

Configuración de Firepower Management Center y FTD con LDAP para autenticación externa

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Configurar](#)

[Configuración básica de LDAP en la GUI de FMC](#)

[Acceso al shell para usuarios externos](#)

[Autenticación externa a FTD](#)

[Funciones de usuario](#)

[SSL o TLS](#)

[Verificación](#)

[Base de búsqueda de pruebas](#)

[Probar integración LDAP](#)

[Troubleshoot](#)

[¿Cómo interactúan FMC/FTD y LDAP para descargar usuarios?](#)

[¿Cómo interactúan FMC/FTD y LDAP para autenticar una solicitud de inicio de sesión de un usuario?](#)

[SSL o TLS no funcionan como se esperaba](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo habilitar la autenticación externa del protocolo ligero de acceso a directorios (LDAP) de Microsoft con Cisco Firepower Management Center (FMC) y Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- FTD de Cisco
- Cisco FMC
- LDAP de Microsoft

Componentes Utilizados

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

- FTD 6.5.0-123
- FMC 6.5.0-115
- Microsoft Server 2012

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.

Antecedentes

El FMC y los dispositivos gestionados incluyen una cuenta de administración predeterminada para el acceso a la gestión. Puede agregar cuentas de usuario personalizadas en el FMC y en dispositivos administrados, ya sea como usuarios internos o, si se admite para su modelo, como usuarios externos en un servidor LDAP o RADIUS. La autenticación de usuario externo es compatible con FMC y FTD.

· Usuario interno: el dispositivo FMC/FTD comprueba una base de datos local para la autenticación del usuario.

· Usuario externo: Si el usuario no está presente en la base de datos local, la información del sistema de un servidor de autenticación LDAP o RADIUS externo rellena su base de datos de usuarios.

Diagrama de la red



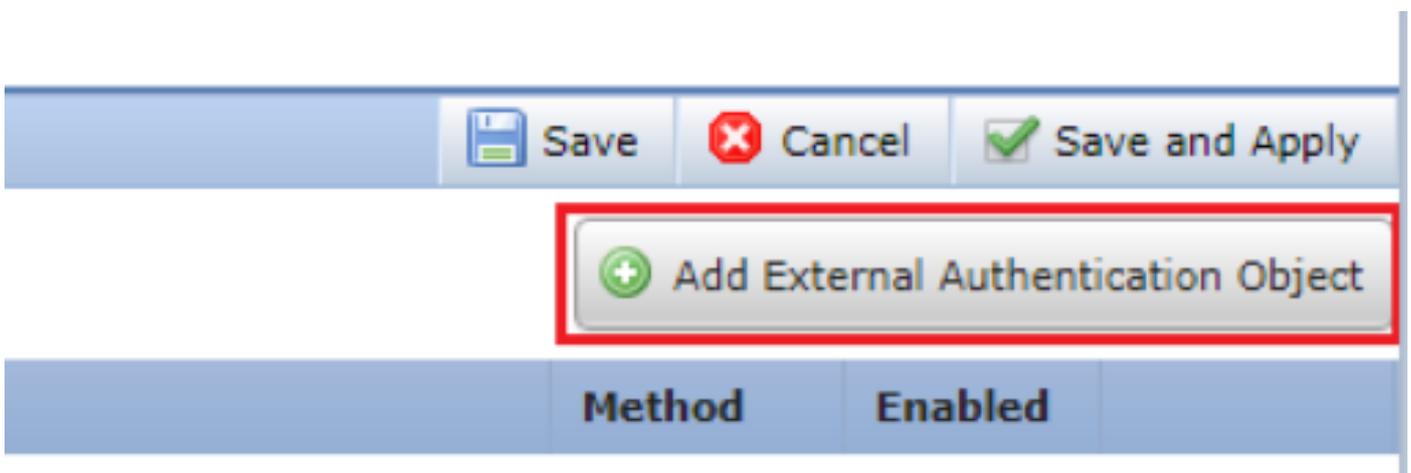
Configurar

Configuración básica de LDAP en la GUI de FMC

Paso 1. Desplácese hasta **System > Users > External Authentication**:



Paso 2. Elegir **Add External Authentication Object**:



Paso 3. Complete los campos obligatorios:

External Authentication Object

Authentication Method: **LDAP**

CAC: Use for CAC authentication and authorization

Name *: **Name the External Authentication Object**

Description:

Server Type: **Choose MS Active Directory and click 'Set Defaults'**

Primary Server

Host Name/IP Address *: ex. IP or hostname

Port *: **Default port is 389 or 636 for SSL**

Backup Server (Optional)

Host Name/IP Address: ex. IP or hostname

Port:

LDAP-Specific Parameters

Base DN *: ***Base DN specifies where users will be found**
ex. dc=sourcefire,dc=com

Base Filter:
ex. (cn=jsmith), (1cn=jsmith), (&(cn=jsmith){!(cn=bsmith)(cn=csmith*)})

User Name *: **Username of LDAP Server admin**
ex. cn=jsmith,dc=sourcefire,dc=com

Password *:

Confirm Password *:

Show Advanced Options:

Attribute Mapping

UI Access Attribute *: ***Default when 'Set Defaults' option is clicked**

Shell Access Attribute *:

Group Controlled Access Roles (Optional) ▾

Access Admin:

Administrator:

Discovery Admin:

External Database User:

Intrusion Admin:

Maintenance User:

Network Admin:

Security Analyst:

Security Analyst (Read Only):

Security Approver:

Threat Intelligence Director (TID) User:

View-Only-User (Read Only):

Default User Role: **To specify the default user role if user is not found in any group**

Group Member Attribute:

Group Member URL Attribute:

Shell Access Filter

Shell Access Filter ⓘ: Same as Base Filter ex. (cn=jsmith), (1cn=jsmith), (&(cn=jsmith){!(cn=bsmith)(cn=csmith*)})

(Mandatory for FTD devices):

Additional Test Parameters

User Name:

Password:

*Required Field

Paso 4. Habilite el External Authentication Objeto y guardar:



Acceso al shell para usuarios externos

El FMC admite dos usuarios de administración interna diferentes: uno para la interfaz web y otro con acceso CLI. Esto significa que existe una clara distinción entre los usuarios que pueden acceder a la GUI y los que también pueden acceder a la CLI. En el momento de la instalación, la contraseña para el usuario admin predeterminado se sincroniza para que sea la misma en la GUI y la CLI, sin embargo, son rastreados por diferentes mecanismos internos, y eventualmente pueden ser diferentes.

Los usuarios externos de LDAP también deben tener acceso al shell.

Paso 1. Desplácese hasta `System > Users > External Authentication` y haga clic en `Shell Authentication` como se ve en la imagen y guardar:



Paso 2. Implementar cambios en FMC.

Una vez configurado el acceso al shell para usuarios externos, se habilita el inicio de sesión a través de SSH como se ve en la imagen:

```
192.0.2.6 - PuTTY
login as: h.potter
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

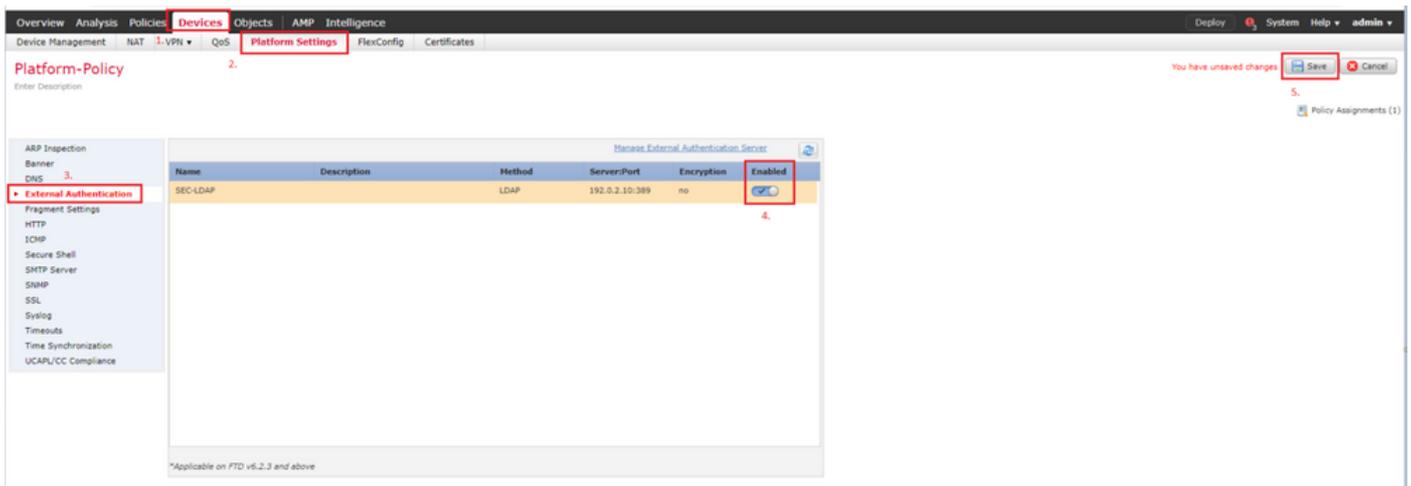
Cisco Fire Linux OS v6.4.0 (build 2)
Cisco Firepower Threat Defense for VMWare v6.4.0 (build 102)

>
```

Autenticación externa a FTD

La autenticación externa se puede habilitar en FTD.

Paso 1. Desplácese hasta **Devices > Platform Settings > External Authentication**. Haga clic en **Enabled** y guarde:



Funciones de usuario

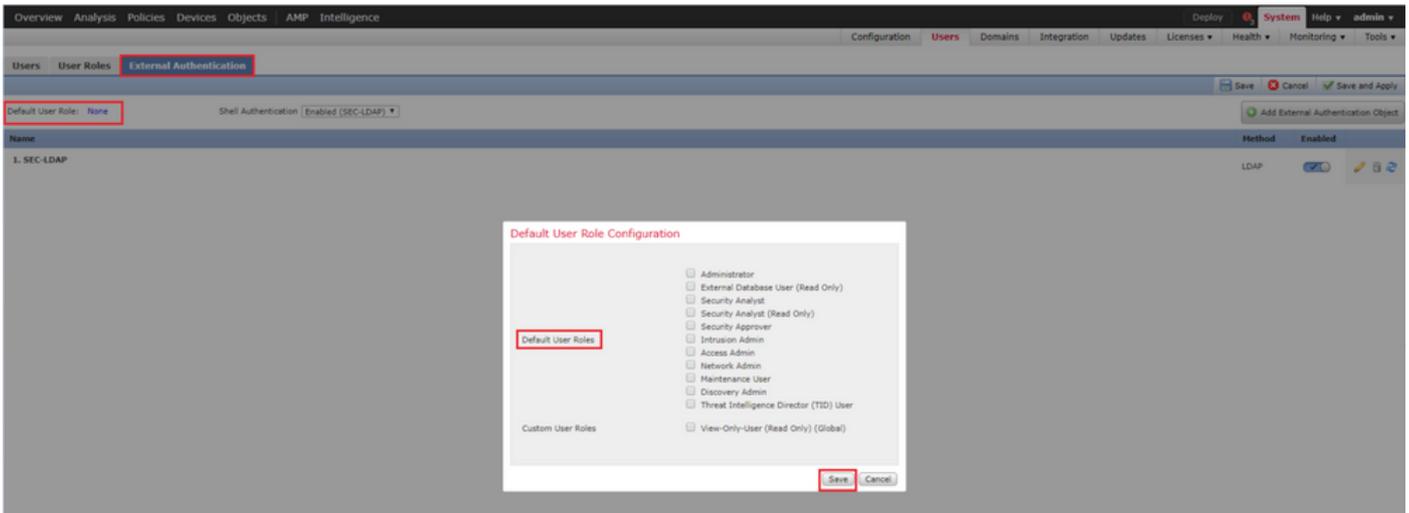
Los privilegios de usuario se basan en la función de usuario asignada. También puede crear roles de usuario personalizados con privilegios de acceso adaptados a las necesidades de su organización o puede utilizar roles predefinidos como Analista de seguridad y Administrador de descubrimiento.

Existen dos tipos de funciones de usuario:

1. Funciones de usuario de interfaz web
2. Funciones de usuario de CLI

Para obtener una lista completa de funciones predefinidas y más información, consulte; [Funciones de usuario](#).

Para configurar un rol de usuario predeterminado para todos los objetos de autenticación externa, navegue hasta System > Users > External Authentication > Default User Role. Elija la función de usuario predeterminada que desee asignar y haga clic en Save.



Para elegir una función de usuario predeterminada o asignar funciones específicas a usuarios específicos de un grupo de objetos determinado, puede elegir el objeto y desplazarse a Group Controlled Access Roles como se ve en la imagen:

Group Controlled Access Roles (Optional) ▾

Access Admin	<input type="text"/>
Administrator	<input type="text" value="h.potter@SEC-LAB"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text" value="s.rogers@SEC-LAB"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text"/>
Network Admin	<input type="text" value="h.simpson@SEC-LAB"/>
Security Analyst	<input type="text" value="r.weasley@SEC-LAB"/>
Security Analyst (Read Only)	<input type="text"/>
Security Approver	<input type="text"/>
Threat Intelligence Director (TID) User	<input type="text"/>
View-Only-User (Read Only)	<input type="text" value="ma.simpson@SEC-LAB"/>

Default User Role

Access Admin
Administrator
 Discovery Admin
 External Database User

SSL o TLS

DNS debe configurarse en el FMC. Esto se debe a que el valor de Asunto del Certificado debe coincidir con el Authentication Object Primary Server Hostname. Una vez configurado el LDAP seguro, las capturas de paquetes ya no muestran solicitudes de enlace de texto sin cifrar.

SSL cambia el puerto predeterminado a 636 y TLS lo mantiene como 389.

 Nota: el cifrado de TLS requiere un certificado en todas las plataformas. Para SSL, el FTD también requiere un certificado. Para otras plataformas, SSL no requiere un certificado. Sin embargo, se recomienda que siempre cargue un certificado para SSL para evitar ataques de intrusos.

Paso 1. Desplácese hasta `Devices > Platform Settings > External Authentication > External Authentication Object` e introduzca la información SSL/TLS de Opciones avanzadas:

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

Show Advanced Options ▼

Encryption SSL TLS None

SSL Certificate Upload Path No file chosen ex. PEM Format (base64 encoded version of DER)

User Name Template ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

Paso 2. Cargue el certificado de la CA que firmó el certificado del servidor. El certificado debe estar en formato PEM.

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

Show Advanced Options ▼

Encryption SSL TLS None

SSL Certificate Upload Path CA-Cert-base64.cer ex. PEM Format (base64 encoded version of DER)

Certificate has been loaded (Select to clear loaded certificate)

User Name Template ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

Paso 3. Guarde la configuración.

Verificación

Base de búsqueda de pruebas

Abra un símbolo del sistema de Windows o PowerShell donde LDAP esté configurado y escriba el comando: `dsquery user -name`

.

