Configure FMC 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 Log In 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 FMC and FTD.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower Threat Defense (FTD)
- Cisco Firepower Management Center (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



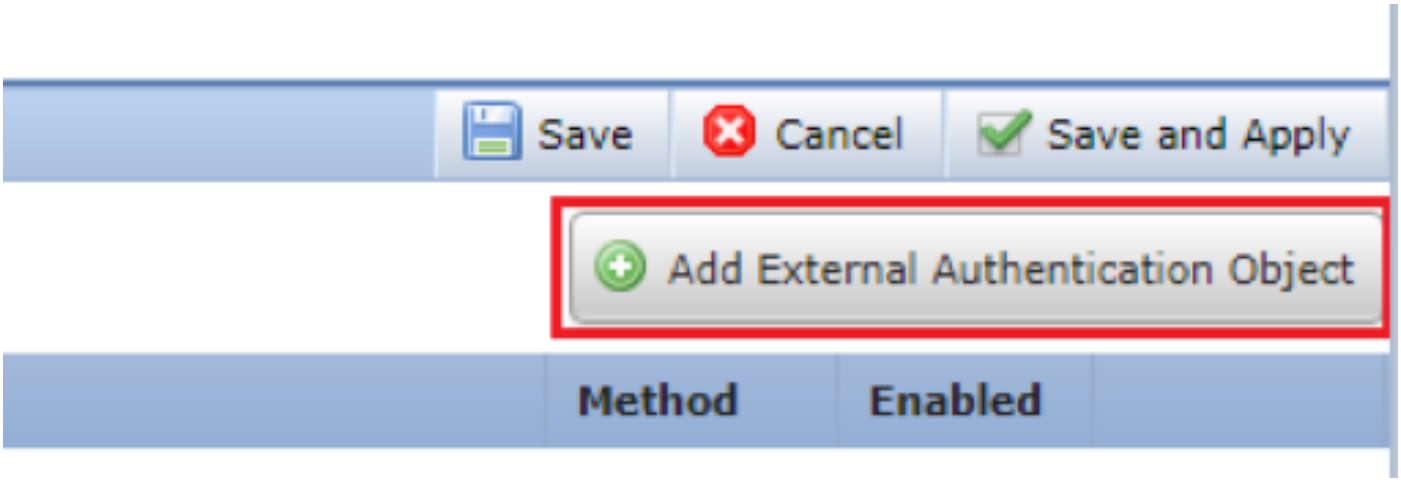
Configure

Basic LDAP Configuration in FMC GUI

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

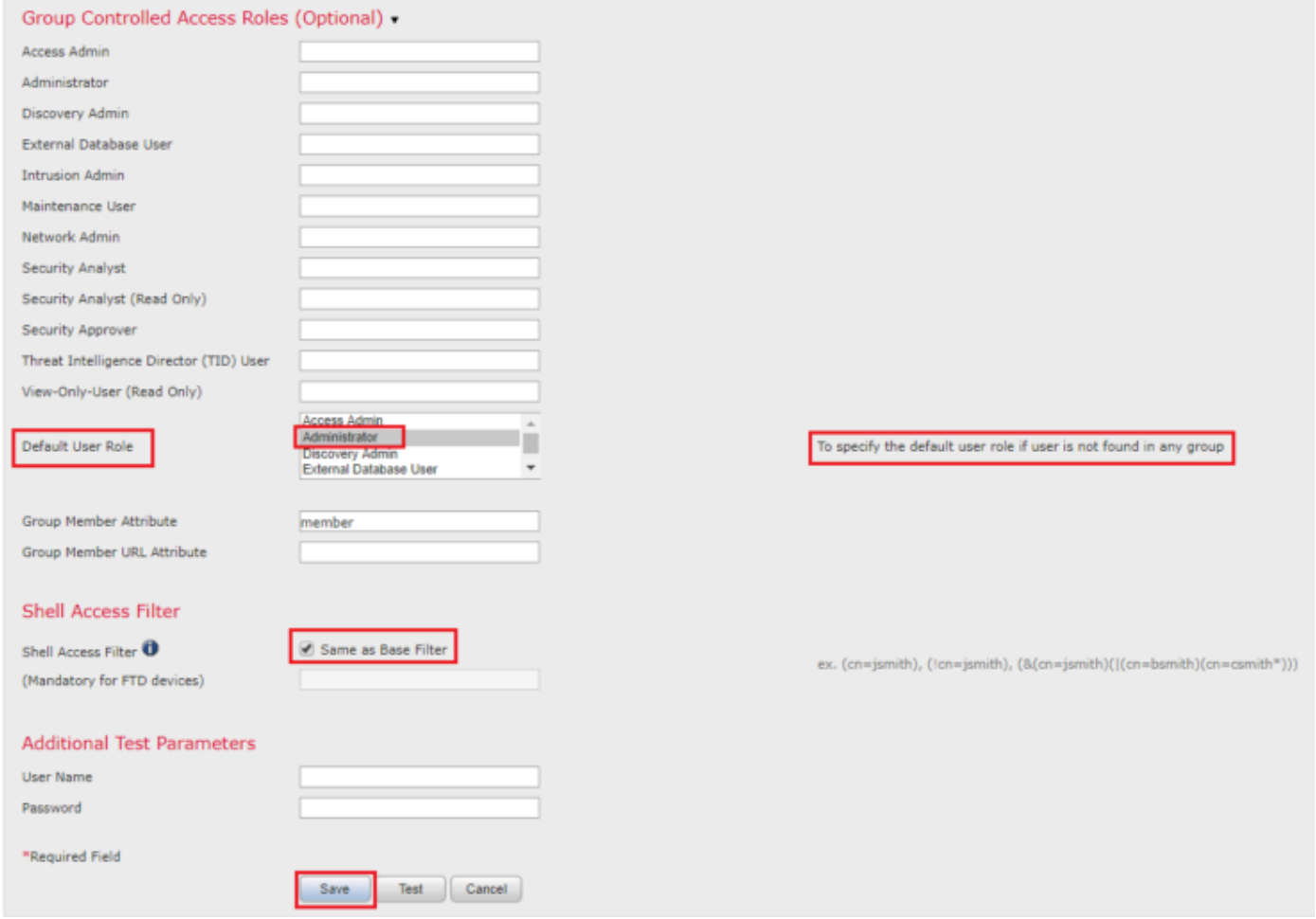


Step 2. Choose Add External Authentication Object:



Step 3. Complete the required fields:





Step 4. Enable 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.

