

# Configurazione dell'autenticazione AD (LDAP) e dell'identità utente su FTD Gestito da FDM per i client AnyConnect

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio e diagramma reticolare](#)

[Configurazioni AD](#)

[Determina DN di base 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 FDM](#)

[Verifica delle licenze](#)

[Imposta origine identità AD](#)

[Configurazione di AnyConnect per l'autenticazione AD](#)

[Abilita criterio di identità e configura criteri di sicurezza per identità utente](#)

[Verifica](#)

[Configurazione finale](#)

[Connettersi con AnyConnect e verificare le regole dei criteri di controllo di accesso](#)

[Risoluzione dei problemi](#)

[Debug](#)

[Debug LDAP in corso](#)

[Impossibile stabilire la 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

Questo documento illustra in dettaglio come configurare l'autenticazione Active Directory (AD) per i client AnyConnect che si connettono a un Cisco Firepower Threat Defense (FTD) gestito da Firepower Device Management (FDM). L'identità dell'utente verrà usata nei criteri di accesso per limitare gli utenti AnyConnect a porte e indirizzi IP specifici.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione di RMA VPN su FDM
- Conoscenze base della configurazione del server LDAP in FDM
- Conoscenze base di Active Directory

## Componenti usati

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

- Server Microsoft 2016
- 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.

# Configurazione

## Esempio e diagramma reticolare



Il server Windows è preconfigurato con Internet Information Services (IIS) e Remote Desktop Protocol (RDP) per verificare l'identità dell'utente. In questa guida alla configurazione verranno creati tre account utente e due gruppi.

Account utente:

- Amministratore FTD: Verrà utilizzato come account di directory per consentire l'associazione di FTD al server AD.
- Amministratore IT: Account dell'amministratore di test utilizzato per dimostrare l'identità dell'utente.
- Utente test: Account utente di prova utilizzato per dimostrare l'identità dell'utente.

Gruppi:

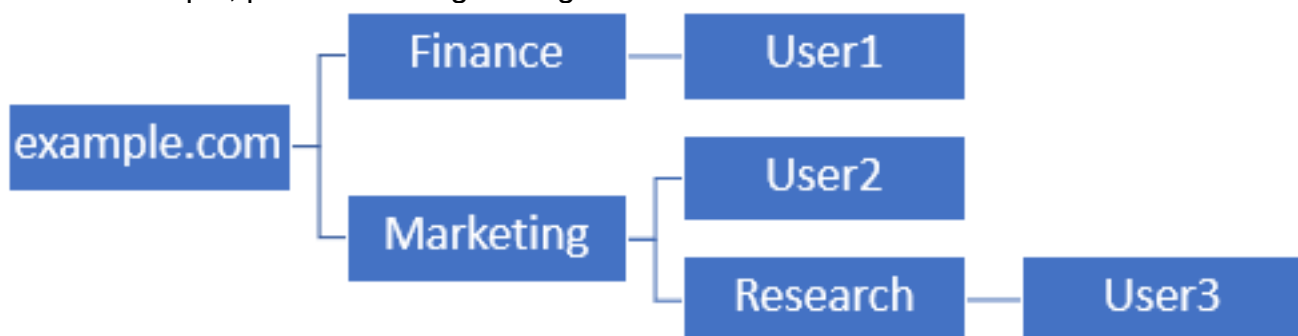
- Amministratori AnyConnect: Gruppo di test a cui verrà aggiunto l'amministratore IT per dimostrare l'identità dell'utente. Questo gruppo avrà accesso RDP solo al server Windows

- Utenti AnyConnect: Gruppo di test a cui verrà aggiunto l'utente di test per dimostrare l'identità dell'utente. Questo gruppo disporrà solo dell'accesso HTTP al server Windows

## Configurazioni AD

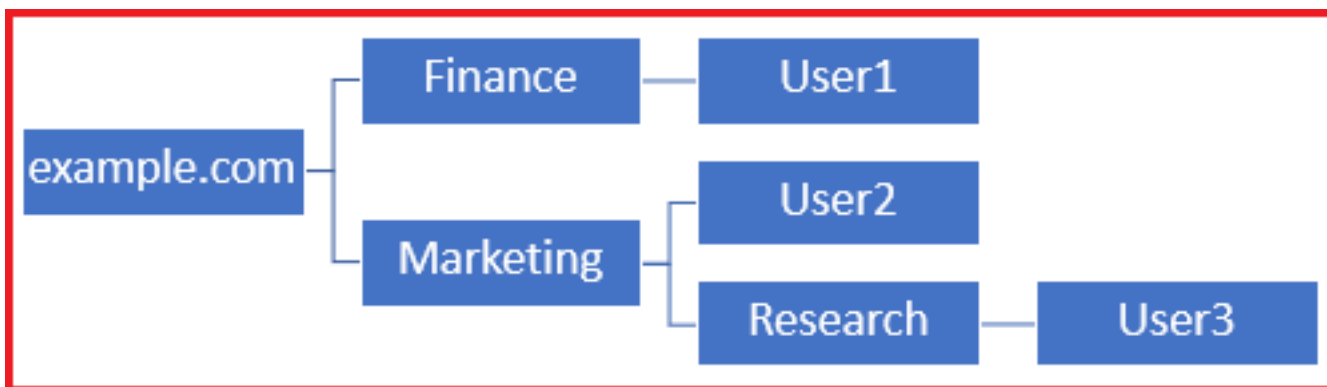
Per configurare correttamente l'autenticazione AD e l'identità utente su FTD, saranno necessari alcuni valori. Tutti questi dettagli devono essere creati o raccolti sul server Microsoft prima di poter eseguire la configurazione su FDM. I valori principali sono:

- Nome dominio: Nome di dominio del server. In questa guida alla configurazione, `example.com` è il nome del dominio.
- Indirizzo IP/FQDN server: Indirizzo IP o FQDN utilizzato per raggiungere il server Microsoft. Se si utilizza un FQDN, è necessario configurare un server DNS in FDM e FTD per risolvere l'FQDN. In questa guida alla configurazione, questi valori sono `win2016.example.com`, che si risolve in `192.168.1.1`.
- Porta server: Porta utilizzata dal servizio LDAP. Per impostazione predefinita, LDAP e STARTTLS utilizzeranno la porta TCP 389 per LDAP e LDAP su SSL (LDAPS) utilizzeranno 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 FDM e FTD per il binding al server LDAP e per l'autenticazione degli utenti e la ricerca di utenti e gruppi. A questo scopo verrà creato un account denominato FTD Admin.
- Nome distinto (DN) base: Il DN di base è il punto di partenza di FDM e l'FTD indicherà ad Active Directory di iniziare la ricerca degli utenti. In questa guida alla configurazione, il dominio radice `example.com` verrà utilizzato come DN di base; tuttavia, per un ambiente di produzione, l'uso di un DN di base all'interno della gerarchia LDAP potrebbe essere migliore. Ad esempio, prendere la seguente gerarchia LDAP:



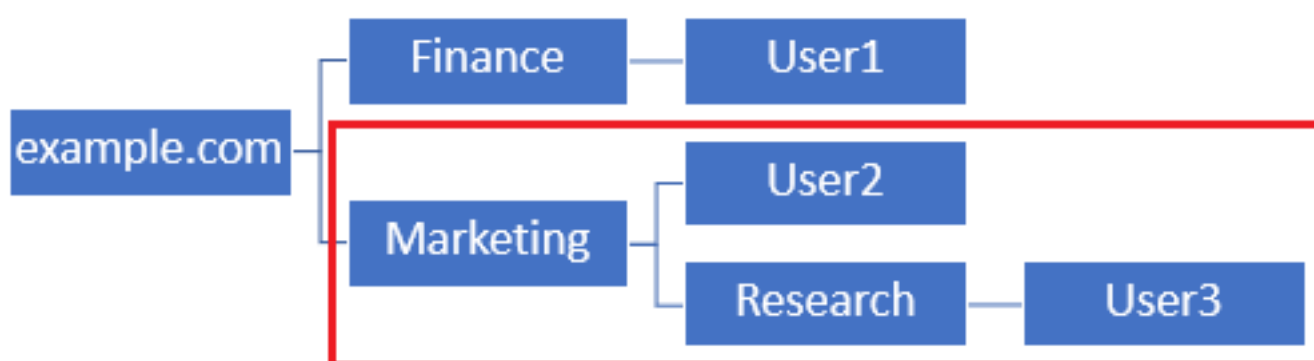
Se un amministratore desidera che gli utenti all'interno dell'unità organizzativa Marketing siano in grado di autenticare il DN di base, è possibile impostare il DN radice (`example.com`). In questo modo, tuttavia, sarà possibile accedere anche all'utente 1 nell'unità organizzativa Finance, poiché la ricerca dell'utente inizierà dalla radice e passerà a Finance, Marketing e Research.

DN di base impostato su `example.com`.



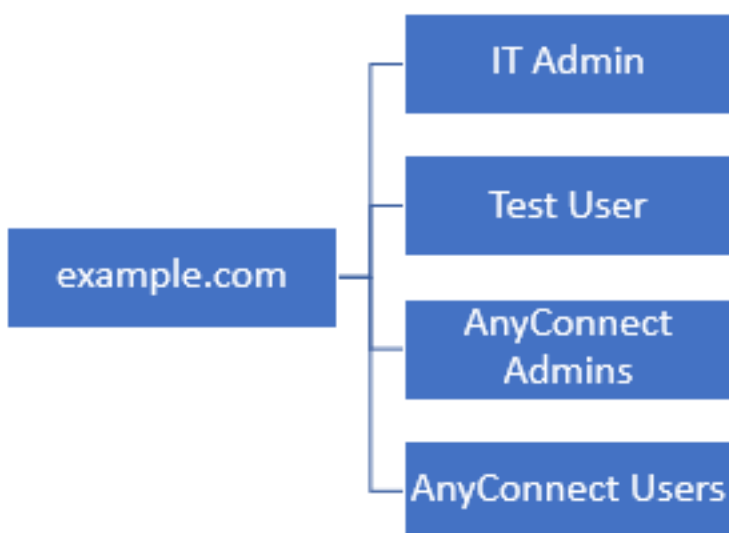
Per limitare gli accessi ai soli utenti dell'unità organizzativa Marketing e di livello inferiore, l'amministratore può invece impostare il DN di base su Marketing. Ora solo l'utente 2 e l'utente 3 saranno in grado di eseguire l'autenticazione perché la ricerca inizierà da Marketing.

DN di base impostato su Marketing:



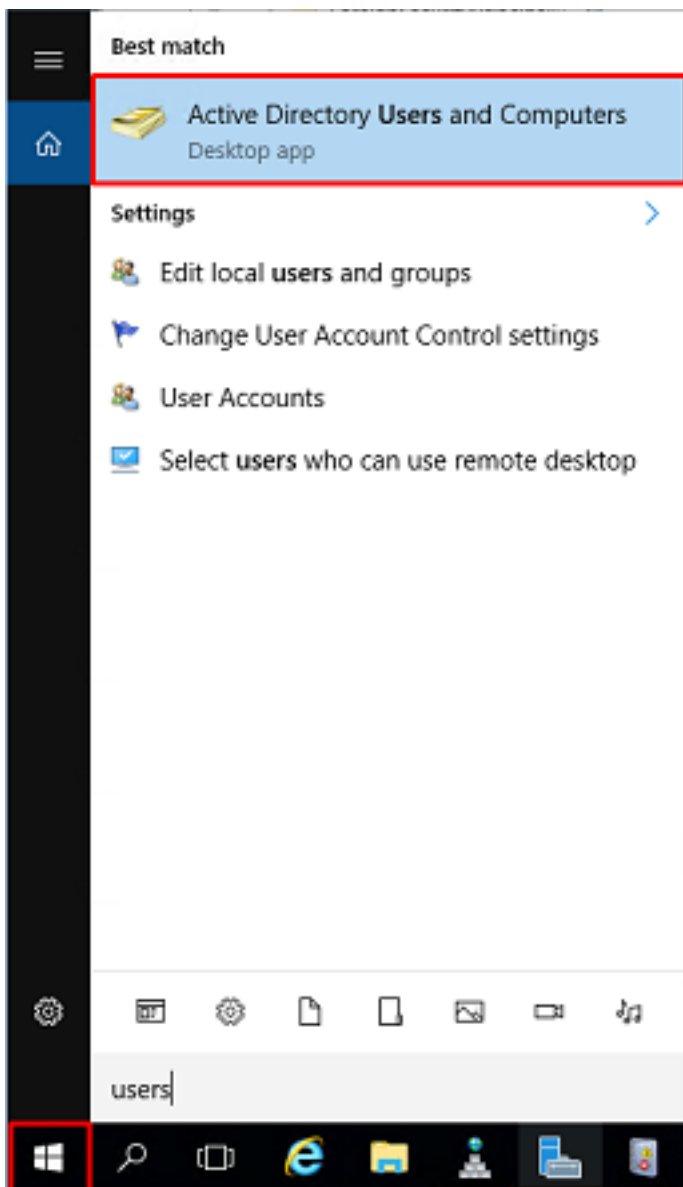
Si noti che per un controllo più granulare all'interno dell'FTD per il quale gli utenti saranno autorizzati a connettersi o assegnare agli utenti autorizzazioni diverse in base ai loro attributi AD, sarà necessario configurare una mappa di autorizzazione LDAP.

Questa gerarchia LDAP semplificata viene utilizzata in questa guida alla configurazione e per il DN di base verrà utilizzato il DN per la directory principale example.com.

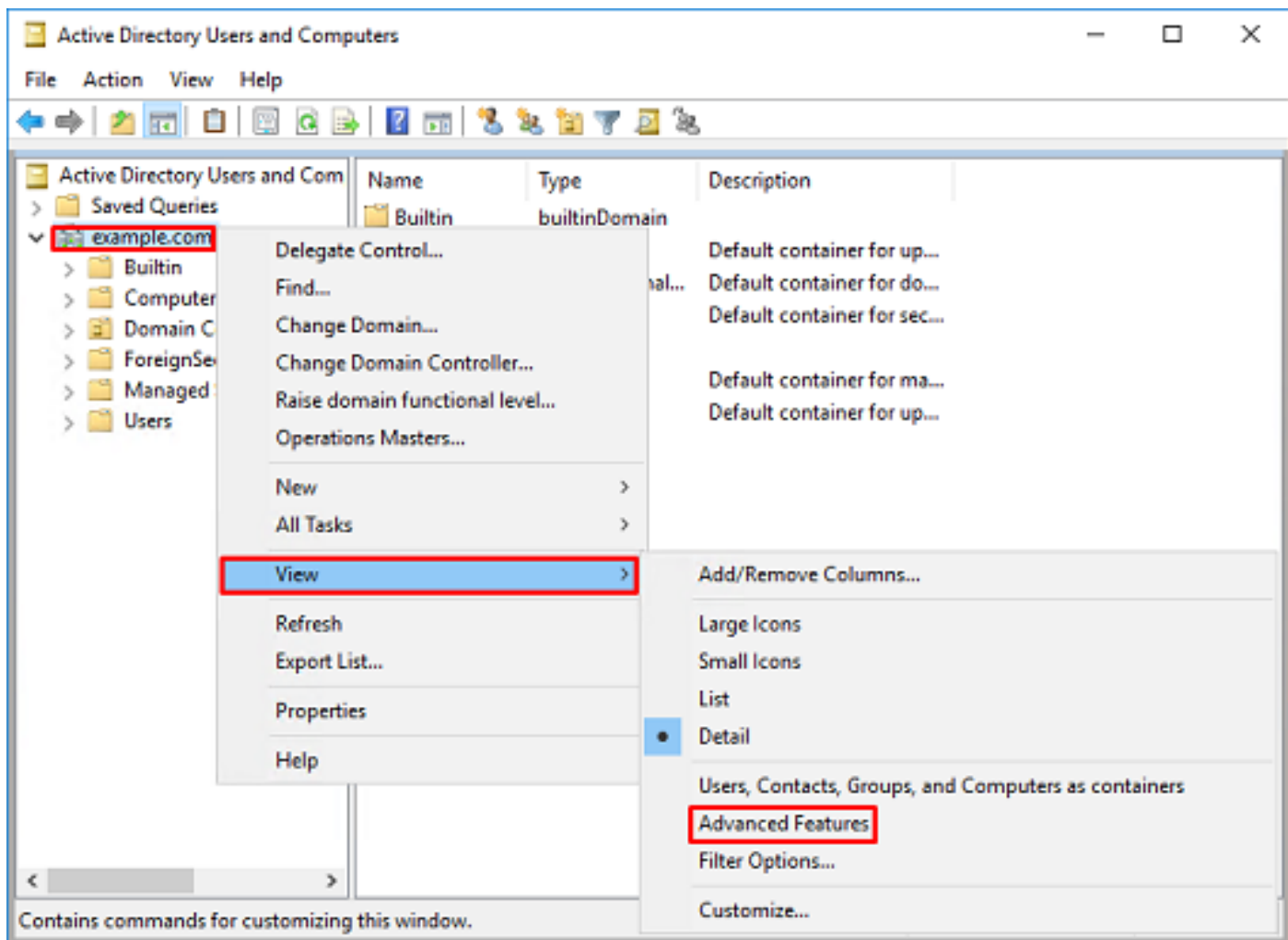


### Determina DN di base LDAP

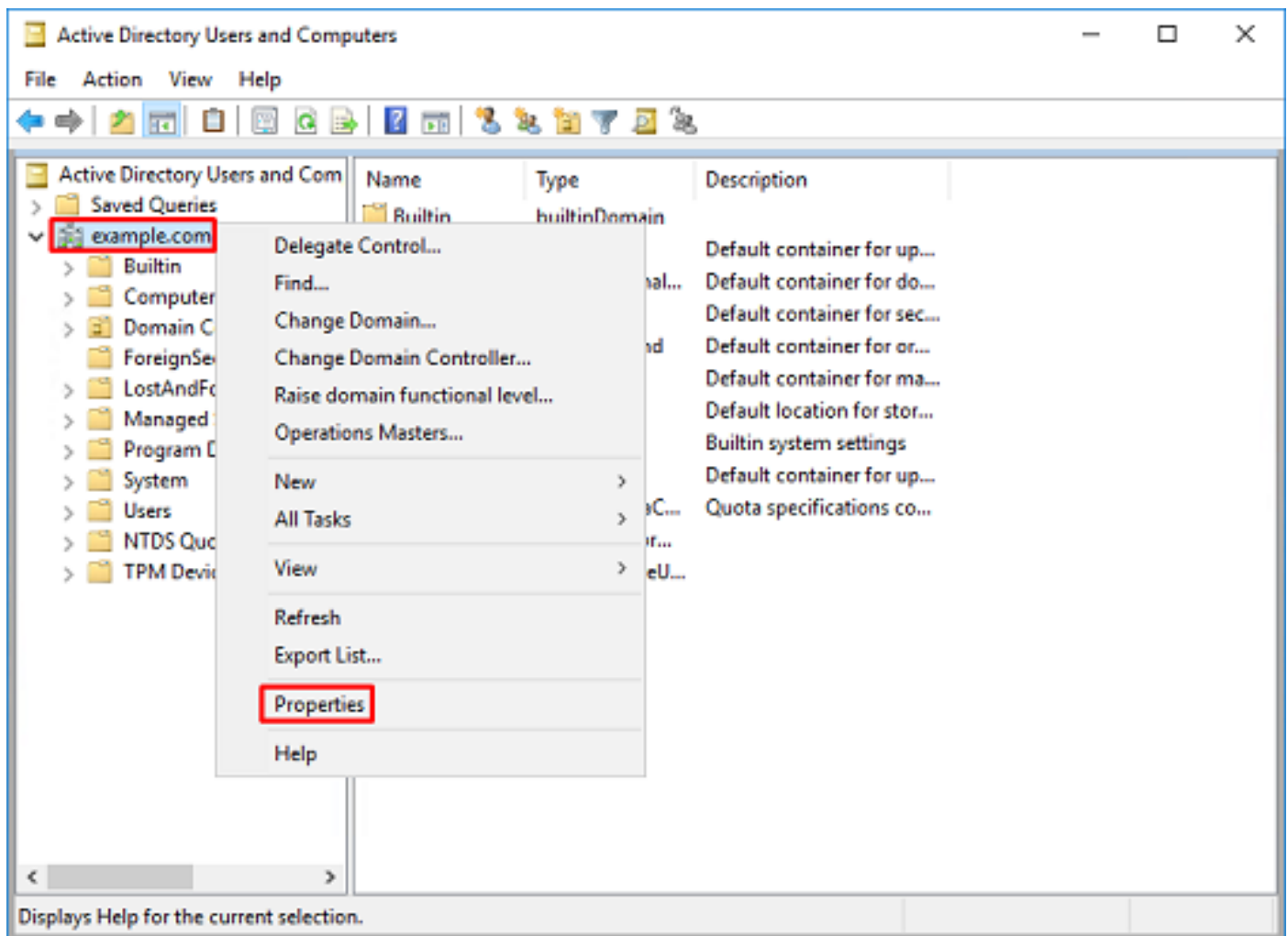
1. Aprire Utenti e computer di Active Directory.



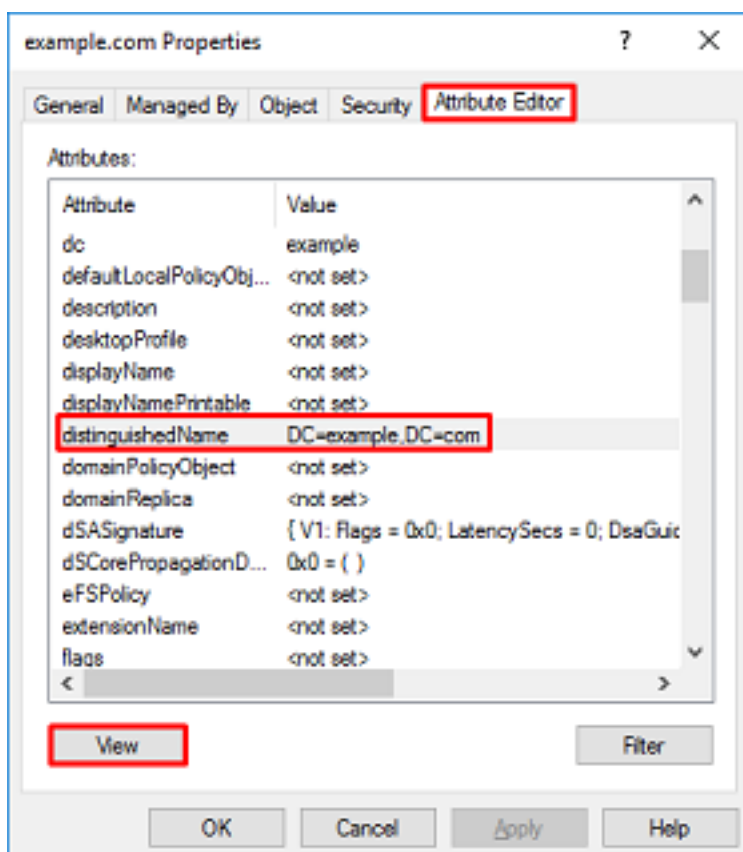
2. Fare clic con il pulsante sinistro del mouse sul dominio radice (per aprire il contenitore), fare clic con il pulsante destro del mouse sul dominio radice, quindi selezionare **Visualizza** e fare clic su **Caratteristiche avanzate**.



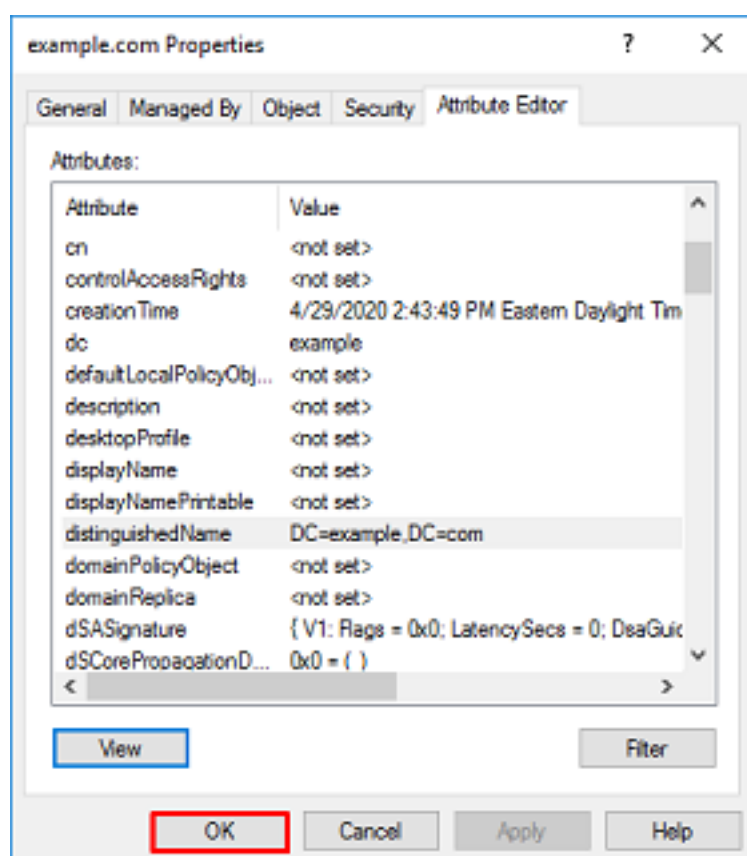
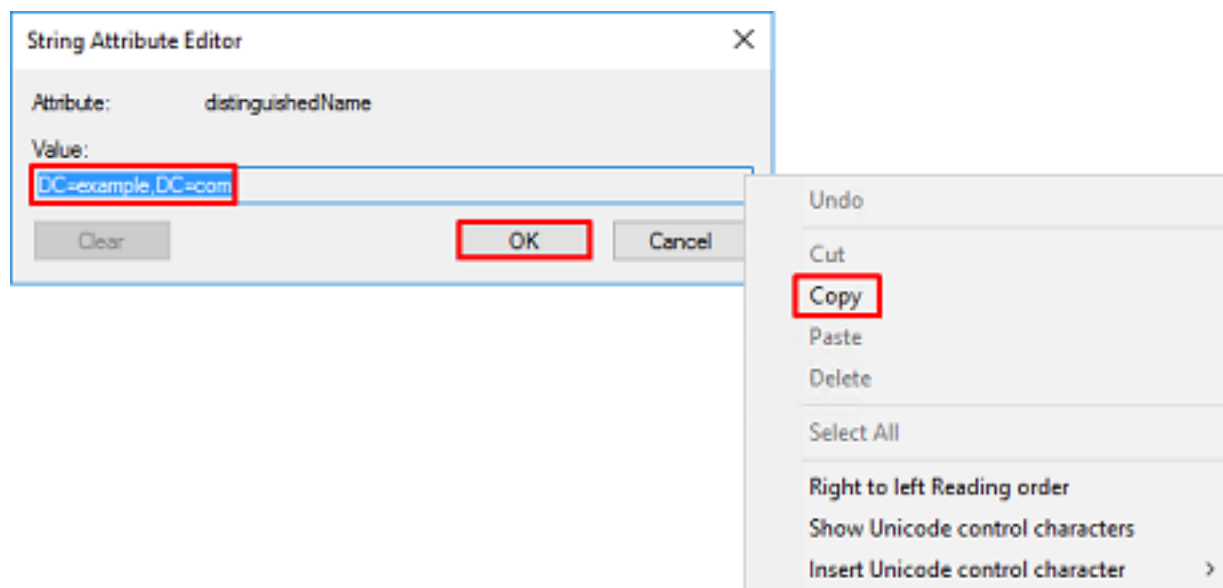
3. In questo modo sarà possibile visualizzare ulteriori proprietà negli oggetti AD. Ad esempio, per trovare il DN per la directory principale example.com, fare clic con il pulsante destro del mouse su **example.com** quindi passare a **Proprietà**.



