Configurazione dell'autenticazione AD per i client AnyConnect

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
  - Premesse
- Configurazione
  - Esempio di rete e scenario
  - Configurazioni di Active Directory
    - Determinare il DN di base e il DN gruppo LDAP
    - Crea un account FTD
    - Creare gruppi AD e aggiungere utenti ai gruppi AD (facoltativo)
    - Copia radice certificato SSL LDAPS (richiesto solo per LDAPS o STARTTLS)
  - Configurazioni FMC
    - Verifica delle licenze
    - Imposta realm
    - Configurazione di AnyConnect per l'autenticazione AD
    - Abilita criteri di identità e configura criteri di sicurezza per l'identità utente
    - Configura esenzione NAT
    - Implementazione
- Verifica
  - Configurazione finale
    - Configurazione AAA
    - Configurazione AnyConnect
  - Connettersi con AnyConnect e verificare le regole dei criteri di controllo di accesso
  - Verifica con gli eventi di connessione FMC
- Risoluzione dei problemi
  - Debug
    - Debug LDAP in corso
    - Impossibile stabilire una connessione con il server LDAP
    - Nome distinto e/o password di accesso binding non corretti
    - Server LDAP: impossibile trovare il nome utente
    - Password non corretta per il nome utente
  - Test AAA
  - Acquisizioni pacchetti
  - Registri del Visualizzatore eventi di Windows Server

Introduzione

In questo documento viene descritto come configurare l'autenticazione Active Directory (AD) per i

client AnyConnect che si connettono a Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di RMA Virtual Private Network (VPN) su Firepower Manage Center (FMC)
- Configurazione del server Lightweight Directory Access Protocol (LDAP) in FMC
- Active Directory (AD)
- Nome dominio completo (FQDN)
- Intersight Infrastructure Services (IIS)
- Protocollo RDP (Remote Desktop Protocol)

Componenti usati

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

- Server Microsoft 2016
- FMCv versione 6.5.0
- FTDv in esecuzione 6.5.0

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 descritto come configurare l'autenticazione Active Directory (AD) per i client AnyConnect che si connettono a Firepower Threat Defense (FTD), gestito da Firepower Management Center (FMC).

L'identità dell'utente viene usata nei criteri di accesso per limitare gli utenti AnyConnect a specifici indirizzi IP e porte.

Configurazione

Esempio di rete e scenario

Il server Windows è preconfigurato con IIS e RDP per verificare l'identità dell'utente. In questa guida alla configurazione vengono creati tre account utente e due gruppi.

Account utente:

- Amministratore FTD: viene utilizzato come account di directory per consentire l'associazione di FTD al server Active Directory.
- Amministratore IT: un account di amministratore di test utilizzato per dimostrare l'identità dell'utente.
- Utente test: un account utente di test utilizzato per dimostrare l'identità dell'utente.

Gruppi:

- AnyConnect Admins: gruppo di test aggiunto dall'amministratore IT per dimostrare l'identità dell'utente. Questo gruppo dispone solo dell'accesso RDP al server Windows.
- Utenti AnyConnect: gruppo di test aggiunto dall'utente di test per dimostrare l'identità dell'utente. Questo gruppo dispone solo dell'accesso HTTP al server Windows.

Configurazioni di Active Directory

Per configurare correttamente l'autenticazione AD e l'identità utente su FTD, sono necessari alcuni valori.

Tutti questi dettagli devono essere creati o raccolti sul server Microsoft prima di poter eseguire la configurazione su FMC. I valori principali sono:

- Nome dominio:

Nome di dominio del server. In questa guida alla configurazione, example.com è il nome del dominio.

- Indirizzo IP/FQDN server:

L'indirizzo IP o il nome di dominio completo (FQDN) utilizzato per raggiungere il server Microsoft. Se si utilizza un FQDN, è necessario configurare un server DNS in FMC e FTD per risolvere l'FQDN.

In questa guida alla configurazione, questo valore è win2016.example.com (che si risolve in 192.168.1.1).

- Porta server:

La porta utilizzata dal servizio LDAP. Per impostazione predefinita, LDAP e STARTTLS utilizzano la porta TCP 389 per LDAP, mentre LDAP over SSL (LDAPS) utilizza la porta TCP 636.

- CA radice:

Se si utilizza LDAPS o STARTTLS, è necessaria la CA radice utilizzata per firmare il certificato SSL utilizzato da LDAPS.

- Nome utente e password directory:

Account utilizzato da FMC e FTD per il binding al server LDAP e per l'autenticazione degli utenti e la ricerca di utenti e gruppi.

A questo scopo viene creato un account denominato FTD Admin.

- Nome distinto (DN) di base e gruppo:

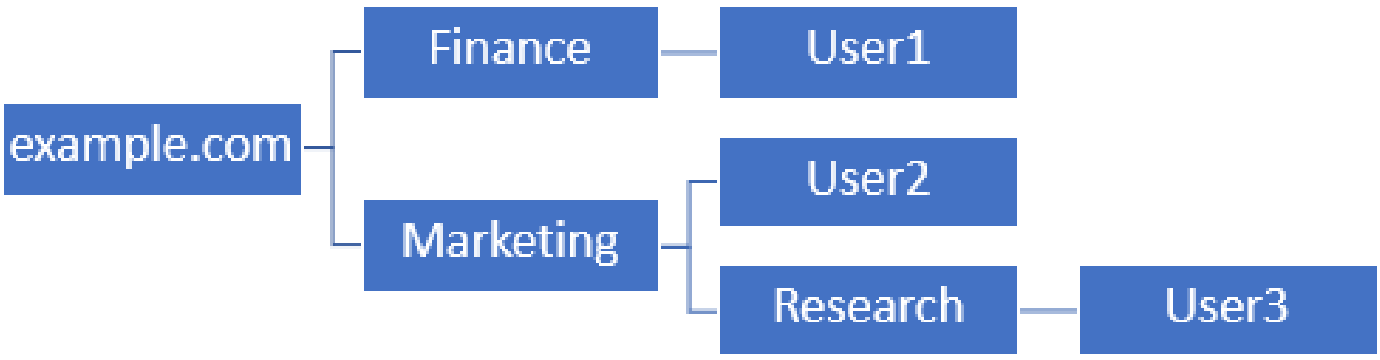
Il DN di base è il punto di partenza di FMC e il FTD indica ad Active Directory di iniziare la ricerca e l'autenticazione degli utenti.

Analogamente, il DN gruppo è il punto di partenza in cui FMC indica ad Active Directory dove iniziare la ricerca dei gruppi per l'identità dell'utente.

In questa guida alla configurazione, il dominio radice example.com viene utilizzato come DN di base e DN gruppo.

Tuttavia, per un ambiente di produzione, è preferibile utilizzare un DN di base e un DN di gruppo ulteriormente all'interno della gerarchia LDAP.

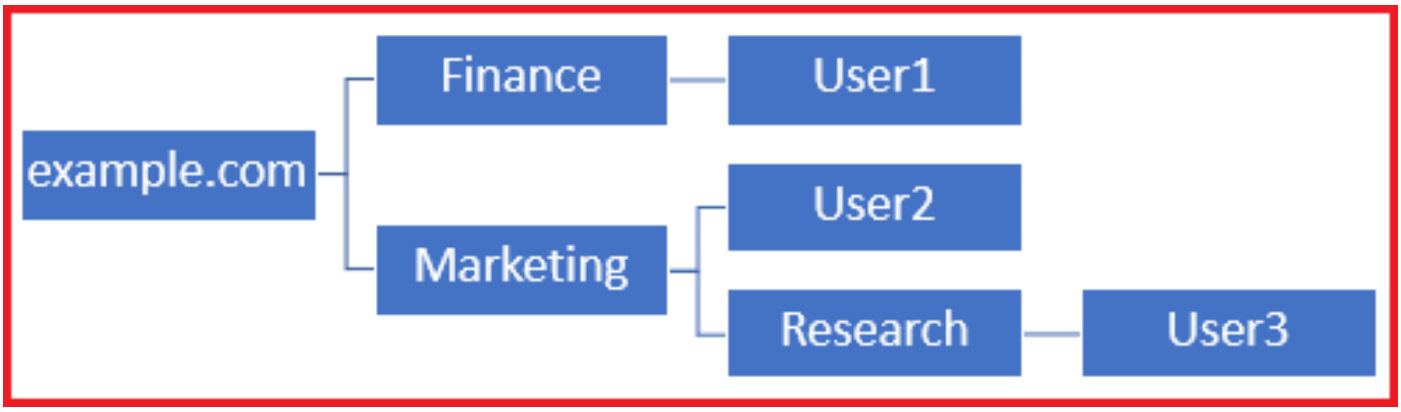
Ad esempio, la seguente gerarchia LDAP:



Se un amministratore desidera che gli utenti all'interno dell'unità organizzativa Marketing siano in grado di autenticare il DN di base, è possibile impostare il DN radice (example.com).

Tuttavia, ciò consente anche all'utente 1 dell'unità organizzativa Finanza di eseguire il login poiché la ricerca dell'utente inizia dalla radice e si conclude in Finanza, Marketing e Ricerca.

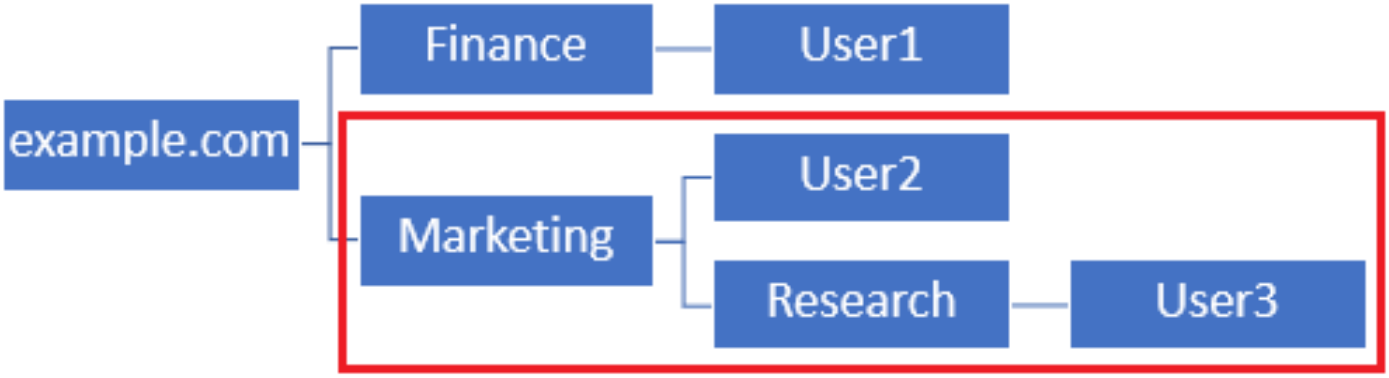
DN di base impostato su example.com



Per limitare l'accesso all'unico utente dell'unità organizzativa Marketing e di livello inferiore, l'amministratore può invece impostare il DN di base su Marketing.

Ora solo l'utente 2 e l'utente 3 sono in grado di eseguire l'autenticazione perché la ricerca ha inizio dal sito Marketing.

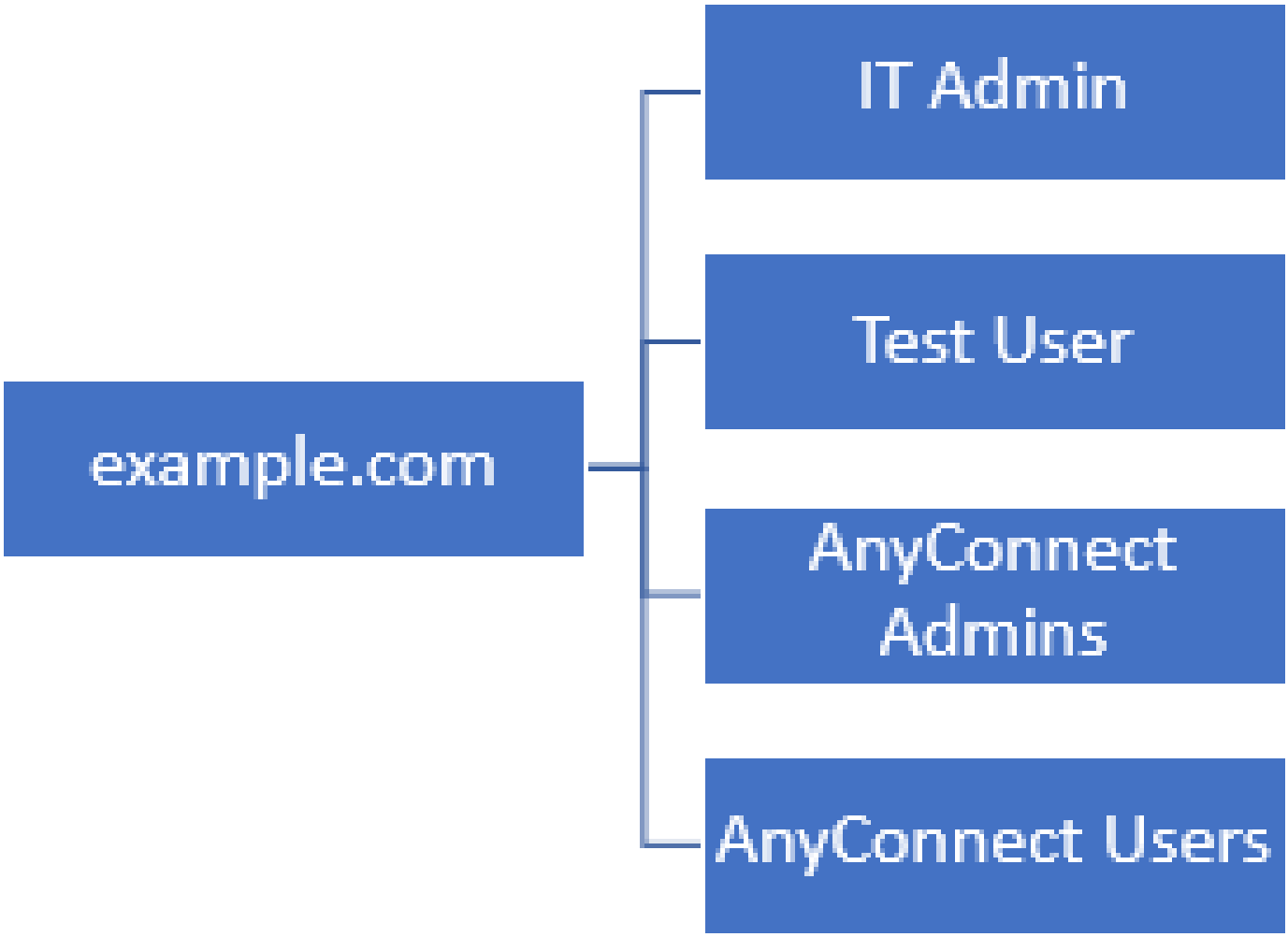
DN di base impostato su Marketing



Si noti che per un controllo più granulare all'interno dell'FTD per il quale gli utenti possono connettersi o assegnare agli utenti autorizzazioni diverse in base ai loro attributi AD, è necessario configurare una mappa di autorizzazione LDAP.

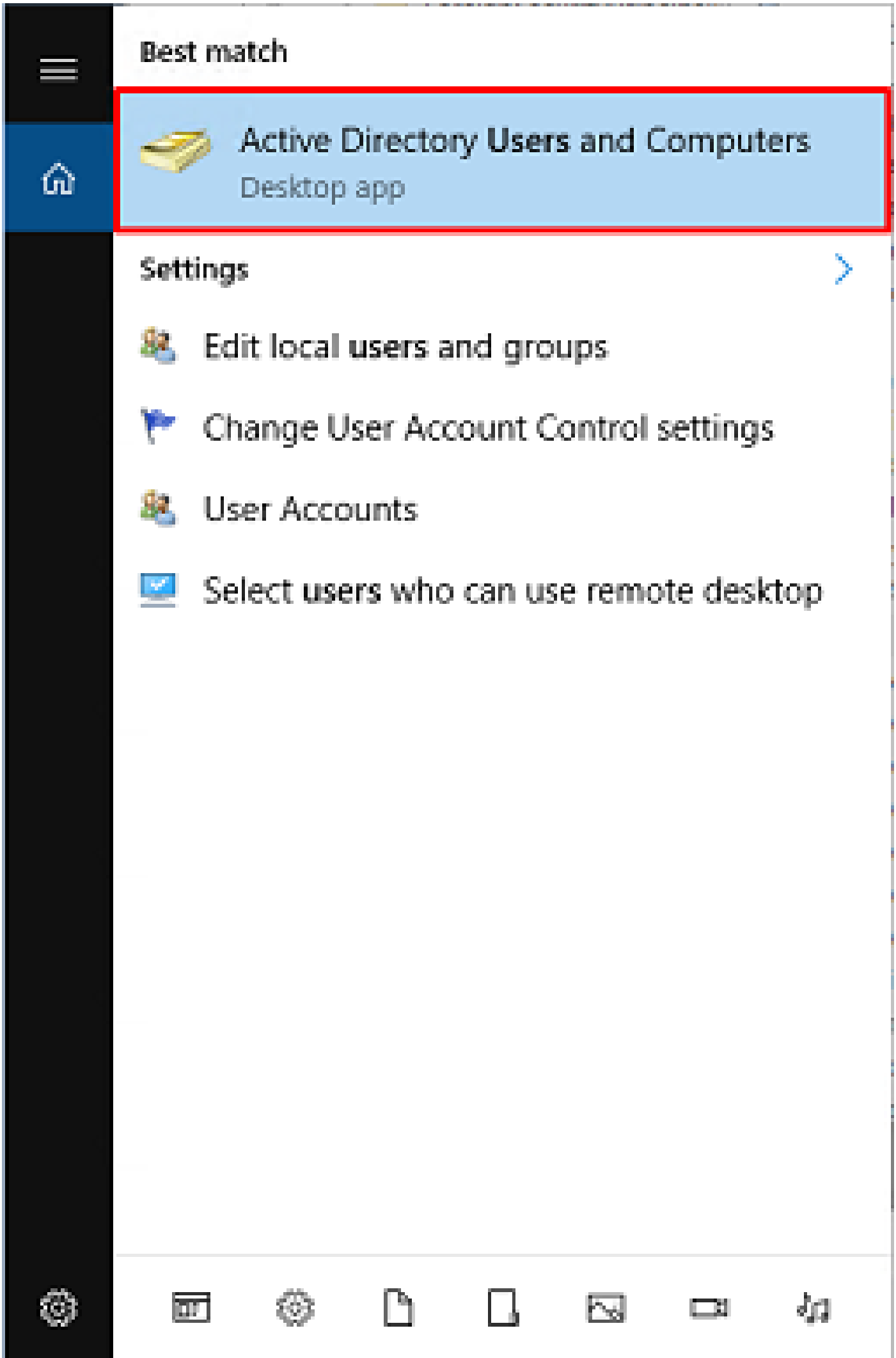
Per ulteriori informazioni, consultare il documento sulla configurazione del mapping LDAP di AnyConnect su Firepower Threat Defense (FTD).

Questa gerarchia LDAP semplificata viene utilizzata in questa guida alla configurazione e il DN per la radice example.com viene utilizzato sia per il DN di base che per il DN di gruppo.



Determinare il DN di base e il DN gruppo LDAP

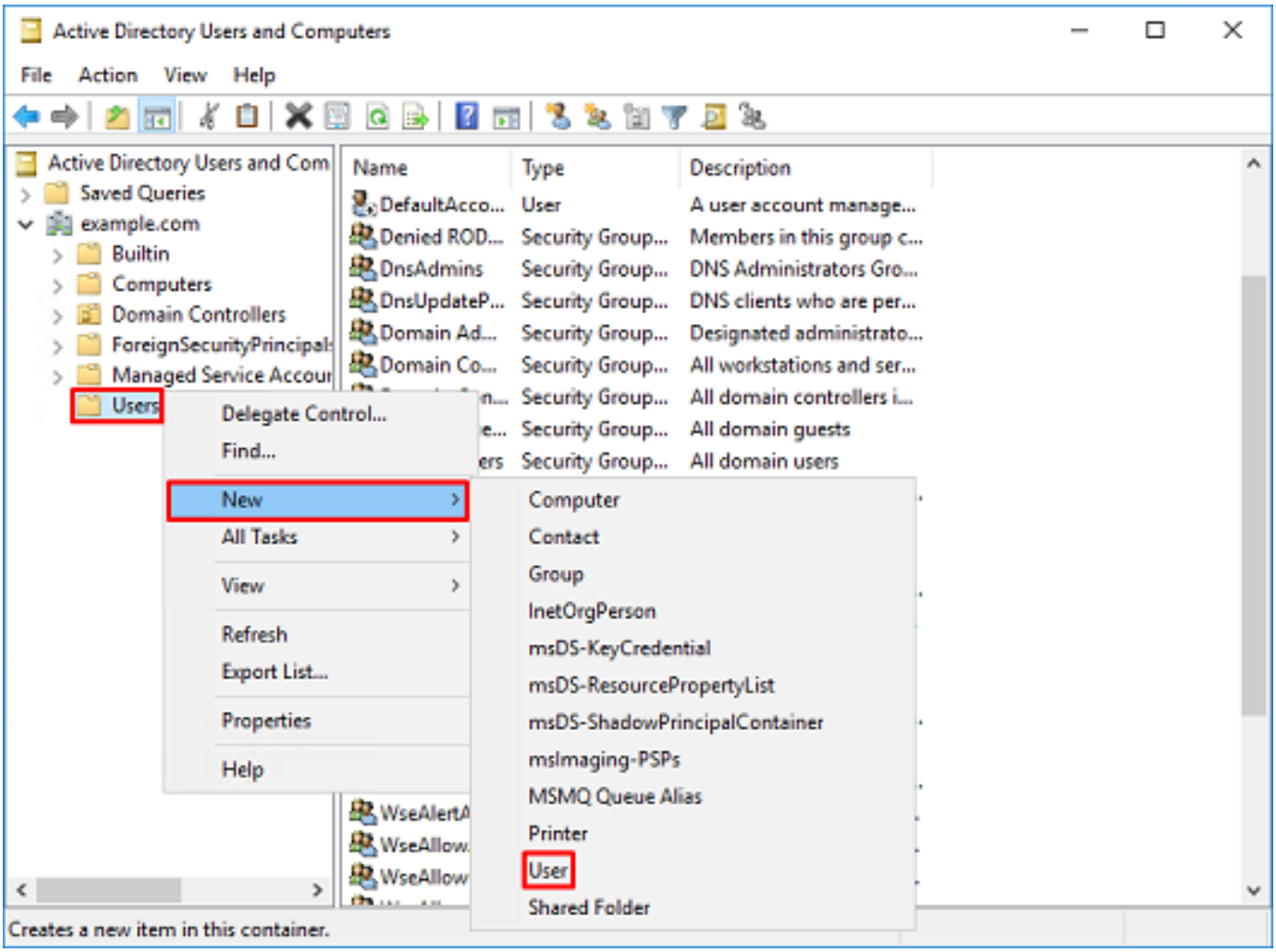
1. Aprire Utenti e computer di Active Directory.


Best match
Active Directory Users and Computers
Desktop app
Settings
Edit local users and groups
Change User Account Control settings
User Accounts
Select users who can use remote desktop

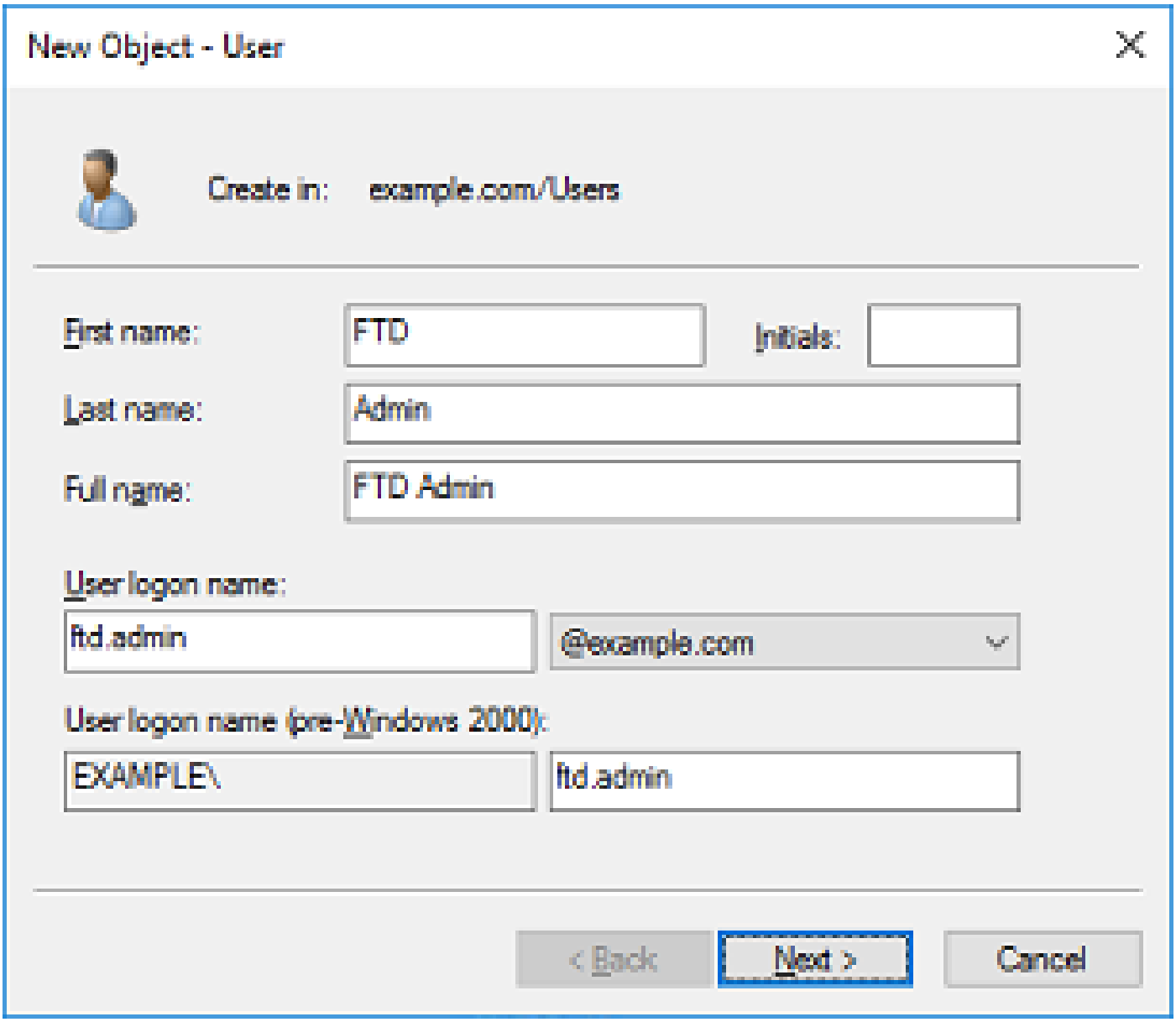
, fare clic con il pulsante destro del mouse sul contenitore/organizzazione a cui viene aggiunto l'account FTD.

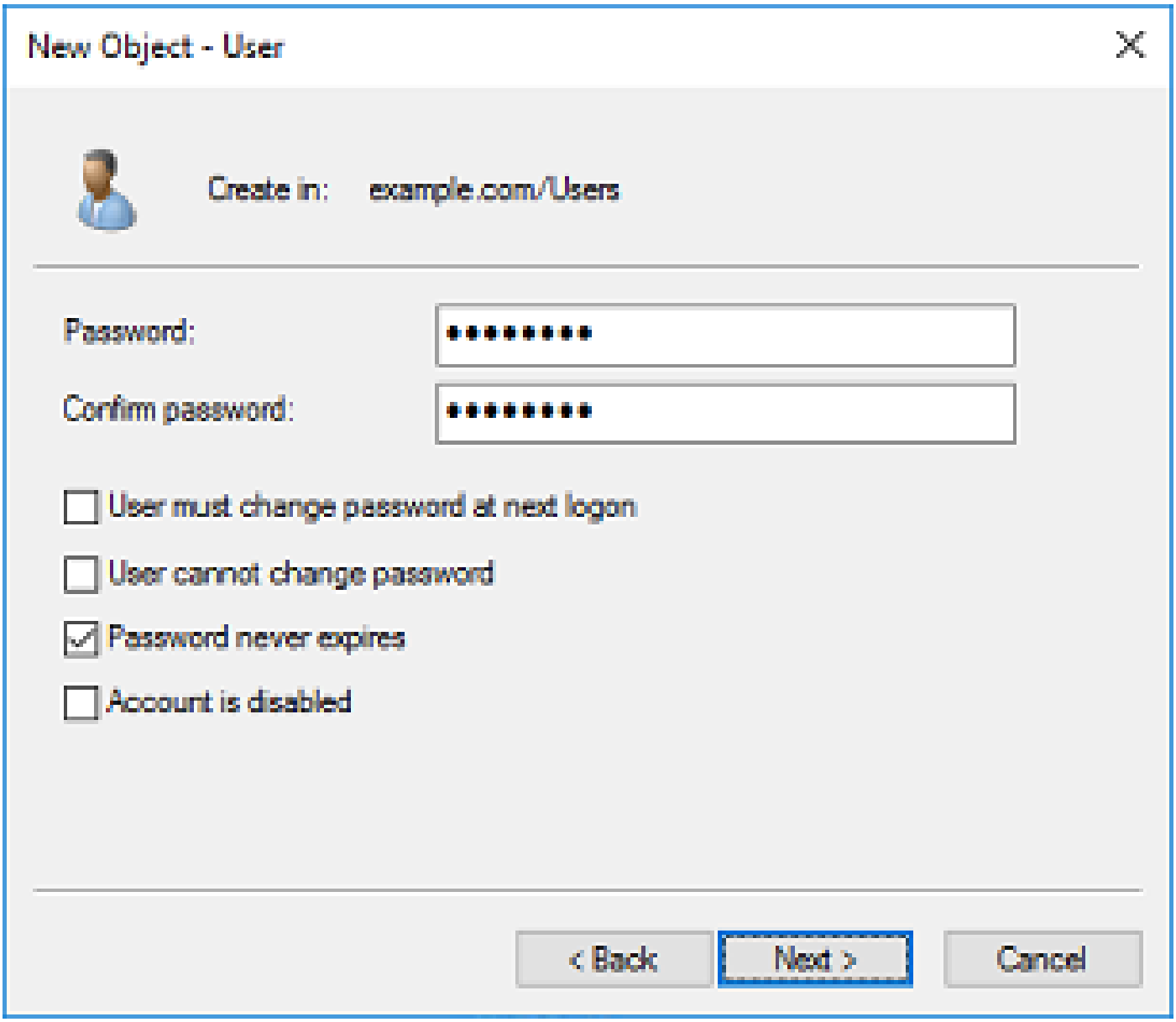
In questa configurazione, l'account FTD viene aggiunto nel contenitore Users sotto il nome utente ftd.admin@example.com.

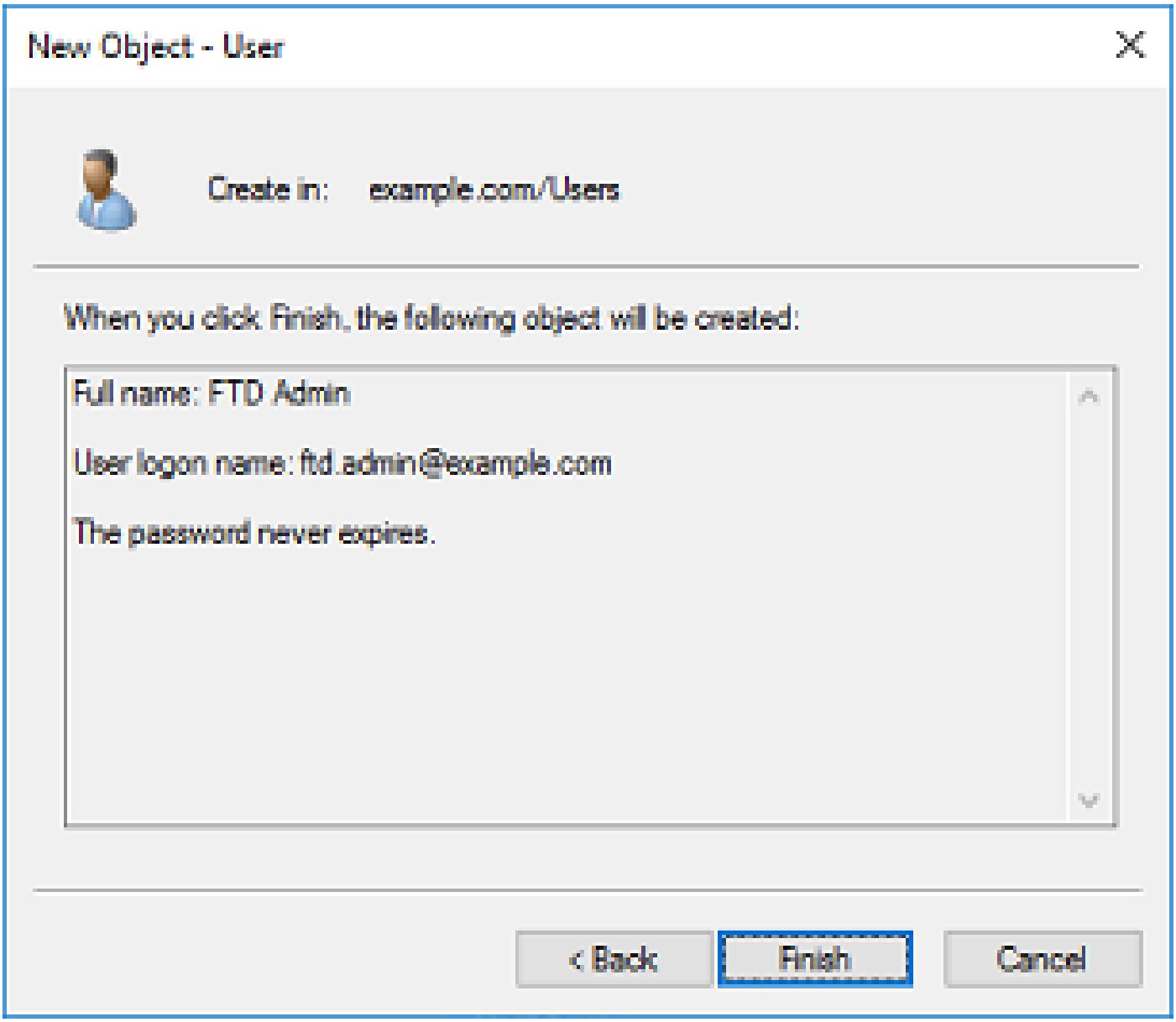
Fare clic con il pulsante destro del mouse su Users, quindi selezionare New > User (Nuovo > Utente).



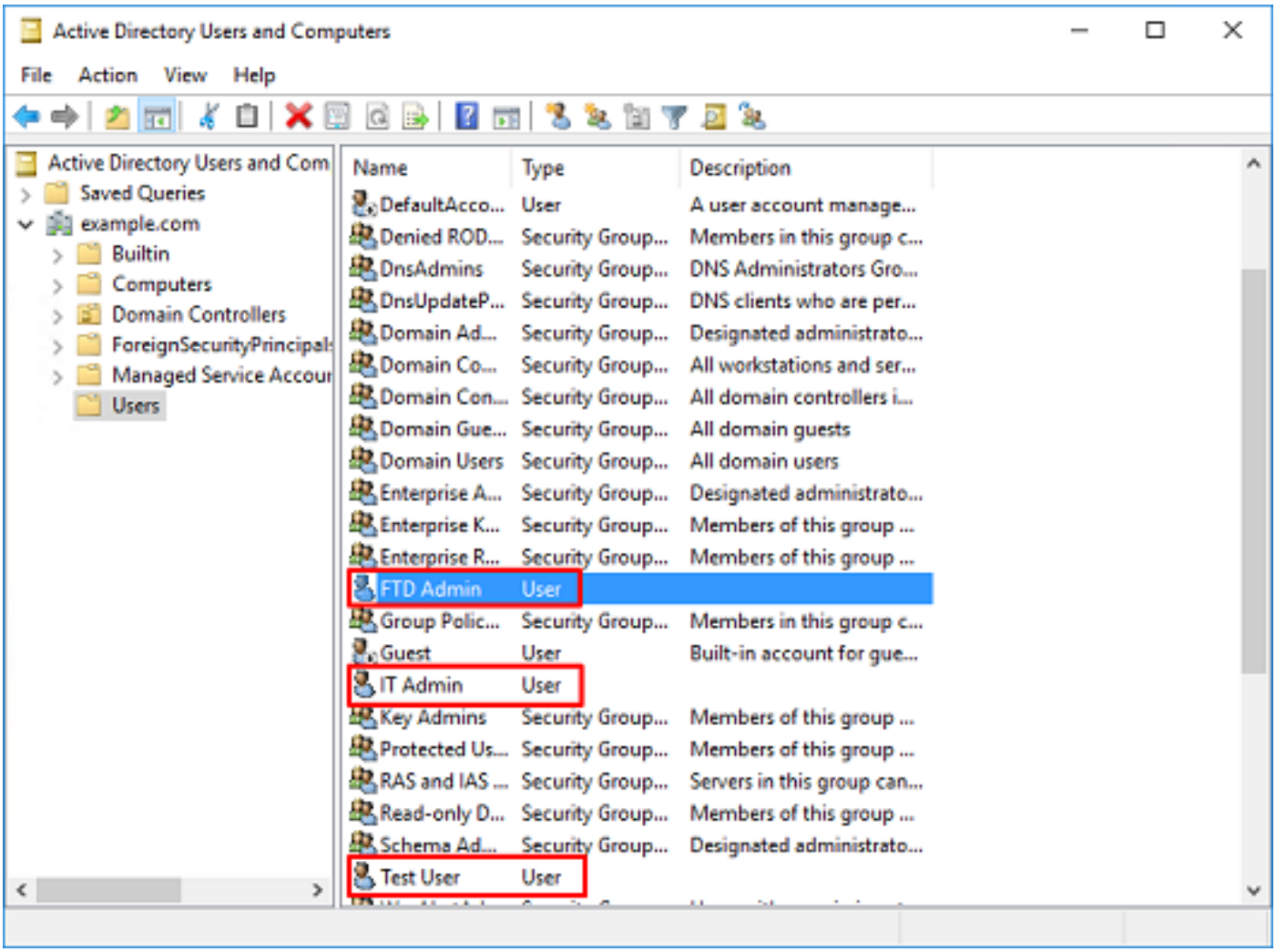
2. Eseguire la Creazione guidata nuovo oggetto - utente.


New Object - User
Create in: example.com/Users
First name:
FTD
Initials:
Last name:
Admin
Full name:
FTD Admin
User logon name:
ftd.admin
@example.com
User logon name (pre-Windows 2000):
EXAMPLE\
ftd.admin
< Back
Next >
Cancel


New Object - User
Create in: example.com/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel



3. Verificare che il conto FTD sia stato creato. Vengono creati due account aggiuntivi: IT Admin e Test User.



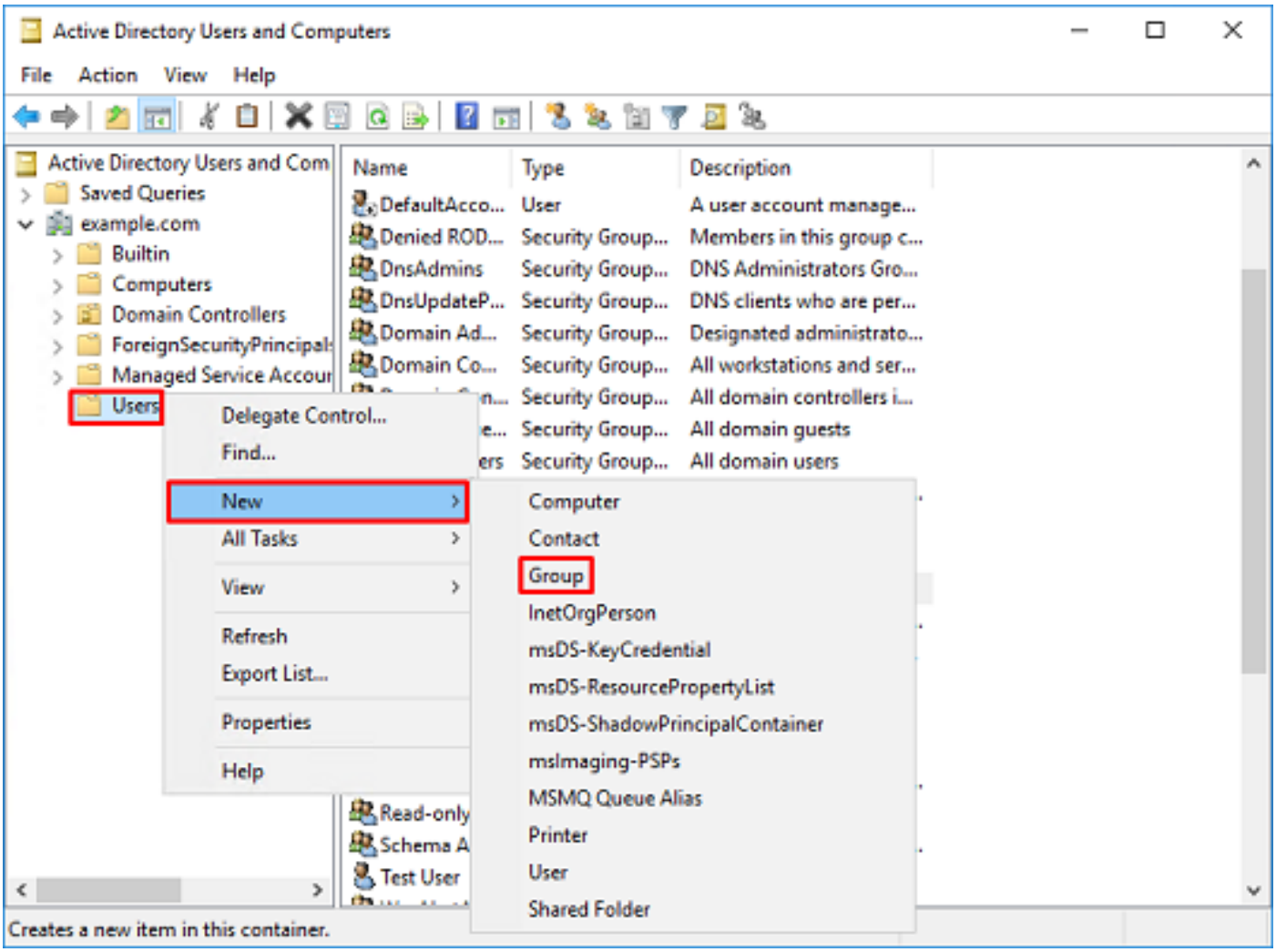
Creare gruppi AD e aggiungere utenti ai gruppi AD (facoltativo)

Sebbene non siano richiesti per l'autenticazione, i gruppi possono essere utilizzati per semplificare l'applicazione di criteri di accesso a più utenti, nonché l'autorizzazione LDAP.

