

Le Jabber pour l'avertissement de certificat de MAC dépannent

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

[Intervention de l'utilisateur](#)

[Certificats Auto-signés](#)

[Tiers Certificats](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit un problème avec le Cisco Jabber pour la version 8.x de Macintosh (MAC) où un avertissement de certificat apparaît sur la procédure de connexion d'utilisateur et présente trois solutions différentes au problème.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Jabber pour Mac
- Gestion de certificat sur des serveurs de Cisco Unified Communications
- Systèmes d'exploitation Mac (SYSTÈME D'EXPLOITATION)

[Composants utilisés](#)

Les informations dans ce document sont basées sur la version 8.x de Cisco Jabber pour Mac.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

Quand vous tentez d'ouvrir une session au Cisco Jabber pour Mac, ce dialogue d'avertissement de certificat apparaît :



Solution

Cette section décrit les trois solutions utilisées afin d'enlever l'avertissement de certificat de la version 8.x de Cisco Jabber pour Mac.

Intervention de l'utilisateur

Vous devez cocher **toujours la case de confiance** afin d'ajouter le certificat auto-signé du serveur de Cisco Unified Presence (TASSES) à la liste de Certificats de confiance. Ceci doit être fait pour tous les Certificats auto-signés qui sont présentés.

Remarque: Vous devez entrer le mot de passe du compte administrateur de MAC OS X afin d'importer les Certificats.

Certificats Auto-signés

Si le Cisco Unified Presence (TASSE) est configuré avec les Certificats auto-signés, alors l'administrateur peut se terminer ces étapes :

1. Extrayez le certificat auto-signé des TASSES : naviguez vers la **gestion de SYSTÈME D'EXPLOITATION de Cisco Unified > la Gestion de Sécurité > de certificat**, cliquez sur le certificat de Tomcat (**tomcat.pem**), et cliquez sur Download.
2. Répétez l'étape un pour tous autres serveurs, le cas échéant, comme le Cisco Unity et le Cisco Unified MeetingPlace.
3. Concaténez les Certificats dans un fichier unique avec **.pem** comme extension (**companyABCcertificates.pem par exemple**).
4. Envoyez le fichier aux utilisateurs et demandez-leur pour le double-cliquer afin de l'ajouter à la liste de Certificats de confiance.

Remarque: L'utilisateur doit entrer le mot de passe du compte administrateur de MAC OS X afin d'importer les Certificats.

Tiers Certificats

Si la TASSE est configurée afin d'utiliser les Certificats signés de tierce partie, l'administrateur peut se terminer ces étapes :

1. Assurez-vous que le certificat racine, avec tous les Certificats intermédiaires, est téléchargé à tous les serveurs de TASSE. Naviguez vers la **gestion de SYSTÈME D'EXPLOITATION de Cisco Unified > la Gestion de Sécurité > de certificat**, et vérifiez que la Tomcat-confiance et la tasse-xmpp-confiance contiennent la chaîne de certificat du Certificate Authority de racine (CA). Cliquez sur le fichier correspondant **.pem** ou **.der** afin de vérifier.
2. Assurez-vous que vous téléchargez les Certificats signés sur tous les serveurs de TASSE : naviguez vers la **gestion de SYSTÈME D'EXPLOITATION de Cisco Unified > la Gestion de Sécurité > de certificat**, et vérifiez que tous les serveurs utilisent les Certificats signés de

tierce partie pour le **chat** et la **tasse-xmpp**.

Remarque: Une fois que les fichiers sont téléchargés, une réinitialisation est exigée pour que les modifications les prennent effet.

3. Si c'est approprié, assurez-vous que les serveurs restants (Cisco Unity, Cisco Unified MeetingPlace) sont également configurés afin d'utiliser les Certificats signés de tierce partie.
4. Assurez-vous que le certificat racine du CA, avec tous les Certificats intermédiaires, est déjà installé sur le MAC OS X.

Dépannez

Si le message d'avertissement de certificat apparaît toujours quand vous tentez d'ouvrir une session au Cisco Jabber pour Mac, cliquez sur le bouton de **certificat d'exposition** afin de trouver plus de détails sur le certificat présenté, et collectez un rapport sur les problèmes.

Informations connexes

- [Aperçu de Cisco Jabber pour Mac - Déployez les Certificats pour le Cisco Jabber pour Mac](#)
- [Support et documentation techniques - Cisco Systems](#)