# 在FMC管理的FTD上,使用RA VPN的LDAP配置 密碼管理

目錄 <u>簡介</u> 必要條件 <u>需求</u> <u>採用元件</u> 組態 網路圖表和案例 確定LDAP基本DN和組DN 複製LDAPS SSL證書根 <u>在LDAP伺服器上的本地電腦儲存中安裝多個證書的情況下(可選)</u> <u>FMC配置</u> 驗證許可 <u>設定領域</u> 配置AnyConnect進行密碼管理 部署 最終配置 AAA組態 <u>AnyConnect配置</u> 驗證 使用AnyConnect連線並驗證使用者連線的密碼管理過程 疑難排解 調試 <u>正在處理的密碼管理調試</u>

密碼管理過程中遇到的常見錯誤

## 簡介

本文檔介紹使用LDAP為連線到Cisco Firepower Threat Defense(FTD)的AnyConnect客戶端配置密碼管理。

必要條件

需求

思科建議您瞭解以下主題的基本知識:

- 基本瞭解FMC上的RA VPN(遠端訪問虛擬專用網路)配置
- FMC上的LDAP伺服器配置基礎知識

• Active Directory基礎知識

## 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Microsoft 2012 R2伺服器
- 運行7.3.0的FMCv
- 執行7.3.0的FTDv

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

## 組態

## 網路圖表和案例



Windows伺服器預配置了ADDS和ADCS以測試使用者密碼管理過程。在此配置指南中,將建立這 些使用者帳戶。

使用者帳戶:

- 管理員:此帳戶用作目錄帳戶,以允許FTD繫結到Active Directory伺服器。
- admin:用於演示使用者身份的測試管理員帳戶。

## 確定LDAP基本DN和組DN

1. 通過Active Directory Users and Computers「Server Manager Dashboard」(伺服器管理器控制面板)開啟。



開啟View Option「頂部」面板上的,然後啟用Advanced Features,如下圖所示:



這允許檢視AD對象下的其他屬性。

例如,若要尋找根的DNrazor.local,請按一下右鍵razor.local,然後選擇Properties,如下圖所示:



在Properties下,選擇Attribute Editor頁籤。在「distinguishedNameAttributes」下查詢,然後按一下View,如下圖所示。

這將開啟一個新視窗,可以在其中複製並稍後將DN貼上到FMC中。

在本例中,根DN是DC=razor, DC=local。複製該值並儲存以備以後使用。按一下OK「字串屬性編輯器」視窗退出,然後按一下OK「 再次按一下」以退出「屬性」。

raz	zor.local Properties ?	x
General Managed By Ob	oject Security Attribute Editor	
Attributes:		
Attribute	Value	~
defaultLocalPolicyObj	<not set=""></not>	
description	<not set=""></not>	
desktop Profile	<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	ng Attribute Editor	x
Attribute: distinguish	edName	
Value:		
DC=razor,DC=local		
Clear	OK Cano	el

•

•

按Win+RE	nter鍵mmc.exe,然後按一下OK,如下圖所示。
🖅 Run	×
<u>O</u> pen:	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
-	OK Cancel <u>B</u> rowse

導覽至File > Add/Remove Snap-in..., ss,如下圖所示:



在「可用管理單元」下,選擇Certificates 然後按一下Add,如下圖所示:

extensible snap-ins, you can Available <u>s</u> nap-ins:	his console from th configure which e	xter	le on your computer and configure the selected set re enabled. Selected snap-ins:	of snap-Ins. For
Snap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor Microsoft Cor		i	Remove
Active Directory Use	Microsoft Cor Microsoft Cor		1	Move <u>U</u> p
AUSI East Authorization Manager	Microsoft Cor Microsoft Cor		d >	Move <u>D</u> own
Certificates	Microsoft Cor			
Component Services	Microsoft Cor Microsoft Cor			
B Device Manager	Microsoft Cor			
T Disk Management	Microsoft and	v		Advanced
Description:				
The Certificates snap-in allo	ws you to browse	the	ts of the certificate stores for yourself, a service, o	r a computer.

