

在FMC管理的FTD上設定AnyConnect動態分割通道

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[限制](#)

[設定](#)

[步驟1.編輯組策略以使用動態拆分隧道](#)

[步驟2.配置AnyConnect自定義屬性](#)

[步驟3.驗證配置，儲存並部署](#)

[驗證](#)

[疑難排解](#)

[問題](#)

[解決方案](#)

[相關資訊](#)

簡介

本檔案介紹如何在Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)上設定AnyConnect動態分割通道。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco AnyConnect
- FMC基礎知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- FMC版本7.0
- FTD版本7.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

由FMC管理的FTD上的AnyConnect動態拆分隧道配置在FMC 7.0版及更新版本上完全可用。如果運行較舊版本，則需要按照[高級AnyConnect VPN部署 \(適用於FMC的Firepower威脅防禦\)](#)中的說明通過FlexConfig對其進行配置。

使用動態拆分隧道配置，您可以根據DNS域名微調拆分隧道配置。由於與完全限定的域名(FQDN)關聯的IP地址可以更改，因此基於DNS名稱的分隔隧道配置可提供更動態的定義，說明哪些流量是包括在遠端訪問虛擬專用網路(VPN)隧道中，哪些流量不是。如果為排除的域名返回的任何地址在VPN中包含的地址池內，則這些地址將被排除。未阻止排除的域。相反，流向這些域的流量保留在VPN隧道之外。

請注意，您還可以設定動態分割通道 定義要包含在通道中的域，否則將根據IP地址排除這些域。

限制

目前，仍不支援這些功能：

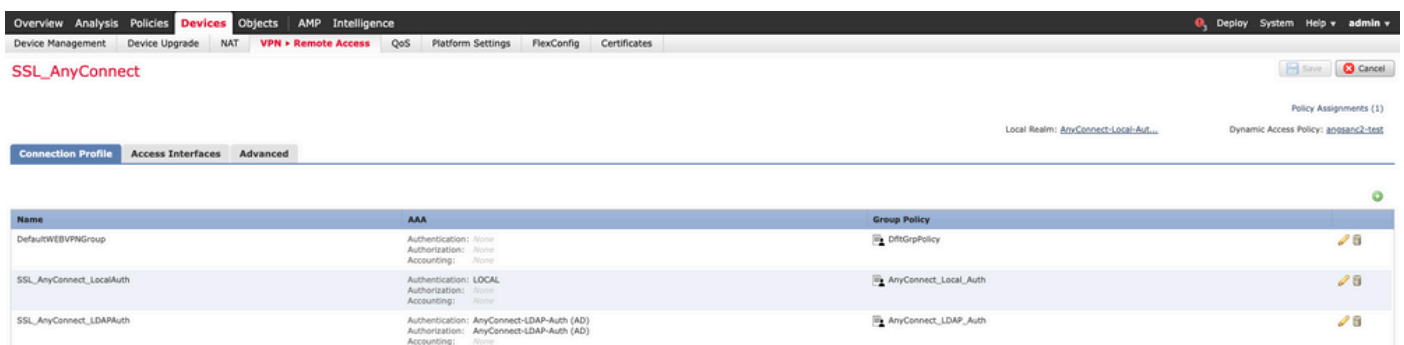
- iOS(Apple)裝置不支援動態拆分隧道。請參閱思科錯誤ID [CSCvr54798](#)
- Anyconnect Linux客戶端不支援動態拆分隧道。請參閱Cisco錯誤ID [CSCvt64988](#)