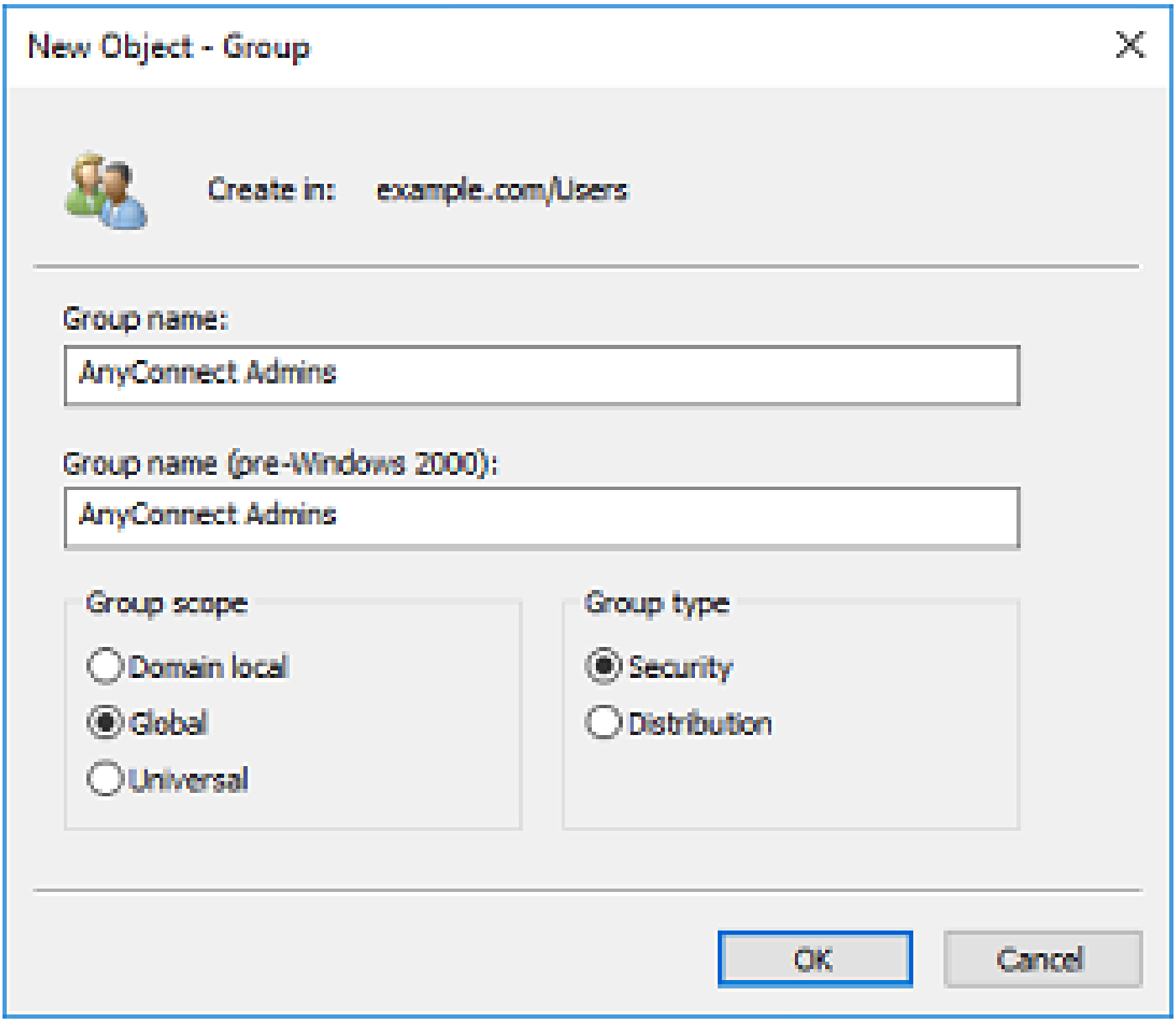
In questa guida alla configurazione i gruppi vengono utilizzati per applicare le impostazioni dei criteri di controllo di accesso in un secondo momento tramite l'identità dell'utente in FMC.

1. In Utenti e computer di Active Directory, fare clic con il pulsante destro del mouse sul contenitore o sull'unità organizzativa a cui viene aggiunto il nuovo gruppo.

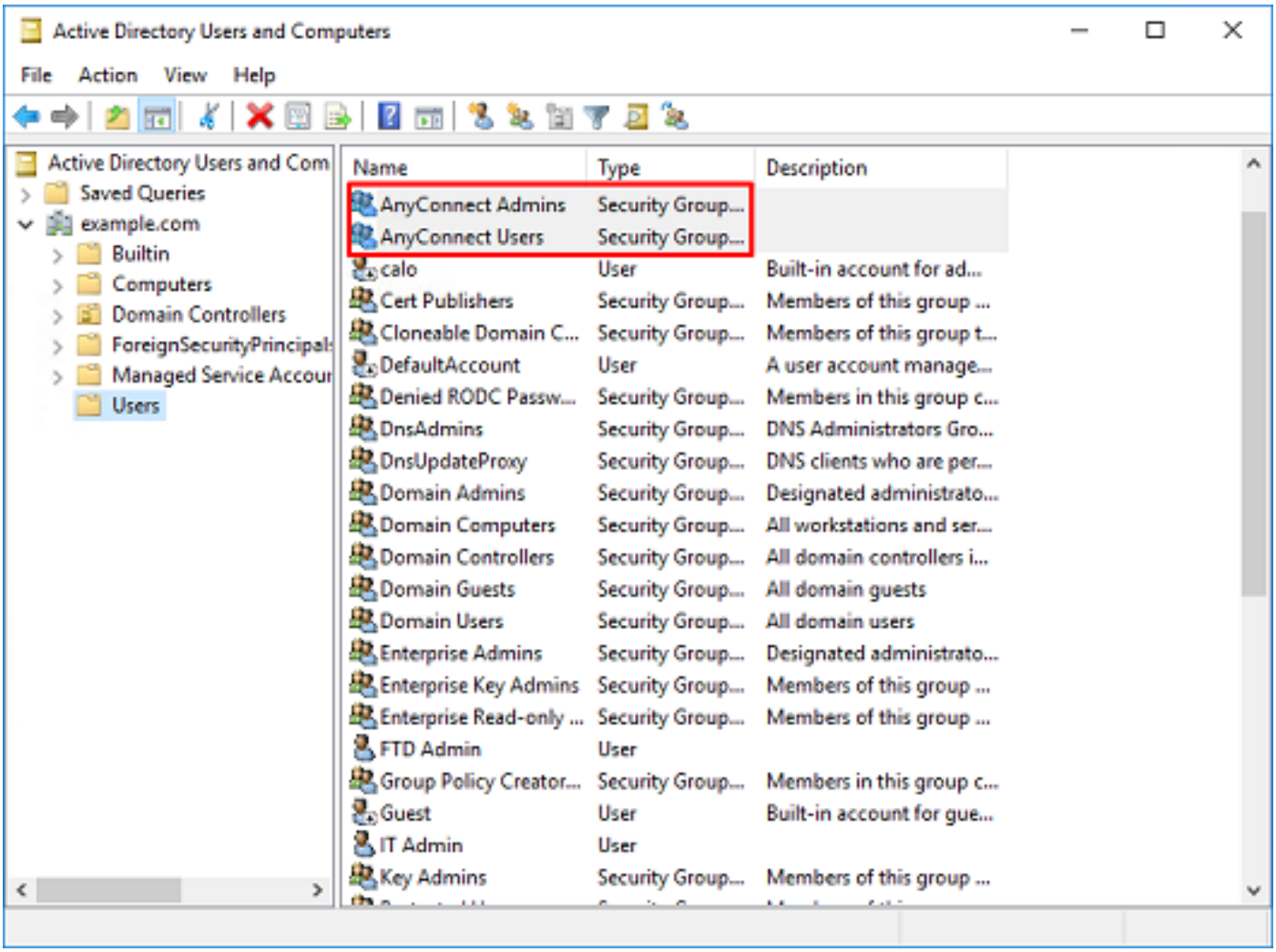
Nell'esempio, il gruppo AnyConnect Admins viene aggiunto al contenitore Users. Fare clic con il pulsante destro del mouse su Utenti, quindi selezionare Nuovo > Gruppo.



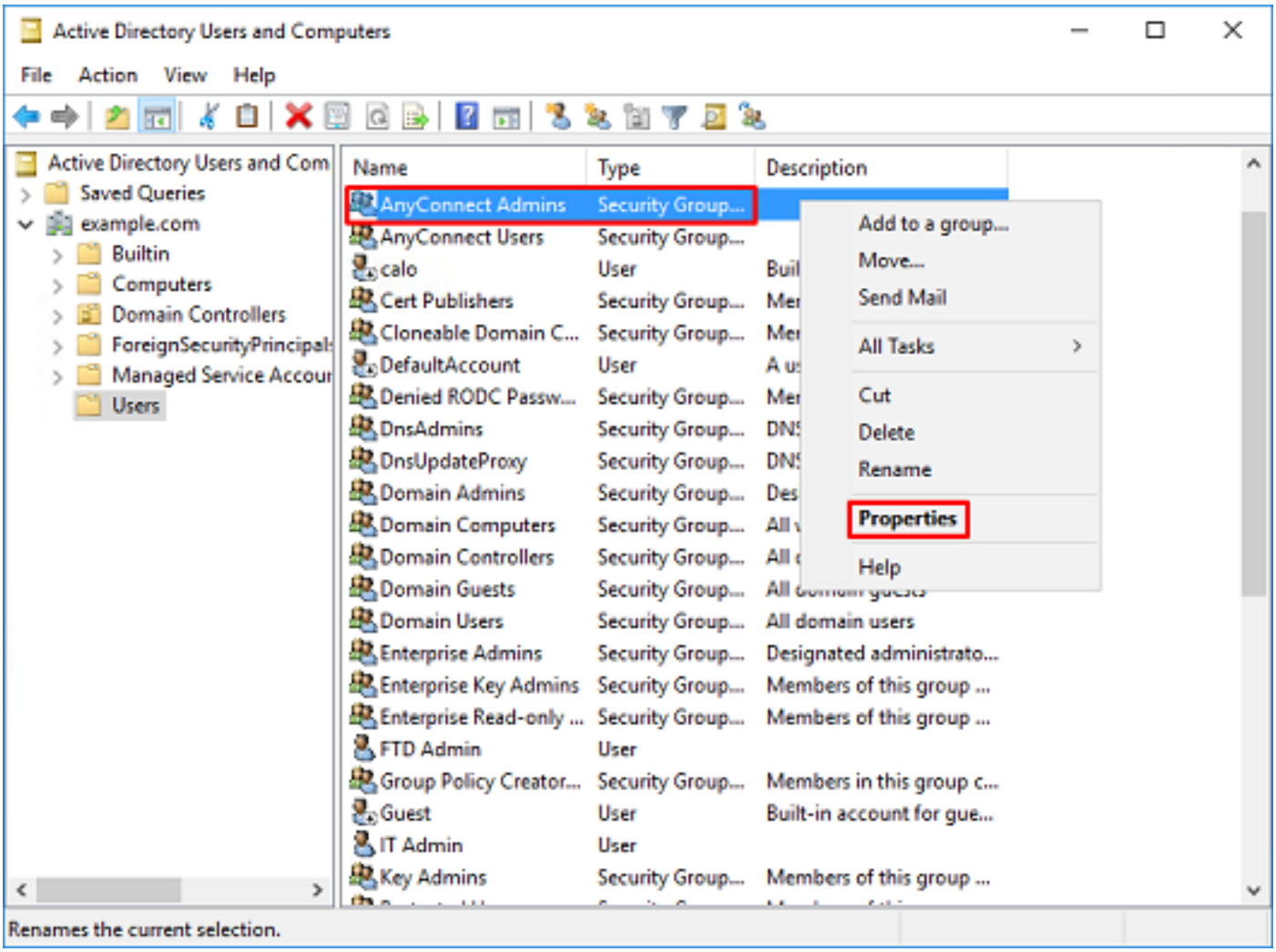
2. Eseguire la Creazione guidata nuovo oggetto - gruppo.



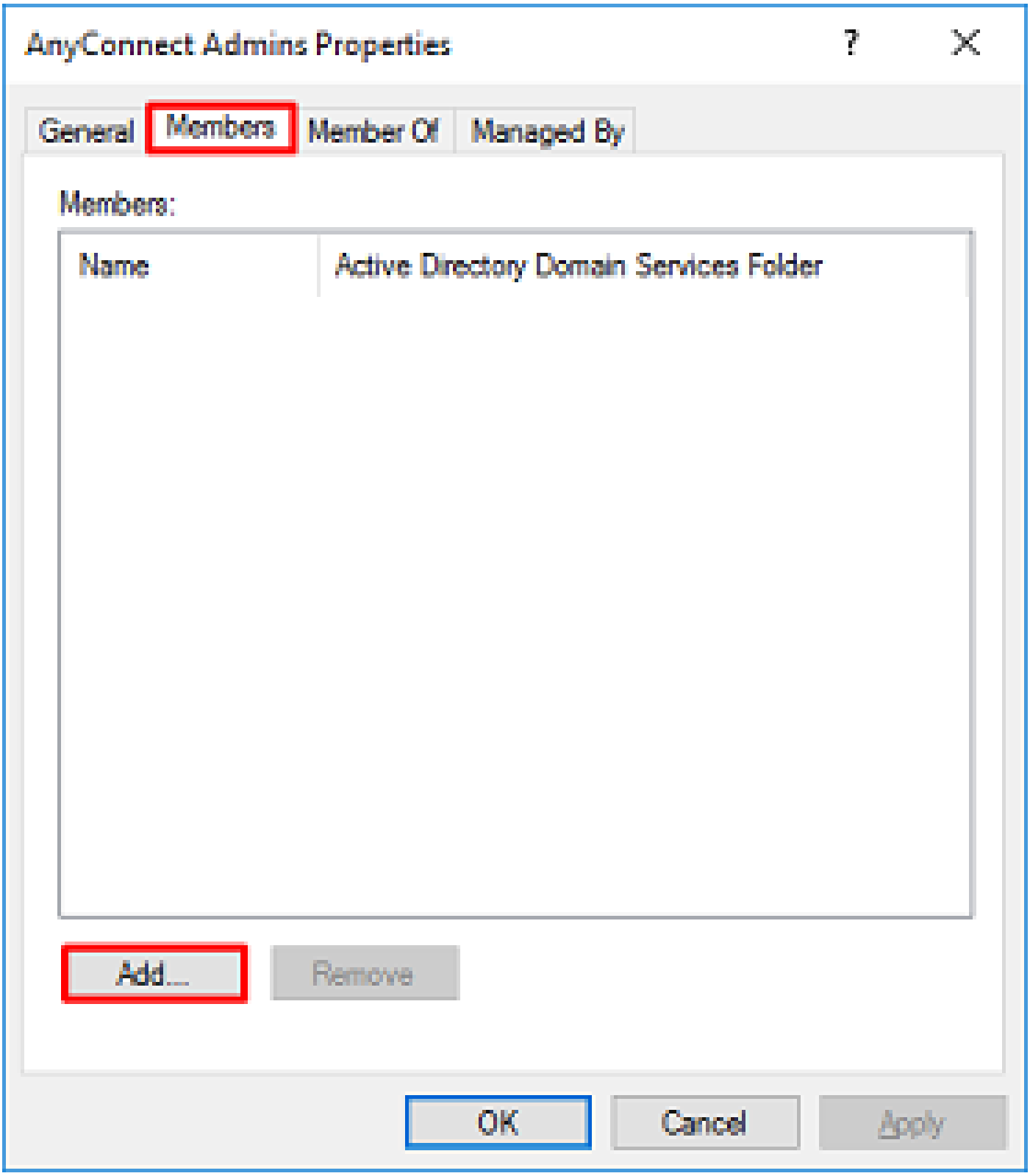
3. Verificare la creazione del gruppo. Viene inoltre creato il gruppo AnyConnect Users.



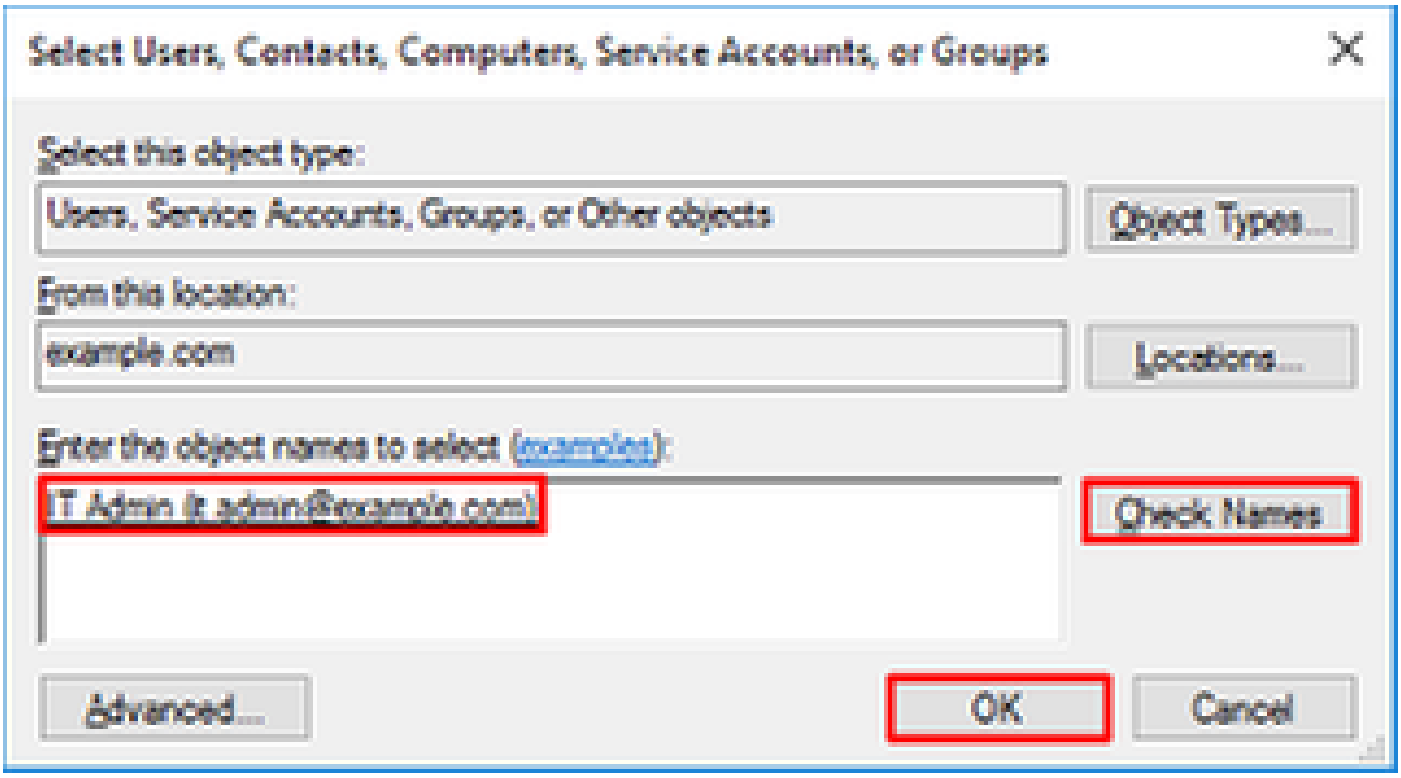
4. Fare clic con il pulsante destro del mouse sul gruppo o sugli utenti e scegliere Proprietà. In questa configurazione, l'utente IT Admin viene aggiunto al gruppo AnyConnect Admins e l'utente Test User viene aggiunto al gruppo AnyConnect Users.



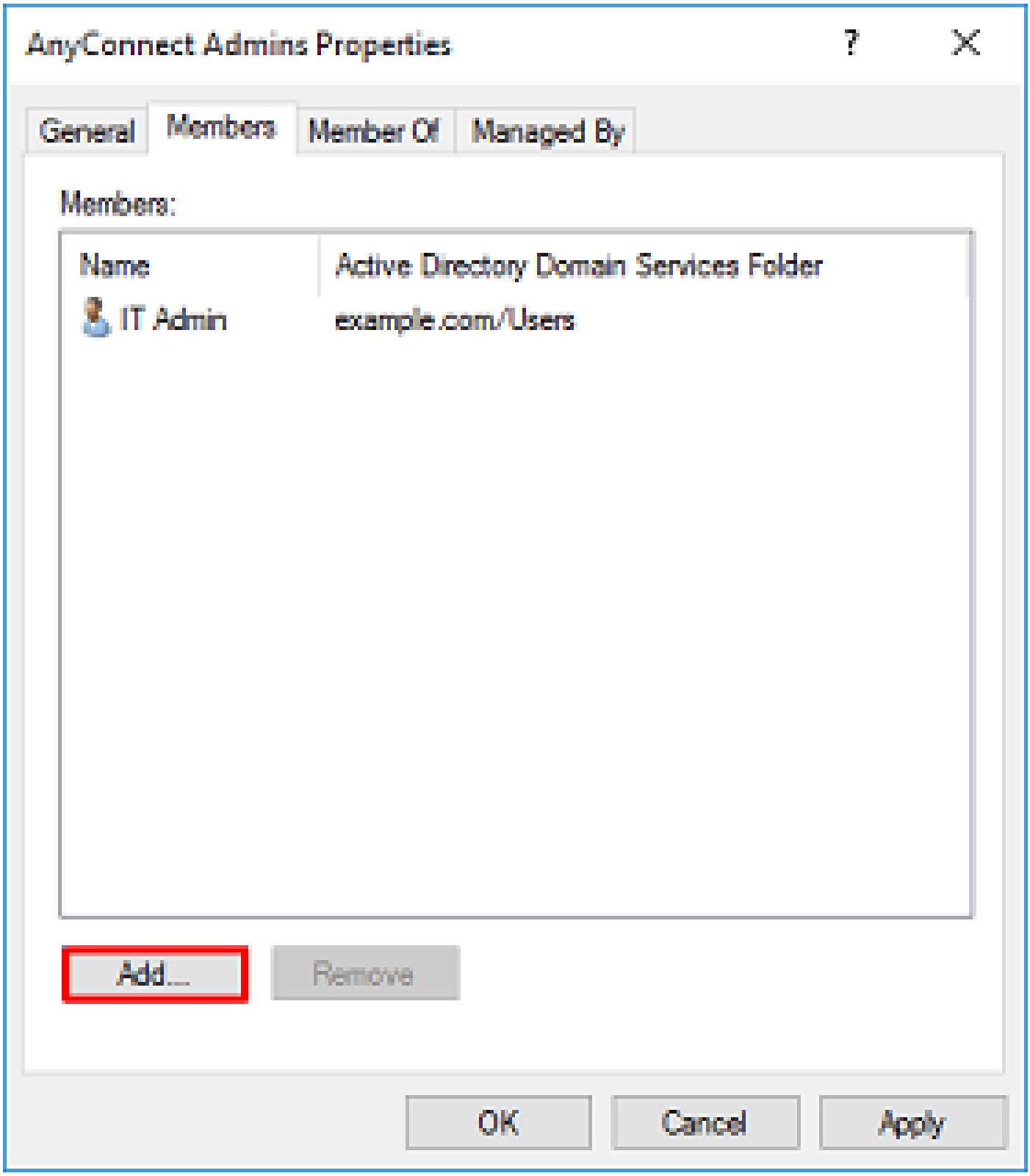
5. In Membri scheda, fare clic su Aggiungi.



Immettere l'utente nel campo e fare clic su Controlla nomi per verificare che l'utente sia stato trovato. Una volta effettuata la verifica, fare clic su OK.

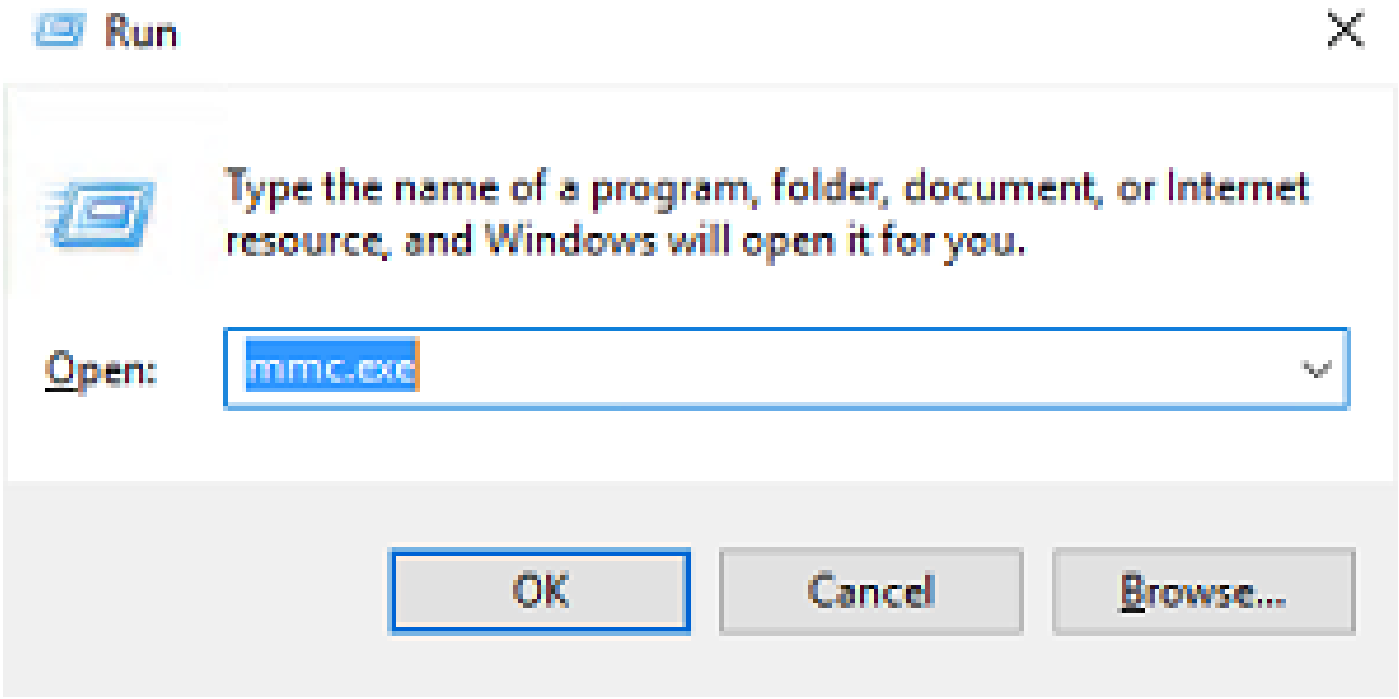


Verificare che sia stato aggiunto l'utente corretto, quindi fare clic su OK. Analogamente, l'utente Test User viene aggiunto al gruppo AnyConnect Users.

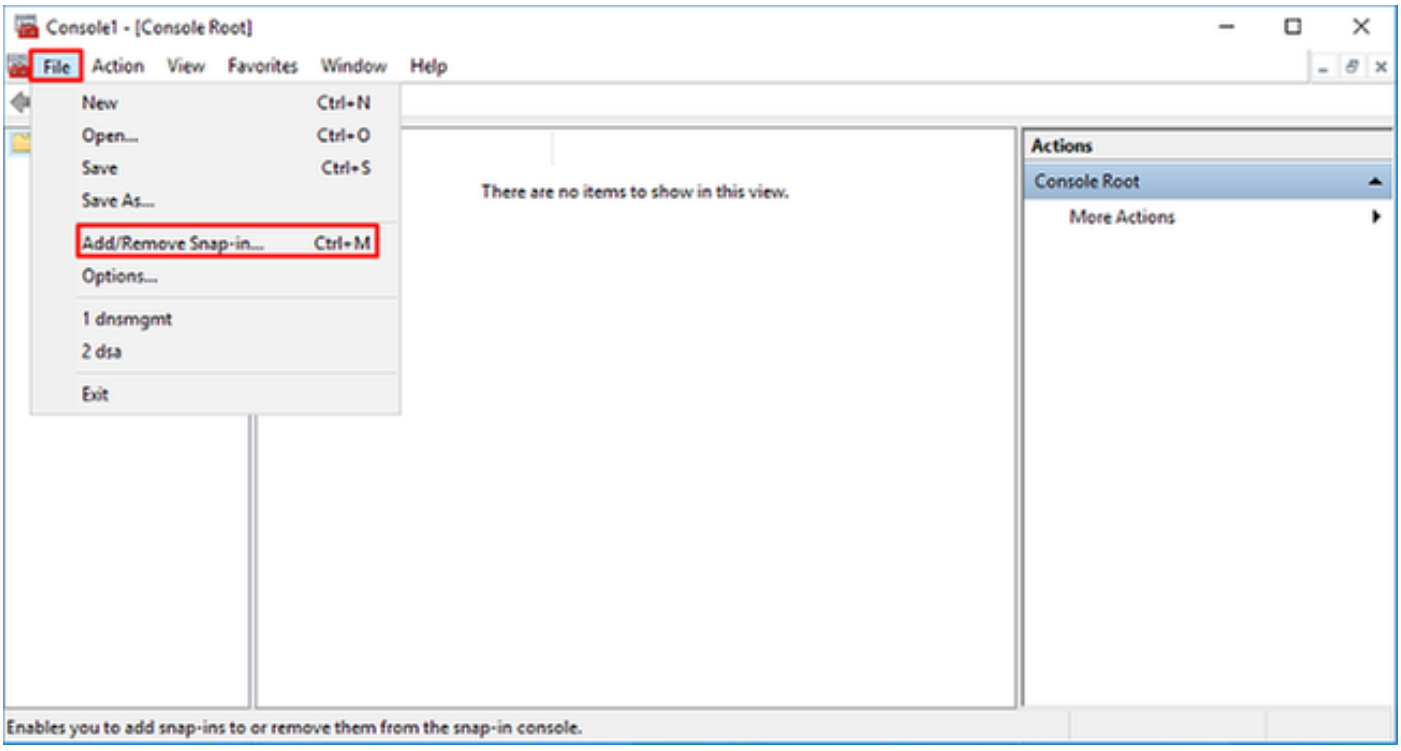


Copia radice certificato SSL LDAPS (richiesto solo per LDAPS o STARTTLS)

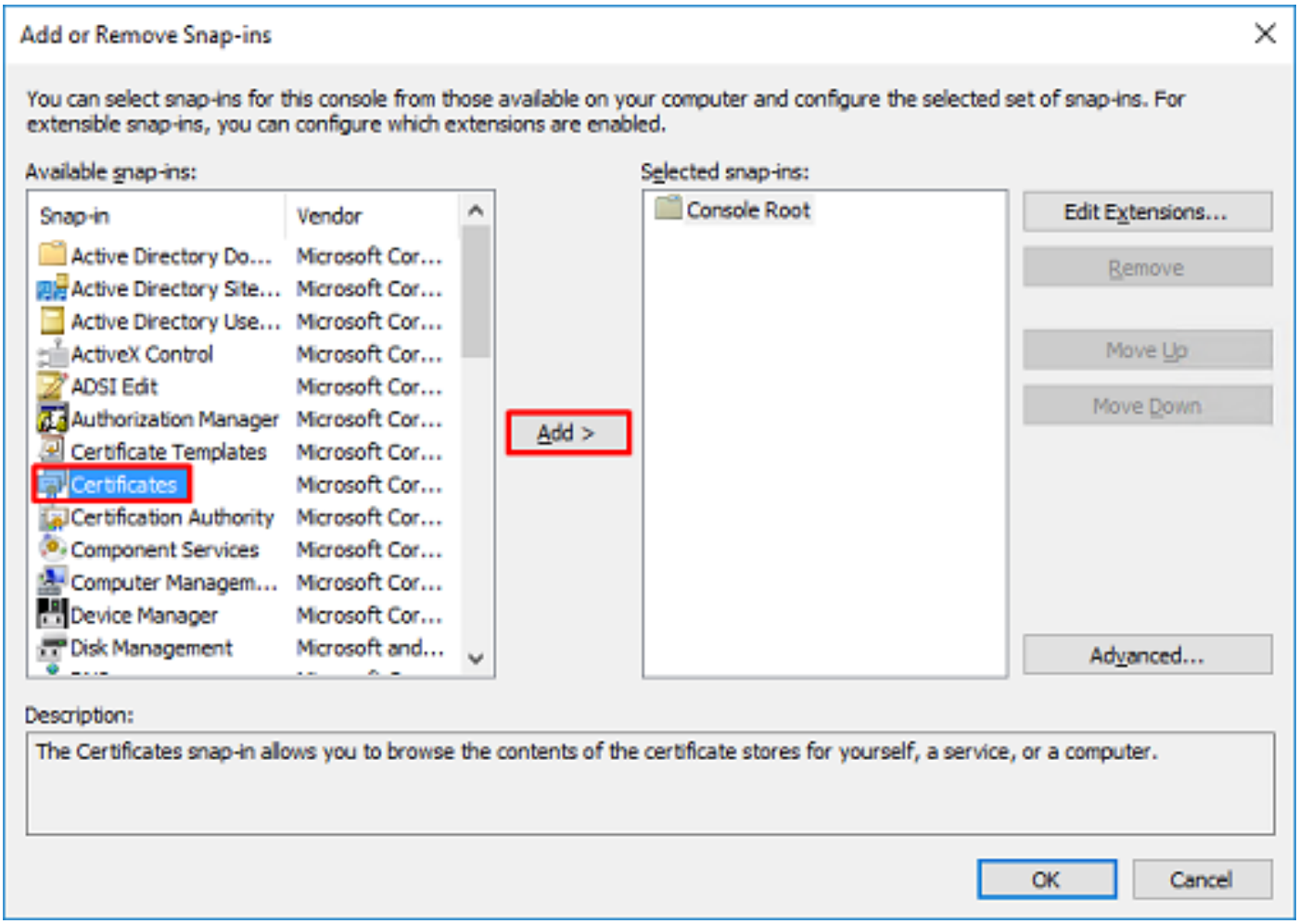
1. Premere Win+R e immettere mmc.exe. Quindi fare clic su OK.



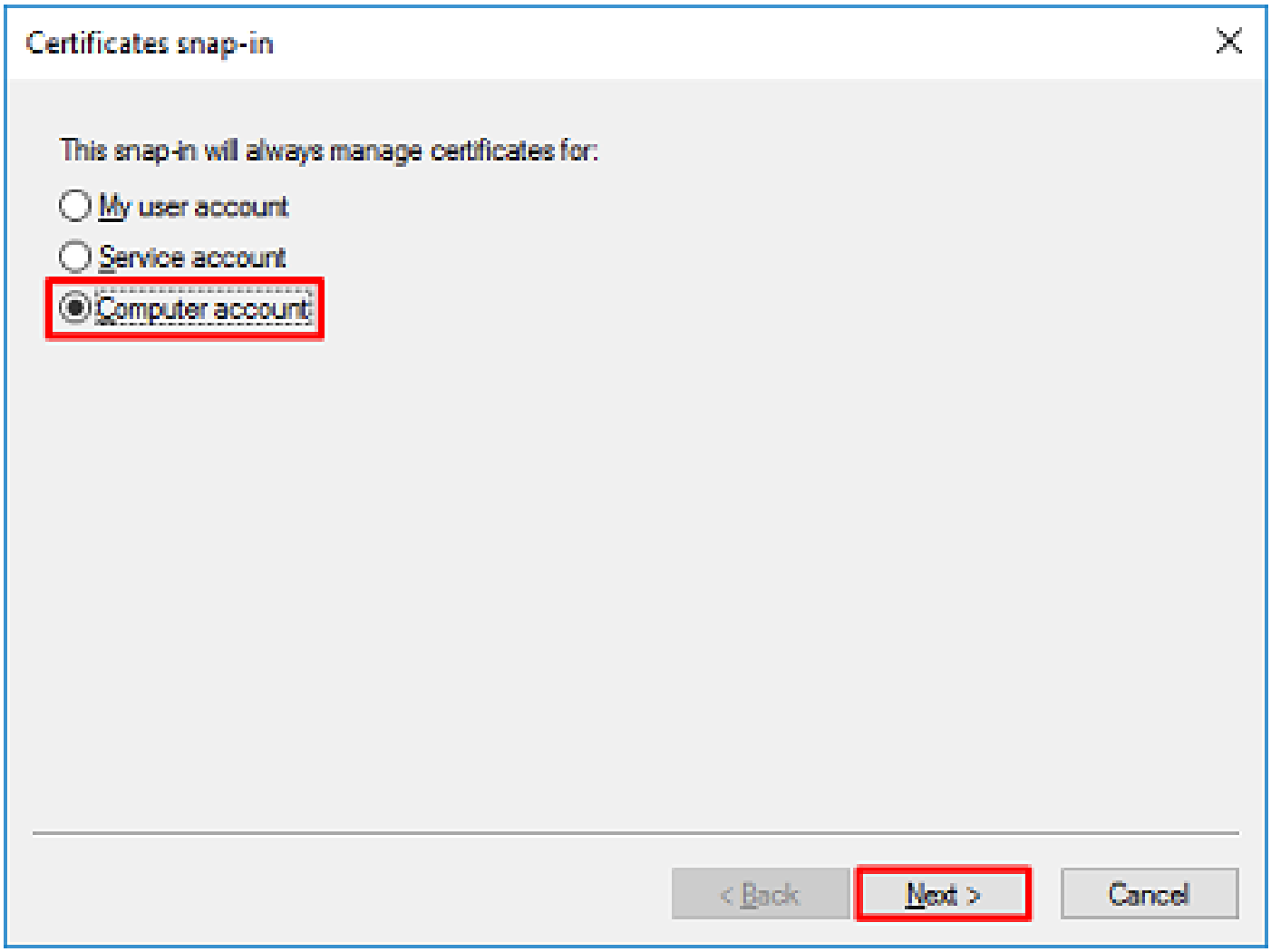
2. Passare a File > Aggiungi/Rimuovi snap-in.



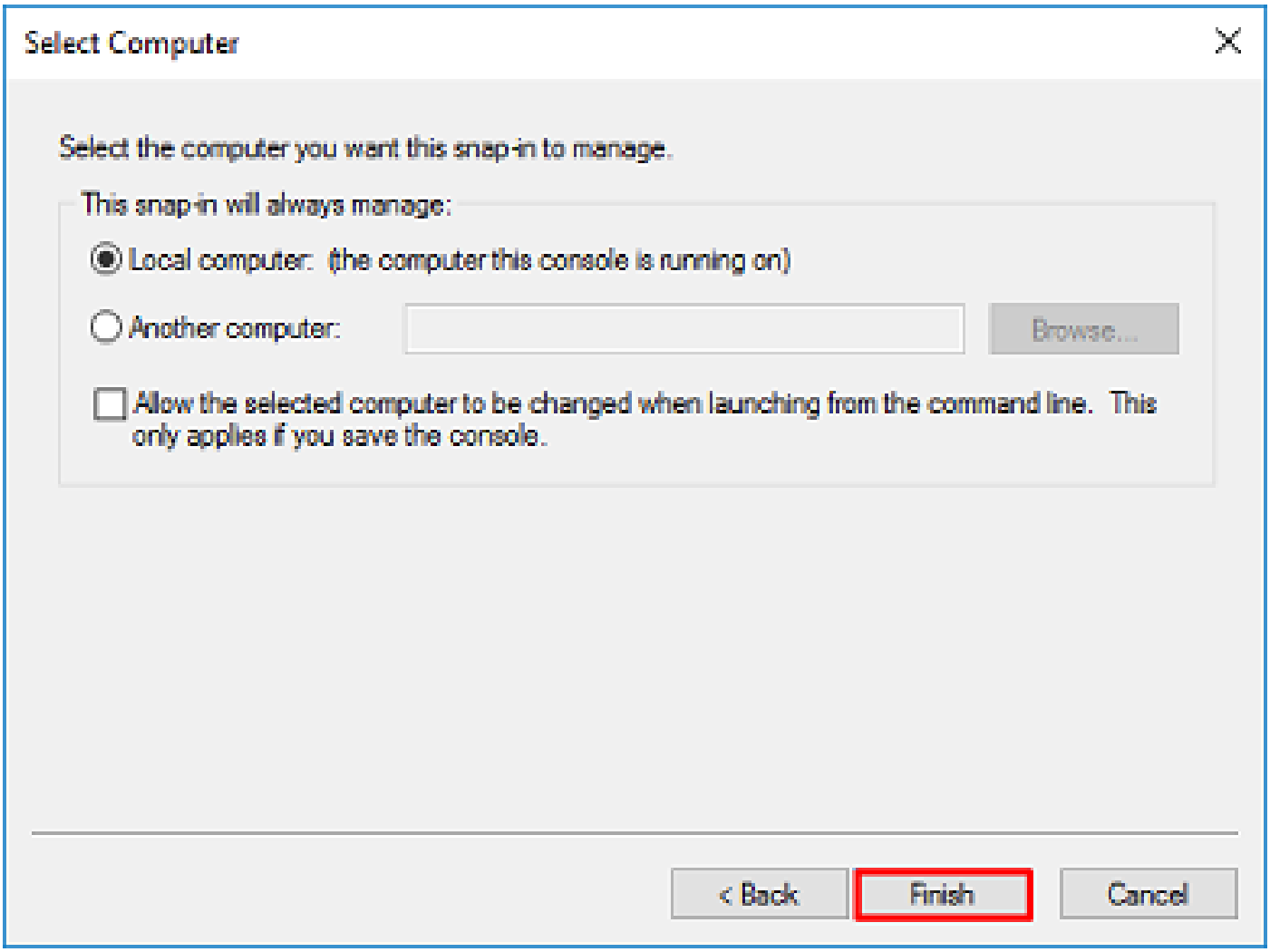
3. In Snap-in disponibili, selezionare Certificati, quindi fare clic su Aggiungi.



