

# 為FTD設定RA VPN及LDAP驗證和授權

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

#### [許可證要求](#)

### [FMC的配置步驟](#)

#### [領域/LDAP伺服器配置](#)

#### [RA VPN配置](#)

### [驗證](#)

---

## 簡介

本文檔介紹如何在由Firepower管理中心管理的Firepower威脅防禦(FTD)上使用LDAP AA配置遠端訪問VPN。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 遠端訪問VPN(RA VPN)工作的基礎知識。
- 瞭解通過Firepower管理中心(FMC)的導航。
- 在Microsoft Windows Server上配置輕量級目錄訪問協定(LDAP)服務。

### 採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco Firepower管理中心版本7.3.0
- Cisco Firepower威脅防禦版本7.3.0
- Microsoft Windows Server 2016，配置為LDAP伺服器

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

本檔案介紹在Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)上，使用輕量型目錄訪問協定(LDAP)驗證和授權的遠端訪問VPN(RA VPN)的配置。

LDAP是一種開放的、供應商中立的行業標準應用協定，用於訪問和維護分散式目錄資訊服務。

LDAP屬性對映將Active Directory(AD)或LDAP伺服器中存在的屬性與Cisco屬性名稱等同。然後，在遠端訪問VPN連線建立期間，當AD或LDAP伺服器向FTD裝置返回身份驗證響應時，FTD裝置可以使用資訊調整AnyConnect客戶端完成連線的方式。

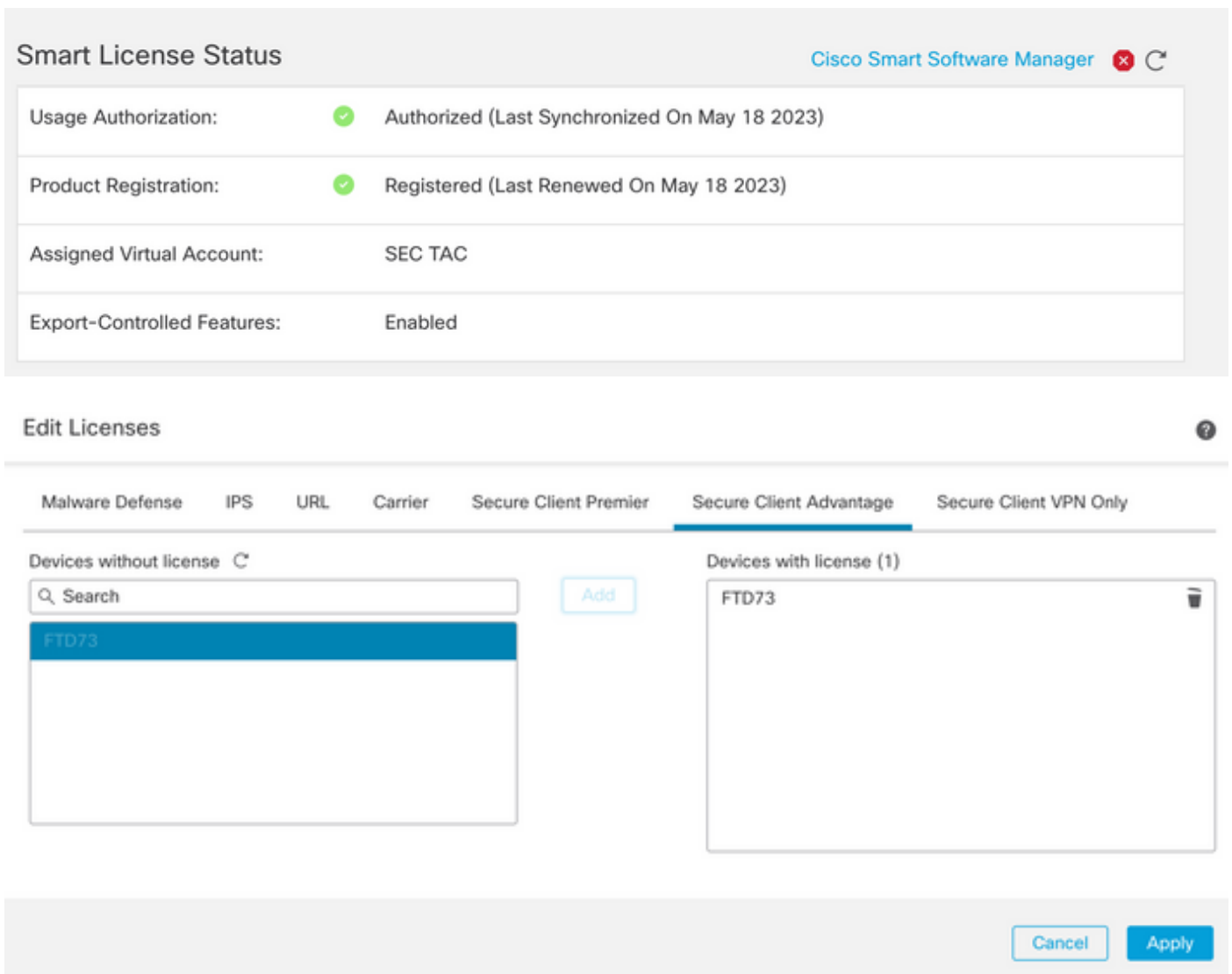
自6.2.1版本起，FMC支援具有LDAP身份驗證的RA VPN，建議通過FlexConfig對FMC 6.7.0版本之前的LDAP授權進行配置，以便配置LDAP屬性對映並將其與領域伺服器相關聯。此功能6.7.0版現已與FMC上的RA VPN配置嚮導整合，不再需要使用FlexConfig。

