

# Démonstration de la migration d'un téléphone IP de CUCM sécurisé vers un CUCM non sécurisé

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit l'une des meilleures pratiques pour migrer des téléphones de Cisco Unified Communication Manager (CUCM) sécurisé vers un CUCM non sécurisé.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CUCM
- Téléphone IP

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Versions CUCM - 12.5.1.16065-1 et 12.5.1.14900-63
- Modèle de téléphone IP - 8865 et version - 12.8(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configurer

## Diagramme du réseau

IP\_Phone > Commutateur Cisco > Routeur Cisco > Commutateur Cisco > Cluster CUCM

## Configurations

Ces scénarios expliquent la migration du téléphone d'un cluster CUCM sécurisé vers un cluster CUCM non sécurisé. Au cours de chaque étape, l'état des fichiers CTL (Certificate Trust List) et ITL (Identity Trust List) sur le téléphone est documenté.

1. Enregistrez un téléphone dans un cluster CUCM non sécurisé.
2. Convertir un cluster non sécurisé en cluster CUCM sécurisé.
3. Convertir de nouveau en cluster non sécurisé à partir de sécurisé
4. Faites migrer le téléphone vers un nouveau cluster CUCM non sécurisé.

1. Enregistrez un téléphone dans un cluster CUCM non sécurisé.

Il s'agit des informations relatives au cluster source non sécurisé.

- Adresse IP : 10.201.251.171
- FQDN - cucm1052.domain.com
- Version : 12.5.1.16065-1

Enregistrez un téléphone dans un cluster CUCM non sécurisé. Pour cela, configurez l'option DHCP (Dynamic Host Configuration Protocol) 150 / 66 pour pointer vers l'adresse IP TFTP (Trivial File Transfer Protocol) (il s'agit du noeud CUCM où le service TFTP est activé).

Pour l'infrastructure où vous ne disposez pas des serveurs DHCP, vous devez configurer manuellement l'adresse IP TFTP sur le téléphone physique.

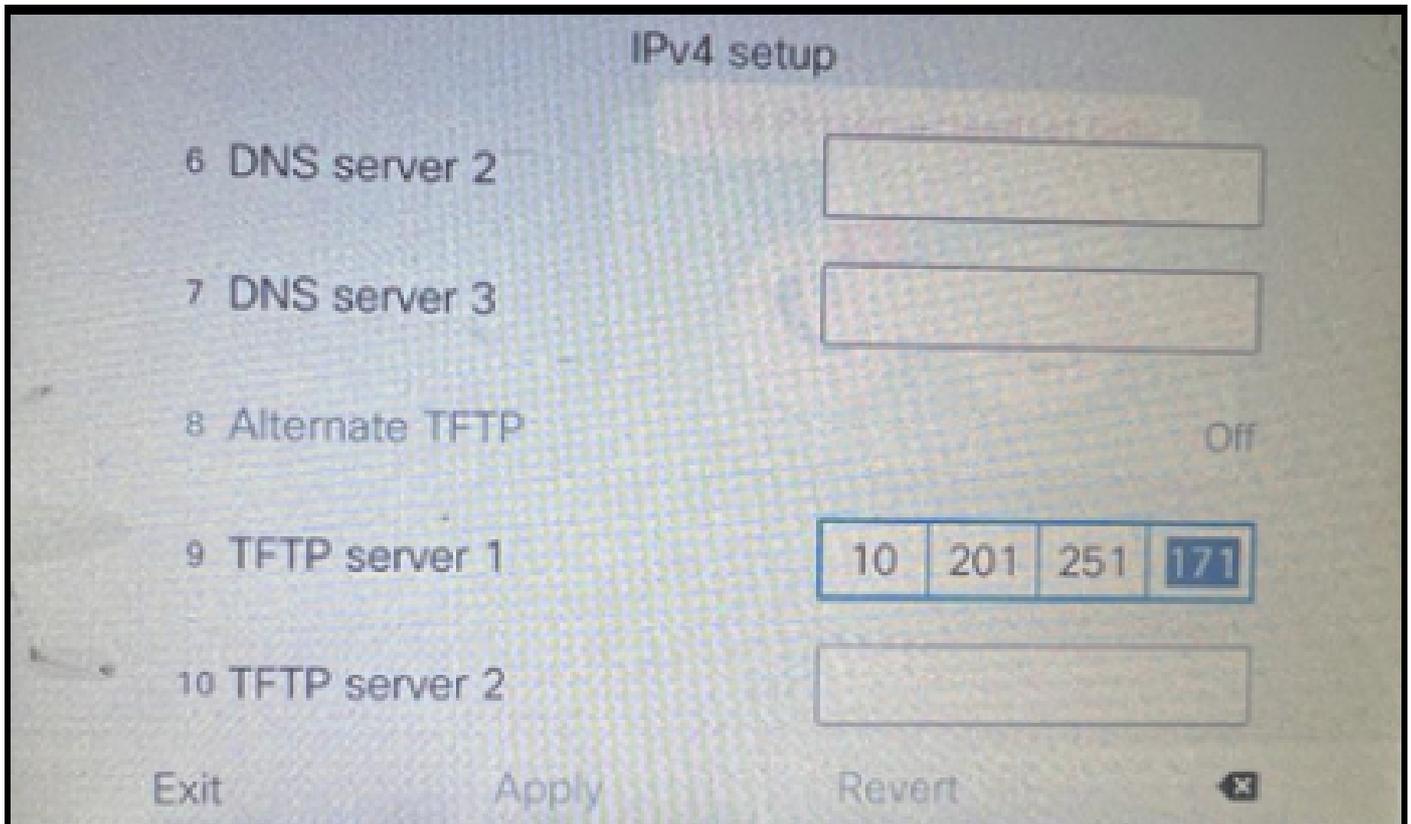
Sur le téléphone physique, accédez à Settings > Admin Settings > Network Setup > Ethernet setup > IPv4 setup.

