行政院及所屬委員會雲端資料中心 NDC 2.0

Symantec Endpoint Protection 用戶端安裝

標準作業程序書

一、 適用對象

行政院及所屬委員會及經經營管理小組同意使用本中心各項服務之機關(以下簡稱用戶)。

二、 使用時機

本中心於 113 年 1 月 2 日起使用新版防毒軟體(Symantec Endpoint Protection)，煩請配合安裝新版防毒軟體。

三、 安裝檔案下載

1. Windows 系統 64 bit
   https://s3.hicloud.net.tw/ndc/sep_download/windows/NDC2.0_WIN64BIT.zip
2. Linux 系統
   https://s3.hicloud.net.tw/ndc/sep_download/linux/NDC2.0_LINUXSTUB.zip
3. 解壓縮密碼 ndc

四、 安裝作業流程(Linux)

(一)安裝前要求與建議

1. 總作業時間約為半小時。
2. 建議使用本機 root 帳號登入並執行，避免安裝失敗或是安裝不完整的問題產生。

(二)安裝前檢查

1. 確認 Linux 主機與中控台網路狀況
   執行方式：開啟 terminal，執行 **telnet 223.200.155.30 443**、**telnet 223.200.155.30 8014**、**telnet 223.200.166.77 7070** 指令檢查網路連線，若無回應，請先檢查相關網路設定與防火牆設定，待排除問題後再進行安裝作業。Linux 的主機防火牆之設定方式可參考（三）安裝前置作業。

2. 確認 Linux 主機與 Symantec 儲存庫伺服器可連線
   因安裝程式會連線至 Symantec Linux 儲存庫下載相依套件。請申請防火牆允許連線該網址 **https://linux-repo.us.securitycloud.symantec.com/**
   若單位主機是屬於封閉環境無法申請對外連線，請來信告知客服人員。

3. 確認 Linux 主機的作業系統版本
   執行方式：執行 **cat /etc/redhat-release**(僅限 CentOS or RHEL 版本) 或 **lsb_release –a**(僅限 Ubuntu)，確認版本是否在支援清單內，若非在清單內請勿安裝，並請回報相關資訊(1.主機名稱，2. IP 位址與 3.作業系統版本等) 提供給客服人員。

   Symantec 線上清單如下
   目前 SEP 14.3 RU8 支援的 Redhat Linux (RHEL) Kernel 版本請參考官方說明：
   https://linux-repo.us.securitycloud.symantec.com/SAL/1.3/seplinux_supported_kernels.html

   其餘 Kernel 版本請參考官方說明(由 Broadcom 原廠更新)：
   https://techdocs.broadcom.com/tw/zh-tw/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Release-Notes/supported-kernels-of-symantec-linux-agent-v133465487-d4155e7808.html

(三)安裝前置作業(Linux)

依照不同作業系統 CentOS 7 執行 **service firewalld status** 或者 Centos 6 執行 **service iptables status**，檢查該主機之防火牆之狀態，並依貴單位之需求將防火牆重新『開啟』或維持『關閉』狀態。

以下為 Centos 7 系統 firewalld 指令的結果

```
[root@chttl-814606bdc73f93ec ~]# service firewalld status
Redirecting to /bin/systemctl status  firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
   Active: active (running) since Thu 2018-02-08 14:25:03 CST; 3s ago
 Main PID: 23103 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─23103 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
```

Linux 伺服器上若有開啟本機 iptables 防火牆或 firewalld 防火牆時，可能會需要開通 SEP 所需防火牆規則，否則 SEP 將無法正常運作。請 Linux 伺服器管理者先確認以下的連線是否有被伺服器上的本機防火牆所限制住。若有限制，則請開通本機防火牆，開啟方式可依管理者實際部署狀況來調整語法。

SEP 所需開啟防火牆規則如下:

- Linux 用戶端與防毒管理伺服器（223.200.155.30）TCP Port 8014 連線
- Linux 用戶端與防毒管理伺服器（223.200.155.30）TCP Port 443 連線
- Linux 用戶端與防毒管理伺服器（223.200.166.77）TCP Port 7070 連線

＊請管理者依據主機防火牆現有設定，斟酌設定方式＊

以下為 iptables 參考範例 (CentOS 6.x)

1. 輸入 **iptables –L** 確認目前設定狀態後，接著輸入以下指令來設定 SEP 所需防火牆規則

/sbin/iptables -I INPUT -p tcp -s 223.200.155.30 --sport 443 -j ACCEPT
/sbin/iptables -I INPUT -p tcp -s 223.200.155.30 --sport 8014 -j ACCEPT
/sbin/iptables -I OUTPUT -p tcp -d 223.200.155.30 --dport 443 -j ACCEPT
/sbin/iptables -I OUTPUT -p tcp -d 223.200.155.30 --dport 8014 -j ACCEPT
/sbin/iptables -I OUTPUT -p tcp -d 223.200.166.77 --dport 7070 -j ACCEPT
/etc/init.d/iptables save

