# 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: II 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.

=	Best match				
ŵ	Active Directory Users and Computers Desktop app				
	Settings >				
	8 Edit local users and groups				
	陀 Change User Account Control settings				
	8 User Accounts				
	Select users who can use remote desktop				
۲	a 🖉 🖞 🗋 🕲 📾				
	users				
-	ዶ 🗆 🤶 🚍 🤱 📕				

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**.

example.	com Propertie	s				?	х
General	Managed By	Object	Security	Attribut	te Editor		
Attribut	69:						
Attribu	ute	Valu	e				^
dc		exan	nple				_
defau	itLocalPolicyOb	j knot	set>				
descr	iption	knot	set>				
deskt	opProfile	knot	set>				
displa	yName	knot	set>				
displa	vNamePrintable	e knot	set>	_			
disting	guishedName	DC=	example_D	C=com			
doma	inPolicyObject	<not< td=""><td>set&gt;</td><td></td><td></td><td></td><td></td></not<>	set>				
doma	inReplica	<not< td=""><td>set&gt;</td><td></td><td></td><td></td><td></td></not<>	set>				
dSAS	ignature	{ V1	: Flags = O	<li>C); Later</li>	icySecs =	: 0; DsaGu	ic 👘
dSCo	rePropagationD	0x0	=()				
eFSP	olicy	<not< td=""><td>set&gt;</td><td></td><td></td><td></td><td></td></not<>	set>				
exten	sionName	<not< td=""><td>set&gt;</td><td></td><td></td><td></td><td></td></not<>	set>				
flags		<not< td=""><td>set&gt;</td><td></td><td></td><td></td><td>~</td></not<>	set>				~
<						>	
W	ew					Filter	
	ОК		Cancel		Apply	He	lp

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.

String Attribute Editor	×	
Attribute: distingu	ishedName	
Value: DC=example;DC=com	OK Carcel	Undo
Uca	UK Canoa	Cut
		Paste Delete
		Select All
		Right to left Reading order Show Unicode control characters Insert Unicode control character
example.com Properties	? ×	
General Managed By C Attributes:	Object Security Attribute Editor	
Attribute	Value	
cn controlAccessRights creationTime	<not set=""> <not set=""> 4/29/2020 2:43:49 PM Eastern Daylight Tim</not></not>	
dc defaultLocalPolicyObj	example <not set=""></not>	
desktopProfile displayName	<not set=""> <not set=""> <not set=""> <td></td></not></not></not>	
displayNamePrintable	<not set=""></not>	
domainPolicyObject domainReplica dSASignature	<pre>cnot set&gt; { V1: Rags = 0x0; LatencySecs = 0; DsaGuic</pre>	
<	UXU = ( )	
View	Filter	
ОК	Cancel Apply Help	

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:

Active Directory Users and C	omputers	-	$\times$
File Action View Help			
🗢 🔿 🙍 🚾 🖌 🗈 👂	Users Properties ? ×		
<ul> <li>Active Directory Users and Q</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrinc</li> <li>LostAndFound</li> <li>Hongram Data</li> <li>System</li> <li>Users</li> <li>NTDS Quotas</li> <li>TPM Devices</li> </ul>	Users Properties ? X General Object Security Attribute Editor Attributes: Attribute Value ^ ^ adminDescription <not set=""> adminDisplayName <not set=""> on Users defaultClassStore <not set=""> defaultClassStore <not set=""> defaultClassStore <not set=""> defaultClassStore <not set=""> displayName <not set=""> fSMORoleOwner <not set=""> instanceType Qx4 = (WRITE) <v </v </not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>		*
	OK Cancel Apply Help		
<			~

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**.

Active Directory Users and Computers				-	×
File Action View Help					
🗢 🔿 🖄 🚾 🐇 💷 🗶 [	🗊 🖸 🔒 🖬 🖬	n   🐮 🔌 în 🦷	r 🗵 🕱		
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Subscription Saved Queries Saved	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Ad Domain Co	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		^
All Tasks View Refresh Export List Properties Help	> > WseAlertA	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue All Printer	ntial PropertyList incipalContainer		
< >> Creates a new item in this container.	& WseAllow	User Shared Folder	-		Ŷ

2. Spostarsi nella Creazione guidata Nuovo oggetto - Utente.

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

New Object - User		×
🤱 Create in: exam	nple.com/Users	
Password:	•••••	
Confirm password:	•••••	
User must change passw	ord at next logon	
User cannot change pass	sword	
Password never expires		
Account is disabled		
	< Back Next >	Cancel
		~
New Object - User		×
New Object - User	nple.com/Users	×
New Object - User Create in: exam When you click Finish, the for	mple.com/Users	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin	nple.com/Users blowing object will be created:	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admine	nple.com/Users Mowing object will be created: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users Mowing object will be created: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	mple.com/Users ollowing object will be created: @example.com 8.	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users ollowing object will be created: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin( The password never expires	nple.com/Users blowing object will be created: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin( The password never expires	nple.com/Users Mowing object will be created: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin( The password never expires	nple.com/Users Mowing object will be created: @example.com t.	×

