

Configurer FMC et FTD avec LDAP pour l'authentification externe

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurer](#)

[Configuration LDAP de base dans l'interface utilisateur FMC](#)

[Accès Shell pour les utilisateurs externes](#)

[Authentification externe vers FTD](#)

[Rôles utilisateur](#)

[SSL ou TLS](#)

[Vérifier](#)

[Base de recherche de test](#)

[Tester l'intégration LDAP](#)

[Dépannage](#)

[Comment FMC/FTD et LDAP interagissent-ils pour télécharger des utilisateurs ?](#)

[Comment FMC/FTD et LDAP interagissent-ils pour authentifier une demande de connexion utilisateur ?](#)

[SSL ou TLS ne fonctionne pas comme prévu](#)

[Informations connexes](#)

Introduction

Ce document décrit comment activer l'authentification externe LDAP (Microsoft Lightweight Directory Access Protocol) avec Cisco FMC et FTD.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Threat Defense (FTD)
- Cisco Firepower Management Center (FMC)
- LDAP Microsoft

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

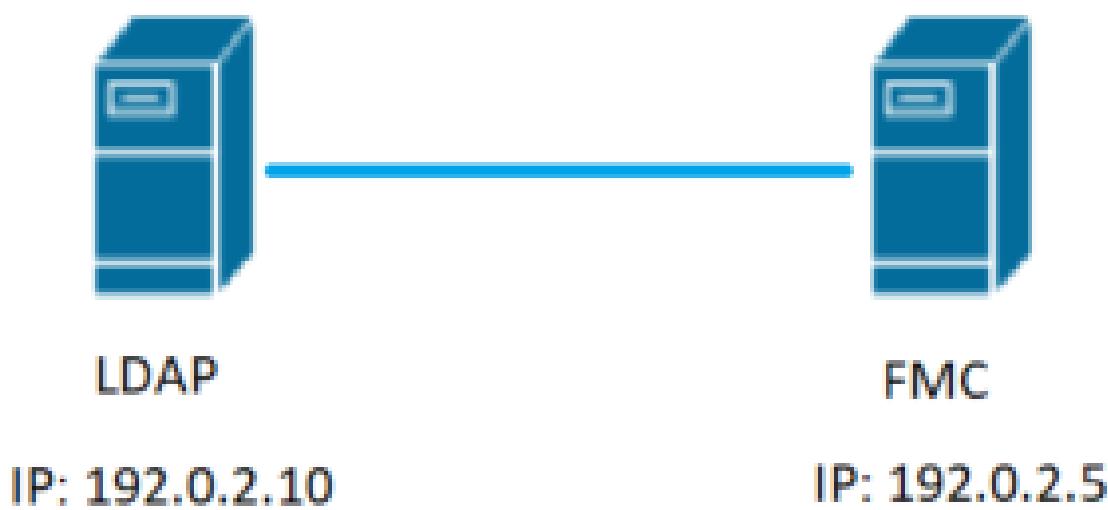
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le FMC et les périphériques gérés incluent un compte d'administrateur par défaut pour l'accès à la gestion. Vous pouvez ajouter des comptes d'utilisateurs personnalisés sur le FMC et sur les périphériques gérés, soit en tant qu'utilisateurs internes, soit, s'ils sont pris en charge pour votre modèle, en tant qu'utilisateurs externes sur un serveur LDAP ou RADIUS. L'authentification utilisateur externe est prise en charge pour FMC et FTD.

- Utilisateur interne : le périphérique FMC/FTD vérifie l'authentification des utilisateurs dans une base de données locale.
- Utilisateur externe : si l'utilisateur n'est pas présent dans la base de données locale, les informations système d'un serveur d'authentification LDAP ou RADIUS externe renseignent sa base de données utilisateur.

Diagramme du réseau



Configurer

Configuration LDAP de base dans l'interface utilisateur FMC

Étape 1. Accédez à System > Users > External Authentication:

The screenshot shows the FMC web interface. At the top, there is a navigation bar with links for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. On the right side of the navigation bar, there are buttons for Deploy, Systems (which is highlighted with a red box), Help, and admin. Below the navigation bar, there is a secondary menu with tabs: Configuration, Users (which is highlighted with a red box), Domains, Integration, Updates, Licenses, Health, Monitoring, and Tools. The main content area has a title "External Authentication". Underneath the title, there are sections for "Default User Role" (set to None) and "Shell Authentication" (set to Disabled). At the bottom of the page, there are buttons for Save, Cancel, and Save and Apply, along with a link to "Add External Authentication Object". A red box highlights the "External Authentication" tab in the secondary menu.

Étape 2. Choisissez Add External Authentication Object.

The screenshot shows a dialog box titled "Add External Authentication Object". The dialog has three buttons at the top: "Save" (blue), "Cancel" (red), and "Save and Apply" (green). Below the buttons, there is a large input field containing the text "Add External Authentication Object", which is also highlighted with a red box. At the bottom of the dialog, there are two buttons: "Method" (blue) and "Enabled" (blue).

