

# Konfigurieren von FirePOWER Management Center und FTD mit LDAP für externe Authentifizierung

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Grundlegende LDAP-Konfiguration in der FMC-GUI](#)

[Shell-Zugriff für externe Benutzer](#)

[Externe Authentifizierung gegenüber FTD](#)

[Benutzerrollen](#)

[SSL oder TLS](#)

[Überprüfung](#)

[Test-Suchbasis](#)

[LDAP-Integration testen](#)

[Fehlerbehebung](#)

[Wie interagieren FMC/FTD und LDAP, um Benutzer herunterzuladen?](#)

[Wie interagieren FMC/FTD und LDAP, um eine Benutzeranmeldeanfrage zu authentifizieren?](#)

[SSL oder TLS funktionieren nicht wie erwartet](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie die externe Authentifizierung über das Microsoft Lightweight Directory Access Protocol (LDAP) mit Cisco FirePOWER Management Center (FMC) und FirePOWER Threat Defense (FTD) aktiviert wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FTD von Cisco
- Cisco FMC
- Microsoft-LDAP

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTD 6.5.0-123

- FMC 6.5.0-115
- Microsoft Server 2012

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Das FMC und die verwalteten Geräte umfassen ein standardmäßiges Administratorkonto für den Verwaltungszugriff. Sie können benutzerdefinierte Benutzerkonten auf dem FMC und auf verwalteten Geräten entweder als interne Benutzer oder, falls für Ihr Modell unterstützt, als externe Benutzer auf einem LDAP- oder RADIUS-Server hinzufügen. Die Authentifizierung externer Benutzer wird für FMC und FTD unterstützt.

ãf» Interner Benutzer - Das FMC/FTD-Gerät überprüft eine lokale Datenbank auf Benutzerauthentifizierung.

ãf» Externer Benutzer - Wenn der Benutzer nicht in der lokalen Datenbank vorhanden ist, werden die Systeminformationen eines externen LDAP- oder RADIUS-Authentifizierungsservers in die Benutzerdatenbank eingefügt.

## Netzwerkdiagramm



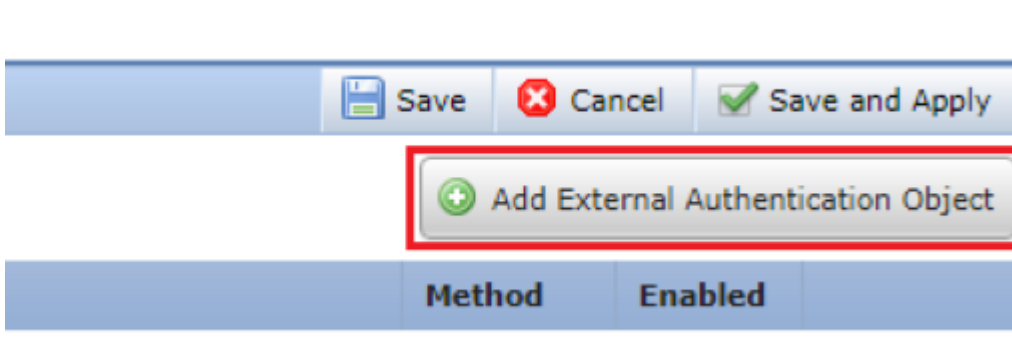
## Konfigurieren

### Grundlegende LDAP-Konfiguration in der FMC-GUI

Schritt 1: Navigieren Sie zu System > Users > External Authentication:



Schritt 2: Auswählen Add External Authentication Object:



Schritt 3: Füllen Sie die erforderlichen Felder aus:

**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 ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith\*)))

(Mandatory for FTD devices)

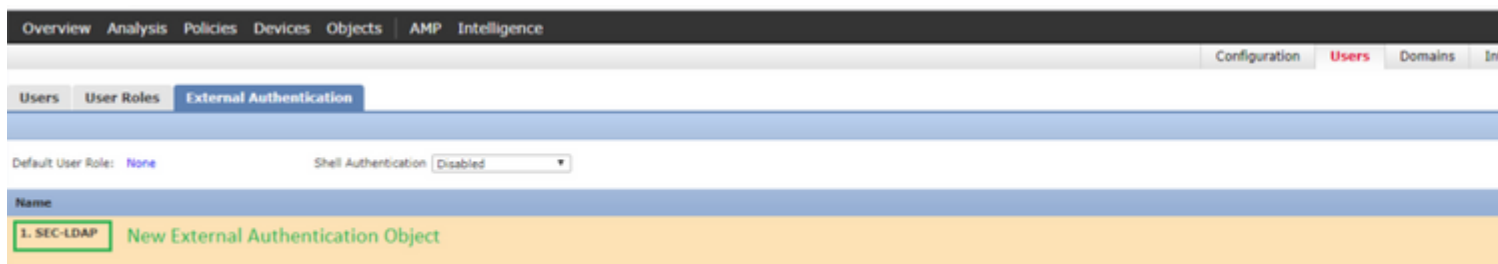
**Additional Test Parameters**

User Name

Password

\*Required Field

Schritt 4: Aktivieren Sie das External Authentication Objekt und Speichern:



## Shell-Zugriff für externe Benutzer

Das FMC unterstützt zwei verschiedene interne Admin-Benutzer: einen für die Webschnittstelle und einen weiteren mit CLI-Zugriff. Das bedeutet, dass klar unterschieden wird, wer auf die GUI zugreifen kann und wer auch auf die CLI zugreifen kann. Zum Zeitpunkt der Installation wird das Kennwort für den Standardadmin-Benutzer synchronisiert, damit es auf der GUI und der CLI identisch ist. Sie werden jedoch von verschiedenen internen Mechanismen überwacht und können sich letztendlich unterscheiden.

