

Configure LDAPS in FXOS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration](#)

[Configure Plain LDAP](#)

[Configure LDAPS](#)

[Troubleshoot](#)

[DNS Resolution](#)

[TCP and SSL Handshake](#)

[Debugging](#)

[Recover from Being Locked Out](#)

[Related Information](#)

Introduction

This document describes how to configure Secure LDAP (LDAPS) on FXOS using Secure Firewall Chassis Manager (FCM) and CLI.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall eXtensible Operating System (FXOS)
- Secure Firewall Chassis Manager (FCM)
- Lightweight Directory Access Protocol (LDAP) concepts

Components Used

The information in this document is based on:

- Secure Firewall 9300 device version 2.12(0.8)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

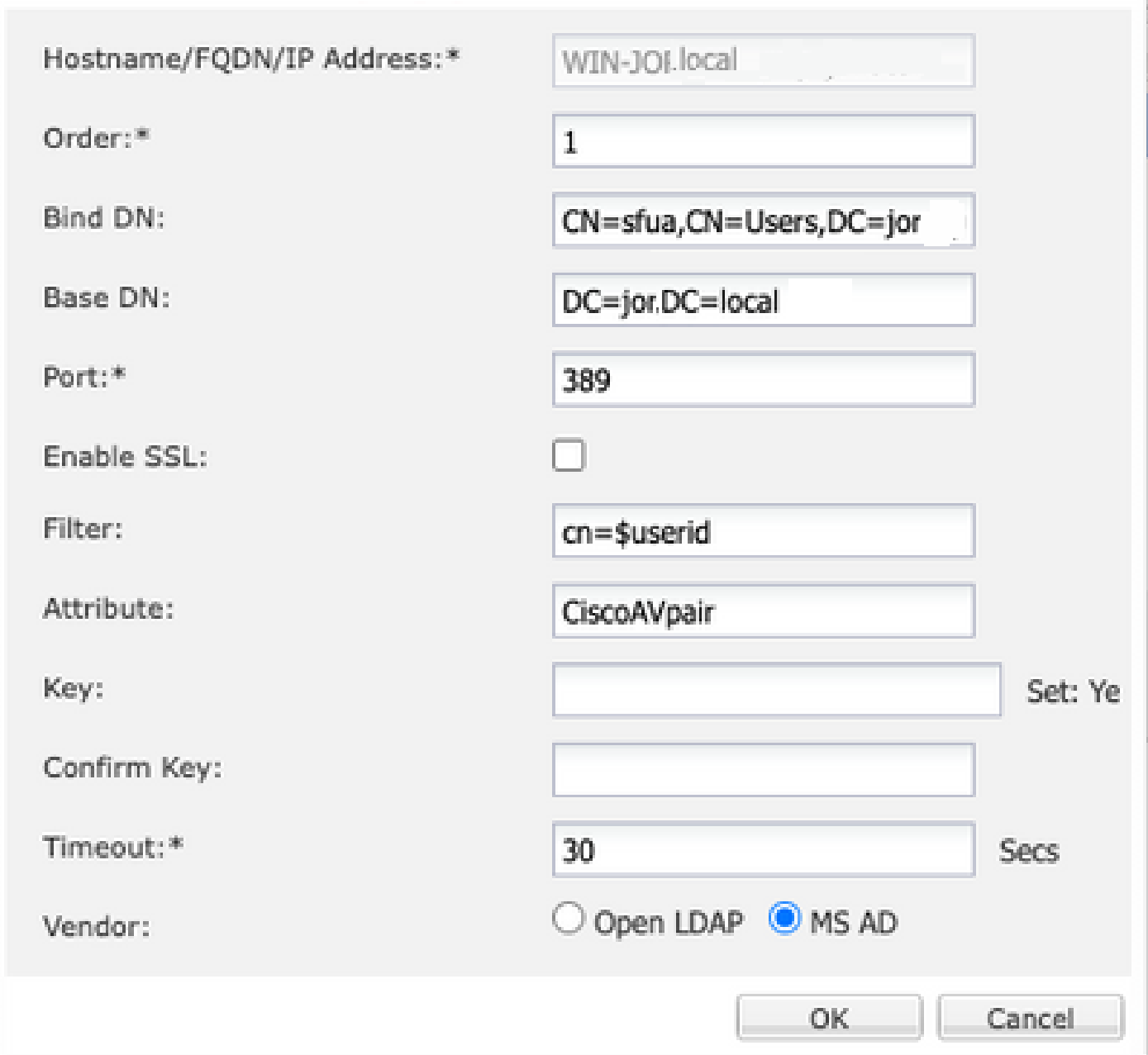
Configuration

It is recommended to test that plain LDAP works on your Secure Firewall device.

Configure Plain LDAP

1. Log into FCM.
2. Navigate to **Platform Settings > AAA > LDAP**
3. Click on **LDAP Providers > Add**
4. Configure LDAP provider and enter Bind DN, Base DN, Attribute and Key information for Microsoft Active Directory (**MS AD**).
5. Use the FQDN of the LDAP server, as this is needed for SSL connection.

Edit WIN-JOR .local



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

OK Cancel

LDAP Configuration

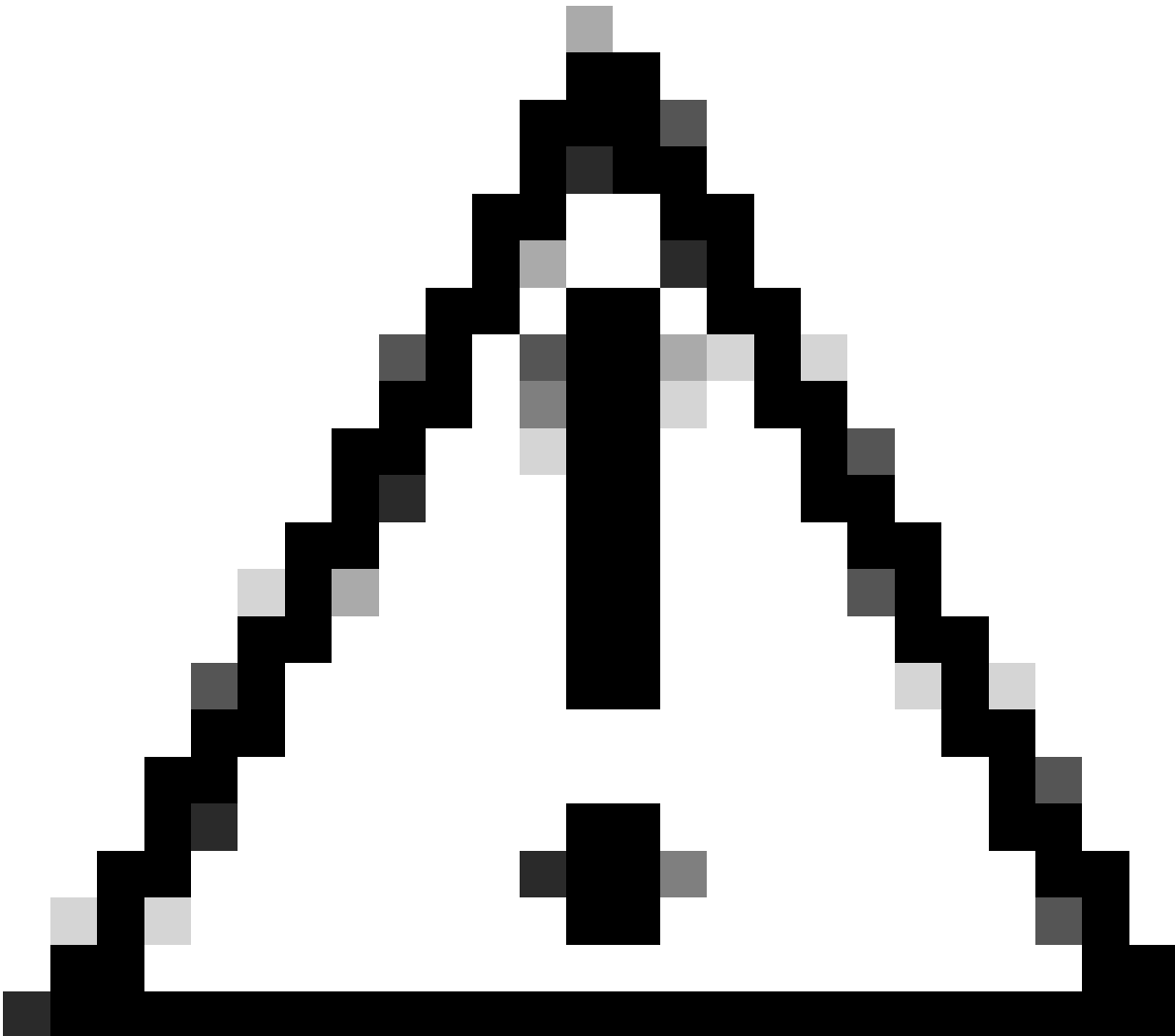
6. Navigate to **System > User Management > Settings**.

