

Configurar LDAPS em FXOS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuração](#)

[Configurar LDAP simples](#)

[Configurar LDAPS](#)

[Troubleshooting](#)

[Resolução DNS](#)

[Handshake TCP e SSL](#)

[Depuração](#)

[Recupere-se após ser bloqueado](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar LDAP seguro (LDAPS) em FXOS usando o Gerenciador de chassi de firewall seguro (FCM) e CLI.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Sistema operacional extensível (FXOS) com firewall seguro
- Gerenciador de chassi de firewall seguro (FCM)
- Conceitos do Lightweight Directory Access Protocol (LDAP)

Componentes Utilizados

As informações neste documento são baseadas em:

- Dispositivo Secure Firewall 9300 versão 2.12(0.8)

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.

Configuração

É recomendável testar se o LDAP simples funciona no dispositivo de firewall seguro.

Configurar LDAP simples

1. Faça login no FCM.
2. Navegue até Platform Settings > AAA > LDAP
3. Clique em Provedores LDAP > Adicionar
4. Configure o provedor LDAP e insira as informações de DN de Ligação, DN Base, Atributo e Chave para o Microsoft Active Directory (MS AD).
5. Use o FQDN do servidor LDAP, pois ele é necessário para a conexão SSL.

Edit WIN-JOR .local



Hostname/FQDN/IP Address:*	<input type="text" value="WIN-JOR.local"/>	
Order:*	<input type="text" value="1"/>	
Bind DN:	<input type="text" value="CN=sfua,CN=Users,DC=jor"/>	
Base DN:	<input type="text" value="DC=jor.DC=local"/>	
Port:*	<input type="text" value="389"/>	
Enable SSL:	<input type="checkbox"/>	
Filter:	<input type="text" value="cn=\$userid"/>	
Attribute:	<input type="text" value="CiscoAVpair"/>	
Key:	<input type="text"/>	Set: Ye
Confirm Key:	<input type="text"/>	
Timeout:*	<input type="text" value="30"/>	Secs
Vendor:	<input type="radio"/> Open LDAP <input checked="" type="radio"/> MS AD	

