技術概要：從 SMS FOR SMTP 移轉。

symantec.

世界連線 信心無限

從 Symantec Mail Security for SMTP 移轉到 Symantec Brightmail Gateway

白皮書：賽門鐵克操作程序

從 Symantec Mail Security for SMTP 移轉到 Symantec Brightmail Gateway

內容

簡介

本文件提供了有關從 Symantec Mail Security for SMTP (SMS for SMTP) 移轉到 Symantec Brightmail Gateway (SBG) 的詳細資料。由於不同通訊環境可能有非常大的差異，因此本文件沒有提供移轉的逐步式程序，而是提供移轉程序的概覽，以及如何儘可能從 SMS for SMTP 順利轉換到 SBG 的提示和秘訣。

關於從 **SMS for SMTP** 移轉到 **SBG**

從 SMS for SMTP 移轉到 SBG 大部分是手動程序。移轉程序包含三個主要任務：

1. 安裝 SBG。
2. 記錄 SMS for SMTP 中的關鍵設定。
3. 從 SMS for SMTP 將設定移轉到 SBG。

本文件著重說明此程序的步驟二和步驟三。如需步驟一的相關協助，請檢視 SBG 的*入門指南*和*安裝指南*。

規劃移轉

在開始移轉之前，客戶應該已在其 8300 系列硬體或 VMware 環境中執行最新版的 SBG。以下網站提供了最新版的詳細資料以及下載位置：

http://www.symantec.com/business/support/overview.jsp?pid=53991

規劃部署 SBG 時，請確保適當調整硬體資源規模，以符合環境的需求。可將 SBG 部署在 8300 系列硬體裝置上，也可以部署在所選擇的執行 VMware ESX 或 ESXi 3.5 版的硬體上。鑒於 SBG 中的處理和連線管理的改進，確切的硬體需求可能與用於 SMS for SMTP 的硬體需求不同。

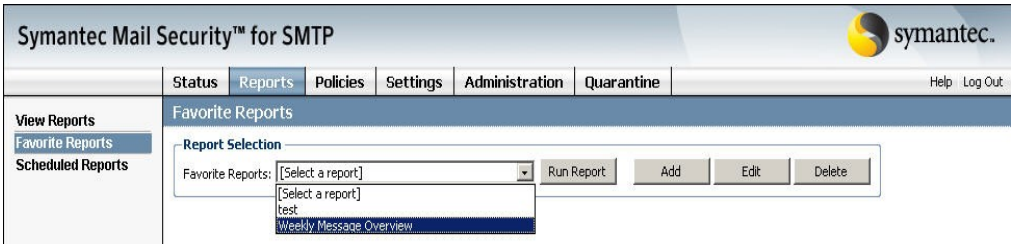
如果您計畫部署在 VMware 上，請確保符合 Brightmail Gateway 虛擬版的系統需求。

如需進一步的資訊，請參閱「SBG 入門指南」的 System requirements and recommendations for virtual deployment (「虛擬部署的系統需求和建議」) 一節。

