

# Accès VPN AnyConnect client sécurisé refusé en raison de problèmes de conformité de la position de sécurité des terminaux

## Table des matières

---

## Problème

Plusieurs utilisateurs ne peuvent pas se connecter à AnyConnect VPN et ZTA (Zero Trust Access) et reçoivent le message d'erreur « Login deny » (Connexion refusée). Votre environnement ne répond pas aux critères d'accès définis par votre administrateur."

Le problème est lié à la conformité de la position des terminaux, où la condition relative à Endpoint Security Agent est signalée comme ne correspondant pas. Les utilisateurs se voient refuser l'accès VPN et ZTA lorsqu'ils tentent de se connecter via Cisco Secure Client.

L'évaluation de la posture indique que la posture de sécurité des terminaux Trellix échoue sur les terminaux affectés, ce qui empêche une authentification réussie au service VPN.

## Environnement

- Cisco Secure Client (AnyConnect et Zero Trust Access)
- Agent Trellix Endpoint Security version 5.8.4.505
- Profil de posture VPN : KFIN\_SECURE\_VPN avec application de l'agent de sécurité des terminaux
- Condition de posture : Agent de sécurité des terminaux exécuté avec des mises à jour au cours des 14 derniers jours
- Terminaux Windows exécutant le service Agent Trellix
- Processus Umbrella Agent détectés sur les terminaux

# Résolution

Le problème a été résolu en réglant les problèmes de conformité de la position de l'agent Trellix Endpoint Security. Les étapes de dépannage et de résolution décrites dans les sections suivantes ont été mises en oeuvre.

## Étape 1: Valider la configuration du profil de posture

Examinez le profil de posture VPN pour confirmer les exigences de l'agent de sécurité des terminaux. Le profil KFIN\_SECURE\_VPN impose l'exécution et la mise à jour d'un agent de sécurité de point d'extrémité au cours des 14 derniers jours.

## Étape 2: Vérifier l'état de sécurité des terminaux Trellix

Vérifiez l'état actuel de l'agent Trellix Endpoint Security sur les terminaux affectés :

```
Trellix Agent Service: masvc.exe  
Version: 5.8.4.505  
Install Location: C:\Program Files\McAfee\Agent\  
Display Name: Trellix Agent  
Publisher: Trellix
```

## Étape 3: Réinstaller Trellix Endpoint Security

Réinstallation complète de Trellix Endpoint Security sur les terminaux concernés :

1. Désinstallez complètement l'agent Trellix Endpoint Security existant.
2. Redémarrez le système.
3. Installez la dernière version approuvée de l'agent Trellix conformément aux normes organisationnelles.

4. Assurez-vous que l'agent s'exécute correctement après l'installation.
5. Confirmez que les mises à jour de signature/contenu se sont terminées correctement.

## Étape 4: Activer la journalisation TRACE pour Cisco Secure Client (ZTA)

Activer la journalisation détaillée pour capturer les détails d'évaluation de posture.

Créez le fichier logconfig.json avec le contenu suivant :

```
{ "global": "DBG_TRACE" }
```

Placez le fichier dans le répertoire approprié :

- Fenêtres: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- macOS : /opt/cisco/secureclient/zta

Redémarrez le service Cisco Secure Client/ZTA après avoir créé le fichier.

## Étape 5: Collecter le bundle DART mis à jour

Après avoir implémenté les modifications, collectez un nouveau bundle DART pour valider la résolution et confirmer la détection de conformité de la position.

## Motif

La cause principale a été identifiée comme des problèmes de conformité de la position des agents Trellix Endpoint Security. Le profil de posture VPN exigeait qu'un agent de sécurité des points d'extrémité exécute les mises à jour au cours des 14 derniers jours, mais l'agent Trellix Endpoint Security ne répondait pas à ces critères de conformité. Le module d'évaluation de position n'a pas pu détecter ou valider correctement l'état de l'agent de sécurité du point d'extrémité, ce qui a

entraîné un refus d'accès pour les connexions VPN et ZTA. Le problème était spécifiquement lié à la configuration de l'agent Trellix et a nécessité l'intervention de l'équipe d'assistance de Trellix pour résoudre les problèmes de conformité de l'agent sous-jacents.

## Autres informations utiles

- [Collecter des journaux ZTNA détaillés pour le dépannage](#)
- [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.