4. In **Proprietà**, fare clic sulla scheda **Editor attributi**. Individuare **distinguishedName** in Attributi, quindi fare clic su **Visualizza**.

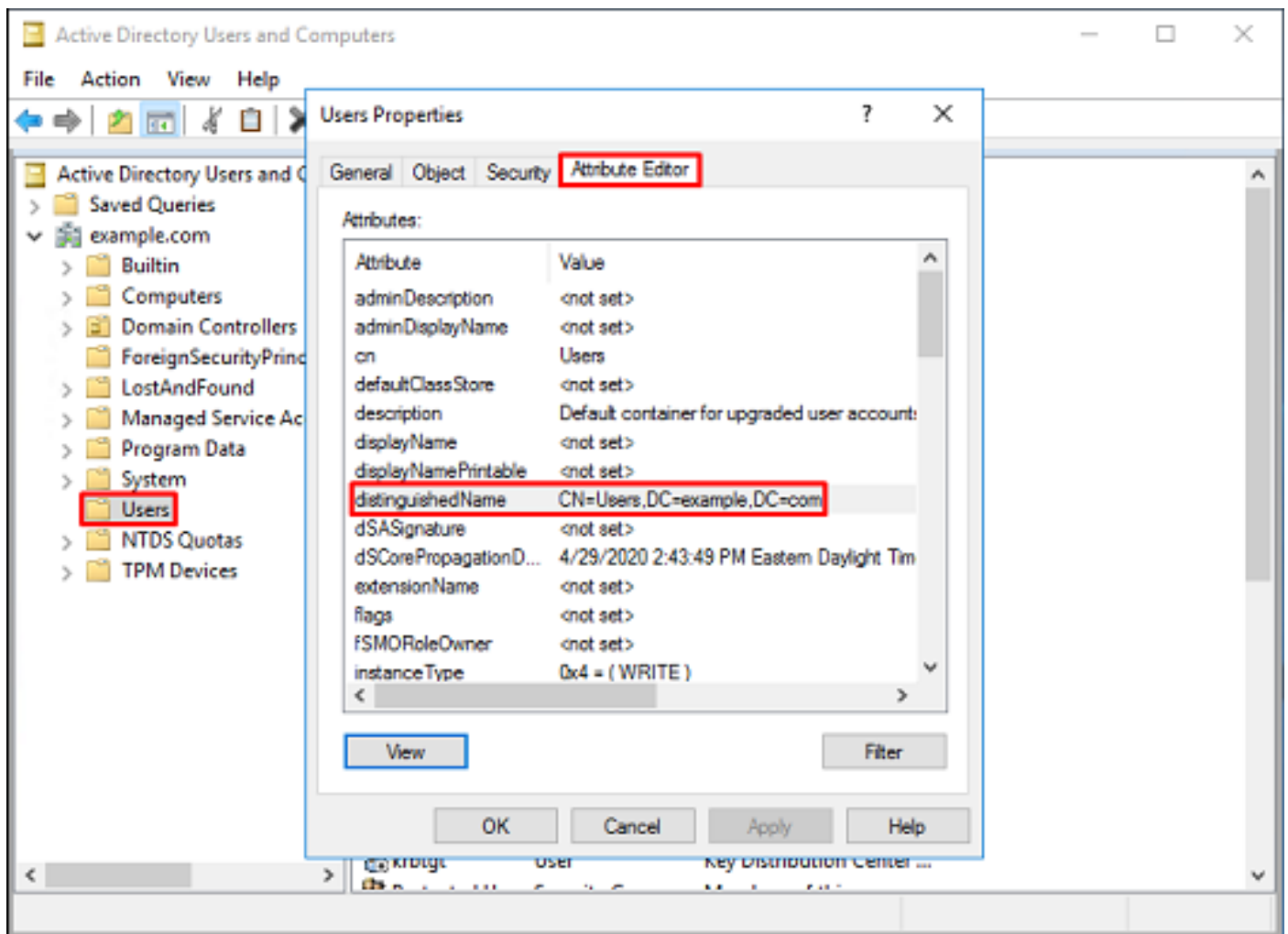


5. Verrà aperta una nuova finestra in cui il DN può essere copiato e incollato in FDM in un secondo momento. In questo esempio, il DN radice è DC=example, DC=com. Copiare il valore. Per uscire dalla finestra Editor attributi stringa, fare clic su **OK**, quindi fare di nuovo clic su **OK** per uscire dalla finestra Proprietà.

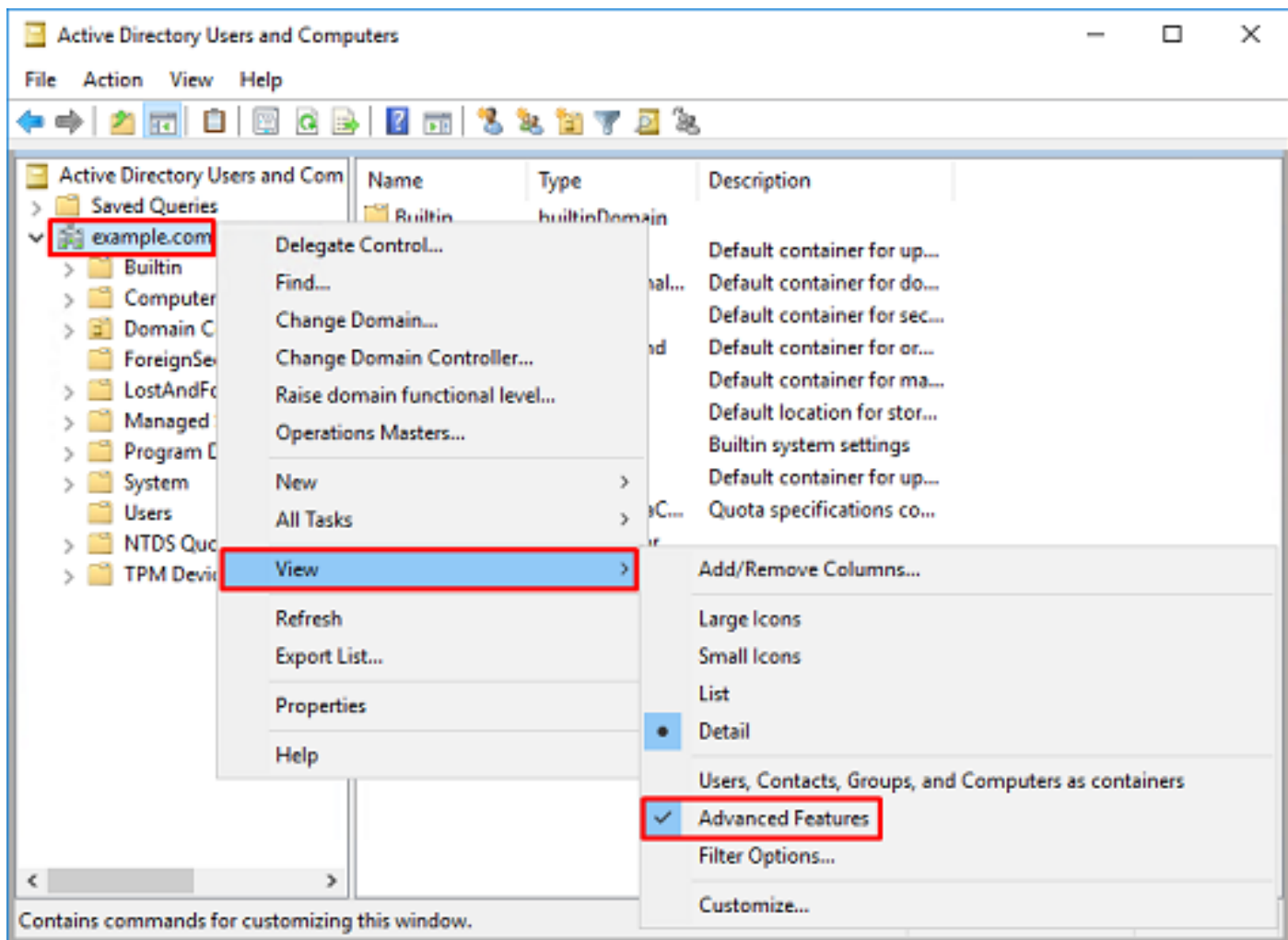


Questa operazione può essere eseguita per più oggetti all'interno di AD. Ad esempio, questi passaggi vengono utilizzati per trovare il DN del contenitore Utente:





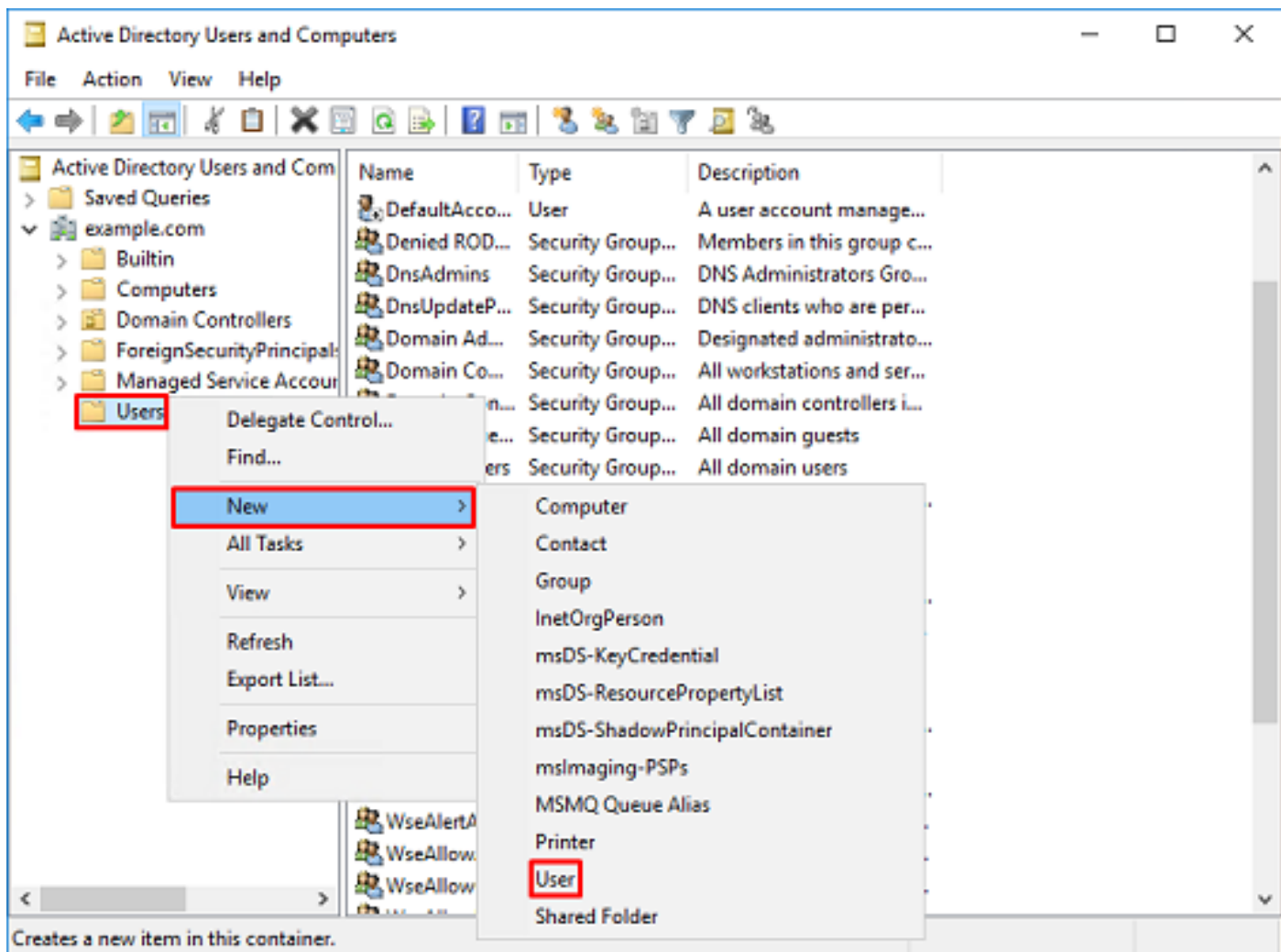
6. È possibile rimuovere la vista Funzioni avanzate. Fare clic con il pulsante destro del mouse sul DN radice, passare a **Visualizza** e fare di nuovo clic su **Caratteristiche avanzate**.



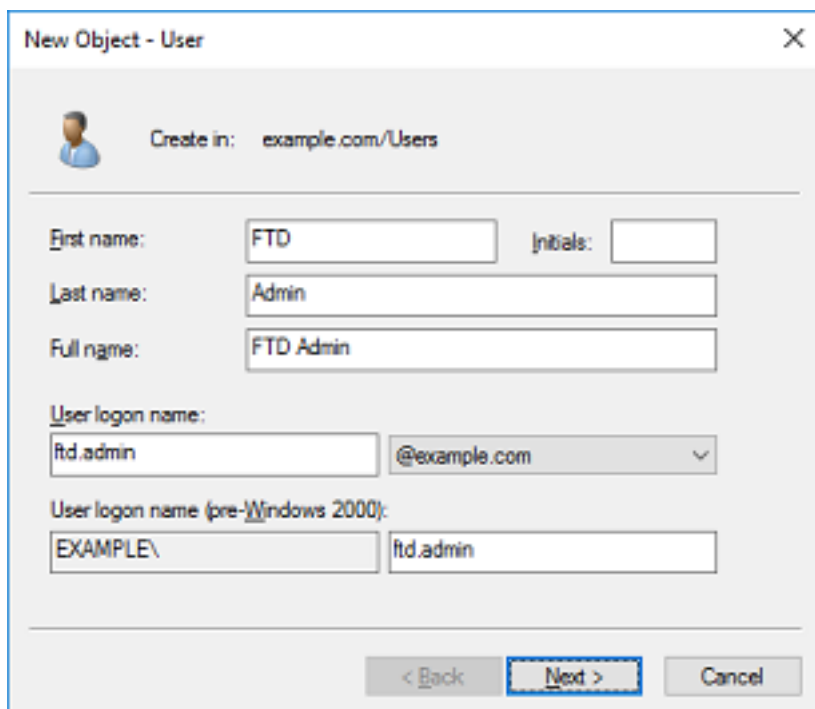
## Crea un account FTD

Questo account utente consente a FDM e FTD di eseguire il binding con AD per cercare utenti e gruppi e autenticarli. Lo scopo della creazione di un account FTD separato è quello di impedire l'accesso non autorizzato in altre parti della rete se le credenziali utilizzate per il binding sono compromesse. Non è necessario che l'account rientri nell'ambito del DN di base.

1. In **Utenti e computer di Active Directory**, fare clic con il pulsante destro del mouse sul contenitore/organizzazione a cui verrà aggiunto l'account FTD. In questa configurazione, l'account FTD verrà aggiunto nel contenitore Utenti sotto il nome utente **ftd.admin@example.com**. Fare clic con il pulsante destro del mouse su **Utenti**, quindi scegliere **Nuovo > Utente**.



2. Spostarsi nella Creazione guidata Nuovo oggetto - Utente.



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

New Object - User

Create in: example.com/Users

When you click Finish, the following object will be created:

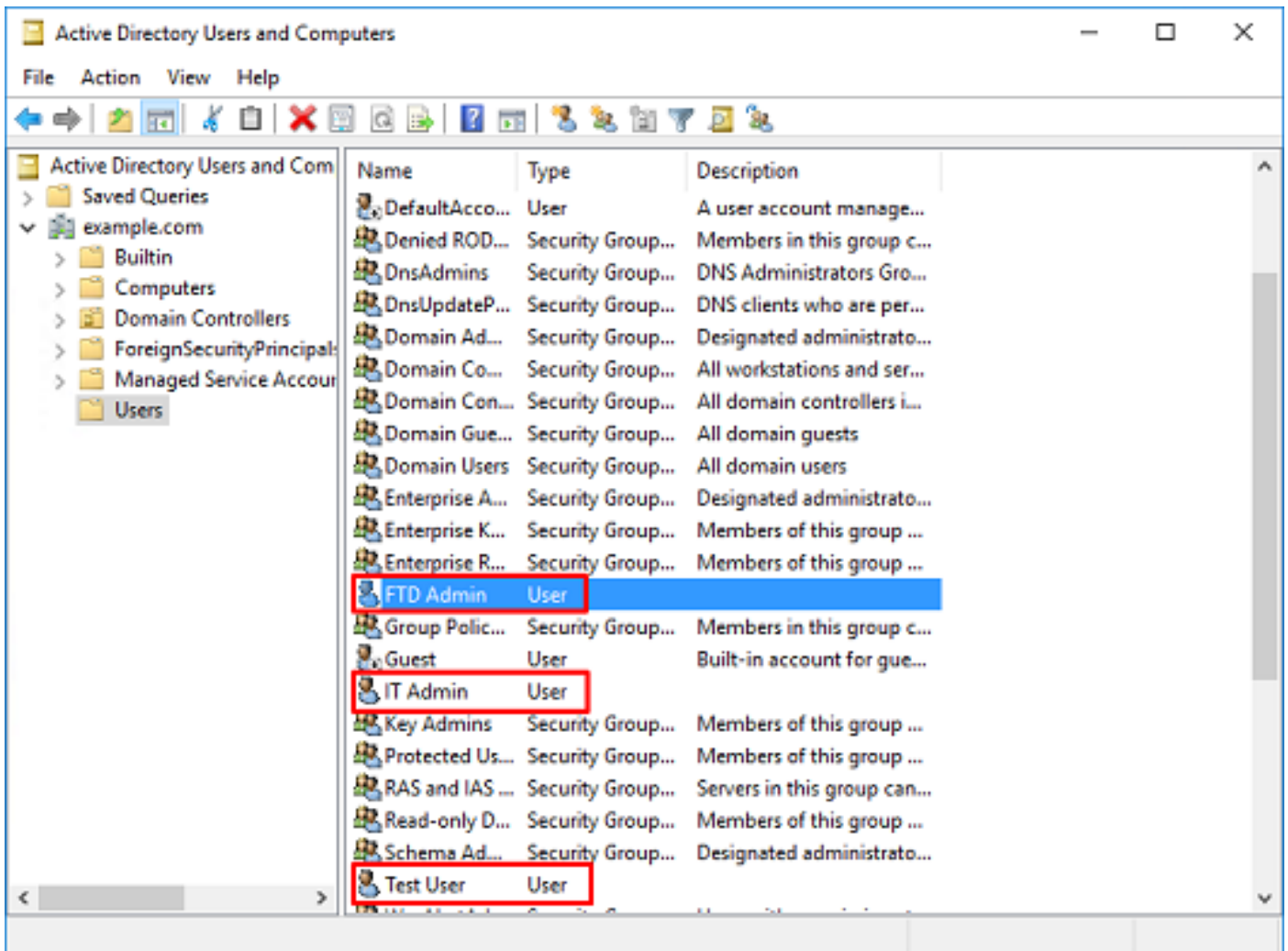
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

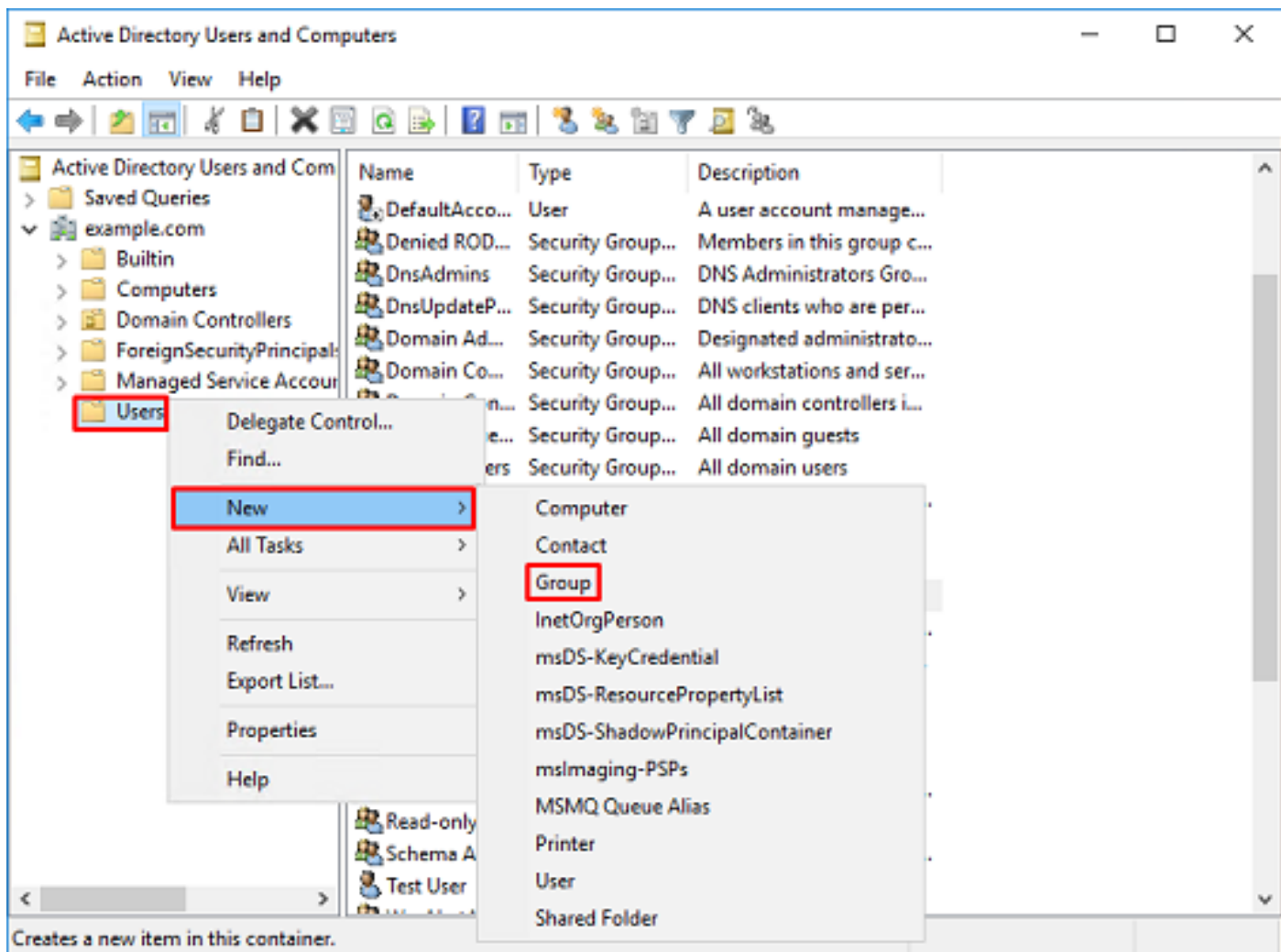
3. Verificare che il conto FTD sia stato creato. Sono stati inoltre creati due account aggiuntivi, **IT Admin** e **Test User**.



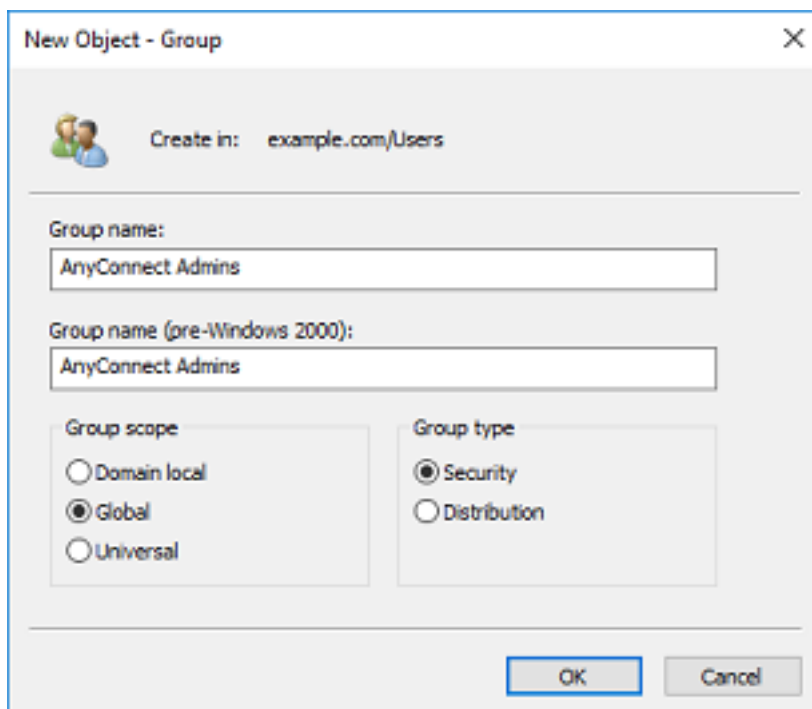
## Creare gruppi AD e aggiungere utenti ai gruppi AD (facoltativo)

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 verranno utilizzati per applicare le impostazioni dei criteri di controllo di accesso in un secondo momento tramite l'identità dell'utente in FDM.

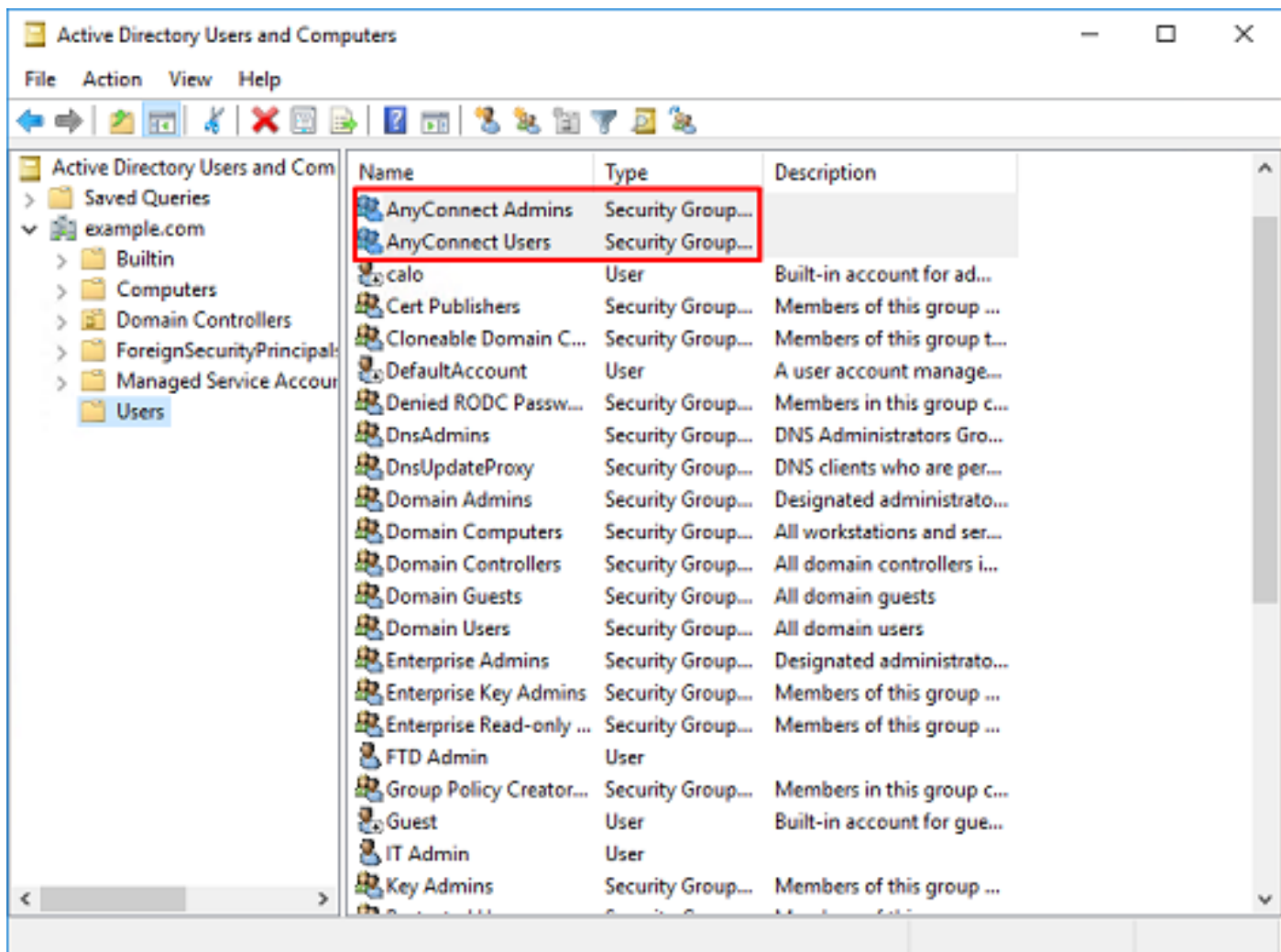
1. In **Utenti e computer di Active Directory**, fare clic con il pulsante destro del mouse sul contenitore/organizzazione a cui verrà aggiunto il nuovo gruppo. Nell'esempio, il gruppo **AnyConnect Admins** verrà aggiunto nel contenitore **Users**. Fare clic con il pulsante destro del mouse su **Utenti**, quindi scegliere **Nuovo > Gruppo**.



