

Configurar o Firepower Management Center e o FTD com LDAP para autenticação externa

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configuração LDAP básica na GUI do FMC](#)

[Acesso Shell para Usuários Externos](#)

[Autenticação externa para FTD](#)

[Funções de usuário](#)

[SSL ou TLS](#)

[Verificar](#)

[Base de Pesquisa de Teste](#)

[Testar integração LDAP](#)

[Troubleshooting](#)

[Como o FMC/FTD e o LDAP interagem para fazer download dos usuários?](#)

[Como o FMC/FTD e o LDAP interagem para autenticar uma solicitação de login de usuário?](#)

[SSL ou TLS não funciona como esperado](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como habilitar a autenticação externa do protocolo LDAP com o Cisco Firepower Management Center (FMC) e o Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FTD da Cisco
- FMC da Cisco
- LDAP da Microsoft

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

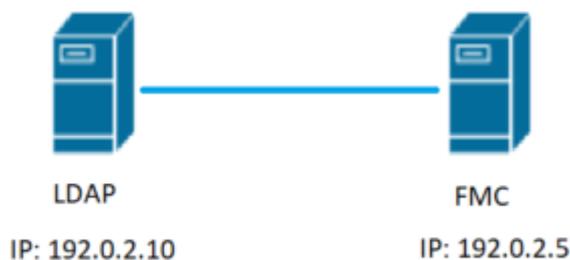
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O FMC e os dispositivos gerenciados incluem uma conta de administrador padrão para acesso de gerenciamento. Você pode adicionar contas de usuário personalizadas no FMC e em dispositivos gerenciados, como usuários internos ou, se suportado para seu modelo, como usuários externos em um servidor LDAP ou RADIUS. A autenticação de utilizador externo é suportada pelo FMC e pelo FTD.

- Usuário interno - O dispositivo FMC/FTD verifica a autenticação do usuário em um banco de dados local.
- Usuário externo - Se o usuário não estiver presente no banco de dados local, as informações do sistema de um servidor de autenticação LDAP ou RADIUS externo preenchem seu banco de dados de usuário.

Diagrama de Rede



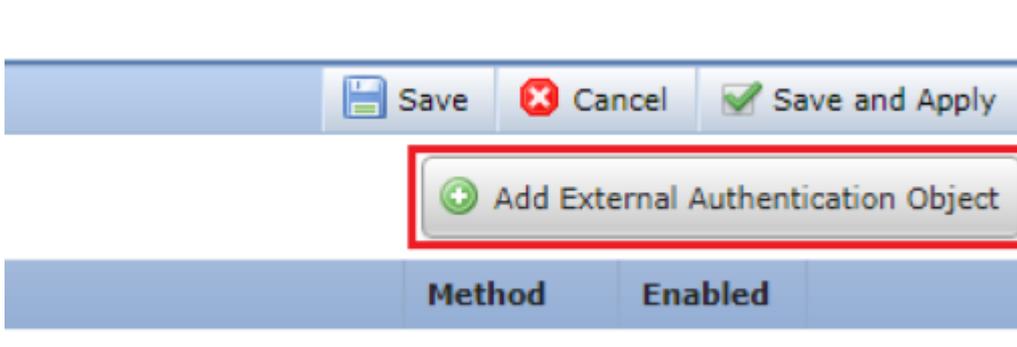
Configurar

Configuração LDAP básica na GUI do FMC

Etapa 1. Navegue até System > Users > External Authentication:



Etapa 2. Escolher Add External Authentication Object:



Etapa 3. Preencha os campos obrigatórios:

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)

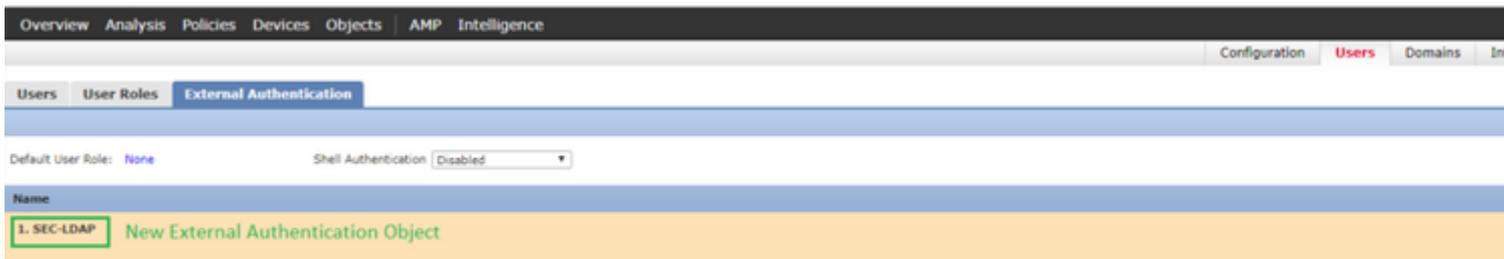
Additional Test Parameters

User Name

Password

*Required Field

Etapa 4. Habilite o External Authentication Objeto e Salvar:



Acesso Shell para Usuários Externos

O FMC oferece suporte a dois usuários administrativos internos diferentes: um para a interface da Web e outro com acesso por CLI. Isso significa que há uma distinção clara entre quem pode acessar a GUI e quem também pode acessar a CLI. No momento da instalação, a senha do usuário admin padrão é sincronizada para ser a mesma na GUI e na CLI. No entanto, eles são rastreados por mecanismos internos diferentes e podem ser diferentes.

