

Symantec Messaging Gateway 10.7.x Virtual Edition 安裝、基本設定及版本升級使用手冊

業界公認 保安資訊--賽門鐵克解決方案專家 We Keep IT Safe, Secure & Save you Time, Cost

服務電話 : 0800-381500 | +886 4 23815000 | <u>http://www.savetime.com.tw</u>



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。

保安資訊有限公司說明

此文件說明如何設定Symantec Message Gateway 10.7.x Virtual Edition使其能正常運作 過濾信件,唯此內容僅止於最簡單的設定, 以下的設定【以 Symantec Message Gateway 10.7.x Virtual Edition **當Gateway閘道】**為例, 若需更進階部署及細項的說明,煩請見原廠 說明文件。

此文件說明的各項建議「設定值」 並不一定會符合 貴組織單位的需求, 請視 貴公司需要修改為最符合 貴公 司需要的設定值。





1 全新安裝

1-1	系統需]求	3
1-2	Symant	ec Message Gateway 10.7.x Virtual Edition 下載	
	(以IS	O 檔安裝為例,虛擬環境請依實際情況擇一參考)	3
	1-2-1	在 VMware 上設定虛擬環境安裝 SMG	5
	1-2-2	在 Hyper-V 上設定虛擬環境安裝 SMG	8
1-3	初始化	·····	14
	1-3-1	需準備一獨立 IP 給 SMG Virtual Edition 使用	14
	1-3-2	開啟 SMG 的 VM 後,從初始 Console 設定基本的 IP,角色等設定	14
っ甘っ	卡约中		
2 基z	本設定		
2 基z 2-1	*設定 一般基	本設定	17
2 基z 2-1	*設定 一般基 2-1-1 ž	本設定····· 進入WEB Console設定·····	17 17
2 基z 2-1	本設定 一般基 2-1-1 ž 2-1-2 名	本設定····· 進入WEB Console設定······ 各個細項設定	17 17
2 基z 2-1	本設定 一般基 2-1-1 対 2-1-2 名	本設定····· 進入WEB Console設定····· 各個細項設定 ② SMTP MTA 細項設定·····	17 17 24
2 基z 2-1	本設定 一般基 2-1-1 対 2-1-2 谷 《	本設定····· 進入WEB Console設定····· 各個細項設定 ② SMTP MTA 細項設定····· ③ 設定群組的規則·····	17 17 24 27
2 基z 2-1	本設定 一般基 2-1-1 対 2-1-2 名 《 《	本設定 進入WEB Console設定 各個細項設定 ② SMTP MTA 細項設定 ③ 設定群組的規則 	17 17 24 27 28

	◎ 報告全部勾選	29
	2-1-3 測試 SMG	30
2-2	內容政策範例	31
2-3	其他的建議設定	36
2-4	備份設定部份	37

3升級

3-1 從WEB介面更新	39
3-2 從命令模式更新	39
附註 A:常用它項進階功能如下,請聯絡保安資訊以獲得更進一步資訊	40
附註 B: SMG 的一些架構流程圖	40

業界公認保安資訊--賽門鐵克解決方案專家

We Keep IT Safe, Secure & Save you Time, Cost



1 全新安裝

1-1 系統需求

SMG VM 版本支援	VMware 或 Micros	soft Hyper-V
-------------	-----------------	--------------

項目	建議值	最少需求	說明
VMware ESXi Server	6.0以後版本	6.0	
Microsoft Hyper-V	Windows 2016 Datacenter Edition	Windows 2012 Standalone	
磁碟空間	150Gb	120Gb	日誌留存及未來升級時需要
CPU	8	4	
RAM	16 to 32 Gb	8 Gb	
網卡	2	1	至少要assign一張

1-2 Symantec Message Gateway 10.7.x Virtual Edition下載 (以ISO檔安裝為例,虛擬環境請依實際情況擇一參考)

■取得Symantec Message Gateway 10.7.x Virtual Edition

您的授權必須是SPSEE或單獨的SMG才能下載,登入MyBroadcom(<u>https://www.</u>

broadcom.com/mybroadcom/login)後依如下操作

BROADCOM' PRODUCTS SOLUTIONS SUPPORT COMPANY HOW TO BUY	
PRODUCT DOCUMENTATION COMMUNITIES MY CASE INFORMATION ENTITLEMENTS MANAGEMENT	DOWNLOADS CART MY TOOLS -
Support / Symantec Enterprise Security	
SYMANTEC ENTERPRISE SECURITY	tomers click here to learn about your new portal experience
Cr Search Support	itical Updates 🕢
Search by Product Name, Solution ID or by Keyword Q	mantee Endpoint Encryption 11.3.0 MP1 hot fix avail pired AddTrust External CA Root causing some sites
CA CA	nsitioning from SEP Cloud of SEP Size to SESE to Symantec Product Migration Alert
Case Management My Entitlements	Product Information
Open, track and update your cases Get license keys, guides and information	Access product specific knowledge and documentation
Product Downloads	Documentation
Obtain the products, upgrades and packages you need	View release notes, installation, implementation, administration, user documentation
	Hello! How may I assist you?

業界公認 保安資訊--賽門鐵克解決方案專家 ■■■ We Keep IT Safe, Secure & Save you Time, Cost



點擊含有 SMG 的產品,以此例為 Protection Suite Enterprise Edition

Support / Symantec Enterprise Se	ecurity / Download Management		
Download Man	agement 9 Symantec cus	stomers click here to learn more about your new dowr	nload experience
	<u> </u>		
	Search Your Prod	duct	
	Search by product name	Q	
	,		
	· · · · · · · · · · · · · · · · · · ·		
Endpoint Security Complete	Protection Suite Enterprise Edit	tion	

然後先選要下載的版本 10.7.3,再按 Protection Suite Enterprise Edition

Protection Suite Enterprise Edi	tion				
SEARCH :		,			
PRODUCTS	RELEASE	ANGUAGE	CART	DOWNLOAD	FTP
Protection Suite Enterprise Edition	10.6.6 10.6.6 10.7.0 10.7.1 10.73	~	<u>+</u>	¢	æ Fre
Showing 1 of 1	14.0.2 14.2.2_MP1				
PRODUCTS SOLUTIONS SUPPORT COMPANY HOW TO BUY Copyright © 2005-2020 Broadcom. All Rights Reserved. The term "Broadcom" r subsidiaries.	14.3 7.5.6 7.9 n Inc	and/or its	f	y in D	

SMG 的下載提供二種檔案:

ISO 檔:供還原模式安裝使用,為實體機器 83xx系統及 Hyper-V、VMware 的虛擬環境可以使用。 ZIP 檔:僅供 VMware 環境以 OVF 檔做滙入式安裝使用。

依此例選擇 iso 檔做下載,實際則可自行依自身環境情況做下載,若使用 ovf 檔則可直接跳 到一般基本設定的部份(滙入 ovf 的部份此文件不詳述)。

Protection Suite Ent Product Files Accessory Files	erprise	e Edition					
			Release		Service Pack		Language
			10.7.3	~	0	~	EN
SEARCH :					Add All To Cart		Download Package
Symantec Messaging Gateway 10.7.3 - M	Iulti-lingual	Release : 10.7.3	Service Pack : 0				~
File iso檔可供二 境做還原模	二種VM環 式的安裝	SHA2	MD5	CART	DOWNLOAD	FTP	Tokens
Symantec_Messaging_Cate_sy_OSrest ore_10.7.3-5_Linux_Int_iso	Jun 12 2020 9:43PM	8b16c8147a803a0 209aa2ea0626183 3da0af8288d989 e5bbb5d8a719f10 73b59	e3a650c1667b390 552f32516b85f44 96	<u>+</u>	Ģ	AN FTP	<u>Generate</u>
Symantec_Messaging_Gateway_VMima ge_10.7.3-5_Linux_Int.zip	zip檔僅可 VMware 以ovf滙入	e9cf03eb27c970fc bae442 母境, 式安裝	8c7df729846ca9 683e36b9b3b797 8f53	<u>+</u>	¢	æ FP	<u>Cenerate</u>





1-2-1 在 VMware 上設定虛擬環境安裝 SMG

虛擬環境的建立非本文重點,請自行參考 VMware 或 Microsoft 文件,以下為透過 SMG iso 檔的安裝步驟。





4 自訂設定

指定此虛擬機的配備內容並指定前一節下

載的 iso 檔

5 即將完成 確定無誤後按完成以建立此 VM



■設定自動啟動

vmware" esxi"				ro	• • •	說明 👻 ।	Q 搜尋	
℃" 導覽器 🔹	·管理							
▼ 3 主機	条統 硬體 授	離 套件 服務 妄	全性和使用者					
監控	進階設定	∕ 編輯設定						1
→ 🗗 虛擬機器 13	自動啟動	已啟用	是					
・目儲存區 1	交 / / / / / / / / / / / / / / / / / / /	開始延遲	120s					
		停止延遲	120s					
		停止動作	關閉電源					
		等待活動訊號	长安資訊 否 AVETIME					
		Bon Formation and Contract Co	ion security 啟動 👸 設定 👸 停用 丨 🕑	重新整理 🛟 動	作	Q 搜	寻	
		虛擬機器		~	關閉行為▼	v 自 v	開 ~	停 ~
		🔁 V)		糸統預設值	取	120 s	120 s
		合 S 合 A			系統預設值 系統預設值	取	120 s	120 s
		1	namaa		系統預設值	4	120 s	120 s
		SMG_LAB			系統預設值 解問	取	120 s	120 s
					1943 1993	100	1203	1203
马尔海的新 马坦	前的新 區 訊号		吉东数田 烏番	it //=	0 457	-		
				50 T F	(Y 搜	导		
虛擬機器	1		→ 開閉行為 →	自動啟	~ 開.		亭、~	
SMG_LAB			系統預設值	6	12	0 s	120 s	
ATO CONDE		SA	刷閉	5	30	Os :	300 s	
₫ \$ 1			011系統預設值	4	12	0 s	120 s	
-R (解閂	3	45	e .	120 s	
设置 一 · · · · · · · · · · · · · · · · · ·								
見ねび湯	100 54							
「ガメロル生力生	120 秒	夏 親實際需求調整						
停止延遲	120 秒							
停止動作	条統預設值	~						
等待活動訊號	SAVETIME	去3頁言乃/吉						
53 1-3 794 EXTRIPUIS		1619.1911月1日						
		儲存 取消						



