외부 인증을 위해 LDAP를 사용하여 Firepower Management Center 및 FTD 구성

목차

소개

이 문서에서는 Cisco FMC(Lightweight Directory Access Protocol) 및 FTD(Firepower Firepower Threat Defense)를 사용하여 Microsoft LDAP(Lightweight Directory Access Protocol) 외부 인증을 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD
- Cisco FMC
- Microsoft LDAP

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FMC 및 관리되는 디바이스에는 관리 액세스를 위한 기본 관리자 계정이 포함되어 있습니다. FMC 및 관리되는 디바이스에서 사용자 지정 사용자 계정을 내부 사용자로 추가하거나, 모델에서 지원되는 경우 LDAP 또는 RADIUS 서버의 외부 사용자로 추가할 수 있습니다. 외부 사용자 인증은 FMC 및 FTD에서 지원됩니다.

· 내부 사용자 - FMC/FTD 디바이스가 사용자 인증을 위해 로컬 데이터베이스를 확인합니다.

· 외부 사용자 - 사용자가 로컬 데이터베이스에 없는 경우 외부 LDAP 또는 RADIUS 인증 서버의 시스템 정보가 사용자 데이터베이스를 채웁니다.

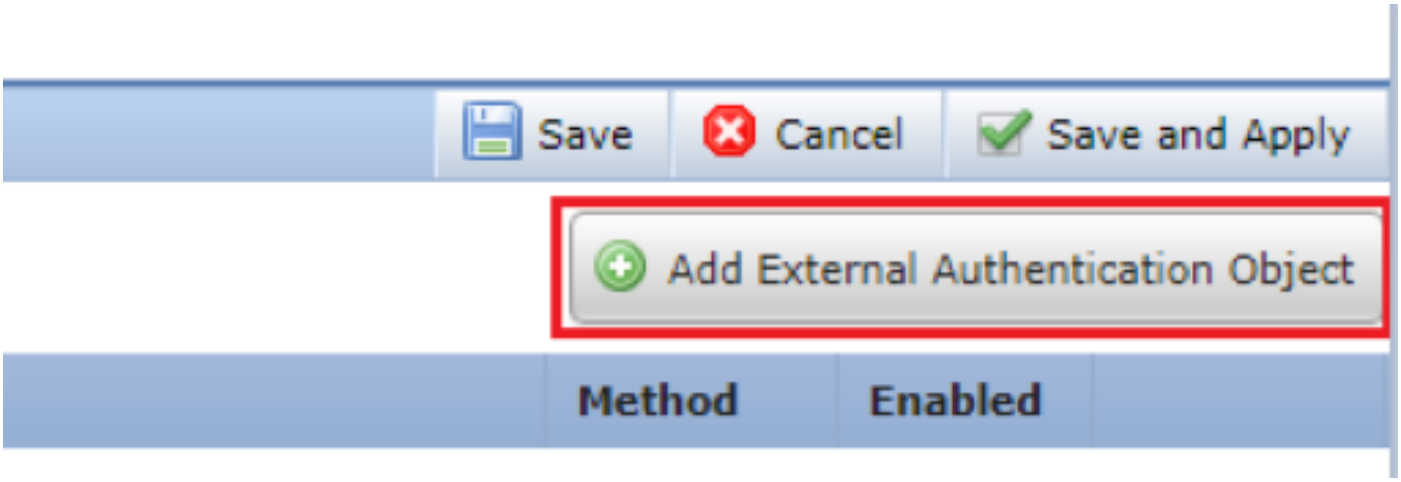
네트워크 다이어그램

구성

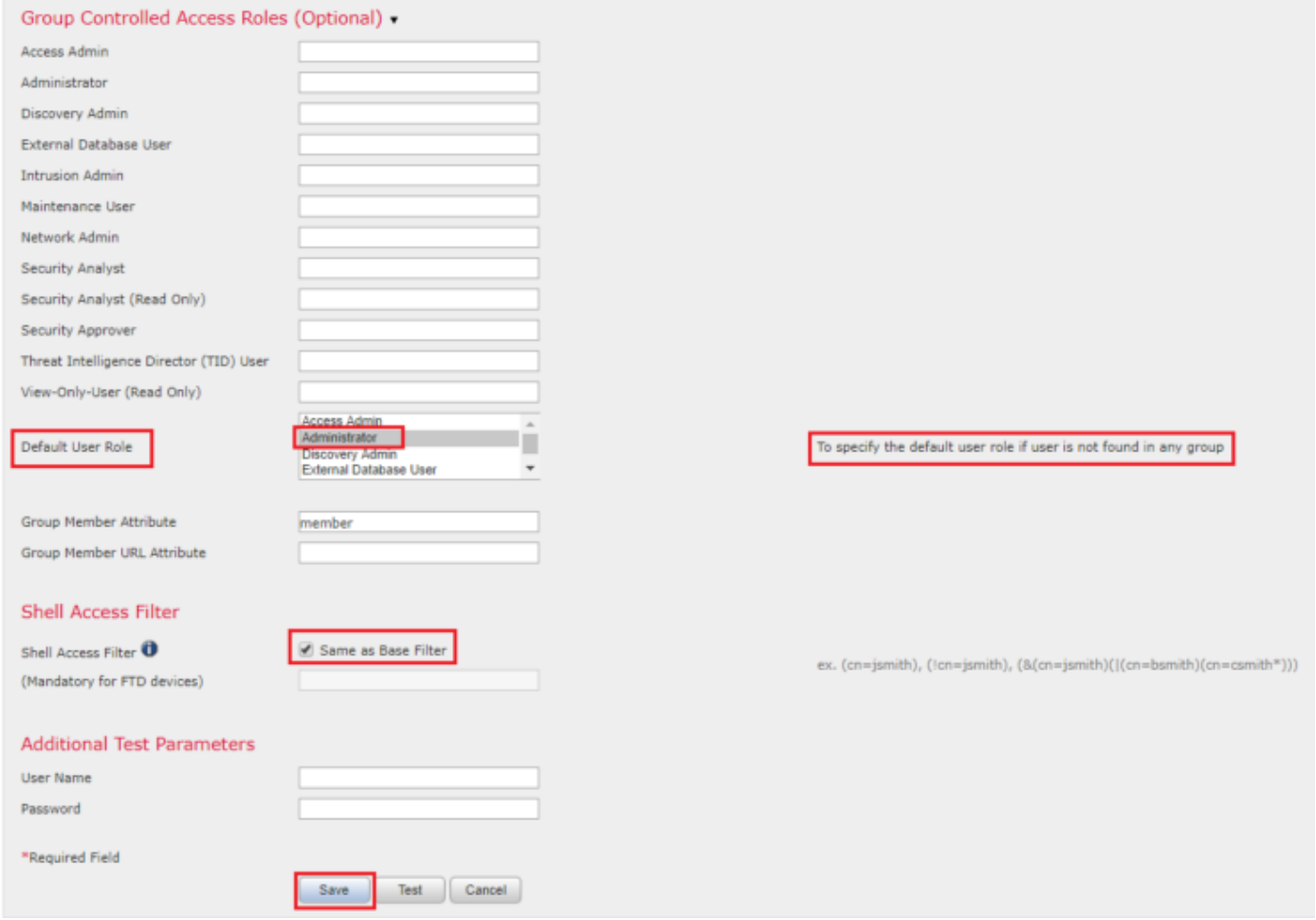
FMC GUI의 기본 LDAP 컨피그레이션

1단계. 탐색 System > Users > External Authentication:

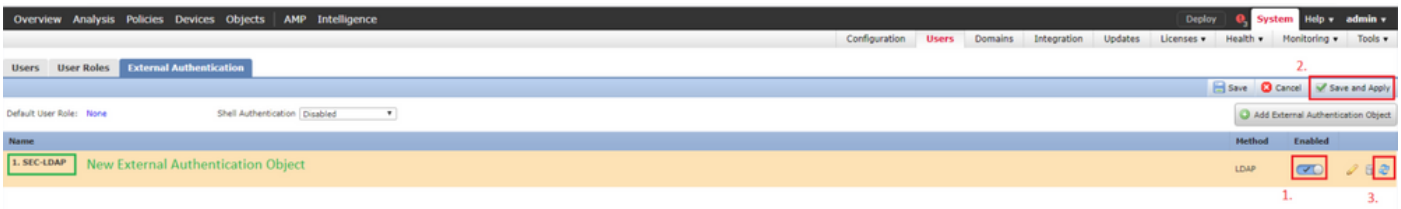
2단계. 선택 Add External Authentication Object:



3단계. 필수 필드를 완료합니다.



