵件隔離所」和內容過濾事件資料夾提交郵件以建立規則之外，管理員也可以直接從控管中心提交郵件。

請參閱第 258 頁的「針對客戶特定規則，從「垃圾郵件隔離所」提交郵件」。

請參閱第 380 頁的「針對客戶特定規則，從隔離所資料夾提交郵件」。

您透過控管中心所提交的郵件必須包含標頭和內文，且必須是有效的 RFC5322 郵件。

附註：儲存為 .msg 檔案的 Outlook 郵件與 RFC 不相容，因此不會被視為有效提交。

請參閱第 228 頁的「如何建立規則，以及為何郵件可能不會產生自訂規則」。

建立規則時，管理員所提交的項目較一般使用者所提交的項目而言將會獲得更優先的考量。但是，不論是從控管中心、「垃圾郵件隔離所」或內容事件資料夾進行提交，所有由管理員所提交的郵件都會獲得相同程度的考量。

即使停用客戶特定垃圾郵件提交功能，賽門鐵克仍會分析您透過「垃圾郵件隔離所」提交的郵件。它將會考量郵件是否符合全域垃圾郵件規則或全域誤報規則，但是並不會建立自訂規則。

只有具備「完整的管理權限」或「管理垃圾郵件提交」修改權限的管理員可以透過控管中心提交郵件。

附註：提交的郵件大小不能超過 5 MB。如果嘗試提交的郵件超過此限制，將會顯示錯誤訊息。

若要透過控管中心提交郵件以建立客戶特定規則

1 在控管中心內，按下**「垃圾郵件」>「提交」>「提交郵件」**。

2 在**「郵件類型」**下，勾選適當的方塊以指出郵件是否為遺漏垃圾郵件或錯誤識別為垃圾郵件。

3 執行下列其中一項工作：

若要上載現有郵件	按下**「上載郵件」**，然後按下**「瀏覽」**。尋找並選取要上載的郵件，然後按下**「開啟」**。
若要貼上郵件內容	從來源複製郵件內容，並在**「貼上郵件」**欄位中貼上郵件內容。

4 按下**「提交郵件」**。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

正在刪除客戶特定垃圾郵件資料

Symantec Messaging Gateway 會保留管理員和一般使用者所提交以建立規則集的郵件資料，以及伴隨的規則。您可能會想要刪除客戶特定垃圾郵件資料，以移除之前的規則，並建立全新的規則。如果您不想再於環境內利用客戶特定規則，您可以永久刪除所有客戶特定垃圾郵件資料。之後，您也應停用該功能。

請參閱第 230 頁的「啟用或停用客戶特定垃圾郵件提交」。

刪除客戶特定垃圾郵件資料時，您將會刪除下列所有項目：

- 所有提交以供建立規則的資料
- 所有賽門鐵克根據該資料建立的規則
- 在垃圾郵件提交報告中使用的資料
- 提交者 ID
- 所有在**「提交者電子郵件地址」**清單中的電子郵件地址

警告：刪除客戶特定垃圾郵件資料後即無法擷取。

此外，積極程度選項將會回復為預設設定，且 Symantec Messaging Gateway 將不再採取您針對垃圾郵件政策條件所指定的動作**「如果郵件是客戶特定垃圾郵件」**。

您必須擁有「完整的管理權限」、「管理垃圾郵件提交」或「管理設定」的修改權限，才能執行此工作。

若要刪除客戶特定垃圾郵件資料

1 在控管中心內，按下**「垃圾郵件」>「設定」>「提交設定」**。

2 在**「客戶特定垃圾郵件資料保留」**下的**「組態」**標籤上，按下**「刪除所有客戶特定垃圾郵件資料」**。

3 在確認對話方塊中，讀取警告並按下**「刪除所有客戶特定垃圾郵件資料」**。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

12

隔離垃圾郵件

本章包含以下主題：

- 關於隔離垃圾郵件
- 使用垃圾郵件隔離所之前
- 隔離已傳送至未解析電子郵件地址的垃圾郵件
- 關於瀏覽垃圾郵件隔離所
- 架構垃圾郵件隔離所設定
- 檢視垃圾郵件隔離所中的郵件
- 處理垃圾郵件隔離所中的郵件
- 架構「垃圾郵件隔離所」通知
- 垃圾郵件隔離所疑難排解
- 大型部署的垃圾郵件隔離所最佳實務準則

關於隔離垃圾郵件

您可以將垃圾郵件、可疑垃圾郵件，或兩者一起路由至「垃圾郵件隔離所」，讓管理員和使用者可以視需要存取這些郵件，檢查是否有誤報的情況。「垃圾郵件隔離所」可協助您微調垃圾郵件設定與垃圾郵件政策。如果出現過多誤報情況，則代表垃圾郵件設定過於嚴格，且應該加以修改。您可選用「垃圾郵件隔離所」。

「垃圾郵件隔離所」會儲存垃圾郵件，並可讓網頁式使用者和管理員存取這些郵件。使用者必須使用自己的 LDAP 使用者名稱與驗證來存取「垃圾郵件隔離所」。如果郵件標示為垃圾郵件或可疑垃圾郵件，但為合法郵件，則使用者可將這些郵件釋放至他們的收件匣中。使用者可以通知您發生誤報情況，讓您可以據此持續地調整垃圾郵件設定與垃圾郵件政策。您也可以將摘要通知設定為傳送至使用者的收件匣中。

您可以架構臨界值來控制配置給「垃圾郵件隔離所」的空間。

請參閱第 240 頁的「使用垃圾郵件隔離所之前」。

請參閱第 242 頁的「架構一般使用者隔離所」。

請參閱第 249 頁的「管理員和使用者之垃圾郵件隔離所的差異」。

使用垃圾郵件隔離所之前

如果您想要允許使用者存取「垃圾郵件隔離所」，則請在使用「垃圾郵件隔離所」之前確定已完成下列所有項目：

建立和啟用可用來隔離垃圾郵件和可疑垃圾郵件的垃圾郵件政策。	一或多個政策群組必須擁有隔離郵件的相關過濾器政策。例如，您可以建立垃圾郵件政策，將「預設」群組的入埠可疑垃圾郵件隔離。 請參閱第 219 頁的「建立偵測垃圾郵件及不必要的電子郵件的政策」。
架構 LDAP 伺服器，並確定其正確運作。	只有當控管中心能夠透過使用驗證存取 LDAP 伺服器時，使用者才能登入垃圾郵件隔離所檢查其隔離郵件。您也需要 LDAP 驗證來擴展 LDAP 電子郵件別名，以及設定**「移除未解析的電子郵件」**。 請參閱第 437 頁的「關於將驗證功能與資料來源搭配使用」。
確定您具有可用的 SMTP 郵件伺服器。	「垃圾郵件隔離所」並不需要另外的 SMTP 郵件伺服器來傳送通知和重送錯誤識別的郵件。不過，必須要有 SMTP 郵件伺服器，才能接收「垃圾郵件隔離所」所傳送的通知和錯誤識別的郵件。因為通知和錯誤識別的郵件不需要過濾，所以您選擇的 SMTP 伺服器應該位於掃描程式的下游。 請參閱第 48 頁的「架構 SMTP 進階設定」。

請參閱第 239 頁的「關於隔離垃圾郵件」。

請參閱第 584 頁的「讓使用者略過控管中心登入憑證」。

隔離已傳送至未解析電子郵件地址的垃圾郵件

如果針對位址解析架構了 LDAP，依預設，傳送至不存在電子郵件地址的郵件 (根據 LDAP 查詢) 會被刪除。如果在控管中心的**「垃圾郵件」>「設定」>「隔離所設定」**頁面上，取消勾選**「刪除傳送至未解析電子郵件地址的郵件」**，則這些郵件都會儲存在「垃圾郵件隔離所」的 `postmaster` 信箱中。

請參閱第 436 頁的「建立位址解析資料來源」。

如果未針對位址解析架構 LDAP，依預設，**「刪除傳送至未解析電子郵件地址的郵件」**會取消勾選並變成灰色。

附註：如果 LDAP 伺服器連線失敗或未正確架構 LDAP 設定，則寄給未解析電子郵件地址的隔離郵件會寄存在掃描程式的延遲佇列中，且會關閉控管中心和掃描程式之間的 SMTP 連線，不論是否有勾選「刪除未解析的電子郵件」核取方塊。在達到掃描程式的延遲重試或逾時限制後，郵件會退回給寄件者。

隔離已傳送至未解析電子郵件地址的垃圾郵件

1. 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。
2. 在「一般設定」區段中，取消勾選**「刪除傳送至未解析電子郵件地址的郵件」**。
3. 按下**「儲存」**。

關於瀏覽垃圾郵件隔離所

下列圖示顯示如何瀏覽「垃圾郵件隔離所」郵件清單頁面：

移至郵件開頭。

瀏覽至最後一頁郵件，如果總共超過 50 頁，則會瀏覽至 50 頁後。

移至上一頁郵件。

移至下一頁郵件。

最多可選擇在每頁顯示目前郵件頁面之前或之後的 500 個項目。

下列圖示顯示如何瀏覽「垃圾郵件隔離所」郵件詳細資料頁面：

移至上一封郵件。

移至下一封郵件。

當您瀏覽至不同郵件頁面時，並不會保留原始頁面中的核取方塊狀態。例如，假設您在第一頁上選取三封郵件，然後移到下一頁。當您返回第一頁時，會清除所有郵件的核取方塊。

架構垃圾郵件隔離所設定

「垃圾郵件隔離所」是一種儲存庫，用來存放 Symantec Messaging Gateway 識別為垃圾郵件的郵件。

表 12-1 描述您可以架構「垃圾郵件隔離所」設定值的方式。您可以視需要以任何順序執行這些工作。

表 12-1 架構「垃圾郵件隔離所」設定

工作	說明
架構個別政策群組的垃圾郵件隔離所	如果您已架構好 LDAP 目錄伺服器，可以架構「垃圾郵件隔離所」，只讓特定政策群組的成員可以存取它。如果只要架構管理員的存取權，請全域啟用隔離所，然後只為「管理」政策群組啟用一般使用者隔離所。 請參閱第 242 頁的「架構一般使用者隔離所」。
視需要啟用語言編碼。	在大多數情況下，「自動偵測」設定可以對「垃圾郵件隔離所」中的郵件正確地判斷語言編碼。不過，對於某些郵件，控制中心可能無法判斷其正確語言編碼。如果郵件呈現亂碼，請選取最可能符合該郵件所使用的語言編碼。 請參閱第 244 頁的「選擇垃圾郵件的語言編碼」。
設定隔離所臨界值，讓隔離所在您硬體裝置上使用的空間降到最低。	「垃圾郵件隔離所」臨界值可讓您控制「垃圾郵件隔離所」的大小上限。您可以使用清除程式來強制「垃圾郵件隔離所」臨界值設定。 請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。 請參閱第 245 頁的「垃圾郵件隔離所的臨界值考量」。
指定隔離所郵件保留期限。	在刪除郵件前，您可以變更垃圾郵件的保留時間。如果隔離的郵件耗用太多磁碟空間，您可以縮短保留時間。 請參閱第 246 頁的「指定垃圾郵件保留在隔離所的時間」。
架構清除程式。	您可以指定「隔離所清除程式」開始執行清除程序的時間和執行清除程序的頻率。清除程式可讓您將「垃圾郵件隔離所」保持在可管理的大小。 請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。
架構誤報通知。	您也可以自動將複本傳送給本機系統管理員、賽門鐵克或兩者。這些郵件應傳送給組織中負責監控錯誤識別之郵件的管理員，以確定 Symantec Messaging Gateway 的有效性。 請參閱第 247 頁的「指定要通知誤報郵件的對象」。

架構一般使用者隔離所

一般使用者隔離所可讓個別使用者存取其「垃圾郵件隔離所」中的郵件，以及接收隔離所通知。如果您已架構好 LDAP 目錄伺服器，可以架構「垃圾郵件隔離所」，只讓特定政策群組的成員可以存取它。

您必須先完成下列基本步驟，才能啟用一般使用者隔離所。

- 步驟 1：選擇您目錄資料來源上的設定
- 步驟 2：全域啟用一般使用者隔離所
- 步驟 3：將一般使用者隔離所權限指派給群組

步驟 1：選擇您目錄資料來源上的設定

一般使用者隔離所使用 LDAP 資訊，驗證嘗試登入並檢視其隔離郵件的一般使用者。隔離所還會將 LDAP 資訊用於位址解析，以將已隔離郵件指派給個別使用者隔離所。

以下指示假設您已新增並架構目錄資料來源。

請參閱第 425 頁的「架構目錄資料整合」。

啟用一般使用者隔離所需要的 LDAP 設定

1 在控管中心內，選取**「管理」>「設定」>「目錄整合」**。

2 在**「目錄整合」**頁面上，選取您的目錄資料來源，然後按下**「編輯」**。

3 在**「驗證」**」標籤上，選取**「啟用驗證」**。從下拉式功能表中，選取**「僅控管中心驗證」**或**「控管中心和 SMTP 驗證」**。

4 在**「位址解析」**標籤上，選取**「啟用位址解析」**。從下拉式功能表中，選取**「僅電子郵件掃描」**或**「控管中心授權和電子郵件掃描」**。

5 按下**「儲存」**。

步驟 2：全域啟用一般使用者隔離所

設定 LDAP 設定後，您可以啟用一般使用者隔離所。此程序的作用類似於一般使用者隔離所的全域開關。

全域架構一般使用者隔離所

1 選取**「垃圾郵件」>「設定」>「隔離所設定」**。

2 在**「一般使用者設定」**面板中，選取**「啟用隔離所」**。

附註：如果您未連線目錄資料來源，**「啟用隔離所」**會停用。

---

3 視需要編輯**「垃圾郵件隔離所登入網址」**。

附註：預設**「垃圾郵件隔離所登入網址」**為 `https://<host_FQDN>:41443/brightmail`。如果您變更主機的完整網域名稱 (FQDN)，預設 URL 會自動變更。不過，如果您自訂**「垃圾郵件隔離所登入網址」**並且稍後又變更主機的 FQDN，則必須手動變更自訂的 URL。

---

4 按下**「儲存」**。

步驟 3：將一般使用者隔離所權限指派給群組

全域啟用一般使用者隔離所後，您必須先針對個別政策群組 (包括管理員政策群組) 啟用該功能，之後一般使用者才能存取其隔離的郵件。

將一般使用者隔離所存取權新增至政策群組

1 在控管中心內，選取**「管理」>「使用者」>「政策群組」**。

2 在「政策群組」頁面上，選取群組並按下**「編輯」**，或按下**「新增」**以新增政策群組。

3 在**「一般使用者」**標籤上，選取**「啟用一般使用者隔離所」**。

4 選用：選取**「啟用此政策群組的一般使用者設定」**。然後啟用**「建立個人之「允許的寄件者」清單和「攔截的寄件者」清單」**和**「指定語言設定」**(如果您想要將這些權限授予群組成員)。

如果您要防止一般使用者修改他們自己的設定，請保留這些設定為停用狀態。

5 按下**「儲存」**。

只針對管理員架構一般使用者隔離所

若要只允許管理員登入和使用一般使用者隔離所，請執行步驟 1：選擇您目錄資料來源上的設定和步驟 2：全域啟用一般使用者隔離所。然後在步驟 3：將一般使用者隔離所權限指派給群組中，將一般使用者隔離所僅指派給您的管理政策群組。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 249 頁的「管理員和使用者之垃圾郵件隔離所的差異」。

選擇垃圾郵件的語言編碼

在大多數情況下，「自動偵測」設定可以對「垃圾郵件隔離所」中的郵件正確地判斷語言編碼。不過，對於某些郵件，控管中心可能無法判斷其正確語言編碼。如果郵件呈現亂碼，請選取最可能符合該郵件所使用的語言編碼。

只有具有「完整管理」權限或「管理隔離所」之修改權限的管理員可以選擇隔離所中之郵件的語言編碼。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

請參閱第 253 頁的「依日期排序隔離所中的垃圾郵件和可疑郵件」。

選擇垃圾郵件的語言編碼

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 按下您要檢視之郵件的主旨行。

3 在「郵件詳細資料」頁面上，從下拉式清單中選取語言編碼。

修改「垃圾郵件隔離所」臨界值

「垃圾郵件隔離所」臨界值可讓您控制「垃圾郵件隔離所」的大小上限。您可以使用清除程式來強制「垃圾郵件隔離所」臨界值設定。只有具備「完整的管理」權限或「管理設定」修改權限的管理員，才能修改隔離所設定。

附註：由於清除程式會維持垃圾郵件隔離所的大小上限，因此在以下一個排程間隔執行清除程式之前，隔離所可能會超過上限臨界值。

請參閱第 246 頁的「指定垃圾郵件保留在隔離所的時間」。

請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。

在修改「垃圾郵件隔離所」臨界值之前，請先確定您瞭解其涵義和考量。

請參閱第 245 頁的「垃圾郵件隔離所的臨界值考量」。

表 12-2 描述了您可以架構的「垃圾郵件隔離所」臨界值。

表 12-2 「垃圾郵件隔離所」臨界值

臨界值	說明
隔離所的大小上限	所有使用者之已隔離郵件所使用的磁碟空間上限。 隔離所的大小上限反映了郵件存放區中的每個郵件檔案在磁碟上的實際大小。實際的磁碟使用量可能會稍高，因為有其他磁碟使用量未納入計算，例如資料庫表格和索引。
每個使用者的大小上限	每個使用者之隔離所郵件所使用的磁碟空間上限。
郵件數量上限	所有使用者的郵件數量上限(傳送至多個收件者的同一郵件計為一則郵件)。
每個使用者的郵件數量上限	每個使用者的隔離所郵件數量上限

修改「垃圾郵件隔離所」臨界值

1 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。

2 在**「臨界值」**下，針對要架構的每一種臨界值，勾選方塊並輸入大小臨界值或郵件臨界值。

您可以架構多個臨界值。

3 按下**「儲存」**。

垃圾郵件隔離所的臨界值考量

表 12-3 說明修改「垃圾郵件隔離所」臨界值之前應考量的問題。

表 12-3 修改「垃圾郵件隔離所」臨界值之前應考量的問題

應考量的問題	詳細資料
清除程式會在執行時實施臨界值。 清除程式會刪除較舊的郵件，以實施臨界值。	在下次清除程式執行之前，可能會暫時超過臨界值。
每個使用者的臨界值是執行處理最多的臨界值。	我們不建議在大型部署中實施每個使用者臨界值，例如超過 5000 位使用者的部署。當清除程式執行時，會在實施其他臨界值之前，先檢查並實施每個使用者臨界值。
「隔離所的大小上限」和**「郵件數上限」**臨界值在磁碟使用量和郵件計數上，能提供最精準的控制。	在郵件較少的情況下，「垃圾郵件隔離所」搜尋的執行速度會更快。
縮短「垃圾郵件隔離所」郵件保留時間，也可以限制「垃圾郵件隔離所」大小。	相較於使用「垃圾郵件隔離所」臨界值，節省磁碟空間是管理「垃圾郵件隔離所」大小較為有效的方法。
如果超過指定的「垃圾郵件隔離所」臨界值，並不會引發警示或通知。	您可以架構**「垃圾郵件隔離所的最大架構磁碟空間使用量已超過」**的警示。 請參閱第 590 頁的「架構警示」。

請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。

指定垃圾郵件保留在隔離所的時間

在刪除郵件前，您可以變更垃圾郵件的保留時間。如果隔離的郵件耗用太多磁碟空間，您可以縮短保留時間。不過，較短的保留時間會導致使用者來不及檢查郵件就已將其刪除。預設保留時間是7天。只有具備「完整的管理」權限或「管理設定」修改權限的管理員，才能修改隔離所設定。

依據預設，清除程式會在每天的上午 1 點刪除超過保留期間的郵件。例如，如果保留時間為 7 天，則清除程式執行時會刪除 7 天前的所有郵件。清除程式也會視需要刪除郵件，以強制「垃圾郵件隔離所」郵件和大小臨界值。

請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。

請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。

您也可以從「垃圾郵件隔離所」中手動刪除郵件。

請參閱第 256 頁的「刪除隔離所中的垃圾郵件」。

指定垃圾郵件保留在隔離所的時間

1 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。

2 在**「垃圾郵件隔離所清除程式」**下方的 **「刪除前在隔離所儲存的天數」**欄位中，輸入天數。

3 按下「隔離所設定」頁面上的**「儲存」**。

指定垃圾郵件隔離所的清除時間與頻率

您可以指定「隔離所清除程式」開始執行清除程序的時間和執行清除程序的頻率。 清除程式可讓您將「垃圾郵件隔離所」保持在可管理的大小。 無法擷取已清除的郵件。 只有具備「完整的管理」權限或「管理設定」修改權限的管理員，才能修改隔離所設定。

請參閱第 246 頁的「指定垃圾郵件保留在隔離所的時間」。

請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。

請參閱第 256 頁的「刪除隔離所中的垃圾郵件」。

您可以從**「狀態」>「已排程工作」**頁面中，檢查已排程工作的狀態。

請參閱第 556 頁的「關於已排程工作」。

指定垃圾郵件隔離所的清除時間與頻率

1 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。

2 按下**「隔離所清除程式頻率」**下拉式清單以指定執行清除程式的頻率。

3 在**「隔離所清除程式開始時間」**下拉式清單中，指定要開始執行清除程式的時間。

4 按下**「儲存」**。

指定要通知誤報郵件的對象

如果使用者或管理員在「垃圾郵件隔離所」中發現誤報郵件，可以按下「釋放」。按下「釋放」會將選取的郵件重新傳送至使用者的一般收件匣中。您也可以自動將副本傳送給本機系統管理員、賽門鐵克或兩者。 這些郵件應傳送給組織中負責監控錯誤識別之郵件的管理員，以確定 Symantec Messaging Gateway 的有效性。

「賽門鐵克安全機制應變中心」會分析郵件提交，以便判斷是否需要變更過濾器。不過，對於錯誤識別的郵件提交，「賽門鐵克安全機制應變中心」不會傳送確認給系統管理員或提交該郵件的使用者。也不保證會依據那些提交郵件而更改過濾器。

附註：賽門鐵克不會將收到可疑垃圾郵件判斷的合法郵件視為誤報，也不會檢閱收到可疑垃圾郵件判斷並提交給賽門鐵克安全機制應變中心的郵件。原因是賽門鐵克無法控制組織架構「可疑垃圾郵件」臨界值的方式。因此，賽門鐵克不會建立過濾器或根據可疑垃圾郵件判斷來修改過濾器。根據設定過低之可疑垃圾郵件臨界值而建立的過濾器，會影響所有賽門鐵克客戶的垃圾郵件效能。

只有具備「完整的管理」權限或「管理設定」修改權限的管理員，才能修改隔離所設定。

請參閱第 256 頁的「從隔離所釋放誤報的郵件」。

指定要通知誤報郵件的對象

1. 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。
2. 若要向賽門鐵克回報錯誤識別的郵件，請在**「錯誤識別的郵件」**下方，按下**「賽門鐵克安全機制應變中心」**。

   預設會選取此選項。
3. 若要傳送錯誤識別的郵件副本給本機管理員，請在**「錯誤識別的郵件」**下方，按下**「管理員」**並輸入正確的電子郵件地址。

   請輸入包括網域名稱在內的完整電子郵件地址，例如 `admin@symantecexample.com`。系統管理員電子郵件地址不可為別名，否則錯誤識別的郵件副本無法傳送到系統管理員電子郵件地址。
4. 按下**「儲存」**。

檢視垃圾郵件隔離所中的郵件

表 12-4 描述了您要檢視「垃圾郵件隔離所」中的郵件時，可執行的工作。您可以視需要以任何順序執行這些工作。

表 12-4 檢視「垃圾郵件隔離所」中的郵件

工作	說明
瞭解使用者的「垃圾郵件隔離所」與管理員的「垃圾郵件隔離所」有何不同。	此主題提供表格說明差異處。 請參閱第 249 頁的「管理員和使用者之垃圾郵件隔離所的差異」。
檢視「垃圾郵件隔離所」中的郵件。	檢視「垃圾郵件隔離所」中的郵件，判斷它們是垃圾郵件或誤報。 請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

工作	說明
檢視傳送至郵件管理員信箱的郵件。	如果「垃圾郵件隔離所」無法判斷所接收郵件的適當收件者，而且您已將它架構為不刪除此類郵件，則它會將該郵件傳送至郵件管理員信箱。郵件管理員信箱可從管理員的「垃圾郵件隔離所」存取。 除了「垃圾郵件隔離所」郵件管理員信箱之外，您的網路中可能還有另一個可使用郵件用戶端存取的郵件管理員信箱。如果 LDAP 組態出現問題，垃圾郵件可能也會傳送至「垃圾郵件隔離所」郵件管理員信箱。 請參閱第 251 頁的「檢視傳送至郵件管理員信箱的垃圾郵件和可疑垃圾郵件」。

管理員和使用者之垃圾郵件隔離所的差異

表 12-5 描述管理員和使用者之「垃圾郵件隔離所」的差異。

表 12-5 管理員與使用者之間的垃圾郵件隔離所差異

頁面	差異
「郵件清單」頁面	「郵件清單」頁面的差異如下： ■ 使用者僅能檢視並刪除自己的已隔離郵件。「隔離所」管理員可以檢視並刪除所有使用者的已隔離郵件，可以逐一刪除、刪除所有郵件，或刪除搜尋結果。 ■ 使用者按下「釋放」之後，該郵件就會傳送至其收件匣。「隔離所」管理員按下「釋放」之後，該郵件就會傳送至每個目標收件者的收件匣中。 ■ 管理員「郵件清單」頁面包括一個「收件者」欄，此欄含有每封郵件的目標收件者。由於使用者僅會看到自己的郵件，因此不需要有「收件者」欄。 ■ 使用者僅能存取「垃圾郵件隔離所」，而無法存取控管中心的其他部分。 **附註：**使用者必須登入控管中心才能存取「垃圾郵件隔離所」。他們使用您 LDAP 伺服器所需的使用者名稱和密碼。
「郵件詳細資料」頁面	使用者僅能檢視並刪除自己的已隔離郵件。「隔離所」管理員可以檢視並刪除所有使用者的郵件。
搜尋過濾器	「隔離所」管理員可以搜尋收件者。 在搜尋結果中，使用者僅能刪除自己的已隔離郵件。「隔離所」管理員則可刪除所有使用者的已隔離郵件。

請參閱第 242 頁的「架構一般使用者隔離所」。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

檢視隔離所中的垃圾郵件與可疑垃圾郵件

檢視「垃圾郵件隔離所」中的郵件，判斷它們是垃圾郵件或誤報。

具有「完整的管理」權限或「管理隔離所」之檢視權限的管理員可以檢視隔離所中的垃圾郵件。但是，這些管理員無法從「垃圾郵件隔離所」釋放郵件或刪除「垃圾郵件隔離所」中的郵件。具有「完整的管理」權限或「管理隔離所」之修改權限的管理員可以檢視、刪除和釋放「垃圾郵件隔離所」中的垃圾郵件。

當您在「郵件清單」頁面按下郵件的主旨行時，郵件的內容會出現在「郵件詳細資料」頁面。完成檢視該垃圾郵件的詳細資料之後，您可以返回「郵件清單」頁面。

請注意下列「郵件詳細資料」頁面行為：

顯示為灰色矩形圖形	郵件中的原始圖形會被灰色矩形圖形取代。這樣做的目的是封鎖攻擊性圖片，並防止垃圾郵件寄發者確認您的電子郵件地址。如果您按下「釋放」釋放郵件，目標收件者將可以檢視原始圖形。在「垃圾郵件隔離所」中，使用者無法檢視原始圖形。
無法檢視附件	附件名稱會列在郵件底端，但無法從「垃圾郵件隔離所」中檢視實際的附件。不過，如果您按下「釋放」重新傳送郵件，則可以在目標收件者的收件匣中存取該郵件及附件。

附註：「郵件清單」頁面中的「收件者」欄表示每封郵件的目標收件者，如郵件信封中所列。考慮此資訊時請特別小心，因為垃圾郵件寄發者經常會偽造此標頭。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

請參閱第 242 頁的「架構一般使用者隔離所」。

請參閱第 249 頁的「管理員和使用者之垃圾郵件隔離所的差異」。

檢視隔離所中的垃圾郵件與可疑垃圾郵件

- 執行下列其中一個步驟：

如果您目前不在「垃圾郵件隔離所」頁面	在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。
如果您目前是在「垃圾郵件隔離所」頁面，而且想要檢視剛送達的郵件	如果未顯示「全部顯示」選項，請按下**「顯示過濾器」**，再按**「全部顯示」**。

檢視垃圾郵件和可疑垃圾郵件的內容

- 按下郵件的主旨行。

  會出現「郵件詳細資料」頁面。

從「郵件詳細資料」頁面返回「郵件清單」頁面

- 若要返回郵件清單，請按下**「回到郵件」**。

檢視傳送至郵件管理員信箱的垃圾郵件和可疑垃圾郵件

除了「垃圾郵件隔離所」郵件管理員信箱之外，您的網路中可能還有另一個可使用郵件用戶端存取的郵件管理員信箱。如果 LDAP 組態出現問題，垃圾郵件可能也會傳送至「垃圾郵件隔離所」郵件管理員信箱。如果您執行 8.0.3 版或更舊版本，而「垃圾郵件隔離所」無法判斷所接收郵件的適當收件者，並且您已將它架構為不刪除此類郵件，則它會將該郵件傳送至可由「垃圾郵件隔離所」進行存取的郵件管理員信箱。

通知郵件不會傳送至郵件管理員信箱。

您必須具有「完整管理」權限或「管理隔離所」之檢視或修改權限，才能檢視郵件管理員信箱中的郵件。

檢視傳送至郵件管理員信箱的垃圾郵件和可疑垃圾郵件

1. 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。
2. 按下**「顯示過濾器」**。
3. 在「收件者」方塊中，鍵入**「郵件管理員」**。
4. 如有需要可指定額外過濾器。
5. 按下**「顯示已過濾」**。

   根據您所使用的 Symantec Messaging Gateway 版本，您應注意下列行為：

8.0.3 或更舊版本	只寄送給未解析的收件者的垃圾郵件顯示什麼樣的內容。
9.0 或更新版本	寄送給已解析 (有效) 和未解析 (無效) 的收件者的垃圾郵件分別顯示什麼樣的內容。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

請參閱第 242 頁的「架構一般使用者隔離所」。

請參閱第 249 頁的「管理員和使用者之垃圾郵件隔離所的差異」。

處理垃圾郵件隔離所中的郵件

表 12-6說明您可對「垃圾郵件隔離所」中的郵件執行的工作。您可以視需要以任何順序執行這些工作。

表 12-6 處理垃圾郵件隔離所中的郵件

工作	說明
自訂郵件清單頁面。	您可以指定郵件清單頁面上一次顯示的項目數。 請參閱第 252 頁的「指定垃圾郵件隔離所之郵件清單頁面上顯示的項目數」。
對垃圾郵件隔離所中的郵件進行排序。	您可以排序「垃圾郵件隔離所」中的郵件，更輕鬆地將郵件分類或尋找特定郵件。預設會以日期順序 (遞減順序) 顯示郵件。最新的郵件會顯示在頁面的最上方。 請參閱第 253 頁的「依日期排序隔離所中的垃圾郵件和可疑郵件」。
在垃圾郵件隔離所中搜尋郵件。	您可以搜尋「垃圾郵件隔離所」中的郵件。搜尋郵件的能力可讓您更輕鬆地找到要檢視或刪除的特定郵件。 請參閱第 253 頁的「搜尋隔離的垃圾郵件」。 請參閱第 254 頁的「垃圾郵件搜尋條件與提示」。
檢視垃圾郵件標頭。	檢視垃圾郵件的標頭可能提供有關郵件來源的線索。但是請記住，垃圾郵件寄發者通常會偽造郵件標頭。 請參閱第 255 頁的「檢視垃圾郵件標頭」。
從垃圾郵件隔離所釋放誤報的郵件。	偶爾您可能會發現「垃圾郵件隔離所」中有非垃圾郵件的郵件。您可以重新傳送這些郵件給目標收件者。 請參閱第 256 頁的「從隔離所釋放誤報的郵件」。
從「垃圾郵件隔離所」刪除垃圾郵件，以釋放磁碟空間。	當您在管理員的「垃圾郵件隔離所」刪除郵件時，也會將該郵件從使用者的「垃圾郵件隔離所」刪除。當您或使用者刪除郵件之後，就無法再存取該郵件。 請參閱第 256 頁的「刪除隔離所中的垃圾郵件」。

指定垃圾郵件隔離所之郵件清單頁面上顯示的項目數

您可以指定郵件清單頁面上一次顯示的項目數。您必須具備「完整管理」權限或「管理隔離所」檢視或修改權限，才能檢視「垃圾郵件隔離所」中的郵件。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

指定垃圾郵件隔離所之郵件清單頁面上顯示的項目數

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 在**「每頁的項目數」**下拉式清單中，按下某個數字。

依日期排序隔離所中的垃圾郵件和可疑郵件

您可以排序「垃圾郵件隔離所」中的郵件，更輕鬆地將郵件分類或尋找特定郵件。預設會以日期順序 (遞減順序) 顯示郵件。最新的郵件會顯示在頁面的最上方。

在日期欄中會出現一個三角形，表示遞增或遞減排序順序。按下欄位標題，即可切換遞增或遞減排序順序。依據預設值，郵件是以日期遞減順序排列，表示最新的郵件會列在頁面最上方。

您必須具備「完整管理」權限或「管理隔離所」檢視或修改權限，才能檢視「垃圾郵件隔離所」中的郵件。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

請參閱第 253 頁的「搜尋隔離的垃圾郵件」。

請參閱第 255 頁的「檢視垃圾郵件標頭」。

依日期排序隔離所中的垃圾郵件和可疑郵件

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 按下**「日期」**欄位標題，依日期排序郵件。

搜尋隔離的垃圾郵件

您可以搜尋「垃圾郵件隔離所」中的郵件。搜尋郵件的能力可讓您更輕鬆地找到要檢視或刪除的特定郵件。您必須具備「完整管理」權限或「管理隔離所」檢視或修改權限，才能檢視「垃圾郵件隔離所」中的郵件。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

請參閱第 253 頁的「依日期排序隔離所中的垃圾郵件和可疑郵件」。

搜尋隔離的垃圾郵件

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 在郵件清單頁面上，按下**「顯示過濾器」**。

3 執行下列任一項操作以進行搜尋：

搜尋郵件信封 To 收件者	在「收件者」方塊中輸入名稱或地址，搜尋郵件信封 RCPT TO: 標頭。 您可以搜尋顯示名稱、電子郵件地址的使用者名稱部分，或顯示名稱或電子郵件使用者名稱的任一部分。若在「收件者」方塊中輸入完整的電子郵件地址，則 Symantec Messaging Gateway 僅會搜尋 user_name@example.com 的使用者名稱部分。該搜尋會限制在信封 To: 中，其中所含資訊可能與郵件詳細資料頁面中所顯示標頭 To: 的資訊不同。您也可以輸入網域，來搜尋電子郵件地址的網域部分。
搜尋 From 標頭	在「寄件者」方塊中輸入名稱或地址，在所有郵件的 From: 標頭中搜尋特定寄件者。 您可以搜尋顯示名稱、電子郵件地址，或顯示名稱或電子郵件地址的任一部分。該搜尋會限制在顯示的郵件 From: 標頭中，在垃圾郵件中該部分通常是偽造的。顯示的郵件 From: 標頭可能含有郵件信封以外的其他資訊。
搜尋郵件 ID 標頭	在「郵件 ID」方塊中輸入內容，以便在所有郵件中搜尋該郵件 ID。 您可以在「垃圾郵件隔離所」中的郵件詳細資料頁面上檢視郵件 ID，只要按下「顯示完整標頭」即可。此外，大部分電子郵件用戶端可以顯示完整郵件標頭，包括郵件 ID。例如，在 Outlook 2000 中，按兩下郵件會另外開啟視窗以顯示郵件，按下**「檢視」**，然後再按下**「選項」**即可。 請參閱第 255 頁的「檢視垃圾郵件標頭」。
搜尋主旨標頭	在「主旨」方塊中輸入內容，以便在所有郵件的 Subject: 標頭中搜尋有關特定主題的郵件。
搜尋時間範圍	從「時間範圍」下拉式清單選取時間範圍，以顯示在該時間範圍內收到的所有郵件。

4 按下**「顯示已過濾」**。

垃圾郵件搜尋條件與提示

搜尋功能已經最佳化，以便搜尋數量龐大的郵件，但是可能會產生非預期的搜尋結果。

請考慮下列提示與資訊，以協助您在「垃圾郵件隔離所」中進行搜尋：

字符	字符會以子字串語義比對。以搜尋目標 <in> 搜尋主旨時，將找出「Lowest rate in 45 years」、「RE: re:Sublime Bulletin (verification)」、「Up to 85% off Ink Cartridges + no shipping!」以及「Re-finance at todays super low rate」。

多字詞搜尋	如果在多字詞搜尋中找到郵件內含有其中任何字，該郵件會視為符合。例如，搜尋 red carpet 時，會找到 red carpet、red wine 與 flying carpet。
區分大小寫	所有文字搜尋都是不分字母大小寫的。例如，假設您在 From 方塊中輸入 emerson。From 標頭中含有 emerson、Emerson 和 eMERSOn 的所有郵件都會出現在搜尋結果中。
完全相同的詞組	若要搜尋完全相同的詞，請在詞的前後加上雙引號 (" ")。
萬用字元	您可以使用 * (星號) 執行萬用字元搜尋。這個字元亦作為邏輯「和」字元使用。
單一字元	即使是單一字元也會視為子字串目標。
特殊字元	您可以使用特殊字元進行搜尋，例如 & (連線符號)、! (驚嘆號)、$ (美元符號)，以及 # (井字號)。
多重特性	如果您搜尋多重特性，則搜尋結果僅會列出同時符合所有特性的郵件。例如，假設您在 From 方塊中輸入 LPQTech，並在「主旨」方塊中輸入 Inkjet。只有在 `From:` 標頭中含有 LPQTech 且在 `Subject:` 標頭中含有 Inkjet 的郵件，才會出現在搜尋結果中。
偽造的標頭資訊	垃圾郵件寄發者通常會「欺騙」或偽造某些顯示的郵件標頭 (例如「寄件者」和「收件者」及看不見的信封資訊)。有時候他們會以實際的電子郵件地址或非相關人士或公司的網域偽造標頭資訊。
執行搜尋的時間	執行搜尋所需的時間，須視您使用的搜尋方塊數量與信箱中的郵件數量而定。在管理員信箱中搜尋會比在使用者信箱中搜尋花更長的時間。

請參閱第 253 頁的「搜尋隔離的垃圾郵件」。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

檢視垃圾郵件標頭

檢視垃圾郵件的標頭可能提供有關郵件來源的線索。但是請記住，垃圾郵件寄發者通常會偽造郵件標頭。您必須具備「完整管理」權限或「管理隔離所」檢視或修改權限，才能檢視「垃圾郵件隔離所」中的郵件。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

請參閱第 256 頁的「從隔離所釋放誤報的郵件」。

請參閱第 253 頁的「依日期排序隔離所中的垃圾郵件和可疑郵件」。

檢視完整的垃圾郵件標頭

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 按下您要檢視之郵件的主旨行。

3 若要顯示「垃圾郵件隔離所」可用的所有標頭，請按下**「顯示完整標頭」**。

檢視簡短的垃圾郵件標頭

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 按下您要檢視之郵件的主旨行。

3 若要僅顯示 `From:`、`To:`、`Subject:` 和 `Date:` 標頭，請按下**「顯示簡短標頭」**。

從隔離所釋放誤報的郵件

偶爾您可能會發現「垃圾郵件隔離所」中有非垃圾郵件的郵件。您可以重新傳送這些郵件給目標收件者。重新傳送郵件時，它也會從「垃圾郵件隔離所」移除該郵件。視您架構「垃圾郵件隔離所」的方式而定，郵件副本可能也會傳送給管理員、賽門鐵克，或兩者都傳送。這個組態可以讓電子郵件管理員或賽門鐵克監控垃圾郵件設定和過濾器的有效性。

請參閱第 247 頁的「指定要通知誤報郵件的對象」。

只有具有「完整的管理」權限或「管理隔離所」之修改權限的管理員可以從隔離所釋放郵件。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 241 頁的「關於瀏覽垃圾郵件隔離所」。

請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。

請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。

請參閱第 256 頁的「刪除隔離所中的垃圾郵件」。

從隔離所郵件清單頁面釋放誤報的郵件

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 按下錯誤識別郵件左方的核取方塊，然後按下**「釋放」**重新傳送該郵件至目標收件者。

從隔離所郵件詳細資料頁面釋放誤報的郵件

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 按下您要檢閱並可能會重新傳送之垃圾郵件的主旨行。

3 在「郵件詳細資料」頁面上，按下**「釋放」**。

刪除隔離所中的垃圾郵件

從「垃圾郵件隔離所」刪除垃圾郵件，以釋放磁碟空間。當您在管理員的「垃圾郵件隔離所」刪除郵件時，也會將該郵件從使用者的「垃圾郵件隔離所」刪除。例如，假設您刪除管理員之

「垃圾郵件隔離所」中的垃圾郵件。郵件的目標收件者將無法在其「垃圾郵件隔離所」中檢視該郵件。

使用者在釋放郵件或刪除郵件時，便會從隔離所移除郵件。當您或使用者刪除郵件之後，就無法再存取該郵件。

請參閱第 256 頁的「從隔離所釋放誤報的郵件」。

您可以從「郵件清單」頁面或「郵件詳細資料」頁面刪除郵件。只有具有「完整的管理」權限或「管理隔離所」之修改權限的管理員可以刪除隔離所中的郵件。使用者不需要特殊的權限，即可刪除自己隔離所中的郵件。

您也可以使用清除程式來自動刪除「垃圾郵件隔離所」中的郵件。清除程式讓您不需要手動刪除「垃圾郵件隔離所」中的郵件，即可釋放空間。清除程式會根據您指定的排程清除郵件。

請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。

從郵件清單頁面刪除個別郵件

1. 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。
2. 按下您要刪除的每一個郵件左邊的核取方塊。
3. 按下**「刪除」**。

從郵件清單頁面刪除所有郵件

1. 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。
2. 按下**「全部刪除」**可刪除「垃圾郵件隔離所」中的所有郵件，包括其他頁面中的郵件。

   此工作會刪除使用者之「垃圾郵件隔離所」中的所有垃圾郵件。使用者在自己的隔離所中不會看到任何郵件。

從郵件詳細資料頁面刪除垃圾郵件

1. 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。
2. 按下您要檢視之郵件的主旨行。
3. 若要刪除您目前正在檢視的郵件，請按下**「刪除」**。

指定通知使用者其隔離所中有垃圾郵件的時間

您可以變更將通知自動傳送給使用者的頻率。預設頻率是每天。若要停用通知郵件，請將「通知頻率」變更為NEVER。

如果您修改通知頻率，請記住頻繁通知的可能影響。如果您有大量的使用者，則每天產生超過一次的通知可能會讓使用者感到過多。頻繁通知可能會影響網路效能。賽門鐵克建議對於較大的部署，通知的產生頻率不應該超過每天一次。

指定通知使用者其隔離所中有垃圾郵件的時間

1 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。

2 在**「通知設定」**下方的**「每個通知的摘要項目數上限」**方塊中，指定摘要通知郵件中包含的項目數。

預設設定是 100。

3 按下**「通知頻率」**下拉式清單並選取您要寄出通知的頻率。

4 按下**「通知開始時間」**下拉式清單並選取您要寄出通知的小時與分鐘。

5 按下**「儲存」**。

針對客戶特定規則，從「垃圾郵件隔離所」提交郵件

您可以將「垃圾郵件隔離所」中的郵件提交到賽門鐵克以供建立客戶特定規則。您必須擁有「完整的管理權限」或「管理垃圾郵件提交」修改權限，才能提交郵件。您也必須具有「管理垃圾郵件隔離所」的檢視或修改權限，才能存取「垃圾郵件隔離所」。

即使停用客戶特定垃圾郵件提交功能，賽門鐵克仍會分析您透過「垃圾郵件隔離所」提交的郵件。它將會考量郵件是否符合全域垃圾郵件規則或全域誤報規則，但是並不會建立自訂規則。

請參閱第 233 頁的「指定誰能夠提交客戶特定規則的郵件」。

若要針對客戶特定規則，從「垃圾郵件隔離所」提交郵件

1 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

2 在**「垃圾郵件隔離所」**頁面上，勾選想要針對自訂規則提交之郵件旁的方塊。

您可以選取多個要提交的郵件。

3 選取下列其中一個選項：

這是垃圾郵件	該郵件為垃圾郵件，且應將其視為垃圾郵件。
這不是垃圾郵件	該郵件為合法郵件，不應被視為垃圾郵件。

4 在確認對話方塊中，視需要按下**「作為垃圾郵件提交」**或**「作為非垃圾郵件提交」**。

如果提交成功，則提交類型將會出現在所選取郵件的**「提交狀態」**欄中。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

架構「垃圾郵件隔離所」通知

表 12-7 描述了可架構以建立「垃圾郵件隔離所」通知的選項。您可以視需要以任何順序執行這些工作。

表 12-7 架構「垃圾郵件隔離所」通知

工作	說明
瞭解垃圾郵件通知郵件。	依據預設，會在每天的上午 4 點執行通知程序。該程序並會判斷自從上次執行通知程序之後，使用者的「垃圾郵件隔離所」中是否有新的垃圾郵件。如果有，則會傳送郵件給有新垃圾郵件的使用者，通知他們檢查「垃圾郵件隔離所」。該程序也會傳送通知摘要至散布清單上的使用者。 請參閱第 259 頁的「關於架構使用者與散布清單通知摘要」。 請參閱第 260 頁的「如何處理寄給散布清單的垃圾郵件」。
指定通知使用者其「垃圾郵件隔離所」中有郵件的頻率。	您可以變更將通知自動傳送給使用者的頻率。預設頻率是每天。 請參閱第 257 頁的「指定通知使用者其隔離所中有垃圾郵件的時間」。
修改垃圾郵件通知範本。	通知摘要範本會決定傳送給使用者的通知郵件外觀，以及郵件主旨與寄件者位址。 請參閱第 261 頁的「修改垃圾郵件通知郵件摘要範本」。 請參閱第 262 頁的「垃圾郵件通知郵件變數」。
指定通知摘要格式。	通知摘要範本會決定要傳送給使用者之通知郵件的 MIME 編碼，也會決定是否要讓「檢視」與「釋放」連結出現在郵件中。 請參閱第 263 頁的「選取通知摘要格式」。

關於架構使用者與散布清單通知摘要

依據預設，會在每天的上午 4 點執行通知程序。該程序並會判斷自從上次執行通知程序之後，使用者的「垃圾郵件隔離所」中是否有新的垃圾郵件。如果有，Symantec Messaging Gateway 會傳送郵件給有新垃圾郵件的使用者，提醒他們檢查「垃圾郵件隔離所」中的垃圾郵件。該程序也會傳送通知摘要至散布清單上的使用者。

附註：如果未架構 LDAP 或已啟用僅供系統管理員存取，則會停用通知郵件和通知設定。

依據預設值，標準已隔離郵件的通知範本與已隔離散布清單郵件的通知範本並不相同。個別範本可讓您自訂每種隔離郵件類型的通知範本。

請參閱第 260 頁的「如何處理寄給散布清單的垃圾郵件」。

請參閱第 257 頁的「指定通知使用者其隔離所中有垃圾郵件的時間」。

如何處理寄給散布清單的垃圾郵件

如果已啟用「垃圾郵件隔離所」，則傳送至別名 (以一對一方式對應使用者電子郵件地址) 的垃圾郵件就會傳送至使用者的一般隔離信箱中。例如，如果 tom 是 `tomevans` 的別名，則所有傳送至 tom 或 `tomevans` 的已隔離郵件都會送至 `tomevans` 的「垃圾郵件隔離所」帳戶。

附註：UNIX 上的「別名」及 Windows 上的「散布清單」都是會轉譯為一或多個其他電子郵件地址的電子郵件地址。在本文中，散布清單指的是轉譯為兩個以上電子郵件地址的電子郵件地址。

對於傳送至目標收件者垃圾郵件隔離所信箱之散布清單的垃圾郵件，Symantec Messaging Gateway 不會將它傳送出去。反之，該郵件會傳送至該散布清單的特殊「垃圾郵件隔離所」信箱中。不過，您可以架構「垃圾郵件隔離所」，將散布清單信箱郵件的通知摘要傳送給該散布清單中的收件者。您可以選取「隔離所設定」頁面上的「通知散布清單」核取方塊，以架構此選項。

附註：當有一個或更多位址解析 DDS 來源，並且啟用**「展開散布清單」**選項時，散布清單展開至個別使用者的清單收件者後，才將郵件傳送到隔離所。在這種情況下，個別使用者接受來自使用者範本 (而非散布清單範本) 的通知。

如果選取了「包括檢視連結」方塊，就會在通知摘要中納入已隔離之散布清單郵件的清單。每個郵件都有「檢視」連結，使用者按下此連結便能檢視「垃圾郵件隔離所」中的該郵件。如果選取「包括釋放連結」方塊，則列在摘要中的每個郵件都會有「釋放」連結。使用者可以按下此連結以釋放該散布清單郵件，而無須存取「垃圾郵件隔離所」。如果任一收件者在已隔離的散布清單信箱中按下郵件的**「釋放」連結**，則該郵件會傳送至散布清單中所有收件者的一般收件匣中。如果通知格式為純文字，則不會顯示「檢視」連結和「釋放」連結。

表 12-8 提供郵件如何繞送至散布清單成員的範例。

表 12-8 散布清單通知與傳送範例

情景	結果
稱為 mktng 的散布清單包含 Ruth、Fareed 與 Darren	傳送至 mktng 並架構為要隔離的垃圾郵件，並不會傳送至 Ruth、Fareed 和 Darren 的「垃圾郵件隔離所」收件匣。
「隔離所設定」頁面上的「通知散布清單」核取方塊已選取	Ruth、Fareed 和 Darren 會收到已隔離 mktng 郵件的電子郵件通知。
「隔離所設定」頁面上的「包括檢視連結」方塊已選取	Ruth、Fareed 和 Darren 可以按下通知摘要中的「檢視」連結，以檢視已隔離的 mktng 郵件。
「包括釋放連結」方塊也已選取	Ruth、Fareed 和 Darren 可以按下通知摘要中的**「釋放」**選項，以重新傳送任何已隔離的 mktng 郵件。

情景	結果
Ruth 為已隔離的 mktng 郵件按下「釋放」選項	郵件會傳送到 Ruth、Fareed 和 Darren 的一般收件匣。

修改垃圾郵件通知郵件摘要範本

通知摘要範本會決定傳送給使用者的通知郵件外觀，以及郵件主旨與寄件者位址。預設的通知範本類似於以下所列的文字。散布清單通知範本沒有如何登入的相關資訊。在您的瀏覽器中，文字不會換行，所以必須水平捲動才能檢視某些字行。如果您選擇以 HTML 格式傳送通知，此配置可防止不正常的斷行或出現額外的行。

```
Spam Quarantine Summary for %USER_NAME%

There are %NEW_MESSAGE_COUNT% new messages in your Spam Quarantine
since you received your last Spam Quarantine Summary. These messages
will automatically be deleted after %QUARANTINE_DAYS% days.

To review the complete text of these messages, go to
%QUARANTINE_URL%
and log in.
====================== NEW QUARANTINE MESSAGES ======================
%NEW_QUARANTINE_MESSAGES%
======================================================================
```

您可以在範本中改變每個變數的位置，或將其移除。只有具備「完整的管理」權限或「管理設定」修改權限的管理員，才能修改隔離所設定。

請參閱第 259 頁的「關於架構使用者與散布清單通知摘要」。

請參閱第 260 頁的「如何處理寄給散布清單的垃圾郵件」。

請參閱第 257 頁的「指定通知使用者其隔離所中有垃圾郵件的時間」。

請參閱第 263 頁的「啟用散布清單的通知摘要」。

請參閱第 263 頁的「選取通知摘要格式」。

修改垃圾郵件通知郵件摘要範本

1. 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。
2. 在**「通知設定」**下，按下「通知範本」旁的**「編輯」**。
3. 在**「編碼」**下拉式清單中，選取通知郵件的字元編碼。

   ISO-8859-1 和 UTF-8 適用於歐洲語系。Windows-31j、EUC-JP 和 ISO-2022-JP 則適用於日文。

4 在**「寄件者:」**方塊中，鍵入要傳送通知摘要的寄件者電子郵件地址。

由於使用者可以回覆您提供的電子郵件地址，請輸入您可以監控使用者有關通知摘要問題的位址。請指定包括網域名稱在內的完整電子郵件地址，例如 `admin@symantecexample.com`

5 在**「主旨」**方塊中，輸入應在通知摘要的 `Subject:` 標頭中顯示的文字，例如「您的可疑垃圾郵件摘要」。

不支援在主旨方塊中使用郵件變數。

對於使用者通知範本與散布清單通知範本，「寄件者:」及「主旨」設定是相同的。

6 視需要編輯使用者通知與散布清單通知。

請參閱第 262 頁的表 12-9。

如果您計劃要以 HTML 格式傳送通知，請勿手動插入分行符號。

7 按下列其中一個圖示：

儲存	儲存並套用您的變更。
預設	刪除目前資訊並以預設值取代。
取消	放棄通知範本的變更並關閉範本編輯視窗。

8 按下「隔離所設定」頁面上的**「儲存」**。

垃圾郵件通知郵件變數

表 12-9 列出垃圾郵件通知郵件變數。

請參閱第 261 頁的「修改垃圾郵件通知郵件摘要範本」。

表 12-9 通知郵件變數

變數	說明
%USER_NAME%	接收通知郵件之使用者的使用者名稱。
%NEW_MESSAGE_COUNT%	自從上次傳送的通知郵件之後，使用者在「垃圾郵件隔離所」中的新郵件數量。
%QUARANTINE_DAYS%	郵件保留在「垃圾郵件隔離所」中的天數。過了該期限，郵件將會被清除。
%QUARANTINE_URL%	使用者按下這個 URL 即會顯示「垃圾郵件隔離所」登入頁面。

變數	說明
%NEW_QUARANTINE_MESSAGES%	自從上次傳送的通知之後，使用者在「垃圾郵件隔離所」中的郵件清單。 對於每一封郵件，將列印 From:、Subject: 和 Date: 標頭的內容。若已啟用「檢視」及「釋放」連結，且已選擇多重格式或 HTML 通知格式，則每一個郵件皆會顯示「檢視」及「釋放」連結。

啟用散布清單的通知摘要

您可以架構「垃圾郵件隔離所」將散布清單信箱郵件中的通知摘要傳送到散布清單中的收件者。只有具備「完整的管理」權限或「管理設定」修改權限的管理員，才能修改隔離所設定。

請參閱第 259 頁的「關於架構使用者與散布清單通知摘要」。

請參閱第 260 頁的「如何處理寄給散布清單的垃圾郵件」。

請參閱第 257 頁的「指定通知使用者其隔離所中有垃圾郵件的時間」。

請參閱第 261 頁的「修改垃圾郵件通知郵件摘要範本」。

請參閱第 263 頁的「選取通知摘要格式」。

啟用散布清單的通知摘要

1. 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。
2. 在**「通知設定」**下，勾選**「通知散布清單」**。
3. 按下**「儲存」**。

選取通知摘要格式

通知摘要範本會決定要傳送給使用者之通知郵件的 MIME 編碼， 也會決定是否要讓**「檢視」**與**「釋放」**連結出現在郵件中。

「檢視」與「釋放」連結的詳細資料如下：

檢視
: 當使用者按下通知摘要郵件中的「檢視」連結時，選取的郵件會以預設瀏覽器顯示在「垃圾郵件隔離所」中。選擇「多重格式(HTML和文字)」或「僅HTML」通知格式時，才能使用此核取方塊。如果移除通知摘要範本中的 %NEW_QUARANTINE_MESSAGES% 變數，則新郵件摘要 (包括「檢視」連結) 將無法使用。

釋放
: **「釋放」**連結是用於錯誤識別郵件。當使用者按下通知摘要郵件中的**「釋放」**連結時，相鄰的郵件會從「垃圾郵件隔離所」中釋放，並傳送至使用者的一般收件匣。選擇「多重格式 (HTML 和文字)」或「僅 HTML」通知格式時，才能使用此核取方塊。如果移除通知摘要範本中的 %NEW_QUARANTINE_MESSAGES% 變數，則新郵件摘要 (包括**「釋放」**連結) 將無法使用。

請參閱第 259 頁的「關於架構使用者與散布清單通知摘要」。

請參閱第 260 頁的「如何處理寄給散布清單的垃圾郵件」。

請參閱第 257 頁的「指定通知使用者其隔離所中有垃圾郵件的時間」。

請參閱第 261 頁的「修改垃圾郵件通知郵件摘要範本」。

請參閱第 263 頁的「啟用散布清單的通知摘要」。

只有具備「完整的管理」權限或「管理設定」修改權限的管理員，才能修改隔離所設定。

選取通知摘要格式

1 在控管中心內，按下**「垃圾郵件」>「設定」>「隔離所設定」**。

2 在**「通知設定」**下，按下列**「通知格式」**下拉式清單中的其中一個項目：

多重格式 (HTML 和文字)	以 MIME 多重格式傳送通知郵件。視使用者所使用的電子郵件用戶端類型及其設定而定，使用者會看到 HTML 版本或文字版本。在文字版摘要郵件中，每個郵件旁邊不會出現「檢視」及「釋放」連結。
僅 HTML	僅以 MIME 類型的文字/HTML 格式傳送通知郵件。
僅文字	僅以 MIME 類型的文字/純文字格式傳送通知郵件。如果選擇「僅文字」，則摘要郵件中的每一則郵件旁邊都不會出現「檢視」與「釋放」連結。

3 若要在通知摘要的郵件摘要中的每一則郵件旁邊包含**「檢視」**連結，請勾選**「包括檢視連結」**方塊。

4 若要在通知摘要的郵件摘要中的每一則郵件旁邊包含**「釋放」**連結，請勾選**「包括釋放連結」**方塊。

5 按下**「儲存」**。

垃圾郵件隔離所疑難排解

表 12-10 列出垃圾郵件隔離所可能會發生的一些問題。

表 12-10 垃圾郵件隔離所的問題

問題	說明/解決方案
日誌檔中的錯誤「error.mail.transport.connect= 無法釋放郵件，無法連線到任何可用的 MTA 服務」	在**「管理」>「主機」>「組態」>「新增/編輯」>SMTP** 標籤中，如果沒有指定入埠和離埠郵件設定的控管中心 IP 位址，則可能發生此錯誤。 請參閱第 39 頁的「關於掃描程式電子郵件設定」。

問題	說明/解決方案
使用者在其「垃圾郵件隔離所」中未看見散布清單郵件	對於傳送到散布清單的垃圾郵件，掃描程式不會傳送到目標收件者的「隔離所」信箱。反之，該郵件會傳送至該散布清單的特殊「垃圾郵件隔離所」信箱中。 請參閱第 260 頁的「如何處理寄給散布清單的垃圾郵件」。
無法傳送的已隔離郵件移至垃圾郵件隔離所郵件管理員信箱	對於 Symantec Messaging Gateway 接收的郵件，如果「垃圾郵件隔離所」無法確定適當的收件者，會將該郵件傳送至可從「垃圾郵件隔離所」進行存取的郵件管理員信箱。或者，您可以在「隔離所設定」頁面指定「刪除已傳送至未解析電子郵件地址的郵件」。除了垃圾郵件隔離所郵件管理員信箱以外，您的網路中可能還有另一個可使用郵件用戶端存取的郵件管理員信箱。不過，如果 LDAP 伺服器失敗或架構不正確，系統就會將送往 LDAP 無法辨識之位址的垃圾郵件，保留在掃描程式的延遲佇列中 (直到達到重試傳送或逾時的次數上限)，而非「垃圾郵件隔離所」的郵件管理員信箱中。 **附註：**通知郵件不會傳送至郵件管理員信箱。 請參閱第 251 頁的「檢視傳送至郵件管理員信箱的垃圾郵件和可疑垃圾郵件」。
使用者收到通知郵件，但無法存取郵件	如果無法存取其郵件的使用者與可以存取其郵件的使用者位於不同的 Active Directory 網域，請在控管中心內架構目錄整合以使用通用類別目錄。此外，請確保您有每個作用中目錄網域的目錄資料來源。 若要架構存取 Active Directory 通用類別目錄，請在**「管理」>「設定」>「LDAP/編輯」**頁面中，指定通用類別目錄的通訊埠，通常為 3268。 請參閱第 426 頁的「建立資料來源」。
複製「垃圾郵件隔離所」中出現的郵件	當您以管理員身分登入「垃圾郵件隔離所」時，可能會發現同一則郵件的多個副本。當您讀取其中一則郵件時，其他的郵件都會標示為已讀取。這樣的行為是有其含意的。若將一則郵件寄給貴公司的多位使用者，則「垃圾郵件隔離所」會在其資料庫中儲存一份該郵件的副本，但是每個使用者的郵件狀態 (已讀取、已刪除等) 則會依照每位使用者加以儲存。因為管理員可以檢視所有使用者的郵件，所以管理員會看到每位使用者的郵件副本。如果管理員按下「釋放」，則該郵件的副本會再次傳送至每個相關使用者的信箱。
「垃圾郵件隔離所」中的郵件數量上限	加總訊息存放區的每個訊息檔案的區塊大小 (磁碟上的大小) 來計算隔離所總大小。請注意，實際磁碟使用量將更高，因為其他資料庫表格與索引等未計算的磁碟使用量。 請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。

問題	說明/解決方案
顯示「無法釋放郵件」訊息	如果您的入埠或離埠郵件流出現問題，便可能出現此訊息。這發生在郵件無法傳送至任何已架構的非本機轉遞 (預設)，或無法傳送至在**「管理」> 「控管中心」> SMTP** 頁面架構的 SMTP 主機時。如果未在控管中心所在的硬體裝置上安裝掃描程式，且未替含有 MTA 的主機設定 SMTP 主機設定，也可能會出現此訊息。這會造成從垃圾郵件隔離所釋放郵件的傳送問題。 請參閱第 595 頁的「架構警示和報告的控管中心 SMTP 設定」。
隔離垃圾郵件與可疑垃圾郵件所花費的時間比預期的時間還要久	此問題可能是因為 LDAP 伺服器存取速度緩慢所造成。 請嘗試下列工作： ■ 如果將 Active Directory 的 LDAP 伺服器架構為通用類別伺服器，請確定您使用的是通訊埠 3268，而不是 389。 請參閱第 426 頁的「建立資料來源」。 ■ 檢查基底 DN 查詢。更精確的 DN 查詢傳回速度會快於一般查詢的速度。例如，ou=quarantine-test,dc=brightmail,dc=com 的查詢比 dc=brightmail,dc=com 更精確。
當管理員按下一封垃圾郵件時，有多封郵件標示為「已讀取」。	當將同一封郵件傳送給不同收件者時會發生這種情況。管理員存取郵件的一個執行個體時，該郵件的所有實例 (無論哪一個收件者) 標示為已讀取。 發生這個情況的原因是因為管理員讀取旗標與郵件本身相關聯。 這個情況不會發生在一般使用者垃圾郵件隔離所。該讀取旗標與每個郵件/收件者組合相關聯。

大型部署的垃圾郵件隔離所最佳實務準則

如果貴組織的部署包括 1,000 位或以上的使用者，請考量使用以下最佳實務準則，來增強垃圾郵件隔離所的效果：

- 隔離所不應執行於與掃描程式所在相同的環境。
  請參閱第 40 頁的「架構郵件流方向」。
- 隔離所清除程式應設為每天執行不超過一次。還應該將清除程式排在離峰時間執行。
  請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。
- 對於 5,000 位或以上使用者的部署，請同時考量以下建議：
  - 停用針對每個使用者的限制 (例如，每個使用者的郵件數量上限)。
    請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。
  - 垃圾郵件隔離所摘要通知可能需要很長的執行時間，因此請將其排為以較低的頻繁度執行。通知程序會影響是否可使用控管中心來接受傳送佇列中的郵件。
    請參閱第 257 頁的「指定通知使用者其隔離所中有垃圾郵件的時間」。

請參閱第 264 頁的「垃圾郵件隔離所疑難排解」。

13

參與 Symantec Probe Network

本章包含以下主題：

- 關於 Symantec Probe Network
- 關於探查帳戶
- 關於建立探查帳戶
- 設定探查帳戶

關於 Symantec Probe Network

「探查網路」是賽門鐵克致力於打擊垃圾郵件的重要關鍵。在垃圾郵件寄發者尋找新方法來略過過濾的同時，Symantec Probe Network 會透過使用探查帳戶來監控濫發垃圾郵件的方法，協助賽門鐵克防範垃圾郵件於未然。

以下原因可說明此探查網路十分有效：

能夠及早偵測垃圾郵件攻擊	探查帳戶是即時偵測及分析垃圾郵件的首要步驟。基本上，探查網路的結構會將 Internet 上正在散播中的即時垃圾郵件串流，提供給賽門鐵克安全機制應變中心。這個由散佈在 Internet 上的多個帳戶組成的虛擬網路，讓賽門鐵克能夠輕鬆地驗證特定郵件是否使用大量郵件的方法傳送。
加速開發精確的過濾器	Symantec Messaging Gateway 獨步市場的關鍵，在於其垃圾郵件過濾技術的精確率近乎完美。防垃圾郵件的功能絕大部分取決於依據實際垃圾郵件所建立的核心過濾器。探查網路也提供重要資料，讓賽門鐵克得以用來開發出更具前瞻性的過濾，例如啟發式技術。而其成敗關鍵，就是即時從探查網路流動到賽門鐵克安全機制應變中心之資料的容量、品質和時效性。

協助持續進行趨勢研究	垃圾郵件寄發者會不停改變策略及散播方法，以避開過濾軟體。賽門鐵克的「客戶應變中心」及「防垃圾郵件系統」團隊會從探查網路中挖掘資料，來提升賽門鐵克的防垃圾郵件技術。例如，能夠始終領先最新的垃圾郵件趨勢、評估在不同產品版本之間擷取垃圾郵件的差異，以及監控不同語言的偵測率。

請參閱第 269 頁的「關於探查帳戶」。

請參閱第 272 頁的「啟用探查參與」。

關於探查帳戶

Symantec Messaging Gateway 可讓您選擇將無效的收件者電子郵件地址轉換為可用於 Symantec Probe Network 的探查帳戶。探查帳戶可協助賽門鐵克追蹤垃圾郵件，並從中獲取相關資訊。賽門鐵克從探查帳戶獲取的情報，可用來持續改善管理垃圾郵件過濾器的規則。過濾器越嚴密表示能侵入網路的垃圾郵件越少。

請參閱第 268 頁的「關於 Symantec Probe Network」。

「垃圾郵件」>「設定」>「探查帳戶」頁面上提供了建立探查帳戶的工具。

請參閱第 272 頁的「啟用探查參與」。

請參閱第 270 頁的「設定探查帳戶」。

請參閱第 272 頁的「從無效收件者電子郵件地址建立探查帳戶」。

請參閱第 273 頁的「手動建立探查帳戶」。

請參閱第 274 頁的「啟用探查帳戶」。

請參閱第 274 頁的「停用探查帳戶」。

請參閱第 275 頁的「刪除探查帳戶」。

您可以透過檢視最常見探查帳戶的追蹤報告，來追蹤探查帳戶的有效性。

請參閱第 498 頁的「報告類型」。

關於建立探查帳戶

建立探查帳戶時，您可能想知道哪些電子郵件地址是最佳的探查帳戶。您可以選取任意多個無效收件者電子郵件地址。您也可以建立任意數量的無效或未使用的電子郵件地址，以用於探查網路。

不過，上載電子郵件地址以作為探查帳戶使用時，請務必考慮下列指導方針：

無效收件者

您應該選取會收到最大量電子郵件的無效收件者地址，或是您認為會收到高比例垃圾郵件的無效收件者地址。 您不應該選取離職員工的地址或公用地址 (例如 support@symantecexample.com) 的常見拼錯形式等無效收件者地址， 這些地址收到的大部分電子郵件可能都是有效的。

若要查看最常見的無效收件者，請使用**「報告」**功能來檢視「無效收件者」報告。

請參閱第 493 頁的「選取要為報告追蹤的資料」。

請參閱第 498 頁的「報告類型」。

請參閱第 272 頁的「從無效收件者電子郵件地址建立探查帳戶」。

手動輸入地址

使用此方法可新增您認為只會收到垃圾郵件內容的其他地址。這可能包括您在 Internet 上取得且預期只會收到垃圾郵件的電子郵件地址。 植入是指刻意在 Internet 上發佈電子郵件地址，以讓垃圾郵件寄發者搜尋並鎖定這些地址。

請參閱第 273 頁的「手動建立探查帳戶」。

控管中心最多可儲存 5000 個探查帳戶。

在某些狀況下，您可能會採用**「別名」**位址。探查帳戶一律覆寫別名。

在建立探查帳戶與別名位址時，請記住以下幾點：

- 如果您為已有別名的地址建立探查帳戶，則探查功能會覆寫該別名。
- 您無法為已經是探查帳戶的地址建立別名。

在某些狀況下，您可能會採用**「偽裝」**位址。偽裝帳戶會覆寫探查帳戶。

例如，您使用報告發現 jay@symantecexample.com 是最常見的無效收件者， 則讓 jay@symantecexample.com 成為探查地址。

日後，公司將名稱從 symantecexample 更改為 symantecdomain 時，所有的電子郵件地址皆變更為 @symantecdomain.com。

使用位址偽裝將網域 symantecexample 偽裝成 symantecdomain，讓寄到 ×××@symantecexample.com 的郵件會寄到新的 ×××@symantecdomain.com 地址。如此一來，會讓 jay@symantecexample.com 探查帳戶無效。所有寄到該地址的郵件看起來是寄到 jay@symantecdomain.com，而這不是探查地址。

請參閱第 81 頁的「新增或編輯位址偽裝 」。

設定探查帳戶

下表說明建立探查帳戶然後將其新增至 Symantec Probe Network 的步驟。

表 13-1 建立探查帳戶

步驟	動作	說明
步驟 1	啟用探查參與。	您必須先啟用探查參與，才能啟用探查帳戶。 請參閱第 272 頁的「啟用探查參與」。
步驟 2	確認網域並啟用收件者驗證。	探查帳戶網域必須與您的其中一個本機網域相符。 確認有相符的網域，且已啟用該網域的收件者驗證。如果沒有相符的網域，您可以使用「新增網域」工作來新增一個。 請參閱第 71 頁的「新增或編輯網域」。
步驟 3	指定無效收件者處理。	您必須在要用於探查帳戶的網域上架構無效收件者處理。 您可以選擇下列三種處理選項之一：接受、拒絕或棄置；您必須選擇一種。 請參閱第 86 頁的「設定無效的收件者處理」。
步驟 4	新增資料來源 (選用) 並啟用收件者驗證。 **附註：**如果您只打算使用手動方法建立探查帳戶，則可略過此步驟。	只有在您想要上載目錄資料服務過濾所擷取的無效收件者電子郵件地址時，才需要已啟用目錄資料來源的收件者驗證。 請參閱第 474 頁的「啟用或編輯收件者驗證功能」。 如果目前尚未有任何的目錄資料來源，則需要建立一個，並啟用收件者驗證。 請參閱第 426 頁的「新增資料來源」。
步驟 5	啟用報告。	若要追蹤最常見的無效收件者及最常見的探查帳戶，請啟用「無效收件者」報告。 請參閱第 493 頁的「選取要為報告追蹤的資料」。 請參閱第 495 頁的「建立、儲存、以電子郵件傳送和列印報告」。
步驟 6	建立探查帳戶。	探查功能提供兩種建立探查帳戶的方法。 您可以輸入電子郵件地址，或從檔案上載電子郵件地址，以手動建立探查帳戶。 此外，您也可以使用無效收件者方法來建立探查帳戶。 請參閱第 273 頁的「手動建立探查帳戶」。 請參閱第 272 頁的「從無效收件者電子郵件地址建立探查帳戶」。
步驟 7	啟用或停用一或多個探查帳戶。	雖然探查帳戶預設為啟用，但是您可能會想要暫時停用某個探查帳戶，並於稍後再次啟用。 請參閱第 274 頁的「啟用探查帳戶」。 請參閱第 274 頁的「停用探查帳戶」。

啟用探查參與

您必須先啟用探查參與，才能新增電子郵件地址以用於 Symantec Probe Network。 啟用探查參與之後，探查帳戶政策群組即會自動建立並新增到您的政策群組清單中。 如果您已有名為「探查帳戶」的政策群組，當啟用探查參與時，您現有的「探查帳戶」政策群組會重新命名為「探查帳戶 <*n*> 的備份」。(如果 Symantec Messaging Gateway 必須重新命名多個現有的探查帳戶政策群組，它會在群組名稱中使用連續的數字編號 <*n*>。)

當您停用探查參與時，會自動刪除探查帳戶政策群組。

啟用探查參與

1 在控管中心內，按下**「垃圾郵件」>「設定」>「探查帳戶」**。

2 在**「探查電子郵件地址」**下，按下**「啟用探查參與」**。

啟用探查參與之後，您就可以選取要啟用或停用的個別探查帳戶。

請參閱第 274 頁的「啟用探查帳戶」。

從無效收件者電子郵件地址建立探查帳戶

您必須先設定幾個次要的系統組態，才能完成此工作。

請參閱第 270 頁的「設定探查帳戶」。

如需如何判斷哪些帳戶是良好探查帳戶的相關協助，請參閱探查帳戶建立指南。

請參閱第 269 頁的「關於建立探查帳戶」。

建立探查帳戶後，您可以執行**「最常見的探查帳戶」**報告，以在**「報告」**標籤上追蹤其有效性。

請參閱第 495 頁的「建立、儲存、以電子郵件傳送和列印報告」。

附註：若要檢視**「最常見的探查帳戶」**報告，您必須先啟用**「管理」>「設定」>「報告」**頁面上的**「無效收件者」**設定。

請參閱第 493 頁的「選取要為報告追蹤的資料」。

附註：控管中心最多可儲存 5000 個探查帳戶。

從無效收件者電子郵件地址建立探查帳戶

1 在控管中心內，按下**「垃圾郵件」>「設定」>「探查帳戶」**。

2 如果尚未勾選**「啟用探查參與」**，請加以勾選。

3 在「**新增探查地址**」下按「**無效收件者**」。

請確定您已架構系統，以追蹤無效的收件者資料，否則會顯示錯誤訊息。

請參閱第 493 頁的「選取要為報告追蹤的資料」。

4 按「**時間範圍**」下拉式清單，選取時間範圍，然後再按「**檢視**」。

在「**無效收件者**」地址表中，使用下拉式功能表來指定每頁要列出的「**項目**」(電子郵件地址) 數量，以及要「**顯示**」哪些項目。您可以選擇 1-10 來查看前 10 個無效收件者帳戶，或選擇 10-20 來查看下 10 個帳戶。使用方向鍵可快速瀏覽結果。

5 勾選要設為探查帳戶之每個地址旁的方塊，然後按下「**將選取的項目新增到探查**」。按下「**全部新增到探查**」可將所有地址新增到 Symantec Probe Network。

這會讓您返回最初的探查帳戶頁面，該頁面上會顯示「**電子郵件地址**」表中已選取且狀態為「**已啟用**」的地址。

手動建立探查帳戶

您必須先設定幾個次要的系統組態，才能完成此工作。

請參閱第 270 頁的「設定探查帳戶」。

如需如何判斷哪些帳戶是良好探查帳戶的相關協助，請參閱探查帳戶建立指南。

請參閱第 269 頁的「關於建立探查帳戶」。

建立探查帳戶後，您可以執行「**最常見的探查帳戶**」報告，以在「**報告**」標籤上追蹤其有效性。

請參閱第 495 頁的「建立、儲存、以電子郵件傳送和列印報告」。

附註：若要檢視「最常見的探查帳戶」報告，您必須先啟用「**管理**」>「**設定**」>「**報告**」頁面上的「**無效收件者**」設定。

請參閱第 493 頁的「選取要為報告追蹤的資料」。

手動建立探查帳戶

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**探查帳戶**」。

2 如果尚未勾選「**啟用探查參與**」方塊，請加以勾選。

3 在「**手動新增探查電子郵件地址**」欄位中，輸入一或多個電子郵件地址 (以逗號隔開) 以新增至探查網路。

或者，也可以按「**瀏覽**」，從外部文字檔案中新增電子郵件地址。開啟「**瀏覽**」視窗後，選取含有想要新增為探查帳戶之電子郵件地址的檔案，然後按「**上載**」。

自文字檔案上載之電子郵件地址的格式必須正確。 每行套用一個電子郵件地址 (沒有逗號)。

控管中心最多可儲存 5000 個探查帳戶。

4 按下「**新增**」。

重新整理畫面時，「**電子郵件地址**」表中會顯示這些探查帳戶，且狀態為「已啟用」。

啟用探查帳戶

建立探查帳戶後，預設會將其啟用。 某些情況下，您可能想要暫時停用某探查帳戶。 當準備重新啟用該帳戶時，您可以使用「**啟用**」選項。

啟用個別探查帳戶前，請確保已勾選「**垃圾郵件**」>「**設定**」>「**探查帳戶**」頁面頂端的「**啟用探查參與**」核取方塊。如果未勾選此方塊，則它會個別覆寫已啟用的探查帳戶，使這些帳戶處於非作用中狀態。

請參閱第 272 頁的「啟用探查參與」。

啟用探查帳戶

1 在控管中心內，按下「**垃圾郵件**」>「**設定**」>「**探查帳戶**」。

2 從探查帳戶清單中，勾選要啟用的每個探查帳戶。

您也可以勾選最上方的方塊來選取頁面上列出的所有帳戶。

透過按下依英文字母順序排列帳戶的欄標題「**電子郵件地址**」，可以對探查帳戶清單進行排序。若要依狀態對探查地址進行排序，請按下「**已啟用**」表格標題。

3 按下「**啟用**」。

所選探查帳戶現在於 Symantec Probe Network 中處於作用中狀態。

停用探查帳戶

想要暫時停用 Symantec Probe Network 中的探查帳戶時，請使用「**停用**」選項。

附註：若要永久移除探查帳戶，請使用「**刪除**」選項。

請參閱第 275 頁的「刪除探查帳戶」。

停用探查帳戶

1 在控管中心內，按下**「垃圾郵件」>「設定」>「探查帳戶」**。

2 在**「電子郵件地址」**表中，勾選要停用之每個探查帳戶，或按最上方的方塊來選取頁面上列出的所有帳戶。

3 按下**「停用」**。

停用的帳戶不再處於作用中狀態，但該帳戶仍會保留在 Symantec Probe Network 中，並可重新啟用。

刪除探查帳戶

如果您不再需要 Symantec Probe Network 中的某個探查帳戶，則可以使用**「刪除」**選項將其從網路中永久移除。

附註：如果想要儲存某個探查帳戶，但要將其從 Symantec Probe Network 中暫時移除，請使用**「停用」**選項。

請參閱第 274 頁的「停用探查帳戶」。

刪除探查帳戶

1 在控管中心內，按下**「垃圾郵件」>「設定」>「探查帳戶」**。

2 在**「電子郵件地址」**表中，勾選要刪除之每個探查帳戶旁的核取方塊。您也可以勾選最上方的方塊來選取頁面上列出的所有帳戶。

3 按**「刪除」**或**「全部刪除」**。

刪除的帳戶會從 Symantec Probe Network 中移除，並且不會再出現在探查帳戶清單中。

14

過濾內容

本章包含以下主題：

- 關於內容過濾
- 檢視、編輯、新增和管理內容過濾政策
- 建立內容過濾政策
- 定義內容過濾政策的條件
- 將動作新增至內容過濾政策
- 套用內容過濾政策至政策群組
- 測試內容過濾政策的提示
- 管理套用多個內容過濾政策的方式
- 郵件稽核日誌如何協助微調及疑難排解內容過濾政策

關於內容過濾

內容過濾政策可確定 Symantec Messaging Gateway 對於電子郵件訊息 (包括其內容、附件和屬性) 的評估方式。Symantec Messaging Gateway 會針對您設定的特定條件掃描郵件內容。當郵件符合政策條件，且寄件者或收件者屬於指派有政策的群組的一部分時，政策會觸發判斷。然後，Symantec Messaging Gateway 會套用政策動作。

例如，您可以使用內容過濾政策：

- 限制電子郵件使用者傳達或進行有違貴組織價值觀與政策之活動的能力。
- 防止機密或敏感的資訊自貴組織流出。
- 如果您的組織包含上述其中一個系統，請將點擊 URL 要求傳送至 Symantec Email Threat Isolation 或 Symantec Blue Coat ProxySG。
- 將郵件繞送至替代郵件伺服器以進行流量控制或特殊處理。

- 將郵件複本傳送至封存伺服器，以將其保留供日後參考。
- 如果您的組織包含該系統，請隔離並矯正 Data Loss Prevention 使用其回應規則所偵測到的郵件。

安裝 Symantec Messaging Gateway 之後，**「內容」>「政策」>「電子郵件」>「電子郵件內容過濾政策」**頁面會顯示預設政策的清單。這些政策已啟用。您可以立即將其指派給您的政策群組，也可以自訂條件和動作以符合您組織的需求。

從**「電子郵件內容過濾政策」**頁面，可建立、編輯、複製、刪除和管理內容過濾政策的優先順序。

檢視、編輯、新增和管理內容過濾政策

「內容」>「政策」>「電子郵件」>「電子郵件內容過濾政策」頁面會列出所有內容過濾政策。Symantec Messaging Gateway 會按照出現於此頁面上的順序評估內容過濾政策。先評估清單頂端的政策。最後評估清單底端的政策。

- 若要新增政策，請按下**「新增」**。
  請參閱第 278 頁的「建立內容過濾政策」。
- 若要變更現有政策，請選取政策，然後按下**「編輯」**或按下政策名稱。**「編輯電子郵件內容過濾政策」**頁面與**「新增電子郵件內容過濾政策」**頁面具有相同的控件。
- 若要複製政策，請選取政策，然後按下**「複製」**。例如，您可以複製類似政策，而不是從頭建立新的內容過濾政策。然後，您可以編輯複本以建立新政策。
- 若要刪除政策，請選取政策，然後按下**「刪除」**。
- 若要啟用政策，請選取政策，然後按下**「啟用」**。
  如果政策具有 **?** 狀態，您必須新增遺失的資源，然後才能啟用政策。
- 若要停用政策，請選取政策，然後按下**「停用」**。
- 若要變更政策的優先順序，請將其拖曳到清單中的新位置。
  請注意**「後續政策動作」**欄中的設定。新位置會影響目前位於清單底端的政策。例如，假設您將具有略過動作的政策從清單底端移動到清單頂端。當此政策觸發判斷時，SMG 不會再評估任何其他內容過濾政策。

「電子郵件內容過濾政策」頁面還會針對每個政策提供下列資訊。

表 14-1 電子郵件內容過濾政策詳細資料

資料欄	說明
已啟用	顯示以下其中一個狀態： ✓ 政策已啟用。 — 政策已停用。 ? 政策已停用，因為它需要資源。例如，如果此政策使用辭典且該辭典為空白，您會看到問號。如果您將單字新增至辭典，政策狀態會變更為已停用。然後，可以將其啟用 (如果需要)。 在掃描期間，SMG 僅評估已啟用的政策。
套用至	顯示使用政策來掃描入埠郵件、離埠郵件，還是同時掃描入埠郵件和離埠郵件。 ■ **入埠** - 政策僅套用至指派有政策之政策群組中的收件者。 ■ **離埠** - 政策僅套用至指派有政策之政策群組中的寄件者。 ■ **入埠和離埠** - 政策僅套用至指派有政策之政策群組中的寄件者和收件者。
群組數量	顯示指派有政策的群組數量。
後續政策動作	顯示當政策觸發判斷時，位於清單底端的政策會發生什麼情況。政策的**「後續內容過濾處理」**設定可控制此行為。 ■ **所有非衝突項目**：SMG 會評估位於清單底端的內容過濾政策。當下一個政策觸發判斷時，SMG 會新增所有政策動作。SMG 會在所有過濾完成後套用這些動作，除非它們與優先順序較高的動作發生衝突。 請參閱第 720 頁的「來自多個判斷的動作組合」。 政策的**「後續內容過濾處理」**設定為**「繼續進行評估和動作」**。 ■ **略過**：SMG 會在此政策觸發判斷時停止評估內容過濾政策。將略過位於清單底端的所有政策。 政策的**「後續內容過濾處理」**設定為**「中斷評估和動作」**。 ■ **僅事件和通知**：當下一個政策觸發判斷時，SMG 會繼續評估郵件，但略過除事件動作和通知動作以外的所有政策動作。 政策的**「後續內容過濾處理」**設定為**「僅提供事件和通知動作」**。 請參閱第 298 頁的「管理套用多個內容過濾政策的方式」。

建立內容過濾政策

內容過濾政策條件和動作通常使用註釋、通知、附件清單和辭典等資源。可從**「內容」>「資源」**功能表設定這些資源。在您開始建立內容過濾政策之前，請確定您具備所需的資源。如果沒有提前設定資源，您必須在未完成狀態下儲存您的政策。然後，您可以設定資源並編輯政策，以將其新增。

建立內容過濾政策

1 在控管中心內，選取「**內容**」>「**政策**」>「**電子郵件**」。

2 在「**電子郵件內容過濾政策**」頁面上，按下「**新增**」。

3 選取範本，然後按下「**選取**」。

- 預設「**空白**」範本沒有預先進行程式設計的條件或動作。
- 「**描述性內容**」範本會從「**內容**」>「**資源**」功能表使用現有的資源。例如，「信用卡」範本會在「**信用卡號碼關鍵字**」辭典和「**信用卡**」樣式中搜尋單字。
- 「**結構化資料**」範本包含需要「**記錄**」資源中的自訂資料的條件。這些條件以紅色顯示「**未定義**」。您必須設定「**記錄**」資源，然後編輯新增資源的條件，才能使用「**結構化資料**」範本。
  請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

4 在「**新增內容過濾政策**」頁面上，輸入政策的名稱。名稱必須是唯一的，且應說明政策的用途。

5 如果您想要檢視關於此政策違規的報告，請確定「**在控制面板和報告中追蹤此政策的違規**」已啟用。如果您停用此選項，可以在郵件稽核日誌中檢視政策活動，而不是在控制面板或報告中。

例如，您可能想要啟用此選項，以針對傳送可執行檔附件追蹤政策的違規。您可能想要針對將隱私權註釋新增到每個外寄郵件的政策停用此選項。

6 您可以使用「**啟用或停用清單中檔案的分解**」選項，以限制掃描哪些附件。如果取消勾選此選項 (此為預設設定)，Symantec Messaging Gateway 會分解和掃描所有附件。

- 若要僅掃描清單中的附件類型，請勾選此選項，並選取「**啟用**」。然後，從下拉式功能表中選取附件清單。
- 若要掃描除所選清單中的附件類型以外的所有附件類型，請勾選此選項，然後選取「**停用**」。然後，從下拉式功能表中選取附件清單。

附註：如果您停用附件類型，SMG 將不會掃描內嵌於這些附件的檔案。例如，如果您停用採用 Word 格式的附件，SMG 不會偵測到內嵌於 Word 檔案的 Excel 檔案。

您可以從「**內容**」>「**資源**」>「**附件清單**」頁面，建立其他附件清單。建立附件清單後，清單名稱會顯示在下拉式功能表中。

7 選取「**後續內容過濾處理**」設定。此設定會影響觸發判斷的下一個內容過濾政策。

請參閱第 298 頁的「管理套用多個內容過濾政策的方式」。

8 在「**條件**」面板中，選取將政策套用至「**入埠郵件**」、「**離埠郵件**」或「**入埠和離埠郵件**」，然後選取內容過濾條件。

請參閱第 280 頁的「定義內容過濾政策的條件」。

9 在「**動作**」面板中，可以新增您希望 Symantec Messaging Gateway 在郵件符合政策條件時所要採取的動作。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

10 在「**套用至下列政策群組**」面板中，勾選「**政策群組**」旁邊的方塊，針對所有群組啟用此政策。或者，勾選個別群組旁邊的方塊，僅針對所選群組啟用此政策。

11 按下「**儲存**」。

12 在「**電子郵件內容過濾政策**」頁面上，視需要調整新政策的位置。

請參閱第 298 頁的「管理套用多個內容過濾政策的方式」。

定義內容過濾政策的條件

若要定義內容過濾政策的條件，您可以視需要新增多個個別條件。然後，您可以將上述任何條件群組在一起，以建立複合條件來掃描您想要偵測的具體內容。

群組條件

您可以設定您的政策以單獨評估每個條件，也可以將條件群組在一起。若要將條件群組在一起，請選取這些條件，然後按下 **(X&Y)**。若要將條件取消群組，請選取群組，然後按下 **(X),(Y)**。

在政策中，每個條件只能屬於一個群組。例如，若要偵測有效信用卡、美國郵遞區號與美國電話號碼的組合，或有效社會安全號碼、美國郵遞區號與美國電話號碼的組合，您必須建立兩個不同的政策。

選擇「任何」或「全部」

從「**必須符合下列哪一個條件**」功能表中選擇「**任何**」，可在符合政策中的一個條件時觸發判斷。選擇「**全部**」，僅當符合政策中的每個條件時才會觸發判斷。群組的條件將視為單一條件。

例如，假設政策具有以下條件：

- 郵件內文部分中的文字包含 2 處或更多處「機密」一詞
- 郵件大小大於 56 MB
- 檔案中繼資料的檔案名稱中包含文字「最高機密」

以下範例顯示「**任何**」或「**全部**」設定如何影響 SMG 根據該政策評估郵件的方式。

必須符合所有條件	您所指定的每一個條件都必須存在於電子郵件中，才會觸發違規。 例如： 電子郵件訊息不包含附件、大小為 70 MB，且在其內文中「機密」一詞出現兩次。此郵件不符合檔案名稱條件，因此不會觸發違規。 電子郵件包含附件 TOP SECRET.doc、大小為 70 MB，且在其內文中「機密」一詞出現兩次。此郵件符合所有條件，因此會觸發違規。
符合任一條件即可	最少一個條件存在於電子郵件中，即會觸發違規。 例如： 電子郵件不包含附件、大小為 10 MB，且在其內文中「機密」一詞出現一次。此郵件不符合任何政策條件，因此不會觸發違規。 電子郵件訊息不包含附件、大小為 70 MB，且在其內文中「機密」一詞出現一次。此郵件符合「大於 56 MB」的條件，因此會觸發違規。
符合任一條件即可 及 您群組了前兩個條件	最少一個條件存在於電子郵件中，即會觸發違規。但是，「機密」一詞在內文部分出現兩次以上，且郵件大小大於 56 MB 僅視為一個條件。 例如： 電子郵件不包含附件、大小為 10 MB，且在其內文中「機密」一詞出現十次，將不會觸發違規。 電子郵件不包含附件、大小為 70 MB，且在其內文中「機密」一詞未出現，將不會觸發違規。 郵件內文中「機密」一詞出現 10 次、大小為 70 MB，且沒有附件的電子郵件將會觸發違規。 電子郵件包含附件「TOP SECRET.doc」、大小為 10 MB，且在其內文中「機密」一詞未出現，將會觸發違規。

請參閱第 278 頁的「建立內容過濾政策」。

請參閱第 281 頁的「內容過濾政策條件的考量」。

內容過濾政策條件的考量

建立內容過濾政策條件時，請務必熟記下列建議和需求：

使用否定條件

若要在建立政策時提供更大的彈性，您可以將否定條件新增至內容過濾政策。不過，如果您建立一個具有相同條件的肯定和否定版本的政策，則該政策中的每個郵件都會觸發判斷或沒有任何郵件會觸發判斷。

例如，假設您使用「主旨、內文或附件中的文字包含財務關鍵字辭典中的一個或多個單字」條件建立政策。然後，您可以新增「主旨、內文或附件中的文字**不**包含財務關鍵字辭典中的一個或多個單字」條件。

如果政策指定必須符合**任何**條件，則所有郵件都會觸發違規。郵件中必須包含財務關鍵字辭典中的單字，或不包含財務關鍵字辭典中的單字。

如果政策指定必須符合**全部**條件，則郵件不會觸發違規。相同郵件不得包含財務關鍵字辭典中的單字，且不包含財務關鍵字辭典中的單字。

如果您想要掃描相同條件的肯定和否定版本，請建立兩個不同的政策。

請參閱第 729 頁的「肯定與否定內容過濾規則條件範例 」。

與 Enforce Server 整合時使用條件

Enforce Server 會將標頭新增至違反政策的郵件。為了讓 Symantec Messaging Gateway 偵測到這些標頭，您必須在政策條件中描述此標頭。

例如，假設 Enforce Server 將標頭「X-DLP-violation：是」新增至違反政策的郵件。您可以在您的內容過濾政策中新增以下條件：「如果郵件標頭 'X-DLP-violation' 的文字包含 1 或多個 '是'」。

請參閱第 403 頁的「將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合」。

檔案附件大小限制

建立一個使用檔案附件大小限制的政策，然後收到壓縮檔時，Messaging Gateway 會評估該檔案的大小，來判斷附件大小是否超過您指定的限制。依據預設，容器內的壓縮檔 (例如 ZIP 檔案) 會根據其未壓縮大小進行評估。未包含在容器中的壓縮檔案 (例如使用 Linux `gzip` 指令建立的檔案) 會根據其壓縮和未壓縮大小進行評估，如果任一大小超過您政策中設定的限制，就會觸發政策。

壓縮檔

如果未壓縮的附件超過**「開啟時的個別檔案大小上限」**配置區限制，SMG 不會掃描壓縮檔附件。您可以在**「通訊協定」> SMTP >「設定」>「內容掃描」**標籤的**「配置區限制」**面板中，設定此檔案大小。

請確定您對內容過濾政策條件中的附件檔案大小設定的任何限制皆未超過配置區檔的限制。如果附件檔案大小條件超過**「開啟時的個別檔案大小上限」**配置區限制，觸發政策的任何郵件會收到「無法掃描」判斷。

請參閱第 196 頁的「設定巢狀檔案的限制」。

區分大小寫

單字和詞組的所有測試不區分大小寫。條件中的小寫字母會比對郵件中的小寫和大寫字母。而條件中的大寫字母也會比對郵件中的小寫和大寫字母。

多個空格

電子郵件標頭或內文的多個空格會被視為單一空格。

請參閱第 729 頁的「肯定與否定內容過濾規則條件範例 」。

請參閱第 384 頁的「檢視違反內容過濾政策的文字」。

內容過濾條件比對條件

表 14-2 說明 Symantec Messaging Gateway 如何評估內容過濾政策條件中的比對條件 (例如符合/不符合)。

表 14-2 條件比對條件

比對條件	說明
包含/不包含	此比對會根據其使用進行評估： ■ 辭典 依據在選取的辭典中找到的字詞或副檔名來測試郵件內容。 ■ 使用者定義的文字 測試指定元件內使用者定義的文字。有時候稱為子字串測試。 ■ 發生次數 測試使用者指定的發生次數。
符合規則運算式/不符合規則運算式	依據使用者指定的規則運算式來測試郵件內容。規則運算式會合併英數字元與 metacharacter 變數，以識別樣式變體。
符合樣式/不符合樣式	依據已知的規則運算式樣式 (例如在社會安全號碼或信用卡號碼樣式中找到的樣式) 來測試郵件內容。
比對記錄資源中的資料	比較郵件內容與選取之記錄中的資料。
始於/不始於 結束於/不結束於 完全相符/不完全相符	與 ^text 相同的規則運算式。* 與 *text 相同的規則運算式。$ 等同於完全相符或不完全相符提供的文字。
包含郵件部分/不包含郵件部分	依據使用者指定的郵件部分，測試郵件來查看該郵件部分是否存在。
等於/大於/小於	比較郵件大小或附件大小與指定數目的位元組、千位元組 (KB) 或百萬位元組 (MB)。
是位於附件清單/不是位於附件清單 (僅真實檔案類型和類別)	將內文部分和郵件附件與使用者指定的附件清單進行比較，以查看其是否出現在清單中。 **附註：**若條件為**「位於附件清單」**，SMG 會評估內嵌於郵件內文的附件和任何物件的真實檔案類型、真實檔案類別、檔案名稱、副檔名和 MIME。 若條件為**「不是位於附件清單」**，SMG 則會評估內嵌於郵件內文的附件和物件的真實檔案類型和真實檔案類別。SMG 不會針對此條件測試檔案名稱、副檔名或 MIME 類型。
其檔案名稱包含/其檔案名稱不包含	比較檔案名稱和使用者指定的檔案名稱，以確定是否有相符。

比對條件	說明
其 MIME 類型是/其 MIME 類型不是	測試郵件，以確定是否與使用者定義的 MIME 類型相同。
其檔案名稱源自辭典/其檔案名稱不是源自辭典	比較檔案名稱和使用者指定辭典中的檔案名稱，以確定是否有相符。
其副檔名源自辭典/其副檔名不是源自辭典	比較副檔名和使用者指定辭典中的副檔名，以確定是否有相符。

附註：所有文字測試都不區分大小寫。

請參閱第 280 頁的「定義內容過濾政策的條件」。

請參閱第 729 頁的「肯定與否定內容過濾規則條件範例 」。

請參閱第 384 頁的「檢視違反內容過濾政策的文字」。

在內容過濾政策條件中使用規則運算式

規則運算式是您希望 SMG 用來識別特定資訊的樣式。當您建立內容過濾規則的條件時，您可以使用 Perl 規則運算式。若要使用 Perl 運算式，您必須使用**「符合規則運算式」**或**「不符合規則運算式」**作為政策條件。

SMG 以下列方式比對規則運算式：

- 在比對郵件內文時，會針對整個內文文字比對，而非逐行比對。
- 在比對郵件中的每個附件時，會針對整個附件文字比對，而非逐行比對。

依據預設，Symantec Messaging Gateway 不區分規則運算式的大小寫。不過，您可以使用下列字串，將區分大小寫變更為不同模式。

(?i) 停用區分大小寫	在規則運算式陳述式中輸入字串 (?i)，其後面的所有輸入都會忽略區分大小寫。
(?-i) 啟用區分大小寫	在規則運算式陳述式中輸入字串 (?-i)，其後面的所有輸入都會區分大小寫。

您可以隨時將規則運算式查詢由不區分大小寫切換為區分大小寫。

若要使用樣式來比對某些特殊字元 (包括正斜線)，則必須在每個字元前面加上反斜線 (\)。

請參閱第 354 頁的「Perl 相容規則運算式」。

如需有關與 Perl 相容規則運算式的詳細資訊，請搜尋文件，網址為 https://www.perl.org/。

將動作新增至內容過濾政策

當您建立內容過濾政策時，您可以新增您希望 Symantec Messaging Gateway 在郵件符合政策條件時所要採取的動作。

您可以選取在發生政策違規時所要執行的多個動作。Symantec Messaging Gateway 會按照出現於政策之「**動作**」清單中的順序套用動作。

新增內容過濾政策動作

1 在「**新增電子郵件內容過濾政策**」頁面上的「**動作**」下，按下「**新增**」。

2 在「**架構動作**」對話方塊中，選取您希望 SMG 在郵件違反政策條件時所要採取的動作。

對於某些動作，您必須提供其他資訊。

請參閱第 285 頁的「政策動作及其功能」。

3 按下「**新增動作**」。

4 如果您選取「**建立隔離事件**」動作，還必須指定在隔離管理員處理郵件時所要採取的動作。

- 按下「**新增核准的動作**」。在「**架構動作**」頁面上，選取動作，然後按下「**新增核准的動作**」。
- 按下「**新增拒絕的動作**」。在「**架構動作**」頁面上，選取動作，然後按下「**新增拒絕的動作**」。
- 按下「**新增自訂動作**」。在「**架構動作**」頁面上，選取動作，然後按下「**新增自訂動作**」。
  如果與 Enforce Server 整合，請確保 Enforce Server 管理主控台中的回應規則動作與 SMG 動作 (「**核准**」、「**拒絕**」以及「**自訂**」) 一致。
  如果未與 Enforce Server 整合，則仍必須選取自訂動作以取得舊版支援。
  請參閱第 403 頁的「將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合」。

5 重複此程序，視需要新增多個動作。

請參閱第 278 頁的「建立內容過濾政策」。

政策動作及其功能

下表說明您可以新增至 Symantec Messaging Gateway 政策的動作。

表 14-3 政策動作

動作	說明與額外選項
正常傳送郵件	將郵件傳送至目標收件者，但不對郵件進行任何修改。

動作	說明與額外選項
刪除郵件	永久刪除郵件。無法擷取郵件。
將郵件保留在垃圾郵件隔離所	將郵件放置在一般使用者的垃圾郵件隔離所。 請參閱第 239 頁的「關於隔離垃圾郵件」。
轉寄郵件的複本	將郵件複本傳送給您指定的人員。 您還必須提供此額外資訊： ■ **轉寄至** 輸入想要接收轉寄的郵件副本之人員的電子郵件地址。請以逗號分隔多個項目。
繞送郵件	將原始郵件傳送至指定的郵件伺服器，以傳送給原始收件者。 您還必須提供此額外資訊： ■ **主機** 指定您要繞送郵件的主機。 ■ **通訊埠** 指定主機的通訊埠號。 ■ **使用 MX 查詢** 如果您要使用 MX 查詢來尋找與 SMTP 主機對應的資訊，以繞送郵件，請勾選此方塊。 您可以使用**「繞送郵件」**進行流量控制。例如，假設您的定期郵件伺服器無法接受附件大小超過 100 GB 的郵件。您可以建立內容過濾政策，將附件大小超過 100 GB 的所有郵件繞送至不同的郵件伺服器。

動作	說明與額外選項
封存郵件	指定傳送郵件封存複本的位置。 完成以下資訊： ■ **封存電子郵件地址** 輸入傳送郵件封存複本的電子郵件地址。 如果您在**「內容」>「設定」>「封存」**頁面上輸入封存電子郵件地址，該地址則為預設值。 ■ **選用的封存標籤** 指定封存標籤，將 `X-archive:` 標頭新增到封存的郵件，置於您的文字前面。您可以輸入任何字元，除了換行字元、換行符號或分號。 `X-archive:` 標頭有助於您在使用電子郵件用戶端檢視封存的郵件時，對封存郵件進行排序。但是，Symantec Messaging Gateway 本身並不會使用 `X-archive:` 標頭。 如果多個政策動作封存相同的郵件，則會將每個唯一的 `X-archive:` 標頭新增到郵件中。例如，封存標籤 `Docket 53745` 在封存時會將 `X-archive: Docket 53745` 標頭新增至郵件。 ■ **編碼** 指定封存標籤的編碼。 ■ **架構封存伺服器** 如果您在**「內容」>「設定」>「封存」**頁面上輸入封存伺服器資訊，該郵件伺服器則為預設封存伺服器。如果尚未輸入，這些欄位會顯示空白。您可以使用預設伺服器或輸入下列資訊： ■ **封存伺服器主機** 輸入封存郵件伺服器的主機名稱或 IP 位址。 ■ **封存伺服器通訊埠** 如果您已指定封存伺服器主機，也請輸入封存伺服器通訊埠。 ■ **啟用 MX 查詢** 如果您要使用 MX 查詢來尋找與封存伺服器主機對應的資訊，以繞送封存郵件，請勾選此方塊。 電子郵件地址為必填。封存伺服器資訊為選填。如果您僅輸入電子郵件地址，SMG 會使用一般繞送將郵件傳送到封存位址。 請參閱第 356 頁的「指定封存郵件的儲存位置」。
寄送傳送狀態通知	將郵件連同說明傳回其 `From:` 位址，並將郵件傳送給收件者。 您還必須提供此額外資訊： ■ **說明** 輸入通知寄件者傳送狀態的郵件文字。 ■ **編碼** 指定您要用於通知的編碼。 ■ **包括原始郵件** 勾選此方塊，可在傳送給寄件者的通知中包括原始郵件。

動作	說明與額外選項
新增密件副本收件者	將郵件的密件副本傳送給您指定的電子郵件收件者。密件副本收件者並不會顯示在郵件的地址行中。 您還必須提供此額外資訊： ■ **密件副本收件者** 指定要接收郵件密件副本的收件者電子郵件地址。請以逗號分隔多個項目。
修改郵件主旨行	將文字新增至郵件 `Subject:` 行的開頭或結尾。 您還必須提供此額外資訊： ■ **修改** 輸入您想要新增至主旨行的文字。 ■ **編碼** 按下拉式清單，然後選取郵件的編碼。 ■ 選取**「添加至主旨前面」**，可將**「修改」**文字新增至主旨行的開頭。選取**「添加至主旨後面」**，可將**「修改」**文字新增至主旨行的結尾。
新增標頭	將標頭新增至郵件。 您還必須提供此額外資訊： ■ **標頭** 輸入想要新增至郵件的標頭，例如 **X-Cfilter**。 ■ **值** 輸入標頭的值，例如 **Data violation incident**。 ■ **編碼** 選取要用於標頭的編碼。
新增註釋	將註釋新增至郵件內文。 您還必須提供此額外資訊： ■ **註釋** 選取您要使用的註釋。 您可以從**「內容」**>**「資源」**>**「註釋」**頁面，將註釋新增至下拉式清單。 ■ 選取**「在前面添加註釋」**，可在郵件內文前面新增註釋。選取**「在後面添加註釋」**，可在郵件內文後面新增註釋。 請參閱第 341 頁的「建立和管理政策違規的註釋」。
傳送通知	將原始郵件傳送給目標收件者，並傳送預先定義的通知。 您還必須提供此額外資訊： ■ **通知** 選取您要傳送的通知。 您可以從**「內容」**>**「資源」**>**「通知」**頁面，將通知新增至下拉式清單。 請參閱第 321 頁的「關於政策違規通知」。

動作	說明與額外選項
刪除附件	刪除符合指定選項的附件。 可從下列選項中選擇： ■ **刪除所有附件** 刪除所有附件，不管附件是否違反政策。 ■ **刪除附件清單** 按下拉式清單，然後選取您要刪除的附件類型，不管其中是否有任何附件違反政策。 ■ **刪除相符附件** 只刪除違反政策的附件。
建立資訊事件	當違反政策時，將郵件複本傳送到您指定的**「資訊事件」**資料夾。除非您選取刪除動作或隔離動作，否則會傳送原始郵件。 您還必須提供此額外資訊： ■ **在內容資訊事件資料夾中** 按下拉式清單，然後選取要在其中建立事件的「資訊事件」資料夾。 如果您未指定「資訊事件」資料夾，則會在預設的「資訊事件」資料夾中建立事件。 請參閱第 359 頁的「關於內容事件資料夾」。
建立隔離事件	將原始郵件傳送到您指定的「隔離事件」資料夾。 您還必須提供此額外資訊： ■ **在內容隔離事件資料夾中** 按下拉式清單，然後選取要在其中建立事件的「隔離事件」資料夾。 如果您未指定「隔離事件」資料夾，則會在預設的「隔離事件」資料夾中建立事件。 新增**「建立隔離事件」**動作之後，三個**「郵件檢閱」**動作會出現在**「動作」**清單中。您必須為每個**「郵件檢閱」**動作選取一個動作。 ■ 按下**「新增核准的動作」**，然後從資料夾的**「事件管理」**頁面中選取您希望 SMG 在管理員核准已隔離的電子郵件時所要採取的動作。 ■ 按下**「新增拒絕的動作」**，然後選取您希望 SMG 在管理員拒絕已隔離的電子郵件時所要採取的動作。 ■ 按下**「新增自訂動作」**，然後選取您希望 SMG 在管理員針對已隔離的電子郵件選取「自訂」選項時所要採取的動作。 此選項提供用於舊版支援，因此不建議使用。不過，您必須新增自訂動作。 每個政策一次只能套用一個隔離事件動作。 **附註：**新增隔離事件動作後，您可能還想要將通知動作新增至政策。例如，若要隔離大型郵件，您可以傳送一個通知，來告知收件者已收到隔離的大型郵件。通知可能包含寄件者、附件資訊及聯絡管理員以取得原始郵件的方式。 請參閱第 359 頁的「關於內容事件資料夾」。

動作	說明與額外選項
傳送 TLS 加密的郵件	透過加密的通道傳送郵件。 根據收件者主機預期的加密，指定下列其中一個選項： ■ **嘗試 TLS 加密** ■ **需要 TLS 加密但不驗證憑證** ■ **需要 TLS 加密且驗證憑證**
傳送內容加密的郵件	傳送內容加密的郵件。 **附註：**您必須安裝內容加密授權，才能選取此動作。 請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。
視為垃圾郵件	將郵件視為垃圾郵件，並採取垃圾郵件政策中所指定的動作。 請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。 請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。
視為可疑垃圾郵件	將郵件視為可疑垃圾郵件，並採取可疑垃圾郵件政策中所指定的動作。 請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。 請參閱第 214 頁的「預設垃圾郵件及不必要的電子郵件政策」。
視為病毒	將郵件視為病毒，並採取病毒政策中所指定的動作。 請參閱第 176 頁的「關於偵測病毒、惡意軟體與惡意攻擊」。 請參閱第 188 頁的「預設電子郵件惡意軟體政策」。
視為大量郵件病蟲	根據關聯之大量郵件病蟲政策中的動作來處理郵件。 請參閱第 176 頁的「關於偵測病毒、惡意軟體與惡意攻擊」。 請參閱第 188 頁的「預設電子郵件惡意軟體政策」。
視為攔截的寄件者	根據您在「本機攔截的寄件者網域」群組中指定的動作來處理郵件。即使已停用「本機攔截的寄件者網域」群組，還是會套用此動作。 請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。
視為允許的寄件者	根據您在「本機允許的寄件者網域」群組中指定的動作來處理郵件。即使已停用「本機允許的寄件者網域」群組，還是會套用此動作。不會掃描這些郵件是否為垃圾郵件。 請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。
略過垃圾郵件掃描	不掃描郵件中的垃圾郵件。 請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。
略過解除掃描	請勿使用解除掃描功能來找到並移除附件中的潛在惡意內容。 請參閱第 179 頁的「關於「解除」」。

動作	說明與額外選項
略過威脅防禦掃描	不要將郵件傳送至 Content Analysis 進行進階威脅掃描。 請參閱第 390 頁的「關於威脅防禦掃描」。
修改可按式 URL	變更、取代或刪除郵件中的所有可按式連結。 選取**「服務類型」**並輸入選項： ■ 選取**「Email Threat Isolation」**，以透過您的賽門鐵克威脅隔離實例繞送所有 URL 要求。在**「前置值」**欄位中，輸入 Email Threat Isolation 實例的完整網域名稱 (FQDN) 或 IP 位址。此外，請確保針對政策選取**「僅入埠」**條件。請參閱第 292 頁的「將 Symantec Messaging Gateway 與 Symantec Email Threat Isolation 整合」。 ■ 選取**「Web 服務 (ProxySG)」**，以透過您的 Symantec Blue Coat ProxySG 伺服器繞送所有 URL 要求。在**「代理 URL」**欄位中，採用 **https://FQDN/** 格式輸入 ProxySG 伺服器的 URL。URL 必須包含 ProxySG 硬體裝置的完整網域名稱 (FQDN)，並且必須以正斜線 (/) 結尾。此外，請確保針對政策選取**「僅入埠」**條件。請參閱第 294 頁的「將 URL 重新導向至 ProxySG 硬體裝置」。 ■ 選取**「在郵件中取代可按式 URL」**，將郵件中的所有 URL 變更為您在**「值」**欄位中輸入的字串。 　■ 對於 HTML 格式的郵件，所有基礎 URL 位址均變更為**「值」**字串。收件者會看到郵件中的原始 URL，但均不為可按式。 　■ 對於文字格式的郵件，基礎 URL 與可見 URL 相同，因此收件者會看到已修改的 URL。 　■ 如果您用一個 URL 取代所有 URL，新的 URL 可能為可按式，視電子郵件用戶端而定。 請參閱第 291 頁的「修改 URL 以抵禦威脅和未經授權的存取」。 ■ 選取**「在郵件中停用可按式 URL」**，防止在收件者按下某個連結時，瀏覽器瀏覽至目的地 URL。原始連結會顯示在郵件內文中，但無法使用。 請參閱第 291 頁的「修改 URL 以抵禦威脅和未經授權的存取」。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

請參閱第 298 頁的「管理套用多個內容過濾政策的方式」。

修改 URL 以抵禦威脅和未經授權的存取

當您建立內容過濾政策時，您可以新增**「在郵件中修改可按式 URL」**動作。傳送郵件之前，此動作會變更該郵件中的所有 URL。您可以選擇下列其中一個選項來進一步自訂動作：

- **「Email Threat Isolation」**會將瀏覽器傳送至賽門鐵克威脅隔離實例來執行虛擬沙箱。請參閱第 292 頁的「將 Symantec Messaging Gateway 與 Symantec Email Threat Isolation 整合」。
- **Web 服務 (ProxySG)**：將瀏覽器傳送至 Symantec Blue Coat ProxySG 硬體裝置進行安全網頁瀏覽。

請參閱第 294 頁的「將 URL 重新導向至 ProxySG 硬體裝置」。

- **在郵件中取代可按式 URL**：將郵件中的所有 URL 變更為您在對話方塊中輸入的**值**。如果郵件採用 HTML 格式，則基礎 URL 變更，但該郵件會顯示原始 URL。如果郵件採用文字格式，收件者會看到**值**字串而不是原始 URL。
  請參閱第 295 頁的「取代郵件中的可按式 URL」。
- **在郵件中停用可按式 URL**：將字串 `noclick_` 插入每個 URL 的主機名稱中。
  當收件者按下郵件中的URL時，沒有任何作用發生。如果郵件採用純文字格式，收件者可能會發現 URL 已經過修改。如果郵件採用 HTML 格式，則無法看到 URL 修改。
  賽門鐵克建議您將其他動作新增至政策，讓收件者知道郵件中的 URL 已被刻意停用。例如，您可以選取「**修改郵件主旨行**」，然後新增修改 **For security, URLs in this message are disabled**。

SMG 只能對郵件執行一個「**在郵件中修改可按式 URL**」動作。如果郵件觸發兩個或多個具有不同「**在郵件中修改可按式 URL**」動作的政策，SMG 會使用下列優先順序選取要執行的動作：

1. Email Threat Isolation
2. Web 服務 (ProxySG)
3. 在郵件中取代可按式 URL
4. 在郵件中停用可按式 URL

將 Symantec Messaging Gateway 與 Symantec Email Threat Isolation 整合

Symantec Email Threat Isolation可針對 Web 互動提供安全的執行環境。當使用者按下電子郵件訊息中的連結時，Email Threat Isolation 會將瀏覽器與 Internet 隔離。Email Threat Isolation 會執行所有的潛在惡意內容。僅向使用者傳送安全的視覺串流。

透過將「修改 URL」動作新增至內容過濾政策，您可以將 Symantec Messaging Gateway 與 Email Threat Isolation 整合。當政策觸發判斷時，此動作會修改受影響郵件中的每個 URL。如果收件者在郵件中按下連結，瀏覽器會將要求重新導向至 Email Threat Isolation 以進行隔離和執行。

將 Symantec Email Threat Isolation 新增至內容過濾政策

1 在控管中心內，從「**內容**」>「**政策**」>「**電子郵件**」頁面上，按下「**新增**」以建立新的內容過濾政策。或選取政策，然後按下「**編輯**」將 Email Threat Isolation 新增至現有的內容過濾政策。

請參閱第 278 頁的「建立內容過濾政策」。

2 從「**條件**」下的「**套用至**」功能表中，選取「**入埠郵件**」。

警告：永遠不會將 Email Threat Isolation 套用至離埠郵件。在大多數情況下，離埠收件者沒有存取 Email Threat Isolation 實例的權限。其結果是含已修改 URL 的連結可能會失效。

3 在「**動作**」面板中，按下「**新增**」。

4 在「**架構動作**」對話方塊中，選取「**在郵件中修改可按式 URL**」。

5 在「**服務類型**」欄位中，選取「**Email Threat Isolation**」。

6 在「**前置值**」欄位中，輸入 Symantec Email Threat Isolation 實例的完整網域名稱 (FQDN) 或 IP 位址。

附註：對於 Symantec Messaging Gateway 10.6.5，請參閱 https://www.symantec.com/docs/HOWTO127807，以瞭解有關如何針對該版本輸入「**前置值**」的相關指示。

7 按下「**新增動作**」。

當郵件觸發判斷時，Symantec Messaging Gateway 會修改郵件中的所有 URL，以將其重新導向至您在「**前置值**」中指定的主機名稱。當收件者按下已修改的連結時，會將瀏覽器要求繞送至 Email Threat Isolation 實例。

8 當您完成建立或編輯政策時，請按下「**儲存**」。

使用 Email Threat Isolation 保護您所有的使用者

建立將 Email Threat Isolation 防護套用到所有入埠郵件的內容過濾政策：

1 在「**電子郵件內容過濾政策**」頁面上，按下「**新增**」。

2 選取「**空白**」範本。

3 在「**設定**」面板上，停用「**在控制面板和報告中追蹤此政策的違規**」。

4 從「**條件**」面板的「**套用至**」功能表中，選取「**入埠郵件**」。

5 按下「**新增**」來新增條件。

6 選取「**針對所有郵件**」，然後按下「**新增條件**」。

7 在「**動作**」面板中，按下「**新增**」。按照上述程序中的步驟新增「**修改可按式 URL**」動作。

8 將政策套用到所有政策群組，然後按下「**儲存**」。

9 在「**電子郵件內容過濾政策**」頁面上，將政策拖曳到清單最上方。

將 URL 重新導向至 ProxySG 硬體裝置

您可以新增動作至 Symantec Messaging Gateway 內容過濾政策，以將所有瀏覽器要求重新導向至您的 Symantec Blue Coat ProxySG 硬體裝置。如果郵件觸發政策的判斷，該動作會將 ProxySG URL 新增到郵件中的每個可按式 URL 的開頭。當使用者按下連結時，電腦會將瀏覽器要求重新導向至 ProxySG URL。然後，ProxySG 政策會決定使用者是否可以存取連結網頁。

附註：您的使用者的電腦和瀏覽器必須設定為與 ProxySG 硬體裝置進行通訊。此外，您必須在 ProxySG 上定義政策，以評估和處理瀏覽器要求。ProxySG 預設為拒絕存取，因此，從 SMG 重新導向瀏覽器的所有要求都將失敗，直到您定義相關政策為止。如需如何設定 ProxySG 政策的相關指示，請參閱 ProxySG 文件。

將瀏覽器要求傳送至 Symantec Secure Web Gateway (ProxySG)

1 在控管中心內，從「**內容**」>「**政策**」>「**電子郵件**」頁面上，按下「**新增**」以建立新的內容過濾政策。或選取政策，然後按下「**編輯**」將 ProxySG 重新導向新增至現有的內容過濾政策。

請參閱第 278 頁的「建立內容過濾政策」。

2 從「**條件**」下的「**套用至**」功能表中，選取「**入埠郵件**」。

警告：永遠不會將重新導向至 ProxySG 的政策套用至離埠郵件。離埠收件者不具有存取 ProxySG 硬體裝置的權限，因此，含已修改 URL 的連結將會失效。

---

3 在「**動作**」面板中，按下「**新增**」。

4 在「**架構動作**」對話方塊中，選取「**在郵件中修改可按式 URL**」。

5 在「**服務類型**」欄位中，選取「**Web 服務 (ProxySG)**」。

6 在「**代理 URL**」欄位中，採用 **https://FQDN/** 格式輸入 ProxySG 硬體裝置的 URL。

例如：**https://mycompanyproxy.com/**

URL 必須包含 ProxySG 硬體裝置的完整網域名稱 (FQDN)，並且必須以正斜線 (/) 結尾。

7 按下「**新增動作**」。

當郵件觸發判斷時，Symantec Messaging Gateway 會將「**代理 URL**」新增到郵件中的所有 URL 的開頭。當收件者按下已修改的連結時，「**代理 URL**」會將瀏覽器要求繞送至 ProxySG。

8 若要測試「**代理 URL**」，請將其輸入至瀏覽器的地址行中。然後，將已知有效的 URL 新增到「**代理 URL**」的結尾，然後按 **Enter**。

例如：

如果您的「**代理 URL**」為 **https://mycompanyproxy.com/**，

且 URL 為 **https://www.symantec.com**，

請將 **https://mycompanyproxy.com/https://www.symantec.com**

輸入至瀏覽器中。

如果「**代理 URL**」正確，瀏覽器會顯示賽門鐵克公司首頁。

測試電腦必須設定為與您的 ProxySG 硬體裝置進行通訊，並且 ProxySG 必須具有允許此存取權的政策。

9 當您完成建立或編輯政策時，請按下「**儲存**」。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

使用 ProxySG 保護您所有的使用者

建立將 ProxySG 防護套用到所有入埠郵件的內容過濾政策：

1 在「**電子郵件內容過濾政策**」頁面上，按下「**新增**」。

2 選取「**空白**」範本。

3 在「**設定**」面板上，停用「**在控制面板和報告中追蹤此政策的違規**」。

4 從「**條件**」面板的「**套用至**」功能表中，選取「**入埠郵件**」。

5 按下「**新增**」來新增條件。

6 選取「**針對所有郵件**」，然後按下「**新增條件**」。

7 在「**動作**」面板中，按下「**新增**」。按照上述程序中的步驟新增「**修改可按式 URL**」動作。

8 將政策套用到所有政策群組，然後按下「**儲存**」。

9 在「**電子郵件內容過濾政策**」頁面上，將政策拖曳到清單最上方。

取代郵件中的可按式 URL

當您選取內容過濾政策動作「**在郵件中修改可按式 URL**」，並選擇選項「**在郵件中取代可按式 URL**」，則輸入取代所有可按式 URL 的「**值**」字串。收件者的使用者體驗取決於「**值**」字串，以及該郵件是否以 HTML 或文字格式傳送。

表 14-4 修改可按式 URL 時的結果

將每個 URL 取代為下列內容時：	郵件採用 HTML 格式時的結果：	郵件採用文字格式時的結果：
不含 URL 的文字	收件者會看到郵件中的原始 URL，但基礎連結將變更為您所指定的文字字串。 當收件者按下修改後的連結時，瀏覽器視窗隨即開啟，並顯示找不到網頁的錯誤訊息。	新文字會取代郵件中的每個 URL。收件者無法看到原始 URL。 新文字不是可按式。
包含 URL 的文字	收件者會在檢視自己的郵件時看到原始 URL，但基礎連結將變更為您所指定的文字和 URL 字串。 當收件者按下修改後的連結時，瀏覽器視窗隨即開啟，並顯示找不到網頁的錯誤訊息。	新文字和 URL 字串會取代郵件中的每個原始 URL。收件者無法看到原始 URL。 新 URL 可能為可按式，視電子郵件用戶端的功能而定。
其他 URL (沒有其他文字)	收件者會在檢視自己的郵件時看到原始 URL，但基礎連結將變更為您所指定的 URL。 當收件者按下郵件中的連結時，瀏覽器視窗隨即開啟，並顯示取代 URL 的網頁。	新 URL 會取代郵件中的每個原始 URL。收件者無法看到原始URL。 新 URL 可能為可按式，視電子郵件用戶端的功能而定。

若要在您支援以 HTML 和文字格式傳送郵件時提供最佳使用者體驗，請執行以下任一作業：

- 將所有URL取代為其他URL。例如，您可以輸入說明組織隱私權政策之網頁的完整URL。請不要包含其他文字。
  測試結果以確保採用 HTML 和文字格式的取代 URL 均為可按式。
- 將所有URL取代為文字字串；例如，「已針對您的防護停用連結。」然後，將標頭動作或註釋動作新增至政策，以通知收件者該郵件中的所有原始 URL 皆已停用。
  如果郵件採用 HTML 格式，收件者會看到說明為何可見連結均無法使用的標頭或註釋。如果郵件採用文字格式，收件者會看到取代文字，而不是原始 URL。還會看到標頭或註釋。

套用內容過濾政策至政策群組

定義內容過濾政策的動作之後，請指定要套用該政策的政策群組。

對於符合類似條件但需對不同政策群組採取不同動作的郵件，您必須建立不同的政策。同樣地，對於入埠郵件的處理方式可能與符合某個政策群組之相同條件的離埠郵件不同。

例如，假設繞送含有機密人力資源資料的電子郵件，就需要採取不同的動作。請建立一個政策，其中傳送給總經理的郵件不會包含附件。建立包含相同條件的不同政策，但傳送給經理的郵件需保留以供檢視。

您可以透過以下任一方式將內容過濾政策套用至政策群組：

- 先建立政策群組，然後在建立內容過濾政策時，將政策套用至該群組。
  建立內容過濾政策的程序會假設已經先建立政策群組，然後將政策套用至該群組。
- 建立內容過濾政策，然後建立政策群組，並將內容過濾政策套用至該群組。
  政策建立之後，如果新增了員工或政策群組，請使用此方法。

建立內容過濾政策之後，就會自動啟用該政策。如果您還不必要使用該內容過濾政策，請加以停用。

指定內容過濾政策要套用的政策群組

1 在**「政策群組」**下，勾選應套用此政策的一或多個群組。

2 按下**「儲存」**。

3 建立內容過濾政策之後，請指定要評估政策的順序。

請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

測試內容過濾政策的提示

當您新增內容過濾政策時，應執行測試以確保該政策如預期般過濾。當政策包括破壞性動作(如**「刪除郵件」**)時，測試尤其重要。您可能還想要在對現有政策進行有意義的變更時執行測試。

以下提供一些測試內容過濾政策的建議：

1. 使用您想要的條件建立政策。
2. 新增至少一個您可以輕鬆追蹤的動作。例如，您可以：
   - 選取**「新增標頭」**動作並新增自訂標頭。然後，您可以監控郵件標頭，以確定觸發政策判斷的郵件。
   - 選取**「建立資訊事件」**動作。每當政策觸發判斷時，SMG 都會新增您可以檢視的資訊事件。
3. 將政策指派給測試政策群組。或者，如果您將政策指派給生產環境中的政策群組，則在完成測試之前，不會將破壞性動作納入政策中。
4. 傳送挑戰政策的測試電子郵件。包含您不希望觸發判斷的測試電子郵件。
5. 如果您對政策如預期般運作感到滿意，請編輯政策以包含您要指派的最終動作。

管理套用多個內容過濾政策的方式

Symantec Messaging Gateway 會按照出現於「**電子郵件內容過濾政策**」頁面中的順序評估政策。Symantec Messaging Gateway 會首先評估清單中顯示的第一個政策，接著評估下一個政策，依此類推。您可以將政策拖曳至不同位置以變更順序。

「後續內容過濾處理」設定如何影響觸發判斷的下一個政策

當內容過濾政策觸發第一個判斷時，Symantec Messaging Gateway 會將該政策的所有動作新增至動作清單。SMG 使用該政策的「**後續內容過濾處理**」設定，來決定當清單中的第二個內容過濾政策觸發判斷時應採取的動作。第二個政策的「**後續內容過濾處理**」設定決定當第三個政策觸發判斷時 SMG 應採取的動作，依此類推。下表說明每個設定及其影響。

表 14-5 「後續內容過濾處理」設定和結果

如果已觸發的上一個政策具有以下設定：	Symantec Messaging Gateway 會執行此操作：
繼續進行評估和動作	繼續評估其餘內容過濾政策。 如果另一個內容過濾政策觸發判斷，SMG 會為該政策新增動作。然後，SMG 會針對新觸發的政策使用「**後續內容過濾處理**」設定來決定接下來怎麼做。
僅提供事件和通知動作	**附註：**此設定提供用於舊版支援，因此不建議使用。 僅新增「**建立資訊事件**」和「**傳送通知**」動作至清單。如果政策有該動作，將「**建立隔離事件**」變更為「**建立資訊事件**」。忽略所有其他動作，並正常傳送郵件。
中斷評估和動作	不會評估位於清單底端的任何政策。不會在清單中新增任何其他動作。

完成所有過濾後，Symantec Messaging Gateway 會依動作優先順序排序動作清單。當多個動作發生衝突時，Symantec Messaging Gateway 會刪除優先度較低的所有動作。