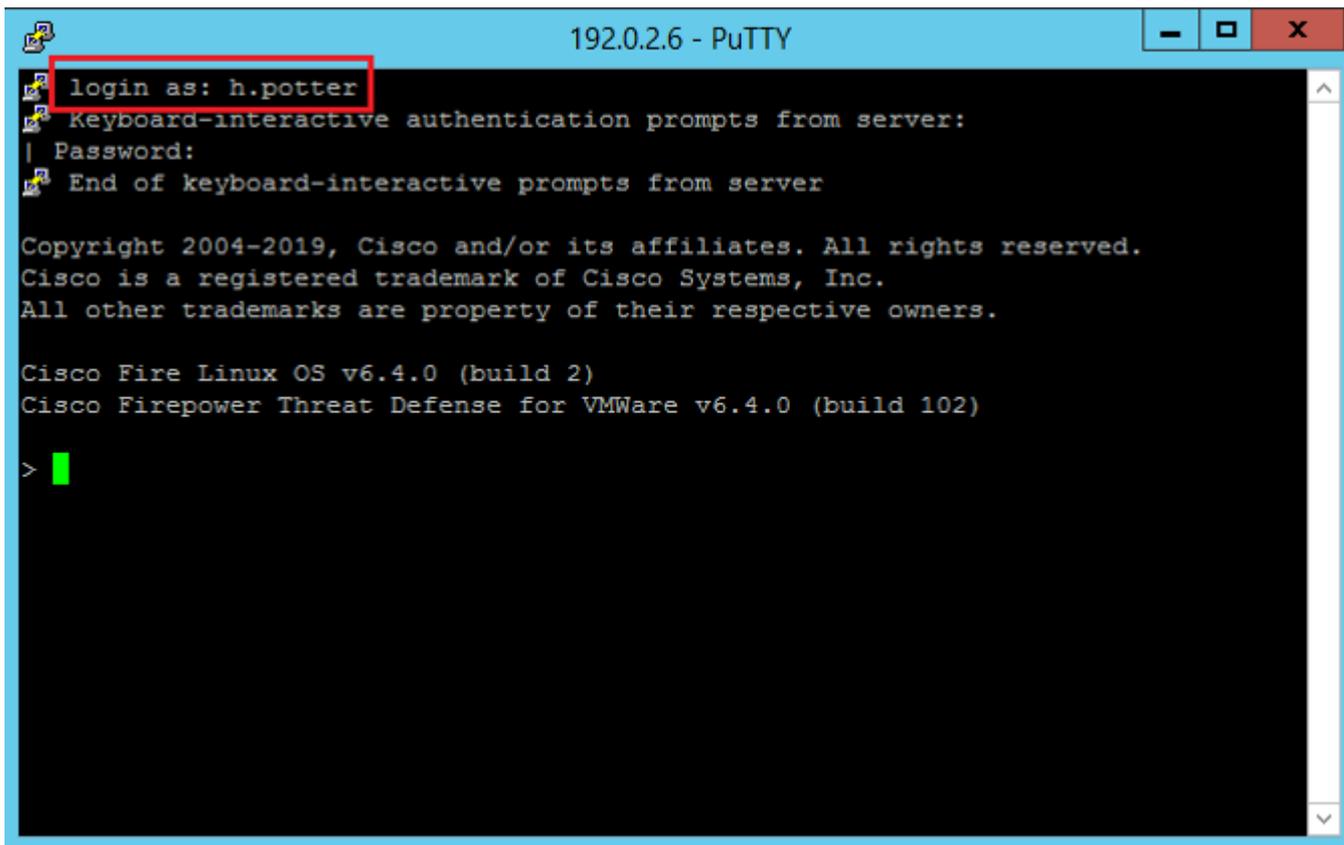
Usuários externos LDAP também devem receber acesso de shell.

Etapa 1. Navegue até System > Users > External Authentication e clique em Shell Authentication como visto na imagem e salve:



Etapa 2. Implantar alterações no FMC.