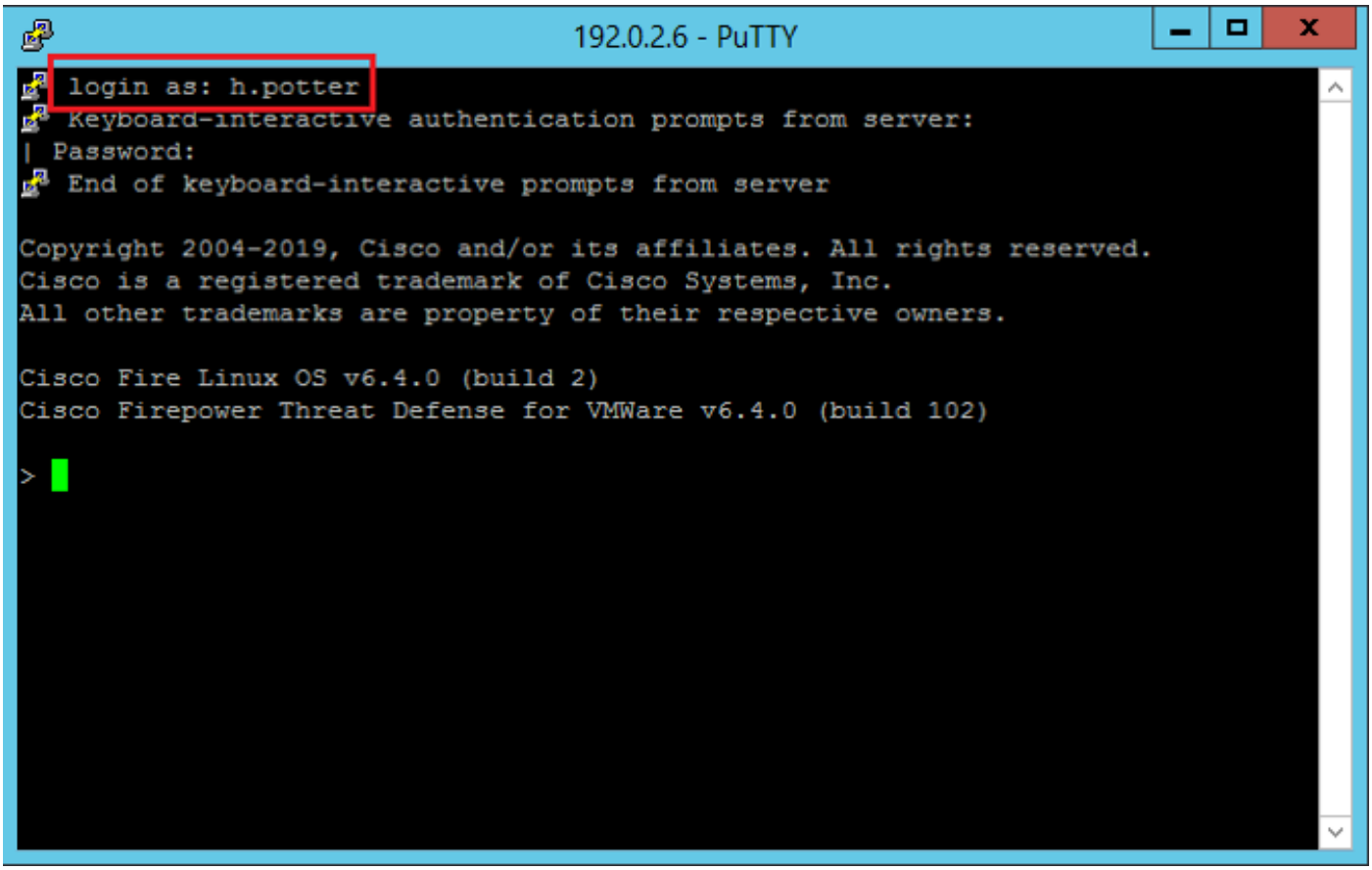
LDAP External users must also be granted shell access.

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.

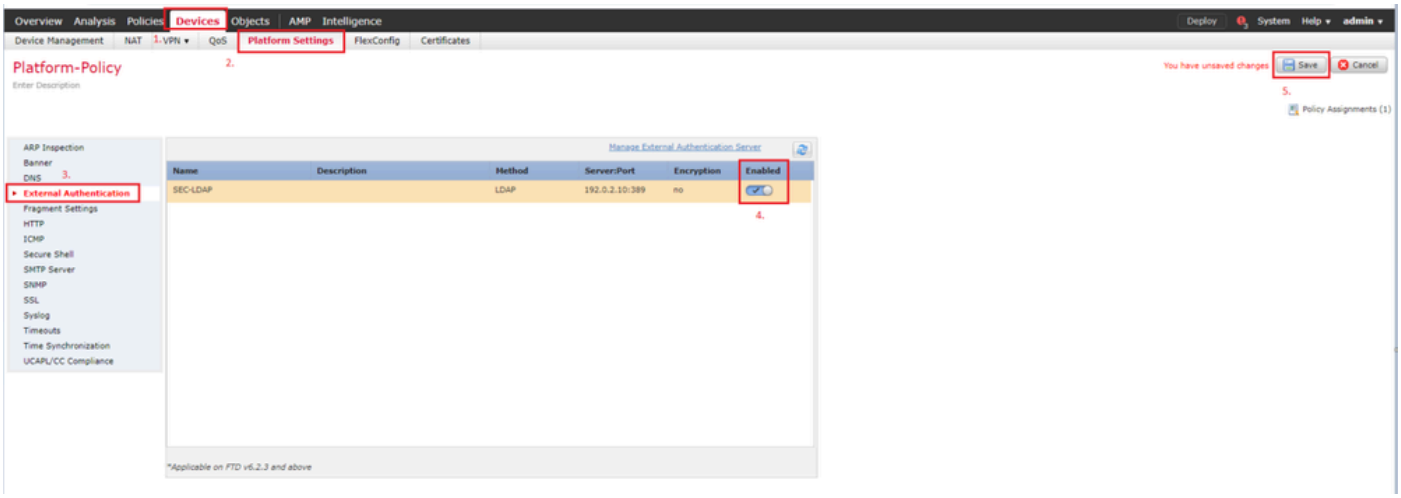
Once shell access for external users is configured, log in via SSH is enabled as seen in the image:



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

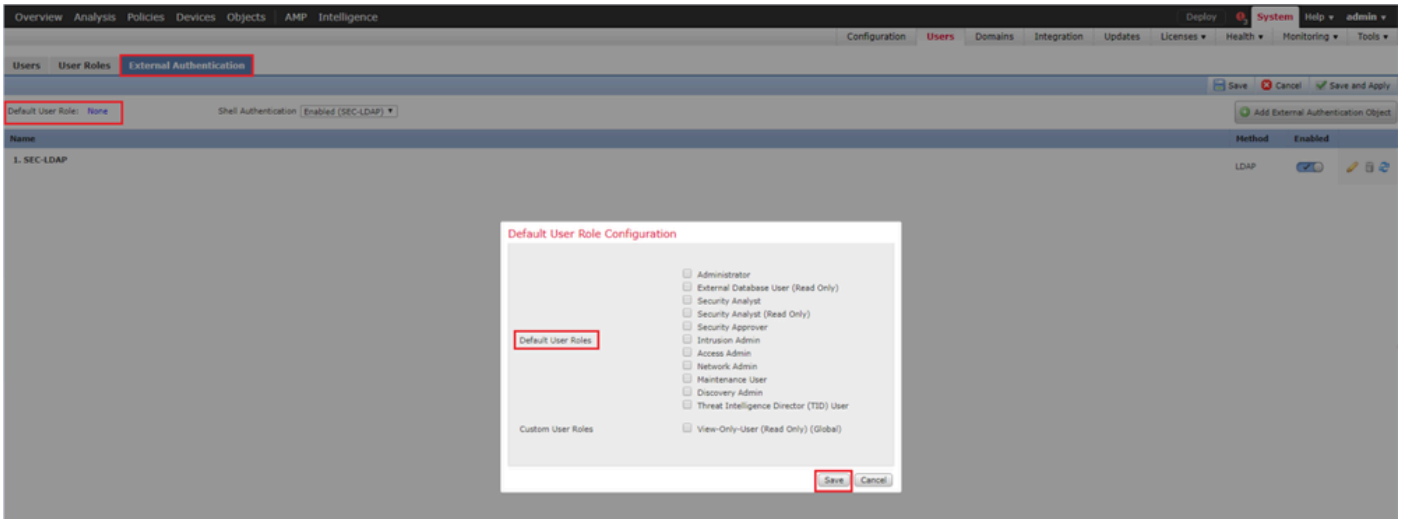
and Discovery Admin.

