# Configura & Autenticazione SAML DUO

## Sommario



## Introduzione

Questo documento descrive un esempio di implementazione dell'autenticazione basata su certificati e dell'autenticazione DUO SAML.

## Prerequisiti

Gli strumenti e i dispositivi utilizzati nella guida sono:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- CA (Certification Authority) interna
- Cisco DUO Premier Account
- Cisco DUO Authentication Proxy
- Cisco Secure Client (CSC)

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN di base,
- SSL/TLS

- Infrastruttura a chiave pubblica
- Esperienza con FMC
- Cisco Secure Client
- Codice FTD 7.2.0 o superiore
- Cisco DUO Authentication Proxy

### Componenti usati

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

- Cisco FTD (7.3.1)
- Cisco FMC (7.3.1)
- Cisco Secure Client (5.0.02075)
- Cisco DUO Authentication Proxy (6.0.1)
- Mac OS (13.4.1)
- Active Directory

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.

## Configurazione delle fasi su DUO

In questa sezione vengono descritti i passaggi per configurare Cisco DUO Single Sign-on (SSO). Prima di iniziare, verificare che il proxy di autenticazione sia implementato.

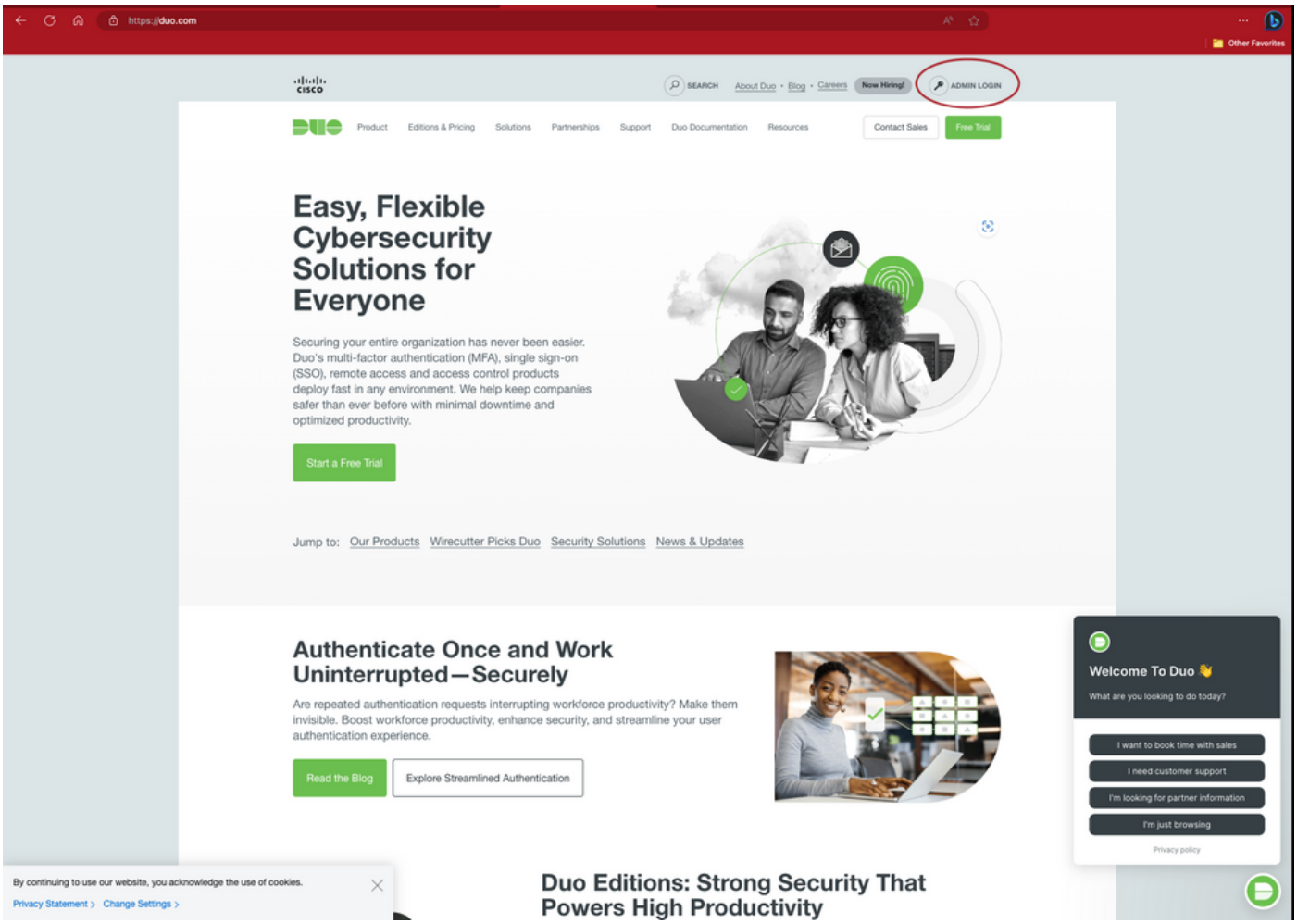
---

Avviso: Se non è stato implementato un proxy di autenticazione, questo collegamento contiene la guida per questa attività. DUO Authentication Proxy Guide

---

### Creare un criterio di protezione delle applicazioni

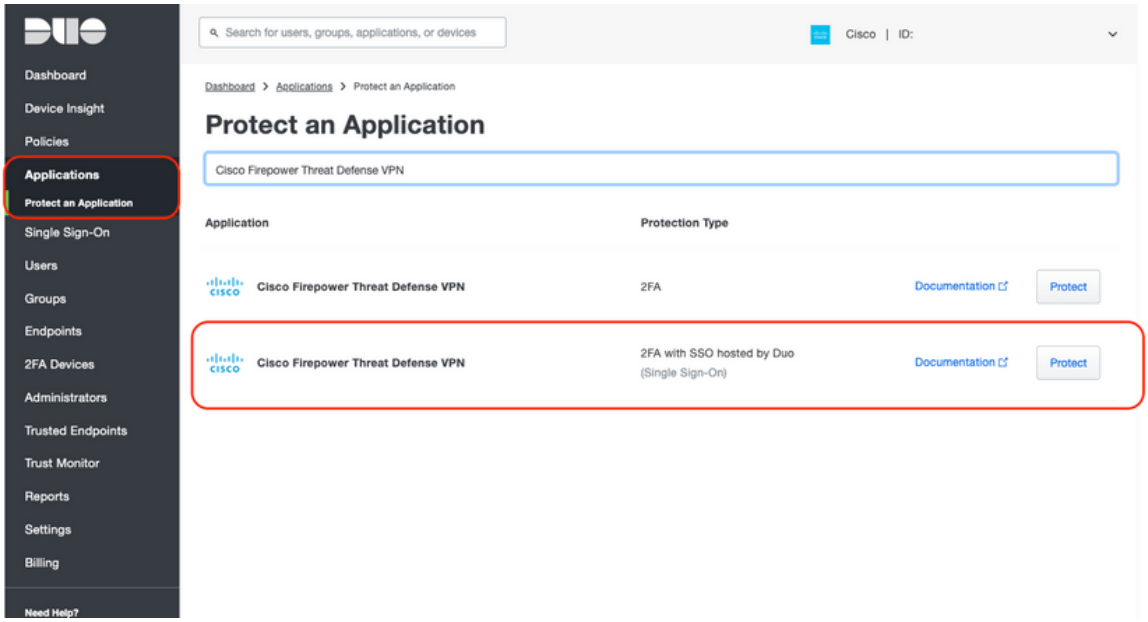
Passaggio 1. Accedere al pannello di amministrazione tramite questo collegamento a Cisco Duo




Home page Cisco DUO

Passaggio 2. Passare a Dashboard > Applicazioni > Proteggi applicazione.

Nella barra di ricerca, immettere "Cisco Firepower Threat Defense VPN" e selezionare "Proteggi".




Proteggere uno screenshot di un'applicazione

Selezionare l'opzione solo con il tipo di protezione "2FA con SSO ospitato da Duo".

Passaggio 3: Copiare queste informazioni URL in Metadati.

- ID entità provider di identità
- URL SSO
- URL di disconnessione


Esempio di informazioni da copiare

Nota: I link sono stati omessi dallo screenshot.

Passaggio 4. Selezionare "Scarica certificato" per scaricare il certificato del provider di identità in Download.