以下為示意圖

```
root@sep6:~
[root@sep6 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@sep6 ~]#
root@sep6 ~]# /sbin/iptables -I INPUT -p tcp -s 192.168.0.11 --sport 443 -j ACCEPT
root@sep6 ~]# /sbin/iptables -I INPUT -p tcp -s 192.168.0.11 --sport 8014 -j ACCEPT
root@sep6 ~]# /sbin/iptables -I INPUT -p tcp -s 192.168.0.13 --sport 7070 -j ACCEPT
root@sep6 ~]# /sbin/iptables -I OUTPUT -p tcp -d 192.168.0.11 --dport 443 -j ACCEPT
root@sep6 ~]# /sbin/iptables -I OUTPUT -p tcp -d 192.168.0.11 --dport 8014 -j ACCEPT
root@sep6 ~]# /sbin/iptables -I OUTPUT -p tcp -d 192.168.0.13 --dport 7070 -j ACCEPT
root@sep6 ~]# /etc/init.d/iptables save
ptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
[root@sep6 ~]#
```

2. 設定完成 SEP 規則後，再次輸入 **iptables –L** 確認目前設定狀態 (示意圖)

```
[root@sep6 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.0.13         anywhere            tcp spt:arcp
ACCEPT     tcp  --  192.168.0.11         anywhere            tcp spt:8014
ACCEPT     tcp  --  192.168.0.11         anywhere            tcp spt:https
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.0.13        tcp dpt:arcp
ACCEPT     tcp  --  anywhere             192.168.0.11        tcp dpt:8014
ACCEPT     tcp  --  anywhere             192.168.0.11        tcp dpt:https
[root@sep6 ~]#
```

<u>以下為 firewalld 參考範例（CentOS 7.x）</u>

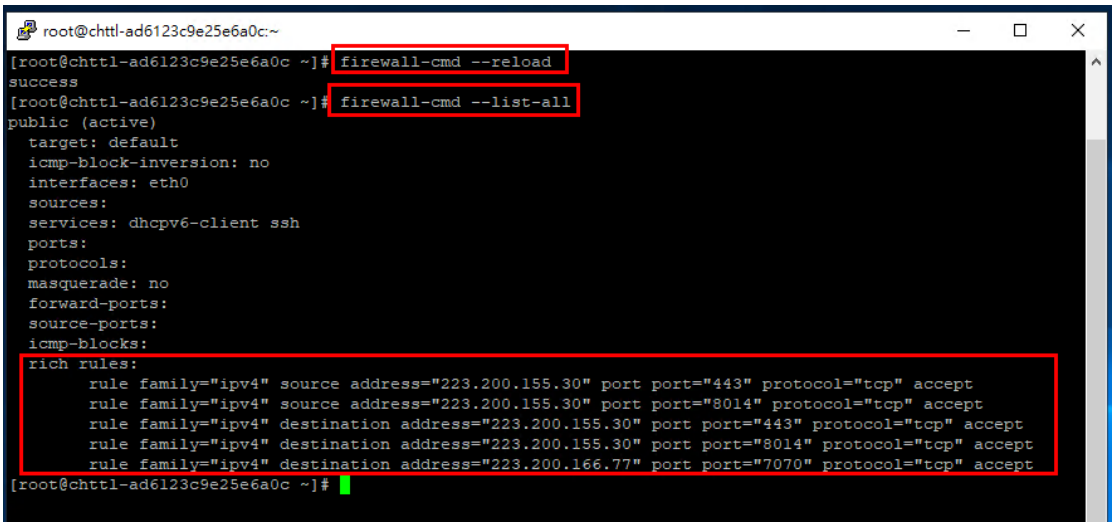
1. 輸入 **firewall-cmd --list-all** 確認目前設定狀態後，接著輸入以下指令來設定 SEP 所需防火牆規則

```
sudo firewall-cmd --add-rich-rule 'rule \family="ipv4" source
address="223.200.155.30" port port="443" protocol="tcp" accept'
\--permanent
sudo firewall-cmd --add-rich-rule 'rule \family="ipv4" source
address="223.200.155.30" port port="8014" protocol="tcp" accept'
\--permanent
sudo firewall-cmd --add-rich-rule 'rule \family="ipv4" destination
address="223.200.155.30" port port="443" protocol="tcp" accept'
\--permanent
sudo firewall-cmd --add-rich-rule 'rule \family="ipv4" destination
```

address="223.200.155.30" port port="8014" protocol="tcp" accept' \--permanent

sudo firewall-cmd --add-rich-rule 'rule \family="ipv4" destination address="223.200.166.77" port port="7070" protocol="tcp" accept' \--permanent

2. 設定完成 SEP 規則後，輸入 **firewall-cmd --reload** 載入新設定，輸入 **firewall-cmd --list-all** 讀取防火牆確認目前設定狀態。



