

Certificat d'authentification externe LDAPS FMC

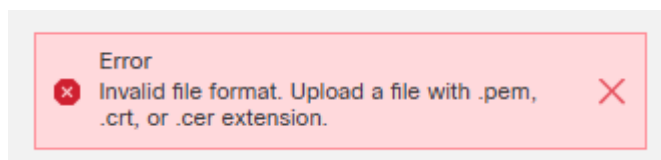
- Erreur de format de fichier non valide

Table des matières

Problème

- Lorsque vous essayez d'utiliser un certificat renouvelé pour l'authentification externe LDAP (LDAP sur SSL) sur Cisco Firepower Management Center (FMC) version 7.6.5, le système affiche le message d'erreur suivant dans la page Authentification externe :

"Format de fichier non valide. Téléchargez un fichier portant l'extension .pem, .crt ou .cer."



- Cette erreur empêche la configuration LDAPS de fonctionner correctement et empêche les utilisateurs externes de se connecter au FMC.
- Des détails d'erreur supplémentaires provenant des journaux des messages FMC indiquent que le certificat n'a pas été renouvelé lors de l'exécution d'un test de connexion à partir de la page Authentification externe FMC :

```
[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]
```

Environnement

- Cisco Firepower Management Center (FMC) avec configuration précédente d'authentification externe LDAPS

- Processus de renouvellement de certificat impliquant une expiration de certificat intermédiaire

Résolution

Assurez-vous que le fichier de certificat respecte les exigences de formatage FMC pour l'authentification LDAPS :

1.- Le fichier de certificat doit être codé en PEM et inclure la chaîne de certificats complète dans cet ordre :

```
-----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.- Vérifiez que le fichier de certificat contient :

- Aucune ligne ou espace vide supplémentaire avant les marqueurs -----BEGIN CERTIFICATE-----
- Aucun texte supplémentaire après les marqueurs -----END CERTIFICATE-----
- Codage Base64 approprié entre les marqueurs de certificat
- Aucun codage de format binaire

3.- Assurez-vous que le certificat inclut :

- Certificat de serveur pour le serveur LDAP
- Certificat CA intermédiaire
- Certificat CA racine
- Contraintes de base marquées comme "critiques" si l'autorité de certification est définie sur

"Vrai"

Résolution De Remplacement

Si les problèmes de formatage de certificat persistent, envisagez d'implémenter l'authentification SSO (Single Sign-On) comme alternative à l'authentification basée sur les certificats LDAPS. Cette approche élimine les exigences immédiates de formatage de certificat tout en offrant des fonctionnalités d'authentification externe sécurisées.

Motif

Le problème est causé par un fichier de certificat mal formaté téléchargé lors du processus de renouvellement de certificat LDAPS. Plus précisément, le certificat renouvelé ne répondait pas aux exigences du CGF concernant :

- Format de codage PEM correct
- Structure complète de la chaîne de certificats
- En-têtes et pieds de page de certificat appropriés
- Absence de codage binaire ou de caractères de mise en forme supplémentaires

Le processus de validation FMC a détecté des problèmes de format de certificat et a rejeté le fichier comme étant non valide, empêchant le téléchargement et la configuration réussis du certificat LDAPS renouvelé.

Autres informations utiles

- [Configurer FMC et FTD avec LDAP pour l'authentification externe](#)
- [Format approprié du certificat pour FMC](#)
- [Créer un fichier PEM unique](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.