

# Configure Firepower Management Center and FTD with LDAP for External Authentication

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Network Diagram](#)

[Configure](#)

[Basic LDAP Configuration in FMC GUI](#)

[Shell Access for External Users](#)

[External Authentication to FTD](#)

[User Roles](#)

[SSL or TLS](#)

[Verify](#)

[Test Search Base](#)

[Test LDAP Integration](#)

[Troubleshoot](#)

[How do FMC/FTD and LDAP interact to download users?](#)

[How do FMC/FTD and LDAP interact to authenticate a user login request?](#)

[SSL or TLS does not Work as Expected](#)

[Related Information](#)

## Introduction

This document describes how to enable Microsoft Lightweight Directory Access Protocol (LDAP) External Authentication with Cisco Firepower Management Center (FMC) and Firepower Threat Defense (FTD).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco FTD
- Cisco FMC
- Microsoft LDAP

### Components Used

The information in this document is based on these software and hardware versions:

- FTD 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. If your network is live, ensure that you understand the potential impact of any command.

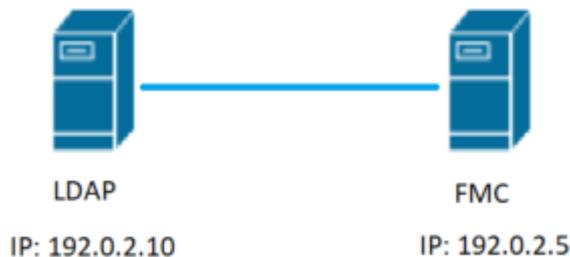
## Background Information

The FMC and managed devices include a default admin account for management access. You can add custom user accounts on the FMC and on managed devices, either as internal users or, if supported for your model, as external users on an LDAP or RADIUS server. External user authentication is supported for FMC and FTD.

• Internal user - The FMC/FTD device checks a local database for user authentication.

• External user - If the user is not present in the local database, the system information from an external LDAP or RADIUS authentication server populates its user database.

## Network Diagram



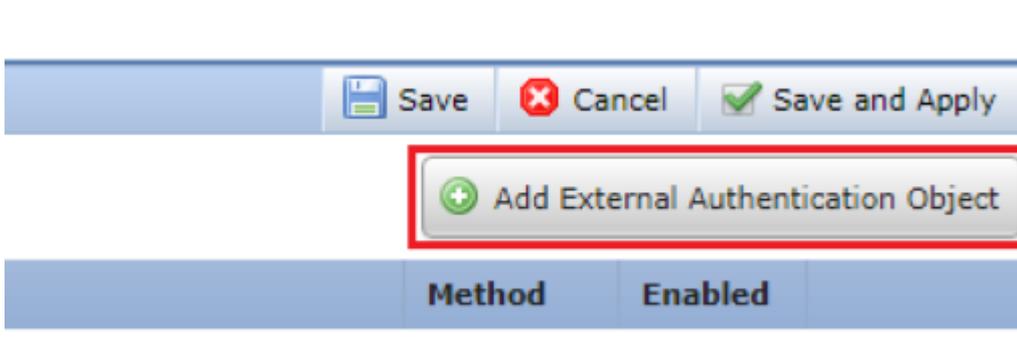
## Configure

### Basic LDAP Configuration in FMC GUI

Step 1. Navigate to System > Users > External Authentication:



Step 2. Choose Add External Authentication Object:



Step 3. Complete the required fields:

**External Authentication Object**

Authentication Method:  **LDAP**

CAC:  Use for CAC authentication and authorization

Name \*:  **SEC-LDAP** 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 \*:  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:

Port:

**LDAP-Specific Parameters**

\*Base DN specifies where users will be found

Base DN \*:  DC=SEC-LAB  ex. dc=sourcefire,dc=com

Base Filter:

User Name \*:  Administrator@SEC-LAB0 Username of LDAP Server admin

Password \*:

Confirm Password \*:

Show Advanced Options:

**Attribute Mapping**

\*Default when 'Set Defaults' option is clicked

UI Access Attribute \*:  sAMAccountName

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

Step 4. Enable the External Authentication Object and Save:

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration **Users** Domains In

Users User Roles **External Authentication**

Default User Role: None Shell Authentication: Disabled

Name

**1. SEC-LDAP** New External Authentication Object

## Shell Access for External Users

The FMC supports two different internal admin users: one for the web interface, and another with CLI access. This means there is a clear distinction between who can access the GUI and who can also access CLI. At the time of installation, the password for the default admin user is synchronized in order to be the same on both GUI and CLI, however, they are tracked by different internal mechanisms, and can eventually be different.