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

Active Directory Users and Computers			_	×	
File Action View Help					
🗢 🔿 🖄 📆 🖌 🗎  🛠	🗉 🗟 📑 🚺 🖬	1 🗏 🐮 🕅 🦷	1 🔟 🗽		
<ul> <li>Active Directory Users and Com</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipale</li> <li>Managed Service Account</li> <li>Users</li> </ul>	Name DefaultAcco DefaultAcco DefaultAcco Donain ROD DosUpdateP Domain Ad Domain Co Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Co Comain Co Domain Co Comain C	Type User Security Group Security Group User User User Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue Members of this group		^
	Read-only D	Security Group	Members of this group		
< >	Test User	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**.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙇 🚾 🕹 🗱	🗊 🙆 📑 🚺 🖬	e i 😤 📚 în 🤋	r 🧕 🕱		
Active Directory Users and Com Saved Queries Saved Queries Delegate Con Find	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Ad Domain Co ntrol ers	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		~
All Tasks View Refresh	> > >	Computer Contact Group InetOrgPerson msDS-KevCreder	ntial .		
Export List Properties Help	Read-only	msDS-ResourceF msDS-ShadowPr msImaging-PSP: MSMQ Queue Al	ropertyList incipalContainer ; ias		
Creates a new item in this container.	Schema A	Printer User Shared Folder			~

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

New Object - Group		×
🥵 Create in: example.o	om/Users	
Group name:		
AnyConnect Admins		
Group name (pre-Windows 2000):		
AnyConnect Admins		
Group scope	Group type	
O Domain local	Security	
Global	ODistribution	
OUniversal		
	OK Cance	1

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

Active Directory Users and Computers				_	×
File Action View Help					
🗢 🔿 🖄 📰 🕹	è   🛛 🖬   🐍 🔌 🛍 '	7 🗾 🐍			
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Solution ForeignSecurityPrincipals Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Domain RODC Passw DnsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Type Security Group Security Group User Security Group User Security Group Security Group User User User Security Group	Description Built-in account for ad Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		~
	104 S				

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**.

Active Directory Users and Computers				-	×
File Action View Help					
🗢 🔿 🖄 📰 🔏 🗈 🗙 🛙	1 @ 🔒 🛛 🖬 🔧	ዾ 🖹 🔻 🗾 🕯	6		
Active Directory Users and Com > in Saved Queries	Name Rt Am/Connect Admine	Type Security Group	Description		^
<ul> <li>example.com</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>Managed Service Accour</li> <li>Users</li> </ul>	Cloneable Domain C	Security Group User Security Group Security Group	curity Group     Add to a group       er     Buil     Move       curity Group     Mer     Send Mail       curity Group     Mer     All Tasks       er     A u:     Cut       curity Group     Mer     Cut       curity Group     DNS     Delete       curity Group     DNS     Rename       curity Group     Des     Properties       curity Group     All v     Help	· ·	
	DefaultAccount User     Denied RODC Passw Security     DonsAdmins Security     DonsUpdateProxy Security     Domain Admins Security     Domain Computers Security	User Security Group Security Group Security Group Security Group Security Group			
	Domain Guests Domain Users Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Security Group Security Group Security Group Security Group User User User User Security Group	All domain users Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue		
Renames the current selection.	m				~

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

AnyConnect Admins Properties	?	×
General Members Member Of Managed By		
Members:		
Name Active Directory Domain Services Folder		
Add Remove		
OK Cancel	Appl	y

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**.

Select Users, Contacts, Computers, Service Accounts,	or Groups	×
Select this object type:		
Users, Service Accounts, Groups, or Other objects		Qbject Types
From this location:		
example.com		Locations
Enter the object names to select (examples):		
IT Admin (It.admin@example.com)		Check Names
Advanced	OK	Cancel

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.

AnyConn	ect Admin	s Properties			?	×
General	Members	Member Of	Managed By			
Membe	rs:					_
Name	Admin	Active Dir example.c	ectory Domain :om/Users	Services Folder		
Ad	4	Remove	1			-
	u	1 Kino 10				
			ОК	Cancel	Ар	ply

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

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

🖅 Run			>
0	Type the name of a progra resource, and Windows wi	im, folder, docum Il open it for you.	ent, or Internet
<u>O</u> pen:	mmc.exe		~
	ОК	Cancel	Browse

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

🚡 Cons	ole1 - [Console R	oot]		-	o x
🚡 File	Action View	Favorites	Window	Help	- 8 ×
4 1	New		Ctrl+N		
	Open		Ctrl+O	Actions	
S	Save Save Ar		Ctrl+S	There are no items to show in this view. Console Root	-
2 ( 1 2 8	Add/Remove Snap Options I dnsmgmt 2 dsa Exit	p-in	Ctrl+M	More Actions	<b>F</b>
Enables yo	ou to add snap-ins	to or remo	ove them fro	om the snap-in console.	

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

Add or Remove Snap-ins				X
You can select snap-ins for t extensible snap-ins, you car	this console from the configure which e	nose xter	e available on your computer and configure the selected set of snap-ins. For ensions are enabled.	
Available snap-ins:			Selected snap-ins:	_
Snap-in	Vendor	^	Console Root Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor		Bemove	
Active Directory Use	Microsoft Cor Microsoft Cor		Move Up	1
AUSI Edit	Microsoft Cor		Add >	
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			
Device Manager	Microsoft Cor			_
Disk Management	Microsoft and	$\checkmark$	Advanced	
Description:	we you to browea	the	e contants of the certificate stores for yourself a service, or a computer	
	ins you to bromse		e contento or are certandate stores for yoursen, a service, or a computer.	
			OK Cancel	

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

Certificates snap-in	×
This snap-in will always manage certificates for: 	
< Back Next > Cancel	

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

Select Computer	×
Select the computer you want this snap-in to manage.         This snap-in will always manage: <ul> <li>Local computer: (the computer this console is running on)</li> <li>Another computer:</li> <li>Another computer:</li> <li>Browse</li> </ul> Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

