保安資訊
SAVETIME
INFORMATION SECURITY

Symantec Messaging Gateway 10.7.x Virtual Edition

安裝、基本設定及版本升級使用手冊

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。

目　錄

1 全新安裝

1-1 系統需求

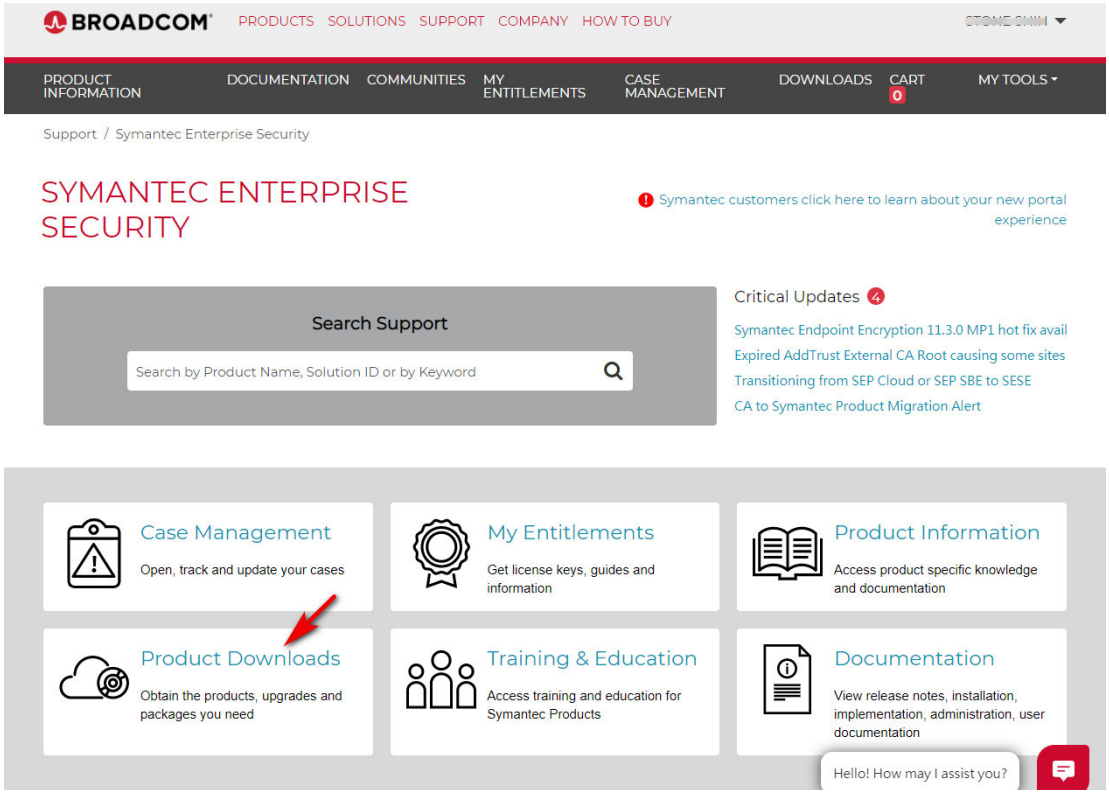
SMG VM 版本支援 VMware 或 Microsoft Hyper-V

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

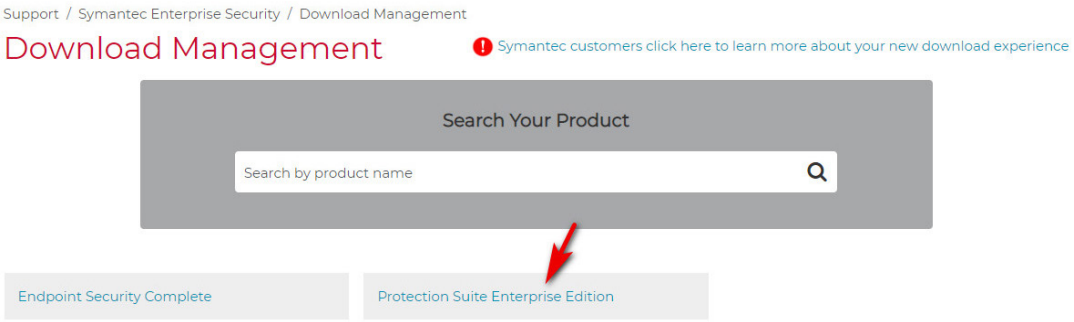
1-2 Symantec Message Gateway 10.7.x Virtual Edition下載（以ISO檔安裝為例，虛擬環境請依實際情況擇一參考）

■取得Symantec Message Gateway 10.7.x Virtual Edition

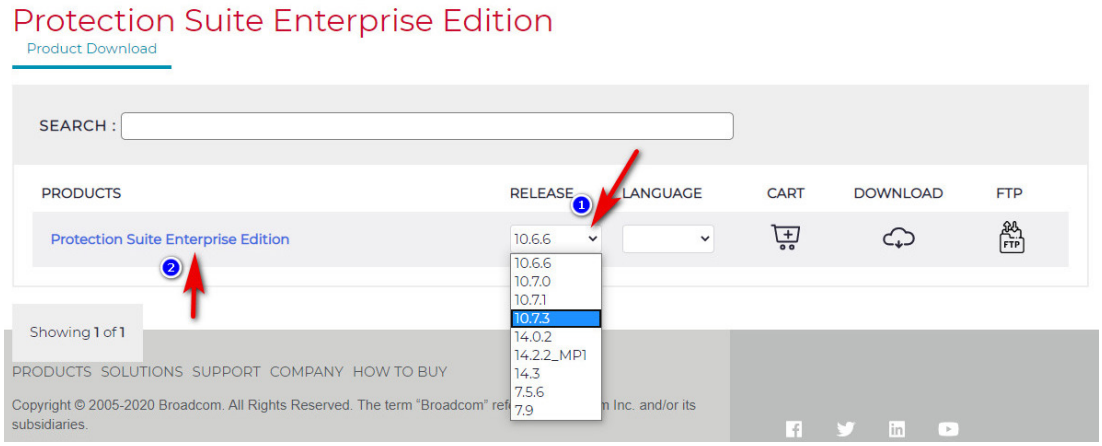
您的授權必須是SPSEE或單獨的SMG才能下載，登入MyBroadcom(https://www.broadcom.com/mybroadcom/login)後依如下操作



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



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

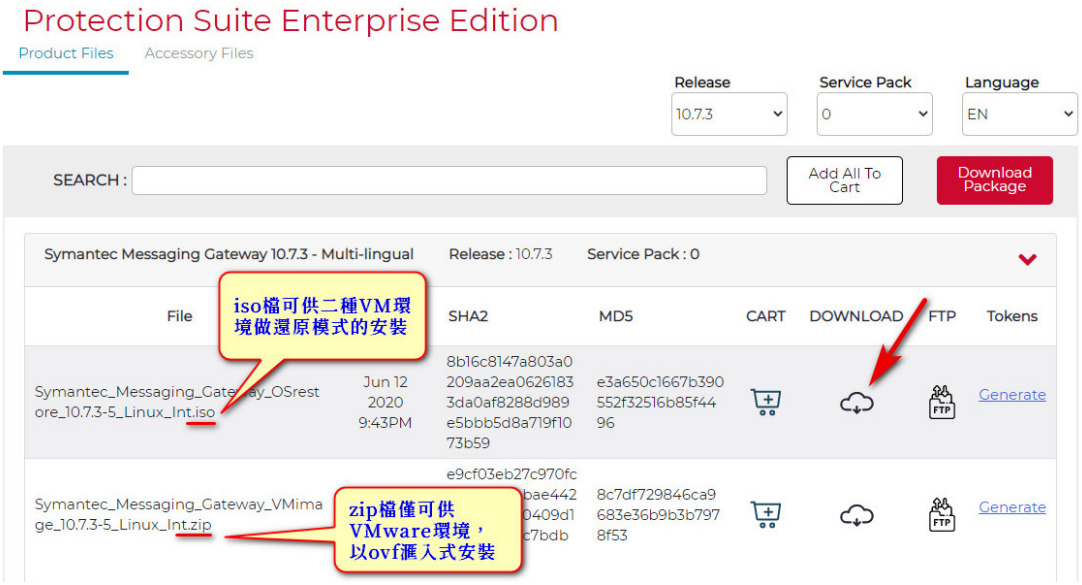


SMG 的下載提供二種檔案：

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）。



1-2-1 在 VMware 上設定虛擬環境安裝 SMG

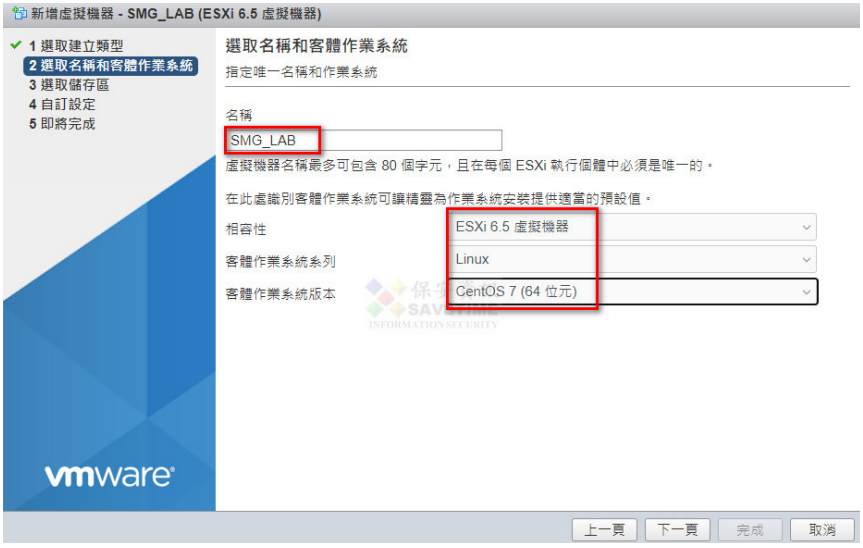
虛擬環境的建立非本文重點，請自行參考 VMware 或 Microsoft 文件，以下為透過 SMG iso 檔的安裝步驟。

