

使用LDAP配置Firepower管理中心和FTD以進行外部身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[FMC GUI中的基本LDAP配置](#)

[外部使用者的外殼訪問](#)

[FTD的外部驗證](#)

[使用者角色](#)

[SSL或TLS](#)

[驗證](#)

[測試搜尋庫](#)

[測試LDAP整合](#)

[疑難排解](#)

[FMC/FTD和LDAP如何進行互動以下載使用者？](#)

[FMC/FTD和LDAP如何互動以驗證使用者登入請求？](#)

[SSL或TLS未按預期工作](#)

[相關資訊](#)

簡介

本檔案介紹如何使用Cisco Firepower管理中心(FMC)和Firepower威脅防禦(FTD)啟用Microsoft輕型目錄訪問協定(LDAP)外部身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco FTD
- Cisco FMC
- Microsoft LDAP

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

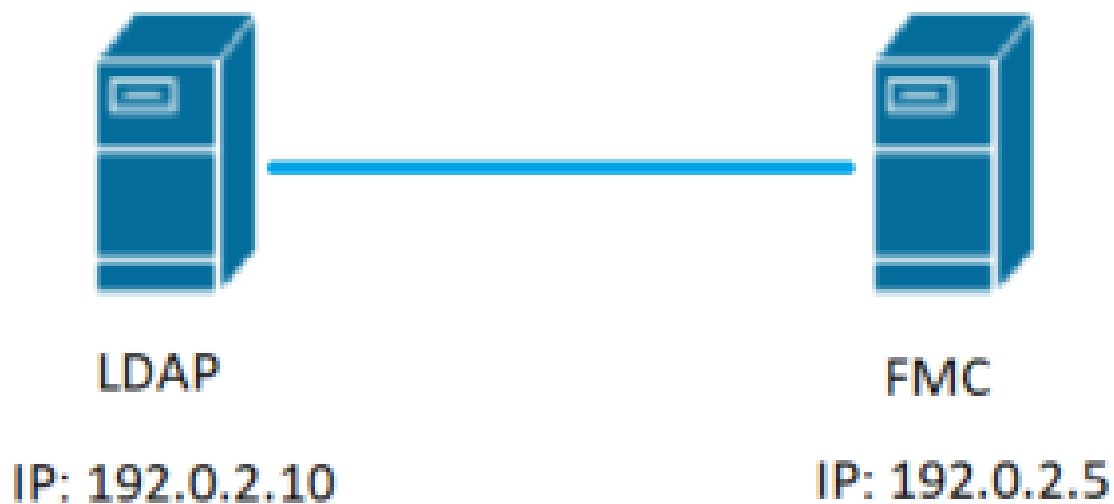
背景資訊

FMC和受管裝置包括用於管理訪問的預設管理員帳戶。您可以在FMC和受管裝置上新增自定義使用者帳戶，以內部使用者的身份新增，或者，如果您的模型支援，以LDAP或RADIUS伺服器上的外部使用者的身份新增。FMC和FTD支援外部使用者驗證。

·內部使用者 — FMC/FTD裝置檢查本地資料庫的使用者身份驗證。

·外部使用者 — 如果本地資料庫中不存在該使用者，則來自外部LDAP或RADIUS身份驗證伺服器的系統資訊將填充其使用者資料庫。

網路圖表



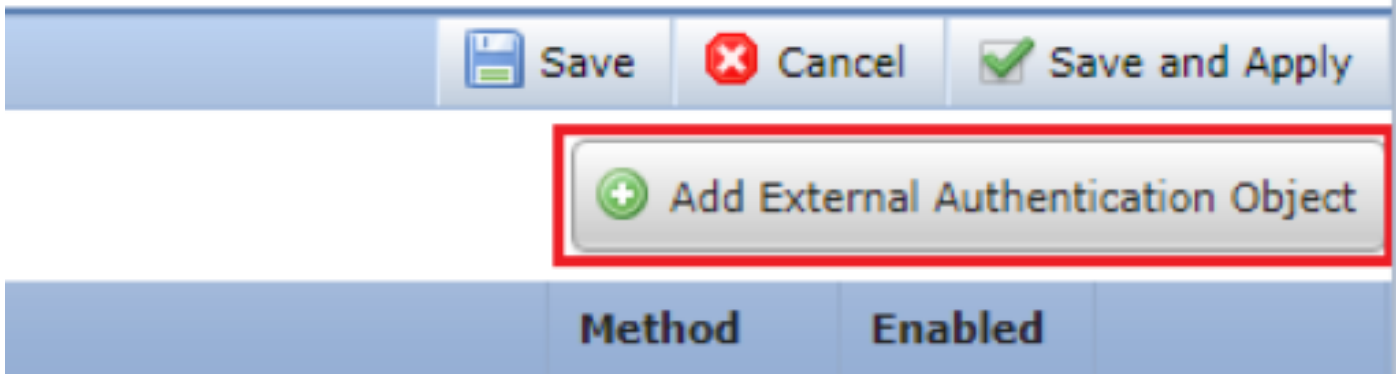
設定

FMC GUI中的基本LDAP配置

步驟 1. 導航至 `System > Users > External Authentication`。



步驟 2.選擇 Add External Authentication Object:



步驟 3.填寫必填欄位：

External Authentication Object

Authentication Method: **LDAP**

CAC: Use for CAC authentication and authorization

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

Description:

Server Type: **MS Active Directory** **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:

Port:

LDAP-Specific Parameters

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

Base Filter:

User Name *: **Username of LDAP Server admin**
ex. (cn=jsmith), (|cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

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

(Mandatory for FTD devices)

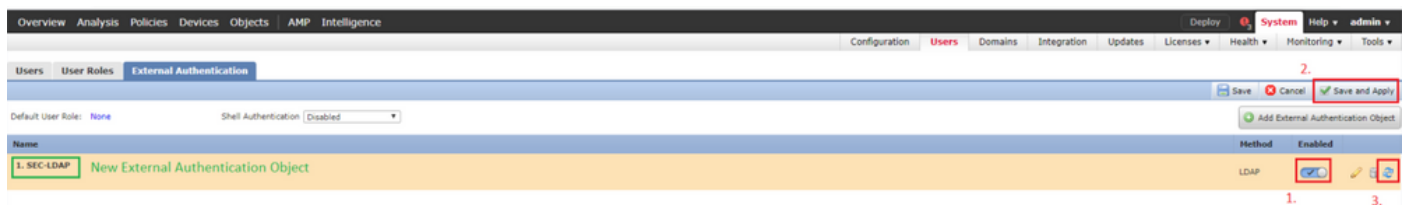
Additional Test Parameters

User Name

Password

*Required Field

步驟 4. 啟用 External Authentication 對象並儲存：



外部使用者的外殼訪問

FMC支援兩個不同的內部管理員使用者：一個用於Web介面，另一個具有CLI訪問許可權。這表示哪些人可以訪問GUI，哪些人也可以訪問CLI，兩者之間有明顯的區別。安裝時，預設管理員使用者的密碼會同步，以便在GUI和CLI上相同，但是，不同的內部機制會跟蹤這些密碼，而且最終可能會不同。

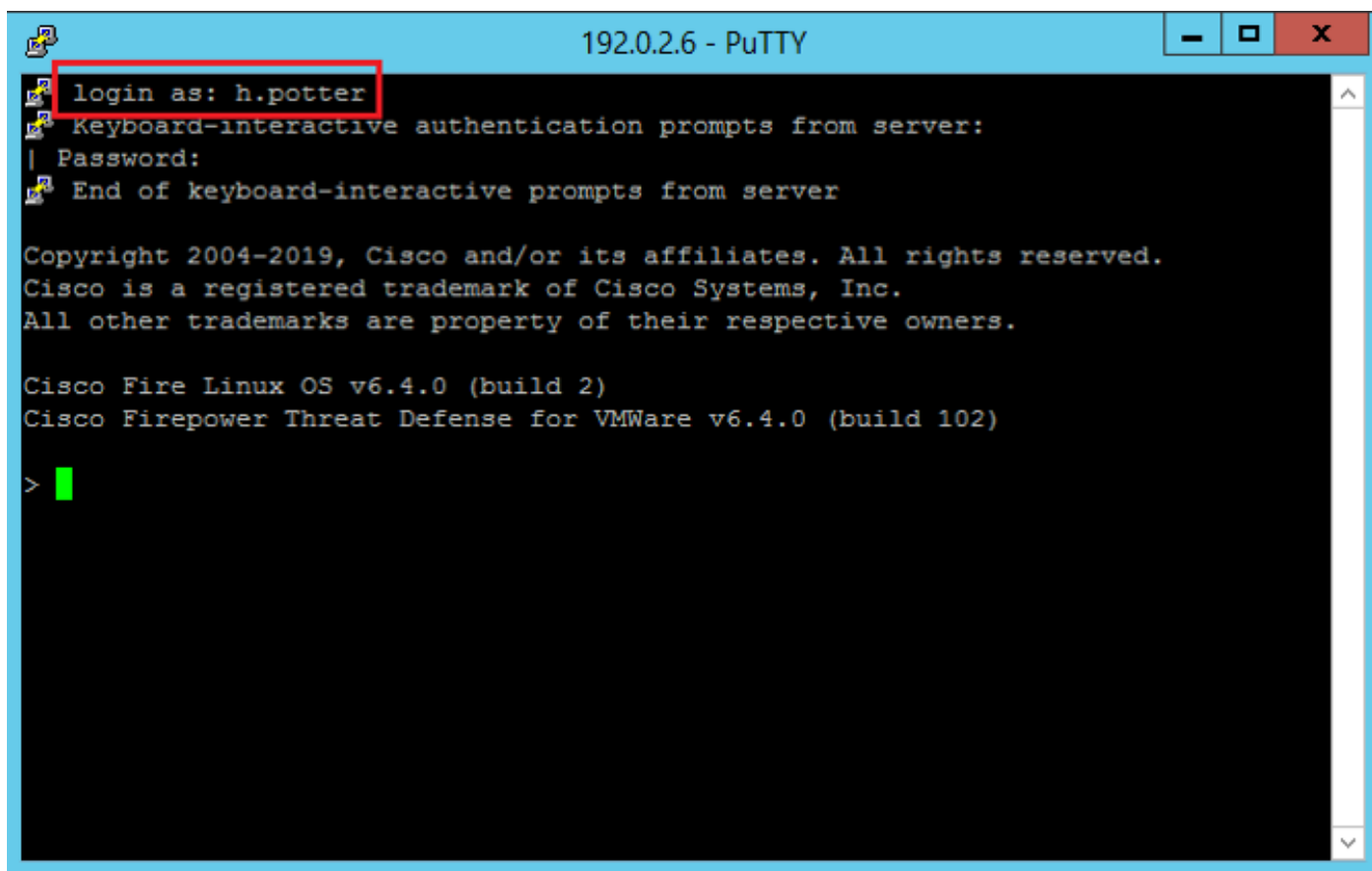
還必須授予LDAP外部使用者外殼訪問許可權。

步驟 1. 導航至 System > Users > External Authentication 然後按一下 Shell Authentication 下拉框並儲存：