Configuração LDAP

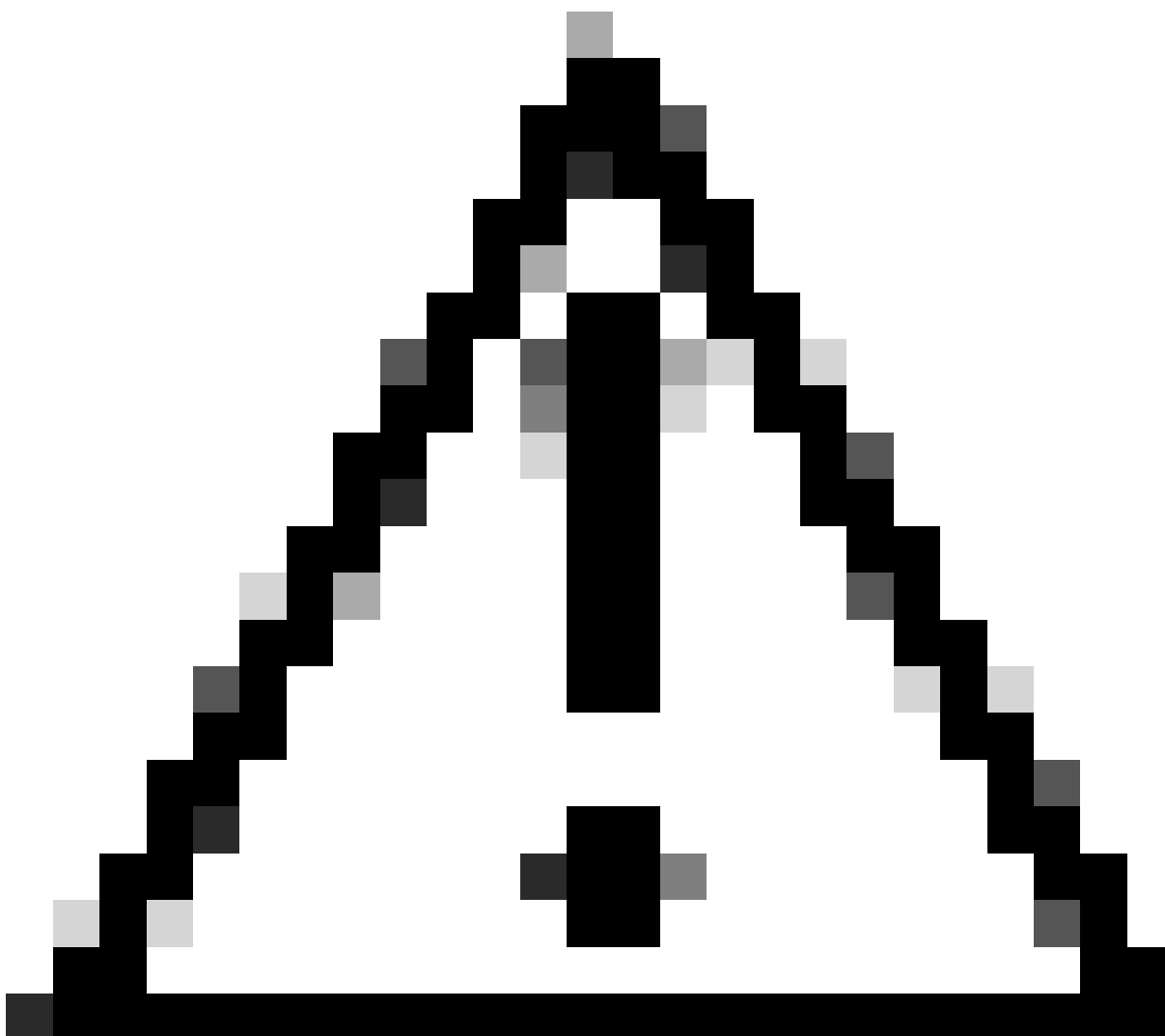
6. Navegue até System > User Management > Settings.

7. Defina a autenticação Padrão ou de Console como LDAP.

Local Users	Settings
Default Authentication	<input type="text" value="LDAP"/> <input type="button" value="v"/> *Local is fallback authentication method
Console Authentication	<input type="text" value="Local"/> <input type="button" value="v"/>

Seleção de método de autenticação

8. Tente fazer login via SSH no chassi para testar a autenticação com um usuário LDAP.



Cuidado: tenha cuidado ao testar a autenticação LDAP. Se houver um erro na configuração, essa alteração poderá bloqueá-lo. Teste com uma sessão duplicada ou a partir do acesso do console com autenticação local para que a reversão ou solução de problemas possa ser executada.

