

# Configurazione dell'autenticazione VPN SSL tramite FTD, ISE, DUO e Active Directory

## Sommario

---

[Introduzione](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazioni FTD.](#)

[Integrazione di un server RADIUS in Firepower Management Center \(FMC\)](#)

[Configurare la VPN remota.](#)

[Configurazioni ISE.](#)

[Integrazione di DUO come server Radius esterno.](#)

[Integrare l'FTD come dispositivo di accesso alla rete.](#)

[configurazioni DUO.](#)

[Installazione del proxy DUO.](#)

[Integrazione di DUO Proxy con ISE e DUO Cloud.](#)

[Integrazione di DUO con Active Directory.](#)

[Esporta account utente da Active Directory \(AD\) tramite DUO Cloud.](#)

[Registrare gli utenti nel cloud Cisco DUO.](#)

[Procedura di convalida della configurazione.](#)

[Problemi comuni.](#)

[Scenario di lavoro.](#)

[Errore 11353: nessun altro server RADIUS esterno. Impossibile eseguire il failover](#)

[Le sessioni RADIUS non vengono visualizzate nei log live di ISE.](#)

[Ulteriori procedure di risoluzione dei problemi.](#)

---

## Introduzione

Questo documento descrive l'integrazione di SSLVPN in Firepower Threat Defense tramite Cisco ISE e DUO Security per AAA.

## Requisiti

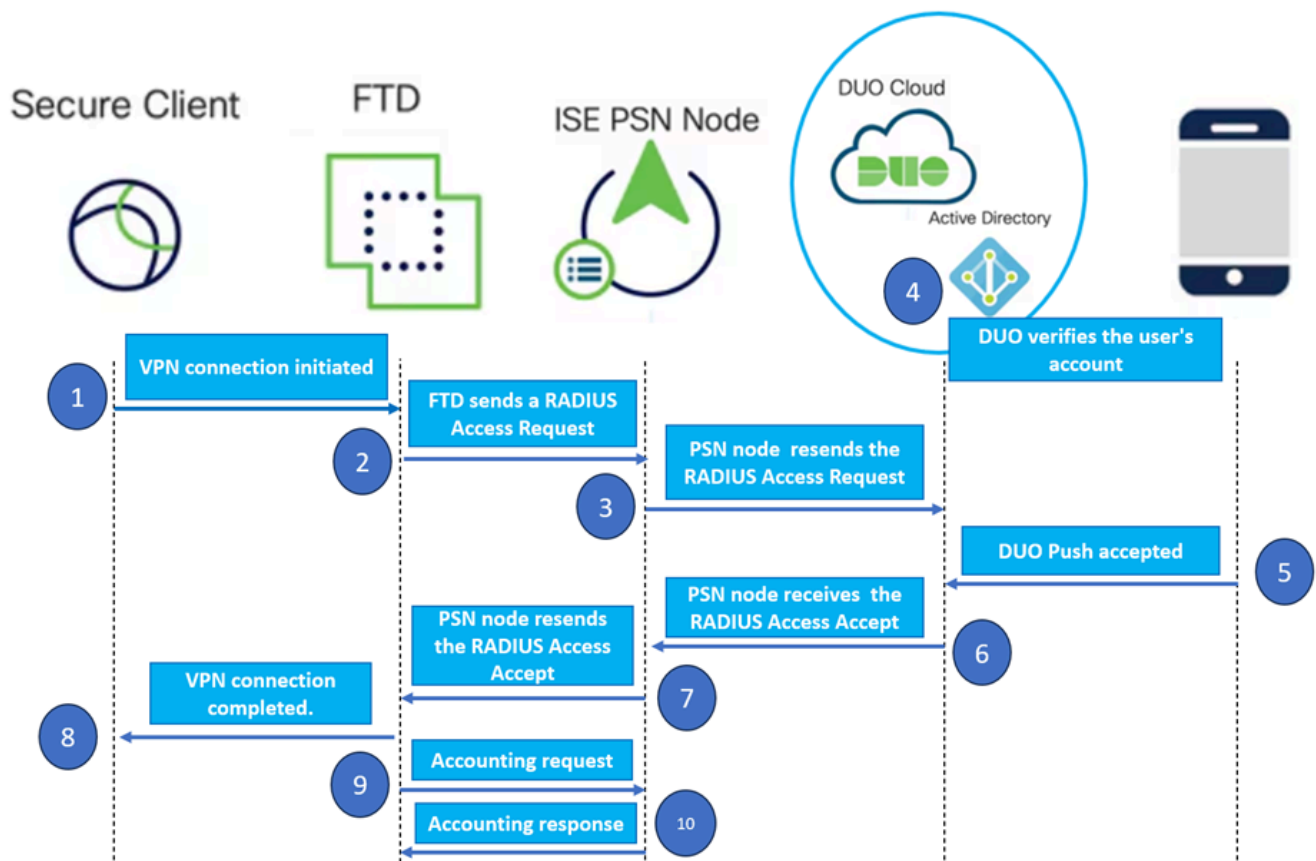
- ISE 3.0 o versione successiva.
- FMC 7.0 o versione successiva.
- FTD 7.0 o versione successiva.
- Duo Authentication Proxy.
- Licenze ISE Essentials
- Licenze DUO Essentials.

## Componenti usati

- Patch 3 per ISE 3.2
- CCP 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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.

## Esempio di rete



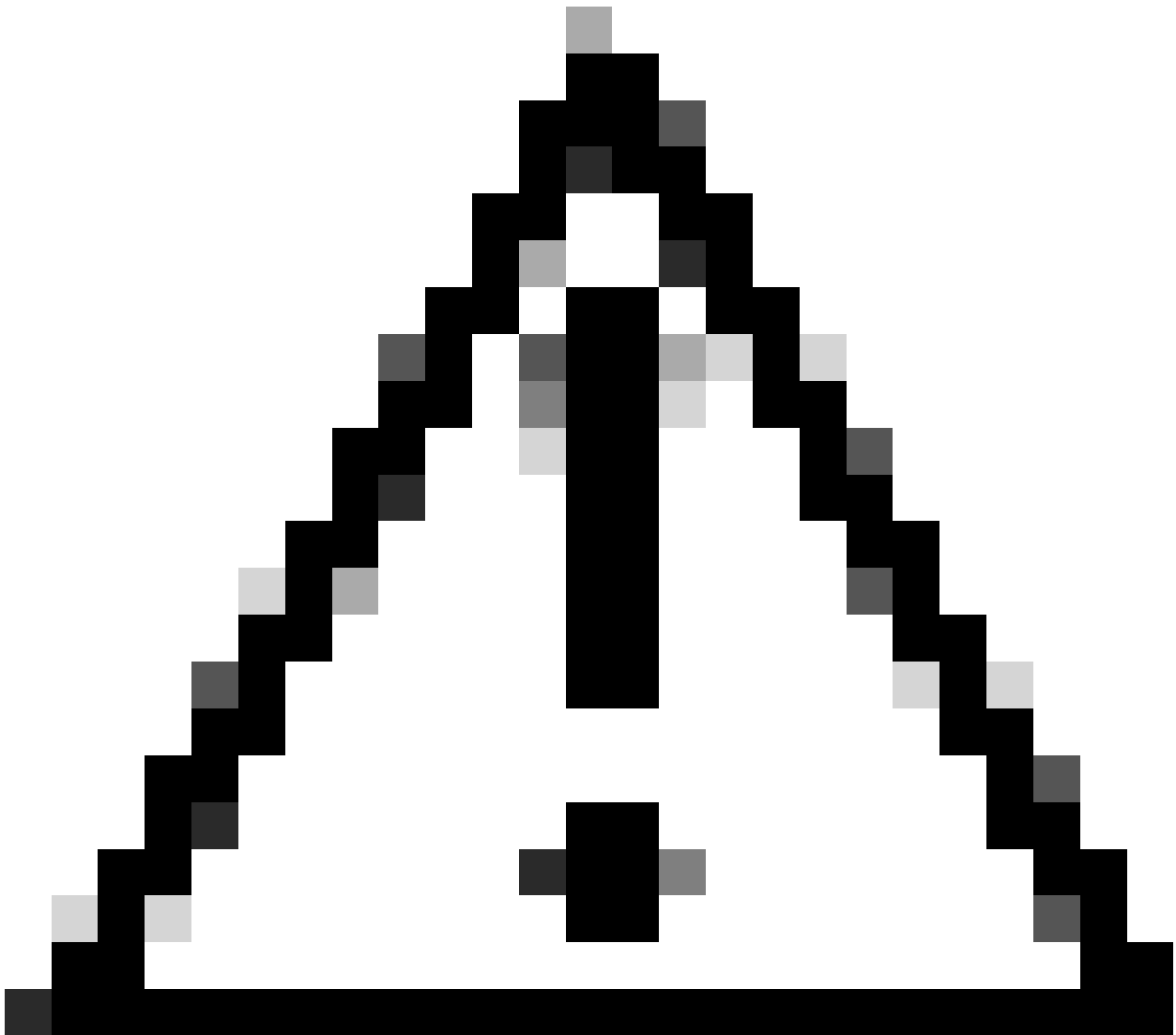
Topologia.

Nella soluzione proposta, Cisco ISE è un proxy server RADIUS fondamentale. Anziché valutare direttamente i criteri di autenticazione o autorizzazione, ISE è configurata per inoltrare i pacchetti RADIUS dall'FTD al proxy di autenticazione DUO.

Il proxy di autenticazione DUO opera come intermediario dedicato all'interno di questo flusso di autenticazione. Installato su un server Windows, colma il divario tra Cisco ISE e il cloud DUOs. La funzione primaria del proxy è quella di trasmettere le richieste di autenticazione - incapsulate nei pacchetti RADIUS - al cloud DUO. Il cloud DUO infine consente o nega l'accesso alla rete in base

alle configurazioni di autenticazione a due fattori.

1. L'utente avvia il processo di autenticazione VPN immettendo il nome utente e la password univoci.
2. Firewall Threat Defense (FTD) invia la richiesta di autenticazione a Cisco Identity Services Engine (ISE).
3. Il PSN (Policy Services Node) inoltra la richiesta di autenticazione al server proxy di autenticazione DUO. Successivamente, il server di autenticazione DUO convalida le credenziali tramite il servizio cloud DUO.
4. Il cloud DUO convalida il nome utente e la password rispetto al proprio database sincronizzato.



Attenzione: per mantenere aggiornato un database utenti nel cloud DUO, è necessario che la sincronizzazione tra il cloud DUO e le organizzazioni Active Directory sia attiva.

5. Una volta completata l'autenticazione, il cloud DUO avvia un Push DUO per gli utenti registrati

sul dispositivo mobile tramite una notifica push sicura e crittografata. L'utente deve quindi approvare il Push DUO per confermare la propria identità e procedere.

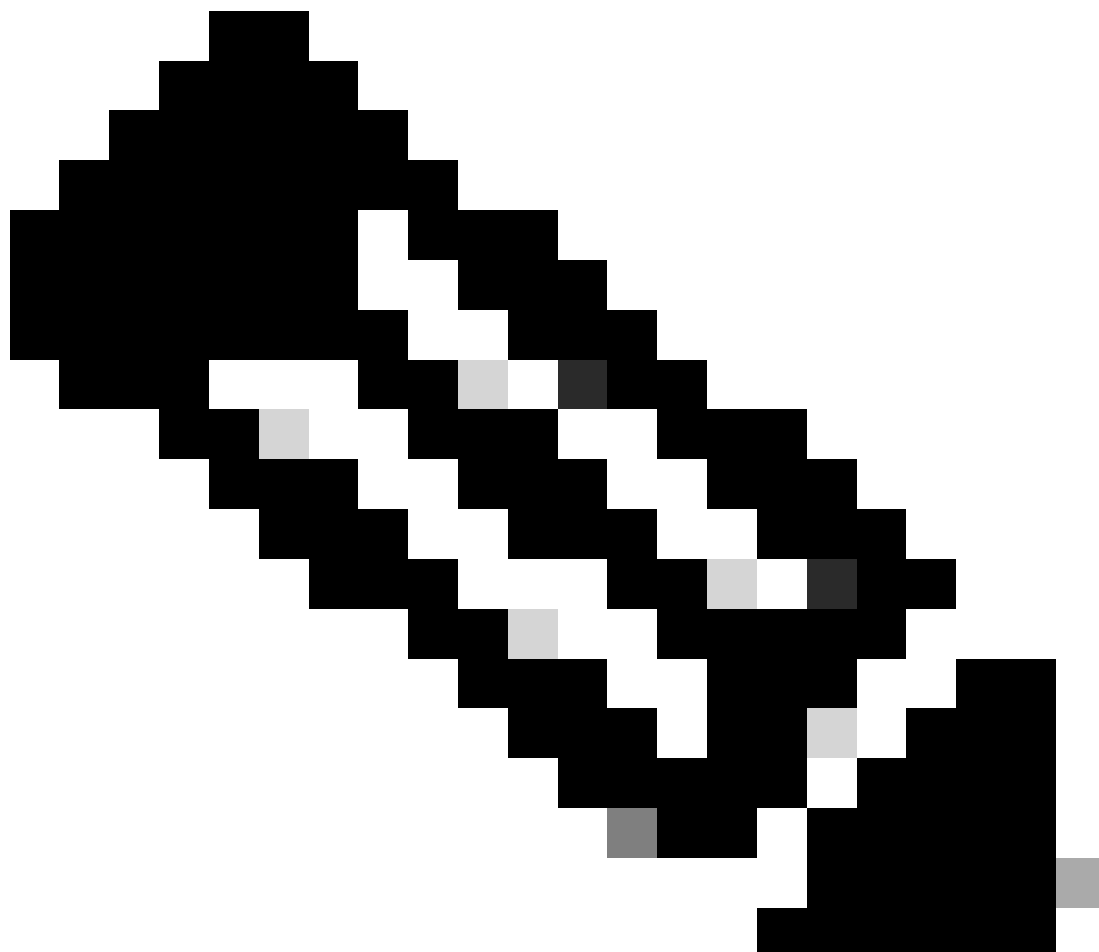
6. Una volta che l'utente ha approvato il Push DUO, il server proxy di autenticazione DUO invia una conferma al PSN per indicare che la richiesta di autenticazione è stata accettata dall'utente.

