

Firepower Management Center en FTD configureren met LDAP voor externe verificatie

Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Achtergrondinformatie](#)
- [Netwerkdigram](#)
- [Configureren](#)
- [Basis LDAP-configuratie in FMC GUI](#)
- [Shell Access voor externe gebruikers](#)
- [Externe verificatie naar FTD](#)
- [Gebruikersrollen](#)
- [SSL of TLS](#)
- [Verifiëren](#)
- [Zoekbasis testen](#)
- [Test LDAP-integratie](#)
- [Problemen oplossen](#)
- [Hoe werken FMC/FTD en LDAP samen om gebruikers te downloaden?](#)
- [Hoe werken FMC/FTD en LDAP samen om een gebruikersaanmelding te verifiëren?](#)
- [SSL of TLS werkt niet zoals verwacht](#)
- [Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de externe verificatie van Microsoft Lichtgewicht Directory Access Protocol (LDAP) kunt inschakelen met Cisco Firepower Management Center (FMC) en Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco FTD
- Cisco VCC
- Microsoft LDAP

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FTD 6.5.0-123
- VCC 6.5.0-15
- Microsoft Server 2012

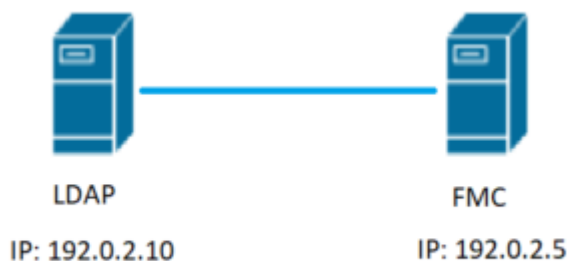
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het VCC en de beheerde apparaten omvatten een standaard admin-account voor beheertoegang. U kunt aangepaste gebruikersaccounts toevoegen op het VCC en op beheerde apparaten, als interne gebruikers of, indien ondersteund voor uw model, als externe gebruikers op een LDAP- of RADIUS-server. Externe gebruikersverificatie wordt ondersteund voor FMC en FTD.

- Interne gebruiker - Het FMC/FTD-apparaat controleert een lokale database op gebruikersverificatie.
- Externe gebruiker - Als de gebruiker niet aanwezig is in de lokale database, vult de systeem informatie van een externe LDAP- of RADIUS-verificatieserver zijn gebruikersdatabase in.

Netwerkdigram



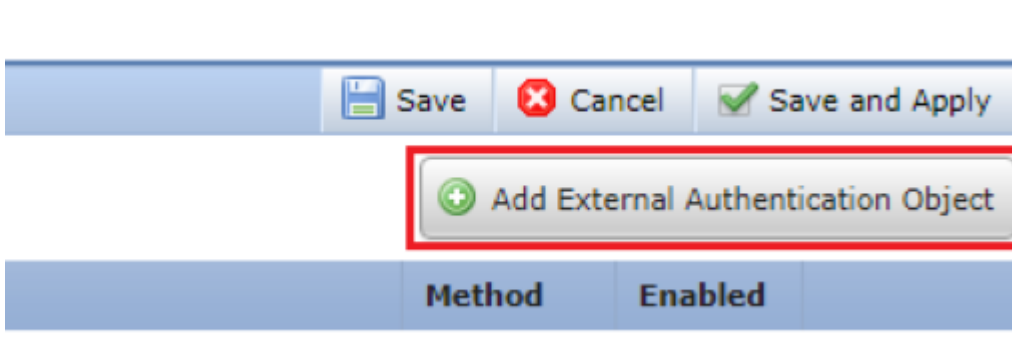
Configureren

Basis LDAP-configuratie in FMC GUI

Stap 1. Naar navigeren System > Users > External Authentication:



Stap 2. Kiezen Add External Authentication Object:



Stap 3. Vul de vereiste velden in:

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

Stap 4. Schakel de External Authentication Voorwerp en opslaan:



Shell Access voor externe gebruikers

Het FMC ondersteunt twee verschillende interne admin-gebruikers: een voor de webinterface en een ander met CLI-toegang. Dit betekent dat er een duidelijk onderscheid bestaat tussen wie toegang heeft tot de GUI en wie ook toegang heeft tot CLI. Op het moment van installatie is het wachtwoord voor de standaard beheerder gebruiker gesynchroniseerd om hetzelfde te zijn op zowel GUI als CLI, maar ze worden bijgehouden door verschillende interne mechanismen en kunnen uiteindelijk anders zijn.