請參閱第 720 頁的「來自多個判斷的動作組合」。

「後續內容過濾處理」如何影響政策與動作的範例

表 14-6 範例和結果

範例	結果
範例 1 ■ 政策 1 具有「**修改郵件主旨行**」動作。「**後續內容過濾處理**」選項為「**僅提供事件和通知動作**」。 ■ 政策 2 具有「**新增標頭**」和「**建立資訊事件**」動作。後續政策選項為「**繼續進行評估和動作**」。 ■ 政策 3 具有「**新增註釋**」動作。後續政策選項為「**繼續進行評估和動作**」。	Symantec Messaging Gateway 會評估所有三個政策，而所有三個政策都違規。 Symantec Messaging Gateway 會修改政策 1 的郵件主旨行。 政策 1 指定「**僅提供事件和通知動作**」。當政策 2 觸發判斷時，Symantec Messaging Gateway 新增資訊事件，但不會新增標頭。 政策 2 指定「**繼續進行評估和動作**」。當政策 3 觸發判斷時，Symantec Messaging Gateway 會新增註釋。 其結果是 Symantec Messaging Gateway 修改主旨行、新增註釋、建立資訊事件，並傳送郵件。
範例 2： ■ 政策 1 具有「**新增標頭**」動作。後續政策選項為「**僅提供事件和通知動作**」。 ■ 政策 2 具有「**建立隔離事件**」動作。後續政策選項為「**繼續進行評估和動作**」。 ■ 政策 3 具有「**刪除郵件**」動作。後續政策選項為「**中斷評估和動作**」。	Symantec Messaging Gateway 會評估所有三個政策，而所有三個政策都違規。 對於政策 1，Symantec Messaging Gateway 會將「**新增標頭**」新增至動作清單。 政策 1 指定「**僅提供事件和通知動作**」。當政策 2 觸發判斷時，Symantec Messaging Gateway 會將「**建立資訊事件**」(而不是「**建立隔離事件**」) 新增至動作清單。 政策 2 指定「**繼續進行評估和動作**」。當政策 3 觸發判斷時，Symantec Messaging Gateway 會將「**刪除郵件**」新增至動作清單。 政策 3 指定「**中斷評估和動作**」，因此 Symantec Messaging Gateway 不會評估任何其他內容過濾政策。 當所有處理完成後，Symantec Messaging Gateway 會評估動作。「**刪除郵件**」動作會覆寫「**新增標頭**」動作。「**刪除郵件**」和「**建立資訊事件**」具有相同的優先度。其結果是 Symantec Messaging Gateway 刪除該郵件並建立資訊事件。

範例	結果
範例 3： ■ 政策 1 具有「**新增標頭**」動作。後續政策選項為「**中斷評估和動作**」。 ■ 政策 2 具有「**建立隔離事件**」動作。後續政策選項為「**繼續進行評估和動作**」。 ■ 政策 3 具有「**刪除郵件**」動作。後續政策選項為「**僅提供事件和通知動作**」。	對於政策 1，Symantec Messaging Gateway 會將「**新增標頭**」新增至動作清單。 政策 1 指定「**中斷評估和動作**」，因此 Symantec Messaging Gateway 不會評估政策 2 或政策 3。 其結果是 Symantec Messaging Gateway 新增標頭並傳送該郵件。

請參閱第 278 頁的「建立內容過濾政策」。

郵件稽核日誌如何協助微調及疑難排解內容過濾政策

Symantec Messaging Gateway 可讓您建立內容過濾政策來監控入埠和離埠電子郵件訊息的內容。

您也可以建立內容過濾政策來執行下列操作：

- 遵從政府頒佈的法規。
- 根據內部政策攔截或保留郵件以供檢閱。
- 部署更積極的規則以攔截特定類型的郵件內容。

當使用者發現電子郵件未送達或抱怨其收件匣收到不必要的電子郵件時，由於牽涉到許多政策，使用者可能無法立即明瞭如何調整適當的政策以修正問題。若要疑難排解這些問題，您可以檢視郵件稽核日誌。

郵件稽核日誌會指出違反政策的文字，以及其中包含違規的郵件部分。

例如，架構內容過濾政策以使用規則運算式來進行內容比對。您可以設定政策的動作以刪除郵件。您開始收到關於電子郵件訊息未送達的抱怨。您可以在郵件稽核日誌中檢視郵件以查看違反政策的內容來疑難排解此問題。您可以根據您的調查結果，視需要微調政策。

請參閱第 545 頁的「搜尋郵件稽核日誌中的郵件」。

請參閱第 385 頁的「升級現有內容對相符文字功能的影響 」。

請參閱第 283 頁的「內容過濾條件比對條件」。

15

使用內容過濾資源來過濾內容

本章包含以下主題：

- 關於內容過濾政策資源
- 在內容過濾政策中使用結構化資料
- 關於記錄檢視
- 處理內容過濾違規通知
- 使用辭典
- 使用樣式偵測政策違規
- 建立和管理政策違規的註釋
- 使用清單偵測禁止的附件
- 指定封存郵件的儲存位置

關於內容過濾政策資源

Symantec Messaging Gateway 提供了下列資源，可以用來建立內容過濾政策：

註釋	您可以將文字附加到違反政策的郵件上。您選擇的文字取決於政策。例如，它會告知收件者伴隨的電子郵件違反公司規範和企業管理政策。 請參閱第 341 頁的「建立和管理政策違規的註釋」。

封存

有些規定會要求封存可能違反企業政策的所有郵件。您可以將要封存的郵件副本傳送到一般郵件伺服器上的指定電子郵件地址， 還可以將郵件副本傳送至封存伺服器。

請參閱第 356 頁的「指定封存郵件的儲存位置」。

附件清單

附件清單是根據附件的真實檔案類型、MIME 類型或副檔名所預先定義的清單。附件清單包含您希望 Symantec Messaging Gateway 偵測的副檔名和檔案應用程式類型。您可以使用附件清單作為內容過濾政策的條件。Symantec Messaging Gateway 偵測到附件具有副檔名清單上的副檔名時，會套用您指定的動作。Symantec Messaging Gateway 能根據建立電子郵件附件的應用程式來判斷該附件的類型，而不管其副檔名為何。

請參閱第 343 頁的「關於附件清單」。

辭典

建立政策條件時，辭典會提供您可以使用的預先定義的字詞清單。例如，您可以使用辭典來偵測粗俗的語言或暗示求職活動的語言。

請參閱第 325 頁的「關於內容過濾辭典」。

通知

Symantec Messaging Gateway 可以在符合政策的條件時，將自訂通知傳送給電子郵件的寄件者或收件者。通知可以連同或不連同伴隨的郵件一併傳送。您也可以架構政策，以通知負責實施違反政策的內容過濾主管、經理或管理員。

請參閱第 321 頁的「關於政策違規通知」。

樣式

樣式是預先定義的字元樣式清單，與您可能要限制的物件類型或資料類型相關聯。例如，透過搜尋標準信用卡樣式，您可以使用樣式來檢查外寄郵件中是否有信用卡號碼。

請參閱第 338 頁的「關於樣式」。

記錄

記錄由貴組織提供的結構化資料組成。結構化資料包含要保護的公司特定資料(已分隔)。您可以建立要用於內容過濾政策(可偵測郵件中是否有資料來源檔案的內容)中之記錄的檢視。可偵測內送電子郵件和外寄電子郵件中的內容。如果內送或外寄郵件的內容符合資料來源記錄中定義的資料，則可以指定您希望 Symantec Messaging Gateway 採取的動作。

請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

在內容過濾政策中使用結構化資料

表 15-1 描述了將結構化資料用於內容過濾政策的程序。

表 15-1 如何將結構化資料用於政策

步驟	工作	說明
1	確定您要用於建立內容過濾政策的「結構化資料」政策範本。	資料來源檔案中的樣式欄位必須對應於「結構化資料」政策範本所使用的資料類型。 例如，假設您要使用「客戶資料保護」範本來建立政策。您應使用與社會安全號碼、信用卡號碼、電話及電子郵件相對應的樣式欄位。
2	從資料庫管理員取得資料來源檔案。	結構化資料包含由貴公司提供的資料來源檔案。此檔案包含由要保護的公司特定資料 (已分隔) 構成的欄。 請參閱第 304 頁的「關於您的資料來源檔案」。
3	建立記錄。	建立記錄時，可以指定該記錄的名稱、說明 (選用)、資料來源屬性，以及處理錯誤臨界值。 請參閱第 306 頁的「建立結構化資料的記錄」。
4	對應資料來源檔案中的欄。	您必須將資料來源檔案中每一欄的樣式對應至 Symantec Messaging Gateway 中的對應欄位。 請參閱第 308 頁的「關於對應資料來源檔案欄」。 請參閱第 307 頁的「將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位」。 請參閱第 310 頁的「系統樣式」。
5	上載資料來源檔案。	Symantec Messaging Gateway 會在您上載檔案時驗證檔案，並通知您上載是否成功。如果上載成功，Symantec Messaging Gateway 會對該檔案建立索引。如果上載失敗，則會顯示錯誤訊息，指出失敗原因。 請參閱第 312 頁的「上載資料來源檔案」。
6	複寫記錄。	您必須先將記錄複寫到已附加且已啟用的所有掃描程式，然後才能將其用於內容過濾政策。 將資料來源檔案複寫到掃描程式可能會相當耗時，您可能要等到離峰時間來複寫記錄。 請參閱第 313 頁的「複寫記錄」。

步驟	工作	說明
7	為記錄定義一或多個檢視。	使用檢視，您可以指定在 Symantec Messaging Gateway 評估郵件時，要在記錄中搜尋的欄位。您也可以指定郵件中必須有多少此類欄位時，檢視才會出現。 記錄可以有一或多個檢視。例如，一個檢視可能包含信用卡號碼樣式、電子郵件地址樣式，以及 IP 位址樣式。同一記錄的另一個檢視，則可能包含信用卡號碼樣式、台灣電話樣式，以及台灣郵遞區號樣式。使用多個檢視，您可以從同一政策的單一記錄或多個條件，建立多個內容過濾政策。 您必須先定義至少一個檢視，然後才能將記錄用於內容過濾政策。 請參閱第 318 頁的「建立記錄檢視」。 請參閱第 318 頁的「編輯記錄檢視」。
8	使用「結構化資料」政策範本建立內容過濾政策。	您必須使用「結構化資料」政策範本或空白範本，才能將記錄檢視用作政策條件。 請參閱第 278 頁的「建立內容過濾政策」。
9	架構政策以將記錄檢視用作條件。	在內容過濾政策中，指定必須出現幾次才會構成政策違規。 請參閱第 280 頁的「定義內容過濾政策的條件」。

關於您的資料來源檔案

若要在內容過濾政策中使用結構化資料，您必須向資料庫管理員取得資料來源檔案。

表 15-2 說明有關您資料來源檔案的需求與考量。

表 15-2　　資料來源檔案的需求與考量

需求或考量	說明
每個分隔欄位只有一個單字是由至少兩個英數字元所組成	每一個項目必須至少包含兩個英數字元。欄位不支援單一字元項目。 此外，資料來源檔案的每個分隔欄位只能有一個單字。例如，如果您要比對「1st Street」這份資料，就應該將 1st 放在某個分隔欄位， 且將「Street」放在另一個 (下一個) 欄位。如果您在欄位中放入兩個以上的單字，就很難找到符合的結果。 例如，如果您將「1st street」字串放在單一分隔欄位，就等於在同一個儲存格中放入多個「單字」。而這樣無法進行比對，原因是除非要檢查的資料是表格格式，否則不會有比對結果。在表格格式中，(1st) 和 (Street) 這兩個字串會視為單一字串 (1st Street)。嘗試比對以不同方式來辨識空格的語言 (例如韓文或中文) 時，也會有類似的行為。

需求或考量	說明
信用卡號碼樣式只能辨識特定分隔符號	Symantec Messaging Gateway 嘗試比對信用卡號碼樣式欄位中的記錄項目時，只能辨識某些分隔符號字元。 信用卡號碼樣式欄位可辨識的分隔符號字元 (不含空格) 如下： ■ 標籤 ■ 逗號 (,) ■ 井字號 (#) ■ 連字號 (-) ■ 加號 (+) ■ 管道字元 (|) ■ 分號 (;) ■ 冒號 (:) Symantec Messaging Gateway 會將任何包含無法辨識之分隔符號的號碼解譯為單字。例如，4123*6666*7777*8888 若與信用卡號碼欄位比對，將不會傳回有效的符合結果。Symantec Messaging Gateway 會將此內容解譯為單字：4123*6666*7777*8888。
使用逗號以外的分隔符號來分隔相鄰的號碼樣式	請使用 Tab 或管道字元 (|) 取代逗號作為欄位的分隔符號，來分隔相鄰的兩個號碼樣式欄位。否則，「記錄」驗證器會將相鄰欄位的兩個號碼解譯為單一號碼。 例如，假設有兩個相鄰的欄位：「年齡」與「體重」。假設您已使用逗號來分隔「年齡」與「體重」等欄位；例如：25,150。Symantec Messaging Gateway 可能會將 25,150 解譯為屬於「年齡」欄位，而非將 25 解譯為屬於「年齡」欄位，而 150 屬於「體重」欄位。
資料來源檔案必須有「結構化資料」範本所需的最少欄位	請確定您的資料來源檔案包含您要用來定義檢視的欄位。例如，假設您使用的「結構化資料」政策要求最少三個欄位才能觸發違規。記錄中就必須對應那三個欄位，以便 Symantec Messaging Gateway 能夠參照那些欄位。 例如，假設您使用的是「歐盟資料保護指令」政策範本。存取「歐盟資料保護指令」政策的任何檢視，都應該架構為符合以下五個欄位中至少四個欄位的項目： 姓氏、電子郵件、電話號碼、帳號和使用者名稱。 請參閱第 318 頁的「建立記錄檢視」。
樣式欄位應與政策範本中所用的資料類型相符	樣式欄位必須對應到「結構化資料」政策範本所使用的資料類型。例如，假設您要使用「客戶資料保護」範本來建立政策。您必須使用對應至社會安全號碼、信用卡號碼、電話號碼以及電子郵件欄位的樣式欄位。
對應必須符合標頭列的欄位。	如果記錄中的對應不符合標頭列的欄位，則 Symantec Messaging Gateway 會將實際標頭列算成無效列。因為標頭列會傳回非預期的值，所以會視為無效。 請參閱第 308 頁的「關於對應資料來源檔案欄」。

需求或考量	說明
信用卡號碼必須通過 Luhn 總和檢查碼測試	所有信用卡號碼必須通過 Luhn 總和檢查碼測試，其中總計與 10 的模數等於 0，才能產生相符。Luhn 測試是用來區分有效數字與隨機數集合。
位於資料來源檔案之列前面的 CRLF 換行符號會包括在列計數中。	如果資料來源檔案不含 CRLF，則 Symantec Messaging Gateway 會在列計數中略過標頭列。如果資料來源檔案含有 CRLF，則 Symantec Messaging Gateway 會將第一個 CRLF 視為標頭列。所以，它會傳回後續列的值，包括實際標頭列的值在內。 例如，若對應一個欄位來辨識台灣郵遞區號樣式，而且資料集的開頭為一個以上的 CRLF， 則 Symantec Messaging Gateway 會將實際標頭列算成一般列。該欄中預期應傳回 5 位數。當實際標頭列傳回單字值而非 5 位數字時，Symantec Messaging Gateway 會將其算成無效列。 Symantec Messaging Gateway 會忽略出現在資料集內或資料集結尾的 CRLF。這種 CRLF 不算成列。
出現超過 99 次的列不會進行比對	由於實作限制，Symantec Messaging Gateway 無法比對出現超過 99 次的列。

請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

建立結構化資料的記錄

取得資料來源檔案之後，可以建立記錄。

請參閱第 304 頁的「關於您的資料來源檔案」。

建立記錄時，可定義下列條件：

名稱和說明

指定記錄的名稱和說明。選取可識別記錄所含資料的名稱。記錄的說明是選用的。

如果變更記錄的名稱，參考該記錄之檢視的所有條件都會反映出名稱變更。

請參閱第 314 頁的「修改記錄」。

資料來源屬性

指定資料來源檔案所使用的分隔符號。支援的分隔符號為 Tab、逗號 (,) 或管道 (|) 字元。

也會指出您的資料來源檔案是否包含標頭列。記錄中既不處理也不包括標頭列。

如果您將所有欄位定義為系統樣式，則不需要勾選**「資料來源檔案包含一個標頭列」**方塊。

請參閱第 307 頁的「將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位」。

錯誤臨界值	將**「可允許的錯誤數目上限」**設為上載資料來源檔案時可以安全傳回錯誤且仍可繼續處理之總列數百分比。如果百分比過低，則可能很難完成處理資料來源檔案，而資料來源檔案若完成處理將很有用。百分比設得太高，則可能無法得知記錄檔案是否有部分損毀。

若要建立記錄，您必須具有「完整的管理」權限或修改設定的權限。

建立結構化資料的記錄

1. 在控管中心內，按下**「內容」>「資源」>「記錄」**。
2. 按下**「新增」**。
3. 在**「記錄資源名稱」**欄位中，輸入記錄的名稱。
4. 在**「選用說明」**欄位中，輸入記錄的說明。
5. 在**「資料來源屬性」**下，按下**「分隔符號」**下拉式清單，然後選取資料來源檔案的分隔符號字元。
6. 如果資料來源檔包含標頭列，請勾選 **「資料來源檔案包含一個標頭列」** 核取方塊。
7. 在**「錯誤臨界值」**下，輸入在中斷處理之前允許出現錯誤的百分比上限。

   定義記錄之後，請將資料來源檔案欄對應至 Symantec Messaging Gateway 中的欄位。

   請參閱第 307 頁的「將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位」。

將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位

定義記錄之後，請將資料來源檔案中的欄對應到 Symantec Messaging Gateway 中的欄位。您可以使用預先定義的系統樣式欄位，也可以建立自訂欄位。

請參閱第 306 頁的「建立結構化資料的記錄」。

請參閱第 308 頁的「關於對應資料來源檔案欄」。

請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

若要對應資料來源檔案，您必須具有「完整的管理」權限或修改設定的權限。

將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位

1 在「**新增記錄資源**」頁面的「**對應**」下，按下「**欄位名稱**」下拉式清單，然後執行下列其中一項工作：

使用系統樣式欄位	選取您要與資料來源檔案中對應欄相關聯的系統樣式。 例如，如果資料來源檔案中的欄 1 包含電話號碼，請在欄 1 選取「**台灣電話樣式**」。 請參閱第 310 頁的「系統樣式」。
建立自己的自訂欄位	選取「**自訂**」，然後在相鄰的文字欄位中，輸入唯一的自訂欄位名稱。自訂欄位名稱不得與預先定義的欄位名稱清單中的任一欄位名稱相同， 也不得與記錄中任何其他自訂欄位名稱相同。 例如，假設資料來源檔案的欄 3 包含姓氏。在欄 3 中，選取「**自訂**」，然後在相鄰的方塊中，輸入 **first_name**。

2 若要變更欄位的順序，請勾選您要移動之欄位名稱旁的方塊，然後按「**上移**」或「**下移**」。

3 若要新增額外的欄位，請按下「**新增**」，然後重複執行步驟 1 中的工作以使用系統樣式，或建立自己的自訂欄位。

4 按「**下一步**」。

對應資料來源檔案欄之後，請上載該資料來源檔案。

請參閱第 312 頁的「上載資料來源檔案」。

關於對應資料來源檔案欄

樣式就是指定的規則運算式或系統樣式，用來描述一般已知的資料物件，例如信用卡號碼的樣式。您必須將資料來源檔案中每一欄的樣式對應至 Symantec Messaging Gateway 中的對應欄位。

表 15-3 說明對應資料來源檔案時可使用的欄位類型。

表 15-3 欄位類型

欄位類型	說明
系統樣式	Symantec Messaging Gateway 會將資料來源檔案中每一欄的資料，與系統樣式進行比對。一組規則運算式可定義一個系統樣式。資料來源檔中的資料必須符合資料檔案的其中一個規則運算式，才能順利上載及編製索引。 系統樣式如下： ■ 信用卡號碼樣式 ■ 電子郵件樣式 ■ IP 位址樣式 ■ 數字樣式 ■ 百分比樣式 ■ 台灣電話樣式 ■ 台灣郵遞區號樣式 ■ SSN/ITIN 樣式 請參閱第 310 頁的「系統樣式」。
自訂	如果資料來源檔案中的資料未歸類至其中一種系統樣式類別，則您可以建立自訂欄位。Symantec Messaging Gateway 只會將自訂欄位辨識為 WORD 樣式。自訂欄位不會編製索引，也不會經過驗證。 賽門鐵克建議您使用與資料來源檔案中欄位名稱相似的自訂欄位名稱。例如，如果資料來源檔案中的第一個欄位是 first_name，則您可以將 Symantec Messaging Gateway 中的對應欄位命名為 first_name。自訂欄位名稱不得與預先定義的欄位名稱清單中的任一欄位名稱相同， 也不得與記錄中任何其他自訂欄位名稱相同。

表 15-4 提供如何對應資料來源檔案的範例。

表 15-4 資料來源檔案對應範例

資料來源檔案欄	資料來源檔案欄中包含的資料	Symantec Messaging Gateway 欄	欄位名稱
1	信用卡號碼	1	**信用卡號碼樣式**
2	電子郵件地址	2	**電子郵件樣式**
3	姓氏	3	**自訂** 自訂欄位名稱： first_name
4	名字	4	**自訂** 自訂欄位名稱： last_name

請參閱第 304 頁的「關於您的資料來源檔案」。

請參閱第 307 頁的「將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位」。

請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

系統樣式

表 15-5 描述了對應資料來源檔案欄至 Symantec Messaging Gateway 時可使用的系統樣式。

表 15-5 系統樣式

系統樣式	範例	說明
信用卡號碼	5369 7777 8888 9999	MasterCard： 任何 16 位數字，開頭為 5，第二位數字是 1 到 5 的數字，分成 4 組 4 位數，以空格或連字號隔開。
	5369-7777-8888-9999	
	4567 1234 5678 9123	VISA 卡： 任何 16 位數字，開頭為 4，分成 4 組 4 位數，以空格或連字號隔開，或任何開頭為 4 的 12 位數字。
	4123-6666-7777-8888	
	4123456789012	
	3442 456789 12345 3758 456789 12345	美國運通卡： 任何 15 位數字，開頭為 34 或 37，分成 3 組，分別為 4、6 和 5 位數，以空格或連字號隔開。
	3056 123456 7890 3667 123456 7890 3878 123456 7890 3056-123456-7890 3667-123456-7890 3842-123456-7890	大來卡： 任何 15 位數字，開頭為 30、36 或 38，分別為 4、6 和 5 位數，以空格或連字號隔開。
	6011 1234 5678 9012	發現卡： 任何 16 位數字，開頭為 6011，分成 4 組 4 位數，以空格或連字號隔開。
	6011-1234-5678-9012	
	2014 123456 78901	Enroute 卡： 任何 15 位數字，開頭為 2014 或 2149，分成三組，分別為 4、6 和 5 位數，以空格或連字號隔開。
	2149-123456-78901	
	3123 4567 8901 1234	JCB 卡： 任何 16 位數字，分成 4 組 4 位數，以空格或連字號隔開，開頭為 3；或任何 15 位數字，開頭為 2131 或 1800，後接 11 位數字。
	3123-4567-8901-1234	
	213112345678901 1800123245678901	

系統樣式	範例	說明
電子郵件	jabberwocky @symantec.com mister_smith @senate.gov tom.swift @gadgets.arpa t-rex9@nature. museum harry@hogwarts.edu.uk	任何英數字串，以底線 (_)、連字號 (-) 或句點隔開，後接 @ 符號及英數字串、一個句點和所列出的其中一個網域名稱延伸。 Symantec Messaging Gateway 無法驗證兩個字母的最上層網域，其中一個或兩個字母為大寫。不過，它可以驗證大寫的三字母網域。例如，它不會驗證 harry@hogwarts.edu.UK 或 bilbo@canterbury.ac.Nz。但是，Symantec Messaging Gateway 會驗證 mister_smith @senate.GOV。
IP 位址	1.2.3.4 10.0.0.0 18.255.30.41 10.0.10.0/24 10.0.10.0/1 10.0.10.0/0	任何 4 組數字，前三組是 1 位、2 位或小於 256 的 3 位數，以句點隔開。 CIDR 位址範圍可以用 0 至 32 (含) 的 1 或 2 位數表示，且與開頭 IP 位址之間以正斜線隔開。 若終端字元不是前面有正斜線的 1 或 2 位數字，Symantec Messaging Gateway 便不會進行剖析。因此，10.113.14.10a 不會視為有效的 IP 位址。
數字	10 10.99 0.33 9999 10,000 6.999,66 99.999.999 -9,999 -10.99	Symantec Messaging Gateway 可辨識歐式數字 (其中逗號作為小數點，句點則隔開 3 位數的群組)。小數前面必須有數字，必要時包括零 (0) 在內，並以十進位表示。 雖然支援含逗號的 8 位數或更小數字，賽門鐵克建議您使用 Tab 或 | 分隔的資料來源文字檔，其中包含使用逗號的數字。使用 Tab 或管道字元分隔符號可避免數字中的逗號被誤認為是欄位分隔符號。 會將大於 8 位的數字解譯為 WORD 類型。

系統樣式	範例	說明
百分比	76% 23.4% 56.78% -1.089,01% -0.32%	Symantec Messaging Gateway 可辨識歐式數字(其中逗號作為小數點，句點則隔開 3 位數的群組)。百分比的小數前面必須有數字，必要時包括零 (0) 在內，並以十進位表示。只有與百分比符號 (%) 相鄰的數字 (不含空格) 才視為有效的百分比。 下列樣式不會產生相符項目： .32 32% 32per 5 3/4%
台灣電話號碼	(238) 832 5555 (238) 832-5555 238-832-5555 238 8325555 1-238-832-5555 238.832.5555 1 - (238) 8325555 1 - (238) 832-5555 1 - (238) 832 5555	任何 10 位數電話號碼，開頭為 2-9，及/或前面加 1，後面接著連字號，或是空格、連字號、空格。3 位數區碼可以包含 (也可以不包含) 在括弧中，後接空格、連字號或句點，7 位數字分成 3 位數和 4 位數的群組，中間用空格、連字號或句點隔開，也可以完全不隔開。
台灣郵遞區號	90210 89412-4321	任何 5 位數郵遞區號或 5 位數代碼加 4 位數延伸碼的組合 (以連字號隔開)。
SSN/ITIN	777-77-7777 777 77 7777 123456789	任何 9 位數字，可以是連續的，也可以分成 3 組 3、2 和 4 位數，以空格或連字號隔開。第一組 3 位數不得為 000。第二組數字必須大於或等於 1，最後一組數字必須大於 0。

請參閱第 308 頁的「關於對應資料來源檔案欄」。

請參閱第 307 頁的「將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位」。

上載資料來源檔案

對應資料來源檔案欄之後，您必須上載資料來源檔案。如果上載失敗，則會顯示錯誤訊息，指出失敗原因。如果上載成功，則 Symantec Messaging Gateway 會編製該記錄的索引。和未

編製索引的記錄相比，為記錄編製索引可協助 Symantec Messaging Gateway 更快在資料來源檔案中找到對應列。

請參閱第 307 頁的「將資料來源檔案欄對應到 Symantec Messaging Gateway 中的欄位」。

請參閱第 314 頁的「修改記錄」。

「記錄資源狀態」頁面會顯示上載程序的狀態。它會顯示上載程序的開始和完成時間，也會指出上載成功與上載失敗的列數。

上載大型資料來源檔案可能需要大量的處理能力，而且可能相當耗時。請考慮在離峰時間上載資料來源檔案。

附註：Symantec Messaging Gateway 不支援上載超過 1.5 GB 的資料來源檔案。

若要上載記錄，您必須具有「完整的管理」權限或修改設定的權限。

上載資料來源檔案

1. 在**「編輯記錄資源」**頁面的**「記錄資源資料來源」**下方，按下**「瀏覽」**以尋找想要上載的資料來源檔案。
2. 按下**「上載」**。

   成功上載記錄之後，您必須將該記錄複寫到掃描程式。

   請參閱第 313 頁的「複寫記錄」。

複寫記錄

成功上載資料來源檔案之後，您必須將該檔案複寫到所有掃描程式。將大型記錄傳送至一或多個掃描程式，可能會花費相當大量的時間和處理資源。因此，Symantec Brightmail Gateway 可讓您在建立新記錄時複寫記錄，或是稍後再進行複寫。

請參閱第 312 頁的「上載資料來源檔案」。

「記錄資源狀態」頁面會顯示狀態、複寫的開始和結束時間，以及複寫的記錄大小。

若要複寫記錄，您必須具有「完整的管理」權限或修改設定的權限。

建立新記錄時複寫記錄

1. 在**「記錄資源狀態」**頁面的**「處理中狀態」**下，確定狀態是**「已完成」**。
2. 在**「複寫狀態」**下，按下**「立即複寫」**。
3. 成功完成複寫後，請按下**「確定」**。

稍後複寫記錄

1. 在控管中心內，按下**「內容」>「資源」>「記錄」**。
2. 勾選要複寫之記錄旁的方塊，然後按下**「狀態詳細資料」**。

3 如果「**記錄資源狀態**」頁面顯示資料來源檔案已經上載，請在「**複寫狀態**」下，按下「**立即複寫**」。

如果狀態是「**上載失敗**」，則您必須嘗試再次上載資料來源檔案，才能再複寫該檔案。

請參閱第 312 頁的「上載資料來源檔案」。

4 按下「**確定**」。

若要取消記錄資源複寫到所有已啟用的掃描程式，按下「**取消複寫**」。

複寫記錄之後，請建立檢視。

請參閱第 315 頁的「關於記錄檢視」。

請參閱第 318 頁的「建立記錄檢視」。

修改記錄

只要沒有進行中或擱置中的記錄上載，就可以修改記錄。修改記錄後，您必須再次上載和複寫記錄。

參照某個記錄檢視的政策會繼續使用該記錄的現有資料，直到 Symantec Messaging Gateway 上載、編製索引及複寫新的資料為止。如果變更記錄的名稱，參考該記錄之檢視的所有條件都會反映出名稱變更。

此外，如果您修改任何對應，則在更新期間，政策條件參照的任何現有檢視仍然保持有效。上載和複寫更新的記錄之後，所有先前定義的政策都仍然保持有效。新欄欄位可用來建立檢視。

如果某個具名的欄位是任何現有檢視的一部分，則不能從該記錄中刪除該欄位。無論政策條件是否參照該檢視，此限制皆適用。如果嘗試刪除這類欄位，則 Symantec Messaging Gateway 會在「**編輯記錄資源**」頁面上方顯示一則錯誤訊息。

請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

請參閱第 315 頁的「刪除記錄」。

修改記錄

1 在控管中心內，按下「**內容**」>「**資源**」>「**記錄**」。

2 勾選您要修改之記錄旁的方塊，然後按下「**編輯**」。

您也可以按下記錄的名稱來加以編輯。

3 在「**編輯記錄資源**」頁面上，進行所需的變更，然後按「**下一步**」。

請參閱第 306 頁的「建立結構化資料的記錄」。

4 在「**編輯記錄資源**」頁面的「**記錄資源資料來源**」下方，按下「**瀏覽**」以尋找想要上載的資料來源檔案。

5 按下「**上載**」。

請參閱第 312 頁的「上載資料來源檔案」。

6 在「**記錄資源狀態**」頁面的「**處理中狀態**」下，確定狀態是「**已完成**」。

7 在「**複寫狀態**」下，按下「**立即複寫**」。

8 成功完成複寫後，請按下「**確定**」。

請參閱第 313 頁的「複寫記錄」。

刪除記錄

若要刪除記錄，您必須先從所有內容過濾政策條件中刪除任何記錄的檢視。「**記錄資源檢視**」頁面會列出您所建立的所有檢視。此頁面會指出您已針對檢視選取的欄位數， 同時還會顯示使用該檢視作為條件的政策數。不過，此頁面不會指出哪些政策使用了該檢視。當您嘗試刪除記錄時，Symantec Messaging Gateway 可讓您瞭解哪些政策使用了該記錄的檢視。

若要刪除記錄，您必須具有「完整的管理」權限或修改設定的權限。

刪除記錄

1 在控管中心內，按下「**內容**」>「**資源**」>「**記錄**」。

2 勾選要移除之記錄旁的方塊，然後按下「**刪除**」。

出現在頁面上方的訊息會指出有哪些內容過濾政策使用了從此記錄建立的檢視。請先刪除或修改這些政策中的此條件，再重複此程序。

請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

請參閱第 319 頁的「刪除記錄檢視」。

請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

關於記錄檢視

您必須建立要在內容過濾政策條件中使用的記錄檢視。您可以使用檢視，來指定想要 Symantec Messaging Gateway 在郵件中比對記錄的哪些欄位或欄位組合。

您可以從一項記錄中建立一或多個檢視。多重檢視的好處是可以為一項政策建立數個條件，每個條件還可以使用不同的檢視。多重檢視也可讓您將同一個記錄用於數個政策，每項政策還可以使用不同的檢視。

「**記錄資源檢視**」頁面會列出您所建立的所有檢視。此頁面會指出您已針對檢視選取的欄位數， 同時還會顯示使用該檢視作為條件的政策數。

表 15-6 說明用來建立檢視的選項， 並提供範例。為了舉例說明，假設有「記錄 A」。同時，假設「記錄 A」及「檢視 A」是用於已啟用的內容過濾政策中。

表 15-6　　如何架構記錄檢視

選項	說明	範例
檢視名稱	您應指定唯一的名稱，說明該檢視的用途。	在我們的範例中，該檢視名稱為「檢視 A」。
欄位選擇	建立檢視時，該記錄對應的所有欄位都會顯示在**「新增記錄資源」**頁面上的**「欄位」**清單。您可以指定要在檢視中使用哪些欄位。	假設「記錄 A」包含以下欄位： ■ 信用卡號碼樣式 ■ 電子郵件樣式 ■ IP 位址樣式 ■ 數字樣式 ■ 百分比樣式 ■ 台灣電話樣式 ■ 台灣郵遞區號樣式 ■ SSN/ITIN 樣式 現在，假設您為此檢視選取了下列欄位： ■ 信用卡號碼樣式 ■ 電子郵件樣式 ■ IP 位址樣式 ■ 台灣電話樣式 ■ 台灣郵遞區號樣式 ■ SSN/ITIN 樣式
要顯示「檢視」所需的最少相符選取欄位數	此選項可指定郵件內必須出現檢視中的多少欄位，才能構成「出現相符」。 例如，假設您為檢視選取了六個欄位，而**「出現所需之相符的所選欄位數目下限」**為四。如果郵件中找到所選取的四個欄位 (或更多欄位) 中的任一欄位，則 Symantec Messaging Gateway 就會視為出現一次相符。 出現相符並不代表違規。建立使用此檢視的政策時，您可以指定違反政策之前，郵件中可以出現相符的次數。 請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。	假設您將**「出現所需之相符的所選欄位數目下限」**指定為三。出現三個或超過三個相符欄位的郵件就視為出現一次相符。 所以，如果郵件中唯一的相符欄位是**「電子郵件地址樣式」**，就不算出現相符。 如果郵件中相符的欄位只有**「電子郵件地址樣式」**及**「台灣電話樣式」**，也不算出現違規。 但是，如果郵件包含**「電子郵件地址樣式」**、**「台灣電話樣式」**及 **SSN/ITIN** 樣式，這樣的結果就算出現相符。

選項	說明	範例
例外組合	某些特定欄位組合在郵件中是可被接受的。所以 Symantec Messaging Gateway 可讓您排除欄位組合，以免將其視為出現相符。 您可以建立多種例外狀況。	假定您建立一個包含**「台灣電話樣式」**及**「電子郵件地址樣式」**的例外狀況。如果 Symantec Messaging Gateway 在郵件中偵測到此欄位組合，就不會視為出現相符。 *範例 1* 包含下列相符欄位的郵件： ■ **電子郵件地址樣式** ■ **台灣電話樣式** ■ **SSN/ITIN 樣式** 因為允許使用**「台灣電話樣式」**及**「電子郵件地址樣式」**的組合，所以不會偵測到出現相符。因此，只有以下項目相符：(1)**「SSN/ITIN 樣式」**和**「台灣電話樣式」**，以及 (2)**「SSN/ITIN 樣式」**和**「電子郵件地址樣式」**。這兩個相符項目都只有兩個樣式，少於三個樣式的臨界值。 *範例 2* 包含下列相符欄位的郵件： ■ **電子郵件地址樣式** ■ **台灣電話樣式** ■ **SSN/ITIN 樣式** ■ **台灣郵遞區號樣式** 會偵測到出現相符。雖然允許使用**「台灣電話樣式」**及**「電子郵件地址樣式」**組合，但不允許使用它們與其他樣式形成的組合。因此，將存在具有下列樣式的相符項目：(1)**「電子郵件地址樣式」**、**「SSN/ITIN 樣式」**和**「台灣郵遞區號樣式」**；(2)**「台灣電話樣式」**、**「SSN/ITIN 樣式」**和**「台灣郵遞區號樣式」**。
		範例 3 包含下列相符欄位的郵件： ■ **台灣電話樣式** ■ **SSN/ITIN 樣式** ■ **台灣郵遞區號樣式** ■ **IP 位址樣式** 會偵測到出現相符。郵件含有四個相符的欄位 (超過出現相符的臨界值) 且其中沒有任何相符欄位屬於例外狀況。

請參閱第 302 頁的「在內容過濾政策中使用結構化資料」。

請參閱第 308 頁的「關於對應資料來源檔案欄」。

請參閱第 318 頁的「建立記錄檢視」。

建立記錄檢視

將記錄複寫至掃描程式之後，您可以定義檢視。檢視可用於識別內容過濾政策條件中會使用關聯記錄中的哪些欄位。Symantec Brightmail Gateway 使用檢視 (而非記錄) 來建立政策條件，因此，必須為每個記錄至少建立一個檢視。

請參閱第 313 頁的「複寫記錄」。

請參閱第 315 頁的「關於記錄檢視」。

請參閱第 318 頁的「編輯記錄檢視」。

建立檢視

1. 在控管中心內，按下**「內容」>「資源」>「記錄」**。
2. 在**「記錄」**頁面上，勾選您要為其建立檢視之記錄旁邊的方塊。
3. 按下**「檢視」**。
4. 在**「記錄資源檢視」**頁面上，按下**「新增」**。
5. 在**「檢視名稱」**欄位中，輸入檢視的唯一名稱。
6. 在**「欄位選擇」**下，勾選您要包含在此檢視中的欄位。
7. 在**「出現所需之相符的所選欄位數目下限」**方塊中，指定郵件中必須符合多少個欄位，才會出現。
8. 若要建立例外狀況，請在**「例外組合」**下，按下**「新增」**。
9. 選取您要省略符合評估之欄位的組合。
10. 按下**「儲存」**。
11. 在**「新增記錄資源」**頁面上，按下**「儲存」**。

    建立檢視之後，可以在內容過濾政策條件中進行使用。

    請參閱第 278 頁的「建立內容過濾政策」。

編輯記錄檢視

您隨時可以修改檢視。您也可以新增、編輯或刪除**「例外組合」**。修改檢視時，變更會自動傳用至使用該檢視的任何內容過濾政策。

請參閱第 315 頁的「關於記錄檢視」。

請參閱第 318 頁的「建立記錄檢視」。

請參閱第 319 頁的「刪除記錄檢視」。

編輯檢視

1. 在控管中心內，按下**「內容」>「資源」>「記錄」**。
2. 在**「記錄」**頁面上，勾選包含您要編輯之檢視的記錄旁的方塊。
3. 按下**「檢視」**。
4. 在**「記錄資源檢視」**頁面上，勾選您要編輯之檢視旁的方塊。
5. 按下**「編輯」**。
6. 對名稱、欄位以及顯示檢視需達到之所選欄位數量下限進行所需變更。
7. 執行下列其中一個工作：

新增例外組合	執行下列所有工作： ■ 在**「例外組合」**下，按下**「新增」**。 ■ 選取您要省略符合評估之欄位的組合。 ■ 按下**「儲存」**。
修改現有的例外組合	執行下列所有工作： ■ 在**「例外組合」**下，勾選您要編輯之例外組合旁的方塊。 ■ 按下**「編輯」**。 ■ 選取您要省略符合評估之欄位的組合。 ■ 按下**「儲存」**。
刪除現有的例外組合	執行下列所有工作： ■ 在**「例外組合」**下，勾選您要刪除之例外組合旁的方塊。 ■ 按下**「刪除」**。

8. 在**「記錄資源檢視」**頁面上，按下**「儲存」**。

刪除記錄檢視

若要刪除檢視，您必須先從使用該檢視的任何內容過濾政策條件中，將該檢視刪除。**「記錄資源檢視」**頁面會列出您所建立的所有檢視。 此頁面會指出您已針對檢視選取的欄位數， 同時還會顯示使用該檢視作為條件的政策數。不過，此頁面不會指出哪些政策使用了該檢視。Symantec Messaging Gateway 會在您嘗試刪除檢視時，讓您知道哪些政策使用該檢視。

請參閱第 315 頁的「關於記錄檢視」。

請參閱第 315 頁的「刪除記錄」。

請參閱第 318 頁的「編輯記錄檢視」。

刪除檢視

1 在控管中心內，按下**「內容」>「資源」>「記錄」**。

2 在**「記錄」**頁面上，勾選包含您要刪除之檢視的記錄旁的方塊。

3 按下**「檢視」**。

4 在**「記錄資源檢視」**頁面上，勾選您要刪除之檢視旁的方塊。

5 按下**「刪除」**。

頁面最上方會顯示一則訊息，指出含有條件使用此檢視的內容過濾政策。請先刪除或修改這些政策中的此條件，再重複此程序。

請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

處理內容過濾違規通知

表 15-7說明您可對內容過濾違規通知執行的動作。您可以視需要以任何順序執行這些工作。

表 15-7 您可對內容過濾違規通知執行的動作

工作	說明
深入瞭解何謂內容過濾政策違規通知。	通知就是在違反內容過濾政策，且政策動作為**「傳送通知」**時所傳送的郵件。 請參閱第 321 頁的「關於政策違規通知」。
建立政策違規通知。	通知可以傳送給下列任何人： ■ 郵件寄件者 ■ 郵件收件者 ■ 第三方 (例如管理員) 請參閱第 321 頁的「建立政策違規通知」。
視需要修改現有政策違規通知。	您可以視需要修改預先定義及自訂的政策違規通知，但無法變更預先定義之政策違規通知的通訊協定。 請參閱第 323 頁的「編輯政策違規通知」。
刪除不再需要的政策違規通知。	如果您不再需要政策違規通知，可將其刪除。若要刪除政策違規通知，您必須先從使用該通知的任何內容過濾政策動作中，將該通知刪除。當您嘗試刪除通知時，Symantec Messaging Gateway 會告知您哪些政策使用該通知。 請參閱第 324 頁的「刪除政策違規通知」。

關於政策違規通知

通知就是在違反政策，且政策動作為**「傳送通知」**時所傳送的郵件。通知與註釋不同，註釋是新增至郵件的內容，而通知則是單獨的一封郵件。當您指定傳送通知時，除非指定執行其他的動作，否則會將原始郵件傳送給原始收件者。通知適用於任何類型的政策。您可以在指定政策的動作時，選取所要使用的表示法。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

請參閱第 285 頁的「政策動作及其功能」。

Symantec Brightmail Gateway 提供了數種預先定義的通知，供您使用。您也可以建立自己的通知郵件。可以修改預先定義的通知，但只有在不使用於政策時，才能將其刪除。

通知可以傳送給下列任何人：

- 郵件寄件者
- 郵件收件者
- 第三方 (例如管理員)

您可以使用變數自訂通知郵件主旨和內文文字。例如：

```
The message concerning $subject$ sent by $sender$
to $recipients$ was stripped of $attachments$.
```

請參閱第 321 頁的「建立政策違規通知」。

建立政策違規通知

通知是預先定義的郵件，當郵件符合政策條件且動作為傳送通知時，SMG 即會傳送該郵件。當您建立通知時，您指定的通知名稱會出現在**「通知」**頁面上。如果針對信譽、垃圾郵件、惡意軟體、威脅防禦或內容過濾政策選擇**「傳送通知」**動作，此名稱還會出現在**「通知」**清單中。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

通知的收件者可以回覆傳送通知的電子郵件地址。回覆會送往信封地址，而不是 From: 標頭地址。作為最佳實務準則，請為受監控的帳戶提供電子郵件地址，或是在通知中納入回應不受監控的聲明。

使用電子郵件通知變數可以自訂通知主旨文字和內文文字。您可以在文字中使用一或多個通知變數，也可以不使用通知變數。

表 15-8 列出了您可以用於自訂郵件主旨文字和內文文字，以及將標籤取代為哪些內容的通知變數。

表 15-8 電子郵件通知變數屬性

屬性名稱	變數標籤	郵件結果
寄件者	$sender$	在傳送的通知郵件中，會將此變數標籤取代為寄件者的電子郵件地址。
收件者	$recipients$	在傳送的通知郵件中，會將此變數標籤取代為收件者電子郵件地址的逗號區隔清單。
主旨	$subject$	在傳送的通知郵件中，會將此變數標籤取代為原始郵件的主旨行。
附件名稱	$attachments$	在傳送的通知郵件中，會將此變數標籤取代為原始郵件最上層附件的逗號區隔清單。
郵件 ID	$messageid$ **附註：**此變數不會顯示在**「包括郵件屬性 (選用):」**功能表中。若要將其新增至通知，您必須在通知主旨或內文文字中輸入此變數標籤。	在傳送的通知郵件中，會將此變數標籤取代為原始郵件的郵件 ID。 對於管理員來說，郵件 ID 是通知中最有用的內容。當郵件的其他相關資訊在系統中傳遞時，管理員可以使用郵件 ID 快速追蹤此資訊。

若要建立通知，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 321 頁的「關於政策違規通知」。

建立政策違規通知

1 在控管中心內，按下**「內容」>「資源」>「通知」**。

2 按下**「新增」**。

3 在**「通知說明」**方塊中，輸入通知的名稱。

您的說明不能超過 255 個字元。

4 在**「寄件者」**方塊中，輸入要顯示在通知郵件之 `From` 標頭的電子郵件地址。

指定包括網域名稱在內的完整電子郵件地址，例如 admin@symantecexample.com。

5 在「**傳送到**」下，選取下列其中一個或多個選項：

寄件者	勾選這個方塊，將通知傳送給郵件信封中列出的寄件者 (而非 From: 標頭中列出的寄件者)。
收件者	勾選這個方塊，將通知傳送給郵件信封中列出的收件者 (而非 To: 標頭中列出的收件者)。
其他	勾選這個方塊，將通知傳送給您指定的一或多個完整的電子郵件地址。然後，輸入電子郵件地址。請以逗號、分號或空格分隔多個電子郵件地址。

6 在「**主旨**」下方，按下「**編碼**」下拉式清單，以變更通知主旨行的字元編碼。

7 (可選)按下「**包括郵件屬性**」下拉式清單，以選取要包含在主旨行中的變數類型，然後按下「**新增**」。

變數會顯示在「**主旨**」文字方塊中。

8 在「**主旨**」文字方塊中，輸入通知郵件的主旨標頭文字。

9 在「**內文**」下方，按下「**編碼**」下拉式清單，以變更通知內文的字元編碼。

10 (可選)按下「**包括郵件屬性**」下拉式清單，以選取要包含在內文中的變數類型，然後按下「**新增**」。

變數會顯示在「**郵件內文**」文字方塊中。

11 在「**郵件內文**」文字方塊中，輸入通知郵件的內文文字。

12 選擇性地勾選「**附加原始郵件**」，將原始郵件附加至通知郵件。

13 按下「**儲存**」。

編輯政策違規通知

您可以視需要修改預先定義及自訂的政策違規通知，但無法變更預先定義之政策違規通知的通訊協定。

若要編輯政策違規通知，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 321 頁的「建立政策違規通知」。

請參閱第 324 頁的「刪除政策違規通知」。

編輯政策違規通知

1 在控管中心內，按下「**內容**」>「**資源**」>「**通知**」。

2 勾選您要編輯之通知旁的方塊。

3 按下「**編輯**」。

您也可以按下想要編輯的通知。

4 進行所需的變更。

5 按下「**儲存**」。

刪除政策違規通知

如果您不再需要政策違規通知，可將其刪除。若要刪除政策違規通知，您必須先從使用該通知的任何內容過濾政策動作中，將該通知刪除。當您嘗試刪除通知時，Symantec Messaging Gateway 會告知您哪些政策使用該通知。

若要刪除政策違規通知，您必須具有「完整的管理」權限或修改政策的權限。

刪除政策違規通知

1 在控管中心內，按下「**內容**」>「**資源**」>「**通知**」。

2 勾選您要刪除之通知旁的方塊。

3 按下「**刪除**」。

頁面頂端會顯示一則訊息，指出其中有動作使用此通知的內容過濾政策。 請先刪除或修改這些政策中的此動作，再重複此程序。

請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

請參閱第 321 頁的「關於政策違規通知」。

使用辭典

您可以使用禁用詞語辭典，並將其套用至內容過濾政策條件。

表 15-9說明您可使用內容過濾辭典的所有方式。您可視需要依任何順序執行任何工作。

表 15-9 使用辭典

工作	說明
瞭解 Symantec Messaging Gateway 如何在內容過濾政策規則中使用辭典。	辭典是有關特定主題之單字、詞組、檔案名稱和副檔名的清單。當辭典包含在內容過濾政策條件中時，Symantec Messaging Gateway 就會搜尋電子郵件，尋找其中是否有辭典的內容。 請參閱第 325 頁的「關於內容過濾辭典」。 請參閱第 327 頁的「使用辭典時的考量」。 請參閱第 333 頁的「高階與自訂內容過濾辭典」。
依據辭典中的內容掃描文字檔案。	Symantec Messaging Gateway 可以依據辭典檢查非純文字檔案的任何檔案附件。雖然掃描非純文字檔案會將內容過濾的效果提高到最大，但也會對系統負載造成影響，並降低效能。 請參閱第 328 頁的「在非純文字檔案附件中掃描內容過濾違規」。

工作	說明
將單字或詞組匯入或匯出辭典。	當您設定新的控管中心及掃描程式部署時，此功能會很有幫助。假設現有的控管中心及掃描程式部署中包含了某些辭典單字與詞組，而您想要將這些單字與詞組用於新的部署中。您可以匯出想用於新部署中的單字與詞組。接著，您可以透過控管中心的電腦，將該些單字與詞組匯入新的部署中。 請參閱第 328 頁的「從辭典匯出單字或詞組」。 請參閱第 330 頁的「將單字或詞組匯入辭典中」。
啟用或停用辭典中的單字和詞組。	預先定義的單字和詞組是指 Symantec Messaging Gateway 所提供的單字或詞組。您無法刪除預先定義的辭典單字或詞組。但是，您可以將不想用於內容過濾政策的預先定義的單字或詞組停用。 請參閱第 329 頁的「停用和啟用辭典中預先定義的單字或詞組」。
建立您自己的辭典。	Symantec Messaging Gateway 提供高階辭典和自訂辭典，供您在內容過濾政策中使用。但是，您可以建立自己的使用者定義辭典，以符合您的特定需求。 請參閱第 329 頁的「建立使用者定義的辭典」。
視需要編輯辭典。	您可以視需要修改任何類型的辭典 (高階、自訂、使用者定義)。 請參閱第 331 頁的「編輯辭典」。
從辭典中刪除使用者定義的單字或詞組。	使用者定義的單字或詞組，就是您新增至任何類型的辭典 (進階、自訂及使用者定義) 的單字或詞組。如果您不再需要使用者定義的單字或詞組，可將其刪除。 請參閱第 331 頁的「從辭典中刪除使用者定義的單字或詞組」。
尋找辭典中的單字或詞組。	您有時可能會想要啟用或停用、修改或刪除多個辭典中的某個單字或詞組。Symantec Messaging Gateway 可讓您搜尋所有類型辭典 (高階、自訂及使用者定義) 中使用的單字與詞組。 請參閱第 332 頁的「尋找辭典中的單字或詞組」。
刪除辭典。	除非自訂過濾政策中使用了任何您建立的使用者定義辭典，否則您可以加以刪除。 請參閱第 332 頁的「刪除辭典」。

關於內容過濾辭典

辭典是有關特定主題之單字、詞組、檔案名稱和副檔名的清單。當辭典包含在內容過濾政策條件中時，Symantec Messaging Gateway 就會搜尋電子郵件，尋找其中是否有辭典的內容。如果您架構 Symantec Messaging Gateway 掃描非純文字檔案附件，則也會掃描這些附件是否含有辭典內容。

請參閱第 328 頁的「在非純文字檔案附件中掃描內容過濾違規」。

內容過濾政策會使用子字串文字分析而非規則運算式分析，來評估參考辭典的相符項。當郵件中有子字串符合辭典項目時，Symantec Messaging Gateway 就會採取政策中指定的動作。

為了符合辭典，單字僅包含英數字元 A-Z、a-z 和 0-9。所有其他字元均為分隔符號。例如，在辭典中搜尋單字「bad」會偵測到相符項 (如變體「bad_guy」)，因為底線將被視為單字分隔符號。但是，「bad1」不會偵測到相符項，因為數字「1」被視為單字的一部分。

辭典項目可能包含分隔符號。如果辭典術語 (例如，「chocolate ice cream is tasty!」或「pls call me (415-738-2623) ASAP!)」的任一邊存在分隔符號字元，則辭典術語「ice cream」或「415-738-2623」可能符合郵件。「pls call me (415-738-2623x12) ASAP!」等變體將不符合，因為「x12」被視為單字「2623x12」的一部分。

您可使用的辭典類型如下：

高階辭典和自訂辭典

Symantec Messaging Gateway 所提供的高階辭典和自訂辭典大多已經包含預先定義的單字、詞組和字元。您可以檢視高階辭典和自訂辭典的內容，啟用和停用現有的關鍵字，以及新增單字、詞組或字元。

請在使用前，先檢查高階辭典和自訂辭典的內容，以確定其是否符合您的需求。 如果不符合，您可以新增所需的新使用者所定義單字和詞組。 您也可以停用不想使用的預先定義單字和詞組。

某些高階辭典和自訂辭典是空的。 您必須先將使用者定義的單字或詞組填入這些辭典，才能在內容過濾政策中使用它們。

附註：標記為 ambiguous 的辭典 (例如 **Profanity (ambiguous)**) 所包含的辭彙，在特定情況下使用時可能是合法的。

請參閱第 333 頁的「高階與自訂內容過濾辭典」。

使用者定義的辭典

除了高階辭典和自訂辭典，您還可以建立使用者定義的辭典。 您可以填入使用者定義的辭典以符合網站特定需求或業務需求。 這些辭典必須至少包含一個單字或詞組。

表 15-10 描述了使用不同類型的辭典可以執行的工作。

表 15-10 根據類型使用辭典可以執行的工作

工作	高階或自訂	使用者定義
建立新辭典 請參閱第 329 頁的「建立使用者定義的辭典」。		X
編輯辭典 請參閱第 331 頁的「編輯辭典」。	X	X
刪除辭典 請參閱第 332 頁的「刪除辭典」。		X
將單字或詞組匯入辭典 請參閱第 330 頁的「將單字或詞組匯入辭典中」。	X	X

工作	高階或自訂	使用者定義
從辭典匯出單字或詞組 請參閱第 328 頁的「從辭典匯出單字或詞組」。	X	
啟用和停用辭典中的單字和詞組 請參閱第 329 頁的「停用和啟用辭典中預先定義的單字或詞組」。		X
刪除辭典中的單字或詞組 請參閱第331頁的「從辭典中刪除使用者定義的單字或詞組」。	X	
搜尋辭典中的單字或詞組 請參閱第 332 頁的「尋找辭典中的單字或詞組」。	X	X

請參閱第 327 頁的「使用辭典時的考量」。

使用辭典時的考量

請注意以下關於辭典的額外資訊：

- 單字必須與辭典中所顯示的單字完全相符，才能夠偵測出來。辭典中的單字若有變化形 (例如動詞時態)，將會無法偵測。例如，selling 與 sell 不相符。
- 辭典不支援萬用字元。
- 最多支援 100 個辭典，每個辭典可容納高達 10,000 個字詞。
- 辭典中的單字與詞組無法設定優先順序。
- 一個辭典可以在多個內容過濾政策中使用。
- 將單字新增至辭典時，請注意，某些字可能會同時視為錯用和合法，須從上下文判斷。 例如，breast 可能被視為非適當用字，但結合 cancer 後就是適當的。
- Symantec Brightmail Gateway 不會在 HTML 郵件或附件的 HTML 標頭或標籤中搜尋辭典相符項目。
- 單字並不區分大小寫。
- 標點符號字元 (例如問號 (?)) 不可用作單字的第一個字元。

請參閱第 325 頁的「關於內容過濾辭典」。

請參閱第 329 頁的「建立使用者定義的辭典」。

在非純文字檔案附件中掃描內容過濾違規

Symantec Messaging Gateway 可根據辭典檢查任何檔案附件中的文字 (例如 list.example.org) 以偵測內容過濾違規。雖然掃描檔案附件會將內容過濾的效果提高到最大，但也會對系統負載造成影響，並降低效能。

請參閱第 324 頁的「使用辭典」。

請參閱第 276 頁的「關於內容過濾」。

在檔案附件中掃描內容過濾違規

1 按下「**通訊協定**」**> SMTP >**「**設定**」，然後按下「**內容掃描**」標籤。

2 勾選「**啟用在附件中掃描辭典文字的功能**」。

3 按下「**儲存**」。

從辭典匯出單字或詞組

Symantec Messaging Gateway 可讓您從自訂辭典匯出單字與詞組。匯出的單字與詞組預設會儲存到名為 `DictionaryWords.txt` 的文字檔案中。您無法選擇匯出特定單字或詞組。您必須匯出辭典中的所有單字與詞組。

附註：您無法從高階辭典中匯出單字或詞組。

當您設定新的控管中心及掃描程式部署時，此功能會很有幫助。假設現有的控管中心及掃描程式部署中包含了某些辭典單字與詞組，而您想要將這些單字與詞組用於新的部署中。您可以匯出想用於新部署中的單字與詞組。接著，您可以透過控管中心的電腦，將該些單字與詞組匯入新的部署中。

請參閱第 330 頁的「將單字或詞組匯入辭典中」。

您可能想在刪除自訂辭典之前先將其匯出，以保留作為記錄。如有需要，您也可以還原匯出的檔案。

請參閱第 332 頁的「刪除辭典」。

若要從自訂辭典匯出單字或詞組，您必須具有「完整的管理」權限或修改設定的權限。

從辭典匯出單字或詞組

1 在控管中心內，按下「**內容**」>「**資源**」>「**辭典**」。

2 勾選含有您要匯出的單字或詞組之辭典旁的方塊，然後按下「**編輯**」。

3 按下「**匯出**」。

4 在「**檔案下載**」對話方塊中，按下「**儲存**」。

5 在「**另存新檔**」對話方塊中，輸入檔案名稱，並選取您要儲存檔案的位置。

6 按下「**儲存**」。

7 在「**下載已完成**」對話方塊中，按下「**開啟**」來檢視文字檔案，或按下「**關閉**」來關閉對話方塊。

停用和啟用辭典中預先定義的單字或詞組

預先定義的單字和詞組是指 Symantec Brightmail Gateway 所提供的單字或詞組。 您無法刪除預先定義的辭典單字或詞組。但是，您可以將不想用於內容過濾政策的預先定義的單字或詞組停用。

附註：您無法停用任何辭典 (高階、自訂或使用者定義) 中使用者定義的單字或詞組。 如果不想使用使用者定義的單字，您可以予以刪除。

請參閱第 331 頁的「從辭典中刪除使用者定義的單字或詞組」。

若要啟用或停用預先定義的單字或詞組，您必須具備「完整的管理」權限或修改政策的權限。

請參閱第 325 頁的「關於內容過濾辭典」。

請參閱第 329 頁的「建立使用者定義的辭典」。

停用或啟用辭典中預先定義的單字或詞組

1 在控管中心內，按下「**內容**」>「**資源**」>「**辭典**」。

2 勾選含有您要停用或啟用之單字或詞組的辭典旁的方塊，然後按下「**編輯**」。

請參閱第 332 頁的「尋找辭典中的單字或詞組」。

3 勾選您要啟用或停用之預先定義的單字或詞組旁的方塊。

勾選「**單字或詞組**」以選取清單中的所有單字和詞組。

4 執行下列其中一項工作：

按下「**停用**」。	如果辭典是政策的條件，Symantec Brightmail Gateway 在評估郵件時，不會搜尋此單字或詞組。
按下「**啟用**」。	Symantec Brightmail Gateway 在評估郵件時，會搜尋單字或詞組。

5 按下「**儲存**」。

建立使用者定義的辭典

Symantec Brightmail Gateway 提供高階辭典和自訂辭典，供您在內容過濾政策中使用。但是，您可以建立自己的使用者定義辭典，以符合您的特定需求。

若要新增使用者定義的辭典，您必須具有「完整的管理」權限或是修改政策的權限。

請參閱第 325 頁的「關於內容過濾辭典」。

請參閱第 330 頁的「將單字或詞組匯入辭典中」。

請參閱第 331 頁的「編輯辭典」。

請參閱第 329 頁的「停用和啟用辭典中預先定義的單字或詞組」。

建立使用者定義的辭典

1. 在控管中心內，按下**「內容」>「資源」>「辭典」**。
2. 按下**「新增」**。
3. 在**「辭典名稱」**欄位中，輸入辭典的名稱。
4. 在**「選用說明」**欄位中，輸入辭典的說明。
5. 在**「輸入單字或詞組」**欄位中，輸入您要新增到辭典的單字或詞組。
6. 按下**「新增」**，將單字或詞組新增至**「單字或詞組」**清單中。

   新增後的單字或詞組會自動啟用。
7. 重複步驟 5 和 6，來新增更多單字和詞組。
8. 按下**「儲存」**。

將單字或詞組匯入辭典中

您可以將單字或詞組匯入至所有類型的辭典中 (高階和自訂)。您匯入的檔案必須是 UTF-8 格式的新行分隔文字檔，每個單字或詞組必須獨立成行。該檔案必須能夠由控管中心電腦存取。

附註：不支援有擴充 ASCII 的檔案。

請參閱第 325 頁的「關於內容過濾辭典」。

請參閱第 329 頁的「建立使用者定義的辭典」。

請參閱第 331 頁的「編輯辭典」。

請參閱第 329 頁的「停用和啟用辭典中預先定義的單字或詞組」。

將單字或詞組匯入辭典中

1. 在控管中心內，按下**「內容」>「資源」>「辭典」**。
2. 勾選要匯入單字或詞組的辭典旁的方塊，然後按下**「編輯」**。
3. 在**「新增辭典」**頁面上，按下**「匯入」**。
4. 在**「匯入」**下方，執行下列其中一項工作：
   - 在**「檔案名稱」**方塊中，輸入您要匯入的文字檔案名稱。
   - 按下**「瀏覽」**以尋找您要匯入的文字檔。

依預設啟用新匯入的文字或詞組。

5 按下**「儲存」**。

編輯辭典

您可以視需要修改任何類型的辭典 (高階、自訂、使用者定義)。

請參閱第 329 頁的「建立使用者定義的辭典」。

附註：建立使用者定義的辭典並新增至少一個單字後，您必須永遠在該辭典中至少有一個單字。 如果您不再需要使用者定義的辭典，可以將其刪除。

請參閱第 332 頁的「刪除辭典」。

若要編輯辭典，您必須具有「完整的管理」權限或修改政策的權限。

編輯辭典

1 在控管中心內，按下**「內容」>「資源」>「辭典」**。

2 勾選要編輯的辭典旁的方塊，並按下**「編輯」**。

3 進行所需的修改。

請參閱第 329 頁的「建立使用者定義的辭典」。

請參閱第 330 頁的「將單字或詞組匯入辭典中」。

請參閱第 329 頁的「停用和啟用辭典中預先定義的單字或詞組」。

請參閱第 331 頁的「從辭典中刪除使用者定義的單字或詞組」。

4 按下**「儲存」**。

從辭典中刪除使用者定義的單字或詞組

使用者定義的單字或詞組，就是您新增至任何類型的辭典 (進階、自訂及使用者定義) 的單字或詞組。 如果您不再需要使用者定義的單字或詞組，可將其刪除。

附註：您無法刪除預先定義的單字或詞組。 但是，您可以停用不想用於內容過濾政策中的預先定義的單字或詞組。

請參閱第 329 頁的「停用和啟用辭典中預先定義的單字或詞組」。

若要從辭典中刪除使用者定義的單字或詞組，您必須具有「完整的管理」權限或修改政策的權限。

從辭典中刪除使用者定義的單字或詞組

1 在控管中心內，按下**「內容」>「資源」>「辭典」**。

2 請勾選包含您要刪除的使用者定義的單字或詞組之辭典旁的方塊，然後按下**「編輯」**。

請參閱第 332 頁的「尋找辭典中的單字或詞組」。

3 在**「編輯辭典」**頁面上，勾選您要移除的使用者定義的單字或詞組旁的方塊。

勾選**「單字或詞組」**以選取清單中的所有單字和詞組。

4 按下**「刪除」**。

5 按下**「儲存」**。

尋找辭典中的單字或詞組

您有時可能會想要啟用或停用、修改或刪除多個辭典中的某個單字或詞組。Symantec Brightmail Gateway 可讓您搜尋所有類型辭典 (進階、自訂及使用者定義) 中使用的單字與詞組。

搜尋單字或詞組時，Symantec Brightmail Gateway 會在**「辭典」**頁面頂端顯示一則訊息。該訊息會列出包含該單字或詞組的所有辭典。如果找不到符合項目，則會顯示下列訊息：沒有任何辭典符合單字或詞組。

若要在辭典中搜尋單字或詞組，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 329 頁的「建立使用者定義的辭典」。

在辭典中尋找單字或詞組

1 在控管中心內，按下**「內容」>「資源」>「辭典」**。

2 在**「辭典」**頁面的**「尋找單字或詞組」**欄位中，輸入您要尋找的單字或詞組。

3 按下**「尋找」**。

刪除辭典

除非自訂過濾政策中使用了任何您建立的使用者定義辭典，否則您可以加以刪除。 刪除使用者定義辭典前，您可以先將單字與詞組匯出至文字檔案中，以保留作為記錄。 可視需要重新匯入文字檔案。

附註：您無法刪除高階或自訂的辭典。

請參閱第 328 頁的「從辭典匯出單字或詞組」。

請參閱第 330 頁的「將單字或詞組匯入辭典中」。

若要刪除使用者定義的辭典，您必須從使用該辭典的任何內容過濾政策條件中，將該辭典刪除。 Symantec Messaging Gateway 會在您嘗試刪除辭典時，讓您知道哪些政策使用該辭典。

若要刪除使用者定義的辭典，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 325 頁的「關於內容過濾辭典」。

刪除辭典

1 在控管中心內，按下**「內容」>「資源」>「辭典」**。

2 在**「辭典」**頁面上，勾選要刪除之辭典旁的方塊。

3 按下**「刪除」**。

頁面頂端會出現一則訊息，指出其中有條件使用此辭典的內容過濾政策。請先刪除或修改這些政策中的此條件，再重複此程序。

請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

高階與自訂內容過濾辭典

Symantec Brightmail Gateway 提供了高階辭典與自訂內容過濾辭典，您可以在建立內容過濾政策條件時使用。

請參閱第 325 頁的「關於內容過濾辭典」。

表 15-11 列出了進階辭典和自訂辭典，以及建議的使用這些辭典所藉由的政策範本。

表 15-11 高階辭典、自訂辭典及相關範本

辭典名稱	關聯的範本
ABA 轉帳號碼關鍵字 (ABA Routing Number Keywords)	PIPEDA；員工資料保護；客戶資料保護；SWIFT 代碼；員工資料保護；州資料隱私法；金融服務法案 (Gramm-Leach-Bliley)
關聯網域 (Affiliate Domains)	州資料隱私法
分析師的電子郵件地址 (Analysts' Email Addresses)	NASD 規定 2711 與 NYSE 規定 351 和 472
加州關鍵字 美國伊利諾州關鍵字 (Illinois Keywords) 字母/12 位數 駕照號碼地區關鍵字 (Letter/12 Num. DLN State Words) 美國新澤西州關鍵字 (New Jersey Keywords) 紐約關鍵字 (New York Keywords)	州資料隱私法
加拿大社會保險號碼單字 (Canadian Social Ins. No. Words)	PIPEDA；加拿大社會保險號碼

辭典名稱	關聯的範本
公司名稱關鍵字 (Company Name Keywords) (使用者定義)	SEC 公平揭露規定；沙賓法案 (Sarbanes-Oxley)
競爭對手網域 (Competitor Domains)	競爭對手通訊
機密關鍵字 (Confidential Keywords) (使用者定義) 內部專用關鍵字 (Internal Use Only Keywords) (使用者定義) 專利關鍵字 (Proprietary Keywords) (使用者定義) 禁止散布文字 (Not for Distribution Words) (使用者定義)	機密文件
機密/專利單字 (Confidential/Proprietary Words)	沙賓法案
信用卡號碼關鍵字 (Credit Card Number Keywords)	信用卡號碼；付款卡業界資料安全標準；客戶資料保護；員工資料保護；PIPEDA
設計文件延伸 (Design Documents Extensions)	設計文件
疾病名稱 (Disease Names)	HIPAA (包括 PHI)；考爾迪科特報告
EAR CCL 關鍵字 (EAR CCL Keywords)；EAR 國碼 (EAR Country Codes)	出口管理條例規定 (EAR)
歐盟國碼 (EU Country Codes)	歐盟資料保護指令
財務關鍵字 (Financial Keywords)	沙賓法案 財務資訊
已確認的賭博關鍵字 (Gambling Keywords, Confirmed)；可疑的賭博關鍵字 (Gambling Keywords, Suspect)	賭博
GPG 加密關鍵字 (GPG Encryption Keywords) PGP 檔案副檔名 (PGP file extensions) PGP8 關鍵字 (PGP8 Keywords)	加密的資料
駭客關鍵字 (Hacker Keywords)；鍵盤記錄關鍵字 (Keylogger Keywords)	網路安全
ITAR 國碼 (ITAR Country Codes) ITAR 軍品 (ITAR Munition Names)	國際武器運輸條例規定 (ITAR)

辭典名稱	關聯的範本
教育類職位搜尋關鍵字 (Job Search Keywords, Education) 一般職位搜尋關鍵字 (Job Search Keywords, General) 工作類職位搜尋關鍵字 (Job Search Keywords, Work)	履歷表
合併及收購專案代碼名稱 (& A Project Code Names) (使用者定義)	合併及收購資料
大批量製造的 受管制物品 (Manufd. Controlled Substances) 市售毒品名稱 (Street Drug Names)	違禁藥品
媒體檔副檔名 (Media Files Extensions)	媒體檔
醫學治療關鍵字 (Medical Treatment Keywords)	HIPAA (包括 PHI)
NASD 2711 關鍵字 (NASD 2711 Keywords) (使用者定義)	NASD 規定 2711 與 NYSE 規定 351 和 472
NASD 3010 一般關鍵字 (NASD 3010 General Keywords) NASD 3010 股票關鍵字 (NASD 3010 Stock Keywords) NASD 3010 購買或出售關鍵字 (NASD 3010 Buy/Sell Keywords)	NASD 規定 3010 與 NYSE 規定 342
OFAC 國碼 (OFAC Country Codes) OFAC SDN 國碼 (OFAC SDN Country Codes) SDN 清單 (SDN List)	海外資產控制局 (OFAC)
明顯攻擊性語言 (Offensive Language, Explicit) 一般攻擊性語言 (Offensive Language, General)	攻擊性語言
其他敏感資訊 (Other Sensitive Information)	美國智慧型控制標記 (CAPCO) & DCID 1/7
密碼檔名 (Password Filenames)	密碼檔
處方藥品名稱 (Prescription Drug Names)	HIPAA (包括 PHI) 考爾迪科特報告

辭典名稱	關聯的範本
出版文件副檔名 (Publishing Document Extensions)	出版文件
種族主義語言	種族主義語言
限制的收件者	限制的收件者
SEC 公平揭露關鍵字 (SEC Fair Disclosure Keywords)	SEC 公平揭露規定
機密 (Secret) 最高機密 (Top Secret) 已分類或受限制 (Classified or Restricted)	防禦郵件系統 (DMS) GENSER 分類 美國智慧型控制標記 (CAPCO) & DCID 1/7
敏感關鍵字 (Sensitive Keywords)	電業的 NERC 安全指導原則
敏感專案代碼名稱 (Sensitive Project Code Names)	專案資料
可能 色情關鍵字 (Sex. Explicit Words, Confirmed) 可能 色情關鍵字 (Sex. Explicit Words, Possible) 可能 色情關鍵字 (Sex. Explicit Words, Suspect)	色情語言
原始程式碼延伸 (Source Code Extensions)	原始程式碼
SWIFT 代碼關鍵字 (SWIFT Code Keywords)	SWIFT 代碼
TPO 電子郵件地址 (TPO Email Addresses)	HIPAA (包括 PHI)
英國選民登記號碼單字 (UK Electoral Roll Number Words)	英國選民登記號碼 1998 年資料保護法 1998 年人權法
英國稅務 ID 號碼關鍵字 (UK Tax ID Number Keywords)	英國稅務 ID 號碼 1998 年資料保護法
英國國家保險號碼關鍵字 (UK NIN Keywords)	英國國家保險號碼 1998 年資料保護法 考爾迪科特報告

辭典名稱	關聯的範本
英國關鍵字 (UK Keywords)	英國駕照號碼 英國選民登記號碼 1998 年資料保護法 1998 年人權法
英國護照關鍵字 (UK Passport Keywords)	英國護照號碼 1998 年資料保護法
英國個人資料關鍵字 (UK Personal Data Keywords)	1998 年人權法
美國報稅號碼關鍵字 (US ITIN Keywords)	美國報稅號碼
美國社會安全號碼關鍵字 (US SSN Keywords)	社會安全號碼 員工資料保護
暴力關鍵字 (Violence Keywords) 武器關鍵字 (Weapons Keywords)	暴力與武器
漏洞關鍵字 (Vulnerability Keywords)	電業的 NERC 安全指導原則

使用樣式偵測政策違規

Symantec Messaging Gateway 提供預先定義的基本樣式和高階樣式，供您在內容過濾政策條件中使用。

表 15-12說明您可對樣式執行的動作。您可以視需要以任何順序執行這些工作。

表 15-12　　管理樣式

工作	說明
深入瞭解何謂樣式及如何使用。您也可以瞭解與 Symantec Messaging Gateway 一起安裝的樣式類型。	Symantec Messaging Gateway 提供使用樣式來偵測政策違規的功能。樣式為規則運算式或系統樣式，用來描述一般所知的內容形式，例如信用卡號碼的樣式。Symantec Messaging Gateway 提供預先定義的基本樣式和高階樣式，您也可以建立自己的自訂樣式。 請參閱第 338 頁的「關於樣式」。
建立自訂樣式。	您可以使用從基本樣式或規則運算式複製的語法，來建立自己的自訂樣式。您可以檢視、編輯和刪除自訂樣式。非美國電話號碼的樣式就是自訂樣式的範例。 請參閱第 339 頁的「建立您自己的自訂樣式」。

工作	說明
編輯您的自訂樣式。	您無法編輯基本樣式和高階樣式， 但可以編輯所建立的自訂樣式。 請參閱第 340 頁的「編輯樣式」。
刪除自訂樣式。	您無法編輯基本樣式或高階樣式， 但可以在不再需要時，刪除所建立的自訂樣式。 請參閱第 341 頁的「刪除樣式」。

關於樣式

Symantec Messaging Gateway 提供使用樣式來偵測政策違規的功能。樣式為規則運算式或系統樣式，用來描述一般所知的內容形式，例如信用卡號碼的樣式。Symantec Messaging Gateway 提供預先定義的基本樣式和高階樣式，您也可以建立自己的自訂樣式。

定義政策條件時，您可以在**「內容過濾政策條件」**頁面的**「符合樣式/不符合樣式」**下拉式清單中，找到所有這些樣式。

表 15-13 描述了可使用的樣式類型。

表 15-13 內容過濾政策條件的樣式

樣式	說明
基本	基本樣式為已知且經過效能測試的規則運算式，您可以在政策中使用，也可以在建立自訂樣式時將其用作範例。您可以檢視基本樣式，但是無法編輯或刪除這些樣式。 基本信用卡樣式僅偵測 Visa、Master Card、AMEX 和發現卡。 預先定義的基本樣式及其語法如下： ■ 信用卡 \b(?<!-)((4\d{3})|(5[1-5]\d{2})|(6011))(-?)\d{4}\5\d{4}\5\d{4}(?!-)\b|(\b)(?<!-)3[4,7]\d{13}(?!-)\b ■ 電子郵件地址 \b([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,9})\b ■ 社會安全號碼 \b(?<!-)(\d{3})([-]?)(\d{2})\2(\d{4})(?!-)\b ■ 台灣電話號碼 \b(?<!-)((1([\s.-]?)[2-9]\d{2}\3\d{3}\3\d{4})|([2-9]\d(2)([.-]?)\d{3}\2\d{4})|(\d{3}([.-]?)\d{4}))(?!-)\b ■ 台灣郵遞區號 \b(?<!-)((\d{5})|(\d{5}\-\d{4}))(?!-)\b

樣式	說明
高階	高階樣式除了規則運算式定義，還能執行進一步的檢查和驗證 (例如 Luhn 檢查)，減少誤報的情況。無法檢視、編輯或刪除這些樣式。 可配合使用的預先定義之高階樣式和政策範本的項目如下： ■ 有效的信用卡 信用卡號碼；客戶資料保護；員工資料保護；PIPEDA；州資料隱私法；支付卡業界資料安全標準；金融服務法案 (Gramm-Leach-Bliley) ■ 有效的 IP 位址 網路圖 ■ 有效的社會安全號碼 HIPAA；金融服務法案 (Gramm-Leach-Bliley)；社會安全號碼；美國報稅號碼 (ITIN)；州資料隱私法；客戶資料保護；員工資料保護 **附註：**「有效信用卡」和「有效社會安全號碼」樣式與基本樣式中提供的「信用卡」和「社會安全號碼」樣式不同。有效的樣式包含規則檢查功能，以協助確保其完整性與準確性。
自訂	您可以使用從基本樣式或規則運算式複製的語法，來建立自己的自訂樣式。您可以檢視、編輯和刪除自訂樣式。非美國電話號碼的樣式就是自訂樣式的範例。 若要建構自己的樣式，您應參閱有關規則運算式的進階資源。

請參閱第 278 頁的「建立內容過濾政策」。

請參閱第 339 頁的「建立您自己的自訂樣式」。

請參閱第 340 頁的「編輯樣式」。

請參閱第 341 頁的「刪除樣式」。

建立您自己的自訂樣式

Symantec Messaging Gateway 提供基本樣式和高階樣式，供您在政策條件中參考。Symantec Messaging Gateway 使用這些樣式來搜尋郵件，以尋找您所想要限制之資料的字元樣式。

您可以複製基本樣式的所有或任何部份，以便在您自訂的樣式中使用，或者您也可以使用規則運算式。

請參閱第 338 頁的「關於樣式」。

請參閱第 284 頁的「在內容過濾政策條件中使用規則運算式」。

您可以建立之自訂樣式的一個範例是非美國地區的電話號碼。 例如，澳大利亞有多種電話號碼格式。 其中一種格式遵循以下樣式：nn nnnn nnnn

若要偵測遵循此格式的澳大利亞電話號碼，您可以建立下列樣式：

\b(([(]0\d[)]|0\d)\s)?\d{4}\s\d{4}\b

您的樣式也可以包括含有國碼的格式，以供國際撥號使用。

附註：若要建構自己的樣式，您應參閱有關規則運算式的進階資源。

若要建立自訂樣式，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 340 頁的「編輯樣式」。

請參閱第 341 頁的「刪除樣式」。

建立您自己的自訂樣式

1. 在控管中心內，按下**「內容」>「資源」>「樣式」**。
2. 按下**「自訂」**標籤。
3. 按下**「新增」**。
4. 在**「樣式名稱」**欄位中，輸入自訂樣式的名稱。
5. 在**「規則運算式」**欄位中，輸入規則運算式。
6. 按下**「儲存」**。

編輯樣式

您無法編輯基本樣式和高階樣式，但可以編輯所建立的自訂樣式。您一次只能編輯一個樣式。若要編輯自訂樣式，您必須具有「完整的管理」權限或是修改政策的權限。

編輯樣式

1. 在控管中心內，按下**「內容」>「資源」>「樣式」**。
2. 按下**「自訂」**標籤。
3. 勾選您要編輯之樣式旁的方塊，然後按下**「編輯」**。

   您也可以按下自訂樣式名稱來編輯該樣式。
4. 在**「樣式名稱」**欄位中，依需要編輯樣式名稱。

   若樣式名稱已變更，名稱變更就會傳到參考自訂樣式的所有政策。
5. 在**「規則運算式」**欄位中，依需要編輯規則運算式。
6. 按下**「儲存」**。

請參閱第 338 頁的「關於樣式」。

請參閱第 284 頁的「在內容過濾政策條件中使用規則運算式」。

請參閱第 339 頁的「建立您自己的自訂樣式」。

請參閱第 341 頁的「刪除樣式」。

刪除樣式

您無法編輯基本樣式或高階樣式， 但可以在不再需要時，刪除所建立的自訂樣式。

若要刪除自訂樣式，您必須先從任何使用它的內容過濾政策中，刪除作為條件的該樣式。Symantec Messaging Gateway 會在您嘗試刪除樣式時，讓您知道哪些政策使用該樣式。

若要刪除自訂樣式，您必須具有「完整的管理」權限或是修改政策的權限。

請參閱第 338 頁的「關於樣式」。

刪除樣式

1. 在控管中心內，按下**「內容」>「資源」>「樣式」**。
2. 按下**「自訂」**標籤。
3. 勾選您要刪除之樣式旁的方塊。

   勾選**「樣式」**旁的方塊，以選取所有要刪除的樣式。
4. 按下**「刪除」**。

   頁面最上方會出現一個訊息，指出哪些內容過濾政策中存在使用此樣式的條件。請先刪除或修改這些政策中的此條件，再重複此程序。

請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

請參閱第 338 頁的「關於樣式」。

建立和管理政策違規的註釋

註釋是 Symantec Messaging Gateway 在郵件違反過濾政策時新增至郵件內文的文字。當您建立政策時，可以選取**「新增註釋」**動作，然後從下拉式功能表中選擇註釋。您可以將註釋新增到此功能表，或從**「內容」>「資源」>「註釋」**頁面編輯或刪除現有注釋。

若要新增或編輯註釋，您必須具有「完整的管理權限」或修改政策的權限。

附註：註釋與通知不同。註釋文字會新增至郵件。通知是當違反政策且政策動作為**「傳送通知」**時，所傳送的獨立郵件。

建立註釋

1. 在控管中心內，選取**「內容」>「資源」>「注釋」**。
2. 在**「註釋」**頁面，按下**「新增」**。
3. 在**「新增註釋」**頁面上，輸入註釋的說明。

   當您新增註釋動作至政策時，此說明會出現在下拉式功能表中。
4. 選取編碼類型。

5 在「**純文字 (必要)**」方塊中，輸入您想要新增至郵件的文字。

內容過濾郵件的文字不應超過 65,000 個字元。

當您選取「**新增註釋**」作為政策動作時，您可以選擇在郵件內文的開頭前面新增註釋。或者，您可以將註釋附加至郵件結尾。註釋會出現在郵件內文的單獨一行上。不過，您可以在註釋文字的開頭和結尾新增一個空行或一行破折號，從視覺上更好地與郵件內文區分。

6 (選用) 在 HTML 方塊中，輸入您想要新增至郵件 HTML 部分的文字 (如果存在)。

作為最佳實務準則，純文字郵件和 HTML 郵件應相同。如果不新增 HTML 文字，純文字註釋會新增至 HTML 郵件。

HTML 文字不應超過 128 個字元。您可以使用 HTML 格式標籤，例如此處為粗體文字，但不支援 HTML 結構標籤。

7 按下「**儲存**」。

若要編輯註釋，請在「**內容**」>「**資源**」>「**註釋**」上選取註釋，然後按下「**編輯**」。

若要刪除註釋，請在「**內容**」>「**資源**」>「**註釋**」上選取註釋，然後按下「**刪除**」。

請參閱第 285 頁的「政策動作及其功能」。

使用清單偵測禁止的附件

表 15-14說明您可如何在政策條件中使用附件清單來識別禁止的附件類型。您可以視需要以任何順序執行這些工作。

表 15-14 管理清單

工作	說明
深入瞭解您可以如何在政策中使用附件清單。	附件清單包含您希望 Symantec Messaging Gateway 偵測的副檔名和檔案應用程式類型。您可以使用附件清單作為內容過濾政策的條件。Symantec Messaging Gateway 偵測到附件具有副檔名清單上的副檔名時，會套用您指定的動作。Symantec Messaging Gateway 能根據建立電子郵件附件的應用程式來判斷該附件的類型，而不管其副檔名為何。 請參閱第 343 頁的「關於附件清單」。
建立附件清單。	Symantec Messaging Gateway 提供預先定義的附件清單，您可使用這些清單來建立附件清單，也可建立自訂的附件清單。 請參閱第 351 頁的「建立偵測檔案附件類型的清單」。
修改現有附件清單。	您可以視需要修改現有附件清單。 請參閱第 353 頁的「編輯附件清單」。

工作	說明
刪除您不再需要的自訂附件清單。	如果您不再需要所建立的附件清單，可將其刪除。無法刪除預先定義的附件清單。 請參閱第 354 頁的「刪除附件清單」。
檢視預設附件清單。	本主題說明所有預先定義的附件清單。 請參閱第 344 頁的「預設附件清單」。
瞭解您可以如何在附件清單中使用 Perl 相容規則運算式。	這些主題說明您可在內容過濾政策中使用的 Perl 相容規則運算式以及範例。 請參閱第 354 頁的「Perl 相容規則運算式」。 請參閱第 355 頁的「Perl 相容規則運算式範例」。

關於附件清單

附件清單包含您希望 Symantec Messaging Gateway 偵測的副檔名和檔案應用程式類型。Symantec Messaging Gateway 偵測到附件具有副檔名清單上的副檔名時，會套用您指定的動作。Symantec Messaging Gateway 能根據建立電子郵件附件的應用程式來判斷該附件的類型，而不管其副檔名為何。

您可以使用下列項目的任意組合來建立附件清單：

真實檔案類別

真實檔案類別是類似檔案類型和應用程式所歸入的類別。例如，**「桌上出版」**和**「影片檔」**是真實檔案類別。

真實檔案類型位於真實檔案類別之內。例如，FrameMaker 是「桌面出版」真實檔案類別內的真實檔案類型。

您無法修改真實檔案類別內真實檔案類型的清單。您必須依現狀使用該清單。

真實檔案類型

真實檔案類型包含在真實檔案類別內。真實檔案類型由副檔名或應用程式組成。例如，FrameMaker 是類別**「桌面出版」**內的真實檔案類型。MPEG 電影是類別**「電影檔」**內的真實檔案類型。

您可以新增和刪除真實檔案類型清單中的項目。

附註：「封存檔案」附件清單不支援真實檔案類型 MIME。「文件檔」附件清單則不支援真實檔案類型 HTML。

一般副檔名和 MIME 類型

您可以指定一般副檔名和 MIME 類型。例如，您可以濾除所有 .jpeg 檔案附件，而不管建立它的應用程式為何。

如需 MIME 的技術說明，請參閱下列 RFC：

https://www.ietf.org/rfc/rfc2045.txt

Symantec Messaging Gateway 提供預設的附件清單。您不能修改預設的附件清單，但可以視需要複製它們並修改複本。或者，您也可以建立自己的自訂附件清單。

請參閱第 344 頁的「預設附件清單」。

請參閱第 351 頁的「建立偵測檔案附件類型的清單」。

預設附件清單

表 15-15 說明預設的附件清單。

表 15-15 預設附件清單

附件清單	真實檔案類別	預先定義的真實檔案類型
封存檔	封裝格式	Apple Double、Apple Single、ASCII-armored PGP encoded、ASCII-armored PGP Public Keyring、ASCII-armored PGP signed、BinHex、Compactor / Compact Pro、cpio archive (CHR Header)、cpio archive (CRC Header)、Disk Doubler、GZ Compress、LHA Archive、IBM Lotus Notes Database NSF/NTF、MacBinary、Microsoft Outlook、Microsoft Outlook PST、MIME、OLE Compound Document、PAK/ARC Archive、OpenPGP Message Format (具有新的封包格式)、PGP Compressed Data、PGP Encrypted Data、PGP Public Keyring、PGP Secret Keyring、GP Signature Certificate、PGP Signed and Encrypted Data、PGP Signed Data、RAR、Serialized Object Format (SOF)、SHAR、SMTP、StuffIt (MAC)、SUN PEX Binary Archive、TAR、Unix Compress、UU encoded、WANG Office GDL Header、ZIP Archive、Mac Disk Copy Disk Image File、Microsoft Entourage Database Format、7 Zip Format(7z)、Bzip 2 Compressed File、ISO-9660 CD Disc Image Format、Microsoft Cabinet File (CAB)、Nero Encrypted File(.nef)、Legato EMailXtender Archives Format (EMX)
設計文件	向量圖形格式	Document F97、Lotus Freelance for DOS、Lotus Freelance for OS/2、Lotus Freelance for Windows；Persuasion、Microsoft PPT 2007 XML、Microsoft PPT Macro 2007 XML、Microsoft Visio、PowerPoint 95、PowerPoint 97、PowerPoint MAC、PowerPoint PC、Extensible Forms Description Language (.xfdl, .xfd)、Apple iWork Keynote
設計文件	排程/規劃格式	Microsoft Project 2000、Microsoft Project 4、Microsoft Project 4.1、Microsoft Project 98、Microsoft Project Activity、Microsoft Project Calculation、Microsoft Project Resource、PlanPerfect

附件清單	真實檔案類別	預先定義的真實檔案類型
文件檔		Ability Spreadsheet、ACT、ALIS、Apple Binary Property List Format、Apple iChat、Apple iWork Keynote、Apple iWork Numbers、Apple iWork Pages、AppleWorks、APPLIX ASTERIX、Applix Graphics、Applix Spreadsheets、Applix Words、BlackBerry Activation File (etp.dat)、CDA / DDIF、CEOwrite、COMET TOP、Convergent Technologies DEF Comm.、Corel Presentations、CPT、CSV (逗號分隔值)、Data Interchange Format (DIF)、DCA-FFT (IBM Final Form)、DCA-RFT (IBM Revisable Form)、DCF Script、DCS、DECdx、DG Common Data Stream (CDS)、Display Write、DocuWorks Format (.xdw)、DSA101 (Honeywell Bull)、EBCDIC Text、Electronic Publication、Enable Spreadsheet、Enable Word Processing、Envoy、Extensible Forms Description Language (.xfdl、.xfd)、Folio Flat File、Founder Chinese E-paper Basic (ceb)、FrameMaker、FrameMaker Book、Harvard Graphics、Health level7 message、HP Word PC、HWP(Arae-Ah Hangul)、IBM 1403 Line Printer IBM Writing Assistant、ICHITARO V4-10、IFilter、Interleaf、Lotus 1-2-3、Lotus 1-2-3 97、Lotus 1-2-3 Formatting、Lotus 1-2-3 Release 9、Lotus Ami Pro、Lotus Ami Pro Style Sheet、Lotus Freelance 96、Lotus Freelance 97、Lotus Freelance for DOS、Lotus Freelance for OS/2、Lotus Freelance for Windows、Lotus Notes CDF、Lotus Word Pro 96、Lotus Word Pro 97、Lyrix Word Processing、MacWrite、MacWrite II、Maker Interchange Format (MIF)、Maker Markup Language、MASS-11、MHT format、Microsoft Excel、Microsoft Excel 2000、Microsoft Excel 2007 XML、Microsoft Excel 95、Microsoft Excel 97、Microsoft Excel Binary 2007、Microsoft Excel Chart、Microsoft Excel Macro、Microsoft Excel Macro 2007 XML、Microsoft Excel XML、Microsoft Office Groove Format、Microsoft Pocket Word、Microsoft PowerPoint 2000、Microsoft PPT 2007 XML、Microsoft PPT Macro 2007 XML Microsoft Project 2000、Microsoft Project 2007、Microsoft Project 4、Microsoft Project 4.1、Microsoft Project 98、Microsoft Project Activity

附件清單	真實檔案類別	預先定義的真實檔案類型
文件檔		Microsoft Project Calculation、Microsoft Project Resource、Microsoft Publisher、Microsoft Publisher 98/2000/2002/2003/2007、Microsoft Visio、Microsoft Visio XML、Microsoft Word 2000、Microsoft Word 2007 XML、Microsoft Word 95、Microsoft Word 97、Microsoft Word for Macintosh、Microsoft Word for PC、Microsoft Word for PC Driver、Microsoft Word for PC Glossary、Microsoft Word for PC Miscellaneous File、Microsoft Word for PC Style Sheet、Microsoft Word for Windows、Microsoft Word Macro 2007 XML、Microsoft Word UNIX、Microsoft Word XML、Microsoft Works for DOS Spreadsheet、Microsoft Works for DOS Word Processor、Microsoft Works for MAC Spreadsheet、Microsoft Works for MAC Word Processor、Microsoft Works for Windows Spreadsheet、Microsoft Works for Windows Word Processor、Microsoft XML Paper Specification(XPS)、MultiMate、MultiMate Advantage、MultiMate Advantage Footnote File、MultiMate Advantage II、MultiMate Advantage II Footnote File、MultiMate Footnote File、Multiplan (Mac)、Multiplan (PC)、Multiplus (AES)、Navy DIF、NBI Async Archive Format、NBI Net Archive Format、NIOS TOP、Oasys format、ODA / ODIF FOD26、ODA / ODIF FOD36、ODA / ODIF Q111、ODA / ODIF Q112、ODF Presentation、ODF Spreadsheet、ODF Text、Office Writer、OLIDIF (Olivetti)、Omni Outliner (.oo3) File、Omni Outliner (.opml) File、OneNote Note Format (.one)、OOutliner (.ooutline) File、PageMaker for Macintosh、PageMaker for Windows、PeachCalc、Persuasion、Philips Script、PlanPerfect、Portable Document Format、PowerPoint 95、PowerPoint 97、PowerPoint MAC、PowerPoint PC、PRIMEWORD、Q & A for DOS、Q & A for Windows、Q-One V1.93J、Q-One V2.0、Quark Xpress MAC、Quattro Pro 9+ for Windows、Quattro Pro for DOS、Quattro Pro for Windows、RealLegal E-Transcript File(*.ptx)、Rich Text Format (RTF)、SAMNA Word、Samsung Electronics Jungum Global document (*.gul)、SGML、Skype Log File

附件清單	真實檔案類別	預先定義的真實檔案類型
文件檔		SmartWare II Spreadsheet、SmartWare II Word Processor、StarOffice Presentation XML、StarOffice Spreadsheet XML、StarOffice Text XML、Supercalc、SWF、SYLK、Symphony、Targon Word、UltraCalc、Unicode、Unicode HTML、Uniplex、Uniplex Ucalc、USENET、Verity XML、Vistaword、Volkswriter、WANG PC、WANG WITA、WANG WPS、Windows Write、Word Connection、WordERA、WordMARC、WordPerfect、WordPerfect Configuration File、WordPerfect Driver、WordPerfect Hyphenation Dictionary、WordPerfect MAC、WordPerfect Macro、WordPerfect Miscellaneous File、WordPerfect Resource File、WordPerfect Spelling Dictionary、WordPerfect Thesaurus、WordPerfect VAX、WordStar、WordStar 2000、WPS-PLUS、WriteNow MAC、Xerox 860、Xerox Writer、XHTML、XML、XYWrite / Nota Bene、Yahoo Instant Messenger History、以 application/ms-excel 為開頭的 MIME 類型、以 application/msword 為開頭的 MIME 類型、以 application/pdf 為開頭的 MIME 類型、以 application/vnd.ms-access 為開頭的 MIME 類型、以 application/vnd.ms-excel 為開頭的 MIME 類型、以 application/vnd.ms-powerpoint 為開頭的 MIME 類型、以 application/vnd.ms-project 為開頭的 MIME 類型、以 application/vnd.ms-works 為開頭的 MIME 類型、以 application/vnd.visio 為開頭的 MIME 類型、副檔名為 doc、副檔名為 dot、副檔名為 mpp、副檔名為 pdf、副檔名為 ppt、副檔名為 ps、副檔名為 rtf、副檔名為 txt、副檔名為 vsd、副檔名為 wk1、副檔名為 wks、副檔名為 wp、副檔名為 xls
執行檔	執行檔	ELF Executable、MS-DOS Batch File、MSDOS Device Driver、MSDOS/Windows Program、PC (.COM)、Unix Executable (3B20)、Unix Executable (Basic-16)、Unix Executable (Bell 5.0)、Unix Executable (iAPX 286)、Unix Executable (MC680x0)、Unix Executable (PDP-11/pre-System V VAX)、Unix Executable (VAX)、Unix Executable (WE32000)、Unix Executable (x86)
財務資訊	試算表格式	Applix Spreadsheets、CSV (逗號分隔值)、Lotus 1-2-3、Microsoft Excel、Microsoft Excel Chart、Microsoft Excel Macro、Microsoft Excel XML、Microsoft Works for DOS Spreadsheet、Microsoft Works for MAC Spreadsheet、Microsoft Works for Windows Spreadsheet、Multiplan (Mac)、Multiplan (PC)、Quattro Pro for DOS、Quattro Pro for Windows、SYLK

附件清單	真實檔案類別	預先定義的真實檔案類型
影像檔	向量圖形文件	Ability Word Processor AutoCAD DXF Binary AutoCAD DXF Text AutoDesk Drawing (DWG) AutoDesk WHIP AutoShade Rendering、CCITT G3 1D、Curses Screen Image、Encapsulated PostScript、Encapsulated PostScript with Preview、FPX Format、GEM Bit Image、Computer Graphics Metafile (CGM) Binary、Computer Graphics Metafile (CGM) Character、Computer Graphics Metafile (CGM) Clear Text、Corel CMX、Corel Draw、DeVice Independent file (DVI)、Enhanced Metafile、Freehand MAC、GEM VDI、Graphics Interchange Format (GIF87a)、Graphics Interchange Format (GIF89a)、JPEG Interchange Format、Micrografx Designer Microsoft Office Drawing MicroStation V8 DGN (OLE) OS/2 PM Metafile, PostScript QuickDraw 3D Metafile Simple Vector Format (SVF) VRML Windows Draw (Micrografx) Windows Metafile (無標頭)、CATIA Formats (CAT*)、ODF Drawing, Omni Graffle (.graffle) XML File、SolidWorks Format (.sldasm、.sldprt、.slddrw)
影像檔	光柵影像文件	MacPaint、MS Windows Device Independent Bitmap、OLE DIB object、OS/2 PM Metafile、PC Paintbrush Graphics (PCX)、PCD Format、Portable Bitmap Utilities ASCII Format、Portable Bitmap Utilities Binary Format、Portable Greymap Utilities ASCII Format、Portable Greymap Utilities Binary Format、Microsoft Document Imaging Format、Photoshop Document (.psd)
機密文件 不發佈的文件 僅限內部使用的文件 專利文件	試算表格式	Applix Spreadsheets、CSV (逗號分隔值)、Lotus 1-2-3、Lotus 1-2-3 97、Lotus 1-2-3 Release 9、Microsoft Excel、Microsoft Excel 2000、Microsoft Excel 2007、Microsoft Excel 95、Microsoft Excel 97、Microsoft Excel Chart、Microsoft Excel Macro、Microsoft Excel XML、Microsoft Works for DOS Spreadsheet、Microsoft Works for MAC Spreadsheet、Microsoft Works for Windows Spreadsheet、Multiplan (Mac)、Multiplan (PC)、Portable Document Format、Quattro Pro for DOS、Quattro Pro for Windows、SYLK
機密文件 不發佈的文件 僅限內部使用的文件 專利文件	文書處理	Microsoft Word 2000、Microsoft Word 2007、Microsoft Word 95、Microsoft Word 97、Microsoft Word for Macintosh、Microsoft Word for PC、Microsoft Word for Windows、Microsoft Word UNIX、Microsoft Word XML

附件清單	真實檔案類別	預先定義的真實檔案類型
機密文件 不發佈的文件 僅限內部使用的文件 專利文件	簡報	Microsoft PowerPoint 2000、PowerPoint 95、PowerPoint 97、PowerPoint MAC、PowerPoint PC
媒體檔	動畫檔	Macromedia Director、Macromedia Flash
媒體檔	向量圖形文件	Quickdraw 3D Metafile、VRML
媒體檔	影片檔	QuickTime Movie、RIFF Multimedia Movie、Video for Windows (AVI)、RealMedia Streaming Media (.rm、.ra)
媒體檔	音效檔格式	Microsoft Wave、MIDI、MP3 (MPEG Audio)、RealAudio、RIFF MIDI、AC3 Audio File Format (.ac3)
MSAccess 檔案與執行檔	程式庫	DOS/Windows Object Library
MSAccess 檔案與執行檔	資料庫文件	Microsoft Access、Microsoft Access 2000、Microsoft Access 95、MicrosoftAccess 97
MSAccess 檔案與執行檔	執行檔	MSDOS Device Driver、PC (.COM)、MSDOS/Windows Program、Unix Executable (3B20)、Unix Executable (Basic-16)、Unix Executable (Bell 5.0)、Unix Executable (iAPX 286)、Unix Executable (MC680x0)、Unix Executable (PDP-11/pre-System V VAX)、Unix Executable (VAX)、Unix Executable (WE32000)、Unix Executable (x86)
MSAccess 檔案與執行檔	物件模組格式	Unix Object Module (old MS 8086)、Unix Object Module (VAX Demand)、Unix Object Module (Z8000)
多媒體檔	影片檔	MPEG Movie、QuickTime Movie、RIFF Multimedia Movie、Video for Windows (AVI)
多媒體檔	音效檔格式	Amiga IFF (8SVX) Sound、Amiga MOD、Audio Interchange File Format (AIFF)、Creative Voice (VOC)、Microsoft Wave、MIDI、MPEG Audio、NeXT/Sun Audio Data、Real Audio、RIFF MIDI、AC3 Audio File Format(.ac3)、RealMedia Streaming Media (.rm、.ra)
包含 IP 位址關鍵字的網路圖 包含 IP 位址的網路圖	簡報文件	Microsoft Visio

附件清單	真實檔案類別	預先定義的真實檔案類型
包含 IP 位址關鍵字的網路圖 包含 IP 位址的網路圖	文書處理文件	Microsoft Visio XML
密碼保護的檔案	試算表格式 (密碼保護)	Microsoft Excel、Microsoft Excel 2000、Microsoft Excel 2007、Microsoft Excel 95、Microsoft Excel 97、Microsoft Excel Chart、Microsoft Excel XML
密碼保護的檔案	簡報文件 (密碼保護)	Microsoft PowerPoint2000、PowerPoint 95、PowerPoint 97、PowerPoint MAC、PowerPoint PC
密碼保護的檔案	文書處理文件 (密碼保護)	Microsoft Word 2000、Microsoft Word 2007、Microsoft Word 95、Microsoft Word 97、Microsoft Word for Macintosh、Microsoft Word for PC、Microsoft Word for Windows、Microsoft Word UNIX、Microsoft Word XML
密碼保護的檔案	封裝格式 (密碼保護)	ZIP Archive
PGP 檔案	封裝格式	ASCII-armored PGP encoded、ASCII-armored PGP Public Keyring、ASCII-armored PGP signed、PGP Compressed Data、PGP Encrypted Data、PGP Public Keyring、PGP Secret Keyring、PGP Signature Certificate、PGP Signed and Encrypted Data、PGP Signed Data
出版文件	桌上出版	FrameMaker、FrameMaker Book、Microsoft Publisher、PageMaker for Macintosh、PageMaker for Windows、Quark Xpress MAC
所有履歷表 員工履歷表	文書處理文件	Microsoft Word 2000、Microsoft Word 2007、Microsoft Word 95、Microsoft Word 97、Microsoft Word for Macintosh、Microsoft Word for PC、Microsoft Word for Windows、Microsoft Word UNIX、Microsoft Word XML
SEC 公平揭露規定	試算表格式	Applix Spreadsheets、CSV (逗號分隔值)、Lotus 1-2-3、Lotus 1-2-3 97、Lotus 1-2-3 Release 9、Microsoft Excel、Microsoft Excel 2000、Microsoft Excel 2007、Microsoft Excel 95、Microsoft Excel 97、Microsoft Excel Chart、Microsoft Excel Macro、Microsoft Excel XML、Microsoft Works for DOS Spreadsheet、Microsoft Works for MAC Spreadsheet、Microsoft Works for Windows Spreadsheet、Multiplan (Mac)、Multiplan (PC)、Quattro Pro for DOS、Quattro Pro for Windows、SYLK

附件清單	真實檔案類別	預先定義的真實檔案類型
SEC 公平揭露規定	文書處理文件	Microsoft Word 2000、Microsoft Word 2007、Microsoft Word 95、Microsoft Word 97、Microsoft Word for Macintosh、Microsoft Word for PC、Microsoft Word for Windows、Microsoft Word UNIX、Microsoft Word XML、Portable Document Format、WordPerfect、WordPerfect MAC、WordPerfect VAX
真實類型執行檔	執行檔	ELF Executable、MS-DOS Batch File、MSDOS Device Driver、MSDOS/Windows Program、PC (.COM)、Unix Executable (3B20)、Unix Executable (Basic-16)、Unix Executable (Bell 5.0)、Unix Executable (iAPX 286)、Unix Executable (MC680x0)、Unix Executable (PDP-11/pre-System V VAX)、Unix Executable (VAX)、Unix Executable (WE32000)、Unix Executable (x86)

有幾個真實檔案類別未被任何「附件清單」參照。然而，可以從檔案類別及檔案類型清單內存取這些檔案類別及其相關真實檔案類型，方法如同選取其他檔案類別及類型一般。您可以將其中任一個檔案類型新增至現有的附件清單，或建立新的附件清單。

表 15-16　其他檔案類別及類型

真實檔案類別	真實檔案類型
通訊格式	Ability Communications、FTP Session Data、Microsoft Works for MAC Communications、SmartWare II Communications
FAX 格式	DCX FAX Format (PCX 影像)
字型類型文件	NeWS bitmap font、SUN vfont、Definition TrueType Font
一般用途文件	Microsoft Office 2007、Program Information File (PIF)、Windows Group、Windows Help File、WordPerfect auxiliary file
混合類型文件	Framework、Framework II、Windows C++ Object Storage
規劃/大綱格式	MORE Database MAC

請參閱第 343 頁的「關於附件清單」。

建立偵測檔案附件類型的清單

在內容過濾政策條件中使用附件清單，可對電子郵件附件檔案類型進行偵測並採取行動。例如，您可以將可偵測含有 .exe 檔案附件之郵件的附件清單，指派為內容過濾政策中的條件。

然後，您可以指定在偵測到具有 .exe 檔案附件的郵件時，希望 Symantec Messaging Gateway 採取的動作。

Symantec Messaging Gateway 提供預設的附件清單，您可使用這些清單來建立自己的附件清單。所有的附件清單 (預設的和自訂的) 會顯示在**「電子郵件內容過濾政策」**頁面的**「條件」**區段中。所以，架構內容過濾政策時，您可以方便地選取要用作條件的附件清單。

建立附件清單時，可以使用真實檔案類別、真實檔案類型、一般副檔名及 MIME 類型的任意組合。

附註：MIME 類型和副檔名式的附件清單對刪除 MIME 標頭中未描述的附件 (例如對於某些轉寄的郵件) 無效。若要確保刪除附件檔案類型的所有實例，請儘可能架構附件清單使用真實檔案類型。

若要建立附件清單，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 343 頁的「關於附件清單」。

請參閱第 353 頁的「編輯附件清單」。

建立偵測檔案附件類型的清單

1. 在控管中心內，按下**「內容」>「資源」>「附件清單」**。
2. 按下**「新增」**。
3. 在**「附件清單名稱」**方塊中，輸入附件清單的名稱。
4. 在**「新增附件類型」**下，執行下列任何工作：

將真實檔案類別新增至附件清單	執行下列所有工作： ■ 在**「檔案類別」**清單上方，按下**「如果」**旁的選擇鈕。 ■ 按下附件類型下拉式清單，並選取**「真實檔案類別」**。 ■ 在**「檔案類別」**清單中，選取您要新增至附件清單的類別。您可以按住 **Ctrl** 以選取多個不連續的項目。您也可以按住 **Shift** 來選取一組連續的項目。 選取真實檔案類別時，會將該類別內的每個真實檔案類型新增至附件清單。您無法新增或移除任何檔案類型。

將真實檔案類型新增至附件清單

執行下列所有工作：

- 在「**檔案類別**」清單上方，按下「**如果**」旁的選擇鈕。
- 按下附件類型下拉式清單，並選取「**真實檔案類型**」。
  「**真實檔案類型**」為預設選項。
- 在「**檔案類別**」清單中，選取含有您要新增至附件清單之真實檔案類型的真實檔案類別。
  您可以按住 **Ctrl** 以選取多個不連續的項目。您也可以按住 **Shift** 來選取一組連續的項目。
  請參閱第 344 頁的「預設附件清單」。
- 在「**檔案類型**」方塊中，選取您要新增至附件清單的真實檔案類型。

根據檔案名稱、副檔名或 MIME 類型新增副檔名

執行下列所有工作：

- 若要新增自己的副檔名，請在「**檔案類別**」清單下，按下「**如果**」旁的選擇鈕。
- 按下「**副檔名**」下拉式清單，然後選取下列其中一個選項：
  - 檔案名稱
  - 副檔名
    此值為預設值。
  - MIME 類型
- 按下「**是**」下拉式清單，然後選取下列其中一個選項：
  - **含有**
  - **開頭是**
  - **結束於**
  - **是**
    此值為預設值。
- 在相鄰的文字方塊中，僅輸入一個檔案名稱、副檔名或 MIME 類型。
  輸入完整的 MIME 類型，例如 image 或 image/gif。

5 按下「**新增**」即可將附件類型新增至附件清單。

6 重複進行步驟 4 和 5，將更多附件類型新增至附件清單。

7 按下「**儲存**」。

編輯附件清單

您可以編輯所建立的自訂附件清單。您不能修改預設的高階附件清單。

請參閱第 344 頁的「預設附件清單」。

您可以修改清單名稱、向清單中新增副檔名，或從清單中移除副檔名。

若要編輯附件清單，您必須具有「完整的管理」權限及修改政策的權限。

請參閱第 343 頁的「關於附件清單」。

編輯附件清單

1 在控管中心內，按下**「內容」>「資源」>「附件清單」**。

2 在**「附件清單」**頁面中，勾選您要修改之自訂附件清單旁的方塊，然後按下**「編輯」**。

您也可以按下附件清單的名稱來進行編輯。

3 執行下列其中一個工作：

- 修改附件清單名稱。
- 將檔案類別、副檔名或檔案類型新增至清單。
  請參閱第 351 頁的「建立偵測檔案附件類型的清單」。
- 在**「附件類型」**清單中，選取您要移除的附件類型，然後按下**「刪除」**。

4 按下**「儲存」**。

刪除附件清單

如果您不再需要自訂附件清單，可將其刪除。您無法刪除高階附件清單。

若要刪除附件清單，您必須先從使用該附件清單的所有內容過濾政策中，將使用該附件清單的條件刪除。當您嘗試刪除附件清單時，Symantec Messaging Gateway 會告知您哪些政策使用該附件清單。

若要刪除附件清單，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 343 頁的「關於附件清單」。

刪除附件清單

1 在控管中心內，按下**「內容」>「資源」>「附件清單」**。

2 在**「附件清單」**頁面上，勾選要刪除之附件清單旁的方塊。

3 按下**「刪除」**。

頁面頂端會顯示一則訊息，指出其中有條件使用此附件清單的內容過濾政策。請先刪除或修改這些政策中的此條件，再重複此程序。

請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

Perl 相容規則運算式

本節描述了可以用於內容過濾政策的 Perl 相容規則運算式。

表 15-17 規則運算式 metacharacter

Metacharacter/ 建構	說明
.	句點： 符合輸入順序的任何單一字元。
^	長音符： 代表輸入行的開頭。例如，^A 是符合行開頭之英文字母 A 的規則運算式。^ 字元是唯一允許放在規則運算式開頭或 (或 | 字元後面的特殊字元。
$	貨幣符號： 代表輸入行的結尾。例如，A$ 是符合行結尾之英文字母 A 的規則運算式。$ 字元是唯一允許放在規則運算式結尾或) 或 | 字元前面的特殊字元。 請注意，這個 metacharacter 不得用於郵件內文的逐行比對。
*	星號： 符合星號左邊緊鄰字串的零個以上實例。例如，A* 符合 A、AA、AAA 等。也符合 Null 字串 (未出現 A)。
?	問號： 符合問號左邊緊鄰字串的零或一個實例。
+	加號： 符合加號左邊緊鄰字串的一個以上實例。
\	逸出字元： 開啟或關閉 metacharacter 的特殊意義。例如\。僅符合點字元。\$ 符合字面上的貨幣符號字元。請注意，\\ 符合字面上的 \ 字元。
|	管道字元： 符合管道字元任一邊的運算式。例如，exe|com|zip 符合 exe、com 或 zip。
[字串]	方括弧： 在方括弧內，符合單一字元或對照元素 (如清單中所述)。方括弧內的字元不區分大小寫。 方括弧內的字串會評估為文字，就和在字串的每個字元前面加上逸出字元 (\) 一樣。 如果方括弧內的初始字元是長音符 (^)，則運算式會符合任何字元或對照元素，但不含方括弧運算式內的字元。 如果任何潛在長音符 (^) 後面的第一個字元是破折號 (-) 或右方括弧 (])，則該字元只會符合字面上的破折號或右方括弧。
(字串) \(字串\)	大括號： 將規則運算式的各個部分集為群組，讓大括號內的字串的優先順序高於其餘字串。

請參閱第 355 頁的「Perl 相容規則運算式範例」。

Perl 相容規則運算式範例

表 15-18 提供了一些 Perl 相容運算式範例。

請參閱第 354 頁的「Perl 相容規則運算式」。

表 15-18 範例 Perl 相容規則運算式

字元	說明	範例	相符項範例
.	符合任何一個字元	j.n	jen、jon、j2n、j$n
..	符合任何兩個字元	jo..	john、josh、jo4#
.*	符合零個或多個字元	sara.*	sara、sarah、sarahjane、saraabc%123
.*		s.*m.*	sm、sam、simone、s321m$xyz
.+	符合一個或多個字元	sara.+	sarah、sarahjane、saraabc%123
.+		s.+m.+	simone、s321m$xyz
\.	符合句點	stop\.	stop.
*	符合星號	b**	b**
\+	符合加號字元	18\+	18+
\/	符合正斜線	18\/	18/
[0-9]{n}	符合任何數字 n 次 (例如符合社會安全號碼)	[0-9]{3}-[0-9]{2}-[0-9]{4}	123-45-6789

指定封存郵件的儲存位置

貴組織可以保留違反特定政策之郵件的副本。若要使用封存功能，必須在建立內容過濾政策時指定**「封存郵件」**動作。

您也可以根據每個政策來架構封存電子郵件目的地。

請參閱第 285 頁的「政策動作及其功能」。

此功能在貴組織面對以下境況時會非常有用，例如：

- 要準備對員工或其他組織提出可能的法律訴訟
- 必須保留記錄以達成法規遵循目的
- 要保留某些員工群組的記錄

如果郵件觸發了政策違規，且該政策的動作是**「封存郵件」**，則 Symantec Brightmail Gateway 將複製這些郵件， 然後將副本傳送至一或兩個您所指定的電子郵件地址，或傳送至封存伺服器。

若要封存郵件，您必須具有「完整的管理」權限或修改政策的權限。

指定封存郵件的儲存位置

1 在控管中心內，按下**「內容」>「設定」>「封存」**。

2 在**「封存電子郵件地址」**方塊中，輸入完整的電子郵件地址 (如 kyi@symantecexample.com)。

3 在**「封存伺服器主機」**欄位中，輸入封存伺服器主機的名稱。

此伺服器主機是您在步驟 2 中所提供封存電子郵件地址的主機名稱或 IP 位址。

4 若您提供了**「封存伺服器主機」**，請在**「封存伺服器通訊埠」**中，輸入該伺服器主機的通訊埠號。

5 如果您要使用 MX 查詢來尋找對應於封存伺服器主機的資訊，以繞送封存郵件，請勾選**「啟用 MX 查詢」**。

6 若要使所有現有政策都可以使用封存伺服器的資訊，請按下**「套用至目前所有政策」**。

7 按下**「儲存」**。

16

處理內容過濾事件

本章包含以下主題：

- 架構內容事件資料夾
- 監控及因應事件
- 使用 Symantec Content Encryption 加密資料
- 架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料

架構內容事件資料夾

表 16-1說明您可如何管理內容事件資料夾。您可以視需要以任何順序執行這些工作。

表 16-1　　管理內容事件資料夾

工作	說明
瞭解何謂內容事件資料夾以及它們可如何幫助您管理內容過濾事件。	內容事件資料夾能協助您組織、監控及管理內容過濾政策違規事件。作為最佳實務準則，您應為您所使用的每種類型的內容過濾政策建立一個內容事件資料夾。例如，如果您使用 HIPAA 範本來建立一個政策，就可以建立一個 HIPAA 內容事件資料夾。您可以使用該資料夾監控 HIPAA 政策事件。 請參閱第 359 頁的「關於內容事件資料夾」。
熟悉如何將資料夾維持在可管理的大小。	Symantec Messaging Gateway 提供了清除程式，可管理內容事件資料夾的大小。清除程式會依您指定的頻率自動執行。 請參閱第 360 頁的「關於管理內容事件資料夾的大小」。
建立內容事件資料夾。	建立內容事件資料夾，以幫助您組織、監控及管理內容政策違規所產生的事件。包括預設的資訊事件及「隔離所」事件資料夾在內，您最多可以擁有 1,000 個資料夾。 請參閱第 361 頁的「建立內容事件資料夾」。

工作	說明
修改現有內容事件資料夾。	您可以視需要編輯任何內容事件資料夾。 請參閱第 364 頁的「編輯內容事件資料夾」。
刪除現有內容事件資料夾。	當您不再需要您所建立的內容事件資料夾時，可以予以刪除。但是，您無法刪除預設的「資訊事件」資料夾或「隔離事件」資料夾。 請參閱第 364 頁的「刪除內容事件資料夾」。
若要最大化磁碟空間，請排程清除程式來移除內容事件資料夾中的郵件。	Symantec Messaging Gateway 提供了清除程式，可用於管理內容事件資料夾的大小。您可以指定清除程式的執行頻率。 請參閱第 365 頁的「排程內容事件資料夾清除程式」。

關於內容事件資料夾

內容事件資料夾能協助您組織、監控及管理內容過濾政策違規事件。作為最佳實務準則，您應為您所使用的每種類型的內容過濾政策建立一個內容事件資料夾。例如，如果您使用 HIPAA 範本來建立一個政策，就可以建立一個 HIPAA 內容事件資料夾。您可以使用該資料夾監控 HIPAA 政策事件。

在您架構內容過濾政策之前，應先建立內容事件資料夾。這樣，如果要建立內容過濾政策，選擇建立事件的動作時，就可使用此資料夾選項。若您未指定建立事件的資料夾，違反該政策的郵件就會歸檔至**「資訊事件」**資料夾中。

請參閱第 278 頁的「建立內容過濾政策」。

當您建立內容過濾資料夾時，您必須選擇要使用的資料夾的類型。

Symantec Messaging Gateway 提供下列類型的內容事件資料夾：

保留供檢閱 (內容隔離所)
: 對於您要檢閱的事件，請使用此類型的資料夾。此資料夾可讓您保留觸發內容過濾違規的郵件，以便您檢閱並決定處理方式。該政策的任何其他動作都會延遲，直到事件完成檢閱為止。

  附註：在**「保留供檢閱」(內容隔離)**資料夾中的郵件會依據您所指定的設定加以清除，即使尚未檢閱過這些郵件亦然。

  這些資料夾會在控管中心內顯示為「隔離事件」資料夾。

  請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

資訊事件
: 使用此類型的資料夾，可追蹤優先順序低於保留供檢閱之事件的事件。

您也可以為每個資料夾架構下列的設定：

- 封存標籤及為標籤編碼
  本設定為可選設定。
- 清除程式設定

最大內容事件資料夾大小為必填。在清除前保留的事件的天數設定是可選擇的。

- 表示事件已記錄至該資料夾的通知郵件，以及您希望收到該通知的人
  本設定為可選設定。

Symantec Messaging Gateway 最多能支援 1,000 個內容事件資料夾，包括預設的「資訊事件」及「隔離事件」資料夾。您必須具有「完整的管理」權限或修改設定值的權限，才能建立內容事件資料夾。

請參閱第 361 頁的「建立內容事件資料夾」。

關於管理內容事件資料夾的大小

出現下列一種或兩種情況時，內容事件資料夾會很快填滿並佔用大量磁碟空間：

- 您有很多動作為在內容事件資料夾中建立事件的內容過濾政策。
- 您有大量違反政策的郵件。

Symantec Messaging Gateway 提供了清除程式，可管理內容事件資料夾的大小。清除程式會依您指定的頻率自動執行。

清除程式執行時，會根據下列條件來清除內容事件資料夾中的事件：

依內容事件資料夾大小上限

內容事件資料夾大小上限是資料夾中每個郵件檔案之區塊大小 (在磁碟上的大小) 的總和。實際磁碟使用量可能會更多。

資料夾達到其大小上限時，會傳送一則訊息至 BrightmailLog.log。資料夾達到您為警示指定的大小上限 (例如，大小上限 120%) 時，便會傳送警示。如果多個資料夾同時達到其大小上限，則只會傳送一個警示。但是，您會持續收到警示電子郵件，這些電子郵件會就之後超過其大小上限的任何資料夾通知您。會刪除最舊的事件，直到資料夾恢復到其大小上限。

請參閱第 590 頁的「架構警示」。

賽門鐵克建議根據大小來清除資料夾，同時微調內容過濾政策。之後，您可視需要修改清除程式設定。

您必須指定內容事件資料夾大小上限。預設大小上限為 5 GB，但您可修改此設定。

依您希望儲存事件的天數

(可選)您可以在清除程式執行下列其中一項動作之前，先指定儲存事件的天數：

- 核准
  此選項僅適用於內容隔離事件資料夾。清除程式核准事件後，就會將其從資料夾中刪除。
- 拒絕
  此選項僅適用於內容隔離事件資料夾。清除程式拒絕事件後，就會將其從資料夾中刪除。
- 自訂
  這是您在建立政策動作以建立隔離事件時指定的自訂動作。此選項僅適用於內容隔離事件資料夾。在清除程式對資料夾套用自訂動作之後，對事件所採取的動作就是在政策中定義的動作。
- 刪除
  此選項同時適用於內容隔離事件資料夾和資訊事件資料夾。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

附註：達到此臨界值時，會清除隔離事件資料夾中的事件，即使這些事件尚未經過檢閱，也是如此。Symantec Messaging Gateway 會採取您在內容過濾政策中指定的動作，從最舊的事件開始執行。Symantec Messaging Gateway 會根據接收郵件的時間來確定電子郵件的保留期限。

您可以在建立內容事件資料夾時架構清除程式條件。您可以指定資料夾大小臨界值及(或)儲存這些臨界值的天數。此後您還可以隨時修改設定。達到臨界值時，資料夾中不會進一步建立任何事件。

請參閱第 361 頁的「建立內容事件資料夾」。

清除程式週期會套用至所有內容過濾資料夾。

請參閱第 365 頁的「排程內容事件資料夾清除程式」。

請參閱第 359 頁的「關於內容事件資料夾」。

建立內容事件資料夾

建立內容事件資料夾，以幫助您組織、監控及管理內容政策違規所產生的事件。包括預設的資訊事件及「隔離所」事件資料夾在內，您最多可以擁有 1,000 個資料夾。

若想建立內容事件資料夾，您必須具有「完整的管理」權限或修改政策的權限。

請參閱第 359 頁的「關於內容事件資料夾」。

請參閱第 364 頁的「編輯內容事件資料夾」。

請參閱第 365 頁的「排程內容事件資料夾清除程式」。

請參閱第 364 頁的「刪除內容事件資料夾」。

建立內容事件資料夾

1 在控管中心內，按下**「內容」>「設定」>「內容事件資料夾」**。

2 按下**「新增」**。

3 在**「內容事件資料夾名稱」**欄位中，輸入內容事件資料夾的名稱。

作為最佳實務準則，您應使用可以反映您想要在該資料夾中收集的內容類型的名稱。例如，如果您想要在本資料夾中放置違反 HIPPA 政策的郵件，可以將本資料夾命名為 HIPPA。

4 按下**「內容事件資料夾」**類型下拉式清單，以選擇您想要使用的資料夾類型。

5 另外，可在**「選擇性封存標籤」**欄位中，輸入您想要識別本資料夾的文字，以供封存之用。

當您在本內容事件資料夾中指定一個封存動作時，該文字會附帶在事件內。

6 如果您指定了事件封存標籤，可以在**「編碼」**下拉式清單中選擇標籤使用的字元編碼。

7 勾選**「啟用此資料夾中的郵件提交按鈕」**以啟用提交功能。

僅在您啟用客戶特定垃圾郵件提交功能時才會顯示此選項。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

8 在**「清除程式設定」**下，執行下列工作：

指定在清除事件前保留的天數 (選用)	執行下列所有工作： ■ 勾選**「執行預設動作前的儲存天數」**，並在其旁邊的欄位中輸入天數。 ■ 在**「預設清除程式動作」**下，指定在清除事件時您想要採取的動作。 若資料夾是**「資訊事件」**資料夾，唯一可用的選項就是**「刪除」**。
指定最大的資料夾大小 (必填)	在**「臨界值」**中，以千位元組、百萬位元組或十億位元組指定大小。

請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

9 或者，按下**「通知格式」**下拉式清單，並選擇事件通知的格式。

本通知會傳送至您在步驟 11 及在步驟 12 中所指定的人，以表示有一個事件加入本資料夾。

請參閱第 368 頁的「建立事件通知」。

10 按下**「編輯」**檢視或編輯事件通知範本。

11 在**「通知收件者地址」**欄位中，輸入內容過濾主管的電子郵件地址，該主管應會收到有關此資料夾事件的通知。

請以逗號、分號或空格分隔多個地址。

12 在「**管理員通知**」清單中，勾選要在這個資料夾中出現事件時通知的管理員。若您不必要傳送通知，請將本欄位留白。

當您新增管理員或修改管理員設定時，可以指定要向其通知本資料夾事件的管理員。

13 按下「**儲存**」。

內容過濾通知變數

在通知郵件文字中，Symantec Messaging Gateway 會以事件編號清單和觸發這些事件的政策，取代預設變數「*%NEW_COMPLIANCE_MESSAGES%*」。您可以在此變數前後輸入文字。您也可以修改此變數以符合較為特定的需求。

例如，您可以在變數前面鍵入下面這段文字，並以資料夾名稱取代「*名稱*」：

```
New incidents have been created. Please access the Name Content Incident Folder
for incident details.
```