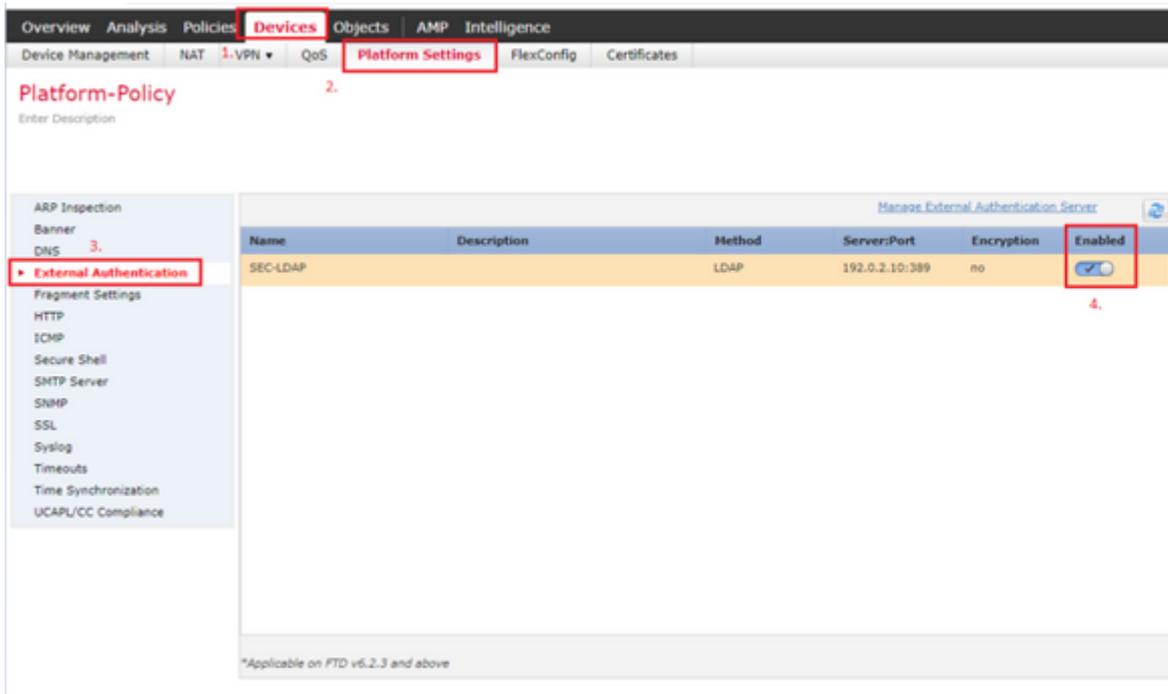
Uma vez que o acesso do shell para usuários externos esteja configurado, o login via SSH é ativado como visto na imagem:



Autenticação externa para FTD

A autenticação externa pode ser habilitada no FTD.

Etapa 1. Navegue até `Devices > Platform Settings > External Authentication`. Clique em `Enabled` e salvar:



Funções de usuário

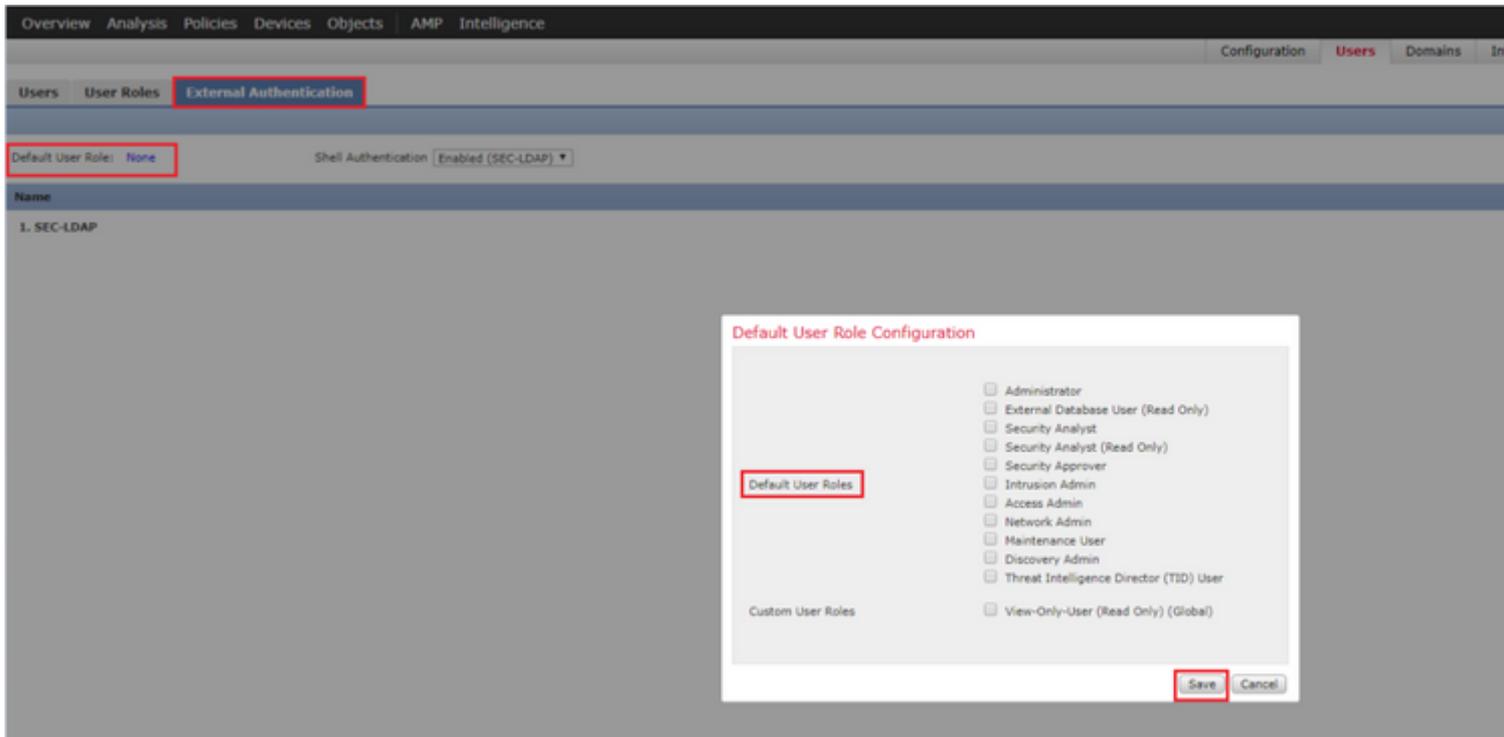
Os privilégios de usuário se baseiam na função de usuário atribuída. Você também pode criar funções de usuário personalizadas com privilégios de acesso personalizados de acordo com as necessidades da sua organização ou pode usar funções predefinidas, como analista de segurança e administrador de descoberta.

