思科安全終端：命令列交換機介紹

目錄

簡介

背景資訊

思科安全終端命令列交換機

- 安全終端安裝程式交換機
  - amp_installer.exe
- 安全終端支援診斷工具交換機
  - ipsupporttool.exe
- 安全終端UI交換機
  - iptraytool.exe
- 安全終端SFC交換機
  - sfc.exe

相關資訊

簡介

本文檔介紹可用於思科安全終端的命令列(CLI)交換機。

背景資訊

Cisco Secure Endpoint包含許多可自定義的功能和操作，可透過命令列開關在終端本地執行。本檔案會示範這些案例。

思科安全終端命令列交換機

安全終端安裝程式交換機

amp_installer.exe

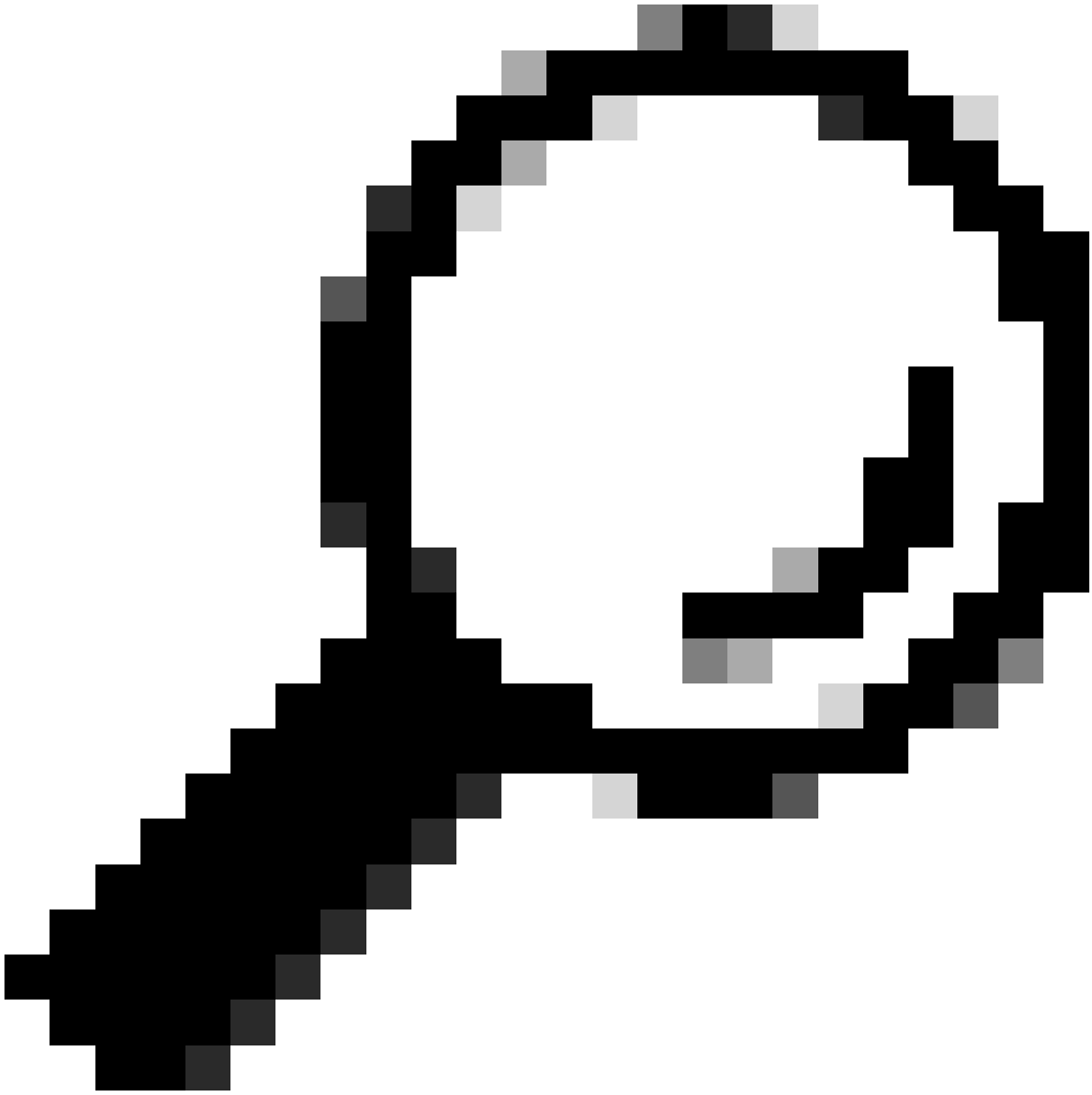
1. 在Windows上打開命令提示符。
2. 在命令提示符下導航到安裝程式所在的資料夾(Downloads folder used as below)。

```
cd C:\Users\sysadmin\Downloads
```