7. Set either Default or Console authentication to LDAP.

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

Authentication method selection

8. Try to log in from SSH to the chassis to test authentication with an LDAP user.

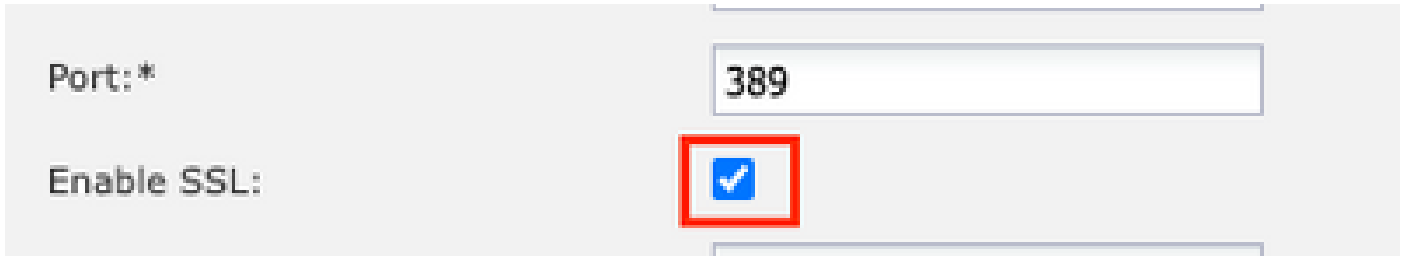


Caution: Be careful when testing LDAP authentication. If there is an error in the configuration, this change can lock you out. Test with a duplicate session or from console access with local authentication so rollback or troubleshoot can be performed.

