FMCによって管理されるFTD上のRA VPNに対 するLDAPを使用したパスワード管理の設定

内容

概要 前提条件 要件 使用するコンポーネント コンフィギュレーション ネットワークダイアグラムとシナリオ LDAPベースDNとグループDNの決定 LDAPS SSL証明書ルートのコピー LDAPサーバのローカルマシンストアに複数の証明書がインストールされている場合(オプショ ント FMCの設定 ライセンスの確認 レルムの設定 パスワード管理用のAnyConnectの設定 展開 **Final Configuration** AAA 設定 AnvConnectの設定 検証 AnyConnectに接続し、ユーザ接続のパスワード管理プロセスを確認する トラブルシュート <u>デバッグ</u> パスワード管理のデバッグの実行 パスワード管理中に発生する一般的なエラー

概要

このドキュメントでは、Cisco Password Threat Défense(FTD)に接続するAnyConnectクライアントのLDAPを使用したFirepower管理(PMS)の設定について説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

• FMCでのRA VPN(リモートアクセス仮想プライベートネットワーク)設定に関する基本的

な知識

- FMCでのLDAPサーバ設定に関する基本的な知識
- Active Directoryの基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft 2012 R2サーバ
- 7.3.0を実行するFMCv
- 7.3.0が稼働するFTDv

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

コンフィギュレーション

ネットワークダイアグラムとシナリオ



Windowsサーバは、ユーザパスワード管理プロセスをテストするために、ADDSおよびADCSで 事前設定されています。この設定ガイドでは、これらのユーザアカウントが作成されます。

ユーザアカウント:

- 管理者:これは、FTDがActive Directoryサーバにバインドできるようにするためのディレクトリアカウントとして使用されます。
- admin:ユーザーIDを示すために使用されるテスト管理者アカウント。

LDAPベースDNとグループDNの決定

1. 開く Active Directory Users and Computers Server Manager Dashboardを使用します。

Server Ma Server Ma Local Server	nager • Dashboard welcome to server manager		CO Manage Tools View Holp Active Directory Administrative Center Active Directory Domains and Truts Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Lifes and Computer
III An Servers R AD CS III AD DS 과 AD FS 으 DNS IIIS 약 NAP	Configure this local server Add roles and features Add other servers to manage Add other servers Add other servers Add other servers to manage Add other servers Add ot	1 Image AD FS 1 Image ability Events 1 Image ability Events<	File File File File File File Service Monitor Service System Information Service Servic
	IIS 1 IIS 1 Imageability Imageability Events Events Services Services Performance Performance BPA results BPA results	1 Image ability 1 Image ability Events Services Performance BPA results BPA results	Windows PowerShell Windows PowerShell (s88) Windows PowerShell (s8 Windows Server Backup Windows Server Backup Activate Windows Go to Action Center to activate Windows.

2. を開きます。 View Option をオンにし、 Advanced Featuresをクリックします(図を参照)。

	Active Directory	Users and Computers	_ □ ×
File Action View	v Help		
🗢 🔿 🖄 [Add/Remove Columns		
Active Direc Saved C Saved C	Large Icons Small Icons List Detail Users, Contacts, Groups, and Computers as containers Advanced Features Filter Options Customize tas ces NTDS Quotas msDS-QuotaC Quota TPM Devices msTPM-Infor Infrastructure infrastructureU	n ntainer for up ntainer for do ntainer for sec ntainer for ma ation for stor em settings 	
Displays items in a list			

3. これにより、ADオブジェクトの下に追加のプロパティを表示できます。 たとえば、ルートのDNを見つけるには、 razor.local、右クリック razor.localを選択し、 Properties次 の図に示すように、

	Active Directory Users and Cor	nputers	D X			
File Action View Help						
🗢 🌩 🙇 🗊 📋 🖾 🧟 😹						
Active Directory Users and Com Name Ty	Description					
Saved Queries Builtin builtin Built Delegate Control Built Find Change Domain Change Domain Controller Change Domain functional level Operations Masters Man Operations Masters Man New Syste New User: All Tasks NTD TPM	nDomain ner Default container for up, zational Default container for do. ner Default container for or. ner Default container for ma ner Default location for stor. ner Builtin system settings ner Default container for up. QuotaC Quota specifications co. 1-Infor uctureU					
Opens the properties dialog box for the current selection.						

