

Configure AnyConnect Management VPN Tunnel on ASA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Working of Management Tunnel](#)

[Limitations](#)

[Configure](#)

[Configuration on ASA through ASDM/CLI](#)

[Creation of AnyConnect Management VPN Profile](#)

[Deployment Methods for AnyConnect Management VPN Profile](#)

[\(Optional\) Configure a Custom Attribute to Support Tunnel-All Configuration](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes configuring ASA as the VPN gateway accepts connections from AnyConnect Secure Mobility Client through Management VPN tunnel.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:


- VPN configuration through Adaptive Security Device Manager (ASDM)
- Basic Adaptive Security Appliance (ASA) CLI Configuration
- X509 Certificates

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA software version 9.12(3)9
- Cisco ASDM software version 7.12.2
- Windows 10 with Cisco AnyConnect Secure Mobility Client version 4.8.03036

 **Note:** Download the AnyConnect VPN Web deploy package (anyconnect-win*.pkg or anyconnect-macos*.pkg)

 from the Cisco [Software Download](#) (registered customers only). Copy the AnyConnect VPN client to the flash memory of the ASA that is to be downloaded to the remote user computers to establish the SSL VPN connection with the ASA. Refer to [Installing the AnyConnect Client](#) section of the ASA configuration guide for more information.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

A management VPN tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts that require corporate network connectivity also benefit from this feature.

AnyConnect Management Tunnel allows administrators to have AnyConnect connected without user intervention prior to when the user logs in. AnyConnect Management tunnel can work in conjunction with Trusted Network Detection and therefore is triggered only when the endpoint is off-premise and disconnected from a User-initiated VPN. AnyConnect Management tunnel is transparent to the end user and disconnects automatically when the user initiates VPN.

OS/Application	Minimum Version Requirements
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect Version	4.7.00136
macOS AnyConnect Version	4.7.01076
Linux	Unsupported

Working of Management Tunnel

AnyConnect VPN agent service is automatically started upon system boot-up. It detects that the management tunnel feature is enabled (via the management VPN profile), therefore it launches the management client application to initiate a management tunnel connection. The management client application uses the host entry from the management VPN profile to initiate the connection. Then the VPN tunnel is established as usual, with one exception: no software update is performed during a management tunnel connection since the management tunnel is meant to be transparent to the user.


The user initiates a VPN tunnel via the AnyConnect UI, which triggers the management tunnel termination. Upon management tunnel termination, the user tunnel establishment continues as usual.

The user disconnects the VPN tunnel, which triggers the automatic re-establishment of the management tunnel.

Limitations

- User interaction is not supported
- Certificate-based authentication through Machine Certificate Store (Windows) is only supported

- Strict Server Certificate checking is enforced
- A private proxy is not supported
- A public proxy is not supported (ProxyNative value is supported on platforms where Native Proxy settings are not retrieved from the browser)
- AnyConnect Customization Scripts are not supported


 **Note:** For more information, refer to [About the Management VPN Tunnel](#).

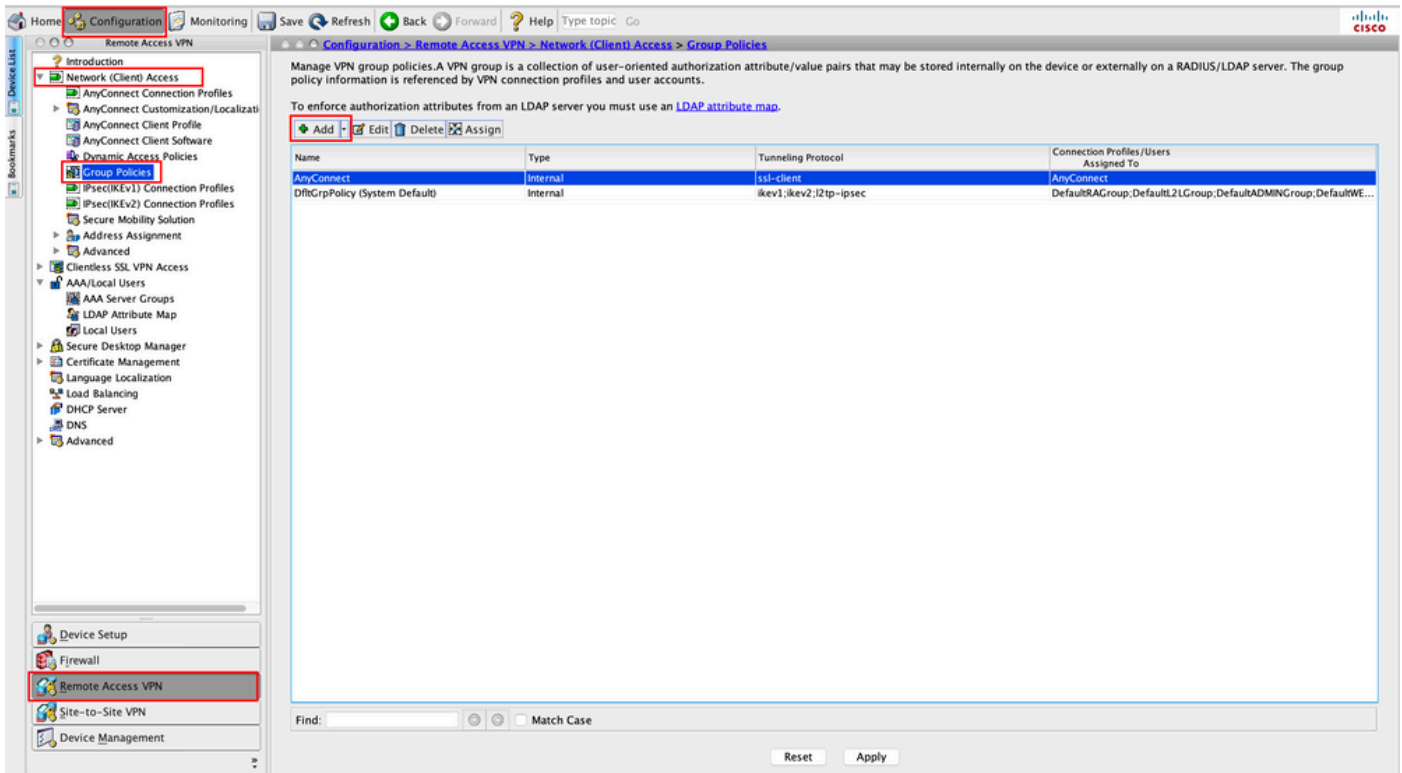
Configure

This section describes how to configure the Cisco ASA as the VPN gateway to accept connections from AnyConnect clients through the Management VPN tunnel.

Configuration on ASA through ASDM/CLI

Step 1. Create the AnyConnect Group Policy. Navigate to Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Click Add.

 **Note:** It is advisable to create a new AnyConnect Group Policy which is used for the AnyConnect Management tunnel only.



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](#).

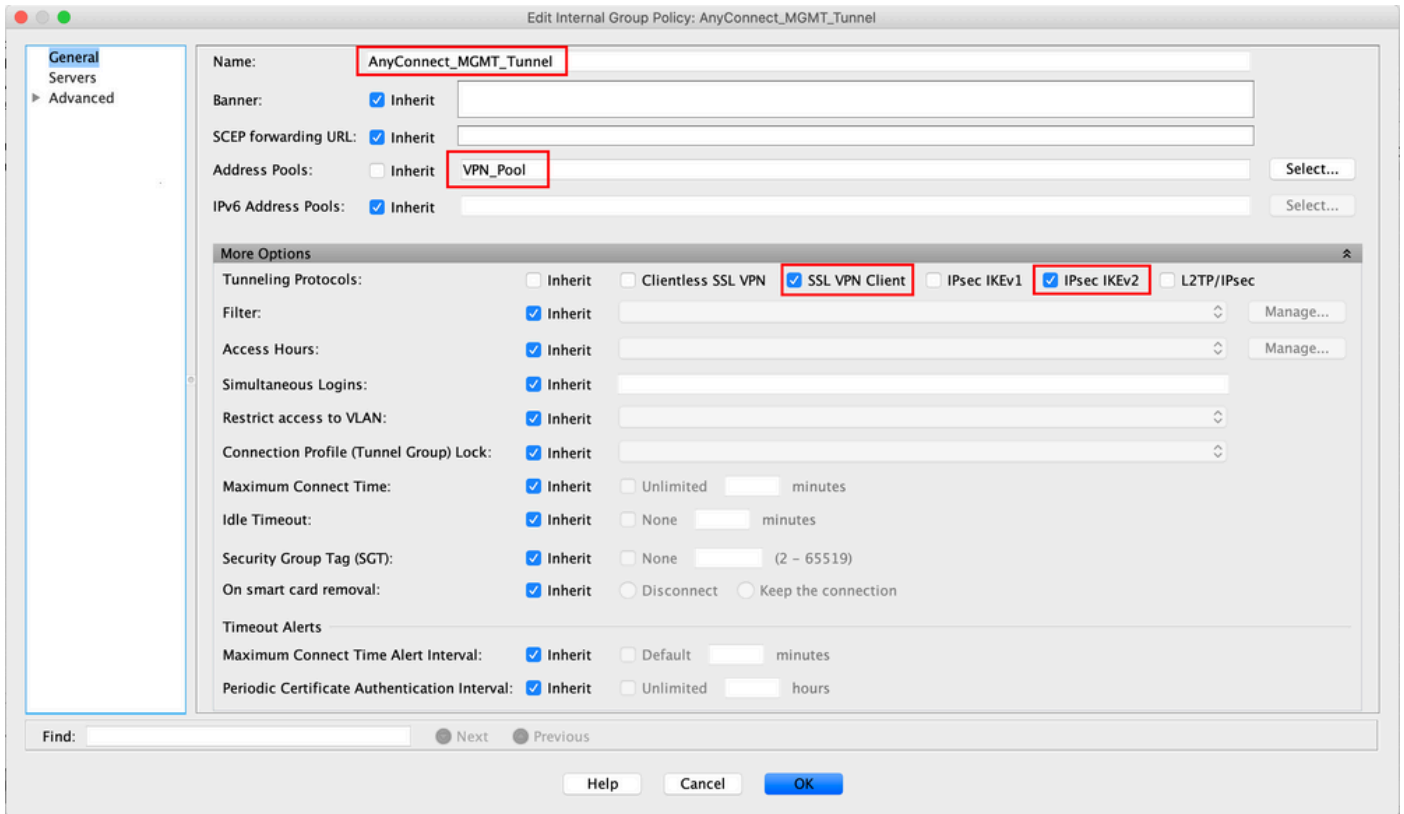
Add Edit Delete Assign

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...

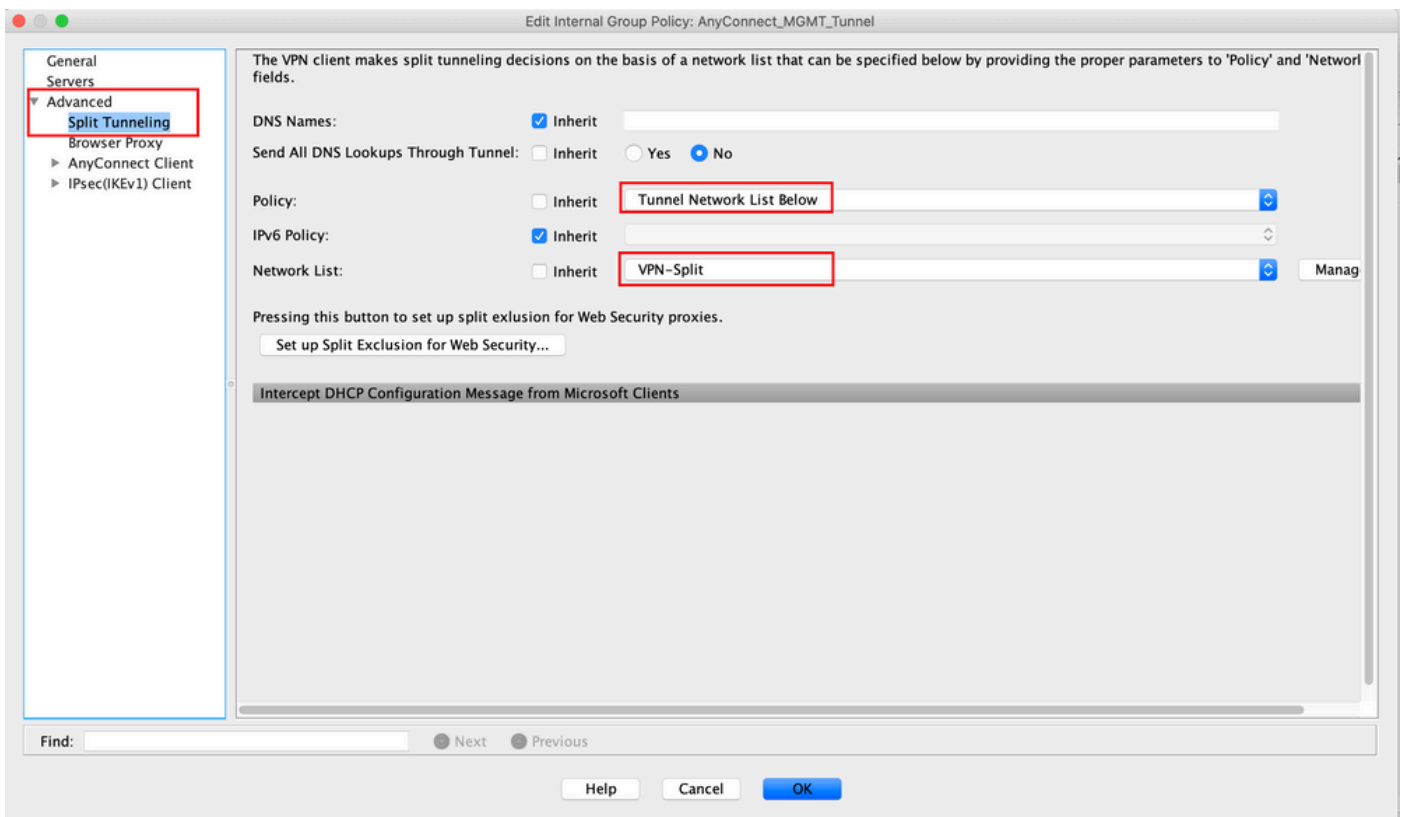
Find: Match Case

Reset Apply

Step 2. Provide a Name for the Group Policy. Assign/Create an Address Pool. Choose Tunneling Protocols as SSL VPN Client and/or IPsec IKEv2, as shown in the image.