7. Il nodo PSN invia la conferma all'FTD per informare che l'utente è stato autenticato.

8. L'FTD riceve la conferma di autenticazione e stabilisce la connessione VPN all'endpoint con le misure di sicurezza appropriate in atto.

9. L'FTD registra i dettagli della connessione VPN riuscita e trasmette in modo sicuro i dati di contabilità al nodo ISE per scopi di registrazione e verifica.

10. Il nodo ISE registra le informazioni contabili nei propri registri, garantendo che tutti i record siano archiviati in modo sicuro e siano accessibili per futuri audit o controlli di conformità.



Nota:

L'impostazione di questa guida utilizza i seguenti parametri di rete:

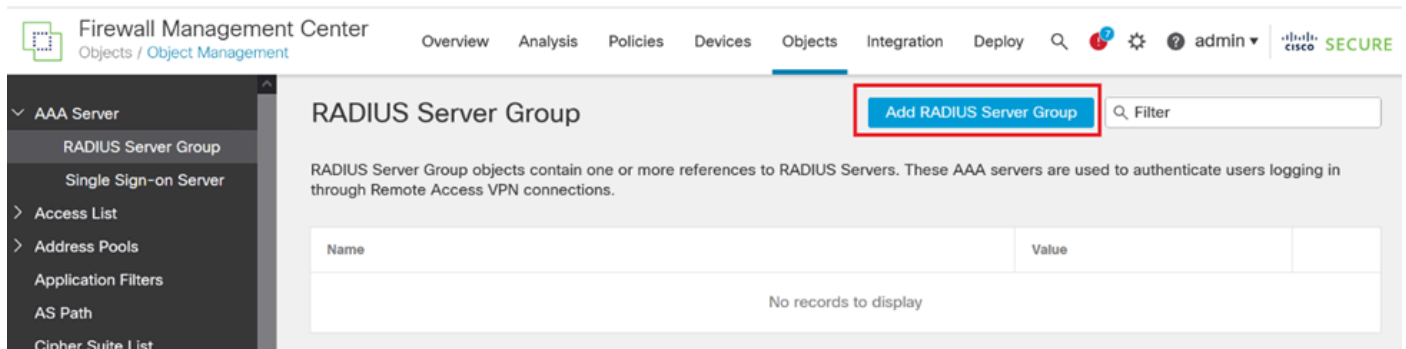
- IP nodo PNS (Primary Network Server): 10.4.23.21
- Firepower Threat Defense (FTD) IP per VPN peer: 10.4.23.53
- IP proxy di autenticazione DUO: 10.31.126.207
- Nome dominio: testlab.local

## Configurazioni

### Configurazioni FTD.

Integrazione di un server RADIUS in Firepower Management Center (FMC)

1. Accedere al CCP avviando il browser Web e immettendo l'indirizzo IP del CCP per aprire l'interfaccia grafica dell'utente (GUI).
2. Passare al menu Oggetti, selezionare Server AAA, quindi passare all'opzione Gruppo server RADIUS.
3. Fare clic sul pulsante Aggiungi gruppo di server RADIUS per creare un nuovo gruppo per i server RADIUS.



Gruppo server RADIUS.

4. Inserire un nome descrittivo per il nuovo gruppo di server AAA RADIUS per garantire una chiara identificazione all'interno dell'infrastruttura di rete.
5. Procedere con l'aggiunta di un nuovo server RADIUS selezionando l'opzione appropriata nella configurazione di gruppo.

Server

## RADIUS Servers (Maximum 16 servers)

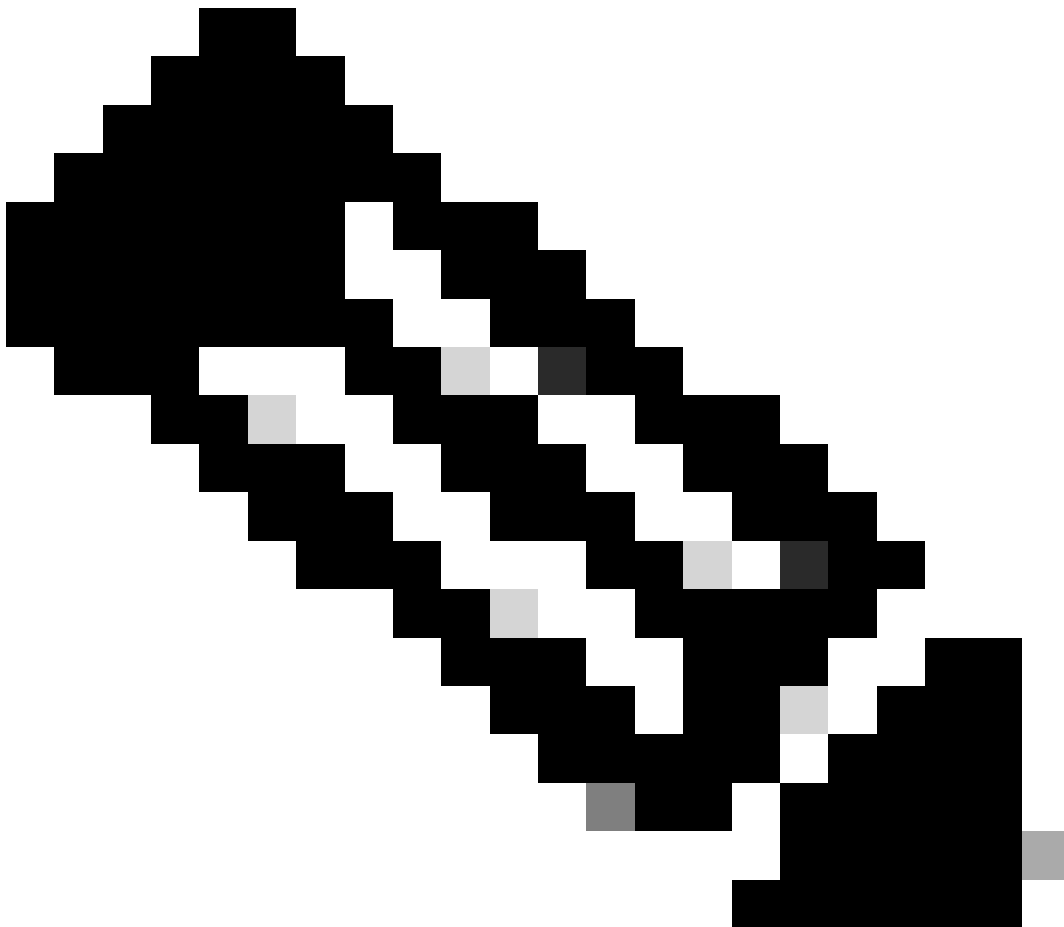


IP Address/Hostname	
No records to display	

RADIUS.

6. Specificare l'indirizzo IP dei server RADIUS e immettere la chiave segreta condivisa.

---



**Nota:** per stabilire una connessione RADIUS riuscita, è essenziale che questa chiave segreta venga condivisa in modo sicuro con il server ISE.

---

## New RADIUS Server



IP Address/Hostname:\*

10.4.23.21

*Configure DNS at Threat Defense Platform Settings to resolve hostname*

Authentication Port:\* (1-65535)

1812

Key:\*

●●●●●●●●

Confirm Key:\*

●●●●●●●●

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing  Specific Interface



Cancel

Save

*Nuovo server RADIUS.*

7. Dopo aver configurato i dettagli del server RADIUS, fare clic su Salva per salvare le impostazioni per il gruppo di server RADIUS.

## Add RADIUS Server Group



Enable authorize only

Enable interim account update

Interval:\* (1-120) hours

24

Enable dynamic authorization

Port:\* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

10.4.23.21



Cancel

Save

Dettagli gruppo server.

8. Per finalizzare e implementare la configurazione del server AAA nella rete, passare al menu Distribuisci, quindi selezionare Distribuisci tutto per applicare le impostazioni.

Name	ISE
FTD_01	Ready for Deployment

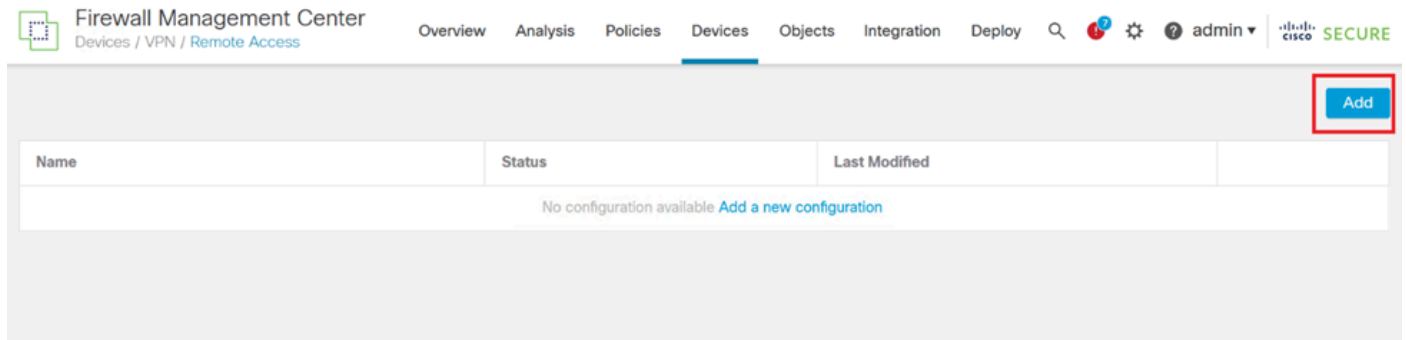
Distribuzione del server AAA.

Configurare la VPN remota.



1. Selezionare Devices > VPN > Remote Access (Dispositivi > Accesso remoto) nell'interfaccia utente di FMC per avviare il processo di configurazione della VPN.

2. Fare clic sul pulsante Add (Aggiungi) per creare un nuovo profilo di connessione VPN.

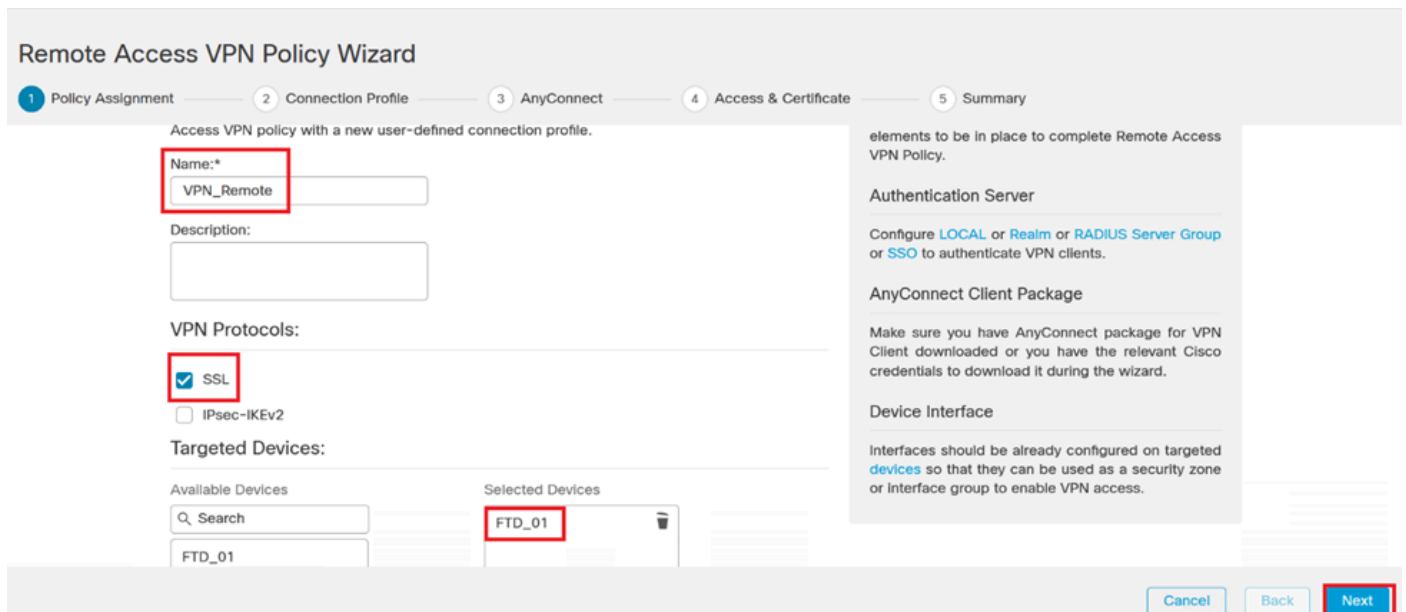


Profilo connessione VPN.