Há dois tipos de funções de usuário:

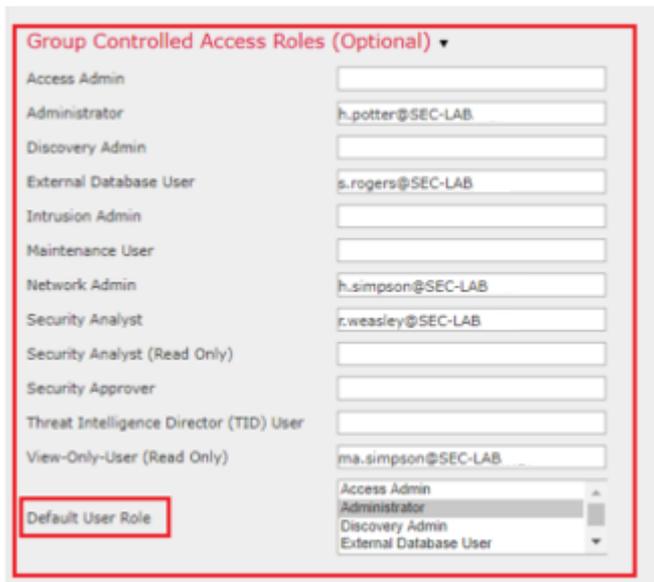
1. Funções de usuário da interface da Web
2. Funções de usuário CLI

Para obter uma lista completa de funções predefinidas e mais informações, consulte; [Funções de usuário](#).

Para configurar uma função de usuário padrão para todos os Objetos de Autenticação Externa, navegue até System > Users > External Authentication > Default User Role. Escolha a função de usuário padrão que deseja atribuir e clique em Save.



Para escolher uma função de usuário padrão ou atribuir funções específicas a usuários específicos em um grupo de objetos específico, você pode escolher o objeto e navegar até Group Controlled Access Roles como visto na imagem:



SSL ou TLS

O DNS deve ser configurado no FMC. Isso ocorre porque o valor do assunto do certificado deve corresponder ao Authentication Object Primary Server Hostname. Depois que o LDAP seguro for configurado, as capturas de pacotes não mostrarão mais solicitações de ligação de texto simples.

O SSL altera a porta padrão para 636 e o TLS a mantém como 389.

Observação: a criptografia TLS requer um certificado em todas as plataformas. Para SSL, o FTD também exige um certificado. Para outras plataformas, o SSL não exige um certificado. No entanto, é recomendável que você sempre carregue um certificado para SSL a fim de evitar ataques man-in-the-

middle.

Etapa 1. Navegue até Devices > Platform Settings > External Authentication > External Authentication Object e insira as informações de SSL/TLS de opções avançadas:

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)

Etapa 2. Carregue o certificado da autoridade de certificação que assinou o certificado do servidor. O certificado deve estar no 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)

Etapa 3. Salve a configuração.

