

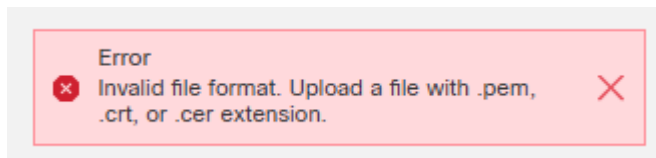
FMC LDAPS外部驗證證書 — 無效檔案格式錯誤

目錄

問題

- 在Cisco Firepower Management Center(FMC)版本7.6.5上嘗試為LDAPS(LDAP over SSL)外部身份驗證使用更新的證書時，系統會在外部身份驗證頁面中顯示以下錯誤消息：

"無效的檔案格式。上傳副檔名為.pem、.crt或.cer的檔案。"



- 此錯誤使LDAPS配置無法正常工作，並使外部使用者無法登入到FMC。
- FMC消息日誌的其他錯誤詳細資訊顯示從FMC External Authentication頁面運行測試登入時證書未續訂：

```
[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]
```

環境

- 具有先前LDAPS外部身份驗證配置的Cisco Firepower管理中心(FMC)
- 涉及中間證書到期的證書續訂過程

解析

確保證書檔案滿足LDAPS身份驗證的FMC格式要求：

1. — 憑證檔案必須採用PEM編碼，並按以下順序包括整個憑證鏈結：

```
-----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. — 驗證證書檔案是否包含：

- 在(BEGIN CERTIFICATE)標籤之前沒-----額外的空行-----空格
- 在[END CERTIFICATE]標籤-----後沒有其他-----本
- 證書標籤之間的正確base64編碼
- 無二進位制格式編碼

3. — 確保證書包括：

- LDAP伺服器的伺服器證書
- 中間CA證書
- 根CA證書
- 如果CA設定為「True」，則標籤為「關鍵」的基本約束

替代解決方案

如果憑證格式問題持續存在，請考慮實作單一登入(SSO)驗證，以替代基於LDAPS憑證的驗證。此方法消除了直接的證書格式要求，同時提供了安全的外部身份驗證功能。

原因

此問題是由在LDAPS證書續訂過程中上載格式不正確的證書檔案導致的。具體而言，續訂的證書不符合FMC的要求：

- 正確的PEM編碼格式
- 完整的證書鏈結構
- 正確的證書頁首和頁尾
- 缺少二進位制編碼或額外的格式字元

FMC驗證過程檢測到證書格式問題，並拒絕該檔案無效，從而阻止了續訂LDAPS證書的上傳和配置。

相關內容

- [使用LDAP為外部身份驗證配置FMC和FTD](#)
- [FMC證書的正確格式](#)
- [建立單個PEM檔案](#)
- [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）。