Désactivez le protocole DHCP et fournissez les détails IP statiques de votre réseau. Ensuite, indiquez l'adresse IP CUCM non sécurisée dans la section TFTP Server 1, comme indiqué dans la capture d'écran.



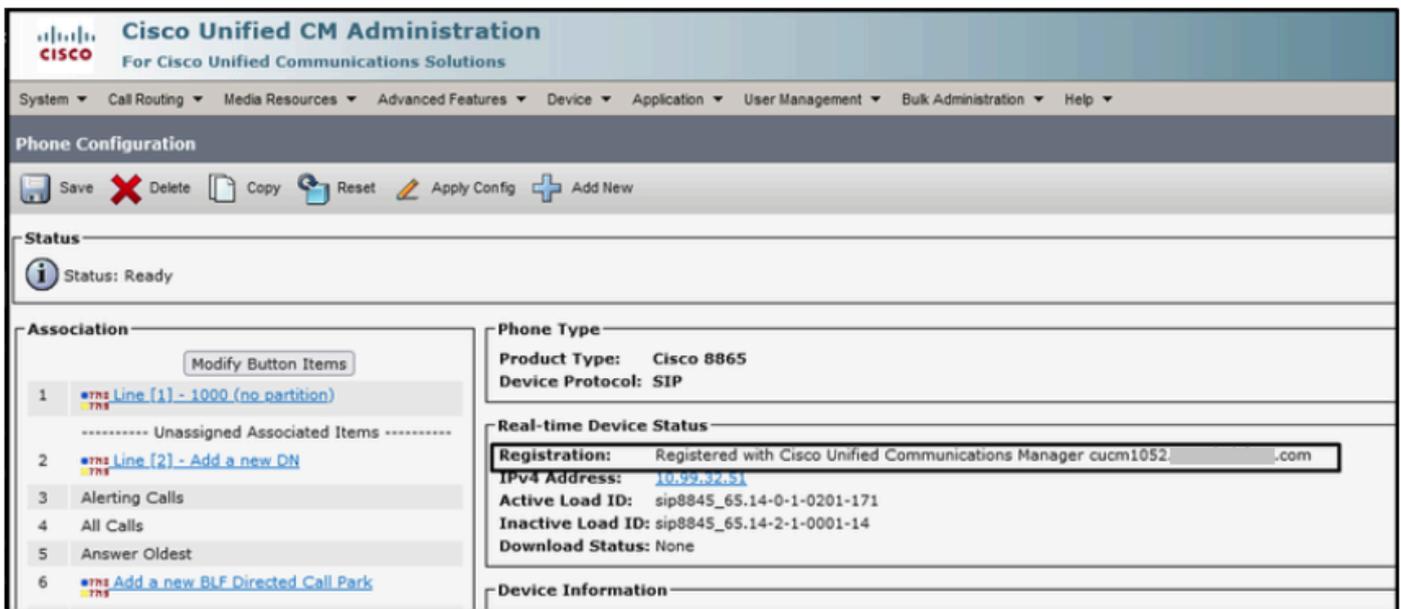
Remarque : ce processus équivaut à modifier l'adresse IP TFTP sur l'étendue DHCP - option 150 / 66. Et si le cluster est configuré avec un nom de domaine, vous devez également définir les serveurs DNS (Domain Name System) appropriés dans l'étendue DHCP.