設定

本節介紹如何在FMC管理的FTD上設定AnyConnect動態分割通道。

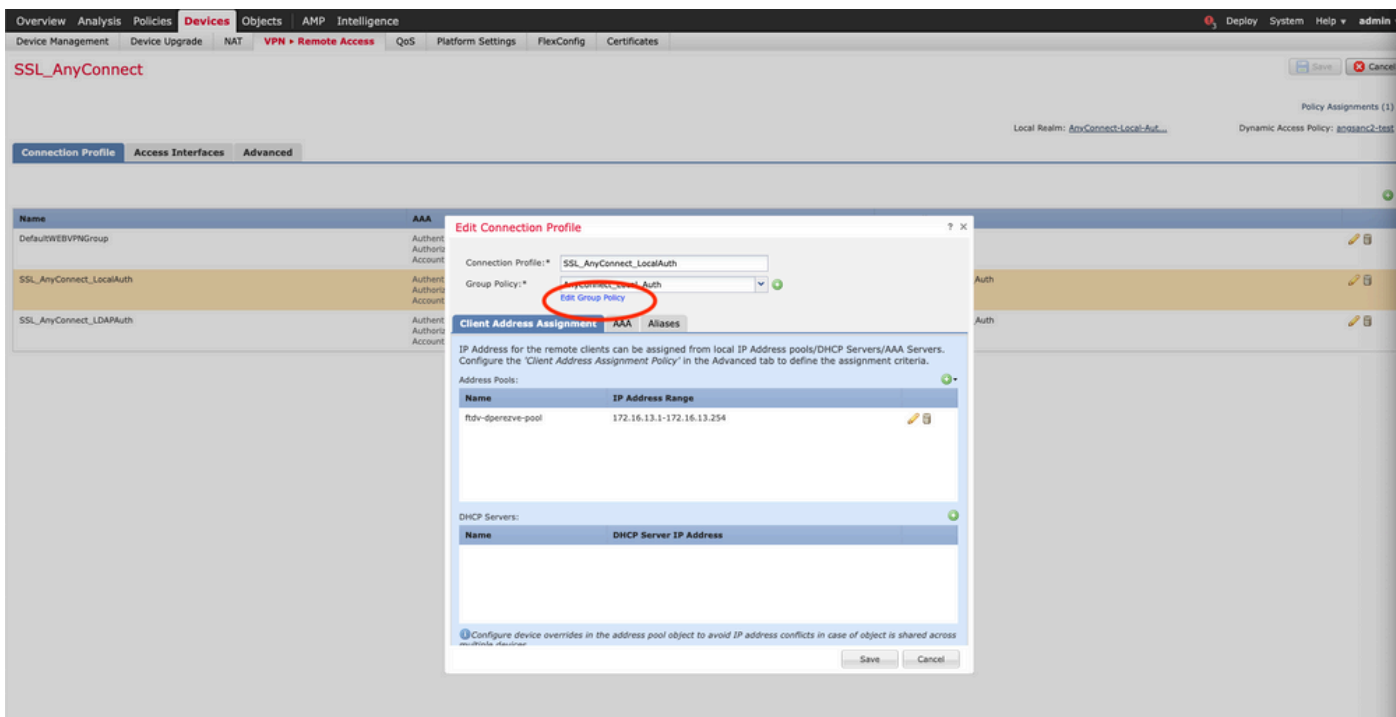
步驟1.編輯組策略以使用動態拆分隧道

1.在FMC上，導航至Devices > VPN > Remote Access，然後選擇您要應用配置的Connection Profile。



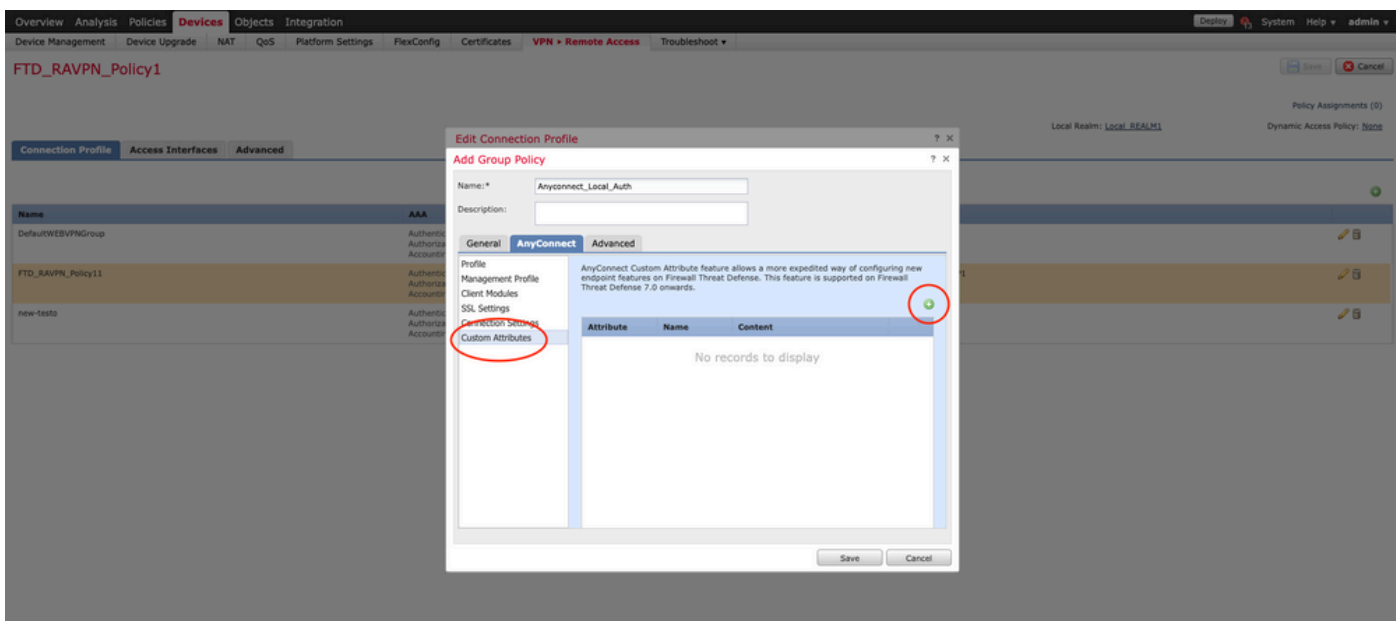
Name	AAA	Group Policy
DefaultWEBVpngGroup	Authentication: none Authorization: none Accounting: none	DefaultGrpPolicy
SSL_AnyConnect_LocalAuth	Authentication: LOCAL Authorization: none Accounting: none	AnyConnect_Local_Auth
SSL_AnyConnect_LDAPAuth	Authentication: AnyConnect-LDAP-Auth (AD) Authorization: AnyConnect-LDAP-Auth (AD) Accounting: none	AnyConnect_LDAP_Auth

