Symantec™ Messaging Gateway 10.7 安裝指南

由 Brightmail™ 提供

Symantec

Symantec™ Messaging Gateway 10.7 安裝指南

文件版本：4.3

法律聲明

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com/region/tw

技術支援

賽門鐵克技術支援能維護全球支援中心。技術支援的主要任務是回應有關特定產品特性和功能的特定查詢。技術支援小組也會建立我們的線上知識庫內容。技術支援小組會與賽門鐵克內部的其他功能性部門共同合作，在最短時間內回答您的問題。例如，技術支援小組會與產品工程部門和賽門鐵克安全機制應變中心一起合作，提供警示服務和病毒定義檔更新。

賽門鐵克的支援服務包含：

- 多種支援選項，無論組織規模為何，您都能夠靈活選取最適合的服務
- 電話支援和/或網頁式支援，可提供快速回應與最新資訊
- 升級保證，可傳送軟體升級
- 購買的全球支援，以地區的上班時間或隨時待命為基礎
- 包含帳戶管理服務的頂級服務

若需賽門鐵克支援服務的相關資訊，請造訪我們的網站，URL 如下：

support.symantec.com

所有支援服務都會根據您的支援許可協議以及當時的企業技術支援政策提供。

聯絡技術支援

目前擁有支援許可協議的用戶可在下列 URL 存取技術支援資訊：

www.symantec.com/business/support/

在聯絡技術支援之前，請確定您的系統符合產品說明文件中所列的系統需求。同時，問題發生時，您應在發生問題的電腦旁邊，以重現所發生的問題 (如果需要)。

當您聯絡技術支援時，請提供下列資訊：

- 產品版本層級
- 硬體資訊
- 可用記憶體、磁碟空間和 NIC 資訊
- 作業系統
- 版本和修補程式層級
- 網路拓撲
- 路由器、閘道和 IP 位址資訊
- 問題說明：
  - 錯誤訊息和日誌檔案
  - 聯絡 Symantec 之前執行的疑難排解動作

- 最近的軟體組態變更和網路變更

授權和註冊

如果您的 Symantec 產品要求註冊或使用授權金鑰，請存取我們的技術支援 Web 頁面，網址為：

www.symantec.com/business/support/

客戶服務

您可在以下 URL 中取得客戶服務資訊：

www.symantec.com/business/support/

客戶服務可協助解決非技術性問題，例如以下類型的問題：

- 關於產品授權或序列化的問題
- 產品註冊更新，例如位址或名稱變更
- 一般產品資訊 (功能、可用語言、本地經銷商)
- 關於產品更新和升級的最新資訊
- 關於升級保證和支援合約的資訊
- 關於 Symantec 採購方案的資訊
- 關於 Symantec 技術支援選項的建議
- 非技術性的預售問題
- 光碟、DVD 或手冊的相關問題

支援許可協議資源

如果您想要針對現有支援許可協議與 Symantec 聯絡，請與您當地的支援許可協議管理團隊聯絡，各地區的聯絡方式如下：

亞太和日本	customercare_apac@symantec.com
歐洲、中東和非洲	semea@symantec.com
北美和拉丁美洲	supportsolutions@symantec.com

目錄

1

系統需求

本章包含以下主題：

系統組態選項

您可以透過下列方式安裝和執行 (Symantec Messaging Gateway)：

- 您可以使用賽門鐵克提供的硬體裝置。硬體選項包括：
  - 8380
  - 8380-S450
    附註：SMG 10.7 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 iDRAC，但 Symantec 8380-S450 平台不支援。
  - 8360
  - 8340
- 可以在您選擇的硬體上使用 VMware 或 Microsoft Hyper-V 安裝和執行虛擬硬體裝置。
- 安裝和執行實體元件與虛擬元件的組合。

在 VMware 上部署的系統需求

表 1-1 列出了以訪客形式將 Symantec Messaging Gateway 部署於 VMware ESXi Server 的系統需求。您必須安裝並架構 VMware 伺服器，然後才能安裝 Symantec Messaging Gateway 虛擬版 ()。

附註：Symantec Messaging Gateway 不提供任何版本的 BusLogic 控制器。

如需專屬於 VMware ESXi Server 的需求，請參閱 VMware 文件。

表 1-1 VMware 上支援的 組態

說明	建議	最低	注意事項
VMware ESXi Server	ESXi 6.0 版或更新版本	6.0 版	支援的版本為: ESXi/vSphere 6.0/6.5/6.7Server。 主機上的處理器必須支援 VT，並於安裝 之前，已在 BIOS 中啟用此設定。
磁碟類型	固定磁碟	----	Symantec Messaging Gateway 不支援在配備彈性磁碟的虛擬機器上進行安裝。
磁碟空間	如需詳細資訊，請參閱賽門鐵克知識庫文章 *Disk Space Recommendations for Symantec Messaging Gateway Virtual Edition* (「對於 Symantec Messaging Gateway 虛擬版的磁碟空間建議」)。	120 GB	對於僅限掃描程式、僅限控管中心及組合掃描程式與控管中心的虛擬機器，建議的最小磁碟空間相同。
記憶體	16 GB 至 32 GB	8 GB	執行 Symantec Messaging Gateway 和虛擬機器至少需要 8 GB。
CPU	8	4	根據工作量需求和硬體組態，賽門鐵克建議配置八顆以上 CPU。 **附註：**您的環境必須支援 64 位元應用程式。
NIC	2	1	一部虛擬機器只需要一張網路配接卡。 **附註：**支援的 NIC 數量上限為 2。
網路配接卡	VMXNET3		
儲存控制器			自動選擇相關的控制器。

請參閱第 26 頁的「關於 Symantec Messaging Gateway 虛擬版」。

在 Microsoft Hyper-V 上部署的系統需求

表 1-2 列出了以訪客形式將 Symantec Messaging Gateway 部署於 Microsoft Hyper-V Server 的系統需求。您必須先安裝並架構其中一個伺服器，然後才能安裝 Symantec Messaging Gateway 虛擬版。

如需專屬於 Microsoft Hyper-V Server 的需求，請參閱 Microsoft Hyper-V 文件。

表 1-2 Hyper-V 上支援的 組態

說明	建議	最低	注意事項
Microsoft Hyper-V	Windows 2016 Datacenter Edition	Windows 2012 Standalone	主機上的處理器必須支援 VT，並且在安裝前已於 BIOS 中啟用此設定以支援 64 位元核心。
磁碟類型	固定磁碟	----	Symantec Messaging Gateway 不支援安裝在配備動態磁碟的虛擬機器上。
磁碟空間	如需詳細資訊，請參閱賽門鐵克知識庫文章 *Disk Space Recommendations for Symantec Messaging Gateway Virtual Edition*（「對於 Symantec Messaging Gateway 虛擬版的磁碟空間建議」）。	120 GB	對於僅限掃描程式、僅限控管中心及組合掃描程式與控管中心的虛擬機器，建議的最小磁碟空間相同。
記憶體	16 至 32	8 GB	執行 Symantec Messaging Gateway 和虛擬機器至少需要 8 GB。
CPU	8	4	根據工作量需求和硬體組態，賽門鐵克建議配置 8 顆 CPU。 **附註：**您的環境必須支援 64 位元應用程式。
NIC	2	1	一部虛擬機器只需要一張網路配接卡。Symantec Messaging Gateway 僅支援使用合成 NIC。 **附註：**支援的 NIC 數量上限為 2。

請參閱第 26 頁的「關於 Symantec Messaging Gateway 虛擬版」。

LDAP 和網頁瀏覽器系統需求

表 1-3 列出了最低的網頁瀏覽器和 LDAP 系統需求。

請參閱第 9 頁的「在 Microsoft Hyper-V 上部署的系統需求」。

請參閱第 11 頁的「安裝前準備」。

表 1-3 系統需求

項目	需求
網頁瀏覽器	控管中心支援下列瀏覽器： ■ Microsoft Internet Explorer 11 或更新版本 ■ Mozilla Firefox 63 或更新版本 ■ Chrome 70 或更新版本
LDAP	Symantec Messaging Gateway 支援下列 LDAP 目錄類型： ■ Windows® 2012 Active Directory® (LDAP 和通用類別目錄) ■ Windows 2008 Active Directory (LDAP 和 Global Catalog) ■ Oracle® Directory Server Enterprise Edition 11.1.1.7 ■ Sun™ Directory Server 7.0 (EOL Dec 2017) ■ IBM® Domino® (先前稱為 Lotus Domino) LDAP Server 8.5.3 ■ IBM LDAP Server 8.5.2 ■ IBM Domino LDAP Server 8.5 ■ OpenLDAP 2.4 ■ OpenLDAP 2.3 Symantec Messaging Gateway 與 LDAP v.3 相容，可架構為與其他目錄伺服器類型搭配運作。 如需有關如何架構 Symantec Messaging Gateway 以與 LDAP 搭配使用的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

2

規劃安裝

本章包含以下主題：

安裝前準備

表 2-1 列出了安裝 Symantec Messaging Gateway 之前要執行的工作。

表 2-1 安裝前工作

工作	說明
規劃部署。	請檢閱下列主題，以協助您規劃部署。 請參閱第 7 頁的「系統組態選項」。 請參閱第 19 頁的「您的掃描程式該放置於哪裡」。 請參閱第 19 頁的「影響效能的環境因素」。

工作	說明
符合系統需求。	驗證您的環境符合最低系統需求。 請參閱第 10 頁的「LDAP 和網頁瀏覽器系統需求」。 請參閱第 7 頁的「在 VMware 上部署的系統需求」。 請參閱第 9 頁的「在 Microsoft Hyper-V 上部署的系統需求」。
收集安裝前檢查清單中的項目及資訊。	安裝前檢查清單指明您在安裝及設定硬體裝置時必須準備好的項目及資訊。 請參閱第 12 頁的System Requirements。
可能的話，架構您的防火牆。	如果在任何硬體裝置與 Internet 之間有防火牆，請將防火牆架構為允許透過特定通訊埠的網路流量。 請參閱第 56 頁的「Symantec Messaging Gateway 使用的通訊埠」。
確定能提供所需要的通訊埠。	Symantec Messaging Gateway 要求某些通訊埠必須可供使用。 請參閱第 55 頁的「必要通訊埠」。
僅虛擬環境：擷取快照。	如果您打算更新現有虛擬部署，賽門鐵克建議您在開始更新前擷取現有組態的快照。如需如何擷取快照的資訊，請查閱虛擬環境的相關文件。

安裝檢查清單

表 2-2 列出了在您執行啟動程序並執行 Symantec Messaging Gateway 的初始組態時，需要備妥的項目和資訊。

表 2-2 初始組態檢查清單

動作/項目	說明
驗證系統需求	您可以將 (Symantec Messaging Gateway) 安裝為實體裝置或虛擬硬體裝置。實體裝置與虛擬硬體裝置可共同存在於相同的企業網路內。 請參閱第 7 頁的章 1。
下載虛擬影像檔案 (僅限虛擬硬體裝置)	將虛擬影像檔案從 https://fileconnect.symantec.com/ 下載到一個可以從主控台存取的目錄中。

