

在FXOS中配置LDAPS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[配置純LDAP](#)

[配置LDAPS](#)

[疑難排解](#)

[DNS解析](#)

[TCP和SSL握手](#)

[偵錯](#)

[從鎖定狀態中恢復](#)

[相關資訊](#)

簡介

本檔案介紹如何使用安全防火牆機箱管理員(FCM)和CLI在FXOS上設定Secure LDAP (LDAPS)。

必要條件

需求

思科建議您瞭解以下主題：

- 安全防火牆可擴充作業系統(FXOS)
- 安全防火牆機箱管理員(FCM)
- 輕量型目錄存取通訊協定(LDAP)概念

採用元件

本文檔中的資訊基於：

- 安全防火牆9300裝置版本2.12(0.8)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

建議測試普通LDAP在安全防火牆裝置上是否正常工作。

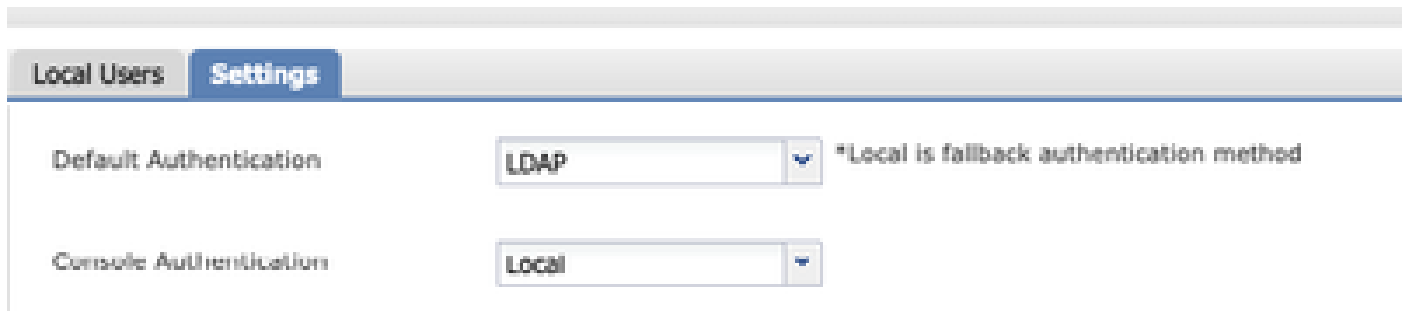
配置純LDAP

1. 登入FCM。
2. 導航到平台設定> AAA > LDAP
3. 按一下LDAP Providers > Add
4. 配置LDAP提供程式，並輸入Microsoft Active Directory (MS AD)的繫結DN、基本DN、屬性和金鑰資訊。
5. 使用LDAP伺服器的FQDN，因為SSL連線需要此項。