Configurar LDAPS

9. Depois de testar uma conexão LDAP bem-sucedida, navegue novamente para Platform Settings > AAA > LDAP.

10. Edite seu provedor LDAP e habilite SSL.

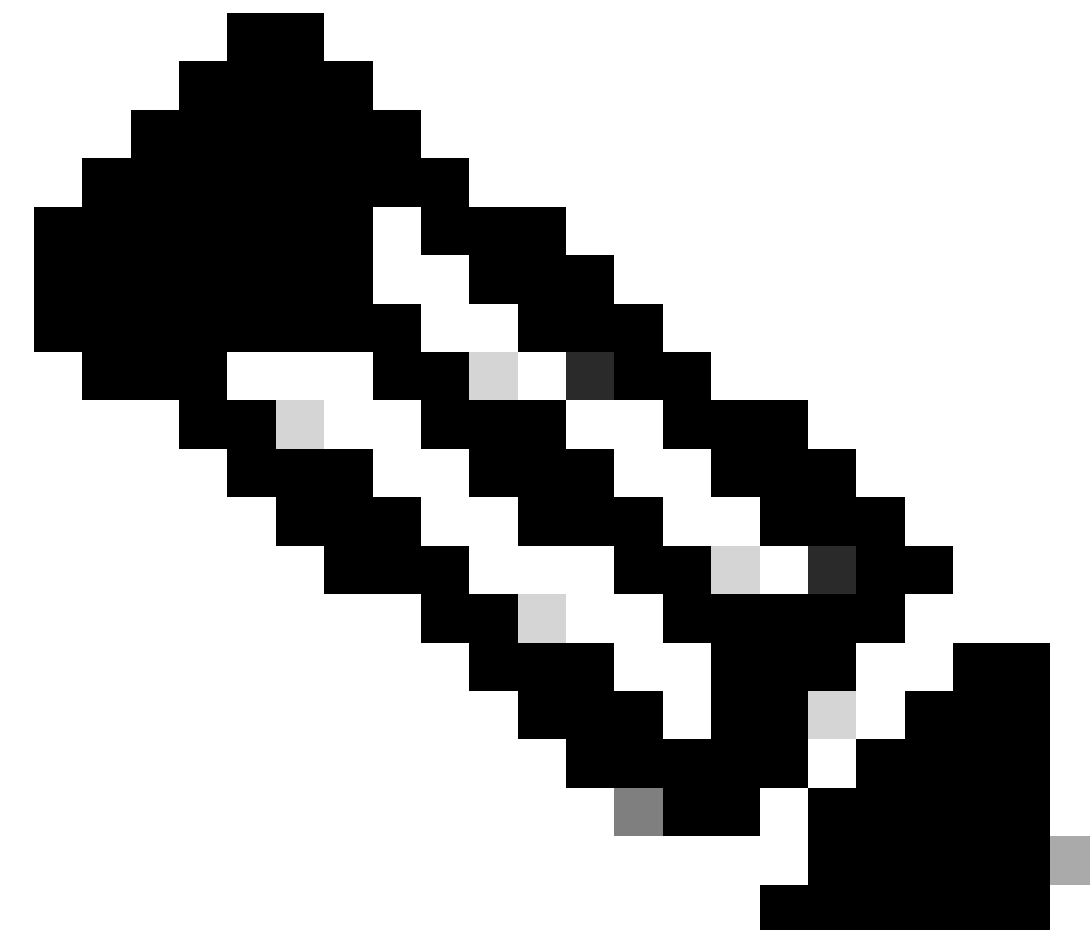
Port:*

389

Enable SSL:



GUI de seleção de porta



Observação: a porta 389 precisa ser usada para criptografia. A porta 636 não funciona. O aprimoramento da ID de bug da Cisco [CSCwc9347](#) foi arquivado para adicionar portas personalizadas para LDAPS

11. O certificado CA raiz do servidor LDAP deve ser importado para o chassi. Se houver certificados intermediários, importe a cadeia.

Crie um ponto confiável a partir da CLI do FXOS para executar isso.

<#root>

FPR9300-01#

scope security

FPR9300-01 /security #

create trustpoint LDAPS

>^CFPR9300-01 /security/trustpoint* #

set certchain

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:

>-----BEGIN CERTIFICATE-----

>

MIIDmTCCAoGgAwIBAgIQYPxqSjXdYLJCpz+rOqfXpjANBqkqhkiG9w0BAQsFAADBT

>MRUwEwYKcZImiZPyLQBGryFbG9jYwWxFzAVBgoJkiaJk/IsZAEZFgdqb3JnZWp1

>MSEwHwYDVQQDEExqb3JnZWp1LVdJTl1KTlJHRUpVLUNBLTEwHhcNMjEzMDc0

>MDAwWhcNMjEzMDc0OTU5WjBTMRUwEwYKcZImiZPyLQBGryFbG9jYwWxFzAV

>BgoJkiaJk/IsZAEZFgdqb3JnZWp1MSEwHwYDVQQDEExqb3JnZWp1LVdJTl1KTlJH

>RUPLUNBLTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDmBTWU6Leu

>bPxvc+EhC7fxjowEjjL0EXlMo3x7Pe3EW6Gng2iOMB1UpBNgSObbct83P6y6EmQi

>0RCCnEFfzy4stYPz/7499wALwMLSGNQWr10rjVB64ihfugbx95iDBcwuv6XK67h/

>T1caN4GZiLtYZjURGs5mLNB2f8hLp9QR2WoZqfAvrfvFB4I5RJjx0FYKIXW1dmPT

>AAPa/Qi+1Qv1exfzvXHXx1GMDCHle2yItFgl6o7OujT0AE3oplA/qQD+mTAJmdcR

>QLUDiUptqqYKgcbrH4Hu4PMje3INLd1vw1ThAwMFn+oXjRTM0KbEQ0/JEM6xRFMv

>LqzmDwxA8IoRagMBAAGjaTBnMBMGCSsGAQQBgyjUAgQGHgQAQwBBMA4GA1UdDwEB

>/wQEAWIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBQoweZEEke7BIOd94R5

>YxjvJHdzsjaQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAYGli

>n77K0OiqSljTeg+C1VLRX8VJwr7Pp5p4Mu0mRhZckmIKSUtYDla3ToVix5k4dXSU

>7MaVWDkW/1NvReaqCfis5mgfrpzoPUkqKGiz7Zhd57gA4tBU/XbP/CXpTuAR3Isa

>NKz7yy+6tisf+8vfLtrN8c3IclS6ncyrdAdJ2iJY74jJm1eUPs3muaqApPPwoRF2

>GdALD/Y+Pq36cSjK+jGP1+2rD6cWl6thBp9plOOTL+qpq4DL+W6uctWeRMgGxcWn

>GsKhHysno9dZ+DnnOlx0tP+S1B9fmxF7ycCmmn328dZVEG7JXjHc8KoqwwWe+fwu

>GXLRM+rKaAICH52EEw==

>-----END CERTIFICATE-----

>ENDOFBUF

FPR9300-01 /security/trustpoint* #

commit-buffer

12. Insira a configuração do servidor LDAP conforme configurado no provedor LDAP. Anote o nome do seu servidor LDAP.

13. Defina a política de revogação como relaxada.

<#root>

FPR9300-01 /security #

scope ldap

FPR9300-01 /security/ldap #

show server

LDAP server:

Hostname, FQDN or IP address DN to search and read Port SSL Key CRL Password

```
-----  
WIN-JOR.jor.local CN=sfua,CN=Users,DC=jor,DC=local  
389 Yes Strict ****
```

```
FPR9300-01 /security/ldap #
```

```
scope server WIN-JOR.jor.local
```

```
FPR9300-01 /security/ldap/server #
```

```
set revoke-policy relaxed
```

```
FPR9300-01 /security/ldap/server* #
```

```
commit-buffer
```

```
FPR9300-01 /security/ldap/server #
```

```
show
```

```
LDAP server:
```

```
Hostname, FQDN or IP address DN to search and read Port SSL Key CRL Password
```

```
-----  
WIN-JOR.jor.local CN=sfua,CN=Users,DC=jor,DC=local  
389 Yes Relaxed ****
```

14. Salve as alterações usando commit-buffer.

Troubleshooting

Resolução DNS

Verifique se o FQDN está sendo resolvido para o IP correto. Pode haver problemas com a resolução de nomes:

```
<#root>
```

```
FPR9300-01#
```

```
connect fxos
```

```
FPR9300-01(fxos)#
```

```
ethalyzer local interface mgmt capture-filter "udp port 53" limit-captured-frames 100
```

```
Capturing on 'eth0'
```

```
1 2024-02-01 11:36:43.822089169 10.4.23.202 → 10.88.243.91 DNS 85 Standard query 0x1b86 AAAA WIN-JOR.jor.local
```



```
2 2024-02-01 11:36:43.857989995 10.88.243.91 → 10.4.23.202 DNS 160 Standard query response 0x1b86 No such nam
```