1 選取建立類型

在 ESXi/vSphere 的 console 介面上，新增虛擬機器

2 選取名稱和客體作業系統

給予虛擬機器名稱及指定作業系統及版本對應



3 選取儲存區

指定存放此虛擬機的儲存區

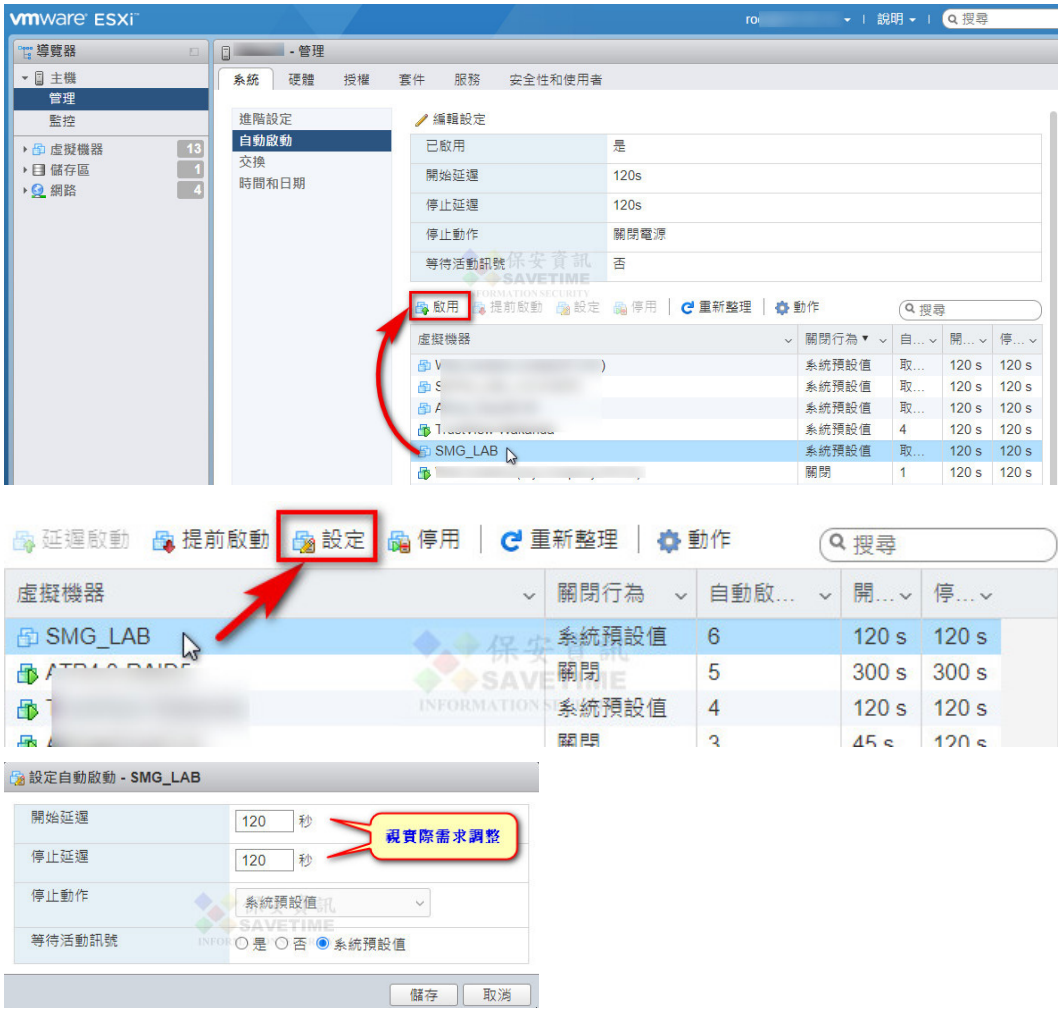
4 自訂設定

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

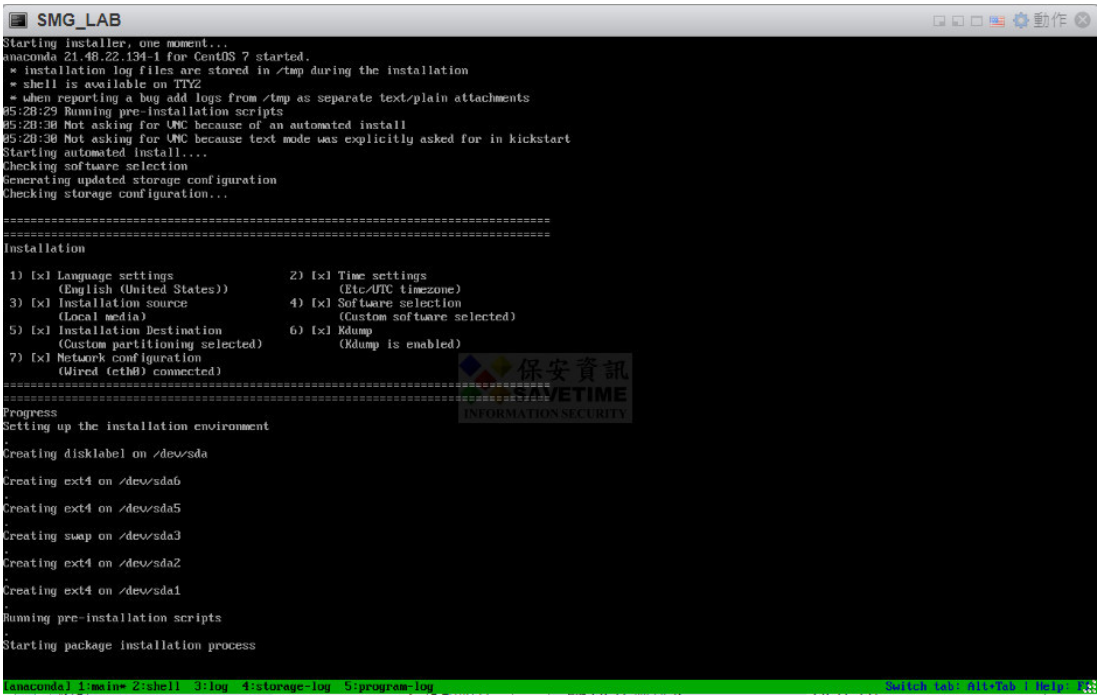
確定無誤後按完成以建立此 VM

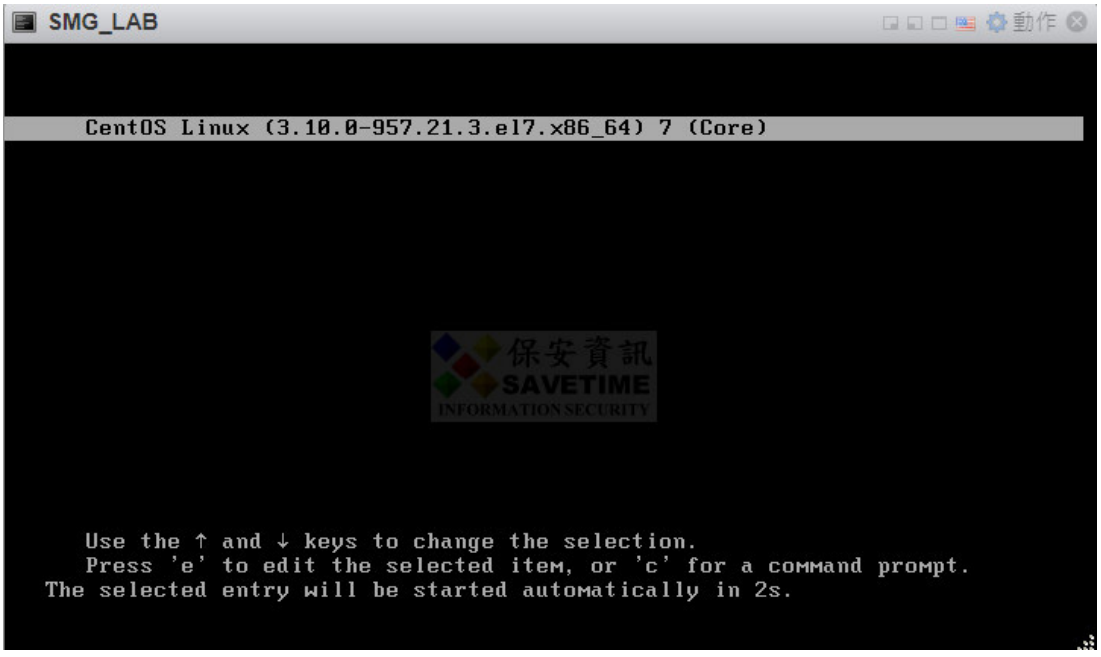
■設定自動啟動



■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



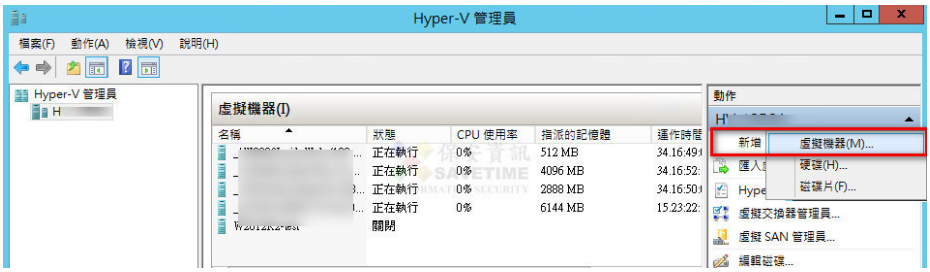


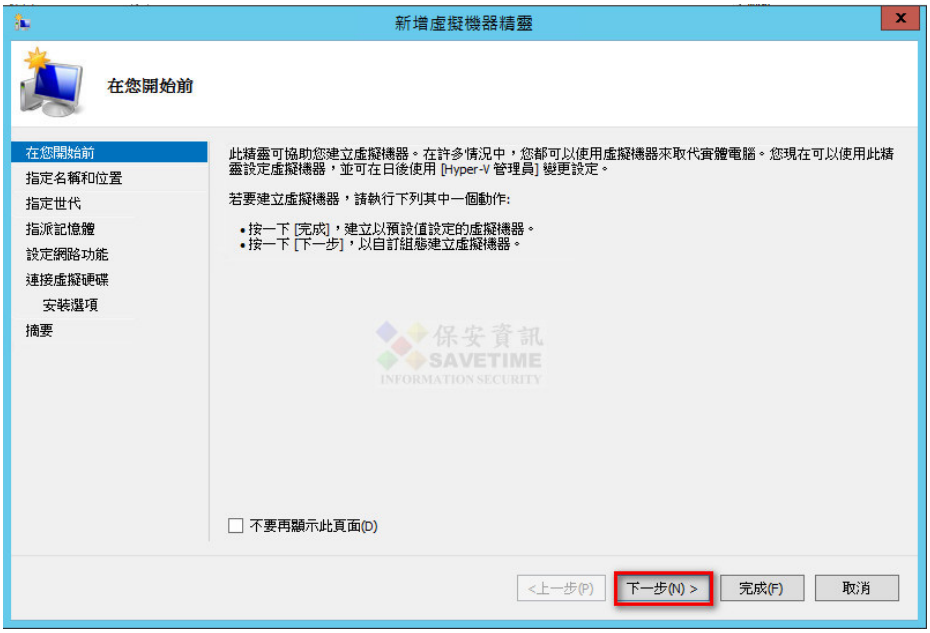
