Configurare la gestione delle password utilizzando LDAP per RA VPN su FTD Gestito da FMC

Sommario

Introduzione **Prerequisiti Requisiti** Componenti usati Configurazione Esempio di rete e scenario Determinare il DN di base e il DN gruppo LDAP Copia radice certificato SSL LDAPS In caso di più certificati installati nell'archivio del computer locale sul server LDAP (facoltativo) **Configurazioni FMC** Verifica delle licenze Imposta realm Configurazione di AnyConnect per la gestione delle password Implementazione **Configurazione finale Configurazione AAA Configurazione AnyConnect** Verifica Connettersi con AnyConnect e verificare il processo di gestione delle password per la connessione utente Risoluzione dei problemi Debua Debug relativi alla gestione delle password durante il lavoro Errori comuni rilevati durante la gestione delle password

Introduzione

In questo documento viene descritto come configurare la gestione delle password con gli elenchi LDAP per i client AnyConnect che si connettono a Cisco Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Conoscenze base della configurazione di RMA VPN (Remote Access Virtual Private Network) su FMC
- Conoscenze base della configurazione del server LDAP in FMC
- Conoscenze base di Active Directory

Componenti usati

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

- Server Microsoft 2012 R2
- FMCv con versione 7.3.0
- FTDv in esecuzione 7.3.0

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 di rete e scenario



Il server Windows è preconfigurato con ADDS e ADCS per verificare il processo di gestione delle password degli utenti. In questa guida alla configurazione, vengono creati questi account utente.

Account utente:

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

Determinare il DN di base e il DN gruppo LDAP

1. Open (Aperto) Active Directory Users and Computers tramite il dashboard di Server Manager.

Server Ma	nager • Dashboard		
Example 2 Construction Example 2 Const	CUICK START CUICK START CUICK START C Add roles and features Add roles and features Add roles and features Add roles and features C Add roles	Active Directory Module for Windows PowerShell Active Directory Dises and Services Active Directory Users and Computers AD F5 Management AD5 Edit Certification Authority Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management Health Registration Authority Internet Information Services (IIS) Manager (ICS) Initiator Local Security Policy	
	Role: 7 Server group: 1 Servers total: 1 AD CS Manageability Events Services Performance BPA results 	1 AD FS 1 Image ability Image ability Events Events Services Services Performance BPA results	Network Policy Server OBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) Man Resource Monitor Even Services Servit Services Servit System Information BPA Task Scheduler Windows Firewall with Advanced Security Windows Memory Diagnostic Windows PowerShell
	IIS 1 • Manageability • Manageability Events • Manageability Services Performance BPA results BPA results	1 Imageability Imageability Imageability Events Services Performance BPA results BPA results	Windows PowerShell (k86) Windows PowerShell ISE Windows PowerShell ISE Windows Server Backup Windows Server Backup

2. Aprire il view Option nel pannello superiore e attivare Advanced Features, come mostrato nell'immagine:

	Active Directory U	Jsers and Computers	_ □ ×
File Action View	/ Help		
🗢 🔿 🖄 [Add/Remove Columns		
Active Direct Add/Remove Columns Active Direct Large Icons Saved Q Small Icons Built Detail Corr Detail Fore Addvanced Features Filter Options Filter Options Pros Customize		n ntainer for up ntainer for do ntainer for sec ntainer for or ntainer for ma :ation for stor :em settings ntainer for up	
 Systèm Users NTDS Que TPM Devision 	tas tas tes	pecifications co	
Displays items in a list			
Displays items in a list			

 In questo modo è possibile visualizzare proprietà aggiuntive negli oggetti AD.
 Ad esempio, per trovare il DN per la radice razor.local, fare clic con il pulsante destro del mouse razor.locale quindi scegliere Properties, come mostrato nell'immagine:



4. Inferiore Properties, scegliere il Attribute Editor scheda. Cerca distinguishedName in Attributi (Attributes), fate clic su View, come illustrato nell'immagine.

Verrà visualizzata una nuova finestra in cui il DN può essere copiato e incollato in FMC in un secondo momento.

In questo esempio, il DN radice è _{DC=razor}, _{DC=local}. Copiare il valore e salvarlo per utilizzarlo in seguito. Fare clic su _{OK} per uscire dalla finestra Editor attributi stringa e fare clic su _{OK} per uscire dalla finestra di dialogo Proprietà.

raz	zor.local Properties ?	x				
General Managed By Ob	oject Security Attribute Editor					
Attributes:						
Attribute	Value	~				
defaultLocalPolicyObj	<not set=""></not>					
description	<not set=""></not>					
desktopProfile	<not set=""></not>	=				
displayName	<not set=""></not>					
displayNamePrintable	<not set=""></not>					
distinguishedName	DC=razor,DC=local					
domainPolicyObject	<not set=""></not>					
domainReplica	<not set=""></not>					
dSASignature	{ V1: Flags = 0x0; LatencySecs = 0; DsaGuid					
dSCorePropagationD	0x0 = ()					
eFSPolicy	<not set=""></not>					
extensionName	<not set=""></not>					
flags	<not set=""></not>					
forceLogoff	(never)	~				
< 111	>					
View	Filter					
Stri	String Attribute Editor					
Attribute: distinguishedName						
Value						
DC=razor,DC=local						
Clear	OK Cano	el				