 注意：此功能要求FMC在6.7.0版上；而託管FTD可以位於任何高於6.3.0的版本上。

## 許可證要求

需要啟用匯出控制功能的AnyConnect Apex、AnyConnect Plus或AnyConnect VPN Only許可證。

要檢查許可證，請導航至 [System > Licenses > Smart Licenses](#).



The screenshot displays the Cisco Smart Software Manager interface for license management. The top section, titled "Smart License Status", shows the following details:

Usage Authorization:	✓	Authorized (Last Synchronized On May 18 2023)
Product Registration:	✓	Registered (Last Renewed On May 18 2023)
Assigned Virtual Account:		SEC TAC
Export-Controlled Features:		Enabled


The "Edit Licenses" section below features a navigation bar with tabs for Malware Defense, IPS, URL, Carrier, Secure Client Premier, Secure Client Advantage (selected), and Secure Client VPN Only. It is divided into two panes:

- Devices without license:** Contains a search bar and a list with one entry, "FTD73", which is highlighted in blue.
- Devices with license (1):** Contains a list with one entry, "FTD73", which is also highlighted in blue.

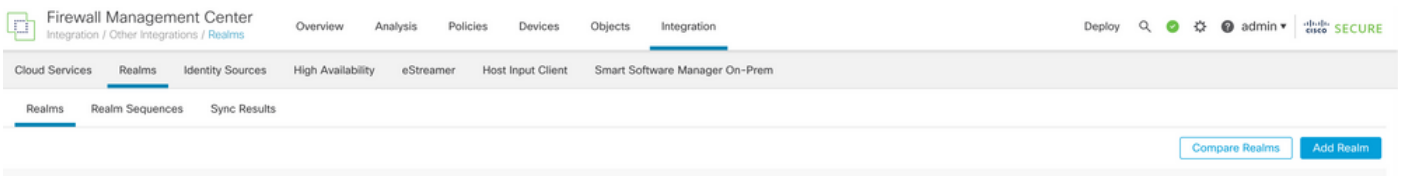
An "Add" button is positioned between the two panes. At the bottom right, there are "Cancel" and "Apply" buttons.

