

# FXOSでのLDAPSの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[プレーンLDAPの設定](#)

[LDAPSの設定](#)

[トラブルシューティング](#)

[DNS解決](#)

[TCPおよびSSLハンドシェイク](#)

[デバッグ](#)

[ロックアウトされた状態からの回復](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Secure Firewall Chassis Manager(FCM)およびCLIを使用して、FXOSでSecure LDAP(LDAPS)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Secure Firewall eXtensible Operating System(FXOS)
- Secure Firewall Chassis Manager(FCM)
- 軽量ディレクトリアクセスプロトコル(LDAP)の概念

### 使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Secure Firewall 9300デバイスバージョン2.12(0.8)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

# コンフィギュレーション

セキュアファイアウォールデバイスでプレーンLDAPが動作することをテストすることをお勧めします。

## プレーンLDAPの設定

1. FCMにログインします。
2. Platform Settings > AAA > LDAPの順に移動します。
3. LDAP Providers > Addの順にクリックします。
4. LDAPプロバイダーを設定し、バインドDN、ベースDN、Microsoft Active Directory(MS AD)の属性およびキー情報を入力します。
5. SSL接続に必要なLDAPサーバのFQDNを使用します。

## 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: Yes
Confirm Key:	<input type="text"/>	
Timeout:*	<input type="text" value="30"/>	Secs
Vendor:	<input type="radio"/> Open LDAP <input checked="" type="radio"/> MS AD	

