Configure Firepower Management Center and FTD with LDAP for External Authentication

Contents

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.

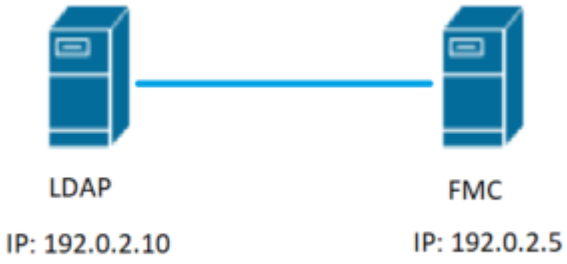
Background Information

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.

â€¢ Internal user - The FMC/FTD device checks a local database for user authentication.

â€¢ 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

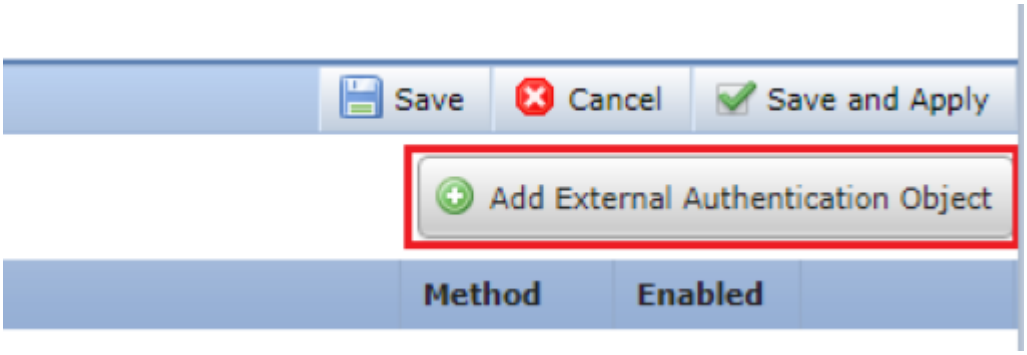


Configure

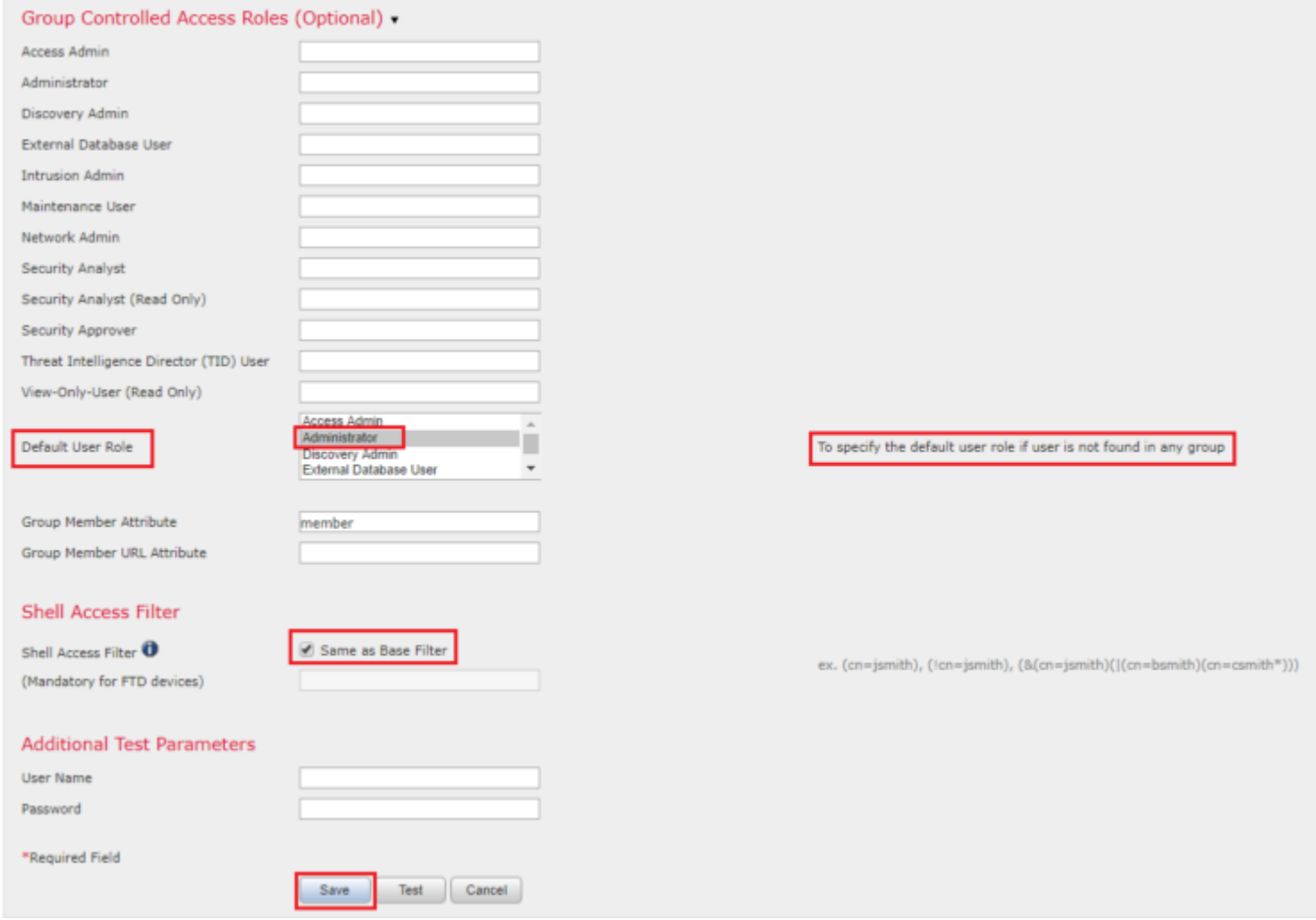
Basic LDAP Configuration in FMC GUI

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

Step 2. Choose Add External Authentication Object:



Step 3. Complete the required fields:



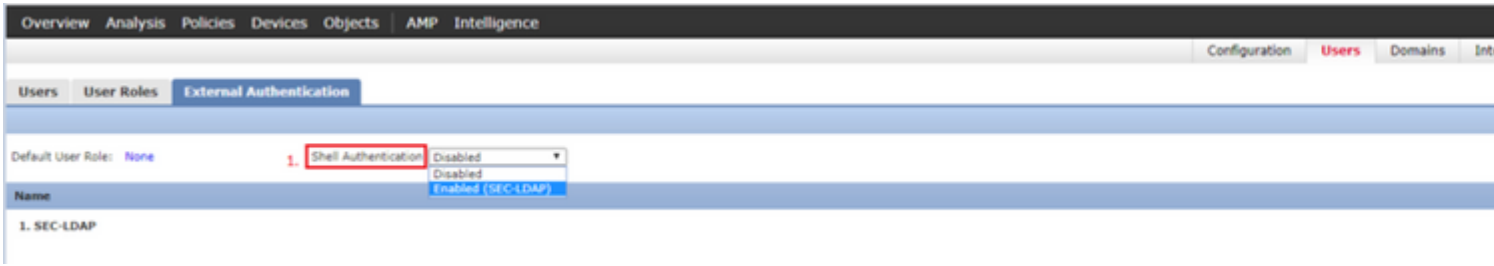
Step 4. Enable the External Authentication Object and Save:

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.