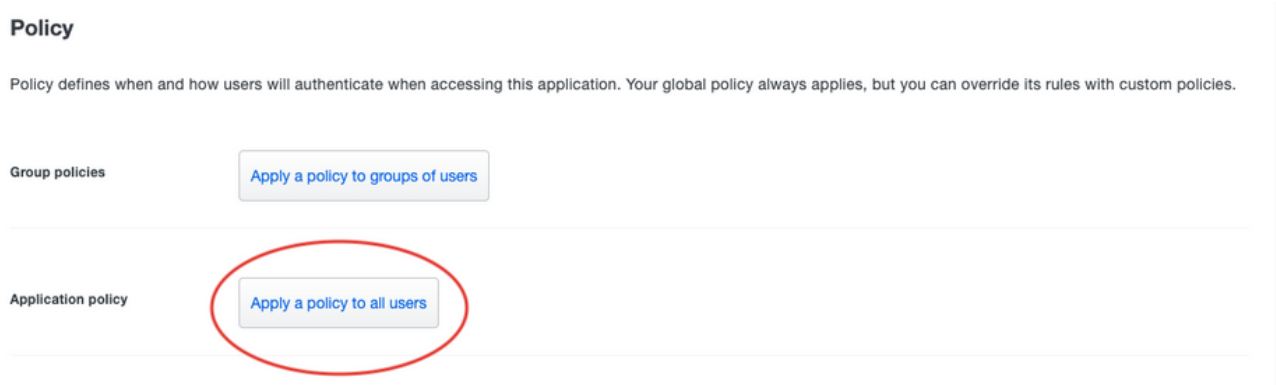
Passaggio 5. Inserire le informazioni sul provider di servizi

URL di base di Cisco Firepower: FQDN utilizzato per raggiungere l'FTD

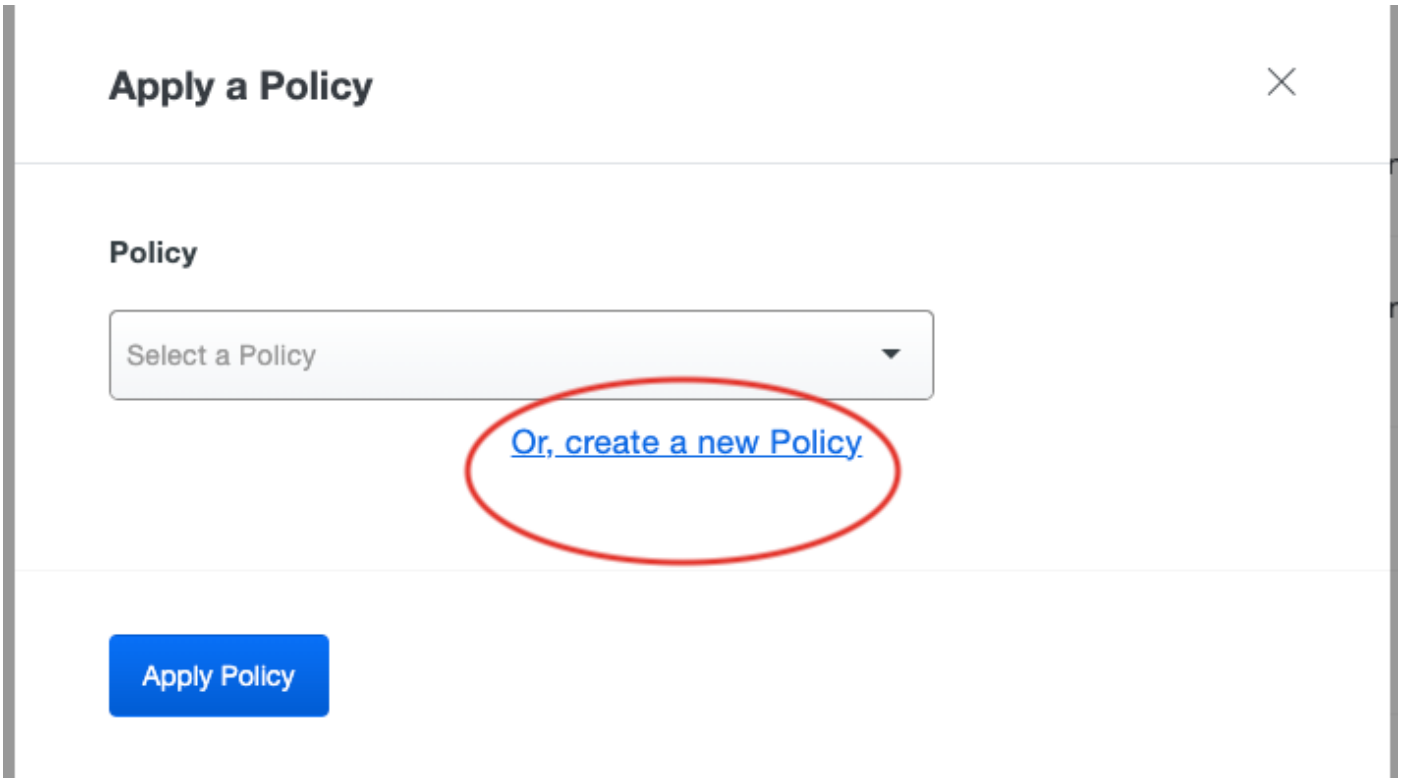
Nome profilo connessione: il nome del gruppo di tunnel

## Crea criterio di applicazione

Passaggio 1: Per creare un criterio di applicazione in Criterio Selezionare "Applica un criterio a tutti gli utenti", quindi selezionare "Oppure, crea un nuovo criterio" come mostrato nell'immagine.

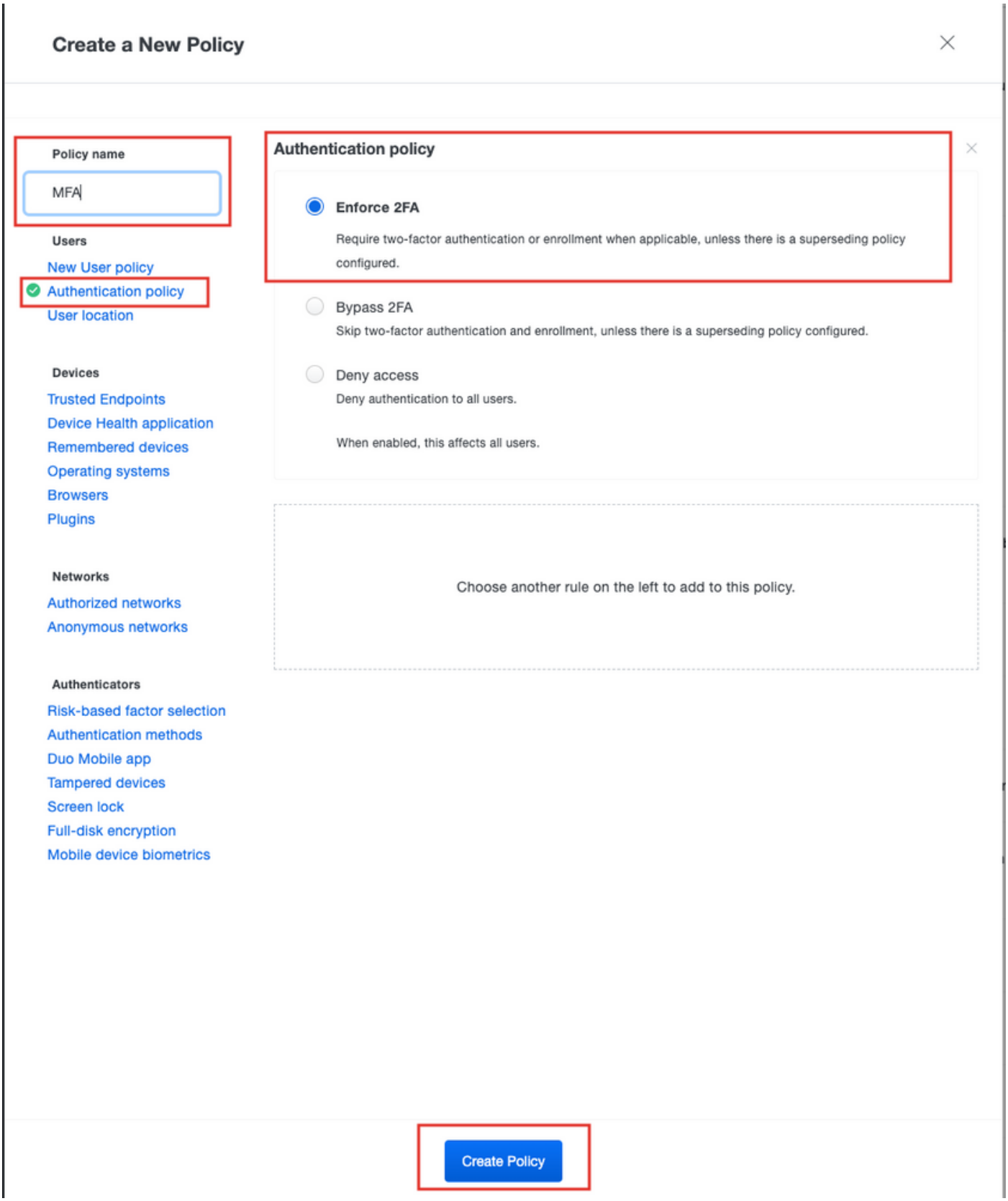



Esempio di creazione di un criterio di applicazione




Esempio di creazione di un criterio di applicazione

Passaggio 2. In Nome criterio, immettere il nome desiderato, selezionare "Criterio di autenticazione" in Utenti e selezionare "Imponi 2FA." Quindi salvare con "Crea criterio".




