Configuración de la administración de contraseñas mediante LDAPs para VPN de RA en FTD administrado por FMC

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configuración
Diagrama y escenario de la red
Determinar DN Base LDAP y DN de Grupo
Copiar la raíz del certificado SSL LDAPS
En caso de tener varios certificados instalados en el almacén del equipo local en el servidor LDAPs (opcional)
Configuraciones de FMC
Verificar licencia
Rango de configuración
Configuración de AnyConnect para la gestión de contraseñas
Implementación
Configuración final
Configuración AAA
Configuración de AnyConnect
Verificación
Conectar con AnyConnect y verificar el proceso de administración de contraseñas para la conexión de usuario
Troubleshoot
Depuraciones
Depuraciones de administración de contraseñas en funcionamiento
Errores comunes encontrados durante la administración de contraseñas

Introducción

Este documento describe la configuración de la administración de contraseñas mediante LDAP para los clientes de AnyConnect que se conectan a Cisco Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Conocimiento básico de la configuración de VPN (red privada virtual de acceso remoto) de RA en FMC
- Conocimiento básico de la configuración del servidor LDAP en FMC
- Conocimientos básicos de Active Directory

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor Microsoft 2012 R2
- FMCv con 7.3.0
- FTDv con 7.3.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración

Diagrama y escenario de la red



Windows Server está preconfigurado con ADDS y ADCS para probar el proceso de administración de contraseñas de usuario. En esta guía de configuración, se crean estas cuentas de usuario.

Cuentas de usuario:

- Administrador: se utiliza como cuenta de directorio para permitir que el FTD se enlace al servidor de Active Directory.
- admin: cuenta de administrador de prueba utilizada para demostrar la identidad del usuario.

Determinar DN Base LDAP y DN de Grupo

1. Abra Active Directory Users and Computers a través del panel del Administrador del servidor.



Abra el View Option en el panel superior y habilite el Advanced Features, como se muestra en la imagen:

٠



Esto permite ver propiedades adicionales debajo de los objetos de AD.

•

Por ejemplo, para buscar el DN para la raízrazor.local, haga clic con el botón derecho razor.local y luego elija Properties, como se muestra en esta imagen:



En Properties, elija la Attribute Editor ficha. Busque distinguishedName en Atributos y, a continuación, haga clic en View, como se muestra en la imagen.

Esto abre una nueva ventana donde el DN se puede copiar y pegar en FMC más adelante.

En este ejemplo, el DN raíz es DC=razor, DC=local. Copie el valor y guárdelo para más tarde. Haga clic OK para salir de la ventana Editor de atributos de cadena y haga clic OK nuevamente para salir de Propiedades.

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

•

٠

Presione Win+R e ingrese mmc.exe, luego haga clic en OK, como se muestra en esta imagen.

🖅 Run	×
9	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

Navegue hasta File > Add/Remove Snap-in..., como se muestra en esta imagen:



En complementos disponibles, elija Certificates y haga clic en Add, como se muestra en esta imagen:

•

		Console Noor	Edit Extensions
Microsoft Cor			
Microsoft Cor			Remove
Microsoft Cor			
Microsoft Cor			Move Up
Microsoft Cor			Marco Decision
Microsoft Cor		Add >	Move Down
Microsoft Cor		Con .	
Microsoft Cor			
Microsoft and	~		Advanced
	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor

Elija Computer account y luego haga clic Next, como se muestra en esta imagen:

•

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

Como se muestra aquí, haga clic en Finish.

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: Another computer: Allow the selected computer to be changed when launching from the command line. This only applies if you save the console. 	
< Back Finish Cance	I

Ahora, haga clic OK, como se muestra en esta imagen.

•

nap-in	Vendor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			up certificates (Local Computer	Remove
Active Directory Site	Microsoft Cor				-
Active Directory Use	Microsoft Cor				Marcalda
ActiveX Control	Microsoft Cor				Move <u>U</u> p
ADSI Edit	Microsoft Cor				Move Down
Authorization Manager	Microsoft Cor		<u>A</u> dd >		
Certificate Templates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor.				
Device Manager	Microsoft Cor				
Disk Management	Microsoft and	~			Advanced
			l l		
cription:					

Expanda la Personal carpeta y haga clic en Certificates. El certificado utilizado por LDAP debe emitirse con el nombre de dominio completo (FQDN) del servidor de Windows. En este servidor, hay tres certificados enumerados:

Se ha emitido un certificado de CA a y por razor-WIN-E3SKFJQD6J7-CA.

•

•

•

•

Certificado de CA emitido a y por supinfo-WIN-FNJVP9QUEH9-CA.

Ha emitido un certificado de identidad WIN-E3SKFJQD6J7.razor.local para razor-WIN-E3SKFJQD6J7-CA.

uso como certificado SSL de LDAPs. El certificado de identidad emitido para WIN-E3SKFJQD6J7.razor.local es un certificado emitido automáticamente por el servicio de CA de Windows Server. Haga doble clic en el certificado para verificar los detalles.

🚡 (Console1 - [Console Root\Certif	icates (Local Computer)\Perso	nal\Certificates]		- 🗆 X
🚟 File Action View Favorites Window	v Help				_ 8 ×
🗢 🏟 🖄 📰 📋 🙆 🕞 🚺 🗊					
Console Root	Issued To 📩	Issued By	Expiration Date	Actions	
Certificates (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	🛱 WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	,
Irusted Root Certification Autho Enterprise Trust					
Enterprise Trust =					
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					
Vieb Hosting	<		>		
Personal store contains 3 certificates.				1	

Para ser utilizado como certificado SSL de LDAPs, el certificado debe cumplir con estos requisitos:

•

•

•

El nombre común o el nombre alternativo de asunto DNS coincide con el FQDN del servidor de Windows.

El certificado tiene autenticación de servidor en el campo Enhanced Key Usage (Uso mejorado de clave).

En la Details ficha del certificado, elija Subject Alternative Name, donde WIN-E3SKFJQD6J7.razor.local aparece el FQDN.

Cer	tificate ×					
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	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						
Learn more about <u>certificate details</u>						
	ОК					

Debajo Enhanced Key Usage, Server Authentication está presente.

Cer	tificate X				
General Details Certification Path	1				
Show: <all></all>	~				
Field	Value ^				
Certificate Template Inform	Template=LDAPoverSSL(1.3.6				
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 🗸				
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				

•

Una vez confirmado, en la Certification Path ficha, elija el certificado de nivel superior que es el certificado de CA raíz y, a continuación, haga clic en View Certificate. Esto abre los detalles del certificado para el certificado de CA raíz como se muestra en la imagen:

Certificate	x	Certificate X
General Details Certification Path Certification path Tazor-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
		Issued to: razor-WIN-E3SKFJQD6J7-CA
View Certific	ate	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	OK

En la Details ficha del certificado de la CA raíz, haga clic en Copy to File y navegue por lasCertificate Export Wizard que exporta la CA raíz en formato PEM.

Elija Base-64 encoded X.509 como formato de archivo.

٠

🛞 🥃 C	Certificate Export Wizard		
c	Completing the Certificate Exp	oort Wizard	
Y	ou have successfully completed the Certificate	Export wizard.	
Y	ou have specified the following settings:		_
	File Name	C:\Users\Administrator\Downloads\r	oc
	Export Keys	No	
	Include all certificates in the certification path	No	
	File Format	Base64 Encoded X.509 (~.cer)	
	< 111	3	>
			_
		Finish	Cancel

Abra el certificado de CA raíz almacenado en la ubicación seleccionada en el equipo con un bloc de notas u otro editor de texto.

Muestra el certificado de formato PEM. Guarde esto para más tarde.

-----BEGIN CERTIFICATE-----

 CSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhujlx4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEAAaNRME8w DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUAOdY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0C AA4IBAQCiSm5U7U6Y7zXdx+dleJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6qZu 4sMZffbVrGlRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylbBfn0NEX7l GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+of0kWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X -----END CERTIFICATE-----

En caso de tener varios certificados instalados en el almacén del equipo local en el servidor LDAPs (opcional)

1. En una situación de múltiples certificados de identidad que pueden ser utilizados por LDAPS y cuando hay incertidumbre sobre cuál se utiliza, o no hay acceso al servidor LDAPS, todavía es posible extraer la CA raíz de una captura de paquetes realizada en el FTD.

2. En el caso de que tenga varios certificados válidos para Autenticación de servidor en el almacén de certificados del equipo local del servidor LDAP (como el controlador de dominio AD DS), se puede observar que se utiliza un certificado diferente para las comunicaciones LDAP. La mejor solución para este problema es quitar todos los certificados innecesarios del almacén de certificados del equipo local y tener sólo un certificado válido para la autenticación del servidor.

Sin embargo, si hay un motivo legítimo para que necesite dos o más certificados y tenga al menos un servidor LDAP de Windows Server 2008, se puede utilizar el almacén de certificados de Servicios de dominio de Active Directory (NTDS\Personal) para las comunicaciones LDAP.

Estos pasos muestran cómo exportar un certificado habilitado para LDAPS desde un almacén de certificados de equipo local del controlador de dominio al almacén de certificados del servicio de Servicios de dominio de Active Directory (NTDS\Personal).

Vaya a la consola de MMC en el servidor de Active Directory, elija Archivo y, a continuación, haga clic en Add/Remove Snap-in.

Haga clic Certificates y, a continuación, haga clic en Add.

En la Certificates snap-in, elija Computer account y, a continuación, haga clic en Next.

En Select Computer, elija Local Computer, haga clic en OK y, a continuación, haga clic en Finish. En Add or Remove Snap-ins, haga clic en OK.

En la consola de certificados de un equipo que contiene un certificado utilizado para la Autenticación de servidor, haga clic con el botón secundario del mouse en el certificate, haga clic en All Tasks y, a continuación, haga clic en Export.

a (Console1 - [Console Root\Certifi	cates (Local Computer)\Perso	nal\Certificates]	_ D X
藩 File Action View Favorites Window	w Help			_ 8 ×
🗢 🏟 🖄 📰 🐇 🔝 🛋				
Console Root	Issued To 📩	Issued By	Expiration Date	Actions
△ 💭 Certificates (Local Computer)	azor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates
Personal Certificates	supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025	More Actions
Trusted Root Certification Autho		Open		WINLESSKEIOD617 razor local
▷ Enterprise Trust		All Task	s 🕨 Op	ben
Intermediate Certification Autho Trusted Publichers		Cut	Re	quest Certificate with New Key
Difference Publishers		Conv	Re	new Certificate with New Key
Third-Party Root Certification Au		Delete	ive	new certaincate with New Key
Trusted People		Delete	Ma	anage Private Keys
Client Authentication Issuers		Properti	es Ad	Ivanced Operations
Other People		Help	Exp	port
Remote Desktop				
Certificate Enrollment Requests Smart Card Trusted Roots				
Trusted Devices				
▷ I Web Hosting ✓				
< III >	< III		>	
Export a certificate				

• Exporte el certificado en el pfx formato de las secciones siguientes. Consulte este artículo sobre cómo exportar un certificado en el pfx formato de MMC:

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

Una vez que haya finalizado la exportación del certificado, navegue hasta Add/Remove Snap-in en MMC console. Haga clic Certificates y, a continuación, haga clic en Add.

Elija Service account y haga clic en Next.

•

•

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

En el Select Computer cuadro de diálogo, elija Local Computer y haga clic en Next.

Elija Active Directory Domain Services y haga clic en Finish.

•

•

•

•

Certificate	s snap-in 🛛 🗙
Select a service account to manage on the local co	mputer.
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 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

En el Add/Remove Snap-ins cuadro de diálogo, haga clic en OK.

Expanda Certificates - Services (Active Directory Domain Services) y, a continuación, haga clic en NTDS\Personal.

Haga clic con el botón secundario NTDS\Personal, haga clic en All Tasks y, a continuación, haga clic en Import.

•

•

•

•

Console1 - [Console Re	pot\Certificates - Service (Active Directory Domain Services) on Local Comput	er\NTDS\Personal]
🔚 File Action View Favorites Window	Help	_ 8 ×
🗢 🔿 🙇 🗊 📋 🔍 🖬		
Console Root	Object Type	Actions
Certificates (Local Computer)	Certificates	NTDS\Personal
NTOCO		More Actions
▶ 🖹 NT Find Certificates		
III Tasks	Find Certificates	
⊳ NT View	Import	
NT New Window from Here	Advanced Operations	
NT New Taskpad View		
NT Refresh		
Export List		
Help		
< III >		
Add a certificate to a store		

En la Certificate Import Wizard pantalla de bienvenida, haga clic en Next.

En la pantalla Archivo para importar, haga clic en Browse y localice el archivo de certificado que exportó anteriormente.

En la pantalla Abrir, asegúrese de que está seleccionado Intercambio de información personal (*pfx,*.p12) como tipo de archivo y, a continuación, desplácese por el sistema de archivos para localizar el certificado exportado anteriormente. A continuación, haga clic en ese certificado.

	Oper	י <u></u>			x
🔄 💿 🝷 🕇 📑 🕨 Libr	aries 🕨 Documents		♥ 🖒 Search D	ocuments	Q,
Organize 🔻 New folder				• == •	
🔆 Favorites	Name	Date modified	Туре	Size	
Desktop	🏂 Idapcert	4/25/2022 12:01	Personal Informati	5 KB	
Downloads Recent places					
演 Libraries					
Documents					
J Music					
Pictures					
H Videos					
🛒 Computer					
🙀 Network					
File nar	me: Idapcert		✓ Persona	I Information Excl	nange 🗸
			Ор	en Ca	incel

Haga clic Open y, a continuación, haga clic en Next.

•

•

•

En la pantalla Password (Contraseña), introduzca la contraseña establecida para el archivo y, a continuación, haga clic en Next.

En la página Almacén de certificados, asegúrese de que la opción Colocar todos los certificados está seleccionada y lea Almacén de certificados: NTDS\Personal y, a continuación, haga clic en Next.

€	Ø 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

En la pantallaCertificate Import Wizard de finalización, haga clic en Finish. A continuación, verá un mensaje que indica que la importación se ha realizado correctamente. Haga clic en OK. Se observa que el certificado se ha importado en el almacén de certificados: NTDS\Personal.

•

Console1 - [Console Root\Certific	ates - Service (Active Directory	Domain Services) on Local C	Computer\NTDS\Pe	ersonal\Certificates]	- 🗆 X
藩 File Action View Favorites Window	v Help				_ & ×
🗢 🏟 🖄 📰 🐇 🖬 🛸 🚺					
Console Root	Issued To	Issued By	Expiration Date	Actions	
Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates	
∠ Certificates - Service (Active Directory D	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
Initial Supersonal Certificates				more Actions	
NTDS\Trusted Root Certification Au				WIN-E3SKFJQD6J7.r	azor.local 🔺
NTDS\Enterprise Trust				More Actions	•
NTDS\Intermediate Certification Au					
NTDS\Trusted Publishers					
NTDS\Untrusted Certificates					
NIDS\Third-Party Root Certification					
NTDS\Client Authentication Issuers					
< III >	<		>		
NTDS\Personal store contains 2 certificates.					

Configuraciones de FMC

Verificar licencia

Para implementar la configuración de AnyConnect, el FTD debe estar registrado con el servidor de licencias inteligentes y se debe aplicar al dispositivo una licencia válida Plus, Apex o VPN Only.

Rango de configuración

•

Desplácese hasta System > Integration. Navegue hasta Realms y haga clic en Add Realm, como se muestra en esta imagen:

Overview Analysi	s Policies Devices Objects	AMP Intelligence							Po Deploy Sy	stem Help v	admin 🔻
				Configuration U	Users Domains	Integration	Updates	Licenses v Logg	ing • Health •	¹ Monitoring •	Tools •
	3					2					
Cloud Services	Realms Identity Sources	High Availability eStre	amer Host Input Client	Smart Software Manage	er On-Prem						
Realms Re	alm Sequences Sync Results										4
									Compa	re Realms Ad	d Realm
Name 👻	Description	Туре	Domain	AD Primary Domain		Base DN			State		

Rellene los campos mostrados en función de la información recopilada del servidor de Microsoft para LDAP. Antes de esto, importe el certificado de CA raíz que ha firmado el certificado de servicio LDAPs en el servidor de Windows bajo Objects > PKI > Trusted CAs > Add Trusted CA, ya que se hace referencia a este en Directory Server Configuration el rango del rango. Una vez hecho esto, haga clic en 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	
 WIN-E3SKFJQD6J7.razor.local:636 	
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	
 Choose an interface 	
Default: Management/Diagnostic Interface	\sim
Test	
Add another directory	

 $\mathbf{0} \times$

autenticación de AnyConnect, ya que las solicitudes de autenticación LDAP de AnyConnect se inician desde una de las interfaces enrutables del FTD.

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 Resolve via route lookup Choose an interface	ctory server i
Default: Management/Diag	gnostic Interface 🗸 🗸
Test 📀 Test connection s	succeeded
	Cancel OK

Habilite el nuevo rango.

•

									-			
Overview Analy:	sis Policies Devices Objects	AMP Intelligence							<u>ę</u> c	eploy Sys	stem Help *	admin v
				Configuration Users	Domains	Integration	Updates	Licenses *	Logging *	Health *	Monitoring •	Tools •
Cloud Services	Realms Identity Sources	High Availability eStream	er Host Input Client	Smart Software Manager Or	-Prem							
Realms F	Realm Sequences Sync Results											
		-								Compa	re Realms	id Realm
Name +	Description	Туре	Domain	AD Primary Domain		Base DN				State		
AC-Local		LOCAL	Global							C Enabl	ed 🗼	/ fa 🖥
LDAP		AD	Global	cisco01.com		OU=Users,O	U=CISCO,DC	C=cisco01,DC=c	om	C Enabl	ed 🛨	/ ¶ 🗑
LDAP-Server		AD	Global	razor.local		DC=razor,DC	=local			C Enabl	ed 🛨	/ fa 🗑

Configuración de AnyConnect para la gestión de contraseñas

•

•

Elija el perfil de conexión existente o cree uno nuevo, si es una configuración inicial de AnyConnect. Aquí, se utiliza un perfil de conexión existente denominado 'AnyConnect-AD' asignado con la autenticación local.

Overview Analysis Policies Devices Objects	AMP Intelligence			🆺 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN >	Remote Access 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	AAA		Group Policy	
DefaultWE8VPNGroup	Authentication: None Authorization: None Accounting: None		DftGrpPolicy	/ 8
AnyConnect	Authentication: Radius (RADIUS) Authorization: Radius (RADIUS) Accounting: None		DfttGrpPelicy	/ 6
AnyConnect-AD	Authentication: LOCAL Authorization: None Accounting: None		🗎 AnyConnect-Group	/ 5

Edite el perfil de conexión y asigne el nuevo servidor LDAPs configurado en los pasos anteriores, en la configuración AAA del perfil de conexión. Una vez hecho esto, haga clic Save en la esquina superior derecha.

Firepower Management Center Overview Devices / VPN / Edit Connection Profile	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🔞 admin 🔻
AnyConnect Enter Description		Save Cancel Policy Assianments (1)
Connection Profile Access Interfaces Advanced	Edit Connection Profile	Local Realm: None Dynamic Access Policy: Hostscan
	Group Policy:* AnyConnect-AD	+
Name	Client Address Assignment AAA Aliases	42
DerautwEBVPNGroup	Authentication	7
AnyConnect	Authentication Method: AAA Only Authentication Server: LDAP-Server (AD)	/1
AnyConnect-AD	Fallback to LOCAL Authentication	<i>∕</i> ≆
	Use secondary authentication Use secondary authentication Authorization	
	Authorization Server: Use same authentication server Authorization database Authorization database	
	Configure LDAP Attribute Map	
	Accounting Server: Advanced Settings	
	Strip Realm from username Cancel Save	

Active la gestión de contraseñas en la AAA > Advanced Settings y guarde la configuración.

Overview Analysis Policies Devices Objects AMP Intellig	nce	🎨 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN + Remote Access AnyConnect Frier Description	QoS Platform Settings FlexConfig Certificates	Save Cancel
		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 Edit Group Policy	0
DefaultWEBVPNGroup	Client Address Assignment AAA Aliases	/ 8
AnyConnect	LDAP-Server (AD)	/8
AnyConnect-AD	Use secondary authentication Authorization	Ø 8
sjobs	Authorization Server: Use same authentication server Authorization Server Authorization construction only if user exists in authorization database Configure LDAP Attribute Map	/ 8
	Accounting Accounting Server: Advanced Settings	
	Strip Realm from username Strip Realm from username Handle Reale Real Real Real Real Real Real R	
	Save Cancel	

Implementación

•

•

Overview Analysis Policies Devices Objects AMP Intelligence

•

Una vez finalizada la configuración, haga clic en elDeploy botón de la parte superior derecha.

Haga clic en la casilla de verificación junto a la configuración de FTD que se le ha aplicado y, a continuación, haga clic en Deploy, como se muestra en esta imagen:

P Deploy System Help v admin v

Overview	Analysis Polic	es Devices Obje	ects AMP In	ntelligence						P Deploy Sys	item Help v	admin 🔻
										Deploymen	t Deploym	nent History
1 device selected Deploy time: Estimate Depl									Deploy			
•	Device			Modified by	Inspect Interrup	tion Type	Group	Last Deploy Time	Preview	Status		
> 🛛	10.197.224.190	_FTD1		admin		FTD		May 30, 2022 7:34 AM	E.	Pending		

Configuración final

Esta es la configuración que se observa en la CLI de FTD después de la implementación correcta.

Configuración AAA

<#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

Configuración de AnyConnect

<#root>

> show running-config webvpn

webvpn

enable Outside

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

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

anyconnect enable

tunnel-group-list enable

cache

no disable

```
error-recovery disable
```

> show running-config tunnel-group

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

authentication-server-group LDAP-Server

default-group-policy AnyConnect-Group

password-management password-expire-in-days 1

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

> show running-config group-policy AnyConnect-Group

group-policy

<----- LDAPs Serve

<----- Password-management

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

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

<---- Protocol

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

Verificación

Conectar con AnyConnect y verificar el proceso de administración de contraseñas para la conexión de usuario

1. Inicie una conexión con el perfil de conexión correspondiente. Una vez que se determina en el inicio de sesión inicial que la contraseña debe cambiarse, ya que el servidor de Microsoft rechazó la contraseña anterior al expirar, se le pide al usuario que cambie la contraseña.

S Cisco AnyConnect FTD-Hostname	X Sico AnyConnect Secure Mobility Client – X
Group: Dev ~ Username: admin Password: [VPR Contacting FTD-Hosthame.
OK Cancel	

Cisco AnyConnect FTD-Hostname New Password: Verify Password: Password with a minimum length of 7 to continue. Continue Cancel Verify Cancel Verify Contacting FTD-Hostname. FTD-Hostname		
• •	-thethe CARGE	

Una vez que el usuario introduzca la nueva contraseña para el inicio de sesión, la conexión se establecerá correctamente.

🚳 Cisco AnyC	onnect Secure Mobility Client		-		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnec	t
00:02:43					IPv4
¢ (i)					dialia

Verifique la conexión del usuario en la CLI de FTD:

<#root>

•

•

FTD_2# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : admin : 7 Index <----- 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 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Encryption : 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 Security Grp : none Tunnel Zone : 0

Troubleshoot

Depuraciones

Esta depuración se puede ejecutar en la CLI de diagnóstico para resolver problemas relacionados con la administración de contraseñas: **debug ldap 255**.

Depuraciones de administración de contraseñas en funcionamiento

<#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

Errores comunes encontrados durante la administración de contraseñas

Normalmente, si la directiva de contraseñas establecida por el servidor de Microsoft no se cumple durante el tiempo que el usuario proporciona la nueva contraseña, la conexión finaliza con el error "La contraseña no cumple los requisitos de la directiva de contraseñas". Por lo tanto, asegúrese de que la nueva contraseña cumpla con la política establecida por el servidor de Microsoft para LDAP.

S Cisco AnyConnect FTD-Hostnam	e ×			
Cannot complete password cha password policy requirements. complexity, and password histo	nge because the password does not meet the Check the minimum password length, password ry requirements.			
Group: Dev	× 🚳	Cisco AnyConnect Secure Mobility Clien	t – 🗆 🗙	
Username: admin				
Password:		Cannot complete password ch	ange because the password	
	OK Cancel	does not meet the password p	volicy requirements. Check	
	0	¢ ()	alfaalfa CISCO	
	(Cisco AnyConnect	×	
		Cannot complete password char does not meet the password pol minimum password length, pass password history requirements.	nge because the password ligr requirements. Check the word complexity, and	
			ОК	

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).