

# ةقداصم مادختساب RA VPN ةكبش نيوكت FTD ل ليوختلاو LDAP

## تايوتحمل

[ةمدقملا](#)

[ةيساسالابابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[صيخرتلا تابلطتم](#)

[FMC لعل نيوكتلا تاوطخ](#)

[LDAP مداخت نيوكت / قاطنلا](#)

[RA VPN نيوكت](#)

[ةحصللا نم ققحتلا](#)

## ةمدقملا

ىلع AA LDAP مادختساب دعب نع لوصول VPN ةكبش نيوكت ةيفيك دنتسملا اذه فصوي FirePOWER ةرادا زكرم ةطساوب ةرادملا " (FTD) ةيرانلا ةقاطلا ديهت دص ةيامح".

## ةيساسالابابلطتملا

### تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت ناب Cisco يصوت:

- (RA VPN) دعب نع لوصول VPN ةكبش لمعب ةيساسا ةفرعم.
- Firepower (FMC) ةرادا زكرم لالخنم لقننتلامهف.
- Microsoft Windows LDAP ليلدل لوصول فيفخال لوكوتوربلا تامدخت نيوكت Server.

### ةمدختسملا تانوكملا

ةيلاتلا جماربال تارادصلا دنتسملا اذه في ةدراولا تامولعملا دنتست:

- Cisco Firepower Management Center، رادصلا 7.3.0
- Cisco نم FirePOWER ديهت دص عافدلا جمانرب نم 7.3.0 رادصلا
- Microsoft Windows Server 2016، LDAP مداخت هنيوكت مت

ةصاخ ةيلمعم ةئيبي في ةدوجوملا ةزهجالا نم دنتسملا اذه في ةدراولا تامولعملا عاشنإ مت تناك اذا. (يضارتفا) حوسمم نيوكتب دنتسملا اذه في ةمدختسملا ةزهجالا عيمجتأدب رمايال لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتكككبش.

# ةيساسأ تامول عم

لوكوتورب ةقداصم عم (RA VPN) دع ب نع لوصولل VPN ةكبش نيوكت دنتسملا اذه فصوي FirePOWER ديدهت نع عافدلا يل ع ضيوفتلاو (LDAP) نزولا فيفخ ليلدلا يل لوصولا (FTD) FirePOWER (FMC) ةرادا زكرم ةطساوب رادملا.

ةعانصلا ريياعم عم قفاوتمو ةئابل نم دياحم وحتفم قيبطت لوكوتورب وه LDAP اهت نايصو ةعزوملا ليلدلا تامول عم تامدخ يل لوصولل.

عم LDAP مداخ وأ Active Directory (AD) يف ةدوجوملا تامسلا ةلداعم ب LDAP ةمس نييعة موقوي FTD زاغ يل ةقداصملا تاباجتسا عاجراب LDAP وأ AD مداخ موقوي ام دنع ، م Cisco تامس عامسأ طبضل تامول عملا مادختسا FTD زاغل نكمي ، دع ب نع لوصولل VPN لاصتا عاشن انثأ لاصتال AnyConnect ليمع لامك ةيفي ك.





ثي ح (FMC) ةيساسأ ةرادإلا يف مكحتلا ةدحو يل ع LDAP ةقداصم عم RA VPN ةكبش معد مت FlexConfig ربع FMC 6.7.0 رادصإ لب ق LDAP ضيوفتو 6.2.1 رادصإل حصنلا مي دقت مت نآلا ، 6.7.0 رادصإلا عم ، ةزيملا هذه جم دمت . قاطنلا مداخ به انارقإو LDAP تامس ةطيرخ نيوكتل نآلا دع ب FlexConfig مادختسا بلطتت الو FMC يل ع RA VPN نيوكت جلاع م عم .

 FTD نوكي نأ نكمي ثي ح ، 6.7.0 رادصإلا يل ع FMC نوكت نأ ةزيملا هذه بلطتت : ةظحالم 6.3.0 نم يل ع رادصإلا يل ع رادملا .

## صخيخرتلا تابلطتم

نيكمت عم طوق AnyConnect VPN وأ AnyConnect Plus وأ AnyConnect Apex صخيخرت بلطتي ري دصتلا يف مكحتت يتلا فئاظولا .