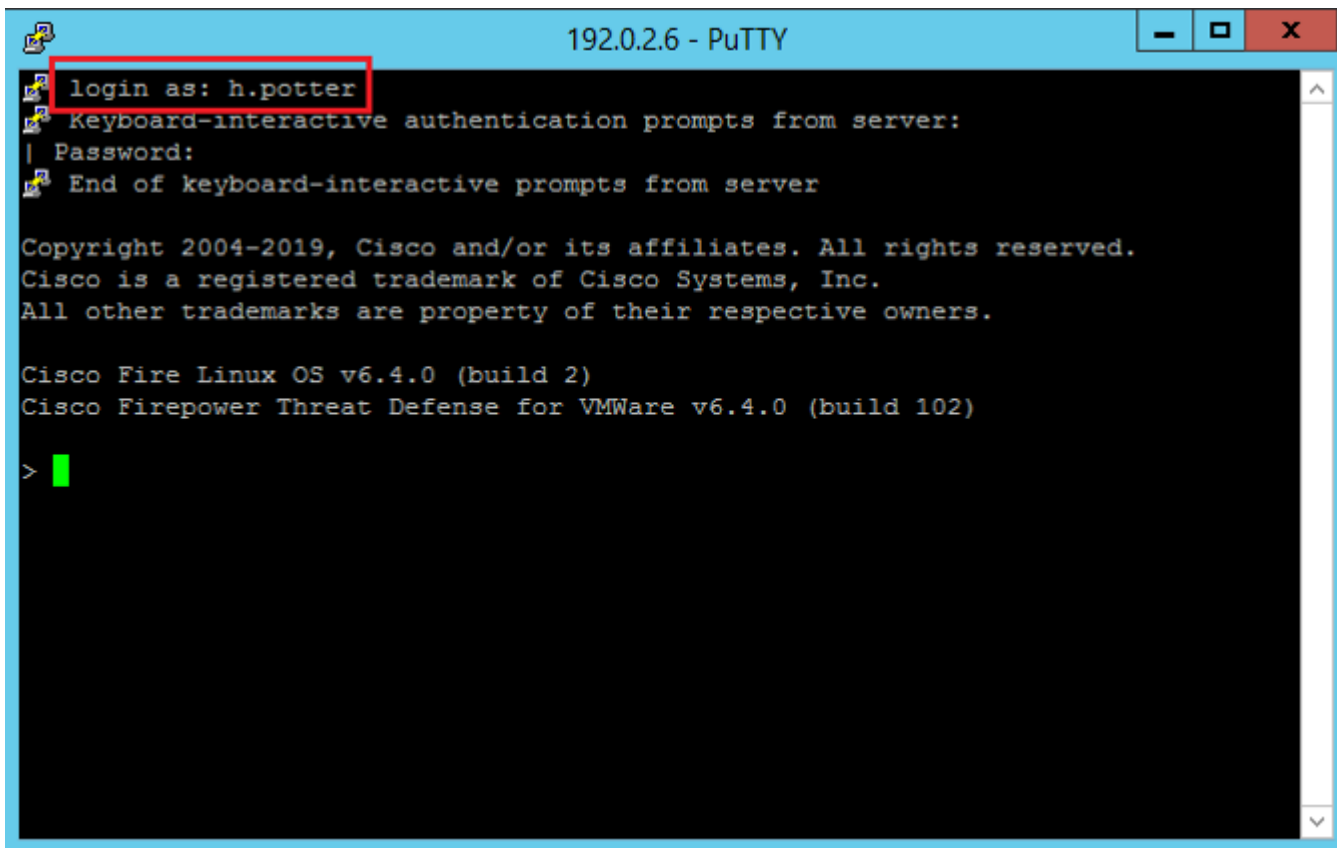
LDAP Externe gebruikers moeten ook toegang tot shell krijgen.

Stap 1. Naar navigeren System > Users > External Authentication en klik op Shell Authentication vervolgkeuzelijst zoals in de afbeelding en opslaan:



Stap 2. Veranderingen in het VCC toepassen.

Zodra shell-toegang voor externe gebruikers is geconfigureerd, wordt login via SSH ingeschakeld zoals in de afbeelding:



Externe verificatie naar FTD

Externe verificatie kan worden ingeschakeld op FTD.

Stap 1. Naar navigeren `Devices > Platform Settings > External Authentication`. Klik op de knop `Enabled` en opslaan:

The screenshot shows the Cisco FTD configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this, there are tabs for 'Device Management', 'NAT', '1-VPN', 'QoS', 'Platform Settings', 'FlexConfig', and 'Certificates'. The main heading is 'Platform-Policy' with a sub-heading 'Enter Description'. On the left, a sidebar menu lists various settings: 'ARP Inspection', 'Banner', 'DNS', 'External Authentication', 'Fragment Settings', 'HTTP', 'ICMP', 'Secure Shell', 'SMTP Server', 'SNMP', 'SSL', 'Syslog', 'Timeouts', 'Time Synchronization', and 'UCAPL/CC Compliance'. The 'External Authentication' option is highlighted. The main content area is titled 'Manage External Authentication Server' and contains a table with the following data:

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

At the bottom of the main content area, there is a note: '*Applicable on FTD v6.2.3 and above'. The 'Enabled' checkbox in the table is highlighted with a red box and labeled '4'.

