

Configurazione di RSA VPN con autenticazione e autorizzazione LDAP per FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Requisiti di licenza](#)

[Procedura di configurazione in FMC](#)

[Configurazione realm/server LDAP](#)

[Configurazione VPN Autorità registrazione](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come configurare una VPN ad accesso remoto con LDAP AA su un Firepower Threat Defense (FTD) gestito da un centro di gestione Firepower.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del funzionamento di VPN ad accesso remoto (RA VPN).
- Comprendere la navigazione attraverso Firepower Management Center (FMC).
- Configurazione dei servizi LDAP (Lightweight Directory Access Protocol) in Microsoft Windows Server.

Componenti usati

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

- Cisco Firepower Management Center versione 7.3.0
- Cisco Firepower Threat Defense versione 7.3.0
- Microsoft Windows Server 2016, configurato come server LDAP

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

In questo documento viene descritta la configurazione della VPN ad accesso remoto (RA VPN) con autenticazione e autorizzazione LDAP (Lightweight Directory Access Protocol) su un FTD (Firepower Threat Defense) gestito da un centro di gestione di Firepower.

LDAP è un protocollo applicativo aperto, indipendente dal fornitore e standard del settore per l'accesso e la gestione dei servizi di informazioni delle directory distribuite.

Una mappa di attributi LDAP identifica gli attributi esistenti nel server Active Directory (AD) o LDAP con i nomi degli attributi Cisco. Quindi, quando il server AD o LDAP restituisce le risposte di autenticazione al dispositivo FTD durante la connessione VPN ad accesso remoto, il dispositivo FTD può utilizzare le informazioni per modificare il modo in cui il client AnyConnect completa la connessione.

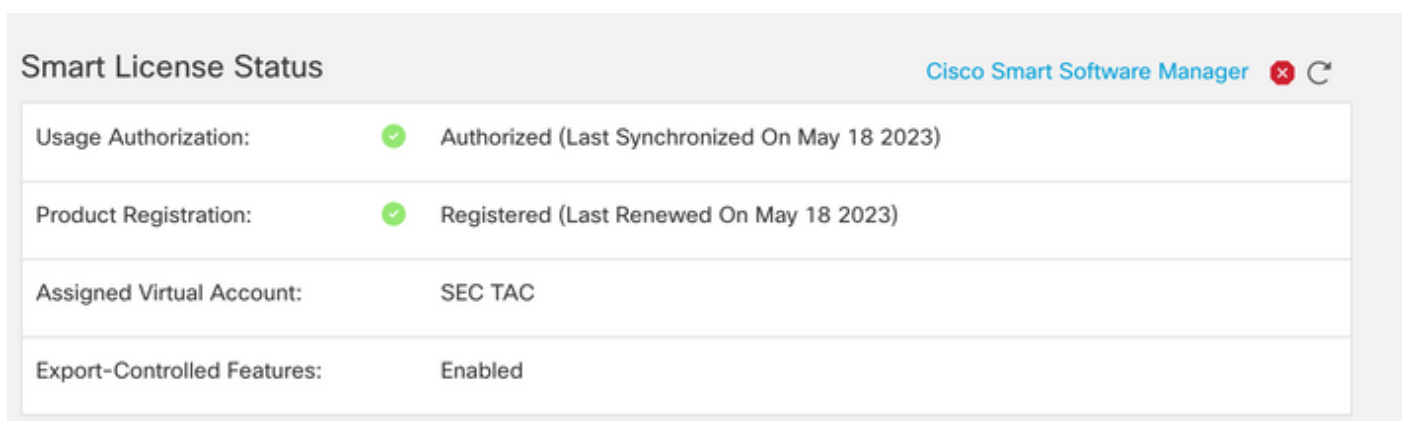
La VPN RSA con autenticazione LDAP è supportata in FMC dalla versione 6.2.1 e l'autorizzazione LDAP precedente alla versione 6.7.0 è stata consigliata tramite FlexConfig per configurare la mappa degli attributi LDAP e associarla al server del realm. Questa funzionalità, disponibile nella versione 6.7.0, è stata ora integrata con la configurazione guidata VPN di base nel FMC e non richiede più l'utilizzo di FlexConfig.