---



Configuration de l'adresse IP TFTP sur le téléphone

Le téléphone IP s'enregistre auprès du cluster CUCM non sécurisé mentionné.



Téléphone enregistré auprès du CUCM

Connectez-vous à l'interface Web d'administration de CUCM et accédez à System > Enterprise Parameters.

Il s'agit de la valeur des paramètres définie dans la page Enterprise parameter du cluster CUCM non sécurisé.

- Le mode de sécurité du cluster est défini sur 0, ce qui confirme que le cluster n'est pas

sécurisé.



Le mode de sécurité du cluster est défini sur 0

- La valeur de Prepare Cluster for Rollback to pre 8.0 est False. Ainsi, le contenu des fichiers ITL et CTL est conservé avec les valeurs appropriées.



La valeur False est attribuée à l'option Prepare Cluster for Rollback to pre 8.0

Comme le cluster n'est pas sécurisé, il n'y a pas de fichier CTL dans le serveur TFTP. Vous pouvez le vérifier en exécutant la commande show ctl sur la session Secure Shell (SSH) du noeud CUCM.

```
admin:
admin:
admin:show ctl
Length of CTL file: 0
CTL File not found. Please run CTLClient plugin or run the CLI - utils ctl.. to generate the CTL file.
Error parsing the CTL File.
admin:
```

Le fichier CTL est absent

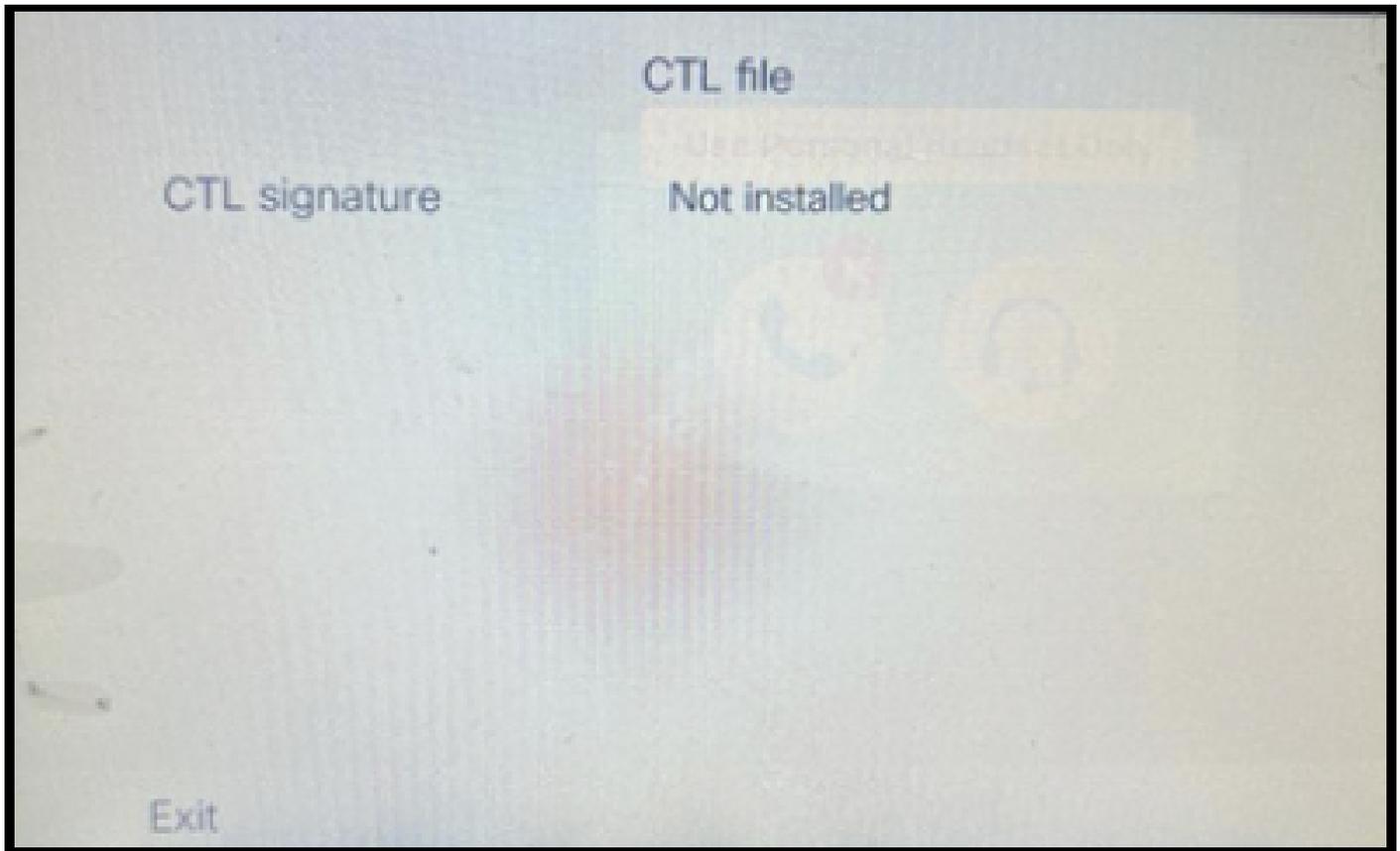
Sur le téléphone physique, vous pouvez vérifier qu'aucun fichier CTL n'est installé. Cependant, vous voyez le fichier ITL.