■開啟 SMG 的 VM,從初始 Console 設定基本的 IP、角色等設定 將此 VM 開機後即會開始自動安裝,並重開機





請接續 1-3 做後續初始化設定





1-2-2 在 Hyper-V 上設定虛擬環境安裝 SMG

若使用 VMware 環境請直接跳到 1-3 做後續初始化設定。

■新增虛擬機器

in .	Hyper-V 管理員	_ D ×
檔案(F) 動作(A) 檢視(V) 說明(H)	
🗢 🔿 🙍 📰 🚺		
₩ Hyper-V 管理員 日	佐段機器(U) 名師 本価 X種 CPU使用率 描派的記憶種 運作時間 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	動作 新油 虚虹機器(M) 新油 虚虹機器(M) 磁煤片(F) 建煤火炉器管理員 螺 虚短交换器管理員 螺 虚短交换器管理員 缓 经 SAN 管理員 缓 編型磁碟
3	新増虛擬機器精靈	X
在您開始前		
在您開始前 指定名稱和位置 指定世代 指派記憶體 設定網路功能 速接虛擬硬碟 安裝還項 摘要	は積極可協助窓建立産凝機器。在許多情況中,您都可以使用虛凝機器來取代 蓋決定産凝機器, 述の在日後使用(hyper/管理員) 變更設定。 若要建立虛擬機器, 諸執行下列其中一個動作: . (按一下 (完成), 建立以預設值設定的虛擬機器。 . (按一下 (下一步),以自訂組態建立虛擬機器。 . (次一下 (下一步),以自訂組態建立虛擬機器。)	賣體電腦。您現在可以使用此 精
	 (<上一步(P)) 下一步(N) >	完成(F) 取消

■設定虛擬機器名稱及指定其儲存位置

8.	新増虛擬機器精靈	x
指定名稱和位	<u>#</u>	
在您開始前	選擇此虛擬機器的名稱與位置。	
指定名稱和位置 指定世代	名稱總顯示在 Hyper-V 管理員之中。建議您使用便於識別此虛擬機器的名稱,例如,客體作業系統或工作; 動的名稱。	負
指派記憶體 設定網路功能	名稱(M): SMG-LAB	
連接虛擬硬碟 安裝選項	您可以建立資料夾或使用現有資料夾來儲存虛擬機器。若未攜取資料夾,虛擬機器將儲存在此伺服器所設定 預設資料夾。	的
摘要	✓ 將虛擬機器儲存在不同位置(S)	
	位置(L): H:\SMG-LAB SAVETIME 瀏覽(B)	
您可以依實際需 求變更儲存位置	4. 一方您計劃建立此虛擬機器的檢查點,請選取一個有足夠可用空間的位置。檢查點包含虛擬機器資料, 此可能需要大量的空間。	因
	 <上一步(P) 下一步(N) > 完成(F) 取消	

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■



■設用第一代虛擬機器



■指定記憶體



■ 依實際狀況指定網路卡



業界公認 保安資訊--賽門鐵克解決方案專家 ■■ We Keep IT Safe, Secure & Save you Time, Cost



■調整硬碟大小

8e	新増虛擬機器精靈	x
建接虚擬硬碟		
在您開始前 指定名稱和0位置 指定世代 指派記憶體 設定網路功能 建接虛擬硬課 安裝選項 摘要	虚擬撮影需要存放裝置,以便安装作業系統。您可以現在指定存放裝置,或稍後修改虛擬撮影的 放裝置。 建立虛擬硬碟(C) 使用此描項來建立 VHOX 動態擴充虛擬硬碟。 名範(M): SMG-LAB.VhOX 位置(L): H:SMG-LAB.VMCLAB.Virtual Hard Disks(大小(S): 150] 8 (上限: 64 T8) 使用現有的虛擬硬碟(0) 使用現有的虛擬硬碟(0))內容以設定存 浏覽(6)
	 ① (立置(L): [C:\+Y\-disk\ ① (竹後連結虛擬硬磲(A) 使用此還項來暫時輸過此步驟, 桁後再連結現有的虛擬硬磲。 	测题(B) 取消

■指定安裝需求的 SMG iso 檔

36	新増虛擬機器精靈	x
安裝邊項		
在您關始前 指定名稱和位置 指定世代 指派計值體 說定網路功能 建接虛擬硬碼 安裝聲質 摘要	如果您具有安裝保體的存取權限,則可以立即安裝作業系統,或是稅後再安裝。	
	<上一步(P) 下一步(N) > 完成(F) 取()	Í

■Review 上面的設定, 若没問題按完成





■虛擬機器建立中



若要建立虛擬機器並關閉精靈,請按一下 [完成]。

■修改設定

處理器改為4顆

🗉 🎚 網路介面卡

Intel(R) I210 Gigabit Network ...

調為自動啟動,延遲時間請依實際狀況設定



業界公認 保安資訊--賽門鐵克解決方案專家 We Keep IT Safe, Secure & Save you Time, Cost

100

相對權數(W):



■啟動虛擬機器並開啟 console 介面





檔案(F)	動作(A)	媒體(M)	檢視(V)	說明(H)						
30		0 1		り感						
			止在	啟動虛	擬機	器 'S	SMG-	LAB		
			1							
狀態:正在	E啟動									

■自動安裝進行中,裝完會自動重開機到登入狀態頁



業界公認 保安資訊--賽門鐵克解決方案專家 We Keep IT Safe, Secure & Save you Time, Cost ■■■



1-3 初始化

1-3-1 需準備一獨立 IP 給 SMG Virtual Edition 使用

1-3-2 開啟 SMG 的 VM 後,從初始 Console 設定基本的 IP,角色等設定

- ■開始初始設定
- ■預設帳號:admin,密碼:symantec
- ■重設密碼,請記住此設定的密碼,稍後的web介面均使用此帳密
- ■以 FQDN 模式,指定此 VM 的電腦名稱及網域
- ■時區的部份可先打?做查詢

Symantec Messaging Gateway Version 10.7.3-5 Copyright (c) 1998-2019 Symantec Corporation. All rights reserved. localhost login: admin Password:<mark>Symantec</mark> Last login: Thu Jul 905:44:09 on ttyl Welcome to Symantec Messaging Gateway Before you can begin using this appliance, it needs to be configured. This wizard will guide you through the configuration process. First you need to change your password. New password: Retype new password: Specify a fully qualified host name for this appliance. (example: mail6.company.com): smg999.savetime.com.tw Enter the number corresponding to the timezone for this appliance. Press '?' for a list:

- ■台北的時區代號為65
- ■輸入指定此 SMG 的 ip、subnet mask
- Static route 的部份,如果 貴單位環境內需要請自行輸入,否則預設為 NO,直接 按 Enter 即可

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■



	_
60. (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi	
61. (GT1+05:00) Irkutsk 62. (CMT:00:00) Vois 1. Louiseur	
02. (Gril+00.00) Audia Lumpur 63. (CMT+08:00) Singapone	
64 (CMT+08:00) Perth	
65 (GMT+08:00) Taitei	
6. (GMT+08:00) Halper	
67. (GMT+19:00) Osaka, Samoro, Tokuo	
68. (GMT+09:00) Seoul	
69. (GMT+09:30) Adelaide	
70. (GMT+09:30) Darwin	
71. (GMT+10:00) Brisbane	
72. (GMT+10:00) Canberra, Melbourne, Sydney	
73. (GMT+10:00) Guam, Port Moresby	
74. (GMT+10:00) Hobart	
75. (GMT+10:00) Yakutsk	
76. (GMT+11:00) Solomon Is., New Caledonia	
77. (GMT+11:00) Vladivostok	
78. (GMT+12:00) Auckland, Wellington	
79. (GMT+12:00) Fiji, Kamchatka	
80. (GMT+12:00) Magadan	
81. (GMT+12:00) Marshall Is.	
82. (GMT+13:00) Nuku'alofa	
Enter the number corresponding to the timezone for this appliance. Press '?' for a list: > <mark>65</mark>	
You will now configure the first ethernet interface for your appliance. For registration to succeed, you must correctly enter valid IP addresses for your ethernet interfaces, default gateway, and DNS server. If you do not correctly enter these IP addresses, you will be required to restart this process.	
Specify the first <u>IP address</u> that you want to assign to this appliance. (example: 192.168.0.1): > 10.10.2.248	
Specify the <u>subnet mask</u> that is associated with this ethernet interface. (example: 255.255.255.0): [default: 255.255.255.0]> <mark>255.255.0</mark>	
Do you want to configure a <u>static route</u> to connect to the Internet, your DNS server, your LDAP server, or another appliance? You can configure up to 3 static routes. For more information on when to use a static route, refer to the Symantec Messaging Gateway Appliance Installation Guide. [default: NO]> _	

- 輸入 default gateway 及 DNS
- 若要再輸入第二筆 DNS 則直接按 Enter 或輸入 YES 後按 Enter
- 第三筆 DNS 通常不需要,所以輸入 NO 後按 Enter,若需要請再做一筆,打 YES 做輸入即可
 - **請注意**上述的 ip 相關設定需能連上 internet, 否則後續滙入註冊檔的動作若無法成功,則需 重頭再來一次
- 指定此 SMG 的角色,除非有多台,不然一般都是選 3 身兼 Scanner 及 Control Center
- Review 一下設定是否正確,若不正確請直按Enter從輸入 FQDN 的電腦名稱開始重新確定並做 變更,若正確則打YES後按Enter讓它做初始化,完成後直接會重新開機

We Keep IT Safe, Secure & Save you Time, Cost



Specify the IP address of the <u>default gateway</u> (also known as the default router) on your network. (example: 192.168.0.20): > 10.10.2.254
Specify the IP address of your <u>first DNS server</u> . (example: 192.168.0.45): > 10.10.2.254
Would you like to specify another DNS server? [default: YES]> <mark>YES</mark>
Specify the IP address of your <u>second DNS server</u> . (example: 192.168.0.45): > 8.8.8.8
Would you like to specify another DNS server? [default: YES]> <mark>NO</mark>
Specify the role for this appliance. Available roles are:
1. Scanner only 2. Control Center only 3. Scanner and Control Center
See the Installation Guide for more information. If you have only one Symantec Messaging Gateway appliance, choose 'Scanner and Control Center'. What is the role for this appliance? (Type 1, 2, or 3): > 3
Please confirm your configuration:
Host Name: smg999.savetime.com.tw Timezone: 65. (GMT+08:00) Taipei Ethernet Interface 1: IP Address: 10.10.2.248 Subnet Mask: 255.255.0 Static IP Routes: N/A Default Gateway: 10.10.2.254 DNS Server 1: 10.10.2.254 DNS Server 2: 8.8.8.8 Role: Scanner and Control Center
Is this correct? [default: NO]> YES_

■ 開機完成到此登入畫面時,我們就可移至瀏覽器做後續的初始設定了



業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ 1■



2 基本設定

2-1 一般基本設定

2-1-1 進入WEB Console設定

■ 在網址列輸入前述設定的 SMG ip, https://10.10.2.248

← → × ☆ ▲ 不安全 10.10.2.248		2	
COMPANY OF THE OWNER	選取憑證		×
	請選取你在 10.10.2.248:443 的驗證憑	證 	
	主旨	發行者	序列
	fa4ea47a-549c-4786-a4d9-9578	MS-Organization-Acc	0212FD3605EFE681
4			ſ
-			4
你	憑證資訊	l	確定 取消
攻擊者	可能會試圖從 10.10.2.248 竊耳	饭你的資訊 (例如密碼、	郵件或信用卡資料)。 瞭解詳情
NET::E	RR CERT AUTHORITY INVALID		
日間	<u>你造訪的部分網頁網址、特定的</u>	条統資訊以及部分網頁	<u>內容</u> 傳送給 Google,協助改善
	IOITIE 的女主任。 <u>履位催叹束</u>		
際語	就詳細資料		返回安全性瀏覽
回服器 回能是	無法證明其屬於 10.10.2.248 編 因為設定錯誤,或有攻 <u>擊者攔</u>	周域;其安全性憑證未明 國你的連線所致。	Q得你電腦作業系統的信仕。這
	<u> 往 10.10.2.248 網站 (不安全)</u>		

■ 輸入前步驟中的帳密

← → C ① ▲ 不安全 10.10.2.248/bri	ghtmail/	\$	
	Symantec Messagi 版本 10.7.3	ing Gateway	
	歡迎使用 Symantec Messaging Gateway 是查需要登人說明? 保安 資訊 SAVETIME INFORMATION SECURITY	選取語言: 中文(繁體) 使用者名稱: admin 密碼: ••••••• 登入	✓ ● <
	Symantec. Copyright © 1998-2019 Symantec Corpo	ration. All rights reser	ved.



