

# Configurazione di Firepower Management Center e FTD con LDAP per l'autenticazione esterna

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione LDAP di base nell'interfaccia utente di FMC](#)

[Accesso shell per utenti esterni](#)

[Autenticazione esterna per FTD](#)

[Ruoli utente](#)

[SSL o TLS](#)

[Verifica](#)

[Base di ricerca test](#)

[Verifica integrazione LDAP](#)

[Risoluzione dei problemi](#)

[Come interagiscono FMC/FTD e LDAP per scaricare gli utenti?](#)

[Come interagiscono FMC/FTD e LDAP per autenticare una richiesta di accesso utente?](#)

[SSL o TLS non funziona come previsto](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come abilitare l'autenticazione esterna LDAP (Lightweight Directory Access Protocol) di Microsoft con Cisco Firepower Management Center (FMC) e Firepower Threat Defense (FTD).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco FTD
- Cisco FMC
- LDAP Microsoft

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

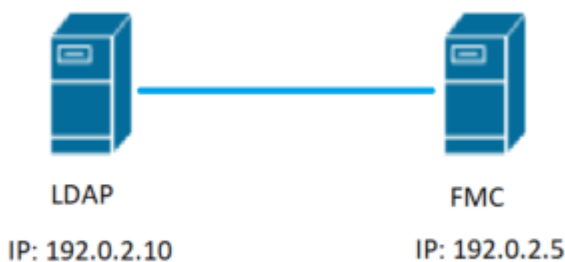
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

FMC e dispositivi gestiti includono un account amministratore predefinito per l'accesso alla gestione. È possibile aggiungere account utente personalizzati nel FMC e nei dispositivi gestiti, come utenti interni o, se supportato per il modello, come utenti esterni su un server LDAP o RADIUS. L'autenticazione utente esterno è supportata per FMC e FTD.

- Utente interno - Il dispositivo FMC/FTD controlla un database locale per l'autenticazione dell'utente.
- Utente esterno - Se l'utente non è presente nel database locale, le informazioni di sistema provenienti da un server di autenticazione LDAP o RADIUS esterno popolano il relativo database utenti.

## Esempio di rete



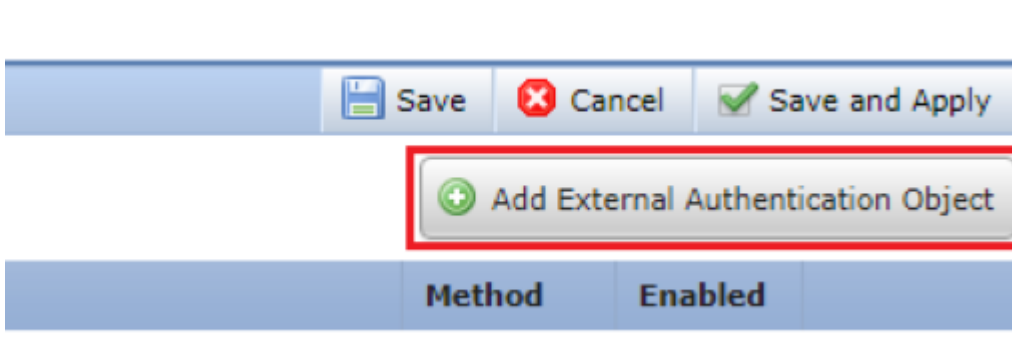
## Configurazione

### Configurazione LDAP di base nell'interfaccia utente di FMC

Passaggio 1. Passa a System > Users > External Authentication:



Passaggio 2. Scegli Add External Authentication Object:



Passaggio 3. Completare i campi obbligatori:

**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 \*:  ex. IP or hostname

Port \*:  Default port is 389 or 636 for SSL

**Backup Server (Optional)**

Host Name/IP Address:  ex. IP or hostname

Port:

**LDAP-Specific Parameters**

\*Base DN specifies where users will be found

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

Base Filter:  ex. (cn=jsmith), (|cn=jsmith), (&(cn=jsmith)(|(cn=bsmith)(cn=csmith\*)))

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 \*:

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)

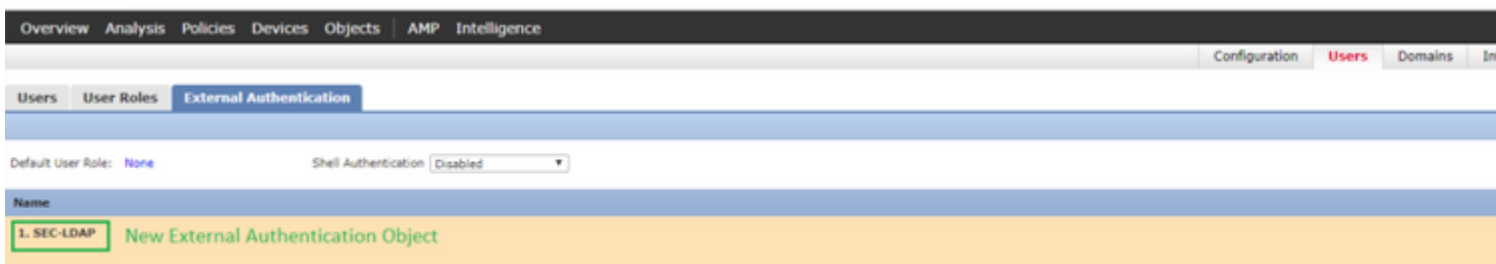
**Additional Test Parameters**

User Name

Password

\*Required Field

Passaggio 4. Attivare External Authentication Oggetto e salvataggio:



## Accesso shell per utenti esterni

La FMC supporta due diversi utenti amministratori interni: uno per l'interfaccia Web e l'altro con accesso alla CLI. Ciò significa che esiste una chiara distinzione tra chi può accedere alla GUI e chi può accedere anche alla CLI. Al momento dell'installazione, la password dell'utente amministratore predefinito viene sincronizzata in modo da essere la stessa sia sulla GUI sia sulla CLI; tuttavia, viene tenuta traccia di tali password da meccanismi interni diversi e può anche essere diversa.

