

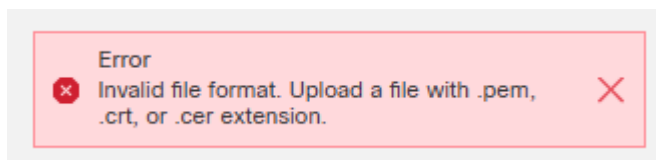
FMC LDAPS External Authentication Certificate - Invalid File Format Error

Contents

Issue

- When attempting to use a renewed certificate for LDAPS (LDAP over SSL) External Authentication on Cisco Firepower Management Center (FMC) version 7.6.5, the system displays this error message in the External Authentication page:

"Invalid file format. Upload a file with .pem, .crt, or .cer extension."



- This error prevents the LDAPS configuration from working correctly and denies external users the ability to login to the FMC.
- Additional error details from the FMC messages logs show the certificate as not renewed when running a test login from the FMC External Authentication page:

```
[Wed May 06 15:14:08.156870 2026] [cgi:error] [pid 5067:tid 23059043894848] [client 10.X.X.36:4972]
[Wed May 06 15:14:08.156971 2026] [cgi:error] [pid 5067:tid 23059043894848] [client 10.X.X.36:4972]
[Wed May 06 15:14:08.157014 2026] [cgi:error] [pid 5067:tid 23059043894848] [client 10.X.X.36:4972]
[Wed May 06 15:14:08.157065 2026] [cgi:error] [pid 5067:tid 23059043894848] [client 10.X.X.36:4972]
```

Environment

- Cisco Firepower Management Center (FMC) with previous LDAPS External Authentication configuration
- Certificate renewal process involving intermediate certificate expiration

Resolution

Ensure the certificate file meets FMC formatting requirements for LDAPS authentication:

1.- The certificate file must be PEM-encoded and include the entire certificate chain in this order:

```
-----BEGIN CERTIFICATE-----  
(certificate for your server)  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
(the intermediate certificate)  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
(the root certificate for the CA)  
-----END CERTIFICATE-----
```

2.- Verify that the certificate file contains:

- No extra blank lines or spaces before -----BEGIN CERTIFICATE----- markers
- No additional text after -----END CERTIFICATE----- markers
- Proper base64 encoding between certificate markers
- No binary format encoding

3.- Ensure the certificate includes:

- Server certificate for the LDAP server
- Intermediate CA certificate
- Root CA certificate
- Basic constraints marked as "critical" if CA is set to "True"

Alternative Resolution

If certificate formatting issues persist, consider implementing Single Sign-On (SSO) authentication as an alternative to LDAPS certificate-based authentication. This approach eliminates the immediate certificate formatting requirements while providing secure external authentication capabilities.

Cause

The issue is caused by an improperly formatted certificate file being uploaded during the LDAPS certificate renewal process. Specifically, the renewed certificate did not meet FMC requirements for:

- Correct PEM encoding format
- Complete certificate chain structure
- Proper certificate headers and footers
- Absence of binary encoding or extra formatting characters

The FMC validation process detected the certificate format issues and rejected the file as invalid, preventing successful upload and configuration of the renewed LDAPS certificate.

Related Content

- [Configure FMC and FTD with LDAP for External Authentication](#)
- [Proper format of the Certificate for FMC](#)
- [Create a single PEM file](#)
- [Cisco Technical Support & Downloads](#)