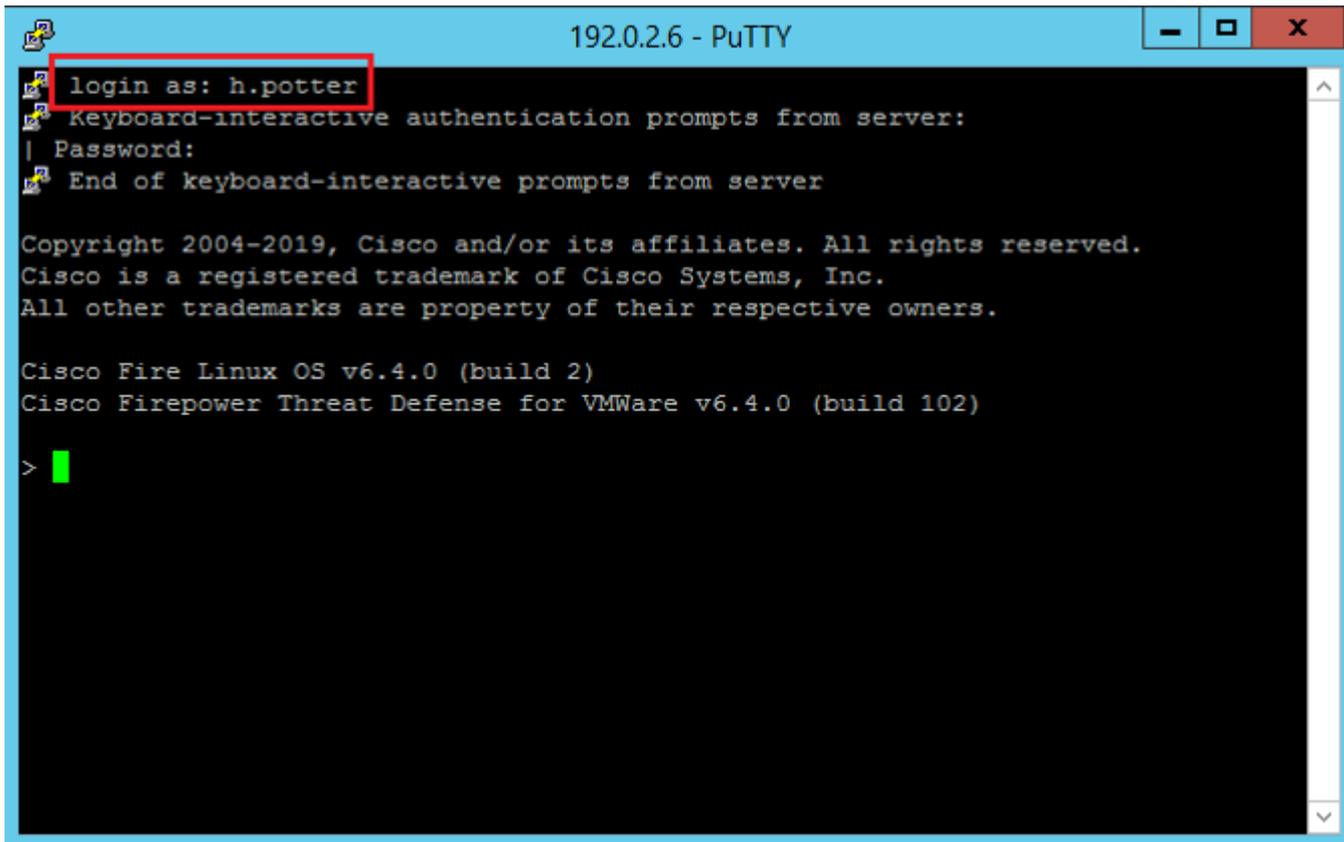
LDAP External users must also be granted shell access.

Step 1. Navigate to System > Users > External Authentication and click Shell Authentication drop-down box as seen in the image and save:



Step 2. Deploy changes in FMC.

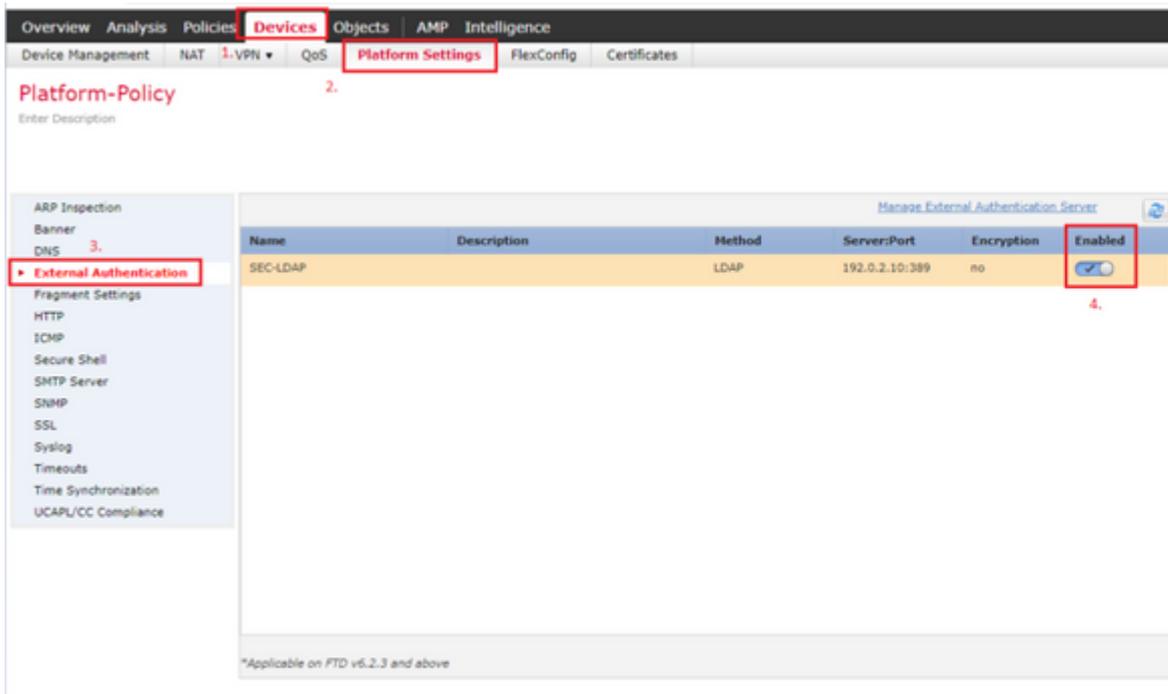
Once shell access for external users is configured, login via SSH is enabled as seen in the image:



## External Authentication to FTD

External authentication can be enabled on FTD.