記錄 **SMS for SMTP** 的關鍵設定，然後移轉到 **SBG**

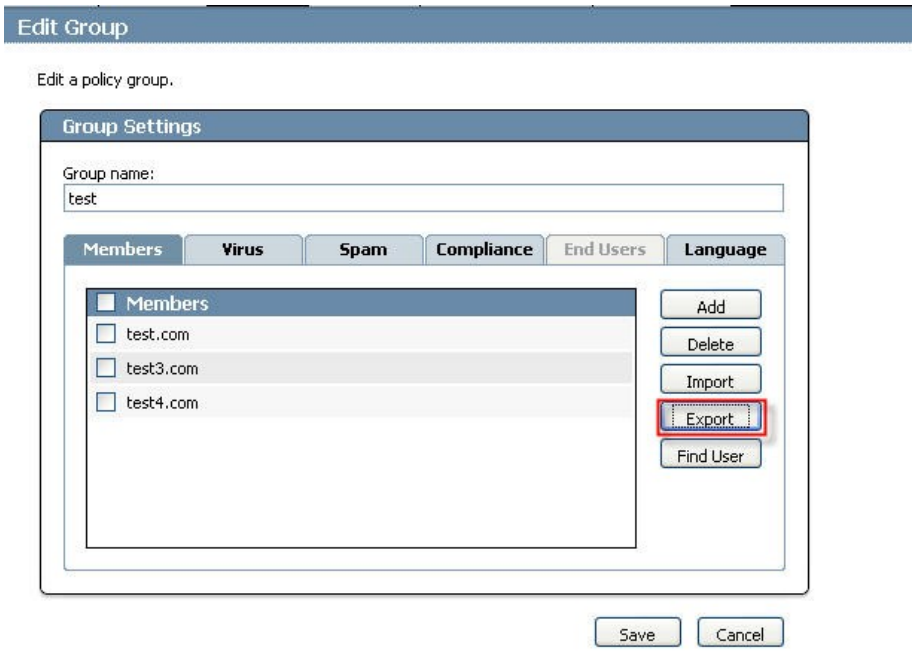
以下列出了移轉到新 SBG 環境時您要記錄的最重要功能和設定。

1. 報告 - 在 SMS for SMTP 的「報告」頁面上，按下「我的最愛報告」和「已排程報告」連結。編輯這些位置儲存的所有報告，並記錄這些報告上的詳細資料以複寫到 SBG。在 SBG 中建立這些報告時，您可能會注意到來自 SMS for SMTP 的某些報告已不存在。如果是這樣，則表示這些報告已由 SBG 中提供的功能更強大的報告所取代。



2. 群組政策 - 記錄環境中「政策」->「群組政策」頁面上的所有群組政策。對於每個群組政策，請記錄以下詳細資料：

    - 屬於該群組的成員。如果群組成員不是以 LDAP 群組為基礎，則可以將此資料匯出到文字檔，然後匯入 SBG，如下圖所示。如果群組成員是以 LDAP 群組為基礎，則應記錄此資料，在設定「LDAP 同步化」來源後，可以將群組新增到 SBG 中的新群組。



    - 記錄病毒政策詳細資料，包括套用至每種判斷類型的不同政策名稱。在「政策」->「過濾器政策」->「病毒」頁面上，編輯套用至群組的不同政策，然後記錄所採取的動作 (大多數情況下，政策的名稱對所採取的動作會有些許暗示)。設定 SBG 時，您可以建立類似的政策，以套用至建立的新群組。
    - 記錄垃圾郵件政策詳細資料，包括套用至每種判斷類型的不同政策名稱。在「政策」->「過濾器政策」->「垃圾郵件」頁面上，編輯套用至群組的不同政策，然後記錄所採取的動作 (大多數情況下，政策的名稱對所採取的動作會有些許暗示)。設定 SBG 時，您可以建立類似的政策，以套用至建立的新群組。
    - 記錄套用至群組的所有遵循政策，包括套用至群組的不同遵循政策名稱。在「政策」->「過濾器政策」->「遵循」頁面上，編輯不同的群組政策，並記錄不同政策的條件和採取的動作。在 SBG 中重新建立這些群組時，您可以利用明顯改進的進階內容過濾和資料損失預防功能。您可能想要調查如何使用某些新功能使您的政策功能更強大。

3. 電子郵件防火牆政策 – 在「政策」->「電子郵件防火牆政策」頁面上，記錄目前啟用的電子郵件防火牆政策：

- 在「攻擊」頁面上是否架構了攻擊？記錄是否啟用了電子郵件地址搜尋攻擊 (DHA)。如果是，則在 SBG 中架構 LDAP 同步化來源後，即可再次啟用 DHA。SBG 中還有一個更好的新選項，讓您可以使用新的 LDAP 收件者驗證來源啟用 DHA 功能。如需進一步的詳細資料，請參閱*「SBG 管理指南」*。
- 如果已啟用垃圾郵件攻擊功能，則在 SBG 中已由連線類別功能取代，依預設，會在新的 SBG 安裝中啟用該功能。如需進一步的詳細資料，請參閱*「SBG 管理指南」*。
- 如果已啟用病毒攻擊功能，請記錄所架構的臨界值，然後將類似設定套用至 SBG 的「信譽」-> 「寄件者」->「電子郵件病毒攻擊」頁面。
- 如果已啟用寄件者驗證，請記錄所使用的寄件者驗證技術 (SPF 或寄件者識別碼)，記錄哪些網域啟用了寄件者驗證，並記錄郵件未通過驗證時會採取的動作。然後，可以將這些設定複寫到 SBG 的「垃圾郵件」->「設定」->「寄件者驗證」設定頁面。
- 在「寄件者群組」頁面上，查看是否已啟用或填入任何「攔截的寄件者」或「允許的寄件者」(網域式、IP 式或第三方服務) 清單。如果未架構任何內容，則不需要採取任何動作。如果已填入其中任何清單，請記錄針對該特定清單所採取的動作。藉由編輯其中任何清單並使用匯出功能，您可以將所有清單中包含的資料匯出到名為 allowedblockedlist.txt 的檔案。在 SBG 中，「允許的寄件者」(Allowed Senders) 和「攔截的寄件者」(Blocked Senders) 清單已分別重新命名為「允許的寄件者」(Good Senders) 和「攔截的寄件者」(Bad Senders) 清單。透過在 SBG 的「信譽」->「政策」->「允許的寄件者」和「攔截的寄件者」頁面，編輯任何「本機允許的寄件者」或「本機攔截的寄件者」清單，並使用匯入功能，可以將 allowedblockedlist.txt 檔案匯入到 SBG。匯入清單後，請確保對不同的清單採取所需的動作，並確保啟用您要啟用的清單。
- 在 SBG 中，「開啟代理伺服器寄件者」清單和「可疑的垃圾郵件寄發者」清單已由「賽門鐵克全域攔截的寄件者」清單取代。在 SBG 中，這些清單更為有效，賽門鐵克強烈建議您讓此清單保持啟用狀態，並保持預設動作為拒絕。
- 在 SBG 中，「安全寄件者」清單已由「賽門鐵克全域允許的寄件者」清單取代。賽門鐵克強烈建議您讓此清單保持啟用狀態，並保留預設動作。