There are two types of user roles:

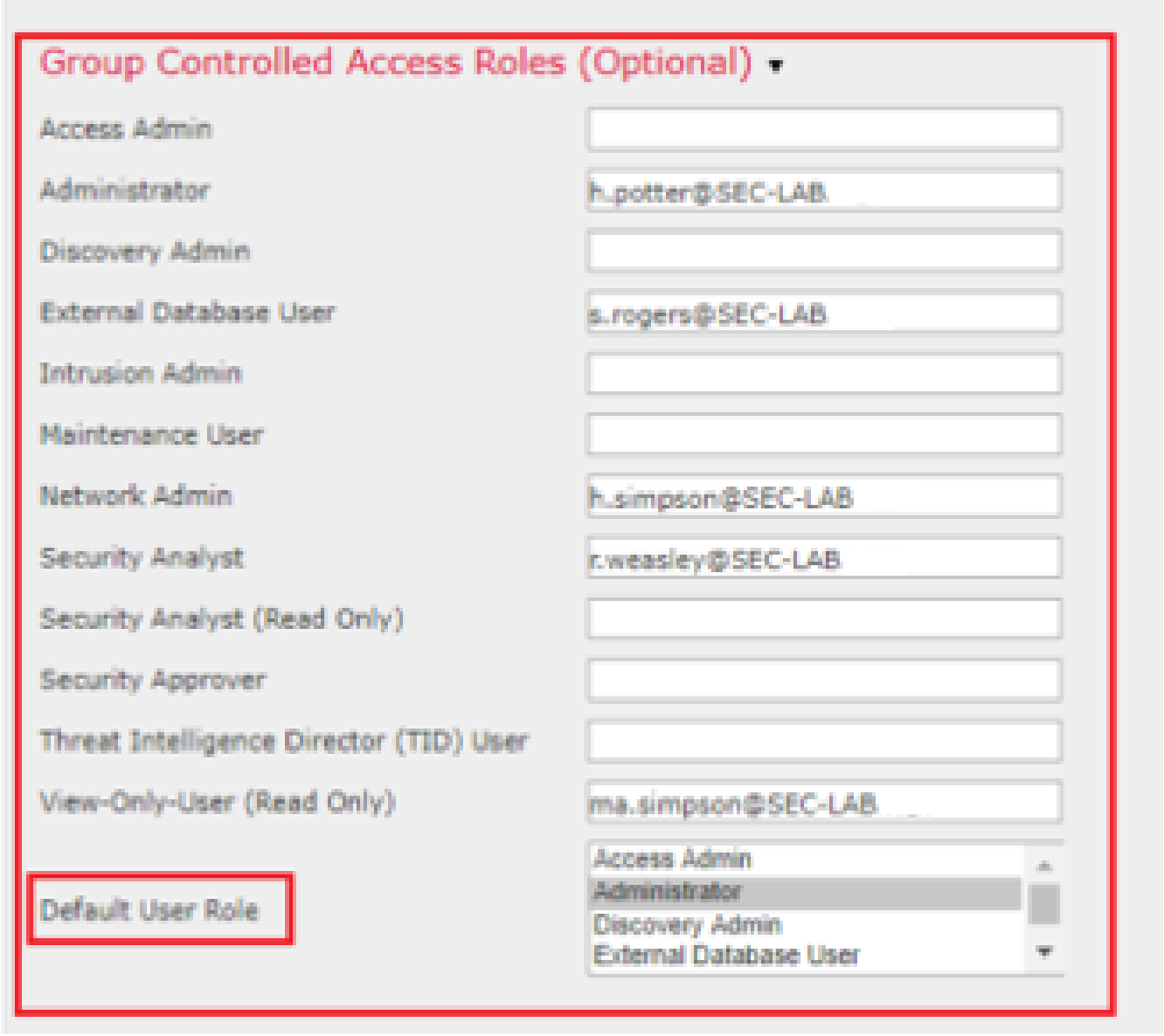
1. Web Interface User Roles
2. CLI User Roles

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:



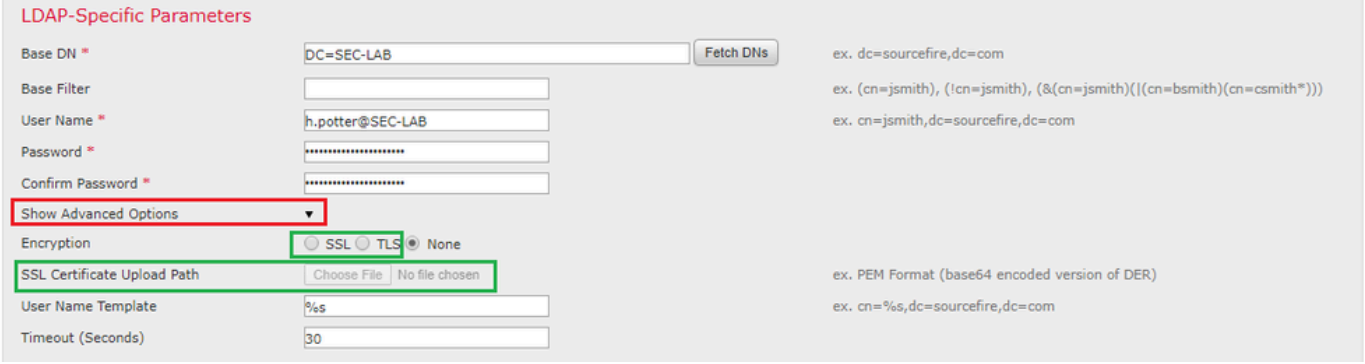
SSL or TLS

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.

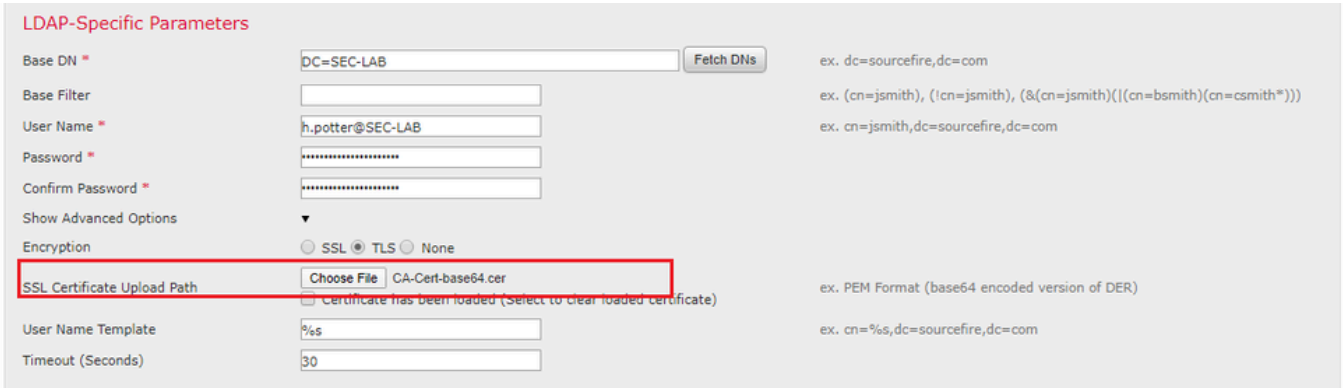
SSL changes the default port to 636, and TLS keeps it as 389.

