設定 ASA 的 AnyConnect VPN 管理通道

目錄

簡介
必要條件
需求
採用元件
背景資訊
管理隧道的工作
限制
設定
通過ASDM/CLI在ASA上進行配置
建立AnyConnect管理VPN配置檔案
AnyConnect管理VPN配置檔案的部署方法
（可選）配置自定義屬性以支援全隧道配置
驗證
疑難排解
相關資訊

簡介

本文檔介紹如何將ASA配置為VPN網關通過管理VPN隧道接受來自Cisco AnyConnect安全移動客戶端的連線。

必要條件

需求

思科建議您瞭解以下主題：

- 通過自適應安全裝置管理器(ASDM)配置VPN
- 基本自適應安全裝置(ASA)CLI配置
- X509憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA軟體版本9.12(3)9
- Cisco ASDM軟體版本7.12.2
- Windows 10與Cisco AnyConnect安全移動客戶端版本4.8.03036

注意：下載AnyConnect VPN Web部署包(anyconnect-win*.pkg or anyconnect-macos*.pkg)從Cisco Software Download(僅限註冊客戶)網站下載。將AnyConnect VPN客戶端複製到要下載到遠端使用者電腦的ASA的快閃記憶體，以與ASA建立SSL VPN連線。有關詳細資訊，請參閱

ASA配置指南的安裝AnyConnect客戶端部分。

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

管理VPN隧道確保無論何時客戶端系統通電時連線到公司網路，而不僅僅是在終端使用者建立VPN連線時。您可以對辦公室外端點（尤其是使用者通過VPN不經常連線到辦公室網路的裝置）執行補丁管理。需要企業網路連線的終端作業系統登入指令碼也受益於此功能。

AnyConnect管理隧道允許管理員在使用者登入之前連線AnyConnect，而無需使用者干預。AnyConnect管理隧道可與受信任網路檢測結合使用，因此僅當終端位於外部並與使用者啟動的VPN斷開連線時才會觸發。AnyConnect管理隧道對終端使用者是透明的，在使用者發起VPN時自動斷開。

作業系統/應用程式	**最低版本要求**
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect版本	4.7.00136
macOS AnyConnect版本	4.7.01076
Linux	不支援

管理隧道的工作

AnyConnect VPN代理服務在系統啟動時自動啟動。它檢測到管理隧道功能已啟用（通過管理VPN配置檔案），因此它啟動管理客戶端應用程式以啟動管理隧道連線。管理客戶端應用程式使用管理VPN配置檔案中的主機條目來啟動連線。然後，VPN隧道按慣例建立，但有一個例外：管理隧道連線期間不執行軟體更新，因為管理隧道對使用者是透明的。

使用者通過AnyConnect UI啟動VPN隧道，這將觸發管理隧道終止。一旦管理隧道終止，使用者隧道建立將照常繼續。

使用者斷開VPN隧道的連線，從而觸發管理隧道的自動重建。

限制

- 不支援使用者互動
- 僅支援通過電腦證書儲存區(Windows)進行的基於證書的身份驗證
- 強制實施嚴格的伺服器證書檢查
- 不支援專用代理
- 不支援公共代理（在無法從瀏覽器中檢索本機代理設定的平台上支援ProxyNative值）
- 不支援AnyConnect自定義指令碼

注意：有關詳細資訊，請參閱關於管理VPN隧道。

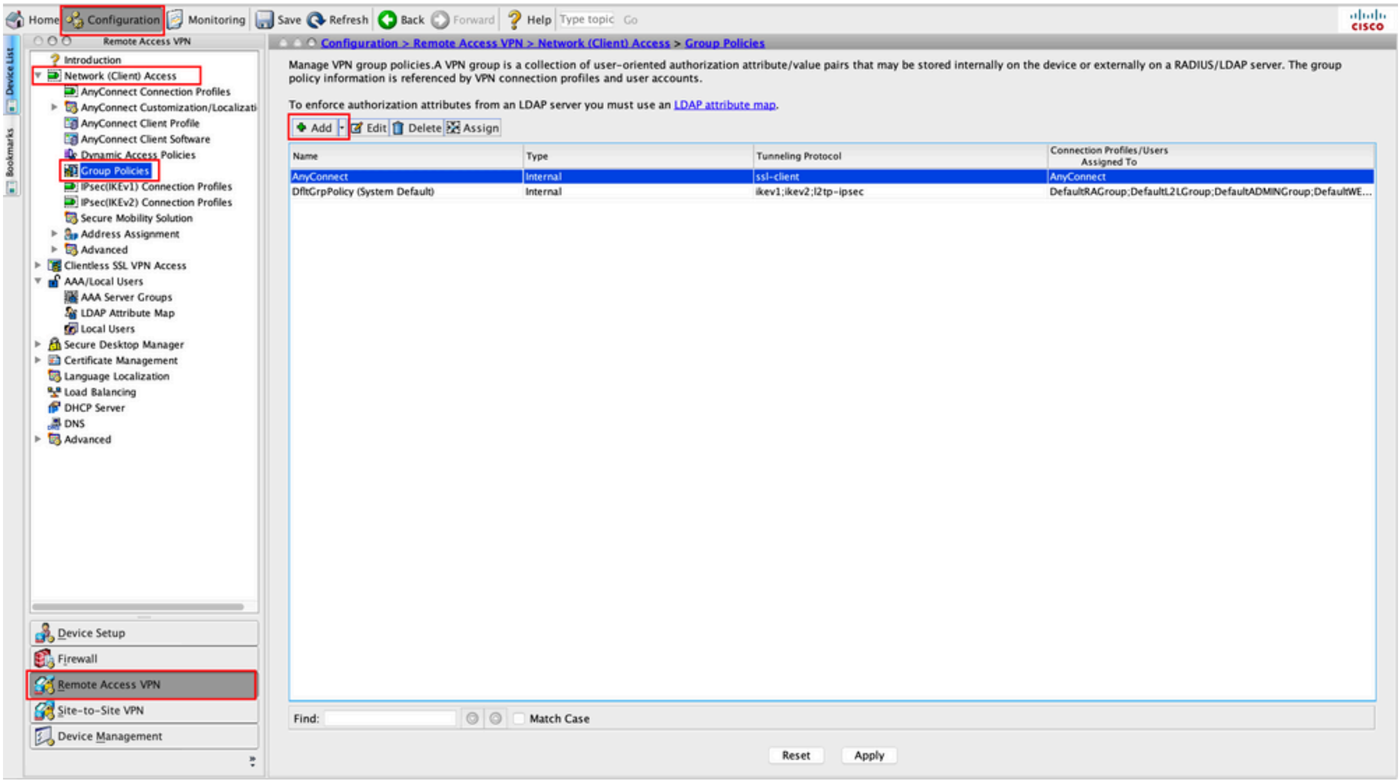
設定

本節介紹如何將Cisco ASA配置為VPN網關，以便通過管理VPN隧道從AnyConnect客戶端接受連線。

通過ASDM/CLI在ASA上進行配置

步驟1.建立AnyConnect組策略。導航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.按一下 Add.

> **注意：**建議您建立僅用於AnyConnect管理隧道的新AnyConnect組策略。



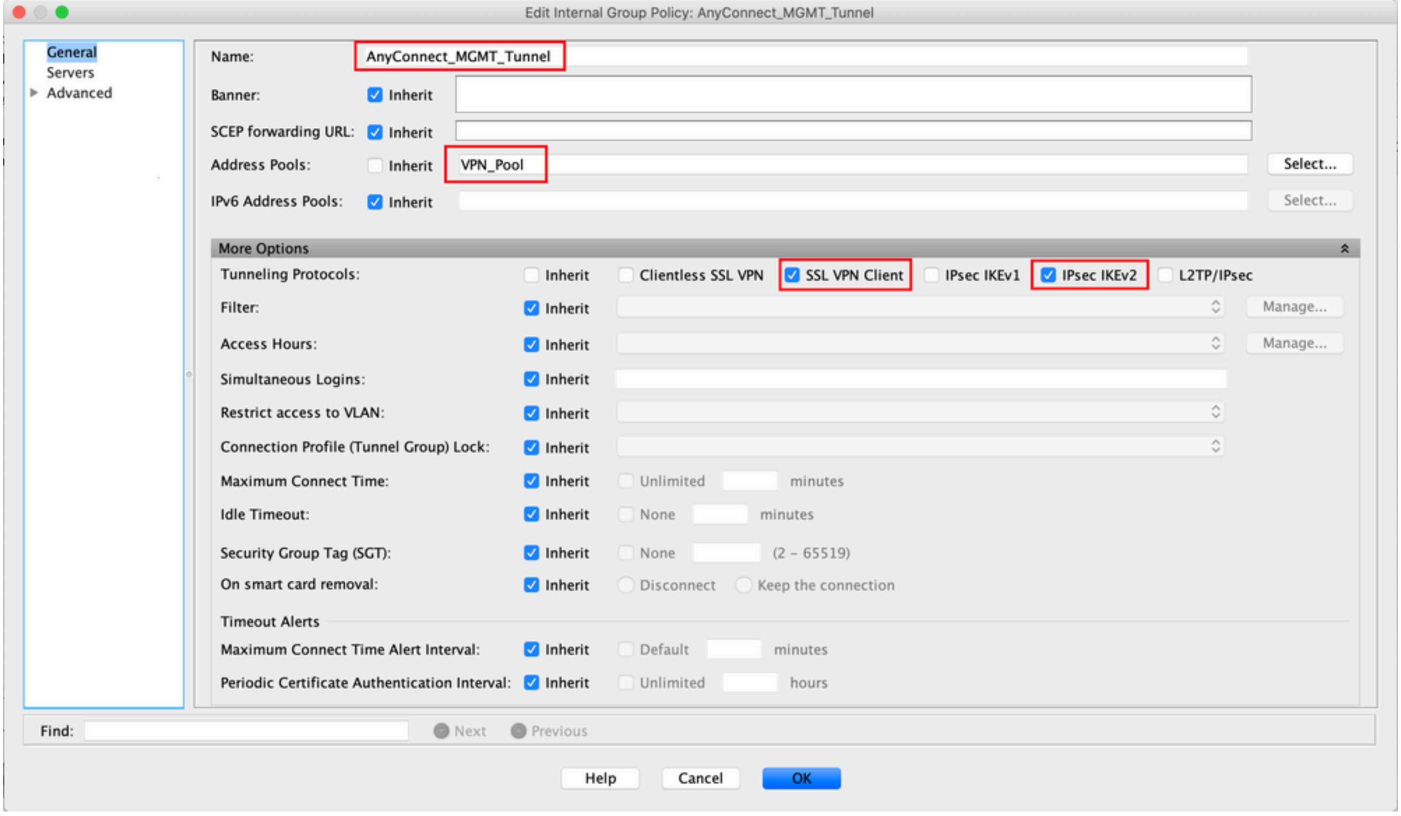
Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE...

步驟2.提供 Name 用於組策略。分配/建立 Address Pool.選擇 Tunneling Protocols 作為 SSL VPN Client 和/或 IPsec IKEv2中，如圖所示。



Edit Internal Group Policy: AnyConnect_MGMT_Tunnel

Name: AnyConnect_MGMT_Tunnel

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

Address Pools: □ Inherit VPN_Pool

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec IKEv1 ☑ IPsec IKEv2 □ L2TP/IPsec

Filter: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ None minutes

Security Group Tag (SGT): ☑ Inherit □ None (2 – 65519)

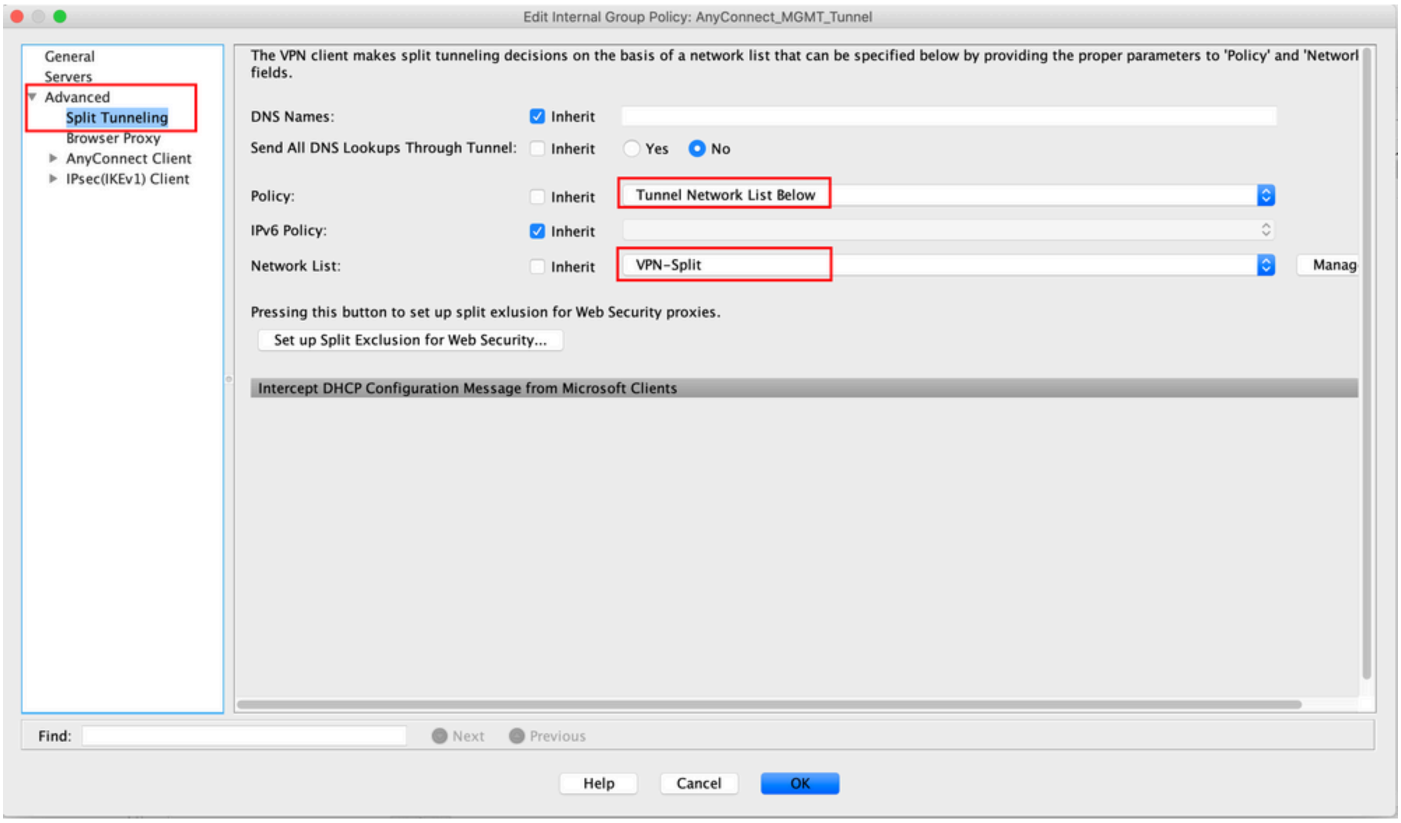
On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

Timeout Alerts

Maximum Connect Time Alert Interval: ☑ Inherit □ Default minutes

Periodic Certificate Authentication Interval: ☑ Inherit □ Unlimited hours

步驟3. 導航至 Advanced > Split Tunneling.配置 Policy 作為 Tunnel Network List Below 並選擇 Network List中，如圖所示。



Edit Internal Group Policy: AnyConnect_MGMT_Tunnel

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Networl fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: □ Inherit ○ Yes ● No