Uma resolução de nome DNS bem-sucedida se parece com esta:

```
<#root>
```

```
FPR9300-01(fxos)#
```

```
ethanalyzer local interface mgmt capture-filter "udp port 53" limit-captured-frames 100
```

```
Capturing on 'eth0'
```

```
1 2022-09-06 00:49:00.059899379 10.88.146.73 → 10.88.243.91 DNS 85 Standard query 0xc512 AAAA WIN-JOR.jor.local
2 2022-09-06 00:49:00.061349442 10.88.243.91 → 10.88.146.73 DNS 113 Standard query response 0xc512 AAAA WIN-J
3 2022-09-06 00:49:00.061515561 10.88.146.73 → 10.88.243.91 DNS 85 Standard query 0xc513 A WIN-JOR.jor.local
4 2022-09-06 00:49:00.061727264 10.88.243.91 → 10.88.146.73 DNS 101 Standard query response 0xc513 A WIN-JOR.
```

Handshake TCP e SSL

Para verificar a conexão LDAPS, configure as capturas na porta 389.

Se você vir alertas como CA desconhecida, isso significa que o certificado CA raiz do servidor LDAP não corresponde. Verifique se o certificado é realmente a CA raiz do servidor.

```
<#root>
```

```
7 2024-02-01 12:10:37.260940300 10.4.23.202 → 10.4.23.128 TLSv1 345 Client Hello
8 2024-02-01 12:10:37.264016628 10.4.23.128 → 10.4.23.202 TCP 1514 [TCP segment of a reassembled PDU]
9 2024-02-01 12:10:37.264115319 10.4.23.128 → 10.4.23.202 TLSv1.2 617 Server Hello, Certificate, Server Key E
10 2024-02-01 12:10:37.264131122 10.4.23.202 → 10.4.23.128 TCP 66 40638 → 389 [ACK] Seq=311 Ack=2046 Win=3532
11 2024-02-01 12:10:37.264430791 10.4.23.202 → 10.4.23.128 TLSv1.2 73 Alert (Level: Fatal,
```

```
Description: Unknown CA
```

```
)
```

```
12 2024-02-01 12:10:37.264548228 10.4.23.202 → 10.4.23.128 TLSv1.2 73 Ignored Unknown Record
```

Uma conexão bem-sucedida se parece com isto:

```
<#root>
```

```
FPR9300-01(fxos)#
```

```
ethanalyzer local interface mgmt capture-filter "tcp port 389" limit-captured-frames 100
```

```
Capturing on 'eth0'
```

```
1 2024-02-01 12:12:49.131155860 10.4.23.202 → 10.4.23.128 TCP 74 42396 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=
2 2024-02-01 12:12:49.131403319 10.4.23.128 → 10.4.23.202 TCP 74 389 → 42396 [SYN, ACK] Seq=0 Ack=1 Win=8192
```

```
3 2024-02-01 12:12:49.131431506 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [ACK] Seq=1 Ack=1 Win=29696 Len=
4 2024-02-01 12:12:49.131455795 10.4.23.202 → 10.4.23.128 LDAP 97 extendedReq(1) LDAP_START_TLS_OID
5 2024-02-01 12:12:49.131914129 10.4.23.128 → 10.4.23.202 LDAP 112 extendedResp(1) LDAP_START_TLS_OID
6 2024-02-01 12:12:49.131931868 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [ACK] Seq=32 Ack=47 Win=29696 Le
7 2024-02-01 12:12:49.133238650 10.4.23.202 → 10.4.23.128 TLSv1 345 Client Hello
8 2024-02-01 12:12:49.135557845 10.4.23.128 → 10.4.23.202 TLSv1.2 2065 Server Hello, Certificate, Server Key
9 2024-02-01 12:12:49.135595847 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [ACK] Seq=311 Ack=2046 Win=33280
10 2024-02-01 12:12:49.150071315 10.4.23.202 → 10.4.23.128 TLSv1.2 171 Certificate, Client Key Exchange, Chan
11 2024-02-01 12:12:49.150995765 10.4.23.128 → 10.4.23.202 TLSv1.2 117 Change Cipher Spec, Encrypted Handshak
12 2024-02-01 12:12:49.151218671 10.4.23.202 → 10.4.23.128 TLSv1.2 153 Application Data
13 2024-02-01 12:12:49.152638865 10.4.23.128 → 10.4.23.202 TLSv1.2 117 Application Data
14 2024-02-01 12:12:49.152782132 10.4.23.202 → 10.4.23.128 TLSv1.2 165 Application Data
15 2024-02-01 12:12:49.153310263 10.4.23.128 → 10.4.23.202 TLSv1.2 430 Application Data
16 2024-02-01 12:12:49.153463478 10.4.23.202 → 10.4.23.128 TLSv1.2 153 Application Data
17 2024-02-01 12:12:49.154673694 10.4.23.128 → 10.4.23.202 TLSv1.2 117 Application Data
18 2024-02-01 12:12:49.155219271 10.4.23.202 → 10.4.23.128 TLSv1.2 102 Application Data
19 2024-02-01 12:12:49.155254255 10.4.23.202 → 10.4.23.128 TLSv1.2 97 Encrypted Alert
20 2024-02-01 12:12:49.155273807 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [FIN, ACK] Seq=756 Ack=2563 Win
21 2024-02-01 12:12:49.155483352 10.4.23.128 → 10.4.23.202 TCP 60 389 → 42396 [RST, ACK] Seq=2563 Ack=725 Win
```