يل لقتنا ، صخيخرتلا نم ققحتلل System > Licenses > Smart Licenses .

Smart License Status		Cisco Smart Software Manager  
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

Malware Defense

IPS

URL

Carrier

Secure Client Premier

Secure Client Advantage

Secure Client VPN Only

Devices without license C

Q Search

Add

FTD73

Devices with license (1)

FTD73

Cancel

Apply

## FMC ىل ع نىوكتل تاوطخ

### LDAP مداخل نىوكت / قاطنلا

ناك اذا. ديدج REALM / LDAP مداخل نىوكتل ناك اذا طقف ةبولطم ةجردملا تاوطخلا: ةظالم  
VPN RA، ةكبش يف ةقداصم لل هم ادختس نكمي يذلاو، اقبس م هنىوكت مت مداخل كيدل  
[RA VPN نىوكت](#) ىل لقتنا ذئدنعف.

ةروصلا هذه يف حضورم وه امك، System > Other Integrations > Realms ىل لقتنا 1. ةوطخلا

Add a new realm. رقتنا، ةروصلا يف حضورم وه امك. 2. ةوطخلا

Compare Realms

Add Realm

OK. تانالعال ليلدو مداخ ليرصافات ريفوتب مق 3 ةوطخال

ةرهاطملا هذه ضارغالو

مسال: LDAP

عونل: AD

AD: test.com ليرصااسال لاجملا

ليرلدل مدختسم مسا: CN=Administrator,CN=Users,DC=test,DC=com

<يفخم> ليرلدل رورم ةملك

ةكبش DN ليرصااسال: DC=test, DC=com

ةومجم dn: DC=test, DC=com

## Add New Realm



Name*	Description
<input type="text"/>	<input type="text"/>
Type	AD Primary Domain
AD	<input type="text"/>
	<i>E.g. domain.com</i>
Directory Username*	Directory Password*
<input type="text"/>	<input type="password"/>
<i>E.g. user@domain.com</i>	
Base DN	Group DN
<input type="text"/>	<input type="text"/>
<i>E.g. ou=group,dc=cisco,dc=com</i>	<i>E.g. ou=group,dc=cisco,dc=com</i>

### Directory Server Configuration

^ New Configuration

Hostname/IP Address*	Port*
<input type="text"/>	636
Encryption	CA Certificate*
LDAPS	Select certificate

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

[Add another directory](#)

Cancel

Configure Groups and Users

ةروصللا هذه في حضورم وه امك ،للدل/قطنللا تاريخيغت ظفحل Save رقنا 4. ةوطخللا

Cancel

Save

ةروصللا هذه يف حضورم وه امك ،نكمم ىلإ مداخللا ةلاح ريغيغتلا رز State ليدبت 5. ةوطخللا

State



Enabled



نيوكت RA VPN

تاكبش يف مدختس مل هن ييغت متي يذلاو ،"ةومجمل جهن" نيوكتلا تاوطخللا هذه دوجوم زلي  
5. ةوطخللا ىلإ لقتناف ،لعللاب افرعم "ةومجمل جهن" ناك اذا .نيدمتعمل VPN

ىلإ لقتننا 1. ةوطخللا Objects > Object Management.