# FMC的配置步驟

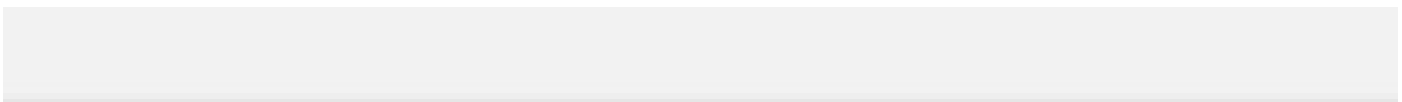
## 領域/LDAP伺服器配置

 注意：只有在配置新的領域/LDAP伺服器時才需要列出這些步驟。如果您擁有預配置的伺服器（可以在RA VPN中用於身份驗證），請導航至[RA VPN配置](#)。

步驟 1.導航至 System > Other Integrations > Realms如圖所示。



步驟 2.如圖所示，按一下 **Add a new realm.**



Compare Realms

Add Realm

步驟 3.提供AD伺服器和目錄的詳細資訊。按一下 OK.

在本演示中：

名稱：LDAP

類型：AD

AD主域:test.com

目錄用戶名：CN=Administrator，CN=Users，DC=test，DC=com

目錄密碼：<Hidden>

基本DN:DC=test，DC=com

組DN:DC=test , DC=com

## Add New Realm



Name\*

Description

Type

AD Primary Domain

*E.g. domain.com*

Directory Username\*

*E.g. user@domain.com*

Directory Password\*

Base DN

*E.g. ou=group,dc=cisco,dc=com*

Group DN

*E.g. ou=group,dc=cisco,dc=com*

## Directory Server Configuration

### ^ New Configuration

Hostname/IP Address\*

Port\*

Encryption

CA Certificate\*



Interface used to connect to Directory server

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

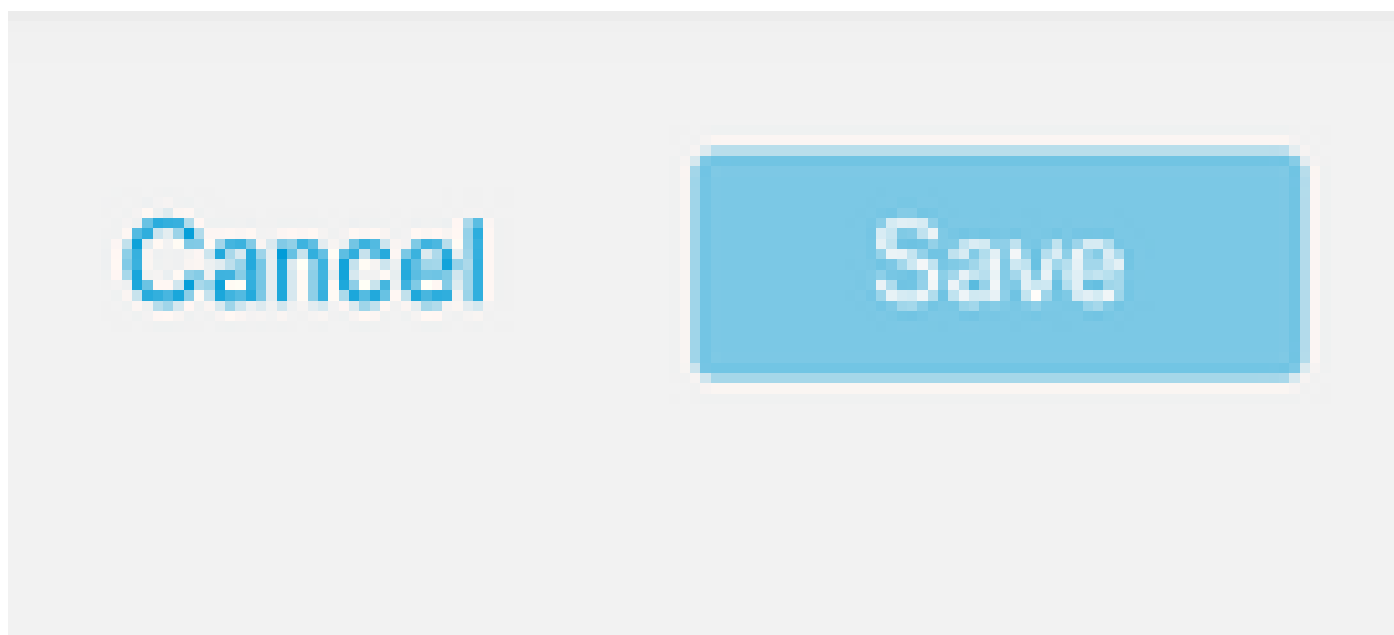
Test

[Add another directory](#)