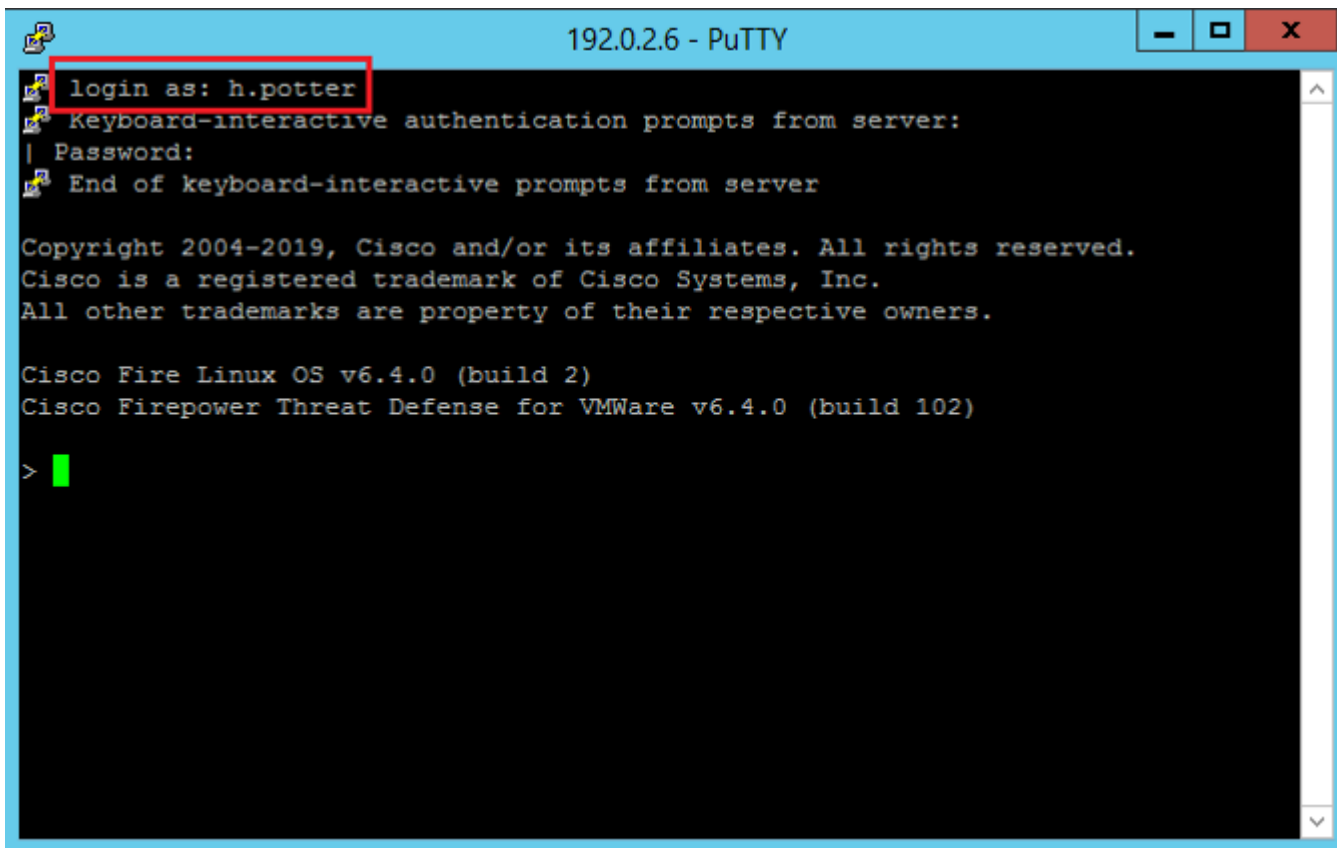
Agli utenti esterni LDAP deve inoltre essere concesso l'accesso alla shell.

Passaggio 1. Passa a System > Users > External Authentication e fare clic su Shell Authentication come nell'immagine e salvare:



Passaggio 2. Distribuire le modifiche in FMC.