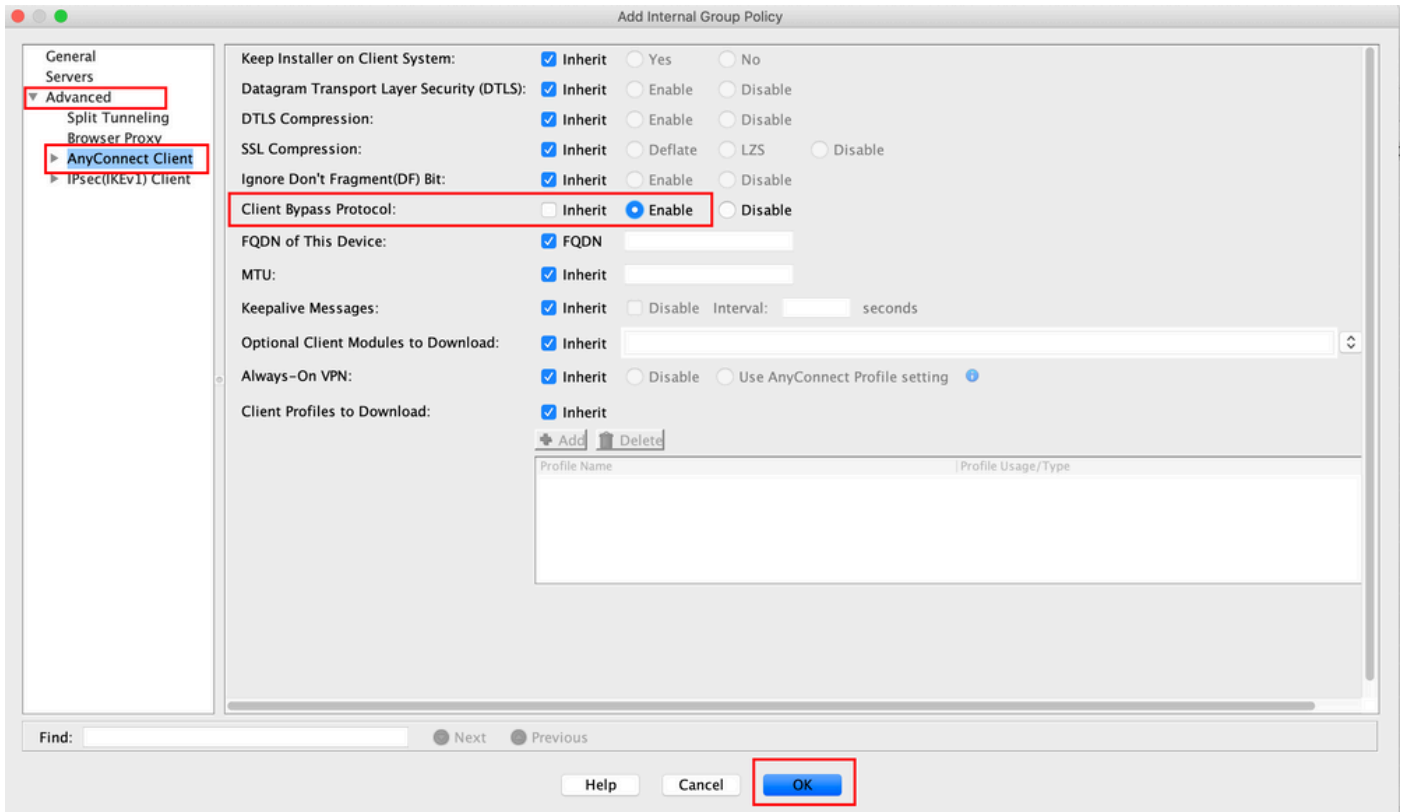


Step 3. Navigate to **Advanced > Split Tunneling**. Configure the Policy as **Tunnel Network List Below** and choose the **Network List**, as shown in the image.

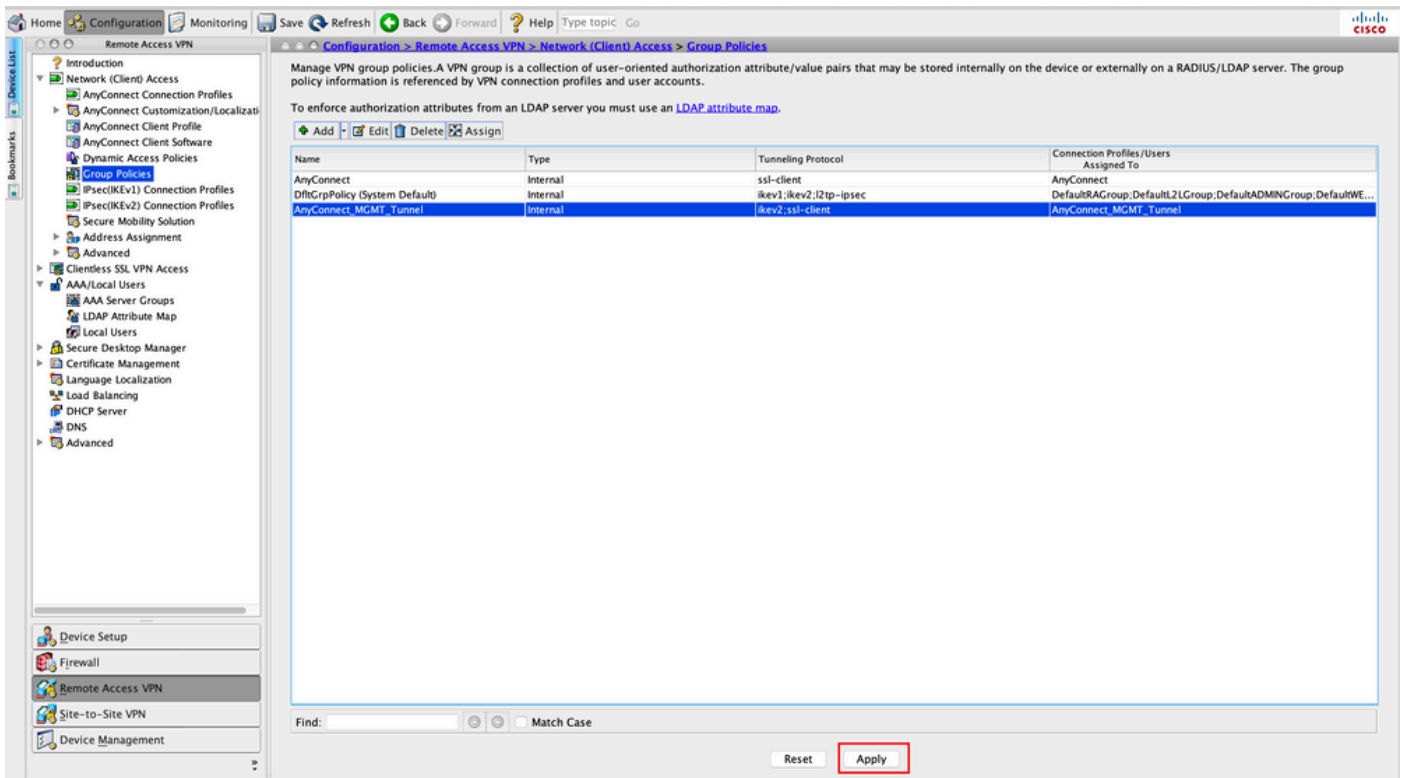


Note: If a client address is not pushed for both IP protocols (IPv4 and IPv6), the **Client Bypass Protocol** setting must be enabled so that the traffic that corresponds is not disrupted by the management tunnel. To configure, refer to [Step 4](#).

Step 4. Navigate to **Advanced > AnyConnect Client**. Set **Client Bypass Protocol** to **Enable**. Click **OK** to Save, as shown in the image.



Step 5. As shown in this image, click **Apply** to push the configuration to the ASA.



CLI Configuration for Group Policy:

```
<#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
```

Step 6. Create the AnyConnect Connection Profile. Navigate to [Configuration > Remote Access VPN > Network \(Client\) Access > AnyConnect Connection Profile](#). Click **Add**.



Note: It is advisable to create a new AnyConnect Connection Profile which is used for the AnyConnect Management tunnel only.

The screenshot shows the Cisco AnyConnect configuration interface. The left sidebar contains a navigation tree with 'Remote Access VPN' selected. The main content area is titled 'AnyConnect Connection Profiles' and includes the following sections:

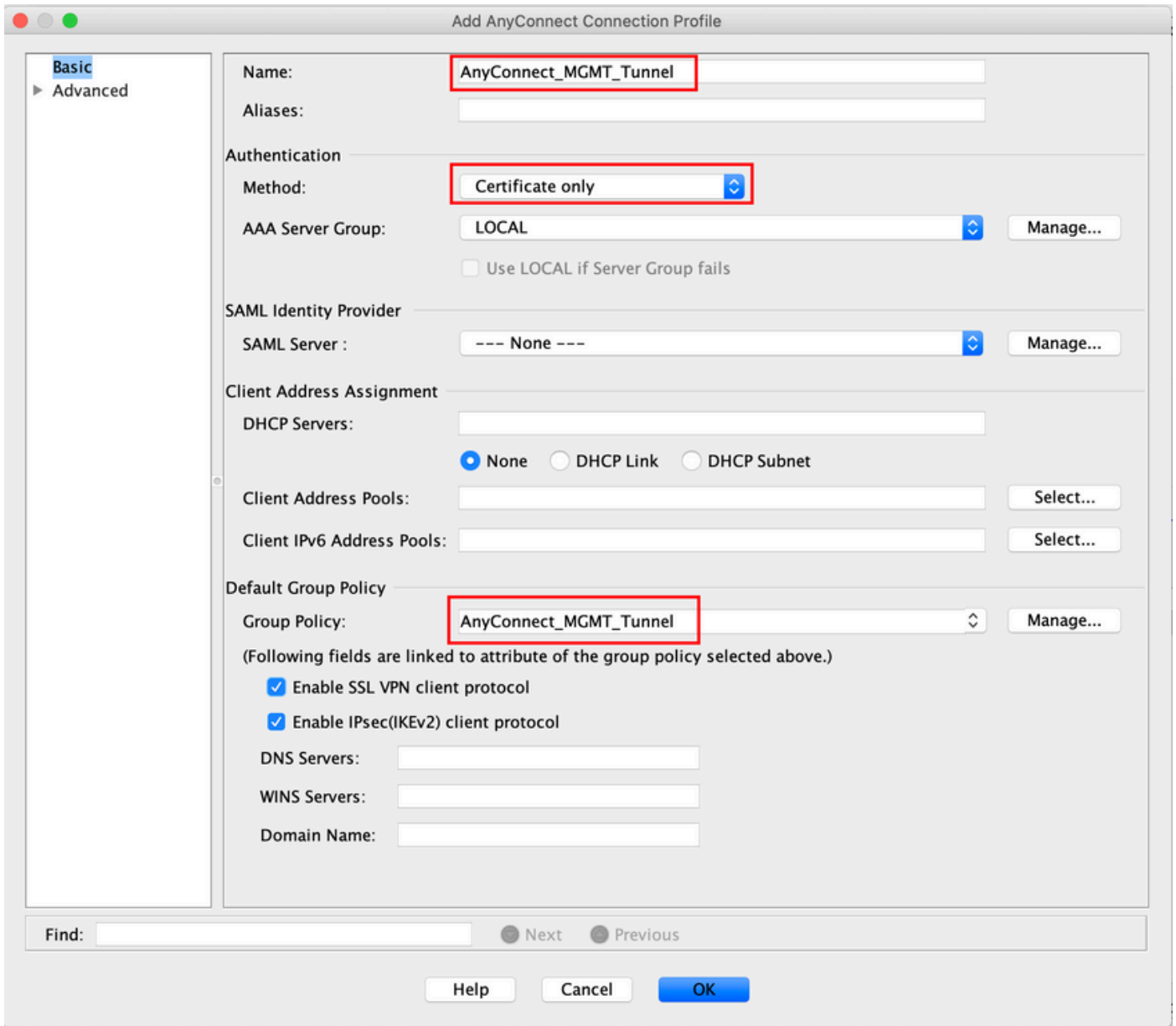
- Access Interfaces:** A table for configuring interface access.