Gebruikersrollen

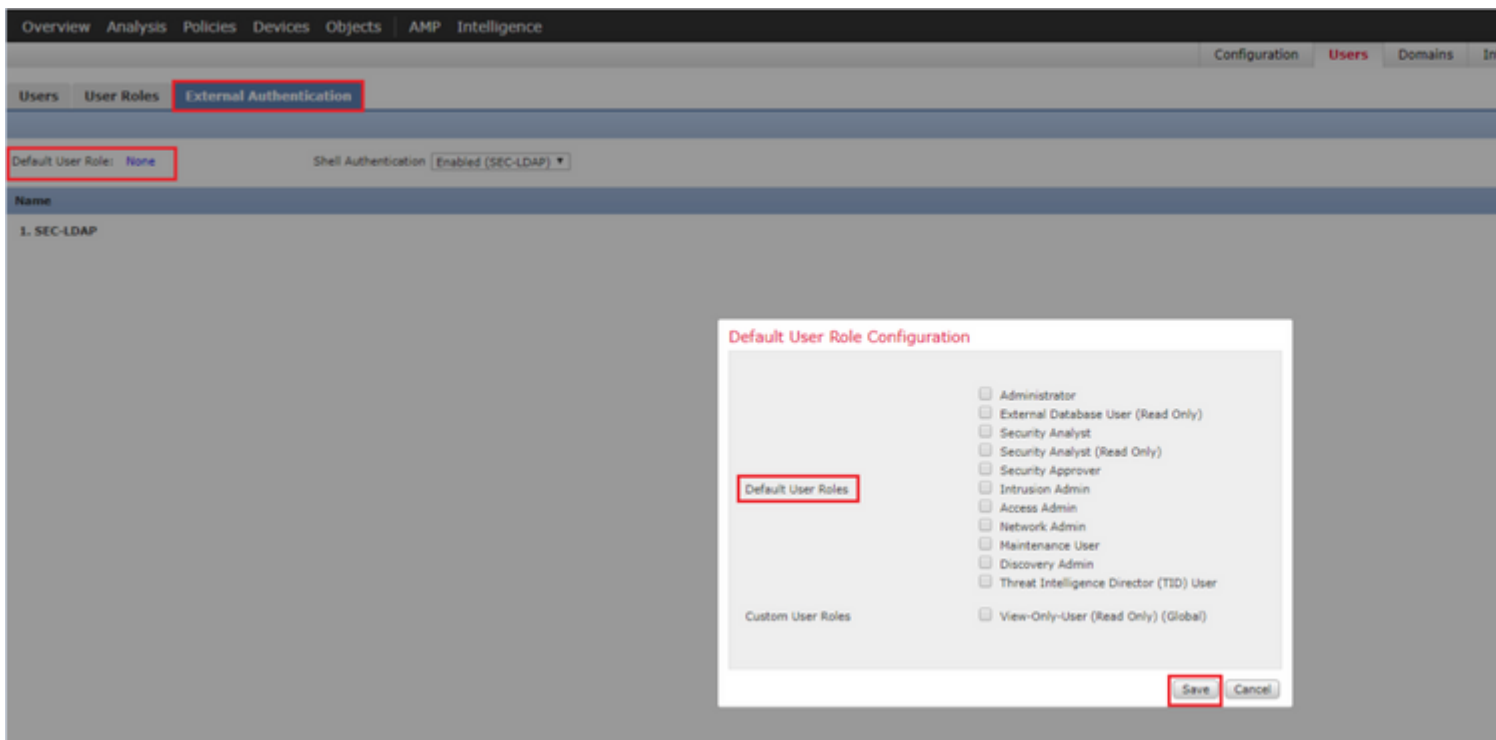
Gebruikersrechten zijn gebaseerd op de toegewezen gebruikersrol. U kunt ook aangepaste gebruikersrollen maken met toegangsrechten die zijn afgestemd op de behoeften van uw organisatie of u kunt vooraf gedefinieerde rollen gebruiken zoals Security Analyst en Discovery Admin.

Er zijn twee soorten gebruikersrollen:

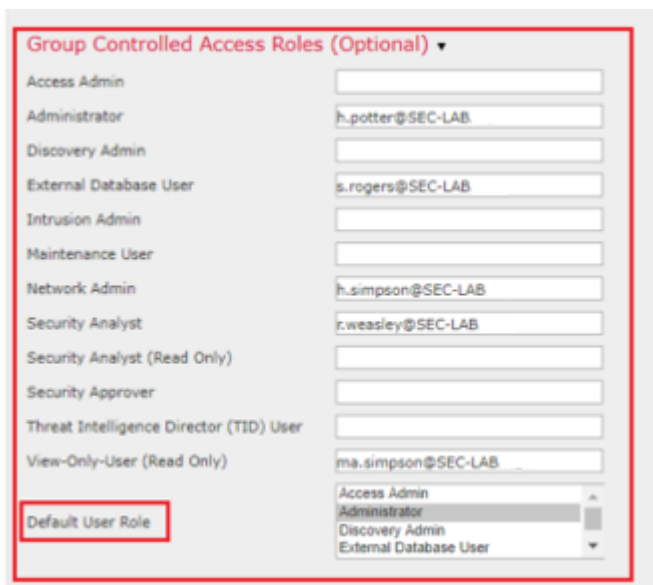
1. Gebruikersrollen voor webinterfaces
2. CLI-gebruikersrollen

Voor een volledige lijst van vooraf gedefinieerde rollen en meer informatie, raadpleegt u: [Gebruikersrollen](#).