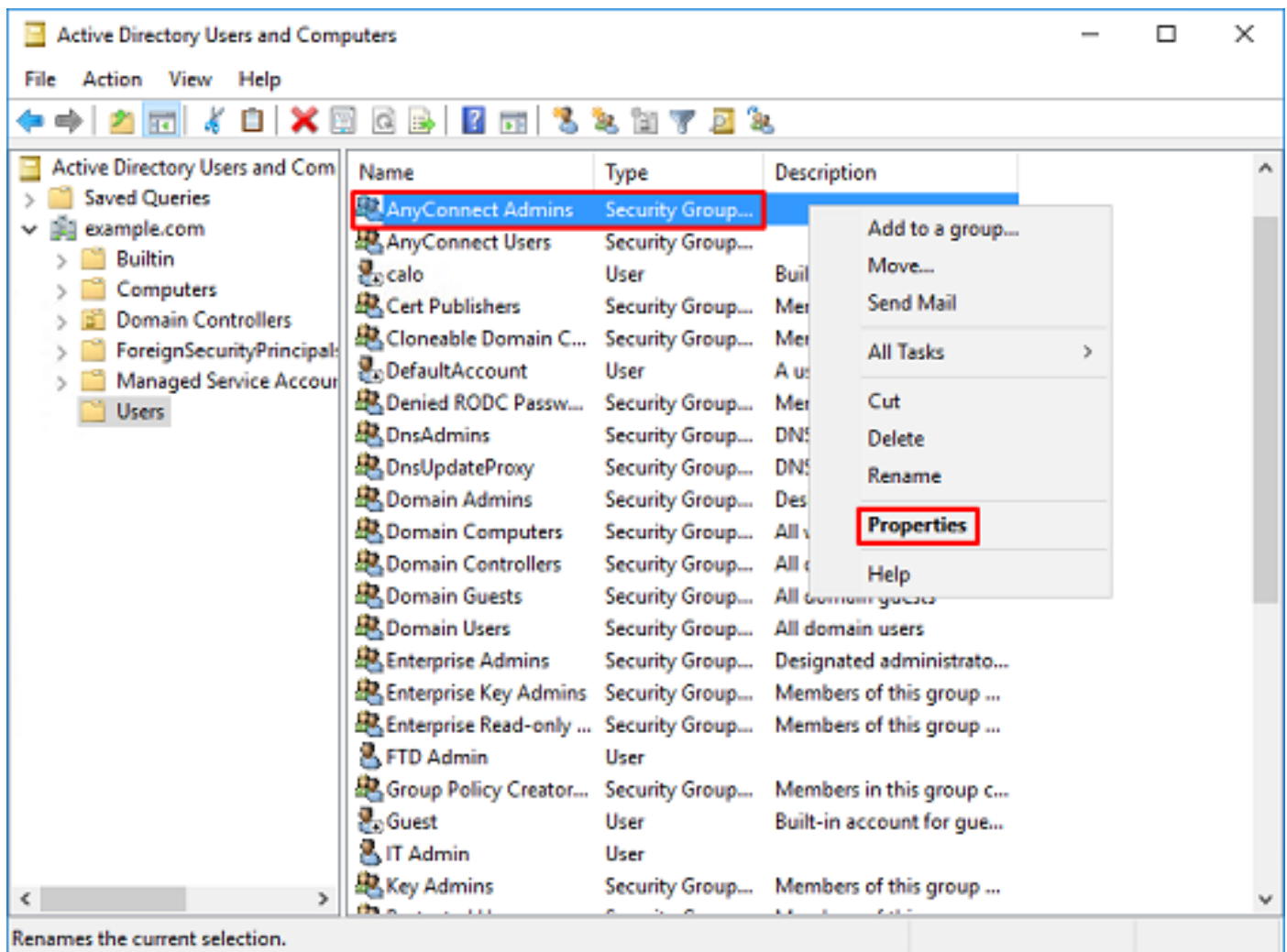
2. Spostarsi nella Creazione guidata Nuovo oggetto - Gruppo come mostrato nell'immagine.



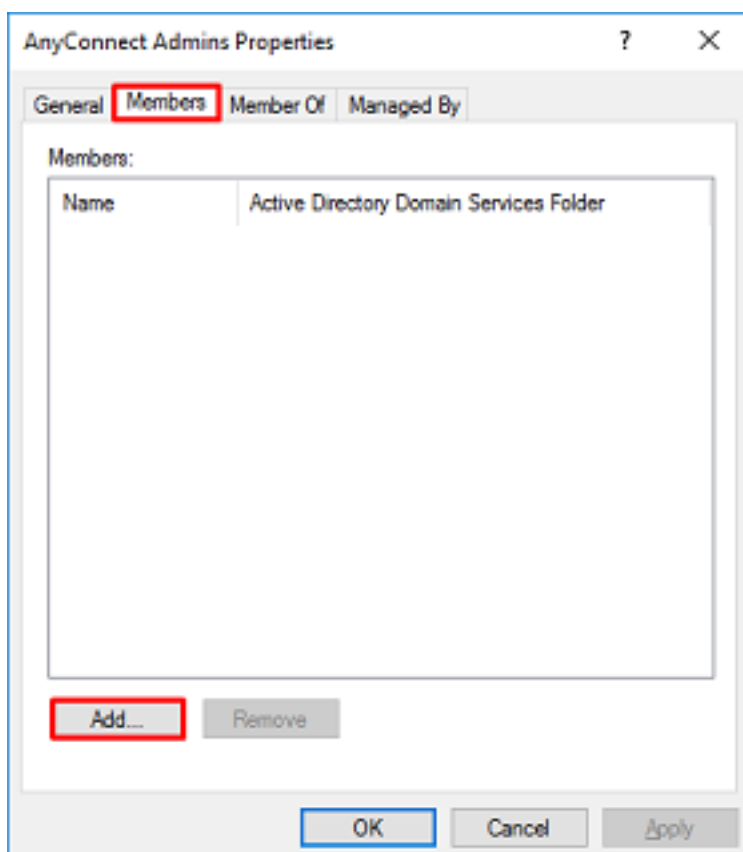
3. Verificare che il gruppo sia stato creato. È stato inoltre creato il gruppo **AnyConnect Users**.



4. Fare clic con il pulsante destro del mouse sul gruppo a cui verranno aggiunti gli utenti, quindi selezionare **Proprietà**. In questa configurazione, l'utente **IT Admin** verrà aggiunto al gruppo **AnyConnect Admins** e l'utente **Test User** verrà aggiunto al gruppo **AnyConnect Users**.

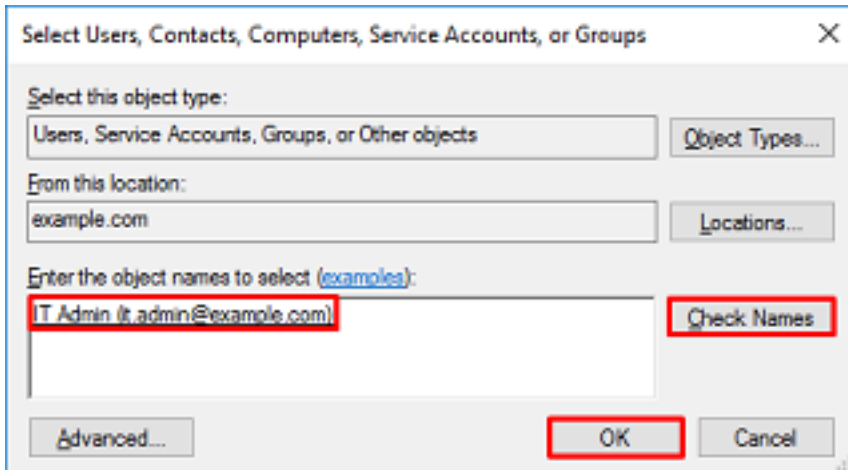


5. Fare clic sulla scheda **Membri**, quindi fare clic su **Aggiungi** come mostrato nell'immagine.

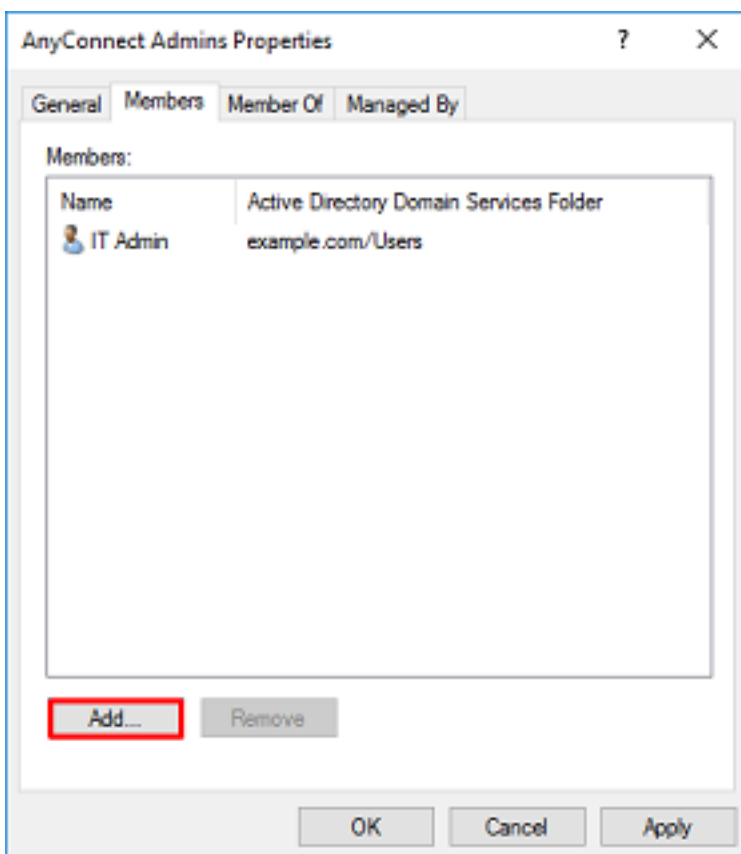




Immettere l'utente nel campo e fare clic sul pulsante **Controlla nomi** per verificare che l'utente sia stato trovato. Dopo la verifica, fare clic su **OK**.

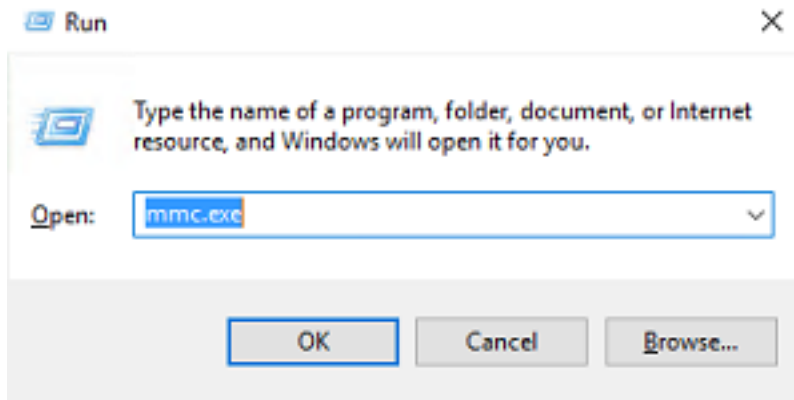


Verificare che sia stato aggiunto l'utente corretto, quindi fare clic sul pulsante **OK**. L'utente Test User viene aggiunto anche al gruppo AnyConnect Users seguendo la stessa procedura.

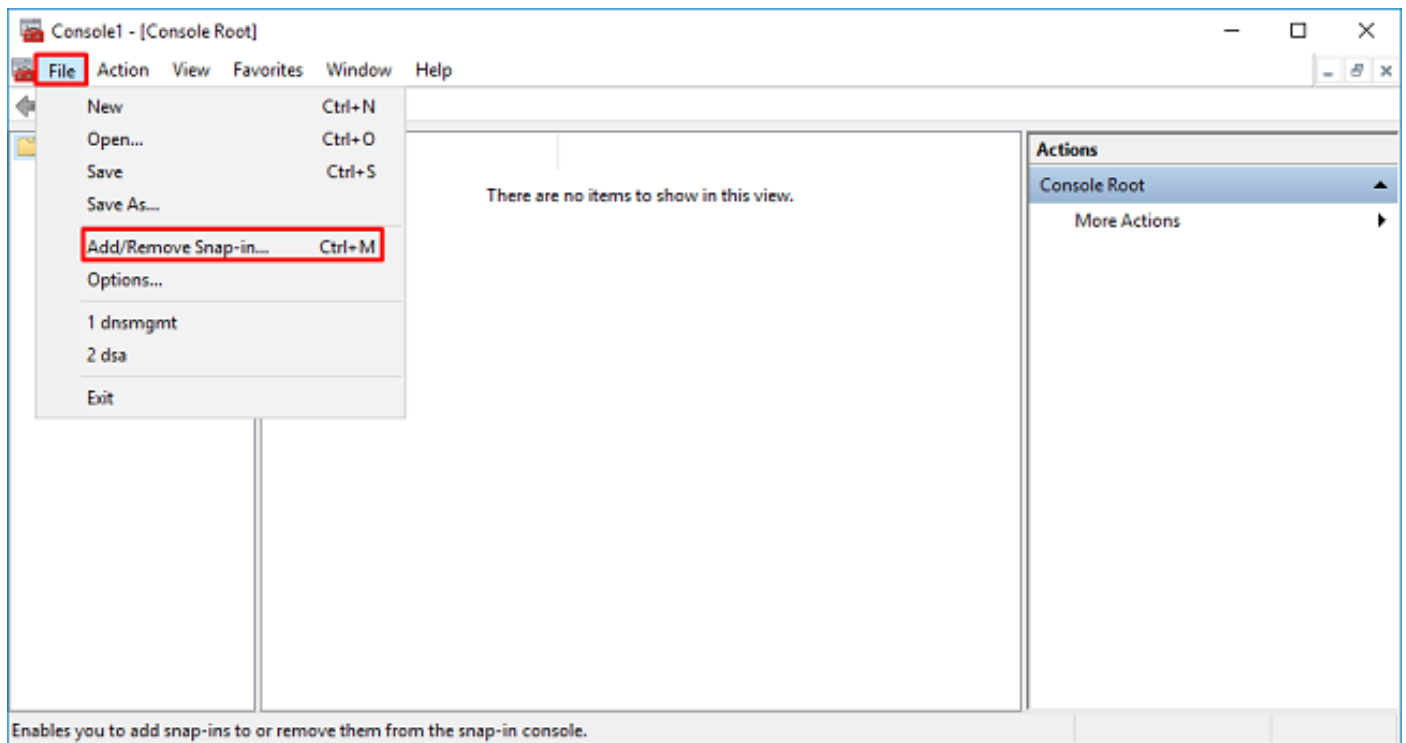


**Copia radice certificato SSL LDAPS (richiesto solo per LDAPS o STARTTLS)**

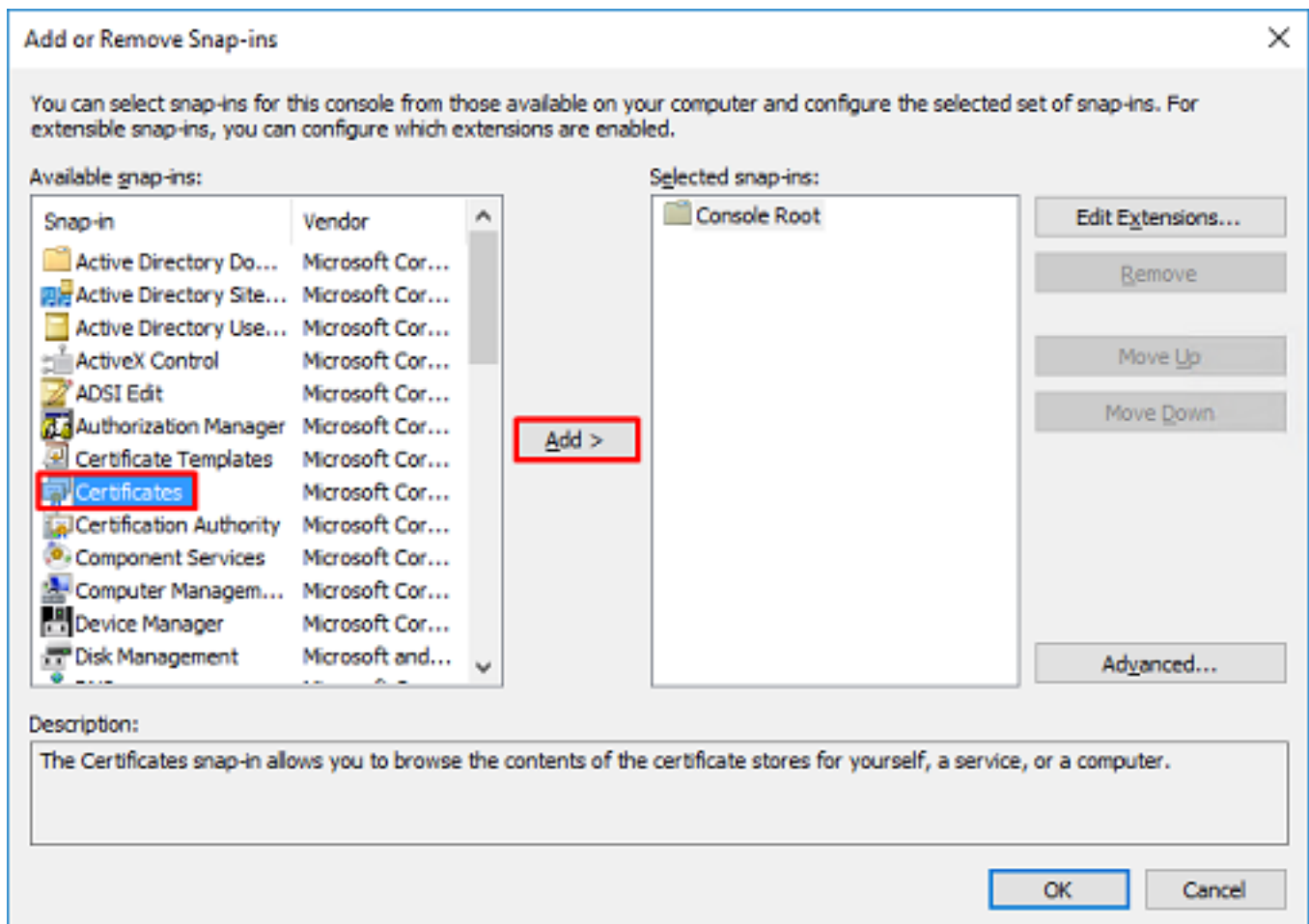
1. Premere **Win+R** e digitare **mmc.exe**. Fare clic su **OK**.



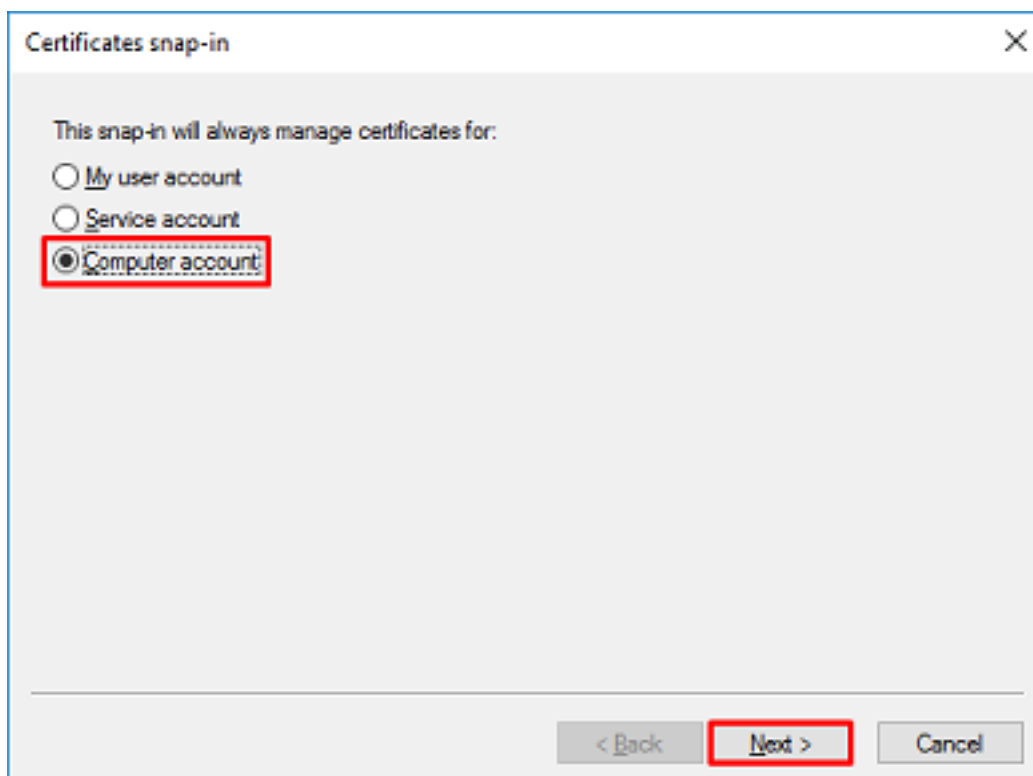
2. Passare a **File > Aggiungi/Rimuovi snap-in...** come mostrato nell'immagine.



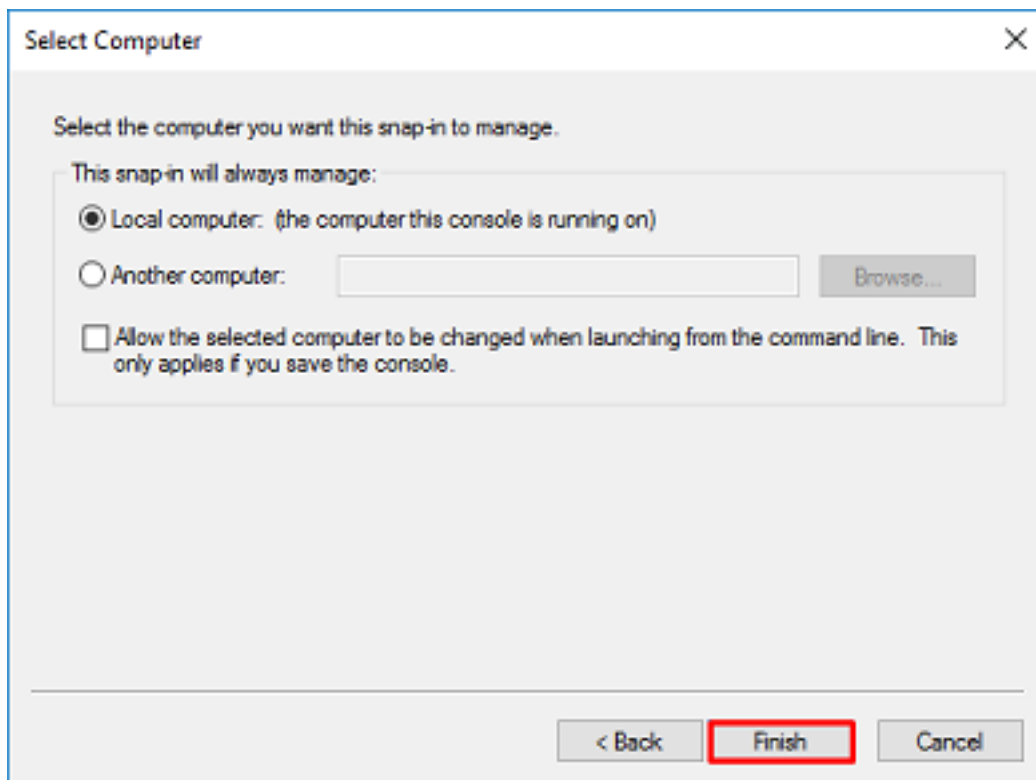
3. In snap-in disponibili fare clic su **Certificati**, quindi su **Aggiungi**.



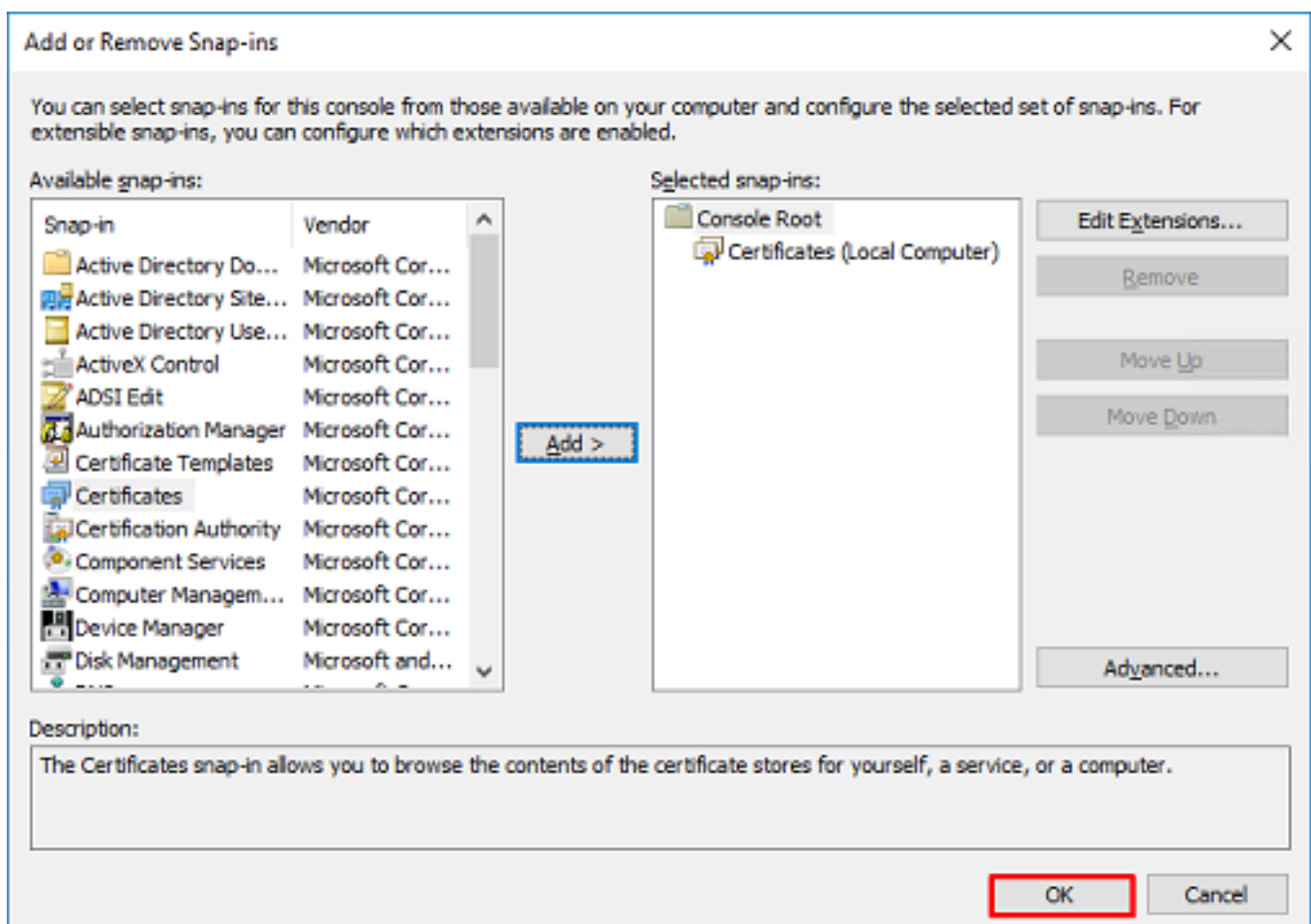
4. Selezionare **Account computer**, quindi fare clic su **Avanti** come mostrato nell'immagine.