ent Center  
ent

Overview

Analysis

Policies

Devices

Objects

Integration

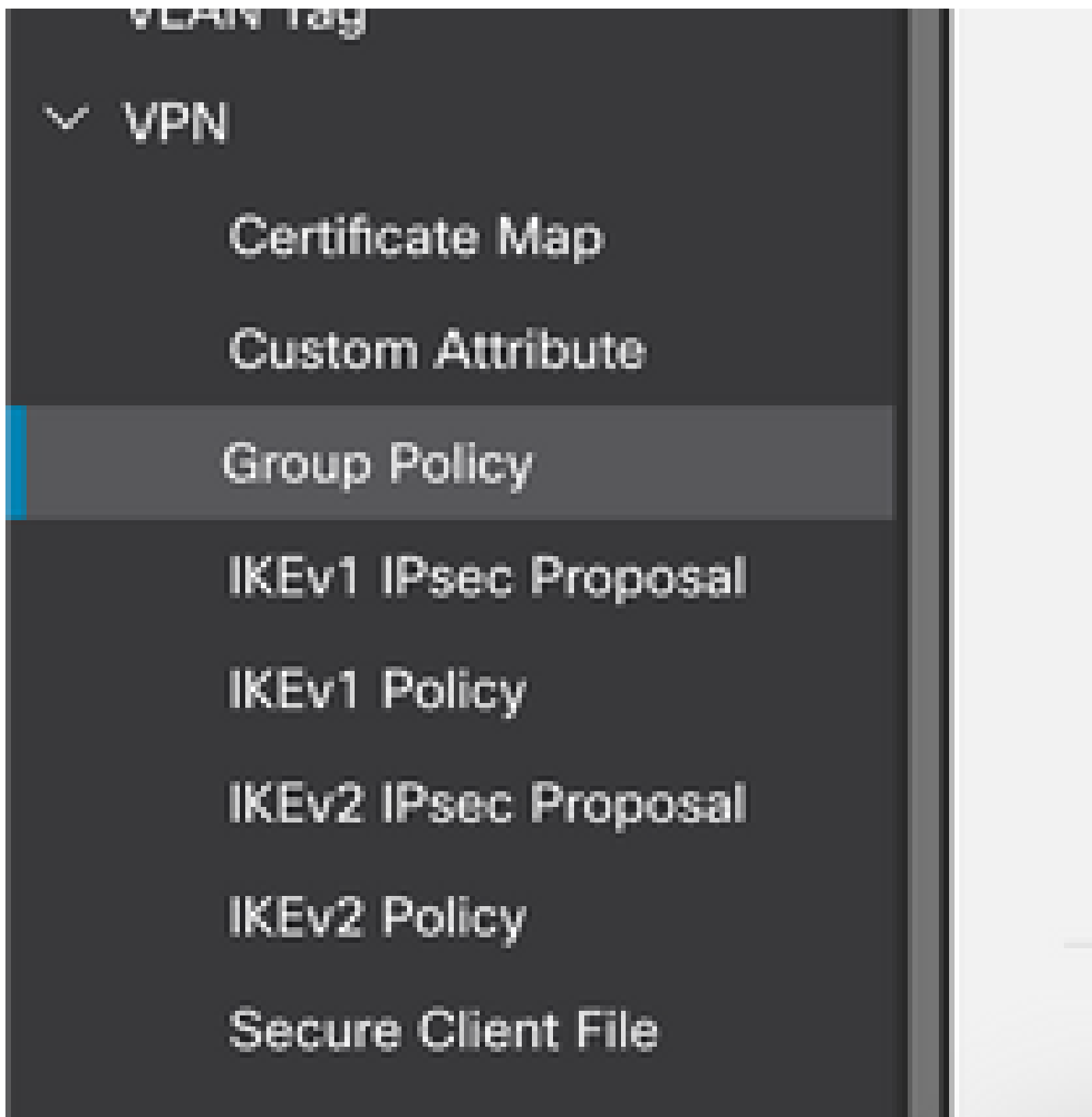
Network

A network object represents one or more IP addresses. Network objects are used in various places, including ac reports, and so on.

Object Management

Intrusion Rules

VPN > Group Policy إلى لقتنا ،رسيال عزال يف 2: ةوطخال



Add Group Policy رقنا 3: ةوطخال

[Add Group Policy](#)

ةوعومجملا جهن مي ق ري فوت :4 ةوطخلا

ة:ره اظملا هذه ضارغألو

مسال: RA-VPN

VPN ! ةكبش يف مكب اب حرم ! :راعش

(يضا رتفال) 3 :مدختسم لكلك نمازت مالا لوخذلا ليحست

## Add Group Policy



Name:\*

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)



## 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)

Devices > VPN > Remote Access. إلى لوقتنا 5. ةوطخلا

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

Add a new configuration. رقنا 6. ةوطخلا



## 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](#)

9. ةوطخل ريفوت LDAP Attribute Name و Cisco Attribute Name. Add Value Map رقنا.