## 5. Fare clic su OK.

Add or Remove Snap-ins						×
You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	ose xter	available on you nsions are enable	r computer and configure the selected d.	set of snap-ins. For	
Available snap-ins:				elected snap-ins:	_	
Snap-in	Vendor	^		Console Root	Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor			ଢ니 Certificates (Local Computer)	Remove	
Active Directory Use	Microsoft Cor Microsoft Cor				Move <u>U</u> p	
Authorization Manager	Microsoft Cor Microsoft Cor		Add >		Move <u>D</u> own	
Certificates	Microsoft Cor Microsoft Cor					
Component Services	Microsoft Cor Microsoft Cor					
Disk Management	Microsoft and	v			Ad <u>v</u> anced	
Description:						
The Certificates snap-in allo	ows you to browse	the	contents of the	certificate stores for yourself, a servic	e, or a computer.	
					OK Cancel	

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.

ᡖ Console1 - [Console Root\Certific	ates (Local Computer)\Personal\C	ertificates]		-	o x
File Action View Favorites	Window Help				- 8 ×
🗢 🏟 🖄 📆 📋 🙆 😹	<b>I</b>				
Console Root     Certificates (Local Computer)     Certificates (Local Computer)     Personal     Certificates     Trusted Root Certification     Enterprise Trust     Intermediate Certification     Trusted Publishers     Untrusted Publishers     Untrusted Certificates     Third-Party Root Certificat     Trusted People     Client Authentication Issue     Preview Build Roots     Local NonRemovable Cert     Remote Desktop     Certificate Enrollment Req     Smart Card Trusted People	Issued To	Issued By example-WIN2016-CA example-WIN2016-CA example-WIN2016-CA	Expiration Da 4/19/2060 4/27/2025 4/28/2021	Actions Certificates More Actions	• •
Sinar Card indice nous     Trusted Devices     Web Hosting     Windows Live ID Token Iss					
< >	<		>		
Personal store contains 3 certificates.					

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**.

🙀 Certif	ficate				×
General	Details	Certification Pa	1th		
Show:	<al></al>		~		
Field			Value		^
<u>詞</u> Sut	bject		win2016.examp	le.com	
📋 Put	blic key		RSA (2048 Bits)		
Put	blic key pa	arameters	05 00		
Ce	rtificate T	emplate Name	DomainControlle	r	
Ent Contraction	hanced Ke	ey Usage	Client Authentic	ation (1.3.6.1	
() () () () () () () () () () () () () (	IME Capa	Dilities	[1]SMIME Capat	olity: Object I	
	bject Key Iboritu Ka	Identifier	30 D7 20 He H8 0	27 fb 11 16	¥
CN = w	in2016.e:	<pre>kample.com</pre>			
		[	Edit Properties	Copy to File	
				O	¢

🙀 Certif	ficate			×
General	Details	Certification Path		
Show:	<al></al>		$\sim$	
Field	bject Key thority Ke L Distribu thority In	Identifier ty Identifier tion Points formation Access	Value 30 b7 2b 4e 48 0f 2f 17 17 e6 KeyID=3d 9f 26 37 fb 11 1f 4 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc Other Name-DS Object Guid=	^
Ke: The The	y Usage umbprint umborint	algorithm	Digital Signature, Key Encipher sha1 ca.8e 11 3d eb.bc 0f 6e 4a 00	~
Other N DS 0 18 DNS Na	lame: Object Gu me=win2	id=04 10 90 99 a9 016.example.com	a2 38 24 65 47 84 74 64 26 cd c6 8	D
		Ed	It Properties Copy to File	
			0	¢

In Utilizzo chiavi avanzato è presente Autenticazione server.

General       Details       Certification Path         Show: <al>          Field       Value         Subject       win2016.example.com         Public key       RSA (2048 Bits)         Public key parameters       05 00         Certificate Template Name       DomainController         Enhanced Key Usage       Client Authentication (1.3.6.1         Subject Key Identifier       30 b7 2b 4e 48 0f 2f 17 17 e6         Subject Key Identifier       Sol b7 2b 4e 48 0f 2f 17 17 e6         Authority Key Identifier       KeyID=3d 9f 26 37 fb 111 1f 4</al>	🙀 Certi	ficate			×
Show:       <	General	Details	Certification Path		
Field       Value         Subject       win2016.example.com         Public key       RSA (2048 Bits)         Public key parameters       05 00         Certificate Template Name       DomainController         Enhanced Key Usage       Clent Authentication (1.3.6.1         SMIME Capabilities       [1]SMIME Capability: Object I         Subject Key Identifier       30 b7 2b 4e 48 0f 2f 17 17 e6         Subject Key Identifier       KevID=3d 9f 26 37 fb 11 1f 4	Show:	<al)></al)>		~	
Subject       win2016.example.com         Public key       RSA (2048 Bits)         Public key parameters       05 00         Certificate Template Name       DomainController         Enhanced Key Usage       Clent Authentication (1.3.6.1         SMIME Capabilities       [1]SMIME Capability: Object I         Subject Key Identifier       30 b7 2b 4e 48 0f 2f 17 17 e6         Authority Key Identifier       KeyID=3d 9f 26 37 fb 11 1f 4	Field			Value	^
Clert function (1.3.6.1         Enhanced Key Usage         Clent Authentication (1.3.6.1         Subject Key Identifier         30 b7 2b 4e 48 0f 2f 17 17 e6         Authority Key Identifier         KeyID=3d 9f 26 37 fb 11 1f 4	E Sul E Pul	bject blic key blic key pr	arameters	win2016.example.com RSA (2048 Bits) 05 00	
Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1) Edit Properties Copy to File	E SM	rtificate T hanced Ki IIME Capa bject Key	emplate Name ey Usage bilities Identifier	Client Authentication (1.3.6.1 [1]SMIME Capability: Object I 30 b7 2b 4e 48 0f 2f 17 17 e6	~
Edit Properties Copy to File	Client / Server	Authentic	tion (1.3.6.1.5.5.) ation (1.3.6.1.5.5	7.3.2) .7.3.1)	
OK			Ed	It Properties Copy to File	

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**.