Fare clic su **Finish** (Fine).



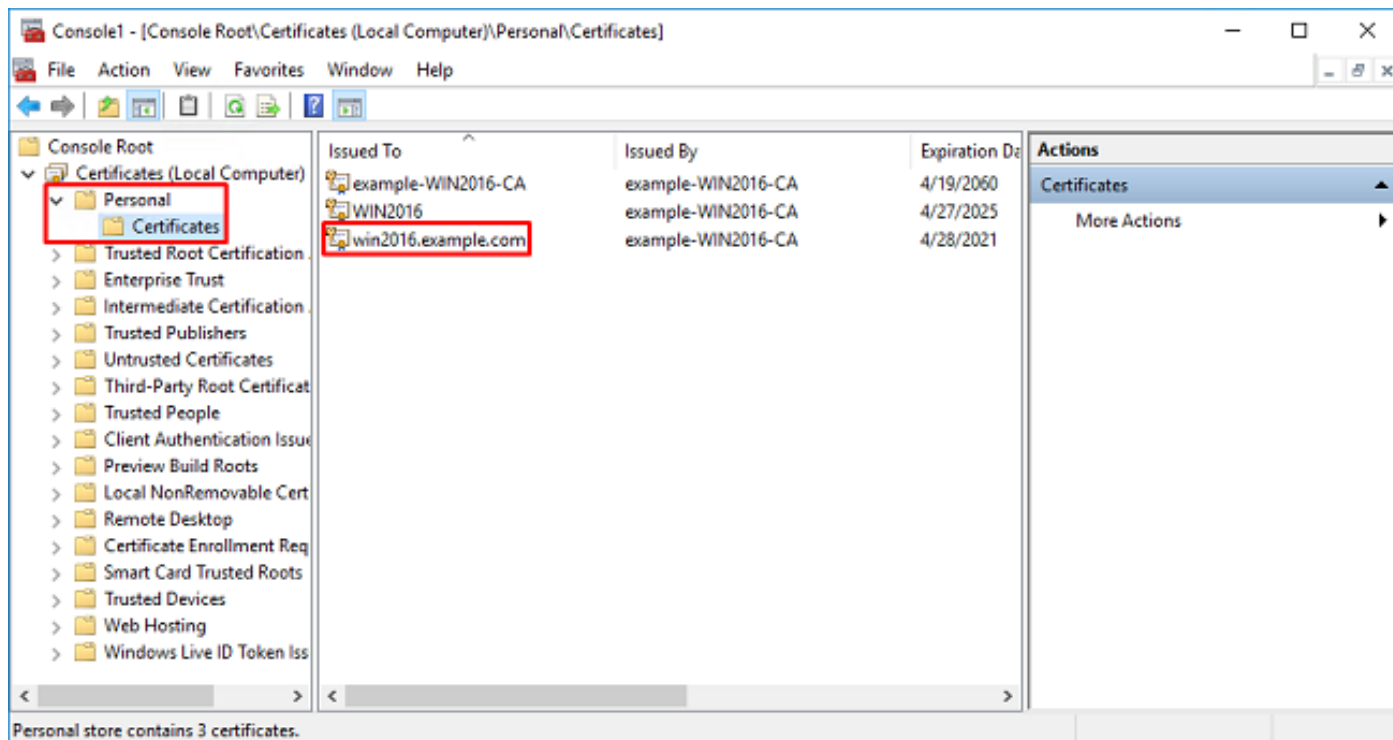
5. Fare clic su OK.



6. Espandere la cartella **Personale**, quindi fare clic su **Certificati**. Il certificato utilizzato da LDAPS deve essere 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.

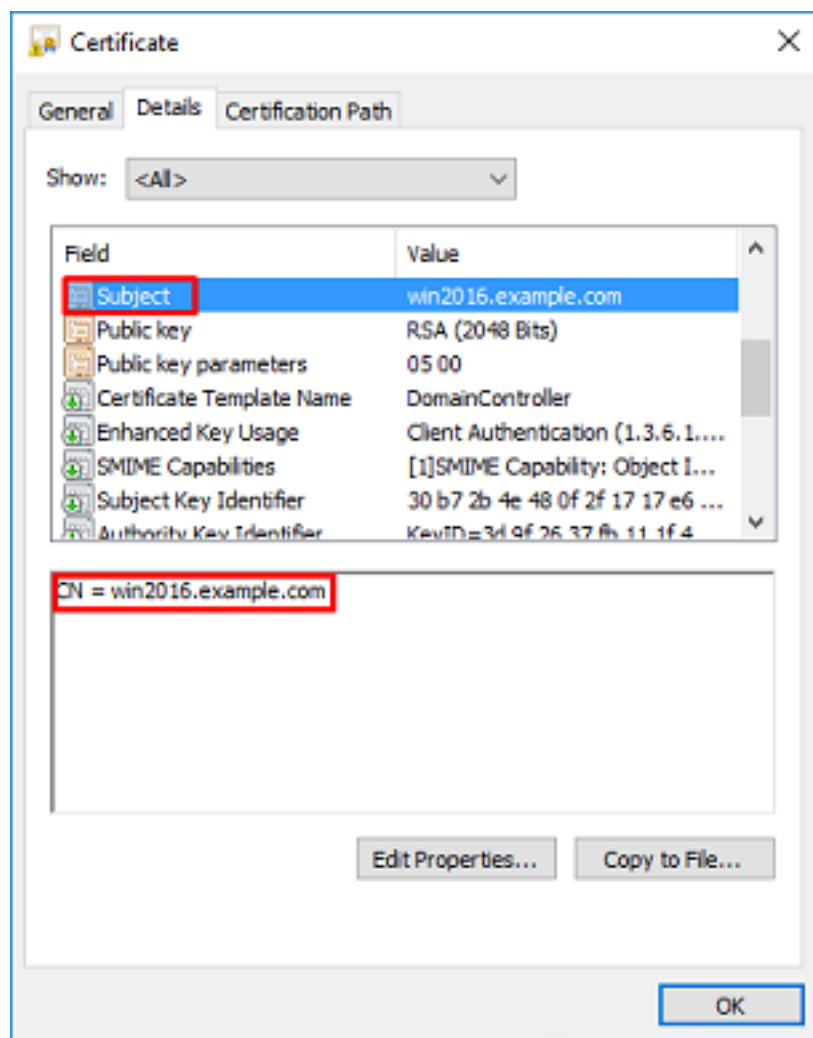
In questa guida alla configurazione, il nome di dominio completo (FQDN) è win2016.example.com, quindi i primi 2 certificati non sono validi per l'utilizzo come certificato SSL LDAPS. Il certificato di identità rilasciato a win2016.example.com è un certificato rilasciato automaticamente dal servizio CA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

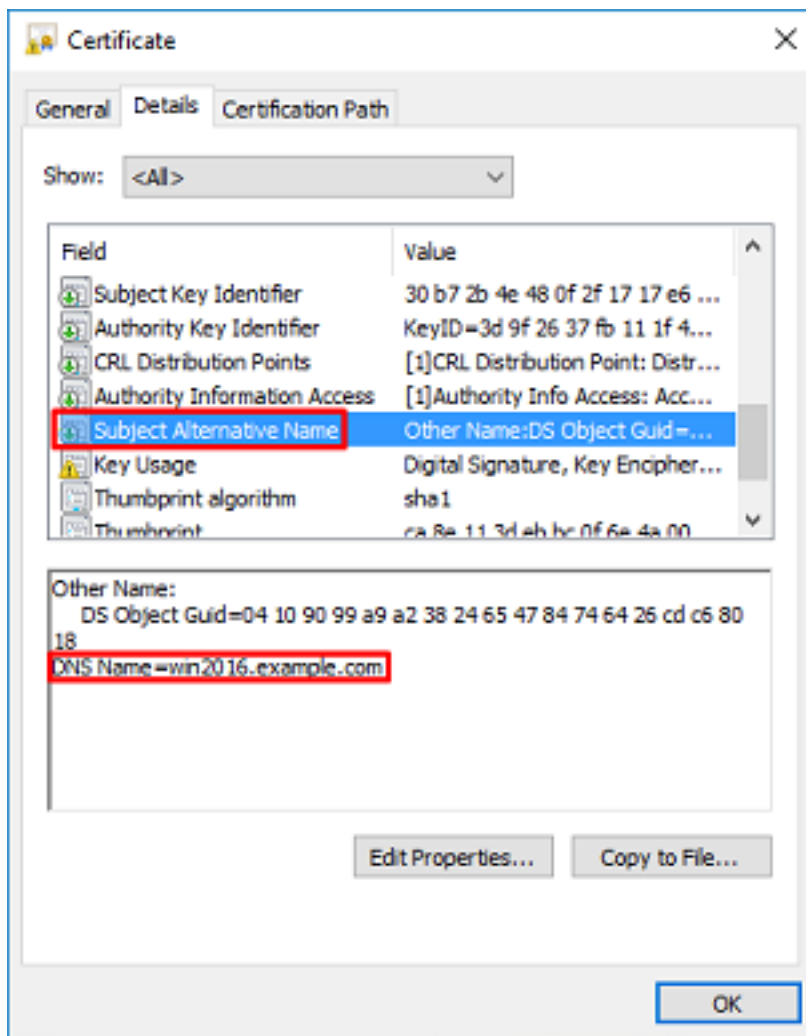


7. Per poter essere utilizzato come certificato SSL LDAPS, il certificato deve soddisfare i seguenti requisiti:

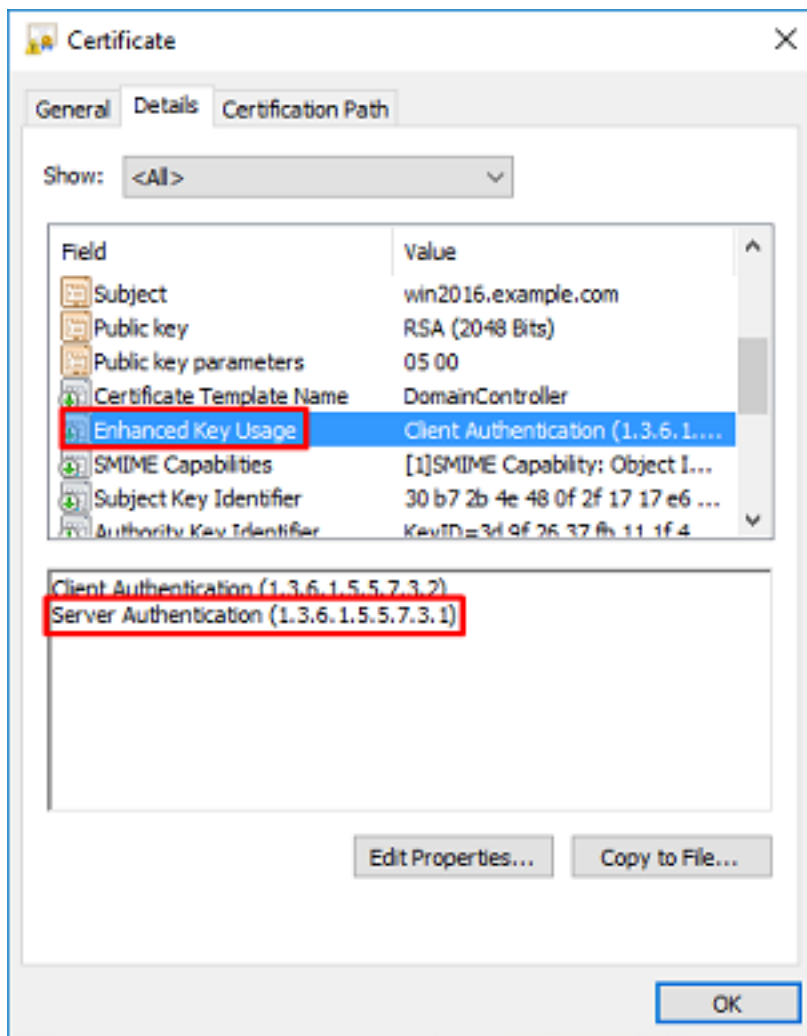
- Il nome comune o il nome alternativo del soggetto DNS corrisponde al nome di dominio completo (FQDN) di Windows Server.
- Nel campo Utilizzo chiavi avanzato del certificato è impostata l'autenticazione server.

Nella scheda Dettagli relativa al certificato, in **Oggetto** e **Nome alternativo soggetto**, è presente il nome di dominio completo (FQDN) **win2016.example.com**.



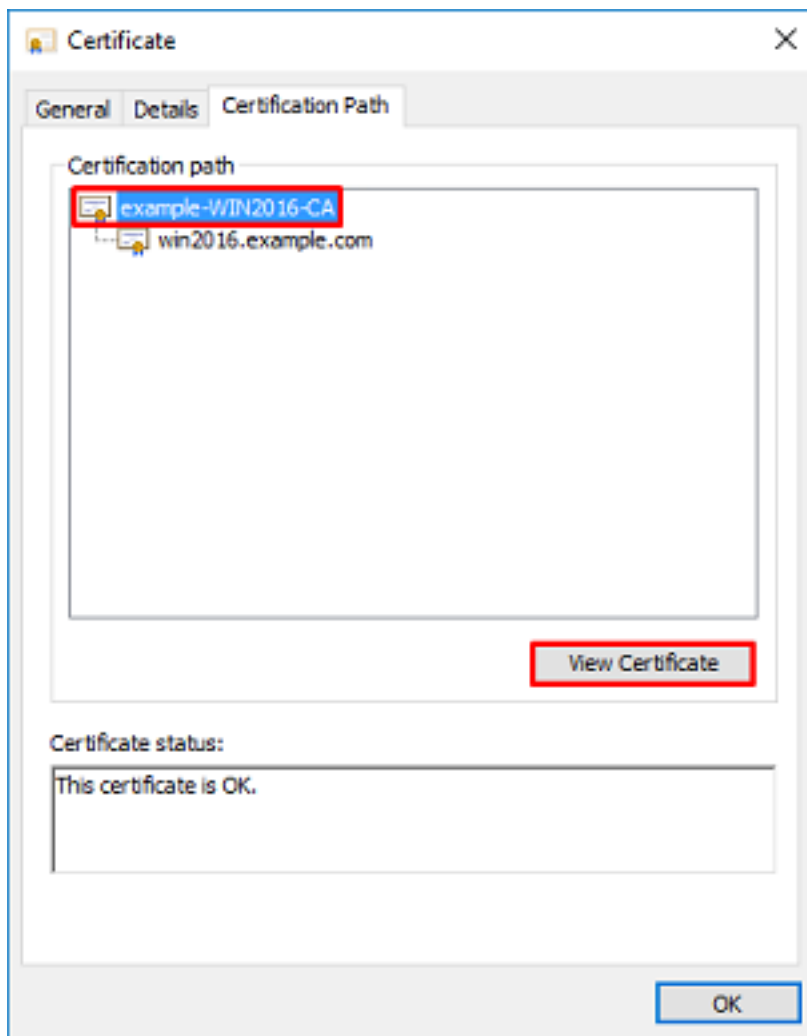


In **Utilizzo chiavi avanzato** è presente **Autenticazione server**.

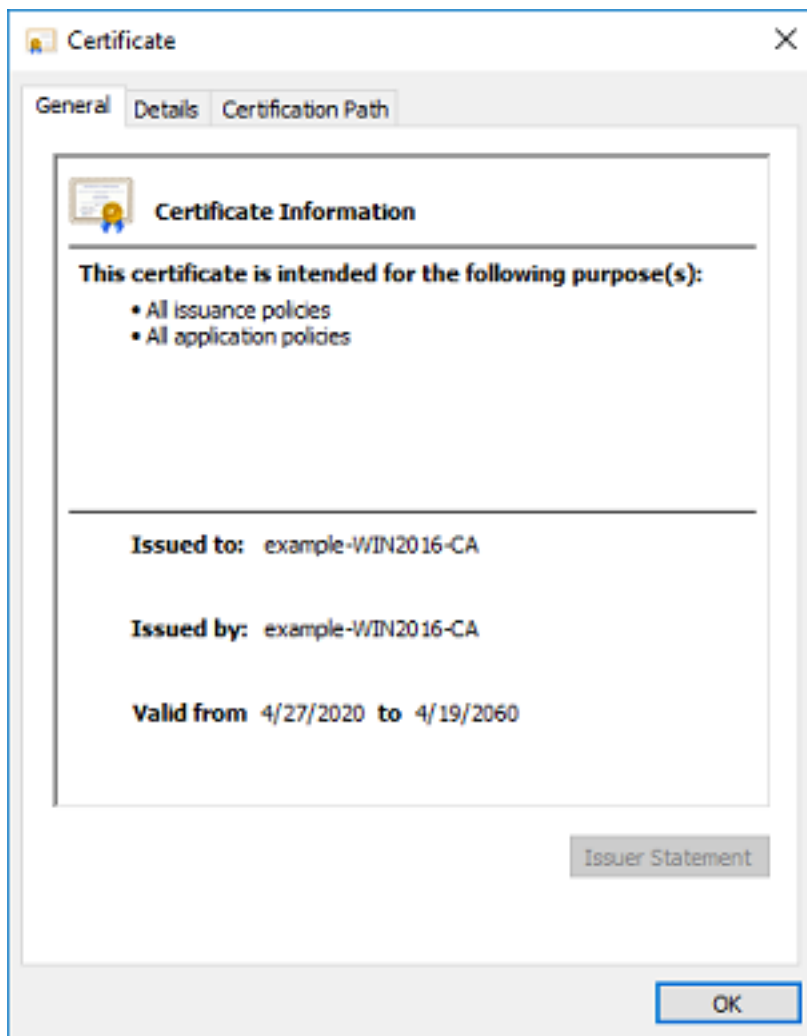


8. Una volta confermato, passare alla scheda **Percorso certificazione**. Fare clic sul primo certificato che deve essere il certificato CA radice, quindi fare clic sul pulsante **Visualizza certificato**.

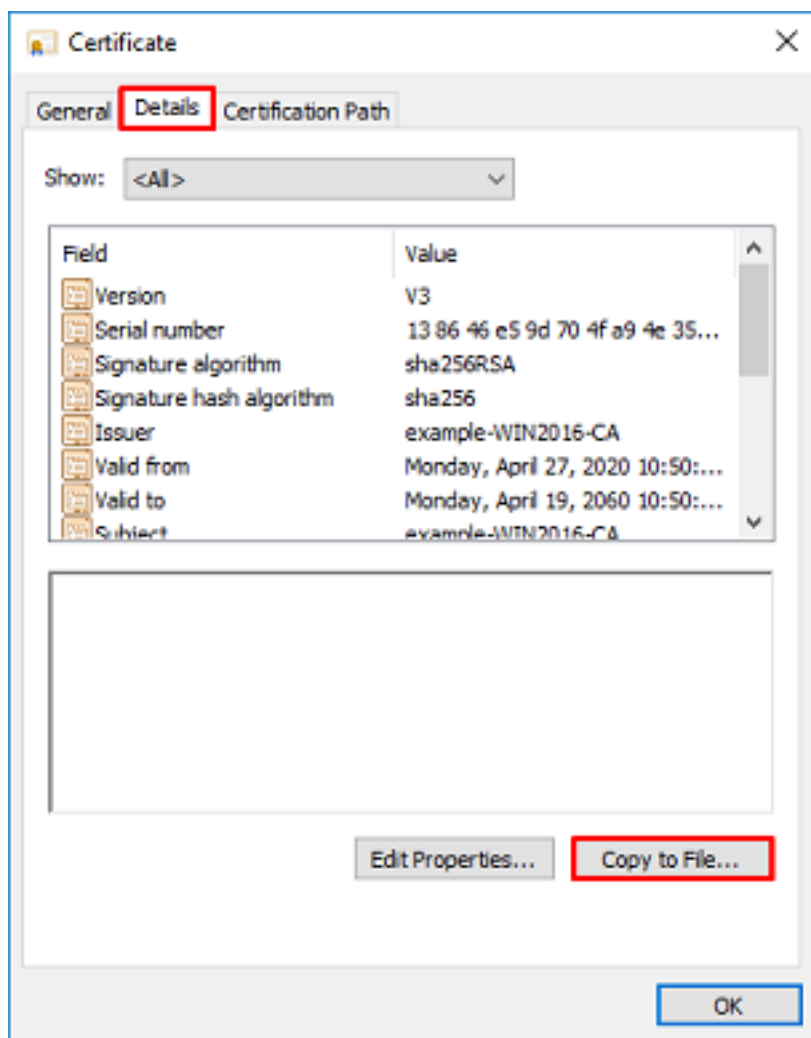




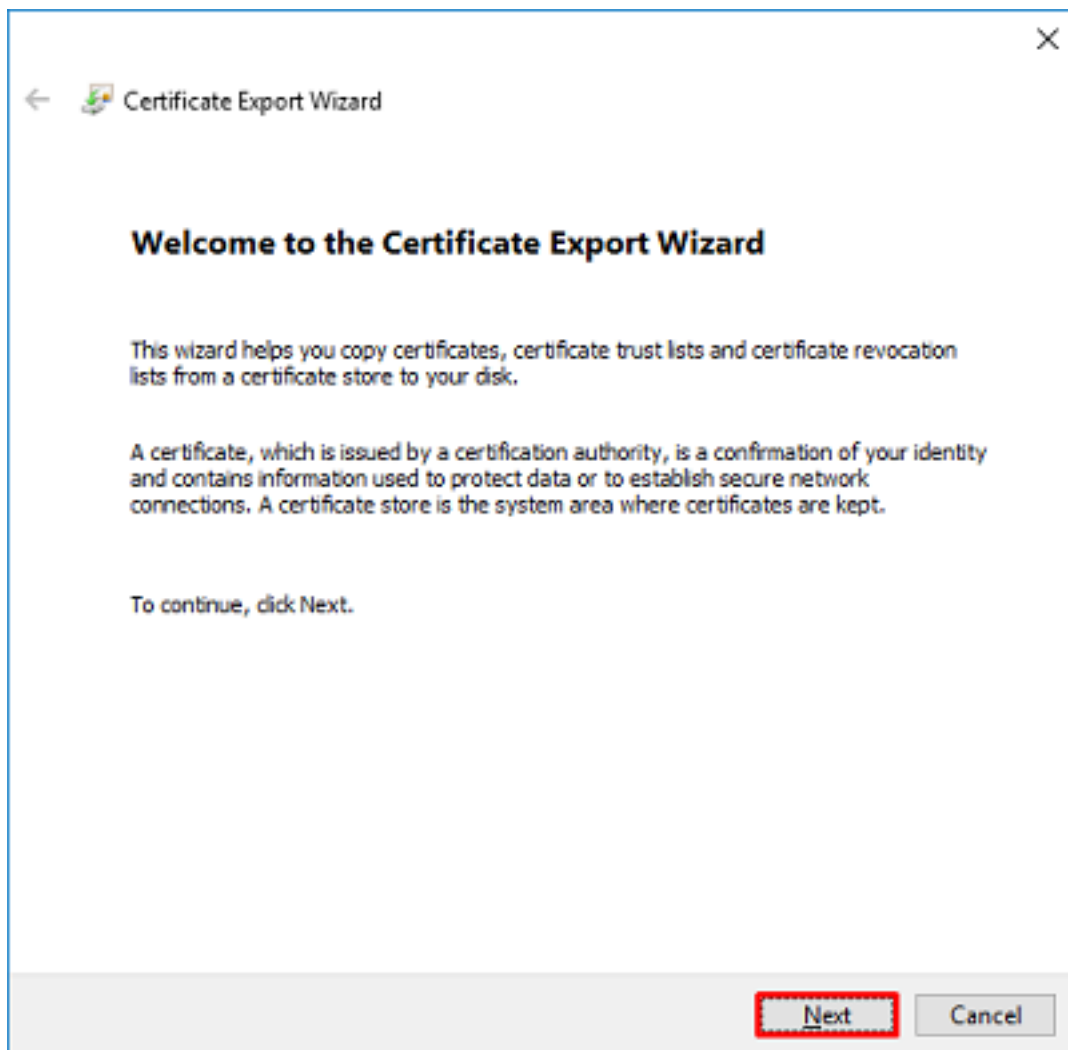
9. Verranno aperti i dettagli del certificato della CA radice.



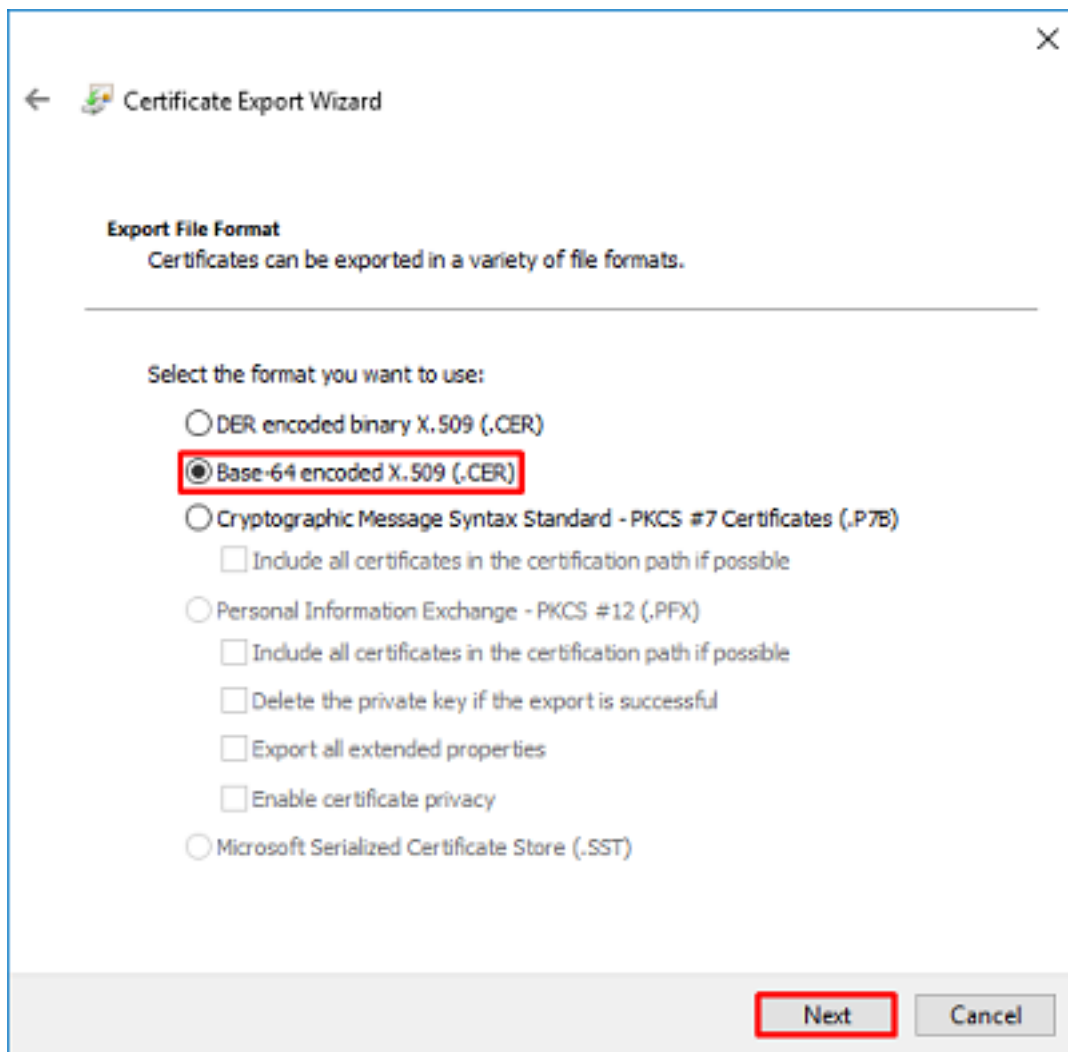
10. Aprire la scheda **Dettagli**, quindi fare clic su **Copia su file...** come mostrato nell'immagine.