Step 1. Navigate to Devices > Platform Settings > External Authentication. Click Enabled and save:



## User Roles

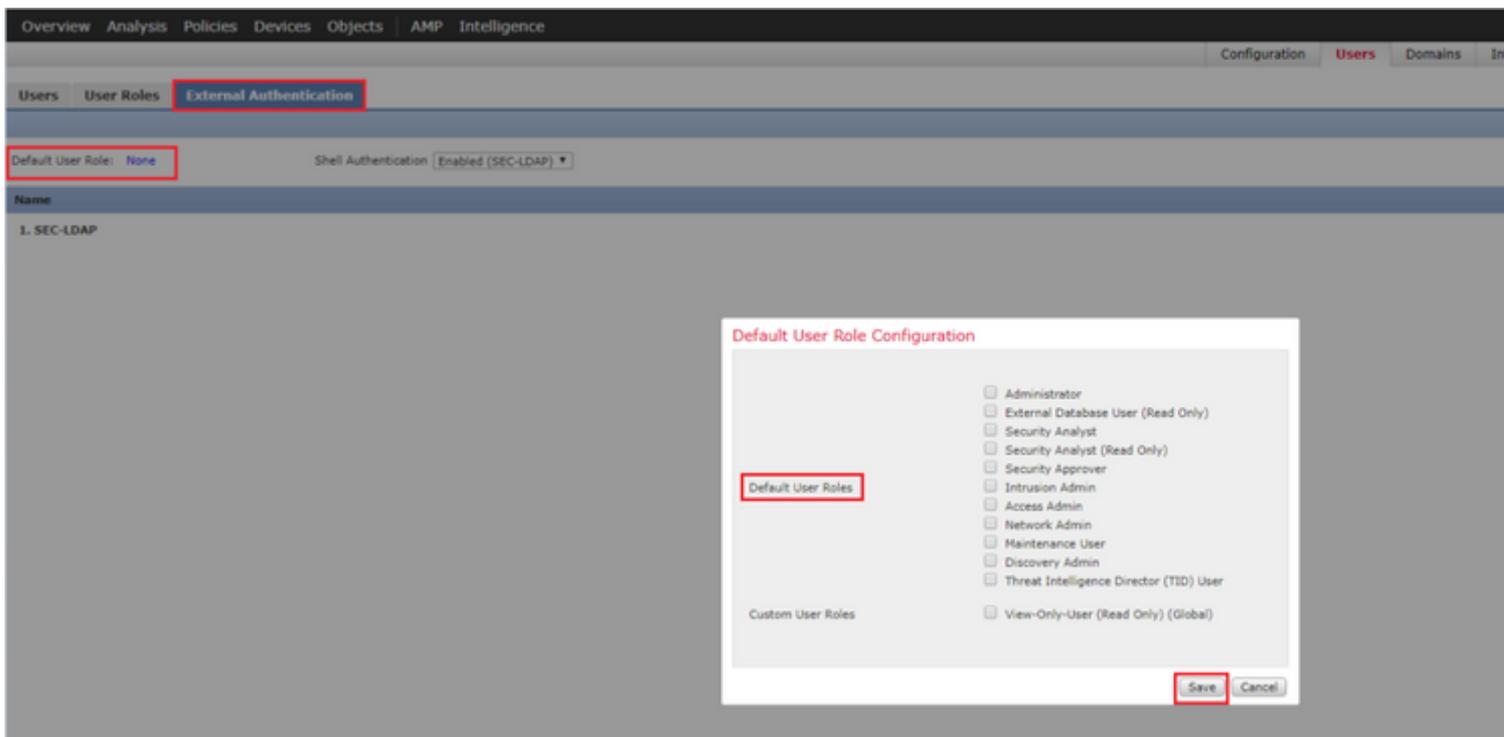
User privileges are based on the assigned user role. You can also create custom user roles with access privileges tailored to the needs of your organization or you can use predefined roles such as Security Analyst and Discovery Admin.

There are two types of user roles:

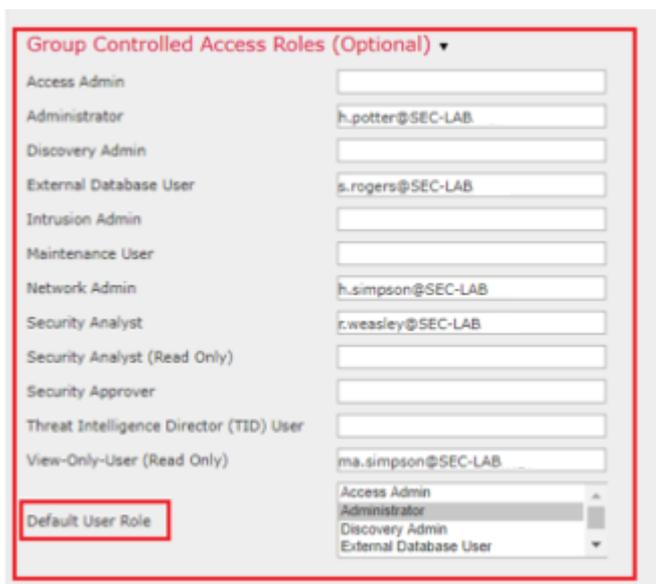
1. Web Interface User Roles
2. CLI User Roles

For a full list of predefined roles and more information, refer to; [User Roles](#).

In order to configure a default user role for all External Authentication Objects, navigate to System > Users > External Authentication > Default User Role. Choose the default user role you like to assign and click Save.



In order to choose a default user role or assign specific roles to specific users in a particular object group, you can choose the object and navigate to Group Controlled Access Roles as seen in the image:



## SSL or TLS

DNS must be configured in the FMC. This is because the Subject value of the Certificate must match the Authentication Object Primary Server Hostname. Once Secure LDAP is configured, packet captures no longer show clear text bind requests.

SSL changes the default port to 636, and TLS keeps it as 389.

**Note:** TLS encryption requires a certificate on all platforms. For SSL, the FTD also requires a certificate. For other platforms, SSL does not require a certificate. However, it is recommended that you always upload a certificate for SSL in order to prevent man-in-the-middle attacks.

Step 1. Navigate to Devices > Platform Settings > External Authentication > External Authentication Object and enter the Advanced Options SSL/TLS information:

LDAP-Specific Parameters

Base DN \* DC=SEC-LAB Fetch DNS ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (!cn=jsmith)

User Name \* h.potter@SEC-LAB ex. cn=jsmith,dc=sourcefire,

Password \* .....

Confirm Password \* .....