Esempio di creazione di un criterio di applicazione

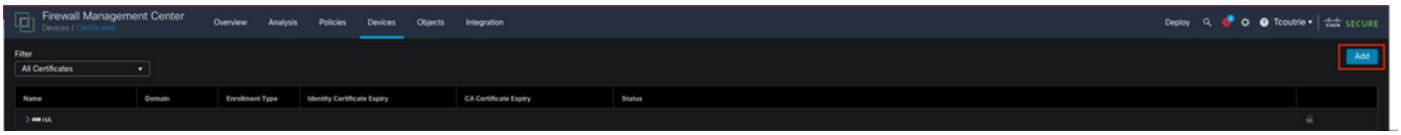
Passaggio 3. Applicare il criterio con "Applica criterio" nella finestra successiva. quindi scorrere fino alla fine della pagina e selezionare "Save" (Salva) per completare le configurazioni DUO

# Procedura di configurazione di FMC

## Distribuisci certificato di identità nell'FTD

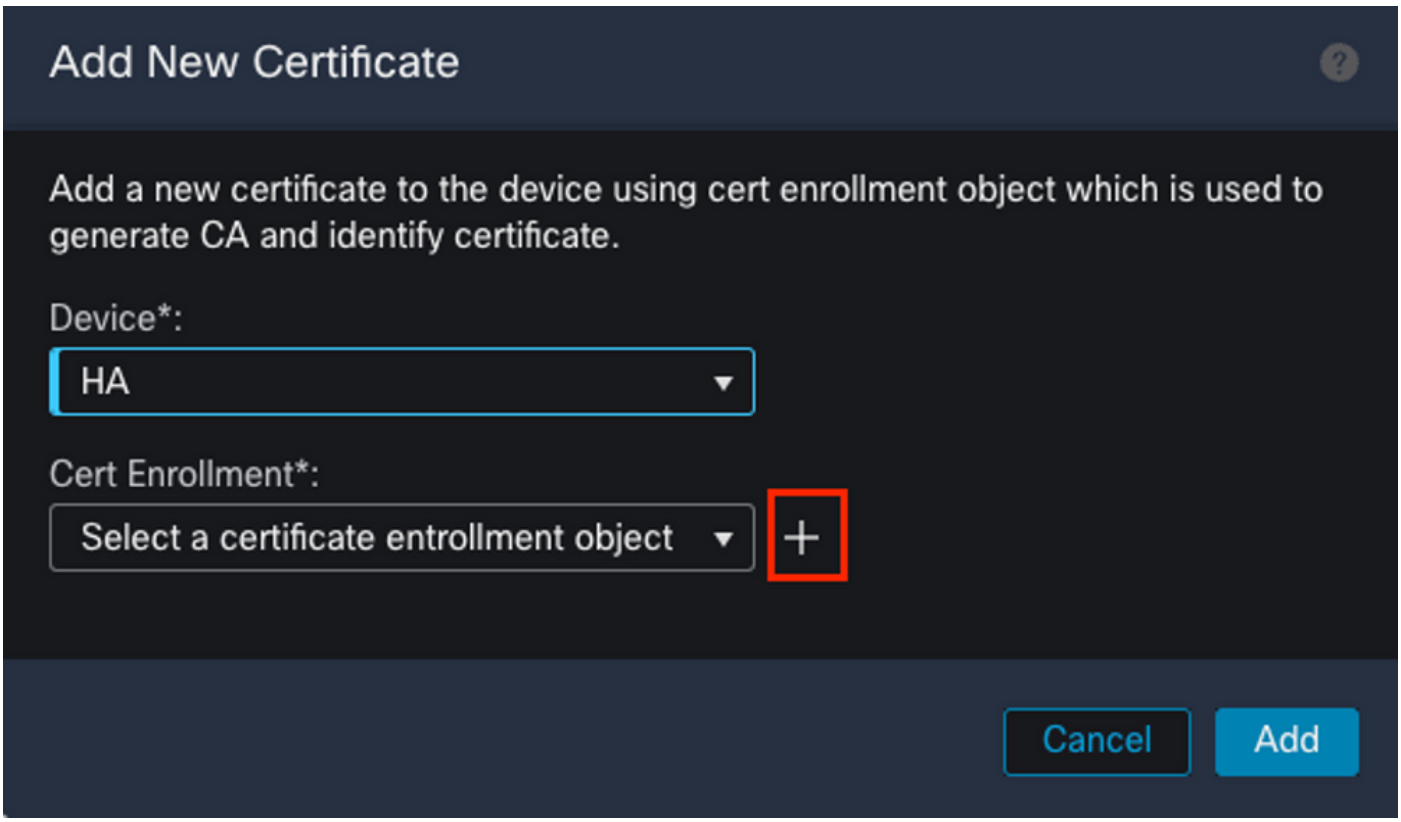
In questa sezione viene descritta la configurazione e la distribuzione del certificato di identità nell'FTD necessario per l'autenticazione del certificato. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

Passaggio 1. Passare a Dispositivi > Certificato e scegliere Aggiungi, come mostrato nell'immagine.



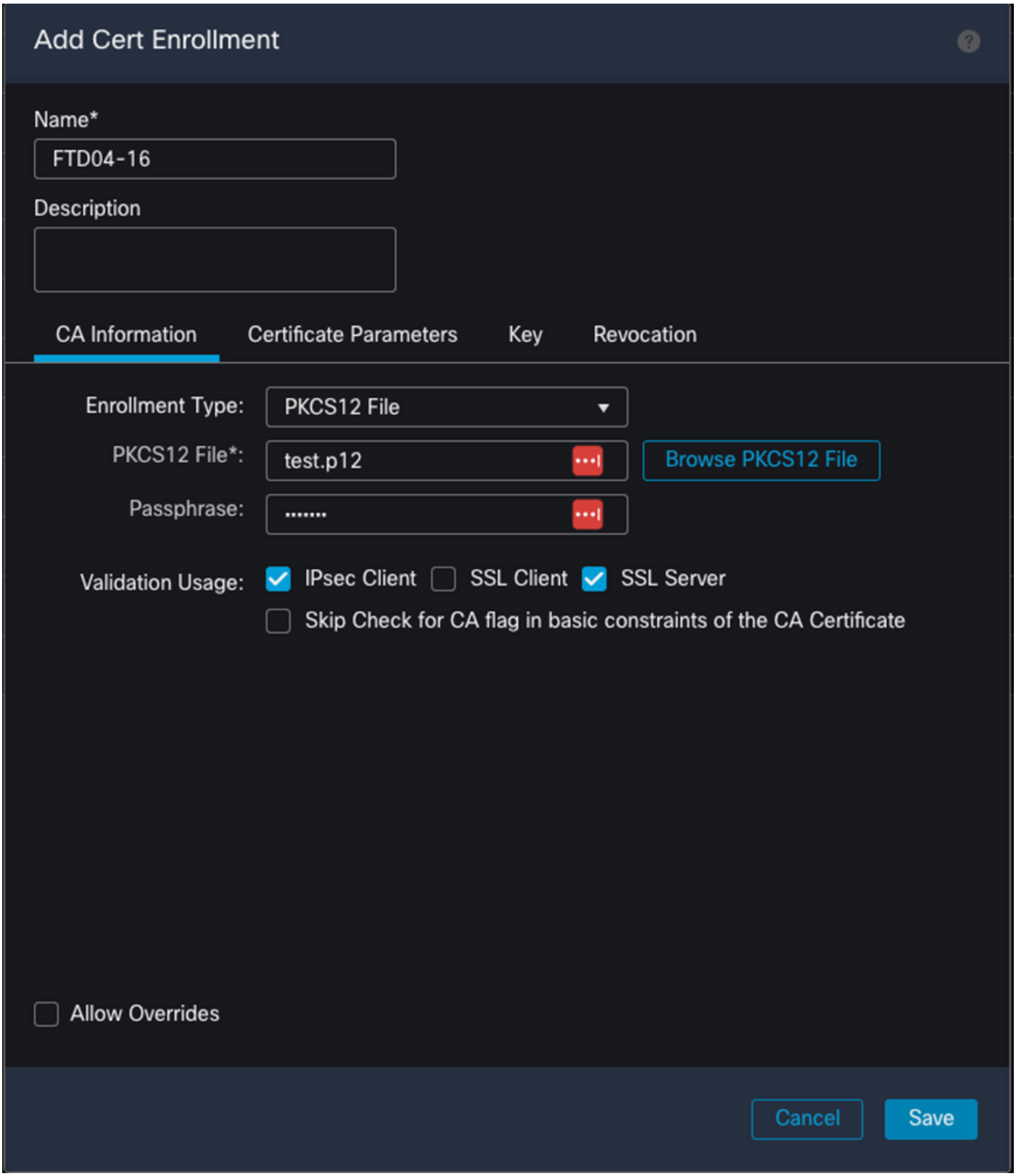

Schermata di dispositivi/certificati

Passaggio 2: Selezionare l'accessorio FTD dal menu a discesa dei dispositivi. Fare clic sull'icona + per aggiungere un nuovo metodo di registrazione dei certificati.




Schermata Aggiungi nuovo certificato

Passaggio 3: scegliere l'opzione che rappresenta il metodo preferito per ottenere i certificati nell'ambiente tramite il "Tipo di registrazione", come mostrato nell'immagine.




Schermata della nuova pagina di registrazione del certificato

Suggerimento: Le opzioni disponibili sono: Certificato autofirmato - Genera un nuovo certificato localmente, SCEP - Utilizza il protocollo SCEP (Simple Certificate Enrollment Protocol) per ottenere un certificato da una CA, Manual - Installa manualmente il certificato radice e identità, PKCS12 - Carica il bundle di certificati crittografati con radice,

identità e chiave privata.