Depuração

Você pode habilitar depurações para LDAP para obter mais informações em caso de solução de problemas mais profunda.

Uma conexão SSL bem-sucedida se parece com esta, nenhum erro grave é observado:

```
<#root>
```

```
FPR9300-01(fxos)#
```

```
debug ldap all
```

```
2024 Feb 1 11:51:16.243245 ldap: 0x00000101/111 -> 0x00000101/0 id0x2F06F sz370 [REQ] op4093 rr0x2F06F
2024 Feb 1 11:51:16.243275 ldap: mts_ldap_aaa_request_handler: session id 0, list handle is NULL
2024 Feb 1 11:51:16.243289 ldap: mts_ldap_aaa_request_handler: user :sfua:, user_len 4, user_data_len 8
2024 Feb 1 11:51:16.243298 ldap: ldap_authenticate: user sfua with server group ldap
2024 Feb 1 11:51:16.243337 ldap: ldap_authenticate:3150 the value of login_type is 0
2024 Feb 1 11:51:16.243394 ldap: ldap_global_config: entering ...
2024 Feb 1 11:51:16.243637 ldap: ldap_read_group_config:
2024 Feb 1 11:51:16.243831 ldap: ldap_server_config: GET_REQ: server index: 1 addr:
2024 Feb 1 11:51:16.244059 ldap: ldap_client_auth_init: attr_memberof not configured for server
2024 Feb 1 11:51:16.244268 ldap: ldap_client_auth_init: (user sfua) - ldap_init success for host WIN-JO
2024 Feb 1 11:51:16.244487 ldap: ldap_client_lib_init_ssl: set ldap options cipher_suite ALL:!DHE-PSK-A
SHA:!EDH-DSS-DES-CBC3-SHA:!DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDI
RSA-AES256-SHA:!ECDHE-ECDSA-AES256-SHA:!
2024 Feb 1 11:51:16.246568 ldap: ldap_do_TLS: - ldap_tls initiated
2024 Feb 1 11:51:16.246598 ldap: ldap_client_auth_init:(user sfua) - awaiting for response, issl: 1
2024 Feb 1 11:51:16.247104 ldap: ldap_socket_ready_callback: entering...
2024 Feb 1 11:51:16.247116 ldap: ldap_process_result: entering... for user sfua
2024 Feb 1 11:51:16.247124 ldap: ldap_process_result: ldap_result sess->state: LDAP_SESS_TLS_SENT
2024 Feb 1 11:51:16.247146 ldap: ldap_process_result: (user sfua) - tls extended resp.
2024 Feb 1 11:51:16.247153 ldap: ldap_do_process_tls_resp: entering for user sfua
2024 Feb 1 11:51:16.247169 ldap: ldap_do_process_tls_resp: (user sfua) - ldap start TLS sent successful
2024 Feb 1 11:51:16.249856 ldap: ldap_app_cb: - ldap_app_ctx 0x100ad224 ldap session 0x1217a53c ssl 0x1
```

```
2024 Feb 1 12:19:20.512383 ldap: ldap_app_cb: - Check the configured hostname WIN-JORGEJU.jorgeju.local
2024 Feb 1 12:19:20.512418 ldap: ldap_app_cb: Non CC mode - hostname WIN-JORGEJU.jorgeju.local.
2024 Feb 1 12:19:20.520346 ldap: ldap_cr1s_http_and_local_cb: - get CRL from CRLDP
2024 Feb 1 12:19:20.520626 ldap: ldap_cr1s_http_and_local_cb: - cr1s 0x121787dc
2024 Feb 1 12:19:20.520900 ldap: ldap_load_cr1_cr1dp: - get CRL from CRLDP
2024 Feb 1 12:19:20.521135 ldap: ldap_load_cr1_cr1dp: - cr1s 0x121787dc
2024 Feb 1 12:19:20.521364 ldap: ldap_get_dp_url: - get URI from CRLDP
2024 Feb 1 12:19:20.521592 ldap: ldap_load_cr1_http: - entering...
```

