

# FTDのLDAP認証および許可を使用したRA VPNの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ライセンス要件](#)

[FMCでの設定手順](#)

[レルム/LDAPサーバの設定](#)

[RA VPNの設定](#)

[確認](#)

---

## はじめに

このドキュメントでは、Firepower Management Center(UCMC)によって管理されるFirepower Threat Defense(FTD)でLDAP AAを使用してリモートアクセスVPN(RVPN)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- リモートアクセスVPN(RA VPN)の動作に関する基本的な知識
- firepower Management Center(FMC)を介したナビゲーションについて理解します。
- Microsoft Windows ServerでのLightweight Directory Access Protocol(LDAP)サービスの設定
- 

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Firepower マネジメントセンターバージョン7.3.0
- Cisco Firepower 脅威対策バージョン7.3.0
- LDAPサーバとして設定されたMicrosoft Windows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。


## 背景説明

このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepower Threat Defense(FTD)でのLightweight Directory Access Protocol(LDAP)認証および許可を使用したリモートアクセスVPN(RA VPN)の設定について説明します。

LDAPは、分散ディレクトリ情報サービスにアクセスして維持するための、ベンダーに依存しないオープンな業界標準アプリケーションプロトコルです。

LDAP属性マップは、Active Directory(AD)またはLDAPサーバに存在する属性をCisco属性名と同等にします。その後、リモートアクセスVPN接続の確立中にADサーバまたはLDAPサーバがFTDデバイスに認証応答を返すと、FTDデバイスはその情報を使用して、AnyConnectクライアントが接続を完了する方法を調整できます。

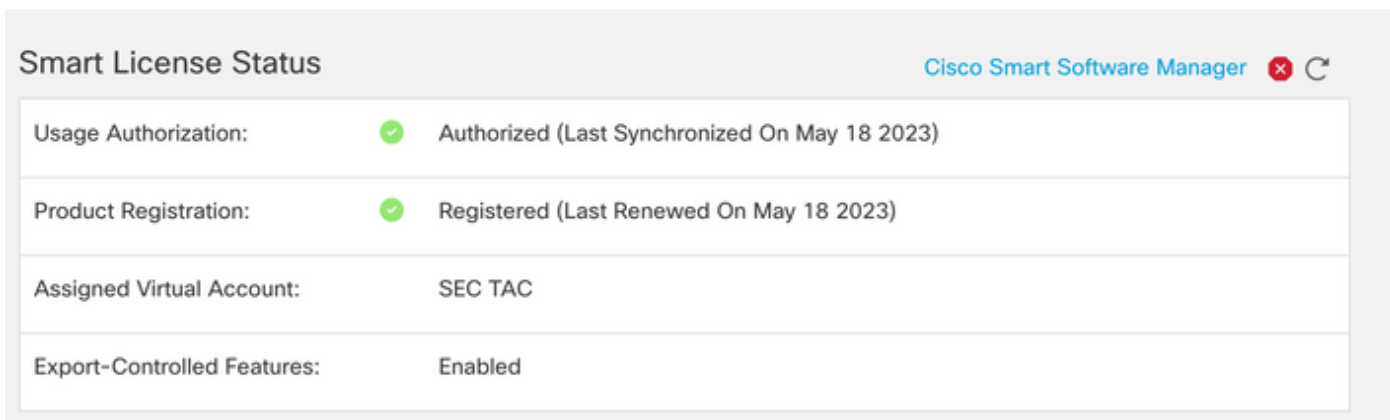
LDAP認証を使用するRA VPNはバージョン6.2.1以降でサポートされており、FMCバージョン6.7.0より前のLDAP認可は、LDAP属性マップを設定してレルムサーバに関連付けるために、FlexConfigを介して通知されました。バージョン6.7.0のこの機能は、FMCのRA VPNコンフィギュレーションウィザードに統合され、FlexConfigを使用する必要がなくなりました。

 **注：**この機能を使用するには、FMCがバージョン6.7.0である必要があります。一方、管理対象FTDは6.3.0より上位の任意のバージョンである可能性があります。

## ライセンス要件

エクスポート制御機能が有効になっているAnyConnect Apex、AnyConnect Plus、またはAnyConnect VPN Onlyライセンスが必要。

ライセンスを確認するには、 [System > Licenses > Smart Licenses](#) を参照。



The screenshot shows the 'Smart License Status' page in the Cisco Smart Software Manager. The page title is 'Smart License Status' and the Cisco Smart Software Manager logo is in the top right corner. The status is summarized in a table below:

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

  
FTD73

Add

Devices with license (1)


FTD73

Cancel

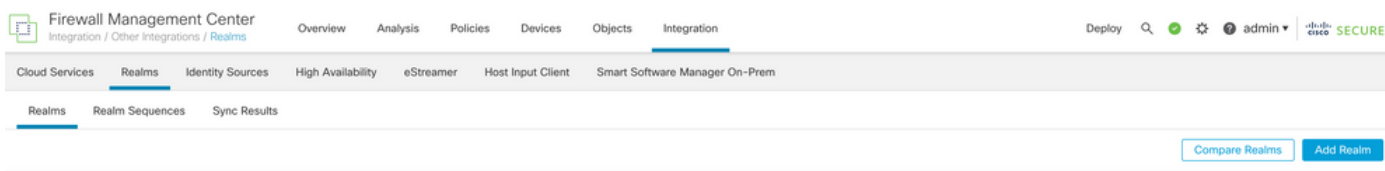
Apply

## FMCでの設定手順

### レルム/LDAPサーバの設定

 注：ここに示す手順は、新しいレルム/LDAPサーバを設定する場合にのみ必要です。RA VPNでの認証に使用できる設定済みのサーバがある場合は、[RA VPN Configuration](#)に移動します。

ステップ 1：移動先 System > Other Integrations > Realms, 以下の図に、出力例を示します。



Firewall Management Center  
Integration / Other Integrations / Realms

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings User admin

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Realms Realm Sequences Sync Results

Compare Realms Add Realm

ステップ 2：図に示すように、**Add a new realm**を参照。

Compare Realms

Add Realm

ステップ 3 : ADサーバとディレクトリの詳細を指定します。クリック **OK**を参照。

このデモンストレーションの目的は次のとおりです。

名前:LDAP

タイプ:AD

ADプライマリドメイン:test.com

ディレクトリユーザ名:CN=Administrator,CN=Users,DC=test,DC=com

ディレクトリパスワード: <Hidden>

ベースDN:DC=test,DC=com

グループ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

ステップ 4 : クリック **Save** 次の図に示すように、レルム/ディレクトリの変更を保存します。

Cancel

Save

ステップ 5： を切り替えます。 `State` ボタンをクリックして、次の図に示すように、サーバの状態を有効に変更します。

State



Enabled



## RA VPNの設定

これらの手順は、承認済みVPNユーザに割り当てられるグループポリシーを設定するために必要です。グループポリシーがすでに定義されている場合は、[ステップ5](#)に進みます。