請接續 1-3 做後續初始化設定

1-2-2 在 Hyper-V 上設定虛擬環境安裝 SMG

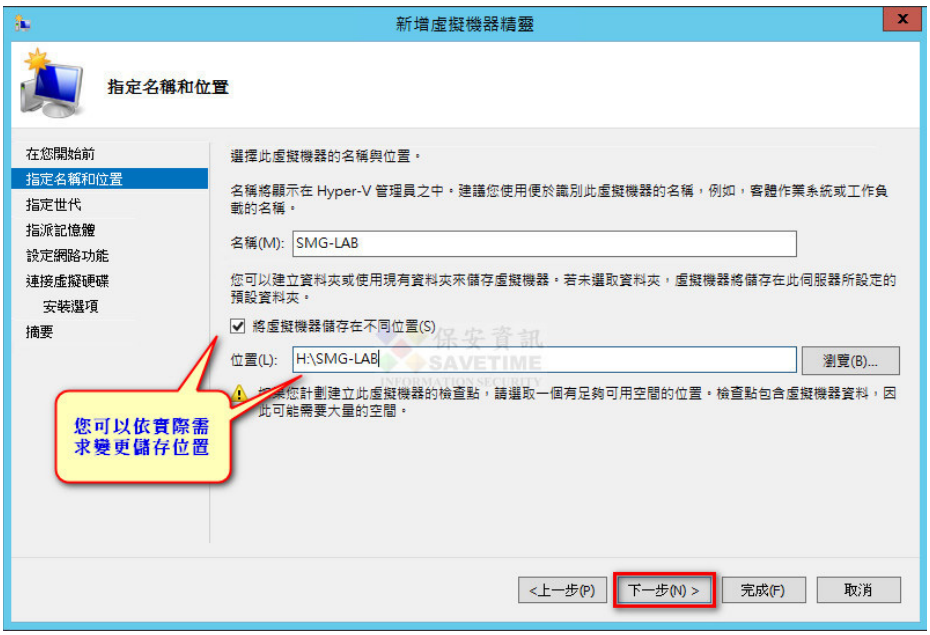
若使用 VMware 環境請直接跳到 1-3 做後續初始化設定。

■新增虛擬機器

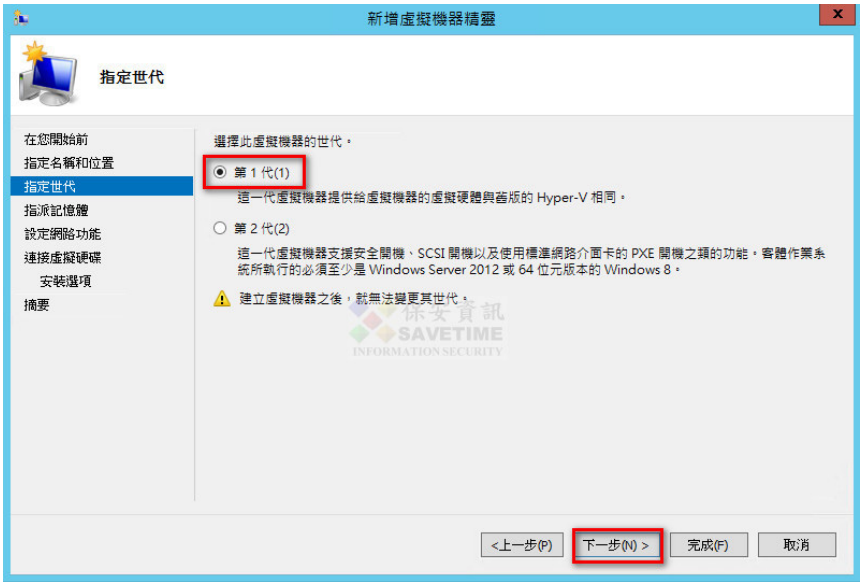




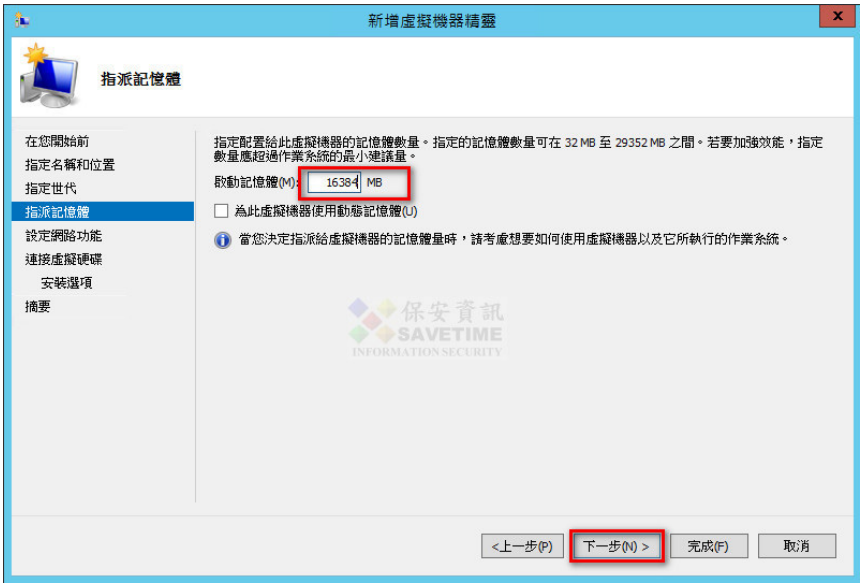
■設定虛擬機器名稱及指定其儲存位置



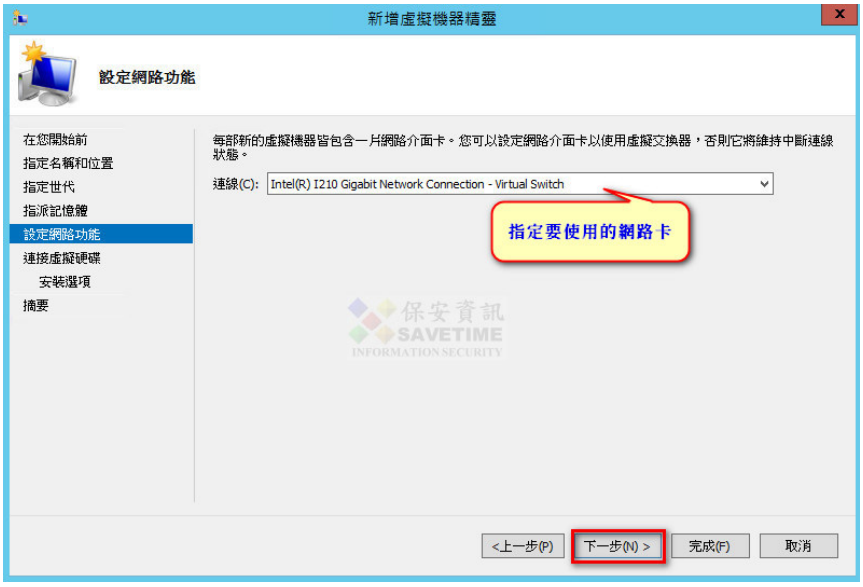
■ 設用第一代虛擬機器



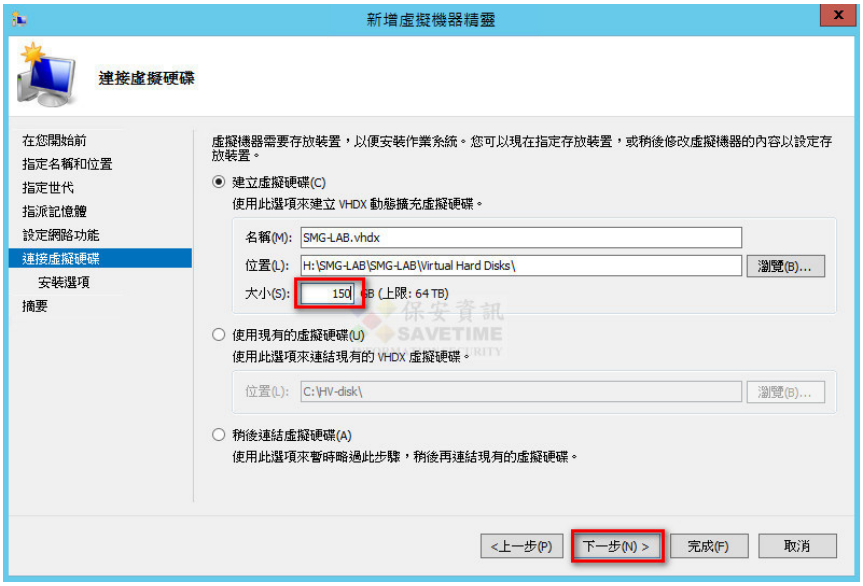
■ 指定記憶體



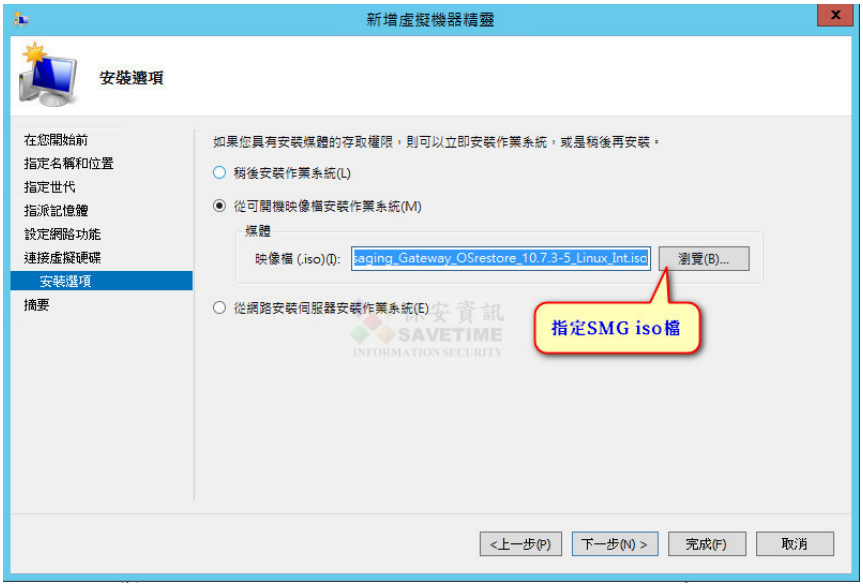
■ 依實際狀況指定網路卡



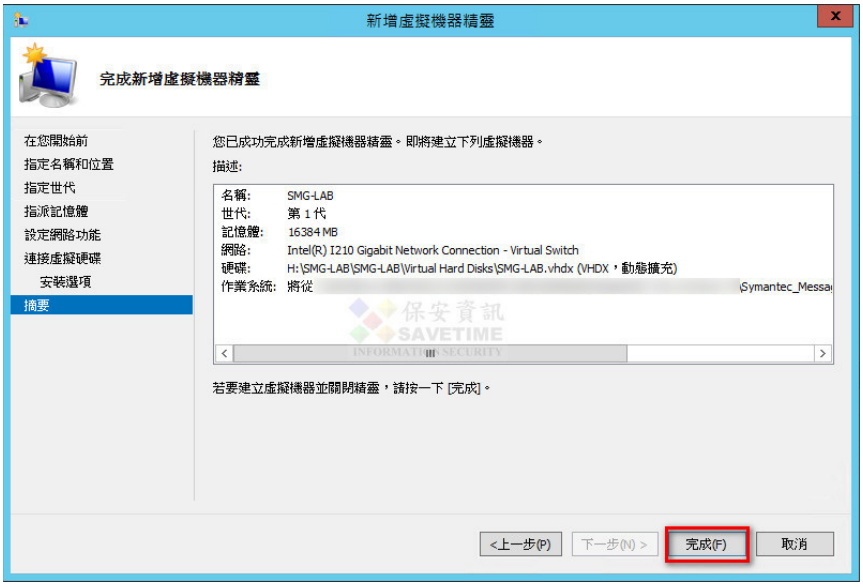
■調整硬碟大小



■指定安裝需求的 SMG iso 檔