Om een standaardgebruikersrol voor alle externe verificatieobjecten te configureren, navigeer naar System > Users > External Authentication > Default User Role. Kies de standaardgebruikersrol die u wilt toewijzen en klik op Save.



Om een standaardgebruikersrol te kiezen of specifieke rollen toe te wijzen aan specifieke gebruikers in een bepaalde objectgroep, kunt u het object kiezen en naar navigeren Group Controlled Access Roles zoals te zien op de afbeelding:



SSL of TLS

DNS moet in het VCC worden geconfigureerd. Dit komt doordat de onderwerpwaarde van het certificaat moet overeenkomen met de Authentication Object Primary Server Hostname. Zodra Secure LDAP is geconfigureerd, tonen pakketopnamen geen duidelijke tekstbindverzoeken meer.

SSL verandert de standaardpoort in 636 en TLS houdt het als 389.

Opmerking: voor TLS-versleuteling is een certificaat op alle platforms vereist. Voor SSL vereist het FTD ook een certificaat. Voor andere platforms heeft SSL geen certificaat nodig. Het wordt echter aanbevolen om altijd een certificaat voor SSL te uploaden om man-in-the-middle aanvallen te

voorkomen.

Stap 1. Naar navigeren Devices > Platform Settings > External Authentication > External Authentication Object en voer de SSL/TLS-informatie over geavanceerde opties in:

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)

Stap 2. Upload het certificaat van de CA die het certificaat van de server heeft ondertekend. Het certificaat moet in PEM-formaat zijn opgesteld.

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)

Stap 3. Sla de configuratie op.

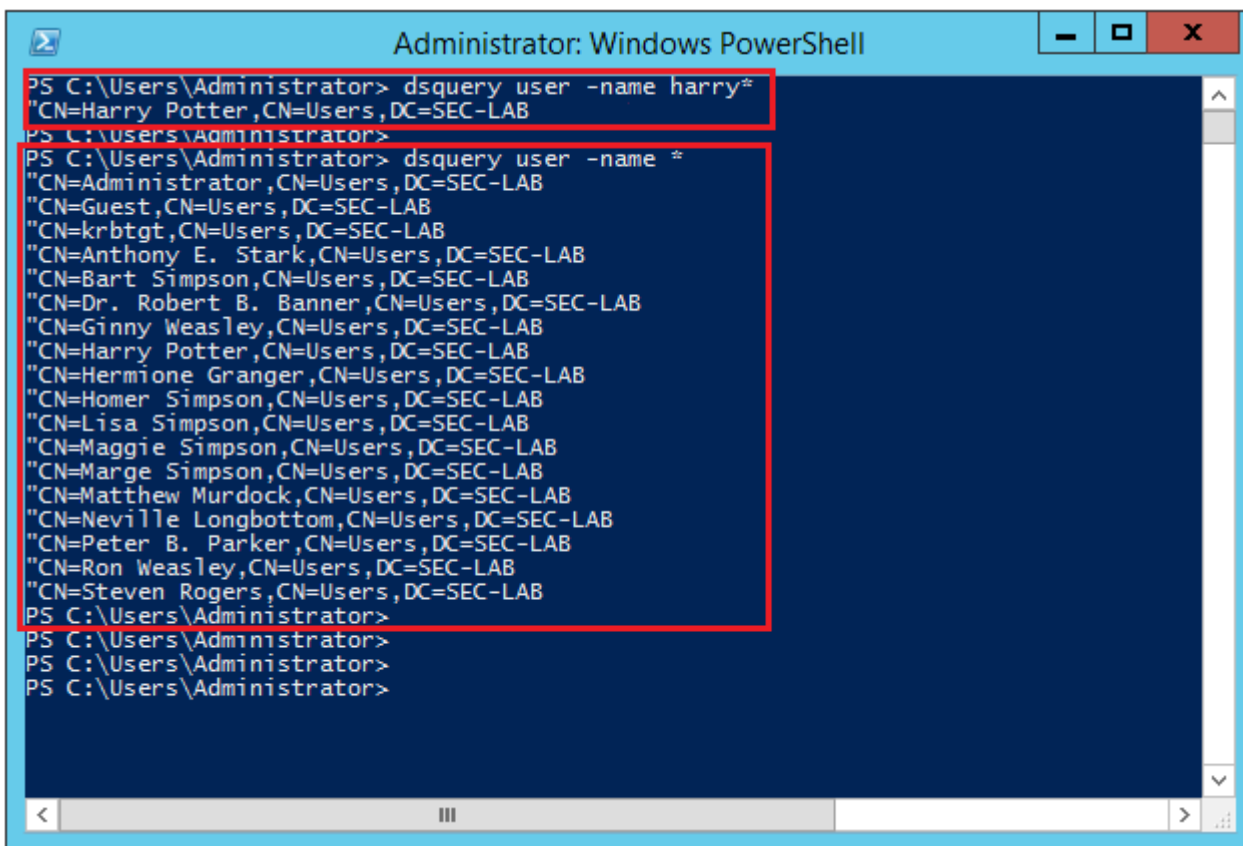
Verifiëren

Zoekbasis testen

Open een Windows-opdrachtprompt of PowerShell waar LDAP is geconfigureerd en typ de opdracht: dsquery user -name