3. Inserisci un nome univoco e descrittivo per la VPN per identificarla all'interno delle impostazioni di rete.

4. Scegliere l'opzione SSL per garantire una connessione protetta utilizzando il protocollo SSL VPN.

5. Dall'elenco dei dispositivi, selezionare il dispositivo FTD specifico.



Impostazioni VPN.

6. Configurare il metodo AAA per utilizzare il nodo PSN nelle impostazioni di autenticazione.

## Remote Access VPN Policy Wizard

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

### 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: **AAA Only** ▼

Authentication Server:\* **ISE** ▼ +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: **Use same authentication server** ▼ +

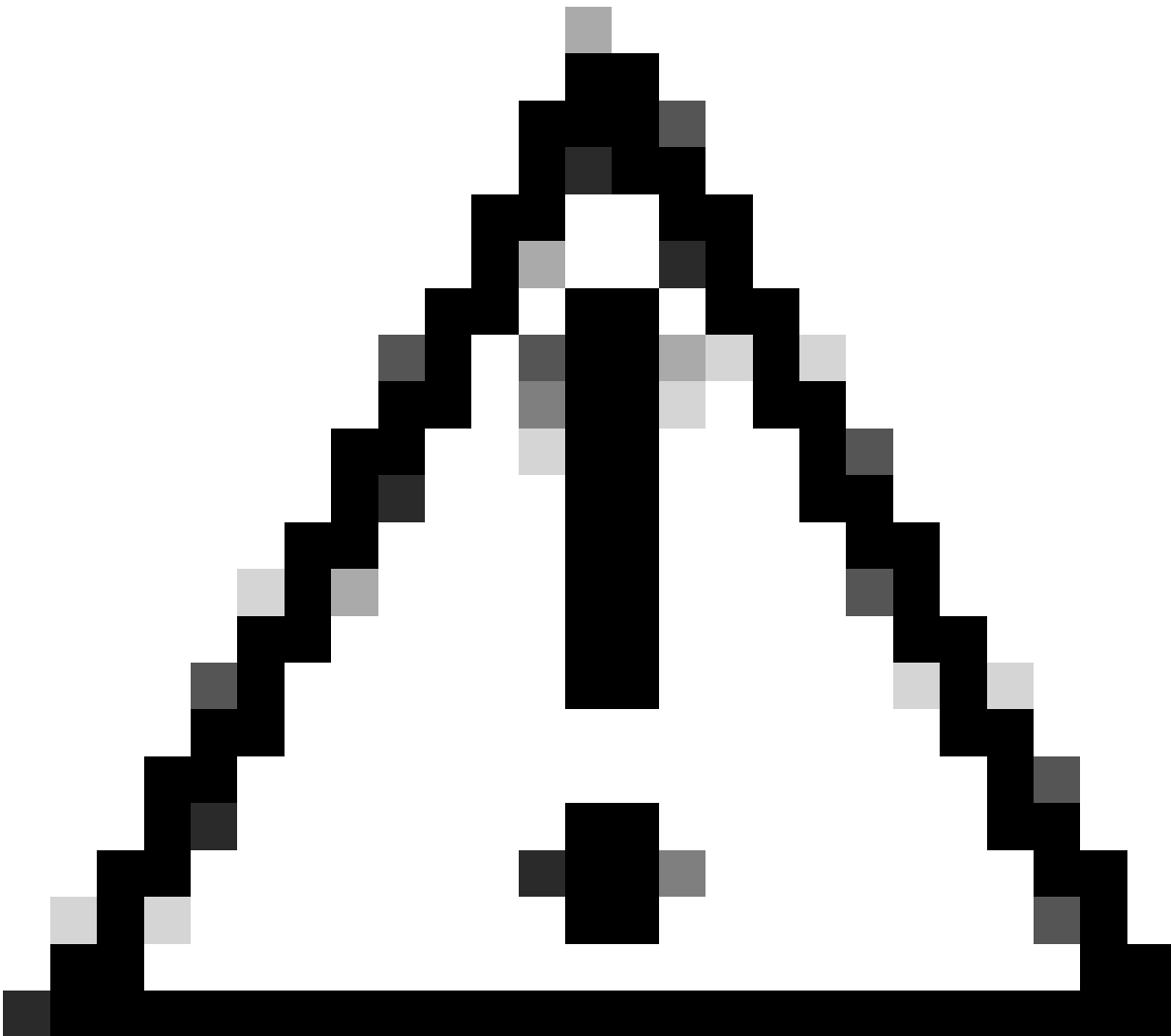
(realm or RADIUS)

Accounting Server: **ISE** ▼ +

(RADIUS)

*Profilo di connessione.*

7. Impostare l'assegnazione dell'indirizzo IP dinamico per la VPN.



---

Attenzione: ad esempio, è stato selezionato il pool VPN DHCP.

---

#### Client Address Assignment:

---

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:  

IPv6 Address Pools:  

*Pool di indirizzi IP.*

8. Procedere con la creazione di un nuovo oggetto Criteri di gruppo.

#### Group Policy:

---

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*   

[Edit Group Policy](#)

*Criteri di gruppo.*

9. Nelle impostazioni di Criteri di gruppo, verificare che sia selezionato il protocollo SSL.

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

### VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

Protocolli VPN

10. Creare un nuovo pool VPN o selezionarne uno esistente per definire l'intervallo di indirizzi IP disponibili per i client VPN.

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:



Name

IP Address Range

Cancel

Save

VPN pool.

11. Specificare i dettagli del server DNS per la connessione VPN.

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server:

+

Secondary DNS Server:

+

Primary WINS Server:

+

Secondary WINS Server:

+

DHCP Network Scope:

+

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel

Save

Impostazioni DNS.



Avviso: per questa configurazione, altre funzionalità come le opzioni Banner, Split Tunneling, AnyConnect e Advanced sono considerate facoltative.

---

12. Dopo aver configurato i dettagli necessari, fare clic su Next (Avanti) per procedere alla fase successiva dell'installazione.

## Remote Access VPN Policy Wizard

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

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*

[Edit Group Policy](#)

Cancel

Back

Next

*Criteria di gruppo.*

13. Selezionare il pacchetto AnyConnect appropriato per gli utenti VPN. Se il pacchetto richiesto non è presente nell'elenco, in questa fase è possibile aggiungere il pacchetto necessario.

## Remote Access VPN Policy Wizard

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

The VPN gateway can automatically download the latest AnyConnect 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 AnyConnect Client packages from [Cisco Software Download Center](#).

Select at least one AnyConnect Client image

[Show Re-order buttons](#)

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect-win-4.10.08029-we...	anyconnect-win-4.10.08029-webdeploy-k9...	Windows

Cancel

Back

Next

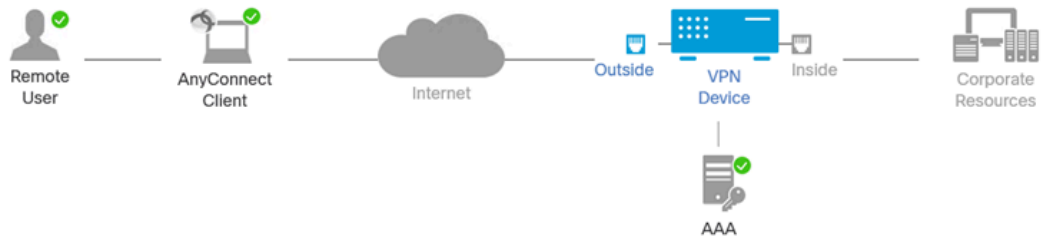
*Installazione del pacchetto.*

14. Scegliere l'interfaccia di rete sul dispositivo FTD in cui si desidera abilitare la funzione remota VPN.



## Remote Access VPN Policy Wizard

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



### 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.

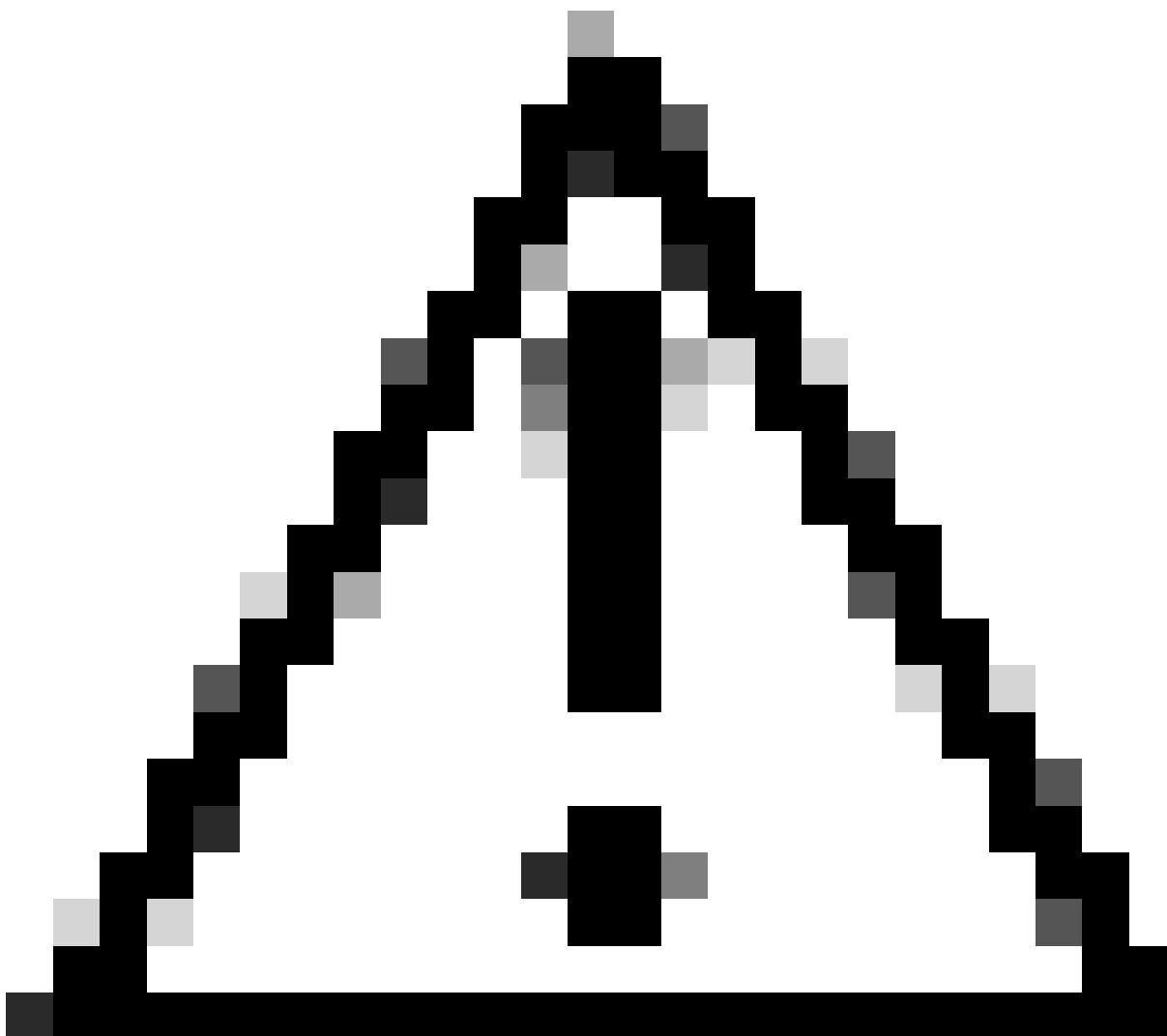
Interface group/Security Zone:\*  +

Enable DTLS on member interfaces

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

*Interfaccia VPN*

15. Stabilire una procedura di registrazione dei certificati selezionando uno dei metodi disponibili per creare e installare il certificato sul firewall, che è fondamentale per le connessioni VPN sicure.



Attenzione: ad esempio, in questa guida è stato selezionato un certificato autofirmato.

---

## 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:\*

*Certificato dispositivo.*

## Add Cert Enrollment



Name\*

Description

CA Information   Certificate Parameters   Key   Revocation

Enrollment Type: SCEP

Enrollment URL:\* Self Signed Certificate

Challenge Password: EST

Confirm Password: SCEP

Retry Period: Manual

Retry Count: 10 (Range 0-100)

Fingerprint:

PKCS12 File

Cancel Save

Registrazione certificato.

