Téléphone IP sécurisé de Cisco sous la batterie de mode mixte CUCM

ID de document : 113333

Mis à jour : Nov. 28, 2011

Produits connexes

- Téléphone IP Cisco Unified 7971G-GE
- Téléphone IP Cisco Unified 7941G-GE
- Téléphone IP Cisco Unified 7970G
- Téléphone IP Cisco Unified 7960G
- Téléphone IP Cisco Unified 7941G
- Téléphone IP Cisco Unified 7961G
- + exposition davantage

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Liste de confiance de certificat
Comment sécuriser le téléphone IP
Informations connexes
Cisco relatif prennent en charge des discussions de la Communauté

Introduction

Ce document décrit la procédure pas à pas pour déplacer un téléphone IP en mode sécurisé d'une batterie du gestionnaire de Cisco Unified Communications de source (CUCM) à une batterie de la destination CUCM sans manuellement manipulation du fichier certifié de la liste de confiance (CTL) installé sur un tel téléphone IP.

Remarque: Cette procédure est indépendant de :

1. Protocole de signalisation utilisé par le téléphone. On le suppose que le protocole de

signalisation dans la source et le cluster de destination demeurent le même pour un téléphone IP spécifique.
2. Téléphonez modèle qu'exclut Cisco 7940/7960 modèle parce que les téléphones de 7940/7960 exigent de l'intervention d'utilisateur final d'entrer une chaîne d'authentification puisqu'ils n'ont pas une MIC intégrée.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur Cisco Unified Communications Manager 7.x.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Liste de confiance de certificat

Tous les serveurs dans la batterie CUCM génère les Certificats auto-signés. Les téléphones obtiennent leurs propres Certificats, qui est de deux types.

1. La fabrication a installé le certificat donné par Cisco quand vous achetez un nouveau téléphone.
2. Localement - certificat significatif remis par fonction de proxy d'autorité de Cisco.

Le CTL est une liste de Certificats auto-signés de tous les serveurs dans la batterie CUCM à la laquelle le téléphone peut faire confiance. Le CTL est enregistré sur le serveur TFTP et envoyé aux Téléphones IP.

Le périphérique, le fichier, et l'authentification de signalisation se fondent sur la création du fichier CTL, qui est créé quand vous installez et configurez le client de Cisco CTL sur des guichets uniques le poste de travail ou le serveur qui ont un port USB.

Le fichier CTL contient un certificat de serveur, une clé publique, un numéro de série, une signature, un nom d'émetteur, un nom du sujet, une fonction de serveur, un nom DNS, et une adresse IP pour chaque serveur. Quand vous configurez un Pare-feu dans le fichier CTL, vous pouvez sécuriser un Pare-feu de Cisco ASA en tant qu'élément d'un système Cisco Unified Communications Manager sécurisé. Le client de Cisco CTL affiche le certificat de Pare-feu comme certificat *CCM*. La gestion de Cisco Unified Communications Manager emploie un eToken pour authentifier la connexion de TLS entre le client de Cisco CTL et le fournisseur de Cisco CTL.

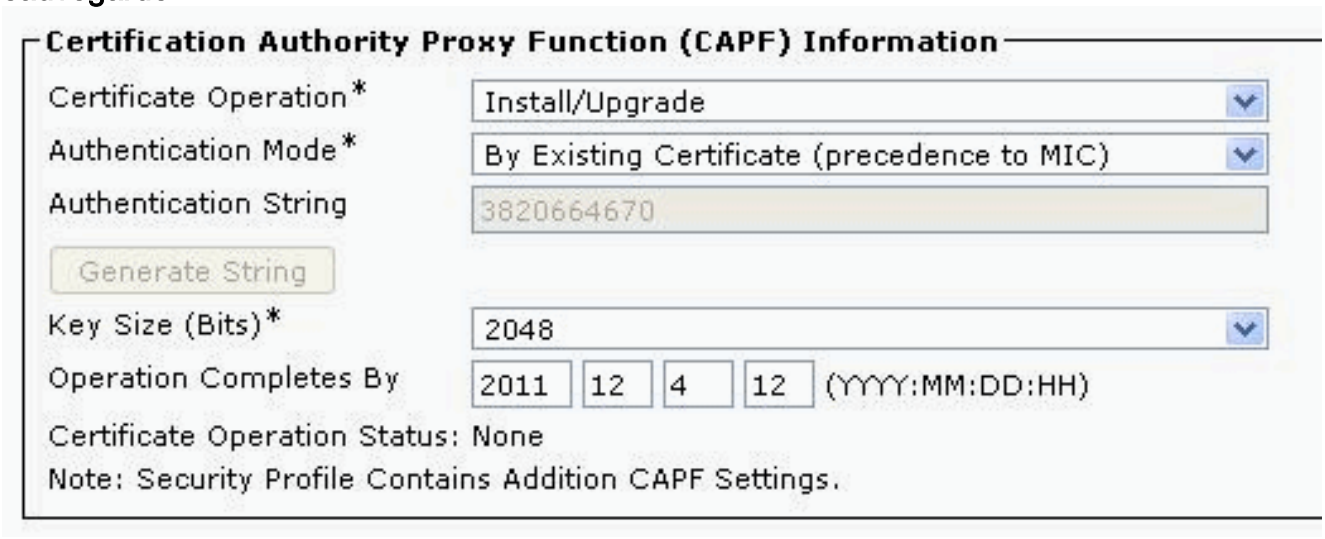
Sur la version 8.X et ultérieures CUCM, la demande de Téléphones IP un fichier CTL par défaut même si ceci n'a pas été créé. Les fichiers CTL ne sont pas considérés essentiel ; ils sont juste une partie des nouvelles fonctionnalités de sécurité qui sont livré avec le CUCM 8.x. Référez-vous à configurer le pour en savoir plus de client de Cisco CTL.