表 16-2 會列出內容過濾通知變數。

表 16-2 內容過濾通知變數

變數	說明
%NEW_COMPLIANCE_MESSAGES%	列出事件編號和觸發這些事件的政策。
%NEW_COMPLIANCE_MESSAGES_DETAILED%	提供更詳細的事件資訊。例如事件 ID、收件者、寄件者、主旨，以及附件詳細資料和事件所在的事件資料夾名稱。
%NEW_COMPLIANCE_MESSAGES_REMEDIATION_REQUIRES_AUTHENTICATION%	指定違反的政策，以及郵件的「寄件者」、「收件者」、「主旨」和「日期」詳細資料。提供可讓使用者按下以補救隔離事件的連結。另外也要求使用者向 Symantec Messaging Gateway 進行驗證以補救。
%NEW_COMPLIANCE_MESSAGES_REMEDIATION_AUTO_AUTHENTICATION%	指定違反的政策，以及郵件的「寄件者」、「收件者」、「主旨」和「日期」詳細資料。提供可讓使用者按下以補救隔離事件的連結。但是，它也會要求使用者向 Symantec Messaging Gateway 進行驗證以補救。
%NEW_INFORMATIONAL_INCIDENT_MESSAGES_REQUIRES_AUTHENTICATION%	指定違反的政策，以及郵件的「寄件者」、「收件者」、「主旨」和「日期」詳細資料。提供可讓使用者按下以補救資訊事件的連結。另外也要求使用者向 Symantec Messaging Gateway 進行驗證以檢視事件詳細資料。
%NEW_INFORMATIONAL_INCIDENT_MESSAGES_AUTO_AUTHENTICATION%	指定違反的政策，以及郵件的「寄件者」、「收件者」、「主旨」和「日期」詳細資料。提供可讓使用者按下以補救資訊事件的連結。但是，它也會要求使用者向 Symantec Messaging Gateway 進行驗證以檢視事件詳細資料。

請參閱第 370 頁的「關於從電子郵件通知補救事件」。

請參閱第 368 頁的「建立事件通知」。

編輯內容事件資料夾

您可以視需要編輯任何內容事件資料夾。 若要編輯內容事件資料夾，您必須具有「完整的管理」權限或是修改政策的權限。

請參閱第 359 頁的「關於內容事件資料夾」。

請參閱第 364 頁的「刪除內容事件資料夾」。

請參閱第 361 頁的「建立內容事件資料夾」。

編輯內容事件資料夾

1. 在控管中心內，按下**「內容」>「設定」>「內容事件資料夾」**。
2. 勾選您要編輯之內容事件資料夾旁的方塊，然後按下**「編輯」**。

   您也可以按下內容事件資料夾名稱來進行編輯。
3. 視需要編輯內容事件資料夾設定。
4. 按下**「儲存」**。

刪除內容事件資料夾

當您不再需要您所建立的內容事件資料夾時，可以予以刪除。但是，您無法刪除預設的「資訊事件」資料夾或「隔離事件」資料夾。

刪除資料夾之前，您可能想要先確定資料夾中的所有項目是否都已經檢閱，並視需要已經解決。您還必須從使用該資料夾的任何內容過濾政策中，刪除將事件記錄至資料夾的動作。Symantec Brightmail Gateway 會在您嘗試刪除資料夾時，讓您知道哪些政策於動作中使用該資料夾。

若要刪除內容事件資料夾，您必須具有「完整的管理」權限或是修改政策的權限。

請參閱第 359 頁的「關於內容事件資料夾」。

請參閱第 364 頁的「編輯內容事件資料夾」。

請參閱第 365 頁的「排程內容事件資料夾清除程式」。

刪除內容事件資料夾

1. 在控管中心內，按下**「內容」>「設定」>「內容事件資料夾」**。
2. 勾選您要刪除之內容事件資料夾旁的方塊。

   勾選**「內容事件資料夾」**旁的方塊，以選取所有的資料夾。

3 按下「**刪除**」。

4 在確認對話方塊中，按下「**刪除**」。

頁面最上方會出現一個訊息，指出哪些內容過濾政策中存在記錄事件至此資料夾的動作。請先刪除或修改這些政策中的此動作，再重複此程序。

排程內容事件資料夾清除程式

Symantec Brightmail Gateway 提供了清除程式，可用於管理內容事件資料夾的大小。您可以指定清除程式的執行頻率。 預設頻率是每天上午 4:00。當清除程式執行時，它會採取您在內容過濾政策中指定的預設動作。 然後，它會根據臨界值條件 (資料夾大小或儲存在資料夾中的天數) 來刪除事件。

請參閱第 361 頁的「建立內容事件資料夾」。

請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

請參閱第 359 頁的「關於內容事件資料夾」。

您可以從「**狀態**」>「**已排程工作**」頁面中，檢查已排程工作的狀態。

請參閱第 556 頁的「關於已排程工作」。

您必須具有「完整的管理」權限或修改設定的權限，才能排程內容事件資料夾清除程式。

請參閱第 566 頁的「管理員權限」。

排程內容事件資料夾清除程式

1 在控管中心內，按下「**內容**」>「**設定**」>「**內容事件資料夾**」。

2 在「**內容過濾清除週期**」下的「**事件清除程式頻率**」下拉式清單中，選取清除程式的執行頻率。

3 在「**事件清除程式開始時間**」下拉式清單中，指定清除程式執行的小時和分鐘。

4 按下「**儲存**」。

架構郵件提交選項，使其顯示於隔離事件資料夾中

管理員可以從隔離事件資料夾將郵件提交到賽門鐵克以供建立客戶特定規則。但是，您必須先架構這些選項，使其顯示於您想要使用此功能的各內容隔離事件資料夾中。啟用此選項時，管理員將會在事件詳細資料頁面中看見「**這是垃圾郵件**」和「**這不是垃圾郵件**」選項。

附註：此功能不可用於資訊事件資料夾。

您必須具有「完整的管理」權限或「管理設定」修改權限，才能架構此選項。

若要架構郵件提交選項，使其顯示於隔離事件資料夾中

1 在控管中心內，按下「**內容**」>「**設定**」>「**內容事件資料夾**」。

2 在「**內容事件資料夾設定**」上新增或編輯現有的內容隔離事件資料夾。

3 在「**提交**」下的「**新增/編輯內容事件資料夾**」頁面上，勾選「**啟用此資料夾中的郵件提交按鈕**」。

4 按下「**儲存**」。

請參閱第 361 頁的「建立內容事件資料夾」。

請參閱第 364 頁的「編輯內容事件資料夾」。

請參閱第 228 頁的「設定客戶特定垃圾郵件提交」。

請參閱第 366 頁的「監控及因應事件」。

監控及因應事件

內容事件資料夾可讓您監控事件，並判斷是否需要調整政策。它們也可讓您管理 Symantec Messaging Gateway 依據您架構的政策偵測到的事件。

表 16-3說明您可如何監控及管理事件。您可以視需要以任何順序執行這些工作。

表 16-3 監控事件及對事件採取行動

工作	說明
深入瞭解您可對內容事件資料夾中的郵件執行的動作。	內容事件資料夾包含違反政策條件之郵件的事件。事件的相關資訊可幫助您瞭解、避免、回應及稽核可能的違規情況。 請參閱第 368 頁的「關於監控及因應事件」。
通知內容管理員有郵件在內容事件資料夾中。	Symantec Messaging Gateway 可以向您所指定的人通知已有事件新增至內容事件資料夾。Symantec Messaging Gateway 會提供預設的通知郵件，您可以依需要對其加以修改。 請參閱第 368 頁的「建立事件通知」。
檢閱內容事件資料夾中的事件。	本主題說明您可在**事件管理**頁面執行的動作。 請參閱第 371 頁的「檢視內容事件資料夾中的事件」。
對多個事件執行相同的動作。	您可以一次對多個事件執行相同的動作。例如，您可能要拒絕來自特定寄件者的所有事件。 請參閱第 372 頁的「一次對多個事件執行動作」。

工作	說明
提交郵件來建立自訂規則。	您可以通知賽門鐵克該郵件是遺漏的垃圾郵件或誤報的正常郵件。賽門鐵克會依據此資訊建立自訂規則，以便改善垃圾郵件偵測能力，並幫助管理員控制誤報事件。 **附註：**此功能僅適用於隔離事件資料夾。 請參閱第 380 頁的「針對客戶特定規則，從隔離所資料夾提交郵件」。
熟悉您可以在內容事件資料夾中執行的動作。	本主題說明您可對內容事件資料夾中的事件採取的動作。 請參閱第 372 頁的「內容事件動作」。
檢閱後封存郵件。	檢閱事件並採取所需動作之後，即可封存郵件。您可以從**「資安事端管理程式」**頁面中封存一或多封郵件，也可以從事件的詳細資料頁面中一次封存一封郵件。 請參閱第 374 頁的「封存事件」。
匯出事件的歷史記錄。	您可以匯出有關事件之歷史記錄的所有資訊， 例如事件的建立時間、狀態的變更時間、郵件檢閱動作及註解。您可以選取要用於匯出的編碼及分隔符號。 請參閱第 378 頁的「匯出事件的歷史記錄」。
轉寄事件.	您可以轉寄事件資料夾中的事件，以進行進一步檢閱。轉寄事件時，您可以為接收轉寄郵件的人建立註解，以提供指示或期限。您也可以指定是否要附加原始郵件。 請參閱第 378 頁的「轉寄事件」。
檢閱後刪除事件。	賽門鐵克建議在檢閱事件和對事件執行動作之後刪除事件，以減少事件資料夾中的事件量。刪除某個事件之後，該事件便不會再顯示於事件資料夾中，且無法擷取該事件。 請參閱第 379 頁的「刪除事件」。
對事件採取行動。	檢閱「隔離事件」資料夾中的事件後，您可以核准、拒絕事件，對其執行自訂動作，或繼續保留該事件。對「隔離事件」資料夾中的事件進行補救後，Symantec Messaging Gateway 會採取您在「郵件檢閱核准的動作」、「郵件檢閱拒絕的動作」及「郵件檢閱自訂動作」的內容過濾政策動作中指定的動作。 請參閱第 381 頁的「補救已隔離的事件」。
更新事件的狀態以監控其進度。	您可以更新事件的狀態來反映對事件的變更。事件的狀態可讓檢閱者瞭解事件目前處於檢閱程序的哪個階段，以及檢閱的結果為何。 請參閱第 382 頁的「更新事件的狀態」。
修改事件的嚴重性層級。	檢閱事件時，可以修改其嚴重性層級。 請參閱第 382 頁的「變更事件的嚴重性層級」。

工作	說明
檢視事件的歷史記錄。	您可以檢視事件的歷史記錄以查看事件的進度。 請參閱第 383 頁的「檢視事件的歷史記錄」。

關於監控及因應事件

內容事件資料夾包含違反政策條件之郵件的事件。事件的相關資訊可幫助您瞭解、避免、回應及稽核可能的違規情況。例如，您可以使用事件資料夾，在採納永久政策之前監控公司的內容過濾政策違規情況。

請參閱第 359 頁的「關於內容事件資料夾」。

內容事件資料夾所儲存的事件可讓您執行以下動作：

監控資訊事件資料夾中的事件

您可以監控所發生的事件，但不必因應這些事件。

您必須建立一個內容過濾政策，其中至少包含一個在所指定的資料夾中建立資訊事件的動作。若發生政策違規，就會在資訊事件資料夾中建立事件，以供您方便時檢閱。

將事件保留於隔離事件資料夾中以供檢閱或補救

您可以在隔離事件資料夾中保留郵件，以供檢閱及決定想要採取的動作。

內容過濾主管可以執行下列任一工作：

- 核准事件。
- 拒絕事件。
- 執行自訂動作。
- 刪除事件。

您必須建立一個政策，其中至少包含一個在所指定的資料夾中建立隔離事件的動作。若發生政策違規，就會在該資料夾中建立事件，以供您檢閱及採取動作。

保留於內容事件資料夾中的郵件，在經過補救或被清除程式清除之前皆會繼續保留在資料夾中。

請參閱第 371 頁的「檢視內容事件資料夾中的事件」。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

請參閱第 372 頁的「內容事件動作」。

請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

建立事件通知

發生事件時，Symantec Messaging Gateway 可以通知您所指定的人員。Symantec Messaging Gateway 會提供預設的通知郵件，您可以依需要對其加以修改。

您可以自訂通知訊息，讓收件者可以檢視或透過按下電子郵件通知訊息中之連結以補救事件。該連結將會讓使用者移至控管中心頁面以解決事件。您也可以指定使用者在按下連結後是否仍必須輸入其憑證以存取控管中心，或可以進行自動驗證。

請參閱第 370 頁的「關於從電子郵件通知補救事件」。

請參閱第 363 頁的「內容過濾通知變數」。

請參閱第 403 頁的「將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合」。

您可以讓每一個事件資料夾具有一個通知郵件。該郵件可以是唯一的，或可以在不同的事件資料夾使用的相同的郵件。

附註：本通知與通知資源並不相同。通知資源可讓您對郵件寄件者、郵件收件者，或是第三方傳送通知郵件，以表示已違反某一政策。通知資源是在政策動作設定為**「傳送通知」**時所傳送的通知。

請參閱第 321 頁的「關於政策違規通知」。

您必須具有「完整的管理」權限或修改設定值的權限，才能建立事件通知。

請參閱第 566 頁的「管理員權限」。

建立事件通知

1. 在控管中心內，按下**「內容」>「設定」>「內容事件資料夾」**。
2. 在**「內容事件資料夾」**清單中，按下您想要建立事件通知郵件的內容事件資料夾名稱。

   或者，也可以勾選內容事件資料夾名稱旁邊的方塊，再按下**「編輯」**。
3. 在**「內容事件資料夾設定」**頁面的**「通知設定」**下，按下**「通知格式」**下拉式清單，並選擇您想要使用通知郵件的格式。

   您可以選擇多重格式 (HTML 和文字)、僅 HTML 或僅文字。
4. 如果您要修改通知郵件，請按下**「通知範本」**旁邊的**「編輯」**。
5. 在**「通知範本」**頁面上，在**「編碼類型」**下，按下拉式清單並選擇通知郵件的字元編碼。
6. 在**「寄件者」**方塊中，輸入要在資安事端通知郵件中顯示的 `From` 標頭的位址。
7. 在**「主旨」**方塊中，輸入您想在資安事端通知郵件中顯示的 `Subject` 標頭。
8. 在**「通知」**方塊中，視需要修改文字。
9. 按下**「儲存」**。
10. 在**「每個通知的摘要項目數上限」**欄位中，輸入您希望要包含在通知郵件中的項目數上限。
11. 按下**「通知頻率」**下拉式清單，然後指定您希望 Symantec Messaging Gateway 多久寄送一次通知。

12 在「**通知開始時間**」中，按下下拉式功能表，然後指定 Symantec Messaging Gateway 開始寄送通知的時間。

13 若想指定應由誰接收本通知，請進行下列任何一項工作：

通知管理員	在「**管理員通知**」下，勾選您想要其接收本通知的管理員旁的方塊。
通知非管理員的人員	在「**通知收件者地址**」方塊中，輸入任何您想要其接收通知郵件的人的電子郵件地址。 請以逗號分隔多個項目。

14 按下「**儲存**」。

關於從電子郵件通知補救事件

您可以架構 Symantec Messaging Gateway 以傳送通知給管理員或通知收件者，以通知管理員或通知收件者已建立了內容過濾事件。您也可以指定想要傳送通知的頻率，以及包含於通知郵件中的事件數量上限。

請參閱第 361 頁的「建立內容事件資料夾」。

根據預設，通知郵件包含了各事件的簡短說明。但是，您可以自訂通知郵件，使其包含讓使用者可以前往控管中心頁面的連結，以便使用者在控管中心處理事件。您也可以指定在使用者補救事件之前是否允許其自動驗證，或是否必須輸入其憑證才能存取控管中心。

請參閱第 363 頁的「內容過濾通知變數」。

如果事件位於資訊資料夾中，則通知郵件會包含檢視事件的連結。如果事件位於隔離事件資料夾中，則郵件會包含檢視並補救事件的連結。若要補救事件，使用者可以加以核准、拒絕，或是套用自訂動作 (如果有定義自訂動作)。

請參閱第 285 頁的「將動作新增至內容過濾政策」。

具有控管中心存取權限的使用者將能前往控管中心內適當的資料夾事件頁面， 並在此頁面上檢視並補救事件。沒有控管中心存取權限的使用者會看到控管中心內顯示了郵件摘要詳細資料的頁面， 但無法看見其他頁面，或瀏覽到控管中心內任何其他位置。

若使用者可以自動驗證，則在通知中按下的連結將會自動套用到事件。必須進行驗證的使用者將會前往控管中心登入頁面，且必須輸入其憑證。登入後，這些使用者便會自動前往能夠檢視或補救事件的頁面。管理員和通知收件者皆可自動驗證。

附註：您必須允許沒有控管中心存取權限的使用者進行自動驗證。否則，他們便無法看到事件詳細資料，也無法補救隔離事件。

如果您要與 Enforce Server 整合，則使用者按下補救連結時所採取的動作將會在下次更新發生時於 Enforce Server 管理主控台上更新。

請參閱第 388 頁的「架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料」。

檢視內容事件資料夾中的事件

您可以在**「事件管理」**頁面上執行下列任一工作以檢視事件：

- 使用過濾來縮小或擴大事件的搜尋範圍。
- 從該頁面檢視特定事件的詳細資料。
- 以遞增順序或遞減順序對欄排序。

可以將**「資料夾總覽」**連結用於所有內容事件資料夾的高級摘要，也可以一次用於一個資料夾的高級摘要。

Symantec Messaging Gateway 在**「事件管理」**頁面上提供下列工具，以協助您自訂檢視及在事件中進行瀏覽：

每頁的項目數	此設定可讓您指定要在每個頁面上顯示的項目數量。您可以指定 10、25、50、100、200、或 500。
顯示	此設定可讓您指定要顯示的項目範圍。
向前及向後箭頭	使用向後 (<|) 及向前 (|>) 箭頭，可以移至第一頁或最後一頁。 使用向後 (<|) 及向前 (|>) 箭頭，可以一次向前或向後移動一個頁面。

在您對資安事端執行動作 (刪除或封存) 或清除資安事端之前，資安事端會保留在內容資安事端資料夾中。

若要檢視事件資料夾的內容，您必須具有「完整的管理」權限或分別存取每個內容事件資料夾的權限。

檢視內容事件資料夾中所含內容的摘要

1 在控管中心內，按下**「內容」>「資料夾總覽」**。

依預設，所有資料夾均顯示在**「內容事件」**表格中。

2 在**「內容事件資料夾」**下拉式清單中，選取您要查看總覽的資料夾。

3 按下**「顯示」**。

狀態將顯示在**「內容事件資料夾」**表格中。

檢視內容事件資料夾中的事件

1 在控管中心內，按下**「內容」**。

2 在**「事件管理」**工作窗格中，選取包含您要檢視之事件的資料夾。

請參閱第 385 頁的「升級現有內容對相符文字功能的影響 」。

請參閱第 368 頁的「關於監控及因應事件」。

請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

請參閱第 372 頁的「內容事件動作」。

一次對多個事件執行動作

您可以一次對多個事件執行相同的動作。 例如，您可能要拒絕來自特定寄件者的所有事件。

請參閱第 372 頁的「內容事件動作」。

若要對事件資料夾中的事件執行動作，您必須具有「完整的管理」權限或分別存取每個內容事件資料夾的權限。

一次對多個事件執行動作

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**工作窗格中，選取包含您要執行動作之事件的資料夾。
3. 針對您要執行動作的所有事件，勾選這些事件 ID 旁的方塊。

   勾選「事件 ID」欄標題旁的方塊，以選取該頁面上顯示的所有事件。
4. 按下您要對所選所有事件執行之工作的選項。

   請參閱第 368 頁的「關於監控及因應事件」。
5. 執行需要的步驟完成動作。

   例如，如果要匯出事件，則必須指定要匯出檔案的目的位置。

內容事件動作

表 16-4 列出了您可以對內容事件資料夾中的事件採取的動作。

表 16-4 內容事件動作

動作	說明
封存	封存事件。 您可以一次封存單一事件，也可以一次封存多個事件。 請參閱第 374 頁的「封存事件」。
匯出事件歷史記錄	將事件的歷史記錄匯出到指定的位置。 您可以一次匯出單一事件的歷史記錄，也可以一次匯出多個事件歷史記錄。 請參閱第 378 頁的「匯出事件的歷史記錄」。

動作	說明
轉寄事件	將事件轉寄到指定的電子郵件地址。 您可以新增電子郵件的主旨及註解， 還可以選取郵件編碼，並指定轉寄郵件時是否包括原始郵件。 您可以一次轉寄單一事件，也可以一次轉寄多個事件。 請參閱第 378 頁的「轉寄事件」。
刪除事件	一次刪除單一事件，或一次刪除多個事件。 請參閱第 379 頁的「刪除事件」。
補救事件	指定如何對已隔離的事件執行動作。 當您在隔離事件資料夾中補救事件時，Symantec Messaging Gateway 會採取您為內容過濾政策動作中指定的動作：**「郵件檢閱核准的動作」**、**「郵件檢閱拒絕的動作」**及**「郵件檢閱自訂動作」**。 您可以一次補救一個事件，也可以一次補救多個事件。您可以指定一次只保留單一事件。 請參閱第 381 頁的「補救已隔離的事件」。
更新事件狀態	指定事件的狀態。 狀態選項如下： ■ 新增 ■ 作用中 ■ 已確認 ■ 誤報 您一次只能變更單一事件的狀態。 請參閱第 382 頁的「更新事件的狀態」。
修改事件的嚴重性	指定事件的嚴重性。 嚴重性層級如下： ■ 不明 ■ 高 ■ 中 ■ 低 您一次只能變更單一事件的嚴重性。 請參閱第 382 頁的「變更事件的嚴重性層級」。

動作	說明
檢閱事件的歷史記錄	顯示事件的整個歷史記錄。 歷史記錄可包括事件建立時間、狀態或嚴重性的變更時間，或採取動作的時間。事件歷史記錄包含事件發生的日期與時間，以及您建立的與事件相關的所有註解。 您一次只能檢視一個事件的歷史記錄。 請參閱第 383 頁的「檢視事件的歷史記錄」。

請參閱第 368 頁的「關於監控及因應事件」。

請參閱第 359 頁的「關於內容事件資料夾」。

請參閱第 384 頁的「檢視違反內容過濾政策的文字」。

封存事件

檢閱事件並採取所需動作之後，即可封存郵件。您可以從「資安事端管理程式」頁面中封存一或多封郵件，也可以從事件的詳細資料頁面中一次封存一封郵件。

請參閱第 368 頁的「關於監控及因應事件」。

請參閱第 356 頁的「指定封存郵件的儲存位置」。

若要封存事件，您必須具有「完整的管理」權限或檢視特定內容事件資料夾的權限。

從「事件管理」頁面封存事件

1 在控管中心內，按下**「內容」**。

2 在**「事件管理」**下，選取包含您要檢閱及封存之事件的資料夾。

3 勾選您要封存之一或多個事件旁的方塊。

4 按下**「封存」**。

從「事件管理」詳細資料頁面封存事件

1 在控管中心內，按下**「內容」**。

2 在**「事件管理」**下，選取包含您要檢閱及封存之事件的資料夾。

3 在**「事件 ID」**欄中，按下您要檢閱及封存的事件編號。

4 在**「事件管理」**詳細資料頁面中，於右窗格內的**「事件動作」**下，按下**「封存」**。

監控垃圾郵件提交

您可以監控您的組織針對控管中心內之客戶特定規則所做出的提交。

下面是您可以從垃圾郵件提交詳細資料確認的詳細資料：

- 最常提交郵件的使用者。
- 提交頻率最高的郵件類型 (遺漏垃圾郵件或誤報)。
- 是否有來自於特定電子郵件寄件者或寄到單一目標收件者的異常大量提交。
- 提交的郵件是否有效，以及是否因此導致自訂規則的出現。如果郵件無效的話，其無效的原因為何。
- 因該次提交而建立的規則目前是否仍在作用中。如果仍在作用中的話，該規則所偵測到的違規郵件數量。

控管中心讓您過濾垃圾郵件提交，以更輕鬆地找出想要的資訊。按下搜尋結果中的任何項目，以檢視**「提交詳細資料」**頁面，其中提供了更多關於提交和相關郵件的資訊。

請參閱第 228 頁的「如何建立規則，以及為何郵件可能不會產生自訂規則」。

您必須具有「完整的管理權限」、「管理垃圾郵件提交」或「管理狀態和日誌」的檢視或修改權限，才能檢視**「提交」**和**「提交詳細資料」**頁面。

監控垃圾郵件提交

1 在控管中心內，按下**「狀態」>「提交」>「提交詳細資料」**。

2 在**「提交」**頁面上按下**「提交類型」**下拉式功能表以指定要過濾的提交類型。

您可以選取下列任一選項：

- **無限制**
- **遺漏的垃圾郵件**
- **錯誤識別為垃圾郵件**

3 按下**「提交者類型」**下拉式功能表並選取提交者類別。

您可以從下列選項中選取：

- **全部**
- **管理**
- **已攔截**
- **一般使用者**

4 按下**「時間範圍」**下拉式功能表以指定提交郵件的時間。

您可以選取下列任一選項：

- **過去 1 小時內**
- **過去 1 天內**
- **過去 1 週內**
- **過去 1 個月內**

- **自訂**
  選取此選項時，您可以指定開始日期和時間，以及結束日期和時間。

5 按下「**主旨**」下拉式功能表以指定郵件的主旨。

根據下列搜尋條件指定主旨內容：

- **符合/不相符**
- 依如下所示指定符合/不相符條件：
  - **子字串 (區分大小寫)**
  - **子字串 (不區分大小寫)**
  - **完全相符 (區分大小寫)**
  - **完全相符 (不區分大小寫)**
  - **萬用字元運算式**
    此欄位接受下列標籤符號字元：點 (.)、小老鼠 (@)、連字號 (-) 和底線 (_)。星號 (*) 將被辨識為萬用字元 metacharacter。
- 在相鄰的文字方塊中輸入字串、文字或萬用字元運算式。

6 根據下列搜尋條件指定特定提交者電子郵件地址：

- **符合/不相符**
- 依如下所示指定符合/不相符條件：
  - **子字串 (區分大小寫)**
  - **子字串 (不區分大小寫)**
  - **完全相符 (區分大小寫)**
  - **完全相符 (不區分大小寫)**
  - **萬用字元運算式**
    此欄位接受下列標籤符號字元：點 (.)、小老鼠 (@)、連字號 (-) 和底線 (_)。星號 (*) 將被辨識為萬用字元 metacharacter。
- 在相鄰的文字方塊中輸入字串、文字或萬用字元運算式。

7 根據下列搜尋條件指定特定寄件者：

- **符合/不相符**
- 依如下所示指定符合/不相符條件：
  - **子字串 (區分大小寫)**
  - **子字串 (不區分大小寫)**
  - **完全相符 (區分大小寫)**

- **完全相符 (不區分大小寫)**
- **萬用字元運算式**
  此欄位接受下列標籤符號字元：點 (.)、小老鼠 (@)、連字號 (-) 和底線 (_)。星號 (*) 將被辨識為萬用字元 metacharacter。

- 在相鄰的文字方塊中輸入字串、文字或萬用字元運算式。

8 根據下列搜尋條件指定目標收件者：

- **符合/不相符**
- 依如下所示指定符合/不相符條件：
  - **子字串 (區分大小寫)**
  - **子字串 (不區分大小寫)**
  - **完全相符 (區分大小寫)**
  - **完全相符 (不區分大小寫)**
  - **萬用字元運算式**
    此欄位接受下列標籤符號字元：點 (.)、小老鼠 (@)、連字號 (-) 和底線 (_)。星號 (*) 將被辨識為萬用字元 metacharacter。
- 在相鄰的文字方塊中輸入字串、文字或萬用字元運算式。

9 選取下列其中一個選項：

清除過濾器	清除記憶體中目前的過濾條件。
顯示已過濾	搜尋並顯示符合條件的郵件。 選取此選項時，符合的提交會顯示在表格中。

10 若要檢視更多關於特定提交的資訊，請按下該項目以檢視**「提交詳細資料」**頁面。

11 或者，如果您想要匯出搜尋結果，請完成下列所有步驟：

- 按下**「匯出 CSV」**。
- 在**「匯出提交狀態」**對話方塊中，按下**「檔案編碼」**下拉式清單並指定您想要使用的編碼類型。
- 按下**「CSV 分隔符號」**下拉式清單並選取分隔符號類型。
- 按下**「匯出」**。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

匯出事件的歷史記錄

您可以匯出有關事件之歷史記錄的所有資訊，例如事件的建立時間、狀態的變更時間、郵件檢閱動作及註解。您可以選取要用於匯出的編碼及分隔符號。

您可以一次匯出一或多個事件歷史記錄。若要匯出事件的歷史記錄，您必須具有「完整的管理」權限或檢視特定內容事件資料夾的權限。

請參閱第 368 頁的「關於監控及因應事件」。

請參閱第 383 頁的「檢視事件的歷史記錄」。

匯出事件的歷史記錄

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**下，選取包含您要匯出之事件歷史記錄的資料夾。
3. 勾選您要匯出其歷史記錄之一或多個事件旁的方塊。
4. 按下**「編碼」**下拉式清單以選取編碼。
5. 按下**「分隔符號」**下拉式清單，以選取您要使用的分隔符號。
6. 按下**「匯出事件歷史記錄」**，以匯出事件歷史記錄。
7. 選取是要儲存檔案還是要開啟檔案。如果您要儲存檔案，請瀏覽並選取所需的位置。

轉寄事件

您可以轉寄事件資料夾中的事件，以進行進一步檢閱。轉寄事件時，您可以為接收轉寄郵件的人建立註解，以提供指示或期限。您也可以指定是否要附加原始郵件。

您可以從**「事件管理」**頁面轉寄一或多封郵件，也可以從事件的詳細資料頁面一次轉寄一個事件。

若要轉寄事件，您必須具有「完整的管理」權限或修改特定內容事件資料夾的權限。

請參閱第 368 頁的「關於監控及因應事件」。

從「事件管理」頁面轉寄事件

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**下，選取含有您要檢閱和轉寄之事件的資料夾。
3. 勾選您要轉寄之一或多個事件旁的方塊。
4. 按下**「轉寄事件」**。
5. 在**「轉寄郵件」**頁面的**「編碼」**下，按下拉式清單來選取編碼類型。
6. 在**「郵件內容」**下的**「轉寄至」**文字方塊中，輸入電子郵件地址。
7. 在**「主旨」**文字方塊中，輸入主旨名稱。

8 如果您想轉寄郵件而不進行任何修改，請勾選**「轉寄原始郵件」**。

此動作會以郵件的原始狀態轉寄郵件，不採取可能影響郵件的任何以政策為基礎的動作(例如移除或清除附件)。

9 在**「註解」**文字方塊中，輸入要隨著事件電子郵件一起傳送的訊息。

10 按下**「傳送」**。

從「事件管理」詳細資料頁面轉寄事件

1 在控管中心內，按下**「內容」**。

2 在**「事件管理」**下，選取含有您要檢閱和轉寄之事件的資料夾。

3 在**「事件 ID」**欄中，按下您要檢視並轉寄的事件編號。

4 在**「事件管理」**詳細資料頁面右窗格的**「事件動作」**下，按下**「轉寄」**。

5 在**「轉寄郵件」**頁面的**「編碼」**下，按下拉式清單來選取編碼類型。

6 在**「郵件內容」**下的**「轉寄至」**文字方塊中，輸入電子郵件地址。

7 在**「主旨」**文字方塊中，輸入主旨名稱。

8 如果您想轉寄郵件而不進行任何修改，請勾選**「轉寄原始郵件」**。

此動作會以郵件的原始狀態轉寄郵件，不採取可能影響郵件的任何以政策為基礎的動作(例如移除或清除附件)。

9 在**「註解」**文字方塊中，輸入電子郵件要隨附的訊息。

10 按下**「傳送」**。

刪除事件

賽門鐵克建議在檢閱事件和對事件執行動作之後刪除事件，以減少事件資料夾中的事件量。刪除某個事件之後，該事件便不會再顯示於事件資料夾中，且無法擷取該事件。

會自動刪除符合清除程式臨界值的事件。

請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

您可以從「資安事端管理程式」頁面中刪除一或多個郵件，也可以從事件的詳細資料頁面中一次刪除一個事件。

若要刪除事件，您必須具有「完整的管理」權限或檢視特定內容事件資料夾的權限。

請參閱第 368 頁的「關於監控及因應事件」。

從「事件管理」頁面刪除事件

1 在控管中心內，按下**「內容」**。

2 在**「事件管理」**下，選取包含您要檢閱和刪除之事件的資料夾。

3 勾選您要刪除之一或多個事件旁的方塊。

4 按下「**刪除**」。

(可選)您可以按下「**全部刪除**」以刪除該頁面上的所有事件，並在確認對話方塊中，按下「**確定**」。

從「事件管理」詳細資料頁面刪除事件

1 在控管中心內，按下「**內容**」。

2 在「**事件管理**」下，選取包含您要檢閱和刪除之事件的資料夾。

3 在「**事件 ID**」欄中，按下您要檢閱及刪除的事件編號。

4 在「**事件管理**」詳細資料頁面中，於右窗格內的「**事件動作**」下，按下「**刪除**」。

針對客戶特定規則，從隔離所資料夾提交郵件

您可以針對客戶特定規則將內容隔離事件資料夾中的郵件提交到賽門鐵克。但是，管理員必須先架構這些選項，使其出現在內容事件資料夾中。

附註：資訊事件資料夾無法使用這個選項。

請參閱第 365 頁的「架構郵件提交選項，使其顯示於隔離事件資料夾中」。

您必須擁有「完整的管理權限」或「管理垃圾郵件提交」修改權限，才能提交郵件。您也必須具有修改或檢視權限，才能存取特定內容事件資料夾。

若要針對客戶特定規則，從隔離所資料夾提交郵件

1 在控管中心內，按下「**內容**」。

2 在「**事件管理**」下，選取包含您要針對自訂規則提交之郵件的內容隔離事件資料夾。

3 執行下列其中一項工作：

若要從「**隔離事件**」頁面提交一個或多個郵件	在「**事件 ID**」欄中，勾選要提交之郵件旁的方塊，然後按下「**這是垃圾郵件**」或「**這不是垃圾郵件**」。
若要先檢視事件詳細資料再提交郵件	在「**事件 ID**」欄中，連按兩下事件編號以檢視其詳細資料，然後在「**內容事件管理**」頁面上按下「**這是垃圾郵件**」或「**這不是垃圾郵件**」。

4 在確認對話方塊中，視需要按下「**這是垃圾郵件**」或「**這不是垃圾郵件**」。

如果提交成功，則提交類型將會出現在所選取郵件的「**提交狀態**」欄中。

請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

請參閱第 366 頁的「監控及因應事件」。

補救已隔離的事件

檢閱隔離事件資料夾中的事件後，您可以進行補救(核准、拒絕或套用自訂動作)。您也可以繼續保留該事件。

當您補救隔離事件資料夾中的事件時，Symantec Messaging Gateway 會採取您在內容過濾政策中，針對以下項目所指定的動作：

- 郵件檢閱核准的動作
- 郵件檢閱拒絕的動作
- 郵件檢閱自訂動作

請參閱第 285 頁的「將動作新增至內容過濾政策」。

例如，假設您建立了一個內容過濾政策，其動作是在**「隔離事件」**資料夾中建立事件。**「郵件檢閱核准的動作」**是傳送郵件。**「郵件檢閱拒絕的動作」**是刪除郵件。**「郵件檢閱自訂動作」**是封存郵件。假設違反此政策，且在**「隔離事件」**資料夾中建立了一個事件。如果您核准該事件，便會傳送該郵件。如果拒絕該事件，則會刪除該郵件。如果選取自訂動作，便會封存郵件。

如果已與 Enforce Server 整合，則可以透過 Symantec Messaging Gateway 控管中心或 Enforce Server 管理主控台來補救事件。透過 Enforce Server 管理主控台補救時，Symantec Messaging Gateway 和 Enforce Server 上的狀態都會立即更新。不過，透過通知郵件連結或透過控管中心採取的補救動作，只有在 Symantec Messaging Gateway 透過 Enforce Server 更新其資料時，才會在 Enforce Server 管理主控台上進行更新。

請參閱第 388 頁的「架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料」。

請參閱第 403 頁的「將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合」。

您可以從**「事件管理」**頁面中補救一或多個郵件。您可以從事件的詳細資料頁面中，一次補救或繼續保留一個事件。

請參閱第 368 頁的「關於監控及因應事件」。

若要補救事件，您必須具有「完整的管理」權限或修改特定內容事件資料夾的權限。

從「事件管理」頁面補救已隔離的事件

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**下，選取包含您要檢閱和補救之事件的隔離事件資料夾。
3. 勾選您要補救之一或多個事件旁的方塊。
4. 按下**「核准」**、**「拒絕」**或**「自訂」**。

從「事件管理」詳細資料頁面補救已隔離的事件

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**下，選取包含您要補救或繼續保留之事件的隔離事件資料夾。

3 在「**事件 ID**」欄中，按下您要檢閱、補救或繼續保留的事件編號。

4 在「**事件管理**」詳細資料頁面的右窗格中，按下「**郵件檢閱動作**」下拉式清單，然後選取您要採取的動作。

5 (可選) 在「**註解**」方塊中輸入有關該動作的註解。

6 按下「**更新**」。

更新事件的狀態

您可以更新事件的狀態來反映對事件的變更。事件的狀態可讓檢閱者瞭解事件目前處於檢閱程序的哪個階段，以及檢閱的結果為何。

狀態選項如下：

新增	事件已發生，但狀態尚未更新。 此設定是最初建立事件時為其指派的預設狀態。
作用中	表示正在檢視事件。
已確認	表示事件有效。
誤報	表示事件無效。

您一次只能變更單一事件的狀態。

請參閱第 368 頁的「關於監控及因應事件」。

若要更新事件的狀態，您必須具有「完整的管理」權限或檢視特定內容事件資料夾的權限。

更新事件的狀態

1 在控管中心內，按下「**內容**」。

2 在「**事件管理**」下，選取包含您要檢閱、補救或繼續保留之事件的隔離事件資料夾。

3 在「**事件 ID**」欄中，按下您要檢閱、補救或繼續保留的事件編號。

4 在「**事件管理**」詳細資料頁面的右窗格中，按「**更新狀態至**」下拉式清單，然後選取新狀態。

5 (可選) 在「**註解**」方塊中輸入註解。

6 按下「**更新**」。

變更事件的嚴重性層級

檢閱事件時，可以修改其嚴重性層級。

嚴重性層級如下：

- 不明

此設定為事件建立時的預設嚴重性。

- 高
- 中
- 低

您一次只能變更單一事件的嚴重性。

請參閱第 368 頁的「關於監控及因應事件」。

若要更新事件的嚴重性，您必須具有「完整的管理」權限或檢視特定內容事件資料夾的權限。

更新事件的嚴重性

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**下，選取包含您要變更其嚴重性之事件的資料夾。
3. 在**「事件 ID」**欄中，按下您要變更其嚴重性的事件編號。
4. 在**「事件管理」**詳細資料頁面的右窗格中，按**「更新嚴重性至」**下拉式清單，然後選取新狀態。
5. (可選) 在**「註解」**方塊中輸入註解。
6. 按下**「更新」**。

檢視事件的歷史記錄

您可以檢視事件的歷史記錄以查看事件的進度。

您一次只能檢視單一事件的歷史記錄。

請參閱第 368 頁的「關於監控及因應事件」。

若要檢視事件的歷史記錄，您必須具有「完整的管理」權限或檢視特定內容事件資料夾的權限。

請參閱第 378 頁的「匯出事件的歷史記錄」。

檢視事件的歷史記錄

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**下，選取包含您要檢閱之事件歷史記錄的資料夾。
3. 在**「事件 ID」**欄中，按下您要檢閱其歷史記錄的事件編號。

   事件歷史記錄將顯示在**「事件管理」**詳細資料頁面的**「事件歷史記錄」**下。

檢視違反內容過濾政策的文字

Symantec Messaging Gateway 可以識別違反內容過濾政策的文字。它也會指出包含該文字的郵件部分 (例如，郵件主旨行或郵件內文)。當您檢視特定事件的詳細資料時，可以查看此資訊。您可以使用此資訊來協助您微調及疑難排解內容過濾政策。

可讓您檢視違反政策之文字的唯一內容過濾條件如下：

- 含有
- 符合規則運算式
- 符合樣式
- 始於
- 結束於
- 完全相符

對於每一封郵件，Symantec Messaging Gateway 可以顯示每個政策群組最多 50 個相符字串。每個相符字串僅顯示文字的前 100 個位元組。

附註：在升級至 Symantec Messaging Gateway 9.5 之前，無法對任何已存在的事件使用此功能。

若要檢視事件資料夾的內容，您必須具有「完整的管理」權限或分別存取每個內容事件資料夾的權限。

檢視違反內容過濾政策的文字

1. 在控管中心內，按下**「內容」**。
2. 在**「事件管理」**工作窗格中，選取包含您要檢視之事件的內容事件資料夾。
3. 在**「事件 ID」**欄中，按下您要檢視其詳細資料之事件的事件 ID 號碼。
4. 在**「事件詳細資料」**下，按下**「郵件掃描結果: <政策名稱>」**旁的超連結，以檢視違反政策的內容。該超連結是政策的名稱。

   違反政策的文字及包含該文字的郵件部分會顯示在**「<政策名稱> 政策相符文字」**視窗中。

   例如，名稱 XYZ 的政策是內容過濾政策。當電子郵件違反此政策時，請在**「事件詳細資料」**下，按下**「郵件掃描結果: XYZ」**中的 XYZ 超連結。您可以檢視違反政策 XYZ 的內容。違反政策的文字及包含該文字的郵件部分會顯示在**「XYZ 政策相符文字」**視窗中。
5. 按下**「關閉」**以關閉**「<政策名稱> 政策相符文字」**視窗。

   顯示在此視窗中的**「<政策名稱>」**是導致郵件被傳送至事件資料夾之政策的名稱。

請參閱第 385 頁的「升級現有內容對相符文字功能的影響 」。

請參閱第 283 頁的「內容過濾條件比對條件」。

請參閱第 368 頁的「關於監控及因應事件」。

升級現有內容對相符文字功能的影響

當您從 Symantec Brightmail Gateway 9.0.x 版或更舊版本升級時，會保留您先前的設定及這些設定的行為。不過，在升級至 Symantec Messaging Gateway 9.5 更新版本之前，您無法對郵件稽核日誌中存在的任何郵件使用相符文字功能。在升級之前，也同樣無法對內容事件資料夾中的事件使用相符文字功能。

當您選擇檢視已存在之郵件的相符文字資訊時，**「<政策名稱> 政策相符文字」**視窗會顯示下列訊息：

```
Policy Match Text information is not available.
```

請參閱第 384 頁的「檢視違反內容過濾政策的文字」。

請參閱第 300 頁的「郵件稽核日誌如何協助微調及疑難排解內容過濾政策」。

請參閱第 283 頁的「內容過濾條件比對條件」。

使用 Symantec Content Encryption 加密資料

Symantec Messaging Gateway 會使用由 Symantec Email Security.Cloud 提供的 Symantec Content Encryption，加密離埠郵件以獲得更高的安全性。

您必須購買 Symantec Content Encryption 授權、架構系統以進行加密、佈建加密帳戶，才能使用 Symantec Content Encryption。然後，建立和指派加密離埠郵件的政策。

您可以在控管中心的「狀態」控制面板中追蹤加密的郵件統計資料，以及在「郵件稽核日誌」報告中檢視郵件日誌。

表 16-5說明如何設定及架構 Symantec Content Encryption 對離埠郵件進行加密的程序。

表 16-5　　加密離埠郵件資料

步驟	說明
步驟 1：購買 Symantec Content Encryption 授權。	您可以在下列頁面上找到授權資訊： **「內容」>「設定」>「內容加密」** 請參閱第 614 頁的「授權您的產品」。
步驟 2：架構您的硬體裝置。	從支援的憑證授權中心購買並安裝 SSL 憑證，然後架構主機以進行內容加密。 請參閱第 386 頁的「準備好系統以進行內容加密」。
步驟 3：架構主機和通訊埠。	下一步您必須為加密帳戶架構主機資訊和通訊埠資訊。 請參閱第 387 頁的「管理內容加密的主機與通訊埠資訊」。

步驟	說明
步驟 4：佈建您的加密帳戶。	若要將內容加密套用至郵件，您必須與賽門鐵克合作來佈建加密帳戶。 請參閱第 387 頁的「 佈建內容加密帳戶」。
步驟 5：使用動作**「傳送內容加密的郵件」**建立內容政策。	為硬體裝置設定並架構內容加密後，您可以建立內容過濾政策，以使用離埠郵件加密。 請參閱第 278 頁的「建立內容過濾政策」。

準備好系統以進行內容加密

取得內容加密授權後，您必須透過賽門鐵克來佈建帳戶，然後再架構系統以進行內容加密。若要架構系統以進行內容加密，您必須在透過賽門鐵克開始佈建程序之前或之後，完成本主題所述的工作。您必須先完成這些工作，才能使用新的加密帳戶。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

準備憑證

1 必要時，請為網域提供防護，並購買網域的憑證。

您必須使用賽門鐵克提供之佈建表單中所列的憑證授權中心 (CA)。如果您已擁有憑證，但是該憑證不在核准 CA 的清單上，則需要使用此清單中的 CA 憑證來取代您的憑證。

2 在 Symantec Messaging Gateway 中，按下**「管理」>「設定」>「憑證」**，再按下**「TLS 和 HTTP 憑證」**標籤來要求和建立新憑證。

請參閱第 151 頁的「要求憑證授權中心簽署的憑證」。

3 匯入 CA 所核發的憑證。憑證的「主旨一般名稱」必須與 Symantec Messaging Gateway 主機的完整網域名稱相符。例如，如果 update5.brightmailtest.info 是您用來接收郵件的 Symantec Messaging Gateway 主機名稱，則憑證及連線到該主機的 SMTP 用戶端都必須使用 update5.brightmailtest.info 為「主旨一般名稱」。

請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。

4 將 CA 憑證或 CA 憑證組新增至系統。

請參閱第 150 頁的「新增 CA 或中繼憑證」。

架構主機以進行內容加密

1 按下**「管理」>「主機」>「組態」**。

2 選取第一個主機，並按下**「編輯」**，然後再按 **SMTP** 標籤。

3 在**「郵件過濾」**下，確認您已選取**「僅入埠郵件過濾」**或**「入埠和離埠郵件過濾」**。

4 在**「入埠郵件設定」**下，勾選**「接受 TLS 加密」**並選取新的憑證。

5 您可以選擇性勾選**「要求用戶端憑證」**。

此選項會將用戶端憑證驗證交易新增到 Received 標頭中。此資訊對於建立政策可能很有幫助。

6 如果您的主機僅使用一個 IP 位址，請按下**「儲存」**以儲存您的變更，然後重複步驟 2 到 5 為下一台主機啟用 TLS。

如果您的主機使用多個 IP 位址，請移至步驟 7。

7 按頁面最下方的**「進階設定」**以顯示 SMTP 組態頁面。

8 在**「傳送」**標籤的**「SMTP 傳送繫結」**下，將**「動態繞送的郵件」**設定為**「自動」**。

9 按下**「繼續」**回到**「編輯主機組態」**頁面。

10 按下**「儲存」**儲存對此主機所做的變更。

使用此程序可架構所有主機進行 TLS 加密。

管理內容加密的主機與通訊埠資訊

佈建的加密帳戶之主機資訊是由賽門鐵克佈建代表來決定，該代表會決定最適合您系統的主機與通訊埠。

本節說明如何管理加密帳戶的主機與通訊埠資訊。若要佈建加密帳戶，您必須取得授權、架構系統以進行加密、與佈建代表合作來佈建帳戶，然後建立指示系統加密離埠郵件的政策群組。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

編輯內容加密的主機與通訊埠資訊

1 若要檢視「內容加密」主機與通訊埠資訊，請按下**「內容」>「設定」>「內容加密」**，然後按下**「顯示進階」**。

2 若要變更主機資訊，請在**「主機」**欄位中提供新的 Email Security.cloud 加密主機名稱。

3 若要變更通訊埠資訊，請在**「通訊埠」**欄位中提供新的通訊埠。

4 按下**「儲存」**以儲存新的主機與通訊埠資訊。

佈建內容加密帳戶

若要將內容加密套用至郵件，您必須與賽門鐵克合作來佈建加密帳戶。

本節會說明如何佈建現有授權。如果尚未取得 Symantec Content Encryption 授權，可按**「內容」>「設定」>「內容加密」**來瞭解有關該服務的詳細資訊。除了佈建帳戶之外，您還必須架構系統以進行加密，並建立指示系統將離埠郵件加密的政策群組。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

佈建內容加密授權

1 選取**「內容」>「設定」>「內容加密」**。

- 如過您尚未購買 Symantec Content Encryption 授權，則可以透過「內容加密」頁面來瞭解有關該服務的詳細資訊。請按**「按下這裡」**。購買授權後，請移至步驟 2。
- 如果您尚未佈建加密帳戶，則**「內容加密」**頁面會提供連結以加速佈建程序。移至步驟 2。
- 如果您已佈建加密帳戶，則**「內容加密」**頁面會顯示您的授權資訊，並提供主機及通訊埠設定的預設值。 如果此時要編輯您的連線資訊，請按下**「顯示進階」**。
  請參閱第 387 頁的「管理內容加密的主機與通訊埠資訊」。

2 在「內容加密」頁面中，按**「按下這裡」**。

此時會顯示一個頁面，提供可下載的佈建表單，並附有佈建內容加密帳戶的指示。

3 依照指示填寫「內容加密佈建」表單。若要讓加密完全生效，您必須將所有網域及掃描程式的資訊都填入佈建表單中。

如果您之後新增了網域或掃描程式，請務必通知您的賽門鐵克佈建代表。 如需詳細資訊，請按下**「內容」>「設定」>「內容加密」**，然後再按**「按下這裡」**連結，以參閱「Symantec Content Encryption 佈建」頁面。

您還必須架構新主機以進行加密。

請參閱第 386 頁的「準備好系統以進行內容加密」。

4 完成後，請使用電子郵件將佈建表單傳送到提供的電子郵件地址。

寄出填好的表單後，賽門鐵克 Email Security.cloud 團隊的員工將會與您聯絡，以加速佈建帳戶並在帳戶處於作用中狀態時通知您。

請參閱第 387 頁的「管理內容加密的主機與通訊埠資訊」。

架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料

Symantec Messaging Gateway 可以使用 Enforce Server 更新內容過濾事件資訊及其狀態。同步可讓管理員從 Enforce Server 管理主控台檢視目前的 Symantec Messaging Gateway 事件詳細資料。

請參閱第 403 頁的「關於將 Symantec Data Loss Prevention 與 Symantec Messaging Gateway 整合」。

您必須向 Symantec Messaging Gateway 提供正確的 Enforce Server 憑證並指定事件數量和事件資料更新頻率。您指定的憑證必須已經存在於 Enforce Server 上。

如需詳細資訊，請參閱「Symantec Data Loss Prevention 管理指南」中關於管理使用者和角色的方式以及已儲存之憑證的章節。

您必須具有「完整的管理」權限或「管理設定」修改權限，才能架構這些選項。

請參閱第 403 頁的「將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合」。

若要架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料

1. 在控管中心內，按下**「內容」>「設定」>「DLP 連線」**。
2. 按下**「Enforce Server 存取權」**標籤。
3. 勾選**「啟用與 Enforce Server 的連線」**。
4. 在**「已註冊的 Enforce Server 管理主控台主機或 IP 位址」**欄位中指定 Enforce Server 所在之伺服器主機名稱或 IP 位址。
5. 在**「使用者名稱」**欄位中輸入使用者名稱。
6. 在**「密碼」**欄位中輸入密碼。
7. 在**「供狀態更新事件數上限」**欄位中，指定每次更新時可以傳送的事件數量。

   預設值為 5000。
8. 在**「與 Enforce Server 同步的時間間隔 (分鐘)」**中，指定 Enforce Server 和 Symantec Messaging Gateway 同步事件資料的頻率。

   您可以選取的最短時間 (即預設值) 是每 5 分鐘一次。
9. 按下**「儲存」**。

17

使用 Symantec Content Analysis 進行威脅防禦掃描

本章包含以下主題：

- 關於威脅防禦掃描
- 準備 Symantec Content Analysis 以連線至 Symantec Messaging Gateway
- 將 Symantec Messaging Gateway 連線至 Content Analysis 硬體裝置
- 架構威脅防禦掃描設定
- 預設和範例威脅防禦政策
- 建立新的威脅防禦政策集
- 選取用於政策群組的威脅防禦政策
- 檢視 Content Analysis 佇列

關於威脅防禦掃描

透過 Symantec Messaging Gateway 10.6.3 版及更新版本，您可以連線至 Symantec Content Analysis 2.1 版或更新版本以提供威脅防禦掃描。Content Analysis 提供深度內容檢查以實現新一代惡意軟體偵測，並提供 On-box 沙箱以進行真實內部部署分析。透過威脅防禦整合，您可以將這些功能新增至現有 Symantec Messaging Gateway 防護。

威脅防禦會掃描郵件的 HTML 內文及郵件附件。如果附件是純文字檔案、XML 檔案或空白檔案，威脅防禦掃描會忽略此檔案。同時也會忽略郵件的文字內文。如果附件是電子郵件訊息，威脅防禦會以掃描其他任何郵件的相同方式掃描附加的郵件。

下表摘要說明需要在 Symantec Content Analysis 和 Symantec Messaging Gateway 上執行哪些操作來設定威脅防禦掃描。

請參閱第 392 頁的「將 Symantec Messaging Gateway 連線至 Content Analysis 硬體裝置」。

表 17-1 Symantec Messaging Gateway 的設定步驟

步驟	說明
1	在每個 Symantec Content Analysis 硬體裝置上產生 API 金鑰、啟用 HTTPS 管理，並架構通訊埠。 請參閱第 391 頁的「準備 Symantec Content Analysis 以連線至 Symantec Messaging Gateway」。
2	在**「威脅防禦」**>**「設定」**>**「CA 連線」**頁面上架構 Content Analysis 連線設定時，請使用 API 金鑰和通訊埠資訊。 請參閱第 392 頁的「將 Symantec Messaging Gateway 連線至 Content Analysis 硬體裝置」。
3	在**「威脅防禦」**>**「設定」**>**「掃描設定」**頁面上架構掃描設定。 請參閱第 392 頁的「架構威脅防禦掃描設定」。
4	在**「威脅防禦」**>**「政策」**>**「電子郵件」**頁面上對威脅防禦政策進行任何必要變更。 請參閱第 395 頁的「預設和範例威脅防禦政策」。
5	在**「管理」**>**「使用者」**>**「政策群組」**>**「編輯政策群組」**>**「威脅防禦」**標籤上，為每個政策群組啟用 Content Analysis，並選擇適用於群組的政策。 請參閱第 400 頁的「選取用於政策群組的威脅防禦政策」。

準備 Symantec Content Analysis 以連線至 Symantec Messaging Gateway

您必須先在 Content Analysis 硬體裝置上執行特定步驟，然後才能將 Symantec Messaging Gateway 連線至 Content Analysis 硬體裝置。

設定 Symantec Content Analysis 硬體裝置進行威脅防禦掃描

1 為 Content Analysis 和 Symantec Messaging Gateway 之間的介面產生 API 金鑰。

在 Content Analysis 硬體裝置的指令行介面中產生 API 金鑰。如需指示，請參閱「Content Analysis 檔案提交 REST API 開發指南」。

2 啟用**「HTTPS 管理」**並指定**「HTTPS 通訊埠」**

在 Content Analysis 控制中心內，選取**「設定」**>**「Web 管理」**。在**「Web 伺服器」**面板中，選取**「啟用 HTTPS 管理」**並輸入**「通訊埠」**號。

3 確保 Content Analysis 硬體裝置具有有效的憑證。

Content Analysis Web 介面需要憑證。每台 Content Analysis 硬體裝置會一併安裝預設憑證。Content Analysis 硬體裝置上必須安裝預設憑證或者有效的替代憑證。

4 如果您已授權此選項，請啟用 Content Analysis 硬體裝置上的 On-box 沙箱。

如需指示，請參閱「Symantec Content Analysis 2.1 Web 指南」。

附註：在某些情況下，在正由 Symantec Messaging Gateway 使用的 Content Analysis 實例上啟用**「即時沙箱」**來過濾物件可能會快速溢出 Content Analysis 實例，從而導致掃描失敗和「不可掃描」的判斷。

將 Symantec Messaging Gateway 連線至 Content Analysis 硬體裝置

產生 API 金鑰並在 Content Analysis 硬體裝置上架構通訊埠後，請使用下列程序在 Symantec Messaging Gateway 控制中心中架構連線。

在 Symantec Messaging Gateway 中架構 Content Analysis 連線設定

1 在**「威脅防禦」**>**「設定」**>**「CA 連線」**>**「Symantec Content Analysis 設定」**頁面上，針對 Content Analysis 硬體裝置輸入主機名稱或 IP 位址、HTTPS 通訊埠編號以及 API 金鑰。

2 為此硬體裝置指定**喜好設定**。**「喜好設定」**值會引導 Symantec Messaging Gateway 存取作為主要伺服器的一或多台硬體裝置，並且僅當主要伺服器無法使用或忙碌時存取其他硬體裝置。

- 編號越小，喜好設定優先順序越高。例如，Symantec Messaging Gateway 會先嘗試連線至喜好設定為 1 的 Content Analysis 硬體裝置，再嘗試連線至喜好設定為 2 的硬體裝置。
- 如果兩台 Content Analysis 硬體裝置有相同的喜好設定編號，Symantec Messaging Gateway 會嘗試同等使用每台硬體裝置。僅當喜好設定編號較小的兩個主機都無法使用時，才會使用喜好設定編號較高的 Content Analysis 硬體裝置。

架構威脅防禦掃描設定

威脅防禦掃描設定可協助您管理傳送至 Content Analysis 進行掃描的郵件佇列。

其他影響 Content Analysis 佇列的因素，例如：

- 內送流量的數量
- 外寄流量的數量 (如果您的政策包括外寄郵件的威脅防禦掃描)

- 連線的 Content Analysis 硬體裝置的容量和可用性
- 網路效能

將 Content Analysis 硬體裝置連線至 SMG 後，您可能想要評估預設設定的結果，然後根據需要進行調整。

編輯威脅防禦掃描設定

1 在控制中心內，選取**「威脅防禦」**>**「設定」**>**「掃描設定」**>**「威脅防禦掃描設定」**。

2 在**「一般」**標籤 >**「結果快取 TTL」**上，輸入 **7** 至 **90** 分鐘之間的值，以指定快取來自 Content Analysis 的結果或判斷的分鐘數。

- 結果快取會儲存 Content Analysis 為其分析的每個檔案雜湊傳送的判斷。將內送電子郵件中檔案的雜湊值與快取結果比較。如果相符，則 SMG 使用快取結果，並且不會傳送檔案至 Content Analysis 進行掃描。任何不符合快取結果的檔案都將傳送至 Content Analysis 進行掃描。
- 超過 TTL (存留時間) 限制後，會刪除快取結果。含相符雜湊的下一個檔案會傳送至 Content Analysis 以取得更新結果，並且 TTL 計時器會重設。
- 較短的**結果快取 TTL** 會增加 Content Analysis 硬體裝置上的負載，但是會在威脅判斷變更時為您的組織提供更快的更新。例如，當 Content Analysis 收到來自沙箱分析的結果時，威脅判斷可能會變更。但是，較短的 TTL 可能會導致 SMG 將非惡意檔案的許多複本傳送至 Content Analysis 進行掃描。重複的掃描會增加 Content Analysis 硬體裝置上的佇列大小和負載，並且不會增加安全性優勢。
- 較長的**結果快取 TTL** 意味著當 SMG 等待更新快取判斷時，可能會傳送惡意檔案。但是，較長的 TTL 可防止 SMG 將相同的非惡意檔案傳送至 Content Analysis。例如，傳送至散布清單的檔案附件不會移至 Content Analysis 進行重複掃描。
- **「結果快取 TTL」**必須比您在步驟 3 中指定的**「掃描逾時」**至少長 6 分鐘。

3 針對**「掃描逾時」**，輸入 **1** 至 **60** 分鐘之間的值。

「掃描逾時」指定 SMG 等待 Content Analysis 硬體裝置傳回結果的分鐘數。如果超過掃描逾時值，則會根據**「無法掃描是否存在進階威脅」**條件的政策處理郵件。

- 較短的**「掃描逾時」**可能會增加無法掃描的結果數量。
- 套用內嵌政策時，較長的**「掃描逾時」**可能會增加 CA 佇列的大小並導致傳送延遲。

請參閱第 400 頁的「選取用於政策群組的威脅防禦政策」。

4 針對**「Content Analysis 佇列中的郵件數目上限」**，請輸入介於 1 到 1,000,000 之間的值。

「Content Analysis 佇列中的郵件數目上限」值是可在佇列中等待以進行 Content Analysis 掃描的郵件上限。如果 SMG 已開始處理郵件，此限制不會攔截郵件進入 CA 佇列。

5 啟用或停用**「當 Content Analysis 佇列已滿時略過掃描」**，以指定佇列超出限制時 SMG 的動作。

- 啟用**「當 Content Analysis 佇列已滿時略過掃描」**時，SMG 不會傳送檔案和附件至 Content Analysis 進行掃描。SMG 仍使用其他啟用的過濾器掃描郵件。然後根據其他過濾器的政策處理郵件。
- 停用**「當 Content Analysis 佇列已滿時略過掃描」**時，SMG 會延遲入埠郵件。

當 Content Analysis 處理更多郵件，並且佇列大小低於上限時，會恢復正常作業。

6 如果您不想將某些類型的檔案傳送至 Content Analysis 進行掃描，請按下**「排除掃描」**標籤，然後將檔案類型新增至清單。

雖然**「排除掃描」**清單完全獨立於 Content Analysis 和惡意軟體掃描，但您可以採用類似的方式維護清單。您可以依類型或類別排除檔案。您無法依檔案名稱或副檔名從 Content Analysis 掃描排除檔案。

7 按下**「儲存」**。

從威脅防禦掃描中排除檔案類型

Symantec Messaging Gateway 可讓您建立不想傳送到 Content Analysis 以進行威脅防禦掃描的檔案類型清單。您可以建立單一清單，也可以建立多個清單，以協助您分類檔案類型。

為了協助您建立自己的清單，Symantec Messaging Gateway 會提供分組類似檔案類型的檔案類別。您可以選擇檔案類別中的每個檔案類型，也可以選取要從威脅防禦掃描中排除的個別檔案類型。此外，還可以選取**「所有檔案類別」**以建立 SMG 提供的每個檔案類別的清單。

從威脅防禦掃描中排除檔案類型

1 在控制中心，按下**「威脅防禦」>「設定」>「掃描設定」**。

2 在**「排除掃描」**標籤上，按下**「新增」**。

3 在**「排除掃描清單名稱」**方塊中，輸入清單的名稱。

4 在**「檔案類別」**清單中，選取您要從掃描中排除的檔案類別。

- 若要選取多個類別，請按住 **Ctrl** 鍵並同時按下檔案類別的名稱。
- 若要選取**「檔案類別」**清單中的每個檔案類別，請按下**「所有檔案類別」**。

5 **「檔案類型」**清單會顯示與所選檔案類別相關聯的所有檔案類型。

- 若要從威脅防禦掃描中排除**「檔案類型」**清單中的每個檔案類型，請按下**「新增檔案類別」**。
- 若要從排除清單中移除檔案類型，請在按住 **Ctrl** 鍵的同時取消選取檔案類型。然後，按下**「新增檔案類別」**以新增其餘的所選檔案類型。

6 按下**「儲存」**。

檔案類型的名稱隨即出現在**「說明」**清單中。

當您建立新清單時，預設會啟用它。如果您希望 SMG 在掃描期間使用排除掃描清單，則必須啟用該清單。如果某封郵件包含符合已排除檔案類型的附件，SMG 不會將該檔案傳送至 Content

Analysis 進行掃描。在「**威脅防禦**」>「**掃描設定**」>「**排除掃描**」標籤上，可以編輯、刪除、停用、啟用或匯出排除掃描清單。

預設和範例威脅防禦政策

「**威脅防禦**」>「**政策**」>「**電子郵件**」>「**電子郵件威脅防禦政策**」頁面顯示 Symantec Messaging Gateway 為 Symantec Content Analysis 威脅防禦掃描提供的範例政策。這些威脅防禦政策以集的形式進行分組，以在所有掃描條件和威脅防禦判斷下取得特定結果。政策名稱以「**內嵌**」、「**監控**」和「**安全預覽**」開頭，指出應作為集指派給個別政策群組的政策。

- 「**內嵌**」政策可確保在傳送郵件之前對所有郵件進行掃描。
- 「**監控**」政策可確保及時傳送郵件。傳送郵件之後，可能會搜尋惡意軟體。
- 「**安全預覽**」政策可傳送每個郵件的複本 (已刪除附件)。當 Content Analysis 掃描判斷附件並非惡意後，會傳送原始郵件和附件。

依據預設，會將內嵌政策指派給所有政策群組。但是，您必須啟用內嵌政策，或者從「**管理**」>「**政策群組**」頁面，將不同威脅防禦政策集套用至您的群組。

用於「內嵌」模式的預設威脅防禦政策

預設的「內嵌」政策集支援安全性為最重要考量的工作流程。傳送郵件之前，收件者可能會遇到短暫延遲。

當您針對某個群組啟用預設內嵌政策時，未經掃描不應傳送任何郵件。但是，內嵌政策包含通知動作，用於確保收件者知道觸發提早釋放的非預期條件或錯誤。提早釋放意味著在 Content Analysis 掃描郵件之前，收件者會收到郵件複本。例如，如果收件者從具有監控政策的群組移至具有內嵌政策的群組，SMG 可能會在內嵌政策生效之前傳送已感染的郵件。

表 17-2 說明了每個內嵌政策的設定。

表 17-2　　內嵌威脅防禦政策

政策名稱	如果符合下列條件	要對在提早釋放前觸發此政策的郵件採取的動作	要對在提早釋放後觸發此政策的郵件採取的動作
內嵌 - 進階威脅：刪除郵件 (預設)	Content Analysis 在郵件中已偵測到威脅	刪除郵件	寄送通知「威脅防禦 - 進階威脅已傳送」 刪除已傳送進行 Content Analysis 掃描的郵件複本
內嵌 - 無法掃描：使用「[郵件未經威脅防禦掃描]」修改主旨行 (預設)	Content Analysis 無法掃描郵件	在主旨行前面添加「[郵件未經威脅防禦掃描]」並傳送郵件	寄送通知「威脅防禦 - 郵件無法掃描」 刪除已傳送進行 Content Analysis 掃描的郵件複本

政策名稱	如果符合下列條件	要對在提早釋放前觸發此政策的郵件採取的動作	要對在提早釋放後觸發此政策的郵件採取的動作
內嵌 - 非惡意：正常傳送 (預設)	Content Analysis 在郵件中未偵測到威脅	正常傳送郵件	刪除已傳送進行 Content Analysis 掃描的郵件複本

內嵌政策標示為**「(預設)」**。這些預設政策會自動指派給所有政策群組，但是您必須為每個群組明確啟用這些政策。您無法刪除預設政策。

用於「監控」模式的範例威脅防禦政策

「監控」政策集支援無法接受任何電子郵件傳送延遲的工作流程。「監控」模式亦可用於評估在部署到整個組織之前針對測試群組啟用 Content Analysis 掃描的效果。

將所有範例監控政策指派給群組時：

- 郵件會立即傳送給收件者。
- 如果結果快取不包含郵件中附件或檔案的判斷，則 Symantec Messaging Gateway 會將複本傳送至 Content Analysis 進行掃描。
- 如果 Content Analysis 傳回進階威脅或無法掃描的判斷，SMG 會將通知傳送給收件者。
- 如果 Content Analysis 傳回的結果為未偵測到任何威脅，則不會採取進一步動作，因為該郵件已傳送。
- 如果結果快取包含郵件中所有附件和檔案的判斷，則無需將複本傳送至 Content Analysis 進行掃描。Symantec Messaging Gateway 立即執行**「在提早釋放前，要對觸發此政策的郵件採取的動作」**。

下表說明每個監控政策的設定。

表 17-3　　監控模式提早釋放政策

政策名稱	如果符合下列條件	對釋放的複本採取的動作
監控 - 提早釋放：毫不延遲立即傳送	如果 Content Analysis 檢查時間超過 0 秒	正常傳送郵件。 其他隱含動作是將複本傳送至 Content Analysis 進行掃描

表 17-4 依威脅防禦掃描結果的監控模式政策

政策名稱	如果符合下列條件	要對在提早釋放前觸發此政策的郵件採取的動作	要對在提早釋放後觸發此政策的郵件採取的動作
監控 - 進階威脅：寄送通知「威脅防禦 - 進階威脅已傳送」	Content Analysis 在掃描的郵件複本中偵測到威脅。	刪除郵件	寄送通知「威脅防禦 - 進階威脅已傳送」 刪除已傳送進行 Content Analysis 掃描的郵件複本
監控 - 無法掃描：寄送通知「威脅防禦 - 郵件無法掃描」	Content Analysis 無法掃描郵件複本。	在主旨行前面添加「[郵件未經威脅防禦掃描]」並傳送郵件	寄送通知「威脅防禦 - 郵件無法掃描」 刪除已傳送進行 Content Analysis 掃描的郵件複本
監控 - 非惡意：不採取任何動作，郵件已傳送	Content Analysis 在掃描的郵件複本中未偵測到威脅。	正常傳送郵件	刪除已傳送進行 Content Analysis 掃描的郵件複本

用於安全預覽的範例威脅防禦政策

安全預覽政策集支援收件者可以容忍掃描其郵件是否存在威脅時短暫延遲的工作流程。但是，收件者需要採用安全方式來立即接收其郵件的詳細資料。

將所有範例安全預覽政策指派給群組時：

- 附件會從每個郵件的複本中刪除，並且 Symantec Messaging Gateway 會將註釋「威脅防禦 - 安全預覽」新增至每個主旨行。然後這些複本會立即傳送給收件者。
- Symantec Messaging Gateway 會將包含附件的完整郵件傳送至 Content Analysis 進行掃描。
- 如果 Content Analysis 傳回進階威脅或無法掃描的判斷，Symantec Messaging Gateway 會將通知傳送給收件者。
- 如果 Content Analysis 已掃描郵件但未偵測到惡意軟體，則會將原始郵件傳送給收件者。
- 如果結果快取包含郵件中所有附件和檔案的判斷，則無需將複本傳送至 Content Analysis 進行掃描。Symantec Messaging Gateway 立即執行**「在提早釋放前，要對觸發此政策的郵件採取的動作」**。

表 17-6 說明了監控政策的設定。

表 17-5 觸發立即傳送的安全預覽威脅防禦政策

政策名稱	如果符合下列條件	對釋放的複本採取的動作
安全預覽 - 提早釋放：刪除所有附件並毫不延遲立即傳送	如果 Content Analysis 檢查時間超過 0 秒	從郵件中刪除所有附件。新增註釋「威脅防禦 - 安全預覽」並傳送已修改的郵件。 其他隱含動作是將包含附件的完整郵件複本傳送至 Content Analysis 進行掃描。

表 17-6 安全預覽威脅防禦政策

政策名稱	如果符合下列條件	要對在提早釋放前觸發此政策的郵件採取的動作	要對在提早釋放後觸發此政策的郵件採取的動作
安全預覽 - 進階威脅：刪除郵件	Content Analysis 掃描已判斷該郵件包含進階威脅	刪除原始郵件	刪除原始郵件
安全預覽 - 無法掃描：使用「[郵件未經威脅防禦掃描]」修改主旨行並重新傳送含附件的郵件	Content Analysis 無法掃描一或多個附件	在主旨行前面添加「[郵件未經威脅防禦掃描]」並傳送含附件的原始郵件	在主旨行前面添加「[郵件未經威脅防禦掃描]」並傳送含附件的原始郵件
安全預覽 - 非惡意：使用「[威脅防禦掃描已完成，找不到任何威脅]」修改主旨行並重新傳送含附件的郵件	Content Analysis 掃描已判斷該郵件不包含惡意內容	在主旨行前面添加「[威脅防禦掃描已完成，找不到任何威脅]」並傳送含附件的原始郵件	在主旨行前面添加「[威脅防禦掃描已完成，找不到任何威脅]」並傳送含附件的原始郵件

建立新的威脅防禦政策集

範例威脅防禦政策具有可表示政策所屬政策集的名稱。新增威脅防禦政策時，應建立政策集以確保 SMG 在下列所有條件下採取適當的動作：

- **提早釋放**
  「提早釋放」政策具有**「如果 Content Analysis 檢查時間超過 X 秒」**條件。如果您輸入 **0**，SMG 會立即傳送郵件。
  建立「提早釋放」政策時，政策集中的所有其他政策必須與「提早釋放」政策協調一致。例如，如果「提早釋放」政策傳送完整郵件，則相應的「偵測到進階威脅」政策必須指定傳送惡意軟體時要採取的動作。
- **偵測到進階威脅**
  「偵測到進階威脅」政策決定 SMG 如何針對**「如果郵件包含進階威脅」**條件處理郵件。
- **無法掃描**

「無法掃描」政策決定 SMG 如何針對**「如果無法掃描郵件是否存在進階威脅」**條件處理郵件。**絕**大多數無法掃描的檔案不是惡意的，但有些可能是惡意的。

- **非惡意**
  「非惡意」政策決定 SMG 如何針對**「如果郵件不包含進階威脅」**條件處理郵件。

建立威脅防禦政策的最佳實務準則

您指派到政策群組的威脅防禦政策必須針對清單中的每個條件和判斷正確地處理郵件。為避免出現非預期的結果，賽門鐵克建議您從範例政策集的複本建立新的威脅防禦政策集，並遵循下列方針：

- 選擇一個唯一名稱，將其包含在政策集的所有政策名稱中，以識別屬於該政策集的政策。例如，範例政策以內嵌、監控或安全預覽開頭。這種命名慣例可降低將政策指派到政策群組時發生錯誤的機率。
- 即使您只想修改一個或兩個政策，也請複製範例政策集中的全部政策。此做法可讓您將相同的命名慣例套用到整個政策集。
- 為每個政策選擇可說明政策目的的名稱。將政策集名稱附加到此名稱的開頭。例如，無法掃描判斷的「監控」政策將命名為**監控 - 無法掃描：寄送通知「威脅防禦 - 郵件無法掃描」**。

從複本建立新的威脅防禦政策

從現有政策建立威脅防禦政策

1. 在控管中心內，選取**「威脅防禦」>「政策」>「電子郵件」**。
2. 在**「電子郵件威脅防禦政策」**頁面上，按下想要用作起始點的範例政策旁的方塊，然後按下**「複製」**。

   請參閱第 395 頁的「預設和範例威脅防禦政策」。
3. 在出現的**「新增電子郵件威脅防禦政策」**頁面上，輸入政策的名稱。遵循方針以包含政策集名稱和政策目的。
4. 根據需要變更政策條件和動作。例如，您可以：
   - 選擇通知動作，然後從清單選擇通知。該通知將以單獨的電子郵件形式傳送。系統會根據政策處理原始郵件。
     您可以在**「內容」>「資源」>「通知」**頁面上，將通知新增到清單或編輯現有通知。
     請參閱第 321 頁的「關於政策違規通知」。
   - 選擇註釋動作，然後選擇要附加到電子郵件訊息後面的註釋。
     您可以在**「內容」>「資源」>「註釋」**頁面上新增或編輯註釋。
     請參閱第 341 頁的「建立和管理政策違規的註釋」。
   - 選擇解除動作。
     您可以在**「惡意軟體」>「設定」>「電子郵件掃描設定」>「解除」**標籤上檢視和變更解除設定。相同的解除設定適用於惡意軟體掃描和威脅防禦掃描。
     請參閱第 179 頁的「關於「解除」」。

5 請勿在「**套用至下列政策群組**」面板中變更任何內容。

賽門鐵克建議您在建立完所有新政策之後，從「**管理**」>「**使用者**」>「**政策群組**」頁面指派威脅防禦政策。此做法可確保您將一致的政策集套用到政策群組。

請參閱第 400 頁的「選取用於政策群組的威脅防禦政策」。

6 按下「**儲存**」。

7 重複步驟 2 至 6 以在政策集中建立下一個政策。繼續建立政策，直至政策集完成。

選取用於政策群組的威脅防禦政策

威脅防禦政策可指定如何處理傳送至 Symantec Content Analysis 進行掃描的電子郵件。Symantec Messaging Gateway 包括支援「內嵌」、「監控」和「安全預覽」模式的範例政策集，以確保 Symantec Messaging Gateway 針對每個條件和判斷正確處理郵件。您必須將威脅防禦政策集指派給政策群組，來為群組啟用威脅防禦掃描。

警告：請勿混合不同政策集中的政策，否則您可能會取得非預期的結果。例如，如果您將範例「安全預覽 - 提早釋放」政策與預設「內嵌 - 非惡意」政策混合，收件者會收到不含附件的安全預覽郵件。當 Content Analysis 傳回的判斷為非惡意時，「內嵌 - 非惡意」政策會通知 SMG 刪除郵件。最終導致收件者從不會收到含附件的原始郵件。

選取用於政策群組的威脅防禦政策

1 在控制中心內，按下「**管理**」>「**使用者**」>「**政策群組**」。

2 在「**政策群組**」頁面上，按下您要為其選取威脅防禦政策的政策群組。

3 在「**編輯政策群組**」頁面上，按下「**威脅防禦**」標籤。

4 如果您希望 Content Analysis 掃描入埠郵件，請按下「**為此政策群組啟用入埠 Content Analysis**」，然後為群組選取政策。您可以按下「**檢視**」來查看所選政策的特性。

- 「**入埠進階威脅政策**」定義 SMG 應如何處理包含進階惡意軟體的郵件。
- 「**入埠無法掃描政策**」定義 SMG 應如何處理 Content Analysis 無法掃描的郵件。(例如，可能存在加密附件。)
- 「**入埠非惡意政策**」定義 SMG 應如何處理未包含進階威脅的郵件。
- 「**入埠提早釋放政策**」定義 SMG 在 Content Analysis 傳回判斷前傳送郵件時應執行什麼動作。

5 如果您希望 Content Analysis 掃描離埠郵件，請按下**「為此政策群組啟用離埠 Content Analysis」**，然後為群組選取政策。

依據預設，僅為離埠郵件啟用「內嵌」政策。如果您要將「監控」或「安全預覽」政策指派給群組，則必須編輯這些政策以針對離埠郵件加以啟用。

6 按下**「儲存」**。

請參閱第 395 頁的「預設和範例威脅防禦政策」。

請參閱第 398 頁的「建立新的威脅防禦政策集」。

檢視 Content Analysis 佇列

每個掃描程式的 Content Analysis 佇列均包含目前等待進行威脅防禦掃描的郵件。

檢視掃描程式的 Content Analysis 佇列

1 在控制中心內，選取**「威脅防禦」> SMTP >「CA 佇列」**。

2 在**「Content Analysis 佇列」**面上的**「主機」**功能表中，選取「掃描程式」。

3 從**「方向」**功能表中，選取您要檢視**「入埠」**還是**「離埠」**郵件。

4 (選擇性)在**「收件者」**欄位中，輸入收件者的電子郵件地址。您可以輸入多個電子郵件地址 (以分號隔開)。

5 (選擇性) 在**「寄件者」**欄位中，輸入寄件者的電子郵件地址。

6 按下**「顯示已過濾」**來檢視搜尋結果。您可以按下**「日期」**標題，依各個郵件首次進入佇列的日期排序結果。

若要啟動新搜尋，請按下**「清除過濾器」**。

18

利用 Symantec Network Prevent

本章包含以下主題：

- 關於將 Symantec Data Loss Prevention 與 Symantec Messaging Gateway 整合
- 將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合
- 關於 Data Loss Prevention Network Prevent
- Data Loss Prevention Network Prevent 整合所需的通訊埠
- Symantec Messaging Gateway 與 Data Loss Prevention Network Prevent 如何互動
- 常用的 Data Loss Prevention Network Prevent 動作
- 支援的 Data Loss Prevention Network Prevent 傳送模式
- 關於 Data Loss Prevention Network Prevent 的故障行為
- 如何解決備份至 Symantec Network Prevent 的傳送佇列
- 啟用或停用 Data Loss Prevention Network Prevent 的略過
- 如何在啟用 Symantec Network Prevent 略過時，建立政策來偵測未經掃描的電子郵件
- 關於 Data Loss Prevention Network Prevent 報告
- 關於 Data Loss Prevention Network Prevent 整合會對效能造成的影響
- 關於 Data Loss Prevention Network Prevent 喜好設定順序
- 疑難排解 Data Loss Prevention Network Prevent 整合：郵件退回
- Data Loss Prevention Network Prevent 整合疑難排解：延遲的郵件

- 如何架構 Symantec Network Prevent 將電子郵件傳回給 Symantec Messaging Gateway
- 架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線
- 根據 Symantec Network Prevent 標頭標記建立事件
- 關於讓 Data Loss Prevention Network Prevent 伺服器離線以進行維護

關於將 Symantec Data Loss Prevention 與 Symantec Messaging Gateway 整合

Symantec Messaging Gateway 與下列 Symantec Data Loss Prevention 元件進行整合：

Data Loss Prevention Network Prevent for Email	離埠流量可以從 Symantec Messaging Gateway 透過 Data Loss Prevention Network Prevent 伺服器進行繞送。Network Prevent 會根據您架構的政策修改、繞送或攔截郵件。違反內容過濾政策的郵件將會被保留於 Symantec Messaging Gateway 事件資料夾中，以供補救和檢閱。 請參閱第 406 頁的「關於 Data Loss Prevention Network Prevent」。 請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。
Enforce Server	Enforce Server 提供了集中化的網頁式管理主控台和事件儲存庫。 這樣的整合可讓您從 Symantec Messaging Gateway 控管中心或 Enforce Server 管理主控台來補救隔離的郵件。如果是從 Enforce Server 進行補救，它會將狀態寫入到 Symantec Messaging Gateway，以便使事件狀態保持同步。您也可以將 Symantec Messaging Gateway 的狀態更新同步到 Enforce Server。 請參閱第 403 頁的「將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合」。 請參閱第 388 頁的「架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料」。 如需其他資訊，請參閱 Data Loss Prevention Server FlexResponse 外掛程式隨附的「*Symantec Data Loss Prevention SMG Release from Quarantine FlexResponse Plug-In 操作指南*」。

將 Symantec Data Loss Prevention Enforce Server 和 Symantec Messaging Gateway 整合

將 Symantec Messaging Gateway 和 Symantec Data Loss Prevention Enforce Server 整合之前，請確定兩項產品皆已授權。

請參閱第 403 頁的「關於將 Symantec Data Loss Prevention 與 Symantec Messaging Gateway 整合」。

表 18-1 說明將 Symantec Messaging Gateway 和 Symantec Data Loss Prevention Enforce Server 整合的必要步驟。同時也說明了您必須在其中執行組態的產品或產品元件。

表 18-1 將 Symantec Messaging Gateway 和 Enforce Server 整合的步驟

步驟	工作	產品或元件	說明
步驟 1	確定已正確架構 Data Loss Prevention Network Prevent 以供郵件繞送。	Symantec Messaging Gateway	將離埠電子郵件繞送到 Data Loss Prevention Network Prevent 並架構 Data Loss Prevention Network Prevent 以將電子郵件繞送回 Symantec Messaging Gateway。如果您有多個離埠掃描程式，則可以針對每個掃描程式將離埠郵件繞送到不同的 Data Loss Prevention Network Prevent 伺服器。或者，您也可以將相同的設定套用到所有離埠掃描程式。 請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。
步驟 2	安裝和架構 Email Quarantine Connect Plug-in，然後架構外掛程式的內容。	Enforce Server	請參閱「*Symantec Data Loss Prevention SMG Release from Email Quarantine Connect Plug-In 操作指南*」中說明外掛程式安裝方式的部分。
步驟 3	匯出控管中心 HTTPS 憑證。	Symantec Messaging Gateway	匯出用於控管中心 HTTPS 介面的憑證。此憑證可讓 Enforce Server 驗證到 Symantec Messaging Gateway。 請參閱第 158 頁的「匯出 TLS 與 HTTPS 憑證」。 請參閱第 151 頁的「要求憑證授權中心簽署的憑證」。 請參閱第 160 頁的「指派使用者介面 HTTPS 憑證給控管中心」。

步驟	工作	產品或元件	說明
步驟 4	匯入 Symantec Messaging Gateway 憑證。	Enforce Server	將 Symantec Messaging Gateway 憑證匯入到 Enforce Server 信任儲存區。 請參閱「*Symantec Data Loss Prevention 安裝指南 (Windows)*」或「*Symantec Data Loss Prevention 安裝指南 (Linux)*」中關於匯入憑證的部分。
步驟 5	建立用戶端憑證。	Enforce Server	從 Enforce Server 指令行的 Symantec Messaging Gateway 以伺服器憑證建立用戶端憑證和信任儲存區。 請參閱「*Symantec Data Loss Prevention SMG Release from Quarantine FlexResponse Plug-In 操作指南*」中說明外掛程式安裝方式的部分。
步驟 6	建立使用者和角色。	Enforce Server	請參閱「*Symantec Data Loss Prevention 安裝指南 (Windows)*」或「*Symantec Data Loss Prevention 安裝指南 (Linux)*」中關於建立憑證的部分。
步驟 7	匯入 Enforce Server 憑證。	Symantec Messaging Gateway	將 Enforce Server 憑證匯入到 Symantec Messaging Gateway 控管中心內。 請參閱第 154 頁的「匯入應用程式憑證」。
步驟 8	架構 Enforce Server 連線詳細資訊。	Symantec Messaging Gateway	指定 Enforce Sever 憑證並架構同步設定。 確定您用來存取 Enforce Server 的帳戶具有補救事件的適當角色。 請參閱「*Symantec Data Loss Prevention 管理指南 (Windows)*」或「*Symantec Data Loss Prevention 管理指南 (Linux)*」中關於管理角色和使用者的部分。 請參閱第 388 頁的「架構 Symantec Messaging Gateway 以使用 Enforce Server 更新資料」。

步驟	工作	產品或元件	說明
步驟 9	架構政策及其偵測規則。	Enforce Server	架構回應政策以及將標頭插入違反政策之郵件的規則。 請參閱「*Symantec Data Loss Prevention 管理指南 (Windows)*」或「*Symantec Data Loss Prevention 管理指南 (Linux)*」中關於執行政策偵測和政策回應的部分。
步驟 10	建立事件資料夾，擷取違反內容過濾政策的郵件並加以保留，以供補救或檢閱。	Symantec Messaging Gateway	選取資料夾類型**「保留供檢閱 (內容隔離)」**，將事件保留以供補救。或者您也可以選擇**「資訊事件」**，將事件保留以供檢閱。 請參閱第 361 頁的「建立內容事件資料夾」。
步驟 11	建立內容過濾政策以偵測 Data Loss Prevention 回應規則所新增的標頭。	Symantec Messaging Gateway	建立 Data Loss Prevention (Network Prevent for Enforce) 插入電子郵件訊息中之標頭的掃描政策。 Symantec Messaging Gateway 會過濾郵件中是否含有這些標頭。根據您所指定的政策動作，系統會在隔離事件資料夾或資訊事件資料夾中建立事件。 指定政策動作**「建立隔離事件」**，將這些事件保留以供補救。或您也可以指定政策動作為**「建立資訊事件」**，將這些事件保留以供檢閱。 請參閱第 278 頁的「建立內容過濾政策」。

關於 Data Loss Prevention Network Prevent

Symantec Messaging Gateway 整合 Data Loss Prevention Network Prevent 後，可傳送、繞送、保留或攔截電子郵件流量。Data Loss Prevention Network Prevent 是 Symantec Data Loss Prevention 的元件，Symantec Data Loss Prevention 可以搜尋、監控及保護機密資料 (無論是儲存還是使用的機密資料)。Data Loss Prevention Network Prevent 必須安裝在獨立伺服器上。您必須為離埠郵件過濾至少架構一個掃描程式，才能將電子郵件繞送到 Data Loss Prevention Network Prevent。

附註：您無法透過 Data Loss Prevention Network Prevent 繞送入埠郵件。

您可以架構 Data Loss Prevention Network Prevent 政策，根據偵測到的資料類型對郵件執行下列動作：

攔截	攔截郵件並傳回自訂的退回郵件給寄件者。
重新導向	將郵件繞送至其他收件者。
標籤	修改郵件的主旨行或在郵件中加入新標頭。

請參閱第 409 頁的「常用的 Data Loss Prevention Network Prevent 動作」。

根據 Data Loss Prevention Network Prevent 對郵件所做的修改而定，您也可以在 Symantec Messaging Gateway 架構政策以執行動作，例如：

封存	傳送郵件到特定電子郵件地址以進行封存。
建立事件	將郵件繞送到內容過濾資料夾進行檢閱，然後再傳送。您可以選擇架構繞送到內容過濾資料夾之郵件的通知。
加密	政府法規或您組織的政策可能要求您必須加密敏感郵件。

請參閱第 408 頁的「Symantec Messaging Gateway 與 Data Loss Prevention Network Prevent 如何互動」。

Data Loss Prevention Network Prevent 整合所需的通訊埠

表 18-2 說明將電子郵件繞送至一或多部 Data Loss Prevention Network Prevent 伺服器時使用的預設通訊埠。

表 18-2 用於 Data Loss Prevention Network Prevent 整合的通訊埠

通訊埠	通訊協定	來源	目的地	說明	注意事項
25	SMTP	內部郵件伺服器	掃描程式	離埠電子郵件	—
10025	SMTP	掃描程式	Data Loss Prevention Network Prevent	將由 Data Loss Prevention Network Prevent 處理的離埠電子郵件	—

通訊埠	通訊協定	來源	目的地	說明	注意事項
25	SMTP	Data Loss Prevention Network Prevent	掃描程式	由 Data Loss Prevention Network Prevent 處理的離埠電子郵件	依據預設，Data Loss Prevention Network Prevent 會將電子郵件退回到通訊埠 10026。您可能必須變更 Data Loss Prevention Network Prevent 上的**「遠端 SMTP 接聽程式通訊埠」**設定，以符合 Symantec Messaging Gateway 所預期的通訊埠，如通訊埠 25。

請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。

Symantec Messaging Gateway 與 Data Loss Prevention Network Prevent 如何互動

如果您架構 Symantec Messaging Gateway 將電子郵件繞送到 Data Loss Prevention Network Prevent，電子郵件通常會以下列順序繞送：

- Symantec Messaging Gateway 會在閘道上的通訊埠 25 (預設通訊埠) 接受離埠郵件。
- Symantec Messaging Gateway 會使用通訊埠 10025 (預設通訊埠) 將離埠郵件傳遞給 Data Loss Prevention Network Prevent。
- Data Loss Prevention Network Prevent 會掃描郵件，並視情況攔截郵件、重新導向郵件，或為郵件加上標籤以便由 MTA 採取進一步的動作。
- 請參閱第 409 頁的「常用的 Data Loss Prevention Network Prevent 動作」。
- Data Loss Prevention Network Prevent 會使用通訊埠 25 (預設值) 將郵件傳回給 Symantec Messaging Gateway (如果 Data Loss Prevention Network Prevent 沒有拒絕該郵件)。如果 Symantec Network Prevent 拒絕該郵件，Symantec Messaging Gateway 會將郵件傳回給寄件者並附上 SMTP 5xx 失敗回應代碼。郵件會包括您所指定的文字。
- Symantec Messaging Gateway 會依架構的組態處理郵件。Symantec Messaging Gateway 可以根據 Data Loss Prevention Network Prevent 在郵件修改的主旨行或新增的標頭標記來處理郵件。重新導向的郵件會傳送給其他收件者，而非原始收件者。

以上所列的通訊埠號是建議的通訊埠號。在您的網站中，實際的通訊埠號可能會不一樣。

請參閱第 407 頁的「Data Loss Prevention Network Prevent 整合所需的通訊埠」。

如果您有多個離埠掃描程式，則可以在**「Symantec Data Loss Prevention 設定」**頁面中，針對每個掃描程式，分別將離埠郵件繞送到 Data Loss Prevention Network Prevent 伺服器，或將設定套用至所有離埠掃描程式。

每個掃描程式都會根據以下喜好設定順序，將電子郵件繞送到針對該掃描程式所架構的所有 Data Loss Prevention Network Prevent 伺服器：

反映模式	如果 Data Loss Prevention Network Prevent 架構成反映模式，那麼每部 Data Loss Prevention Network Prevent 伺服器都會將每個郵件傳回到送出郵件的掃描程式。
轉寄模式	如果是在轉寄模式下架構 Data Loss Prevention Network Prevent，Data Loss Prevention Network Prevent 伺服器會將郵件傳遞至下一個目的地。 v19465700

請參閱第 415 頁的「關於 Data Loss Prevention Network Prevent 喜好設定順序」。

請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。

Symantec Messaging Gateway 透過 SMTP 用戶端 IP 位址型繞送與 Data Loss Prevention Network Prevent 整合。

常用的 Data Loss Prevention Network Prevent 動作

Symantec Messaging Gateway 和 Data Loss Prevention Network Prevent 透過交換 SMTP 郵件彼此合作。Data Loss Prevention Network Prevent 透過回應規則和政策來修改、重新繞送及拒絕郵件。您架構 Data Loss Prevention Network Prevent 針對電子郵件採取的某些動作不需要 Symantec Messaging Gateway 採取進一步的動作。其他動作則要求您必須架構 Symantec Messaging Gateway。

表 18-3 常用的 Data Loss Prevention Network Prevent 動作

動作	說明
攔截	將郵件退回給寄件者
重新導向	將郵件傳送給其他收件者 您可以架構 Data Loss Prevention Network Prevent 將郵件重新導向給新的收件者，例如管理員的電子郵件地址。
加上標籤 - 標頭標記	新增自訂電子郵件標頭至郵件 您可以新增標頭至電子郵件訊息，例如 X-Sensitive-Data: SSN。您可以架構 Symantec Messaging Gateway，讓它搜尋自訂標頭並針對找到的郵件採取指定的動作。Symantec Messaging Gateway 可以刪除郵件、封存郵件、為郵件建立事件，或保留郵件以供檢閱。 您也可以建立報告，瞭解 Symantec Messaging Gateway 在符合的郵件上採取了哪些動作。 請參閱第 419 頁的「根據 Symantec Network Prevent 標頭標記建立事件」。
加上標籤 - 主旨修改	變更主旨行 就像標頭標記，您可以架構 Symantec Messaging Gateway，讓它搜尋主旨行中的特定文字，並針對符合的郵件採取指定的動作。

支援的 Data Loss Prevention Network Prevent 傳送模式

您可以將 Data Loss Prevention Network Prevent 整合至您的網路架構。Data Loss Prevention Network Prevent 不會在磁碟上製作它自己的郵件副本。郵件只會保留在記憶體中。而在離埠郵件交易成功之前，都不會認可內送郵件交易。

您可以透過下列方法，將 Data Loss Prevention Network Prevent 整合至您的網路架構中：

反映	處理郵件之後，Data Loss Prevention Network Prevent 會將郵件傳回給它的來源掃描程式。
轉寄	處理郵件之後，Data Loss Prevention Network Prevent 會將郵件傳遞給您指定的 MTA。

選擇的方法取決於您網站的特定需求。

關於 Data Loss Prevention Network Prevent 的故障行為

如果無法連線到 Data Loss Prevention Network Prevent，電子郵件可能不會經由 Data Loss Prevention Network Prevent 處理，或是會在郵件佇列中等候。所採取的行為取決於有多少 Data Loss Prevention Network Prevent 伺服器無法連線，以及是否已啟用略過功能。預設會啟用略過功能。

請參閱第 412 頁的「啟用或停用 Data Loss Prevention Network Prevent 的略過」。

無法連線到 Data Loss Prevention Network Prevent 伺服器的原因包括：

- 網路故障
- 執行 Data Loss Prevention Network Prevent 的硬體故障
- 網路頻寬、硬體速度或 Data Loss Prevention Network Prevent 伺服器數目不符合郵件流的需求

表 18-4 Data Loss Prevention Network Prevent 的故障行為

略過狀態	Data Loss Prevention Network Prevent 伺服器狀態	系統行為
已停用或已啟用略過功能	兩部以上的伺服器中有一部無法連線	系統會略過無法連線的 Data Loss Prevention Network Prevent 伺服器。電子郵件會依據喜好設定清單或 MX 記錄 (或兩者)，繞送到下一部 Data Loss Prevention Network Prevent 伺服器。

略過狀態	Data Loss Prevention Network Prevent 伺服器狀態	系統行為
已停用略過功能	全部都無法連線	電子郵件會儲存在 Symantec Messaging Gateway 的傳送佇列中。不會傳送任何離埠電子郵件。如果仍然無法連線到 Data Loss Prevention Network Prevent 伺服器，傳送佇列會隨著時間的經過越變越大。 如果符合下列條件，郵件可能會塞在 Symantec Messaging Gateway 中： ■ 達到「傳送佇列中的郵件數目上限」限制。 ■ 已啟用選項**「傳送佇列被佔滿時延遲新連線」**。 當傳送佇列被佔滿時，系統會延遲新的入埠連線和離埠連線。 請參閱第 411 頁的「如何解決備份至 Symantec Network Prevent 的傳送佇列」。 請參閱第 48 頁的「架構 SMTP 進階設定」。
已啟用略過功能(預設)	全部都無法連線	電子郵件不會被繞送到 Data Loss Prevention Network Prevent 伺服器，但 Symantec Messaging Gateway 確實會處理郵件。除非適當地架構 Symantec Messaging Gateway，否則敏感性資料可能會未經掃描即從您的網站送出。 請參閱第 413 頁的「如何在啟用 Symantec Network Prevent 略過時，建立政策來偵測未經掃描的電子郵件」。

如何解決備份至 Symantec Network Prevent 的傳送佇列

如果停用 Symantec Network Prevent 伺服器的略過，而且伺服器無法連線，則郵件會備份在傳送佇列中。一般而言，如果 Symantec Network Prevent 伺服器再次變成可以重新連線，則伺服器處理郵件時會自動清空傳送佇列。

而傳送佇列可能會因下列任一原因而無法自動清空：

- Symantec Messaging Gateway 的可用硬碟空間容量太低。
- Symantec Messaging Gateway 的可用記憶體容量太低。
- 符合 Symantec Messaging Gateway 的下列條件：
  - 達到「傳送佇列中的郵件數目上限」限制。
  - 已啟用**「傳送佇列被佔滿時延遲新連線」**選項。

請參閱第 410 頁的「關於 Data Loss Prevention Network Prevent 的故障行為」。

如果 Symantec Network Prevent 伺服器持續無法使用，則佇列可能會增長到最大大小，而且耗用大量磁碟空間。磁碟空間減少可能會影響 Symantec Messaging Gateway 傳送郵件的能力。

表 18-5　　解決傳送佇列備份的程序

步驟	工作
1	更正 Symantec Network Prevent 伺服器的問題。確認 Symantec Network Prevent 伺服器執行中、容量足以處理指定的電子郵件數，而且網路路徑可以連線。
2	如果 Symantec Messaging Gateway 掃描程式上的磁碟空間不足，請釋放磁碟空間。釋放磁碟空間的方法範例包括刪除報告資料或日誌。 請參閱第 647 頁的delete。
3	暫時或永久啟用略過。除非適當地架構 Symantec Messaging Gateway，否則敏感性資料可能會未經掃描即從您的網站送出。 請參閱第 413 頁的「如何在啟用 Symantec Network Prevent 略過時，建立政策來偵測未經掃描的電子郵件」。 請參閱第 412 頁的「啟用或停用 Data Loss Prevention Network Prevent 的略過」。
4	暫時將內送郵件流轉向至不同的掃描程式。
5	在控管中心內，存取**「管理」>「主機」>「組態」**。選取掃描程式，並存取 **SMTP** 標籤，然後選取**「進階設定」**。 暫時變更下列設定： ■ **「傳送佇列中的郵件數目上限」**：增加。 ■ **「傳送佇列被佔滿時延遲新連線」**：取消勾選。 請參閱第 48 頁的「架構 SMTP 進階設定」。
6	(選擇性) 在控管中心內，按下**「狀態」> SMTP >「郵件佇列」**，然後重新傳送所有佇列。 MTA 會自動重新傳送佇列，但是此手動動作可加速佇列處理。

啟用或停用 Data Loss Prevention Network Prevent 的略過

離埠電子郵件預設會在無法使用所有 Data Loss Prevention Network Prevent 伺服器時，略過 Data Loss Prevention Network Prevent。只有在無法與 Data Loss Prevention Network Prevent 伺服器建立連線時，才會觸發略過。

下列情況不會觸發略過：

■ 已建立與 Data Loss Prevention Network Prevent 伺服器的連線，但連線已被延遲。

- 電子郵件造成 SMTP 4xx 暫時性錯誤。Symantec Messaging Gateway MTA 稍後會嘗試重新傳送郵件。
- 電子郵件造成 SMTP 5xx 永久性錯誤。Symantec Messaging Gateway MTA 會將退回郵件傳送給寄件者。
- Data Loss Prevention Network Prevent 伺服器處理 SMTP 連線的速度緩慢。不過，如果 SMTP 連線逾時，且其他 Data Loss Prevention Network Prevent 伺服器都無法使用，則會觸發略過。

如果 Data Loss Prevention Network Prevent 伺服器無法使用，敏感性資料可能會未經掃描即從您的站台送出。如果停用略過，而且 Data Loss Prevention Network Prevent 無法連線，所有離埠電子郵件都會在傳送佇列中等候，這樣會造成無法即時傳送郵件。

請參閱第 410 頁的「關於 Data Loss Prevention Network Prevent 的故障行為」。

請參閱第 413 頁的「如何在啟用 Symantec Network Prevent 略過時，建立政策來偵測未經掃描的電子郵件」。

啟用或停用 Data Loss Prevention Network Prevent 的略過

1. 在控管中心內，按下**「內容」>「設定」>「DLP 連線」**。
2. 若要選擇您要架構的離埠掃描程式，請勾選**「為離埠掃描程式主機啟用 DLP」**，然後從下拉式功能表中選擇掃描程式。
3. 若要啟用略過，請勾選**「當所有 DLP 伺服器都無法連線時啟用略過」**。

   若要停用略過，請取消勾選**「當所有 DLP 伺服器都無法連線時啟用略過」**。
4. 若要將設定套用至所有離埠掃描程式，請勾選**「套用至所有離埠掃描程式主機」**。
5. 按下**「儲存」**。

如何在啟用 Symantec Network Prevent 略過時，建立政策來偵測未經掃描的電子郵件

如果 Symantec Network Prevent 無法使用，離埠電子郵件預設會略過 Symantec Network Prevent。如果 Symantec Network Prevent 伺服器無法使用，敏感性資料可能會未經掃描即從您的網站送出。不過，您可以在 Symantec Brightmail Gateway 上架構政策，防止無法掃描的郵件離開您的網站。

您可以針對未經掃描的郵件建立內容過濾政策，以防止未經掃描的郵件離開您的網站。在此政策組態中，內容過濾資料夾的管理員會在偵測到未經掃描的郵件時收到通知。未經掃描的郵件會保留在內容事件資料夾中，以供檢閱。

表 18-6 說明您可以遵循以防止略過的電子郵件離開您網站的程序。

表 18-6 建立內容過濾政策以防止略過的電子郵件離開您網站的程序

步驟	工作
1	確定 Symantec Network Prevent 伺服器將標頭新增至它所處理的郵件。依據預設，Symantec Network Prevent 會將標頭 `X-CFilter-Loop:` 新增至自己處理的郵件。
2	在 Symantec Brightmail Gateway 中，針對未掃描的郵件建立內容過濾資料夾，並架構內容過濾資料夾的電子郵件通知。
3	在 Symantec Brightmail Gateway 中，建立具有下列特性的電子郵件內容過濾政策： ■ 政策範本：空白 ■ 套用至：離埠郵件 ■ 條件 - 在此郵件指定部分中的文字： 郵件標頭 ■ 條件 - 標頭名稱：`X-Cfilter-Loop` ■ 條件 - 郵件標頭：不存在 ■ 執行下列動作：建立事件。新增其他的核准和拒絕動作。 ■ 在內容事件資料夾中：您建立的資料夾 ■ 保留郵件以供檢閱：已勾選 請參閱第 278 頁的「建立內容過濾政策」。

或者，您可能不需要儲存無法掃描的郵件，而是想要在無法掃描郵件時收到通知。您可以在 Symantec Brightmail Gateway 上建立電子郵件內容過濾政策，以在偵測到未經掃描的郵件時傳送電子郵件通知。

請參閱第 321 頁的「關於政策違規通知」。

關於 Data Loss Prevention Network Prevent 報告

Symantec Messaging Gateway 不會特別提供 Data Loss Prevention Network Prevent 活動的報告。請使用 Data Loss Prevention Network Prevent 來報告其上的活動。某些與 Data Loss Prevention Network Prevent 相關的活動可能是 Symantec Messaging Gateway 上的報告。例如，您可以為 Data Loss Prevention Network Prevent 所標示的郵件建立事件。該事件活動會反映在某些內容過濾報告上。

關於 Data Loss Prevention Network Prevent 整合會對效能造成的影響

由於牽涉到額外的處理，整合 Data Loss Prevention Network Prevent 可能會造成離埠電子郵件傳送速度有些許延遲。

延遲量取決於下列因素：

- 您網站的離埠電子郵件數

- Data Loss Prevention Network Prevent 內容過濾政策的數目與複雜性
- 郵件內容和大小
- 相較於郵件數的 Data Loss Prevention Network Prevent 伺服器數目

您可以透過執行下列任何工作減少延遲並提高傳輸量：

- 新增其他 Data Loss Prevention Network Prevent 伺服器
- 微調離埠 SMTP 和 SMTP 傳送的**「連線數上限」**和**「來自單一 IP 位址的連線數上限」**設定。此設定為 Symantec Messaging Gateway 掃描程式設定。
  請參閱第 48 頁的「架構 SMTP 進階設定」。
- 微調 Data Loss Prevention Network Prevent 伺服器的 **NumThreads** 設定，以根據您站台的離埠電子郵件數最佳化傳輸量。

請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。

關於 Data Loss Prevention Network Prevent 喜好設定順序

如果您有多部 Data Loss Prevention Network Prevent 伺服器，則可以架構 Symantec Messaging Gateway 使用 Data Loss Prevention Network Prevent 伺服器的順序。您可以在控管中心或 MX 記錄中設定喜好設定。

表 18-7 描述了喜好設定類型以及在哪設定這些類型。

表 18-7　　可用的喜好設定類型

喜好設定類型	說明
「Symantec Data Loss Prevention 設定」頁面上的喜好設定	請在控管中心的**「內容」>「設定」>「DLP 連線」>「Symantec Data Loss Prevention 設定」**頁面上，架構此喜好設定類型。 請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。
MX 記錄喜好設定	請使用 DNS 軟體，在 Data Loss Prevention Network Prevent 的 DNS 記錄中，架構 MX 記錄喜好設定。如果您指定的主機名稱會繞送至多部 Data Loss Prevention Network Prevent 伺服器，則必須架構 MX 記錄喜好設定。有效的 MX 喜好設定範圍是 0 - 65535。一般值是 10 與 100 之間的每 10 個數字。

- 對於在網路頻寬較大且具有充沛 CPU 和硬碟資源之電腦上執行的 Data Loss Prevention Network Prevent 伺服器，請選擇較小的喜好設定數字。對於在網路頻寬較小且 CPU 和硬碟資源有限之電腦上執行的 Data Loss Prevention Network Prevent 伺服器，請選擇較大的喜好設定數字。

- 在這兩種類型的喜好設定中，會先嘗試較小的數字，再嘗試較大的數字。如果 Data Loss Prevention Network Prevent 伺服器無法連線，則會嘗試下一個喜好設定數字較大的伺服器。例如，會先嘗試喜好設定為 1 的 Data Loss Prevention Network Prevent 伺服器，再嘗試喜好設定為 2 的 Data Loss Prevention Network Prevent 伺服器。
- 在控管中心內，如果您將喜好設定值 1 指派給兩個 Data Loss Prevention Network Prevent 伺服器，Symantec Messaging Gateway 會隨機挑選其中一個伺服器。如果該伺服器變為不可用，則另一個喜好設定為 1 的伺服器將變為主要伺服器。如果該伺服器變為不可用，Symantec Messaging Gateway 將嘗試與第一個伺服器重新連線。僅當喜好設定為 1 的兩個主機都無法使用時，才會使用下一個喜好設定值較高的 Data Loss Prevention Network Prevent 伺服器。
- 您可以組合使用這兩種類型的喜好設定。檢查所選擇主機名稱之 MX 記錄的喜好設定之前，會先比較「**Symantec Data Loss Prevention 設定**」頁面上的喜好設定。

請參閱第 414 頁的「關於 Data Loss Prevention Network Prevent 整合會對效能造成的影響」。

請參閱第 406 頁的「關於 Data Loss Prevention Network Prevent」。

請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。

疑難排解 Data Loss Prevention Network Prevent 整合：郵件退回

如果您最近已啟用繞送至 Data Loss Prevention Network Prevent，而電子郵件訊息遭到退回，則請檢查下列項目：

- **接受來自 DLP 伺服器的已掃描郵件**：已在「Symantec Data Loss Prevention 設定」頁面上正確架構 IP 位址。
- 已使用指向掃描程式通訊埠的反映通訊埠設定來正確架構 Prevent 伺服器。

請參閱第 416 頁的「Data Loss Prevention Network Prevent 整合疑難排解：延遲的郵件」。

請參閱第 406 頁的「關於 Data Loss Prevention Network Prevent」。

請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。

Data Loss Prevention Network Prevent 整合疑難排解：延遲的郵件

如果傳回的離埠電子郵件含有下列錯誤：

```
421 Forwarding agent unavailable. Closing connection.
```

Data Loss Prevention Network Prevent 的「**遠端 SMTP 接聽程式通訊埠**」與 Symantec Messaging Gateway 上的入埠電子郵件通訊埠不符。

請參閱第 417 頁的「如何架構 Symantec Network Prevent 將電子郵件傳回給 Symantec Messaging Gateway」。

此訊息描述了在 Symantec 8.1 版本的 Symantec Data Loss Prevention 中看到的錯誤。未來的版本可能會產生不同的錯誤。

如何架構 Symantec Network Prevent 將電子郵件傳回給 Symantec Messaging Gateway

您必須架構 Symantec Network Prevent 伺服器，以透過預期通訊埠將電子郵件傳回給 Symantec Messaging Gateway。Symantec Messaging Gateway 的預設離埠電子郵件通訊埠為 25。Symantec Network Prevent 中的預設遠端 SMTP 接聽程式通訊埠為 10026。變更 Symantec Network Prevent 通訊埠，以符合 Symantec Messaging Gateway 離埠電子郵件通訊埠。

請參閱第 417 頁的「架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線」。

表 18-8 架構 Symantec Network Prevent 將郵件傳回給 Symantec Messaging Gateway 的程序

步驟	動作	說明
1	檢查 Symantec Messaging Gateway 上的預設離埠電子郵件通訊埠。	離埠郵件 IP 位址通訊埠會顯示在控管中心內「**主機組態**」頁面的 **SMTP** 標籤中。
2	設定 Symantec Network Prevent 的「**遠端 SMTP 接聽程式通訊埠**」。	將 Symantec Network Prevent 的「**遠端 SMTP 接聽程式通訊埠**」設為 Symantec Messaging Gateway 所使用的離埠電子郵件通訊埠。如需組態詳細資料，請參閱 Symantec Network Prevent 說明文件。

架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線

如果您擁有一部或多部 Data Loss Prevention Network Prevent 伺服器，則可以將電子郵件從 Symantec Messaging Gateway 繞送至伺服器。您也必須架構 Data Loss Prevention Network Prevent 來將電子郵件繞送回 Symantec Messaging Gateway。如果您有多個離埠掃描程式，則可以針對每個掃描程式，分別將離埠郵件繞送到 Data Loss Prevention Network Prevent 伺服器，或將相同的設定套用至所有離埠掃描程式。

請參閱第 417 頁的「如何架構 Symantec Network Prevent 將電子郵件傳回給 Symantec Messaging Gateway」。

架構與 Data Loss Prevention Network Prevent 之間的電子郵件連線

1 在控管中心內，按下「**內容**」>「**設定**」>「**DLP 連線**」。

2 按下「**為離埠掃描程式主機啟用 DLP**」，選擇您要架構的離埠掃描程式。

如果只有一個離埠掃描程式，則可以略過此步驟。如果您想將相同的設定套用至所有離埠掃描程式，請先選擇其中一個，可以稍候勾選「**套用至所有離埠掃描程式主機**」。

3 在「**繞送離埠郵件到 DLP 伺服器**」下，按下「**新增**」新增空白列。

4 在「**主機或 IP 位址**」下，指定 Data Loss Prevention Network Prevent 伺服器的網域名稱或 IP 位址。

網域名稱的格式可以是 server1.symantecexample.com，也可以是 symantecexample.com。如果針對 Data Loss Prevention Network Prevent 伺服器架構 MX 記錄，則請指定網域名稱 (非 IP 位址)。

5 在「**通訊埠**」下，指定離埠電子郵件應該繞送至的目標 Data Loss Prevention Network Prevent 伺服器上的通訊埠號。

預設通訊埠為 10025。請確定 Data Loss Prevention Network Prevent 伺服器上的「本機 SMTP 接聽程式通訊埠」已設定為相同的通訊埠號。

6 勾選「**MX 查詢**」啟用 Data Loss Prevention Network Prevent 伺服器的 MX 查詢。

如果您勾選「**MX 查詢**」，則請確定已指定格式為 server1.symantecexample.com 或 symantecexample.com 的網域名稱 (而不是 IP 位址)。

7 在「**喜好設定 (1 - 100)**」下，指定此 Data Loss Prevention Network Prevent 伺服器的喜好設定 (與所有定義的 Data Loss Prevention Network Prevent 伺服器相較之下)。

請參閱第 415 頁的「關於 Data Loss Prevention Network Prevent 喜好設定順序」。

「**當所有 DLP 伺服器都無法連線時啟用略過**」會在另一節予以描述。

請參閱第 412 頁的「啟用或停用 Data Loss Prevention Network Prevent 的略過」。

8 在「**TLS 加密**」下方，勾選「**選用的傳送加密**」，以嘗試或需要使用 TLS 加密來傳送郵件至 Data Loss Prevention Network Prevent。如果您啟用傳送加密，必須選擇三個憑證選項之一：

- **嘗試 TLS 加密**：嘗試，但不需要使用 TLS 加密。需要在 Symantec Messaging Gateway 和 Data Loss Prevention Network Prevent 伺服器上使用自行簽署或憑證授權中心簽署的憑證。
- **需要 TLS 加密但不驗證憑證**：需要在 Symantec Messaging Gateway 和 Data Loss Prevention Network Prevent 伺服器上使用自行簽署或憑證授權中心簽署的憑證。
- **需要 TLS 加密且驗證憑證**：需要同時在 Symantec Messaging Gateway 和 Data Loss Prevention Network Prevent 伺服器上安裝憑證授權中心簽署的有效憑證。

為加強安全性，您可以在「**通訊協定**」> **SMTP** >「**設定**」> **SMTP** 標籤上停用對提早加密通訊協定的支援。「**SSL 限制**」設定會影響 SMG 可用來加密其與 Data Loss Prevention Network Prevent 交換之通訊的通訊協定。

請參閱第 83 頁的「指定 TLS 通訊的 SSL 限制」。

如果 Symantec Messaging Gateway 隨附的非預設憑證授權中心需要簽署用於 TLS 加密的憑證，您可以在「**管理**」>「**設定**」>「**憑證設定**」頁面上匯入此憑證。

9 在「**接受來自 DLP 伺服器的已掃描郵件**」下，按下「**新增**」新增空白列。

10 指定 Symantec Messaging Gateway 應該預期接受來自 Data Loss Prevention Network Prevent 之電子郵件的 IP 位址。

可以新增額外列，來指定 Symantec Messaging Gateway 應該預期接受電子郵件之所有來源 Data Loss Prevention Network Prevent 伺服器的 IP 位址。例如，您可能只在「**繞送離埠郵件到 DLP 伺服器**」下指定一個主機名稱。但是，如果該主機名稱解析為多個 Data Loss Prevention Network Prevent 伺服器，則請新增所有那些伺服器的 IP 位址。

11 如果您想要將設定套用至所有離埠掃描程式，請勾選「**套用至所有離埠掃描程式主機**」。

12 按下「**儲存**」。

根據 Symantec Network Prevent 標頭標記建立事件

以下是處理 Symantec Network Prevent 偵測到之任何敏感性資料的範例方法。 此方法需要同時架構 Symantec Network Prevent 和 Symantec Brightmail Gateway。

在此範例中，Symantec Network Prevent 會將自訂標頭新增至相符郵件中。 Symantec Brightmail Gateway 會為具有自訂標頭的郵件建立事件，並保留郵件以供檢閱。 因此，郵件不會傳送給原始收件者，而是改為繞送至 Symantec Brightmail Gateway 上的內容過濾資料夾。 而管理員可以核准、拒絕、轉寄、封存、刪除和管理內容過濾資料夾中的郵件。

表 18-9 說明根據 Symantec Network Prevent 標頭標記建立事件的程序。

表 18-9 如何根據 Symantec Network Prevent 標頭標記建立事件

步驟	工作
1	在「**新增/編輯回應規則**」畫面的「**建立修改 SMTP 郵件回應**」規則下，架構 Symantec Network Prevent 在偵測到含有敏感性資料的郵件時，將自訂標頭新增至郵件。 您最多可以新增三個 RFC 2822 標頭行。 賽門鐵克建議使用含有不同值的標頭 `X-Cfilter:`，這取決於想要對 Symantec Brightmail Gateway 或掃描判斷採取的動作。 例如，您可以指定 `X-Cfilter: Symantec Incident` 標記內容資安事端資料夾的郵件，或指定 `X-Cfilter: SSN` 表示任何含有社會安全號碼的郵件。

步驟	工作
2	在 Symantec Brightmail Gateway 中，建立內容過濾資料夾 (如 Symantec Incidents)。 您也許想要啟用內容過濾資料夾的電子郵件通知。 請參閱第 359 頁的「關於內容事件資料夾」。
3	在 Symantec Brightmail Gateway 中，建立具有下列特性的電子郵件內容過濾政策： ■ 政策範本：空白 ■ 套用至：離埠郵件 ■ 條件 - 在此郵件指定部分中的文字： 郵件標頭 ■ 條件 - 標頭名稱：架構的標頭，例如 `X-Cfilter: Symantec Incident` ■ 條件 - 郵件標頭：存在 ■ 執行下列動作：建立事件。新增其他的核准和拒絕動作。 ■ 在內容事件資料夾中：您建立的資料夾 ■ 保留郵件以供檢閱：已勾選

關於讓 Data Loss Prevention Network Prevent 伺服器離線以進行維護

有時候，您可能需要讓一或多部 Data Loss Prevention Network Prevent 伺服器離線以執行維護，如安裝新軟體版本。

表 18-10 說明可用的選項對郵件流造成的影響。

表 18-10 讓 Data Loss Prevention Network Prevent 伺服器離線的選項

選項	說明
如果您有多部 Data Loss Prevention Network Prevent 伺服器，請一次針對一部伺服器執行維護	如果符合下列任一情況，您可以一次在一部伺服器上執行維護： ■ 您已在 Symantec Messaging Gateway 架構多部 Data Loss Prevention Network Prevent 伺服器 ■ 您在 Symantec Messaging Gateway 為 Data Loss Prevention Network Prevent 指定的位址使用 MX 記錄解析為多部 Data Loss Prevention Network Prevent 伺服器 會忽略無法連線的 Data Loss Prevention Network Prevent 伺服器，並使用喜好設定清單中下一部可用的 Data Loss Prevention Network Prevent 伺服器。

選項	說明
停用繞送到 Data Loss Prevention Network Prevent	離埠電子郵件會略過 Data Loss Prevention Network Prevent 伺服器。 當 Data Loss Prevention Network Prevent 伺服器可以再度使用時，您必須手動重新啟用繞送到這些伺服器。敏感性資料可能未經 Data Loss Prevention Network Prevent 伺服器掃描即從您的站台送出。 請參閱第 413 頁的「如何在啟用 Symantec Network Prevent 略過時，建立政策來偵測未經掃描的電子郵件」。 請參閱第 412 頁的「啟用或停用 Data Loss Prevention Network Prevent 的略過」。
啟用略過	如果沒有可用的 Data Loss Prevention Network Prevent 伺服器，則離埠電子郵件會直接送出而不會經過這些伺服器掃描。敏感性資料可能未經 Data Loss Prevention Network Prevent 伺服器掃描即從您的站台送出。當 Data Loss Prevention Network Prevent 伺服器可以再度使用時，Symantec Messaging Gateway 會自動將離埠電子郵件繞送到這些伺服器。 預設會啟用略過。 如果停用略過，離埠電子郵件就會保留在傳送佇列中。當您稍後啟動 Data Loss Prevention Network Prevent 伺服器之後，伺服器就會掃描延遲的電子郵件中是否包含敏感性資料。但是，如果未及時重新建立連線，離埠電子郵件可能會被退回寄件者。退回郵件之前，預設會先將郵件保留在佇列中最多三天。 如果啟用略過，當執行下列工作時，您可以在 Data Loss Prevention Network Prevent 伺服器上執行維護： ■ 在 Symantec Messaging Gateway 的控管中心啟用略過。 ■ 在 Data Loss Prevention Network Prevent 伺服器執行維護。 ■ 在伺服器上執行完維護工作之後，讓 Data Loss Prevention Network Prevent 伺服器重新上線。 ■ 在 Symantec Messaging Gateway 的控管中心停用略過。 確定您組織的政策允許您暫時啟用略過。 請參閱第 412 頁的「啟用或停用 Data Loss Prevention Network Prevent 的略過」。
停止離埠郵件佇列	停止佇列時不會傳送任何離埠郵件。Data Loss Prevention Network Prevent 伺服器和 Symantec Messaging Gateway 終究會掃描所有離埠郵件。當 Data Loss Prevention Network Prevent 伺服器可以再度使用時，您必須手動重新啟用離埠郵件佇列。 請參閱第 65 頁的「MTA 與郵件佇列行為」。

選項	說明
啟用繞送到 Data Loss Prevention Network Prevent 但停用略過	離埠郵件會備份在傳送佇列中。 請參閱第 412 頁的「啟用或停用 Data Loss Prevention Network Prevent 的略過」。

19

架構目錄資料整合

本章包含以下主題：

- 關於使用目錄資料服務
- 架構目錄資料整合
- 建立資料來源
- 新增資料來源
- 啟用新資料來源的功能
- 關於資料來源查詢

關於使用目錄資料服務

使用目錄資料服務可以將儲存在輕量型目錄存取通訊協定 (LDAP) 目錄中的資訊，用於 Symantec Messaging Gateway 中的功能。

對於資料來源，Symantec Messaging Gateway 提供您可以啟用的四種功能：驗證、位址解析、繞送或收件者驗證。對於每一個資料來源，您可以啟用其中一個功能，或這些功能的組合。

請參閱第 429 頁的「關於資料來源和功能」。

若要將目錄資料用於這些功能，您可以架構所需功能的資料來源，也可以在 Symantec Messaging Gateway 中架構其他功能。

請參閱第 426 頁的「建立資料來源」。

您可以使用下列功能來支援 Symantec Messaging Gateway 中的功能組態。

表 19-1 說明 Symantec Messaging Gateway 中依賴目錄資料服務組態的功能。

表 19-1 Symantec Messaging Gateway 中使用所架構的資料來源的功能

功能	要啟用的資料來源功能	額外的設定工作
拒絕或棄置無效收件者。	收件者驗證	架構無效收件者的處理並且啟用至少一個網域的收件者驗證。 請參閱第 86 頁的「設定無效的收件者處理」。 請參閱第 71 頁的「新增或編輯網域」。
使用電子郵件地址搜尋攻擊辨識。	收件者驗證	架構電子郵件地址搜尋攻擊和網域。 請參閱第 71 頁的「新增或編輯網域」。 請參閱第 128 頁的「架構電子郵件地址搜尋攻擊辨識」。
加入 Symantec Probe Network。	收件者驗證	啟用至少一個網域的收件者驗證。 請參閱第 71 頁的「新增或編輯網域」。 請參閱第 272 頁的「從無效收件者電子郵件地址建立探查帳戶」。
實作一般使用者隔離所，並允許一般使用者存取垃圾郵件隔離所郵件。	驗證	至少架構一個政策群組來隔離垃圾郵件、架構隔離所設定和架構垃圾郵件過濾。 請參閱第 168 頁的「關於選取政策群組的過濾政策」。 請參閱第 239 頁的「關於隔離垃圾郵件」。 請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。 請參閱第 239 頁的「關於隔離垃圾郵件」。
讓已驗證的一般使用者透過 SMTP 驗證通訊協定從遠端傳送電子郵件。	驗證	設定 SMTP 驗證。 請參閱第 90 頁的「關於使用 SMTP 驗證」。

功能	要啟用的資料來源功能	額外的設定工作
使用 LDAP 群組和散布清單來套用政策。	位址解析	新增 LDAP 群組或散布清單作為政策群組的成員。 請參閱第 168 頁的「關於選取政策群組的過濾政策」。
允許一般使用者架構電子郵件語言喜好設定和「允許的寄件者」和「攔截的寄件者」清單。	位址解析和驗證 使用者喜好設定功能需要啟用資料來源的兩種驗證 (以讓使用者登入和設定喜好設定) 和位址解析 (以將喜好設定複寫至掃描程式)。	至少啟用一般使用者設定的一個政策群組。 請參閱第 168 頁的「關於選取政策群組的過濾政策」。
根據目錄資訊，將使用者電子郵件重新繞送至替代地址或替代郵件主機。	繞送	架構網域。 請參閱第 71 頁的「新增或編輯網域」。

架構目錄資料整合

表 19-2 設定目錄資料服務的程序

步驟	動作	說明
步驟 1	建立新資料來源。	請參閱第 426 頁的「建立資料來源」。 請參閱第 426 頁的「新增資料來源」。
步驟 2	啟用新資料來源的功能。	請參閱第 428 頁的「啟用新資料來源的功能」。 請參閱第 430 頁的「建立收件者驗證資料來源」。 請參閱第 431 頁的「建立驗證資料來源」。 請參閱第 434 頁的「建立繞送資料來源」。 請參閱第 436 頁的「建立位址解析資料來源」。
步驟 3	自訂及測試資料來源查詢。	請參閱第 443 頁的「建立和測試自訂的收件者驗證查詢」。 請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。 請參閱第 448 頁的「建立和測試自訂繞送查詢」。 請參閱第 450 頁的「建立和測試自訂位址解析查詢」。
步驟 4	設定目錄資料快取。	請參閱第 482 頁的「關於預先載入目錄資料快取」。 請參閱第 482 頁的「預先載入資料快取」。

步驟	動作	說明
步驟 5	架構進階設定。	請參閱第 484 頁的「架構資料來源進階設定」。

建立資料來源

Symantec Messaging Gateway 提供一個精靈，可引導您完成建立新資料來源的程序。

表 19-3說明建立資料來源的程序。

表 19-3 如何建立資料來源

步驟	工作	說明
步驟 1	提供代管目錄資料的LDAP 伺服器詳細資料。	這類詳細資料包括主機設定、繫結DN、憑證及SSL狀態。 請參閱第 426 頁的「新增資料來源」。
步驟 2	(可選) 調整連線設定和快取設定。	您可以選擇使用預設值，或是編輯以快取設定和連線設定，來符合自己的需求。 請參閱第 484 頁的「架構資料來源進階設定」。
步驟 3	啟用和架構您要資料來源提供的功能。	對於一個資料來源，您可以架構一或多個功能。 請參閱第 428 頁的「啟用新資料來源的功能」。

在儲存新的資料來源之後，可以視需要加以修改。

請參閱第 460 頁的「編輯資料來源」。

新增資料來源

「新增目錄資料來源」精靈會引導您完成建立和架構新資料來源所需的工作。此程序的第一個步驟，就是架構為目錄來源提供資料的 LDAP 伺服器。

請參閱第 426 頁的「建立資料來源」。

對於驗證、位址解析或繞送資料來源，傳回的結果必須是唯一的。因此，您不會有相同或重疊的資料來源 (在兩個資料來源可能傳回相同結果的情況下)。如果在**「警示」**頁面上已架構**「目錄資料完整性錯誤」**警示，那麼在偵測到此情況時，就會觸發該警示。