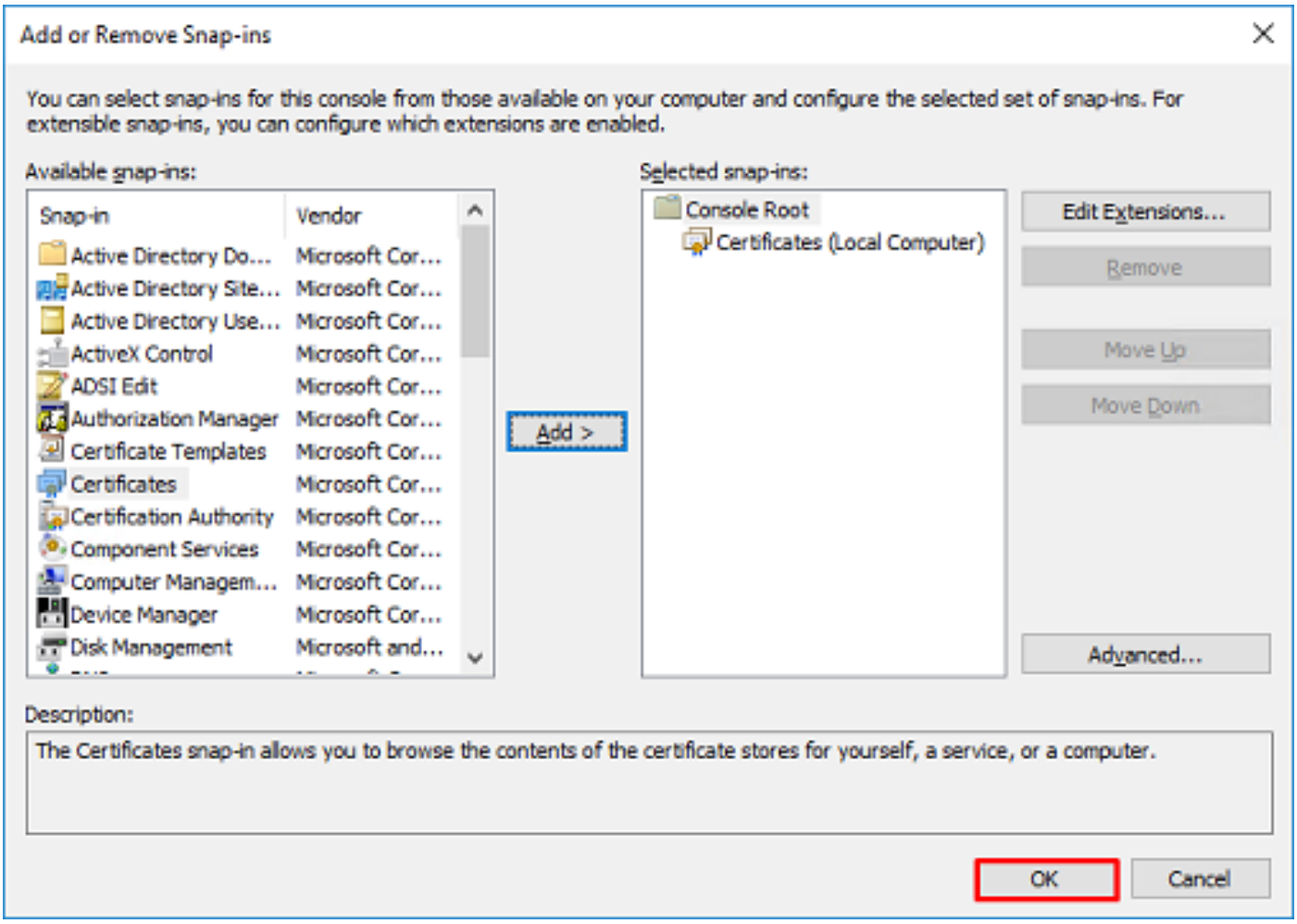
4. Selezionare Account computer, quindi fare clic su Avanti.



Fare clic su Finish (Fine).



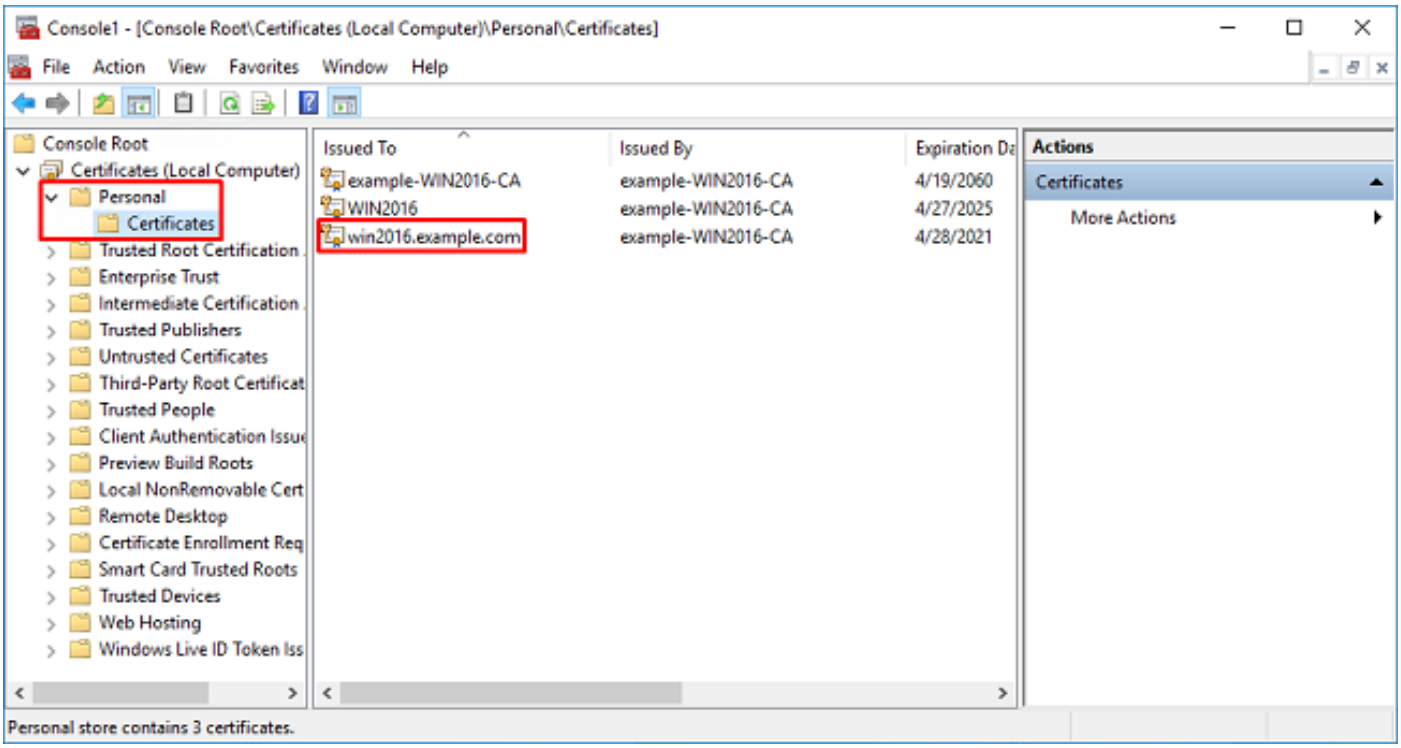
5. Fare clic su OK.



6. Espandere la cartella Personale, quindi fare clic su Certificati. Il certificato utilizzato da LDAPS viene rilasciato al nome di dominio completo (FQDN) del server Windows. In questo server sono elencati 3 certificati.

- Certificato CA rilasciato a e da example-WIN2016-CA.
- Certificato di identità rilasciato a WIN2016 da example-WIN2016-CA.
- Certificato di identità rilasciato a win2016.example.com da example-WIN2016-CA.

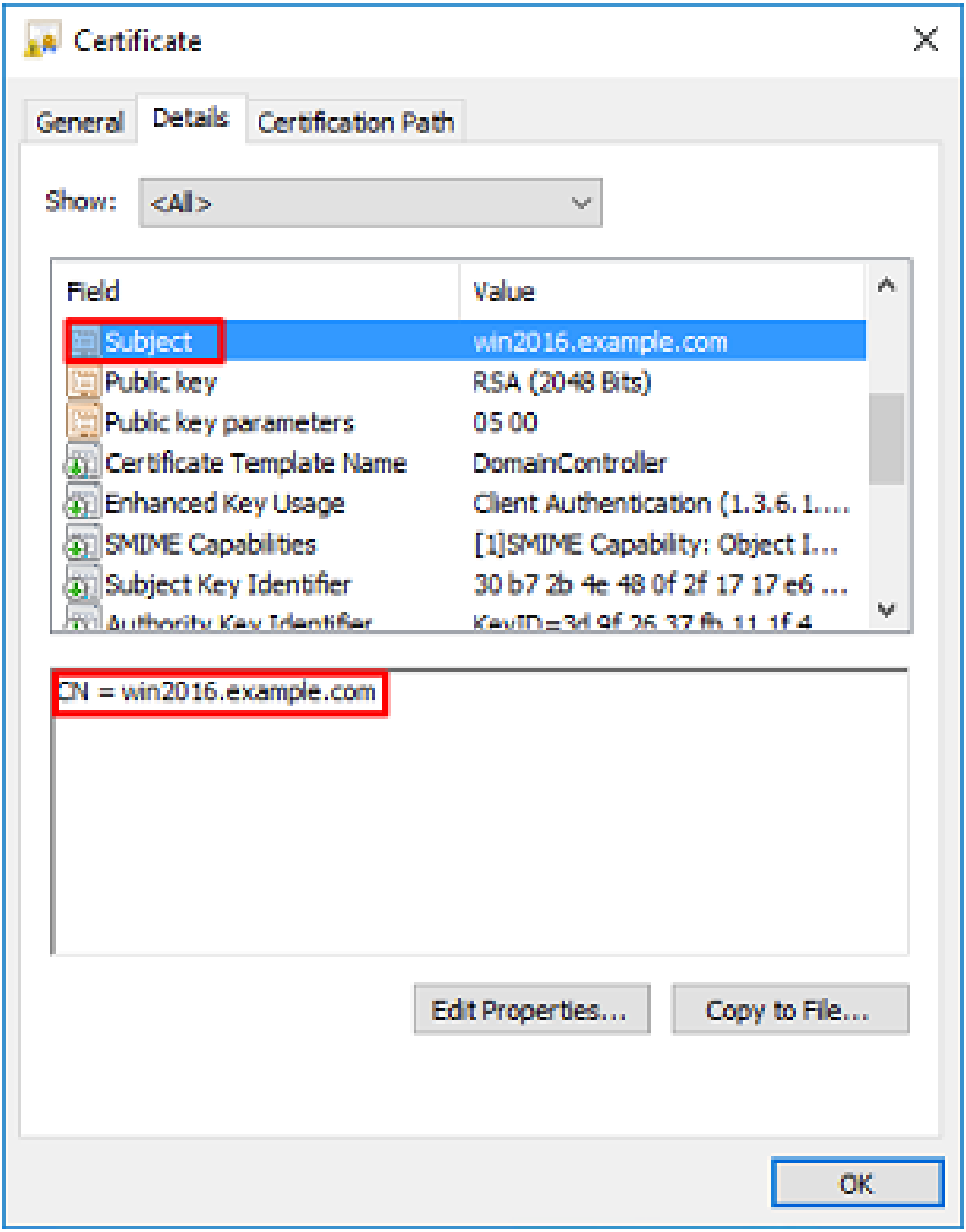
In questa guida alla configurazione, il nome di dominio completo (FQDN) è win2016.example.com, quindi i primi 2 certificati non sono validi per l'utilizzo come certificato SSL LDAPS. Il certificato di identità rilasciato a win2016.example.com è un certificato rilasciato automaticamente dal servizio CA di Windows Server. Fare doppio clic sul certificato per controllare i dettagli.



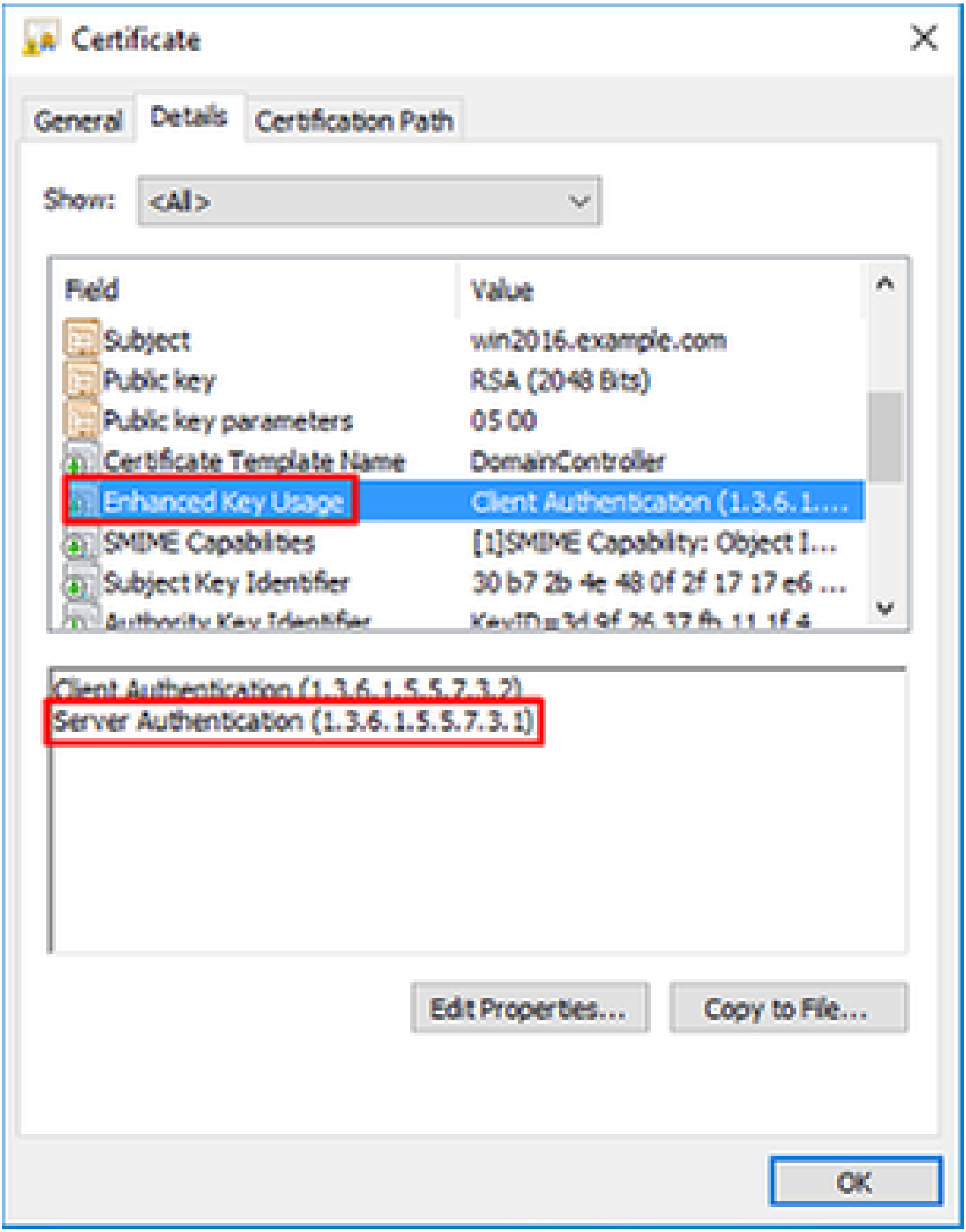
7. Per poter essere utilizzato come certificato SSL LDAPS, il certificato deve soddisfare i seguenti requisiti:

- Il nome comune o il nome alternativo del soggetto DNS corrisponde al nome di dominio completo (FQDN) del server Windows.
- Nel campo Utilizzo chiavi avanzato del certificato è presente Autenticazione server.

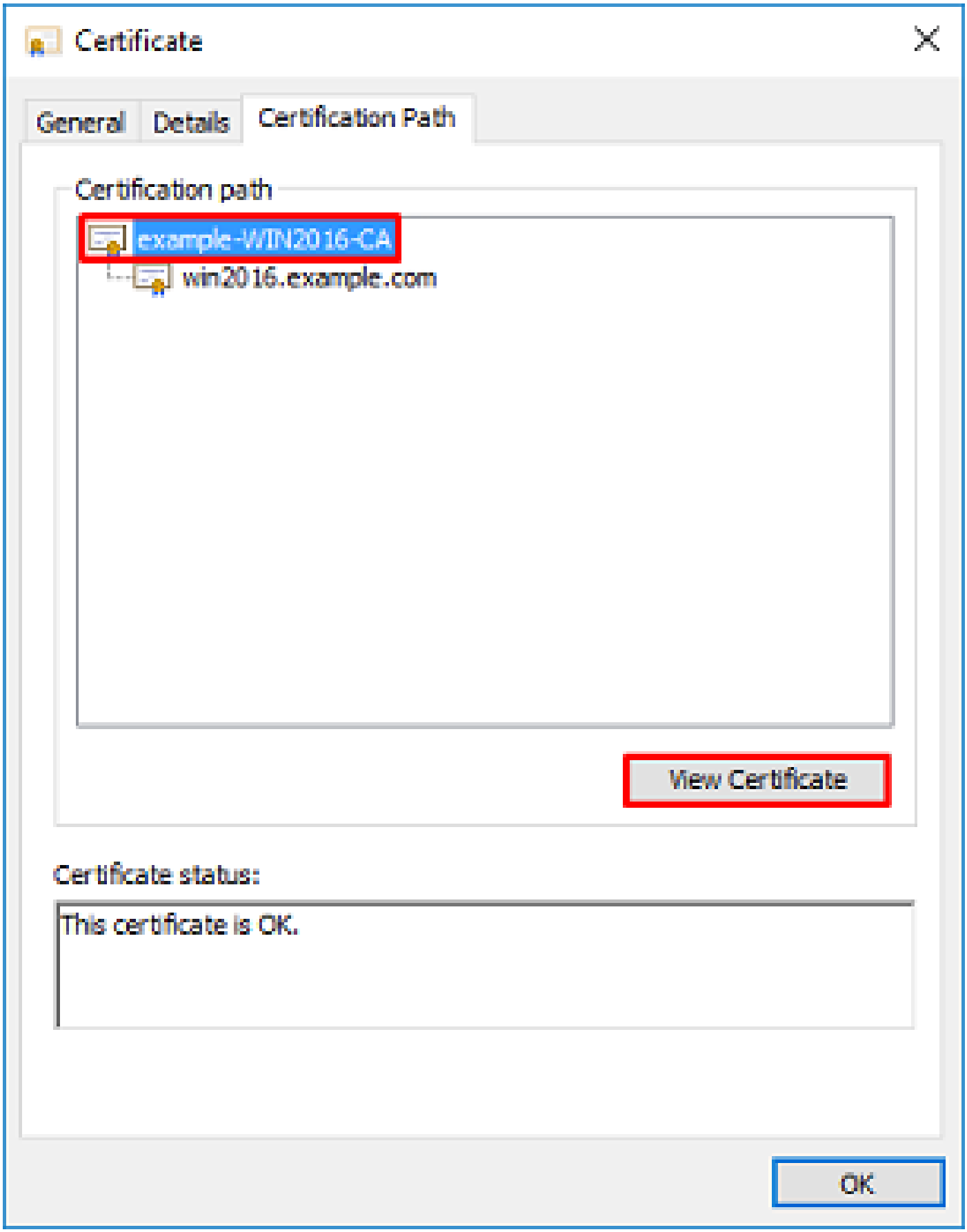
Nella scheda Dettagli del certificato selezionare Soggetto e Nome alternativo soggetto per visualizzare il nome FQDN win2016.example.com.



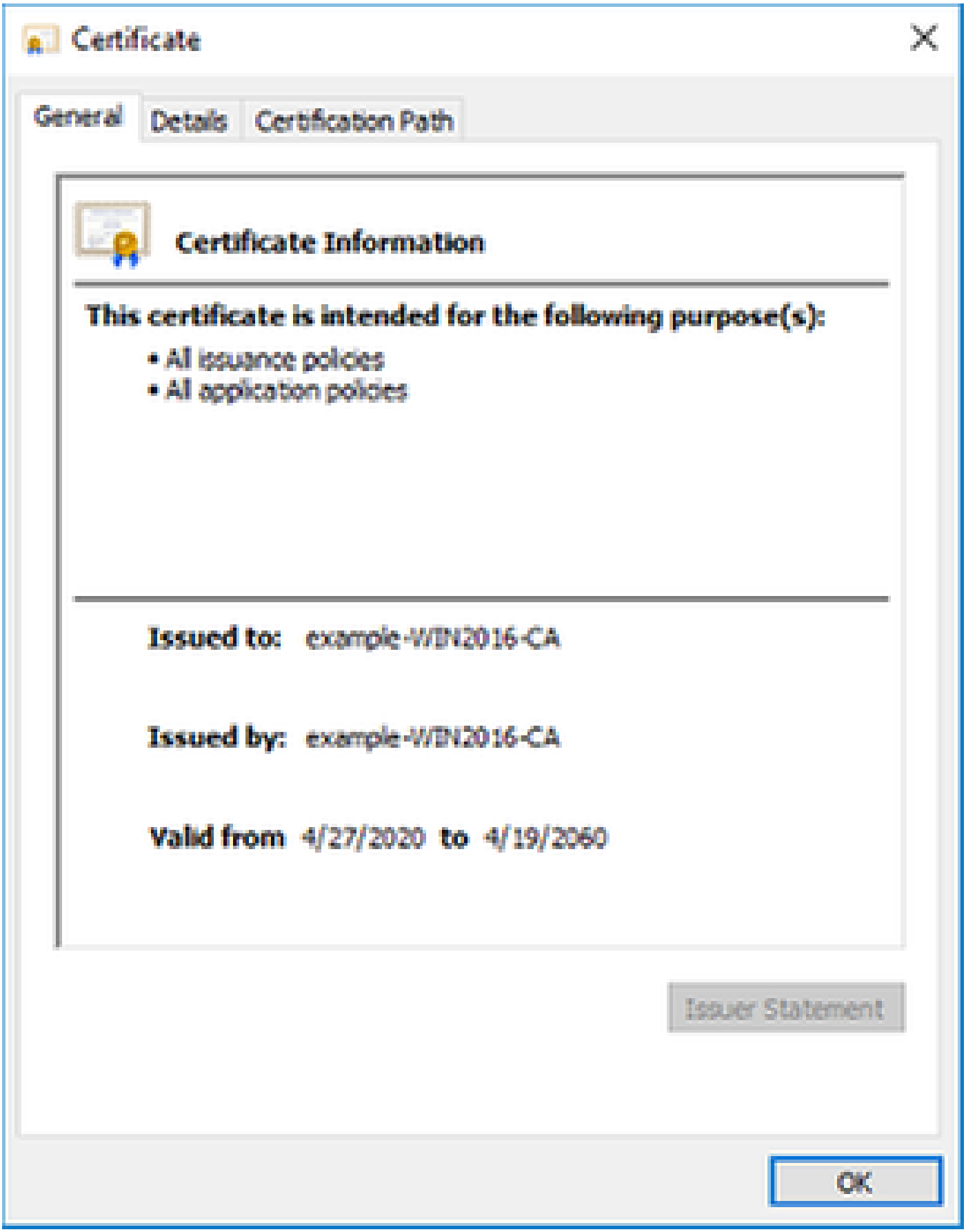
In Utilizzo chiavi avanzato è presente Autenticazione server.



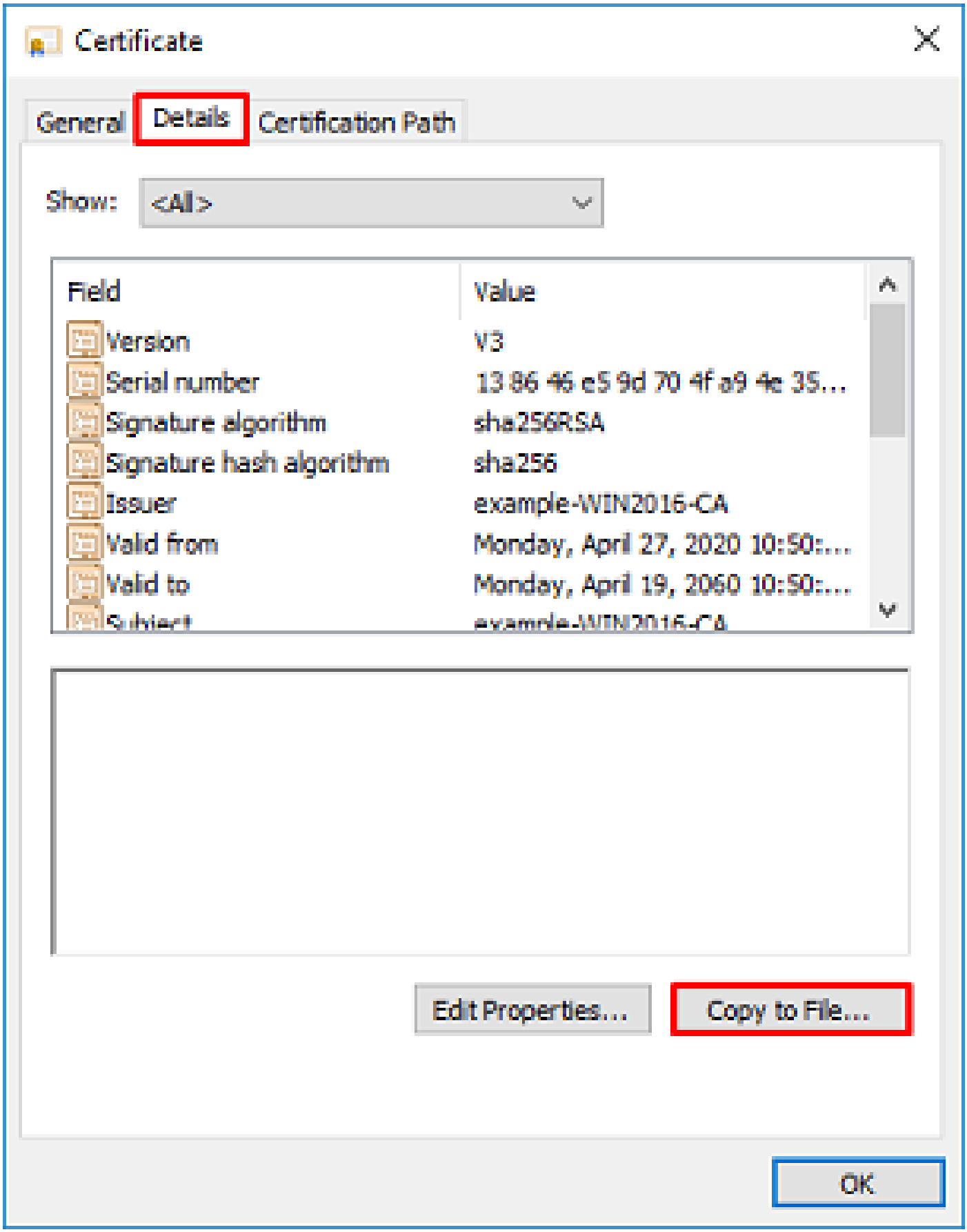
8. Dopo la conferma, nella scheda Percorso certificazione selezionare il primo certificato che corrisponde al certificato CA radice, quindi fare clic su Visualizza certificato.



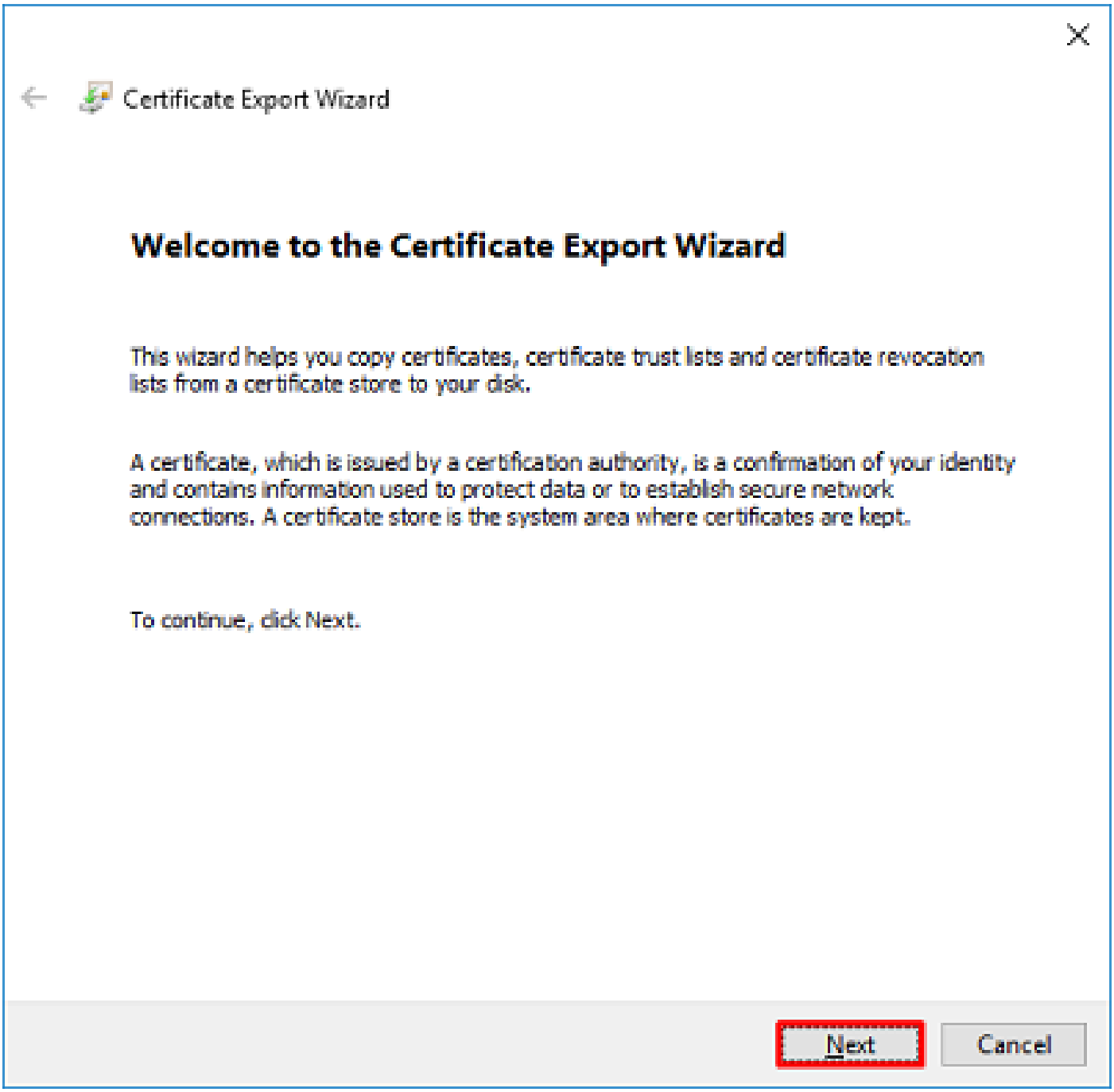
9. Verranno aperti i dettagli Certificati per il certificato CA radice.



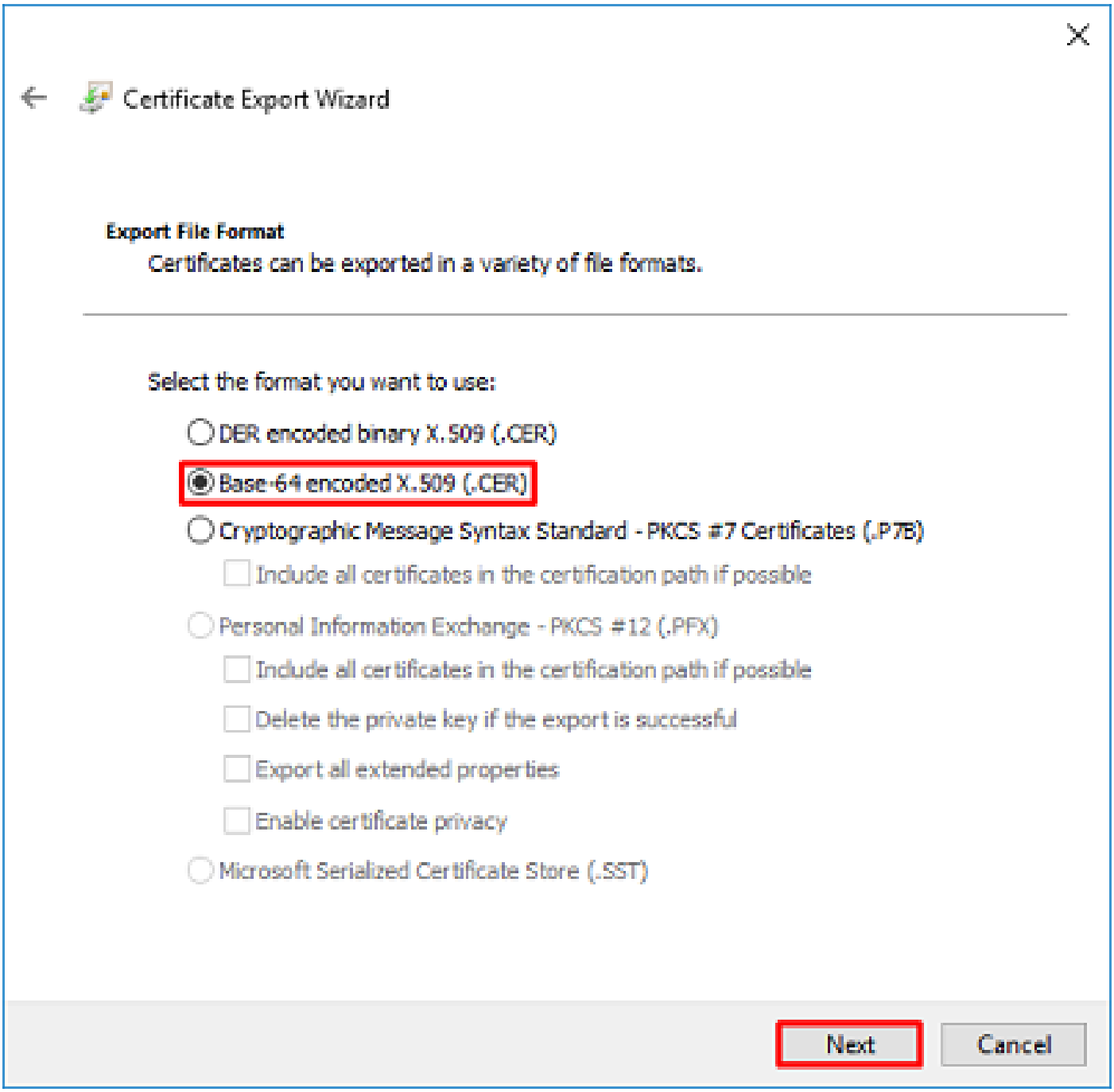
Nella scheda Dettagli fare clic su Copia nel file.



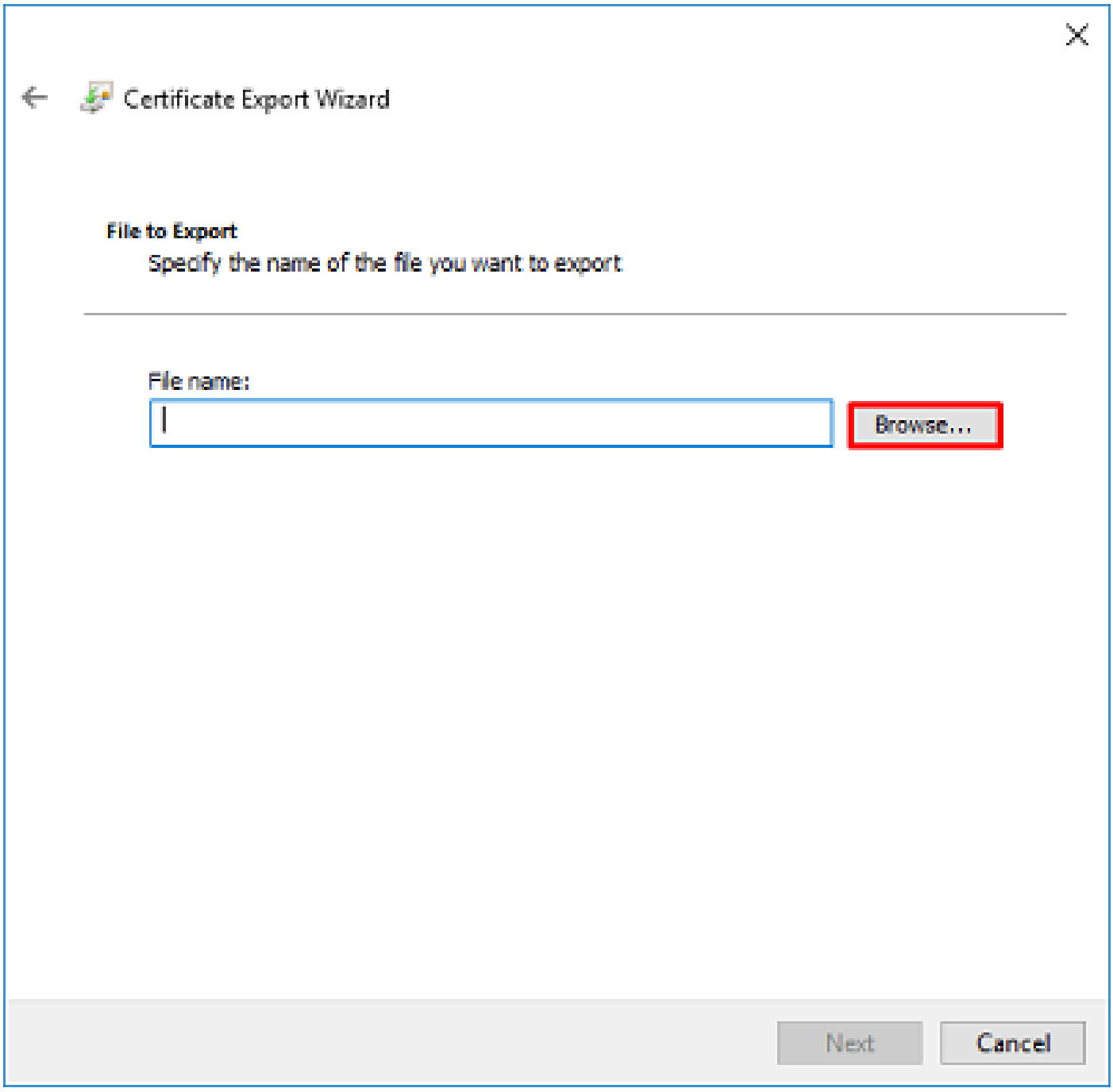
10. Esaminare l'Esportazione guidata certificati. La procedura guidata esporta la CA radice in formato PEM.