ITL est présent en raison de la fonctionnalité Sécurité par défaut (SBD) dans le CUCM. Pour plus d'informations sur le SMD, cliquez [ici](#) .

Sur le téléphone physique, accédez à Paramètres > Paramètres d'administration > Configuration de la sécurité > Liste de confiance.

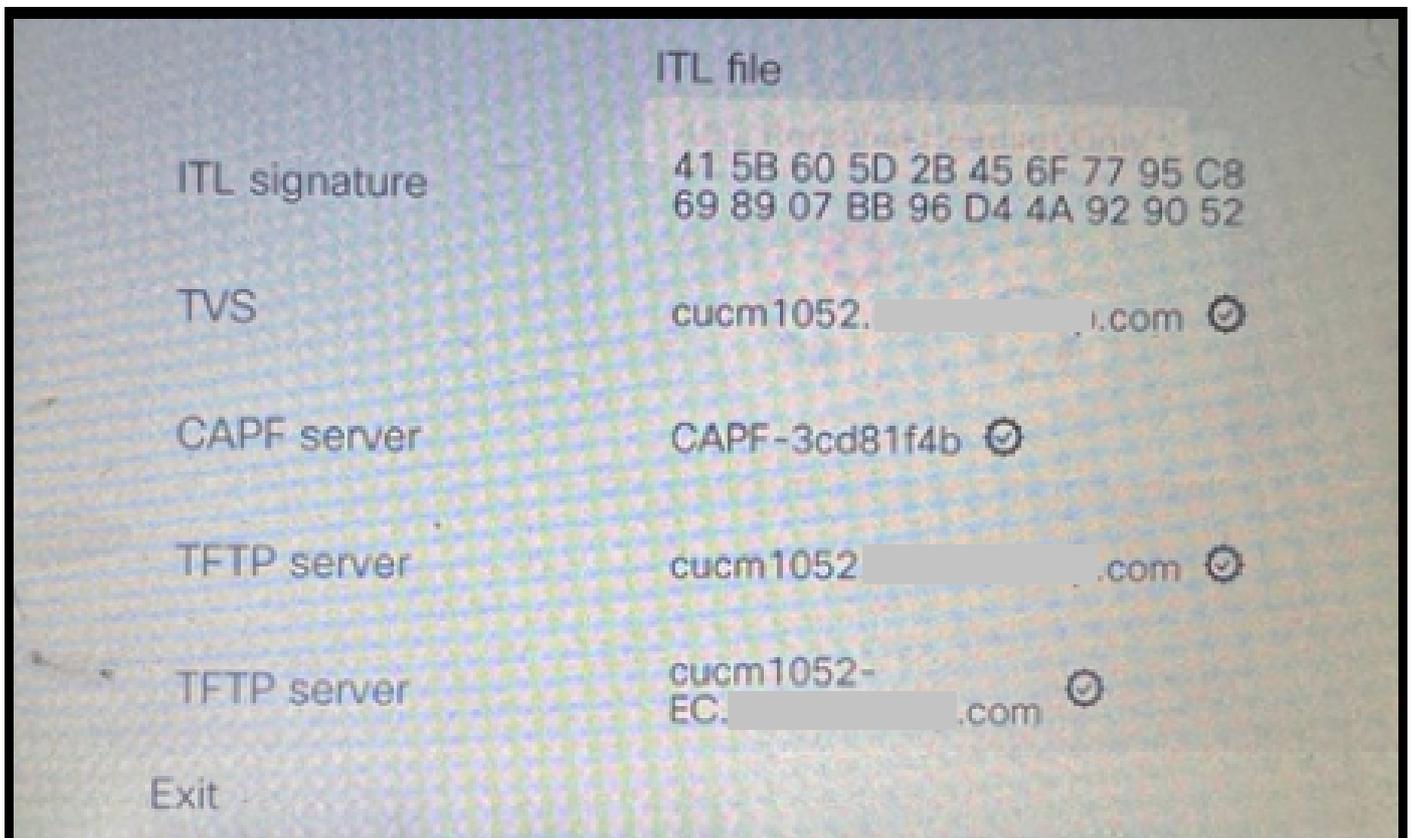
Vous trouverez ici l'état des fichiers CTL et ITL.