Copia radice certificato SSL LDAPS

1. Premere Win+R e immettere mmc.exe, quindi scegliere OK, come mostrato nell'immagine.



2. Passa a File > Add/Remove Snap-in..., come mostrato nell'immagine:

Sec. 1997	Console1 - [Console Root]	_ D X
File Action View Favorites Window Help		_ <i>8</i> ×
New Ctrl+N		
Open Ctrl+O	Actions	
Save Ctrl+S	There are no items to show in this view. Console	Root 🔺
Save As	More A	Actions 🕨
Add/Remove Snap-in Ctrl+M		
1 C:\Windows\system32\dsa		
3 C:\Windows\system32\certmar		
4 C:\Windows\system32\certsrv		
Exit		
Enables you to add snap-ins to or remove them from the snap	p-in console.	

3. In snap-in disponibili scegliere Certificates e quindi fare clic su Add, come mostrato nell'immagine:

nap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Remove
Active Directory Site	Microsoft Cor			Genove
Active Directory Use	Microsoft Cor			
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			Move Down
Authorization Manager	Microsoft Cor		<u>A</u> dd >	
Certificate Templates	Microsoft Cor			
Cerdicates	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
Disk Management	Microsoft and			Advanced
		~		Auvanced

4. Scegli Computer account e quindi fare clic su Next, come mostrato nell'immagine:

Certificates snap-in	×
This snap+n will always manage certificates for: ○ My user account ○ Service account ⓒ Computer account	
< <u>B</u> ack <u>N</u> ext > Cancel	

Come mostrato di seguito, fare clic su Finish.

Select Computer	Х
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: (the computer this console is running on) Another computer:	
< Back Finish Cancel	

5. Fare clic su $_{\rm OK}$, come mostrato nell'immagine.

nap-in	Vendor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Certificates (Local Computer)	Remove
Active Directory Site	Microsoft Cor				Lawrence and the second s
Active Directory Use	Microsoft Cor				
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor				Move Down
Authorization Manager	Microsoft Cor		<u>A</u> dd >		and the second se
Certificate Templates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
Disk Management	Microsoft and	~			Advanced
)		
cription:					

- 6. Espandere la Personal, quindi fare clic su Certificates. Il certificato utilizzato da LDAP deve essere rilasciato al nome di dominio completo (FQDN) del server Windows. In questo server sono elencati tre certificati:
- Certificato CA rilasciato a e da razor-WIN-E3SKFJQD6J7-CA.
- Certificato CA rilasciato a e da supinfo-WIN-FNJVP9QUEH9-CA.
- Un certificato di identità è stato rilasciato a WIN-E3SKFJQD6J7.razor.local da razor-WIN-E3SKFJQD6J7-CA.

In questa guida alla configurazione, il nome di dominio completo è WIN-E3SKFJQD6J7.razor.local i primi due certificati non sono pertanto validi per l'utilizzo come certificato SSL LDAP. Il certificato di identità rilasciato a WIN-E3SKFJQD6J7.razor.local è un certificato rilasciato automaticamente dal servizio CA di Windows Server. Fare doppio clic sul certificato per controllare i dettagli.



- 7. Per essere utilizzato come certificato SSL LDAP, 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.

Nell'ambito Details per il certificato, scegliere Subject Alternative Name, dove FQDN WIN-E3SKFJQD6J7.razor.local presente.

Ce Ce	rtificate ×					
General Details Certification Path	1					
Show: <all></all>	~					
Field	Value					
Enhanced Key Usage	Client Authentication (1.3.6.1					
Application Policies	[1]Application Certificate Polic					
Subject Key Identifier	1b 34 75 f8 c4 3e ef 58 fb 43					
Authority Key Identifier	KeyID=cf 83 92 a4 14 00 e7 5					
CRL Distribution Points	[1]CRL Distribution Point: Distr					
Authority Information Access	[1]Authority Info Access: Acc					
🖳 Key Usage	Digital Signature, Key Encipher					
Subject Alternative Name	DNS Name=WIN-E3SKFJQD6J 🗸					
DNS Name=WIN-E3SKFJQD6J7.razor.local						
DNS Name=razor.local DNS Name=RAZOR						
F	dit Properties Copy to File					
	copy which					
Learn more about <u>certificate details</u>						
	OK					
	UK					

Inferiore Enhanced Key Usage, Server Authentication presente.