請參閱第 590 頁的「架構警示」。

目錄資料服務無法與 LDAP 伺服器正常通訊時 (例如，如果 LDAP 伺服器的網路連結中斷，或發生資料完整性問題)，會影響郵件處理與使用者驗證。

請參閱第 429 頁的「關於資料來源和功能」。

新增資料來源

1 按下「**管理**」>「**設定**」>「**目錄整合**」。

2 在「**目錄整合設定**」->「**目錄資料來源**」頁面上，按下「**新增**」。

此時會出現「**LDAP 伺服器組態**」頁面。

3 在「**資料來源名稱**」欄位中，提供資料來源的唯一名稱。

4 選取 LDAP 來源所使用的「**目錄類型**」。可用選項如下：

- Active Directory
- Active Directory 通用類別目錄
- iPlanet/Sun ONE/Java Directory Server
- Domino
- 其他 (可以是任何 LDAPv3 相容的目錄)

雖然 Symantec Messaging Gateway 與任何 LDAPv3 目錄皆相容，但它的設計是專門來支援具有此處所列之四種特定目錄類型的組態。如果您選取「其他」作為目錄類型，則可能需要參閱目錄文件以確保功能運作正常。

5 在「**主機名稱**」欄位中，輸入 LDAP 伺服器的主機名稱或 IP 位址。

6 「**通訊埠**」用於存取 LDAP 伺服器。通訊埠會根據您的目錄類型和 SSL 設定自動填入，但您可以在此欄位中輸入新的值來加以修改。

7 如果您想要啟用所有對 LDAP 伺服器主機之連線的 SSL，請勾選「**啟用 SSL**」。無論用來簽署 LDAP 伺服器 x.509 憑證的憑證授權中心為何，皆會提供加密功能。如果您變更此核取方塊，則會自動將通訊埠更新為目錄類型的預設通訊埠。如果您變更此設定，請確認通訊埠。

8 如果您想要讓目錄資料服務連線至 LDAP 伺服器，而無需提供特定的使用者 ID 和密碼資訊，請勾選「**匿名繫結**」。或是勾選「**使用下列項目**」，以提供含特定驗證憑證的目錄資料服務。

9 如果您勾選「**使用下列項目**」，請在下列欄位中提供繫結憑證：

- **名稱 (繫結 DN)**
  用於對 LDAP 伺服器進行驗證的辨別名稱 (DN)。
  對於 Active Directory 或通用類別目錄伺服器，您可以選擇性使用完整 DN、NetBIOS 和登入名稱 (NetBIOS\SAM 帳戶名稱) 或使用者主要名稱。
- **密碼**
  用來驗證到 LDAP 伺服器的密碼。

10 按下**「測試登入」**以驗證對 LDAP 伺服器的驗證。

此測試僅確認是否可連線至 LDAP 伺服器，以及帳戶是否具有目錄伺服器上目錄資料樹狀結構之根目錄的讀取權限。因此，測試結果成功，並不保證憑證在目錄中的其他位置也可成功。對於匿名存取而言尤其如此。架構資料來源的個別功能時，請先使用「測試查詢」功能來確認存取權，再進行部署。

11 如果您想要架構選用 LDAP 伺服器和快取設定，請按下**「顯示進階設定」**。

請參閱第 484 頁的「架構資料來源進階設定」。

12 完成時，請按**「下一步」**以架構資料來源的功能。

請參閱第 428 頁的「啟用新資料來源的功能」。

啟用新資料來源的功能

「新增目錄資料來源」精靈中的第二個步驟，是啟用並架構資料來源的功能。啟用資料來源的功能之前，您必須先完成精靈中的第一個步驟，並在**「LDAP 伺服器組態」**頁面確認或架構該來源的 LDAP 連線設定。

請參閱第 426 頁的「新增資料來源」。

這些功能可以對資料來源啟用特定行為，並且可以讓您利用 Symantec Messaging Gateway 的許多功能。您可以架構一或多個功能的資料來源。

請參閱第 429 頁的「關於資料來源和功能」。

啟用新資料來源的功能

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上執行下列工作：

- 若要啟用並架構資料來源以進行一般使用者驗證、隔離所位址解析或 SMTP 驗證，請勾選**「驗證」**。
  請參閱第 431 頁的「建立驗證資料來源」。
  請參閱第 90 頁的「關於使用 SMTP 驗證」。
  若要自訂驗證、隔離所位址解析或 SMTP 驗證查詢，請勾選**「自訂查詢」**。
  請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。
- 若要啟用並架構資料來源以進行位址解析，請勾選**「位址解析」**。
  請參閱第 436 頁的「建立位址解析資料來源」。
  若要自訂位址解析組態，請勾選**「自訂查詢」**。
  請參閱第 450 頁的「建立和測試自訂位址解析查詢」。
- 若要啟用並架構資料來源以進行繞送，請勾選**「繞送」**。
  請參閱第 434 頁的「建立繞送資料來源」。

若要自訂繞送組態，請按下**「自訂查詢」**。
請參閱第 448 頁的「建立和測試自訂繞送查詢」。

- 若要啟用並架構資料來源以進行收件者驗證，請勾選**「收件者驗證」**。
  請參閱第 430 頁的「建立收件者驗證資料來源」。
  若要自訂收件者驗證組態，請勾選**「自訂查詢」**。
  請參閱第 443 頁的「建立和測試自訂的收件者驗證查詢」。

3 架構新資料來源的所有功能之後，請按**「下一步」**並確認組態。

4 若您滿意組態的內容，請按下**「儲存」**以儲存並部署資料來源。

關於資料來源和功能

若要整合 LDAP 目錄到 Symantec Messaging Gateway，您必須先架構資料來源。資料來源是一組組態資料，透過這些資料，可讓您的系統輕鬆地連線至 LDAP 伺服器，並使用 LDAP 伺服器。

當您架構資料來源時，您可以架構連線至 LDAP 伺服器的參數，以及每個資料來源提供的功能。

Symantec Messaging Gateway 僅針對收件者驗證功能支援備援資料來源，因為電子郵件地址或使用者名稱沒有唯一性需求。驗證、繞送和位址解析等其他 DDS 功能具有唯一性需求，並且不支援備援資料來源。

請參閱第 426 頁的「建立資料來源」。

在您架構目錄資料來源之後，便可以架構 Symantec Messaging Gateway 上的其他功能。

例如，如果您想要利用新的資料來源使用 LDAP 群組來套用政策，則必須啟用該資料來源的位址解析功能，並且架構位址解析查詢。

請參閱第 423 頁的「關於使用目錄資料服務」。

您可以針對每個資料來源，架構下列其中一個或多個功能：

- 驗證
  使用驗證功能，以便安全地驗證登入控管中心的一般使用者，以及驗證想要傳送電子郵件的使用者。驗證功能包括隔離所位址解析，這可讓您透過改善別名、散布清單及無效位址的處理，更妥善地管理垃圾郵件隔離所。
  請參閱第 437 頁的「關於將驗證功能與資料來源搭配使用」。
- 收件者驗證
  使用收件者驗證功能可根據目錄資料驗證電子郵件地址，並針對無效收件者棄置郵件或拒絕連線。
  請參閱第 439 頁的「關於透過資料來源使用收件者驗證功能」。
- 繞送
  使用繞送功能可使用目錄資料，根據每個使用者將郵件繞送至替代地址或主機郵件。
  請參閱第 438 頁的「關於搭配使用繞送功能與資料來源」。

- 位址解析
  使用位址解析功能可將政策一致地套用至使用者和群組。
  請參閱第 439 頁的「關於搭配使用位址解析功能與資料來源」。

建立收件者驗證資料來源

收件者驗證可與 Symantec Messaging Gateway 中的其他功能搭配運作，以協助您識別和管理無效的收件者以及傳送至這些收件者的郵件。Symantec Messaging Gateway 僅針對收件者驗證功能支援備援資料來源，因為電子郵件地址或使用者名稱沒有唯一性需求。驗證、繞送和位址解析等其他 DDS 功能具有唯一性需求，並且不支援備援資料來源。

請參閱第 439 頁的「關於透過資料來源使用收件者驗證功能」。

啟用功能是**「新增目錄資料來源」**精靈中的第二個步驟。在執行本主題所述的作業之前，您必須先在**「LDAP 伺服器組態」**頁面上，確認或架構該來源的 LDAP 連線設定。

請參閱第 426 頁的「新增資料來源」。

請參閱第 428 頁的「啟用新資料來源的功能」。

如果要使用無效收件者處理功能，則還必須架構無效收件者處理，並至少為一個網域啟用收件者驗證。

請參閱第 86 頁的「設定無效的收件者處理」。

請參閱第 71 頁的「新增或編輯網域」。

附註：請確認您的資料來源不會產生重疊的結果，以防止發生目錄資料服務錯誤。如果目錄資料服務在嘗試判斷訊息收件者是否有效時，無法與 LDAP 目錄伺服器正確通訊 (例如，如果關閉了至 LDAP 伺服器的網路連結)，MTA 會傳回錯誤，指出應該稍後重試傳送嘗試。請參閱第 429 頁的「關於資料來源和功能」。

架構新資料來源的收件者驗證

1. 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

   請參閱第 426 頁的「新增資料來源」。

2. 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上，勾選**「收件者驗證」**。
3. 在**「測試電子郵件地址」**欄位中，輸入可用來測試和驗證收件者驗證組態的電子郵件地址。賽門鐵克建議至少測試一個有效的地址和一個無效的地址。如果測試產生意料之外的結果，請使用**「自訂查詢」**來確認您的設定和目錄資料。
4. 如果要檢查或修改查詢的預設設定，請按下**「自訂查詢」**。建立自訂查詢可以更準確地反映系統組態。

   請參閱第 443 頁的「建立和測試自訂的收件者驗證查詢」。

5 按下「**測試查詢**」以使用提供的測試電子郵件地址來驗證查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

測試結果僅會反映正在測試中的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

6 您可以架構多個功能的資料來源，或是按「**下一步**」檢閱進行的變更，並儲存您的部署。

附註：如果需要子位址支援，請在「**通訊協定**」**> SMTP >**「**設定**」頁面上，於 **SMTP** 標籤上的「**地址驗證**」下，勾選「**移除收件者驗證目錄查詢中的子位址**」。

子位址由電子郵件地址的本機部分 (@ 之前的部分)，緊接在加號或減號之後的附加文字所組成。若勾選此選項，則 Symantec Messaging Gateway 會在完成 LDAP 收件者驗證查詢之前移除電子郵件地址的 *+詳細資料* 或 *-詳細資料* 部分。

如果您在電子郵件地址中使用加號或減號，但並非用於子位址，則啟用此功能會導致收件者驗證發生錯誤。

請參閱第 428 頁的「啟用新資料來源的功能」。

建立驗證資料來源

驗證可讓一般使用者向 LDAP 伺服器進行驗證，並架構使用者喜好設定。此外，還可以讓您架構 SMTP 驗證。

請參閱第 437 頁的「關於將驗證功能與資料來源搭配使用」。

請參閱第 90 頁的「關於使用 SMTP 驗證」。

啟用功能是「**新增目錄資料來源**」精靈中的第二個步驟。您必須先透過「**LDAP 伺服器組態**」頁面確認或架構該來源的 LDAP 連線設定，才可以啟用資料來源的功能。

請參閱第 426 頁的「新增資料來源」。

為防止出現目錄資料服務錯誤，請務必確保資料來源不會產生重疊的結果。表 19-4 說明目錄資料服務如何處理最常見條件的驗證錯誤。

請參閱第 429 頁的「關於資料來源和功能」。

表 19-4 常見的目錄資料服務驗證錯誤

驗證錯誤	系統行為
當目錄資料服務嘗試對控管中心或 SMTP 伺服器驗證使用者時，無法正確地與 LDAP 目錄伺服器通訊。 例如，當 LDAP 伺服器的網路連結中斷時，就會發生這種情況。	這時會顯示「服務暫時無法使用」錯誤。如果「**警示**」頁面上已經啟用適當的警示，就會觸發「**目錄資料存取錯誤**」警示。

驗證錯誤	系統行為
目錄資料服務無法依據提供的使用者名稱唯一判斷使用者身分。	這時會顯示「服務暫時無法使用」錯誤。如果**「警示」**頁面上已經啟用適當的警示，就會觸發**「目錄資料存取錯誤」**警示。
當目錄資料服務嘗試將隔離郵件的收件者解析為收件者的主要電子郵件地址，或唯一判斷收件者的主要電子郵件地址時，無法正確地與 LDAP 目錄伺服器通訊。	該郵件會保留在傳送佇列中。如果**「警示」**頁面上已經啟用警示，就會觸發適當的警示。

請參閱第 590 頁的「架構警示」。

架構新資料來源的驗證

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上，勾選**「驗證」**。

3 在**「驗證類型」**下拉式功能表中，選擇下列其中一項：

僅控管中心驗證	僅驗證一般使用者是否能存取隔離所或設定一般使用者喜好設定。
僅 SMTP 驗證	讓遠端使用者能夠透過 SMTP 驗證使用 Symantec Messaging Gateway 傳送電子郵件。
控管中心和 SMTP 驗證	同時啟用控管中心與 SMTP 驗證。

4 如果您選取**「僅控管中心驗證」**或**「控管中心和 SMTP 驗證」**作為驗證類型，請確認或架構以下測試資料，或按下**「自訂查詢」**來檢視或自訂您的查詢。

請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。

測試使用者名稱

輸入可用來測試並驗證您的驗證組態的使用者名稱。

賽門鐵克建議您使用旨在產生成功驗證和失敗驗證的多種輸入來確認您的設定。如果測試產生意料之外的結果，請使用**「自訂查詢」**來確認您的設定和目錄資料。

測試密碼

輸入測試使用者名稱的密碼。

測試網域 (選用)

輸入所提供測試憑證的 NetBIOS 網域。

只在使用 Active Directory 或 Active Directory 通用類別目錄，且提供的**「測試使用者名稱」**是網域專屬的使用者名稱時，才需要提供測試網域。

測試查詢

按下可以使用所提供的測試資訊驗證您的查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

測試結果僅會反映正在測試中的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

自訂查詢

如果要檢查或修改查詢的預設設定，請按下**「自訂查詢」**。您可以建立能夠更準確地反映您系統組態的自訂查詢。

請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。

測試電子郵件地址

輸入可用來測試和驗證隔離所位址解析組態的電子郵件地址。賽門鐵克建議您使用位址 (包括使用者位址、散布清單位址、別名位址和無效位址) 的組合來測試您的資料來源。

測試查詢

按下可以使用所提供的測試電子郵件地址來驗證定義的隔離所位址解析查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

測試結果僅會反映正在測試中的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

自訂查詢

如果要檢查或修改查詢的預設設定，請按下**「自訂查詢」**。

請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。

5 如果您選取「**僅驗證 SMTP**」或「**控管中心和 SMTP 驗證**」作為驗證類型，請架構以下欄位，或按下「**自訂查詢**」來檢視或自訂您的查詢。

請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。

如果選取控管中心和 SMTP 驗證，則可以同時勾選「**共用控管中心和 SMTP 驗證查詢詳細資料**」，以使用為控管中心提供的 SMTP 詳細資料來填入 SMTP 詳細資料，然後略過此步驟。

測試使用者名稱 輸入可用來測試並驗證您的 SMTP 驗證組態的使用者名稱。

賽門鐵克建議您使用旨在產生成功驗證和失敗驗證的多種輸入來確認您的設定。如果測試產生意料之外的結果，請按下「**自訂查詢**」來確認您的設定和目錄資料。

測試密碼 輸入測試使用者名稱的密碼。

測試查詢 按下可以使用所提供的測試使用者名稱和密碼來驗證定義的 SMTP 驗證查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

測試結果僅會反映所測試的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

自訂查詢 按下「**自訂查詢**」可以建立自訂查詢，或是檢查查詢的預設設定。

您可以建立能夠更準確地反映您系統組態的自訂查詢。

請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。

6 您可以架構多個功能的資料來源，或是按「**下一步**」檢閱進行的變更，並儲存您的部署。

請參閱第 428 頁的「啟用新資料來源的功能」。

建立繞送資料來源

繞送功能會使用資料來源提供的資訊，將郵件繞送至位址與網域。

請參閱第 438 頁的「關於搭配使用繞送功能與資料來源」。

每個網域都可以架構為根據目錄資料來源、目的主機或 MX 查詢來繞送郵件。 本節將討論使用目錄資料來源的繞送。對於其他繞送類型，您應該查閱網域文件。

請參閱第 71 頁的「新增或編輯網域」。

啟用功能是「**新增目錄資料來源**」精靈中的第二個步驟。您必須先透過「**LDAP 伺服器組態**」頁面架構資料來源的 LDAP 連線設定，才可以啟用該來源的功能。

請參閱第 426 頁的「建立資料來源」。

請確認您的資料來源不會產生重疊的結果，以防止發生目錄資料服務錯誤。表 19-5 說明目錄資料服務如何處理最常見條件的繞送錯誤。

請參閱第 429 頁的「關於資料來源和功能」。

表 19-5 目錄資料服務繞送錯誤

目錄資料服務繞送處理錯誤	系統行為
當目錄資料服務嘗試判斷郵件收件者的繞送資訊時，無法正確地與 LDAP 目錄伺服器通訊。例如，當 LDAP 伺服器的網路連結中斷時，就會發生這種情況。	MTA 會佇列郵件，並定期重新嘗試執行作業。觸發**「目錄資料存取錯誤」**警示。
目錄資料服務無法唯一判斷與收件者對應的 LDAP 項目。	傳送郵件而不嘗試套用繞送資訊。如果**「警示」**頁面上已經啟用適當的警示，就會觸發**「目錄資料完整性錯誤」**警示。

請參閱第 590 頁的「架構警示」。

架構新資料來源的繞送：

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面中，勾選**「繞送」**。

3 在**「測試電子郵件地址」**欄位中，輸入可用來測試和驗證繞送組態的電子郵件地址。如果測試產生意料之外的結果，請使用**「自訂查詢」**來確認您的設定和目錄資料。

此精靈為使用 SunOne 目錄類型的 LDAP 組態提供了一組預設屬性值。如果您的組態使用不同的目錄類型，或者如果您要使用不同的繞送屬性來繞送郵件，請按下**「自訂查詢」**來架構查詢。

請參閱第 448 頁的「建立和測試自訂繞送查詢」。

4 按下**「測試查詢」**以使用提供的測試電子郵件地址來驗證查詢資料。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

測試結果僅會反映所測試的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名與偽裝) 效果的資訊。

5 您可以架構多個功能的資料來源，或是按**「下一步」**檢閱進行的變更，並儲存您的部署。

請參閱第 428 頁的「啟用新資料來源的功能」。

建立位址解析資料來源

位址解析功能會解析別名與散布清單資料。此舉讓您使用以LDAP為基礎的群組成員資格來定義政策，以針對每位使用者套用政策。

請參閱第 439 頁的「關於搭配使用位址解析功能與資料來源」。

啟用功能是**「新增目錄資料來源」**精靈中的第二個步驟。您必須先透過**「LDAP 伺服器組態」**頁面確認或架構該來源的 LDAP 連線設定，才可以執行本主題所述的工作。

請參閱第 426 頁的「新增資料來源」。

請參閱第 428 頁的「啟用新資料來源的功能」。

請確認您的資料來源不會產生重疊的結果，以防止發生目錄資料服務錯誤。表 19-6 說明目錄資料服務如何處理最常見錯誤條件的位址解析錯誤。

請參閱第 429 頁的「關於資料來源和功能」。

表 19-6 目錄資料服務處理位址解析錯誤

位址解析錯誤狀況	系統行為
當目錄資料服務為 BATV 用途而嘗試解析郵件收件者時，無法正確地與 LDAP 目錄伺服器通訊或是唯一判斷符合收件者的 LDAP 項目。 例如，當 LDAP 伺服器的網路連結中斷時，就會發生這種情況。	MTA 傳回「已中斷 451 要求動作： 處理期間發生錯誤」錯誤。 假定**「警示」**頁面上已經啟用目錄資料服務警示，就會觸發適當的目錄資料服務警示。
當目錄資料服務為掃描用途而嘗試解析郵件收件者時，無法正確地與 LDAP 目錄伺服器通訊。	此郵件會放置在入埠延遲佇列並定時重試。如果已啟用警示，就會觸發**「目錄資料存取錯誤」**警示。
目錄資料服務無法唯一判斷與收件者對應的 LDAP 項目。	傳送郵件而不嘗試套用位址解析資訊。政策群組只會依據原始的收件者地址來套用。如果已啟用警示，會同時觸發**「目錄資料完整性錯誤」**警示。

請參閱第 590 頁的「架構警示」。

架構新資料來源的位址解析

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上，勾選**「位址解析」**。

3 在「**測試電子郵件地址**」欄位中，輸入可用來測試和驗證組態的電子郵件地址。

賽門鐵克建議測試多種位址，包括主要位址、別名位址、散布清單位址以及無效位址。如果測試產生意料之外的結果，請按下「**自訂查詢**」來確認您的設定和目錄資料。

由於測試查詢是作為即時查詢執行(與快取查詢相反)，因此賽門鐵克建議測試其中一個較小的散布清單。

4 按下「**測試查詢**」以使用測試電子郵件地址來驗證位址解析查詢資料。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

如果查詢成功，則可按下「**測試查詢**」選項旁邊的圖示，以顯示所有查詢結果。此測試會報告與測試電子郵件地址相關聯的所有電子郵件地址及使用者喜好設定。如果收件者是散布清單，則會將此資訊提供給屬於該散布清單的所有使用者。

測試結果僅會反映正在測試中的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名與偽裝) 效果的資訊。

5 如果要檢查或修改查詢的預設設定，請按下「**自訂查詢**」。建立自訂查詢可以更準確地反映系統組態。

請參閱第 450 頁的「建立和測試自訂位址解析查詢」。

6 按下「**測試查詢**」以使用測試電子郵件地址來驗證群組清單查詢資料。

測試結果僅會反映正在測試中的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

7 如果要檢查或修改群組清單查詢的預設設定，請按下「**自訂查詢**」。

請參閱第 450 頁的「建立和測試自訂位址解析查詢」。

8 您可以架構多個功能的資料來源，或是按「**下一步**」檢閱進行的變更，並儲存您的部署。

請參閱第 428 頁的「啟用新資料來源的功能」。

關於將驗證功能與資料來源搭配使用

驗證資料來源提供一般使用者功能，例如一般使用者喜好設定、一般使用者對垃圾郵件隔離所的存取權，以及 SMTP 驗證。

請參閱第 423 頁的「關於使用目錄資料服務」。

啟用資料來源進行驗證時，系統可以執行下列工作：

- 啟用並驗證一般使用者對「垃圾郵件隔離所」的存取權。
  您也必須至少架構一個政策群組來隔離垃圾郵件，並架構隔離所設定與垃圾郵件過濾。
  請參閱第 168 頁的「關於選取政策群組的過濾政策」。
  請參閱第 239 頁的「關於隔離垃圾郵件」。
  請參閱第 213 頁的「關於過濾垃圾郵件及不必要的郵件」。

- 可讓一般使用者架構「使用者喜好設定」，包含個人允許的寄件者及攔截的寄件者清單以及個人語言設定 (還必須啟用位址解析)。
  請參閱第 439 頁的「關於搭配使用位址解析功能與資料來源」。
  請參閱第 173 頁的「啟用與停用政策群組的使用者設定」。
- 讓已驗證的一般使用者透過 SMTP 驗證通訊協定從遠端傳送電子郵件。
  您還必須設定 SMTP 驗證。
  請參閱第 90 頁的「關於使用 SMTP 驗證」。

啟用驗證時，也會自動啟用隔離所位址解析。此查詢會從入埠郵件取得資訊，並使用該資訊將電子郵件別名解析至隔離郵件之收件者的主要電子郵件地址。因此，不論原來要將郵件傳送至哪個別名，使用者均可存取其所有隔離的郵件。

請參閱第 239 頁的「關於隔離垃圾郵件」。

請參閱第 431 頁的「建立驗證資料來源」。

關於搭配使用繞送功能與資料來源

繞送功能可讓您根據目錄資料架構每個使用者的繞送。例如，您可以使用此功能，繞送目的為已指定替代電子郵件地址或郵件主機之使用者的電子郵件 (如同與使用者自己的帳戶關聯的屬性一樣)。

每個網域都可以架構為根據目錄資料來源、目的主機或 MX 查詢來繞送郵件。本節將討論使用目錄資料來源的繞送。對於其他類型的繞送，請參閱網域文件。

請參閱第 71 頁的「新增或編輯網域」。

在針對目錄型繞送啟用資料來源後，您可以架構目錄資料服務，將電子郵件繞送至替代電子郵件地址和郵件主機。

請參閱第 434 頁的「建立繞送資料來源」。

如果您同時架構**「替代地址屬性」**和**「替代郵件主機屬性」**，目錄資料服務會先解析所有的替代電子郵件地址，然後再解析替代郵件主機。如果找到替代地址屬性，則資料服務會嘗試評估新地址。 如果是本機地址，資料服務接著會嘗試尋找新的替代地址。

一旦所有的本機替代地址均完成解析，就會接著套用該最後的位址的規則，以用於替代郵件主機繞送。

以下範例顯示當您將郵件傳送給同時有替代郵件主機與替代地址值的繞送使用者時，會發生什麼狀況：

1 傳送到此使用者的郵件將解析為替代地址，並被轉寄到新地址。

2 如果新地址是本機地址，並且該使用者也已建立關聯的替代地址，則郵件會被轉寄至下一個地址。

3 如果只與最後一個地址有關聯的使用者已建立了替代郵件主機值，則會透過定義的郵件主機將郵件傳送至最後的電子郵件地址。

附註：如果 LDAP 項目有多個替代郵件主機屬性值，則每次將郵件傳送給該收件者時，MTA 會隨機選擇其中一個值使用。提供替代電子郵件地址屬性時，前往原始使用者的郵件會重新繞送至新的電子郵件地址。如果提供了多個替代地址值，則此郵件會重新繞送到所有替代地址。

若要將郵件繞送至替代地址或郵件主機，您必須將所需的網域與繞送資料來源產生關聯。

請參閱第 71 頁的「新增或編輯網域」。

請參閱第 70 頁的「關於電子郵件網域」。

請參閱第 434 頁的「建立繞送資料來源」。

關於搭配使用位址解析功能與資料來源

位址解析功能可解析別名和散布清單資料，讓您能夠針對每位使用者套用政策。您可以使用以 LDAP 為基礎的群組成員資格定義政策來完成此項工作。

為位址解析啟用資料來源可提供以下優點：

- 系統可以解析目錄群組和散布清單成員資格，讓掃描程式能套用過濾器政策至政策群組。請注意，必須啟用散布清單展開，才能將政策套用至散布清單中的使用者。
  請參閱第 168 頁的「關於選取政策群組的過濾政策」。
  請參閱第 455 頁的「關於展開散布清單和保留收件者地址」。
- 系統可以將別名電子郵件地址重寫為主要電子郵件地址，以確保一致地套用政策。
- 您可以讓一般使用者根據電子郵件地址架構「使用者喜好設定」，例如個人的語言設定以及「允許的寄件者」清單和「攔截的寄件者」清單。請注意，同時也必須啟用驗證。
  請參閱第 437 頁的「關於將驗證功能與資料來源搭配使用」。
  請參閱第 173 頁的「啟用與停用政策群組的使用者設定」。
- 啟用位址解析時，會自動啟用選用群組清單查詢。此功能可讓您透過從 LDAP 使用者和群組清單中進行選取，更輕鬆地定義所屬政策群阻。架構群組清單查詢時，會將查詢所擷取之所有 LDAP 群組的清單 (包括 LDAP 散布清單) 填入**「新增政策群組」**頁面中的群組清單。

  您可以從此清單選取要新增至政策的群組，也可以自行輸入 LDAP 群組辨別名稱來新增群組。如果您的組織擁有大量群組，可能需要在架構資料來源時停用此查詢。

請參閱第 436 頁的「建立位址解析資料來源」。

關於透過資料來源使用收件者驗證功能

收件者驗證可確定收件者地址是否有效。如果地址位於至少一個為了進行收件者驗證而啟用的資料來源中，則為有效地址。如果查詢地址有效且已啟用快取，則會快取對應的收件者項目供將來使用 (快取預設為啟用)。如果某個查詢地址無效，則會將該地址快取至無效收件者快取中。

收件者驗證可與 Symantec Messaging Gateway 中的其他功能搭配運作，以協助您識別和管理無效的收件者以及傳送至這些收件者的郵件。

請參閱第 423 頁的「關於使用目錄資料服務」。

啟用資料來源以進行收件者驗證可提供以下優點：

- 驗證電子郵件收件者並拒絕連線，或棄置無效收件者的郵件。您還必須正確架構無效收件者處理，才能啟用此行為。
  請參閱第 86 頁的「設定無效的收件者處理」。
- 執行電子郵件地址搜尋攻擊識別。您還必須架構電子郵件地址搜尋攻擊識別，才能啟用此行為。
- 擷取無效收件者電子郵件地址，Symantec Probe Network 會將其用作探查帳戶。
  請參閱第 269 頁的「關於探查帳戶」。

請參閱第 430 頁的「建立收件者驗證資料來源」。

啟用無效的收件者處理，以拒絕或棄置傳送至無效收件者的郵件之後，就無法再刪除或停用該來源。若要刪除或停用此類資料來源，您必須將無效的收件者處理重新架構為接受所有郵件。

Symantec Messaging Gateway 僅針對收件者驗證功能支援備援資料來源，因為電子郵件地址或使用者名稱對此功能沒有唯一性需求。

請參閱第 86 頁的「設定無效的收件者處理」。

關於資料來源查詢

Symantec Messaging Gateway 針對適用於最常見之郵件系統組態的每個功能，提供了預設查詢。可使用功能頁面上的**「自訂查詢」**選項來檢視和確認這些設定。如果您的 LDAP 架構需要唯一查詢，則可以針對任何已啟用的功能建立查詢，來變更範圍並支援自訂目錄架構。

首先，可使用**「基準 DN」**欄位來設定目錄搜尋的範圍。

您可以為要搜尋的目錄子集提供辨別名稱 (DN)。目錄子集越小，系統傳回資料的速度就越快。

例如，全球公司的預設查詢可能是：dc=company, dc=com。如果您需要將搜尋範圍限制在紐約辦公室，則可以設定基準 DN，將搜尋範圍限制在目錄中的該子配置區。在此情況下，自訂基準 DN 可能是：ou=NewYork, dc=company, dc=com。

附註：此欄位中不會提供所有目錄類型的**「基準 DN」**，但 Domino 或 Active Directory 通用類別目錄查詢例外。

在**「查詢過濾」**欄位中，您可以定義目錄資料服務用來搜尋目錄中項目的規則。透過使用描述特定 LDAP 查詢語法的屬性和 Token，來使用讓目錄資料服務傳回資料的自訂查詢過濾。

查詢過濾是以標準 LDAP 查詢語法指定的。例如，email=%s 描述的過濾，會找出名為 email 的屬性符合以完整形式提供之電子郵件地址 (如 %s 查詢過濾 Token 所示) 的所有記錄。

查詢過濾至少需要一個 Token。表 19-7 說明您可用來建構查詢過濾的 Token。您所使用的 Token 同樣取決於您的目錄類型。如需有關您的目錄支援下列哪些 Token 的資訊，請查詢適用於您的目錄類型的文件。

表 19-7 Symantec Messaging Gateway 支援的查詢過濾的 Token

語法	指示目錄資料服務在擷取項目時查詢下列資訊：	傳回含有下列類型資訊的項目
%s	要尋找的電子郵件地址，包含使用者 ID 和完整的網域名稱。	joe_smith@example.com
%u	要尋找之電子郵件地址的本機部分。	joe_smith
%d	要尋找之電子郵件地址的網域部分。	example.com
%n	要尋找的完整名稱。 句點與底線會以空格字元加以取代。連續句點或底線會以單一空格加以取代。如此可將相同地址的多個版本合併成快取中的單一項目，從而有利於隔離所位址解析。 由於 Domino 可以架構為將 FullName (cn) 屬性視為可傳送電子郵件地址，因此在使用 Domino 時，這項 Token 會很有用。	joe smith

您可以結合具有和不具有 Token 的屬性，以縮小傳回資料的範圍。例如，如果您將查詢過濾 mail=%s 與收件者驗證功能配合使用，且只想傳回個別使用者 (而非散布清單等)，則可以使用下列過濾：(&(objectClass=person)(mail=%s))。

表 19-8 說明您可用來架構查詢過濾的運算子。

表 19-8 Symantec Messaging Gateway 支援的查詢過濾運算子

運算子	指出其值為	範例	傳回的資料
=	等於	o=symantec	組織名稱為 Symantec 的項目。
~=	約等於	(sn~=Johnson)	名稱類似於 Johnson 的項目。 尋找類似所提供名稱的項目。例如，目錄伺服器可能會傳回姓氏為 Jonson 及 Johnsen 的項目。 大約相符的規則視目錄類型而有所不同，而且並非所有目錄類型都支援此運算子。如需詳細資訊，請查閱您的目錄文件。

運算子	指出其值為	範例	傳回的資料
<=	小於或等於	(st<=ca)	出現在所提供資訊之英文字母之前或相同位置的項目。 在此情況下，名稱 ca 以及英文字母狀態屬性清單中出現在 ca 之前的名稱 (例如 ak) 都會傳回。
>=	大於或等於	(st>=ca)	出現在所提供資訊之英文字母之後或相同位置的項目。 在此情況下，名稱 ca 以及英文字母狀態屬性清單中出現在 ca 之後的名稱 (例如 va) 都會傳回。
&	和	(&(o=symantec)(co=france))	組織名稱為 Symantec 且國家為 France 的項目。
=*	存在	(&(mail=%s)(mailboxFile=*))	郵件屬性與完整的收件者地址完全相符的項目，以及所含的任何 mailboxFile 屬性值可表示使用者具有作用中電子郵件信箱的項目。
|	或	(|(o=symantec)(sn=simpson) (cn=simpson))	組織為 Symantec、姓氏為 Simpson，或一般名稱為 Simpson 的項目。
!	非	(!(STREET=*))	不含 StreetAddress 屬性的項目。 請注意，使用 ! 運算子時，必須將其放在括弧外，如下所示：(!(<filter>))。
*	萬用字元	(o=*yma*)	含有字串 yma 的組織名稱 (例如 Symantec) 以及完全與 yma 相符的字串 (如果有)。

最後，請依需要自訂屬性 (例如**「主要電子郵件屬性」**) 以及物件類別 (例如「**散布清單物件類別**」)，以符合您的特定需求。

請確保用來連線至 LDAP 伺服器的管理員憑證可存取您提供的屬性。如果帳戶沒有適當的存取權，或提供的屬性不存在或拼錯，則查詢結果會表示沒有與此屬性相關聯的資料。

請參閱第 426 頁的「建立資料來源」。

請參閱第 444 頁的「建立及測試自訂驗證與隔離所位址解析查詢」。

請參閱第 443 頁的「建立和測試自訂的收件者驗證查詢」。

請參閱第 448 頁的「建立和測試自訂繞送查詢」。

請參閱第 450 頁的「建立和測試自訂位址解析查詢」。

建立和測試自訂的收件者驗證查詢

您可以檢視預設查詢資訊，也可以透過架構自訂屬性及過濾器來自訂查詢，以變更查詢範圍並支援唯一目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

賽門鐵克建議您在部署新資料來源之前，先測試所有查詢。

為新資料來源架構自訂的收件者驗證查詢：

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上，勾選**「收件者驗證」**，然後按下**「自訂查詢」**。

請參閱第 428 頁的「啟用新資料來源的功能」。

3 提供以下資訊：

基準 DN	提供查詢的**「基準 DN」**。 系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。
自訂查詢起點	如果在**「基準DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。 您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。**「自訂查詢起點」**可讓您架構查詢，以符合特定需求並更快速地傳回資料。
查詢過濾	提供查詢的**「查詢過濾」**。查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。
還原預設值	如果您要移除對收件者驗證查詢組態欄位所進行的編輯，並使用預設值加以取代，請按下**「還原預設值」**。
測試電子郵件地址	提供可用來測試及驗證收件者驗證組態的**「測試電子郵件位址」**。賽門鐵克建議至少測試一個有效的地址和一個無效的地址。
測試查詢	按下**「測試查詢」**，使用提供的測試電子郵件地址來驗證已定義的查詢。 此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。 測試結果僅會反映正在測試中的資料來源。測試結果不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

4 按下**「儲存」**返回**「新增目錄資料來源」->「目錄資料來源功能」**頁面。

請參閱第 428 頁的「啟用新資料來源的功能」。

建立及測試自訂驗證與隔離所位址解析查詢

您可透過將自訂屬性及過濾器架構為符合系統組態來自訂查詢。使用自訂查詢可變更範圍並支援唯一目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

自訂新資料來源的驗證查詢

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上，勾選**「驗證」**，選取您要使用的驗證類型，然後按下**「自訂查詢」**。

您也可以按下**「自訂查詢」**來檢查查詢的預設值。

請參閱第 428 頁的「啟用新資料來源的功能」。

3 在**「驗證類型」**下拉式清單中，選取您要針對資料來源架構的驗證類型。

僅控管中心驗證	僅驗證一般使用者是否能存取隔離所或設定一般使用者喜好設定。 您必須架構控管中心驗證與隔離所位址解析查詢。
僅 SMTP 驗證	讓遠端使用者能夠透過 SMTP 驗證使用 Symantec Messaging Gateway 傳送電子郵件。 您必須架構 SMTP 驗證查詢。
控管中心和 SMTP 驗證	同時啟用控管中心和 SMTP 驗證的所有功能。 您必須架構控管中心驗證、隔離所位址解析及 SMTP 驗證查詢。如果您要共用查詢詳細資料，則可勾選**「共用控管中心和 SMTP 驗證查詢詳細資料」**。

4 已選取控管中心及 SMTP 驗證時，如果您想將控管中心驗證資訊當做 SMTP 驗證資訊使用，則可勾選**「共用控管中心和 SMTP 驗證查詢詳細資料」**。

5 如果您已選取**「僅控管中心驗證」**或**「控管中心和 SMTP 驗證」**作為驗證類型，則請為控管中心驗證查詢提供下列資訊：

NetBIOS 網域名稱 (選用)	提供系統可用來解析登入不明之 NetBIOS 網域名稱的清單。 此為選用欄位，但是如果符合以下所有情況時，則建議使用： ■ 您的目錄類型為 Active Directory 或 Active Directory 通用類別目錄 ■ 您的目錄使用多個 NetBIOS 網域 ■ 無法確保使用者名稱的唯一性

基準 DN	提供繞送查詢的「**基準 DN**」。 已提供預設值，如果選取自訂，則可以在「**自訂查詢起點**」欄位中提供自訂查詢起點。
自訂查詢起點	如果在「**基準DN**」欄位中選取「自訂」，請提供「**自訂查詢起點**」。
查詢過濾	視需要修改驗證查詢的預設「**查詢過濾**」。 查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。
主要電子郵件屬性	此欄位與 SMTP 驗證無關，但它是控管中心驗證的必要欄位。 輸入 LDAP 架構中可用來儲存驗證查詢之主要電子郵件地址資訊的屬性。 如果您指定 proxyAddresses 的主要電子郵件屬性，則目錄資料服務會自動識別前面加上 SMTP 作為位址的屬性值。您不需要在「主要電子郵件屬性」欄位中指定此字首。
目錄整合設定 - 目錄資料來源驗證方法	選擇您的「**驗證方法**」。 按下「**簡單繫結**」嘗試藉由使用者提供的密碼來登入。 或者，您可以使用密碼取回，以從資料來源取回密碼，並將它與使用者提供的密碼進行比較。按下「**密碼屬性**」來選擇密碼取回。 (可選) 您可以為密碼取回指定「**預設雜湊類型**」。如果您選擇「**無**」，則目錄資料必須在密碼屬性前面添加表示配置的前置位元 (例如 **{PLAIN}**)。如果您選擇「**純文字**」，則不需要配置前置位元。 Symantec Messaging Gateway 透過將簡單繫結用於支援的所有 LDAP 目錄類型，支援透過 LDAP 進行 SMTP 驗證。對於透過使用密碼取回之 LDAP 所進行的 SMTP 驗證，所有支援的目錄類型 (Active Directory、Active Directory 通用類別目錄及 Domino 除外) 都受到支援。
測試使用者名稱	輸入可用來測試並驗證您的驗證組態的使用者名稱。 賽門鐵克建議您使用預期產生成功和失敗驗證的多種輸入來確認您的設定。如果測試產生意料之外的結果，請使用「**自訂查詢**」來確認您的設定和目錄資料。
測試密碼	輸入測試使用者名稱的密碼。
還原預設值	按下「**還原預設值**」，將設定還原為預設值。
測試網域 (選用)	輸入所提供測試憑證的 NetBIOS 網域。 只在使用 Active Directory 且提供的「**測試使用者名稱**」是網域專屬的使用者名稱時，才需要提供測試網域。

測試查詢

按下可以使用所提供的測試電子郵件地址來驗證定義的隔離所位址解析查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不會驗證從連接之掃描程式到 LDAP 伺服器的連線。

測試結果僅會反映所測試的資料來源。結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

6 如果您已選取**「僅控管中心驗證」**或**「控管中心和 SMTP 驗證」**作為驗證類型，則請為隔離所位址解析查詢提供下列資訊：

查詢過濾

在「隔離所位址解析查詢」下的**「查詢過濾」**欄位中，視需要修改預設過濾器。查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。

散布清單物件類別

在**「散布清單物件類別」**欄位中，鍵入 LDAP 架構中應該用來識別散布清單項目的物件類別。

還原預設值

按下**「還原預設值」**，將設定還原為預設值。

測試電子郵件地址

在**「測試電子郵件地址」**欄位中，鍵入可用來測試和驗證隔離所位址解析組態的位址。賽門鐵克建議使用組合位址 (包含使用者位址、散布清單位址、別名位址及無效位址) 來測試資料來源。

測試查詢

按下**「測試查詢」**，使用提供的測試電子郵件地址來驗證已定義的隔離所位址解析查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不會驗證從連接之掃描程式到 LDAP 伺服器的連線。

測試結果僅會反映正在測試中的資料來源。結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

7 如果您已選取**「僅 SMTP 驗證」**或**「控管中心和 SMTP 驗證」**，請為 SMTP 驗證查詢提供下列資訊。

如果架構控管中心和 SMTP 驗證，則可以勾選**「共用控管中心和 SMTP 驗證查詢詳細資料」**，以使用為控管中心提供的 SMTP 詳細資料來填入 SMTP 詳細資料，然後略過此步驟。

基準 DN	提供繞送查詢的**「查詢起點」**。 系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。
自訂查詢起點	如果在**「基準 DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。 您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。這可讓您架構查詢，以符合特定需求並更快速地傳回資料。
查詢過濾	視需要提供**「查詢過濾」**以進行 SMTP 驗證查詢。 登入查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。
主要電子郵件屬性	此欄位與 SMTP 驗證無關， 它是控管中心驗證的必要欄位。 在**「主要電子郵件屬性」**欄位中，鍵入 LDAP 架構中用來儲存 SMTP 驗證查詢之主要電子郵件地址資訊的屬性。
驗證方法	選擇您的**「驗證方法」**。 按下**「簡單繫結」**嘗試藉由使用者提供的密碼來登入。 或者，您可以使用密碼取回，以從資料來源取回密碼，並將它與使用者提供的密碼進行比較。按下**「密碼屬性」**來選擇密碼取回。 您可以使用預設密碼屬性，也可以加以變更。 (可選) 您可以為密碼取回指定**「預設雜湊類型」**。如果您選擇**「無」**，則目錄資料必須在密碼屬性前面添加表示配置的前置位元 (例如**{PLAIN}**)。如果您選擇**「純文字」**，則不需要配置前置位元。 Symantec Messaging Gateway 透過將簡單繫結用於支援的所有 LDAP 目錄類型，支援透過 LDAP 進行 SMTP 驗證。對於透過使用密碼取回之 LDAP 所進行的 SMTP 驗證，所有支援的目錄類型 (Active Directory、Active Directory 通用類別目錄及 Domino 除外) 都受到支援。
還原預設值	按下**「還原預設值」**，將設定還原為預設值。
測試使用者名稱	輸入可用來測試並驗證您的驗證組態的使用者名稱。 賽門鐵克建議您使用預期產生成功和失敗驗證的多種輸入來確認您的設定。如果測試產生意料之外的結果，請使用**「自訂查詢」**來確認您的設定和目錄資料。

測試密碼	輸入測試使用者名稱的密碼。
測試查詢	按下可以使用所提供的測試使用者名稱和密碼來驗證定義的 SMTP 驗證查詢。 此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不會驗證從連接之掃描程式到 LDAP 伺服器的連線。 測試結果僅會反映所測試的資料來源。結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

8 按下**「儲存」**返回**「新增目錄資料來源」->「目錄資料來源功能」**頁面。

請參閱第 428 頁的「啟用新資料來源的功能」。

建立和測試自訂繞送查詢

您可透過將自訂屬性及過濾器架構為符合系統組態來自訂查詢。使用自訂查詢頁面來自訂繞送查詢，可變更範圍並支援自訂目錄架構。根據所選取的目錄類型，繞送屬性可能不會預先填入預設值。如果沒有填入屬性名稱，除非在LDAP 架構描述中至少提供一個屬性，否則無法儲存繞送查詢。

請參閱第 440 頁的「關於資料來源查詢」。

本節涵蓋以目錄為基礎的繞送。如需有關目的主機繞送或MX 查詢之其他繞送方法的資訊，請參閱網域文件。

請參閱第 71 頁的「新增或編輯網域」。

賽門鐵克建議您在部署新資料來源之前，先測試所有查詢。

為新資料來源架構自訂繞送查詢：

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上，勾選**「繞送」**，然後按下**「自訂查詢」**。

請參閱第 428 頁的「啟用新資料來源的功能」。

3 提供以下資訊：

基準 DN	提供查詢的**「基準 DN」**。 系統會提供預設值，或者，您可以選取「自訂」，即可在**「自訂查詢起點」**欄位中提供自己的值。

自訂查詢起點

如果在「**基準 DN**」欄位中選取「自訂」，則必須提供「**自訂查詢起點**」。

您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。「**自訂查詢起點**」可讓您架構查詢，以符合特定需求並更快速地傳回資料。

查詢過濾

視需要提供繞送查詢的「**查詢過濾**」。查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。

替代地址屬性

如果您要啟用每個使用者以目錄為基礎的替代地址繞送，請提供「**替代地址屬性**」。提供替代電子郵件地址屬性後，前往原始使用者的郵件會重新繞送至新的電子郵件地址。如果有多個替代地址，則此郵件會重新繞送到所有替代地址。

附註：若要儲存繞送來源，請提供「**替代地址屬性**」和/或「**替代郵件主機屬性**」。如果您同時架構「**替代地址屬性**」和「**替代郵件主機屬性**」，目錄資料服務便會解析所有的替代電子郵件地址，然後再解析替代郵件主機。

請參閱第 438 頁的「關於搭配使用繞送功能與資料來源」。

替代郵件主機屬性

如果您要啟用以目錄為基礎的替代郵件主機繞送，請提供「**替代郵件主機屬性**」，此屬性對應於您選取用來儲存此資訊之目錄架構中的屬性。

郵件主機應指定為 IP 位址或完整的主機名稱。您可使用冒號後面接著通訊埠來指定通訊埠，例如「:25」。根據預設，SMTP 通訊協定會使用通訊埠 25 來進行電子郵件傳輸。

您可以使用下列有效屬性：

- 10.32.100.64
- 10.32.100.64:25
- myothermailserver.mycompany.com
- myothermailserver.mycompany.com:25

如果 LDAP 項目有多個替代郵件主機屬性值，則每次有郵件傳送至該收件者時，MTA 就會隨機選取其中一個值來使用。

附註：若要儲存繞送來源，請提供「**替代地址屬性**」和/或「**替代郵件主機屬性**」。如果您同時架構「**替代地址屬性**」和「**替代郵件主機屬性**」，目錄資料服務便會解析所有的替代電子郵件地址，然後再解析替代郵件主機。

請參閱第 438 頁的「關於搭配使用繞送功能與資料來源」。

對替代郵件主機執行 MX 查詢

勾選「**對替代郵件主機執行 MX 查詢**」，以允許對指定的替代郵件主機進行 MX 查詢。MX 查詢會對網域執行目錄查詢，並傳回負責接受指向該網域郵件的主機。

還原預設值

如果您要移除對繞送查詢組態欄位所進行的編輯，並使用預設值加以取代，請按下「**還原預設值**」。

測試電子郵件地址

提供可用來測試及驗證繞送組態的「**測試電子郵件位址**」。

測試查詢	按下**「測試查詢」**，使用提供的測試電子郵件地址來驗證已定義的繞送查詢。 此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不會驗證從連接之掃描程式到 LDAP 伺服器的連線。測試結果僅會反映正在測試中的資料來源。並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

4 按下**「儲存」**返回**「新增目錄資料來源」->「目錄資料來源功能」**頁面。

請參閱第 428 頁的「啟用新資料來源的功能」。

建立和測試自訂位址解析查詢

您可透過將自訂屬性及過濾器架構為符合系統組態來自訂查詢。使用自訂查詢可變更範圍並支援唯一目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

賽門鐵克建議您在部署新資料來源之前，先測試所有查詢。

為新資料來源架構自訂位址解析查詢：

1 在**「目錄整合設定」->「LDAP 伺服器組態」**頁面中，新增資料來源並架構伺服器整合設定，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「新增目錄資料來源」->「目錄資料來源功能」**頁面上，勾選**「位址解析」**，然後按下**「自訂查詢」**。

請參閱第 428 頁的「啟用新資料來源的功能」。

3 提供以下資訊：

基準 DN

提供自訂查詢的**「基準 DN」**。

系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。

自訂查詢起點

如果在**「基準 DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。

您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。**「自訂查詢起點」**可讓您架構查詢，以符合特定需求並更快速地傳回資料。

主要電子郵件屬性

視需要為位址解析查詢提供**「主要電子郵件屬性」**。

查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。

主要電子郵件屬性

在**「主要電子郵件屬性」**欄位中，提供 LDAP 架構中用來儲存查詢之主要電子郵件地址資訊的屬性。

如果您提供多個主要電子郵件屬性，則系統會選取第一個屬性 (根據字母順序) 作為查詢之用的主要屬性。但是，只有針對資料來源功能所定義的主要屬性名稱及別名屬性名稱都相同時，後續的值才會顯示為別名。

如果您指定「proxyAddresses」的主要電子郵件屬性，則目錄資料服務會自動識別前面加上「SMTP:」作為位址的屬性值。您不需要在欄位中指定此字首。

電子郵件別名屬性 (選用)

在**「電子郵件別名屬性」**欄位中，提供 LDAP 架構中用來儲存電子郵件別名位址資訊的屬性。

散布清單物件類別

在**「散布清單物件類別」**欄位中，列出 LDAP 架構中用來識別散布清單項目的物件類別。

子成員資格屬性

在**「子成員資格屬性」**欄位中，提供架構中用來定義群組成員的屬性名稱，並以分號分隔。

如果您未提供子成員資格屬性，則不會展開散布清單及群組。選擇不展開群組有益於提升效能。但是，這同時也表示政策僅可套用至收件者的電子郵件地址，因為不會評估 LDAP 群組成員資格。不過，仍會透過電子郵件別名實施間接政策群組。

還原預設值

按下**「還原預設值」**，可移除對位址解析查詢欄位所進行的編輯，並使用預設值加以取代。

測試電子郵件地址

提供可用來測試和驗證查詢的**「測試電子郵件地址」**。

測試查詢

若要依據資料來源驗證已定義的位址解析查詢，請按下**「測試查詢」**。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

如果查詢成功，則可按下**「測試查詢」**選項旁邊的圖示，以顯示所有查詢結果。此測試會報告與測試電子郵件地址相關聯的所有電子郵件地址及使用者喜好設定。如果收件者是散布清單，則會將此資訊提供給屬於該散布清單的所有使用者。

測試結果僅會反映正在測試中的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

查詢過濾 (選用)

視需要為群組清單查詢提供**「查詢過濾 (選用)」**。

此屬性可說明要搜尋的電子郵件地址或屬性元素，而 Token 則說明用來傳回資料的參數。

例如，對於 SunONE 資料來源而言，您可以使用下列查詢過濾來識別目錄中的所有群組：

```
(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames))
```

如果將此欄位留白，則「新增政策群組」頁面不會列出群組。

群組名稱屬性 (選用)

在**「群組名稱屬性 (選用)」**欄位中，從架構中提供用作所傳回之群組顯示名稱的屬性。會傳回群組的代表範例。

如果此欄位保留空白，則只會依照 DN 名稱將針對關聯政策群組所建立的群組列在**「新增政策群組」**頁面上。

請參閱第 161 頁的「關於政策群組」。

還原預設值

按下**「還原預設值」**，以移除對群組清單查詢組態欄位所進行的編輯，並使用預設值加以取代。

測試查詢

按下**「測試查詢」**，依據控管中心主機上執行的資料來源實例來驗證已定義的群組清單查詢。

測試結果僅會反映所測試的資料來源。此查詢會傳回目錄中找到的群組代表範例，而且是依據控管中心主機上執行之目錄資料服務實例來執行，不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

散布清單次要查詢過濾

將次要過濾套用到散布清單。

此查詢過濾會套用到目錄伺服器中因散布清單展開而取得的散布清單。預設值 **(objectclass=*)** 會導致屬於收件者散布清單之子成員的散布清單被納入到結果集中。不論該散布清單是否已被您在初始搜尋時指定的主要查詢過濾排除，此清單都會存在。

附註：如果您使用尚未由目錄伺服器編排索引的屬性來修改此預設值，可能會造成效能降低。

群組次要查詢過濾 將次要過濾套用至群組。

此查詢過濾會套用到目錄伺服器中因群組成員展開而取得的群組。預設值 **(objectclass=*)** 會導致屬於政策群組成員中列出的群組之子成員的任何群組被納入到結果集中。

附註：如果您使用尚未由目錄伺服器編排索引的屬性來修改此預設值，可能會造成效能降低。

4 按下**「儲存」**返回**「新增目錄資料來源」->「目錄資料來源功能」**頁面。

請參閱第 428 頁的「啟用新資料來源的功能」。

20

管理目錄資料整合

本章包含以下主題：

- 展開散布清單和保留收件者地址
- 修改現有資料來源
- 設定目錄資料快取
- 架構資料來源進階設定
- 安全性最佳實務準則
- 擴充性最佳實務準則
- 改善使用目錄資料服務時的訊息和系統負載
- LDAP 連線疑難排解

展開散布清單和保留收件者地址

您可以展開散布清單以解析位址，並將過濾器政策套用至散布清單中的政策群組成員。您可以保留收件者地址來阻止在執行位址解析和隔離所位址解析時，將別名位址重寫為主要位址。

表 20-1說明如何展開散布清單和保留收件者地址。您可以視需要以任何順序執行這些工作。

表 20-1　　如何展開散布清單和保留收件者地址

工作	說明
熟悉如何展開散布清單和保留收件者地址。	散布清單展開功能可讓您解析位址，並將過濾器政策套用至散布清單中的政策群組成員。保留收件者地址可阻止在執行位址解析和隔離所位址解析時，將別名位址重寫為主要位址。 請參閱第 455 頁的「關於展開散布清單和保留收件者地址」。

工作	說明
啟用或停用散布清單展開。	散布清單展開可讓系統使用您的 LDAP 目錄來解析散布清單中的位址，並較為一致地將過濾器政策套用至政策群組。此欄位預設為啟用。如果您停用此功能，則當散布清單作為政策群組的成員時，您便無法將政策套用至散布清單中的個人。 請參閱第 456 頁的「啟用資料來源的散布清單展開」。
保留收件者位址.	收件者地址保留功能會阻止系統將位址由別名重寫到主要位址，藉以保留位址，通常發生於已啟用位址解析的情況下。啟用此欄位會防止發生此行為，從而影響您的位址解析功能。 請參閱第 456 頁的「保留資料來源的收件者地址」。

關於展開散布清單和保留收件者地址

「啟用散布清單展開」可讓您解析位址，並將過濾器政策套用至散布清單中的政策群組成員。**「保留收件者地址」**可防止在執行位址解析和隔離所位址解析時，將別名重寫為主要。這些設定位於**「管理」>「設定」>「目錄整合」>「目錄整合設定」**頁面。

如果同時勾選**「保留收件者地址」**和**「啟用散布清單展開」**，除非別名屬於單一成員散布清單，否則收件者別名位址會解析為散布清單成員的主要位址，在此情況下，會保留別名位址。

附註：「啟用散布清單展開」適用於散布清單內的成員，但不適用於散布清單本身。若要將政策資訊套用至散布清單和其個別成員，必須新增散布清單別名作為自己的散布清單成員。

請參閱第 456 頁的「啟用資料來源的散布清單展開」。

請參閱第 456 頁的「保留資料來源的收件者地址」。

表 20-2 說明在啟用位址解析時，以**「保留收件者地址」**和**「展開散布清單」**組態組合為基礎的解析輸出。

表 20-2 以收件者地址保留和散布清單展開輸入為基礎的位址解析

輸入類型	保留收件者地址 (預設為停用)	展開散布清單 (預設為啟用)	位址會解析為
使用者的別名位址	已停用	已啟用	使用者的主要位址
散布清單別名位址	已停用	已啟用	散布清單中主要使用者位址的完整清單
使用者的別名位址	已停用	已停用	使用者的主要位址
散布清單別名位址	已停用	已停用	散布清單主要位址

輸入類型	保留收件者地址 (預設為停用)	展開散布清單 (預設為啟用)	位址會解析為
使用者的別名位址	已啟用	已啟用	使用者的別名位址
散布清單別名位址	已啟用	已啟用	散布清單別名
使用者的別名位址	已啟用	已停用	使用者的別名位址
散布清單別名位址	已啟用	已停用	散布清單別名
散布清單主要位址	已啟用	已啟用	散布清單主要

啟用資料來源的散布清單展開

散布清單展開可讓系統使用您的LDAP目錄來解析散布清單中的位址，並較為一致地將過濾器政策套用至政策群組。

此欄位預設為啟用。如果您停用此功能，則當散布清單作為政策群組的成員時，您便無法將政策套用至散布清單中的個人。

如果同時勾選**「保留收件者地址」**及**「啟用散布清單展開」**，則這些功能可能會互相影響進而產生意外的後果。

請參閱第 455 頁的「關於展開散布清單和保留收件者地址」。

請參閱第 461 頁的「編輯資料來源的 LDAP 伺服器組態」。

啟用或停用散布清單展開

1. 按下**「管理」>「設定」>「目錄整合」**。
2. 在**「目錄整合設定」->「目錄資料來源」**頁面中，勾選**「啟用散布清單展開」**以啟用散布清單展開，或取消勾選該方塊以停用散布清單展開。

   系統會提示您**「取消」**或**「變更」**散布清單展開設定。
3. 按下**「變更」**。

   即會啟用或停用所有資料來源中的散布清單展開。

   請參閱第 458 頁的「關於修改現有資料來源」。

保留資料來源的收件者地址

收件者地址保留功能會阻止系統將位址由別名重寫到主要位址，藉以保留位址，通常發生於已啟用位址解析的情況下。啟用此欄位會防止發生此行為，從而影響您的位址解析功能。

如果同時勾選**「保留收件者地址」**及**「啟用散布清單展開」**，則這些功能可能會互相影響進而產生意外的後果。

請參閱第 455 頁的「關於展開散布清單和保留收件者地址」。

請參閱第 456 頁的「啟用資料來源的散布清單展開」。

保留資料來源的收件者地址

1 按下「**管理**」>「**設定**」>「**目錄整合**」。

2 在「**目錄整合設定**」->「**目錄資料來源**」頁面中，勾選「**保留收件者地址**」。系統會提示您「**取消**」或「**變更**」收件者地址保留設定。

3 按下「**變更**」。

請參閱第 458 頁的「關於修改現有資料來源」。

修改現有資料來源

表 20-3 說明您可修改現有資料來源的方式。您可以視需要以任何順序執行這些工作。

表 20-3 修改現有資料來源

工作	說明
深入瞭解變更現有資料來源的影響。	修改儲存的資料來源之前，您應該仔細評估修改可能會對郵件組態所造成的任何意外影響。 請參閱第 458 頁的「關於修改現有資料來源」。
停用儲存的某資料來源，讓系統無法使用該資料來源，而不會遺失組態。	如果之後您需要再次啟用資料來源，則停用資料來源可節省組態時間。如果您想要暫時將該來源離線以進行疑難排解，則停用功能亦十分有用。雖然這些設定都已儲存，但如果日後啟用已停用的資料來源，則會清除並重新建立其快取。 請參閱第 459 頁的「停用或啟用資料來源」。
如果您需要使資料來源或目錄資訊無法供 Symantec Messaging Gateway 使用，可刪除現有資料來源。	修改儲存的資料來源可能會影響或停用現有功能，具體取決於您的現有組態。根據此類組態，您可能也無法刪除某些資料來源。在嘗試刪除資料來源前，請留意此動作可能會對郵件組態造成之任何意外後果。 請參閱第 460 頁的「刪除資料來源」。
編輯現有資料來源。	建立資料來源之後，您就可以修改來源組態、功能及查詢的特定層面。 請參閱第 460 頁的「編輯資料來源」。 部分資料來源編輯作業可包括下列任何一項工作： ■ 請參閱第 461 頁的「編輯資料來源的 LDAP 伺服器組態」。 ■ 請參閱第 463 頁的「啟用或編輯驗證功能」。 ■ 請參閱第 469 頁的「啟用或編輯位址解析功能」。 ■ 請參閱第 472 頁的「啟用或編輯繞送功能」。 ■ 請參閱第 474 頁的「啟用或編輯收件者驗證功能」。 ■ 請參閱第 477 頁的「編輯資料來源的進階設定」。

關於修改現有資料來源

建立資料來源之後，您就可以修改來源組態、功能及查詢的特定層面。 修改儲存的資料來源之前，您應該仔細評估修改可能會對郵件組態所造成的任何意外影響。

編輯資料來源可能會影響您的系統組態，如下所述：

- 停用或刪除某資料來源時，將清除該資料來源的快取。接著會捨棄快取，如果日後啟用或再次新增該資料來源，則會重新填入其快取。
- 如果您於正在處理郵件時，變更查詢或變更會修改查詢結果的任何設定，目錄資料服務會捨棄現有快取，並在收到郵件時建立新的快取。
- 如果您將LDAP設定重新架構為使用不同的目錄類型，查詢資料可能會因無法更新而過期。您必須重新架構所有查詢。 您可以改用**「還原預設值」**選項，使每個啟用的功能根據新目錄類型填入每個查詢的正確預設值。

修改或嘗試修改資料來源而導致功能無法再使用時，可能會對系統造成如下影響：

表 20-4

工作	說明
驗證	■ 停用驗證資料來源會自動停用驗證查詢。 如果針對一般使用者隔離所架構此資料來源，則使用者將無法再登入控管中心並存取一般使用者隔離所。 **「隔離所設定」**頁面中的**「一般使用者隔離所」**欄位處於未勾選狀態，除非資料來源可供使用，否則將無法進行編輯。請參閱第 242 頁的「架構一般使用者隔離所」。 ■ 刪除或停用驗證來源後，便不會再針對該來源進行隔離所位址解析。不會再隔離繫結至單一位址之單一帳戶下的電子郵件。請參閱第 86 頁的「設定無效的收件者處理」。 ■ 停用或刪除 SMTP 驗證來源時，便不會再針對該來源進行 SMTP 驗證。 嘗試透過佇列 (需要 SMTP 驗證) 來傳送郵件的使用者，將無法再進行此動作。
收件者驗證	■ 刪除或停用收件者驗證來源會導致資料來源無法套用無效收件者處理。 您必須針對收件者驗證架構至少一個資料來源，才能棄置或拒絕無效的收件者。 如果您的系統架構為棄置或拒絕，則您將無法刪除最後的收件者驗證資料來源。 請參閱第 86 頁的「設定無效的收件者處理」。 ■ 刪除或停用所有收件者驗證來源，會影響您電子郵件地址搜尋攻擊組態的行為。如果收件者驗證資料來源不止一個，則電子郵件地址搜尋攻擊只會對非本機收件者進行攻擊，這些收件者被視為無效收件者，僅用於統計資料目的。因為沒有可供驗證的目錄資料，所以電子郵件地址搜尋攻擊不會評估本機郵件，系統會嘗試正常傳送所有本機郵件。
位址解析	■ 刪除或停用位址解析來源，會導致無法將別名位址解析為主要位址，同時使得該來源中項目的散布清單無法展開。 ■ **「新增政策群組」**頁面中的選項將不再提供與已刪除或已停用之資料來源關聯的群組。 請參閱第 163 頁的「產生政策群組」。

工作	說明
繞送	如果已啟用的網域與繞送資料來源相關聯，則無法刪除或停用該來源。若要修改或移除該資料來源，必須先使用**「網域」**頁面移除網域關聯性。 請參閱第 71 頁的「新增或編輯網域」。

您可以修改資料來源，如下所述：

- 您可以變更資料來源的 LDAP 資訊。
  請參閱第 461 頁的「編輯資料來源的 LDAP 伺服器組態」。
- 您可以刪除資料來源。
  請參閱第 460 頁的「刪除資料來源」。
- 您可以停用或啟用資料來源。
  請參閱第 459 頁的「停用或啟用資料來源」。
- 您可以修改進階設定資料，例如啟用或停用快取功能、設定 TTL 或 TTL 散播，以及架構用戶端設定。
  請參閱第 477 頁的「編輯資料來源的進階設定」。
- 您可以停用、啟用或修改某個資料來源的控管中心驗證、隔離所位址解析功能或 SMTP 驗證以及相關查詢。
  請參閱第 463 頁的「啟用或編輯驗證功能」。
- 您可以停用、啟用或修改某個資料來源的位址解析功能與查詢。
  請參閱第 469 頁的「啟用或編輯位址解析功能」。
- 您可以停用、啟用或修改某個資料來源的繞送功能與查詢。
  請參閱第 472 頁的「啟用或編輯繞送功能」。
- 您可以停用、啟用或修改某個資料來源的收件者驗證功能與查詢 (包括群組清單查詢)。
  請參閱第 474 頁的「啟用或編輯收件者驗證功能」。
- 您可以啟用或停用某個資料來源的散布清單展開。
  請參閱第 456 頁的「啟用資料來源的散布清單展開」。
- 您可以啟用或停用某個資料來源的收件者地址保留。
  請參閱第 456 頁的「保留資料來源的收件者地址」。

停用或啟用資料來源

您可以停用儲存的某資料來源，讓系統無法使用該資料來源，而不會遺失組態。如果之後您需要再次啟用資料來源，則停用資料來源可節省組態時間。如果您想要暫時將該來源離線以進行疑難排解，則停用功能亦十分有用。雖然這些設定都已儲存，但如果日後啟用已停用的資料來源，則會清除並重新建立其快取。

停用資料來源可能會影響其他功能，具體取決於您的系統組態。受影響的功能可能包括無效的收件者處理、電子郵件地址搜尋攻擊和一般使用者喜好設定。如果有特定功能相依性，則系統不會允許您停用已儲存的來源。

請參閱第 458 頁的「關於修改現有資料來源」。

停用或啟用資料來源

1 按下**「管理」>「設定」>「目錄整合」**。

2 在**「目錄整合設定」->「目錄資料來源」**頁面中，針對想要啟用或停用的資料來源勾選方塊。

3 按下**「停用」**以停用選取的資料來源，或按下**「啟用」**以啟用選取的資料來源。

刪除資料來源

如果您需要使資料來源或目錄資訊無法供 Symantec Messaging Gateway 使用，則可以刪除現有資料來源。

修改儲存的資料來源可能會影響或停用現有功能，具體取決於您的現有組態。根據此類組態，您可能也無法刪除某些資料來源。在嘗試刪除資料來源前，請留意此動作可能會對郵件組態造成之任何意外後果。

請參閱第 458 頁的「關於修改現有資料來源」。

刪除資料來源

1 按下**「管理」>「設定」>「目錄整合」**。

2 在**「目錄整合設定」->「目錄資料來源」**頁面中，勾選您要刪除之資料來源的方塊。

3 按下**「刪除」**。

編輯資料來源

編輯資料來源可能會影響其他功能，這取決於您的系統組態。

如果存在特定功能相依性，系統將不允許您停用所儲存來源或部分來源的已架構功能。

附註：如果您停用某個資料來源的功能，系統不會儲存該功能的設定與查詢組態資訊。如果日後再啟用該功能，就必須重新架構查詢設定。

請參閱第 458 頁的「關於修改現有資料來源」。

編輯資料來源

1 按下**「管理」>「設定」>「目錄整合」**。

2 在**「目錄整合設定」->「目錄資料來源」**頁面中，勾選要修改的資料來源。

3 按下「**編輯**」。

4 按以下其中一個標籤來編輯資料來源設定及組態：

- LDAP 伺服器
  請參閱第 461 頁的「編輯資料來源的 LDAP 伺服器組態」。
- 驗證
  請參閱第 463 頁的「啟用或編輯驗證功能」。
- 收件者驗證
  請參閱第 474 頁的「啟用或編輯收件者驗證功能」。
- 繞送
  請參閱第 472 頁的「啟用或編輯繞送功能」。
- 位址解析
  請參閱第 469 頁的「啟用或編輯位址解析功能」。
- 進階
  請參閱第 477 頁的「編輯資料來源的進階設定」。

編輯資料來源的 LDAP 伺服器組態

如果現有資料來源的 LDAP 伺服器組態發生變更，您必須在 Symantec Messaging Gateway 中更新該資訊。

在修改部署的資料來源之前，請確保先評估所做的變更對任何相關組態或程序可能造成的影響。

影響查詢結果的任何修改都會導致清除並隨後重新建置快取，這可能會使郵件傳送速度變慢。在資料來源開始正式服務之前，可使用測試功能來協助診斷問題。

請參閱第 458 頁的「關於修改現有資料來源」。

編輯資料來源的 LDAP 伺服器組態

1 按下「**管理**」>「**設定**」>「**目錄整合**」。

2 在「**目錄整合設定**」->「**目錄資料來源**」頁面中，勾選要編輯之資料來源的方塊。

3 按下「**編輯**」，然後按下「**LDAP 伺服器**」標籤。

4 您可以編輯下列任一欄位：

欄位	說明
資料來源名稱	您可以編輯資料來源的唯一名稱。

欄位	說明
目錄類型	您可以變更 LDAP 來源所使用的目錄類型。如果變更已儲存資料來源的目錄類型，您的查詢預設值並不會隨之更新。您必須對查詢個別進行重新架構，或對每個功能使用**「還原預設值」**選項。 可用選項如下： ■ Active Directory ■ Active Directory 通用類別目錄 ■ iPlanet/Sun ONE/Java Directory Server ■ Domino ■ 其他 (可以是 LDAPv3 相容的任何目錄類型) 雖然 Symantec Messaging Gateway 與任何 LDAPv3 目錄皆相容，但它的設計目的是專門支援使用所列四種特定目錄類型的組態。如果您選取「其他」作為目錄類型，請查閱目錄文件以取得詳細資訊。 如果您使用「Active Directory 通用類別目錄」，則可能會發生驗證問題，這取決於您的查詢組態。複寫通用類別目錄即可解決這些問題。
主機名稱	修改 LDAP 伺服器的主機名稱或 IP 位址。
通訊埠	修改用來存取 LDAP 伺服器的 TCP/IP 通訊埠。
啟用 SSL	啟用或停用至 LDAP 伺服器主機之所有連線上的 SSL。修改此欄位時，請確認您的通訊埠設定。
匿名繫結	勾選此選項可讓目錄資料服務連線至 LDAP 伺服器，而不必提供特定的使用者 ID 和密碼資訊。
使用下列項目	如果您要架構特定的登入憑證，以對LDAP伺服器進行驗證，請勾選此選項。
名稱 (繫結 DN)	用於對 LDAP 伺服器進行驗證的辨別名稱 (DN)。 **附註：** 對於 Active Directory 或通用類別目錄伺服器，您可以選擇性使用完整 DN、NetBIOS 和登入名稱 (NetBIOS\SAM 帳戶名稱) 或使用者主要名稱。
密碼	用於對 LDAP 伺服器進行驗證的密碼。如果勾選**「使用下列項目」**，則必須填寫密碼。

5 編輯所需欄位完成時，按下**「測試登入」**以連線至用戶端，並確保LDAP連線設定有效。

此測試僅確認是否可連線至LDAP伺服器，以及提供的帳戶是否具有目錄伺服器上目錄資料樹狀結構之根目錄的讀取權限。測試結果成功，並不保證憑證在目錄中的其他位置也可成功。對於匿名存取而言尤其如此。在部署之前，您應該確認存取權。

6 按下**「儲存」**。

啟用或編輯驗證功能

您可透過將自訂屬性及過濾器架構為符合系統組態來自訂查詢。使用自訂查詢可變更範圍並支援唯一目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

根據系統組態而定，編輯驗證資料來源可能會影響其他功能的作用。如果其他功能與某個驗證來源相關聯，您可能就無法將該驗證來源停用。

請參閱第 458 頁的「關於修改現有資料來源」。

變更資料來源的驗證類型所造成的影響與停用相同。

例如，假設您為針對控管中心驗證啟用的資料來源架構一般使用者隔離所。如果您稍後啟用資料來源的「僅 SMTP 驗證」功能，則會自動停用一般使用者隔離所，因為此功能依賴控管中心驗證。但如果您啟用資料來源的「控管中心和SMTP驗證」功能，則您可啟用SMTP功能，並保留所有以控管中心驗證為基礎的組態。

啟用資料來源進行驗證時，系統可以：

- 驗證一般使用者的「垃圾郵件隔離所」登入資訊。
- 可讓一般使用者依據電子郵件地址來架構個人的「允許的寄件者」清單和「攔截的寄件者」清單 (也需要位址解析)。
- 驗證「垃圾郵件隔離所」中所儲存郵件的電子郵件收件者。
- 可讓一般使用者架構個人語言設定 (也需要位址解析)。
- 驗證使用 SMTP 驗證來傳送郵件的使用者。

請參閱第 437 頁的「關於將驗證功能與資料來源搭配使用」。

請參閱第 458 頁的「關於修改現有資料來源」。

請參閱第 90 頁的「關於使用 SMTP 驗證」。

編輯資料來源的驗證

1. 按下**「管理」>「設定」>「目錄整合」**。
2. 在**「目錄整合設定」->「目錄資料來源」**頁面中，勾選您要編輯的資料來源。
3. 按下**「編輯」**。
4. 按下**「驗證」**標籤。
5. 請勾選**「啟用驗證」**以啟用驗證，或取消勾選該項目，以停止對資料來源進行驗證。

   當您停用某個資料來源的功能，以移除該來源的功能時，系統不會儲存該來源的設定與查詢組態資訊，而且您需要將其重新架構。

6 在下拉式清單中，選取您要針對資料來源架構的驗證類型。

附註：將一個專屬驗證類型編輯為其他驗證類型時，會停用通訊系統中的某些相依功能。如果您不確定變更如何影響系統，賽門鐵克建議您選取「控管中心和 SMTP 驗證」，以保留現有的功能。

僅控管中心驗證	僅驗證一般使用者，以存取隔離所或設定一般使用者喜好設定 (也需要驗證)。 您必須架構控管中心驗證與隔離所位址解析詳細資料。
僅 SMTP 驗證	使用 SMTP 驗證通訊協定，讓遠端使用者傳送郵件，而不需要 VPN 連線。 您必須架構 SMTP 驗證詳細資料。
控管中心和 SMTP 驗證	啟用控管中心和 SMTP 驗證的功能。 您必須架構控管中心驗證、隔離所位址解析及 SMTP 驗證詳細資料。如果您要共用查詢詳細資料，則可勾選**「共用控管中心和 SMTP 驗證查詢詳細資料」**。

7 已選取控管中心及 SMTP 驗證時，如果您想使用相同的查詢詳細資料來進行控管中心和 SMTP 驗證，則可勾選**「共用控管中心和 SMTP 驗證查詢詳細資料」**。

8 如果您已選取**「僅控管中心驗證」**或**「控管中心和 SMTP 驗證」**(但未勾選**「共用控管中心和 SMTP 驗證查詢詳細資料」**) 作為驗證類型，則請提供下列資訊以進行控管中心驗證查詢：

測試使用者名稱	輸入可用來測試並驗證您的驗證組態的使用者名稱。 賽門鐵克建議您使用旨在產生成功結果和失敗結果的多種輸入來確認您的設定。如果測試產生意料之外的結果，請使用**「自訂查詢」**來確認您的設定和目錄資料。
測試密碼	輸入測試使用者名稱的密碼。
測試網域 (選用)	輸入所提供測試憑證的 NetBIOS 網域。 (可選) 您可以指定 NetBIOS 網域以進行驗證查詢測試。如果在資料來源的範圍內，您的**「測試使用者名稱」**不是跨多個網域的唯一名稱，則需要此欄位。只有在您使用 Active Directory 或 Active Directory 通用類別目錄時，才能使用此欄位。

測試查詢

按下此選項可使用提供的測試資訊，來驗證隔離所位址解析查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不會驗證從連接之掃描程式到 LDAP 伺服器的連線。

測試結果僅會反映所測試的資料來源。結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

自訂查詢

按下此選項可顯示自訂查詢欄位。

您可以檢查查詢的預設值，或建立自訂查詢以變更範圍並支援自訂目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

NetBIOS 網域名稱 (選用)

提供系統可用來解析登入不明之 NetBIOS 網域名稱的清單。

此為選用欄位，但是如果符合以下所有情況時，則建議使用：

- 您的目錄類型為 Active Directory 或 Active Directory 通用類別目錄
- 您的目錄使用多個 NetBIOS 網域
- 無法確保使用者名稱的唯一性

基準 DN

提供繞送查詢的**「基準 DN」**。

系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。

自訂查詢起點

如果在**「基準 DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。

您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。**「自訂查詢起點」**可讓您架構查詢，以符合特定需求並更快速地傳回資料。

查詢過濾

視需要提供**「查詢過濾」**以進行驗證查詢。

查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。

主要電子郵件屬性

此欄位與 SMTP 驗證無關， 它是控管中心驗證的必要欄位。

在**「主要電子郵件屬性」**欄位中，鍵入 LDAP 架構中用來儲存驗證查詢之主要電子郵件地址資訊的屬性。

如果您指定 proxyAddresses 的主要電子郵件屬性，則目錄資料服務會自動識別前面加上 SMTP 作為位址的屬性值。您不需要在「主要電子郵件屬性」欄位中指定此字首。

驗證方法

選擇您的**「驗證方法」**。

按下**「簡單繫結」**嘗試藉由使用者提供的密碼來登入。

或者，您可以使用密碼取回，以從資料來源取回密碼，並將它與使用者提供的密碼進行比較。按下**「密碼屬性」**來選擇密碼取回。您可以使用預設密碼屬性，也可以加以變更。

(可選)您可以為密碼取回指定**「預設雜湊類型」**。如果您選擇**「無」**，則目錄資料必須在密碼屬性前面添加表示配置的前置位元 (例如 **{PLAIN}**)。如果您選擇**「純文字」**，則不需要配置前置位元。

若要停用密碼取回，您可以停用驗證來源的快取。您也可以使用**「簡單繫結」**作為驗證方法。

Symantec Messaging Gateway 透過將簡單繫結用於支援的所有 LDAP 目錄類型，支援透過 LDAP 進行 SMTP 驗證。對於透過使用密碼取回之 LDAP 所進行的 SMTP 驗證，所有支援的目錄類型 (Active Directory、Active Directory 通用類別目錄及 Domino 除外) 都受到支援。

隱藏查詢

按下此選項可隱藏自訂查詢欄位。

還原預設值

按下此選項可移除對查詢組態欄位所做的編輯，並使用預設值加以取代。

9 如果您已選取**「僅控管中心驗證」**或**「控管中心和 SMTP 驗證」**作為驗證類型，則請為隔離所位址解析查詢提供下列資訊。您可以勾選**「共用控管中心和 SMTP 驗證查詢詳細資料」**來使用控管中心資訊：

測試電子郵件地址 在**「測試電子郵件地址」**欄位中，鍵入可用來測試和驗證隔離所位址解析組態的位址。賽門鐵克建議使用組合位址 (包含使用者位址、散布清單位址、別名位址及無效位址) 來測試資料來源。

測試查詢 按下**「測試查詢」**以使用提供的測試電子郵件地址來驗證隔離所位址解析查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。

測試結果僅會反映所測試的資料來源。此測試結果並不會提供有關其他資料來源或系統設定 (例如別名與偽裝) 效果的資訊。

自訂查詢 按下此選項可顯示自訂查詢欄位。您可以檢視預設查詢，或自訂查詢以變更範圍並支援自訂目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

查詢過濾 在「隔離所位址解析查詢」下方的**「查詢過濾」**欄位中，視需要輸入隔離所位址解析查詢的自訂過濾器。查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。

散布清單物件類別 在**「散布清單物件類別」**欄位中，鍵入 LDAP 架構中應該用來識別散布清單項目的物件類別。

隱藏查詢 按下此選項可隱藏自訂查詢欄位。

還原預設值 按下此選項可移除對查詢組態欄位所做的編輯，並使用預設值加以取代。

10 如果您已選取**「僅 SMTP 驗證」**或**「控管中心和 SMTP 驗證」**作為驗證類型，請提供下列資訊以進行 SMTP 驗證查詢：

測試使用者名稱

輸入可用來測試並驗證您的驗證組態的使用者名稱。

賽門鐵克建議您使用旨在產生成功結果和失敗結果的多種輸入來確認您的設定。如果測試產生意料之外的結果，請使用**「自訂查詢」**來確認您的設定和目錄資料。

測試密碼

輸入測試使用者名稱的密碼。

測試查詢

按下此選項可使用提供的測試資訊，來驗證隔離所位址解析查詢。

此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不會驗證從連接之掃描程式到 LDAP 伺服器的連線。

測試結果僅會反映所測試的資料來源。並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。

自訂查詢

按下此選項可顯示自訂查詢欄位。建立自訂查詢以變更範圍並支援自訂目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

基準 DN

提供繞送查詢的**「基準 DN」**。

系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。

自訂查詢起點

如果在**「基準 DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。

您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。**「自訂查詢起點」**可讓您架構查詢，以符合特定需求並更快速地傳回資料。

查詢過濾

視需要提供**「查詢過濾」**以進行驗證查詢。

查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。

主要電子郵件屬性 (選用)

此欄位與 SMTP 驗證無關， 它是控管中心驗證的必要欄位。

在**「主要電子郵件屬性」**欄位中，鍵入 LDAP 架構中用來儲存驗證查詢之主要電子郵件地址資訊的屬性。

驗證方法	選擇您的**「驗證方法」**。 按下**「簡單繫結」**嘗試藉由使用者提供的密碼來登入。 或者，您可以使用密碼取回，以從資料來源取回密碼，並將它與使用者提供的密碼進行比較。按下**「密碼屬性」**來選擇密碼取回。您可以使用預設密碼屬性，也可以加以變更。 (可選) 您可以為密碼取回指定**「預設雜湊類型」**。如果您選擇**「無」**，則目錄資料必須在密碼屬性前面添加表示配置的前置位元 (例如 **{PLAIN}**)。如果您選擇**「純文字」**，則不需要配置前置位元。 若要停用密碼取回，您可以停用驗證來源的快取。您也可以使用**「簡單繫結」**作為驗證方法。 Symantec Messaging Gateway 透過將簡單繫結用於支援的所有 LDAP 目錄類型，支援透過 LDAP 進行 SMTP 驗證。對於透過使用密碼取回之 LDAP 所進行的 SMTP 驗證，所有支援的目錄類型 (Active Directory、Active Directory 通用類別目錄及 Domino 除外) 都受到支援。
隱藏查詢	按下此選項可隱藏自訂查詢欄位。
還原預設值	按下此選項可移除對查詢組態欄位所做的編輯，並使用預設值加以取代。

11 按下**「儲存」**。

啟用或編輯位址解析功能

您可透過將自訂屬性及過濾器架構為符合系統組態來自訂查詢。使用自訂查詢可變更範圍並支援唯一目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

根據系統組態而定，編輯或停用已儲存資料來源的位址解析功能，可能會影響其他功能的作用。

請參閱第 458 頁的「關於修改現有資料來源」。

編輯資料來源的位址解析組態

1 按下**「管理」>「設定」>「目錄整合」**。

2 在**「目錄整合設定」->「目錄資料來源」**頁面中，勾選要編輯之資料來源的方塊。

3 按下**「編輯」**。

4 按下**「位址解析」**標籤。

5 您可以編輯下列任一欄位：

項目	說明
資料來源名稱	您可以編輯資料來源的唯一名稱。
啟用位址解析	位址解析功能可解析別名和散布清單資料，讓您使用以LDAP為基礎的群組成員資格來定義政策，以根據每個使用者套用政策。 請參閱第 439 頁的「關於搭配使用位址解析功能與資料來源」。 如果您停用某個資料來源的功能，以移除該來源的功能時，系統不會儲存該來源的設定與查詢組態資訊。如日後再啟用該功能，就必須重新架構此資訊。 請參閱第 458 頁的「關於修改現有資料來源」。
測試電子郵件地址	提供可用來測試和驗證位址解析組態的電子郵件地址。
測試查詢	按下此選項可使用提供的測試電子郵件地址，來測試和驗證已定義的位址解析查詢。 此測試會報告與測試電子郵件地址關聯的所有電子郵件地址、散布清單成員資格及目錄群組成員資格。此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。 如果查詢成功，則可按下**「測試查詢」**選項旁邊的圖示，以顯示所有查詢結果。此測試會報告與測試電子郵件地址相關聯的所有電子郵件地址及使用者喜好設定。如果收件者是散布清單，則會將此資訊提供給與該散布清單相關聯的所有使用者。 測試結果僅會反映正在測試中的資料來源。並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。
自訂查詢	按下此選項可檢視或自訂預設位址解析查詢。建立自訂查詢以變更範圍並支援自訂目錄架構。 請參閱第 440 頁的「關於資料來源查詢」。
基準 DN	指定目錄中要開始搜尋驗證項目的位置名稱。 系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。
自訂查詢起點	如果在**「基準 DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。 您可以自訂基準DN，將搜尋重新聚焦在目錄樹的特定部分。**「自訂查詢起點」**可讓您架構查詢，以符合特定需求並更快速地傳回資料。
查詢過濾	查詢過濾會使用描述特定LDAP查詢語法的屬性和Token，來指示目錄資料服務傳回資料。

項目	說明
主要電子郵件屬性	指定 LDAP 架構中可用來儲存主要電子郵件地址資訊的屬性。 如果您指定 proxyAddresses 的主要電子郵件屬性，則目錄資料服務會自動識別前面加上 SMTP 作為位址的屬性值。您不需要在「**主要電子郵件屬性**」欄位中指定此字首。
電子郵件別名屬性 (選用)	指定 LDAP 架構中可用來儲存電子郵件別名位址資訊的屬性。
散布清單物件類別	列出 LDAP 架構中可用來識別散布清單項目的物件類別。
子成員資格屬性	提供架構中用來定義群組成員的屬性名稱，並以分號分隔。 如果您未提供子成員資格屬性，則不會展開散布清單及群組。此舉可產生效能優勢。但是，這同時也表示政策僅可套用至收件者的電子郵件地址，因為不會評估 LDAP 群組成員資格。不過，仍會透過電子郵件別名實施間接政策群組。
隱藏查詢	按下此選項可隱藏自訂查詢欄位。
還原預設值	按下此選項可移除對查詢組態欄位所做的編輯，並使用預設值加以取代。
測試查詢	按下此選項可使用提供的測試資訊來測試和驗證群組清單查詢。 此測試係針對於控管中心主機執行的目錄資料服務實例來進行，不會驗證從連接之掃描程式到 LDAP 伺服器的連線。 測試結果僅會反映所測試的資料來源。
自訂查詢	按下此選項可建立自訂群組清單查詢。 建立自訂查詢以變更範圍並支援自訂目錄架構。 請參閱第 440 頁的「關於資料來源查詢」。
查詢過濾 (選用)	查詢過濾會定義目錄資料服務用於搜尋目錄中群組的規則。使用標準 LDAP 查詢語法對其進行指定。 例如，對於 SunONE 資料來源而言，您可以使用下列查詢過濾來識別目錄中的所有群組： `(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames))` 如果將此欄位留白，則「新增政策群組」頁面不會列出群組。 請參閱第 161 頁的「關於政策群組」。
群組名稱屬性 (選用)	指定架構中可作為傳回之群組顯示名稱的屬性。 請參閱第 161 頁的「關於政策群組」。
隱藏查詢	按下此選項可隱藏自訂查詢欄位。
還原預設值	按下此選項可移除對查詢組態欄位所做的編輯，並使用預設值加以取代。

項目	說明
散布清單次要查詢過濾	將次要過濾套用到散布清單。 此查詢過濾會套用到目錄伺服器中因散布清單展開而取得的散布清單。預設值 **(objectclass=*)** 會導致屬於收件者散布清單之子成員的散布清單被納入到結果集中。不論該散布清單是否已被您在初始搜尋時指定的主要查詢過濾排除，此清單都會存在。 **附註：**如果您使用尚未由目錄伺服器編排索引的屬性來修改此預設值，可能會造成效能降低。
群組次要查詢過濾	將次要過濾套用至群組。 此查詢過濾會套用到目錄伺服器中因群組成員展開而取得的群組。預設值 **(objectclass=*)** 會導致屬於政策群組成員中列出的群組之子成員的任何群組被納入到結果集中。 **附註：**如果您使用尚未由目錄伺服器編排索引的屬性來修改此預設值，可能會造成效能降低。

6 按下**「儲存」**。

啟用或編輯繞送功能

您可透過將自訂屬性及過濾器架構為符合系統組態來自訂查詢。使用自訂查詢可變更範圍並支援唯一目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

視系統組態而定，編輯已儲存資料來源的繞送功能可能會影響其他功能。

請參閱第 458 頁的「關於修改現有資料來源」。

編輯資料來源的繞送功能

1 按下**「管理」>「設定」>「目錄整合」**。

2 在**「目錄整合設定」->「目錄資料來源」**頁面中，勾選要編輯之資料來源的方塊。

3 按下**「編輯」**。

4 按下**「繞送」**標籤。

5 您可以編輯下列任一欄位：

項目	說明
資料來源名稱	您可以編輯資料來源的唯一名稱。

項目	說明
啟用繞送	繞送功能會使用資料來源提供的資訊，將郵件繞送至位址與網域。 請參閱第 438 頁的「關於搭配使用繞送功能與資料來源」。 您無法刪除與網域相關聯的繞送來源。如果您要停用這類繞送來源，則必須透過**「網域」**頁面來移除關聯性。 當您停用某個資料來源的功能，以移除該來源的功能時，系統不會儲存該來源的設定與查詢組態資訊。如日後再啟用該功能，就必須重新架構此資訊。 請參閱第 458 頁的「關於修改現有資料來源」。
測試電子郵件地址	提供可用來測試和驗證繞送組態的電子郵件地址。
測試查詢	按下此選項可使用提供的測試電子郵件地址，來測試和驗證已定義的繞送查詢。 此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。 測試結果僅會反映所測試的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。
自訂查詢	按下此選項可顯示自訂查詢欄位。 建立自訂查詢以變更範圍並支援自訂目錄架構。 請參閱第 440 頁的「關於資料來源查詢」。
基準 DN	指定目錄中要開始搜尋驗證項目的位置名稱。 系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。
自訂查詢起點	如果在**「基準 DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。 您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。**「自訂查詢起點」**可讓您架構查詢，以符合特定需求並更快速地傳回資料。
查詢過濾	查詢過濾會使用描述特定LDAP查詢語法的屬性和Token，來指示目錄資料服務傳回資料。
替代地址屬性	如果您要啟用每個使用者以目錄為基礎的替代地址繞送，請提供**「替代地址屬性」**。提供替代電子郵件地址屬性後，前往原始使用者的郵件會重新繞送至新的電子郵件地址。 **附註：**若要儲存繞送來源，請提供**「替代地址屬性」**和/或**「替代郵件主機屬性」**。如果您同時架構**「替代地址屬性」**和**「替代郵件主機屬性」**，則目錄資料服務會先解析所有替代電子郵件地址，然後再解析替代郵件主機值。 請參閱第 438 頁的「關於搭配使用繞送功能與資料來源」。

項目	說明
替代郵件主機屬性	如果您要啟用以目錄為基礎的替代郵件主機繞送，請提供**「替代郵件主機屬性」**，此屬性對應於您選取用來儲存此資訊之目錄架構中的屬性。 郵件主機應指定為 IP 位址或完整的主機名稱。您可使用冒號後面接著通訊埠來指定通訊埠，例如「:25」。根據預設，SMTP 通訊協定會使用通訊埠 25 來進行電子郵件傳輸。 您可以使用下列有效屬性： ■ 10.32.100.64 ■ 10.32.100.64:25 ■ myothermailserver.mycompany.com ■ myothermailserver.mycompany.com:25 如果 LDAP 項目有多個替代郵件主機屬性值，則每次有郵件傳送至該收件者時，MTA 就會隨機選取其中一個值來使用。 **附註：**若要儲存繞送來源，請提供**「替代地址屬性」**和/或**「替代郵件主機屬性」**。如果您同時架構**「替代地址屬性」**和**「替代郵件主機屬性」**，則目錄資料服務會先解析所有替代電子郵件地址，然後再解析替代郵件主機值。 請參閱第 438 頁的「關於搭配使用繞送功能與資料來源」。 如需有關目的主機繞送或 MX 查詢之其他繞送方法的資訊，請參閱網域文件。 請參閱第 71 頁的「新增或編輯網域」。
對替代郵件主機執行 MX 查詢	允許對指定的替代郵件主機進行 MX 查詢。
隱藏查詢	按下此選項可隱藏自訂查詢欄位。
還原預設值	按下此選項可移除對查詢組態欄位所做的編輯，並使用預設值加以取代。

6 按下**「儲存」**。

啟用或編輯收件者驗證功能

您可透過將自訂屬性及過濾器架構為符合系統組態來自訂查詢。使用自訂查詢可變更範圍並支援唯一目錄架構。

請參閱第 440 頁的「關於資料來源查詢」。

視系統組態而定，編輯已儲存資料來源的收件者驗證功能可能會影響其他功能。

請參閱第 458 頁的「關於修改現有資料來源」。

編輯資料來源的收件者驗證功能

1 在控管中心內，按下**「管理」>「設定」>「目錄整合」**。

2 在**「目錄整合設定」->「目錄資料來源」**頁面中，勾選要編輯之資料來源的方塊。

3 按下**「編輯」**。

4 按下**「收件者驗證」**標籤。

5 若要啟用資料來源上的收件者驗證，請勾選**「啟用收件者驗證」**。

6 您可以編輯下列任一欄位：

項目	說明
資料來源名稱	您可以編輯資料來源的唯一名稱。
啟用收件者驗證	按下**「啟用收件者驗證」**。 收件者驗證可與 Symantec Messaging Gateway 中的其他功能搭配運作，以協助您識別和管理無效的收件者以及傳送至這些收件者的郵件。 請參閱第 439 頁的「關於透過資料來源使用收件者驗證功能」。 如果您已將無效的收件者處理架構為棄置郵件或拒絕無效收件者，便無法停用或刪除最後一個收件者驗證來源。您必須將無效收件者處理設定為接收所有郵件，才能刪除或停用最後一個收件者驗證來源。 當您停用某個資料來源的功能，以移除該來源的功能時，系統不會儲存該來源的設定與查詢組態資訊。如日後再啟用該功能，就必須重新架構此資訊。 請參閱第 458 頁的「關於修改現有資料來源」。
測試電子郵件地址	輸入可用來測試並驗證收件者驗證組態的電子郵件地址。
測試查詢	按下此選項可使用提供的測試電子郵件地址，來測試並驗證已定義的收件者驗證查詢。 此測試係針對於控管中心主機執行的目錄資料服務實例來進行， 不能用於驗證所附加掃描程式與 LDAP 伺服器之間的連線。 測試結果僅會反映所測試的資料來源。測試結果並不會提供有關其他資料來源或系統設定 (例如別名和偽裝) 效果的資訊。
自訂查詢	按下此選項可顯示自訂查詢欄位。 您可以檢閱預設查詢資訊，或建立自訂收件者驗證查詢以變更範圍並支援自訂目錄架構。 請參閱第 440 頁的「關於資料來源查詢」。
基準 DN	指定目錄中要開始搜尋驗證項目的位置名稱。 系統會提供預設值，選取「自訂」可在**「自訂查詢起點」**欄位中提供自己的值。
自訂查詢起點	如果在**「基準 DN」**欄位中選取「自訂」，請提供**「自訂查詢起點」**。 您可以自訂基準 DN，將搜尋重新聚焦在目錄樹的特定部分。**「自訂查詢起點」**可讓您架構查詢，以符合特定需求並更快速地傳回資料。
查詢過濾	查詢過濾會使用描述特定 LDAP 查詢語法的屬性和 Token，來指示目錄資料服務傳回資料。
隱藏查詢	按下此選項可隱藏自訂查詢欄位。

項目	說明
還原預設值	按下此選項可移除對查詢組態欄位所做的編輯，並使用預設值加以取代。

7 按下「**儲存**」。

編輯資料來源的進階設定

在已部署的資料來源上編輯設定時，請謹慎小心，因為變更可能會影響目前的組態和程序。例如，修改快取設定可能會清除快取，而修改轉介尋求則可能會導致轉介無法運作。

請參閱第 481 頁的「關於目錄資料快取」。

請參閱第 458 頁的「關於修改現有資料來源」。

編輯資料來源的進階設定

1 按下「**管理**」>「**設定**」>「**目錄整合**」。

2 在「**目錄整合設定**」->「**目錄資料來源**」頁面中，勾選要編輯之資料來源的方塊。

3 按下「**編輯**」。

4 按下「**進階設定**」標籤。

5 您可以編輯下列任一欄位：

項目	說明
連線數目上限	指定一次可建立的用戶端連線 (繫結作業) 數上限。 如果此欄位設為零，則會關閉連線共用，並針對每個要求建立新連線。
連線數目下限	指定當來源服務第一個要求時，會新增至連線共用的連線數目。 零值表示所建立的連線僅用於服務實際的擱置要求。如果連線的閒置時間長於指定的閒置逾時值，則會釋放這些連線。
連線逾時	指定應該經過多長時間，連線至LDAP伺服器主機的嘗試便會逾時並自動結束。 零值表示用戶端的連線永不逾時 (LDAP 伺服器仍然可以關閉連線)。
閒置逾時	指定用戶端連線自動關閉前，能夠保持閒置狀態的時間長度。 零值表示連線無限期保持閒置，不會關閉 (雖然 LDAP 伺服器也可以關閉連線)。
搜尋逾時	指定目錄資料服務結束作業並顯示部分結果之前，要求/搜尋作業所應執行的時間長度 (以秒為單位)。目錄伺服器可強制使用低於此值的搜尋逾時。
頁面大小	決定查詢成功時傳回的初始項目數上限。 將此值設定得太低會影響效能。頁面大小若超出LDAP伺服器所設定的限制，則會在頁面大小超出該限制時導致作業失敗。此值的預設伺服器端限制視目錄類型而有所不同。若要變更目錄伺服器的這個限制，請參閱目錄伺服器文件。 若要完全停用分頁搜尋，請將此值設為 0。 **附註：** 請確定架構給 LDAP 來源使用之管理憑證的「名稱 (繫結 DN)」，具有足夠的存取權可以略過搜尋限制。
尋求轉介	伺服器可能傳回查詢回應，建議目錄資料服務查詢其他LDAP伺服器。啟用此欄位時，目錄資料服務會在執行查詢時遵循此類轉介。 目錄資料服務會使用相同的繫結憑證，來連線至轉介伺服器。如果所轉介的LDAP伺服器無法辨識相同的繫結憑證，則查詢可能會傳回錯誤。

項目	說明
啟用快取	快取會儲存先前要求中的位址項目資料， 這使得目錄資料服務能夠透過使用此快取資料 (而非查閱 LDAP 伺服器) 更加快速地處理要求。 請參閱第 481 頁的「關於目錄資料快取」。 快取預設為啟用。
快取大小	指定可儲存於快取中的項目數上限。超過快取大小限制時，會刪除最久未使用的項目，以釋放空間給新項目。 您應該根據系統需求與可用記憶體空間來設定快取大小。賽門鐵克建議將此值設為等於或大於環境中的使用者和群組 (包括散布清單、聯絡人和公用資料夾) 的數目。 如果您將快取設為零個項目，則會在將每個新的無效收件者新增至快取時加以修剪。這會造成任何指定時間的總數都是 0。 請參閱第 481 頁的「關於目錄資料快取」。
快取索引大小倍增器	指定與快取相關的電子郵件地址索引大小。此設定允許索引在快取中為每個項目儲存多個別名。例如，倍增器為二表示兩倍的快取大小，每個快取項目允許使用平均兩個別名。
最小快取 TTL	設定快取中項目的存留時間 (TTL) 下限。 達到快取 TTL 時，該快取中的項目會到期，並且會在查詢後重新整理這些項目。快取到期的最小值和最大值可建立一個時間段，在該時間段之後，這些項目將到期並進行重新整理。這樣有助於調整系統的工作量。 若為位址解析來源，則此設定也會決定為政策中使用之 LDAP 群組重新建立成員資格資訊的頻率。 請參閱第 481 頁的「關於目錄資料快取」。
最大快取 TTL	設定快取中項目的存留時間 (TTL) 上限。 達到快取 TTL 時，該快取中的項目會到期，並且會在查詢後重新整理這些項目。快取到期的最小值和最大值可建立一個時間段，在該時間段之後，這些項目將到期並進行重新整理。這樣有助於調整系統的工作量。 請參閱第 481 頁的「關於目錄資料快取」。

項目	說明
無效收件者快取大小	提供可儲存於無效收件者快取的項目數上限。 當目錄資料服務在目錄中找不到項目時，就會將該項目視為無效，然後將其新增至無效收件者快取中。將來查詢項目時，載入時間會縮短，因為目錄資料服務會先檢查快取，然後查詢目錄。 您應該根據系統需求與可用記憶體空間來設定快取大小。如果您將快取設定為 0，則會在將每個無效的收件者新增至快取時加以修剪，造成任何指定時間的總數都是 0。
無效收件者快取 TTL	電子郵件地址項目應該保留在無效收件者快取中的期間。
清除快取	按下此選項可清除所有項目的快取。
還原預設值	按下此選項可還原所有「進階設定」欄位的預設值。

6 按下**「儲存」**。

設定目錄資料快取

您可以根據系統需求與可用記憶體空間來架構適當的目錄資料快取大小。您也可以預先載入目錄資料快取並啟用快取持續性。

表 20-5說明設定目錄資料快取的方式。您可以視需要以任何順序執行這些工作。

表 20-5 設定目錄資料快取

工作	說明
深入瞭解目錄資料快取。	Symantec Messaging Gateway 提供了快取功能，該功能可儲存先前要求中的目錄資料。這使得目錄資料服務能夠透過使用此快取資料 (而非較為耗時的 LDAP 目錄查詢) 更加快速地處理要求。 請參閱第 481 頁的「關於目錄資料快取」。
啟用快取持續性.	每次目錄資料服務因 Symantec Messaging Gateway 關閉或重新開機而停止時，快取持續性會將現有快取儲存到檔案。之後會在重新開機時讀取此快取，以防止快取資料遺失。快取預設為啟用。 請參閱第 481 頁的「啟用快取持續性」。
深入瞭解預先載入目錄資料快取的優點。	如果您有大量的 LDAP 項目，或是 LDAP 連線速度緩慢，您可以預先載入目錄快取，以避免在初始目錄快取建立程序期間於系統中備份郵件。在大多數的情況下，快取預先載入並不必要，因為在正常作業流程期間且系統效能良好狀況下，會逐漸建立快取。 請參閱第 482 頁的「關於預先載入目錄資料快取」。

工作	說明
預先載入資料快取。	快取是在符合系統效能需求的正常作業期間逐漸建立而成。如果系統組態相當複雜或資料來源太大，您就可以預先載入目錄快取，以防止郵件在初始目錄快取建立程序期間，於系統中進行備份。 請參閱第 482 頁的「預先載入資料快取」。

關於目錄資料快取

Symantec Messaging Gateway 提供了快取功能，該功能可儲存先前要求中的目錄資料。這使得目錄資料服務能夠透過使用此快取資料 (而非較為耗時的 LDAP 目錄查詢) 更加快速地處理要求。

預設會啟用快取，在接收和驗證項目之後，會將項目新增至快取。當目錄資料服務收到要求時，它會搜尋所有快取，直到找到收件者或沒有其他快取可供搜尋為止。如果在快取中找不到收件者，目錄資料服務就會接著搜尋資料來源目錄。如果在資料來源中找到收件者，便會將該收件者新增至關聯的快取中。

如果在資料來源中找不到收件者，目錄資料服務就會針對該資料來源將快取項目新增至無效收件者快取中。

請根據系統需求與可用記憶體空間來架構適當的快取大小。賽門鐵克建議將此值設為等於或大於環境中的使用者和群組的數目。 此清單應包括散布清單、聯絡人和公用資料夾。

您可以控制每個快取的層面，如下所述：

- 使用「進階設定」頁面設定快取大小及項目壽命。
  請參閱第 477 頁的「編輯資料來源的進階設定」。
  使用「進階設定」頁面的**「最小 TTL」**(存留時間) 和**「最大 TTL」**設定，找出重新整理頻率與保持病毒資料最新之間的適當平衡點。
- 設定警示，以便在超過快取大小時通知您。
  請參閱第 590 頁的「架構警示」。
- 如果您的目錄非常大或 LDAP 連線速度緩慢，則可預先載入快取，以避免因快取建立程序而導致在郵件佇列中進行備份。
  請參閱第 482 頁的「關於預先載入目錄資料快取」。
- 停用您的快取。 請注意，如果停用快取，則 LDAP 主機將針對每個要求進行查詢。 停用快取會增加處理時間。
  請參閱第 477 頁的「編輯資料來源的進階設定」。

啟用快取持續性

每次目錄資料服務因 Symantec Messaging Gateway 關閉或重新開機而停止時，快取持續性會將現有快取儲存到檔案。之後會在重新開機時讀取此快取，以防止快取資料遺失。快取預設為啟用。

請參閱第 481 頁的「關於目錄資料快取」。

啟用或停用資料來源之快取持續性

1 按下「**管理**」>「**設定**」>「**目錄整合**」。

2 在「**目錄整合設定**」->「**目錄資料來源**」頁面上，勾選「**啟用快取持續性**」以啟用快取持續性，或取消勾選該方塊以停用快取持續性。

系統會提示您「**取消**」或「**變更**」散布清單展開設定。

3 按下「**變更**」。

即會啟用或停用所有資料來源中的快取持續性。

請參閱第 458 頁的「關於修改現有資料來源」。

關於預先載入目錄資料快取

如果您有大量的 LDAP 項目，或是 LDAP 連線速度緩慢，您可以預先載入目錄快取，以避免在初始目錄快取建立程序期間於系統中備份郵件。在大多數的情況下，快取預先載入並不必要，因為在正常作業流程期間且系統效能良好狀況下，會逐漸建立快取。

快取預先載入以每個功能為基礎來執行，並且受下列功能支援：

- 隔離所位址解析
- 收件者驗證
- 繞送
- 位址解析

對於繞送以外的所有功能而言，單一輸入檔案會填入已啟用該功能的所有資料來源。對於繞送，則需要獨立的輸入檔案來填入各個資料來源。

如果您停用某資料來源，則針對該資料來源所啟用之所有功能的快取將遭到清除。如果要建立新資料來源或啟用已停用的資料來源，則必須再次預先載入快取。

請參閱第 482 頁的「預先載入資料快取」。

請參閱第 481 頁的「關於目錄資料快取」。

預先載入資料快取

快取是在符合系統效能需求的正常作業期間逐漸建立而成。如果系統組態相當複雜或資料來源太大，您就可以預先載入目錄快取，以防止郵件在初始目錄快取建立程序期間，於系統中進行備份。

您必須在開始預先載入程序之前，上載所有的輸入檔案。每個匯入檔案都必須包含以新行分隔的電子郵件地址，並使用 ASCII 或 UTF8 編碼。

預先載入資料來源快取

1 選取「**管理**」>「**設定**」>「**目錄整合**」。

2 按下「**預先載入快取**」。

3 在「**預先載入組態和狀態**」頁面中，瀏覽到您要用來預先載入快取的輸入檔案。

此檔案必須包含使用 ASCII 或 UTF 格式的新行分隔電子郵件地址。

4 在「**功能**」欄位中，選取上載檔案所使用的功能。

快取預先載入會以每個功能為基礎來執行，且支援下列已啟用及已架構的功能：隔離所位址解析、收件者驗證、繞送及位址解析。對於繞送以外的所有功能而言，單一輸入檔案會在已啟用該功能的所有資料來源中共用。若要進行繞送，您必須讓資料來源輸入檔案與每個繞送功能產生關聯。

5 按下「**上載**」。

6 繼續上載檔案，直到上載完您要預先載入的所有檔案為止。您必須針對每個功能上載資料來源檔案。如果多個功能共用電子郵件地址清單，那麼您必須為每個功能上載同一個輸入檔案。

7 上載完所有檔案後，請按下「**啟動預先載入**」。

您可以在控管中心重新啟動之前，隨時返回此頁面來檢查狀態。因為頁面會自動重新整理，所以「預先載入完成 %」欄位會顯示每個功能的更新。 您也可以按下「**重新整理**」來手動重新整理狀態。

預先載入狀態顯示如下：

- 進行中
  預先載入程序已開始，但尚未完成。
- 成功完成
  已成功載入所有檔案。
- 已啟動取消
  已啟動取消，但尚未完成。
- 已取消
  已停止檔案載入程序。
- 已失敗
  檔案載入程序失敗。

您可以隨時返回以檢查狀態，直到控管中心重新啟動為止。您也可以參閱控管中心記錄以取得其他資訊。

請參閱第 525 頁的「關於日誌」。

架構資料來源進階設定

除了可在「架構 LDAP 伺服器」頁面中設定 LDAP 伺服器之外，您還可以在「進階設定」欄位進一步調整快取大小與網路設定。

請參閱第 481 頁的「關於目錄資料快取」。

架構資料來源的進階設定

1 在**「目錄整合設定」->「目錄資料來源」**頁面上新增資料來源，然後按**「下一步」**。

請參閱第 426 頁的「新增資料來源」。

2 在**「LDAP 伺服器組態」**頁面上，架構伺服器整合設定，然後按下**「顯示進階設定」**。

3 您可以針對新的資料來源架構下列任一設定。所有欄位皆為選擇性的，且僅在系統具有特殊需求時才需要架構。

項目	說明
連線數目上限	指定一次可建立的用戶端連線 (繫結作業) 數上限。 如果此欄位設為零，則會關閉連線共用，並針對每個要求建立新連線。
連線數目下限	指定當來源服務第一個要求時，會新增至連線共用的連線數目。 零值表示所建立的連線僅用於服務實際的擱置要求。如果所建立連線的閒置時間長於指定的閒置逾時值，則會釋放建立的連線。
連線逾時	指定應該經過多長時間，連線至 LDAP 伺服器主機的嘗試便會逾時並自動結束。 零值表示連線永不逾時 (雖然 LDAP 伺服器也可以關閉連線)。
閒置逾時	指定用戶端連線自動關閉前，能夠保持閒置狀態的時間長度。 零值表示連線無限期保持閒置，不會關閉 (雖然 LDAP 伺服器也可以關閉連線)。
搜尋逾時	指定目錄資料服務結束作業並顯示部分結果之前，要求/搜尋作業所應執行的時間長度 (以秒為單位)。請注意，LDAP 伺服器可強制使用低於此值的搜尋逾時。
頁面大小	決定查詢成功時傳回的初始項目數上限。 將此值設定得太低會影響效能。頁面大小若超出 LDAP 伺服器所設定的限制，則會在頁面大小超出該限制時導致作業失敗。此值的預設伺服器端限制視目錄類型而有所不同。若要變更目錄伺服器的這個限制，請參閱目錄伺服器文件。 若要完全停用分頁搜尋，請將此值設為 0。 **附註：** 請確保所提供的「管理憑證」具有足以略過搜尋限制的存取權。
尋求轉介	處理要求時，伺服器可能會傳回建議目錄資料服務查詢其他 LDAP 伺服器的查詢回應。啟用此欄位時，目錄資料服務會在執行查詢時遵循此類轉介。 目錄資料服務會使用相同的繫結憑證，來連線至所轉介的伺服器。如果所轉介的 LDAP 伺服器無法辨識相同的繫結憑證，則查詢可能會傳回錯誤。

項目	說明
啟用快取	快取會儲存先前要求中的位址項目資料， 快取可讓目錄資料服務使用此快取資料更快速的處理要求，而非直接向 LDAP 伺服器查閱每個查詢。 請參閱第 481 頁的「關於目錄資料快取」。 快取預設為啟用。
快取大小	指定可儲存於快取中的項目數上限。超過快取大小限制時，會刪除最久未使用的項目，以釋放空間給新項目。 您應該根據系統需求與可用記憶體空間來設定快取大小。賽門鐵克建議將此值設為等於或大於環境中的使用者和群組 (包括散布清單、聯絡人和公用資料夾) 的數目。 如果您將快取設為零個項目，則會有效地停用快取功能。
快取索引大小倍增器	指定與快取相關的電子郵件地址索引大小。此設定允許索引在快取中為每個項目儲存多個別名。例如，倍數 2 代表快取大小的兩倍，而每個快取項目平均可擁有兩個別名。 賽門鐵克建議將此值設為等於或大於與使用者相關聯之主要位址和別名位址的平均數目。
最小快取 TTL	設定快取中項目的存留時間 (TTL) 下限。 達到快取 TTL 時，該快取中的項目會到期，並且會在查詢後重新整理這些項目。快取到期的最小值和最大值可建立一個時間段，在該時間段之後，這些項目將到期並進行重新整理。這樣可以確保所有項目都不會同時過期，以幫助調整系統的工作量。 若為位址解析來源，則此設定也會決定為政策中使用之 LDAP 群組重新建立成員資格資訊的頻率。 請參閱第 481 頁的「關於目錄資料快取」。
最大快取 TTL	設定快取中項目的存留時間 (TTL) 上限。 達到快取 TTL 時，該快取中的項目會到期，並且會在查詢後重新整理這些項目。快取到期的最小值和最大值可建立一個時間段，在該時間段之後，這些項目將到期並進行重新整理。這樣可以確保所有項目都不會同時過期，以幫助調整系統的工作量。 請參閱第 481 頁的「關於目錄資料快取」。

項目	說明
無效收件者快取大小	提供可儲存於無效收件者快取的項目數上限。 當目錄資料服務在目錄中找不到項目時，就會將該項目視為無效，然後將其新增至無效收件者快取中。將來查詢項目時，載入時間會縮短，因為目錄資料服務會先檢查快取，然後查詢目錄。 您應該根據系統需求與可用記憶體空間來設定快取大小。如果您將快取設為 0，則會有效地停用快取功能。
無效收件者快取 TTL	提供電子郵件地址項目應該保留在無效收件者快取中的時間長度。

4 若要復原變更，請按下**「還原預設值」**。

系統會還原所有「進階設定」欄位的原始預設值。

5 若要在「LDAP 伺服器組態」頁面中隱藏上述欄位，請按下**「隱藏進階設定」**。

6 完成時，請按**「下一步」**以架構資料來源的功能。

請參閱第 428 頁的「啟用新資料來源的功能」。

安全性最佳實務準則

整合目錄資料服務時，請務必採取適當的預防措施來保護您的目錄系統與資料。

賽門鐵克建議您實作下列某些 (或全部) 項目以增加部署安全性：

- 設定 LDAP 伺服器組態時，勾選 SSL 核取方塊以啟用安全通訊端層功能。
  SSL 可以單獨使用，也可以用來提升密碼雜湊等級以提供更多層保護。賽門鐵克建議您儘可能針對資料來源使用 SSL，並強烈建議針對驗證來源使用 SSL。您可以在設定或編輯資料來源的伺服器組態時，一併啟用 SSL。
  請參閱第 426 頁的「新增資料來源」。
  此外，您必須確保目錄伺服器已經架構為使用 SSL。如需詳細資訊，請洽詢您的目錄管理員或是參閱目錄文件。
- 使用密碼雜湊演算法來保護儲存在目錄伺服器上的密碼。
  雖然雜湊演算法可提供更多保護，但在單獨使用時卻無法為使用者密碼資料提供足夠的安全性，因此請勿用來替代 SSL。為保護傳輸中的使用者名稱與密碼資料，必須針對驗證來源使用 SSL。
- 請針對您的目錄資料來源管理員憑證使用僅限唯讀存取的帳戶。
  可能的話，請避免針對此類帳戶使用匿名繫結。
  請參閱第 426 頁的「新增資料來源」。
  請參閱第 461 頁的「編輯資料來源的 LDAP 伺服器組態」。
- 請使用最基本的存取權來限制您的伺服器存取。

限制存取命名空間、物件類別或特定項目屬性。例如，除了將資料來源的繫結 DN 架構為唯讀存取之外，目錄的存取控制應該只將讀取存取權授予 objectClass 以及電子郵件地址、郵件主機與群組成員所使用的屬性。您可以查詢現有來源的自訂查詢資訊，找到這些屬性名稱。

請參閱第 463 頁的「啟用或編輯驗證功能」。

如需特定目錄建議，請參閱您的目錄文件。

- 如果您的硬體裝置使用兩個 NIC，您可以將其中一個置於內部子網路，並將系統架構為僅使用該 NIC 來傳輸 LDAP 流量。

  此舉可隔離您的 LDAP 伺服器與目錄資料，使其免於遭受來自網際網路的潛在風險威脅。

  請參閱第 59 頁的「修改掃描程式組態」。

擴充性最佳實務準則

若在大型或分散式環境中使用目錄資料服務，請考慮採用下列最佳實務準則以提升系統效能與擴充性：

- 使用目錄資料服務快取功能來增加目錄伺服器上的傳輸量並減少負載。

  您應該根據系統需求與可用記憶體空間來設定快取大小。賽門鐵克建議將此值設為等於或大於環境中的使用者和群組的數目。此數量應該包含散布清單、聯絡人、公用資料夾與任何其他列出可傳送之電子郵件地址或使用者名稱的 LDAP 項目。

  請參閱第 484 頁的「架構資料來源進階設定」。
  請參閱第 477 頁的「編輯資料來源的進階設定」。

- 使用警示設定來管理您的程序與快取。

  「監控交換空間使用率」警示會在交換超出指定的使用率時觸發。使用交換警示可確保系統提供足夠的 RAM 給所有 Symantec Messaging Gateway 程序，包括目錄資料服務快取。此警示的預設觸發值為 60%，可以加以修改以符合您的需求。為提供充分的記憶體以達到更高的部署效能，請將交換空間使用率降至最低或零。賽門鐵克建議您針對此類部署將交換空間警示臨界值設為只有幾個百分比。

  「資料來源快取大小不足」警示可讓您立即瞭解何時需要增加快取大小以支援資料所需。

  請參閱第 590 頁的「架構警示」。

- 使用 Symantec Messaging Gateway 目錄快取預載程式來完成快取建立程序，接著再將您的生產環境之郵件流導向系統。

  在大多數部署環境中，您並不需要預先載入快取，而是藉由充足的系統效能並透過正常的系統活動來逐漸建立快取。不過，在某些包含超大型目錄或緩慢 LDAP 連線的部署環境中，您可以透過預載程式來避免在建立超大型快取時可能會出現的暫時效能問題。

  請在離線狀態下執行此工作 (例如，在系統維護期間)，因為預先載入的快取必須等到程序完成之後才會提供給掃描程式使用。

  請參閱第 482 頁的「關於預先載入目錄資料快取」。

- 使用**「進階設定」**頁面上的**「最小 TTL」**(存留時間) 與**「最大 TTL」**設定，找到快取重新整理頻率與資料最新狀態之間的最佳平衡。

充分分散策略可隨機提供快取項目到期時間，來撫平 LDAP 伺服器上的負載。若重新整理頻率太高，會增加處理時間，但不進行重新整理，又會導致資料陳舊。請與您的目錄管理員合作，決定最適合您系統的重新整理頻率。

請參閱第 481 頁的「關於目錄資料快取」。

請參閱第 484 頁的「架構資料來源進階設定」。

請參閱第 477 頁的「編輯資料來源的進階設定」。

- 關閉散布清單展開功能來提升 Symantec Messaging Gateway 系統效能。

  停用**「散布清單展開」**可以大幅提升郵件傳送傳輸量。不過，一旦停用**「散布清單展開」**，散布清單將無法解析為個別成員以進行政策評估。

  亦即，傳送至散布清單的郵件只會受制於與散布清單本身關聯的政策 (經由電子郵件地址或辨別名稱) 。即使其個別成員相關聯的政策擁有較高的優先度，仍舊不會加以套用。

  請參閱第 456 頁的「啟用資料來源的散布清單展開」。

- 限制 LDAP 群組的數量與大小，以及與您的政策群組關聯的散布清單。

  如果您清除資料來源快取，或是對政策群組或目錄資料來源進行組態變更，Symantec Messaging Gateway 必須從您的目錄重新載入群組資訊。如此一來，您的入埠或離埠郵件佇列會一直成長。

  在大多數部署環境中，此程序只需要幾秒鐘就能完成，即使出現佇列備份，也不用太在意。不過，一旦出現 LDAP 存取緩慢的情況，或是政策群組參照數千個 LDAP 使用者時，就會出現明顯的備份情況。為達到最佳效能，賽門鐵克建議您使用預設群組來實作最常見的行為，並在必要時將特定政策指派給較小的群組。

  請參閱第 163 頁的「產生政策群組」。

- 為提升查詢效能，請將 LDAP 查詢的基底 DN 限制為僅包含資料來源所需的資料。

  查詢的範圍越大，搜尋時間就會越久。進行隔離所位址解析時，低落的查詢效能會導致傳送佇列出現備份情況。低落的位址解析查詢效能會導致入埠或離埠查詢開始備份。

  請參閱第 440 頁的「關於資料來源查詢」。

  如果資料來源使用 Active Directory 通用類別目錄，請記得將目錄資料服務架構為使用通用類別目錄通訊埠 (預設為 3268)，而非使用網域控制器通訊埠 (預設為 389)。

  請參閱第 426 頁的「新增資料來源」。

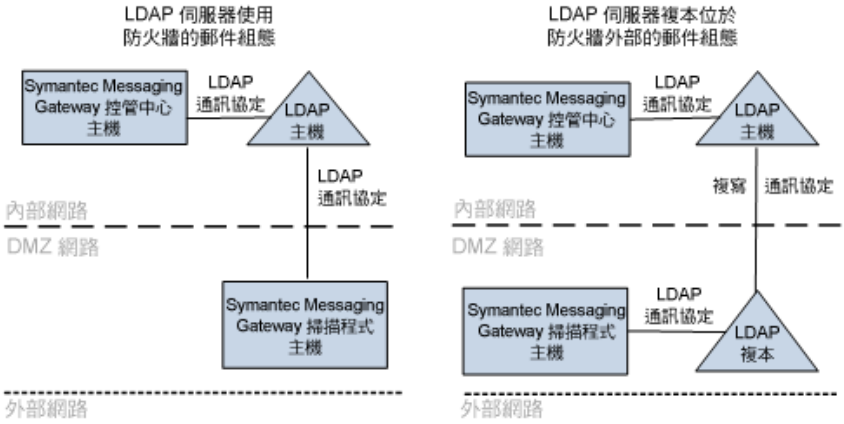
- 針對使用防火牆的 LDAP 伺服器建立唯讀副本，然後將這些副本置於防火牆外部以提升連線效率。

  當環境裡的掃描程式主機位於防火牆外部，且 LDAP 伺服器位於防火牆內部時，您可以在防火牆外部並在網路中鄰近掃描程式的地方設定這些 LDAP 伺服器的複本，以加快連線速度和查詢時間。

  圖 20-1 提供的範例描述使用防火牆的伺服器組態，以及如何使用 LDAP 伺服器複本來提升處理效率。

  您的目錄管理員可以依據系統組態，為此動作決定最佳的途徑。

圖 20-1 使用防火牆的伺服器郵件組態範例



改善使用目錄資料服務時的訊息和系統負載

視您的組態而定，您可能需要採取額外的步驟，以確保達到最佳訊息或負載平衡。嘗試解決負載或訊息問題時，請考慮使用下列組態選項。

- 建立防火牆後的 LDAP 伺服器複本，讓用戶端存取更容易。
  如果組態使用位於防火牆之後的 LDAP 用戶端，您可以設定其 LDAP 伺服器 (靠近位於網路中的掃描程式)的複本來解決連線問題。您的目錄管理員將依據您的組態，為此動作決定最佳的途徑。
- 關閉散布清單展開功能，以加快查詢時間。
  您可以停用散布清單展開來提升效能。如果使用此選項，則無法為個別成員評估散布清單，只能將散布清單當成單一實體來管理。
- 使用子成員資格屬性，以加速查詢時間。
  在查詢中提供父項屬性，可讓用戶端立即確定子項所屬的群組，以及避免查詢目錄。
  Active Directory 預設會提供使用這些屬性的功能。更多可自訂的目錄 (例如 SunOne 或 OpenLDAP)可以展開，以攜帶父和子成員資格屬性。如需詳細資訊，請查閱目錄提供者的文件。
- 使用快取和快取預先載入器，以節省查詢時間。
  若要最佳化效能，請建立會合併所有項目的快取，包括散布清單成員、所有主要使用者及所有別名，然後如果可行則進行預估。

LDAP 連線疑難排解

當目錄資料服務無法與 LDAP 伺服器正常通訊時，使用者驗證和郵件處理可能會受影響。例如，LDAP 伺服器的網路連結可能會中斷，或者資料完整性問題可能會阻礙驗證或位址解析。對郵件處理造成的影響視受影響的目錄資料服務功能而異。

您可能需要與系統管理員聯絡以尋求協助，或者可透過目錄資料服務組態嘗試下列策略。

- 在 Symantec Messaging Gateway 主機與 LDAP 目錄之間使用網路負載平衡器，以在目錄資料的複本之間散佈要求。這可以改善效能，並在其中一部伺服器無法使用時提供容錯移轉。
- 如果未使用網路負載平衡器，目錄資料服務會以循環配置資源的方式在您指派給 LDAP 伺服器的 IP 位址之間循環連線。
- 確保資料來源快取大小與存留時間 (TTL) 值適用於您的部署。如果目錄資料服務無法與 LDAP 伺服器連線，則該快取的結果會很有用，即使該快取項目的 TTL 已到期亦如此。請參閱第 477 頁的「編輯資料來源的進階設定」。

附註：如果 Symantec Messaging Gateway 在 60 秒期間遇到 10 個資料來源存取錯誤，則會將目錄資料來源標記為在 300 秒內無法使用。在這期間，系統會從快取處理所有要求。當向不穩定的 LDAP 伺服器主機發出要求導致產生較長的網路逾時，此動作可減少對郵件傳送的影響。

21

報告

本章包含以下主題：

- 報告總覽
- 選取要為報告追蹤的資料
- 保留、刪除和清除報告資料
- 指定報告匯出設定
- 建立、儲存、以電子郵件傳送和列印報告
- 複製、編輯、排程和刪除我的最愛報告
- 將報告排程為自動產生
- 報告類型
- 疑難排解報告產生問題
- 產生的報告配置與資料

報告總覽

SMG 隨附有 10 個預先定義的報告項目，稱為報告類型。當您建立新報告時，可以選擇一種報告類型開始使用。您可以將 SMG 架構為儲存將新增至您報告的其他資料。請參閱第 498 頁的「報告類型」。中說明了包含在每種報告類型中的資料。

您可以在控管中心內的兩個位置中架構報告。

- 在**「設定」->「報告」**的「管理」標籤下，您可以：
  - 選取要追蹤的其他資料集。請參閱第 493 頁的「選取要為報告追蹤的資料」。
  - 設定保留資料的時間長度，以及何時自動刪除資料和已儲存的報告。請參閱第 493 頁的「保留、刪除和清除報告資料 」。