Voorbeeld:


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

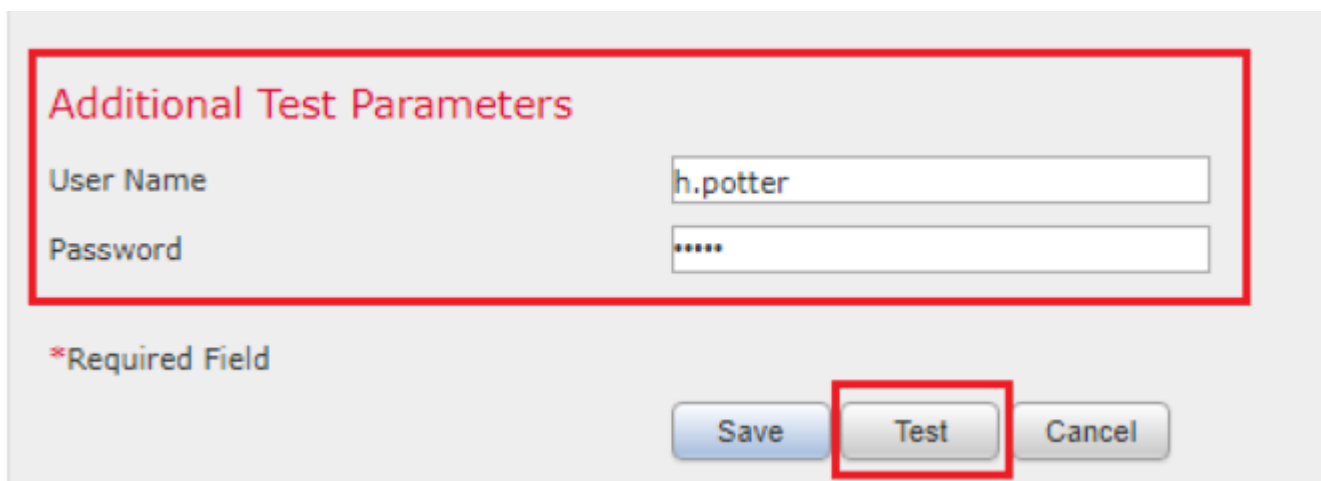


The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The terminal output is as follows:

```
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>
```