📃 Cer	tificate X				
General Details Certification Path					
Show: <all></all>	×				
Field Certificate Template Inform	Value ^ Template=LDAPoverSSL(1.3.6 Client Authentication (1.3.6.1				
Application Policies Subject Key Identifier Authority Key Identifier	[1] Application Certificate Polic 1b 34 75 f8 c4 3e ef 58 fb 43 KeyID=cf 83 92 a4 14 00 e7 5 ≡ [1] CPL Diatribution Daipt. Diatr				
Authority Information Access	[1] Authority Info Access: Acc Digital Signature, Key Encipher V				
Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) KDC Authentication (1.3.6.1.5.2.3.5)					
Edit Properties Copy to File Learn more about <u>certificate details</u>					
	ОК				

8. Una volta confermata, ai sensi dell'articolo Certification Path, scegliere il certificato di primo livello che corrisponde al certificato CA radice e quindi fare clic su View Certificate. Verranno aperti i dettagli del certificato della CA radice, come illustrato nell'immagine:

Certificate	x	R Certificate X
General Details Certification Path Certification path Tay razor-WIN-E3SKFJQD6J7-CA WIN-E3SKFJQD6J7.razor.local		General Details Certification Path Image: Certificate Information This certificate is intended for the following purpose(s): • All issuance policies • All application policies
View Certificate]	Issued to: razor-WIN-E3SKFJQD6J7-CA Issued by: razor-WIN-E3SKFJQD6J7-CA
Certificate status: This certificate is OK.		Valid from 3/22/2021 to 3/22/2026
Learn more about <u>certification paths</u>		Issuer Statement
OK		OK

9. Nell'ambito Details del certificato CA radice, fare clic su Copy to File e navigare attraversoCertificate Export Wizard che esporta la CA radice in formato PEM.

Scegli Base-64 encoded X.509 come formato di file.

e 🦻	Certificate Export Wizard		
	Completing the Certificate Exp	port Wizard	
	You have successfully completed the Certificate	Export wizard.	
	You have specified the following settings:		
	File Name	C:\Users\Administrator\Downloads\roo	
	Export Keys Include all certificates in the certification path	No No	
	File Format	Base64 Encoded X.509 (*.cer)	
	< 111	>	J
		Finish C	ancel

10. Aprire il certificato CA radice archiviato nel percorso selezionato nel computer con un blocco note o un altro editor di testo.

Mostra il certificato del formato PEM. Salva per uso futuro.

----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgovcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCguBWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvcGCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41nOAziGs4ZMNM1X8UWeKuwi8w9kncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61EOAVCCSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIAA4IBAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q4sMZffbVrG1Rz7twW36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1bGuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi2OZy1tHR1dfUUbwVENSFQtDnFA7X

In caso di più certificati installati nell'archivio del computer locale sul server LDAP (facoltativo)

1. In una situazione di più certificati di identità utilizzabili da LDAPS e in caso di incertezza sul tipo di certificato utilizzato o in assenza di accesso al server LDAPS, è ancora possibile estrarre la CA radice da un'acquisizione di pacchetti effettuata sul FTD.

2. Se si dispone di più certificati validi per l'autenticazione server nell'archivio certificati del computer locale del server LDAP (ad esempio il controller di dominio di Servizi di dominio Active Directory), si noterà che per le comunicazioni LDAPS viene utilizzato un certificato diverso. La soluzione migliore per questo problema è rimuovere tutti i certificati non necessari dall'archivio certificati del computer locale e disporre di un solo certificato valido per l'autenticazione del server.

Se tuttavia esiste un motivo legittimo per cui sono necessari due o più certificati e si dispone almeno di un server LDAP di Windows Server 2008, è possibile utilizzare l'archivio certificati di Servizi di dominio Active Directory (NTDS\Personale) per le comunicazioni LDAP.

In questa procedura viene illustrato come esportare un certificato abilitato per LDAPS dall'archivio certificati di un computer locale del controller di dominio all'archivio certificati del servizio Servizi di dominio Active Directory (NTDS\Personale).

- Passare alla console MMC nel server Active Directory, scegliere File e quindi fare clic su Add/Remove Snap-in.
- Fare clic su Certificates e quindi fare clic su Add.
- Nella scheda Certificates snap-in, scegliere Computer account e quindi fare clic su Next.
- Dentro Select Computer, scegliere Local Computer, fare clic su OKe quindi fare clic su Finish. Dentro Add or Remove Snap-ins, fare clic su OK.
- Nella console dei certificati di un computer che contiene un certificato utilizzato per l'autenticazione del server, fare clic con il pulsante destro del mouse sulla scheda certificate, fare clic su All Taskse quindi fare clic su Export.

a (Console1 - [Console Root\Certifi	cates (Local Computer)\Pers	onal\Certificates]	_ D X
🚟 File Action View Favorites Window	w Help			_ 8 ×
🗢 🔿 🚈 🐻 🖌 🖬 🛤 🚺	? 💼			
Console Root	Issued To	Issued By	Expiration Date	Actions
⊿	azor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates
⊿ Personal	supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025	More Actions
Certificates	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD617 CA	A / 25 / 2022	More Actions
Irusted Koot Certification Autho Enterprise Trust		Open		WIN-E3SKEIOD617 razor local
Enterprise Trust Intermediate Certification Authority		All Ta	sks ▶ Op	pen 🕨
Trusted Publishers		Cut	Re	quest Certificate with New Key
Untrusted Certificates		Copy	Re	new Certificate with New Key
Third-Party Root Certification Au		Delete		
Trusted People	-		Ma	anage Private Keys
Client Authentication Issuers		Prope	rties Ad	Ivanced Operations
Other People		Help	Ex	port
Remote Desktop				
Certificate Enrollment Requests				
Smart Card Trusted Roots				
Irusted Devices	-			
< III >	<		>	
Export a certificate	16 -			,

• Esporta il certificato in pfx nelle sezioni successive. Fare riferimento a questo articolo per informazioni su come esportare un certificato in pfx formato da MMC:

https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technotewsa-00.html.