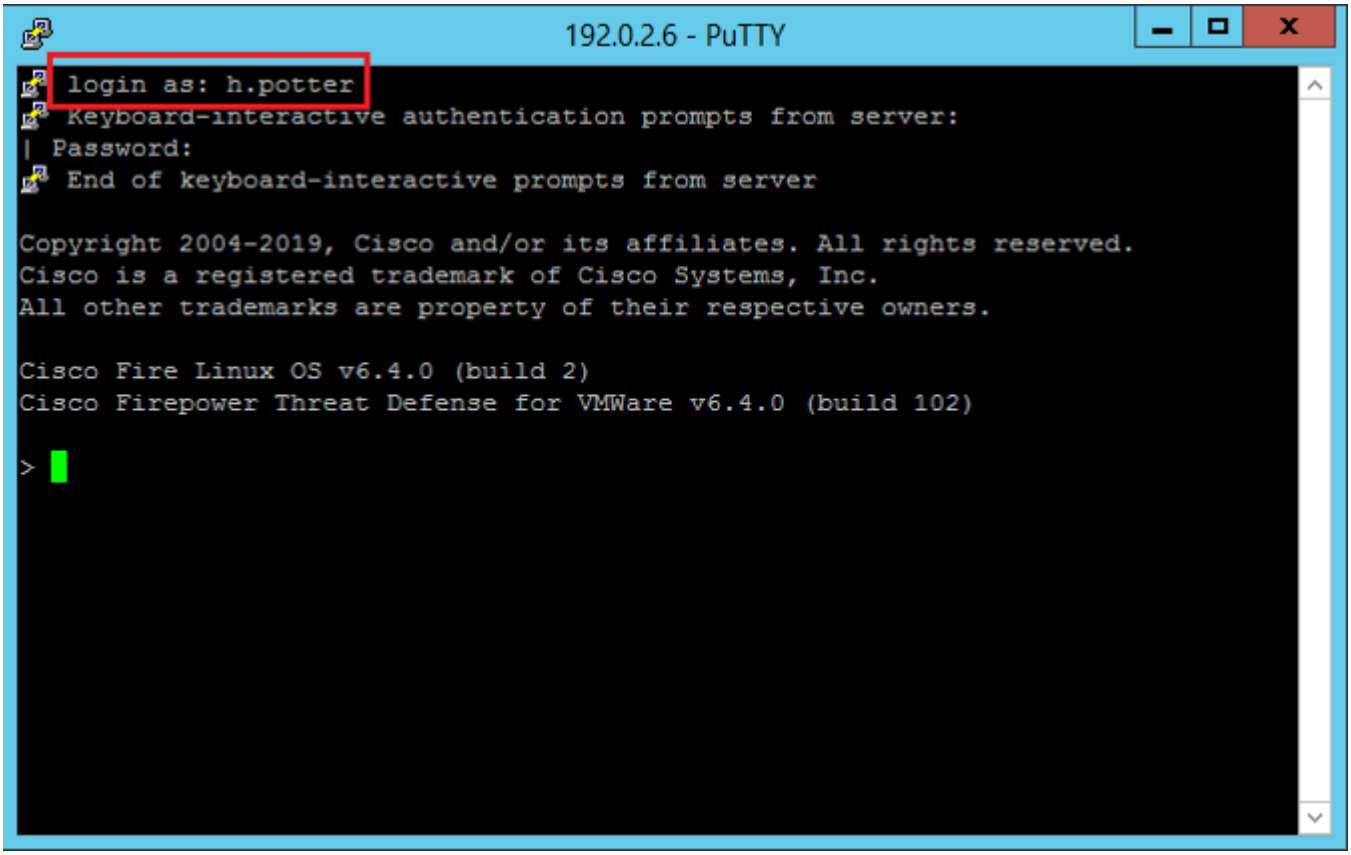
LDAP External users must also be granted shell access.

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.

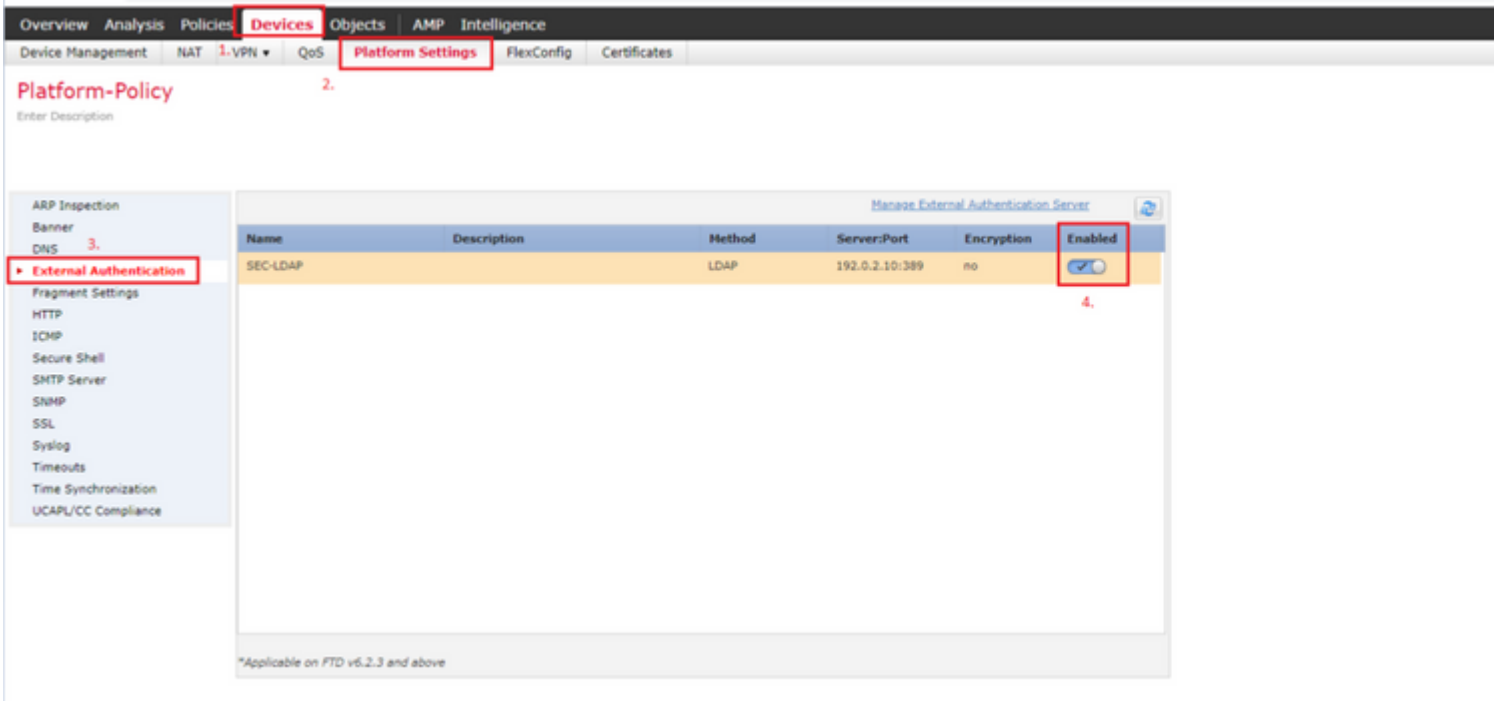
Once shell access for external users is configured, login via SSH is enabled as seen in the image:



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

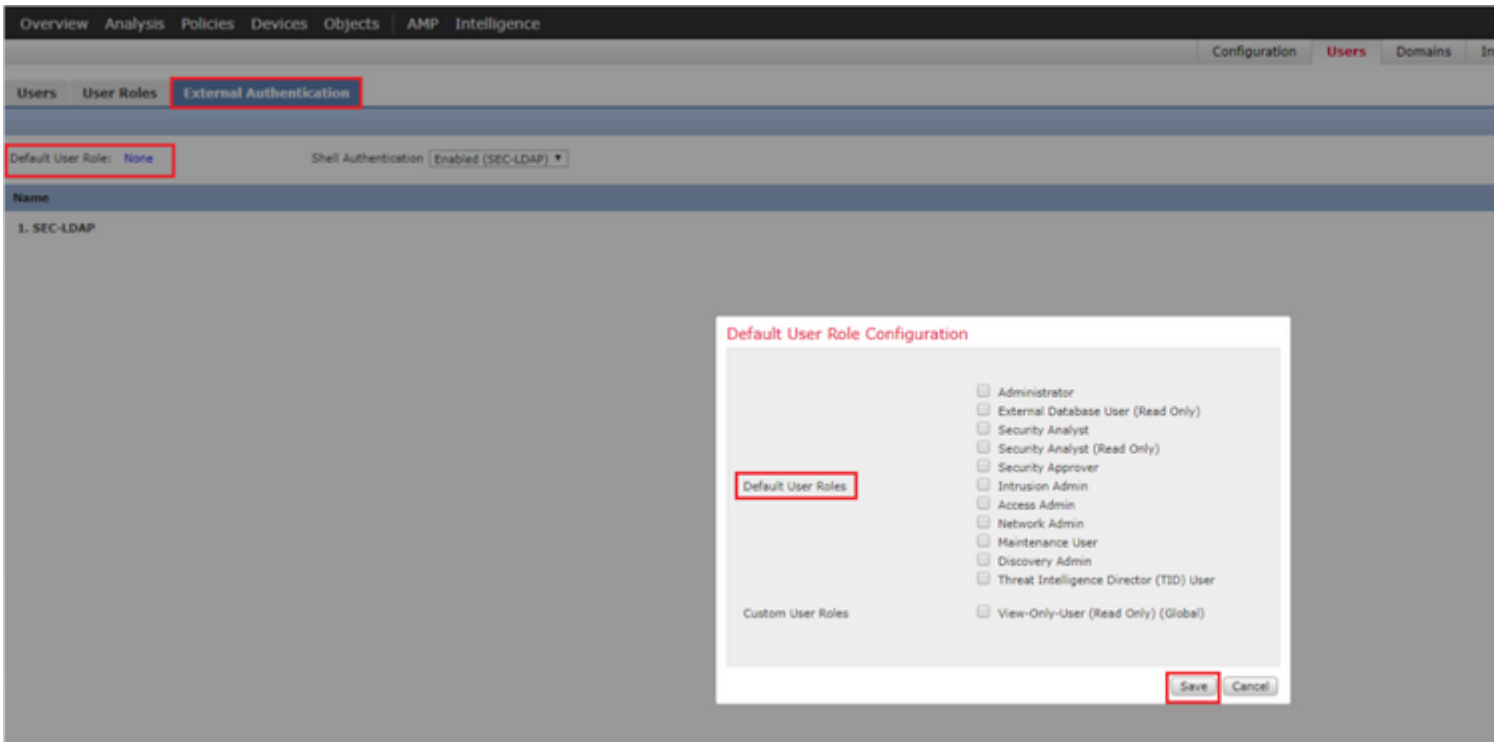
User privileges are based on the assigned user role. You can also create custom user roles with access privileges tailored to the needs of your organization or you can use predefined roles such as Security Analyst and Discovery Admin.

There are two types of user roles:

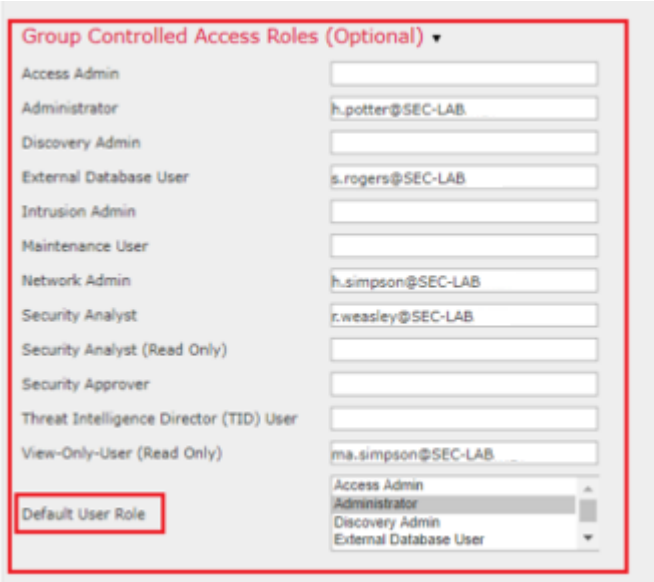
1. Web Interface User Roles
2. CLI User Roles

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:



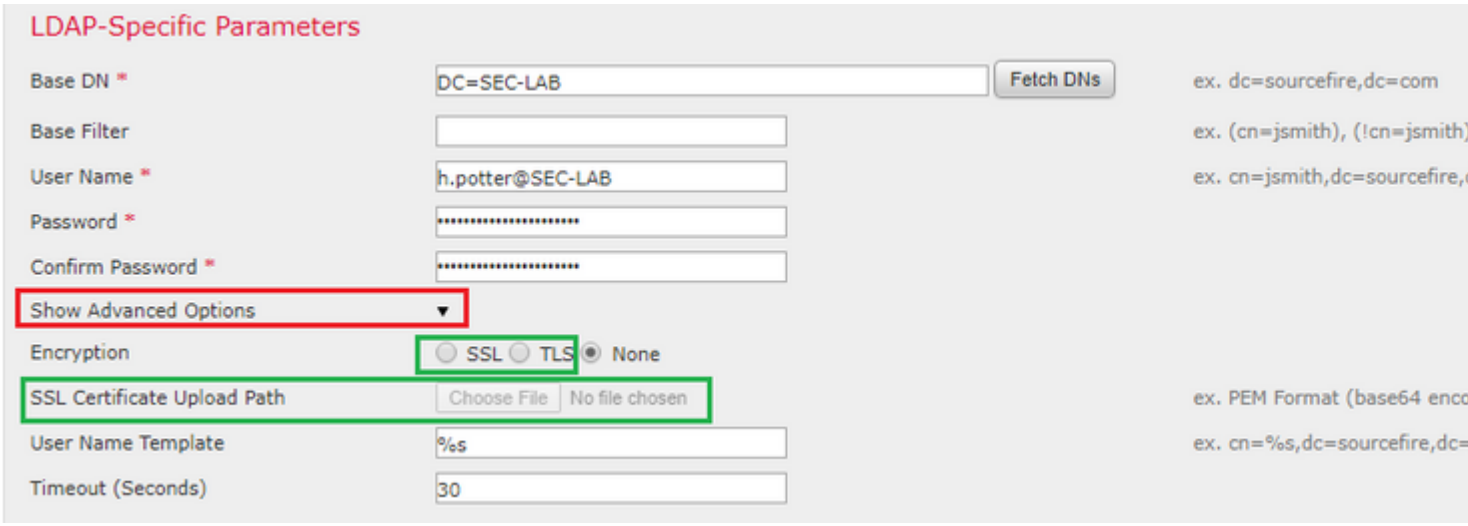
SSL or TLS

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.