Policy: □ Inherit Tunnel Network List Below

IPv6 Policy: ☑ Inherit

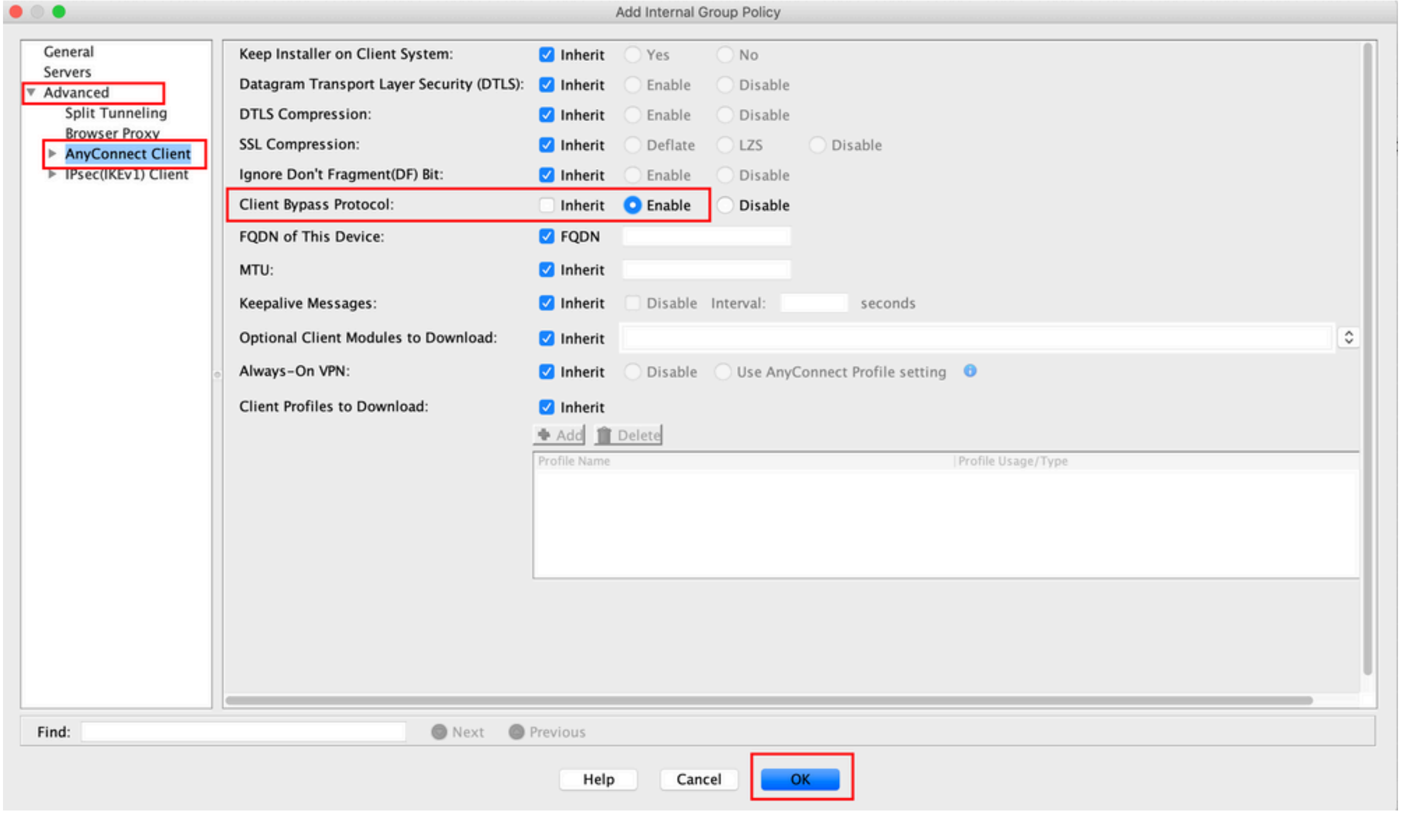
Network List: □ Inherit VPN-Split

Pressing this button to set up split exlusion for Web Security proxies.

Intercept DHCP Configuration Message from Microsoft Clients

注意：如果未同時為IP協定（IPv4和IPv6）推送客戶端地址， **Client Bypass Protocol** 設定必須為 enabled 以使對應的流量不會被管理通道中斷。要配置，請參閱步驟4。

步驟4. 導航至 Advanced > AnyConnect Client. 設定 Client Bypass Protocol 成長至 Enable. 按一下 OK 儲存，如圖所示。



Keep Installer on Client System: ☑ Inherit ○ Yes ○ No

Datagram Transport Layer Security (DTLS): ☑ Inherit ○ Enable ○ Disable

DTLS Compression: ☑ Inherit ○ Enable ○ Disable

SSL Compression: ☑ Inherit ○ Deflate ○ LZS ○ Disable

Ignore Don't Fragment(DF) Bit: ☑ Inherit ○ Enable ○ Disable

Client Bypass Protocol: □ Inherit ● Enable ○ Disable

FQDN of This Device: ☑ FQDN

MTU: ☑ Inherit

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

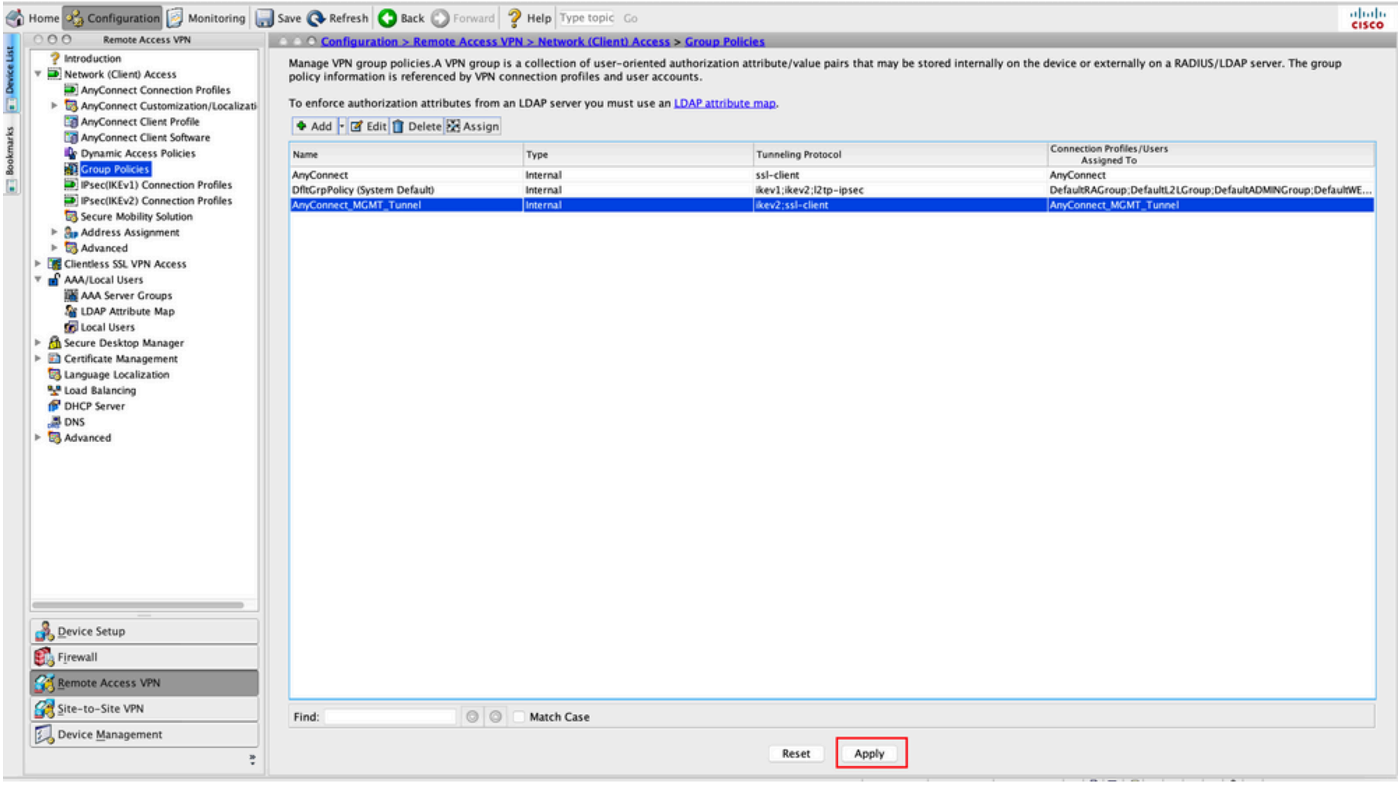
Optional Client Modules to Download: ☑ Inherit

Always-On VPN: ☑ Inherit ○ Disable ○ Use AnyConnect Profile setting

Client Profiles to Download: ☑ Inherit

Profile Name	Profile Usage/Type

步驟5.如圖所示，按一下 Apply 將配置推送到ASA。



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE...
AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel

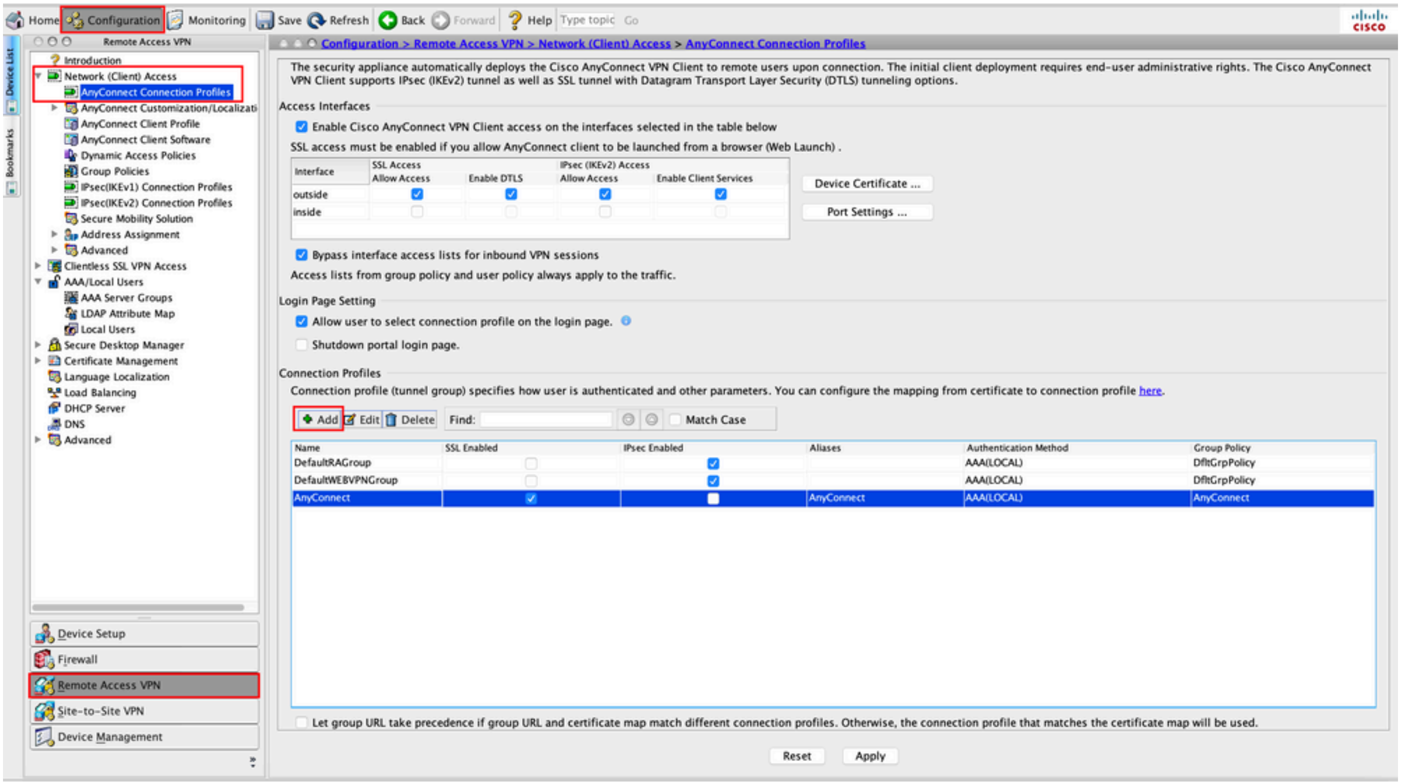
組策略的CLI配置：

```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
```

```
split-tunnel-network-list value VPN-Split
client-bypass-protocol enable
address-pools value VPN_Pool
```

步驟6.建立AnyConnect連線配置檔案。導航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. 按一下 Add.

注意：建議您建立僅用於AnyConnect管理隧道的新AnyConnect連線配置檔案。



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☑	☑
inside	□	□	□	□

Device Certificate ...

Port Settings ...

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile on the login page.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

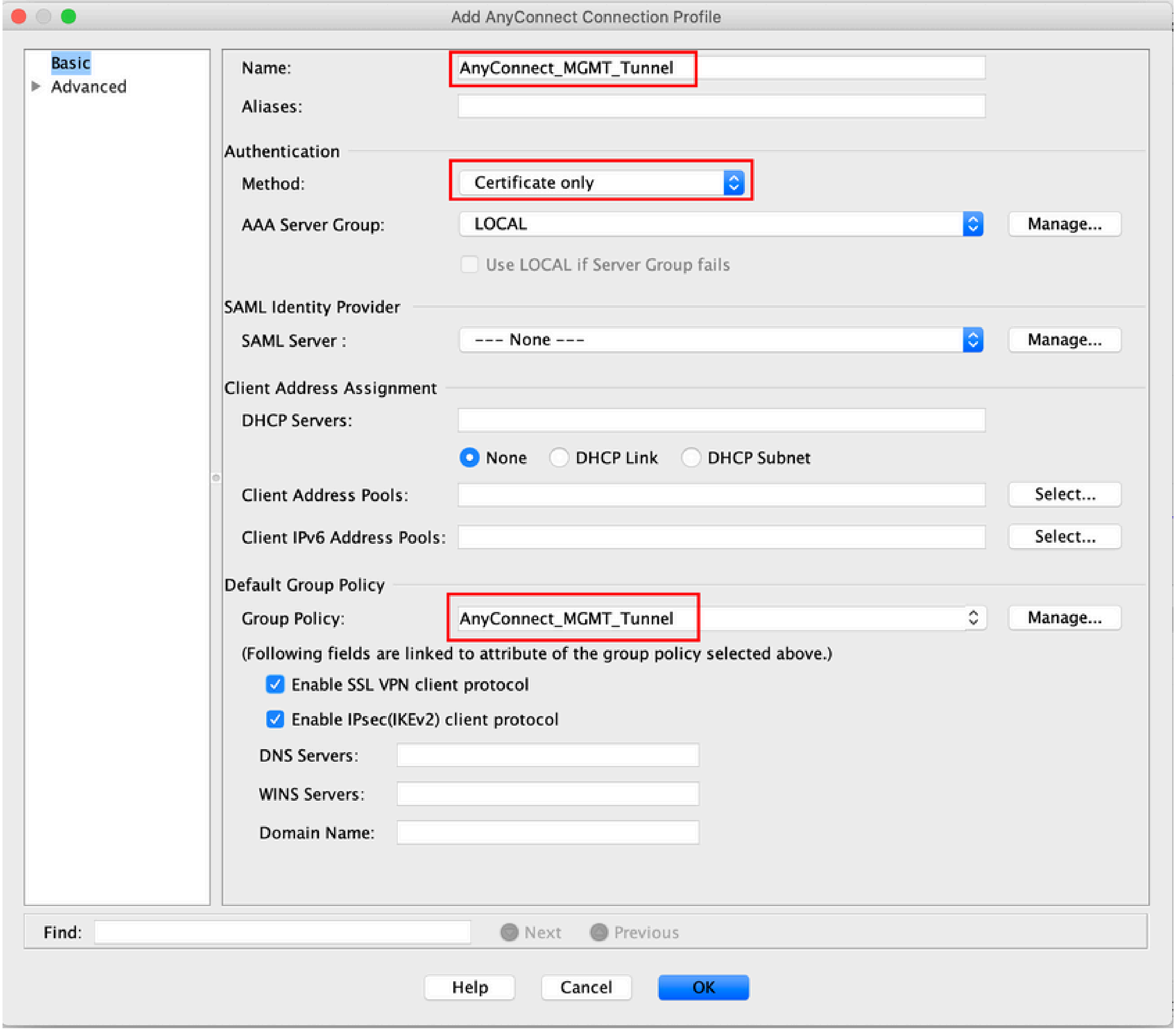
Add | Edit | Delete | Find: | □ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
AnyConnect	☑	□	AnyConnect	AAA(LOCAL)	AnyConnect