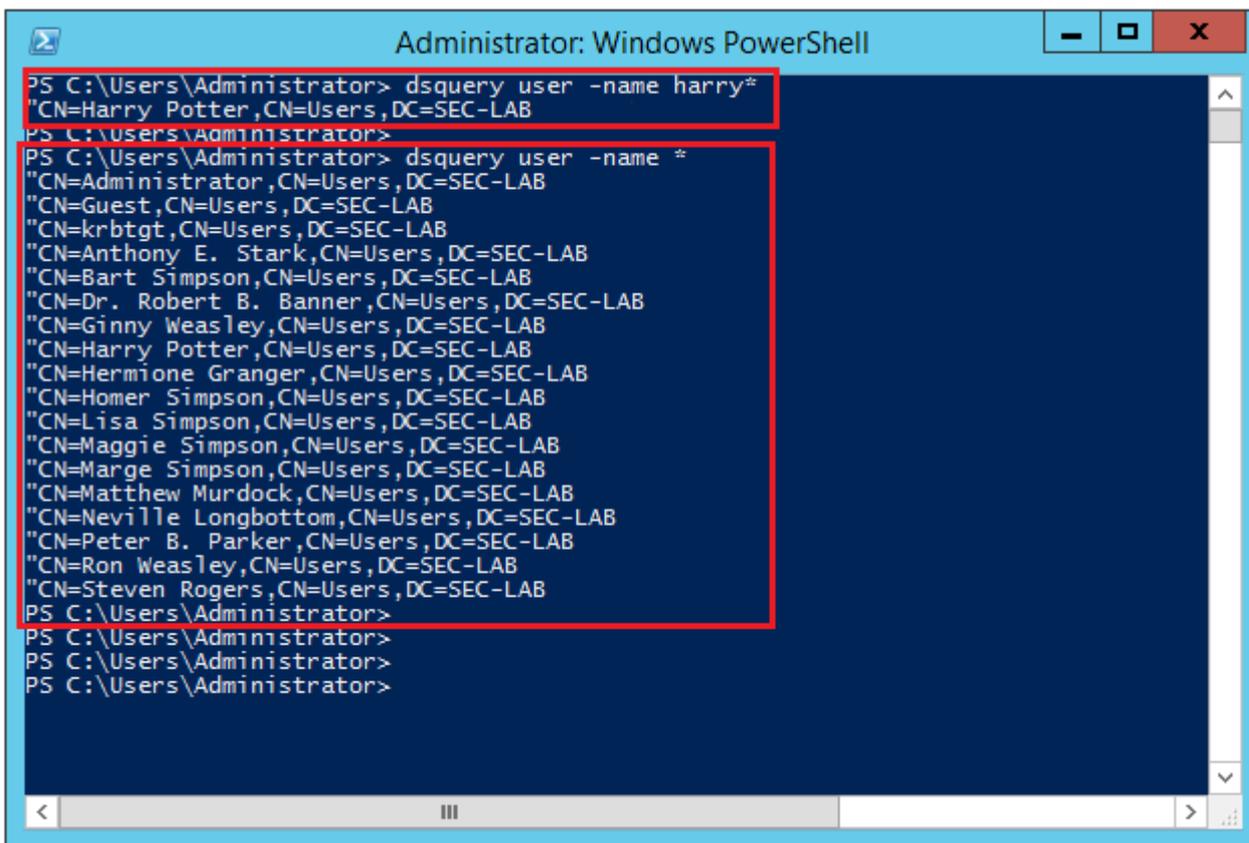
Verificar

Base de Pesquisa de Teste

Abra um prompt de comando do Windows ou o PowerShell onde o LDAP está configurado e digite o comando: `dsquery user -name`

Por exemplo:

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

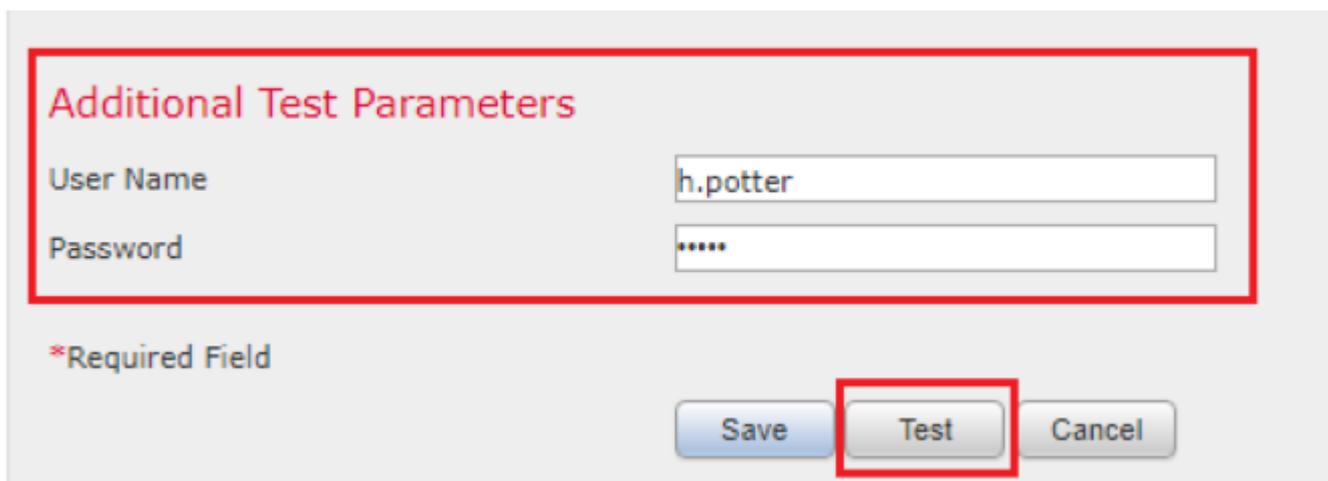


The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the following commands and their outputs:

```
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>
```