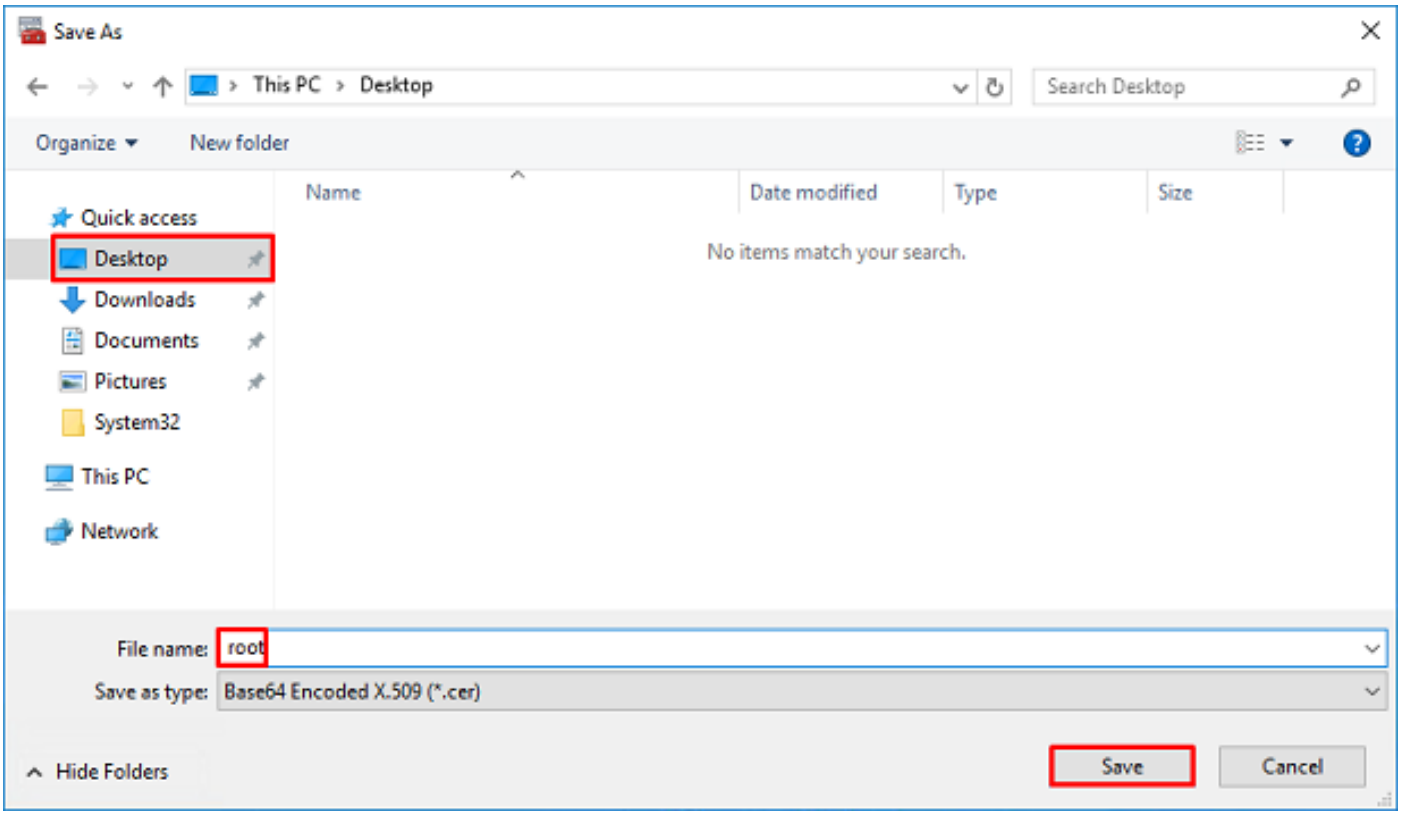


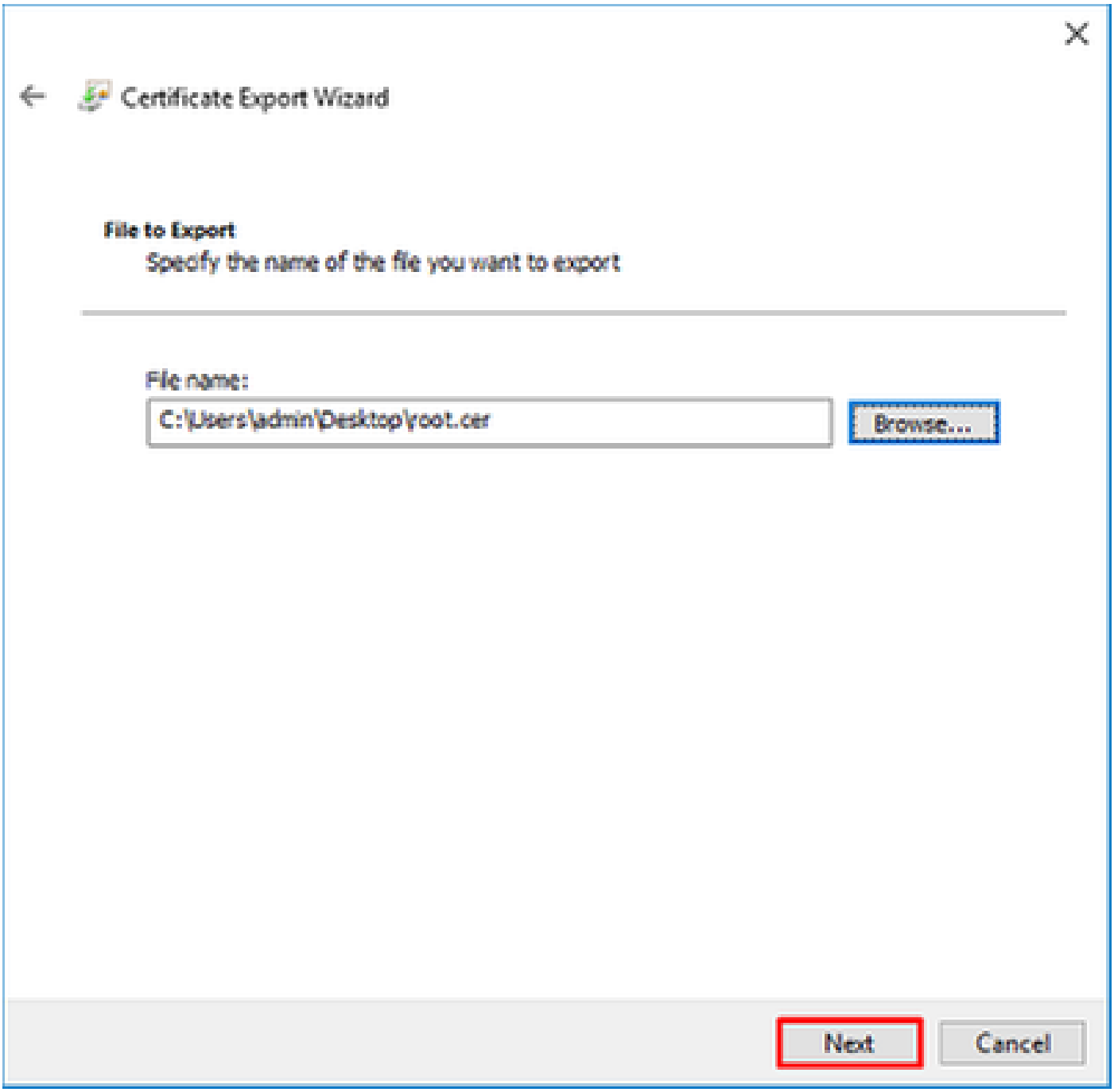
Selezionate X.509 con codifica Base 64.



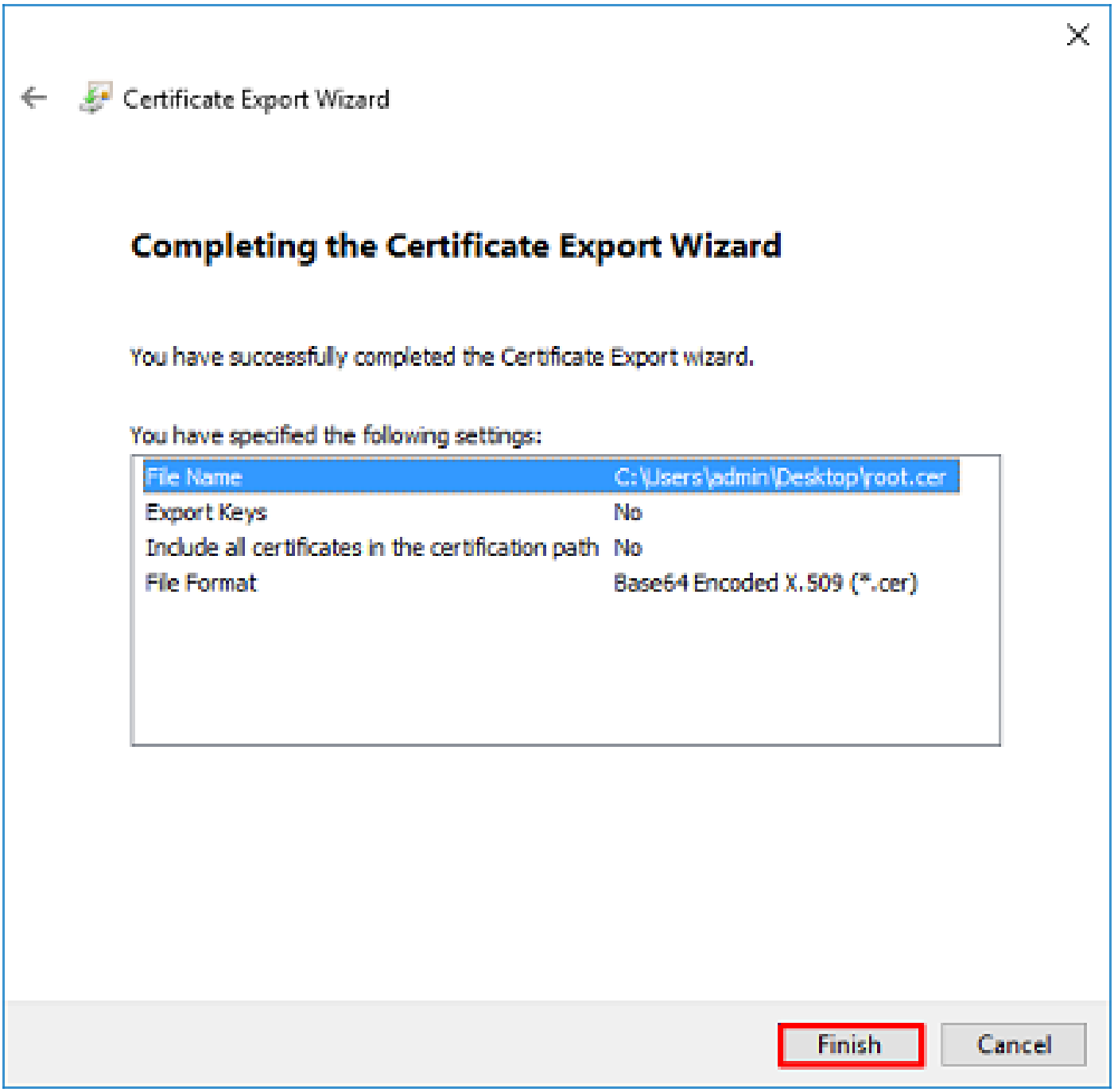
Selezionare il nome del file e la destinazione dell'esportazione.


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
Next
Cancel


Save As
This PC
Desktop
Search Desktop
Organize
New folder
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
No items match your search.
File name:
root
Save as type:
Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel



Fare clic su Fine.



11. Passare al percorso e aprire il certificato con un blocco note o un altro editor di testo. Mostra il certificato del formato PEM. Salva per uso futuro.

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
```

```
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0AnfsojK9IcDr2vpOMTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

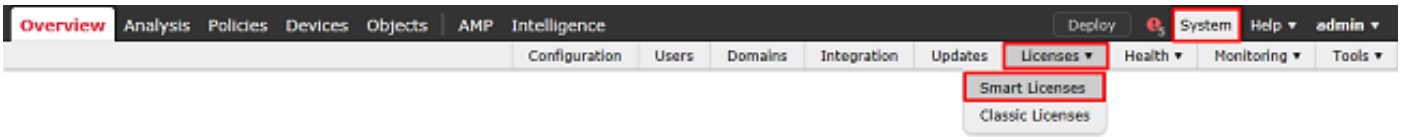
12. (Facoltativo) Nel caso in cui esistano più certificati di identità che possono essere utilizzati da LDAPS e vi siano dubbi sul tipo di certificato utilizzato o non vi sia accesso al server LDAPS, è possibile estrarre la CA radice da un'acquisizione di pacchetti eseguita sul server Windows o FTD dopo.

Configurazioni FMC

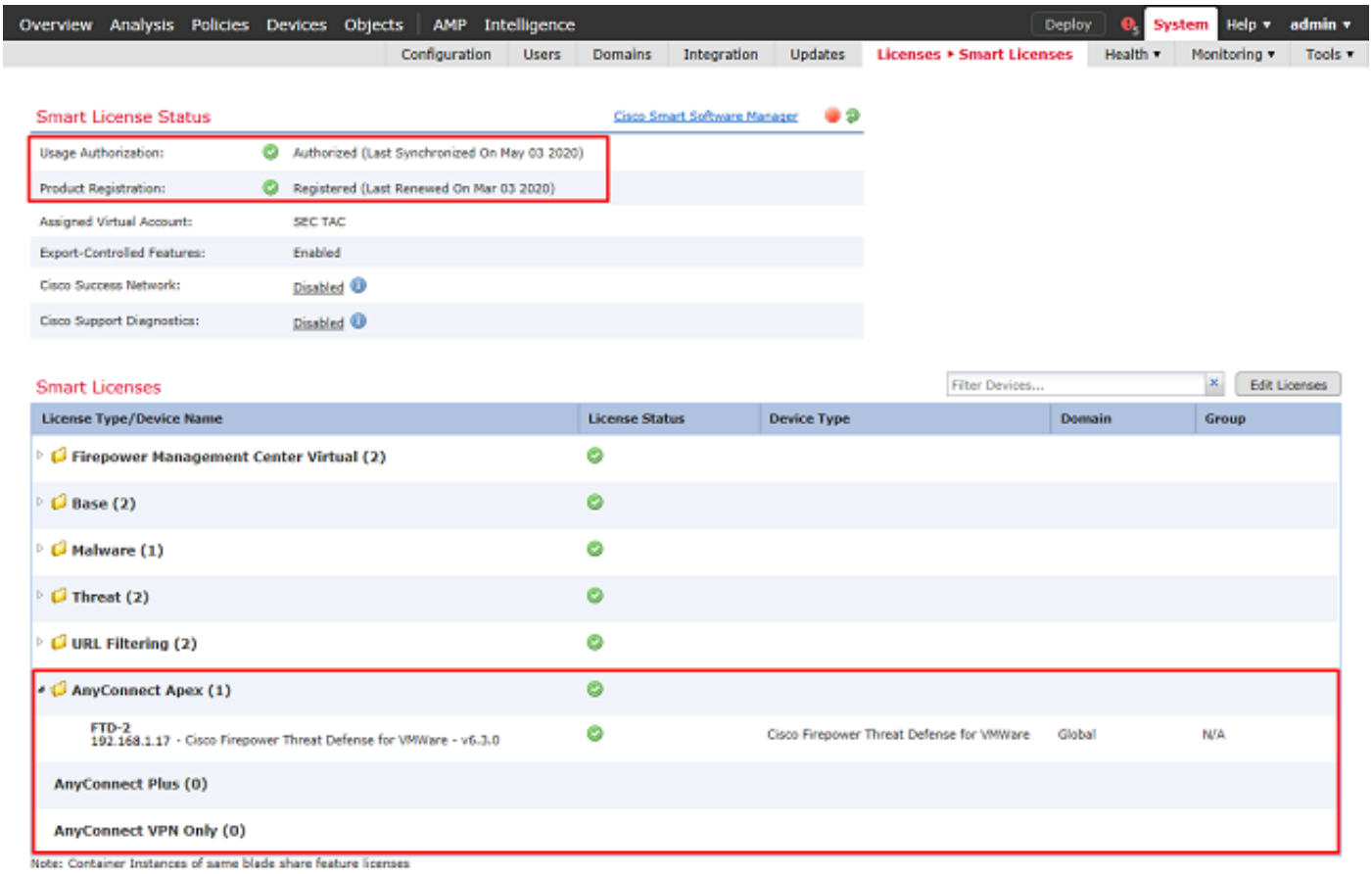
Verifica delle licenze

Per implementare la configurazione AnyConnect, è necessario registrare l'FTD sul server delle licenze Smart e applicare una licenza Plus, Apex o VPN Only valida al dispositivo.

1. Passare a Sistema > Licenze > Smart Licensing.

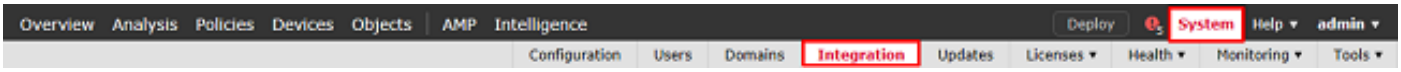


2. Verificare che i dispositivi siano conformi e registrati correttamente. Verificare che il dispositivo sia registrato con una licenza AnyConnect Apex, Plus o VPN Only.

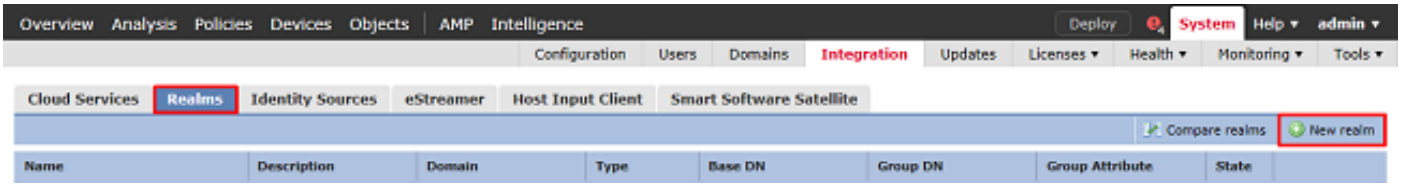


Imposta realm

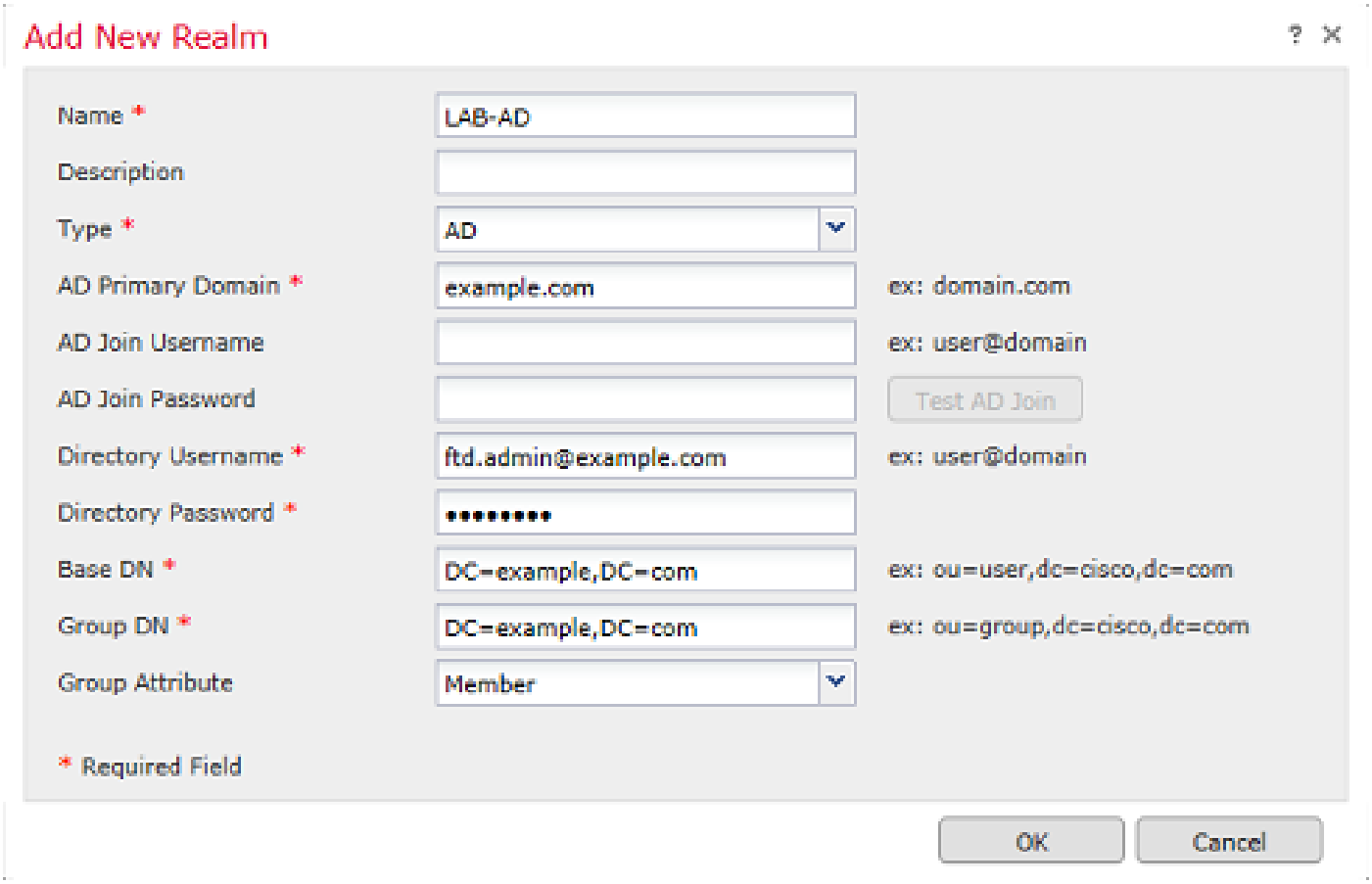
1. Passare a Sistema > Integrazione.



2. In Realm, fare clic su Nuovo realm.



3. Compilare i campi appropriati in base alle informazioni raccolte dal server Microsoft. Quindi fare clic su OK.

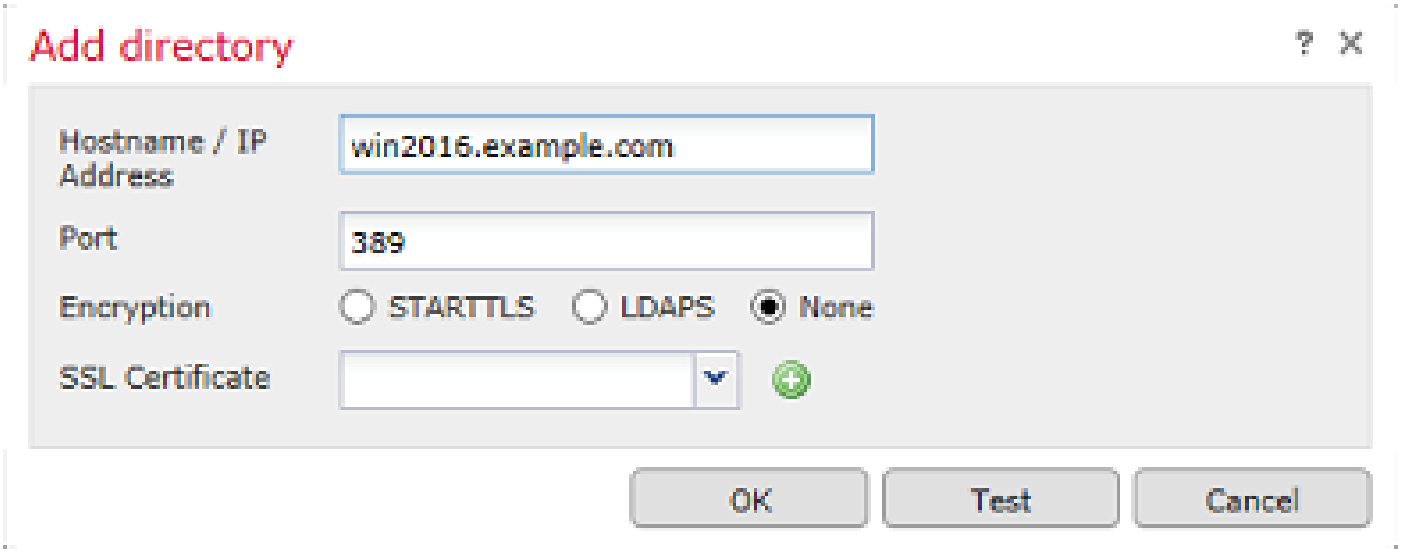


4. Nella nuova finestra, selezionare Directory, se non è già stato scelto, fare clic su Aggiungi directory.

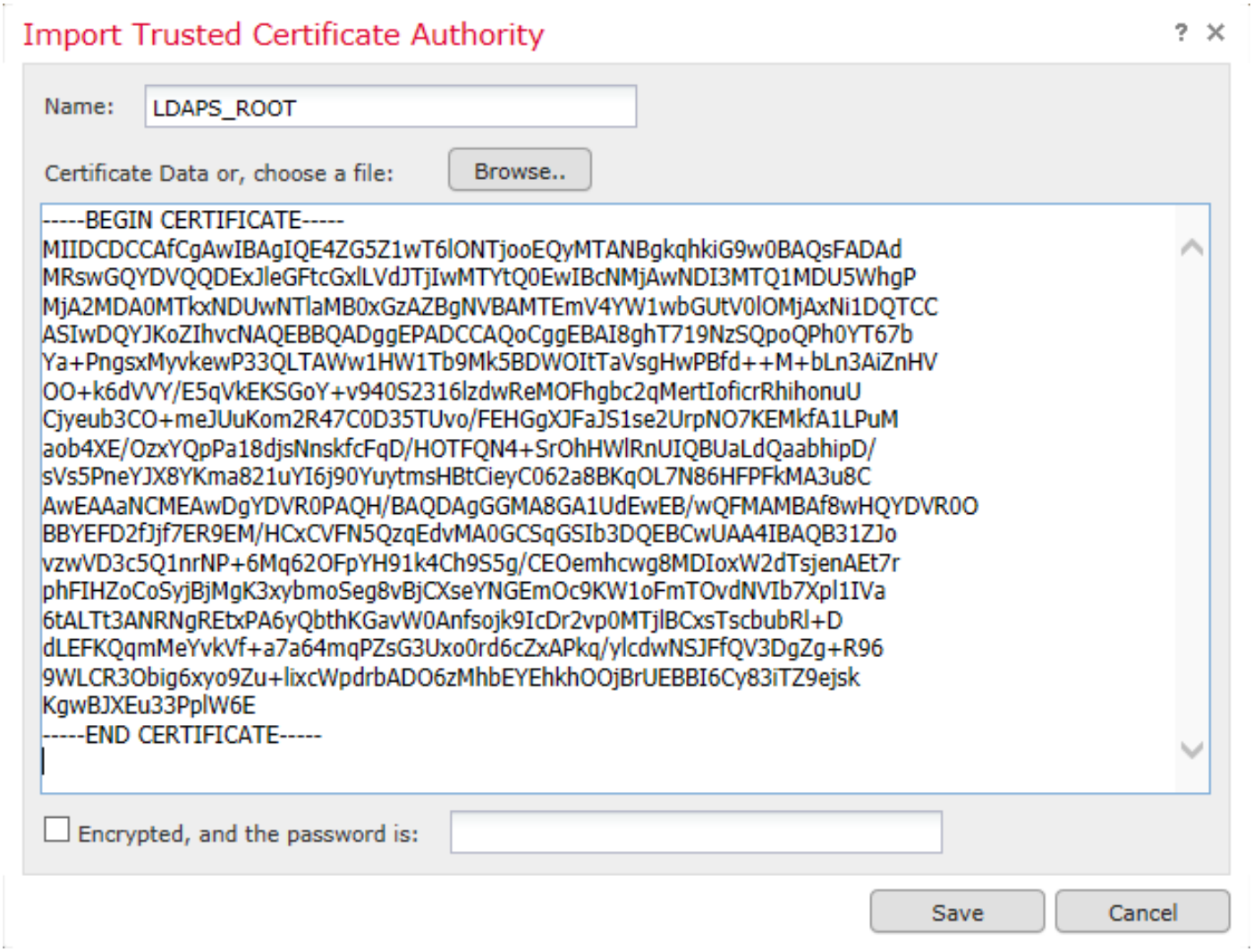
Specificare i dettagli per il server AD. Si noti che se si utilizza il nome di dominio completo (FQDN), FMC e FTD non sono in grado di eseguire correttamente il binding a meno che DNS non sia configurato per risolvere il nome di dominio completo.

Per configurare DNS per FMC, passare a Sistema > Configurazione e selezionare Interfacce di gestione.

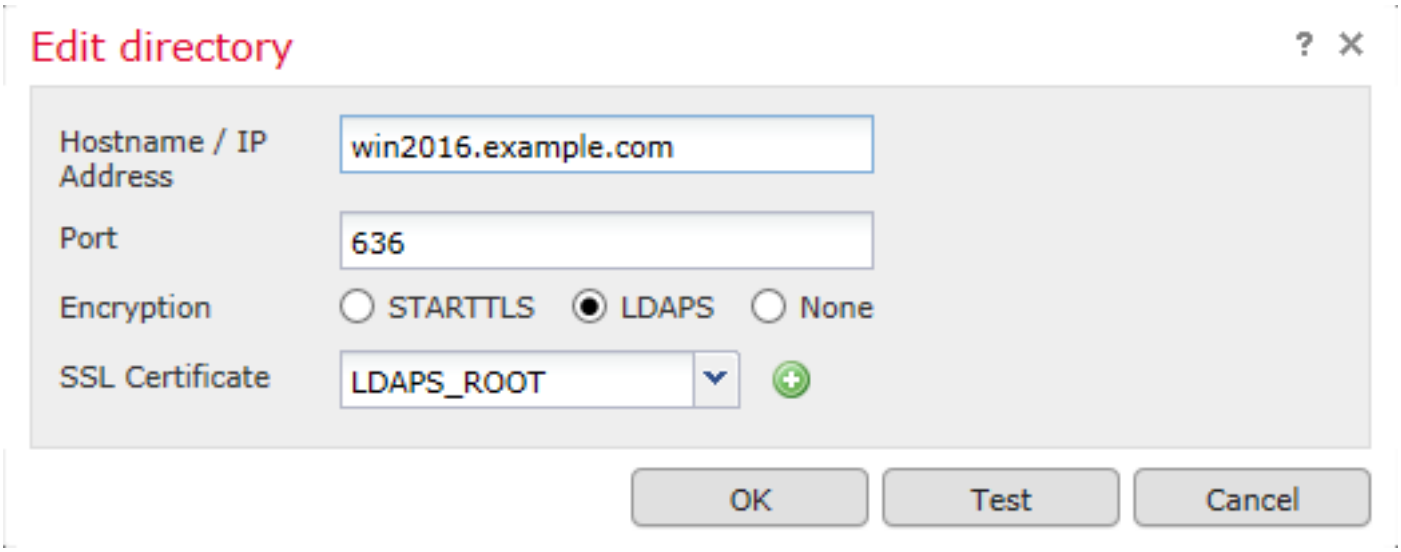
Per configurare il DNS per l'FTD, selezionare Dispositivi > Impostazioni piattaforma, creare un nuovo criterio o modificare un criterio corrente, quindi passare a DNS.



Se si utilizza LDAPS o STARTTLS, fare clic sul simbolo verde + (più), assegnare un nome al certificato e copiare il certificato CA radice in formato PEM. Quindi fare clic su Salva.



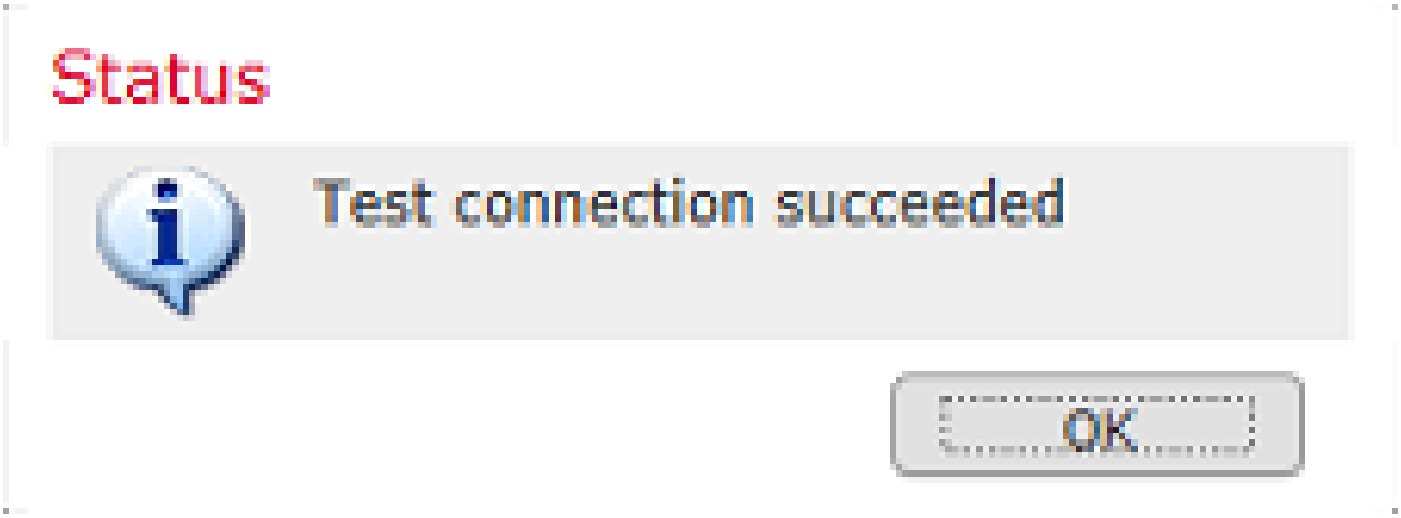
Selezionare la CA radice appena aggiunta dal menu a discesa accanto a Certificato SSL e fare clic su STARTTLS o LDAPS.



Fare clic su Test per verificare che FMC sia in grado di eseguire correttamente il binding con il nome utente e la password della directory forniti nel passaggio precedente.

Poiché questi test vengono avviati dal FMC e non tramite una delle interfacce instradabili configurate sull'FTD (come interna, esterna, dmz), una connessione riuscita (o non riuscita) non garantisce lo stesso risultato per l'autenticazione AnyConnect perché le richieste di autenticazione LDAP AnyConnect vengono avviate da una delle interfacce instradabili FTD.

Per ulteriori informazioni sul test delle connessioni LDAP dall'FTD, consultare le sezioni Test AAA e Packet Capture nell'area Risoluzione dei problemi.



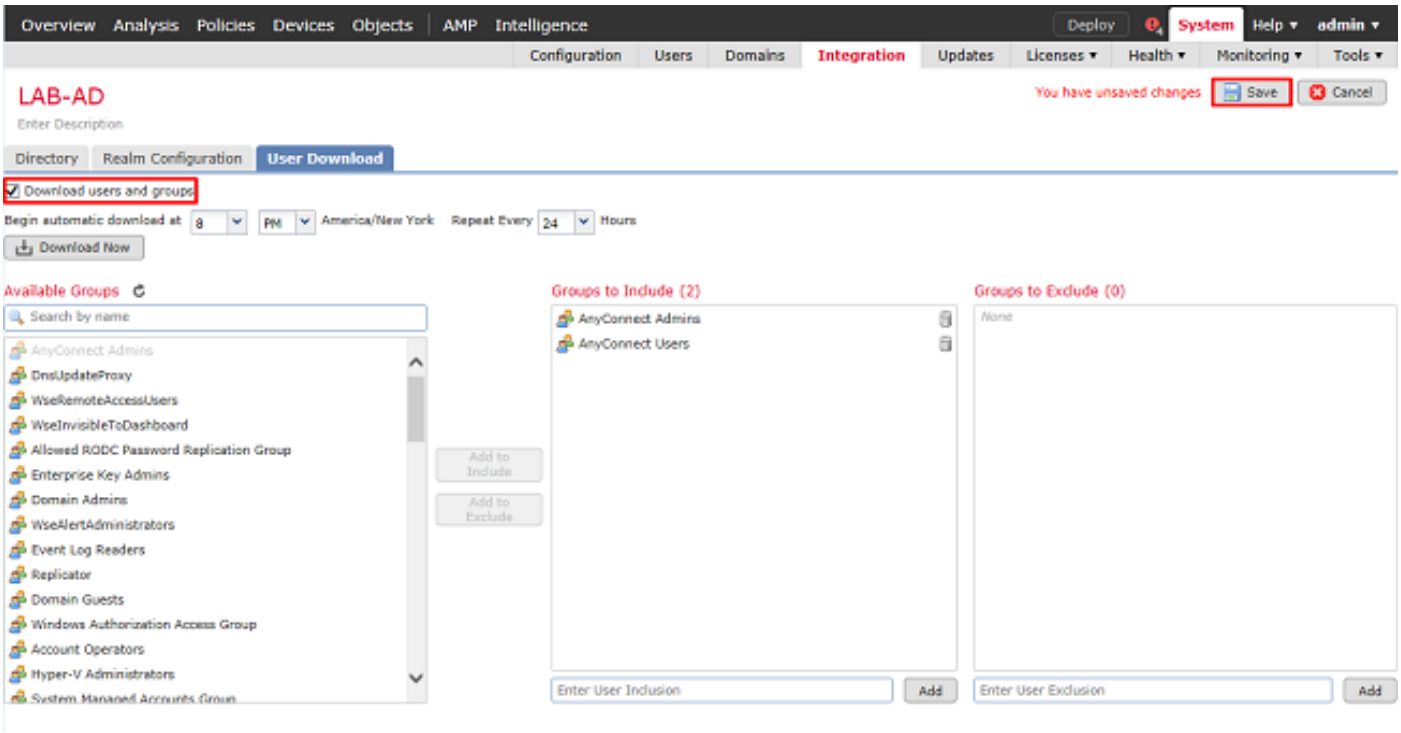
5. In Download utente, scaricare i gruppi utilizzati per l'identità dell'utente nei passaggi successivi.

Selezionare la casella Scarica utenti e gruppi e la colonna Gruppi disponibili viene popolata con i gruppi configurati in Active Directory.

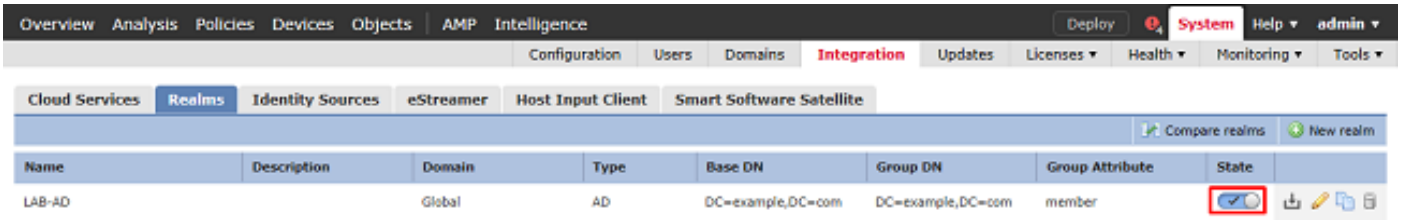
I gruppi possono essere inclusi o esclusi, tuttavia per impostazione predefinita vengono inclusi tutti i gruppi presenti nel DN gruppo.

È possibile includere o escludere anche utenti specifici. Tutti i gruppi e gli utenti inclusi sono disponibili per la selezione dell'identità utente in un secondo momento.

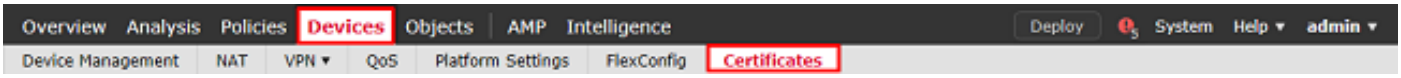
Al termine, fare clic su Salva.



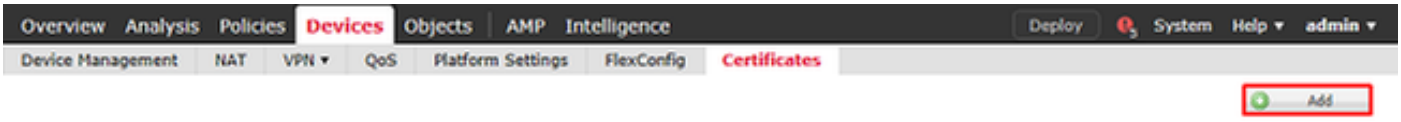
6. Abilitare il nuovo realm.



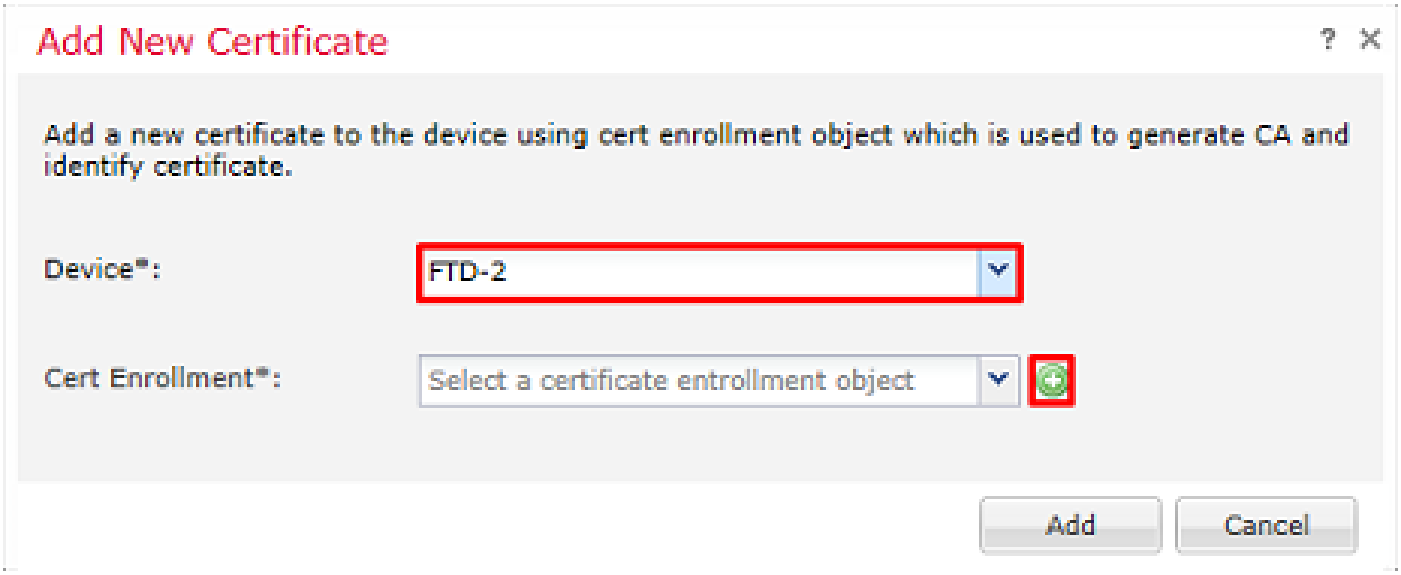
7. Se si utilizza LDAPS o STARTTLS, anche la CA radice deve essere considerata attendibile dall'FTD. A tale scopo, selezionare Dispositivi > Certificati.