4단계. Enable(활성화) External Authentication 개체 및 저장:

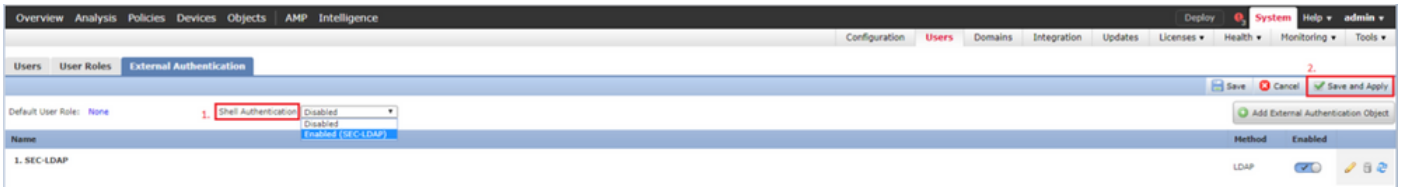


외부 사용자에 대한 셸 액세스

FMC는 서로 다른 두 내부 관리자 사용자, 즉 웹 인터페이스용 사용자와 CLI 액세스용 사용자를 지원합니다. 즉, GUI에 액세스할 수 있는 사용자와 CLI에 액세스할 수 있는 사용자의 구분이 명확합니다. 설치 시 기본 관리자 사용자의 비밀번호는 GUI 및 CLI에서 동일하기 위해 동기화되지만, 서로 다른 내부 메커니즘에 의해 추적되므로 결국 다를 수 있습니다.

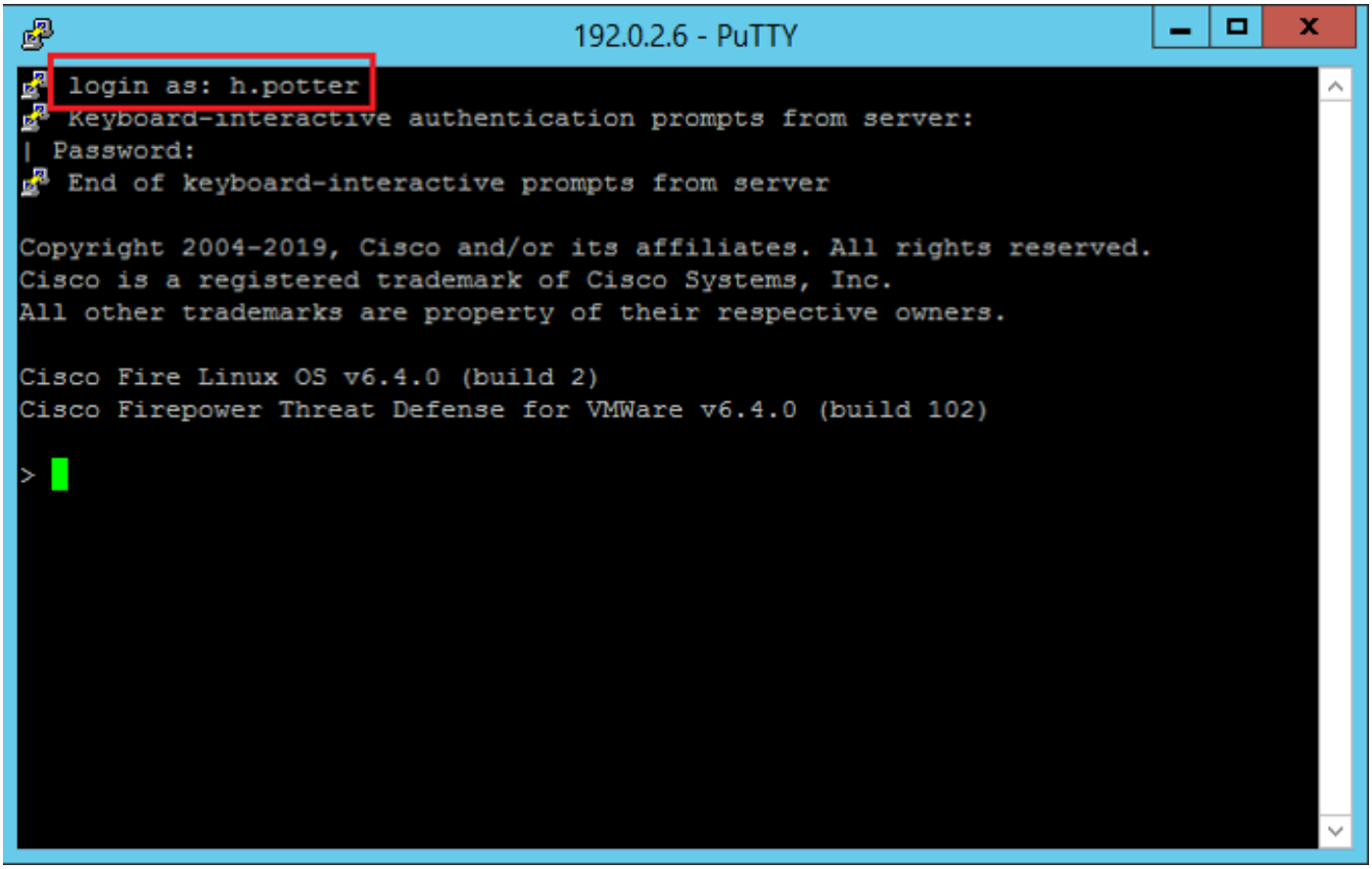
LDAP 외부 사용자에게도 셸 액세스 권한을 부여해야 합니다.

1단계. 탐색 System > Users > External Authentication 을 클릭하고 Shell Authentication 드롭다운 상자(이미지 및 저장 참조):



2단계. FMC에서 변경 사항 구축

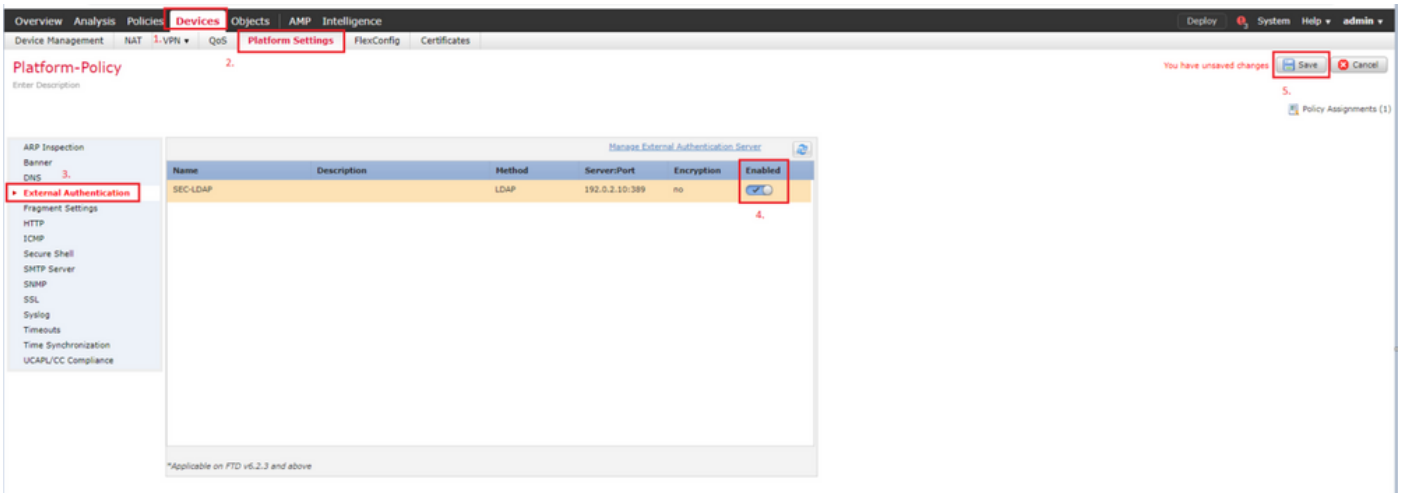
외부 사용자에 대한 셸 액세스가 구성되면 이미지에 표시된 대로 SSH를 통한 로그인이 활성화됩니다.