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.

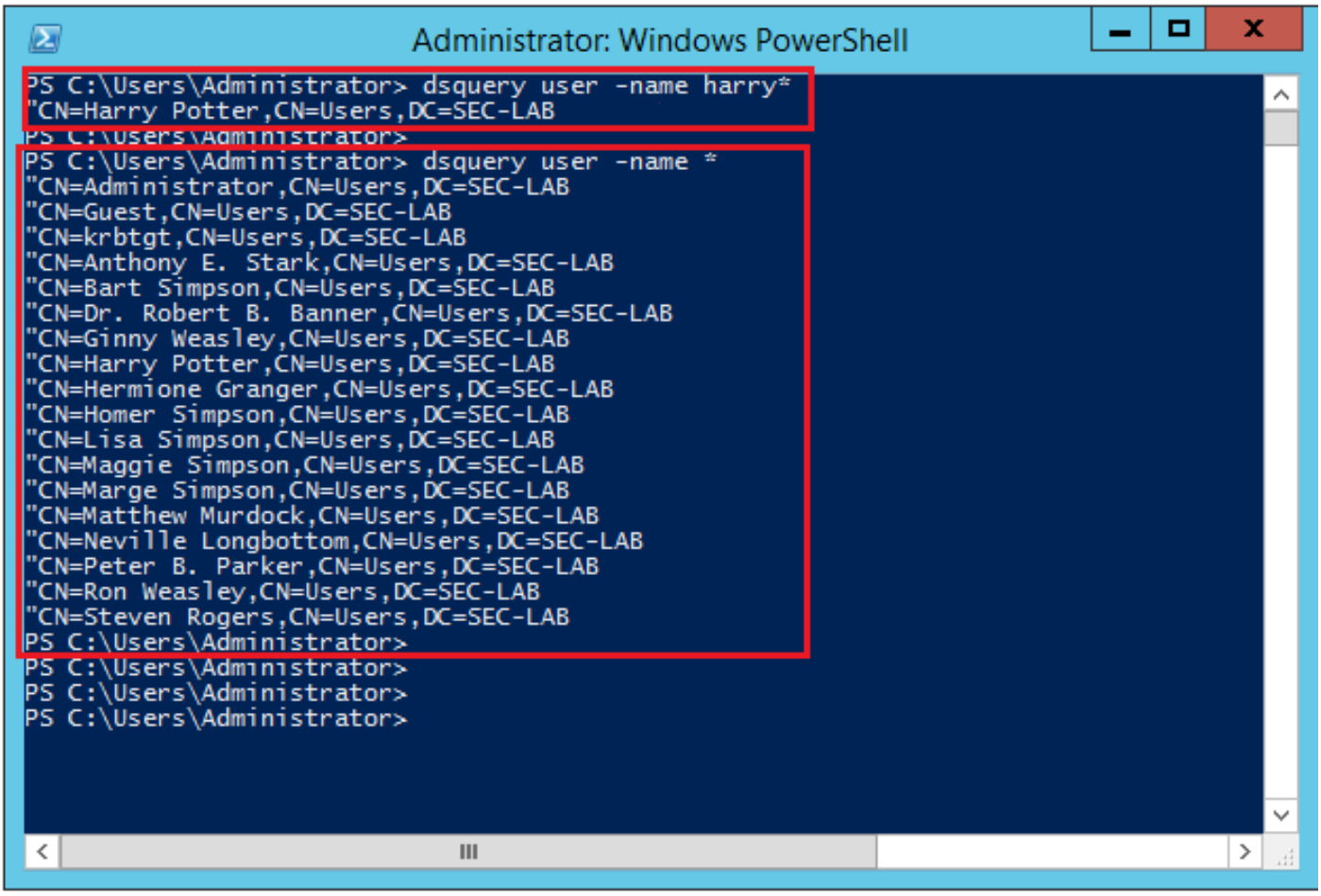
Verify

Test Search Base

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

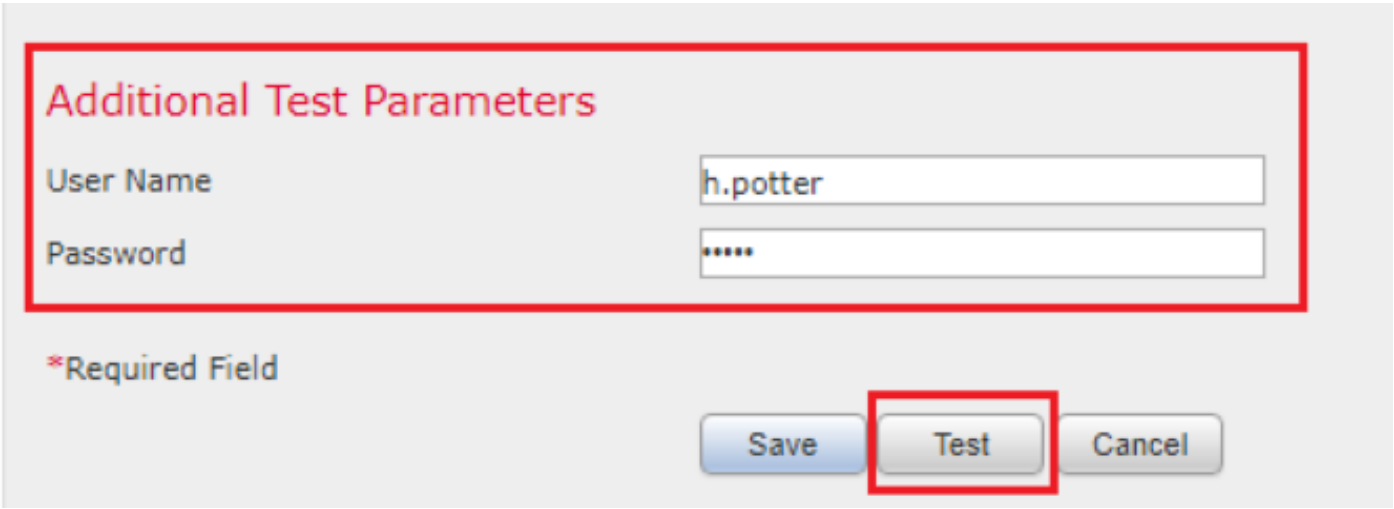
For example:

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

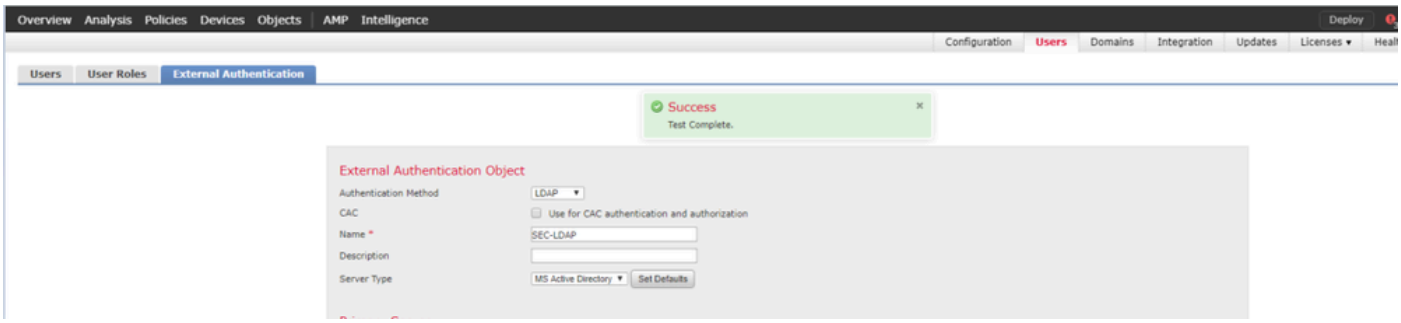


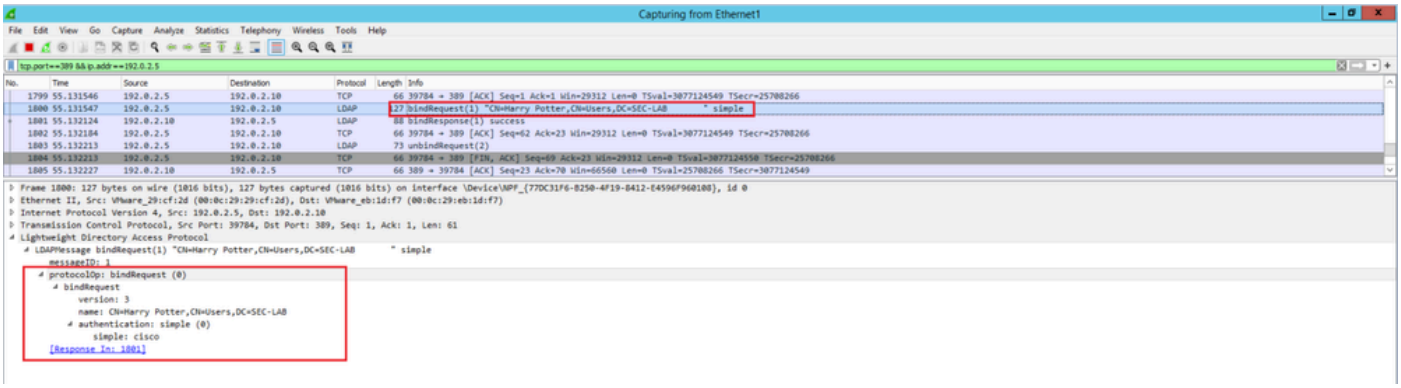
Test LDAP Integration

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 **Test** in order to see the results.





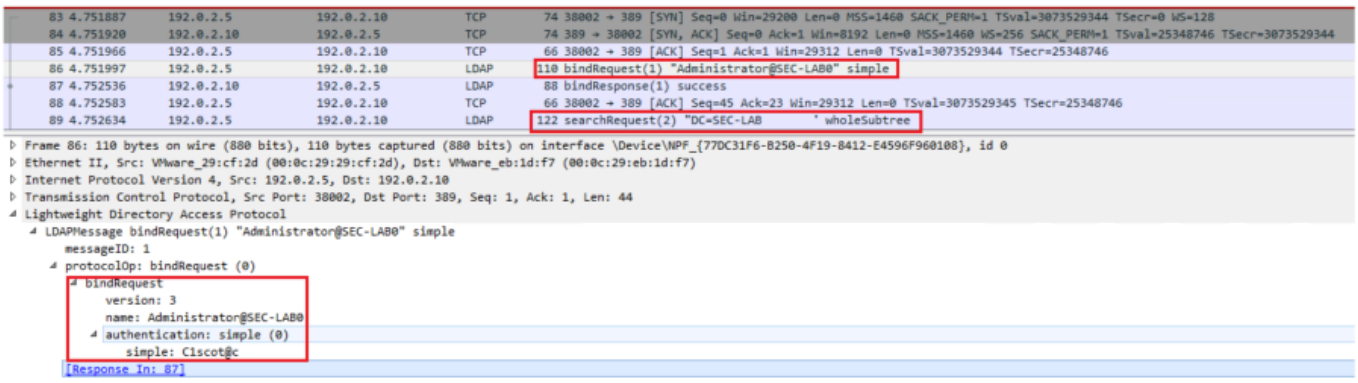
Troubleshoot

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

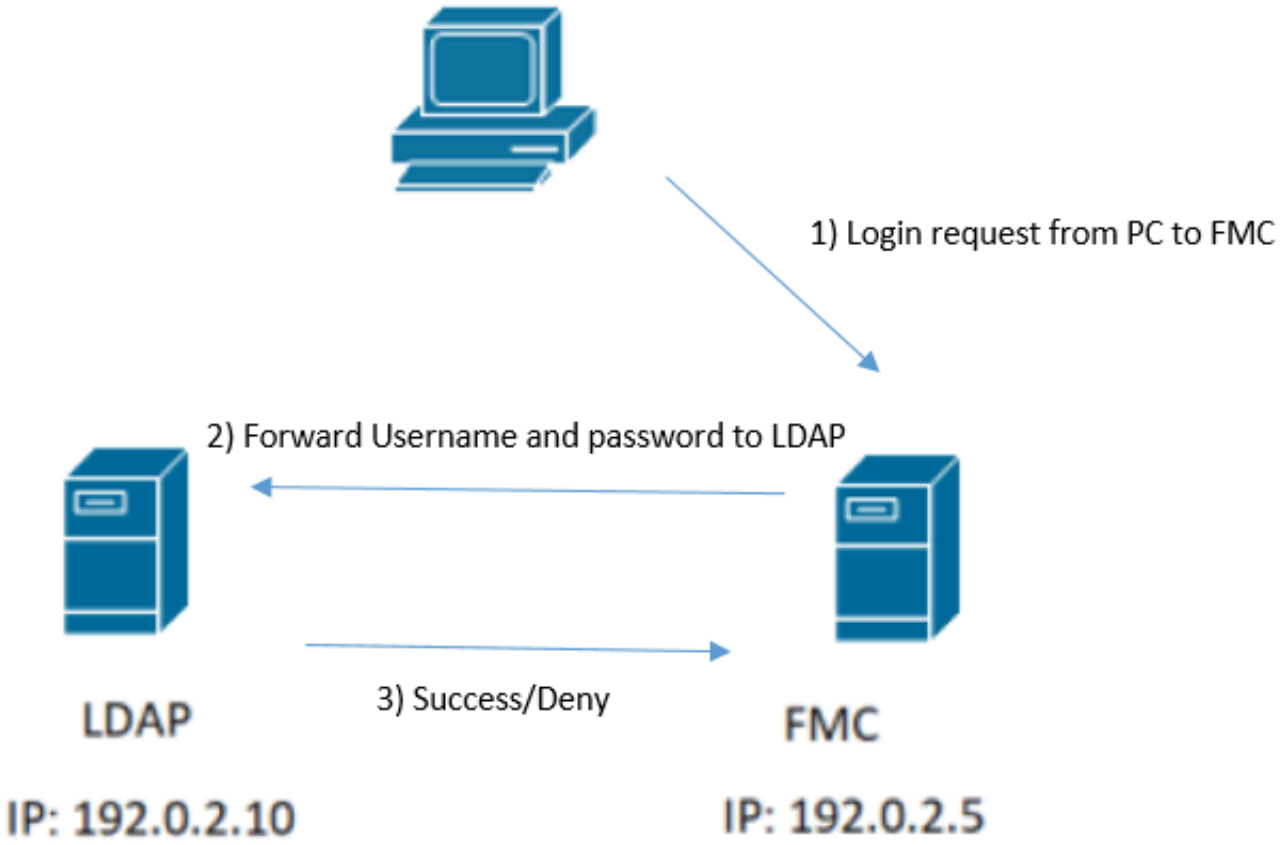
Notice that the authentication sends passwords in the clear by default:

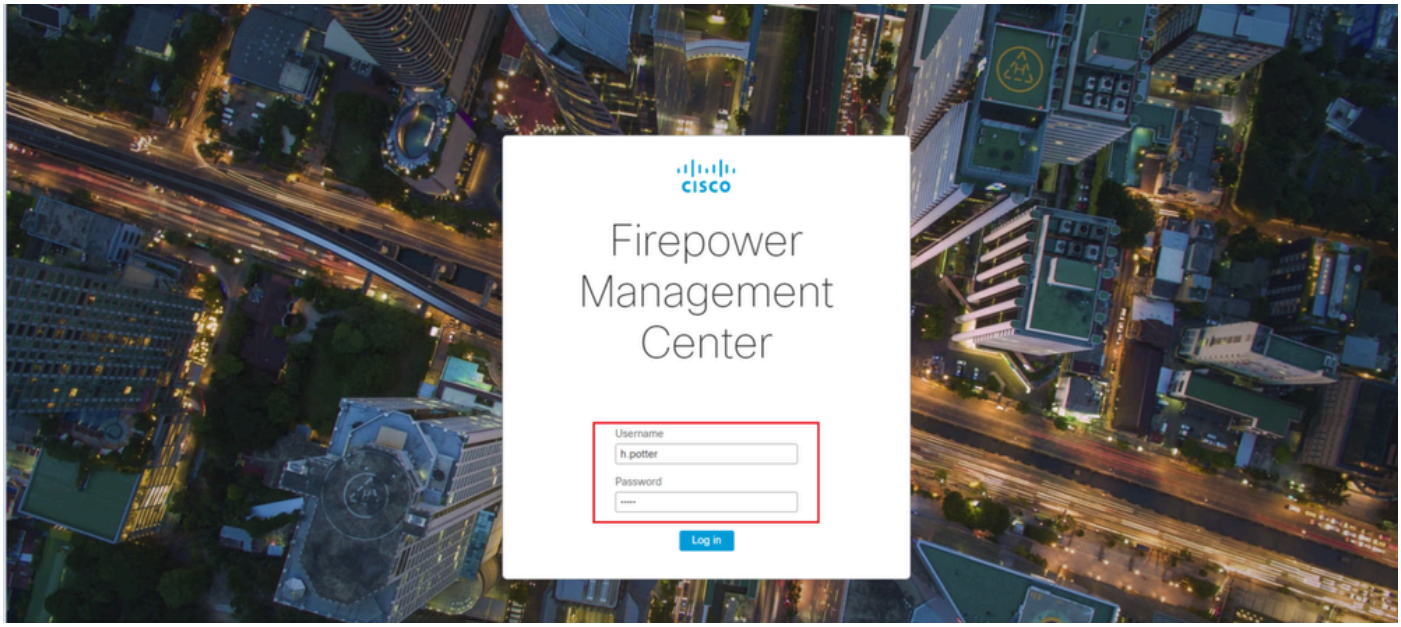


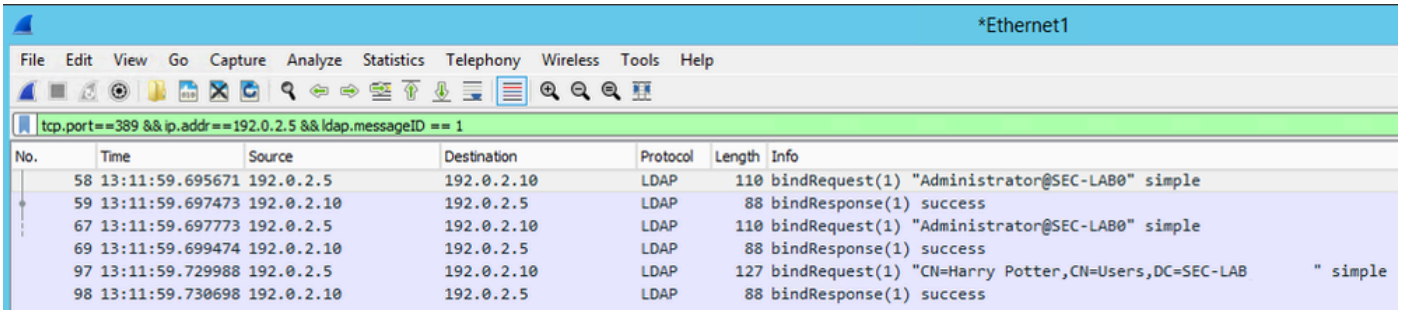
How Do FMC/FTD and LDAP Interact to Authenticate a User Log In Request

In order for a user to be able to log in to FMC or FTD while LDAP authentication is enabled, the initial log in 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:

Log in — the log in name

UID — the numeric user ID
Auth (Local or Remote) — how the user is authenticated
Access (Basic or Config) — the privilege level of the user
Enabled (Enabled or Disabled) — whether the user is active
Reset (Yes or No) — whether the user must change the password at the next log in
Exp (Never or a number) — the number of days until the password of the user must be changed
Warn (N/A or a number) — the number of days a user is given in order to change their password before it expires
Str (Yes or No) — whether the password of the user must meet the criteria to check the strength
Lock (Yes or No) — whether the account of the user has been locked due to too manylog in failures
Max (N/A or a number) — the maximum number of failed log ins before the account of the user is locked