選擇「Computer account 」,然後按一下Next「」,如下圖所示:

Certificates snap-in			×
This snap-in will always manage certificates for: <u>Service account</u> <u>Service account</u>			
<	: <u>B</u> ack	<u>N</u> ext >	Cancel

如圖所示,按一下Finish。

Select Computer	$\times$
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>Browse</li> </ul> Another computer:       Browse         Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cance	1

現在,按一下OK,如下圖所示。

Snap-in	Vendor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			up Certificates (Local Computer)	<u>R</u> emove
Active Directory Site	Microsoft Cor				
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor				Maria David
Authorization Manager	Microsoft Cor		Add		Move Down
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
E Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
T Disk Management	Microsoft and	v			Advanced
			1		
escription:					

展開檔案夾Personal,然後按一下Certificates。LDAP使用的證書必須頒發給Windows伺服器的完全限定域名(FQDN)。在此伺服器上列出三個憑證:

CA證書頒發給和頒發者razor-WIN-E3SKFJQD6J7-CA。

٠

•

•

•

頒發給和頒發者的CA證書supinfo-WIN-FNJVP9QUEH9-CA。

已將身份證書頒發給WIN-E3SKFJQD6J7.razor.local。razor-WIN-E3SKFJQD6J7-CA。

在此配置指南中,FQDN為WIN-E3SKFJQD6J7.razor.local,因此前兩個證書不能用作LDAP的SSL證書。頒發給的身份證書WIN-E3SKFJQD6J7.razor.local,是由Windows Server CA服務自動頒發的證書。按兩下憑證以檢查詳細資訊。

<b>a</b> (	Console1 - [Console Root\Certif	icates (Local Computer)\Persor	nal\Certificates]		_ 🗆 X
🚟 File Action View Favorites Window	w Help				_ & ×
🗢 🏟 🖄 📰 📋 🙆 📦 🖉 📷					
Console Root	Issued To 📩	Issued By	Expiration Date	Actions	
∠ G Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates	<b>_</b>
⊿ Personal	Supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025	More Actions	•
Trusted Root Certification Autho	En WIN-ESSKPJQD07.razor.local	razor-wilk-ESSKFJQD6J7-CA	4/23/2023		
▷ Contemprise Trust =					
Intermediate Certification Autho					
Trusted Publishers					
Untrusted Certificates					
Third-Party Root Certification Au					
Trusted People					
Client Authentication Issuers					
Other People					
Remote Desktop					
Certificate Enrollment Requests					
Smart Card Trusted Roots					
Trusted Devices					
Web Hosting					
<	<		>		
Personal store contains 3 certificates.					

要用作LDAP的SSL證書,證書必須滿足以下要求:

٠

•

公用名稱或DNS使用者替代名稱與Windows Server的FQDN匹配。

證書在Enhanced Key Usage欄位下有Server Authentication。

在證書的頁籤下Details,選擇Subject Alternative NameFQDN所在的WIN-E3SKFJQD6J7.razor.local位置。

Cer	tificate	x
General Details Certification Path		
Show: <all></all>	~	
Field	Value	ו ר
Enhanced Key Lisage	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	KevID=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	1 1
Subject Alternative Name	DNS Name=WIN-E3SKFJQD6J 🗸	
DNS Name=WIN-E3SKFJQD6J7.raz	or.local	
DNS Name=razor.local DNS Name=PAZOP		
DINS Mallie - RAZOR		
	the Descent for the State	n
Ed	Copy to File	
Learn more about <u>certificate details</u>		
	OK	

在Enhanced Key Usage下Server Authentication,存在。

Cer	tificate	x				
General Details Certification Path						
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	KevID=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	~				
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>						
	OK					

確認後,在Certification Path頁籤下,選擇作為根CA證書的頂級證書,然後按一下View Certificate。這將開啟根CA證書的證書 詳細資訊,如下圖所示:

Certificate	x	Certificate X
General Details Certification Path Certification path a razor-WIN-E3SKFJQD6J7-CA WIN-E3SKFJQD6J7.razor.local		General       Details       Certification Path         Image: Certificate Information       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
C	К	OK

在根CADetails證書的頁籤下,按一下Copy to File 並導航到以PEM格式匯出根CA的Certificate Export Wizard。

選擇Base-64 encoded X.509 作為檔案格式。

e 🦻	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\Administrator\Downloads\roo	
	Export Keys	No	
	File Format	NO Base64 Encoded X, 509 (*.cer)	
	<		
		Finish	ancel

Y

使用記事本或其他文本編輯器開啟儲存在電腦上選定位置的根CA證書。

這顯示PEM格式證書。儲存以備以後使用。

#### -----BEGIN CERTIFICATE-----

 CSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhujlx4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEAAaNRME8w DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUAOdY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0C AA4IBAQCiSm5U7U6Y7zXdx+dleJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6qZu 4sMZffbVrGlRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8XlvpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylbBfn0NEX7l GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+of0kWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X

在LDAP伺服器上的本地電腦儲存中安裝多個證書的情況下(可選)

1.在LDAPS可以使用多個身份證書的情況下,當使用哪個身份證書存在不確定性,或者無法訪問LDAPS伺服器時,仍然可以從在 FTD上完成的資料包捕獲中提取根CA。

2.如果在LDAP伺服器(如AD DS域控制器)本地電腦證書儲存中有多個對伺服器身份驗證有效的證書,則可以注意到,不同的證書 用於LDAPS通訊。解決此類問題的最佳方法是從本地電腦證書儲存中刪除所有不必要的證書,並且僅具有一個對伺服器身份驗證有 效的證書。

但是,如果有正當理由需要兩個或更多證書並且至少具有一個Windows Server 2008 LDAP伺服器,則Active Directory域服務 (NTDS\Personal)證書儲存區可用於LDAP通訊。

以下步驟演示如何從域控制器本地電腦證書儲存匯出啟用LDAPS的證書到Active Directory域服務證書儲存(NTDS\Personal)。

導航到Active Directory伺服器上的MMC控制檯,選擇檔案,然後按一下Add/Remove Snap-in。

按一下Certificates,然後按一下Add。

在中Certificates snap-in, 選擇Computer account, 然後按一下Next。

在Select Computer,選擇Local Computer,按一下OK,然後按一下Finish。在Add or Remove Snap-ins中,按一下OK。

在包含用於伺服器身份驗證的證書的電腦證書控制檯中,按一下右鍵certificate,按一下All Tasks,然後按一下Export。

<b>a</b>	Co	onsole1 - [Console Root\Certifi	cates (Le	ocal Comp	uter	)\Person	al\Certifi	cates]		x
藩 File Action View Favorites Windo	ow	Help							_ 8	×
🗢 🄿 🖄 📰 🐇 🔝 🔂	?									
📔 Console Root 🛛	-	Issued To	Issued By	/			Expiration	Date	Actions	
∠ Gertificates (Local Computer)		azor-WIN-E3SKFJQD6J7-CA	razor-WI	N-E3SKFJQD	6J7-C	A	3/22/2026	j	Certificates	
⊿ Personal		supinfo-WIN-FNJVP9QUEH9-CA	supinfo-	WIN-FNJVP9	QUE	H9-CA	2/23/2025		More Actions	•
Certificates		WIN-E3SKFJQD6J7.razor.local	razor-WI	N-E3SKFJQD	6177	Open	A71573672			_
Enterprise Trust	=					All Tasks	•	0	WIN-E3SKEIOD617 razor local	ŕ.
Intermediate Certification Autho						All Tasks	,	0	pen	
Trusted Publishers						Cut		Re	equest Certificate with New Key	
Untrusted Certificates						Сору		Re	new Certificate with New Key	
I I hird-Party Root Certification Au Trusted People						Delete		M	anage Private Keys	
Client Authentication Issuers						Properties		A	dvanced Operations	
Other People						Help		Fy	port	1
Remote Desktop						Theip				
Certificate Enrollment Requests										
Smart Card Trusted Roots										
Trusted Devices										
< III >		<						>		
Export a certificate										