FTD에 대한 외부 인증

외부 인증은 FTD에서 활성화할 수 있습니다.

1단계. 탐색 Devices > Platform Settings > External Authentication. 클릭 Enabled 및 저장:



사용자 역할

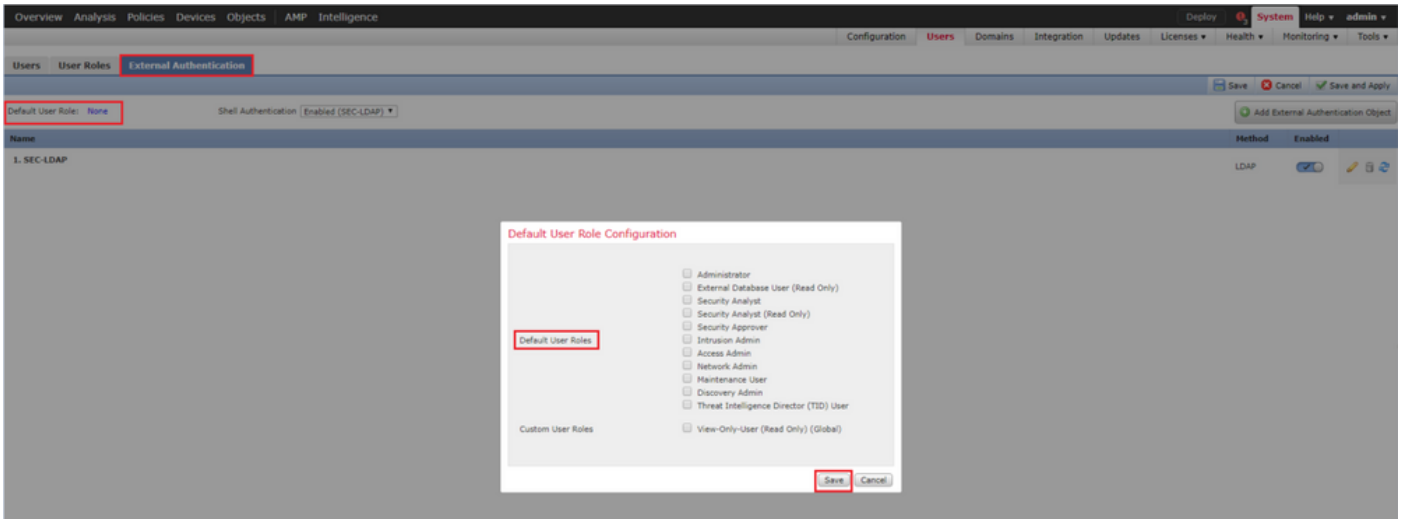
사용자 권한은 할당된 사용자 역할을 기반으로 합니다. 또한 조직의 요구 사항에 맞게 조정된 액세스 권한으로 사용자 지정 사용자 역할을 생성하거나 보안 분석가 및 검색 관리자와 같은 사전 정의된 역할을 사용할 수 있습니다.

사용자 역할에는 두 가지 유형이 있습니다.

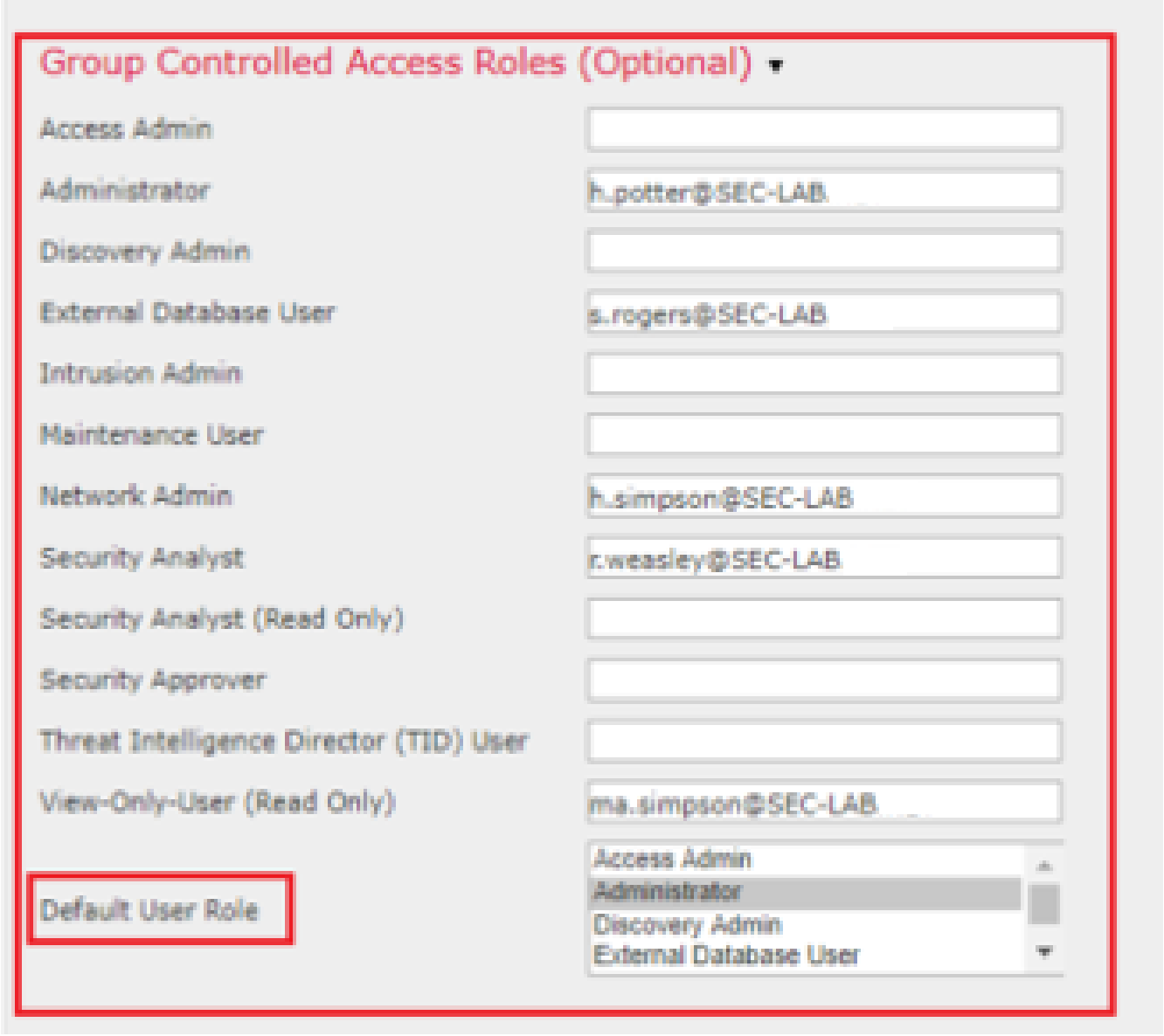
1. 웹 인터페이스 사용자 역할
2. CLI 사용자 역할

사전 정의된 역할의 전체 목록 및 자세한 내용은 사용자 역할을 참조하십시오.

모든 외부 인증 객체에 대한 기본 사용자 역할을 구성하려면 System > Users > External Authentication > Default User Role. 할당할 기본 사용자 역할을 선택하고 Save.