Por ejemplo:

```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> dsquery user -name harr*
"CN=Harry Potter,CN=Users,DC=SEC-LAB
PS C:\Users\Administrator>
PS C:\Users\Administrator> dsquery user -name *
"CN=Administrator,CN=Users,DC=SEC-LAB
"CN=Guest,CN=Users,DC=SEC-LAB
"CN=krbtgt,CN=Users,DC=SEC-LAB
"CN=Anthony E. Stark,CN=Users,DC=SEC-LAB
"CN=Bart Simpson,CN=Users,DC=SEC-LAB
"CN=Dr. Robert B. Banner,CN=Users,DC=SEC-LAB
"CN=Ginny Weasley,CN=Users,DC=SEC-LAB
"CN=Harry Potter,CN=Users,DC=SEC-LAB
"CN=Hermione Granger,CN=Users,DC=SEC-LAB
"CN=Homer Simpson,CN=Users,DC=SEC-LAB
"CN=Lisa Simpson,CN=Users,DC=SEC-LAB
"CN=Maggie Simpson,CN=Users,DC=SEC-LAB
"CN=Marge Simpson,CN=Users,DC=SEC-LAB
"CN=Matthew Murdock,CN=Users,DC=SEC-LAB
"CN=Neville Longbottom,CN=Users,DC=SEC-LAB
"CN=Peter B. Parker,CN=Users,DC=SEC-LAB
"CN=Ron Weasley,CN=Users,DC=SEC-LAB
"CN=Steven Rogers,CN=Users,DC=SEC-LAB
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

Probar integración LDAP

Desplácese hasta `System > Users > External Authentication > External Authentication Object`. En la parte inferior de la página, hay un `Additional Test Parameters` como se ve en la imagen:

Additional Test Parameters

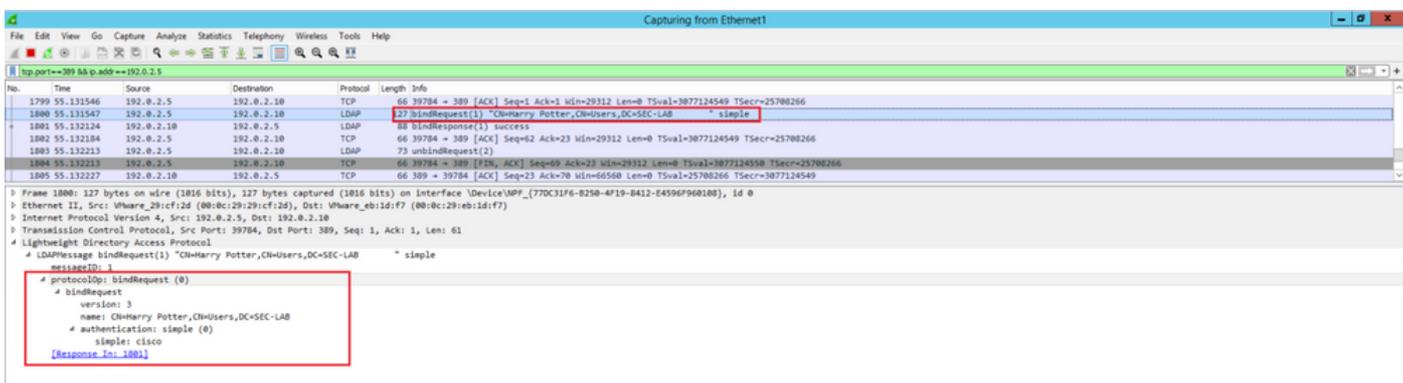