Étape 3. Renseignez les champs obligatoires :

External Authentication Object

Authentication Method: **LDAP**

CAC: Use for CAC authentication and authorization

Name *: **SEC-LDAP**

Description:

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

Primary Server

Host Name/IP Address *: **192.0.2.10** ex. IP or hostname

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

Backup Server (Optional)

Host Name/IP Address: ex. IP or hostname

Port: **389**

LDAP-Specific Parameters

*Base DN specifies where users will be found: **DC=SEC-LAB**

Base Filter:

User Name *: **Administrator@SEC-LABO** **Username of LDAP Server admin**

Password *: *********

Confirm Password *: *********

Show Advanced Options:

Attribute Mapping

UI Access Attribute *: **sAMAccountName**

Shell Access Attribute *: **sAMAccountName**

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: **Administrator** To specify the default user role if user is not found in any group

Group Member Attribute: **member**

Group Member URL Attribute:

Shell Access Filter

Shell Access Filter Same as Base Filter (Mandatory for FTD devices) ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(!(cn=bsmith)(cn=csmith*)))

Additional Test Parameters

User Name:

Password:

*Required Field

Étape 4. Activation de l'External Authentication Objet et enregistrement :



Accès Shell pour les utilisateurs externes

Le FMC prend en charge deux utilisateurs d'administration interne différents : un pour l'interface Web et un autre avec un accès CLI. Cela signifie qu'il existe une distinction claire entre les utilisateurs autorisés à accéder à l'interface utilisateur graphique et ceux autorisés à accéder à l'interface de ligne de commande. Au moment de l'installation, le mot de passe de l'utilisateur admin par défaut est synchronisé afin d'être le même sur l'interface graphique et l'interface de ligne de commande, cependant, ils sont suivis par différents mécanismes internes, et peuvent éventuellement être différents.

Les utilisateurs externes LDAP doivent également disposer d'un accès shell.

Étape 1. Naviguez jusqu'à **System > Users > External Authentication** et cliquez sur la zone de **Shell Authentication** liste déroulante comme on le voit dans l'image et enregistrez :



Étape 2 : déploiement des modifications dans FMC

Une fois que l'accès shell pour les utilisateurs externes est configuré, la connexion via SSH est activée comme indiqué dans l'image :

```

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)

> 

```

Authentification externe vers FTD

L'authentification externe peut être activée sur FTD.

Étape 1. Accédez à Devices > Platform Settings > External Authentication. Cliquez sur Enabled et enregistrez :

Name	Description	Method	Server:Port	Encryption	Enabled
SEC-LDAP		LDAP	192.0.2.10:389	no	<input checked="" type="checkbox"/>

Rôles utilisateur

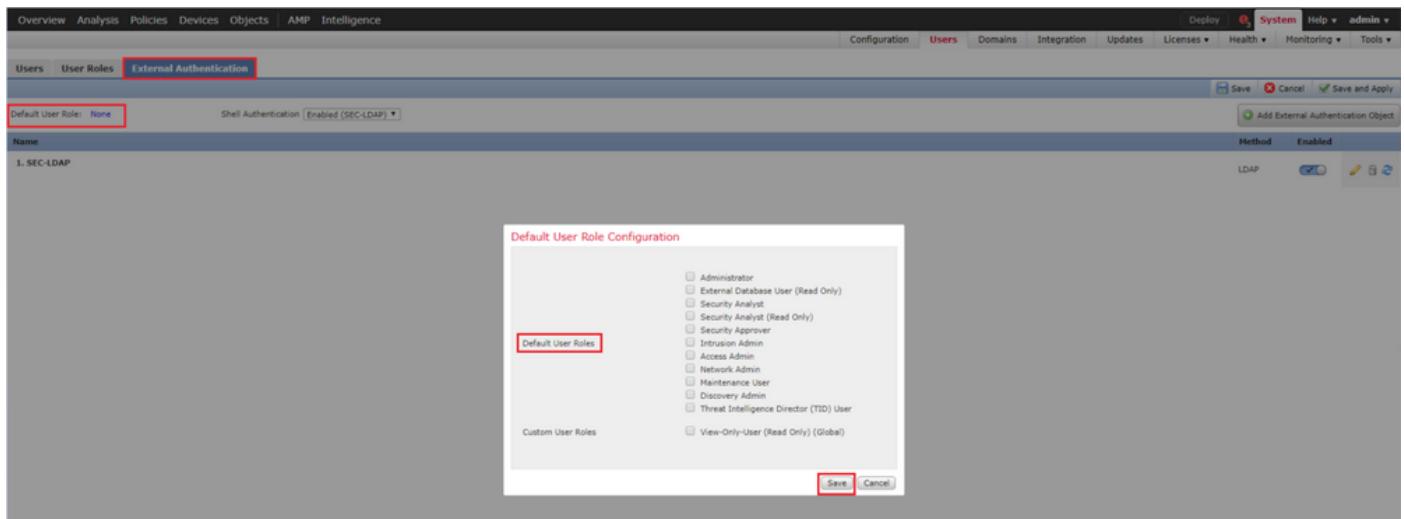
Les privilèges utilisateur sont basés sur le rôle utilisateur attribué. Vous pouvez également créer des rôles d'utilisateur personnalisés avec des privilèges d'accès adaptés aux besoins de votre organisation ou utiliser des rôles prédéfinis tels que Analyste de sécurité et Administrateur de découverte.