步驟 2.在FMC中部署更改。

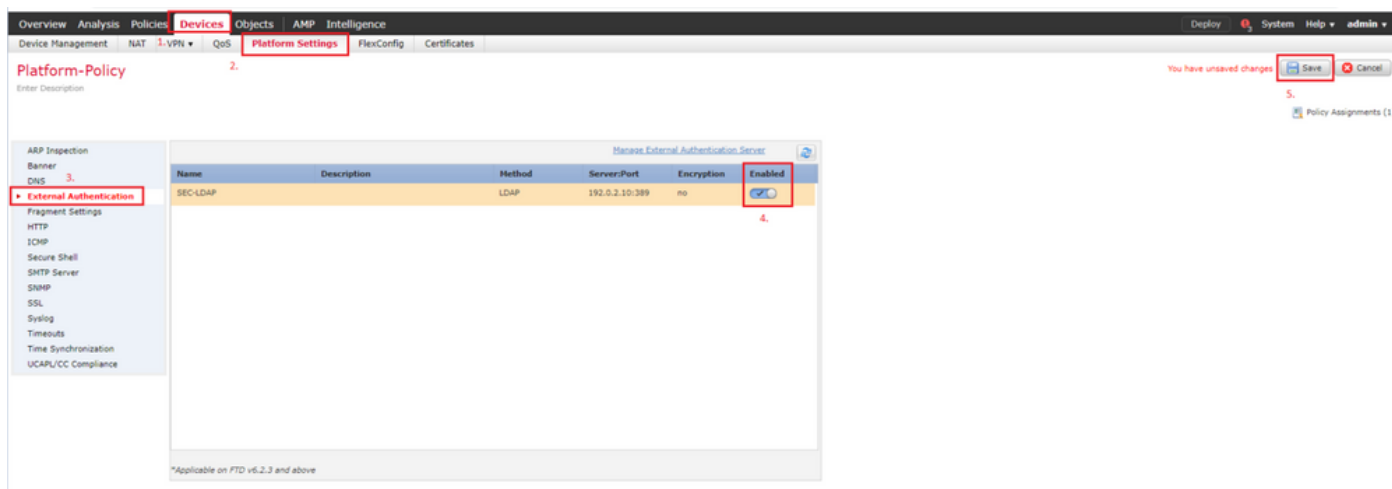
為外部使用者配置外殼訪問後，將啟用通過SSH登入，如下圖所示：



FTD的外部驗證

可在FTD上啟用外部驗證。

步驟 1.導航至 **Devices > Platform Settings > External Authentication**.按一下 **Enabled** 並儲存：



使用者角色

使用者許可權基於分配的使用者角色。您還可以建立自定義使用者角色，這些角色具有根據組織需

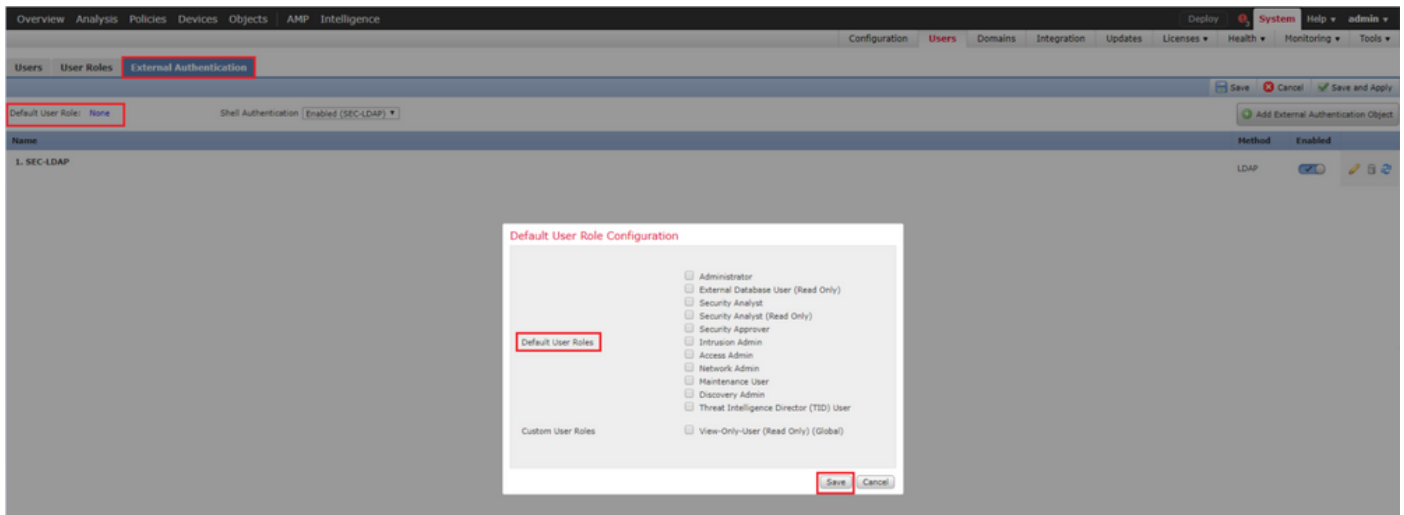
求定製的訪問許可權，或者您可以使用預定義的角色，如安全分析師和發現管理員。

有兩種型別的使用者角色：

1. Web介面使用者角色
2. CLI使用者角色

有關預定義角色的完整清單以及更多資訊，請參閱[使用者角色](#)。

若要為所有外部身份驗證對象配置預設使用者角色，請導航至 System > Users > External Authentication > Default User Role. 選擇要分配的預設使用者角色，然後按一下 Save.