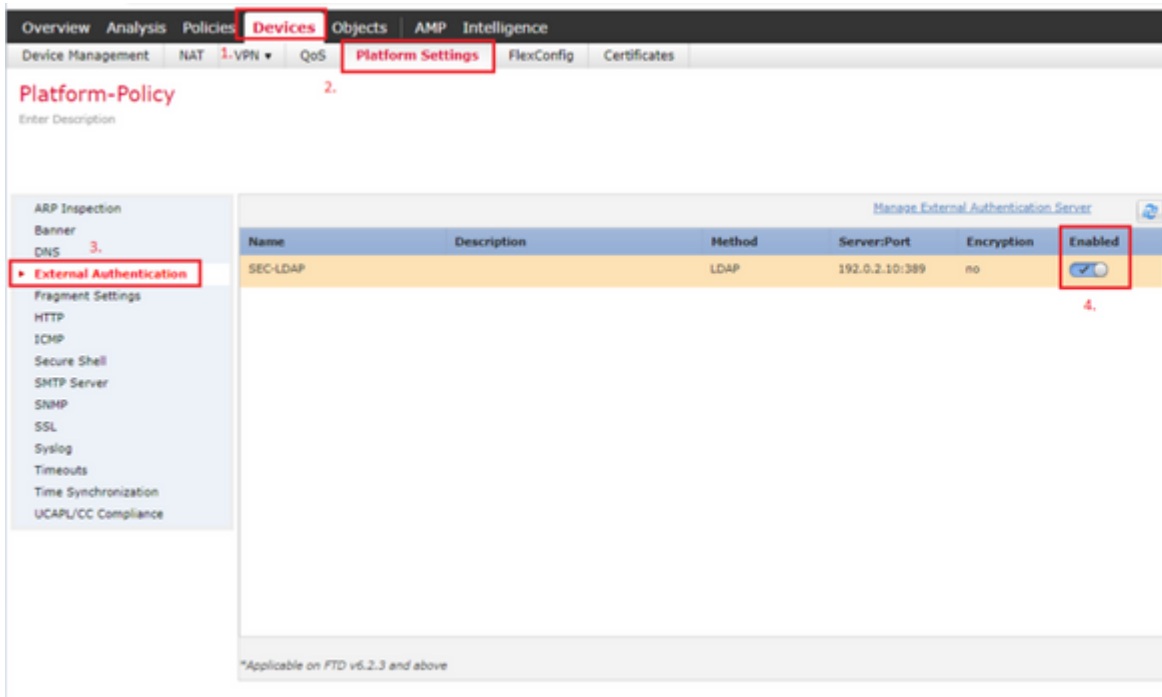
Una volta configurato l'accesso alla shell per gli utenti esterni, l'accesso tramite SSH è abilitato come mostrato nell'immagine:



## Autenticazione esterna per FTD

L'autenticazione esterna può essere abilitata sull'FTD.

Passaggio 1. Passa a Devices > Platform Settings > External Authentication. Fare clic su Enabled e salvare:



## Ruoli utente

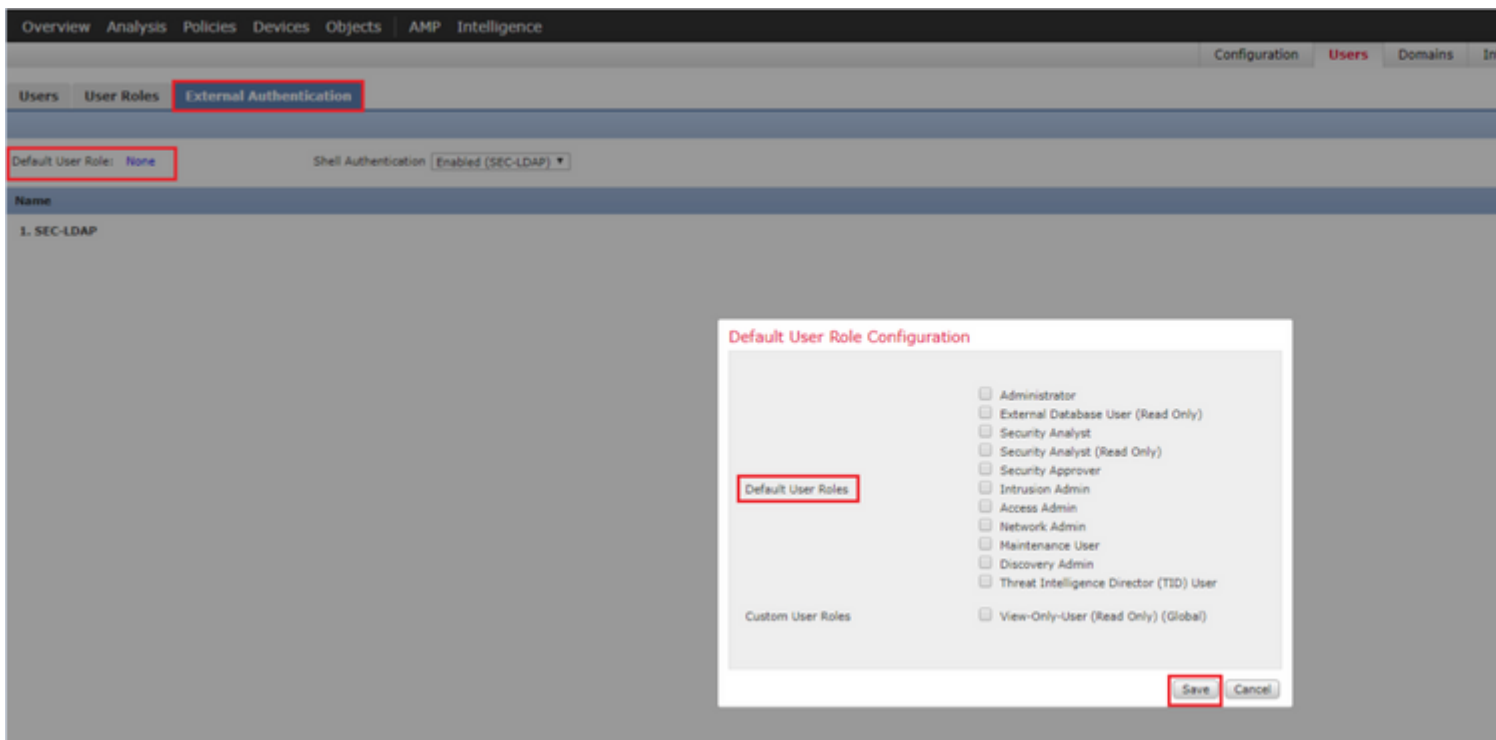
I privilegi utente sono basati sul ruolo utente assegnato. È inoltre possibile creare ruoli utente personalizzati con privilegi di accesso personalizzati in base alle esigenze dell'organizzazione oppure utilizzare ruoli predefiniti quali Security Analyst e Discovery Admin.