## Distribuisci certificato IDP nell'FTD

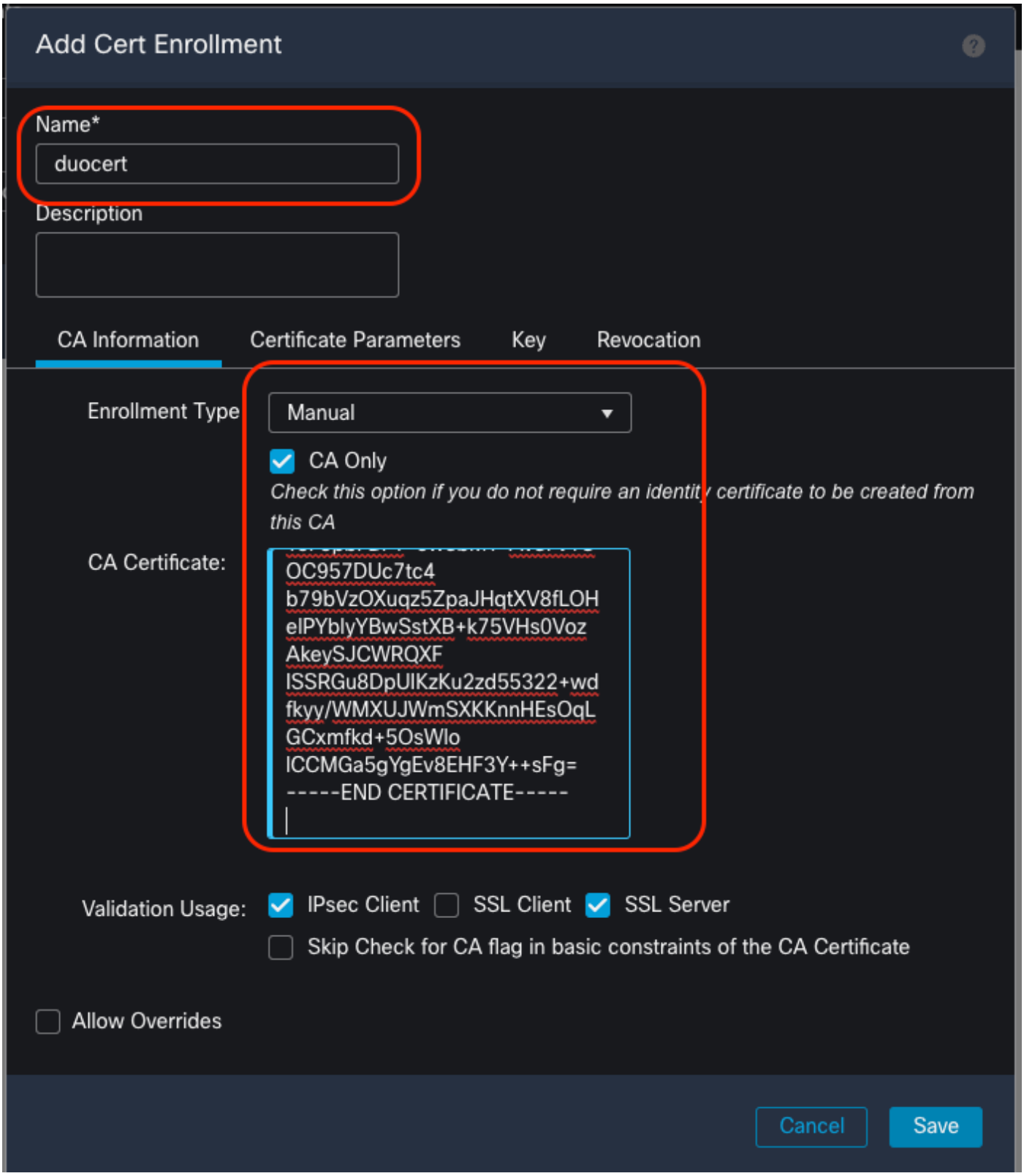
In questa sezione viene descritto come configurare e distribuire il certificato IDP nell'FTD. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

Passaggio 1: Passare a Dispositivi > Certificato e scegliere Aggiungi."

Passaggio 2: Selezionare l'accessorio FTD dal menu a discesa dei dispositivi. Fare clic sull'icona + per aggiungere un nuovo metodo di registrazione dei certificati.

Passaggio 3: Nella finestra Aggiungi registrazione certificato, immettere le informazioni richieste come mostrato nell'immagine, quindi "Salva" come mostrato nell'immagine.

- Nome: Nome dell'oggetto
- Tipo di iscrizione: Manuale
- Casella di controllo attivata: Solo CA
- Certificato CA: Formato Pem del certificato

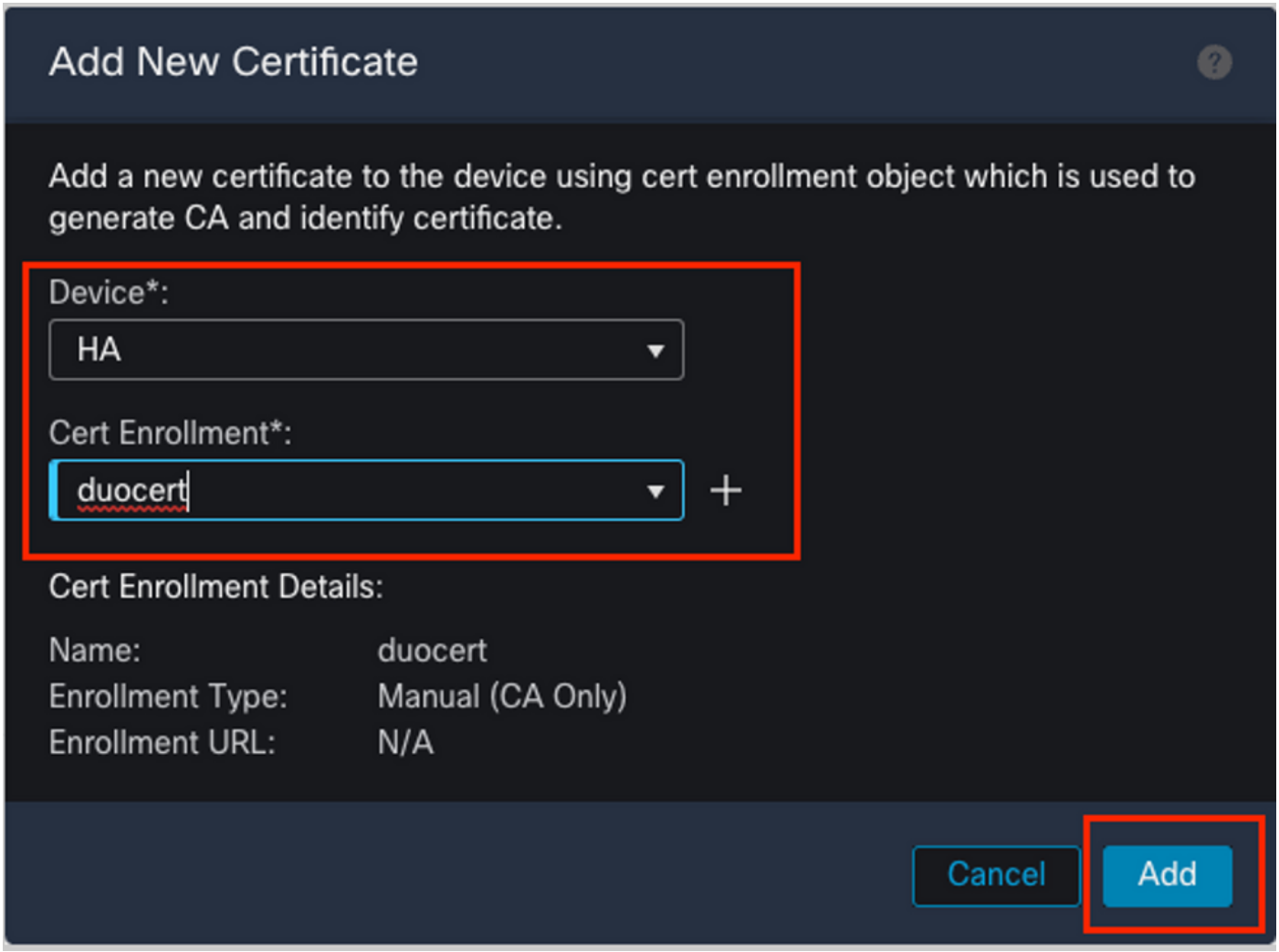



Esempio di creazione di un oggetto di registrazione certificato

⚠ Attenzione: Se necessario, è possibile utilizzare "Ignora il contrassegno CA nei vincoli di base del certificato CA". Utilizzare questa opzione con cautela.

Passaggio 4: Selezionare l'oggetto di registrazione certificato appena creato in "Registrazione

certificato*:", quindi selezionare "Aggiungi" come mostrato nell'immagine.