기본 사용자 역할을 선택하거나 특정 객체 그룹의 특정 사용자에게 특정 역할을 할당하려면 객체를 선택하고 Group Controlled Access Roles 그림에서 볼 수 있듯이:



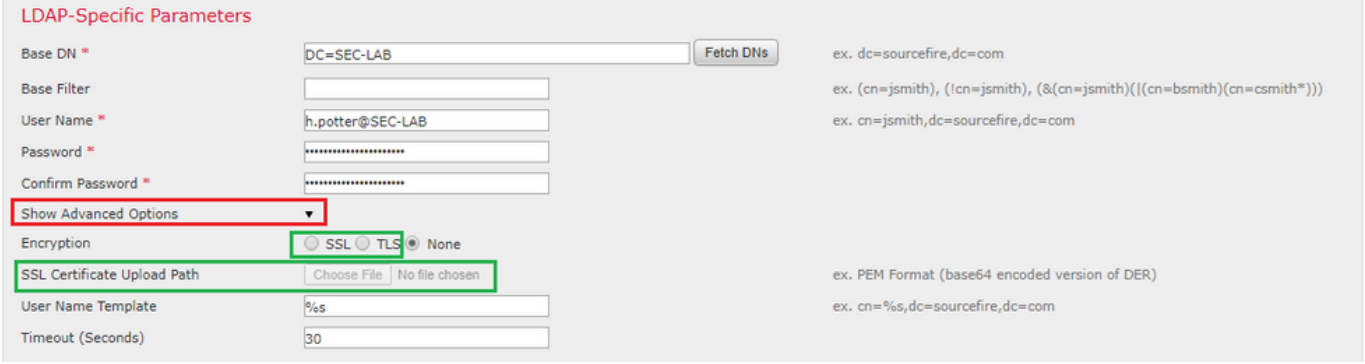
SSL 또는 TLS

DNS는 FMC에서 구성해야 합니다. 이는 인증서의 Subject 값이 Authentication Object Primary Server Hostname. 보안 LDAP가 구성되면 패킷 캡처에 더 이상 일반 텍스트 바인딩 요청이 표시되지 않습니다.

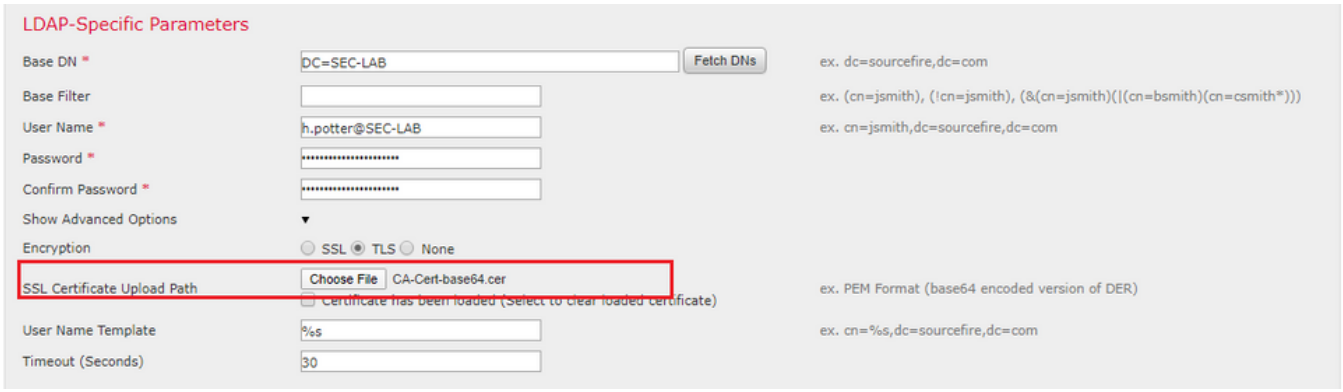
SSL은 기본 포트를 636으로 변경하고 TLS는 이를 389로 유지합니다.

참고: TLS 암호화에는 모든 플랫폼에 인증서가 필요합니다. SSL의 경우 FTD에도 인증서가 필요합니다. 다른 플랫폼의 경우 SSL에는 인증서가 필요하지 않습니다. 그러나 중간자 공격(man-in-the-middle attack)을 방지하려면 항상 SSL용 인증서를 업로드하는 것이 좋습니다.

1단계. 탐색 Devices > Platform Settings > External Authentication > External Authentication Object 고급 옵션 SSL/TLS 정보를 입력합니다.



2단계. 서버의 인증서에 서명한 CA의 인증서를 업로드합니다. 인증서는 PEM 형식이어야 합니다.



3단계. 설정 저장.

다음을 확인합니다.

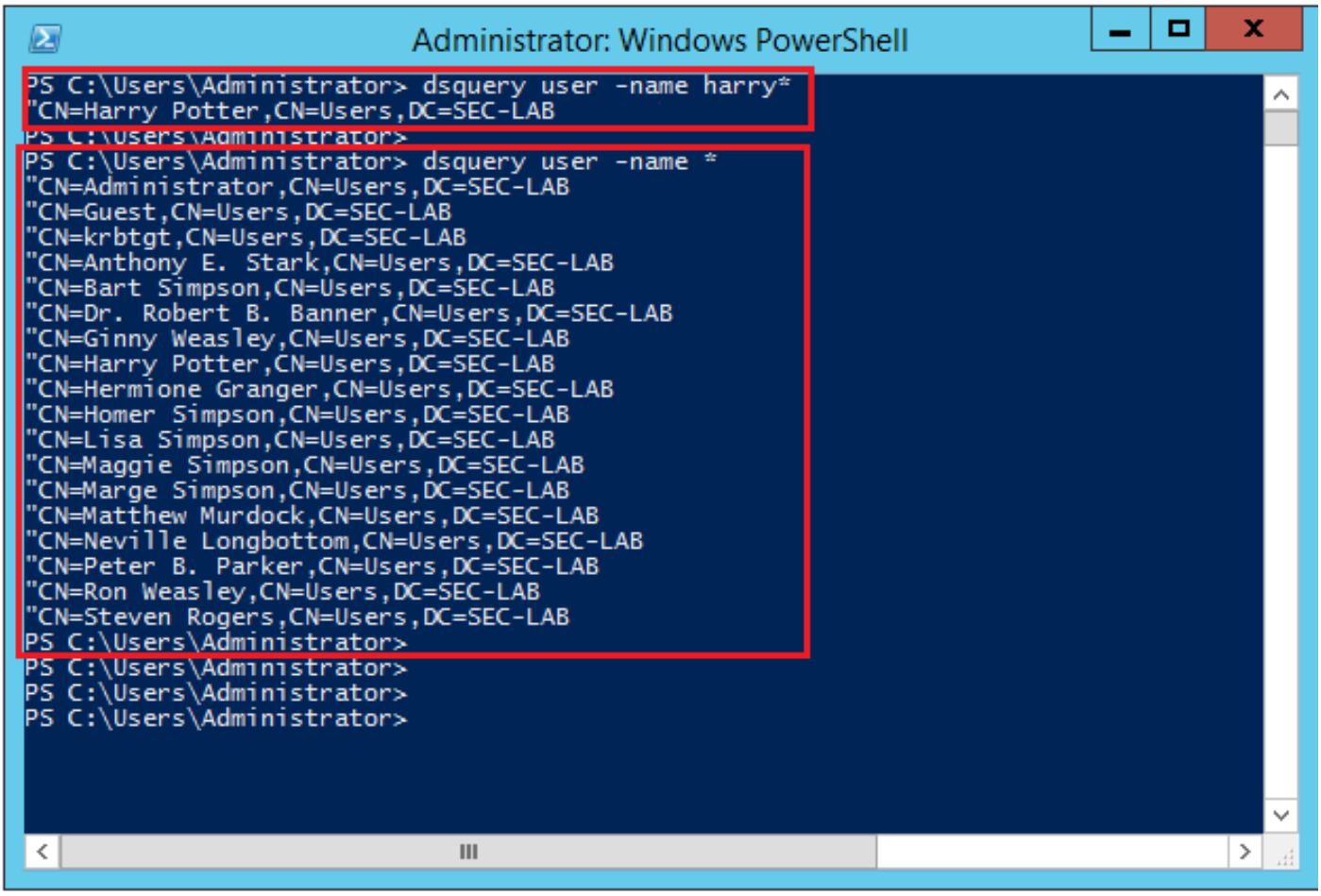
테스트 검색 기준

LDAP가 구성된 Windows 명령 프롬프트 또는 PowerShell을 열고 명령을 입력합니다. dsquery user -name

.