□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Reset | Apply

步驟7.提供 Name 連線配置檔案，並設定 Authentication Method 作為 Certificate only.選擇 Group Policy 作為在步驟1中建立的路徑。



Add AnyConnect Connection Profile

Basic
▶ Advanced

Name: AnyConnect_MGMT_Tunnel

Aliases:

Authentication

Method: Certificate only

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : --- None ---

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: AnyConnect_MGMT_Tunnel

(Following fields are linked to attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

☑ Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

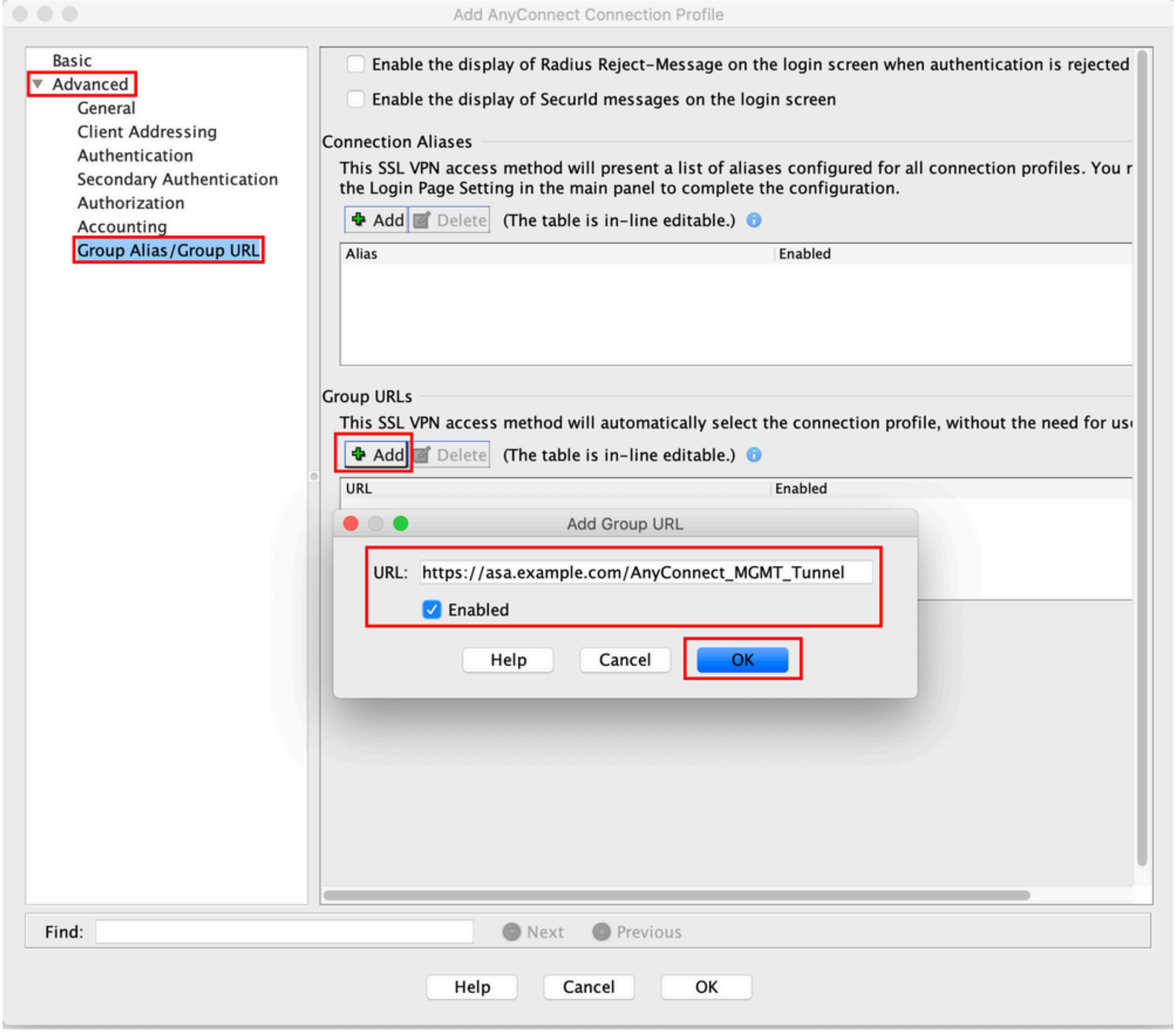
Domain Name:

Find:

注意：確保ASA上存在來自本地CA的根證書。 導航至 Configuration > Remote Access VPN > Certificate Management > CA Certificates 以新增/檢視證書。

注意：請確保由同一本地CA頒發的身份證書存在於電腦證書儲存區(Windows)和/或系統金鑰鏈(MacOS)中。

步驟8.導航至 Advanced > Group Alias/Group URL.按一下 Add 在 Group URLs 並新增 URL.確保 Enabled 已選中。按一下 OK 儲存，如圖所示。



□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You r
the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

Alias	Enabled

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for us

(The table is in-line editable.)

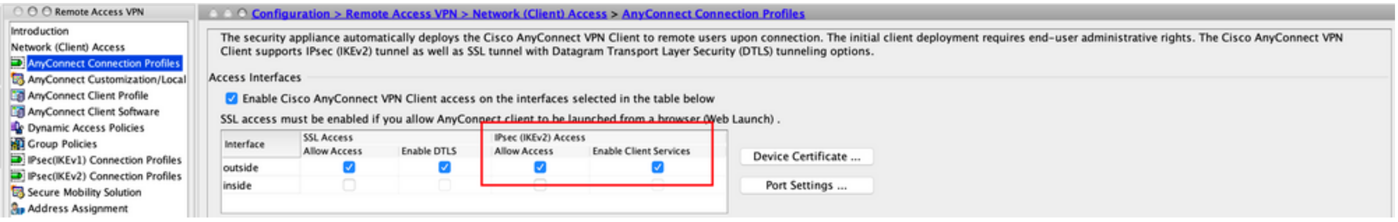
URL	Enabled

Add Group URL

URL: https://asa.example.com/AnyConnect_MGMT_Tunnel

☑ Enabled

如果使用IKEv2，請確保 IPsec (IKEv2) Access 在用於AnyConnect的介面上啟用。


Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Local
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
IPsec(IKEv2) Connection Profiles
Secure Mobility Solution
Address Assignment
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
Device Certificate ...
Port Settings ...

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

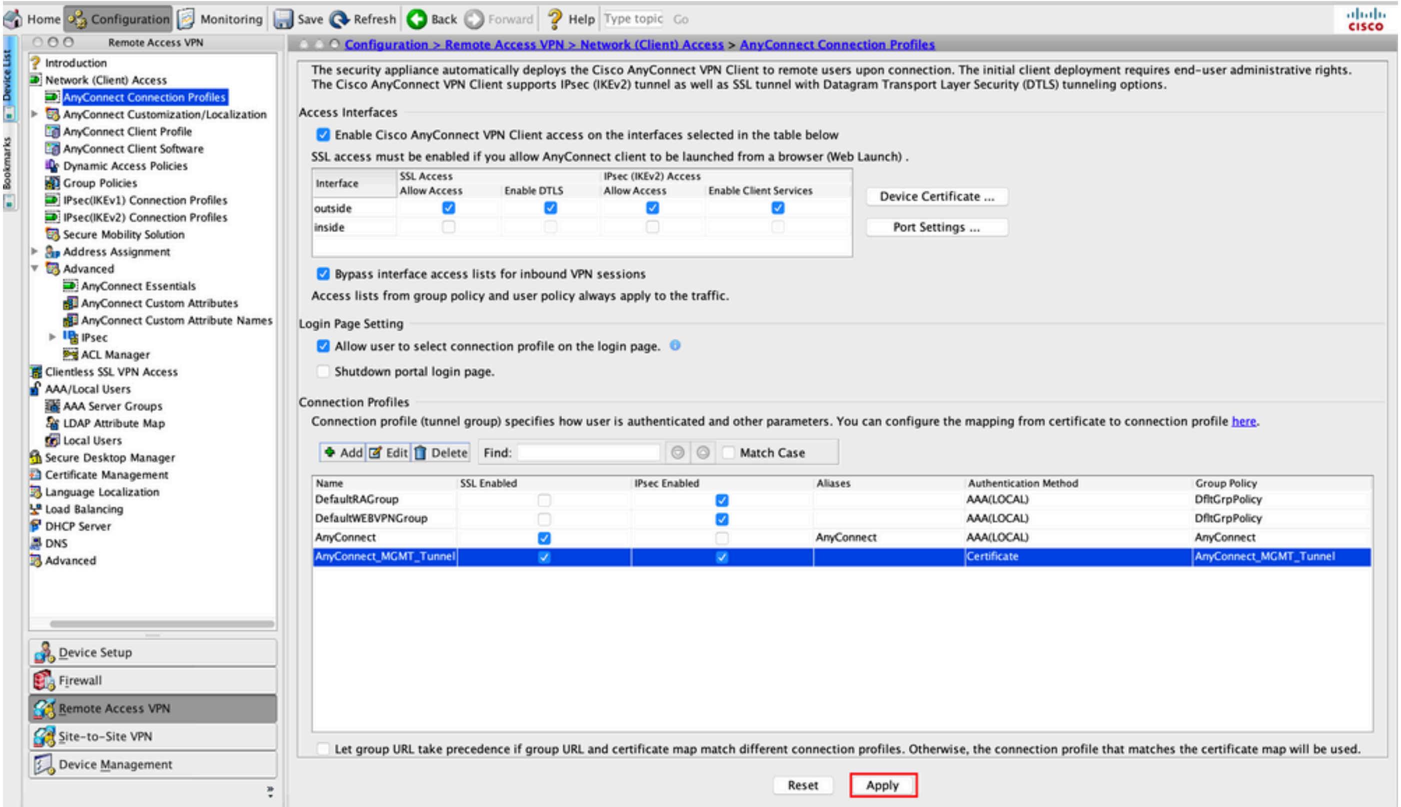
Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☑	☑
inside	□	□	□	□

步驟9.按一下 Apply 將配置推送到ASA。



The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☑	☑
inside	□	□	□	□

Device Certificate ...

Port Settings ...

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile on the login page.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Add Edit Delete Find: □ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
AnyConnect	☑	□	AnyConnect	AAA(LOCAL)	AnyConnect
AnyConnect_MGMT_Tunnel	☑	☑		Certificate	AnyConnect_MGMT_Tunnel