- 架構匯出設定，例如傳送已完成報告的電子郵件地址，以及已傳送電子郵件的自訂主旨和檔案名稱格式。請參閱第 494 頁的「指定報告匯出設定」。

- 在「報告」標籤下，您可以：
  - 建立、儲存和派送新報告。請參閱第 495 頁的「建立、儲存、以電子郵件傳送和列印報告」。
  - 複製、編輯、排程和刪除我的最愛報告。請參閱第 496 頁的「複製、編輯、排程和刪除我的最愛報告」。
  - 修改配置和報告中的資料 - 請參閱第 510 頁的「產生的報告配置與資料」。
  - 將報告排程為在您需要時執行。請參閱第 497 頁的「將報告排程為自動產生」。

附註：如果您的瀏覽器設為攔截彈出式視窗，則只能在取消攔截彈出式視窗時查看您執行的報告。

選取要為報告追蹤的資料

本節說明如何將 SMG 架構為追蹤並儲存將新增至基本報告的資料。您必須提前 24 小時將 SMG 架構為追蹤並儲存已新增的資料。僅在選取適當的選項時，才會收集擴充統計資料 (例如「最常見的寄件者」、「最常見的寄件者網域」以及「無效收件者」資料)。

選取要為報告追蹤的資料

1. 在控管中心內，按下**「管理」>「設定」>「報告」**。
2. 在**「電子郵件報告資料」**下，勾選要追蹤之報告資料旁的方塊。您可以選取多項。
   - 若要追蹤擴充統計資料，請選取所有的**「寄件者」**相關方塊。
   - 若要檢視**「最常見的探查帳戶」**報告，請選取**「收件者」**，然後啟用**「無效收件者」**。
3. 寄件者統計資料通常會使用大量的磁碟空間。請選擇足夠儲存報告資料的時間長度。

   請參閱第 493 頁的「保留、刪除和清除報告資料 」。
4. 按下**「儲存」**。

一旦選取要追蹤的資料，24 小時之後即可檢視該資料的報告。

請參閱第 495 頁的「建立、儲存、以電子郵件傳送和列印報告」。

保留、刪除和清除報告資料

依據預設，報告和儀表板資料會保留 7 天。如果 SMG 已經有 7 天的資料，則每儲存一小時新的資料，就會刪除最早一小時的資料。您可能想要修改 SMG 保留報告資料的時間長度。

清除資料的操作十分耗費資源，因此，您可能會想將「清除程式」架構為在離峰時間執行。無法擷取已清除的報告資料。

您可以從**「狀態」>「已排程工作」**頁面中，檢查已排程工作的狀態。

您必須具有完整的管理權限或者檢視或修改報告設定的權限。

指定報告資料保留的時間長度

1 在控管中心內，按下**「管理」>「設定」>「報告」**。

2 在**「報告和儀表板清除程式設定」**下，按下**「刪除下列時間以前的資料」**下拉式清單，選取 SMG 保留報告資料的時間長度。

3 按下**「儲存」**。

同時刪除所有報告資料

1 在控管中心內，按下**「管理」>「設定」>「報告」**。

2 在**「立即刪除所有報告和儀表板資料」**旁邊，按下**「立即刪除資料」**移除至今所儲存的所有報告資料。

3 在確認對話方塊中，按下**「確定」**。

指定報告資料的清除時間與頻率

1 在控管中心內，按下**「管理」>「設定」>「報告」**。

2 在**「報告和儀表板清除程式設定」**下，從**「執行清除程式」**下拉式清單中選取清除程式頻率。

3 按下**「清除程式啟動時間」**下拉式清單，並指定清除程式的開始時間。

「小時」下拉式清單使用 24 小時制。預設設定為 03:00:00 A.M。

4 按下**「儲存」**。

指定報告匯出設定

您可以設定預設寄件者電子郵件地址，並自訂透過電子郵件從 SMG 傳送的報告的預設主旨行。您指定的預設寄件者電子郵件地址必須是網域的有效電子郵件地址。

當您安裝 SMG 時，預設電子郵件地址是 ReportAdmin@yourcompany.com。使用者無法回覆預設寄件者電子郵件地址。

報告的預設主旨行包含報告標題和報告範圍日期。您可以指定含有靜態文字和變數組合的自訂主旨行。

預設報告主旨行如下：

依照小時或日的報告	%TITLE% ({yyyy年MM月dd日·a·hh:mm} 到 {yyyy年MM月dd日·a·hh:mm z}) 例如： DailyReport (2008 年 12 月 28 日 12:20 PM 到 2008 年 12 月 29 日 12:20 PM PST)
依照週或月的報告	%TITLE% ({yyyy年MM月dd日} 到 {yyyy年MM月dd日 z}) 例如： MonthlyReport (2008 年 12 月 1 日 到 2009 年 1 月 1 日 PST)

您必須具有完整的管理權限或者檢視或修改報告設定的權限。

指定報告電子郵件通知寄件者和主旨行

1 在控管中心內，按下**「管理」>「設定」>「報告」**。

2 在**「電子郵件來自」**方塊中，輸入想要在報告通知電子郵件上顯示為寄件者的電子郵件地址。

3 如果您想要套用報告電子郵件的自訂主旨行，請勾選**「套用自訂主旨與檔名格式」**。

如果已取消勾選，則會在主旨行中使用預設文字。

4 視需要修改主旨。

5 按下**「儲存」**。

建立、儲存、以電子郵件傳送和列印報告

本節說明如何建立和架構報告，自訂過濾器，以及如何將您的報告儲存至「我的最愛報告」頁面。

您可以在報告的預設資料中新增特定的資料集，例如「最常見的寄件者」、「最常見的寄件者網域」與「無效收件者」。您必須提前 24 小時將 SMG 架構為追蹤並儲存已新增的統計資料。請參閱第 493 頁的「選取要為報告追蹤的資料」。

您必須具有完整的管理權限，才能建立、檢視或修改報告。

建立和產生報告

1 在控管中心內，移至**「報告」>「檢視」>「建立報告」**。

2 在**「報告類型」**下拉式清單中，選取某個報告類別。

3 在「**報告類型**」欄位旁的下拉式清單中，選取某個特定報告。

此步驟不適用於「**執行摘要**」報告。

如果您已參與 Symantec Probe Network，並且想要查看「**最常見的探查帳戶**」報告，請選取「**無效收件者**」>「**最常見的探查帳戶**」。

對於「**垃圾郵件及不想要的郵件**」報告類型，您還可以選取「**垃圾郵件處理**」，前提是您選取下列任何一個值：**最常見的寄件者網域**、**最常見的寄件者**、**最常見的寄件者 Helo 網域**、**最常見的寄件者 IP 連線**、**最常見的收件者網域**、**最常見的收件者**、**特定寄件者**或**特定收件者**。

4 如果您選擇的報告類型對特定元素進行過濾，則會顯示具有該特定元素名稱的新欄位。輸入該元素的準則。

對於依**寄件者名稱**過濾的報告，您可以使用空值的寄件者地址 **<>** 來過濾不含寄件者名稱的郵件。

5 某些報告可讓您從以下下拉式清單中選取：

- **方向**
- **時間範圍**附註：您必須啟用瀏覽器的 JavaScript 才能使用彈出式行事曆。
- **分組方式**
- 如需排列結果的報告，請在「**項目**」方塊中，輸入在「**分組方式**」下拉式清單中所指定的每個時間範圍的最大值。
- 顯示為**圖表**和/或**表格**
- 要顯示在報告中的欄
- **字元集**

6 若要將報告儲存至「我的最愛報告」頁面，請輸入報告名稱，然後按下「**儲存至我的最愛**」。

7 若要產生報告，請按下「**執行**」。

8 當您產生報告時，報告會出現在新的瀏覽器視窗中。從該處，您可以 HTML、CSV 或 PDF 格式儲存報告並透過電子郵件將其傳送到多個收件者。請以逗號、分號或空格分隔多個電子郵件地址。

9 若要列印報告，請在「**報告**」瀏覽器視窗中按下滑鼠右鍵，然後選取「**列印**」。

複製、編輯、排程和刪除我的最愛報告

本節說明如何編輯、複製、刪除和產生我的最愛報告。

您必須具有完整的管理權限或者檢視或修改報告的權限，才能刪除我的最愛報告。

複製我的最愛報告

1 在控管中心內，按下**「報告」>「檢視」>「我的最愛報告」**。

2 在**「報告名稱」**欄中，勾選想要複製之報告旁邊的方塊。

3 按下**「複製」**。

4 按下加上底線之全新複製報告的名稱。

5 視需要變更報告中的值。

6 按下**「儲存」**。

當您複製報告時，新報告的名稱為：<原始報告名稱> 的副本。請為新的報告指定唯一名稱，以協助您記憶報告的範圍。

在我的最愛報告中編輯過濾選項

1 在控管中心內，按下**「報告」>「檢視」>「我的最愛報告」**。

2 在清單中，按下加上底線的報告名稱。

3 視需要變更報告中的值。

4 按下**「儲存」**。

編輯執行我的最愛報告的排程

1 在控管中心內，按下**「報告」>「檢視」>「我的最愛報告」**。

2 勾選要編輯之報告旁的方塊，然後按下**「檢視排程」**。

3 變更設定。

4 按下**「儲存」**。

刪除我的最愛報告

1 在控管中心內，按下**「報告」>「檢視」>「我的最愛報告」**。

2 勾選您要刪除之報告旁的方塊。

3 按下**「刪除」**。

報告刪除後，便無法擷取報告組態。

將報告排程為自動產生

您可以排程我的最愛報告，讓它們在指定的間隔自動執行。排程的報告無法自動儲存到主機電腦。必須將它們以電子郵件傳送到至少一個收件者。

您可以從**「狀態」>「已排程工作」**頁面中，檢查已排程工作的狀態。

您必須具有完整的管理權限或者檢視或修改報告的權限，才能建立自動產生的報告。

將報告排程為自動產生

1 在控管中心內，按下**「報告」>「檢視」>「我的最愛報告」**。

2 勾選要排程之報告旁的方塊，然後按下**「檢視排程」**。

若要取消已排程的報告，請勾選您不想再排程之報告旁的方塊，然後按下**「清除排程」**。

3 在**「排程」**標籤下，設定一天中產生報告的時間。

4 在**「匯出」**標籤下，指定報告的格式。

5 在**「匯出」**標籤下，輸入寄件者和收件者的電子郵件地址。以空格、逗號或分號來分隔多個收件者電子郵件地址。

6 在**「字元集」**下拉式清單中，選取該電子郵件訊息之收件者適用的字元集。

7 按下**「儲存」**。

執行隨選報告

1 建立報告。

請參閱第 495 頁的「建立、儲存、以電子郵件傳送和列印報告」。

2 按下**「執行」**。

報告會出現在另一個瀏覽器視窗中。

附註：如果控管中心出現「彈出式視窗已攔截」訊息，請按下訊息並允許來自 SMG 控管中心的彈出式視窗。

執行隨選已排程報告

1 在控管中心內，按下**「報告」>「檢視」>「我的最愛報告」**。

2 在**「報告名稱」**欄中，勾選想要執行之報告旁邊的方塊。

3 按下**「執行」**。

報告會出現在另一個瀏覽器視窗中。

附註：如果控管中心出現「彈出式視窗已攔截」訊息，請按下訊息並允許來自 SMG 控管中心的彈出式視窗。

報告類型

SMG 隨附有 10 個預先定義的報告項目，稱為報告類型。當您建立新報告時，可以選擇一種報告類型開始使用。本節中的表格說明每種報告類型中包含哪些資訊。每一表格的最後一欄會列出您希望系統追蹤的資料類型。您必須先指定一或多個選項，才能夠產生該報告。

請參閱第 493 頁的「選取要為報告追蹤的資料」。

請參閱第 510 頁的「產生的報告配置與資料」。

表 21-1 摘要報告

報告	說明	必要的資料儲存選項
執行	安全性設定檔的總覽，包括已處理的郵件和威脅總數，以及惡意軟體與內容過濾摘要。	無
內容過濾	影響您組織之內容過濾違規及趨勢的總覽。包括觸發的政策數目，以及觸發政策對已處理郵件總數的百分比。	無
電子郵件訊息	電子郵件訊息威脅計數與威脅類型的概觀。	無
無效收件者	無效收件者資料的總覽。	無
IP 連線	進入您系統之電子郵件的 IP 連線總覽。	無
垃圾郵件及不必要的電子郵件	垃圾郵件和不必要的電子郵件總覽。	無
提交	垃圾郵件提交總覽。	無
惡意軟體	您組織目前惡意軟體威脅的總覽。包括郵件摘要、惡意軟體摘要、可疑惡意軟體結果，以及顯示已知和可能惡意軟體威脅之統計資料的不同表格。	無
威脅防禦	目前會影響您組織的進階威脅總覽。	無
解除	在電子郵件附件中偵測到並移除的潛在惡意內容容器和威脅類型的總覽。	無
無法掃描	總覽無法掃描的電子郵件。	無

表 21-2 說明可用的內容過濾報告。

表 21-2 內容過濾報告

報告	說明	必要的資料儲存選項
摘要	偵測到的內容過濾違規總體摘要。	無
最常見的寄件者網域	偵測到最多符合內容過濾的網域。針對每一個網域，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。	寄件者網域
最常見的寄件者	偵測到最多符合內容過濾的電子郵件地址。針對每一個電子郵件地址，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。	寄件者、寄件者網域

報告	說明	必要的資料儲存選項
最常見的寄件者HELO網域	偵測到最多符合內容過濾的SMTP HELO網域名稱。針對每一個HELO網域，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。指定特定時間範圍內要列出的最大 HELO 網域數。	寄件者 HELO 網域
最常見的寄件者 IP 連線	偵測到最多符合內容過濾的 IP 位址。針對每一個 IP 位址，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。指定特定時間範圍內要列出的最大 IP 位址數。	寄件者 IP 連線
最常見的收件者網域	偵測到多最符合內容過濾的收件者網域。針對每一個收件者網域，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。指定特定時間範圍內要列出的最大收件者網域數。	收件者網域
最常見的收件者	偵測到最多符合內容過濾的電子郵件地址。針對每一個電子郵件地址，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。指定特定時間範圍內要列出的最大電子郵件地址數。	收件者、收件者網域
特定寄件者	從指定的寄件者電子郵件地址所觸發之內容過濾政策的數目。針對每一個群組，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。	寄件者、寄件者網域
特定收件者	從指定的收件者電子郵件地址所觸發之內容過濾政策的數目。針對每一個群組，列出已處理的郵件總數，以及已觸發之內容過濾政策的數量及百分比。	收件者、收件者網域
最常見的政策	最常見的符合內容過濾的名稱、觸發的政策數目，以及觸發政策對已處理郵件總數的百分比。 您可選擇限制特定內容事件資料夾的報告。	無

表 21-3 說明可用的電子郵件訊息報告。

表 21-3 電子郵件訊息報告

報告	說明	必要的資料儲存選項
摘要	以下清單是總體郵件及符合下列項目之過濾器的郵件摘要： ■ 垃圾郵件 ■ 可疑垃圾郵件 ■ 不必要的電子郵件 ■ 攻擊 (電子郵件地址搜尋攻擊、病毒和垃圾郵件攻擊) ■ 攔截的寄件者群組 ■ 病毒 ■ 可疑附件 ■ 病蟲 ■ 惡意軟體 (間諜軟體和廣告軟體) ■ 加密的附件 ■ 內容過濾。 ■ 潛在惡意內容 (解除)	無
自訂	讓您選擇要在報告中顯示的欄。	無
平均郵件大小	以 KB 為單位的郵件平均大小。	無
總體郵件大小	報告中以KB為單位的所有郵件總體大小，以及每個群組的總體大小。	無
郵件數	報告中的所有郵件數量，以及每個群組的數量。	無
收件者數量	報告中的收件者數量，以及每個群組中的收件者數量。郵件中的每一位收件者 (To:、Cc: 及 Bcc) 算一個。	無
最常見的寄件者網域	處理最多郵件的來源網域。針對每一個網域，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。指定特定時間範圍內要列出的最大網域數。	寄件者網域
最常見的寄件者	處理最多郵件的來源電子郵件地址。針對每一個電子郵件地址，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。指定特定時間範圍內要列出的最大電子郵件地址數。	寄件者、寄件者網域
最常見的寄件者HELO網域	處理最多郵件的來源 SMTP HELO 網域名稱。針對每一個 HELO 網域，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。指定特定時間範圍內要列出的最大 HELO 網域數。	寄件者 HELO 網域
最常見的寄件者 IP 連線	處理最多訊息的來源 IP 位址。針對每一個 IP 位址，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。指定特定時間範圍內要列出的最大 IP 位址數。	寄件者 IP 連線

報告	說明	必要的資料儲存選項
最常見的收件者網域	處理最多郵件的收件者網域。針對每一個收件者網域，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。指定特定時間範圍內要列出的最大收件者網域數。	收件者網域
最常見的收件者	處理最多郵件的電子郵件地址。針對每一個電子郵件地址，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。指定特定時間範圍內要列出的最大電子郵件地址數。	收件者、收件者網域
特定寄件者	針對您指定的寄件者電子郵件地址所處理的郵件數量。針對每一個群組，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。	寄件者、寄件者網域
特定收件者	針對您指定的收件者電子郵件地址所處理的郵件數量。針對每一個群組，列出已處理總數，以及惡意軟體、垃圾郵件和不必要的電子郵件數量。	收件者、收件者網域

表 21-4 說明無效收件者報告的可用類型。

表 21-4 無效收件者報告

報告	說明	必要的資料儲存選項
摘要	所有進入您網路的無效收件者電子郵件摘要。	無
最常見的無效收件者	具有最多內送郵件的無效收件者電子郵件地址。	收件者、收件者網域、無效收件者
最常見的探查帳戶	具有最多內送郵件的探查帳戶。	收件者、收件者網域、無效收件者
特定的無效收件者	具有最多內送郵件之特定的無效電子郵件地址。	收件者、收件者網域、無效收件者

表 21-5 說明可用的 IP 連線相關報告。

表 21-5 IP 連線報告

報告	說明	必要的資料儲存選項
信譽摘要	對於進入您網路的郵件之所有良好信譽與不良信譽判斷的摘要。包括「快速通過」與「連線類別」。	寄件者 IP 連線
連線總覽	在連線時間嘗試、接受、拒絕和延遲的連線數目。	寄件者 IP 連線
連線類別摘要	根據連線類別來區分不同連線的摘要。 請參閱第 124 頁的「關於管理閘道的連線負載」。	寄件者 IP 連線

報告	說明	必要的資料儲存選項
最常見的成功連線	偵測到最成功的 SMTP 連線的來源 IP 位址。	寄件者 IP 連線
最常見的失敗連線	偵測到最失敗的 SMTP 連線的來源 IP 位址。	寄件者 IP 連線
最常見的拒絕連線	偵測到最常被拒絕的 SMTP 連線的來源 IP 位址。	寄件者 IP 連線
最常見的病毒攻擊	偵測到最多惡意軟體攻擊的來源 IP 位址。針對每一個 IP 位址，列出已處理的郵件總數，以及惡意軟體攻擊的數量與百分比。	寄件者 IP 連線
最常見的郵件目錄攻擊	偵測到最多電子郵件地址搜尋攻擊的來源 IP 位址。針對每一個 IP 位址，列出已處理的郵件總數，以及電子郵件地址搜尋攻擊的數量與百分比。	寄件者 IP 連線

表 21-6 說明可用的垃圾郵件報告。

表 21-6 垃圾郵件及不必要的電子郵件報告

報告	說明	必要的資料儲存選項
摘要	偵測到的垃圾郵件及不必要的電子郵件 (垃圾郵件、攔截的寄件者、可疑垃圾郵件及不必要的電子郵件) 的總數摘要。此摘要包含由客戶特定垃圾郵件規則集偵測到的郵件。	無
最常見的寄件者網域	偵測到最多垃圾郵件及不必要的電子郵件的來源網域。針對每一個網域，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 指定特定時間範圍內要列出的最大寄件者數量。 從「判斷」功能表指定進行過濾所依據的特定判斷。根據預設，**「判斷」**功能表中列出的所有判斷都會包含在報告中。	寄件者網域
最常見的寄件者	偵測到最多垃圾郵件及不必要的電子郵件的來源電子郵件地址。針對每一個電子郵件地址，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 指定特定時間範圍內要列出的最大電子郵件地址數。 從「判斷」功能表指定進行過濾所依據的判斷。依據預設，**「判斷」**功能表中列出的所有判斷都會包含在報告中。	寄件者、寄件者網域

報告	說明	必要的資料儲存選項
最常見的寄件者HELO網域	偵測到最多垃圾郵件及不必要的電子郵件的來源 SMTP HELO 網域名稱。針對每一個 HELO 網域，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 指定特定時間範圍內要列出的最大 HELO 網域數。 從**「判斷」**功能表指定進行過濾所依據的判斷。依據預設，「判斷」功能表中列出的所有判斷都會包含在報告中。	寄件者 HELO 網域
最常見的寄件者 IP 連線	偵測到最多垃圾郵件及不必要的電子郵件的來源 IP 位址。針對每一個 IP 位址，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 指定特定時間範圍內要列出的最大 IP 位址數。 從**「判斷」**功能表指定進行過濾所依據的判斷。依據預設，「判斷」功能表中列出的所有判斷都會包含在報告中。	寄件者 IP 連線
最常見的收件者網域	偵測到最多垃圾郵件及不必要的電子郵件的收件者網域。針對每一個收件者網域，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 指定特定時間範圍內要列出的最大收件者網域數。 從**「判斷」**功能表指定進行過濾所依據的判斷。依據預設，「判斷」功能表中列出的所有判斷都會包含在報告中。	收件者網域
最常見的收件者	偵測到最多垃圾郵件及不必要的電子郵件的電子郵件地址。針對每一個電子郵件地址，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 指定特定時間範圍內要列出的最大電子郵件地址數。 從**「判斷」**功能表指定進行過濾所依據的判斷。依據預設，「判斷」功能表中列出的所有判斷都會包含在報告中。	收件者、收件者網域
特定寄件者	從您指定的寄件者電子郵件地址所偵測到的垃圾郵件及不必要的電子郵件數量。針對每一個群組，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 從**「判斷」**功能表指定進行過濾所依據的特定判斷。根據預設，「判斷」功能表中列出的所有判斷都會包含在報告中。	寄件者、寄件者網域

報告	說明	必要的資料儲存選項
特定收件者	針對您指定的收件者電子郵件地址所偵測到的垃圾郵件及不必要的電子郵件數量。針對每一個群組，列出垃圾郵件佔處理總數的百分比、處理總數，以及垃圾郵件、可疑垃圾郵件、不必要的電子郵件和攔截的寄件者郵件數量。 從**「判斷」**功能表指定進行過濾所依據的特定判斷。根據預設，「判斷」功能表中列出的所有判斷都會包含在報告中。	收件者、收件者網域
寄件者驗證總覽	已處理的郵件總數，以及已嘗試、未嘗試、成功及失敗的寄件者驗證階段作業數量與百分比。	無
最常見的已嘗試寄件者	偵測到最多寄件者驗證嘗試的來源電子郵件地址。針對每一個電子郵件地址，列出已處理的郵件總數，以及寄件者驗證嘗試數量與百分比。	寄件者
最常見的未嘗試寄件者	偵測到最少寄件者驗證攻擊的來源電子郵件地址。針對每一個電子郵件地址，列出已處理的郵件總數，以及未嘗試的寄件者驗證階段作業數量與百分比。	寄件者
最常見的成功寄件者	偵測到最成功之寄件者驗證嘗試的來源電子郵件地址。針對每一個電子郵件地址，列出已處理的郵件總數，以及成功的寄件者驗證嘗試數量與百分比。	寄件者
最常見的失敗寄件者	偵測到最失敗寄件者驗證嘗試的來源電子郵件地址。針對每一個電子郵件地址，列出已處理的郵件總數，以及失敗的寄件者驗證嘗試數量與百分比。	寄件者
隔離所	已隔離之郵件及隔離所釋放的總數。	無

表 21-7 說明可用的垃圾郵件提交報告。

表 21-7 提交報告

報告	說明	必要的資料儲存選項
摘要	客戶特定垃圾郵件提交的摘要 (此摘要不包含一般垃圾郵件提交)。	無
最常見的提交者	最常針對客戶特定規則集提交垃圾郵件之使用者的電子郵件地址。	無
最常見的管理員提交者	最常針對客戶特定規則集提交垃圾郵件之管理員的電子郵件地址。	無
最常見的被攔截提交者	最常針對客戶特定規則集提交垃圾郵件之被攔截提交者的電子郵件地址。 請參閱第 233 頁的「指定誰能夠提交客戶特定規則的郵件」。	無

報告	說明	必要的資料儲存選項
最常見的一般使用者提交者	最常針對客戶特定規則集提交垃圾郵件之一般使用者的電子郵件地址。	無

附註：無法掃描的郵件不再包括在「惡意軟體」報告中，現在改為使用另外的「無法掃描」報告群組。無法掃描的郵件不再增加到任何「惡意軟體」報告中的計數。

表 21-8 惡意軟體報告

報告	說明	必要的資料儲存選項
摘要	偵測到的惡意軟體實例總數摘要。 **「偵測到威脅」**欄不會以**「已處理郵件」**欄中顯示之郵件總數的百分比來呈現偵測到的威脅。**「偵測到威脅」**欄是其右側所有欄 (病毒、病蟲、惡意軟體、可疑病毒和加密的附件) 的總計。因此，**「偵測到威脅」**欄只會是 100% (如果偵測到任何威脅) 或 0% (如果未偵測到任何威脅)。	無
最常見的寄件者網域	偵測到最多惡意軟體郵件的來源網域。針對每一個網域，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。指定特定時間範圍內要列出的最大寄件者數量。	寄件者網域
最常見的寄件者	偵測到最多惡意軟體郵件的來源電子郵件地址。針對每一個電子郵件地址，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。指定特定時間範圍內要列出的最大電子郵件地址數。	寄件者、寄件者網域
最常見的寄件者 HELO 網域	偵測到最多惡意軟體郵件的來源 SMTP HELO 網域名稱。針對每一個 HELO 網域，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。指定特定時間範圍內要列出的最大 HELO 網域數。	寄件者 HELO 網域
最常見的寄件者 IP 連線	偵測到最多惡意軟體郵件的來源 IP 位址。針對每一個 IP 位址，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。指定特定時間範圍內要列出的最大 IP 位址數。	寄件者 IP 連線
最常見的收件者網域	偵測到最多惡意軟體郵件的收件者網域。針對每一個收件者網域，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。指定特定時間範圍內要列出的最大收件者網域數。	收件者網域
最常見的收件者	偵測到最多惡意軟體郵件的電子郵件地址。針對每一個電子郵件地址，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。指定特定時間範圍內要列出的最大電子郵件地址數。	收件者、收件者網域

報告	說明	必要的資料儲存選項
最常見的病毒和病蟲	偵測到的最常見惡意軟體名稱。針對每一個群組，列出惡意軟體佔處理總數的百分比、惡意軟體佔全部惡意軟體與病蟲的百分比，以及最近一次出現的惡意軟體和病蟲。	無
特定寄件者	從您指定的寄件者電子郵件地址所偵測到的惡意軟體郵件數量。針對每一個群組，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。	寄件者、寄件者網域
特定收件者	針對您指定的收件者電子郵件地址所偵測到的惡意軟體郵件數量。針對每一個群組，列出惡意軟體佔處理總數的百分比、處理總數，以及所有類型之惡意軟體實例的數量。	收件者、收件者網域

表 21-9 說明可用的解除報告。

表 21-9 解除報告

報告	說明	必要的資料儲存選項
摘要	偵測到的內含潛在惡意附件的郵件總數摘要。**「多重威脅」**欄計數僅包括內含兩種以上不同威脅類型(例如，PMC和垃圾郵件)的郵件。包含數種不同類型 PMC 的郵件只能計為一個威脅。	無
最常見的寄件者	偵測到其中附件具有PMC之最多郵件的來源電子郵件地址。針對每一個網域，列出 PMC 佔處理總數的百分比、處理總數，以及 PMC 實例的數量。指定特定時間範圍內要列出的最大寄件者數量。	寄件者、寄件者網域
最常見的寄件者網域	偵測到其中附件具有PMC之最多郵件的來源網域。針對每一個網域，列出 PMC 佔處理總數的百分比、處理總數，以及 PMC 實例的數量。指定特定時間範圍內要列出的最大寄件者數量。	寄件者網域
最常見的寄件者HELO網域	偵測到具有 PMC 之最多郵件的來源 SMTP HELO 網域名稱。針對每一個 HELO 網域，列出 PMC 佔處理總數的百分比、處理總數，以及 PMC 實例的數量。指定特定時間範圍內要列出的最大寄件者數量。指定特定時間範圍內要列出的最大 HELO 網域數。	寄件者 HELO 網域
最常見的寄件者 IP 連線	偵測到具有 PMC 之最多郵件的來源 IP 位址。針對每一個 IP 位址，列出 PMC 佔處理總數的百分比、處理總數，以及 PMC 實例的數量。指定特定時間範圍內要列出的最大 IP 位址數。	寄件者 IP 連線
最常見的收件者	偵測到具有PMC之最多郵件的電子郵件地址。針對每一個電子郵件地址，列出 PMC 佔處理總數的百分比、處理總數，以及 PMC 實例的數量。指定特定時間範圍內要列出的最大電子郵件地址數。	收件者、收件者網域

報告	說明	必要的資料儲存選項
最常見的收件者網域	偵測到具有 PMC 之最多郵件的收件者網域。針對每一個收件者網域，列出 PMC 佔處理總數的百分比、處理總數，以及具有 PMC 之郵件的數量。指定特定時間範圍內要列出的最大收件者網域數。	收件者網域
特定寄件者	從您指定的寄件者電子郵件地址所偵測到具有 PMC 之郵件的數量。針對每一個群組，列出 PMC 佔處理總數的百分比、處理總數，以及具有 PMC 之郵件的數量。	寄件者、寄件者網域
特定收件者	針對您指定的收件者電子郵件地址所偵測到具有 PMC 之郵件的數量。針對每一個群組，列出 PMC 佔處理總數的百分比、處理總數，以及具有 PMC 之郵件的數量。	收件者、收件者網域

表 21-10 說明可用的無法掃描報告。

表 21-10 無法掃描報告

報告	說明	必要的資料儲存選項
摘要	偵測到的無法掃描郵件和附件的總數摘要。 **「偵測到威脅」**欄不會以**「已處理郵件」**欄中顯示之郵件總數的百分比來呈現偵測到的威脅。**「偵測到威脅」**欄是其右側所有欄 (郵件無法掃描的不同原因) 的總計。因此，**「偵測到威脅」**欄只會是 100% (如果偵測到任何威脅) 或 0% (如果未偵測到任何威脅)。	無
最常見的寄件者網域	偵測到最多無法掃描郵件和附件的來源網域。針對每一個網域，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。指定特定時間範圍內要列出的最大寄件者數量。	寄件者網域
最常見的寄件者	偵測到最多無法掃描郵件和附件的來源電子郵件地址。針對每一個電子郵件地址，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。指定特定時間範圍內要列出的最大電子郵件地址數。	寄件者、寄件者網域
最常見的寄件者 HELO 網域	偵測到最多無法掃描郵件和附件的來源 SMTP HELO 網域名稱。針對每一個 HELO 網域，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。指定特定時間範圍內要列出的最大 HELO 網域數。	寄件者 HELO 網域
最常見的寄件者 IP 連線	偵測到最多無法掃描郵件和附件的來源 IP 位址。針對每一個 IP 位址，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。指定特定時間範圍內要列出的最大 IP 位址數。	寄件者 IP 連線

報告	說明	必要的資料儲存選項
最常見的收件者網域	偵測到最多無法掃描郵件和附件的收件者網域。針對每一個收件者網域，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。指定特定時間範圍內要列出的最大收件者網域數。	收件者網域
最常見的收件者	偵測到最多無法掃描郵件和附件的電子郵件地址。針對每一個電子郵件地址，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。指定特定時間範圍內要列出的最大電子郵件地址數。	收件者、收件者網域
特定寄件者	從您指定的寄件者電子郵件地址所偵測到無法掃描郵件和附件的數量。針對每一個群組，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。	寄件者、寄件者網域
特定收件者	針對您指定的收件者電子郵件地址所偵測到無法掃描郵件和附件的數量。針對每一個群組，列出無法掃描佔處理總數的百分比、處理總數，以及無法掃描之郵件的數量。	收件者、收件者網域

疑難排解報告產生問題

表 21-11 列出您在產生報告時可能會發生的問題。

表 21-11 報告產生問題

問題	資訊
指定的報告類型沒有可用資料	SMG 可能不會顯示您所預期的報告，而是顯示下列訊息： `No data is available for the report type and time range specified.` 如果收到此訊息，請確認下列事項： ■ 所指定的過濾器有資料存在。 例如，針對「特定收件者」報告，也許在特定期間內您所指定的收件者位址並未收到任何電子郵件。 ■ SMG 已架構為保留該報告類型的資料。 有些報告需要先啟用報告資料，才能執行。 請參閱第 493 頁的「選取要為報告追蹤的資料」。 有時候，即使目前沒有啟用資料收集，仍然可以產生報告。如果您過去曾經啟用資料收集，然後又關閉資料收集，就可能會發生這種情況。收集的資料可以用來產生報告，直到資料過舊而自動清除為止。超過該期間之後，就無法報告產生。在「報告設定」頁面上的「刪除下列時間以前的資料」設定，可以控制此保留期限。

問題	資訊
可疑病毒結果中的差異	在「惡意軟體摘要」報告圖表部分的底部附近，有一個稱為「可疑病毒結果」的區段。同一個報告中的表格部分則包含「可疑病毒」欄。可疑病毒結果總數有可能與可疑病毒欄不符。 產生此差異的可能原因為： ■ 只有在郵件與包含「刪除和延遲可疑病毒隔離所中的郵件」或「將郵件保留在可疑病毒隔離所」動作的政策相符時，才會計入可疑病毒結果。 ■ 即使相符的政策可能會對郵件觸發上述其中一個動作，但其他政策仍可能符合郵件，進而獲得優先權。例如，如果某郵件中含有病毒與可疑病毒，且相符的惡意軟體政策是「刪除郵件」，而相符的可疑病毒政策是「將郵件保留在可疑病毒隔離所」，則會刪除該郵件。因為刪除動作的優先權高於「將郵件保留在可疑病毒隔離所」，所以會刪除郵件。
「內容過濾摘要」報告中的資料可能會不一致	依預設，「內容過濾摘要」報告底部會有一個表格，列出一個最常觸發的內容過濾摘要政策。此表格中包含**「已觸發政策」**欄位與**「已建立事件」**欄位。邏輯上，**「已建立事件」**的數目不應超過**「已觸發政策」**的數目。但是，由於不同的資料來源與時機問題，**「已建立事件」**的數目有時可能會超過**「已觸發政策」**的數目。

產生的報告配置與資料

使用下列資訊，可協助您瞭解顯示在您產生之報告中的配置與資料。

表 21-12 提供如何顯示報告的相關資訊。

表 21-12 報告配置

元素	說明
圖表與表格	您可以指定是否要將報告資料顯示在圖表、表格或是兩者中。「執行摘要」報告中無法使用圖表和表格選項。 顯示圖表與表格的報告資料選項如下： ■ 圖表 - 總覽 每一類別的報告資料圖。 此圖表不含列在總覽表格中的摘要資訊 (整個時間週期的總數及平均數)。 ■ 圖表 - 其他 (非總覽) 顯示所選擇的報告類型中，每一項目的長條圖。 摘要報告以外的其他報告在長條圖中最多可以顯示 20 個項目。 ■ 表格 建立報告資料的數字呈現方式。 對於所有報告，表格式報告可列出 20 個以上的項目。 將圖表與表格儲存至檔案的方法，要視報告格式以及是否儲存或以電子郵件傳送報告而定。
列數	任何報告 (包含已排程的報告) 的大小上限都是 1,000 列。如果您遇到此限制，請縮短時間範圍、以較長時間間隔來分組或減少上方項目欄位 (適用於某些報告)。 **附註：**此限制無法架構。 **附註：**如果您要求前 50 個無效收件者的報告，可能會看到下列可忽略的錯誤：*估計的報告大小超過 1000 列。請修改可用的搜尋條件來限制報告大小。例如，減少時間範圍或按間隔來分組。*
報告圖表中的額外橫條	報告圖表會包含目前零星時數本身的長條。此資訊可確保完整呈現所選的時間範圍。此額外長條所代表的資料通常遠少於其餘長條。 請考慮以下範例： ■ 您在星期二下午 2:22 執行了過去 1 小時的報告： ■ 所得到的資料集是從下午 1:00 到下午 2:22。 ■ 資料會依照小時來顯示，分散於兩個長條上。 ■ 您在星期二下午 2:22 執行了過去 24 小時的報告： ■ 所得到的資料是從星期一下午 2:00 到星期二下午 2:22。 ■ 資料會依照小時來顯示，分散於 25 個長條上。
時間範圍	報告統計資料的儲存單位為每小時的 0 分 0 秒至 59 分 59 秒。例如，上午 1:00 至上午 1:59 是一個單位，上午 2:00 至上午 2:59 則是另一個單位。因為此結構的關係，報告將無法以小於一小時的時間範圍顯示，或以小於一小時的間隔分組。

表 21-13 提供資訊以協助您解譯報告中的資訊。

表 21-13 報告資料詳細資料

問題	說明
構成威脅的項目	摘要報告和儀表板包含威脅摘要圖表和表格。威脅是指電子郵件訊息中有害或可能有害的屬性。例如，威脅包括垃圾郵件、惡意軟體和內容過濾政策違規。類似的郵件判斷會歸入威脅類別。
單一威脅、多重威脅及安全郵件	摘要報告和儀表板會將郵件分類為單一威脅、多重威脅和安全郵件。多重威脅郵件包含不止一種威脅。例如，含有垃圾郵件和惡意軟體的郵件，就是多重威脅郵件。安全郵件不含已知的威脅。
郵件與連線計數	硬體裝置採用許多技術來追蹤和過濾電子郵件。其中某些技術必須先在電子郵件連線階段運作，然後才能產生和傳送實際電子郵件訊息。因觸發不良信譽過濾器而導致連線遭拒絕或延遲時，則將該連線計為一封郵件。
可疑病毒郵件的判斷	郵件在繞送至「可疑病毒隔離所」後，重新掃描郵件的結果就不會計入威脅總計數中。但是，重新掃描郵件的結果會顯示在「可疑病毒結果」圖表中。該圖表指示可疑病毒是否已刪除、是否確定為病毒，或者仍在「可疑病毒隔離所」中。

問題	說明
寄件者 HELO 網域或 IP 連線會顯示閘道資訊	如果任何掃描程式接受閘道電腦轉遞的郵件，則 SMTP HELO 名稱就是該閘道電腦的名稱或 IP 位址。IP 連線位址是連線至閘道電腦之電腦的 IP 位址。 受影響的報告如下： ■ 最常見的寄件者 HELO 網域 所有最常見的寄件者 HELO 網域報告都會受到影響 ■ 最常見的寄件者 IP 連線 所有最常見的寄件者 IP 連線報告都會受到影響 ■ 最常見的成功連線 SMTP 報告 ■ 最常見的失敗連線 SMTP 報告 ■ 最常見的拒絕連線 SMTP 報告 判斷 SMG 所用 IP 位址的程序如下： 1 SMG 首先會檢查連線的 IP 位址是否位於內部範圍之外。如果是，則連線的 IP 位址是邏輯 IP 位址。 2 如果連線的 IP 位址位於內部範圍之內，則 SMG 會依序處理所有收到的標頭。SMG 透過將第一個收到的標頭視為目前收到的標頭，來開始此程序。 3 如果目前收到的標頭含有一個 IP 位址，則 SMG 會檢查該位址是否位於內部範圍之外。如果是，則此 IP 位址是邏輯 IP 位址。 4 如果目前收到的標頭含有一個位於內部範圍之內的 IP 位址，則 SMG 會搜尋下一個收到的標頭。 5 當找到下一個收到的標頭時，SMG 會使其成為目前收到的新標頭，然後返回步驟 3 重複此程序。 6 如果不再收到其他標頭，則此鏈將成功結束於內部 IP 位址。SMG 會使用連線的 IP 位址作為邏輯 IP 位址。 7 如果 SMG 因為其中一個收到的標頭包含 0 個或多個 IP 位址，而無法成功依序處理所有收到的標頭，便會將標頭鏈視為中斷。SMG 會報告 IP 位址為 255.255.255.255。
已處理的郵件計數	對於列出已處理郵件數目的報告而言，已處理的郵件數目是以每封郵件為單位來計算，而非以每位收件者為單位。例如，如果單一郵件列出 12 位收件者，則已處理郵件計數會增加 1，而非 12。

問題	說明
如何報告每封郵件的重複判斷	每個電子郵件訊息都可能包含多位收件者和多種威脅。同一封電子郵件訊息中的不同收件者可能會觸發不同的威脅。會發生此情況是因為不同收件者可能屬於不同政策群組。例如，群組 A 中的收件者可能會因為員工資料保護條款而啟用內容過濾，而群組 B 中的收件者則不會。 某些判斷會有相關聯的名稱，以呈現該判斷類型的獨特性。例如，已知病毒可能稱為 W32.Zoltan 或 VBS.Throckmorton。每個具名判斷都會單獨計數。如果在一封郵件中同時發現 W32.Zoltan 和 VBS.Throckmorton 一或多次，則惡意軟體計數會增加 2。郵件會視為多重威脅郵件。 下列判斷具有唯一名稱： ■ 內容過濾政策 ■ 惡意軟體 ■ 病毒 ■ 病蟲 此清單以外的判斷在一封郵件中只算為一次，即使在郵件中出現多次也一樣。例如，在寄給三位收件者的一封郵件中， 加密內容有兩次是針對收件者 A、有兩次是針對收件者 B， 沒有任何一次是針對收件者 C， 則郵件的加密內容總計數是 1， 郵件的惡意軟體威脅計數是 1 (加密內容計為不具唯一名稱的惡意軟體)。如果在郵件中未偵測到其他威脅，則視為單一威脅郵件。 請參閱第 518 頁的「威脅類別元件」。

22

監控 Symantec Messaging Gateway 的狀態

本章包含以下主題：

- 關於監控系統狀態
- 使用儀表板
- 監控主機電腦和服務狀態
- 監控日誌資料
- 監控遠端伺服器上的日誌
- 處理郵件稽核日誌和郵件佇列
- 監控已排程工作

關於監控系統狀態

您可以從控管中心監控 Symantec Messaging Gateway 的狀態。監控產品狀態的能力可讓您掌握最新的產品效能與活動。在某些情況下，您可以使用過濾器自訂狀態資訊，例如指定時間範圍。

表 22-1 以下說明您可以監控的項目。

表 22-1 您可以監控的狀態項目

類別	說明
系統	您可以監控下列系統狀態： ■ 控制面板 檢視「控制面板」，以取得產品狀態與過濾活動在各個時間範圍內的動態檢視。 請參閱第 516 頁的「使用儀表板」。 ■ 主機 您可以監控硬體的狀態及郵件佇列的大小與數量。您也可以檢視已安裝的軟硬體與服務的相關資訊。 請參閱第 520 頁的「檢視硬體的相關資訊」。 請參閱第 522 頁的「軟體和服務狀態定義」。 請參閱第 521 頁的「檢視您的硬體狀態」。 請參閱第 554 頁的「監控郵件佇列大小和數量」。 ■ 日誌 Symantec Messaging Gateway 可記錄控管中心、垃圾郵件隔離所、目錄資料服務與每個掃描程式日誌的相關資訊。您可以檢視這些日誌來監控產品狀態並解決問題。 請參閱第 525 頁的「關於日誌」。
SMTP	您可以監控下列 SMTP 狀態： ■ 郵件稽核日誌 Symantec Messaging Gateway 提供的郵件稽核元件可讓您搜尋郵件，以瞭解發生的事件。您可以檢視郵件稽核日誌，判定掃描程式接受和處理的郵件追蹤記錄。 ■ 郵件佇列 郵件佇列是郵件在到達目的前暫時保留的區域。您可以檢視佇列在任何郵件佇列中的郵件。 請參閱第 550 頁的「關於郵件佇列」。

使用儀表板

「儀表板」頁面會顯示摘要說明 Symantec Messaging Gateway 狀態及郵件過濾活動的圖表及表格。

- 從下拉式功能表中，選取是顯示入埠郵件、離埠郵件還是入埠郵件和離埠郵件的摘要資訊。從其他下拉式功能表中，選取資料的時段。表 22-2 說明 Symantec Messaging Gateway 針對您的選擇顯示的摘要資訊。
- 表 22-3 說明「儀表板」底部的**「系統狀態」**表格，以及 Symantec ThreatCon 層級顯示。

此頁面是您登入控管中心後看到的第一個頁面。若要從其他控管中心頁面返回「儀表板」，請選取**「狀態」>「系統」>「儀表板」**。

表 22-2 「儀表板」摘要資訊

項目	說明
「郵件」圖表	顯示下列類別的郵件計數： ■ **單一威脅郵件**：每個郵件觸發一個違規。 ■ **多重威脅郵件**：每個郵件觸發多個違規。 ■ **安全郵件**：未觸發任何違規。 所有資料皆取決於您在下拉式功能表中指定的時間範圍。
「郵件」表格	針對指定的時間範圍，顯示單一威脅郵件、多重威脅郵件及安全郵件的實際計數和整體郵件數百分比。
「威脅」圖表	針對指定的時間範圍，顯示最常見的郵件判斷估偵測到之威脅總量的比例。
「威脅」表格	列出指定時段內最常見郵件判斷的個別計數及郵件總數百分比。 請參閱第 518 頁的「威脅類別元件」。
「最常見的 5 種病毒」表格	列出在指定的時間範圍內，惡意軟體過濾器偵測到的最普遍的病毒及病蟲。該表格會依頻率列出惡意軟體類型。按下**「詳細資料」**連結可存取威脅系統之病毒的更精細報告。 **附註：「最常見的 5 種病毒」**統計資料和連結的報告不包含來自威脅防禦掃描的資料。
「最常見的 5 個內容過濾政策」表格	列出在指定的時間範圍內，數量最多的內容過濾政策違規 (依頻率排名)。按下**「詳細資料」**可存取最常見之內容過濾問題的更精細資料。

表 22-3 「系統狀態」表格

項目	說明
系統	系統中硬體元件及軟體元件的狀態。這些狀態包括目前軟體版本、所有可由控管中心存取的掃描程式、硬體狀態以及提交服務狀態。 如需各項目的詳細狀態，請按下其相關連結。
授權	您從賽門鐵克購買的授權狀態。 **附註：「授權」**表格會顯示針對功能而授權的所有掃描程式的最舊授權。

項目	說明
定義	可透過 Symantec LiveUpdate 取得之垃圾郵件、客戶特定垃圾郵件及病毒定義的狀態。按下**「病毒定義」**欄位旁的日期，即可存取**「LiveUpdate 設定」**頁面。按下**「客戶特定垃圾郵件定義」**旁的連結即可存取**「客戶特定垃圾郵件提交」**頁面。 **附註：「定義」**顯示針對功能而授權的所有掃描程式的最舊定義。
Symantec ThreatCon 層級	全球威脅漏洞的評比，會在 Symantec DeepSight Threat Management System 中提供。 Symantec ThreatCon 指示器位於「儀表板」左側。

請參閱第 518 頁的「威脅類別元件」。

威脅類別元件

「控制面板」包含數個威脅類別的資料。

表 22-4 列出構成每個威脅類別的判斷條件，這樣您就能更有效地解讀和分析資料。

表 22-4 威脅類別元件

威脅類別	構成每個威脅類別的判斷條件
內容違規	內容違規類別包括下列元件： ■ 一般使用者和管理員定義的語言政策 ■ 一般使用者攔截的寄件者 ■ 本機攔截的寄件者網域 如果已勾選**「新增/編輯電子郵件內容過濾政策」**頁面上的**「在儀表板和報告中追蹤此政策的違規」**，則會將下列內容過濾政策視為威脅： ■ 已觸發內容過濾政策 ■ 已建立事件 ■ 保留的郵件： 　■ 已核准 　■ 已拒絕 　■ 目前已保留 請參閱第 277 頁的「檢視、編輯、新增和管理內容過濾政策」。

威脅類別	構成每個威脅類別的判斷條件
惡意軟體	惡意軟體威脅類別元件如下： ■ 病毒 ■ 病蟲 ■ 惡意軟體 可能的惡意軟體威脅類別元件如下： ■ 可疑病毒 ■ 加密的附件
無效收件者	■ 無效收件者
不良信譽	不良信譽威脅類別元件如下： ■ 電子郵件地址搜尋攻擊 ■ 病毒攻擊 ■ 本機攔截的寄件者 IP ■ 連線類別 ■ 賽門鐵克全域攔截的寄件者 ■ 反向 DNS 驗證失敗 良好信譽威脅類別元件如下： ■ 賽門鐵克全域允許的寄件者 ■ 允許的 IP ■ 快速通過
垃圾郵件及不必要的電子郵件	■ 寄件者驗證失敗 ■ 垃圾郵件 ■ 可疑垃圾郵件 ■ 退回攻擊 ■ 行銷電子郵件 ■ 電子報 ■ 重新導向 URL 內容
無法掃描的郵件和附件	■ 因任何原因而無法掃描是否存在惡意軟體和內容過濾 ■ 因超出限制而無法掃描是否存在惡意軟體和內容過濾 ■ 因其他原因而無法掃描是否存在惡意軟體和內容過濾 ■ 因解除而無法掃描
解除的郵件	解除的附件
威脅防禦 - 進階威脅	Symantec Content Analysis 偵測的進階威脅

請參閱第 516 頁的「使用儀表板」。

監控主機電腦和服務狀態

表 22-5說明您可如何監控主機電腦、軟體和服務。您可以視需要以任何順序執行這些工作。

表 22-5 監控主機電腦和服務狀態

工作	說明
檢視控管中心主機的相關資訊，以及控管中心所管理的每個掃描程式的相關資訊。	某些硬體資訊不適用於利用 VMware 產品所架構的虛擬電腦。有些情況下，不會顯示 Dell 硬體的硬體資訊欄位。 請參閱第 520 頁的「檢視硬體的相關資訊」。
監控控管中心管理之所有掃描程式的硬體狀態。	如果有錯誤條件，有些項目就會以紅色顯示。顯示的狀態根據儲存的資料而定，因此可能已有數分鐘之久。欄中的破折號 (–) 表示該硬體無法使用此資料。 請參閱第 521 頁的「檢視您的硬體狀態」。
檢視安裝在控管中心管理之元件上的軟體版本。	您也可以查看針對每個元件執行的服務的狀態。 請參閱第 521 頁的「檢視軟體和服務的狀態」。
檢視軟體和服務的狀態。	硬體裝置的狀態詳細資料取決於每個硬體裝置的架構方式。您可以將硬體裝置架構為控管中心、掃描程式或兩者。 請參閱第 522 頁的「軟體和服務狀態定義」。

檢視硬體的相關資訊

您可以檢視控管中心主機的相關資訊，以及控管中心所管理的每個掃描程式的相關資訊。某些硬體資訊不適用於利用 VMware 產品所架構的虛擬電腦。有些情況下，不會顯示 Dell 硬體的硬體資訊欄位。

顯示的資訊如下：

- 主機名稱
- 型號
- 處理器類型
- 處理器核心
- Dell 服務標籤
- 總記憶體
- 磁碟

硬體資訊會動態地更新。硬體裝置啟動時，可能無法使用部分資料。

您必須具備完整的管理權限或管理狀態和日誌檢視或修改權限，才能檢視硬體的相關資訊。

請參閱第 521 頁的「檢視您的硬體狀態」。

請參閱第 522 頁的「軟體和服務狀態定義」。

檢視硬體的相關資訊

1 在控管中心內，按下**「狀態」>「系統」>「主機」**。

2 按下**「硬體資訊」**標籤。

檢視您的硬體狀態

您可以監控控管中心管理之所有掃描程式的硬體狀態。如果有錯誤條件，有些項目就會以紅色顯示。顯示的狀態根據儲存的資料而定，因此可能已有數分鐘之久。欄中的破折號 (–) 表示該硬體無法使用此資料。

您必須具備「完整的管理權限」或「管理狀態和日誌」檢視或修改權限，才能檢視硬體的狀態資訊。

請參閱第 522 頁的「軟體和服務狀態定義」。

檢視您的硬體狀態

1 在控管中心內，按下**「狀態」>「系統」>「主機」**。

2 按下**「硬體狀態」**標籤。

3 若要檢視其他的狀態資訊，請按下主機名稱。

當您按下主機名稱時，會從主機讀取資料以提供即時狀態。

檢視軟體和服務的狀態

您可以檢視安裝在控管中心管理之元件上的軟體版本。您也可以查看針對每個元件執行的服務的狀態。

請參閱第 522 頁的「軟體和服務狀態定義」。

如果要啟用或進行任何修改，同一頁面提供了按下連結文字的捷徑。

檢視軟體和服務的狀態

1 在控管中心內，按下**「狀態」>「系統」>「主機」**。

2 按下**「軟體和服務」**標籤。

3 若要檢視有關主機的其他資訊，請按下您要檢查的主機。

按下任何元件旁邊出現的加號，以檢視該元件的其他資訊。

4 若要啟用或修改掃描程式，請按下任何連結文字，以存取**「編輯主機組態」**頁面。

請參閱第 59 頁的「修改掃描程式組態」。

請參閱第 64 頁的「掃描程式服務」。

軟體和服務狀態定義

硬體裝置的狀態詳細資料取決於每個硬體裝置的架構方式。您可以將硬體裝置架構為控管中心、掃描程式或兩者。

表 22-6 說明了控管中心的軟體和服務狀態。

表 22-7 說明了掃描程式的軟體和服務狀態。

請參閱第 521 頁的「檢視軟體和服務的狀態」。

表 22-6 控管中心軟體和服務狀態

項目	說明
控管中心	按下控管中心名稱連結，以取得其他詳細資料。**「服務」**頁面會以樹狀結構模式顯示。按下**「返回服務狀態」**時，該主機的資訊會隨之更新。綠色勾號表示已安裝 Symantec Messaging Gateway 最新版本。黃色驚嘆號 (!) 表示 Symantec Messaging Gateway 已有更新的版本可供使用。紅色 X 表示控管中心版本與掃描程式版本不相同。
版本	目前安裝的 Symantec Messaging Gateway 版本。如果更新的版本可供使用，則此版本會以紅色顯示。
垃圾郵件隔離所	垃圾郵件隔離所含有已隔離的垃圾郵件。您可以搜尋、刪除、排序和釋放已隔離的郵件。
垃圾郵件隔離所磁碟使用量	垃圾郵件隔離所使用的磁碟空間量。
可疑病毒隔離所	可疑病毒隔離所包含可能有病毒的郵件。您可以搜尋、刪除、排序和釋放已隔離的郵件。
可疑病毒隔離所磁碟使用量	可疑病毒隔離所所使用的磁碟空間量。
內容事件資料夾	內容事件資料夾有助於組織、監控及管理觸發內容過濾政策的事件，而政策的動作是在內容事件資料夾中建立事件。
內容資安事端資料夾磁碟使用量	內容過濾隔離所使用的磁碟空間量。
目錄資料服務	LDAP 的狀態會是**「執行中」**或**「已停止」**。

表 22-7 掃描程式軟體和服務狀態

項目	說明
掃描程式	按下掃描程式名稱連結，以取得其他詳細資料。**「服務」**頁面會以樹狀結構模式顯示。按下**「返回服務狀態」**時，該主機的資訊會隨之更新。綠色勾號表示已安裝 Symantec Messaging Gateway 最新版本。黃色驚嘆號 (!) 表示 Symantec Messaging Gateway 已有更新的版本可供使用。紅色 X 表示控管中心版本與掃描程式版本不相同。
版本	目前安裝的 Symantec Messaging Gateway 版本。如果更新的版本可供使用，則此版本會以紅色顯示。
病毒定義	上次更新病毒定義檔的日期。如果病毒定義檔已經過時或最近一次 LiveUpdate 嘗試執行失敗，則日期會以紅色顯示。
掃描程式	掃描程式的狀態會是「已啟用」或「已停用」。
代理程式	代理程式的狀態會是**「執行中」**(黑色) 或**「已停止」**(紅色)。如果代理程式在過去 24 小時內曾當機，則狀態下方會出現底線。將滑鼠放在紅色底線上，就可以檢視過去 24 小時內發生的當機次數。 代理程式會傳輸控管中心與連接且啟用的掃描程式之間的組態資訊。
管道	管道的狀態會是**「執行中」**(黑色) 或**「已停止」**(紅色)。如果管道在過去 24 小時內曾當機，則狀態下方會出現底線。將滑鼠放在紅色底線上，就可以檢視過去 24 小時內發生的當機次數。 透過安全的 HTTPS 檔案傳輸，管道會從賽門鐵克安全機制應變中心擷取全新和更新的過濾器。
目錄資料服務	目錄資料服務的狀態會是**「執行中」**(黑色) 或**「已停止」**(紅色)。如果目錄資料服務在過去 24 小時內曾當機，則狀態下方會出現底線。將滑鼠放在紅色底線上，就可以檢視過去 24 小時內發生的當機次數。 使用目錄資料服務可以將儲存在輕量型目錄存取通訊協定 (LDAP) 目錄中的資訊，用於 Symantec Messaging Gateway 中的功能。
LiveUpdate	LiveUpdate 的狀態會是**「執行中」**(黑色) 或**「已停止」**(紅色)。如果 LiveUpdate 在過去 24 小時內曾當機，則狀態下方會出現底線。將滑鼠放在紅色底線上，就可以檢視過去 24 小時內發生的當機次數。 LiveUpdate 會從賽門鐵克安全機制應變中心自動下載病毒定義檔至掃描程式。
Brightmail 引擎	Brightmail 引擎的狀態會是**「執行中」**(黑色) 或**「已停止」**(紅色)。如果 Brightmail 引擎在過去 24 小時內曾當機，則狀態下方會出現底線。將滑鼠放在紅色底線上，就可以檢視過去 24 小時內發生的當機次數。 Brightmail 引擎會掃描電子郵件和附件是否存在病毒和垃圾郵件，並根據您架構的過濾器政策進行內容過濾。

項目	說明
MTA	郵件傳輸代理程式的狀態會是「**執行中**」(黑色) 或「**已停止**」(紅色)。如果 MTA 在過去 24 小時內曾當機，則狀態下方會出現底線。將滑鼠放在紅色底線上，就可以檢視過去 24 小時內發生的當機次數。 MTA 會將入埠郵件與離埠郵件繞送到 Brightmail 引擎進行處理，並將已過濾的郵件傳送到其內部目的地或 Internet。

監控日誌資料

Symantec Messaging Gateway 可記錄控管中心、垃圾郵件隔離所、目錄資料服務與每個掃描程式日誌的相關資訊。

表 22-8說明您可如何監控此資料。

表 22-8 監控日誌資料

工作	說明
深入瞭解 Symantec Messaging Gateway。	Symantec Messaging Gateway 會保留 Symantec Messaging Gateway 之元件活動的日誌記錄。如果 Symantec Messaging Gateway 的任何部分無法正常運作，您可檢視日誌以調查問題。即使沒有發現任何問題，賽門鐵克仍建議您定期檢視日誌，以檢查元件的狀態。 請參閱第 525 頁的「關於日誌」。
瞭解可使用的日誌類型。	檢視掃描程式可用的日誌類型清單。 請參閱第 526 頁的「日誌類型」。
檢視為控管中心、掃描程式、目錄資料服務和隔離所記錄的事件。	如果 Symantec Messaging Gateway 的任何部分無法正常運作，您可檢視日誌以調查問題。即使沒有發現任何問題，賽門鐵克仍建議您定期檢視日誌，以檢查元件的狀態。 請參閱第 528 頁的「檢視日誌檔」。
您可能會想要定期檢視控管中心錯誤日誌，以疑難排解問題。	所有與控管中心相關的錯誤都會寫入 BrightmailLog.log 檔案中。 請參閱第 529 頁的「檢視控管中心錯誤日誌」。
儲存日誌檔，以協助進行疑難排解。	當您儲存日誌檔時，就可以使用文字編輯器應用程式來檢視和列印該檔案。您也可以以電子郵件傳送此檔案。日誌檔的儲存格式是 .txt。 請參閱第 530 頁的「儲存日誌檔」。

工作	說明
確保您的日誌資料庫未超過上限。	視環境與指定的記錄層級而定，日誌資料庫可能會快速增大到無法管理的大小。為了防止擴增，Symantec Messaging Gateway 提供了控制方法，即指定資料庫大小上限 (預設值為 50 MB)。此外還提供了日誌清除程式公用程式，可清除較舊的日誌，防止資料庫超過設定的限制 (預設設定為「每日」)。使用者也可以建立自訂組態，以符合特定需求或暫時需求。 請參閱第 531 頁的「管理日誌資料庫大小」。
為掃描程式元件指定要儲存的日誌資料量。	您可以設定五種掃描程式記錄層級 (從錯誤層級遞增至偵錯層級)。在錯誤層級之後的每個後續記錄層級包括前面所有記錄層級的日誌資料。 請參閱第 533 頁的「架構記錄層級」。
手動從日誌資料庫刪除日誌。	您可以從控管中心日誌資料庫的**「狀態」>「系統」>「日誌」**頁面上，清除掃描程式日誌檔和目錄資料服務日誌檔。 請參閱第 535 頁的「手動刪除日誌檔」。
瞭解日誌磁碟空間警示的運作方式。	Symantec Messaging Gateway 包括增強的記錄功能，可讓系統管理員啟用在記錄掃描程式上的磁碟空間接近或達到容量時發出警示。達到預設臨界值層級時，系統就會切換至減少或停止記錄模式，然後向指定的管理員傳送電子郵件通知。您需要啟用磁碟空間不足警示，才能收到此通知。 請參閱第 535 頁的「關於記錄磁碟空間警示」。
清除磁碟空間。	檢視清除控管中心與掃描程式硬體裝置上的磁碟空間時可用的選項清單。如果您判斷低磁碟空間可用性目前已經影響到系統效能，請使用下列選項。 請參閱第 536 頁的「清除磁碟空間檢查清單」。

關於日誌

Symantec Messaging Gateway 會保留 Symantec Messaging Gateway 之元件活動的日誌記錄。如果 Symantec Messaging Gateway 的任何部分無法正常運作，您可檢視日誌以調查問題。即使沒有發現任何問題，賽門鐵克仍建議您定期檢視日誌，以檢查元件的狀態。

您可以為您的每個掃描程式指定想要記錄的資訊層級。某些層級會產生大量資料。將記錄層級設定為符合您監控需求的最低層級。預設的警告記錄層級通常是適當的。

您可以在控管中心檢視日誌資料。您可以排序日誌資料、建立日誌報告，以及從資料庫清除日誌檔。您也可以透過指令行介面使用 `cat`、`grep`、`more` 及 `tail` 指令檢視日誌。指令行介面可顯示即時的日誌資料。

請參閱第 528 頁的「檢視日誌檔」。

請參閱第 530 頁的「儲存日誌檔」。

請參閱第 685 頁的more。

除了使用控管中心檢視日誌外，還可將某些掃描程式日誌傳送至遠端伺服器上的 syslog。

請參閱第 538 頁的「將遠端記錄架構為 syslog」。

Symantec Messaging Gateway 可讓您架構日誌資料庫大小，以防止資料庫將硬碟填滿。它還提供了日誌清除程式公用程式，讓您設定在指定的間隔內自動清除。

請參閱第 531 頁的「管理日誌資料庫大小」。

請參閱第 526 頁的「日誌類型」。

在控管中心內，透過以下兩個步驟使掃描程式日誌可供使用： 首先，將內送資料檔案擷取至掃描程式的暫存位置。然後，控管中心會存取該暫存位置，並將資料複製到控管中心日誌資料庫。將日誌資料從掃描程式傳輸至控管中心後，系統就會刪除掃描程式上的日誌資料，以節省磁碟空間。

在某些情況下，掃描程式日誌可能會比控管中心將資料複製到日誌資料庫更快填滿磁碟。若掃描程式磁碟已接近或達到容量，系統會減少或停止記錄，不會再將任何日誌複製到控管中心日誌資料庫。您必須釋放磁碟空間，才能繼續正常的記錄。

請參閱第 535 頁的「關於記錄磁碟空間警示」。

請參閱第 536 頁的「清除磁碟空間檢查清單」。

日誌類型

使用 Symantec Messaging Gateway 日誌可以監控掃描程式、控管中心、目錄資料服務以及垃圾郵件隔離所的事件。

表 22-9 說明掃描程式可用的日誌類型。

表 22-9 掃描程式日誌類型

掃描程式日誌類型	說明
管道	記錄關於下載防垃圾郵件規則和上載統計資料的狀態。
Brightmail 用戶端	記錄關於郵件過濾的狀態。
Brightmail 引擎	記錄 Brightmail 引擎的狀態。
JLU 控制器	記錄關於 Java LiveUpdate 病毒定義的下載狀態。此日誌為對 LiveUpdate 問題進行疑難排解時應使用的主要日誌檔。
JLU 用戶端	JLU 控制器日誌檔的輔助日誌檔，其中記錄關於 Java LiveUpdate 病毒定義下載的狀態。僅在 JLU 控制器日誌檔未包含足夠的資訊來疑難排解問題時，才使用此日誌檔。
MTA	記錄關於傳送和接收電子郵件的狀態。
內容過濾	記錄關於內容過濾的狀態。

表 22-10 說明控管中心主控台可用的日誌類型。

表 22-10 控管中心日誌類型 - 主控台

主控台日誌檔	說明
BrightmailLog.log	記錄關於控管中心互動的狀態。
catalina<date>.log 和 catalina.out	記錄 Tomcat Web 伺服器的狀態。控管中心在 Tomcat 伺服器內執行。這些檔案包含由 Tomcat 伺服器及 Tomcat 內執行之應用程式所產生的訊息。

表 22-11 說明控管中心資料庫可用的日誌類型。

表 22-11 控管中心日誌類型 - 資料庫

資料庫日誌檔	說明
error.log 和 error.log.#.gz	記錄控管中心存取 MySQL 資料庫時發生的所有錯誤。
slow-queries.log 和 slow-queries.log.#.gz	記錄緩慢的 MySQL 查詢。

表 22-12 描述了可用於控管中心事件的日誌類型。

表 22-12 控管中心日誌類型 - 事件

事件日誌檔	說明
Brightmail_Admin_Events.<yyy-mm-dd>.log	記錄在日誌檔名稱所指示的日期內，控管中心內的所有變更。

表 22-13 描述了「垃圾郵件隔離所」可用的日誌。

表 22-13 隔離所日誌

隔離所日誌	說明
釋放	記錄垃圾郵件隔離所釋放之每封郵件的收件者位址、寄件者位址和主旨。同時它也會記錄發出每封郵件的使用者和時間戳記。

表 22-14 描述了目錄資料服務可用的日誌。

表 22-14 目錄資料服務日誌

DDS 日誌	說明
目錄資料服務	記錄關於目錄資料服務的狀態。

請參閱第 525 頁的「關於日誌」。

請參閱第 528 頁的「檢視日誌檔」。

檢視日誌檔

您可以檢視為控管中心、掃描程式、目錄資料服務和隔離所記錄的事件。 如果 Symantec Messaging Gateway 的任何部分無法正常運作，您可檢視日誌以調查問題。即使沒有發現任何問題，賽門鐵克仍建議您定期檢視日誌，以檢查元件的狀態。

指定過濾並按下**「顯示」**時，Symantec Messaging Gateway 會顯示符合該過濾的日誌事件。您必須具有下列其中一種存取層級，才能檢視日誌：

- **完整的管理權限**
- **「管理狀態和日誌」**的**「檢視」**或**「修改」**權限

請參閱第 525 頁的「關於日誌」。

對於掃描程式日誌，可用的日誌資料量取決於您為掃描程式元件設定的記錄層級。例如，若是您將「管道」記錄層級設定為警告，將不會儲存任何日誌資料，也不提供通知、資訊，或偵錯層級事件的任何資料。在**「管理」>「設定」>「日誌」**頁面上，設定掃描程式元件記錄層級。

請參閱第 533 頁的「架構記錄層級」。

控管中心會在錯誤層級掃描程式日誌的說明旁顯示一個問號。按下圖示可顯示包含有關錯誤之更多資訊的網頁。網頁會在新的網頁瀏覽器視窗開啟，並可能指出賽門鐵克尚未發布有關該錯誤的資訊。 賽門鐵克會追蹤錯誤資訊要求，並持續新增錯誤資訊。

表 22-15 列出可以用來檢視特定日誌事件的過濾器選項。

表 22-15 日誌檢視選項

項目	說明
「主機」(下拉式)	從清單選取主機。 此選項僅可用於掃描程式與目錄資料服務日誌。
「嚴重性」(下拉式)	從清單選取嚴重性層級。 此選項僅可用於掃描程式與目錄資料服務日誌。
「時間範圍」(下拉式)	從清單選取時間範圍或建立自訂的時間範圍。 如果最近變更過控管中心的時區，則此變更不會立即反映，但是您需要重新啟動此硬體裝置。
「元件」(下拉式)	選取要檢視其日誌的元件：**「掃描程式」**、**「控管中心」**、**「隔離所」**或**「目錄資料服務」**。
「日誌類型」(下拉式)	從清單選取日誌類型。 請參閱第 526 頁的「日誌類型」。

項目	說明
「記錄動作」(下拉式)	選取要顯示的動作類型：**「系統事件」**、**「攔截動作」**、**「郵件動作」**或**「全部」**。

如果掃描程式日誌中的某字元無法列印或不是 ASCII，系統就會以 \xAB 序列來列印，而非用原本的字元。 其中 AB 是該字元的十六進位值。舉例來說,一個十進位值為 128 的字元就會顯示為 \x80。

由於日誌資訊是動態資訊，因此您可以按下**「顯示」**來隨時重新整理檢視。

請參閱第 530 頁的「儲存日誌檔」。

請參閱第 531 頁的「管理日誌資料庫大小」。

檢視日誌檔

1. 在控管中心內，按下**「狀態」>「系統」>「日誌」**。
2. 在**「過濾器」**下，指定您要檢視之日誌事件的選擇條件。
3. 按下**「顯示」**。

   過濾結果會出現在「日誌」頁面上。

檢視控管中心錯誤日誌

您可能會想要定期檢視控管中心錯誤日誌，以疑難排解問題。所有與控管中心相關的錯誤都會寫入 `BrightmailLog.log` 檔案中。

每個問題都會在錯誤日誌中產生一段文字。例如，當「垃圾郵件隔離所」收到了無法處理的大型郵件時，就會出現以下文字：

```
com.mysql.jdbc.PacketTooBigException:
Packet for query is too large (3595207 > 1048576)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1554)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1540)
at com.mysql.jdbc.MysqlIO.sendCommand(MysqlIO.java:1005)
at com.mysql.jdbc.MysqlIO.sqlQueryDirect(MysqlIO.java:1109)
at com.mysql.jdbc.Connection.execSQL(Connection.java:2030)
at com.mysql.jdbc.PreparedStatement.executeUpdate
(PreparedStatement.java:1750)
at com.mysql.jdbc.PreparedStatement.executeUpdate
(PreparedStatement.java:1596)
at org.apache.commons.dbcp.DelegatingPreparedStatement.executeUpdate
(DelegatingPreparedStatement.java:207)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate
(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate
```

```
(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLTransaction.create
(Unknown Source)
at com.brightmail.bl.bo.impl.SpamManager.create
(Unknown Source)
at com.brightmail.service.smtp.impl.SmtpConsumer.run
 (Unknown Source)
```

請參閱第 525 頁的「關於日誌」。

檢視控管中心錯誤日誌

1. 在控管中心內，按下**「狀態」>「日誌」**。
2. 在**「元件」**下拉式清單中，選取**「控管中心」**。
3. 在「日誌檔」表格中，按下 **BrightmailLog.log**。
4. 開啟日誌檔或將其儲存到本機磁碟中。

儲存日誌檔

Symantec Messaging Gateway 可讓您儲存日誌檔。日誌檔的儲存格式是 .txt。

當您儲存日誌檔時，就可以使用文字編輯器應用程式來檢視和列印該檔案。您也可以以電子郵件傳送此檔案。您必須要有「完整的管理」權限和「管理狀態和日誌」檢視或修改權限，才能儲存日誌檔。

掃描程式日誌檔未含與控管中心日誌類似的個別日誌檔連結。當您儲存掃描程式日誌檔時，此文字檔會包含出現在「控管中心」頁面上的所有詳細日誌項目。控管中心日誌需要您分別儲存想要的日誌檔。

儲存日誌檔

1. 在控管中心內，按下**「狀態」>「系統」>「日誌」**。
2. 建立日誌。
3. 執行下列任一項：

儲存掃描程式日誌檔	按下**「儲存日誌」**。
儲存控管中心日誌	執行下列所有步驟： ■ 在**「日誌檔」**欄中，按下想要儲存的日誌檔。 ■ 在**「檔案下載」**對話方塊中，按下**「儲存」**。

4 在「**另存新檔**」對話方塊中，指定想要儲存檔案的檔案名稱和位置，並按下「**儲存**」。

預設檔案名稱是 LogDetails.txt。

5 在「**下載已完成**」對話方塊中，按下「**關閉**」。

請參閱第 525 頁的「關於日誌」。

請參閱第 528 頁的「檢視日誌檔」。

管理日誌資料庫大小

控管中心日誌資料庫會依排程的間隔，定期從掃描程式取得日誌資料。視環境與指定的記錄層級而定，日誌資料庫可能會快速增大到無法管理的大小。為了防止擴增，Symantec Messaging Gateway 提供了控制方法，即指定資料庫大小上限 (預設值為 50 MB)。此外還提供了日誌清除程式公用程式，可清除較舊的日誌，防止資料庫超過設定的限制 (預設設定為「每日」)。使用者也可以建立自訂組態，以符合特定需求或暫時需求。

附註：於此處指定的設定應考量到所設定的記錄層級。例如，如果記錄層級 (例如「偵錯」層級) 會產生大量的日誌資料，則您可能要暫時增加資料庫大小和記錄清除速率。當您恢復正常的記錄層級時，可以恢復這些設定。

請參閱第 533 頁的「架構記錄層級」。

請參閱第 525 頁的「關於日誌」。

請參閱第 535 頁的「關於記錄磁碟空間警示」。

附註：如果需要，您也可以手動從日誌資料庫清除檔案。

請參閱第 535 頁的「手動刪除日誌檔」。

表 22-16 日誌資料庫大小控管選項

選項	說明
日誌大小上限	指定資料庫日誌的大小上限。 日誌大小上限會在「日誌清除程式」執行時強制執行。在下次「日誌清除程式」程序執行之前，可能會暫時超過日誌大小上限。 預設值為 50 MB。
刪除資料前，所需要儲存日誌資料的天數	指定日誌檔在清除之前保留在資料庫日誌中的天數。 預設值為 7。

選項	說明
日誌清除程式頻率	指定「清除程式」公用程式的執行頻率。 「日誌清除程式」會刪除較舊的日誌檔，以強制執行日誌大小上限。 預設設定是「每天」。
日誌清除程式開始時間	指定「清除程式」的開始時間。 此時間是 24 時制。例如，23:00 就是下午 11:00。 預設設定是 02:00 (2:00 A.M.)。 您可以從**「狀態」>「已排程工作」**頁面中，檢查已排程工作的狀態。 請參閱第 556 頁的「關於已排程工作」。

附註：日誌清除程式執行時，會刪除日誌資料庫中的日誌項目。它不會壓縮資料庫。 為了壓縮資料庫並縮小其大小，Symantec Messaging Gateway 會執行最佳化程序。此程序會根據磁碟使用量自動執行，所以您不需要架構它。不過，因為最佳化程序需要大量的處理能力，所以通常是在離峰時段執行 (預設設定為上午 2:00)。因此，雖然清除程式可能會刪除日誌資料庫中的列，但是除非執行最佳化，否則資料庫大小不會縮小。

附註：您必須具有**「完整的管理」**或**「修改」**權限，才能變更日誌資料庫設定。 請參閱第 566 頁的「管理員權限」。

管理日誌資料庫大小

1. 在控管中心內，按下**「管理」>「設定」>「日誌」**。
2. 按下**「區域」**標籤。
3. 在**「資料庫日誌儲存限制」**下，勾選**「日誌大小上限」**。
4. 在相鄰的方塊中，輸入您要為日誌資料庫配置的大小上限。
5. 在**「刪除資料前，所需要儲存日誌資料的天數」**方塊中，輸入日誌資料的儲存天數。
6. 在**「日誌清除程式」**下方，選擇控管中心執行日誌清除程式以刪除日誌資料的頻率及開始時間。

   小時下拉式清單使用 24 小時制格式。例如，23:00 就是下午 11:00。
7. 按下**「儲存」**。

架構記錄層級

您可以為掃描程式元件指定要儲存的日誌資料量。您可以設定五種掃描程式記錄層級 (從錯誤層級遞增至偵錯層級)。在錯誤層級之後的每個後續記錄層級包括前面所有記錄層級的日誌資料。

請參閱第 525 頁的「關於日誌」。

例如，如果您將「管道」的記錄層級設為通知層級，則也會儲存「管道」錯誤和警告事件。您僅可檢視有關通知、錯誤和警告事件的「管道」日誌資料。在此範例中，「管道」資訊和偵錯事件不會儲存，也無法在控管中心或 Syslog 中進行檢視。

選取的層級應該包含想要監控的資訊類型。請避免選取資訊和偵錯記錄層級，因為它們會耗用大量磁碟空間，並且需要大量處理資源來建立日誌報告。

您隨時都可以修改記錄層級。例如，如果您需要疑難排解問題，則可以增加記錄層級。當您解決問題時，可以將記錄層級回復為其先前的設定。

附註：在變更記錄層級後，可能需要重新啟動掃描程式服務。

警告：高記錄層級會產生大量資料，但傾向於非緊急的狀況。低記錄層級會產生較少的資料，但傾向於較為緊急的狀況。

高記錄層級 (例如偵錯) 會影響記錄程序。如果掃描程式磁碟快取已接近或達到總容量，則系統會切換為降低的記錄模式，或中斷記錄模式。在降低的模式下，僅會將緊急日誌複製到控管中心日誌資料庫。在中斷的模式下，不會將任何日誌檔複製到日誌資料庫。您必須清除磁碟快取、清除日誌資料庫，並調整記錄層級才能繼續正常記錄。

請參閱第 535 頁的「關於記錄磁碟空間警示」。

請參閱第 603 頁的「關於維護足夠的磁碟空間」。

請參閱第 531 頁的「管理日誌資料庫大小」。

請參閱第 536 頁的「清除磁碟空間檢查清單」。

表 22-17 列出了可用的記錄層級。

表 22-17 記錄層級

層級	說明
錯誤	提供最重要的資訊。 此層級提供最少的日誌資訊量。
警告	提供警告和錯誤層級資料。 此層級是所有掃描程式元件 (本機和遠端) 的預設記錄層級。

層級	說明
通知	提供通知資訊以及警告和錯誤層級資料。
資訊	提供資訊訊息以及警告、錯誤和通知資料。
偵錯	提供偵錯資訊以及警告、錯誤、通知和資訊資料。 此層級提供最大的日誌資訊量。 **警告：**請先洽詢賽門鐵克技術支援，再使用此記錄層級。

請參閱第 526 頁的「日誌類型」。

您可以指定本機掃描程式和遠端掃描程式的記錄層級。您可以為每個本機掃描程式架構不同的記錄層級，也可以將設定傳播給所有本機掃描程式。您必須具有「完整的管理」權限和「管理狀態和日誌」修改權限，才能變更記錄層級。您無法變更控管中心和垃圾郵件隔離所的記錄層級。

請參閱第 528 頁的「檢視日誌檔」。

架構特定本機掃描程式的記錄層級

1. 在控管中心內，按下**「管理」>「設定」>「日誌」**。
2. 按下**「區域」**標籤。
3. 在**「本機記錄」**下，勾選**「啟用下列主機元件的本機記錄」**，然後按下要儲存本機記錄的主機。
4. 使用**「元件本機記錄層級」**下拉式清單，選取每個元件的記錄層級。
5. 按下**「儲存」**。

架構遠端掃描程式的記錄層級

1. 在控管中心內，按下**「管理」>「設定」>「日誌」**。
2. 按下**「遠端」**標籤。
3. 在**「遠端記錄」**下，勾選**「啟用下列主機的 Syslog」**，然後按下要傳送其日誌資料的主機。
4. 在**「Syslog 設定值」**下，為遠端 syslog 指定主機名稱、通訊埠和通訊協定。
5. 使用**「元件遠端記錄層級」**下拉式清單，選取每個元件的記錄層級和功能。

   請參閱第 538 頁的「將遠端記錄架構為 syslog」。
6. 按下**「儲存」**。

手動刪除日誌檔

日誌清除程式公用程式可讓您排程定期清除日誌資料庫。但是，某些情況下，您可能想要手動從日誌資料庫刪除日誌。您可以從控管中心日誌資料庫的**「狀態」>「系統」>「日誌」**頁面上，清除掃描程式日誌檔和目錄資料服務日誌檔。您也可以使用 `delete` 指令手動刪除日誌檔。

請參閱第 647 頁的delete。

附註：從控管中心日誌資料庫刪除掃描程式日誌檔和目錄資料服務日誌檔時，不會從掃描程式硬體裝置移除原始日誌檔。若要刪除原始掃描程式日誌檔和目錄資料服務日誌檔，您必須使用指令行介面。

請參閱第 536 頁的「清除磁碟空間檢查清單」。

請參閱第 531 頁的「管理日誌資料庫大小」。

請參閱第 535 頁的「關於記錄磁碟空間警示」。

請參閱第 528 頁的「檢視日誌檔」。

您必須要有完整的管理權限、管理狀態權限或日誌修改權限，才能手動刪除日誌。

手動刪除日誌檔

1. 在控管中心內，按下**「狀態」>「系統」>「日誌」**。
2. 從「過濾」區段的元件下拉式功能表中，選取**「掃描程式」**或**「目錄資料服務」**。
3. 針對掃描程式日誌按下**「清除全部掃描程式日誌」**，針對目錄資料服務日誌按下**「清除全部 DDS 日誌」**。

關於記錄磁碟空間警示

Symantec Messaging Gateway 包括增強的記錄功能，可讓系統管理員啟用在記錄掃描程式上的磁碟空間接近或達到容量時發出警示。達到預設臨界值層級時，系統就會切換至減少或停止記錄模式，然後向指定的管理員傳送電子郵件通知。您需要啟用磁碟空間不足警示，才能收到此通知。

請參閱第 590 頁的「架構警示」。

記錄模式變更通常是控管中心的記錄層級變更所導致。如果管理員將記錄層級設定成會產生大量資料的層級 (例如「偵錯」層級)，則控管中心可能無法以配合內送資料的傳送速度，將資料檔案從掃描程式複製到日誌資料庫。 日誌檔會保留在掃描程式上，而且很快就會填滿磁碟空間。

請參閱第 531 頁的「管理日誌資料庫大小」。

系統切換至減少記錄模式時，只會記錄緊急記錄層級 (例如「錯誤」與「警告」)。產生過多非緊急性質之資料的記錄層級 (例如「通知」、「資訊」以及「偵錯」) 會中斷，直到磁碟釋出空

間為止。發生中斷情況時，會中斷所有記錄層級。只有將該磁碟的日誌檔傳輸出去之後，才會繼續正常的記錄功能。

附註：減少與停止記錄功能只適用於作為掃描程式或目錄資料服務 (DDS) 運作的硬體裝置。

請參閱第 536 頁的「清除磁碟空間檢查清單」。

清除磁碟空間檢查清單

下列為可用來清除控管中心與掃描程式硬體裝置上之磁碟空間的選項清單。如果您判斷低磁碟空間可用性目前已經影響到系統效能，請使用下列選項。

請參閱第 535 頁的「關於記錄磁碟空間警示」。

請參閱第 525 頁的「關於日誌」。

請參閱第 535 頁的「手動刪除日誌檔」。

附註：有些記錄檔是硬體裝置正常運作的一部分，因此不應刪除。如果您注意到這些目錄含有大量檔案，或這些目錄含有任何異常大的檔案，則在刪除任何檔案之前，應該洽詢賽門鐵克支援。使用這些動作的一部分可能足以將磁碟還原為正常運作狀態。請謹慎地刪除資料。

表 22-18　　控管中心資料

控管中心儲存的資料	說明
隔離的郵件	按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**頁面上的**「全部刪除」**，可刪除垃圾郵件隔離所中儲存的所有垃圾郵件。
內容過濾事件	舊的內容過濾事件可以從**「內容」>「事件管理」>[內容事件管理資料夾]**刪除。按下**「刪除」**或**「全部刪除」**以刪除內容。
報告資料	按下**「管理」>「設定」>「報告」**頁面上的**「立即刪除資料」**，可刪除所有報告資料與控制面板資料。
儲存在日誌資料庫中的掃描程式資料	在**「狀態」>「系統」>「日誌」**頁面上，選取**「元件」**清單中的**「掃描程式」**，然後按下**「清除全部掃描程式日誌」**，以從日誌資料庫中刪除掃描程式日誌。
日誌資料庫中儲存的目錄資料服務 (DDS) 資料	在**「狀態」>「系統」>「日誌」**頁面上，選取**「元件」**清單中的**「目錄資料服務」**，然後按下**「清除全部 DDS 日誌」**，以刪除目錄資料服務日誌。
本機儲存的資料庫備份	這些備份儲存在硬體裝置的 /data/backups/ 或 /data/backups/tmp/ 中。 按下**「管理」>「主機」>「版本」>「還原/下載」**頁面上的**「刪除」**，可刪除儲存在硬體裝置本機上的舊備份。

控管中心儲存的資料	說明
舊的軟體更新資料	位於 /data/apt/ 目錄與其子目錄中的檔案。若要刪除舊的軟體更新資料，在指令行中輸入下列字行： `delete sudata`

您可以使用指令行刪除資料檔。

請參閱第 627 頁的「透過指令行管理 Symantec Messaging Gateway」。

請參閱第 647 頁的delete。

請參閱第 686 頁的mta-control。

表 22-19　　掃描程式資料

掃描程式儲存的資料	說明
核心檔案	位於 /data/scanner/jobs/ 目錄與其子目錄中的檔案。若要刪除核心檔案，在指令行中輸入下列字行： `delete cores`
日誌檔	位於 /data/logs/ 目錄與其子目錄中，且控管中心尚未擷取的檔案。若要刪除所有日誌檔案，在指令行中輸入下列字行： `delete alllogs`
Stats 檔案	位於 /data/scanner/stats/ 目錄中，且控管中心尚未擷取的檔案。若要刪除 stats 檔案，在指令行中輸入下列字行： `delete alldata` 除了 stats 檔案之外，此指令還會刪除其他資料。僅在必要時使用 `delete alldata`。
Tmp 檔案	位於 /tmp/ 與 /var/tmp/ 目錄與其子目錄中的檔案。若要刪除個別檔案，在指令行中輸入下列字行： `delete file /tmp/`*`filename`* 或 `delete file /data/tmp/`*`filename`*
稽核日誌	位於 /data/logs/scanner/ 目錄中，且其名稱開頭為 audit_ 的檔案。若要刪除稽核日誌，在指令行中輸入下列字行： `delete mallogs`
塞在入埠、離埠和傳送郵件佇列中的舊郵件	位於 /data/mta/queues/ 目錄與其子目錄中的檔案。若要刪除塞在佇列中的郵件，在指令行中輸入下列字行： `mta-control all delete-all-msgs`

掃描程式儲存的資料	說明
錯誤郵件資料夾中儲存的郵件	位於 /data/mta/bad-messages 中的檔案。若要刪除錯誤郵件，在指令行中輸入下列字行： `mta-control all bad-msg-delete all`
舊的軟體更新資料	位於 /data/apt/ 目錄與其子目錄中的檔案。若要刪除舊的軟體更新資料，在指令行中輸入下列字行： `delete sudata`

監控遠端伺服器上的日誌

表 22-20說明您可監控遠端伺服器上日誌的方式。您可以視需要以任何順序執行這些工作。

表 22-20 監控遠端伺服器上的日誌

工作	說明
架構 Symantec Messaging Gateway 以將掃描程式日誌資料傳送至遠端 syslog。	有些掃描程式日誌可以傳送至遠端伺服器上的 syslog。請確定已將遠端 syslog 架構成符合控管中心內的設定。您必須啟用本機記錄、遠端記錄或同時啟用兩者。 請參閱第 538 頁的「將遠端記錄架構為 syslog」。
熟悉掃描程式日誌的標準字首。	您可以讓傳送至遠端 syslog 的所有掃描程式日誌訊息都採取標準形式。 請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。
熟悉日誌格式。	下列主題說明可用的各種日誌格式： ■ 請參閱第 540 頁的「遠端 syslog 之 boot.log、cron、郵件和安全元件的日誌格式」。 ■ 請參閱第 540 頁的「遠端 syslog 之管道、Brightmail 用戶端、Brightmail 引擎和 JLU 控制器的日誌格式」。 ■ 請參閱第 542 頁的「遠端 syslog 之郵件傳輸代理程式的日誌格式」。 ■ 請參閱第 542 頁的「遠端 syslog 之郵件稽核日誌的日誌格式」。

將遠端記錄架構為 syslog

有些掃描程式日誌可以傳送至遠端伺服器上的 syslog。請確定已將遠端 syslog 架構成符合控管中心內的設定。您必須啟用本機記錄、遠端記錄或同時啟用兩者。

將遠端記錄架構為 syslog

1 在控管中心內，按下**「管理」>「設定」>「日誌」**。

2 按下**「遠端」**標籤。

3 按下「**啟用下列主機的 Syslog**」，然後按下某個主機，以從該主機將日誌資料傳送至遠端 syslog。

4 在「**主機**」欄位中，指定 syslog 伺服器的 IP 位址。

5 在「**通訊埠**」欄位中，指定 syslog 伺服器上用於處理日誌資料的通訊埠。

6 在「**通訊協定**」欄位中，指定 syslog 通訊協定：UDP 或 TCP。

7 在「**元件遠端記錄層級**」下，指定每個元件的記錄層級和設施。

8 按下「**啟用郵件日誌**」，將郵件日誌傳送到遠端 syslog。

9 按下「**郵件記錄設施**」。

10 按下「**將這些遠端記錄設定套用至所有主機**」(如有需要)。

11 按下「**儲存**」儲存變更。

日誌元件可能需要重新啟動。

傳送至遠端 syslog 之掃描程式日誌的標準字首

您可以架構 Symantec Messaging Gateway 以將掃描程式日誌資料傳送至遠端 syslog。而傳送至遠端 syslog 的所有掃描程式日誌訊息都採取下列形式：

日期和時間	功能層級	IP 位址	原始日誌訊息
`1-15-2009 15:42`	`Local3.Info`	`10.217.32.13`	`Jan 15 15:38:05 scanner1 jlu-controller: [Brightmail] (INFO:21145.3071248064): [54038] AV definitions are up-to-date.`
日期為「月-日-年」格式。時間為「小時: 分鐘」格式。而且時間是以 24 時制表示。 此日期和時間就是日誌訊息傳送至遠端 syslog 的日期和時間。	功能、期間和記錄層級。功能可針對日誌資料傳送目的地的遠端 syslog 指定功能。記錄層級是掃描程式上架構的記錄層級。	傳送日誌訊息之 Symantec Messaging Gateway 主機的 IP 位址。	出現在掃描程式上的原始日誌訊息。這部分的格式取決於日誌元件。

前三欄組成出現在所有日誌訊息傳送至遠端 syslog 之前的標準字首。下列是出現在遠端 syslog 上之某個事件的日誌訊息。

```
1-15-2009 15:42 Local3.Info 10.217.32.13 Jan  15 15:38:05
scanner1 jlu-controller: [Brightmail] (INFO:21145.3071248064):
[54038] AV definitions are up-to-date.
```

請參閱第 538 頁的「將遠端記錄架構為 syslog」。

遠端 syslog 之 boot.log、cron、郵件和安全元件的日誌格式

您可以架構 Symantec Messaging Gateway 以將掃描程式日誌資料傳送至遠端 syslog。如果啟用遠端 syslog，則 boot.log、cron、郵件和安全元件的日誌資料會傳送至遠端 syslog。這些是標準 UNIX 日誌元件。這些元件的日誌資料會傳送至遠端 syslog 的標準 syslog 功能。則無法架構這些元件的記錄層級。傳送至遠端 syslog 的所有日誌訊息都具有相同的字首文字。

請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。

而傳送至遠端 syslog 的日誌訊息採取下列形式：

標準字首	日期和時間	掃描程式主機名稱	程序[PID]:	訊息
日期、時間、功能、記錄層級和 IP 位址	`Jan 15 11:51:33`	`scanner1`	`syslog-ng [25257]:`	`syslog-ng version 1.6.5 starting`
請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。	日期為「月份日期」格式。時間為「小時:分鐘」格式。而且時間是以 24 時制表示。 此日期和時間就是日誌訊息記錄在掃描程式上的日期和時間。	在其上建立日誌訊息的掃描程式名稱。	產生日誌訊息之程序的名稱和程序 ID。	日誌訊息。

下列是出現在遠端 syslog 上之某個事件的日誌訊息。

```
01-15-2009 11:52:44 Syslog.Notice 10.217.32.13 Jan 15 11:51:33
scanner1 syslog-ng[25257]:syslog-ng version 1.6.5 starting
```

遠端 syslog 之管道、Brightmail 用戶端、Brightmail 引擎和 JLU 控制器的日誌格式

您可以架構 Symantec Messaging Gateway 以將掃描程式日誌資料傳送至遠端 syslog。傳送至遠端 syslog 的所有日誌訊息都具有相同的字首文字。

請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。

下表包含下列元件的範例日誌訊息 (依相同順序列出)：

- 管道
- Brightmail 用戶端
- Brightmail 引擎

- JLU 控制器

標準字首	日期和時間	掃描程式主機名稱	Process: [Brightmail]	(LogLevel: PID: ThreadID):	[EC/Source: #:Function]	郵件
日期、時間、功能、記錄層級和 IP 位址	Jan 15 11:34:51	scanner1	conduit: [Brightmail]	(DEBUG: 19713. 3071461056):	[src/rda_ controller.cc: 586:initial ize]	Appending HTTP header: 'Spamwall_ID: (null)'
	Jan 15 11:36:16	scanner1	ecelerity: [Brightmail]	(DEBUG: 20132. 3082545888):	[src/sms_ dpp.c:359: dpp_init]	DPP system initialized
	Jan 15 11:37:05	scanner1	bmserver: [Brightmail]	(DEBUG: 20516. 3066324672):	[src/rhk_ hint.c:497: rhk_hint_ parse]	rhk hint for rule 43731290 has been successfully parsed
	Jan 15 11:38:05	scanner1	jlu-controller: [Brightmail]	(INFO: 21145. 3071248064):	[54038]	AV definitions are up-to-date.
請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。	日期為「月份日期」格式。時間為「小時:分鐘」格式。而且時間是以 24 時制表示。 此日期和時間就是日誌訊息記錄在掃描程式上的日期和時間。	在其上建立日誌訊息的掃描程式名稱。	產生日誌訊息的程序、一個冒號、一個空格，以及使用方括弧括住的 Brightmail 名稱。	在小括弧中，是記錄層級、一個冒號、程序 ID、一個句點，以及執行緒 ID (後接冒號)。	在方括弧中，是錯誤碼縮寫 (EC)、原始程式碼檔案名稱、行號以及原始程式碼檔案中的函數呼叫。 對於 JLU 控制器，此值就是對應到日誌訊息的內部錯誤代碼編號。	日誌訊息。

下列是出現在遠端 syslog 上之某個事件的日誌訊息。

```
01-15-2009 11:38:16 Local2.Debug 10.217.32.13 Jan  15 11:37:05
scanner1 bmserver: [Brightmail] (DEBUG:20516.3066324672):
[src/rhk_hint.c:497:rhk_hint_parse] rhk hint for rule 43731290
has been successfully parsed
```

遠端 syslog 之郵件傳輸代理程式的日誌格式

您可以架構 Symantec Messaging Gateway 以將掃描程式日誌資料傳送至遠端 syslog。如果啟用遠端 syslog，則 MTA 日誌資料會傳送至遠端 syslog。傳送至遠端 syslog 的所有日誌訊息都具有相同的字首文字。

請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。

而傳送至遠端 syslog 的 MTA 日誌訊息採取下列形式：

標準字首	日期和時間	掃描程式主機名稱	程序:[PID]	郵件
日期、時間、功能、記錄層級和 IP 位址	`Jan 15 11:39`	`scanner1`	`ecelerity: [21911]`	`THPL-00150: Defer_queue_ suspect_bad_message thread -1696945232 starting`
MTA 郵件的功能一律為 `mail`。 請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。	日期為「月份日期」格式。時間為「小時:分鐘」格式。而且時間是以 24 時制表示。 此日期和時間就是日誌訊息記錄在掃描程式上的日期和時間。	在其上建立日誌訊息的掃描程式名稱。	產生日誌訊息之程序的名稱和程序 ID。而名稱一律為 MTA 名稱：`ecelerity`。	日誌訊息。

下列是出現在遠端 syslog 上之某個事件的日誌訊息。

```
01-15-2009 11:40:34 Mail.Debug 10.217.32.13 Jan  15 11:39:23
scanner1 ecelerity: [21911] THPL-00150: Defer_queue_suspect_bad_message
thread -1696945232 starting
```

遠端 syslog 之郵件稽核日誌的日誌格式

您可以架構 Symantec Messaging Gateway 以將郵件稽核日誌資料傳送至遠端 syslog。傳送至遠端 syslog 的所有日誌訊息都具有相同的字首文字。

請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。

而傳送至遠端 syslog 的郵件稽核日誌訊息採取下列形式：

標準字首	日期和時間	掃描程式主機名稱	程序:	郵件
日期、時間、功能、記錄層級和 IP 位址	Jan 15 15:42	scanner1	ecelerity:	1230876822|0ad9200d-b7b61ae00000 5b81-00-495db08c9df2| DELIVER|10.217.32.13| rashu1@symantecs.org
請參閱第 539 頁的「傳送至遠端 syslog 之掃描程式日誌的標準字首」。	日期為「月份日期」格式。時間為「小時:分鐘」格式。而且時間是以 24 時制表示。 這是在掃描程式上記錄日誌訊息的日期和時間。	在其上建立日誌訊息的掃描程式名稱。	產生日誌訊息之程序的名稱。	日誌訊息。

下列是出現在遠端 syslog 上之某個事件的日誌訊息。

```
01-15-2009 11:44:53 Local3.Info 10.217.32.13 Jan  15 15:42:42
scanner1 ecelerity: 1230876822|0ad9200d-b7b61ae000005b81-00-
495db08c9df2|DELIVER|10.217.32.13|rashu1@symantecs.org
```

處理郵件稽核日誌和郵件佇列

表 22-21說明您可使用郵件稽核日誌和郵件佇列監控 SMTP 狀態的方式。您可以視需要以任何順序執行這些工作。

表 22-21 處理郵件稽核日誌和郵件佇列

工作	說明
深入瞭解 Symantec Messaging Gateway 郵件稽核日誌。	Symantec Messaging Gateway 提供的郵件稽核元件可讓您搜尋郵件，並瞭解這些郵件所發生的事件。啟用郵件稽核日誌後，系統管理員可以追蹤掃描程式已接受及處理的每一封郵件之詳細資訊。稽核資訊可用於在單一掃描程式架構中追蹤做出了哪些決策。郵件稽核日誌的目的並不在於取代偵錯或資訊層級的日誌。不同於標準的掃描程式日誌，郵件稽核日誌會提供與特定郵件相關的資訊。
熟悉稽核日誌格式和事件。	每個寫入郵件稽核資訊的軟體元件會寫入本身的稽核記錄。稽核記錄中的每個項目由至少三個欄位組成。 稽核日誌事件 ID 說明已記錄的稽核事件類型。有些事件 ID 後面是參數。每個軟體元件皆使用自己的日誌參數。

工作	說明
啟用或停用郵件稽核日誌。	依預設，會針對本機記錄啟用郵件稽核日誌，並會針對遠端記錄停用郵件稽核日誌。必須先啟用此功能，才能取得稽核資訊來進行檢視或搜尋。郵件稽核的儲存區可能會變得很龐大，而搜尋日誌則可能會讓掃描程式的處理時間變得冗長。 請參閱第 545 頁的「啟用郵件稽核日誌」。
在郵件稽核日誌中尋找特定郵件。	本硬體裝置提供了一個可讓您搜尋日誌的查詢工具，以判斷是否有一或多個郵件符合您所要搜尋郵件的條件。 請參閱第 545 頁的「搜尋郵件稽核日誌中的郵件」。
將郵件稽核日誌資料匯出為 .csv 檔。	若要在 Microsoft Excel 中檢視含有雙位元組字元的 CSV 檔，請在 MSExcel 文字匯入精靈中指定逗號分隔的 UTF-8 檔。或者，您可以用能將 UTF-8 轉成 Unicode 的文字編輯器 (如 Notepad) 開啟 CSV 檔，然後把它儲存為 Unicode。 請參閱第 549 頁的「匯出郵件稽核日誌資料」。
深入瞭解郵件佇列。	郵件佇列是郵件在到達目的前暫時保留的區域。郵件佇列為： 入埠、離埠和傳送佇列。郵件佇列的大小會根據郵件流而變動。 如果佇列繼續增長而沒有縮減大小，就表示郵件的傳送發生問題。 請參閱第 550 頁的「關於郵件佇列」。 請參閱第 65 頁的「MTA 與郵件佇列行為」。
隨時檢視佇列的郵件以疑難排解問題。	您至少必須指定主機以及想要檢視的佇列：入埠、離埠或傳送。Symantec Messaging Gateway 還具有過濾選項，可讓您進一步自訂要檢視的排入佇列的郵件。根據過濾條件，Symantec Messaging Gateway 會顯示當時該佇列中的郵件。如果郵件具有關聯的錯誤，則該郵件會顯示在**「郵件」**欄中。 請參閱第 550 頁的「檢視佇列的郵件」。
重新繞送郵件佇列中的郵件。	您可以從特定路由或一組路由中搜尋傳送佇列中的郵件。您也可以從一個路由將郵件重新繞送至其他路由。 請參閱第 551 頁的「重新繞送傳送佇列中的郵件」。
從郵件佇列中刪除郵件。	當您檢視郵件佇列時，可能會發現有郵件堵塞佇列。您可以刪除該郵件，讓該郵件後面的郵件可以通過佇列。當您刪除佇列的郵件之後，就無法擷取該郵件。您可以刪除佇列中的所有郵件。 請參閱第 552 頁的「刪除佇列的郵件」。
停止郵件流。	您可能需要停止郵件流 (例如在您重新傳送郵件佇列之前)。停止郵件流前，請確保您瞭解其影響。 請參閱第 553 頁的「停止郵件流」。

工作	說明
清除郵件佇列。	重新傳送郵件佇列時，就是指示 MTA 嘗試重新傳送任何由於傳送問題而延遲的郵件。關閉硬體裝置之前，您可能要清除入埠、離埠和傳送電子郵件的佇列。 請參閱第 554 頁的「清除郵件佇列」。
監控郵件佇列的狀態，以判斷郵件佇列是否已滿。	您可以檢視佇列的郵件數以及所有郵件佇列的佇列大小。您可以在**「SMTP 進階設定」**頁面上設定每個郵件佇列的大小上限，以及決定是否在佇列已滿時延遲郵件。 請參閱第 554 頁的「監控郵件佇列大小和數量」。
解決郵件佇列問題。	如果郵件佇列過大，則 Symantec Messaging Gateway 會沒有回應或當機。為了防止出現此問題，Symantec Messaging Gateway 預設在佇列已滿時延遲新的郵件。最佳作法是啟用此設定，並使佇列限制保持在建議的預設臨界值以下。 請參閱第 555 頁的「疑難排解郵件佇列」。

啟用郵件稽核日誌

依預設，會針對本機記錄啟用郵件稽核日誌，並會針對遠端記錄停用郵件稽核日誌。必須先啟用此功能，才能取得稽核資訊來進行檢視或搜尋。郵件稽核的儲存區可能會變得很龐大，而搜尋日誌則可能會讓掃描程式的處理時間變得冗長。

針對本機記錄啟用或停用郵件稽核日誌

1. 在控管中心內，按下**「管理」>「設定」>「日誌」**。
2. 在「區域」標籤的「郵件稽核日誌」下，勾選或取消勾選**「啟用郵件日誌」**。
3. 按下**「儲存」**。

針對遠端記錄啟用或停用郵件稽核日誌

1. 在控管中心內，按下**「管理」>「設定」>「日誌」**。
2. 在「遠端」標籤的「郵件稽核日誌」下，勾選或取消勾選**「啟用郵件日誌」**。
3. 從下拉式清單中選取**「郵件記錄設施」**。
4. 按下**「儲存」**。

搜尋郵件稽核日誌中的郵件

本硬體裝置提供了一個可讓您搜尋日誌的查詢工具，以判斷是否有一或多個郵件符合您所要搜尋郵件的條件。

「狀態」> SMTP >「郵件稽核日誌」頁面，可讓您指定一至兩個條件，以及下列相關補充資訊：

主機	執行 Symantec Messaging Gateway 軟體的一或多個掃描程式。若要找出所有的郵件詳細資訊，請搜尋所有連線的掃描程式。
時間範圍	搜尋查詢稽核日誌的期間。即使您可以搜尋更長的時間期間，但仍建議不要搜尋超過一週以前的訊息。
必要過濾器	選取用來過濾郵件的資訊類型。請參閱「表 22-22」。
必要過濾器值	輸入對應到所選必要過濾器類型的字串。例，如果選擇要依寄件者過濾郵件，請在此輸入有效的電子郵件地址。
選用過濾器	從選用過濾器條件清單中進行選取。請參閱「表 22-23」。
選用過濾器值	視需要輸入字串或是選擇對應到所選取之選用過濾器類型的值。例，如果選擇要依「連線 IP」過濾郵件，請在此輸入有效的 IP 位址。如果選擇要依「採取動作」過濾郵件，則請選取要尋找的郵件動作。
清除過濾器	清除記憶體中目前的過濾條件。
顯示已過濾	搜尋並顯示符合條件的郵件。

表 22-22 說明可以為單一必要過濾器選擇的項目。

表 22-22 必要搜尋條件的選項

條件	說明
寄件者	郵件寄件者的名稱。指定 <> 以過濾不包含寄件者名稱的郵件。
收件者	郵件收件者的名稱。
主旨	郵件主旨。
稽核 ID	Symantec Messaging Gateway 所產生且作為郵件標頭內含的唯一識別碼。
連線 IP	連線伺服器的 IP 位址。在 Symantec Messaging Gateway 拒絕某 IP 連線時，這會導致將某列的寄件者識別為「無」。郵件詳細資料會包含 IP 位址和拒絕原因。 Symantec Messaging Gateway 支援 IPv4 位址和 IPv6 位址。
邏輯 IP	連線伺服器的邏輯 IP 位址。 邏輯連線 IP 用於特定部署，這種部署中含有可將郵件轉寄到 Symantec Messaging Gateway 伺服器的內部郵件伺服器。邏輯連線 IP 位址是第一個非內部伺服器連線的位址。 邏輯連線 IP 位址是從郵件內容的 Received: 標頭衍生的。Symantec Messaging Gateway 使用此 IP 位址來進行過濾。依據您的部署，此位址可能與「接受自」IP 位址相同。 選取**「邏輯 IP」**之後，您就可以指定 IPv4 位址、IPv6 位址或 IPv6 CIDR 範圍。僅當字首為 4 的倍數時，才接受 CIDR 範圍。

表 22-23 說明可以為單一選用過濾器選擇的項目。

表 22-23 選擇性搜尋條件的選項

條件	說明
寄件者	郵件寄件者的名稱。指定 <> 以過濾不包含寄件者名稱的郵件。
已驗證的寄件者	已驗證的寄件者的名稱。
收件者	郵件收件者的名稱
主旨	郵件主旨。
郵件 ID	通常由啟動郵件傳送的電子郵件軟體所產生的唯一識別碼，並以郵件標頭的方式含括在郵件之內。垃圾郵件寄發者會利用這個標頭來隱藏郵件發出人的身分。
判斷	郵件的判斷及/或其他特性。選取此過濾選項時，**「選用過濾器值」**下拉式清單中會出現可能的判斷清單。使用這些值可以過濾導致特定判斷的郵件。例如，您可以將**「選用過濾器值」**設定為**「郵件屬於電子報」**。
未經測試的判斷	未經掃描程式測試的可用判斷。系統會提供一份判斷選項的下拉式清單。
採取動作	郵件發生的事件。選取此過濾選項時，「選用過濾器值」下拉式清單中會出現可能的動作清單。使用這些值可以過濾觸發套用特定動作之政策的郵件。 如果您在「選用過濾器值」下拉式清單選取「拒絕郵件」，郵件詳細資料中就會出現拒絕原因。 ■ 拒絕的非本機收件者郵件 ■ 拒絕超出大小限制的郵件 ■ 由 MTA 拒絕的郵件 ■ 拒絕未通過退回攻擊驗證的郵件 ■ 拒絕遭收件者拒絕的超出大小限制的無效郵件 ■ 所有收件者均無效
連線 IP	用來接收郵件的連線 IP。 Symantec Messaging Gateway 支援 IPv4 位址和 IPv6 位址。

條件	說明
邏輯 IP	連線伺服器的邏輯 IP 位址。 邏輯連線 IP 用於特定部署，這種部署中含有可將郵件轉寄到 Symantec Messaging Gateway 伺服器的內部郵件伺服器。邏輯連線 IP 位址是第一個非內部伺服器連線的位址。 邏輯連線 IP 位址是從郵件內容的 Received: 標頭衍生的。Symantec Messaging Gateway 使用此 IP 位址來進行過濾。依據您的部署，此位址可能與「接受自」IP 位址相同。 選取**「邏輯 IP」**之後，您就可以指定 IPv4 位址、IPv6 位址或 IPv6 CIDR 範圍。僅當字首為 4 的倍數時，才接受 CIDR 範圍。
目標 IP	郵件目的地的 IP 位址。
政策群組	決定要套用至郵件之過濾器政策的群組 (收件者群組或寄件者群組) 名稱。
過濾器政策	套用至郵件的過濾器政策名稱。
病毒	郵件包含的病毒名稱。
附件	郵件附件的名稱。
可疑附件	觸發內容過濾政策的郵件附件名稱。
無法掃描判斷的原因	郵件符合「如果因任何原因而無法掃描郵件是否存在惡意軟體和內容過濾」情況的原因。系統會提供一份無法掃描原因的下拉式清單。
來源	指出郵件來自內部或外部。
解除的內容	指出郵件附件是否包含潛在惡意內容。

搜尋時將使用以下的規則：

- 在每次搜尋中，每個掃描程式最多可搜尋 1,000 封郵件。
- 自由格式的文字欄位，是不區分字母大小寫的子字串搜尋。

附註：「郵件稽核日誌」提供每個收件者收到之每封郵件的資訊。例如，如果有 10 個收件者收到相同的郵件，則您會在「郵件稽核日誌」中看到 10 個項目。若要達到傳回郵件數目為 1,000 的限制，Symantec Messaging Gateway 會將相同郵件之不同收件者的多個項目計為一封郵件。

在郵件稽核日誌中，會將傳送失敗的電子郵件追蹤記錄為傳送失敗。例如，會將因傳送給不存在的使用者而退回的郵件視為傳送失敗。在「稽核日誌」頁面的「傳送」區段中，會以「傳送失敗」標題來註明傳送失敗。除了在「稽核日誌」頁面上註明之外，還會使用新的 DELIVERY_FAILURE 稽核日誌事件來記錄未傳送的郵件。DELIVERY_FAILURE 事件會使用以下格式記錄：`utc|uid|DELIVERY_FAILURE|recipient|reason`

「動作」欄會指出掃描程式對郵件採取的動作，但不會指出管理員或使用者對郵件採取的動作。例如，若管理員或使用者從「垃圾郵件隔離所」中釋放郵件，則此活動會列於**「垃圾郵件隔離所」**(而非 **「動作」**) 下。

搜尋郵件稽核日誌和檢視郵件詳細資料

1. 在控管中心內，按下**「狀態」> SMTP >「郵件稽核日誌」**。
2. 從**「主機」**下拉式清單中選取要搜尋其日誌的掃描程式，或選取**「所有掃描程式」**。
3. 完成所要的搜尋條件。
4. 按下**「顯示已過濾」**。

   使用**「每頁的項目數」**下拉單指定每頁要顯示的記錄數。使用**「顯示」**下拉單選擇要顯示的資料範圍。
5. 按下「收件者」欄中的郵件收件者，以檢視該郵件的處理詳細資訊。

搜尋郵件稽核日誌是否存在內容過濾事件

1. 在控管中心內，按下**「狀態」> SMTP >「郵件稽核日誌」**。
2. 從**「主機」**下拉式清單中選取要搜尋其日誌的掃描程式，或選取**「所有掃描程式」**。
3. 從**「必要過濾器」**下拉式清單中進行選擇，並在**「必要過濾器值」**欄位中輸入適當值。
4. 從**「選用過濾器」**下拉式清單中，選擇**「採取動作」**。
5. 從**「選用過濾器值」**下拉式清單中，選擇**「建立資訊事件」**或**「建立隔離事件」**。
6. 按下**「顯示已過濾」**。

   使用**「每頁的項目數」**下拉單指定每頁要顯示的記錄數。使用**「顯示」**下拉單選擇要顯示的資料範圍。
7. 按下**「收件者」**欄中的郵件收件者，以檢視該郵件的處理詳細資訊。

在郵件稽核日誌中檢視郵件的 TLS 加密傳送狀態

1. 在郵件稽核日誌中找到郵件。
2. 展開**「收件者資料」>「傳送」**。
3. 按下**「詳細資料」**。

請參閱第 300 頁的「郵件稽核日誌如何協助微調及疑難排解內容過濾政策」。

匯出郵件稽核日誌資料

在選取過濾條件並按下**「顯示已過濾」**之後，您可以將日誌資料匯出到 CSV 檔案。

若要在 Microsoft Excel 中檢視含有雙位元組字元的 CSV 檔，請在 MS Excel 文字匯入精靈中指定逗號分隔的 UTF-8 檔。或者，您可以用能將 UTF-8 轉成 Unicode 的文字編輯器 (如 Notepad) 開啟 CSV 檔，然後把它儲存為 Unicode。

匯出郵件稽核日誌資料

1. 在控管中心內，按下「**狀態**」**> SMTP >**「**郵件稽核日誌**」。
2. 從「**主機**」下拉式清單中選取要搜尋其日誌的掃描程式，或選取「**所有掃描程式**」。
3. 完成搜尋條件。
4. 按下「**顯示已過濾**」。
5. 按下「**匯出 CSV**」。
6. 按下「**檔案編碼**」下拉式清單，為 CSV 檔案選擇字元編碼。

   ISO-8859-1 和 UTF-8 適用於歐洲語系。Windows-31j、EUC-JP 和 ISO-2022-JP 則適用於日文。
7. 按下「**CSV 分隔符號**」下拉式清單，為 CSV 檔案選擇分隔符號。

   Symantec Messaging Gateway 會在檔案中的項目之間插入所選擇的分隔字元。

關於郵件佇列

郵件佇列是郵件在到達目的前暫時保留的區域。郵件佇列為：入埠、離埠和傳送佇列。郵件佇列的大小會根據郵件流而變動。

如果佇列繼續增長而沒有縮減大小，就表示郵件的傳送發生問題。您可以隨時檢視佇列的郵件以疑難排解問題。郵件佇列會提供關於 MTA 無法傳送郵件的原因、已嘗試傳送的次數，以及排程的下次嘗試傳送時間等詳細資料。

請參閱第 554 頁的「監控郵件佇列大小和數量」。

請參閱第 550 頁的「檢視佇列的郵件」。

請參閱第 552 頁的「刪除佇列的郵件」。

請參閱第 553 頁的「停止郵件流」。

請參閱第 554 頁的「清除郵件佇列」。

請參閱第 555 頁的「疑難排解郵件佇列」。

檢視佇列的郵件

您可以檢視郵件佇列中的郵件。您至少必須指定主機以及想要檢視的佇列：入埠、離埠或傳送。Symantec Messaging Gateway 還具有過濾選項，可讓您進一步自訂要檢視的排入佇列的郵件。根據過濾條件，Symantec Messaging Gateway 會顯示當時該佇列中的郵件。

郵件佇列提供有關 MTA 為何無法傳送郵件、嘗試傳送郵件的次數，以及排程嘗試下次傳送的時間等詳細資料。

您有時可能會想要判斷特定郵件是否位在佇列中。您可以針對特定電子郵件地址所接收或傳送的郵件進行過濾。您還可以搜尋來自某個特定路由或一組路由的郵件，此功能僅限於傳送佇列。您也可以從一個路由將郵件重新繞送至其他路由。

請參閱第 551 頁的「重新繞送傳送佇列中的郵件」。

您可以對寄件者 (「寄件者」欄位) 或收件者 (「收件者」欄位) 執行萬用字元搜尋。這些搜尋會區分大小寫。支援使用星號 (*) 和問號 (?) 萬用字元。對於傳送佇列，您還可以使用萬用字元來搜尋自訂路由。

如果您未停止郵件流，則在新的郵件進入佇列時，佇列中的郵件可能會繼續流動，而舊的郵件會結束。您可以視需要重新整理檢視。

您必須具有「完整的管理」權限或「管理狀態和日誌」檢視或修改權限，才能檢視郵件佇列。

檢視佇列的郵件

1. 在控管中心內，按下**「狀態」> SMTP >「郵件佇列」**。
2. 在**「郵件佇列」**頁面上，選取主機與佇列。
3. 在提供的欄位中輸入搜尋值。
4. 按下**「顯示已過濾」**。
5. 若要清除**「收件者」**和**「寄件者」**欄位以開始新的搜尋，請按下**「清除過濾器」**。

   會保留您進行的其他所有下拉式功能表選擇。

重新整理檢視

- 在**「郵件佇列」**頁面上，按下**「重新整理」**。

請參閱第 401 頁的「檢視 Content Analysis 佇列」。

重新繞送傳送佇列中的郵件

您可以從特定路由或一組路由中搜尋傳送佇列中的郵件。您也可以從一個路由將郵件重新繞送至其他路由。

請參閱第 550 頁的「檢視佇列的郵件」。

您可以使用萬用字元來搜尋寄件者、收件者或自訂路由。搜尋不區分大小寫。

重新繞送傳送佇列中的郵件

1. 在控管中心內，按下**「狀態」> SMTP >「郵件佇列」**。
2. 在「郵件佇列」頁面上，選取主機與**「傳送」**佇列。

3 在「**繞送**」欄位中，選取下列其中一個選項：

預設本機路由	本機網域的預設路由。
預設非本機路由	非本機網域的預設路由。
控管中心	此掃描程式用來與控管中心通訊的路由。
DLP	此掃描程式用來與 Symantec Network Prevent 伺服器通訊的路由。
自訂	您在「**自訂路由**」欄位中指定的路由。選取「**自訂**」後，會出現「**自訂路由**」欄位。

4 如果選取「**自訂**」，請在「**自訂路由**」欄位中輸入您要搜尋的路由主機名稱或「IP 位址:通訊埠」。 如果您選取其他選項，請略過此步驟。

如果您指定的 CIDR 區塊會從多個路由傳回郵件，將無法重新繞送郵件。 如果過濾的郵件全部來自同一個路由，則「**全部重新繞送**」按鈕會變成作用中狀態。

5 選擇性填寫其他搜尋欄位。

6 按下「**顯示已過濾**」。

7 在「**重新繞送原始目標為已過濾路由的所有郵件**」下，在「**新路由**」欄位中輸入新路由的主機名稱、IP 位址:通訊埠、CIDR 區塊或子網路。

8 如果您輸入主機名稱，則可視需要勾選「**MX 查詢**」。

9 按下「**全部重新繞送**」。

刪除佇列的郵件

當您檢視郵件佇列時，可能會發現有郵件堵塞佇列。您可以刪除該郵件，讓該郵件後面的郵件可以通過佇列。

您可以透過 `mta-control` 指令，來存取排入佇列的郵件並儲存這些郵件。

請參閱第 686 頁的mta-control。

當您刪除佇列的郵件之後，就無法擷取該郵件。

您可以刪除佇列中的所有郵件。選擇「**全部刪除**」時，會刪除當時在該佇列中的郵件，包括其他頁面上的郵件。在您刪除所有佇列的郵件之前，可能會想要暫時停止郵件流。

請參閱第 553 頁的「停止郵件流」。

您必須具有「完整的管理」權限或「管理狀態和日誌」修改權限，才能刪除佇列的郵件。

請參閱第 564 頁的「設定本機和 LDAP 管理員帳戶」。

刪除佇列的郵件

1 在控管中心內，按下「**狀態**」> **SMTP** >「**郵件佇列**」。

2 指定想要檢視的佇列。

請參閱第 550 頁的「檢視佇列的郵件」。

3 執行下列任一項：

刪除郵件	選取想要刪除的郵件，然後按下「**刪除**」。
刪除佇列中的所有郵件，包括其他頁面上的郵件	按下「**全部刪除**」。

停止郵件流

您可能需要停止郵件流 (例如在您重新傳送郵件佇列之前)。

請參閱第 554 頁的「清除郵件佇列」。

請參閱第 552 頁的「刪除佇列的郵件」。

停止郵件流之前，請考慮下列各項：

- 如果停止入埠郵件流，則不會接受任何入埠郵件。不會掃描入埠郵件佇列中的郵件，且會繼續傳送郵件。
- 如果停止離埠郵件流，則不會接受任何離埠郵件。不會掃描離埠郵件佇列中的郵件，且會繼續傳送郵件。
- 如果停止傳送郵件流，則郵件不會傳送至下游的本機或遠端郵件伺服器。會掃描入埠郵件佇列和離埠郵件佇列中的郵件，並將這些郵件累積在傳送郵件佇列中。

請參閱第 65 頁的「MTA 與郵件佇列行為」。

請參閱第 604 頁的「關閉硬體裝置」。

請參閱第 63 頁的「服務與 MTA 作業」。

停止郵件流

1 在控管中心內，按下「**狀態**」> **SMTP** >「**郵件佇列**」。

2 在「**主機**」下拉式清單中選取伺服器。

3 在「**佇列**」下拉式清單中選取「**入埠**」，然後按下「**顯示已過濾**」。

4 如果佇列已啟動，請按下「**停止**」。

5 在「**佇列**」下拉式清單中選取「**離埠**」，然後按下「**顯示已過濾**」。

6 如果佇列已啟動，請按下「**停止**」。

7 在「**佇列**」下拉式清單中選取「**傳送**」，然後按下「**顯示已過濾**」。

8 如果佇列已啟動，請按下「**停止**」。

清除郵件佇列

重新傳送郵件佇列時，就是指示 MTA 嘗試重新傳送任何由於傳送問題而延遲的郵件。關閉硬體裝置之前，您可能要清除入埠、離埠和傳送電子郵件的佇列。

重新傳送郵件佇列之前，請暫時停止入埠電子郵件流。

附註：停止郵件流或判定郵件流已經停止後，賽門鐵克建議您等候 2 分鐘再清除該郵件佇列。

請參閱第 553 頁的「停止郵件流」。

請參閱第 65 頁的「MTA 與郵件佇列行為」。

請參閱第 63 頁的「服務與 MTA 作業」。

您必須具有「完整的管理」權限或「管理狀態和日誌」修改權限，才能重新傳送郵件佇列。

您也可以從指令行清除電子郵件佇列。

請參閱第 686 頁的mta-control。

從控管中心清除電子郵件佇列

1 在控管中心內，按下「**狀態**」**>** **SMTP** **>**「**郵件佇列**」。

2 從「**主機**」下拉式清單中選擇主機。

3 在「**佇列**」下拉式清單中，選取所需的佇列。

請參閱第 550 頁的「檢視佇列的郵件」。

4 按下「**全部重新傳送**」。

將清除所有郵件 (包括其他頁面上的郵件)。

5 待郵件佇列清空 (視需要重複執行上一步)。

監控郵件佇列大小和數量

您可以檢視佇列的郵件數以及所有郵件佇列的佇列大小。監控此狀態可以判斷郵件佇列是否已滿。

您必須要有「完整的管理」權限或「管理狀態和日誌」檢視權限。

監控郵件佇列大小和數量

1 在控管中心內，按下「**狀態**」**>**「**系統**」**>**「**主機**」。

2 按下「**郵件佇列**」標籤。

您可以在「SMTP 進階設定」頁面上設定每個郵件佇列的大小上限，以及決定是否在佇列已滿時延遲郵件。

請參閱第 48 頁的「架構 SMTP 進階設定」。

您可以在「警示」頁面上架構郵件佇列的警示。

請參閱第 590 頁的「架構警示」。

疑難排解郵件佇列

如果郵件佇列過大，則 Symantec Messaging Gateway 會沒有回應或當機。 為了防止出現此問題，Symantec Messaging Gateway 預設在佇列已滿時延遲新的郵件。最佳作法是啟用此設定，並使佇列限制保持在建議的預設臨界值以下。

請參閱第 48 頁的「架構 SMTP 進階設定」。

如果您遇到郵件佇列問題，請嘗試執行下列動作：

- 確認下游傳送主機正在運行和接受郵件。
  請參閱第 522 頁的「軟體和服務狀態定義」。
- 架構 MTA 以拒絕內送郵件。
  請參閱第 63 頁的「服務與 MTA 作業」。
- 在佇列達到可接受的限制之前，對其進行觀察和監控。
  請參閱第 550 頁的「檢視佇列的郵件」。

重複執行上述措施，直到解決問題為止。

監控已排程工作

表 22-24 描述了您如何監控已排程工作。您可以視需要以任何順序執行這些工作。

表 22-24 監控已排程工作

工作	說明
瞭解可排程為自動發生的 Symantec Messaging Gateway 工作。	Symantec Messaging Gateway 具有一些自動化工作和已排程工作，您可以透過控管中心進行架構。無法完成已排程工作時，Symantec Messaging Gateway 會提供含有失敗相關詳細資料的電子郵件警示選項。如果啟用電子郵件警示選項，系統將在控管中心任何的已排程工作失敗時通知指定的管理員。 請參閱第 556 頁的「關於已排程工作」。
排程工作為自動執行。	每個已排程工作都會顯示開始時間、完成時間以及下一次執行該工作的時間。 請參閱第 556 頁的「已排程工作類型」。

工作	說明
設定在已排程工作失敗時進行通知的警示。	如果工作失敗，就會向指定的管理員傳送電子郵件通知，指出哪項工作失敗以及是在哪個主機上發生。控管中心日誌可提供有關失敗的進一步詳細資料。 請參閱第 590 頁的「架構警示」。

關於已排程工作

Symantec Messaging Gateway 具有一些自動化工作和已排程工作，您可以透過控管中心進行架構。在**「狀態」**標籤下，可檢視及追蹤已排程工作的狀態。已排程工作會依據關聯的工作類型分至不同的子標籤。各個子標籤頁面都包含已排程工作的名稱及狀態。如果成功完成工作，表格會顯示開始時間、結束時間，以及下一個已排程工作的執行時間。如果無法完成工作，**「已完成」**欄會顯示**「已失敗」**的狀態。

無法完成已排程工作時，Symantec Messaging Gateway 會提供含有失敗相關詳細資料的電子郵件警示選項。如果啟用電子郵件警示選項，系統將在控管中心任何的已排程工作失敗時通知指定的管理員。

系統會追蹤下列類型的已排程工作：

- 備份
- 清除程式
- 通知
- 隔離所
- 報告
- 喜好設定

請參閱第 556 頁的「已排程工作類型」。

請參閱第 590 頁的「架構警示」。

已排程工作類型

Symantec Messaging Gateway 有許多自動化和已排程工作。您可以在**「狀態」>「系統」>「已排程工作」**頁面上，檢視所有控管中心工作的狀態。