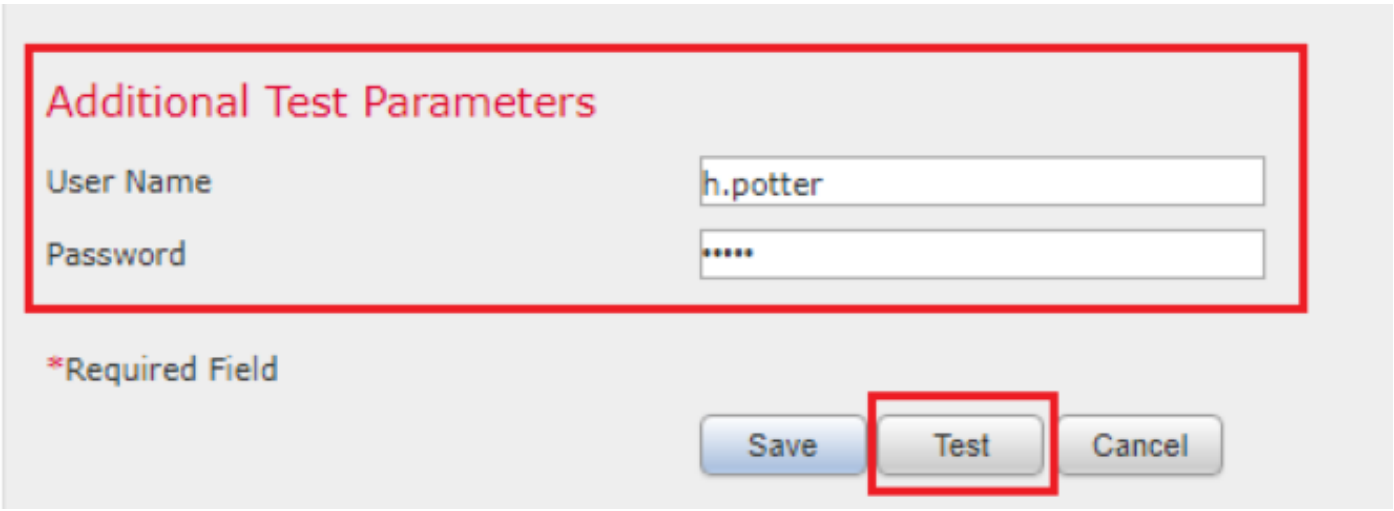
예를 들면 다음과 같습니다.

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

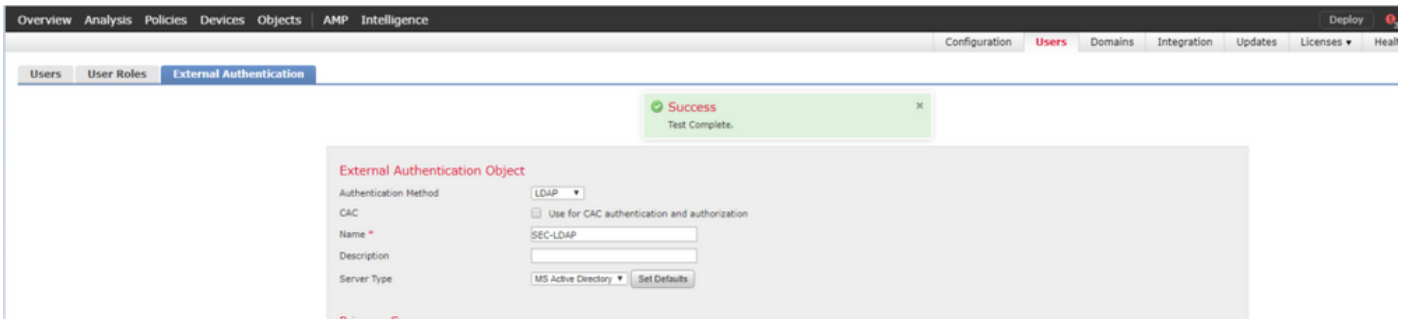


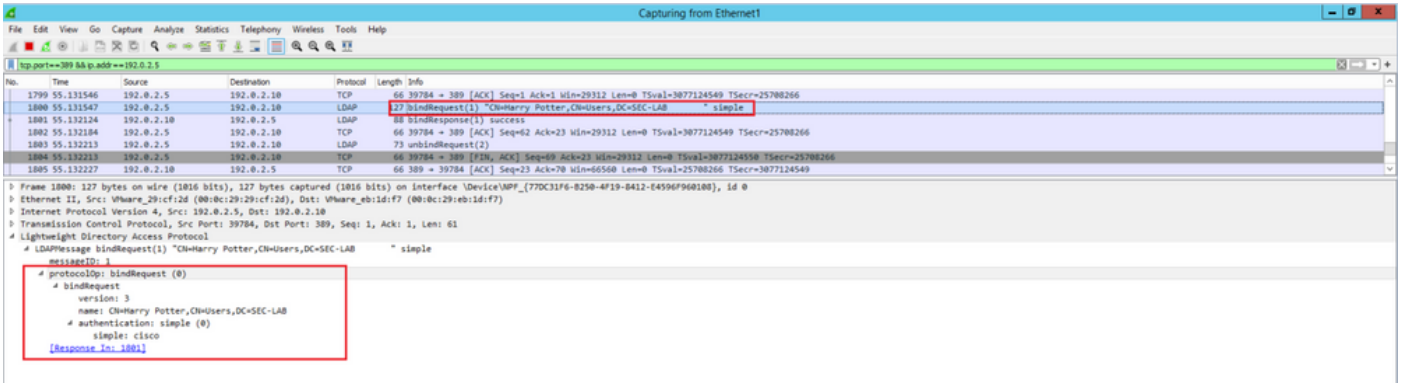
LDAP 통합 테스트

탐색 System > Users > External Authentication > External Authentication Object. 페이지 하단에 Additional Test Parameters 섹션 (이미지 참조):



결과를 보려면 테스트를 선택합니다.





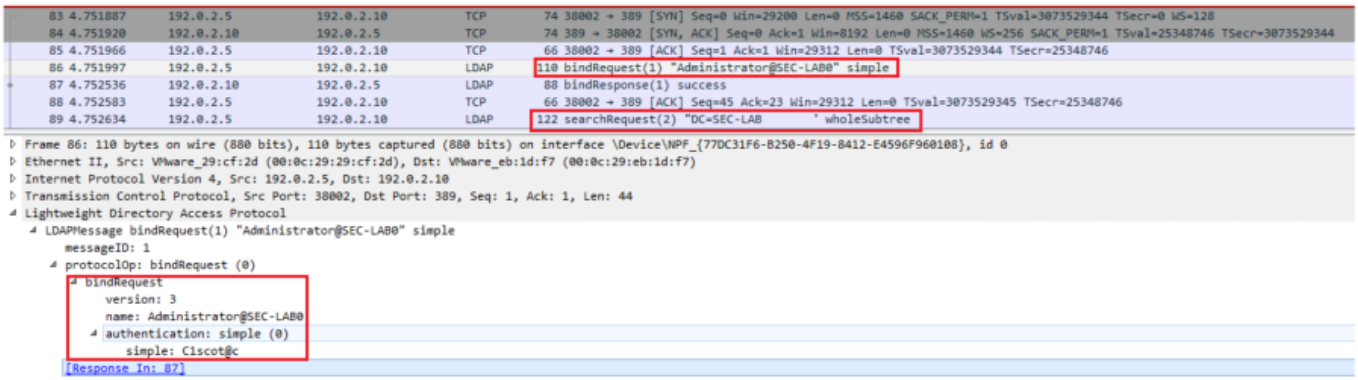
문제 해결

FMC/FTD와 LDAP는 사용자를 다운로드하기 위해 어떻게 상호 작용합니까?