4. 政策資源 – 在「群組政策」->「政策資源」頁面上，記錄以下各項：
    - 如果已建立任何自訂註釋，並由遵循政策所使用，請記錄註釋名稱並編輯註釋，以便可以將文字剪下並貼至文字編輯器中。然後，您可以在 SBG 的「遵循」->「資源」->「註釋」頁面上重新建立註釋，並將文字貼到新註釋中。
    - 如果有任何政策使用「封存」動作，請記錄封存電子郵件地址、伺服器主機和通訊埠，然後在 SBG 的「遵循」->「設定」->「封存」頁面上輸入這些資料。
    - 如果已建立任何自訂附件清單，請記錄該清單名稱，編輯自訂附件清單，然後記錄與該清單關聯的所有真實檔案類型、副檔名和 MIME 類型。然後，您可以在 SBG 的「遵循」->「資源」-> 「附件清單」頁面上重新建立這些清單。另請注意，與 SMS for SMTP 比較，SBG 具有改進的且更廣泛的內建附件清單。

- 如果已建立任何自訂辭典，請記錄辭典名稱，編輯辭典，然後拖曳滑鼠選擇所有單字，將其複製並貼至文字編輯器。另存成文字檔，然後在 SBG 的「遵循」->「資源」->「辭典」頁面上重新建立清單。然後，您可以使用新辭典中的匯入功能，匯入儲存舊辭典單字的文字檔。另請注意，SBG 具有大幅擴充的預設辭典可供使用，包括為協助防止資料損失和強制遵從而設計的許多辭典。
- 如果已建立任何自訂通知，請記錄通知名稱，然後編輯通知，並記錄通知的寄件者、通知的收件者、主旨、郵件內文以及原始郵件是否附加於通知等詳細資料。然後可以在 SBG 的「遵循」->「資源」->「通知」頁面上重新建立通知。請注意，SBG 具有新增郵件屬性變數的功能，可協助進一步自訂通知。如需進一步的詳細資料，請參閱*「SBG 管理指南」*。

5. 如果您已架構「可疑垃圾郵件」設定，請記錄臨界值 (介於 25 到 89 之間)，然後在 SBG 的「垃圾郵件」->「設定」->「掃描設定」頁面上輸入相同的值。請確保適當的「可疑垃圾郵件」政策在 SBG 中已啟用，並已架構為符合 SMS for SMTP 組態中的政策。

6. 在 SMS for SMTP 的「設定」->「電子郵件掃描」->「病毒」設定下，記錄 LiveUpdate 組態。在 SBG 的「病毒」->「設定」-> LiveUpdate 頁面上輸入相同的組態。SBG 支援防毒規則集更新摘要之各種來源的組態：透過直接白金級病毒定義檔下載，或透過架構的 LAN 主機或代理伺服器主機。如果在 SMS for SMTP 中，已架構排除在病毒掃描範圍之外的檔案類型，則可以在 SBG 的「病毒」->「設定」->「掃描設定」->「排除掃描」頁面上架構相同的內容。同樣，如果在 SMS for SMTP 中已架構 Bloodhound 積極層級，則在 SBG 的「病毒」->「設定」->「掃描設定」->「一般」頁面上可以設定相同的內容。

7. 如果在 SMS for SMTP 中，已架構「配置區設定」(在「設定」->「電子郵件掃描」->「掃描」中)，則在 SBG 中，可以透過「通訊協定」-> SMTP ->「設定」->「掃描設定」頁面，手動設定相同的臨界值。

8. 如果有定義用於驗證或同步化的 LDAP 伺服器，則需要在 SBG 中，透過「管理」->「設定」-> LDAP 頁面，新增具有相同管理員憑證和查詢詳細資料的 LDAP 伺服器。選取 LDAP 伺服器用於「驗證」及/或「同步化」。請注意，「路由和收件者驗證」選擇是 SBG 的新功能。如需進一步的資訊，請參閱*「SBG 管理指南」*。