■ 勾選授權許可

Symantec Messaging Gateway	Symantec Messaging
安裝精靈	安裝精靈
請先詳閱授權許可協議之條款,並且接受條款內容之後則得以繼續。	歡迎使用 Symantec N 心,因此您必須輸入
使用者授權許可協議	+100+486 = 十 100 二次 十0
賽門鐵克軟體授權許可協議 在權益確認書中所指之賽門鐵克公司及(或)其子公司(以下稱「賽門鐵克」) 授權閣下個人、公司或法律實體(以下皆稱「閣下」或「閣下的」)使用所附 授權軟體的條件為,關下接受本賽門覺提權許可協議的全部條款和條件 下客只是思想:(古德和下)(供認為「總總許可招集)、古使思想:(書)	Symantec Antiviru
及產品设用僅稱於具料(定表以下)(就得給:2次僅計10歲讓了)。在设用投權執 體前,請詳閱讀本授權許可協議。本文件為閣下與賽門鐵克之間合法且強制的 合約。只要下載、安裝、複製本授權軟體、點選「我同意」或「是」按鈕,或 以電子形式表示同意,或是使用本授權軟體。皆表示閣下同意本授權許可協議 的條款和條件。若閣下不同意本授權許可協議,請點選「我不同意」或「否」 按鈕,或以其他方式表示拒絕,並完全停止使用本授權軟體。	Symantec Premiu Symantec Content 軟體更新 註冊授權 指示授權
 定義。除非本許可協議中另有規定,否則大寫詞彙悉依下文之定義為準, 並且這些大寫詞彙可能根據上下文之要求而採用單數或複數形式。 「收集的資料,是指義門裁古可能收集、保留、皮理、提帶和使用的某些資 	選擇檔案
☑ 我接受授權許可協議的條款。	

■ 指定授權檔對按註冊授權

權註冊資訊		
功能	狀態	過期
Symantec Antispam	未授權	
Symantec Antivirus	未授權	
Symantec Premium Content Control	未授權	-
Symantec Content Encryption	www.未授權	
軟體更新	未授權	
註冊授權 指定授權備; 選擇檔案 slf	代理伺服器	公用程式

■ 授權滙入成功後請按下一步,否則請重頭來過

legistration Suc				
使用 Symantec M	essaging Gateway 控	管中心・由於翅	這是您第一次登入控管中	· 使體裝置註冊
四応応必須輸入計	111頁前1/7月經續。			軟體更新
離註冊資訊				管理員設定
功	皓	狀態	過期	時間設定
ymantec Antispan	1	已授權	2023年06月04日	系統地區設定
ymantec Antivirus		已授權	2023年06月04日	掃描程式角色
ymantec Premium	Content Control	已授權	2023年06月04日	虚概 IP
ymantec Content	Encryption	未授權		1 追那件调造
次體更新	INFORMATIONS	ECU已授權	2023年06月04日	八坪野什迿應
註冊授權				本機網域
指定授權檔:				離埠郵件過濾
│選擇檔案│未選打	睪任何檔案	代理伺服器	公用程式	安裝摘要
				Syı

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■





■ 輸入管理員郵件地址,此地址預設可收到相關的 SMG 通知信件



■ 指定 NTP 伺服器,在台灣,通常就直接用國內的,若 貴單位有特定使用方式則依 貴單位 設定值設定

引設定				
一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	到NTD (司服器,用款/只结	建碎的多碎咕朗,武书,你可	×	<i>使體裝</i> 置註卌
(手動設定系統時間。 (手動設定系統時間。	י אוא אנערי אא אמערי איזא איז איזא איז איז איז איז איז איז	M自WERY系統時间。 现4日, 返 9		軟體更新
目前的硬體裝置時間。			\checkmark	管理員設定
「畠此貝囬載人時此健第	2020年07月09日 2020年07月09日	日 <i>星期四下午 02:20:09 TST</i>		時間設定
時間		544 - 366296264 - 58 - 90 		系統地區設定
○ 不要變更時間				掃描程式角色
○ 手動設定時間		▲ ▲ R 中 杰		虛擬 IP
日期: 時間:		S 2020-7-9		入埠郵件過濾
● 使用 NTP 伺服器		INFORMATION SECURITY		本機網域
NTP 伺服器 1:	time.stdtime.gov.tw			離埠郵件過濾
NTP 伺服器 2: NTP 伺服器 3:	clock.stdtime.gov.tw			安裝摘要
NTP 伺服器 4: NTP 伺服器 5:				Symante

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■



■ 指定地區及編碼



■ 指先改入埠郵件過濾,若連離埠也需過濾則事後再調整即可

人名文 中月 五座	安裝	精靈步驟
帰猫程式角色	~	硬體裝置註冊
指定此掃描程式將過濾的郵件類型。		軟體更新
● 入埠郵件過渡	~	管理員設定
 ○ 離埠郵件週源 ○ 入埠和離埠郵件過濾 	~	時間設定
	~	系統地區設定
◆◆保安資訊		掃描程式角色
SAVETIME		虛擬 IP
INFORMATION SECURITY		入埠郵件過濾
		本機網域
		離埠郵件過濾
		安裝摘要
< 上─步 下─步 > 取消		Sumantos





■ 指定入埠過濾的IP位址,預設即為前述設定的 SMG ip



■ 接收所有寄過來的信件

	安裝	精靈步驟
局郵件過濾 - 已接受的主機 ────────────────────────────────────	 Image: A set of the set of the	硬體裝置註冊
希望讓這台主機直接接收來自 Internet 上的郵件,或者通過網路或托管主機 的上游電子郵件伺服器傳送?若要讓電子郵件防火達在上游電子郵件伺服器		軟體更新
正常運作,則必須列出所有的上游郵件伺服器。	 Image: A second s	管理員設定
)所有 IP 位址 ②	 	時間設定
)特定 IP 位址 ③ 輸入 IP 位址、CIDR 範圍或網域的清單。您亦可以彈取現有的 IP 位址、	 Image: A start of the start of	系統地區設定
	 Image: A second s	掃描程式角色
IP 位址/網域:		虛擬 IP
□ 可用的 IP 位址/網域 INFORMATION SECURITY		入埠郵件過濾
0 10.10.2.248		本機網域
		離埠郵件過濾
		安裝摘要
		de





■ 指定往後送往的 mail server ip

	× 70	帽盘沙咖
早野件週濾 - 野件傳送	×	硬體裝置註冊
?義過濾的郵件將傳送到的目的地 IP 位址和通訊埠,例如您的下游 Exchange J服器。		軟體更新
主機名稱或 IP 位址: 10.10.1.242	✓	管理員設定
通訊埠: 25	✓	時間設定
	✓	系統地區設定
Mail Server th IP	~	掃描程式角色
SAVETIME		虛擬 IP
INFORMATION SECURITY		入埠郵件過濾
		本機網域
		離埠郵件過濾
		安裝摘要

■ 入埠郵件過濾時非本機郵件傳送時透過何種方式做查詢對方網域,預設用 MX 方式查詢即可

安裝精靈			安裝	精靈步驟
入埠郵件過濾 - 非	本機郵件傳送		~	硬體裝置註冊
指定非本機網域到	8件在經由這個主機過濾後要轉	遞至的主機。		軟體更新
◎ 使用預設 MX	查詢 🕐		 Image: A start of the start of	管理員設定
 定義新主機 主機名種或 II 	0 位址·		 Image: A set of the set of the	時間設定
通訊埠:	25		~	系統地區設定
□ 啟用此主	幾的 MX 查詢 ^②	◆◆保定咨询	 Image: A start of the start of	掃描程式角色
○ 使用現有的主	機: 10.10.1.242:25	SAVETIME Y		虛擬 IP
		INFORMATIONSECURITY		入埠郵件過濾
				本機網域
				離埠郵件過濾
				安裝摘要
	< _	上一步 下一步 >		Symantec.