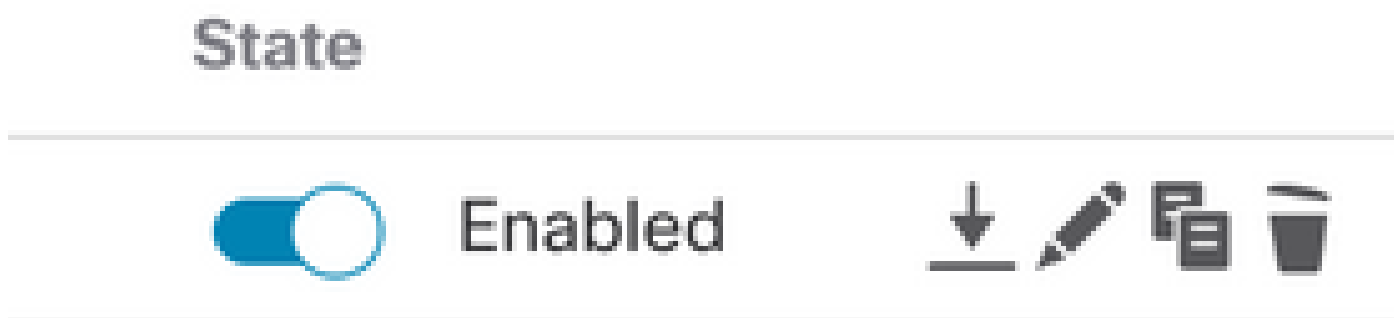
Cancel

Configure Groups and Users

步驟 4.按一下 **Save** 儲存領域/目錄更改，如下圖所示。



步驟 5.切換 **State** 按鈕將伺服器的狀態更改為「已啟用」，如下圖所示。



## RA VPN配置

配置組策略時需要執行以下步驟，該組策略分配給授權VPN使用者。如果已定義組策略，請移至[步驟5。](#)

步驟 1.導航至 **Objects > Object Management**.

## Network

A network object represents one or more IP addresses. Network objects are used in various processes, including access control, intrusion detection, and reporting, and so on.

Object Management

Intrusion Rules

第2步：在左窗格中，導航到 VPN > Group Policy.

▼ VPN

Certificate Map

Custom Attribute

Group Policy

IKEv1 IPsec Proposal

IKEv1 Policy

IKEv2 IPsec Proposal

IKEv2 Policy

Secure Client File

第3步：按一下 Add Group Policy.

Add Group Policy

 Filter

第4步：提供組策略值。

在本演示中：

名稱：RA-VPN

橫幅：!歡迎使用VPN!

每個使用者的同時登錄：3 (預設值)

## Add Group Policy

Name:\*

RA-VPN

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

**Banner**

DNS/WINS

Split Tunneling

**Banner:**

Maximum total size: 3999, Maximum characters in a line : 497.

In case of a line spanning more than 497 characters, split the line into multiple lines.

\*\* Only plain text is supported (symbols '<' and '>' are not allowed)

! Welcome to VPN!

## Add Group Policy

Name:\*

RA-VPN

Description:

General

Secure Client

Advanced

Traffic Filter

Session Settings

Access Hours:

Unrestricted



Simultaneous Login Per User:

3

(Range 0-2147483647)

步驟 5. 導航至 [Devices > VPN > Remote Access](#).