□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

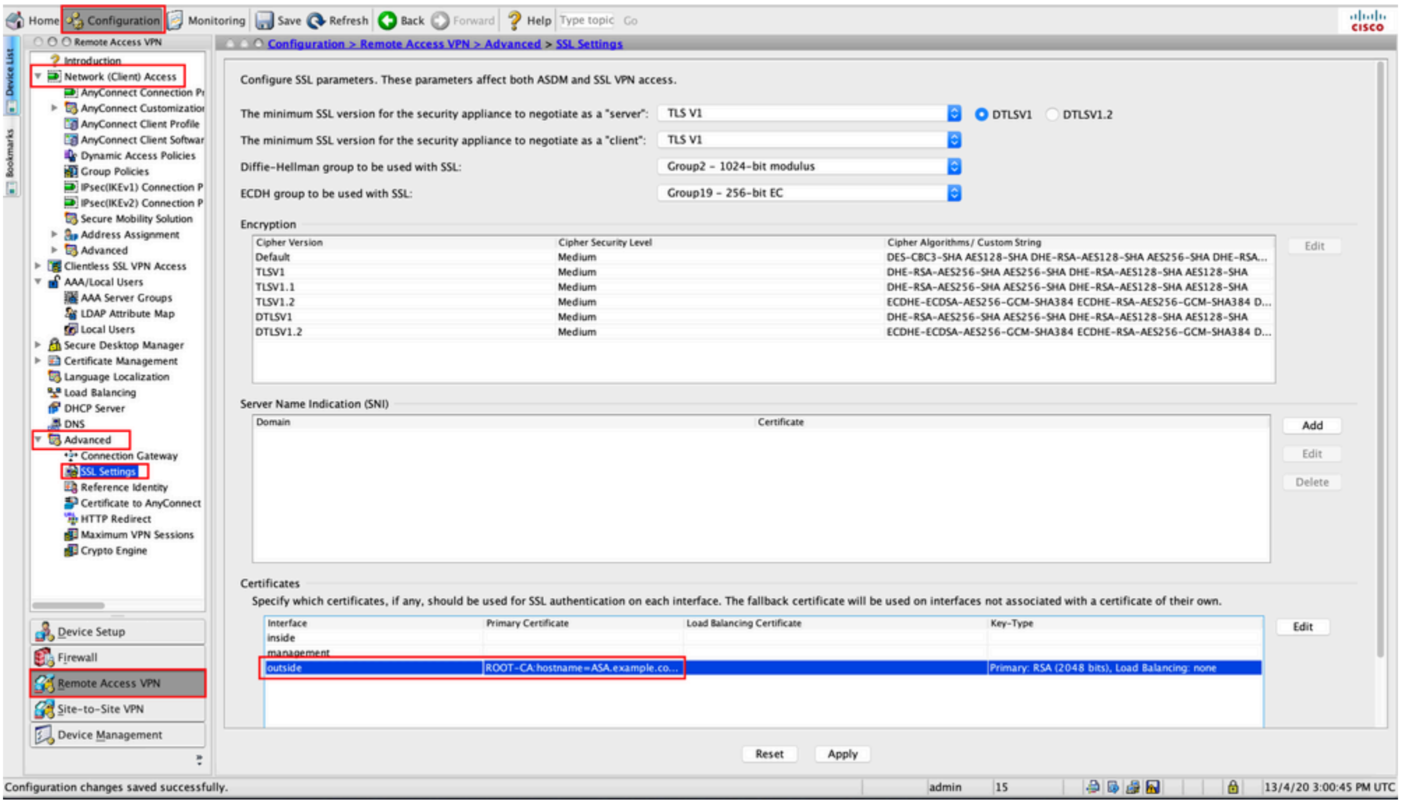
Reset Apply

連線配置檔案的CLI配置（隧道組）：

```
tunnel-group AnyConnect_MGMT_Tunnel type remote-access
tunnel-group AnyConnect_MGMT_Tunnel general-attributes
 default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
 authentication certificate
 group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

步驟10.確保在ASA上安裝受信任證書並繫結到用於AnyConnect連線的介面。導航至 Configuration > Remote Access VPN > Advanced > SSL Settings 新增/檢視此設定。

注意：請參閱在ASA上安裝身份證書。



Configuration > Remote Access VPN > Advanced > SSL Settings

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

The minimum SSL version for the security appliance to negotiate as a "server": TLS V1 ● DTLSV1 ○ DTLSV1.2

The minimum SSL version for the security appliance to negotiate as a "client": TLS V1

Diffie-Hellman group to be used with SSL: Group2 - 1024-bit modulus

ECDH group to be used with SSL: Group19 - 256-bit EC

Encryption

Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA DHE-RSA...
TLSV1	Medium	DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA
TLSV1.1	Medium	DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA
TLSV1.2	Medium	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D...
DTLSV1	Medium	DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA
DTLSV1.2	Medium	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D...

Server Name Indication (SNI)

Domain	Certificate

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
inside			
management			
outside	ROOT-CA:hostname=ASA.example.co...		Primary: RSA (2048 bits), Load Balancing: none

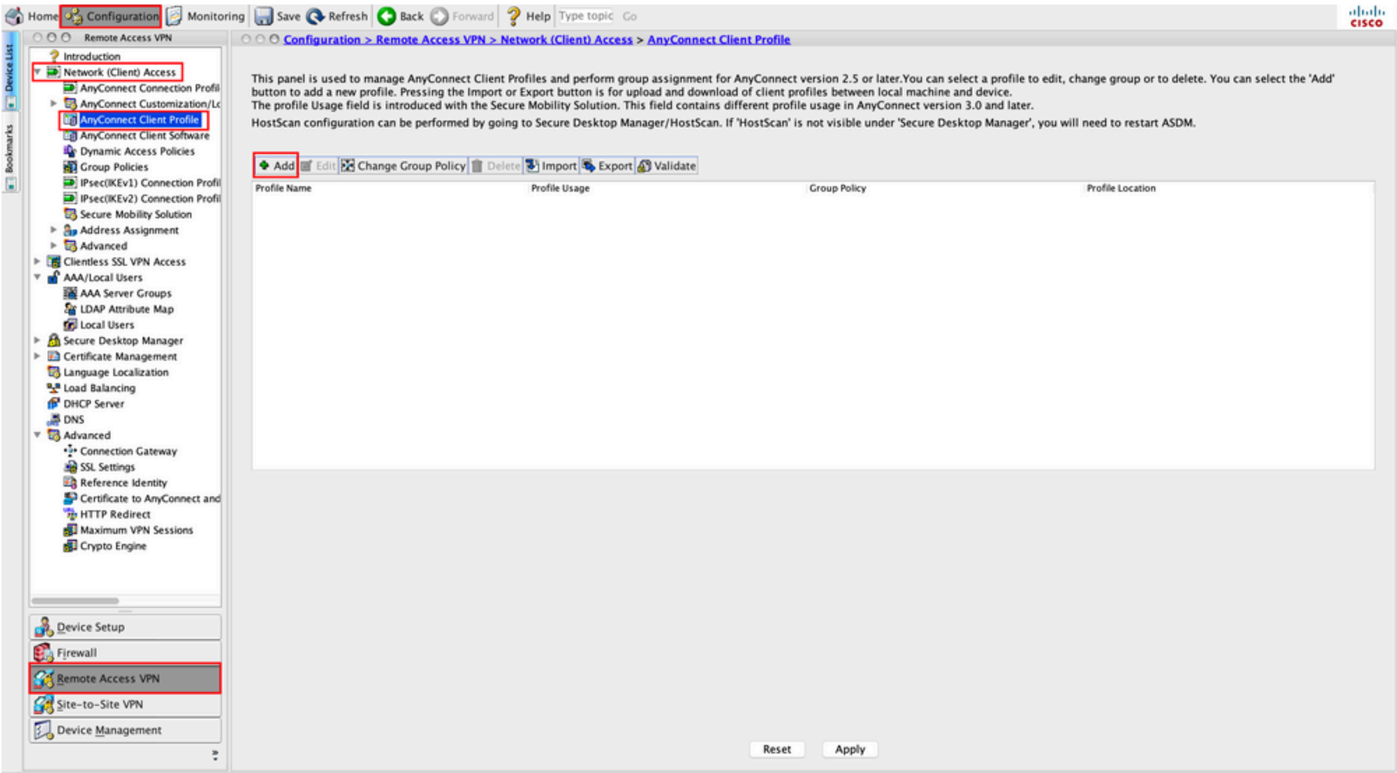
Configuration changes saved successfully. admin 15 13/4/20 3:00:45 PM UTC

SSL信任點的CLI配置：

```
ssl trust-point ROOT-CA outside
```

建立AnyConnect管理VPN配置檔案

步驟1. 建立AnyConnect客戶端配置檔案。導航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.按一下 Add中，如圖所示。

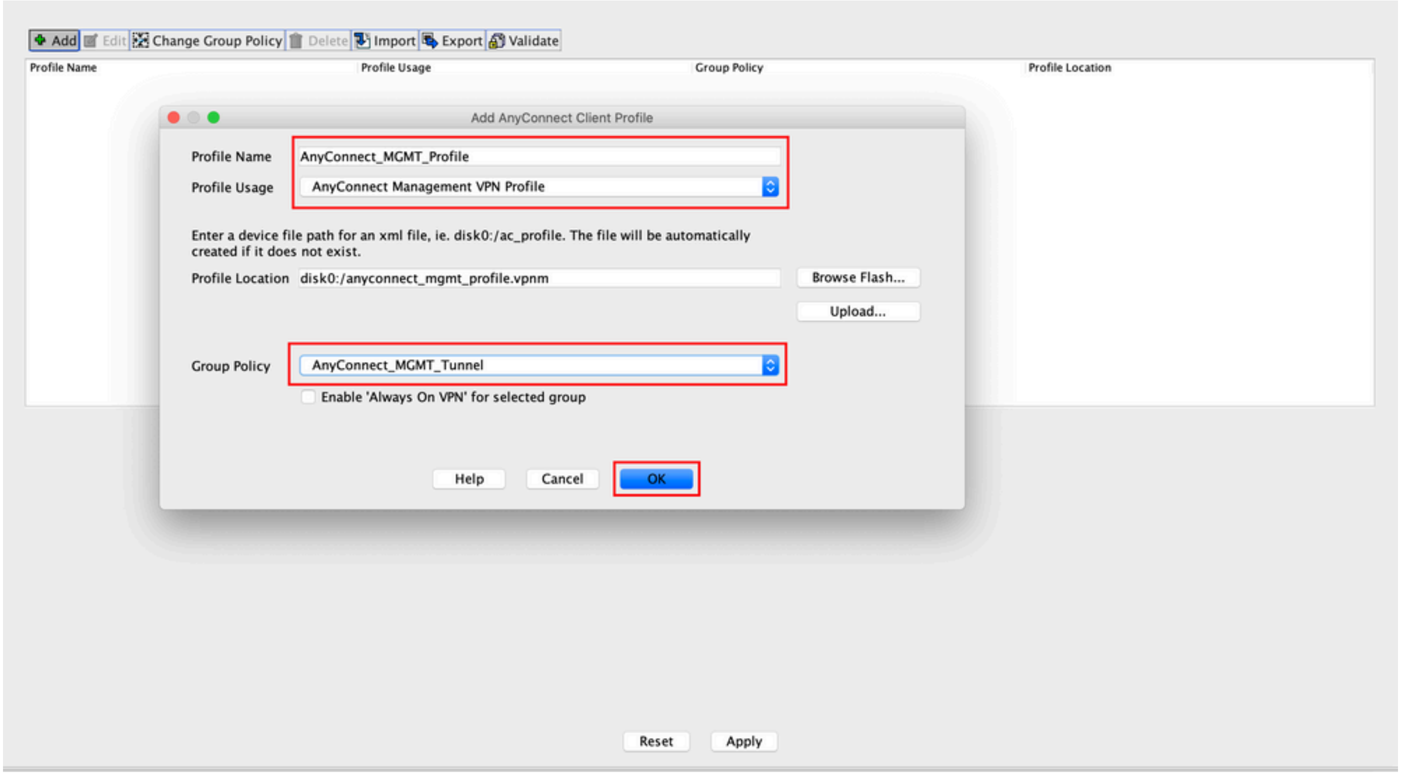


Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
HostScan configuration can be performed by going to Secure Desktop Manager/HostScan. If 'HostScan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Profile Name	Profile Usage	Group Policy	Profile Location

步驟2.提供 Profile Name.選擇 Profile Usage 作為 AnyConnect Management VPN profile.選擇 Group Policy 在步驟1中建立。按一下 OK 中，如圖所示。



Profile Name: AnyConnect_MGMT_Profile

Profile Usage: AnyConnect Management VPN Profile

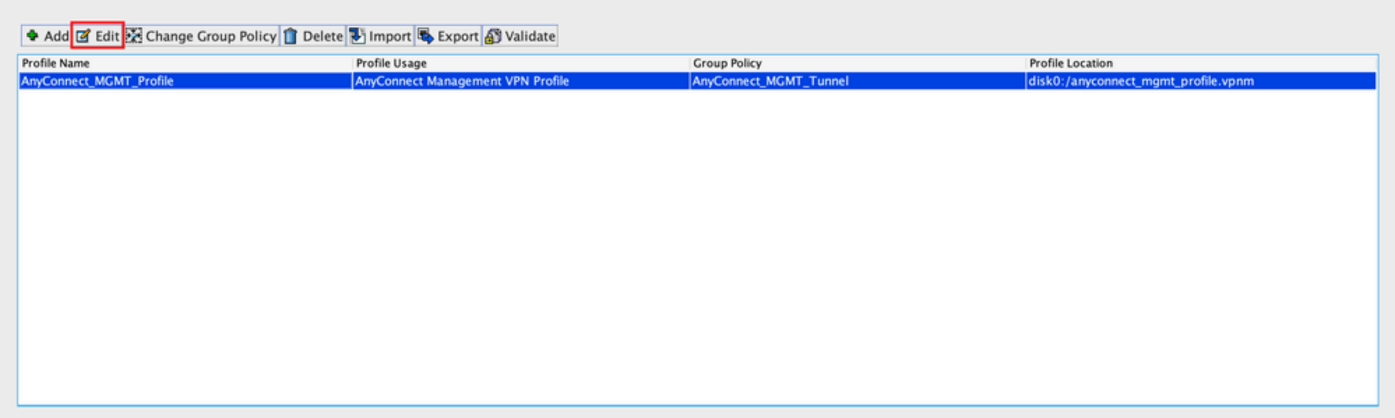
Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/anyconnect_mgmt_profile.vpnm

Group Policy: AnyConnect_MGMT_Tunnel

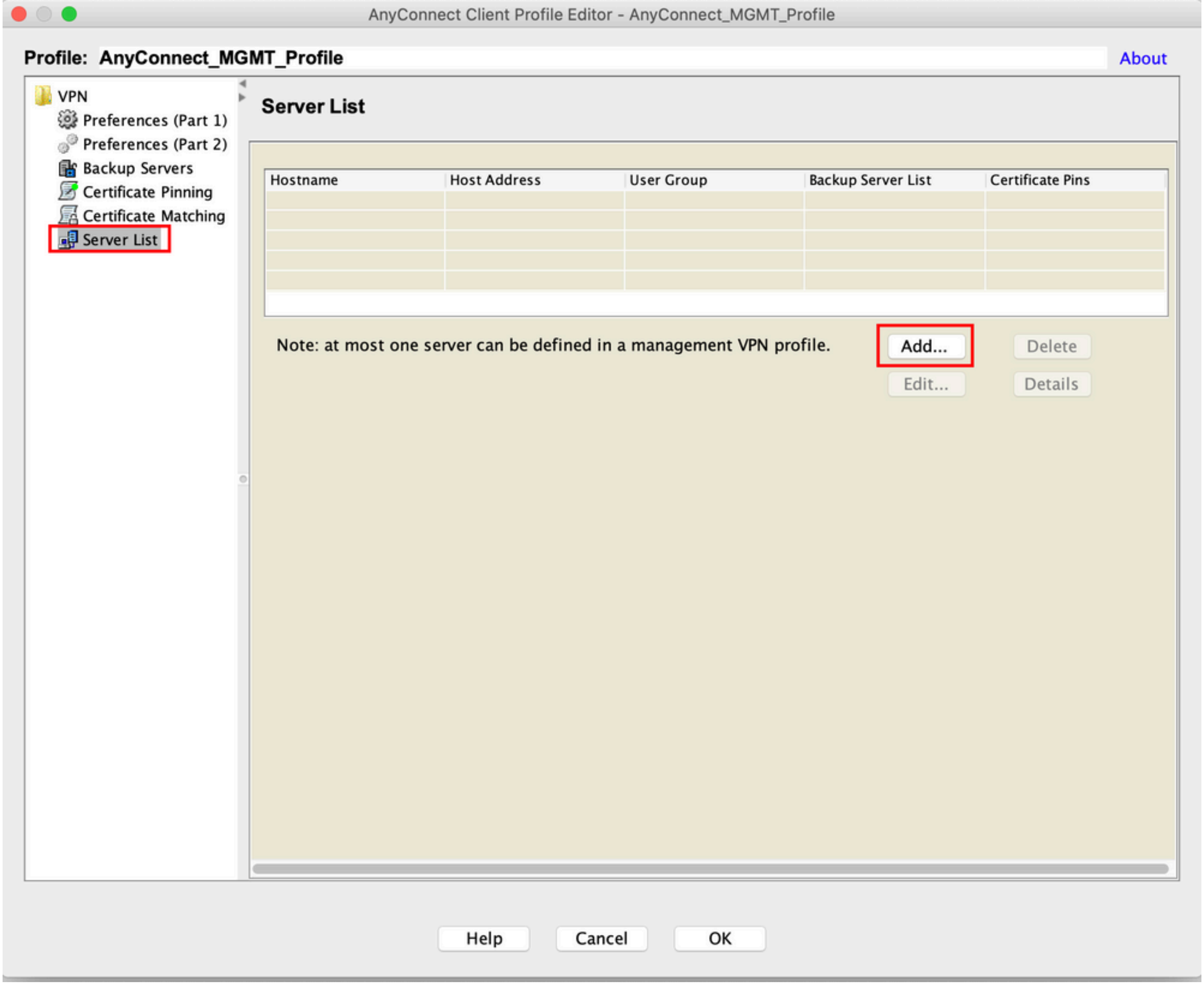
□ Enable 'Always On VPN' for selected group

步驟3.選擇建立的配置檔案，然後按一下 Edit中，如圖所示。



Profile Name	Profile Usage	Group Policy	Profile Location
AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

步驟4.導航至 Server List.按一下 Add 以新增新的伺服器清單條目，如下圖所示。



AnyConnect Client Profile Editor - AnyConnect_MGMT_Profile

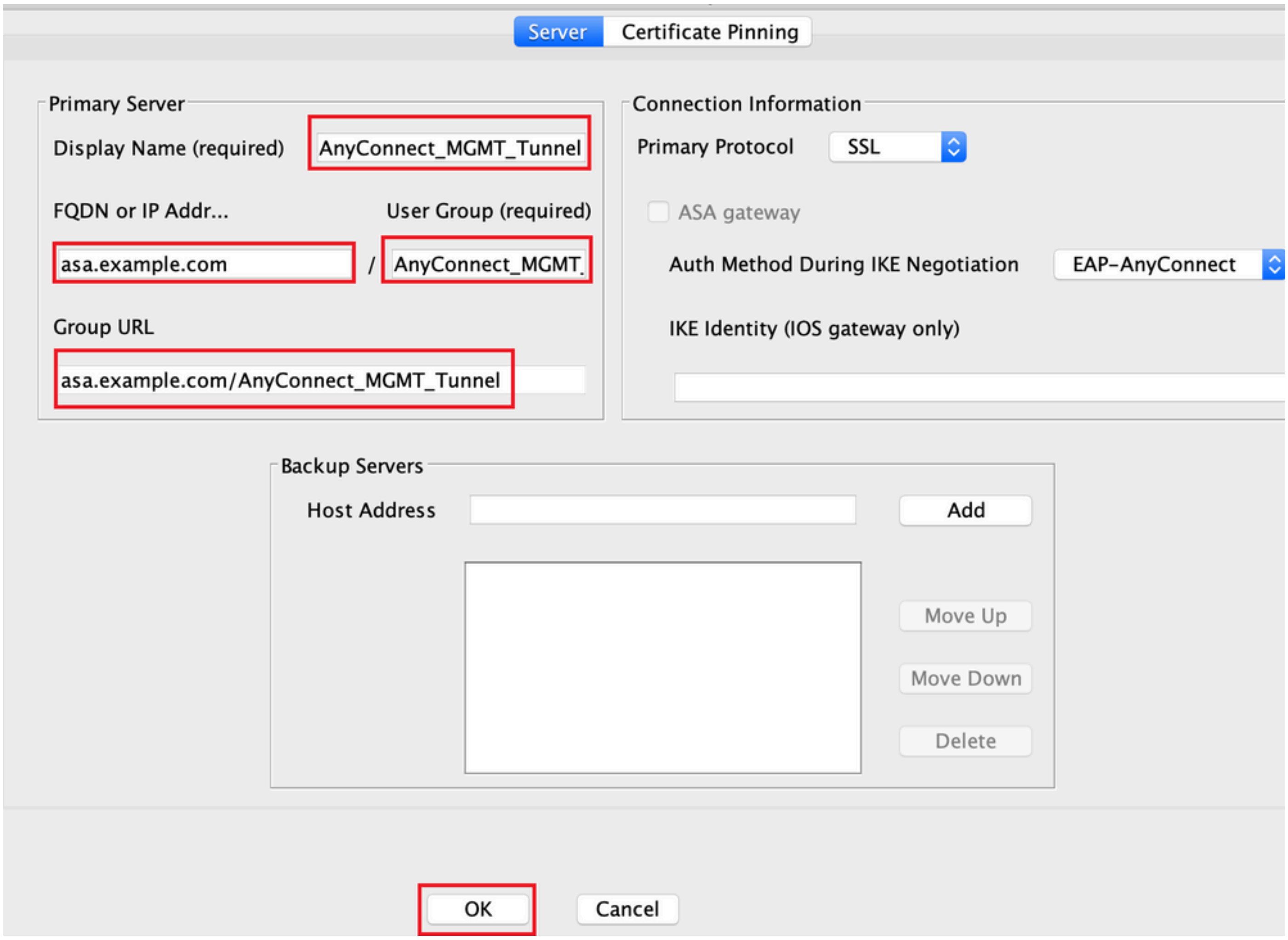
Profile: AnyConnect_MGMT_Profile

Server List

Hostname	Host Address	User Group	Backup Server List	Certificate Pins

Note: at most one server can be defined in a management VPN profile.

步驟5.提供 Display Name.新增 FQDN/IP address ASA的。提供 User Group 作為隧道組名稱。 Group URL 自動填入 FQDN 和 User Group.按一下 OK.



Primary Server

Display Name (required): AnyConnect_MGMT_Tunnel

FQDN or IP Addr...: asa.example.com / User Group (required): AnyConnect_MGMT_

Group URL: asa.example.com/AnyConnect_MGMT_Tunnel

Connection Information

Primary Protocol: SSL

□ ASA gateway

Auth Method During IKE Negotiation: EAP-AnyConnect

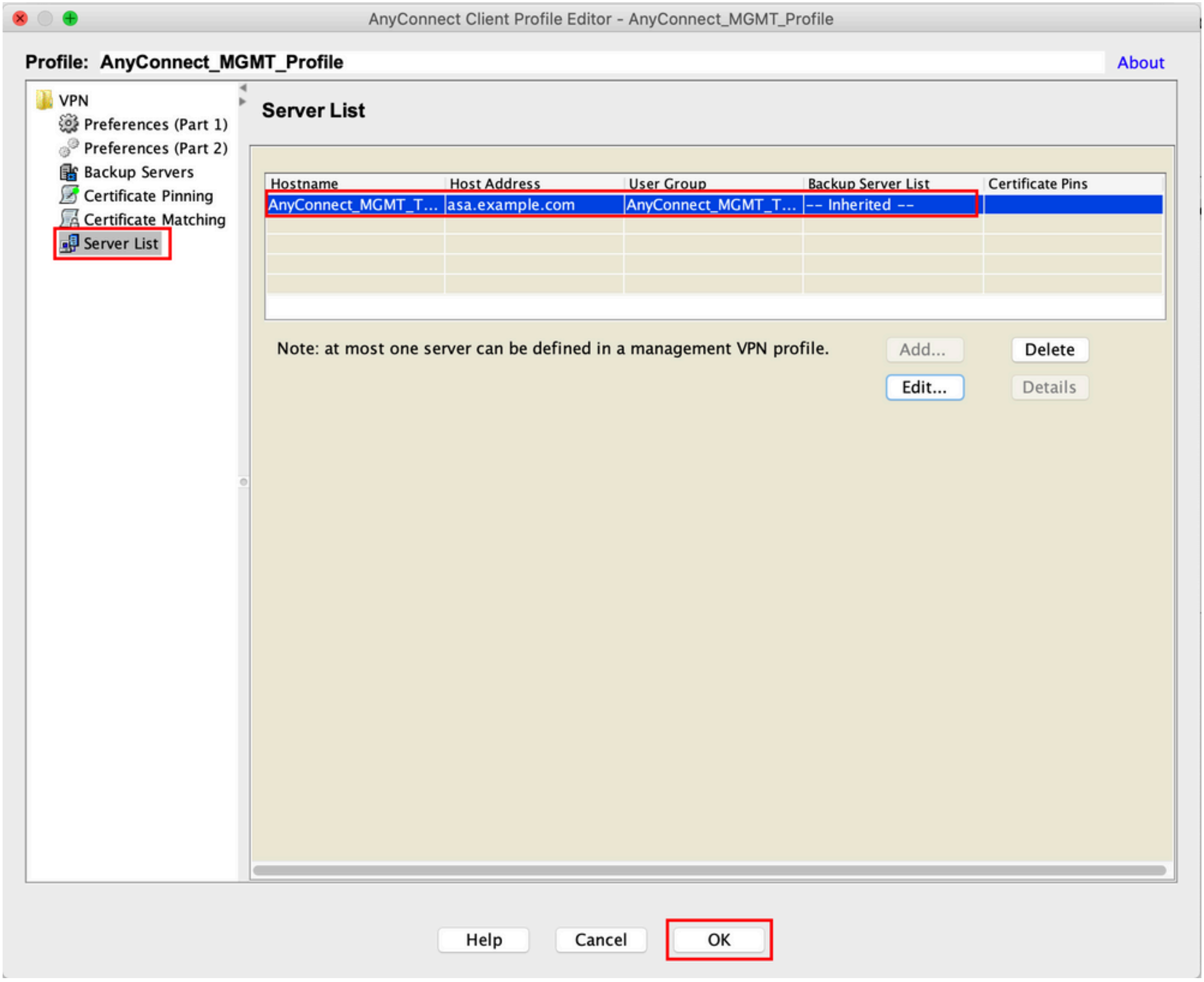
IKE Identity (IOS gateway only)

Host Address

注意：FQDN/IP地址+使用者組必須與步驟8中配置AnyConnect連線配置檔案時提到的組URL相同。

注意：將IKEv2作為協定的AnyConnect也可用於建立到ASA的管理VPN。確保 Primary Protocol 設定為 IPsec 在步驟5中。

步驟6.如圖所示，按一下 OK 儲存。



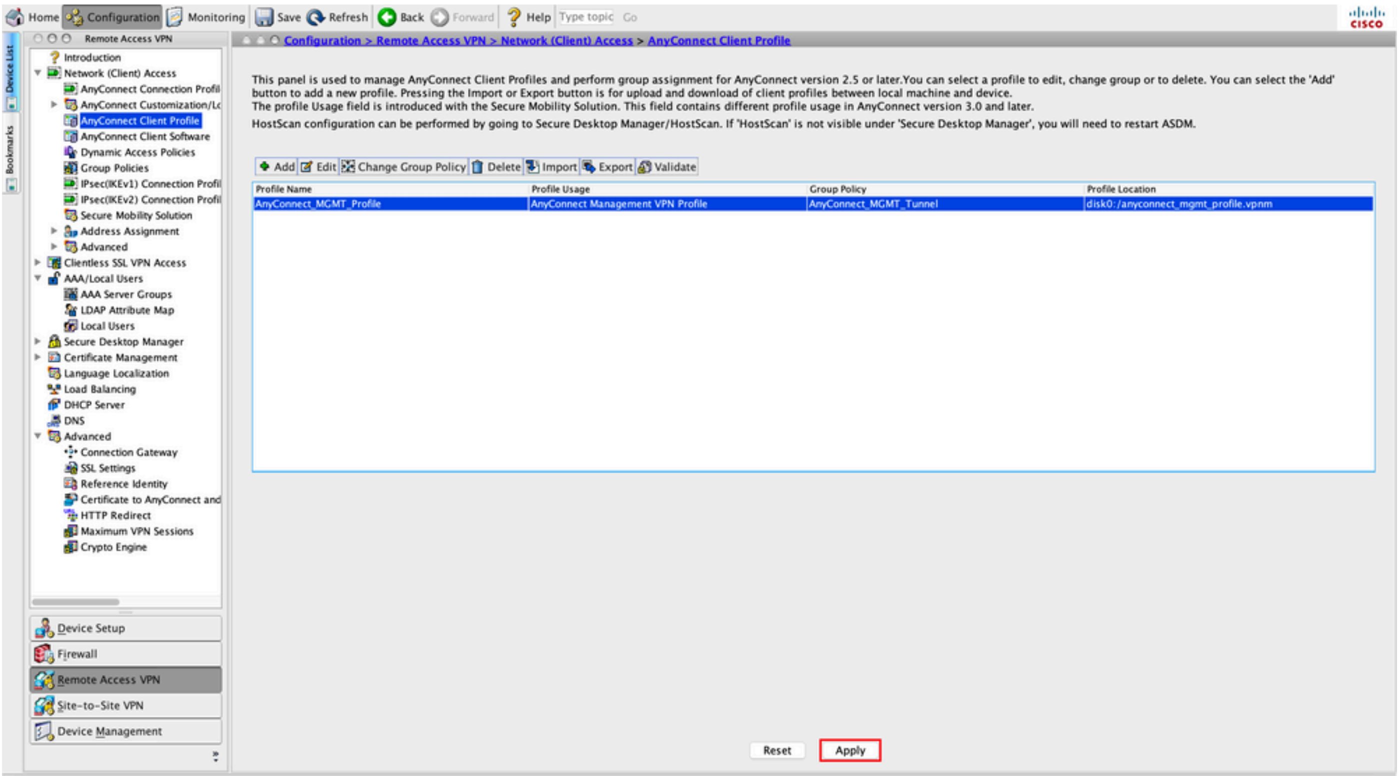
Profile: AnyConnect_MGMT_Profile

Server List

Hostname	Host Address	User Group	Backup Server List	Certificate Pins
AnyConnect_MGMT_T...	asa.example.com	AnyConnect_MGMT_T...	-- Inherited --	

Note: at most one server can be defined in a management VPN profile.

步驟7.按一下 Apply t將配置推送到ASA，如圖所示。



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
HostScan configuration can be performed by going to Secure Desktop Manager/HostScan. If 'HostScan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Profile Name	Profile Usage	Group Policy	Profile Location
AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

新增AnyConnect管理VPN配置檔案後的CLI配置。