■ 指定本機收件的網域及其往送送的郵件伺服器 ip

8t 192				
			~	硬體裝置註冊
目定您希望接受入垾郵(= ####21#	牛的網域和電子郵件地址。			軟體更新
⊅磯網域 ₴受入埠郵件的網域或♡	電子郵件地址:		✓	管理員設定
savetime.com.tw		1	✓	時間設定
- 選用目的主機 選擇性地繞送至下列	日的土料・	通知 侣•	~	条統地區設定
10.10.1.242		25	 Image: A start of the start of	掃描程式角色
		保安资訊		虛擬 IP
<u>0</u>	Mall Server 的IP	<u>医匯入</u> 新增	 Image: A second s	入埠郵件過濾
刪除				本機網域
□ 本機網域	目的主機	MX 查詢		離埠郵件過減
				安裝摘要
未指定				

■ Review 上述的設定,若没問題按完成即可

裝精靈」已完成。			
		×	硬體裝置註冊
21035			軟體更新
檢閱您的設定。如果想要進行變更 」。	1,請按「上一步」;否則,請按下「完	~	管理員設定
曾理員電子郵件地址: mis@savetir	ne.com.tw	✓	時間設定
時區: Asia/Taipei 時間設定: 使用 NTP 伺服器		1	系統地區設定
NTP 伺服器名稱:		\checkmark	掃描程式角色
line.statime.gov.tw lock.statime.gov.tw	保安資訊		虛擬 IP
	INFORMATION SECURITY	 ✓ 	入埠郵件過濾
本機網域: savetime.com.tw -> 10	.10.1.242	~	本機網域
糸統地區設定: 中文 (台灣) 遞補語言編碼: 西歐語系 (ISO-885	9-1)		離塢鄅件鴻謯
使用 HTTP 代理伺服器: 否			ᄚᆤᆍ
邼件過濾: 僅入埠郵件過濾	-		安装摘罢
			de

業界公認 保安資訊--賽門鐵克解決方案專家 ■ ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■



■ 初始設定儲存更新



2-1-2 各個細項設定

◎ SMTP MTA細項設定

進入 MTA 細項設定

Symantec Messa	aging Gateway								登入為: adm	in [smg999.savet
👺 狀態	山報告	🎦 通訊協定	🔛 信譽	² 垃圾郵件	豪惡	意軟體 🦉	威脅防禦	🗟 內容	管理	
▲ 政管使管一尋政設警 憑控歸加 第理用理過使使群 員使使群 定示證管整整 告局報智 SNMP L 主組授關知 人 金 名 一 尋政設警 應控 告 整 版 管 使 管 一 尋政設 警 憑 定 示證 管 是 管 使 管 一 尋政設 整 憑 思 告 思 之 定 。 一 尋 政 設 警 憑 一 尋 四 記 》 一 尋 四 記 》 一 一 尋 四 記 》 一 四 章 一 四 章 》 之 一 马 四 之 二 二 一 一 四 一 四 一 四 一 四 一 四 一 四 一 四 一 四 一		王機組態 新架構構描程式或控作 新増 重機名稱 smg999.savetime. Click	管中心主機。	啟用 已 Sat NFORMATION	啟用 ✓ 拿訊 ETIME SECURITY	IP 位址 10.10.2.248	版本 10.7.3-5	掃描程	角色 式及控管中心	Wall ID 98321513
版本										



symantec mes	saging Gatew	ау							登入為: admin [s	mg9999.sa
📟 狀態	山報告	3 通訊協定	🔛 信譽	🛃 垃圾郵件	- 🗞 惡j	意軟體	🖳 威脅防禦	🛃 內容	🗟 管理	
文策		絙 居 士 樾 炤 能								
理		約冊 判 工 1成 約1 25								
理員		重新架構掃描程式或控	管中心主機。							
·般使用者 ·地使用者		編輯主機組態								
我使用者 策群組		主機名稱:		smg999	.savetime.co	m.tw				
定		主機說明:		Local H	ost					
示 證		服務 C	DNS/時間 1	代理伺服器	乙太網路	SMTP	内部	部件主機		
管中心		郵件遏濾								
绿整合 誌		此掃描程式將用	於:							
		○ 不過濾任何	郵件							
唐卡 MD		 ● 催入埠勤件: ○ 僅離埠郵件: 	通渡							
S		○ 入埠和離埠	鄞件遏濾							
機										
康 韓		入埠								
告閉		——入埠郵件設定	:							
用程式		入埠郵件 IP	- ☆北ト:		通訊埠:					
4		Ethernet 1:	(10.10.2.248)	~	25					
		選用人理必任	PV6 17 JF:	~	通訊埠: 25					
		加密								
		□ 接受 TLS	加密		未指定	~				
		→ 安水戸	日)—— 30两 200 百豆 T							
		 接受來自 	所有 IP 位址和	網域的人埋郵件制	1 線 音加					
		○ 只接受來	自下列 IP 位址	和網域的入埠郵伯	+連線:					
		每頁的項	目數: 10 ~	顯示: 0 ▼	/ 0					
		新措	新聞尊貴	刪除	全部刪除	匯入				
		匯出								
		□ IP 位	址 ▲							
		未指定I	P位址・							
		入埠本機郵件	傳送							
		將本機網域到	8件轉遞至下列3	主機:						
		新増	編輯	刪除						
			+ #928) ≭ ±0+€	MX	喜好設定			
			土協	42	25	查詢	(1-100)			
		1 培非未搬西	10.10.1.2	72	25		1			
		 へ厚非本機 ● 為非本機 ○ 將非本機 	ハ〒1₩355 網域郵件使用 N 網域郵件轉遞至	1X 查詢 5下列主機:						
		新增	11 AS FE	副除						
			主機		通訊埠	MX 查詢	喜好設定 (1-100)			
		□ 套用上述設定	至所有掃描程式	ť					進	皆設定
									-	

以下的設定請視 貴單位實際情況更改

最大連線數目、郵件大小上限(以 位元組為單位)、每封郵件的收件者數 上限、已傳送郵件的逾時時間(需注意 :值修改後需按【繼續】然後回上一層 按【儲存】才算修改完成)

SMTP 進階設定

架構此掃描程式的「SMTP 連線」。

入塇	離埠	傳送	驗證	
		120-		
埠 SMTP 組態				
劃線數上限:			2000	
ミ自單一 IPv4 位址	或 IPv6 範圍的連續	象數上限:	20	
(若是 IPv4, 啟)	用「連線類別」時	會被覆寫)		
《自單一 IPv6 範圍	的連線數上限的II	Pv6 CIDR 字首:	64	
《件大小上限 (以位	1元組為單位):		10485760	
目封郵件的收件者	敗上限:	除安貧訊	1024	
每個階段作業的郵作	+數上限:	SAVETIME	100	
(若是 IPv4, 啟)	用「連線類別」時	會被覆寫)		
、埠佇列中的郵件數	故目上限:		5000	
∠ 入埠佇列被佔滿	師延遲新連線			
2 在入埠郵件插入	、RECEIVED 標頭			
✓ 啟用反向 DNS 計	查詢②			
皆段作業逾時:			30	秒
■ 帝昭式 並 得。				
则灵住私业们:	2			

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■



主機名種・		cn	10999 savetime com tw		
· 上 // 日 ///·		51 #+8	」 /庙注	医会 主部	
八垾	đ	田早	博达	利式百豆	
SMTP 傳送組	態				
外部連線數上	限:			100	
單一 IP 位址的	的外部連線數	收上限:		50	
所有內部郵件	伺服器的連	線數上限		100	
每個單一內部	郵件伺服器	的連線數	上限:	50	
傳送佇列中的	郵件數目上	限:		150000	
傳送佇列中每	封郵件的收	件者數上	限:	100	
連線的外寄郵	《件數上限:			0	
☑ 傳送佇列補	被佔滿時延續	星新連線			
最小重試間隔	:			15	☆鐘 ∨
最大重試間隔	:			4	
已傳送郵件的	谕時時間:			5	1 T V
退回郵件的論	時時間・			1	-
通知前位到中	的都准动量。	哇問,		1	
2四天山月11丁グリヤ	· 用了到的十些)///	바카(B): 리/14:94:44		4	\ \
	時达的所有! 田氏純准約	即升短门	ILS 加密		
□ 症洪 ILS 法确论的	用戶峏憑證			未指定	~
建線逦時:				30	秒 ▼
EHLO/HELO	· 逦時:			5	分鐘 ▼
MAIL FROM 刻	愈時:			5	分鐘 ▼
RCPT TO 逾時	寺:			5	分鐘 ▼
DATA 逾時:				10	分鐘 ▼
RSET 逾時:				10	分鐘、
閒置逾時:				5	1/ ·
enne kannes rueld. Delle					
SMTP 傳送繫	結				
本機郵件:				10.10.2	.248 🗸
非本機郵件:				自動	~
動態繞送的郵	6件:			白動	~
目標為控管中	心的郵件:			10.10.2	.248 🗸
每一網域的非	本機 SMTP	傳送繫編			
	I調戏,然後	選擇從這	些網塊所奇迗郵件將使用的	傳迗蘩結。	
指定一或多個			IP 位址:		
指定一或多個網域:					
指定一或多個 網域: savetime.com	n.tw	*	10.10.2.248		
指定一或多個 網域: savetime.con	n.tw	*	10.10.2.248	•	新増
指定一或多個 網域: savetime.con	n.tw	•	10.10.2.248	•	新増
指定一或多個 網域: savetime.con	n.tw	* *	10.10.2.248 每頁的項目數: 10 > 顯	↓ ↓ [示: 0 √ / 0	新増
指定一或多個 網域: savetime.com	n.tw	* *	10.10.2.248 辱頁的項目數: 10 > 願	↓ ↓ !示: 0 ~ / 0	新増 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
指定一或多個 網域: savetime.con	n.tw 全部刪除	*	10.10.2.248 每頁的項目數: 10 願	↓ ↓ i示: 0 ∨ / 0	新増
指定一或多個 網域: savetime.com	n.tw 全部刪除 月城	4	10.10.2.248 辱頁的項目數: 10 顧	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	新増
指定一或多個 網域: savetime.com	n.tw 全部删除 J城	* *	10.10.2.248 辱頁的項目數: 10 顯	↓ 「示: 0 ▼ / 0 IP 位址	新増 (()) ()
指定一或多個 網域: savetime.com 回除 高件者網 調度程式並行	n.tw 全部删除 列城 テ:	4 2	10.10.2.248 厚頁的項目數: 10 > 願	↓ 「示: 0 ∨ / 0 IP 位址	新増
指定一或多個 網域: savetime.con 副除 高件者網 調度程式並行	n.tw 全部刪除 別域 テ:	4 2	10.10.2.248 每頁的項目數: 10 > 願	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	新増 (()))
指定一或多個 網域: savetime.con 副除 寄件者網 調度程式並行	n.tw 全部删除 引城 7:	4 2	10.10.2.248 每頁的項目數: 10 > 願	↓ □ □ □ □ □ ↓ 0 □ ↓ 0 □ ↓ 0 □ □ ↓ 0 □ □ ↓ 0 □ ↓ □ ↓ □ ↓ □ ↓ □ ↓ □ □ □ □ □ □ □ □ □ □ □ □ □	
指定一或多個 網域: savetime.com	n.tw 全部删除 J城 J:	4 2	10.10.2.248 每頁的項目數: 10 願	↓ □ □ □ □ □ □ □ □ □ □ □ □ □	新増 (()) 縦續 間
指定一或多個 網域: savetime.com 副除 寄件者網 調度程式並行	n.tw 全部删除 月城 7:	4 2	10.10.2.248 辱頁的項目數: 10 ▼ 願	↓ i示: 0 √ / 0 IP 位址	新増 (()) ² ² ² ² ¹ ¹ ¹ ¹ ¹ ¹ ¹ ¹
指定一或多個 網域: savetime.com 回除 高件者網 調度程式並行	n.tw 全部删除 引城 7: 	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	10.10.2.248 每頁的項目數: 10 ▼ 願 埠 MX 高好設定 (1-100)	↓ □ □ □ □ □ ↓ 0 ↓ 0 0 ↓ 0 0 ↓ 0 0 ↓ 0 0 ↓ 0 0 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	新増 (()) 縦續 周 間
指定一或多個 網域: savetime.com 回除 高件者網 調度程式並行	n.tw 全部删除 引城 了: 	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	10.10.2.248 写頁的項目數: 10 ▼ 願 埠 MX 高好設定 (1-100)	↓ □ □ □ □ □ □ □ □ □ □ □ □ □	新増 (()) 繼續
指定一或多個 網域: savetime.con	n.tw 全部删除 引城 了: 編輯 一 制約 主機 書描程式	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	10.10.2.248 写頁的項目數: 10 ▼ 願 埠 MX 喜好設定 (1-100) ◆ 保安資訊	↓ □ □ □ □ □ □ □ □ □ □ □ □ □	新増 (()) 繼續 [単陶
指定一或多個 網域: savetime.con	n.tw 全部删除 <mark>月城</mark> <u></u> 7: 編輯 創始 主機 器描程式	▲ ↓ 2 通訊	10.10.2.248 每頁的項目數: 10 ▼ 願 場 MX 裏好設定 音詢 (1-100)	↓ i示: ○ ✓ / 0 IP 位址	新増 (()) 縦續 進階
指定一或多個 網域: savetime.con 副除 寄件者網 調度程式並行	n.tw 全部删除 引城 了: 編輯 副時 主機 器描程式	▲ ↓ 2 通訊	10.10.2.248 写真的項目數: 10 ▼ 願 場 MX 高好設定 音詢 (1-100)	↓ i示: ○ ✓ / 0 IP 位址	新増 (()) 縦續 進階
指定一或多個 網域: savetime.con	n.tw 全部删除 引城 了: 編輯 副師 主機 器描程式	▲ ↓ 2 通訊	10.10.2.248 写頁的項目數: 10 ▼ 願 場 MX 高好設定	↓ □ □ □ □ □ ↓ 0 ↓ 0 ↓ 0 □ ↓ 0 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	
指定一或多個 網域: savetime.con	n.tw 全部删除 引城 了: 编辑 一部 書描程式	また。 (2) 通信 通信	10.10.2.248 与頁的項目數: 10 ▼ 顯 場 <u>MX</u> <u>當好設定</u> (1-100)	↓ i示: 0 √ / 0 IP 位址	
指定一或多個 網域: Savetime.com	n.tw 全部刪除 引城 7: 編輯 制約 主機 器描程式 正在儲不	· · · · · · · · · · · · · · · · · · ·	10.10.2.248 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	↓ 示: 0 √ / 0 IP 位址	
指定一或多個 網域: savetime.con	n.tw 全部刪除 現城 7: 編輯 副約 主機 開始程式 正在儲存	▲ ▲ ▲ ▲ ★ ▲ ★ <	10.10.2.248 ■ ■ ■ ■ MX ● ■ ■ ■ MX ● <td>↓ □ □ □ ↓ 0 √ / 0 IP 位址 → □</td> <td></td>	↓ □ □ □ ↓ 0 √ / 0 IP 位址 → □	
指定一或多個 網域: savetime.con	n.tw 全部刪除 引城 7: #輯 書機 書描程式 正在儲存 正在儲存	₹ ₹ ₹ ₹ ₹ ₹ ₩	10.10.2.248 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	↓ □ □ □ □ □ ↓ □ □ ↓ □ □ ↓ □ □ □ □ ↓ □ □ □ ↓ □ □ □ ↓ □ □ □ ↓ □ □ □ □ □ □ □ □ □ □ □ □ □	
指定一或多個 網域: Savetime.com	n.tw 全部刪除 引城 7: 編輯 制約 主聯 開業 開業 正在儲存 「 同服 長	↓ <	10.10.2.248 □	▲ 示: 0 ~ / 0 IP 位址 → □	
指定一或多個 網域: savetime.con	n.tw 全部删除 ^{開城} ⁷ : ^{編輯} ^曲 ^曲 ^曲 ^田 ^田 ^正 在儲存主 「同服手	▲ ④ ④ ④ ④ ④ ● <	10.10.2.248 專頁的項目數: 10 ▼ 願 場 MX 雪詢 (1-100) 余安音軌 SAVETIME B (1-100) シスクション (1-100) シスク	↓ □示: ○ ✓ / 0 IP 位址 → □	
指定一或多個 網域: savetime.con	n.tw 全部删除 ^{月城} ⁷ : ^{編編} 制約 主機 ^{編編} ^{正在儲存} 「 一 一 一 一 一 一 一 一 一 一 一 一 一	₹	10.10.2.248 每頁的項目數: 10 ▼ 顯 場 強約 (1-100) 保安資訊 55000 設定 主更新設定・這可能需要數/ 請務候	▲ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	