ステップ 1： 移動先 `Objects > Object Management` を参照。

ent Center  
ent

Overview

Analysis

Policies

Devices

Objects

Integration

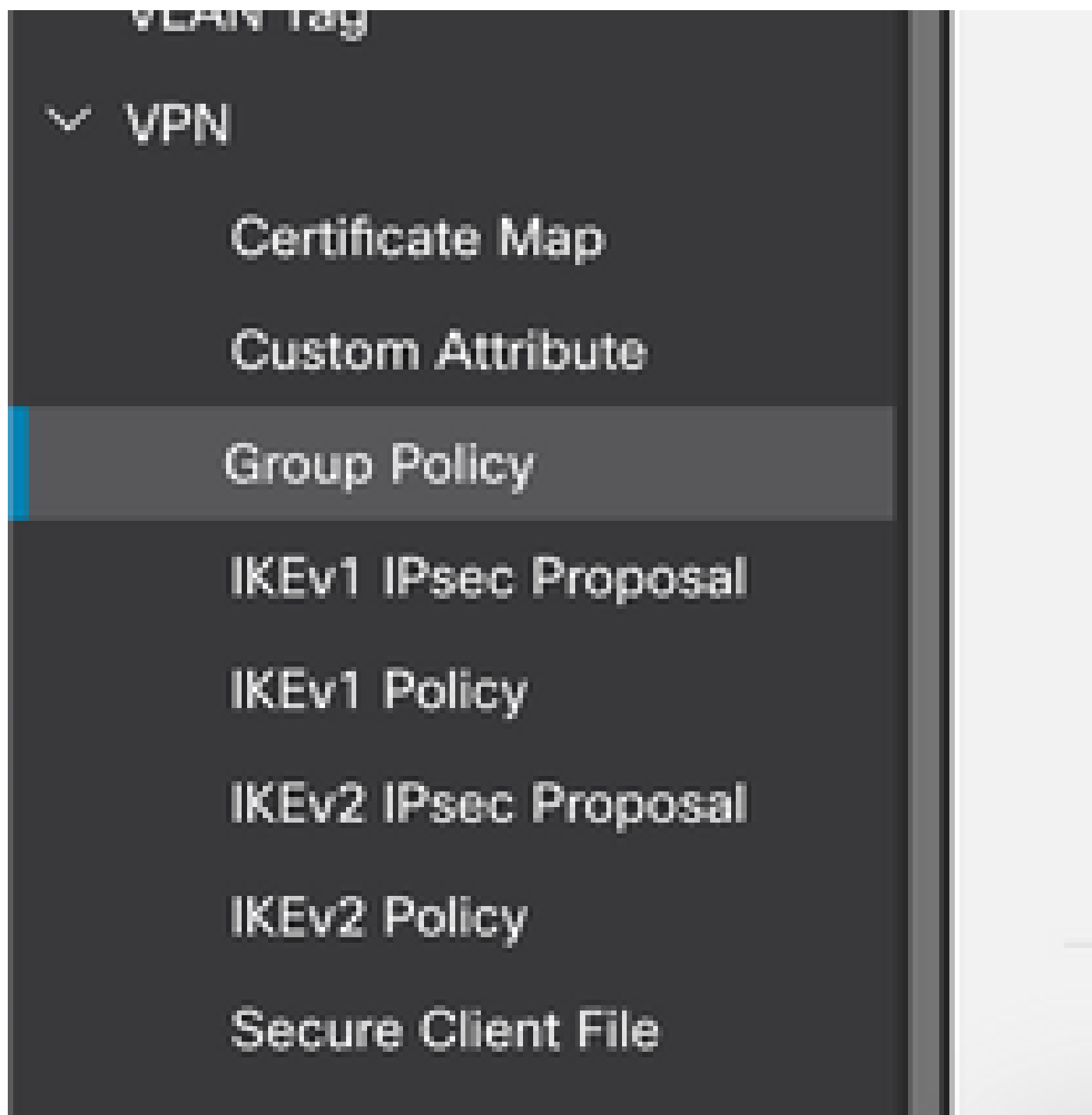
### Network

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

Object Management

Intrusion Rules

ステップ2 : 左側のペインで、 VPN > Group Policy を参照。



ステップ3 : クリック Add Group Policy を参照。

[Add Group Policy](#)

ステップ4 : グループポリシーの値を指定します。

このデモンストレーションの目的は次のとおりです。

名前:RA-VPN

バナー: !VPNへようこそ!

Simultaneous Login Per User:3 ( デフォルト )

## 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)

ステップ 5 : 移動先 [Devices > VPN > Remote Access](#) を参照。

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

手順 6 : クリック [Add a new configuration](#) を参照。

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

手順 7 : 次を提供します。 Name RA VPNポリシー用に設定します。 選択 VPN Protocols 選択します Targeted Devicesを参照。 クリック Nextを参照。

このデモンストレーションの目的は次のとおりです。

名前:RA-VPN

VPNプロトコル:SSL

対象デバイス: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="Search"/> <div style="border: 1px solid #ccc; padding: 2px;">FTD73</div>	<div style="border: 1px solid #ccc; padding: 2px;">FTD73 <span style="float: right;">✕</span></div>

ステップ 8 : の場合 Authentication Method,選択 AAA Onlyを参照。 WLCのREALM/LDAPサーバを Authentication Serverを参照。 クリック Configure LDAP Attribute Map ( LDAP許可を設定するため )。

## 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](#)

ステップ 9：次を提供します。 LDAP Attribute Name および Cisco Attribute Name を参照。クリック [Add Value Map](#) を参照。

このデモンストレーションの目的は次のとおりです。

LDAP属性名: memberOf

Cisco属性名: 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

ステップ 10 : 次を提供します。 LDAP Attribute Value および Cisco Attribute Value を参照。クリック OKを参照。

このデモンストレーションの目的は次のとおりです。

LDAP属性値:DC=tlalocan,DC=sec

Cisco属性値: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"/>



 注：要件に応じて、バリュemapをさらに追加できます。

ステップ 11次を追加します。 Address Pool ローカルアドレスの割り当てに使用します。クリック OKを参照。

### Address Pools ?

Available IPv4 Pools ⌂ +

VPN-Pool

Add

Selected IPv4 Pools

VPN-Pool 🗑️

Cancel

OK

ステップ 12次を提供します。 Connection Profile Name および Group-Policyを参照。クリック Nextを参照。

このデモンストレーションの目的は次のとおりです。


接続プロファイル名:RA-VPN

認証方式:AAAのみ

認証サーバ:LDAP

IPv4アドレスプール:VPNプール

グループポリシー：アクセスなし

 注：認証方式、認証サーバ、およびIPV4アドレスプールは、前の手順で設定しました。

No-Accessグループポリシーには、 Simultaneous Login Per User パラメータを0に設定します（デフォルトのNo-Accessグループポリシーを受け取ったユーザがログインできないようにするため）。