- Al termine dell'esportazione del certificato, passare a Add/Remove Snap-in ON MMC console. Fare clic su Certificates e quindi fare clic su Add.
- Scegli Service account e quindi fare clic su Next.

Certificates snap-in	x
This snap-in will always manage certificates for: O My user account Service account Computer account	

- Nella scheda Select Computer , scegliere Local Computer e fare clic su Next.
- Scegli Active Directory Domain Services e quindi fare clic su Finish.

Certificate	es snap-in 🛛 🗙
Select a service account to manage on the local of	omputer.
Active Directory Certificate Services Active Directory Domain Services Active Directory Web Services AD FS Windows Service Application Experience Application Host Helper Service Application Identity Application Information Application Layer Gateway Service Application Management ASP.NET State Service Background Intelligent Transfer Service Background Tasks Infrastructure Service Base Filtering Engine	
	< Back Finish Cancel

- Nella scheda Add/Remove Snap-ins fare clic su OK.
- Espansione Certificates Services (Active Directory Domain Services) e quindi fare clic su NTDS\Personal.
- Clic con il pulsante destro del mouse NTDS\Personal, fare clic su All Taskse quindi fare clic su Import.

Console1 - [Console	Root\Certificates - Service (Active Directory Domain Services) on Local	Computer\NTDS\Personal]	- 🗆 X
🚟 File Action View Favorites Window	v Help		_ 8 ×
🗢 🏟 🙇 📰 📋 🗟 📑			
Console Root	Object Type	Actions	
Certificates (Local Computer)	Certificates	NTDS\Personal	
Certificates - Service (Active Directory D NTOCOMMENT		More Actions	•
▶ MT Find Certificates			
▷ 🛄 NT All Tasks	Find Certificates		
▷ INI ▷ INI View	Import		
▷ 🖾 NT New Window from Here	Advanced Operations		
NT New Taskpad View			
▷ 🔤 NT Refresh			
Export List			
Help			
Add a certificate to a store	1		

- Nella scheda Certificate Import Wizard schermata iniziale, fare clic su Next.
- Nella schermata File da importare fare clic su Browsee individuare il file del certificato esportato in precedenza.
- Nella schermata Apri, verificare che Scambio di informazioni personali (*pfx,*.p12) è selezionato come tipo di file, quindi spostarsi nel file system per individuare il certificato esportato in precedenza. Fare quindi clic sul certificato.

-	Oper	n .			x
€ 🕘 ▼ ↑ 📑 ኑ Lib	raries > Documents		✓ C Search Do	ocuments	Q
Organize 👻 New folder					
🔆 Favorites	Name	Date modified	Туре	Size	
Desktop	🦻 Idapcert	4/25/2022 12:01	Personal Informati	5 KB	
i Downloads ا Recent places					
🕞 Libraries					
Documents					
Videos					
1 Computer					
🙀 Network					
File na	me: Idapcert		✓ Personal	Information Excl	hange ∨
			Оре	n Ca	ancel

- Fare clic su Open e quindi fare clic su Next.
- Nella schermata Password, immettere la password impostata per il file, quindi fare clic su Next.
- Nella pagina Archivio certificati verificare che l'opzione Inserisci tutti i certificati sia selezionata e leggere Archivio certificati: NTDS\Personal e quindi fare clic su Next.

€	🕖 Certificate Import Wizard
	Certificate Store
	Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for the certificate.
	\bigcirc Automatically select the certificate store based on the type of certificate
	Place all certificates in the following store
	Certificate store:
	NTDS\Personal Browse
	Learn more about <u>certificate stores</u>
	Next Cancel

х

• Nella scheda Certificate Import Wizard completamento, fare clic su Finish. Viene quindi visualizzato un messaggio che indica che l'importazione è stata completata. Fare clic su OK. Il certificato è stato importato nell'archivio certificati: NTDS\Personal.

Console1 - [Console Root\Certific	ates - Service (Active Directory	Domain Services) on Local C	Computer\NTDS\Pe	ersonal\Certificates]	_ 🗆 X
藩 File Action View Favorites Window	/ Help				_ & ×
🗢 🤿 🖄 📰 🔏 🐁 🔛 📓					
Console Root	Issued To 📩	Issued By	Expiration Date	Actions	
Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates	
Certificates - Service (Active Directory D Image: A Image: Active Directory D Image: A Image: Active Directory D Image: Active D Image: Actined D Image: Active D Image: Active D Image: Active D	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
Certificates				WIN-E3SKFJQD6J7.r	azor.local 🔺
NIDS\Irusted Koot Certification Au MTDS\Enterprise Trust MTDS\Intermediate Certification Au MTDS\Intermediate Certificates MTDS\Untrusted Publishers MTDS\Third-Party Root Certification MTDS\Trusted People MTDS\Client Authentication Issuers				More Actions	,
< <u> </u>	< III		>		
NTDS\Personal store contains 2 certificates.					