◎ 設定群組的規則

預設群組 Default 是代表所有人 (內部網域所有帳號),若 貴公司有些人須做例外處理可在 此新增群組→指定 (內部) 帳號→然後套用不同的 Antispam or Antivirus、內容政策

antec Messa	ging Gateway							登入為	; admir	n [smg999
状態	山報告	🎦 通訊協定	₩ 信譽	🛃 垃圾郵件	🖗 惡意軟體	📃 🖳 威脅防禦	! 🛃 內容		管理	
書	因	2 策群組	次策群组的调谐	政策。						
員 使用者					安谷祖	→				
吏用者 詳組						母代世用者 亞音韵體 威索阿	访御 拉摄郵件	內容渦濾	答押	一般使用
	(Default				✓ —	- V	-	-	-
+ \		click	on it							
員政策 ^{政策群組}	詳組									
ξ群組設定										
策群組名和 -feult	爯:									
erault 成員	惡意	軟體 威脅	方禦	立圾郵件	內容過濾		理 -	-般使用者	Í	語言
一電子郵付 ✓ 啟月 ↓ #	件 用此政策群編 「「「「「「」」	組的入埠惡意軟體	掃描							
Vir	en/J毋以承: us: Clean m =+=====	nessage (default)					``	∙ 檢視		
入 国 Wo	F大重邺奇派 prm: Delete	丙蝨以末: message (default)					• 檢視		
入地	[■] 加密附件I	2策:	Li a D				T NOT VERI			
Enc λ +t	crypted Atta	achment: Modify s	ubject line w	Ith [WARNING	- ENCRYPTE	D ATTACHMEN		(
無	ENTRY PARA	10000-120					``	• 檢視		
入 」 Inb	目可疑附件的 oound suspe	友策: ect virus: Strip att	achments an	id hold message	e in Suspect \	/irus Quarantin	e (default) 🔹	• 檢視		
入垣	目諜程式//	廣告程式政策:			0.6%				_	
Th	reat: Modify	y subject line with	"[SPYWARE	OR ADWARE IN	NFECTED]" (a	lefault)		• 檢視		
無法	5掃猫的人類 因超出限制	卓榴茶 政策而無法掃描的	入埠檔案:							
	Unscannab	ole for Malware an	d Content Fi	Itering: Delete r	message (def	ault)		• 檢視		
	因其他政策	而無法掃描的入埠	檔案: d Contont Fi	ltoring: Doloto I	mossaga (daf	out)		↓ 1会 1目		
天敵	Unscannal	metor Maiware an		itering: Delete i	message (dei	auit)		111176		
無		*/ム1中1曲日1777年1曲ま	<u></u>	IN SECURITY			•	• 檢視		
日啟	用此政策群 防毒政策:	組的離埠惡意軟體	「「「」「「」「」「」「」「」「」「」「」」「」「」」「」」「」」「」」「」」	肖預設勾選	J					
Vir	us: Clean m	nessage (default)						• 檢視		
離増 Wo	和 「 大量郵寄病 orm: Delete	<u> </u>)					∙ 檢視		
離増 End	副加密附件政 Crypted Atta	文策: achment: Modify s	, ubject line w	vith "[WARNING	G - ENCRYPTE	D ATTACHMEN		• 檢視		
離増	解除政策:						`	• 檢視		
離垣 Out	目 可疑附件政 tbound sus	文策: pect virus: Hold m	essage in Su	uspect Virus Ou	arantine (def	ault)		/ 檢視		
離坞 Thr	目諜程式// reat: Modify	富告程式政策: / subiect line with	"[SPYWARE	OR ADWARE II	NFECTED]" (a	default)		/ 檢視		
無法	法掃描的離 地 因紹出限制	旱檔案 政策而無法掃描的	· · · · · · · · · · · · · · · · · · ·							
	Unscannab	ble for Malware an	d Content Fi	ltering: Delete r	message <mark>(</mark> def	ault)	•	• 檢視		
	因其他政策 Unscannab	而無法掃描的離埠 ble for Malware an	·檔案: d Content Fi	ltering: Delete r	message (def	ault)	、	• 檢視		
因解	<u> </u>	無法掃描的離埠檔 録	義:					· 社会 2月		
#								」「魚祝		

儲存 取消

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ 1■



遇到垃圾信處理規則,請改為隔離,不需要用到的取消掉

洋組設定							
群組名稱:							
ault							
成員	惡意軟體	威裔防禦	垃圾郵件	內容過濾	管理	一般使用者	語言
雷子郵件							
5 5h FE		<u>-</u>	再的雨 乙 和 件 特 性				
入埠防	垃圾郵件政策:	AU AX HEIT THAN NO.					
Spam	or Suspected Sp	am: Quarantine	message			✔ 檢視	
不相要	的雪子報件 ②			百步			
入埠可	疑垃圾郵件政策:				动 변경 南北	1945 - 194	
Spam	or Suspected Sp	am: Quarantine	message			✔ 檢視	
入埠客	戶特定垃圾郵件ī						
無						✓ 檢視	
入埠行	鐵電子郵件政策:						
Marke	ting Mail: Modify	subject line with	"[Marketing Mail]	"		► 檢視	
入埠雷	子報政策:			一 此二功	自可視需求情况	Я	
News	etter: Modify sub	ject line with "[N	lewsletter]"		啓用	✓ 檢視	
入埠重	新導向 LIDI 政策	- A -	限电零切				
無			SAVETIME			✓ 檢視	
		INFOR	MATION SECURITY				
□ 啟用山	;政策群組的離埠	垃圾郵件和不想	要的電子郵件掃描				
Spam:	Modify subject	line with "[Spam]	l" (default)			✔ 检視	
7 *8 冊		Lobert Cobert	(ucidally)				
小忠安 離場可	的电子那件 🔮 騷拉協報件政策:						
Suspe	cted Spam: Mod	ify subject line w	ith "[Suspected Sp	am]" (default)		✔ 檢視	
離埠客	戶特定垃圾郵件	 段策:					
無						✔ 檢視	
離埠行	銷電子郵件政策:						
無						✔ 檢視	
離埠電	子報政策:						
無						◆ 檢視	
離埠重	新導向 URL 政策					14 AM	
						一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	
□ 啟用山	政策群組的退回	攻擊防護			てきません		
退回攻	擊防護政策:			JL J	貝可幌 斋 水 啓)	н	
Failed	Bounce Attack V	alidation Reject	message (default			檢視	