CTI n'est pas installé sur le téléphone.



Fichier CTL sur le téléphone

Le téléphone contient le fichier ITL.



Fichier ITL sur le téléphone

## 2. Convertissez un cluster non sécurisé en cluster CUCM sécurisé.

Activez le mode mixte en exécutant la commande `utils ctl set-cluster mixed-mode` sur l'interface de ligne de commande (CLI) du serveur de publication CUCM. Cela permet de convertir le cluster de non sécurisé en cluster sécurisé.

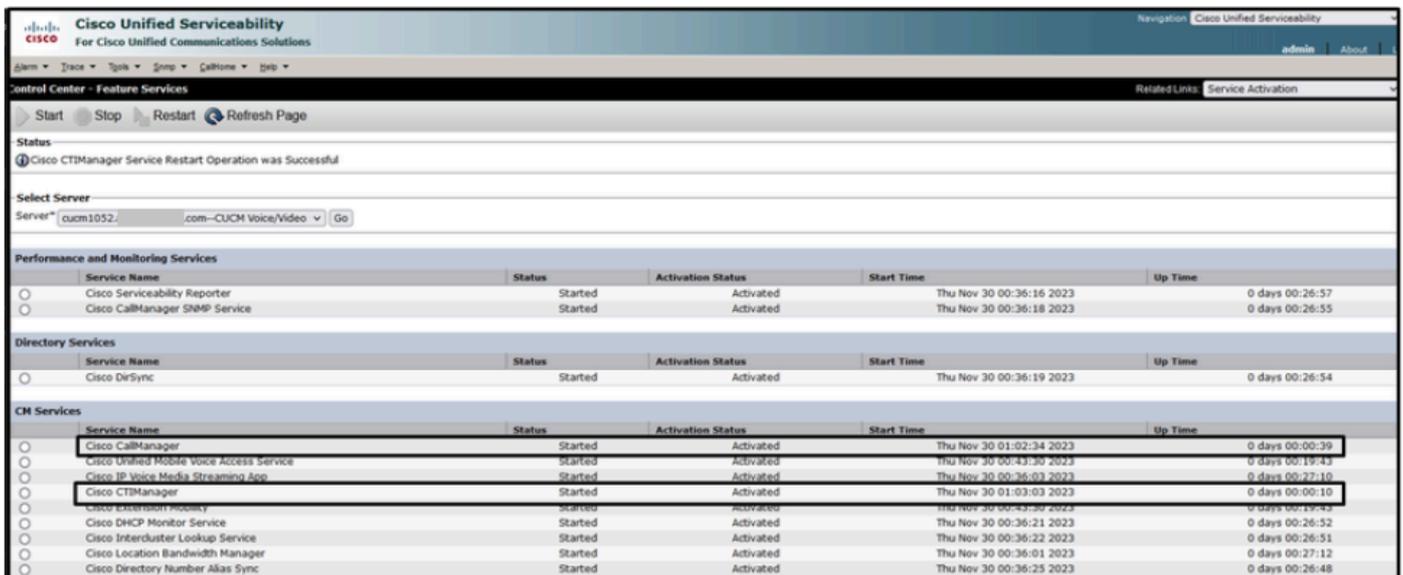
```
admin:
admin:
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.

admin:
admin:
```

Convertir en cluster sécurisé

Après avoir exécuté la commande, redémarrez les services Cisco CallManager (CCM) et Cisco TManager (CTI) sur tous les noeuds du cluster.