Show Advanced Options ▼

Encryption  SSL  TLS  None

SSL Certificate Upload Path Choose File No file chosen ex. PEM Format (base64 enc

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

Timeout (Seconds) 30

Step 2. Upload the certificate of the CA who signed the certificate of the server. The certificate must be in PEM format.

LDAP-Specific Parameters

Base DN \* DC=SEC-LAB Fetch DNS ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (!cn=jsmith)

User Name \* h.potter@SEC-LAB ex. cn=jsmith,dc=sourcefire

Password \* .....

Confirm Password \* .....

Show Advanced Options ▼

Encryption  SSL  TLS  None

SSL Certificate Upload Path Choose File CA-Cert-base64.cer ex. PEM Format (base64 enc

Certificate has been loaded (select to clear loaded certificate)

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

Timeout (Seconds) 30

Step 3. Save the configuration.

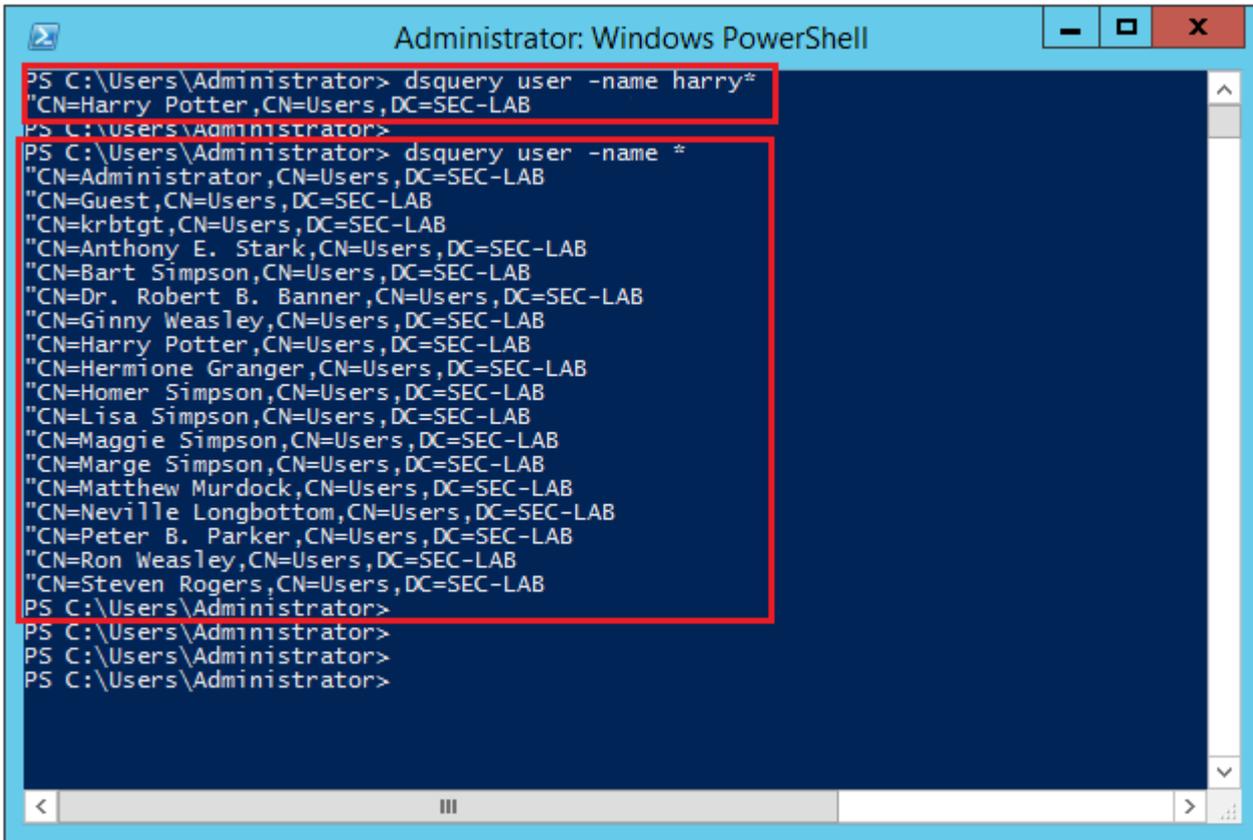
## Verify

### Test Search Base

Open a Windows command prompt or PowerShell where LDAP is configured and type the command: dsquery user -name <known username> .

For example:

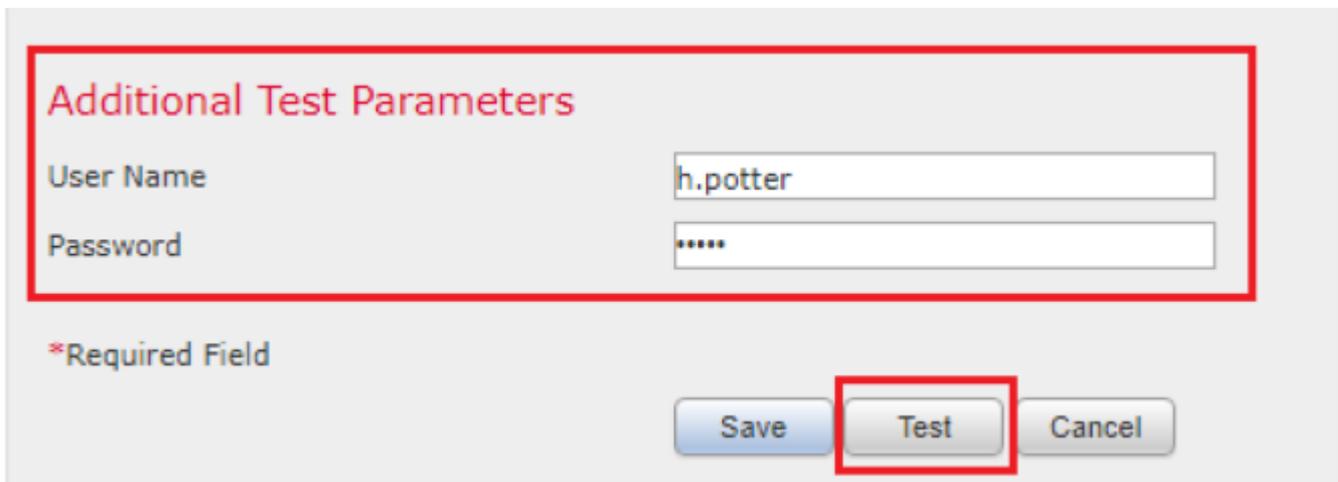
```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```



