

# Configurazione del tunnel VPN di gestione di AnyConnect sull'ASA

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Funzionamento del tunnel di gestione](#)

[Limitazioni](#)

[Configurazione](#)

[Configurazione su ASA tramite ASDM/CLI](#)

[Creazione del profilo VPN di gestione di AnyConnect](#)

[Metodi di distribuzione per il profilo VPN di gestione di AnyConnect](#)

[\(Facoltativo\) Configurare un attributo personalizzato per supportare la configurazione tunnel-tutto](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare l'ASA in modo che il gateway VPN accetti le connessioni da AnyConnect Secure Mobility Client tramite il tunnel VPN di gestione.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:


- Configurazione VPN tramite Adaptive Security Device Manager (ASDM)
- Configurazione CLI ASA (Basic Adaptive Security Appliance)
- Certificati X509

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco ASA versione 9.12(3)9

- Software Cisco ASDM versione 7.12.2
- Windows 10 con Cisco AnyConnect Secure Mobility Client versione 4.8.03036

 **Nota:** scaricare il pacchetto AnyConnect VPN Web Deployment (`anyconnect-win*.pkg` or `anyconnect-macos*.pkg`) dal sito Cisco [Software Download](#) (solo utenti registrati). Copiare il client VPN AnyConnect nella memoria flash dell'ASA da scaricare sui computer degli utenti remoti per stabilire la connessione VPN SSL con l'ASA. Per ulteriori informazioni, consultare la sezione [Installazione del client AnyConnect](#) della guida alla configurazione delle appliance ASA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Un tunnel VPN di gestione assicura la connettività alla rete aziendale ogni volta che il sistema client viene acceso, non solo quando l'utente finale stabilisce una connessione VPN. È possibile eseguire la gestione delle patch sugli endpoint fuori sede, in particolare sui dispositivi che l'utente raramente connette alla rete aziendale tramite VPN. Questa funzionalità offre inoltre vantaggi agli script di accesso al sistema operativo degli endpoint che richiedono la connettività di rete aziendale.

AnyConnect Management Tunnel consente agli amministratori di connettere AnyConnect senza l'intervento dell'utente prima del momento in cui l'utente esegue l'accesso. Il tunnel di gestione di AnyConnect può funzionare insieme al rilevamento di reti attendibili e quindi viene attivato solo quando l'endpoint è fuori sede e disconnesso da una VPN avviata dall'utente. Il tunnel di gestione di AnyConnect è trasparente per l'utente finale e si disconnette automaticamente quando l'utente avvia la VPN.

SO/applicazione	Requisiti minimi di versione
ASA	9.0.1
ASDM	7.10.1
Versione di Windows AnyConnect	4.7.00136
Versione macOS AnyConnect	4.7.01076
Linux	Non supportato

## Funzionamento del tunnel di gestione

Il servizio agente VPN AnyConnect viene avviato automaticamente all'avvio del sistema. Rileva che la funzionalità tunnel di gestione è abilitata (tramite il profilo VPN di gestione), quindi avvia l'applicazione client di gestione per avviare una connessione tunnel di gestione. L'applicazione client di gestione utilizza la voce host del profilo VPN di gestione per avviare la connessione. Il

tunnel VPN viene quindi stabilito come di consueto, con una sola eccezione: non viene eseguito alcun aggiornamento software durante una connessione al tunnel di gestione, in quanto il tunnel di gestione deve essere trasparente per l'utente.

L'utente avvia un tunnel VPN tramite l'interfaccia utente di AnyConnect, che attiva la terminazione del tunnel di gestione. Dopo l'interruzione del tunnel di gestione, l'impostazione del tunnel utente continua normalmente.

L'utente disconnette il tunnel VPN, che attiva il ripristino automatico del tunnel di gestione.

## Limitazioni

- Interazione utente non supportata
- L'autenticazione basata su certificati tramite l'archivio certificati del computer (Windows) è supportata solo
- La verifica rigorosa dei certificati del server è applicata
- Un proxy privato non è supportato
- Un proxy pubblico non è supportato (il valore ProxyNative è supportato sulle piattaforme in cui le impostazioni Proxy nativo non vengono recuperate dal browser)
- Script di personalizzazione AnyConnect non supportati

---

 Nota: per ulteriori informazioni, fare riferimento a [Informazioni sul tunnel VPN di gestione](#).

---


## Configurazione

In questa sezione viene descritto come configurare Cisco ASA come gateway VPN per accettare le connessioni dai client AnyConnect tramite il tunnel VPN di gestione.

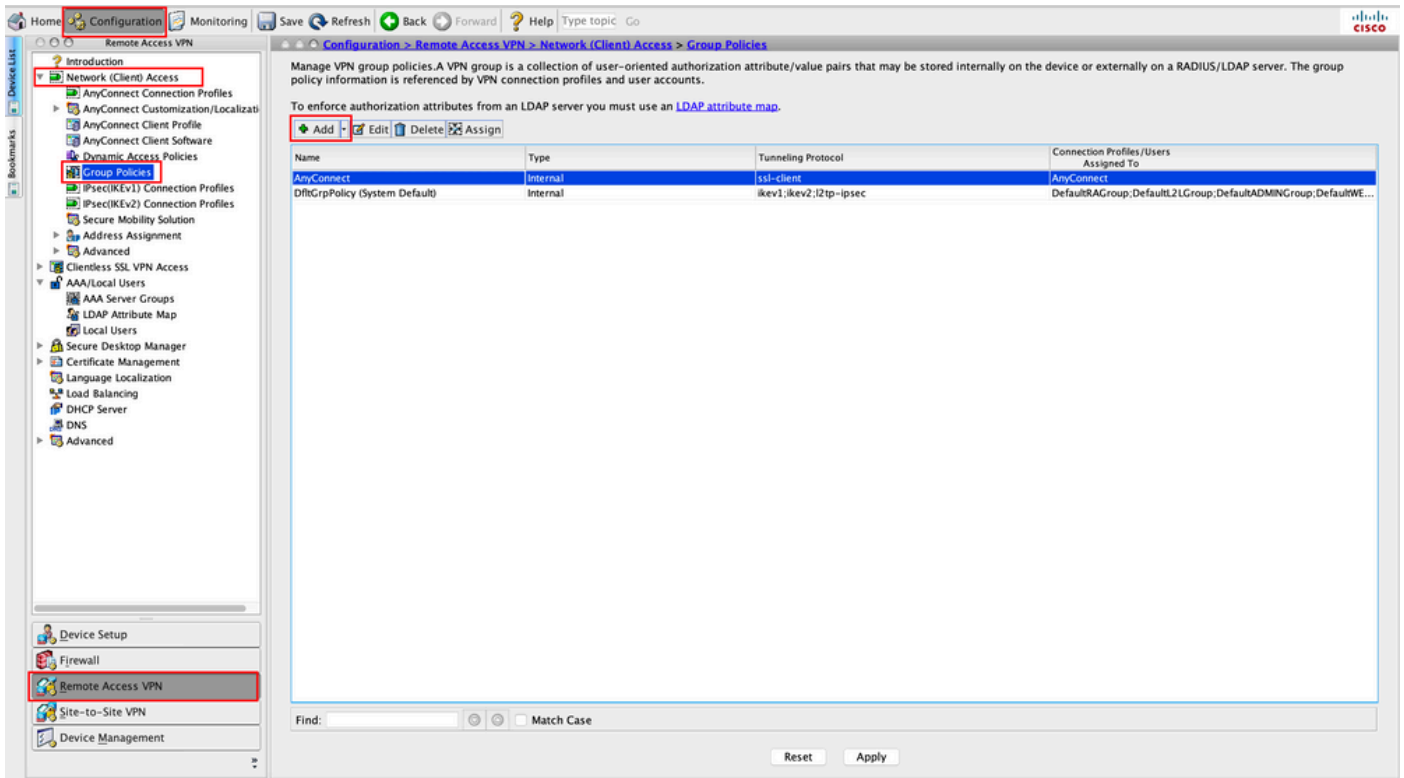
### Configurazione su ASA tramite ASDM/CLI

Passaggio 1. Creare i Criteri di gruppo AnyConnect. Passare a `Configuration > Remote Access VPN > Network (Client) Access > Group Policies`. Fare clic su `.Add`

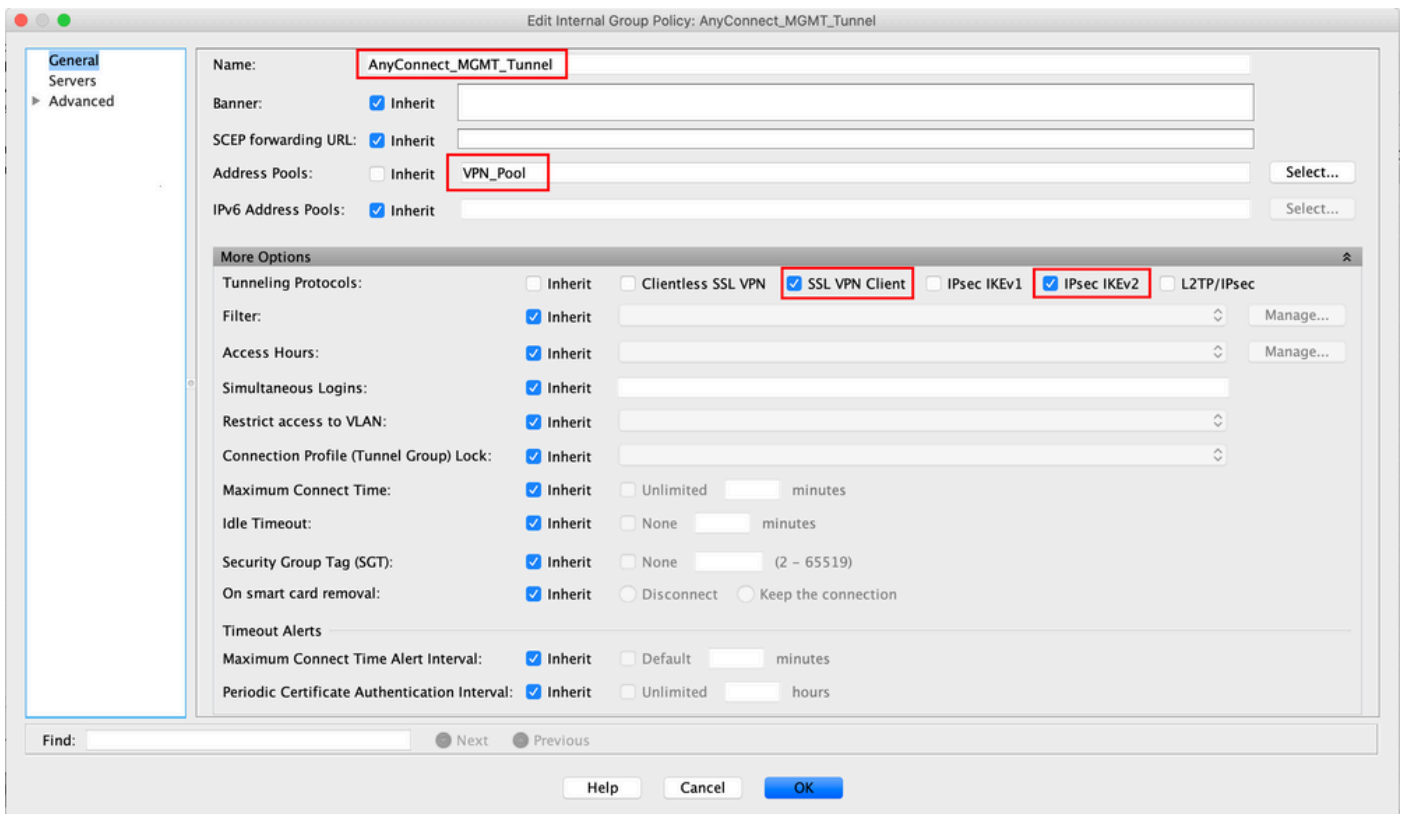
---

 Nota: si consiglia di creare un nuovo criterio di gruppo AnyConnect che venga utilizzato solo per il tunnel di gestione di AnyConnect.