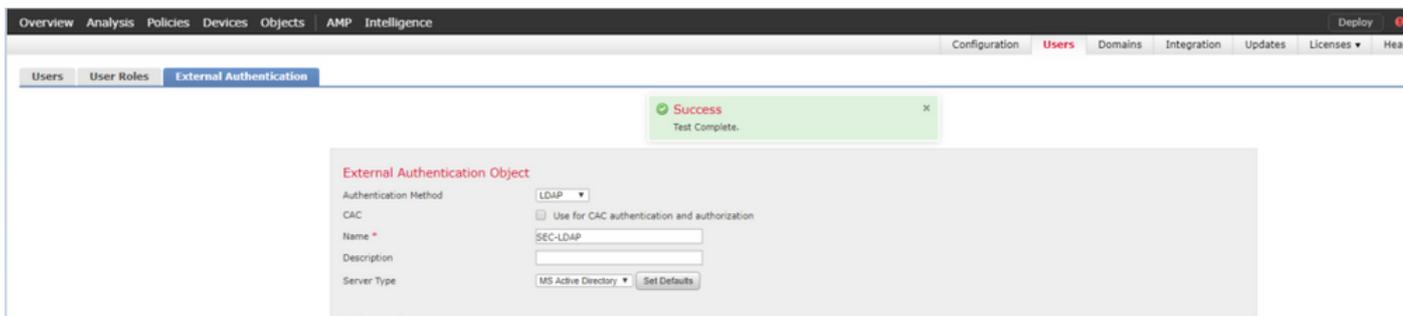
User Name:

Password:

*Required Field

Save Test Cancel

Elija el Test para ver los resultados.



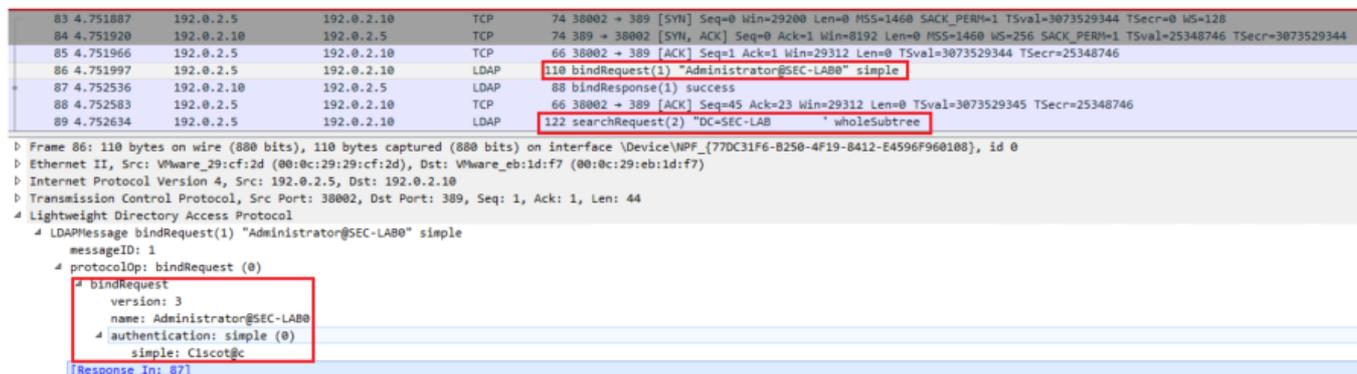
Troubleshoot

¿Cómo interactúan FMC/FTD y LDAP para descargar usuarios?

Para que FMC pueda extraer usuarios de un servidor LDAP de Microsoft, primero debe enviar una solicitud de enlace en el puerto 389 o 636 (SSL) con las credenciales de administrador LDAP. Una vez que el servidor LDAP es capaz de autenticar FMC, responde con un mensaje de éxito. Por último, el CSP puede realizar una solicitud con el mensaje de solicitud de búsqueda que se describe en el diagrama:

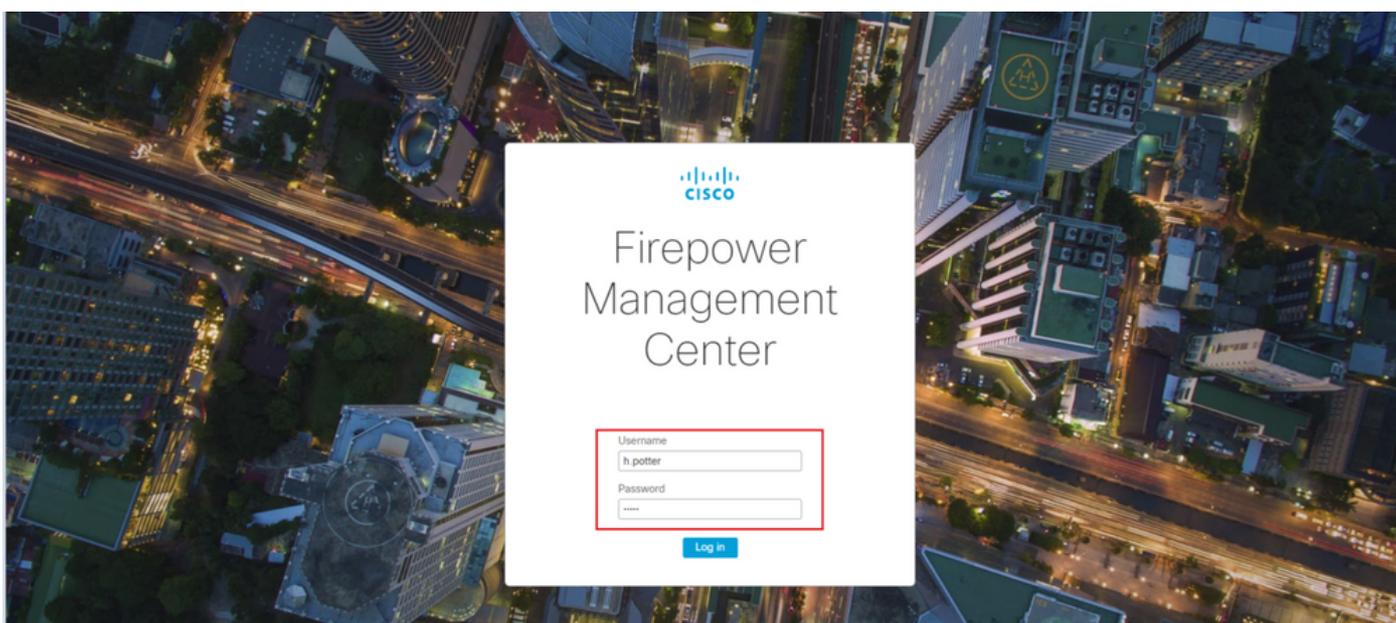
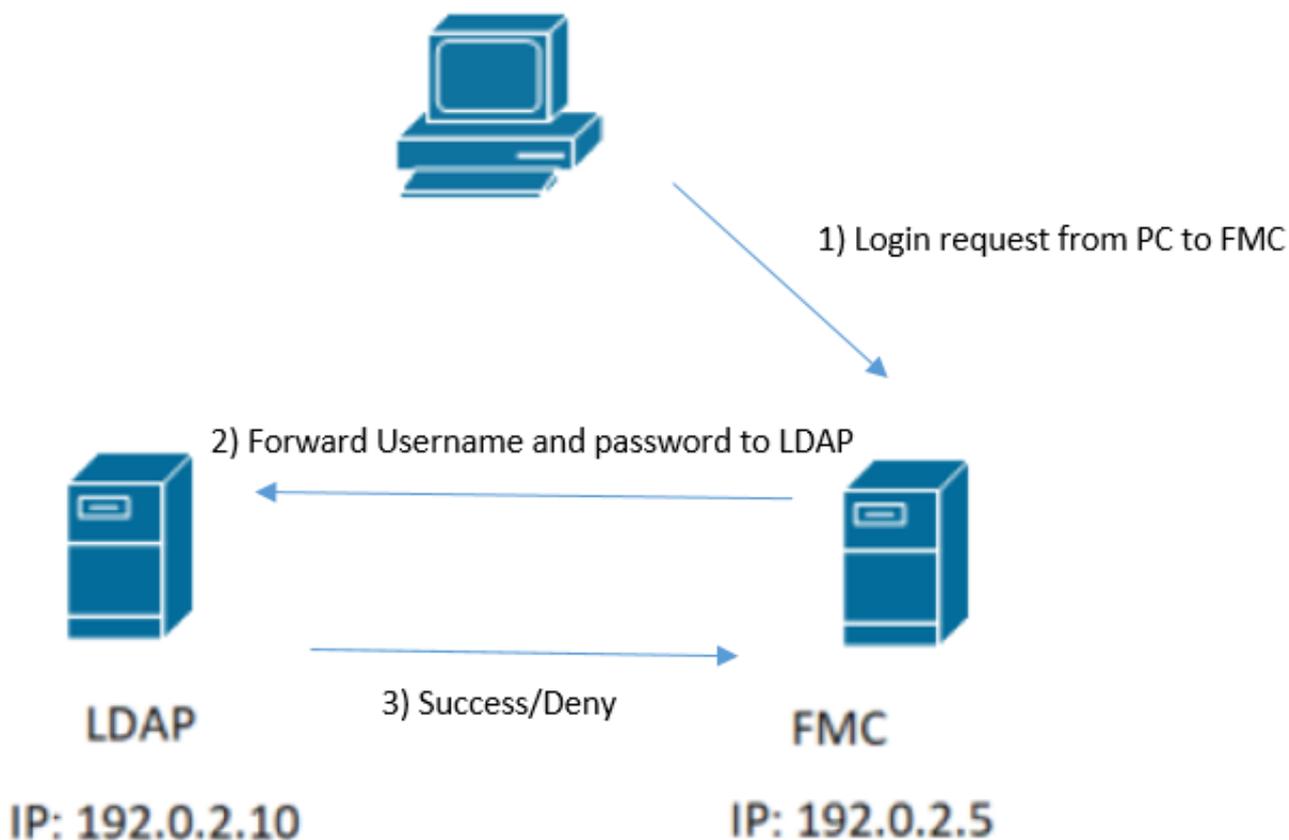
<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << ---
 FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

Observe que la autenticación envía contraseñas en el modo claro de forma predeterminada:



¿Cómo interactúan FMC/FTD y LDAP para autenticar una solicitud de inicio de sesión de un usuario?

Para que un usuario pueda iniciar sesión en FMC o FTD mientras esté habilitada la autenticación LDAP, la solicitud de inicio de sesión inicial se envía a Firepower; sin embargo, el nombre de usuario y la