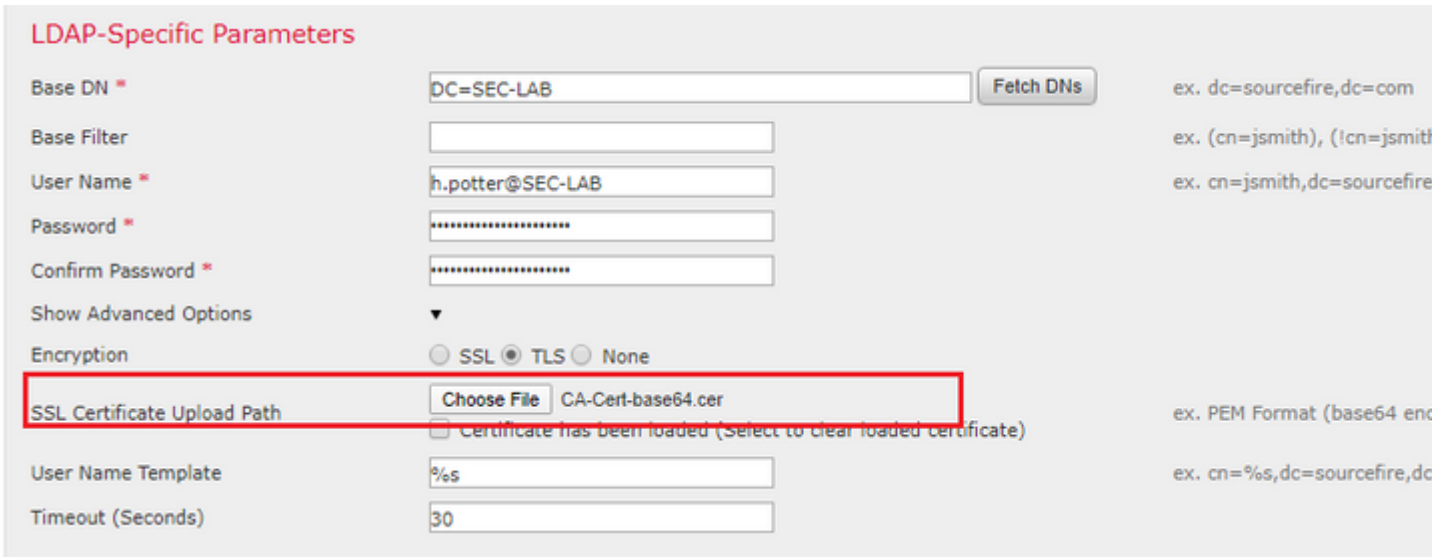
SSL changes the default port to 636, and TLS keeps it as 389.

> **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:



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



Step 3. Save the configuration.

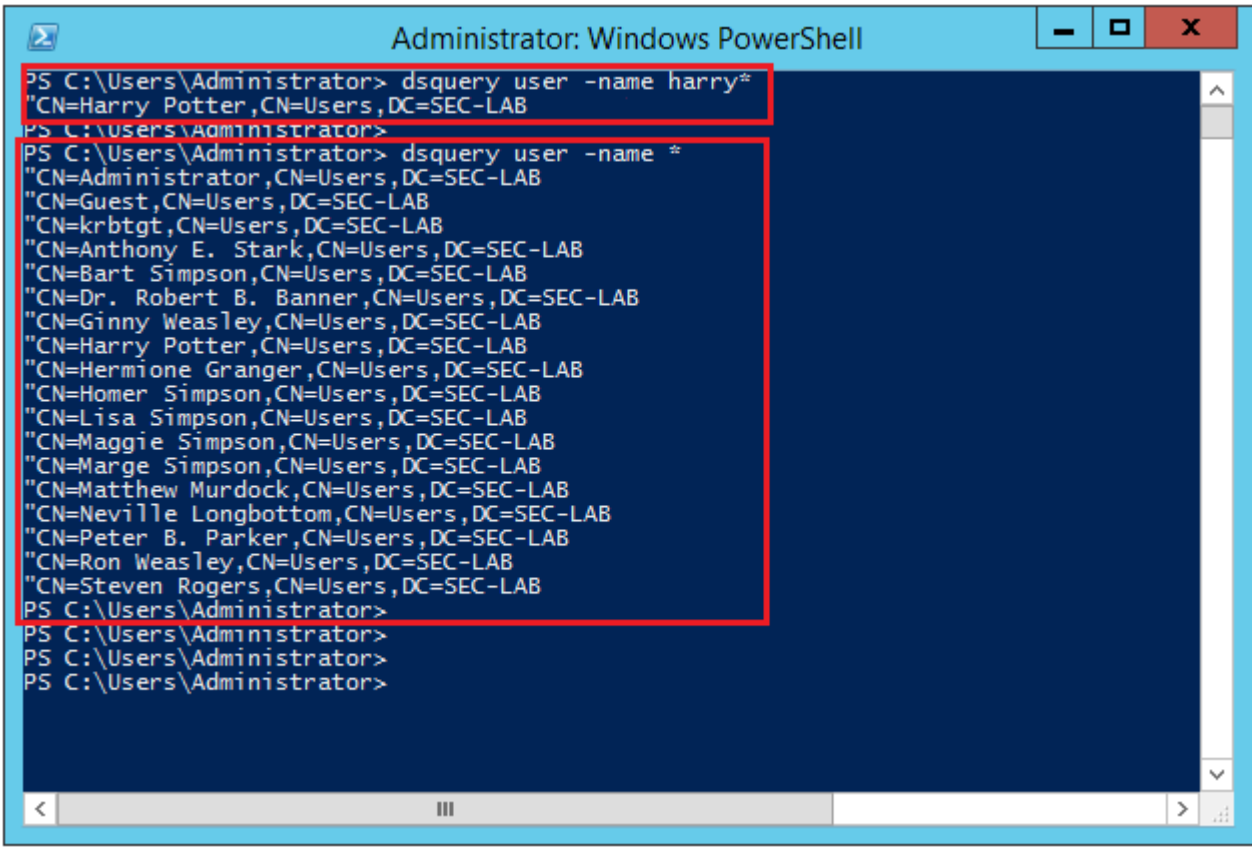
Verify

Test Search Base

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

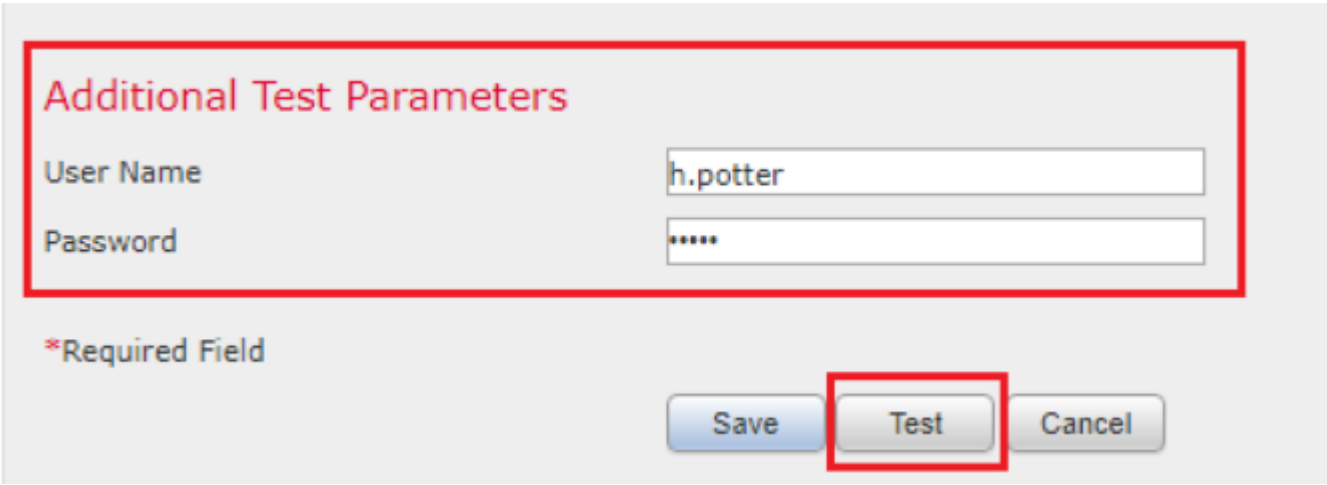
For example:

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

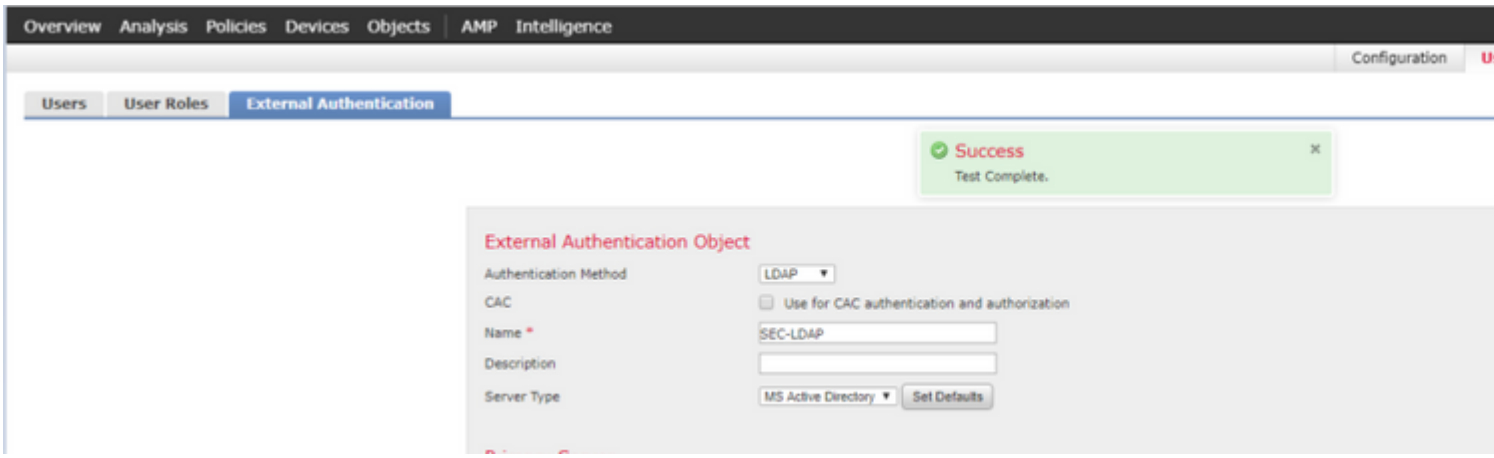


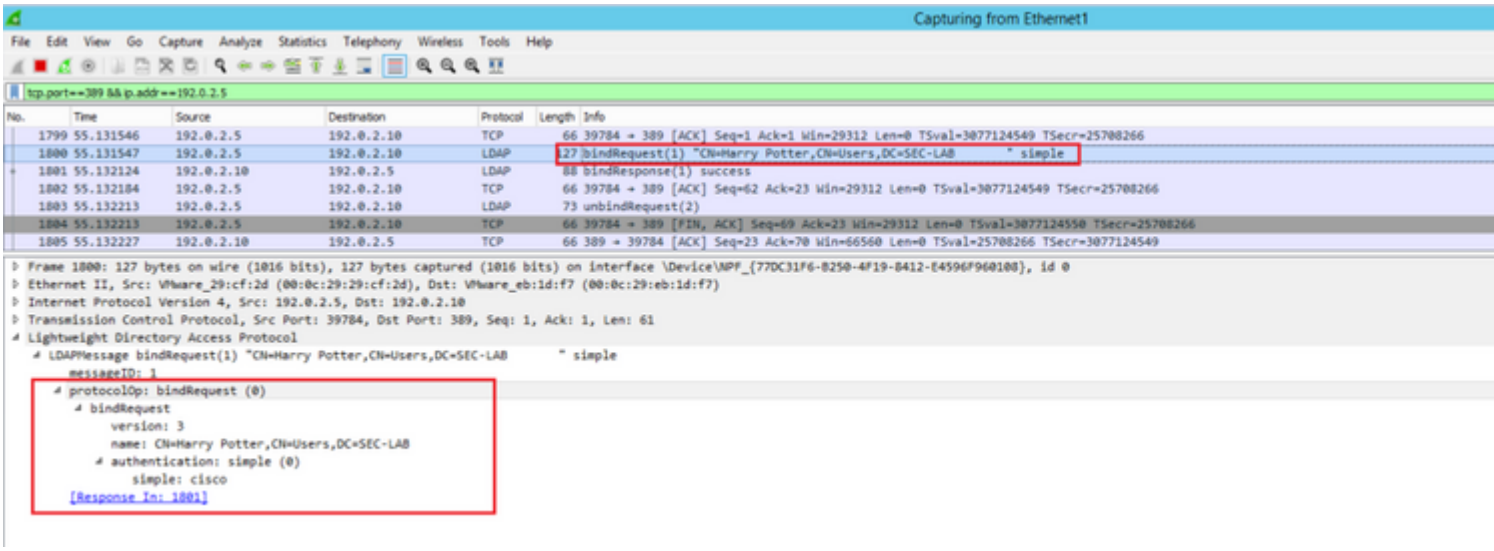
Test LDAP Integration

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:



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:

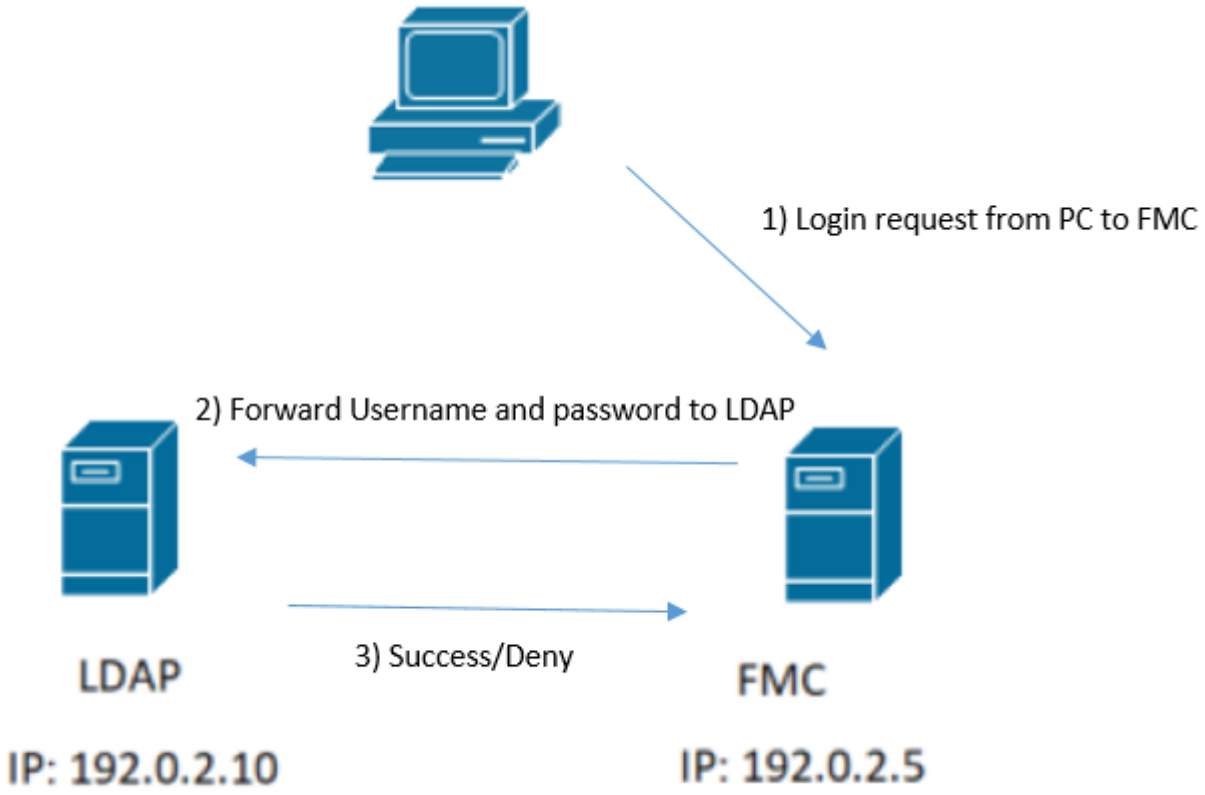
<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << --- FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