Test LDAP-integratie

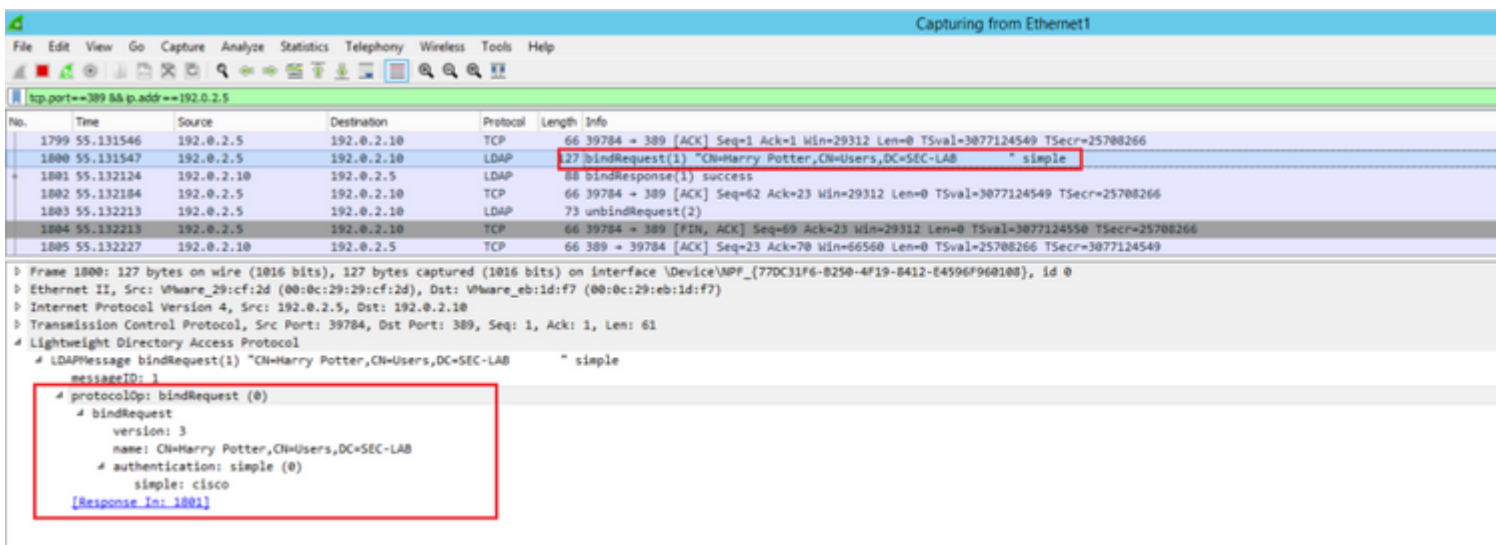
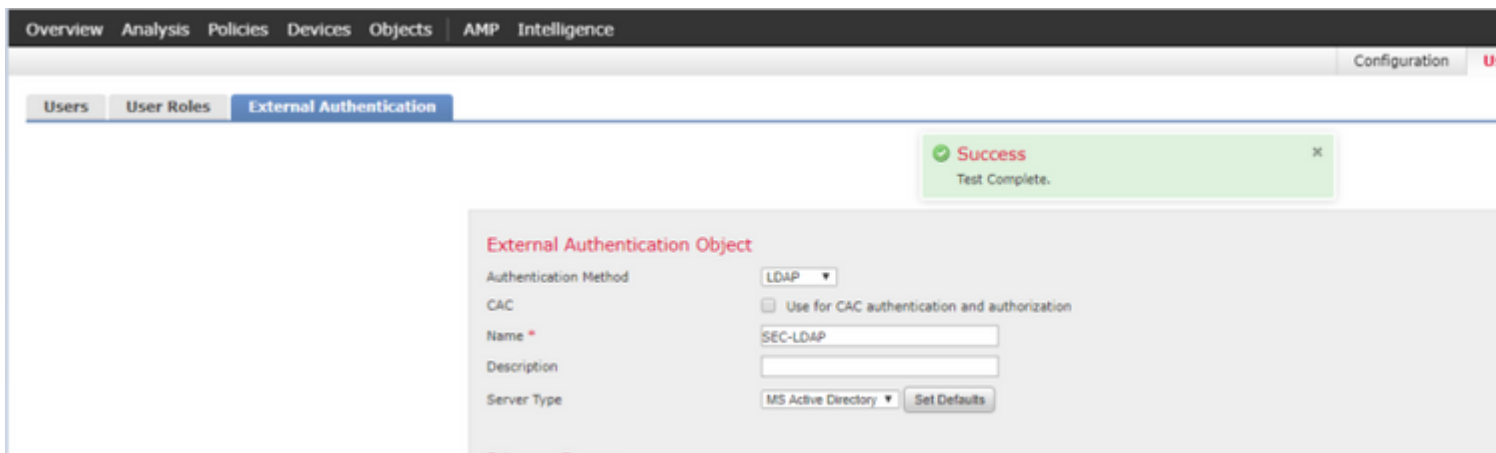
Naar navigeren System > Users > External Authentication > External Authentication Object. Onderaan de pagina is een Additional Test Parameters gedeelte zoals in het beeld:



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 label indicating that the fields are required.
- Buttons:** "Save", "Test", and "Cancel". The "Test" button is highlighted with a red box.

Kies de Test om de resultaten te zien.



Problemen oplossen

Hoe werken FMC/FTD en LDAP samen om gebruikers te downloaden?

Om het VCC in staat te stellen gebruikers van een Microsoft LDAP-server te halen, moet het VCC eerst een bind verzoek verzenden op poort 389 of 636 (SSL) met de LDAP-beheerderreferenties. Zodra de LDAP-server in staat is om het VCC te authenticeren, reageert het met een succesbericht. Tot slot kan het VCC een verzoek indienen met het bericht "zoekopdracht" Aanvraag zoals beschreven in het 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
```

Bericht dat de authenticatie wachtwoorden in duidelijk door gebrek verzendt:

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

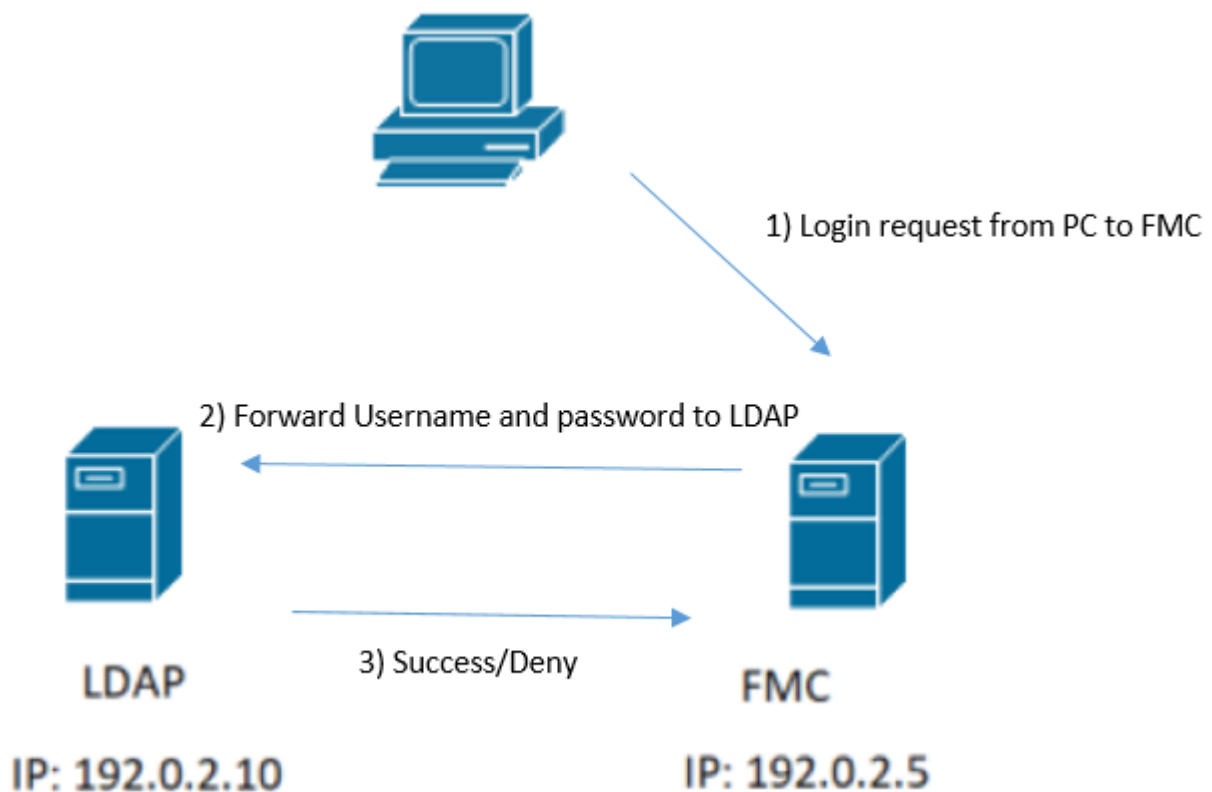
```