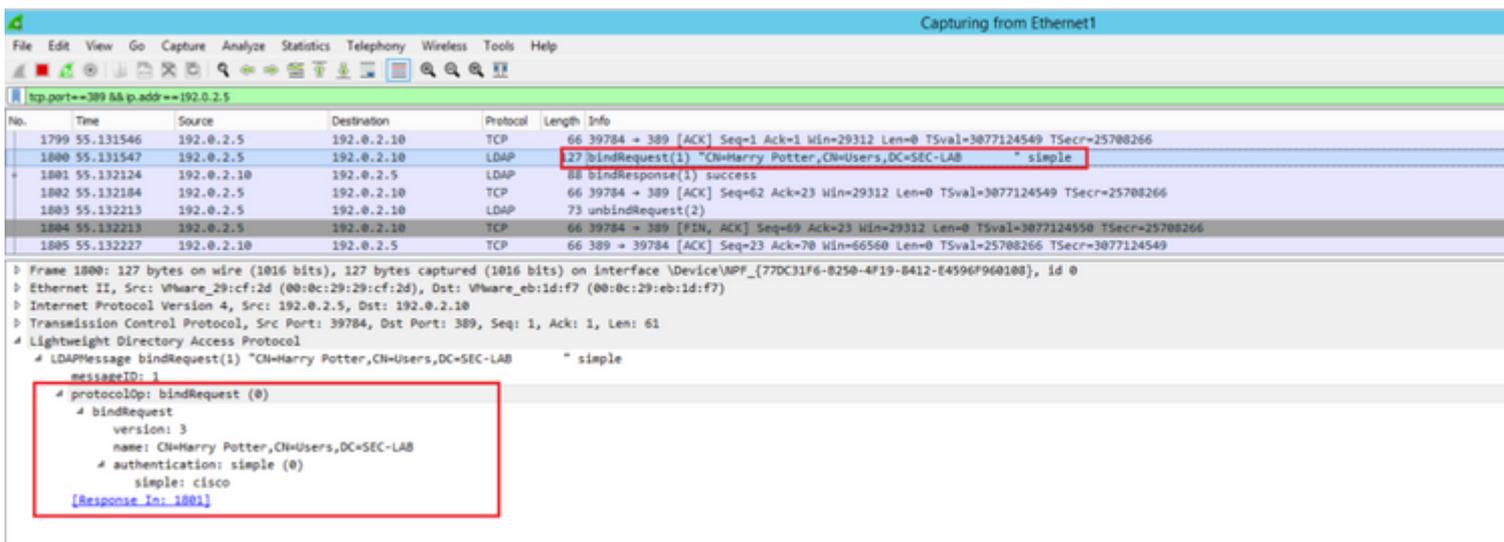
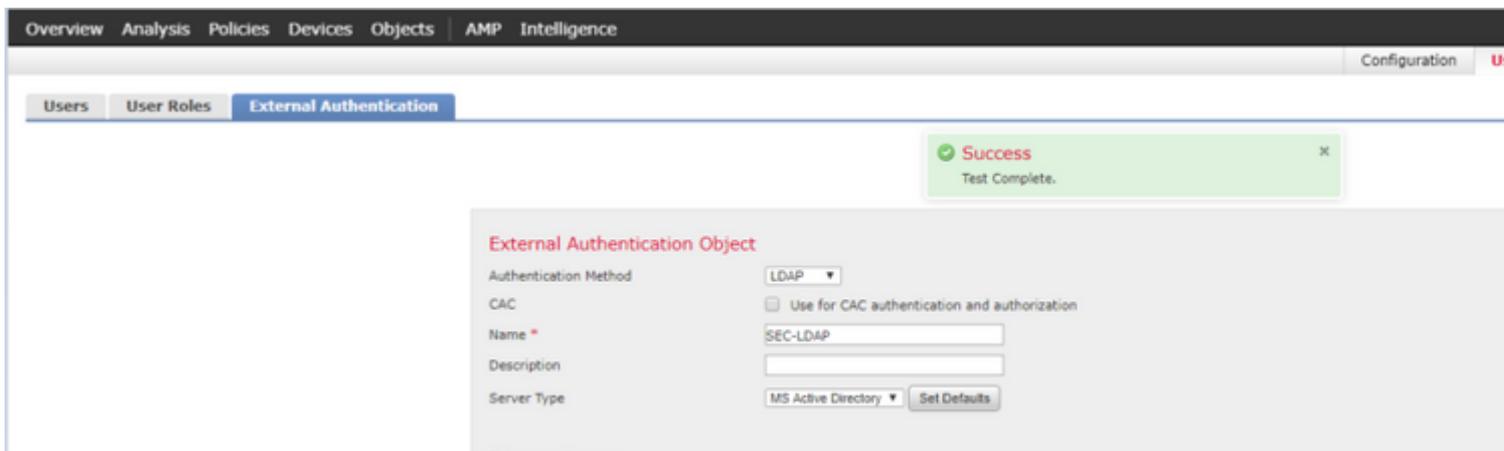
Testar integração LDAP

Navegue até System > Users > External Authentication > External Authentication Object. Na parte inferior da página, há um Additional Test Parameters como visto na imagem:



The screenshot shows the "Additional Test Parameters" section of the External Authentication Object configuration. It contains two input fields: "User Name" with the value "h.potter" and "Password" with masked characters "*****". Below the fields is a red asterisk and the text "*Required Field". At the bottom, there are three buttons: "Save", "Test", and "Cancel". The "Test" button is highlighted with a red box.

Escolha o Teste para ver os resultados.



Troubleshooting

Como o FMC/FTD e o LDAP interagem para fazer download dos usuários?

Para que o FMC possa receber usuários de um servidor LDAP da Microsoft, ele deve primeiro enviar uma solicitação de ligação na porta 389 ou 636 (SSL) com as credenciais de administrador LDAP. Quando o servidor LDAP puder autenticar o FMC, ele responderá com uma mensagem de êxito. Por último, o CVP pode apresentar um pedido com a mensagem de pedido de pesquisa descrita no diagrama:

```
<< --- 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
```

Observe que a autenticação envia senhas no modo clear por padrão:

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 TSecr=25348746
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 TSval=3073529344 TSecr=25348746
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