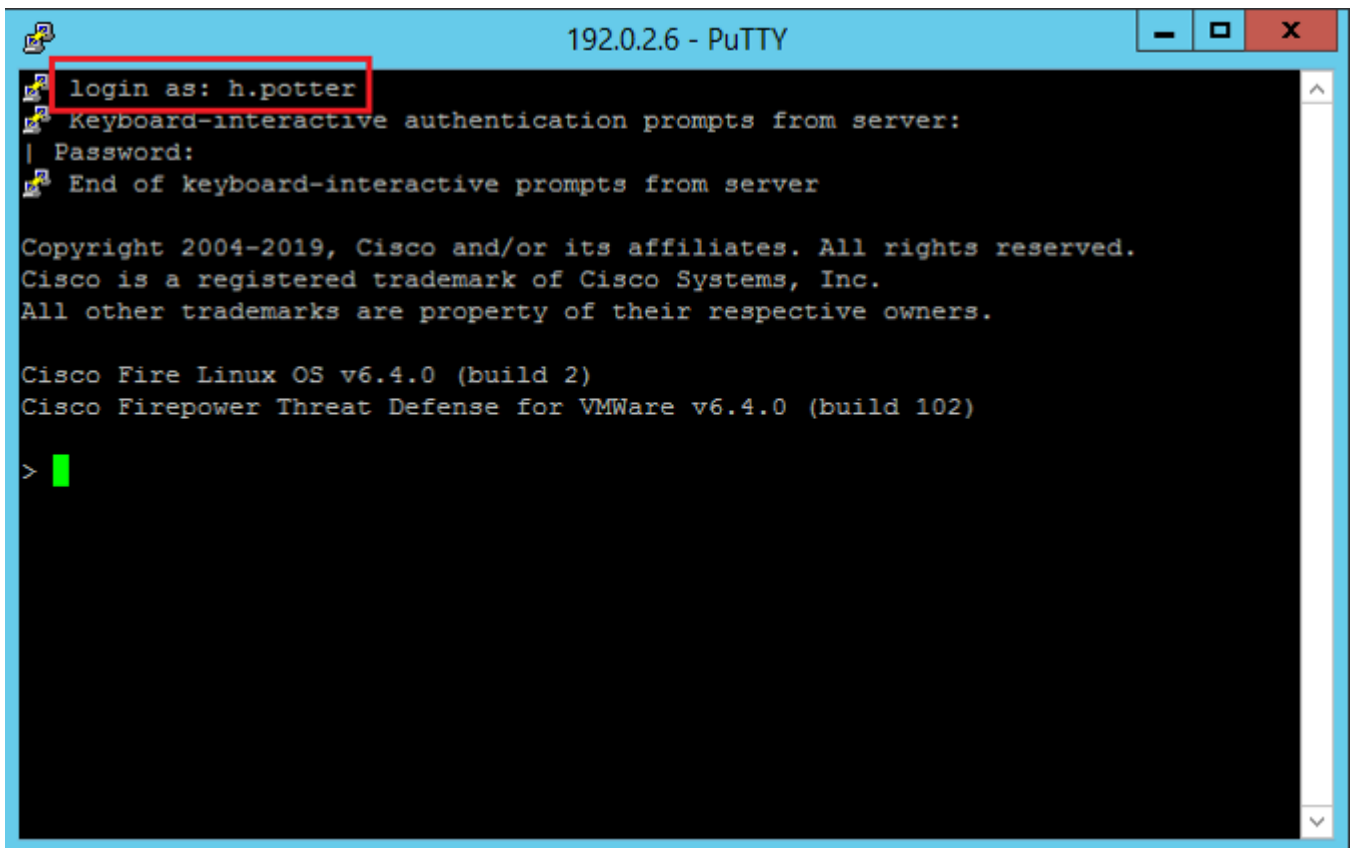
Externen LDAP-Benutzern muss ebenfalls der Zugriff auf die Shell gewährt werden.

Schritt 1: Navigieren Sie zu System > Users > External Authentication und klicke auf Shell Authentication Dropdown-Feld, wie im Bild zu sehen und zu speichern:



Schritt 2: Bereitstellen von Änderungen in FMC

Nach der Konfiguration des Shell-Zugriffs für externe Benutzer wird die Anmeldung über SSH aktiviert (siehe Abbildung):



## Externe Authentifizierung gegenüber FTD

Die externe Authentifizierung kann auf FTD aktiviert werden.