contraseña se reenvían a LDAP para obtener una respuesta de denegación/éxito. Esto significa que el FMC y el FTD no mantienen la información de contraseña localmente en la base de datos y, en su lugar, esperan la confirmación de LDAP sobre cómo proceder.



No.	Time	Source	Destination	Protocol	Length	Info
58	13:11:59.695671	192.0.2.5	192.0.2.10	LDAP	110	bindRequest(1) "Administrator@SEC-LAB0" simple
59	13:11:59.697473	192.0.2.10	192.0.2.5	LDAP	88	bindResponse(1) success
67	13:11:59.697773	192.0.2.5	192.0.2.10	LDAP	110	bindRequest(1) "Administrator@SEC-LAB0" simple
69	13:11:59.699474	192.0.2.10	192.0.2.5	LDAP	88	bindResponse(1) success
97	13:11:59.729988	192.0.2.5	192.0.2.10	LDAP	127	bindRequest(1) "CN=Harry Potter,CN=Users,DC=SEC-LAB" simple
98	13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	88	bindResponse(1) success

Si se aceptan el nombre de usuario y la contraseña, se agrega una entrada en la GUI web como se ve en la imagen:

Username	Roles	Authentication Method	Password Lifetime
admin	Administrator	Internal	Unlimited
h.potter	Administrator	External	

Ejecute el comando show user en FMC CLISH para verificar la información del usuario: > show user

El comando muestra información de configuración detallada para los usuarios especificados. Se muestran estos valores:

Login: el nombre de inicio de sesión

UID: el ID de usuario numérico

Autenticación (local o remota): cómo se autentica al usuario

Acceso (básico o de configuración): el nivel de privilegio del usuario

Habilitado (habilitado o deshabilitado): indica si el usuario está activo.

Restablecer (Sí o No): indica si el usuario debe cambiar la contraseña la próxima vez que inicie sesión.

Exp (Nunca o un número): el número de días hasta que se debe cambiar la contraseña del usuario

Advertencia (N/D o número): el número de días que se concede a un usuario para cambiar su contraseña antes de que caduque

Str (Sí o No): si la contraseña del usuario debe cumplir los criterios para comprobar la seguridad

Bloquear (Sí o No): indica si la cuenta del usuario se ha bloqueado debido a demasiados errores de inicio de sesión.

Max (N/D o un número): el número máximo de inicios de sesión fallidos antes de que se bloquee la cuenta del usuario

SSL o TLS no funcionan como se esperaba

Si no habilita DNS en los FTD, puede ver errores en el registro de conexiones que sugieren que LDAP es inalcanzable:

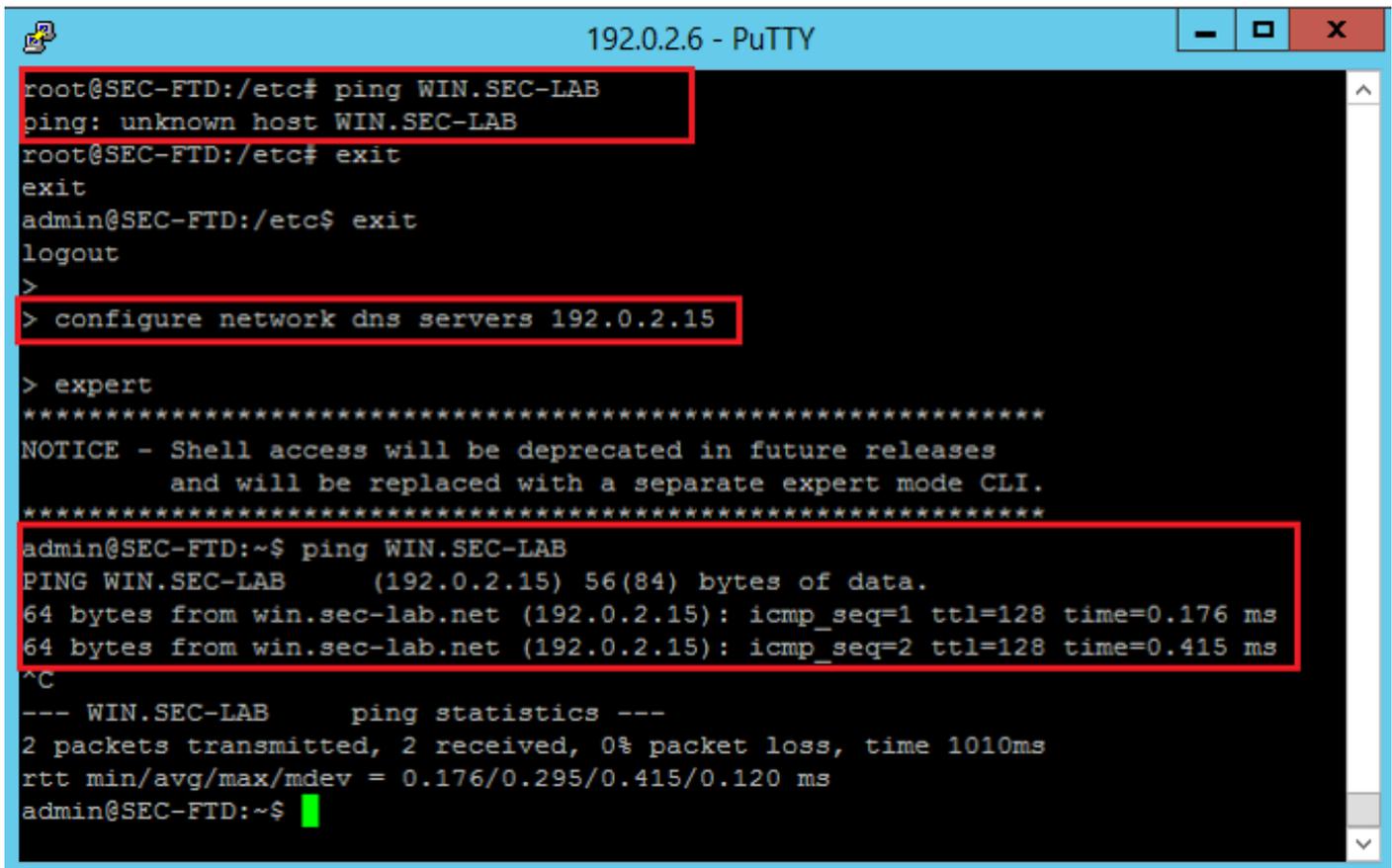
```
root@SEC-FMC:/$ sudo cd /var/common
```