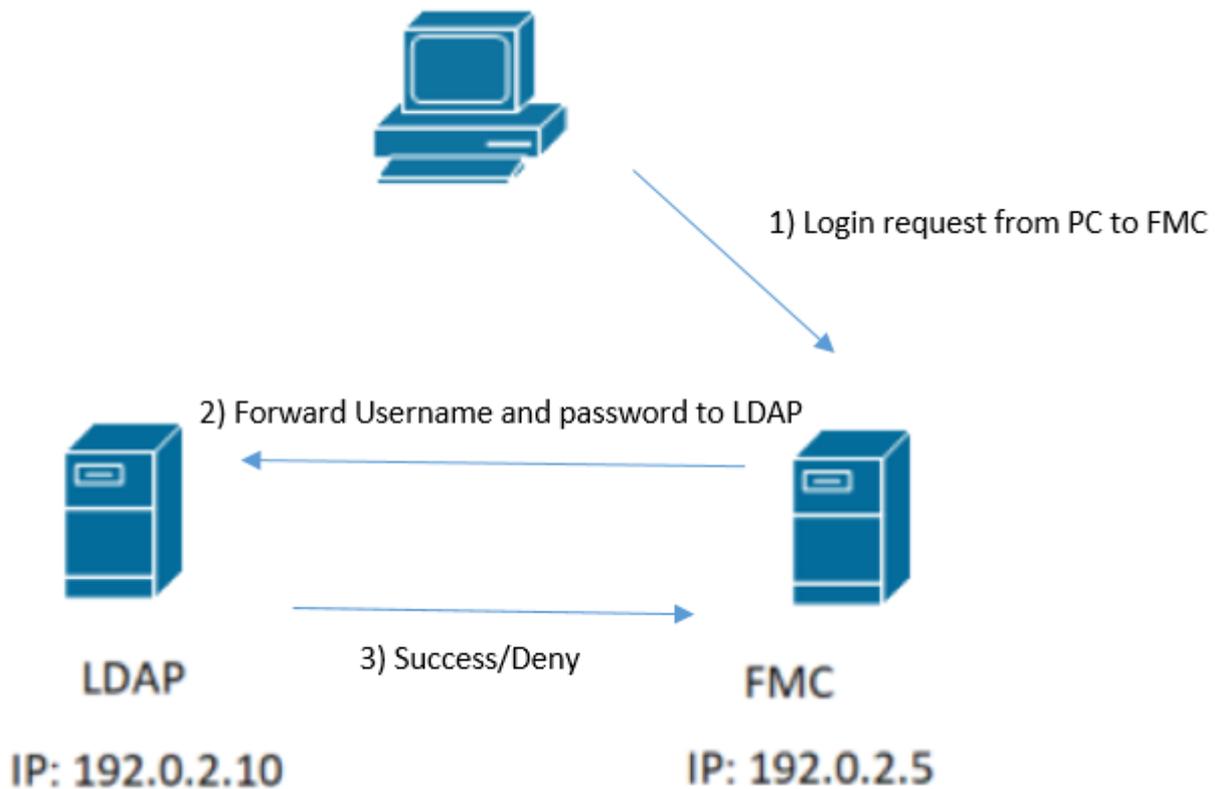
```

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]

```

Como o FMC/FTD e o LDAP interagem para autenticar uma solicitação de login de usuário?

Para que um usuário possa fazer login no FMC ou no FTD enquanto a autenticação LDAP estiver habilitada, a solicitação de login inicial é enviada ao Firepower, no entanto, o nome de usuário e a senha são encaminhados ao LDAP para uma resposta de êxito/negação. Isso significa que o FMC e o FTD não mantêm as informações de senha localmente no banco de dados e, em vez disso, aguardam a confirmação do LDAP sobre como proceder.





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 o nome de usuário e a senha forem aceitos, uma entrada será adicionada à GUI da Web conforme visto na imagem:

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

Execute o comando show user no FMC CLISH para verificar as informações do usuário: > show user

O comando exibe informações de configuração detalhadas para o(s) usuário(s) especificado(s). Estes valores

são exibidos:

Login – o nome de login

UID – a ID numérica do usuário

Autenticação (Local ou Remota) – como o usuário é autenticado

Acesso (Básico ou Config.) – o nível de privilégio do usuário

Ativado (Ativado ou Desativado) – se o usuário está ativo

Redefinir (Sim ou Não) – se o usuário deve alterar a senha no próximo login

Exp (Nunca ou um número) – o número de dias até que a senha do usuário deva ser alterada

Aviso (N/A ou um número) – o número de dias que um usuário recebe para alterar sua senha antes que ela expire

Str (Sim ou Não) – se a senha do usuário deve atender aos critérios para verificar a intensidade

Bloquear (Sim ou Não) – se a conta do usuário foi bloqueada devido a muitas falhas de login

Máx. (N/A ou um número) – o número máximo de logins com falha antes que a conta do usuário seja bloqueada

SSL ou TLS não funciona como esperado

Se você não habilitar o DNS nos FTDs, poderá ver erros no log pigtail que sugerem que o LDAP está inacessível:

```
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
```

Verifique se o Firepower consegue resolver o FQDN de servidores LDAP. Caso contrário, adicione o DNS correto conforme visto na imagem.

FTD: Acesse o CLISH do FTD e execute o comando: > configure network dns servers

The image shows a PuTTY terminal window titled "192.0.2.6 - PuTTY". The terminal output is as follows:

```
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:~$
```