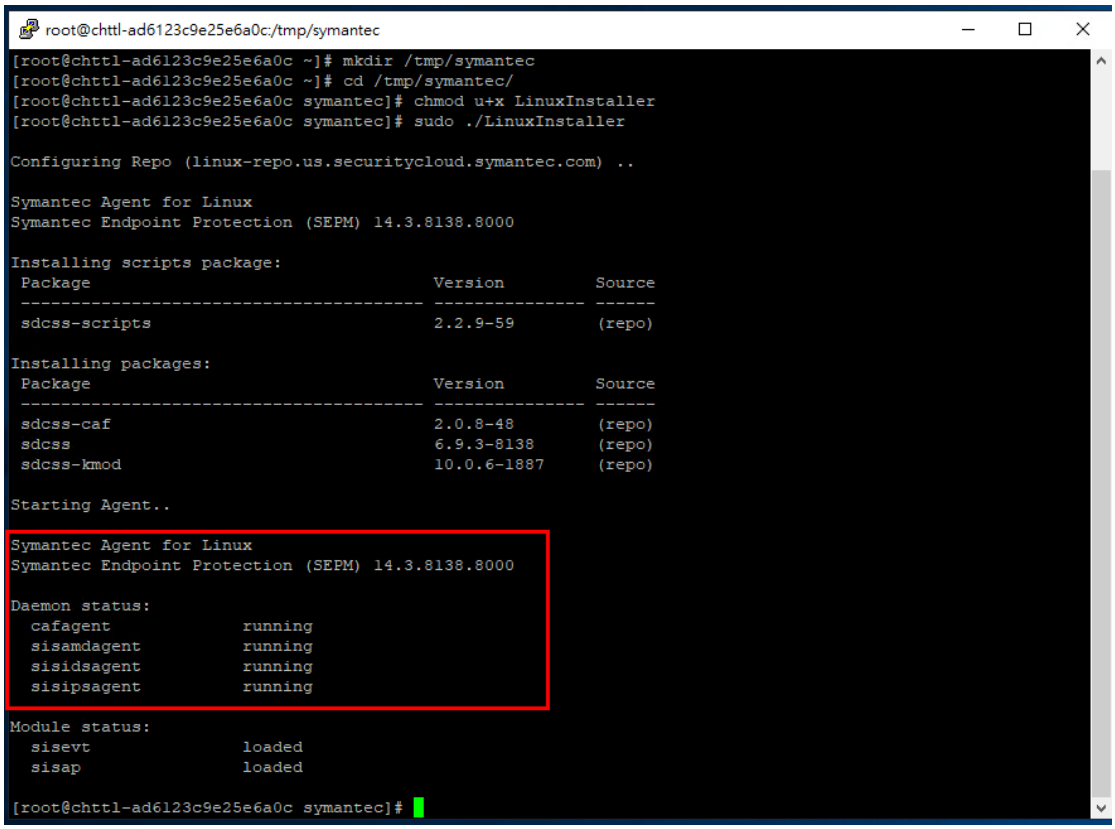
(四)安裝作業流程(Linux)

1. 上傳 SEP 安裝檔案 LinuxInstaller
   (1) 執行指令建立目錄 **mkdir /tmp/symantec**
   (2) 將安裝檔上傳至/tmp/symantec 目錄下

2. 將 LinuxInstaller 檔案設為可執行檔：
   (1) 執行 cd /tmp/symantec 指令切換至安裝檔上傳的目錄
   (2) 執行 **chmod u+x LinuxInstaller**

3. 執行安裝作業：
   (1) 必須以 root 身分執行指令，或是使用 sudo 方式
   (2) 執行 **sudo ./LinuxInstaller** 等待幾分鐘，看到跑出 4 支 daemon 的狀態應是 running，兩個 Module 狀態應是 loaded。後續驗證安裝時確認 Definition 與 AP 是否有正常更新與運作。

4. 以上安裝完畢後，請先**重新開機**才能確保服務正常啟用



5. 驗證安裝
   (1) 確認已載入的模組而且精靈正在執行(running 與 loaded)
   (2) 執行 **cd /usr/lib/Symantec** 指令切換至目錄
   (3) 執行**./status.sh** 指令

```
[root@chttl-ad6123c9e25e6a0c symantec]# cd /usr/lib/symantec/
[root@chttl-ad6123c9e25e6a0c symantec]# ./status.sh

Symantec Agent for Linux
Symantec Endpoint Protection (SEPM) 14.3.8138.8000

Daemon status:
  cafagent              running
  sisamdagent           running
  sisidsagent           running
  sisipsagent           running

Module status:
  sisevt                loaded
  sisap                 loaded
```

(4) 檢查自動防護狀態，指令 **cat /proc/sisap/status**

6. 執行病毒碼更新作業：
   (1) 執行 **cd /opt/Symantec/sdcssagent/AMD/tools** 指令切換至目錄，
   (2) 執行**./sav liveupdate –u** 進行更新作業。若看到 update was successful 就表示更新成功，若是 update is triggered 代表已觸發更新，需等待一些時間等病毒碼下載更新完成。

```
[root@chttl-ad6123c9e25e6a0c symantec]# cd /opt/Symantec/sdcssagent/AMD/tools
[root@chttl-ad6123c9e25e6a0c tools]# ./sav liveupdate -u
Live update is triggered
```

7. 執行**./sav info -d** 確認目前防護定義檔資訊 (最新病毒碼的日期為前天或昨天的日期，例如：今天日期為 12/2，則病毒碼日期應該是 12/1 或 11/30)。

```
[root@chttl-ad6123c9e25e6a0c tools]# ./sav info -d
12/18/2023 rev. 116
```

8. 若遇到安裝問題，請參考以下異常狀況之處理或聯絡客服人員。

(五)異常狀況之處理(Linux)