• 在後續部分中pfx,以格式匯出證書。有關如何從MMC匯出格式證書的文章pfx,請參閱以下文章:

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

匯出憑證後,導覽至Add/Remove Snap-in onMMC console。按一下Certificates,然後按一下Add。

選擇Service account,然後按一下Next。

## Certificates snap-in

х

This snap-in will always manage certificates for:

My user account

Service account

Computer account

在對話Select Computer框中,選擇Local Computer,然後按一下Next。

選擇Active Directory Domain Services,然後按一下Finish。

•

٠

Certifica	ates snap-in
Select a service account to manage on the loca	al computer.
Service account:	
Active Directory Certificate Services	<u>^</u>
Active Directory Domain Services	
AD FS Windows Service	
Application Experience	
Application Host Helper Service	
Application Information	
Application Layer Gateway Service	
ASP.NET State Service	
Background Intelligent Transfer Service	
Background Tasks Infrastructure Service Base Filtering Engine	~
	< Back Finish Cancel

在對話Add/Remove Snap-ins框中,按一下OK。

•

•

٠

展開Certificates - Services (Active Directory Domain Services),然後按一下NTDS\Personal。

Console1 - [Console Root\C	Certificates - Service (Active Directory Domain Services) on Local Comput	ter\NTDS\Personal] 🗕 🗖 🗙
🗃 File Action View Favorites Window Help	p	_ 8 ×
🗢 🔿 🙍 🗊 📋 🧟 🔂 🗊		
Console Root Object	t Type	Actions
Certificates (Local Computer)	rtificates	NTDS\Personal
	1	More Actions
Find Certificates		
▷ NT All Tasks ►	Find Certificates	
▶ S NT View ▶	Import	
▷ INT New Window from Here	Advanced Operations	
New Taskpad View		
⊳ 🖺 NT Refresh		
Export List		
Help		
	~ 	
Add a certificate to a store		

在歡迎螢幕Certificate Import Wizard,按一下Next。

•

•

٠

在「File to Import(要匯入的檔案)」螢幕上,按一下Browse,然後找到您之前匯出的證書檔案。

在「開啟」螢幕上,確保選擇「個人資訊交換」(\*pfx,\*.p12)作為檔案型別,然後導航到檔案系統以找到先前匯出的證書。然後,按一下該證書。

<b>.</b>	Oper	י <u></u>	I.		x
🕞 💿 🔻 🕇 📑 🕨 Libr	raries + Documents		♥ 🖒 Search Do	cuments	ρ
Organize 🔻 New folder				· · ·	?
🔆 Favorites	Name	Date modified	Туре	Size	
Desktop	😼 Idapcert	4/25/2022 12:01	Personal Informati	5 KB	
i Downloads					
🥽 Libraries					
Documents					
J Music					
Pictures					
📑 Videos					
👰 Computer					
👽 Network					
File nar	me: Idapcert		✓ Personal	Information Exchange	~
			Оре	n Cancel	

按一下Open,然後按一下Next。

•

•

•

在「密碼」螢幕上,輸入為檔案設定的密碼,然後按一下Next。

在「證書儲存」頁面上,確保選中「放置所有證書」,然後閱讀「證書儲存:NTDS\Personal」,然後按一下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.
	O 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

在完成螢幕上Certificate Import Wizard,按一下Finish。然後您會看到一條消息,說明匯入成功。按一下OK。您會看到證書已 匯入到證書儲存區:NTDS\Personal。

Console1 - [Console Root\Certific	ates - Service (Active Directory	/ Domain Services) on Local (	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	
∠	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
Certificates				WIN-E3SKFJQD6J7.ra	azor.local 🔺
ATDS\Enterprise Trust     TDS\Intermediate Certification Au     ATDS\Intermediate Certification Au     ATDS\Trusted Publishers     TDS\Untrusted Certificates     ATDS\Third-Party Root Certificatior     ATDS\Trusted People     ATDS\Client Authentication Issuers				More Actions	· ·
< III >	< III		>		
NTDS\Personal store contains 2 certificates.					