Il existe deux types de rôles d'utilisateur :

1. Rôles utilisateur de l'interface Web
2. Rôles utilisateur CLI

Pour obtenir la liste complète des rôles prédefinis et plus d'informations, reportez-vous à : [Rôles d'utilisateur](#).

Afin de configurer un rôle d'utilisateur par défaut pour tous les objets d'authentification externes, accédez à System > Users > External Authentication > Default User Role. Choisissez le rôle d'utilisateur par défaut que vous souhaitez affecter et cliquez sur Save.



Afin de choisir un rôle d'utilisateur par défaut ou d'attribuer des rôles spécifiques à des utilisateurs spécifiques dans un groupe d'objets particulier, vous pouvez choisir l'objet et naviguer jusqu'à Group Controlled Access Roles comme indiqué dans l'image :

Group Controlled Access Roles (Optional) ▾

Access Admin	
Administrator	h.potter@SEC-LAB
Discovery Admin	
External Database User	s.rogers@SEC-LAB
Intrusion Admin	
Maintenance User	
Network Admin	h.simpson@SEC-LAB
Security Analyst	r.weasley@SEC-LAB
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	
View-Only-User (Read Only)	m.a.simpson@SEC-LAB
Default User Role	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Access Admin Administrator Discovery Admin External Database User </div>

SSL ou TLS

DNS doit être configuré dans le FMC. En effet, la valeur Objet du certificat doit correspondre à la Authentication Object Primary Server Hostname. Une fois le protocole LDAP sécurisé configuré, les captures de paquets n'affichent plus les requêtes de liaison en texte clair.

SSL change le port par défaut en 636 et TLS le garde en 389.



Remarque : Le chiffrement TLS nécessite un certificat sur toutes les plates-formes. Pour SSL, le FTD nécessite également un certificat. Pour les autres plates-formes, SSL ne nécessite pas de certificat. Cependant, il est recommandé de toujours télécharger un certificat pour SSL afin d'empêcher les attaques de l'homme du milieu.

Étape 1. Accédez à Devices > Platform Settings > External Authentication > External Authentication Object Options avancées et saisissez les informations SSL/TLS :

LDAP-Specific Parameters

Base DN *	DC=SEC-LAB	Fetch DNS	ex. dc=sourcefire,dc=com
Base Filter			ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB		ex. cn=jsmith,dc=sourcefire,dc=com
Password *	*****		
Confirm Password *	*****		
Show Advanced Options	<input type="button" value="▼"/>		
Encryption	<input type="radio"/> SSL <input checked="" type="radio"/> TLS <input type="radio"/> None		
SSL Certificate Upload Path	<input type="button" value="Choose File"/> CA-Cert-base64.cer	No file chosen	ex. PEM Format (base64 encoded version of DER)
User Name Template	%\$		ex. cn=%\$s,dc=sourcefire,dc=com
Timeout (Seconds)	30		

Étape 2. Téléchargez le certificat de l'autorité de certification qui a signé le certificat du serveur. Le certificat doit être au format PEM.

LDAP-Specific Parameters

Base DN *	DC=SEC-LAB	Fetch DNS	ex. dc=sourcefire,dc=com
Base Filter			ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB		ex. cn=jsmith,dc=sourcefire,dc=com
Password *	*****		
Confirm Password *	*****		
Show Advanced Options	<input type="button" value="▼"/>		
Encryption	<input type="radio"/> SSL <input checked="" type="radio"/> TLS <input type="radio"/> None		
SSL Certificate Upload Path	<input type="button" value="Choose File"/> CA-Cert-base64.cer	Certificate has been loaded (Select to clear loaded certificate)	ex. PEM Format (base64 encoded version of DER)
User Name Template	%\$		ex. cn=%\$s,dc=sourcefire,dc=com
Timeout (Seconds)	30		

Étape 3 : enregistrement de la configuration

Vérifier

Base de recherche de test

Ouvrez une invite de commandes Windows ou PowerShell où LDAP est configuré et tapez la commande :dsquery user -name

Exemple :

```
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 harry*
"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>
```