◎ 警示通知信的設定,請視 貴單位需求更改值

👺 狀態	山報告	; 💦 通訊協定	🔛 信譽	🛃 垃圾郵件	🖗 惡意軟體	🖳 威脅防禦	🛃 內容	중 管理
 ★ 政策 管使用者 管使用者 管理 ▲ 使用度員 一般技使用者 母数等形命 		警示設定 管理疫情、垃圾製件和 排程工作、服務、硬體 警示設定	病毒過濾、郵件 、交換空間和 U	佇列、磁碟空間、 PS 問題 ▪	SMTP 驗證、目錄	、授權、軟體更新利	口事件等的警示通	知・事件包括已
以設定		 通知资牛者 通知须率: 寄件者: 警示收件者 警示收件者 警示收件者地址: 管理員警示 ② 管理員 ③ admin 		◆ 保安責	<mark>現實際情況調</mark> 知信寄件者地 ^訊		lertAdmin@yourd	小時 ✓ company.ใช้d
UPS ▲ 主機		疫情 過滤	「器 佇歹		SMTP	DDS	授權/更新	事件
1组態 授權 關閉 程式 版本		 事件 2 交換空間使月 2 服務無回應月 2 確確立確 2 確認立確 第開服務 2 戦動服務 2 UPS 狀態 2 已排程工作約 	用率超出 成末正常運作 閉之後啟動服務 失敗	視實際情裡的	況調整這些類 [通知項目	BU	60	%
							儲存	取淌

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■



📟 狀態 🛄 報告	🖬 通訊協定 🔛 信譽 🗖	🖁 垃圾郵件 🛛 😽 惡意軟體	🖳 威脅防禦	🛃 內容 💦 🛜 管理
 ▲ 政策 管理 ◆ 使用者 管理員 一般使用者 	日誌檔設定值 架構本機和遠端記錄的設定。 日誌 題刊			
尋找使用者				
政策群組 金 鉛定	本機 遠端			
警示	─ 本機記錄 ✓ 啟用下列主機元件的本機記錄:	Loca	l Host 🗸	
速管 中心 目読整合 日誌 報告 智慧卡 SNMP UPS	元件本機記錄層級 管道: Brightmail 用戶端: Brightmail 引擎: 鄞件傳輸代理程式: 目錄資料服務: 解除:	警告 警告 警告 警告 警告 警告	> > > > > > > >	
▲ 主機 組版 授權 關閉 公用程式 版本	内容過濾本機記錄層級 内容過濾:	警告 E操长安 貢 訊 SAVETIME MATON SCORT	• 00 MB •	
	日誌清除程式 日誌清除程式頻率: 日誌清除程式開始時間:	[# [0	每天 ∨ 2 ∨ : 00 ∨	親需求情況 調整
	郵件種核日誌 ✓ 取用郵件日誌 刪除資料前,所需要儲存日誌資料 要額取的日誌資料數上限:	4的天數: <u>3</u> 1	2 0000	
	外部日誌說明連結 ☑ 在日該說明中歐用說明連結			
	1		儲存 取消	

◎ 日誌設定,郵件稽核日誌一定要啟用才能追蹤郵件進出的Log

◎ 報告全部勾選

🖾 狀態 📊 報行	吉 🎦 通訊協定	🔛 信譽 🛃 垃圾郵件	<table-cell> 惡意軟體</table-cell>	🔍 威脅防禦	🛃 內容	☐管理
 ▲ 政策 管理 ◆ 使用君 ●使用君 ● 愛求 ● 愛求 ● 愛求 ※ 證 * 設定 警憑 管 證 空 證 ● 心 日 録 ● 登 白 目 録 ● 記 ● 密 ● 日 ● 記 ● 密 ● 日 ● 認 ● 記 ● 密 ● 日 ● 記 ● 図 ● 記 ● ○ 	 報告設定 決定您的報告設定,包括(報告設定 在選擇儲存報告資料 電子郵件報告資料 電子郵件報告資料 電件者 電件者 目で、 電件者 目で、 に、 中者 日 一次 中者 日 一次 日 前 日 一次 日 前 前 一次 日 前 前 前 前 第 日 前 <	儲存的資料量、清除程式速率, 前,請檢查管理指南中有關報 全部勾選 程式設定 將FORMATION SECO 當名格式: 字在MM月d日 hh:mm a}到 {y 07月08日 04:04 下午到 2020年 制面板資料	以及匯出運作方式・]]]] 	符合實際情況的 ail Address	





2-1-3 測試 SMG → 實際 Mail Server flow 是否 OK

以 http://www.alexnolan.net/software/SMTPProber.exe 工具測試 mail flow



稽核 SMG 上的日誌

Symantec Messaging Gatew	ay					登入為:	admin [smg	999.savetime.com.tw] Ф
🖾 狀態 📙 報告	🖬 通訊協定 🔛 信譽	🛃 垃圾郵件	♦ 惡意軟體	🔍 威脅防禦	🗟 内容	📑 管理		
 糸筋 控制面板 主機 日誌 日誌 子類理工作 SMP 野牛疫列 提交詳細資料 		在「必要類型」和「值 式 :代表全部 為邊邊依據的項目] → CSV 分隔符號: 經 寄件者	」 欄位中輸入值。	間範圍: 問題多天的範圍可 [[[[[[[[[[] [[] [] [] [^{過去} 1小時内 該會需要比較長的 清除過濾器 <mark>click heref</mark> 原始主旨	授尋時間 顧示 股石細節 毎頁的項目數:	▼ □通渡 25 ▼) ; 判斷	願示: 1 ▼ / 1 ▼ (*) >) 動作
	2020年07月09日 星期四 下午 04:13	:01 TST jack@microso	ft.com stone.sh	hih@savetime.com	testing mail fr	om 248	無	正常傳送郵件
70 // 70 / · · · · ·								
郵件稽核日誌								
(<上一封)(下一封>	返回郵件日誌							
□ 郵件資料								
ID: 郵件-ID: 接受自: 使用 TLS 接收: 掃描程式: 接受的時間: 方向: 寄件者: 已驗證的使用者名稱: 原始以件者: 原始主旨: 郵件大小: 調別的附件: 可疑附件: 可疑附件:	0a0a02H8-a91ff7000000 <00.00.23872.d81d60ff 否 Local Host 2020年07月09日 星期四 入埠 jack@microsoft.com (無) stone.shih@savetime.co testing mail from 248 1 KB 無	5640-00-5f06618dt ;@smg999.savetime)] 下午 04:13:01 TST m.tw	81b e.com.tw> ♥					
日収件者資料								
目標收件者:	stone.shih@savetime.co	om.tw						
 田 判斷: 田 追蹤程式: 	<u>詳細資料</u> 詳細資料	已成功傳送給	後端					
採取動作:	正常傳送郵件	mail server						
回 俥祥!	◎ 成功 詳細資料							
已傳送至 10.10.1.242:25	• 1997) <u>新日期早日</u> 使用 TLS 傳送 否		傳送時間 2020年07	月09日 星期四	下午 04:13:04	收件者 TST stone.	f shih@save	time.com.tw
觸發的判斷:	無							
未經測試的判斷; 因 MIME 格式錯誤而無 Delete Executable File Authentication: Sende Violations,內容過濾過 subject line with "[Ser 內容過濾過規: Legal [用者允許,使用者拒絕	思法帰措,解除,因解除而無法傷。 s Violations,内容過濾連視:Ser ID Softfail: Modify subject line 現:Sender Authentication:DM der Auth Failure]",内容遏減違 Disclaimer,内容遏減違規:Delet ,病毒攻擊,電子娶件地址授尋び	當, 內容過濾違規: S der Authentication: with "[SenderID So RAC, SPF, SenderID 現: Sender Authenti a True Type Executa 戰, 連線預別, 攔截	ender Authent DKIM Failure: ftfail]", 內容過 Failure: Deleti cation: Validat able Files Viola 的語言, 已知語	cation: SPF So Modify subject 濾違規: Symar e, 內容過濾違 on error: Modi tions, 內容過濾 言	ftfail: Modify su line with "[DK] litec Data Loss i 見: Sender Auth fy subject line v 違規: Sender A	ubject line wi IM Failure]", Prevention, P entication: S with "[Sende Authenticatio	th "[SPF Sc 內容過濾違 內容過濾違: PF, Sender rAuthentica n: DMARC	oftfail]", 內容遏濾達規: 說: Sender 現: Delete Email Policy ID Failure: Modify ation Validation Error]", Failure: Quarantine, 使



2-2 內容政策範例

設定內容過濾條件

簡單解釋:註釋、附件清單、辭典、通知是設定內容可能會用到的資源條件,你可以先設 定或者用預設的即可,也可以用預設的修改。

附件清單的範例~1

Exexcutable Files 可執行檔的定義,如圖,預設清單不能修改,所以我們可先複製再調整清單內容

Symantec Messa	iging Gatew	<i>r</i> ay							登入為: a
쯛 狀態	<u> </u> 報告		🚼 通訊協定	🔛 信譽	² 垃圾郵件	椂 惡意軟體	🔍 威脅防禦	🗟 內容	🗧 😤
 ▲ 政策 電子郵件 ▲ 資源 		附代	牛清單						
社 課 附件清單 辭典		管理	您可以用於定義內 新 新	容過濾政策的附 	件清單。				
通知			附件清單		◆保安資訊		類型	2	
記錄			Archive Files (def	ault) 🗛 📉			高	t.	
▲ 設定			Confidential Docu	<u>ments (refault)</u>	RMATION SECURITY		高隆	ti i	
封存			Design Document	<u>s (default</u>			高	ž	
内谷加密 內容車件資料本			Document Files (lefault)			高降	t.	
DLP 連線			Documents Not F	or Distribution	(default)		高降	2	
△ 事件管理			Executable Files (default)			高隆	ž.	
資料夾總覽			Financial Informa	tion (default)			高別	ž.	
資訊資料夾		0		1.5			n		

附件清單的範例~2

假設我們也要把字型加入 Executable Files 的話,可依下圖方式操作,最後記得按儲存

新增附件清單

新增您可以用於定義內容過濾政策的附件清單。
新增附件清單
附件清單名稱:
MyExecutable Files
新増附件類型
 ● 如果 <u>真實檔案類型</u> ✓ 是 檔案類別:
Database Document Raster image Document Mixed Type Document Communications Format Font Type Document Vector graphic Document Vector graphic Document FAX Format Movie File Object Module Format Executable File General Purpose Documen Scheduling/Planning Form Spreadsheet Document Presentation Document
○ 如果 副權名 ♥ 是 ♥
新增
刪除
□ 附件類型 ^
□ 真實檔案類型 是 ELF Executable
□ 真實檔案類型 是 MS-DOS Batch File
□ 直會檔案類型 是 MSDOS Device Driver