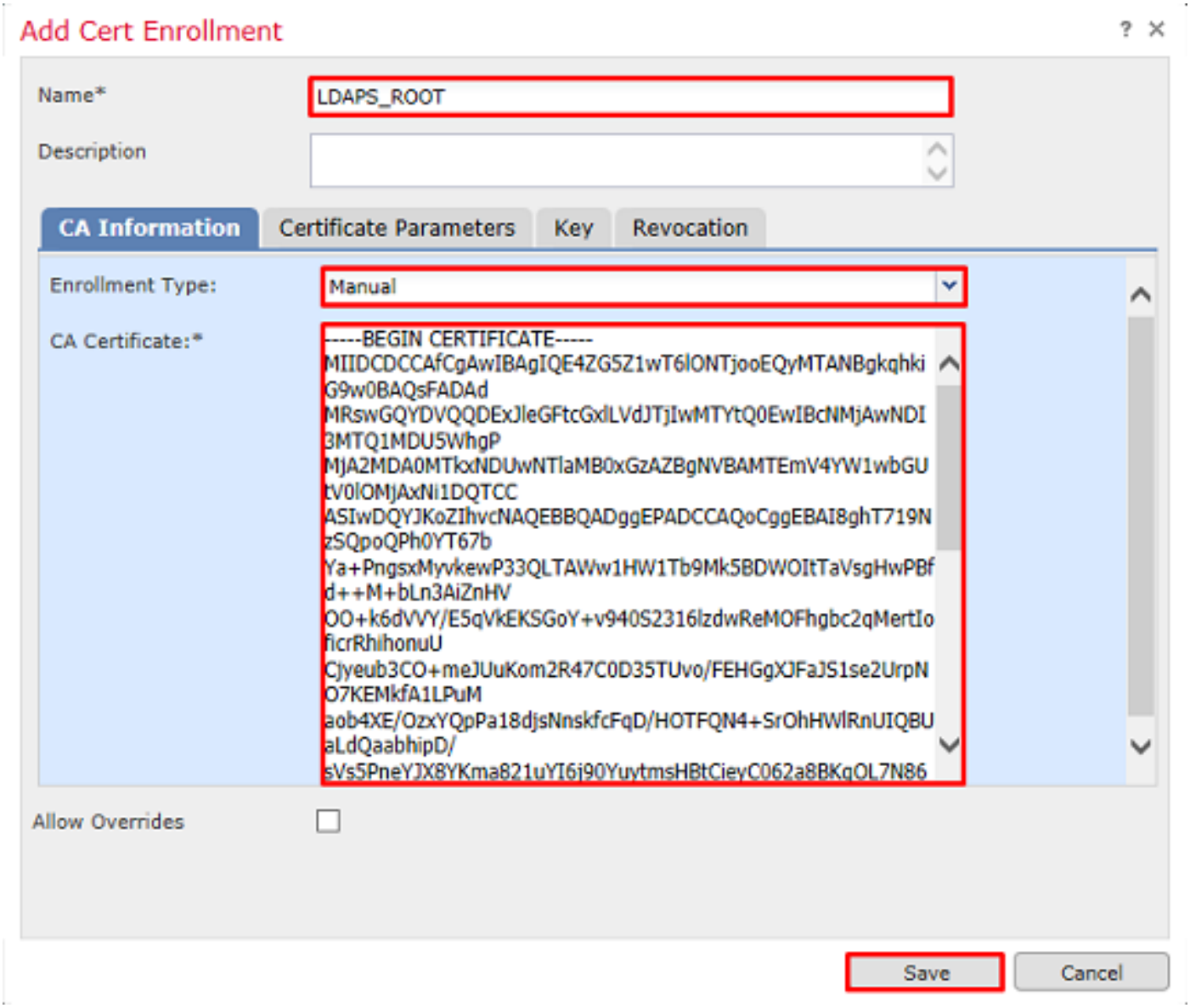
Fare clic su Add (Aggiungi) in alto a destra.



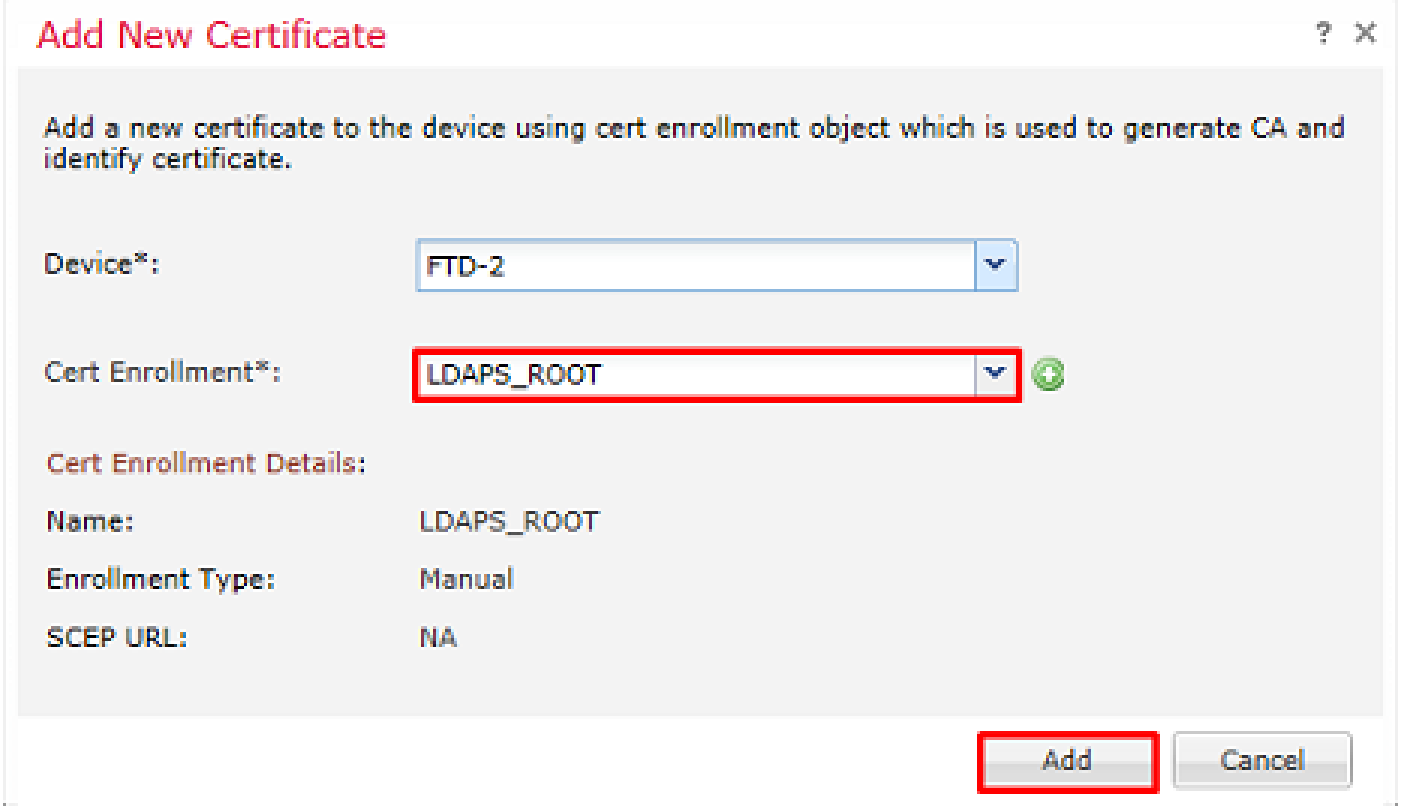
Selezionare l'FTD, la configurazione LDAP viene aggiunta a, quindi fare clic sul simbolo + (più).



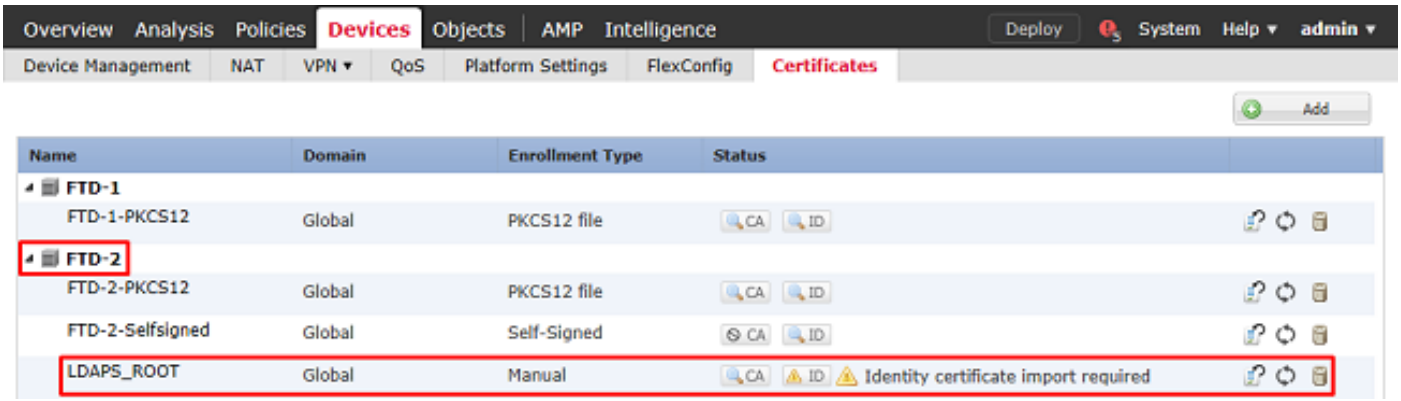
Assegnare un nome al trust point, quindi scegliere Iscrizione manuale dal menu a discesa Tipo di iscrizione. Incollare qui il certificato CA radice PEM, quindi fare clic su Salva.



Verificare che il trust point creato sia selezionato, quindi fare clic su Aggiungi.



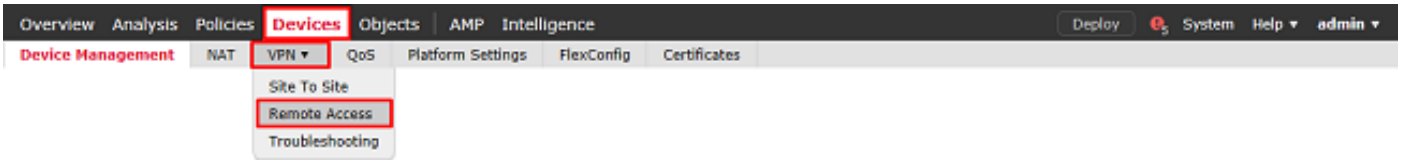
Il nuovo trust point viene visualizzato sotto FTD. Sebbene indichi che l'importazione del certificato di identità è obbligatoria, non è richiesto per l'FTD per autenticare il certificato SSL inviato dal server LDAPS. Questo messaggio può essere ignorato.



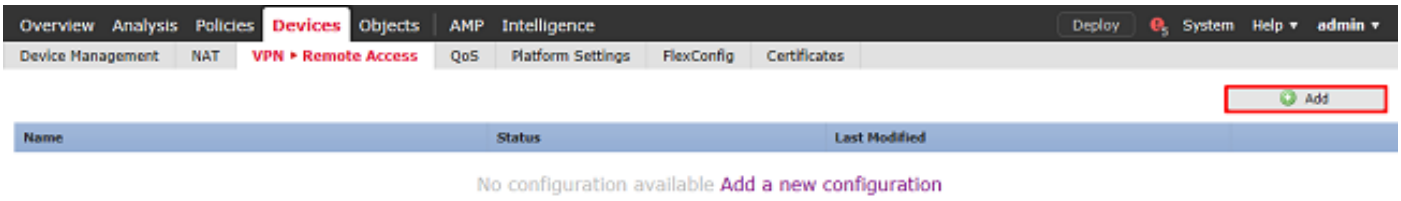
Configurazione di AnyConnect per l'autenticazione AD

1. In questa procedura si presuppone che non sia già stato creato alcun criterio VPN di accesso remoto. Se ne è stato creato uno, fare clic sul pulsante Modifica relativo al criterio e andare al passaggio 3.

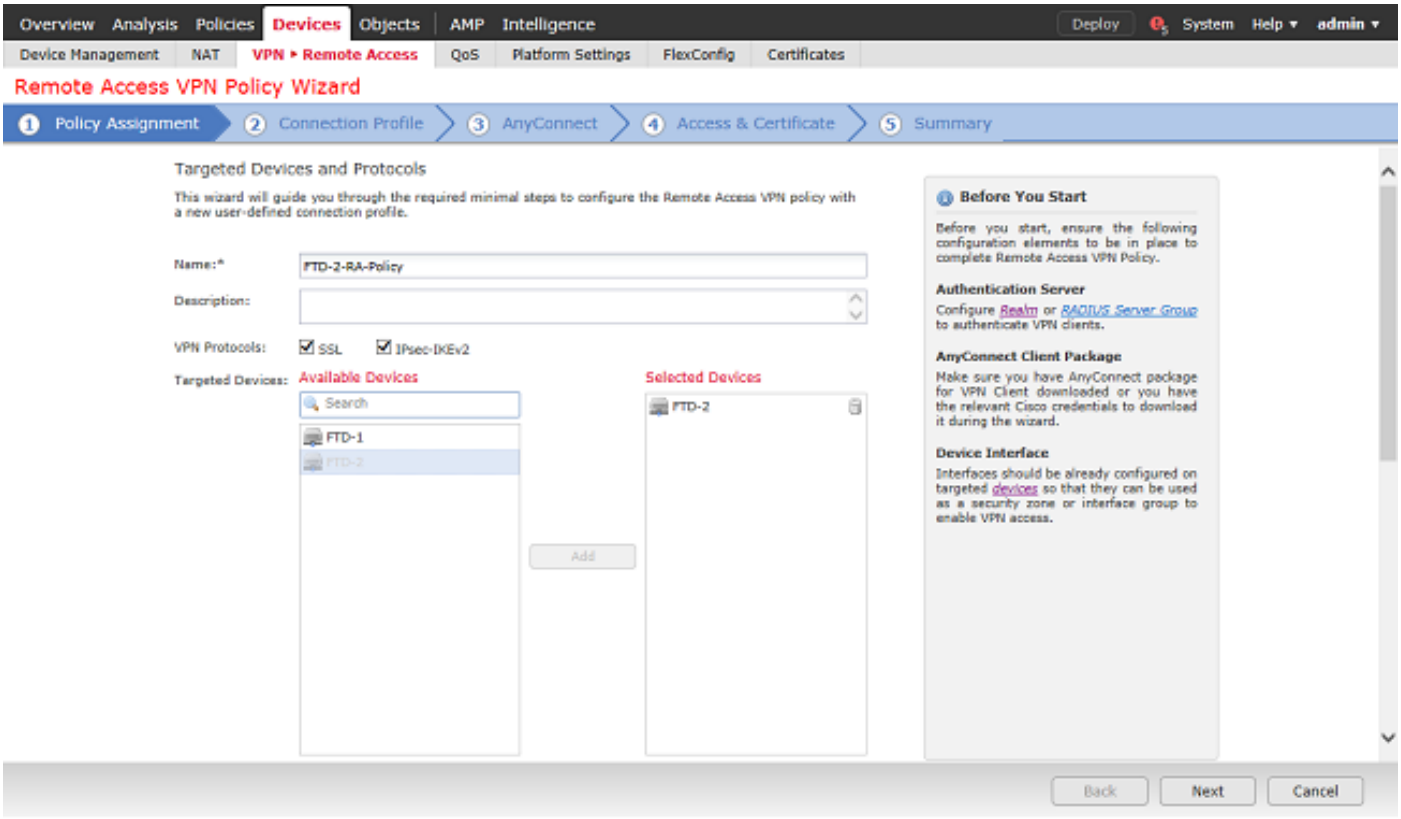
Selezionare Dispositivi > VPN > Accesso remoto.



Fare clic su Aggiungi per creare un nuovo criterio VPN di Accesso remoto



2. Completare la Creazione guidata criteri VPN di accesso remoto. In Assegnazione criterio specificare un nome per il criterio e i dispositivi a cui viene applicato.

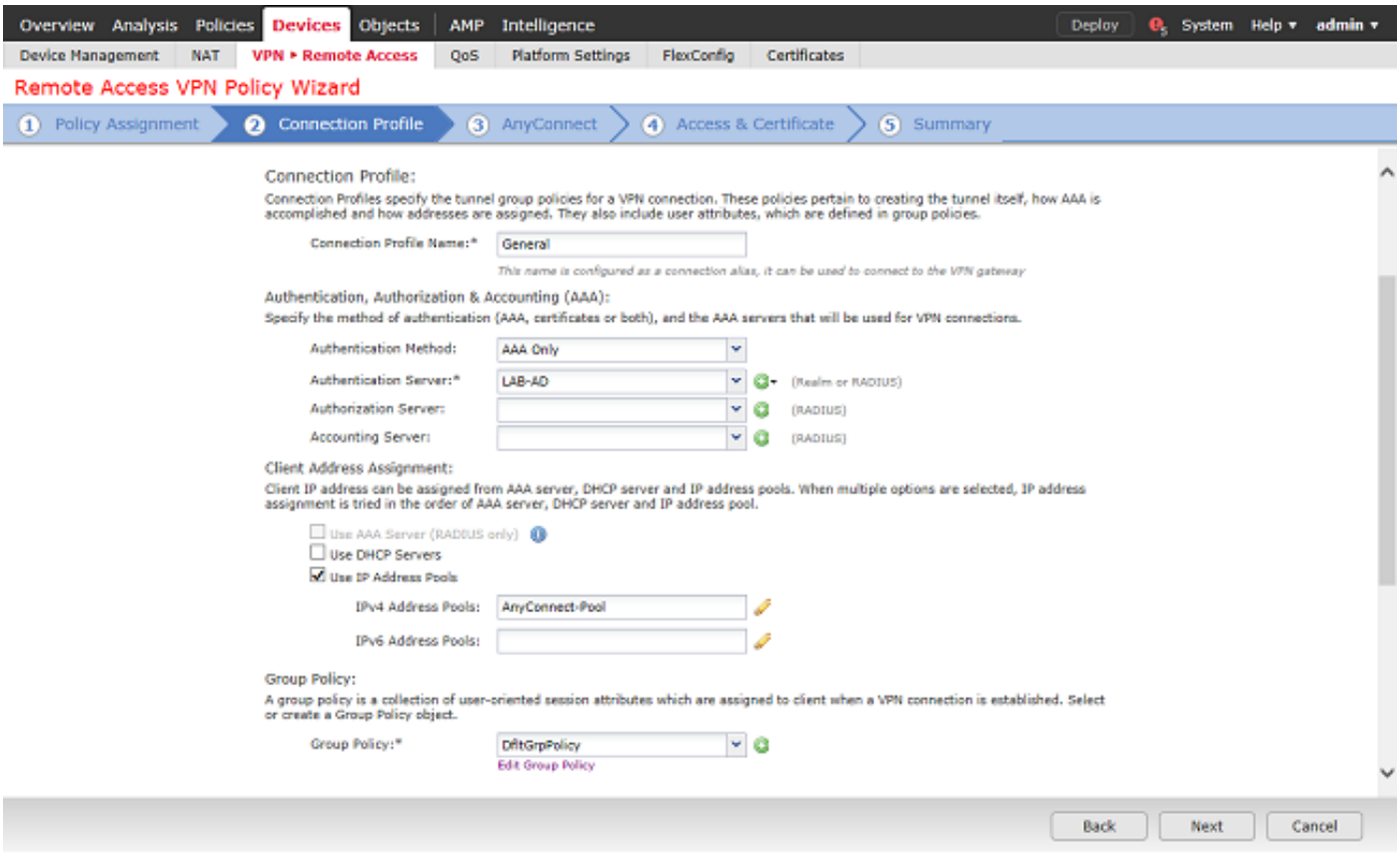


In Profilo di connessione, specificare il nome del Profilo di connessione che viene utilizzato anche come alias di gruppo visualizzato agli utenti AnyConnect quando si connettono.

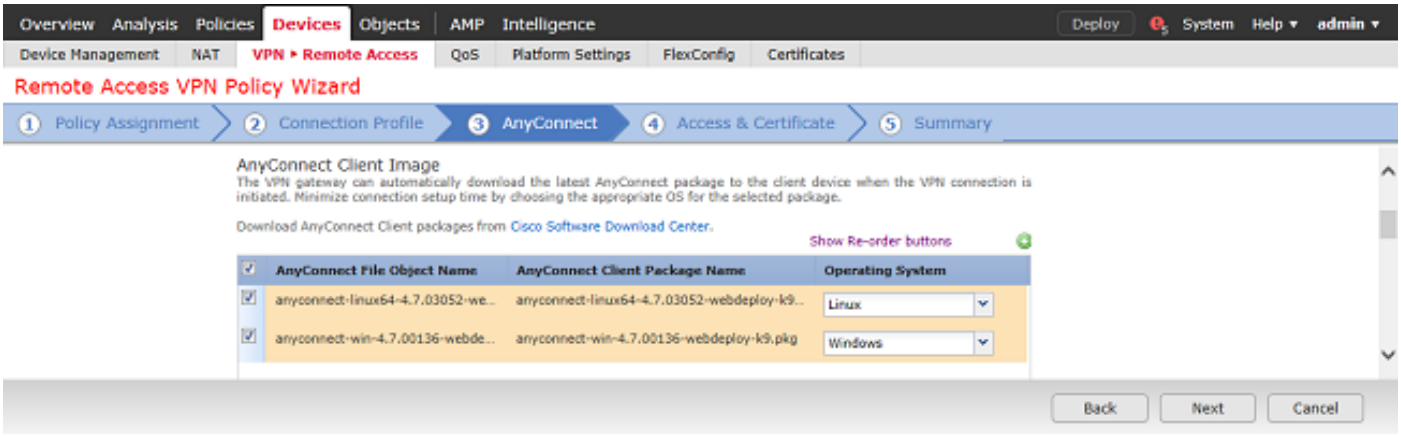
Specificare l'area di autenticazione creata in precedenza in Server di autenticazione.

Specificare il metodo con cui assegnare gli indirizzi IP ai client AnyConnect.

Specificare i Criteri di gruppo predefiniti utilizzati per il profilo di connessione.



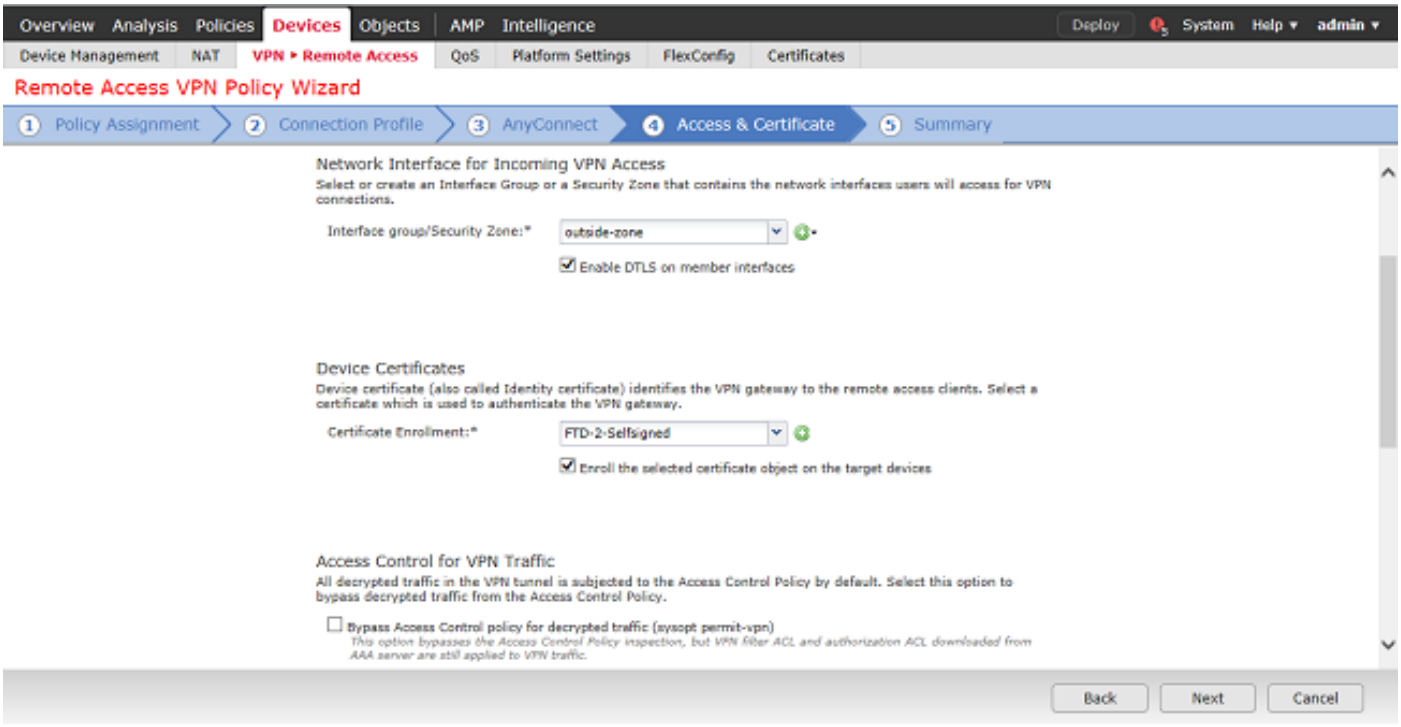
In AnyConnect, caricare e specificare i pacchetti AnyConnect che verranno utilizzati.



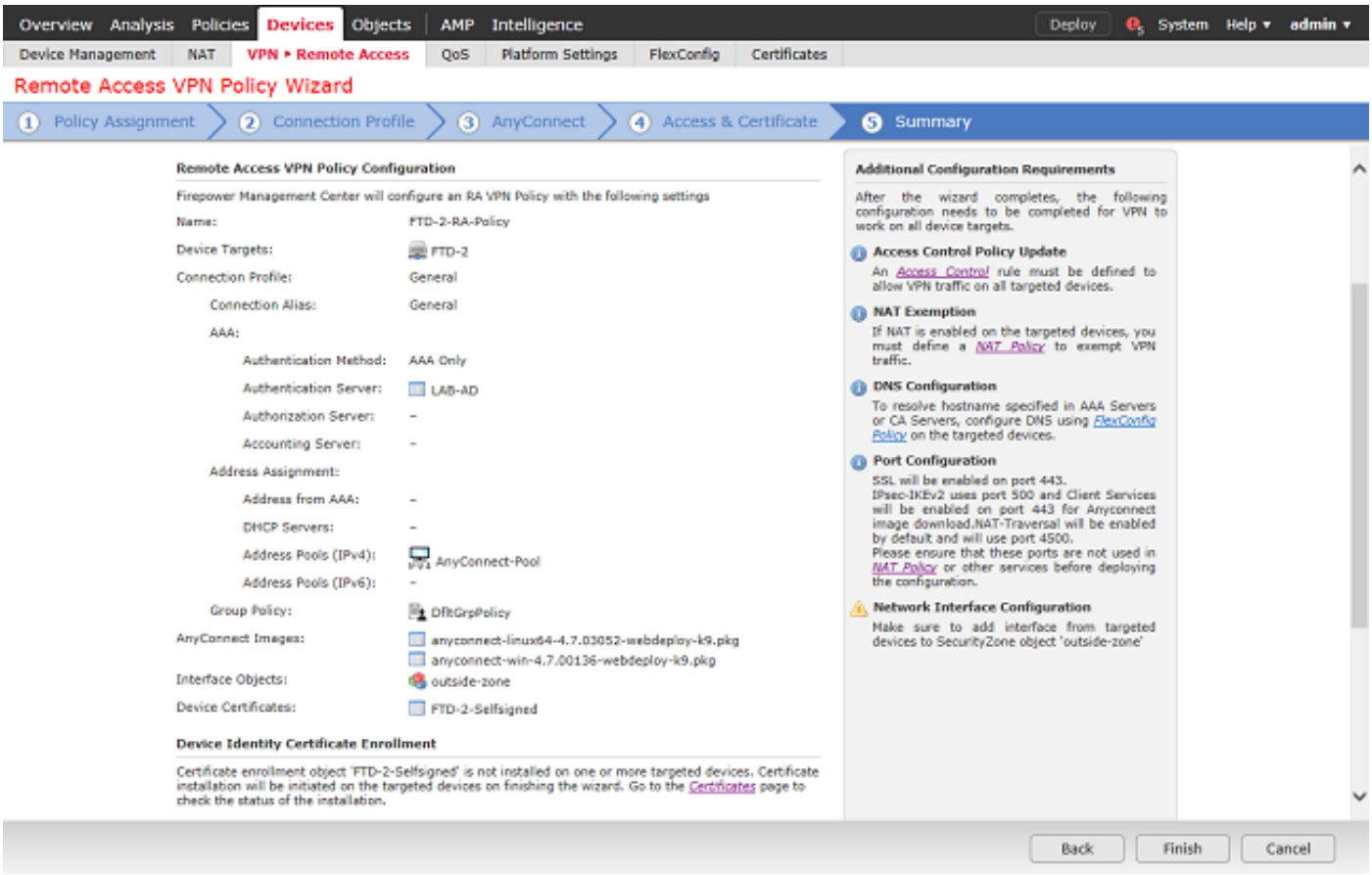
In Accesso e certificato, specificare l'interfaccia a cui accedono gli utenti AnyConnect per AnyConnect.

Creare e/o specificare il certificato utilizzato dall'FTD durante l'handshake SSL.

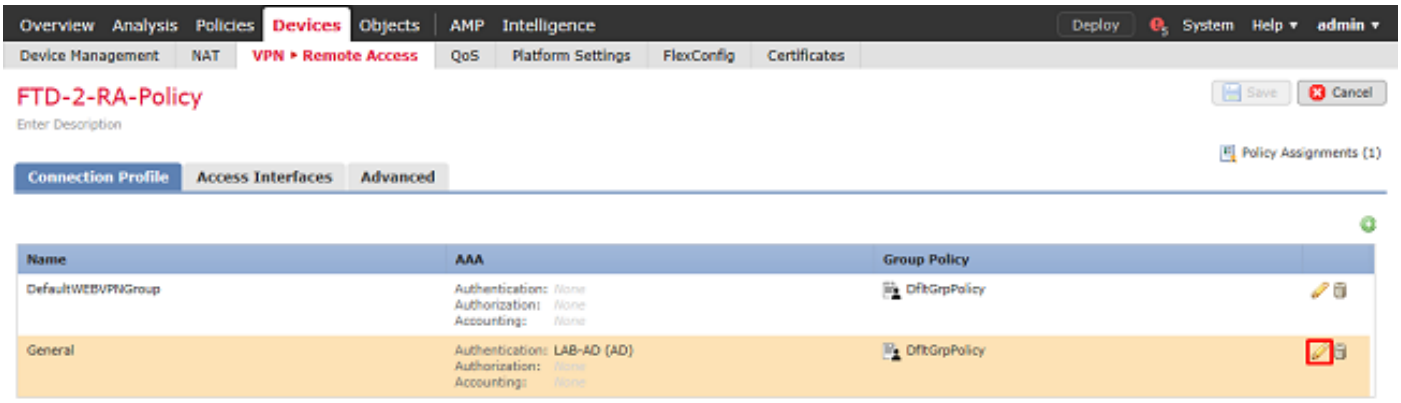
Verificare che la casella di controllo Ignora i criteri di controllo di accesso per il traffico decrittografato (sysopt allow-vpn) sia deselezionata in modo che l'identità utente creata successivamente diventi effettiva per le connessioni RAVPN.



In Riepilogo, rivedere la configurazione e fare clic su Fine.



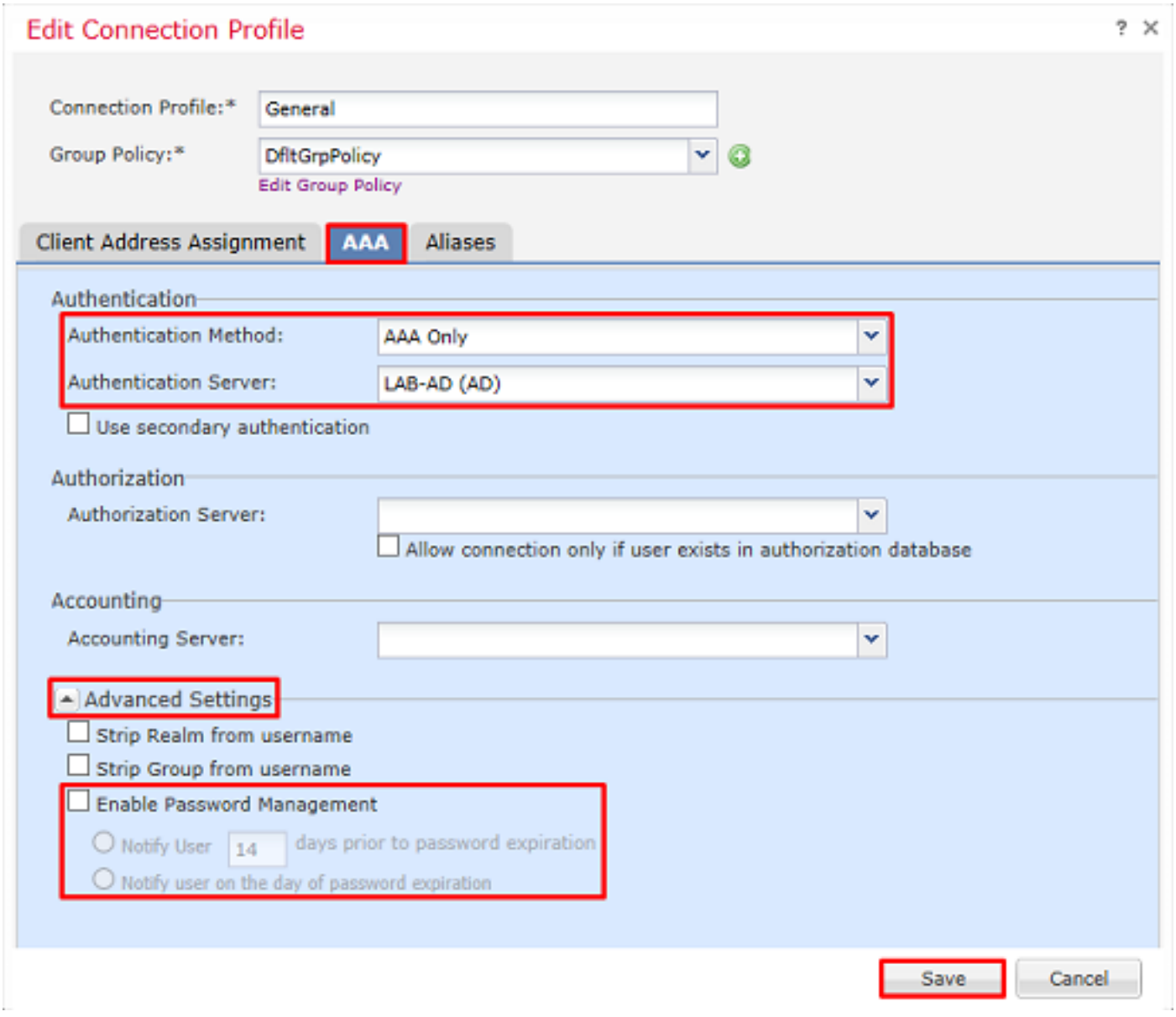
3. Sotto il criterio VPN > Accesso remoto, fare clic su Modifica icona (matita) per il profilo di connessione appropriato.



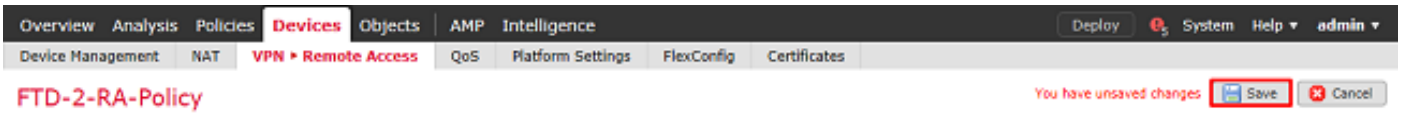
Verificare che il server di autenticazione sia impostato sul realm creato in precedenza.

In Impostazioni avanzate è possibile selezionare Attiva gestione password per consentire agli utenti di modificare la password prima o quando scade.

Tuttavia, questa impostazione richiede che il realm utilizzi LDAPS. Se sono state apportate modifiche, fare clic su Salva.

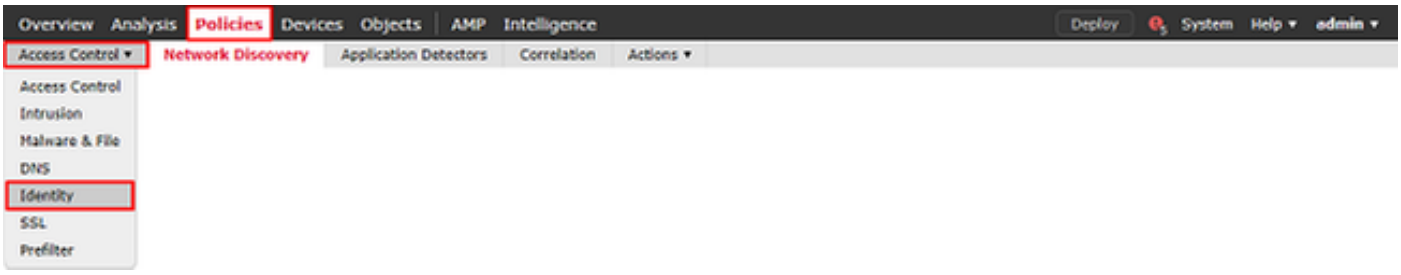


Al termine, fare clic su Salva.



Abilita criteri di identità e configura criteri di sicurezza per l'identità utente

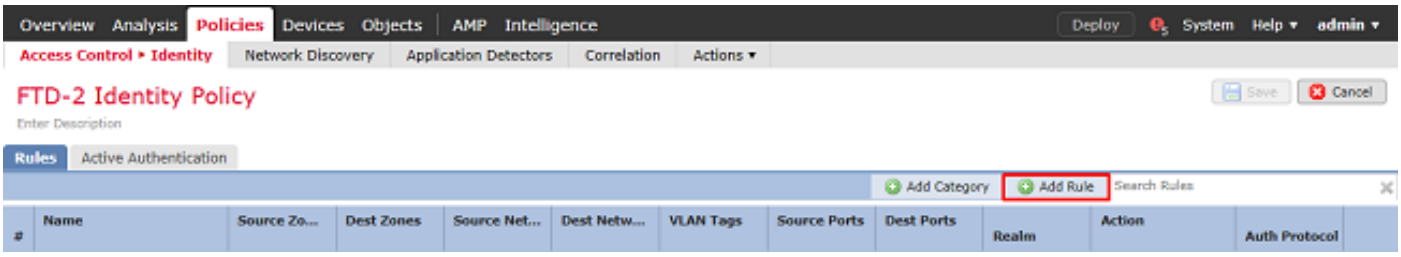
1. Passare a Criteri > Controllo accesso > Identità.



Crea un nuovo criterio di identità.

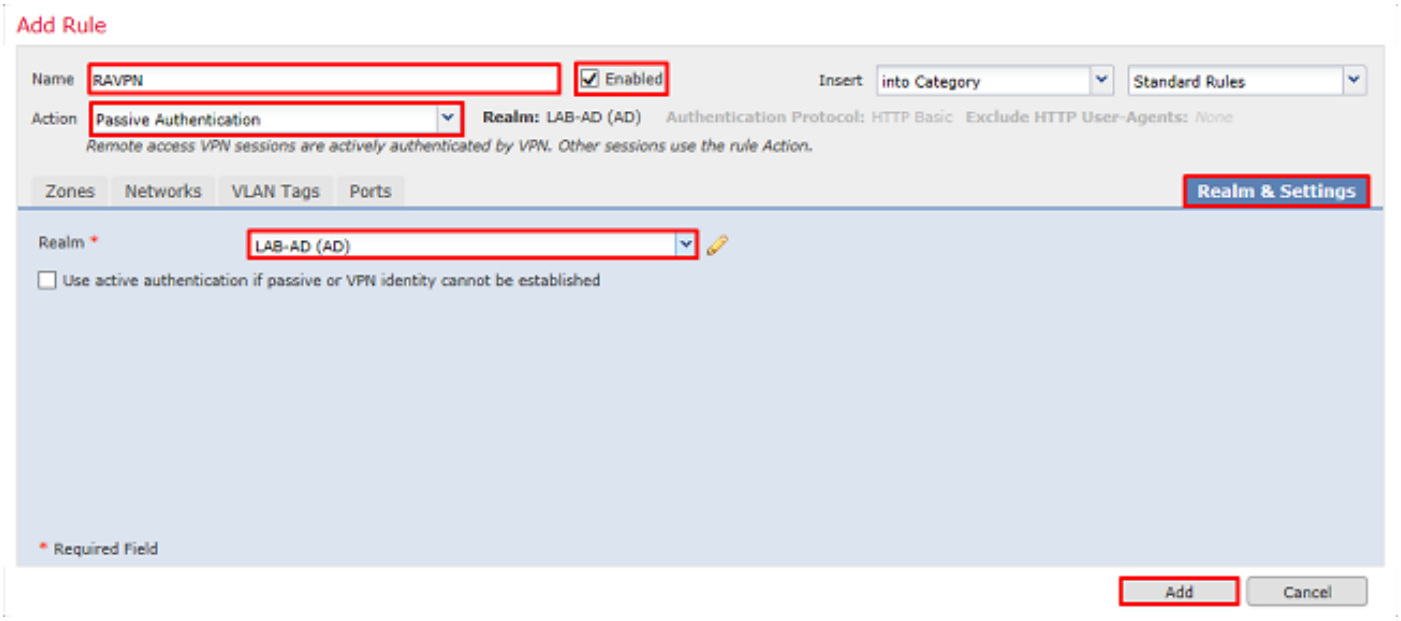
Specificare un nome per il nuovo criterio di identità.