ةراطملا هذو ضارغألو:

LDAP: memberOf ةمس مسا

Cisco: ةومحمل جهن ةمس مسا

## 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

OK رقنا Cisco Attribute Value و LDAP Attribute Value ريفوت 10 ةوطخلا

ةره اظملا هذه ضارغألو

LDAP: DC=tlalocan,DC=sec ةمس ةميقي

Cisco: RA-VPN ةمس ةميقي

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"/>

[+](#)

Copyright © 2013 Cisco

تابلطتم لل اقفو ةمي قلا طئارخ نم ديزملا ةفاضل كنكمي :ةظحالم

OK رقنا .ي لحملا ناوعلا نييعتل Address Pool ةفاضل 11 ةوطخلا

## Address Pools



### Available IPv4 Pools



Search

VPN-Pool

Add

### Selected IPv4 Pools

VPN-Pool

Cancel

OK

Next رقنا . Group-Policy و Connection Profile Name ريفوت 12 ةوطخلا

ةرهاظملا هذه ضارغألو

RA-VPN :لاصتالا فيرعت فلم مسا

طقف AAA :ةقداصملا بولسا

LDAP :ةقداصملا مداخ

VPN-POOL :IPv4 نيوانع عمجت

لوصول مدع :ةومجملا جهن

تاوطخلا في IPv4 نيوانع عمجت و ةقداصملا مداخو ةقداصملا بولسا نيوكت مت :ةظحالم  
ةقباسلا

مدع ل) 0 لىل ةملمعمل نييعت مت Simultaneous Login Per User لىل لوصول مدع ةومجم جهن يوتحي  
لوصول مدع ةومجم جهن يقلت ةلاح في لوخدلا ليحستب نيمدختسملل حامسلا



## Add Secure Client File



Name:\*

mac

File Name:\*

anyconnect-macos-4.10.07061-webdep

Browse..

File Type:\*

Secure Client Image

Description:

Cancel

Save

Next. رونا .مادختسالال نم اهنكمتل ةروصلل رواجمل ريشأتلا عبرم رونا . 15 ةوطخال

### 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

Next. رونا . Device Certificate و Interface group/Security Zone رتخأ . 16 ةوطخال

ةره اظم ل هذه ضارغ ألو

ةقطنم ل ا جراخ : نام أ ل ا ةقطنم / ةه ج اول ا ةعوم جم

ي تاذ عي قوت : زا ه ل ا ةداهش

ي ط خ ت ل ي ف ا ف ت ل ل ا ل ا ل و ص و ل ا ي ف م ك ح ت ل ا ة س ا ي س ر ا ي خ ن ي ك م ت ر ا ي ت خ | ك ن ك م ي : ة ظ ح ا ل م (ي ض ا ر ت ف ا ل ك ش ب ة ل ط ع م) ة ر ف ش م ل ا (VPN) ر و ر م ة ك ر ح ل ل و ص و ل ا ي ف م ك ح ت ل ل ص ح ف ي أ



AAA

## 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)

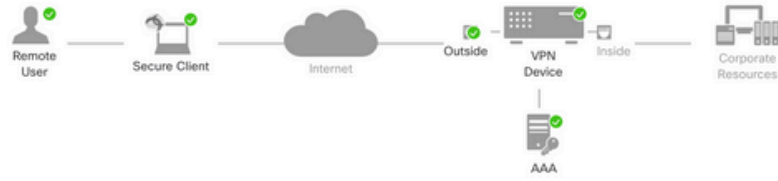
*This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

ةر و ص ل ا ي ف ح ز و م و ه ا م ك ، ظ ف ح ل ل Finish ر ق ن ا . RA VPN ن ي و ك ت ص خ ل م ض ر ع . 17 ة و ط خ ل ا



## 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

Deploy. رقنا. هل نيوكتال رشن مزلي يذال FTD رتخ. Deploy > Deployment. الى لقتنا. 18 ةوطخلال

ةججانال رشنال ةيلمع دعب FTD ب ةصاخال (CLI) رماوالا رطس ةهجاو الى نيوكتال عفد متي

```
<#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
```