動作/項目	說明
主控台對硬體裝置的存取	鍵盤及 VGA 監視器，或從其他電腦透過序列埠進行存取。 該序列埠必須是使用 DB9 接頭的虛擬數據機纜線，並設定為 9600 bps、8/N/1。 ___鍵盤及 VGA 監視器 或 ___序列埠 或 ___DRAC 請參閱第 24 頁的「安裝 8300 系列硬體裝置 」。
在防火牆和其他網路裝置上開啟必要的通訊埠	您的防火牆可能需要開啟某些通訊埠，Dell Remote Access Controller (DRAC) 才能進行存取。如需詳細資訊，請參閱您的 iDRAC 版本所適用的 Dell 支援。 需要的通訊埠為 TCP 22、53、80、443、41000 和 41002。以及 UDP 53 和 123。請參閱第 55 頁的「必要通訊埠」。 以瞭解 SMG 上所有通訊埠的使用狀況的資訊。
乙太網路纜線 (最多四根普通纜線和兩根跳接纜線) 可用	纜線的數量和類型取決於您的網路組態以及硬體裝置上 LAN 和 WAN 通訊埠的數量。您可能需要跳接纜線以進行內嵌部署。如果連線至 WAN 通訊埠和 LAN 通訊埠的一或兩個裝置 (交換器、防火牆) 具有自動 MDI/MDI-X，則不需要跳接纜線。
新密碼和主機網域名稱	為您開始啟動程序時輸入的管理員使用者指定新的安全密碼。此管理員使用者和密碼用於主控台存取，以使用啟動程序和指令行介面。 **附註：**此帳戶資訊不存在復原機制。確定保護好此資訊，以供日後使用。 為避免郵件繞送的問題，請不要單獨使用郵件網域作為主機名稱，例如 symantecexample.com。 主機名稱應該類似下列格式： `host6.symantecexample.com` 新密碼： _____ 主機網域名稱： _____ 請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

動作/項目	說明
為整合式 Dell Remote Access Controller (iDRAC) 選擇 IP 位址、子網路遮罩、預設閘道位址和密碼。僅限實體裝置。	乙太網路 1 用於入埠電子郵件，乙太網路 2 則用於離埠電子郵件。如果您不打算將該硬體裝置用於離埠掃描，則不需要指定乙太網路介面 2。 實體裝置上的整合式 Dell Remote Access Controller (iDRAC) 提供對硬體裝置的主控台存取。雖然已整合，iDRAC 仍是單獨的裝置，需要具備自己的網路位址，才能正常運作。存取 iDRAC 基於瀏覽器的介面需要密碼。 在 8380-S450 上，使用主機電腦的 IP 位址。8380-S450 硬體裝置上沒有 iDRAC。 乙太網路介面 1 的 IP 位址： _____ 乙太網路介面 1 的子網路遮罩： _____ 乙太網路介面 2 的 IP 位址： _____ 乙太網路介面 2 的子網路遮罩： _____ 預設閘道 (預設路由器) IP 位址： _____ 請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。
靜態 IP 位址	靜態 IP 位址用於郵件繞送。您可以設定多個靜態 IP 位址，也可以不設定任何靜態 IP 位址。 目的主機或網路的 IP 位址或 CIDR 區塊： 1. _____ 2. _____ 3. _____ 請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。
網域名稱伺服器 (DNS)	繞送電子郵件需要有 DNS。您可以使用 Internet 根 DNS 伺服器，或指定內部 DNS 伺服器。您最多可以擁有三個 DNS 伺服器。 DNS 伺服器 IP 位址： 1. _____ 2. _____ 3. _____ 請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

動作/項目	說明
硬體裝置角色	可用的選項如下： ■ 僅限掃描程式 ■ 僅限控管中心 ■ 掃描程式及控管中心 對於僅限掃描程式安裝，您需要提供管理掃描程式之控管中心的 IP 位址。 硬體裝置角色： _____ 控管中心的 IP 位址 (適用於僅限掃描程式安裝)： _____
有效的授權檔	在您完成賽門鐵克授權網頁上的授權資訊後，賽門鐵克會透過電子郵件將授權檔傳送給您。授權檔具有 .slf 尾碼。同一個授權檔可用於授權多個硬體裝置。 您必須可以從控管中心存取授權檔。 授權檔的檔案位置： _____ 請參閱第 38 頁的「註冊您的授權」。
代理伺服器主機名稱及通訊埠 (選用)	如果您使用代理伺服器與賽門鐵克通訊，則僅需提供代理伺服器資訊。 代理伺服器主機名稱： _____ 代理伺服器通訊埠： _____ 請參閱第 38 頁的「註冊您的授權」。
管理員電子郵件地址 (僅限控管中心組態)	如果啟用警示通知，Symantec Messaging Gateway 會將警示傳送至此地址。 管理員電子郵件地址： _____
NTP 伺服器 (選用)	您可以指定 Internet 或內部 NTP 伺服器來管理時間。您最多可以指定三個伺服器。 NTP 伺服器： 1. _____ 2. _____ 3. _____

動作/項目	說明
掃描程式角色	掃描程式角色如下： ■ 入埠和離埠郵件過濾 ■ 僅入埠郵件過濾 ■ 僅離埠郵件過濾 掃描程式角色： _____
掃描程式主機名稱或 IP 位址 (僅限掃描程式組態)	您必須提供掃描程式的主機名稱或 IP 位址。 掃描程式主機名稱或 IP 位址： _____
虛擬 IP 位址 (僅限掃描程式組態)	如果掃描程式執行多項功能 (例如入埠和離埠郵件過濾)，您必須具有多個乙太網路介面。您可以透過建立虛擬 IP 位址來建立多個乙太網路介面。 虛擬 IP 位址： _____ 網路遮罩： _____ 通訊埠： _____

表 2-3 列出了在您架構掃描程式以過濾入埠郵件時，需要備妥的資訊。

表 2-3 入埠郵件過濾檢查清單

項目	說明
入埠郵件位址	此位址是用於入埠郵件過濾的位址和通訊埠。 此位址很可能是乙太網路 1 的通訊埠的位址。 入埠郵件過濾 IP 位址： _____ 通訊埠： _____

項目	說明
入埠郵件接收	接受來自所有來源的郵件。 或 要接受其郵件之網域的 IP 位址或主機名稱： 1. _____ 2. _____ 3. _____
入埠本機郵件傳送	您可以指定特定的伺服器，也可以使用「啟用 MX 查詢」。 此伺服器通常是下游郵件伺服器，例如公司郵件伺服器。 您可以指定不限數目的伺服器來接受入埠郵件轉遞。 要接受郵件轉遞之郵件伺服器的 IP 位址： 1. _____ 通訊埠：_____ 2. _____ 通訊埠：_____ 3. _____ 通訊埠：_____ 或 「MX 查詢」主機名稱 (不使用 IP 位址)： _____
非本機郵件傳送	您可以使用 MX 查詢、新增主機，或使用現有的主機。 如果在掃描程式與 Internet 之間有獨立的閘道 MTA，請提供該 MTA 的主機名稱或 IP 位址與通訊埠。 主機名稱或 IP 位址： _____ 或 「MX 查詢」主機名稱： _____

項目	說明
本機網域	會將這些位址新增至**「本機網域」**清單。 網域或 IP 位址： 1. _____ 2. _____ 3. _____ 或 「MX 查詢」主機名稱： _____

表 2-4 列出了在您架構掃描程式以過濾離埠郵件時，需要備妥的資訊。

表 2-4 離埠郵件過濾檢查清單

已完成	項目	說明
_____	離埠郵件位址	此位址是用於離埠郵件過濾的位址和通訊埠。 此位址很可能是乙太網路 2 的通訊埠的位址。 離埠郵件過濾 IP 位址： _____ 通訊埠： _____
_____	離埠郵件接收	提供 IP 位址或網域。您可以指定多個位址和網域。 IP 位址或網域： 1. _____ 2. _____ 3. _____
_____	離埠本機郵件傳送	您可以指定特定的伺服器，也可以使用「啟用 MX 查詢」。 此伺服器通常是下游郵件伺服器，例如公司郵件伺服器。 要接受郵件轉遞之郵件伺服器的 IP 位址： _____ 或 「MX 查詢」主機名稱： _____

已完成	項目	說明
_____	非本機郵件傳送	您可以使用 MX 查詢、新增主機，或使用現有的主機。 如果在掃描程式與 Internet 之間有獨立的閘道 MTA，請提供該 MTA 的主機名稱或 IP 位址與通訊埠。 主機名稱或 IP 位址： _____ 或 「MX 查詢」主機名稱： _____

您的掃描程式該放置於哪裡

最佳實務準則是將 Symantec Messaging Gateway 掃描程式放置於其他過濾產品與 MTA 的前面，其理由如下：

- 過濾產品及 MTA 可以更改或移除已存在的郵件標頭，或修改郵件內文。Symantec Messaging Gateway 需要未經改變的郵件標頭及郵件內文，方能正確地過濾電子郵件。
- 如果您的掃描程式不在訊息閘道上，掃描程式可能會將閘道 MTA 的 IP 位址識別為垃圾郵件的來源。
- 當掃描程式位於內部 MTA 的下游時，某些信譽功能會無法正確運作。這些功能包括與 IP 位址相符的連線類別、快速通過和寄件者群組。為了確保正確識別所有內送 IP 位址且不與內部 IP 位址相混淆，請將掃描程式放置在訊息閘道上。

如果您打算將您的掃描程式放置於 MTA 的下游，請在設定硬體裝置時指定閘道 MTA 的 IP 位址。您也可以透過控管中心安裝後，再指定閘道 MTA 的 IP 位址。

如需有關如何透過控管中心指定閘道 MTA 的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

請參閱第 7 頁的「系統組態選項」。

影響效能的環境因素

環境因素會影響效能，包括特定部署的過去使用樣式。在您安裝硬體裝置之前，請收集與您的環境相關的資訊，以瞭解典型使用樣式。

外寄 SMTP 連線可能會導致額外負荷， 它們可能會在電子郵件因寄往可能無法立即接收新電子郵件的遠端郵件伺服器的情況下，促使磁碟佇列增大。磁碟上存放大型的佇列可能會使 MTA 的效能降低。若為較大型組織，則可在獨立的掃描程式上架構入埠和離埠郵件串流。

傳送和接收的郵件特性可影響效能，其中該注意的主要參數如下:

- 平均郵件大小
- 內含附件的郵件數目
- 平均的附件大小
- 附件的類型
- 在電子郵件流量中感染病毒的郵件比例

請參閱第 19 頁的「您的掃描程式該放置於哪裡」。

請參閱第 7 頁的「系統組態選項」。

會影響效能的功能

表 2-5 描述功能會如何影響效能以及如何補償效能需求。

表 2-5 會影響效能的功能

功能	如何會影響效能
政策群組	您可以定義政策群組，在每個政策群組中包含共用過濾需求的使用者。如果郵件具有分屬不同政策群組成員的多個收件者，則掃描程式會分割郵件(分成一或多個郵件)。多個政策群組的郵件分割，可能會使效能降低。因此，請視需要使用政策群組，但注意使用大量政策群組可能會影響效能。 如需有關政策群組的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。
掃描程式	當控管中心必須收集來自多個掃描程式的記錄和統計資料時，即會影響到效能。當您新增掃描程式時，請監控效能以確保新增的掃描程式並未造成效能降低至無法接受的程度。 如需有關掃描程式角色的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。
日誌	記錄層級愈高，控管中心必須透過網路合併的資料就越多。除非您需要進行疑難排解，否則可將記錄層級保持在相對較低的程度。您也可以設定較頻繁地清除日誌。 如需有關管理日誌資料庫大小的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。
報告	將已排程報告架構為在硬體裝置使用率低時執行。此種組態可有助於減少尖峰期間對於系統資源的需求。 請僅將所需報告的報告資料按所需時間進行儲存。 如需有關報告和儲存報告資料的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