Tester l'intégration LDAP

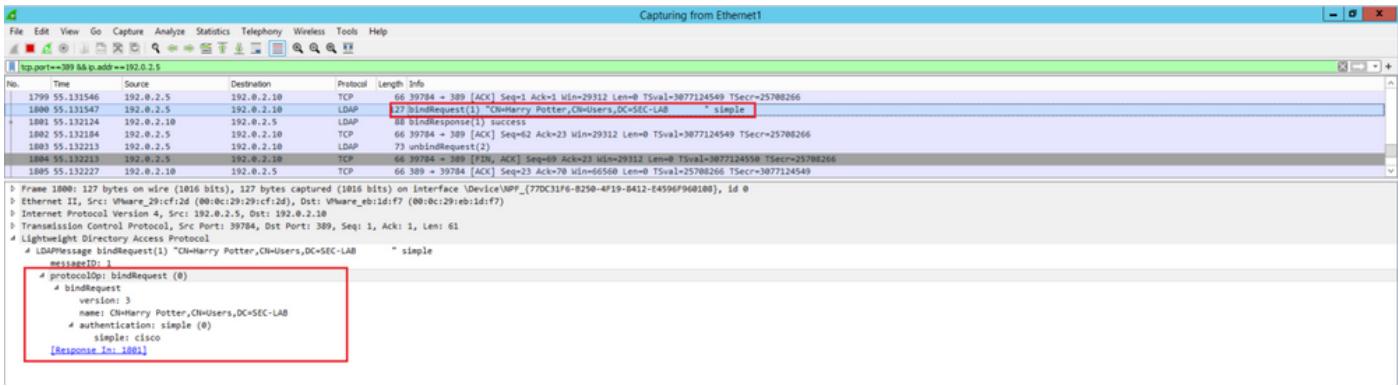
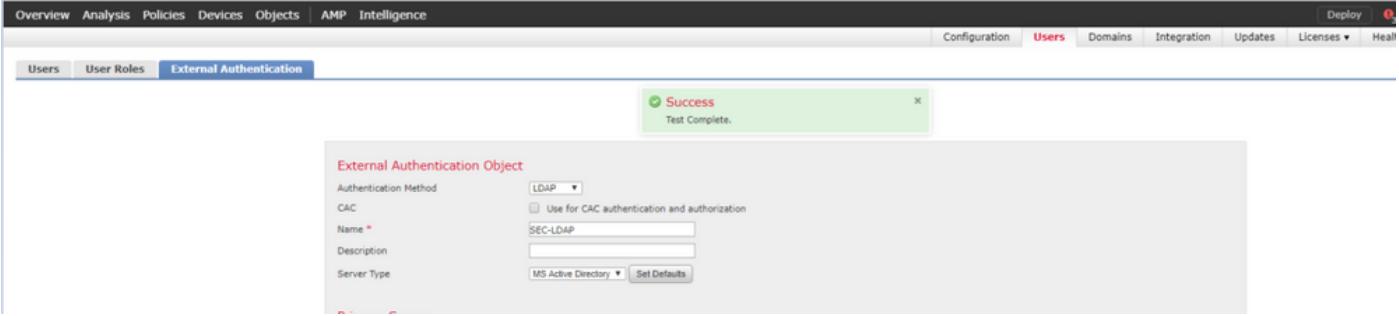
Accédez à System > Users > External Authentication > External Authentication Object. Au bas de la page, il y a une Additional Test Parameters section telle qu'elle apparaît dans l'image :

Additional Test Parameters

User Name	<input type="text" value="h.potter"/>
Password	<input type="password" value="*****"/>

*Required Field

Choisissez Test afin de voir les résultats.



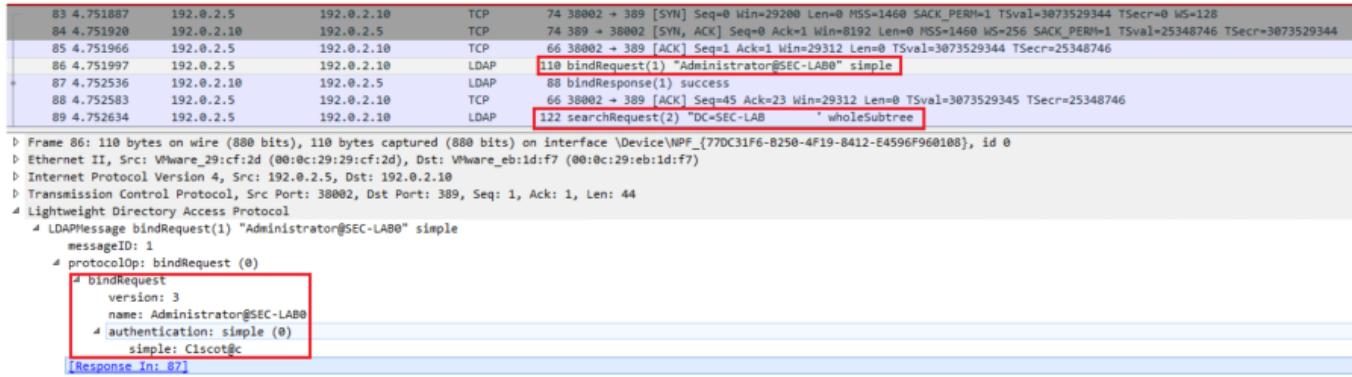
Dépannage

Comment FMC/FTD et LDAP interagissent-ils pour télécharger des utilisateurs ?

Pour que FMC puisse extraire des utilisateurs d'un serveur Microsoft LDAP, il doit d'abord envoyer une demande de liaison sur le port 389 ou 636 (SSL) avec les informations d'identification de l'administrateur LDAP. Une fois que le serveur LDAP est en mesure d'authentifier FMC, il répond avec un message de réussite. Enfin, FMC peut effectuer une requête avec le message de requête de recherche comme décrit dans le schéma :