Configurazioni FMC

Verifica delle licenze

Per implementare la configurazione AnyConnect, l'FTD deve essere registrato con il server delle licenze Smart, e al dispositivo deve essere applicata una licenza Plus, Apex o VPN Only valida.

Imposta realm

1. Passa a System > Integration. Passa a Realms, quindi scegliere Add Realm, come mostrato nell'immagine:

Overview Analysi	is Policies Devices Objects	AMP Intelligence							-	Deploy Syste	em Help 🔻	admin 🔻
				Configuration Use	ers Domains	Integration	Updates	Licenses v	Logging •	Health • 1	Monitoring •	Tools •
	3					2						
Cloud Services	Realms Identity Sources	High Availability	eStreamer Host Input Client	Smart Software Manager	Dn-Prem							
Realms Re	ealm Sequences Sync Results											4
										Compare	Realms	id Realm
Name -	Description		Demain	AD Delevery Demain		Base DN				Charles		

 Compilare i campi visualizzati in base alle informazioni raccolte dal server Microsoft per LDAP. In precedenza, importare il certificato CA radice che ha firmato il certificato del servizio LDAP sul server Windows in Objects > PKI > Trusted CAs > Add Trusted CA, in quanto è indicato nell'Directory Server Configuration del Realm. Al termine, fare clic su ок.

Firepower Manag Objects / Object Manage	ement Center Overview Analy	sis Policies Devices Objects AMP Intelligence		Deploy Q 🚱 🔅 (admin 🔹
AAA Server Access List Address Pools Application Elitere	Trusted CAs Trusted certificate authority (CA) object	represents a CA public key certificate belonging to a trusted CA. You can use e	xternal CA objects in	Add Trusted CA Q. Filter SSL policy, realm configurations and ISE/ISE-PIC connection	on.
AS Path Cipher Suite List Community List	Name ISRG-Root-X1 Izence.com			Value CN=ISRG Root X1, ORG=Internet Security Research G CN=Izenoe.com, ORG=IZENPE S.A., C=ES	11
DNS Server Group External Attributes Eile List	LDAPS-ROOT-CERT Microsec-e-Szigno-Root-CA-2009	Edit Trusted Certificate Authority	0	CN=razor-WIN-E3SKFJQD6J7-CA CN=Microsec e-Szigno Root CA 2009, ORG=Microse	11
FlexConfig Geolocation Interface	NetLock-Arany-Class-Gold-FAtanAosAtv OISTE-WISeKey-Global-Root-GA-CA	Name: LDAPS-ROOT-CERT		CN=NetLock Arany (Class Gold) FA tanA2sÅtvÅjny, CN=OISTE WISeKey Global Root GA CA, ORG=WISeK	/1
Key Chain Network V PKI	OISTE-WISeKey-Global-Root-GB-CA OISTE-WISeKey-Global-Root-GC-CA	Subject: Common Name: razor-WIN-E3SKFJQD6J7-CA Organization:		CN=OISTE WISeKey Global Root GB CA, ORG=WISeK CN=OISTE WISeKey Global Root GC CA, ORG=WISeK	/1
Cert Enrollment External Cert Groups External Certs	QuoVadis-Root-CA-1-G3 QuoVadis-Root-CA-2	Organization Unit: Issuer: Common Name: razor-WIN-E3SKFJQD6J7-CA		CN=QuoVadis Root CA 1 G3, ORG=QuoVadis Limited, CN=QuoVadis Root CA 2, ORG=QuoVadis Limited, C=	/1
Internal CA Groups Internal CAs Internal Cert Groups	QuoVadis-Root-CA-3 QuoVadis-Root-CA-3-G3	Organization: Organization Unit: Not Valid Before:		CN=QuoVadis Root CA 3, ORG=QuoVadis Limited, C= CN=QuoVadis Root CA 3 G3, ORG=QuoVadis Limited,	11
Internal Certs Trusted CA Groups Trusted CAs	QuoVadis-Root-Certification-Authority Secure-Global-CA	Mar 22 14:33:15 2021 GMT Not Valid After: Mar 22 14:43:15 2026 GMT		CN=QueVadis Root Certification Authority, ORG=QueV CN=Secure Global CA, ORG=SecureTrust Corporation	11
Policy List Port	SecureTrust-CA	Install Certificate Cance	el Save	CN*SecureTrust CA, ORG*SecureTrust Corporation, Displaying 81 - 100 of 125 rows < < Page 5	/ ⊒ 017 > > C

