# **Configure Password Management Using LDAPs for RA VPN on FTD Managed by FMC**

# Contents

Introduction Prerequisites **Requirements** Components Used Configuration Network Diagram and Scenario Determine LDAP Base DN and Group DN Copy the LDAPS SSL Certificate Root In Case of Multiple Certificates Installed in the Local Machine Store on the LDAPs Server (Optional) **FMC** Configurations Verify Licensing Setup Realm Configure AnyConnect for Password-Management **Deploy Final Configuration AAA** Configuration AnyConnect Configuration Verification Connect with AnyConnect and Verify the Password-Management Process for the User Connection **Troubleshoot** Debugs Working Password-Management Debugs Common Errors Encountered During the Password-Management

# Introduction

This document describes configuring Password Management using LDAPs for AnyConnect Clients connecting to Cisco Firepower Threat Défense (FTD).

# Prerequisites

### Requirements

Cisco recommends that you have basic knowledge of these topics:

- Basic knowledge of RA VPN (Remote Access Virtual Private Network) configuration on FMC
- Basic knowledge of LDAP server configuration on FMC
- Basic knowledge of Active Directory

### **Components Used**

The information in this document is based on these software and hardware versions:

- Microsoft 2012 R2 Server
- FMCv running 7.3.0
- FTDv running 7.3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configuration

### **Network Diagram and Scenario**



Windows server is pre-configured with ADDS and ADCS in order to test the user password-management process. In this configuration guide, these user accounts are created.

User Accounts:

- Administrator: This is used as the directory account in order to allow the FTD to bind to the Active Directory server.
- admin: A test administrator account used to demonstrate user identity.

### **Determine LDAP Base DN and Group DN**

1. Open Active Directory Users and Computers through the Server Manager Dashboard.

Server Manager • Dashboard • 🗇   🚩 Manage Tools View Help						
Image: Construction of the second	WELCOME TO SERVER MANAGER		Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Module for Windows PowerShell Active Directory Users and Computers Active Directory Users and Computers ADS faid Certification Authonity Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management Health Registration Authonity Intervet Information Services (IIS) Manager ISCSI Initiator			
	Roles 7   Server GROUPS Roles 7   Server groups: 1   Servers total AD CS 1 Manageability Events Services Performance BPA results	Image AD DS     1       Image AD If X     Image AD If X       Image AD If X     Image AD If X </th <th>1 DNS 1 Manageability Events Services Performance BPA results</th> <th>File a Serv Mana Even Servi Perfo BPA a</th> <th>Network Policy Server ODBC Data Sources (2-bit) ODBC Data Sources (64-bit) Performance Monitor Resource Monitor Security Configuration Wizard Services System Information Task Scheduler Task Scheduler Windows Firemall with Advanced Security Windows Memory Diagnostic Windows Memory Diagnostic</th>	1 DNS 1 Manageability Events Services Performance BPA results	File a Serv Mana Even Servi Perfo BPA a	Network Policy Server ODBC Data Sources (2-bit) ODBC Data Sources (64-bit) Performance Monitor Resource Monitor Security Configuration Wizard Services System Information Task Scheduler Task Scheduler Windows Firemall with Advanced Security Windows Memory Diagnostic Windows Memory Diagnostic	
	IIS     1       ① Manageability       Events       Services       Performance       BPA results	Manageability     I       Image ability     Image ability       Events     Events       Services     Performance       BPA results     BPA results	1 Manageability Events Services Performance BPA results	Ac Go	Windows PowerShell (x88) Windows PowerShell (\$2 Windows PowerShell (\$2 Windows Server Backup Crivate Windows to Action Center to activate Windows.	

2. Open the View Option on the top panel, and enable the Advanced Features, as shown in the image:

	Active Directory U	sers and Computers	L	- 0	x
File Action View	v Help				
🗢 🔿 🙍	Add/Remove Columns				
📄 Active Direc	Large Icons	n			
▷ Saved Q	Small Icons				
≥ inazor.iot	List	ntainer for up ntainer for do			
⊳ 📫 Com 🎴	Detail	ntainer for sec			
▷ Dom	Dor Users, Contacts, Groups, and Computers as containers	ntainer for or			
▷ 📫 Lost	Advanced Features	ntainer for ma			
⊳ 🧰 Man	Customics	tem settings			
▷ Prog ▷ System	Customize	ntainer for up			
i Users ▷ i NTDS Qua ▷ i TPM Devi	otas ces				
Displays items in a list					
Displays items in a list	•				

3. This allows the view of additional properties under the AD objects.

For example, in order to find the DN for the root razor.local, right-click razor.local, and then choose Properties, as shown in this image:

<b>a</b>	Acti	ive Directory Users an	d Computers	Ŀ	- 🗆 X
File Action View Help					
🗢 🄿 🖄 📰 🗋 🔝 🐼 🗟	🛛 🖬 🗏 📚 🛅 🍸	2 🕺			
<ul> <li>Active Directory Users and Com</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Sourcloc</li> <li>Built</li> <li>Com</li> <li>Change Domain</li> <li>Change Domain</li> <li>Change Domain</li> <li>Change Domain</li> <li>Change Domain</li> <li>Change Domain</li> <li>Prog</li> <li>Syste</li> <li>NTD</li> <li>Syste</li> <li>NTD</li> <li>TPM</li> <li>View</li> <li>Refresh</li> <li>Export List</li> <li>Properties</li> <li>Help</li> </ul>	Name Type Builtin builtinDor Builtin builtinDor DI ner Name Type Selection of the selection of the s	Description main r Default container r Default container r Default container r Default container r Default container r Default location f r Builtin system set r Default container yotaC Quota specification infor tureU	for up for do for sec for or ma or stor tings for up ons co		
< III >					
Opens the properties dialog box for the	e current selection.				

4. Under Properties, choose the Attribute Editor tab. Find distinguishedName under the Attributes, then click View, as shown in the image.

This opens a new window where the DN can be copied and pasted into FMC later.

In this example, the root DN is DC=razor, DC=local. Copy the value and save it for later. Click OK in order to exit the String Attribute Editor window and click OK again in order to exit the Properties.

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	ng Attribute Editor	x		
Attribute: distinguishedName				
Value:				
DC=razor,DC=local				
Clear	OK Cano	el		

### **Copy the LDAPS SSL Certificate Root**

1. Press Win+R and enter mmc.exe, then click OK, as shown in this image.



2. Navigate to File > Add/Remove Snap-in..., ss shown in this image:

<b>a</b>	Console1 - [Console Root]	_ <b>D</b> 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 Actions
Add/Remove Snap-in Ctrl+M		
Options		
1 C:\Windows\system32\dsa		
2 C:\Windows\system32\eventvwr		
4 C:\Windows\system32\certrn/		
F.A		
Exit		
Enables you to add snap-ins to or remove them from the snap	o-in console.	

3. Under available snap-ins, choose Certificates and then click Add, as shown in this image:

Remove
Remove
Move Up
_
Move Down
Advanced

4. Choose Computer account and then click Next, as shown in this image:

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

As shown here, click 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>Another computer:</li> <li>Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.</li> </ul>	
< Back Finish Cancel	

5. Now, click OK, as shown in this image.

nap-in	Vendor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			uge Certificates (Local Computer)	Remove
Active Directory Site	Microsoft Cor				-
Active Directory Use	Microsoft Cor				Mauralle
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor		<u>A</u> dd >		Move Down
Contification Manager	Microsoft Cor				_
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
	Marrie and				

- 6. Expand the Personal folder, then click Certificates. The certificate used by LDAPs must be issued to the Fully Qualified Domain Name (FQDN) of the Windows server. On this server, there are three certificates listed:
- A CA Certificate was issued to and by razor-WIN-E3SKFJQD6J7-CA.
- A CA Certificate issued to and by supinfo-WIN-FNJVP9QUEH9-CA.
- An identity certificate was issued to WIN-E3SKFJQD6J7.razor.local by razor-WIN-E3SKFJQD6J7-CA.

In this configuration guide, the FQDN is WIN-E3SKFJQD6J7.razor.local and so the first two certificates are not valid for use as the LDAPs SSL certificate. The identity certificate issued to WIN-E3SKFJQD6J7.razor.local is a certificate that was automatically issued by the Windows Server CA service. Double-click the certificate in order to check the details.



- 7. In order to be used as the LDAPs SSL Certificate, the certificate must meet these requirements:
- The common name or DNS Subject Alternate Name matches the FQDN of the Windows Server.
- The Certificate has Server Authentication under the Enhanced Key Usage field.

Under the Details tab for the certificate, choose Subject Alternative Name, where the FQDN WIN-E3SKFJQD6J7.razor.local is present.

Cer	tificate	x			
General Details Certification Path					
Show: <all></all>	~				
Field	Value	a			
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.razor.local					
DNS Name = RAZOR					
DINS Name=RAZOR					
	the Descent for the State	n			
Ed	Copy to File				
Learn more about <u>certificate details</u>					
	OK				

Under Enhanced Key Usage, Server Authentication is present.

Cer	tificate X				
General Details Certification Path					
Show: <all></all>	×				
Field Certificate Template Inform	Value     ^       Template=LDAPoverSSL(1.3.6				
<ul> <li>Application Policies</li> <li>Subject Key Identifier</li> <li>Authority Key Identifier</li> <li>CRL Distribution Points</li> <li>Authority Information Access</li> <li>Key Usage</li> </ul>	[1] Application Certificate Polic1b 34 75 f8 c4 3e ef 58 fb 43KeyID=cf 83 92 a4 14 00 e7 5[1] CRL Distribution Point: Distr[1] Authority Info Access: AccDigital 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>					
	ОК				

8. Once that is confirmed, under the Certification Path tab, choose the top-level certificate which is the root CA certificate, and then click View Certificate. This opens the certificate details for the root CA certificate as shown in the image:

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. Under the Details tab of the root CA certificate, click Copy to File and navigate through theCertificate Export Wizard which exports the root CA in PEM format.

Choose Base-64 encoded X.509 as the file format.

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\roc	
	Export Keys	No	
	Include all certificates in the certification path	No Base64 Encoded V 509 (* cer)	
		2	
		Finish Cano	cel

10. Open the Root CA certificate stored in the selected location on the machine with a notepad or some other text editor.

This shows the PEM format certificate. Save this for later.

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

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo vcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCgu BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvcd CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41nOAziGs4ZMNM1X8UWeKuwi8w 9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61EOAV CSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEA DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI AA4IBAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q 4sMZffbVrG1Rz7twWY36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1b GuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi2OZy1tHR1dfUUbwVENSFQtDnFA7X ----END CERTIFICATE----

### In Case of Multiple Certificates Installed in the Local Machine Store on the LDAPs Server (Optional)

1. In a situation of multiple identity certificates that can be used by LDAPS and when there is uncertainty as to which is used, or there is no access to the LDAPS server, it is still possible to extract the root CA from a packet capture done on the FTD.

2. In the case where you have multiple certificates valid for Server Authentication in the LDAP server (such as AD DS domain controller) local computer certificate store, it can be noticed that a different certificate is used for LDAPS communications. The best resolution for such an issue is to remove all unnecessary certificates from the local computer certificate store and have only one certificate that is valid for server authentication.

However, if there is a legitimate reason that you require two or more certificates and have at least a Windows Server 2008 LDAP server, the Active Directory Domain Services (NTDS\Personal) certificate store can be used for LDAPs communications.

These steps demonstrate how to export an LDAPS-enabled certificate from a domain controller local computer certificate store to the Active Directory Domain Services service certificate store (NTDS\Personal).

- Navigate to the MMC console on the Active Directory Server, choose File, and then click Add/Remove Snap-in.
- Click Certificates and then click Add.
- In the Certificates snap-in, choose Computer account and then click Next.
- In Select Computer, choose Local Computer, click OK, and then click Finish. In Add or Remove Snap-ins, click OK.
- In the certificates console of a computer that contains a certificate used for Server Authentication, right-click the certificate, click All Tasks, and then click Export.

<b>a</b>	C	onsole1 - [Console Root\Certifi	cates (L	ocal Compu	uter	)\Persona	al\Certifi	cates]	_ <b>D</b> X
🚡 File Action View Favorites Wind	low	Help							_ 8 ×
🗢 🔿 🙍 🔚 🔏 🖼 📄 😣	?								
Console Root	_	Issued To	Issued B	y			Expiration	Date	Actions
∠ Gretificates (Local Computer)		razor-WIN-E3SKFJQD6J7-CA	razor-WI	N-E3SKFJQD6J	J7-C	A	3/22/2026		Certificates
Personal     Certificates		supinfo-WIN-FNJVP9QUEH9-CA	supinfo-	WIN-FNJVP9Q	QUEF	19-CA	2/23/2025		More Actions
Trusted Root Certification Autho			18201-101	N-ESSKI JQE		Open			WIN-E3SKEIOD617 razor local
Enterprise Trust	=					All Tasks	+	0	pen
Intermediate Certification Autno     Trusted Publishers						Cut		R	equest Certificate with New Key
Untrusted Certificates						Сору		R	enew Certificate with New Key
Third-Party Root Certification Au						Delete		N	Nanage Private Kevs
Trusted People						Properties		A	dvanced Operations
Other People						Help		F	vport
Remote Desktop						Theip			
Certificate Enrollment Requests									
Smart Card Trusted Roots									
Web Hosting	-								
		< III						>	
Export a certificate									

• Export the certificate in the pfx format in the subsequent sections. Reference this article on how to export a certificate in the pfx format from MMC:

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

- Once the export of the certificate is done, navigate to Add/Remove Snap-in on MMC console. Click Certificates and then click Add.
- Choose Service account and then click Next.

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

- In the Select Computer dialog box, choose Local Computer and click Next.
- Choose Active Directory Domain Services and then click Finish.

Certificates	snap-in X
Select a service account to manage on the local co	mputer.
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

- On the Add/Remove Snap-ins dialog box, click OK.
- Expand Certificates Services (Active Directory Domain Services) and then click NTDS\Personal.
- Right-click NTDS\Personal, click All Tasks, and then click Import.

Console1 - [Console Roo	ot\Certificates - Service (Active Directory Domain Services) on Local Comput	er\NTDS\Personal] 💶 🗙
🔚 File Action View Favorites Window	Help	_ <i>8</i> ×
🗢 🄿 🙇 🗊 📋 🧟 📷		
Console Root C	Dbject Type	Actions
Certificates (Local Computer)	Certificates	NTDS\Personal
Certificates - Service (Active Directory D     MT Find Certificates		More Actions
D 🛄 NT 🛛 All Tasks	Find Certificates	
▶ III NT ▶ III NT View	Minport	
NT New Window from Here	Advanced Operations	
NT New Taskpad View		
▶ 🛄 NT Refresh		
Export List		
Help		
Add a certificate to a store		,

- On the Certificate Import Wizard welcome screen, click Next.
- On the File to Import screen, click Browse, and locate the certificate file that you exported previously.
- On the Open screen, ensure that Personal Information Exchange (\*pfx,\*.p12) is selected as the file type and then navigate the file system to locate the certificate you exported previously. Then, click that certificate.

<b>a</b>	Oper	n			x			
🕞 💿 🔻 🕇 📑 🕨 Lib	raries > Documents		✓ ♂ Search Documents					
Organize 🔻 New folder				•				
🔆 Favorites	Name	Date modified	Туре	Size				
Desktop	🦻 Idapcert	4/25/2022 12:01	Personal Informati	5 KB				
i Downloads								
詞 Libraries								
Documents								
J Music								
Pictures								
💾 Videos								
👰 Computer								
🙀 Network								
File na	me: Idapcert		✓ Personal	Information Exchan	ge 🗸			
			Оре	n Canc	el			

- Click Open and then click Next.
- On the Password screen, enter the password you set for the file, and then click Next.
- On the Certificate Store page, ensure that Place all certificates are selected and read Certificate Store: NTDS\Personal and then click 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

• On the Certificate Import Wizard completion screen, click Finish. You then see a message that the import was successful. Click OK. It is seen that the certificate has been imported under the Certificate store: NTDS\Personal.

Console1 - [Console Root\Certific	ates - Service (Active Directory	Domain Services) on Local C	Computer\NTDS\P	ersonal\Certificates]	- 🗆 X
藩 File Action View Favorites Window	v Help				_ & ×
🗢 🔿 🙍 📰 🤞 ы 🔀 🗈					
Console Root	Issued To A	Issued By	Expiration Date	Actions	
Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates	<b></b>
∠ → Certificates - Service (Active Directory D ∠ → NTDS\Personal	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
Certificates				WIN-E3SKFJQD6J7.r	azor.local 🔺
ATDS\Interprise Trust     MTDS\Interprise Trust     MTDS\Intermediate Certification Au     MTDS\Intrusted Publishers     MTDS\Untrusted Certificates     MTDS\Intrusted Certificates     MTDS\Trusted People     MTDS\Client Authentication Issuers				More Actions	•
< III >	<		>		
NTDS\Personal store contains 2 certificates.					

### **FMC Configurations**

### Verify Licensing

In order to deploy the AnyConnect configuration, the FTD must be registered with the smart licensing server, and a valid Plus, Apex, or VPN Only license must be applied to the device.

### **Setup Realm**

1. Navigate to System > Integration. Navigate to Realms, then click Add Realm, as shown in this image:

Overview Analys	sis Policies Devices Objec	ts AMP Intelligence							<u></u>	Deploy Sys	tem Help 🔻	admin 🔻
				Configuration	Users Domains	Integration	Updates	Licenses v	Logging v	Health <b>v</b>	<sup>1</sup> Monitoring •	Tools •
	3					2						
Cloud Services	Realms Identity Source	High Availability	eStreamer Host Input Client	Smart Software Manag	ger On-Prem							
Realms - F	Carlin Caquancas Sunc Pasi	lte										
Realms	Realm Sequences Sync Rest	iits										•
										Compa	re Realms Ad	d Realm
Name +	Description	Туре	Domain	AD Primary Domain		Base DN				State		

2. Fill out the displayed fields based on the information collected from the Microsoft server for LDAPs. Prior to this, import the Root CA Certificate that has signed the LDAPs service Certificate on the Windows Server under Objects > PKI > Trusted CAs > Add Trusted CA, as this is referenced under theDirectory Server Configuration of the Realm. Once done, click 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 V	
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 (i)	
Resolve via route lookup	
Choose an interface	
Default: Management/Diagnostic Interface	~
Test	
Add another directory	

0 ×

3. Click Test in order to ensure FMC can successfully bind with the Directory Username and password provided in the earlier step. Since these tests are initiated from the FMC and not through one of the routable interfaces configured on the FTD (such as inside, outside, dmz), a successful (or failed) connection does not guarantee the same result for AnyConnect authentication since AnyConnect LDAP authentication requests are initiated from one of the FTD routable interfaces.

Add Directory	@ ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc	Port* 636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
Interface used to connect to Dire	ctory server 👔
Resolve via route lookup	
<ul> <li>Choose an interface</li> </ul>	
Default: Management/Diag	nostic Interface 🗸
Test 📀 Test connection s	succeeded
	Cancel OK

4. Enable the new realm.

Overview Ana	alysis Policies Devices Objects	AMP Intelligence							🔒 C	eploy Sys	Help *	admin v
				Configuration Users	Domains	Integration	Updates	Licenses v	Logging •	Health <b>v</b>	Monitoring •	Tools •
Cloud Service	es Realms Identity Sources	High Availability eStream	er Host Input Client	Smart Software Manager On-	Prem							
Realms	Realm Sequences Sync Results											
										Compa	re Realms Ac	id Realm
Name +	Description	Туре	Domain	AD Primary Domain		Base DN				State		
AC-Local		LOCAL	Global							🛑 Enabli	ed 🕂	· 🖥 🖥
LDAP		AD	Global	cisco01.com		OU=Users,OU	=CISCO,DC=	=cisco01,DC=c	om	C Enabl	ed 🛨 🌶	· G 🗑
LDAP-Server		AD	Global	razor.local		DC=razor,DC+	=local			C Enabl	ed 🛨 🖌	1 B 🗑

### **Configure AnyConnect for Password-Management**

1. Choose the existing Connection Profile or create a new one, if it is an initial setup of AnyConnect. Here, an existing Connection Profile named 'AnyConnect-AD' mapped with Local Authentication is used.

Overview Analysis Policies Devices Objects AMP Intelligence of Devices Objects AMP Intelligence							r admin <del>v</del>					
Device Management	Device Upgrade	NAT VPN •	Remote Access	QoS	Platform Settings	FlexConfig	Certificates					
AnyConnect											Save	Cancel
											Policy Assi	gnments (1)
									Local Realm: asa	D	ynamic Access Polic	ty: <u>Hostscan</u>
Connection Profile	Access Interfaces	Advanced										
												•
Name			A/	M.				Group Policy				
DefaultWE8VPNGroup			Au Au Ac	thentication thorization: counting:	None None None			DfltGrpPolicy				/8
AnyConnect			Au Au	thentication thorization: counting:	: Radius (RADIUS) Radius (RADIUS) None			DfltGrpPolicy				/ 8
AnyConnect-AD			Au Au	thentication thorization:	: LOCAL None None			AnyConnect-Group				/ 9

2. Edit the Connection profile and map the new LDAPs server configured in the earlier steps, under the AAA settings of the Connection Profile. Once done, click save on the top right corner.