4. 通常の Propertiesを選択し、 Attribute Editor tab.検索 distinguishedName 「属性」の下のをクリックし、 Viewをクリックします。

新しいウィンドウが開き、DNをコピーして後でFMCに貼り付けることができます。

この例では、ルートDNは _{DC=razor}、 _{DC=local}を参照。値をコピーして、後で使用できるように保存 します。クリック ок String Attribute Editorウィンドウを終了し、 ок プロパティを終了します。

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:	Value					
DC=razor,DC=local						
Clear	OK Cano	el				

LDAPS SSL証明書ルートのコピー

1. プレス Win+R 次のように入力します。 mmc.exeをクリックし、 OK,以下の図に、出力例を示します。

🖅 Run	\times
0	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	mmc.exe ~
	OK Cancel <u>B</u> rowse

2. 移動先 File > Add/Remove Snap-in...、次の図に示すss:

5				Console1 - [Console Root]		_ 🗆 X
	File	Action View Favorites Window	Help			_ 8 ×
		New	Ctrl+N			
		Open	Ctrl+0		Actions	
		Save	Ctrl+S	There are no items to show in this view.	Console Root	•
	_	Save As	C 1 1 1		More Actions	•
		Add/Remove Snap-in	Ctrl+M			
		1 CONTRACT OF 200				
		1 C:\Windows\system32\dsa				
		3 C:\Windows\system32\certmar				
		4 C:\Windows\system32\certsrv				
		Exit				
1						
Enal	oles	/ou to add snap-ins to or remove them f	rom the sna	-in console.	1	
		•			1	

3. [使用可能なスナップイン]で、 Certificates 次に、 Add次の図に示すように、

venuor	^	Console Root	Edit Extensions
Microsoft Cor			Remove
 Microsoft Cor 			Dennere
Microsoft Cor			Mauralda
Microsoft Cor			move <u>U</u> p
Microsoft Cor			Move Down
Microsoft Cor		<u>A</u> dd >	
Microsoft Cor			
Microsoft and			
	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor

4. 選択 Computer account 次に、 Next次の図に示すように、

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

次に示すように、 Finishを参照。

Select Computer	\times
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: Browse 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 Cancel	

5. ここで、ок,以下の図に、出力例を示します。

ap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor		Certificates (Local Computer)	Remove
Active Directory Site	Microsoft Cor			Genere
Active Directory Use	Microsoft Cor			
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			Move Down
Authorization Manager	Microsoft Cor		Add >	nore gomi
Certificate Templates	Microsoft Cor		bear for an and	
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
*Disk Management	Microsoft and	¥		Advanced

- 6. を展開します Personal フォルダを選択し、 Certificatesを参照。LDAPで使用される証明書は、 Windowsサーバの完全修飾ドメイン名(FQDN)に対して発行する必要があります。このサー バには、次の3つの証明書がリストされています。
- ・ CA証明書の発行先および発行元 razor-WIN-E3SKFJQD6J7-CAを参照。
- ・およびによって発行されたCA証明書 supinfo-WIN-FNJVP9QUEH9-CAを参照。
- ・ ID証明書が発行されました WIN-E3SKFJQD6J7.razor.local by razor-WIN-E3SKFJQD6J7-CAを参照。

この設定ガイドでは、FQDNは WIN-E3SKFJQD6J7.razor.local したがって、最初の2つの証明書はLDAP SSL証明書として使用することはできません。ID証明書の発行先 WIN-E3SKFJQD6J7.razor.local は、 Windows Server CAサービスによって自動的に発行された証明書です。詳細を確認するには、証 明書をダブルクリックします。



- 7. LDAP SSL証明書として使用するには、証明書が次の要件を満たしている必要があります。
- ・ 共通名またはDNSサブジェクトの別名がWindows ServerのFQDNと一致します。
- 証明書のEnhanced Key Usageフィールドにサーバ認証が設定されている。

の下 Details タブをクリックし、 Subject Alternative NameFQDNが WIN-E3SKFJQD6J7.razor.local が存在します。

Certificate	x				
General Details Certification Path					
	٦				
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					
Edit Proportion					
Copy to Pile					
Learn more about <u>certificate details</u>					
OK	5				
OK					

通常の Enhanced Key Usage、 Server Authentication が存在します。

📃 Cer	tificate X			
General Details Certification Path				
Show: <all></all>	~			
Field	Value ^ Template=LDAPoverSSL(1.3.6			
Enhanced Key Usage	Client Authentication (1.3.6.1			
Application Policies	[1]Application Certificate Polic			
Authority Key Identifier	$10 34 75 78 c4 3e er 58 70 43 KeyID=cf 83 92 a4 14 00 e7 5 \equiv$			
CRL Distribution Points	[1]CRL Distribution Point: Distr [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>				
	ОК			

8. これが確認されたら、 Certification Path タブで、ルートCA証明書である最上位の証明書を選択 し、 View Certificateを参照。次の図に示すように、ルートCA証明書の詳細な証明書が開きます。

Certificate	x	Certificate X
General Details Certification Path Certification path arcor-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
		Issued to: razor-WIN-E3SKFJQD6J7-CA
View Certificate		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>		Learn more about <u>certificates</u>
ОК		ОК

9. の下 Details タブをクリックし、 Copy to File ネットワーク内のCertificate Export Wizard ルートCAを PEM形式でエクスポートします。

選択 Base-64 encoded X.509をファイル形式として使用します。

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\roc	
	Export Keys Include all certificates in the certification path	No No	
	File Format	Base64 Encoded X.509 (*.cer)	
	< III	>	
		Finish Cano	cel

10. メモ帳またはその他のテキストエディタを使用して、マシン上の選択した場所に格納されて いるルートCA証明書を開きます。

PEM形式の証明書を示します。後で使用するために保存します。

----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo vcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCgr BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvc CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41nOAziGs4ZMNM1X8UWeKuwi8 9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61E0AV CSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwE DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI AA4IBAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q 4sMZffbVrG1Rz7twW36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1b GuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi2OZy1tHR1dfUUbwVENSFQtDnFA7X

LDAPサーバのローカルマシンストアに複数の証明書がインストールされている場合(オプション)

1. LDAPSで使用できるID証明書が複数ある状況で、使用されるIDが不明な場合、または LDAPSサーバへのアクセスがない場合でも、FTDで実行されたパケットキャプチャからルート CAを抽出することは可能です。

2. LDAPサーバー(AD DSドメインコントローラーなど)のローカルコンピューターの証明書ス トアに、サーバー認証に有効な証明書が複数ある場合は、LDAPS通信に別の証明書が使用されて いる可能性があります。このような問題の最善の解決策は、ローカルコンピュータの証明書スト アから不要な証明書をすべて削除し、サーバ認証に有効な証明書を1つだけ保持することです。

ただし、複数の証明書が必要で、少なくとも1台のWindows Server 2008 LDAPサーバを所有して いるという正当な理由がある場合は、LDAP通信にActive Directoryドメインサービス (NTDS\Personal)証明書ストアを使用できます。

次の手順では、LDAPS対応の証明書をドメインコントローラーのローカルコンピューターの証明 書ストアからActive Directoryドメインサービスのサービスの証明書ストア(NTDS\Personal)にエ クスポートする方法を示します。

- Active DirectoryサーバのMMCコンソールに移動し、Fileを選択して、 Add/Remove Snap-inを参照
 。
- クリック Certificates 次に、Addを参照。
- 内 Certificates snap-in, 選択 Computer account 次に、 Nextを参照。
- イン Select Computer,選択 Local Computerをクリックし、OKをクリックし、Finishを参照。イン Add or Remove Snap-insをクリックし、OKを参照。
- ・サーバ認証に使用する証明書が格納されているコンピュータの証明書コンソールで、 certificateをクリックし、All Tasksをクリックし、Exportを参照。

2	onsole1 - [Console Root\Certificates (Local Computer)\Perso	onal\Certificates]
🚟 File Action View Favorites Windo	/ Help	_ <i>8</i> ×
🗢 🔿 🚈 🔣 🖬 🕹 📘		
Console Root	Issued To Issued By	Expiration Date Actions
∠ Gertificates (Local Computer)	razor-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	A WIN-E3SKFJQD6J7.razor.local razor-WIN-E3SKFJQD517.co	
Enterprise Trust =		WIN-E3SKEIOD617 razor local
Intermediate Certification Autho	All Tas	open V
Trusted Publishers	Cut	Request Certificate with New Key
Untrusted Certificates	Сору	Renew Certificate with New Key
Third-Party Root Certification Au	Delete	Manage Private Keys
Client Authentication Issuer	Propert	ies Advanced Operations
Client Authentication issuers Other People		
Remote Desktop	Help	Export
Certificate Enrollment Requests		
Smart Card Trusted Roots		
Trusted Devices		
Web Hosting		
Export a certificate		

 証明書を pfx フォーマットについては、以降のセクションを参照してください。で証明書を エクスポートする方法については、この記事を参照してください。 pfx mmcからのフォーマ ット:

<u>https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html</u> にアクセスしてください。

- 証明書のエクスポートが完了したら、 Add/Remove Snap-in 日付: MMC consoleを参照。クリック Certificates 次に、 Addを参照。
- ・ 選択 Service account 次に、 Nextを参照。

Certificates snap-in

х

This snap-in will always manage certificates for:

- My user account
- Service account
- Computer account
- 内 Select Computer ダイアログボックス、選択 Local Computer をクリックして Nextを参照。

• 選択 Active Directory Domain Services 次に、 Finishを参照。

Certificate	es snap-in
Select a service account to manage on the local o	:omputer.
Service account:	
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 Eitering Engine	
	< Back Finish Cancel

- ・ 次の Add/Remove Snap-ins ダイアログボックスを開き、 OKを参照。
- ・ 拡張 Certificates Services (Active Directory Domain Services) 次に、 NTDS\Personalを参照。
- 右クリック NTDS\Personalをクリックし、 All Tasksをクリックし、 Importを参照。

Console1 - [Console Root\C	ertificates - Service (Active Directory Domain Services) o	n Local Computer\NTDS\Personal]		
藩 File Action View Favorites Window Help	,	_ <i>8</i> ×		
🗢 🔿 🙍 🗂 📋 🧟 🖬				
Console Root Object	t Type	Actions		
Certificates (Local Computer)	rtificates	NTDS\Personal		
Certificates - Service (Active Directory D		More Actions		
NT All Tasks	Find Certificates			
▷ INT ▷ INT View ▷ INT View ▷ INT New Window from Here	Import Import NT NT			
NT New Taskpad View				
▷ NI ▷ NT Refresh Export List				
Help				
Add a certificate to a store				

- 次の Certificate Import Wizard ようこそ画面で、 Nextを参照。
- [インポートするファイル]画面で、Browseをクリックし、以前にエクスポートした証明書ファイルを探します。
- Open画面で、Personal Information Exchange(*pfx、*.p12)をファイルタイプとして選択し、 ファイルシステムをナビゲートして、以前にエクスポートした証明書を見つけます。次に、 その証明書をクリックします。

-	Ope	n	/		x
🕞 🕘 ▾ ↑ 📑 ኑ Lib	oraries > Documents		♥ 🖒 Search Do	ocuments	Q
Organize 👻 New folder				•	
🔶 Favorites	Name	Date modified	Туре	Size	
Desktop	🌛 ldapcert	4/25/2022 12:01	Personal Informati	5 KB	
i Downloads ا Recent places					
Cibraries					
Pictures					
🛃 Videos					
👰 Computer					
🗣 Network					
File na	me: Idapcert		✓ Personal	Information Exc	:hange ∨
			Оре	n C	ancel

- クリック Open 次に、 Nextを参照。
- [パスワード]画面で、ファイルに設定したパスワードを入力し、Nextを参照。
- ・ Certificate Storeページで、Place all certificatesが選択されていることを確認し、Certificate Storeを読み取ります。 NTDS\Personal 次に、 Nextを参照。

€	🔗 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

• 次の Certificate Import Wizard 完了の画面で、 Finishを参照。インポートが成功したことを示すメッ セージが表示されます。クリック OKを参照。証明書が証明書ストアにインポートされたこ とを確認できます。 NTDS/Personalを参照。

Console1 - [Console Root\Certifica	ates - Service (Active Directory	Domain Services) on Local C	computer\NTDS\Pe	ersonal\Certificates] 🗕 🗖	x
藩 File Action View Favorites Window	/ Help			_ (5 ×
🗢 🔿 🙋 📰 🤞 💺 🖬 🛃					
Console Root	Issued To	Issued By	Expiration Date	Actions	
Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates	
⊿ GU Certificates - Service (Active Directory D)	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
⊿ IntoS\Personal				More Actions	·
NTDS\Trusted Root Certification Au				WIN-E3SKFJQD6J7.razor.local	-
NTDS\Enterprise Trust				More Actions	•
NTDS\Intermediate Certification Au					
NTDS\Trusted Publishers					
NTDS\Untrusted Certificates					
NTDS\Third-Party Root Certification					
INTDS\Trusted People					
NTDS\Client Authentication Issuers					
< III >	< III		>		
NTDS\Personal store contains 2 certificates.					

FMCの設定

ライセンスの確認

AnyConnect設定を導入するには、FTDがスマートライセンスサーバに登録され、有効なPlus、 Apex、またはVPN Onlyライセンスがデバイスに適用されている必要があります。

レルムの設定

1. 移動先 System > Integrationを参照。移動先 Realmsをクリックし、 Add Realm次の図に示すように、

Overview Analy	ysis Policies Dev	vices Objects	AMP Intelligence										%	Deploy Sy	stem Help 🔻	admin 🔻
							Configuration	Users	Domains	Integration	Updates	Licenses v	Logging v	Health •	¹ Monitoring •	Tools •
	3									2						
Cloud Services	s Realms Id	dentity Sources	High Availability	eStreamer	Host Input Client	Smai	rt Software Man	ager On-I	Prem							
Realms	Realm Sequences	Sync Results														4
														Compa	re Realms	id Realm
Name -	Description		Type	De	omain		AD Primary Domai			Base DN				State		

2. LDAPに関してMicrosoftサーバから収集した情報に基づいて、表示されているフィールドに 入力します。その前に、LDAPsサービス証明書に署名したルートCA証明書をWindows Serverの Objects > PKI > Trusted CAs > Add Trusted CAを参照してください。これはDirectory Server Configuration を指定します。完了したら、 OKを参照。

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 Izenoe.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	
Гуре	
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	
 WIN-E3SKFJQD6J7.razor.local:636 	
Hostname/IP Address*	Port*
WIN-E3SKFJQD6J7.razor.local	636
Encryption	CA Certificate*
LDAPS V	LDAPS-ROOT-CERT V +
Interface used to connect to Directory server	,
Choose an Interrace	
Default: Management/Diagnostic Interface	×
Test	

 $0 \times$

3. クリック Test FMCが、前の手順で指定したディレクトリのユーザ名とパスワードで正常にバ インドできることを確認します。これらのテストは、FTDに設定されたルーティング可能な インターフェイス(inside、outside、dmzなど)の1つではなく、FMCから開始されるため 、接続が成功(または失敗)しても、AnyConnect LDAP認証要求がFTDのルーティング可 能なインターフェイスの1つから開始されるため、AnyConnect認証で同じ結果が得られることは保証されません。

Add Directory	? ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc Encryption	Port* 636 CA Certificate*
LDAPS	LDAPS-ROOT-CERT +
 Resolve via route lookup 	
O Choose an interface	
Default: Management/Dia	gnostic Interface 🗸
Test Test connection 	succeeded
	Cancel OK

4. 新しいレルムを有効にします。

Overview Analy	ysis Policies Devices Objects	AMP Intelligence					👫 Deploy Sys	tem Help + admin +
				Configuration Users	Domains Integration	Updates Licenses •	Logging • Health •	Monitoring • Tools •
Cloud Services	Realms Identity Sources	High Availability eStreame	r Host Input Client	Smart Software Manager On-Pre	2m			
Realms	Realm Sequences Sync Results							
							Compar	e Realms Add Realm
Name +	Description	Туре	Domain	AD Primary Domain	Base DN		State	
AC-Local		LOCAL	Global				Enable	d 🗼 🖊 🖥 🗑
LDAP		AD	Global	cisco01.com	OU=Users,0	U=CISCO,DC=cisco01,DC=	com 💽 Enable	d 🛓 🖊 🛍 🗑
LDAP-Server		AD	Global	razor.local	DC=razor,D0	C=local	Enable	d ±∕ ∎∎

パスワード管理用のAnyConnectの設定

1. AnyConnectの初期設定の場合は、既存の接続プロファイルを選択するか、新しい接続プロ ファイルを作成します。ここでは、ローカル認証にマッピングされた「AnyConnect-AD」 という名前の既存の接続プロファイルが使用されます。

Overview Analysis Policies Devices Objects AMP Inte	elligence	•	Deploy System Help v admin v
Device Management Device Upgrade NAT VPN > Remote Acc	cess QoS Platform Settings FlexConfig Certificates		
AnyConnect Enter Description			Save Cancel
			Policy Assignments (1)
		Local Realm: asa	Dynamic Access Policy: Hostscan
Connection Profile Access Interfaces Advanced			
			0
Name	ААА	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/ 6
AnyConnect	Authentication: Radius (RADIUS) Authentization: Radius (RADIUS) Accounting: Anone	DftGrpPolicy	/ 6
AnyConnect-AD	Authentication: LOCAL Authentization: None Accounting: None	AnyConnect-Group	/ 6

2. 接続プロファイルを編集し、前の手順で設定した新しいLDAPサーバを接続プロファイルの AAA設定の下にマッピングします。完了したら、 Save をクリックします。

CISCO Evices / VPN / Edit Connection Profile Overview	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🔞 admin 🔻
AnyConnect		Save
Enter Description		Policy Assignments (1)
Connection Profile Assess Introduces Advanced	Edit Connection Profile	Local Realm: None Dynamic Access Policy: Hostscan
Connection Prome Access interfaces Advanced	Connection Profile:* AnyConnect-AD	
	Group Policy:* AnyConnect-Group +	+
Name	Edit Group Policy Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Authentication	/1
AnyConnect	Authentication Method: AAA Only	/≆
AnyConnect-AD	Authentication Server: LDAP-Server (AD)	/i
	Fallback to LOCAL Authentication	
	Use secondary authentication	
	Authorization Server: Use same authentication server	
	Allow connection only if user exists in authorization database Confoure LDAP Attribute Man	
	Accounting	
	Accounting Server:	
	 Advanced Settings 	
	Strip Realm from username	
	Cancel Save	

3. パスワード管理を有効にする AAA > Advanced Settings 設定を保存します。

Overview Analysis Policies Devices Objects AMP Intellig	Cocc Platform Settings ElevConfig. Cartificates	🇛 Deploy System Help 🕶 admin 🕶
AnyConnect Enter Description	Cos riscom scores cerurates	Save Cancel
		Policy Assignments (1) Local Realm: asa Dynamic Access Policy: <u>Hostscan</u>
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? ×	
	Connection Profile: * AnyConnect-AD Group Policy: * AnyConnect-Group V O	0
DefaultWEBVPNGroup		18
	Client Address Assignment AAA Aliases	
AnyConnect	LDAP-Server (AD)	/ 8
AnyConnect-AD	Use secondary authentication	28
	Authorization Authorization Server: Use same authentication server	
sjobs	Allow connection only if user exists in authorization database Configure LDAP Attribute Map	2 B
	Accounting	
	Accounting Server:	
	Advanced Settings	
	Strip Realm from username	
	Strip Group from username	
	Notify User I days prior to password expiration	
	Notify user on the day of password expiration	
	Save Cancel	

展開

1. すべての設定が完了したら、Deploy ボタンをクリックします。

Overview Analysis Policies Devices Objects AMP Intelligence

2. 適用されているFTD設定の横にあるチェックボックスをクリックし、 Deploy次の図に示すように、

Overview a	Analysis Policies Devices Objects AMP	Intelligence						90 Deploy System Help + admin +
								Deployment Deployment History
Y Q	Search using device name, user name, type, group or	status						1 device selected Deploy time: Estimate Deploy
•	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	B	Pending

Final Configuration

これは、導入が成功した後にFTD CLIに表示される設定です。

AAA 設定

<#root>

> show running-config aaa-server

aaa-server LDAP-Server protocol ldap

PDEPloy 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

AnyConnectの設定

<#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

検証

AnyConnectに接続し、ユーザ接続のパスワード管理プロセスを確認する

1.関連する接続プロファイルへの接続を開始します。初期ログイン時に、パスワードの有効期限 が切れていたため以前のパスワードがMicrosoft Serverによって拒否されたため、パスワードを変 更する必要があると判断されると、パスワードの変更を求めるメッセージがユーザーに表示され ます。

Group: Der Usernane: drinn Password: [Cisco AnyConnect Secure Mobility Client - × Contacting PTD-Hostname. PTD-Hostname Connect	
© Cisco AnyConnect FTD-Hostn	Carcel © ©	
Verify Password: Password change required password with a minimum k	y you must enter a new ength of 7 to continue. Control Cont	

2. ユーザがログイン用の新しいパスワードを入力すると、接続が正常に確立されます。

🕙 Cisco AnyC		—		×	
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnect	
00:02:43				I	Pv4
۞ (i)					cisco

3. FTD CLIでユーザ接続を確認します。

<#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 2022 Duration : 0h:00m:51s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5e0fa000070006266a090 Security Grp : none Tunnel Zone : 0

トラブルシュート

デバッグ

このデバッグは、パスワード管理に関連する問題をトラブルシューティングするために、診断 CLI(debug Idap 255)で実行できます。

パスワード管理のデバッグの実行

<#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

パスワード管理中に発生する一般的なエラー

通常、ユーザーが新しいパスワードを入力する間にMicrosoft Serverによって設定されたパスワー ドポリシーが満たされない場合、接続は終了し、「パスワードがパスワードポリシーの要件を満 たしていません」というエラーが表示されます。したがって、新しいパスワードがMicrosoft Serverで設定されているLDAPのポリシーを満たしていることを確認します。

Sisco AnyConne	ect I FTD-Hostname X		
Cannot com password p complexity,	inglet password change because the password does not meet the olicy requirements. Check the minimum password length, password , and password history requirements.		
Group:	Dev 🗸	🕙 Cisco AnyConnect Secure Mobility Client — 🗆 🗙	
Username:	admin		
Password:		Cannot complete password change because the password does not meet the password policy requirements. Check	
	OK Cancel	FTD-Hostname v Connect	
		O este	
		Cisco AnyConnect X	
		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	

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。