2.選擇編輯組策略以修改已建立的一個組策略。

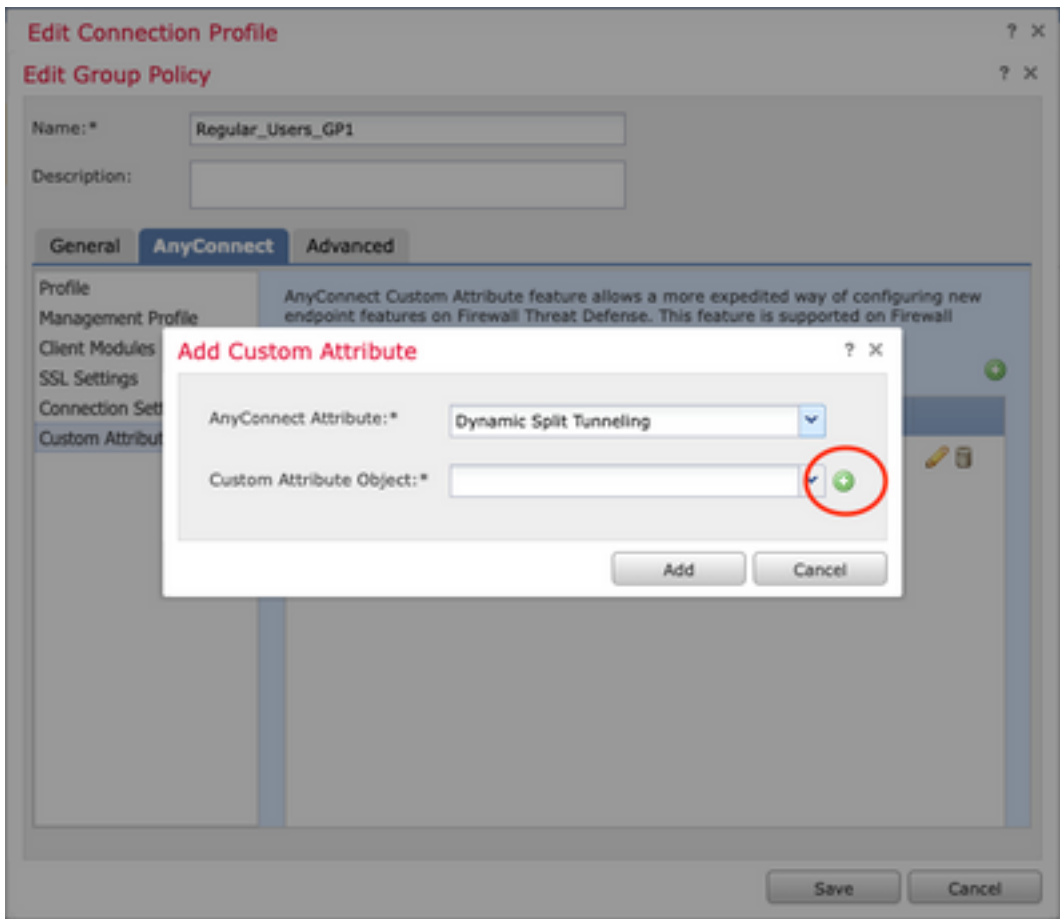


步驟2.配置AnyConnect自定義屬性

1.在「組策略」配置下，導航至Anyconnect > 自定義屬性，單擊Add(+)按鈕：

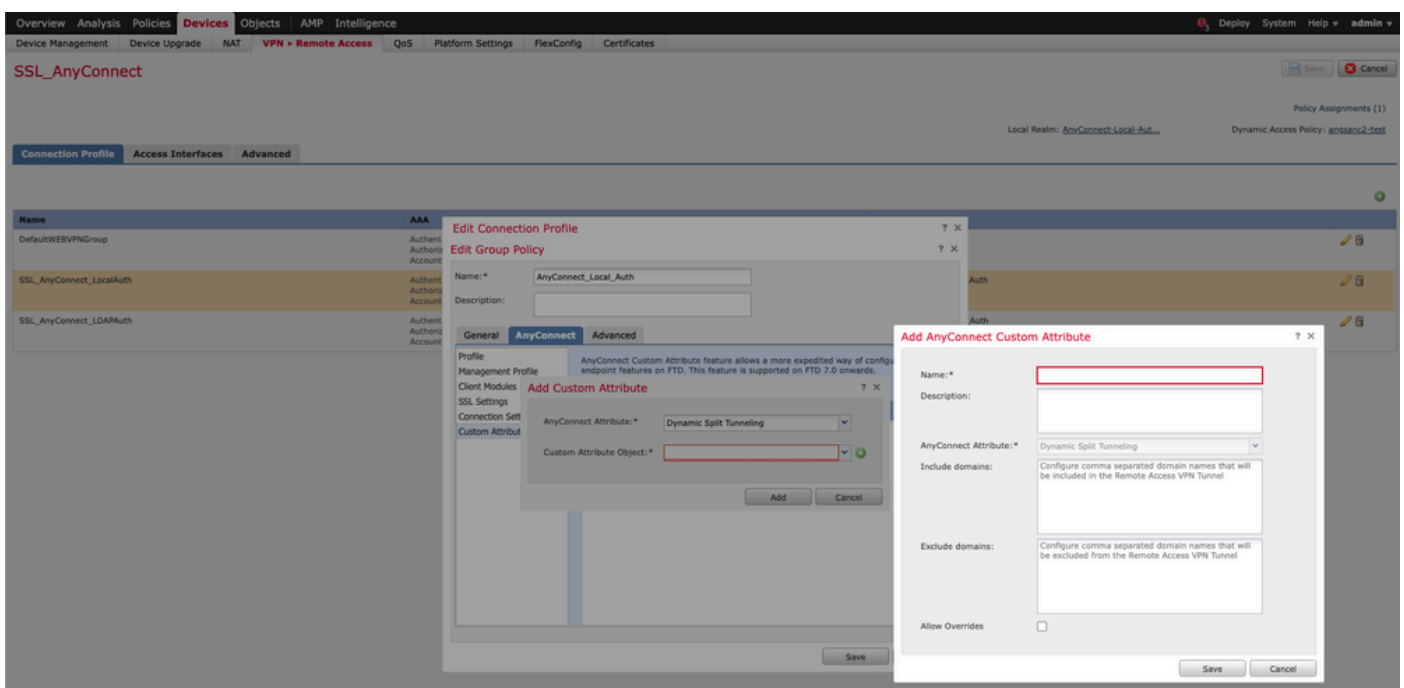


2.選擇Dynamic Split Tunneling AnyConnect屬性，然後按一下Add(+)按鈕以建立新的自定義屬性對象：



3. 輸入AnyConnect自定義屬性的名稱，並將域配置為動態包含或排除。

注意：您只能配置Include domains或Exclude domains。



在本例中，我們將cisco.com設定為要排除的網域，並將自訂屬性命名為Dynamic-Split-Tunnel，如下圖所示：

Add AnyConnect Custom Attribute

Name:*

Description:

AnyConnect Attribute:*

Include domains:

Exclude domains:

Allow Overrides

步驟3.驗證配置，儲存並部署

驗證已設定的自訂屬性是否正確，儲存組態，並將變更部署至問題中的FTD。

Add Group Policy

Name:*

Description:

General **AnyConnect** **Advanced**

Profile
Management Profile
Client Modules
SSL Settings
Connection Settings
Custom Attributes

AnyConnect Custom Attribute feature allows a more expedited way of configuring new endpoint features on FTD. This feature is supported on FTD 7.0 onwards.

Attribute	Name	Content
Dynamic Split Tunneling	Dynamic-Split...	Include domains: None Exclude domains: cisco.com

驗證

您可以透過指令行介面(CLI)在FTD上運行以下命令，以確認動態分割通道組態：

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy <group-policy的名稱>

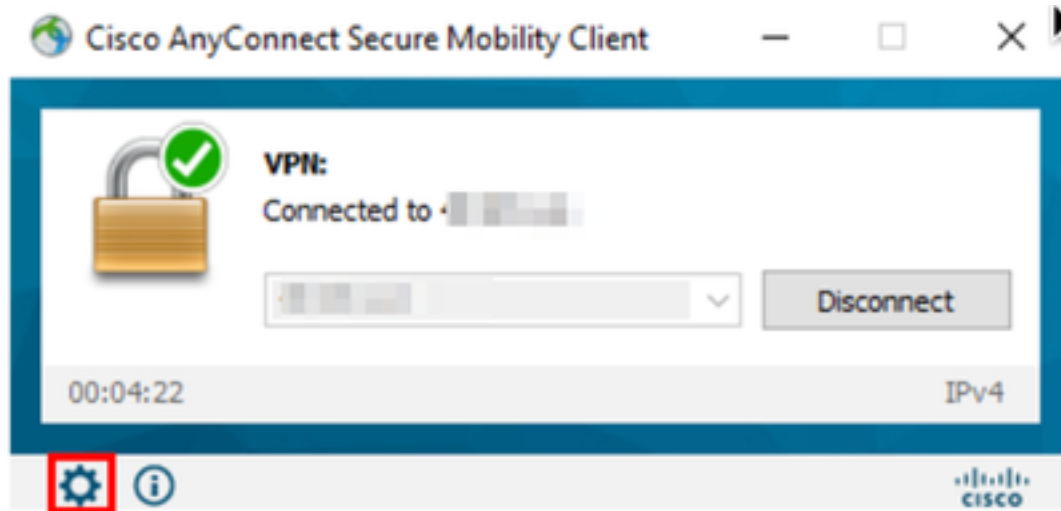
在本範例中，組態是下一步：

```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
anyconnect-custom dynamic-split-exclude-domains value cisco.com
anyconnect-custom dynamic-split-include-domains none
```