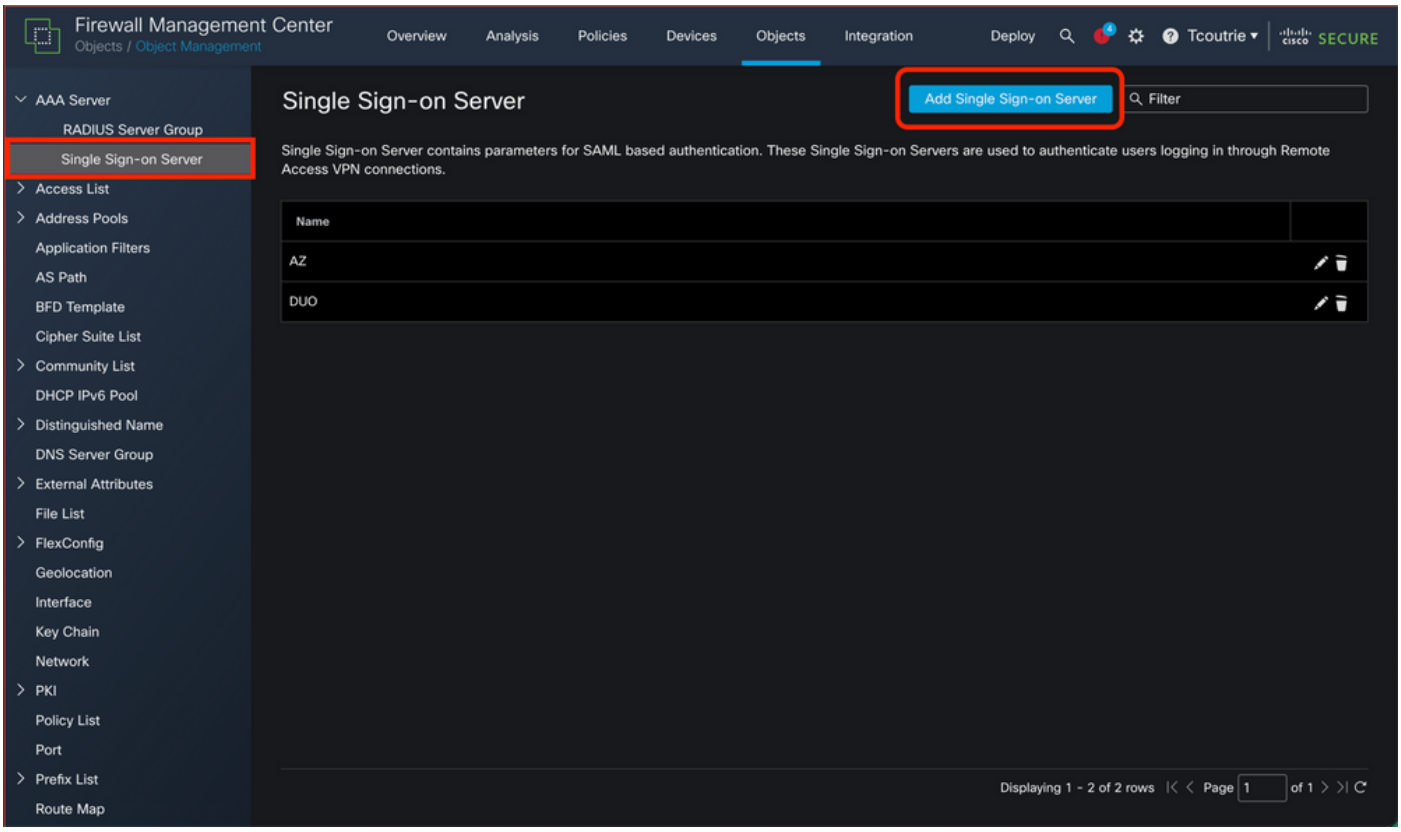

Schermata del dispositivo e dell'oggetto di registrazione del certificato aggiunto

Nota: Dopo l'aggiunta, il certificato viene distribuito immediatamente.

## Creazione dell'oggetto SAML SSO

In questa sezione vengono descritti i passaggi per configurare SAML SSO tramite FMC. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

Passaggio 1. Passare a Oggetti > Server AAA > Server Single Sign-on e selezionare "Aggiungi server Single Sign-on".

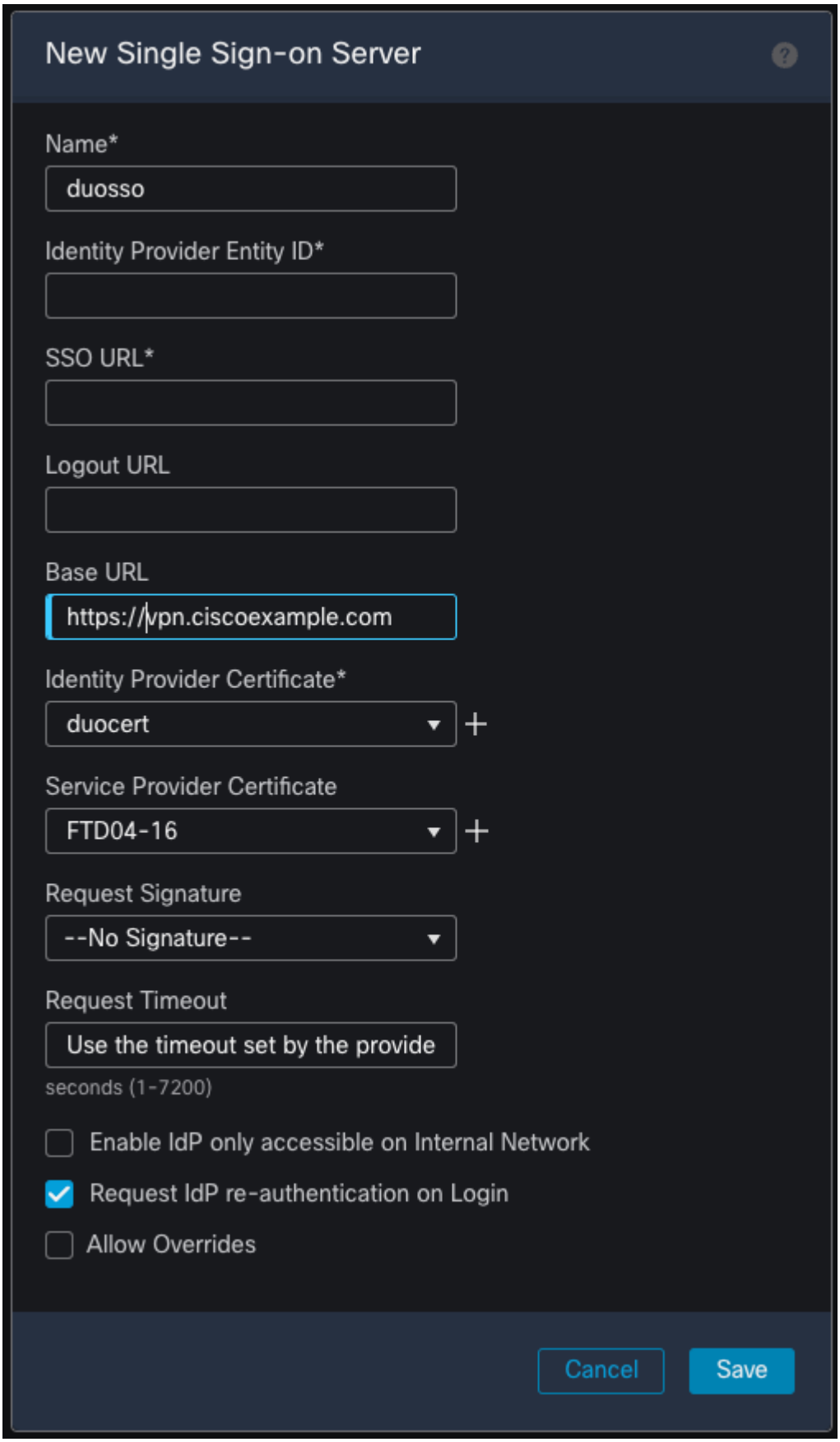



esempio di creazione di un nuovo oggetto SSO

Passaggio 2. Immettere le informazioni richieste da "Crea criteri di protezione applicazione"

". Per continuare, selezionare "Salva".

- Nome*: Nome dell'oggetto
- ID entità provider di identità*: ID entità dal passaggio 3
- URL SSO*: URL di accesso copiato dal passaggio 3
- URL di disconnessione: URL di disconnessione copiato dal passaggio 3
- URL di base: Utilizzare lo stesso FQDN di "Cisco Firepower Base URL" nel passaggio 5
- Certificato del provider di identità*: Certificato IDP distribuito
- Certificato provider di servizi: Certificato sull'interfaccia esterna dell'FTD




Esempio di nuovo oggetto SSO.

Nota: I collegamenti ID entità, URL SSO e URL di disconnessione sono stati omessi dallo

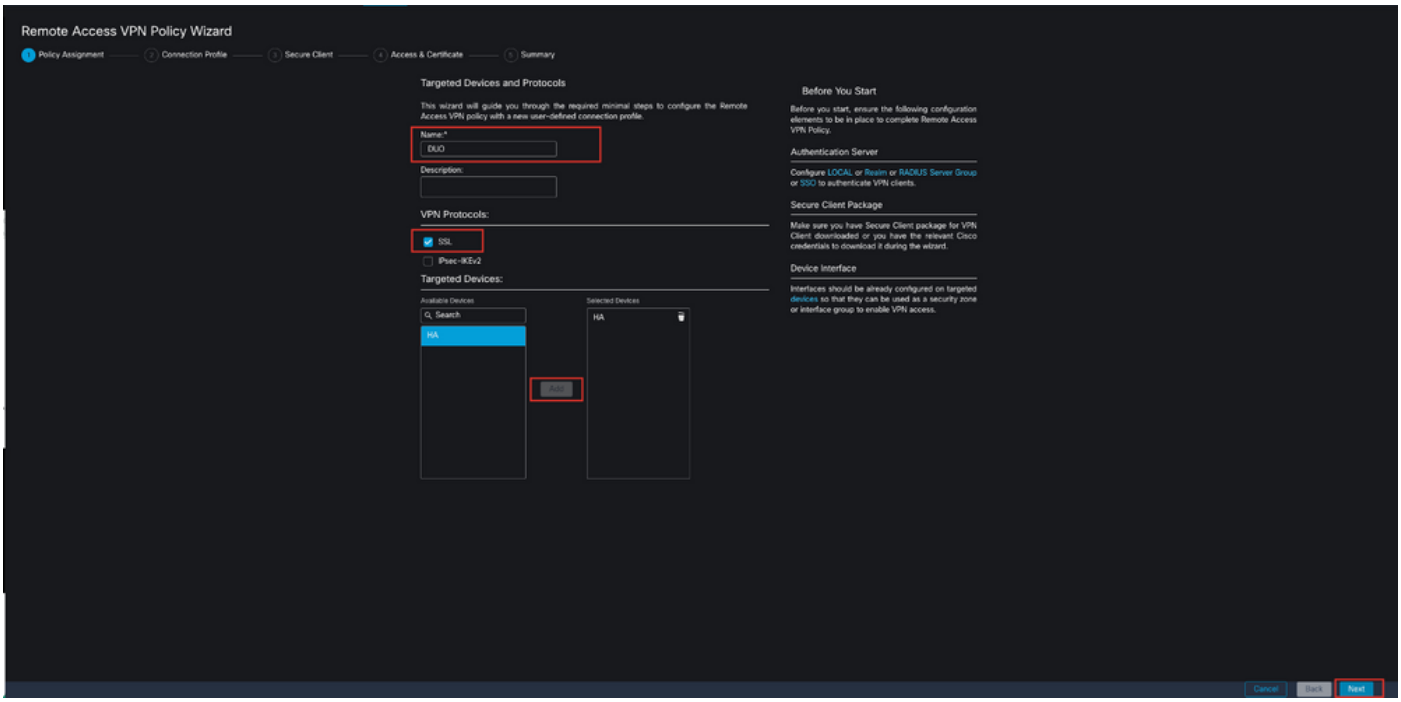
screenshot

## Crea configurazione RAVPN (Virtual Private Network) di accesso remoto

In questa sezione vengono descritti i passaggi per configurare RAVPN utilizzando la procedura guidata.