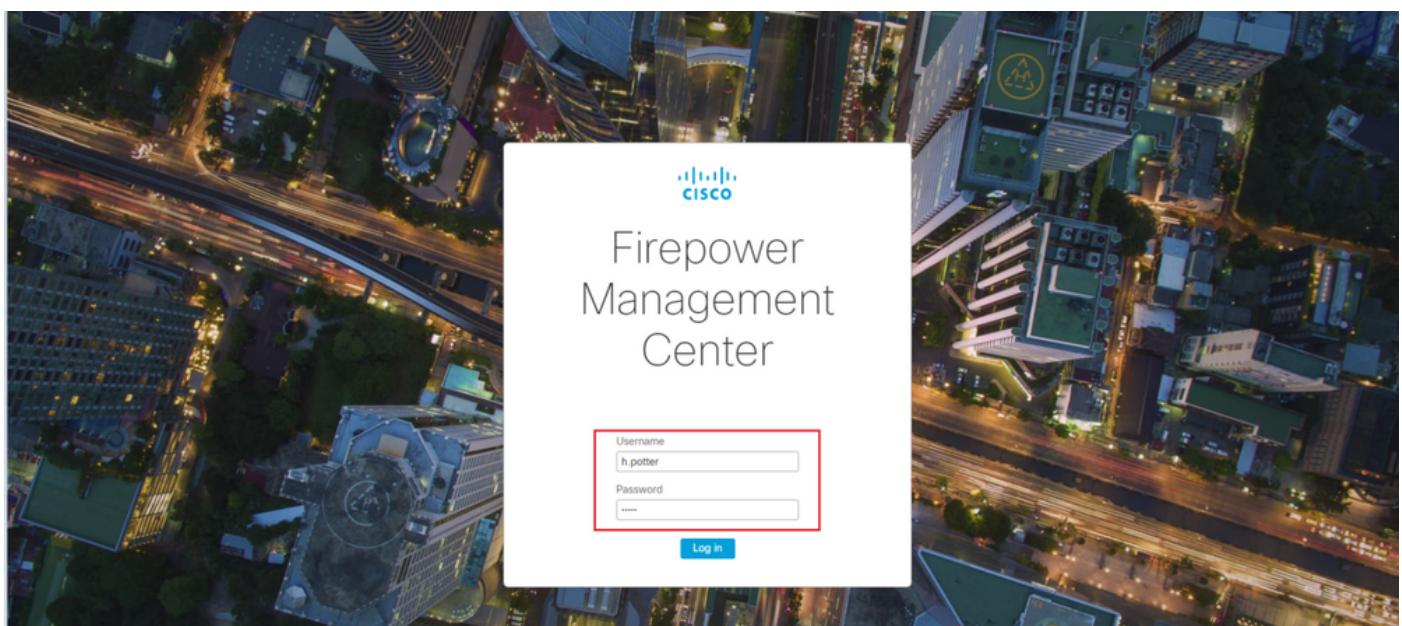
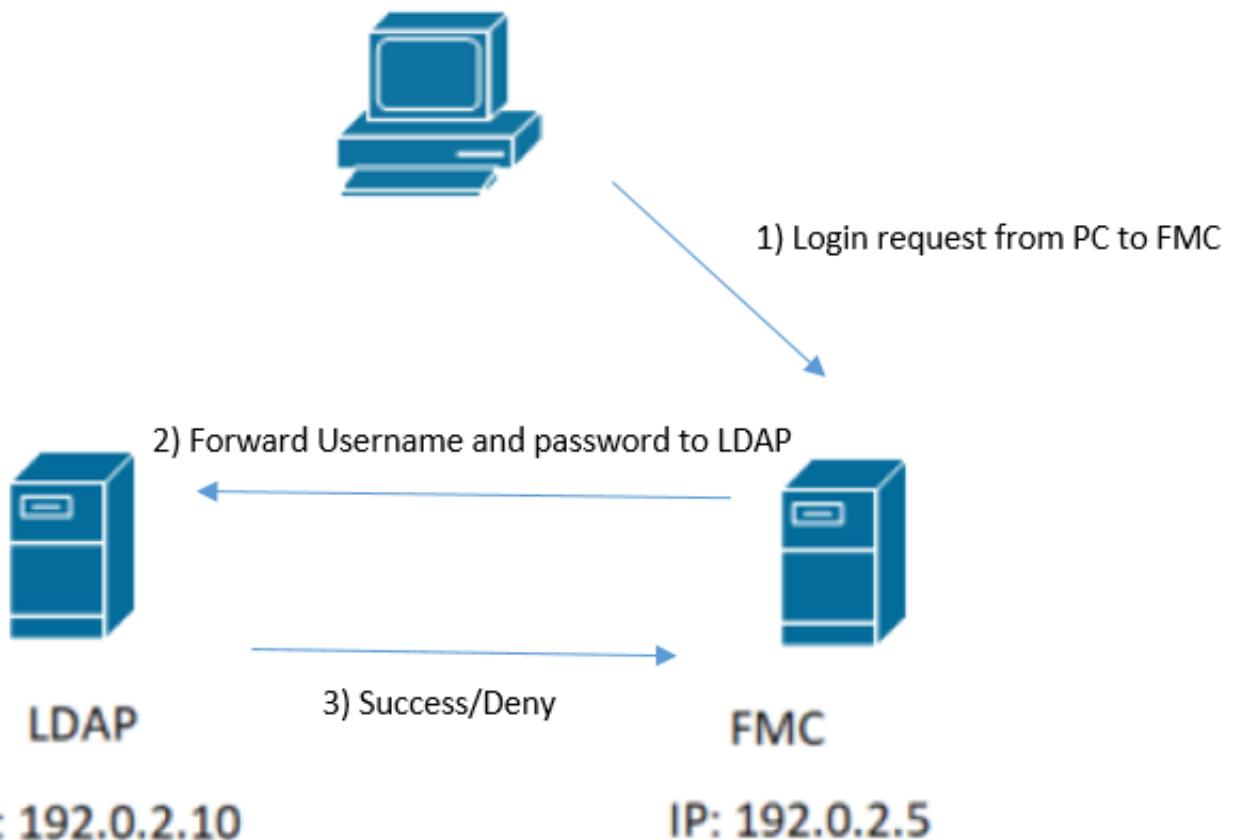
<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << ---
FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

Notez que l'authentification envoie des mots de passe en clair par défaut :



Comment FMC/FTD et LDAP interagissent-ils pour authentifier une demande de connexion utilisateur ?