Certificate	×
General Details Certification Path	
Certification path	
win2016.example.com	
View Certificate	ווכ
Certificate status:	_
This certificate is OK.	
0	ĸ

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

Certificate	×
General Details Certification Path	
Certificate Information This certificate is intended for the following purpose(s):	
All issuance policies     All application policies	
Issued to: example-WIN2016-CA	
Issued by: example-WIN2016-CA	
Valid from 4/27/2020 to 4/19/2060	
Top or Statement	
Issuer Statement	
OK	

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

Certificate		×
General Details Certification Path		
Show: <all></all>	~	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to Subject	V3 13 86 46 e5 9d 70 4f a9 4e 35 sha256RSA sha256 example-WIN2016-CA Monday, April 27, 2020 10:50: Monday, April 19, 2060 10:50: example-WIN2016-CA	>
E	dit Properties Copy to File	
	OK	(

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

÷	F Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, dick Next.	
	Net	
	Cancer	

12. Selezionare X.509 con codifica Base 64.

5° Certificate Export Wizard	
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible	
<ul> <li>Personal Information Exchange - PKCS #12 (.PFX)</li> <li>Include all certificates in the certification path if possible</li> </ul>	
Delete the private key if the export is successful	
Export all extended properties	
Enable certificate privacy	
O Microsoft Serialized Certificate Store (.SST)	

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

Everificate 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	∨ Ö Si	arch Desktop 🔎
Organize 🔻 New folder		III 🔹 😮
Image: Point of the second	Date modified Type No items match your search.	Size
File name: root		~
Save as type: Base64 Encoded X.509 (*.cer)		v
∧ Hide Folders	[	Save Cancel

÷	🚰 Certificate Export Wizard	×
	File to Export Specify the name of the file you want to export	
	File name:	
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cancel	

14. Fare clic su Fine.

÷	Ş	Certificate Export Wizard		×
		Completing the Certificate Exp	oort Wizard	
		You have successfully completed the Certificate	Export wizard.	
		You have specified the following settings:		
		File Name	C:\Users\admin\Desktop\root.cer	
		Export Keys	No	
		Include all certificates in the certification path	No	
		File Format	Base64 Encoded X.509 (*.cer)	
			Finish Can	cel

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----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
\texttt{AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O}
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
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 Plux, Apex o VPN Only sia abilitata.

CISCO. Firepower Device Manager Monitoring Policies Objects	Device: FTD-3
Device Summary Smart License	
CONNECTED Last sync: 16 Apr 2020 08:27 AM SUFFICIENT LICENSE Next sync: 16 Apr 2020 08:37 AM	Go to Cloud Services 🛛 🗢 🗸
SUBSCRIPTION LICENSES INCLUDED	
Threat ENABLE © Disabled by user	Malware Environmental Environm
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.	This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: 🎕 Intrusion Policy	Includes: C File Policy
URL License DISABLE	RA VPN License Type PLUS V DISABLE
C Enabled	S Enabled
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.
Includes: URL Reputation	Includes: RA-VPN

#### Imposta origine identità AD

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

#### mostrato nell'immagine.

cisco. Firepower Devic	ce Manager Monitoring	Policies Objects Device: FTD-3	: ? @ ا	admin Administrator
Object Types 🔶 ^	Identity Sources			
C Networks	1 object		Q Search	+ ~
와 Ports	n NAME	THE	VALUE	RADIUS Server
🔒 Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
🐔 Application Filters				AD
🖉 URLs				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🏫 IPSec Proposals				
🔒 AnyConnect Client				
E Identity Sources				
1 Users				
R Certificates				
🔒 Secret Keys				
DNS Groups				
Vert List Filters				

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

Ŀ.

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

Name	Туре
LAB-AD	Active Directory (AD) ~
Directory Username	Directory Password
ftd.admin@example.com	••••••
e.g. user@example.com	
Base DN	AD Primary Domain
DC=example,DC=com	example.com
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
win2016.example.com:389	*
Hostname / IP Address	Port
Hostname / IP Address win2016.example.com	90rt 389
Hostname / IP Address win2016.example.com e.g. ad.example.com	Port 389
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption	Port 389 Trusted CA certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate   V

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 MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxILVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC ASIwDOX_IKoZlbycNAQEBBQADooEPADCCAQoCcoEBAI8ohT719NzSQooQDb0YT67b	<ul><li></li></ul>
CANCEL	ОК
Directory Server Configuration	
win2016.example.com:636	<b>^</b>

Port

636

Trusted CA certificate

LDAPS\_ROOT

8 ×

```
TEST
```

Hostname / IP Address

e.g. ad.example.com

Encryption

LDAPS

win2016.example.com

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.

cisco. Firepower De	vice Manager Monitoring Policies	Objects Device: FTD-3	* admin * Administrator
Object Types 🛛 🗧 🗧	Identity Sources		
C Networks	2 objects	Q. Snarrh	+ ~
S Ports	H NAME	TYPE VALUE	ACTIONS
Security Zones	1 LocalIdentitySource	LOCAL	
Application Filters	2 LAB-AD	AD win2016.example.com	

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

Pe	ending Changes	<b>@</b> 2	×
<b>O</b> I	Last Deployment Completed Successfully 01 May 2020 12:54 PM. See Deployment History		
	Deployed Version (01 May 2020 12:54 PM)	Pending Version CLEGEND Removed Added Ed	ited
0	Active Directory Realm Added: LAB-AD		^
	- - - - - - - -	<pre>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</pre>	~
м	DRE ACTIONS Y	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.