2. Fare clic su Aggiungi regola.

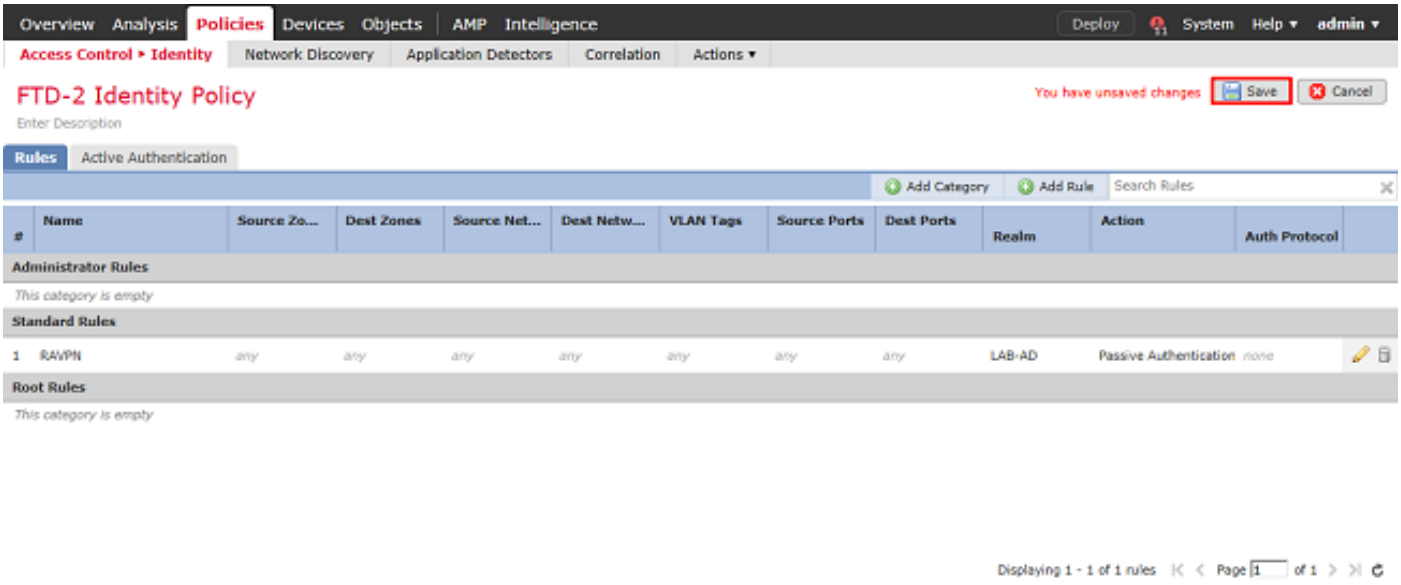


3. Specificare un nome per la nuova regola. Verificare che sia abilitato e che l'azione sia impostata su Autenticazione passiva.

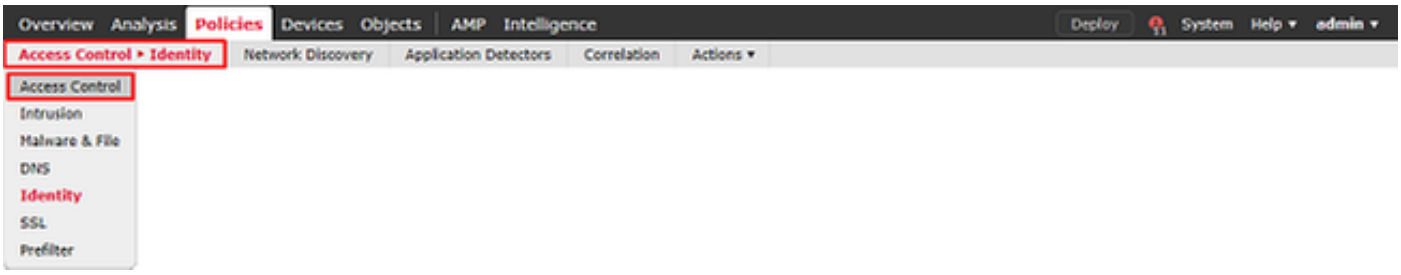
Fare clic sulla scheda Realm & Settings e selezionare il realm creato in precedenza. Al termine, fare clic su Add (Aggiungi).



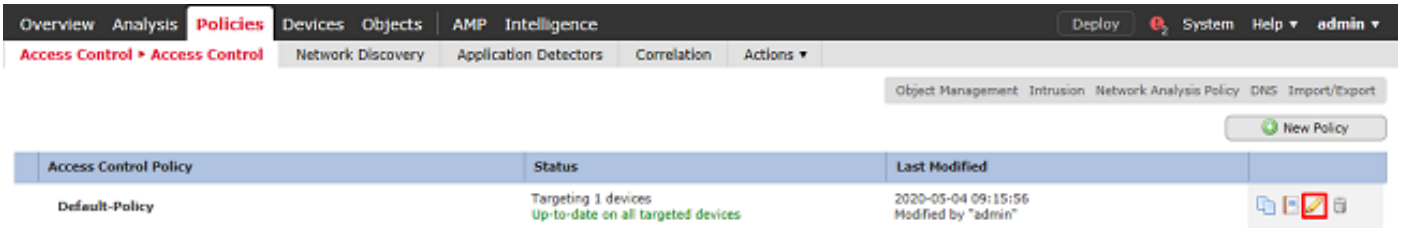
4. Fare clic su Salva.



5. Passare a Policy > Controllo accesso > Controllo accesso.



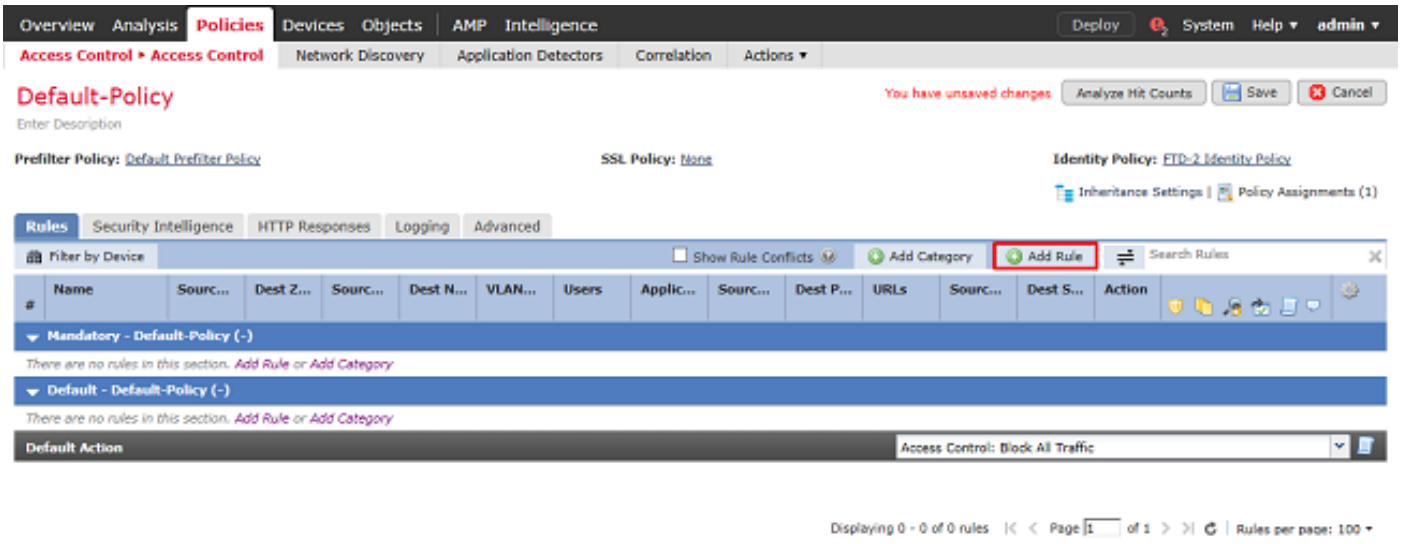
6. Modificare la Policy di controllo dell'accesso in cui è configurato l'FTD.



7. Fare clic sul valore accanto a Criterio di identità.

Selezionare il criterio di identità creato in precedenza, quindi fare clic su OK.

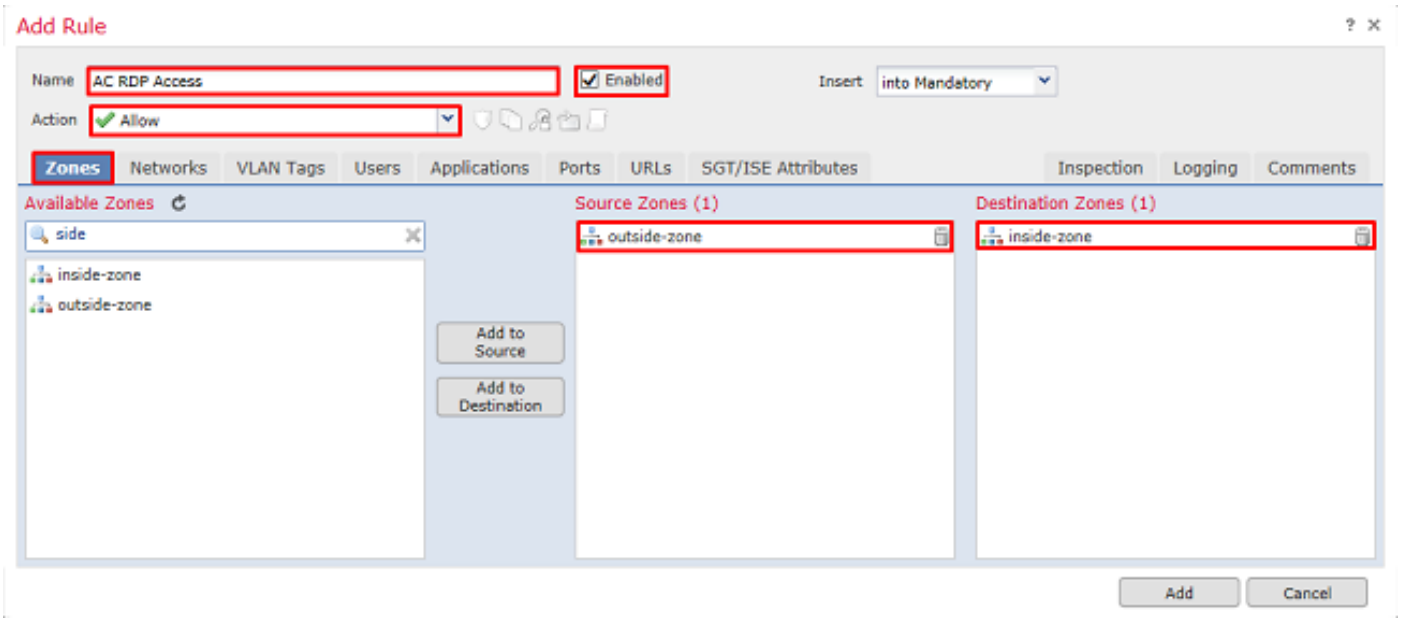
8. Fare clic su Aggiungi regola per creare una nuova regola ACP. Questa procedura consente di creare una regola per consentire all'utente del gruppo AnyConnect Admins di connettersi ai dispositivi della rete interna utilizzando RDP.



Specificare un nome per la regola. Verificare che la regola sia Abilitata e che disponga dell'azione appropriata.

Nella scheda Zone, specificare le zone appropriate per il traffico di interesse.

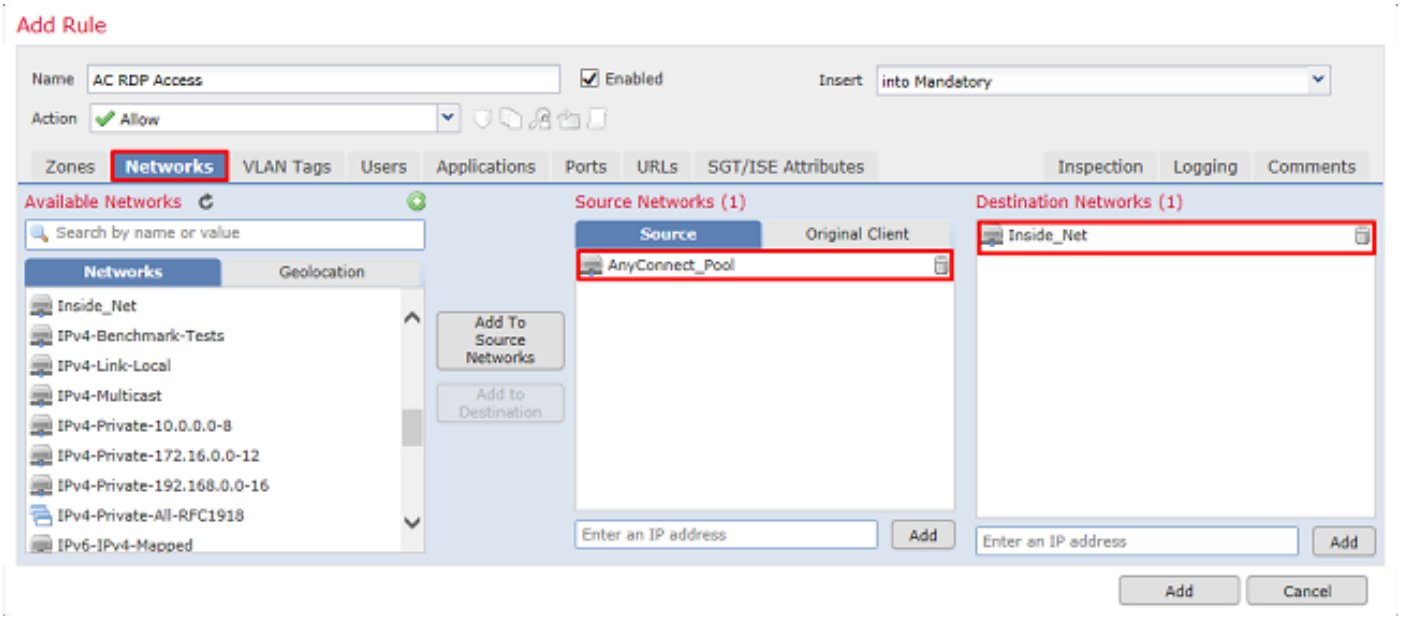
Il traffico RDP avviato dagli utenti arriva all'FTD proveniente dall'interfaccia della zona esterna ed esce dalla zona interna.



In Reti definire le reti di origine e di destinazione.

L'oggetto AnyConnect_Pool include gli indirizzi IP assegnati ai client AnyConnect.

L'oggetto Inside_Net include la subnet della rete interna.

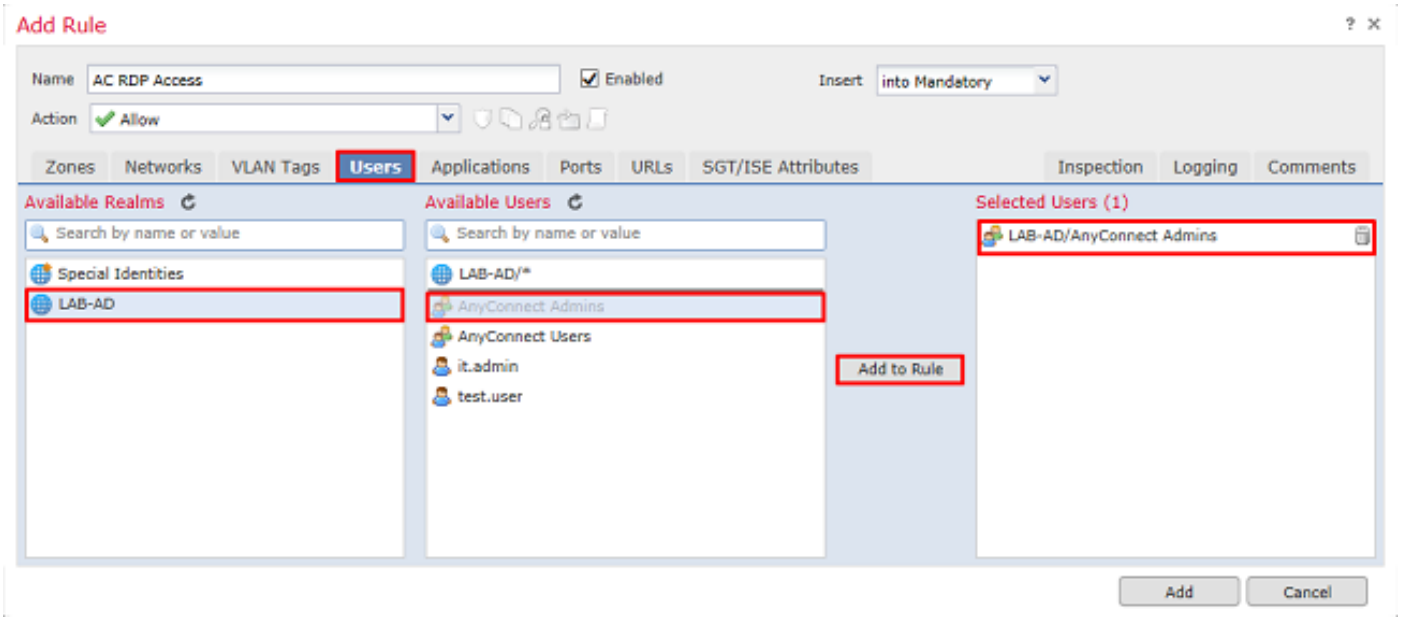


In Utenti, fare clic sul realm creato in precedenza in Realm disponibili, fare clic sul gruppo/utente appropriato in Utenti disponibili, quindi fare clic su Aggiungi a regola.

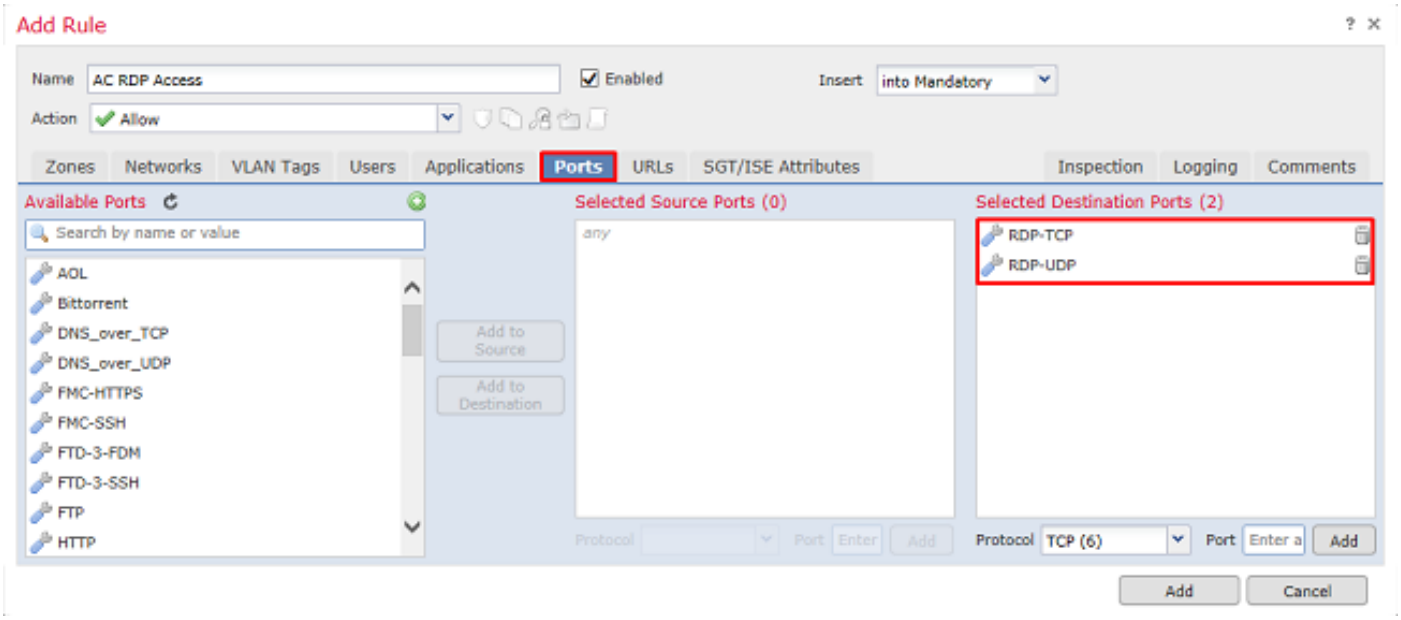
Se non sono disponibili utenti o gruppi nella sezione Utenti disponibili, verificare che FMC abbia scaricato Utenti e gruppi nella sezione del realm e che i Gruppi/Utenti appropriati siano inclusi.

Gli utenti/gruppi specificati qui vengono controllati dal punto di vista dell'origine.

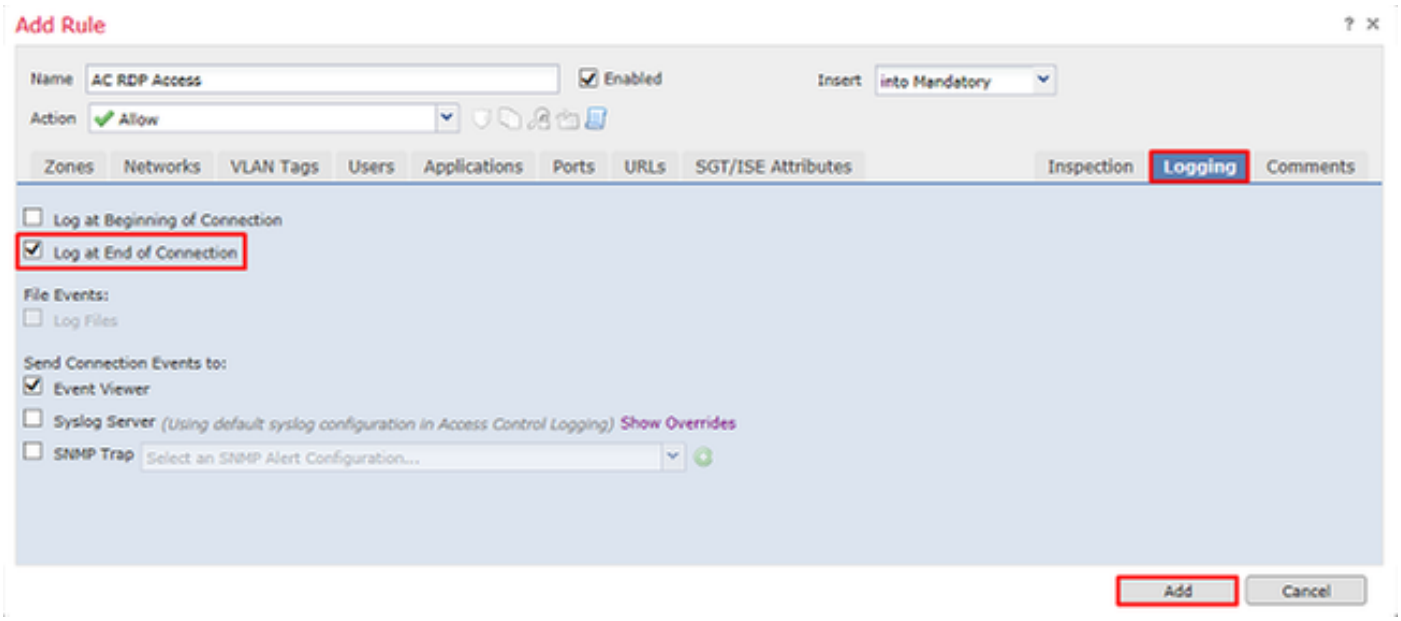
Ad esempio, in base a quanto finora definito in questa regola, l'FTD valuta che il traffico abbia origine dalla zona esterna e sia destinato alla zona interna, provenga dalla rete nell'oggetto AnyConnect_Pools e sia destinato alla rete nell'oggetto Inside_Net e provenga da un utente del gruppo AnyConnect Admins.



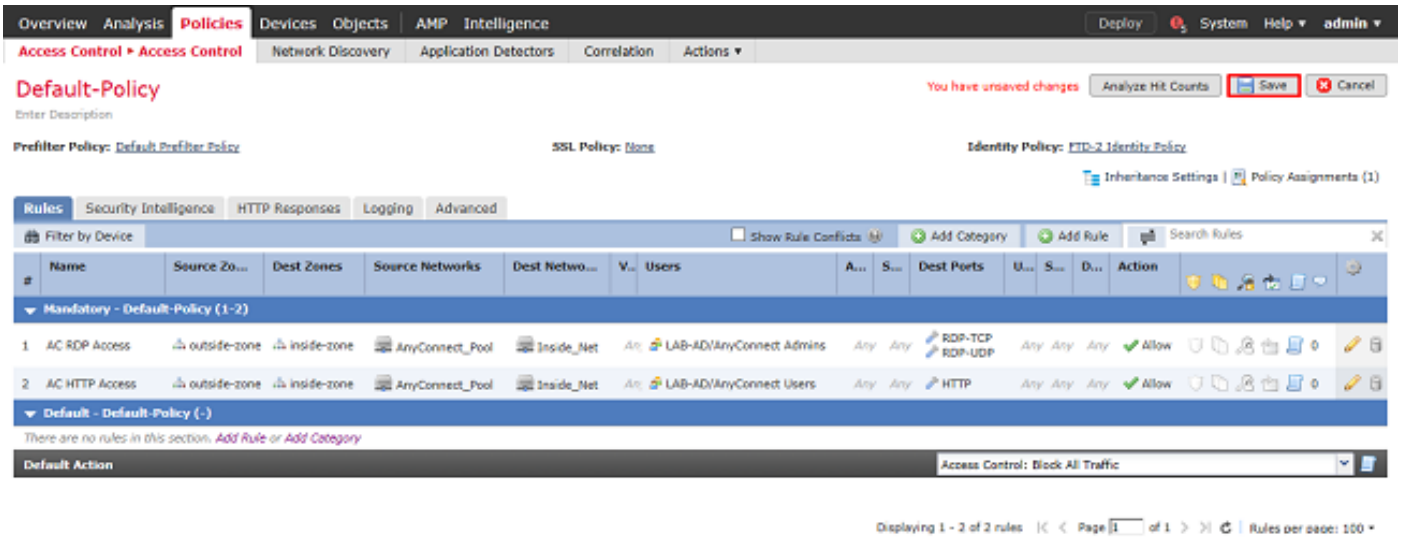
In Porte (Ports), sono stati creati e aggiunti oggetti RDP personalizzati per consentire la porta TCP e UDP 3389. Si noti che è possibile aggiungere RDP nella sezione Applicazioni, ma per semplicità, vengono controllate solo le porte.



Infine, assicurarsi che in Registrazione, Registra alla fine della connessione sia selezionato per ulteriori verifiche in seguito. Al termine, fare clic su Add (Aggiungi).



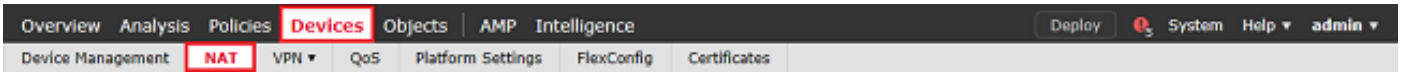
9. Viene creata una regola aggiuntiva per l'accesso HTTP per consentire agli utenti del gruppo AnyConnect User di accedere al sito Web IIS di Windows Server. Fare clic su Save (Salva).



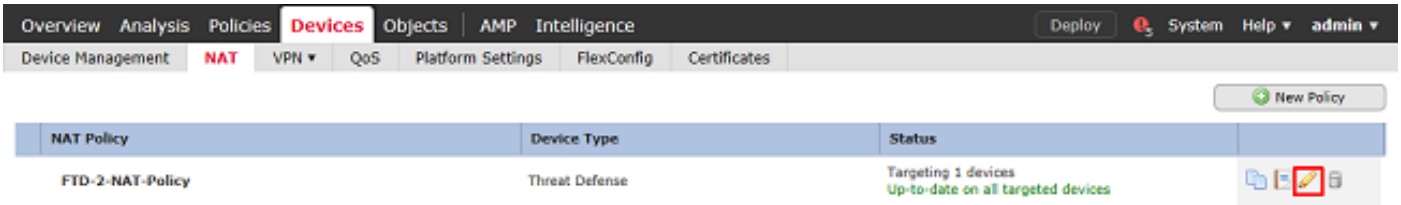
Configura esenzione NAT

Se ci sono regole NAT che influenzano il traffico AnyConnect, ad esempio le regole Internet PAT, è importante configurare le regole di esenzione NAT in modo che il traffico AnyConnect non venga influenzato da NAT.

1. Passare a Dispositivi > NAT.

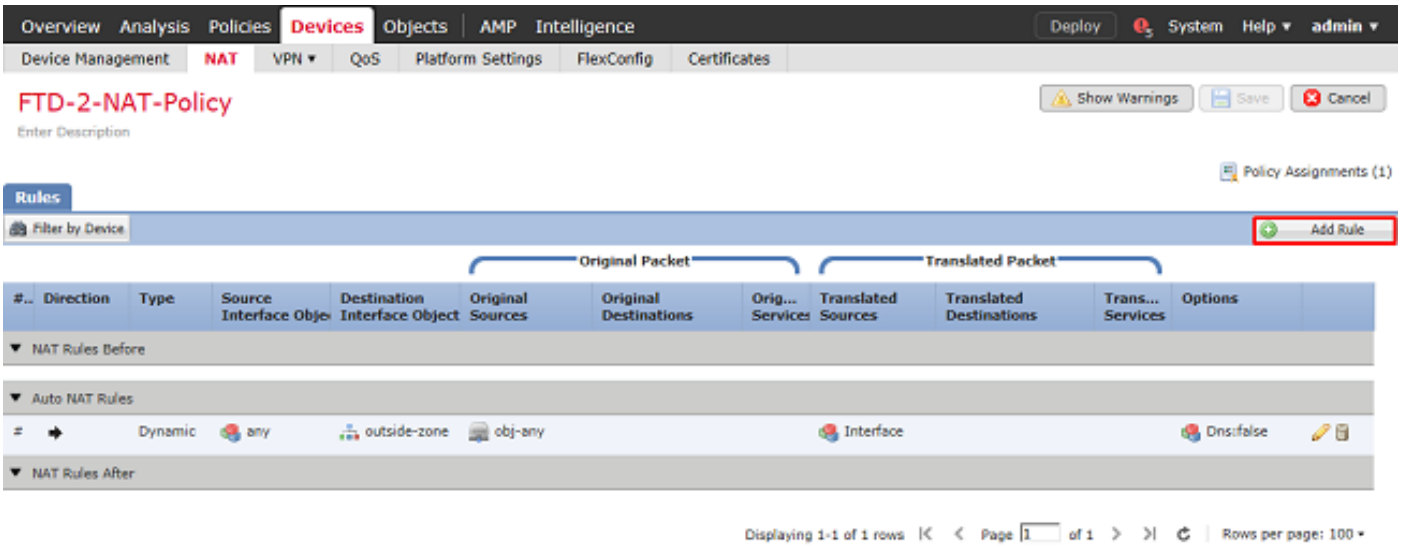


Selezionare il criterio NAT applicato all'FTD.



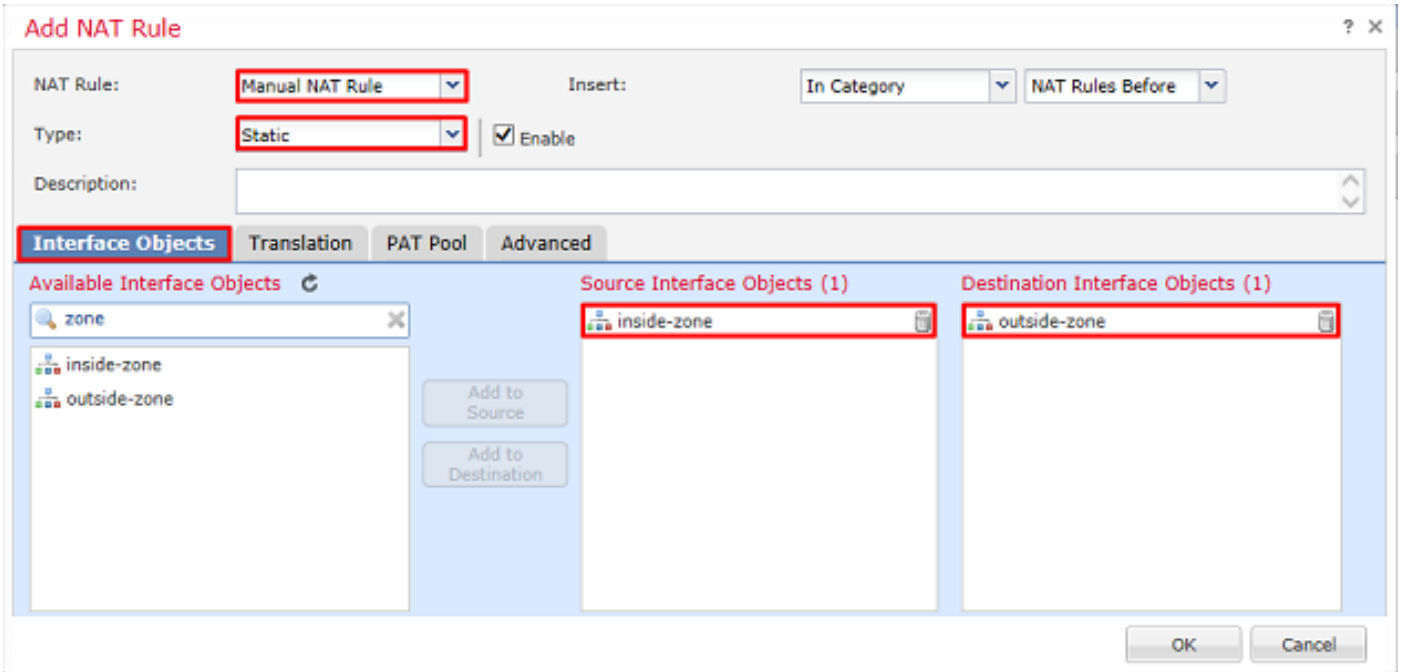
2. Nella presente policy NAT, la porta termina con una parte dinamica che influenza tutto il traffico (incluso il traffico AnyConnect) e porta l'interfaccia esterna all'interfaccia esterna.

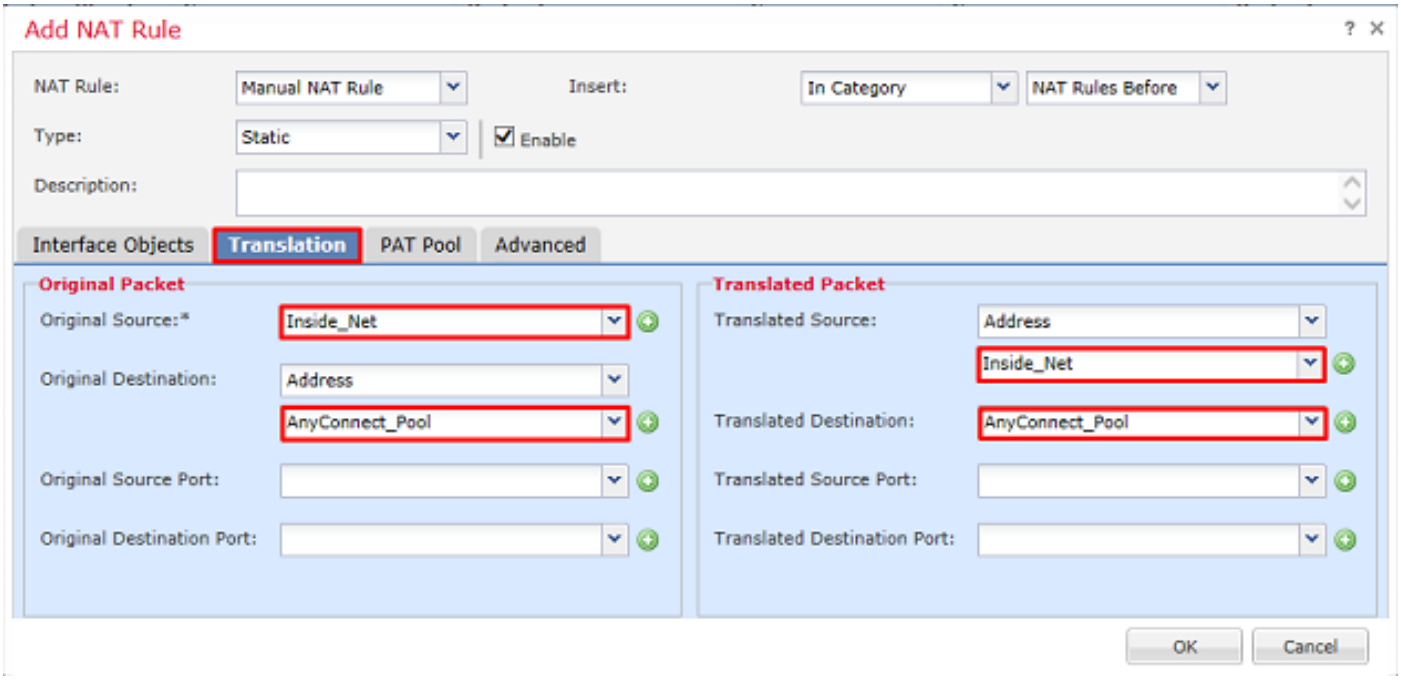
Per evitare che il traffico AnyConnect venga influenzato da NAT, fare clic su Add Rule.



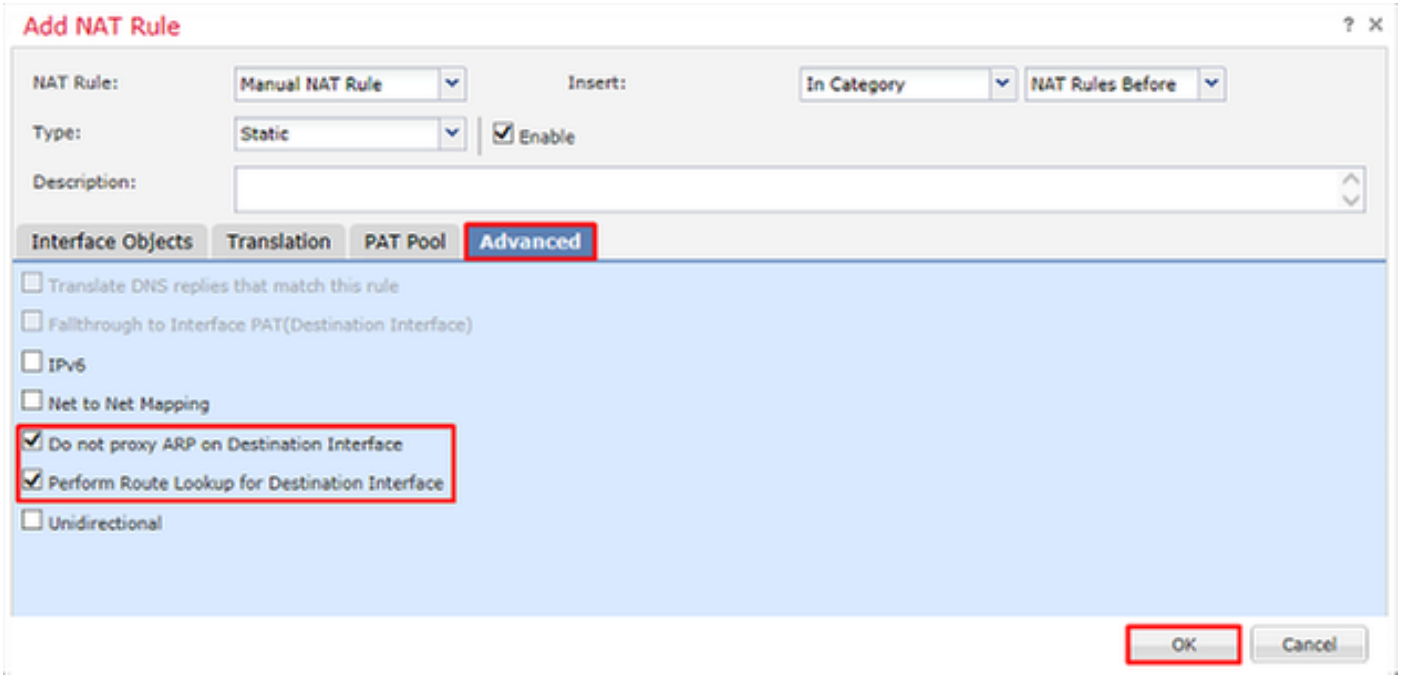
3. Configurare una regola di esenzione NAT, verificare che si tratti di una regola NAT manuale con il tipo Static. Questa è una regola NAT bidirezionale che si applica al traffico AnyConnect.