1. 用戶端異常，執行移除作業
   (建議使用 root 身分執行指令，或是使用 sudo 方式)
   (1) 執行 **cd /usr/lib/symantec/**，切換至目錄
   (2) 執行**./uninstall.sh -u** 移除 Linux 用戶端。
   或**./uninstall.sh -u SEPL**
   (3) 若 LinuxInstaller 檔案還存在，也可透過他進行移除
   切換到該檔案目錄 **cd /tmp/Symantec**
   執行 **sudo ./LinuxInstaller -u**

```
[root@RHEL86 tmp]# ./LinuxInstaller -u
Stopping Agent..
Uninstalling Symantec Agent for Linux
Symantec Endpoint Protection (SEPM) ...
Removing packages sdcss-caf sdcss sdcss-kmod sdcss-scripts
[root@RHEL86 tmp]#
```

(4) 解除安裝完成後，請重新啟動電腦。

2. 協助收集相關日誌送交分析

(1) 使用 GetAgentInfo 程序檔將所有日誌檔都收集到一個 ZIP 檔案。

(2) 切換至 **cd /opt/Symantec/sdcssagent/IPS/tools/**

(3) 以 **root** 身分執行 **./getagentinfo.sh**

(4) 將會在 **/tmp/** 目錄中產生 ZIP 檔案

檔案名稱將會類似 20201208_184935_0001_CU_mihsan-rhel8.zip

```
*** Please send the Info File:
***   /tmp/20231219_091535_0001_CU_localhost.localdomain.zip
*** to Broadcom
```

(5) 再透過 sftp 的方式將檔案匯出，交予客服人員。

客服電話：(02) 2344-2836#1105、客服信箱：ndcdc@ndc.gov.tw。

五、 安裝作業流程(Windows)

(一)安裝前要求與建議

1. 安裝期間會需要重新開機，總作業時間約為半小時。
2. 用本機 administrator 或是具備 administrators 權限的帳號登入，避免安裝失敗或是安裝不完整的問題產生。
3. 安裝過程中，若有失敗的狀況發生，請提供 c:\temp 或是 c:\windows\temp 下的 SEP_INST.LOG 或是 SYMEVENT.LOG 提供給客服人員確認。
   客服電話：(02) 2344-2836#1105、客服信箱：ndcdc@ndc.gov.tw。

(二)安裝前檢查

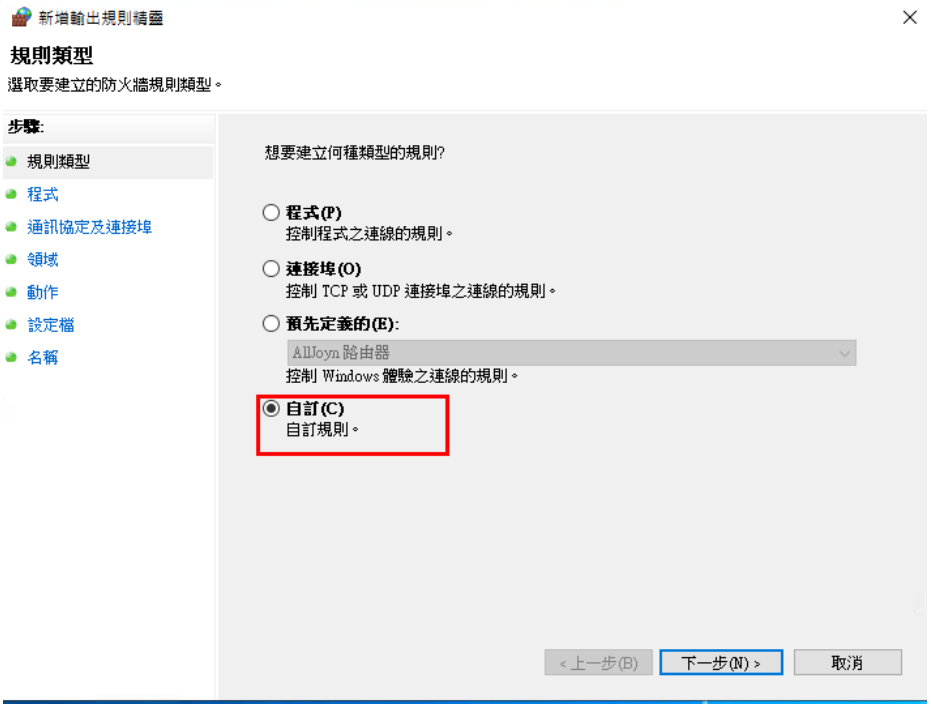
確認 Windows 主機與中控台網路狀況。
執行方式：開啟命令提示字元，執行 telnet 223.200.155.30 443 與 telnet 223.200.155.30 8014 確認網路連線，若無法連線，請先檢查相關網路設定與防火牆設定，待排除問題後再進行安裝作業。

(三)安裝前置作業(Windows)