16. Fare clic su Avanti dopo aver configurato la registrazione del certificato.

## Remote Access VPN Policy Wizard

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

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:\*  +

### 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.

Riepilogo di accesso e servizi

17. Esaminare il riepilogo di tutte le configurazioni per verificare che siano accurate e corrispondano alla configurazione desiderata.

## Remote Access VPN Policy Wizard

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

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

Name:	VPN_Remote
Device Targets:	FTD_01
Connection Profile:	VPN_Remote
Connection Alias:	VPN_Remote
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE (RADIUS)
Authorization Server:	ISE (RADIUS)
Accounting Server:	ISE
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	Pool_VPN
Address Pools (IPv6):	-
Group Policy:	VPN_Remote_Policy
AnyConnect Images:	anyconnect-win-4.10.08029-webdeploy-k9.pkg
Interface Objects:	Outside
Device Certificates:	Cert_Enrollment

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. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- ▲ Network Interface Configuration
 

Make sure to add interface from targeted

Riepilogo delle impostazioni VPN.

18. Per applicare e attivare la configurazione dell'accesso remoto VPN, passare a Distribuisci > Distribuisci tutto ed eseguire la distribuzione sul dispositivo FTD selezionato.

Firewall Management Center  
Devices / VPN / Edit Connection Profile

Overview Analysis Policies Devices Objects Integration **Deploy** admin

VPN\_Remote  
Enter Description

Connection Profile Access Interfaces Advanced

Name	AAA
DefaultWEBVPGNGroup	Authentication: No Authorization: No Accounting: No
VPN_Remote	Authentication: IS Authorization: IS Accounting: IS

Advanced Deploy **Deploy All**

FTD\_01 Ready for Deployment (1)

1 device is available for deployment

Distribuzione delle impostazioni VPN.

## Configurazioni ISE.

Integrazione di DUO come server Radius esterno.

1. Selezionare Amministrazione > Risorse di rete > Server RADIUS esterni nell'interfaccia di amministrazione di Cisco ISE.
2. Fare clic sul pulsante Aggiungi per configurare un nuovo server RADIUS esterno.

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences NAC Managers More

External RADIUS Servers

Selected 0 Total 0

Edit **Add** Duplicate Delete

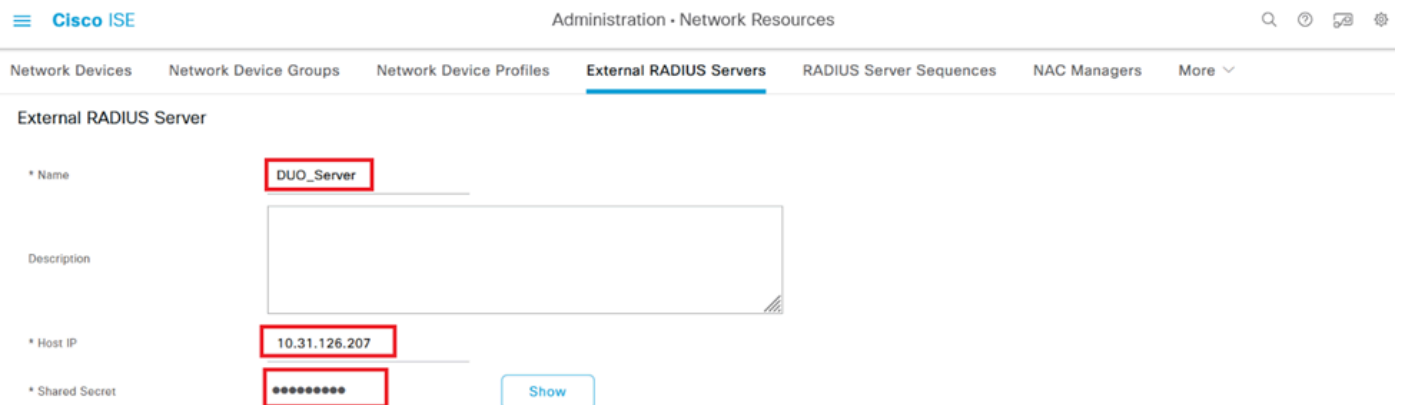
Name	Description
No data available	

Server Radius esterni

3. Inserire un nome per il server proxy DUO.
4. Immettere l'indirizzo IP corretto per il server Proxy DUO per garantire una corretta comunicazione tra il server ISE e il server DUO.
5. Impostare la chiave segreta condivisa.

**Nota:** per stabilire una connessione RADIUS correttamente, è necessario configurare la chiave segreta condivisa nel server proxy DUO.

6. Una volta immessi correttamente tutti i dettagli, fare clic su **Submit** (Invia) per salvare la nuova configurazione del server Proxy DUO.



The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb navigation is "Administration > Network Resources". The "External RADIUS Servers" tab is selected. The configuration form includes the following fields:

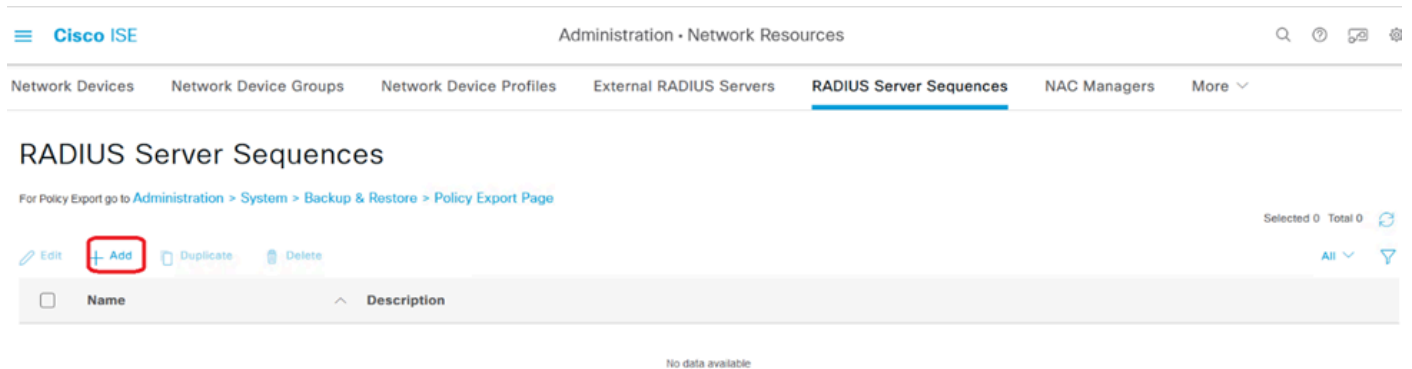
- Name:** DUO\_Server
- Description:** (Empty text area)
- Host IP:** 10.31.126.207
- Shared Secret:** (Masked with asterisks)

A "Show" button is located next to the Shared Secret field.

Server RADIUS esterni

7. Passare a Amministrazione > Sequenze server RADIUS.

8. Fare clic su Add per creare una nuova sequenza di server RADIUS.

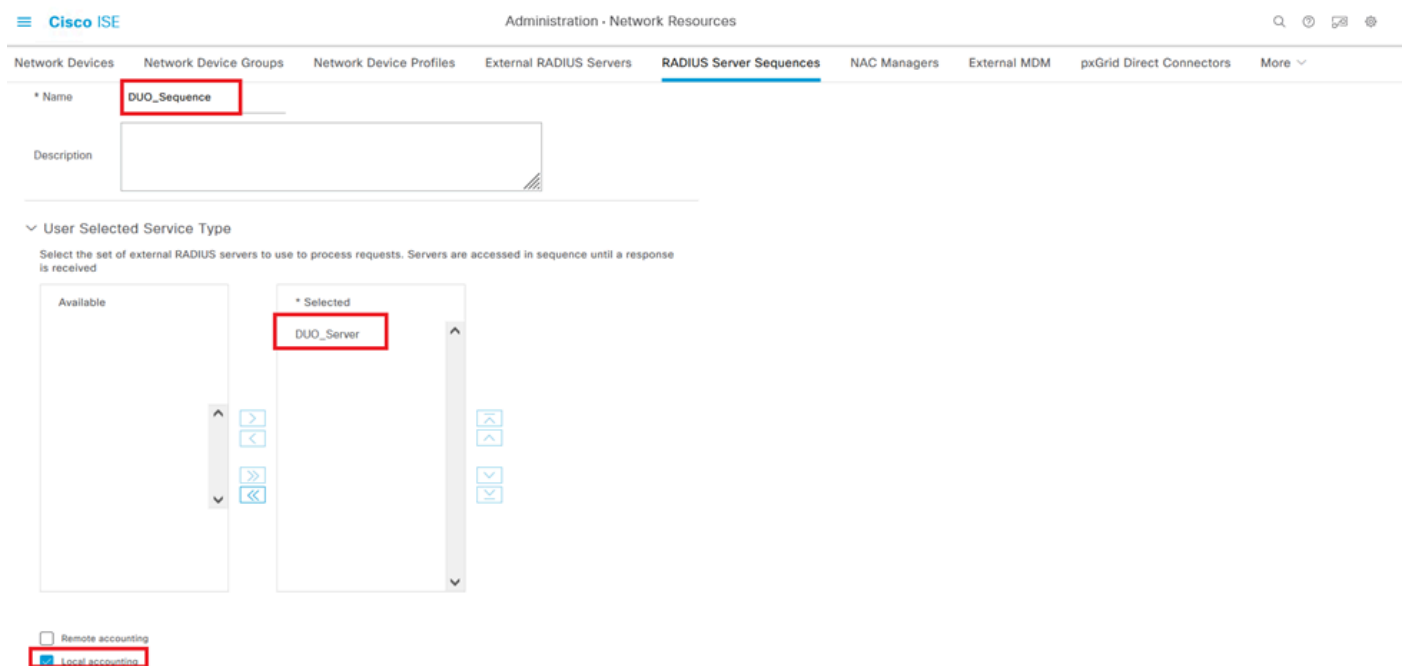


Sequenze server RADIUS

9. Fornire un nome distinto per la sequenza di server RADIUS per una facile identificazione.

10. Individuare il server RADIUS DUO precedentemente configurato, indicato come DUO\_Server in questa guida, e spostarlo nell'elenco selezionato a destra per includerlo nella sequenza.

11. Fare clic su Submit (Invia) per finalizzare e salvare la configurazione della sequenza di server RADIUS.

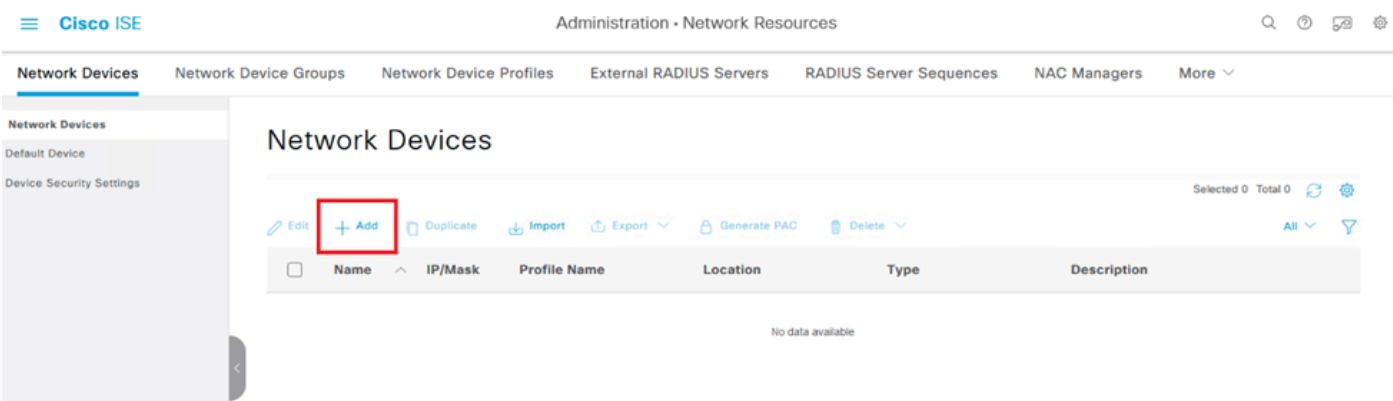


Configurazione delle sequenze del server Radius.

Integrare l'FTD come dispositivo di accesso alla rete.

1. Passare alla sezione Amministrazione nell'interfaccia di sistema e da qui, selezionare Risorse di rete per accedere all'area di configurazione per i dispositivi di rete.

2. Nella sezione Risorse di rete, individuare e fare clic sul pulsante Aggiungi per avviare il processo di aggiunta di un nuovo dispositivo di accesso alla rete.



Dispositivi di accesso alla rete.

3. Nei campi forniti, inserire il nome del dispositivo di accesso alla rete per identificare il dispositivo all'interno della rete.
4. Continuare a specificare l'indirizzo IP del dispositivo FTD (Firepower Threat Defense).
5. Inserire la chiave precedentemente stabilita durante l'installazione di FMC (Firepower Management Center). Questa chiave è essenziale per una comunicazione sicura tra i dispositivi.
6. Completare il processo facendo clic sul pulsante Sottometti.

[Network Devices List](#) > **FTD**

## Network Devices

Name **FTD**

Description

IP Address  \* IP : **10.4.23.53** / **32**

Aggiunta di FTD come AND.