CISCO. Firepower Device Manager	國 👘 蒜 Monitoring Policies Objects	Device: FTD-3	admin Administrator
	[005 [		
Interfaces Connected Enabled 3 of 4 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Wanagement Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Configured 1 connection   2 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

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



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 a in	nd the A nside net	nyConnect clients they can use to connect to the twork.
Connection Profile Name This name is configured as a connection allas, it can	n be used	to connect to the VPN gateway
General		
Group Alias		Group URL
General		
Add Group Alias		Add Group URL
Primary Identity Source		
Authentication Type		
AAA Only Client Certificate Only	AAA a	nd Client Certificate
Primary Identity Source for User Authenticat	ion	Fallback Local Identity Source 🔔
Filter	~	Please Select Local Identity Source
LocalIdentitySource		^
11 LAB-AD	0	
1 Special-Identities-Realm		~
Create new Y		

#### Client Address Pool Assignment

IPv4 Address Pool Endpoints are provided an address from this pool	IPv6 Address Pool Endpoints are provided an address from this pool
C AnyConnect-Pool	]
+	
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.

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

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

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 deselezionare 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: <u>https://software.cisco.com/download/home</u>. 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	Outside Interface
FTD-3-Manual V	outside (GigabitEthernet0/0)
Fully-qualified Domain Name for the Outside Interf	ace
ftd3.example.com	
e.g. ravpn.example.com	
Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy policy for decrypted traffic option bypasses the access cor and the authorization ACL downloaded from the AAA serve	r inspection by default. Enabling the Bypass Access Control ntrol policy, but for remote access VPN, the VPN Filter ACL er are still applied to VPN traffic
Bypass Access Control policy for decrypted to	raffic (sysopt permit-vpn)
NAT Exempt	
<b>()</b> 0	
Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks +	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.
inside (GigabitEthernet0/1)	+
	الله any-ipv4
AnyConnect Package	
If a user does not already have the right AnyConnect package installer when the client authenticates for the first time. The	ge installed, the system will launch the AnyConnect user can then install the package from the system.
You can download AnyConnect packages from software.cls You must have the necessary AnyConnect software license.	ico.com.
Deskapes	



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	DN .	
Primary Identity Source		
Authentication Type	AAA Only	
Primary Identity Source	赴 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	-	
O Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		

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

cisco. Firepower Dev	rice Manager Monitoring Policies	Device: FTD-3	> 🛃 🔊 🤅	admin Administrator
RA VPN ←	Device Summary Remote Access VPN Connection Profiles			
Connection Profiles	1 object		Q. Search	+
	# NAME	***	GROUP POLICY	ACTIONS
	1 General	Authentication: AAA Only Authorization: None Accounting: None	DfttGrpPolicy	

8. Fare clic su Distribuisci ora.

Pe	ending Changes	0	X	Clos
0	Last Deployment Completed Successfully 16 Apr 2020 12:41 PM. <u>See Deployment History</u>			.105
	Deployed Version (16 Apr 2020 12:41 PM)	Pending Version C LEGEND Removed Added	Edite	d
0	Network Object Added: AnyConnect-Pool			^
	-	<pre>subType: Network value: 10.10.10.0/24 isSystemDefined: false dnsResolution: IPV4_AND_IPV6 name: AnyConnect-Pool</pre>		
0	RA VPN Added: NGFW-Remote-Access-VPN			
	-	<pre>vpnGatewaySettings[0].exemptNatRule: true vpnGatewaySettings[0].outsideFqdn: ftd3.example.com vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: name: NGFW-Remote-Access-VPN</pre>	t	l
	anyconnectPackageFiles:			
	-	anyconnect-win-4.7.03052-webdeploy-k9.pkg		
	-	FTD-3-Manual		
	<pre>vpnGatewaySettings[0].outsideInterface:</pre>			
	-	outside		
	<pre>vpnGatewaySettings[0].insideInterfaces:</pre>	- Local da		
	vpnGatewaySettings[0].insideNetworks;	inside		~
м	DRE ACTIONS Y	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.

cisco. Firepower De	wice Manager Monitoring	Policies Objects	Device: FTD-3	> 🗎	3 ?	admin Administrator	
Security Policie     ⊡ → ○ SSL Decry	rS potion → <mark>O identity</mark> → O Seci	unity Intelligence $\rightarrow$	NAT $ ightarrow$ Access Control				
	Establishing User Identity You can use identity policies to collect identity information from connections, can then view usage based on user ide in the dashboards, and configure acce control based on user or user group. B linking network behavior, traffic, and er directly to individual users, the system help you identify the source of policy breaches, attacks, or network vulnerabilities.	t user You entity ess By USERS in can	How Identity policies Passive authentication Action PASSIVE AUTHENTING WULTIPLE MULTIPLE MU	Cies work	ge identity		
			ENABLE IDENTITY I	POLICY			