Schritt 1: Navigieren Sie zu `Devices > Platform Settings > External Authentication`. Klicken Sie auf `Enabled` und speichern:

Platform-Policy

Enter Description

Manage External Authentication Server

Name	Description	Method	Server:Port	Encryption	Enabled
SEC-LDAP		LDAP	192.0.2.10:389	no	<input checked="" type="checkbox"/>

\*Applicable on FTD v6.2.3 and above

## Benutzerrollen

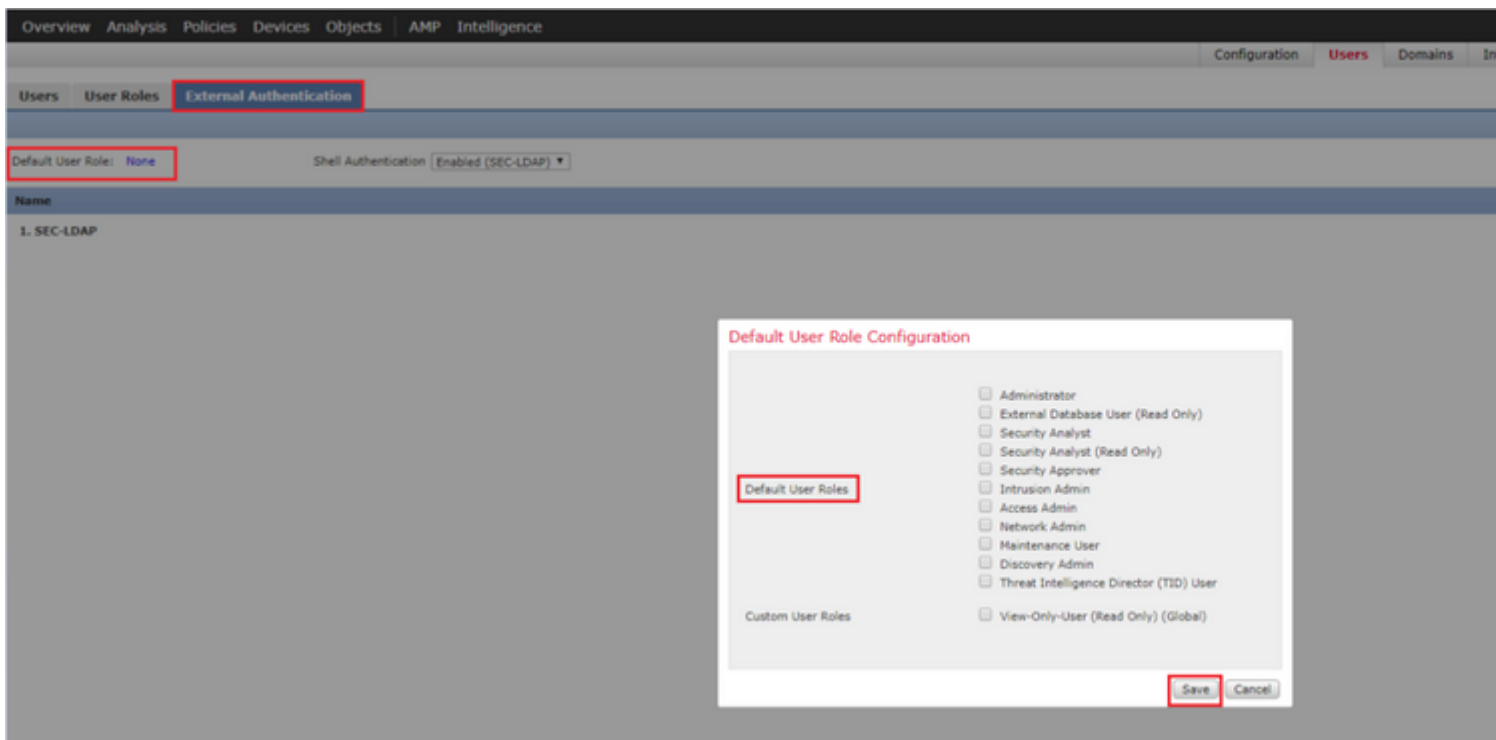
Benutzerberechtigungen basieren auf der zugewiesenen Benutzerrolle. Sie können auch benutzerdefinierte Benutzerrollen mit Zugriffsberechtigungen erstellen, die auf die Anforderungen Ihrer Organisation zugeschnitten sind, oder Sie können vordefinierte Rollen verwenden, z. B. Sicherheitsanalyst und Ermittlungsadministrator.

Es gibt zwei Arten von Benutzerrollen:

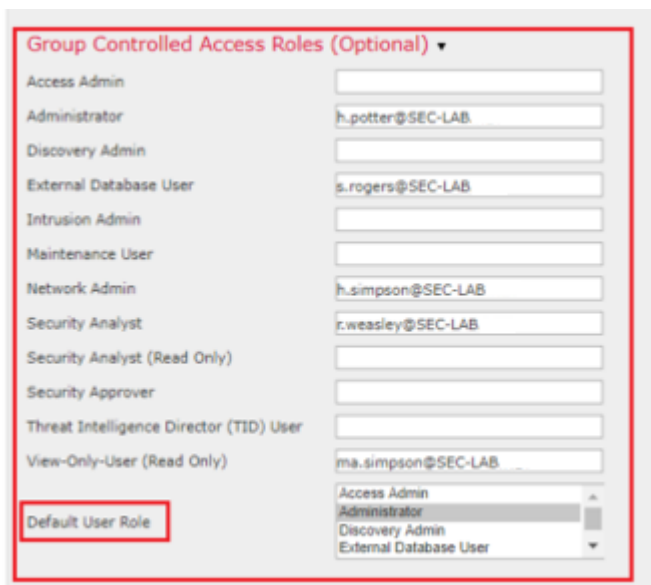
1. Benutzerrollen für Webschnittstelle
2. CLI-Benutzerrollen

Eine vollständige Liste der vordefinierten Rollen und weitere Informationen finden Sie unter [Benutzerrollen](#).

Um eine Standardbenutzerrolle für alle externen Authentifizierungsobjekte zu konfigurieren, navigieren Sie zu System > Users > External Authentication > Default User Role. Wählen Sie die Standard-Benutzerrolle aus, die Sie zuweisen möchten, und klicken Sie auf Save.