Esistono due tipi di ruoli utente:

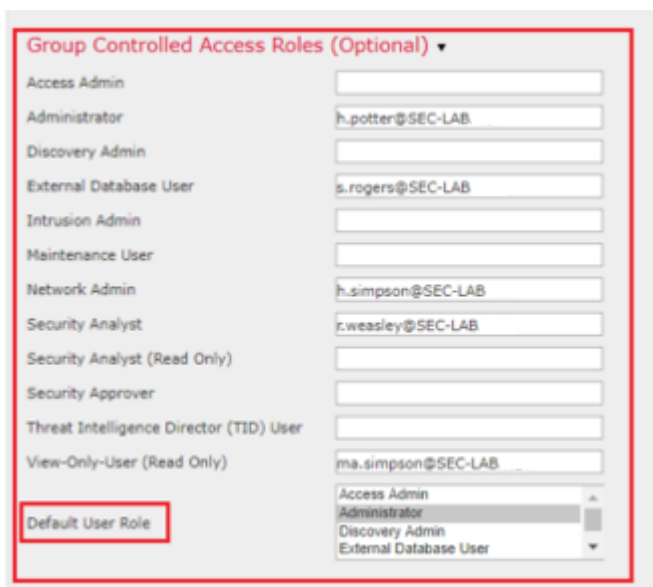
1. Ruoli utente interfaccia Web
2. Ruoli utente CLI

Per un elenco completo dei ruoli predefiniti e per ulteriori informazioni, vedere; [Ruoli utente](#).

Per configurare un ruolo utente predefinito per tutti gli oggetti di autenticazione esterna, passare a System > Users > External Authentication > Default User Role. Scegliere il ruolo utente predefinito da assegnare e fare clic su Save.



Per scegliere un ruolo utente predefinito o assegnare ruoli specifici a utenti specifici in un particolare gruppo di oggetti, è possibile scegliere l'oggetto e passare a Group Controlled Access Roles come mostrato nell'immagine:



## SSL o TLS

Il DNS deve essere configurato nel CCP. Infatti il valore Subject del certificato deve corrispondere al Authentication Object Primary Server Hostname. Dopo aver configurato Secure LDAP, le acquisizioni dei pacchetti non mostrano più le richieste di associazione in testo non crittografato.

Il protocollo SSL cambia la porta predefinita a 636 e il protocollo TLS la mantiene a 389.

**Nota:** la crittografia TLS richiede un certificato su tutte le piattaforme. Per SSL, l'FTD richiede anche un certificato. Per le altre piattaforme, SSL non richiede un certificato. Tuttavia, è consigliabile caricare sempre un certificato per SSL per evitare attacchi man-in-the-middle.

Passaggio 1. Passa a Devices > Platform Settings > External Authentication > External Authentication Object e immettere le informazioni SSL/TLS di Opzioni avanzate:

**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  No file chosen ex. PEM Format (base64 encod

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

Timeout (Seconds)

Passaggio 2. Caricare il certificato della CA che ha firmato il certificato del server. Il certificato deve essere in formato PEM.

**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)

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

Timeout (Seconds)

Passaggio 3. Salvare la configurazione.