Firepower Management Center Devices / VPN / Edit Connection Profile	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🙆 admin 🔻
AnyConnect Enter Description		Save Cancel
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 Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Authentication	/i
AnyConnect-AD	Authentication Netroc: Add Oliny * Authentication Server: LDAP-Server (AD) *	/i
	Fallback to LOCAL Authentication     Use secondary authentication     Authorization	
	Authorization Server: Use same authentication server	
	Accounting Accounting Server:	
	Advanced Settings     Strip Realm from username	
	Cancel Save	

3. Enable password management under the AAA > Advanced Settings and save the configuration.

Overview Analysis Policies Devices Objects AMP Intellig	ence	🇛 Deploy System Help 🕶 admin 🕶
AnyConnect Enter Description	Qoo Hadorm Settings HexLoning Certificates	Save Cancel
		Policy Assignments (1) Local Realm: asa Dynamic Access Policy: <u>Hostscan</u>
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? ×	
Name	Connection Profile:* AnyConnect-AD Group Policy:* AnyConnect-Group Edit Group Policy	0
DefaultWEBVPNGroup	Client Address Assignment AAA Aliases	/8
	(DAP-Gener (AD)	
AnyConnect	Fallback to LOCAL Authentication	/ 8
AnuConnect-AD	Use secondary authentication	29
Any Connect Ho	Authorization	2 U
sjobs	Authorization Server: Use same authoritication server  Authorization Server: Allow connection only if user exists in authorization database Configure LOPA Attribute Map	/ 6
	Accounting	
	Accounting Server:	
	Advanced Settings	
	Strip Realm from username	
	Strip Group from username	
	Netfor law	
	Notify user on the day of password expiration	
	Save Cancel	

### Deploy

1. Once done with all the configuration, click theDeploy button on the top right.

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

2. Click the checkbox next to the FTD configuration applied to it and then click Deploy, as shown in this image:

Overview	Analysis	olicies Devices Objects	s AMP Intelligence						9 Deploy System Help + admin +
									Deployment Deployment History
	Search usin	device name, user name, tvpe	a oroup or status						1 device selected Deploy time: Estimate Deploy
ШC	obaron abili	dence name, user name, type	, group or status						
•	Device		Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status
> 🛛	10.197.22	190_FTD1	admin		FTD		May 30, 2022 7:34 AM	B	Pending

### **Final Configuration**

This is the configuration seen in the FTD CLI after the successful deployment.

### **AAA Configuration**

<#root>

> show running-config aaa-server

aaa-server LDAP-Server protocol ldap

```
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 Configuration**

<#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

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

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

<---- Protocol

<---- LDAPs Serve

<----- Password-management

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

# Verification

# **Connect with AnyConnect and Verify the Password-Management Process for the User Connection**

1. Initiate a Connection to the concerned connection profile. Once it is determined at the initial login that the password must be changed since the earlier password was rejected by the Microsoft Server as it is expired, the user is prompted with the change of password.

Cisco AnyConnect   FTD-Hostname X	Cisco AnyConnect Secure Mobility Client     Viiii     Viiii     Contactor ITD Hostname.      TD Hostname     Contactor ITD Hostname
OK Cancel	



2. Once the user enters the new password for login, the connection is established successfully.

🚳 Cisco AnyC	onnect Secure Mobility Client		_		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnect	
00:02:43				I	Pv4
<b>\$</b> (i)					cisco

3. Verify the user connection on the FTD CLI:

```
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
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
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 : 0h:00m:51s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                   VLAN
                                              : none
Audt Sess ID : 0ac5e0fa000070006266a090
                                   Tunnel Zone : 0
Security Grp : none
```

# Troubleshoot

### Debugs

This debug can be run in diagnostic CLI in order to troubleshoot password management-related issues: **debug ldap 255**.

## Working Password-Management Debugs

<#ro	ot>
[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]	<pre>supportedLDAPVersion: value = 3</pre>
[24]	<pre>supportedLDAPVersion: value = 2</pre>
[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

### **Common Errors Encountered During the Password-Management**

Usually, if the password policy that is set by the Microsoft Server is not met during the time the user provides the new password, the connection gets terminated with the error "Password does not meet the Password Policy Requirements". Hence, ensure that the new password meets the policy set by the Microsoft Server for LDAPs.

Carnot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password policy requirements.		
Group: Dev v	Cisco AnyConnect Secure Mobility Client —      X     VPI:     Carnot complete password change because the password does not meet the password policy requirements. Check	
OK Cancel	FTD-Hostname 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.	