SSL or TLS does not Work as Expected

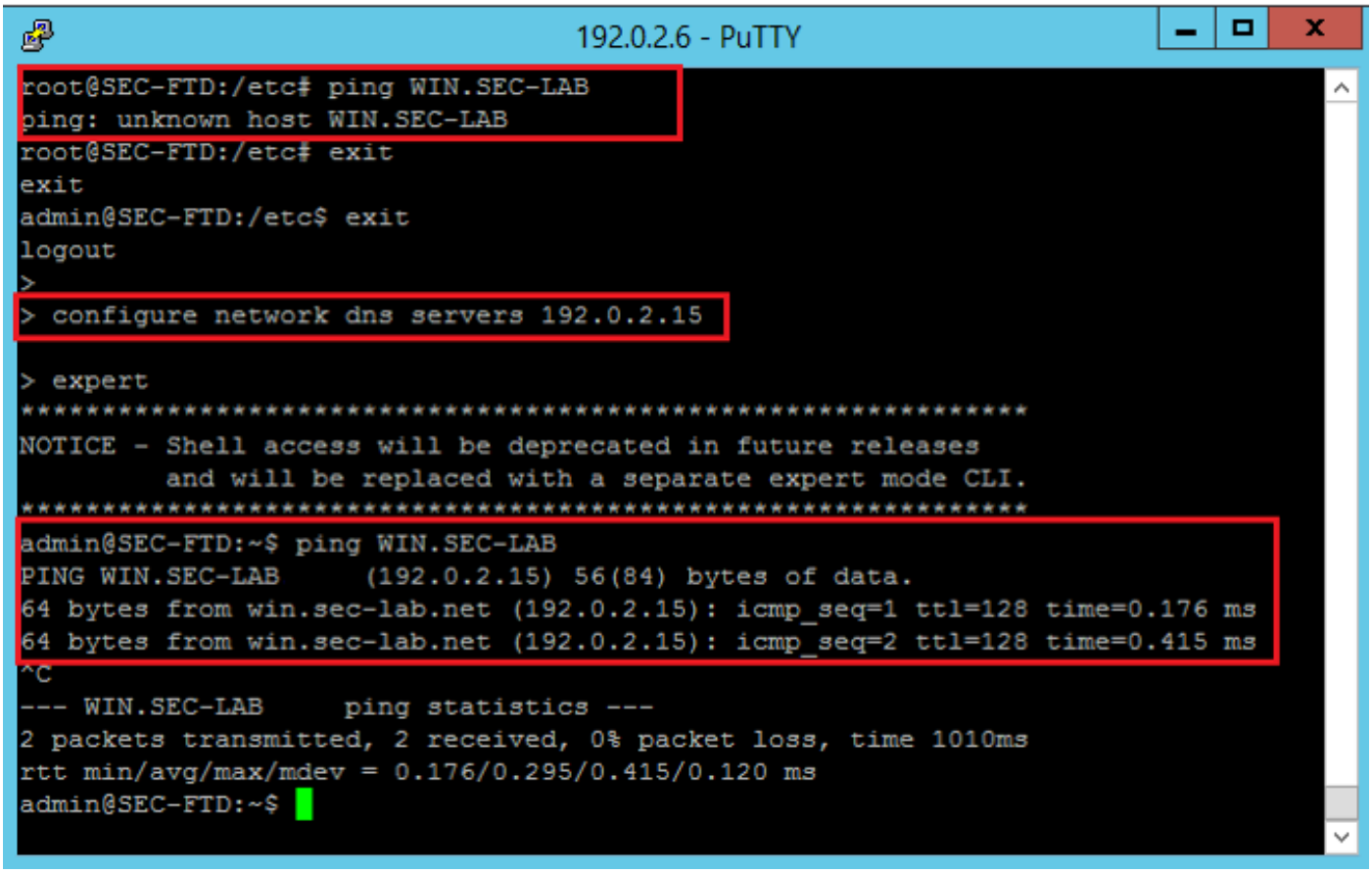
If you do not enable DNS on the FTDs, you can see errors in the pigtail log that suggest that LDAP is unreachable:

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

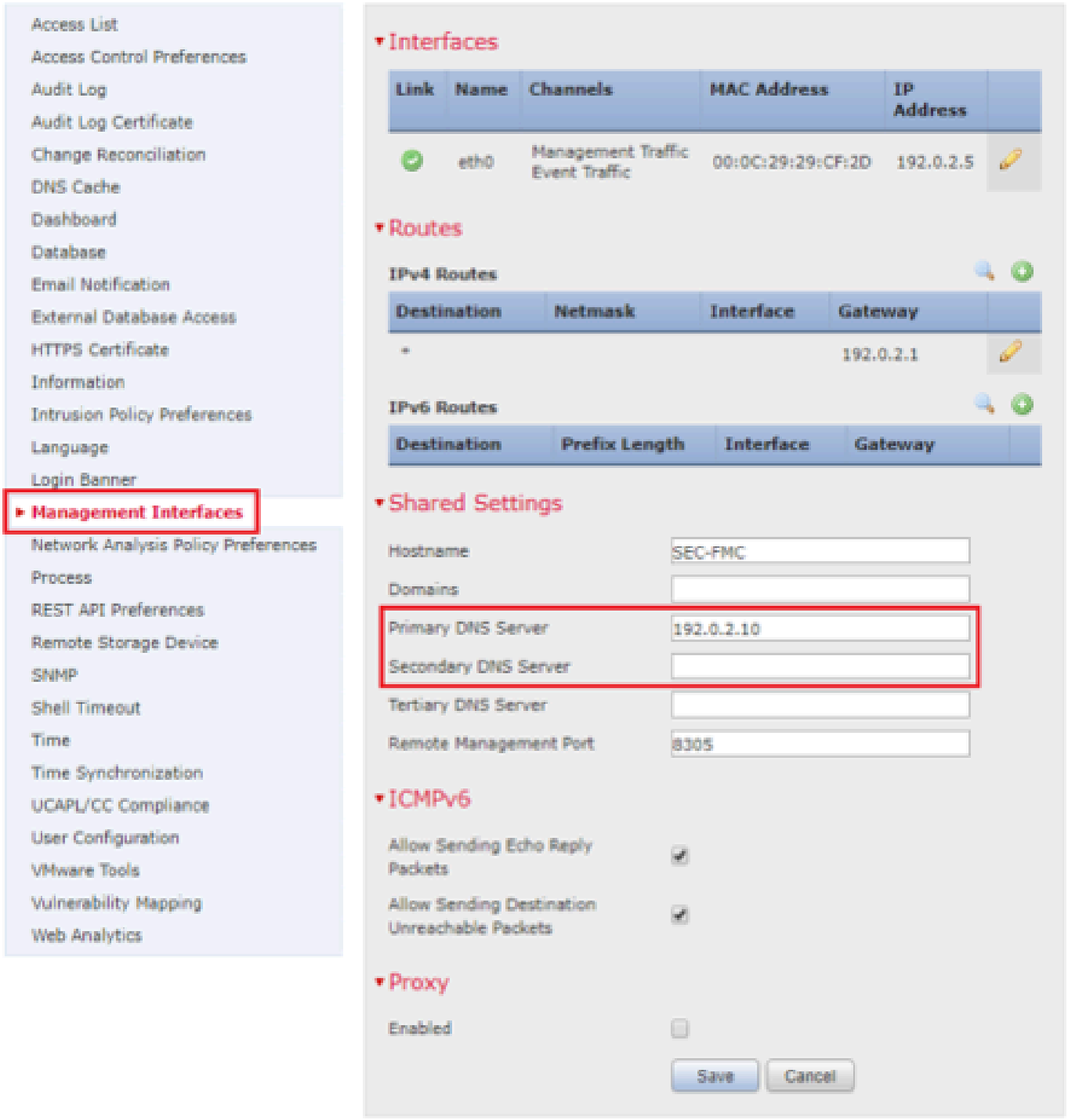
```
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2.
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
```

Ensure that Firepower is able to resolve the LDAP Servers Fully Qualified Domain Name (FQDN). If not, add the correct DNS as seen in the image.