註釋的範例

注釋就是在郵件內文裡插入一段文字警告或聲明,此例我們新增一個(往下設定內容範例 會用到)



插入文字敘述(請自行定義)

Symantec Messag	ging Gateway						
₩ 狀態	山報告	計 通訊協定	🔛 信譽	🚽 垃圾郵件	😽 惡意軟體	🖳 威脅防禦	内容
 ➡ 政策 電子郵件 ▲ 資源 ■ 資源 ■ 請評評局單 ● 期時 ● 請評評局單 ● 請評評局單 ● 請評評局單 ● 算件 ● 第 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		↓ 通訊協定	Unicod 、不符公司政策 Unicod 件含有可執行權 !	■ <u>U</u> 双野件 e (UTF-8) , 已被移除該執行 , 已被移除該執行 e (UTF-8) , 不符公司政策,		■ 嚴脅防禦	
				8 00 00	100		



新增內容政策

Symantec Messa	aging Gateway							登
🗠 狀態	山報告	🚼 通訊協定	₩ 信譽	<mark>-</mark> 垃圾郵件	🖗 惡意軟體	🖳 威脅防禦	🗟 內容	
政策 電子郵件		子郵件內容 鏈 ^{理您組織的內容過濾 新增 電子郵件內容過濾 Delete Executable}	D 濾 政策 · · · · · · · · · · · · ·	系安資訊 AVETIME 別除 ^{、CO} CRITE 版用	停用			\$

直接選用空白政策即可

新增內容過濾政策

建立新的內容過濾政策。

政策範本		任何資	源類型
空白		(•
	SAVETIME INFORMATION SECURITY	選取	取消
政策範本		描述的 内容	結構化
Caldicott Report		0	0
Canadian Social Insurance	Numbers	0	
Competitor Communication	s	0	

給上可自行辨識的政策名稱,改為入埠郵件即,然後按新增

新增電子郵件內容過濾政策

-刪除可執行檔附件			
設定			
✓ 在控制面板和報告中 ○ 停用 ✓ 清單中相 ※ 續內容禍濾處理	[•] 追蹤此政策的 當案的分解	建規 Archive Files (default)	~
繼續進行評估	和動作	保安資訊	~
條件		SAVETIME	
賽用至: 必須符合下列哪一個條何	INFORM	<u>入埠郵件</u> 任何	~
新増 編輯		€ (X & Y) (X),(Y)	
□ 條件			Ξ

業界公認 保安資訊--賽門鐵克解決方案專家 ■ ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■



點選「附件或內文部份」並點「位於附件清單」,按下拉選單找到前述自訂的清單名稱,然後 按新增條件

內容過濾政策條件

新增條件至內容過濾政策。

內容過濾	政策條件	
○ 主旨□ 啟用	、內文或附件中的文字: HTML 標籤掃描 (郵件內文)	
0	含有 🖌 🖌 個或更多文字源自於:	ABA Routing Number Keyworc 🗸
0	符合規則運算式 🗸 🗸	4
0	符合樣式 🖌 🖌	Credit Card (基本) 🗸
Ot	北對記錄資源中的資料:	~
杓	<u></u>	~
콖	需要出現的最少次數:	1
○ 在此	郵件指定部分中的文字: 会右	[選取郵件部分] ✔
0		
0	符合規則運算式 🗸 🗸	
0	符合儀式 INFORMATION♥ CURTY	Credit Card (基本) 💙
〇在此	郵件標頭指定部分中的文字:	信封收件者
含有	頁 ▼ 電子郵件地址 》源自辭典:	ABA Routing Number Keyworc 🗸
	【包含 ~	[選取郵件部分] 🖌
〇郵作	≢大小 ~	等於 🖌 🔽 位元組 🖌
○ 附件	或內文部分:	
•	位於附件清單:	MyExecutable Files
0	其福業名稱包含: ✓	
0	其 MIME 類型為: 🛛 🖌	N
0	其檔案名稱源自辭典: 🖌 🖌	ABA Routing Number Keyworc 🗸
0	其副檔名源自辭典:	ABA Routing Number Keyworc 🗸

- RA-479 /+ FR

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ 1■



設定動作

新增二項動作,一為刪除附 件,指定為前述所作的可執 行檔附件清單,二為新增註 釋動作,指定前述的註釋, 且群組務必一定要勾選才會 生效,然後按儲存

00-刪除可執	架構動作 🛛 🔀
設定	milta 04 14
✓ 仕控制	
後續內容對	○ 刪除所有附件
	● 刪除附件清單: MyExecutable Files ✔
—條件 春田	○刪除相符附件 需要特別套用至附件的條件要求
▲// 五/ 必須	本 女 頁 部 SAVETIME
75.146	INFORMATION SECURITY
新項	架構動作
	新焼註羅
- N I	◎ 在後面添加註釋
動作 指定要對學 新增 ① 動作 ② 新牌註	新增二個 動作 如前作 編輯 刪除 單「MyExecutable Files」中的附件 運「MyExecutable Files」中的附件
套用至下列	
☑ 政策群	‡#E
Deraul	
記得	要打勾
	儲存 取消

可到管理→群組→Default→内容過濾驗證我們設的內容條件有加進來囉!

政策を稱・

₩ 狀態	山報告	🚼 通訊協定	🦾 信譽		🖗 惡意軟體	🖳 威脅防禦	🛃 內容		🗟 管理	
 ▲ 政策 管理 ▲ 管使用者 管使用者 一般使用者 政策群組 ▲ 設元 		編輯政策群組。 編輯政策群組。 政策群組設定 政策群組名稱: Default	∄	 ▲ ▲ /2, 42 	答胡					
 憑證 控管中心 目錄整合 日誌告 報告 SNMP UPS ▲ 主機 		成員 図 啟用此政 内容過濾頭 [選取「か 〕 入埠!	惡意軟體 策群組的入埠「P 20天: 1容過濾」政策] 內容過濾政策 別除可執行描附件	威發防禦 Strormations 9容過濾」	应扱郵件 A	的容過濾		 一般● 新増 刪除 檢視 	檢視	語言





2-3 其他的建議設定

👺 狀態	山報告	🚰 通訊協定	₩ 信譽	🚅 垃圾郵件	🖗 惡意軟體	🔍 威脅防禦	🛃 內容
 ▲ 政策 攔截的寄件者 連線類別 允許的寄件者 ▲ 信智工具 尋找寄件者 	損	載截的寄件者 不良信誉的寄件者等 可以選擇 Symantec 防。	e構群組。可建立 Messaging Gatev	和管理由管理員本機 vay 對每個群組的鄧	定義的攔載的寄件 件採取的動作。您(者群組、第三方清單 也可以架構電子郵件	I以及賽門鐵克全域攔着 +地址搜尋攻擊預防和者
11 信誉宣関	(漏戰 高件者群組 □ 本機攔截的寄件者 □ 本機管理員新増的	限用 停用	3		已啟用	動作 刪除郵件
		□ <u>本機攔截的寄件者</u> 本機管理員新增的	IP ①IP 位址。	Yボ安貧訊 SAVETIME		✓	拒絕 SMTP 連線
		□ <u>攔截的第三方寄件</u> 本機管理員訂購的	<u>*者</u> 5第三方 IP 位址清	揮。		1	拒絕 SMTP 連線
	l	□ <u>賽門鐵克全域攔着</u> 由賽門鐵克基於全 Network 一部分的	<u>t的寄件者</u> ≧球信譽資料 (這些 ∋ Brightmail IQ 服	些資料來自屬於 Syma 發務) 提供的 IP 位址	antec Global Intelli °	gence 🗸	拒絕 SMTP 連線
		□ <u>電子郵件地址搜</u> 易 □ 架構電子郵件地址 動作。	<u>教戰</u> 上搜尋攻擊識別, 1	並指定發生電子郵件	地址搜尋攻擊時要;	採取的 —	延遲 SMTP 連線
		□ <u>電子郵件病毒攻</u> 響 架構電子郵件病费	屢攻擊識別,並指:	定發生電子郵件病毒	攻擊時要採取的動作	/۴ · –	延遲 SMTP 連線

		5 250 all 1000 AE	間當	业极野件	∞ 法意軟體	
 ▶ 政策	電- 架構 電-	▲ 理由 mode 子 郵 件 病 毒 功 電子 郵件病毒 攻擊 子 郵件病毒 攻擊 不動用電子 郵件病 電子 郵件病毒 攻擊 不動用電子 郵件病 電子 郵件 協力 電子 郵件 協力 能用電子 郵件 「 市場 郵 件 取目 下 腐 中 間 常 一 、 、 、 、 、 、 、 、 、 、 、 、 、	the first f	■ 型級郵件 主電子郵件病毒攻擊 50 2 10 90 30 40 50 2 10 90	☆ 法息軟賠	
		□ 動作				
		U 姓狸 SMTP 建	AF.			
					儲存	取消





2-4 備份設定部份

₩ 狀態	山報告	🚼 通訊協定	🔛 信譽	🛃 垃圾郵件	🖗 惡意軟體	🖳 威脅防禦	🗟 內容	🗟 管理
 ▲ 政策 管理 ▲ 使用者 管理員 一般使用者 		主機版本 管理您主機的軟體版本・ 版本	,					
尋找使用者 政策群組 ▲ 設定 警示		備份 執行未排程備份		還原/下載	重設為出廠值		更新 立即備1	Э
憑證 控管中心 目錄整合 日誌		新增		除 安 了 SAVETIN	資料		排程	
報告 智慧卡 SNMP UPS								
▲ 主機 組態 授權								
開閉 公用程式 版本								

建議做最少備份即可

強烈建議一定要用 FTP 備一份設定檔到外部儲存媒體(新增第二筆備份排程),不然一旦 SMG 全掛,則儲存在 SMG 內部儲存檔案系統的設定檔備份應該也是撈不回來。