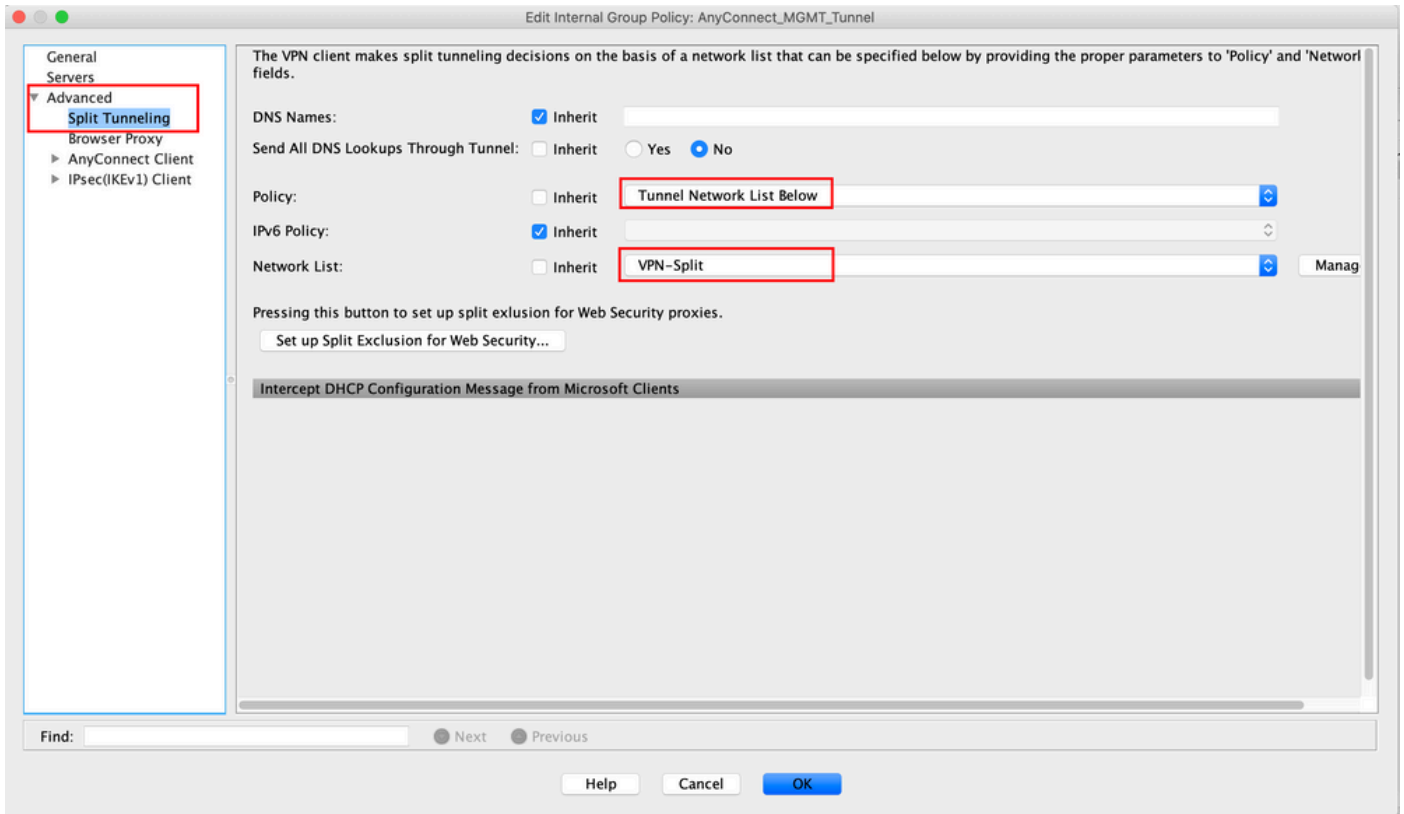
---




Passaggio 2. Fornire un nome per i Criteri di gruppo. Assegnare/creare un Address Pool oggetto. Scegliere Tunneling Protocols come SSL VPN Client e/o IPsec IKEv2, come illustrato nell'immagine.

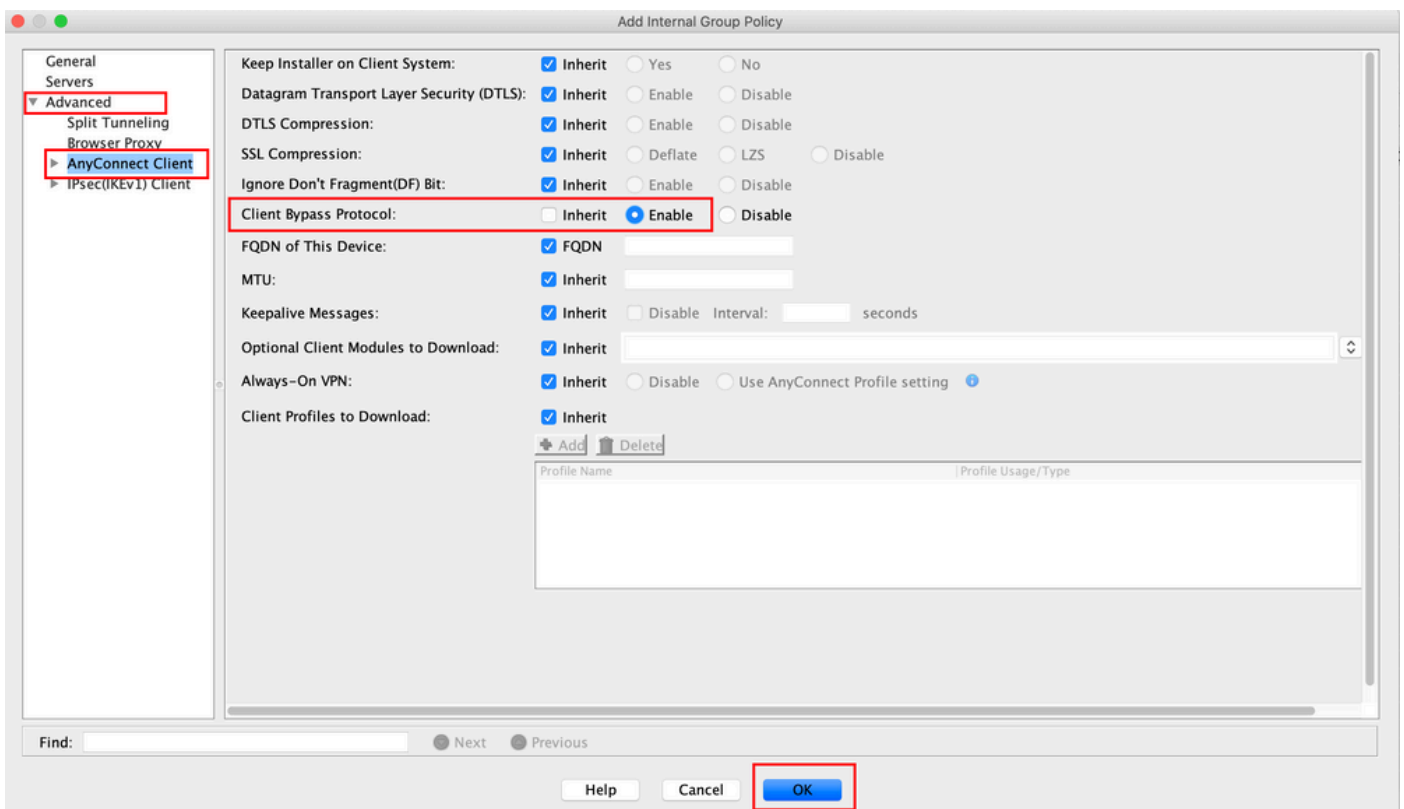


Passaggio 3. Passare a Advanced > Split Tunneling. Configurare il Policy come Tunnel Network List Below e scegliere il Network List, come mostrato nell'immagine.

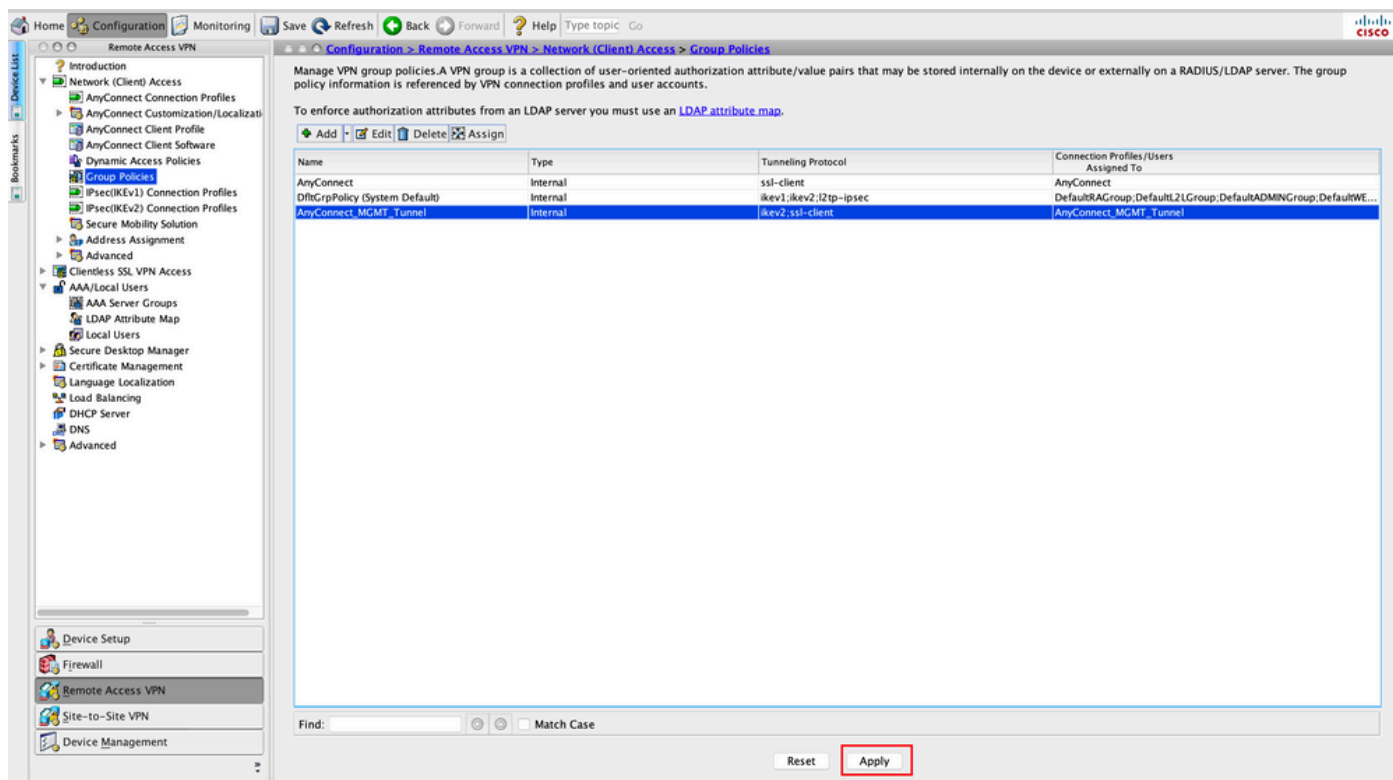


 Nota: se non viene eseguito il push di un indirizzo client per entrambi i protocolli IP (IPv4 e IPv6), l'impostazione deve essere tale che il traffico corrispondente non venga interrotto dal tunnel di gestione. Per configurare, fare riferimento al [passo 4](#).

Passaggio 4. Passare a **Advanced > AnyConnect Client**. Impostare **Client Bypass Protocol** su **Enable**. Fare clic **OK** per salvare, come mostrato nell'immagine.



Passaggio 5. Come mostrato nell'immagine, fare clic su **Apply** per inviare la configurazione all'appliance ASA.