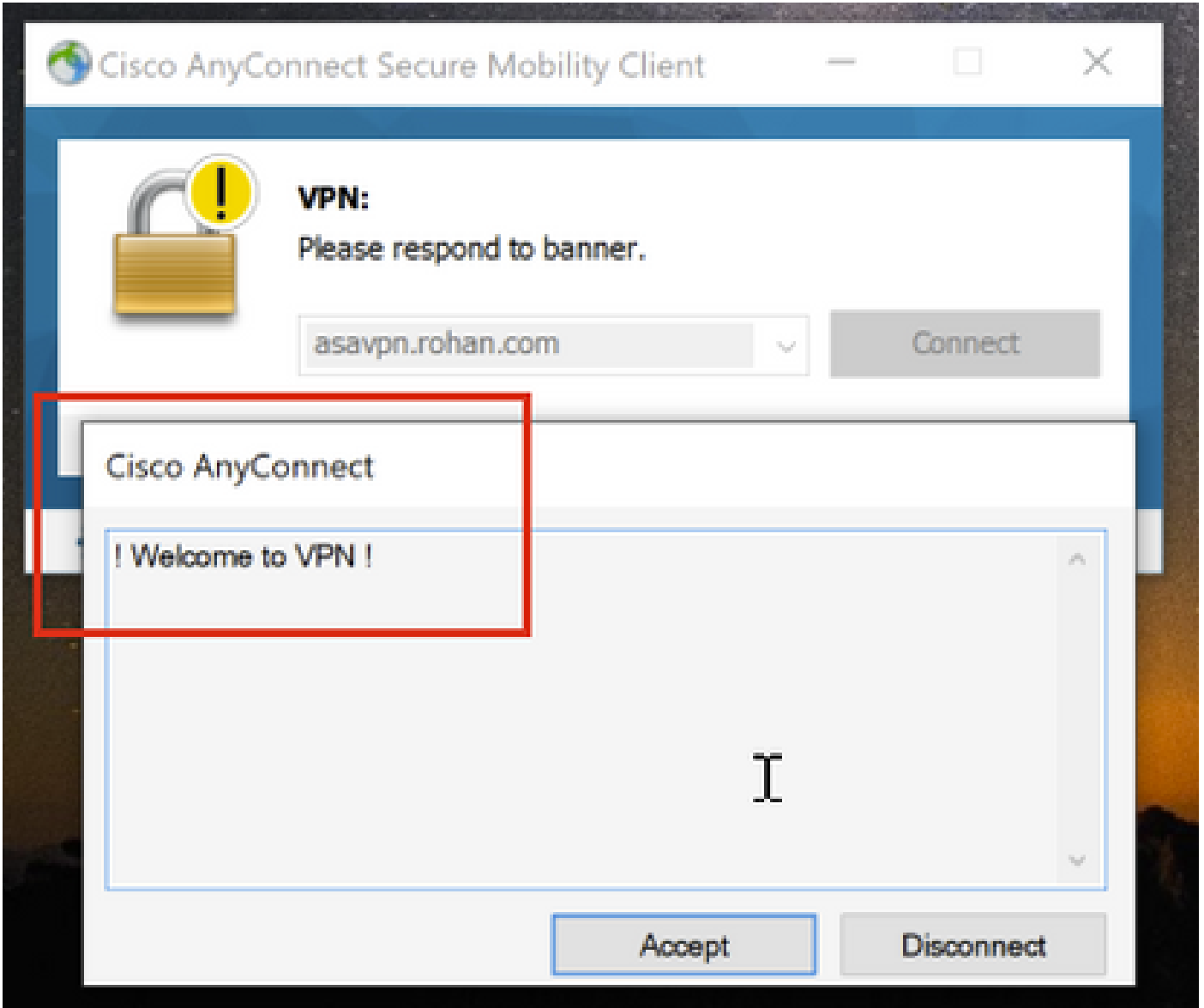
```
default-group-policy No-Access
```

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

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

## ةحصلال ن م ق قحتال

VPN يم دختسم ةومجم دامتعا تانايب مادختساب لوخدلا ليجستب مق AnyConnect ليمع يف LDAP ةمس ةطيرخ ةطساوب ني عمل احي حصلال ةومجم لاهن لعل لصحتسو، ةحصلال



LDAP لال لعل ةقباطم لانه تيأر عيطتسي تنأ (debug ldap 255) debug snippet لال ن م ةطيرخ ةمس:

```
<#root>
```