Configure LDAPS

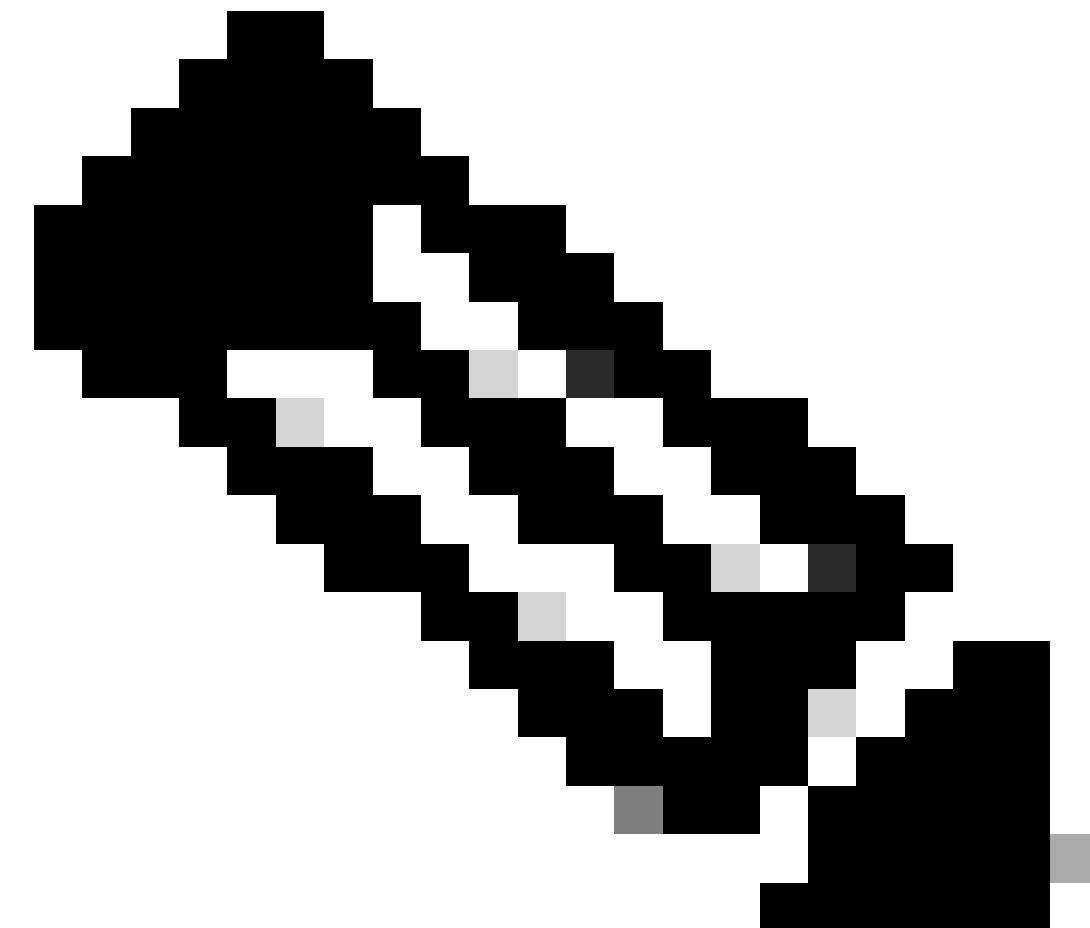
9. Once you have tested a successful LDAP connection, navigate again to **Platform Settings > AAA > LDAP**.

10. Edit your LDAP provider and enable SSL.



The screenshot shows a configuration interface for LDAP. It features two rows of controls. The first row has the label "Port:*" on the left and a text input field containing the number "389". The second row has the label "Enable SSL:" on the left and a checked checkbox. The checkbox is highlighted with a red square border.

Port Selection GUI



Note: Port 389 needs to be used for encryption. Port 636 does not work. Enhancement Cisco bug ID [CSCwc93347](#) was filed to add custom ports for LDAPS

11. The root CA certificate of the LDAP server has to be imported to the Chassis. If there are intermediate certificates, import the chain together.

Create a trustpoint from FXOS CLI to perform this.

```
<#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
```

```
>MRUwEwYKCZImiZPyLQGGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdqb3JnZWp1
```

```
>MSEwHwYDVQQDEExqb3JnZWp1LVdJTlKT1JHRUpVLUNBLTEwHhcNMjEzMDc0
```

```
>MDAwWhcNMjEzMDc0OTU5WjBTMRUwEwYKCZImiZPyLQGGRYFbG9jYWwxFzAV
```

```
>BgoJkiaJk/IsZAEZFgdqb3JnZWp1MSEwHwYDVQQDEExqb3JnZWp1LVdJTlKT1JH
```

```
>RUpVLUNBLTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQMmBTWU6Leu
```

```
>bPxvc+EhC7fxjowEjjL0EXlMo3x7Pe3EW6Gng2iOMB1UpBNgSObbct83P6y6EmQi
```

```
>ORCCnEFfzy4stYPz/7499wALwMLSGNQWr10rjVB64ihfugbx95iDBcwuv6XK67h/
```

```
>T1caN4GZiLtYZjURGs5mLNB2f8hLp9QR2WoZqfAvrfvFB4I5RJjx0FYKIXW1dmPT
```

```
>AAPa/Qi+1Qv1exfzvXHXx1GMDCHle2yItFgl6o7OuJT0AE3op1A/qQD+mTAJmdcR
```