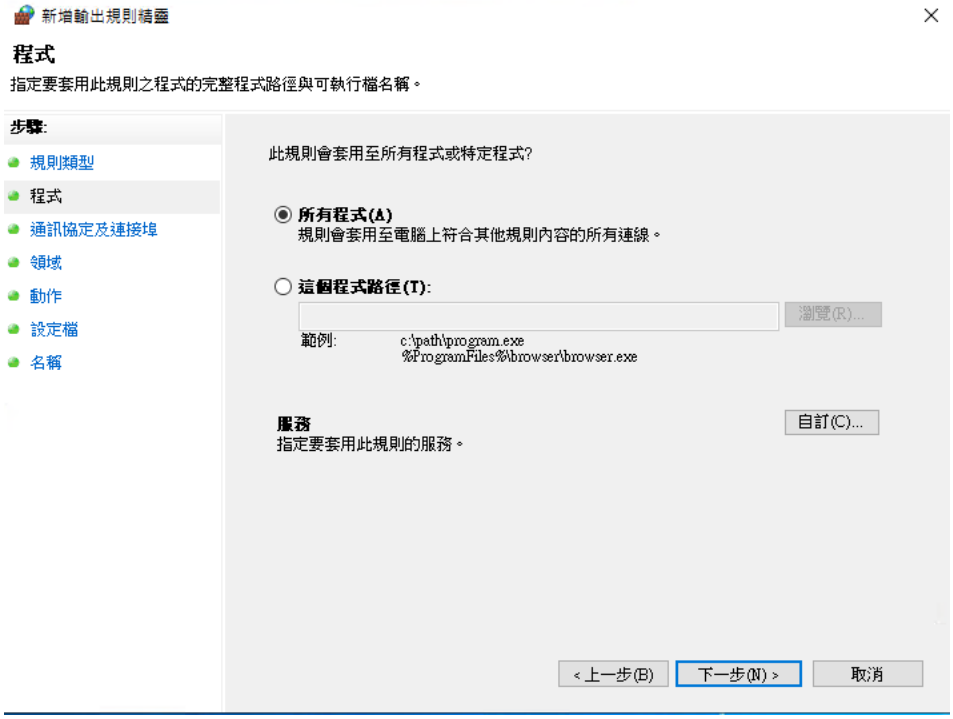
SEP 需開通 Windows 防火牆規則，SEPM 使用的 IP 為 223.200.155.30，使用的 TCP Port 為 443 與 8014，用戶可依照本身習慣來調整防火牆規則。以下為簡單範例