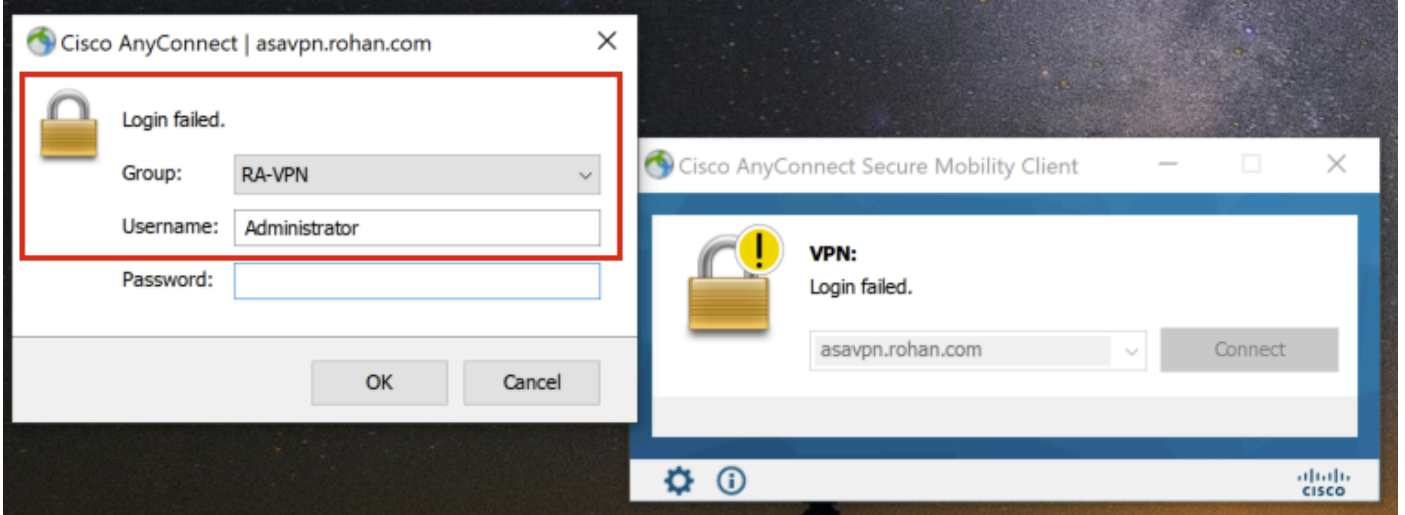
```
Authentication successful for test to 10.106.56.137
```

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

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

mapped to LDAP-Class: value = RA-VPN

VPN يمدختم سمعة ومجم دامت عا تانايب مادختساب لوخدلا ليجستب مق AnyConnect، لي مع يف لوصول المدعة ومجم جهن لعل لصحتو وحلالص ريغ.



<#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
```

يف قباطت دجوي ال هنأ ىرت نأ كنكمي، LDAP (debug ldap 255) اطاخأ حيحصتة صاصق نم LDAP: ةمس ةطيرخ

<#root>

```
Authentication successful for Administrator to 10.106.56.137
```

```
memberOf: value = CN=Group Policy Creator Owners,CN=Users,DC=t1alocan,DC=sec
mapped to Group-Policy: value = CN=Group Policy Creator Owners,CN=Users,DC=t1alocan,DC=sec
mapped to LDAP-Class: value = CN=Group Policy Creator Owners,CN=Users,DC=t1alocan,DC=sec
memberOf: value = CN=Domain Admins,CN=Users,DC=t1alocan,DC=sec
mapped to Group-Policy: value = CN=Domain Admins,CN=Users,DC=t1alocan,DC=sec
mapped to LDAP-Class: value = CN=Domain Admins,CN=Users,DC=t1alocan,DC=sec
memberOf: value = CN=Enterprise Admins,CN=Users,DC=t1alocan,DC=sec
mapped to Group-Policy: value = CN=Enterprise Admins,CN=Users,DC=t1alocan,DC=sec
mapped to LDAP-Class: value = CN=Enterprise Admins,CN=Users,DC=t1alocan,DC=sec
memberOf: value = CN=Schema Admins,CN=Users,DC=t1alocan,DC=sec
mapped to Group-Policy: value = CN=Schema Admins,CN=Users,DC=t1alocan,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=tlalocan,DC=sec  
mapped to Group-Policy: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec  
mapped to LDAP-Class: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا