# Contenu



# Introduction

Ce document décrit le processus pour dépanner le couplage de la téléphonie et de l'informatique sécurisé (CTI) pour l'intégration de Cisco Unified Communications (UC) avec l'IBM Sametime.

# Conditions préalables

## Conditions requises

Cisco recommande que vous ayez la connaissance de Cisco Unified Communications Manager.

## Composants utilisés

Les informations dans ce document sont basées sur la release 8.x de gestionnaire d'appel de Cisco Unified.

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.

# Dépannez

1. Assurez que le jeton de Sécurité a été installé sur le Cisco Call manager.
   - Allez à la **page d'admin de gestionnaire d'appel > au System > Enterprise Parameters > aux paramètres de Sécurité**.
   - Si la security mode de batterie est "0", ceci indique que le client de la liste de confiance de certificat (CTL) n'est pas configuré ou n'est pas installé dans la security mode.
   - La security mode de batterie est "1" quand elle a été installée.
2. Assurez que l'utilisateur a activé des fonctionnalités de sécurité.

- Allez à la **page > à la gestion des utilisateurs > à l'utilisateur final d'admin de gestionnaire d'appel - > les informations d'autorisations**.

3. Assurez que « la connexion sécurisée standard CTI » est ajoutée aux autorisations de groupe.
4. Vérifiez l'autorité de certification de client que des fichiers de la fonction de proxy (CAPF) sont créés et sont nommés correctement.
   - Allez au **profil de page > de gestion des utilisateurs > d'utilisateur final CAPF d'admin de gestionnaire d'appel**.
   - Assurez que les fichiers CAPF pour l'utilisateur sont créés.
   - Le format pour l'ID d'exemple de fichier CAPF doit être ><num> d'user-id de gestionnaire de <Call où le <num> est un entier de "0" à "4".
5. Vérifiez le client et serveur que des fichiers du certificat ont été téléchargés avec succès.
   - Ces fichiers se trouvent à :
     Windows XP : <username> de C:\Documents and Settings\ \ configurations locales \ données des applications \ Cisco \ SametimePhone \ Certificats \ (Windows XP)Windows 7 : <username> \ AppData \ gens du pays \ Cisco de C:\Users\ \ SametimePhone \ Certificats \Les débuts de nom du répertoire avec le <username><server> et devraient contenir :
     Au moins un fichier de serveurUn fichier clientUn fichier CTLFichiers d'exemple pour l'utilisateur « johndoe » :
     CTLFile.tlv.sgnJtapiServerKeySote-johndoe-johndoe0JtapiClientKeyStore-johndoe-johndoe0
6. Assurez-vous que ces champs sont correctement configurés dans la section sécurisée de connexion CTI de l'utilitaire de configuration :
   - L'indicateur « de connexion sécurisée d'utilisation » est vérifié
   - Serveur TFTP (habituellement le serveur de gestionnaire d'appel)
   - Port TFTP (par défaut 69)
   - Serveur CAPF (habituellement le serveur de gestionnaire d'appel)
   - Port CAPF (par défaut 3804)
   - Allez aux **préférences de Sametime > au Cisco > au contrôle de téléphone**, et assurez que le gisement de « serveurs » n'est pas editable. On ne lui permet pas de changer les serveurs sécurisés au délai d'exécution.

L'administrateur peut placer ce champ comme en lecture seule, mais s'il est editable le CTI sécurisé n'est pas activé.

## Informations connexes

- Cisco UC Integration pour l'IBM Sametime
- Support et documentation techniques - Cisco Systems