```
webvpn
 enable outside
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

AnyConnect客戶端電腦上的AnyConnect管理VPN配置檔案：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>

       <ShowPreConnectMessage>false</ShowPreConnectMessage>

       <ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

```
</AnyConnectProfile>
```

注意：如果使用者AnyConnect VPN配置檔案中使用了受信任網路檢測(TND)，則建議匹配管理VPN配置檔案中的相同設定，以獲得一致的使用者體驗。根據應用到使用者VPN隧道配置檔案的TND設定觸發管理VPN隧道。 此外，管理VPN配置檔案中的TND連線操作（僅在管理VPN隧道處於活動狀態時實施）始終應用於使用者VPN隧道，以確保管理VPN隧道對終端使用者透明。

注意：在任何最終用戶PC上，如果管理VPN配置檔案啟用了TND設定，且使用者VPN配置檔案缺失，則它會考慮TND的預設首選項設定（在AC客戶端應用程式中的預設首選項中禁用了該設定）來代替缺失的使用者VPN配置檔案。這種不匹配可能會導致意外/未定義的行為。
預設情況下，在預設首選項中禁用TND設定。
要克服AnyConnect客戶端應用程式中的預設首選項硬編碼設定，終端使用者PC必須擁有兩個VPN配置檔案，一個使用者VPN配置檔案和一個交流管理VPN配置檔案，並且兩者必須具有相同的TND設定。
管理VPN隧道連線和斷開背後的邏輯是，為了建立管理VPN隧道，AC代理使用使用者VPN配置檔案TND設定，而對於管理VPN隧道的斷開，它將檢查管理VPN配置檔案TND設定。

AnyConnect管理VPN配置檔案的部署方法

- 使用ASA連線配置檔案成功完成使用者VPN連線，以便從VPN網關下載AnyConnect管理VPN配置檔案。

  注意：如果用於管理VPN隧道的協定是IKEv2，則需要通過SSL建立第一個連線（為了從ASA下載AnyConnect管理VPN配置檔案）。

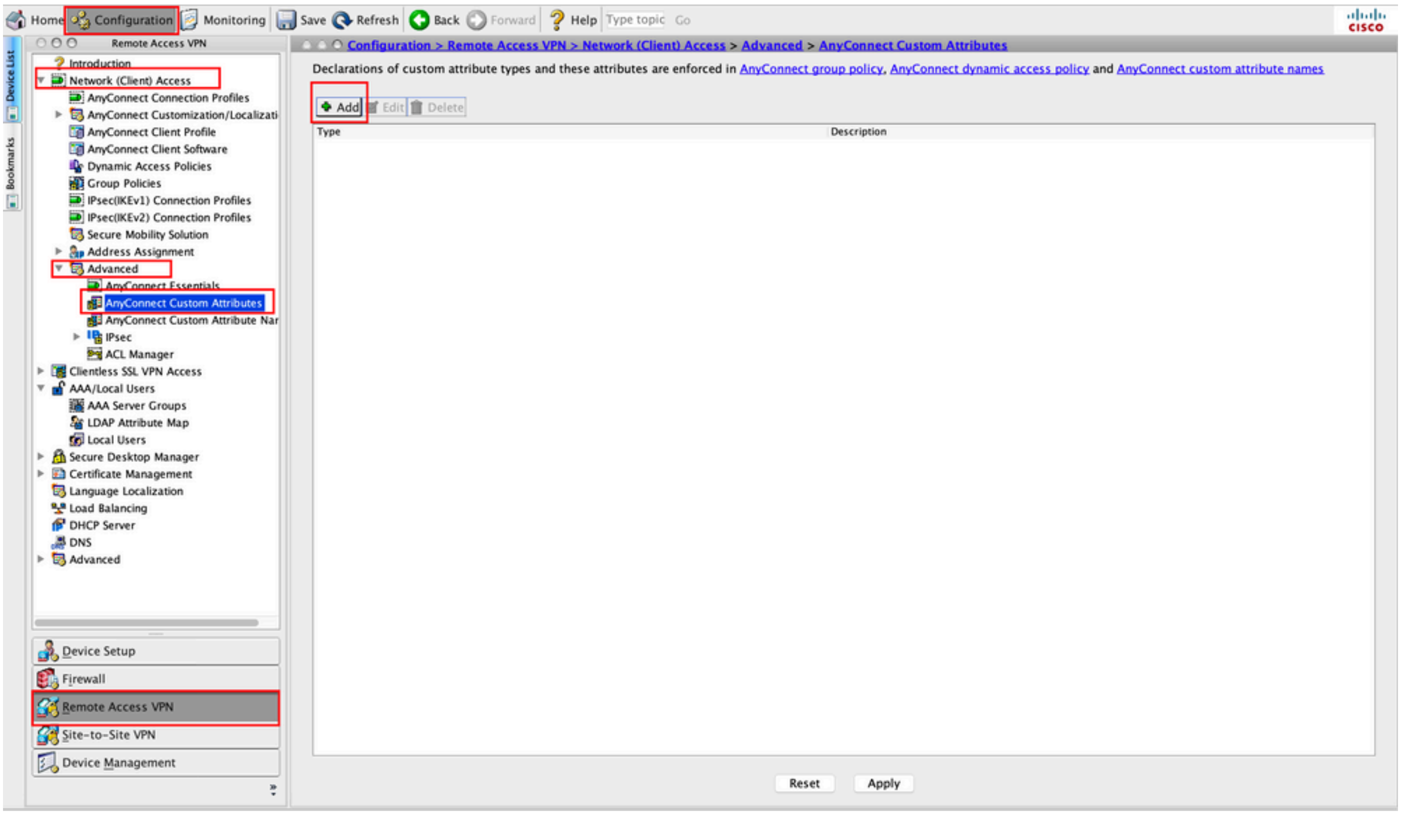
- AnyConnect管理VPN配置檔案可以通過GPO推送或手動安裝手動上傳到客戶端電腦(確保配置檔名稱為 VpnMgmtTunProfile.xml)。