Um eine Standardbenutzerrolle auszuwählen oder bestimmten Benutzern in einer bestimmten Objektgruppe bestimmte Rollen zuzuweisen, können Sie das Objekt auswählen und zu navigieren. Group Controlled Access Roles wie im Bild zu sehen:



## SSL oder TLS

DNS muss im FMC konfiguriert werden. Der Grund hierfür ist, dass der Betreff-Wert des Zertifikats mit dem des Authentication Object Primary Server Hostname. Nach der Konfiguration von Secure LDAP werden bei der Paketerfassung keine Anforderungen für die Klartextbindung mehr angezeigt.

SSL ändert den Standardport in 636, und TLS behält den Wert 389 bei.

**Hinweis:** Für die TLS-Verschlüsselung ist ein Zertifikat auf allen Plattformen erforderlich. Für SSL benötigt die FTD auch ein Zertifikat. Für andere Plattformen ist für SSL kein Zertifikat erforderlich. Es wird jedoch empfohlen, immer ein Zertifikat für SSL hochzuladen, um Man-in-the-Middle-

Angriffe zu verhindern.

Schritt 1: Navigieren Sie zu Devices > Platform Settings > External Authentication > External Authentication Object und geben Sie die SSL/TLS-Informationen für die erweiterten Optionen ein:

**LDAP-Specific Parameters**

Base DN \*   ex. dc=sourcefire,dc=com

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

User Name \*  ex. cn=jsmith,dc=sourcefire,

Password \*

Confirm Password \*

Show Advanced Options ▼

Encryption  SSL  TLS  None

SSL Certificate Upload Path   ex. PEM Format (base64 encod

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

Timeout (Seconds)

Schritt 2: Laden Sie das Zertifikat der Zertifizierungsstelle hoch, die das Zertifikat des Servers signiert hat. Das Zertifikat muss im PEM-Format vorliegen.

**LDAP-Specific Parameters**

Base DN \*   ex. dc=sourcefire,dc=com

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

User Name \*  ex. cn=jsmith,dc=sourcefire

Password \*

Confirm Password \*

Show Advanced Options ▼

Encryption  SSL  TLS  None

SSL Certificate Upload Path  CA-Cert-base64.cer ex. PEM Format (base64 encod

Certificate has been loaded (Select to clear loaded certificate) ex. cn=%s,dc=sourcefire,dc=

User Name Template

Timeout (Seconds)

Schritt 3: Speichern Sie die Konfiguration.

## Überprüfung

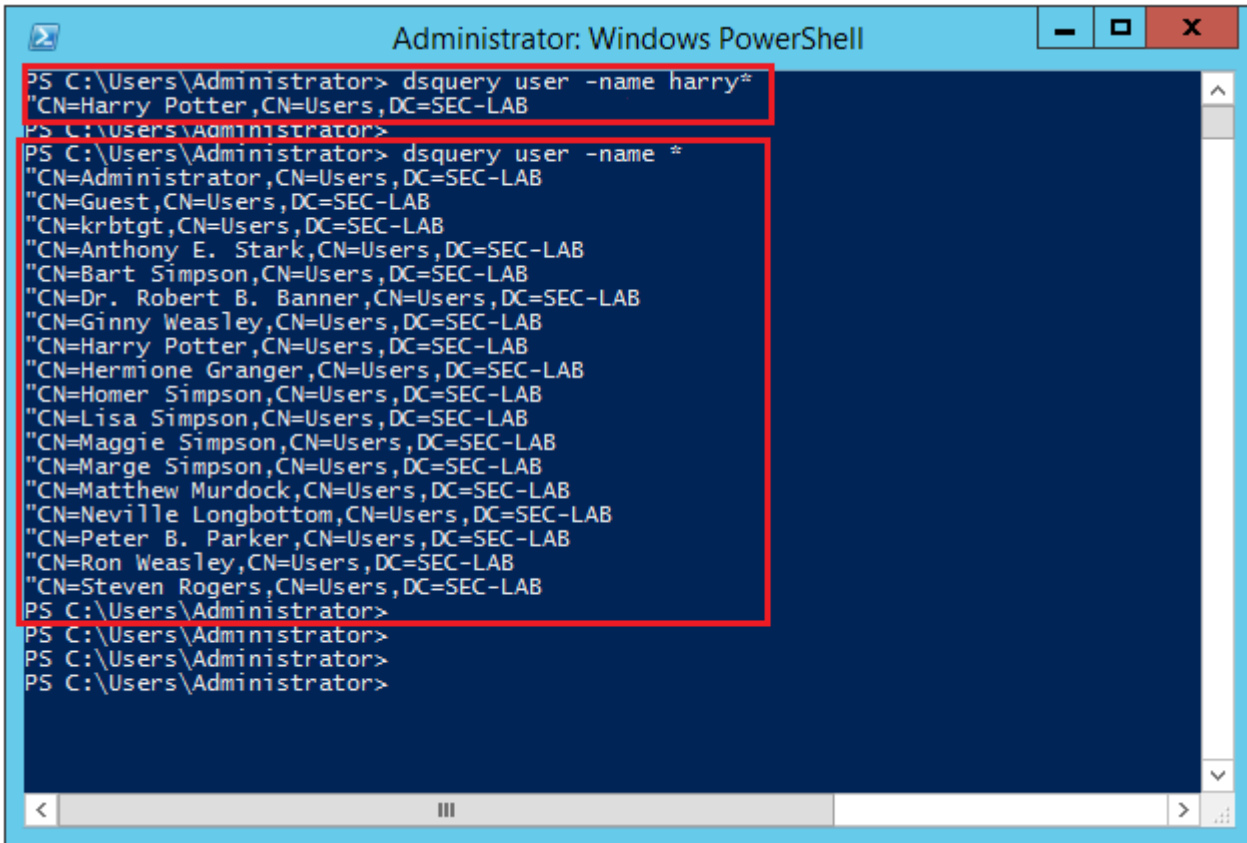
### Test-Suchbasis

Öffnen Sie eine Windows-Eingabeaufforderung oder PowerShell, in der LDAP konfiguriert ist, und geben Sie den folgenden Befehl ein: `dsquery user -name`