要選擇預設使用者角色或將特定角色分配給特定對象組中的特定使用者，您可以選擇對象並導航至 Group Controlled Access Roles 如下圖所示：

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或TLS

必須在FMC中配置DNS。這是因為證書的Subject值必須與 Authentication Object Primary Server Hostname. 配置 Secure LDAP後，資料包捕獲不再顯示明文繫結請求。

SSL將預設埠更改為636,TLS將其保留為389。

 注意:TLS加密需要所有平台上的證書。若是SSL，FTD也需要憑證。對於其他平台，SSL不需要證書。但是，建議您始終上傳用於SSL的證書，以防止中間人攻擊。

步驟 1. 導航至 [Devices > Platform Settings > External Authentication > External Authentication Object](#) 並輸入高級選項 SSL/TLS資訊：

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)

步驟 2.上傳簽署伺服器證書的CA的證書。證書必須是PEM格式。

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)

步驟 3.儲存組態。

驗證

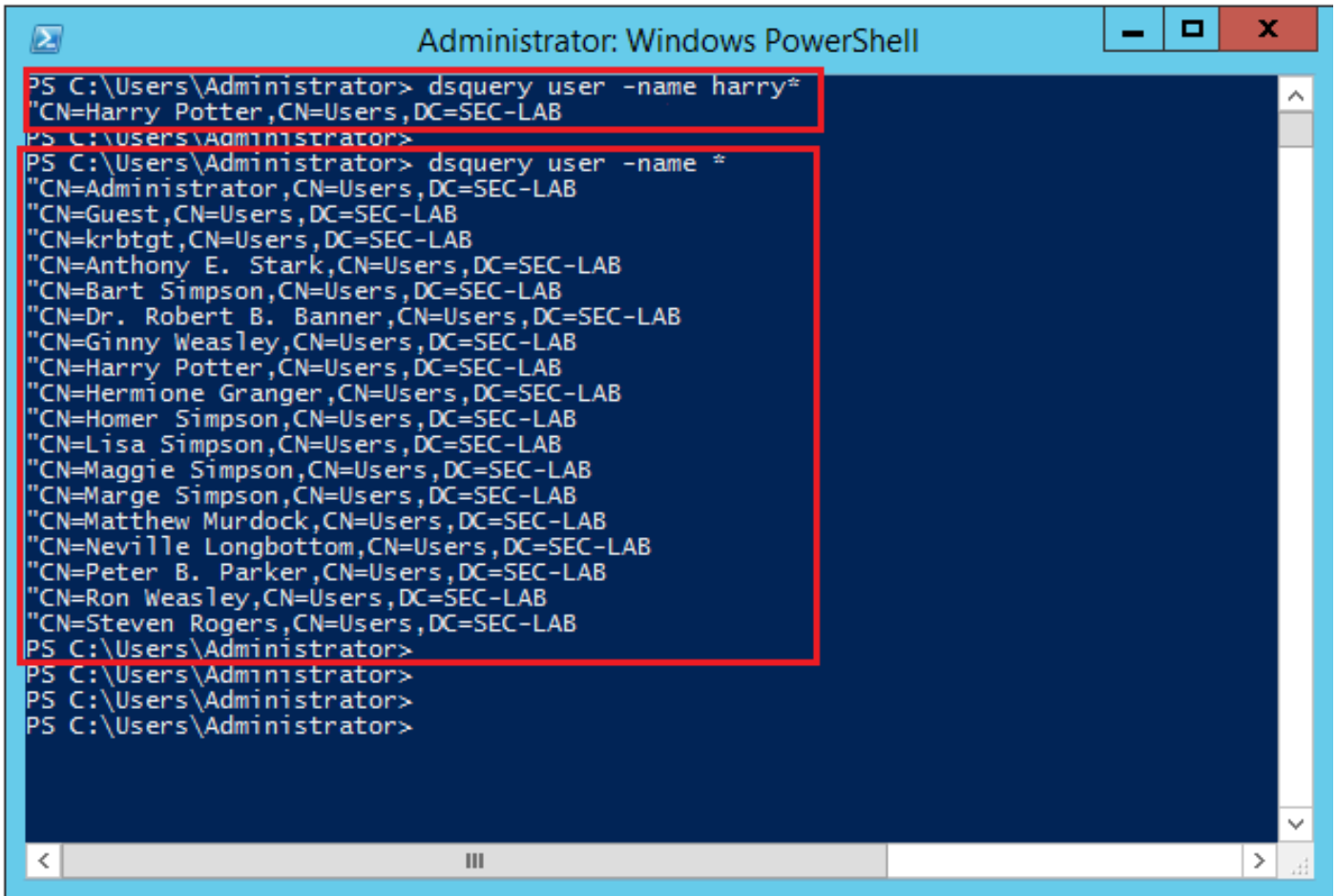
測試搜尋庫

開啟已配置LDAP的Windows命令提示符或PowerShell，然後鍵入命令：`dsquery user -name`

.