>QLUDiUptqqYKgcbrH4Hu4PMje3INLd1vw1ThAwMFn+oXjRTM0KbEQ0/JEM6xRFMv

>LqzDwxA8IoRagMBAAGjaTBnMBMGCSsGAQQBgcUAgQGHgQAQwBBMA4GA1UdDwEB

>/wQEAWIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBQoweZEEke7BIOd94R5

>YxjvJHdzsjaQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAYGli

>n77K00iqSljTeg+ClVLRX8VJwr7Pp5p4Mu0mRhZckmIKSUtYDla3ToVix5k4dXSU

>7MaVWDkW/1NvReaqCfis5mgfrpzoPukqKGiz7Zhd57gA4tBU/XbP/CXpTuAR3Isa

>NKz7yy+6tisf+8vfLtrN8c3IclS6ncyrdAdJ2iJY74jJmleUPS3muaqApPPwoRF2

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

>GsKhHysno9dZ+DnnOlX0tP+S1B9fmxF7ycCmmn328dZVEG7JXjHc8KoqwwWe+fwu

>GXLRM+rKaAICH52EEw==

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

>ENDOFBUF

FPR9300-01 /security/trustpoint* #

commit-buffer

12. Enter LDAP server configuration as configured on LDAP provider. Take note of the name of your LDAP server.

13. Set the revoke-policy to relaxed.

<#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. Save changes using commit-buffer.

Troubleshoot

DNS Resolution

Check that FQDN is being resolved to the correct IP. There can be problems with name resolution:

```
<#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
```

A successful DNS name resolution looks like this:

```
<#root>
```

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

```
ethalyzer 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 and SSL Handshake

In order to verify LDAPS connection, set captures on port 389.

If you see alerts such as Unknown CA, it means that the root CA certificate of the LDAP server is not matching. Verify that the certificate is indeed the root CA of the server.

```
<#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, Reason: 0)
```

```
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
```

A successful connection looks like this:

```
<#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=1460
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 Len=0
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=0
```



```
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 Len=0
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 Exchange, 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 Len=0
10 2024-02-01 12:12:49.150071315 10.4.23.202 → 10.4.23.128 TLSv1.2 171 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake
11 2024-02-01 12:12:49.150995765 10.4.23.128 → 10.4.23.202 TLSv1.2 117 Change Cipher Spec, Encrypted Handshake
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=0 Len=0
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=0 Len=0
```

Debugging

You can enable debugs for LDAP for more information in case of deeper troubleshoot.

A successful SSL connection looks like this, no major error is observed:

```
<#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-JORGEJU
2024 Feb 1 11:51:16.244487 ldap: ldap_client_lib_init_ssl: set ldap options cipher_suite ALL:!DHE-PSK-AES256-SHA:!EDH-DSS-DES-CBC3-SHA:!DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM+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 0x121787dc
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_crl_crldp: - get CRL from CRLDP
2024 Feb 1 12:19:20.521135 ldap: ldap_load_crl_crldp: - 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...
```

When the root CA certificate of the server is not matching, you can observe certificate errors on the `ldap_check_cert_chain_cb` process:

```
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
```

Recover from Being Locked Out

If you were locked out for any reason from the Chassis Manager GUI and LDAPS is not working, you can still recover if you have CLI access.

This is done by changing the authentication method back to local either for Default Authentication or Console Authentication.

```
<#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
```

After these changes, try to log in to FCM once again.

Related Information

- [Cisco Technical Support & Downloads](#)