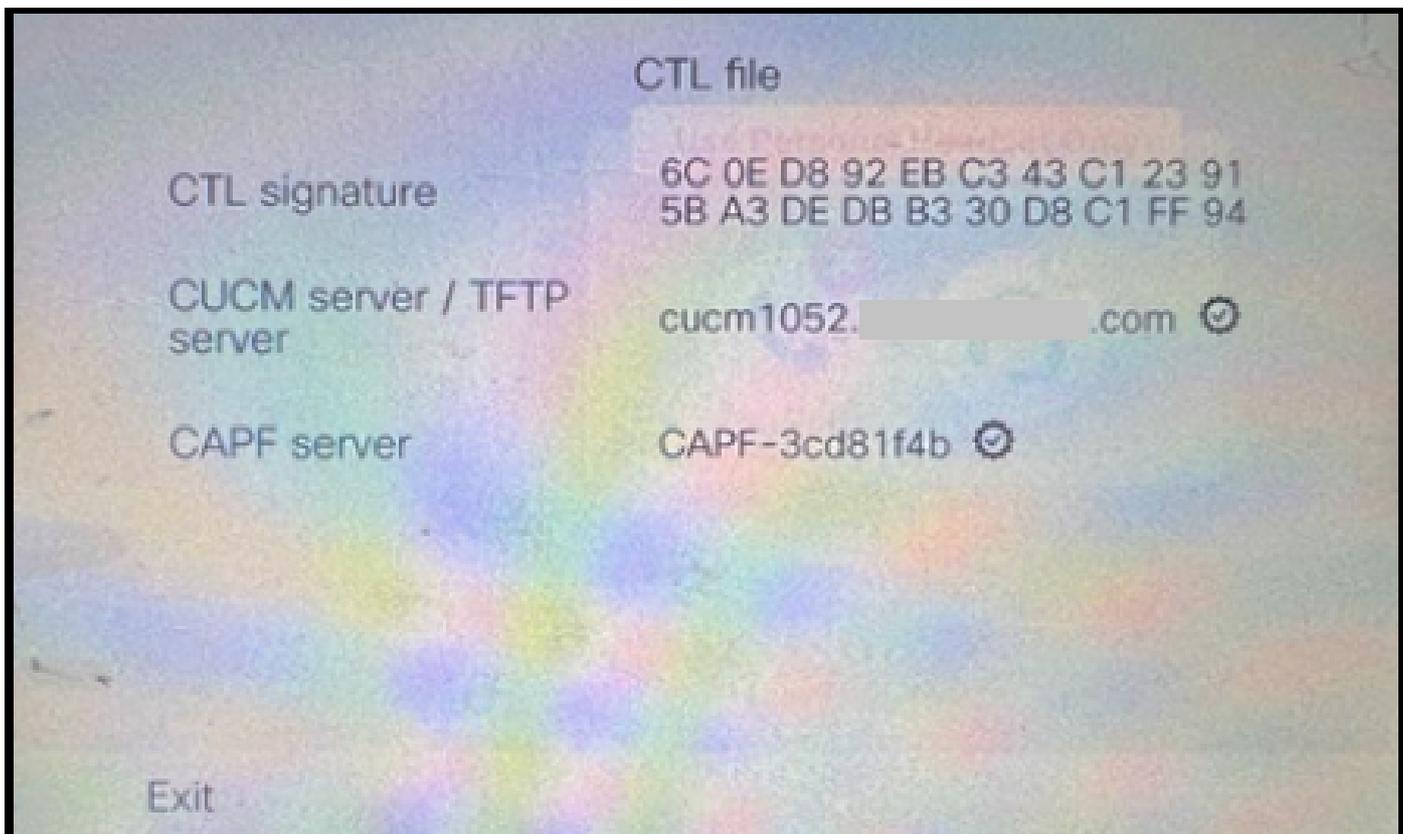


The screenshot shows the Cisco Unified Serviceability interface. At the top, there's a navigation bar with 'Cisco Unified Serviceability' and 'For Cisco Unified Communications Solutions'. Below that, there's a 'Control Center - Feature Services' section with buttons for 'Start', 'Stop', 'Restart', and 'Refresh Page'. A status message indicates 'Cisco CTIManager Service Restart Operation was Successful'. There's a 'Select Server' dropdown menu with 'cucm1052' selected. The main content area displays a table of services, categorized into 'Performance and Monitoring Services', 'Directory Services', and 'CM Services'. The 'CM Services' table is highlighted, showing the following data:

Service Name	Status	Activation Status	Start Time	Up Time
Cisco CallManager	Started	Activated	Thu Nov 30 01:02:34 2023	0 days 00:00:39
Cisco Unified Mobile Voice Access Service	Started	Activated	Thu Nov 30 00:43:30 2023	0 days 00:19:43
Cisco IP Voice Media Streaming App	Started	Activated	Thu Nov 30 00:36:03 2023	0 days 00:27:10
Cisco CTIManager	Started	Activated	Thu Nov 30 01:03:03 2023	0 days 00:00:10
Cisco Extension Mobility	Started	Activated	Thu Nov 30 00:43:30 2023	0 days 00:19:43
Cisco DHCP Monitor Service	Started	Activated	Thu Nov 30 00:36:21 2023	0 days 00:26:52
Cisco Intercluster Lookup Service	Started	Activated	Thu Nov 30 00:36:22 2023	0 days 00:26:51
Cisco Location Bandwidth Manager	Started	Activated	Thu Nov 30 00:36:01 2023	0 days 00:27:12
Cisco Directory Number Alias Sync	Started	Activated	Thu Nov 30 00:36:25 2023	0 days 00:26:48

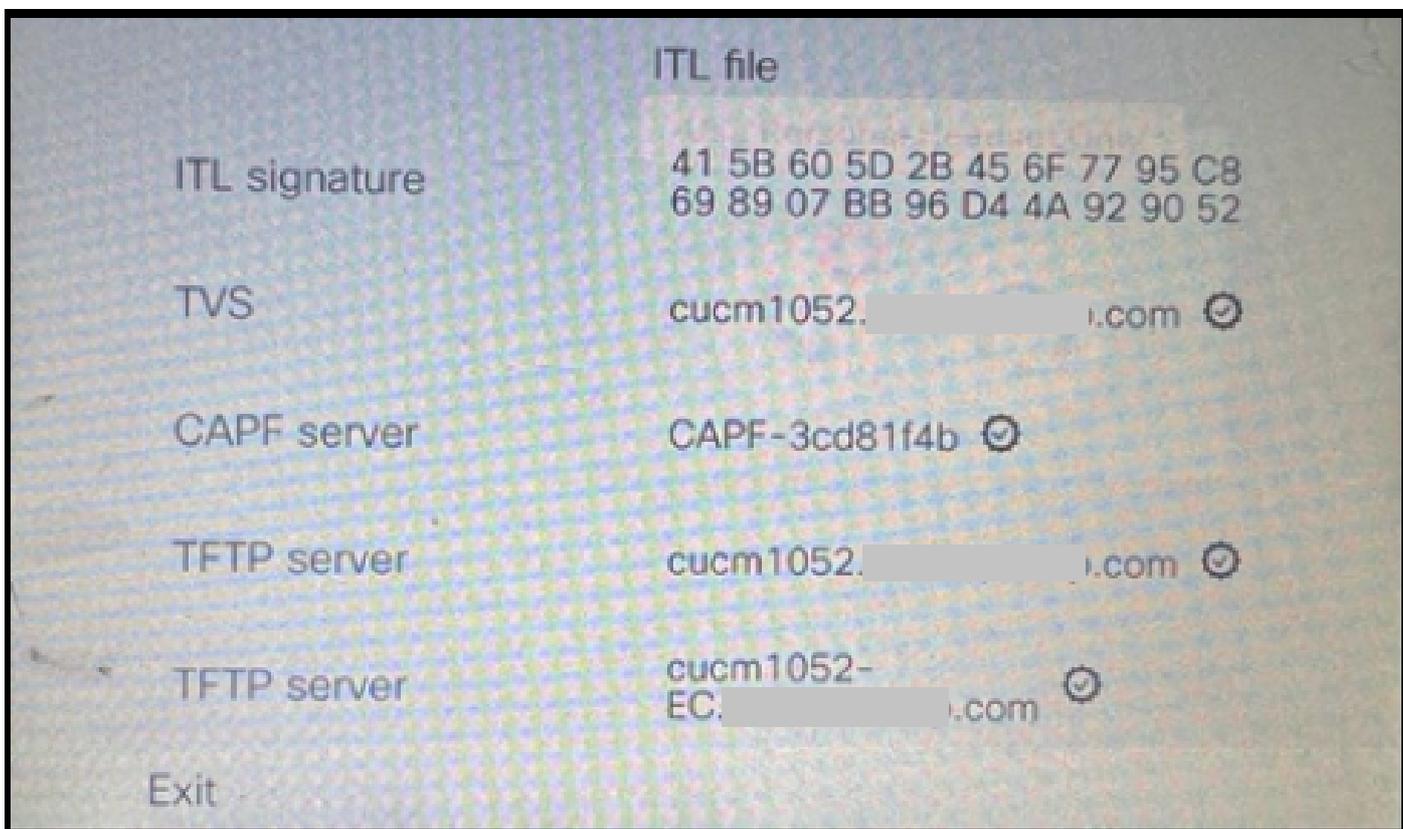
Redémarrez les services CCM et CTI

Maintenant, sur le téléphone physique, vous pouvez voir la présence du fichier CTL.