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

cisco. Firepo	wer Device Manage	r Mor	itoring Policies	詳正 Objects	Device: FTD-3		D 🔒 🛛	?:	admin Administrator	,
🛷 Security P	olicies									
<b>₽</b> → 0 s	SL Decryption $\rightarrow$	Identity $\Rightarrow$	O Security Intellige	nce 🔿 🕝 NA	AT $ ightarrow$ 🕗 Acc	ess Control \Rightarrow 👋 I	intrusion			
Identity Policy	D					Q Search			¢ <u>a</u> +	
			SOURCE			DESTINATION				
H NAME	AUTHONTICATION	AUTH, TYPE	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	ACTIONS	
				These are on k	dentify rules wet.					
				Start by creating t	he first identity rule					
				CREATE ID	ENTITY RULE					
Default Action	Passive Auth Any	Identity Source	· 0							

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.

cisco. Firepowe	er Device I	Manager	Monitorin	g Policies	Objects	Device: FTD-3		۵. 🚑	3	admin Admini	strator
🛷 Security Po	licies										
□ → O sst	Decryption	-> 📀 Id	entity $\rightarrow$ ()	Security Intelligen	ce $ ightarrow$ 🖌 NA	T $ ightarrow$ 🖉 Acce	ess Control $\rightarrow$	S Intrusion			
1 rule							4	Q Search			+
			OFFICINAL PACKET				TRANSLATED PACKE	T			
II NAME	TYPE	INTERFACES	SOUNCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	SOURCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS
Auto NAT Rules											
> # Internet_PAT	DYNAMIC	J 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.

cisco. Firepo	wer Device Manager	题 Monitoring	Ø Policies	前面 Objects	Device: FTD-3		o. 🔮	0 ?	ad Ad	min v Iministrator
🕫 Security F	Policies									
□ → ○ 5	SSL Decryption $\rightarrow$ 🥏	Identity $\rightarrow$ () s	Security Intelligen	ce 🔿 🕝 N/	AT $ ightarrow$ Acces	is Control 🔿 🛛 🍕	Intrusion			
						Q Search				®. +
	SOURCE			DESTINATION						
* NAME	ACTION ZONES	METWORKS	PORTS	20463	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
				There are no i	access rules yet.					
				Start by creating	the first access rule.					
				CREATE A	CCESS RULE					
Default Action	Access Control 😑 Block	9, B, I v								

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 connetteranno 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	Rul	e										×
Order Title 1  AC R Source/Destination	DP Ad	pplications URLs (	Use	Action Allow rs Intrusion Policy	~ F	File policy						
SOURCE						DESTINATION						
Zones	+	Networks	÷	Ports +		Zones	÷	Networks	+	Ports/Protocols		+
outside_zone		AnyConnect-Pool		ANY		inside_zone		C Inside_Net				
										$\Leftrightarrow$ RDP-UDP		
Show Diagram	$\supset$	e     Not hit yet							C/	WCEL	ок	

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	Ø 1	×
Order Title 1  AC RDP Access Source/Destination Applications URLs Users	Action       Allow     Y       Intrusion Policy     File policy   Logging	
AVAILABLE USERS	L CONTROLLING ACCESS FOR USERS AND USER GROUPS	
▼ Filter Identity Sources Groups Users 主 LAB-AD \ Account Operators 主 LAB-AD \ Administrators 主 LAB-AD \ Allowed RODC Password Replication Group ② 主 LAB-AD \ AnyConnect Admins 主 LAB-AD \ AnyConnect Users	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.	5
Show Diagram	CANCEL OK	

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

Add Access Rule	• ×
Order     Title     Action       1     AC RDP Access     Image: Comparison of the second	w ❤ ♥ File policy♥ Logging
AVAILABLE USERS	Lt 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	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 Ru	le				o ×
Order Title		Action			
2 Y AC HTTP	Access	Allow 🚿			
Source/Destination A	opplications URLs Use	ers Intrusion Policy	File policy Logging		
SOURCE			DESTINATION		
Zones +	Networks +	Ports +	Zones	Networks	+ Ports/Protocols +
outside_zone	AnyConnect-Pool	ANY	a inside_zone	Inside_Net	5 нттр
Show Diagram	O     Not hit yet				CANCEL OK
Edit Access Ru	le				Ø X
Order Title	Arrass	Action			
2 · Auntr	ALCERS		•		
Source/Destination A	opplications URLs Use	ars Intrusion Policy	File policy Logging		
AVAILABLE USERS		+	1 CONTROLLING ACCES	S FOR USERS AND USER	GROUPS
LAB-AD \ AnyConnect	Users		If you configure identity address, you can contr membership. By contro appropriate access cor different address throu network access change from one group to anot	policies to establish u of access based on use ling access based on use trois whether the user gh DHCP. If you base n is as users change role her.	ser identity based on source IP or name or user group user identity, you can apply the changes workstations or obtains a ules on group membership, user is in your organization, moving
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.