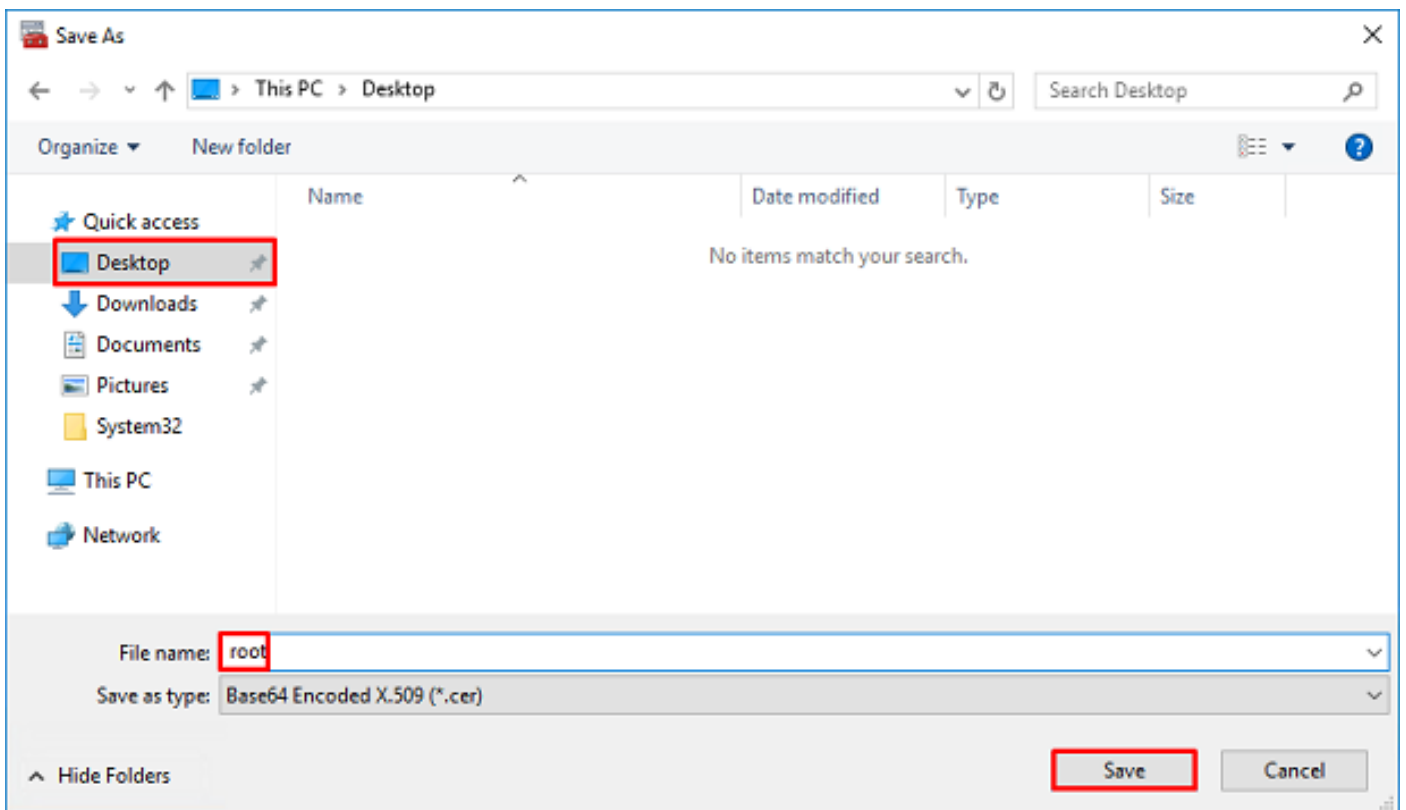
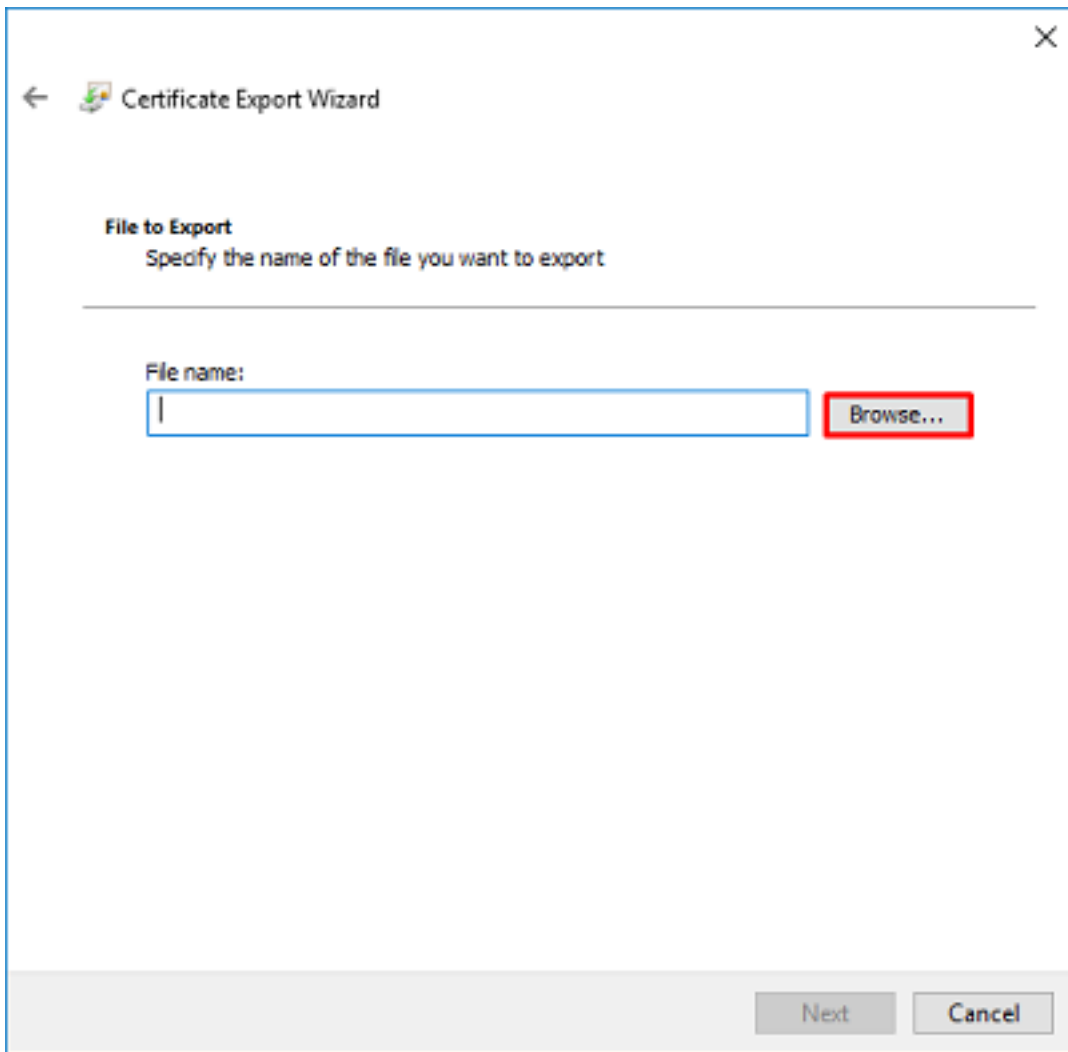
11. Esplorare l'Esportazione guidata certificati per esportare la CA radice in formato PEM.

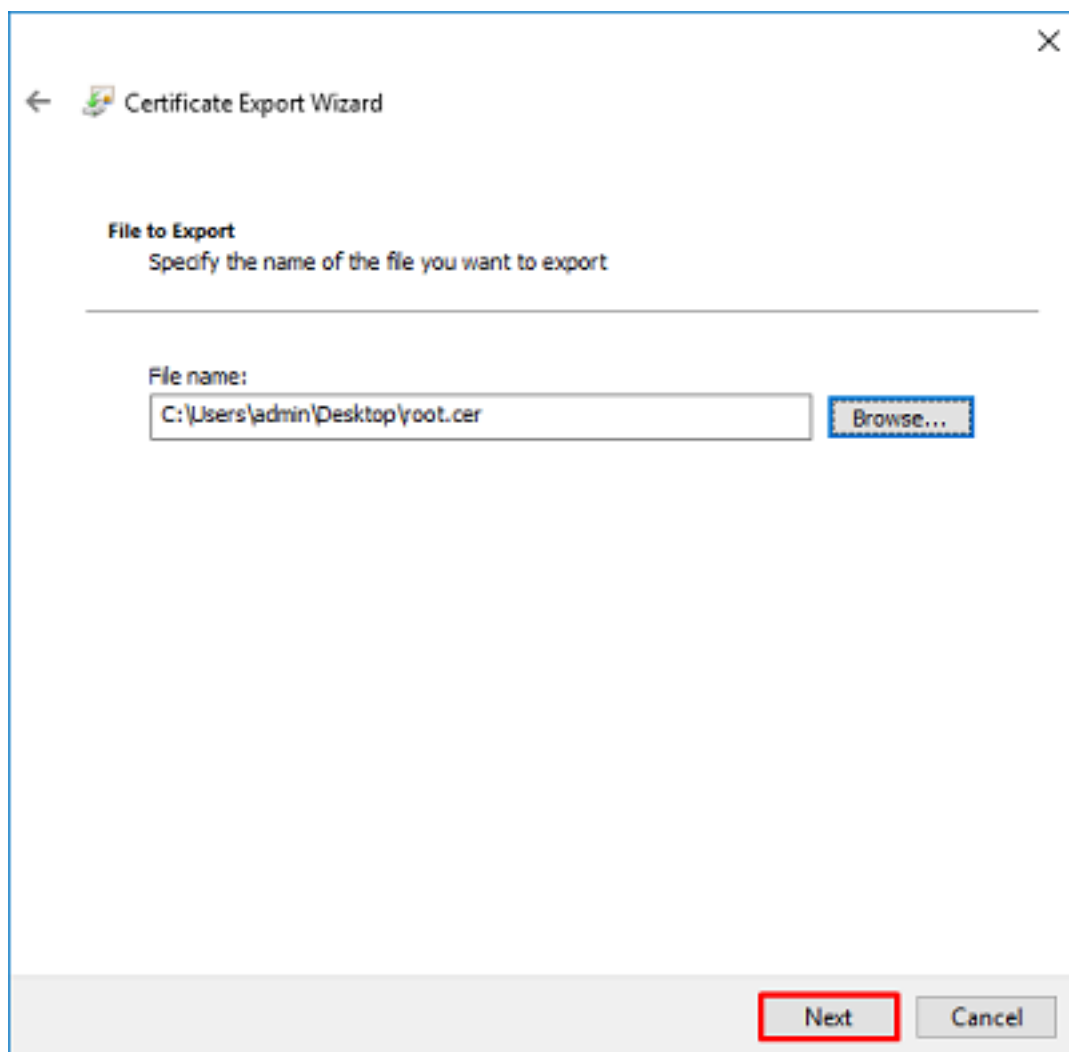


12. Selezionare X.509 con codifica Base 64.

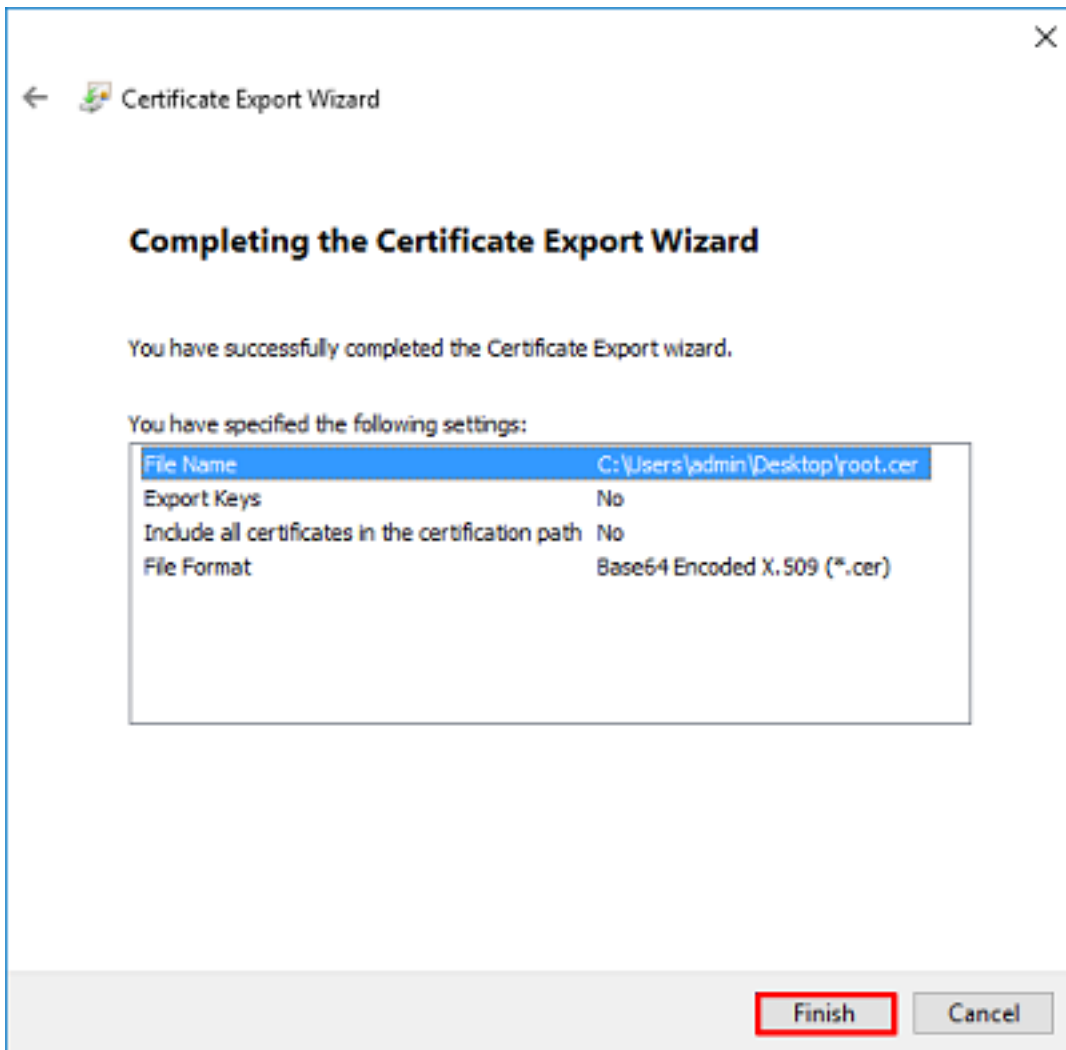


13. Selezionare il nome del file e la destinazione in cui verrà esportato.





14. Fare clic su **Next**.



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

```
-----BEGIN CERTIFICATE-----
MIIDCCCAFcgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1lDQTC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++m+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfKMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgrEtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixwPdrbADO6zMhbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgWBJXEu33PplW6E
-----END CERTIFICATE-----
```

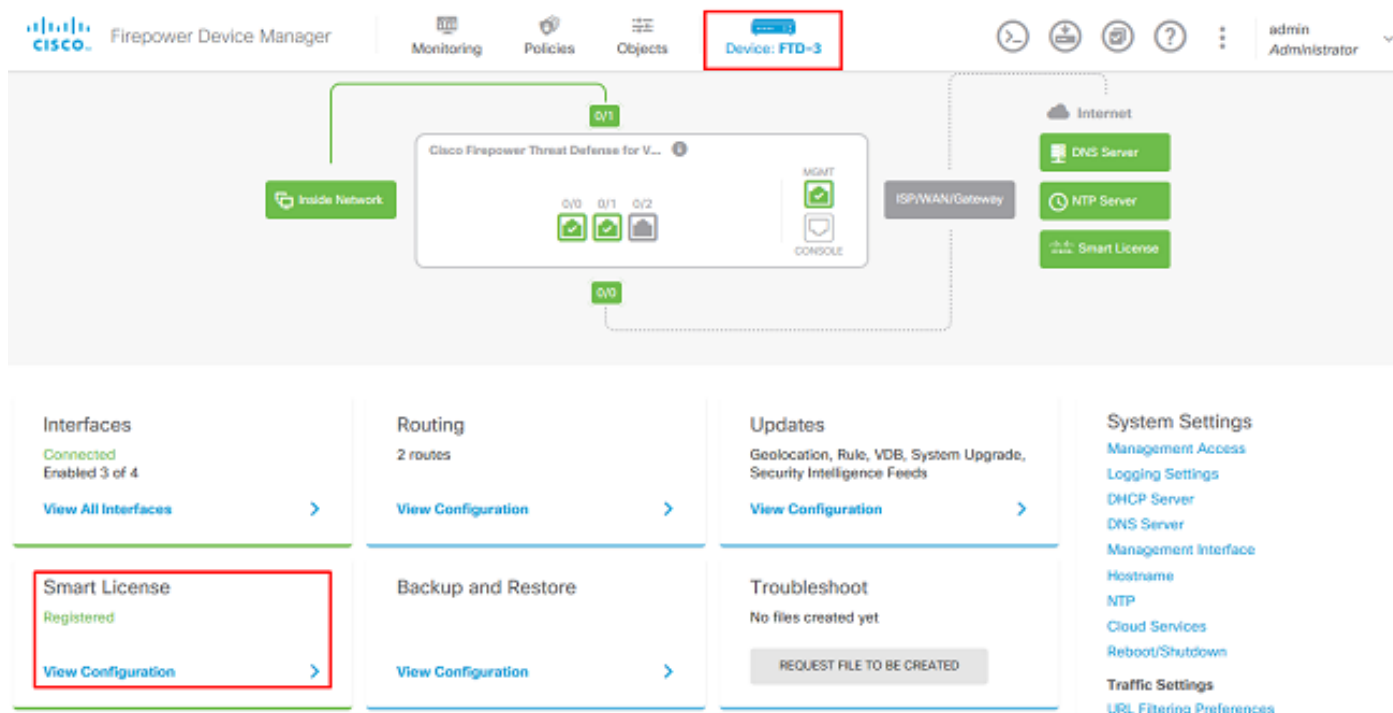
## Configurazioni FDM

### Verifica delle licenze

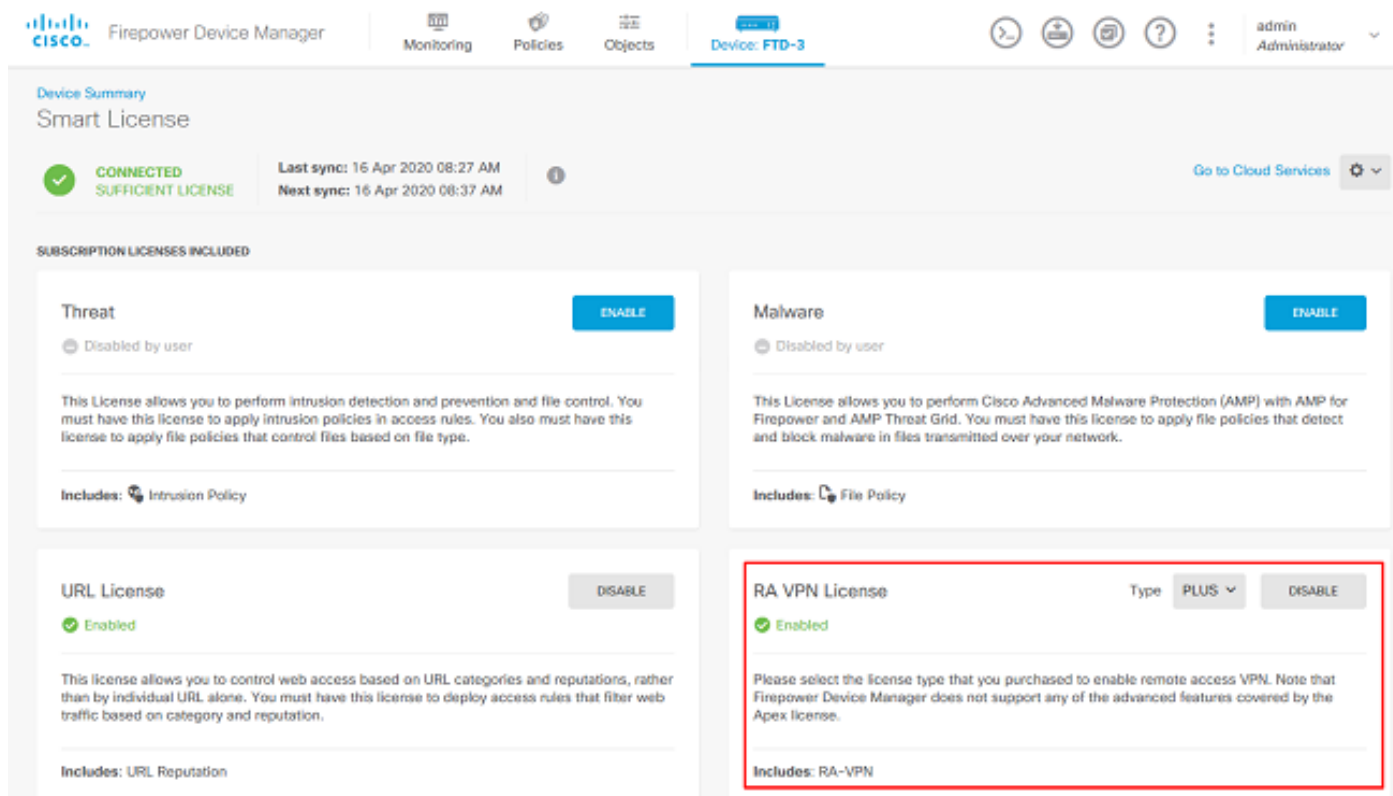


Per configurare AnyConnect su FDM, l'FTD deve essere registrato sul server delle licenze Smart e una licenza Plus, Apex o VPN Only valida deve essere applicata al dispositivo.

1. Passare a **Periferica > Smart License**, come mostrato nell'immagine.



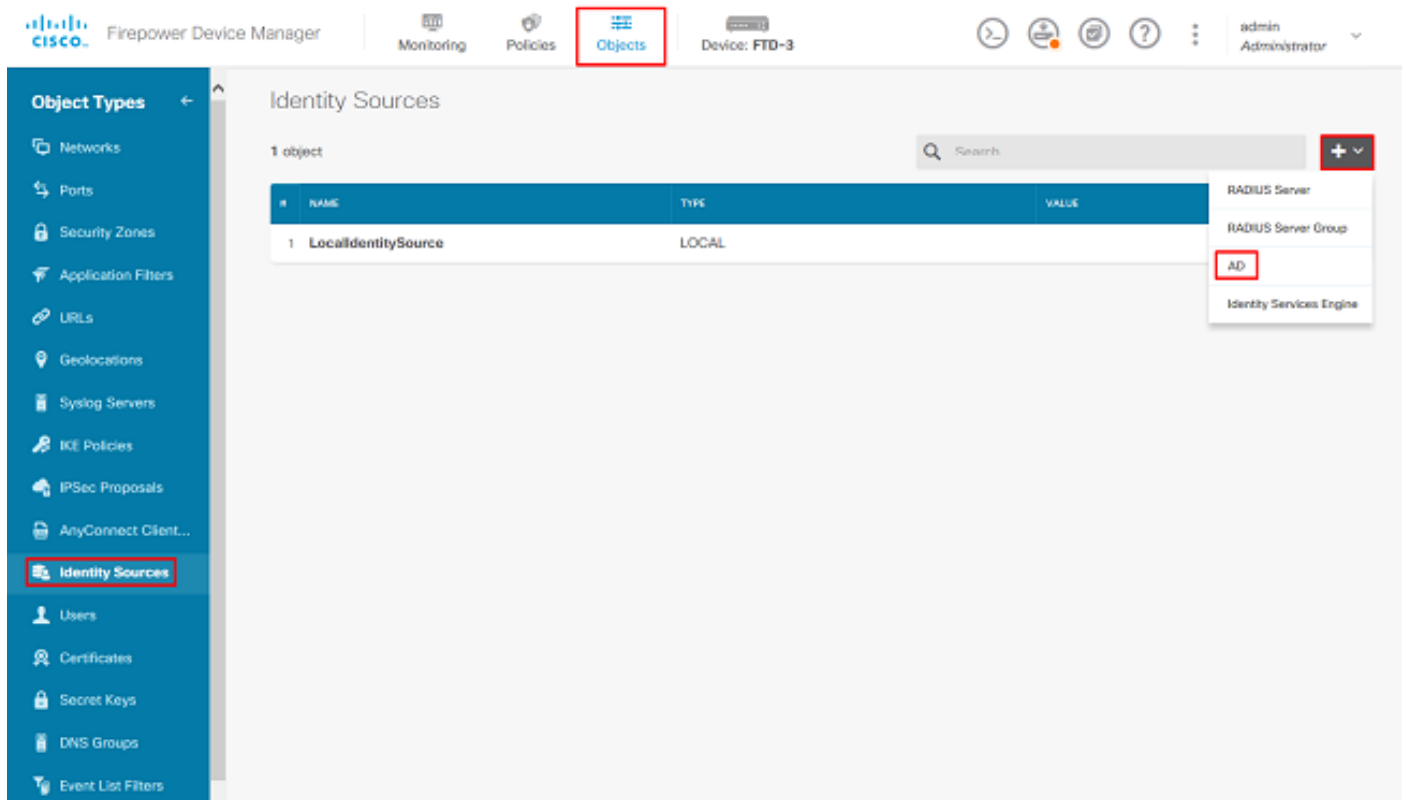
2. Verificare che l'FTD sia registrato sul server delle licenze Smart e che la licenza AnyConnect Plus, Apex o VPN Only sia abilitata.



**Imposta origine identità AD**

1. Passare a **Oggetti > Origini identità**, quindi fare clic sul simbolo + e selezionare **AD** come

mostrato nell'immagine.