Passaggio 1. Passare a Dispositivi > Accesso remoto Selezionare "Aggiungi".

Passaggio 2. Nella procedura guidata, immettere il nome della nuova Creazione guidata criteri RAVPN, selezionare SSL in Protocolli VPN: Aggiungi dispositivi di destinazione, come mostrato nell'immagine. Selezionare "Avanti" al termine.




Passaggio 1 della procedura guidata RAVPN

Passaggio 2. Per il profilo di connessione, impostare le opzioni (mostrate qui): selezionare "Avanti" una volta completato.

- Nome profilo connessione:  Utilizzare il nome del gruppo di tunnel nel passaggio 5 di "Creazione di un criterio di protezione dell'applicazione".

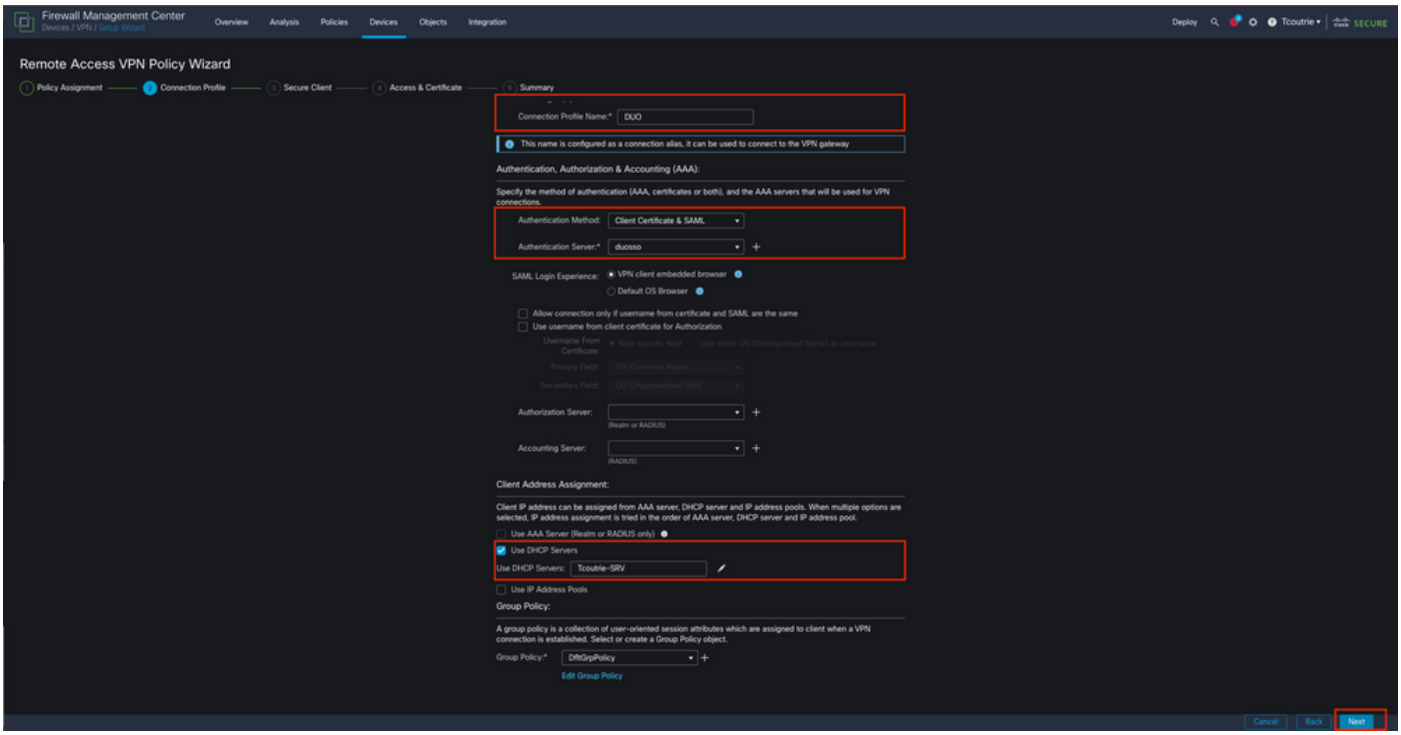
Autenticazione, autorizzazione e accounting (AAA):

- Metodo di autenticazione: Certificato client e SAML
- Server di autenticazione:* Selezionare l'oggetto SSO creato durante la creazione dell'oggetto SSO SAML.

Assegnazione indirizzo client:

- Usa server AAA (solo realm o RADIUS) - Radius o LDAP

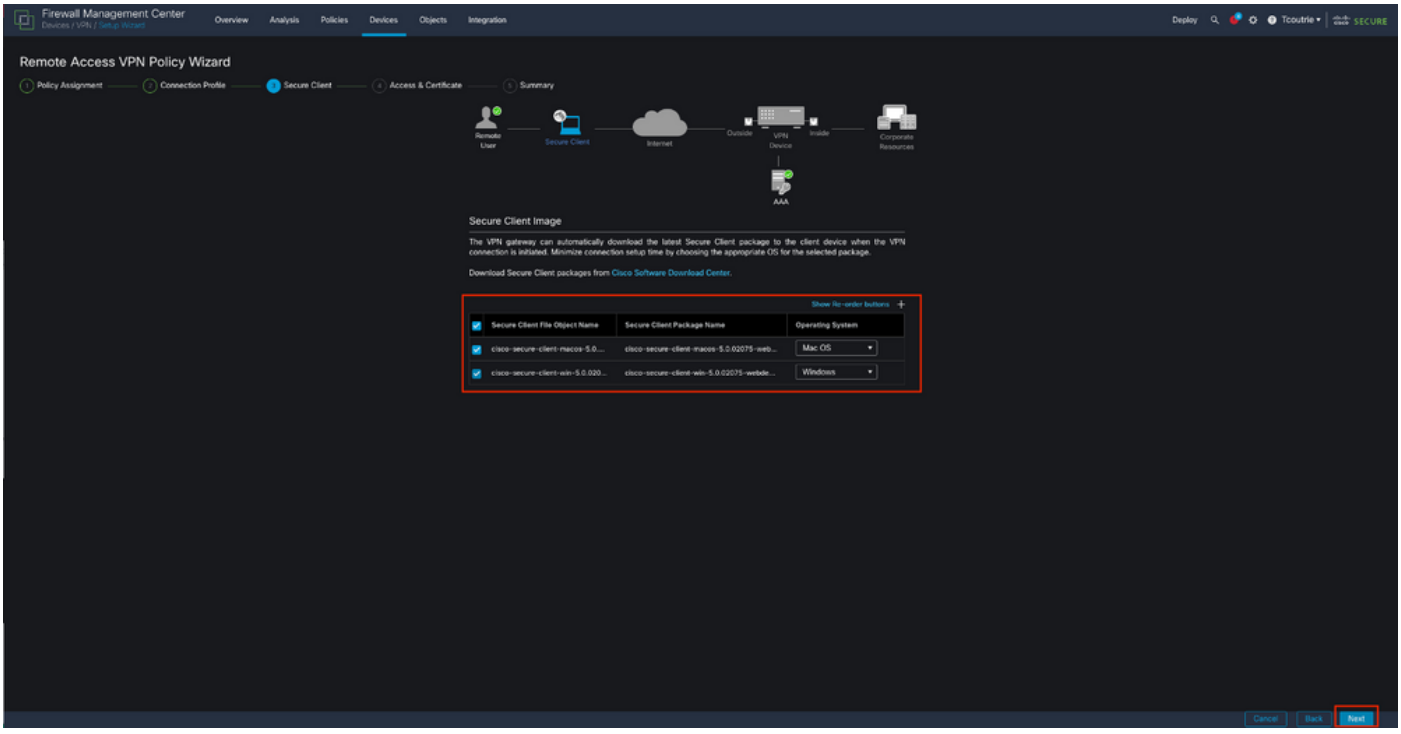
- Usa server DHCP - Server DHCP
- Utilizza pool di indirizzi IP - Pool locale nell'FTD




Passaggio 2 della procedura guidata RAVPN

Suggerimento: In questa esercitazione viene utilizzato un server DHCP.

Passaggio 3. Selezionare "+" per caricare un'immagine di distribuzione Web di Cisco Secure Client da distribuire. Quindi selezionare la casella di controllo dell'immagine CSC da distribuire. Come mostrato nell'immagine. Selezionare "Next" (Avanti) una volta completato.