ului cisc	Firepowe	er Device	e Manager	Monitoring	Policies	HE Objects D	evice: FTD-3		0	0?	) : (;	idmin Administrat	or ~
øs	Security Policies												
Ð	$\rightarrow$ $\bigcirc$ SSL	Decryptio	o 🔶 🥑 Idem	tity $\rightarrow$ $\bigcirc$ Se	curity Intelligence	ightarrow 📀 nat	→ 🖌 Access	Control $\Rightarrow$ 9	Intrusion				
2 rules								Q Search				0	+
			SOURCE			DESTINATION	3						
	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO_	APPLICATIONS	UNLS	USERS		ACTIONS
> 1	AC RDP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Not	RDP-TCP RDP-UDP	ANY	ANY	AnyConne	Ф.С.	
> 2	AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne	9 C	
Defau	It Action Acco	ess Control	O Block	₽									

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

Pe	ending Changes		0	×				
•	Last Deployment Completed Successfully     28 Apr 2020 01:35 PM. See Deployment History							
	Deployed Version (28 Apr 2020 01:35 PM)	Pending Version CLEGEND Removed	Added	Edited				
0	Access Rule Added: AC HTTP Access			^				
	- - - -	users[0].name: AnyConnect Users logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HTTP Access						
	sourceZones:	estrida zona						
	destinationZones:	ourside_tone						
	-	inside_zone						
	sourceNetworks:							
	-	AnyConnect-Pool						
	destinationNetworks:							
	-	Inside_Net						
	destinationPorts:	11770						
	- users[0] identitySource:	nir						
	-	LAB-AD						
				~				
0	Access Rule Added: AC RDP Access							
M	ORE ACTIONS Y	CANCEL DEPLOY N	woi	~				

# 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 serverport 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password \*\*\*\*\* ldap-logindn 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

Cisco AnyConnect Secure M VPN: Contacting ftd3.4 ftd3.example.co	example.com.
	Sisco AnyConnect   ftd3.example.com   Group:   General   Username:   it.admin   Password:
	OK Cancel
Cisco AnyConnect Secure M VPN: Connected to ftd ftd3.example.co 00:00:14	obility Client – X 3.example.com. m V Disconnect IPv4

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 Idap 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 0x00002bld13f4bbf0, 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
       objectClass: value = person
[53]
[53]
      objectClass: value = organizationalPerson
[53] objectClass: value = user
[53]
      cn: value = IT Admin
      sn: value = Admin
[53]
      givenName: value = IT
[53]
[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
      badPasswordTime: value = 132320354378176394
[53]
[53]
      lastLogoff: value = 0
      lastLogon: value = 0
[53]
[53]
      pwdLastSet: value = 132319114917186142
      primaryGroupID: value = 513
[53]
      objectSid: value = .....{I...;....j...
[53]
      accountExpires: value = 9223372036854775807
[53]
      logonCount: value = 0
[53]
[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
      dSCorePropagationData: value = 16010101000000.0Z
[53]
      lastLogonTimestamp: value = 132319755825875876
[53]
[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 **Idp.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 Idp.exe.

💷 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	ldp.exe 🗸
	OK Cancel <u>B</u> rowse

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

🕼 Ldp	_		×
Connection Browse View Options Utilities Help			
Connect			
Bind Ctrl+B			
Disconnect			
New Ctrl+N			
Save			
Exit			
		NUM	

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

Connect		×
<u>S</u> erver:	localhost	
Port:	389	Connectionless
<u>0</u> K		<u>C</u> ancel

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

🔝 Idap://wi	in2016.exar	mple.co	m/DC:	DC=example,DC=com					×
Connection	Browse	View	Optio	ns Utilities	Help				
Connec Bind Disconn New Save Save As Exit	t	Ctrl+B Ctrl+N		Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD configur CN= current Tim defaultM dnsHos domain dsServi Sett Firs Nan con forestFu highest( isGlobal isSynch IdanSer	en ("localho connection ase DSA in tries: SE) rationNamin =Configurati Time: 5/1/20 e; VamingConte tName: win ControllerFu Functionality iceName: Cl tings,CN=W it-Site- me,CN=Sites n; unctionality: CommittedU ICatalogRea pronized: TF	est", 389); to localhost. formation gContext: ion,DC=examp 2016.example inctionality: 7 = y: 7 = (WIN201 N=NTDS /IN2016,CN=Se s,CN=Configur SN: 13410; ady: TRUE; RUE; example.com	le,DC=c I Easter ple,DC= .com; = ( WIN2 16 ); ervers,C ation,DC 6 ); win2016	:om; 'n Daylight com; 2016 ); 2N=Default- C=example,D	)C=
									7

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

Bind	×
<u>U</u> ser: Password:	ftd.admin@example.com
Domain: Bind type Bind as <u>cu</u> Bind with c Simple bind Advanced	rrently logged on user credentials (DIGEST) affic after bind
Ad <u>v</u> anced	Cancel OK

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

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		×	
Connection	Browse	View	Options	Utilities	Help					
				1.2.3 1.2.3 1.2.3 Supports Max Max Max Max Max Max Max Max Max Supports Supports SPN	840.113556 840.113556 840.113556 edLDAPPolic PercentDirs ReceiveBut Connection BatchRetur DirSyncDur ResultSetSi ResultSetSi ValRange; I edLDAPVer edSASLMed IEGO; EXTEI	.1.4.2255; .1.4.2256; .1.4.2309; cies (20): Ma SyncRequest ffer; InitRecv s; MaxConnk nMessages; ation; MaxTe ize; MinResu PerConn; Ma: MaxValRang Limit; System sion (2): 3; 2 chanisms (4) RNAL; DIGES s(Id, 'ftd.adn	xPoolThre s; MaxDa Timeout; dleTime; M MaxQuer empTableS ItSets; xNotificat eTransitiv MemoryL ; : GSSAPI 5T-MD5;	eads; tagramRe MaxPageS yDuration Size; ionPerCon re; imitPerce ; GSS-	ecv; Size; n; nn; nn;	^
			-	uthenticate	ed as: 'EXAI	/IPLE\ftd.adm	iin'.		J	~
Ready			1							