工作會依照類型，以下列標籤來分組：

- 備份
- 清除程式
- 通知
- 隔離所

- 報告
- 喜好設定

您會在每個標籤下看見包含相關工作表格的頁面。每個已排程工作都會顯示開始時間、完成時間以及下一次執行該工作的時間。如果工作因任何原因而失敗，則**「已完成」**欄位中就會顯示**「已失敗」**一詞。

您可以設定在已排程工作失敗時進行通知的警示。

「備份」標籤可報告建立控管中心資料庫或資料庫組態 (例如內容過濾郵件、事件、日誌以及報告) 之副本的工作。

附註：新增備份組態之前，此表格都是空白。

表 22-25 備份

工作	說明
備份	請參閱第 606 頁的「排程備份」。

「清除程式」標籤可報告從控管中心儲存庫刪除資料 (例如垃圾郵件隔離所中的郵件、日誌資料庫中的日誌檔、報告以及內容事件資料夾中的資料) 之工作。

表 22-26 清除程式

工作	說明
垃圾郵件清除程式	請參閱第 247 頁的「指定垃圾郵件隔離所的清除時間與頻率」。
日誌清除程式	請參閱第 531 頁的「管理日誌資料庫大小」。
報告清除程式	
內容清除程式	請參閱第 365 頁的「排程內容事件資料夾清除程式」。

「通知」標籤可報告自動產生電子郵件傳送給系統管理員的工作，例如有關系統變更或可能需要注意之狀況的警示。

表 22-27 通知

工作	說明
警示通知	請參閱第 590 頁的「架構警示」。
內容過濾通知 (資訊事件)	請參閱第 368 頁的「建立事件通知」。

工作	說明
內容過濾通知 (隔離事件)	請參閱第 368 頁的「建立事件通知」。
垃圾郵件通知	請參閱第 257 頁的「指定通知使用者其隔離所中有垃圾郵件的時間」。

「隔離所」標籤可報告釋放隔離之可疑病毒的工作。

表 22-28　　隔離所

工作	說明
可疑病毒郵件隔離所釋放	請參閱第 207 頁的「指定可疑病毒郵件保留在隔離所的時間」。

「報告」標籤可報告按指定的間隔執行**「我的最愛報告」**，然後使用電子郵件寄給指定收件者的工作。報告類型包括：摘要、內容過濾、電子郵件訊息、無效收件者、IP 連線、垃圾郵件以及病毒報告。

表 22-29　　報告

工作	說明
報告	請參閱第 497 頁的「將報告排程為自動產生」。

「喜好設定」標籤可報告將目錄資料服務之資料傳播給掃描程式的工作。

表 22-30　　喜好設定

工作	說明
使用者喜好設定	請參閱第 585 頁的「架構一般使用者喜好設定資料的複寫」。

請參閱第 556 頁的「關於已排程工作」。

23

透過控制中心管理產品

本章包含以下主題：

- 管理管理員
- 架構控管中心
- 自訂控管中心內的使用者喜好設定
- 設定警示
- 管理密碼
- 硬體裝置維護
- 關於 Symantec Messaging Gateway 和 Symantec Protection Center
- 管理備份
- 保持產品在最新狀態
- 使用診斷

管理管理員

表 23-1 說明可執行哪些工作來管理管理員。您可以視需要以任何順序執行這些工作。

表 23-1 管理管理員

工作	說明
新增本機管理員 (一次一個)。	新增本機管理員時，請手動輸入使用者資料，然後選取存取層級並啟用特定權限。 請參閱第 564 頁的「設定本機和 LDAP 管理員帳戶」。

工作	說明
新增 LDAP 管理員。	您可以使用 LDAP 目錄結構新增管理員 (逐一或以群組方式) 以授權他們。您可以使用管理政策和政策群組來指派存取層級和啟用特定權限。 請參閱第 564 頁的「設定本機和 LDAP 管理員帳戶」。
請熟悉各層級的管理員擁有哪些權限。	管理員根據其擁有「無」、「檢視」或「修改」權限來存取控管中心的不同頁面。每種類型的有限的管理員權限，均會授與管理員檢視控管中心頁面子集的權限。 請參閱第 566 頁的「管理員權限」。
編輯現有管理員。	您可以視需要，修改現有管理員的權限或資訊。 請參閱第 572 頁的「編輯管理員」。
刪除管理員。	您隨時都可以刪除管理員。不過，刪除管理員之後，就無法再擷取這些設定。如果管理員仍然需要存取控管中心，則您可以考慮修改管理員的權限，而不是刪除管理員。 請參閱第 573 頁的「刪除管理員」。
設定管理員/一般使用者混合型檢視以查看及管理隔離所	您可以為管理員設定混合型檢視，以便他們可以存取自己的一般使用者隔離所及執行管理工作，而不需要另外的憑證。 請參閱第 564 頁的「關於管理員和一般使用者檢視」。

關於使用 LDAP 來源新增及授權管理員

您可以根據您的 LDAP 目錄結構中現有的屬性和群組成員資格來新增管理員。您可以架構管理政策並將政策指定給以 LDAP 為基礎的群組。您也可以將預設政策指派給現有的管理員 (稱為「本機」，因為過去是以手動方式或從本機新增至控管中心)。您可以建立新政策並套用至個人或群組。現有的管理員會保留他們升級前的權限，這些權限對應至五個預設管理政策。

使用 LDAP 組群新增及架構管理員的帳戶 (必要工作)

您必須執行下列工作，從 LDAP 結構新增及授權管理員。請務必按順序執行工作。

工作	說明
架構目錄資料來源 (DDS)	若要使用 LDAP 目錄新增管理員，首先要建立新的資料來源或是架構現有的資料來源，以啟用驗證和位址解析。 您必須在同時啟用了驗證與位址解析的情況下架構 DDS。在**「驗證」**標籤中，啟用控管中心的驗證。在**「位址解析」**標籤中，啟用電子郵件掃描的授權。

工作	說明
建立管理政策群組	將新增的以 LDAP 為基礎的管理員或現有的本機管理員指派到使用五個預設管理政策之一的政策群組： ■ **完整**：檢視並修改所有控管中心和掃描程式功能 ■ **監控**：檢視狀態、日誌、報告、政策和設定 ■ **完整報告**：檢視及修改報告 ■ **隔離所**：檢視及修改垃圾郵件和病毒隔離所 ■ **內容控管**：檢視及修改資訊事件資料夾和隔離事件資料夾 您也可以從頭開始建立新的管理政策，或是複製並修改其中一個預設政策。然後可以將這些政策指派到管理政策群組。
新增成員	您可以在**「管理」>「政策群組」>「編輯政策群組」>「成員」**標籤中，新增成員至管理政策群組。按下**「新增」**按鈕即可顯示**「新增政策群組成員」**頁面。 透過輸入電子郵件地址或 LDAP 辨別名稱，或是透過指定「組織單位」(OU) 的 LDAP 辨別名稱或「配置區」項目來新增群組成員。OU 路徑所構成的子樹狀結構中的任何使用者項目也會新增到群組。
啟用管理政策	將成員新增至管理政策群組後，瀏覽至**「管理」>「政策群組」>「編輯政策群組」>「成員」**標籤，然後勾選**「為此政策群組啟用管理政策」**方塊。接著從下拉式清單中選取管理政策，然後按下**「儲存」**。
確認管理政策優先於管理員所屬的所有其他政策	政策生效的優先順序，是以它們在**「管理」>「政策群組」**標籤上清單中的位置而定。管理政策必須排在清單中的第一位，才能確保管理員接收到您為其指定的權限。如果管理政策群組不是在清單中的第一位，請按下群組名稱加以選取並拖曳至位置，將其移至清單的第一位。

使用 LDAP 組群新增及架構管理員的帳戶 (選擇性工作)

如有需要，您可以執行下列工作來啟用與 LDAP 群組相關的功能 (一般使用者隔離所、通知和警示，以及將政策套用至個別管理員)。您可以任何順序執行這些工作。

工作	說明
架構一般使用者隔離所	您必須在兩處位置啟用一般使用者隔離所 (在**「垃圾郵件」>「隔離所設定」>「一般使用者設定」**標籤中全域啟用，以及在**「管理」>「使用者」>「新增政策群組」>「一般使用者」**標籤中針對特定政策群組啟用)，才能允許政策群組的成員存取一般使用者隔離所。 若要為政策群組啟用一般使用者隔離所，您必須先為「控管中心驗證」和「僅電子郵件位址解析」架構目錄資料來源 (位於**「管理」>「設定」>「目錄整合」>「編輯目錄資料來源」>「驗證」**和**「位址解析」**標籤)。 **更新注意事項** 控管中心的管理員同時也是使用者，因此他們也必須可以檢視及管理其自己的隔離所。在本版之前的版本中，管理員需要兩個不同的登入資訊 (管理員和使用者登入資訊，均不以 LDAP 結構為基礎) 才能存取其隔離所。此版本採用「混合型檢視」，讓管理員可以使用單一LDAP 型帳戶來同時執行管理工作及存取自己的一般使用者隔離所。
架構內容事件通知	如果您希望內容事件通知都可以傳送至管理政策群組，請在**「內容」>「設定」>「內容事件資料夾」>「編輯內容事件資料夾」**標籤中為每個政策群組指定 DL。
架構電子郵件警示	如果您希望電子郵件警示可以傳送至管理政策群組，請在**「管理」>「設定」>「警示」**標籤中為每個政策群組指定 DL。
將管理政策套用至不屬於政策群組的本機管理員	您不用為每個本機管理員指定權限，而是可以在**「管理」>「使用者」>「管理員」>「新增管理員」**頁面上，將可以套用於管理政策群組的相同管理政策套用至本機管理員。

關於預設管理政策

SMG 會使用預先架構的管理政策進行安裝。預設會啟用這些政策，您可以將這些政策套用至政策群組。您可以停用或修改政策動作，以及套用政策的政策群組。對於標示為預設的預先架構管理員政策，您不能修改其政策名稱和管理員權限。不過，您可以複製並修改預設政策，然後將它們套用至政策群組。

如果某個特定管理員屬於多個政策群組，則只會套用至具有最高群組優先權的群組。政策群組優先權由「政策群組」頁面上的群組順序決定。

如果管理員權限(通常可允許修改其他權限)不是清單中的第一位，則政策群組優先權可能導致意外結果。例如，請考慮下列情景。管理員是兩個政策群組的成員，具有如下權限：

群組名稱	權限
所有 IT	垃圾郵件：刪除 病毒：刪除 內容過濾：刪除 管理員權限：無
Symantec Messaging Gateway 管理員	垃圾郵件：新增標頭 病毒：隔離 內容過濾：正常傳送 管理員權限：完整檢視及修改

屬於這兩個群組的管理員 (若群組是按此順序列出) 將無法登入 SMG，因為授予該權限的政策群組列在拒絕該權限的政策群組之下。

預設政策群組始終為清單中的最後一個群組。您無法變更預設政策群組的優先度。

表 23-2 列出由每個預設管理政策授予的權限。

表 23-2 預設管理政策

政策名稱	管理員權限
完整管理權限	檢視及修改： ■ 狀態和日誌 ■ 報告 ■ 政策 ■ 設定 ■ 管理員 ■ 垃圾郵件提交 ■ 隔離所 ■ 資訊事件資料夾 ■ 隔離事件資料夾
監控存取	■ 狀態和日誌 ■ 報告 ■ 政策 ■ 設定
完整報告權限	修改： ■ 報告

政策名稱	管理員權限
隔離所管理權限	修改： ■ 管理垃圾郵件隔離所 ■ 管理病毒隔離所 ■ 管理垃圾郵件隔離所 ■ 管理病毒隔離所
內容控管管理權限	■ 資訊事件資料夾 ■ 隔離事件資料夾

請參閱第 168 頁的「編輯、刪除、啟用或停用政策群組」。

請參閱第 175 頁的「設定政策群組優先度」。

請參閱第 166 頁的「研究使用者所屬的政策群組」。

請參閱第 163 頁的「產生政策群組」。

請參閱第 165 頁的「匯入及匯出政策群組成員」。

關於管理員和一般使用者檢視

系統可將隔離所管理權限授予控管中心管理員，以便他們管理所有使用者的隔離所。不過，如果管理員沒有這些權限，他們仍然必須可以檢視及管理自己個人的隔離所 (在已啟用一般使用者隔離所的情況下)。Symantec Messaging Gateway 支援兩種檢視 (**「管理員檢視」**和**「一般使用者檢視」**)，可讓管理員檢視及管理自己的隔離所，不論其對於隔離所的管理員權限為何。

若要取得混合型檢視的存取權，管理員必須是 LDAP 型帳戶 (即已在目錄資料來源中架構驗證和位址解析)，而不是本機帳戶 (在控管中心內手動輸入電子郵件地址和主機)。如果您希望現有的本機管理員可以存取此功能，請將他們新增至 LDAP 群組。請參閱第 564 頁的「設定本機和 LDAP 管理員帳戶」。

必須同時全域啟用 (在**「垃圾郵件」>「隔離所設定」>「一般使用者設定」**頁面上架構)，以及針對每個群組啟用 (在**「政策群組」>「編輯政策群組的一般使用者」**標籤中架構) 一般使用者隔離所。如果只嘗試在其中一處啟用一般使用者隔離所，則您會收到警告訊息。若未啟用一般使用者隔離所，則只有具有檢視及管理隔離所權限的管理員可以檢視及管理隔離所，而且只會顯示「管理員」檢視。

請參閱第 242 頁的「架構一般使用者隔離所」。

設定本機和 LDAP 管理員帳戶

新增管理員時，必須選取存取層級並啟用特定權限。您可以一次設定一個或一組管理員的帳戶。您可以手動輸入資訊來新增本機管理員，也可以使用 LDAP 目錄結構中現有的資訊來新增管理員。

設定本機管理員的帳戶

您可以手動輸入使用者資料，來新增本機管理員。輸入管理員的資訊後，您可以將現有的管理政策套用至該管理員，也可以建立新的自訂政策。請遵循下列步驟，新增單一管理員並指派可指定管理員權限的管理政策。

設定本機管理員的帳戶

1. 在控管中心內，按下**「管理」>「使用者」>「管理員」**。
2. 按下**「新增」**。
3. 在**「使用者名稱」**方塊中，輸入使用者名稱 (使用 US ASCII 字元)。
4. 在**「密碼」**方塊中，輸入密碼。
5. 在**「確認密碼」**方塊中，再次輸入密碼加以確認。
6. 在**「電子郵件地址」**方塊中，輸入管理員的電子郵件地址。
7. 如果希望這位管理員收到系統警示，請勾選**「接收警示通知」**。
8. 在**「內容事件資料夾通知」**中，選擇此管理員應在哪些資料夾中的事件增加時收到通知：

資料夾	選取/取消選取所有內容事件資料夾 (資訊和隔離)
資訊事件	僅選取/取消選取資訊事件資料夾
隔離事件	僅選取/取消選取隔離事件資料夾

9. 在**「管理政策」**區域中，進行下列任一操作：
   - 從清單中選擇現有的管理政策。
   - 輸入您要建立之新管理政策的名稱，然後輸入政策的說明。

   新增管理政策後，請選擇要指派給新政策的管理權限，如下所示：

完整的管理權限	按下**「完整的管理權限」**，可讓管理員檢視和修改所有可用的權限。
有限的管理權限	按下**「有限的管理權限」**，為這位管理員選擇特定的權限，如下所示： ■ 無 管理員對於選取的工作或內容事件資料夾均沒有任何權限。 ■ 檢視 管理員可以檢視適當的頁面和內容事件資料夾，但無法管理它們。 ■ 修改 管理員具有檢視及修改選取之工作和內容事件資料夾的完整權限。 請參閱第 566 頁的「管理員權限」。

會套用完整管理權限和有限管理權限的系統功能	■ 狀態和日誌 ■ 報告 ■ 政策 ■ 設定 ■ 管理 ■ 垃圾郵件提交 ■ 隔離所 ■ 資訊事件資料夾 ■ 隔離事件資料夾

10 如果這是新的管理政策，則為政策選擇內容事件資料夾存取：

資訊事件	管理員可以在指出的內容事件資料夾中檢視事件，但無法對其進行管理。具有「檢視」權限的管理員，無法對指定的內容事件資料夾中的事件執行任何動作。
隔離事件	管理員可以檢視和修改指定之內容事件資料夾中的所有事件。

11 按下**「儲存」**。

設定 LDAP 管理員的帳戶

若要使用 LDAP 目錄新增管理員，首先要建立新的資料來源或是架構現有的資料來源，以啟用驗證和位址解析。請參閱第 426 頁的「新增資料來源」。

架構好資料來源後，請依照下列的步驟新增 LDAP 管理員。

設定 LDAP 管理員的帳戶

◆ 在控管中心內，按下**「管理」>「使用者」>「政策群組」**，然後進行下列任一操作：

- 如果您要向其新增管理員的政策群組已經存在，請按下它加以選取，然後按下**「新增」**。此時會顯示**「編輯政策群組」**頁面。請參閱第 164 頁的「新增成員至政策群組」。
- 如果您要向其新增管理員的政策群組並不存在，請在未選取任何群組名稱的情況下按下**「新增」**。此時會顯示**「編輯政策群組」**頁面。請參閱第 163 頁的「產生政策群組」。
- 將成員新增到政策群組後，請按下**「管理」**標籤，然後為群組啟用並選取「管理」政策。若要變更管理政策的特定權限，請按下**「管理」>「政策」>「管理」**，接著選擇政策，然後按下**「編輯」**。視需要編輯管理政策。

管理員權限

具有「完整的管理權限」的管理員可以檢視、存取及修改控管中心的任何頁面。

您可以將具有下列存取權的「有限的管理權限」授予管理員：

無	管理員沒有執行所選工作的任何權限，無法檢視對應的頁面。
檢視	管理員可以檢視適當的頁面，但無法管理它們。
修改	管理員具有檢視與修改工作的完整權限。

每種類型的有限的管理員權限，均會授與管理員檢視控管中心頁面子集的權限。您可以將「有限的管理權限」授予以下功能：

- 狀態和日誌
- 報告
- 政策
- 設定
- 管理
- 垃圾郵件提交
- 隔離所

此外，在**「內容事件資料夾」**下，可以針對所建立的每個內容事件資料夾，選擇**「無」**、**「檢視」**或**「修改」**。您也可以為任何內容事件資料夾勾選**「接收事件通知」**。

沒有**「完整的管理權限」**或**「管理中心」**權限的任何管理員都可看到**「管理」>「使用者」>「管理員」**頁面。但管理員只能在該頁面上變更自己的密碼。只有具有「完整的管理權限」的管理員才能修改具有「完整的管理權限」的其他管理員。

附註：若要檢視或修改內容資安事端資料夾的內容，對於**「新增管理員」**或**「編輯管理員」**頁面的**「內容資安事端資料夾」**下的資料夾，您必須擁有**「檢視」**或**「修改」**權限。許多類型的受限管理員權限可讓您檢視所有內容資安事端資料夾的頁面，而不是這些資料夾的內容。

表 23-3 顯示具有**「管理狀態和日誌」**檢視或修改權限之管理員可用的頁面。

表 23-3 「管理狀態和日誌」頁面

標籤	功能表	頁面
狀態	系統	■ 控制面板 ■ 主機 ■ 日誌 ■ 已排程工作
狀態	SMTP	■ 郵件稽核日誌 ■ 郵件佇列
狀態	提交	提交詳細資料

標籤	功能表	頁面
內容	事件管理	■ 內容事件資料夾總覽 ■ 資訊事件 ■ 隔離事件 當管理員沒有適當的權限檢視事件資料夾的內容時，會顯示以下訊息： 「您沒有足夠的權限，無法檢視這些內容過濾事件。請聯絡系統管理員，以取得此內容事件資料夾的存取權。」
管理	使用者	管理員
管理	設定	日誌
管理	主機	■ 組態 ■ 授權 ■ 公用程式

表 23-4 顯示具有「**管理報告**」檢視或修改權限之管理員可用的頁面。

表 23-4 「管理報告」頁面

標籤	功能表	頁面
報告	檢視	■ 建立報告 ■ 我的最愛報告
內容	事件管理	當管理員沒有適當的權限檢視事件資料夾的內容時，會顯示以下訊息： 「您沒有足夠的權限，無法檢視這些內容過濾事件。請聯絡系統管理員，以取得此內容事件資料夾的存取權。」
管理	使用者	管理員
管理	設定	報告

表 23-5 顯示具有「**管理政策**」檢視或修改權限之管理員可用的頁面。

表 23-5 「管理政策」頁面

標籤	功能表	頁面
信譽	政策	■ 攔截的寄件者 ■ 連線類別 ■ 允許的寄件者
信譽	信譽工具	■ 尋找寄件者 ■ IP 信譽查詢
垃圾郵件	政策	電子郵件
垃圾郵件	設定	寄件者驗證
惡意軟體	政策	電子郵件
威脅防禦	政策	電子郵件
內容	政策	電子郵件
內容	資源	■ 註釋 ■ 附件清單 ■ 辭典 ■ 通知 ■ 樣式 ■ 記錄
管理	使用者	■ 管理員 ■ 尋找使用者 ■ 政策群組

表 23-6 顯示具有「**管理設定**」檢視或修改權限之管理員可用的頁面。

表 23-6 「管理設定」頁面

標籤	功能表	頁面
通訊協定	**SMTP**	■ 位址偽裝 ■ 別名 ■ 網域 ■ 無效收件者 ■ 設定

標籤	功能表	頁面
垃圾郵件	設定	■ 探查帳戶 ■ 隔離所設定 ■ 掃描設定 ■ 提交設定
惡意軟體	設定	■ LiveUpdate ■ 掃描設定 ■ 可疑病毒設定
威脅防禦	設定	■ CA 連線 ■ 掃描設定
威脅防禦	SMTP	CA 佇列
內容	設定	■ 封存 ■ 內容加密 ■ 內容事件資料夾 ■ DLP 連線 當管理員沒有適當的權限檢視事件資料夾的內容時，會顯示以下訊息： 「您沒有足夠的權限，無法檢視這些內容過濾事件。請聯絡系統管理員，以取得此內容事件資料夾的存取權。」
管理	使用者	管理員
管理	設定	■ 警示 ■ 憑證 ■ 控管中心 ■ 目錄整合 ■ 日誌 ■ 報告 ■ SNMP ■ UPS
管理	主機	組態

表 23-7 顯示具有「**管理監管**」檢視或修改權限之管理員可用的頁面。

表 23-7 「管理中心」頁面

標籤	功能表	頁面
管理	使用者	■ 管理員 ■ 一般使用者
管理	主機	■ 授權 ■ 關閉 ■ 版本
內容	資訊管理	■ 資訊事件 ■ 隔離事件 當管理員沒有適當的權限檢視事件資料夾的內容時，會顯示以下訊息： 「您沒有足夠的權限，無法檢視這些內容過濾事件。請聯絡系統管理員，以取得此內容事件資料夾的存取權。」

表 23-8 顯示具有**「管理提交」**檢視或修改權限之管理員可用的頁面。

表 23-8 管理垃圾郵件提交頁面

標籤	功能表	頁面
狀態	系統	控制面板
狀態	提交	提交詳細資料
垃圾郵件	設定	提交設定
垃圾郵件	提交	提交郵件
內容	事件管理	■ 資訊事件 ■ 隔離事件 ■ 自訂內容事件資料夾 當管理員沒有適當的權限檢視事件資料夾的內容時，會顯示以下訊息： 「您沒有足夠的權限，無法檢視這些內容過濾事件。請聯絡系統管理員，以取得此內容事件資料夾的存取權。」

標籤	功能表	頁面
管理	使用者	管理員

表 23-9 顯示具有「**管理隔離所**」檢視或修改權限之管理員可用的頁面。

表 23-9 「管理隔離所」頁面

標籤	功能表	頁面
垃圾郵件	設定	隔離所設定
垃圾郵件	隔離所	垃圾郵件
病毒	設定	可疑病毒設定
病毒	隔離所	電子郵件可疑病毒
內容	事件管理	■ 資訊事件 ■ 隔離事件 ■ 自訂內容事件資料夾 當管理員沒有適當的權限檢視事件資料夾的內容時，會顯示以下訊息： 「您沒有足夠的權限，無法檢視這些內容過濾事件。請聯絡系統管理員，以取得此內容事件資料夾的存取權。」
管理	使用者	管理員

請參閱第 564 頁的「設定本機和 LDAP 管理員帳戶」。

編輯管理員

您可以編輯管理員，以修改下列任一項目：

- 管理員的名稱
- 管理員的電子郵件地址
- 管理員的密碼
- 管理員是否接收通知
- 管理員的權限
  請參閱第 566 頁的「管理員權限」。
- 管理員是否接收有關內容事件資料夾事件的通知

請參閱第 564 頁的「設定本機和 LDAP 管理員帳戶」。

編輯管理員

1 在控管中心內，按下**「管理」>「使用者」>「管理員」**。

2 從清單中選取管理員並按下**「編輯」**。

3 視需要變更管理員的定義。

4 按下**「儲存」**。

刪除管理員

您隨時都可以刪除管理員。不過，刪除管理員之後，就無法再擷取這些設定。如果管理員仍然需要存取控管中心，則您可以考慮修改管理員的權限，而不是刪除管理員。

請參閱第 572 頁的「編輯管理員」。

刪除管理員

1 在控管中心內，按下**「管理」>「使用者」>「管理員」**。

2 勾選您要移除之管理員旁的方塊。

3 按下**「刪除」**。

4 在確認對話方塊中，按下**「確定」**以確認刪除。

架構控管中心

控管中心是一種採用瀏覽器架構的應用程式，是存取 Symantec Messaging Gateway 系統的介面。

表 23-10 說明您可架構控管中心的方式。您可以視需要以任何順序執行這些工作。

表 23-10 架構控管中心

工作	說明
瞭解多位使用者如何可以同時存取控管中心。	多個一般使用者可以同時存取控管中心，例如檢閱「垃圾郵件隔離所」中的郵件。多個管理員可以同時存取控管中心，並執行管理工作。 請參閱第 575 頁的「關於同時存取控管中心」。
瞭解如何讓用戶端連線至控管中心。	在指定可存取控管中心的主機名稱時，啟用控制中心可讓用戶端依據控管中心的 DNS 信息進行連線。若用戶端的 IP 位址解析後的名稱符合允許的主機名稱 (「反向查詢」)，則控管中心允許存取此用戶端。 請參閱第 576 頁的「關於指定可存取控管中心的主機名稱」。

工作	說明
指定允許存取控管中心的主機。	您可透過網頁瀏覽器存取控管中心。根據預設，擁有正確位址與登入資訊的使用者可從任何主機進行存取，但您也可以選擇指定哪些主機可以存取控管中心。嘗試經由未經授權電腦登入控管中心的使用者，將會在其網頁瀏覽器中收到「403 禁止」頁面訊息。您必須啟動 DNS 軟體中的反向網域名稱伺服器 (DNS) 查詢，此功能才能搭配主機名稱使用。 請參閱第 576 頁的「指定哪些主機可以存取控管中心」。
透過 SNMP 監控控管中心事件。	簡易網路管理通訊協定 (SNMP) 可讓管理員監控網路裝置 (例如控管中心和掃描程式)。您可以指定 SNMP 社群字串和陷阱。您也可以管理環境中多達四部主機的 SNMP 代理程式存取權限。如果您啟用 SNMP v3，則還可以指定驗證和加密設定。 請參閱第 577 頁的「架構 SNMP 設定以監控網路裝置」。
視需要變更接聽程式通訊埠。	依據預設，垃圾郵件隔離所、可疑病毒隔離所和內容資安事端資料夾均接受通訊埠 41025 上來自掃描程式的郵件。不過，您可以視需要變更此通訊埠。您不需要變更任何掃描程式設定即可符合接聽程式通訊埠的變更。您也可以停用接聽程式通訊埠。 請參閱第 578 頁的「架構控管中心接聽程式通訊埠」。
安裝自行簽署的憑證或 CA 簽署的憑證，以用於控管中心存取。	控管中心預設會使用示範憑證，來驗證對控管中心的存取。當您存取控管中心時，示範憑證會使瀏覽器出現安全警告。您可以忽略安全警告，並繼續存取控管中心。但是，也可以安裝憑證，以加強瀏覽器到控管中心的通訊安全性，以避免出現這類安全警告。 請參閱第 579 頁的「存取控管中心時略過安全警告」。
透過控管中心指定使用者介面 HTTPS 憑證。	此憑證可強化控管中心以及登入控管中心之人員的安全性。 請參閱第 580 頁的「指定控管中心憑證」。
使用「地區設定」，架構控管中心使用單位元組與雙位元組字元集，以及適當的數字、日期與時間設定。	例如，「地區設定」會影響控管中心所傳送的電子郵件訊息 (如通知、警示與報告) 的格式。 當語言識別功能無法正確判定隔離之電子郵件訊息的語言時，您也可以選取「遞補語言編碼」選項供控管中心使用。 請參閱第 580 頁的「設定地區設定編碼與遞補語言編碼」。
轉換 8 位元 MIME 郵件。	如果 MTA 發生問題，無法處理 8 位元 MIME 時，您可以強制傳送的 MTA 將 8 位元 MIME 郵件轉換為 7 位元 MIME。 請參閱第 581 頁的「將 8 位元 MIME 郵件轉換為 7 位元 MIME」。
修改預設日期格式與時間格式。	Symantec Messaging Gateway 會在安裝時使用預設的日期與時間格式。不過，您可以修改這些格式。 請參閱第 581 頁的「自訂日期格式與時間格式」。 請參閱第 582 頁的「日期格式與時間格式樣式語法」。

架構控管中心設定

表 23-11 架構控管中心設定的程序

步驟	動作	說明
步驟 1	設定主機與用戶端對應。	指定主機名稱以啟用反向 DNS 查詢。 請參閱第 576 頁的「關於指定可存取控管中心的主機名稱」。 指定哪些電腦或網路可以存取控管中心。 請參閱第 576 頁的「指定哪些主機可以存取控管中心」。
步驟 2	提高控管中心的安全性。	指定使用者介面憑證 HTTPS。 請參閱第 580 頁的「指定控管中心憑證」。 修改預設示範憑證以避免出現安全性警告。 請參閱第 579 頁的「存取控管中心時略過安全警告」。
步驟 3	修改預設設定。	變更或停用接聽程式通訊埠。 請參閱第 578 頁的「架構控管中心接聽程式通訊埠」。 為產品產生的警示與報告通知指定主機設定。 請參閱第 595 頁的「架構警示和報告的控管中心 SMTP 設定」。 為單位元組與雙位元組字元集以及數字、日期與時間設定架構控管中心。 請參閱第 580 頁的「設定地區設定編碼與遞補語言編碼」。
步驟 4	自訂使用者登入體驗。	自訂**「登入說明」**頁面。 請參閱第 584 頁的「指定自訂使用者登入說明頁面」。 啟用「記住我」功能以自動登入。 請參閱第 584 頁的「讓使用者略過控管中心登入憑證」。 將使用者喜好設定擴充到附加的掃描程式。 請參閱第 585 頁的「架構一般使用者喜好設定資料的複寫」。

關於同時存取控管中心

多個一般使用者可以同時存取控管中心，例如檢閱「垃圾郵件隔離所」中的郵件。

多個管理員可以同時存取控管中心，並執行管理工作。但是在某些情況下，每個管理員可能均會發現錯誤。特別是在各管理員在控管中心同時嘗試執行耗費大量資源的工作時，會發生錯誤。例如，同時查詢郵件稽核日誌和 IP 信譽時，會產生錯誤。

請參閱第 575 頁的「架構控管中心設定」。

關於指定可存取控管中心的主機名稱

在指定可存取控管中心的主機名稱時，啟用控制中心可讓用戶端依據控管中心的 DNS 信息進行連線。若用戶端的 IP 位址解析後的名稱符合允許的主機名稱 (「反向查詢」)，則控管中心允許存取此用戶端。控管中心會解析並同時接受 IPv4 位址範圍與 IPv6 位址範圍進行存取控管。

網段 (通常屬於相同組織的 IP 位址範圍) 的擁有者控制 IP 位址的反向查詢。使用者通常無法控制其 IP 位址解析後的名稱。此外，DNS 伺服器可能有相同網段的唯一對應。

請注意以下資訊：

- 在用戶端的授權 DNS 伺服器中，用戶端 IP 位址的反向查詢記錄是 `m1.symantecexample.com`。
- 在架構為控管中心主要 DNS 伺服器的 DNS 中，具有同一 IP 位址的 `dhcp23.symantecexample.com` 之反向對應。

在此情況下，只要用戶端進行連線，控管中心就會看到 `dhcp23.symantecexample.com` 名稱。因此，控管中心看到的名稱，就是您在控管中心的主機存取控制清單中輸入的名稱。相較於公用 Internet，這種情形在私有網路上更常發生。

請參閱第 576 頁的「指定哪些主機可以存取控管中心」。

指定哪些主機可以存取控管中心

您可透過網頁瀏覽器存取控管中心。根據預設，擁有正確位址與登入資訊的使用者可從任何主機進行存取，但您也可以選擇指定哪些主機可以存取控管中心。嘗試經由未經授權電腦登入控管中心的使用者，將會在其網頁瀏覽器中收到「403 禁止」頁面訊息。

您必須啟動 DNS 軟體中的反向網域名稱伺服器 (DNS) 查詢，此功能才能搭配主機名稱使用。

請參閱第 576 頁的「關於指定可存取控管中心的主機名稱」。

附註：如果您在輸入主機名稱時發生錯誤，則會完全攔截對控管中心的存取權。如果發生此情形，請使用指令行指令 `delete bcchostacl` 來清除允許存取控管中心之電腦的清單。

請參閱第 647 頁的delete。

指定哪些主機可以存取控管中心

1 在控管中心內，按下「**管理**」>「**設定**」>「**控管中心**」。

2 按下「**存取**」標籤。

3 在「**控管中心存取**」下方，執行下列其中一項工作：

若要允許任何主機存取控管中心	勾選「**所有主機**」。
若要指派特定主機來存取控管中心	勾選「**僅限下列主機**」，然後輸入主機名稱、IP 位址、含子網路遮罩的 IP 位址或 Classless Inter-Domain Routing (CIDR) 網段。 視需要指定額外的電腦或網路。不在此清單中的主機無法存取控管中心。 支援 IPv4 位址和 IPv6 位址。

4 按下「**新增**」。

5 按下「**儲存**」。

架構 SNMP 設定以監控網路裝置

簡易網路管理通訊協定 (SNMP) 可讓管理員監控網路裝置 (例如控管中心和掃描程式)。您可以指定 SNMP 社群字串和陷阱。您也可以管理環境中多達四部主機的 SNMP 代理程式存取權限。如果您啟用 SNMP v3，則還可以指定驗證和加密設定。

在您架構 SNMP 設定之前，必須先下載「管理資訊基礎 (MIB)」資料庫，並將它匯入至 SNMP 用戶端。

如需有關如何查詢和測試 Messaging Gateway 10.x 最相關的 SNMP 物件識別碼 (OID) 的資訊，請移至 https://support.symantec.com/en_US/article.TECH227540.html。

架構 SNMP 設定以監控網路裝置

1 在控管中心內，按下「**管理**」>「**設定**」> **SNMP**。

2 在「**伺服器**」標籤中，請勾選「**啟用 SNMP**」。

3 在「**SNMP 陷阱主機 IP 位址**」方塊中，輸入接收 SNMP 陷阱警示之裝置的 IP 位址。

不支援完整網域名稱 (FQDN)。

4 在「**SNMP 接聽通訊埠**」方塊中，輸入 SNMP 代理程式接聽網路流量所在的通訊埠。

5 按下「**版本**」標籤。

6 勾選所要使用的版本。

您可以選擇 SNMP v2、SNMP v3 或兩者都選。如果只選擇 SNMP v3，請跳至步驟 12。

7 在「**SNMP 社群字串**」方塊中，輸入 SNMP 代理程式的社群字串。

8 在「**SNMP 用戶端存取**」下，執行下列其中一項工作，以指定可以存取 SNMP 代理程式的主機：

- 按下「**所有主機**」，以授予所有主機存取 SNMP 用戶端的權限。
- 按下「**僅限下列主機**」。然後，輸入您希望對 SNMP 用戶端有存取權的特定主機 IP 位址、主機名稱或 CIDR 範圍。

9 按下「**新增**」。

10 您可以勾選目前啟用 SNMP 存取之主機名稱旁的方塊，再按下「**刪除**」，以刪除這些主機。

11 如果沒有選擇 SNMP v3，請按下「**儲存**」。如果選擇了 SNMP v3，請繼續進行以下步驟。

12 按下以選擇「**驗證類型**」。

您可以選擇訊息摘要演算法 5 (MD5) 或安全雜湊演算法 (SHA)。

13 在「**驗證使用者名稱**」欄位中，輸入使用者名稱。

14 在「**驗證密碼**」欄位中，輸入密碼。

密碼長度必須至少有八個字元。

15 在「**確認密碼**」欄位中再次輸入密碼。

16 如果您要使用加密，請按下「**啟用 SNMP v3 加密**」。

17 按下以選擇「**加密類型**」。

您可以選擇進階加密標準 (AES) 或資料加密標準 (DES)。

18 在「**加密密碼**」欄位中，輸入密碼。

密碼長度必須至少有八個字元。

19 在「**確認密碼**」欄位中再次輸入密碼。

20 在 **MIB** 標籤中，按下 **SNMP MIB**。

21 按下 MIB 進行下載。將 MIB 匯入 SNMP 用戶端。

22 按下「**儲存**」。

架構控管中心接聽程式通訊埠

依據預設，垃圾郵件隔離所、可疑病毒隔離所和內容資安事端資料夾均接受通訊埠 41025 上來自掃描程式的郵件。不過，您可以視需要變更此通訊埠。只有具備「完整的管理」權限或管理設定修改權限的管理員，才能修改這些設定。您不需要變更任何掃描程式設定即可符合接聽程式通訊埠的變更。

您也可以停用接聽程式通訊埠。如果您的電腦沒有防火牆保護，而又擔心安全風險，則可以停用接聽程式通訊埠。 如果停用接聽程式通訊埠，也請停用隔離郵件的任何政策。 否則，已隔離的郵件會備份在傳送郵件流佇列中直到到期為止，然後會退回給原始寄件者。

請參閱第 359 頁的「關於內容事件資料夾」。

請參閱第 239 頁的「關於隔離垃圾郵件」。

請參閱第 204 頁的「關於隔離可疑病毒」。

修改或停用控管中心用來接受郵件的接聽程式通訊埠

1. 在控管中心內，按下**「管理」>「設定」>「控管中心」**。
2. 按下**「接聽程式」**標籤。
3. 在**「通訊埠」**方塊的**「接聽程式通訊埠」**中，執行下列其中一項：
   - 輸入新的通訊埠號。
   - 輸入 **0** 停用接聽程式通訊埠。
4. 按下**「儲存」**。

存取控管中心時略過安全警告

控管中心預設會使用示範憑證，來驗證對控管中心的存取。當您存取控管中心時，示範憑證會使瀏覽器出現安全警告。您可以忽略安全警告，並繼續存取控管中心。但是，也可以安裝憑證，以加強瀏覽器到控管中心的通訊安全性，以避免出現這類安全警告。

請決定您要使用自行簽署的憑證或 CA 簽署的憑證。自行簽署的憑證所提供的安全層級不如 CA 簽署的憑證。若要取得 CA 簽署的憑證，必須將 CSR 傳送至憑證授權中心。

下列程序假設您使用的是 CA 簽署的憑證。

存取控管中心時略過安全警告

1. 在控管中心內新增憑證，並將 CSR 傳送至憑證授權中心以取得憑證。

   請確定 CSR 中的主機名稱符合控管中心的主機名稱。

   請參閱第 151 頁的「要求憑證授權中心簽署的憑證」。
2. 匯入您從憑證授權中心收到的憑證。

   請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。
3. 若有需要，請安裝中繼憑證。

   請參閱第 150 頁的「新增 CA 或中繼憑證」。
4. 將此憑證指派為控管中心 HTTPS 憑證。

   請參閱第 160 頁的「指派使用者介面 HTTPS 憑證給控管中心」。
5. 使用您在 CSR 上提供的完整網域名稱來存取控管中心。

指定控管中心憑證

您可以透過控管中心指定使用者介面 HTTPS 憑證。此憑證可強化控管中心以及登入控管中心之人員的安全性。

請參閱第 579 頁的「存取控管中心時略過安全警告」。

指定控管中心憑證

1. 在控管中心內，按下**「管理」>「設定」>「控管中心」**。
2. 按下**「憑證」**標籤。
3. 在**「控管中心憑證」**下，按下**「使用者介面 HTTPS 憑證」**下拉式清單以選取您要使用的憑證。

   請參閱第 145 頁的「關於憑證」。
4. 按下**「儲存」**。

設定地區設定編碼與遞補語言編碼

使用「地區設定」，架構控管中心使用單位元組與雙位元組字元集，以及適當的數字、日期與時間設定。例如，「地區設定」會影響控管中心所傳送的電子郵件訊息(如通知、警示與報告)的格式。

當語言識別功能無法正確判定隔離之電子郵件訊息的語言時，您也可以選取「遞補語言編碼」選項供控管中心使用。

如果郵件標頭或內文包含下列任何項目時，語言識別即可能失敗：

- 編碼資訊遺失或損毀的原始 8 位元字元
- 較少編碼資訊遺失或損毀的字元
- 僅只少數混用兩種或更多編碼類型的字元

請將遞補語言編碼設定為您所在的地區或國家最常用的編碼。

請參閱第 581 頁的「自訂日期格式與時間格式」。

設定地區設定編碼與遞補語言編碼

1. 在控管中心內，按下**「管理」>「設定」>「控管中心」**。
2. 按下**「地區設定」**標籤。
3. 在**「系統地區設定和遞補語言編碼」**下，按下**「系統地區設定」**下拉式清單並選取編碼。
4. 按下**「隔離遞補語言編碼」**下拉式清單並選取編碼。
5. 按下**「儲存」**。

將 8 位元 MIME 郵件轉換為 7 位元 MIME

如果 MTA 發生問題，無法處理 8 位元 MIME 時，您可以強制傳送的 MTA 將 8 位元 MIME 郵件轉換為 7 位元 MIME。

請參閱第 87 頁的「關於電子郵件訊息流」。

將 8 位元 MIME 郵件轉換為 7 位元 MIME

1. 在控管中心內，按下**「通訊協定」> SMTP >「設定」**。
2. 在 **SMTP** 標籤的**「Mime 處理」**下，勾選**「不公告 8BITMIME」**。
3. 按下**「儲存」**。

自訂日期格式與時間格式

Symantec Messaging Gateway 會在安裝時使用預設的日期與時間格式。不過，您可以修改這些格式。您必須具有「完整的管理」權限或「管理設定」權限，才能修改日期與時間格式。

表 23-12　　架構日期與時間格式

格式	語法與預設值	範例
時間	hh:mm:ss a	02:29:34 PM
簡短日期	MM/dd/yy	2/25/10
完整日期	MMMM dd, yyyy	February 25, 2010
完整日期與時間	EEEE, MMM dd, yyyy hh:mm:ss a zz	Thursday, Feb 25, 2010 01:23:45 PM PST
AM/PM 符號	AM/PM	AM

Symantec Messaging Gateway 會套用您架構的日期格式與時間格式，如下所示：

詳細資料檢視	完整日期與時間
清單檢視	完整日期
信箱	完整日期格式與時間的組合 針對同一天的電子郵件使用時間格式；針對其他所有項目使用完整格式
報告	簡短日期與時間

您可指定的語法長度上限為 32 個字元。32 個字元的限制不包含空格。

請參閱第 582 頁的「日期格式與時間格式樣式語法」。

預設會停用自訂日期格式與時間格式的選項。您必須啟用此功能，才可以修改日期與時間格式。

架構日期格式與時間格式

1 在控管中心內，按下「**管理**」>「**設定**」>「**控管中心**」。

2 按下「**地區設定**」標籤。

3 勾選「**套用自訂日期與時間戳記格式**」。

4 指定您要使用的自訂日期與時間戳記格式。

5 按下「**儲存**」。

日期格式與時間格式樣式語法

表 23-13 提供了支援的日期格式與時間格式語法。

表 23-13 日期與時間格式語法

字母	元件	簡報	美國地區設定範例
G	西元	文字	AD
yyyy；yy	年	年	2010; 10
MMMM；MMM；MM	年中的某個月分	月	July；Jul；07
w	年中的某一週	數字	27
W	月中的某一週	數字	2
DDD	年中的某一日	數字	189
d	月中的某一日	數字	10
F	月中的某一天	數字	2
EEEE；EEE	週中的某一天	文字	Tuesday；Tue
a	AM/PM 標記	文字	PM
H	一天 (24 小時制) 中的某個小時 (0-23)	數字	0
k	一天 (24 小時制) 中的某個小時 (1-24)	數字	24
K	一天中 (12 小時制) 的某個小時 (0-11)	數字	0

字母	元件	簡報	美國地區設定範例
h	一天中 (12 小時制) 的某個小時 (1-12)	數字	12
m	一小時中的某一分鐘	數字	20
s	一分中的某一秒	數字	55
S	毫秒	數字	978
z zz zzzz	時區	時區	Pacific Daylight Time；PDT
Z	時區	RFC822	-0800

請參閱第 581 頁的「自訂日期格式與時間格式」。

自訂控管中心內的使用者喜好設定

表 23-14描述了您要自訂控管中心時，可執行的工作。您可以視需要以任何順序執行這些工作。

表 23-14　　自訂控管中心內的使用者喜好設定

工作	說明
您可以使用自訂登入的「說明」頁面URL來自訂登入說明。	建立一個告訴使用者如何登入的網頁，並讓該網頁在您的網路上可供存取。不論使用者從任何電腦登入，應該都可以存取該網頁。 請參閱第 584 頁的「指定自訂使用者登入說明頁面」。
讓 Symantec Messaging Gateway 將Cookie放在使用者的電腦上，讓使用者能夠略過登入憑證。	Symantec Messaging Gateway 具有一項啟用後可以記住使用者的登入憑證之功能。當管理員啟用記住我功能時，Symantec Messaging Gateway的「登入」頁面會顯示「記住我」選項。如果啟用此功能，則包括一般使用者在內的所有使用者均可使用此功能。 請參閱第 584 頁的「讓使用者略過控管中心登入憑證」。
指定將使用者喜好設定複寫到控管中心的頻率。	在控管中心內，複寫指的是將使用者喜好設定從控管中心傳播到已連接並啟用之掃描程式的程序。控管中心的全域設定會控制複寫程序。 請參閱第 585 頁的「架構一般使用者喜好設定資料的複寫」。

工作	說明
修改預設的 SMTP 問候語與郵件管理員地址。	當 Symantec Messaging Gateway 與其他郵件伺服器連線以起始入埠或離埠郵件流量時，會以問候語開始 SMTP 通訊協定轉換。 您也可以變更郵件管理員地址。Symantec Messaging Gateway 會將郵件管理員地址包含在退回郵件中。 請參閱第 586 頁的「設定 SMTP 問候語與郵件管理員地址」。

指定自訂使用者登入說明頁面

依據預設，當使用者按下**「是否需要登入說明?」**連結 (位於控管中心**「登入」**頁面) 時，會開啟賽門鐵克線上說明視窗。您可以使用自訂登入的「說明」頁面 URL 來自訂登入說明。此項變更僅會影響登入說明頁面，不會影響其他線上說明。

建立一個告訴使用者如何登入的網頁，並讓該網頁在您的網路上可供存取。不論使用者從任何電腦登入，應該都可以存取該網頁。

請參閱第 250 頁的「檢視隔離所中的垃圾郵件與可疑垃圾郵件」。

請參閱第 584 頁的「讓使用者略過控管中心登入憑證」。

指定自訂使用者登入說明頁面

1. 在控管中心內，按下**「管理」>「設定」>「控管中心」**。
2. 按下**「使用者」**標籤。
3. 在**「登入說明 URL」**方塊的**「使用者說明」**下，輸入您要使用之網頁的 URL。

   若要停用自訂的登入說明頁面，請刪除**「登入說明 URL」**方塊中的內容。
4. 按下**「儲存」**。

讓使用者略過控管中心登入憑證

Symantec Messaging Gateway 具有一項啟用後可以記住使用者的登入憑證之功能。當管理員啟用**「記住我」**功能時，Symantec Messaging Gateway 的「登入」頁面會顯示**「記住我」**選項。如果啟用此功能，則包括一般使用者在內的所有使用者均可使用此功能。

如果使用者在登入控管中心時勾選**「記住我」**選項，則 Symantec Messaging Gateway 會在使用者的電腦中置入 Cookie (不會在用戶端電腦或瀏覽器中儲存任何個人資訊)。此後，當使用者存取控管中心的 URL 時，會略過「登入」畫面，並直接移至 Symantec Messaging Gateway 的「控制面板」頁面。如果使用者階段作業逾時 (階段作業會在無活動 30 分鐘之後逾時)，會將使用者導向「控制面板」頁面。

警告：如果使用者啟用此功能，則可以存取其電腦的任何使用者也都可以存取控管中心。我們不建議管理員登入使用此功能。

「記住我」功能因瀏覽器而異。例如，假設使用者透過 Internet Explorer 登入控管中心並啟用**「記住我」**選項。如果使用者隨後透過 Firefox 登入控管中心，則使用者必須輸入登入憑證。

Cookie 會在您指定的天數 (最多 180 天) 後到期。但是，如果您使用強式密碼功能，到期日期可能會變更。

是否可以使用強式密碼搭配**「記住我」**功能，將取決於功能的啟用順序，如下所述：

先啟用強式密碼，然後管理員啟用**「記住我」**功能。	當啟用**「記住我」**功能時，如果略過持續時間大於 60 天 (這是允許使用強式密碼的日數上限)，則會將登入略過持續時間的到期日期設為與強式密碼相同。 此變更不會反映在控管中心設定中。
先啟用**「記住我」**功能，然後管理員啟用強式密碼。	控管中心的**「記住我」**功能會停用。

請參閱第 597 頁的「強制強式密碼」。

請參閱第 584 頁的「指定自訂使用者登入說明頁面」。

讓使用者略過控管中心登入憑證

1. 在控管中心內，按下**「管理」>「設定」>「控管中心」**。
2. 按下**「使用者」**標籤。
3. 在**「使用者說明」**下，勾選**「啟用記住我功能」**。
4. 在**「登入略過持續時間」**方塊中，輸入使用者登入憑證有效的天數。

   您可以輸入 1 到 180 之間的值。預設值為 30 天。

   如果修改此值，會在使用者下次登入並選取**「記住我」**選項時，對他們套用此變更。
5. 按下**「儲存」**。

架構一般使用者喜好設定資料的複寫

在控管中心內，複寫指的是將使用者喜好設定從控管中心傳播到已連接並啟用之掃描程式的程序。控管中心的全域設定會控制複寫程序。

您可以從**「狀態」>「已排程工作」**頁面中，檢查自動化使用者喜好設定的狀態。

請參閱第 556 頁的「關於已排程工作」。

架構一般使用者喜好設定資料的複寫

1. 在控管中心內，按下**「管理」>「設定」>「控管中心」**。
2. 按下**「使用者」**標籤。
3. 在**「複寫頻率」**方塊與下拉式清單中，您可以設定複寫頻率。

   您可以選擇**「從不」**來關閉複寫。

4 在「**複寫開始時間**」下拉式清單中，您可以指定開始複寫的時間。

5 您可以按下「**立即複寫**」，以立即將 LDAP 資料複寫到所有已連線並啟用的掃描程式。

6 您可以按下「**立即刪除**」，以刪除所有的一般使用者喜好設定資料。

7 按下「**儲存**」。

設定 SMTP 問候語與郵件管理員地址

當 Symantec Messaging Gateway 與其他郵件伺服器連線以起始入埠或離埠郵件流量時，會以問候語開始 SMTP 通訊協定轉換。

Symantec Messaging Gateway 預設使用下列問候語：

Symantec Messaging Gateway

您可以變更 Symantec Messaging Gateway 所使用的入埠 SMTP 問候語和離埠 SMTP 問候語。

您也可以變更郵件管理員地址。Symantec Messaging Gateway 會將郵件管理員地址包含在退回郵件中。

請參閱第 595 頁的「架構警示和報告的控管中心 SMTP 設定」。

設定 SMTP 問候語與郵件管理員地址

1 在控管中心內，按下「**通訊協定**」**> SMTP >**「**設定**」。

2 在 **SMTP** 標籤中，將「**入埠 SMTP 問候語**」欄位中的文字反白，然後輸入您要使用的文字。

3 將「**離埠 SMTP 問候語**」欄位中的文字反白，然後輸入您要使用的文字。

4 將「**郵件管理員地址**」欄位中的文字反白，然後輸入您要使用的電子郵件地址。

郵件管理員地址必須是有效的電子郵件地址或 postmaster。

5 按下「**儲存**」。

設定警示

表 23-15 描述了您在設定各種類型的警示時，可執行的工作。您可以視需要以任何順序執行這些工作。

表 23-15 設定警示

工作	說明
熟悉您可為 Symantec Messaging Gateway 設定的警示類型。	警示是自動傳送的電子郵件通知，可通知管理員可能需要注意的狀況。您可以選擇傳送的警示類型、警示郵件中顯示的 From: 標頭，以及收到警示的系統管理員。 請參閱第 587 頁的「警示類型」。
設定您要的警示。	您可以架構 Symantec Messaging Gateway 事件的警示，例如電子郵件佇列大小、垃圾郵件隔離所大小、授權到期以及硬體問題。您可以指定在警示通知電子郵件中顯示的電子郵件地址，以及傳送警示的頻率。 除了 UPS 狀態警示，警示不會在發生警示狀況的當時立即傳送， 而是會以可架構的間隔傳送警示 (預設值為每小時)。 請參閱第 590 頁的「架構警示」。
在您硬體裝置的磁碟空間不足時，便會傳送警示通知。	若要確保系統會在掃描程式的磁碟空間接近或達到容量上限時通知您，您必須啟用磁碟空間不足警示。
在您排程的工作失敗時，便會傳送警示通知。	Symantec Messaging Gateway 可讓您設定已排程工作無法執行時的電子郵件警示。如果工作失敗，就會向指定的管理員傳送電子郵件通知，指出哪項工作失敗以及是在哪個主機上發生。控管中心日誌可提供有關失敗的進一步詳細資料。 請參閱第 595 頁的「設定已排程工作失敗警示」。
指定 SMT 警示與報告設定。	您必須提供要接收控管中心所傳送資訊的 SMTP 主機 IP 位址和通訊埠號。 請參閱第 595 頁的「架構警示和報告的控管中心 SMTP 設定」。

警示類型

警示是自動傳送的電子郵件通知，可通知管理員可能需要注意的狀況。您可以選擇傳送的警示類型、警示郵件中顯示的 `From:` 標頭，以及收到警示的管理員。

請參閱第 590 頁的「架構警示」。

表 23-16 說明可用的警示設定。

表 23-16 警示頁面

警示設定	說明
通知寄件者	這些設定會套用至所有警示
通知頻率	傳送通知的間隔。預設值為每小時。
寄件者	顯示在警示通知的 `From:` 標頭中的電子郵件地址。

警示設定	說明
警示收件者	非本機管理員的電子郵件地址，此管理員會接收您傳送的警示。
管理員警示	選取和取消選取要接收您傳送警示的本機管理員。
疫情	與病毒疫情相關的警示
疫情偵測	在指定的時數、天數、週數或月數期間偵測到指定的病毒數量時傳送警示。
過濾器	與垃圾郵件或病毒過濾器相關的警示
垃圾郵件過濾早於	由於垃圾郵件過濾器更新之間的間隔時間而傳送警示。垃圾郵件過濾器會週期性更新，在不同間隔更新不同的過濾器類型。為了避免非必要的警示，建議使用兩小時的最小設定。
病毒過濾早於	由於病毒過濾器更新 (通常一週發生多次) 之間的間隔時間而傳送警示。為了避免非必要的警示，建議的最小設定值為七天。預設設定是 10 天。
取得新的病毒過濾	由於有新的病毒規則可供下載，因此會傳送警示。
佇列	與郵件佇列相關的警示
結合的郵件佇列大於	當所有郵件佇列的總大小超過警示說明旁指定的大小時，便會傳送警示。郵件佇列包括「入埠」、「離埠」、Content Analysis 及「傳送」。當特定佇列已停止或暫停時，或當無法傳送的郵件攔截了佇列時，「入埠」、「離埠」和「傳送」佇列可能會增加。如果 Content Analysis 伺服器正在忙碌或無法使用，則 Content Analysis 佇列可能會增加。
佇列達到郵件限制	當「入埠」、「離埠」或「傳送」佇列超過**「SMTP 進階設定」**頁面上針對掃描程式設定的郵件數目上限時，會傳送警示。當 Content Analysis 佇列超過**「威脅防禦」>「設定」>「掃描設定」>「威脅防禦掃描設定」**頁面上設定的郵件數目上限時，也會傳送警示。 請參閱第 48 頁的「架構 SMTP 進階設定」。 請參閱第 392 頁的「架構威脅防禦掃描設定」。
磁碟空間	與可用磁碟空間相關的警示
可用磁碟空間少於	當硬體裝置上的可用磁碟空間小於指定的大小，便會傳送警示。磁碟空間不足會導致 Symantec Messaging Gateway 發生效能和穩定性問題。
垃圾郵件隔離所的最大架構磁碟空間使用量已超過	當「垃圾郵件隔離所」所用的磁碟空間超過架構的「垃圾郵件隔離所」大小上限百分比時，便會傳送警示。請在**「垃圾郵件」>「設定」>「隔離所設定」**頁面上，設定垃圾郵件隔離所的大小上限。 請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。
內容事件資料夾的最大架構磁碟空間使用量已超過	當任何內容事件資料夾的可用磁碟空間超過指定的百分比時，便會傳送警示。 請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

警示設定	說明
磁碟空間不足提示已減少或中斷記錄	當掃描程式磁碟空間接近或到達容量，並且系統減少或中斷記錄時，便會傳送警示。 請參閱第 535 頁的「關於記錄磁碟空間警示」。
SMTP	與 SMTP 驗證相關的警示
發生單一使用者登入失敗	當使用者嘗試使用 SMTP 驗證登入且發生失敗時，如果該使用者的失敗次數在指定的時間間隔內等於或超過指定的次數，便會傳送警示。此外，您也可以指定要在每個通知中顯示的使用者數目上限。
發生從單一 IP 登入失敗	當使用者嘗試使用 SMTP 驗證登入且發生失敗時，如果該 IP 位址的失敗次數在指定的時間間隔內等於或超過指定的次數，便會傳送警示。此外，您也可以指定要在每個通知中顯示的 IP 位址數目上限。
DDS	與目錄資料服務有關的警示
目錄資料存取錯誤	由於目錄資料服務無法讀取 LDAP 伺服器的資料，因此會傳送警示。
目錄資料完整性錯誤	指出造成目錄資料服務作業無法成功的客戶目錄資料問題。
資料來源快取大小不足	因為目錄資料來源快取或快取索引的大小不足，而無法保留記憶體中要求的所有資料，所以會傳送警示。
使用者喜好設定複寫錯誤	由於將使用者喜好設定複寫至掃描程式時發生錯誤，因此會傳送警示。
授權/更新	與授權、憑證及軟體更新相關的警示
Symantec Premium Content Control 授權已過期	當 PCC 授權快到期時，便會傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
Symantec Antivirus 授權已過期	當您的防毒授權快到期時，便會傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
Symantec Antispam 授權已過期	當 Symantec Antispam 授權快到期時，便會傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
Symantec Content Encryption 授權已到期	Symantec Content Encryption 授權快到期時，便會傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
軟體更新授權已過期	當您的軟體更新授權快到期時，便會傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
SSL/TLS 憑證到期警告	當憑證到期時，便會傳送警示。您可以進入「憑證設定」頁面並按下「檢視」，檢查您的憑證狀態。第一次的到期警告會在到期日的七天前傳送。一小時後，便會傳送第二個警告。每個憑證不會傳送超過兩次警告。

警示設定	說明
新軟體更新版本可用	當有新軟體更新版本可用時，便會傳送警示。
檢查更新頻率:	以分鐘、小時或天數，指定 Symantec Messaging Gateway 檢查新軟體更新的頻率。
事件	與系統作業相關的警示
交換空間使用率超出	可用的交換記憶體超過指定的百分比時，便會傳送警示。
服務無回應或未正常運作	當服務無回應時，便會傳送警示。服務包括管道、LiveUpdate、Brightmail 引擎、MTA 及目錄資料服務。
硬體故障	由於硬體問題而傳送警示，例如風扇或磁碟故障。
在非正常關機之後啟動服務	在非正常關機之後啟動服務時，便會傳送警示。服務包括管道、LiveUpdate、Brightmail 引擎、MTA 及目錄資料服務。
關閉服務	當服務正常關閉時，便會傳送警示。服務包括管道、LiveUpdate、Brightmail 引擎、MTA 及目錄資料服務。
啟動服務	當服務啟動時，便會傳送警示。服務包括管道、LiveUpdate、Brightmail 引擎、MTA、代理程式及目錄資料服務。
UPS 狀態	由於不斷電系統狀態發生變化而傳送警示。此警示可以縮短至每隔七分鐘傳送一次。
已排程的工作失敗	無法執行您已排程的工作時，便會傳送警示。已排程工作在各自的標籤中進行架構，但您可在**「狀態」>「系統」>「已排程工作」**頁面上檢視所有已排程工作的狀態。

架構警示

警示是在出現可能需要注意的特定狀況時，Symantec Messaging Gateway 傳送給管理員的自動電子郵件通知。您可以選擇要傳送的警示類型、警示郵件中顯示的 `From:` 標頭，以及收到警示的管理員。

附註：若要管理員能夠接收警示，從**「管理」>「使用者」>「管理員」**頁面新增或編輯管理員時，您必須選取**「為此管理員啟用警示通知」**。

請參閱第 564 頁的「設定本機和 LDAP 管理員帳戶」。

設定警示

1 選取「**管理**」>「**設定**」>「**警示**」。

2 從「**通知頻率**」功能表中，選取您希望 SMG 傳送通知的頻率。

SMG 不會在發生警示狀況的當時立即傳送警示。您所設定的「**通知頻率**」會決定何時傳送除 UPS 狀態警示外的所有警示。

3 在「**寄件者**」方塊中，輸入要傳送所有警示的寄件者電子郵件地址。

4 在「**警示收件者地址**」方塊中，輸入要接收您傳送的警示的非本機管理員電子郵件地址。

5 在「**管理員警示**」清單中，選取或取消選取要接收您傳送警示的本機管理員。

6 按下每個標籤，並設定每種警示類型的警示條件。

請參閱第 591 頁的"疫情"。

請參閱第 591 頁的"過濾器"。

請參閱第 592 頁的"佇列"。

請參閱第 592 頁的"磁碟空間"。

請參閱第 593 頁的"SMTP"。

請參閱第 593 頁的"DDS"。

請參閱第 594 頁的"授權/更新"。

請參閱第 594 頁的"事件"。

7 按下「**儲存**」。

疫情

設定病毒疫情的警示。

表 23-17 「疫情」標籤

警示設定	說明
疫情偵測	啟用「**疫情偵測**」可在指定的時數、天數、週數或月數期間偵測到指定的病毒數量時傳送警示。
臨界值	選取要觸發警示的病毒偵測數目下限。
間隔	選取必須達到臨界值數目的病毒才能觸發警示的時段。

過濾器

設定與垃圾郵件或病毒過濾器更新相關的警示

表 23-18 「過濾器」標籤

警示設定	說明
垃圾郵件及不必要的電子郵件過濾早於	由於垃圾郵件過濾器更新之間的間隔時間而傳送警示。垃圾郵件過濾器會週期性更新，在不同間隔更新不同的過濾器類型。為了避免非必要的警示，建議使用兩小時的最小設定。
病毒過濾早於	由於病毒過濾器更新 (通常一週發生多次) 之間的間隔時間而傳送警示。為了避免非必要的警示，建議的最小設定為 7 天。預設設定是 10 天。

佇列

設定郵件佇列限制的警示

表 23-19 「佇列」標籤

警示設定	說明
結合的郵件佇列大於	當所有郵件佇列的總大小超過警示說明旁指定的大小時，便會傳送警示。郵件佇列包括「入埠」、「離埠」、Content Analysis 及「傳送」。當特定佇列已停止或暫停時，或當無法傳送的郵件攔截了佇列時，「入埠」、「離埠」和「傳送」佇列可能會增加。 如果 Content Analysis 伺服器過於繁忙或無法使用，則 Content Analysis 佇列可能會增加。
佇列達到郵件限制	當「入埠」、「離埠」或「傳送」佇列超過**「SMTP 進階設定」**頁面上針對掃描程式設定的郵件數目上限時，會傳送警示。 請參閱第 48 頁的「架構 SMTP 進階設定」。 當 Content Analysis 佇列超過**「威脅防禦」>「設定」>「掃描設定」>「威脅防禦掃描設定」**頁面上設定的郵件數目上限時，也會傳送警示。 請參閱第 392 頁的「架構威脅防禦掃描設定」。

磁碟空間

若要確保系統會在掃描程式的磁碟空間接近或達到容量上限時通知您，請設定磁碟空間不足警示。

表 23-20 「磁碟空間」標籤

警示設定	說明
可用磁碟空間少於	當硬體裝置上的可用磁碟空間小於指定的大小，便會傳送警示。磁碟空間不足會導致 Symantec Messaging Gateway 發生效能和穩定性問題。

警示設定	說明
垃圾郵件隔離所的最大架構磁碟空間使用量已超過	當「垃圾郵件隔離所」所用的磁碟空間超過架構的「垃圾郵件隔離所」大小上限百分比時，便會傳送警示。請在**「垃圾郵件」>「設定」>「隔離所設定」**頁面上，設定垃圾郵件隔離所的大小上限。 請參閱第 245 頁的「修改「垃圾郵件隔離所」臨界值」。
內容事件資料夾的最大架構磁碟空間使用量已超過	當任何內容事件資料夾的可用磁碟空間超過指定的百分比時，便會傳送警示。 請參閱第 360 頁的「關於管理內容事件資料夾的大小」。
磁碟空間不足提示已減少或中斷記錄	當掃描程式磁碟空間接近或到達容量，並且系統減少或中斷記錄時，便會傳送警示。 請參閱第 535 頁的「關於記錄磁碟空間警示」。

SMTP

設定 SMTP 驗證失敗的警示。

您必須提供要接收控管中心所傳送資訊的 SMTP 主機 IP 位址和通訊埠號。

請參閱第 595 頁的「架構警示和報告的控管中心 SMTP 設定」。

表 23-21 SMTP 標籤

警示設定	說明
發生單一使用者登入失敗	當使用者嘗試使用 SMTP 驗證登入且發生失敗時，如果該使用者的失敗次數在指定的時間間隔內 等於或 超過指定的次數，便會傳送警示。此外，您也可以指定要在每個通知中顯示的使用者數目上限。
發生從單一 IP 登入失敗	當使用者嘗試使用 SMTP 驗證登入且發生失敗時，如果該 IP 位址的失敗次數在指定的時間間隔內 等於或 超過指定的次數，便會傳送警示。此外，您也可以指定要在每個通知中顯示的 IP 位址數目上限。

DDS

設定目錄資料服務 (DDS) 問題的警示。

表 23-22 DDS 標籤

警示設定	說明
目錄資料存取錯誤	由於目錄資料服務無法讀取 LDAP 伺服器的資料，因此會傳送警示。
目錄資料完整性錯誤	指出造成目錄資料服務作業無法成功的客戶目錄資料問題。
資料來源快取大小不足	因為目錄資料來源快取或快取索引的大小不足，而無法保留記憶體中要求的所有資料，所以會傳送警示。

警示設定	說明
使用者喜好設定複寫錯誤	由於將使用者喜好設定複寫至掃描程式時發生錯誤，因此會傳送警示。

授權/更新

設定授權、憑證及軟體更新問題的警示。

表 23-23 「授權/更新」標籤

警示設定	說明
Symantec Premium Content Control 授權已過期	當 PCC 授權快到期時，便會發出警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
Symantec Antivirus 授權已過期	當您的防毒授權快到期時，便會傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
Symantec Antispam 授權已過期	當 Symantec AntiSpam 授權即將到期時傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
Symantec Content Encryption 授權已到期	Symantec Content Encryption 授權快到期時，便會傳送警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
軟體更新授權已過期	當您的軟體更新授權快到期時，便會發出警示。授權到期後，則送出另一警示。請聯繫賽門鐵克銷售代理商以取得協助。
SSL/TLS 憑證到期警告	當憑證到期時，便會傳送警示。您可以進入「憑證設定」頁面並按下「檢視」，檢查您的憑證狀態。第一次的到期警告會在到期日的七天前傳送。一小時後，便會傳送第二個警告。每個憑證不會傳送超過兩次警告。
新軟體更新版本可用	當有新軟體更新版本可用時，便會傳送警示。
檢查更新頻率:	以分鐘、小時或天數，指定 Symantec Messaging Gateway 檢查新軟體更新的頻率。

事件

設定系統作業問題的警示。

表 23-24 「事件」標籤

警示設定	說明
交換空間使用率超出	可用的交換記憶體超過指定的百分比時，便會傳送警示。
服務無回應或未正常運作	當服務無回應時，便會傳送警示。服務包括管道、LiveUpdate、Brightmail 引擎、MTA 及目錄資料服務。

警示設定	說明
硬體故障	由於硬體問題而傳送警示，例如風扇或磁碟故障。
在非正常關機之後啟動服務	在非正常關機之後啟動服務時，便會傳送警示。服務包括代理程式、管道、LiveUpdate、Brightmail 引擎、MTA 及目錄資料服務。
關閉服務	當服務正常關閉時，便會傳送警示。服務包括管道、LiveUpdate、Brightmail 引擎、MTA 及目錄資料服務。
啟動服務	當服務啟動時，便會傳送警示。服務包括管道、LiveUpdate、Brightmail 引擎、MTA、代理程式及目錄資料服務。
UPS 狀態	由於不斷電系統狀態發生變化而傳送警示。此警示可以縮短至每隔七分鐘傳送一次。
已排程工作失敗	無法執行排程工作時，便會傳送警示。控管中心日誌可提供有關失敗的其他詳細資料。排程工作在各自的標籤中進行架構，但您可在**「狀態」>「系統」>「排程工作」**頁面上檢視所有排程工作的狀態。

設定已排程工作失敗警示

Symantec Messaging Gateway 可讓您設定已排程工作無法執行時的電子郵件警示。如果工作失敗，就會向指定的管理員傳送電子郵件通知，指出哪項工作失敗以及是在哪個主機上發生。控管中心日誌可提供有關失敗的進一步詳細資料。

設定已排程工作失敗警示

1 在控管中心內，按下**「管理」>「設定」>「警示」**。

2 在**「事件」**標籤下，勾選**「已排程工作失敗」**，然後按下**「儲存」**。

請參閱第 556 頁的「關於已排程工作」。

請參閱第 556 頁的「已排程工作類型」。

架構警示和報告的控管中心 SMTP 設定

控管中心可將下列資訊傳送到您網站上指定的電子郵件地址與儲存庫：

- 警示通知
- 報告
- 垃圾郵件隔離所的郵件

您必須提供要接收控管中心所傳送資訊的 SMTP 主機 IP 位址和通訊埠號。

附註：Symantec Messaging Gateway 會驗證在控管中心與掃描程式中執行的產品版本是否相同。如果產品版本不同，則 Symantec Messaging Gateway 便會發出錯誤訊息。您應該執行掃描程式的軟體更新，並再次於「控管中心設定」頁面上定義 SMTP 主機。

請參閱第 619 頁的「下載及安裝軟體更新」。

架構警示和報告的控管中心 SMTP 設定

1 在控管中心內，按下**「管理」>「設定」>「控管中心」**。

2 按下 **SMTP** 標籤。

3 在**「控管中心 SMTP 設定」**下，執行下列其中一項：

若要指定控管中心產生的電子郵件必須使用非本機轉遞來寄送電子郵件	按下**「使用現有的非本機轉遞設定」**。 請參閱第 43 頁的「架構掃描程式入埠電子郵件傳送設定」。
若要指定電腦 (其上正在運作 MTA) 的 IP 位址或完整網域名稱	按下**「定義新主機」**。 如果未在控管中心所在的硬體裝置上安裝掃描程式，請由預設值加以變更。指定要用於 SMTP 的通訊埠。預設值為 25。

4 按下**「儲存」**。

管理密碼

表 23-25說明可執行哪些工作來管理密碼。您可以視需要以任何順序執行這些工作。

表 23-25 管理密碼

工作	說明
重設密碼。	若管理員忘記密碼，可能需要重設控管中心的管理員密碼。 請參閱第 597 頁的「重設管理員密碼」。
需要強式密碼，才能增強控管中心的存取安全性。	利用強式密碼存取控管中心可以更安全。啟用強式密碼功能時，所有管理員目前的密碼都會到期。不過，admin 管理員的密碼不會到期。管理員下次存取控管中心時，必須設定新的強式密碼。 請參閱第 597 頁的「強制強式密碼」。
瞭解強式密碼準則。	啟用強式密碼功能時，密碼必須符合最低準則 (如 8 個或以上的字元)。 請參閱第 599 頁的「強式密碼條件」。

工作	說明
熟悉密碼的某些最佳實務準則。	檢視關於建立安全密碼的建議。 請參閱第 598 頁的「密碼最佳實務準則」。

重設管理員密碼

若管理員忘記密碼，可能需要重設控管中心的管理員密碼。

附註：如果已啟用「需要強式密碼」設定且未超過密碼的一天最短保存期限，則只有 admin 管理員可變更其他管理員的密碼。在其他情況下，任何具有「管理中心」權限之管理員都可以變更其他管理員的密碼。

請參閱第 566 頁的「管理員權限」。

重設管理員密碼後，請使用安全的方式 (例如電話) 來通知管理員新密碼。一般來說，電子郵件並非安全的方法。

請參閱第 597 頁的「強制強式密碼」。

請參閱第 572 頁的「編輯管理員」。

重設管理員密碼

1. 在控管中心內，按下**「管理」>「使用者」>「管理員」**。
2. 勾選您要變更其密碼之管理員旁邊的方塊，然後按下**「編輯」**。
3. 在**「密碼」**方塊中，輸入新密碼。
4. 在**「確認密碼」**方塊中，再次輸入密碼。
5. 按下**「儲存」**。

強制強式密碼

您可以啟用或停用強式密碼。利用強式密碼存取控管中心可以更安全。啟用強式密碼功能時，所有管理員目前的密碼都會到期。不過，admin 管理員的密碼不會到期。管理員下次存取控管中心時，必須設定新的強式密碼。

如果停用強式密碼功能，則會刪除密碼記錄。如果之後再次開啟強式密碼，管理員就可以再次使用啟用強式密碼時所不允許的舊密碼。

是否可以使用強式密碼搭配**「記住我」**功能，將取決於功能的啟用順序，如下所述：

先啟用強式密碼，然後管理員啟用**「記住我」**功能。	當啟用**「記住我」**功能時，如果略過持續時間大於 90 天 (這是允許使用強式密碼的日數上限)，則會將登入略過持續時間的到期日期設為與強式密碼相同。 此變更不會反映在控管中心設定中。
先啟用**「記住我」**功能，然後管理員啟用強式密碼。	控管中心的**「記住我」**功能會停用。

強制強式密碼

1 在控管中心內，按下**「管理」>「使用者」>「管理員」**。

2 執行下列其中一個步驟：

- 若要啟用強式密碼，請勾選**「需要強式密碼」**。
- 若要停用強式密碼，請取消勾選**「需要強式密碼」**。
  新的強式密碼政策會立即生效。

3 在**「密碼到期」**方塊中，輸入使用者必須在多少天之後變更其密碼。

您可以輸入介於 1 到 90 之間的值。預設值為 60 天。

請參閱第 599 頁的「強式密碼條件」。

請參閱第 597 頁的「重設管理員密碼」。

請參閱第 584 頁的「讓使用者略過控管中心登入憑證」。

密碼最佳實務準則

若要建立安全的密碼，請考慮下列建議：

- 請勿使用下列任一格式建立密碼：
  - 可以在 (任何語言或術語) 辭典中找到的文字
  - 名稱 (例如配偶、父母、孩子、寵物、科幻人物、名人或地點等名稱)
  - 任何您個人名稱或帳戶名稱改編的名稱
  - 關於您或環境且容易獲得的資訊 (例如電話號碼、汽車牌照或社會安全號碼)
  - 生日或容易辨識的樣式 (例如反向寫法、後面加一個數字或前面加一個數字)
- 請根據下列建議建立密碼：
  - 使用混合大小寫字母和數字或標點符號
  - 請確定此密碼與之前的任何密碼都沒關於聯
  - 使用長密碼 (8 個字元或更長)
  - 考慮使用插入標點符號的字詞
  - 考慮使用密語 (一串可讀的文字)

- 考慮使用密語中各個單字的首字母

請參閱第 599 頁的「強式密碼條件」。

重設管理員密碼後，請使用安全的方式 (例如電話) 來通知管理員新密碼。一般來說，電子郵件並非安全的方法。

強式密碼條件

強式密碼必須符合下列所有需求：

- US-ASCII 字元編碼
- 至少 8 個字元
- 至少 1 個大寫字元
- 至少 1 個小寫字元
- 至少 1 個數字

請參閱第 597 頁的「強制強式密碼」。

強式密碼的變更頻率不得超過一天一次，但必須至少每 60 天變更一次。不能與使用者最近使用的五個密碼中的任何一個相同。

硬體裝置維護

管理員可以監控磁碟和電源的使用情況，以確保控管中心、掃描程式和附接的裝置有足夠的磁碟空間且能正確執行。

表 23-26說明可執行哪些工作來維護硬體裝置。您可以視需要以任何順序執行這些工作。

表 23-26　　硬體裝置維護

工作	說明
深入瞭解如何維護充足的磁碟空間。	Symantec Messaging Gateway 在有較多的可用磁碟空間時，效能更佳。某些功能 (如擴充報告功能資料與垃圾郵件隔離所) 可能會使用大量的磁碟空間並加重系統資源的負擔。定期比較磁碟使用量與磁碟容量，以確保控管中心與掃描程式都有足夠的磁碟空間。 請參閱第 603 頁的「關於維護足夠的磁碟空間」。
必要時，關閉硬體裝置。	在您關閉硬體裝置之前，請先停止郵件流。為求保險起見，最好也能清除入埠、離埠和傳送郵件佇列。 請參閱第 604 頁的「關閉硬體裝置」。

工作	說明
視需要，重新啟動硬體裝置。	您也可以一次重新啟動所有硬體裝置。重新啟動硬體裝置需要硬體裝置關閉本身，然後再重新啟動本身。 請參閱第 600 頁的「重新啟動硬體裝置」。
將硬體裝置還原回出廠預設狀況。	重設是硬體裝置上所安裝的最新版本。 請參閱第 600 頁的「將硬體裝置重設為出廠預設值 」。
架構 UPS 設定以防電源中斷。	Symantec Messaging Gateway 可以監控 USB 連線的 APC UPS 裝置。此外，也可以在電源中斷時，執行正常關機。 請參閱第 601 頁的「架構 UPS 設定」。
從不同網路組態還原硬體裝置。	在下列情況下，您可能需要執行此工作： ■ 災難復原 ■ 資料中心移轉 ■ 硬體升級移轉 ■ 實體硬體裝置移轉至虛擬硬體裝置 ■ 虛擬硬體裝置移轉至實體硬體裝置 請參閱第 602 頁的「從不同網路組態還原硬體裝置」。

重新啟動硬體裝置

您可以視需要重新啟動硬體裝置。您也可以一次重新啟動所有硬體裝置。重新啟動硬體裝置需要硬體裝置關閉本身，然後再重新啟動本身。

請參閱第 604 頁的「關閉硬體裝置」。

重新啟動硬體裝置

1. 在控管中心內，按下**「管理」>「主機」>「關閉」**。
2. 在**「系統關機」**下，按下**「主機」**下拉式清單，並選取要重新啟動的硬體裝置。若要重新啟動所有硬體裝置，請選取**「所有主機」**。
3. 按下**「重新開機」**。

   所有連線都會關閉，系統會重新啟動。

將硬體裝置重設為出廠預設值

您可以將硬體裝置恢復成硬體裝置上所安裝最新版本的出廠預設設定。

啟用此功能時，Symantec Messaging Gateway 會對您所選取的主機執行下列所有動作：

- 停止掃描程式主機
- 從主機表清除主機

- 從資料庫清除日誌
- 從資料庫清除報告
- 從資料庫清除狀態資訊
- 將所有設定和政策重設為預設值
- 刪除所有儲存在硬體裝置上的備份檔案
- 停用垃圾郵件提交功能並將所有相關的垃圾郵件提交功能回復到出廠預設值設定。
  此功能包含移除所有提交者類型和提交者位址，以及清除提交者 ID。
  請參閱第 226 頁的「關於針對客戶特定垃圾郵件規則提交郵件」。

附註：對特定掃描程式執行重設為出廠值之後，您必須透過控管中心刪除該掃描程式，然後再次加以新增。

請參閱第 32 頁的「新增掃描程式」。

在您重設硬體裝置之後，就會自動登出。

將硬體裝置重設為出廠預設值

1. 在控管中心內，按下**「管理」>「主機」>「版本」**。
2. 在**「重設為出廠值」**標籤上，按下**「主機」**下拉式清單，然後選取單一主機或**「所有主機」**。

   「所有主機」選項可以將所有主機同時恢復成硬體裝置上所安裝最新版本的出廠預設狀況。
3. 按下 **「重設」**。

   此時會顯示確認視窗。
4. 按下**「重設」**確認重設，或按下**「取消」**停止程序。

請參閱第 600 頁的「重新啟動硬體裝置」。

架構 UPS 設定

Symantec Messaging Gateway 可以監控 USB 連線的 APC UPS 裝置。電源中斷且符合下列任一條件時，它還可保證裝置正常關機：

電池電量	出現電源故障時，剩餘的電池電量百分比 (透過 UPS 報告)低於或等於指定的值
執行時期分鐘數	出現電源故障時，剩餘執行時期分鐘數 (透過 UPS 內部計算) 低於或等於指定的值

逾時分鐘數	出現電源故障時，UPS 藉由電池供電達到逾時分鐘數 **附註：**如果您有智慧型 UPS，則可以停用逾時分鐘數功能，並使用其他設定來控制關閉時間。

請參閱第 707 頁的shutdown。

架構 UPS 設定

1 在控管中心內，按下**「管理」>「設定」> UPS**。

2 勾選**「啟用 UPS 監控」**，然後選取要在哪些狀況下讓硬體裝置自行關閉。

從不同網路組態還原硬體裝置

您可以在下列任一情況下從不同的網路組態還原硬體裝置：

- 災難復原
- 資料中心移轉
- 硬體升級移轉
- 實體硬體裝置移轉至虛擬硬體裝置
- 虛擬硬體裝置移轉至實體硬體裝置

附註：如果要重新架構控管中心主機，請刪除所有日誌、組態和資料。您可以透過控管中心或使用指令行介面來執行刪除操作。

請參閱第 535 頁的「手動刪除日誌檔」。

請參閱第 647 頁的delete。

還原作業完成後，預設不會啟動掃描程式服務。如果您略過網站安裝精靈並從指令行介面執行 `db-restore` 指令，則必須在還原作業完成後手動啟動掃描程式服務。

當備份從一個網路組態中進行而在另一個網路組態中還原，則還原不會成功，除非 BCC/AIO 和其他掃描程式的 IP 位址與備份中採用的 IP 位址相符。

從不同網路組態還原硬體裝置

1 安裝及架構新主機。

您在架構期間選擇的主機角色必須與備份的角色相同。例如，如果備份是從全方位部署生成的，則新主機角色必須是控管中心和掃描程式。

2 從網站安裝精靈匯入授權檔來註冊新主機。

3 或者，完成網站安裝精靈。

如果您完成網站安裝精靈，還原作業將會複寫安裝資訊。不過，完成網站安裝精靈，您就可以透過控管中心 (而不是指令行介面) 執行軟體更新和還原。網站安裝精靈還可讓您在進行還原作業之前建立虛擬 IP。

請參閱第 645 頁的db-restore。

4 透過登出控管中心結束安裝精靈。

5 請確保新主機上的軟體版本與執行備份時使用的版本相同。

如果軟體版本不相同：

- 透過指令行介面來更新主機。
- 如果您已完成網站安裝，請透過控管中心來更新主機。

請參閱第 718 頁的update。

6 登入每個掃描程式主機。將新控管中心 IP 位址新增到 `/data/scanner/etc/agentconfig.xml` 檔案中的允許 IP 清單。

您可以透過指令行介面使用 `agent-config` 指令來新增允許 IP 清單。

請參閱第 634 頁的agent-config。

7 在新主機上透過指令行介面執行 `db-restore` 指令。

請參閱第 645 頁的db-restore。

8 確保 MTA 和控管中心憑證在新主機上有效。

9 如果已啟用內容加密，請聯絡賽門鐵克佈建代表佈建可進行內容加密的新主機。

關於維護足夠的磁碟空間

Symantec Messaging Gateway 在有較多的可用磁碟空間時，效能更佳。某些功能 (如擴充報告功能資料與垃圾郵件隔離所) 可能會使用大量的磁碟空間並加重系統資源的負擔。定期比較磁碟使用量與磁碟容量，以確保控管中心與掃描程式都有足夠的磁碟空間。

請參閱第 521 頁的「檢視您的硬體狀態」。

檢查掃描程式及控管中心是否有舊的或不必要的日誌檔，並手動將其刪除。

請參閱第 536 頁的「清除磁碟空間檢查清單」。

若要減輕系統因過度產生日誌資料而造成的負擔，請設定日誌資料庫大小、記錄層級，並設定較舊日誌資料的清除頻率。

請參閱第 531 頁的「管理日誌資料庫大小」。

為垃圾郵件病毒隔離所及內容事件資料夾指定較小的磁碟空間使用量。

請參閱第 207 頁的「修改為可疑病毒隔離所分配的磁碟空間」。

請參閱第 360 頁的「關於管理內容事件資料夾的大小」。

排程清除程式以定期的間隔執行。

請參閱第 556 頁的「已排程工作類型」。

關閉硬體裝置

當您關閉硬體裝置時，程序會隨即開始。如果您的郵件佇列中有電子郵件，這些電子郵件會保留在佇列中。在您關閉硬體裝置之前，請先停止郵件流。為求保險起見，最好也能清除入埠、離埠和傳送郵件佇列。

請參閱第 65 頁的「MTA 與郵件佇列行為」。

請參閱第 63 頁的「服務與 MTA 作業」。

請參閱第 600 頁的「重新啟動硬體裝置」。

關閉硬體裝置

1. 在控管中心內，按下**「管理」>「主機」>「組態」**。
2. 勾選要關閉之掃描程式旁的方塊，並按下**「編輯」**。

   「編輯主機組態」頁面隨即出現，並顯示**「服務」**標籤。
3. 在**「MTA 作業」**之下，按下**「不接受內送郵件」**。
4. 按下**「儲存」**。
5. 在**「狀態」> SMTP >「郵件佇列」**頁面上，檢視郵件佇列以查看是否為空白。
6. 按下**「全部重新傳送」**以重新傳送包含郵件的所有佇列。

   您也可以按**「刪除」**刪除郵件，或按**「全部刪除」**刪除佇列中的所有郵件。
7. 重複上述步驟，直到清空所有佇列。
8. 在**「管理」>「主機」>「關閉」**頁面上，按下**「主機」**下拉式清單，選取要關閉的主機。
9. 按下**「關閉」**。

   在您關閉硬體裝置的電源之前，請確定本機連線或透過序列連線的視訊主控台上顯示**「關機」**訊息。

關於 Symantec Messaging Gateway 和 Symantec Protection Center

Symantec Protection Center 可讓您將適合的賽門鐵克安全性產品的管理功能整合到單一環境中。透過將 Symantec Messaging Gateway 和其他賽門鐵克安全性產品整合到 Symantec Protection Center，您可以擁有：

- 控制面板，可為適合的安全性產品提供通用的使用者介面，以及從單一位置對威脅進行評估及排除。
- 彙總的報告，可讓您合併或比較所有已整合產品的資料。
- Symantec Global Intelligence Network (GIN) 的即時回應，可提供您關於已偵測到的漏洞、客戶網路內部偵測到的威脅，以及來自這些網路的惡意流量之最新資訊。

如需有關 Symantec Protection Center 的詳細資訊，請參閱 Symantec Protection Center 產品文件。

請參閱第 605 頁的「將 Symantec Messaging Gateway 與 Symantec Protection Center 整合」。

請參閱第 605 頁的「Symantec Protection Center 如何使用 Symantec Messaging Gateway 資料來強化報告」。

將 Symantec Messaging Gateway 與 Symantec Protection Center 整合

Symantec Protection Center 實作了新的 Web 服務層，可讓 Protection Center 與 Symantec Messaging Gateway 及其他整合的應用程式進行通訊。

在整合 Symantec Messaging Gateway 之前，必須先安裝及架構 Protection Center。 賽門鐵克隨即會提供簡單的引導程序，協助您將 Symantec Messaging Gateway 和其他支援的產品新增至 Protection Center。 如需如何設定 Protection Center 及新增產品的詳細資訊，請參閱 Protection Center 文件。

若要將 Symantec Messaging Gateway 與 Protection Center 整合，請確保 Protection Center 伺服器能夠透過通訊埠 8443 與所有 Symantec Messaging Gateway 硬體裝置進行通訊。根據您的環境而定，這可能需要變更防火牆。

請參閱第 604 頁的「關於 Symantec Messaging Gateway 和 Symantec Protection Center」。

請參閱第 605 頁的「Symantec Protection Center 如何使用 Symantec Messaging Gateway 資料來強化報告」。

Symantec Protection Center 如何使用 Symantec Messaging Gateway 資料來強化報告

除了 Symantec Messaging Gateway 已提供的標準報告之外，Protection Center 也有提供可合併多個已整合產品之資料的報告。 例如，如果您已將 Symantec Messaging Gateway 和 Symantec Endpoint Protection 整合到 Protection Center 主控台中，您就可以執行合併這兩者資料的報告。

您可以過濾並儲存這些報告，然後透過電子郵件將其散佈出去。 如需有關 Protection Center 報告的詳細資訊，請參閱 Protection Center 文件。

請參閱第 604 頁的「關於 Symantec Messaging Gateway 和 Symantec Protection Center」。

管理備份

表 23-27說明可執行哪些工作來管理備份。您可以視需要以任何順序執行這些工作。

表 23-27 管理備份

工作	說明
排程在指定時間自動執行備份。	您可以排程完整備份、部分備份，或僅備份系統組態。 請參閱第 606 頁的「排程備份」。
修改備份排程。	視需要修改已排程備份，例如備份時間及備份內容。 請參閱第 608 頁的「編輯排程的備份」。
刪除不再需要的備份排程。	已排程的備份在刪除後，就無法還原。 請參閱第 609 頁的「刪除排程的備份」。
視需要執行手動備份。	您可能需要在對硬體裝置執行任何維護之前、清除或刪除資料之前，執行此工作。 請參閱第 609 頁的「執行隨選備份」。
從備份還原硬體裝置。	如果您先前備份了資料庫，便可以從任何可用的備份儲存區還原這些資料庫。如果是要將備份從一硬體裝置還原到另一實體硬體裝置，請確定新的硬體裝置上設定了正確的日期。這項驗證可確保原始備份時存放於隔離所中的郵件在還原之後正確顯示。 請參閱第 611 頁的「從備份還原硬體裝置」。
瞭解關於備份日誌資料的最佳實務準則。	一般來說，並沒有備份日誌檔的必要。進行疑難排解時，未設定為「資訊」或「偵錯」(可提供最多詳細資料) 的日誌所能提供的效用相當有限。 請參閱第 613 頁的「關於備份日誌資料」。

排程備份

作為最佳實務準則，請經常排程備份以確定您在需要時可使用最新的組態資訊和資料。

您可以排程完整備份、僅政策的備份，或是指定項目的組態備份。在設定備份排程後，就可以從**「狀態」>「已排程工作」**頁面監控備份狀態。

請參閱第 556 頁的「關於已排程工作」。

自訂備份類型的功能提供更高的彈性。例如，假設您想要備份郵件並將其保留在事件資料夾或法規遵循中，但沒有足夠的儲存空間。您可以備份政策及內容事件，並將備份儲存在外部。或者，您有時可能會想要將您在某個控管中心上擁有的政策複製到另一個控管中心。您可以備份政策，然後在其他控管中心內將其還原。

備份不包括真實授權檔 (授權檔的副檔名是 .slf)。因此，還原備份時，必須重新註冊授權。如果找不到授權檔，則必須要求新授權檔。

請參閱第 615 頁的「取得更換授權檔」。

您可以在需要時還原備份，但在此之前務必記住幾個注意事項。

請參閱第 611 頁的「從備份還原硬體裝置」。

附註：`db-backup` 指令可以使用 SCP 來備份硬體裝置。控管中心也 提供此選項。

請參閱第 641 頁的db-backup。

排程備份

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「備份」**標籤上，按下**「新增」**。

「新增排程的備份」頁面隨即出現。

3 在**「備份說明」**下，指定備份的名稱。

4 在**「備份資料」**下，從下列備份類型中進行選擇：

完整備份

備份完整資料庫及下列項目：

- 垃圾郵件隔離所的郵件
- 可疑病毒隔離所郵件
- 垃圾郵件提交提交者 ID
- 垃圾郵件提交提交者清單
- 儲存於磁碟資訊事件資料夾中的內容過濾郵件
- 儲存在磁碟上的「隔離事件」資料夾中的內容過濾郵件。

自訂備份

「自訂備份」選項包括下列子選項：

- **僅政策**
  備份垃圾郵件、惡意軟體、信譽與內容過濾政策、威脅防禦政策、政策群組，及所有政策資源。
- **組態 (包括政策)**
  備份所有組態資料 (其中包含控管中心內所有可修改的設定、垃圾郵件提交的提交者 ID，以及提交者清單) 和政策。同時，也備份您所選取的如下額外項目：
  - 包括內容事件郵件
    除了組態資料與政策外，亦備份所有內容事件資料夾中所有的郵件。
  - 包括報告資料
    除了組態資料與政策外，亦備份所有的報告資料。
  - 包括日誌資料
    除了組態資料與政策外，亦備份所有的日誌資料。

5 在**「備份排程」**下方，定義執行備份的時間和頻率。

6 在**「備份至」**下，選取下列其中一個項目：

在伺服器上儲存備份

此選項會在本機伺服器上儲存備份。指定使用**「要儲存的備份數目」**欄位保留多少個備份版本。

當在本機儲存檔案時，只需要指定將保留的備份版本數。請輸入介於 1 到 25 之間的值。預設值為 3。

在遠端位置上儲存備份

請指定下列值：

- 通訊協定：從下拉式清單中選取 FTP 或 SCP
- 主機 /IP 位址：例如，host.symantecs.org (或 192.168.2.42)
- 通訊埠號。
- 輸入路徑。例如：`/home/username/backups/`
- 勾選以指出傳送是否需要驗證。

  如果需要，請指定以下內容：
  - 使用者名稱
  - 密碼

7 按下**「儲存」**。

編輯排程的備份

您可以視需要修改排程的備份。

編輯已排程備份

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「備份」**標籤上，勾選要編輯之備份旁的方塊。

3 按下**「編輯」**。

「編輯已排程備份」頁面隨即出現。

4 編輯排程之備份的選項。

5 按下**「儲存」**。

刪除排程的備份

排程的備份不再需要時就可以予以刪除。

請參閱第 606 頁的「排程備份」。

刪除已排程備份

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「備份」**標籤上，勾選要刪除之備份旁的方塊。

3 按下**「刪除」**。

執行隨選備份

您可以隨時執行完整備份，僅備份政策，或指定項目的組態備份。

自訂備份類型的功能提供更高的彈性。例如，假設您要備份並維護事件資料夾中的郵件以符合遵從要求，但是沒有足夠的儲存空間。您可以備份政策及內容事件，並將備份儲存在外部。或者，您有時可能會想要將您在某個控管中心上擁有的政策複製到另一個控管中心。您可以備份政策，然後在其他控管中心上將其還原。

備份不包括真實授權檔 (授權檔的副檔名是 .slf)。因此，還原備份時，必須重新註冊授權。如果找不到授權檔，則必須要求新授權檔。

請參閱第 615 頁的「取得更換授權檔」。

您可以在需要時還原備份，但在此之前務必記住幾個注意事項。

請參閱第 611 頁的「從備份還原硬體裝置」。

附註：`db-backup` 指令可以使用 SCP 來備份硬體裝置。控管中心也會提供此選項。

請參閱第 641 頁的db-backup。

執行隨選備份

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「備份」**標籤上，按下**「立即備份」**。

3 在**「備份資料」**下，從下列備份類型中進行選擇：

完整備份

備份完整資料庫及下列項目：

- 垃圾郵件隔離所的郵件
- 可疑病毒隔離所郵件
- 垃圾郵件提交提交者 ID
- 垃圾郵件提交提交者清單
- 儲存於磁碟資訊事件資料夾中的內容過濾郵件
- 儲存在磁碟上的「隔離事件」資料夾中的內容過濾郵件。

自訂備份

「自訂備份」選項包括下列子選項：

- **僅政策**
  備份垃圾郵件、惡意軟體、信譽與內容過濾政策、威脅防禦政策、政策群組，及所有政策資源。
- **組態 (包括政策)**
  備份所有組態資料 (其中包含控管中心內所有可修改的設定、垃圾郵件提交的提交者 ID，以及提交者清單) 和政策。同時，也備份您所選取的如下額外項目：
  - 包括內容事件郵件
    除了組態資料與政策外，亦備份所有內容事件資料夾中所有的郵件。
  - 包括報告資料
    除了組態資料與政策外，亦備份所有的報告資料。
  - 包括日誌資料
    除了組態資料與政策外，亦備份所有的日誌資料。

4 在**「備份至」**下，選取下列其中一個項目：

在伺服器上儲存備份

此選項會在本機伺服器上儲存備份。指定使用**「要儲存的備份數目」**欄位保留多少個備份版本。

當在本機儲存檔案時，只需要指定將保留的備份版本數。請輸入介於 1 到 25 之間的值。預設值為 3。

在遠端位置上儲存備份 請指定下列值：

- 通訊協定：從下拉式清單中選取 FTP 或 SCP
- 主機 /IP 位址：例如，host.symantecs.org (或 192.168.2.42)
- 通訊埠號。
- 輸入路徑。例如：`/home/username/backups/`
- 勾選以指出傳送是否需要驗證。

  如果需要，請指定以下內容：
  - 使用者名稱
  - 密碼

5 按下**「立即備份」**。

從備份還原硬體裝置

您可以視需要還原手動或排程備份。

下列為關於還原備份應該要瞭解的幾件事：

- 您必須還原備份至與建立備份時相同的產品版本。
- 針對僅政策的備份，政策群組成員資格備份詳細資料必須與還原備份的控管中心DDS組態相符。

  僅政策備份中並未包含 DDS 組態，但完整備份和組態備份則有包含 DDS 組態。
- 針對僅政策的備份，內容過濾政策動作必須與還原備份的控管中心事件資料夾組態相符。
- 針對僅政策的備份，在還原之後，政策群組可能會包含不存在於架構位址解析架構資料來源的 LDAP 成員。
- 針對僅政策的備份，在還原之後，您必須確保用於處理架構位址解析資料來源的政策群組成員皆仍有效。
- 如果是要將備份從一硬體裝置還原到另一實體硬體裝置，請確定新的硬體裝置上設定了正確的日期。這項驗證可確保原始備份時存放於隔離所中的郵件在還原之後正確顯示。
- 如果您在執行備份前啟用了客戶特定垃圾郵件功能，則當可以還原備份但無法還原提交設定時，便會在登入頁面上顯示相應的訊息。若要解決此問題，請移至**「垃圾郵件」>「設定」>「提交設定」**頁面並按下**「儲存」**。控管中心會將您的設定與賽門鐵克伺服器上的設定同步，並因此還原您的客戶特定垃圾郵件提交組態。

附註：當備份從一個網路組態中進行而在另一個網路組態中還原，則還原不會成功，除非 BCC/AIO 和其他掃描程式的 IP 位址與備份中採用的 IP 位址相符。從原始 IP 位址以外的其他 IP 位址還原作為控管中心的硬體裝置之後，請重新啟動硬體裝置。如果該硬體裝置也裝載了掃描程式，請先停止該掃描程式。

請參閱第 602 頁的「從不同網路組態還原硬體裝置」。

還原備份後，會出現訊息， 其內容包含還原程序的簡短摘要，並描述了任何應採取的後續步驟。

請參閱第 600 頁的「重新啟動硬體裝置」。

請參閱第 60 頁的「停止和啟動掃描程式」。

從本機備份還原硬體裝置

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「還原/下載」**標籤上，按下**「從伺服器還原/下載備份」**。

3 在**「可用的備份」**下，勾選要還原之備份旁的方塊。

4 按下**「還原」**。

從執行控管中心的硬體裝置下載備份檔案

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「還原/下載」**標籤上，按下**「從伺服器還原/下載備份」**。

3 在**「可用的備份」**下，勾選要下載之備份旁的方塊。

4 按下**「下載」**。

從遠端備份還原硬體裝置

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「還原/下載」**標籤上，按下**「從遠端位置還原備份」**。

提供通訊協定、網域 (主機名稱) 或 IP 位址、通訊埠及檔案的完整 (絕對) 路徑。必要時，提供驗證資訊。

下面是從遠端備份來還原系統的範例值：

主機/IP 位址	host.symantecs.org (或是 192.168.2.42)
通訊埠	21
路徑	/home/username/backups/file.bz2

3 按下**「還原」**。

從本機檔案還原系統

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「還原/下載」**標籤上，按下**「從您的本機電腦上載備份檔案」**。

此步驟是假設您已有備份檔案的本機副本，例如，在 FTP 上的備份。

3 按下**「還原」**。

請參閱第 645 頁的db-restore。

請參閱第 606 頁的「排程備份」。

請參閱第 609 頁的「執行隨選備份」。

關於備份日誌資料

一般來說，並沒有備份日誌檔的必要。進行疑難排解時，未設定為「資訊」或「偵錯」(可提供最多詳細資料) 的日誌所能提供的效用相當有限。最佳實務準則是視需要檢視並儲存目前的日誌，並設定適當的記錄資料保留時間。

請參閱第 531 頁的「管理日誌資料庫大小」。

保持產品在最新狀態

表 23-28說明可執行哪些工作來保持硬體裝置在最新狀態。您可以視需要以任何順序執行這些工作。

表 23-28 保持產品在最新狀態

工作	說明
安裝授權以取得更新的定義檔。	購買 Symantec Messaging Gateway 或續購現有的授權後，您可以從賽門鐵克取得授權檔案。您必須為要安裝和啟用的每個掃描程式註冊授權，才能使用 Symantec Messaging Gateway 功能。您可以使用同一個授權檔案註冊多個掃描程式。 除此授權外，您還可以取得個別授權以啟用 Symantec Content Encryption。內容加密讓您能夠加密離埠郵件以獲得更高的安全性，並透過控管中心追蹤這些郵件的統計資料。 請參閱第 614 頁的「授權您的產品」。
檢視授權狀態，以判斷要授權供每個掃描程式使用的功能，以及授權何時到期。	控管中心內的**「授權」**頁面包含所有需要授權的 Symantec Messaging Gateway 功能。此頁面也會列出功能是否已授權，以及授權何時到期。 請參閱第 615 頁的「檢視授權狀態」。
瞭解 Symantec Messaging Gateway 軟體更新。	賽門鐵克會定期發行新版本的 Symantec Messaging Gateway 軟體。新版本包含新功能以及解決軟體瑕疵的修正。賽門鐵克建議您使用最新版本的軟體，使硬體裝置保持在最新狀態。不過，部分軟體更新可能包含 Symantec Messaging Gateway 基礎架構變更。 請參閱第 618 頁的「關於軟體更新」。 請參閱第 616 頁的「更新 Symantec Messaging Gateway 軟體 」。

工作	說明
執行 Symantec Messaging Gateway 軟體更新。	您可以透過控管中心或指令行更新軟體。 請參閱第 619 頁的「下載及安裝軟體更新」。 請參閱第 718 頁的update。 請參閱第 620 頁的「使用指令行介面來監控軟體更新」。
檢查軟體版本號碼。	您可能需要先執行這個工作，然後再聯絡技術支援。 請參閱第 619 頁的「確定所安裝軟體的版本」。

授權您的產品

購買 Symantec Messaging Gateway 或續購現有的授權後，您可以從賽門鐵克取得授權檔案。您必須為要安裝和啟用的每個掃描程式註冊授權，才能使用 Symantec Messaging Gateway 功能。您可以使用同一個授權檔案註冊多個掃描程式。

附註：需要有單一授權才能使用 Symantec Messaging Gateway 的基本產品功能。除此授權外，您還可以取得個別授權以啟用 Symantec Content Encryption。內容加密讓您能夠加密離埠郵件以獲得更高的安全性，並透過控管中心追蹤這些郵件的統計資料。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

從賽門鐵克取得授權檔案後，請將該檔案儲存到可從控管中心存取的位置。

Symantec Messaging Gateway 會將授權序號儲存在硬體裝置本機上。這些序號會顯示在**「管理」>「主機」>「授權」**頁面上。作為最佳實務準則，建議您將這些序號寫下來。

進行備份還原對您的授權沒有任何影響。不過，如果您將備份還原到未經授權的硬體裝置上，將不會顯示任何序號。

請參閱第 609 頁的「執行隨選備份」。

請參閱第 606 頁的「排程備份」。

請參閱第 611 頁的「從備份還原硬體裝置」。

授權您的產品

1. 在控管中心內，按下**「管理」>「主機」>「授權」**。
2. 按下**「瀏覽」**，並找到授權檔案。
3. 按下**「註冊授權」**。

請參閱第 615 頁的「檢視授權狀態」。

請參閱第 615 頁的「取得更換授權檔」。

檢視授權狀態

您可以檢視授權狀態，以判斷要授權供每個掃描程式使用的功能，以及授權何時到期。

控管中心內的「授權」頁面包含所有需要授權的 Symantec Messaging Gateway 功能。此頁面也會列出功能是否已授權，以及授權何時到期。

附註：當授權快到期時，便會傳送警示。授權到期後，會送出另一則警示。請聯絡賽門鐵克銷售代理商以取得更新授權的協助。

請參閱第 614 頁的「授權您的產品」。

檢視授權狀態

1. 在控管中心內，按下**「管理」>「主機」>「授權」**。
2. 在**「主機」**下拉式清單中，選取主機名稱。

   隨即會出現授權的狀態與到期日。

取得更換授權檔

您可能會遇到必須取得新授權檔的情況。例如，備份並未包含實際的授權檔。因此，還原備份時，必須重新註冊授權。如果您找不到授權檔，那麼便可以在 Symantec Licensing Portal 上取得新的授權檔。

附註：需要有單一授權才能使用 Symantec Messaging Gateway 的基本產品功能。但是，除此授權外，您也可以取得授權以啟用 Symantec Content Encryption。內容加密讓您能夠加密離埠郵件以獲得更高的安全性，並透過控管中心追蹤這些郵件的統計資料。

請參閱第 385 頁的「使用 Symantec Content Encryption 加密資料」。

Symantec Messaging Gateway 會將授權序號儲存在硬體裝置本機上。這些序號會顯示在**「管理」>「主機」>「授權」**頁面上。作為最佳實務準則，您應寫下這些號碼。

進行備份還原對您的授權沒有任何影響。不過，如果您將備份還原到未經授權的硬體裝置上，將不會顯示任何序號。

請參閱第 611 頁的「從備份還原硬體裝置」。

若要取得更換授權檔

1. 在控管中心內，按下**「管理」>「主機」>「授權」**。

   您已註冊的所有授權序號都會出現於**「授權」**頁面上。
2. 請記下您必須取得的所有授權檔序號。

3 連上 Internet 並移至下列 URL：

https://licensing.symantec.com/acctmgmt/home/LicensePortalHome.jsp

4 輸入您的登入 ID 和密碼，然後按下**「登入」**。

如果您沒有登入 ID 和密碼，則必須先註冊一組才能繼續。

5 在**「首頁」**頁面上按下**「購買新產品及更新產品」**。

6 在**「取得新產品授權碼」**頁面上輸入序號。

7 按下**「提交」**。

系統將會顯示您可以用於註冊此產品的序號清單。

8 執行下列其中一項工作：

您先前註冊過的所有序號皆會出現。	若要為某序號取得新授權檔，請勾選其方塊，然後按下**「下一步」**。
您先前所註冊過的所有序號皆沒有出現，或僅出現一部分。	執行下列所有工作： ■ 若要為出現的某序號取得新授權檔，請勾選其方塊。 ■ 若有任何序號並未出現於清單中，請將其輸入**「序號」**方塊，然後按下**「新增」**。 ■ 按**「下一步」**。

9 輸入授權檔收件者的電子郵件地址和您的訊息。

10 指定可以聯絡賽門鐵克支援部門的技術聯絡人。

11 或者新增任何註解。

12 按下**「完成註冊」**。

您的授權檔將會寄至您所指定的電子郵件地址。該授權檔會包含於 .zip 檔中，且副檔名為 .slf。

警告：嘗試修改 .slf 授權檔可能會導致檔案損毀而因此失效。

13 安裝授權檔。

請參閱第 614 頁的「授權您的產品」。

更新 Symantec Messaging Gateway 軟體

附註：執行軟體更新時，請勿重新啟動或關閉硬體裝置。否則裝置可能會毀損，而且之後您可能無法登入控管中心。如需詳細資訊，可以檢視 Linux 主控台。極可能需要重新安裝產品。

表 23-29 說明軟體更新的準備與執行步驟。

表 23-29 軟體更新程序

步驟	動作	說明
步驟 1	下載最新版本並燒錄成 DVD。	從 https://fileconnect.symantec.com/ 下載最新版本並燒錄成 DVD，以在進行復原作業時使用。
步驟 2	閱讀軟體更新文件。	閱讀軟體更新說明、版本說明，以及軟體更新的最新訊息。文件可能會說明軟體更新的具體準備步驟。 請參閱第 618 頁的「關於軟體更新」。 請參閱第 619 頁的「下載及安裝軟體更新」。
步驟 3	執行備份前減少儲存的資料量。	賽門鐵克建議您先減少儲存裝置使用率，然後再升級控管中心硬體裝置。在執行備份之前先減少儲存的資料量，不但可釋放磁碟空間供備份作業使用，還能縮短軟體更新的時間。 您可以執行下列任一或所有步驟來減少儲存的資料量： ■ 儲存在控管中心磁碟中的垃圾郵件和內容已隔離的郵件。 從垃圾郵件隔離所和內容隔離所刪除所有郵件，以釋放控管中心磁碟空間。 請參閱第 647 頁的delete。 ■ 儲存在控制中心資料庫中的報告和記錄資料。 若要縮減控管中心資料庫大小： ■ 清除所有報告。 ■ 若網站政策允許，刪除所有日誌檔。 請參閱第 535 頁的「手動刪除日誌檔」。
步驟 4	執行備份。	執行備份以儲存您的組態設定和事件。 請參閱第 609 頁的「執行隨選備份」。 請參閱第 641 頁的db-backup。
步驟 5	停止內送郵件並清空佇列。	如果您要在掃描程式或控管中心與掃描程式的組合上執行軟體更新，請將 MTA 設為**「不接受內送郵件」**。此時將會暫時拒絕內送郵件。停止內送郵件後，請重新傳送郵件，以便從佇列中清空這些郵件。 請參閱第 63 頁的「服務與 MTA 作業」。 如該章節所述，請勿按停止掃描程式。

步驟	動作	說明
步驟 6	驗證資料庫。	請務必使用 `cc-config database --check` 指令來驗證資料庫。 請參閱第 637 頁的cc-config。
步驟 7	執行軟體更新。	使用控管中心或從指令行介面使用 `update` 指令執行軟體更新。 請參閱第 619 頁的「下載及安裝軟體更新」。 請參閱第 718 頁的update。
步驟 8	監控更新進度。	您可以在**「軟體更新進度」**頁面上監控更新的進度。 您可以選擇在指令行上執行 `tail -f update.log`，來監控更新程序。在執行軟體更新之前，執行此指令，可以看到資料寫入日誌。 請參閱第 620 頁的「使用指令行介面來監控軟體更新」。
步驟 9	重新啟動內送訊息。	更新完成後，您的網頁瀏覽器視窗會重新啟動並顯示登入頁面。登入控管中心。如果您是在掃描程式或控管中心與掃描程式的組合上執行軟體更新，請將 MTA 設為**「照常接受和傳送郵件」**。 請參閱第 63 頁的「服務與 MTA 作業」。

關於軟體更新

賽門鐵克會定期發行新版本的 Symantec Messaging Gateway 軟體。新版本包含新功能以及解決軟體瑕疵的修正。賽門鐵克建議您使用最新版本的軟體，使硬體裝置保持在最新狀態。不過，部分軟體更新可能包含 Symantec Messaging Gateway 基礎架構變更。在進行更新之前，請務必詳讀軟體更新注意事項與版本說明，以瞭解具體的指示。

請參閱第 619 頁的「下載及安裝軟體更新」。

請參閱第 616 頁的「更新 Symantec Messaging Gateway 軟體 」。

您必須在控管中心與所有掃描程式上執行軟體更新。軟體更新套用於硬體裝置的順序沒有影響。例如，您可以先更新控管中心，再更新掃描程式，也可以先更新掃描程式，再更新控管中心。一次只能更新一個硬體裝置。

表 23-30 哪裡可以取得軟體更新的詳細資訊

文件	位置	說明
軟體更新注意事項	在控管中心內，按下**「管理」>「主機」>「版本」>「更新」**。按下**「檢查更新」**，然後選取所需的更新版本。按下**「檢視說明」**。	「軟體更新說明」包含縮簡的更新資訊，以及在新版本中已解決的問題清單。
版本說明	檢視您的軟體版本的版本說明： 1 在 Internet 上，移至 Symantec 支援網站： https://support.symantec.com 2 在功能區上，按下**「文件」**連結。 3 從**「版本」**下拉式功能表中，選取軟體版本。 4 從**「所有文件類型」**下拉式功能表中，選取**「版本說明」**。	「版本說明」包含更多有關更新為新版本的詳細資訊。此外，「版本說明」還會描述新功能，以及列出新版本中尚未修正的已知問題。
最新消息	最新消息的 URL 會列在軟體更新說明與版本說明中。	最新消息網頁可能包含軟體更新說明與版本說明所未提及的版本相關資訊。

確定所安裝軟體的版本

您可以判斷硬體裝置上所安裝軟體的版本。

請參閱第 619 頁的「下載及安裝軟體更新」。

確定所安裝軟體的版本

1 在控管中心內，按下**「管理」>「主機」>「版本」**。

2 在**「更新」**標籤上，按下**「主機」**下拉式清單並選取主機。

隨即顯示軟體的版本和狀態。

下載及安裝軟體更新

若提供新版本，您即可更新您的控管中心及掃描程式。

附註：賽門鐵克建議您使用**「僅下載」**選項下載軟體更新，然後使用**「立即安裝」**或**「稍後安裝」**選項進行安裝。

請參閱第 618 頁的「關於軟體更新」。

請參閱第 616 頁的「更新 Symantec Messaging Gateway 軟體 」。

您也可以使用指令行介面進行更新。

請參閱第 718 頁的update。

從控管中心更新軟體

1. 在控管中心內，按下**「管理」>「主機」>「版本」**。
2. 在**「更新」**標籤上，選取主機。
3. 按下**「檢查更新」**。
4. 如果有軟體更新，請選取軟體更新版本並按下**「檢視說明」**。
5. 如果您要下載軟體更新並在稍後安裝下載的軟體，請按下**「僅下載」**。即會開始下載。

   或

   如果您要安裝軟體更新，請按下**「安裝」**。此選項會下載軟體更新並完成安裝。

使用指令行介面來監控軟體更新

軟體更新程序可能需要數分鐘或數小時才能完成。如果您使用控管中心進行更新，將難以判斷軟體更新是否發生問題。您可以在更新程序寫入 `update.log` 檔案時檢視該檔案，以監控軟體更新的進度。如果您發現資訊定期寫入 `update.log`，則通常表示更新正常進行。

請參閱第 618 頁的「關於軟體更新」。

您可以在執行軟體更新之前或開始軟體更新之後，開始此程序。如果您使用控管中心或指令行執行軟體更新，則可以使用此程序。如果您使用 SSH 用戶端在指令行上執行更新，請在獨立的 SSH 用戶端視窗中執行 `tail -f update.log`，而不是執行 `update install` 指令。如果您使用主控台存取指令行以執行更新，將無法在該主控台上使用更新同時執行 `tail -f update.log`。

請參閱第 712 頁的tail。

使用指令行介面來監控軟體更新

1. 使用 SSH 用戶端或主控台，並登入您要更新的硬體裝置。
2. 輸入下列指令：

```
tail -f update.log
```

使用診斷

管理員可以產生診斷報告，來協助支援人員對系統變慢及故障情形進行疑難排解。

表 23-31說明使用 Symantec Messaging Gateway 診斷可執行的工作。您可以視需要以任何順序執行這些工作。

表 23-31 使用診斷

工作	說明
深入瞭解如何使用診斷套件來疑難排解問題。	如果您在使用 Symantec Messaging Gateway 時遇到問題，賽門鐵克支援中心可能會要求您建立並傳送診斷套件。診斷套件可協助賽門鐵克支援中心疑難排解產品的問題。 請參閱第 621 頁的「關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解」。
執行網路公用程式來疑難排解問題。	控管中心提供網路公用程式來協助您疑難排解問題 (如 traceroute 和 ping)。 請參閱第 622 頁的「從控管中心執行網路公用程式 」。
指定您要包含在診斷套件中的資料。	診斷套件使用預設資料，不過您可以修改要包含在診斷套件中的資料。 請參閱第 622 頁的「指定要包含於診斷套件中的內容」。
產生稍後您要下載的診斷套件。	產生要下載的診斷套件時，Symantec Messaging Gateway 會在執行套件的主機上建立套件。Symantec Messaging Gateway 建立套件後，該套件會顯示在控管中心的**「可用的診斷套件」**清單中。您可以在產生套件後立即將套件下載至控管中心電腦，也可以稍後在您方便時再執行此動作。 請參閱第 623 頁的「產生和下載診斷套件」。
產生稍後您要傳輸的診斷套件。	產生診斷套件時，Symantec Messaging Gateway 會在產生套件的主機上建立套件。建立套件後，您即可將其傳輸至遠端位置。 請參閱第 625 頁的「產生診斷套件並將套件傳輸至遠端位置」。
刪除不再需要的診斷套件。	從**「可用的診斷套件」**清單刪除套件時，會刪除儲存於控管中心的檔案。 請參閱第 626 頁的「刪除診斷套件」。

關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解

如果您在使用 Symantec Messaging Gateway 時遇到問題，賽門鐵克支援中心可能會要求您建立並傳送診斷套件。診斷套件可協助賽門鐵克支援中心疑難排解產品的問題。

所有診斷套件預設都會包含特定元件。不過，您也可以指定要包含於套件中的任何其他元件。如果未指定任何元件，則會產生預設診斷套件。

請參閱第 622 頁的「指定要包含於診斷套件中的內容」。

產生診斷套件時，Symantec Messaging Gateway 會在執行套件的主機上建立套件。然後，您可以使用傳輸通訊協定將套件的複本傳輸至指定的位置。您也可以將套件下載到執行瀏覽器的本機電腦上。此功能僅適用於使用與控管中心相同之 Symantec Messaging Gateway 版本的主機。您一次只能產生一個套件。

請參閱第 625 頁的「產生診斷套件並將套件傳輸至遠端位置」。

請參閱第 623 頁的「產生和下載診斷套件」。

如果您不再需要某個套件，可從控管中心主機加以刪除，以釋放控管中心上的磁碟空間。

請參閱第 626 頁的「刪除診斷套件」。

您也可以從指令行執行此工作。

請參閱第 652 頁的diagnostics。

從控管中心執行網路公用程式

您可以從控管中心執行下列網路公用程式：

Nslookup	查詢 Internet 上的電腦的 DNS 資訊
Traceroute	列出負責在選取的主機和 Internet 上的電腦之間傳輸 Internet 資料的 IPv4 主機，以及經過時間
Traceroute6	列出負責在選取的主機和 Internet 上的電腦之間傳輸 Internet 資料的 IPv6 主機，以及經過時間
Ping	測試來自 Internet 上具有 IPv4 位址之某台電腦的回應。
Ping6	測試來自 Internet 上具有 IPv6 位址之某台電腦的回應。

請參閱第 621 頁的「關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解」。

從控管中心執行網路公用程式

1. 在控管中心內，按下**「管理」>「主機」>「公用程式」**。
2. 按下**「疑難排解」**標籤。
3. 從**「主機」**下拉式清單選取主機名稱。
4. 在**「選取公用程式」**區域下，使用下拉式清單指定公用程式名稱以及主機名稱或 IP 位址。

   如果在**「公用程式」**下拉式清單中選取 Nslookup，則也必須在**「記錄類型」**下拉式清單中指定 DNS 查詢類型。
5. 按下**「執行」**。

   作業的結果會出現在**「結果」**方塊中。

指定要包含於診斷套件中的內容

診斷套件包含下列預設內容：

- 組態資料
- /data/scanner/jobs 下每項工作的五個最新核心目錄 (不含這些目錄中的核心檔案)
- 日誌資料 (每個檔案最多 100,000 行)

若需預設診斷套件中所含內容的詳細資訊，請參閱建立診斷套件的指令行說明。

請參閱第 652 頁的diagnostics。

從控管中心執行診斷時，會始終包含預設的診斷套件。從指令行執行診斷時，只會看到明確包含為指令選項的內容。如果不想匯出診斷套件中的預設內容，必須從指令行執行診斷。

在**「管理」>「主機」>「公用程式」>「診斷」**標籤上，您也可以指定要包含於套件中的其他資料。

- 如果您選取**「郵件追蹤」**，則報告會包含磁碟中的所有郵件追蹤。
- 如果您選取**「所有日誌資料」**，則報告會包含目前可用的所有日誌資料。
- 如果您選取任何核心檔案選項，則報告會包含最新可用的核心檔案。

指定要包含於報告套件中的內容後，請產生套件並將其傳輸或下載至您選擇的位置。您一次只能產生一個套件。若要產生診斷套件，您必須擁有「完整的管理」權限或管理狀態的權限。

請參閱第 625 頁的「產生診斷套件並將套件傳輸至遠端位置」。

請參閱第 623 頁的「產生和下載診斷套件」。

請參閱第 621 頁的「關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解」。

指定要包含於診斷套件中的內容

1. 在控管中心內，按下**「管理」>「主機」>「公用程式」**。
2. 按下**「診斷」**標籤。
3. 按下**「主機」**下拉式功能表，然後選取您要執行診斷套件的主機。
4. 在**「選取元件」**下方，勾選您要包含於診斷套件中的項目。

   如果您未選取任何元件，則會產生預設診斷套件。

   如果您選取僅為控管中心的主機，則只會提供下列元件選項：

   - **所有日誌資料**
   - **所有核心檔案 - 代理程式核心檔案**
   - **所有核心檔案 - 其他核心檔案**
5. 在**「診斷套件包含的核心數目上限」**欄位中，指定您要包含於診斷報告中的核心數目。

   預設值為 5。

   請參閱第 625 頁的「產生診斷套件並將套件傳輸至遠端位置」。

產生和下載診斷套件

產生要下載的診斷套件時，Symantec Messaging Gateway 會在執行套件的主機上建立套件。Symantec Messaging Gateway 建立套件後，該套件會顯示在控管中心的**「可用的診斷套件」**

清單中。您可以在產生套件後立即將套件下載至控管中心電腦，也可以稍後在您方便時再執行此動作。

您一次只能產生一個診斷套件，因此**「可用的診斷套件」**清單中一次只會顯示一個套件。

附註：Symantec Messaging Gateway 不支援下載任何超過 2 GB 的診斷套件。如果診斷套件超過 2 GB，則會顯示錯誤訊息。請重新產生套件，然後透過其中一個支援的通訊協定，將套件傳輸至遠端位置。

請參閱第 625 頁的「產生診斷套件並將套件傳輸至遠端位置」。

成功產生套件後，該套件便會顯示在**「可用的診斷套件」**清單中。如果產生套件未成功完成，控管中心便會顯示錯誤訊息。只有在您未從該頁面瀏覽其他內容時，才會顯示錯誤訊息。此錯誤也會記錄至 Symantec Messaging Gateway 的 BrightmailLog.log 日誌。

如果您離開「診斷」頁面瀏覽其他內容並返回，可能就不會在**「可用的診斷套件」**清單中看到診斷套件。

發生下列其中一個事件：

成功產生套件。	重新整理瀏覽器。套件會顯示在**「可用的診斷套件」**清單中。
套件仍在產生中。	控管中心未顯示任何狀態。請勿再次按下**「產生」**。反之，請重新整理瀏覽器，以查看是否已完成產生套件。如果已完成，則該套件會顯示在**「可用的診斷套件」**清單中。
未成功產生套件。	不會顯示錯誤訊息，但是會將錯誤記錄至 Symantec Messaging Gateway 的 BrightmailLog.log 日誌。

請參閱第 621 頁的「關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解」。

如果您不再需要某個診斷套件，請從控管中心將其刪除以釋放空間。

請參閱第 626 頁的「刪除診斷套件」。

若要產生診斷套件，您必須具有「完整的管理」權限或管理狀態的權限。

產生和下載診斷套件

1. 指定您要包含在診斷套件和主機中的內容。

   請參閱第 622 頁的「指定要包含於診斷套件中的內容」。

2. 在**「通訊協定類型」**下拉式清單中，選取**「下載到桌面」**。
3. 按下**「產生」**。
4. 執行下列其中一項工作：

產生套件後立即下載套件	在**「另存新檔」**對話方塊中，輸入要儲存診斷套件的位置，然後按下**「儲存」**。

稍後再下載套件	執行下列所有工作： ■ 按下「**下載**」。 如果「**可用的診斷套件**」清單中未顯示任何診斷套件，則會停用「**下載**」選項。 ■ 在「**另存新檔**」對話方塊中，輸入要儲存診斷套件的位置，然後按下「**儲存**」。

產生診斷套件並將套件傳輸至遠端位置

產生診斷套件時，Symantec Messaging Gateway 會在產生套件的主機上建立套件。建立套件後，您即可將其傳輸至遠端位置。您一次只能產生一個診斷套件。若要建立診斷套件，您必須具有「完整的管理」權限或管理狀態的權限。

如果您在產生套件後仍停留於「**診斷**」頁面，則會收到關於是否已成功產生套件的回應。建議您在收到此確認回應之前停留於「**診斷**」頁面。

如果您在產生套件後從「**診斷**」頁面瀏覽其他內容，則不會收到關於是否已完成或成功產生套件的回應。如果產生套件工作仍在處理中，且您嘗試重新產生套件，則會顯示錯誤訊息指出正在執行產生套件工作。