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	

6. 導航到系統>使用者管理>設定。
7. 將「預設」或「主控台」驗證設為LDAP。



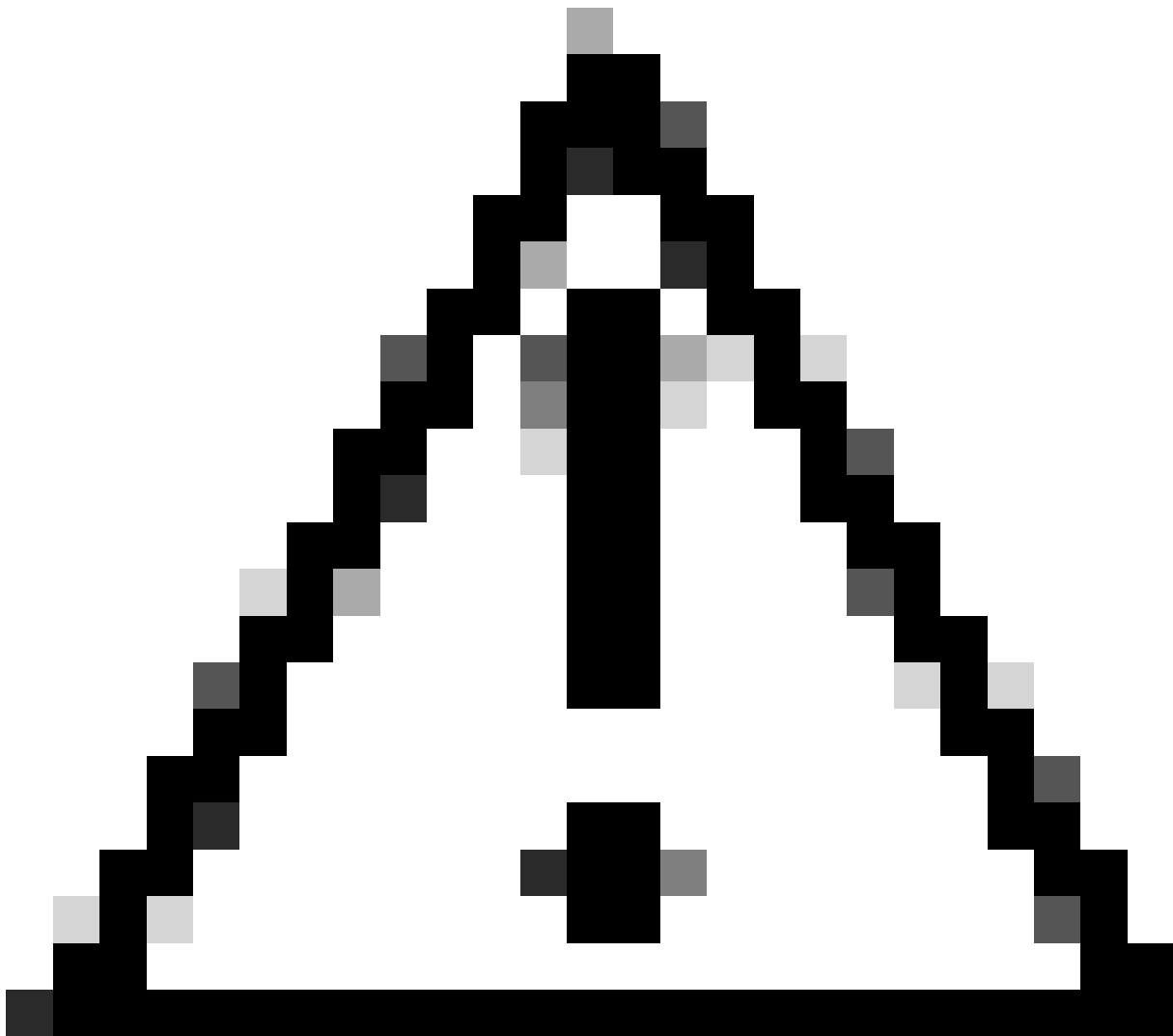
Local Users Settings

Default Authentication: LDAP *Local is fallback authentication method

Console Authentication: Local

身份驗證方法選擇

8. 嘗試從SSH登入到機箱以測試使用LDAP使用者的身份驗證。



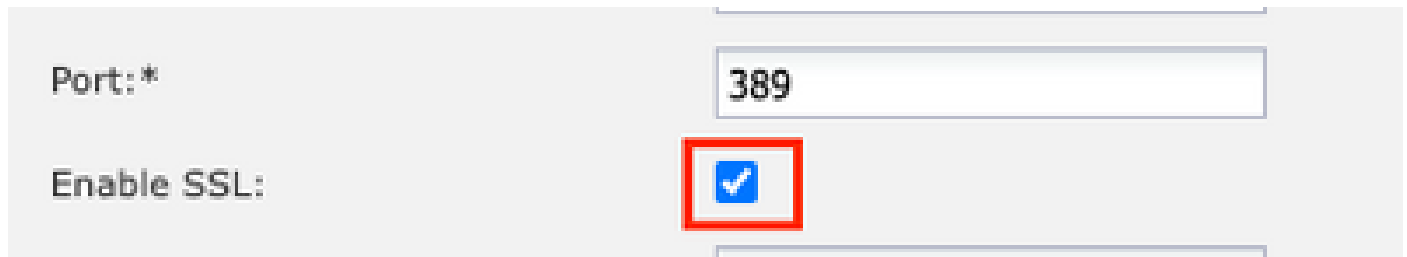
注意：測試LDAP身份驗證時要小心。如果組態發生錯誤，此變更可能會將您鎖定。使用重