■Review 上面的設定，
若沒問題按完成

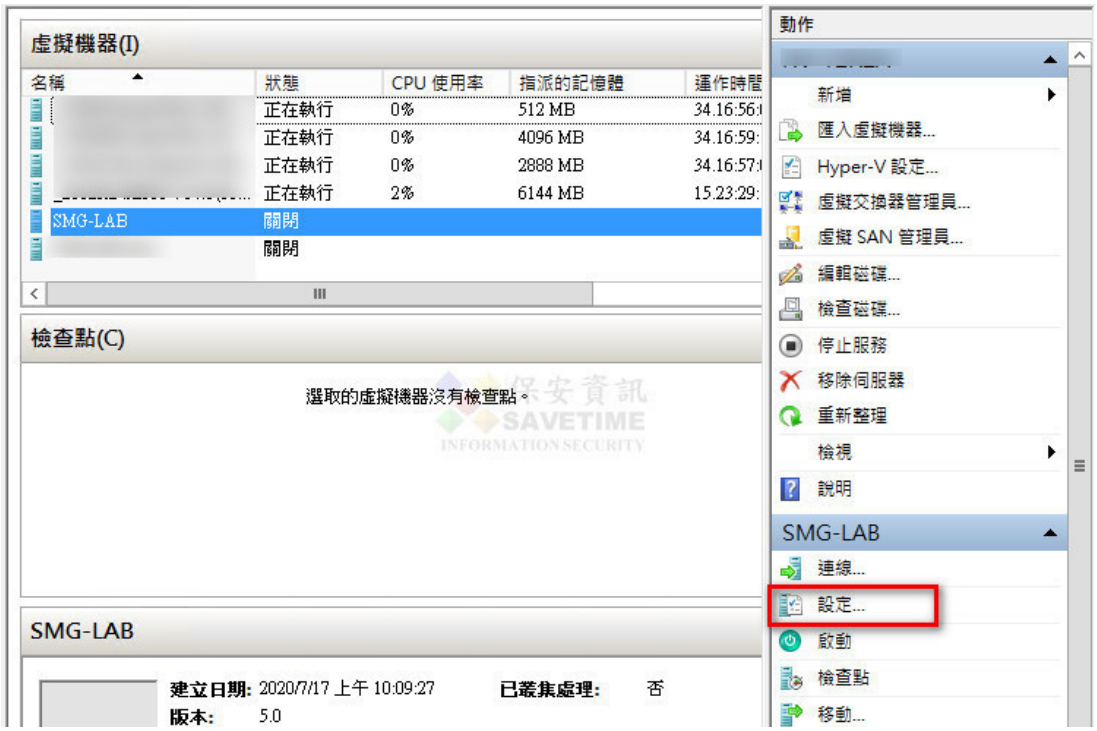


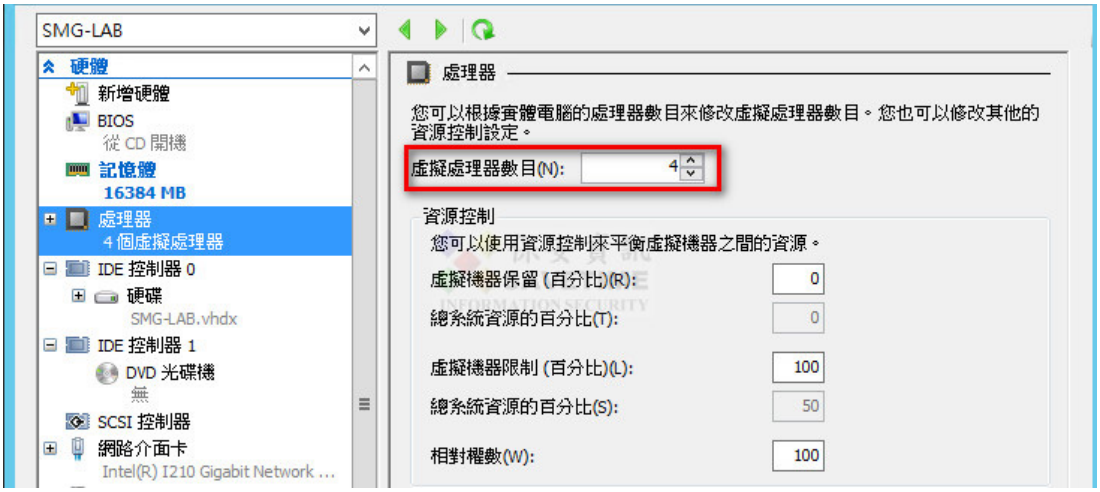
■虛擬機器建立中

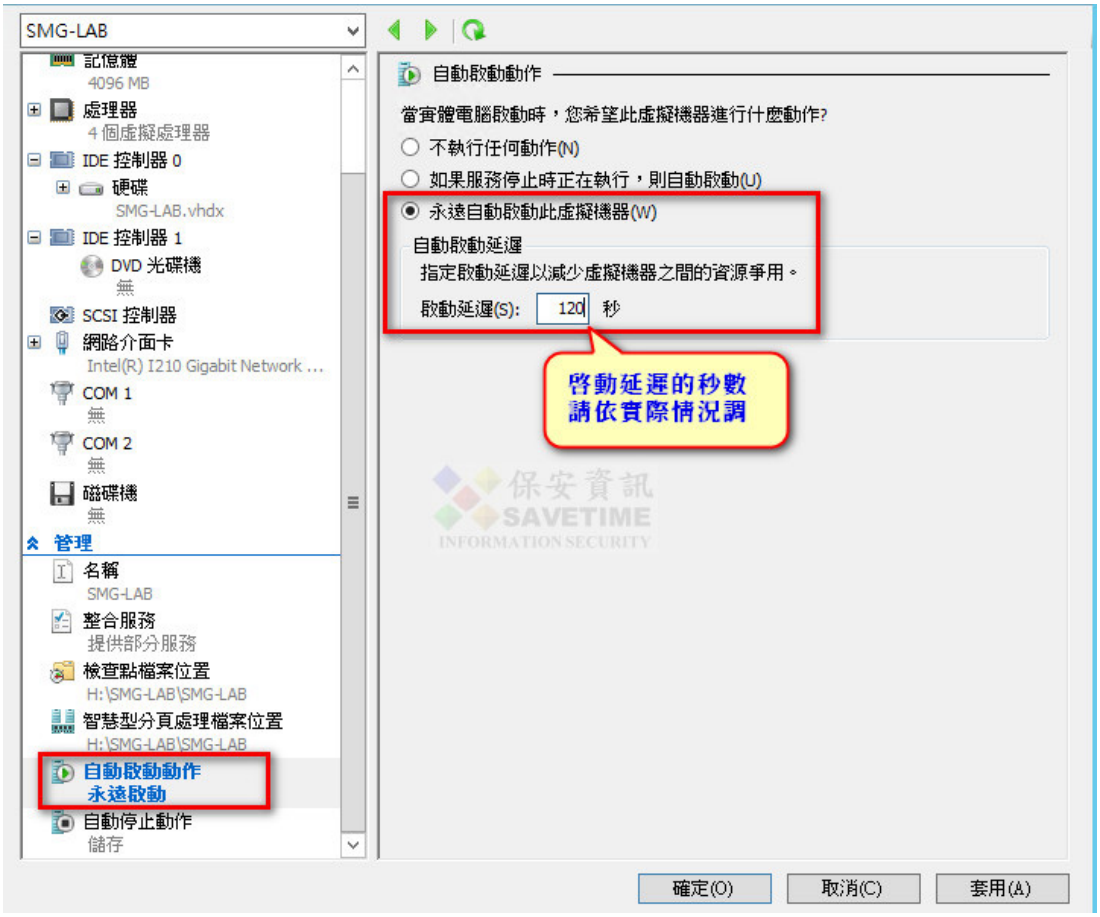
■修改設定

處理器改為 4 顆

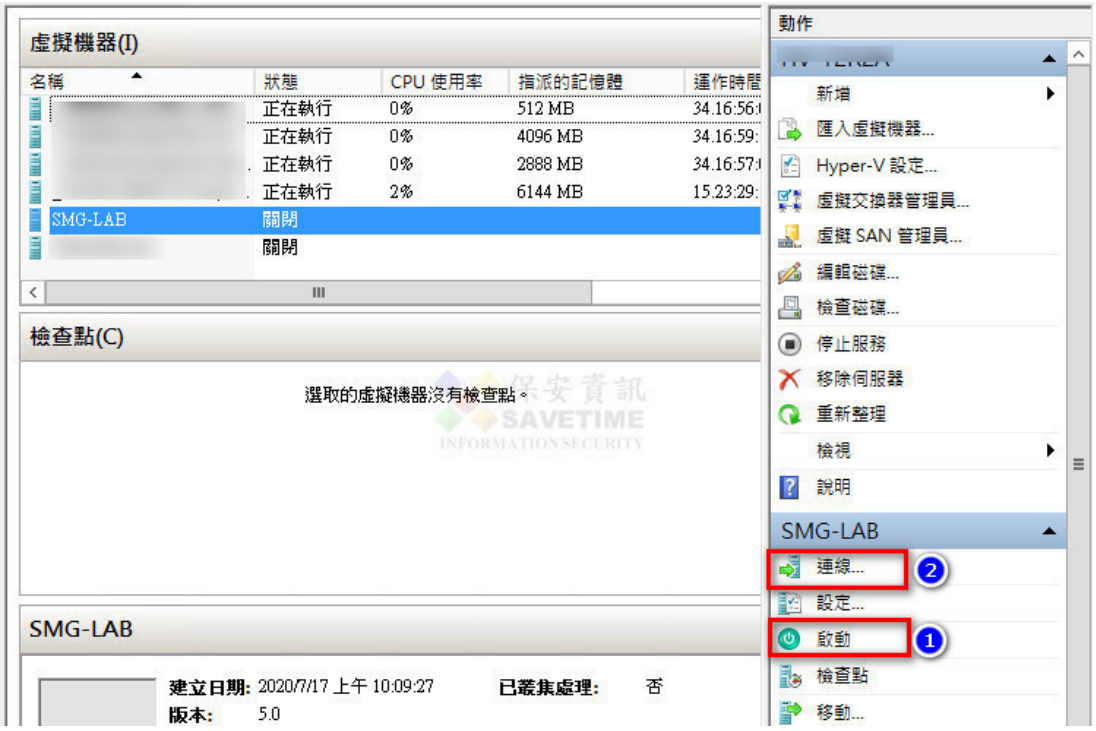
調為自動啟動，延遲時間請依實際狀況設定



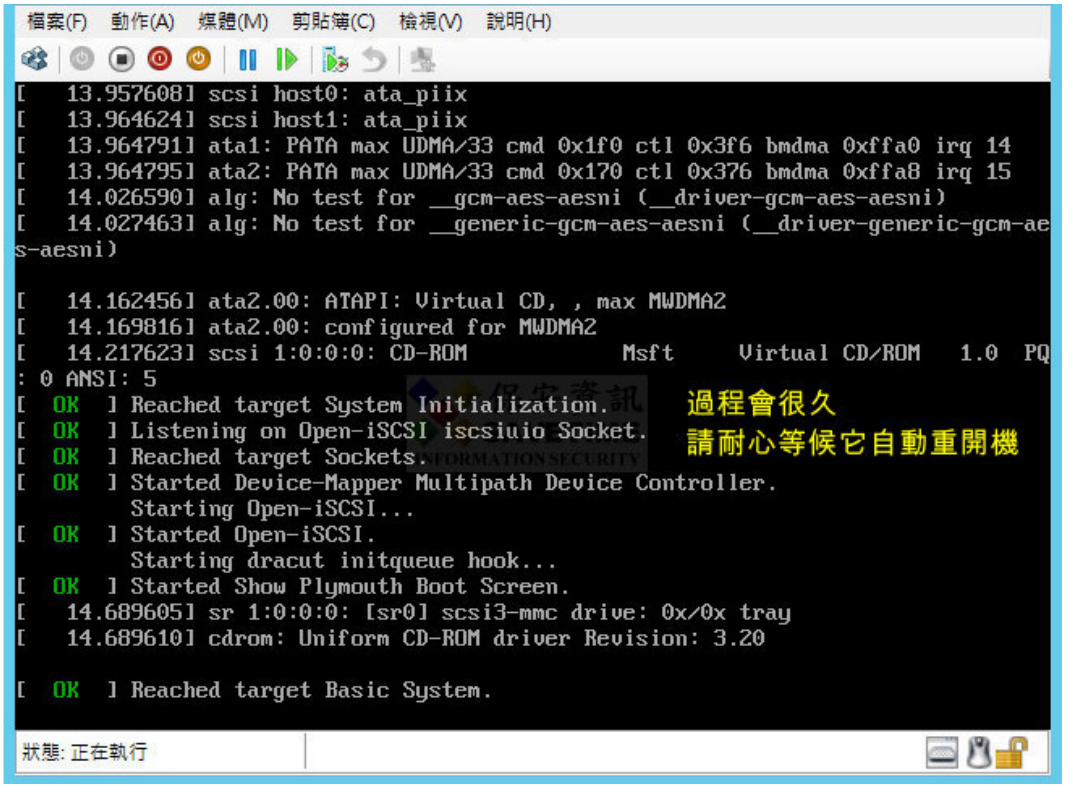




■啟動虛擬機器並開啟 console 介面



■自動安裝進行中，裝完會自動重開機到登入狀態頁



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

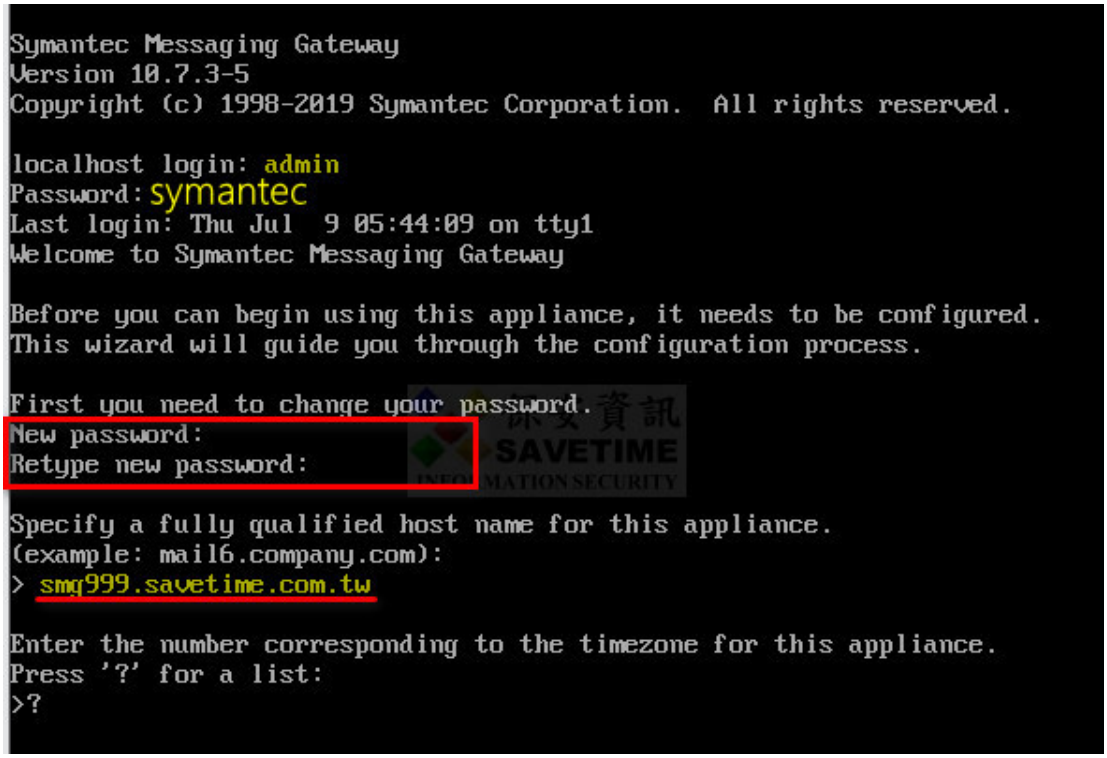
■開始初始設定