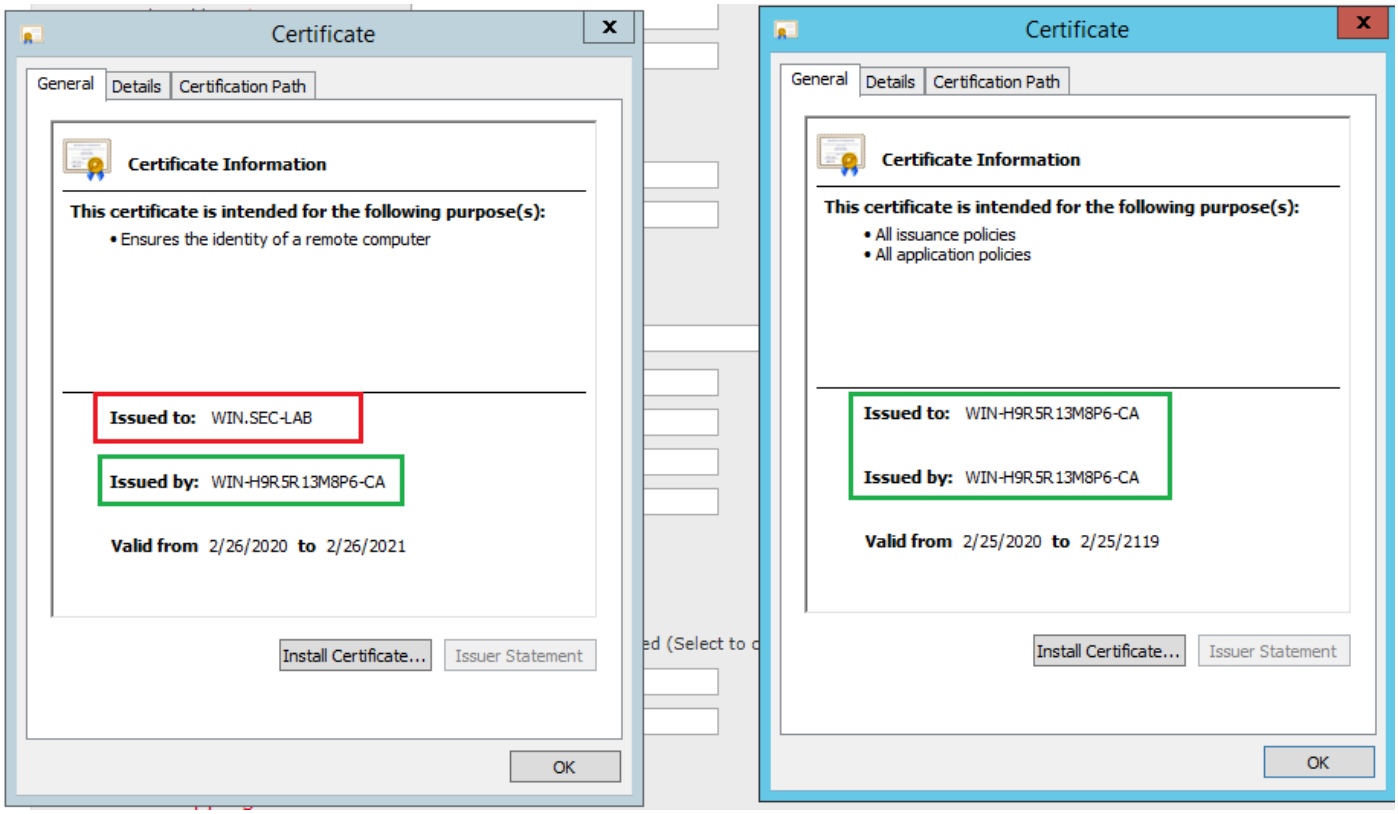
FTD: Access the FTD CLISH and run the command: > configure network dns servers <IP Address>.



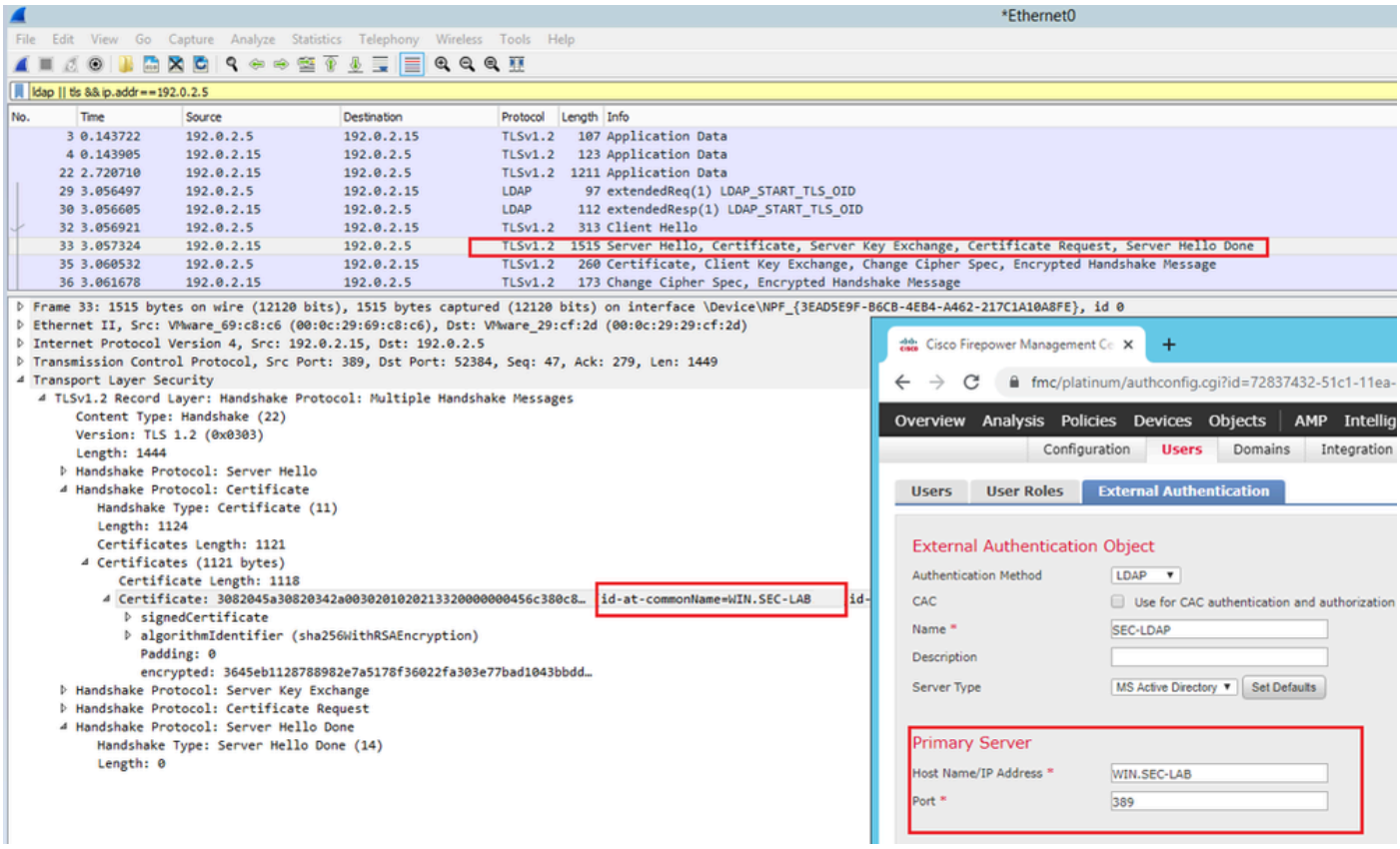
FMC: Choose System > Configuration, and then choose **Management Interfaces** as seen in the image:



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