Devices

Objects

Integration

Device Management

Device Upgrade

NAT

QoS

Platform Settings

FlexConfig

Certificates

VPN

Site To Site

Remote Access

Dynamic Access Policy

Troubleshooting

Troubleshoot

File Download

Threat Defense CLI

Packet Tracer

Packet Capture

步驟 6. 按一下 [Add a new configuration](#).



Status	Last Modified
No configuration available <a href="#">Add a new configuration</a>	

步驟 7. 提供 Name 用於RA VPN策略。選擇 VPN Protocols 選擇 Targeted Devices. 按一下 Next.

在本演示中：

名稱：RA-VPN

VPN協定:SSL

目標裝置:FTD

### Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

#### Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:\*

Description:

VPN Protocols:

SSL  
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Q Search"/> <div style="background-color: #0070C0; color: white; padding: 2px;">FTD73</div>	<div style="border: 1px solid #ccc; padding: 5px;">FTD73 <span style="float: right;">🗑</span></div>

步驟 8. 對於 Authentication Method，選擇 AAA Only. 為選擇領域/LDAP伺服器 Authentication Server. 按一下 Configure LDAP Attribute Map (配置LDAP授權)。

## Connection Profile:

---

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:\*

**i** This name is configured as a connection alias, it can be used to connect to the VPN gateway

## Authentication, Authorization & Accounting (AAA):

---

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server:\*  +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server:  +

(Realm or RADIUS)

[Configure LDAP Attribute Map](#)

步驟 9.提供 LDAP Attribute Name 和 Cisco Attribute Name.按一下 **Add Value Map**.

在本演示中：

LDAP屬性名稱:memberOf

Cisco Attribute Name: Group-Policy

## Configure LDAP Attribute Map



Realm:

AD (AD)

LDAP attribute Maps:



Name Map:

LDAP Attribute Name	Cisco Attribute Name
<input type="text" value="memberOf"/>	<input type="text" value="Group-Policy"/>

Value Maps:

LDAP Attribute Value	Cisco Attribute Value
	<input type="text" value=""/>

[Add Value Map](#)

Cancel

OK

步驟 10. 提供 LDAP Attribute Value 和 Cisco Attribute Value. 按一下 OK.

在本演示中：

LDAP 屬性值：DC=tlalocan , DC=sec

思科屬性值：RA-VPN

LDAP attribute Maps:



Name Map:


LDAP Attribute Name	Cisco Attribute Name
<input type="text" value="memberOf"/>	<input type="text" value="Group-Policy"/>

Value Maps:

LDAP Attribute Value	Cisco Attribute Value
<input type="text" value="dc=tlalocan,dc=sec"/>	<input type="text" value="RA-VPN"/>

[Add Value Map](#)



 注意：您可以根據需要新增更多價值對映。

步驟 11. 新增 Address Pool 用於本地地址分配。按一下 OK.

### Address Pools ?

Available IPv4 Pools ↻ +

- VPN-Pool

Add

Selected IPv4 Pools

VPN-Pool 🗑️

Cancel OK

步驟 12. 提供 Connection Profile Name 和 Group-Policy. 按一下 Next.

在本演示中：


連線配置檔案名稱：RA-VPN

驗證方法：僅AAA

身份驗證服務器：LDAP

IPv4地址池：VPN池

Group-Policy：無訪問

 注意：Authentication Method、Authentication Server和IPV4地址池是在前面的步驟中配置的。

No-Access group-policy Simultaneous Login Per User 引數設定為0 ( 如果使用者接收到預設的No-Access組策略，則不允許使用者登入 )。

## Add Group Policy

Name:\*

No-Access

Description:

General

Secure Client

Advanced

Traffic Filter

Session Settings

Access Hours:

Unrestricted

+

Simultaneous Login Per User:

0

(Range 0-2147483647)

步驟 13. 按一下 [Add new AnyConnect Image](#) 為了新增 [AnyConnect Client Image](#) 到FTD。

### Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Select at least one Secure Client image

[Show Re-order buttons](#) +

<input checked="" type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
No Secure Client Images configured <a href="#">Add new Secure Client Image</a>			

步驟 14. 提供 [Name](#) 上傳的映像並從本地儲存中瀏覽以上傳映像。按一下 [Save](#).