## RADIUS Authentication Settings

### RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret  [Show](#)

Use Second Shared Secret [i](#)

Second Shared Secret  [Show](#)

CoA Port **1700** [Set To Default](#)

Impostazioni RADIUS

configurazioni DUO.

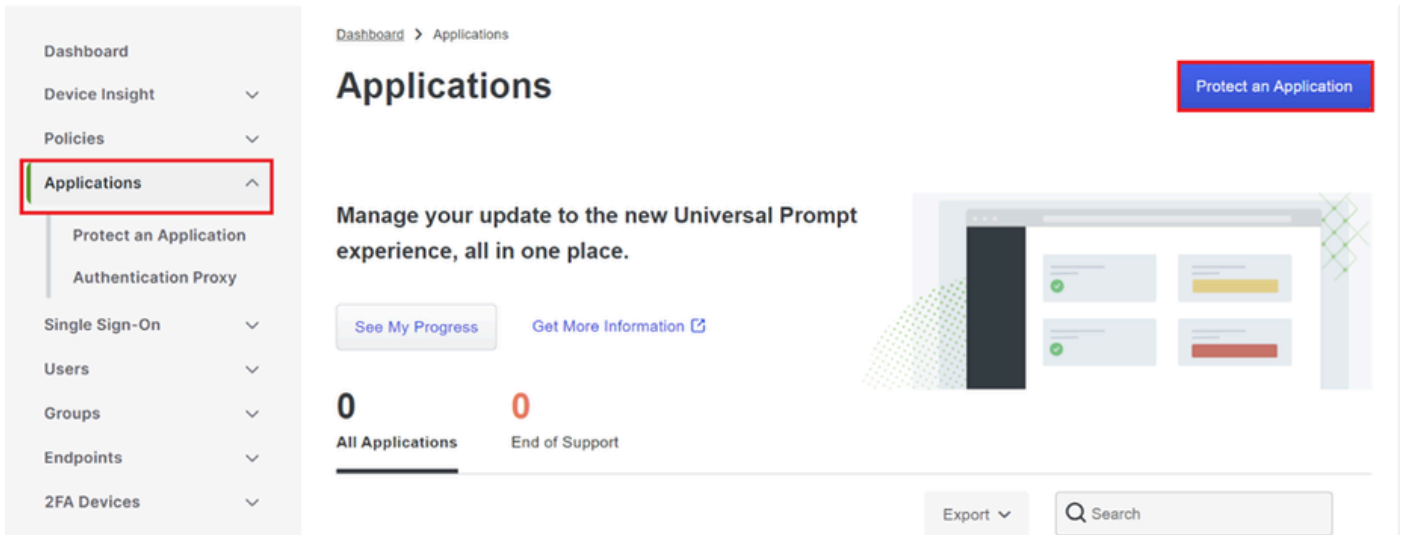
Installazione del proxy DUO.

Accedere alla DUO Proxy Download and Installation Guide facendo clic sul collegamento successivo:

<https://duo.com/docs/authproxy-reference>

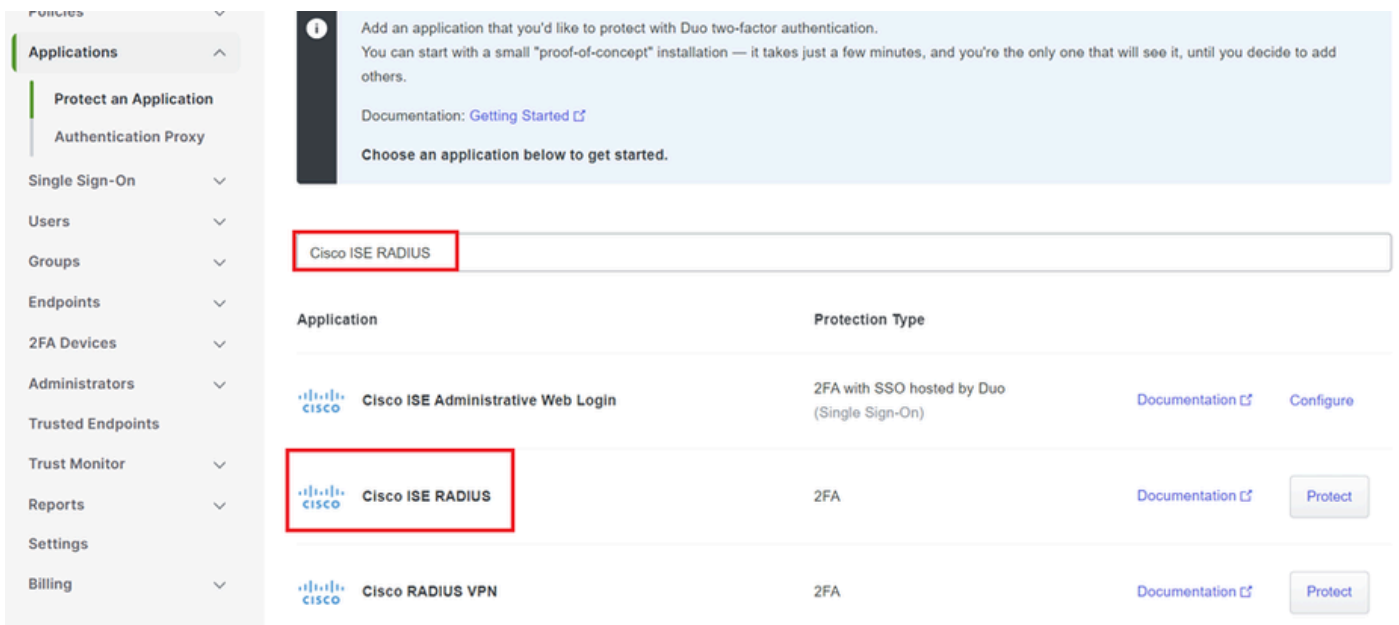
Integrazione di DUO Proxy con ISE e DUO Cloud.

1. Accedere al sito Web DUO Security all'indirizzo <https://duo.com/> utilizzando le proprie credenziali.
2. Passare alla sezione Applicazioni e selezionare Proteggi un'applicazione per continuare.



Applicazioni DUO

3. Cercare l'opzione "Cisco ISE RADIUS" nell'elenco e fare clic su Proteggi per aggiungerla alle applicazioni.



opzione ISE RADIUS

4. Una volta completata l'aggiunta, vedrai i dettagli della richiesta DUO. Scorrere verso il basso e fare clic su Salva.

5. Copiare la chiave di integrazione, la chiave segreta e il nome host dell'API forniti. Questi elementi sono fondamentali per le fasi successive.

✓ Application modified successfully.

Dashboard > Applications > Cisco ISE RADIUS

# Cisco ISE RADIUS

Authentication Log | Remove Application

Follow the [Cisco ISE RADIUS instructions](#).

## Details

Reset Secret Key

Integration key	DIX [REDACTED]	Copy
Secret key	.....ywLM	Copy
Don't write down your secret key or share it with anyone.		
API hostname	[REDACTED] duosecurity.com	Copy

[Dettagli sul server ISE](#)

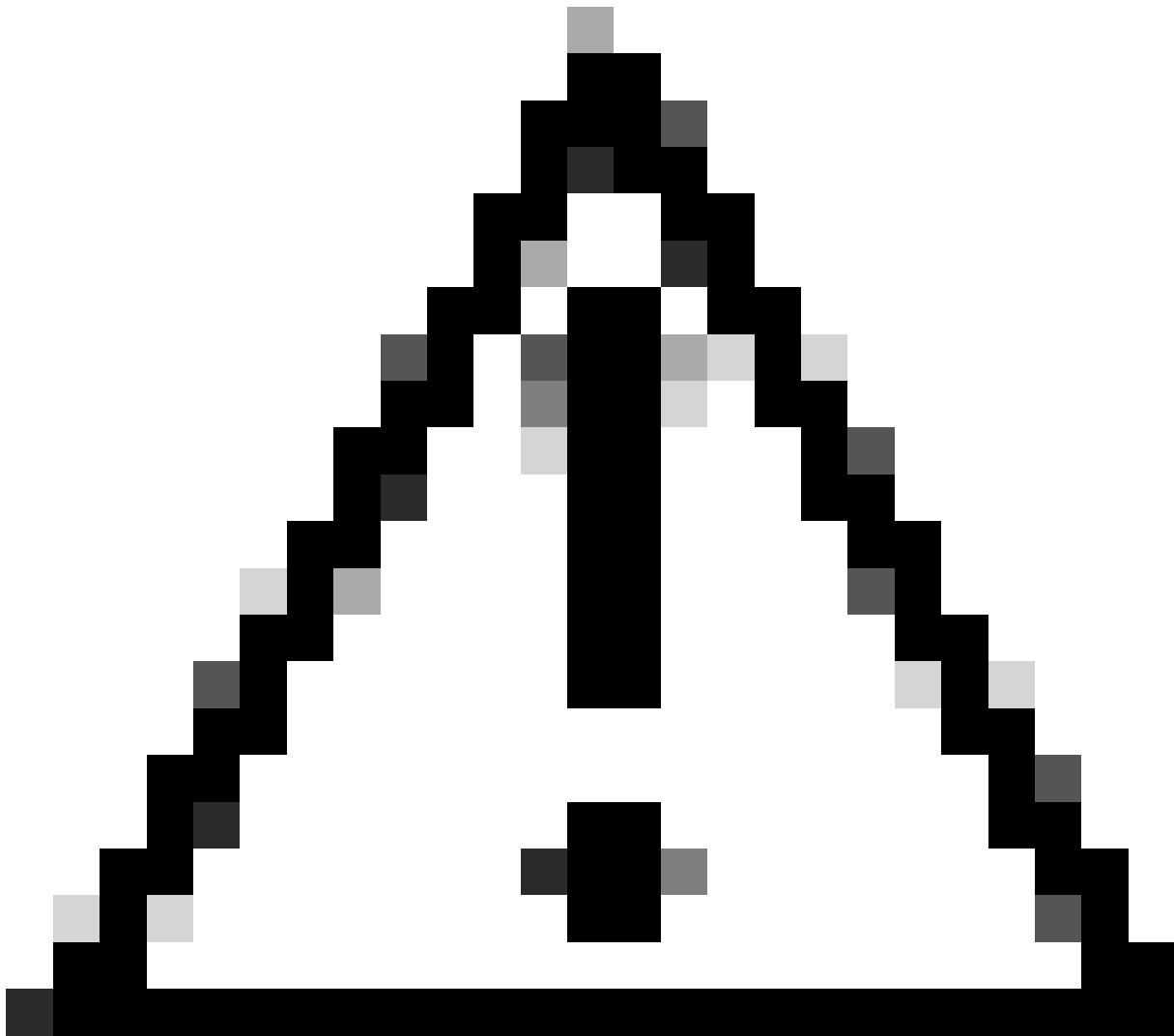
6. Avviare DUO Proxy Manager sul sistema per continuare l'installazione.