Pour qu'un utilisateur puisse se connecter à FMC ou FTD alors que l'authentification LDAP est activée, la demande de connexion initiale est envoyée à Firepower, mais le nom d'utilisateur et le mot de passe sont transférés à LDAP pour une réponse de réussite/refus. Cela signifie que FMC et FTD ne conservent pas les informations de mot de passe localement dans la base de données et attendent plutôt la confirmation de LDAP sur la façon de procéder.



tcp.port==389 && ip.addr == 192.0.2.5 && ldap.messageID == 1						
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 le nom d'utilisateur et le mot de passe sont acceptés, une entrée est ajoutée dans l'interface utilisateur graphique Web, comme indiqué dans l'image :

The screenshot shows the FortiWeb interface under the 'Users' tab. A new user entry for 'h.potter' has been added, highlighted with a red box. The 'Authentication Method' field for this user is set to 'External', also highlighted with a red box. Other users listed are 'admin' (Internal) and another user whose name is partially visible.

Exécutez la commande show user in FMC CLISH afin de vérifier les informations utilisateur : > show user

La commande affiche des informations de configuration détaillées pour le ou les utilisateurs spécifiés. Ces valeurs s'affichent :

Log in : nom de connexion

UID : l'ID utilisateur numérique

Auth (local ou distant) : mode d'authentification de l'utilisateur

Access (Basic ou Config) : niveau de privilège de l'utilisateur

Enabled (Enabled ou Disabled) : indique si l'utilisateur est actif

Reset (Yes ou No) : indique si l'utilisateur doit modifier le mot de passe lors de la prochaine connexion

Exp (Never ou a number) : nombre de jours avant la modification du mot de passe de l'utilisateur

Warn (N/A ou un nombre) : nombre de jours qu'un utilisateur reçoit pour modifier son mot de passe avant qu'il expire

Str (Yes or No) : indique si le mot de passe de l'utilisateur doit répondre aux critères de vérification de la puissance

Lock (Yes ou No) : indique si le compte de l'utilisateur a été verrouillé en raison d'un trop grand nombre d'échecs de connexion

Max (N/A ou un nombre) : nombre maximal d'échecs de connexion avant le verrouillage du compte de l'utilisateur

SSL ou TLS ne fonctionne pas comme prévu

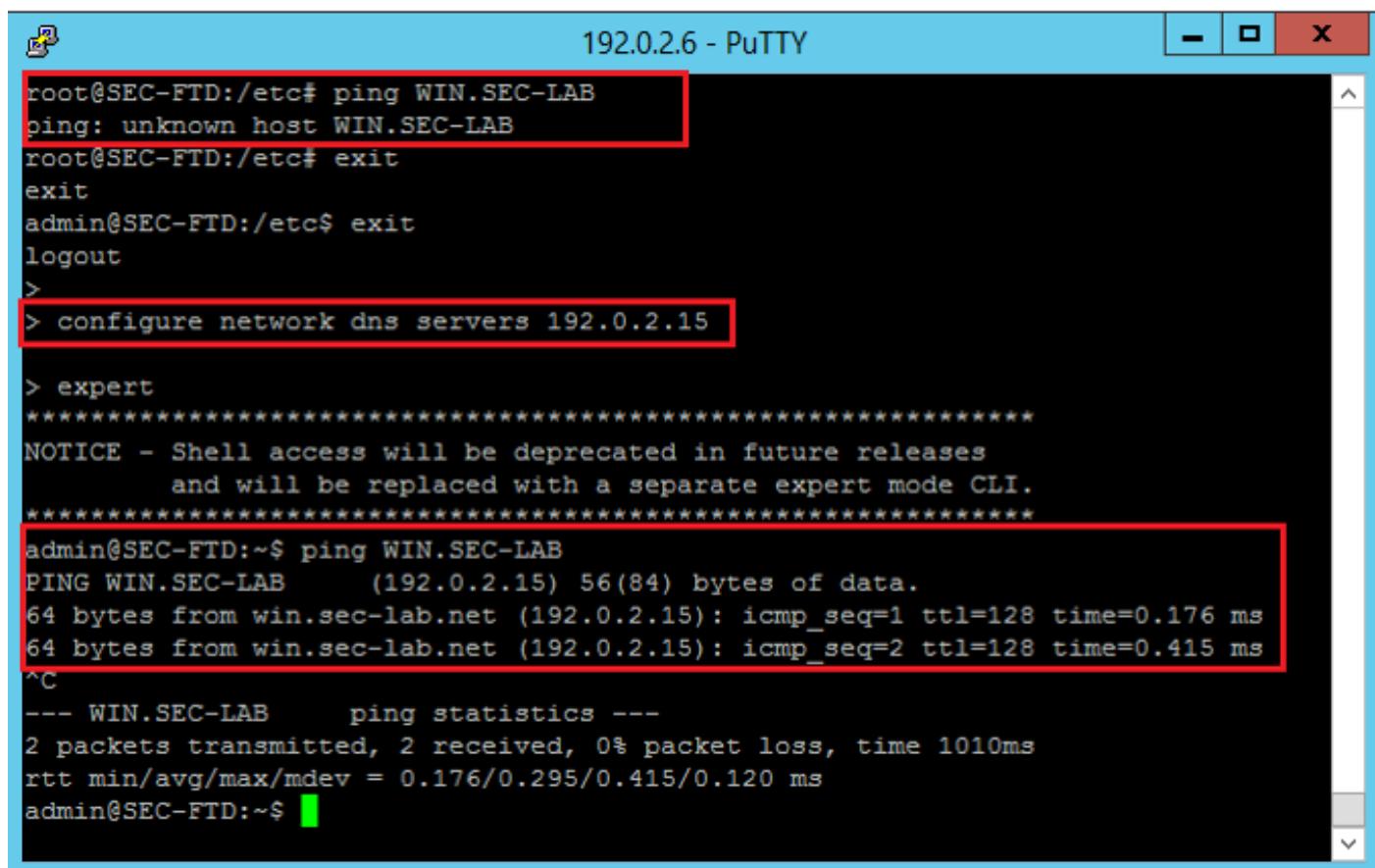
Si vous n'activez pas DNS sur les FTD, vous pouvez voir des erreurs dans le journal en queue de file qui suggèrent que LDAP est inaccessible :