■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

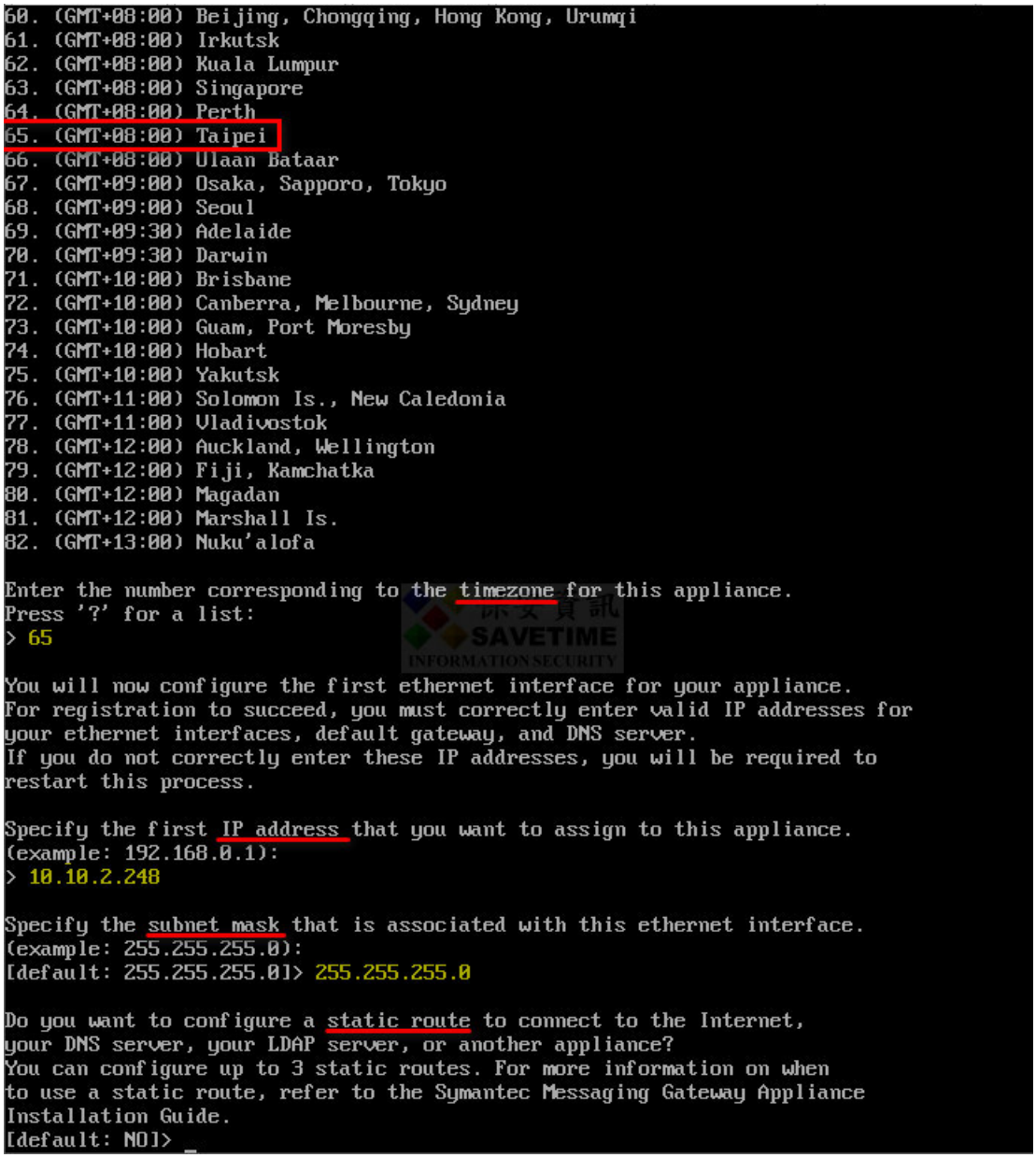
■時區的部份可先打？做查詢



■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



- 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

```
Specify the IP address of the default gateway
(also known as the default router) on your network.
(example: 192.168.0.20):
> 10.10.2.254

Specify the IP address of your first DNS server.
(example: 192.168.0.45):
> 10.10.2.254

Would you like to specify another DNS server?