Add New Realm

Name*	Description
LDAP-Server	
Туре	
LDAP	
Directory Username*	Directory Password*
Administrator@razor.local	
E.g. user@domain.com	
Base DN*	Group DN*
DC=razor,DC=local	DC=razor,DC=local
E.g. ou=group,dc=cisco,dc=com	E.g. ou=group,dc=cisco,dc=com
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.local	Port* 636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT +
Interface used to connect to Directory server 🚺	
Resolve via route lookup	
 Choose an interface 	
Default: Management/Diagnostic Interface	~
Test	
Add another directory	

0 ×

3. Fare clic su Test per garantire che FMC sia in grado di eseguire correttamente il binding con il nome utente e la password della directory forniti nel passaggio precedente. Poiché questi test vengono avviati dal FMC e non tramite una delle interfacce instradabili configurate sull'FTD (come interna, esterna, dmz), una connessione riuscita (o non riuscita) non garantisce lo stesso risultato per l'autenticazione AnyConnect poiché le richieste di autenticazione LDAP AnyConnect vengono avviate da una delle interfacce instradabili FTD.

Add Directory	0 ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc	Port* 636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
Interface used to connect to Dire	ectory server ()
Resolve via route lookup	
 Choose an interface 	
Default: Management/Dia	gnostic Interface 🗸 🗸
Test Test connection 	succeeded
	Cancel OK

4. Abilitare il nuovo realm.

Overview Anal	lysis Policies Devices Objects	AMP Intelligence				Poploy System Help	o ≠ admin +
				Configuration Users Domains	Integration Updates Licenses •	Logging Health Monitorin	ng 🔹 Tools 🔻
Cloud Service	Realms Identity Sources	High Availability eStreame	Host Input Client	Smart Software Manager On-Prem			
Realms	Realm Sequences Sync Results						
						(A second description of the second descrip	
						Compare Realms	Add Realm
Name +	Description	Туре	Domain	AD Primary Domain	Base DN	State	
AC-Local		LOCAL	Global			Enabled	i / 🖥 🗑
LDAP		AD	Global	cisco01.com	OU=Users,OU=CISCO,DC=cisco01,DC=c	com C Enabled	1 n v
LDAP-Server		AD	Global	razor.local	DC=razor,DC=local	C Enabled	±/昏窗

Configurazione di AnyConnect per la gestione delle password

1. Selezionare il profilo di connessione esistente o crearne uno nuovo, se si tratta dell'impostazione iniziale di AnyConnect. In questo caso, viene utilizzato un profilo di connessione esistente denominato 'AnyConnect-AD' mappato con l'autenticazione locale.

Overview Analysis Policies Devices Objects AMP Inte	elligence		🆺 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN > Remote Acc	cess QoS Platform Settings FlexConfig Certificates		
AnyConnect Enter Description			Save Save
			Policy Assignments (1)
		Local Realm: asa	Dynamic Access Policy: Hostscan
Connection Profile Access Interfaces Advanced			
			0
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authentization: None Accounting: None	DftGrpPolicy	/ 5
AnyConnect	Authentication: Radius (RADIUS) Authentization: Radius (RADIUS) Accounting: Informe	DftGrpPolicy	25
AnyConnect-AD	Authentication: LOCAL Authentization: None Accounting: None	AnyConnect-Group	/ 8

2. Modificare il profilo di connessione ed eseguire il mapping del nuovo server LDAP configurato nei passaggi precedenti, nelle impostazioni AAA del profilo di connessione. Al termine, fare clic su save nell'angolo superiore destro.

Firepower Management Center Overview Overview	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🔞 admin 🔻
AnyConnect Enter Description		Save Cancel
Connection Profile Access Interfaces Advanced	Edit Connection Profile	Policy Assignments.(1) Local Realm: None Dynamic Access Policy: Hostscan
	Connection Profile:* AnyConnect-AD	
Name	Group Policy: AnyConnect-Group + Edt Group Policy	+
Name	Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Authentication	/1
AnyConnect	Authentication Method: AAA Only	/1
AnyConnect-AD	Authentication Server: LDAP-Server (AD)	/i
	Use secondary autoentication	
	Authorization	
	Authorization Server: Use same authentication server 🔻	
	Allow connection only if user exists in authorization database Configure LDAP Attribute Map	
	Accounting	
	Accounting Server:	
	 Advanced Settings 	
	Strip Realm from username	
	Cancel Save	

3. Abilitare la gestione delle password in AAA > Advanced Settings e salvare la configurazione.

Overview Analysis Policies Devices Objects AMP Intellig	nce	🇛 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN + Remote Access AnyConnect Enter Description	QoS Platform Settings FlexConfig Certificates	Save Cancel
	Edit Connection Profile 2 X	Policy Assignments (1) Local Realm: asa Dynamic Access Policy: <u>Hostscan</u>
Connection Profile Access Interfaces Advanced	Connection Profile: * AnyConnect-AD Group Policy: * AnyConnect-Group Edit Group Policy: *	0
DefaultWEBVPNGroup	Client Address Assignment AAA Aliases	/8
AnyConnect	LDAP-Server (AD) v	/8
AnyConnect-AD	Use secondary authentication Authorization	2 5
sjobs	Authorization Server: Use same authentication server Authorization Server: Authorization database Configure LDAY: Altribute Map	/8
	Accounting Accounting Server: Advanced Settings Strip Realm from username Strip Realm from username Model user a days prior to password expiration Notify user on the day of password expiration Notify user on the day of password expiration Save Cancel	