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

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

Assurez-vous que Firepower est en mesure de résoudre le nom de domaine complet (FQDN) des serveurs LDAP. Si ce n'est pas le cas, ajoutez le DNS correct tel qu'il apparaît dans l'image.

DFT : Accédez à FTD CLISH et exécutez la commande suivante : > configure network dns servers



```
192.0.2.6 - PuTTY  
root@SEC-FTD:/etc# ping WIN.SEC-LAB  
ping: unknown host WIN.SEC-LAB  
root@SEC-FTD:/etc# exit  
exit  
admin@SEC-FTD:/etc$ exit  
logout  
>  
> configure network dns servers 192.0.2.15  
  
> expert  
*****  
NOTICE - Shell access will be deprecated in future releases  
and will be replaced with a separate expert mode CLI.  
*****  
admin@SEC-FTD:~$ ping WIN.SEC-LAB  
PING WIN.SEC-LAB (192.0.2.15) 56(84) bytes of data.  
64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=1 ttl=128 time=0.176 ms  
64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=2 ttl=128 time=0.415 ms  
^C  
--- WIN.SEC-LAB ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1010ms  
rtt min/avg/max/mdev = 0.176/0.295/0.415/0.120 ms  
admin@SEC-FTD:~$
```

FMC : Sélectionnez System > Configuration, puis Interfaces de gestion comme indiqué dans l'image :

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
VHware 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	<input type="text" value="SEC-FMC"/>
Domains	<input type="text"/>
Primary DNS Server	<input type="text" value="192.0.2.10"/>
Secondary DNS Server	<input type="text"/>
Tertiary DNS Server	<input type="text"/>
Remote Management Port	<input type="text" value="8305"/>