如果因任何原因使得產生工作失敗，則會將錯誤記錄至 BrightmailLog.log 中。

請參閱第 621 頁的「關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解」。

產生診斷套件並將套件傳輸至遠端位置

1 指定您要包含在診斷套件和主機中的內容。

請參閱第 622 頁的「指定要包含於診斷套件中的內容」。

2 按下「**通訊協定類型**」下拉式清單，然後選取下列其中一個選項：

- 下載到桌面
- **FTP**
- **SCP**

預設設定為「**下載到桌面**」。

如果選取 FTP 或 SCP，則您也必須指定通訊協定參數和憑證。

如果您選取「**下載到桌面**」，請繼續執行步驟 7。

3 在「**主機**」方塊中，輸入您要傳送套件之電腦的主機名稱或 IP 位址。

4 在「**通訊埠**」方塊中，輸入您要傳送套件之電腦的通訊埠號。

預設 FTP 通訊埠為 21，而預設 SCP 通訊埠為 22。

5 在「**路徑**」欄位中輸入路徑。

如果檔案路徑結尾為正斜線，則系統會假設其為目錄，並在正斜線後附加預設檔案名稱。如果檔案路徑結尾並非正斜線，則系統會假設其為完整檔案路徑名稱。

6 如果「**通訊協定類型**」為 **FTP** 且需要驗證，請勾選「**需要驗證**」選項。否則會嘗試匿名登入。若已選取「**需要驗證**」選項：

- 在「**使用者名稱**」方塊中輸入使用者名稱。
  不支援特殊字元 (如 $、#、%)。
- 在「**密碼**」方塊中輸入密碼。

或

如果「**通訊協定類型**」為 **SCP**：

- 在「**使用者名稱**」方塊中輸入使用者名稱。
  不支援特殊字元 (如 $、#、%)。
- 在「**密碼**」方塊中輸入密碼。

7 按下「**產生**」。

刪除診斷套件

建立診斷套件並選取「**下載到桌面**」選項後，該套件會顯示在「**可用的診斷套件**」清單中(「**可用的診斷套件**」清單中一次只會顯示一個套件)。如果您不再需要此套件，可將其刪除。從「**可用的診斷套件**」清單刪除套件時，會刪除儲存於控管中心的檔案。

若要刪除診斷套件，您必須具有「完整的管理」權限或管理狀態的權限。

請參閱第 625 頁的「產生診斷套件並將套件傳輸至遠端位置」。

請參閱第 623 頁的「產生和下載診斷套件」。

請參閱第 621 頁的「關於使用診斷進行 Symantec Messaging Gateway 問題的疑難排解」。

刪除診斷套件

1 在控管中心內，按下「**管理**」>「**主機**」>「**公用程式**」。

2 按下「**診斷**」標籤。

3 在「**可用的診斷套件**」下，按下「**刪除**」。

24

透過指令行管理 Symantec Messaging Gateway

本章包含以下主題：

- 透過指令行管理 Symantec Messaging Gateway
- 指令行介面存取方法

透過指令行管理 Symantec Messaging Gateway

每部硬體裝置 (實體或虛擬) 都具備一組指令，可讓您用來架構、最佳化和管理產品。您可以從 SSH 階段作業或從系統主控台來執行這些指令。系統會以 Linux 手冊頁格式來呈現這些指令的說明。

請參閱第 630 頁的「指令行介面存取方法」。

這些說明頁面會使用下列 Linux 手冊頁慣例：

- 方括弧 ([]) 是指陳述式為選用
- 管道字元 (|) 是指可指定兩個陳述式的其中一個
- *斜體*文字表示該文字必須由您指定的文字取代

Symantec Messaging Gateway 手冊頁包含以下部分：

- 概要
  指令可用選項與引數的說明。
- 說明
  關於指令的一般資訊。
- 選項
  您可以用來控制指令行為的選項。選項始終以一或兩個破折號開頭，例如 `-s` 或 `--status`。對於完整的詞，請使用兩個破折號；對於縮寫的詞則使用一個破折號。

某些選項具有引數。例如，`--log`*level*。方括弧表示指令的元素為選用。
並非所有指令都有選項。

- 引數
  某些指令需要使用引數。引數包括檔案名稱、主機名稱、IP 位址等等，您可以指定這些引數來控制指令行為。並非所有指令都有引數。和選項不同的是，您不能在引數前面加上破折號。
- 範例
  本節提供了指令用法範例。並非所有指令都有範例。
- 另請參閱
  本節列出了相關指令。並非所有指令都有「另請參閱」參照。

使用下列指令可在手冊頁中瀏覽：

- f 或 SPACE
  移至下一個視窗
- b
  移至上一個視窗
- /pattern
  搜尋單字或樣式
- <
  移至文件開頭
- >
  移至文件結尾
- q
  結束
- h
  使用手冊頁顯示更多說明

輸入 `help` *`command_name`* 即可取得有關特定指令的資訊。輸入 `help` 即可取得有關指令行手冊頁的一般資訊。

提供的指令包括：

- agent-config
- cat
- cc-config
- clear
- db-backup
- db-restore

- delete
- diagnostics
- dns-control
- fipsmode
- grep
- help
- ifconfig
- iostat
- ip
- ldapsearch
- list
- mallog
- malquery
- monitor
- more
- mta-control
- netstat
- nslookup
- password
- patch
- ping
- ping6
- reboot
- route
- rpmdb
- rsa-金鑰
- service
- show
- shutdown
- sshd-config

- symdiag
- tail
- telnet
- traceroute
- traceroute6
- update

指令行介面存取方法

您可以登入每個 Symantec Messaging Gateway 硬體裝置的指令行介面。當中有某些指令與控管中心裡的功能重複。某些指令則是提供控管中心裡沒有的功能。

請參閱第 627 頁的「透過指令行管理 Symantec Messaging Gateway」。

表 24-1 與表 24-2 說明您可用來存取指令行介面的方法。連線至指令行介面之後，於 `login as:` 提示中輸入 **`admin`**，然後於 `password:` 提示中輸入管理員密碼。

表 24-1 實體硬體裝置的指令行介面存取方法

存取方法	連線方式
使用直接附加的鍵盤與 VGA 顯示器存取系統主控台	您必須能夠實際存取硬體裝置，才能使用鍵盤與 VGA 顯示器存取指令行介面。 將鍵盤連接至硬體裝置上的鍵盤通訊埠。將 VGA 相容顯示器連接到硬體裝置上的 D-sub 15 VGA 通訊埠。 您也可以將硬體裝置上的鍵盤與 VGA 通訊埠連接至 KVM 切換器。
使用序列纜線存取系統主控台	您必須能夠實際存取硬體裝置，才能使用序列纜線存取指令行介面。 使用虛擬數據機纜線將硬體裝置的 DB9 序列埠與另一台電腦的序列埠連接。使用電腦上的終端機模擬軟體，並透過序列埠存取硬體裝置。在 Windows 電腦上，確保終端機模擬軟體已設為使用正確的 COM 通訊埠。將電腦上的終端機模擬軟體架構為下列設定： ■ 9600 bps ■ 8 個資料位元 ■ 無同位檢查位元 ■ 1 個停止位元

存取方法	連線方式
使用 SSH 用戶端進行遠端存取	您可以透過 SSH 用戶端，從網路上任何一台電腦存取指令行介面 (除非防火牆規則禁止存取)。 在 Windows 電腦上，請使用 PuTTY 之類的 SSH 用戶端。在 UNIX 電腦上，您可以使用通常包含於作業系統的 `ssh` 指令。 透過 SSH 用戶端來連線時使用的主機名稱或 IP 位址，就是您最初架構硬體裝置時所指定的名稱。在控管中心硬體裝置上，主機名稱同時也是您用來存取控管中心的 URL 中的名稱。

表 24-2 虛擬硬體裝置的指令行介面存取方法

存取方法	連線方式
VMware 虛擬機器主控台	您可以使用 VMware 虛擬機器主控台來登入虛擬硬體裝置。請參閱 VMware 虛擬機器主控台文件以取得相關資訊。
使用 SSH 用戶端進行遠端存取	如果您已使用可在網路上解析之主機名稱或 IP 位址來架構虛擬硬體裝置，則可以使用 SSH 用戶端來存取指令行介面。除非防火牆規則禁止存取，否則您可以從網路上任何一台電腦存取虛擬硬體裝置。 在 Windows 電腦上，請使用 PuTTY 之類的 SSH 用戶端。在 UNIX 電腦上，您可以使用通常包含於作業系統的 `ssh` 指令。

附錄 A

指令行參考

本附錄包含以下主題：

- agent-config
- cat
- cc-config
- clear
- db-backup
- db-restore
- delete
- diagnostics
- dns-control
- fipsmode
- grep
- help
- ifconfig
- iostat
- ip
- ldapsearch
- list
- mallog

- malquery
- monitor
- more
- mta-control
- netstat
- nslookup
- password
- patch
- ping
- ping6
- reboot
- route
- rpmdb
- rsa-金鑰
- service
- show
- shutdown
- sshd-config
- symdiag
- tail
- telnet
- traceroute
- traceroute6
- update

agent-config

agent-config – 架構將主機連線至控管中心的代理程式

大綱

```
agent-config [--norestart] [--force] --add | --delete ip

agent-config --help | --status

agent-config [--norestart] --log level
```

說明

agent-config 指令可讓您編輯允許的掃描程式 IP 組態。變更控管中心的 IP 位址時，請使用此指令。您必須在每個主機上執行此指令，才能重新允許新的控管中心 IP 連線到主機。除非您在指令中包含 --norestart，否則在允許的 IP 清單中新增或刪除 IP 位址時，代理程式會重新啟動。

選項

--add, -a *ip*

新增 IP 位址至代理程式允許的 IP 位址清單。請以句點四等分格式指定 IP 位址。例如 192.168.2.1。

--delete, -d *ip*

從代理程式允許的 IP 位址清單中刪除 IP 位址。請以句點四等分格式指定 IP 位址。例如 192.168.2.1。

--log, -l *level*

設定記錄層級。以下列出了這些記錄層級 (從最不詳細到最詳細)，每個層級都包含前一個層級。例如，如果您指定 errors 層級，則只會儲存最緊急的日誌訊息。如果您指定 notices 層級，則會儲存 errors、warnings 和 notices 層級的日誌訊息。

請指定下列記錄層級之一：

- errors
- warnings
- notices
- information
- debug

`--force, -f`

與 `--delete` 選項搭配使用可略過刪除警告。

`--help, -h`

顯示此郵件。

`--norestart, -n`

修改 IP 位址清單或記錄層級之後，請勿重新啟動代理程式。

`--status, -s`

顯示允許的 IP 位址清單及目前記錄層級。

cat

cat – 用來檢視檔案的標準 Linux 指令

說明

cat 指令顯示純文字檔案的內容。要列出長的檔案或多個檔案，more 指令比 cat 更有用。

如需 help cat 可用選項的詳細資訊，請在指令行輸入 cat。所顯示的資訊可能包含 Symantec Messaging Gateway 並未提供之指令的參考。

cat 指令是標準 Linux 指令，已修改為僅顯示 list 指令所顯示的檔案。

另請參閱

請參閱第 670 頁的list。

請參閱第 685 頁的more。

cc-config

cc-config – 架構控管中心的記錄與網路存取

大綱

```
cc-config ( --help | --status )

cc-config cclog --level level

cc-config compliancelog --days days

cc-config database ( --status | --check [tableName] | --repair [tableName] |
--optimize [tableName] )

cc-config http ( --on | --off )

cc-config port-443 ( --on | --off )

cc-config set-min-tls-level (--tls1 | --tls11 | --tls12)
```

說明

cc-config 指令可讓您修改控管中心使用的所選設定。這些設定包括內容過濾稽核日誌、通訊埠 443 存取等等。

引數

cclog

變更主要控管中心日誌 (BrightmailLog.log) 的記錄層級。

將其套用至控管中心日誌時，cc-config 會將指令行參數寫入 log4j 內容檔案，然後重新啟動控管中心。

compliancelog

變更內容過濾日誌的變換頻率。

database

列示、最佳化、驗證或修復控管中心使用的資料庫表格。

在更新 Symantec Messaging Gateway 之前，請務必使用 cc-config database --check 指令來驗證資料庫。如果表格中有任何錯誤，請使用 cc-config database --repair [tableName] 指令修復錯誤的表格，然後再更新 Symantec Messaging Gateway。

http

開啟或關閉使用 HTTP 和通訊埠 41080 對控管中心的存取。

如果 http 存取已關閉，則您無法使用以 http:// 開頭的 URL 來存取控管中心。如果 http 存取已開啟，則您可以使用以 http:// 開頭的 URL 來存取控管中心。若要使用 http 存取控管中心，請將 :41080 附加到 URL。無論 http 設定為何，您始終可以使用以 https:// 開頭的 URL 來存取控管中心。與 HTTPS 不同，HTTP 不是安全通訊協定，因此第三方可能會監控網頁瀏覽器和控管中心之間的通訊。

`port-443`

開啟或關閉使用 HTTPS 和通訊埠 443 (Web 伺服器標準的 SSL 安全通訊埠) 對控管中心的存取。

如果通訊埠 443 存取已關閉，則您在使用 https:// URL 來存取控管中心時，必須將 :41443 附加至該 URL。如果通訊埠 443 存取已啟用，則您不需要對 https:// URL 附加通訊埠號，即可存取控管中心。

`set_tls_min_level`

設定最小的 TLS 層級。

選項

`--check, -c`

檢查指定的資料庫表格。如果未指定任何表格名稱，則會檢查所有表格。

`--days, -d`

設定要保留日誌多少天後才對其進行變換。

`--help, -h`

顯示此郵件。

`--level, -l`

設定記錄層級。以下列出了這些記錄層級 (從最不詳細到最詳細)，每個層級都包含前一個層級。例如，如果您指定 `errors` 層級，則只會儲存最緊急的日誌訊息。如果您指定 `debug` 層級，則會儲存 `errors`、`warnings`、`information` 和 `debug` 層級的日誌訊息。

請指定下列記錄層級之一：

- errors
- warnings
- information
- debug

`--off`

停用功能。

`--on`

啟用功能。

`--optimize, -o`

最佳化表格，以便使其佔用較少的磁碟空間。如果未指定任何表格名稱，則會最佳化所有表格。

`--repair, -r`

修復指定的資料庫表格。如果未指定任何表格名稱，則會嘗試對所有已損壞的表格進行修復作業。

`--status, -s`

顯示目前的日誌設定及通訊埠狀態。

`--tls1 --tls11 --tls12`

TLS 版本：--tls1 = TLSv1；--tls11 = TLSv1.1；--tls12 = TLSv1.2

clear

`clear` – 可清除畫面的標準 Linux 指令

大綱

```
clear
```

說明

`clear` 指令清除畫面上的所有文字，並在畫面最上方顯示指令提示。

此指令是未經修改的標準 Linux 指令。

db-backup

db-backup – 備份控管中心資料庫

大綱

```
db-backup [options]
```

說明

db-backup 指令會備份 Brightmail 資料庫 (例如政策組態設定、報告資料、日誌資料和資安事端)。您可以將備份儲存在硬體裝置或遠端伺服器上。僅在包含控管中心的硬體裝置上執行此指令。此指令無法在僅限掃描程式的硬體裝置上運作。一次只能執行一個 db-backup 實例。

依據預設，備份檔案在寫入磁碟之前會先壓縮，以使備份檔案大小降為最小。db-backup 指令會計算備份檔案所需磁碟空間。/data 分割區上的可用空間必須至少是所需空間量的兩倍，此指令才能執行。

請使用 db-restore 或控管中心還原功能來還原硬體裝置上的備份，或遠端電腦上的備份。如果您為硬體裝置的備份指定 --file *path*，則只能使用 db-restore 指令 (而無法使用控管中心還原功能) 來還原此備份。

您也可以使用控管中心來建立備份。在控管中心內，按下**「管理」>「主機」>「版本」>「備份」**。

請參閱第 609 頁的「執行隨選備份」。

選項

--backup, -b *number*

儲存在硬體裝置上的備份數目。如果儲存的備份數超過 *number*，會刪除較舊的備份。會分別保留類型與排程的每種獨特組合。如果您沒有指定 --backup *number*，每一個類型與排程的組合預設值為 5。請參閱範例 4 和 6。

--file, -f *path*

備份的儲存名稱以及位置 (選擇性)。使用 --file 選項來指定備份檔案的替代檔案名稱，或是將備份檔儲存至遠端電腦。如果您沒有指定 --file *path*，備份會以 db-backup.*<product version>*.brightmail.*Mon-Day-Year-Hour-Min*.full.manual.tar.bz2 儲存至硬體裝置。

您可以使用 FTP (檔案傳輸通訊協定) 或 SCP (安全複製通訊協定) 將備份儲存至遠端電腦。如果路徑以 / 結尾，則備份會以預設檔案名稱儲存在該目錄中。如果路徑以檔案名稱結尾，則備份會以該名稱儲存在指定的路徑中。當您將備份儲存至遠端電腦時，db-backup

會暫時將備份檔案儲存在硬體裝置上，然後檢查檔案的資料完整性並將檔案複製到遠端電腦，最後檢查以確定檔案是否成功複製。

使用下列兩種路徑格式之一，可以將備份儲存至遠端伺服器：

FTP

使用以下格式：`ftp://'user':'password'@host[:port]/path`。如果密碼包含特殊字元，必須以單引號 (') 括住密碼。如果密碼中的特殊字元包含單引號，則可改用雙引號 (")。同時包含單引號和雙引號的密碼無效。如果未指定任何使用者名稱和密碼，則會使用匿名登入。

SCP

使用以下格式：`scp://'user'@host/path`。您必須指定使用者名稱。db-backup 指令會提示您輸入密碼。

`--gzip, -g`

使用 gzip 壓縮演算法，而非預設的 bzip2 壓縮演算法。gzip 演算法的壓縮效率低於 bzip2。

`--list, -l`

列出硬體裝置中現有的備份。

`--help, -h`

顯示此郵件。

`--incidents, -i`

將內容資安事端郵件包含在組態備份中。只有與 `--type config` 搭配使用時才有效。

`--logs, -o`

將日誌資料包含在組態備份中。只有與 `--type config` 搭配使用時才有效。

`--nocompress, -n`

請勿壓縮備份檔案。如果您想要目視掃描檔案內容，請使用此選項。

`--purge, -p`

清除備份。使用 `--purge` 選項可刪除所有符合您指定之參數的舊備份檔案。若要刪除 *number* 個最新的類型與排程組合備份之外的所有備份，請指定 `--purge --backup number` 及類型與排程。指定 `--purge --backup 0` 以刪除所有類型與排程組合的備份。若要刪除特定檔案，請指定 `--file file` 與 `--purge`。請參閱範例 5 和 6。

`--reports, -r`

將報告資料包含在組態備份中。只有與 `--type config` 搭配使用時才有效。

`--schedule, -s schedule`

要包括在備份檔案名稱中的排程名稱。如果指定排程名稱，則 db-backup 不會建立依該間隔的自動備份。指定的排程只會使用該名稱來命名備份檔。排程名稱與備份名稱不同。請參閱 `--backup` 與 `--purge` 以取得詳細資訊。請使用控管中心的備份功能來建立自動排程的備份。下列排程可供使用：

`manual`

將此備份標示為手動備份。此選項為預設選項。

`daily`

將此備份標示為每日手動備份。

`weekly`

將此備份標示為每週手動備份。

`monthly`

將此備份標示為每月手動備份。

`--type, -t` *type*

要建立的備份類型。每種備份類型都有兩個別名，作為備份類型替代性簡短版本。請參閱範例 4。以下類型可供使用：

`full`

執行完整備份 (別名：`f`, `1`)。這是預設選項。

`config-incidents`

備份組態與內容過濾事件資料 (別名：`ci`, `2`)。

`config-incidents-reports-logs`

備份組態、內容過濾事件、報告與日誌資料 (別名：`cirl`, `3`)。

`config`

備份包括政策在內的所有組態 (別名：`c`, `4`)。使用 `--log` 將日誌資料包含在此備份中。使用 `--reports` 將報告資料包含在此備份中。使用 `-- incidents` 將內容資安事端郵件包含在此備份中。此選項為預設選項。

`政策`

備份垃圾郵件、惡意軟體、信譽和內容過濾政策，以及政策群組和政策資源 (別名：`p`, `5`)。

範例

範例 1

使用預設的 `manual` 排程與預設的 `full` 類型，在硬體裝置上儲存完整的備份。將保留五個使用 `manual` 排程與 `full` 類型的最新備份 (包括剛建立的備份)，然後將符合該組合的所有剩餘備份刪除。

```
db-backup
```

範例 2

使用 SCP 將完整備份儲存在遠端伺服器上。格式為 `db-backup.<`*產品版本*`>.brightmail` **檔名儲存至硬體裝置**。*date-time*`.full.manual.tar.bz2` 的資料庫備份檔案會透過 SCP 複製到 192.168.2.42 的 /tmp 目錄中。使用 `support` 使用者帳戶來登入 SCP 伺服器。`db-backup` 指令會提示您輸入 `support` 使用者帳戶的密碼。

```
db-backup --file scp://support@192.168.2.42/tmp/
```

範例 3

使用 FTP 將完整備份儲存在遠端伺服器上。資料庫備份檔案 db-backup.<*產品版本*>.brightmail **檔名儲存至硬體裝置**。*date-time*.full.manual.tar.bz2 會複製到 host.symantecexample.org (位於 /user/jmuir 目錄中)。使用 jmuir 使用者帳戶與 secret 密碼來登入 FTP 伺服器。

```
db-backup -f ftp://jmuir:secret@host.symantecexample.org/user/jmuir/
```

範例 4

將組態與內容過濾資安事端資料備份至硬體裝置，然後在備份檔案名稱中包含 weekly 文字。除了新建立的備份之外，額外保留一份檔案名稱內含有 config-incidents 與 weekly 的現有備份。

```
db-backup --backup 2 --schedule weekly --type ci
```

範例 5

刪除單一備份檔。

```
db-backup --purge --file
db-backup.10.0.0-1.brightmail.Feb-25-12-19-26.config-incidents.weekly.tar.bz2
```

範例 6

刪除一個類型為 config-incidents 與排程為 manual 的最新備份檔案之外的所有備份。

```
db-backup --purge --backup 1 --type config-incidents --schedule manual
```

另請參閱

請參閱第 645 頁的db-restore。

db-restore

`db-restore` – 從先前建立在硬體裝置上的備份，或透過 FTP 和 SCP 從遠端位置將 Brightmail 資料庫還原至硬體裝置

大綱

```
db-restore [--force --list --help] file
```

說明

`db-restore` 指令會從先前建立的單一備份，將 Brightmail 資料庫還原至硬體裝置。這些備份是您先前在硬體裝置上，或是透過 FTP 和 SCP 從遠端位置產生並儲存的備份。如果嘗試一次執行 `db-restore` 的多個實例，則會產生錯誤。如果作業的任何部分失敗，則 `db-restore` 將失敗，並在指令行上顯示說明訊息。您必須位於控管中心主機上，才能使用 `db-restore` 指令。

附註：在將硬體裝置重設回出廠預設值之後立即還原該硬體裝置，可能會導致硬體裝置處於不穩定的狀態。因此，您必須先完成網站安裝，然後再將重設回其出廠預設值的硬體裝置還原。

在並非建立資料庫備份的硬體裝置上還原資料庫備份時，請謹記下列考量：

- 當備份從一個網路組態中進行而在另一個網路組態中還原，則還原不會成功，除非BCC/AIO和其他掃描程式的 IP 位址與備份中採用的 IP 位址相符。
- 如果您從取自其他硬體裝置上的備份來還原硬體裝置，還原的硬體裝置並不會影響新主機上的組態設定。不過，在進行架構期間將不會建立虛擬 IP 位址。舊控管中心主機中定義的虛擬 IP 依預設會對應至新控管中心主機上的介面。您可以透過完成網站安裝，來避免舊控管中心主機中的虛擬 IP 對應至新控管中心主機上的介面。或者，您可以在還原之後於新控管中心主機上建立虛擬 IP。
- 如果您嘗試將備份還原到並非建立該備份的硬體裝置，則必須重新啟動該硬體裝置。

此作業執行時，請停止控管中心。還原完成時，請重新啟動控管中心。

選項

`--force, -f`

強制進行還原，即使備份檔案中的硬體裝置軟體版本與目前硬體裝置上的軟體不同，也是如此。

`--list, -l`

列出儲存在硬體裝置上的備份檔案。

`--help, -h`

顯示此郵件。

引數

使用下列其中一種格式指定 ***file***。如果檔案儲存在遠端電腦上，請指定該檔案的目錄路徑。

`file`

輸入沒有 FTP 或 SCP 字首的檔案名稱，以指定儲存在本機的備份。

`ftp://`*`user`*`:`*`password`*`@[:`*`port`*`] /`*`path`*

使用 FTP 從遠端位置複製檔案。

會嘗試使用您在指令行提供的使用者名稱與密碼憑證進行登入。如果密碼包含特殊字元，請將該密碼包含在單引號 (') 中。如果密碼中的特殊字元包含單引號，則可改用雙引號 (")。若未指定任何憑證，則會使用匿名登入。錯誤檢查可確保複製完整。

`scp://`*`username`*`@`*`host`*`/`*`path`*

使用 SCP 從遠端位置複製備份檔案。透過 SCP 指定備份檔案時，需要完整的路徑、檔案名稱以及使用者名稱。會提示您輸入您所指定使用者名稱的密碼。會檢查傳回碼，以確保從遠端主機複製整個備份檔案。失敗時，指令碼會以非零狀態結束。如果指令碼失敗，則會顯示錯誤訊息。錯誤檢查可確保複製完整。

另請參閱

請參閱第 641 頁的db-backup。

請參閱第 652 頁的diagnostics。

請參閱第 230 頁的「佈建客戶特定垃圾郵件提交的提交者 ID」。

請參閱第 234 頁的「處理「提交者電子郵件地址」清單」。

請參閱第 611 頁的「從備份還原硬體裝置」。

請參閱第 600 頁的「重新啟動硬體裝置」。

請參閱第 60 頁的「停止和啟動掃描程式」。

delete

delete – 清除日誌、組態資訊及資料

大綱

```
delete [--purge num] component component ...

delete file file
```

說明

使用 delete 指令可刪除日誌、組態資訊及其他資料。您可能想要在磁碟空間不足時刪除資料，或清除組態資料以修正或診斷問題。如果需要，delete 指令會在執行 delete 指令之後重新啟動 Brightmail 引擎。

選項

--purge, -p *num*

刪除所有資料庫備份檔案 (除了 *num* 個最新檔案之外)。此選項僅對 database 元件有效。

引數

您可以刪除個別檔案，也可以指定一或多個元件來刪除檔案的邏輯群組。

file *file*

刪除您指定的檔案。您僅可刪除使用 list 指令能夠檢視的檔案。指定由 list 指令所示檔案的整個路徑。

賽門鐵克建議您透過指定元件，而不是使用刪除個別檔案的方式來刪除項目。如果您刪除個別檔案，則可能會變更 Symantec Messaging Gateway 的效率或效能。如果使用 delete file *file* 指令來刪除日誌檔或暫存檔案，則可能會遺失某些日誌資料。若要刪除日誌檔，請在日誌元件群組中指定一個元件。

如果使用 delete file *file* 指令刪除個別的日誌檔，請重新啟動適用於所刪除之日誌檔的服務。例如，如果您刪除控管中心日誌檔 Brightmaillog.log，請重新啟動控管中心服務。使用 service 指令或控管中心來重新啟動服務。

可以使用以下元件，這些元件列示於類似行為的群組中。

日誌元件：

alllogs

刪除日誌元件群組中的所有日誌。

`bcclogs`
: 刪除所有控管中心日誌。

`ddslogs`
: 刪除所有目錄資料服務日誌。

`mallogs`
: 刪除所有郵件稽核日誌。

`oslogs`
: 刪除所有作業系統日誌。

`scannerlogs`
: 刪除所有掃描程式日誌。

組態元件：

`allconfig`
: 刪除組態元件群組中的所有組態資料。

`bccconfig`
: 刪除所有控管中心組態檔。

`clearsockets`
: 刪除 `/var/tmp` 目錄中的所有通訊端檔案。

`scannerconfig`
: 刪除指定掃描程式的所有掃描程式組態檔 (包括支援過濾指令碼)。它不影響已儲存在控管中心內的掃描程式組態資訊。

  執行 `delete scannerconfig` 時，它會重新啟動執行指令的硬體裝置。執行 `delete scannerconfig` 後，您必須將掃描程式組態資訊從控管中心重新提交到磁碟，並且對掃描程式重新授權。

  您可以不經變更就將掃描程式資訊重新提交到磁碟，也可以在儲存到磁碟之前先編輯該資訊，以修正可能的問題。若要執行上述任一工作，請在控管中心內存取**「管理」>「主機」>「組態」**，然後選取「掃描程式」，再按下**「編輯」**。若要重新提交未變更的資訊，請按下**「儲存」**。或者，視需要編輯此掃描程式的任何設定以修正組態中的問題，然後按下**「儲存」**。

  如果變更某個獨立掃描程式硬體裝置的掃描程式組態，則可將其刪除，然後可以使用「新增掃描程式精靈」再次新增該掃描程式組態。此選項不適用於同時執行控管中心與掃描程式的硬體裝置。

  賽門鐵克建議不要使用 `delete scannerconfig`。

資料元件：

`alldata`
: 刪除資料元件群組中的所有資料。

`bccdata`

刪除所有控管中心資料(包括所有授權檔案)。之後，您的組態即與首次安裝產品時的控管中心組態相同。

`ddsdata`

刪除所有目錄資料服務資料。

`keystore`

從 keystore 刪除控管中心 HTTPS 憑證。

`scannerdata`

刪除 MTA 佇列的郵件以及下列檔案：

`/data/scanner/rules/matchEngine/tmp/data_match_engine_jce_keystore`

`spcdata`

刪除所有 Symantec Protection Center (SPC) 資料，然後解除註冊任何 Symantec Messaging Gateway SPC 實例。使用 `spcdata` 之後，您必須向 SPC 伺服器重新註冊控管中心，以繼續將控管中心與 SPC 搭配使用。

`statsdata`

從掃描程式刪除 stats 檔案。

`sudata`

刪除與軟體更新相關的所有檔案。

隔離所元件：

`allquarantine`

從所有隔離所刪除所有郵件。

`contentquarantine`

刪除所有內容隔離所郵件和資訊郵件。

`spamquarantine`

從垃圾郵件隔離所刪除所有郵件。

`virusquarantine`

從可疑病毒隔離所刪除所有郵件。

規則元件：

`allrules`

刪除所有規則，並使用出廠預設規則加以取代。

`avrules`

刪除所有防毒規則，並使用出廠預設規則加以取代。

`bodyhashrules`

刪除 bodyhash 規則，並使用出廠預設規則加以取代。

`dayzerorules`

刪除所有初始規則，並使用出廠預設規則加以取代。

`fastpassrules`

刪除所有快速通過規則。

`gatekeeperrules`

刪除閘道管理員防垃圾郵件規則，並使用出廠預設規則加以取代。

`intsigrules`

刪除所有 IntSig 規則，並使用出廠預設規則加以取代。

`ipfreqrules`

刪除 IP 頻率規則。

`permitrules`

刪除 permit 規則，並使用出廠預設規則加以取代。

`regexrules`

刪除規則運算式過濾規則。

`spamhunterrules`

刪除所有 Spamhunter 規則，並使用出廠預設規則加以取代。

`spamsigrules`

刪除 spamsig 規則，並使用出廠預設規則加以取代。

`statsigrules`

刪除 statsig 規則，並使用出廠預設規則加以取代。

附註：`delete` 指令可能需要 30 秒的時間才能刪除規則。請等候指令提示返回，然後再執行其他指令。請勿在執行 `delete` 指令時按 **Ctrl+C** 來停止該指令。

其他元件：

`all`

刪除所有日誌、組態資料、密碼、支援過濾指令碼、掃描程式資料、核心、診斷套件、規則、佇列資料、SPC 資料以及備份檔案，以將硬體裝置還原至原始出廠組態。

`bcchostacl`

刪除在**「管理」>「設定」>「控管中心」**頁面上進行的掃描程式存取控制，以允許從所有掃描程式進行存取。

`cores`

刪除所有核心目錄。

`database`

刪除使用 `db-backup` 建立的所有控管中心資料庫備份。

`diagnostics`

刪除所有診斷套件。

`fips`

刪除 fips 設定，並以非 FIPS 模式的出廠預設值設定加以取代。

`help`

顯示您可以刪除的元件的摘要。

`monitor`

刪除使用 `monitor` 指令建立的檔案。

範例

範例 1

刪除 `BrightmailLog.log` 檔案。

```
delete file /data/logs/bcc/BrightmailLog.log
```

範例 2

刪除垃圾郵件隔離所的所有郵件。

```
delete spamquarantine
```

範例 3

刪除硬體裝置上儲存的所有控管中心資料庫備份檔案 (除了三個最新的備份檔案之外)。

```
delete --purge 3 database
```

另請參閱

請參閱第 636 頁的cat。

請參閱第 670 頁的list。

請參閱第 685 頁的more。

請參閱第 536 頁的「清除磁碟空間檢查清單」。

diagnostics

`diagnostics` – 產生診斷套件

大綱

`diagnostics [options] url`

說明

`diagnostics` 指令會產生診斷套件，賽門鐵克支援可使用該診斷套件來分析產品的問題。

除非您使用 `--find-other-cores` 選項，否則應指定有效的 URL。如果您指定了有效的 URL，但未指定資料收集選項，則依據預設，`diagnostics` 會使用下列參數：

```
--config --crash-info 5 --logs 100000
```

這些參數可產生具有以下內容的診斷套件：

- 組態資料
- /data/scanner/jobs 下每項工作的五個最新核心目錄 (不含這些目錄中的核心檔案)
- 日誌資料 (每個檔案最多 100,000 行)

如果您指定任何選項，則不會包含這些參數，除非您明確地將這些參數新增到指令中。

URL 中包含使用者名稱或密碼時，如果其中包含任何特殊 shell 字元，則應將使用者名稱或密碼包含在引號中。可在 URL 中或密碼提示時指定密碼。URL 語法的範例如下所示：

```
scp://'user':'password'\@host[:port]/path
```

如果您指定以正斜線結尾的路徑，則會將診斷檔案寫入所指定具有預設檔案名稱的路徑。如果您指定不是以正斜線結尾的路徑，則會寫入具有路徑中所指定檔案名稱的備份檔案。

預設診斷檔案名稱具有下列格式：

```
diagnostics.yy-mmm-dd-hh-mm.hostname.tar.gz
```

例如： `diagnostics.09-Sep-10-15-42.host9902.symantecexample.com.tar.gz`

無論選項是完整形式還是簡短形式，指定選項均不可超過一次。對於 `--cores` 選項，使用元件名稱或便利字串 `all` 指定元件不可超過一次。如果您嘗試指定重複的選項，則會顯示錯誤訊息以及相應的用法文字。

選項

`--bad-messages, -b`

收集 MTA 錯誤郵件。

`--config, -c`

僅收集組態資料。組態資料包括 Symantec Protection Center (SPC) 註冊詳細資料 (如果有)。

`--cores, -o componentn`

收集最新的 *n* 個核心目錄，包括元件的核心檔案。*n* 的有效範圍是 1 到 9,999。

元件的清單包含下列內容：

- `--cores mta n` 收集 MTA 核心套件
- `--cores bmagent n` 收集 Brightmail 代理程式核心套件
- `--cores bmserver n` 收集 Brightmail 伺服器核心套件
- `--cores conduit n` 收集管道核心套件
- `--cores jlu-controller n` 收集 Java LiveUpdate 核心套件
- `--cores dds n` 收集目錄資料服務核心套件
- `--cores other n` 收集未使用其他選項收集的其他核心檔案。
- `--cores all n`
  `all` 是便利的識別碼，代表所有元件。

`--crash-info n, -a`

為以下程序收集最新的 *n* 個核心目錄 (這些目錄中的核心檔案除外)：

- mta
- bmagent
- bmserver
- conduit
- jlu-controller
- dds

n 的有效範圍是 1 到 9,999。

`--edm, -e`

收集完全資料符合 (EDM) 記錄集。

`--find-other-cores, -d`

搜尋 `/data/scanner/jobs` 以外的所有核心檔案，並將這些核心檔案移至 `/data/scanner/jobs/other`。

如果 Symantec Messaging Gateway 發現任何核心檔案並進行移動，則會傳送電子郵件通知給所指定接收警示的管理員。如果未發現，則不會傳送任何電子郵件通知。

您可以將此選項與 `delete cores` 指令配合使用，以清除產品上的核心檔案。請先執行此指令，將並非位於 jobs 目錄的核心檔案移至 jobs 目錄。然後使用 `delete cores` 刪除核心檔案。

如果 `--find-other-cores` 是唯一指定的資料收集選項，則不需要 URL。不會產生任何診斷套件。

`--force, -f`

強制執行診斷，即使從使用者介面啟動的診斷收集仍在進行中，也是如此。如果正在建立套件，則現有的診斷收集將失敗。

`--gcore, -g` *component*

產生指定元件的核心影像，並下載它。您可以使用此選項在重新啟動元件之前，擷取有關無回應或運作中元件的必要資料。此選項不會停止或重新啟動程序，但可能造成程序短暫暫停。可用的元件包括：

- `bmagent`
- `bmserver`
- `conduit`
- `mta`
- `jlu-controller`

`--help, -h`

顯示此郵件。

`--include-old-queues, -i`

從舊的 postfix 佇列中收集佇列資料。

此指令僅適用於從 7.7 版或更舊版本移轉 Symantec Messaging Gateway 的組態。此指令不適用於 Symantec Messaging Gateway 版本 8 或更高版本。

`--ldap, -p`

收集舊式 ldapsync 資料。

此指令僅適用於從 8 版或更舊版本移轉 Symantec Messaging Gateway 的組態。此指令不適用於 Symantec Messaging Gateway 版本 9 或更高版本。

`--logs all, -l`

收集所有日誌檔的全部日誌。

`--logs` *n*`, -l`

收集僅限於每個日誌檔之 *n* 行的日誌資料。

n 的有效範圍是 1 到 2,147,483,647。

`--monitor, -m`

收集下列 `monitor` 指令的快照輸出：`monitor -c 6 --proc bmserver --proc mta system database disk mta p_all` 和 `/data/monitor` 下的現有監控日誌。

`--rules, -r`

收集掃描程式上出現的所有規則 (完全資料符合的資料除外)。

`--tracking, -t`

收集郵件稽核日誌檔案。

`--verbose, -v`

在詳細資訊模式下顯示指令程序。

引數

此指令所參照 URL 路徑的語法如下：

- scp://'user':'password'\@host[:port]/path
  透過 SCP 從遠端複製診斷套件。
- ftp://'user':'password'\@host[:port]/path
  透過 FTP 從遠端複製診斷套件。
  如果未指定任何使用者名稱和密碼，則會使用匿名登入。

會嘗試使用在指令行上提供的使用者名稱和密碼憑證進行登入。如果密碼包含特殊字元，必須以單引號 (') 括住密碼。如果密碼中的特殊字元包含單引號，則可改用雙引號 (")。若未指定任何憑證，則會使用匿名登入。

範例

建立診斷檔案，並使用 SCP 通訊協定進行傳輸。會將診斷檔案 (格式為：`diagnostics.yy-mmm-dd-hh-mm.hostname.tar.gz`) 傳輸到 SCP 目的地。

```
diagnostics scp://'support'@10.160.248.128/tmp/
```

附註：月份會以三字母格式 (而非兩位數格式) 表示。

dns-control

dns-control – 控制本機 DNS 快取

大綱

dns-control *command*

說明

dns-control 指令會管理名稱伺服器的本機快取。

所有 dns-control 指令輸出的結尾都是完成訊息或錯誤訊息。範例包括「指令 cmdname 已成功完成」及「指令 cmdname 失敗」。

某些指令需要先執行 DNS 快取，然後才能執行。在這些情況下，唯一的輸出為：「DNS 快取目前已停止」。請使用 dns-control start 指令啟動快取，然後再執行這些指令。

引數

指令元件如下所示：

start
: 啟動本機快取名稱伺服器。

stop
: 停止本機快取名稱伺服器。

restart
: 重新啟動本機快取名稱伺服器。

狀態
: 顯示本機快取名稱伺服器的狀態。

flush
: 清除快取。

list
: 為解析程式列出本機架構的名稱伺服器。

trace
: 遞增追蹤 (除錯) 層級 (+1)。

notrace
: 停用追蹤 (除錯)。

`reconfig`

強制重新載入名稱伺服器組態資訊。

`help`

顯示此頁面。

fipsmode

`fipsmode` – 啟用、停用或檢查 FIPS 模式

大綱

```
fipsmode --help

fipsmode(on|off|status)
```

說明

啟用、停用或檢查硬體裝置的 FIPS 模式的狀態 (無論硬體裝置是否為 FIPS 模式)。變更 FIPS 模式的狀態會提示重新開機。

`fipsmode` 會將其動作記錄至 syslog /data/logs/messages。

選項

`--help, -h`
顯示使用資訊。

引數

`on`
開啟 FIPS 模式。會提示您允許重新開機。

如果當系統已在 FIPS 模式中時呼叫 `fipsmode on` 指令，則程序檔會回報「未變更 FIPS 模式」。

`off`
關閉 FIPS 模式。會提示您允許重新開機。

如果當系統不在 FIPS 模式中時使用 `fipsmode off` 指令，則程序檔會回報「未變更 FIPS 模式」。

狀態
顯示主機為「FIPS 模式」或「非 FIPS 模式」。

grep

grep – 在檔案中搜尋文字或規則運算式

說明

grep 指令會在您指定的檔案中搜尋文字或規則運算式。

如需 grep 可用選項的詳細資訊，請在指令行輸入 grep --help。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是標準 Linux 指令，在 Symantec Messaging Gateway 中無法完全發揮其效用。管理員只能將 grep 用於：

- 可透過 list 指令取得的檔案名稱。
- 透過將其他指令的輸出傳送給 grep 指令。

help

help – 顯示個別指令的說明或顯示所有可用指令

大綱

```
help [ --list | command ]
```

說明

help 指令可顯示產品的可用指令清單。如果您指定指令名稱，則 help 指令會顯示該指令的說明。

指令的說明以 Linux 手冊頁格式來顯示。這些說明頁面使用下列 Linux 手冊頁慣例。執行指令時請勿輸入方括弧、圓括弧或管道字元符號。

Brackets [ ]
: 方括弧中列示的選項和引數為選用項目。未在方括弧中列示的選項和引數為必要項目。

Parenthesis ( )
: 圓括弧中列示的選項和引數為必要項目，但彼此互斥。管道字元符號會分隔彼此互斥的選項或引數。

Pipe |
: 管道字元符號代表彼此互斥的選項或引數。例如，[-e *pattern* | -f *file*] 表示您可以指定 -e *pattern* 或 -f *file*，但無法同時指定這兩者。

Colored, italic, or underlined text
: 斜體、彩色或加上底線的文字代表您應該使用指定文字來替代該文字。輸入 help *command* 時，您用來存取指令行的終端機或終端機軟體會確定此文字的顯示方式。檢視 PDF 或線上說明形式的說明頁面時，此類文字會以斜體顯示。

--option, -o
: 某些指令選項具有完整形式與簡短形式。完整形式和簡短形式會產生相同行為。請使用對您最方便的形式。在「選項」部分，這些選項會先以完整形式顯示，後接逗號，然後顯示簡短形式。完整形式前加兩個破折號，而簡短形式前加一個破折號。某些選項需要您在該選項後指定參數，例如記錄層級或 IP 位址。

說明頁面包含以下部分：

概要
: 指令可用選項與引數的說明。

說明
: 關於指令的一般資訊。

選項

您可以用來控制指令行為的選項。選項始終以一或兩個破折號開頭，例如 `-s` 或 `--status`。如果「概要」中的方括弧中列出了某個選項，則代表其為選用選項。否則即為必要選項。

某些選項具有引數。例如，`--log`*level*。方括弧代表選用引數。

並非所有指令都有選項。

引數

某些指令需要使用引數。引數包括檔案名稱、主機名稱、IP 位址等等，您可以指定這些引數來控制指令行為。並非所有指令都有引數。

範例

「範例」部分提供了指令用法範例。並非所有指令都有範例。

另請參閱

「另請參閱」部分列出了相關指令。並非所有指令都有「另請參閱」參照。

使用下列指令可在說明頁面中瀏覽：

`f` **或** `SPACE`

下一個畫面

`b`

上一個畫面

`/pattern`

搜尋單字或樣式

`<`

移至文件開頭

`>`

移至文件結尾

`q`

結束文件，並顯示指令提示

`h`

顯示有關瀏覽說明頁面的其他資訊

選項

`--list, -l`

顯示所有可用指令的清單。

引數

command

顯示特定指令的說明。

如果您未指定指令，則會顯示 `help` 指令的說明 (此頁面)。指定下列其中一個指令：

`agent-config`

架構將主機連線至控管中心的代理程式

`cat`

用來檢視檔案的標準 Linux 指令

`cc-config`

架構控管中心的記錄與網路存取

`clear`

用來清除畫面的標準 Linux 指令

`db-backup`

備份控管中心資料庫

`db-restore`

從先前建立在硬體裝置上的備份，或透過 FTP、SCP 和 HTTP 從遠端位置將 Brightmail 資料庫還原至硬體裝置

`delete`

清除日誌、組態資訊及資料

`diagnostics`

產生診斷套件

`dns-control`

控制本機 DNS 快取

`fipsmode`

啟用、停用或檢查 FIPS 模式

`grep`

在檔案中搜尋文字或規則運算式的標準 Linux 指令

`help`

顯示個別指令的說明或顯示所有可用指令

`ifconfig`

用來架構網路介面的標準 Linux 指令

`iostat`

用來顯示 CPU 和裝置負載的標準 Linux 指令

`ip`

擷取正由 Symantec Messaging Gateway 使用的位址資訊

`ldapsearch`

用來查詢 LDAP 目錄的標準 Linux 指令

`list`

顯示特定指令可以操作的所有檔案的檔案名稱

`mallog`

列出、備份或還原郵件稽核日誌

`malquery`

查詢郵件稽核日誌

`monitor`

檢視和記錄 Brightmail 專屬程序的相關資訊

`more`

用來翻頁瀏覽文字檔案的標準 Linux 指令

`mta-control`

控制 MTA 程序，以及備份與還原郵件佇列

`netstat`

用來檢視網路連線的標準 Linux 指令

`nslookup`

用來查詢 DNS 伺服器的標準 Linux 指令

`password`

變更管理密碼

`ping`

用來測試遠端電腦回應的標準 Linux 指令

`ping6`

測試發出機器和所提供的 IPv6 主機名稱或 IP 位址之間的資料傳輸

標準 Linux 指令

`patch`

處理與修補程式相關的所有必要函數

`reboot`

重新啟動硬體裝置

`route`

用來顯示和操作 IP 繞送表的標準 Linux 指令

`rpmdb`
: 管理與修復 RPM 資料庫

`service`
: 用來啟動或停止服務的標準 Linux 指令

`show`
: 顯示系統資訊

`shutdown`
: 關閉硬體裝置但不重新啟動

`sshd-config`
: 架構使用 SSH 可連線至硬體裝置的位址

`tail`
: 用來檢視檔案結尾的標準 Linux 指令

`telnet`
: 用來連線至遠端電腦的標準 Linux 指令

`traceroute`
: 用來檢視網路封包所採用路徑的標準 Linux 指令

`traceroute6`
: 追蹤繞送至提供之主機名稱或 IPv6 位址的網路路由

`update`
: 更新硬體裝置軟體

歷史記錄

在 Symantec Brightmail Gateway 9.0 版中，某些存在於 8.0 版和舊版的指令會重新命名、併到其他指令中，或是移除。以下是 9.0 版中經過變更的指令：

`agentconfig`
: 取代為 `agent-config`。

`clear`
: 取代為 `delete`。在 9.0 版中，`clear` 指令可以清除畫面。

`crawler`
: 併入 `diagnostics`。

`date`
: 取代為 `show --date`。

`deleter`
: 取代為 `delete cores`。

`dn-normalize`

`dn-normalize` 指令的功能不適用於 9.0 版。

`eula`

取代為 `show --eula`。

`http`

取代為 `cc-config http`。

`install`

取代為 `update install`。

`ls`

取代為 `list`。

`mta-stats`

取代為 `monitor mta`。

`passwd`

取代為 `password`。

`pause-mode`

取代為 `mta-control pause-mode`。

`rebuildrpmdb`

取代為 `rpmdb --repair`。

`rm`

取代為 `delete files`。

`set-control-center-port-443`

取代為 `cc-config port-443`。

`sshdctl`

取代為 `sshd-config`。

`sshdver`

取代為 `sshd-config --version`。

`sys-info`

取代為 `show --info`。

`system-stats`

取代為 `monitor system`。

`tls-ca-cert-control`

`tls-ca-cert-control` 指令的功能不適用於 9.0 版。

ifconfig

`ifconfig` – 用來架構網路介面的標準 Linux 指令

說明

`ifconfig` 指令顯示網路介面的狀態和組態，並且可以對介面組態進行臨時變更。

如需 `ifconfig` 可用選項的詳細資訊，請在指令行輸入 `help ifconfig`。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

iostat

`iostat` – 用來顯示 CPU 和裝置負載的標準 Linux 指令

說明

`iostat` 指令透過觀察時間裝置相對於其平均傳輸速率是否為作用中狀態，來監控系統輸入/輸出裝置載入。

如需 `iostat` 可用選項的詳細資訊，請在指令行輸入 `help iostat`。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

ip

ip – 擷取 IP 位址相關資訊的標準 Linux 指令

說明

ip 指令可讓您檢視及修改 IP 位址的相關資訊。

如需 ip 可用選項的詳細資訊，請在指令行輸入 help ip。所顯示的資訊可能包含 Symantec Messaging Gateway 並未提供之指令的參考。

ldapsearch

`ldapsearch` – 用來查詢 LDAP 目錄的標準 Linux 指令

說明

`ldapsearch` 指令會在您指定的 LDAP 來源中進行搜尋，並顯示相符記錄。

如需 `ldapsearch` 可用選項的詳細資訊，請在指令行輸入 `help ldapsearch`。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

list

`list` – 顯示特定指令可以操作的所有檔案的檔案名稱

大綱

```
list [--all] [--cores] [--diagnostics] [--logs] [--monitor] [--temp] [--top]

list --help
```

說明

`list` 指令可顯示能夠由特定指令操作的所有檔案的檔案名稱。下列指令可以操作使用 `list` 所列出的檔案：

`cat`
: 顯示一或多個檔案的內容。

`delete`
: 刪除一或多個檔案。

`more`
: 顯示一或多個檔案的內容，並且在各個畫面的結尾暫停。

`tail`
: 顯示指定日誌檔的最後 50 行。

選項

指定某個選項時，如果 `list` 未列出任何檔案，則表示該類別中沒有任何檔案。

`--all, -a`
: 列出所有檔案。

`--cores, -c`
: 列出所有核心檔案。

`--diagnostics, -d`
: 列出所有診斷套件。

`--help, -h`
: 顯示此郵件。

`--logs, -l`
: 列出所有日誌檔。

`--monitor, -m`

列出所有監控檔案。

`--temp, -p`

列出所有暫存檔。

`--top, -t`

列出管理員可以刪除的最大檔案以及其大小。

範例

範例 1

列出可以使用 `cat` 檢視的所有檔案 (除了核心檔案和診斷檔案之外)，或可以使用 `delete` 刪除的所有檔案。

```
list --all
```

範例 2

列出您可以刪除的最大檔案。如果您不需要大型檔案，可以使用 `delete` 指令將其刪除。

```
list --top
```

另請參閱

請參閱第 636 頁的cat。

請參閱第 647 頁的delete。

請參閱第 685 頁的more。

mallog

mallog – 列出、備份或還原郵件稽核日誌

大綱

```
mallog [ --list ]

mallog [ --backup | --restore ] url
```

說明

mallog 指令會備份和還原位於掃描程式中的郵件稽核日誌資料。mallog 指令也會列出掃描程式中的郵件稽核日誌檔案。若要檢視郵件稽核日誌中的郵件活動，請使用控管中心或 malquery 指令。

可用的日誌檔包括：

- /data/logs/scanner/audit_bmengine_log*
- /data/logs/scanner/audit_mte_log*
- /data/logs/scanner/audit_mta_log*

附註：執行 mallog --backup 或 mallog --restore 指令時，會停止處理電子郵件。此時不會傳送任何入埠電子郵件或離埠電子郵件。如果您組織的電子郵件可用性政策很嚴格，那麼限制只在下班時間執行這些指令，可能比較適當。

選項

--backup *url*

建立 tar.gz 格式之所有郵件追蹤日誌的備份，並將產生的檔案上載至指定的 URL。

附註：此選項會在執行指令時中斷郵件處理。

--list

列出檔案系統上的個別郵件追蹤日誌，及其時間戳記與大小。

--restore *url*

從指定的 URL 還原郵件追蹤日誌。現有的日誌會被覆寫。

附註：此選項會在執行指令時中斷郵件處理。

URL 可採用 FTP、SCP 或 HTTP 配置 (僅供還原)。

如果您指定以正斜線結尾的路徑，則會將診斷檔案寫入所指定具有預設檔案名稱的路徑。如果您指定不是以正斜線結尾的路徑，則會寫入具有路徑中所指定檔案名稱的備份檔案。`--restore` 選項需要使用包含檔案名稱的完整路徑名稱。整個 URL 應包含在雙引號中。如果 URL 的任何部分包含特殊字元 (例如全引號或雙引號)，請使用反斜線來逸出特殊字元。如果密碼是 URL 的一部分，並且其中包含特殊 shell 字元，則應將該密碼包含在引號中。

`url`

將套件透過 SCP 或 FTP 傳輸至 *url* 位置。

整個 URL 應包含在雙引號中。如果 URL 的任何部分包含特殊字元 (例如全引號或雙引號)，請使用反斜線來逸出特殊字元。如果密碼是 URL 的一部分，並且其中包含特殊 shell 字元，則應將該密碼包含在引號中。

另請參閱

請參閱第 674 頁的malquery。

malquery

`malquery` – 查詢郵件稽核日誌

大綱

```
malquery (-l start,end | -g start,end | -s start [ -n end] | -p range)

(-u uid [-u uid ...] | -e event[,arg_num]<=|*>string [-e ...] | -q
event[,arg_num]<=|*>quoted-printable-string [-q ...])

[-m max_results] [-I index_max] [-o url] [-v]
```

說明

您可以透過查詢郵件稽核日誌，在控管中心內追蹤郵件。或者，您也可以使用 `malquery` 指令行指令來追蹤郵件。如果是複雜查詢或可能產生大量資料的查詢，請使用 `malquery`，而不用控管中心。`malquery` 指令僅會傳回您登入之掃描程式的資料。

啟用郵件稽核記錄會導致每封郵件產生大約 800 位元組的稽核日誌。如果您的網站每天收到 1,000,000 封以上的郵件，郵件稽核記錄可能會引起效能及儲存問題。

比目前日期還舊的稽核記錄會往後延，其檔名會加上格式為 yyyymmdd 的當地日期。而比預設保留期限 2 天還舊的稽核日誌則會加以刪除。

malquery 指令行產生的結果既不反映控管中心所產生的事件，也不反映那些在其他掃描程式上產生的事件。

`malquery` 會輸出為 .xml 格式，例如：

```
<malResults count="message result count">
        <message AID="aid">
            <events>
                <event time="utc" name="event id">parameters</event>
                <event time="utc" name="event id">parameters</event>
                <event time="utc" name="event id">parameters</event>
                <event time="utc" name="event id">parameters</event>
            </events>
        </message>
</malResults>
```

選項

`-a, --audit` *`audit_id`*

尋找具有指定稽核 ID (aid) 的電子郵件訊息。

`-e ..., --event`

尋找包含符合指定條件之事件的電子郵件。

範例：

-e RCPTS=dale@company.com

RCPTS 為收件者。在此範例中，收件者為 dale@company.com。

-e "SUBJECT*my flowers"

SUBJECT 為電子郵件訊息的主旨。在此範例中，主旨包含文字 my flowers。

使用等於字元 (=) 表示完全相符。使用星號 (*) 表示包含。搜尋不區分大小寫。

您可以搜尋的更多常用元素清單如下：

- ACCEPT
  連線 IP
- ATTACH
  附件檔案名稱
- MSGID
  郵件 ID
- RCPTS
  收件者位址
- SENDER
  寄件者位址
- SUBJECT
  郵件主旨

`-g, --gmt start,end`

依 GMT 日期範圍尋找要在 UNIX 時間 (自 1/1/1970 新紀元時間之後所經過的時間單位數) 中搜尋的郵件。例如，

July 4, 2008, 11:59 P.M. = 1215212340。

請以逗號 (不含空格) 分隔開始日期與結束日期。

`-i, --index index_max_n`

如果相符結果數量小於或等於 *index_max_n*，請使用索引 (.idx 檔案)。否則會忽略索引。此選項會搜尋一般文字檔案，在查詢大量事件時可節省時間。

index_max_n 的預設值為 1000。

`-l, --date start,end`

要搜尋的日期範圍。日期格式為 YYYYMMDDhhmm。例如：

July 4, 2008, 11:59 P.M. = 200807042359。

請以逗號 (不含空格) 分隔開始日期與結束日期。

`-m, --max max_results`

傳回 *max_results* 則郵件。預設值為 1000。

`-n, --end`

要搜尋之日期範圍的結束日期。日期應使用以下格式：YYYYMMDDhhmm。例如：

July 4, 2008, 11:59 P.M. = 200807042359。

`-o, --output file`

將符合結果的資料輸出至指定的 URL。

使用包含以下語法的 SCP 或 FTP URL：

scp://'user':'password'@host[:port]/path

如果您指定以正斜線 (/) 結尾的路徑，則會將檔案寫入所指定具有預設檔案名稱的路徑。如果您指定不是以正斜線結尾的路徑，則會寫入具有路徑中所指定檔案名稱的檔案。URL 中包含使用者名稱或密碼時，如果其中包含任何特殊 shell 字元，則應將使用者名稱或密碼包含在引號中。您可以在 URL 中或密碼提示時指定密碼。

例如：

```
malquery -p 1h -e RCPTS=dale@company.com -e "SUBJECT*check this out" \ -m
500 -o ftp://evan@ftp.company.com/home/evan/audit.info.txt
```

`-p, --previous`

搜尋上次的範圍時間。

範圍時間的格式為 <integer><*type*>，其中 *type* 是 m (分鐘數)、h (時數)、d (天數) 或 w (週數)。

例如，5h 會搜尋最近 5 小時。

`-q ..., --qevent`

尋找包含符合指定條件之事件且具有 quoted-printable 編碼的電子郵件。例如：

-q "SUBJECT*red =3D rose" -- subject contains 'red = rose'

使用等於字元 (=) 表示完全相符。使用星號 (*) 表示包含。搜尋不區分大小寫。

您可以搜尋的更多常用元素清單如下：

- ACCEPT
  連線 IP
- ATTACH
  附件檔案名稱
- MSGID
  郵件 ID
- RCPTS

收件者位址

- SENDER
  寄件者位址
- SUBJECT
  郵件主旨

`-s, --start`

要搜尋之日期範圍的開始日期。日期應使用以下格式：YYYYMMDDhhmm。例如：July 4, 2008, 11:59 P.M. = 200807042359。

`-v, --verbose`

在詳細資訊模式下顯示指令程序 (偵錯記錄)。

範例

範例 1

根據下列條件搜尋電子郵件：

- 開始日期介於 2008 年 7 月 4 日下午 2:00 與 2008 年 7 月 4 日下午 11:59 (GMT 時間) 之間
- 收件者為 dale@company.com
- 主旨包含文字 check this out
- 輸出上限為 500 個結果
- 透過 FTP 將輸出傳送至 host.domain.com 上的 user

```
malquery -g 1215140340,1215212340 -e RCPTS=dale@company.com -e "SUBJECT*check
this out" -m 500 -o
ftp://user:password@host.domain.com/home/user/malquery_output.xml
```

範例 2

根據下列條件搜尋電子郵件：

- 開始日期介於 2009 年 7 月 4 日下午 11:00 與 2009 年 7 月 4 日下午 11:59 之間。
- Audit ID：0aa0f22b-b7c99ae000005dd7-47-4e6e7b0468ad
- 輸出上限為 500 個結果

```
malquery -l 200907042300,200907042359 -a
0aa0f22b-b7c99ae000005dd7-47-4e6e7b0468ad -m 500
```

範例 3

根據下列條件搜尋電子郵件：

- 開始日期介於 2009 年 7 月 4 日下午 11:00 與目前時間之間
- 收件者是使用 quoted-printable 編碼字串的 dale@company.com
- 主旨包含使用 quoted-printable 編碼字串 Barney=27s Grill 的 Barney's Grill 文字
- 輸出上限為 500 個結果

```
malquery -s 200907040000 -q RCPTS=3Ddale@company.com -q "SUBJECT*Barney=27s
Grill" -m 500
```

範例 4

根據下列條件搜尋電子郵件：

- 日期在最近 2 天內
- 收件者為 dale@company.com
- 主旨包含文字 check this out
- 此指令的相符結果數量預設為 1000 (index_max)
- 透過 SCP 將輸出傳送至 host.domain.com 上的 user

```
malquery -p 2d -e RCPTS=dale@company.com -e "SUBJECT*check this out" -i -o
scp://user:password@host.domain.com/home/user/malquery_output.xml
```

範例 5

搜尋因信譽判斷而遭拒絕的郵件的稽核日誌：

- 日期在最近 3 小時內

```
malquery --previous 3h --event "RCPTS=<NONE>"
```

另請參閱

請參閱第 672 頁的mallog。

monitor

monitor – 檢視和記錄 Symantec Messaging Gateway 專屬程序的相關資訊

大綱

```
monitor options [--proc name] [identifier ...]

monitor list

monitor stop ( pid | all )
```

說明

monitor 指令可讓您檢視和記錄 Symantec Messaging Gateway 及其程序的相關詳細資訊。

選項

--count, -c *num*

產生 *num* 個範例。

預設值為 1。上限是 2^31-1 (大約 21 億)。

--help, -h

顯示此郵件。

--interval, -i *num*

以間隔 *num* (單位為秒) 進行取樣。

預設值為 10 秒。若為寫入磁碟之任何長時間執行的監控工作，則應增加此間隔 (至 60 或以上)。如果磁碟空間已滿，則 monitor 程序會停止。請增加間隔時間以避免發生此問題。

--output, -o *file*

將輸出儲存至檔案，而非列印至主控台。檔案會另存為 /data/monitor/*file*。

使用此選項時，monitor 會於背景中執行，並傳回監控程序的程序 ID (PID)。使用 cat、more 或 tail 來檢視檔案。檔案名稱可包含 ASCII 字元。

--proc, -p *name*

收集下列其中一個 Symantec Messaging Gateway 程序及其子系的資料。這些程序及其子系所代表的有效程序名稱及程式如下：

bmagent

Brightmail 代理程式可為控管中心與各掃描程式之間的組態資訊通訊提供便利。

bmserver

bmserver 程序可過濾電子郵件訊息。

conduit
「管道」可擷取更新的電子郵件過濾器並管理統計資料。

controlcenter
控管中心提供集中化的 Web 管理，可收集統計資料並託管隔離所。

liveupdate
LiveUpdate 會從賽門鐵克安全機制應變中心將病毒定義下載至掃描程式。

lsisnmpd
lsisnmpd 程序提供某些 Dell PowerEdge 可擴充 RAID 控制器的 SNMP 資訊。

所有目前支援的硬體應正在執行 lsisnmpd 程序。目前支援的虛擬環境不應執行此程序。

monitor
monitor 程序會顯示或儲存 Symantec Messaging Gateway 程序的相關資訊。

mta
郵件傳輸代理程式會將入埠和離埠郵件繞送到 Brightmail 引擎進行處理，並傳送過濾的郵件。

mysql
控管中心的 MySQL 資料庫可儲存設定和郵件資訊。

snmpd
snmpd 程序會等候來自 SNMP 管理軟體的要求。

--quiet, -q
抑制來自監控程式的任何警告。

--tab, -t
產生表格格式的資料。搭配使用 --tab 選項和 --output 選項，可以建立要匯入試算表的輸出。--tab 不會正確設定畫面的文字格式。例如，畫面上的欄標題不會與欄資料對齊。

設定 --tab 表格式輸出的資料格式時，每個識別碼的欄標題都會以程序名稱作為開頭。例如 controlcenter_p_%user。

引數

list
產生所有監控程序、其 PID，以及執行時期所用選項的清單。monitor list 指令始終會將 monitor list 指令顯示為其中一個執行中的監控程序。這是正常行為。

stop (*pid* | all)
停止指定的監控程序。輸入 PID 可停止單一程序。輸入 all 單字可停止所有監控程序。

identifiers

顯示或儲存的資訊取決於您指定的識別碼。如果您未指定一或多個識別碼，則會使用預設值 `system`。某些識別碼可表示多個識別碼，為了方便使用均已提供。可用的五組識別碼為： 系統、資料庫、磁碟、MTA 和程序。

系統識別碼如下：

- `%user` - 在使用者模式中所用的可用 CPU 時間百分比。
- `%nice` - 作為 nice 執行時所用的可用 CPU 時間百分比。
- `%sys` - 在系統模式下所用的可用 CPU 時間百分比。
- `%wait` - 在 IO 等待時所用的可用 CPU 時間百分比。
- `%idle` - 閒置時所用的可用 CPU 時間百分比。
- `memt` - 總記憶體 (k)
- `memu` - 使用中記憶體 (k)。
- `pageout` - 交換到磁碟的記憶體頁數。
- `system` - 便利的識別碼，包括下列系統識別碼：`%user %sys %wait memt memu memf.`

資料庫識別碼 - 這些識別碼代表控管中心資料庫的大小、控管中心各種隔離所的大小，以及其中所包含的郵件數量。這些識別碼如下：

- `db_size` - 控管中心資料庫的總計大小 (KB)。
- `db_qsize` - 垃圾郵件隔離所目錄的大小 (KB)。
- `db_qqty` - 垃圾郵件隔離所中的郵件數量。
- `db_vsize` - 可疑病毒隔離所目錄的大小 (KB)。
- `dv_vqty` - 可疑病毒隔離所中的郵件數量。
- `db_csize` - 內容資安事端目錄的大小。
- `db_cqty` - 內容資安事端隔離所中的郵件數量。
- `database` - 便利的識別碼，包括所有資料庫識別碼。

磁碟識別碼 - 磁碟識別碼提供有關管理員控制之分割區的磁碟使用率資訊。這些識別碼如下：

- `data_used` - `/data` 分割區正在使用的空間量 (KB)。
- `data_free` - `/data` 分割區中的可用空間量 (KB)。
- `opt_used` - `/opt` 分割區正在使用的空間量 (KB)。
- `opt_free` - `/opt` 分割區中的可用空間量 (KB)。
- `other_used` - `/` 分割區正在使用的空間量 (KB)。

- other_free - / 分割區中的可用空間量 (KB)。
- disk - 便利的識別碼，包括上述所有磁碟資料。

MTA 識別碼 - 這些識別碼會報告 MTA 統計資料。這些識別碼如下：

- i_conn - 入埠連線數。
- i_qmsgs - 排入佇列的入埠郵件數。
- i_dmsgs - 延遲的入埠郵件數。
- i_qsize - 入埠佇列大小 (MB)。
- i_drate - 入埠接聽程式資料速率 (kbps)。
- i_mrate - 入埠接聽程式郵件速率。
- mta_in - 所有入埠統計資料 (以 i_ 開頭的識別碼)。
- o_conn - 離埠連線數。
- o_qmsgs - 排入佇列的離埠郵件數。
- o_dmsgs - 延遲的離埠郵件數。
- o_qsize - 離埠佇列大小 (MB)。
- o_drate - 離埠接聽程式資料速率 (kbps)。
- o_mrate - 離埠接聽程式郵件速率。
- mta_out - 所有離埠統計資料 (以 o_ 開頭的識別碼)。
- d_conn - 傳送連線數。
- d_qmsgs - 排入佇列的傳送郵件數。
- d_dmsgs - 延遲的傳送郵件數。
- d_qsize - 傳送佇列大小 (MB)。
- d_drate - 傳送接聽程式資料速率 (kbps)。
- d_mrate - 傳送接聽程式郵件速率。
- mta_del - 所有傳送統計資料 (以 d_ 開頭的識別碼)。
- mta - 便利的識別碼，包括所有 MTA 識別碼。

  所收集的資訊取決於提供的識別碼。如果未提供任何識別碼，則會使用預設值：system。某些識別碼可表示多個識別碼，為了方便使用均已提供。

  此指令不會提供單一範例與下個範例之間之平均負載或工作完成量等任何相關指示。每個範例皆為當時 MTA 狀態的快照。

程序識別碼 - `--proc` 選項可讓您監控 Symantec Messaging Gateway 程序群組的統計資料。如果使用不含任何 p_* 識別碼的 `--proc` 旗標，則會使用下列預設值：`p_%user p_%sys p_memv p_memr p_mems`。搭配 `--proc` 使用的識別碼包括：

- `p_%user` - 在使用者模式中所用的可用 CPU 時間百分比。
- `p_%sys` - 在系統模式下所用的可用 CPU 時間百分比。
- `p_memv` 程序使用的虛擬記憶體 (k)。
- `p_memr` 程序正在使用的常駐記憶體 (k)。
- `p_mems` - 任一程序使用的共用記憶體最大量 (k)。
- `p_all` 所有程序識別碼。

範例

下列範例說明了可使用 `monitor` 指令的某些方式。這些範例包含某些選項名稱的完整形式與簡短形式的混合，例如 `-o` 和 `--output`。

範例 1

對管道服務所耗用的可用 CPU 時間與記憶體的百分比進行一次檢查。將結果儲存至檔案 `/data/monitor/conduit_mon`。

```
monitor --proc conduit --output conduit_mon
```

範例 2

每 3 秒收集 1000 次系統上 MTA 服務的平均負載。使用標籤格式來顯示系統上 MTA 服務的平均負載，並寫入檔案 `/data/monitor/mta_mon`。

```
monitor --proc mta --interval 3 --count 1000 --tab --output mta_mon
```

範例 3

對 LiveUpdate 服務所使用的可用 CPU 時間與記憶體的百分比進行一次檢查。將結果儲存至檔案 `/data/monitor/liveupdate_mon`。

```
monitor --proc liveupdate --output liveupdate_mon
```

範例 4

對監控服務所耗用的可用 CPU 時間與記憶體的百分比進行一次檢查。使用標籤格式將結果儲存至檔案 `/data/monitor/monitor_mon`。

```
monitor --proc monitor --output monitor_mon --tab
```

另請參閱

請參閱第 636 頁的cat。

請參閱第 647 頁的delete。

請參閱第 670 頁的list。

請參閱第 685 頁的more。

請參閱第 712 頁的tail。

more

more – 用來翻頁瀏覽文字檔案的標準 Linux 指令

說明

more 指令會顯示純文字檔案的內容，一次顯示一個畫面。按**空格鍵**可檢視下一個畫面。使用 list 指令可列出 more 可顯示的檔案。

您可以執行 more 的其他指令的輸出，以檢視輸出 (一次檢視一個畫面)。執行指令後，請輸入管道字元符號，然後再輸入 more。請參閱以下範例。

如需 more 可用選項的詳細資訊，請在指令行輸入 help more。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

more 指令是標準 Linux 指令，已進行修改以僅顯示 list 指令所顯示的檔案。

範例

範例 1

顯示 BrightmailLog.log，一次顯示一個畫面。

```
more /data/logs/bcc/BrightmailLog.log
```

範例 2

檢查 list --top 的輸出，一次檢查一個畫面。

```
list --top | more
```

另請參閱

請參閱第 670 頁的list。

mta-control

`mta-control` – 控制 MTA 程序，以及備份與還原郵件佇列

大綱

`mta-control` *queuecommand*

`mta-control pause-mode` *mode*

說明

`mta-control` 指令可讓您查詢 MTA 佇列，以及控制 MTA 郵件處理中的特定元素。例如，您可以清除郵件佇列。

附註：指定輸出檔名、路徑、密碼、電子郵件地址和使用者名稱 (用於匯出) 時，請勿使用 ~ (波狀符號) 字元。請指定完整路徑名稱。

引數

指定下列其中一個 MTA 佇列：

- 入埠
- 離埠
- 重新提交
- 傳送
- 全部

可用的元件如下：

- start – 啟動佇列。
- stop – 停止佇列。
- status - 顯示目前狀態。狀態可以是：執行中、未執行中、已啟用或已停用。
- restart – 重新啟動佇列。
- flush - 重新嘗試清除所有排入佇列的郵件。
- delete-msgs-by-sender *regexp* - 從佇列刪除信封寄件者符合指定 Perl 規則運算式 (區分大小寫) 的所有郵件。
- delete-msgs-by-rcpt *regexp* - 從佇列刪除信封收件者符合指定 Perl 規則運算式 (區分大小寫) 的所有郵件。

附註：這樣會刪除整個郵件，而非只刪除收件者。

- delete-msg-by-id *queue-ID* - 從佇列刪除指定佇列 ID 的郵件。
- delete-all-msgs - 從佇列刪除全部郵件。
- bypass-resubm-by-sender *regexp* - 針對重新提交佇列中信封寄件者符合指定 Perl 規則運算式的所有郵件，略過重新提交。(不區分大小寫)
- bypass-resubm-by-rcpt *regexp* – 針對重新提交佇列中信封收件者符合指定 Perl 規則運算式的所有郵件，略過重新提交。(不區分大小寫)
- bypass-resubm-by-id *queue-ID* - 針對重新提交佇列中具有指定佇列 ID 的郵件，略過重新提交。各個實例的 ID 是唯一的。
- bypass-resubm-all - 針對重新提交佇列中的所有郵件，略過重新提交。
- active-routes - 列印所有作用中路由以及每個路由的郵件數。
- num-messages-in-route *route* - 列印指定路由的郵件數。
- num-msgs-by-rcpt *route* - 列印指定路由上每個收件者網域的郵件數。
- num-msgs-by-rcpt-all-routes - 列印指定路由上每個收件者網域的郵件數。
- list-msgs *route* - 列印指定路由的郵件。
- list-msg-details *msgid* - 列印具有指定郵件 ID 之郵件的詳細資料。
- route-info *route* - 顯示某個路由的 DNS 查詢資訊、目的地及郵件數。
- reroute *src-routedst-route* – 將郵件從 *src-route* 重新繞送至 *dst-route*。
- delete-msgs-by-sender *perl regexp* - 從佇列刪除信封寄件者符合指定 Perl 規則運算式 (區分大小寫) 的所有郵件。
- delete-msgs-by-rcpt *perl regexp* - 從佇列刪除信封收件者符合指定 Perl 規則運算式 (區分大小寫) 的所有郵件。請注意，這樣會刪除整個郵件，而非只刪除收件者 (區分大小寫)。
- delete-msg-by-id *queue-ID* - 從佇列刪除指定佇列 ID 的郵件。請注意，各個佇列的 ID 是唯一的。
- delete-all-msgs - 從佇列刪除全部郵件。
- import-queues *url* - 從備份匯入整個郵件佇列。為佇列指定 `all`。請先確保 MTA 已在執行中，然後再匯入郵件佇列。若要啟動 MTA，請執行 `mta-control all start`。依所述方法指定 export-msg-by-id 元件的 URL。
- export-queues *url* - 將郵件佇列備份至 URL。為佇列指定 `all`。請先確保 MTA 已停止，然後再匯出郵件佇列。若要停止 MTA，請執行 `mta-control all stop`。依所述方法指定 export-msg-by-id 元件的 URL。

- export-msg-by-id *queue-ID* [*url*] - 從佇列匯出指定佇列 ID 的郵件，並儲存在指定的 URL。如果您未指定 URL，則畫面會顯示郵件資料。如果您未指定 FTP 密碼，則 `mta-control` 會提示您輸入密碼。如果您指定以 / 結尾的路徑，則 Symantec Messaging Gateway 會使用預設檔案名稱，將檔案儲存在該位置。否則，Symantec Messaging Gateway 會以您在路徑中指定的檔案名稱來儲存檔案。URL 語法如下：
  scp://'user'\@host/path (會提示使用者輸入密碼)
  ftp://'user':'password'\@host[:port]/path
  ftp://'user'\@host[:port]/path
  請在 URL 前後加上雙引號字元。如果 URL 的任何部分包含特殊字元 (例如完整引號或雙引號)，請在每個特殊字元之前加上反斜線。
- query-queue - 查詢郵件佇列。
  - 可接受下列其他參數：
  - sender_match=perl regexp
  - rcpt_match=perl regexp
  - deferred - 選取延遲的郵件
  - include_subject
  - start=N
  - limit=N
  - format=neat|xml
    如果出現 sender_match、rcpt_match 和 deferred 參數，則將對其進行邏輯 AND 運算。套用這些比對所得到的中間結果集會依照日期排序，然後套用 start 和 limit：略過 \$start 郵件，並傳回 \$limit 郵件。預設是用可辨識的格式顯示所有郵件，也就是可供人閱讀的格式。
- bad-msg-list - 列出錯誤郵件佇列中郵件的時間和 ID。佇列可以是入埠或離埠佇列。
- bad-msg-export *queue-ID* [*url*] - 匯出或顯示郵件。關於 URL 格式，請參閱 export-msg-by-id。
  若要在畫面上顯示郵件，請輸入 `mta-control queue bad-msg-export queue-ID`。
  依所述方法指定 export-msg-by-id 元件的 URL。
- bad-msg-delete *queue-ID* - 刪除郵件。
- bad-msg-bypass *queue-ID* - 傳送郵件以交付給原始收件者，並略過掃描。
- bad-msg-forward *queue-IDaddress* - 傳送郵件複本以交付給指定的位址，並略過掃描。原始的錯誤郵件仍在錯誤郵件佇列中。
- bad-msg-retry *queue-ID* - 重試掃描郵件，將其視作新郵件看待。
- regen-dh-keys – 重新產生 MTA 使用的 Diffie Hellman 加密金鑰，以進行 TLS 通訊。

有六種暫停模式會影響電子郵件掃描 (scan)、接受 (accept) 和傳送 (delivery)。無論 scan、accept 和 delivery 先前的狀態為何，每個暫停模式都會將掃描、接受和傳送設定為特定狀態，如下所述。這些暫停模式如下：

- status - 顯示目前的暫停模式狀態。如果您輸入 mta-control pause-mode，則 mta-control 會顯示暫停模式狀態。
- pause-accept - 將 scan 設定為執行中，並將 accept 設定為已暫停。delivery 狀態不受 pause-accept 影響。
- pause-deliver - 將 delivery 設定為已暫停。accept 和 scan 狀態不受 pause-deliver 影響。此指令與 mta-control delivery stop 等效。
- pause-scan - 將 scan 設定為已暫停，並將 accept 設定為執行中。delivery 狀態不受 pause-scan 影響。
- resume-accept - 將 scan 設定為執行中，並將 accept 設定為執行中。delivery 狀態不受 resume-accept. 影響。
- resume-deliver - 將 delivery 設定為執行中。accept 和 scan 狀態不受 resume-deliver 影響。此指令與 mta-control delivery start 等效。
- resume-scan - 將 scan 設定為執行中，並將 accept 設定為執行中。delivery 狀態不受 resume-scan 影響。

範例

範例 1

顯示 MTA 的狀態 (入埠、離埠和傳送佇列，以及其是否正在執行)。

```
mta-control pause-mode status
```

範例 2

不接受硬體裝置上的任何新郵件，但會掃描佇列中的郵件。此指令不會影響電子郵件的傳送。

```
mta-control pause-mode pause-accept
```

範例 3

接受硬體裝置上的電子郵件，但不對其進行掃描。此指令不會影響電子郵件的傳送。

```
mta-control pause-mode pause-scan
```

範例 4

不傳送硬體裝置上的電子郵件。

```
mta-control pause-mode pause-deliver
```

範例 5

接受並掃描硬體裝置上的電子郵件。此指令不會影響電子郵件的傳送。

```
mta-control pause-mode resume-accept
```

範例 6

接受並掃描硬體裝置上的電子郵件。此指令不會影響電子郵件的傳送。

```
mta-control pause-mode resume-scan
```

範例 7

傳送硬體裝置上的電子郵件。

```
mta-control pause-mode resume-deliver
```

範例 8

顯示傳送佇列中郵件的佇列 ID。

```
mta-control delivery query-queue
```

範例 9

檢視傳送佇列中具有某個郵件佇列 ID 的原始郵件。

```
mta-control delivery export-msg-by-id 00/00-25597-EFD46794
```

範例 10

匯出傳送佇列中具有某個郵件佇列 ID 的特定郵件。郵件佇列 ID 為 00/00-25597-EFD46794。使用支援帳戶將其匯出至 192.168.159.99 SCP 伺服器的 /tmp 目錄中。`mta-control` 會查詢密碼。

```
mta-control delivery export-msg-by-id 00/00-25597-EFD46794
"scp://support\@192.168.159.99/tmp/"
```

範例 11

匯出所有郵件佇列。使用 sysadmin 帳戶將郵件佇列檔案匯出至 192.168.159.99 FTP 伺服器的 /tmp 目錄中。由於未指定密碼，因此 `mta-control` 會查詢密碼。

```
mta-control all export-queues "ftp://sysadmin\@192.168.159.99/tmp/"
```

範例 12

顯示目前位於入埠佇列、離埠佇列、傳送佇列和重新提交佇列中的所有郵件。

```
mta-control all query-queue
```

範例 13

針對重新提交佇列中信封寄件者符合指定 Perl 規則運算式的所有郵件，略過重新提交。

```
mta-control resubmission bypass-resubm-by-sender user@company.com
```

範例 14

針對重新提交佇列中信封收件者符合指定 Perl 規則運算式的所有郵件，略過重新提交。

```
mta-control resubmission bypass-resubm-by-rcpt user@company.com
```

範例 15

針對重新提交佇列中具有指定佇列 ID 的郵件，略過重新提交。

```
mta-control resubmission bypass-resubm-by-id AC/B7-30310-4CDE7E85
```

範例 16

針對重新提交佇列中的所有郵件，略過重新提交。

```
mta-control resubmission bypass-resubm-all
```

netstat

`netstat` – 用來檢視網路連線的標準 Linux 指令

說明

`netstat` 指令列印網路連線、路由表、介面統計資料、偽裝連線和多點傳播成員資格。

如需 `netstat` 可用選項的詳細資訊，請在指令行輸入 `help netstat`。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

範例

範例 1

顯示網路連線。

```
netstat -an
```

範例 2

顯示繞送表。

```
netstat -r
```

nslookup

nslookup – 用來查詢 DNS 伺服器的標準 Linux 指令

說明

nslookup 指令對指定主機名稱或 IP 位址執行 DNS 查詢。

如需 nslookup 可用選項的詳細資訊，請在指令行輸入 help nslookup。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是標準 Linux 指令集的一部分。已修改此指令，使其可供 Symantec Messaging Gateway 使用，但此修改不影響指令功能。

範例

查閱網域 (例如 yahoo.com) 的 MX 記錄：

```
nslookup -querytype=mx yahoo.com
```

password

`password` – 變更管理密碼

大綱

```
password [--help] [--reset]
```

說明

`password` 指令可變更您用來登入指令行的密碼。會提示您輸入舊密碼，然後再輸入兩次新密碼。

附註：如果在變更密碼時，正在使用控管中心硬體裝置，則用於登入控管中心的管理密碼也會隨之變更。

選項

`--help, -h`

顯示此郵件。

`--reset, -r`

將管理密碼設為出廠預設值。

patch

patch – 處理與 SMG 修正程式相關的所有必要函數

大綱

```
patch [-o | --options ]

patch -help

patch [--releaseversion | -r n] list

patch [--patchversion | -p n] notes

patch <--patchversion | -p n> check | download | install

patch remove

patch localinstall <URL-to-ISO-file>

patch localcleanup
```

說明

patch 指令可處理與 SMG 修正程式相關的所有必要函數。

引數

check

測試修正程式。此引數可執行所有更新前檢查，但不會更新您的硬體裝置軟體。

check 指令需要修正程式版本引數，並且提供的版本必須符合目前已安裝的 SMG 版本 (例如，若要安裝修正程式 10.6.4-X，硬體裝置必須為 10.6.4-Y 版)

download

擷取修正程式版本

download 指令需要修正程式版本選項，並且提供的版本必須符合目前已安裝的 SMG 版本 (例如，若要安裝修正程式 10.6.4-X，硬體裝置必須為 10.6.4-Y 版)

install

安裝修正程式，視需要進行下載

install 指令需要修正程式版本選項，並且提供的版本必須符合目前已安裝的 SMG 版本 (例如，若要安裝修正程式 10.6.4-X，硬體裝置必須為 10.6.4-Y 版)

install 指令會在繼續之前提示您進行確認，並在成功完成後強制重新開機。

`remove`

退出所有已安裝的修正程式 (以安裝的相反順序進行)

`remove` 指令會在繼續之前提示您進行確認，並在成功完成後強制重新開機。

`list`

顯示特定發行版本 (預設為目前安裝的版本) 之可用修正程式的清單，然後會顯示修正程式安裝歷程記錄 (如果適用)

與 `check`、`download` 和 `install` 指令一樣，`list` 指令會採用選用版本選項，但是對可接受的版本號碼沒有限制。

`notes`

顯示修正程式 (預設為目前已安裝的修正程式) 的說明

與 `check`、`download` 和 `install` 指令一樣，`notes` 指令會採用選用版本選項，但是對可接受的版本號碼沒有限制。

`localinstall <URL-to-ISO-file>`

透過從指定的 URL 下載 ISO 來安裝修正程式

`localinstall` 指令會根據已下載的 ISO 檔案中的可用修正程式檢查版本。

`localcleanup`

移除由於先前 localinstall 嘗試失敗可能遺留的暫存檔

選項

`--releaseversion,-r`

指定發行版本號碼。例如 `10.6.3`。

`--patchversion,-p`

指定修正程式版本號碼。例如 `10.6.3-008`。

`--help, -h`

取得更加廣泛的說明。

ping

ping – 用來測試遠端電腦回應的標準 Linux 指令

說明

ping 指令透過資料封包測試硬體裝置與所指定的主機名稱或 IP 位址之間的資料傳輸。

如需 ping 可用選項的詳細資訊，請在指令行輸入 help ping。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

ping6

ping6 – 測試發出機器和所提供的 IPv6 主機名稱或 IP 位址之間的資料傳輸之標準 Linux 指令

說明

此指令是標準 Linux 指令集的一部分。

如需 ping6 可用選項的詳細資訊，請在指令行輸入 help ping6。所顯示的資訊可能包含 Symantec Messaging Gateway 並未提供之指令的參考。

reboot

`reboot` – 重新啟動硬體裝置

大綱

```
reboot [--force]
```

說明

`reboot` 指令會停止所有服務，然後重新啟動硬體裝置。

附註：出現提示時，您必須輸入 **yes** 才能完成關機。輸入 **y** 將導致顯示錯誤訊息。

附註： 如果在 Symantec Messaging Gateway 上執行軟體更新時重新啟動硬體裝置，則可能會損毀硬體裝置軟體。

選項

`--force, -f`

即使軟體更新正在執行，也重新啟動硬體裝置(不建議)。硬體裝置可能會損毀，而且需要重新安裝。如需有關重新安裝硬體裝置軟體的資訊，請聯絡賽門鐵克技術支援。

`--help, -h`

顯示此郵件。

另請參閱

請參閱第 707 頁的shutdown。

route

`route` – 用來顯示和操作 IP 繞送表的標準 Linux 指令

說明

`route`指令可讓您檢視路由表或暫時新增項目至路由表。該指令的主要用途在於檢視路由表。

如需 `route` 可用選項的詳細資訊，請在指令行輸入 `help route`。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

rpmdb

rpmdb – 管理與修復 RPM 資料庫

大綱

```
rpmdb [--verify] [--repair]
```

說明

rpmdb 指令可讓您驗證並重建目前的 RPM 資料庫。在資料庫已損毀並想要進行修復時，此指令非常有用。Symantec Messaging Gateway 的軟體更新會儲存為 RPM 套件。

選項

`--repair, -r`

重新建立 RPM 資料庫。

`--verify, -v`

確認目前的 RPM 資料庫。

rsa-金鑰

`rsa-金鑰` – 匯入、匯出、測試、顯示或刪除 RSA 金鑰

大綱

```
rsa-key
```

說明

匯入、匯出、測試、顯示或刪除 RSA 金鑰。

引數

`rsa-key export` - 顯示匯入遠端主機的金鑰

`rsa-key import (key)` - 複製金鑰到本機 Keyring。您需要用引號括住這個 key 值。

`rsa-key test (user@host)` - 測試與主機使用者的連線

`rsa-key status` - 顯示本機 Keyring

`rsa-key clear (option)` - 刪除所有金鑰和 Keyring，選項為下列其一：local_key、keyring、known_hosts、all

service

service – 用來啟動或停止服務的標準 Linux 指令

大綱

```
service namecommand

service name help
```

說明

使用 service 指令來啟動、停止和檢查 Symantec Messaging Gateway 服務的狀態。服務是持續運作以執行特定工作的程式。在正常運作期間，您不必停止或啟動服務。您可能需要停止或啟動服務，以診斷或解決 Symantec Messaging Gateway 的問題。

service 指令是標準 Linux 指令，已進行修改以與 Symantec Messaging Gateway 提供的服務搭配使用。

引數

執行 service 時，請指定服務 *name* 和 *command*。

name

請指定下列其中一個服務名稱：

agent

Brightmail 代理程式可為控管中心與各掃描程式之間的組態資訊通訊提供便利。

connector

管道與 LiveUpdate 服務會下載垃圾郵件和病毒定義。

controlcenter

控管中心提供集中化的 Web 管理，可收集統計資料並託管隔離所。

dds

具有 LDAP 的目錄資料服務介面，可提供驗證、電子郵件地址驗證、郵件路由和政策群組。

如果您重新啟動 dds 服務，則 bmclient_log 和 bmserver_log 日誌檔可能會包含許多 Could not connect: Connection refused 錯誤。這些錯誤是正常的。

lsisnmpd

lsisnmpd 服務提供某些 Dell PowerEdge 可擴充 RAID 控制器的 SNMP 資訊。

mta

郵件傳輸代理程式會與 Brightmail 引擎搭配運作，以處理、繞送和傳送電子郵件。

`mysql`
控管中心的 MySQL 資料庫可儲存設定和郵件資訊。

`osconfig`
`osconfig` 服務可管理網路介面和相關服務。

`smsswapfile`
`smsswapfile` 服務可管理次要分頁檔空間。

`snmpd`
`snmpd` 服務會等候來自 SNMP 管理軟體的要求。

`casoop`
casoop 服務管理 SMG 和 CA 伺服器之間的通訊。

`command`
可以使用以下指令。某些指令不適用於特定指令。輸入 `service` *`name`* `help` 可顯示套用至服務的指令。

`condrestart`
僅在目前正在執行服務時，才重新啟動服務。此指令僅適用於 `controlcenter`、`snmpd` 和 `mta` 服務。

`delete`
刪除硬體裝置上的分頁檔。此指令僅適用於 `smsswapfile` 服務。

`help`
顯示適用於所指定服務的指令。

`reload`
此指令僅適用於 `mysql` 服務。

`restart`
停止服務後再啟動服務。

`status`
顯示服務的狀態。

`start`
啟動服務。

`stop`
停止服務。

範例

範例 1

顯示適用於 `mta` 服務的指令。

```
service mta help
```

範例 2

顯示 mta 服務的狀態。

```
service mta status
```

範例 3

停止 mta 服務。

```
service mta stop
```

範例 4

停止管道、LiveUpdate 和 JLU 控制器。

```
service connector stop
```

show

show – 顯示系統資訊

大綱

```
show [--date] [--eula] [--info] [--version]

show --help
```

說明

show 指令會顯示下列資訊：

- 目前日期與時間
- 一般使用者授權合約
- 系統資訊
- 產品版本號碼

選項

--date, -d
: 顯示目前日期與時間。

--eula, -e
: 顯示「使用者授權許可協議」。

--help, -h
: 顯示此郵件。

--info, -i
: 顯示系統硬體資訊。

--version, -v
: 顯示產品版本號碼和安裝日期。

shutdown

`shutdown` – 關閉硬體裝置但不重新啟動

大綱

```
shutdown [--help | --force]
```

說明

`shutdown` 指令會立即關閉硬體裝置。系統不會重新啟動硬體裝置。此時會立即關機，而電子郵件則會保留在佇列中。若要在執行 `shutdown` 指令後啟動硬體裝置，您必須按硬體裝置電源按鈕 (除非您已架構硬體裝置硬體的遠端存取權)。

附註：出現提示時，您必須輸入 **yes** 才能完成關機。輸入 **y** 將導致顯示錯誤訊息。

附註： 如果您在軟體更新程序期間中關閉硬體裝置，則可能會損毀硬體裝置軟體。

選項

`--help, -h`
顯示此郵件。

`--force, -f`
即使軟體更新正在執行中，也要關閉硬體裝置 (不建議)。硬體裝置可能會損毀，而且需要重新安裝。如需有關重新安裝硬體裝置軟體的資訊，請聯絡賽門鐵克技術支援。

另請參閱

請參閱第 699 頁的reboot。

請參閱第 604 頁的「關閉硬體裝置」。

sshd-config

`sshd-config` – 架構使用 SSH 可連線至硬體裝置的位址

大綱

```
sshd-config (--list | --help)

sshd-config --add (allow|deny) [IPv6 address] or IPv4 address

sshd-config --delete (allow|deny) rule#

sshd-config --version [1|2]

sshd-config --cbc [on|off]

sshd-config --mac [on|off]
```

說明

`sshd-config` 指令可讓您指定可以透過 SSH 存取硬體裝置的位址。

附註：IPv6 位址必須以括號括住。

選項

`--add, -a`
新增規則。

`--cbc, -c`
開啟或關閉對 CBC 加密 (亦稱為區塊加密) 的支援。

`--delete, -d`
刪除作用中規則。

`--help, -h`
顯示此郵件。

`--list, -l`
顯示作用中規則和目前的通訊協定號碼。

`-m,--mac`
開啟或關閉對 HMAC 演算法的有限支援。

`--version, -v`
顯示通訊協定的版本號碼、CBC 加密和有限 MAC，以及設定或變更所用通訊協定的版本號碼。

- 設定要使用的通訊協定版本號碼 (1 或 2)。
- 顯示 1 或 2 以外的設定，例如：

```
crt-vwei-08> sshd-config -v

Requires protocol version 2

Support for CBC ciphers is ENABLED

Support for limited MACs (hmac-sha2-256,hmac-sha2-512) is ENABLED
```

引數

`allow/deny`

SSH 用戶端連線時，會依下列順序將用戶端位址與允許清單和拒絕清單進行比對：

- 如果用戶端位址符合任何允許規則，即會允許該連線。
- 如果用戶端位址符合任何拒絕規則，即會拒絕該連線。

`rule`

每個規則都是一或多個位址和萬用字元的清單，並以逗號分隔，如下所示：

- some.hostname.com
  符合特定主機
- *some* | *other*.hostname.com
  符合 some.hostname.com 和 other.hostname.com
- 1.2.3.4
  符合特定 IP 位址
- 1.2.
  符合任何以 1.2 開頭的 IP 位址
- 1.2.3.0/255.255.255.0
  符合 1.2.3.* 子網路中的任何 IP 位址
  EXCEPT 關鍵字可用來排除位址的子網路。例如：hostname.com EXCEPT forbidden.hostname.com。
- [n:n:n:n:n:n:n:n]/m
  如果「net」的 prefixlen 位元等於某個位址的 prefixlen，則 IPv6 主機位址與該位址相符。例如，[net]/prefixlen pattern [3ffe:505:2:1::]/64 會與 3ffe:505:2:1:: 到 3ffe:505:2:1:ffff:ffff:ffff:ffff 範圍內的所有位址相符。

您可以指定下列其中一個關鍵字來取代位址參數的主機名稱或 IP 位址。請謹慎使用 KNOWN 和 UNKNOWN 關鍵字，因為這些關鍵字取決於 DNS 服務。

- ALL
  符合任一位址
- LOCAL
  符合名稱不包含點字元的任何主機
- KNOWN
  符合名稱和位址皆為已知的任何主機
- UNKNOWN
  符合名稱或位址為未知的任何主機

symdiag

symdiag – 收集並匯出系統診斷

大綱

```
symdiag [--proactive | --healthcheck][--verbose][url]

symdiag [--help]
```

說明

symdiag 指令會收集系統診斷，並將診斷檔案匯出至使用者指定的位置。

如果未指定任何選項，則會執行 proactive 和 healthcheck 動作。如果同時指定 proactive 和 healthcheck，會顯示錯誤訊息，並且不執行任何動作。

URL 中包含使用者名稱或密碼時，如果其中包含任何特殊 shell 字元，則應將使用者名稱或密碼包含在引號中。可在 URL 中或密碼提示時指定密碼。URL 語法的範例如下所示：

```
scp://'user':'password'\@host[:port]/path/
```

指令引數中的 URL 必須以「/」結尾。您無法指定檔案名稱，只能指定將放置輸出檔案的目錄。診斷檔案將寫入以預設檔案名稱指定的路徑。

輸出檔案名稱採用下列格式：

```
'<hostname>__<date>__<time>__AAAAAA.sdbz'
```

其中 AAAAAA 是 6 位數的十六進位數字。

還會以 TEST 而非 6 位數的十六進位數字建立零位元組檔案。執行用於產生輸出的指令之前，會建立此檔案以驗證 URL 中的使用者名稱、密碼、主機名稱等。

選項

--proactive, -p
: 針對「檢閱組態」主動式服務收集和報告資訊。

--healthcheck, -c
: 檢查核心系統。

--verbose, -v
: 在詳細資訊模式下收集診斷資訊。

--help, -h
: 顯示此訊息。

tail

`tail` – 用來檢視檔案結尾的標準 Linux 指令

大綱

```
tail [-f | --help ] log_name
```

說明

`tail` 指令屬於標準 Linux 指令集，可顯示具名日誌檔的最後 50 行。

但是，可以透過下列方式修改此指令：

- 只有此處說明的 `-f` 與 `--help` 選項可供使用。
- 如果日誌檔中的某字元無法列印或不是 ASCII 字元，則會改為顯示 \xAB 序列，而不顯示該字元。其中 AB 是該字元的十六進位值。例如，十進位值為 128 的字元將顯示為 \x80。
- 此指令僅限用於可從 `list` 指令取得的檔案名稱。`list` 指令可顯示能夠由特定指令操作的所有檔案的檔案名稱。除了 `tail` 指令之外，下列指令也可以操作使用 `list` 列出的檔案：

  `cat`
  : 顯示一或多個檔案的內容。

  `delete`
  : 刪除一或多個檔案。

  `more`
  : 顯示一或多個檔案的內容，並且在各個畫面的結尾暫停。

選項

`-f`
: 將新文字新增到檔案時遵循該檔案。`tail -f` 指令會列印檔案的最後 10 行，但不會結束。將新文字行新增到檔案時，`tail` 會顯示新的文字行。`-f` 選項有助於在將其他資訊新增到日誌檔時監控該日誌檔。如果您輸入 `tail -f log_name`，但沒有任何回應，則表示該檔案是空的且/或並非在寫入該檔案。

  若要停止監控檔案，請按 **Ctrl+C**。

`--help, -h`
: 顯示此郵件。

引數

log_name

log_name 可以是以下任何一項：

- agent_log
- battery.log
- bmclient_log
- bmserver_log
- boot.log
- BrightmailLog.log
- conduit_log
- cron
- db-migration.log
- dds.log
- dmesg
- imlinkage_log
- jlu-controller_log
- liveupdt.log
- maillog
- messages
- named.run
- secure
- update.log

範例

範例 1

顯示 BrightmailLog.log 日誌檔的最後 50 行。

```
tail BrightmailLog.log
```

範例 2

在更新期間監控 update.log 日誌檔。如果您發現資訊定期寫入 update.log，則通常表示更新正常進行。

```
tail -f update.log
```

另請參閱

請參閱第 670 頁的list。

telnet

`telnet` – 用來連線至遠端電腦的標準 Linux 指令

說明

`telnet` 指令可讓您從硬體裝置記錄到網路上的另一台電腦的指令行。

如需 `telnet` 可用選項的詳細資訊，請在指令行輸入 `help telnet`。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

traceroute

`traceroute` – 用來檢視網路封包所採用路徑的標準 Linux 指令

說明

`traceroute` 指令顯示指定主機名稱或 IP 位址的網路路由。

如需 `traceroute` 可用選項的詳細資訊，請在指令行輸入 `help traceroute`。所顯示的資訊可能包含對 Symantec Messaging Gateway 並未提供之指令的參考。

此指令是未經修改的標準 Linux 指令。

traceroute6

`traceroute6` – 追蹤繞送至提供之主機名稱或 IPv6 位址的網路路由的標準 Linux 指令

說明

此指令是標準 Linux 指令集的一部分。

如需 `traceroute6` 可用選項的詳細資訊，請在指令行輸入 `traceroute6 --help`。所顯示的資訊可能包含 Symantec Messaging Gateway 並未提供之指令的參考。

update

update – 更新硬體裝置軟體

大綱

```
update list

update [--version | -v number] ( check | download | install | notes )

update localinstall URL to ISO file

update localcleanup

update --help
```

說明

您可以使用 update 指令執行下列工作：

- 檢查新的軟體更新
- 下載軟體更新
- 從 Internet 或本機安裝軟體更新
- 列出可供下載或安裝的可用軟體更新

更新軟體之前，請先確認硬體裝置未執行任何工作；如果有，則在重設硬體裝置之後可能會造成問題。另請確定執行資料庫的備份。

請參閱第 641 頁的db-backup。

選項

--help, -h
: 顯示此郵件。

[--version | -v n] check | notes | download | install
: 針對 check、download、install 或 notes 引數指定軟體更新版本號碼。

引數

check
: 執行測試更新。

  如果您選擇執行軟體更新，則測試更新會展示發生的狀況。執行 update check 並不會更新硬體裝置軟體。如果未指定版本，則測試更新會使用最新的軟體版本。例如，如果執行

`update check` 而未指定版本，且您的硬體裝置目前正在執行的版本必須先更新為中間版本，然後才能更新為最新版本，則測試會失敗。您可查看「版本說明」找到有關已核准更新路徑的資訊。

`download`

下載但不安裝軟體更新。預設為最新發行的版本。

下載軟體更新後，可以輸入 `update install` 來進行安裝。如果未指定版本，則會下載最新的軟體更新。

`install`

下載並安裝軟體更新。如果未指定版本，則會在您的硬體裝置上安裝最新的軟體更新。

預設為最新發行的版本。

`list`

顯示可用的軟體更新。

`localinstall` *`URL to ISO file`*

其中 *URL to ISO file* 是 Symantec Messaging Gateway 可以從其中擷取 OSRestore ISO 的 HTTP 位置。

在沒有 Internet 連線情況下更新軟體版本。

先從賽門鐵克下載 ISO 影像，然後將其放在透過硬體裝置可存取的 HTTP 伺服器。

`localcleanup`

移除可能由於先前 localinstall 嘗試失敗而遺留的暫存檔。

`notes`

顯示軟體更新說明。如果未指定版本，則會顯示最新的軟體更新說明。

範例

```
update download
```

下載但不安裝軟體更新。下載軟體更新後，可以輸入 `update install` 來進行安裝。

另請參閱

請參閱第 616 頁的「更新 Symantec Messaging Gateway 軟體 」。

附錄 B

郵件過濾選項

本附錄包含以下主題：

- 來自多個判斷的動作組合
- 依判斷類別判斷
- 判斷組合
- 肯定與否定內容過濾規則條件範例

來自多個判斷的動作組合

每當郵件觸發判斷時，SMG 會將對應政策的動作新增至動作清單。完成所有過濾後，SMG 會從清單中移除精確的重複項目，然後評估其餘動作。動作可以結合，或一個動作可以覆寫另一個動作。

動作群組

表 B-1、表 B-2 以及表 B-3 說明 SMG 如何在郵件觸發多個判斷時結合或覆寫動作以處理郵件。這些表格參考了以下政策動作群組：

「防火牆」動作：	延遲 SMTP 連線、拒絕 SMTP 連線、拒絕未通過退回攻擊驗證的郵件
「事件」動作：	封存郵件、建立資訊事件、轉寄郵件的複本、寄送傳送狀態通知、傳送通知
「延遲病毒」動作：	將郵件保留在可疑病毒隔離所、刪除和延遲可疑病毒隔離所中的郵件
「延遲內容」動作：	建立隔離事件
「刪除」動作：	刪除郵件
「修改」動作：	新增標頭、新增註釋、新增密件副本收件者、清除郵件、傳送 TLS 加密的郵件、修改郵件主旨行、移除未解析的收件者、刪除附件、解除附件

「修改 URL」動作： 在郵件中修改可按式 URL：Email Threat Isolation、Web 服務 (ProxySG)、取代 URL、停用 URL

「繞送」動作： 將郵件保留在垃圾郵件隔離所、繞送郵件、傳送內容加密的郵件(此動作會顯示繞送和修改類別行為)

「沒有動作」動作： 正常傳送郵件

所有動作群組都結合「防火牆」、「事件」和「延遲病毒」動作時的結果

下表顯示這些群組中的動作如何結合其他動作或與其他動作發生衝突。如需所有群組中的完整動作清單，請參閱動作群組。

表 B-1 「防火牆」、「事件」和「延遲病毒」動作組合

	防火牆： **延遲 SMTP 連線、拒絕 SMTP 連線、拒絕未通過退回攻擊驗證的郵件**	**事件：** **封存郵件、建立資訊事件、轉寄郵件的複本、寄送傳送狀態通知、傳送通知**	**延遲病毒：** **將郵件保留在可疑病毒隔離所、刪除和延遲可疑病毒隔離所中的郵件**
防火牆	防火牆	防火牆	防火牆
事件	防火牆	事件 + 事件	事件 + 延遲
延遲病毒	防火牆	事件 + 延遲	重複出現**「將郵件保留在可疑病毒隔離所」**或**「刪除和延遲可疑病毒隔離所中的郵件」**動作時，僅延遲一次 **「刪除和延遲可疑病毒隔離所中的郵件」**會覆寫**「將郵件保留在可疑病毒隔離所」**。
延遲內容	防火牆	事件 + 延遲	延遲內容、延期延遲病毒
刪除	防火牆	刪除 + 事件	刪除
修改	防火牆	修改 + 事件	延遲、延遲修改
修改 URL	防火牆	修改 + 事件	延遲、延遲修改
繞送	防火牆	繞送 + 事件	延遲、延遲繞送
沒有動作	防火牆	事件	延遲

所有動作群組都結合「延遲內容」、「刪除」和「修改」動作時的結果

下表顯示這些群組中的動作如何結合其他動作或與其他動作發生衝突。如需所有群組中的完整動作清單，請參閱動作群組。

表 B-2 「延遲內容」、「刪除」和「修改」動作組合

	延遲內容： **建立隔離事件**	**刪除：** **刪除郵件**	**修改：** **新增標頭、新增註釋、新增密件副本收件者、清除郵件、傳送 TLS 加密的郵件、修改郵件主旨行、移除未解析的收件者、刪除附件、解除附件**
防火牆	防火牆	防火牆	防火牆
事件	事件 + 延遲 如果**「建立隔離事件」**動作具有依字母順序排序早於**「建立資訊事件」**資料夾的資料夾名稱，則 SMG 會在從隔離所釋放郵件後執行**「建立資訊事件」**動作。如果從隔離所刪除郵件，則不會建立資訊事件。	刪除 + 事件	修改 + 事件
延遲病毒	延遲內容、延期延遲病毒	刪除	延遲、延遲修改
延遲內容	對於多個**「建立隔離事件」**動作，郵件會放置在以英數字元排序最先顯示的隔離所資料夾中。如果該郵件從隔離所釋放，便會前往依字母順序排序為第二的資料夾。程序會重複進行，直到釋放或刪除郵件為止。	延遲、延遲刪除	延遲、延遲修改
刪除	延遲、延遲刪除	刪除一次	刪除
修改	延遲、延遲修改	刪除	修改 + 修改 如果有多個**「傳送 TLS 加密的郵件」**動作，僅執行最強的加密。
修改 URL	延遲、延遲修改 URL	刪除	修改 + 修改 URL

	延遲內容： 建立隔離事件	刪除： 刪除郵件	修改： 新增標頭、新增註釋、新增密件副本收件者、清除郵件、傳送 TLS 加密的郵件、修改郵件主旨行、移除未解析的收件者、刪除附件、解除附件
繞送	延遲、延遲繞送	刪除	修改 + 繞送 「將郵件保留在垃圾郵件隔離所」會覆寫「傳送 TLS 加密的郵件」 「傳送內容加密的郵件」會覆寫「傳送 TLS 加密的郵件」。
沒有動作	延遲	刪除	修改

所有動作群組都結合「修改URL」、「繞送」和「沒有動作」群組時的結果

下表顯示這些群組中的動作如何結合其他動作或與其他動作發生衝突。如需所有群組中的完整動作清單，請參閱動作群組。

表 B-3 「修改 URL」、「繞送」和「沒有動作」組合

	修改 URL： Email Threat Isolation 、Web 服務 (ProxySG)、取代 URL、停用 URL	繞送： 將郵件保留在垃圾郵件隔離所、繞送郵件、傳送內容加密的郵件	沒有動作： 正常傳送郵件
防火牆	防火牆	防火牆	防火牆
事件	修改 URL + 事件	繞送 + 事件	事件
延遲病毒	延遲、延遲修改 URL	延遲、延遲繞送	延遲
延遲內容	延遲、延遲修改 URL	延遲、延遲繞送	延遲
刪除	刪除	刪除	刪除
修改	修改 + 修改 URL	修改 + 繞送 如果一個動作是「將郵件保留在垃圾郵件隔離所」，另一個動作是「傳送 TLS 加密的郵件」，則不會進行 TLS 加密。	修改

	修改 URL： Email Threat Isolation 、Web 服務 (ProxySG)、取代 URL、停用 URL	繞送： 將郵件保留在垃圾郵件隔離所、繞送郵件、傳送內容加密的郵件	沒有動作： 正常傳送郵件
修改 URL	一個「修改 URL」動作會以此順序優先執行：(1) Email Threat Isolation，(2) Web 服務 (ProxySG)，(3) 在郵件中取代可按式 URL，(4) 在郵件中停用可按式 URL	修改 + 繞送	修改
繞送	修改 URL + 繞送	一個繞送成功。 **「將郵件保留在垃圾郵件隔離所」**會覆寫**「繞送郵件」**。 **「傳送內容加密的郵件」**會覆寫**「繞送郵件」**。 **「傳送內容加密的郵件」**會覆寫**「將郵件保留在垃圾郵件隔離所」**。 如果有多個**「繞送郵件」**動作，則郵件會繞送至以英數字元排序最先顯示的繞送位址。	路由
沒有動作	修改 URL	路由	傳送

附註：一般使用者的「允許的寄件者」和「攔截的寄件者」群組中的動作會覆寫除內容過濾政策動作以外的所有動作。

依判斷類別判斷

下表依判斷類別說明判斷。判斷類別對應至控管中心內的功能表，您可以在其中針對每個判斷建立或編輯政策。當您從這些功能表建立或編輯政策時，可以設定每個判斷的偵測條件。在每個政策中，也可以選取您希望 SMG 在郵件符合政策條件並觸發判斷時所要採取的動作。

表 B-4　　依判斷類別判斷

判斷類別	判斷	說明
信譽	電子郵件地址搜尋攻擊	正在嘗試擷取有效的電子郵件地址。當相同的 IP 位址將指定百分比的電子郵件從不存在的收件者傳送到您的網域時，SMG 會偵測電子郵件地址搜尋攻擊。
信譽	電子郵件病毒攻擊	相同的 IP 位址會將指定百分比的受感染電子郵件訊息傳送到您的網域。

判斷類別	判斷	說明
信譽	攔截的寄件者群組	電子郵件訊息、網域或 IP 位址是下列其中一個群組的成員： ■ 本機攔截的寄件者網域 ■ 本機攔截的寄件者 IP ■ 攔截的第三方寄件者 ■ 賽門鐵克全域攔截的寄件者 請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。
信譽	允許的寄件者群組	電子郵件訊息、網域或 IP 位址是下列其中一個群組的成員： ■ 本機允許的寄件者網域 ■ 本機允許的寄件者 IP ■ 允許的第三方寄件者 ■ 賽門鐵克全域允許的寄件者 請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。
信譽	快速通過	允許大部分來自已驗證「允許的寄件者」的電子郵件訊息略過垃圾郵件過濾。您無法針對「快速通過」判斷指定任何動作。
惡意軟體	病毒	依據目前的賽門鐵克病毒過濾器，電子郵件含有病毒。
惡意軟體	大量郵件病蟲	依據目前的賽門鐵克病毒過濾器，電子郵件含有大量郵件病蟲。
惡意軟體	因任何原因而無法掃描是否存在惡意軟體或內容過濾	由於對應到精細判斷的四個原因中的任一原因，無法掃描電子郵件。這些原因是：附件超出限制或其他。「其他」包括任何不適用於附件超出限制判斷的原因。
惡意軟體	因超出限制而無法掃描是否存在惡意軟體或內容過濾	郵件的附件超過您所設定的配置區限制。 可以在**「通訊協定」> SMTP >「設定」>「內容掃描」**標籤上設定配置區限制。
惡意軟體	因其他原因而無法掃描是否存在惡意軟體或內容過濾	郵件或附件因為其他無法掃描判斷中所列舉原因以外的原因而無法掃描。例如，郵件所包含的附件被分割為多個以其他方式支援之附件類型的實例。
惡意軟體	因解除而無法掃描	電子郵件包含的附件因「解除」而無法掃描。例如，加密的附件無法「解除」。
惡意軟體	加密的附件	因為電子郵件中包含加密或由密碼保護的附件，因此無法掃描。
惡意軟體	間諜程式或廣告程式	電子郵件包含下列任何類型的安全風險：間諜程式、廣告程式、駭客工具、撥號工具、惡作劇程式或遠端存取程式。 請參閱第 184 頁的「間諜程式或廣告程式判斷詳細資訊」。
惡意軟體	可疑附件	電子郵件顯示有病毒跡象，或因為在含有該附件的郵件流量上偵測到可疑的新樣式。

判斷類別	判斷	說明
惡意軟體	解除	電子郵件包含的附件中偵測到潛在惡意內容。 請參閱第 179 頁的「關於「解除」」。
垃圾郵件及不必要的電子郵件	垃圾郵件	依據目前賽門鐵克垃圾郵件過濾器，電子郵件訊息是垃圾郵件。
垃圾郵件及不必要的電子郵件	可疑垃圾郵件	依據可在**「垃圾郵件」>「設定」>「掃描設定」**頁面上調整的可疑垃圾郵件臨界值，電子郵件訊息是可疑垃圾郵件。
垃圾郵件及不必要的電子郵件	無法通過退回攻擊驗證	根據退回攻擊驗證過濾，電子郵件訊息屬於退回攻擊的一部分。 請參閱第 137 頁的「關於防衛退回攻擊」。
垃圾郵件及不必要的電子郵件	行銷郵件	依據賽門鐵克不必要的電子郵件過濾器，電子郵件訊息屬於行銷電子郵件。
垃圾郵件及不必要的電子郵件	電子報	依據賽門鐵克不必要的電子郵件過濾器，電子郵件訊息屬於電子報。
垃圾郵件及不必要的電子郵件	重新導向 URL	依據賽門鐵克不必要的電子郵件過濾器，電子郵件訊息包含一或多個重新導向 URL。
垃圾郵件及不必要的電子郵件	客戶特定垃圾郵件	依據從客戶特定垃圾郵件提交所建立的規則，電子郵件訊息是垃圾郵件。您可以從**「垃圾郵件」>「設定」>「提交設定」>「客戶特定垃圾郵件提交」**頁面，啟用客戶特定垃圾郵件提交。
垃圾郵件及不必要的電子郵件	寄件者驗證	電子郵件訊息未通過 SPF 或寄件者 ID 驗證。 請參閱第 98 頁的「寄件者驗證的運作方式」。
威脅防禦	包含進階威脅	根據 Symantec Content Analysis 執行的威脅防禦偵測，電子郵件訊息包含進階惡意軟體。
威脅防禦	不包含進階威脅	根據 Symantec Content Analysis 執行的威脅防禦偵測，電子郵件訊息不包含進階惡意軟體。
威脅防禦	無法掃描是否存在進階威脅	Symantec Content Analysis 無法掃描電子郵件訊息。
威脅防禦	檢查時間超過 <x> 秒	威脅防禦掃描沒有在指定的**「掃描逾時」**限制內評估電子郵件訊息。
內容	主旨、內文或附件中的文字	電子郵件訊息： ■ 包含或不包含可架構辭典中的關鍵字 ■ 符合或不符合規則運算式 ■ 符合或不符合樣式 ■ 比對記錄中的資料

判斷類別	判斷	說明
內容	在此郵件指定部分中的文字	在任何指定的郵件部分中，電子郵件訊息： ■ 包含或不包含特定文字 ■ 以特定文字開頭或結尾、不以特定文字開頭或結尾、與特定文字完全相符/與特定文字不相符 ■ 符合規則運算式或不符合您指定的規則運算式 ■ 符合樣式或不符合您指定的樣式
內容	此郵件標頭特定部分中的文字	信封收件者或信封寄件者中的文字包含或不包含電子郵件地址、網域或特定辭典中的國碼。
內容	包含郵件部分/不包含郵件部分	郵件包含或不包含所指定的郵件部分。
內容	郵件大小/附件大小	郵件大小或附件大小等於/大於/小於特定數目的位元組、KB 或 MB。
內容	附件或內文部分	附件位於或不位於附件清單中、擁有特定檔案名稱或MIME 類型，或擁有不是來自特定辭典的特定檔案名稱或 MIME 類型。 **附註：**SMG 會評估內嵌於郵件內文的附件和任何物件的真實檔案類型、真實檔案類別、檔案名稱、副檔名和 MIME。若條件為**「不是位於附件清單」**，SMG 則會評估內嵌於郵件內文的附件和物件的真實檔案類型和真實檔案類別。 SMG 不會測試檔案名稱、副檔名或 MIME 類型，因為寄件者可輕易地偽造這些項目。因此，這些項目不是用於政策的安全條件。
內容	針對所有郵件	您可以建立套用至所有郵件的內容過濾規則。例如，您可以建立一個政策，用於將註釋附加到所有入埠或離埠電子郵件訊息。 標示所有電子郵件。

請參閱第 729 頁的「肯定與否定內容過濾規則條件範例 」。

判斷組合

一般而言，來自「允許的寄件者」群組之寄件者的郵件會略過垃圾郵件過濾，但不會略過病毒過濾或內容過濾。本節進一步說明此過程是如何進行的。

到達閘道的郵件會先進行連線時間處理。

可依據下列資訊延遲、拒絕或接受來自特定網域或 IP 位址的郵件：

- 本機 (在您的系統內) 收集的信譽資訊
- 全球收集的信譽資訊
- 本機允許的寄件者群組和攔截的寄件者群組

- 全域允許的寄件者群組和攔截的寄件者群組

這些動作發生在 Brightmail 引擎處理郵件之前。

請參閱第 25 頁的「Symantec Messaging Gateway 的運作方式」。

表 B-5 顯示可在連線處理期間略過的步驟。

表 B-5 連線時間允許的寄件者處理

如果任何一項相符：	Symantec Messaging Gateway 不會檢查下列任一項：
本機允許的寄件者 IP 允許的第三方寄件者 賽門鐵克全域允許的寄件者	攔截的第三方寄件者
本機允許的寄件者 IP 賽門鐵克全域允許的寄件者	賽門鐵克全域攔截的寄件者
本機允許的寄件者 IP	本機攔截的寄件者 IP

請參閱第 130 頁的「關於使用寄件者群組攔截和允許郵件」。

請參閱第 724 頁的「依判斷類別判斷」。

表 B-6說明 Brightmail 引擎郵件處理可能會略過的步驟。

表 B-6 Brightmail 引擎入埠郵件處理

如果任何一項相符：	Symantec Messaging Gateway 不會檢查下列任一項：
本機允許的寄件者網域 本機允許的寄件者 IP 具有「略過垃圾郵件掃描」動作的內容過濾政策 具有「視為允許的寄件者」動作的內容過濾政策 賽門鐵克全域允許的寄件者 一般使用者「允許的寄件者清單」 允許的第三方寄件者	垃圾郵件 可疑垃圾郵件 電子報 行銷電子郵件 重新導向 URL 寄件者驗證失敗
具有「視為允許的寄件者」動作的內容過濾政策 本機允許的寄件者網域	本機攔截的寄件者網域

如果任何一項相符：	Symantec Messaging Gateway 不會檢查下列任一項：
垃圾郵件	可疑垃圾郵件 電子報 行銷電子郵件 重新導向 URL
當相關聯的政策指定「略過內容過濾政策」動作時： ■ 本機允許的寄件者網域 ■ 本機允許的寄件者 IP ■ 允許的第三方寄件者 ■ 本機攔截的寄件者網域 ■ 本機攔截的寄件者 IP ■ 攔截的第三方寄件者 ■ 賽門鐵克全域允許的寄件者 ■ 賽門鐵克全域攔截的寄件者 ■ 垃圾郵件 ■ 可疑垃圾郵件 ■ 不必要的電子郵件 ■ 寄件者驗證失敗	所有內容過濾政策，或政策中指定的內容過濾政策

肯定與否定內容過濾規則條件範例

當您瞭解如何評估肯定規則條件和否定規則條件時，可建立更有效率的政策。

肯定規則是指條件必須存在才會觸發判斷的規則。例如，肯定規則是：**如果郵件的任何部分包含「財務關鍵字」辭典中的 2 個 (含) 以上字詞。**如果郵件包含「財務關鍵字」辭典中的 2 個 (含) 以上字詞，便會觸發判斷。

否定規則是指條件必須存在才會觸發判斷的規則。例如，否定規則是：**「不包含主旨」**。

表 B-7 列出了具有肯定與否定規則的條件，並提供郵件何時觸發和不觸發判斷的範例。

表 B-7 肯定與否定規則比對動詞與範例

條件	範例 1： 郵件不包含任何附件。僅內文中的內容符合條件。郵件的任何其他部分均不符合條件。	範例 2： 郵件包含一個附件。郵件的任何其他部分均不符合條件。	範例 3： 郵件包含多個附件。只有一個附件符合條件。郵件的任何其他部分均不符合條件。
主旨、內文或附件中的文字： 包含辭典中的 *n* 個或更多個字。	觸發判斷	不觸發判斷	觸發判斷
主旨、內文或附件中的文字： 不包含辭典中的 *n* 個或更多個字。	觸發判斷	不觸發判斷	觸發判斷
主旨、內文或附件中的文字： 符合規則運算式	觸發判斷	不觸發判斷	觸發判斷
主旨、內文或附件中的文字： 不符合規則運算式	觸發判斷	不觸發判斷	觸發判斷
主旨、內文或附件中的文字： 符合樣式	觸發判斷	不觸發判斷	觸發判斷
主旨、內文或附件中的文字： 不符合樣式	觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 位於附件清單	觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 不是位於附件清單	觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 其檔案名稱包含	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷

條件	範例 1： 郵件不包含任何附件。僅內文中的內容符合條件。郵件的任何其他部分均不符合條件。	範例 2： 郵件包含一個附件。郵件的任何其他部分均不符合條件。	範例 3： 郵件包含多個附件。只有一個附件符合條件。郵件的任何其他部分均不符合條件。
附件或內文部分： 其檔案名稱不包含	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 其 MIME 類型為	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 其 MIME 類型不是	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 其檔案名稱源自辭典	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 其檔案名稱不是源自辭典	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 其副檔名源自辭典	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷
附件或內文部分： 其副檔名不是源自辭典	如果郵件有符合名稱的內嵌檔案，則觸發判斷 如果沒有，則不觸發判斷	不觸發判斷	觸發判斷

附註：若條件為**「附件或內文部分: 位於附件清單」**，SMG 會評估內嵌於郵件內文的附件和任何物件的真實檔案類型、真實檔案類別、檔案名稱、副檔名和 MIME。

若條件為**「附件或內文部分: 不是位於附件清單」**，SMG 則會評估內嵌於郵件內文的附件和物件的真實檔案類型和真實檔案類別。SMG 不會針對此條件測試檔案名稱、副檔名或 MIME 類型。

附錄 C

內容過濾範本

本附錄包含以下主題：

- 考爾迪科特報告政策範本
- 加拿大社會保險號碼政策範本
- 競爭對手通訊政策範本
- 機密文件政策範本
- 信用卡號碼政策範本
- 客戶資料保護政策範本
- 1998 年資料保護法政策範本
- 防禦郵件系統 (DMS) GENSER 分類政策範本
- 設計文件政策範本
- 員工資料保護政策範本
- 加密的資料政策範本
- 歐盟資料保護指令政策範本
- 出口管理條例規定 (EAR) 政策範本
- 財務資訊政策範本
- 賭博政策範本
- 金融服務法案 (Gramm-Leach-Bliley) 政策範本
- HIPAA 政策範本
- 1998 年人權法政策範本

- 違禁藥品政策範本
- 美國報稅號碼 (ITIN) 政策範本
- 國際武器運輸條例規定 (ITAR) 政策範本
- 媒體檔政策範本
- 合併與收購資料政策範本
- NASD 規定 2711 與 NYSE 規定 351 和 472 政策範本
- NASD 規定 3010 與 NYSE 規定 342 政策範本
- 電業的 NERC 安全指導原則政策範本
- 網路圖政策範本
- 網路安全政策範本
- 攻擊性語言政策範本
- 海外資產控制局 (OFAC) 政策範本
- 密碼檔政策範本
- 付款卡產業資料安全標準政策範本
- PIPEDA 政策範本
- 價格資訊政策範本
- 專案資料政策範本
- 出版文件政策範本
- 種族主義語言政策範本
- 限制的檔案政策範本
- 限制的收件者政策範本
- 履歷表政策範本
- 沙賓法案 (Sarbanes-Oxley) 政策範本
- SEC 公平揭露規定政策範本
- 色情語言政策範本
- 原始程式碼政策範本
- 州資料隱密性政策範本

- SWIFT 代碼政策範本
- 英國駕照號碼政策範本
- 英國選民登記號碼政策範本
- 英國國家保險號碼政策範本
- 英國護照號碼政策範本
- 英國稅務 ID 號碼政策範本
- 美國智慧型控制標記 (CAPCO) 及 DCID 1/7 政策範本
- 美國社會安全號碼政策範本
- 暴力與武器政策範本

考爾迪科特報告政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 英國國家保險號碼與藥品關鍵字 - 搜尋英國國家保險號碼關鍵字辭典中的關鍵字，再加上符合 UK NIN 規則運算式的樣式，以及處方藥品名稱辭典中的關鍵字。
- 英國國家保險號碼與疾病關鍵字 - 搜尋英國國家保險號碼關鍵字辭典中的關鍵字，再加上符合 UK NIN 規則運算式的樣式，以及疾病名稱辭典中的關鍵字。
- 英國國家保險號碼與治療關鍵字 - 搜尋英國國家保險號碼關鍵字辭典中的關鍵字，再加上符合 UK NIN 規則運算式的樣式，以及醫學治療關鍵字辭典中的關鍵字。

結構化資料條件如下：

- 病患資料和藥品關鍵字 - 在「記錄資源檢視」中尋找下列任何資料的相符項目： NIN (國家保險號碼)、帳號、姓氏、ID 卡號、電子郵件、電話及 UK NHS (國民保健服務) 號碼。此資料必須連同處方藥品名稱辭典中的一個關鍵字一起出現。
- 病患資料和疾病關鍵字 - 在「記錄資源檢視」中尋找下列任何資料的相符項目： NIN (國家保險號碼)、帳號、姓氏、ID 卡號、電子郵件、電話及 UK NHS (國民保健服務) 號碼。此資料必須連同疾病名稱辭典中的一個關鍵字一起出現。
- 病患資料和治療關鍵字 - 在「記錄資源檢視」中尋找下列任何資料的相符項目： NIN (國家保險號碼)、帳號、姓氏、ID 卡號、電子郵件、電話及 UK NHS (國民保健服務) 號碼。此資料必須連同醫學治療關鍵字辭典中的一個關鍵字一起出現。

隨附的辭典如下：

- 處方藥品名稱 (Prescription Drug Names)
- 疾病名稱 (Disease Names)
- 醫學治療關鍵字 (Medical Treatment Keywords)
- 英國國家保險號碼關鍵字 (UK NIN Keywords)

加拿大社會保險號碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為加拿大社會保險號碼。此條件會搜尋符合加拿大社會保險號碼規則運算式的項目，以及加拿大社會保險號碼單字 (Canadian Social Ins. No. Words) 辭典中的關鍵字。

隨附的辭典是「加拿大社會保險號碼單字 (Canadian Social Ins. No. Words)」。

競爭對手通訊政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為競爭對手清單。此條件會搜尋由使用者定義的競爭對手網域辭典中的關鍵字 (網域)。