功能	如何會影響效能
硬體裝置角色	在您將硬體裝置架構為「控管中心」和「掃描程式」時，該硬體裝置即需要資源來完成此兩種角色。在中、大型環境中，該組態即會降低效能。請考慮於個別的硬體裝置上設定「控管中心」和「掃描程式」。
垃圾郵件隔離所	Symantec Messaging Gateway 繞送至「垃圾郵件隔離所」的郵件愈多，「隔離所」就愈大，需要的處理也就愈多。 ■ 隔離的垃圾郵件不要超過您所需的數量。 ■ 請縮減「垃圾郵件隔離所」大小上限。您可以將已識別為垃圾郵件的郵件刪除，或是縮短保留垃圾郵件的時間。 如需有關垃圾郵件隔離所臨界值的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。 ■ 考慮僅針對可疑垃圾郵件使用隔離所。 ■ 考慮僅針對需要的使用者使用政策群組以隔離垃圾郵件。 存取「垃圾郵件隔離所」的使用者愈多，所需要的效能管理成本也就愈高。一般使用者隔離所比僅限管理員隔離所的費用更高。 ■ 當大量一般使用者登入以進行隔離管理時，控管中心效能會受到影響。僅限管理員存取「垃圾郵件隔離所」可明顯增加效能。 ■ 垃圾郵件隔離所通知器亦會增加控管中心額外負荷。 請確定您的系統已經過設定，可高效地處理垃圾郵件隔離所。 ■ 每個使用者清除程式臨界值使用的資源遠遠高於全域臨界值。 ■ 分散已排程工作 (特別是清除程式)，以便不會發生重疊。 ■ 請確定 LDAP 伺服器上具有足夠的容量。LDAP 會查詢郵件收件者，防止由於 LDAP 伺服器的容量有限而嚴重影響「垃圾郵件隔離所」的效能。 ■ 「垃圾郵件隔離所」的 SMTP 伺服器速度可能變慢。如果出現此情況，則當目的 MTA 接收郵件的速度變慢或完全無法接收時，掃描程式的傳送 MTA 即會進行備份。在此種情況下，某些合法的郵件訊息可能會延遲發送。
以文字為基礎的附件掃描	Symantec Messaging Gateway 可以掃描附件，以確定電子郵件訊息中是否有垃圾郵件。啟用此選項可能會導致 Symantec Messaging Gateway 的效能變慢。 依據預設，此選項會在新安裝 Symantec Messaging Gateway 時啟用，在進行升級時停用。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。
DKIM 簽署	啟用 DKIM 簽署會影響離埠郵件傳遞效能。使用較短的加密金鑰可降低此影響。
SMTP 驗證	SMTP 驗證會增加額外負荷，進而會影響到離埠郵件傳遞效能。

如需有關這些主題的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

掃描程式通訊埠組態範例

在您將硬體裝置架構為過濾入埠電子郵件及離埠電子郵件時，掃描程式需要下列其中一種組態：

- 兩個 IP 位址
- 一個 IP 位址和兩個 TCP 通訊埠
- 一個 IP 位址和一個 TCP 通訊埠

表 2-6 提供了您可以使用的一些通訊埠組態範例 (但它並未包含所有可能的 IP 位址及通訊埠)。

表 2-6 掃描程式通訊埠組態範例

通訊埠組態	範例 IP 位址及通訊埠	注意事項
■ 兩個實體通訊埠 (eth0 及 eth1) ■ 每個通訊埠有一個 IP 位址	192.0.32.1:25 192.0.47.255:25	硬體裝置會將入埠電子郵件及離埠電子郵件繞送到個別乙太網路通訊埠上。 此組態是大多數情況下的最佳選項，因為它提供最多的網路頻寬。
■ 一個實體通訊埠 ■ 一個 IP 位址 ■ 兩個不同的 TCP 通訊埠	192.0.32.1:25 192.0.32.1:50	硬體裝置會透過同一實體乙太網路通訊埠 (但使用兩個不同的 TCP 通訊埠) 來繞送入埠電子郵件及離埠電子郵件。 此組態可能造成網路瓶頸，但適用於電子郵件流量相對較低的網站。
■ 一個實體通訊埠 ■ 一個標準 IP 位址 ■ 一個虛擬 IP 位址	192.0.32.1:25 192.0.36.128:25	硬體裝置會透過同一實體乙太網路通訊埠來繞送入埠電子郵件及離埠電子郵件。此組態使用兩個不同的 IP 位址，其中一個為虛擬 IP 位址。 此組態可能造成網路瓶頸，但適用於電子郵件流量相對較低的網站。
■ 一個實體通訊埠 ■ 一個標準 IP 位址	192.0.32.1:25	硬體裝置會透過同一實體乙太網路通訊埠，並使用相同的 IP 位址來繞送入埠電子郵件及離埠電子郵件。 此組態可能造成網路瓶頸，但適用於電子郵件流量相對較低的網站。

請參閱第 11 頁的「安裝前準備」。

安裝工作流程

在安裝 Symantec Messaging Gateway 之前，請檢閱並完成安裝前工作。

表 2-7 Symantec Messaging Gateway 安裝工作流程

步驟	工作及說明
1	如需安裝硬體，請解除封裝硬體裝置、進行掛載，並連接適當的纜線。 請參閱第 24 頁的「安裝 8300 系列硬體裝置 」。 如需安裝 ，請透過 VMware vSphere Client 或 Microsoft Hyper-V 管理主控台存取 Symantec Messaging Gateway 虛擬機器。 請參閱第 27 頁的「在 VMware 上安裝 Symantec Messaging Gateway」。 或 請參閱第 32 頁的「在 Hyper-V 上安裝 」。
2	針對硬體，開啟硬體裝置。安裝精靈會引導您完成安裝程序。 若是在 VMware vSphere Client 中安裝 ，請於「Symantec Messaging Gateway 虛擬機器」上按下滑鼠右鍵，然後選取**「開機」**。 若是在 Microsoft Hyper-V 用戶端中安裝 ，請於「Messaging Gateway 虛擬機器」上按下滑鼠右鍵，然後選取**「啟動」**。 請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。
3	指定乙太網路設定。
4	為繞送指定 IP 位址。 此步驟為可選步驟。
5	為預設閘道及您的 DNS 伺服器指定 IP 位址。
6	指定硬體裝置的角色。
7	註冊您的授權。 請參閱第 38 頁的「註冊您的授權」。
8	如有必要，請使用最新的軟體更新 Symantec Messaging Gateway。 請參閱第 54 頁的「於安裝期間更新為最新軟體」。
9	安裝及架構控管中心。 請參閱第 40 頁的「架構控管中心」。
10	設定掃描程式。 根據下列其中一種情景設定掃描程式： ■ 當掃描程式與控管中心位於相同的硬體裝置上時，您可在設定控管中心後立即新增掃描程式。 請參閱第 40 頁的「架構控管中心」。 ■ 如果掃描程式與控管中心位於不同的硬體裝置上，您可透過控管中心安裝掃描程式。 請參閱第 41 頁的「透過控管中心新增掃描程式」。

3

安裝實體裝置

本章包含以下主題：

- 安裝 8300 系列硬體裝置
- 安裝 8380-S450 硬體裝置

安裝 8300 系列硬體裝置

本節說明如何設定 SMG 8380 硬體裝置，使其準備就緒以安裝軟體。

請參閱第 22 頁的「 安裝工作流程」。

設定硬體裝置硬體

1 打開硬體裝置的包裝，然後安裝在機架上或放置在平面上。

2 接著插上交流電源。

3 將乙太網路纜線插入 iDRAC 通訊埠，然後啟用 iDRAC。如需有關 iDRAC 的詳細資訊，請參閱 Dell 支援。

4 以下列任何一種方法連線硬體裝置：

- 將鍵盤和 VGA 顯示器連線到硬體裝置。
- 以序列埠將另一台電腦連線到硬體裝置。
  使用 DB9 接頭的虛擬數據機纜線，並設定為 9600 bps、8/N/1。
- 從遠端電腦透過 iDRAC 主控台連線到硬體裝置。

5 將乙太網路纜線連接到硬體裝置背面面板上標示為 **1** 的插孔。此插孔對應到 eth0。

對於離埠流量，將第二根纜線連接到硬體裝置背面標示為 **2** 的插孔。此插孔對應到 eth1。

請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

安裝 8380-S450 硬體裝置

本節說明如何設定 SMG 8380-S450 硬體裝置，使其準備就緒以安裝軟體。

設定硬體裝置硬體

1 打開硬體裝置的包裝，然後安裝在機架上或放置在平面上。

2 接著插上交流電源。

3 以下列任何一種方法連線硬體裝置：

- 將鍵盤和 VGA 顯示器連線到硬體裝置。
- 以序列埠將另一台電腦連線到硬體裝置。
  使用 DB9 接頭的虛擬數據機纜線，並設定為 9600 bps、8/N/1。

4 將乙太網路纜線連接到硬體裝置背面面板上標示為 **0:0** 的插孔。此插孔對應到 eth0。

對於離埠流量，將第二根纜線連接到硬體裝置背面標示為 **1:0** 的插孔。此插孔對應到 eth1。

請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

5 開啟程式，例如 Microsoft HyperTerminal®、PuTTY、Tera Term 或 ProComm™，並將其架構為使用下列設定：

傳輸速率：
9600 bps

資料位元數：8

同位檢查：
無

停止位元數：1

流量控制：
無

6 開啟硬體裝置。如果硬體裝置未自動開啟，請按下後面的軟電源開關。

7 BIOS 出現時，按下 CTRL C 以從磁碟開機。

8 顯示「您是否要切換模式?」問題時，請輸入「Y」。即開始安裝 SMG 軟體。在安裝完成時，硬體裝置會重新啟動並且會顯示提示。

4

安裝虛擬硬體裝置

本章包含以下主題：

關於 Symantec Messaging Gateway 虛擬版

Symantec Messaging Gateway 虛擬版 () 在 VMware ESXi 或 Microsoft Hyper-V Server 上安裝 Symantec Messaging Gateway。 以類似於獨立式硬體平台的方式在虛擬環境中執行。

您可以將 Symantec Messaging Gateway 部署為使用 ISO 影像或作業系統還原光碟的虛擬機器 (VM)。

- 請參閱第 27 頁的「在 ESXi Server 上建立虛擬機器 」。
  請參閱第 32 頁的「在 Hyper-V Server 上建立虛擬機器 」。
- 您可以在 ESXi/vSphere 上使用 OVF 將 Symantec Messaging Gateway 安裝為虛擬機器，用於示範或測試用途。賽門鐵克不建議在生產環境中的 ESXi/vSphere 上部署 OVF。
  請參閱第 30 頁的「在 ESXi/vSphere 上安裝 OVF 範本」。

附註：對於 Microsoft Hyper-V，Symantec Messaging Gateway 不支援 VHD。

本文件假設以下內容：

- 您的環境已具有可部署 64 位元架構的現有 VMware ESXi 或 Hyper-V Server 部署。
- 您熟悉管理虛擬機器。

- 您的環境符合系統需求的所有先決條件。確認在主機伺服器的 BIOS 中啟用 64 位元虛擬化。
  請參閱第 7 頁的「在 VMware 上部署的系統需求」。
  請參閱第 9 頁的「在 Microsoft Hyper-V 上部署的系統需求」。

如需有關 VMware 的詳細資訊，以及若要下載試用版軟體與必要條件應用程式，請造訪 VMware 網站，網址為 www.vmware.com。

如需有關 Microsoft Hyper-V 的詳細資訊，請造訪 Microsoft 網站，網址為 www.microsoft.com。

請參閱第 34 頁的「虛擬軟體術語」。

在 VMware 上安裝 Symantec Messaging Gateway

您可以使用 ISO 影像或作業系統還原光碟在 VMware 上安裝 。使用 VMware vSphere Client 存取 VMware ESXi Server。從 VMware 網站下載用戶端軟體，或者，若您的 VMware ESXi Server 已架構為允許 https 存取，也可直接從您的硬體裝置下載。

使用 VMware vSphere Client 啟動

1. 在 VMware vSphere Client 中，於**「Symantec Messaging Gateway 虛擬機器」**上按下滑鼠右鍵，然後從右鍵功能表中選取**「開機」**。
2. 在 VMware vSphere Client 中，選取 Symantec Messaging Gateway 虛擬機器，然後按下**「主控台」**標籤。