Con queste impostazioni, quando il FTD rileva il traffico proveniente da Inside_Net e destinato all'indirizzo IP di AnyConnect (definito da AnyConnect_Pool), l'origine viene convertita allo stesso valore (Inside_Net) e la destinazione viene convertita allo stesso valore (AnyConnect_Pool) quando il traffico entra nella zona_interna ed esce dalla zona_esterna. In questo modo si ignora il NAT quando vengono soddisfatte queste condizioni.

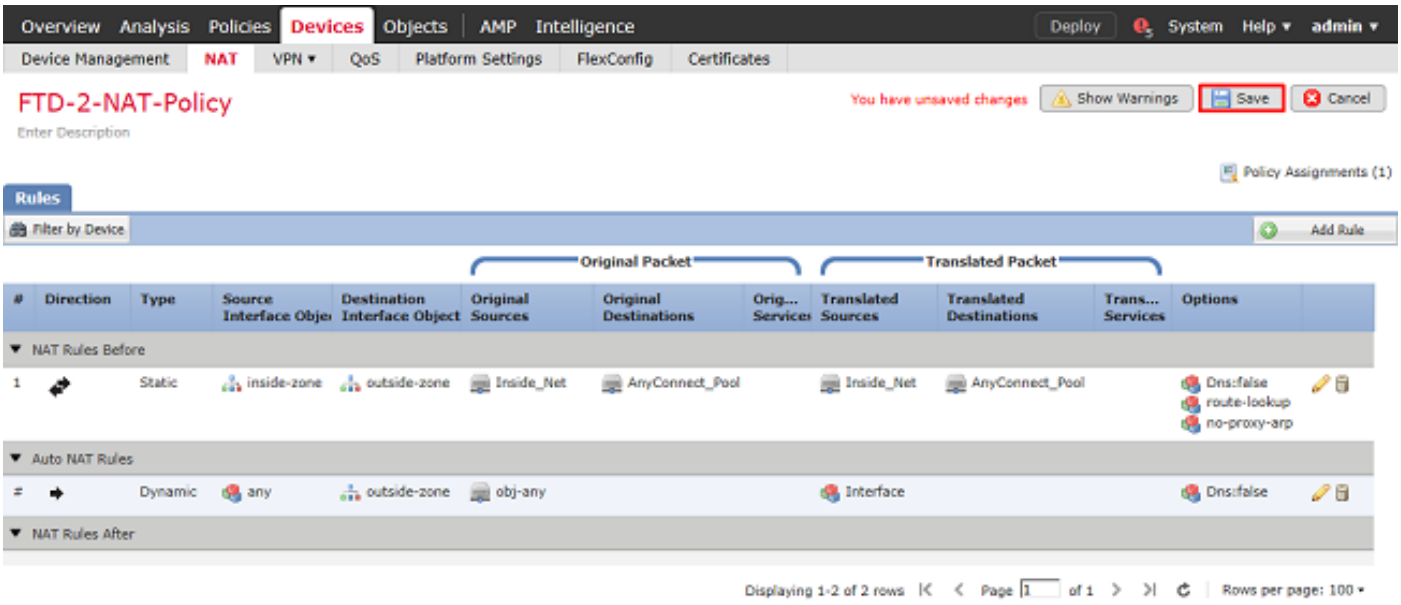




Inoltre, l'FTD è impostato per eseguire una ricerca route su questo traffico e non su ARP proxy. Al termine, fare clic su OK.

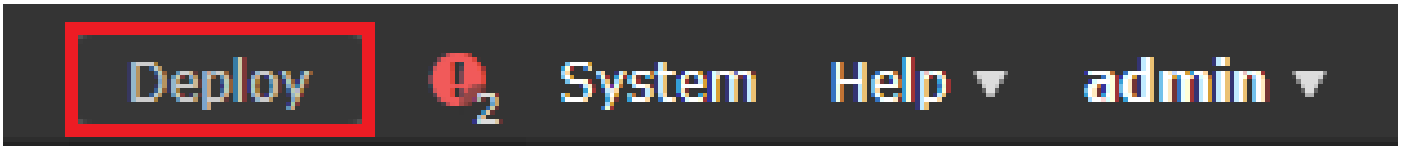


4. Fare clic su Salva.

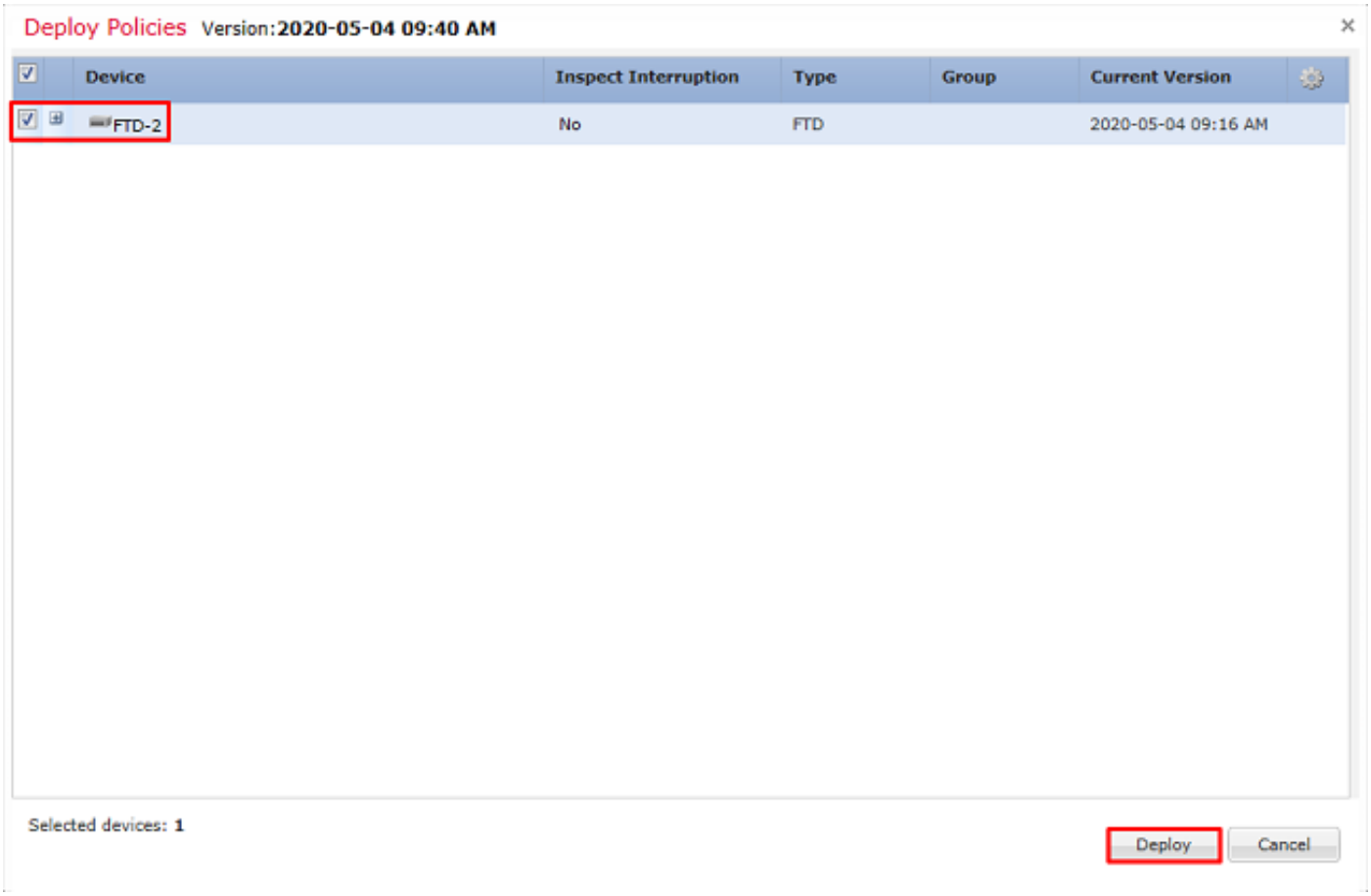


Implementazione

1. Al termine della configurazione, fare clic su Distribuisci.



2. Fare clic sulla casella di controllo accanto all'FTD a cui viene applicata la configurazione e quindi fare clic su Distribuisci.



Verifica

Configurazione finale

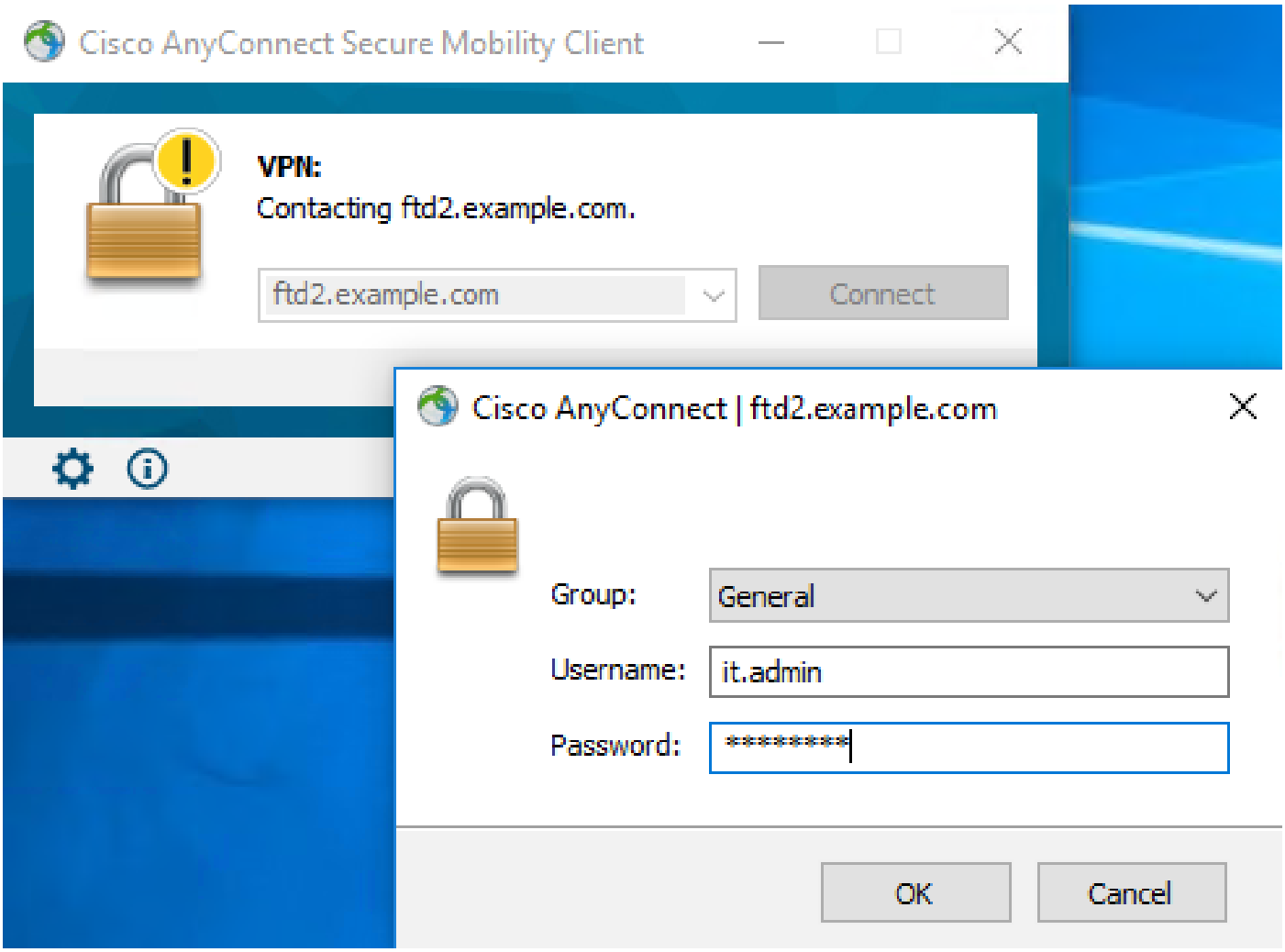
Configurazione AAA

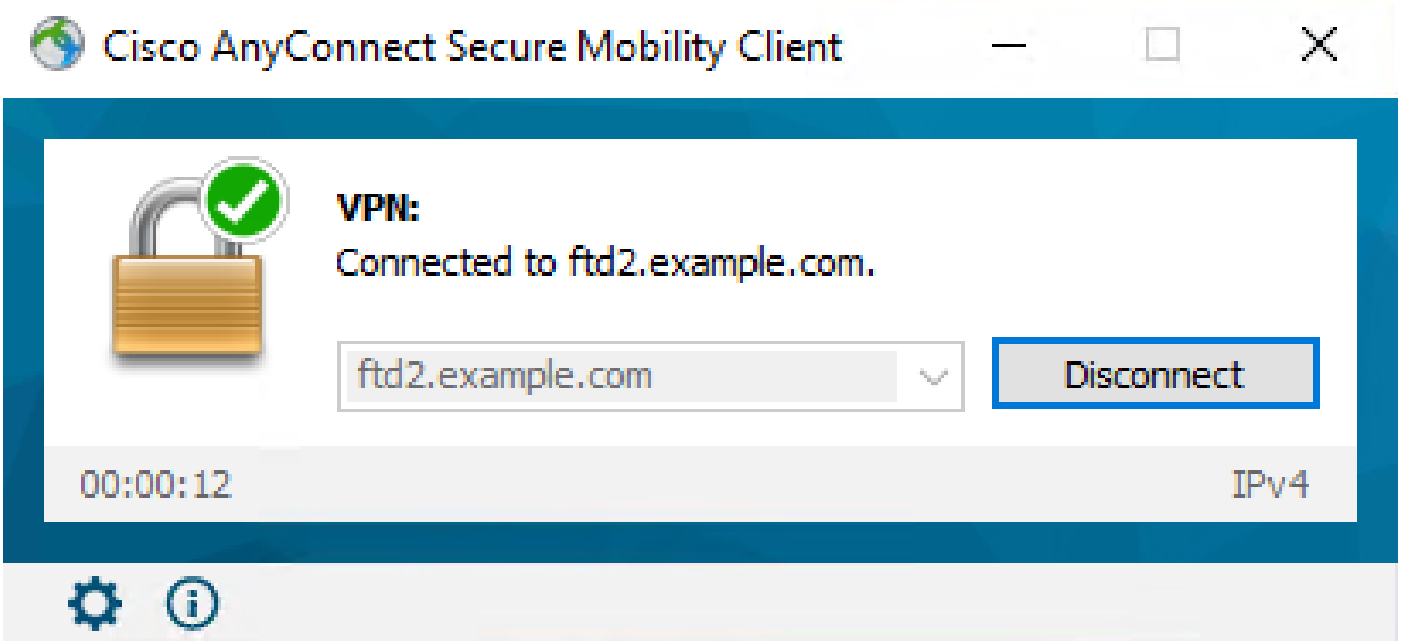
```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 max-failed-attempts 4
 realm-id 5
aaa-server LAB-AD host win2016.example.com
 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-group-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-naming-attribute samaccountname
 ldap-login-password *****
 ldap-login-dn ftd.admin@example.com
 server-type microsoft
```

Configurazione AnyConnect

```
> show running-config webvpn
webvpn
 enable Outside
 anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
 anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
 anyconnect profiles Lab disk0:/csm/lab.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  no disable
 error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
 address-pool AnyConnect-Pool
 authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
 group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Lab
 user-authentication-idle-timeout none
 webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable

> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

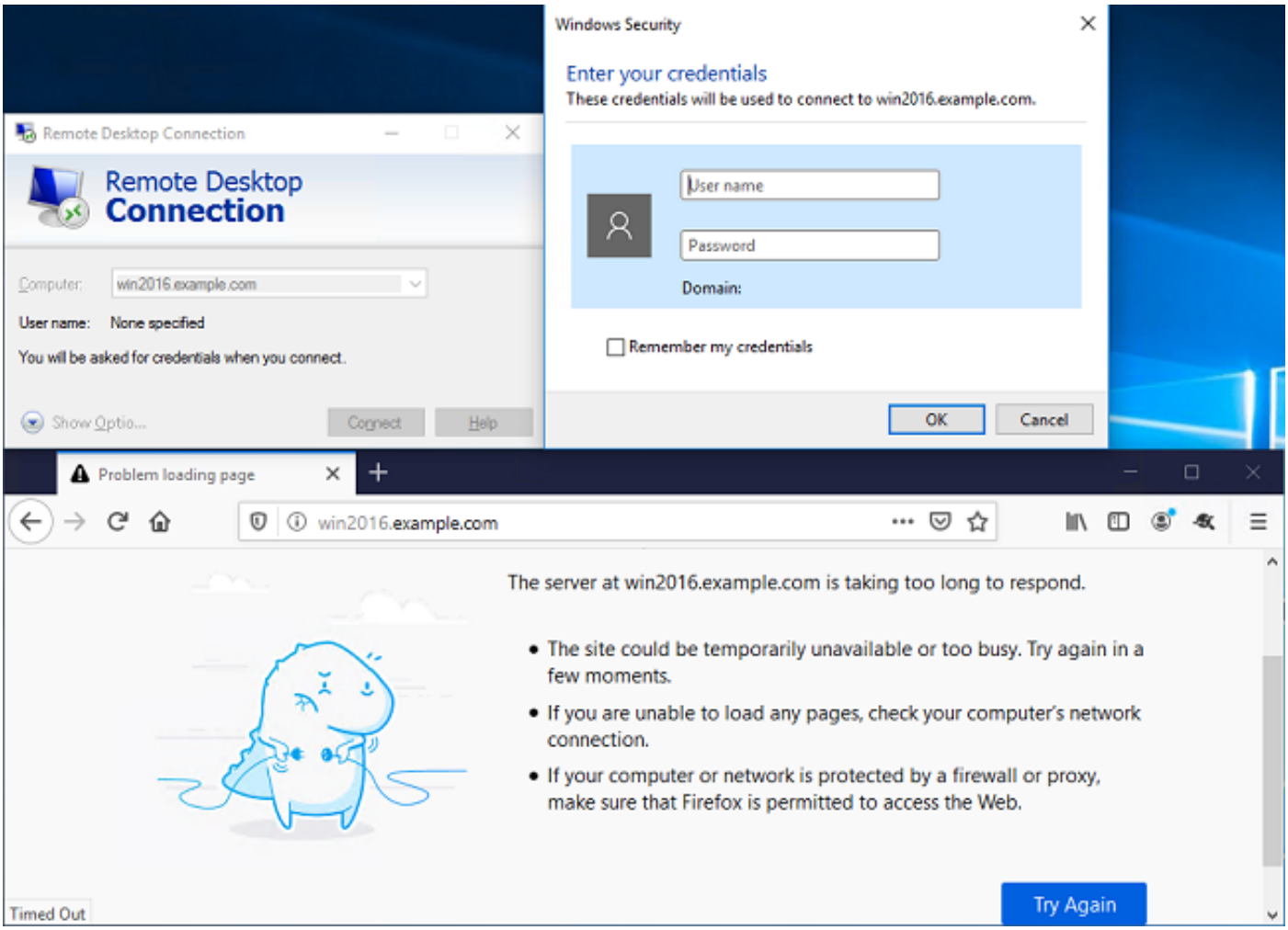
Connettersi con AnyConnect e verificare le regole dei criteri di controllo di accesso



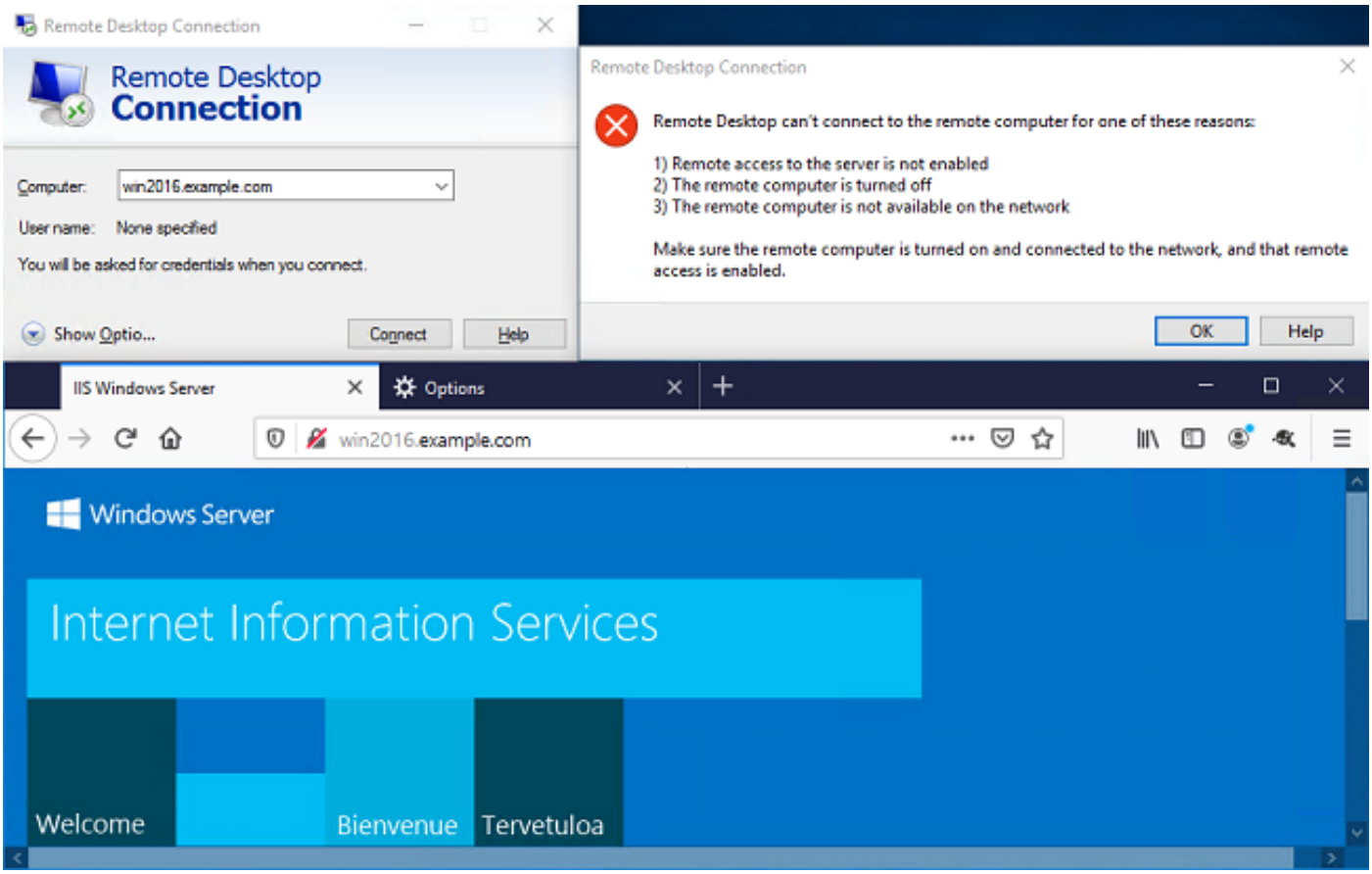


L'utente IT Admin appartiene al gruppo AnyConnect Admins, che ha accesso RDP al server Windows. Non dispone tuttavia dell'accesso a HTTP.

L'apertura di una sessione RDP e Firefox su questo server verifica che l'utente possa accedere al server solo tramite RDP.



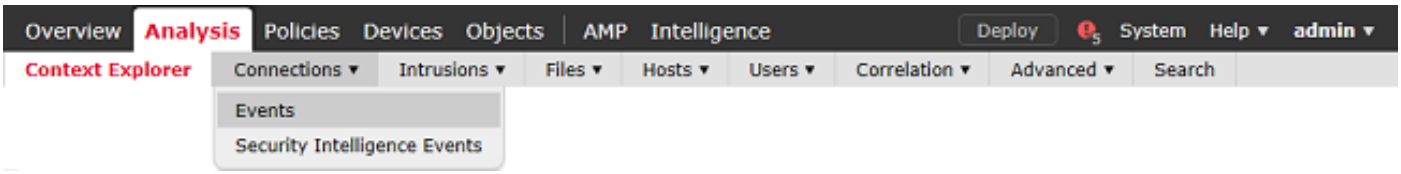
Se l'accesso è stato eseguito con l'utente Test User che fa parte del gruppo AnyConnect Users, che dispone dell'accesso HTTP ma non dell'accesso RDP, è possibile verificare che le regole di controllo dell'accesso siano effettive.



Verifica con gli eventi di connessione FMC

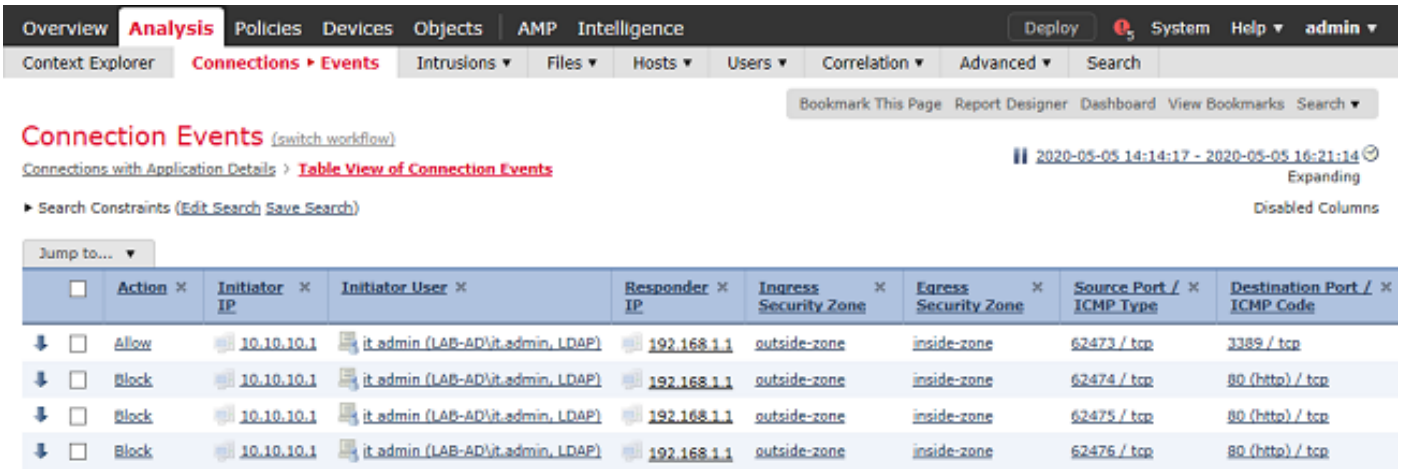
Poiché la registrazione è stata attivata nelle regole dei criteri di controllo di accesso, è possibile controllare gli eventi di connessione per verificare se il traffico soddisfa tali regole.

Passare ad Analisi > Connessioni > Eventi.

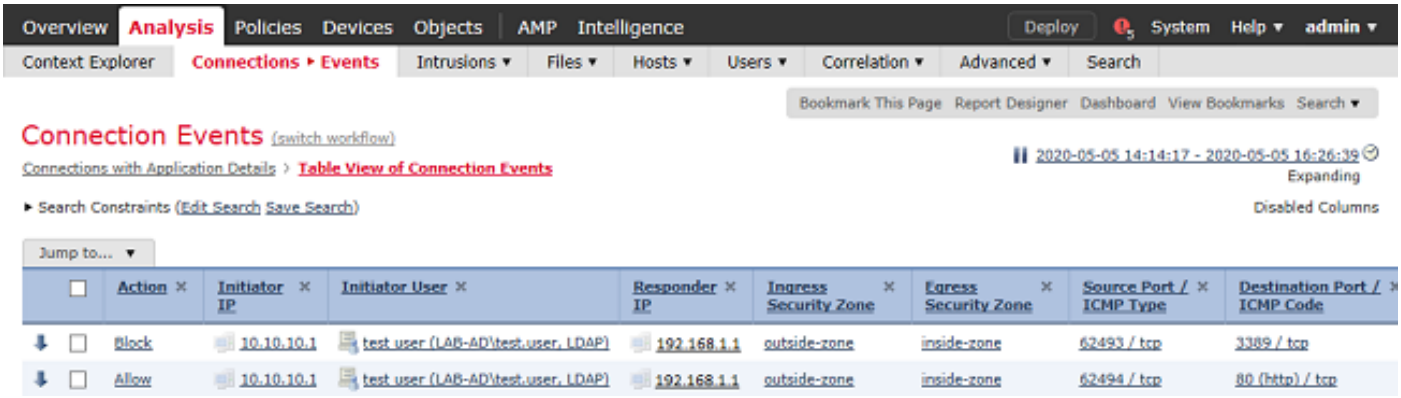


Nella visualizzazione a tabella degli eventi di connessione, i registri vengono filtrati in modo da visualizzare solo gli eventi di connessione per l'amministratore IT.

In questa finestra è possibile verificare che il traffico RDP diretto al server (TCP e UDP 3389) sia consentito, tuttavia il traffico della porta 80 è bloccato.



Per l'utente Test User, è possibile verificare che il traffico RDP verso il server sia bloccato e che il traffico della porta 80 sia consentito.



Risoluzione dei problemi

Debug

Questo debug può essere eseguito nella CLI di diagnostica per risolvere i problemi relativi all'autenticazione LDAP: debug ldap 255.

Per risolvere i problemi relativi ai criteri di controllo di accesso per l'identità degli utenti, è possibile eseguire in client il supporto di sistema per il debug del motore del firewall per determinare il motivo per cui il traffico viene autorizzato o bloccato in modo imprevisto.

Debug LDAP in corso

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
```

```
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
        Base DN = [DC=example,DC=com]
        Filter  = [sAMAccountName=it.admin]
        Scope   = [SUBTREE]
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]    objectClass: value = top
[53]    objectClass: value = person
[53]    objectClass: value = organizationalPerson
[53]    objectClass: value = user
[53]    cn: value = IT Admin
[53]    sn: value = Admin
[53]    givenName: value = IT
[53]    distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]    instanceType: value = 4
[53]    whenCreated: value = 20200421025811.0Z
[53]    whenChanged: value = 20200421204622.0Z
[53]    displayName: value = IT Admin
[53]    uSNCreated: value = 25896
[53]    memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]    uSNChanged: value = 26119
[53]    name: value = IT Admin
[53]    objectGUID: value = &...J..O..2w...c
[53]    userAccountControl: value = 512
[53]    badPwdCount: value = 6
[53]    codePage: value = 0
[53]    countryCode: value = 0
[53]    badPasswordTime: value = 132320354378176394
[53]    lastLogoff: value = 0
[53]    lastLogon: value = 0
[53]    pwdLastSet: value = 132319114917186142
[53]    primaryGroupID: value = 513
[53]    objectSid: value = .............{I...;.....j...
[53]    accountExpires: value = 9223372036854775807
[53]    logonCount: value = 0
[53]    sAMAccountName: value = it.admin
[53]    sAMAccountType: value = 805306368
[53]    userPrincipalName: value = it.admin@example.com
[53]    objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]    dSCorePropagationData: value = 16010101000000.0Z
[53]    lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

Impossibile stabilire una connessione con il server LDAP

<#root>

```
[-2147483611] Session Start
```

```
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611]
```

Connect to LDAP server: ldap://172.16.1.1:389, status = Failed

```
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

Soluzioni potenziali:

- Controllare il routing e assicurarsi che l'FTD riceva una risposta dal server LDAP.
- Se si utilizza LDAPS o STARTTLS, verificare che il certificato CA radice corretto sia attendibile in modo che l'handshake SSL possa essere completato correttamente.
- Verificare che vengano utilizzati l'indirizzo IP e la porta corretti. Se viene utilizzato un nome host, verificare che DNS sia in grado di risolverlo nell'indirizzo IP corretto.

Nome distinto e/o password di accesso binding non corretti

<#root>

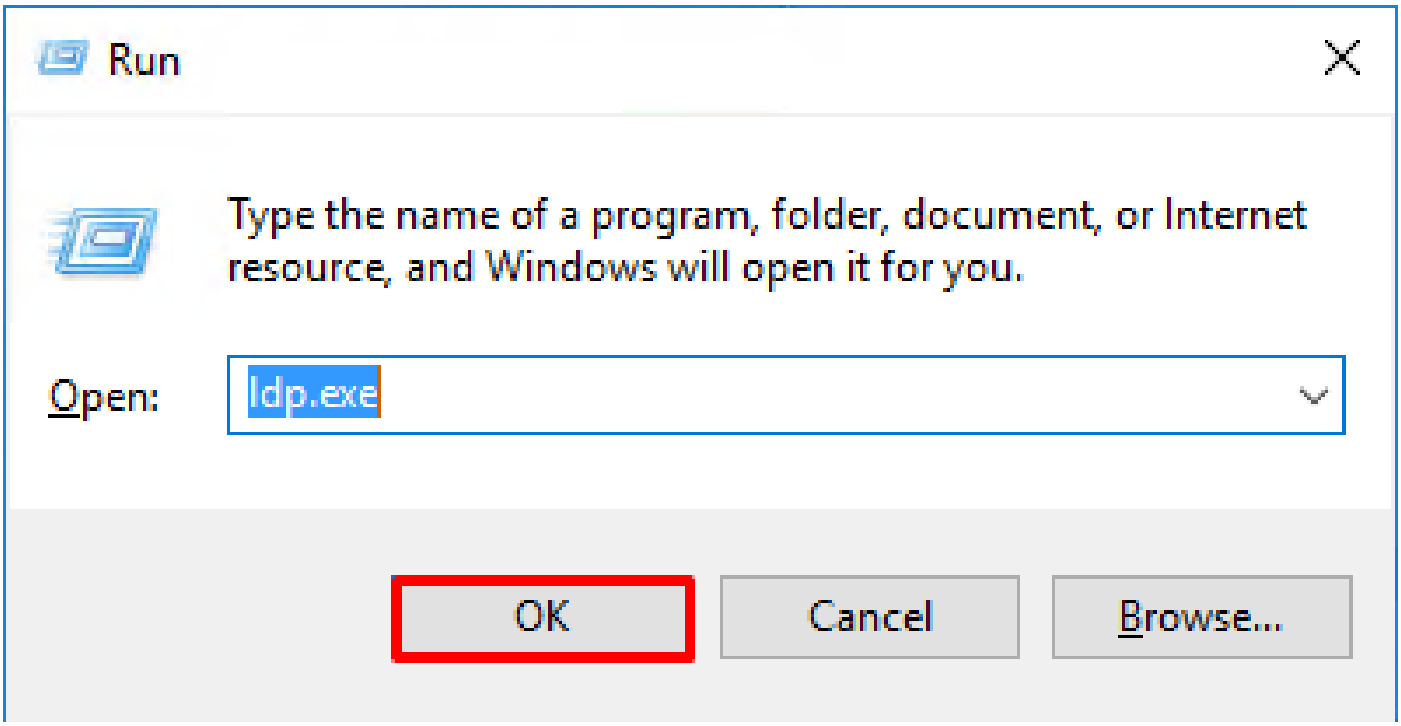
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid credentials
[-2147483615]
```

Failed to bind as administrator returned code (-1) Can't contact LDAP server

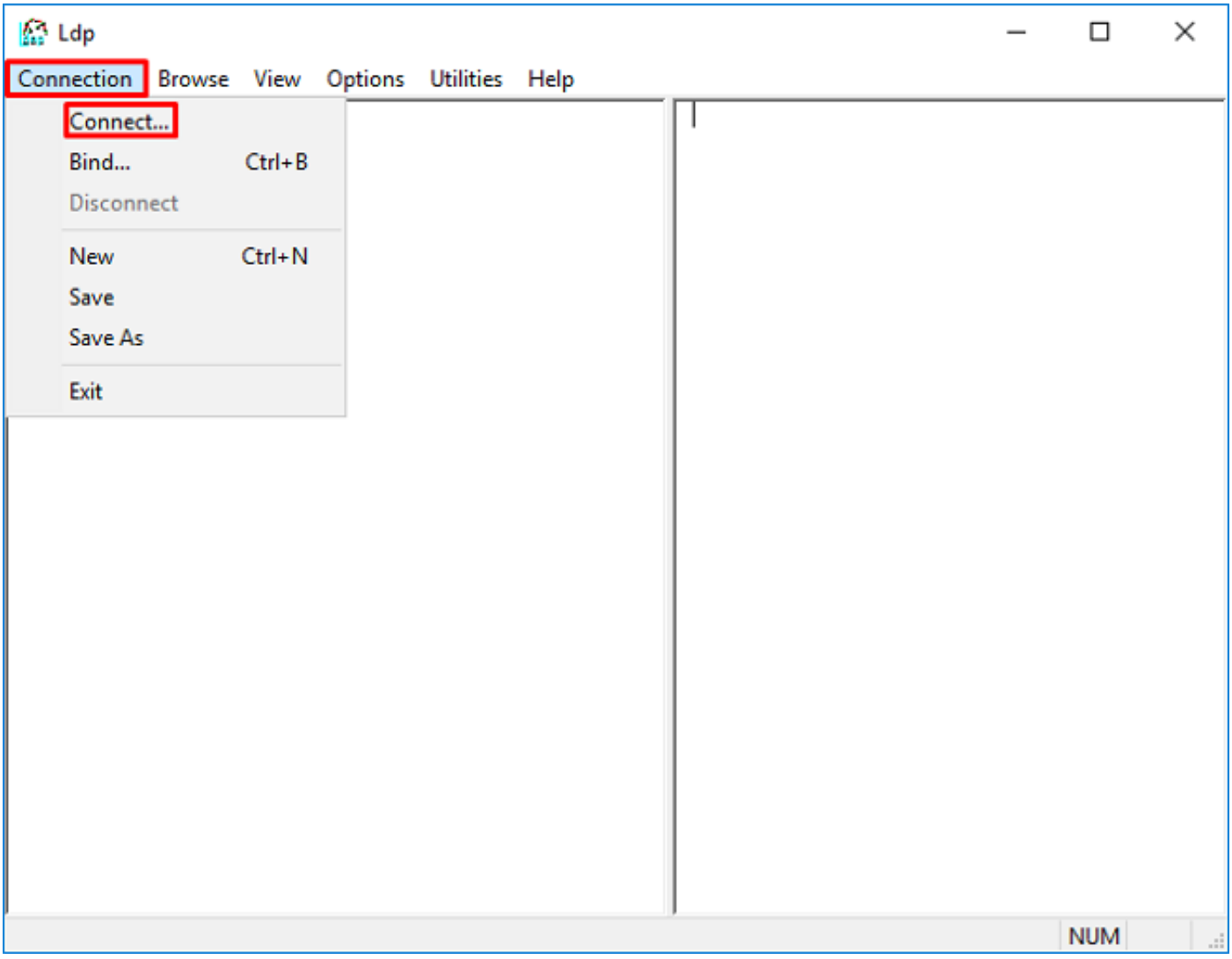
```
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

Soluzione potenziale: verificare che il DN di accesso e la password di accesso siano configurati correttamente. È possibile verificare questa condizione sul server AD con ldp.exe. Per verificare che un account possa essere associato correttamente tramite LDAP, eseguire la procedura seguente:

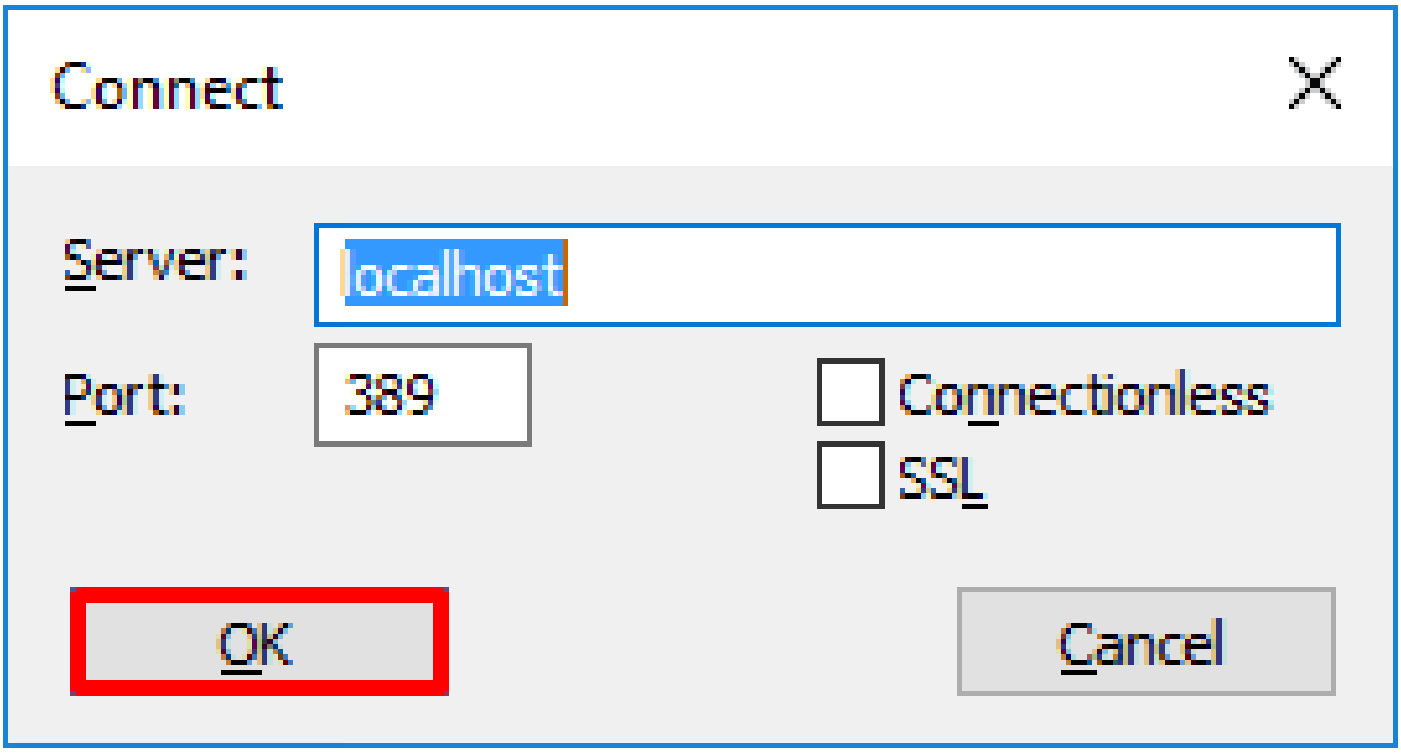
1. Sul server AD, premere Win+R e cercare ldp.exe



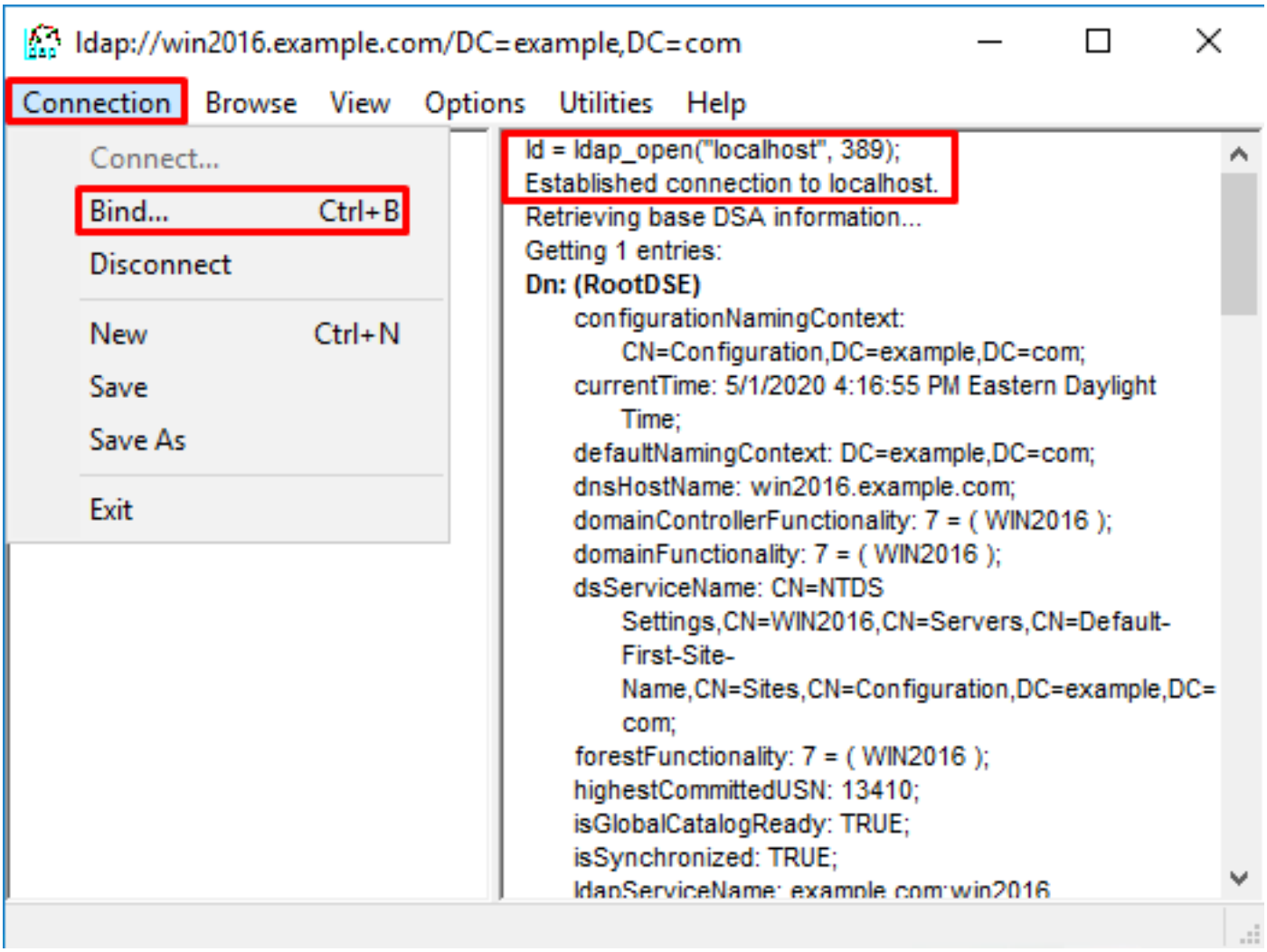
2. In Connessione, selezionare Connetti.