FMC가 Microsoft LDAP 서버에서 사용자를 가져올 수 있으려면 먼저 LDAP 관리자 자격 증명이 포함된 포트 389 또는 636(SSL)에서 바인딩 요청을 보내야 합니다. LDAP 서버가 FMC를 인증할 수 있게 되면 성공 메시지로 응답합니다. 마지막으로, FMC는 다이어그램에 설명된 대로 검색 요청 메시지를 사용하여 요청할 수 있습니다.

<< --- 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

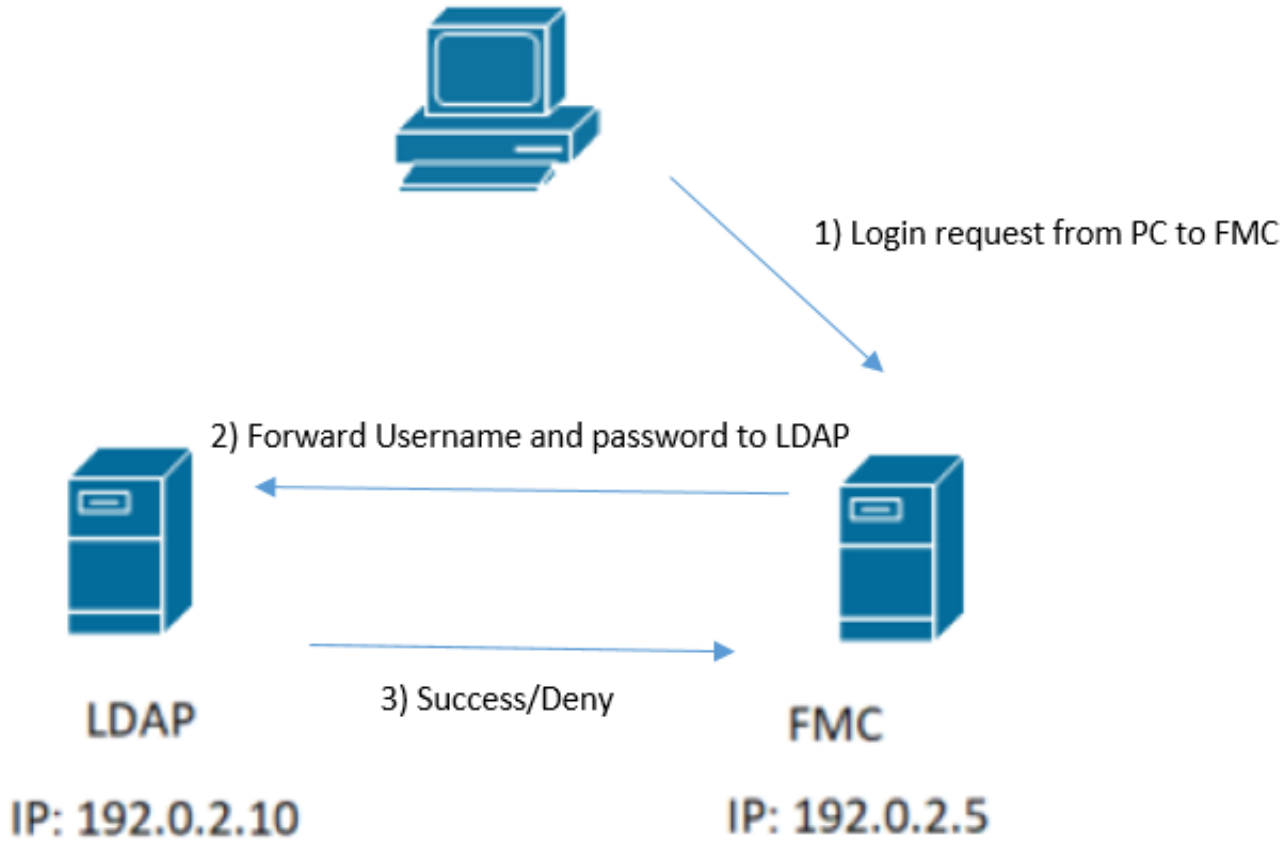
인증은 기본적으로 암호화되지 않은 상태로 비밀번호를 전송합니다.

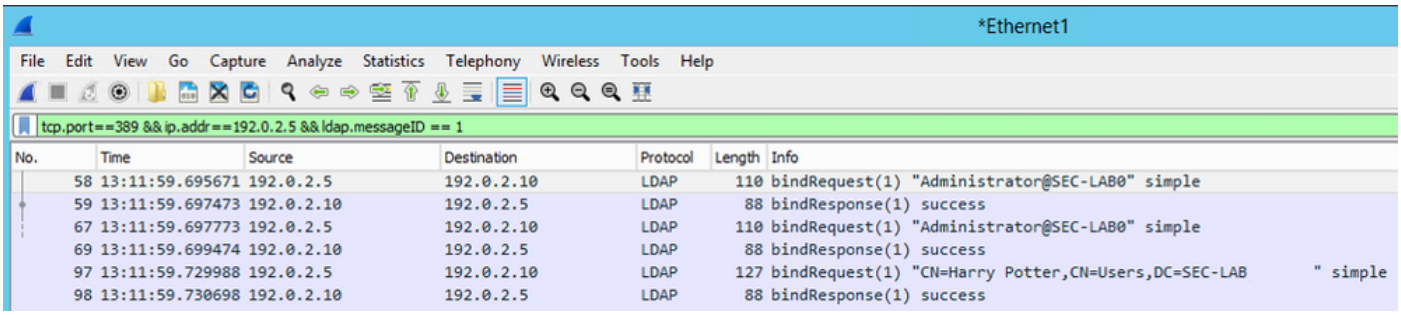


FMC/FTD와 LDAP는 사용자 로그인 요청을 인증하기 위해 어떻게 상호 작용합니까?

LDAP 인증이 활성화된 동안 사용자가 FMC 또는 FTD에 로그인할 수 있도록 초기 로그인 요청이

Firepower으로 전송되지만 성공/거부 응답을 위해 사용자 이름과 비밀번호가 LDAP로 전달됩니다. 즉, FMC 및 FTD는 데이터베이스에 로컬로 비밀번호 정보를 보관하지 않고 대신 LDAP에서 진행 방법에 대한 확인을 기다립니다.





사용자 이름 및 비밀번호가 수락되면 이미지에 표시된 대로 웹 GUI에 항목이 추가됩니다.

사용자 정보를 확인하려면 FMC CLISH에서 show user 명령을 실행합니다. > show user

이 명령은 지정된 사용자에 대한 자세한 컨피그레이션 정보를 표시합니다. 다음 값이 표시됩니다.

Login(로그인) - 로그인 이름

UID — 숫자 사용자 ID
Auth (Local or Remote)(인증(로컬 또는 원격)) - 사용자 인증 방법
Access(Basic 또는 Config) - 사용자의 권한 레벨
Enabled(활성화됨 또는 비활성화됨) — 사용자의 활성 여부
Reset (Yes or No)(재설정(예 또는 아니요) - 사용자가 다음 로그인 시 비밀번호를 변경해야 하는지 여부
Exp(Never 또는 a number) - 사용자의 비밀번호를 변경해야 할 때까지의 일수
경고(N/A 또는 숫자) — 비밀번호가 만료되기 전에 사용자에게 비밀번호를 변경할 수 있는 일 수입니다
Str(Yes 또는 No) — 사용자의 비밀번호가 강도를 확인하기 위한 기준을 충족해야 하는지 여부
Lock (Yes or No)(잠금(예 또는 아니요) - 로그인 실패가 너무 많아 사용자 계정이 잠겼는지 여부
Max(N/A 또는 a number) — 사용자 계정이 잠기기 전 최대 실패 로그인 수

SSL 또는 TLS가 예상대로 작동하지 않음

FTD에서 DNS를 활성화하지 않으면 pigtail 로그에서 LDAP에 연결할 수 없음을 나타내는 오류를 확인할 수 있습니다.