## 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)

ステップ 13 クリック [Add new AnyConnect Image](#) インターフェイスに [AnyConnect Client Image](#) FTDに送信します。

### 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>			

ステップ 14 : 次を提供します。 **Name** イメージをアップロードし、ローカルストレージから参照してイメージをアップロードします。クリック [Save](#) を参照。

## Add Secure Client File



Name:\*

mac

File Name:\*

anyconnect-macos-4.10.07061-webdep

Browse..

File Type:\*

Secure Client Image

Description:

Cancel

Save

ステップ 15 : イメージを使用可能にするには、イメージの横にあるチェックボックスをオンにします。クリック [Next](#) を参照。

### 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


ステップ 16 : 次のいずれかを選択します [Interface group/Security Zone](#) および [Device Certificate](#) を参照。クリ

ック [Next](#) を参照。

このデモンストレーションの目的は次のとおりです。

インターフェイスグループ/セキュリティゾーン : アウトゾーン

デバイス証明書 : 自己署名


 注 : 暗号化された(VPN)トラフィックのアクセスコントロールチェックをバイパスするために、Bypass Access Controlポリシーオプションを有効にすることができます ( デフォルトでは無効 ) 。



## 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.*

ステップ 17 : RA VPN設定の概要を表示します。クリック [Finish](#) をクリックして保存します (  を参照 ) 。



## 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

ステップ 18：移動先 Deploy > Deployment を参照。設定を展開する必要があるFTDを選択します。クリック Deploy を参照。

導入が成功すると、設定がFTD CLIにプッシュされます。

```
<#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
```

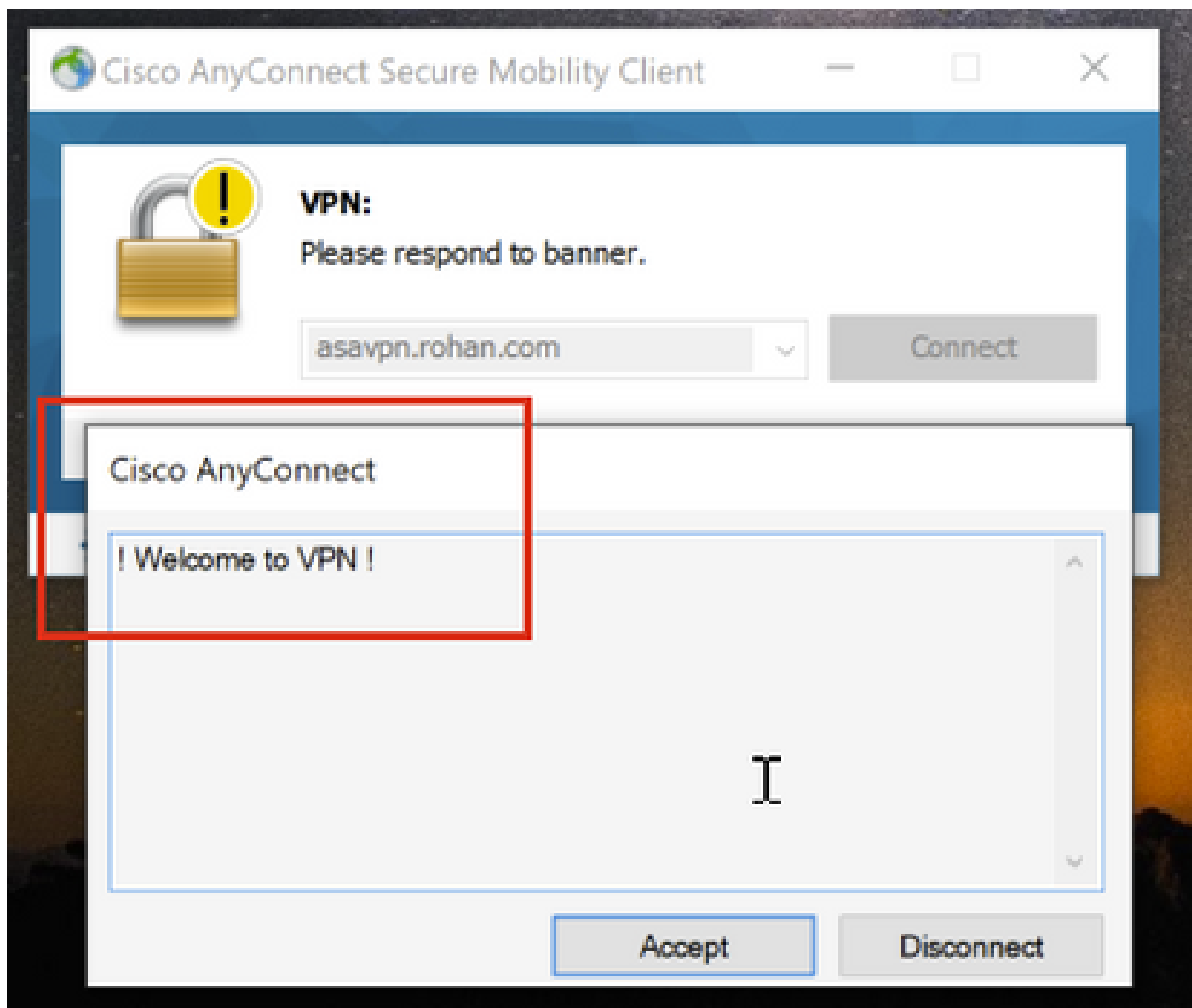
```
authentication-server-group LDAP
```