Configurazione CLI per Criteri di gruppo:

```
<#root>
```

```
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

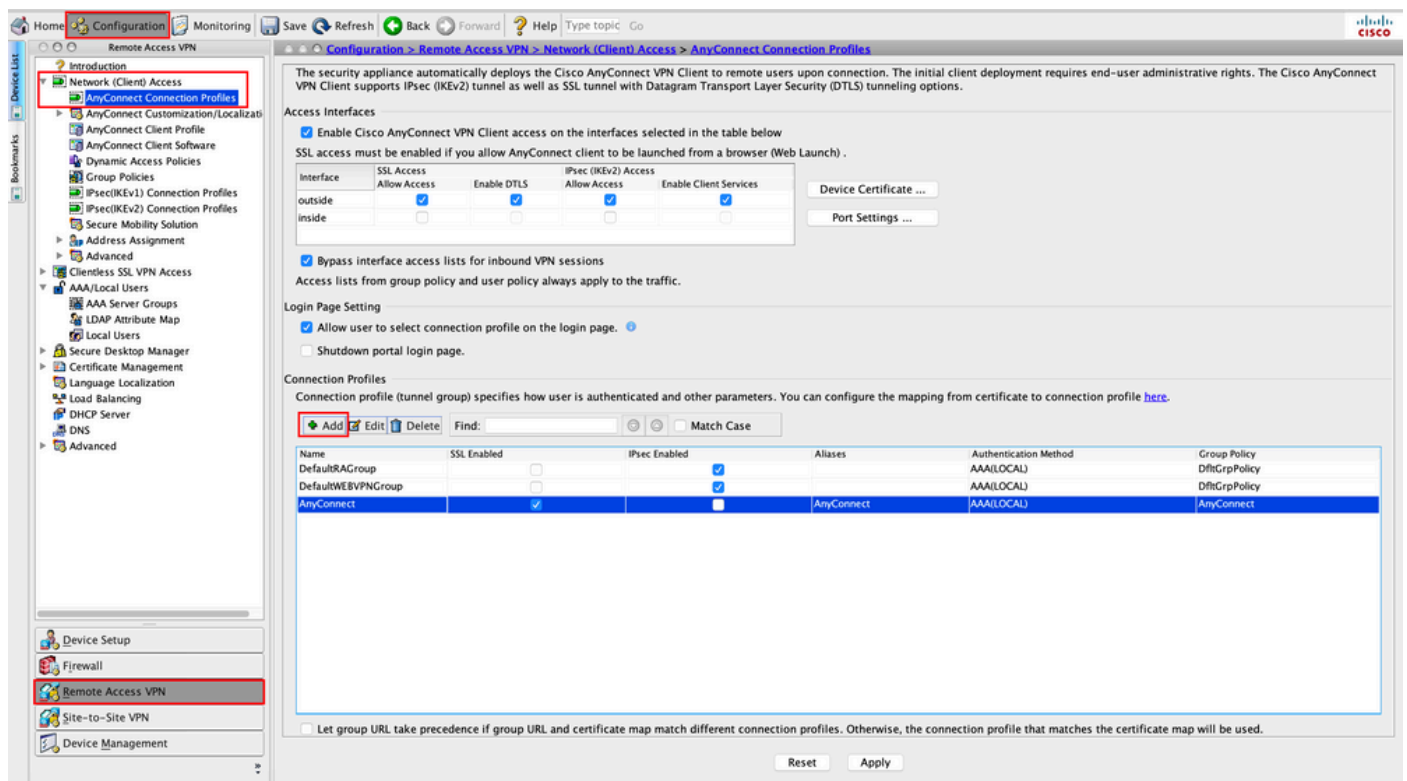
client-bypass-protocol enable

address-pools value

## VPN\_Pool

Passaggio 6. Creare il profilo di connessione AnyConnect. Passare a Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Fare clic su .Add

 Nota: si consiglia di creare un nuovo profilo di connessione AnyConnect che venga usato solo per il tunnel di gestione di AnyConnect.





The screenshot shows the Cisco AnyConnect Configuration page. The left sidebar has 'Remote Access VPN' selected. The main content area is titled 'AnyConnect Connection Profiles'. A table lists the connection profiles:

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LLOCAL)	DfnCrpPolicy
DefaultWEBVPGGroup	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LLOCAL)	DfnCrpPolicy
AnyConnect	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyConnect	AAA(LLOCAL)	AnyConnect

Passaggio 7. Fornire unNameprofilo per il profilo di connessione e impostareAuthentication MethodcomeCertificate only. Scegliete comeGroup Policyquella creata nel [passo 1](#).

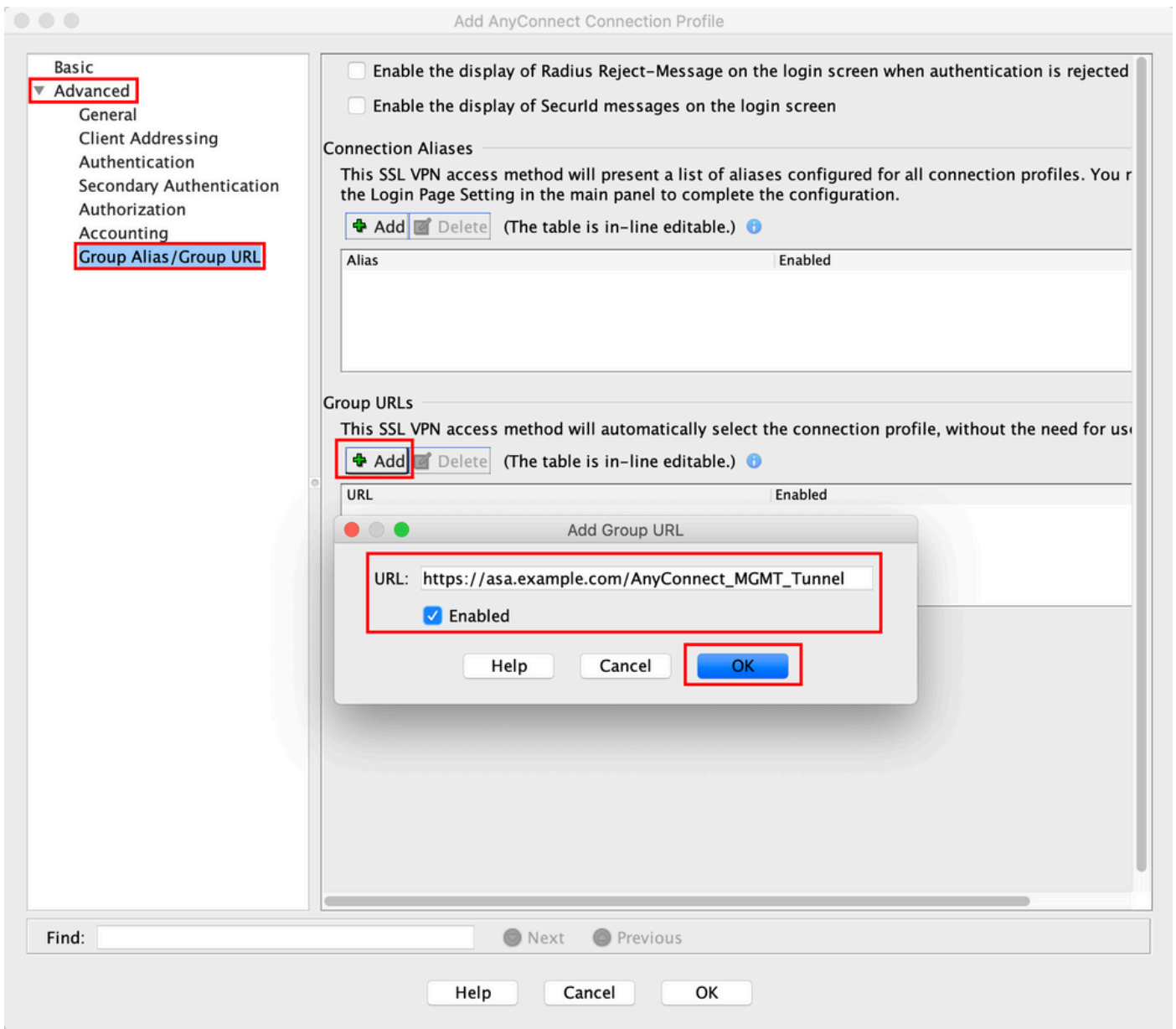
The screenshot shows the 'Add AnyConnect Connection Profile' dialog box. The 'Basic' tab is selected. The 'Name' field contains 'AnyConnect\_MGMT\_Tunnel'. The 'Method' dropdown is set to 'Certificate only'. The 'AAA Server Group' is 'LOCAL'. The 'SAML Server' is 'None'. The 'Client Address Assignment' is 'None'. The 'Default Group Policy' is 'AnyConnect\_MGMT\_Tunnel'. The 'Enable SSL VPN client protocol' and 'Enable IPsec(IKEv2) client protocol' checkboxes are checked. The 'DNS Servers', 'WINS Servers', and 'Domain Name' fields are empty.

 Nota: verificare che il certificato radice della CA locale sia presente sull'appliance ASA. Passare a Configuration > Remote Access VPN > Certificate Management > CA Certificates per aggiungere/visualizzare il certificato.

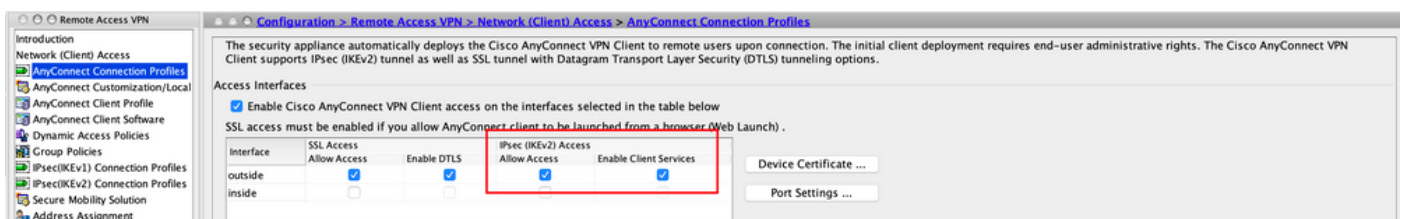
 Nota: verificare che un certificato di identità rilasciato dalla stessa CA locale sia presente nell'archivio certificati del computer (per Windows) e/o nella catena di chiavi di sistema (per macOS).

Passaggio 8. Passare a Advanced > Group Alias/Group URL. Fare clic su Add sotto Group URL e aggiungere un'URL icona. Accertarsi che sia Enabled selezionata. Fare clic OK per salvare, come mostrato nell'immagine.





Se si usa IKEv2, verificare che IPsec (IKEv2) Access sia abilitato sull'interfaccia usata per AnyConnect.




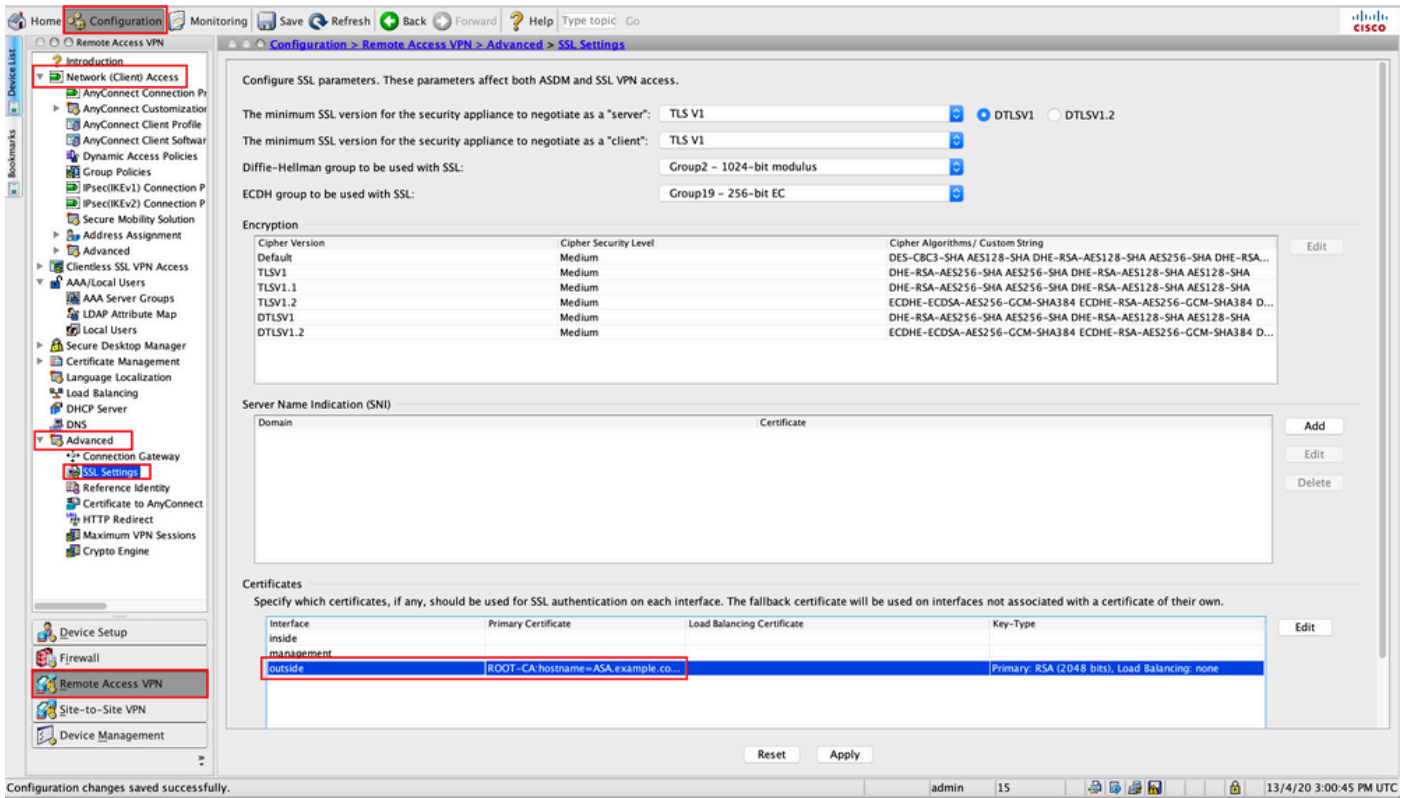
Passaggio 9. Fare clic su questa opzione per inviare la configurazione all'appliance ASA.

Configurazione CLI per il profilo di connessione (gruppo di tunnel):

```
<#root>
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
```

Passaggio 10. Verificare che sull'appliance ASA sia installato un certificato protetto e che il certificato sia associato all'interfaccia usata per le connessioni AnyConnect. Passare Configuration > Remote Access VPN > Advanced > SSL Settings a per aggiungere/visualizzare questa impostazione.

 Nota: per ulteriori informazioni, consultare il documento sull'[installazione del certificato di identità sull'appliance ASA](#).



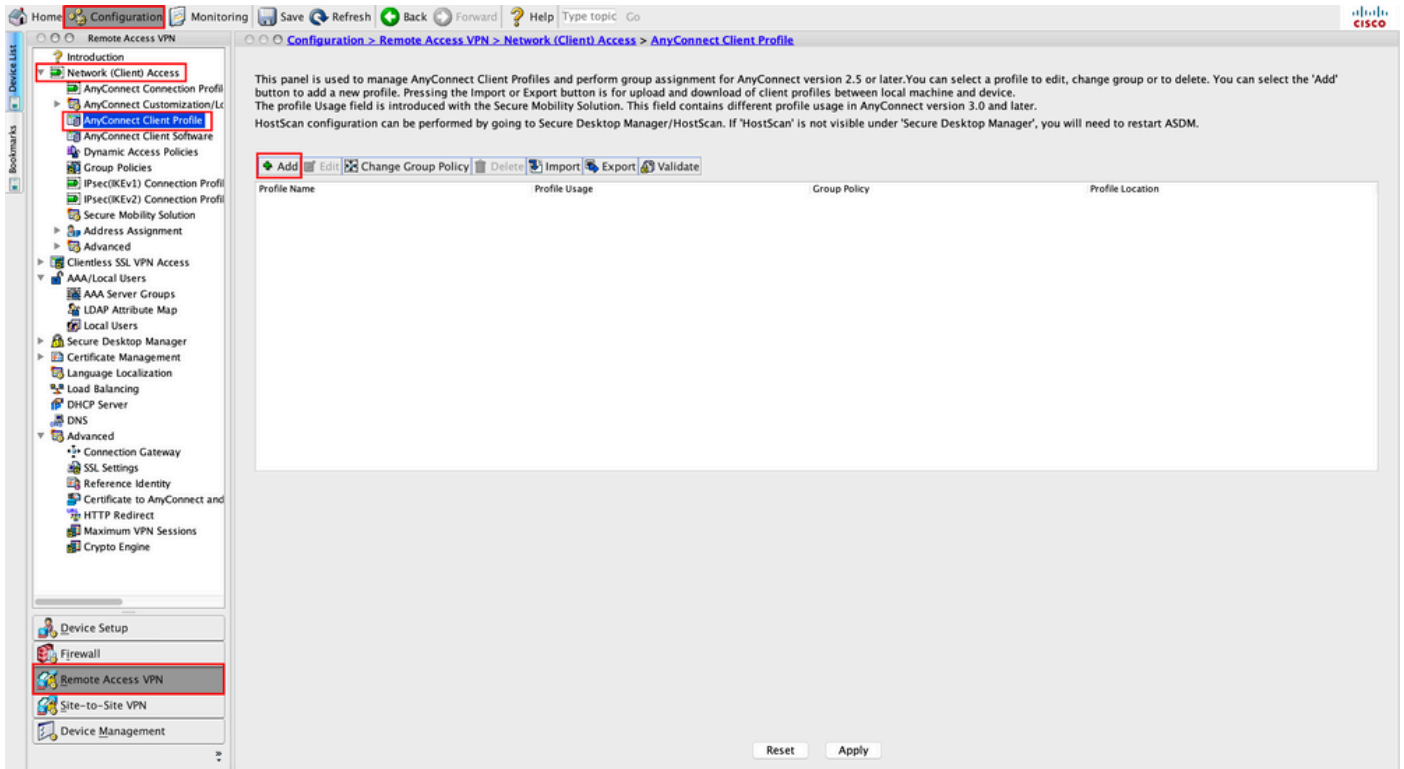
## Configurazione CLI per Trustpoint SSL:

```
<#root>
```

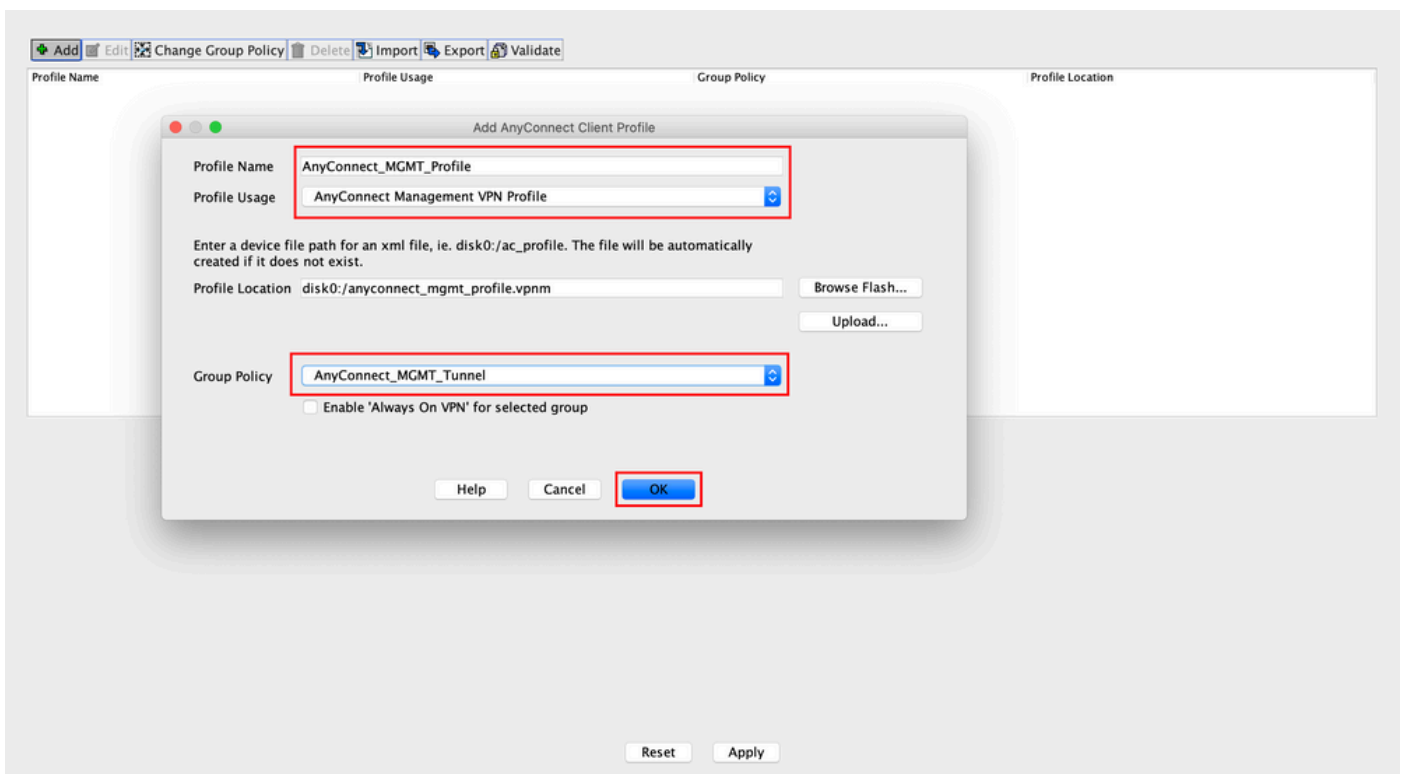
```
ssl trust-point ROOT-CA outside
```

## Creazione del profilo VPN di gestione di AnyConnect

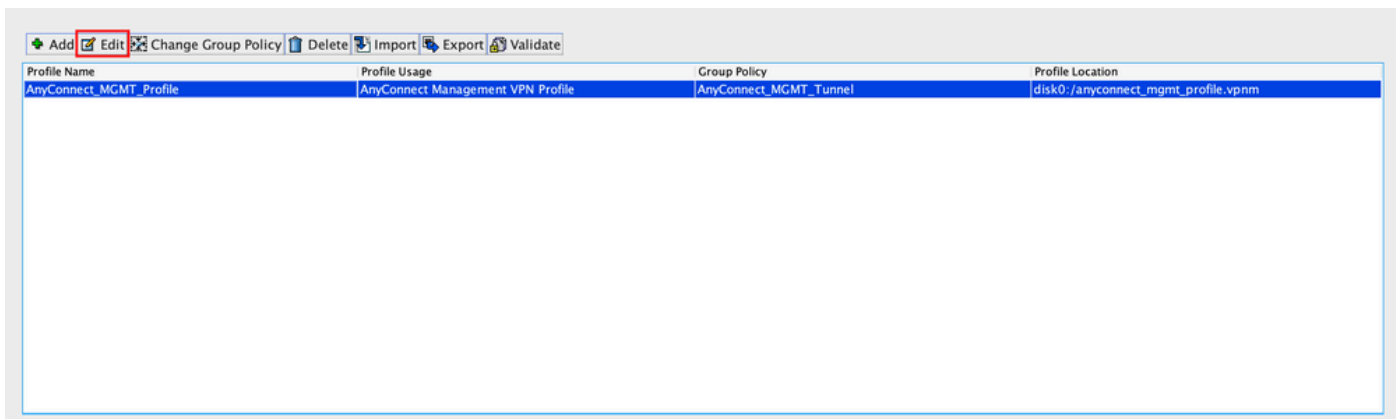
Passaggio 1. Creare il profilo del client AnyConnect. Passare a **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**. Fare clic su **Add**, come mostrato nell'immagine.



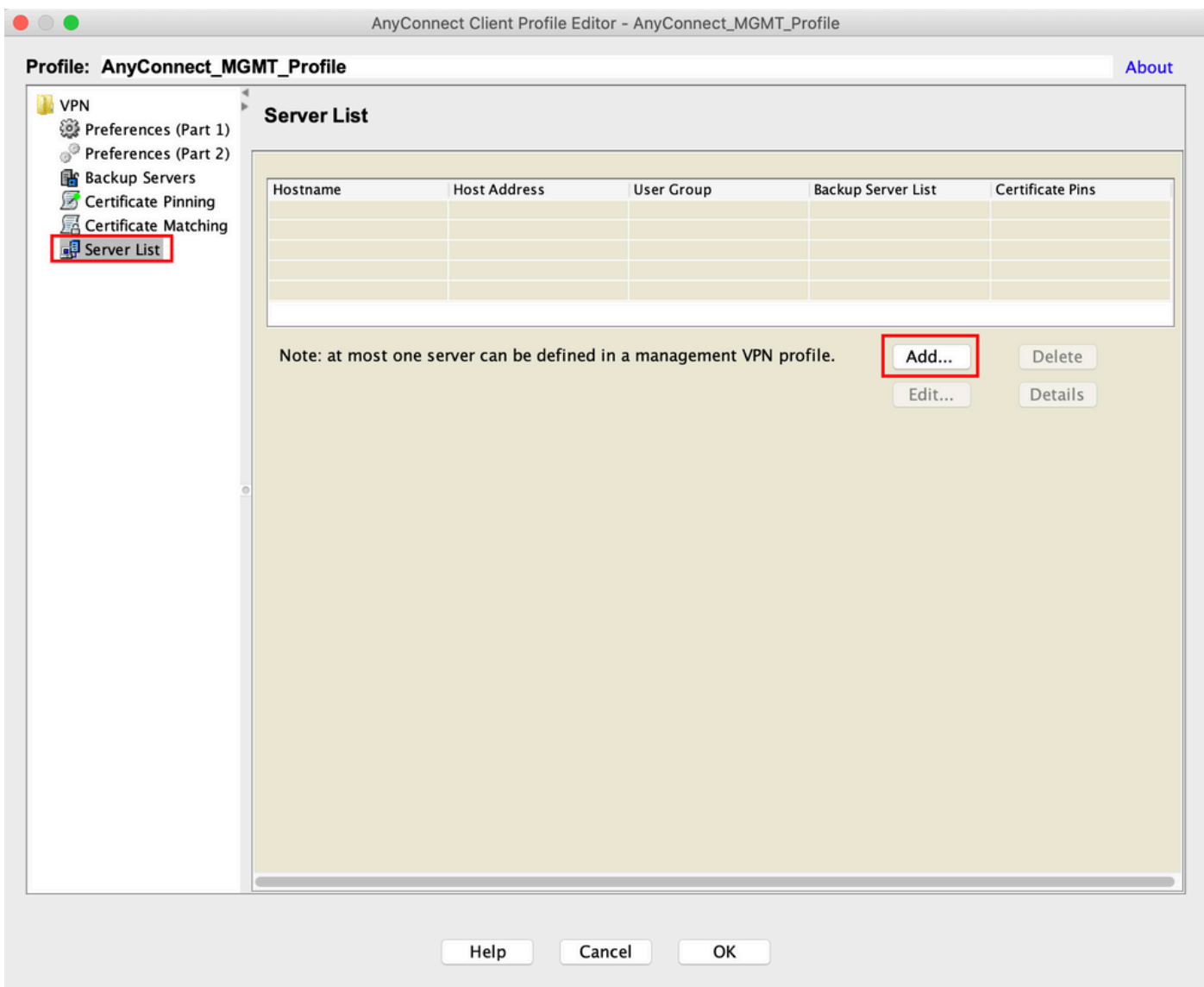
Passaggio 2. Fornire una Profile Name risposta. Scegliere il Profile Usage come AnyConnect Management VPN profile. Scegliere il file Group Policy creato nel [passo 1](#). Fare clic su OK, come mostrato nell'immagine.



Passaggio 3. Scegliere il profilo creato e fare clic su Modifica, come mostrato nell'immagine.



Passaggio 4. Passare a Server List. Fare clic su Add per aggiungere una nuova voce all'elenco dei server, come illustrato nell'immagine.



Passaggio 5. Fornire una Display Name risposta. Aggiungere il valore FQDN/IP address dell'appliance ASA. Fornire come nome del User Group gruppo di tunnel. Group URL viene popolato automaticamente con FQDN User Group. Fare clic su .OK

Server Certificate Pinning

Primary Server

Display Name (required) AnyConnect\_MGMT\_Tunnel

FQDN or IP Addr... User Group (required)

asa.example.com / 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)

Backup Servers

Host Address


Add


Move Up

Move Down

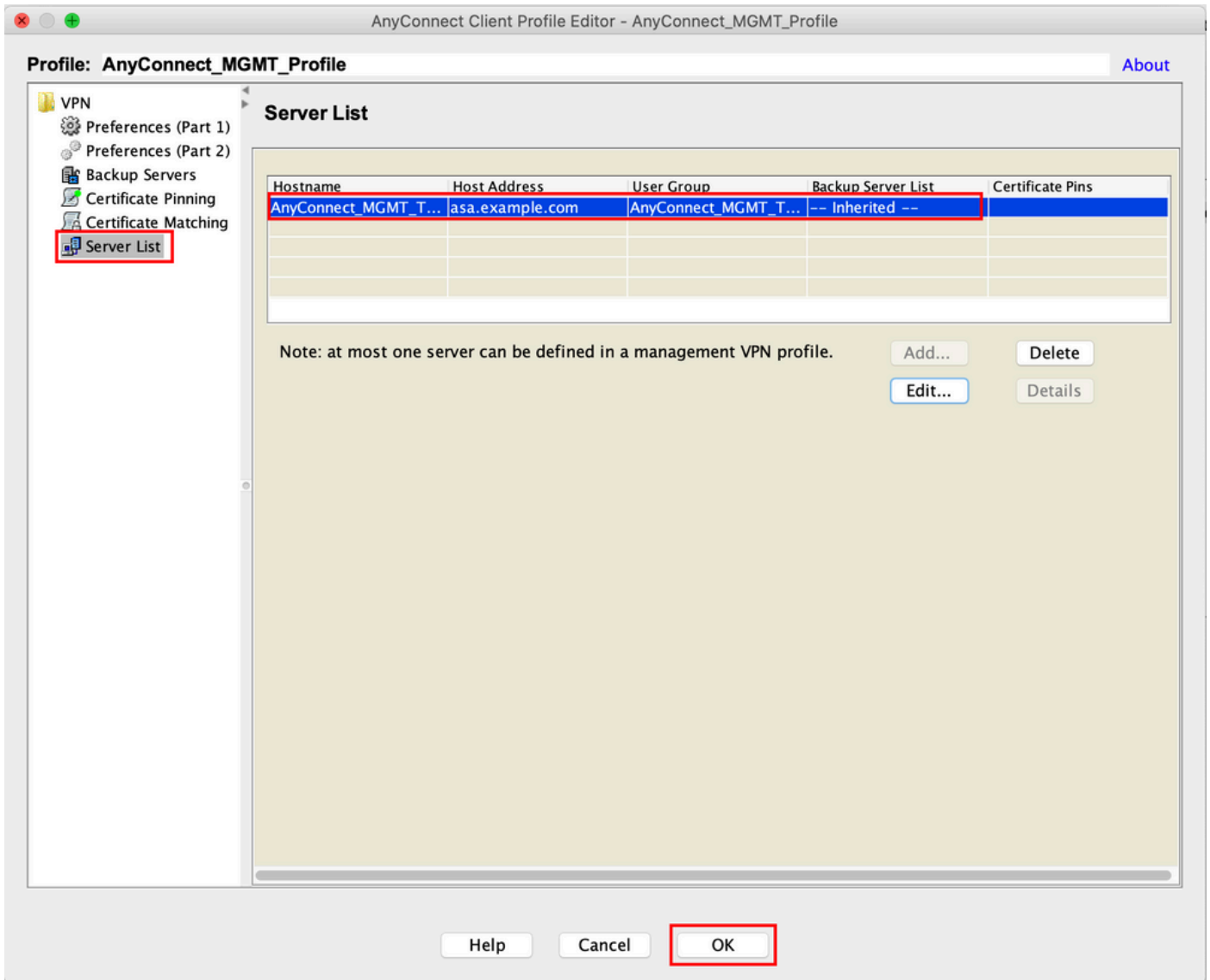
Delete

OK Cancel

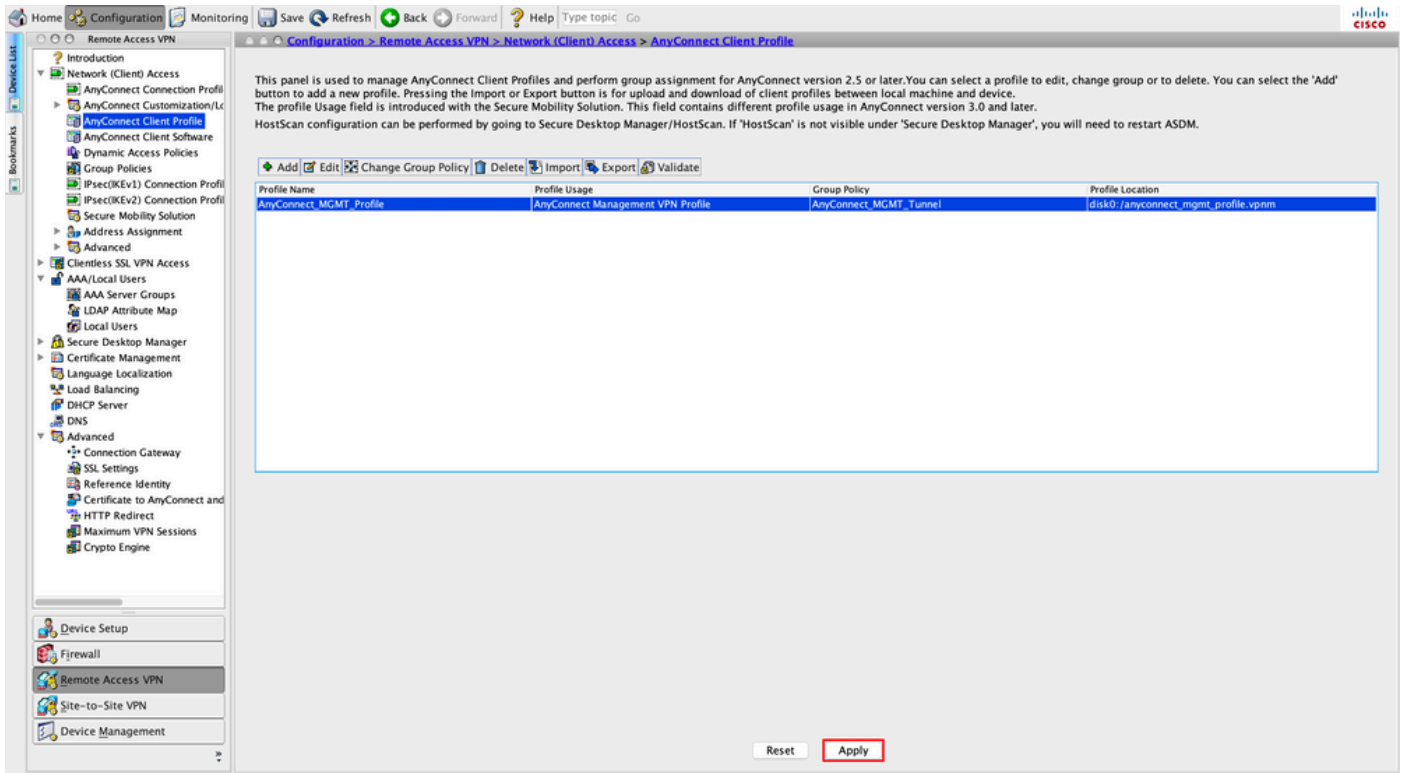
 Nota: l'FQDN/indirizzo IP + gruppo di utenti deve corrispondere all'URL del gruppo indicato durante la configurazione del profilo di connessione AnyConnect al [passaggio 8](#).

 Nota: AnyConnect con IKEv2 come protocollo può essere utilizzato anche per stabilire una VPN di gestione per l'appliance ASA. Accertarsi che Primary Protocol sia impostato IPsec su [Passo 5](#).

Passaggio 6. Come mostrato nell'immagine, fare clic su OK per salvare.



Passaggio 7. Fare clic **Apply** per spostare la configurazione sull'appliance ASA, come mostrato nell'immagine.



Configurazione CLI dopo l'aggiunta del profilo VPN di gestione di AnyConnect.