```
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>
```

## Test LDAP Integration

Navigate to System > Users > External Authentication > External Authentication Object. At the bottom of the page, there is an Additional Test Parameters section as seen in the image:



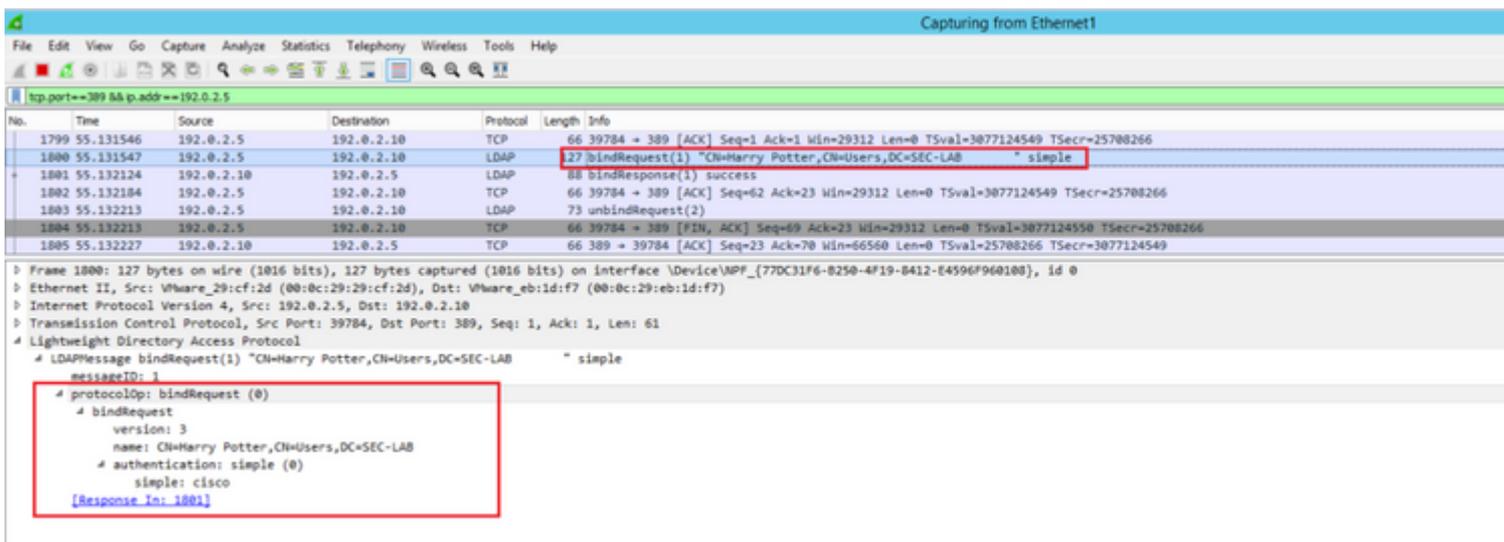
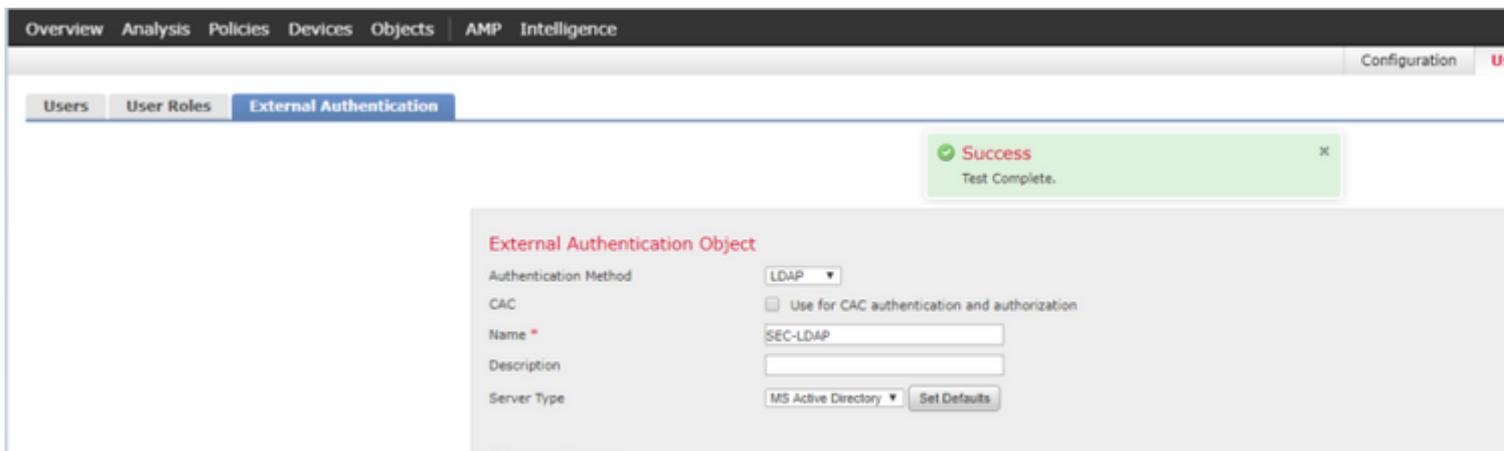
**Additional Test Parameters**

User Name

Password

\*Required Field

Choose the Test in order to see the results.



## Troubleshoot

### How do FMC/FTD and LDAP interact to download users?

In order for FMC to be able to pull users from a Microsoft LDAP server, the FMC must first send a bind request on port 389 or 636 (SSL) with the LDAP administrator credentials. Once the LDAP server is able to authenticate FMC, it responds with a success message. Finally, FMC is able to make a request with the search Request message as described in the diagram:

```
<< --- 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
```

Notice that the authentication sends passwords in the clear by default:

83	4.751887	192.0.2.5	192.0.2.10	TCP	74 38002 + 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3073529344
84	4.751920	192.0.2.10	192.0.2.5	TCP	74 389 + 38002 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
85	4.751966	192.0.2.5	192.0.2.10	TCP	66 38002 + 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3073529344 TSecr=25348746
86	4.751997	192.0.2.5	192.0.2.10	LDAP	110 bindRequest(1) "Administrator@SEC-LAB0" simple
87	4.752536	192.0.2.10	192.0.2.5	LDAP	88 bindResponse(1) success
88	4.752583	192.0.2.5	192.0.2.10	TCP	66 38002 + 389 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSval=3073529345 TSecr=25348746
89	4.752634	192.0.2.5	192.0.2.10	LDAP	122 searchRequest(2) "DC=SEC-LAB" wholeSubtree

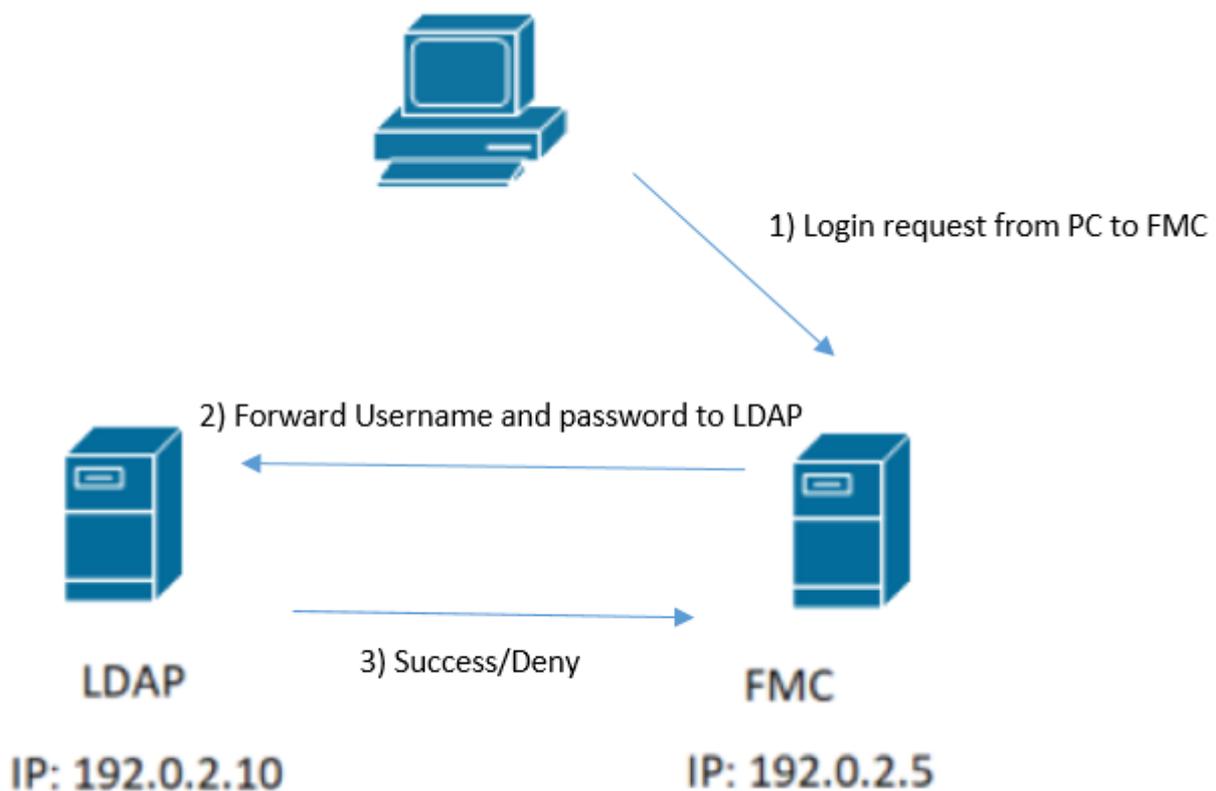
```