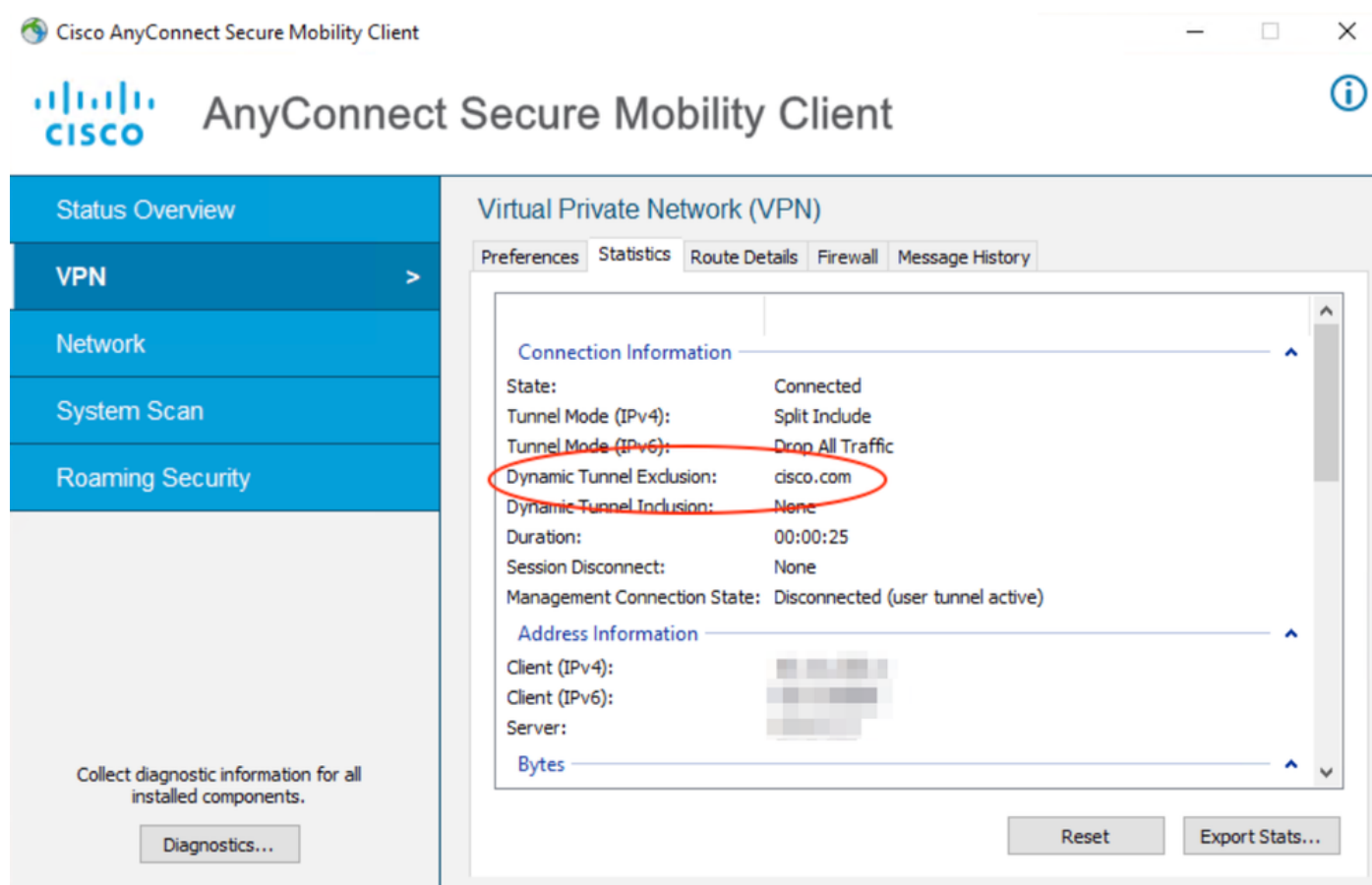
```
ftd# show run webvpn
webvpn
enable outside
anyconnect-custom-attr dynamic-split-exclude-domains
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

若要驗證使用者端上設定的動態通道排除，請執行以下操作：

1. 啟動AnyConnect軟體並按一下齒輪圖示，如下圖所示：



2. 導覽至VPN > Statistics，並確認在Dynamic Split Exclusion/Inclusion下顯示的域：



疑難排解

您可以使用AnyConnect診斷和報告工具(DART)來收集有助於排除AnyConnect安裝和連線問題的資料。

DART彙編了思科技術支援中心(TAC)分析的日誌、狀態和診斷資訊，不需要管理員許可權即可在客戶端電腦上運行。

問題

如果在AnyConnect自定義屬性(例如*.cisco.com)中配置了萬用字元，則AnyConnect會話將斷開。

解決方案

您可以使用cisco.com網域值允許替代萬用字元。此更改允許您包括或排除www、cisco.com和tools.cisco.com等域。

相關資訊

- 如需其他協助，請聯絡技術協助中心(TAC)。需要有效的支援合約：[思科全球支援聯絡人](#)。
- 您還可以訪問Cisco VPN社群 [此處](#)。

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）。