## Verifica

### Base di ricerca test

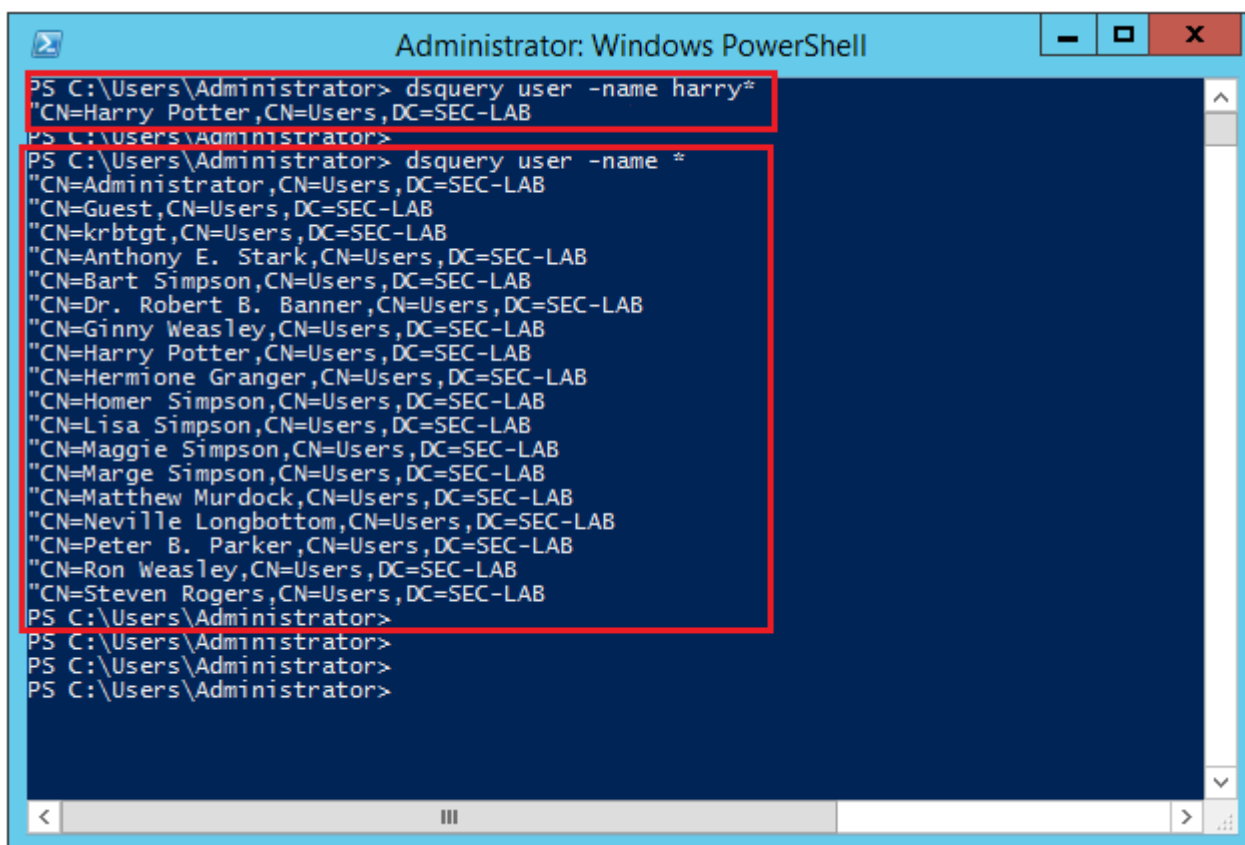
Aprire un prompt dei comandi di Windows o PowerShell in cui è configurato LDAP e digitare il comando: `dsquery user -name`

.

Ad esempio:

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

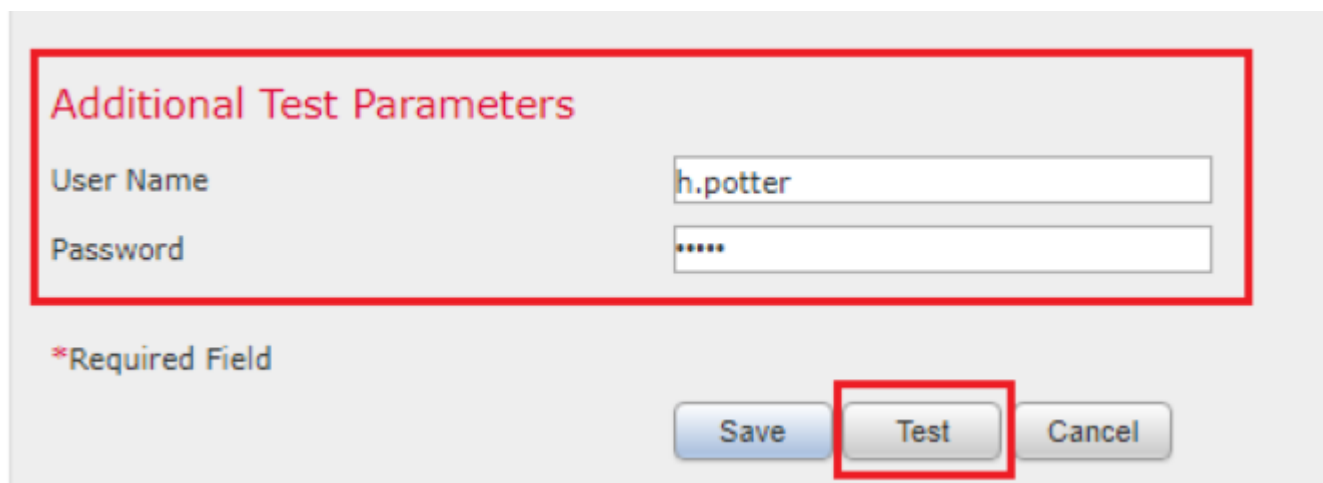




```
Administrator: Windows PowerShell
PS C:\Users\Administrator> dsquery user -name harry*
"CN=Harry Potter,CN=Users,DC=SEC-LAB
PS C:\Users\Administrator>
PS C:\Users\Administrator> dsquery user -name *
"CN=Administrator,CN=Users,DC=SEC-LAB
"CN=Guest,CN=Users,DC=SEC-LAB
"CN=krbtgt,CN=Users,DC=SEC-LAB
"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>
```

## Verifica integrazione LDAP

Passa a System > Users > External Authentication > External Authentication Object. Nella parte inferiore della pagina è presente una Additional Test Parameters come nell'immagine:



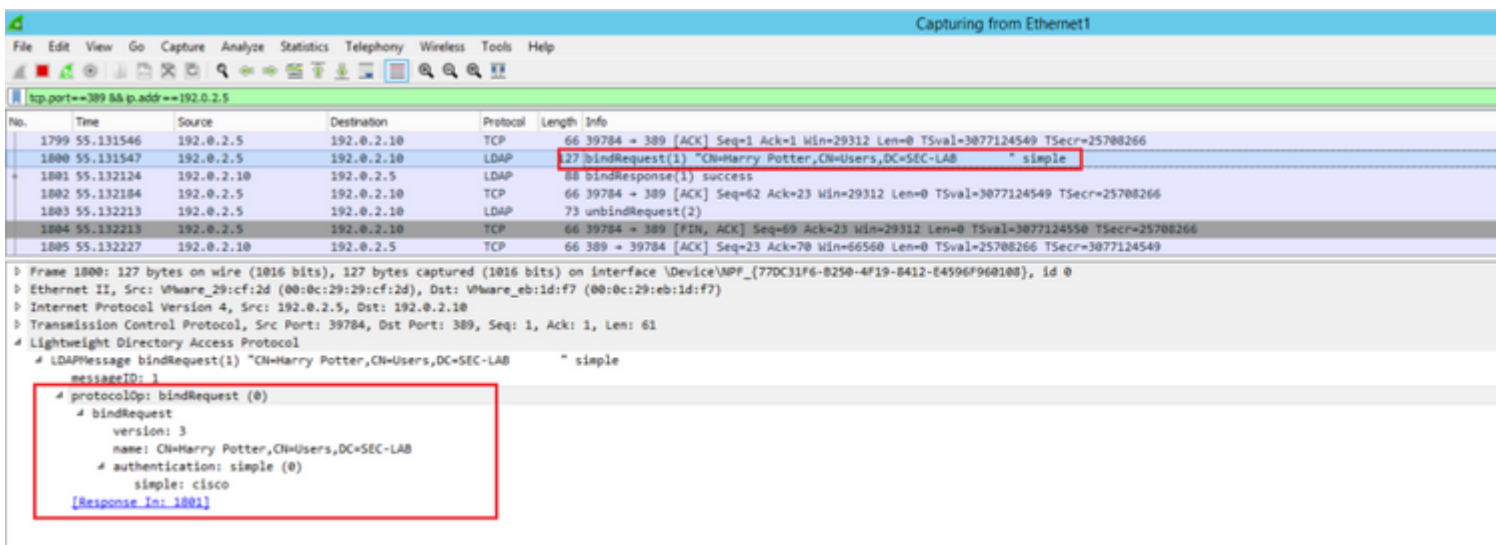
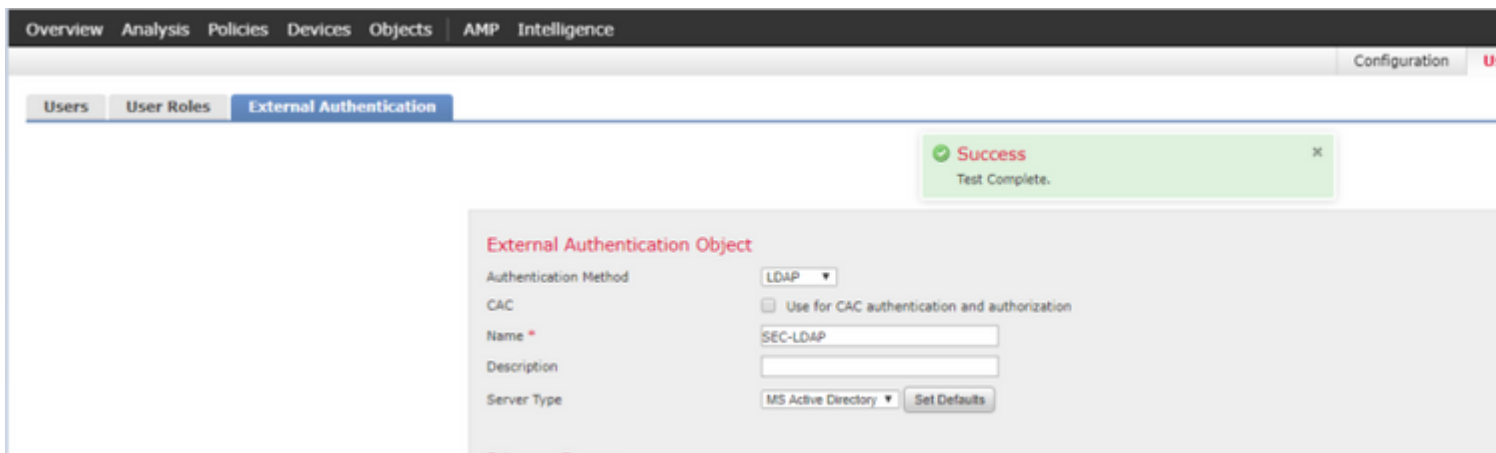
**Additional Test Parameters**

User Name

Password

\*Required Field

Scegliere il Test per visualizzare i risultati.