- 執行提供的可用交換機。

```
amp_protect.exe <switch>
```

注意：執行命令後不會返回任何輸出。



提示：一次可以使用多個交換機。

命令列開關	命令說明	特別說明
/S	用於將安裝程式置於靜默模式。	

/temppath	用於指定要擷取並執行之安裝檔案的自訂暫存位置。	/temppath C:\
/desktopicon 0	用於指定不建立案頭圖示。	這是預設配置，不需要提供。
/desktopicon 1	用於指定建立案頭圖示。	
/startmenu 0	「開始」功能表捷徑並未建立。	
/startmenu 1	「開始」功能表捷徑已建立。	這是預設配置，不需要提供。
/contextmenu 0	停用按一下右鍵上下文選單中的「立即掃描」。	
/contextmenu 1	在右鍵上下文選單中啟用「立即掃描」。	這是預設配置，不需要提供。
/remove 0	解除安裝聯結器並保留檔案以供日後重新安裝。	UUID的XML檔案會保留下來，讓您在重新安裝聯結器時，可以重複使用現有的電腦物件。記錄檔也會保留。如果正在使用聯結器保護密碼，則必須使用/uninstallpassword標誌指定該密碼。
/remove 1	解除安裝聯結器並移除所有相關檔案。	如果正在使用聯結器保護密碼，則必須使用/uninstallpassword標誌指定該密碼。
/uninstallpassword	指定使用/remove標誌時的解除安裝	在標誌後指定解除安裝密碼。

	密碼。如果啟用聯結器保護功能，則必須指定	
/skipdfc 1	略過DFC驅動程式的安裝。	使用此標誌安裝的任何聯結器必須位於停用了網路引擎的策略所在的組中。
/skiptetra 1	略過TETRA驅動程式的安裝。	所有使用此旗標安裝的聯結器必須位於未核取Tetra旗標之原則的群組中。
/D=[路徑]	用於指定要執行安裝的目錄。例如，/D=C:\	必須將其指定為最後一個引數。 對於/D=命令列開關，預設安裝目錄因作業系統而異。以下是Microsoft Windows XP Service Pack 3或更新版本的預設安裝目錄： 對於x86平台： C:\Program Files (x86)\Cisco\AMP 對於x64平台： C:\Program Files\Cisco\AMP
/goldenimage 1	安裝聯結器以準備金色影像	此旗標可協助準備虛擬環境中的金色影像。使用此旗標可防止聯結器在建立金色影像期間啟動和註冊。有關詳情，請參閱：如何使用安全端點準備黃金映像 https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html
/skiposccheck 1	在安裝期間略過作業系統檢查。	此標誌可用於在與不相容的作業系統上安裝安全終結點。