Beispiele:



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

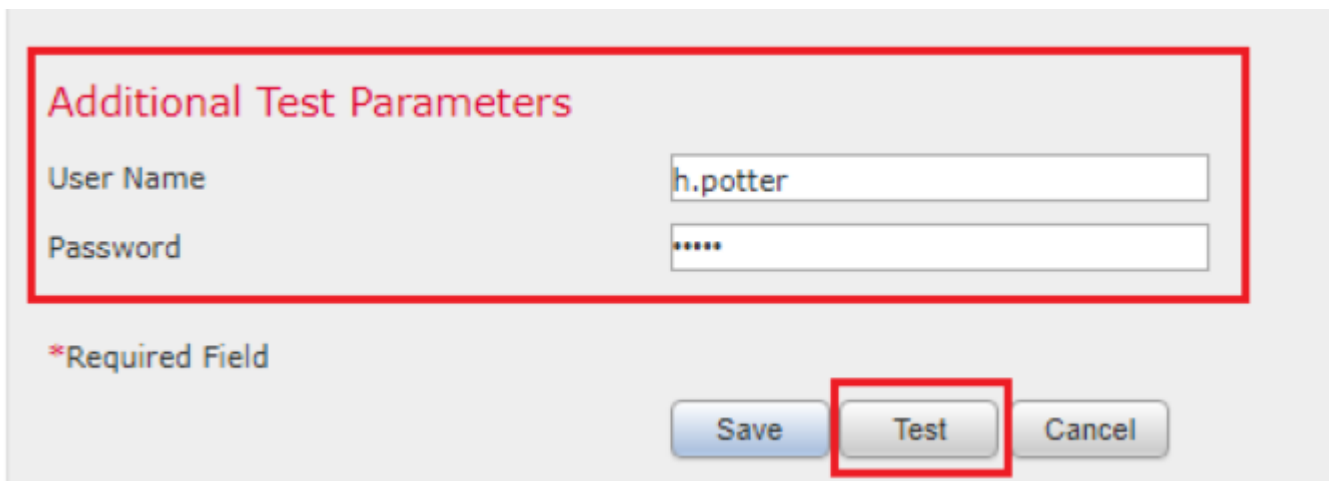


The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the following commands and their outputs:

```
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>
PS C:\Users\Administrator>
```