  需要新增配置檔案的資料夾位置：
  Windows: **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**
  macOS: /opt/cisco/anyconnect/profile/mgmttun/

（可選）配置自定義屬性以支援全隧道配置

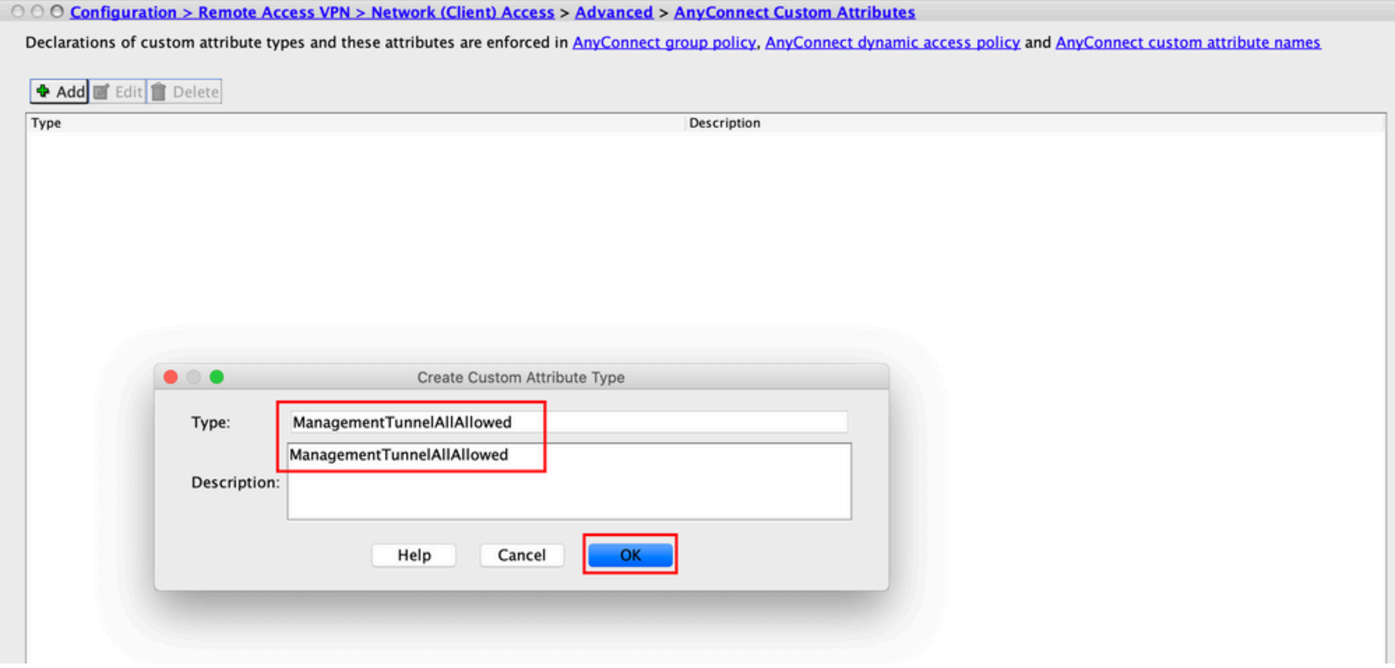
預設情況下，管理VPN隧道需要包括隧道配置的拆分，以避免對使用者發起的網路通訊產生影響。在管理隧道連線使用的組策略中配置自定義屬性時，可以覆蓋此屬性。

步驟1.導航至Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. 按一下 Add中，如圖所示。



Declarations of custom attribute types and these attributes are enforced in AnyConnect group policy, AnyConnect dynamic access policy and AnyConnect custom attribute names

步驟2.將自定義屬性Type設定為 ManagementTunnelAllAllowed 並提供 Description. 按一下 OK中，如圖所示。

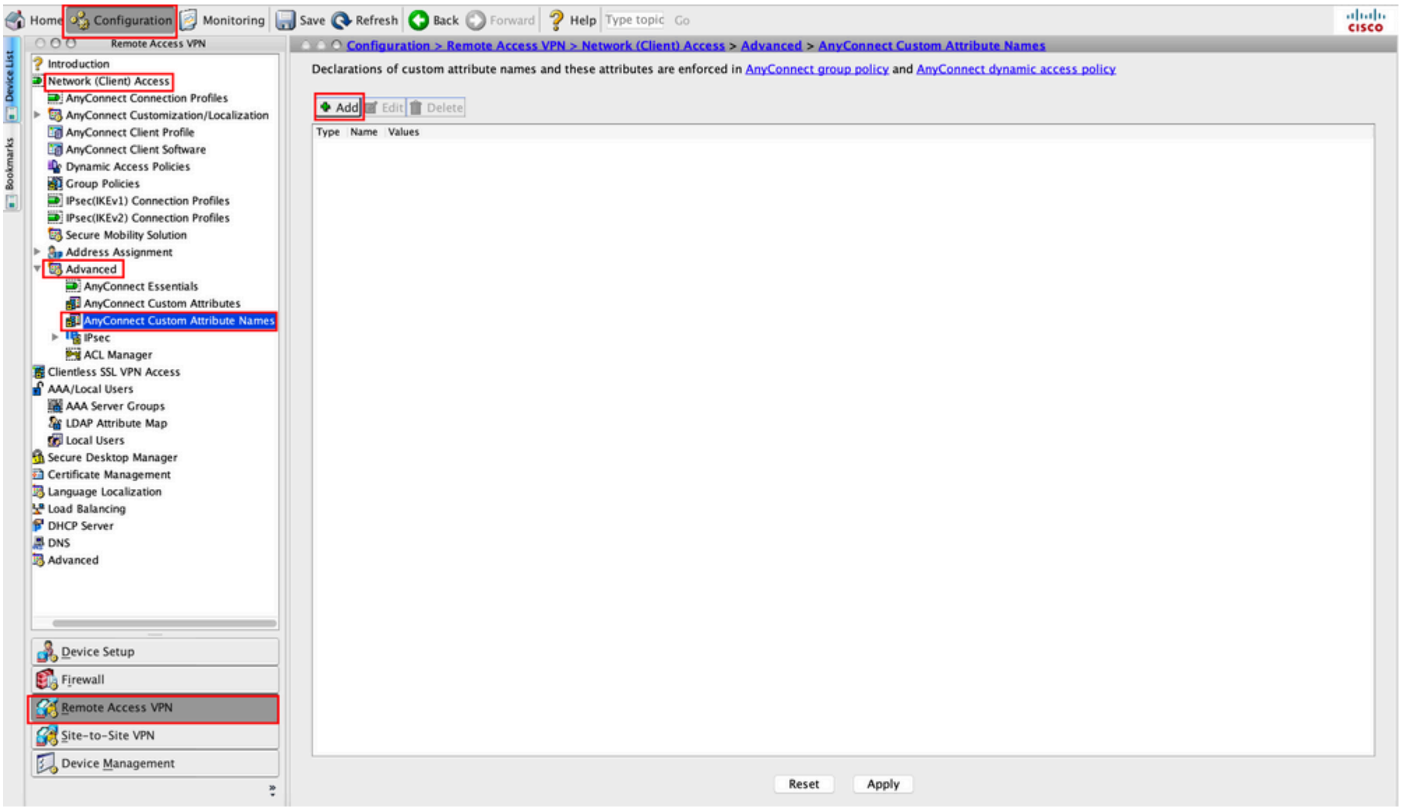

Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes
Add
Edit
Delete
Type
Description
Create Custom Attribute Type
Help
Cancel
OK

Declarations of custom attribute types and these attributes are enforced in AnyConnect group policy, AnyConnect dynamic access policy and AnyConnect custom attribute names

Type: ManagementTunnelAllAllowed

Description: ManagementTunnelAllAllowed

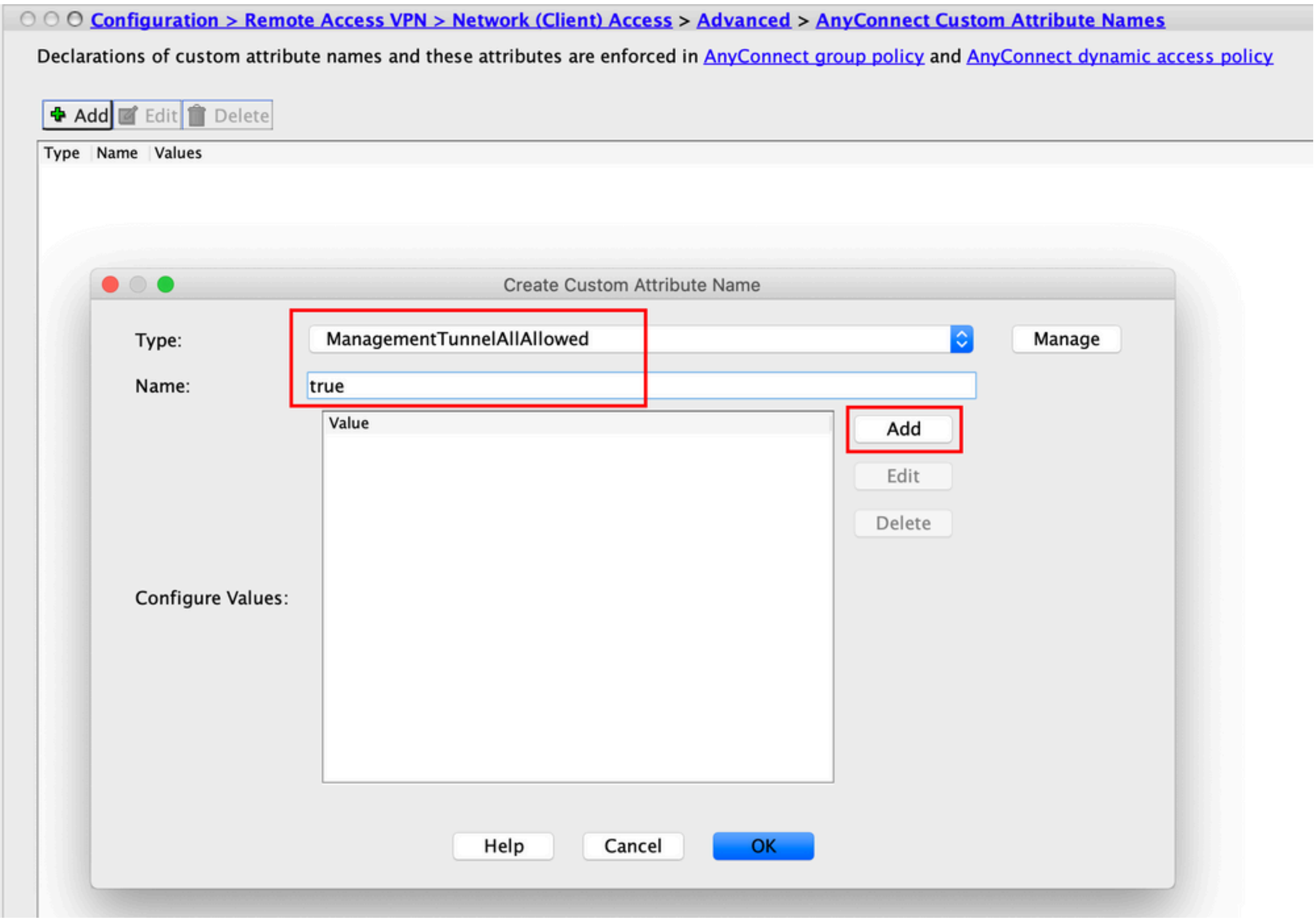
步驟3. 導航至 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. 按一下 Add中，如圖所示。



Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names

Declarations of custom attribute names and these attributes are enforced in AnyConnect group policy and AnyConnect dynamic access policy

步驟4.選擇型別作為 ManagementTunnelAllAllowed．將名稱設定為 true.按一下 Add提供自定義屬性值，如圖所示。



Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names

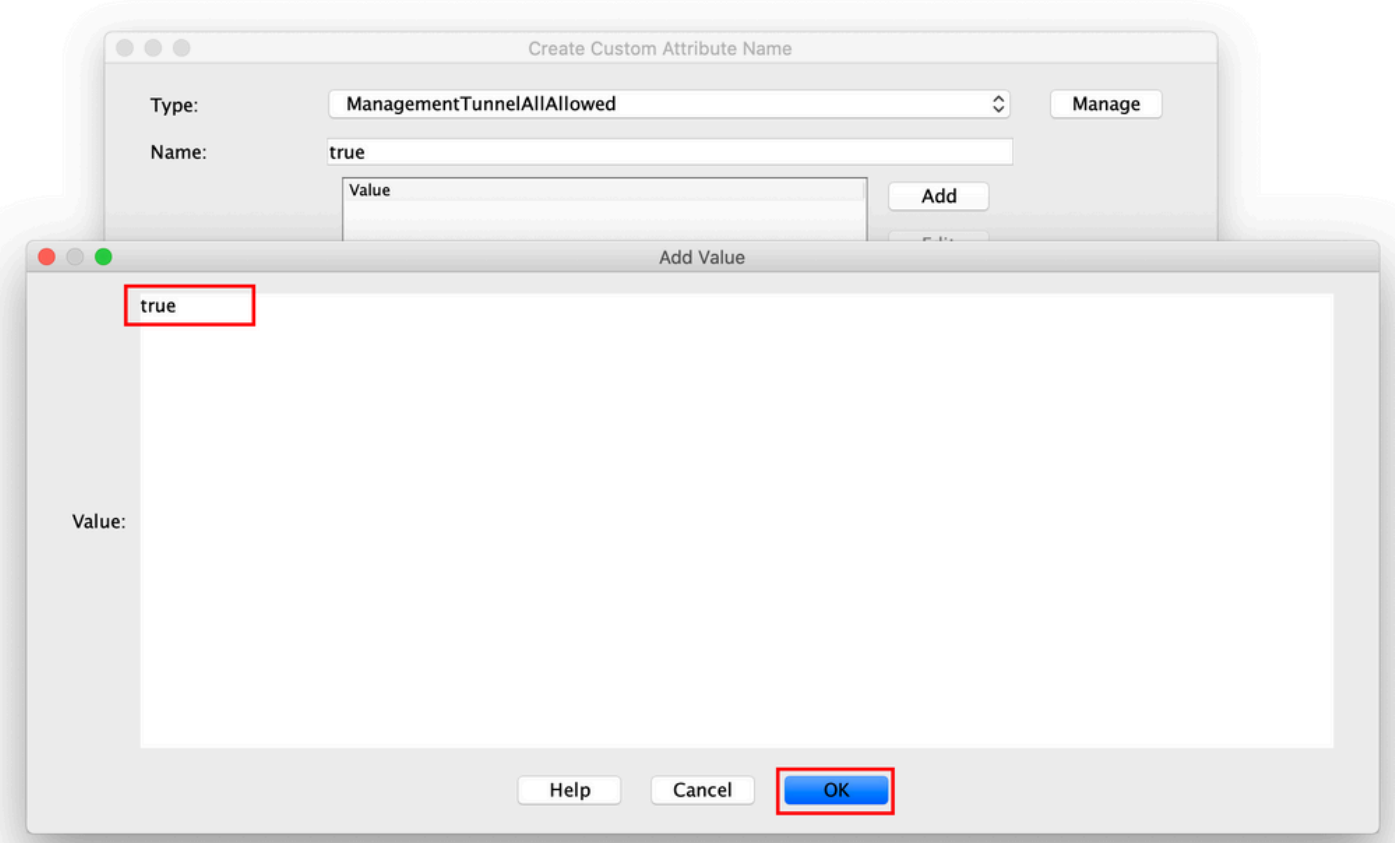
Declarations of custom attribute names and these attributes are enforced in AnyConnect group policy and AnyConnect dynamic access policy