Implementazione

1. Una volta completata la configurazione, fare clic sul pulsanteDeploy in alto a destra.

Overview Analysis Policies Devices Objects	AMP Intelligence
orerrier rindrysis remetes services objects	rom intelligence

2. Fare clic sulla casella di controllo accanto alla configurazione FTD applicata e quindi fare clic su _{Deploy}, come mostrato nell'immagine:

Overview /	Analysis Policies Devices Objects AMP	Intelligence						🎨 Deploy System Help 🕶 admin 🕶
								Deployment Deployment History
T Q	Search using device name, user name, type, group or st	atus						1 device selected Deploy time: Essmate
•	Device	Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status
> 🛛	10.197.224.190_FTD1	admin		FTD		May 30, 2022 7:34 AM	₿.	Pending

Configurazione finale

Questa è la configurazione rilevata nella CLI FTD dopo la corretta distribuzione.

Configurazione AAA

<#root>

> show running-config aaa-server

```
aaa-server LDAP-Server protocol ldap
```

n Deploy System Help v admin v

```
max-failed-attempts 4
```

```
realm-id 8
```

aaa-server LDAP-Server host WIN-E3SKFJQD6J7.razor.local

<----- LDAPs Server to which the queries are sent

```
server-port 636
```

ldap-base-dn DC=razor,DC=local

ldap-group-base-dn DC=razor,DC=local

ldap-scope subtree

ldap-naming-attribute sAMAccountName

ldap-login-password *****

ldap-login-dn *****@razor.local

ldap-over-ssl enable

server-type microsoft

Configurazione AnyConnect

<#root>

> show running-config webvpn

webvpn

```
enable Outside
```

anyconnect image disk0:/csm/anyconnect-win-4.10.01075-webdeploy-k9.pkg 1 regex "Windows"

anyconnect profiles FTD-Client-Prof disk0:/csm/ftd.xml

anyconnect enable

tunnel-group-list enable

cache

no disable

error-recovery disable

```
> show running-config tunnel-group
```

tunnel-group AnyConnect-AD type remote-access tunnel-group AnyConnect-AD general-attributes address-pool Pool-1

authentication-server-group LDAP-Server

default-group-policy AnyConnect-Group

password-management password-expire-in-days 1

tunnel-group AnyConnect-AD webvpn-attributes
group-alias Dev enable

> show running-config group-policy AnyConnect-Group

group-policy

AnyConnect-Group

internal

<----- Group-Policy configuration that is mapped once the user is authenticated</pre>

group-policy AnyConnect-Group attributes

vpn-simultaneous-logins 3

vpn-idle-timeout 35791394

vpn-idle-timeout alert-interval 1

vpn-session-timeout none

vpn-session-timeout alert-interval 1

vpn-filter none

vpn-tunnel-protocol ikev2 ssl-client

```
split-tunnel-policy tunnelspecified
```

split-tunnel-network-list value Remote-Access-Allow

<----- LDAPs Serve

<---- Password-management

<---- Protocol

default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect profiles value FTD-Client-Prof type user anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

> show running-config ssl

ssl trust-point ID-New-Cert Outside

<----- FTD ID-cert trustpoint name mapped to the outside interface on which AnyConnect Connections

Verifica

Connettersi con AnyConnect e verificare il processo di gestione delle password per la connessione utente

1. Avviare una connessione al profilo di connessione interessato. Una volta stabilito al primo accesso che la password deve essere cambiata poiché la password precedente è stata rifiutata da Microsoft Server poiché è scaduta, all'utente viene richiesto di cambiare la password.

Sicce AnyConnect FTD-Hostname Group: Dev ∨ Username: admin Password: [OK Carcel	Cisco AnyConnect Secure Mobility Client Ville Contacting PTD-Hostname. TD-Hostname Connect	
Sisco AnyConnect FTD-Hostname		
New Password:	enter a new la continue. Cisco AnyConnect Secure Mobility Client — X VPIE Contacting FTD-Hostname.	
Contrue		

2. Una volta che l'utente ha immesso la nuova password per l'accesso, la connessione viene stabilita correttamente.

Sisco AnyConnect Secure Mobility Client			-		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconne	ct
00:02:43					IPv4
۞ ()					dhaho cisco

3. Verificare la connessione utente nella CLI FTD:

<#root>

FTD_2# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

```
Username : admin

Index : 7

<----- Username, IP address assigned information of the client

Assigned IP : 10.1.x.x
```

Public IP : 10.106.xx.xx

Protocol

AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

:

License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

Bytes Tx	:	16316	Bytes Rx	:	2109
Group Policy	:	AnyConnect-Group	Tunnel Group	:	AnyConnect-AD
Login Time	:	13:22:24 UTC Mon Apr 25	5 2022		
Duration	:	Oh:00m:51s			
Inactivity	:	Oh:00m:00s			
VLAN Mapping	:	N/A	VLAN	:	none
Audt Sess ID	:	0ac5e0fa000070006266a09	90		
Security Grp	:	none	Tunnel Zone	:	0

Risoluzione dei problemi

Debug

Questo debug può essere eseguito nella CLI diagnostica per risolvere i problemi relativi alla gestione delle password: debug Idap 255.