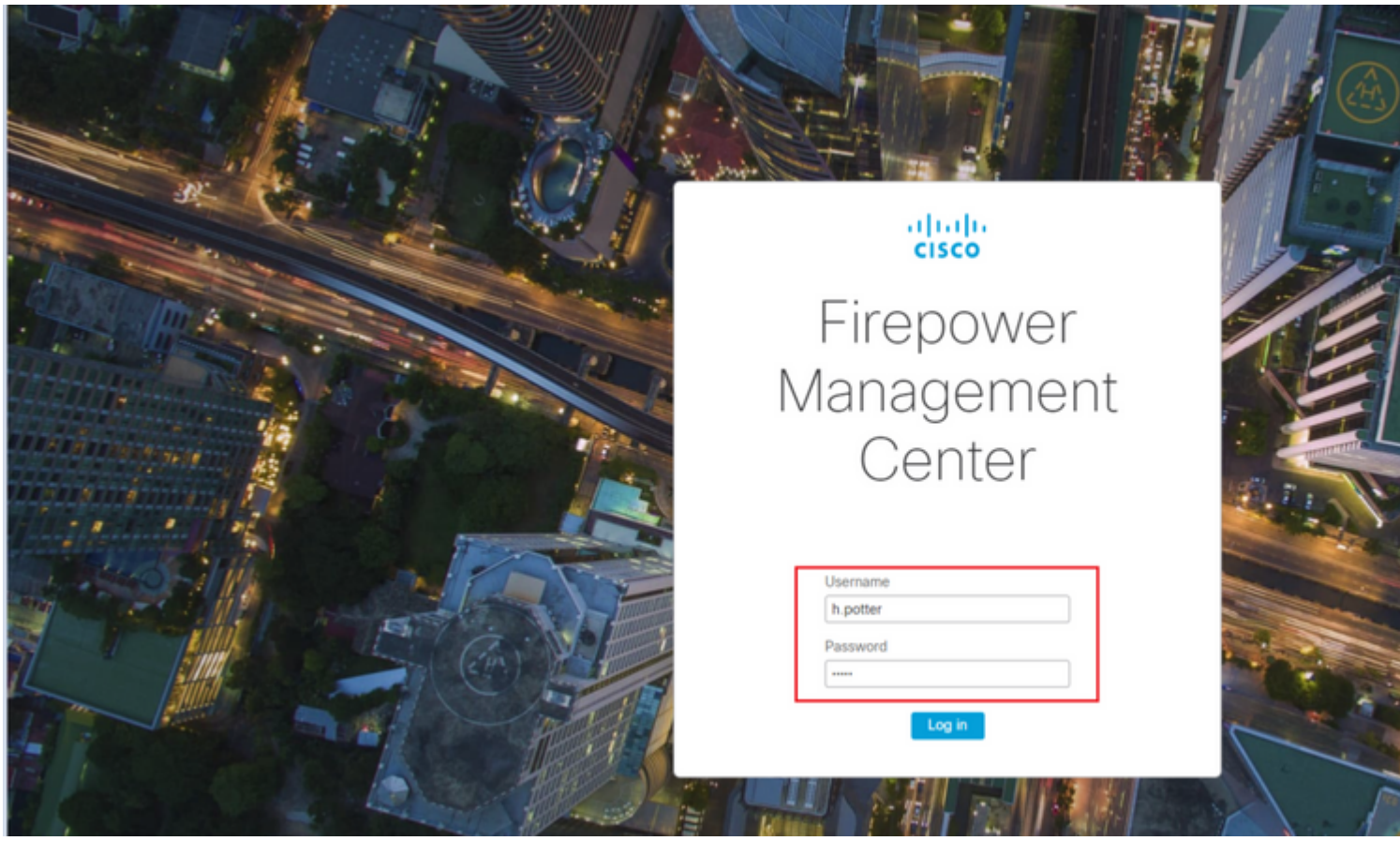
Notice that the authentication sends passwords in the clear by default:

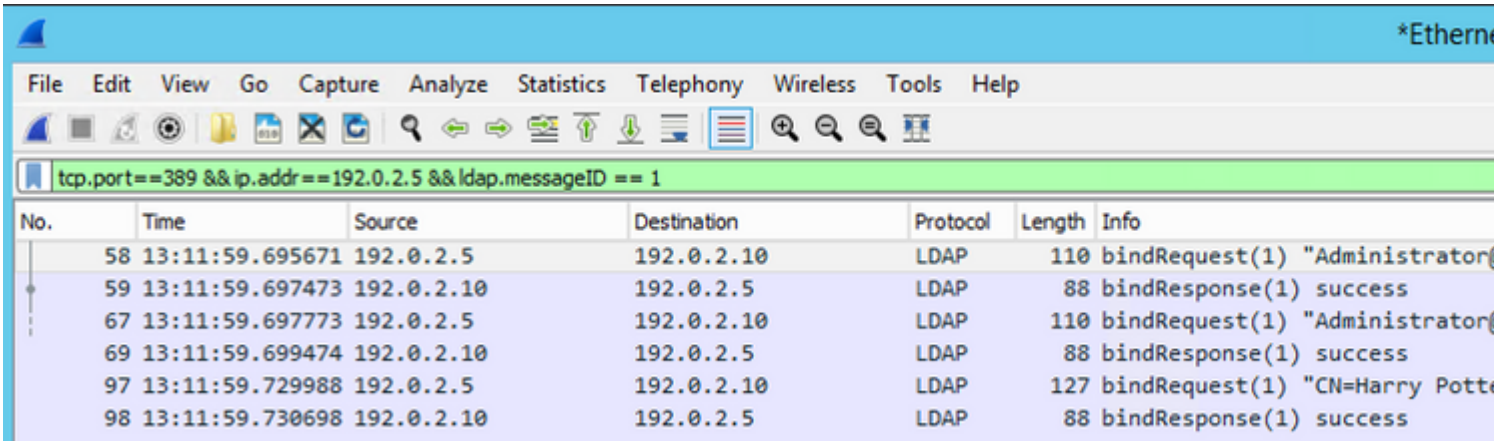
```
    83 4.751887    192.0.2.5     192.0.2.10    TCP      74 38002 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3073529344 T
    84 4.751920    192.0.2.10    192.0.2.5     TCP      74 389 → 38002 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 T
    85 4.751966    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=2534874
    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: Ciscot@c
    [Response In: 87]
```

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

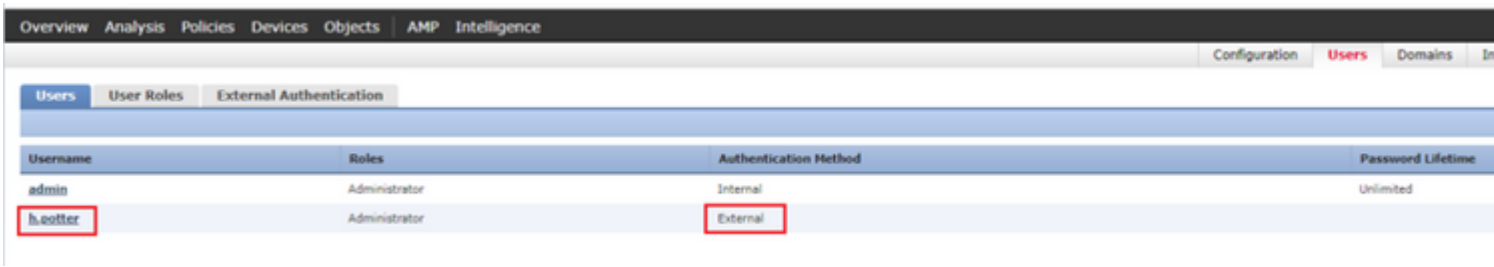
In order for a user to be able to log in to FMC or FTD while LDAP authentication is enabled, the initial login request is sent to Firepower, however, the username and password are forwarded to LDAP for a success/deny response. This means that FMC and FTD do not keep password information locally in the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