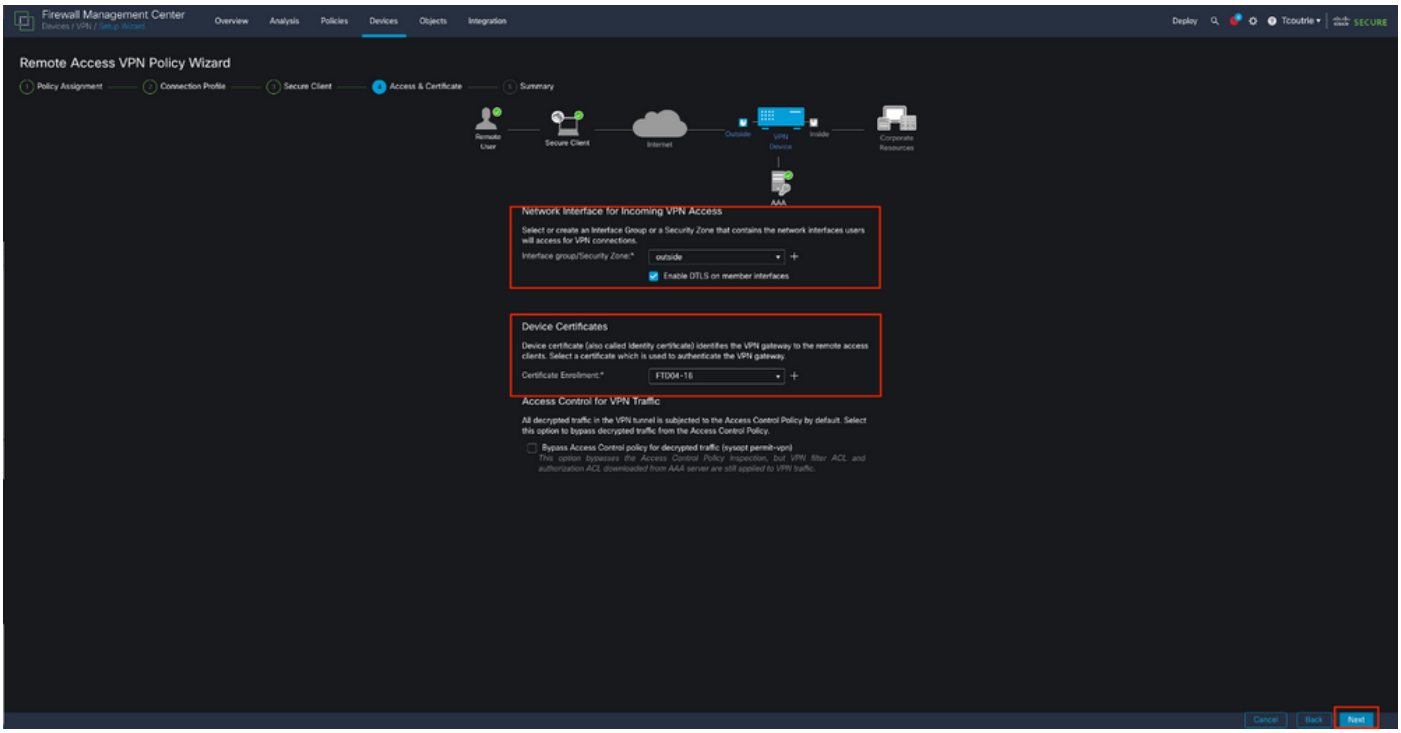


Passaggio 3 Creazione guidata RAVPN

Passaggio 4. Impostare questi oggetti (come mostrato nell'immagine): selezionare "Avanti" una volta completato.

Gruppo interfaccia/Area di sicurezza:*: Interfaccia esterna

"Registrazione certificato:*": Certificato di identità creato durante la sezione "Distribuisci certificato di identità all'FTD" di questa guida

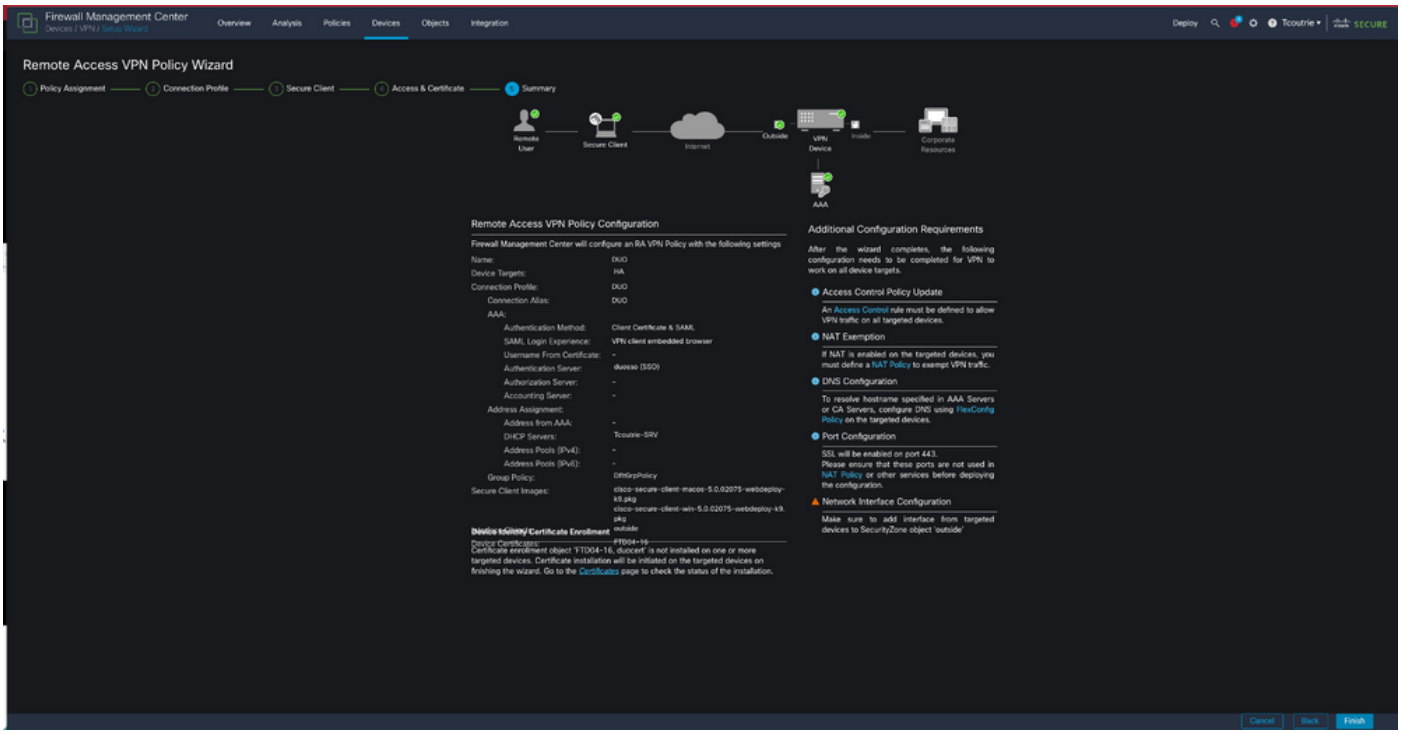



Passaggio 4 della procedura guidata RAVPN

Suggerimento: Se non è stato creato, aggiungere un nuovo oggetto di registrazione certificato selezionando "+".

Passaggio 6. Riepilogo

Verificare tutte le informazioni. Se tutto è corretto, continuare con "Fine".




Pagina di riepilogo

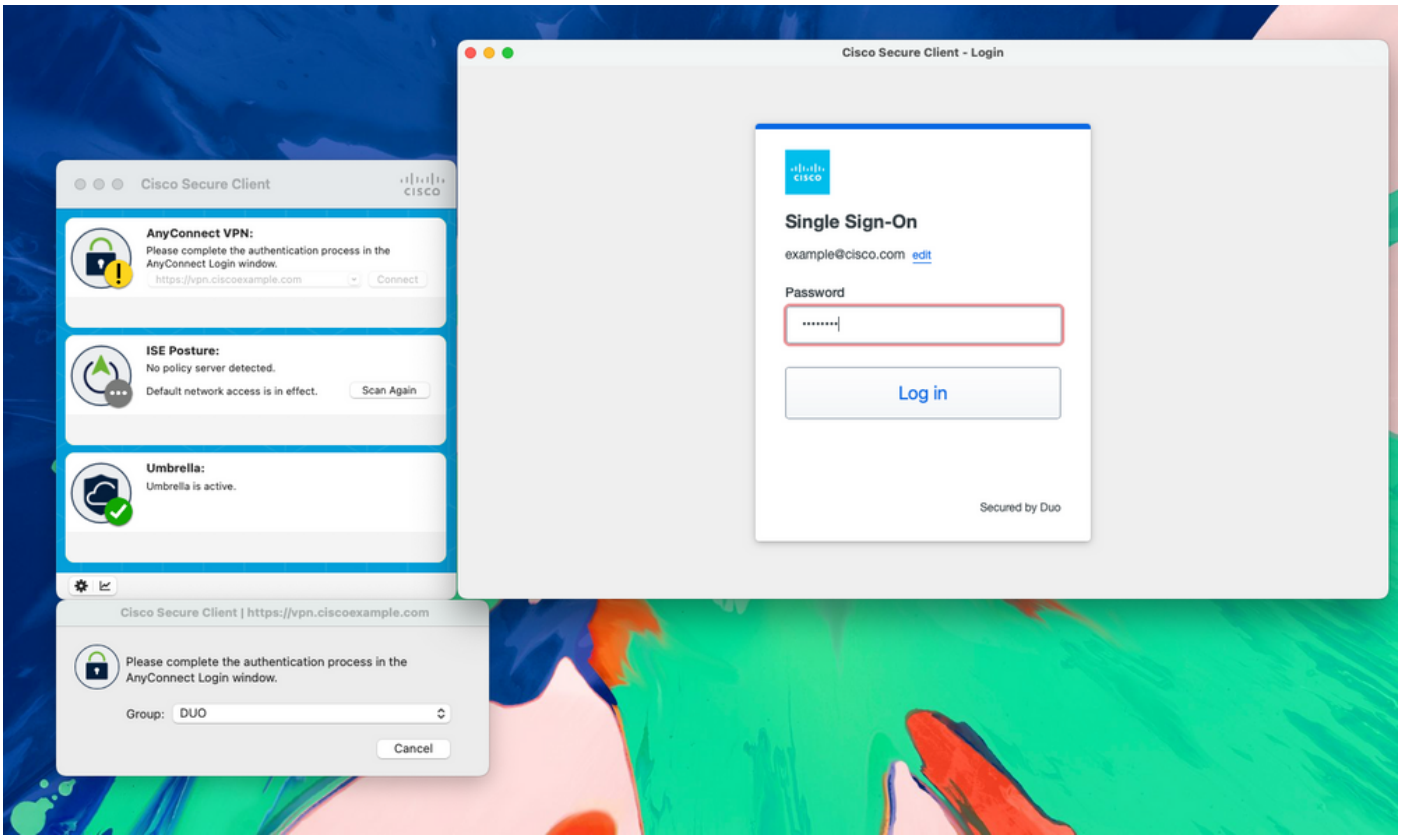
Passaggio 7. Distribuire le configurazioni appena aggiunte.