Debug relativi alla gestione delle password durante il lavoro

<#root> [24] Session Start [24] New request Session, context 0x0000148f3c271830, reqType = Authentication [24] Fiber started [24] Creating LDAP context with uri=ldaps://10.106.71.234:636 [24] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful [24] supportedLDAPVersion: value = 3 [24] supportedLDAPVersion: value = 2 [24] Binding as *****@razor.local [24] Performing Simple authentication for *****@razor.local to 10.106.71.234 [24] LDAP Search:

Base DN = [DC=razor,DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

[24] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[24] Talking to Active Directory server 10.106.71.234

[24] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[24] Read bad password count 3

[24] Binding as admin

[24] Performing Simple authentication for admin to 10.106.71.234

[24] Simple authentication for admin returned code (49) Invalid credentials

[24] Message (admin): 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773,

[24] Checking password policy

[24] New password is required for admin

[24] Fiber exit Tx=622 bytes Rx=2771 bytes, status=-1

[24] Session End

[25] Session Start

[25] New request Session, context 0x0000148f3c271830, reqType = Modify Password

[25] Fiber started

[25] Creating LDAP context with uri=ldaps://10.106.71.234:636

[25] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

- [25] supportedLDAPVersion: value = 3
- [25] supportedLDAPVersion: value = 2
- [25] Binding as *****@razor.local
- [25] Performing Simple authentication for *****@razor.local to 10.106.71.234
- [25] LDAP Search:

Base DN = [DC=razor, DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

- [25] User DN = [CN=admin,CN=Users,DC=razor,DC=local]
- [25] Talking to Active Directory server 10.106.71.234
- [25] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[25] Read bad password count 3

[25] Change Password for admin successfully converted old password to unicode

[25] Change Password for admin successfully converted new password to unicode

[25] Password for admin successfully changed

[25] Retrieved User Attributes:

- [25] objectClass: value = top
- [25] objectClass: value = person
- [25] objectClass: value = organizationalPerson
- [25] objectClass: value = user
- [25] cn: value = admin
- [25] givenName: value = admin
- [25] distinguishedName: value = CN=admin,CN=Users,DC=razor,DC=local
- [25] instanceType: value = 4
- [25] whenCreated: value = 20201029053516.0Z

[25]	whenChanged: value = 20220426032127.0Z
[25]	displayName: value = admin
[25]	uSNCreated: value = 16710
[25]	uSNChanged: value = 98431
[25]	name: value = admin
[25]	objectGUID: value =0.].LH9.4
[25]	userAccountControl: value = 512
[25]	<pre>badPwdCount: value = 3</pre>
[25]	codePage: value = 0
[25]	countryCode: value = 0
[25]	badPasswordTime: value = 132610388348662803
[25]	lastLogoff: value = 0
[25]	lastLogon: value = 132484577284881837
[25]	<pre>pwdLastSet: value = 0</pre>
[25]	primaryGroupID: value = 513
[25]	objectSid: value =7Z RQ
[25]	accountExpires: value = 9223372036854775807
[25]	logonCount: value = 0
[25]	sAMAccountName: value = admin
[25]	sAMAccountType: value = 805306368
[25]	userPrincipalName: value = *****@razor.local
[25]	<pre>objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local</pre>
[25]	dSCorePropagationData: value = 20220425125800.0Z
[25]	dSCorePropagationData: value = 20201029053516.0Z
[25]	dSCorePropagationData: value = 16010101000000.0Z
[25]	lastLogonTimestamp: value = 132953506361126701
[25]	<pre>msDS-SupportedEncryptionTypes: value = 0</pre>
[25]	uid: value = *****@razor.local
[25] F	Fiber exit Tx=714 bytes Rx=2683 bytes, status=1

[25] Session End

Errori comuni rilevati durante la gestione delle password

In genere, se i criteri password impostati da Microsoft Server non vengono soddisfatti durante il periodo di tempo in cui l'utente immette la nuova password, la connessione viene terminata con l'errore "La password non soddisfa i requisiti dei criteri password". Verificare quindi che la nuova password soddisfi i criteri impostati da Microsoft Server per LDAP.

S Cisco AnyCon	nnect FTD-Hostname ×		
Cannot or password complexel	complete password change because the password does not meet the d policy requirements. Check the minimum password length, password ity, and password history requirements.		
Group:	Dev 🗸	🌖 Cisco AnyConnect Secure Mobility Client — 🛛 🔿	
Usernam	ne: admin		
Password	d:	Cannot complete password change because the password does not meet the password policy requirements. Check	
	OK Cancel	FTD-Hostname V Connect	
		Cisco AnyConnect	×
		Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.	
		ОК	

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).