```
<#root>
```

```
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
```



Profilo VPN di gestione di AnyConnect sul computer client AnyConnect:

<#root>

<?xml version="1.0" encoding="UTF-8"?>

<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"

<ClientInitialization>

<UseStartBeforeLogon UserControlable="false">false</UseStartBeforeLogon>

true

<ShowPreConnectMessage>false</ShowPreConnectMessage>

Machine

System

true

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

--- Output Omitted ---


```
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>  
<AllowManualHostInput>false</AllowManualHostInput>  
</ClientInitialization>
```

**AnyConnect\_MGMT\_Tunnel**


asa.example.com

</AnyConnectProfile>

---

 Nota: se si usa TND (Trusted Network Detection) nel profilo VPN AnyConnect dell'utente, si consiglia di usare le stesse impostazioni nel profilo VPN di gestione per garantire un'esperienza utente coerente. Il tunnel VPN di gestione viene attivato in base alle impostazioni TND applicate al profilo del tunnel VPN utente. Inoltre, l'azione TND Connect nel profilo VPN di gestione (applicata solo quando il tunnel VPN di gestione è attivo), si applica sempre al tunnel VPN dell'utente, per garantire che il tunnel VPN di gestione sia trasparente per l'utente finale.

---

 Nota: su qualsiasi PC dell'utente finale, se le impostazioni TND sono abilitate nel profilo VPN di gestione e il profilo VPN dell'utente è mancante, vengono prese in considerazione le impostazioni delle preferenze predefinite per il TND (disabilitato nelle preferenze predefinite nell'applicazione client AC) anziché il profilo VPN dell'utente mancante. Questa mancata corrispondenza può causare un comportamento imprevisto/non definito. Per impostazione predefinita, le impostazioni TND sono disattivate nelle preferenze predefinite. Per superare le impostazioni hardcoded