 Nota: questa funzione richiede che la versione del CCP sia la 6.7.0, mentre la versione del CCP gestito può essere una versione successiva alla 6.3.0.

Requisiti di licenza

Occorre una licenza AnyConnect Apex, AnyConnect Plus o AnyConnect VPN Only con funzionalità di controllo delle esportazioni abilitata.

Per controllare la licenza, passare a [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

Devices without license

Q Search

FTD73

Add

Devices with license (1)

FTD73

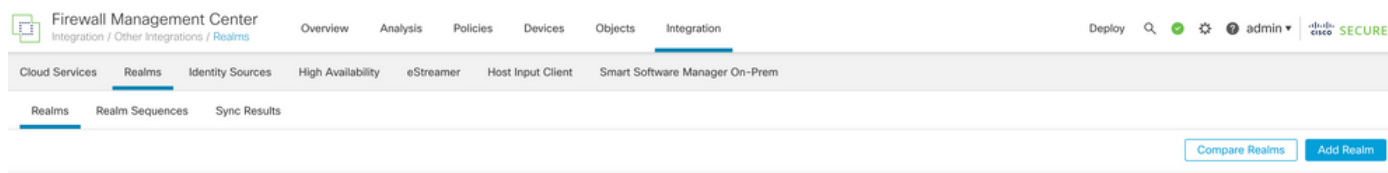
Cancel Apply

Procedura di configurazione in FMC

Configurazione realm/server LDAP

Nota: i passi elencati sono obbligatori solo se si riferiscono alla configurazione di un nuovo realm/server LDAP. Se si dispone di un server preconfigurato, che potrebbe essere utilizzato per l'autenticazione nella VPN RSA, passare alla [configurazione della VPN RSA](#).

Passaggio 1. Passa a System > Other Integrations > Realms, come mostrato nell'immagine.



Passaggio 2. Come mostrato nell'immagine, fare clic su Add a new realm.

[Compare Realms](#)

[Add Realm](#)

Passaggio 3. Fornire i dettagli del server AD e della directory. Fare clic su OK.

Ai fini della presente dimostrazione:

Nome: LDAP

Tipo: AD

Dominio primario AD: test.com

Nome utente directory: CN=Amministratore,CN=Utenti,DC=prova,DC=com

Password directory: <nascosta>

DN di base: DC=test,DC=com

DN gruppo: 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

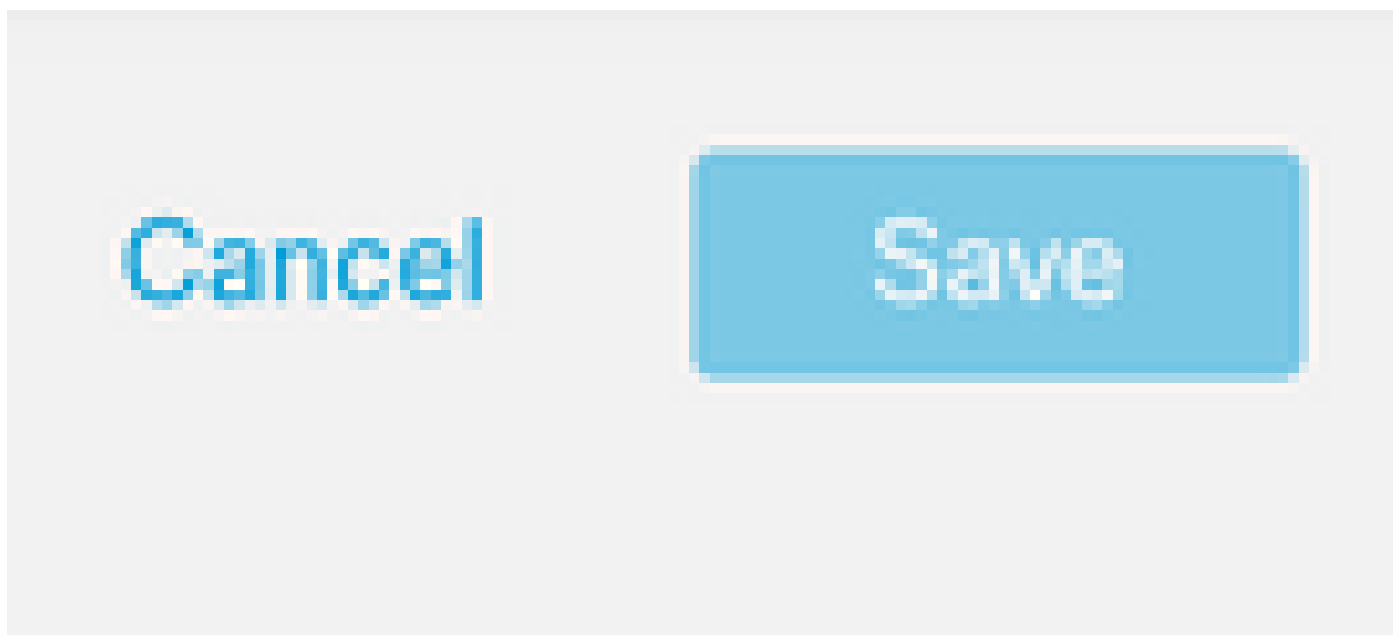
[Add another directory](#)