[default: YES]> YES

Specify the IP address of your second DNS server.
(example: 192.168.0.45):
> 8.8.8.8

Would you like to specify another DNS server?
[default: YES]> NO

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: 255.255.255.0
        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

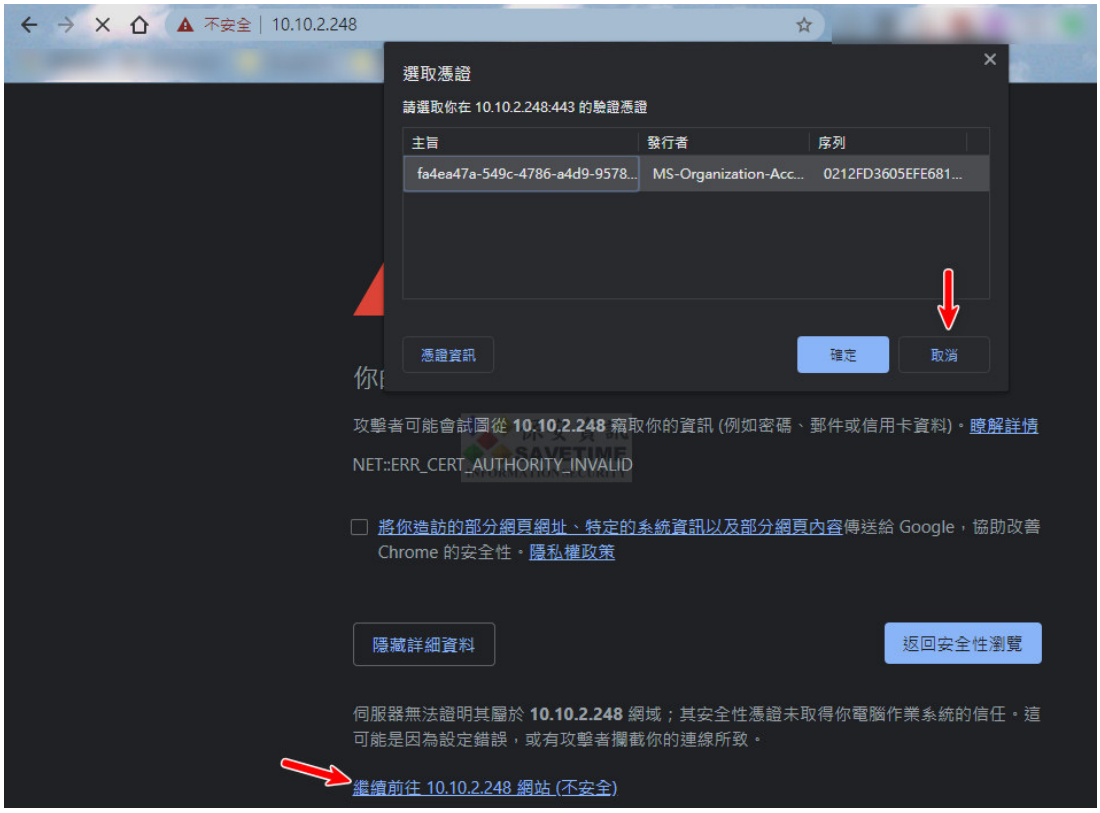
```
Symantec Messaging Gateway
Version 10.7.3-5
Copyright (c) 1998-2019 Symantec Corporation.  All rights reserved.