# Verifica

In questa sezione viene descritta la verifica di un tentativo di connessione riuscito.

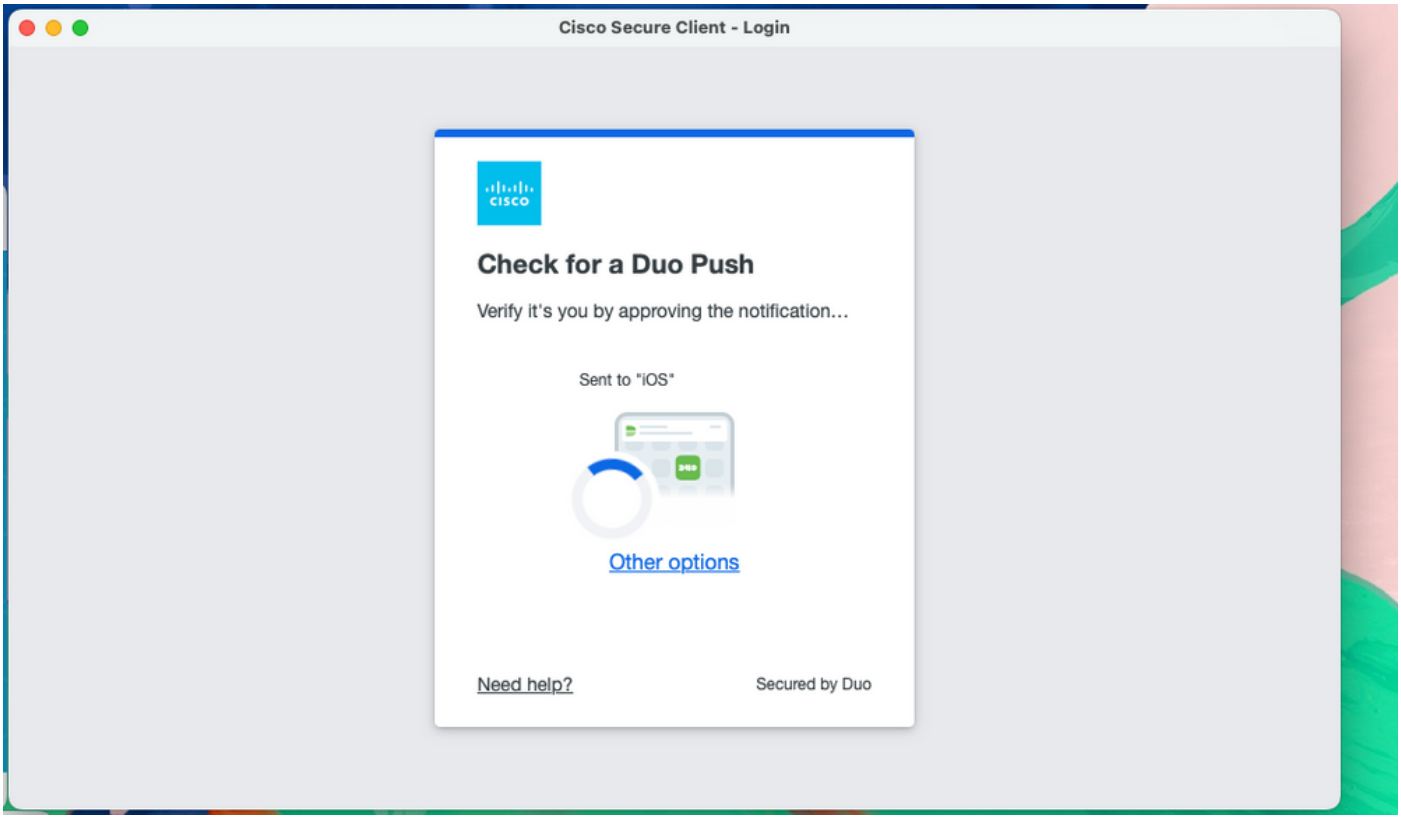
Aprire Cisco Secure Client, immettere il nome di dominio completo (FQDN) dell'FTD e connettersi.

Immettere le credenziali nella pagina SSO.



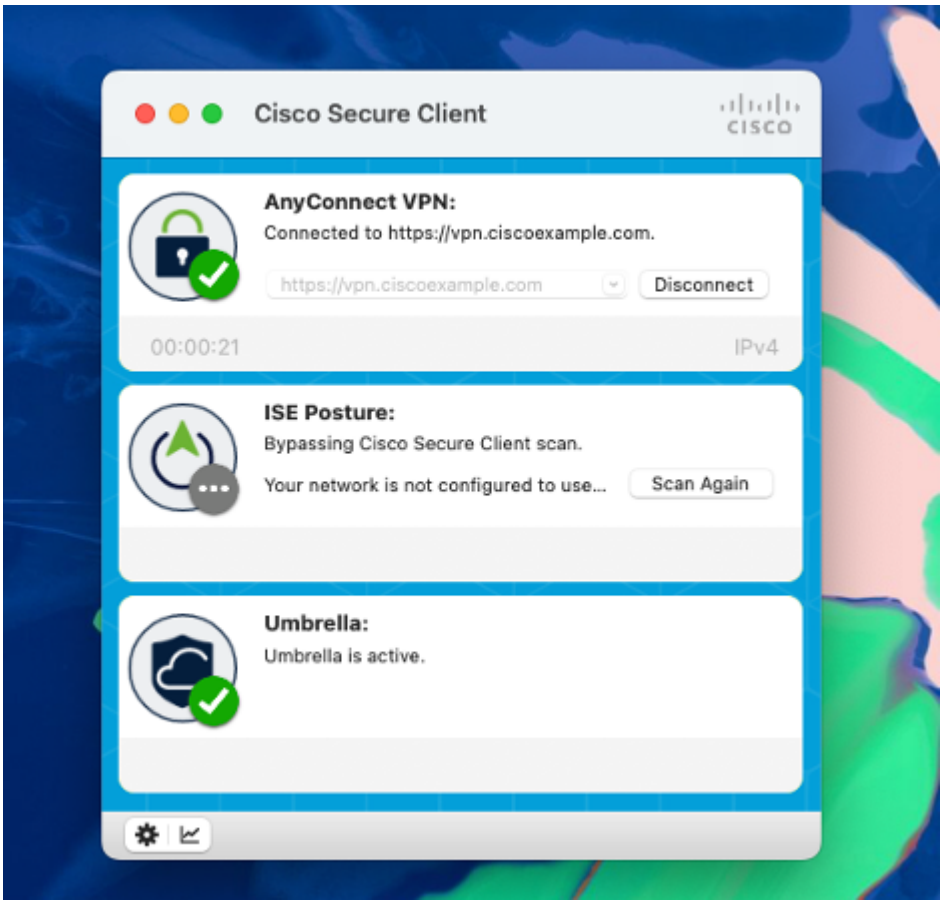

Pagina SSO tramite Cisco Secure Client

Accettare la pressione DUO sul dispositivo registrato.




Push DUO

Connessione riuscita.




Connesso a FTD

Verificare la connessione sull'FTD con il comando: show vpn-sessiondb detail anyconnect

```
tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     :                       Index        : 1916
Assigned IP  :                       Public IP    :
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx     : 390964                Bytes Rx     : 124114
Pkts Tx      : 1216                  Pkts Rx      : 1223
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy :                       Tunnel Group :
Login Time   : 23:54:41 UTC Tue Jul 18 2023
Duration     : 0h:11m:28s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : 0a7aa95d0077c00064b72641
Security Grp : none                  Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 1916.1
  Public IP    :
  Encryption   : none                  Hashing      : none
  TCP Src Port : 53859                 TCP Dst Port : 443
  Auth Mode    : Certificate and SAML
  Idle Time Out: 30 Minutes            Idle TO Left : 18 Minutes
  Client OS    : mac-intel
```

Alcune informazioni sono state omesse dall'esempio di output

# Risoluzione dei problemi

Si tratta di possibili problemi che sorgeranno dopo l'implementazione.

Numero 1: Autenticazione del certificato non riuscita.

Assicurarsi che il certificato radice sia installato sull'FTD;

utilizzare i seguenti debug:

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

numero 2: Errori SAML

I seguenti debug possono essere abilitati per la risoluzione dei problemi:

debug aaa shim 128

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

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).