Interface	SSL Access	Enable DTLS	IPsec (IKEv2) Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Login Page Setting:**
 - Allow user to select connection profile on the login page.
 - Shutdown portal login page.
- Connection Profiles:** A table for defining connection profiles.

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(Local)	DfltGrpPolicy
DefaultWEBVNGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(Local)	DfltGrpPolicy
AnyConnect	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyConnect	AAA(Local)	AnyConnect

Buttons for 'Device Certificate ...' and 'Port Settings ...' are visible. At the bottom, there are 'Reset' and 'Apply' buttons.

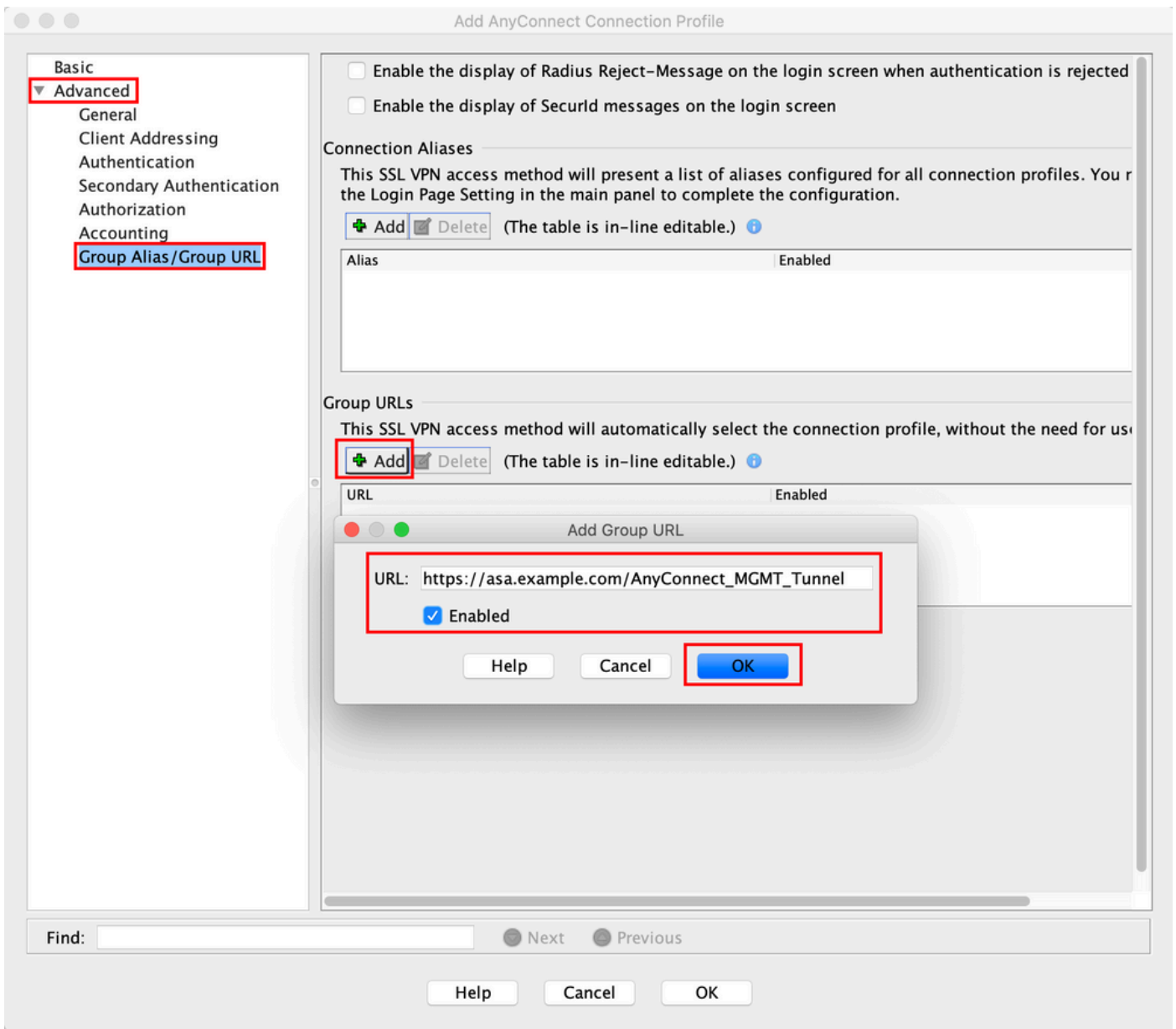
Step 7. Provide a Name for the Connection Profile, and set Authentication Method as Certificate only. Choose the Group Policy as the one created in [Step 1](#).



Note: Ensure that the Root certificate from Local CA is present on the ASA. Navigate to Configuration > Remote Access VPN > Certificate Management > CA Certificates to add/view the certificate.

Note: Ensure that an Identity certificate issued by the same Local CA exists in the Machine Certificate Store (For Windows) and/or in System Keychain (For macOS).

Step 8. Navigate to Advanced > Group Alias/Group URL. Click Add under Group URLs and add an URL. Ensure Enabled is checked. Click OK to Save, as shown in the image.



If IKEv2 is used, ensure IPsec (IKEv2) Access is enabled on the interface used for AnyConnect.



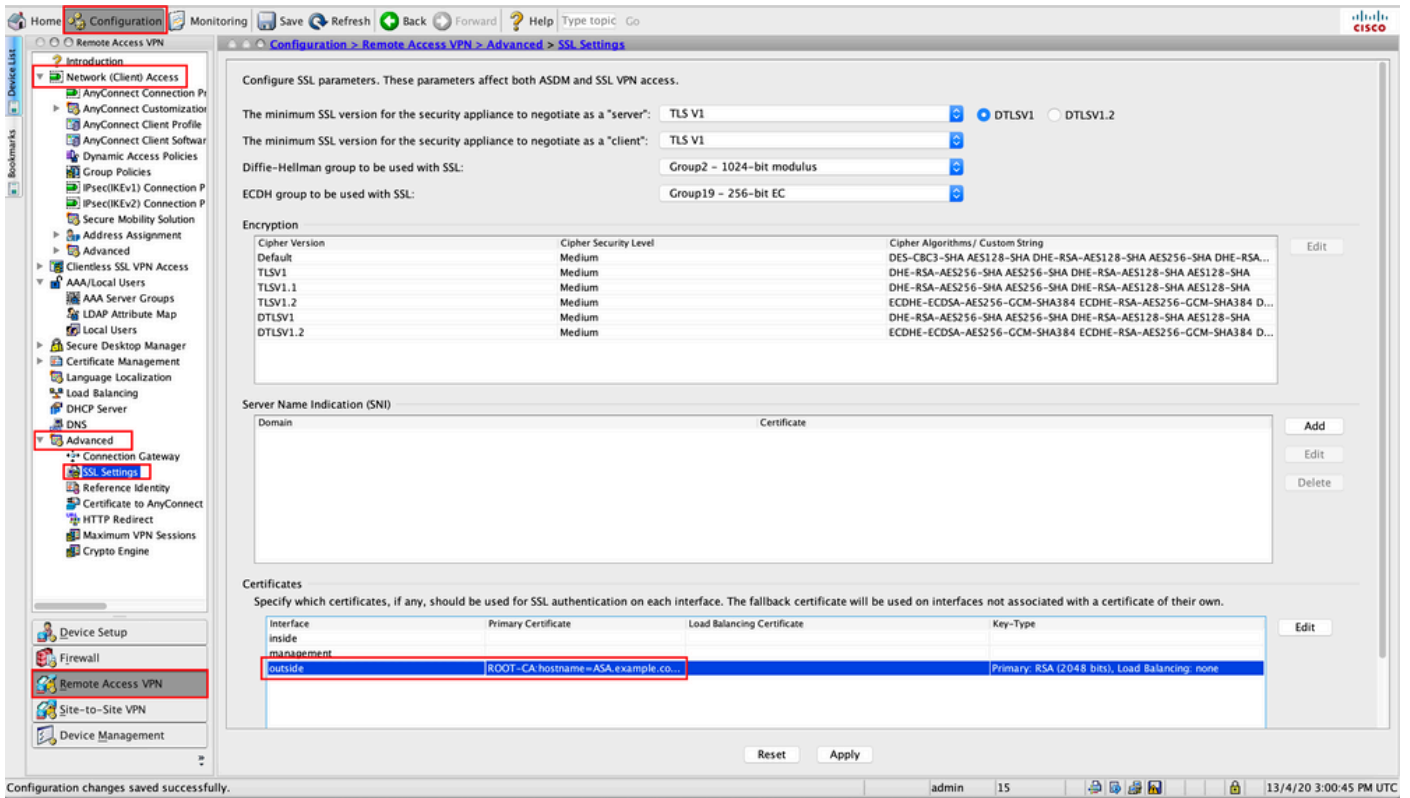
Step 9. Click Apply to push the configuration to the ASA.

CLI configuration for connection profile (tunnel-group):

```
<#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
```

Step 10. Ensure that a trusted certificate is installed on the ASA and bound to the interface used for AnyConnect connections. Navigate to Configuration > Remote Access VPN > Advanced > SSL Settings to add/view this setting.

 **Note:** Refer to [Installation of Identity Certificate on ASA](#).



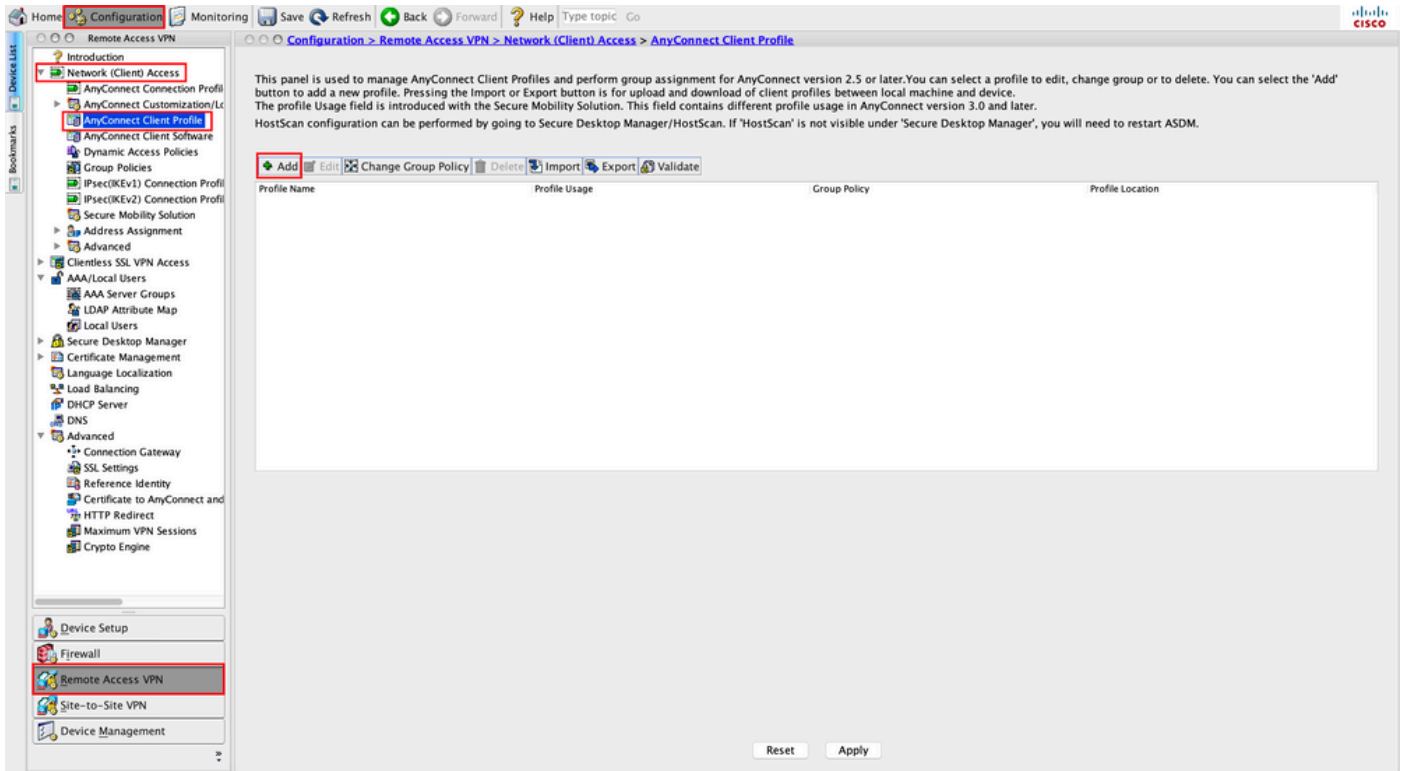
CLI Configuration for SSL Trustpoint:

```
<#root>
```