#### FMC配置

#### 驗證許可

為了部署AnyConnect配置,必須在智慧許可伺服器上註冊FTD,並且必須向裝置應用有效的Plus、Apex或VPN許可證。

#### 設定領域

•

導航至System > Integration。導覽至Realms,然後按一下Add Realm,如下圖所示:

Overview Analy	sis Policies	Devices Objects	AMP Intelligence										•	Deploy Sys	item Help v	admin 🔻
							Configuration	Users	Domains	Integration	Updates	Licenses <b>v</b>	Logging •	Health •	<sup>1</sup> Monitoring •	Tools •
	3									2						
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smar	rt Software Man	ager On-P	rem							
Realms	Realm Sequenc	es Sync Results														4
														Compa	re Realms Ad	d Realm
Name +	Descript	ion	Туре		Domain		D Primary Domain	•		Base DN				State		

根據從Microsoft Server for LDAP收集的資訊填寫顯示的欄位。在此之前,請匯入根CA證書,該證書已在下面的Windows伺服 器上的LDAP服務證書上簽名Objects > PKI > Trusted CAs > Add Trusted CA,因為在「領域」下Directory Server Configuration 會引用該證書。完成後,按一下OK。

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
Directory Server Configuration	
<ul> <li>WIN-E3SKFJQD6J7.razor.local:636</li> </ul>	
Hostname/IP Address*	Port*
WIN-E3SKFJQD6J7.razor.local	636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
Interface used to connect to Directory server ()	
Resolve via route lookup	
<ul> <li>Choose an interface</li> </ul>	
Default: Management/Diagnostic Interface	$\sim$
Test	
Add another directory	

0 ×

按一下Test,確保FMC能夠使用先前步驟中提供的目錄使用者名稱和密碼成功繫結。由於這些測試是從FMC啟動的,而不是 通過FTD上配置的某個可路由介面(如內部、外部、dmz),因此成功(或失敗)的連線不能保證AnyConnect身份驗證的相同

Add Directory			0 ×
Hostname/IP Address* WIN-E3SKFJQD6J7.ra	azor.loc	Port* 636	
Encryption		CA Certificate*	
LDAPS	$\sim$	LDAPS-ROOT-CERT	<ul><li>✓ +</li></ul>
Interface used to connect Resolve via route loc Choose an interface Default: Managem Test • Test cont	t to Direction s	nostic Interface	
		Cancel	ОК

啟用新領域。

Overview Analysi	is Policies Devices Objects	AMP Intelligence								<b>%</b>	Deploy S	stem Help	▼ admin ▼
				Configuration	Users	Domains	Integration	Updates	Licenses •	Logging *	Health •	Monitorin	g 🔹 Tools 🔹
Cloud Services	Realms Identity Sources	High Availability eStreams	r Host Input Client	Smart Software Man	ager On-P	rem							
Realms Re	ealm Sequences Sync Results												
											Comp	are Realms	Add Realm
Name +	Description	Туре	Domain	AD Primary Domai	n		Base DN				State		
AC-Local		LOCAL	Global								🍩 Enat	iled _	/ 🖥 🗑
LDAP		AD	Global	cisco01.com			OU=Users,0	DU=CISCO,D	C=cisco01,DC=	oom	C Enat	led _	/ 5 🗑
LDAP-Server		AD	Global	razor.local			DC=razor,D	C=local			🔹 Enat	led _	/ 🖥 🗑