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]

```

Hoe werken FMC/FTD en LDAP samen om een gebruikersaanmelding te verifiëren?

Om een gebruiker in staat te stellen in te loggen op FMC of FTD terwijl LDAP-verificatie is ingeschakeld, wordt het eerste inlogverzoek naar Firepower gestuurd. De gebruikersnaam en het wachtwoord worden echter doorgestuurd naar LDAP voor een succes/ontkenning-antwoord. Dit betekent dat het VCC en de FTD de wachtwoordinformatie niet lokaal in de gegevensbank bewaren en in plaats daarvan wachten op bevestiging van LDAP over hoe te werk te gaan.





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

Als de gebruikersnaam en het wachtwoord worden geaccepteerd, wordt een vermelding toegevoegd in de web GUI zoals in de afbeelding:

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

Voer de opdracht show user in FMC CLISH om gebruikersinformatie te verifiëren: > show user

Op de opdracht wordt gedetailleerde configuratie-informatie voor de gespecificeerde gebruiker(s)

weergegeven. Deze waarden worden weergegeven:

Aanmelden â€” de inlognaam

UID â€” de numerieke gebruikers-ID

Auth (lokaal of extern) â€” hoe de gebruiker wordt geverifieerd

Toegang (Basis of Config) â€” het prioriteitsniveau van de gebruiker

Ingeschakeld (Ingeschakeld of Uitgeschakeld) â€” of de gebruiker actief is

Reset (Ja of Nee) â€” of de gebruiker het wachtwoord moet wijzigen bij de volgende aanmelding

Exp (Nooit of een getal) â€” het aantal dagen tot het wachtwoord van de gebruiker moet worden gewijzigd

Waarschuwing (N.v.t. of een nummer) â€” het aantal dagen dat een gebruiker krijgt om zijn wachtwoord te wijzigen voordat het verloopt

Str (Ja of Nee) â€” of het wachtwoord van de gebruiker moet voldoen aan de criteria om de sterkte te controleren

Vergrendelen (Ja of Nee) â€” of het account van de gebruiker is vergrendeld vanwege te veel inlogfouten

Max. (N/A of een getal) â€” het maximale aantal mislukte aanmeldingen voordat de account van de gebruiker is vergrendeld

SSL of TLS werkt niet zoals verwacht

Als u DNS op de FTD's niet inschakelt, kunt u fouten in het logboek zien die erop wijzen dat LDAP onbereikbaar is:

```
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
```

Zorg ervoor dat Firepower in staat is om de LDAP servers FQDN op te lossen. Als dit niet het geval is, voegt u de juiste DNS toe zoals in de afbeelding wordt weergegeven.

FTD: Open de FTD CLISH en voer de opdracht uit: > 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:~$
```