*DUO Proxy Manager*

7. (Facoltativo) Se il server proxy DUO richiede una configurazione proxy per la connessione al cloud DUO, immettere i parametri successivi:

```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```

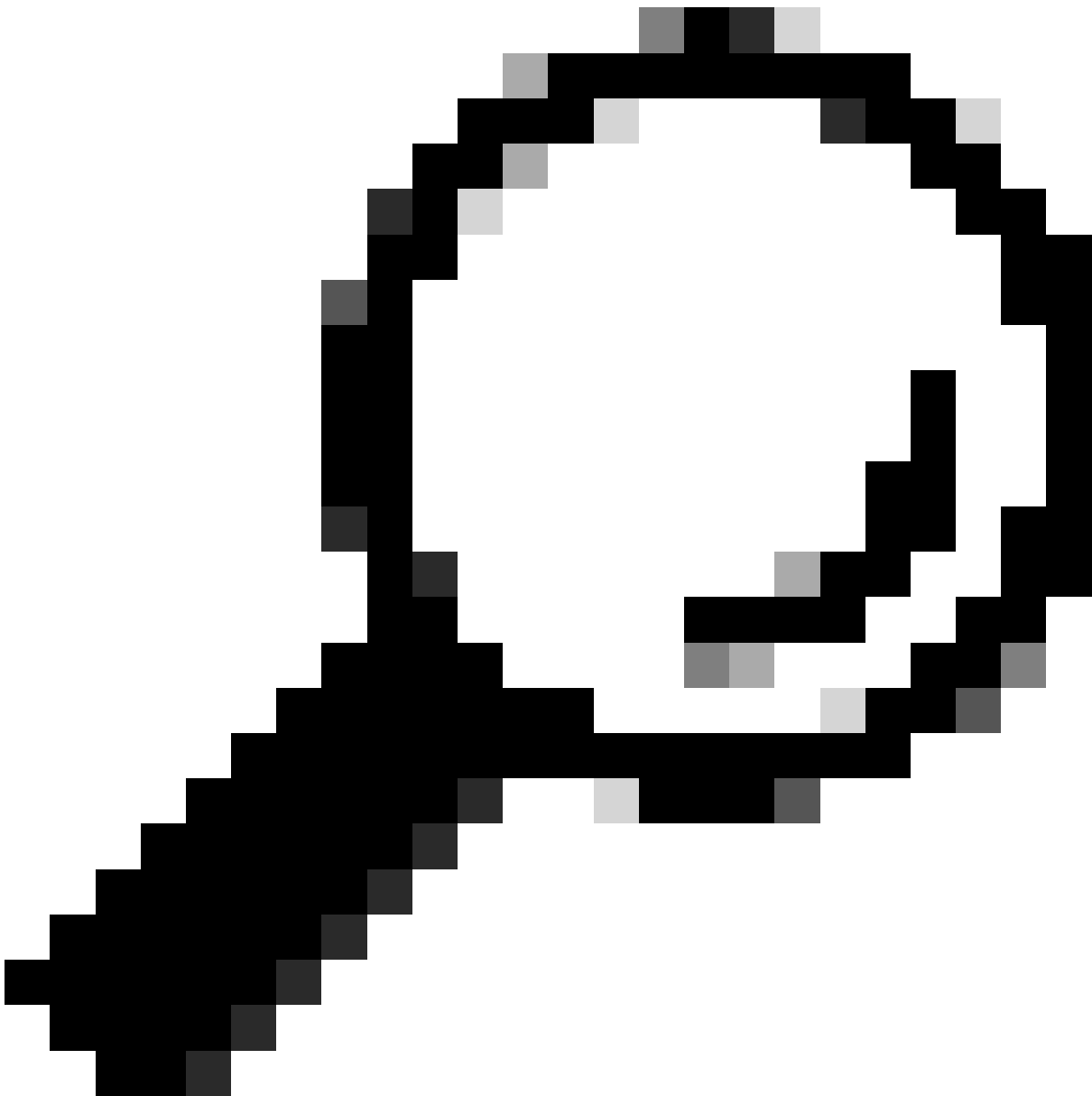


**Attenzione:** accertarsi di sostituire e con i dettagli effettivi del proxy.

---

8. Utilizzare ora le informazioni copiate in precedenza per completare la configurazione dell'integrazione.

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



**Suggerimento:** la riga `client=ad_client` indica che il proxy DUO esegue l'autenticazione utilizzando un account di Active Directory. Verificare che le informazioni siano corrette per completare la sincronizzazione con Active Directory.

---

Integrazione di DUO con Active Directory.

1. Integrare il proxy di autenticazione DUO con Active Directory.

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

2. Accedere ad Active Directory con i servizi cloud DUO. Accedere a <https://duo.com/>.

3. Passare a "Utenti" e selezionare "Sincronizzazione directory" per gestire le impostazioni di sincronizzazione.

Dashboard > Users

**Users** | Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

0 Total Users | 0 Not Enrolled | 0 Inactive Users | 0 Trash | 0 Bypass Users | 0 Locked Out

Select (0) | ... | Export | Search

No users shown based on your search.

*Sincronizzazione directory*

4. Fare clic su "Add New Sync" (Aggiungi nuova sincronizzazione) e scegliere "Active Directory" tra le opzioni disponibili.

Dashboard > Users > Directory Sync

**Directory Sync** | Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

*Aggiungi nuova sincronizzazione*

5. Selezionare Aggiungi nuova connessione e fare clic su Continua.

Dashboard > Users > Directory\_Sync > New Active Directory Sync

## New Active Directory Sync

**Connection**  
Set up a new connection using a new Authentication Proxy.

Reuse existing connection  
 **Add new connection**  
 You will be redirected to a new page

[Continue](#)

---

**Directory Sync Setup**

Waiting for connection to directory

Sync setup is disabled until a connection to the directory has been established.

**Directory Sync Setup**

- Connect to AD
- Add groups
- Review synced attributes

[Complete Setup](#)

Aggiunta di una nuova Active Directory

6. Copiare la chiave di integrazione generata, la chiave segreta e il nome host dell'API.

### Authentication Proxy

[Delete Connection](#) [No Changes](#)

**Status**

Not connected

- Add Authentication Proxy
- Configure Directory

---

**Connected Directory Syncs**

**User Syncs**

[AD Sync](#)

**Configuration metadata**

- To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
- Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).
- If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

**Integration key**  [Copy](#)

**Secret key**  [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

**API hostname**  [Copy](#)

Dettagli proxy di autenticazione

7. Tornare alla configurazione del proxy di autenticazione DUO e configurare la sezione `[cloud]` con i nuovi parametri ottenuti e le credenziali dell'account del servizio per un amministratore di Active Directory:

```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```

8. Convalidare la configurazione selezionando l'opzione "validate" per accertarsi che tutte le impostazioni siano corrette.

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skey=[redacted]uXWYwLM
8 api_host=a[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
16 host=10.4.23.42
17 service_account_username=administrator
18 service_account_password=[redacted]
```

Configurazione di Proxy DUO.

9. Dopo la convalida, salvare la configurazione e riavviare il servizio proxy di autenticazione DUO per applicare le modifiche.

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
several minutes...
[info] Testing section 'main' with configuration:
[info] {'http_proxy_host': 'cx[redacted]',
'http_proxy_port': '3128'}
[info] There are no configuration problems
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': '[redacted].duosecurity.com',
'client': 'ad_client',
'failmode': 'safe',
'http_proxy_host': '[redacted]',
'http_proxy_port': '3128',
'key': 'DIX[redacted]'}
```

Opzione Riavvia servizio.

10. Tornare al dashboard di amministrazione DUO, immettere l'indirizzo IP del server Active Directory insieme al DN di base per la sincronizzazione degli utenti.



---

## Directory Configuration

### Domain controller(s)

Hostname or IP address (1) \*

Port (1) \*

[+ Add Domain controller](#)

The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

---

### Base DN \*

Enter the full distinguished name (DN) of the directory location to search for users and groups. We recommend setting this to the directory root (example: DC=domain,DC=local). If specifying the DN of an OU or container, ensure it is **above both the users and groups to sync**.

---

*Impostazioni directory.*

11. Selezionare l'opzione Plain per configurare il sistema per l'autenticazione non NTLMv2.

---

## Authentication type



**Integrated**

Performs Windows authentication from a domain-joined system.



**NTLMv2**

Performs Windows NTLMv2 authentication.



**Plain**

Performs username-password authentication.

*Tipo di autenticazione.*

12. Salvare le nuove impostazioni per assicurarsi che la configurazione sia aggiornata.

 Delete Connection

Save

## Status

Not connected

Add Authentication Proxy



Configure Directory

---

## Connected Directory Syncs

### User Syncs

[AD Sync](#)

*Salva, opzione*

13. Utilizzare la funzionalità "test connessione" per verificare che il servizio cloud DUO sia in

grado di comunicare con Active Directory.