•

•

選擇現有的連線配置檔案,或建立一個新的連線配置檔案(如果是AnyConnect的初始設定)。此處使用與本地身份驗證對映 的名為「AnyConnect-AD」的現有連線配置檔案。

Overview Analysis	Policies Devi	ces Ot	ojects AMP Int	elligence							🔒 Deploy System Help 🕶	admin 🔻
Device Management	Device Upgrade	NAT	VPN + Remote Ac	cess QoS	Platform Settings	FlexConfig	Certificates					
AnyConnect											Save	8 Cancel
											Policy Assig	nments (1)
										Local Realm: asa	Dynamic Access Policy	y: <u>Hostscan</u>
Connection Profile	Access Interfac	es Ad	fvanced									
												0
Name				AAA				G	roup Policy			
DefaultWEBVPNGroup				Authentication Authorization Accounting:	n: None None None			8	DfltGrpPolicy			/ 5
AnyConnect				Authentication Authorization Accounting:	n: Radius (RADIUS) : Radius (RADIUS) None			8	DfltGrpPolicy			/ 6
AnyConnect-AD				Authentication Authorization Accounting:	n: LOCAL s None None				AnyConnect-Group			/ 6

在連線配置檔案的AAA設定下,編輯連線配置檔案並對映在前面步驟中配置的新LDAP伺服器。完成後Save,按一下右上角。

Firepower Management Center Devices / VPN / Edit Connection Profile	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🙆 admin 🔻
AnyConnect		Save
Enter Description		Policy Accimments (1)
Connection Profile Access Interfaces Advanced	Edit Connection Profile	Local Realm: None Dynamic Access Policy: Hostscan
	Connection Profile:* AnyConnect-AD	
	Group Policy:* AnyConnect-Group + +	+
Name	Edit Group Policy	
DefaultWEBVPNGroup	Cilent Address Assignment AAA Aliases	11
	Authentication	
AnyConnect	Authentication Method: AAA Only	/1
AnyConnect-AD	Authentication Server: LDAP-Server (AD)	13
	Fallback to LOCAL Authentication	· · · · · · · · · · · · · · · · · · ·
	Use secondary authentication	
	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	
AnyConnect-AD	Authentication Server: LDAP-Server (AD) •	/1

#### 在下啟用密碼管理AAA > Advanced Settings, 並儲存配置。

Overview Analysis Policies Devices Objects AMP Intellige Device Management Device Upgrade NAT VPN + Remote Access	nce QoS Platform Settings FlexConfig Certificates	🁥 Deploy System Help 🕶 admin 🕶
AnyConnect		Save Cancel
Enter Veschpton		Policy Assignments (1) Local Realm: asa Dynamic Access Policy: <u>Hostacan</u>
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? ×	
Name	Connection Profile:* AnyConnect-AD Group Policy:* AnyConnect-Group Edit Group Policy:	•
DefaultWEBVPNGroup	Client Address Assignment AAA Aliases	/ 8
AnyConnect	LDAP-Server (AD)	/8
AnyConnect-AD	Use secondary authentication Authorization	28
sjobs A	Authorization Server: Use same authentication server  Calculation server Configure LDAP Attribute Map	/8
	Accounting Accounting Server:	
	Advanced Settings	
	Strip Realm from username	
	Enable Password Management     Notify User     I days prior to password expiration     Notify user on the day of password expiration	
	Save Cancel	

部署

•

•

•

完成所有配置後Deploy,按一下右上角的按鈕。

Overview Analysis Policies Devices Objects AMP Intelligence System Help + admin +

按一下應用於它的FTD設定旁邊的覈取方塊,然後按一下Deploy,如下圖所示:

Overview Analysis Policies Devices Obj	ects AMP Intelligence					Poploy System	Help <b>+ admin +</b>
						Deployment	Deployment History
Y Q. Search using device name, user name,	type, group or status					1 device Deploy time:	Estimate Deploy
Device	Modified by	Inspect Interruption	Type Group	Last Deploy Time	Preview	Status	
> Ø 10.197.224.190_FTD1	admin		FTD	May 30, 2022 7:34 AM	₿.	Pending	

#### 最終配置

這是成功部署後FTD CLI中看到的組態。

AAA組態

<#root>

> show running-config aaa-server

aaa-server LDAP-Server protocol ldap

<----- aaa-server group configured for LDAPs

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

AnyConnect配置

<#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 <---- LDAPs Serve default-group-policy AnyConnect-Group password-management password-expire-in-days 1 <---- Password-management 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
 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
```

<---- Protocol

```
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

#### 驗證

使用AnyConnect連線並驗證使用者連線的密碼管理過程

1.啟動到相關連線配置檔案的連線。初次登入時確定必須更改密碼後,Microsoft Server在密碼到期時拒絕了該較早的密碼,系統將提示使用者更改密碼。

Cisco AnyConnect   FTD-Hostname X	👁 Cisca AnyConnect Secure Mability Client - 🗆 X
Group: Dev v Username: admin Password: [	VPH: Contacting FID-Hosthame.
OK Cancel	

Cisco AnyConnect   FTD-Hostname	Cisco AnyConnect Secure Mobility Client – ×      VPIE Contacting FTD-Hostname.      FTD-Hostname Continue Continue	
	C O abada esto	

🚳 Cisco AnyC	onnect Secure Mobility Client		_		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnect	t
00:02:43				i	IPv4
<b>۞</b> (i)					dialia cisco

在FTD CLI上驗證使用者連線:

<#root>

•

FTD\_2# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : admin

Index : 7

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

	Public IP : 10.106.xx.xx
Protocol	:
AnyConnect-Pa	arent 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 2022
Duration	: Oh:00m:51s
Inactivity	: 0h:00m:00s
VLAN Mapping	: N/A VLAN : none
Audt Sess ID	: 0ac5e0fa000070006266a090
Security Grp	: none Tunnel Zone : 0

#### 疑難排解

#### 調試

此調試可以在診斷CLI中運行,以便解決與密碼管理相關的問題:debug ldap 255。

#### 正在處理的密碼管理調試

#### <#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.].LH.....9.4
- [25] userAccountControl: value = 512
- [25] badPwdCount: value = 3
- [25] codePage: value = 0
- [25] countryCode: value = 0
- [25] badPasswordTime: value = 132610388348662803
- [25] lastLogoff: value = 0
- [25] lastLogon: value = 132484577284881837
- [25] pwdLastSet: value = 0
- [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] objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=razor, DC=local
- [25] dSCorePropagationData: value = 20220425125800.0Z
- [25] dSCorePropagationData: value = 20201029053516.0Z
- [25] dSCorePropagationData: value = 16010101000000.0Z

- [25] lastLogonTimestamp: value = 132953506361126701
- [25] msDS-SupportedEncryptionTypes: value = 0
- [25] uid: value = \*\*\*\*\*@razor.local
- [25] Fiber exit Tx=714 bytes Rx=2683 bytes, status=1
- [25] Session End

#### 密碼管理過程中遇到的常見錯誤

通常,如果在使用者提供新密碼期間未滿足Microsoft Server設定的密碼策略,連線將終止,並出現錯誤「Password does the Password Policy Requirements」。因此,請確保新密碼符合Microsoft Server為LDAP設定的策略。

Cannot com password p complexity	ect   FTD-Hostname mplete password change because the password does not meet the policy requirements. Check the minimum password length, password , and password listory requirements.	×			
Group: Username: Password:	Dev v v v v v v v v v v v v v v v v v v	Cisco An	VConnect Secure Mobility Client – O X VPIE Cannot complete password change because the password does not meet the password polcy requirements. Check FTD Hostname V Connect		
	A Stalley	Cisco Any	dividu esso	×	
		8	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.		

### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。