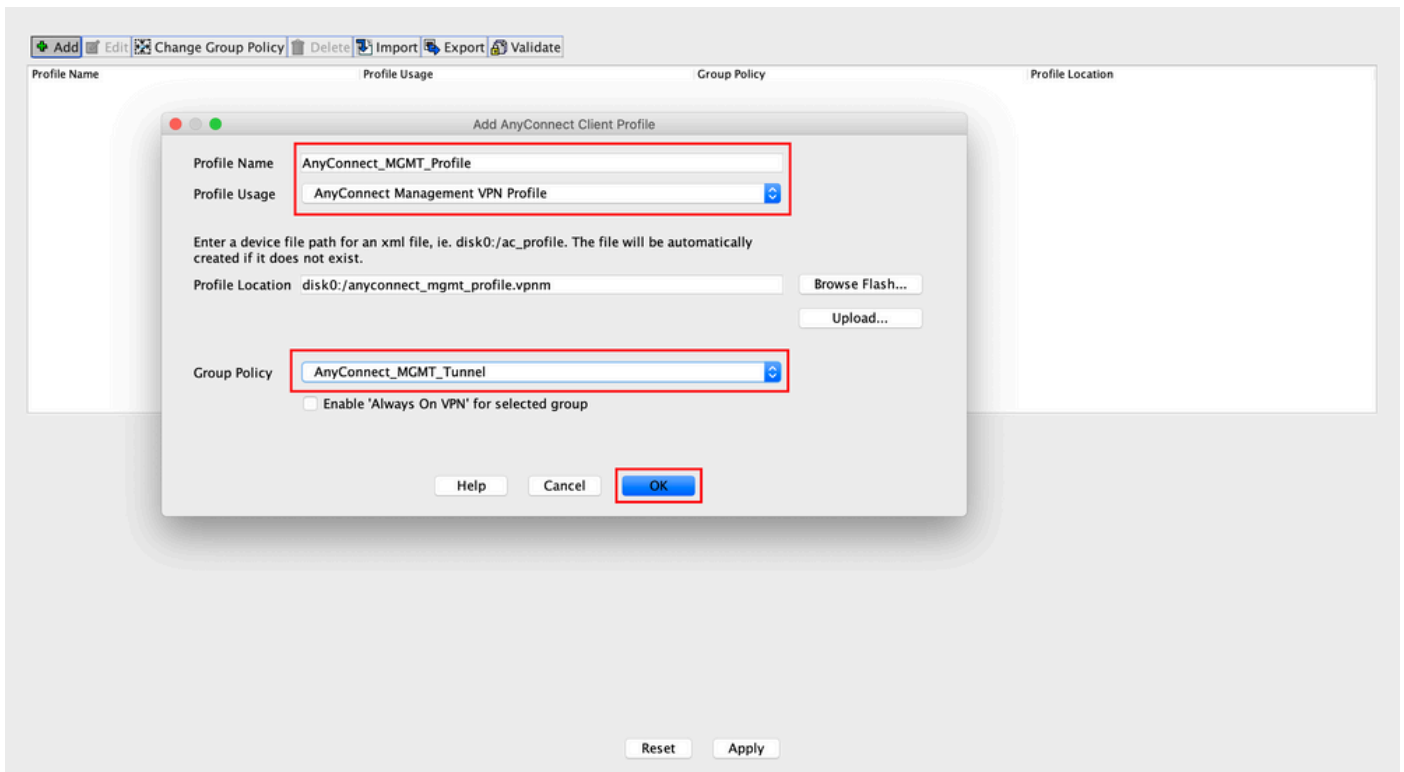
```
ssl trust-point ROOT-CA outside
```

Creation of AnyConnect Management VPN Profile

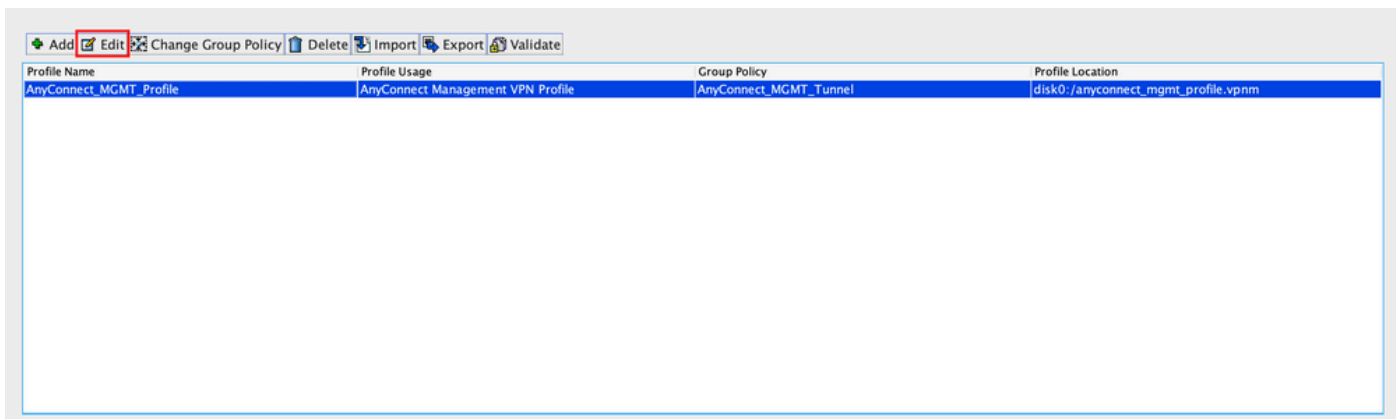
Step 1. Create the AnyConnect Client Profile. Navigate to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Click Add, as shown in the image.



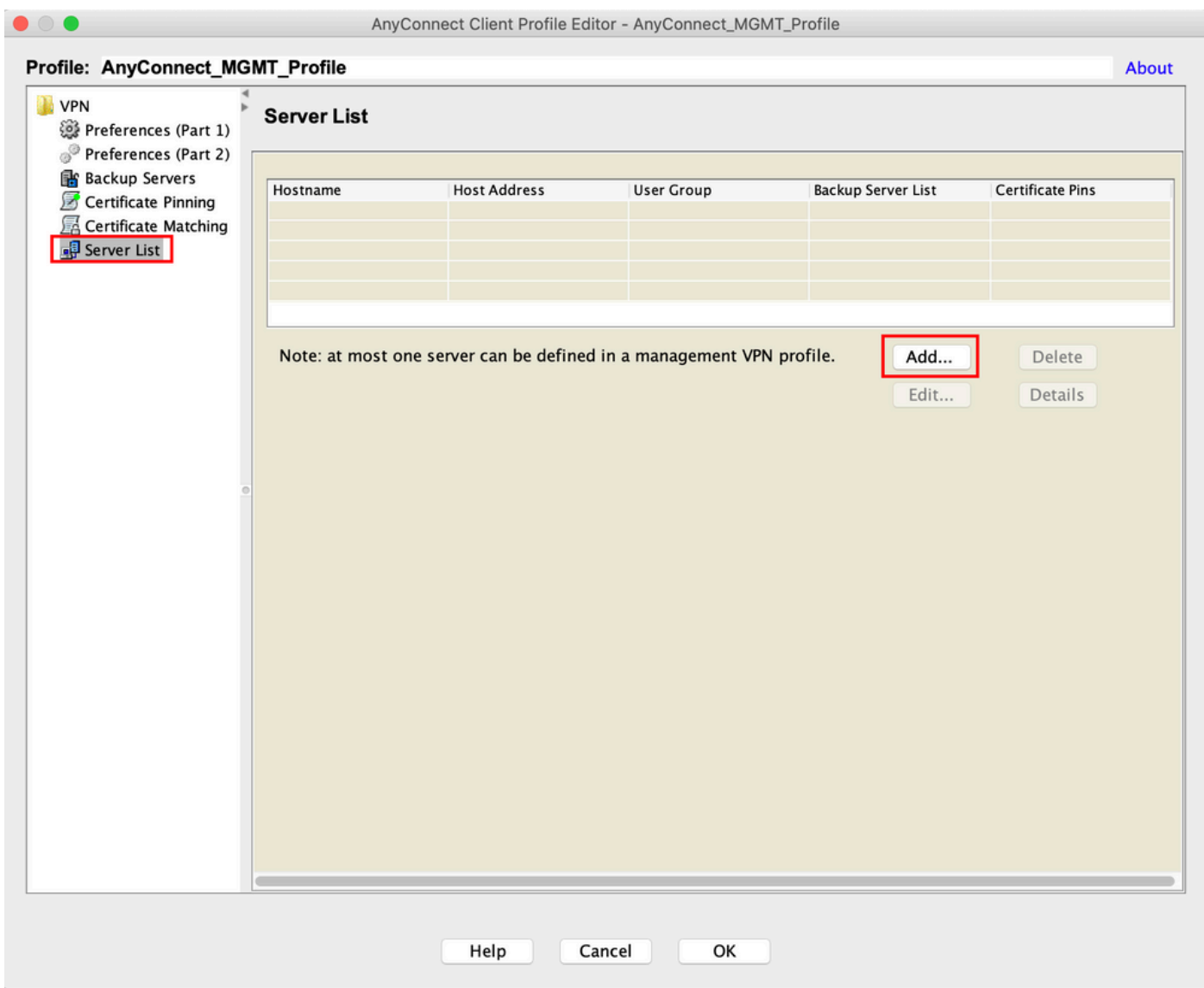
Step 2. Provide a Profile Name. Choose the Profile Usage as AnyConnect Management VPN profile. Choose the Group Policy created in [Step 1](#). Click **OK**, as shown in the image.



Step 3. Choose the Profile created and click **Edit**, as shown in the image.



Step 4. Navigate to **Server List**. Click **Add** to add a new Server List Entry, as shown in the image.



Step 5. Provide a **Display Name**. Add the **FQDN/IP address** of the ASA. Provide the **User Group** as the tunnel group name. **Group URL** is automatically populated with the **FQDN** and **User Group**. Click **OK**.

Server Certificate Pinning

Primary Server

Display Name (required)