## Authentication Proxy

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

**Integration key**  [Copy](#)

**Secret key**  [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

**API hostname**  [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

```
service_account_username=myusername  
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. [Test Connection](#).

*Opzione Test connessione.*

14. Confermare che lo stato di Active Directory sia "Connesso", a indicare che l'integrazione è riuscita.

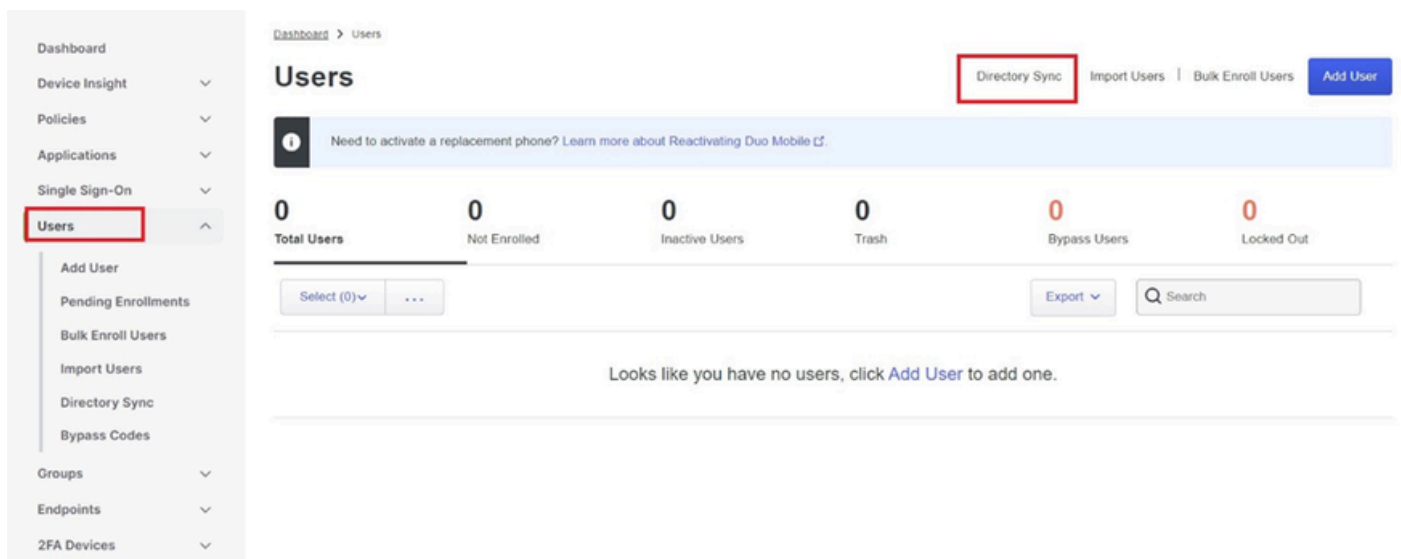
## Status

Connected

*Stato: operazione completata.*

Esporta account utente da Active Directory (AD) tramite DUO Cloud.

1. Passare a Utenti > Sincronizzazione directory nel pannello di amministrazione Duo per individuare le impostazioni relative alla sincronizzazione della directory con Active Directory.

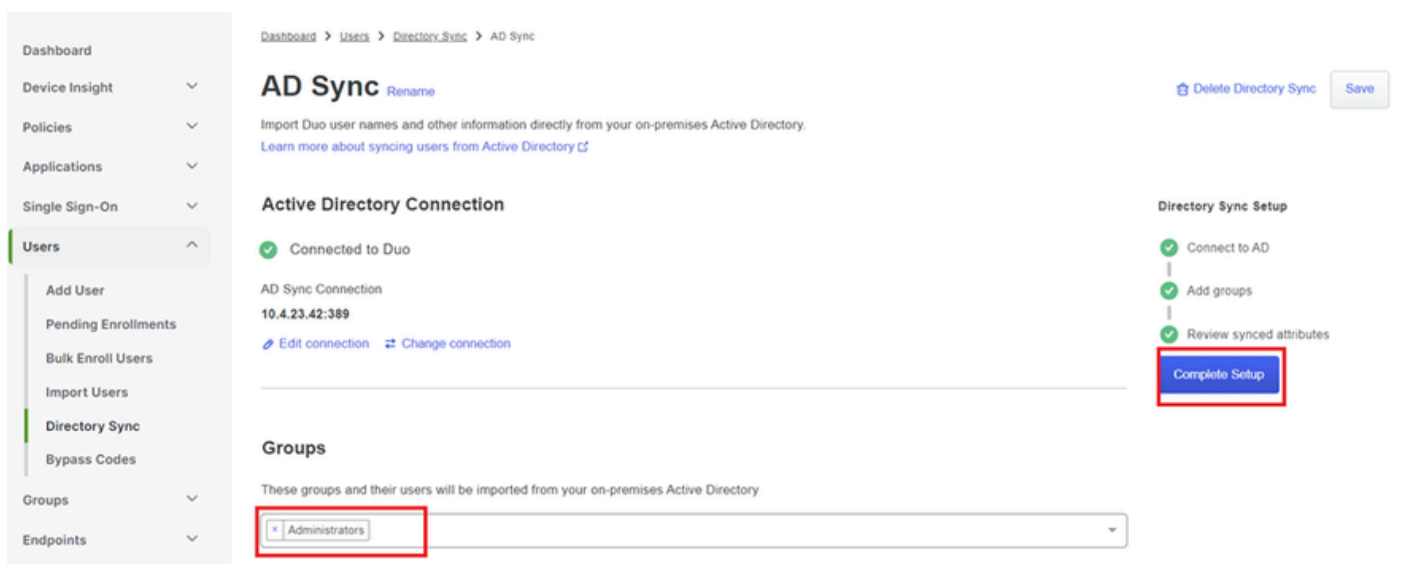


Elenco utenti.

2. Selezionare la configurazione di Active Directory che si desidera gestire.

3. Nelle impostazioni di configurazione, identificare e scegliere i gruppi specifici in Active Directory che si desidera sincronizzare con Duo Cloud. Prendere in considerazione l'utilizzo delle opzioni di filtro per la selezione.

4. Fare clic su Completa impostazione.



Sincronizzazione AD

5. Per avviare immediatamente la sincronizzazione, fare clic su Sincronizza. In questo modo gli account utente vengono esportati dai gruppi specificati in Active Directory nel cloud Duo, consentendo la gestione di tali account nell'ambiente Duo Security.

# AD Sync Rename

Delete Directory Sync No Changes

Import Duo user names and other information directly from your on-premises Active Directory.  
[Learn more about syncing users from Active Directory](#)

## Sync Controls

### Sync status

Scheduled to automatically synchronize every 12 hours, next around 2:00 AM UTC [Pause automatic syncs](#)

**Sync Now**

[Troubleshooting](#)

### Active Directory Connection

Connected to Duo

AD Sync Connection

10.4.23.42:389

[Edit connection](#)

[Change connection](#)

Avvio della sincronizzazione

Registrare gli utenti nel cloud Cisco DUO.

La registrazione degli utenti consente la verifica dell'identità tramite vari metodi, ad esempio l'accesso al codice, il push DUO, i codici SMS e i token.

1. Passare alla sezione Utenti nel dashboard di Cisco Cloud.
2. Individuare e selezionare l'account dell'utente che si desidera iscrivere.

Dashboard > Users

Users Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#)

1 Total Users    1 Not Enrolled    1 Inactive Users    0 Trash    0 Bypass Users    0 Locked Out

Select (0) ...    Export    Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input checked="" type="checkbox"/>	administrator		oteg...			Active	Never authenticated

1 total

Elenco account utente.

3. Fare clic sul pulsante Invia messaggio di posta elettronica iscrizione per avviare il processo di iscrizione.

# administrator

Logs

Send Enrollment Email

Sync This User



This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.



This user was synced from the directory **AD Sync**. Some fields are read-only.

Username

administrator

Username aliases

[+ Add a username alias](#)

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for a specific alias

(e.g., Username alias 1 should only be used for Employee ID).

Iscrizione tramite e-mail.

4. Controllare la posta in arrivo e aprire l'invito di registrazione per completare il processo di autenticazione.

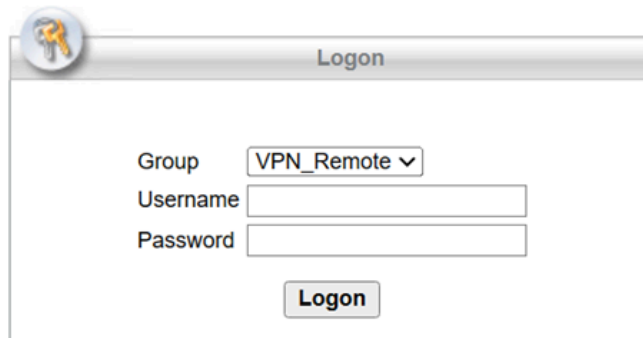
Per ulteriori informazioni sul processo di iscrizione, fare riferimento alle seguenti risorse:

- Guida alla registrazione universale: <https://guide.duo.com/universal-enrollment>
- Guida alle iscrizioni tradizionali: <https://guide.duo.com/traditional-enrollment>

Procedura di convalida della configurazione.

Per garantire l'accuratezza e il funzionamento delle configurazioni, convalidare i passaggi successivi:

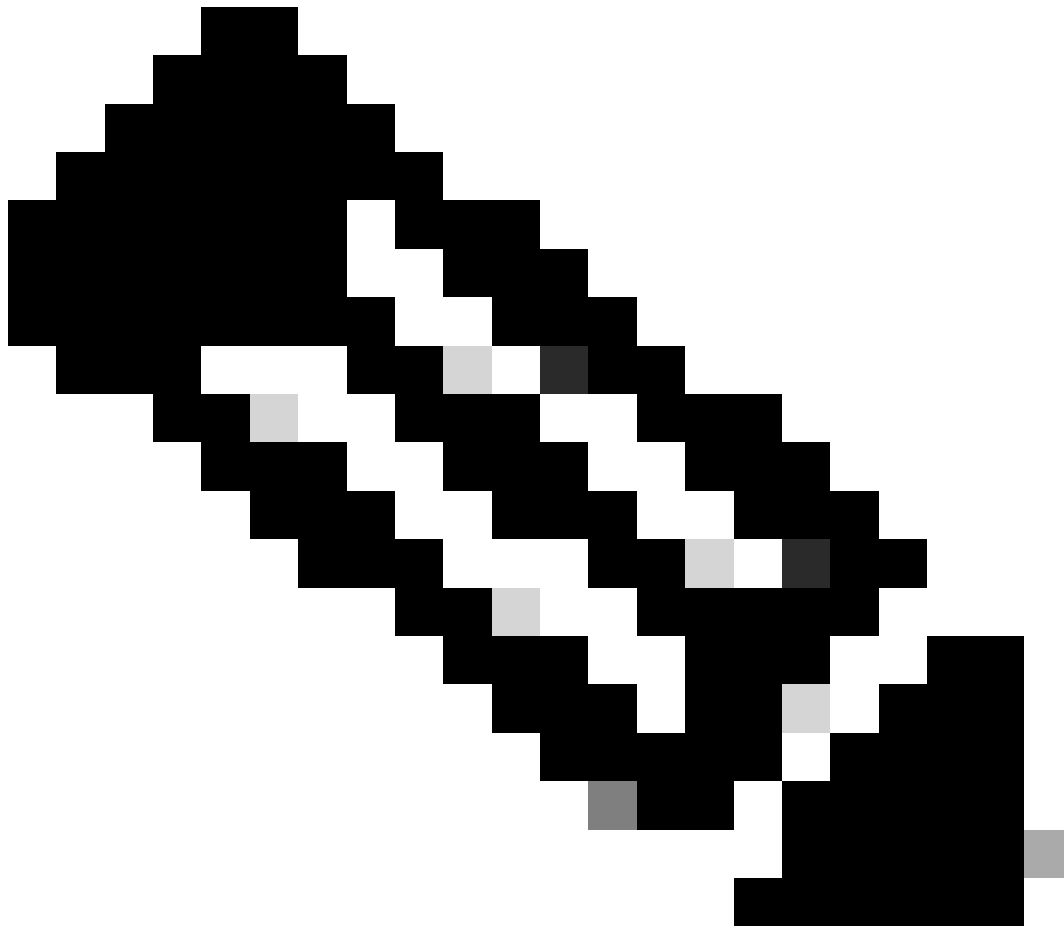
1. Avviare un browser Web e immettere l'indirizzo IP del dispositivo Firepower Threat Defense (FTD) per accedere all'interfaccia VPN.



The image shows a web browser window titled "Logon". The window has a grey header bar with a key icon on the left and the word "Logon" in the center. Below the header, there are three input fields: a dropdown menu for "Group" with "VPN\_Remote" selected, a text box for "Username", and a text box for "Password". Below these fields is a "Logon" button.

Accesso VPN.

2. Inserire il nome utente e la password quando richiesto.



Nota: le credenziali fanno parte degli account di Active Directory.

---

3. Quando si riceve una notifica Push DUO, approvarla utilizzando il software mobile DUO per procedere con il processo di convalida.



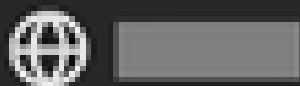


(1) Login request waiting.

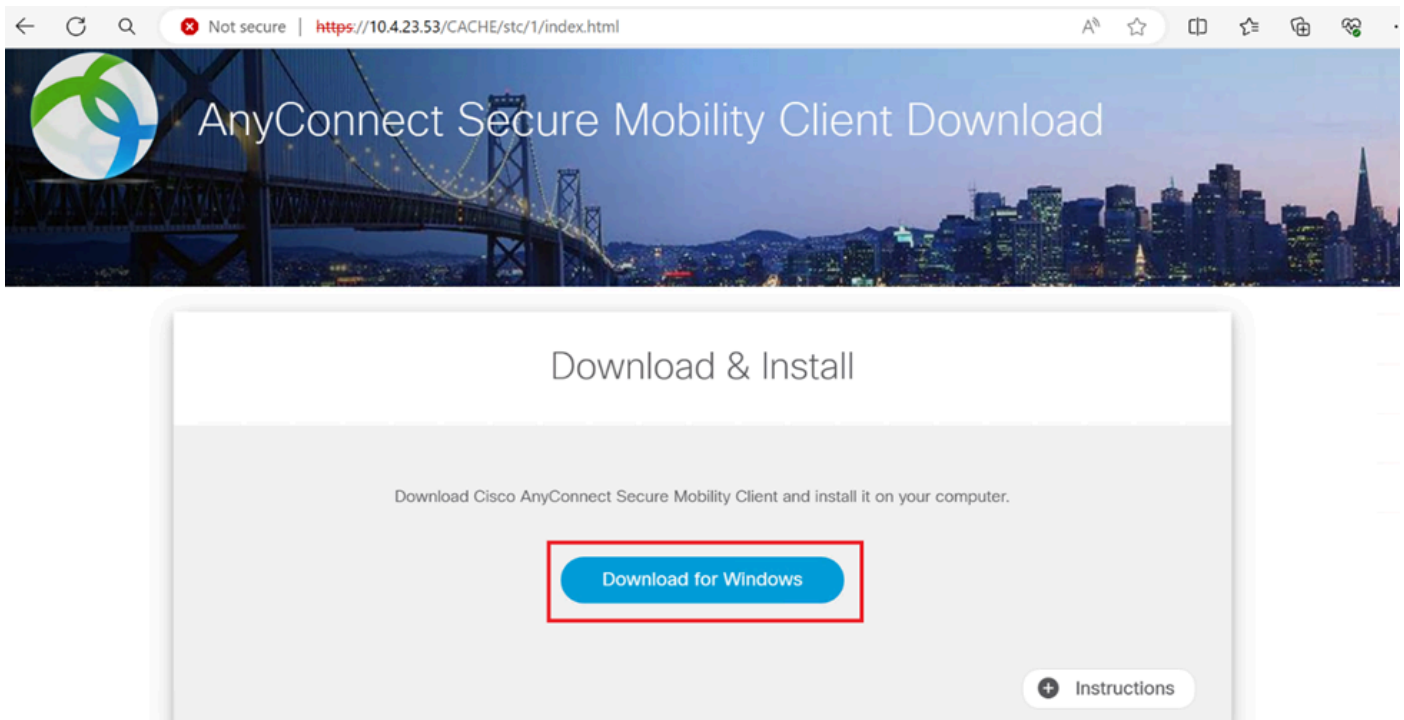
[Respond](#)



Are you logging in to Cisco ISE  
**RADIUS?**



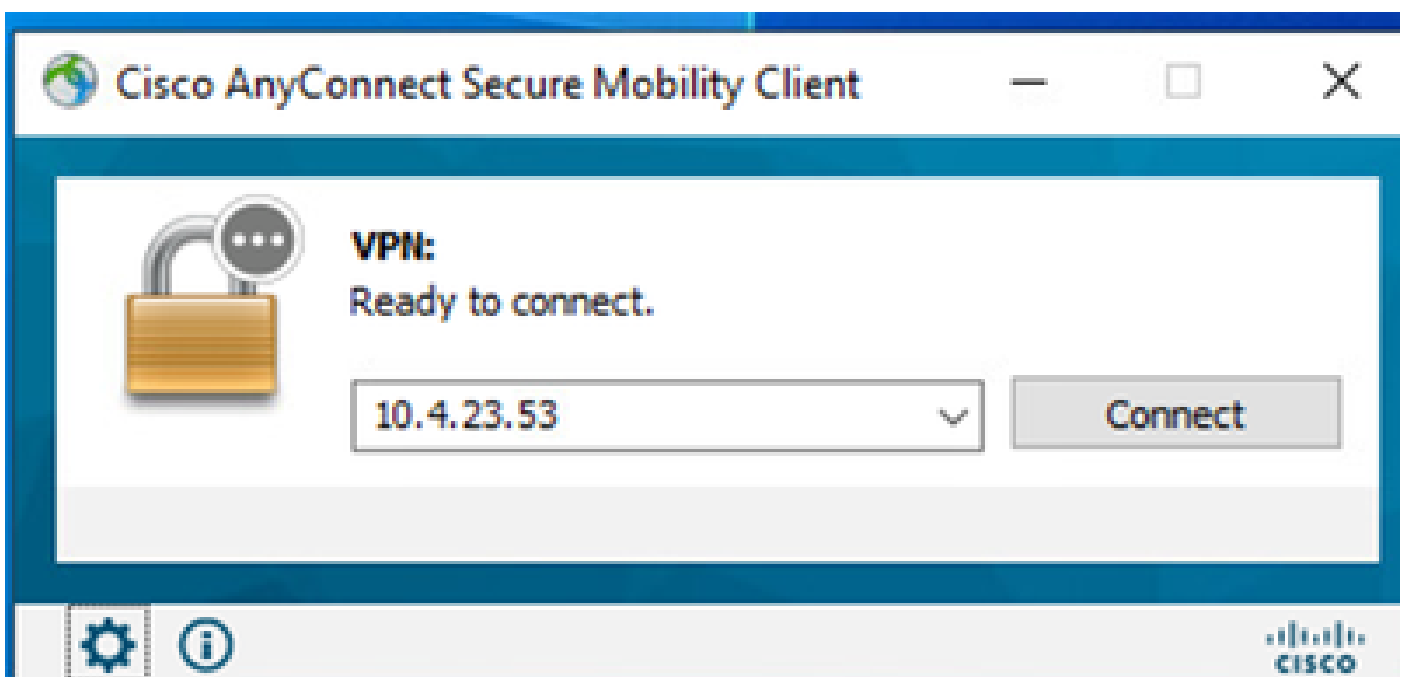
Individuare e scaricare il pacchetto Cisco AnyConnect VPN Client appropriato per i sistemi Windows.



Scarica e installa.

5. Eseguire il file di installazione di AnyConnect scaricato e continuare a completare le istruzioni fornite dal programma di installazione sul dispositivo Windows.

6. Aprire Cisco AnyConnect Secure Mobility Client. Connettersi alla VPN immettendo l'indirizzo IP del dispositivo FTD.



Software Any Connect.

7. Quando richiesto, immettere le credenziali di accesso VPN e autorizzare di nuovo la notifica

Push DUO per autenticare la connessione.



(1) Login request waiting.

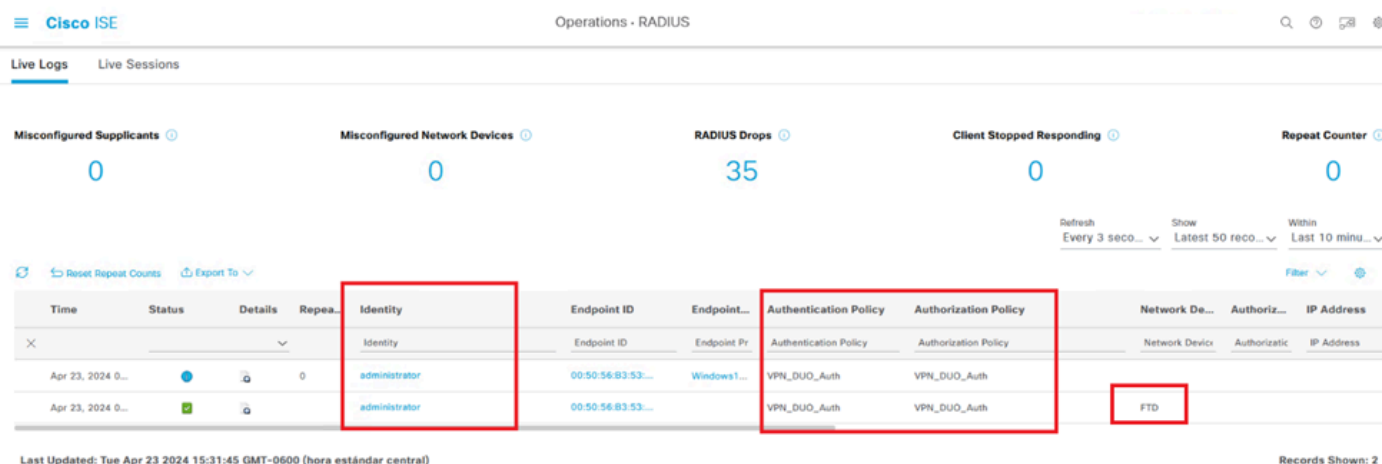
[Respond](#)



Are you logging in to Cisco ISE  
RADIUS?

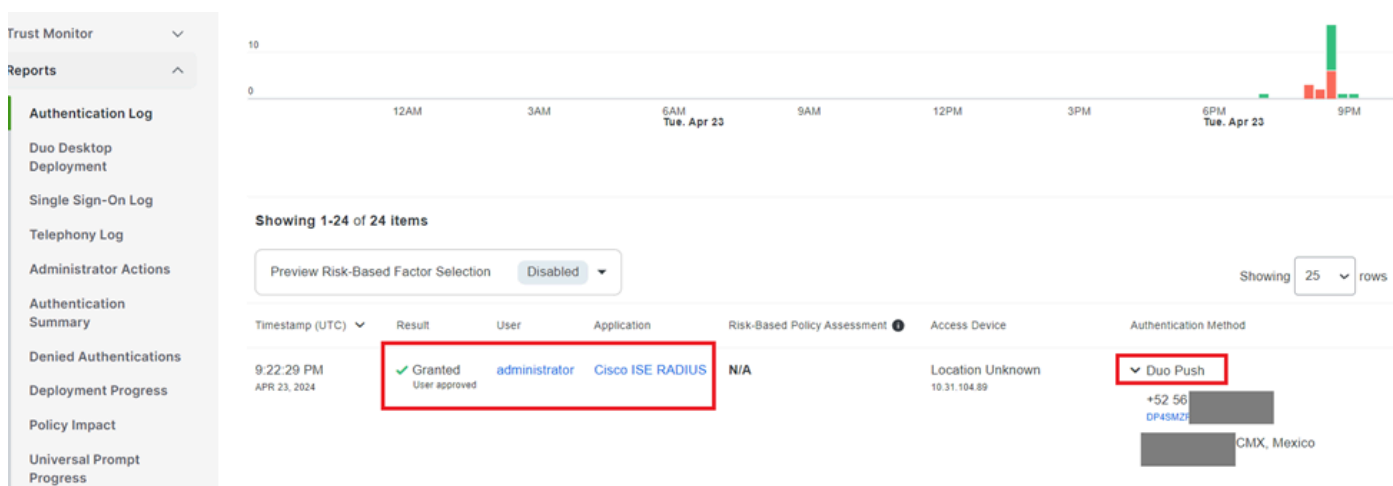


per monitorare l'attività in tempo reale e verificare la corretta connettività, accedere ai log attivi in Cisco Identity Services Engine (ISE).



ISE Livelogs

9. Andare a Rapporti > Log di autenticazione per esaminare i log di autenticazione nel pannello di amministrazione DUO per confermare le verifiche riuscite.



Log di autenticazione.

## Problemi comuni.

### Scenario di lavoro.

Prima di esaminare gli errori specifici relativi a questa integrazione, è fondamentale comprendere lo scenario di lavoro generale.

Nei live log ISE possiamo confermare che ISE ha inoltrato i pacchetti RADIUS al proxy DUO e, una volta che l'utente ha accettato il DUO Push, il server proxy DUO ha inviato il modulo RADIUS Access Accept.

Overview

Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Endpoint Profile	
Authentication Policy	VPN_DUO_Auth