Cancel

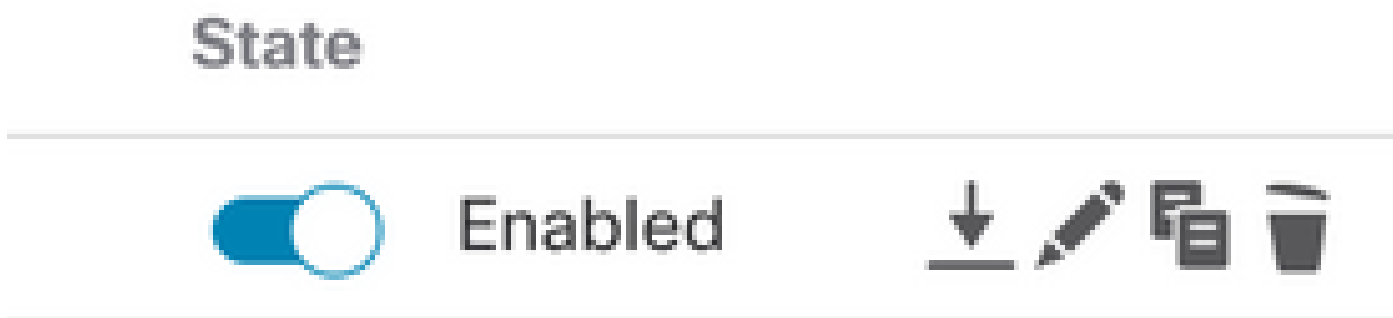
Configure Groups and Users

Passaggio 4. Fare clic su **Save** per salvare le modifiche al realm o alla directory, come mostrato

nell'immagine.



Passaggio 5. Attiva/disattiva *State* per impostare lo stato del server su Attivato, come illustrato in questa immagine.



Configurazione VPN Autorità registrazione

Questi passaggi sono necessari per configurare i Criteri di gruppo assegnati agli utenti VPN autorizzati. Se i Criteri di gruppo sono già stati definiti, passare al [passaggio 5](#).

Passaggio 1. Passa a `Objects > Object Management`.

Network

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

Object Management

Intrusion Rules

Passaggio 2: Nel riquadro di sinistra, passare a VPN > Group Policy.

▼ VPN

Certificate Map

Custom Attribute

Group Policy

IKEv1 IPsec Proposal

IKEv1 Policy

IKEv2 IPsec Proposal

IKEv2 Policy

Secure Client File

Passaggio 3: Fare clic su **Add Group Policy**.

Add Group Policy

 Filter

Passaggio 4: specificare i valori di Criteri di gruppo.

Ai fini della presente dimostrazione:

Nome: RA-VPN

Striscione: Benvenuto alla VPN!

Accesso simultaneo per utente: 3 (predefinito)

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)

Passaggio 5. Passa a [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

Passaggio 6. Fare clic su [Add a new configuration](#).