Quando o certificado raiz da CA do servidor não corresponder, você poderá observar erros de certificado no processo `ldap_check_cert_chain_cb`:

```
2024 Feb 1 12:07:08.624416 ldap: ldap_app_cb: - Check the configured hostname WIN-JOR.jor.local withpe
2024 Feb 1 12:07:08.624453 ldap: ldap_app_cb: Non CC mode - hostname WIN-JOR.jor.local.
2024 Feb 1 12:08:31.274583 ldap: ldap_check_cert_chain_cb: - Enter
2024 Feb 1 12:08:31.274607 ldap: ldap_check_cert_chain_cb: - called ok flag is 0
2024 Feb 1 12:08:31.274620 ldap: ldap_check_cert_chain_cb: - ldap session 0x1217a53c, cr1strict 0.
2024 Feb 1 12:08:31.274632 ldap: ldap_check_cert_chain_cb: - get ctx error is 20
2024 Feb 1 12:08:31.274664 ldap: ldap_check_cert_chain_cb: - cert X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_
2024 Feb 1 12:08:31.274688 ldap: ldap_check_cert_chain_cb: - End ok 0
2024 Feb 1 12:08:31.274833 ldap: ldap_do_process_tls_resp: (user sfua) - TLS START failed
```

Recupere-se após ser bloqueado

Se, por algum motivo, você tiver sido bloqueado na GUI do Gerenciador de chassis e o LDAPS não estiver funcionando, ainda será possível recuperá-lo se você tiver acesso à CLI.

Isso é feito alterando-se o método de autenticação de volta para local, seja para Autenticação padrão ou Autenticação de console.

```
<#root>
```

```
FPR9300-01#
```

```
scope security
```

```
FPR9300-01 /security #
```

```
scope default-auth
```

```
FPR9300-01 /security/default-auth #
```

```
show
```

```
Default authentication:
```

```
Admin Realm Admin Authentication server group Use of 2nd factor
```

```
-----
```

Ldap No

```
FPR9300-01 /security/default-auth #
```

```
set realm local
```

```
FPR9300-01 /security/default-auth* #
```

```
commit-buffer
```

```
FPR9300-01 /security/default-auth #
```

```
show
```

Default authentication:

Admin Realm	Admin Authentication server group	Use of 2nd factor
-------------	-----------------------------------	-------------------

Local		No
-------	--	----

Após essas alterações, tente fazer login no FCM novamente.

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

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.