舉例來說：

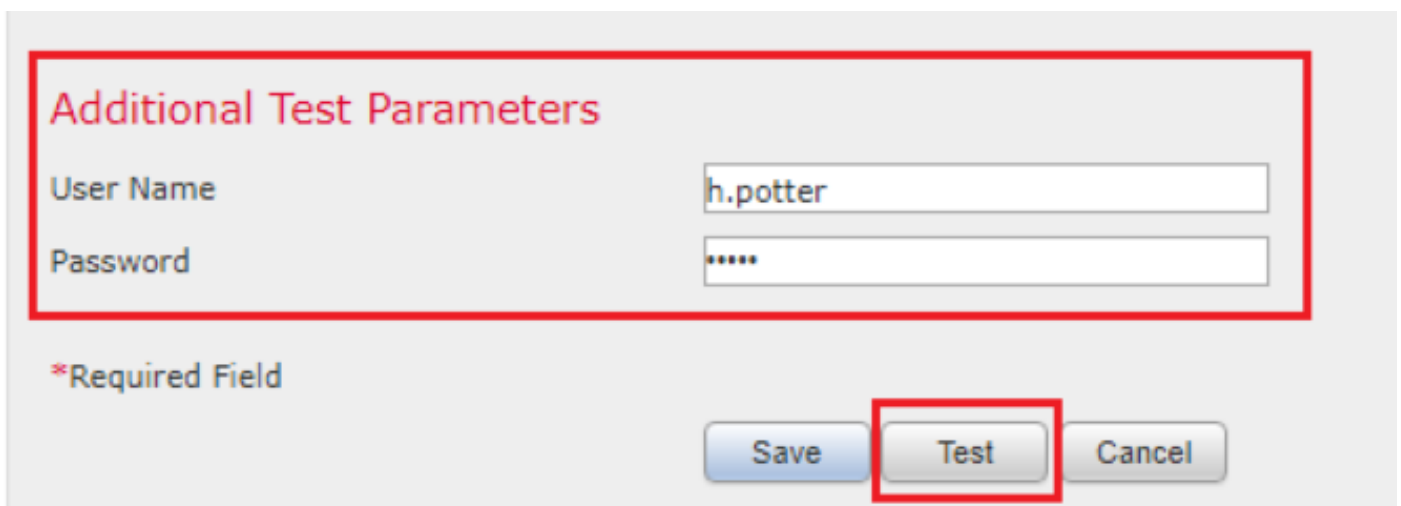
```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```