Status	Last Modified
No configuration available Add a new configuration	

Passaggio 7. Fornire un **Name** per i criteri VPN RA. Scegli **VPN Protocols** e scegliere **Targeted Devices**. Fare clic su **Next**.

Ai fini della presente dimostrazione:

Nome: RA-VPN

Protocolli VPN: SSL

Dispositivi di destinazione: 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

FTD73

Selected Devices

FTD73 ✕

[Add](#)

Passaggio 8. Per il **Authentication Method**, scegliere **AAA Only**. Scegliere il realm/server LDAP per **Authentication Server**. Fare clic su **Configure LDAP Attribute Map** (per configurare l'autorizzazione LDAP).

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](#)

Passaggio 9. Fornire LDAP Attribute Name e Cisco Attribute Name. Fare clic su **Add Value Map**.

Ai fini della presente dimostrazione:

Nome attributo LDAP: memberOfI

Nome attributo Cisco: Criteri di gruppo

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

Passaggio 10. Fornire LDAP Attribute Value e Cisco Attribute Value. Fare clic su OK.

Ai fini della presente dimostrazione:

Valore attributo LDAP: DC=tlalocan,DC=sec

Valore attributo Cisco: 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](#)



 Nota: è possibile aggiungere più mappe valore in base al fabbisogno.

Passaggio 11. Aggiungere la `Address Pool` per l'assegnazione dell'indirizzo locale. Fare clic su **OK**.

Address Pools ?

Available IPv4 Pools ⌂ +

VPN-Pool

Add

Selected IPv4 Pools

VPN-Pool 🗑

Cancel

OK

Passaggio 12. Fornire **Connection Profile Name** e **Group-Policy**. Fare clic su **Next**.

Ai fini della presente dimostrazione:


Nome profilo connessione: RA-VPN

Metodo di autenticazione: solo AAA

Server di autenticazione: LDAP

Pool di indirizzi IPv4: VPN-Pool

Criteri di gruppo: Nessun accesso

 Nota: il metodo di autenticazione, il server di autenticazione e il pool di indirizzi IPV4 sono stati configurati nei passaggi precedenti.

Il criterio di gruppo **Nessun accesso** prevede `Simultaneous Login Per User` Parametro impostato su 0 (per non consentire agli utenti di eseguire l'accesso se ricevono il criterio di gruppo predefinito **Nessun**

accesso).

Add Group Policy

Name:*

Description:

General Secure Client **Advanced**

Traffic Filter

Session Settings

Access Hours:

 +

Simultaneous Login Per User:

 (Range 0-2147483647)

Passaggio 13. Fare clic su [Add new AnyConnect Image](#) per aggiungere un **AnyConnect Client Image** 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 Add new Secure Client Image			

Passaggio 14. Fornire un **Name** per l'immagine caricata e sfogliare dall'archivio locale per caricare l'immagine. Fare clic su **Save**.

Add Secure Client File



Name:*

mac

File Name:*

anyconnect-macos-4.10.07061-webdep

Browse..

File Type:*

Secure Client Image

Description:

Cancel

Save

Passaggio 15. Per attivare l'immagine, fare clic sulla casella di controllo accanto all'immagine stessa. Fare clic su **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

Passaggio 16. Scegliere il **Interface group/Security Zone** e **Device Certificate**. Fare clic su **Next**.

Ai fini della presente dimostrazione:

Gruppo di interfacce/Area di sicurezza: Out-Zone

Certificato dispositivo: autofirmato


 Nota: è possibile scegliere di abilitare l'opzione Ignora criterio di controllo di accesso per ignorare qualsiasi controllo di accesso per il traffico crittografato (VPN) (disabilitato per impostazione predefinita).



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.

Passaggio 17. Visualizzare il riepilogo della configurazione della VPN per l'Autorità registrazione. Fare clic su `Finish` per salvare, come mostrato nell'immagine.

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

Passaggio 18. Passa a Deploy > Deployment. Scegliere l'FTD in cui distribuire la configurazione. Fare clic su Deploy.