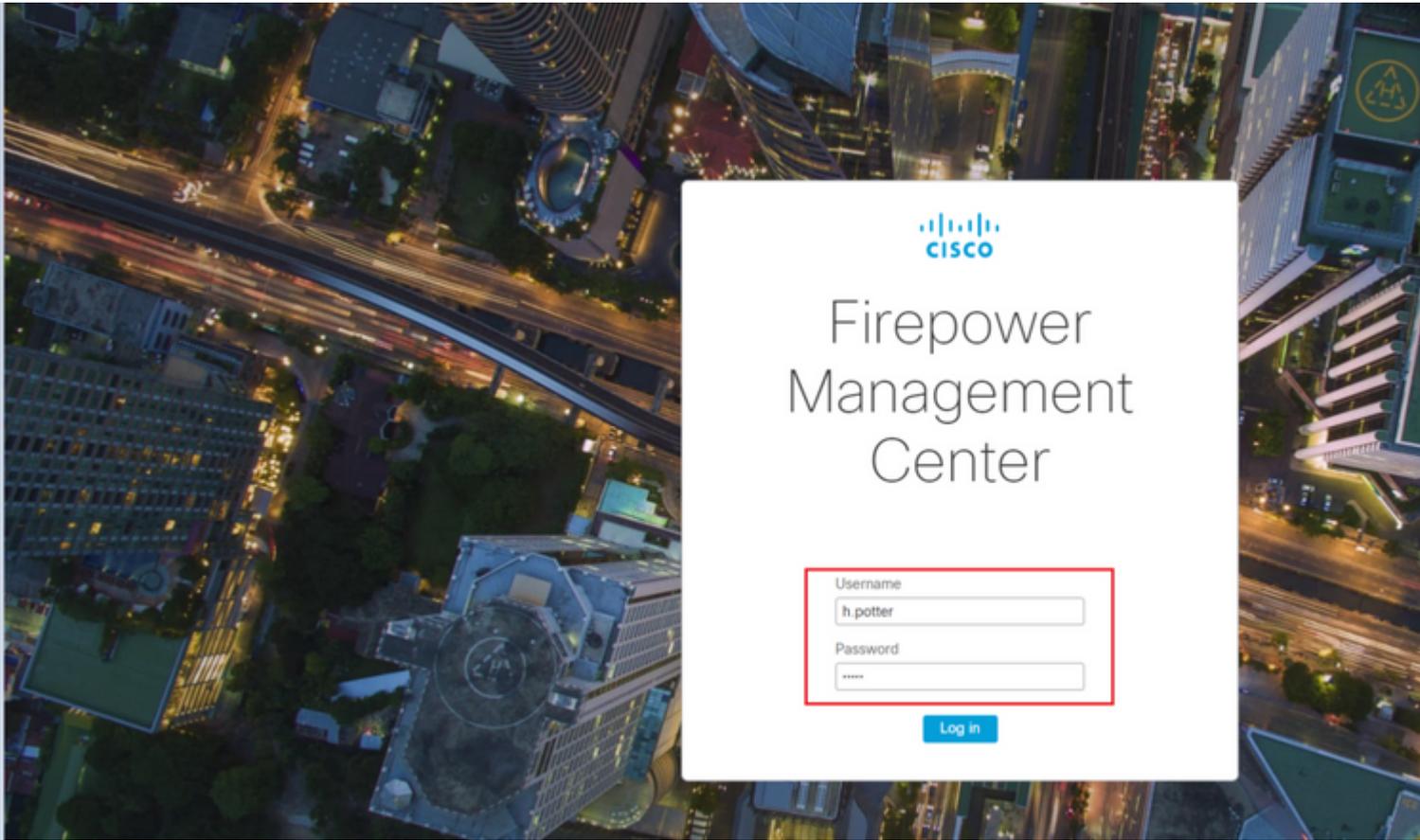
Frame 86: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{77DC31F6-B250-4F19-8412-E4596F960108}, id 0
Ethernet II, Src: VMware_29:cf:2d (00:0c:29:29:cf:2d), Dst: VMware_eb:1d:f7 (00:0c:29:eb:1d:f7)
Internet Protocol Version 4, Src: 192.0.2.5, Dst: 192.0.2.10
Transmission Control Protocol, Src Port: 38002, Dst Port: 389, Seq: 1, Ack: 1, Len: 44
Lightweight Directory Access Protocol
  LDAPMessage bindRequest(1) "Administrator@SEC-LAB0" simple
    messageID: 1
    protocolOp: bindRequest (0)
      bindRequest
        version: 3
        name: Administrator@SEC-LAB0
        authentication: simple (0)
          simple: Cisco@c
    [Response In: 87]

```

## How do FMC/FTD and LDAP interact to authenticate a user login request?

In order for a user to be able to log in to FMC or FTD while LDAP authentication is enabled, the initial login request is sent to Firepower, however, the username and password are forwarded to LDAP for a success/deny response. This means that FMC and FTD do not keep password information locally in the database and instead await confirmation from LDAP on how to proceed.





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"
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"
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"
98	13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	88	bindResponse(1) success

If the username and password are accepted, an entry is added in the web GUI as seen in the image:

Username	Roles	Authentication Method	Password Lifetime
admin	Administrator	Internal	Unlimited
<b>h.potter</b>	Administrator	<b>External</b>	

Run the command show user in FMC CLISH in order to verify user information: > show user <username>

The command displays detailed configuration information for the specified user(s). These values are displayed:

Login "h.potter" the login name

UID â€” the numeric user ID

Auth (Local or Remote) â€” how the user is authenticated

Access (Basic or Config) â€” the privilege level of the user

Enabled (Enabled or Disabled) â€” whether the user is active

Reset (Yes or No) â€” whether the user must change the password at the next login

Exp (Never or a number) â€” the number of days until the password of the user must be changed

Warn (N/A or a number) â€” the number of days a user is given in order to change their password before it expires

Str (Yes or No) â€” whether the password of the user must meet the criteria to check the strength

Lock (Yes or No) â€” whether the account of the user has been locked due to too many login failures

Max (N/A or a number) â€” the maximum number of failed logins before the account of the user is locked

## SSL or TLS does not Work as Expected

If you do not enable DNS on the FTDs, you can see errors in the pigtail log that suggest that LDAP is unreachable:

```
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 euid=0
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 192.0.2.15
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15 port 6144
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter from 192.0.2.15
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 6144
```

Ensure that Firepower is able to resolve the LDAP Servers FQDN. If not, add the correct DNS as seen in the image.

FTD: Access the FTD CLISH and run the command: > configure network dns servers <IP Address>.