## Add Secure Client File



Name:\*

mac

File Name:\*

anyconnect-macos-4.10.07061-webdep

Browse..

File Type:\*

Secure Client Image

Description:

Cancel

Save

步驟 15.按一下影象旁邊的覈取方塊以啟用影象以供使用。按一下 Next.

### Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input checked="" type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	Mac	anyconnect-macos-4.10.07061-webdeploy...	Mac OS

步驟 16.選擇 Interface group/Security Zone 和 Device Certificate.按一下 Next.

在本演示中：

介面組/安全區域：區域外

裝置證書：自簽名

 注意：您可以選擇啟用Bypass Access Control策略選項，以繞過對已加密(VPN)流量的任何訪問控制檢查（預設情況下禁用）。




## Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:\*  +

Enable DTLS on member interfaces

 All the devices must have interfaces as part of the Interface Group/Security Zone selected.

## Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*  +

Enroll the selected certificate object on the target devices

## Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

*This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

步驟 17.檢視RA VPN配置的摘要。按一下 **Finish** 儲存，如圖所示。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

**Remote Access VPN Policy Configuration**

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RA-VPN
Device Targets:	FTD73
Connection Profile:	RA-VPN
Connection Alias:	RA-VPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	AD (AD)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	VPN-Pool
Address Pools (IPv6):	-
Group Policy:	No-Access
Secure Client Images:	Mac
Interface Objects:	InZone

**Additional Configuration Requirements**

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**  
An **Access Control** rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**  
If NAT is enabled on the targeted devices, you must define a **NAT Policy** to exempt VPN traffic.
- DNS Configuration**  
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using **FlexConfig Policy** on the targeted devices.
- Port Configuration**  
SSL will be enabled on port 443.  
IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download.NAT-Traversal will be enabled

步驟 18. 導航至 Deploy > Deployment. 選擇需要將組態部署到的FTD。按一下 Deploy.

成功部署後，組態會被推送到FTD CLI:

```
<#root>
```

```
!--- LDAP Server Configuration ---!
```

```
ldap attribute-map LDAP
```

```
map-name memberOf Group-Policy
map-value memberOf DC=tlalocan,DC=sec RA-VPN
```

```
aaa-server LDAP protocol ldap
max-failed-attempts 4
realm-id 2
aaa-server LDAP host 10.106.56.137
server-port 389
ldap-base-dn DC=tlalocan,DC=sec
ldap-group-base-dn DC=tlalocan,DC=sec
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password *****
ldap-login-dn CN=Administrator,CN=Users,DC=test,DC=com
server-type microsoft
```

```
ldap-attribute-map LDAP
```

```
!--- RA VPN Configuration ---!
```



```
webvpn
enable Outside
anyconnect image disk0:/csm/anyconnect-win-4.10.07061-webdeploy-k9.pkg 1 regex "Mac"
anyconnect enable
tunnel-group-list enable
error-recovery disable
```

```
ssl trust-point Self-Signed
```

```
group-policy No-Access internal
```

```
group-policy No-Access attributes
```

```
vpn-simultaneous-logins 0
```

```
vpn-idle-timeout 30
```

```
!--- Output Omitted ---!
```

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
```

```
group-policy RA-VPN internal
```

```
group-policy RA-VPN attributes
```

```
banner value ! Welcome to VPN !
```

```
vpn-simultaneous-logins 3
```

```
vpn-idle-timeout 30
```

```
!--- Output Omitted ---!
```

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list non
```

```
ip local pool VPN-Pool 10.72.1.1-10.72.1.150 mask 255.255.255.0
```

```
tunnel-group RA-VPN type remote-access
```

```
tunnel-group RA-VPN general-attributes
```

```
address-pool VPN-Pool
```

```
authentication-server-group LDAP
```