在 ESXi Server 上建立虛擬機器

您可以從 ISO 影像或作業系統還原光碟架構虛擬機器及部署 Symantec Messaging Gateway 的實例。您必須先建立 VMware ESXi/vSphere Server。

請參閱第 7 頁的「在 VMware 上部署的系統需求」。

使用管理介面建立虛擬機器時，請只在輸入欄位中使用 ASCII 字元。虛擬機器的顯示名稱和路徑不可包含非 ASCII 字元。建立虛擬機器的檔案名稱和目錄時不可使用空格字元。

最好確定將您的訪客電腦架構成當主機電腦重新啟動時一同重新啟動。如需詳細資訊，請查閱 VMware 文件。

附註：ESXi 預設會使用 DHCP，而且不會使用根密碼。賽門鐵克建議您在安裝之前，事先修改 ESXi 設定以建立根密碼，並指派靜態 IP 位址。

到 ESXi Server 上的虛擬機器

1. 選取您要放置虛擬機器的 ESXi Server。
2. 在**「檔案」**功能表中，按下**「新增」**，然後按下**「虛擬機器」**。
3. 選取**「一般安裝」**選項，然後按**「下一步」**。

4 輸入虛擬機器的名稱，然後按「**下一步**」。

5 選取資料儲存區選項，然後按「**下一步**」。請依據您的特定儲存組態執行此選擇。

6 選取虛擬機器版本。除非另有說明，否則請選取預設值。請參閱 VMware 文件。

7 在作業系統中，按下 **Linux** 作為「訪客作業系統」，並按下「**CentOS 4/5/6/7 (64 位元)**」作為「版本」。按「**下一步**」。

8 保留必要的磁碟空間，然後按「**下一步**」。

請參閱第 7 頁的「在 VMware 上部署的系統需求」。

依據部署情況的不同，您可能需要更多磁碟空間。保留磁碟空間並完成部署後，您必須重複執行作業系統還原程序，才能對磁碟空間進行任何變更。

9 在「**準備完成**」頁面上，勾選「**傳送前編輯虛擬機器設定**」，然後按下「**繼續**」。

10 按下左側的「**記憶體**」。依據部署需求來保留系統記憶體，然後按「**下一步**」。

請參閱第 7 頁的「在 VMware 上部署的系統需求」。

11 按下左側的 **CPU**。選取虛擬 CPU 的數目，然後按「**下一步**」。

12 如果要使用第二個網路介面，請按下最上方的「**新增**」，然後選擇「**乙太網路配接卡**」，按「**下一步**」，再次按「**下一步**」，然後按下「**完成**」。

13 按下「**完成**」。

14 繼續部署，以安裝虛擬硬體裝置。

請參閱第 28 頁的「從作業系統還原光碟在您的 ESXi Server 上安裝 SMG 」。

請參閱第 30 頁的「從資料儲存區在 ESXi Server 上安裝 SMG 」。

請參閱第 29 頁的「從本機電腦在 ESXi Server 上安裝 SMG 」。

從作業系統還原光碟在您的 ESXi Server 上安裝 SMG

在您將虛擬機器架構到 ESXi Server 後，即可使用作業系統還原光碟或 ISO 影像作為您的啟動程序媒體。

請參閱第 27 頁的「在 ESXi Server 上建立虛擬機器 」。

在 ESXi Server 上使用作業系統還原光碟啟動虛擬機器

1 將作業系統還原光碟插入 ESXi Server 的光碟機。

2 按下「**編輯虛擬機器設定**」。

3 在**硬體**標籤上，選取 **CD/DVD 光碟機 1**。

4 選擇「**主機裝置**」，並選擇 **CD**。

5 勾選「**在開機時連線**」並按下「**確定**」。

6 按下「開啟虛擬機器」圖示。

虛擬機器會立即從光碟機重新啟動。

7 按下「**中斷連接 CD/DVD**」，然後從光碟機中移除光碟，以避免系統執行其他作業系統還原。

賽門鐵克建議您在初始開機程序之後立即中斷開機媒體，以免不慎執行作業系統還原。

8 完成安裝程序後，透過用戶端將該電腦關機，然後編輯電腦設定。

9 在**硬體**標籤上，選取 **CD/DVD 光碟機 1**。

10 取消勾選「**在開機時連線**」並按下「**確定**」。

11 重新啟動電腦，以開始執行 Symantec Messaging Gateway 開機順序。

請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

請參閱第 22 頁的「 安裝工作流程」。

從本機電腦在 ESXi Server 上安裝 SMG

在您將虛擬機器架構到 ESXi Server 後，即可使用本機電腦上的 ISO 影像作為您的啟動程序媒體。

請參閱第 27 頁的「在 ESXi Server 上建立虛擬機器 」。

使用本機電腦上的 ISO 影像啟動虛擬機器

1 將 ISO 影像複製到本機硬碟。

2 按下「**編輯虛擬機器設定**」。

3 在「**硬體**」標籤上，選取「**新增 CD/DVD**」，並確定已選取「**用戶端裝置**」作為「裝置類型」。

4 在「**選項**」標籤上，選取「**開機選項**」，然後設定「**強制 BIOS 設定**」。

5 按下「**確定**」。新的虛擬機器會出現在詳細目錄中。

6 按下詳細目錄中的新虛擬機器，然後按下「**主控台**」。

7 按下「開啟虛擬機器」圖示。

8 如果使用的是 ISO 影像，請按下**「連線 CD/DVD」>「使用 ISO 影像」**，然後瀏覽至 ISO 影像。如果使用的是作業系統還原光碟，請選擇 CD/DVD 光碟機的代號。

將開始執行開機程序。

9 完成安裝程序後，將開始執行 Symantec Messaging Gateway 開機順序。

如果未開始執行 Symantec Messaging Gateway 開機順序，請先透過用戶端將電腦關機，再按下**「中斷連接 CD/DVD 裝置」**以中斷與 ISO 影像的連線，然後重新啟動電腦。

請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

請參閱第 22 頁的「 安裝工作流程」。

從資料儲存區在 ESXi Server 上安裝 SMG

在您將虛擬機器架構到 ESXi Server 後，即可使用資料儲存區上的 ISO 影像作為您的啟動程序媒體。

請參閱第 27 頁的「在 ESXi Server 上建立虛擬機器 」。

使用資料儲存區上的 ISO 影像啟動虛擬機器

1 在**「硬體」**標籤中，選取**「新增 CD/DVD」**，並勾選**「資料儲存區 ISO 檔案」**作為「裝置類型」。

2 按下**「瀏覽」**，然後選取資料儲存區中的 ISO 檔案。如果您尚未在資料儲存區中新增 ISO 影像，請參閱 VMware 文件瞭解相關程序。

3 勾選**「在開機時連線」**，然後按下**「完成」**。新的虛擬機器會出現在詳細目錄中。

4 開啟新電腦並存取主控台。將開始執行開機程序。

5 如果主控台提示您分割 SDA 裝置，請在主控台視窗上按下滑鼠，然後按 **Enter** 表示「Yes」。

6 完成安裝程序後，透過用戶端將該電腦關機，然後編輯電腦設定。

7 在**「硬體」**標籤上，選取**「CD/DVD 光碟機 1」**。

8 取消勾選**「在開機時連線」**並按下**「確定」**。

9 重新啟動電腦，以開始執行 Symantec Messaging Gateway 啟動程序。

請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

請參閱第 22 頁的「 安裝工作流程」。

在 ESXi/vSphere 上安裝 OVF 範本

賽門鐵克提供 OVF 範本用於示範或測試用途。如果您無法成功部署 OVF 範本，則可以使用作業系統還原磁碟進行示範或測試。

請參閱第 27 頁的「在 ESXi Server 上建立虛擬機器 」。

注意：只有在賽門鐵克代表明確告知的情況下，才可以在生產環境中使用 OVF 範本。對於任何生產環境，賽門鐵克建議您從 ISO 影像或作業系統還原磁碟進行安裝。

您可以在受支援的 VMware ESXi/vSphere Server 上安裝包含 的 OVF 範本。若要安裝 OVF 範本，請在非託管 ESXi Server 的電腦上使用 vSphere 或 vCenter 用戶端。最好確定將您的訪客電腦架構成當主機電腦重新啟動時一同重新啟動。如需詳細資訊，請查閱 VMware 文件。

部署 OVF 範本

1. 插入包含 OVF 範本的 DVD。如果您線上存取 OVF 檔案，請解壓縮該檔案。
2. 在 vSphere 或 vCenter 用戶端的**「檔案」**功能表中，按下**「部署 OVF 範本」**。
3. 在**「來源」**頁面上，按下**「從檔案部署」**。
4. 瀏覽並選取檔案 `Symantec_Messaging_Gateway_10.6.*.ovf`。
5. 按**「下一步」**。
6. 在**「OVF 範本詳細資料」**頁面上，按**「下一步」**。
7. 在**「名稱和位置」**頁面上，輸入您的部署的名稱，然後按**「下一步」**。
8. 在**「準備完成」**頁面上，按下**「完成」**。

   部署可能需要幾分鐘的時間。部署完成後，新的電腦會出現在清單中。
9. 從您的用戶端存取新的虛擬機器。開始執行標準 Symantec Messaging Gateway 開機順序。

   請參閱第 7 頁的「在 VMware 上部署的系統需求」。

Symantec Messaging Gateway 支援 VMware 工具

Symantec Messaging Gateway 虛擬硬體裝置支援一組數目有限的 VMware 工具。

僅支援的工具如下：

第二代 vmxnet 虛擬 NIC 驅動程式	此工具會在虛擬硬體裝置開機時自動載入。啟用此支援不需執行任何動作。 目前支援 vmxnet 1、2 和 3。
vmtoolsd 精靈	此工具會在虛擬硬體裝置開機時自動啟動。啟用此支援不需執行任何動作。vmtoolsd 精靈支援從 vSphere4 用戶端儀表板使用虛擬硬體裝置的自動關閉功能，vmtoolsd 精靈也支援訪客資訊服務 (Guest Information Service)。
vmmemctl	此工具可提供透明的頁面共用及重新取得訪客作業系統上未使用的記憶體。它也會啟用虛擬機器上的記憶體切換功能。

不支援其他的 VMware 工具功能。

請參閱第 26 頁的「關於 Symantec Messaging Gateway 虛擬版」。

在 Hyper-V 上安裝

使用 在 Hyper-V 虛擬機器上安裝 Symantec Messaging Gateway。

在 Hyper-V Server 上建立虛擬機器

您可以從在受支援 Windows Server 上執行 Standalone 或 Datacenter Hyper-V 之電腦上的 ISO 影像或作業系統還原光碟架構虛擬機器及部署 Symantec Messaging Gateway 的實例。首先，安裝 Hyper-V Server。

使用管理介面建立虛擬機器時，請只在輸入欄位中使用 ASCII 字元。虛擬機器的顯示名稱和路徑不可包含非 ASCII 字元。建立虛擬機器的檔案名稱和目錄時不可使用空格字元。

最好確定將您的訪客電腦架構成當主機電腦重新啟動時一同重新啟動。如需詳細資訊，請查閱 Microsoft 文件。

附註：Microsoft Hyper-V 不支援在虛擬部署中使用動態磁碟。請檢閱 Hyper-V 寄宿的設定，並將磁碟設定為固定磁碟。

建立 Hyper-V 虛擬機器

1. 按下您要放置虛擬機器的 Microsoft Hyper-V Server。
2. 在**「動作」**功能表中，按下**「新增」**，然後按下**「虛擬機器」**。
3. 按**「下一步」**，使用自訂組態建立虛擬機器。
4. 輸入虛擬機器的名稱，接著選取適合您環境的儲存資料夾，然後按**「下一步」**。
5. 依據部署需求指定系統記憶體的數量，然後按**「下一步」**。