## LDAP-Integration testen

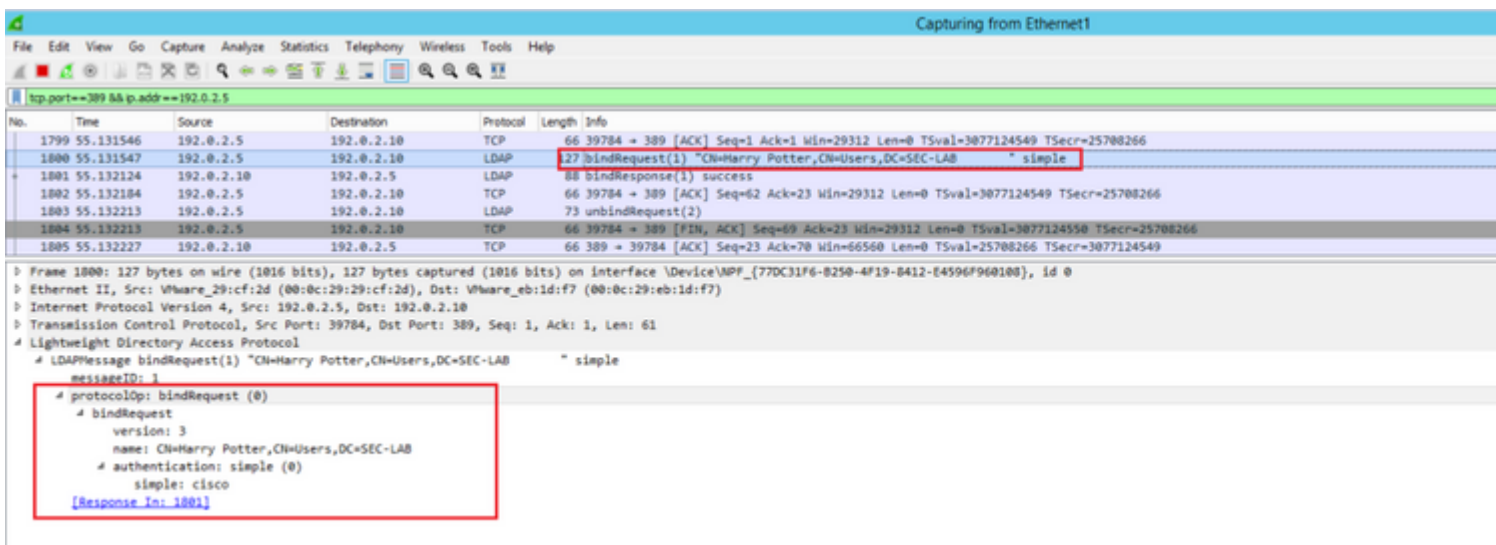
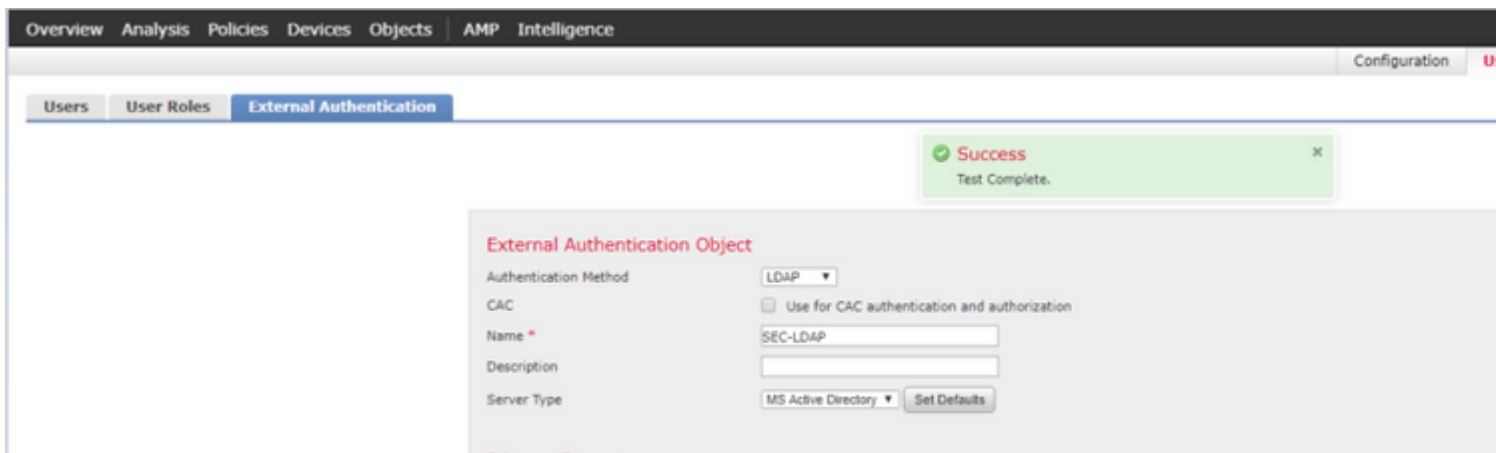
Navigieren Sie zu System > Users > External Authentication > External Authentication Object. Unten auf der Seite befindet sich ein Additional Test Parameters -Bereich, wie im Bild zu sehen:



The screenshot shows a form titled "Additional Test Parameters" with the following fields and buttons:

- User Name:** Input field containing "h.potter".
- Password:** Input field containing "\*\*\*\*\*".
- \*Required Field:** A note indicating that the fields are required.
- Buttons:** "Save", "Test", and "Cancel". The "Test" button is highlighted with a red box.

Wählen Sie den Test aus, um die Ergebnisse anzuzeigen.



## Fehlerbehebung

### Wie interagieren FMC/FTD und LDAP, um Benutzer herunterzuladen?

Damit FMC Benutzer von einem Microsoft LDAP-Server abrufen kann, muss das FMC zunächst eine Verbindungsanforderung an Port 389 oder 636 (SSL) mit den LDAP-Administratoranmeldeinformationen senden. Sobald der LDAP-Server FMC authentifizieren kann, antwortet er mit einer Erfolgsmeldung. Schließlich kann FMC eine Anfrage mit der Suchanforderungsnachricht wie in der folgenden Abbildung beschrieben stellen:

```
<< --- 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
```

Beachten Sie, dass bei der Authentifizierung Kennwörter standardmäßig unverschlüsselt gesendet werden:

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	

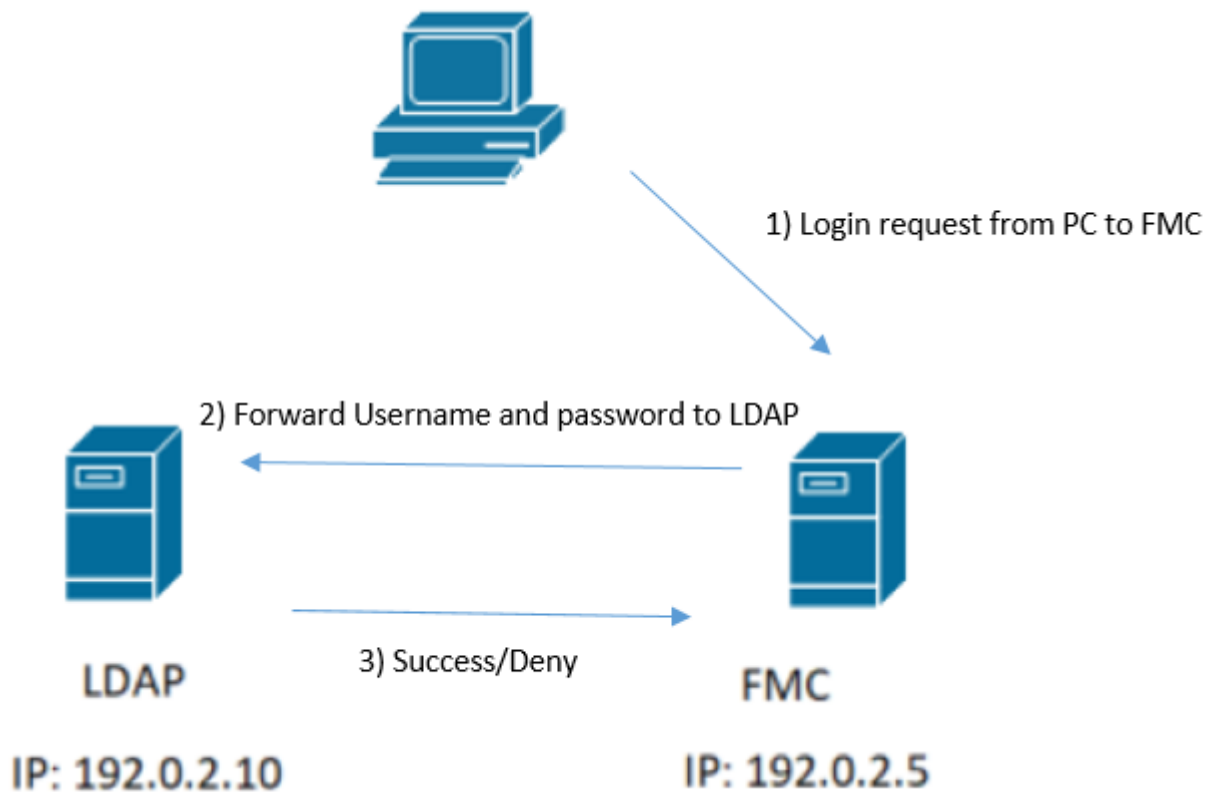
```

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]

```

## Wie interagieren FMC/FTD und LDAP, um eine Benutzeranmeldeanfrage zu authentifizieren?

Damit sich ein Benutzer bei aktivierter LDAP-Authentifizierung bei FMC oder FTD anmelden kann, wird die erste Anmeldeanforderung an Firepower gesendet. Benutzername und Kennwort werden jedoch an LDAP weitergeleitet, um eine Erfolgs-/Ablehnungsantwort zu erhalten. Das bedeutet, dass FMC und FTD Passwortinformationen nicht lokal in der Datenbank speichern und stattdessen auf die Bestätigung des LDAP warten, wie es weitergeht.





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

Wenn der Benutzername und das Passwort akzeptiert werden, wird ein Eintrag in der Web-GUI hinzugefügt, wie im Bild zu sehen:

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

Führen Sie den Befehl show user in FMC CLISH aus, um die Benutzerinformationen zu überprüfen: > show user

Der Befehl zeigt detaillierte Konfigurationsinformationen für die angegebenen Benutzer an. Diese Werte werden angezeigt:

Login (Anmeldung): der Anmelde-name

UID - die numerische Benutzer-ID

Auth (Lokal oder Remote) - wie der Benutzer authentifiziert wird

Zugriff (Basic oder Config) - die Berechtigungs-ebene des Benutzers

Aktiviert (Aktiviert oder Deaktiviert) - ob der Benutzer aktiv ist

Zurücksetzen (Ja oder Nein) - ob der Benutzer das Kennwort bei der nächsten Anmeldung ändern muss

Exp (Niemals oder eine Zahl) - die Anzahl der Tage, bis das Passwort des Benutzers geändert werden muss

Warnen (k. A. oder Zahl): Die Anzahl der Tage, die ein Benutzer erhält, um sein Kennwort vor Ablauf zu ändern

Str (Ja oder Nein) - ob das Passwort des Benutzers die Kriterien zur Überprüfung der Stärke erfüllen muss

Sperren (Ja oder Nein) - ob das Benutzerkonto aufgrund zu vieler Anmeldefehler gesperrt wurde

Max. (k. A. oder Zahl): Die maximale Anzahl fehlgeschlagener Anmeldungen, bevor das Konto des Benutzers gesperrt wird.

## SSL oder TLS funktionieren nicht wie erwartet

Wenn Sie DNS auf den FTDs nicht aktivieren, sehen Sie Fehler im Pigtail-Protokoll, die darauf hindeuten, dass LDAP nicht erreichbar ist:

```
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
```

Stellen Sie sicher, dass Firepower den FQDN der LDAP-Server auflösen kann. Wenn nicht, fügen Sie den richtigen DNS wie im Bild zu sehen.