Il push della configurazione viene eseguito nella CLI FTD dopo la corretta distribuzione:

```
<#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
```

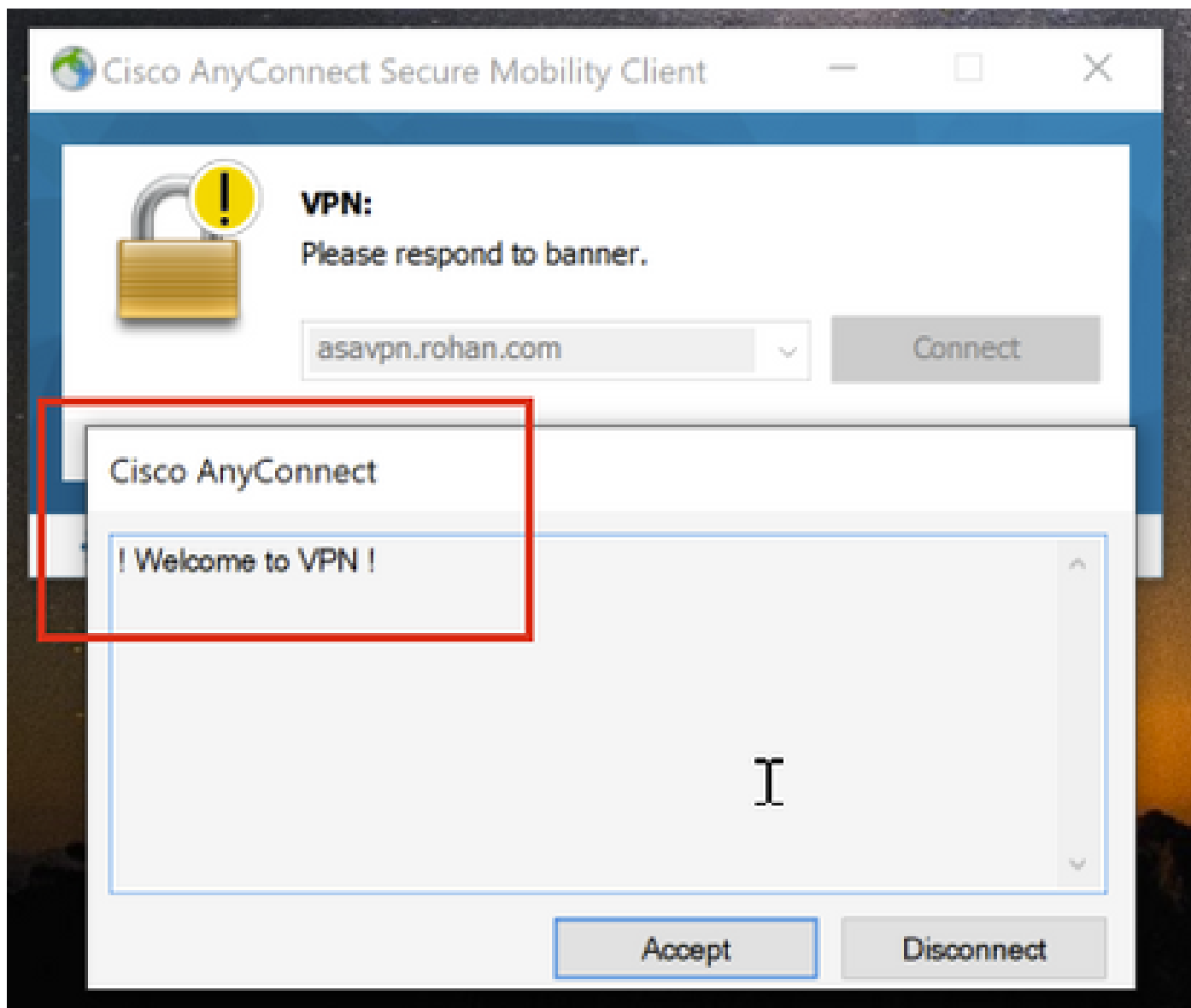
```
authentication-server-group LDAP
```

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

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

Verifica

Sul client AnyConnect, eseguire il login con Credenziali valide per i gruppi di utenti VPN e ottenere i criteri di gruppo corretti assegnati dalla mappa attributi LDAP:



Dal frammento LDAP Debug (debug ldap 255) è possibile vedere una corrispondenza nella mappa degli attributi LDAP:

```
<#root>
```