Type: ManagementTunnelAllAllowed

Name: true

Configure Values:

步驟5.將值設定為 true.按一下 OK中，如圖所示。

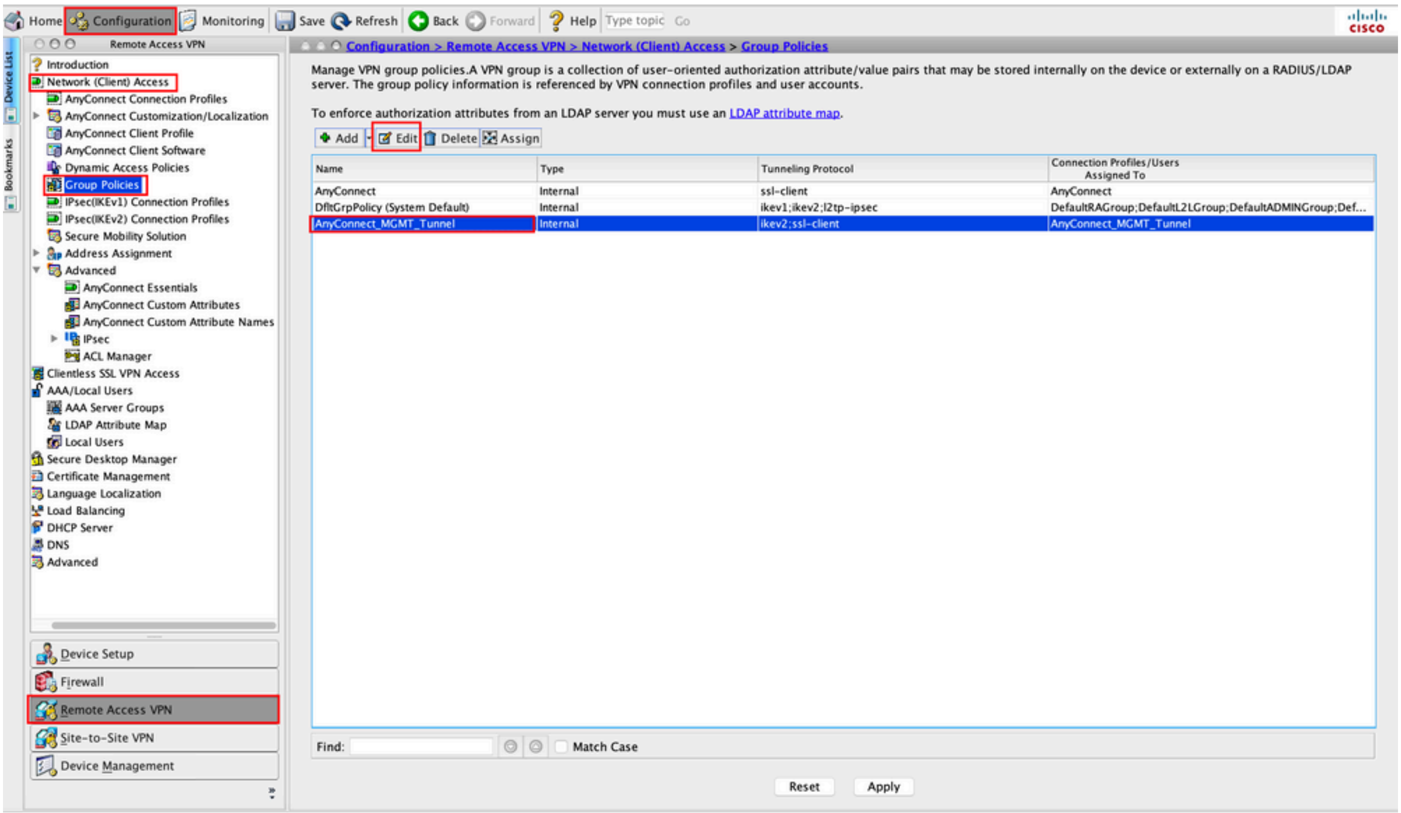


Type: ManagementTunnelAllAllowed

Name: true

Value: true

步驟6.導航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.選擇組策略。 按一下 Edit 中，如圖所示。



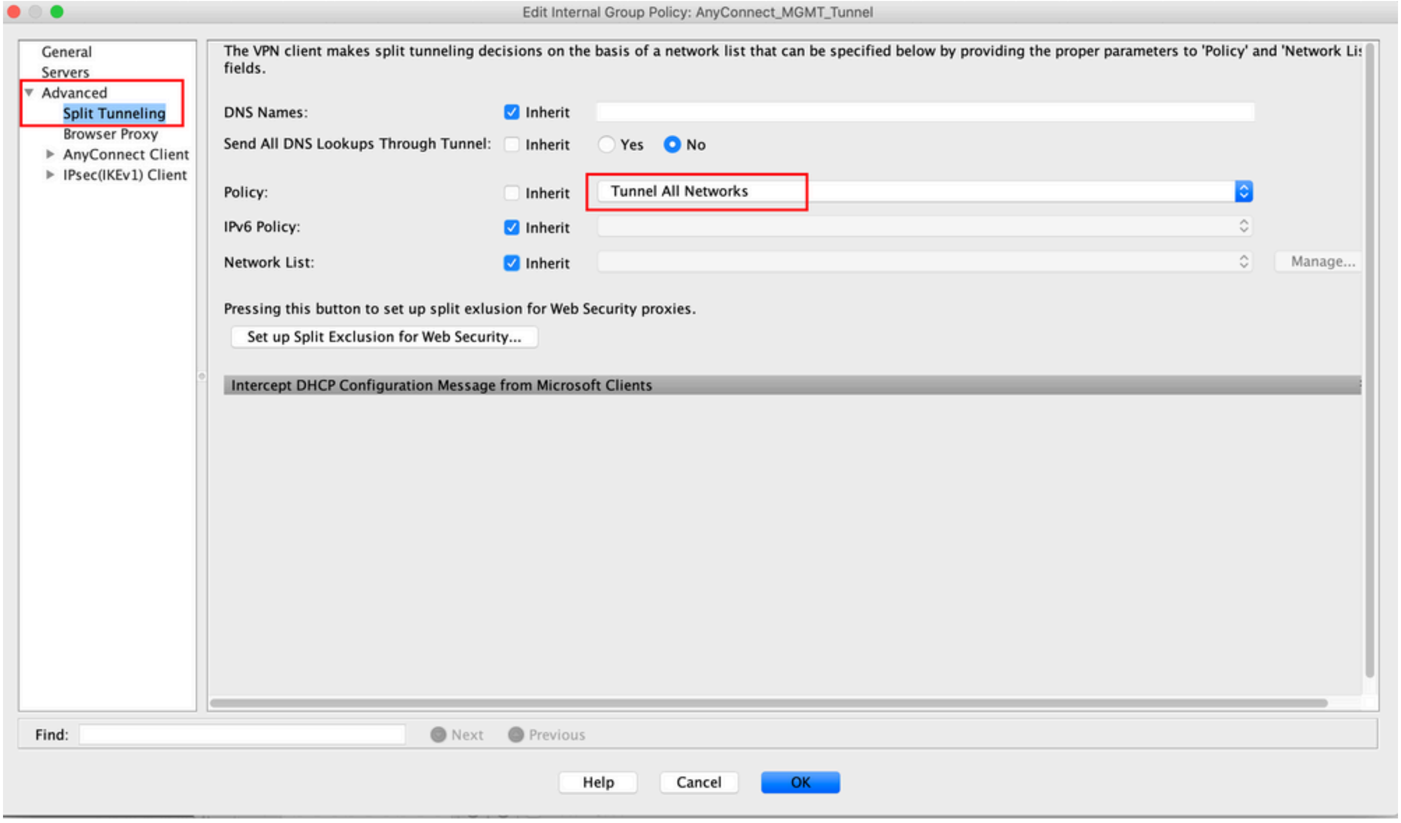
Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...
AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel

步驟7.如圖所示，導覽至 Advanced > Split Tunneling.將策略配置為 Tunnel All Networks.



The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network Li: fields.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: □ Inherit ○ Yes ● No

Policy: □ Inherit Tunnel All Networks

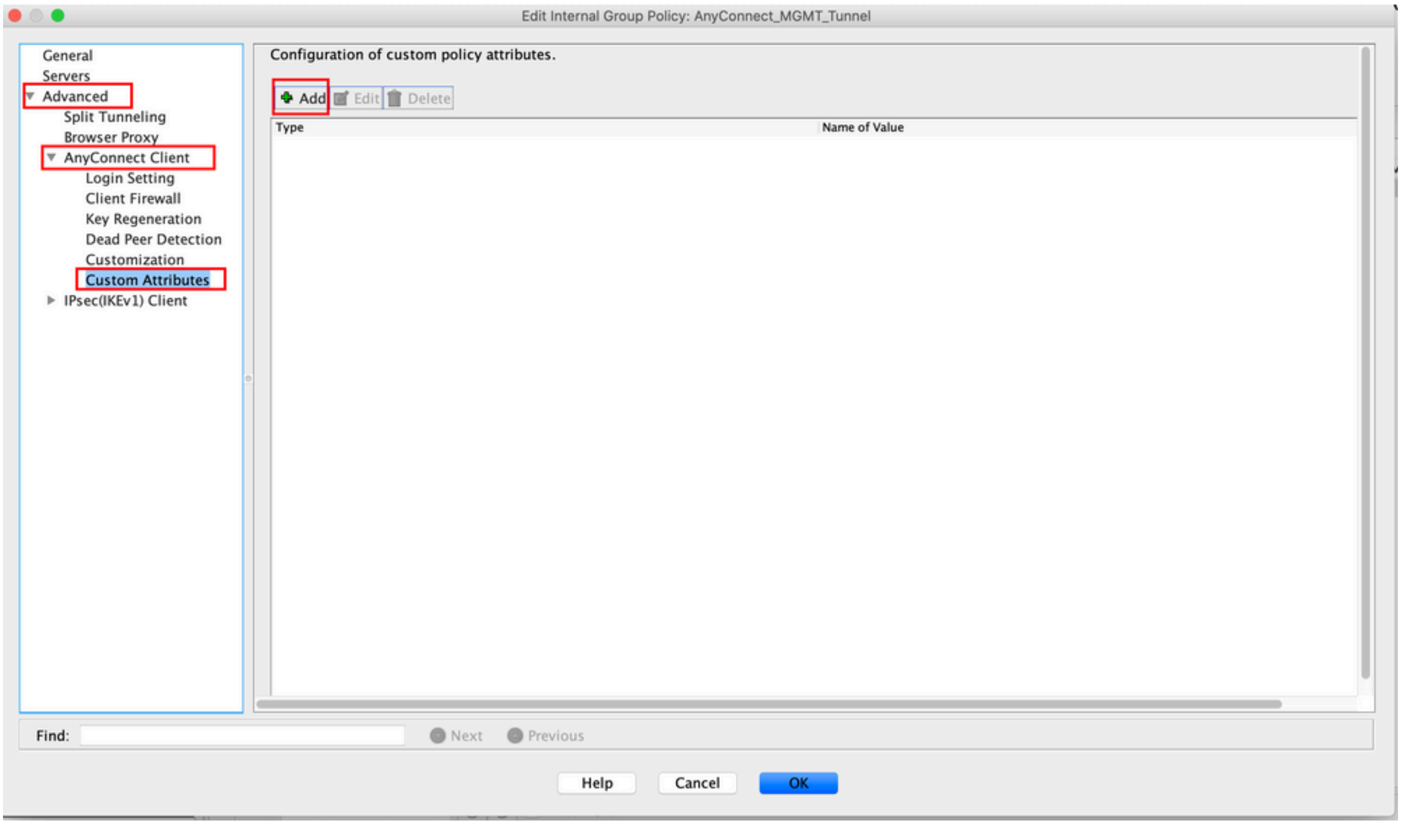
IPv6 Policy: ☑ Inherit

Network List: ☑ Inherit

Pressing this button to set up split exlusion for Web Security proxies.

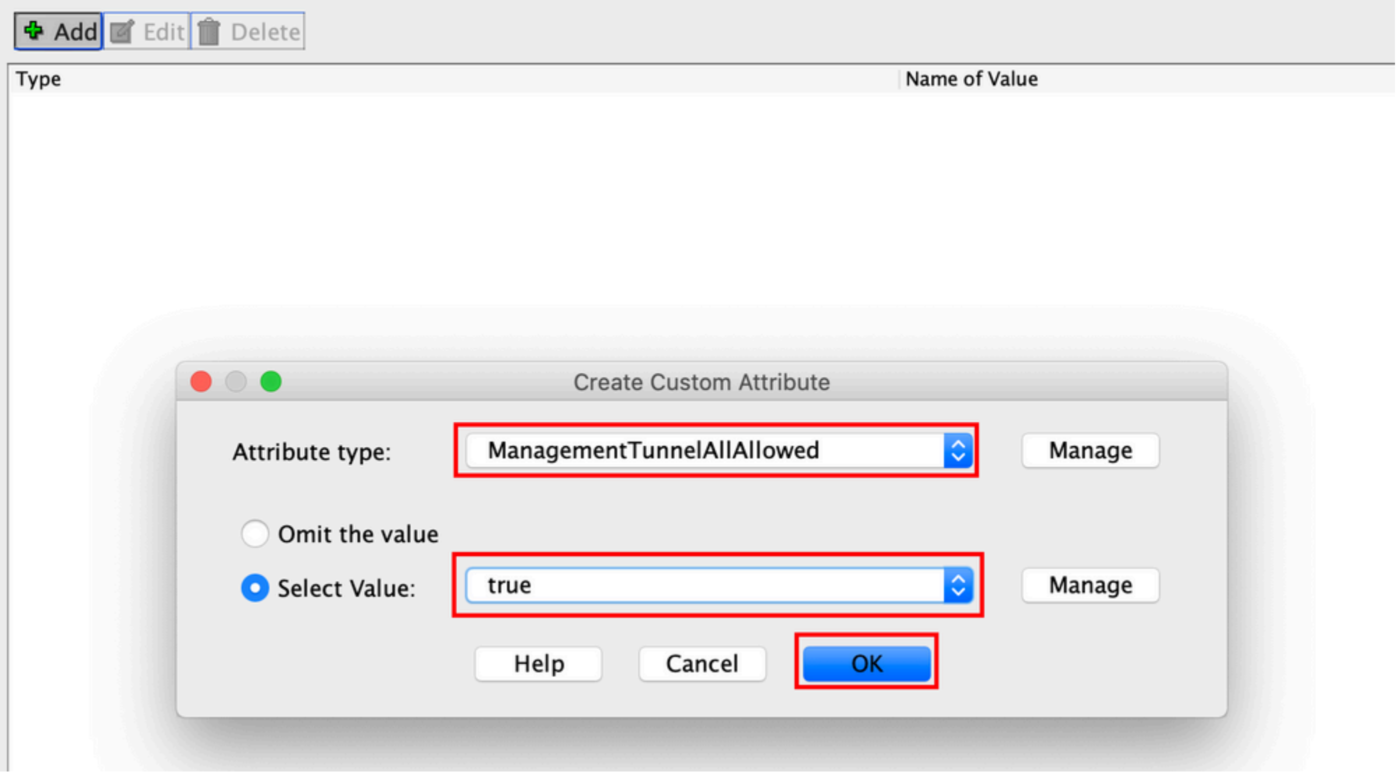
Intercept DHCP Configuration Message from Microsoft Clients

步驟8.導航至 Advanced > Anyconnect Client > Custom Attributes.按一下 Add中，如圖所示。



Configuration of custom policy attributes.