複的階段作業進行測試，或透過主控台存取進行本機驗證進行測試，以便執行倒回或疑難排解。

配置LDAPS

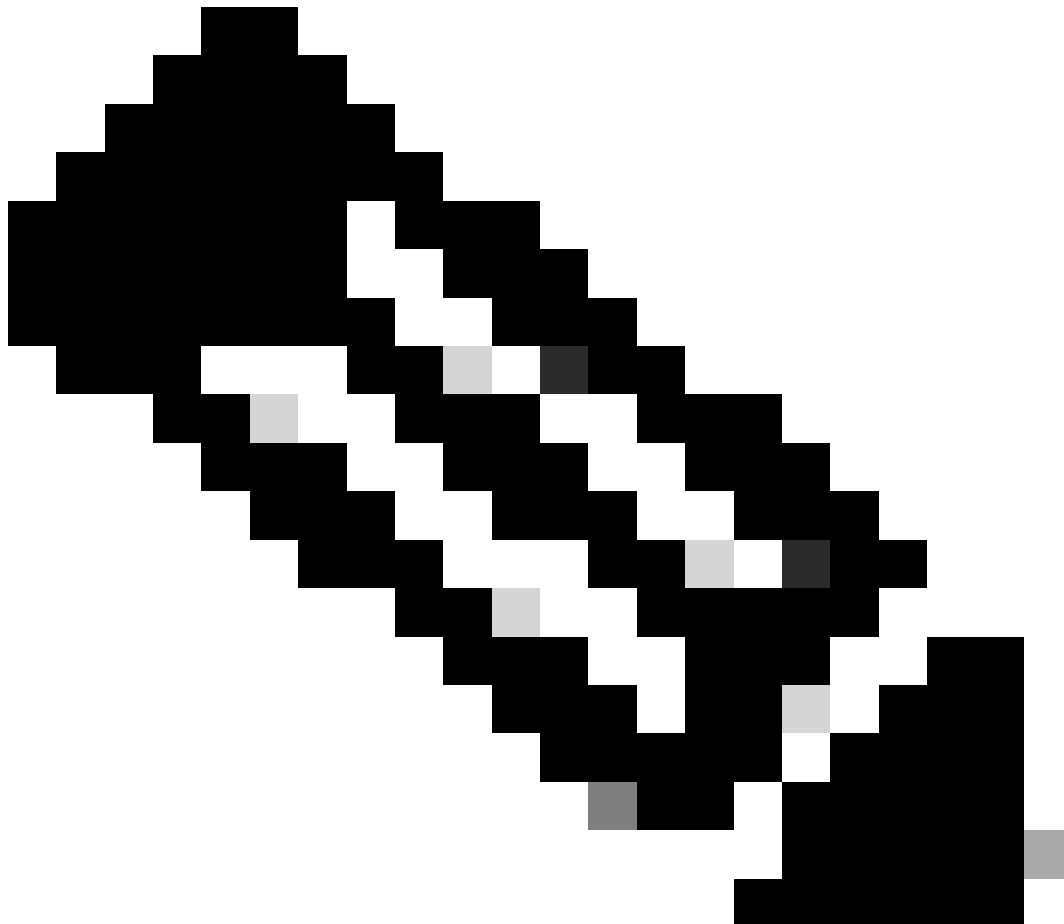
9. 測試成功的LDAP連線後，再次導航到平台設定> AAA > LDAP。

10. 編輯LDAP提供者並啟用SSL。



The screenshot shows a configuration form for LDAP. The 'Port: *' field is set to '389'. The 'Enable SSL:' checkbox is checked and highlighted with a red square. Below the checkbox is a partially visible text field.