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

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC:	=com		_		×
Connection	Browse	View	Options	Utilities	Help				
			r A E S C E	Max Max Max Three supporte supporte SPN es = Idap_s unavailable cuthenticate es = Idap_s unavailable rror <49>: I cerver error comment: Ac rror 0x8009 ivalid	ResultSets ResultSets ValRange; adMemoryl edLDAPVer edSASLMed EGO; EXTE imple_bind_ >); // v.3 ed as: 'EXAI imple_bind_ >); // v.3 dap_simple : 80090308 cceptSecur 90308 The t	ize; MinResi PerConn; Ma MaxValRang Limit; Syster sion (2): 3; 2 chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad MPLE\ftd.adr _s(Id, 'wrong _bind_s() fa : LdapErr: D ityContext e token supplie	ultSets; axNotificat geTransition MemoryL 2; ): GSSAPI ST-MD5; min@exar min". g@examp niled: Invali SID-0C090 rror, data ed to the f	ionPerConn ve; imitPercent ; GSS- mple.com', le.com', id Credentia 042A, 52e, v3839 unction is	Is
Ready									¥

#### 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.

Idap://win2016.exa	Idap://win2016.example.com/DC=example,DC=com								
Connection Browse	Viev	v Options	Utilities	Help					
Connection Browse	Viev	Options Tree Enterprise O Status Bar Set Font	Utilities Configurat Max Max Max Max	AxPoolThreads; sts; MaxDatagramRecv; vTimeout; nkleTime; MaxPageSize s; MaxQueryDuration; ; MaxTempTableSize; linResultSets; onn; MaxNotificationPerConn; /alRangeTransitive; SystemMemoryLimitPercent; (2): 3; 2;					
			Thre supporte supporte SPN es = Idap_s unavailable Authenticate	adMemo adLDAPV adSASLM EGO; EX imple_bir >); // v.3 ad as: 'EX	stemMemo 3; 2; (4): GSS GEST-MD .admin@e admin'.	ryLimitPero API; GSS- 5; xample.co	cent; m',		
								~	,

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

Tree View	×
BaseDN: DC=example,DC=com	~
Cancel	ОК

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

🔝 Idap://wi	n2016.exa	- 🗆 X					
Connection	Browse	View	Options	Utilities	Help		
<u> •</u> · <u> DC=exam</u>	iple,DC=c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy DN Copy Select al Clear ou	ist View DN Id e ed N	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ple,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~
Create a new o	locument						

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

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×	
Connection	Browse View Options Utilities Help		
Search	×	C=example,DC=com; 58811D1ADED00C04FD8D5CD:C	^
Base DN:	DC=example,DC=com ~	58811D1ADED00C04FD8D5CD:C	
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:0	
Scope O Base	One Level Subtree	lers,DC=example,DC=com; \$8811D1ADED00C04FD8D5CD:C =example,DC=com;	
Attributes:	objectClass;name;description;canonicalName $\sim$	68811D1ADED00C04FD8D5CD:C mple,DC=com;	
Options	Run Close	2020 3:43:59 PM Eastern Daylight 20 2:41:57 PM Eastern Daylight	
	 ***Searching Idap_search_s(Id, "DC= "sAMAccountName=it.a Getting 0 entries:	example,DC=com", 2, admi", attrList, 0, &msg)	~
Ready			

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. Idp trova 1 voce nel DN di base dc=example,dc=com e stampa il DN di tale utente.

🔐 Idap://wi	n2016.example.	com/DC=ex	ample,DC	=com		- 🗆 ×	<
Connection	Browse View	Options	Utilities	Help			
Search					$\times$	58811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^
Base <u>D</u> N: Filter:	DC=example,D	C=com ne=it.admin			~	58811D1ADED00C04FD8D5CD:C ample,DC=com; D211D1AA4B00C04FD7D83A:O lers DC=example DC=com;	
Scope	O <u>O</u> ne Level	● <u>S</u> ubtre	e			58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple_DC=com;	
<u>A</u> ttributes:	objectClass;nam	ne;descriptior	n;canonicalN	lame	$\sim$	020 3:43:59 PM Eastern Daylight	
O <u>p</u> tions		<u>R</u> un	1	<u>C</u> lose		)20 2:41:57 PM Eastern Daylight	
		k v C C	**Searching dap_search sAMAccour Setting 1 ent On: CN=IT A canonic name: IT objectCl use	I _s(Id, "I ntName: tries: Admin,( alName: Admin; ass (4): r;	DC=e =it.ad C <b>N=U</b> exar top;	example,DC=com", 2, Imin", attrList, 0, &msg) Isers,DC=example,DC=com mple.com/Users/IT Admin; person; organizationalPerson;	
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]
               = [SUBTREE]
       Scope
[-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>
                        192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
   4: 23:02:16.772482
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
                        192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
  5: 23:02:16.772924
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
                          192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
   6: 23:02:16.772955
<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.

=	Best match										
ŵ	Event Viewer Desktop app										
	Settings	Settings >									
	🖄 Viev	v even	nt logs								
ŝ	चि	ŵ	ß	п	R		ła				
~		÷	U				.44				
	event										
	ו כ	()	e	_	1	2	-				

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\$ Account 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