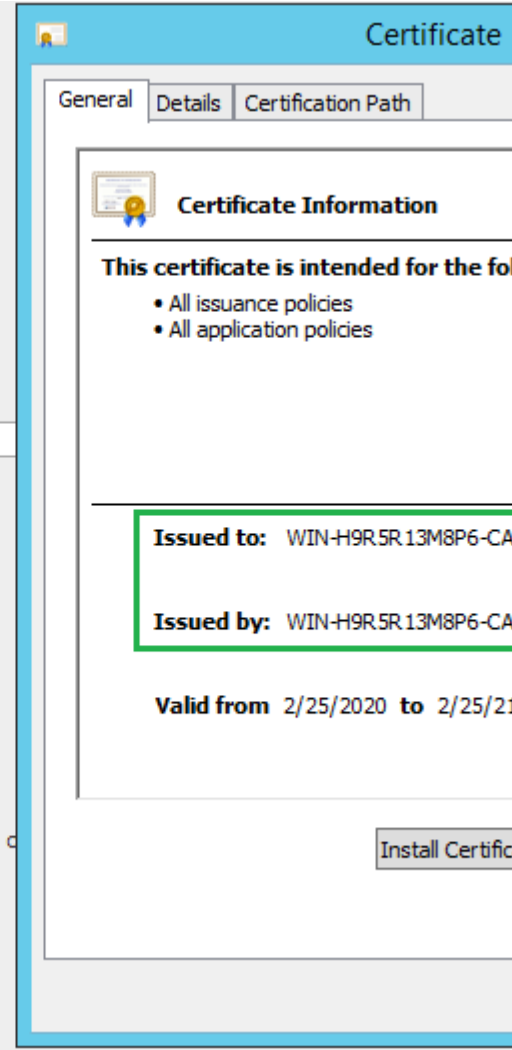
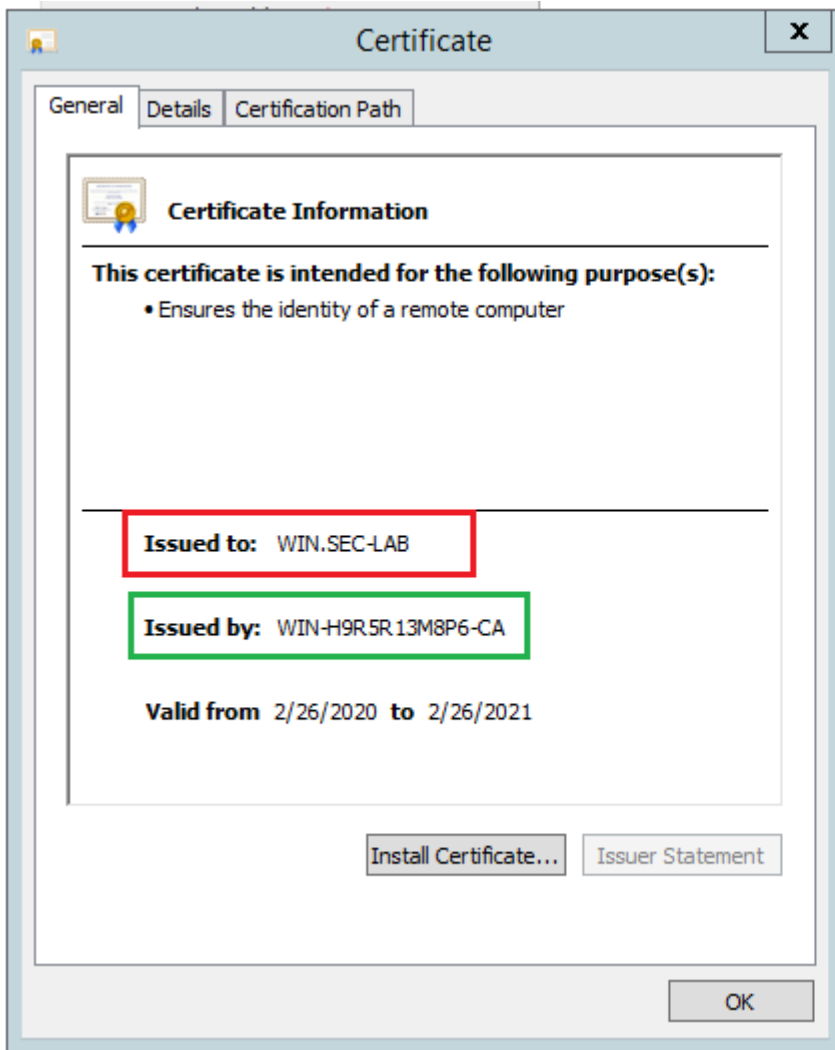
VCC: kies System > Configurationen kies vervolgens Beheerinterfaces zoals in de afbeelding:

The screenshot displays a network configuration interface. 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', and 'IP Address'. It shows one entry for 'eth0' with IP address '192.0.2.5'.
- Routes:** Two sub-sections: 'IPv4 Routes' and 'IPv6 Routes'. The IPv4 section has a table with columns 'Destination', 'Netmask', 'Interface', and 'Gateway', showing a route to '*' 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 DNS Server' field is 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 currently unchecked.

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

Zorg ervoor dat het certificaat dat is geüpload naar het VCC het certificaat is van de CA die het servercertificaat van de LDAP heeft ondertekend, zoals wordt geïllustreerd in de afbeelding:



Gebruik pakketopnamen om te bevestigen dat LDAP-server de juiste informatie verstuurt:

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

Gerelateerde informatie

- [Gebruikersaccounts voor beheertoegang](#)
- [Cisco Firepower Management Center lichtgewicht Directory Access Protocol-verificatie omzeilbaarheid](#)
- [Configuratie van LDAP-verificatieobject op FireSIGHT-systeem](#)
- [Technische ondersteuning en documentatie](#) – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.