2. Specificare le impostazioni appropriate per il server Active Directory con le informazioni raccolte in precedenza. Se per il server Microsoft viene utilizzato un nome host (FQDN) anziché un indirizzo IP, assicurarsi di creare un gruppo DNS appropriato in **Oggetti > Gruppo DNS**. Applicare quindi il gruppo DNS all'FTD passando a **Periferica > Impostazioni di sistema > Server DNS**, applicando il gruppo DNS nell'**interfaccia di gestione** e nell'**interfaccia dati** e quindi specificare l'interfaccia di uscita appropriata per le query DNS. Fare clic sul pulsante **Test** per verificare la corretta configurazione e la raggiungibilità dall'interfaccia di gestione dell'FTD. Poiché questi test vengono avviati dall'interfaccia di gestione dell'FTD 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, in quanto le richieste di autenticazione LDAP AnyConnect verranno avviate da una delle interfacce instradabili dell'FTD. Per ulteriori informazioni sul test delle connessioni LDAP dall'FTD, consultare le sezioni Test AAA e Packet Capture nell'area Risoluzione dei problemi.

# Add Identity Realm



**!** Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name	Type
LAB-AD	Active Directory (AD)
Directory Username	Directory Password
ftd.admin@example.com <small>e.g. user@example.com</small>	••••••••
Base DN	AD Primary Domain
DC=example,DC=com <small>e.g. ou=user, dc=example, dc=com</small>	example.com <small>e.g. example.com</small>

## Directory Server Configuration

win2016.example.com:389

Hostname / IP Address	Port
win2016.example.com <small>e.g. ad.example.com</small>	389
Encryption	Trusted CA certificate
NONE	Please select a certificate

**TEST** ✓ Connection to realm is successful

[Add another configuration](#)

CANCEL

OK

Se si utilizza LDAPS o STARTTLS, selezionare la crittografia appropriata, quindi il certificato CA attendibile. Se la CA radice non è già stata aggiunta, fare clic su **Crea nuovo certificato CA attendibile**. Specificare un nome per il certificato CA radice, quindi incollare il certificato CA radice in formato PEM raccolto in precedenza.

## Add Trusted CA Certificate ? ✕

Name

LDAPS\_ROOT

Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.


```

-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExJleGFtcG9uLmVudjEwMTYtQ0EwIENMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC
AStwDQYJKoZIhvcNAQEFBQADQgEPADCCAQoCggEFAI8chT719NzS0ncOPh0YT67h

```

CANCEL OK

### Directory Server Configuration

 **win2016.example.com:636**

---

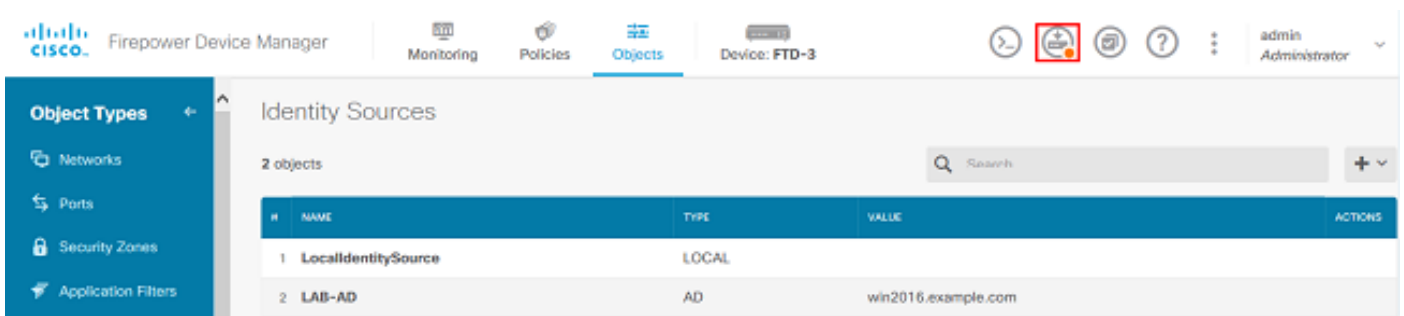
<p>Hostname / IP Address</p> <p style="border: 1px solid #ccc; padding: 2px;">win2016.example.com</p> <p><small>e.g. ad.example.com</small></p>	<p>Port</p> <p style="border: 1px solid #ccc; padding: 2px;">636</p>
<p>Encryption</p> <p style="border: 1px solid #ccc; padding: 2px;">LDAPS <span style="float: right;">▼</span></p>	<p>Trusted CA certificate</p> <p style="border: 1px solid #ccc; padding: 2px;">LDAPS_ROOT <span style="float: right;">▼</span></p>

TEST ✓ Connection to realm is successful

In questa configurazione sono stati utilizzati i seguenti valori:

- Nome: LAB-AD
- Nome utente directory: ftd.admin@example.com
- DN di base: DC=esempio,DC=com
- Dominio primario AD: example.com
- Nome host/Indirizzo IP: win2016.example.com
- Port: 389

3. Fare clic sul pulsante **Modifiche in sospeso** in alto a destra, come mostrato nell'immagine.



The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FTD-3'. The 'Objects' tab is active. On the right side of the top bar, there is a red box highlighting a button with a circular arrow icon, which is the 'Modifiche in sospeso' (Save Changes) button. Below the navigation bar, the 'Identity Sources' section is visible, showing a table with 2 objects:

#	NAME	TYPE	VALUE	ACTIONS
1	LocalIdentitySource	LOCAL		
2	LAB-AD	AD	win2016.example.com	

#### 4. Fare clic sul pulsante **Distribuisci**.

**Pending Changes**

✓ **Last Deployment Completed Successfully**  
01 May 2020 12:54 PM. [See Deployment History](#)

Deployed Version (01 May 2020 12:54 PM) | Pending Version **LEGEND** Removed Added Edited

+ **Active Directory Realm Added: LAB-AD**

```
dirPassword.masked: false
dirPassword.encryptedString: ***
directoryConfigurations[0].port: 389
directoryConfigurations[0].hostname: win2016.example.com
directoryConfigurations[0].encryptionProtocol: NONE
adPrimaryDomain: example.com
dirUsername: ftd.admin@example.com
baseDN: DC=example,DC=com
enabled: true
realmId: 9
name: LAB-AD
```

MORE ACTIONS ▼ | CANCEL | **DEPLOY NOW** ▼

### Configurazione di AnyConnect per l'autenticazione AD

Per utilizzare l'origine dell'identità AD configurata, deve essere applicata alla configurazione AnyConnect.

#### 1. Passare a **Dispositivo > VPN ad accesso remoto** come mostrato nell'immagine.

Firepower Device Manager | Monitoring | Policies | Objects | **Device: FTD-3** | admin Administrator

0/0

<b>Interfaces</b> Connected Enabled 3 of 4 <a href="#">View All Interfaces</a> >	<b>Routing</b> 2 routes <a href="#">View Configuration</a> >	<b>Updates</b> Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds <a href="#">View Configuration</a> >	<b>System Settings</b> Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Reboot/Shutdown <b>Traffic Settings</b> URL Filtering Preferences
<b>Smart License</b> Registered <a href="#">View Configuration</a> >	<b>Backup and Restore</b> <a href="#">View Configuration</a> >	<b>Troubleshoot</b> No files created yet REQUEST FILE TO BE CREATED	<b>Device Administration</b> Audit Events, Deployment History, Download Configuration <a href="#">View Configuration</a> >
<b>Site-to-Site VPN</b> There are no connections yet <a href="#">View Configuration</a> >	<b>Remote Access VPN</b> Configured 1 connection   2 Group Policies <a href="#">View Configuration</a> >	<b>Advanced Configuration</b> Includes: FlexConfig, Smart CLI <a href="#">View Configuration</a> >	

#### 2. Fare clic sul simbolo + o sul pulsante **Crea profilo di connessione** come mostrato nell'immagine.

Firepower Device Manager

Monitoring Policies Objects **Device: FTD-3**

admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

Search

	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

3. Nella sezione Connessione e configurazione client, selezionare l'origine dell'identità AD creata in precedenza. Impostare i valori appropriati per le altre sezioni, inclusi Nome profilo connessione e Assegnazione pool indirizzi client. Al termine, fare clic su **Invia query**.

## Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

### Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

General

### Group Alias

General

[Add Group Alias](#)

### Group URL

[Add Group URL](#)

### Primary Identity Source

#### Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

#### Primary Identity Source for User Authentication

Filter

LocalIdentitySource

LAB-AD

Special-Identities-Realm

[Create new](#)

#### Fallback Local Identity Source ⚠


Please Select Local Identity Source

## Client Address Pool Assignment

### IPv4 Address Pool

Endpoints are provided an address from this pool



 AnyConnect-Pool

### IPv6 Address Pool

Endpoints are provided an address from this pool



### DHCP Servers



CANCEL

SUBMIT QUERY

4. Nella sezione Esperienza utente remota selezionare i Criteri di gruppo appropriati. Per impostazione predefinita, verrà utilizzato **DfltGrpPolicy**. tuttavia, è possibile crearne una diversa.

DfltGrpPolicy

## Policy Group Brief Details

<b>DNS + BANNER</b>		<a href="#">Edit</a>
DNS Server	None	
Banner Text for Authenticated Clients	None	
<b>SESSION SETTINGS</b>		
Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes	
Idle Time / Alert Interval	30 / 1 Minutes	
Simultaneous Login per User	3	
<b>SPLIT TUNNELING</b>		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling	Allow all traffic over tunnel	
<b>ANYCONNECT CLIENT</b>		
AnyConnect Client Profiles	None	

BACK

SUBMIT QUERY

5. Nella sezione Global Settings, specificare almeno il certificato SSL, l'interfaccia esterna e i pacchetti AnyConnect. Se un certificato non è stato creato in precedenza, è possibile selezionare un certificato autofirmato predefinito ([DefaultInternalCertificate](#)) ma verrà visualizzato un messaggio di certificato di un server non attendibile. È necessario deselectare l'opzione Ignora i criteri di controllo di accesso per il traffico decrittografato (sysopt allow-vpn) in modo che le regole dei criteri di accesso all'identità dell'utente diventino effettive in seguito. È possibile configurare qui anche l'esenzione NAT. In questa configurazione, tutto il traffico ipv4 dall'interfaccia interna verso gli indirizzi IP dei client AnyConnect è indirizzato a un'eccezione di NAT. Per le impostazioni più complesse, ad esempio per il hairpinning esterno-esterno, sarà necessario creare ulteriori regole NAT nell'ambito della politica NAT. I pacchetti AnyConnect sono disponibili sul sito del supporto Cisco: <https://software.cisco.com/download/home>. Per scaricare il pacchetto AnyConnect, è necessario acquistare una licenza Plus o Apex valida.



# Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

FTD-3-Manual

Outside Interface

outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface

ftd3.example.com

e.g. ravpn.example.com

## Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

## NAT Exempt



### Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

### Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



any-ipv4

## AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from [software.cisco.com](https://software.cisco.com).

You must have the necessary AnyConnect software license.

### Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.03052-webdeploy-k9.pkg

Linux: anyconnect-linux64-4.7.03052-webdeploy-k9.pkg

BACK

NEXT

6. Nella sezione Summary, verificare che AnyConnect sia impostato correttamente, quindi fare clic su **Submit Query**.

## ^ Summary

Review the summary of the Remote Access VPN configuration.

### General

**STEP 1: CONNECTION AND CLIENT CONFIGURATION**

Primary Identity Source

**Authentication Type** AAA Only

**Primary Identity Source** LAB-AD

**Fallback Local Identity Source** -

**Strip Identity Source server from username** No

**Strip Group from Username** No

Secondary Identity Source

**Secondary Identity Source for User Authentication** -

**Fallback Local Identity Source** -

Advanced

**Authorization Server**

**Accounting Server**

Client Address Pool Assignment

IPv4 Address Pool

BACK SUBMIT QUERY

7. Fare clic sul pulsante **Modifiche in sospeso** in alto a destra, come mostrato nell'immagine.

Firepower Device Manager | Monitoring | Policies | Objects | Device: FTD-3 | admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

#	NAME	AAA	GROUP POLICY	ACTIONS
1	General	Authentication: AAA Only Authorization: None Accounting: None	DfltGrpPolicy	

8. Fare clic su **Distribuisci ora**.

## Pending Changes ? X

✔ Last Deployment Completed Successfully  
16 Apr 2020 12:41 PM, [See Deployment History](#)

Deployed Version (16 Apr 2020 12:41 PM)	Pending Version <span style="float: right;">LEGEND <span style="border: 1px solid #ccc; padding: 2px;">Removed</span> <span style="border: 1px solid #ccc; padding: 2px;">Added</span> <span style="border: 1px solid #ccc; padding: 2px;">Edited</span></span>
<b>+ Network Object Added: AnyConnect-Pool</b>	
-	subType: Network
-	value: 10.10.10.0/24
-	isSystemDefined: false
-	dnsResolution: IPV4_AND_IPV6
-	name: AnyConnect-Pool
<b>+ RA VPN Added: NGFW-Remote-Access-VPN</b>	
-	vpnGatewaySettings[0].exemptNatRule: true
-	vpnGatewaySettings[0].outsideFqdn: ftd3.example.com
-	vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...
-	name: NGFW-Remote-Access-VPN
anyconnectPackageFiles:	
-	anyconnect-win-4.7.03052-webdeploy-k9.pkg
vpnGatewaySettings[0].serverCertificate:	
-	FTD-3-Manual
vpnGatewaySettings[0].outsideInterface:	
-	outside
vpnGatewaySettings[0].insideInterfaces:	
-	inside
vpnGatewaySettings[0].insideNetworks:	

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

### Abilita criterio di identità e configura criteri di sicurezza per identità utente

A questo punto, gli utenti di AnyConnect dovrebbero essere in grado di connettersi correttamente, ma potrebbero non essere in grado di accedere a risorse specifiche. Questo passaggio abiliterà l'identità dell'utente in modo che solo gli utenti con diritti AnyConnect Admins possano connettersi alle risorse interne tramite RDP e che solo gli utenti con diritti AnyConnect nel gruppo possano connettersi alle risorse interne tramite HTTP.

1. Passare a **Criteri > Identità** e fare clic su **Abilita criterio di identità**.

**Establishing User Identity**

You can use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group. By linking network behavior, traffic, and events directly to individual users, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.

**How Identity policies work**

Passive authentication | Active authentication

USERS → PASSIVE AUTHENTICATION → LEVERAGE IDENTITY

IDENTITY SOURCES → MULTIPLE IDENTITIES → PASSIVE AUTHENTICATION

**ENABLE IDENTITY POLICY**

Per questa configurazione non sono necessarie ulteriori configurazioni e l'azione predefinita è sufficiente.

**Identity Policy**

Search

#	NAME	AUTHENTICATION	AUTH. TYPE	SOURCE			DESTINATION			ACTIONS
				ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO...	
There are no Identity rules yet. Start by creating the first identity rule.										

**CREATE IDENTITY RULE**

Default Action: **Passive Auth** | Any Identity Source

2. Passare a **Policies > NAT (Politiche)** e verificare che NAT sia configurato correttamente. Se l'eccezione NAT configurata nelle impostazioni AnyConnect è sufficiente, non è necessaria alcuna configurazione aggiuntiva.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

Security Policies

SSL Decryption Identity Security Intelligence NAT Access Control Intrusion

1 rule

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
>	Internet_PAT	DYNAMIC	ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

3. Passare a **Policy > Controllo accesso**. In questa sezione, l'azione predefinita è Blocca e non è stata creata alcuna regola di accesso, quindi una volta connesso un utente AnyConnect, non potrà accedere a niente. Fare clic sul simbolo + o su Crea regola di accesso per aggiungere una nuova regola.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

Security Policies

SSL Decryption Identity Security Intelligence NAT Access Control Intrusion

Search

#	NAME	ACTION	SOURCE			DESTINATION				ACTIONS	
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO...	APPLICATIONS		URLS
<p>There are no access rules yet.</p> <p>Start by creating the first access rule.</p> <p><a href="#">CREATE ACCESS RULE</a></p>											

Default Action: Access Control - Block

4. Compilare i campi con i valori appropriati. In questa configurazione, gli utenti del gruppo AnyConnect Admins devono avere accesso RDP al server Windows nella rete interna. Per l'origine, la zona è configurata come outside\_zone, che è l'interfaccia esterna a cui si conatteranno gli utenti AnyConnect e la rete è configurata come oggetto AnyConnect-Pool configurato in precedenza per assegnare gli indirizzi IP ai client AnyConnect. Per l'identità utente in FDM, l'origine deve essere la zona e la rete da cui l'utente inizierà la connessione. Per la destinazione, la zona è configurata come inside\_zone, che è l'interfaccia interna del server Windows, la rete è configurata come oggetto Inside\_Net che è un oggetto che definisce la subnet in cui si trova il server Windows e Porte/Protocolli è impostato su due oggetti porta personalizzati per consentire l'accesso RDP su TCP 3389 e UDP 3389.

### Edit Access Rule

Order	Title	Action
1	AC RDP Access	Allow

Source/Destination   Applications   URLs   Users   Intrusion Policy   File policy   Logging

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP

Show Diagram    Not hit yet   CANCEL   OK

Nella sezione Utenti, il gruppo AnyConnect Admins verrà aggiunto in modo che gli utenti che non fanno parte di questo gruppo possano accedere al server Windows tramite RDP. Fare clic sul simbolo +, quindi sulla scheda Gruppi, fare clic sul gruppo appropriato e infine su **OK**. Si noti che è possibile selezionare anche i singoli utenti e l'origine identità.

**Add Access Rule**

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

**AVAILABLE USERS**

Filter: [ ]

Identity Sources: **Groups** | Users

- LAB-AD \ Account Operators
- LAB-AD \ Administrators
- LAB-AD \ Allowed RODC Password Replication Group
- LAB-AD \ AnyConnect Admins**
- LAB-AD \ AnyConnect Users

Create new Identity Realm | CANCEL | **OK**

Show Diagram:

CANCEL | **OK**

Dopo aver selezionato le opzioni appropriate, fare clic su **OK**.

**Add Access Rule**

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

**AVAILABLE USERS**

- LAB-AD \ AnyConnect Admins

Show Diagram:

CANCEL | **OK**

5. Se necessario, creare altre regole di accesso. In questa configurazione, viene creata un'altra

regola di accesso per consentire agli utenti del gruppo AnyConnect Users di accedere al protocollo HTTP di Windows Server.

**Edit Access Rule**

Order: 2 | Title: AC HTTP Access | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

**SOURCE**

Zones	Networks	Ports
outside_zone	AnyConnect-Pool	ANY

**DESTINATION**

Zones	Networks	Ports/Protocols
inside_zone	Inside_Net	HTTP

Show Diagram  | Not hit yet | CANCEL | OK

**Edit Access Rule**

Order: 2 | Title: AC HTTP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

**AVAILABLE USERS**

LAB-AD \ AnyConnect Users
---------------------------

**CONTROLLING ACCESS FOR USERS AND USER GROUPS**

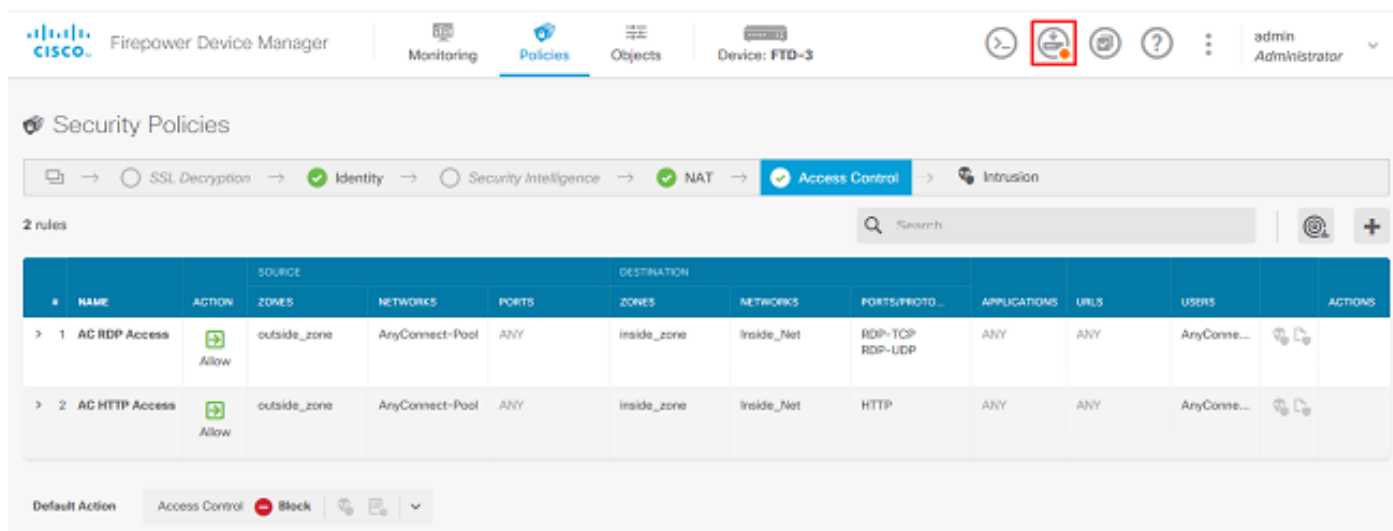
If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram  | Not hit yet | CANCEL | OK

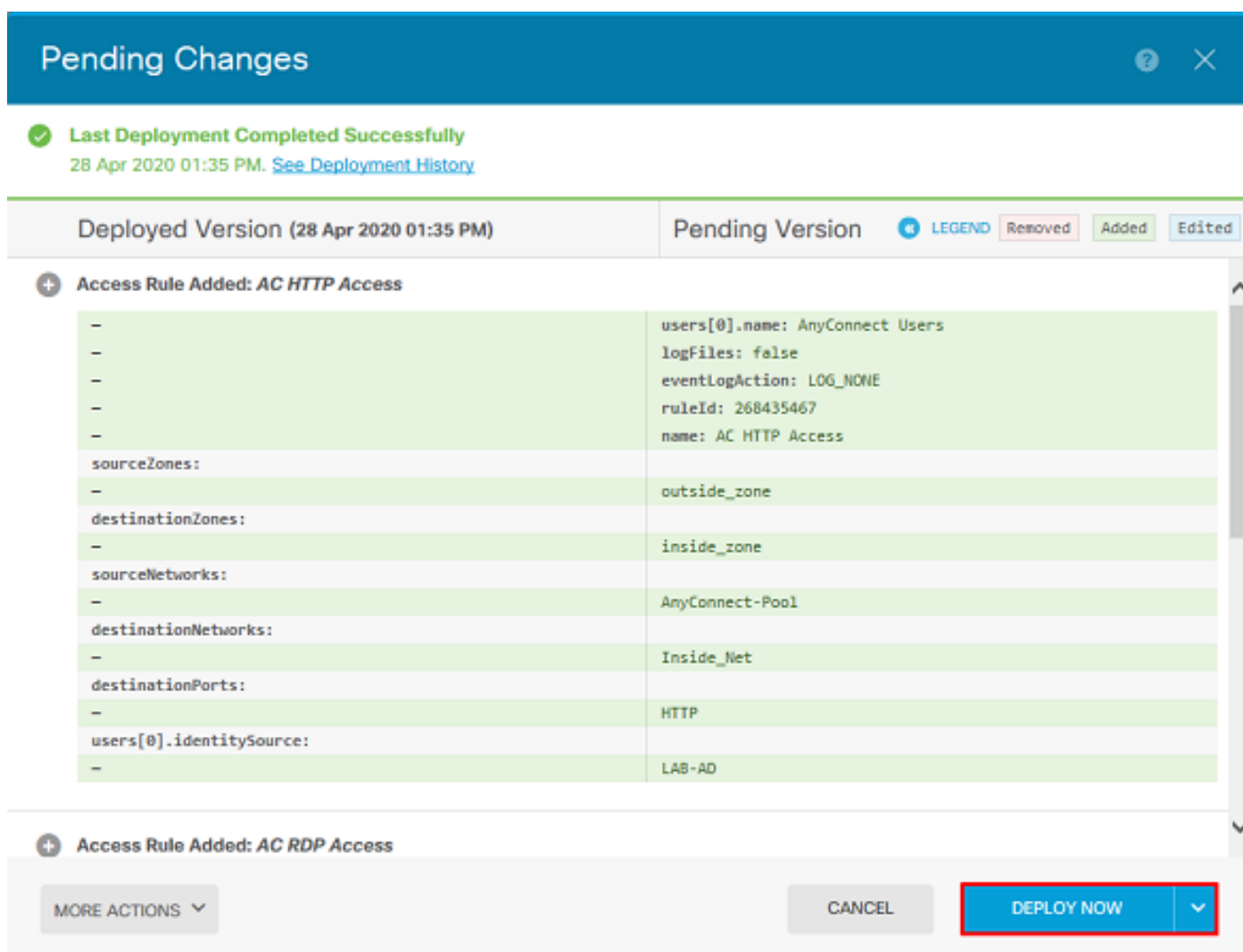
6. Verificare la configurazione della regola di accesso, quindi fare clic sul pulsante **Modifiche in**



sospeso in alto a destra, come mostrato nell'immagine.