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

Group URL

Connection Information

Primary Protocol


ASA gateway


Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

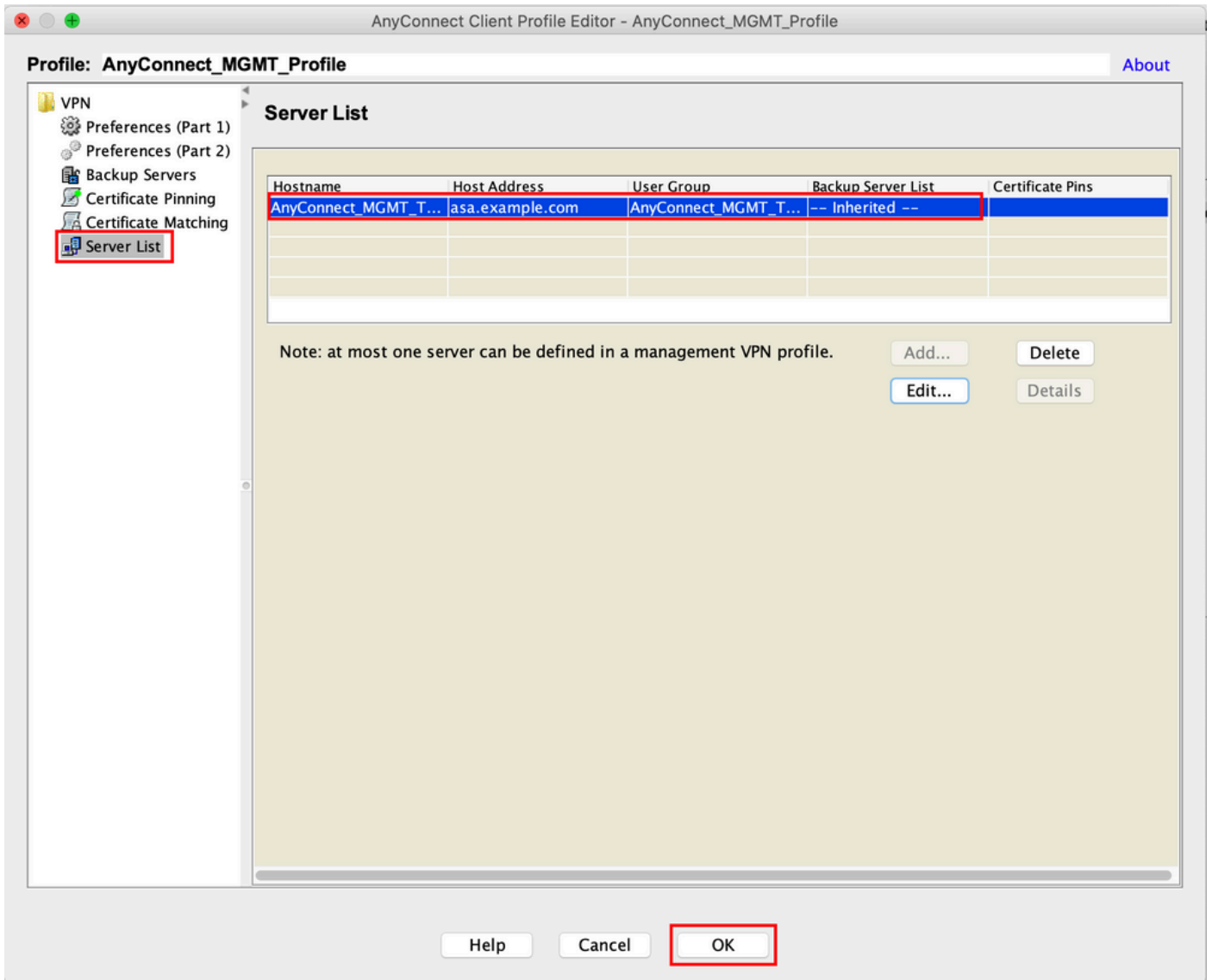
Backup Servers

Host Address

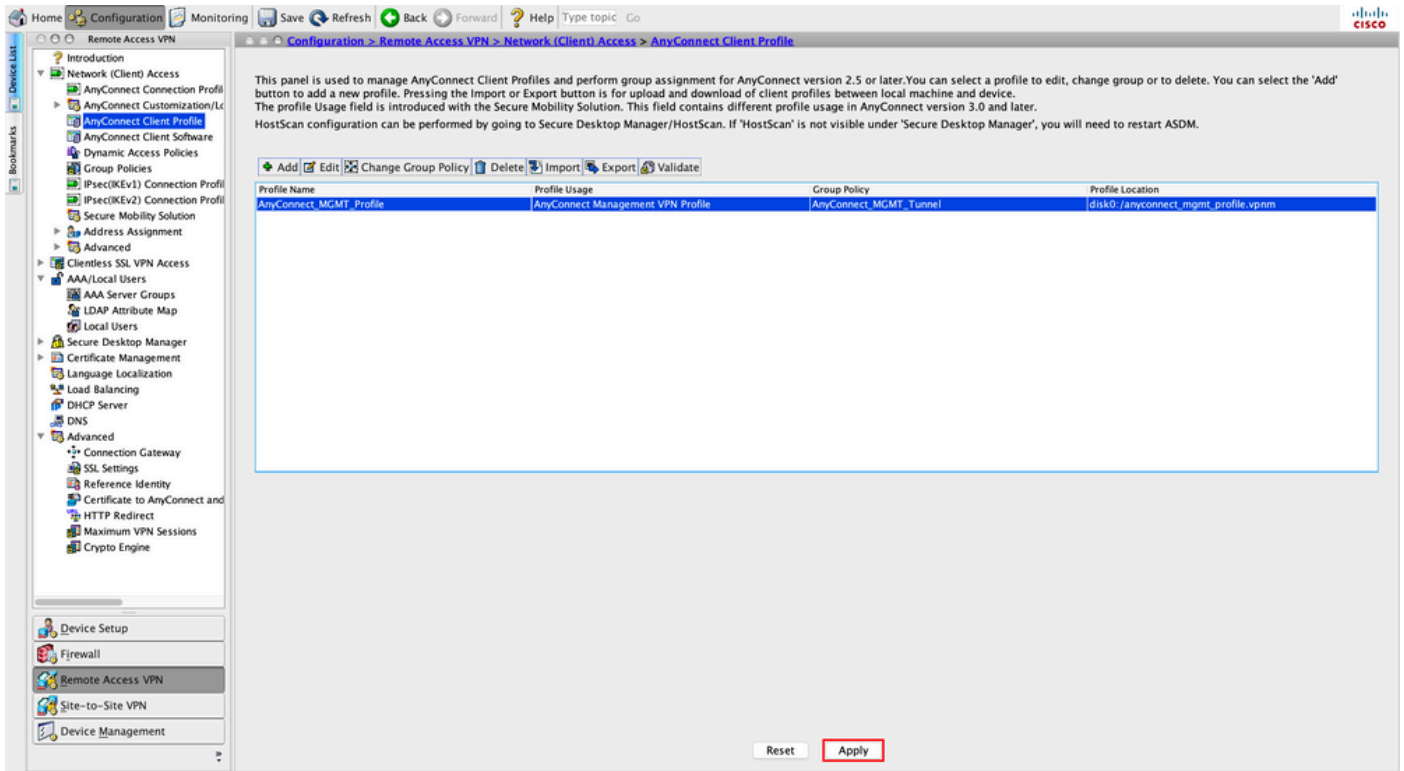
 **Note:** The FQDN/IP Address + User Group must be the same as the Group URL mentioned during the configuration of the AnyConnect Connection Profile in [Step 8](#).

 **Note:** AnyConnect with IKEv2 as a protocol can also be used to establish Management VPN to ASA. Ensure Primary Protocol is set to IPsec in [Step 5](#).

Step 6. As shown in the image, click OK to Save.



Step 7. Click `Apply` to push the configuration to the ASA, as shown in the image.



CLI Configuration after the addition of AnyConnect Management VPN Profile.

```
<#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
```


AnyConnect Management VPN Profile on AnyConnect Client Machine:

```
<#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 UserControllable="false">false</UseStartBeforeLogon>

    <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>

    <ShowPreConnectMessage>false</ShowPreConnectMessage>

    <CertificateStore>Machine</CertificateStore>
    <CertificateStoreMac>System</CertificateStoreMac>
    <CertificateStoreOverride>true</CertificateStoreOverride>

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


--- Output Omitted ---


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


<ServerList>
  <HostEntry>
    <HostName>AnyConnect_MGMT_Tunnel</HostName>
    <HostAddress>asa.example.com</HostAddress>
    <UserGroup>AnyConnect_MGMT_Tunnel</UserGroup>
  </HostEntry>

</ServerList>

</AnyConnectProfile>
```

 **Note:** If Trusted Network Detection (TND) is used in the User AnyConnect VPN profile, it is advisable to match the same settings in the Management VPN Profile for a consistent user experience. The management VPN tunnel is triggered based on the TND settings applied to the User VPN tunnel profile. Additionally, the TND Connect action in the management VPN profile (enforced only when the management VPN tunnel is active), always applies to the user VPN tunnel, to ensure that the management VPN tunnel is transparent to the end user.


 **Note:** On any end-user PC, if the Management VPN profile has the TND settings enabled and if the user VPN profile is missing, it considers the default preferences settings for the TND (it is disabled on the default preferences in the AC client application) in place of missing user VPN profile. This mismatch can lead to unexpected/undefined behavior. By default, TND settings are disabled in the default preferences. To overcome the default preferences hardcoded settings in the AnyConnect Client application, the

 end-user PC must have two VPN profiles, a user VPN profile & an AC Management VPN profile, and both of them must have the same TND settings.

The logic behind Management VPN tunnel connection and disconnection is that to establish a Management VPN tunnel, the AC agent uses the user VPN profile TND settings and for disconnection of the Management VPN tunnel, it checks for management VPN profile TND settings.

Deployment Methods for AnyConnect Management VPN Profile

- A successful User VPN connection is completed with the ASA Connection Profile in order to download the AnyConnect Management VPN Profile from the VPN Gateway.

 **Note:** If the protocol used for the Management VPN tunnel is IKEv2, the first connection is needed to be established through SSL (In order to download the AnyConnect Management VPN profile from the ASA).

- The AnyConnect Management VPN Profile can be manually uploaded to the client machines either through a GPO push or by manual installation (Ensure the name of the profile is VpnMgmtTunProfile.xml).

Location of Folder where the profile needs to be added:

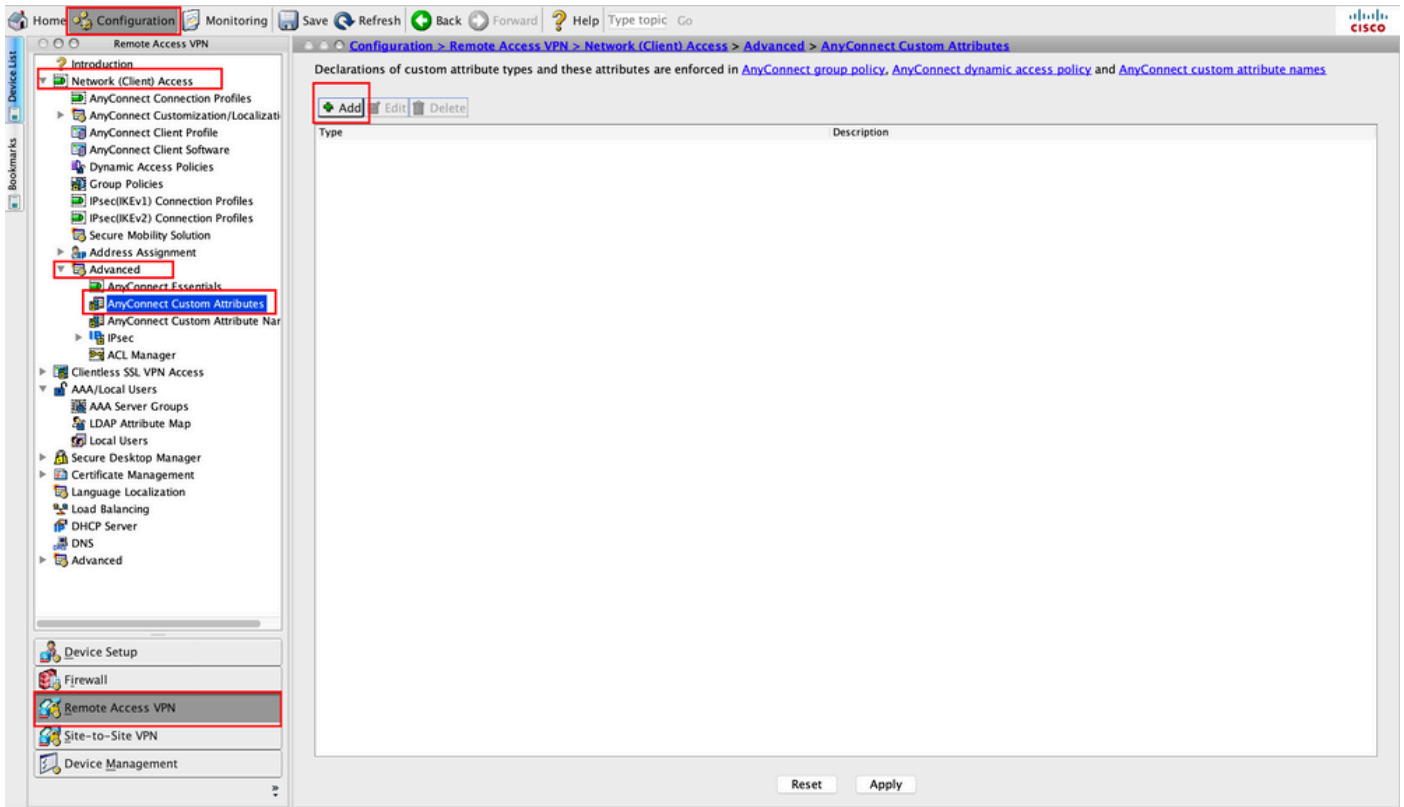
Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun

macOS: /opt/cisco/anyconnect/profile/mgmttun/

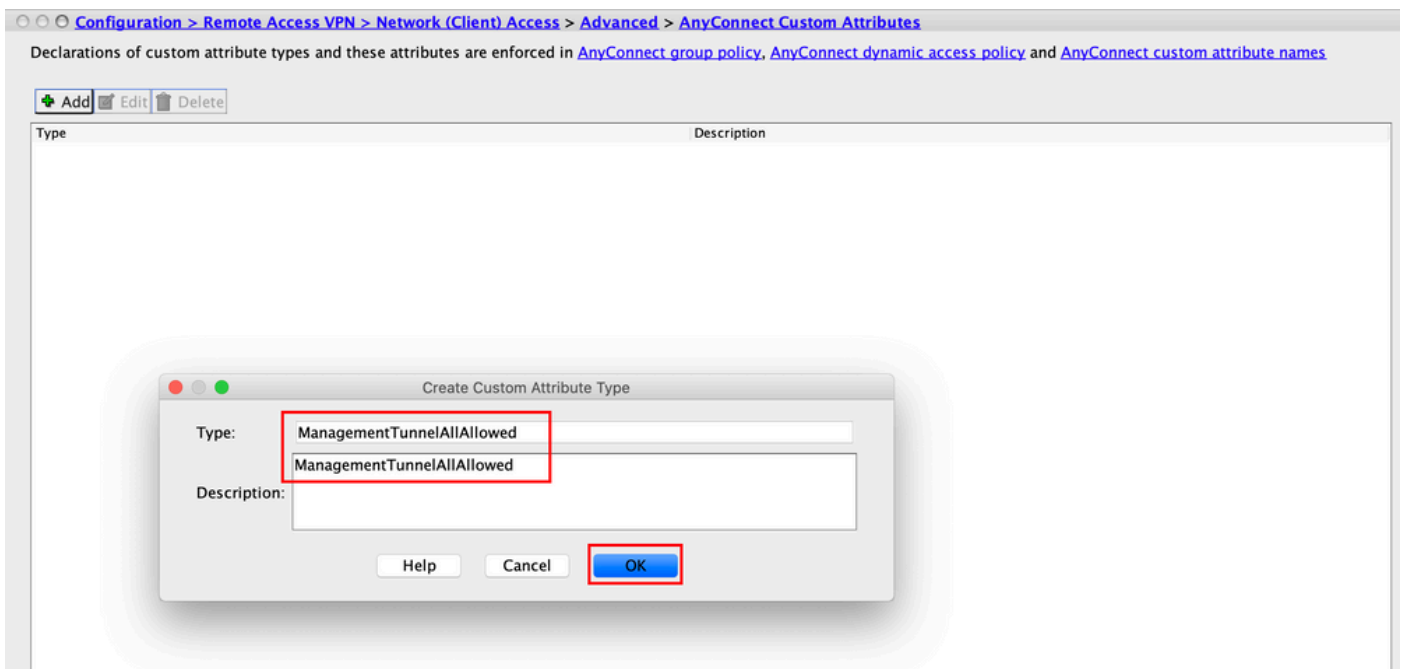
(Optional) Configure a Custom Attribute to Support Tunnel-All Configuration

Management VPN tunnel requires a split that includes tunneling configuration, by default, to avoid an impact on the user-initiated network communication. This can be overridden when you configure the custom attribute in the group policy used by the management tunnel connection.