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

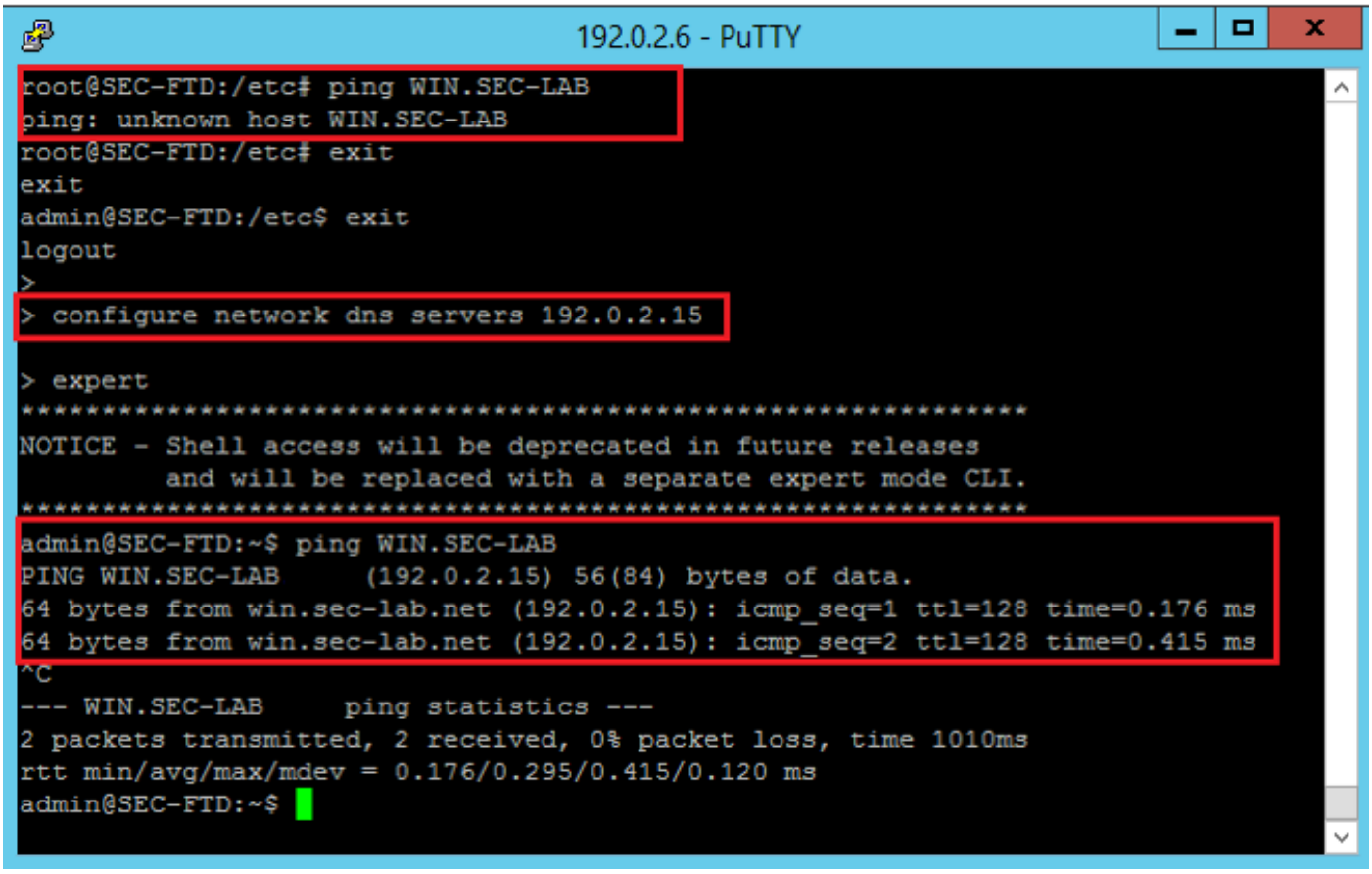
```
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
```

```
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
```

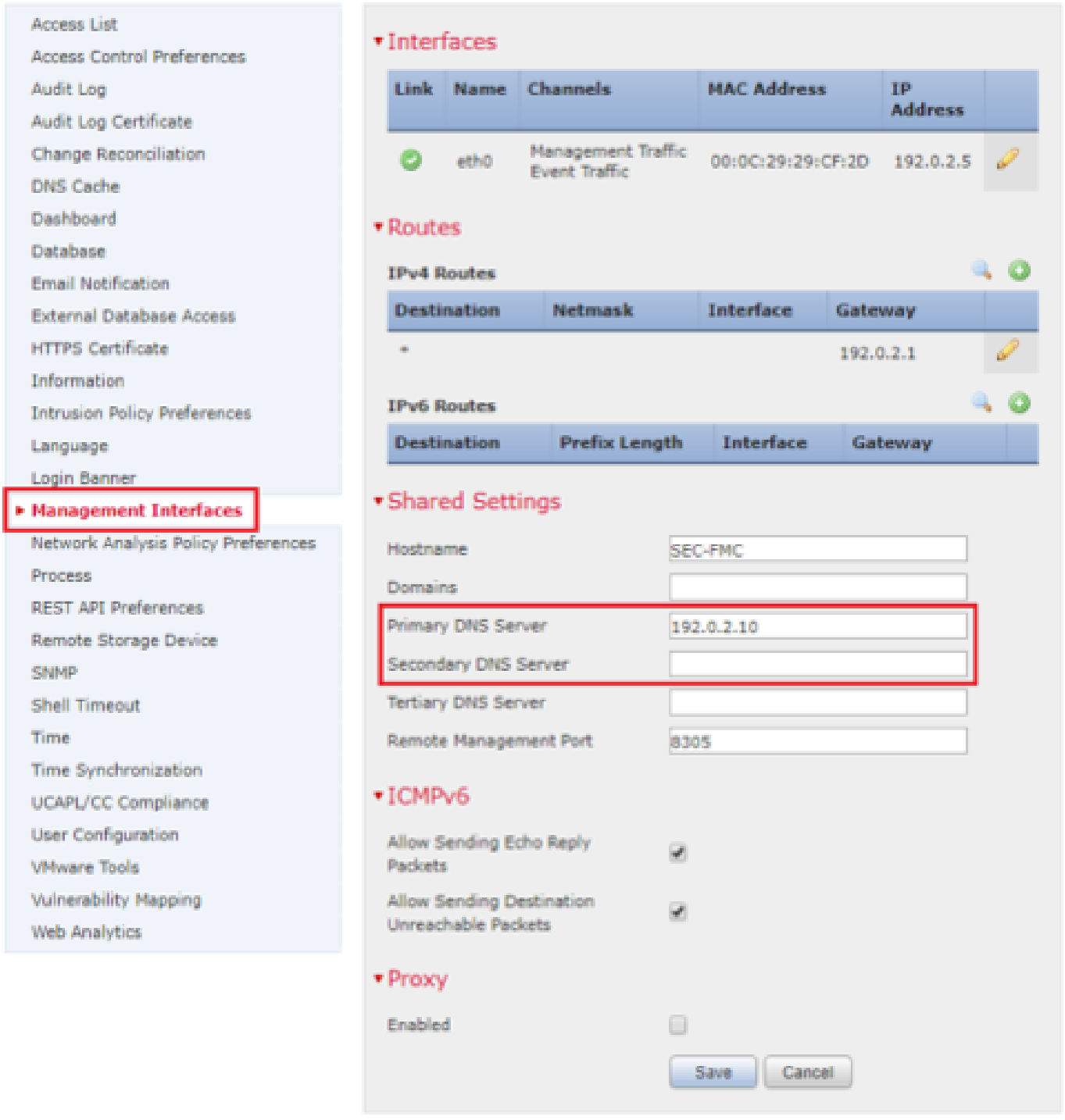
firepower에서 LDAP 서버 FQDN을 확인할 수 있는지 확인합니다. 그렇지 않은 경우 이미지에 표시된 대로 올바른 DNS를 추가합니다.