FTD: Rufen Sie die FTD-CLISH auf, und führen Sie den folgenden Befehl aus: > 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:~$
```

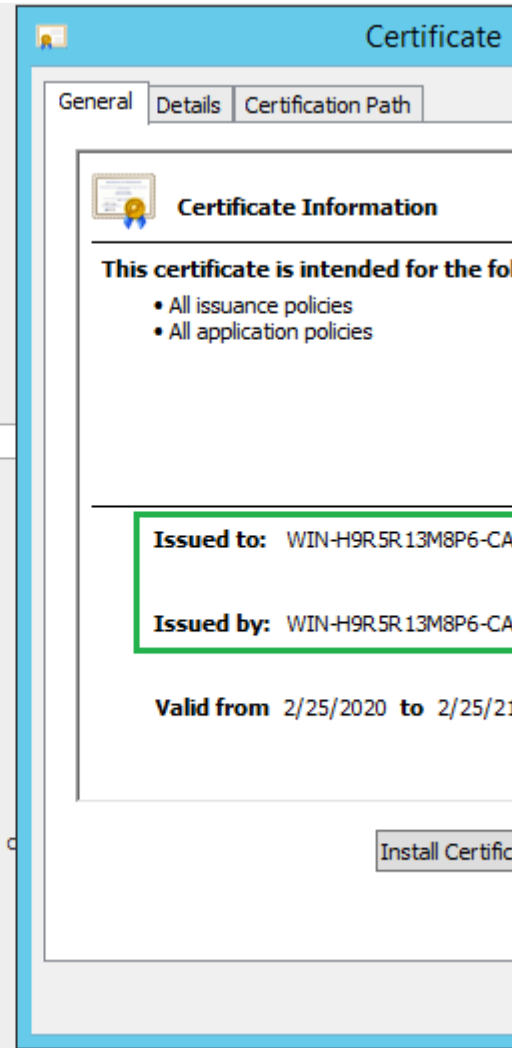
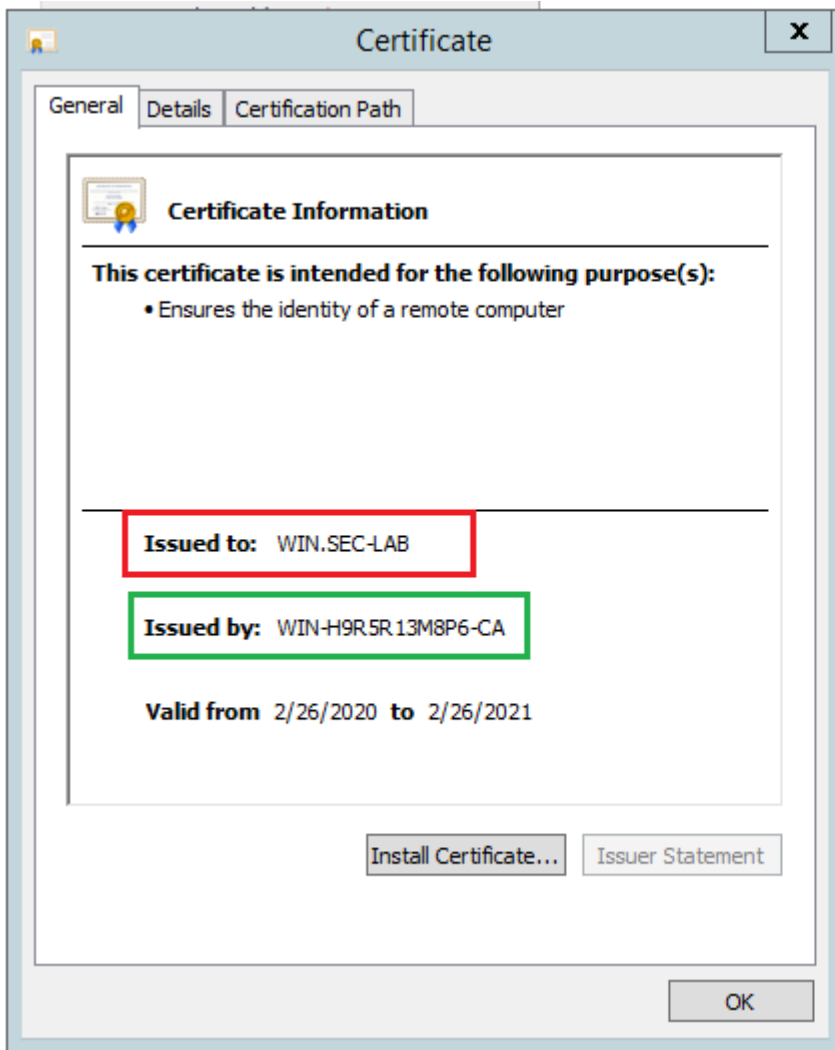
FMC: Auswählen System > Configuration, und wählen Sie dann Management Interfaces (Verwaltungsschnittstellen) aus, wie im Bild zu sehen:

The image shows a network configuration interface with a sidebar on the left and a main content area on the right. The sidebar contains a list of menu items, with 'Management Interfaces' highlighted in a red box. 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 MAC 00:0C:29:29:CF:2D and 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:** A checkbox for 'Enabled' which is unchecked.

At the bottom of the main content area are 'Save' and 'Cancel' buttons.

Stellen Sie sicher, dass es sich bei dem auf FMC hochgeladenen Zertifikat um das Zertifikat der Zertifizierungsstelle handelt, die das Serverzertifikat des LDAP signiert hat, wie im Bild gezeigt:



Verwenden Sie die Paketerfassung, um zu bestätigen, dass der LDAP-Server die richtigen Informationen sendet:



The screenshot displays a network traffic capture in Wireshark. The packet list shows a series of frames, with frame 33 highlighted. The details pane for frame 33 shows the TLSv1.2 record structure, including the Certificate field. The certificate's common name is highlighted as 'id-at-commonName=WIN.SEC-LAB'. On the right, the Cisco Firepower Management Center configuration pane shows the 'Primary Server' settings, with the 'Name' field highlighted as 'id-at-commonName=WIN.SEC-LAB'.

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

## Zugehörige Informationen

- [Benutzerkonten für Managementzugriff](#)
- [Cisco FirePOWER Management Center Lightweight Directory Access Protocol - Authentifizierung Umgehung von Schwachstellen](#)
- [Konfiguration des LDAP-Authentifizierungsobjekts auf dem FireSIGHT-System](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.