```
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:~$
```

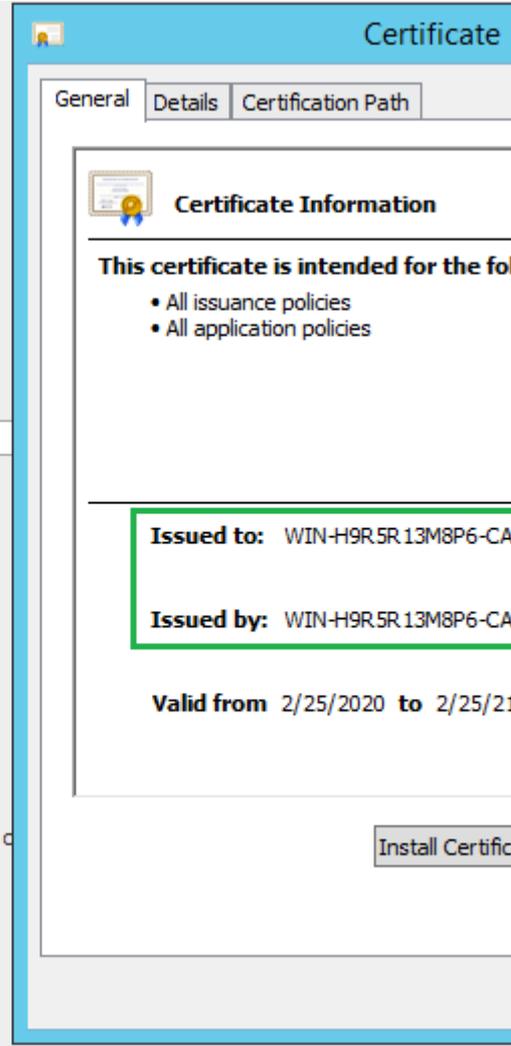
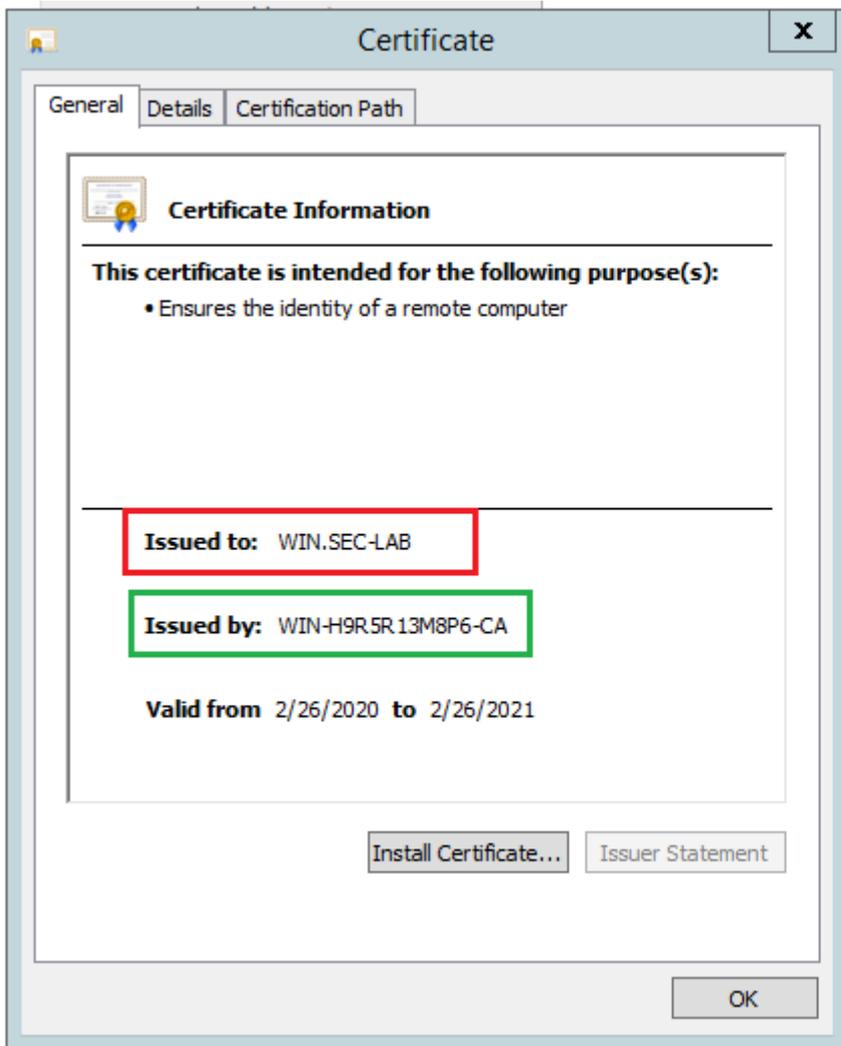
FMC: Choose System > Configuration, and then choose Management Interfaces as seen in the image:

The image shows a configuration page for a network device. On the left is a navigation menu with 'Management Interfaces' highlighted. The main content area is divided into several sections:

- Interfaces:** A table with columns: Link, Name, Channels, MAC Address, IP Address. One entry is visible: eth0 with IP 192.0.2.5.
- Routes:** Two sub-sections: IPv4 Routes and IPv6 Routes. The IPv4 Routes table has columns: Destination, Netmask, Interface, Gateway. One entry is visible: \* with Gateway 192.0.2.1.
- Shared Settings:** A form with fields for Hostname (SEC-FMC), Domains, Primary DNS Server (192.0.2.10), Secondary DNS Server, Tertiary DNS Server, and Remote Management Port (8305). The Primary and Secondary DNS Server fields are highlighted with a red box.
- ICMPv6:** Two checkboxes: 'Allow Sending Echo Reply Packets' and 'Allow Sending Destination Unreachable Packets', both checked.
- Proxy:** An 'Enabled' checkbox which is unchecked.

At the bottom are 'Save' and 'Cancel' buttons.

Ensure the certificate uploaded to FMC is the certificate of the CA who signed the server certificate of the LDAP, as illustrated in the image:



Use packet captures in order to confirm LDAP server sends the correct information:

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
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-4EB4-A462-217C1A10...
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: 52384, 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: 3082045a30820342a0030201020213320000000456c380c8... id-at-commonName=WIN.SEC-LAB id-...
    signedCertificate
    algorithmIdentifier (sha256WithRSAEncryption)
    Padding: 0
    encrypted: 3645eb1128788982e7a5178f36022fa303e77bad1043bbdd...
  Handshake Protocol: Server Key Exchange
  Handshake Protocol: Certificate Request
  Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0
  
```

## Related Information

- [User Accounts for Management Access](#)
- [Cisco Firepower Management Center Lightweight Directory Access Protocol Authentication Bypass Vulnerability](#)
- [Configuration of LDAP Authentication Object on FireSIGHT System](#)
- [Technical Support & Documentation - Cisco Systems](#)