1. 進入控制台，Windows 防火牆，點選 進階設定
2. 點選輸出規則後，點選 新增規則

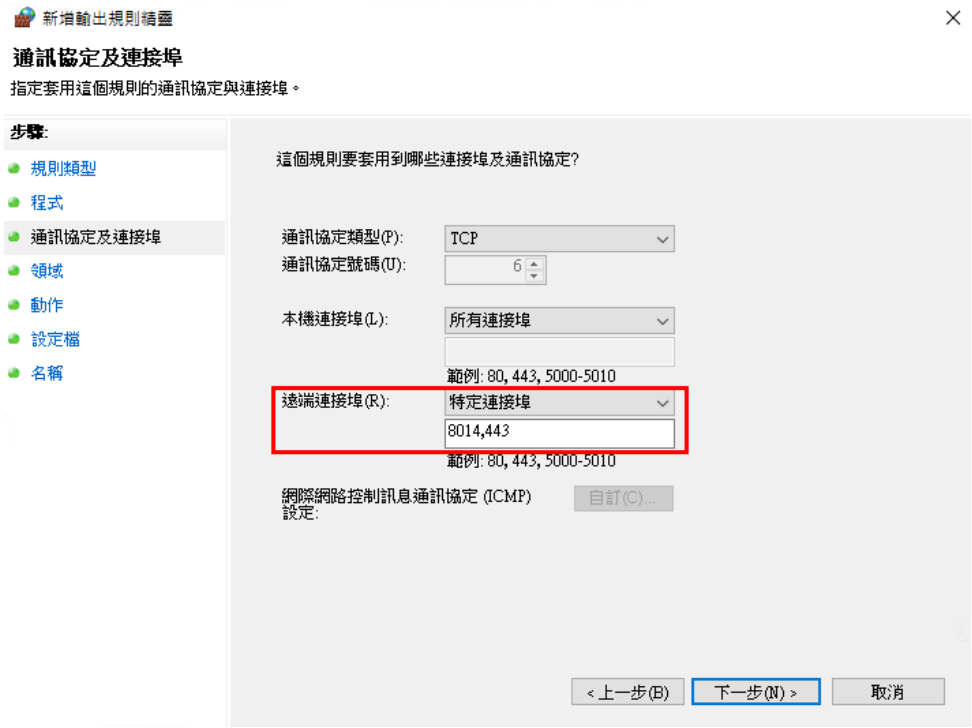
3. 選擇自訂規則



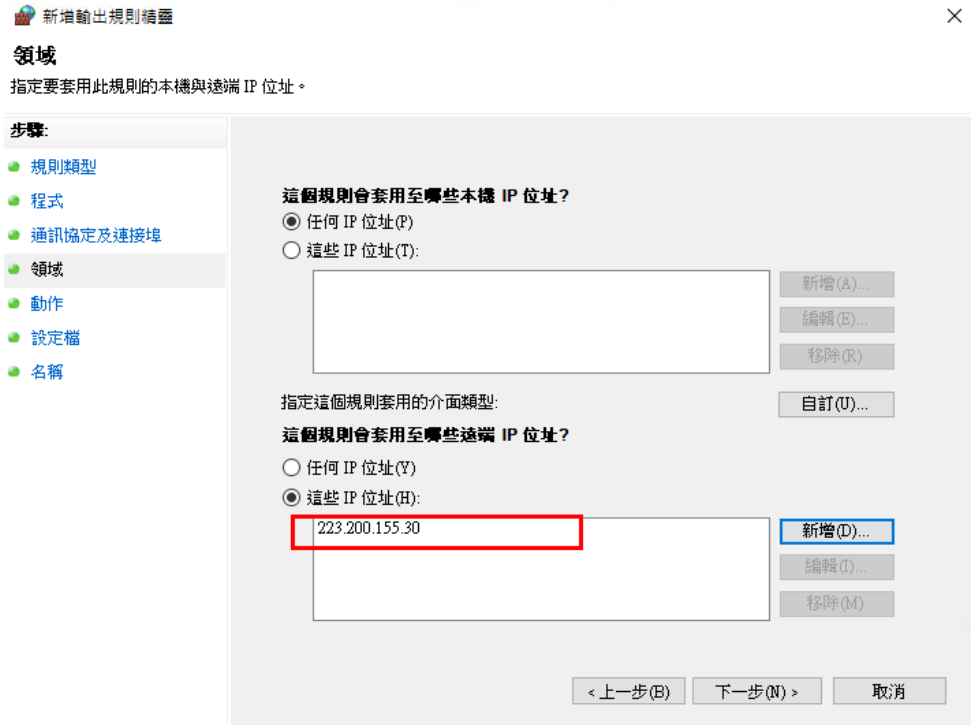
4. 選擇所有程式



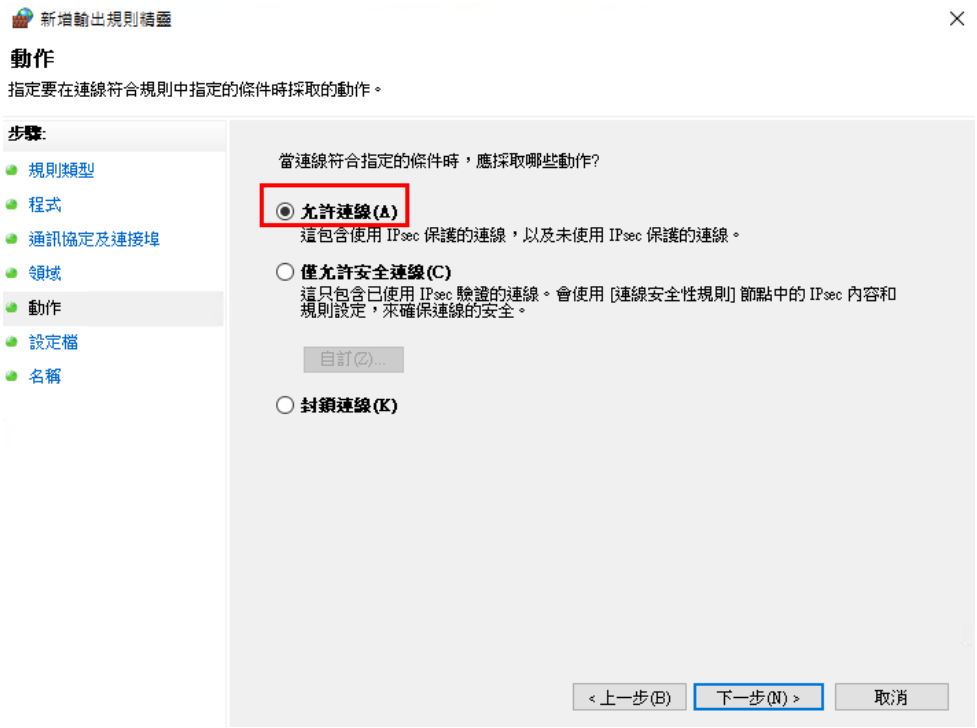
5. 填寫遠端連接埠為 8014,443



6. 填寫遠端 IP 位址為 223.200.155.30

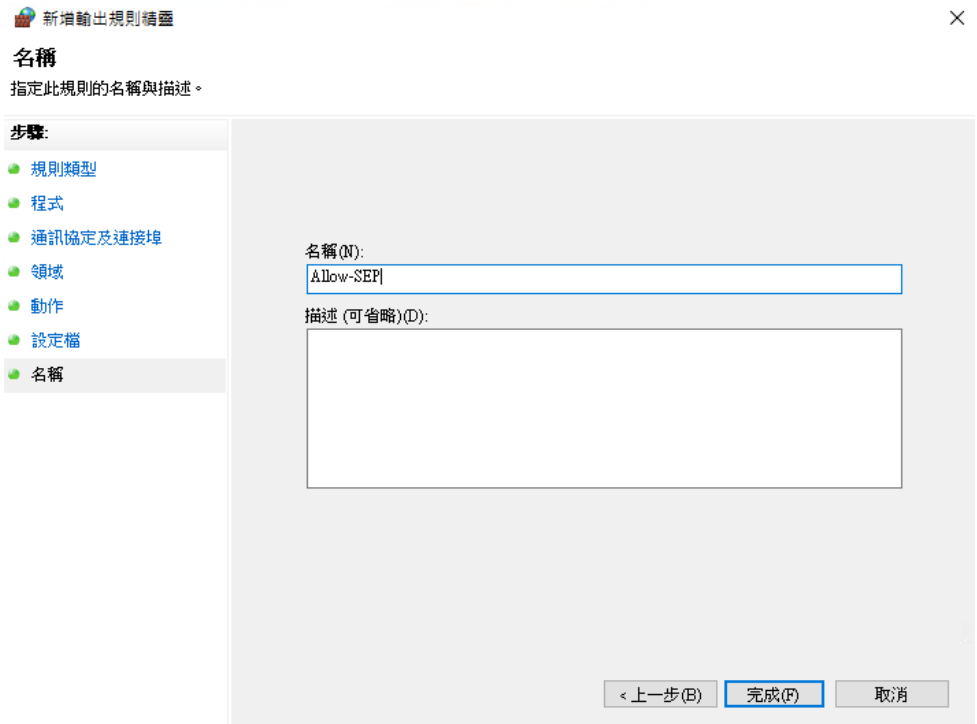


7. 選擇 允許連線