Authorization Policy	VPN_DUO_Auth
Authorization Result	

Authentication Details

Source Timestamp	2024-04-24 20:03:33.142
Received Timestamp	2024-04-24 20:03:33.142
Policy Server	asc-ise32p3-1300
Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Calling Station Id	10.31.104.89
Audit Session Id	000000000002e000662965a9
Network Device	FTD

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.NetworkDeviceName
- 11358 Received request for RADIUS server sequence.
- 11361 Valid incoming authentication request
- 11355 Start forwarding request to remote RADIUS server
- 11365 Modify attributes before sending request to external radius server
- 11100 RADIUS-Client about to send request - ( port = 1812 )
- 11101 RADIUS-Client received response ( Step latency=5299 ms)
- 11357 Successfully forwarded request to current remote RADIUS server
- 11002 Returned RADIUS Access-Accept

Autenticazione riuscita.

CiscoAVPair

mdm-tlv=device-platform=win,  
mdm-tlv=device-mac=00-50-56-b3-53-d6,  
mdm-tlv=device-type=VMware, Inc. VMware7,1,  
mdm-tlv=device-platform-version=10.0.19045 ,  
mdm-tlv=device-public-mac=00-50-56-b3-53-d6,  
mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.08029,  
mdm-tlv=device-uid-  
global=4CEBE2C21A8B81F490AC91086452CF3592593437,  
mdm-tlv=device-  
uid=3C5C68FF5FD3B6FA9D364DDB90E2B0BFA7E44B0EAAA  
CA383D5A8CE0964A799DD,  
audit-session-id=000000000002e000662965a9,  
ip:source-ip=10.31.104.89  
coa-push=true,  
proxy-flow=[10.4.23.53,10.4.23.21]

Result

Reply-Message Success. Logging you in...

Risultato: operazione completata.

Un pacchetto acquisito dal lato ISE mostra le informazioni seguenti:

Source	Destination	Protocol	Length	Info	
10.4.23.53	10.4.23.21	RADIUS	741	Access-Request id=138	→ The FTD sends the RADIUS request to ISE
10.4.23.21	10.31.126.207	RADIUS	883	Access-Request id=41	→ ISE resends the same RADIUS requests to the DUO Proxy
10.31.126.207	10.4.23.21	RADIUS	190	Access-Accept id=41	→ DUO Proxy sends the RADIUS accept (DUO push approved)
10.4.23.21	10.4.23.53	RADIUS	90	Access-Accept id=138	→ ISE resend the RADIUS accept to the FTD
10.4.23.53	10.4.23.21	RADIUS	739	Accounting-Request id=139	→ FTD sends the accounting for the current VPN connection
10.4.23.21	10.4.23.53	RADIUS	62	Accounting-Response id=139	→ ISE registered the accounting on its dashboard

ISE packet capture.

**Errore11368 Esaminare i log sul server RADIUS esterno per determinare la causa esatta dell'errore.**

Event	<b>5400 Authentication failed</b>
Failure Reason	<b>11368 Please review logs on the External RADIUS Server to determine the precise failure reason.</b>
Resolution	Please review logs on the External RADIUS Server to determine the precise failure reason.
Root cause	Please review logs on the External RADIUS Server to determine the precise failure reason.

Errore 1368.

Risoluzione dei problemi:

- Verificare che la chiave segreta condivisa RADIUS in ISE sia la stessa della chiave configurata nel FMC.

1. Aprire l'interfaccia utente grafica di ISE.
  2. Amministrazione > Risorse di rete > Dispositivi di rete.
  3. Scegliere il server proxy DUO.
  4. Accanto al segreto condiviso, fare clic su "Mostra" per visualizzare la chiave in formato testo normale.
  5. Aprire la GUI del CCP.
  6. Oggetti > Gestione oggetti > Server AAA > Gruppo server RADIUS.
  7. Scegliere il server ISE.
  8. Inserire nuovamente la chiave segreta.
- Verificare l'integrazione di Active Directory in DUO.

1. Aprire DUO Authentication Proxy Manager.

2. Confermare utente e password nella sezione [ad\_client].
3. Fare clic su Convalida per confermare che le credenziali correnti sono corrette.

### Errore 11353: nessun altro server RADIUS esterno. Impossibile eseguire il failover

Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover
Resolution	Verify the following: At least one of the remote RADIUS servers in the ISE proxy service is up and configured properly ; Shared secret specified in the ISE proxy service for every remote RADIUS server is same as the shared secret specified for the ISE server ; Port of every remote RADIUS server is properly specified in the ISE proxy service.
Root cause	Failover is not possible because no more external RADIUS servers are configured. Dropping the request.

Errore 1353.

#### Risoluzione dei problemi:

- Verificare che la chiave segreta condivisa RADIUS in ISE sia la stessa chiave configurata nel server proxy DUO.

1. Aprire l'interfaccia utente grafica di ISE.
2. Amministrazione > Risorse di rete > Dispositivi di rete.
3. Scegliere il server proxy DUO.
4. Accanto al segreto condiviso, fare clic su "Mostra" per visualizzare la chiave in formato testo normale.
5. Aprire DUO Authentication Proxy Manager.
6. Verificare la sezione [radius\_server\_auto] e confrontare la chiave segreta condivisa.

Le sessioni RADIUS non vengono visualizzate nei log live di ISE.

#### Risoluzione dei problemi:

- Verificare la configurazione DUO.

1. Aprire DUO Authentication Proxy Manager.
2. Verificare l'indirizzo IP ISE nella sezione [radius\_server\_auto]



- Verificare la configurazione FMC.

1. Aprire la GUI del CCP.

2. Selezionare Oggetti > Gestione oggetti > Server AAA > Gruppo server RADIUS.

3. Scegliere il server ISE.

4. Verificare l'indirizzo IP di ISE.

- Acquisire un pacchetto ad ISE per confermare la ricezione dei pacchetti RADIUS.

1. Selezionare Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Dump TCP

Ulteriori procedure di risoluzione dei problemi.

- Abilitare i componenti successivi nel PSN per il debug:

Policy-engine

Port-JNI

runtime-AAA

Per ulteriori informazioni sulla risoluzione dei problemi in DUO Authentication Proxy Manager, selezionare il collegamento successivo:

[https://help.duo.com/s/article/1126?language=en\\_US](https://help.duo.com/s/article/1126?language=en_US)

## Modello DUO.

È possibile utilizzare il modello successivo per completare la configurazione nel server proxy DUO.

```
[main] <--- OPTIONAL
http_proxy_host=<Proxy IP address or FQDN>
http_proxy_port=<Proxy port>
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxxxxx
radius_ip_1=<PSN IP Address>
radius_secret_1=xxxxxxxxxx
failmode=safe
port=1812
client=ad_client
```

```
[ad_client]
host=<AD IP Address>
service_account_username=xxxxxxxx
service_account_password=xxxxxxxx
```

search\_dn=DC=xxxxxx,DC=xxxx

[cloud]

ikey=xxxxxxxxxxxxxxxxxxxx

skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

api\_host=xxxxxxxxxxxxxxxxxxxx

service\_account\_username=<your domain\username>

service\_account\_password=xxxxxxxxxxxx

## 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).