LDAPの設定

6. システム>ユーザー管理>設定に移動します。

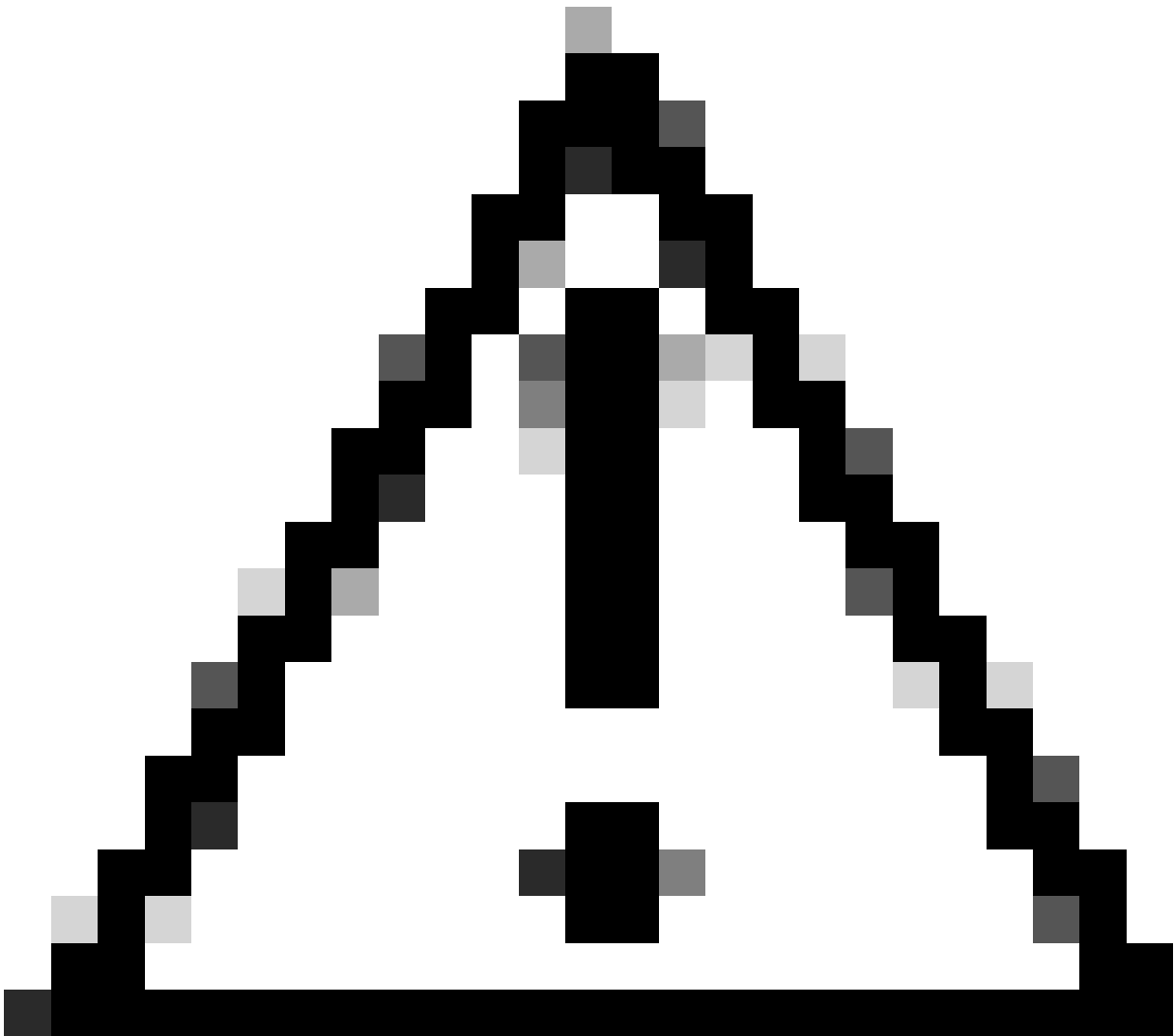
7. デフォルトまたはコンソール認証をLDAPに設定します。

Local Users	<b>Settings</b>
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"/>

認証方式の選択

8. SSHからシャーンにログインして、LDAPユーザによる認証をテストします。

---



注意：LDAP認証をテストする際には注意してください。設定にエラーがある場合、この変更によってロックアウトされる可能性があります。ロールバックまたはトラブルシューティングを実行できるように、重複セッションを使用して、またはローカル認証を使用したコンソールアクセスからテストします。