Comment sécuriser le téléphone IP

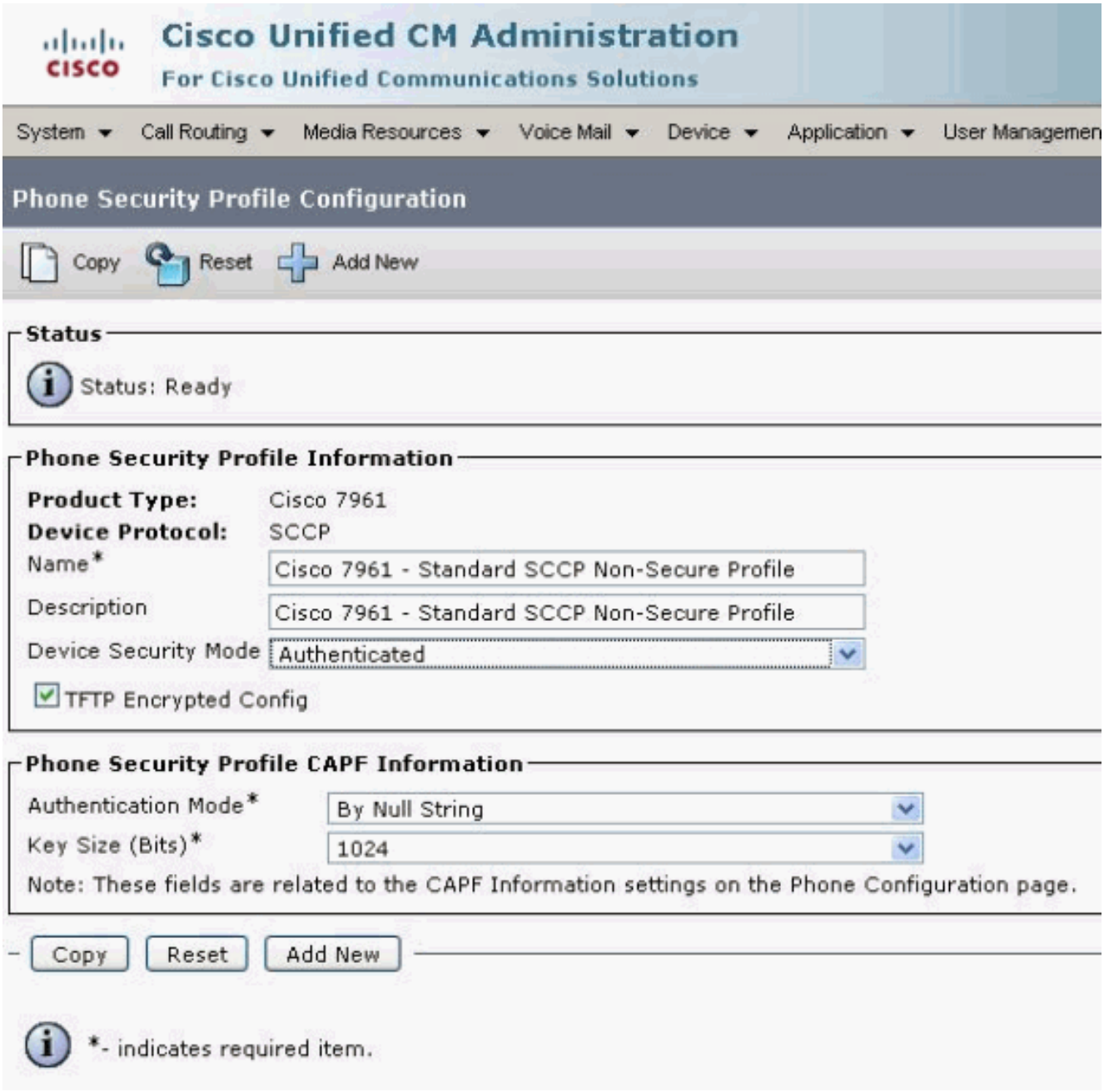
Pour que le téléphone reçoive le fichier CTL de n'importe quelle batterie sans nécessité de supprimer existant exige que le fichier CTL de chaque batterie doit être signé par la même chose ensemble partagé d'eTokens. En d'autres termes, nous devons créer un fichier CTL pour chaque batterie et signer ils tous avec la même chose eToken. Supplémentaire, téléphone la confiance dans les serveurs centralisés TFTP, vous doivent également ajouter les serveurs centralisés TFTP dans chaque fichier CTL.

Terminez-vous ces étapes afin de configurer les propriétés de Sécurité pour un téléphone IP.

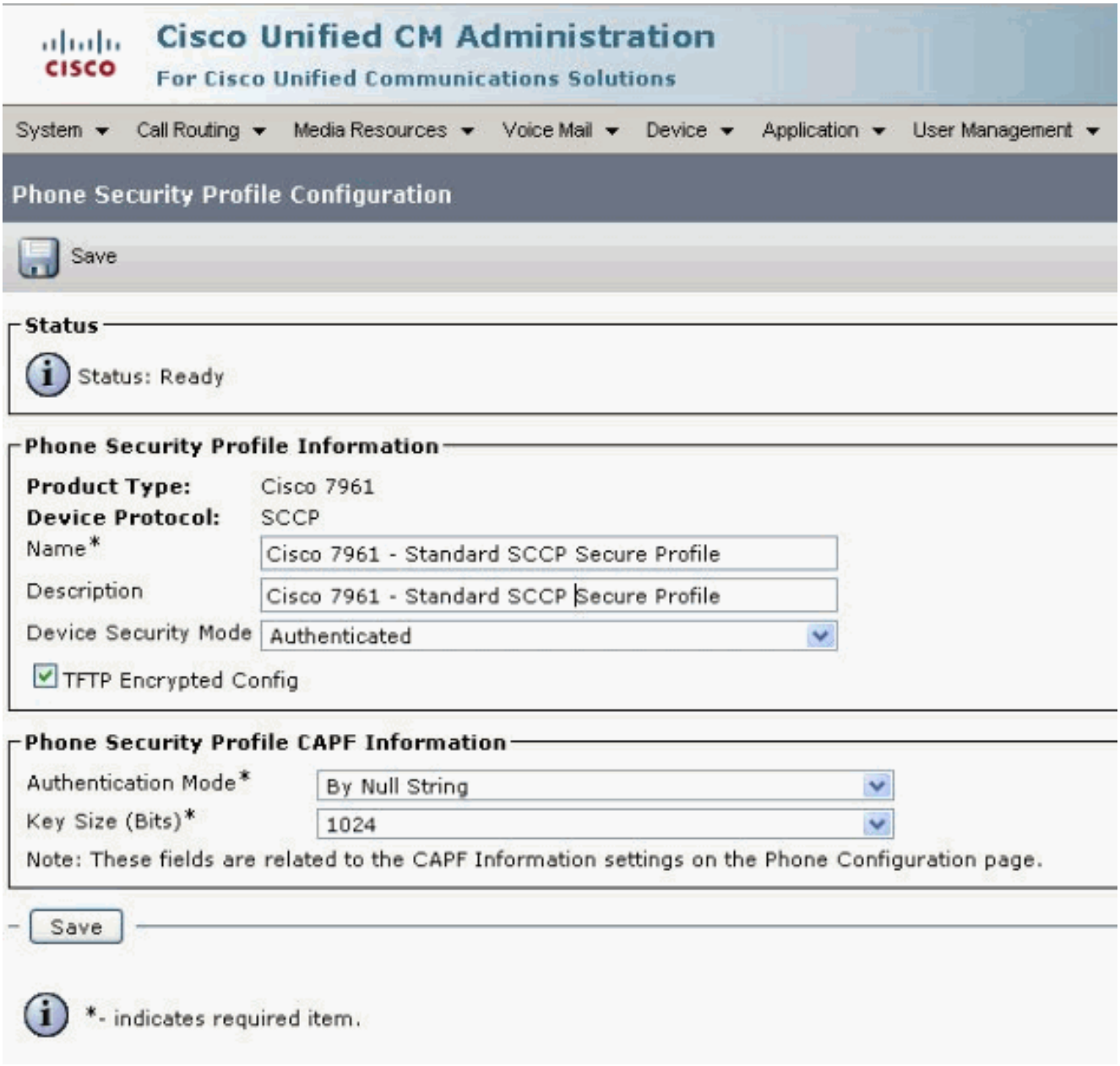
1. Configurez le profil de sécurité des périphériques. Si un profil de sécurité des périphériques approprié n'existe pas dans la liste déroulante de la page de configuration de téléphone IP, laissez-la comme par défaut, **profil Non-sécurisé standard**.
2. Configurez les informations de la fonction de proxy d'autorité de certification (CAPF), pour le téléphone IP pour obtenir un nouveau LSC, signées par la batterie de la destination CUCM.Ceci est fait à la page de configuration de téléphone de CUCM. Choisissez les valeurs du menu déroulant comme affiché et puis cliquez sur la **sauvegarde**.



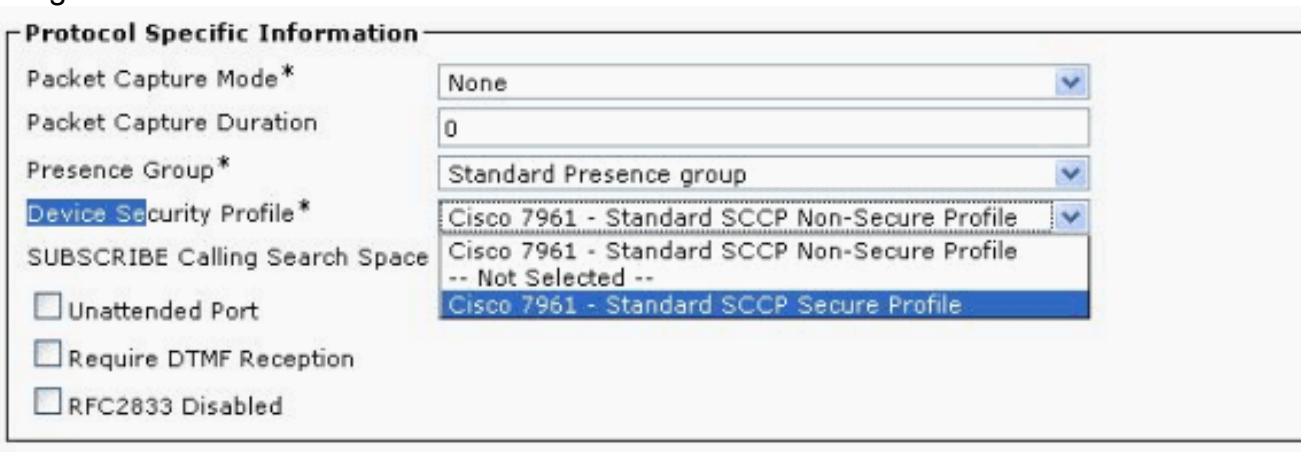
3. Configurez le nouveau profil de sécurité des périphériques créé :Choisissez le **profil de système > de Sécurité > le profil de degré de sécurité de téléphone**.Cliquez sur **Find**.Choisissez le type de téléphone et écrivez les détails
:



Copie de clic.**Sauvegardez** maintenant la configuration comme affiché ici
:



4. Àla page de configuration de téléphone IP, seconde vérification que le *mode* approprié de *sécurité des périphériques* est
configuré.



5. Redémarrez le téléphone IP.
6. Le téléphone devrait maintenant télécharger un nouveau fichier CTL du cluster de destination et devrait obtenir un LSC signé du cluster de destination.
7. Le téléphone fonctionne avec la security mode configurée dans le profil de sécurité des périphériques.

Informations connexes

- Avis de sécurité Cisco : Dépassement de segment de mémoire de fournisseur de Cisco Unified Communications Manager CTL
- Degré de sécurité de téléphone IP et CTL (liste de confiance de certificat)
- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Dépannage des problèmes de téléphonie IP Cisco
- Support et documentation techniques - Cisco Systems

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Nov. 28, 2011
ID de document : 113333