smg999 login:
```

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



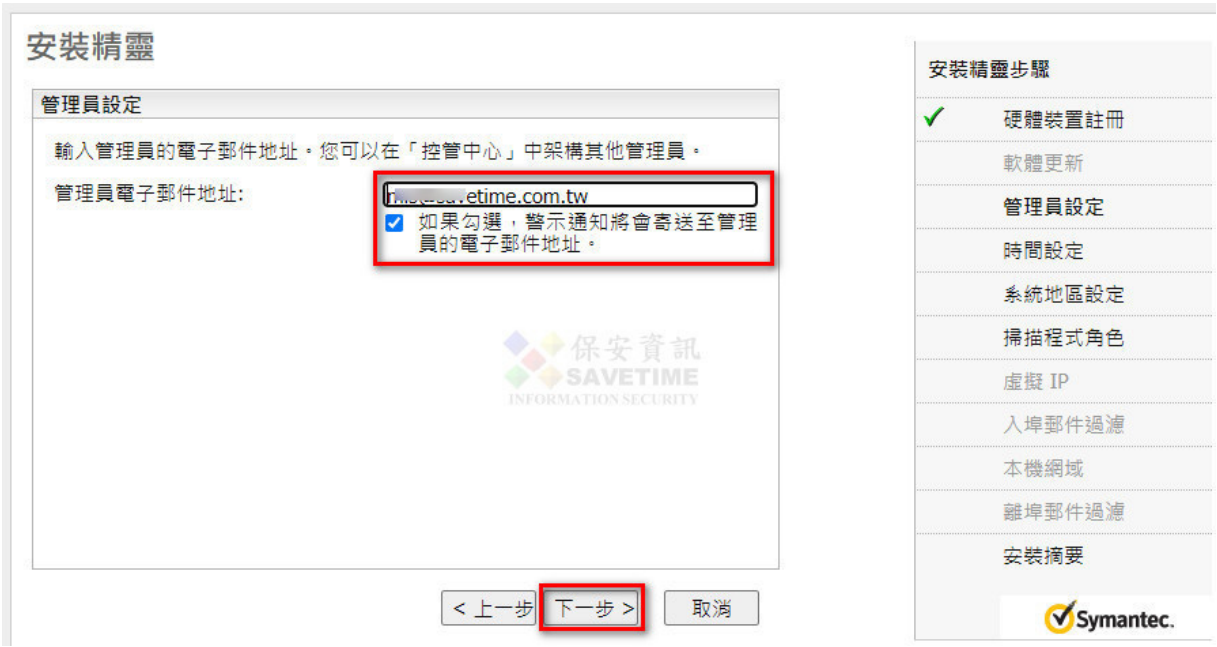
■ 輸入前步驟中的帳密

■ 勾選授權許可

■ 指定授權檔對按註冊授權

■ 授權滙入成功後請按下一步，否則請重頭來過

■ 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

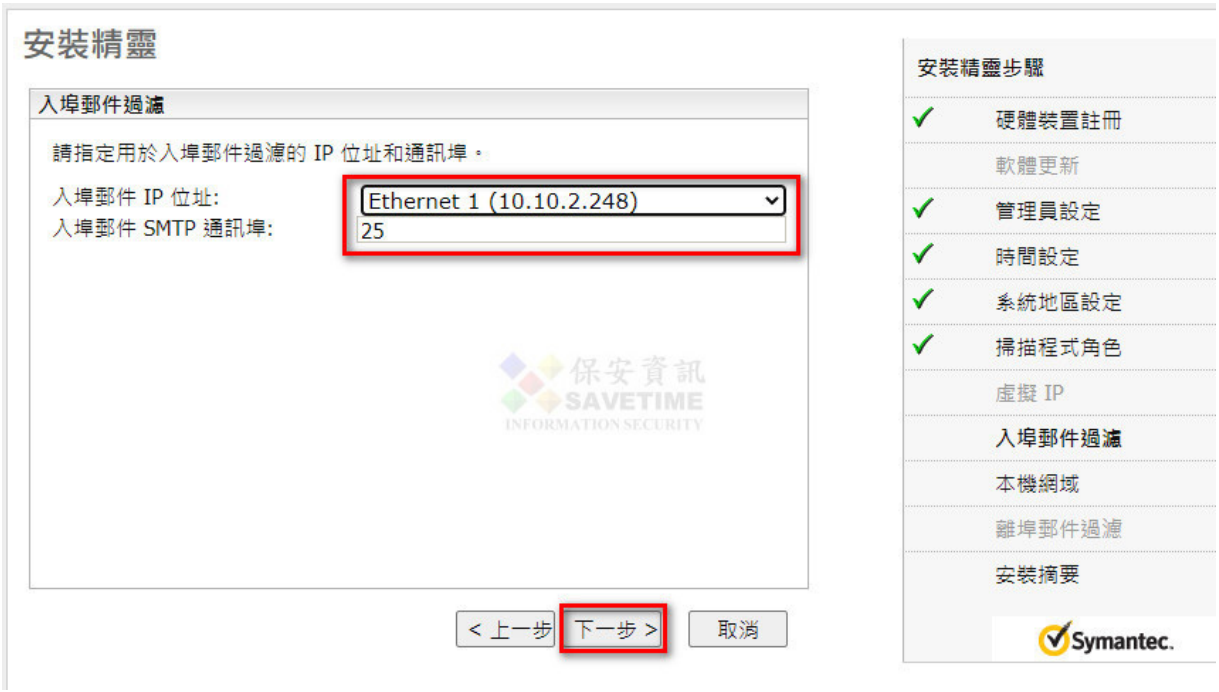


■ 指定 NTP 伺服器，在台灣，通常就直接用國內的，若　貴單位有特定使用方式則依　貴單位設定值設定

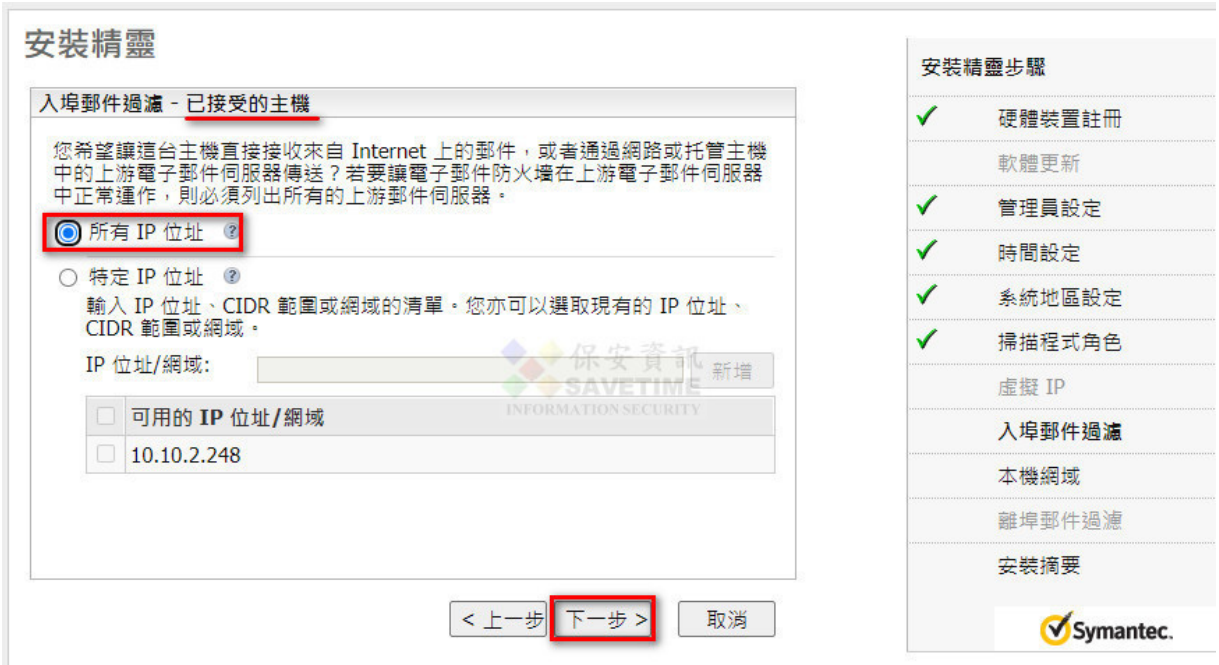
■ 指定地區及編碼

■ 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

■ 指定入埠過濾的IP位址，預設即為前述設定的 SMG ip

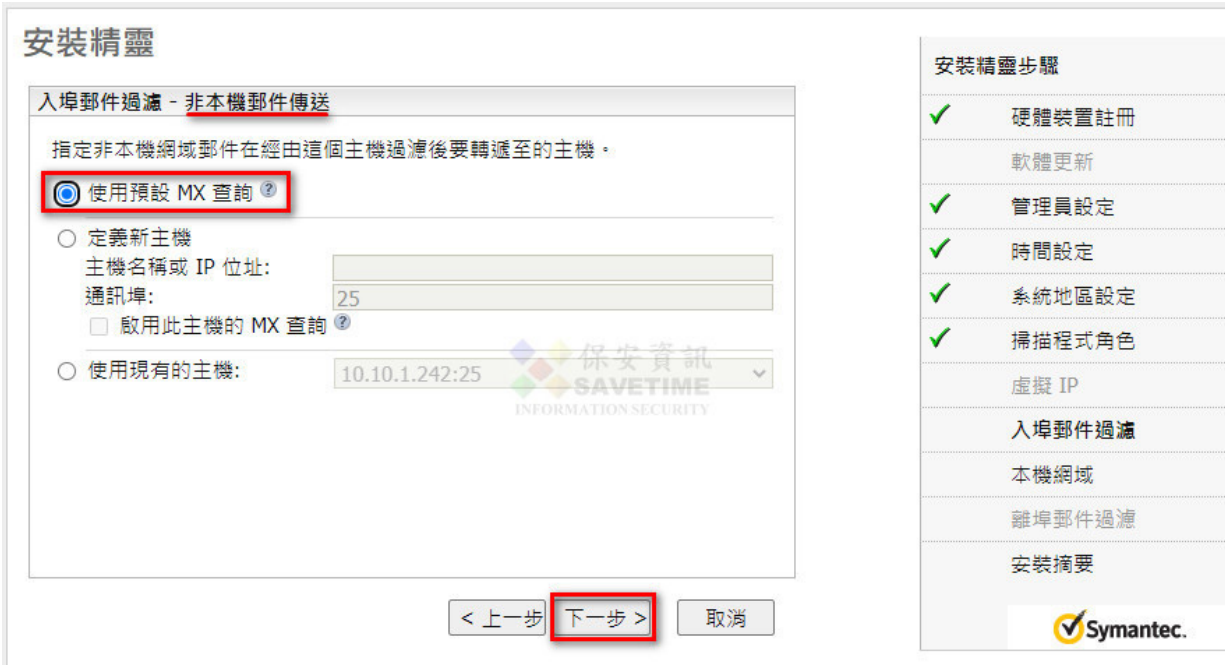


■ 接收所有寄過來的信件



■ 指定往後送往的 mail server ip

■ 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



■ 指定本機收件的網域及其往送送的郵件伺服器 ip

■ Review 上述的設定，若沒問題按完成即可

■ 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

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」。
SMTP 組態
MTA 主機名稱:
smg999.savetime.com.tw
入埠
離埠
傳送
驗證
SMTP 傳送組態
外部連線數上限:
單一 IP 位址的外部連線數上限:
所有內部郵件伺服器的連線數上限:
每個單一內部郵件伺服器的連線數上限:
傳送佇列中的郵件數目上限:
傳送佇列中每封郵件的收件者數上限:
連線的外寄郵件數上限:
傳送佇列被佔滿時延遲新連線
最小重試間隔:
最大重試間隔:
已傳送郵件的逾時時間:
退回郵件的逾時時間:
通知前佇列中的郵件延遲時間:
嘗試針對傳送的所有郵件進行 TLS 加密
提供 TLS 用戶端憑證
連線逾時:
EHLO/HELO 逾時:
MAIL FROM 逾時:
RCPT TO 逾時:
DATA 逾時:
RSET 逾時:
閒置逾時:
SMTP 傳送繫結
本機郵件:
非本機郵件:
動態繞送的郵件:
目標為控管中心的郵件:
每一網域的非本機 SMTP 傳送繫結
指定一或多個網域，然後選擇從這些網域所寄送郵件將使用的傳送繫結。
網域:
IP 位址:
savetime.com.tw
10.10.2.248
新增
每頁的項目數:
顯示:
刪除
全部刪除
寄件者網域
IP 位址
MTA 調度程式並行:
繼續
取消
新增
編輯
刪除
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
進階設定
儲存
取消
正在儲存主機設定
正在儲存主機設定
伺服器現在正在更新設定。這可能需要數分鐘。
請稍候...

◎ 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

遇到垃圾信處理規則，請改為隔離，不需要用到的取消掉

◎ 警示通知信的設定，請視 貴單位需求更改值

◎ 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

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

2-2 內容政策範例

設定內容過濾條件

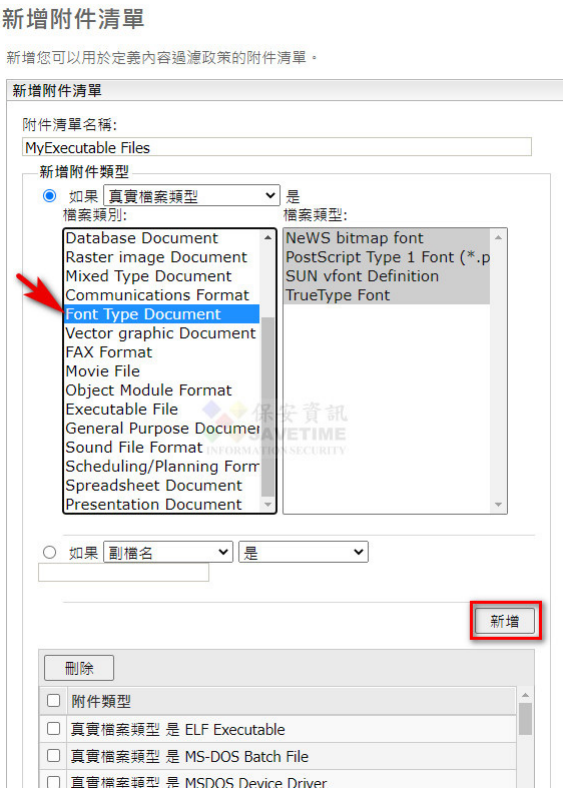
簡單解釋：註釋、附件清單、辭典、通知是設定內容可能會用到的資源條件，你可以先設定或者用預設的即可，也可以用預設的修改。

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

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