   請參閱第 9 頁的「在 Microsoft Hyper-V 上部署的系統需求」。
6. 為網路配接卡選取虛擬交換機，然後按**「下一步」**。如果您需要額外的網路配接卡，可在完成新增虛擬機器精靈後，透過編輯虛擬機器設定來新增。
7. 若要將固定的硬碟新增至虛擬機器，請選取**「稍後附加虛擬硬碟」**，然後按**「下一步」**。
8. 按下**「完成」**。
9. 在新的虛擬機器上按下滑鼠右鍵並選取**「設定」**。
10. 將**「IDE 控制器 0」**反白，然後按下**「新增」**以將新硬碟新增到虛擬機器。
11. 按下**「新增」**建立新硬碟，然後按**「下一步」**。
12. 選取**「固定」**，然後按**「下一步」**。
13. 為新硬碟指定**「名稱」**和**「位置」**，然後按**「下一步」**。

14 保留必要的磁碟空間量，然後按「**下一步**」。

請參閱第 9 頁的「在 Microsoft Hyper-V 上部署的系統需求」。

依據部署情況的不同，您可能需要更多磁碟空間。保留磁碟空間並完成部署後，您必須重複執行作業系統還原程序，才能對磁碟空間進行任何變更。

15 按下「**完成**」，然後按下「**確定**」。

16 繼續部署，以安裝虛擬硬體裝置。

請參閱第 33 頁的「使用作業系統還原光碟在 Hyper-V 虛擬機器上安裝 」。

請參閱第 33 頁的「使用 ISO 影像在 Hyper-V 上安裝 」。

使用 ISO 影像在 Hyper-V 上安裝

在您將虛擬機器架構到 Microsoft Hyper-V Server 後，即可使用 Hyper-V Server 上的 ISO 影像作為您的啟動程序媒體。

請參閱第 32 頁的「在 Hyper-V Server 上建立虛擬機器 」。

使用 ISO 影像在 Hyper-V 上安裝

1 將 Symantec Messaging Gateway 安裝 ISO 複製到 Hyper-V Server 上。

2 在新的 Microsoft Hyper-V 虛擬機器上按下滑鼠右鍵並選取「**連線**」。

3 選取「**媒體**」功能表。

4 選取「**DVD 光碟機**」>「**插入光碟片...**」。

5 選取「Symantec Messaging Gateway 安裝 ISO」，然後按下「**開啟**」。

6 啟動虛擬機器，開始執行 Symantec Messaging Gateway 開機順序。

請參閱第 22 頁的「 安裝工作流程」。

在 Microsoft Hyper-V Hypervisor 上啟動

1 透過 Microsoft Hyper-V Microsoft 管理主控台存取 Microsoft Hyper-V Server。您可以從 Microsoft 網站下載此軟體。

2 在 Microsoft Hyper-V Microsoft 管理主控台中，於 Symantec Messaging Gateway 虛擬機器上按下滑鼠右鍵，然後從右鍵功能表中選取「**啟動**」。

3 在 Microsoft Hyper-V Microsoft 管理主控台中，選取 Symantec Messaging Gateway 虛擬機器，然後按下滑鼠右鍵並選取「**連線**」。

使用作業系統還原光碟在 Hyper-V 虛擬機器上安裝

在您將虛擬機器架構到支援的 Microsoft Windows Hyper-V Server 後，即可使用作業系統還原光碟或 ISO 影像安裝 。

請參閱第 32 頁的「在 Hyper-V Server 上建立虛擬機器 」。

使用作業系統還原光碟在 Hyper-V 虛擬機器上安裝

1. 將作業系統還原光碟插入 Hyper-V Server 的 CD/DVD 光碟機。
2. 在新的 Microsoft Hyper-V 虛擬機器上按下滑鼠右鍵並選取**「連線」**。
3. 選取**「媒體」**功能表。
4. 選取**「DVD 光碟機」>「插入光碟片...」**。
5. 在 CD/DVD 光碟機中選取「Symantec Messaging Gateway 安裝光碟」，然後按下**「開啟」**。
6. 啟動虛擬機器，開始執行 Symantec Messaging Gateway 開機順序。

   請參閱第 36 頁的「執行啟動程序以架構硬體裝置 」。

   請參閱第 22 頁的「 安裝工作流程」。

Symantec Messaging Gateway 支援 Hyper-V 工具

Symantec Messaging Gateway 虛擬硬體裝置支援一組數目有限的 Hyper-V 工具。

僅支援的工具如下：

hv_netvsc	此工具支援 Hyper-V 專用 (或「虛擬」) 網路配接卡。
hv_storvsc	此工具支援所有儲存裝置。
hv_vmbus	此工具是執行 Hyper-V 與虛擬機器的伺服器之間的快速通訊通道。
hv_utils	此工具提供整合式關機、索引鍵-值對資料交換和活動訊號。

請參閱第 26 頁的「關於 Symantec Messaging Gateway 虛擬版」。

虛擬軟體術語

與虛擬軟體相關的關鍵術語如下所示：

虛擬機器	虛擬機器 (VM) 是可讓應用程式堆疊不受實體硬體影響的軟體。
Intel 虛擬化技術	亦稱為 Intel-VT。在 BIOS 中啟用以支援多個作業系統，包括 64 位元架構。在許多 Intel 處理器上，可能會在 BIOS 中停用此設定。在安裝 Symantec Messaging Gateway 之前已啟用此設定。 **附註：**支援 64 位元架構的 AMD 處理器通常預設為啟用此設定。
主機電腦作業系統	主機電腦或作業系統 (OS) 是執行訪客電腦/作業系統的實體硬體和主要作業系統。
訪客電腦作業系統	虛擬機器上安裝的作業系統。 是訪客電腦和作業系統。

VMware ESXi Server	VMware ESXi 是企業級的虛擬機器平台。
Microsoft Hyper-V Server	Microsoft 分派的原生 Hypervisor。它支援在 x86-64 系統上實現平台虛擬化。
虛擬電腦影像	一組 VMware 專屬格式的檔案，其中包含預先架構的虛擬機器和的影像。此影像可以用來將虛擬機器安裝在執行 VMware ESXi Server 的主機電腦上。
ISO 影像或作業系統還原光碟	這是可讓您將 Symantec Messaging Gateway 安裝於執行 VMware ESXi Server 之電腦的影像。
OVF 範本	包括一組軟體的虛擬機器。例如，OVF 範本可以包括 Symantec Messaging Gateway 軟體。
VHD 範本	包括一組軟體的 Microsoft Hyper-V 虛擬機器。 **附註：**Symantec Messaging Gateway 軟體不可用作 VHD 範本。
vSphere 用戶端	連線至 VMWare ESXi Server 的桌面虛擬機器平台。
Microsoft Management Console	管理員可從中管理 Hyper-V Server 的擴展 Windows 主控台。

請參閱第 26 頁的「關於 Symantec Messaging Gateway 虛擬版」。

5

執行啟動程序

本章包含以下主題：

執行啟動程序以架構硬體裝置

啟動程序可架構您的實體 Symantec Messaging Gateway 硬體裝置。您可以將硬體裝置架構為控管中心、網路掃描程式或全功能硬體裝置(同一硬體裝置上的控管中心和掃描程式功能)。它會為管理通訊埠指派靜態 IP 位址，並設定硬體裝置與網路之間的通訊。完成啟動程序後，系統會自動重新啟動。

在本節，您將：

- 指定乙太網路介面
- 為繞送指定靜態 IP 位址
- 指定閘道和 DNS 設定，以及
- 設定硬體裝置的角色

執行啟動程序

1. 開啟硬體裝置上的主控台視窗。
2. 使用登入名稱 `admin` 和密碼 `symantec` 登入。

   當您在架構前首次登入時，啟動程序會自動開始。
3. 收到提示時，輸入新密碼兩次。
4. 收到提示時，輸入此主機完整的網域名稱。

   為避免郵件繞送的問題，請不要使用郵件網域作為主機名稱，例如symantecexample.com。該名稱應該類似下列格式：

   ```
   host6.symantecexample.com
   ```

5 在您收到提示時，請輸入時區的編碼。

輸入 **?** 以顯示時區的清單。

按下空白鍵以捲動清單或輸入 **Q** 以結束清單。

6 收到提示時，請輸入硬體裝置背面標示為 **1** 的乙太網路介面的 IP 位址。

7 收到提示時，請輸入乙太網路介面 1 的子網路遮罩。

8 當系統提示您是否要使用第二個乙太網路介面 interface 2 時，請輸入 **Yes** 或 **No**。

如果輸入 Yes，收到提示時，請輸入乙太網路介面 2 的 IP 位址。

如果輸入 **No**，請跳至步驟 10。

9 收到提示時，請輸入乙太網路介面 2 的子網路遮罩。

10 當系統提示您是否要新增繞送的靜態 IP 位址時，請輸入 **Yes** 或 **No**。

如果輸入 Yes，收到提示時，請指定目的主機或網路的 IP 位址或 CIDR 區塊。

如果輸入 **No**，請移至步驟 13。

11 架構多個乙太網路介面時，會收到指定乙太網路介面編號 (1 或 2，預設為 1) 的提示。本設定會強迫路由與指定的裝置相關聯。

12 當系統提示您是否要新增其他靜態 IP 位址時，請輸入 **Yes** 或 **No**。

如果輸入 Yes，請重複步驟 10。

13 收到提示時，請輸入預設閘道 (預設路由器) 的 IP 位址。

14 收到提示時，請輸入 DNS 伺服器的 IP 位址。

15 當系統提示您是否要輸入其他 DNS 伺服器時，請輸入 **Yes** 或 **No**。

如果輸入 Yes，請輸入 IP 位址。

16 若要繼續安裝，接下來您需指定硬體裝置的角色。

17 在收到提示時，請為該硬體裝置選擇下列任何一種角色：

- 僅限掃描程式
- 僅限控管中心
- 掃描程式及控管中心

18 對於**「僅限掃描程式」**，在收到提示時，輸入您想要用來管理本掃描程式的控管中心的 IP 位址。

19 此時會顯示您已輸入的資訊。

如果資訊不正確，請輸入 **No**。您可以回到程序的開始，以進行變更。

如果資訊正確，請輸入 **Yes**。啟動程序已完成，且硬體裝置重新啟動。在硬體裝置重新啟動之後，您可以註冊您的硬體裝置。

6

執行安裝精靈

本章包含以下主題：

執行安裝精靈

(Symantec Messaging Gateway) 安裝精靈可引導您完成全功能、掃描程式或僅限控管中心硬體裝置的必要組態步驟。您將硬體裝置開機後，便會執行安裝精靈。

在本節，您將：

- 上傳並註冊產品授權
- 設定管理員電子郵件地址、警示通知、位置以及時間設定
- 透過控管中心新增並架構掃描程式

此設定包含建立第一個管理員帳戶，以便您可以登入控管中心。啟動程序中的主控台管理員帳戶獨立於安裝精靈中的管理帳戶。

註冊您的授權

賽門鐵克為您提供授權檔。將此檔案放置在存取控管中心的電腦上。每次新增掃描程式，您必須確認授權或再次註冊。您可以對每個掃描程式使用相同的授權檔。

附註：針對您的掃描程式，確保您的網路架構為允許在通訊埠 443 上離埠連線至賽門鐵克。Symantec Messaging Gateway 透過安全連線與賽門鐵克安全機制應變中心進行通訊，以進行產品註冊和持續運營。