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

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

## 確認

AnyConnectクライアントで、有効なVPNユーザグループクレデンシャルを使用してログインすると、LDAP属性マップによって割り当てられた正しいグループポリシーが取得されます。



LDAPデバッグスニペット(debug ldap 255)から、LDAP属性マップに一致があることがわかります。

```
<#root>
```

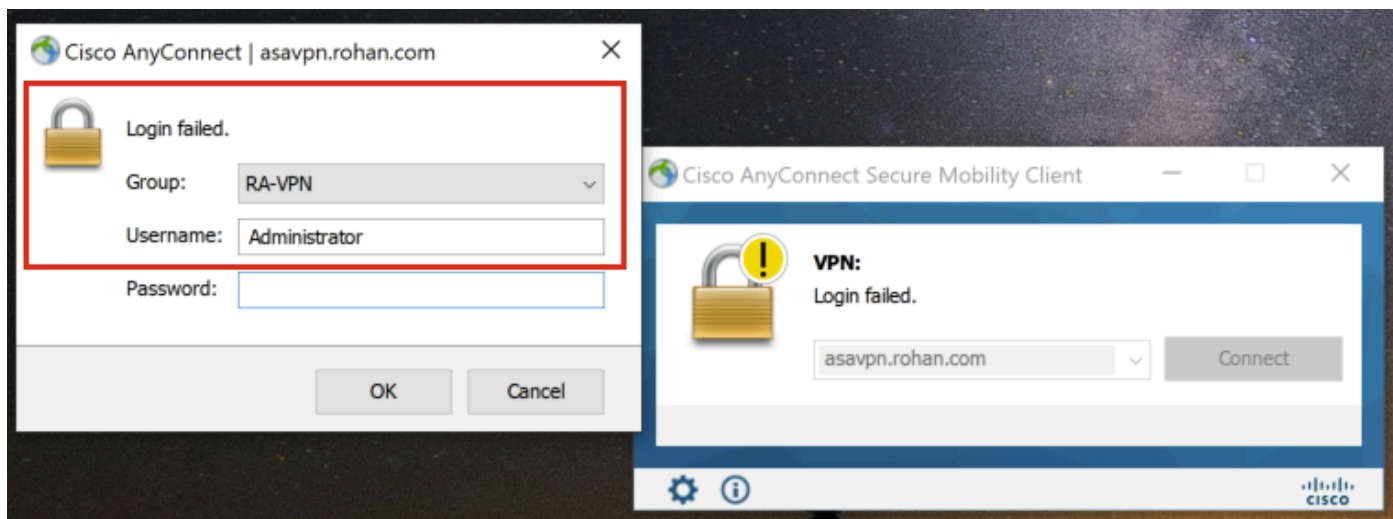
```
Authentication successful for test to 10.106.56.137
```

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

mapped to Group-Policy: value = RA-VPN

mapped to LDAP-Class: value = RA-VPN

AnyConnectクライアントで、Invalid VPN User Group Credentialを使用してログインすると、No-Accessグループポリシーが表示されます。



<#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
```

LDAPデバッグスニペット(debug ldap 255)から、LDAP属性マップに一致するものがないことがわかります。

<#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=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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。