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）

新增內容政策

直接選用空白政策即可

給上可自行辨識的政策名稱，改為入埠郵件即，然後按新增

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

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

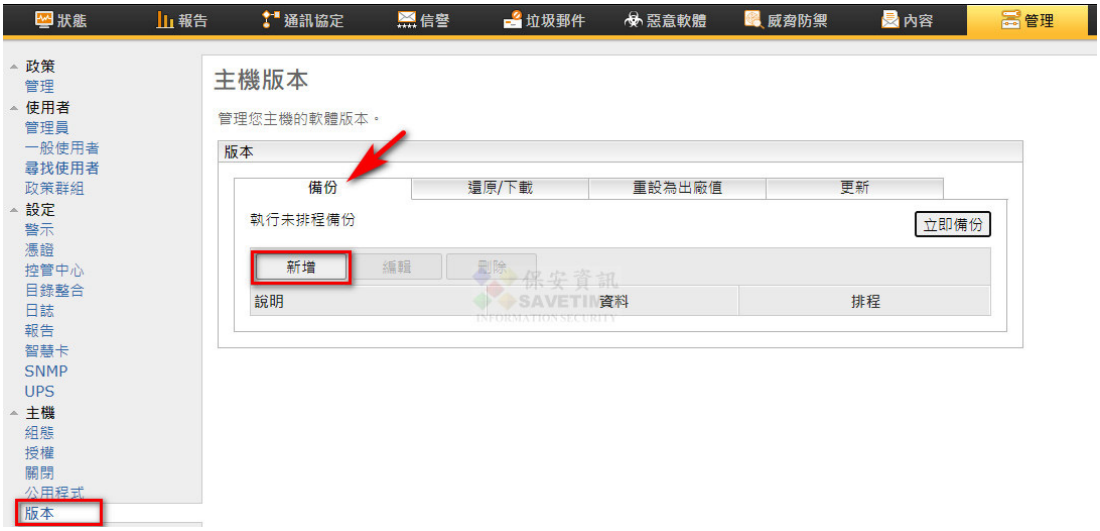
可到管理→群組→Default →內容過濾驗證我們設的內容條件有加進來囉！

2-3 其他的建議設定


狀態
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
信譽工具
尋找寄件者
IP 信譽查閱
攔截的寄件者
為不良信譽的寄件者架構群組。可建立和管理由管理員本機定義的攔截的寄件者群組、第三方清單以及賽門鐵克全域攔截
您可以選擇 Symantec Messaging Gateway 對每個群組的郵件採取的動作。您也可以架構電子郵件地址搜尋攻擊預防和電
預防。
編輯
啟用
停用
寄件者群組
已啟用
動作
本機攔截的寄件者網域
本機管理員新增的電子郵件地址或網域。
刪除郵件
本機攔截的寄件者 IP
本機管理員新增的 IP 位址。
拒絕 SMTP 連線
攔截的第三方寄件者
本機管理員訂購的第三方 IP 位址清單。
拒絕 SMTP 連線
賽門鐵克全域攔截的寄件者
由賽門鐵克基於全球信譽資料 (這些資料來自屬於 Symantec Global Intelligence Network 一部分的 Brightmail IQ 服務) 提供的 IP 位址。
拒絕 SMTP 連線
電子郵件地址搜尋攻擊
架構電子郵件地址搜尋攻擊識別，並指定發生電子郵件地址搜尋攻擊時要採取的動作。
—
延遲 SMTP 連線
電子郵件病毒攻擊
架構電子郵件病毒攻擊識別，並指定發生電子郵件病毒攻擊時要採取的動作。
—
延遲 SMTP 連線

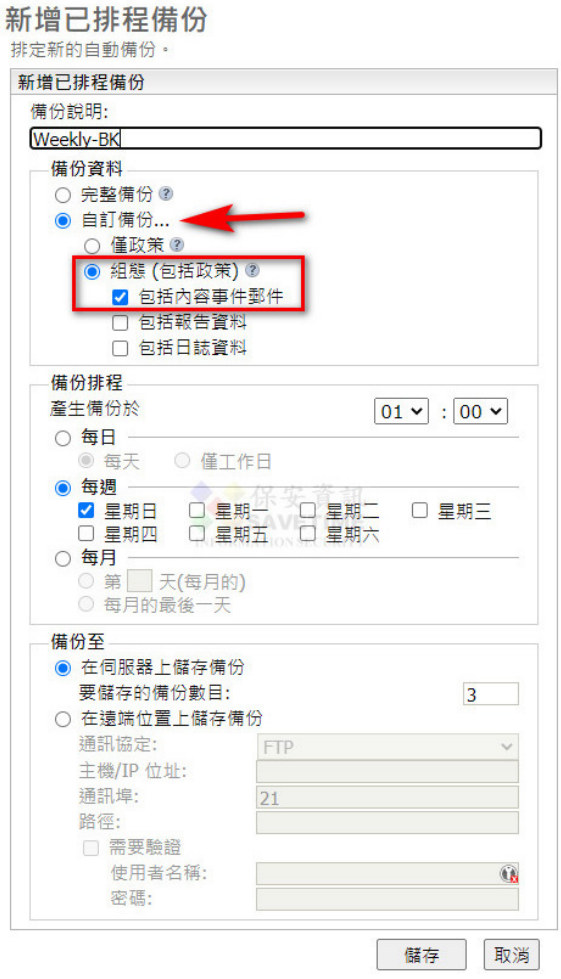

狀態
報告
通訊協定
信譽
垃圾郵件
惡意軟體
威脅防禦
政策
攔截的寄件者
連線類別
允許的寄件者
信譽工具
尋找寄件者
IP 信譽查閱
電子郵件病毒攻擊
架構電子郵件病毒攻擊識別，並指定發生電子郵件病毒攻擊時要採取的動作。
電子郵件病毒攻擊
啟用電子郵件病毒攻擊偵測
電子郵件病毒攻擊組態
病毒郵件百分比下限:
50
病毒郵件數目下限:
2
條件限定時間視窗:
10
分鐘
處罰席時間:
90
分鐘
動作
如果發生電子郵件病毒攻擊:
指定要對觸發此政策之郵件採取的動作。
新增
編輯
刪除
動作
延遲 SMTP 連線
儲存
取消

2-4 備份設定部份



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。



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—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—即從連到 SMG WEB console 的本機電腦處上傳備份檔還原

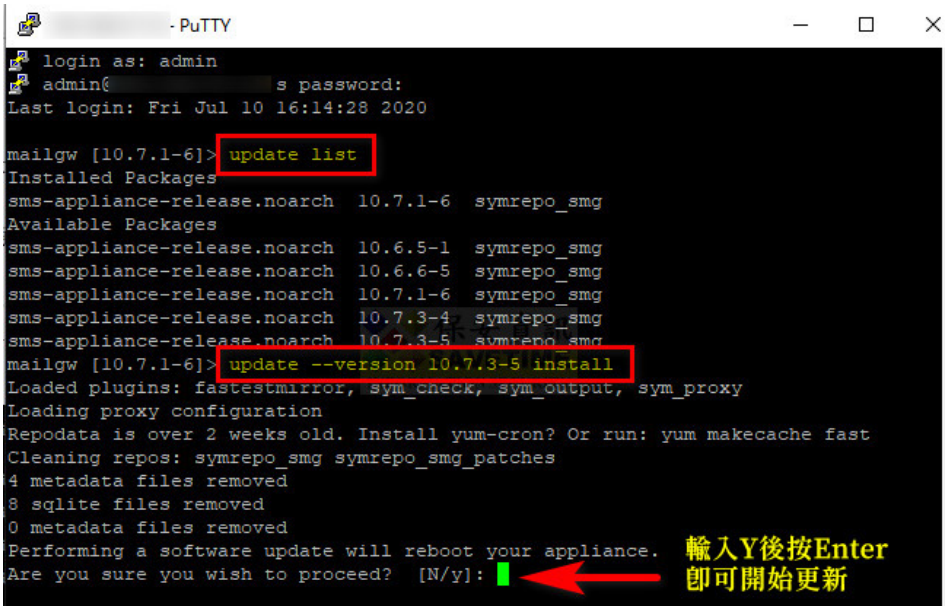
3 升級

3-1 從WEB介面更新

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）

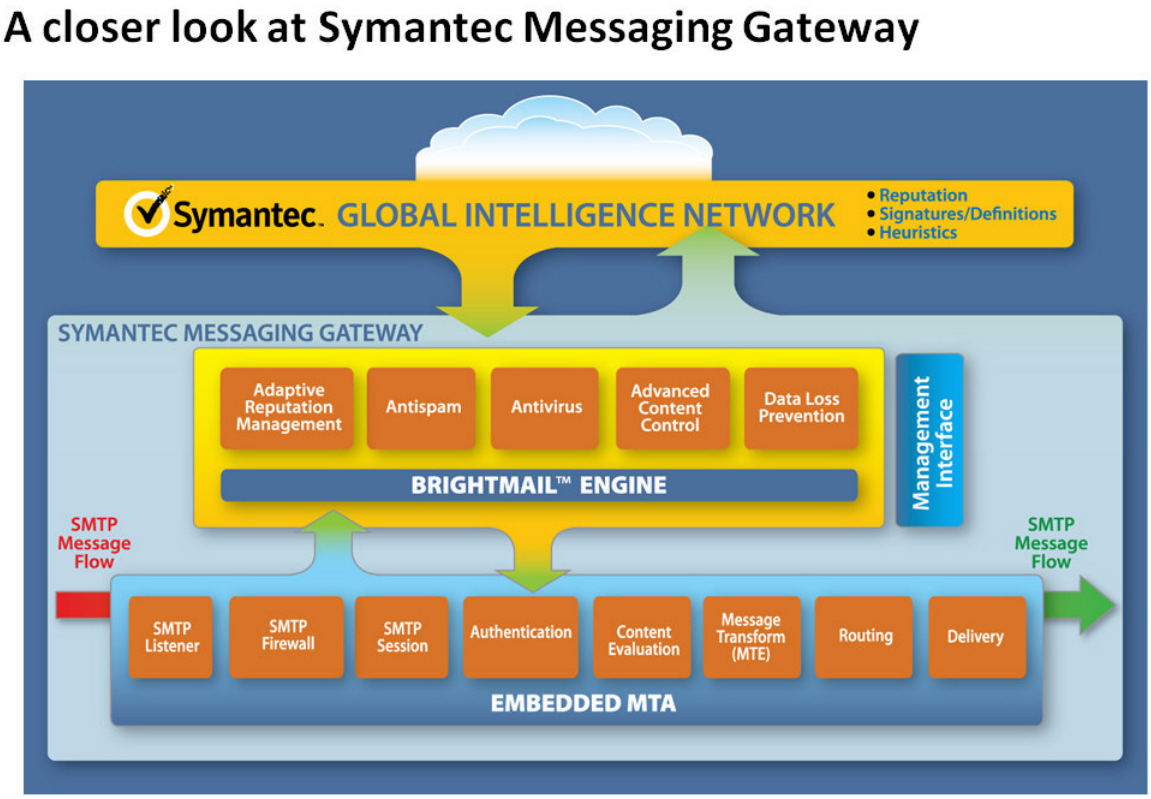
- 開啟 console 介面以admin登入
- 輸入 update list（列出可更新的版本）
- 選擇要更新的版本，如 10.7.3-5，命令如下：
- update --version 10.74.3-5 install



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



更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

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

  http://www.savetime.com.tw

  0800-381500、0936-285588