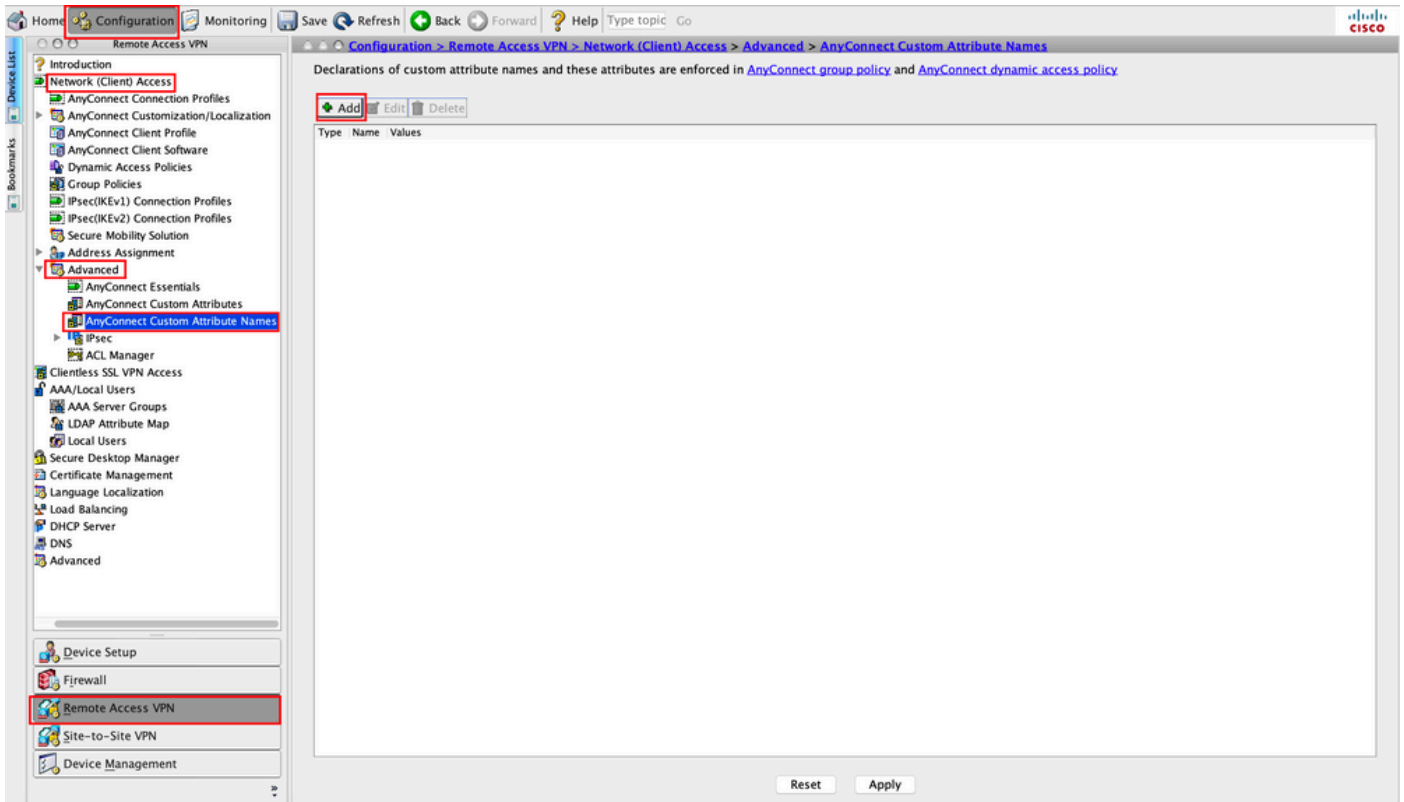
Step 1. Navigate to Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Click Add, as shown in the image.



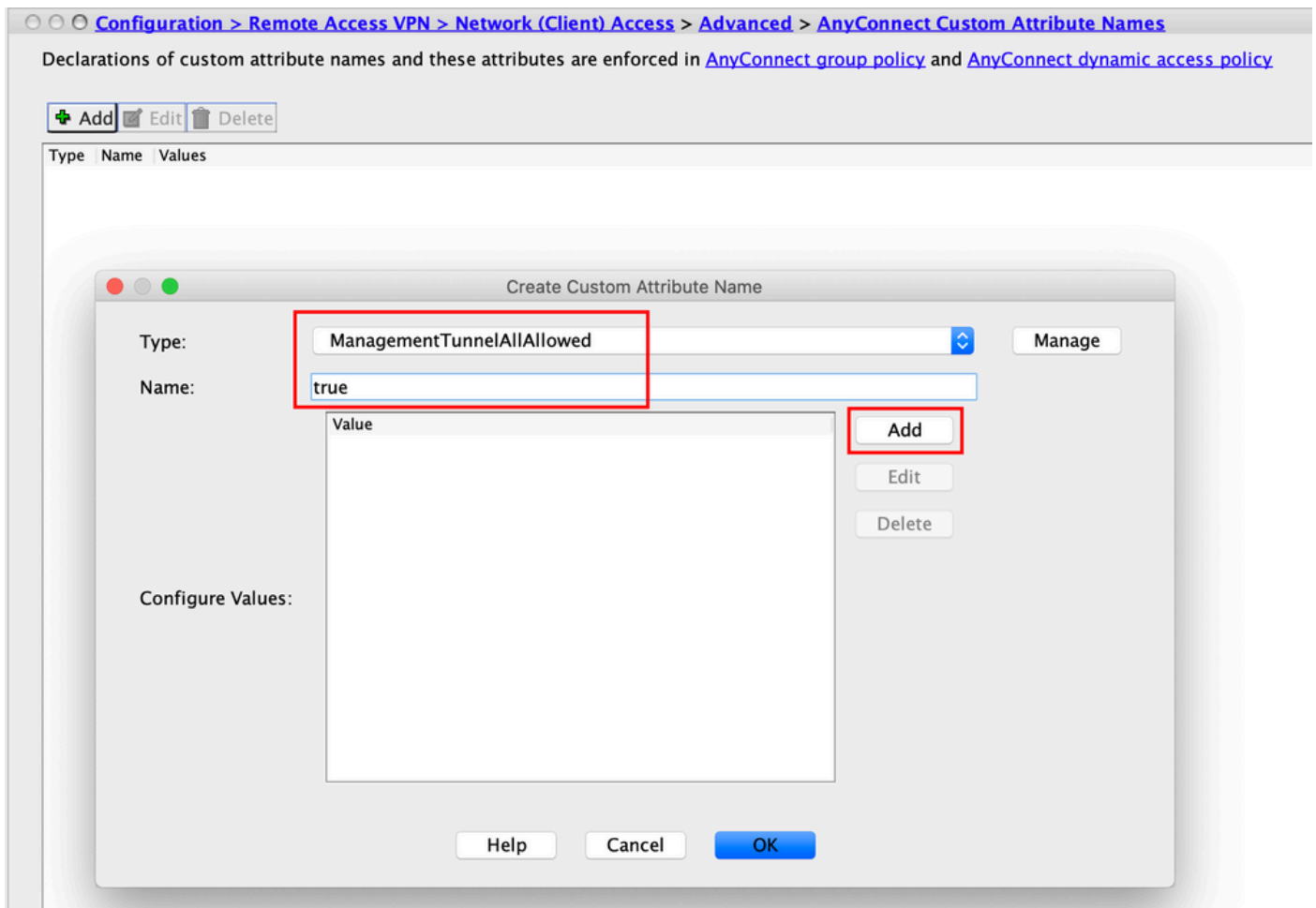
Step 2. Set the custom attribute Type to ManagementTunnelAllAllowed and provide a Description. Click OK, as shown in the image.



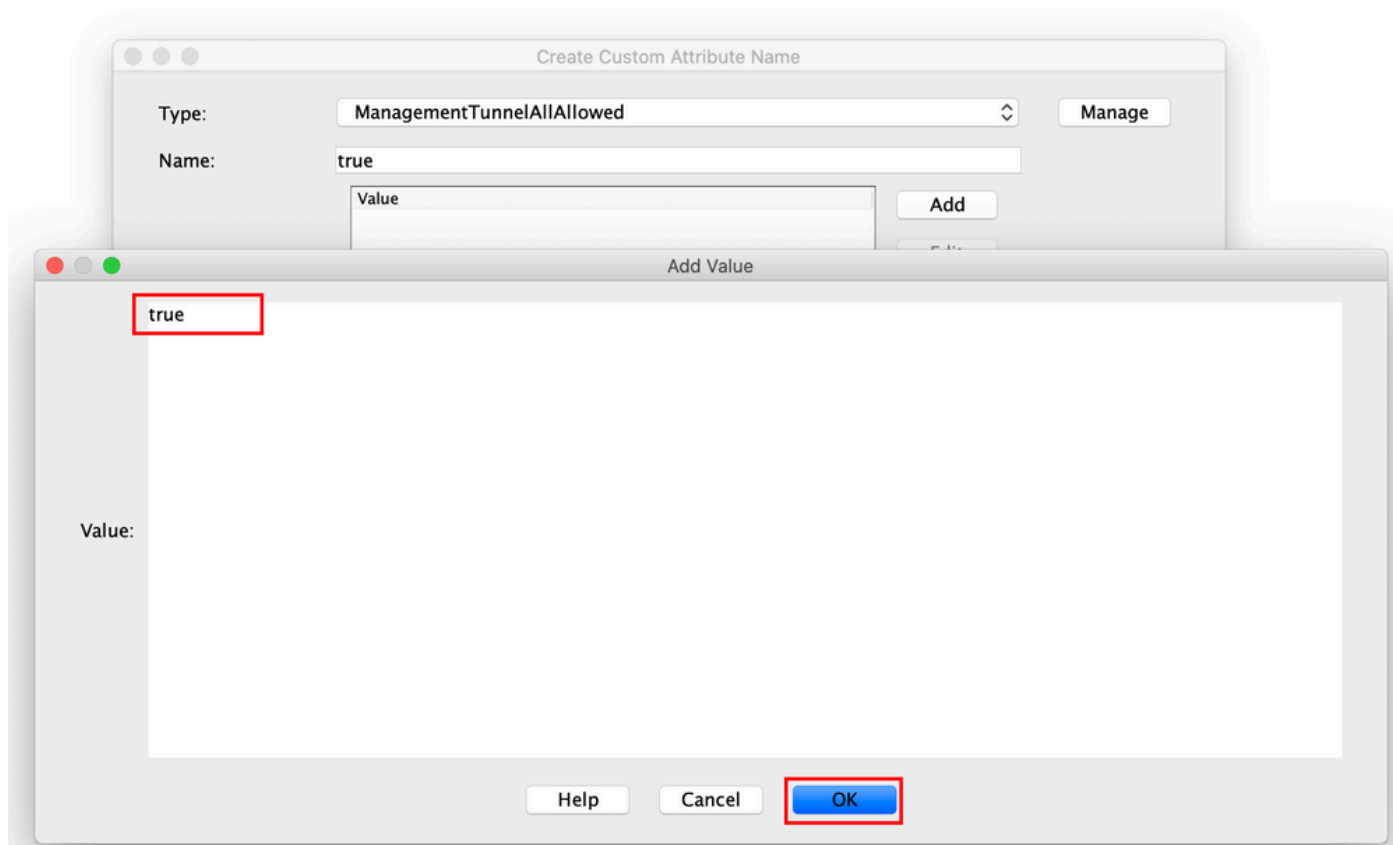
Step 3. Navigate to Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Click Add, as shown in the image.