當執行硬體裝置的初始設定時，重新啟動硬體裝置後，安裝精靈中會出現下列步驟。

請參閱第 22 頁的「 安裝工作流程」。

註冊您的授權

1 在可以存取硬體裝置的電腦上開啟瀏覽器，然後登入 SMG。

預設的登入位址如下：

https://<hostname>

其中 <hostname> 為 IP 位址，或在設定期間指定給硬體裝置的主機名稱。

若要使用 HTTP，則必須經由指令行介面啟用 HTTP 並指定通訊埠 41080。

如需有關 http 指令的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

2 在「控管中心」登入頁面，以 admin 使用者登入並使用在初始設定時指定的密碼。

3 在**「使用者授權許可協議」**頁面上，按下**「我接受授權許可協議的條款」**，然後按**「下一步」**。

4 在**「授權註冊資訊」**頁面，按下**「瀏覽」**找出授權檔。

5 選取授權檔，並按下**「開啟」**，返回**「授權註冊」**頁面。

6 如果掃描程式要使用代理伺服器與賽門鐵克通訊，請按下**「代理伺服器」**。

7 若要指定代理伺服器，請勾選**「使用 HTTP 代理伺服器」**並輸入伺服器主機名稱與通訊埠。請視需要，輸入使用者名稱和密碼。

8 按下**「註冊授權」**。

若註冊成功，將返回**「授權註冊資訊」**頁面。

9 如果註冊失敗，則可能代理伺服器無法存取、通訊埠 443 已關閉，或者授權檔過期、遺失或損毀。

若要疑難排解授權註冊失敗，在「授權資訊註冊」頁面中，按下**「公用程式」**。

在**「公用程式」**欄位下拉式功能表中，選取**「路徑追蹤」**或**「連線偵測」**。然後，在**「主機名稱或 IP 位址」**欄位中，輸入主機名稱或 IP 位址。

請確定您可連線至 https://register.brightmail.com。

按下**「執行」**。結果會出現在**「結果」**文字方塊中。

按下**「註冊授權」**。

完成註冊。

10 如果您有其他不同功能的授權檔，請重複此程序，替每個授權註冊。

11 當所有授權檔皆已成功註冊時，請按「**下一步**」。

如果軟體是最新的，則會顯示安裝精靈。繼續安裝程序。

如果有軟體更新可用，則會顯示「**軟體更新**」頁面。

請參閱第 54 頁的「於安裝期間更新為最新軟體」。

架構控管中心

在您註冊授權或完成軟體更新後，安裝精靈中將顯示「**管理員設定**」頁面。

請參閱第 38 頁的「註冊您的授權」。

請參閱第 54 頁的「於安裝期間更新為最新軟體」。

請參閱第 22 頁的「 安裝工作流程」。

請先架構控管中心，然後再架構任何掃描程式。如果您已指定此硬體裝置作為控管中心和掃描程式，則精靈會繼續進行掃描程式設定。

架構控管中心

1 在「**管理員設定**」頁面上，輸入管理員的電子郵件地址。

2 勾選「**接收警示通知**」，讓 Symantec Messaging Gateway 將警示通知傳送到此地址。

您可以針對疫情、垃圾郵件和病毒過濾、郵件佇列、磁碟空間、SMTP 驗證、目錄、授權、軟體更新和事件設定警示通知。事件包括已排程工作、服務、硬體、交換空間和 UPS 問題。

您可以稍後在控管中心新增其他管理員或修改此管理員的設定。

如需有關設定本機和 LDAP 管理員帳戶以及編輯管理員的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

3 按「**下一步**」。

4 在「**時間設定**」頁面上，若要確認「**目前的硬體裝置時間**」區域中顯示的日期是否正確，請選取下列其中一個選項：

不要變更時間	時間正確，您不希望進行變更。此選項為預設設定。
手動設定時間	您希望手動變更時間。在「**日期**」和「**設定時間**」欄位中輸入正確的值。
使用 NTP 伺服器	您希望使用 NTP 伺服器來管理時間。輸入最多三個 NTP 伺服器的 IP 位址。

5 按「**下一步**」。

6 在「**系統地區設定**」頁面上，指定硬體裝置應該用於設定數字、日期和時間格式的地區設定。此設定為 Symantec Messaging Gateway 用於郵件的語言及地區格式設定。

7 接受預設的「**隔離遞補語言編碼**」格式，或從下拉式清單中選取一種格式。

遞補語言編碼是您在「**系統地區設定**」欄位中指定的格式設定失敗時，Symantec Messaging Gateway 用於已隔離郵件的格式。

8 按「**下一步**」。

如果您的硬體裝置已設定為控管中心和掃描程式，則會出現「**掃描程式角色**」頁面。選取掃描程式角色。

如果您將硬體裝置設定為僅作為控管中心，則「**安裝摘要**」頁面將列出您選取的組態選項。

9 在「**安裝摘要**」頁面上，選取下列任何一個選項：

- **完成**：您滿意設定，不希望進行變更。
- **上一步**：返回修改您的設定。
- **取消**：結束設定程序，而不儲存變更。在完成設定之前，無法使用硬體裝置。

10 如果您的掃描程式不在控管中心上，請在單獨的硬體裝置上設定掃描程式。您可以透過控管中心執行此任務。

請參閱第 41 頁的「新增並架構掃描程式 」。

新增並架構掃描程式

您必須具備完整的管理權限或管理設定修改權限，才能新增掃描程式。

附註：在精靈的最後一個步驟按下「**完成**」後，您在精靈的整個過程中指定的全部設定才算完成。

透過控管中心新增掃描程式

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

2 如果該掃描程式是您要新增的第一個掃描程式，則會出現「**新增掃描程式**」精靈。否則，請在「**主機組態**」頁面上(於「**重新架構掃描程式或控管中心主機**」底下)，依次按下「**新增**」和「**下一步**」。

3 在「**掃描程式主機設定**」頁面上，輸入新掃描程式的說明以及主機名稱或 IP 位址，然後按「**下一步**」。

4 在「**授權註冊**」頁面上，按下「**瀏覽**」找出授權檔。

5 選取授權檔，並按下「**開啟**」，返回「**授權註冊**」頁面。

6 如果掃描程式要使用代理伺服器與賽門鐵克通訊，請按下**「代理伺服器」**。

若要指定代理伺服器，請勾選**「使用 HTTP 代理伺服器」**並輸入伺服器主機名稱與通訊埠。

7 按下**「註冊授權」**。

若註冊成功，將返回**「授權註冊」**頁面。

8 如果在「授權資訊註冊」頁面上註冊失敗，則按下**「公用程式」**以進行疑難排解。

在**「公用程式」**欄位下拉式功能表中，選取**「路徑追蹤」**或**「連線偵測」**。然後，在**「主機名稱或 IP 位址」**欄位中，輸入主機名稱或 IP 位址。

請確定您可連線至 https://register.brightmail.com。

按下**「執行」**。結果會出現在**「結果」**文字方塊中。

按下**「註冊授權」**。

完成註冊。

9 如果您有其他不同功能的授權檔，請重複此程序，替每個授權註冊。

10 當所有授權檔皆已成功註冊時，請按**「下一步」**。

如果您的軟體需要更新，則會出現**「軟體更新」**頁面。請參閱第 54 頁的「於安裝期間更新為最新軟體」。

11 基於其功能架構掃描程式。

12 在**「掃描程式角色」**頁面上，按下下列其中一項，然後按**「下一步」**：

- **入埠和離埠郵件過濾**
- **離埠郵件過濾**
- **入埠郵件過濾**

13 如果在初始設定期間只架構一個 IP 位址，則會出現**「建立選用的虛擬 IP 位址」**頁面。

- 如果不想要建立虛擬 IP 位址，請選取**「否」**。繼續執行步驟 17。
- 如果您想要建立虛擬 IP 位址，請選取**「是」**。

14 按**「下一步」**。

15 在「**建立虛擬 IP 位址**」頁面上，執行下列所有項：

乙太網路	按下以選取乙太網路介面。
IP 位址	輸入虛擬伺服器的 IP 位址。
子網路遮罩	輸入子網路遮罩 IP 位址。
網路	輸入網路 IP 位址。
廣播	輸入廣播 IP 位址。

16 按「**下一步**」。

17 視情況需要，在下列畫面上選取或輸入：

- 用於入埠和離埠郵件過濾的 IP 位址。
- 用於入埠和離埠郵件過濾的 SMTP 通訊埠的通訊埠號。
- 此掃描程式應從中接受入埠郵件的郵件伺服器的 IP 位址。
- 接受其郵件的本機網域。
- 指定此掃描程式在過濾完成後，應將本機網域郵件轉送到的內部主機，或勾選「**啟用此主機的 MX 查詢**」。如果您啟用 MX 查詢，請指定主機名稱 (而非 IP 位址)。

18 若要修改清單，請執行下列任一工作：

新增位址	在「**接受入埠郵件的網域或電子郵件地址**」欄位中輸入位址，然後按下「**新增**」。 對於新增的每個網域位址或電子郵件地址，您也可以指定是否應透過特定的主機和通訊埠來繞送郵件。新增該資訊至「**選擇性地繞送至下列目的主機**」及「**通訊埠**」欄位。
刪除位址	勾選想要移除的位址，然後按下「**刪除**」。
匯入位址清單	按下「**匯入**」，然後瀏覽至現有檔案。
根據所指定主機名稱的MX記錄繞送郵件	勾選「**啟用 MX 查詢**」。如果您啟用了 MX 查詢，則必須指定主機名稱 (不是 IP 位址)。 例如，如果您架構多個下游郵件伺服器並將 MX 記錄用於電子郵件負載平衡，請啟用 MX 查詢。

19 在「**郵件過濾 - 郵件傳送**」頁面上，輸入主機名稱或 IP 位址和通訊埠，以指定轉遞本機網域過濾的郵件方式。

20 或者，勾選「**啟用此主機的 MX 查詢**」。

21 在**「郵件過濾 - 非本機郵件傳送」**頁面上，選取下列其中一個選項，以指定希望如何轉遞已過濾的郵件：

使用預設 MX 查詢	您希望使用 MX 查詢為任何網域傳回主機。
定義新主機	您希望指定新主機。輸入主機名稱或 IP 位址及通訊埠。如果掃描程式位於閘道，賽門鐵克建議您勾選**「啟用此主機的 MX 查詢」**。如果您選擇此選項，請指定主機名稱 (而非 IP 位址)。
使用現有的主機	您希望使用現有的主機。從下拉式清單中選取一台主機。如果在掃描程式與 Internet 之間有獨立的閘道 MTA，請提供該 MTA 的主機名稱或 IP 位址與通訊埠。

22 按**「下一步」**。

23 在**「安裝摘要」**頁面上，檢閱您的設定，並選取下列其中一個選項：

完成	您對設定感到滿意，希望將其儲存。
上一步	您希望修改設定。返回並修改您的設定。
取消	您希望取消變更，且不儲存變更。

7

完成安裝

本章包含以下主題：

安裝後工作

表 7-1 列出了您在安裝 Symantec Messaging Gateway 之後可以執行的選擇性工作。

表 7-1 安裝後工作

工作	說明
修改 DNS MX 記錄，以確保過濾過郵件。	在接收入埠郵件的個別 MTA 前面使用 Symantec Messaging Gateway 時，修改 DNS 郵件交換 (MX) 記錄。 請參閱第 46 頁的「調整 MX 記錄以確保過濾郵件」。
修改預設過濾政策。	請參閱第 47 頁的「關於郵件過濾政策 」。

工作	說明
測試防毒過濾。	請參閱第 47 頁的「測試防毒過濾 」。
測試郵件傳送。	請參閱第 48 頁的「測試合法電子郵件的傳送 」。
測試垃圾郵件過濾。	如果過濾垃圾郵件，請測試垃圾郵件過濾是否正常運作。 請參閱第 48 頁的「測試垃圾郵件過濾 」。
測試垃圾郵件隔離所。	如果您已將 Symantec Messaging Gateway 架構為使用垃圾郵件隔離所，請驗證是否已正確隔離郵件。 請參閱第 49 頁的「測試垃圾郵件是否已經隔離 」。
微調功能以提高效能。	某些功能比其他功能對效能的影響更大。安裝硬體裝置後，您可能想要微調這些功能以避免效能問題。 請參閱第 20 頁的「會影響效能的功能 」。
為電子郵件通知指定管理員電子郵件地址。	在安裝期間，您向管理員提供一個電子郵件地址，Symantec Messaging Gateway 會向該地址傳送警示。但是，此地址不會自動成為已排程報告的電子郵件通知寄件者地址。在安裝後，您可以指定要用於電子郵件報告通知的寄件者地址。 如需更多詳細資料，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