埠選擇GUI




```
>T1caN4GZiLtYZjURGs5mLNB2f8hLp9QR2WoZqfAvrfvFB4I5RJjx0FYKIXWldmPT

>AAPa/Qi+1QvlexfzvXHXx1GMDCHle2yItFgl6o7OujT0AE3oplA/qQD+mTAJmdcR

>QLUDiUptqqYKgcbrH4Hu4PMje3INLdlvw1ThAwMFn+oXjRTM0KbEQ0/JEM6xRFMv

>Lq mzDwxA8IoRagMBAAGjaTBnMBMGCSsGAQQBgcUAgQGHgQAQwBBMA4GA1UdDwEB

>/wQEAWIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQoweZEEke7BIod94R5

>YxjvJHdzsJAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAYGli

>n77K0OiqSljTeg+ClVLRX8VJwr7Pp5p4Mu0mRhZckmIKSUtYDla3ToVix5k4dXSU

>7MaVWDkW/1NvReaqCfis5mgfrpzoPUkqKGiz7Zhd57gA4tBU/XbP/CXpTuAR3Isa

>NKz7yy+6tisf+8vfLtrN8c3IclS6ncyrdAdJ2iJY74jJm1eUPs3muaqApPPwoRF2

>GdALD/Y+Pq36csjK+jGP1+2rD6cW16thBp9p1OoTL+qpq4DL+W6uctWeRMgGxcWn

>GsKhHysno9dZ+Dnn0lx0tP+s1B9fmxF7ycCmmn328dzVEG7JXjHc8KoqwwWe+fwu

>GXLRM+rKaAICH52EEw==

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

>ENDOFBUF

FPR9300-01 /security/trustpoint* #

commit-buffer
```

12. 輸入在LDAP提供者上配置的LDAP伺服器組態。記下LDAP伺服器的名稱。

13. 將撤銷政策設為放寬。

```

<#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. 使用commit-buffer儲存更改。

疑難排解

DNS解析

檢查FQDN是否解析為正確的IP。名稱解析可能有問題：

```

<#root>
FPR9300-01#
connect fxos

FPR9300-01(fxos)#

```

```
ethanalyzer 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 name
```

成功的DNS名稱解析如下所示：

```
<#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-JOR.jor.local
```

```
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.jor.local
```

TCP和SSL握手

為了驗證LDAPS連線，請在埠389上設定捕獲。

如果看到未知CA之類的警報，則表示LDAP伺服器的根CA證書不匹配。驗證憑證是否確實是伺服器的根CA。

```
<#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 Exchange
```

```
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 Len=0
```

```
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)
```

```
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
```

成功的連線如下所示：

```
<#root>
```


FPR9300-01(fxos)#

```
ethalyzer 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
```

偵錯

您可以啟用LDAP調試，以便在進行更深入的故障排除時獲得更多資訊。

成功的SSL連線如下所示，未發現任何重大錯誤：

```
<#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_crls_http_and_local_cb: - get CRL from CRLDP
2024 Feb 1 12:19:20.520626 ldap: ldap_crls_http_and_local_cb: - crls 0x121787dc
2024 Feb 1 12:19:20.520900 ldap: ldap_load_crl_crl_dp: - get CRL from CRLDP
2024 Feb 1 12:19:20.521135 ldap: ldap_load_crl_crl_dp: - crls 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_crl_http: - entering...
```

當伺服器的根CA證書不匹配時，您可以在ldap_check_cert_chain_cb進程中觀察到證書錯誤：

```
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, crlstrict 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
```

從鎖定狀態中恢復

如果由於任何原因被機箱管理器GUI鎖定，並且LDAPS不起作用，則仍可以在訪問CLI的情況下進行恢復。

這可以透過將預設身份驗證或控制檯身份驗證的身份驗證方法更改回本地來完成。

```
<#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
```

完成這些變更後，請再次嘗試登入FCM。

相關資訊

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。