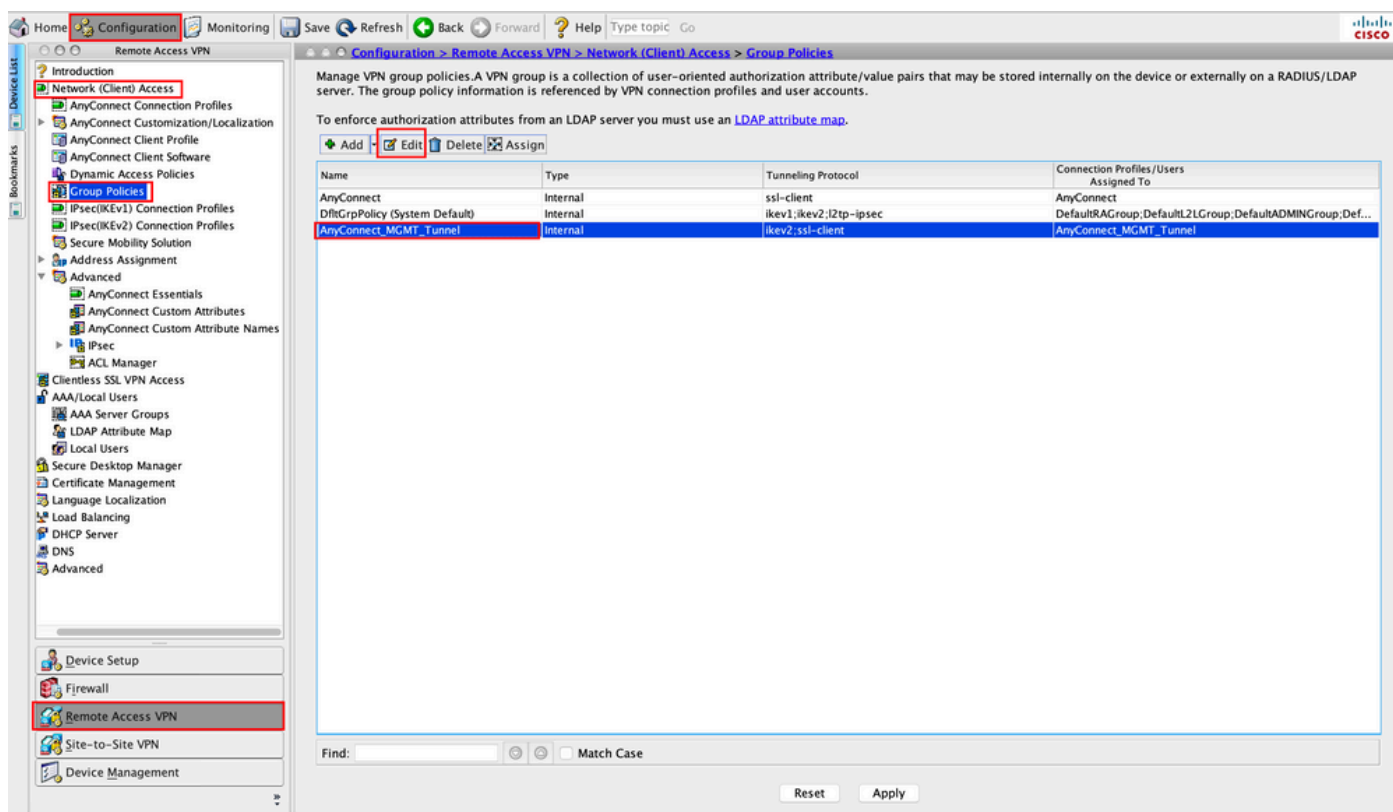
Step 4. Choose the Type as `ManagementTunnelAllAllowed`. Set the Name as `true`. Click `Add` to provide a custom attribute value, as shown in the image.



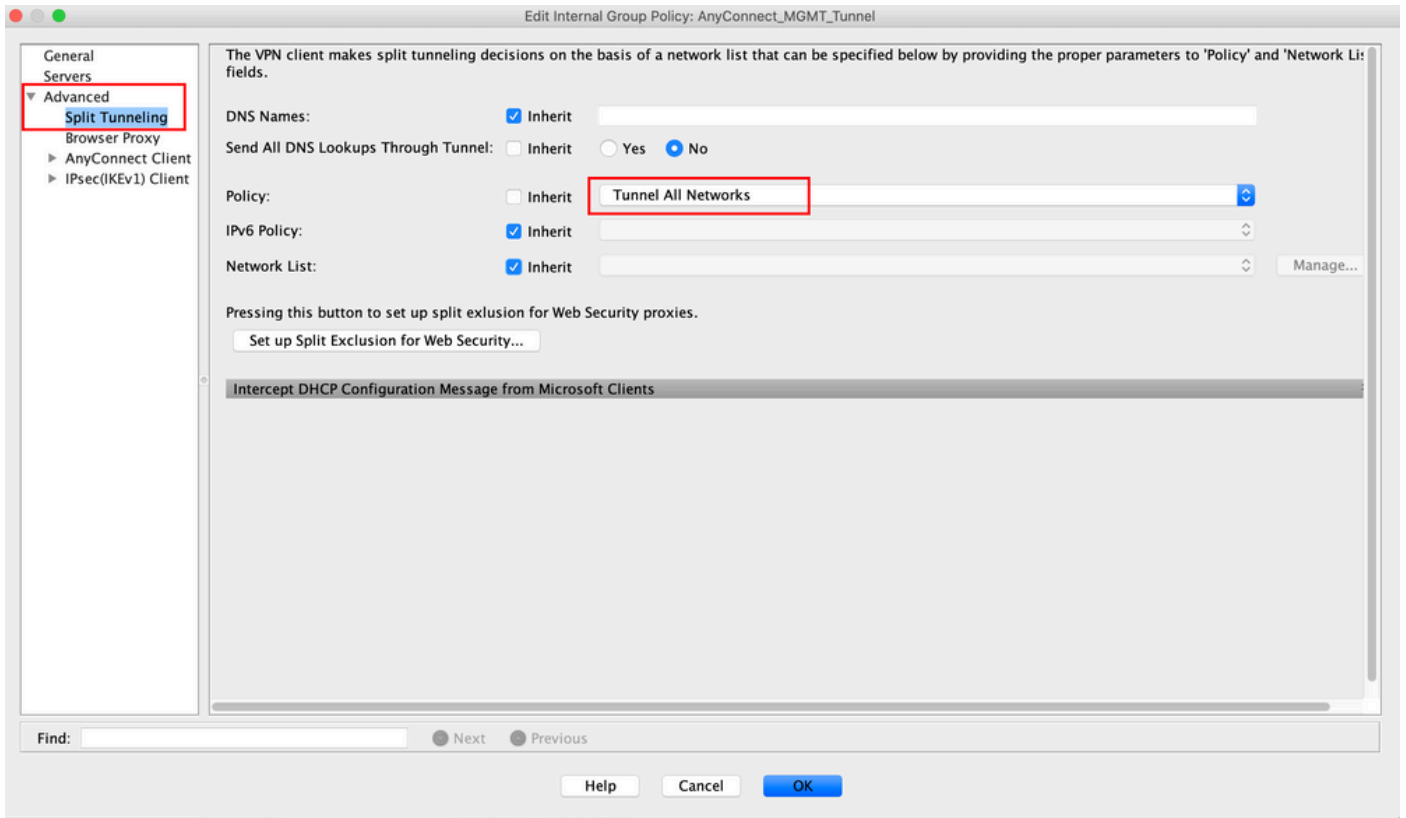
Step 5. Set the Value as `true`. Click `OK`, as shown in the image.



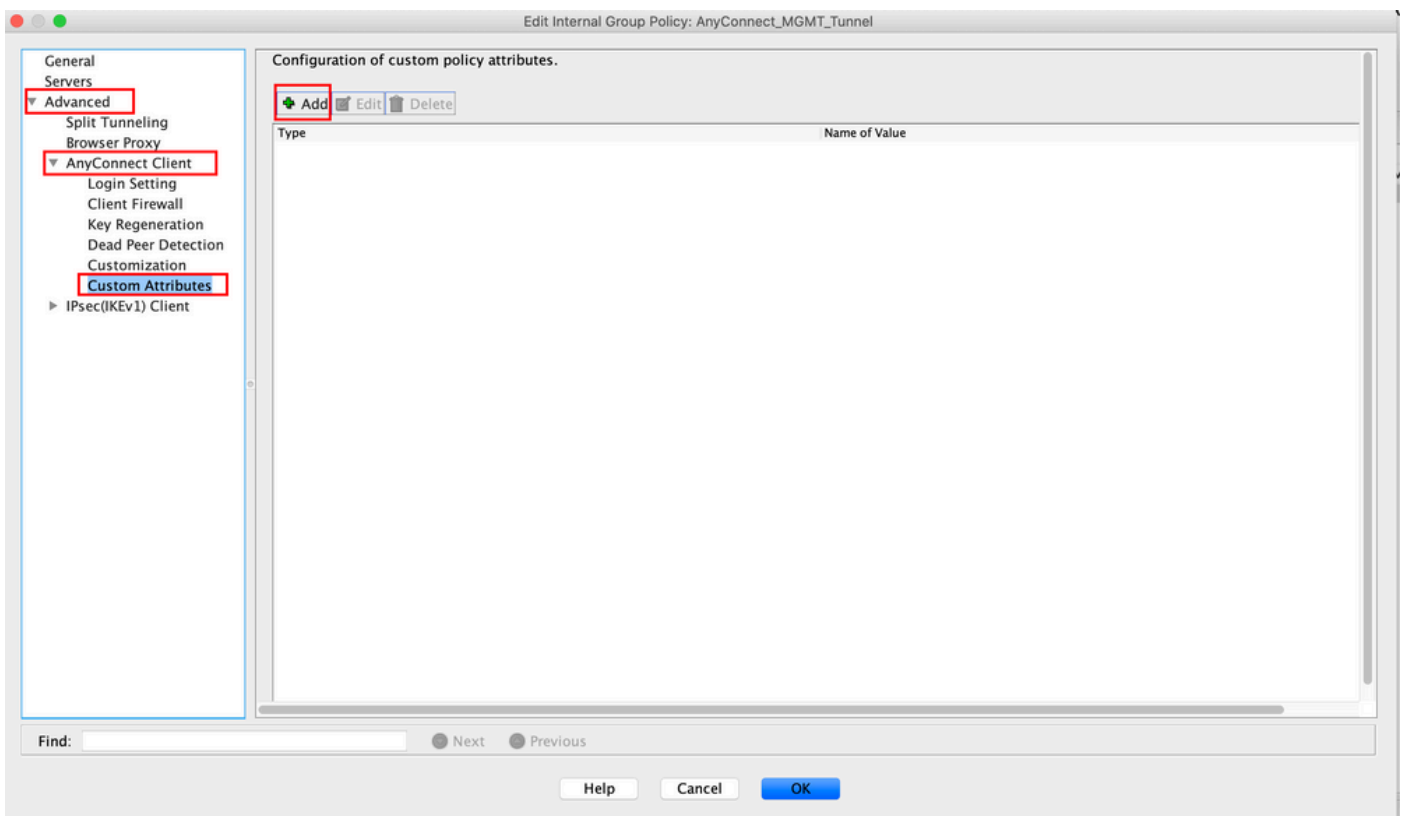
Step 6. Navigate to `Configuration > Remote Access VPN > Network (Client) Access > Group Policies`. Choose the Group Policy. Click `Edit`, as shown in the image.



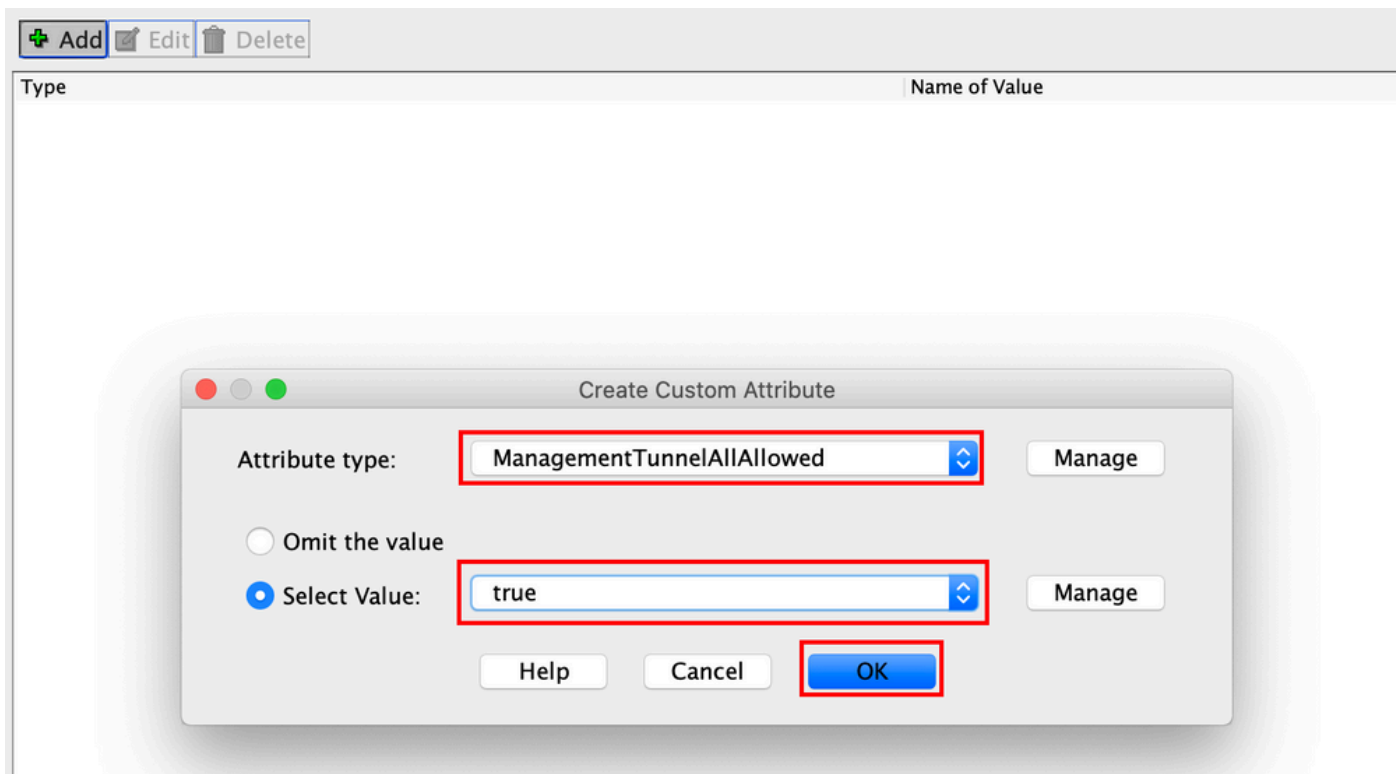
Step 7. As shown in this image, navigate to `Advanced > Split Tunneling`. Configure the Policy as `Tunnel All Networks`.