調整 MX 記錄以確保過濾郵件

當您於接收入埠郵件的個別 MTA 前面實作 Symantec Messaging Gateway 時，必須變更 DNS 郵件交換 (MX) 記錄，以便將內送郵件指向 Symantec Messaging Gateway 掃描程式。

如果您將 Symantec Messaging Gateway 列示為除了現有 MX 記錄之外，具有較高權重的 MX 記錄，則垃圾郵件寄發者可查詢上一個 MTA 的 MX 記錄。如果垃圾郵件寄發者擁有上一個 MTA 的 MX 記錄，即可將垃圾郵件直接傳送至舊有的伺服器並略過垃圾郵件過濾。

若要避免垃圾郵件寄發者攻陷新的垃圾郵件過濾伺服器，請執行下列其中一項工作：

- 將 MX 記錄指向 Symantec Messaging Gateway 掃描程式。不要指向下游 MTA 中的 MX 記錄。從 DNS 移除上一個 MTA 的 MX 記錄。
- 透過防火牆將前一個 MTA 與 Internet 隔開。
- 修改防火牆的網路位址轉譯 (NAT) 表，將外部 IP 位址繞送至內部無法繞送的 IP 位址。 然後，您可以從舊伺服器對應到 Symantec Messaging Gateway。

在命名 Symantec Messaging Gateway 時，請確保所選名稱並未暗示其功能。例如，antispam.yourdomain.com、symantec.yourdomain.com 或 antivirus.yourdomain.com 皆不是好的選擇。

如果想要傳送郵件至下游 MTA，您可以指定下游負載平衡器。

關於郵件過濾政策

Symantec Messaging Gateway 藉由預設的郵件過濾政策進行安裝。您可以使用這些政策，或自訂政策。

初始的預設政策如下：

- 預設政策群組包括所有使用者，並針對垃圾郵件、可疑垃圾郵件、不必要的電子郵件及惡意軟體指定預設的過濾政策。
- 預設的垃圾郵件政策會在郵件主旨行開頭加上 [Spam] 文字，並將郵件傳送至收件匣。
- 預設的可疑垃圾郵件政策會在郵件主旨行開頭加上 [Suspected Spam] 文字，並將郵件傳送至收件匣。
- 下列針對不想要的電子郵件的預設政策僅適用於入埠郵件，且不會指派給預設政策群組：

行銷郵件	預設的行銷電子郵件政策會在郵件主旨行前面加上 [Marketing Mail] 文字，並將郵件傳送至收件匣。
電子報	預設的電子報政策會在郵件主旨行前面加上 [Newsletter] 文字，並將郵件傳送至收件匣。
可疑 URL 內容	包含可疑 URL 之電子郵件的預設政策會在郵件主旨行前面加上 [Caution: Message contains Suspicious URL Content] 文字，並將郵件傳送至收件匣。

- 可疑垃圾郵件臨界值設定為 72。
- 預設的惡意軟體政策會清除相關郵件。
- 預設的病蟲政策會刪除相關郵件。
- 未提供預設的內容過濾政策。
- 未提供使用者組態功能。

如需有關架構政策與設定的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

測試防毒過濾

您可以藉由傳送含有虛擬病毒的測試郵件，確認防毒過濾功能是否正常運作。虛擬病毒並不是真的病毒。

測試防毒過濾

1 在電子郵件用戶端 (如 Microsoft Outlook) 中，建立新電子郵件。

2 將電子郵件的地址設定為測試帳戶，使該帳戶的政策可以清除感染病毒的郵件。

3 在電子郵件中附加病毒測試檔，例如 `eicar.com`。

病毒測試檔位於

http://www.eicar.org/

4 傳送郵件。

5 將一封未含病毒的郵件傳送至同一電子郵件地址。

6 幾分鐘後，在控管中心內按下**「狀態」>「儀表板」**。

通常，幾分鐘即足以更新控管中心上的統計資料。

如果防毒過濾功能正常運作，在**「儀表板」**頁面上的**「病毒」**計數器會加一。

7 檢查測試帳戶的信箱，確認收到內文說明已清除病毒的郵件。

測試合法電子郵件的傳送

您可透過將電子郵件傳送給某位使用者，確認您偏好使用的電子郵件程式是否與掃描程式正常運作以傳送合法郵件。

測試合法電子郵件的傳送

1 在電子郵件用戶端 (如 Microsoft Outlook) 中，建立新電子郵件。

2 將電子郵件的地址設定為有效的使用者。

3 給郵件一個容易尋找的主旨，例如 **Normal Delivery Test**。

4 傳送郵件。

5 確認測試郵件正確到達本機的正常傳送位置。

測試垃圾郵件過濾

此測試假設您為使用預設的安裝設定值，來處理垃圾郵件。

測試垃圾郵件過濾

1 在您的 Mail Delivery Agent (MDA) 上建立 POP3 帳戶。

針對此帳戶的 SMTP 伺服器設定，指定啟用掃描程式的 IP 位址。

2 編寫電子郵件訊息，並將地址設定為在執行該掃描程式電腦上的帳戶。

3 給此郵件一個容易尋找的主旨，例如 **Test Spam Message**。

4 為了將此郵件分類為垃圾郵件，請在郵件內文中包含下列 URL：

http://www.example.com/url-1.blocked/

5 傳送郵件。

6 檢查傳送郵件的目標電子郵件帳戶。

您應該會找到一則主旨相同，其前置文字為 [Spam] 的郵件。

7 將不是垃圾郵件的郵件傳送至同一地址。

8 幾分鐘後，在控管中心內按下**「狀態」>「儀表板」**。

如果垃圾郵件過濾功能正常運作，在**「儀表板」**頁面上的**「垃圾郵件」**計數器會加一。

測試垃圾郵件是否已經隔離

您可以架構 Symantec Messaging Gateway 將垃圾郵件和可疑垃圾郵件轉寄至「垃圾郵件隔離所」。當您完成上述架構，使用者即會在其「垃圾郵件隔離所」中看見垃圾郵件和可疑垃圾郵件。

附註：根據您組織接收到的垃圾郵件數量，第一封垃圾郵件可能會被延遲。

預設的組態會將 [Spam] 插入垃圾郵件的主旨行中，再傳送至使用者的收件匣內，而非「垃圾郵件隔離所」。

測試垃圾郵件是否已經隔離

1 在電子郵件用戶端 (如 Microsoft Outlook) 中，建立新電子郵件。

2 將電子郵件的地址設定為屬於某個已架構過濾垃圾郵件至「垃圾郵件隔離所」之群組的帳戶。

3 給此郵件一個容易尋找的主旨，例如 **Test Spam Message**。

4 為了將此郵件分類為垃圾郵件，請將下列 URL 獨立成行：

http://www.example.com/url-1.blocked/

5 傳送郵件。

6 將郵件傳送至非垃圾郵件亦不含病毒的同一個帳戶。

7 在控管中心內，按下**「垃圾郵件」>「隔離所」>「垃圾郵件」**。

8 按下**「顯示過濾器」**，然後在**「主旨:」**方塊中輸入 **Test Spam Message**。

9 按下**「顯示已過濾」**。如果「垃圾郵件隔離所」架構正確，您傳送的測試垃圾郵件應該會在結果清單當中出現。

若要釋放已隔離的郵件，請選取該郵件並按下「釋放」。

確認該郵件已傳送。

登入與登出

一般使用者可透過控管中心管理其「垃圾郵件隔離所」、個人的「允許的寄件者」清單、「攔截的寄件者」清單及電子郵件語言設定。使用控管中心可以架構 LDAP 來源、啟用 LDAP 驗證，以及啟用上述功能。

附註：請勿為管理員建立與使用者帳戶名稱相同的帳戶。反之，也請不要為使用者建立與管理員帳戶名稱相同的帳戶。如果發生命名衝突，則管理員登入將會取得優先權，而拒絕使用者存取其帳戶。如果管理員和使用者具有相同的密碼和使用者名稱，則使用者將有權存取管理員帳戶。

若要以具有 Active Directory、Oracle、Domino 或其他 LDAP 目錄伺服器帳戶的使用者身分登入，您的管理員必須對控管中心啟用 LDAP 驗證。

如需有關管理管理員的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

以管理員身分登入

1 從瀏覽器存取控管中心。

預設的登入位址如下：

https://<hostname>

其中 <hostname> 為指定給硬體裝置的主機名稱。您也可以使用 IP 位址取代 <hostname>。

2 若您看到安全警示訊息，請接受自我簽署的憑證以繼續後續動作。

此時會顯示控管中心的**「登入」**頁面。

3 選擇您要用來操作隔離所以及控管中心之使用者檢視畫面的語言。

4 在**「使用者名稱」**方塊中，輸入系統管理員指派給您的使用者名稱。

如果您是第一位存取控管中心的管理員，請輸入 **admin**。

5 在**「密碼」**方塊內，輸入您的管理密碼。

若您不知道密碼，請聯絡您的系統管理員。

6 按下**「登入」**。

以一般使用者身分登入

1 確認您擁有 LDAP 驗證來源。

2 從瀏覽器存取控管中心。

預設的登入位址如下：

https://<hostname>

其中 <hostname> 為指定給硬體裝置的主機名稱。您也可以使用 IP 位址取代 <hostname>。

3 若您看到安全警示訊息，請接受自我簽署的憑證以繼續後續動作。

此時會顯示控管中心的「登入」頁面。

4 選擇您要用來操作隔離所以及控管中心之使用者檢視畫面的語言。

5 在**「使用者名稱」**方塊中，輸入完整的電子郵件地址 (例如 kris@symantecexample.com)。

6 在**「密碼」**方塊中，輸入您平常用來登入網路的密碼。

7 按下**「登入」**。

8 若要登出，在任何頁面的右上角，按下**「登出」**圖示。

9 基於安全性考量，請關閉您的瀏覽器視窗以清除瀏覽器的記憶。

初始組態工作

安裝期間，您可設定 Symantec Messaging Gateway 用來運作的初始組態參數。但是，大多數的客戶都能從檢閱初始組態設定、啟用其他功能以及修改不屬於安裝程序的設定等方面獲得好處。

請使用以下四個步驟的程序，驗證您已準備好充分運用 Symantec Messaging Gateway 的強大功能，以符合安裝的特定需求。

表 7-2 初始組態工作

步驟	動作	說明
步驟 1	安裝 Symantec Messaging Gateway 後，請測試郵件流。	請驗證您的硬體裝置過濾器，並傳送郵件。
步驟 2	架構選用的通訊及監控功能。	Symantec Messaging Gateway 提供各種強大的通訊及監控功能。您可以控制 SMTP 通訊參數與安全性。您可以控制在控管中心與掃描程式之間的一般使用者存取及通訊。您可以設定警示、記錄與報告，以及 SNMP 監控和 UPS 備份。 如需有關選用的通訊及監控功能的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

步驟	動作	說明
步驟 3	架構選用目錄整合功能。	您可以使用 LDAP 目錄資料來源，將 Symantec Messaging Gateway 與現有目錄資料基礎架構整合在一起。 如需有關架構目錄資料整合的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。
步驟 4	架構選用的電子郵件管理和過濾功能。	您可以管理電子郵件流及過濾的許多層面。這些功能可大幅提升防垃圾郵件的有效性、降低基礎架構需求，並顯著增強對使用者及資產的保護。 如需有關電子郵件管理的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