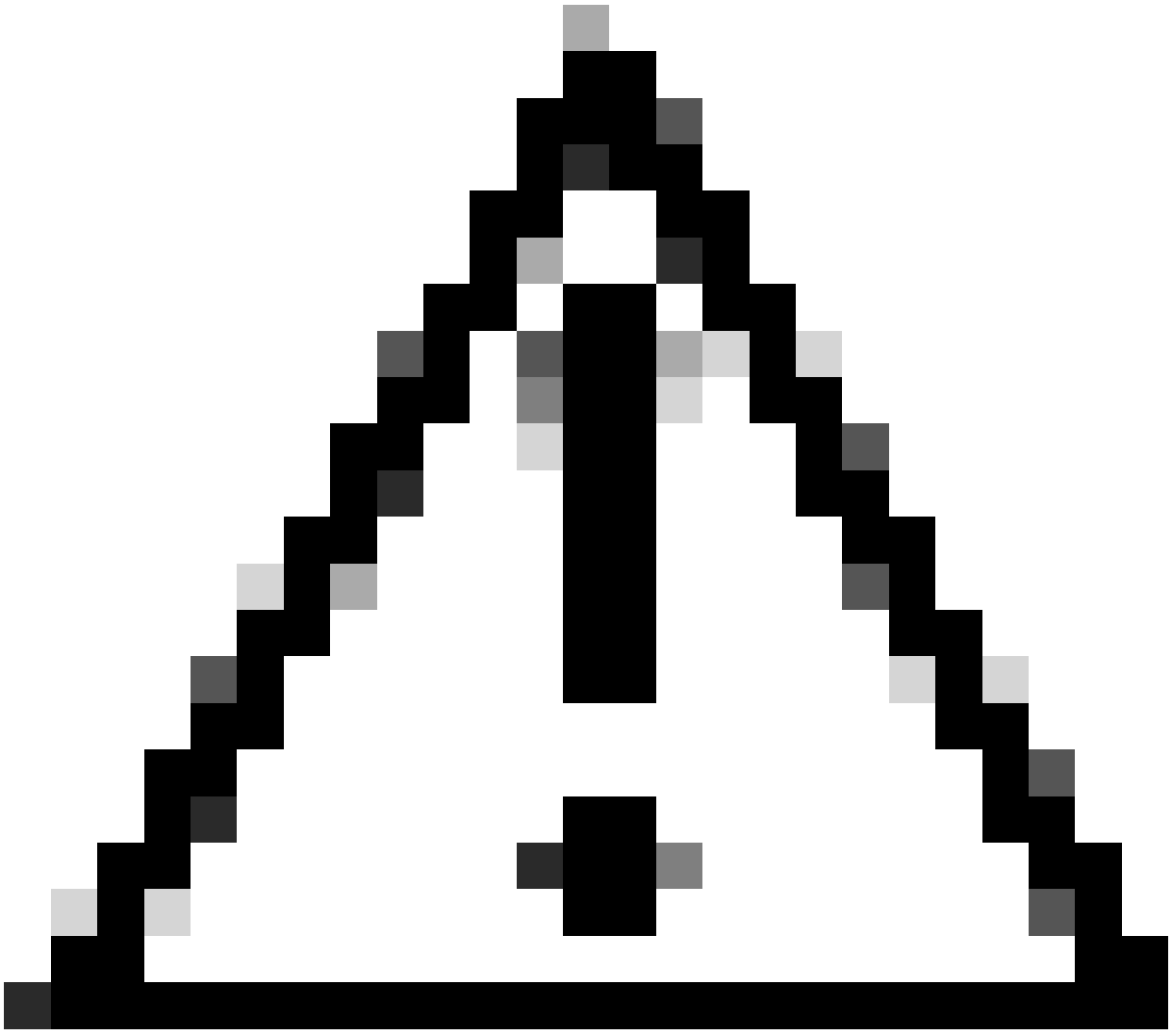
ipsupporttool.exe

- 在Windows上打開命令提示符。

- 在命令提示字元上瀏覽至資料夾。 預設路徑：**C:\Program Files\Cisco\AMP\X.X.X**，X.X.X表示版本號)。
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- 執行提供的可用交換機。
ipsupporttool.exe <switch>