## Risoluzione dei problemi

### Come interagiscono FMC/FTD e LDAP per scaricare gli utenti?

Affinché FMC possa prelevare utenti da un server LDAP Microsoft, deve prima inviare una richiesta di binding sulla porta 389 o 636 (SSL) con le credenziali di amministratore LDAP. Una volta che il server LDAP è in grado di autenticare FMC, risponde con un messaggio di operazione riuscita. Infine, FMC è in grado di effettuare una richiesta con il messaggio Search Request descritto nel diagramma:

```
<< --- 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
```

Si noti che l'autenticazione invia le password in chiaro per impostazione predefinita:

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	

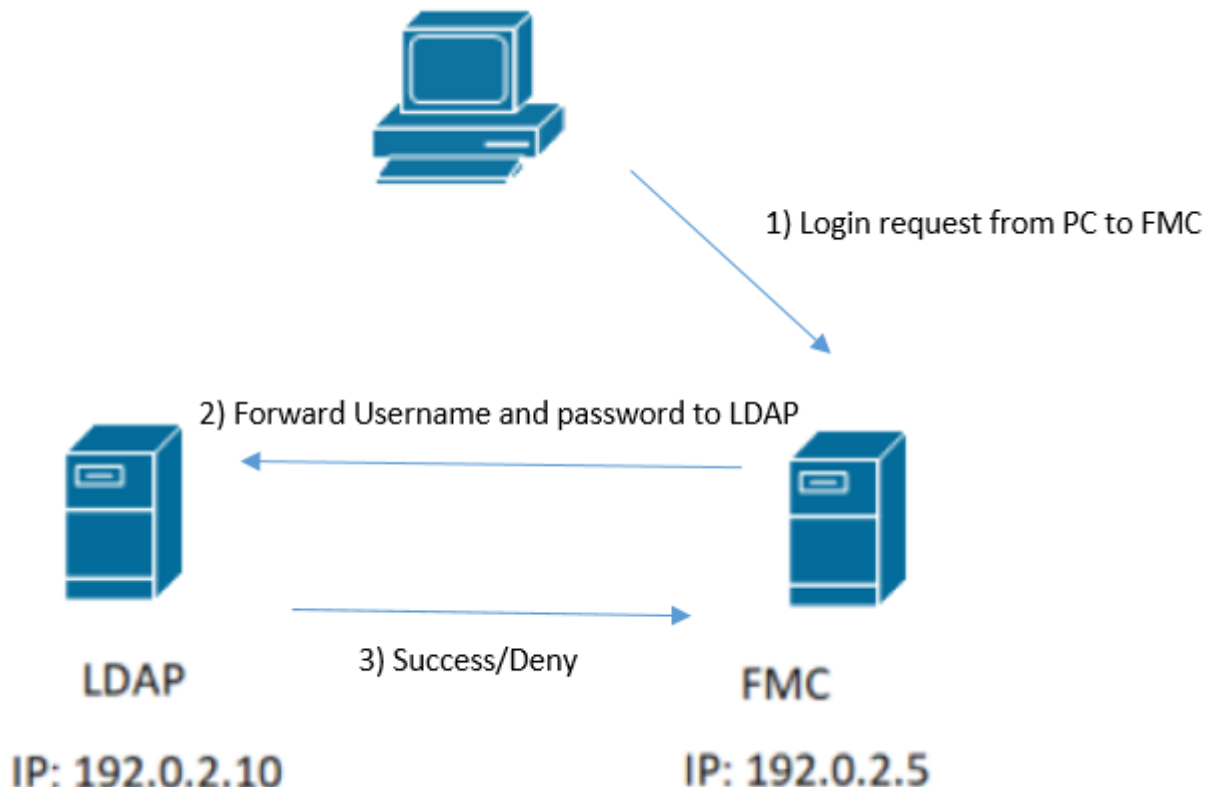
```

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]

```

## Come interagiscono FMC/FTD e LDAP per autenticare una richiesta di accesso utente?

Affinché un utente possa accedere a FMC o FTD mentre l'autenticazione LDAP è abilitata, la richiesta di accesso iniziale viene inviata a Firepower, tuttavia, il nome utente e la password vengono inoltrati a LDAP per una risposta di esito positivo/negativo. Ciò significa che FMC e FTD non conservano le informazioni sulla password localmente nel database e attendono invece la conferma di LDAP su come procedere.





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

Se il nome utente e la password vengono accettati, viene aggiunta una voce nell'interfaccia utente del Web come mostrato nell'immagine:

Username	Roles	Authentication Method	Password Lifetime
admin	Administrator	Internal	Unlimited
h.potter	Administrator	External	

Eeguire il comando show user in FMC CLISH per verificare le informazioni utente: > show user

Il comando visualizza informazioni di configurazione dettagliate per gli utenti specificati. Vengono

visualizzati i seguenti valori:

Login " il nome di login

UID " l'ID utente numerico

Auth (locale o remota) - modalità di autenticazione dell'utente

Access (Basic o Config): il livello di privilegi dell'utente

Abilitato (abilitato o disabilitato) " indica se l'utente è attivo

Reimposta (Sì o No) - Consente di specificare se l'utente deve modificare la password al successivo accesso

Exp (Never o number) - Numero di giorni trascorsi i quali è necessario modificare la password dell'utente.