選用組態工作

根據您的網路環境、您的使用者以及處理需求，您可能需要變更某些組態設定，以最佳化您環境中的 Symantec Messaging Gateway。

賽門鐵克建議您啟用信譽過濾，以提高防垃圾郵件的有效性與處理能力。某些選用功能需要架構 LDAP 目錄資料來源，或是有其他的需求。

如需本節中任何工作的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

表 7-3 通訊與監控

動作	說明
架構其他掃描程式設定。	除了在安裝期間選擇 MTA 和 SMTP，您還可以架構和啟用掃描程式電子郵件設定及 SMTP 過濾。 請參閱第 41 頁的「新增並架構掃描程式 」。
架構控管中心設定。	架構控管中心的憑證、系統地區設定、遞補語言編碼、接聽通訊埠及 SMTP 設定。設定可存取垃圾郵件隔離所的一般使用者登入，以及管理一般使用者的喜好設定資料。 請參閱第 40 頁的「架構控管中心」。

表 7-4 目錄整合

動作	說明
架構目錄整合。	建立並架構 LDAP 目錄資料來源。部分 Symantec Messaging Gateway 功能需要架構目錄資料來源。 如需有關架構目錄資料整合的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

表 7-5 電子郵件管理和過濾

動作	說明
架構電子郵件設定。	架構其他的本機和非本機網域、位址偽裝、別名、無效收件者處理、錯誤郵件處理、SMTP 問候語、郵件管理員地址以及配置區限制。 如需有關架構電子郵件設定的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。
啟用信譽過濾。	啟用在連線時透過「Brightmail 適應性信譽管理」進行初步過濾。透過啟用此功能，您可以大幅降低郵件處理量並增強防護。 如需有關架構信譽過濾的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。
設定電子郵件驗證。	您可以設定五種不同類型的電子郵件驗證：SPF、寄件者 ID、DKIM、DMARC 及 SMTP。 如需有關設定電子郵件驗證的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。
建立政策群組。	您可以設定使用者群組，以便根據群組成員資格，以不同方式處理電子郵件訊息。您可以指派政策給群組； 或者，如果您要將相同動作套用至所有使用者的電子郵件訊息，則可以略過此步驟。 如需有關政策群組的詳細資訊，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

附錄 A

在安裝期間更新軟體

本附錄包含以下主題：

於安裝期間更新為最新軟體

賽門鐵克建議您在註冊授權後更新為最新版本的軟體。

於初始設定時更新為最新軟體

1 在「**軟體更新**」頁面，選取下列任何一個選項：

略過	讓您稍後更新您的軟體。
更新	立即更新您的軟體。 更新後，安裝精靈會出現以協助您架構硬體裝置。 請參閱第 40 頁的「架構控管中心」。
取消	返回至「**授權註冊**」頁面。
上一步	請參閱第 38 頁的「註冊您的授權」。

2 當軟體更新完成時，請執行下列其中一項：

- 重新整理瀏覽器。
- 關閉您的瀏覽器後再重新開啟，以確保快取版本的圖形能夠正確地顯示。

3 若要繼續安裝，請您接著構主機。

請參閱第 40 頁的「架構控管中心」。

如需有關架構掃描程式的詳細資料，請參閱「Symantec™ Messaging Gateway 10.7 管理指南」。

附錄 B

通訊埠和網址

本附錄包含以下主題：

必要通訊埠

必要通訊埠 列出了在您安裝 Symantec Messaging Gateway 之前必須可以使用的通訊埠。

表 B-1 必要通訊埠

需要的通訊協定	名稱	通訊協定	預設通訊埠	注意事項
對硬體裝置的遠端存取	SSH	TCP	22	使用此通訊埠可存取於指令行介面。
存取名稱服務	DNS	UDP (TCP)	53	目的地伺服器可以是內部DNS伺服器或 Internet 根 DNS 伺服器。如果使用 Internet 根 DNS 伺服器，請確定有允許外部存取的規則。
存取控管中心及對外部 Internet 的離埠存取	HTTP	TCP	80	請參閱第 56 頁的「Symantec Messaging Gateway 使用的通訊埠」。
存取時間服務	NTP	UDP	123	
存取控管中心 (安全)	HTTPS	TCP	443	

需要的通訊協定	名稱	通訊協定	預設通訊埠	注意事項
對外部 Internet 的離埠存取 (安全)	HTTPS	TCP	443	
MTA 對掃描程式 (雙向)	---	TCP	41000	
控管中心對掃描程式 (雙向)	---	TCP	41002	41002 (代理程式通訊埠) 上的流量狀況如下： ■ 密件副本至掃描程式 (階段作業要求) ■ 掃描程式至密件副本 (階段作業接受) ■ 密件副本至掃描程式 (代理程式要求) ■ 掃描程式至密件副本 (代理程式回應) ■ 密件副本至掃描程式 (終止階段作業)

Symantec Messaging Gateway 使用的通訊埠

表 B-2 列出了 Symantec Messaging Gateway 元件及功能所使用的通訊埠。請確定您的防火牆允許存取這些通訊埠。依據您的環境及過濾類型 (入埠、離埠或兩者)，這些指派動作可能略有不同。

附註：Symantec Messaging Gateway 過濾的有效性及準確性，取決於來自 Symantec Global Intelligence Network 的持續更新。若要維持硬體裝置的實用性，促進硬體裝置與賽門鐵克之間的自動通訊十分重要。

表 B-2 在網路中針對 Symantec Messaging Gateway 開啟的通訊埠

通訊埠	通訊協定	來源	目的地	說明	注意事項
22	TCP	您的管理主機	控管中心/掃描程式	連到硬體裝置的 SSH 連線	使用此通訊埠可存取於指令行介面。
25	TCP	控管中心/掃描程式	內部郵件伺服器	入埠內部電子郵件串流量	控管中心使用內部郵件主機來傳送警示及報告。
25	TCP	內部郵件伺服器	掃描程式	離埠內部郵件串流量	

通訊埠	通訊協定	來源	目的地	說明	注意事項
25	TCP	Internet	掃描程式	入埠 Internet 郵件串流量	
25	TCP	掃描程式	Internet	離埠 Internet 郵件串流量	
25	TCP	掃描程式	內部 SMTP 伺服器	SMTP 驗證轉寄	
53	UDP	掃描程式	Internet	DNS 查詢	目的地伺服器可以是內部 DNS 伺服器或 Internet 根 DNS 伺服器。如果使用 Internet 根 DNS 伺服器，請確定有允許外部存取的規則。
80	TCP	控管中心	Internet	ThreatCon 更新	ThreatCon 層級會出現在「**儀表板**」頁面。
80	TCP	掃描程式	Internet	預設自動防毒更新和快速回應防毒更新	
123	UDP	控管中心/掃描程式	Internet/內部 NTP 伺服器	硬體裝置的時間同步伺服器	
161	UDP	SNMP 伺服器	控管中心/掃描程式	SNMP 管理	SNMP 通訊的預設通訊埠。此通訊埠可以變更，以符合您的 SNMP 組態。此通訊埠預設為停用。
389	TCP	控管中心/掃描程式	LDAP 伺服器	如果啟用目錄資料服務，則可存取 LDAP 伺服器，以查詢使用者、群組和散布清單。	如果啟用目錄資料服務，控管中心和掃描程式都將使用此通訊埠。
443	TCP	控管中心/掃描程式	Internet	規則更新、軟體更新及授權註冊	賽門鐵克會將規則更新傳送至硬體裝置。
587	TCP	Internet	掃描程式	SMTP 驗證流量	
636	TCP	控管中心/掃描程式	LDAP 伺服器	如果啟用目錄資料服務，則可存取 SSL 加密的 LDAP 伺服器，以查詢使用者、群組和散布清單。	如果啟用目錄資料服務，控管中心和掃描程式都將使用此通訊埠。
3268	TCP	控管中心/掃描程式	LDAP 伺服器	Active Directory 通用類別目錄伺服器 (LDAP)	
3269	TCP	控管中心/掃描程式	LDAP 伺服器	SSL 加密的 Active Directory 通用類別目錄伺服器 (LDAP)	

通訊埠	通訊協定	來源	目的地	說明	注意事項
41000	TCP	MTA/掃描程式	MTA/掃描程式	雙向	
41002	TCP	控管中心/掃描程式	控管中心/掃描程式	控管中心與掃描程式之間的雙向通訊	41002 (代理程式通訊埠) 上的流量狀況如下： ■ 密件副本至掃描程式 (階段作業要求) ■ 掃描程式至密件副本 (階段作業接受) ■ 密件副本至掃描程式 (代理程式要求) ■ 掃描程式至密件副本 (代理程式回應) ■ 密件副本至掃描程式 (終止階段作業)
41015 - 41017	TCP	控管中心	掃描程式	隔離所通訊	
41025	TCP	掃描程式	控管中心	隔離所通訊	掃描程式會使用此通訊埠將隔離的郵件傳送至控管中心。
41080	TCP	您的管理主機	控管中心	控管中心 Web 管理介面 (HTTP)	此通訊埠預設為停用。
41443	TCP	管理主機	控管中心	控管中心 Web 管理介面 (HTTPS)	控管中心的 Web 管理通訊埠。
8443	TCP	SPC 主機	控管中心	SPC 管理介面 (HTTPS)	若要將 ProductName; 與 Symantec Protection Center 整合，請確保防護中心伺服器可以透過通訊埠 8443 與所有 Symantec Messaging Gateway 硬體裝置通訊。根據您的環境而定，這可能需要變更防火牆。

請參閱第 11 頁的「安裝前準備」。

保留的通訊埠

表 B-3 列出在安全性稽核期間，或在疑難排解問題時於記錄檔中可能遇到的通訊埠。

表 B-3 Symantec Messaging Gateway 保留通訊埠

通訊埠	通訊協定	接聽	說明
199	TCP	所有啟用的介面	SNMP 多工通訊協定

通訊埠	通訊協定	接聽	說明
953	TCP	回送介面	DNS
3306	TCP	回送介面	MySQL 資料庫
41015	TCP	所有啟用的介面	傳輸引擎
41016	TCP	所有啟用的介面	入埠內部「可疑病毒隔離所」通訊
41017	TCP	所有啟用的介面	離埠內部「可疑病毒隔離所」通訊
41018	TCP	回送介面	目錄資料服務
41019	TCP	回送介面	關閉目錄資料服務

請參閱第 11 頁的「安裝前準備」。

Symantec Messaging Gateway 使用的網址

表 B-4 列出了 Symantec Messaging Gateway 使用的網址。

表 B-4 Symantec Messaging Gateway 網址

URL	通訊協定	通訊埠	說明
swupdate.brightmail.com	TCP	443	用來擷取新的軟體。
register.brightmail.com	TCP	443	用來註冊硬體裝置。
aztec.brightmail.com	TCP	443	用於下列客戶特定的垃圾郵件提交服務項目： ■ 管理員垃圾郵件提交 ■ 預先佈建提交服務 ■ 服務狀態 ■ 閱讀報告 ■ 服務組態 ■ 規則集擷取
rules.ara.brightmail.com	TCP	443	用於擷取客戶特定的規則集。
submit.ara.brightmail.com	TCP	443	用於一般使用者遺漏的垃圾郵件和誤報垃圾郵件提交。
probes.brightmail.com	TCP	443	用於探查帳戶

URL	通訊協定	通訊埠	說明
tmsg.symantec.com	TCP	443	用於遙測資料的每週通訊。此報告允許賽門鐵克收集有關系統使用率的統計資料以及軟體安裝與授權狀態。遙測套件中不含任何個人識別資訊。
liveupdate.symantecliveupdate.com	TCP	80	預設自動防毒更新
liveupdate.symantec.com	TCP	80	預設自動防毒更新
definitions.symantec.com	TCP	80	迅速回應防毒更新

請參閱第 56 頁的「Symantec Messaging Gateway 使用的通訊埠」。

索引

十一劃

十二劃

十三劃

十四劃