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



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 â€" 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

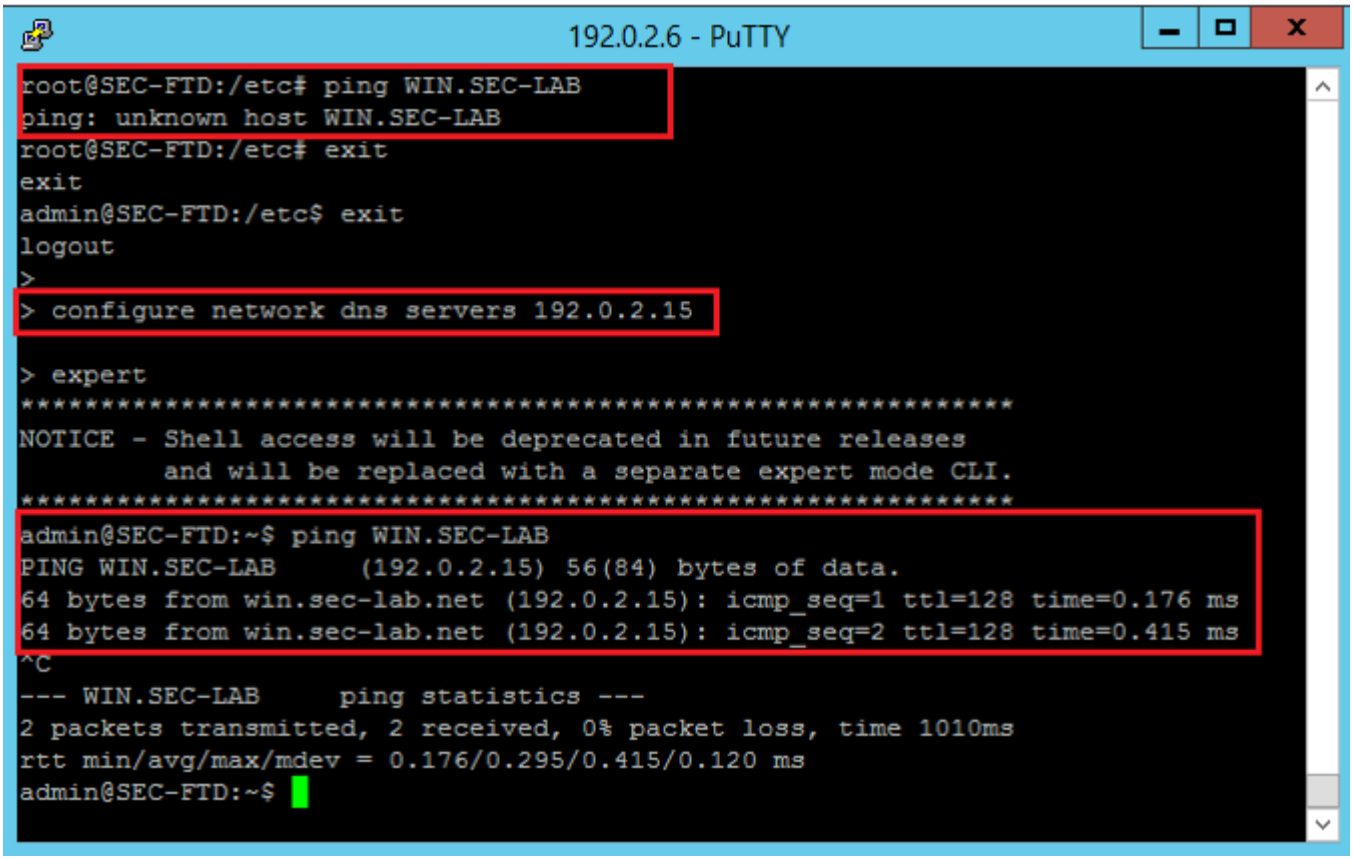
If you do not enable DNS on the FTDs, you can see errors in the pigtail log that suggest that LDAP is unreachable:

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

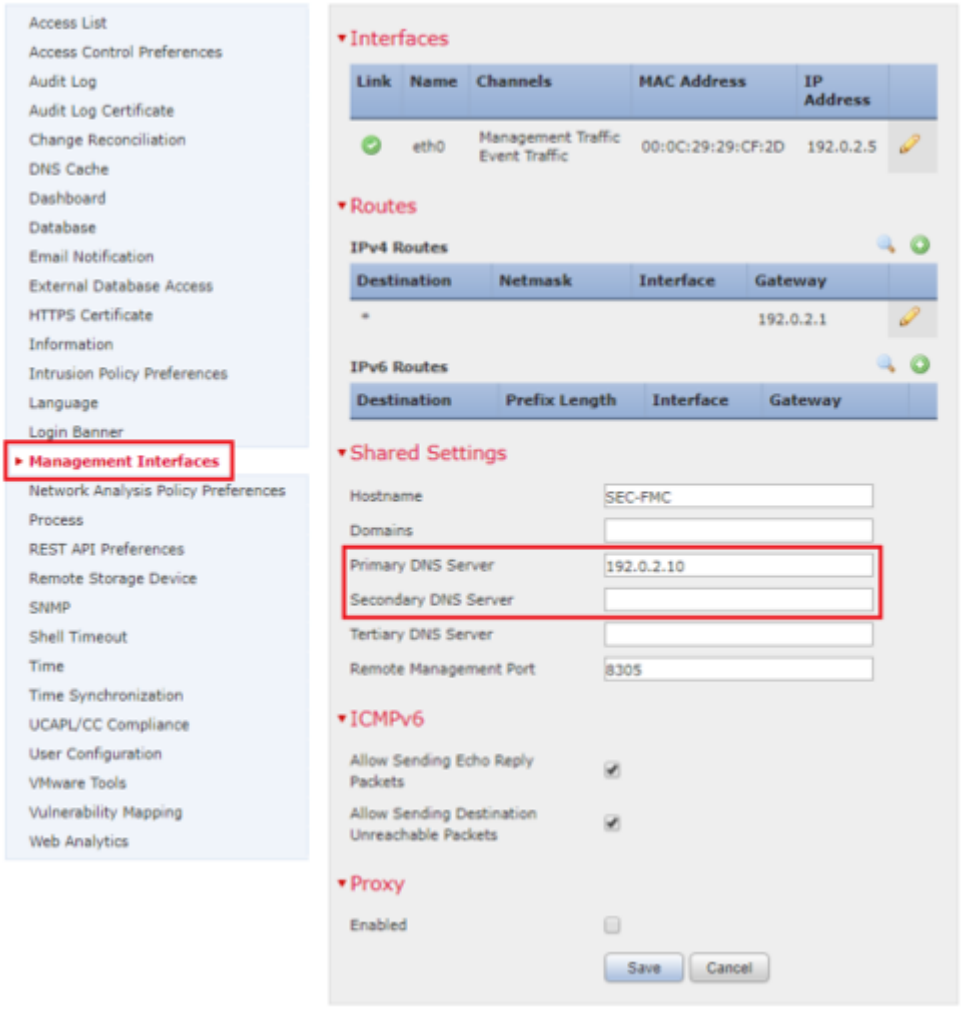
```
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eu
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2.1
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15 p
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter f
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 614
```