---

## LDAPSの設定

9. 正常なLDAP接続をテストしたら、再度Platform Settings > AAA > LDAPに移動します。

10. LDAPプロバイダを編集し、SSLを有効にします。

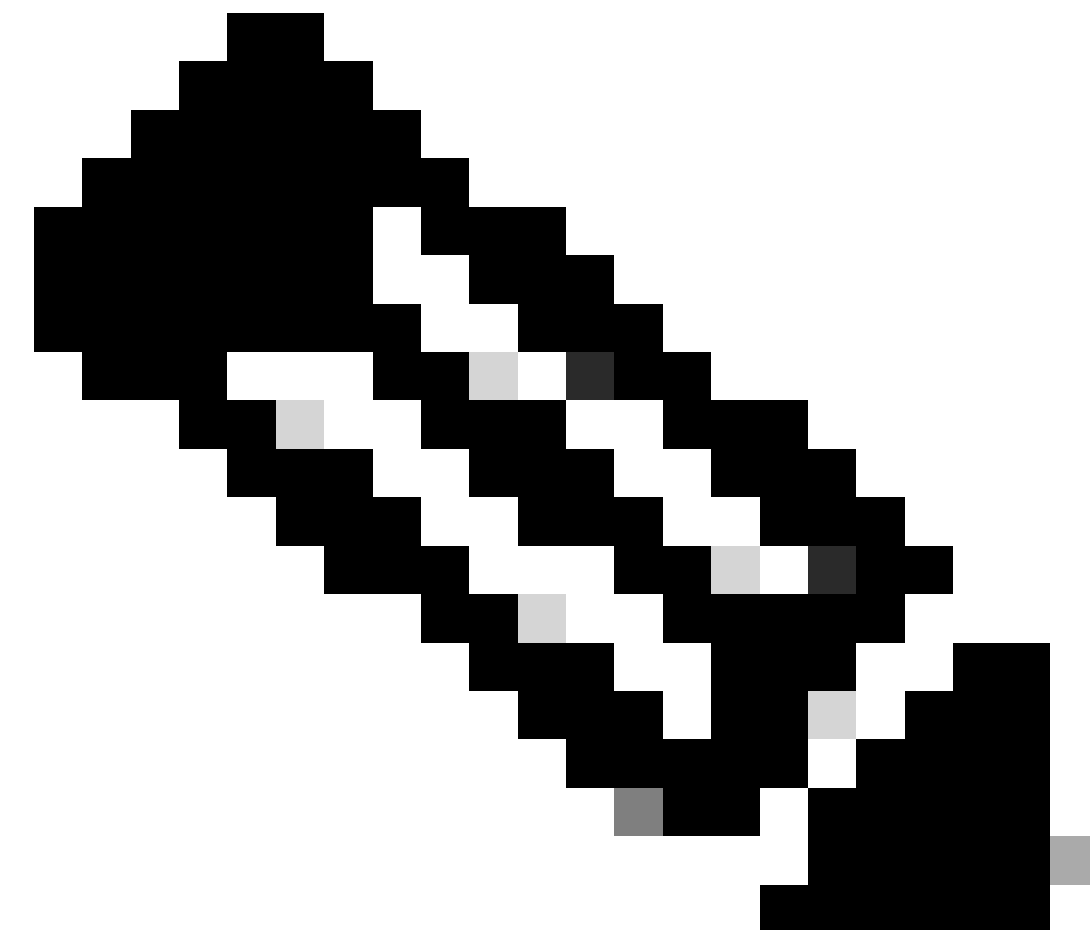
Port:\*

389

Enable SSL:



ポート選択GUI



注：暗号化にはポート389を使用する必要があります。ポート636が機能しません。機能拡張Cisco Bug ID [CSCwc93347](#)が、LDAPS用のカスタムポートを追加するために提出されました

11. LDAPサーバのルートCA証明書をシャースにインポートする必要があります。中間証明書がある場合は、チェーンと一緒にインポートします。

これを実行するには、FXOS CLIからトラストポイントを作成します。

<#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

>MSEwHwYDVQQDExhb3JnZWp1LVdJTl1KTlJHRUpVLUNBLTEwHhcNMjEzMDc0

>MDAwWhcNMjEzMDc0OTU5WjBTMRUwEwYKcZImiZPyLQBGryFbG9jYwWxFzAV

>BgoJkiaJk/IsZAEZFgdqb3JnZWp1MSEwHwYDVQQDExhb3JnZWp1LVdJTl1KTlJH

>RUpVLUNBLTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDmBTWU6Leu

>bPxvc+EhC7fxjowEjjL0EXlMo3x7Pe3EW6Gng2iOMB1UpBNgSObbct83P6y6EmQi

>0RCCnEFfzy4stYPz/7499wALwMLSGNQWr10rjVB64ihfugbx95iDBcwuv6XK67h/

>T1caN4GZiLtYZjURGs5mLNB2f8hLp9QR2WoZqfAvrfvFB4I5RJjx0FYKIXW1dmPT

>AAPa/Qi+1Qv1exfzvXHXx1GMDCHle2yItFgl6o7OujT0AE3oplA/qQD+mTAJmdcR

>QLUDiUptqqYKgcbrH4Hu4PMje3INLd1vw1ThAwMFn+oXjRTM0KbEQ0/JEM6xRFMv

>LqzmDwxA8IoRagMBAAGjaTBnMBMGCSsGAQQBgjcUAgQGHgQAQwBBMA4GA1UdDwEB

>/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. LDAPプロバイダで構成されているLDAPサーバー構成を入力します。LDAPサーバの名前をメモします。

13. 取り消しポリシーをrelaxedに設定します。

<#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. commit-bufferを使用して変更を保存します。

## トラブルシューティング

### DNS解決

FQDNが正しいIPに解決されていることを確認します。名前解決に問題がある可能性があります。

```
<#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
```

DNS名前解決が正常に行われると、次のようになります。

```
<#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.
```

## TCPおよびSSLハンドシェイク

LDAPS接続を確認するには、ポート389でキャプチャを設定します。

「Unknown CA」などのアラートが表示される場合は、LDAPサーバのルートCA証明書が一致していないことを意味します。証明書がサーバのルートCAであることを確認します。

```
<#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
```

接続が正常に行われると、次のようになります。

```
<#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
```

## デバッグ

より詳細なトラブルシューティングの場合の詳細については、LDAPのデバッグを有効にすることが出来ます。

SSL接続が正常に行われると、次のように表示されます。大きなエラーは表示されません。

```
<#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...
```

サーバのルートCA証明書が一致しない場合は、ldap\_check\_cert\_chain\_cbプロセスで証明書エラーを確認できます。

```
2024 Feb 1 12:07:08.624416 ldap: ldap_app_cb: - Check the configured hostname WIN-JOR.jor.local with pe
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
```

## ロックアウトされた状態からの回復

何らかの理由でChassis ManagerのGUIからロックアウトされ、LDAPSが機能していない場合でも、CLIにアクセスできれば回復できます。

これを行うには、デフォルト認証またはコンソール認証で認証方式をローカルに戻します。

```
<#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
```

これらの変更を行った後、もう一度FCMにログインします。

## 関連情報

- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。