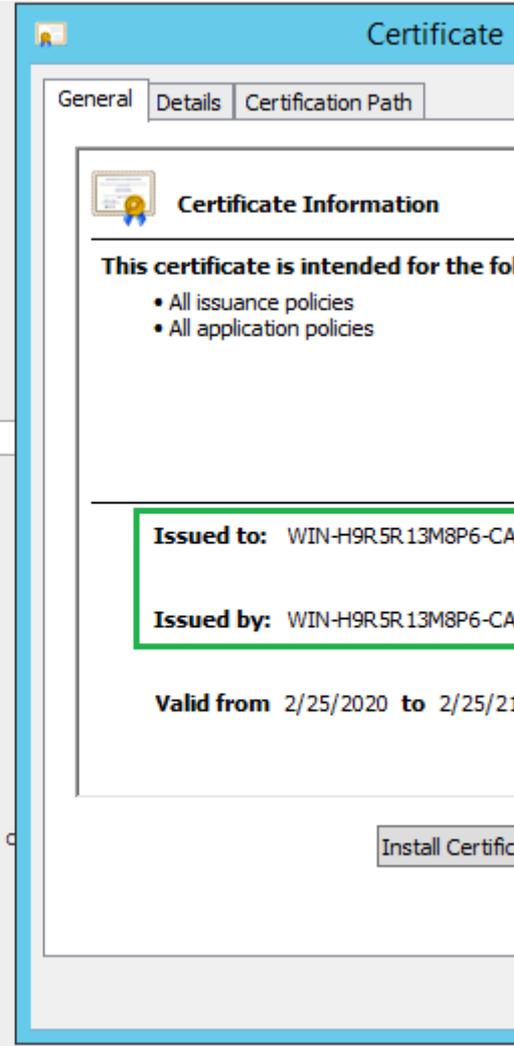
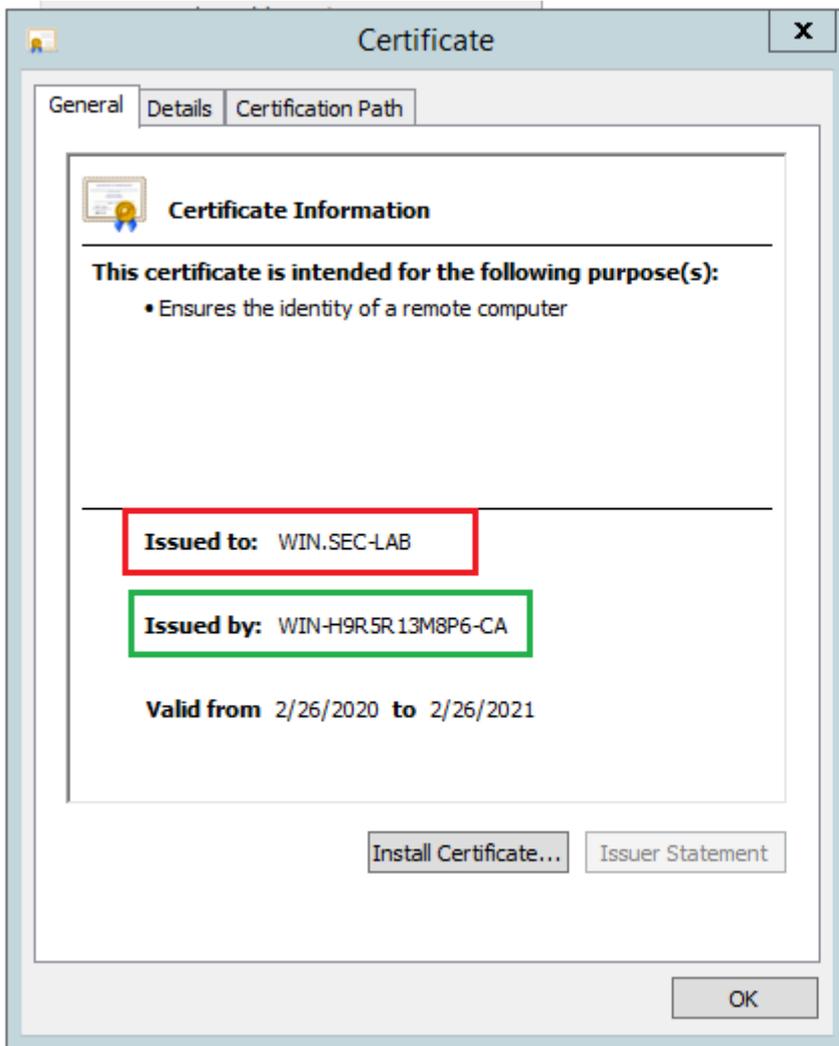
FMC: Escolha System > Configuration, e escolha Interfaces de gerenciamento, conforme ilustrado na imagem:

The image shows a configuration interface for a Security Management Center (FMC). On the left is a navigation menu with various settings categories. The main area is divided into several sections:

- Management 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 tables. The first is for IPv4 Routes with columns: Destination, Netmask, Interface, Gateway. One entry is visible: * with Gateway 192.0.2.1. The second is for IPv6 Routes with columns: Destination, Prefix Length, Interface, Gateway.
- 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:** Checkboxes for '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 area are 'Save' and 'Cancel' buttons.

Verifique se o certificado carregado no FMC é o certificado da CA que assinou o certificado do servidor do LDAP, como ilustrado na imagem:



Use capturas de pacotes para confirmar se o servidor LDAP envia as informações corretas:

The screenshot displays a network traffic capture in Wireshark. The packet list table at the top shows the following data:

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, Server Hello Done
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

The packet details pane for frame 33 shows the following structure:

- 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

On the right side of the image, the Cisco Firepower Management Center configuration pane is visible, showing the 'Primary Server' field with a red box around it.

Informações Relacionadas

- [Contas de Usuário para Acesso de Gerenciamento](#)
- [Vulnerabilidade de desvio de autenticação do protocolo Lightweight Directory Access Protocol do Cisco Firepower Management Center](#)
- [Configuração do objeto de autenticação LDAP no sistema FireSIGHT](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.