Avviso (N/D o numero): il numero di giorni concessi a un utente per modificare la password prima della scadenza

Str (Sì o No) " indica se la password dell'utente deve soddisfare i criteri per verificare il livello

Lock (Yes o No) - se l'account dell'utente è stato bloccato a causa di troppi errori di accesso

Max (N/D o un numero): il numero massimo di accessi non riusciti prima che l'account dell'utente venga bloccato

## SSL o TLS non funziona come previsto

Se non si abilita il DNS sugli FTD, nel log pigtail verranno visualizzati errori che indicano che LDAP non è raggiungibile:

```
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
```

Accertarsi che Firepower sia in grado di risolvere l'FQDN dei server LDAP. In caso contrario, aggiungere il DNS corretto come visualizzato nell'immagine.

FTD: accedere al CLISH FTD ed eseguire il comando: > 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:~$
```

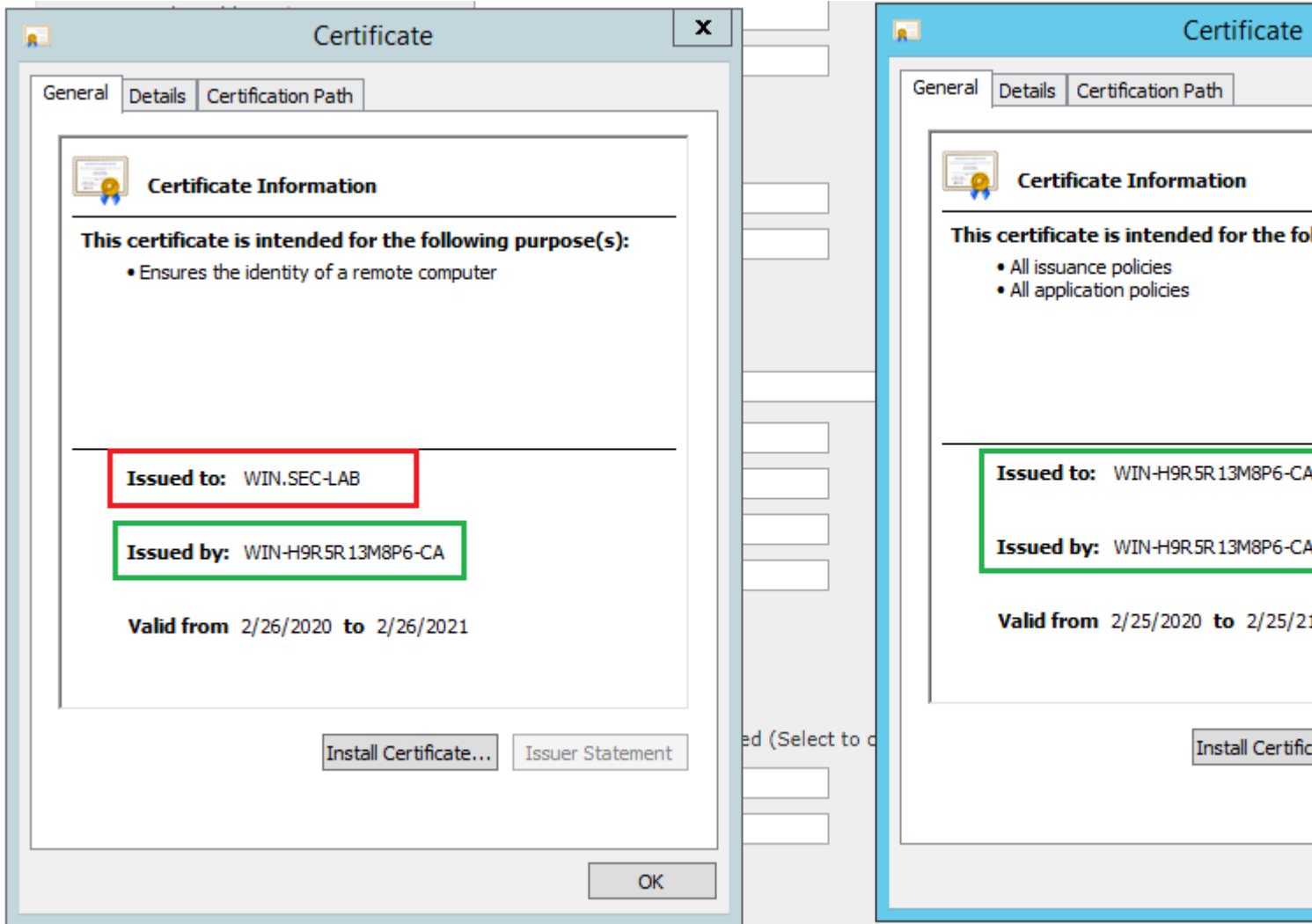
FMC: Scegli System > Configurazione quindi scegliere Interfacce di gestione come illustrato nell'immagine:

The image shows a configuration interface for a network device. On the left is a navigation menu with 'Management Interfaces' highlighted in red. 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 of the main content area are 'Save' and 'Cancel' buttons.

Verificare che il certificato caricato in FMC sia il certificato della CA che ha firmato il certificato server del server LDAP, come illustrato nell'immagine:



Utilizzare le acquisizioni di pacchetti per confermare che il server LDAP invia le informazioni corrette:



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

## Informazioni correlate

- [Account utente per l'accesso alla gestione](#)
- [Cisco Firepower Management Center Lightweight Directory Access Protocol Authentication Bypass Vulnerability](#)
- [Configurazione dell'oggetto di autenticazione LDAP sul sistema FireSIGHT](#)
- [Documentazione e supporto tecnico "Cisco Systems"](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).