delle preferenze predefinite nell'applicazione Client AnyConnect, il PC dell'utente finale deve avere due profili VPN, un profilo VPN utente e un profilo VPN di gestione CA, ed entrambi devono avere le stesse impostazioni TND. La logica alla base della connessione e della disconnessione del tunnel VPN di gestione è che per stabilire un tunnel VPN di gestione, l'agente AC utilizza le impostazioni TND del profilo VPN dell'utente e, per la disconnessione del tunnel VPN di gestione, controlla le impostazioni TND del profilo VPN di gestione.

---

## Metodi di distribuzione per il profilo VPN di gestione di AnyConnect

- Una connessione VPN dell'utente è stata completata con il profilo di connessione ASA per scaricare il profilo VPN di gestione di AnyConnect dal gateway VPN.

---

 Nota: se il protocollo usato per il tunnel VPN di gestione è IKEv2, è necessario stabilire la prima connessione tramite SSL (per scaricare il profilo AnyConnect Management VPN

---

 dall'appliance ASA).

- Il profilo VPN di gestione di AnyConnect può essere caricato manualmente sui computer client tramite un push di oggetti Criteri di gruppo o tramite installazione manuale (verificare che il nome del profilo sia `VpnMgmtTunProfile.xml`).

Percorso della cartella in cui aggiungere il profilo:

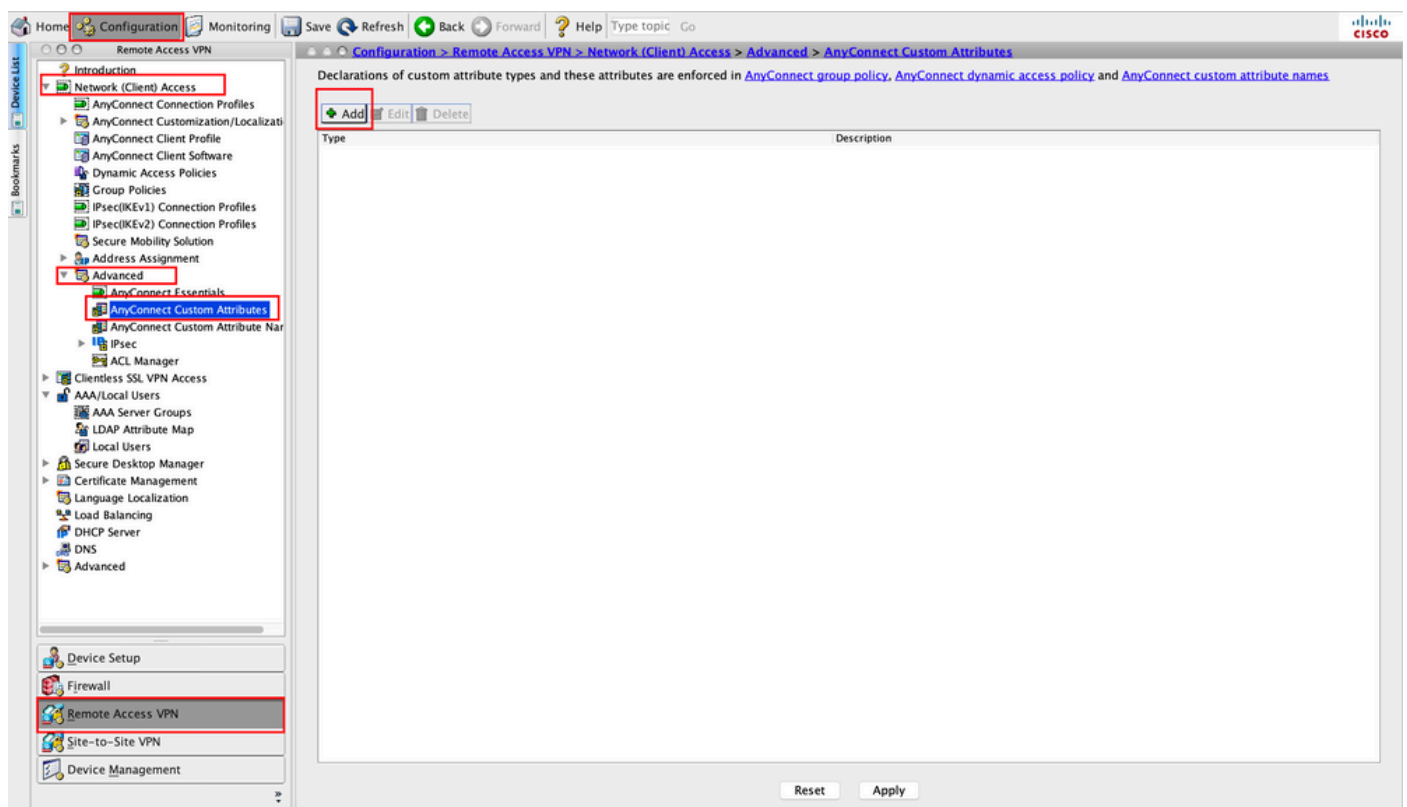
Windows: `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun`

Mac OS: `/opt/cisco/anyconnect/profile/mgmttun/`

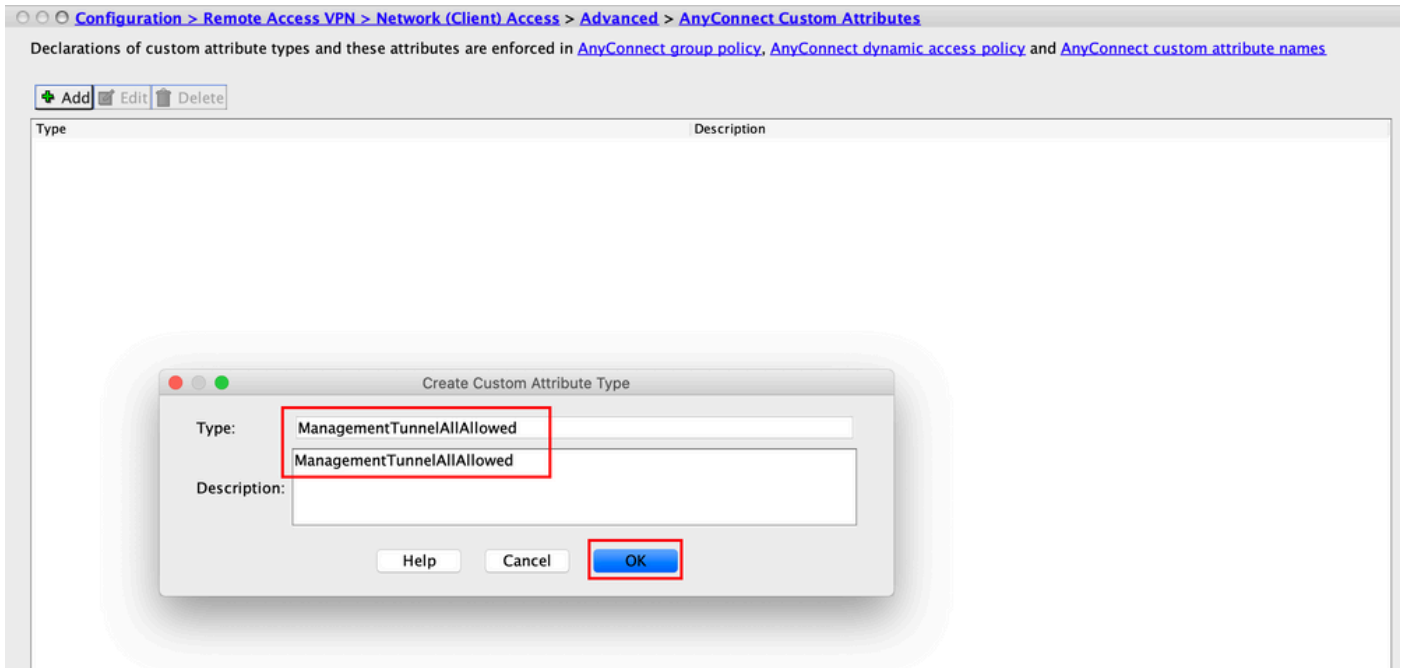
## (Facoltativo) Configurare un attributo personalizzato per supportare la configurazione tunnel-tutto

Il tunnel VPN di gestione richiede una divisione che include la configurazione del tunneling per impostazione predefinita, per evitare un impatto sulla comunicazione di rete avviata dall'utente. È possibile ignorare questa impostazione quando si configura l'attributo personalizzato nei Criteri di gruppo utilizzati dalla connessione del tunnel di gestione.