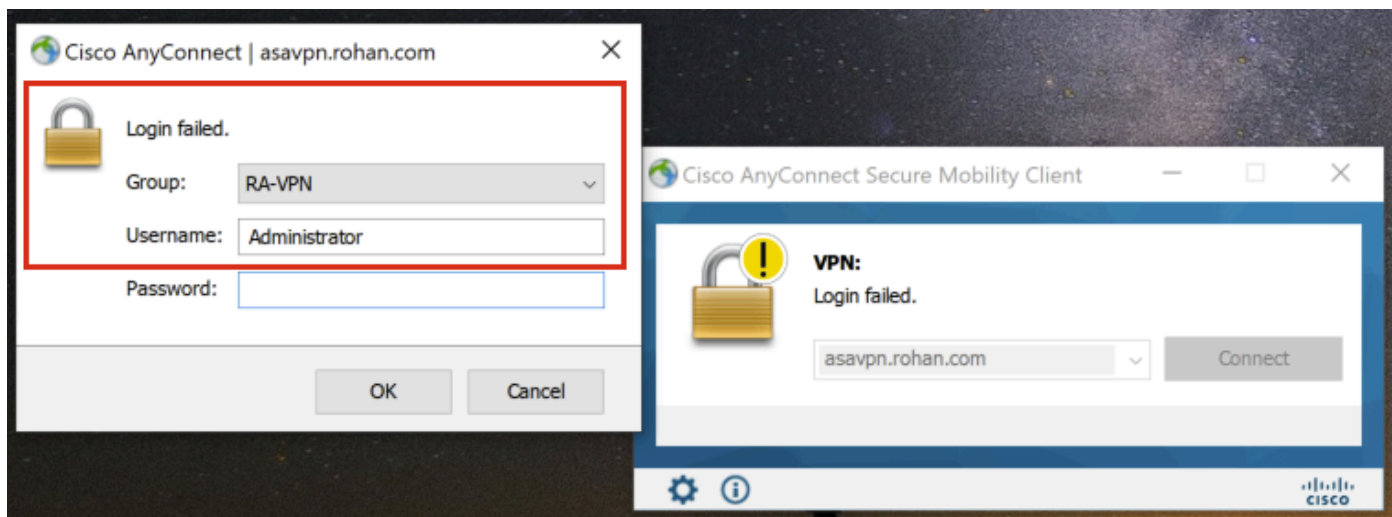
```
Authentication successful for test to 10.106.56.137
```

```
memberOf: value = DC=t1alocan,DC=sec
```

mapped to Group-Policy: value = RA-VPN

mapped to LDAP-Class: value = RA-VPN

Sul client AnyConnect, eseguire l'accesso con una credenziale del gruppo di utenti VPN non valida e ottenere i criteri di gruppo per l'impossibilità di accedere.



<#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
```

Dal frammento di codice di debug LDAP (debug ldap 255), è possibile vedere che non esiste alcuna corrispondenza nella mappa degli attributi LDAP:

<#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=tlaalocan,DC=sec
mapped to LDAP-Class: value = CN=Enterprise Admins,CN=Users,DC=tlaalocan,DC=sec
memberOf: value = CN=Schema Admins,CN=Users,DC=tlaalocan,DC=sec
mapped to Group-Policy: value = CN=Schema Admins,CN=Users,DC=tlaalocan,DC=sec
mapped to LDAP-Class: value = CN=Schema Admins,CN=Users,DC=tlaalocan,DC=sec
memberOf: value = CN=IIS_IUSRS,CN=Builtin,DC=tlaalocan,DC=sec
mapped to Group-Policy: value = CN=IIS_IUSRS,CN=Builtin,DC=tlaalocan,DC=sec
mapped to LDAP-Class: value = CN=IIS_IUSRS,CN=Builtin,DC=tlaalocan,DC=sec
memberOf: value = CN=Administrators,CN=Builtin,DC=tlaalocan,DC=sec
mapped to Group-Policy: value = CN=Administrators,CN=Builtin,DC=tlaalocan,DC=sec
mapped to LDAP-Class: value = CN=Administrators,CN=Builtin,DC=tlaalocan,DC=sec

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).