# Résoudre les problèmes de connectivité de l'agent Cowork (Frontier) lorsque Umbrella est activé

## Table des matières

## Problème

L'agent Cowork (Frontier) ne fonctionnait pas correctement sur les ordinateurs portables lorsque Cisco Umbrella était activé. Lorsque Cisco Umbrella était inactif, l'agent fonctionnait comme prévu. Les utilisateurs n'ont pas pu utiliser la fonctionnalité d'agent Cowork lorsque Umbrella était actif, et aucun journal de blocage n'était visible dans Cisco Umbrella lorsque les utilisateurs ont rencontré ce problème. Des captures d'écran d'erreur montrant les échecs d'application pendant le fonctionnement d'Umbrella ont été fournies.

## Environnement

- Cisco Umbrella déployé sur les ordinateurs portables d'entreprise
- Application d'agent Cowork (Frontier)
- Inspection du trafic SSL/TLS activée dans Cisco Umbrella
- Épinglage de certificat implémenté dans l'application Cowork

## Résolution

Le problème a été résolu en ajoutant l'application Cowork à la liste DND (Do Not Decrypt) dans Cisco Umbrella. Ce changement de configuration permet à l'agent Cowork de contourner l'inspection SSL/TLS et de maintenir sa connexion chiffrée directe aux serveurs Cowork.

### Étapes de configuration de la liste NPD

Étape 1: Accédez au tableau de bord Cisco Umbrella et accédez à la configuration de la stratégie de décodage SSL.

Étape 2: Ajoutez des domaines et des URL associés à Cowork à la liste Ne pas déchiffrer pour contourner l'inspection SSL pour cette application.

Étape 3: Appliquez les modifications de stratégie et laissez le temps à la configuration de se propager à tous les points d'extrémité.

Étape 4: Testez la fonctionnalité de l'agent Cowork avec Cisco Umbrella activé pour vérifier le bon fonctionnement.

### Validation

Après avoir implémenté la configuration de la liste DND, l'application Cowork a fonctionné normalement avec Cisco Umbrella activé. Des tests internes ont confirmé que le problème ne s'était pas reproduit pendant plusieurs jours de surveillance, et tous les utilisateurs ont pu accéder à la fonctionnalité Cowork comme prévu.

## Motif

L'agent Cowork (Frontier) utilise l'épinglage de certificat comme mécanisme de sécurité. L'épinglage de certificat signifie que l'application est codée en dur pour accepter et faire confiance uniquement à son propre certificat de serveur spécifique. Lorsque Cisco Umbrella intercepte le trafic et présente le certificat Cisco au lieu du certificat du serveur d'origine, l'application Cowork détecte cette modification, suppose que la connexion n'est pas sécurisée et abandonne intentionnellement la connexion pour protéger les données. Ce comportement est attendu pour les applications qui implémentent des mesures de sécurité d'épinglage de certificat.

## Autres informations utiles

- Créer une liste de refus de déchiffrement efficace pour les applications Microsoft
- 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.