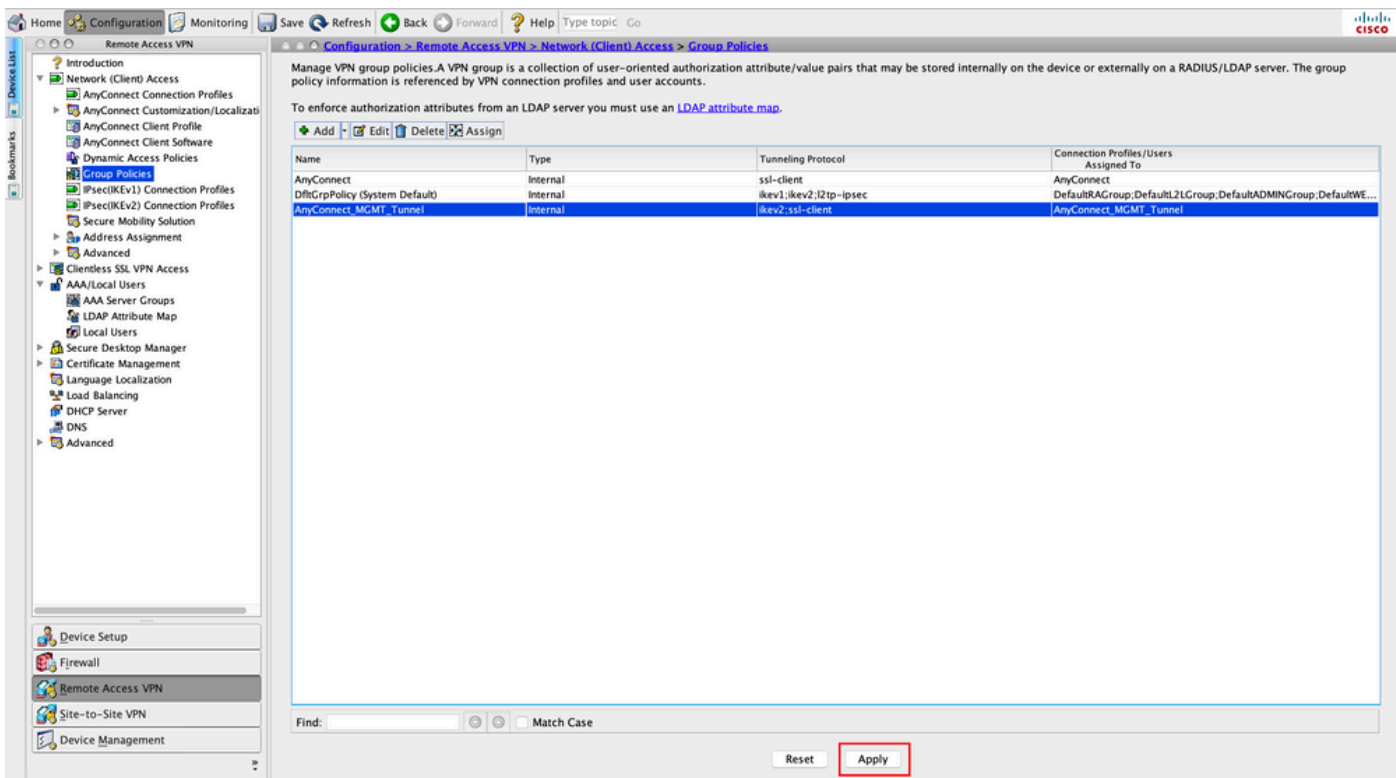
Step 8. Navigate to **Advanced > Anyconnect Client > Custom Attributes**. Click **Add**, as shown in the image.



Step 9. Choose the Attribute type as **ManagementTunnelAllAllowed** and choose the Value as **true**. Click **OK**, as shown in the image.



Step 10. Click **Apply** to push the configuration to the ASA, as shown in the image.



CLI Configuration after the `ManagementTunnelAllAllowed` Custom Attribute is added:

```
<#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

```

Verify

Verify the Management VPN tunnel connection on ASA CLI with the `show vpn-sessiondb detail anyconnect` command.

```
<#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:

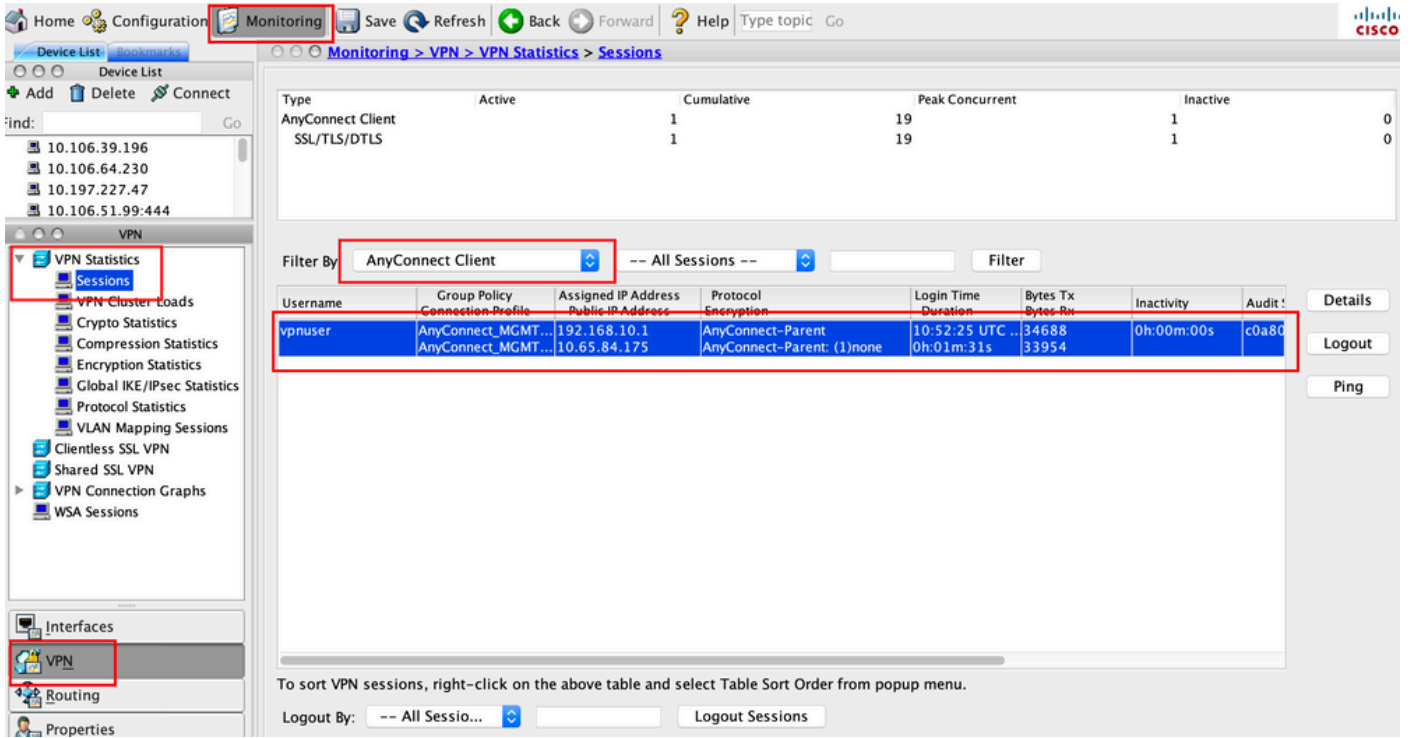
Tunnel ID : 10.3
Assigned IP : 192.168.10.1 Public IP : 10.65.84.175
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 57053
UDP Dst Port : 443

Auth Mode : Certificate

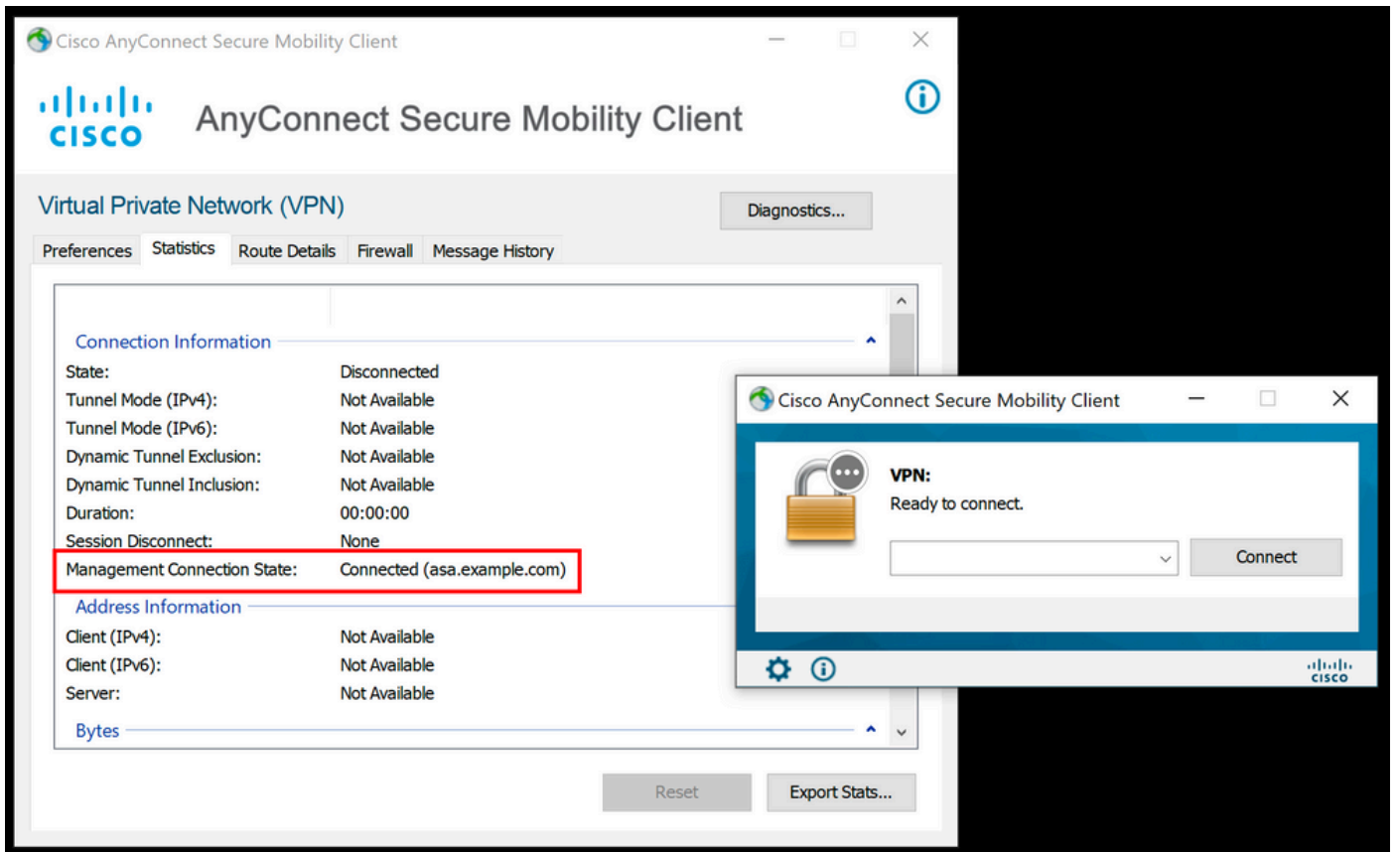
Idle Time Out: 30 Minutes Idle TO Left : 18 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036
Bytes Tx : 17238 Bytes Rx : 1988
Pkts Tx : 12 Pkts Rx : 13
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Verify the Management VPN tunnel connection on ASDM.

Navigate to **Monitoring > VPN > VPN Statistics > Sessions** . Filter By **AnyConnect Client** to see the client session.



Verification of the Management VPN tunnel connection on the Client Machine:



Troubleshoot

The new UI Statistics line (Management Connection State) can be used to troubleshoot management tunnel connectivity issues. These are the commonly seen error states:

Disconnected (disabled):

- The feature is disabled.
- Ensure that the management VPN profile was deployed to the client, via user tunnel connection (requires you to add the management VPN profile to the user tunnel-group policy) or out of band through the manual upload of the profile.
- Ensure that the management VPN profile is configured with a single host entry that includes a tunnel group.

Disconnected (trusted network):

- TND detected a trusted network so the management tunnel is not established.

Disconnected (user tunnel active):

- A user VPN tunnel is currently active.

Disconnected (process launch failed):

- A process launch failure was encountered when the management tunnel connection is attempted.

Disconnected (connect failed):

- A connection failure was encountered when the management tunnel is established.
- Ensure that the certificate authentication is configured in the tunnel group, no banner is present in the group policy, and the server certificate must be trusted.

Disconnected (invalid VPN configuration):

- An invalid split tunneling or client-bypass-protocol configuration was received from the VPN server.
- Check your configuration in the management tunnel-group policy against the documentation.

Disconnected (software update pending):

- An AnyConnect software update is currently pending.

Disconnected:

- The management tunnel is about to be established or can not be established for some other reason.

[Collect DART](#) for further troubleshooting.

Related Information

- [Configuration of Management VPN Tunnel](#)
- [Troubleshooting Management VPN Tunnel](#)
- [Technical Support & Documentation - Cisco Systems](#)