8. 勾選全部 設定檔

9. 名稱填名稱輸入『Allow-SEP』後點選完成。

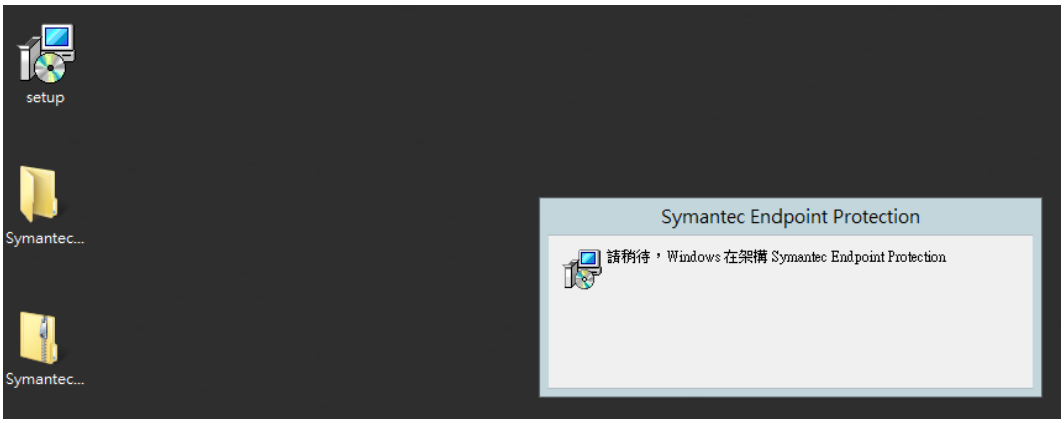


(四)安裝作業流程(Windows)

安裝用戶端程式(約 15 分鐘)

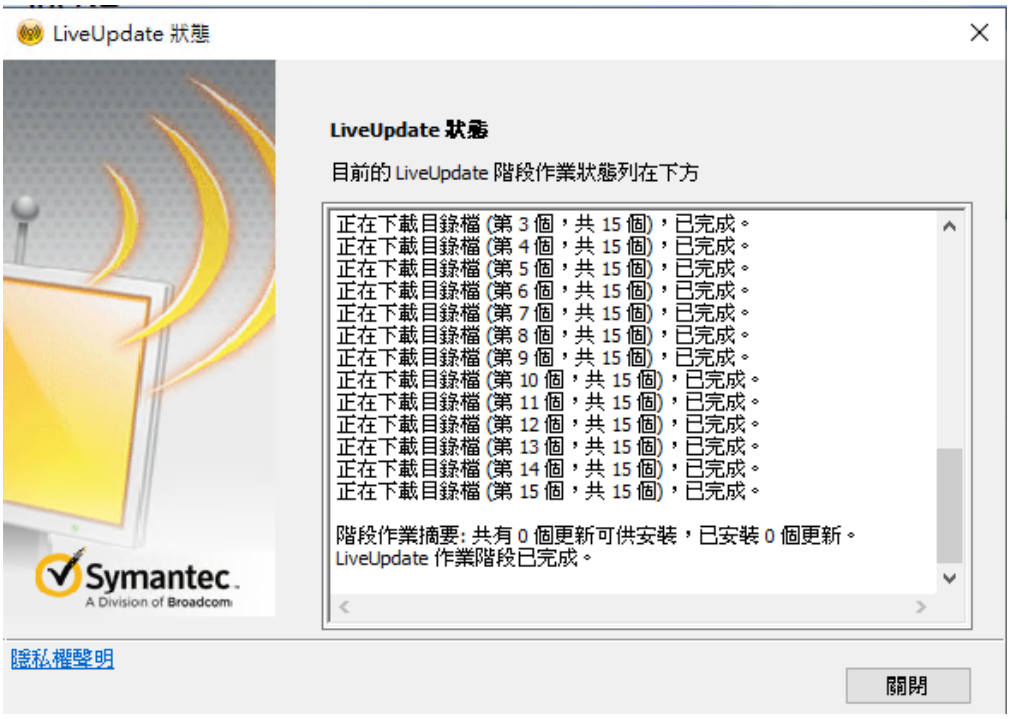
執行方式：

1. 點選 SEP 用戶端安裝程式。
2. 觀察安裝的過程是否正常並且無錯誤訊息發生，完成後，點選關閉。



3. 確認安裝後狀態，是否防護定義檔最新，需待 15 分鐘。
   (最新病毒碼的日期為昨天或前天的日期，例如：今天日期為 11/14，則病毒碼日期應該是 11/12 或是 11/13)