新增已排程備份

11日に 11日 (井 /4)					
埠口排栏1角1万					
第份說明:					
Veekly-BK					
備份資料					
 ○ 完整備份 ♥ ○ 白訂供約 					
● 日司佣切… ~					
○ 催成泉 ●	ξ) ②				
● 温恩 (已泊政外	4 一 1 4 一 1 4 一 1 4 一 1 4 1 4 1 4 1 4 1				
□ 包括報告資	[料]				
□ 包括日誌資	【料				
借份排程					
席(J)非1至 產生備份於		•			
○ 毎日					
 ○ 每日 ● 每天 ○ 僅⁻ 	工作日				
 ○ 毎日 ● 每天 ○ 僅1 ● 毎週 					
 ○ 毎日 ● 每天 ○ 僅 ○ 毎週 ✓ 星期日 	工作日 三期一 □ 星期二 □ 星期三				
 ○ 每日 ○ 每天 ○ 僅 ○ 每週 ✓ 星期日 □ 星期四 □ 星期四 	工作日 				
 毎日 毎天 ● 毎週 ✓ 星期日 ■ 星期日 ■ 星期日 ■ 星期日 ● 毎月 	工作日 開一	借份	<u>주</u>		
 毎日 毎天 ● 毎週 望星期日 星期四 星期四 毎月 第 天(每月) ● 毎月 	工作日 観川一 ロ 星期二 ロ 星期三 副ガ ロ 星期六	備份	至	444	
 毎日 毎天 ● 毎週 望 星期日 星期四 写 毎月 第 天(毎月1) ● 毎月 毎月的最後一天 	工作日 2期一 ロ 星期二 ロ 星期三 2期五 ロ 星期六 約)	備份	至	份	
 毎日 ● 每天 ● 每週 型 星期日 ■ 星期四 □ 星期四 □ 写前 ○ 第一天(每月1) ○ 第一天(每月1) ○ 毎月的最後-7 備份至 ○ 毎句用昭器上様友備 	□ 作日	備份	至 至何服器上儲存備 医儲存的備份數目	份	3
 毎日 ● 每天 ● 每週 型 星期日 星期四 写用 ● 毎月 ● 年伺服器上儲存備 ● 要感在的備份動日 	正作日 朝一 ロ 星期二 ロ 星期三	備份 〇 1 雪	至 车伺服器上儲存備 要儲存的備份數目 运端位置上儲存	份 : 備份	3
 毎日 ● 每天 ● 每週 型 星期日 星期四 9 毎月 ● 毎月 ● 毎月 ● 毎月 毎月的最後→み 備份至 ● 在伺服器上儲存備 要儲存的備份數目 ○ 在遺跡位置上儲存 	正作日 建期一 ロ 星期二 ロ 星期三 開五 ロ 星期六 約) こ 借份 第 二 二 二 二 二 星期三 二 3 二 二 二 二 二 二 二 二 二 二 二 二 二	—備份 ○ 1 ◎ 1 〕	至 至伺服器上儲存備 要儲存的備份數目 至遠端位置上儲存 通訊協定:	份 : 備份 FTP	3
 毎日 ● 每天 ● 僅 ● 每週 ■ 星期田 ■ 星期四 ● 毎月 ● 毎月 ● 毎月的最後→み 備份至 ● 在伺服器上儲存備 要儲存的備份數目 ○ 在遠端位置上儲存 通訊協定: 	正作日 建期二 ロ 星期二 ロ 星期三 副五 ロ 星期六 的) こ 備份 「TP	- 備份 ○ 1 ◎ 1 〕	至 至伺服器上儲存備 要儲存的備份數目 左遠端位置上儲存 通訊協定: 主機/IP 位址:	份 : 備份 	3
 毎日 ● 每天 ● 僅 ● 每週 ■ 星期日 ■ 星期日 ■ 星期日 ● 毎月 ● 毎月 ● 毎月的最後	正作日 星期二 □ 星期二 □ 星期三 開五 □ 星期六 部) で 備份 FTP 「 日	—備份 ○ 和 ◎ 和 ミ	至 车伺服器上儲存備 要儲存的備份數目 主遠端位置上儲存 通訊協定: 主機/IP 位址: 通訊埠:	份 : 備份 	3
 毎日 ● 每天 ● 僅 ● 每週 ☑ 星期田 □ 星期四 □ 雪 ○ 每月 ● 毎月 ○ 毎月 ● 毎月 ○ 毎月 <li< td=""><td>正作日 星期二 □ 星期二 □ 星期三 副五 □ 星期六 的)</td><td>— 備份 ○ 看 ◎ 7 ミ ミ</td><td>至 车伺服器上儲存備 要儲存的備份數目 车遠端位置上儲存 通訊協定: 主機/IP 位址: 通訊埠: ^{各徑:}</td><td>份 : 備份 FTP 21 /SMCPP/</td><td>3</td></li<>	正作日 星期二 □ 星期二 □ 星期三 副五 □ 星期六 的)	— 備份 ○ 看 ◎ 7 ミ ミ	至 车伺服器上儲存備 要儲存的備份數目 车遠端位置上儲存 通訊協定: 主機/IP 位址: 通訊埠: ^{各徑:}	份 : 備份 FTP 21 /SMCPP/	3
 毎日 ● 每天 ● 僅 ● 每週 ■ 星期四 ■ 星期四 ● 毎月 ● 毎月 ● 毎月 ● 毎月的最後	工作日 星期二 □ 星期二 □ 星期三 開五 □ 星期六 的) : : : : : : : : : : : : :	備份 ○ 7 美 王 美 正 王 王 王 王 王 王 王 王 王 王 王 王 王	至 至伺服器上儲存備 要儲存的備份數目 至遠端位置上儲存 通訊協定: }機/IP 位址: 通訊埠: 會徑:	份 : 備份 FTP 21 /SMGBK/	3
 毎日 毎日 毎天 僅 毎週 星期四 毎月 毎 毎	正作日 星期二 □ 星期二 □ 星期三 開五 □ 星期六 部) ご 第 の 第 の ・ 第 の ・ ・ ・ ・ ・ ・ ・ ・ ・	備份 ○ 7 美 王 美 正 日 日 日 日 日 日 日 日 日 日 日 日 日	至 左伺服器上儲存備 要儲存的備份數目 至遠端位置上儲存 通訊協定: }機/IP 位址: 通訊埠: 魯徑: 聲 需要驗證	份 : 備份 FTP 21 /SMGBK/	3 注意路徑寫过 ME RITY
 每日 ● 每日 ● 每天 ● 僅 ● 每週 ■ 星期四 ■ 星期四 ■ 毎月 ● 毎月 ● 毎月前最後一み 備份至 ● 在伺服器上儲存備 要儲存的備份數目 ● 在遠端位置上儲存 ● 在遠端協定: 主機/IP 位址: 通訊埠: 路徑: □ 需要驗證 使用者名稱: 	正作日 星期二 □ 星期二 □ 星期三 開五 □ 星期六 部) 部 、 第 の 、 第 の 、 、 、 、 、 、 、 、 、	備份 ● 1	至 左伺服器上儲存備 要儲存的備份數目 至遠端位置上儲存 翻訊協定: 註機/IP 位址: 通訊埠: 魯徑: ② 需要驗證 使用者名稱:	份 : 備份 FTP 21 /SMGBK/ SMGBK	3 注意路徑寫过 ME RITY

業界公認 保安資訊--賽門鐵克解決方案專家 ■■■ We Keep IT Safe, Secure & Save you Time, Cost ■■■



若有需要可從還原/下載可回復之前的設定

SMG 提供三種方式還原:

- 從伺服器還原/下載備份一即 SMG 本身內的備份檔,即此例中上述設定的備份檔
- 從遠端位置還原備份—即備份到遠端 FTP 內的備份檔
- 從您的本機電腦上載備份檔案一即從連到 SMG WEB console 的本機電腦處上傳備份檔還原

主機版本

<u>x</u>			
備份	還原/下載	重設為出廠值	更新
〇 從伺服器還原/下載備份			
可用的備份			
• db-backup.10.7.3-	5.brightmail.Jul-10-20-	16-10.config-incidents.manua	al.tar.bz2 502.86 KB
○ 從遠端位置還原備份			
通訊協定:		保宙資訊	
主機/IP 位址:		SAVETIME	
通訊埠:		21	
檔案名稱:			
□ 需要驗證			
使用者名稱:			
密碼:			
○ 從您的本機電腦上載備(分檔案		
指定備份檔案:		翅擇樟安	土選擇任何機安
		1年1年1日共	不选择任何抽来

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ 1■



3 升級

3-1 從WEB介面更新

👺 狀態	山報告	🎦 通訊協定	🔛 信譽	² 垃圾郵件	🖗 惡意軟體	🔍 威脅防禦	🛃 內容	🗃 管理
 ▲ 政策 管理 ▲ 使用者 管理員 一般使用者 	主 管理	機版本 ^{里您主機的軟體版本。}						
尋找使用者 政策群組 ▲ 設定 警示		備份 主機:	遭 Local H	原/下載 ost	重設為出廠值	更	新 ✔ 重新整理	
憑證 控管中心 目錄整合 日誌		目前的版本 10.7.1-6		保安資訊 SAVETIME		狀態 更新可用		
報告 SNMP UPS	۲	可用於更新的版本 ● 10.7.3-5				狀態 可供下載		
▲ 主機 組態 授權		0 10.7.3-4	1			可供下載		
開閉 公用程式 版本			檢查更新					

當無法從 WEB 介面正常更新時(大部份都是出現 time out 的狀況),可以選擇從命令模式更新

3-2 從命令模式更新(原廠 prefer 用此方法更新,另有 Command SOP 文件 ,請聯絡保安資訊索取)

- 開啟 console 介面以admin登入
- 輸入 update list (列出可更新的版本)
- ■選擇要更新的版本,如10.7.3-5,命令如下:
- update --version 10.74.3-5 install







附註 A:常用它項進階功能如下,請聯絡保安資訊以獲得更進一步資訊 ……

- 1. 目錄整合設定
- 2. 新增探查電子郵件地址以提高防垃圾郵件的效率
- 3. 客戶特定垃圾郵件提交設定
- 4. 內容事件資料夾的設定

附註 B:SMG 的一些架構流程圖

A closer look at Symantec Messaging Gateway





業界公認 保安資訊--賽門鐵克解決方案專家 We Keep IT Safe, Secure & Save you Time, Cost ■1■



關於保安資訊: 從協助顧客簡單使用賽門鐵克方案開始,到滿足顧客 需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克
 解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽
 門鐵克資訊安全解決方案的銷售、規劃與
 整合、技術支援、教育訓練、顧問服務,
 特別是提供企業 IT 專業人員的技能傳承
 (Knowledge Transfer)的效益上,以及比原廠
 更快速的技術支援回應,深獲許多中大型
 企業與組織的青睞(特別是有IT Team的組
 織),長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是,我 們不吝惜分享我們的專業技能與經驗給顧 客的IT Team,經由常態性的教育訓練、精 簡的快速手冊以及標準SOP 文件的提供,

以及基於比原廠更孰悉顧客的使用環境與 現況的快速回應的品質,在業界建立扎實 的口碑。

 保安資訊一直專注於賽門鐵克領先業界的 資訊系統基礎架構上的安全性與可用性的 解決方案。進而累積了許多與基礎架構整 合的成功經驗,讓導入Symantec 解決方方 案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或 自行摸索的運作風險。

●保安資訊:
 保安資訊有限公司
 <u>http://www.savetime.com.tw</u>
 0800-381500、0936-285588

業界公認 保安資訊--賽門鐵克解決方案專家 ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■