9. 從 SMS for SMTP 的「設定」->「系統設定」頁面，如果已架構垃圾郵件和可疑病毒隔離所設定，則可以在 SBG 中，透過垃圾郵件隔離所的「垃圾郵件」->「設定」->「隔離所設定」頁面，以及可疑病毒隔離所的「病毒」->「設定」->「可疑病毒設定」頁面手動複寫這些設定。如果已架構「報告」設定 (報告資料和清除程式設定)，則可以在 SBG 的「管理」->「設定」->「報告」->「報告設定」頁面架構這些設定。如果已架構日誌設定 (記錄層級、資料庫日誌儲存限制、清除程式、郵件稽核/追蹤日誌，以及 Syslog 設定)，則可以在 SBG 中透過「管理」->「設定」->「日誌」頁面架構這些設定。請注意，使用「遠端」標籤可透過 Syslog 擴充遠端記錄功能。如需進一步的資訊，請參閱*「SBG 管理指南」*。

10. 如果在 SMS for SMTP 中，已架構位址偽裝和別名功能，請將這些項目複製到文字檔，然後可以透過「管理」-> SMTP ->「位址偽裝」和「別名」頁面將該檔案匯入 SBG。請注意 SBG 的匯入功能支援文字檔：

    - 若要匯入偽裝項目，請從檔案 (與 Sendmail virtusertable 類似) 匯入偽裝位址的清單。在「位址偽裝」頁面上按下「匯入」時，就會顯示「匯入偽裝項目」頁面。指定或瀏覽至包含偽裝項目

的檔案並按下「匯入」。匯入完成後，您可以下載一份列出所有未處理項目的報告。注意：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。

- 若要匯入別名，必須使用一或多個空格或 Tab，或空格和 Tab 的組合來分隔文字檔中的各個位址。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。

11. 若要移轉 SMS for SMTP 安裝中所設定的本機網域，您可以將現有的本機網域複製到文字檔，然後透過「通訊協定」-> SMTP ->「網域」頁面，將該文字檔匯入 SBG。請確保本機網域定義和電子郵件地址的清單，是來自 US-ASCII 檔案 (類似 Sendmail mailertable)。您可以將選擇性路由資訊納入預設本機目的主機，作為定義的一部分。

12. 如果已架構多個管理員，並為每個管理員定義了不同角色，則需要在 SBG 中透過「管理」->「使用者」->「管理員」頁面，手動重新新增管理員和電子郵件地址 (可以選擇強制使用強式密碼)。請注意「遵循資料夾」所新增的管理權限精細度，以及管理員是否應該接收事件通知。另請注意，您可能需要在 SBG 中將管理密碼從預設值重設為之前在 SMS for SMTP 安裝中架構的密碼。

13. 如果在 SMS for SMTP 安裝中設定了警示 (從「設定」->「系統設定」->「警示」)，請記錄通知寄件者和警示條件，然後在 SBG 中透過「管理」->「設定」->「警示」頁面重設這些內容。請注意，SBG 中已擴充警示條件，可涵蓋更多事件和條件。

14. 如果在 SMS for SMTP 組態中架構了「反向位址繫結策略」(從「設定」->「主機」-> [選取主機] -> SMTP ->「進階設定 」)，由於 SBG 中提供更大的彈性讓管理員根據介面選取 SMTP 傳送繫結，因此沒有類似的功能。在 SBG 中，可以透過「管理」->「主機」->「組態」-> [選取主機] -> SMTP ->「進階設定」->「SMTP 傳送繫結」頁面來架構此設定。

無法移轉哪些項目？

在 SBG 中，雖然可以重新建立大多數 SMS for SMTP 組態，但是，儲存在 SMS for SMTP 控管中心的大多數資料將無法移轉到 SBG 控管中心。這包括目前的統計值、報告資料、隔離所資料和日誌資料。

如果一般使用者可存取個人的垃圾郵件隔離所，並且在使用 LDAP 驗證和同步化時，可以建立自己的允許清單和攔截清單並設定語言設定，則不會保留這些設定。一般使用者可以將這些設定複製並貼到文字檔，以便在 SBG 隔離所中重新建立清單。

關於賽門鐵克在提供安全、儲存及系統管理解決方案，以協助企業與客戶確保資訊安全和管理其資訊方面，賽門鐵克處於全球領先地位。賽門鐵克總部位於美國加州 Cupertino 市，業務遍及 10 個國家。如需更多資訊，請造訪 www.symantec.com。

如需特定國家營運據點及聯絡電話號碼，請造訪
賽門鐵克網站。如需產品資訊，美國地區請撥打
免付費電話 1 (800) 745 6054。

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com