注意：執行交換機時，不會返回任何輸出。

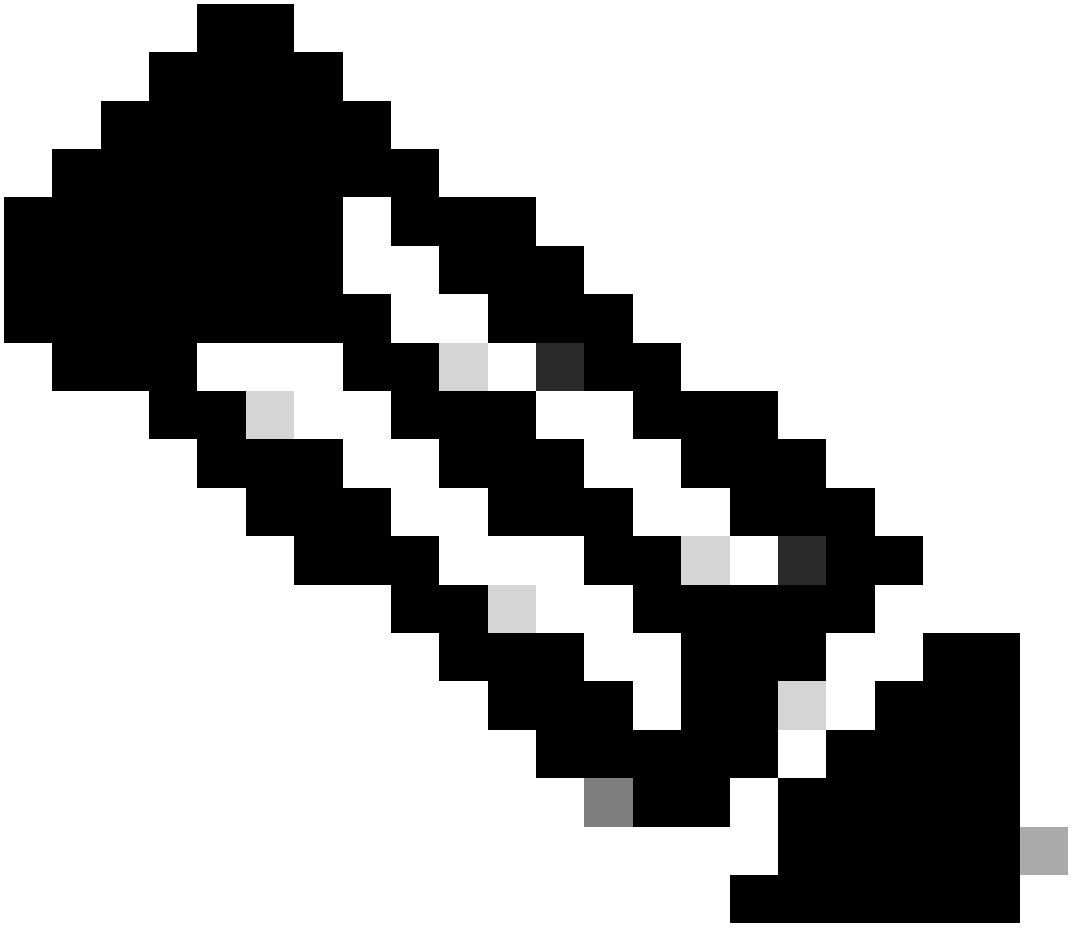


注意：任何參照資料夾選項的切換都需要資料夾已經存在

命令列開關	命令說明	特別說明
-o <路徑>	指定支援工具的輸出資料夾。	如果未指定此選項，則預設為案頭。
-d <安裝路徑>	指定Windows支援工具可以擷取檔案的資料夾。	如果未指定，則預設為Secure Endpoint的預設安裝目錄。
-t <分鐘>	從Windows支援工具運行指定時間的定時調試級別診斷。 以分鐘為單位指定持續時間。	

安全終端UI交換機

iptraytool.exe



註：iptraytool.exe僅在舊版Secure Endpoint上可用。

- 在Windows上打開命令提示符。

- 在命令提示字元上瀏覽至資料夾。 預設路徑：**C:\Program Files\Cisco\AMP\X.X.X**，X.X.X表示版本號)。

```
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
```

- 執行提供的可用交換機。

```
iptray.exe <switch>
```

命令列開關	命令說明	特別說明
-f	允許從命令列啟用客戶端使用者介面。	僅當終端透過策略關閉了GUI，並且未選中Start Client User Interface時，才需要執行此操作。

安全終端SFC交換機

sfc.exe

- 在Windows上打開命令提示符。

- 在命令提示字元上瀏覽至資料夾。 預設路徑：**C:\Program Files\Cisco\AMP\X.X.X**，X.X.X表示版本號)。
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- 執行提供的可用交換機
sfc.exe <switch>

命令列開關	命令說明	特別說明
-s	啟動Immuniet Protect (Windows Connector)服務。 服務必須已經向SCM註冊才能啟動。	
-k	停止Immuniet Protect (Windows Connector)服務。	如果啟用了聯結器保護，請在-k後輸入密碼以成功停止服務。
-u	解除安裝Immunet Protect (Windows Connector)服務。 向Windows服務控制管理器(SCM)註銷服務。 解除安裝程式會使用此選項來解除安裝Windows聯結器服務。	
-r	重設Immuniet Protect (Windows Connector)服務。 這與-i選項非常相似，但不安裝服務。這對於修復local.xml損壞非常有用。	

-l開始	動態切換調試和核心日誌記錄（觸發器為小寫L）。	此狀態將一直保持到關閉、重新啟動服務，或者配置新策略以更改日誌記錄級別。
-l停止	動態關閉調試和核心日誌記錄（觸發器為小寫L）。	
-unblock SHA_of_file	此選項可取消阻止進程執行。 執行此命令切換之後，應用程式可從應用程式封鎖清單的本機核心快取中移除。	當應用程式因誤報或錯誤而遭封鎖，而您想要快速解除封鎖應用程式，而不需等待30分鐘或重新啟動電腦時，即可使用此指令。
-reregister	此選項可以在服務運行時從local.xml和登錄檔清除uuid和證書，並觸發重新註冊。Local.xml和登入會以新值更新。但是，如果啟用了ID同步，並且聯結器再次獲取現有UUID，則會阻止此操作。 如果用於初始安裝的安裝軟體套件已被修改，則此操作可在重新註冊之後將聯結器置於預設組/策略中。	如果啟用了聯結器保護，您需要輸入以下內容：sfc.exe -reregister _password_
-forceupdate	此選項會強制聯結器更新TETRA定義。	
-forceapdeupdate	此選項強制聯結器更新行為保護定義。	您可以在安全終端控制台中的裝置軌跡中檢查終端上安裝的當前行為保護定義。

相關資訊

- 技術支援與文件 - Cisco Systems
- 思科安全終端- TechNotes
- 思科安全終端-使用手冊
- 使用Secure Endpoint Mac/Linux CLI

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。