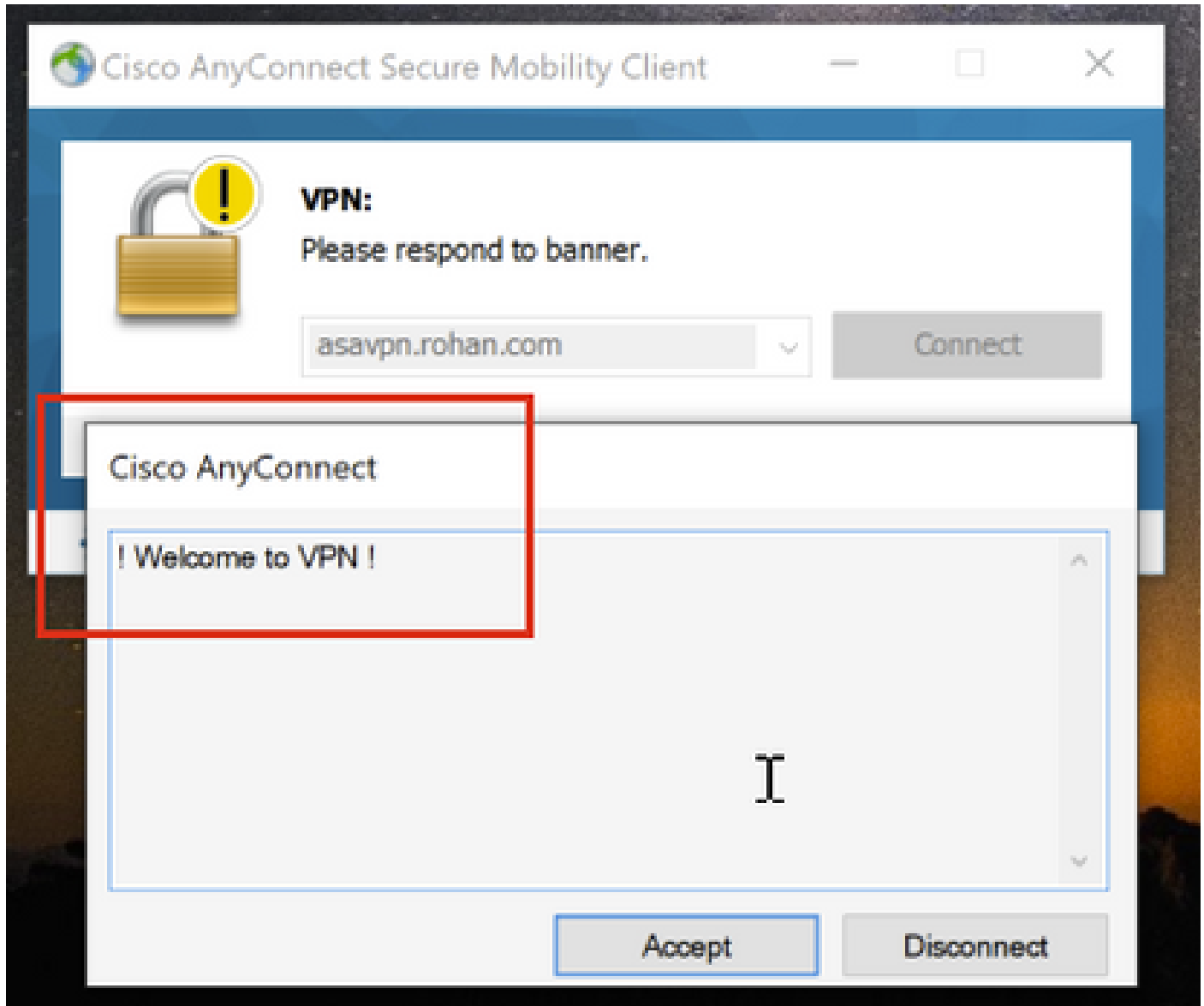
```
default-group-policy No-Access
```

```
tunnel-group RA-VPN webvpn-attributes
```

```
group-alias RA-VPN enable
```