```
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>
```

測試LDAP整合

導航至 System > Users > External Authentication > External Authentication Object. 頁面底部有一個 Additional Test Parameters 一節，如下圖所示：



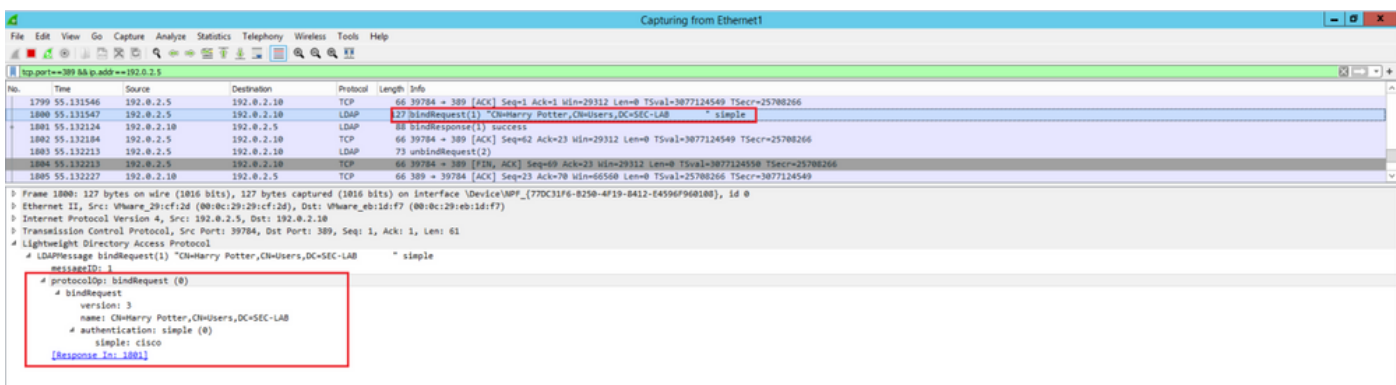
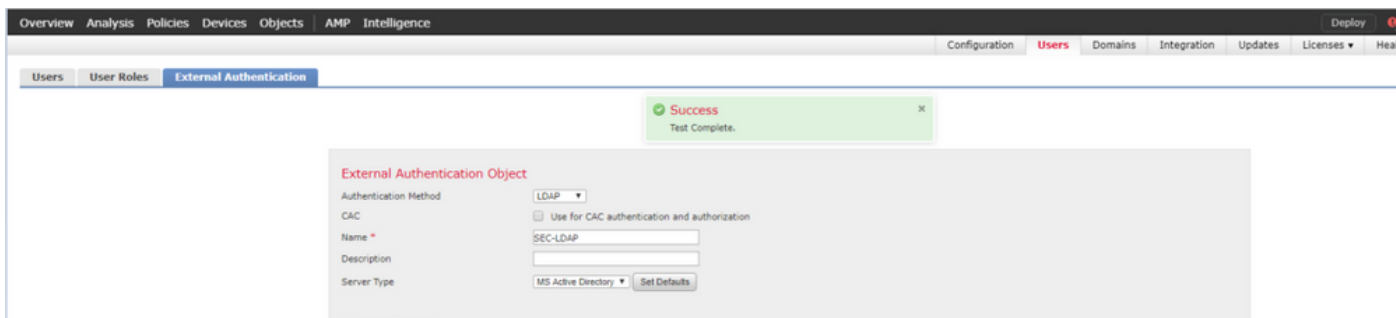
Additional Test Parameters

User Name

Password

*Required Field

選擇「測試」以檢視結果。



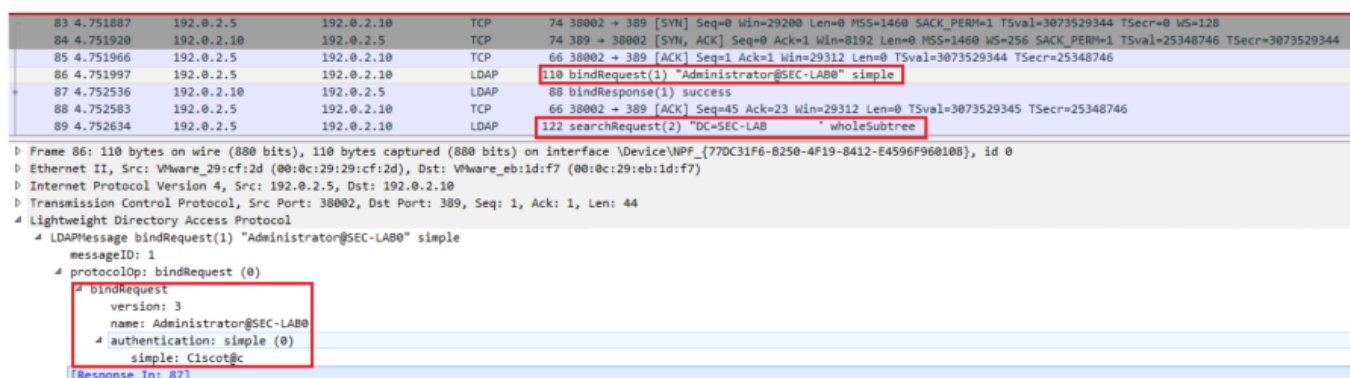
疑難排解

FMC/FTD和LDAP如何進行互動以下載使用者？

為了使FMC能夠從Microsoft LDAP伺服器拉入使用者，FMC必須首先使用LDAP管理員憑據在埠389或636(SSL)上傳送繫結請求。一旦LDAP伺服器能夠對FMC進行身份驗證，它會以成功消息做出響應。最後，FMC能夠使用搜尋請求消息發出請求，如下圖所示：

<< --- 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

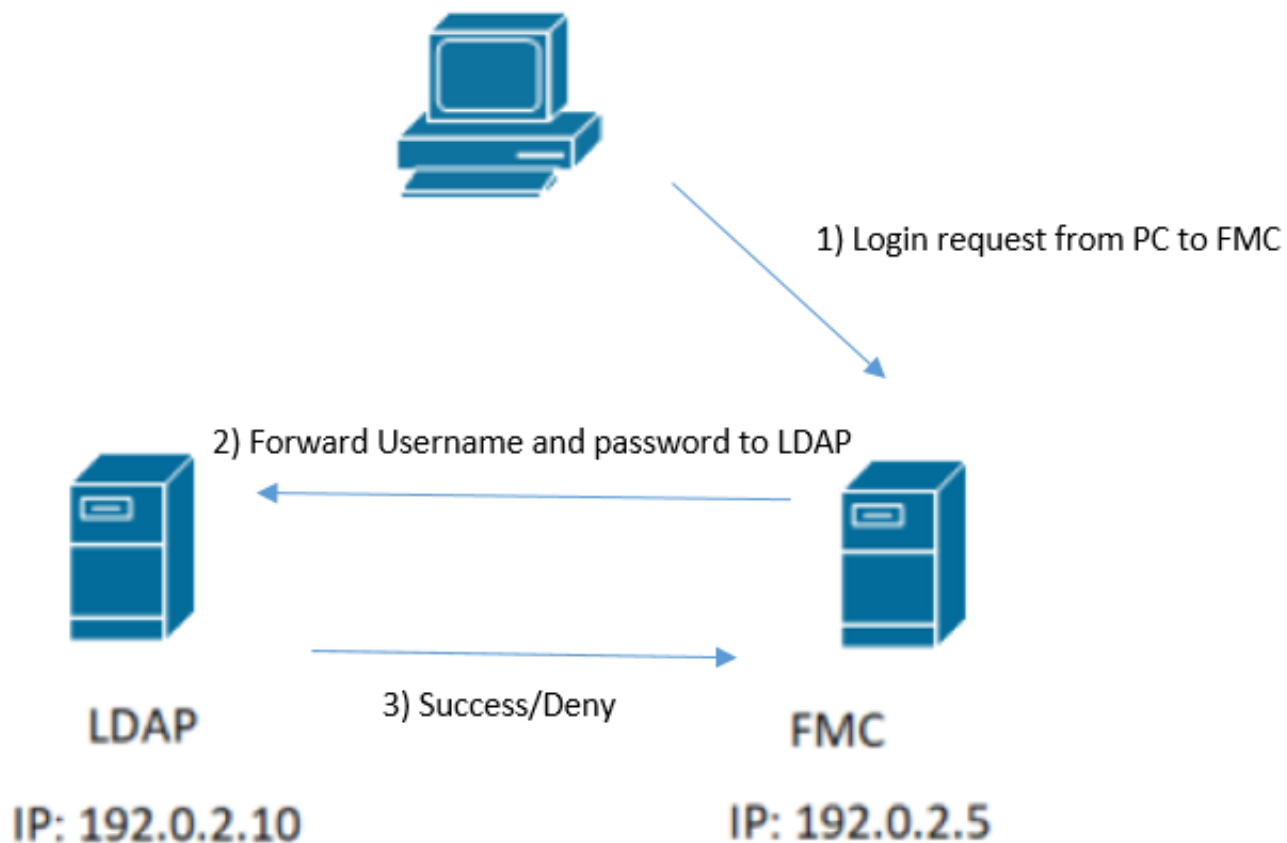
請注意，驗證預設會以明文形式傳送密碼：