7. Verificare le modifiche, quindi fare clic su **Distribuisci ora**.



## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

## Configurazione finale

## Configurazione AAA

```
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
```

## Configurazione di AnyConnect

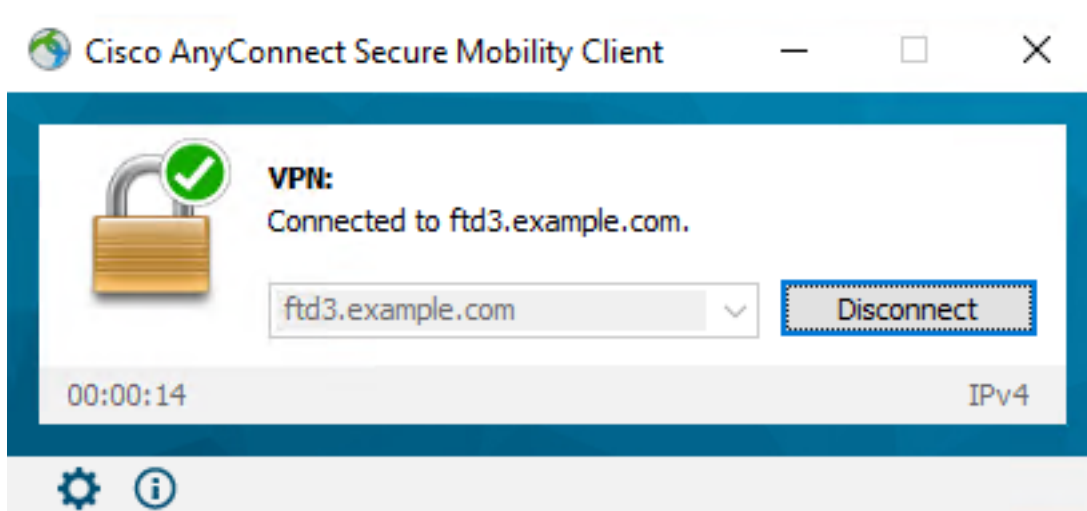
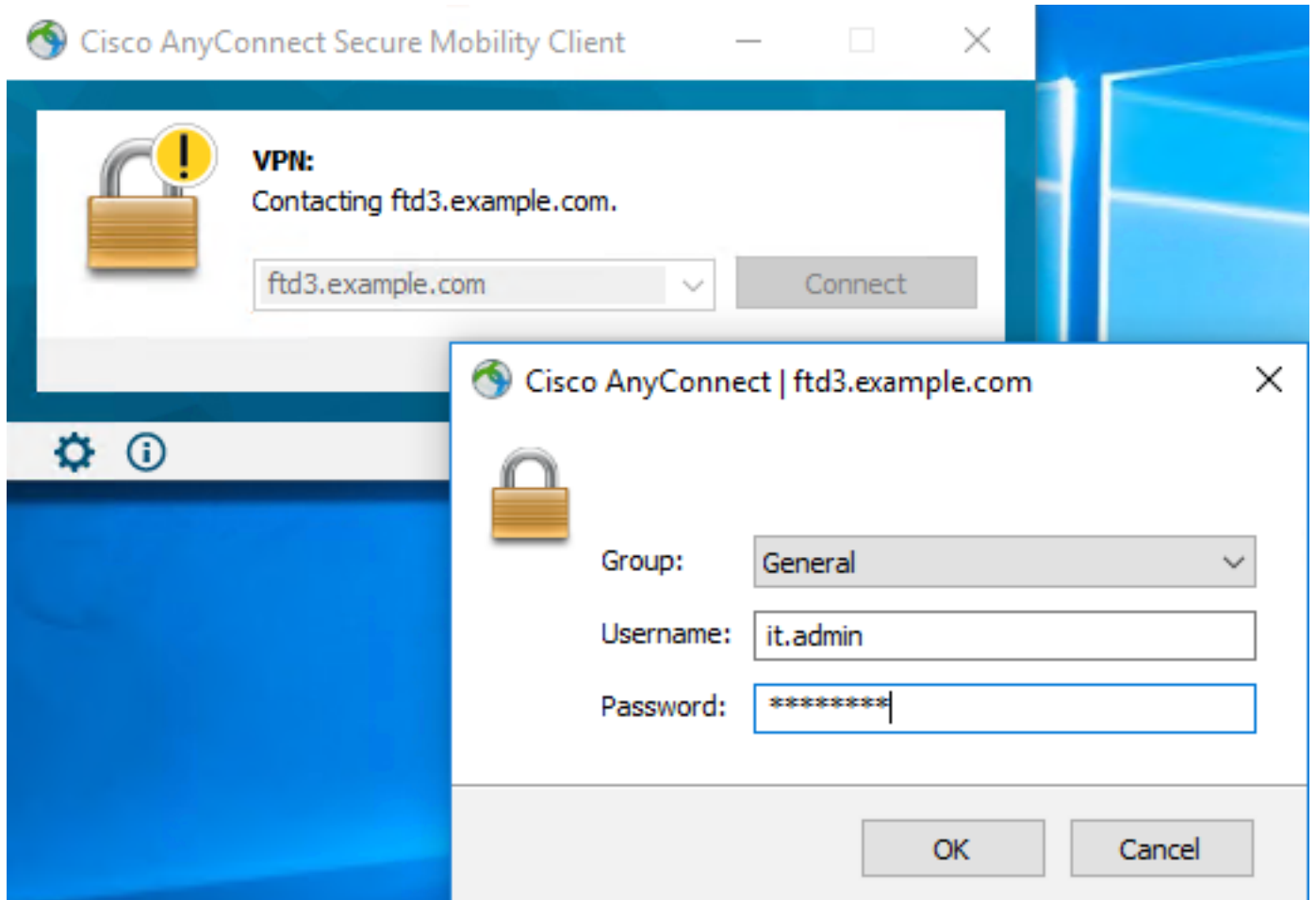
```
> show running-config webvpn
webvpn
  enable outside
  http-headers
    hsts-server
      enable
      max-age 31536000
      include-sub-domains
      no preload
    hsts-client
      enable
  x-content-type-options
  x-xss-protection
  content-security-policy
  anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
  anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
  anyconnect enable
  tunnel-group-list enable
  cache
    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
```

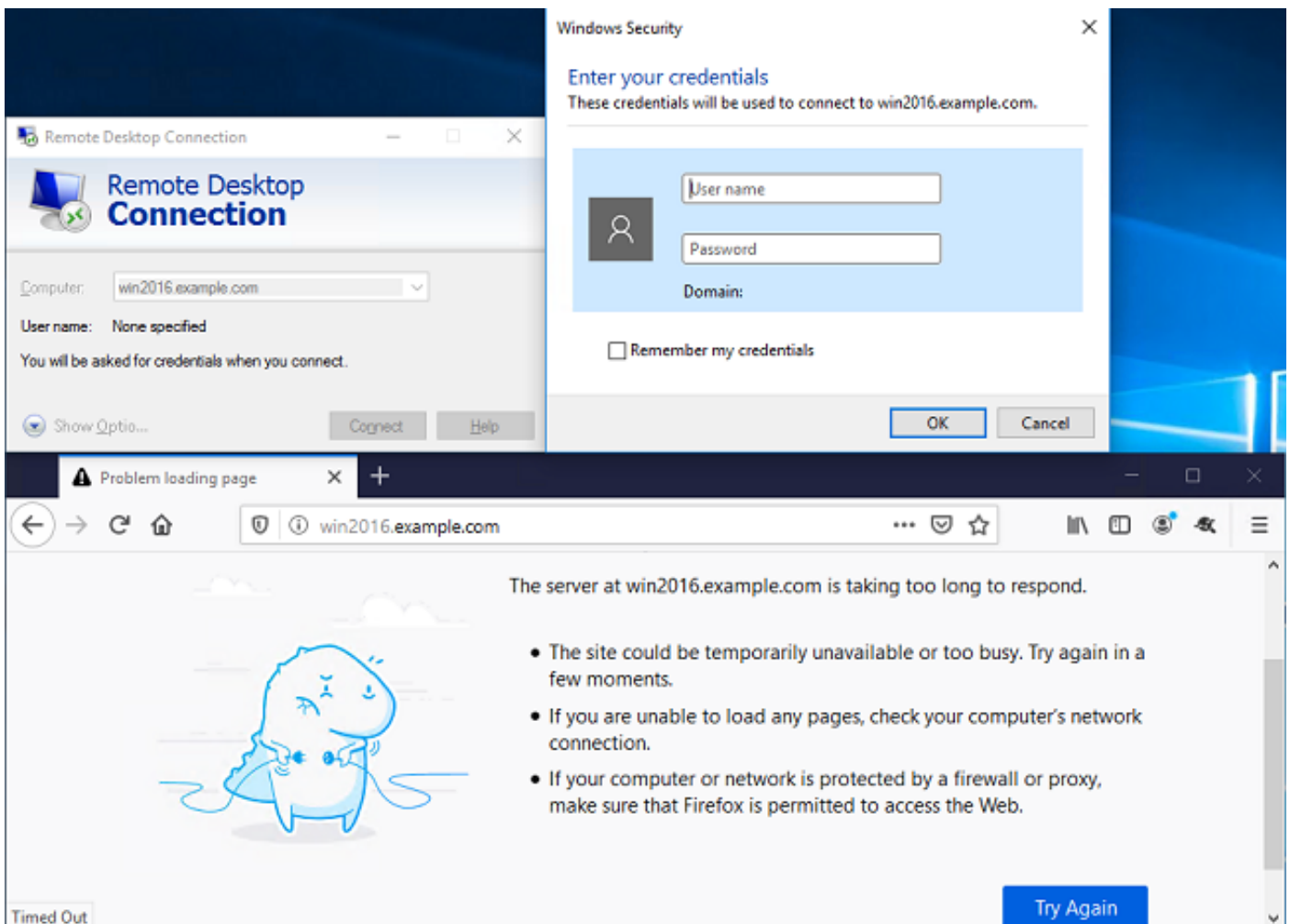
```
> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
  anyconnect ssl dtls none
```

```
> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

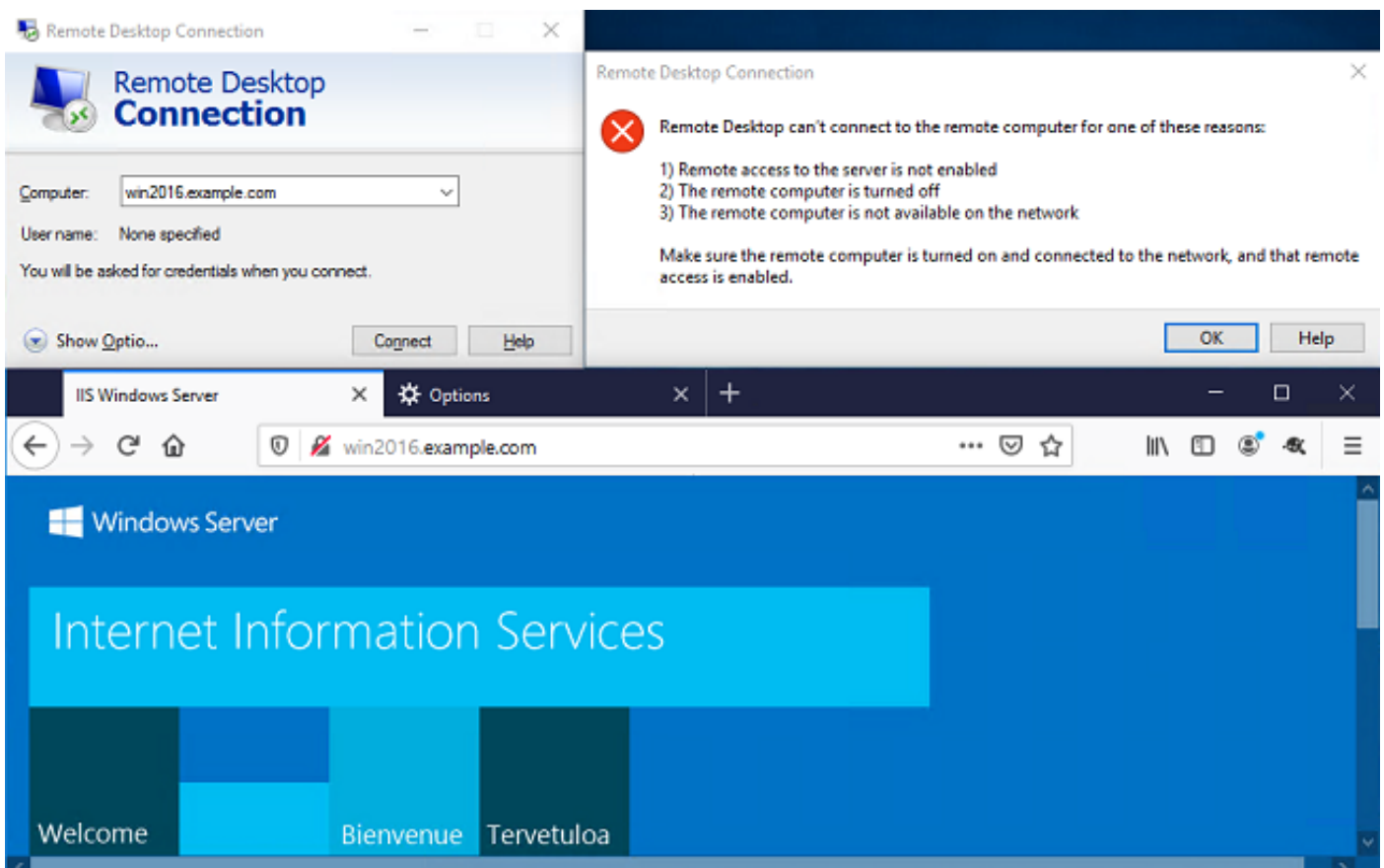
## Connettersi con AnyConnect e verificare le regole dei criteri di controllo di accesso



L'utente IT Admin appartiene al gruppo AnyConnect Admins, che ha accesso RDP al server Windows, ma non ha 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 si è connessi con un utente di prova appartenente al gruppo AnyConnect Users con accesso HTTP ma non RDP, è possibile verificare che le regole del controllo di accesso siano effettive.



# Risoluzione dei problemi

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

## 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 firewall-engine-debug** per stabilire perché il traffico è 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...;.....}...
[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 la connessione con il server LDAP

```
[-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

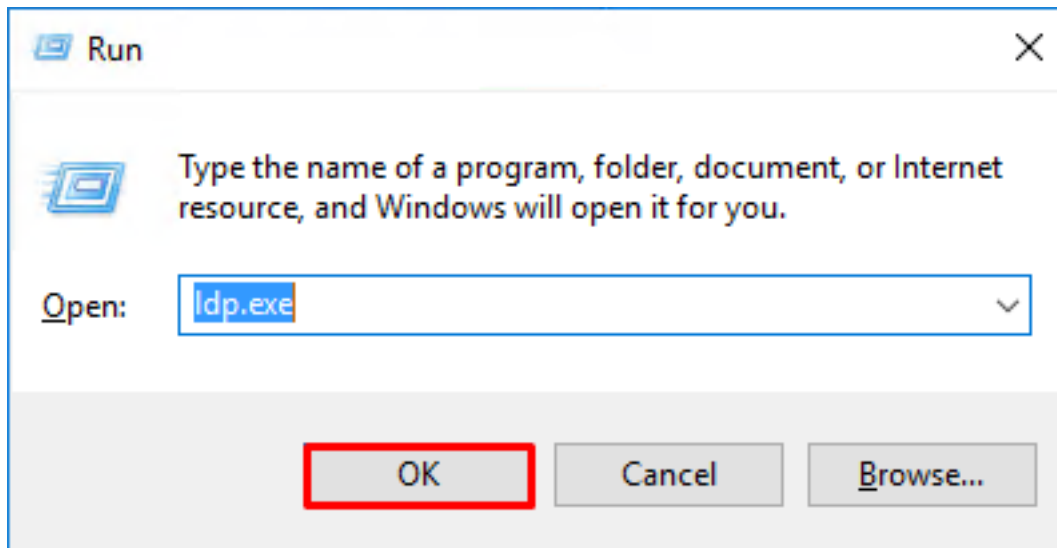
## Nome distinto e/o password di accesso binding non corretti

```
[-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
```

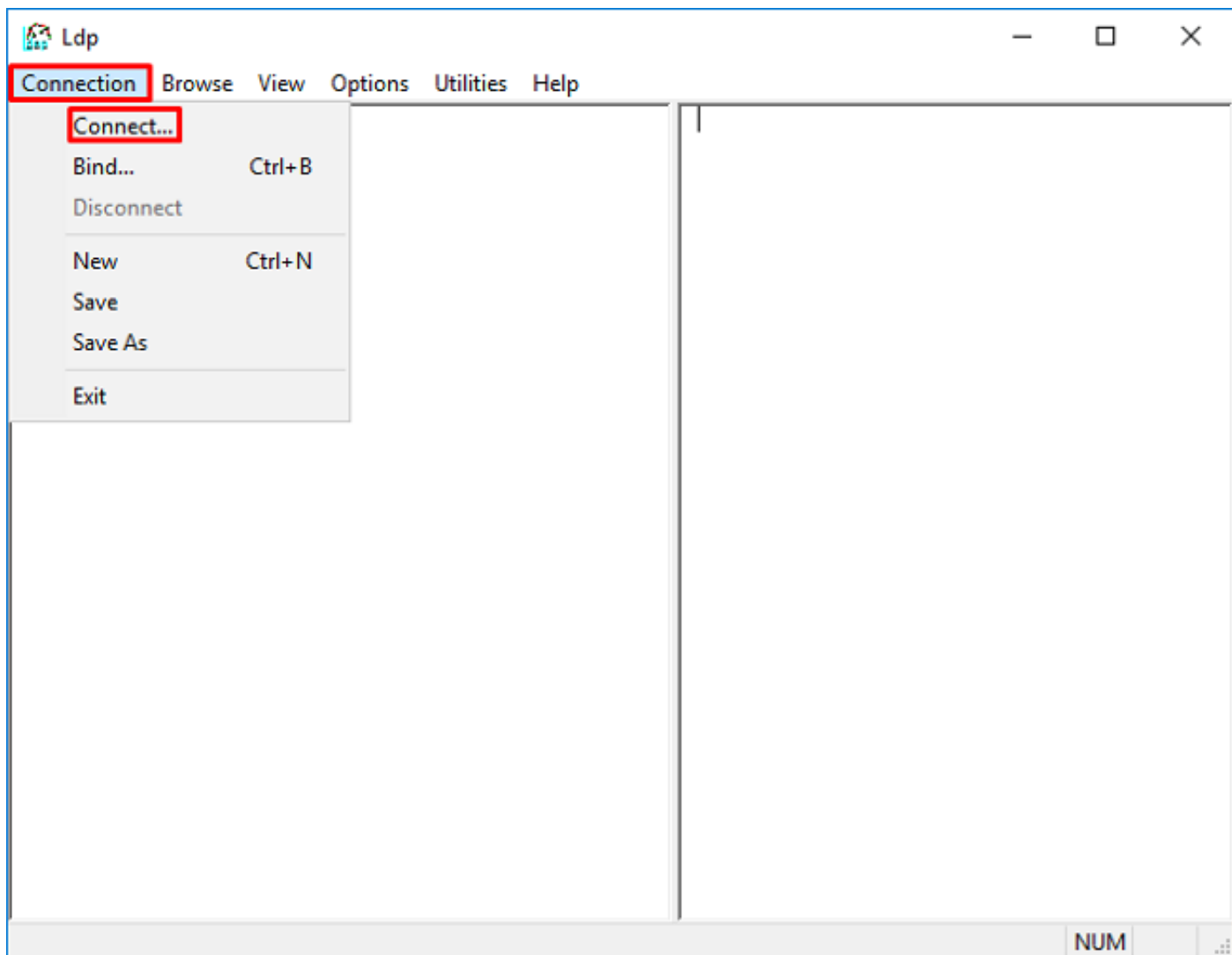
```
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid
credentials
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

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 all'utilizzo di LDAP, eseguire la procedura seguente:

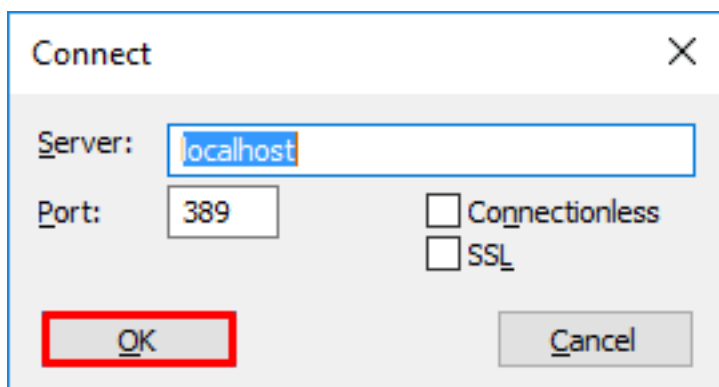
1. Sul server AD, premere **Win+R** e cercare **ldp.exe**.



2. Fare clic su **Connessione > Connetti...** come mostrato nell'immagine.

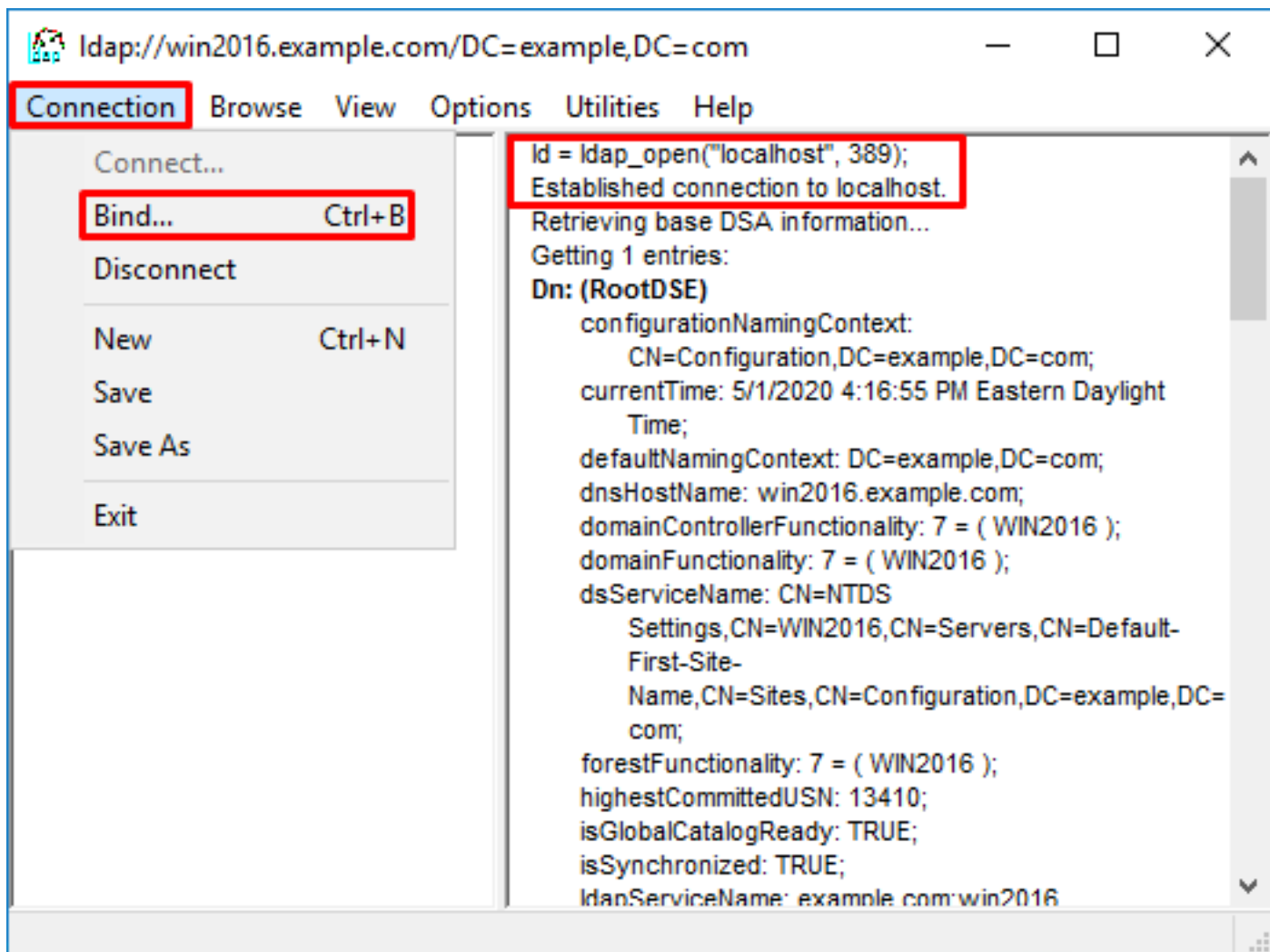


3. Specificare localhost per il server e la porta appropriata, quindi fare clic su **OK**.

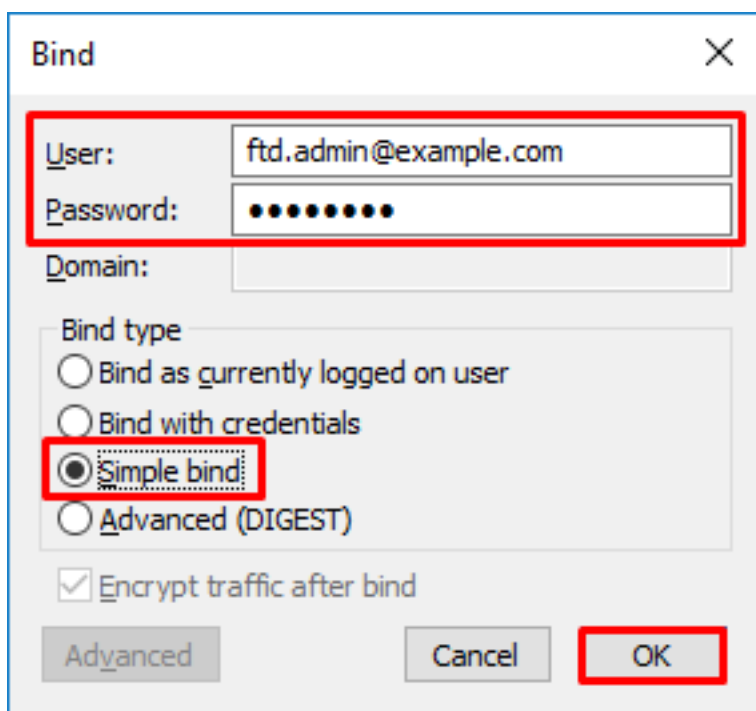


4. La colonna Destra mostra il testo che indica la riuscita della connessione. Fare clic su **Connessione > Associa...** come mostrato nell'immagine.

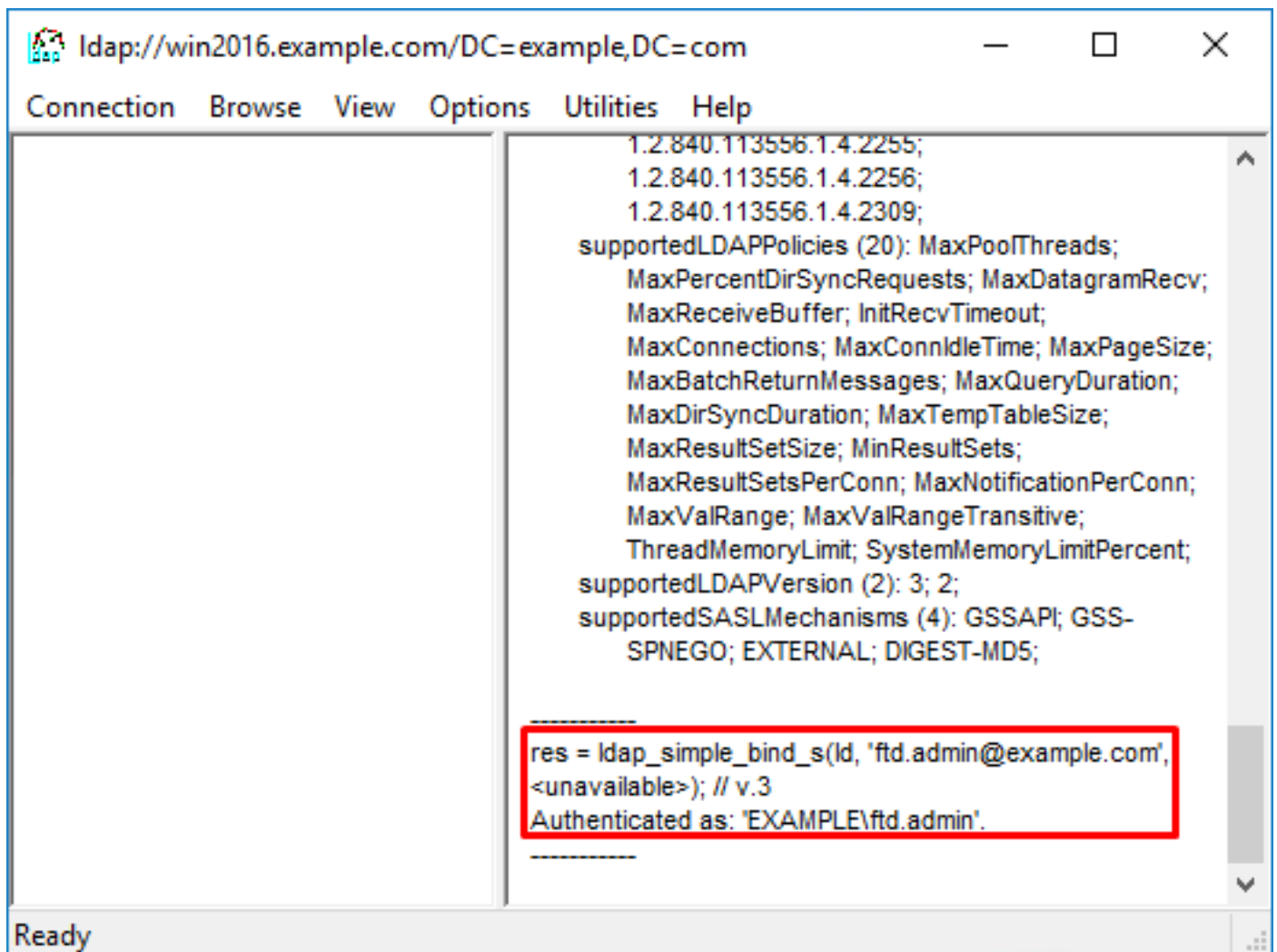




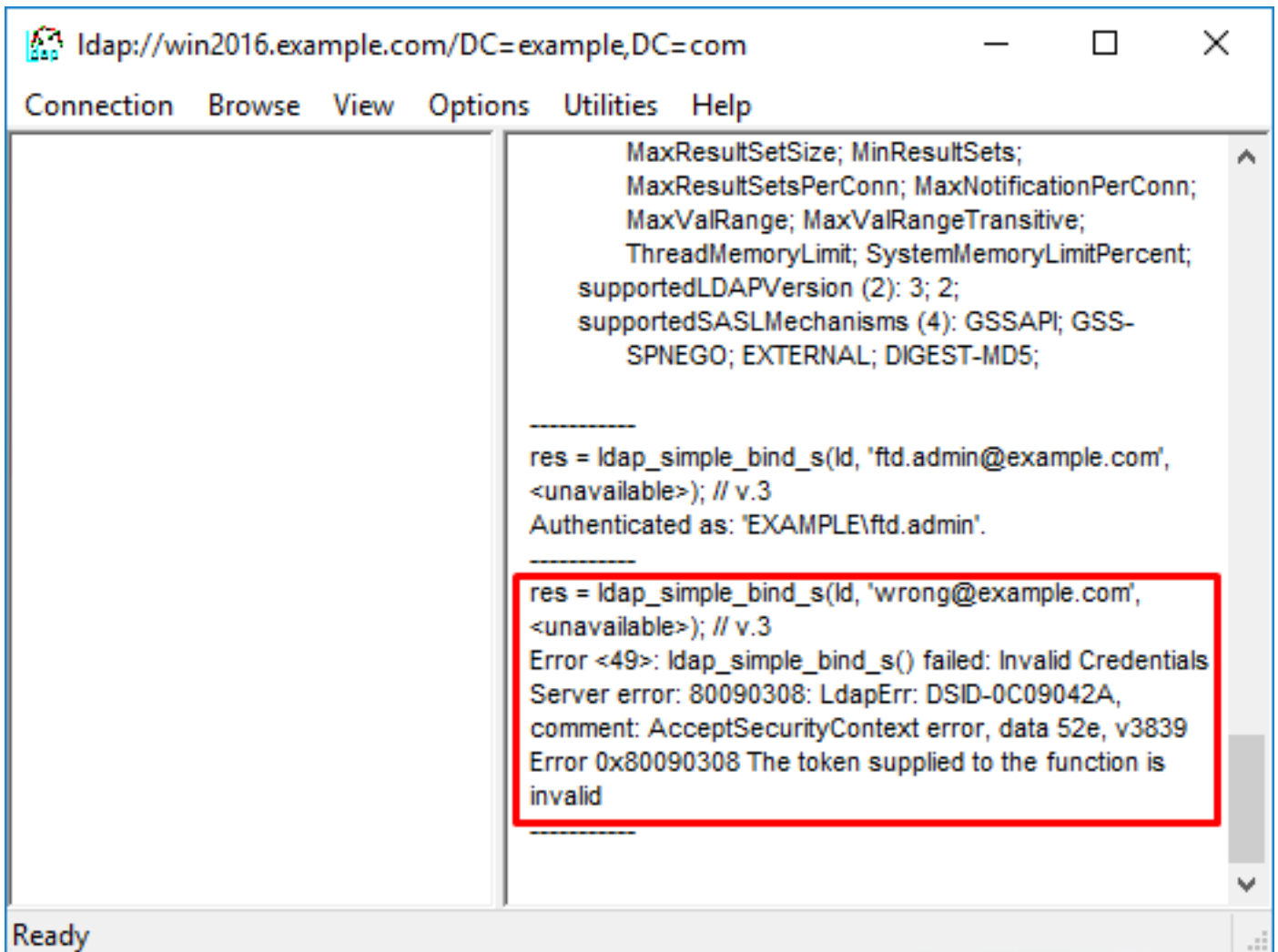
5. Selezionare **Associazione semplice**, quindi specificare il nome utente e la password dell'account della directory. Fare clic su **OK**.



Se il binding ha esito positivo, il comando Idp visualizzerà Authenticated come **DOMAIN\username**.



Se si tenta un'associazione con un nome utente o una password non validi, si verificherà un errore di questo tipo.



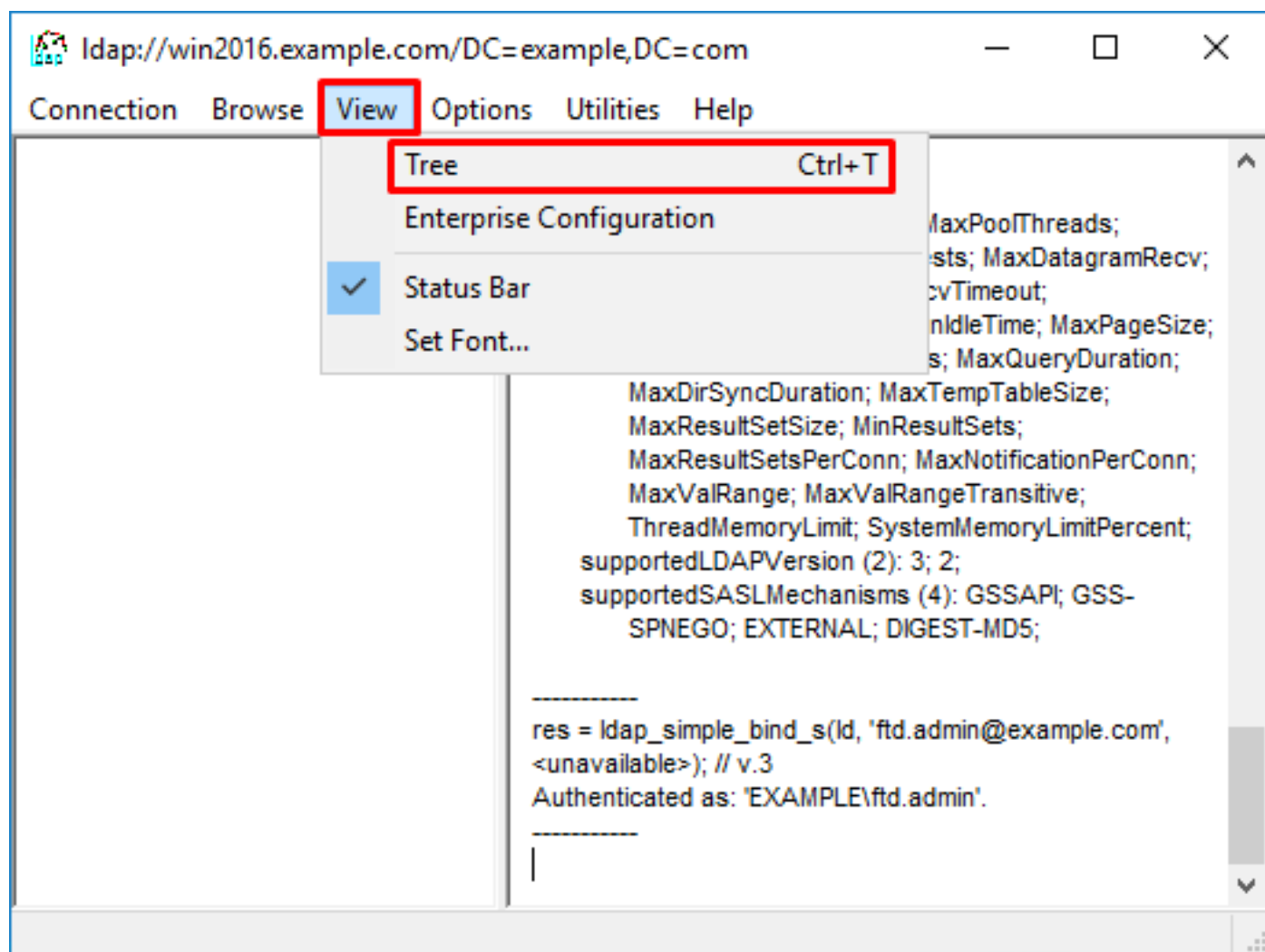
## Server LDAP: impossibile trovare il nome utente