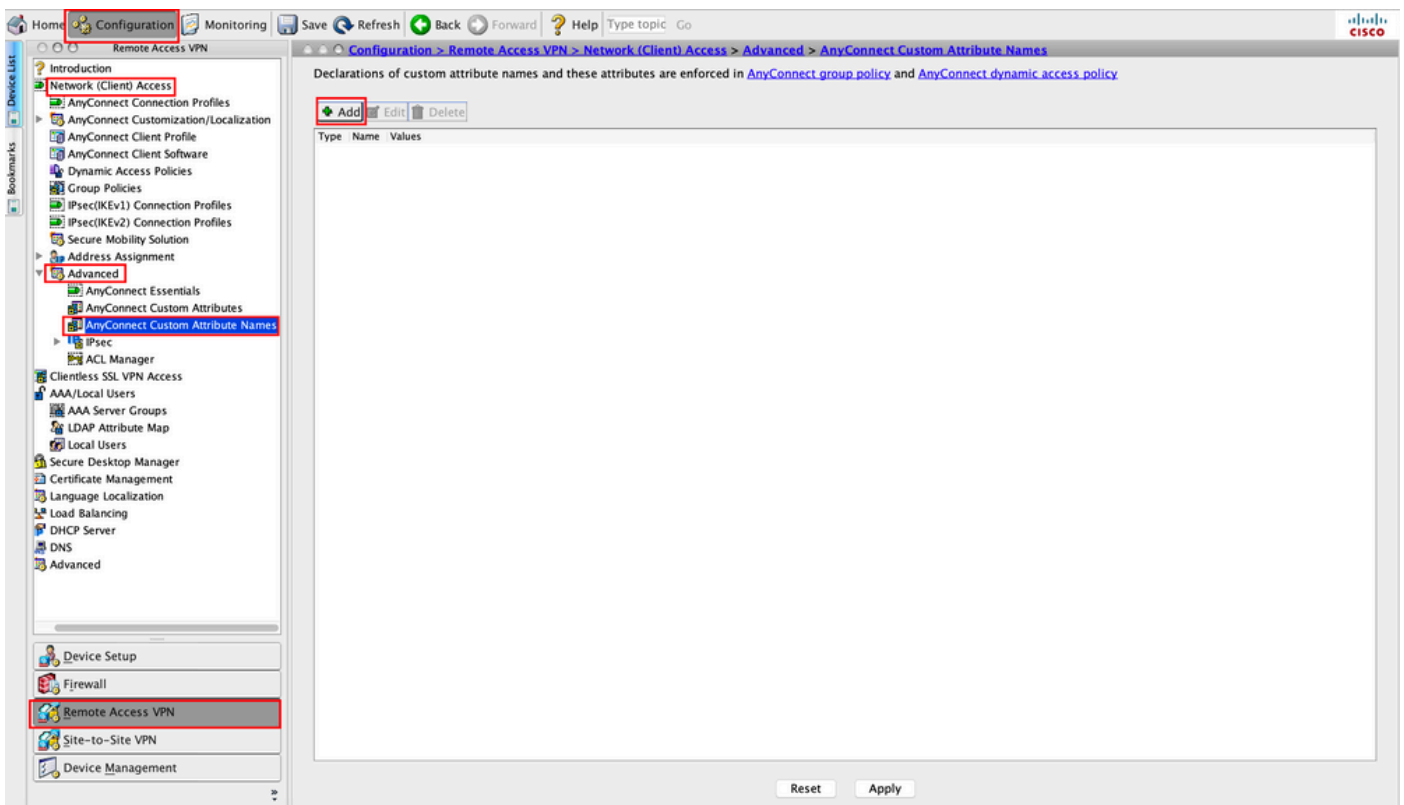
Passaggio 1. Passare `Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes`. Fare clic su `+`, come mostrato nell'immagine.



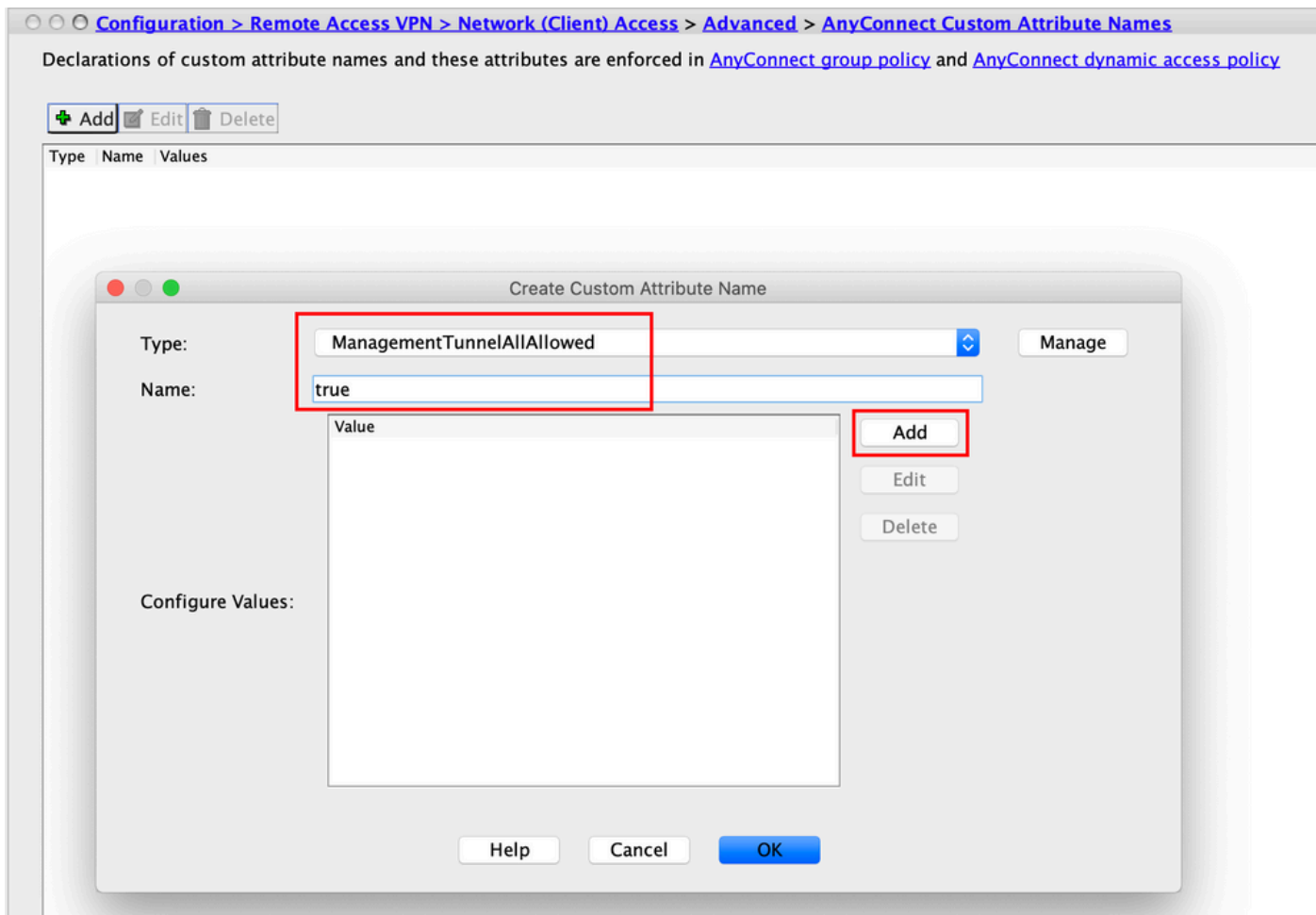
Passaggio 2. Impostare l'attributo personalizzato Tipo su `ManagementTunnelAllAllowed` e fornire un Description. Fare clic su `OK`, come mostrato nell'immagine.



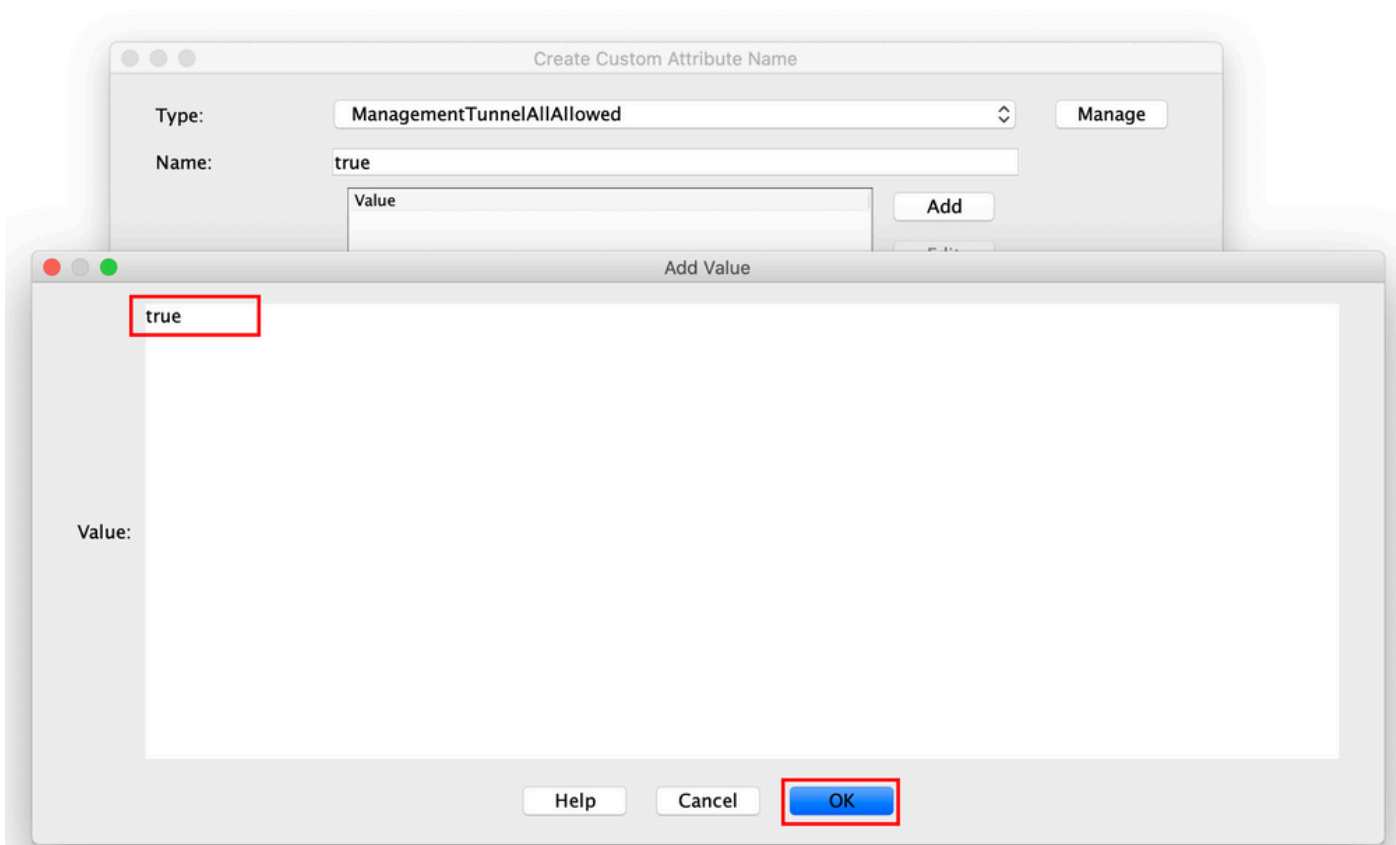
Passaggio 3. Passare a Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Fare clic su, come mostrato nell'immagine.



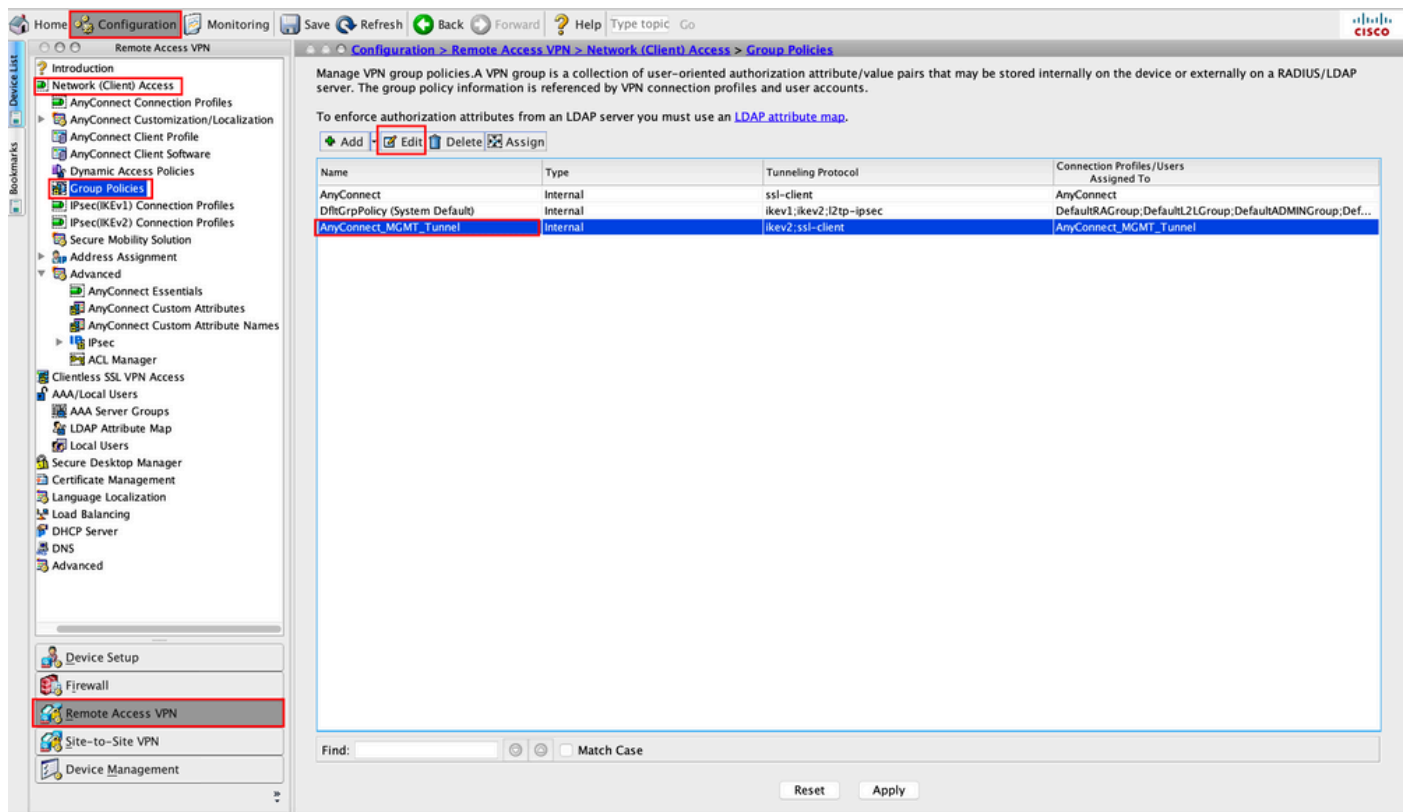
Passaggio 4. Scegliete il Tipo (Type) come ManagementTunnelAllAllowed. Impostare il nome come true. Fare clic su Add per fornire un valore di attributo personalizzato, come mostrato nell'immagine.



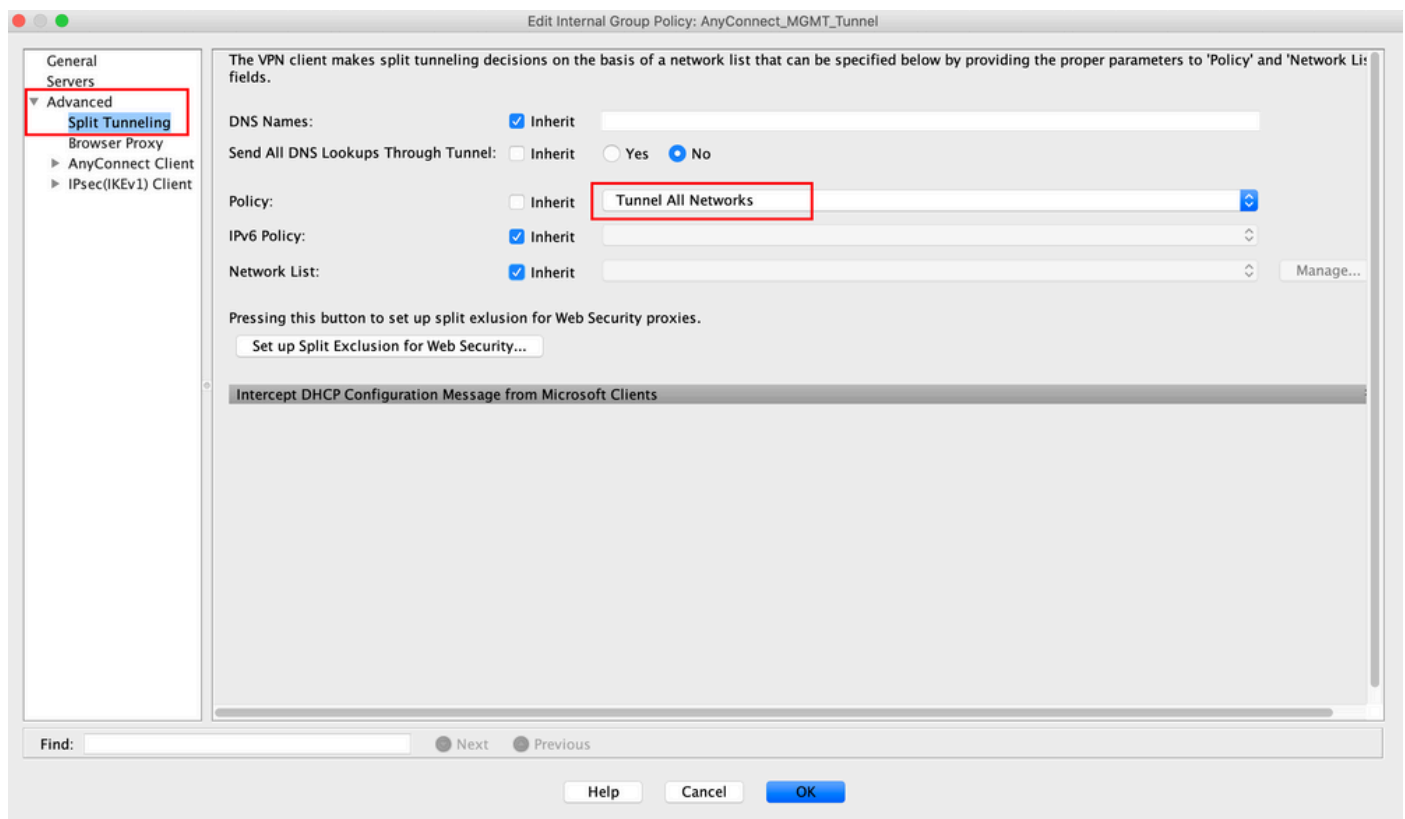
Passaggio 5. Impostare il valore come true. Fare clic su OK, come mostrato nell'immagine.



Passaggio 6. Passare a Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Scegliere Criteri di gruppo. Fare clic su Edit, come illustrato nell'immagine.

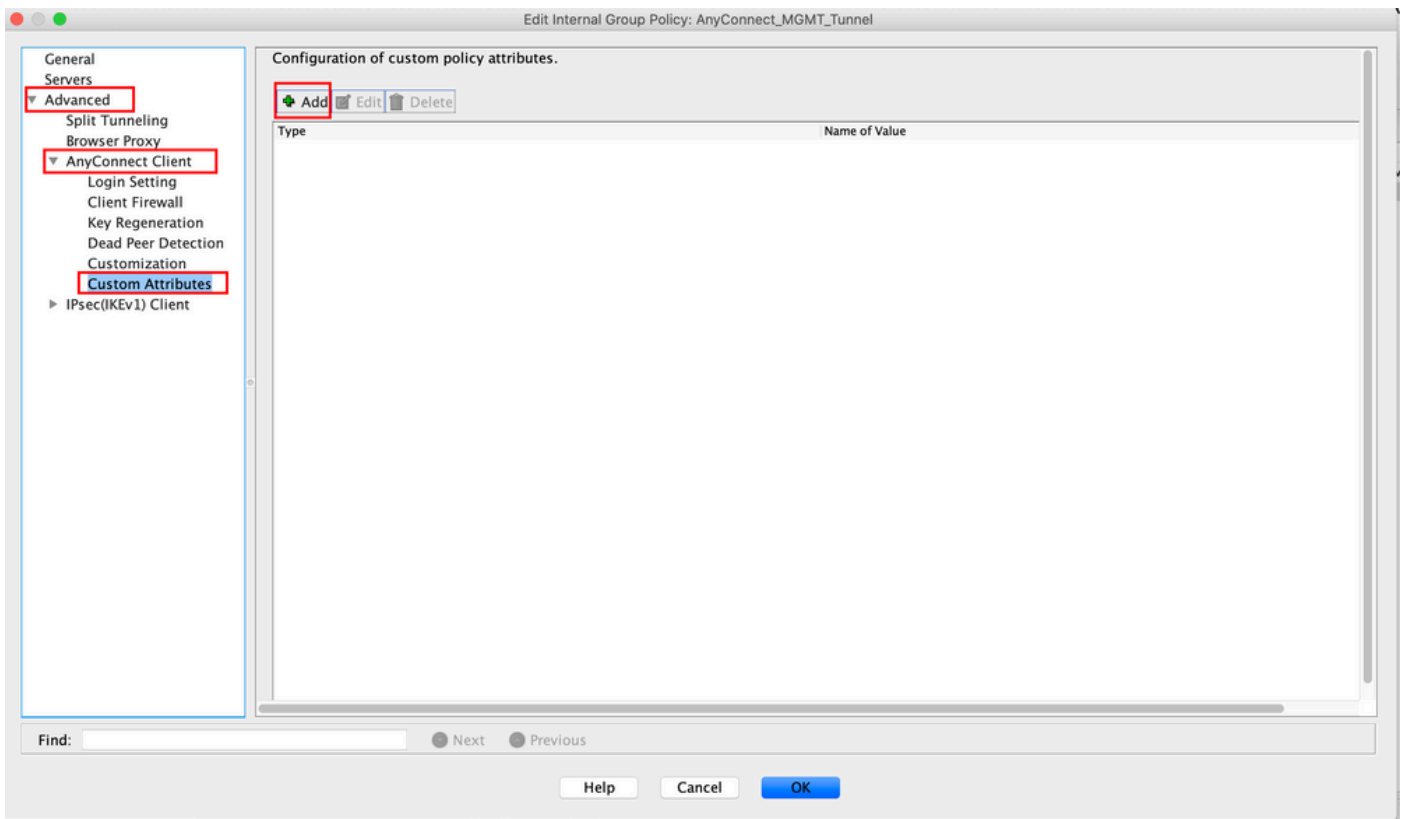


Passaggio 7. Come mostrato nell'immagine, passare a Advanced > Split Tunneling. Configurare il criterio come Tunnel All Networks.

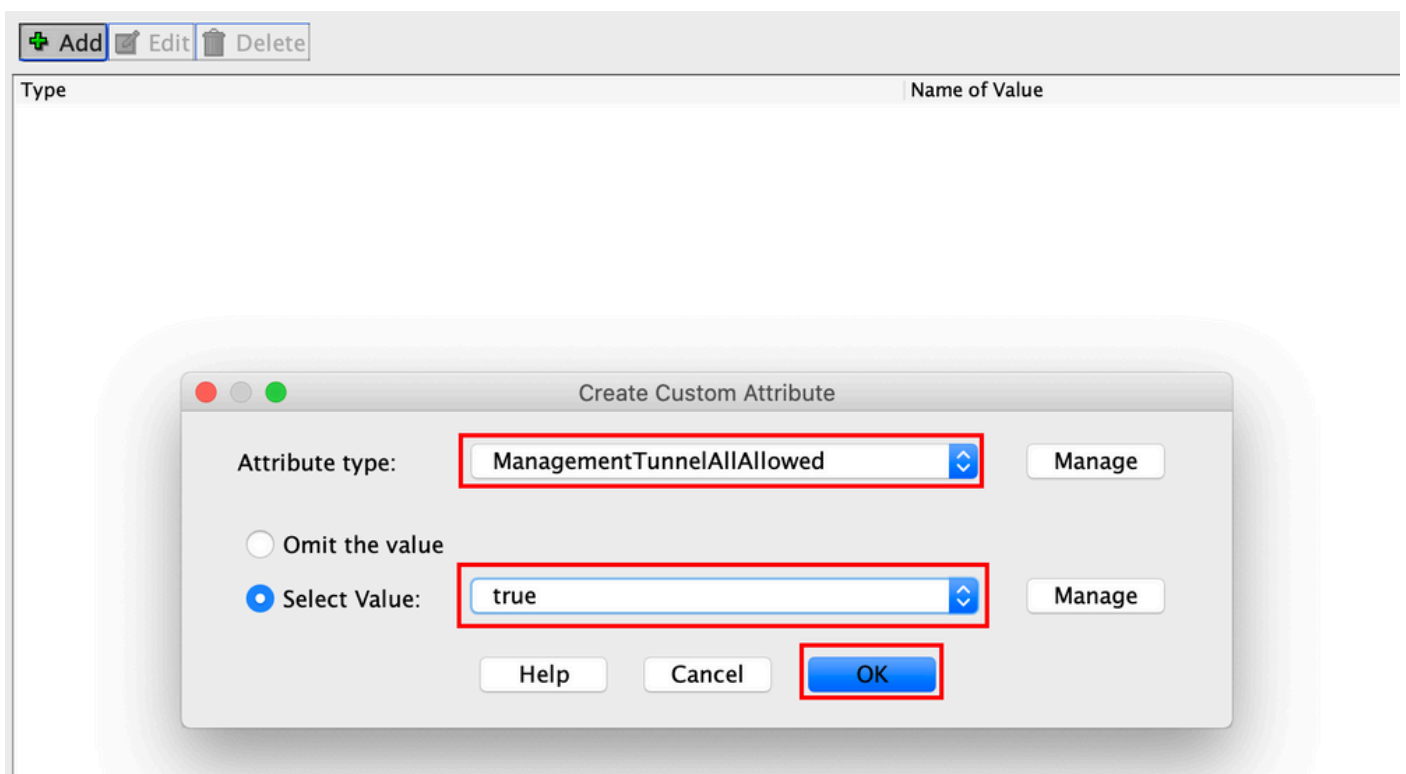


Passaggio 8. Passare a Advanced > Anyconnect Client > Custom Attributes. Fare clic su Add, come mostrato

nell'immagine.

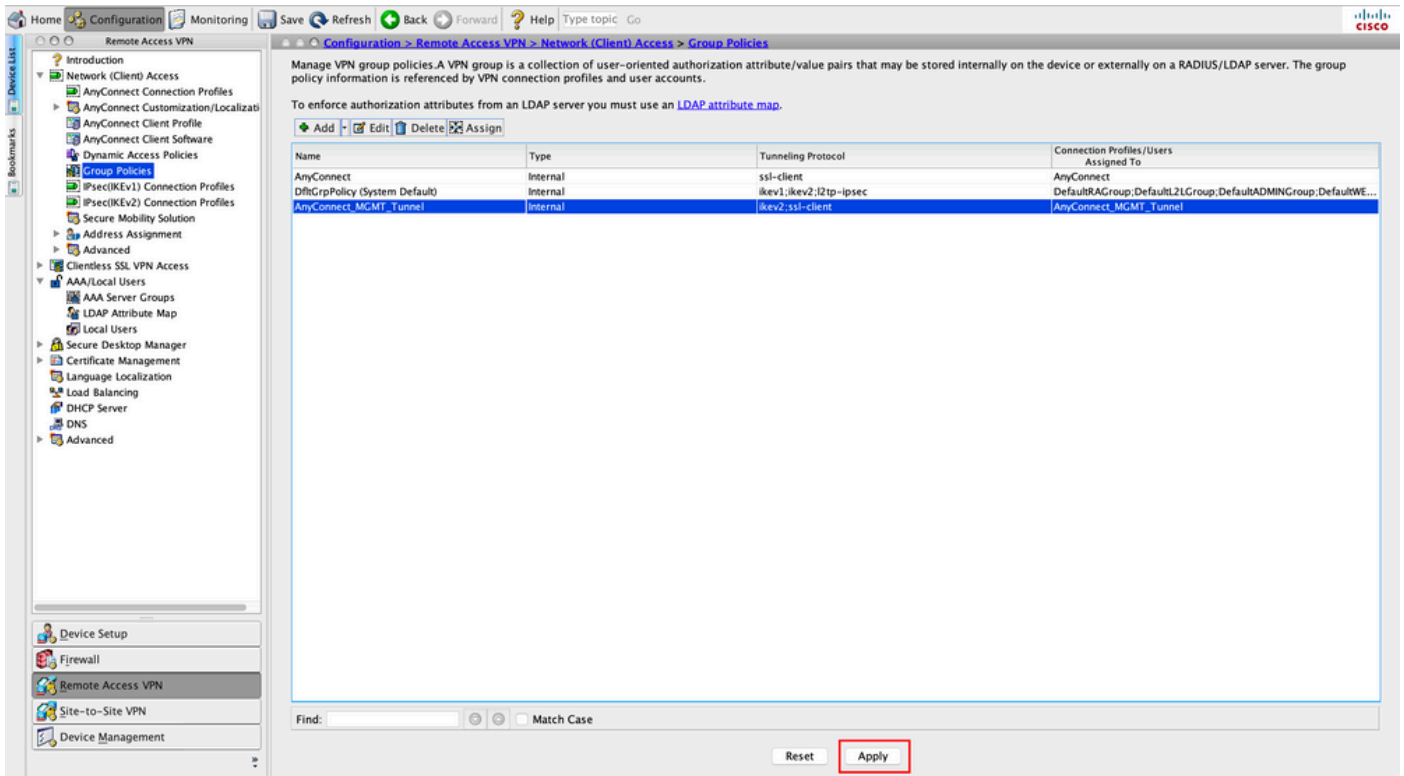


Passaggio 9. Scegliere il tipo di attributo come `ManagementTunnelAllAllowed` e il valore come `true`. Fare clic OK, come mostrato nell'immagine.



Passaggio 10. Fare clic su `Apply` per trasferire la configurazione sull'appliance ASA, come mostrato nell'immagine.





Configurazione CLI dopo l'aggiunta dell'`ManagementTunnelAllAllowed` attributo personalizzato:

```
<#root>
```

```
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
```

## Verifica

Verificare la connessione del tunnel VPN di gestione sulla CLI dell'ASA con il `show vpn-sessiondb detail anyconnect` comando.

```
<#root>
```

```
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:**

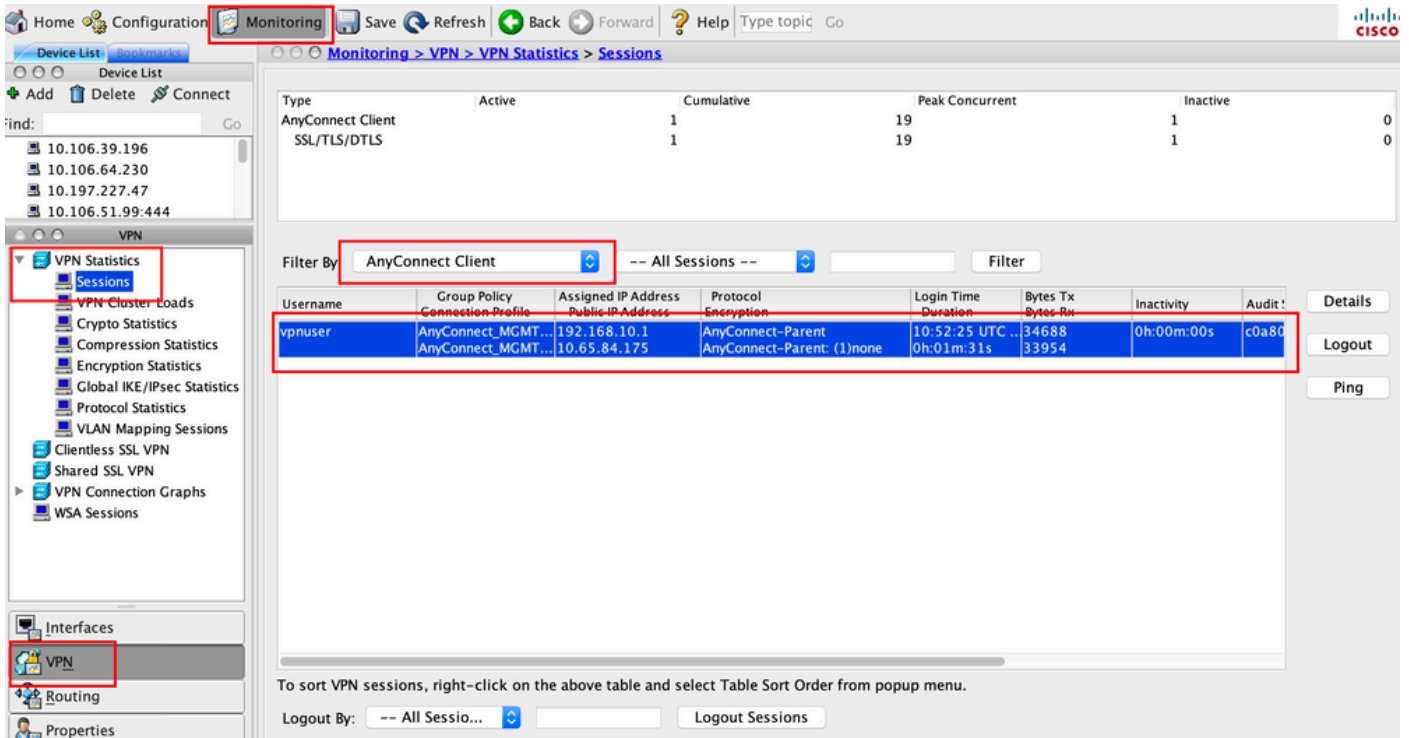
Tunnel ID : 10.3  
Assigned IP : 192.168.10.1                      Public IP : 10.65.84.175  
Encryption : AES-GCM-256                      Hashing : SHA384  
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384  
Encapsulation: DTLSv1.2                      UDP Src Port : 57053  
UDP Dst Port : 443

**Auth Mode : Certificate**

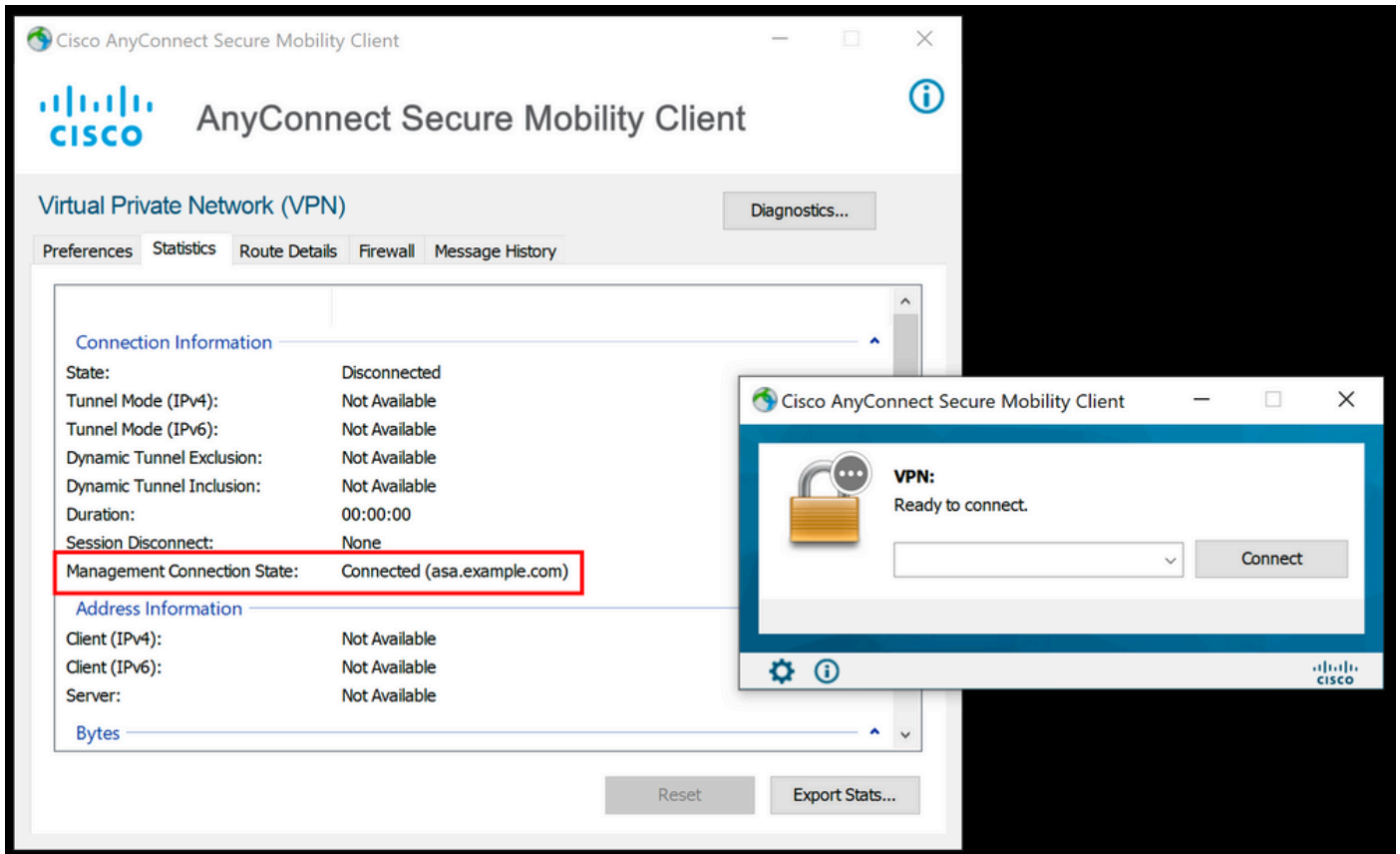
Idle Time Out: 30 Minutes                      Idle TO Left : 18 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036  
Bytes Tx : 17238                                  Bytes Rx : 1988  
Pkts Tx : 12                                      Pkts Rx : 13  
Pkts Tx Drop : 0                                  Pkts Rx Drop : 0

Verificare la connessione del tunnel VPN di gestione su ASDM.

Selezionare Monitoraggio > VPN > Statistiche VPN > Sessioni. Filtra per client AnyConnect per visualizzare la sessione client.



Verifica della connessione del tunnel VPN di gestione sul computer client:



## Risoluzione dei problemi

La nuova riga Statistiche interfaccia utente (Stato connessione di gestione) può essere utilizzata per risolvere i problemi di connettività del tunnel di gestione. Di seguito sono riportati gli stati di errore più comuni:

Disconnesso (disabilitato):

- La funzione è disattivata.
- Verificare che il profilo VPN di gestione sia stato distribuito nel client tramite la connessione al tunnel utente (è necessario aggiungere il profilo VPN di gestione ai criteri di gruppo del tunnel utente) o fuori banda tramite il caricamento manuale del profilo.
- Verificare che il profilo VPN di gestione sia configurato con una singola voce host che includa un gruppo di tunnel.

Disconnesso (rete attendibile):

- TND ha rilevato una rete attendibile, quindi il tunnel di gestione non è stato stabilito.

Disconnesso (tunnel utente attivo):

- Tunnel VPN utente attualmente attivo.

Disconnesso (avvio del processo non riuscito):

- Errore di avvio del processo durante il tentativo di connessione al tunnel di gestione.

Disconnesso (connessione non riuscita):

- Errore di connessione durante la definizione del tunnel di gestione.
- Verificare che l'autenticazione del certificato sia configurata nel gruppo del tunnel, che non sia presente alcun banner nei Criteri di gruppo e che il certificato del server sia attendibile.

Disconnesso (configurazione VPN non valida):

- Configurazione non valida del tunneling suddiviso o del protocollo client da ignorare ricevuta dal server VPN.
- Controllare la configurazione nei criteri di gruppo del tunnel di gestione in base alla documentazione.

Disconnesso (aggiornamento software in sospeso):

- Un aggiornamento software AnyConnect è attualmente in sospeso.

Disconnesso:

- Il tunnel di gestione sta per essere stabilito o non può essere stabilito per altri motivi.

[Raccogli DART](#) per ulteriore risoluzione dei problemi.

## Informazioni correlate

- [Configurazione del tunnel VPN di gestione](#)
- [Risoluzione dei problemi del tunnel VPN di gestione](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).