FMC/FTD和LDAP如何互動以驗證使用者登入請求？

為了使使用者在啟用LDAP身份驗證時能夠登入到FMC或FTD，初始登入請求將傳送到Firepower，但使用者名稱和密碼將轉發到LDAP以獲得成功/拒絕響應。這意味著FMC和FTD不會將

密碼資訊儲存在本地資料庫中，而是等待LDAP確認如何繼續。



*Ethernet1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

如果接受使用者名稱和密碼，則會在Web GUI中新增一個條目，如下圖所示：



在FMC CLISH中運行命令show user以驗證使用者資訊：> show user

命令顯示指定使用者的詳細配置資訊。將顯示以下值：

Login — 登入名

UID — 數字使用者ID

身份驗證（本地或遠端） — 如何對使用者進行身份驗證

訪問（基本或配置） — 使用者的許可權級別

已啟用（啟用或禁用） — 使用者是否處於活動狀態

重設（Yes或No） — 使用者是否必須在下次登入時更改密碼

Exp（Never或數字） — 必須更改使用者密碼之前的天數

Warn(N/A or a number) — 使用者被指定在密碼到期之前更改其密碼的天數

Str（Yes或No） — 使用者的密碼是否必須滿足條件才能檢查強度

Lock（Yes或No） — 使用者帳戶是否由於登入失敗過多而被鎖定

最大（N/A或數字） — 鎖定使用者帳戶之前失敗登入的最大次數

SSL或TLS未按預期工作

如果您沒有在FTD上啟用DNS，則可以在尾日誌中看到錯誤，指示LDAP無法訪問：