```
[-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
```

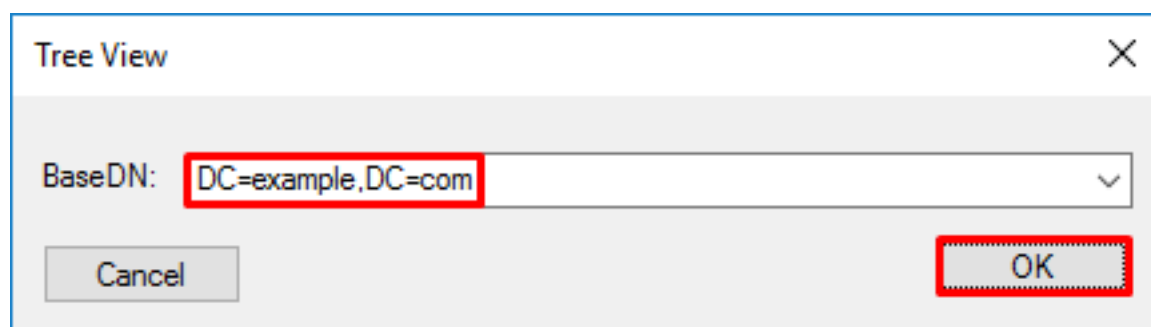
Soluzione potenziale: Verificare che AD sia in grado di trovare l'utente con la ricerca eseguita dall'FTD. Questa operazione può essere eseguita anche con ldp.exe.

1. Dopo aver eseguito correttamente il binding, passare a **Visualizza > Struttura** come mostrato

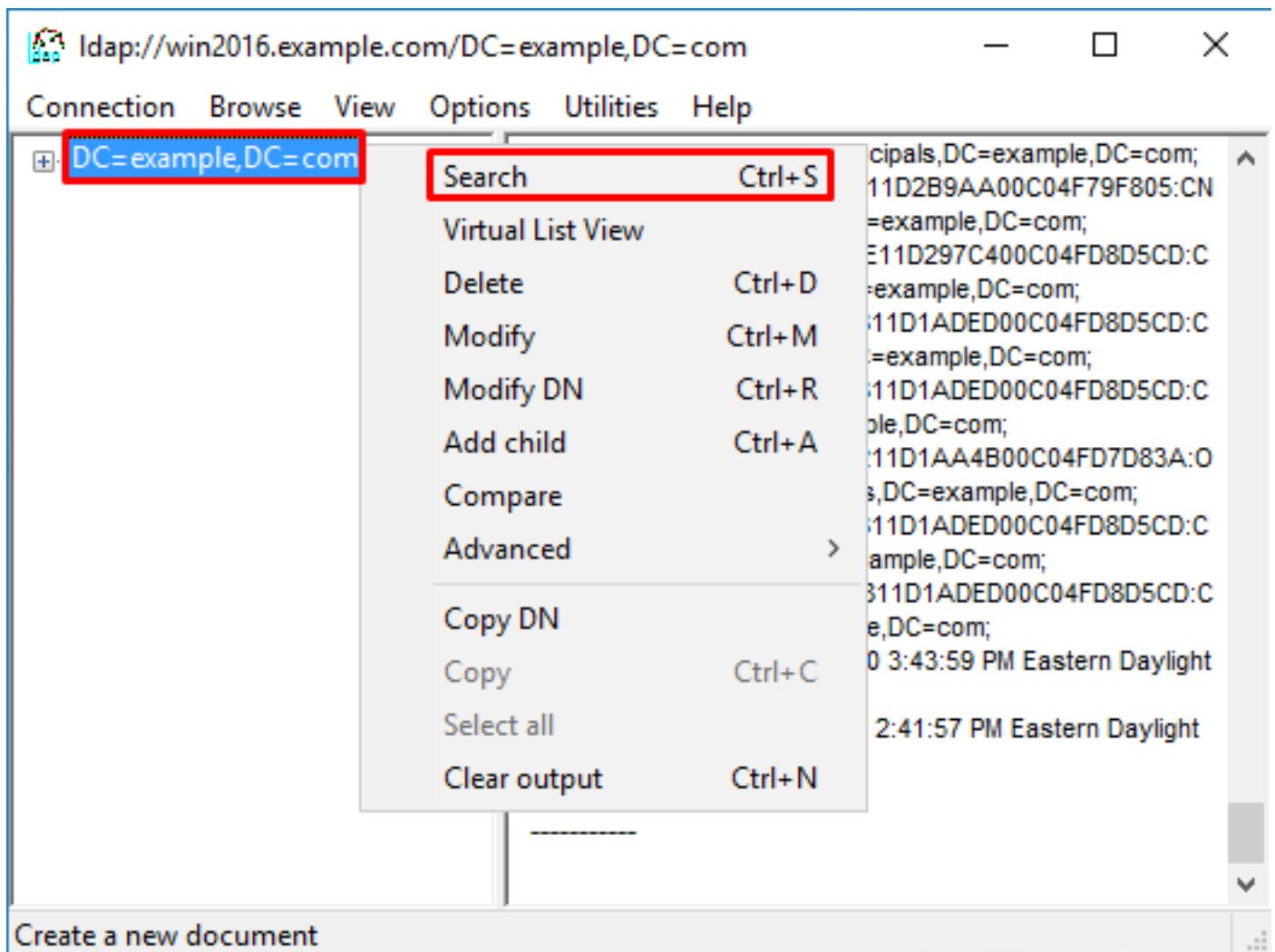
nell'immagine.



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

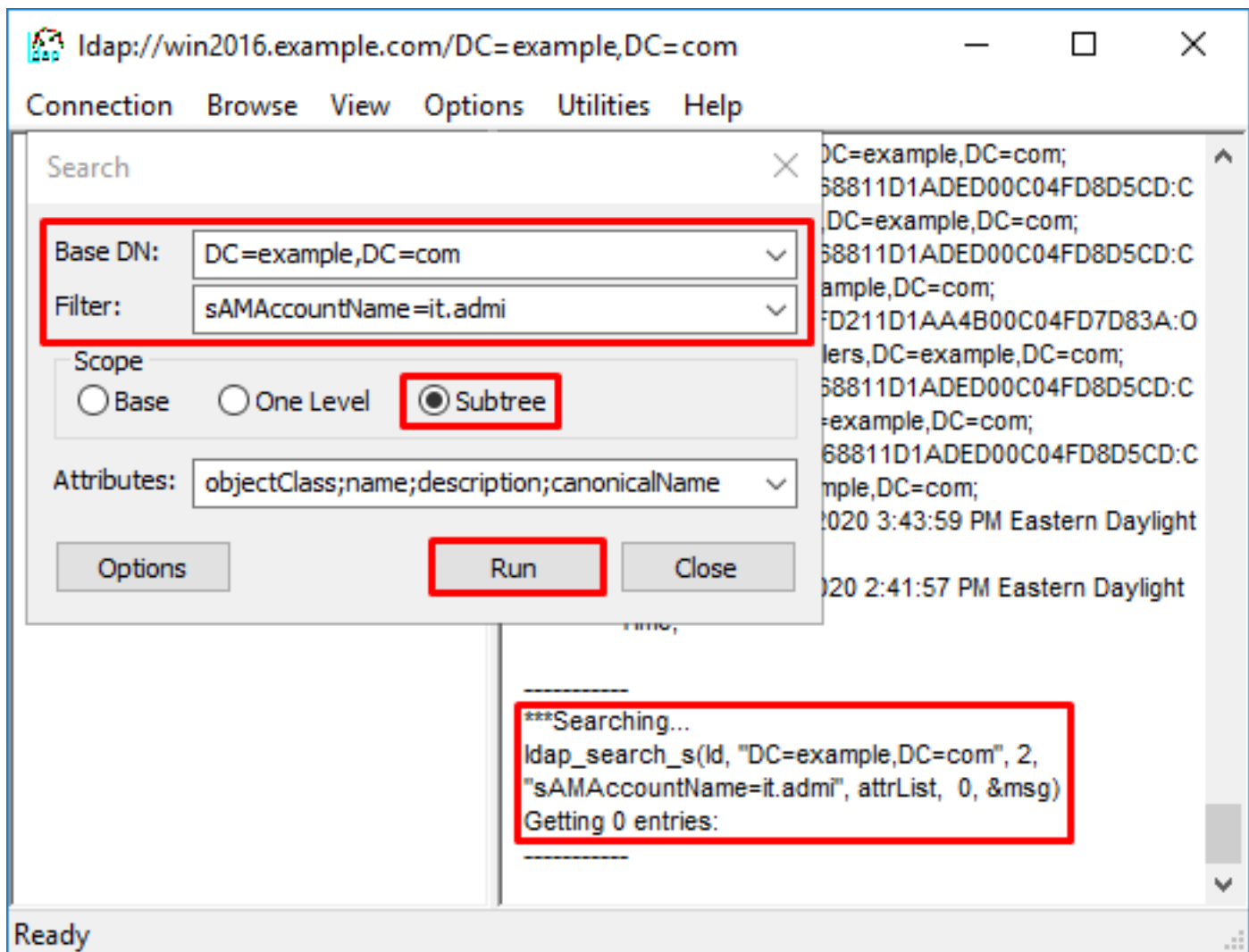


3. Fare clic con il pulsante destro del mouse sul DN di base, quindi scegliere Cerca come mostrato nell'immagine.



4. Specificare gli stessi valori Base DB, Filter e Scope visualizzati nei debug. In questo esempio, sono:

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



Il comando ldp trova 0 voci poiché non esiste alcun account utente con **samaccountname=it.admi** nel DN di base dc=example,dc=com.

Se si tenta di eseguire nuovamente il tentativo con il **samaccountname=it.admin** corretto, verrà visualizzato un risultato diverso. ldp trova 1 voce nel DN di base dc=example,dc=com e stampa il DN di tale utente.

ldap://win2016.example.com/DC=example,DC=com

Connection Browse View Options Utilities Help

Search

Base DN: DC=example,DC=com

Filter: sAMAccountName=it.admin

Scope

Base  One Level  Subtree

Attributes: objectClass;name;description;canonicalName

Options Run Close

68811D1AED00C04FD8D5CD:C  
DC=example,DC=com;  
68811D1AED00C04FD8D5CD:C  
example,DC=com;  
FD211D1AA4B00C04FD7D83A:O  
lers,DC=example,DC=com;  
68811D1AED00C04FD8D5CD:C  
=example,DC=com;  
68811D1AED00C04FD8D5CD:C  
mple,DC=com;  
020 3:43:59 PM Eastern Daylight  
020 2:41:57 PM Eastern Daylight

\*\*\*Searching...  
ldap\_search\_s(ld, "DC=example,DC=com", 2,  
"sAMAccountName=it.admin", attrList, 0, &msg)  
Getting 1 entries:  
**Dn: CN=IT Admin,CN=Users,DC=example,DC=com**  
canonicalName: example.com/Users/IT Admin;  
name: IT Admin;  
objectClass (4): top; person; organizationalPerson;  
user;

Ready

## Password non corretta per il nome utente

```

[-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 error, data 52e, v3839
[-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 dell'utente sia configurata correttamente e che non sia scaduta. Analogamente al DN di accesso, l'FTD eseguirà un'associazione ad Active Directory con le credenziali dell'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 **Associazione DN di login e/o Password errata**. È inoltre possibile esaminare i registri del Visualizzatore eventi del server Microsoft per un motivo potenziale.

## 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. Può essere utilizzato per verificare la presenza di errori di connessione o autenticazione. Il comando è **test di autenticazione aaa-server [AAA-server] host [AD IP/nomehost]**.

```
> 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.

Di seguito viene riportata un'acquisizione che 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

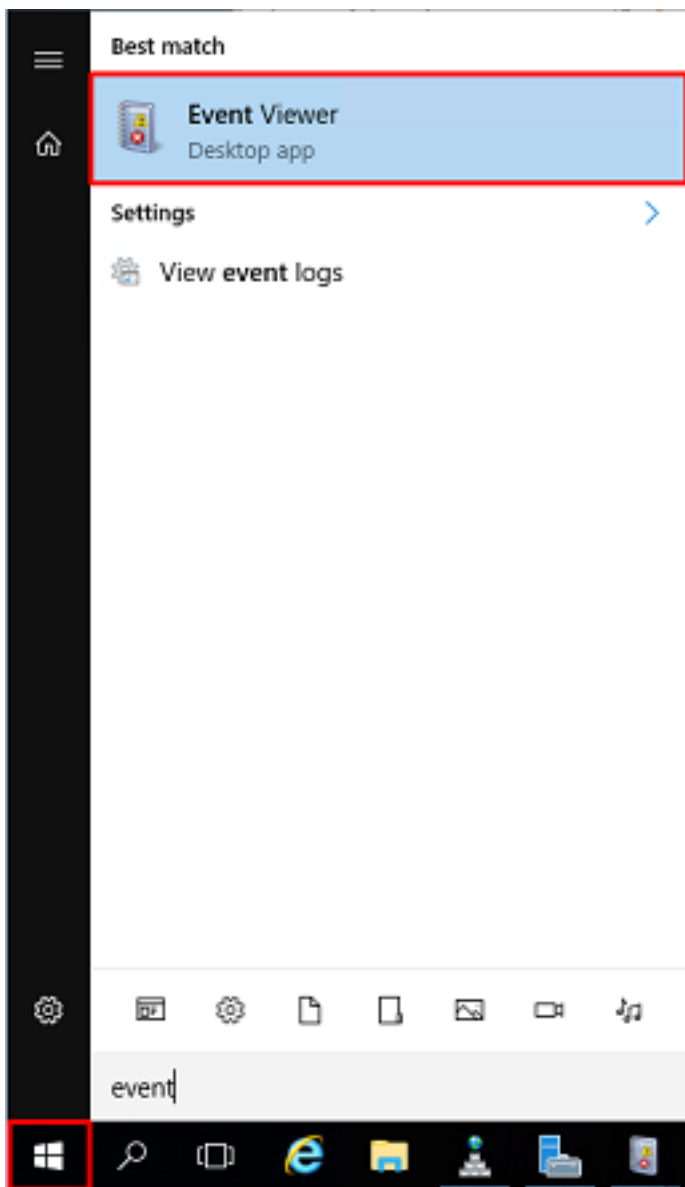
54 packets captured

  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
  3: 23:02:16.772039      192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
<nop,nop,timestamp 1061373058 762393884>
  4: 23:02:16.772482      192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
  5: 23:02:16.772924      192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
  6: 23:02:16.772955      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
  7: 23:02:16.773428      192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
  8: 23:02:16.775030      192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
  9: 23:02:16.775075      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

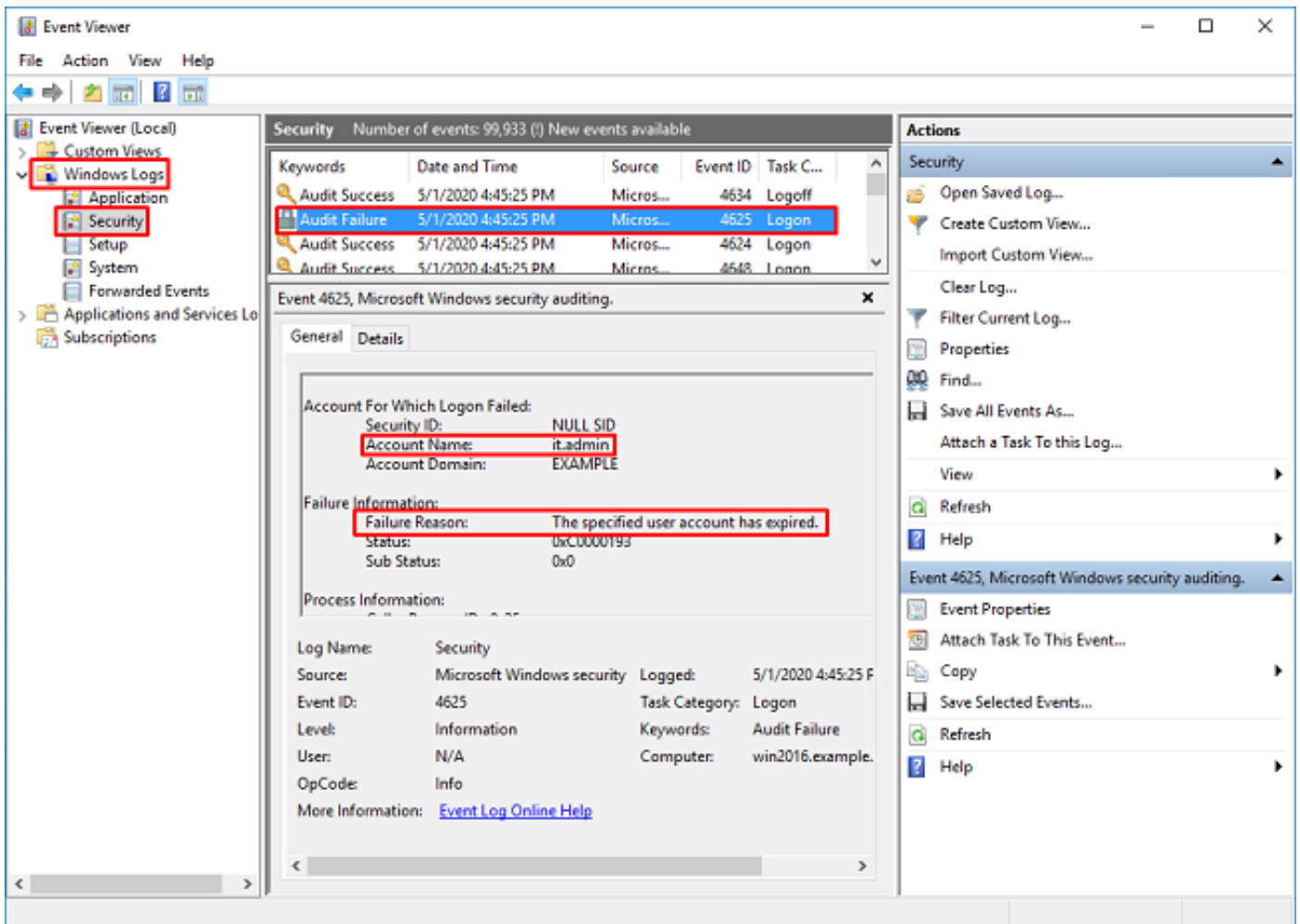
## Registri del Visualizzatore eventi di Windows Server

Il Visualizzatore eventi accede al furgone del server AD e fornisce informazioni più dettagliate sul motivo per cui si è verificato un errore.

### 1. Cercare e aprire il Visualizzatore eventi.



2. Espandere **Registri Windows** e fare clic su **Protezione**. Cercare **Controllo non riuscito** con il nome account dell'utente ed esaminare le informazioni sull'errore come mostrato nell'immagine.



An account failed to log on.

Subject:

Security ID:SYSTEM  
Account Name:WIN2016\$\nAccount Domain:EXAMPLE  
Logon ID:0x3E7

Logon Type:3

Account For Which Logon Failed:

Security ID:NULL SID  
**Account Name:it.admin**  
Account Domain:EXAMPLE

Failure Information:

**Failure Reason:The specified user account has expired.**  
Status:0xC0000193  
Sub Status:0x0

Process Information:

Caller Process ID:0x25c  
Caller Process Name:C:\Windows\System32\lsass.exe

Network Information:

Workstation Name:WIN2016  
Source Network Address:192.168.1.17  
Source Port:56321