FTD: FTD CLISH에 액세스하여 다음 명령을 실행합니다. > configure network dns servers

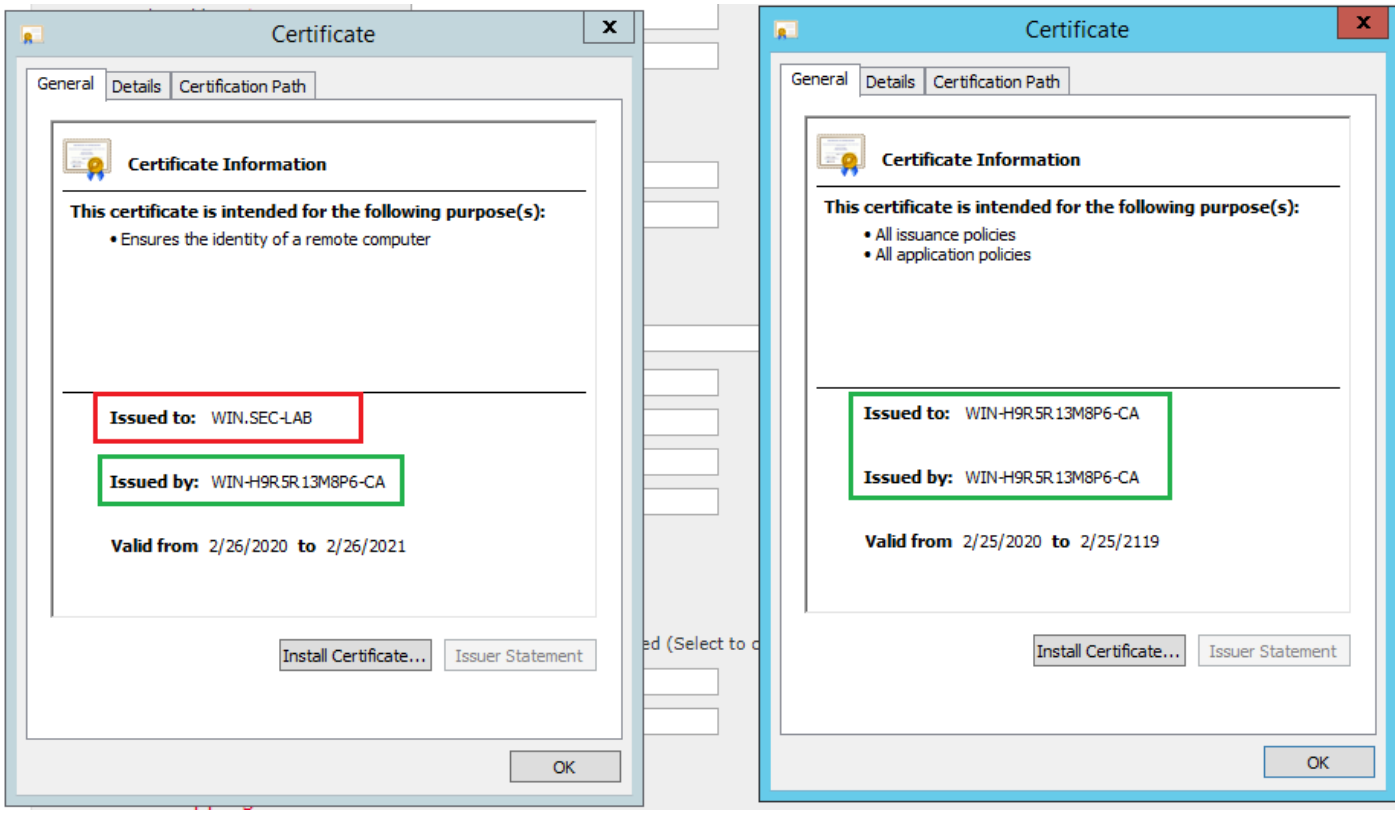
.



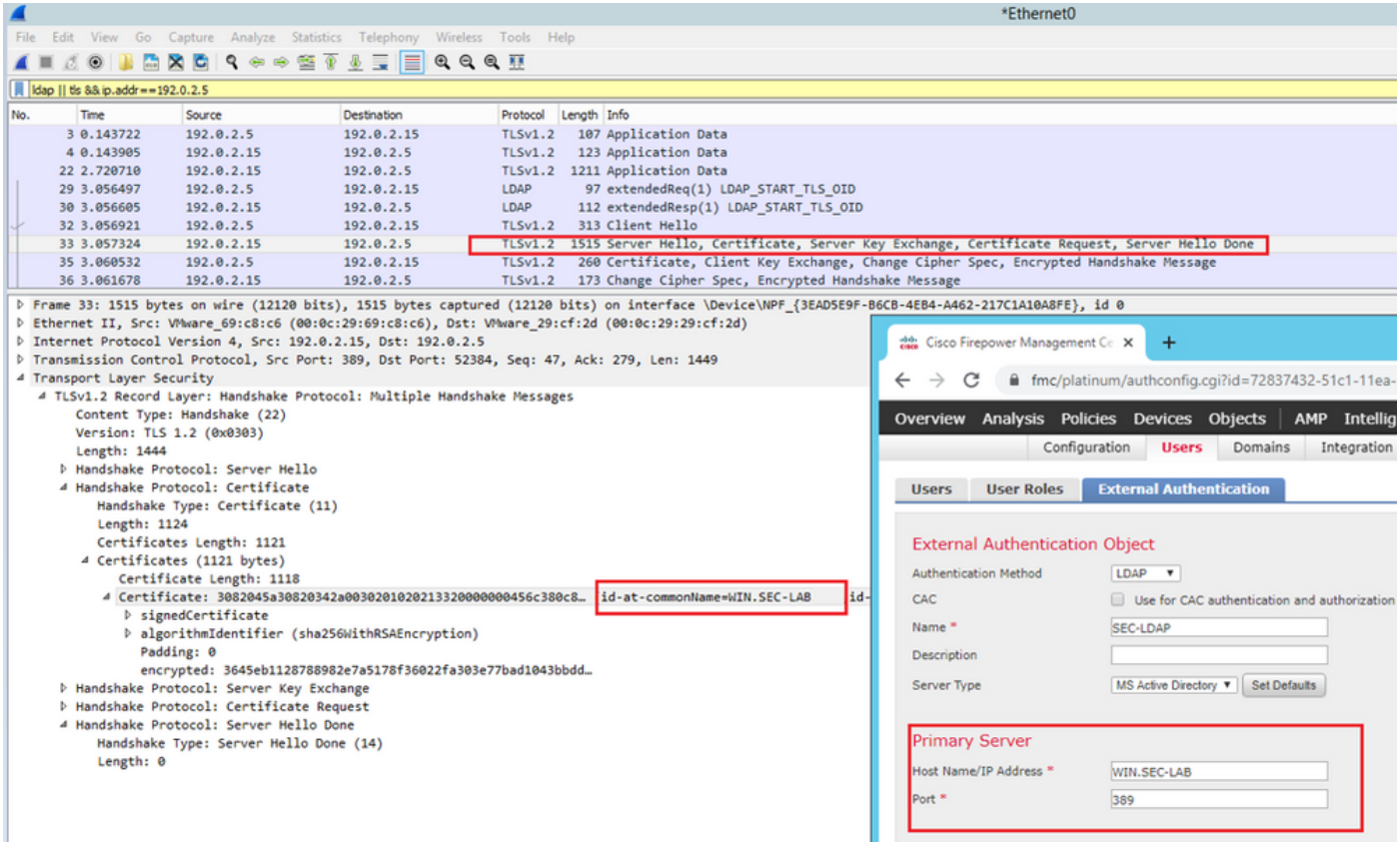
FMC: 선택 System > Configuration를 선택한 다음 이미지에 표시된 대로 Management Interfaces(관리 인터페이스)를 선택합니다.



이미지에 표시된 대로 FMC에 업로드된 인증서가 LDAP의 서버 인증서에 서명한 CA의 인증서인지 확인합니다.



LDAP 서버가 올바른 정보를 전송하는지 확인하려면 패킷 캡처를 사용합니다.



관련 정보

- [관리 액세스를 위한 사용자 계정]

- Cisco Firepower Management Center LDS(Lightweight Directory Access Protocol) 인증 우회 취약성
- FireSIGHT 시스템의 LDAP 인증 객체 컨피그레이션
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.