

安全終端Mac代理自動配置(PAC)設定指南

目錄

[簡介](#)

[支援的作業系統版本](#)

[設定](#)

[其他資訊](#)

[限制](#)

簡介

本檔案介紹Cisco Secure Endpoint Mac connector 1.22.0及更高版本上的代理自動配置(PAC)安裝指南。

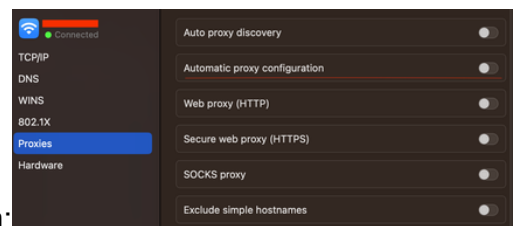
支援的作業系統版本

- macOS Big Sur(11.0)或更高版本

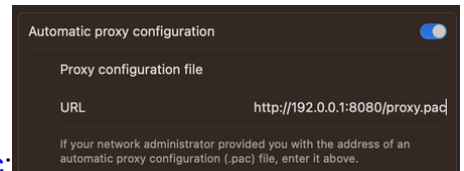
設定

準備一個指定IP地址和代理伺服器型別 (macOS支援HTTP、HTTPS和SOCKS代理) 的有效PAC檔案，並在HTTP或HTTPS (無身份驗證) 伺服器上託管PAC檔案。

系統管理員可以執行以下步驟啟用該功能：



1. 在代理系統網路設定中選擇Automatic proxy configuration:



2. 提供PAC檔案的URL。例如，<http://192.0.0.1:8080/proxy.pac>:
3. 在Web控制檯的Proxy Type下拉選單中選擇MacOS Auto Proxy Configuration以啟用PAC策略選項。
4. 在終端會話中使用ampcli sync命令同步連結器策略。

連結器將嘗試自動使用PAC檔案中指定的代理連線資訊。

其他資訊

- 聯結器每30分鐘查詢一次PAC檔案提供的代理資訊。
- 以下是有效PAC檔案的範例：

```
function FindProxyForURL(url, host) {  
// If the hostname matches, send direct.  
  if (dnsDomainIs(host, "someurl.cisco.com") ||  
      shExpMatch(host, "(*.cisco.com|cisco.com)"))  
    return "DIRECT";  
// If the protocol or URL matches, send direct.  
  if (url.substring(0, 4)=="ftp:" ||  
      shExpMatch(url, "http://cisco.com/folder/*"))  
    return "DIRECT";  
// DEFAULT RULE: All other traffic, use below proxies, in fail-over order.  
  return "PROXY 4.5.6.7:8080; PROXY 7.8.9.10:8080"; }  
}
```

限制

- PAC檔案不能在需要身份驗證的伺服器上託管。
- 安全終結點只能支援指定未經身份驗證的代理的PAC檔案。

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）。