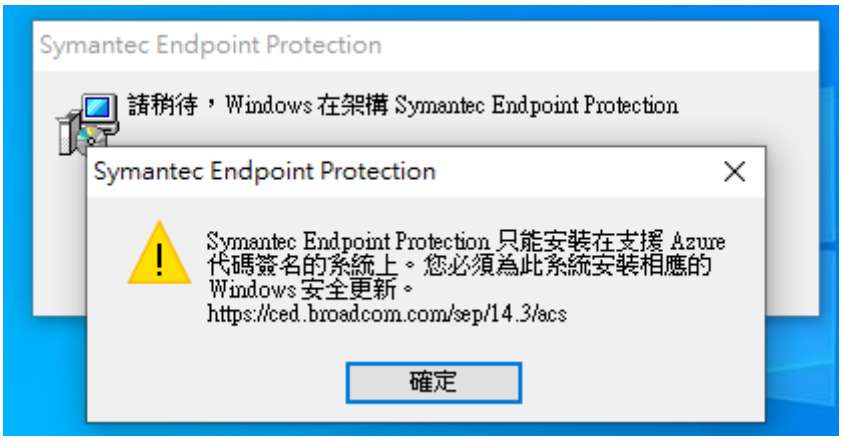
4. 左下角 LiveUpdate 按鈕可觸發透過中控台更新或是連線至 Symantec 原廠執行更新動作，但部分用戶端政策已將此功能鎖定反灰，故用戶無需執行。



(五)異常狀況之處理(Windows)

1. 用戶端異常，執行移除作業。
   執行方式：點選控制台→程式集→程式與功能→選取 Symantec Endpoint Protection，並點選解除安裝，完成後點選"是"，重新開機。

2. 升級或安裝 Symantec Endpoint Protection 14.3 RU8 時，用戶端使用者可能會看到以下錯誤訊息：【Symantec Endpoint Protection 只能安裝於具 Azure Code Signing 支援的系統。您必須為此系統安裝適當的 Windows 安全性更新。】



出現原因為 SEP 安裝程式偵測到電腦未執行支援 Microsoft Azure Code Signing 的 Microsoft Windows 版本，如 Windows 10 21H1 或更早版本。

請依下表所列作業系統版本，比對提供對 Azure Code Signing 的支援。選

擇相對應的 KB 安全更新下載及安裝，以便符合 SEP 安裝需求。

作業系統與版本	微軟 KB 編號	最初發布日期
Windows 11 Windows 10 22H2	出廠預設即支援 ACS – 無需安裝任何更新	
Windows 10 21H2	5011487 (適用於早於 19044.1586 21H2 版本)	2022 年 3 月 8 日
Windows Server 2022	5005619 (先決條件：無)	2021 年 9 月 27 日
Windows 10 2004 Windows 10 20H2 Windows 10 21H1	5005611 (先決條件：需要安裝累積更新 (LCU) 5003173 或更新版本，否則，需要先安裝維護堆疊更新 (SSU) 5005260)	2021 年 9 月 30 日
Windows 10 1909	5005624 (先決條件：需要先安裝累積更新 (LCU) 5004748)	2021 年 9 月 21 日
Windows 10 1809 Windows Server 2019	5005625 (先決條件：需要先安裝累積更新 (LCU) 5005112)	2021 年 9 月 21 日
Windows 10 1607 Windows Server 2016	Microsoft 於 2023 年 9 月 12 日起，不再提供 5006669 此更新 。建議升級到 Windows 10 21H2 或是更新版本。	
Windows 10 1507	Microsoft 於 2023 年 9 月 12 日起，不再提供此更新 。建議升級到 Windows 10 21H2 或是更新版本。	
Windows 8.1 Windows Server 2012 R2	5006714 (每月彙總更新，先決條件：無) 5006729 (僅限安全性更新，先決條件：無)	2021 年 10 月 12 日
Windows Server 2012	5006739 (每月彙總更新，先決條件：需要先安裝維護堆疊更新 (SSU) 5001401) 5006732 (僅限安全性更新，先決條件：需要先安裝維護堆疊更新 (SSU) 5001401)	2021 年 10 月 12 日
Windows Server 2008 SP2	5006736 (每月彙總更新，請自行參閱前述連結的先決條件) 5006715 (僅限安全性更新，請自行參閱前述連結的先決條件)	2021 年 10 月 12 日
Windows 7.0 SP1 Windows Server	5006743 (每月彙總更新，請自行參閱前述	2021 年 10 月 12 日

作業系統與版本	微軟 KB 編號	最初發布日期
2008 R2	連結的先決條件) 5006728 (僅限安全性更新，請自行參閱前述連結的先決條件)	

Symantec Endpoint Protection 官方說明可參考以下網址
https://techdocs.broadcom.com/tw/zh-tw/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/upgrading-to-a-new-release-v14510472-d27e6/acs-support.html

3. 若有失敗的狀況發生，請提供 c:\temp 或是 c:\windows\temp 下的 SEP_INST.LOG 或是 SYMEVENT.LOG 交給客服人員確認。
客服電話：(02) 2344-2836#1105、客服信箱：ndcdc@ndc.gov.tw。