

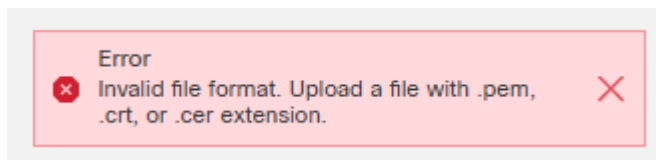
FMC LDAPS外部身份验证证书 — 无效文件格式错误

目录

问题

- 在Cisco Firepower管理中心(FMC)版本7.6.5上尝试为LDAP (SSL上的LDAP) 外部身份验证使用更新证书时，系统会在外部身份验证(External Authentication)页面中显示以下错误消息：

"无效的文件格式.上传扩展名为.pem、.crt或.cer的文件。"



- 此错误会阻止LDAPS配置正常工作，并拒绝外部用户登录到FMC。
- FMC消息日志的其他错误详细信息显示从FMC外部身份验证(FMC External Authentication)页面运行测试登录时证书未续订：

```
[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]
```

环境

- Cisco Firepower管理中心(FMC)，具有以前的LDAPS外部身份验证配置
- 涉及中间证书到期的证书续订流程

分辨率

确保证书文件符合LDAPS身份验证的FMC格式要求：

1. — 证书文件必须采用PEM编码并包括整个证书链，顺序如下：

```
-----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. — 验证证书文件是否包含：

- 在----- BEGIN CERTIFICATE”标记之前没有额外的空白行或空格
- 在[END CERTIFICATE]标记-----后无附加-----本
- 证书标记之间正确的base64编码
- 无二进制格式编码

3. — 确保证书包括：

- LDAP服务器的服务器证书
- 中间CA证书
- 根CA证书
- 如果CA设置为“True”，则标记为“critical”的基本限制

备选解决方案

如果证书格式问题持续存在，请考虑实施单点登录(SSO)身份验证作为LDAPS基于证书的身份验证的替代方案。此方法消除了直接的证书格式要求，同时提供了安全的外部身份验证功能。

原因

此问题是由在LDAPS证书续订过程中上传的格式不正确的证书文件导致的。具体而言，续订的证书不符合以下方面的FMC要求：

- 正确的PEM编码格式
- 完整的证书链结构
- 正确的证书页眉和页脚
- 缺少二进制编码或额外格式字符

FMC验证过程检测到证书格式问题，并拒绝文件为无效，导致更新的LDAPS证书无法成功上传和配置。

相关内容

- [使用LDAP配置FMC和FTD以进行外部身份验证](#)
- [FMC证书的正确格式](#)
- [创建单个PEM文件](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。