隨附的辭典是「競爭對手網域」。

機密文件政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 機密文件 - 使用複合條件搜尋敏感關鍵字辭典中的關鍵字與下列檔案類型的組合： excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、pdf 和 ppt。
- 專利文件 - 使用複合條件搜尋專利關鍵字辭典中的關鍵字與下列檔案類型的組合： excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、pdf 和 ppt。
- 僅限內部使用的文件 - 使用複合條件搜尋內部專用關鍵字辭典中的關鍵字與下列檔案類型的組合：excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、pdf 和 ppt。
- 不得散布的文件 - 使用複合條件搜尋「禁止散布文字」辭典中的關鍵字與下列檔案類型的組合：excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、pdf 和 ppt。

隨附的辭典如下：

- 機密關鍵字 (Confidential Keywords)
- 專利關鍵字 (Proprietary Keywords)
- 內部專用關鍵字 (Internal Use Only Keywords)
- 禁止散布文字 (Not For Distribution Words)

信用卡號碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為所有信用卡號碼。此條件會搜尋符合信用卡號碼系統特徵的項目，以及信用卡號碼關鍵字辭典中的關鍵字。

隨附的辭典是「信用卡號碼關鍵字」。

客戶資料保護政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 身分證號碼樣式 - 搜尋符合身分證號碼規則運算式的項目，以及身分證號碼關鍵字辭典中的關鍵字。
- 所有信用卡號碼 - 搜尋符合信用卡號碼系統樣式的項目，以及信用卡號碼關鍵字辭典中的關鍵字。
- ABA 轉帳號碼 - 搜尋符合 ABA 轉帳號碼規則運算式的項目，以及 ABA 轉帳號碼關鍵字辭典中的關鍵字。

結構化資料條件如下：

- 使用者名稱/密碼組合 - 從「記錄資源檢視」中尋找使用者名稱和密碼的組合。
- 3 個或更多個客戶資料欄位 - 從「記錄資源檢視」中尋找下列任意三個欄位的資料組合： SSN、電話、電子郵件、名字、姓氏、金融卡號碼、帳號、ABA 轉帳號碼、加拿大社會保險號碼，以及英國國家保險號碼、出生日期。 例外狀況： 電話、電子郵件及名字或姓氏的組合；電子郵件或電話及名字和姓氏的組合。
- 準確的 SSN 或 CCN - 在「記錄資源檢視」中尋找 SSN 或金融卡號碼。
- 客戶名錄 - 在「記錄資源檢視」中尋找電話或電子郵件

隨附的辭典如下：

- 美國社會安全號碼關鍵字 (US SSN Keywords)
- 信用卡號碼關鍵字 (Credit Card Number Keywords)
- ABA 轉帳號碼關鍵字 (ABA Routing Number Keywords)

1998 年資料保護法政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件

描述的內容條件如下：

- 英國選民登記號碼 - 搜尋包含三個部分的單一複合條件： 英國關鍵字辭典中的一個關鍵字、符合英國選民登記號碼規則運算式的樣式，以及英國選民登記號碼單字辭典中的一個關鍵字。
- 英國國家保險號碼 - 搜尋符合英國國家保險號碼規則運算式的項目，以及英國國家保險號碼關鍵字辭典中的關鍵字。
- 英國稅務 ID 號碼 - 搜尋符合英國稅務 ID 號碼規則運算式，以及英國稅務 ID 號碼關鍵字辭典中的關鍵字。
- 英國駕照號碼 - 搜尋包含三個部分的單一複合條件： 英國關鍵字辭典中的一個關鍵字、符合英國駕照規則運算式的樣式，以及使用規則運算式對「駕照」一詞所做的不同組合。
- 英國護照號碼 (舊式) - 搜尋英國護照關鍵字辭典中的關鍵字，以及符合英國護照號碼 (舊式) 規則運算式的樣式。
- 英國護照號碼 (新式) - 搜尋英國護照關鍵字辭典中的關鍵字，以及符合英國護照號碼 (新式) 規則運算式的樣式。

結構化資料條件

英國個人資料保護法 - 在「記錄資源檢視」中尋找下列其中三個資料欄位： NIN (國家保險號碼)、帳號、PIN、金融卡號碼、名字、姓氏、駕照、密碼、納稅人 ID、UK NHS 號碼、出生日期、母親姓氏、電子郵件地址及電話號碼。 需要名字和姓氏及 PIN、密碼、電子郵件、電話或母親姓氏的組合。

隨附的辭典

隨附的辭典如下：

- 英國關鍵字 (UK Keywords)
- 英國選民登記號碼單字 (UK Electoral Roll Number Words)
- 英國國家保險號碼關鍵字 (UK NIN Keywords)
- 英國稅務 ID 號碼關鍵字 (UK Tax ID Number Keywords)
- 英國護照關鍵字 (UK Passport Keywords)

防禦郵件系統 (DMS) GENSER 分類政策範本

以下說明此政策範本所使用的條件和辭典。

在機密、最高機密、已分類或受限制或其他敏感資訊辭典中搜尋關鍵字。 非機密、最高機密和已分類或受限制辭典標題中指出的那些關鍵字和字詞，是由使用者定義。 其他敏感資訊辭典包括的字詞是用來分類機密但未分類的資訊。

隨附的辭典如下：

- 機密 (Secret)
- 最高機密 (Top Secret)
- 已分類或受限制 (Classified or Restricted)
- 其他敏感資訊 (Other Sensitive Information)

設計文件政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 設計文件副檔名 - 搜尋「設計文件副檔名」辭典中的指定副檔名。
- 設計文件 - 搜尋指定的檔案類型： cad_draw 和 dwg。

設計文件副檔名

員工資料保護政策範本

描述的內容條件如下：

- 身分證號碼樣式 - 搜尋符合身分證號碼規則運算式的項目，以及身分證號碼關鍵字辭典中的關鍵字。
- 所有信用卡號碼 - 搜尋符合信用卡號碼系統樣式的項目，以及信用卡號碼關鍵字辭典中的關鍵字。
- ABA 轉帳號碼 - 搜尋符合 ABA 轉帳號碼規則運算式的項目，以及 ABA 轉帳號碼關鍵字辭典中的關鍵字。

結構化資料條件如下：

- 使用者名稱/密碼組合 - 從「記錄資源檢視」中尋找使用者名稱和密碼的組合。
- 3 個或更多個員工資料欄位 - 從「記錄資源檢視」中尋找下列任意三個欄位的資料組合： SSN、電話、電子郵件、名字、姓氏、金融卡號碼、帳號、ABA 轉帳號碼、加拿大社會保險號碼，以及英國國家保險號碼、員工號碼、醫療保險號碼、薪資、入帳帳號和出生日期。
- 員工名錄： 在「記錄資源檢視」中尋找電話或電子郵件

隨附的辭典如下：

- 美國社會安全號碼關鍵字 (US SSN Keywords)
- 信用卡號碼關鍵字 (Credit Card Number Keywords)
- ABA 轉帳號碼關鍵字 (ABA Routing Number Keywords)

加密的資料政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 密碼保護檔案 - 在「密碼保護檔案」附件清單資源中尋找下列副檔名： encrypted_zip、encrypted_doc、encrypted_xls 或 encrypted_ppt。
- PGP 檔案 - 搜尋下列檔案類型： pgp
- GPG 檔案 - 搜尋 GPG 加密關鍵字辭典中的關鍵字。
- S/MIME - 搜尋與 S/MIME 規則運算式符合的項目。
- PGP8 標頭關鍵字 - 在 PGP8 檔案標頭中尋找特性關鍵字。
- PGP8 關鍵字 - 在 PGP8 加密檔案中尋找特性字串。
- PGP 加密文件 - 在 PGP 副檔名辭典中尋找 .pgp 和 .aex 郵件或檔案附件副檔名。

隨附的辭典如下：

- GPG 加密關鍵字 (GPG Encryption Keywords)
- PGP 檔案副檔名 (PGP file extensions)
- PGP8 關鍵字 (PGP8 Keywords)

歐盟資料保護指令政策範本

結構化內容條件如下：

- 歐盟資料保護指令
  在歐盟國碼辭典中搜尋與郵件標頭中的收件者部分不符的國碼，並在記錄資源檢視中尋找下列任兩個資料欄： 姓氏、金融卡號碼、駕照、帳號、PIN、病歷號碼、身分證字號、使用者名稱、密碼、ABA 轉帳號碼、電子郵件、電話及母親姓氏 姓氏與電子郵件、電話、帳號和使用者名稱資料的組合例外。
- 歐盟資料保護，聯絡資訊
  在歐盟國碼辭典中搜尋與郵件標頭中的收件者部分不符的國碼，並尋找下列任兩個資料欄：姓氏、電話號碼、帳號、使用者名稱和電子郵件。

出口管理條例規定 (EAR) 政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為 EAR 商業管制清單和收件者。此條件為複合規則，用於搜尋 EAR 國碼辭典中的收件者國碼以及 EAR CCL 關鍵字辭典中的關鍵字。

結構化資料條件是已建立索引的 EAR 商業管制清單項目和收件者。此複合條件會同時搜尋「EAR 國碼」辭典中的收件者國碼以及記錄資源檢視中的特定「SKU」。

隨附的辭典如下：

- EAR 國碼 (EAR Country Codes)
- EAR CCL 關鍵字 (EAR CCL Keywords)

財務資訊政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件如下所示：

財務資訊 - 搜尋指定檔案類型、財務關鍵字辭典中的關鍵字以及機密/財產單字辭典中的關鍵字組合。 指定的檔案類型包括： excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread 和 123。

隨附的辭典如下：

- 財務關鍵字 (Financial Keywords)
- 機密/專利單字 (Confidential/Proprietary Words)

賭博政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 可疑的賭博關鍵 - 搜尋「已確認的賭博關鍵字」辭典中的五個關鍵字。
- 可疑賭博程度較低的關鍵字 - 搜尋「可疑的賭博關鍵字」辭典中的十個關鍵字。

隨附的辭典如下：

- 已確認的賭博關鍵字 (Gambling Keywords, Confirmed)
- 可疑的賭博關鍵字 (Gambling Keywords, Suspect)

金融服務法案 (Gramm-Leach-Bliley) 政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 美國社會安全號碼 - 社會安全號碼。 若要符合此規則，必須有一個號碼符合「有效身分證號碼」進階樣式，還要有一個關鍵單字或詞組表示 US SSN 含有身分證號碼關鍵字辭典中的關鍵字。 加入關鍵字條件的目的是為了避免誤報可能符合 SSN 格式的號碼。
- ABA 轉帳號碼 - 搜尋符合 ABA 轉帳號碼規則運算式的項目，以及 ABA 轉帳號碼關鍵字辭典中的關鍵字。
- 所有信用卡號碼 - 搜尋信用卡號碼。 類似於第一個規則，這個規則也需要有個號碼符合信用卡系統樣式 ccn，且有信用卡號碼關鍵字辭典中的關鍵單字或詞組，表示有信用卡號碼存在。 加入關鍵字條件的目的是為了避免誤報可能符合信用卡格式的號碼。

結構化資料條件如下：

- 使用者名稱/密碼組合 - 從「記錄資源檢視」中尋找使用者名稱和密碼的組合。
- 3 個或更多個重要客戶欄位 - 從「記錄資源檢視」中，尋找除電話、電子郵件及名字或姓氏的組合以外之可單獨代表客戶的其他任意三個欄位。
- 準確的 SSN 或 CCN - 從「記錄資源檢視」中尋找 SSN 或金融卡號碼。
- 客戶名錄 - 從「記錄資源檢視」中尋找電話或電子郵件。

隨附的辭典如下：

- 美國社會安全號碼關鍵字 (US SSN Keywords)
- 信用卡號碼關鍵字 (Credit Card Number Keywords)
- ABA 轉帳號碼關鍵字 (ABA Routing Number Keywords)

HIPAA 政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- SSN 與藥品關鍵字 - 搜尋具有「有效社會安全號碼」進階樣式的身分證號碼 (SSN)，加上美國社會安全號碼關鍵字辭典中的關鍵字，以及處方藥品名稱辭典中的關鍵字。
- SSN 與治療關鍵字 - 搜尋具有「有效社會安全號碼」進階樣式的社會安全號碼 (SSN)，加上美國社會安全號碼關鍵字辭典中的關鍵字，以及醫學治療關鍵字辭典中的關鍵字。
- SSN 與疾病關鍵字 - 搜尋具有「有效社會安全號碼」進階樣式的社會安全號碼 (SSN)，加上美國社會安全號碼關鍵字辭典中的關鍵字，以及疾病名稱辭典中的關鍵字。
- SSN 與藥品代碼 - 搜尋具有「有效社會安全號碼」進階樣式的社會安全號碼 (SSN)，加上美國社會安全號碼關鍵字辭典中的關鍵字，以及使用藥品代碼規則運算式的藥品代碼。

結構化資料條件如下：

- 病患資料和藥品代碼 - 郵件的任何部分符合 NDC 藥品代碼規則運算式，且郵件的任何部分符合「記錄資源檢視」中的文字。
- 病患資料和藥品關鍵字 - 郵件的任何部分符合處方藥品名稱辭典項目，且郵件的任何部分符合「記錄資源檢視」中的項目。
- 病患資料和治療關鍵字 - 郵件的任何部分符合醫學治療關鍵字辭典中的項目，且郵件的任何部分符合「記錄資源檢視」中的文字。
- 病患資料和疾病關鍵字 - 郵件的任何部分符合疾病名稱辭典中的項目，且郵件的任何部分符合「記錄資源檢視」中的文字。

例外條件：

- TPO 例外 - 搜尋符合「TPO 電子郵件地址」辭典中位址的收件者電子郵件地址。 找到符合項目時，即使其他條件符合，也不會觸發政策。

  附註：TPO (治療、給付或醫療作業) 是指與醫療院所合作的公司，可享 HIPPA 資訊限制的特殊豁免。 如果受保護的資訊傳送到這些公司，此規則例外不會觸發政策。 客戶必須將這些公司的電子郵件地址輸入範本。

隨附的辭典如下：

- 美國社會安全號碼關鍵字 (US SSN Keywords)
- 處方藥品名稱 (Prescription Drug Names)
- 醫學治療關鍵字 (Medical Treatment Keywords)
- 疾病名稱 (Disease Names)
- TPO 電子郵件地址 (TPO Email Addresses)

1998 年人權法政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為英國選民登記號碼。此條件會搜尋包含四個部分的單一複合條件：英國關鍵字辭典中的一個關鍵字、符合英國選民登記號碼規則運算式的樣式、英國選民登記號碼單字辭典中的一個關鍵字，以及英國個人資料關鍵字辭典中的一個關鍵字。

結構化資料條件是英國個人資料保護法。此條件為複合規則，用於搜尋由記錄資源檢視中的姓氏和選民登記號碼，以及英國個人資料關鍵字辭典中的關鍵字。

隨附的辭典如下：

- 英國個人資料關鍵字 (UK Personal Data Keywords)
- 英國關鍵字 (UK Keywords)
- 英國選民登記號碼單字 (UK Electoral Roll Number Words)

違禁藥品政策範本

描述的內容條件如下：

- 市售毒品 - 搜尋市售毒品名稱辭典中的五個關鍵字。
- 大批量製造的受管制物品 - 搜尋大批量製造的 受管制物品辭典中的五個關鍵字。

隨附的辭典如下：

- 市售毒品名稱 (Street Drug Names)
- 大批量製造的 受管制物品 (Manufd. Controlled Substances)

美國報稅號碼 (ITIN) 政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為美國報稅號碼。此條件會搜尋符合美國報稅號碼規則運算式的項目，以及「美國報稅號碼關鍵字」字辭典中的關鍵字。

隨附的辭典是「美國報稅號碼關鍵字」。

國際武器運輸條例規定 (ITAR) 政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為 ITAR 軍火清單和收件者。此複合規則會同時搜尋 ITAR 國碼辭典中的收件者國碼以及 ITAR 軍品辭典中的關鍵字。

結構化資料條件是已建立索引的 ITAR 軍火項目和收件者。此複合規則會搜尋 ITAR 國碼辭典中的收件者國碼以及記錄資源檢視中的特定庫存單位 (SKU) 號碼。

隨附的辭典如下：

- ITAR 國碼 (ITAR Country Codes)
- ITAR 軍品 (ITAR Munition Names)

媒體檔政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 媒體檔 - 搜尋下列檔案類型： qt、riff、macromedia_dir、midi、mp3、mpeg_movie、quickdraw、realaudio、wav、video_win 和 vrml。
- 媒體檔副檔名 - 搜尋媒體檔副檔名辭典中的副檔名。

隨附的辭典是「媒體檔副檔名」。

合併與收購資料政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為「合併及收購活動」。此條件會搜尋由使用者定義的合併及收購專案代碼名稱辭典中的任何關鍵字。合併與收購活動極其特定於客戶和專案。在所有合格的客戶和使用者之間沒有一般術語。

隨附的辭典是「合併及收購專案代碼名稱」

NASD 規定 2711 與 NYSE 規定 351 和 472 政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件	描述性內容條件為 NASD 規定 2711 與 NYSE 規定 351 和 472。此複合規則包含寄件者條件和關鍵字條件。寄件者條件須由使用者編輯，這份清單會列出貴公司研究分析師的電子郵件地址辭典。 關鍵字條件則包括任何近期股票上市案、該上市案的內部專案名稱以及上市公司的股市代號 (NASD 2711 關鍵字辭典)。 此規則與寄件者條件一樣，也須由使用者編輯。
隨附的辭典	隨附的辭典如下： ■ 分析師的電子郵件地址 (Analysts' Email Addresses) ■ NASD 2711 關鍵字 (NASD 2711 Keywords)

NASD 規定 3010 與 NYSE 規定 342 政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 股票建議 - 使用複合規則同時搜尋「NASD 3010 股票關鍵字」辭典中的關鍵字以及「NASD 3010 購買或出售關鍵字」辭典中的關鍵字。此規則須有證據同時顯示提供股票建議和買進或賣出動作建議。
- NASD 規定 3010 與 NYSE 規定 342 關鍵字 - 搜尋 NASD 3010 一般關鍵字辭典中的關鍵字。 這些關鍵字會搜尋任何一般股票經紀活動。

隨附的辭典如下：

- NASD 3010 股票關鍵字 (NASD 3010 Stock Keywords)
- NASD 3010 購買或出售關鍵字 (NASD 3010 Buy/Sell Keywords)
- NASD 3010 一般關鍵字 (NASD 3010 General Keywords)

電業的 NERC 安全指導原則政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件是同時在**「敏感關鍵字」**辭典及**「漏洞關鍵字」**辭典中搜尋任何相符關鍵字的一種複合規則。

隨附的辭典如下：

- 敏感關鍵字 (Sensitive Keywords)
- 漏洞關鍵字 (Vulnerability Keywords)

網路圖政策範本

描述的內容條件如下：

- 包含 IP 位址的網路圖 - 搜尋 Visio 檔案類型再加上 IP 位址規則運算式。
- 包含 IP 位址關鍵字的網路圖 - 搜尋 Visio 檔案類型再加上使用規則運算式對 IP 位址一詞所做的不同組合。

網路安全政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- GoToMyPC 活動 - 搜尋使用規則運算式的 GoToMyPC 指令格式。
- 駭客關鍵字 - 搜尋駭客關鍵字辭典中的關鍵字。
- 鍵盤記錄 - 搜尋鍵盤記錄關鍵字辭典中的關鍵字。

隨附的辭典如下：

- 駭客關鍵字 (Hacker Keywords)
- 鍵盤記錄關鍵字 (Keylogger Keywords)

攻擊性語言政策範本

描述的內容條件如下：

- 明顯攻擊性語言 - 搜尋「明顯攻擊性語言」辭典中的任一關鍵字。
- 一般攻擊性語言 - 搜尋「一般攻擊性語言」辭典中的任三個關鍵字。

隨附的辭典如下：

- 明顯攻擊性語言 (Offensive Language, Explicit)
- 一般攻擊性語言 (Offensive Language, General)

海外資產控制局 (OFAC) 政策範本

以下說明此政策範本所使用的條件和辭典。

OFAC 政策範本中有兩個主要條件。一是規定特別指定國民 (SDN) 清單，另一則是一般 OFAC 政策限制。

描述的內容條件如下：

- OFAC 特別指定國民列表與收件者 - 搜尋國碼符合 OFAC SDN 國碼辭典中項目的收件者，以及 SDN 清單辭典中的關鍵字。
  SDN 清單是指受貿易規定限制的特定人或組織。 美國財政部會提供文字檔，列出這些個人與組織的名稱、最後已知地址以及已知別名。 但依據財政部規定，雖地址有可能不是正確或最新地址，然而不同地址不會解除對這些人或組織的限制。
- 與 OFAC 國家的通訊 - 搜尋國碼符合 OFAC 國碼辭典中項目的收件者。
  此條件提供美國財政部對特定國家一般貿易往來的限制規定。 這與 SDN 清單不同，因為這部分並未提及個人或組織。 這個範本會搜尋指定國碼為所列國家的收件者。

隨附的辭典如下：

- SDN 清單 (SDN List)
- OFAC SDN 國碼 (OFAC SDN Country Codes)
- OFAC 國碼 (OFAC Country Codes)

密碼檔政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 密碼檔名 - 搜尋檔名 passwd 或 shadow。
- /etc/passwd 格式 - 搜尋有 /etc/passwd 格式規則運算式的樣式。
- /etc/shadow 格式 - 搜尋有 /etc/shadow 格式規則運算式的樣式。
- SAM P密碼 - 搜尋有 SAM 格式規則運算式的樣式。

隨附的辭典是「密碼檔案名稱」。

付款卡產業資料安全標準政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為所有信用卡號碼。此條件會搜尋符合有效信用卡樣式的項目，以及信用卡號碼關鍵字辭典中的關鍵字。

結構化資料條件會搜尋記錄資源檢視中的相符項目。

隨附的辭典是「信用卡號碼關鍵字」。

PIPEDA 政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 加拿大社會保險號碼 - 搜尋符合加拿大社會保險號碼規則運算式的項目，以及加拿大社會保險號碼單字 (Canadian Social Ins. No. Words) 辭典中的關鍵字。
- ABA 轉帳號碼 - 尋找 ABA 轉帳號碼關鍵字辭典中的字，以及符合 ABA 轉帳號碼規則運算式的項目。
- 所有信用卡號碼 - 尋找信用卡號碼關鍵字辭典中的字，以及符合信用卡號碼系統樣式的項目。

英國選民登記號碼 - 搜尋包含四個部分的單一複合條件： 英國關鍵字辭典中的一個關鍵字、符合英國選民登記號碼規則運算式的樣式、英國選民登記號碼單字辭典中的一個關鍵字，以及英國個人資料關鍵字辭典中的一個關鍵字。

結構化資料條件如下：

- PIPEDA - 在「記錄資源檢視」中尋找下列任意兩個資料欄位： 姓氏、金融卡、醫療帳號、醫療記錄、代理人號碼、帳號、PIN、使用者名稱、密碼、SIN、ABA 轉帳號碼、電子郵件、電話、母親姓氏。 需要姓氏與電子郵件、電話、帳號或使用者名稱的組合。
- PIPEDA，聯絡資訊 - 在「記錄資源檢視」中尋找下列任意兩個資料欄位： 姓氏、電話、帳號、使用者名稱、電子郵件

隨附的辭典如下：

- 加拿大社會保險號碼單字 (Canadian Social Ins. No. Words)
- ABA 轉帳號碼關鍵字 (ABA Routing Number Keywords)
- 信用卡號碼關鍵字 (Credit Card Number Keywords)

價格資訊政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件會在記錄資源檢視中搜尋使用者指定的庫存單位 (SKU) 號碼及該 SKU 號碼的價格之組合。

專案資料政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為「專案活動」。此條件會搜尋由使用者定義的敏感專案代碼名稱辭典中的任何關鍵字。

隨附的辭典是「敏感專案代碼名稱」

出版文件政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 出版文件 - 搜尋指定的檔案類型： qxpress、frame、aldus_pagemaker 和 publ (Microsoft Publisher)。
- 出版文件，副檔名 - 搜尋出版文件副檔名辭典中指定的副檔名。

隨附的辭典是「出版文件副檔名」

種族主義語言政策範本

描述性內容條件為「種族主義語言」。此條件會搜尋種族主義語言辭典中的任一關鍵字。

隨附的辭典是「種族主義語言」。

限制的檔案政策範本

描述性內容條件為「MSAccess 檔案和可執行檔」。此條件會搜尋指定類型的檔案：access、exe 和 exe_unix。

限制的收件者政策範本

描述性內容條件為「限制的收件者」。此條件搜尋電子郵件地址列於「限制的收件者」辭典的收件者郵件。

隨附的辭典是「限制的收件者」。

履歷表政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為所有履歷表。此條件會搜尋指定類型檔案 (.doc)，這些檔案小於 50 KB 且至少符合下列每個辭典中的一個關鍵字：教育類職位搜尋關鍵字、工作類職位搜尋關鍵字和一般職位搜尋關鍵字。

結構化資料條件為員工履歷表。此條件會比對「員工履歷表」附件清單資源中指定的類型 (例如 .doc) 且小於 50 KB 的檔案，以及比對符合下列條件的檔案：(1) 符合下列每個辭典中至少一個關鍵字：教育類職位搜尋關鍵字、工作類職位搜尋關鍵字及一般職位搜尋關鍵字，以及 (2) 符合記錄資源檢視中員工的名字和姓氏。

隨附的辭典如下：

- 教育類職位搜尋關鍵字 (Job Search Keywords, Education)
- 工作類職位搜尋關鍵字 (Job Search Keywords, Work)
- 一般職位搜尋關鍵字 (Job Search Keywords, General)

沙賓法案 (Sarbanes-Oxley) 政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- SEC 公平揭露規定 - 反映 SEC 公平揭露政策的該規定，會搜尋三種不同的條件，而且必須符合所有條件： SEC 公平揭露關鍵字辭典中的任何關鍵字、公司名稱關鍵字辭典中的任何關鍵字，以及試算表或文件檔案格式的任何常用文件。
  SEC 公平揭露關鍵字表示可能在事前揭露財務資訊。公司名稱關鍵字須由使用者編輯。這可能包括意指公司的任何名稱、別名或縮寫。 具體來說，偵測的檔案類型包括： excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、wordperfect 和 pdf。
- 財務資訊 - 必須符合三種不同的條件，包括： 財務關鍵字辭典中的字、機密/財產單字辭典中的字，以及試算表檔案類型。 試算表檔案類型包括 excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread 及 123。

隨附的辭典如下：

- SEC 公平揭露關鍵字 (SEC Fair Disclosure Keywords)
- 公司名稱關鍵字 (Company Name Keywords)
- 財務關鍵字 (Financial Keywords)
- 機密/專利單字 (Confidential/Proprietary Words)

SEC 公平揭露規定政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- SEC 公平揭露規定 - 在 SEC 公平揭露政策中反映該規定，會搜尋三種不同的條件，而且必須符合所有條件： SEC 公平揭露關鍵字辭典中的任何關鍵字、公司名稱關鍵字辭典中的任何關鍵字，以及試算表或文件檔案格式的任何常用文件。
  SEC 公平揭露關鍵字表示可能在事前揭露財務資訊。 公司名稱關鍵字須由使用者編輯。這可能包括意指公司的任何名稱、別名或縮寫。 具體來說，偵測的檔案類型包括： excel_macro、xls、works_spread、sylk、quattro_pro、mod、csv、applix_spread、123、doc、wordperfect 和 pdf。

隨附的辭典如下：

- SEC 公平揭露關鍵字 (SEC Fair Disclosure Keywords)
- 公司名稱關鍵字 (Company Name Keywords)

色情語言政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 已確認的色情關鍵字 - 搜尋「已確認的色情關鍵字」辭典中的任一關鍵字。
- 疑似色情關鍵字 - 搜尋「疑似色情關鍵字」辭典中的任三個關鍵字。
- 可能色情關鍵字 - 搜尋「可能色情關鍵字」辭典中的任三個關鍵字。

隨附的辭典如下：

- 可能 色情關鍵字 (Sex. Explicit Words, Confirmed)
- 可能 色情關鍵字 (Sex. Explicit Words, Suspect)
- 可能 色情關鍵字 (Sex. Explicit Words, Possible)

原始程式碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 原始程式碼延伸 - 搜尋原始程式碼延伸辭典中的副檔名。
- Java 原始程式碼 - 搜尋匯入陳述式或 Java 類別檔規則運算式。
- C 原始程式碼 - 搜尋 C 原始程式碼規則運算式。
- VB 原始程式碼 - 搜尋 VB 原始程式碼規則運算式。
- PERL 原始程式碼 - 搜尋三種不同的 PERL 相關系統樣式和規則運算式。

隨附的辭典是「原始程式碼延伸」

州資料隱密性政策範本

描述的內容條件如下：

- 身分證號碼 - 搜尋身分證號碼關鍵字辭典中的字，以及符合「有效身分證號碼」進階樣式的項目。
- ABA 轉帳號碼 - 搜尋 ABA 轉帳號碼關鍵字辭典中的字，以及符合 ABA 轉帳號碼規則運算式的項目。
- 所有信用卡號碼 - 搜尋信用卡號碼關鍵字辭典中的字，以及信用卡號碼系統樣式。
- 加州駕照號碼 - 搜尋符合加州駕照號碼樣式的項目、符合駕照相關術語規則運算式的項目，以及加州關鍵字辭典中的關鍵字。
- 紐約駕照號碼 - 搜尋符合紐約駕照號碼樣式的項目、符合駕照相關術語規則運算式的項目，以及紐約關鍵字辭典中的關鍵字。
- 字母 + 12 位數的駕照號碼 - 搜尋符合規定駕照號碼樣式的項目、符合駕照相關術語規則運算式的項目，以及字母/12 位數字中的關鍵字。駕照號碼地區關鍵字辭典 (即佛羅里達州、明尼蘇達州和密西根州) 中的關鍵字。
- 伊利諾州駕照號碼 - 搜尋符合伊利諾州駕照號碼樣式的項目、符合駕照相關術語規則運算式的項目，以及美國伊利諾州關鍵字辭典中的關鍵字。
- 紐澤西州駕照號碼 - 搜尋符合紐澤西州駕照號碼樣式的項目、符合駕照相關術語規則運算式的項目，以及美國新澤西州關鍵字辭典中的關鍵字。

例外條件：

- 傳送到附屬網域的電子郵件 - 傳送到附屬網域的電子郵件如依法獲准接收州資料隱私法規定的資訊，則視為例外。關聯網域辭典須由使用者編輯。

州資料隱私法，客戶資料 - 在「記錄資源檢視」中，搜尋除名字、姓氏、pin 及名字、姓氏、密碼外的其他任意三個相符項目。

例外條件：

- 傳送到附屬網域的電子郵件 - 傳送到附屬網域的電子郵件如依法獲准接收州資料隱私法規定的資訊，則視為例外。關聯網域辭典須由使用者編輯。

隨附的辭典如下：

- 美國社會安全號碼關鍵字 (US SSN Keywords)
- ABA 轉帳號碼關鍵字 (ABA Routing Number Keywords)
- 信用卡號碼關鍵字 (Credit Card Number Keywords)
- 加州關鍵字
- 紐約關鍵字 (New York Keywords)
- 字母/12 位數 駕照號碼地區關鍵字 (Letter/12 Num. DLN State Words)
- 美國伊利諾州關鍵字 (Illinois Keywords)
- 美國新澤西州關鍵字 (New Jersey Keywords)
- 關聯網域 (Affiliate Domains)

SWIFT 代碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為「SWIFT 代碼規則運算式」。此條件會搜尋符合 SWIFT 代碼規則運算式的項目，以及「SWIFT 代碼關鍵字」辭典中的關鍵字。

隨附的辭典是「SWIFT 代碼關鍵字」。

英國駕照號碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件是包含三個部分的單一複合條件：「英國關鍵字」辭典中的一個關鍵字、符合英國駕照規則運算式的樣式，以及使用規則運算式對「駕照」一詞所做的不同組合。

隨附的辭典是「英國關鍵字」。

英國選民登記號碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件是包含三個部分的單一複合條件：英國關鍵字辭典中的一個關鍵字、符合英國選民登記號碼規則運算式的樣式，以及英國選民登記號碼單字辭典中的一個關鍵字。

隨附的辭典如下：

- 英國關鍵字 (UK Keywords)
- 英國選民登記號碼單字 (UK Electoral Roll Number Words)

英國國家保險號碼政策範本

描述性內容條件為英國國家保險號碼。此條件會搜尋符合英國國家保險號碼規則運算式的項目，以及英國國家保險號碼關鍵字辭典中的關鍵字。

隨附的辭典是「英國國家保險號碼關鍵字」。

英國護照號碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述的內容條件如下：

- 英國護照號碼 (舊式) - 搜尋英國護照關鍵字辭典中的關鍵字，以及符合英國護照號碼 (舊式) 規則運算式的樣式。
- 英國護照號碼 (新式) - 搜尋英國護照關鍵字辭典中的關鍵字，以及符合英國護照號碼 (新式) 規則運算式的樣式。

隨附的辭典是「英國護照關鍵字」。

英國稅務 ID 號碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為英國稅務 ID 號碼。此條件會搜尋符合英國稅務 ID 號碼規則運算式的項目，以及英國稅務 ID 號碼關鍵字辭典中的關鍵字。

隨附的辭典是「英國稅務 ID 號碼關鍵字」。

美國智慧型控制標記 (CAPCO) 及 DCID 1/7 政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件在機密、最高機密或已分類或受限制辭典中搜尋任何關鍵字。非辭典標題中指出的那些關鍵字和字詞，是由使用者定義。

隨附的辭典如下：

- 機密 (Secret)
- 最高機密 (Top Secret)
- 已分類或受限制 (Classified or Restricted)

美國社會安全號碼政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為美國社會安全號碼特徵。此條件會搜尋符合社會安全號碼規則運算式的項目，以及美國社會安全號碼關鍵字辭典中的關鍵字。

隨附的辭典是「美國社會安全號碼關鍵字」。

暴力與武器政策範本

以下說明此政策範本所使用的條件和辭典。

描述性內容條件為「暴力與武器」。此複合條件搜尋暴力關鍵字辭典中的關鍵字，以及武器關鍵字辭典中的關鍵字。

隨附的辭典如下：

- 暴力關鍵字 (Violence Keywords)
- 武器關鍵字 (Weapons Keywords)

附錄 D

使用 Dell Remote Access Controller

本附錄包含以下主題：

- 關於 Dell Remote Access Controller (DRAC) 卡
- 使用 DRAC 強制重新啟動 Symantec Messaging Gateway 硬體裝置
- 從 DRAC 正常重新啟動 Symantec Messaging Gateway 硬體裝置
- 使用 DRAC 從遠端安裝及架構 Symantec Messaging Gateway 硬體裝置
- 使用 DRAC 從虛擬媒體安裝 Symantec Messaging Gateway 影像
- 使用 DRAC 檢視 Dell 伺服器診斷
- 使用 DRAC 刪除 Symantec Messaging Gateway 硬體裝置的日誌、組態資訊和資料
- 使用 DRAC 將 Symantec Messaging Gateway 硬體裝置還原至原始出廠組態

關於 Dell Remote Access Controller (DRAC) 卡

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

DRAC 卡是 Symantec Messaging Gateway 硬體裝置隨附的硬體控制器。表 D-1 列出賽門鐵克硬體裝置的 DRAC 支援資訊。

表 D-1 賽門鐵克硬體裝置的 DRAC 支援

硬體裝置	DRAC 支援
Symantec Mail Security 8380	是
Symantec Brightmail 8380	是
Symantec 8380	是
Symantec Brightmail 8360	是
Symantec 8360	是
Symantec Mail Security 8360	否
Symantec Mail Security 8340	否
Symantec Mail Security 8320	否

此卡已作為與系統主機板連接的子卡整合到 Symantec Messaging Gateway 硬體裝置中。

您可使用 DRAC 卡執行下列任一工作：

- 在伺服器發生故障後存取伺服器。
- 遠端檢視伺服器內部事件日誌以執行診斷。
- 將主控台輸出 (圖形和文字) 重新導向至遠端主控台，藉以管理伺服器。
- 有序關閉伺服器以進行維護工作。
- 診斷伺服器故障及重新啟動伺服器。
- 在伺服器偵測到錯誤時透過電子郵件或簡易網路管理通訊協定 (SNMP) 陷阱接收警示。

賽門鐵克建議您使用不同網路的子網路來進行 DRAC 管理。

啟用 DRAC 功能後，賽門鐵克建議您變更預設的 DRAC 根密碼。如需變更 DRAC 密碼的詳細資訊，請參閱 Dell 支援網站。

請參閱第 758 頁的「使用 DRAC 強制重新啟動 Symantec Messaging Gateway 硬體裝置」。

請參閱第 758 頁的「從 DRAC 正常重新啟動 Symantec Messaging Gateway 硬體裝置」。

請參閱第 759 頁的「使用 DRAC 從遠端安裝及架構 Symantec Messaging Gateway 硬體裝置」。

請參閱第 760 頁的「使用 DRAC 從虛擬媒體安裝 Symantec Messaging Gateway 影像」。

請參閱第 760 頁的「使用 DRAC 檢視 Dell 伺服器診斷 」。

請參閱第 761 頁的「使用 DRAC 刪除 Symantec Messaging Gateway 硬體裝置的日誌、組態資訊和資料」。

請參閱第 761 頁的「使用 DRAC 將 Symantec Messaging Gateway 硬體裝置還原至原始出廠組態」。

使用 DRAC 強制重新啟動 Symantec Messaging Gateway 硬體裝置

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

如果您有 DRAC 的存取權，但沒有 Symantec Messaging Gateway 硬體裝置上作業系統的存取權，DRAC 可讓您在不存取作業系統的情況下，從遠端強制重新啟動硬體裝置。

使用 DRAC 強制重新啟動 Symantec Messaging Gateway 硬體裝置

1. 在瀏覽器的位址欄位中輸入 DRAC 卡的 IP 位址，然後按 **Enter**。
2. 使用 DRAC 根憑證登入，然後按**「確定」**。
3. 按下**「電源管理」**。
4. 選取**「重新啟動系統電源」**。
5. 按下**「套用」**。

請參閱第 756 頁的「關於 Dell Remote Access Controller (DRAC) 卡」。

從 DRAC 正常重新啟動 Symantec Messaging Gateway 硬體裝置

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

您可以視需要重新啟動硬體裝置。重新啟動硬體裝置需要硬體裝置關閉本身，然後再重新啟動本身。DRAC 可讓您透過支援的網頁瀏覽器從遠端存取硬體裝置。

正常重新啟動 Symantec Messaging Gateway 硬體裝置會停止所有服務，然後重新啟動硬體裝置。

附註：如果在 Symantec Messaging Gateway 上執行軟體更新時重新啟動硬體裝置，則可能會損毀硬體裝置軟體。

從 DRAC 正常重新啟動 Symantec Messaging Gateway 硬體裝置

1. 在瀏覽器的位址欄位中輸入 DRAC 卡的 IP 位址，然後按 **Enter**。
2. 使用 DRAC 根憑證登入，然後按**「確定」**。
3. 按下**「主控台」**。
4. 確定已停用彈出式視窗攔截程式，然後按下**「連線」**。
5. 使用您的 Symantec Messaging Gateway 硬體裝置管理員憑證登入。
6. 執行 `reboot` 指令。

   請參閱第 699 頁的reboot。

請參閱第 756 頁的「關於 Dell Remote Access Controller (DRAC) 卡」。

使用 DRAC 從遠端安裝及架構 Symantec Messaging Gateway 硬體裝置

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

您可能想要從遠端位置安裝及架構 Symantec Messaging Gateway 硬體裝置。DRAC 可讓您透過支援的網頁瀏覽器從遠端存取硬體裝置。

使用 DRAC 從遠端安裝及架構 Symantec Messaging Gateway 硬體裝置

1. 在瀏覽器的位址欄位中輸入 DRAC 卡的 IP 位址，然後按 **Enter**。
2. 使用 DRAC 根憑證登入，然後按**「確定」**。
3. 按下**「主控台」**。
4. 確定已停用彈出式視窗攔截程式，然後按下**「連線」**。
5. 安裝 Symantec Messaging Gateway 產品。

   如需詳細資訊，請參閱「Symantec Messaging Gateway 安裝指南」。

請參閱第 756 頁的「關於 Dell Remote Access Controller (DRAC) 卡」。

使用 DRAC 從虛擬媒體安裝 Symantec Messaging Gateway 影像

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

您可能想要從遠端位置安裝 Symantec Messaging Gateway。使用已對應至本機 ISO 檔案或本機 CD/DVD-ROM 光碟機的虛擬媒體在硬體裝置上安裝 Symantec Messaging Gateway。

使用 DRAC 從虛擬媒體安裝 Symantec Messaging Gateway 影像

1. 將 Symantec Messaging Gateway ISO 影像複製到本機磁碟機，或是將 CD/DVD 插入到本機 CD/DVD-ROM 光碟機中。
2. 在瀏覽器的位址欄位中輸入 DRAC 卡的 IP 位址，然後按 **Enter**。
3. 使用 DRAC 根憑證登入，然後按下**「確定」**。
4. 按下**「媒體」**。
5. 瀏覽至適當位置以選取 Symantec Messaging Gateway ISO 影像檔。

   如果您已將虛擬媒體對應至本機 CD/DVD-ROM 光碟機，請選取本機 CD/DVD-ROM 光碟機。
6. 按下**「連線」**。
7. 重新啟動硬體裝置。
8. 當系統重新啟動時，請輸入適當的功能鍵以選擇開機媒體。

   如需選擇功能鍵的詳細資訊，請參閱 Dell 支援網站。
9. 選取**「虛擬 CDROM」**。

請參閱第 756 頁的「關於 Dell Remote Access Controller (DRAC) 卡」。

使用 DRAC 檢視 Dell 伺服器診斷

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

當 Dell 伺服器出現故障時，您可以使用 DRAC 從遠端連線至系統來檢視 Dell 診斷報告。

使用 DRAC 檢視 Dell 伺服器診斷

1 從遠端重新啟動 Symantec Messaging Gateway。

請參閱第 758 頁的「使用 DRAC 強制重新啟動 Symantec Messaging Gateway 硬體裝置」。

2 當系統重新啟動時，請輸入適當的功能鍵以啟動診斷。

如需選擇功能鍵以啟動診斷的詳細資訊，請參閱 Dell 支援網站。

請參閱第 756 頁的「關於 Dell Remote Access Controller (DRAC) 卡」。

使用 DRAC 刪除 Symantec Messaging Gateway 硬體裝置的日誌、組態資訊和資料

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

您可能想要從遠端刪除日誌、組態資訊和資料。DRAC 可讓您透過支援的網頁瀏覽器從遠端存取硬體裝置。

使用 DRAC 刪除 Symantec Messaging Gateway 硬體裝置的日誌、組態資訊和資料

1 在瀏覽器的位址欄位中輸入 DRAC 卡的 IP 位址，然後按 **Enter**。

2 使用 DRAC 根憑證登入，然後按**「確定」**。

3 按下**「主控台」**。

4 確定已停用彈出式視窗攔截程式，然後按下**「連線」**。

5 使用您的 Symantec Messaging Gateway 硬體裝置管理員憑證登入。

6 執行 `delete` 指令。

請參閱第 647 頁的delete。

請參閱第 756 頁的「關於 Dell Remote Access Controller (DRAC) 卡」。

使用 DRAC 將 Symantec Messaging Gateway 硬體裝置還原至原始出廠組態

附註：SMG 10.7.0 會在兩個不同的硬體平台上執行：Dell 83xx 和 Symantec 8380-S450。Dell 83xx 平台支援 DRAC/iDRAC，但 Symantec 8380-S450 平台不支援。

您可能想要從遠端將您的硬體裝置還原至原始出廠組態。DRAC 可讓您透過支援的網頁瀏覽器從遠端存取硬體裝置。

使用 DRAC 將 Symantec Messaging Gateway 硬體裝置還原至原始出廠組態

1. 在瀏覽器的位址欄位中輸入 DRAC 卡的 IP 位址，然後按 **Enter**。
2. 使用 DRAC 根憑證登入，然後按**「確定」**。
3. 按下**「主控台」**。
4. 確定已停用彈出式視窗攔截程式，然後按下**「連線」**。
5. 使用您的 Symantec Messaging Gateway 硬體裝置管理員憑證登入。
6. 執行 `delete all` 指令。

   請參閱第 647 頁的delete。

請參閱第 756 頁的「關於 Dell Remote Access Controller (DRAC) 卡」。

附錄 E

聯邦資訊處理標準 (FIPS) 法規遵循

本附錄包含以下主題：

- 關於 Symantec Messaging Gateway FIPS 140-2 第 1 級標準遵循
- 關於使用 FIPS 模式時的安裝或升級
- 關於控管中心的憑證信任
- FIPS 模式最佳實務準則與考量
- 關於使用 FIPS 時，部分 Symantec Messaging Gateway 的功能限制
- 開啟或關閉 FIPS 模式

關於 Symantec Messaging Gateway FIPS 140-2 第 1 級標準遵循

FIPS 140-2 是美國國家標準與技術局 (NIST) 標準，其中概述安全設計需求與加密模組實作。許多組織在考慮使用硬體與軟體元件時會採用此標準。

本版本使用的加密模組符合 FIPS 140-2 1 級需求。這些模組已提交至「密碼模組驗證方案」驗證是否符合 FIPS 140-2 第 1 級標準。Symantec 預計在下一個主要 Symantec Messaging Gateway 版本前就會收到美國國家標準與技術局的正式驗證。

Symantec Messaging Gateway 包含以下已通過驗證的加密模組：

- Symantec Scanner Cryptographic Module
- Symantec Control Center Cryptographic Module

本版本使用的加密模組以 NIST 先前驗證的模組為基礎。這些模組符合 FIPS 140-2 第 1 級標準。

下列加密法符合 FIPS 140-2 第 1 級標準，目前正在測試驗證中：

- 從網頁瀏覽器到控管中心的 Web 伺服器 HTTPS 連線
- 從控管中心到掃描程式 (代理程式) 主機的 HTTPS 連線
- 控管中心管理員憑證建立與儲存
- Symantec Messaging Gateway 到 Symantec Global Intelligence Network 的通訊
- SMTP TLS 通訊
- 軟體更新通訊
- Remote Secure Shell 存取
- SNMPv3 加密
- DomainKeys Identified Mail (DKIM) 金鑰
- 資料目錄伺服器安全通訊 (LDAPS)

某些限制適用於某些 Symantec Messaging Gateway 功能。

請參閱第 766 頁的「關於使用 FIPS 時，部分 Symantec Messaging Gateway 的功能限制」。

如需驗證的相關資訊，請連上 Internet 並移至下列 URL：

http://www.symantec.com/docs/TECH167725

如需 FIPS 140-2 1 級測試與驗證目前狀態的詳細資訊，請聯繫您的賽門鐵克客戶代表。

如需 FIPS 140-2 標準與驗證方案的一般資訊，請連上 Internet 並移至下列 URL：

美國國家標準與技術局 (NIST) 密碼模組驗證方案

關於使用 FIPS 模式時的安裝或升級

您安裝或升級本版 Symantec Messaging Gateway 的方式與舊版的安裝或升級方式相同。

下列有關新安裝或升級的資訊十分重要：

- Symantec Messaging Gateway 產品架構相同，無論您將 FIPS 模式開啟或關閉。差異是當 FIPS 模式開啟時，產品會強制執行與 FIPS 140-2 標準關聯的嚴格加密清單。當 FIPS 模式關閉時 Symantec Messaging Gateway 使用的加密清單愈大，會增加與外部郵件傳輸代理程式 (MTA) 之間的互通性。
  請參閱第 767 頁的「開啟或關閉 FIPS 模式」。
- Symantec Messaging Gateway 的新安裝預設為關閉 FIPS 模式。
- 如果您在 9.5.2 或更新版本中使用 FIPS 模式，則在升級時會保留 FIPS 模式的狀態。
- FIPS 模式狀態並未另存為備份的一部分。如果您將主機還原至 FIPS 模式尚未開啟的硬體裝置，還原後您必須手動將它開啟。
  當您進行還原後，最佳實務準則就是檢查 FIPS 模式的狀態，然後視需要變更。

請參閱第 611 頁的「從備份還原硬體裝置」。
請參閱第 767 頁的「開啟或關閉 FIPS 模式」。

- 在開啟 FIPS 模式後，下列動作會將 FIPS 模式變更回其預設設定 (關閉)：
  - 全新安裝 Symantec Messaging Gateway 軟體
  - 全新還原作業系統
  - 傳輸新的主機

在您安裝或升級 Symantec Messaging Gateway 前，請務必閱讀此版本隨附的「版本說明」。

如需有關如何首次安裝此版本或如何從舊版升級的特定詳細資訊，請參閱「*Symantec Messaging Gateway 安裝指南*」。

請務必注意下列資訊：

- 從本版開始，控管中心不再接受 SSLv2 或 SSLv3 HTTPS 連線。只接受 TLS 1.0 連線。
- 本版在開啟 FIPS 模式的情況下，下列動作所花費的時間明顯多於關閉 FIPS 模式的情況：
  - 重新啟動郵件傳輸代理程式 (MTA) 服務
  - 任何會導致 MTA 服務隱式重新啟動的配置更改

  主機可能看似無反應長達數分鐘，但並非如此。
  在您將主機部署到生產環境之前，將啟用 FIPS 模式作為您安裝程序的最終步驟，是避免發生上述情況的最佳實務準則。

關於控管中心的憑證信任

用於控管中心自行簽署憑證的簽章演算法與 FIPS 不相容。如需遵循 FIPS 140-2 第 1 級標準，您必須向憑證授權中心廠商申請與 FIPS 相容的憑證，再將該憑證匯入到控管中心。內含憑證的檔案必須為 PEM 格式。

請參閱第 145 頁的「關於憑證」。

請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。

FIPS 模式最佳實務準則與考量

以下描述使用 FIPS 模式的最佳實務準則與考量：

金鑰長度與 FIPS 遵循	Symantec Messaging Gateway 目前可讓您匯入短於 FIPS 140-2 第 1 層標準所允許金鑰長度下限的 TLS 金鑰與 HTTPS 金鑰。當您使用 SNMPv3 時，請確定使用的金鑰夠長，符合 FIPS 140-2 第 1 級標準。為符合 FIPS 140-2 第 1 級標準，管理員必須記得建立長度為 1024 位元或更長的金鑰。

關於 FIPS 模式與 SNMPv3	如果您使用 SNMPv3 並要以 FIPS 模式執行 Symantec Messaging Gateway，您必須架構控管中心使用 **SHA1withRSA** 驗證類型。 請參閱第 577 頁的「架構 SNMP 設定以監控網路裝置」。
關於 SMTP 授權	請注意，當 FIPS 模式開啟時，SMTP 授權的**「需要 TLS 加密」**選項不會如您預期般的運作。當關閉此選項時，Symantec Messaging Gateway 接受 TLS 和 SSLv3.0 連線。但是當 FIPS 模式開啟時，Symantec Messaging Gateway 支援並僅使用 TLS 加密，所有舊的加密模式會失敗。因此當 FIPS 模式開啟時，即使您已停用**「需要 TLS 加密」**選項，SSLv3.0 連線仍會失敗。 請參閱第 159 頁的「指派 MTA TLS 憑證給掃描程式」。

關於使用 FIPS 時，部分 Symantec Messaging Gateway 的功能限制

以下的 Symantec Messaging Gateway 功能在嚴格遵循 FIPS 140-2 第 1 級標準時無法運作：

遠端憑證儲存	Symantec Messaging Gateway 不使用 FIPS 相容的演算法加密以下實體的憑證： ■ LDAP 管理員密碼 ■ 一般使用者密碼 ■ 排程備份 臨機操作備份不受到影響，因為這些備份不使用儲存的憑證。
完全資料符合 (EDM) 與記錄資源管理	此限制目前沒有暫時性的解決方案。
Symantec Messaging Gateway 不使用 FIPS 相容的演算法儲存 EDM 或記錄資源。	此限制目前沒有暫時性的解決方案。
「垃圾郵件隔離所」發行憑證	Symantec Messaging Gateway 不使用 FIPS 相容的演算法將摘要電子郵件中用於存取一般使用者「垃圾郵件隔離所」的儲存憑證加密。能夠透過 FIPS 模式開啟的「垃圾郵件隔離所」通知核發郵件的使用者與管理員非嚴格的 FIPS 相容。 若要暫時解決這個問題，您可要求一般使用者直接登入隔離所以核發郵件。
使用 LDAPS 之 Domino 目錄伺服器的資料目錄服務連線	FIPS 模式開啟時，Symantec Messaging Gateway 資料目錄服務無法連線至架構為使用 LDAPS 的 Domino 目錄伺服器。 此限制發生的原因是因為在 FIPS 模式中，資料目錄服務僅使用 TLS 1.0。Symantec Messaging Gateway 支援的版本不支援 TLS 1.0。

示範憑證	用於示範控管中心使用者介面憑證的簽章演算法是 **SHA1withRSA**，這不是 FIPS 核准的演算法。為維護與 Windows XP SP2 或更舊版本上所執行之 Internet Explorer 瀏覽器的相容性，示範憑證未變更。 若要暫時解決此問題，您可以手動將使用 FIPS 核准演算法的憑證授權中心廠商憑證匯入到控管中心。 請參閱第 150 頁的「新增 CA 或中繼憑證」。 請參閱第 152 頁的「匯入憑證授權中心簽署的憑證」。

開啟或關閉 FIPS 模式

管理員必須個別登入每個硬體裝置，才能開啟或關閉硬體裝置上的 FIPS 模式。當您開啟或關閉每個主機上的 FIPS 模式後，變更模式只會影響掃描程式使用的加密清單。掃描程式的 FIPS 模式可進行架構，因為您無法控制外部郵件傳輸代理程式 (MTA) 使用的通訊協定與通訊版本。如果您在 FIPS 模式開啟的狀況下執行掃描程式，則部分透過外部 MTA 進行的通訊可能會中斷。

變更 FIPS 模式不會影響控管中心程序。Symantec Messaging Gateway 版本的控管中心一律以 FIPS 模式執行。無論 FIPS 模式為開啟或關閉，Symantec Messaging Gateway 產品架構保持不變。

每個硬體裝置 (實體或虛擬) 都有一組組態指令。您可以從使用 SSH 用戶端的遠端階段作業或從系統主控台來執行這些指令。Symantec Messaging Gateway 的 FIPS 模式只能從指令行實作。您無使用這個版本的控管中心管理 FIPS 模式。

附註：與 FIPS 模式相關的動作會記錄到 syslog 中，並出現在 /data/logs/messages 中。

請參閱第 627 頁的「透過指令行管理 Symantec Messaging Gateway」。

附註：變更 FIPS 模式時，請勿中斷指令。如果您接受提示重新啟動，但您在重新啟動前中斷指令，則 FIPS 模式的狀態不會改變。您未來無法變更 FIPS 模式。

開啟主機的 FIPS 模式

1. 使用您喜好的方法登入硬體裝置的指令行介面。
2. 輸入下列指令：

```
fipsmode on
```

關閉主機的 FIPS 模式

1 使用您喜好的方法登入硬體裝置的指令行介面。

2 輸入下列指令：

```
fipsmode off
```

若要確認 Symantec Messaging Gateway 符合 FIPS 140-2 第 1 級標準，您可以檢查以確認 FIPS 模式狀態為開啟。

檢查主機的 FIPS 模式狀態

1 使用您喜好的方法登入硬體裝置的指令行介面。

2 輸入下列指令：

```
fipsmode status
```

如果 FIPS 模式為開啟，則傳回的狀態為**「FIPS 模式」**。如果 FIPS 模式為關閉，則傳回的狀態為**「非 FIPS 模式」**。

附錄 F

適用於管理員的智慧卡驗證

本附錄包含以下主題：

- 關於適用於管理員的智慧卡驗證
- 在有 Internet 存取的情況下，對控制中心設定智慧卡驗證
- 在無 Internet 存取的情況下，對控制中心設定智慧卡驗證
- 匯入 CA 憑證或憑證撤銷清單
- 檢視 CA 憑證或憑證撤銷清單
- 刪除 CA 憑證或憑證撤銷清單
- 編輯管理員帳戶以啟用智慧卡驗證
- 使用智慧卡登入控制中心

關於適用於管理員的智慧卡驗證

美國聯邦機構現在使用允許智慧卡驗證的軟體系統。美國聯邦智慧卡包含為持卡人授予聯邦設施和資訊系統存取權限所需的資料。此存取權限可確保所有適用的聯邦應用程式具有適當的安全層級。

某些 Windows 用戶端電腦或工作站已具有內置於鍵盤中的 PIV 或 CAC 讀取裝置。其他人使用可使用 USB 纜線連線到工作站或筆記型電腦的智慧卡讀取裝置。Symantec Messaging Gateway 對使用以下類型智慧卡的管理員進行驗證：

- 個人身分驗證 (PIV) 卡 (適用於平民)
- 通用存取卡 (CAC) (適用於軍事人員)。

智慧卡驗證是一種以用戶端憑證為基礎的相互驗證，其中用於識別使用者的憑證位於智慧卡上。在與 Web 伺服器進行 SSL 信號交換期間，瀏覽器將取得憑證。在智慧卡驗證期間，瀏覽器會在控制中心的儲存中以及在插入的智慧卡上執行憑證查詢。

由於瀏覽器是智慧卡驗證的關鍵部分，因此不同瀏覽器的行為會影響管理員使用智慧卡登入時所執行的步驟。

以下為支援的瀏覽器：

- Internet Explorer 11 或更新版本。
- Chrome 70 或更新版本。
- Firefox 63 或更新版本。
  附註：若要將 Firefox 用於智慧卡驗證，您必須取得並安裝外掛程式以支援 PIV。請參閱 https://piv.idmanagement.gov/engineering/firefox/。

請參閱第 770 頁的「在有 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

請參閱第 771 頁的「在無 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

請參閱第 774 頁的「編輯管理員帳戶以啟用智慧卡驗證」。

請參閱第 774 頁的「使用智慧卡登入控制中心」。

在有 Internet 存取的情況下，對控制中心設定智慧卡驗證

您可以架構 Symantec Messaging Gateway 以驗證使用智慧卡登入控制中心的管理員。智慧卡用於為美國聯邦機構或美國軍事機構工作的管理員。透過智慧卡驗證，可以將該卡插入讀取裝置並提供 PIN 號碼。

對於連線到 Internet 的 Messaging Gateway 實例，您必須將 CA 根憑證和中間憑證新增到憑證儲存區。已連線的網路不需要憑證撤銷清單。

表 F-1　在有 Internet 存取的情況下，設定控制中心以進行智慧卡驗證

工作	說明
先決條件	針對您要設定的每個管理員取得智慧卡讀取裝置和智慧卡。 取得至少一個與內嵌於管理員智慧卡中的資料相符的 CA 根憑證和中間憑證。 請確保使用支援的瀏覽器 (Chrome、Internet Explorer 或 Firefox)。如果使用 Firefox，請下載並安裝支援 PIV 的外掛程式，網址為 https://piv.idmanagement.gov/engineering/firefox/。

工作	說明
步驟 1：匯入根/中間 CA 憑證。	首先，必須將至少一個根 CA 憑證和中間 CA 憑證 (如有必要) 匯入到 Messaging Gateway 的控制中心憑證儲存區。在管理員使用者登入期間，Tomcat 和控制中心使用此憑證來驗證智慧卡的憑證。 **附註：**您必須在匯入憑證後重新啟動控制中心。 請參閱第 772 頁的「匯入 CA 憑證或憑證撤銷清單」。
步驟 2：將智慧卡資訊新增到管理員帳戶。	更新每張智慧卡使用者的管理員帳戶，以包括上一步中所匯入憑證的相關資訊。 請參閱第 774 頁的「編輯管理員帳戶以啟用智慧卡驗證」。
步驟 3：使用智慧卡登入控制中心。	要求管理員登入以驗證智慧卡存取是否正常工作。 請參閱第 774 頁的「使用智慧卡登入控制中心」。

請參閱第 769 頁的「關於適用於管理員的智慧卡驗證」。

在無 Internet 存取的情況下，對控制中心設定智慧卡驗證

您可以架構 Symantec Messaging Gateway 以驗證使用智慧卡登入控制中心的管理員。智慧卡用於為美國聯邦機構或美國軍事機構工作的管理員。透過智慧卡驗證，可以將該卡插入讀取裝置並提供 PIN 號碼。

您必須匯入至少一個其通用名稱和組織值與內嵌於管理員智慧卡中的值相符的 CA 憑證。

對於未連線到 Internet 的 Messaging Gateway 實例，還必須匯入至少一個憑證撤銷清單 (CRL)。

警告：如果控制中心伺服器無 Internet 存取，則必須為控制中心架構至少一個 CRL，以便用於對使用者進行驗證。在智慧卡登入期間，控制中心將根據已匯入的任何 CRL 檢查內嵌於管理員智慧卡中的憑證。如果不存在任何 CRL，則已撤銷智慧卡的管理員仍可以登入，這可能會導致安全問題。

表 F-2 在無 Internet 存取的情況下，設定控制中心以進行智慧卡驗證

工作	說明
先決條件	針對您要設定的每個管理員使用者取得智慧卡讀取裝置和智慧卡。 取得至少一個與內嵌於管理員智慧卡中的資料相符的 CA 根憑證和中間憑證。 取得至少一個憑證撤銷清單，以對管理員使用者進行驗證。 請確保使用支援的瀏覽器 (Chrome、Internet Explorer 或 Firefox)。如果使用 Firefox，請下載並安裝支援 PIV 的外掛程式，網址為 https://piv.idmanagement.gov/engineering/firefox/。
步驟 1：匯入 CA 根憑證/中間憑證和憑證撤銷清單。	首先，必須將至少一個根 CA 憑證和中間 CA 憑證 (如有必要) 匯入到 Messaging Gateway 的控制中心憑證儲存區。 **附註：**您必須在匯入憑證後重新啟動控制中心。 對於未連線的網路，還必須將至少一個 CRL 匯入到 Messaging Gateway 的控制中心。此 CRL 用於在管理員使用者登入期間驗證智慧卡的憑證。 請參閱第 772 頁的「匯入 CA 憑證或憑證撤銷清單」。
步驟 2：將智慧卡資訊新增到管理員帳戶。	更新每張智慧卡使用者的管理員帳戶，以包括上一步中所匯入憑證的相關資訊。 請參閱第 774 頁的「編輯管理員帳戶以啟用智慧卡驗證」。
步驟 3：使用智慧卡登入 SMG 控制中心。	要求管理員登入以驗證智慧卡存取是否正常工作。 請參閱第 774 頁的「使用智慧卡登入控制中心」。

請參閱第 769 頁的「關於適用於管理員的智慧卡驗證」。

匯入 CA 憑證或憑證撤銷清單

請遵循以下步驟匯入未連線到 Internet 的網路的憑證和憑證撤銷清單 (CRL)。

請注意：

- 控制中心僅允許您以 `.pem` 格式匯入 CA 憑證，以 `.pem` 或 `.crl` 格式匯入憑證撤銷清單。如果 CA 憑證或 CRL 的格式不受支援，則可以使用 OpenSSL 程式庫對其進行轉換：https://www.openssl.org/。
- CA 根憑證或中間憑證必須與內嵌於管理員智慧卡中的憑證源自同一憑證授權中心。
- 一次只能匯入一個憑證。如果嘗試匯入單個檔案中組合的多個憑證，則匯入程序將失敗。
- 您必須在匯入 CA 根憑證或中間憑證後重新啟動控制中心，才能使憑證生效。若要重新啟動控制中心，請存取指令行介面並執行指令。
  僅針對 CA 根憑證/中間憑證需要重新啟動控制中心。您不需要在匯入 CRL 後執行重新啟動。

匯入 CA 根憑證、中間憑證或憑證撤銷清單

1 在控制中心內，瀏覽至**「管理員」>「設定」>「智慧卡」**。

2 在**「CA 憑證」**標籤或**「憑證撤銷清單」**標籤上，按下**「匯入」**。

此時將顯示**「匯入智慧卡 CA 憑證」**或**「匯入憑證撤銷清單」**對話方塊。

3 輸入憑證或 CRL 名稱，然後按下**「瀏覽」**以查找要匯入的憑證或 CRL 檔。

4 按下**「匯入」**。

5 [僅適用於 CA 根憑證/中間憑證；而 CRL 不需要] 您必須重新啟動控制中心，以便存取新匯入的憑證。若要重新啟動控制中心，請存取指令行介面並執行指令 `service controlcenter restart`。

請參閱第 769 頁的「關於適用於管理員的智慧卡驗證」。

請參閱第 770 頁的「在有 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

請參閱第 771 頁的「在無 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

檢視 CA 憑證或憑證撤銷清單

請遵循以下步驟檢視 CA 憑證或憑證撤銷清單 (CRL) 的內容。

檢視 CA 根憑證、中間憑證或憑證撤銷清單

1 在控制中心內，瀏覽至**「管理員」>「設定」>「智慧卡」**。

2 在**「CA 憑證」**標籤或**「憑證撤銷清單」**標籤上，勾選要檢視之憑證旁邊的方塊。

3 按下**「檢視」**。

當您檢視 CRL 時，會顯示 CRL 的全部內容。

4 檢視完憑證或 CRL 後，按下**「確定」**。

請參閱第 769 頁的「關於適用於管理員的智慧卡驗證」。

請參閱第 770 頁的「在有 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

請參閱第 771 頁的「在無 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

刪除 CA 憑證或憑證撤銷清單

請遵循以下步驟刪除 CA 憑證或憑證撤銷清單 (CRL)。

刪除 CA 根憑證、中間憑證或憑證撤銷清單

1 在控制中心內，瀏覽至**「管理員」>「設定」>「智慧卡」**。

2 按下**「CA 憑證」**或**「憑證撤銷清單」**標籤。

3 勾選要刪除之憑證旁邊的方塊。

4 按下「**刪除**」。

此時會顯示確認視窗。按下「**刪除**」。

5 [僅適用於 CA 根憑證/中間憑證；而 CRL 不需要] 您必須在刪除 CA 憑證後重新啟動控制中心。若要重新啟動控制中心，請存取指令行介面並執行指令 `service controlcenter restart`。

請參閱第 769 頁的「關於適用於管理員的智慧卡驗證」。

請參閱第 770 頁的「在有 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

請參閱第 771 頁的「在無 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

編輯管理員帳戶以啟用智慧卡驗證

您必須先更新 Messaging Gateway 管理員的帳戶，管理員才能使用智慧卡進行驗證。內嵌於管理員智慧卡中的憑證資訊必須與您上傳之憑證中包含的資料相符。

CA 根憑證或中間憑證必須與內嵌於管理員智慧卡中的憑證源自同一憑證授權中心。

編輯管理員帳戶以啟用智慧卡驗證

1 在控制中心內，瀏覽至「**管理**」>「**使用者**」>「**管理員**」，然後按下管理員的連結。

2 此時將顯示標記「**為此管理員啟用智慧卡驗證**」的核取方塊。

選取該核取方塊。此時將顯示兩個新欄位：「**通用名稱 (CN):**」和「**組織 (O):**」。

3 在「**通用名稱 (CN):**」欄位中，輸入與管理員智慧卡相符之憑證中顯示的「**通用名稱**」。

4 在「**組織 (O):**」欄位中，輸入與管理員智慧卡相符之憑證中顯示的「**組織**」。

這兩個欄位的內容必須與內嵌於管理員智慧卡中的憑證上的相應欄位**完全**相符。您可以檢視已上傳憑證的內容，以驗證您輸入的值是否正確。請參閱第 773 頁的「檢視 CA 憑證或憑證撤銷清單」。

5 按下「**儲存**」。

請參閱第 769 頁的「關於適用於管理員的智慧卡驗證」。

請參閱第 770 頁的「在有 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

請參閱第 771 頁的「在無 Internet 存取的情況下，對控制中心設定智慧卡驗證」。

使用智慧卡登入控制中心

開始之前，請將您的智慧卡讀取裝置連線到系統，然後將智慧卡插入讀取裝置。此外，請記下列印在卡背面的智慧卡 PIN。需要使用此 PIN 才能登入控制中心。

以下為支援的瀏覽器：

- Internet Explorer 11 或更新版本。

- Chrome 70 或更新版本。
- Firefox 63 或更新版本。
  附註：若要將 Firefox 用於智慧卡驗證，您必須取得並安裝外掛程式以支援 PIV。請參閱 https://piv.idmanagement.gov/engineering/firefox/。

使用智慧卡登入控制中心

1. 將智慧卡讀取裝置插入系統，然後將您的卡插入讀取裝置。
2. 輸入 Symantec Messaging Gateway 的 URL。

   此時將顯示**「選取憑證」**對話方塊。
3. 選取與您的使用者名稱配對的憑證，然後按下**「確定」**。
4. 此時將顯示**「Windows 安全智慧卡」**對話方塊，並提示**「請輸入您的 PIN」**。
5. 輸入列印在智慧卡背面的 PIN，然後按下**「確定」**。
6. 此時將顯示 Messaging Gateway 登入畫面。
7. 輸入您的使用者名稱。
8. 按下**「選項 > >」**選項以顯示**「使用智慧卡登入」**核取方塊，然後勾選該方塊。此時**「密碼」**欄位處於隱藏狀態。
9. 按下**「登入」**選項。此時將顯示管理員已授權您檢視的 Messaging Gateway 使用者介面部分。

請參閱第 769 頁的「關於適用於管理員的智慧卡驗證」。

小辭彙

Brightmail 引擎	Symantec Messaging Gateway 元件可依據您架構的政策，針對惡意軟體、垃圾郵件和內容過濾來掃描電子郵件和附件，以及檔案傳輸。
CA (憑證授權中心)	發行用於建立數位簽章和公開/私密金鑰組之數位憑證的受信任第三方組織或公司。在此程序中，CA 的角色是保證授權唯一憑證的實體身份和其宣告的身份一致。這意味著 CA 通常和要求實體之間有協議，從而可確認宣告的身份。CA 是資料安全和電子商務中重要的元件，因為 CA 保證了交換資訊的雙方身份和其宣告的身份一致。
CIDR (無類別網域間繞送選擇)	一種使用任意位元數指定位址範圍的方法。例如，CIDR 指定 206.13.1.48/25，即表示將位址前 25 個位元符合 206.13.1.48 前 25 個位元的位址納入其中。
DDS (目錄資料服務)	使用 Symantec Messaging Gateway 服務可以將輕量型目錄存取通訊協定 (LDAP) 目錄中的資訊，用於 Symantec Messaging Gateway 中的功能。
DKIM (Domain Key Identified Mail)	使用公開金鑰加密法的通訊協定，可讓傳送的 MTA 透過收件者 MTA 可驗證的電子方式簽署合法電子郵件。另請參閱「MTA (郵件傳輸代理程式)」。
DNS (網域名稱伺服器) 代理	工作站使用者和網際網路之間的媒介，使企業可確保安全性和管理控制。
DNS (網域名稱系統)	主機命名的階層系統，可對 TCP/IP 主機進行分類。例如，在網際網路命名結構中，名稱中具有 com 副檔名標識的主機在商業類別中。
DNS 伺服器	用於特定網際網路主機之位址資訊的儲存庫。使用網域名稱系統 (DNS) 對伺服器進行命名，從而將 IP 位址和網際網路主機對應。
FIPS (聯邦資訊處理標準)	美國國家標準與技術局 (NIST) 標準，其中概述安全設計需求與加密模組實作。
IP (Internet 通訊協定)	將 Internet 上某一台電腦中的資料傳送到其他電腦所用的方法或通訊協定。Internet 上各台電腦 (也就是主機) 都有至少一個位址，可向 Internet 上的所有其他電腦顯示其唯一的身分。
IP 位址	可用來識別 TCP/IP 網路上的工作站並指定繞送資訊的唯一號碼。網路上的各個工作站，都必須被指派一個唯一的 IP 位址。此唯一 IP 位址是由網路 ID 加上網路管理員指派的唯一主機 ID 所組成。此位址通常是以小數點與十進位方式表示，而當中的十進位值則是以逗號分隔 (例如，123.45.6.24)。
LDAP (輕量型目錄存取通訊協定)	可讓任何使用者定位組織、個人與其他資源 (例如，檔案和裝置) 的軟體通訊協定。這些資源可以是位於 Internet 的資源，或是位於企業 Intranet 內部的資源。LDAP 是輕量型版本的目錄存取通訊協定 (DAP)，它是網路中目錄服務標準 X.500 中的一部分。

MIME (多用途網際網路郵件延伸) 用於透過網際網路傳輸不同格式之文件的通訊協定。

MTA(郵件傳輸代理程式) 在使用 SMTP 的伺服器之間接收和傳送郵件的程式 (例如 Sendmail、postfix 或 qmail) 的通稱。在每個 Symantec Messaging Gateway 掃描程式中的 MTA 會將入埠郵件與離埠郵件繞送到 Brightmail 引擎來進行處理。然後 MTA 會將過濾的郵件傳送到其內部目的地或是遠端目的地。

SMTP (簡易郵件傳輸通訊協定) 允許電子郵件在郵件伺服器之間交換的通訊協定。然後，用戶端才能收到電子郵件，而且通常是透過 POP 通訊協定或 IMAP 通訊協定。

SPF (寄件者政策架構) 用於驗證電子郵件的一組標準實作。如果寄件者的網域擁有者出現在 SPF 中，收件者的 MTA 就可以檢查是否有偽造的退回位址。Symantec Messaging Gateway 可讓您針對無法通過 SPF 驗證的郵件指定要採取的動作。

SSH (安全殼) 允許使用者使用加密透過網路安全地登入其他電腦的程式。SSH 可避免第三方干擾或甚至存取網路上傳送的資訊。

SSL (安全通訊端層) 允許用戶端與伺服器彼此之間進行相互驗證的通訊協定。此通訊協定允許建立已驗證且加密的連線，進而確保在 Internet 上安全地傳送資訊。另請參閱 TLS。

Symantec Network Prevent Symantec Data Loss Prevention 的元件，可以搜尋、監控和保護機密資料 (無論機密資料在何處儲存或使用)。Symantec Messaging Gateway 整合 Symantec Network Prevent 後，可傳送、繞送、保留或攔截電子郵件流量。

TLS (傳輸層安全) 使用連線專屬的金鑰與郵件完整性檢查的對稱加密法，提供 Internet 通訊隱密性的通訊協定。TLS 提供了比 SSL 更好的安全性、可靠性、互通性與擴充性。另請參閱 SSL。

下游 電子郵件流中處於靠後的時間。下游電子郵件伺服器是接收郵件的時間上比其他伺服器稍後的電子郵件伺服器。在多伺服器系統中，入埠郵件的傳遞路徑為從上游電子郵件伺服器到下游郵件伺服器。下游也可以指其他類型的網路路徑或技術。

主機 1. 在網路環境中，為其他電腦提供資料和服務的電腦。服務可能包括週邊裝置，如印表機、資料儲存、電子郵件或 Web 存取。2. 在遠端控制環境中，遠端使用者連接到用於存取或交換資料的電腦。

事件 違反政策條件的郵件。事件的相關資訊可幫助您瞭解、避免、回應及稽核可能的違規情況。在 Symantec Messaging Gateway 中，惡意軟體事件會儲存在「可疑病毒隔離所」，而垃圾郵件事件會儲存在「垃圾郵件隔離所」。內容過濾事件會儲存在「隔離事件」資料夾或「資訊事件」資料夾中。

另請參閱「可疑病毒隔離所」、「垃圾郵件隔離所」、「隔離所事件」和「資訊事件」。

代理伺服器 代表一個或多個其他伺服器的伺服器，通常用於掃描、防火牆或擷取資料，或者是這些目的之綜合。也叫做閘道。通常代理伺服器在公司或企業的內部使用，用來收集所有的網際網路要求，將其轉寄到網際網路伺服器，然後接收回復，並在公司內再將其轉寄到原始申請者。

代理程式 此元件可促進控管中心與各掃描程式之間的組態資訊傳遞。

傳輸引擎 會對郵件執行動作的 Symantec Messaging Gateway 掃描程式元件。

允許的寄件者 您想要接受其電子郵件的寄件者。允許的寄件者是下列其中至少一個群組的成員：「本機允許的寄件者網域」、「本機允許的寄件者 IP」、「允許的第三方寄件者」或「賽門鐵克全域允許的寄件者」。

允許的第三方寄件者 Symantec Messaging Gateway 中的寄件者群組，可讓管理員新增多個由第三方服務編譯的「允許的寄件者」清單。

內容過濾 一組功能，可讓管理員實行企業的電子郵件政策、降低法律負擔，並確保符合法規要求。

加密的附件 已轉換為未授權使用者無法輕易破解之格式的郵件附件。Symantec Messaging Gateway 並不會掃描加密的附件，但可讓您選擇在偵測到加密附件時所要採取的動作。

可疑 URL 內容 包含可濫發垃圾郵件或惡意軟體酬載之 URL 的電子郵件訊息。可疑 URL 包括免費託管網站、URL 縮短服務，以及 URL 重新導向服務。Symantec Messaging Gateway 可以過濾內含一或多個可疑 URL 的電子郵件。

可疑垃圾郵件 Symantec Messaging Gateway 根據特徵比對和誘導式分析所得的分數，認為可能是垃圾郵件的郵件。透過政策，您可以指定對識別為可疑垃圾郵件的郵件所採取的不同動作。請參閱「垃圾郵件」。

可疑病毒隔離所 暫時保存可能包含惡意軟體之郵件的檔案目錄。含有可疑附件的郵件可以保留在可疑病毒隔離所中長達數小時，然後利用新的過濾器 (如果有的話) 重新過濾。這項處理延遲功能可以讓 Symantec Messaging Gateway 在新病毒威脅出現時更有效地進行處理。

可疑附件 經 Symantec Messaging Gateway 判斷為含有惡意軟體的郵件附件。您可以選擇在偵測到可疑附件時所要採取的動作。

名稱伺服器 請參閱 DNS (網域名稱伺服器) 代理伺服器。

啟發式 可以主動攻擊常見樣式的垃圾郵件和病毒的過濾器。

垃圾郵件 1. 未經請求的商業性大量電子郵件。2. 經 Symantec Messaging Gateway 使用過濾器識別為垃圾郵件的電子郵件。

垃圾郵件評分 為郵件評分的程序。Symantec Messaging Gateway 會指定垃圾郵件評分給各封郵件，說明該封郵件是垃圾郵件的可能性。另請參閱「可疑的垃圾郵件」。

垃圾郵件隔離所 儲存電子郵件的檔案目錄 (與一般郵件流量分開)，並允許存取這些郵件。在 Symantec Messaging Gateway 中，「垃圾郵件隔離所」位於控管中心電腦上，可讓使用者以 Web 存取其垃圾郵件。使用者可以瀏覽、搜尋並刪除他們的垃圾郵件，並將識別錯誤的郵件重新傳送到他們的收件匣。管理員帳號可以存取所有隔離的郵件。「垃圾郵件隔離所」可以架構為僅限管理員存取。

子網路遮罩

使用部分未指定的位元來指定區域網路位址，用來將指定的網路位址細分為其他的子網路。子網路遮罩可藉由辨識本機主機網路來達成繞送。子網路遮罩是 IP 主機上必要的組態參數。

指定 IP 位址中哪些位元可指定特定的 IP 網路或子網路中之主機的本機位元遮罩 (一組旗標)。用來「遮罩」IP 位址中的一部分，讓 TCP/IP 可以判斷任何特定的 IP 位址是位於區域網路或遠端網路上。架構有 TCP/IP 的各台電腦都必須定義子網路遮罩。

定義檔

包含用於偵測及去除風險 (例如，惡意軟體和廣告程式) 之必要資訊的內容。定義檔也可用於偵測不必要的電子郵件，例如垃圾郵件。

寄件者 ID

用於驗證電子郵件的一組標準實作。如果寄件者的網域擁有者出現在寄件者 ID 中，收件者的 MTA 就可以檢查是否有偽造的退回位址。Symantec Messaging Gateway 可讓您針對無法通過「寄件者 ID」驗證的郵件指定要採取的動作。

寄件者群組

一種電子郵件寄件者類別，由 Symantec Messaging Gateway 利用 Brightmail 適應性信譽管理 (Brightmail ARM) 功能來管理。寄件者群組的分類可以依據 IP 位址、網域、第三方清單或賽門鐵克清單。您可以架構 Brightmail ARM 對來自各寄件者群組的郵件採取各種動作。

封包

當通訊協定將在網際網路或其他網路中傳送的訊息拆分時形成的資料單位。訊息被拆分成標準大小的封包，從而避免具有大量資料的重載傳輸行。每個封包都將單獨編號並包含目的地的網際網路地址。到達收件者電腦時，通訊協定會將封包重組成原始訊息。

封存

可針對電子郵件執行的動作，郵件會轉寄到特定 SMTP 位址進行長期儲存。

廣播位址

用來將郵件導向 (廣播) 至網路上所有系統的通用位址。廣播位址是以網路位址與子網路遮罩為基礎。

延遲

接收電子郵件的 MTA 所能採取的動作。此動作包括使用 4xx SMTP 回應碼來告知傳送的 MTA 於稍後重新嘗試。

快速通過

Symantec Messaging Gateway 的一項功能，可讓已驗證之「允許的寄件者」所發出的大多數電子郵件均可略過垃圾郵件過濾。「快速通過」可讓具有不傳送垃圾郵件之示範記錄的寄件者，暫時豁免於垃圾郵件掃描之外，藉而節省資源。「快速通過」會減少來自合法來源之郵件所需的處理時間。

惡意軟體

以實施危害為目的而建立的程式和檔案。惡意軟體包括電腦病毒、病蟲及特洛伊木馬程式。

憑證

被密碼編譯系統用作身份證明的檔案。它包含使用者名稱和公開金鑰。

憑證授權中心簽署的 SSL

一種透過憑證授權中心數位簽署的憑證來提供驗證和資料加密的安全通訊端層 (SSL)。

拒絕

接收電子郵件的 MTA 所能採取的動作。此動作包括使用 5xx SMTP 回應碼來告知傳送的 MTA 郵件未被接受。

掃描程式 負責過濾郵件的 Symantec Messaging Gateway 元件。每個網站可以有一或多個掃描程式。可透過控管中心管理各掃描程式的組態。

探查帳戶 無效的電子郵件地址，用來引誘垃圾郵件。您可建立探查帳戶，並透過控管中心將該帳戶新增到 Symantec Probe Network。

探查網路 賽門鐵克的探查網路合作夥伴所提供的電子郵件帳戶網路。賽門鐵克安全機制應變中心可利用探查網路來偵測垃圾郵件，它保有超過 3 億個電子郵件地址的統計數據，並包含 2 百萬個以上的探查帳戶。

探查網路合作夥伴 參與探查網路的 ISP 或公司。

控管中心 網頁式的組態及管理中心。每個網站都有各自的控管中心。控管中心同時附有「垃圾郵件隔離所」以及支援的軟體。您可以從控管中心內架構並監控所有的掃描程式。

提交者 ID 指派給控管中心的 ID，必須在將郵件提交至賽門鐵克以建立自訂垃圾郵件規則時使用。自訂垃圾郵件規則會套用至具有該 ID 之任何控管中心所控制的掃描程式。請參閱「垃圾郵件」。

攔截的寄件者 您不想接受其電子郵件的寄件者。攔截的寄件者是下列其中至少一個群組的成員：「本機攔截的寄件者網域」、「本機攔截的寄件者 IP」、「攔截的第三方寄件者」或「賽門鐵克全域攔截的寄件者」。

攔截的第三方寄件者 Symantec Messaging Gateway 中的寄件者群組，可讓管理員新增多個由第三方服務編譯的「攔截的寄件者」清單。

政策 Symantec Messaging Gateway 對郵件或郵件組執行的一組郵件過濾指示。另請參閱「過濾器政策」、「政策群組」。

政策群組 在 Symantec Messaging Gateway 中，可對其套用一組獨特過濾政策的使用者群組。您可依電子郵件地址或網域來指定使用者。另請參閱「過濾器政策」。

本機允許的寄件者 IP 依預設允許且略過垃圾郵件過濾的寄件者 IP 位址。在控管中心內，指定「本機允許的寄件者 IP」。

本機允許的寄件者網域 依預設允許且略過垃圾郵件過濾的寄件者網域位址。在控管中心內，指定「本機允許的寄件者網域」。

本機攔截的寄件者 IP 您不想接受其郵件的寄件者 IP 位址。在控管中心內，指定「本機攔截的寄件者 IP」。

本機攔截的寄件者網域 您不想接受其郵件的寄件者網域。在控管中心內，指定「本機攔截的寄件者網域」。

清除 包括刪除不可修復的病毒感染，並修復可修復的病毒感染之動作。

清除程式 「垃圾郵件隔離所」和內容過濾隔離事件的元件，位於 Symantec Messaging Gateway 的控管中心電腦中。清除程式可架構為定期移除「垃圾郵件隔離所」或內容過濾事件資料夾中較舊或不必要的郵件或事件。

無法掃描 在 Symantec Messaging Gateway 中，會因多種原因無法對郵件掃描病毒。例如，無法掃描的檔案超出了所架構的最大檔案大小或最大掃描深度，複合郵件，例如包

含許多層次的壓縮檔案，就可能會超出掃描深度上限。您可以架構無法掃描之郵件的處理方式。

特徵 1. 一種活動的狀態或樣式，指出違反政策、容易遭到攻擊的狀態，或與入侵相關的活動。2. 產品中偵測政策違反、容易遭到攻擊的狀態，或與入侵相關的活動之邏輯。此一詞彙亦指特徵定義、運算式、規則、觸發程式或特徵邏輯。3. 關於特徵的資訊包括屬性與說明文字。更明確來說，此一詞彙代表的就是特徵資料。

病毒 一段插入至其他程式的程式碼，可造成許多意外的事件，對於受害者而言，通常是令人不快的事件。病毒可以透過從其他站點上下載程式或存在於磁片上從而進行傳輸。對於下載檔案的來源或者接收的磁片，您通常不會意識到會存在病毒。在出現電腦執行其程式碼的情況之前，病毒一直處於休眠狀態。有些病毒沒有惡意，也不會造成危害，但是有些病毒可能會造成危害，會清除資料或使您的硬碟需要重新格式化。

病蟲 一種特殊的病毒。這種病毒與傳統的病毒不同，不會將自己附加在其他程式中，而是複製自己的複本，並進而產生更多的複本。

目錄資料來源 包含主機連線參數和針對該來源啟用的功能組之組態資料集。

目錄資料來源功能 可啟用 Symantec Messaging Gateway 特定功能的 LDAP 查詢組態。Symantec Messaging Gateway 提供四種目錄資料來源功能：驗證、位址解析、繞送及收件者驗證。

真實檔案類型辨識 用來辨識檔案真正類型的一項技術，不論其副檔名是否符合其類型。在 Symantec Messaging Gateway 中，您可以依據檔案的真實檔案類型或真實檔案類別來指定過濾動作，也可以依據檔案名稱或副檔名來進行過濾。

稽核 ID 在所有經過處理的郵件中，包含在郵件標頭內的唯一識別碼。

管道 透過安全的 HTTPS 檔案傳輸，從賽門鐵克安全機制應變中心擷取全新和更新過濾器的元件。擷取過濾器之後，管道會驗證過濾器，然後警示 Brightmail 引擎接收並且實作新的過濾器。最後，「管道」還可管理可供賽門鐵克安全機制應變中心使用與產生報告的統計數據。

網路釣魚 藉由傳送看似來自知名且值得信賴之公司的郵件，嘗試非法收集個人與財務資訊。網路釣魚郵件通常包含至少一個連到假網站的連結，這些假網站假冒合法的企業網站。這些網站會誘使收件者提供可用於身分竊取或線上財務資訊竊取的資訊。

行銷郵件 內含使用者要求接收的商業性或籌款訊息的電子郵件。這些郵件通常不提供選擇退出功能。

複寫 在 Symantec Messaging Gateway 中，將控管中心的組態資料複製到掃描程式中的程序。

註釋 放置在電子郵件內文開頭處或結尾處的片語或段落。您最多可指定 1000 種不同的註釋，並用於特定收件者政策群組的特定種類的郵件上。您可以使用此功能來自動產生電子郵件免責聲明。

語言識別 在 Symantec Messaging Gateway 中，這項功能可讓您攔截或允許以指定語言撰寫的郵件。例如，您可以選擇僅允許英文郵件，或是攔截英文與西班牙文的郵件並允

許所有其他語言的郵件。管理員可以設定使用者群組的語言識別，或允許使用者指定他們自己的設定值。

誤報

合法的電子郵件，但 Symantec Messaging Gateway 卻誤認為垃圾郵件並歸類為垃圾郵件。

資料來源

(1) 包含主機連線參數和針對該來源啟用的功能組之組態資料集。

(2) 您的資料庫管理員所提供，其中包含公司特定分隔資料欄的檔案。資料來源包含您想要保護，但無法透過規則運算式或關鍵字識別的客戶、病患或其他資料。例如，您可以使用資料來源檔案建立內容過濾政策，來過濾離埠電子郵件中敏感的客戶或員工資料。

資訊事件

其中包含因內容過濾政策違規動作是**「建立資訊事件」**而建立之事件的資料夾。

賽門鐵克全域允許的寄件者

賽門鐵克根據其保護的郵件伺服器中的全域合法寄件者資料，所收集的 IP 位址的清單。Symantec Messaging Gateway 中的其中一個寄件者群組。

賽門鐵克全域攔截的寄件者

賽門鐵克根據其保護的郵件伺服器中的全域垃圾郵件資料，所收集的 IP 位址的清單。Symantec Messaging Gateway 中的其中一個寄件者群組。

賽門鐵克安全機制應變中心

賽門鐵克安全機制應變中心是由一些有奉獻精神的入侵專家、安全工程師、病毒獵人、威脅分析師所組成的團隊。他們是全球技術支援團隊，經由團隊的通力合作，可以為企業與消費者提供更完善的保護範圍。賽門鐵克安全機制應變中心也利用精密的威脅與早期警告系統，為客戶提供全面且全球皆可享有的全天候 Internet 安全專業知識。這些安全專業知識可主動預防當今的混合型 Internet 威脅與複雜的安全風險。

安全機制應變中心服務範圍涵蓋了所有的安全問題，可提供客戶以下領域的完善防護：

· 病毒、惡意軟體、病蟲、特洛伊木馬程式、Bot 傀儡程式與其他的惡意程式碼

· 駭客

· 漏洞

· 間諜程式、廣告程式與撥號程式

· 垃圾郵件

· 網路釣魚以及其他形式的 Internet 詐騙

安全機制應變中心利用其全球的智慧型網路並洞燭先機，預測出新一代的威脅，讓賽門鐵克與客戶提早防範攻擊者入侵。此團隊會提供一年兩次的 Internet 安全威脅研究報告，指出整個安全社群中的重要趨勢與統計數據，讓賽門鐵克在這個瞬息萬變的產業中保持在最前線。

隨著當今威脅變的越來越精密，擁有一個完善的數位資產防衛機制就是抵抗駭客最好的辦法。賽門鐵克安全機制應變中心有一個統一團隊可處理各種安全問題，提供給客戶完全整合的防護，同時結合了上百位安全專家的專業知識，為賽門鐵克的所有產品與服務提供更新及安全情報。賽門鐵克在全球都設立有研究與回應中心。

辭典 用來檢查電子郵件是否有不相符內容的文字與片語清單。Symantec Messaging Gateway 可讓您建立根據特定辭典來過濾電子郵件的內容過濾政策。您可以使用所提供的辭典、在提供的辭典中新增詞彙，或新增額外的辭典。

退回 郵件伺服器可針對電子郵件執行的動作。此動作會使用自訂回應將郵件退回其 From: 地址。

退回攻擊防護 Symantec Messaging Gateway 的功能，可去除因轉向而產生的退回郵件，同時仍允許合法退回郵件的通知。

通訊協定 一套用於編碼和解碼資料的規則，從而使訊息可以在電腦之間進行交換，且每個電腦都能完全理解訊息的意義。在網際網路上，稱為 TCP/IP 的通訊協定組件實現了不同電腦之間的資訊交換。通訊協定可以堆疊，這意味著一次傳輸可以使用兩個或多個通訊協定。例如，FTP 會話使用 FTP 通訊協定來傳輸檔案，TCP 通訊協定用來管理連線，而 IP 通訊協定用來傳遞資料。

通訊埠 1. 用來將資料傳入運算裝置並從中傳出的硬體位置。個人電腦具有不同類型的通訊埠，包括用於連線磁碟機、監視器和鍵盤的內部通訊埠，以及用於連線數據機、印表機、滑鼠裝置和其他周邊裝置的外部通訊埠。2. 在TCP/IP 和 UDP 網路中，邏輯連線的端點名稱。通訊埠號用於識別通訊埠的類型。例如，TCP 和 UDP 都使用通訊埠 80 來傳輸 HTTP 資料。

過濾器 分析電子郵件的方法，用來確定每個郵件上要執行的動作。Symantec Mail Security 使用多種過濾器來處理郵件。過濾器可由賽門鐵克提供，由本機管理員或一般使用者建立，或者由第三方提供。

過濾器政策 在 Symantec Messaging Gateway 中，套用至某一郵件類別的一組動作。過濾器政策中指定的動作會套用至包含過濾器政策之政策群組的成員使用者身上。Symantec Messaging Gateway 使用下列過濾器政策類型：垃圾郵件、惡意軟體和內容過濾政策。過濾器政策也可以利用政策資源。另請參閱「政策群組」、「政策資源」。

郵件閘道 郵件伺服器所在的網路最外部點。所有其他的郵件伺服器都是郵件閘道上郵件伺服器的下游郵件伺服器。

間諜程式 會秘密地監控系統活動及偵測密碼與其他機密資訊，並將這些資訊轉遞給其他電腦的獨立程式。

閘道 用作其他網路入口的網路點。閘道也可以是在網際網路傳輸期間將封包從一個網路傳遞到其他網路的任何電腦或服務。

防火牆 保護某一網路資源免於被其他網路使用者存取的程式。一般來說，擁有 Intranet、可讓員工存取 Internet 的企業，需要防火牆來防止外部人員存取其私有的資料資源。

附件清單 用於過濾的附件類型清單。您可以依據檔案命名 (例如，依據副檔名) 和各檔案真實類型建立附件清單。或者，您也可以使用預先輸入的清單。

電子報 已知定期 (通常每週或每月) 寄送，內含特定主題內容的電子郵件。使用者可能已要求接收這些出版品。通常會提供選擇退出功能。

電子郵件地址搜尋攻擊 垃圾郵件寄發者用以確定有效電子郵件地址的一種手法。垃圾郵件寄發者將大量的可能電子郵件地址傳送至網站時，會發生電子郵件地址搜尋攻擊。未防護的郵件伺

服器會拒絕傳送到無效地址的郵件。透過此行為，垃圾郵件寄發者可以藉由根據原始清單檢查遭拒絕的郵件，從而瞭解有效的電子郵件地址。

電子郵件病毒攻擊 一系列來自特定網域感染病毒的電子郵件。Symantec Messaging Gateway 可讓您選擇要對這些郵件採取的動作。

驗證 確定嘗試存取網路之使用者身分的程序。透過挑戰/回應、基於時間的程式碼序列或其他技術進行驗證。驗證通常包括密碼的使用、憑證、PIN 或其他可用來驗證電腦網路上的身份之資訊。

索引

符號

8-bit MIME 581

A

agent-config 指令 634, 717

B

Brightmail
- ARM (適應性信譽管理) 122
- IQ 服務 122
- 引擎
  - 啟用, 停用 63, 522
  - 關於 64

C

CA (憑證授權中心) 憑證, *請參閱* 憑證
cat 指令 636
cc-config 指令 637
clear 指令 640

D

Data Loss Prevention
- Network Prevent, *請參閱* Data Loss Prevention Network Prevent 整合
- 與 Symantec Messaging Gateway 整合 403
- 關於 403

Data Loss Prevention Network Prevent 整合 406
- *另見* 內容過濾
- TLS 加密 417
- 反映 410
- 多個掃描程式 408
- 架構 412, 417
- 重新導向郵件 409
- 效能 414
- 略過模式 410, 412
- 通訊埠 407–408, 417
- 喜好設定 415
- 郵件佇列 410
- 疑難排解 410, 414, 416
- 維護 420
- 標籤, 郵件 409
- 轉寄 410
- 關於 406
- 攔截郵件 409

db-backup 指令 641
db-restore 指令 645
DBCS 580
delete 指令 647
Dell Remote Access Controller (DRAC) 761, *請參閱* DRAC
diagnostics 620, 760
diagnostics 指令 652
DKIM
- 啟用 DKIM 簽署 106
- 匯入網域金鑰 109
- 新增網域金鑰 109

dns-control 指令 656
DRAC 756
- 安裝 759
- 安裝影像 760
- 刪除 761
- 架構 759
- 重新啟動
  - 強制 758
  - 正常 758
- 檢視診斷 760
- 還原 761

E

Enforce Server
- 同步於 388
- 架構驗證 388
- 整合 403
- 關於 403

F

FIPS
- 安裝或升級 764
- 指令行 658
- 限制 766
- 最佳實務準則 765

開啟與關閉 767
認證的加密模組 763
憑證 765
檢查狀態 767
關於 763
fipsmode 指令 658

G

Global Intelligence Network 122
grep 指令 659

H

help
使用者登入說明 584
help 指令 660
HTTPS
使用者介面憑證 145, 160, 579–580
控管中心 160

I

ifconfig 指令 666
iostat 指令 667
IP 位址
IPv4 35
IPv6 30, 36
架構 35–36
為寄件者群組指定 118
研究信譽 140
變更控管中心 IP 位址 62
ip 指令 668
IP 連線報告 498
IPv4, *請參閱* IP 位址
IPv6, *請參閱* IP 位址

L

LAN 主機 201
LDAP 240
另見 垃圾郵件隔離所
郵件管理員信箱 251
LDAP 伺服器組態, 編輯 461
ldapsearch 指令 669
list 指令 670
LiveUpdate
service
停用 522
啟用 522
來源 201
排程 200
啟動, 停止 63
視需要 201
關於 64, 198

M

MAL, *請參閱* 郵件稽核日誌
mallog 指令 672
malquery 指令 674
monitor 指令 679
more 指令 685
MTA
TLS 憑證 145, 159
作業 63
停止 63, 522, 553
啟動 63, 522, 553
郵件佇列行為 65
管理 65
檢視服務狀態 522
關於 64
mta-control 指令 686

N

netstat 指令 692
nslookup 622
nslookup 指令 693

P

password 指令 694
patch 指令 695
PEM, 格式需求 157
Perl 相容規則運算式 354–355
ping 622
ping 指令 697
ping6 指令 698

R

reboot 指令 699
route 指令 700
rpmdb 指令 701
rsa-金鑰
指令行 702
rsa-金鑰指令 702

S

service 指令 703
show 指令 706
shutdown 指令 707

SMTP
入埠掃描程式設定
傳送 43
架構 41
關於 39
限制接受 42
主機設定 595
進階設定
傳送 52
傳送繫結 54
入埠 49
架構 48
離埠 50
郵件佇列 550
郵件稽核日誌 543
錯誤郵件處理 48
離埠掃描程式設定
傳送 46
架構 44
關於 39
離埠郵件接收 45
驗證 96
SMTP 驗證
建立資料來源 431
架構 90, 93
查詢
修改 463
建立自訂 444
最佳實務準則 96
編輯資料來源 463
總覽 90
關於 89
SNMP 577
sshd-config 指令 708
SSL 487
Symantec Content Encryption, *請參閱* 內容加密
Symantec Mail Security, *請參閱* Symantec Messaging Gateway
Symantec Messaging Gateway 22, 759
另見 DRAC
另見 最佳實務準則
FIPS 遵循 763
日誌 525
功能 23
更新軟體 616
狀態 515
保持在最新狀態 613
架構 25
重新授權 615
偵測病毒的方式 177
授權 614–615
產品文件 27
軟體
更新 619
版本 619
資訊, 取得位置 27
疑難排解 621
與 Enforce Server 整合 403
關於 22
Symantec Network Prevent 整合
政策 413, 419
架構 417, 419
略過模式 411, 413
通訊埠 417
郵件佇列 411
疑難排解 411
Symantec Probe Network 268
symdiag 指令 711
syslog, *請參閱* 日誌, syslog

T

tail 指令 620, 712
telnet 指令 715
TLS 加密
入埠掃描程式設定 41
依非本機網域指定 71
依據網域繞送, 傳送 70
強制執行於入埠 71
最佳實務準則, SMTP 驗證 96
離埠掃描程式設定 44
TLS 憑證 145, 158–159
traceroute 622
traceroute 指令 716

U

update
指令 718
UPS 監控 601
URI (統一資源識別元) 225
URL 信譽過濾 225

Z

zip 炸彈, *請參閱* 配置區限制

一劃

一般使用者設定
架構 173

啟用, 停用 173
需求 174
乙太網路設定
位址
IPv4 35
IPv6 36
進階 37

二劃

人工智慧 (靜態和動態) 177
人工智慧設定 177, 202
入埠 SMTP 設定
限制接受 42
傳送 43
關於 39
變更 41

三劃

大量郵件病蟲 176
已排程工作
控管中心內的位置 556
設定已排程工作失敗警示 556, 595
監控 555
檢視狀態 556

四劃

不必要的電子郵件
定義 221
減少誤報 220
過濾 213
允許的寄件者清單, *請參閱* 允許的寄件者群組
允許的寄件者群組
一般使用者清單 173
刪除寄件者 114
使用的原因 131
寄件者識別方法 118
啟用, 停用
成員 114
群組 111
連線類別的影響 124
匯入資料 115
匯入檔案格式 116
匯出資料 117
新增成員 113
編輯成員 114
選擇動作 112
總覽 130
關於 122
內容事件資料夾, *請參閱* 內容過濾
內容加密
設定 385
關於 385
內容過濾 280, 406
另見 Data Loss Prevention Network Prevent 整合
另見 條件
Perl 相容規則運算式 354–355
內容事件資料夾
保留供檢閱 (內容隔離所) 359
刪除 364
垃圾郵件選項 365
建立 361
提交違規垃圾郵件 380
檢視內容 371
清除 360, 365
監控 366
相符文字 384
管理 358, 366
編輯 364
資訊事件 359
關於 359
多重政策 298
事件
使用 Symantec Network Prevent 標頭標記來建立 419
刪除 379
匯出 378
執行動作 372, 381
封存 374
建立通知 368
更新狀態 382
檢視 371, 383
變更嚴重性 382
轉寄 378
關於 368
附件清單
刪除 354
建立 351
編輯 353
處理 342
關於 343
隨附於產品 344
封存
事件 374
郵件 356
建立 278

政策
動作 285
啟用或停用 277
套用至政策群組 296
微調 300
指派給政策群組 172
條件 280, 283, 729
疑難排解 300
考量 281
複製 277
設定內容加密 385
評估順序 277
相符文字 385
記錄
上載資料來源檔案 312
修改 314
刪除 315
在政策中使用 302
對應資料來源檔案欄位 307–308
檢視 315, 318–319
系統樣式 307–308
結構化資料 302
複寫 313
資料來源檔案 304
關於 302
掃描非純文字檔案附件 328
設定內容加密 385
通知
事件 368
刪除 324
建立 321
編輯 323
處理 320
變數 321, 363
關於 321
報告 498
註釋
刪除 341
建立 341
編輯 341
過濾, 語言式 174
樣式
刪除 341
建立 339
管理 337
編輯 340
關於 338
標頭標記 419
檢視, *請參閱* 內容過濾, 記錄
辭典
停用單字和詞組 329
刪除 332
刪除單字或詞組 331
匯入單字和詞組 330
匯出單字與詞組 328
尋找單字與詞組 332
建立 329
掃描非純文字檔案附件 328
編輯 331
處理 324
關於 325
隨附於產品 333
關於 276
內容遵循, *請參閱* 內容過濾
內容隔離所, *請參閱* 內容過濾
內部郵件主機 57
內部郵件伺服器 130
反向 DNS 69
文件, 產品 27
日期格式 581–582
日誌 543
另見 郵件稽核日誌
syslog 538–540, 542
手動刪除 535
本機掃描程式 533
目錄資料服務 535
系統效能 533
記錄層級 533
控管中心 529
掃描程式 535
清除 531
設定 538
備份 613
資料庫大小 531
監控 524
磁碟空間警示 535
遠端 syslog 538
遠端掃描程式 533
儲存 530
檢視 528
關於 525
類型 526

五劃

主機
SMTP 設定 595
內部郵件主機 57
存取控管中心 576

服務 64
狀態 522
修改 59
停止 60
停用 59
啟用 59
啟動 60
組態設定 35–36
進階組態設定 37
新增 32
關閉 604
代理伺服器
LAN 主機 201
新增 34
編輯 34
出廠預設值, 還原 600, 761
功能
產品 23
預設設定 26
加密 70
另見 TLS 加密
加密的附件 176
可疑病毒隔離所 204
另見 病毒
大小, 上限 207
保留郵件 207
清除 207
郵件
刪除 209
排序 209
搜尋 210–211
搜尋提示 211
檢視 209
處理 208
語言編碼 206
郵件清單頁面上的項目數 206
釋放 210
郵件清單頁面上的項目數 206
語言編碼 206
檢視 209
瀏覽 205
關於 204
可疑附件 176, 184
未經測試的判斷 547
未解析的電子郵件地址 264
本機信譽 130
本機網域 75
另見 網域
指定接受對象 70
架構 71
匯入 74
關於 70
本機路由清單 71
白金級病毒定義, *請參閱* 定義
目錄資料來源
收件者驗證 430, 474
收件者驗證查詢 443
位址解析 436, 469
位址解析查詢 450
刪除 460
快取
修改設定 477
擴充性最佳實務準則 488
關於 481
依賴的功能 423
服務通訊錯誤 426
保留收件者地址 456
架構進階設定 484
修改 457
修改收件者驗證查詢 474
修改位址解析查詢 469
修改繞送查詢 472
修改驗證查詢 463
停用 459
啟用 459
進階設定 477
新增 426
編輯 460
編輯 LDAP 伺服器組態 461
繞送 434, 472
繞送查詢 448
關於 429
關於修改 458
驗證 431, 463
驗證查詢 444
目錄資料來源功能
收件者驗證 439
位址解析 439
新增 428
繞送 438
驗證 437
目錄資料來源查詢
查詢語法 440
關於 440
目錄資料快取
設定快取 480
預載程式 482
關於 481

目錄資料服務
收件者驗證 439
位址解析 439
快取預載程式 482
擴充性 488
繞送 438
關於 423
關於來源和功能 429
關於保留收件者地址 455
關於散布清單展開 455
驗證 437

六劃

全域信譽 130
地區設定 580
安全風險 184
收件者地址保留 456
收件者驗證
功能 439
架構 86
查詢 443
啟用現有的目錄資料來源 474
新增目錄資料來源 430
編輯資料來源 474
總覽 85
收件者驗證資料來源
服務通訊錯誤 430
查詢
修改 474
啟用, 停用 474
建立和測試 443
啟用, 停用 474
新增 430
編輯 474
自行簽署的憑證
重新命名 153
新增 148
關於 145
行銷郵件 213

七劃

佇列, *請參閱* 郵件佇列
位址偽裝
忽略位址中的文字大小寫 83
架構 77
探查帳戶 81
匯入清單 82
新增 81
編輯 81
位址解析
功能 439
查詢
啟用 469
建立 450
編輯 469
資料來源
停用 469
啟用 469
新增 436
服務通訊錯誤 436
查詢 450
編輯 469
資料來源查詢
修改 469
建立自訂 450
判斷
可用的過濾動作
內容過濾 285
未經測試的 547
依類別 724
政策群組優先度 175
省略不予處理 727
間諜程式或廣告程式判斷 184
別名與散布清單
垃圾郵件寄給 260
忽略位址中的文字大小寫 83
架構 77–78
通知
啟用 263
垃圾郵件 259
匯入 79
新增 79
詳細資料, 範例 80
編輯 79
快取, *請參閱* 目錄資料來源, 快取
快取持續性 481
快取設定, 目錄資料來源 484
快速通過
架構 135
啟用, 停用 135
運作方式 133
關於 122
我的最愛報告
自動產生 497
刪除 496
攻擊
架構 185

偵測的技術 177
電子郵件病毒偵測 127
關於 122
關於偵測 176
更新
定義 198
系統
地區設定 580
管理員, *請參閱* 管理員
系統樣式 307–308, 310
防垃圾郵件過濾器 213
另見 垃圾郵件
語言式 173–174
關於 213
防毒 176
另見 病毒
另見 惡意軟體
引擎 177
過濾器 176

八劃

事件, *請參閱* 內容過濾
事件資料夾, *請參閱* 內容過濾
使用者, 在政策群組中尋找 166
使用者介面憑證, HTTPS 145, 579
使用者群組, *請參閱* 政策群組
初始防護 177
垃圾郵件 213
另見 垃圾郵件隔離所
另見 政策
另見 政策群組
不必要的電子郵件 221
可疑垃圾郵件臨界值, 架構 224
自訂規則
刪除 237
啟用和停用 230
提交者 233–234
提交者 ID 230
提交郵件 226, 236, 258, 365, 380
疑難排解 228
監控提交 374
設定 228
關於 226, 228
客戶規則
提交積極程度 232
政策
修改 222
刪除 223
啟用和停用 221
建立 219
指派給政策群組 170
複製 223
退回攻擊防護 140
預先架構 214
將寄件者排除在垃圾郵件掃描之外 133
掃描以文字為基礎的附件 218
略過掃描 135
報告 498
電子郵件地址搜尋攻擊 128
語言式過濾 173–174
關於 213–214
垃圾郵件過濾器 213
另見 垃圾郵件
垃圾郵件隔離所 239
另見 垃圾郵件
日誌 526
未解析的電子郵件地址 240
存取隔離所問題 264
別名與散布清單 260
使用之前 240
使用者登入說明 584
保留郵件 246–247
架構設定 241
清除 246–247
處理郵件 251
通知
使用者 257
修改範本 261
啟用 263
誤報，通知對象 247
變數 262
選取格式 263
郵件範本 259
關於 259
最佳實務準則 266
散布清單, 別名 260
無法傳送的郵件 264
郵件
刪除 256
排序 253
搜尋 253–254
搜尋提示 254
數目上限 264
標頭, 檢視 255
檢視 250
語言編碼 244
誤報，通知對象 247
郵件清單頁面上的項目數 252

郵件管理員信箱 251
針對自訂規則進行提交 258
錯誤識別 256
郵件清單頁面上的項目數 252
郵件管理員信箱 251
僅供管理員的存取 242
疑難排解 264
管理員頁面與使用者頁面之間的差異 249
語言編碼 244
誤報 256
複製郵件 264
錯誤 264
錯誤識別的郵件 256
檢視 241, 250
檢視郵件 248
臨界值 245
瀏覽 241
關於 239–240
定義
白金級 201
更新 177, 198
來源
LAN 主機 201
賽門鐵克 201
狀態 199
停用自動更新 200
排程 200
視需要 201
服務
代理伺服器 34
狀態 522
掃描程式 63
監控 520
關於 64
法規遵循 276
版本說明 618
狀態
SMTP 515
日誌 525
佇列的郵件 550
系統 515
垃圾郵件提交 374
服務 522
控制面板 516
硬體狀態 521
硬體資訊 520
郵件佇列大小 554
關於 515
阻絕服務攻擊
退回攻擊防護 137
配置區限制 196
附件
已加密 176
可疑 176, 184
配置區檔案 196
附件清單, *請參閱* 內容過濾
非本機網域, *請參閱* 網域, 非本機
非純文字檔案附件 328

九劃

保留
可疑病毒隔離所
保留期間 207
垃圾郵件隔離所
保留期間 247
郵件保留時間 246
信譽
本機 130
全域 130
研究 140
威脅防禦
政策
安全預覽 397
關於 395
預設 395
掃描設定
從掃描中排除檔案類型 394
架構 392
報告 498
威脅類別 518
客戶特定垃圾郵件規則, *請參閱* 垃圾郵件: 自訂規則
指令
agent-config 634
cat 636
cc-config 637
clear 640
db-backup 641
db-restore 645
delete 647
diagnostics 652
dns-control 656
fipsmode 658
grep 659
ifconfig 666
iostat 667
ip 668
ldapsearch 669

list 670
mallog 672
malquery 674
monitor 679
more 685
mta-control 686
netstat 692
nslookup 693
password 694
patch 695
ping 697
ping6 698
reboot 699
route 700
rpmdb 701
rsa-金鑰 702
service 703
show 706
shutdown 707
sshd-config 708
symdiag 711
tail 620, 712
telnet 715
traceroute 716
traceroute6 717
更新 718
說明 660
指令行介面 620, 627, 630, 660, 695
政策 176, 213, 276
另見 內容過濾
另見 垃圾郵件
另見 病毒
一般使用者 173–174
威脅防禦, 安全預覽 397
威脅防禦, 預設 395
威脅防禦, 關於 395
指派
內容過濾 172
垃圾郵件 170
惡意軟體 169
病毒 170
語言 174
政策群組優先度 175
病毒, 預設 188
預設值 26
管理惡意軟體 190
語言式 173
政策群組
一般使用者設定 173–174
成員
刪除 165
匯入 165
匯出 165
新增 164
刪除 168
使用者, 尋找 166
建立 162
指派政策
內容過濾 172, 296
垃圾郵件 170
惡意軟體 169
語言 174
啟用, 停用 168
預設政策 26
管理 168
編輯 168
優先度 161, 175, 562
總覽 161, 562
離埠, 入埠效果 161, 562
架構, Symantec Messaging Gateway 25
查詢, 用於資料來源 440
重新導向 URL 213

十劃

效能對有效性 133
時間格式 581–582
格式, 時間與日期 581–582
病毒 184
另見 惡意軟體
人工智慧設定 177, 202
定義
LiveUpdate 198
來源 201
快速回應 198
更新 198
狀態 199
白金級 201
管理 197
視需要 201
配置區限制 196
偵測中 176, 185
偵測的技術 177
將檔案排除在掃描範圍之外, 清單
修改 194
停用 195
刪除 196
匯出 196
啟用 195

建立 193
處理 193
郵件設定 205
類別及預設動作 170
病毒攻擊辨識
架構 127, 176, 185
停用 127
偵測病毒的方式 177
啟用 127
關於 122
記錄, *請參閱* 內容過濾
退回攻擊防護
垃圾郵件政策 140
建立種子值 138
架構 136, 139
總覽 137
配置區限制 176, 196

十一劃

偽裝清單
匯入 82
新增, 編輯 81
動作
內容過濾政策 285, 298
多個
內容過濾政策 298
政策群組優先度 175
組合, 限制
處理限制, 列表 720
寄件者
寄件者識別方法 118
從寄件者群組刪除 114
從寄件者群組匯出 117
啟用, 停用 114
匯入寄件者群組 115
新增至寄件者群組 113
編輯清單 114
攔截的寄件者群組 130
寄件者政策
選擇動作 112
關於 122
寄件者群組
一般使用者清單 173
刪除寄件者 114
寄件者識別方法 118
啟用, 停用
成員 114
群組 111
連線類別的影響 124
匯入資料 115
匯入檔案格式 116
匯出資料 117
新增成員 113
管理成員 112
編輯成員 114
選擇動作 112
總覽 130
關於 122
密碼
重設 597
強式 584, 597, 599
略過 584
最佳實務準則 598
管理 596
將郵件封存 356
掃描程式
DNS 32–33
另見 設定, 掃描程式
IP 位址 35–36
NTP 時間伺服器 33
SMTP 設定
入埠 41
入埠傳送 43
關於 39
限制接受 42
離埠 44
離埠傳送 46
SMTP 進階設定 48
乙太網路 32, 37
日誌 525
代理伺服器 32, 34
刪除 61
定義角色 40
服務
啟動, 停止 63
關於 64
重新授權 615
修改 59
修改 SMTP 設定 40
時間設定 32–33
停止 60
停用 59
授權 614–615
啟用 59
啟動 60
新增 32
電子郵件設定 38
磁碟空間 525, 535

管理郵件流 65
複寫 585
憑證 145, 150, 159
關於 29
關閉 604
掃描程式的複寫 585
授權 614–615
探查參與 272
探查帳戶
Symantec Probe Network 268
手動建立 273
在報告中追蹤 270
位址偽裝 78, 269
別名位址 78, 269
刪除 275
建立 270
建立指南 269
追蹤資料 493
執行報告 495
從無效收件者的電子郵件地址建立 272
啟用 274
報告 498
過濾垃圾郵件 269
關於 269
探查網路 122
接聽程式通訊埠 578
控制面板
內容 516
控管中心
DNS 576
IP 位址 62
IPv6 主機存取 576
日誌 525
主機存取 576
同時存取 575
安全警告 579
使用者登入說明 584
架構 573
重新授權 615
退回攻擊防護 138
接聽程式通訊埠 578
授權 614–615
喜好設定 583
登入與登出 584
憑證 145, 579–580
錯誤日誌 529
條件
比對條件 283
在內容過濾政策中建立 281
考量 280
根據郵件部分 729
消極/否定 729
清單
別名與散布清單
匯入 79
新增 79
編輯 79
詳細資料, 範例 80
關於 78
匯入本機路由/網域清單 71
清單, 附件 343
另見 內容過濾
清除 360
另見 清除程式
內容事件資料夾 360
日誌 531
可疑病毒隔離所 207
垃圾郵件隔離所 246–247
清除程式
內容事件資料夾 360
日誌 525, 531
垃圾郵件隔離所 246
第三方寄件者清單
用來攔截郵件 130
為寄件者群組指定 118
統一資源識別元 (URI), *請參閱* URI (統一資源識別元)
規則, *請參閱* 垃圾郵件
規則運算式, Perl 相容 354–355
設定 213
另見 垃圾郵件
SMTP
入埠 41
進階 48
關於 39
離埠 44
一般使用者 173–174
主機 48
代理伺服器 34
掃描程式 33, 35–37, 48
掃描程式, 電子郵件
入埠 41
入埠傳送 43
關於 39
限制接受 42
離埠 44
離埠傳送 46
離埠郵件接收 45
網域名稱系統 (DNS) 33

網路時間通訊協定 (NTP) 33
靜態路由 35–37
軟體
更新 616, 618–620
更新注意事項 618
版本 619
重新授權 615
授權 614–615
監控 520
通知
內容過濾違規 321
垃圾郵件隔離所
編輯範本 261
選擇格式 263
頻率 257
補救動作 370
通訊埠 578
連線時處理 122
連線類別
架構 125
停用 125
啟用 125
運作方式 124
預設設定 126
對寄件者群組的影響 124
學習模式 124–125
關於 122
部署
在閘道的優點 57
非閘道 57
寄件者群組政策 58, 130

十二劃

備份
日誌資料 613
排程 606, 608–609
視需要 609
管理 606
還原 602, 611
報告
Data Loss Prevention Network Prevent 整合 414
IP 連線 498
內容過濾 498
以電子郵件傳送 494
刪除 496
我的最愛
刪除 496
自動產生 497
垃圾郵件 498
表 510
建立 495
架構資料保留期間 493
配置 510
探查帳戶 498
清除 493
產生
自動 497
惡意軟體 498
無效收件者 498
無效收件者報告 498
郵件 498
資料追蹤
保留 493
要追蹤的項目 493
圖表 510
摘要 498
疑難排解 509
總覽 492
惡作劇程式 184
惡意攻擊
zip 炸彈 196
阻絕服務 196
偵測中 176–177, 185
惡意軟體 184
另見 病毒
判斷 184
政策
修改 191
停用 191
刪除 192
啟用 191
建立 187
指派給政策群組 169
複製 192
預設 188
預設動作 169
偵測 176
報告 498
管理政策 190
提早釋放 395
散布清單, *請參閱* 別名與散布清單
散布清單展開
展開和保留收件者地址 454
啟用和停用資料來源 456
最佳實務準則
FIPS 765
SMTP 驗證 96
垃圾郵件隔離所 266

密碼 598
資料目錄服務
安全性 487
擴充性 488
無效收件者
全部接受 86
拒絕 86
棄置 86
報告 498
總覽 85
無法傳送的垃圾郵件 264
無法掃描的配置區限制 196
登入
垃圾郵件隔離所, 疑難排解 264
略過憑證 584
硬體
狀態 521
相關資訊 520
監控 520
硬體裝置 604
另見 MTA, 管理
使用 DRAC 重新啟動 758
恢復為出廠預設值 600
重新啟動 600
備份 606, 609
維護 599
還原 602, 611
關閉 601, 604
結構化資料, *請參閱* 內容過濾
虛擬 IP 位址
IPv6 36
進階設定 37
診斷 621–623, 625–626
註冊
控管中心 614–615
掃描程式 614–615
註釋, *請參閱* 內容過濾
郵件
可疑病毒隔離所
保留期間 207
搜尋 210–211
檢視 209
瀏覽 205
釋放 210
垃圾郵件隔離所
保留期間 246
允許的上限 264
搜尋 253–254
檢視 250
瀏覽 241
臨界值 245
複製 264
誤報，通知對象 247
郵件保留時間 247
郵件管理員信箱 251
錯誤識別 256
封存 356
重新繞送 550–551
啟動, 停止 63, 65
棄置無效收件者 86
郵件 ID 253, 547
郵件主機, 內部 57
郵件佇列
刪除 552
狀態 554
重新傳送 554
啟動, 停止 65
郵件流 553
搜尋 550
管理 65
錯誤郵件佇列 48
檢視 550
關於 550
郵件報告 498
郵件流 553
另見 MTA
入埠圖 87
省略的判斷 727
停止 553
啟動, 停止 63, 65
減量 122
階段 87
管理 65
總覽 87
總覽, 電子郵件 87
關於 25
郵件稽核日誌
處理 543
郵件管理員信箱 251
間諜程式 176, 184
黑名單, *請參閱* 第三方寄件者清單

十三劃

傳送
可疑病毒隔離所 204
垃圾郵件隔離所
無法傳送的郵件 264
錯誤識別的郵件 256

啟動, 停止 63
搜尋
內容過濾辭典中的單字或詞組 332
可疑病毒隔離所
條件與提示 211
標頭 210
郵件 210
垃圾郵件隔離所
條件與提示 254
標頭 253
郵件 253
群組, 政策, *請參閱* 政策群組
解除 177
資料來源和功能 429
另見 目錄資料來源
資料夾、內容過濾, *請參閱* 內容過濾
資料目錄整合的安全性
最佳實務準則 487
資料目錄服務
安全 487
建立資料來源 426
限制伺服器存取 487
資源 122, 135, 727
資源, 內容過濾, *請參閱* 內容過濾
資訊事件, *請參閱* 內容過濾
過濾器 176, 213
另見 垃圾郵件
另見 病毒
一般使用者 173–174
改善 225
政策群組優先度 175
語言式 173–174
總覽 87
閘道
部署考量 57
管理流量 121
隔離事件, *請參閱* 內容過濾
隔離所, 可疑病毒, *請參閱* 可疑病毒隔離所
隔離所, 垃圾郵件, *請參閱* 垃圾郵件隔離所
隔離所、內容, *請參閱* 內容過濾
電子報 213
電子郵件, *請參閱* 內容過濾, *請參閱* 垃圾郵件, *請參閱* 病毒
電子郵件別名, *請參閱* 別名與散布清單
電子郵件地址, 為群組識別 118
電子郵件地址搜尋攻擊
架構識別 128
關於 122
電子郵件流量, *請參閱* 閘道
電子郵件病毒攻擊
架構識別 127
關於 122
電子郵件網域 69
電子郵件訊息流
入埠圖 87
階段 87
總覽 87
電子郵件設定, 掃描程式 38
電子郵件過濾 176, 213, 276
另見 內容過濾
另見 垃圾郵件
另見 病毒
入埠圖 87
階段 87
總覽 87
電子郵件驗證
DKIM
啟用簽署 106
SMTP 驗證 93
預設值
內部主機清單 58
功能 26
政策 26
連線類別 126
惡意軟體政策動作 169
電子郵件病毒政策動作 170

十四劃

儀表板
威脅類別 518
廣告程式 176, 184
摘要報告 498
撥號工具 184
標頭
可疑病毒隔離所 210
垃圾郵件隔離所
搜尋 253
檢視 255
樣式, *請參閱* 內容過濾
疑難排解
垃圾郵件隔離所 264
報告 509
磁碟空間
清除 536
管理 603
管理員
LDAP 564
本機 564

刪除 573
修改 572
密碼
強式 584, 597
重設 597
僅供管理員的垃圾郵件隔離所存取 242
新增 564
管理 559
管理通知 370
權限 564, 566
管理設定
乙太網路 37
掃描程式 48
管道
啟動, 停止 63, 522
關於 64
網域
反向 DNS 69
本機 71
另見 本機網域
用於離埠郵件接收 45
刪除 75
非本機 71
指定接受對象 70
架構 69
為寄件者群組指定 118
啟用 DKIM 簽署 106
匯入 74
關於 70
網域名稱系統 (DNS) 伺服器 33
網域金鑰
PEM 格式 157
重新命名 153
匯入 109
新增 109
網路, 寄件者群組政策考量 58, 130
網路公用程式 622
網路時間通訊協定 (NTP) 伺服器 33
語言編碼 206, 244
語言識別
一般使用者 173
架構 174
誤報的垃圾郵件 220, 247, 256
說明
Symantec Messaging Gateway 27
遞補語言編碼 580
遠端伺服器日誌 538
遠端存取程式 184

十五劃

稽核 ID 546
編碼 580
複製郵件, 垃圾郵件隔離所 264

十六劃

優先權, 政策群組 175
憑證
HTTPS 145, 158–160
MTA TLS 145, 159
PEM 格式 157
SMTP/TLS 158–159
自行簽署 145, 148, 153, 157, 579
刪除 159
防止資料外洩 154
使用 146
指派 145, 159
指派使用者介面 HTTPS 160
架構 145
重新命名 153
控管中心 580
匯入 154
匯出 155, 158
憑證授權中心簽署
PEM 格式需求 157
修改 149
備份 153
匯入 152
取代 153
存取控管中心 579
新增 148, 150
要求 151
關於 145
應用程式 154, 156
檢視 151, 158
應用程式憑證
刪除 156
匯出 155
編輯 156
遵循, *請參閱* 內容過濾
錯誤, 垃圾郵件隔離所 264
錯誤識別垃圾郵件 247, 264
錯誤郵件
佇列 48
處理 48
靜態路由 35–36
駭客工具 184

十七劃

檢視, *請參閱* 內容過濾, 記錄
聯邦資訊處理標準 (FIPS), *請參閱* FIPS
臨界值
    內容事件資料夾 360
    可疑病毒隔離所 207
    垃圾郵件隔離所 245
賽門鐵克安全機制應變中心 122, 225
還原
    出廠預設值 600
    從不同 IP 位址 602
    從本機備份 611

十八劃

擴充性, 目錄資料服務整合 488
繞送
    功能 438
    查詢 448
    資料來源
        停用 472
        啟用 472
        新增 434
        服務通訊錯誤 434
        查詢 448, 472
        編輯 472
    資料來源查詢
        修改 472
        建立自訂 448
雙位元組字元集 580
離埠 SMTP 設定
    要接受郵件的網域 45
    傳送 46
    關於 39
    變更 44

十九劃

辭典, *請參閱* 內容過濾

二十劃

攔截的寄件者清單, *請參閱* 攔截的寄件者群組
攔截的寄件者群組
    一般使用者清單 173
    刪除寄件者 114
    使用實例 130
    寄件者識別方法 118
    啟用, 停用
        成員 114
        群組 111
    連線類別的影響 124
    匯入資料 115
    匯入檔案格式 116
    匯出資料 117
    新增成員 113
    編輯成員 114
    選擇動作 112
    總覽 130
    關於 122
警示
    SMTP 驗證 96
    條件 587, 590
    設定 586
    磁碟空間不足 587
    類型 587
釋放, 郵件
    從可疑病毒隔離所 210
    從垃圾郵件隔離所 256

二十三劃

變數, 通知郵件 262, 363
驗證
    Enforce Server 388
    功能 437
    查詢 444
    資料來源
        停用 463
        啟用 463
        新增 431
        服務通訊錯誤 431
        查詢 444, 463
        編輯 463
    資料來源查詢
        修改 463
        建立自訂 444