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

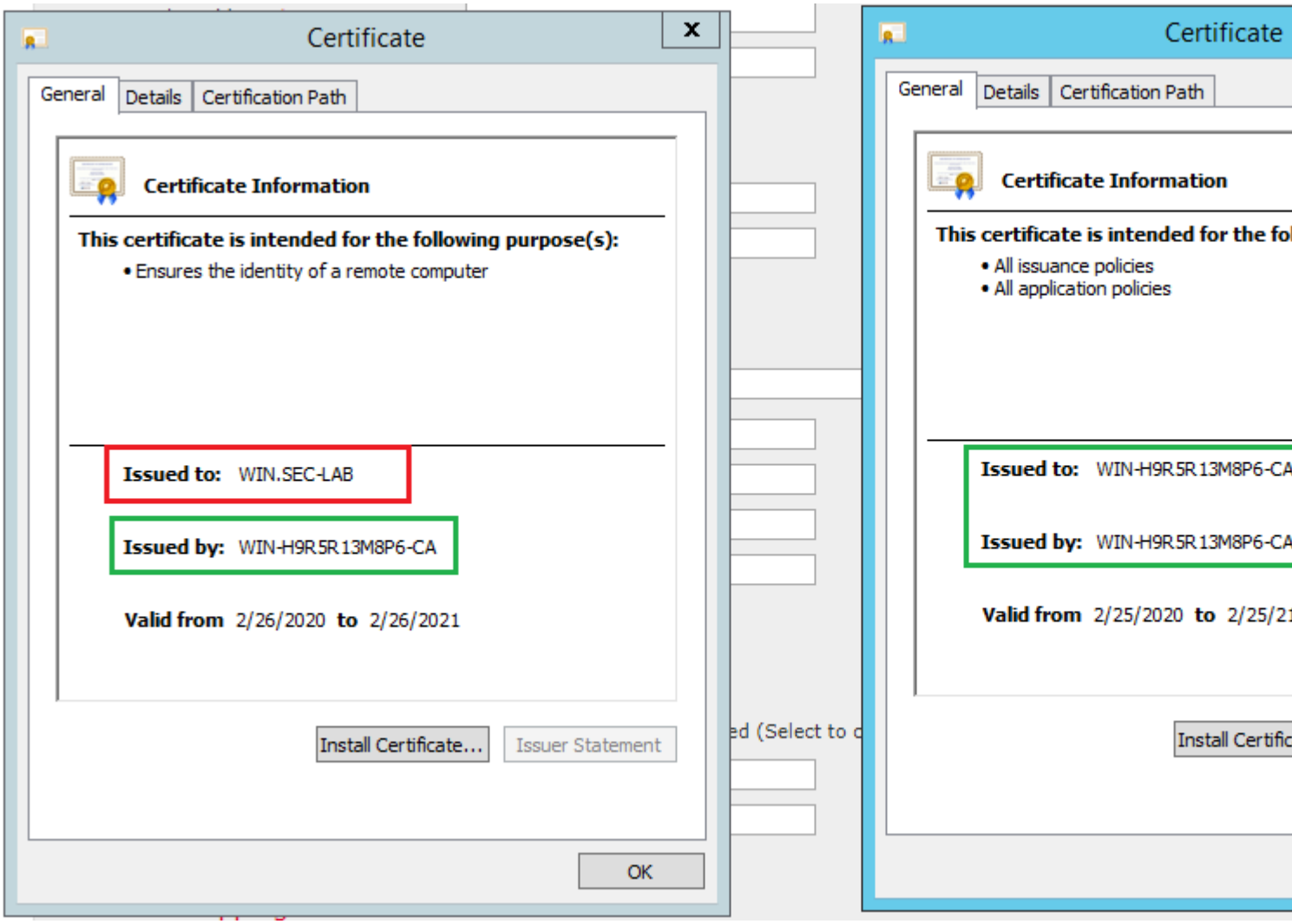
FTD: Access the FTD CLISH and run the command: > configure network dns servers <IP Address>.



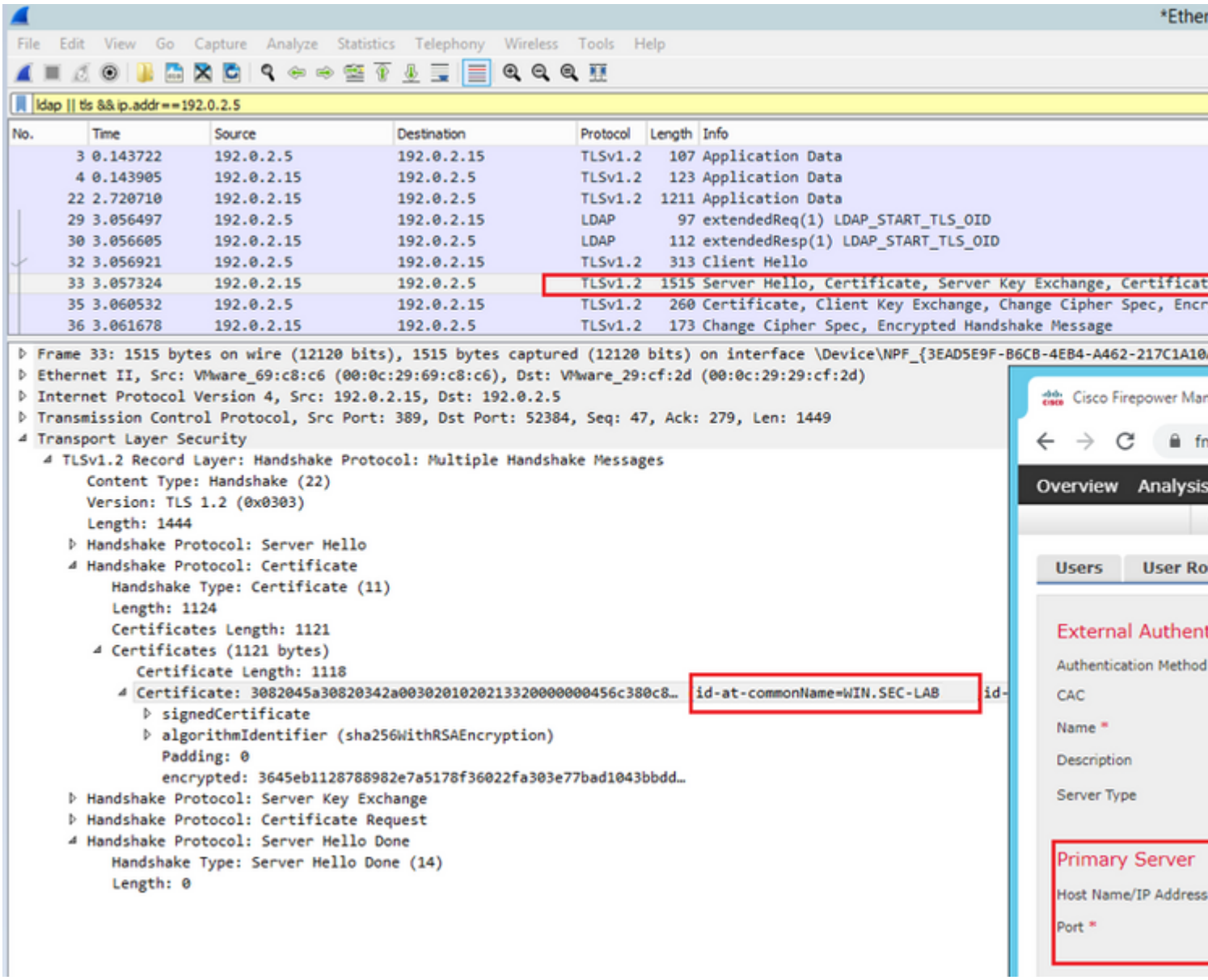
FMC: Choose System > Configuration, and then choose Management Interfaces as seen in the image:



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:



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]