► ICMPv6

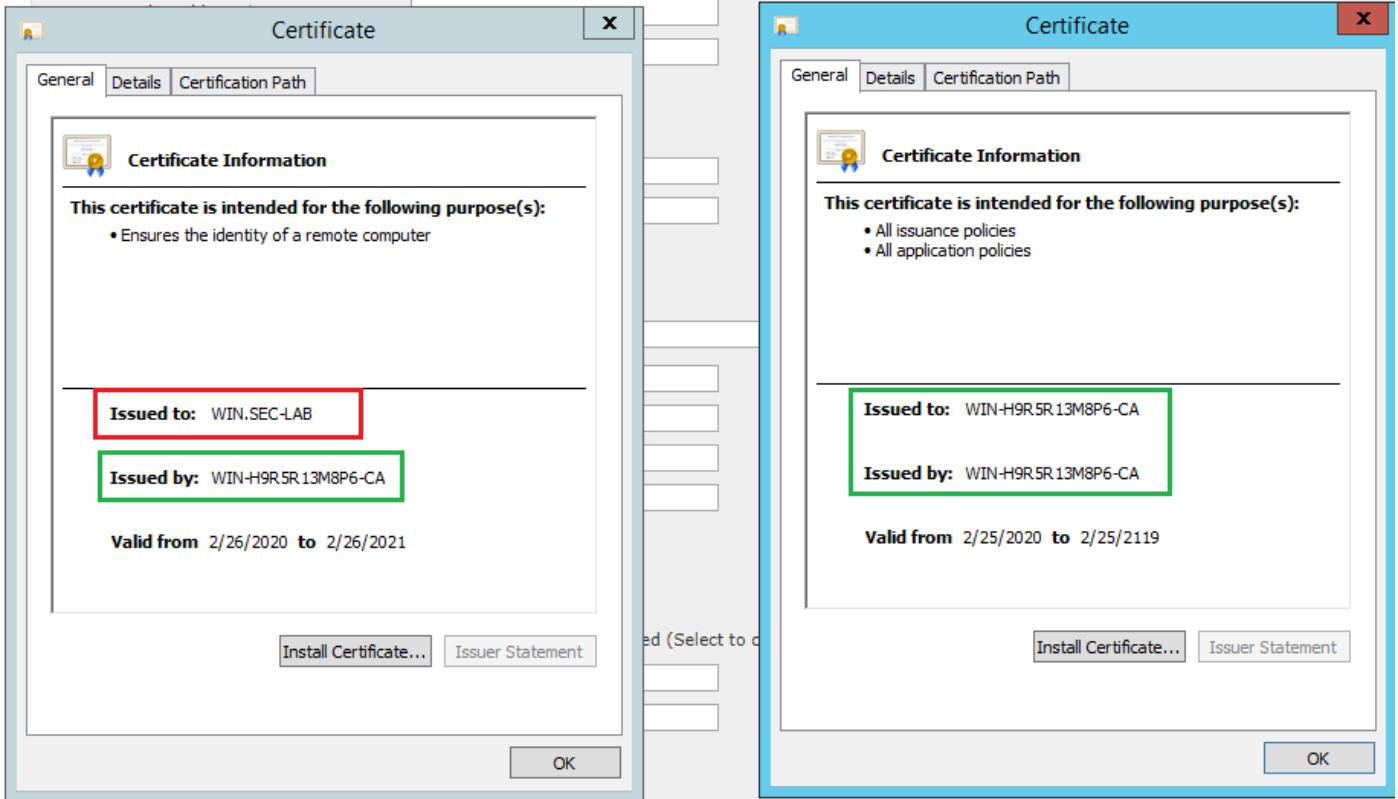
Allow Sending Echo Reply Packets	<input checked="" type="checkbox"/>
Allow Sending Destination Unreachable Packets	<input checked="" type="checkbox"/>

► Proxy

Enabled	<input type="checkbox"/>
---------	--------------------------

Save **Cancel**

Assurez-vous que le certificat téléchargé vers FMC est le certificat de l'autorité de certification qui a signé le certificat de serveur du LDAP, comme illustré dans l'image :



Utilisez les captures de paquets afin de confirmer que le serveur LDAP envoie les informations correctes :

*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Idap || tls && ip.addr == 192.0.2.5

No.	Time	Source	Destination	Protocol	Length	Info
3	0.143722	192.0.2.5	192.0.2.15	TLSv1.2	107	Application Data
4	0.143905	192.0.2.15	192.0.2.5	TLSv1.2	123	Application Data
22	2.720710	192.0.2.15	192.0.2.5	TLSv1.2	1211	Application Data
29	3.056497	192.0.2.5	192.0.2.15	LDAP	97	extendedReq(1) LDAP_START_TLS_OID
30	3.056605	192.0.2.15	192.0.2.5	LDAP	112	extendedResp(1) LDAP_START_TLS_OID
32	3.056921	192.0.2.5	192.0.2.15	TLSv1.2	313	Client Hello
33	3.057324	192.0.2.15	192.0.2.5	TLSv1.2	1515	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
35	3.060532	192.0.2.5	192.0.2.15	TLSv1.2	260	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
36	3.061678	192.0.2.15	192.0.2.5	TLSv1.2	173	Change Cipher Spec, Encrypted Handshake Message

```

Frame 33: 1515 bytes on wire (12120 bits), 1515 bytes captured (12120 bits) on interface \Device\NPF_{3EAD5E9F-B6CB-4E84-A462-217C1A10A8FE}, id 0
Ethernet II, Src: VMware_69:c8:c6 (00:0c:29:69:c8:c6), Dst: VMware_29:cf:2d (00:0c:29:29:cf:2d)
Internet Protocol Version 4, Src: 192.0.2.15, Dst: 192.0.2.5
Transmission Control Protocol, Src Port: 389, Dst Port: 52304, Seq: 47, Ack: 279, Len: 1449
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1444
  Handshake Protocol: Server Hello
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1124
    Certificates Length: 1121
    Certificates (1121 bytes)
      Certificate Length: 1118
      Certificate: 3082045a30620342a0030201020213320000000456c380c...
        signedCertificate
        algorithmIdentifier (sha256WithRSAEncryption)
        Padding: 0
        encrypted: 3645eb1128788982e7a5178f36022fa303e77bad1043bdd...
  Handshake Protocol: Server Key Exchange
  Handshake Protocol: Certificate Request
  Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0

```

Cisco Firepower Management Center

Overview Analysis Policies Devices Objects AMP Intelligence Configuration Users Domains Integration

Users User Roles External Authentication

External Authentication Object

Authentication Method: LDAP

CAC: Use for CAC authentication and authorization

Name: SEC-LDAP

Description:

Server Type: MS Active Directory

Primary Server

Host Name/IP Address: WIN.SEC-LAB

Port: 389

Informations connexes

- [Comptes d'utilisateurs pour accès à la gestion](#)
- [Vulnérabilité de contournement de l'authentification par protocole d'accès annuaire léger de Cisco Firepower Management Center](#)
- [Configuration de l'objet d'authentification LDAP sur le système FireSIGHT](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.