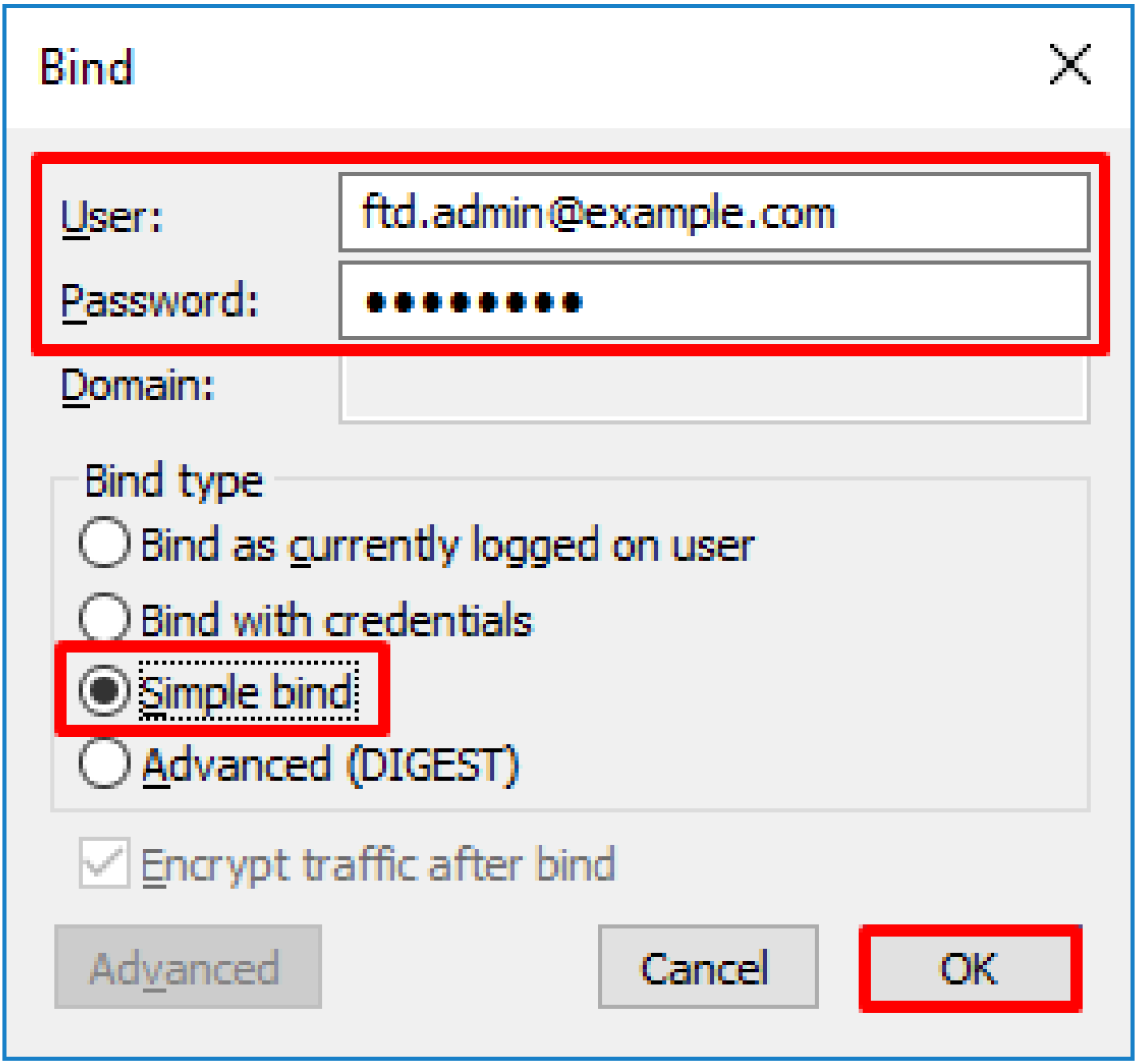
3. Specificare localhost per il server e la porta appropriata, quindi fare clic su OK.



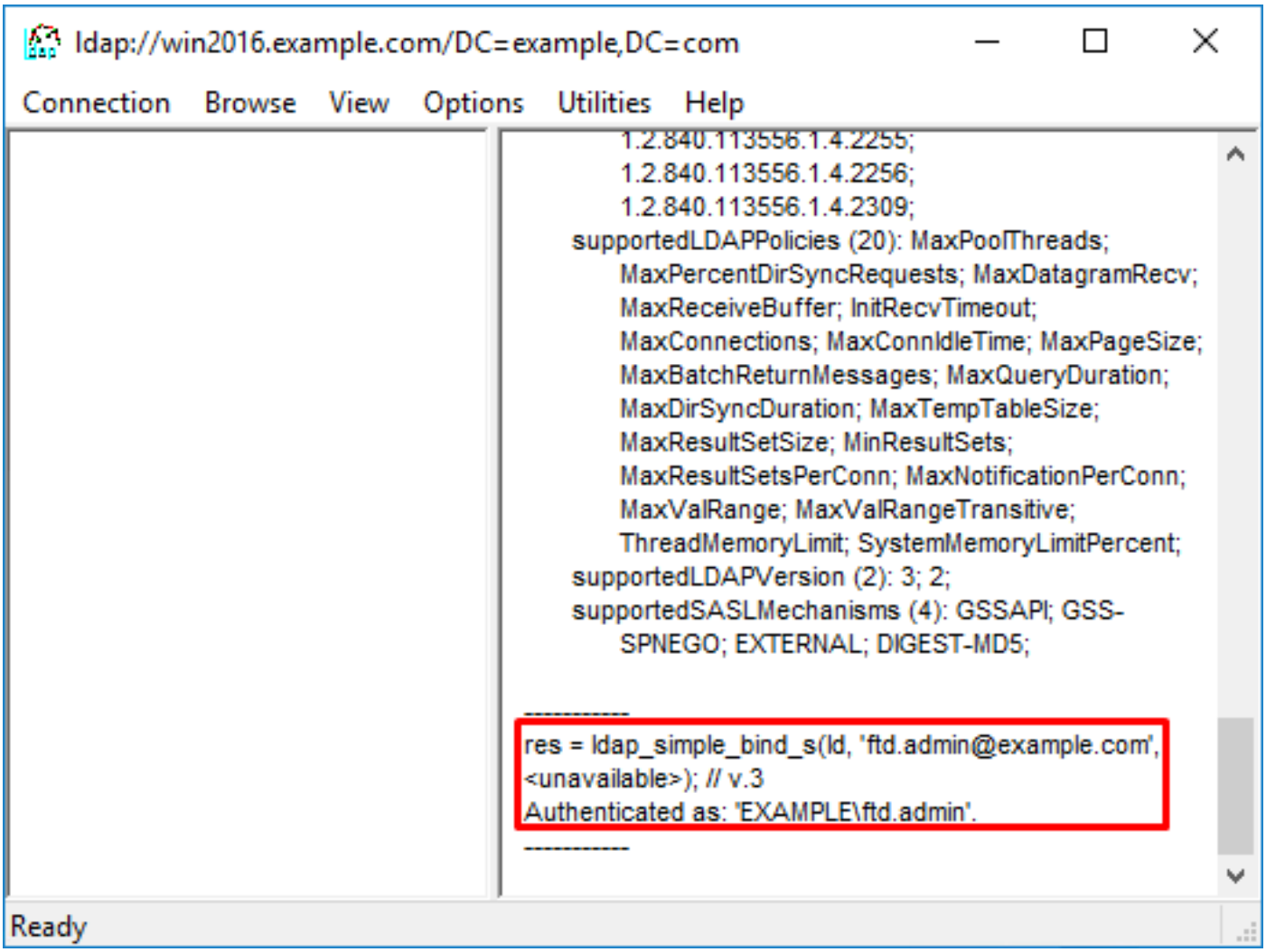
4. La colonna destra contiene il testo che indica la riuscita della connessione. Passare a Connessione > Associazione.



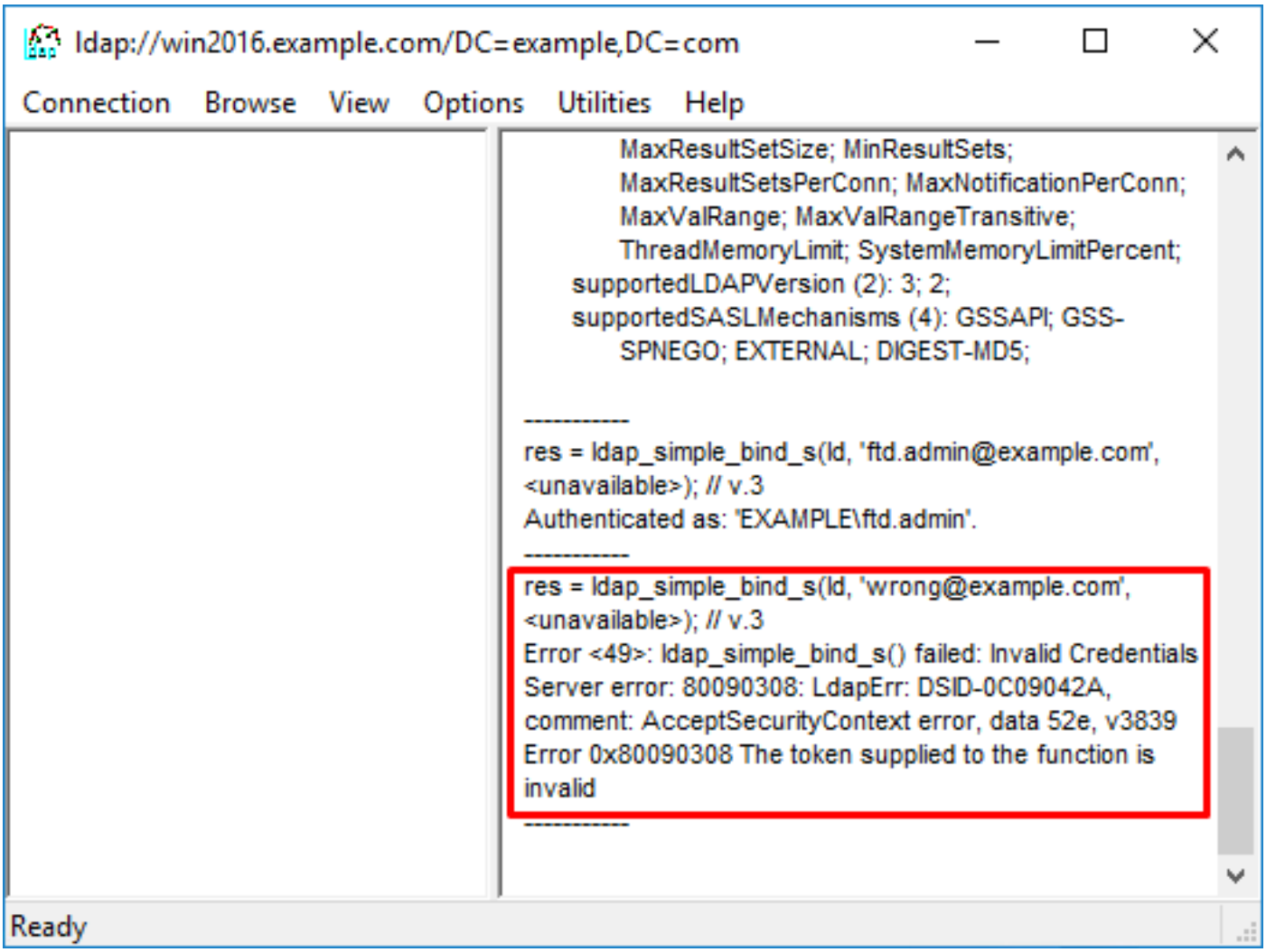
5. Selezionare Associazione semplice, quindi specificare Utente account directory e Password. Fare clic su OK.



Se il binding ha esito positivo, il comando ldp visualizza Autenticato come: DOMINIO\nomeutente



Se si tenta di eseguire il binding con un nome utente o una password non validi, si verificherà un errore come quello rilevato in questo esempio.



Server LDAP: impossibile trovare il nome utente

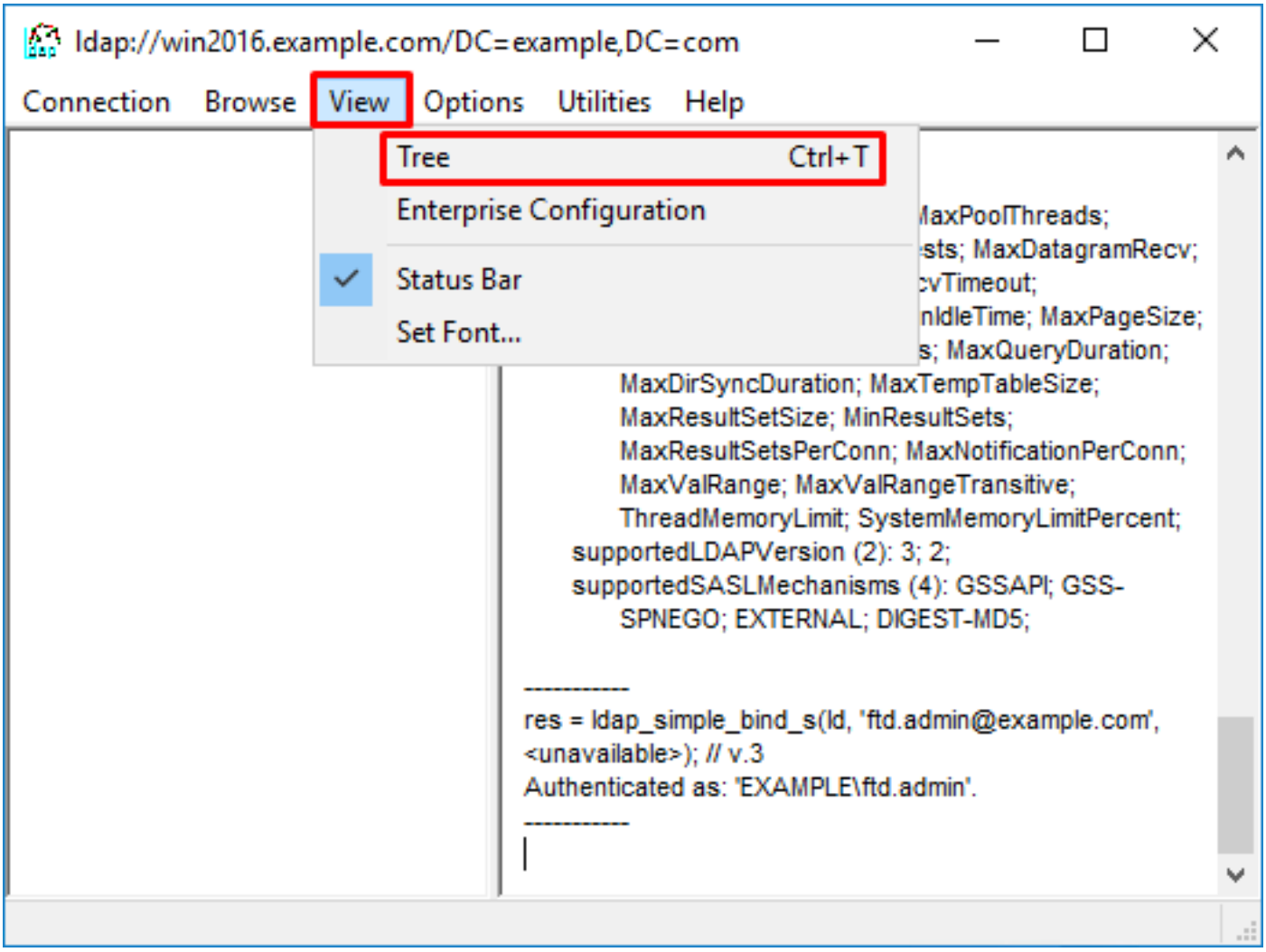
<#root>

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admi]
        Scope   = [SUBTREE]
[-2147483612]

Search result parsing returned failure status

[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
```

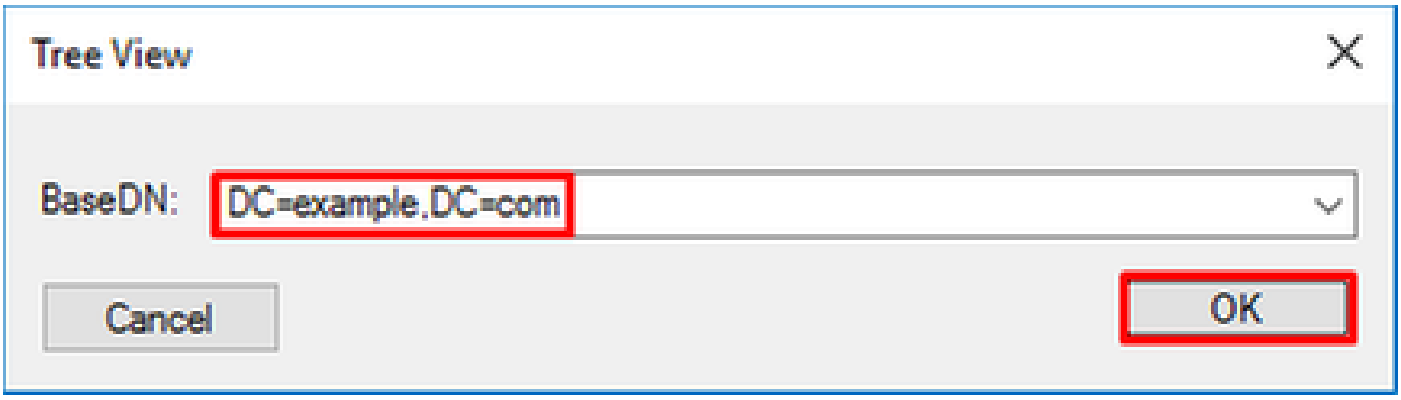
```
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End
```

Soluzione potenziale: verificare che AD sia in grado di trovare l'utente con la ricerca eseguita dall'FTD. Questa operazione può essere eseguita anche con ldp.exe.

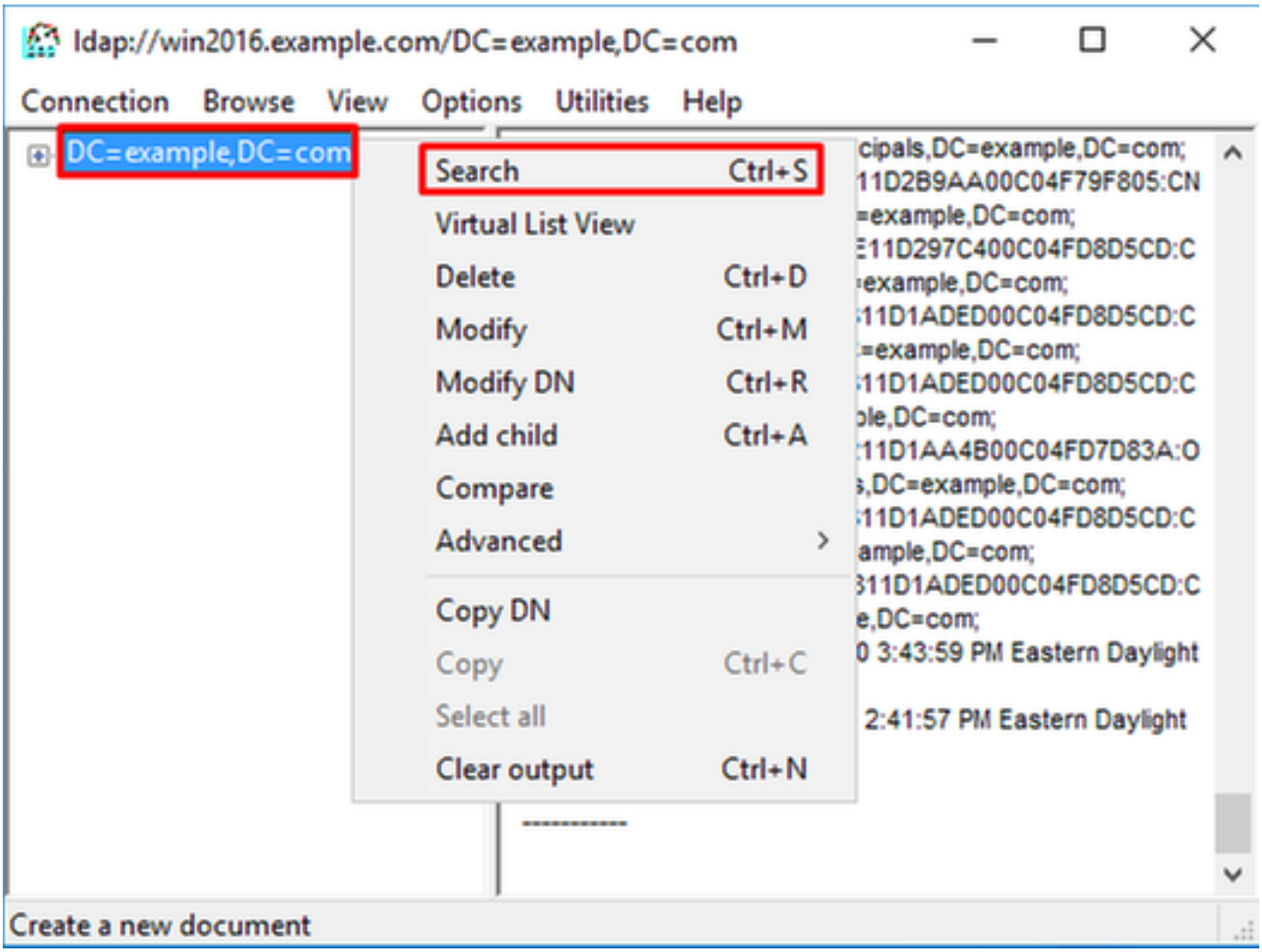
1. Dopo aver eseguito correttamente l'associazione come illustrato in precedenza, passare a Visualizza > Struttura.



2. Specificare il DN di base configurato sull'FTD, quindi fare clic su OK



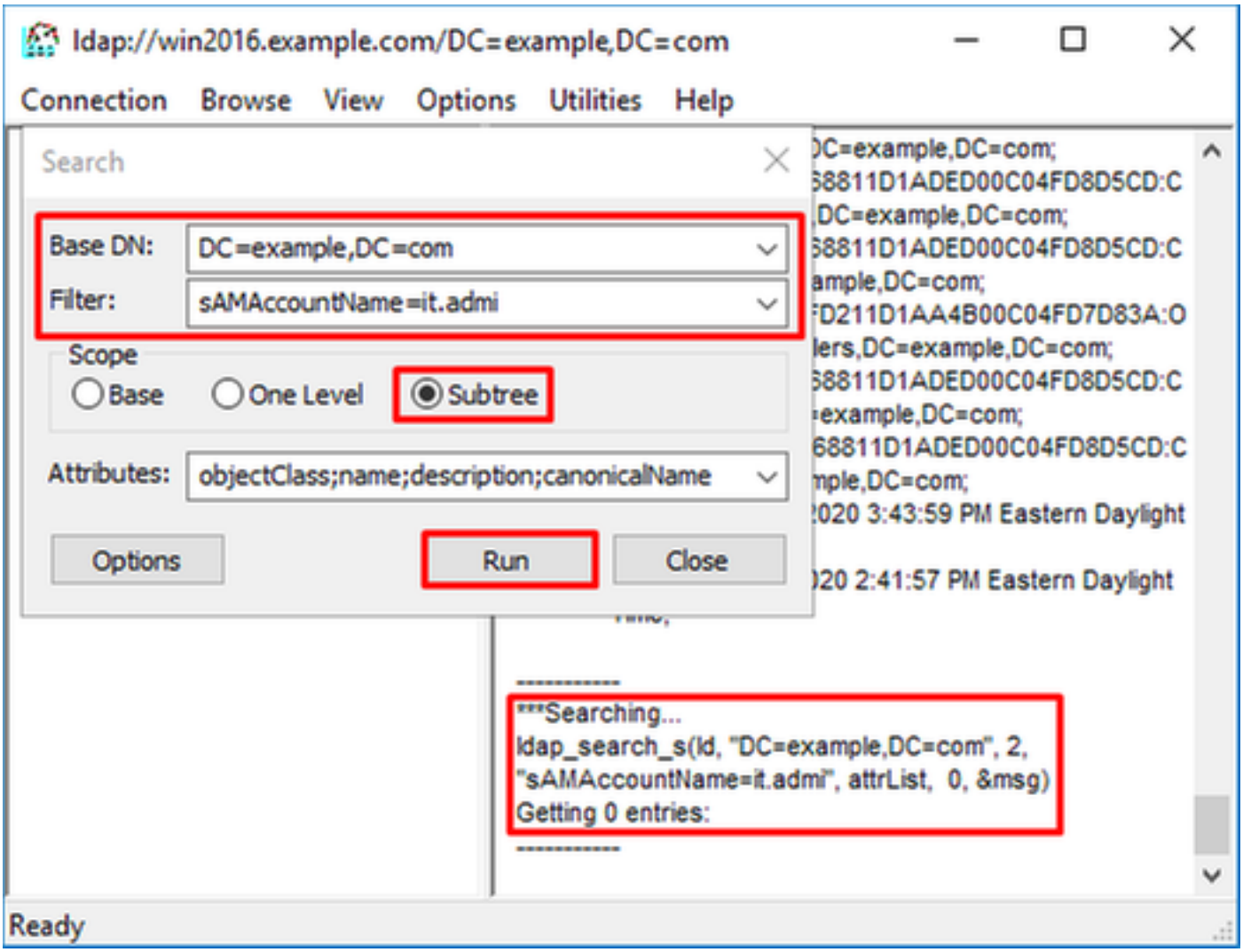
3. Fare clic con il pulsante destro del mouse sul DN di base, quindi scegliere Cerca.



4. Specificare gli stessi valori di DN base, Filtro e Ambito visualizzati nei debug.

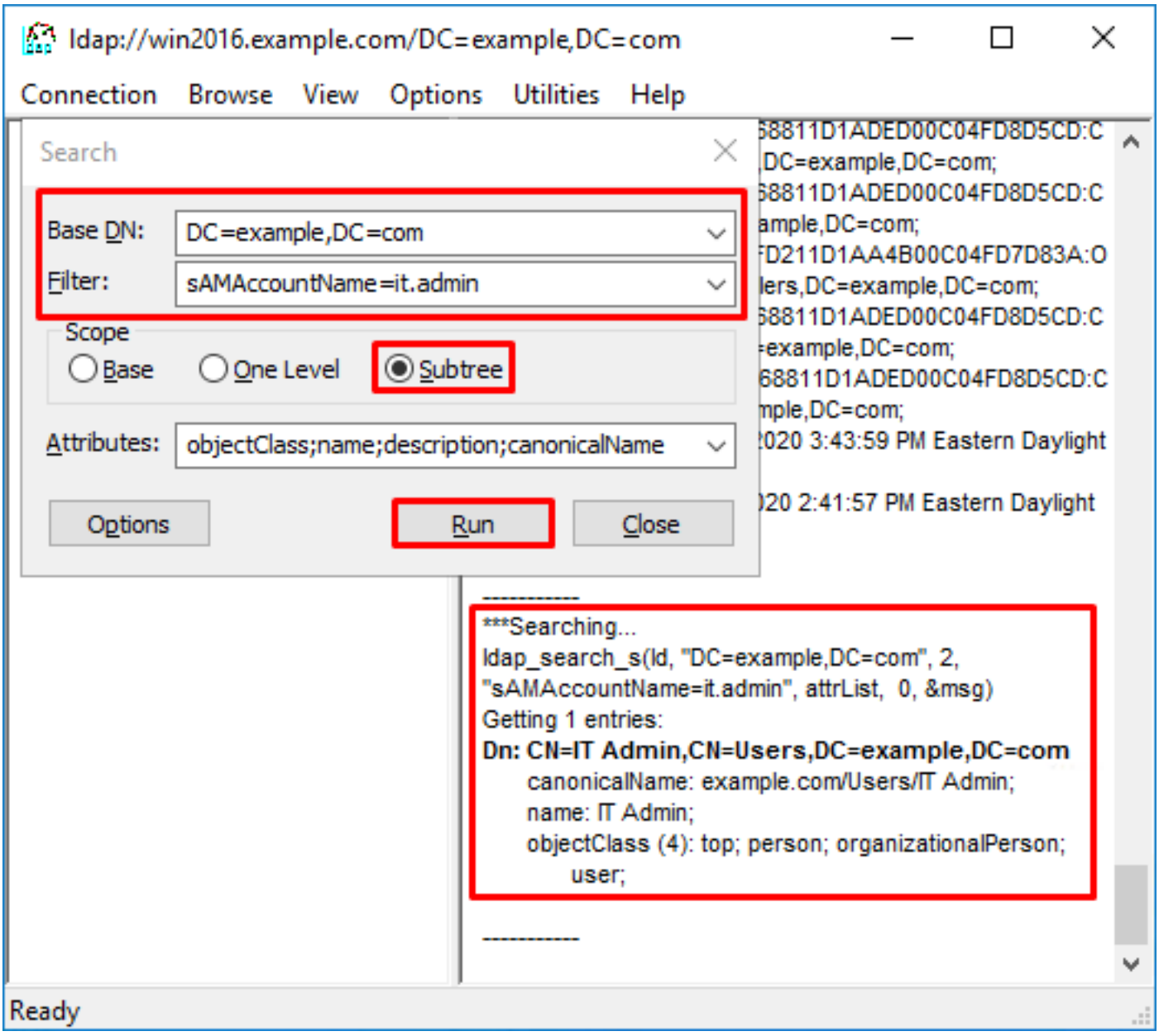
In questo esempio, sono:

- DN di base: dc=esempio,dc=com
- Filtro: samaccountname=it.admi
- Ambito:SUBTREE



ldp trova 0 voci perché non esiste alcun account utente con sAMAccountname it.admi nel DN di base dc=example,dc=com.

Un altro tentativo con il sAMAccountname it.admin corretto mostra un risultato diverso. ldp trova 1 voce sotto il DN di base dc=example,dc=com e stampa quel DN utente.



Password non corretta per il nome utente

<#root>

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admin]
        Scope   = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
```

```
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
[-2147483613]
```

Simple authentication for it.admin returned code (49) Invalid credentials

```
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext erro
[-2147483613]
```

Invalid password for it.admin

```
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

Soluzione potenziale: verificare che la password utente sia configurata correttamente e che non sia scaduta. Analogamente al DN di accesso, l'FTD esegue un'associazione ad Active Directory con le credenziali utente.

Questo binding può essere eseguito anche in ldp per verificare che AD sia in grado di riconoscere le stesse credenziali di nome utente e password. I passaggi in ldp sono illustrati nella sezione DN di login binding e/o password errati.

È inoltre possibile esaminare i registri del Visualizzatore eventi del server Microsoft per individuare eventuali errori.

Test AAA

Il comando test aaa-server può essere usato per simulare un tentativo di autenticazione da parte dell'FTD con un nome utente e una password specifici. Questa opzione può essere utilizzata per verificare la presenza di errori di connessione o autenticazione. Il comando è test di autenticazione aaa-server [AAA-server] host [AD IP/nomehost].

<#root>

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 realm-id 7
aaa-server
```

LAB-AD

```
 host
```

win2016.example.com

```
 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn ftd.admin@example.com
 server-type auto-detect

> test aaa-server authentication
```

```
LAB-AD

 host

win2016.example.com

Username: it.admin
Password: ********
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

Acquisizioni pacchetti

Le acquisizioni di pacchetti possono essere utilizzate per verificare la raggiungibilità al server AD. Se i pacchetti LDAP lasciano l'FTD, ma non c'è risposta, potrebbe essere un problema di routing.

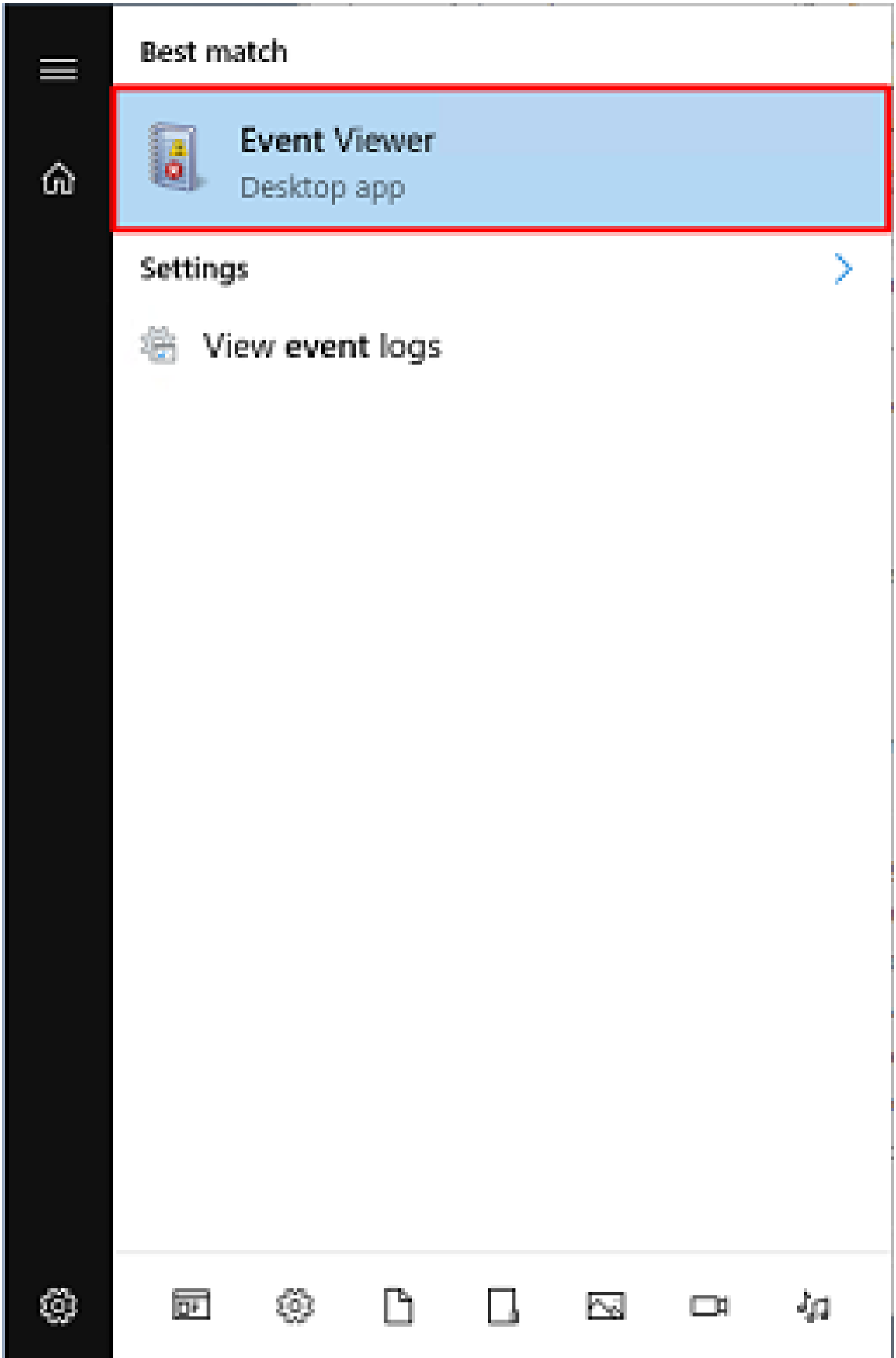
Acquisisci mostra il traffico LDAP bidirezionale.

```
> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via inside
      Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389

> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
  match tcp any host 192.168.1.1 eq ldap

> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password ******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
  match tcp any host 192.168.1.1 eq ldap

> show capture AD

54 packets captured

   1: 23:02:16.770712       192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 32768 <
   2: 23:02:16.772009       192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 36819128
   3: 23:02:16.772039       192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <nop,nop,ti
   4: 23:02:16.772482       192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 4915
   5: 23:02:16.772924       192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 368191
   6: 23:02:16.772955       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,ti
   7: 23:02:16.773428       192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152
   8: 23:02:16.775030       192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913
   9: 23:02:16.775075       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,ti
[...]
54 packets shown
```

Registri del Visualizzatore eventi di Windows Server

I registri del Visualizzatore eventi sul server AD possono fornire informazioni più dettagliate sul motivo per cui si è verificato un errore.

1. Cercare e aprire il Visualizzatore eventi.


Best match
Event Viewer
Desktop app
Settings
View event logs

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).