步驟9. 選擇屬性型別作為 ManagementTunnelAllAllowed 並選擇值作為 true.按一下 OK中，如圖所示。

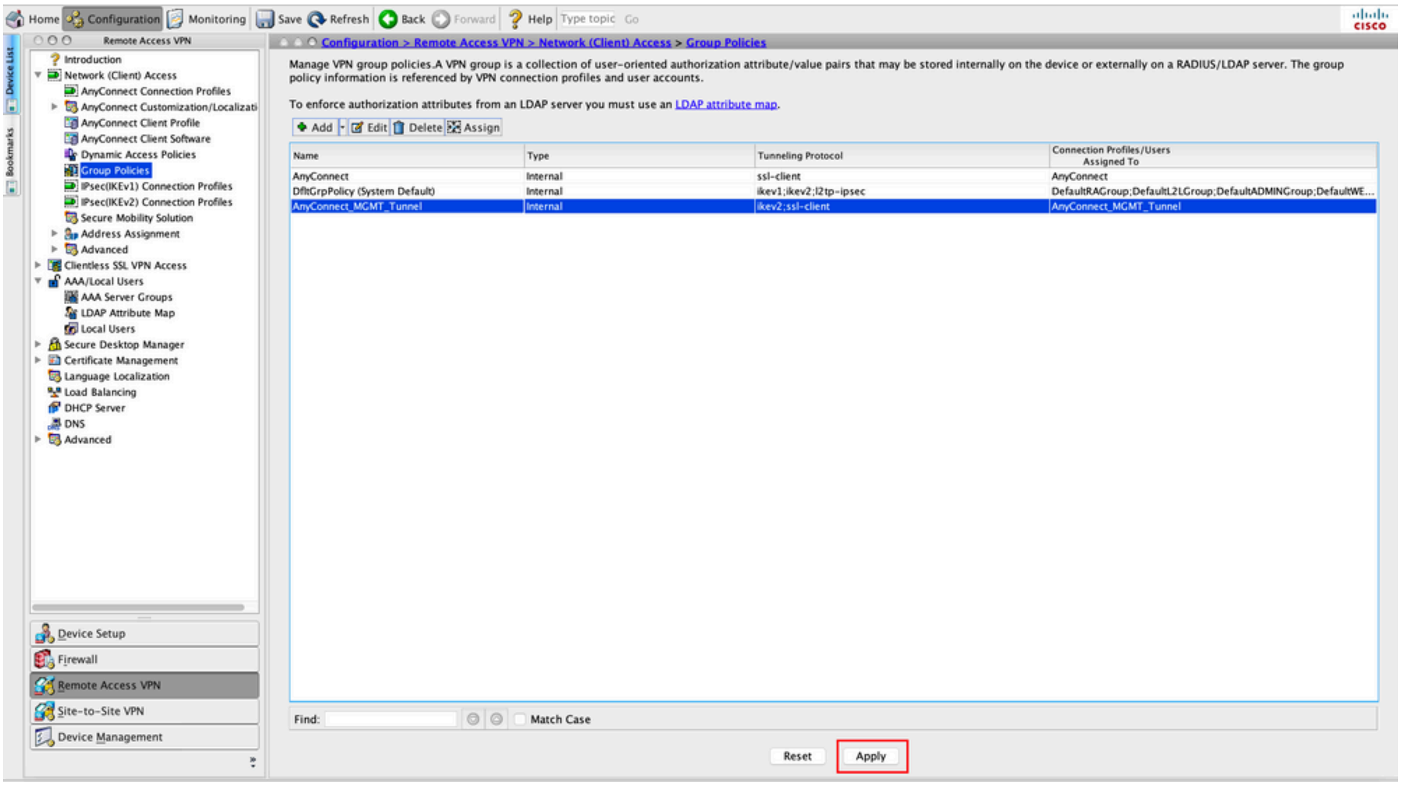


Attribute type: ManagementTunnelAllAllowed

○ Omit the value

● Select Value: true

步驟10.按一下 Apply 將配置推送到ASA，如圖所示。



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
AnyConnect	Internal	ssl-client	AnyConnect
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE...
AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel

CLI配置 ManagementTunnelAllAllowed 新增自定義屬性：

```
webvpn
 enable outside
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
anyconnect-custom-data ManagementTunnelAllAllowed true true
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelall
 client-bypass-protocol enable
 address-pools value VPN_Pool
 anyconnect-custom ManagementTunnelAllAllowed value true
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

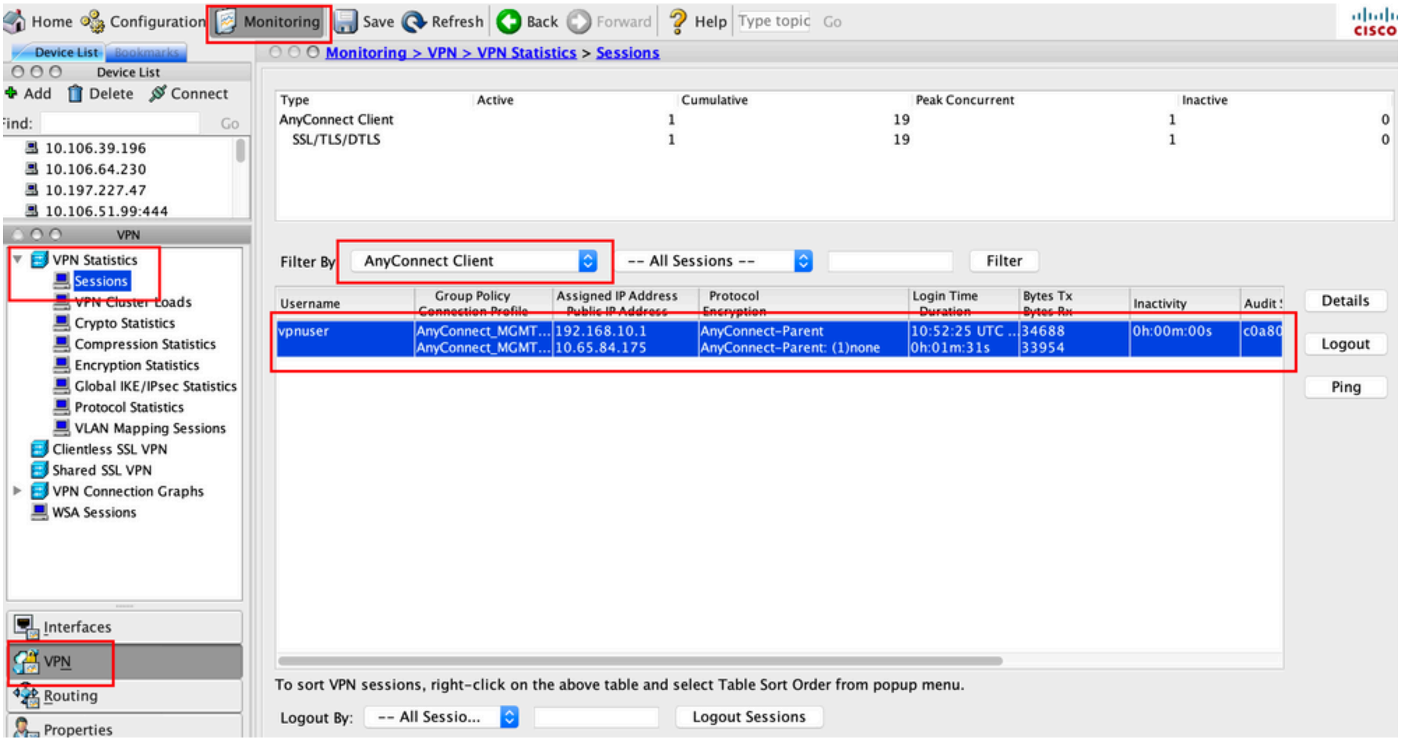
驗證

使用CLI驗證管理VPN隧道連線 show vpn-sessiondb detail anyconnect 指令。

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : vpnuser                Index        : 10
Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-
256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 17238                  Bytes Rx     : 1988
Pkts Tx      : 12                     Pkts Rx      : 13
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time   : 01:23:55 UTC Tue Apr 14 2020
Duration     : 0h:11m:36s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

--- Output Omitted ---
DTLS-Tunnel:
  Tunnel ID    : 10.3
  Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2               UDP Src Port : 57053
  UDP Dst Port : 443                         Auth Mode     : Certificate
  Idle Time Out: 30 Minutes                  Idle TO Left : 18 Minutes
  Client OS     : Windows
  Client Type   : DTLS VPN Client
  Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.8.03036
  Bytes Tx      : 17238                          Bytes Rx      : 1988
  Pkts Tx       : 12                             Pkts Rx       : 13
  Pkts Tx Drop : 0                               Pkts Rx Drop : 0
```

驗證ASDM上的管理VPN隧道連線。

導航到**Monitoring > VPN > VPN Statistics > Sessions**。按**AnyConnect Client**過濾以檢視客戶端會話。



Type	Active	Cumulative	Peak Concurrent	Inactive
AnyConnect Client	1	19	1	0
SSL/TLS/DTLS	1	19	1	0

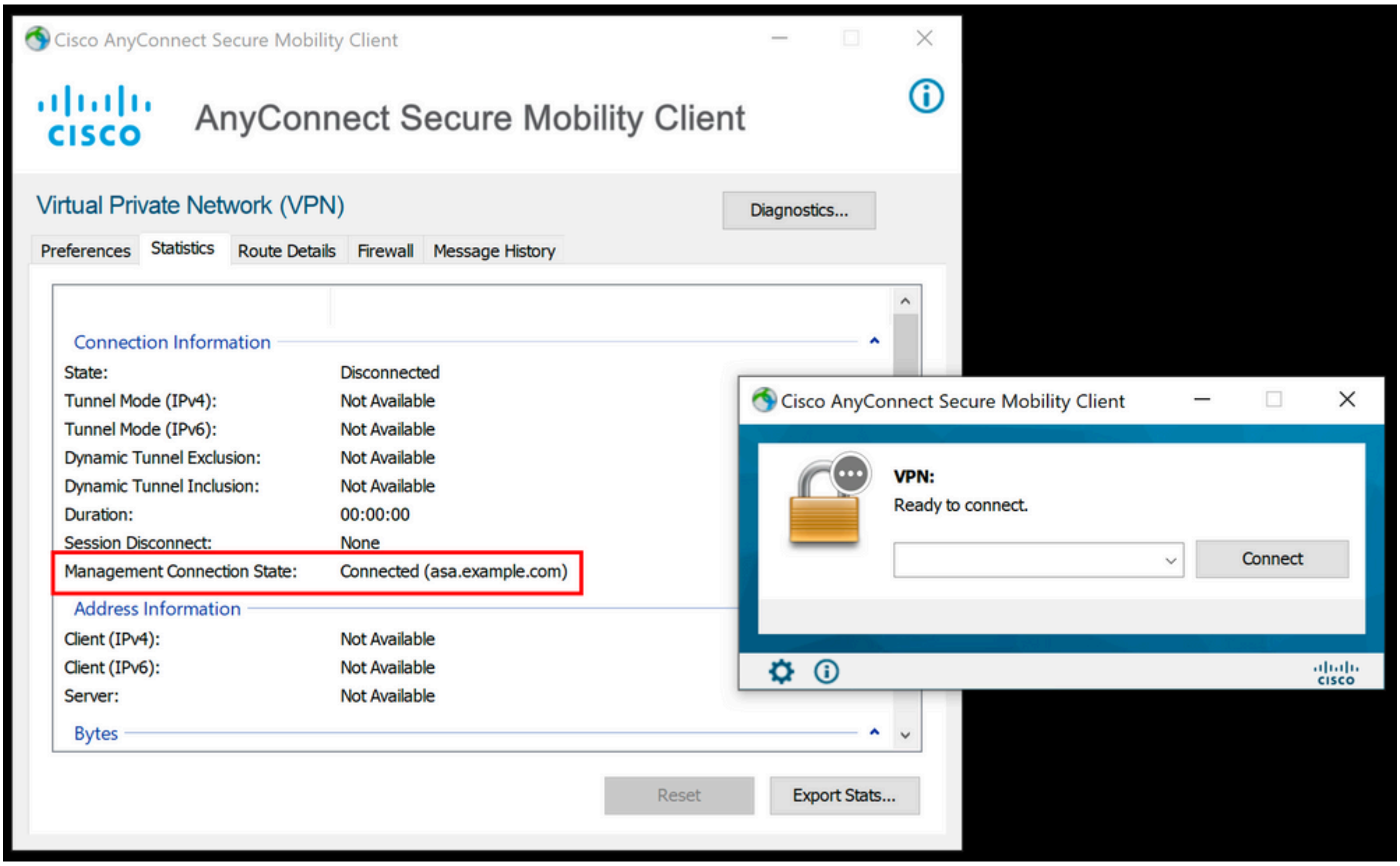
Filter By: AnyConnect Client | -- All Sessions -- | Filter

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Inactivity	Audit :
vpnuser	AnyConnect_MGMT... AnyConnect_MGMT...	192.168.10.1 10.65.84.175	AnyConnect-Parent AnyConnect-Parent: (1)none	10:52:25 UTC ... 0h:01m:31s	34688 33954	0h:00m:00s	c0a80

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessio... | Logout Sessions

驗證客戶端電腦上的管理VPN隧道連線：



Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History

Connection Information

State: Disconnected
Tunnel Mode (IPv4): Not Available
Tunnel Mode (IPv6): Not Available
Dynamic Tunnel Exclusion: Not Available
Dynamic Tunnel Inclusion: Not Available
Duration: 00:00:00
Session Disconnect: None
Management Connection State: Connected (asa.example.com)

Address Information

Client (IPv4): Not Available
Client (IPv6): Not Available
Server: Not Available

Bytes

VPN:
Ready to connect.

疑難排解

新的UI統計資訊行（管理連線狀態）可用於排除管理隧道連線問題。以下是常見的錯誤狀態：

已斷開連線（禁用）：

- 功能已禁用。
- 確保通過使用者隧道連線（要求您將管理VPN配置檔案新增到使用者隧道組策略）或通過手動上傳配置檔案將管理VPN配置檔案部署到客戶端。
- 確保為管理VPN配置檔案配置了一個包含隧道組的單個主機條目。

已斷開連線（受信任網路）：

- TND檢測到受信任網路，因此未建立管理隧道。

已斷開連線（使用者隧道處於活動狀態）：

- 使用者VPN隧道當前處於活動狀態。

已斷開連線（進程啟動失敗）：

- 嘗試管理隧道連線時遇到進程啟動失敗。

已斷開連線（連線失敗）：

- 建立管理隧道時遇到連線故障。
- 確保在隧道組中配置證書身份驗證，組策略中不存在標語，並且伺服器證書必須受信任。

已斷開連線（無效的VPN配置）：

- 從VPN伺服器接收到無效的拆分隧道配置。
- 檢查管理隧道組策略中的拆分隧道配置。

已斷開連線（軟體更新掛起）：

- AnyConnect軟體更新當前掛起。

已斷開連線：

- 管理隧道即將建立或由於其他原因無法建立。

收集DART以進一步進行故障排除。

相關資訊

- 管理VPN隧道的配置
- 管理VPN隧道故障排除
- 技術支援與文件 - Cisco Systems

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）。