## 驗證

在AnyConnect客戶端上，使用有效的VPN使用者組憑據登入，您將獲得由LDAP屬性對映分配的正確的組策略：



在LDAP調試片段(debug ldap 255)中，您可以看到LDAP屬性對映中有匹配項：

```
<#root>
```

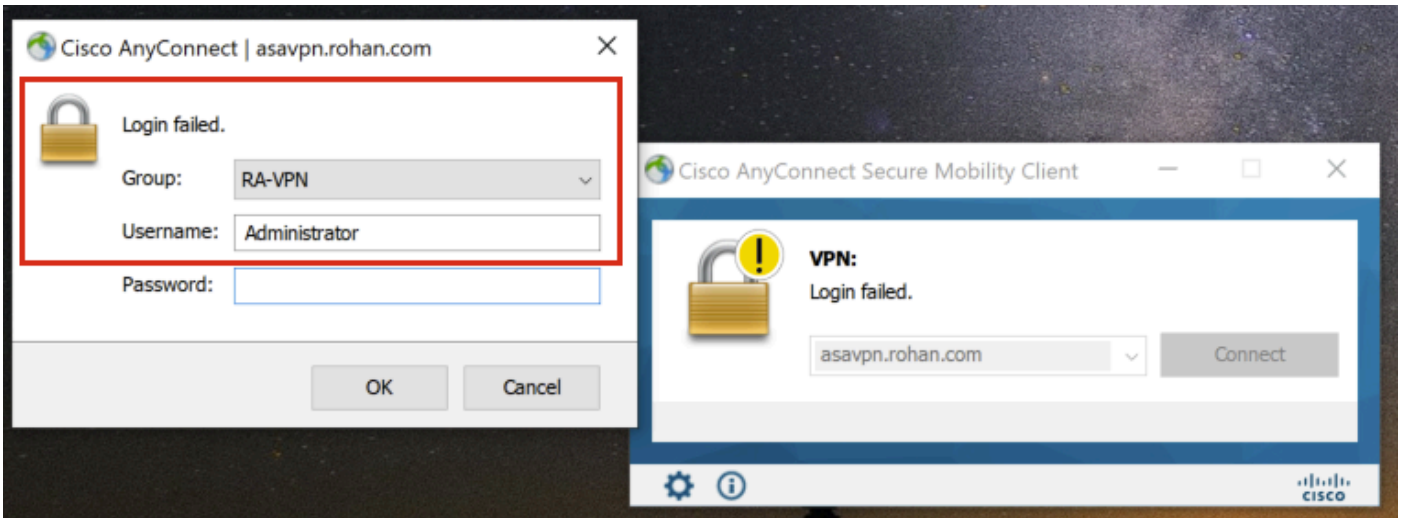
```
Authentication successful for test to 10.106.56.137
```

```
memberOf: value = DC=tlalocan,DC=sec
```

```
mapped to Group-Policy: value = RA-VPN
```

mapped to LDAP-Class: value = RA-VPN

在AnyConnect客戶端上，使用無效的VPN使用者組憑據登入，您將獲得禁止訪問組策略。



<#root>

```
%FTD-6-113004: AAA user authentication Successful : server = 10.106.56.137 : user = Administrator
%FTD-6-113009: AAA retrieved default group policy (No-Access) for user = Administrator

%FTD-6-113013: AAA unable to complete the request Error : reason =
Simultaneous logins exceeded for user : user = Administrator
```

從LDAP調試片段(debug ldap 255)中，可以看到LDAP屬性對映中沒有匹配項：

<#root>

```
Authentication successful for Administrator to 10.106.56.137

memberOf: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
```

memberOf: value = CN=Administrators,CN=Builtin,DC=tlaolocan,DC=sec  
mapped to Group-Policy: value = CN=Administrators,CN=Builtin,DC=tlaolocan,DC=sec  
mapped to LDAP-Class: value = CN=Administrators,CN=Builtin,DC=tlaolocan,DC=sec

## 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）。