```
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
```

確保Firepower能夠解析LDAP伺服器FQDN。如果沒有，請新增正確的DNS，如圖所示。

FTD：存取FTD CLISH並執行命令：> 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：選擇 System > Configuration，然後選擇 Management Interfaces，如下圖所示：

- 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

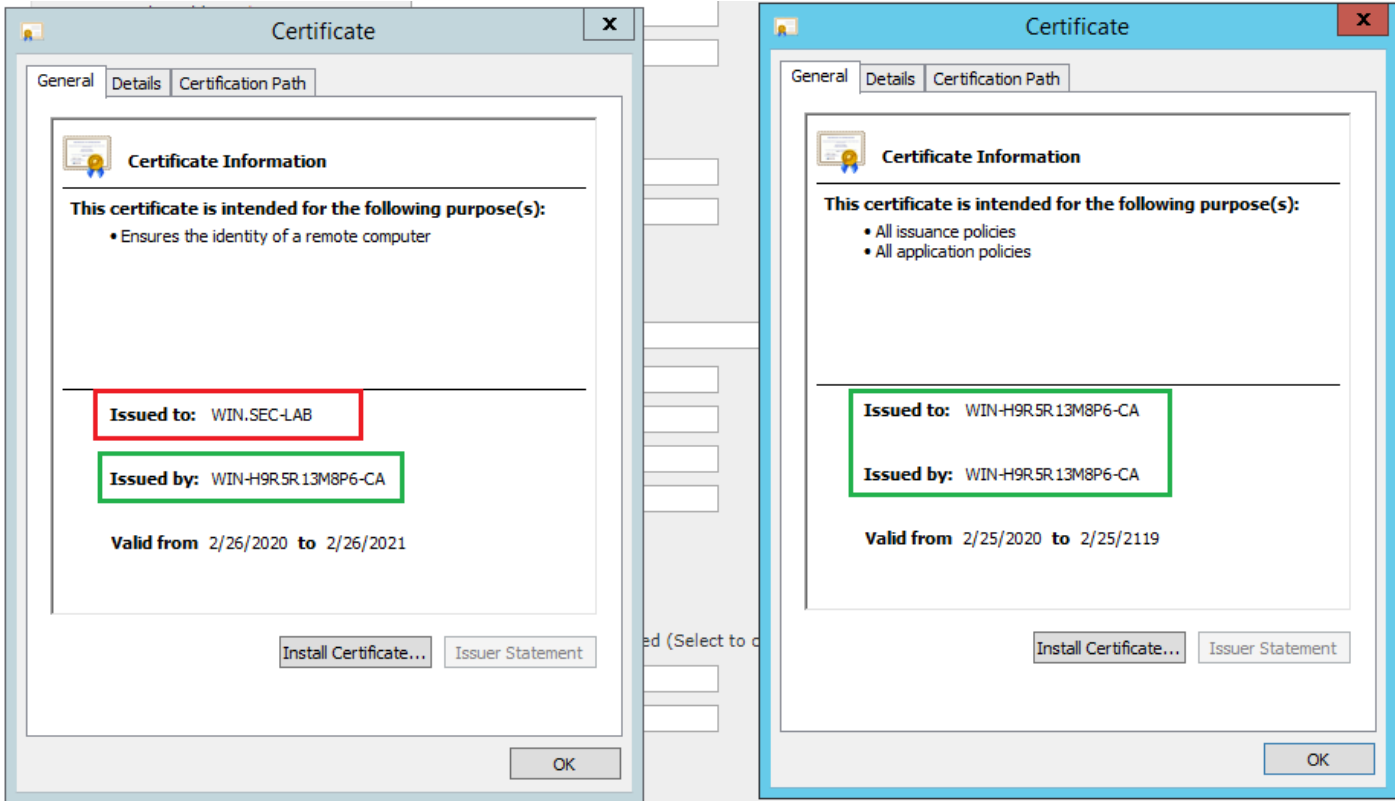
Allow Sending Echo Reply Packets:

Allow Sending Destination Unreachable Packets:

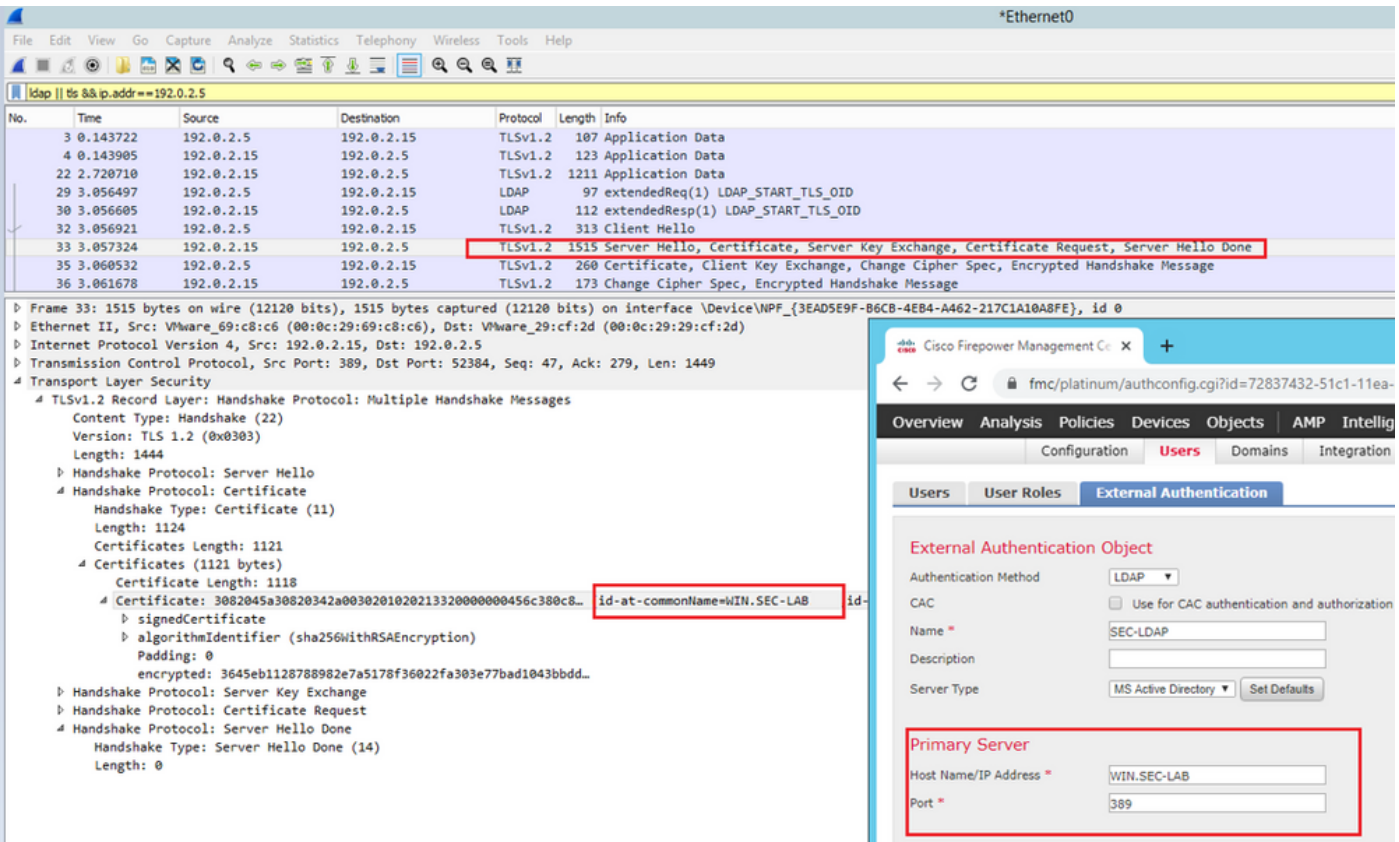
Proxy

Enabled:

確保上傳到FMC的證書是簽署LDAP伺服器證書的CA的證書，如下圖所示：



使用資料包捕獲確認LDAP伺服器傳送正確的資訊：



相關資訊

- [用於管理訪問的使用者帳戶](#)

- [Cisco Firepower管理中心輕型目錄訪問協定身份驗證繞過漏洞](#)
- [在FireSIGHT系統上配置LDAP身份驗證對象](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。