```
root@SEC-FMC:/var/common$ sudo pigtail
```

```
MSGs: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e
MSGs: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 61
```

Asegúrese de que Firepower puede resolver el FQDN de servidores LDAP. Si no es así, agregue el DNS correcto tal como se ve en la imagen.

FTD: Acceda a FTD CLISH y ejecute el comando: > configure network dns servers



FMC: Elegir System > Configuration, a continuación, seleccione Interfaces de gestión como se muestra en la imagen:

- Access List
- Access Control Preferences
- Audit Log
- Audit Log Certificate
- Change Reconciliation
- DNS Cache
- Dashboard
- Database
- Email Notification
- External Database Access
- HTTPS Certificate
- Information
- Intrusion Policy Preferences
- Language
- Login Banner
- Management Interfaces**
- Network Analysis Policy Preferences
- Process
- REST API Preferences
- Remote Storage Device
- SNMP
- Shell Timeout
- Time
- Time Synchronization
- UCAPL/CC Compliance
- User Configuration
- VMware Tools
- Vulnerability Mapping
- Web Analytics

Interfaces

Link	Name	Channels	MAC Address	IP Address	
	eth0	Management Traffic Event Traffic	00:0C:29:29:CF:2D	192.0.2.5	

Routes

IPv4 Routes

Destination	Netmask	Interface	Gateway	
*			192.0.2.1	

IPv6 Routes

Destination	Prefix Length	Interface	Gateway	
-------------	---------------	-----------	---------	--

Shared Settings

Hostname: SEC-FMC

Domains:

Primary DNS Server: 192.0.2.10

Secondary DNS Server:

Tertiary DNS Server:

Remote Management Port: 8305

ICMPv6

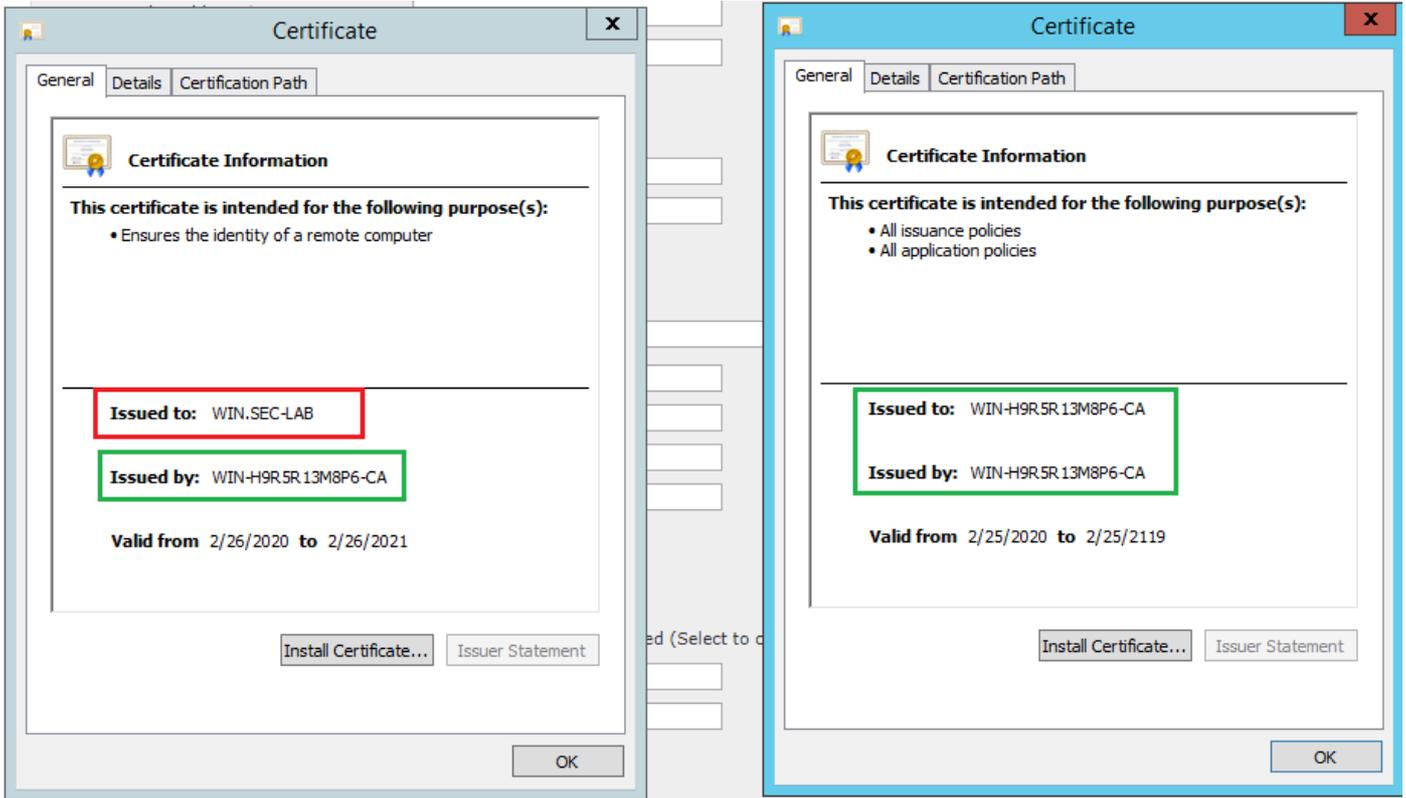
Allow Sending Echo Reply Packets:

Allow Sending Destination Unreachable Packets:

Proxy

Enabled:

Asegúrese de que el certificado cargado en FMC es el certificado de la CA que firmó el certificado de servidor de LDAP, como se muestra en la imagen:



Utilice capturas de paquetes para confirmar que el servidor LDAP envía la información correcta:

The image displays two screenshots related to LDAP authentication configuration and verification.

Left Screenshot (Wireshark): Shows a network capture on interface *Ethernet0. The capture filter is `ldap || !ip.addr == 192.0.2.5`. The packet list shows a TLSv1.2 1515 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done. The packet details for frame 33 show the Certificate field with the attribute `id-at-commonName=WIN.SEC-LAB` highlighted in red.

Right Screenshot (Cisco Firepower Management Center): Shows the configuration for an External Authentication Object. The Authentication Method is set to LDAP. The Primary Server details are highlighted in red, showing Host Name/IP Address as WIN.SEC-LAB and Port as 389.

Información Relacionada

- [Cuentas de usuario para acceso a la gestión](#)

- [Vulnerabilidad de omisión de autenticación del protocolo ligero de acceso a directorios de Cisco Firepower Management Center](#)
- [Configuración del objeto de autenticación LDAP en el sistema FireSIGHT](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

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).