Fichier CTL sur le téléphone

Le fichier ITL a conservé les mêmes valeurs.



Fichier ITL sur le téléphone

3. Convertissez de nouveau en cluster non sécurisé à partir de sécurisé.

Afin de convertir le cluster de sécurisé en non-sécurisé, vous devez exécuter la commande `utils ctl set-cluster non-secure-mode` sur l'interface de ligne de commande du serveur de publication CUCM.

```
admin:
admin:utils ctl set-cluster non-secure-mode
This operation will set the cluster to non secure mode. Do you want to continue? (y/n): y

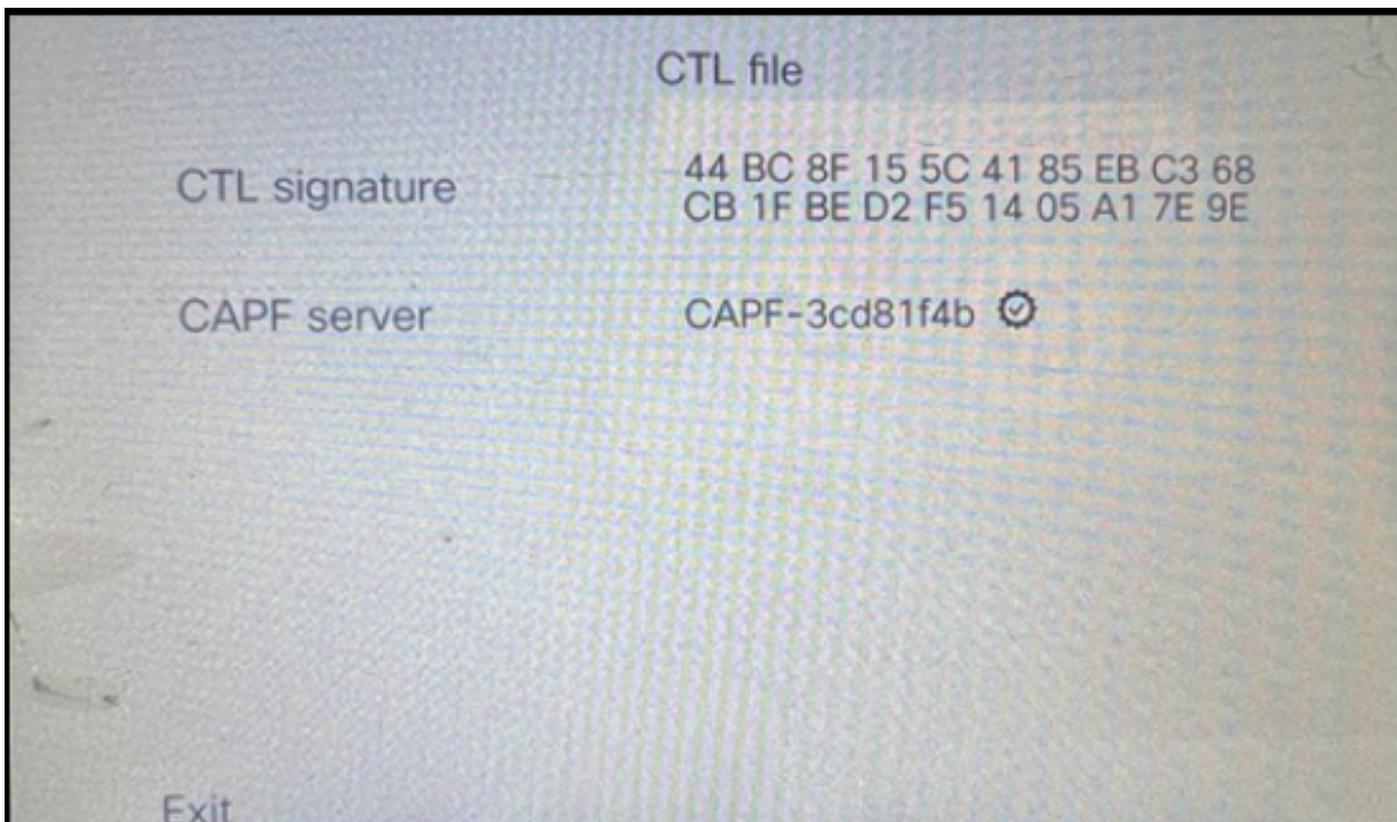
Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.

admin:
admin:
```

Convertir en cluster non sécurisé

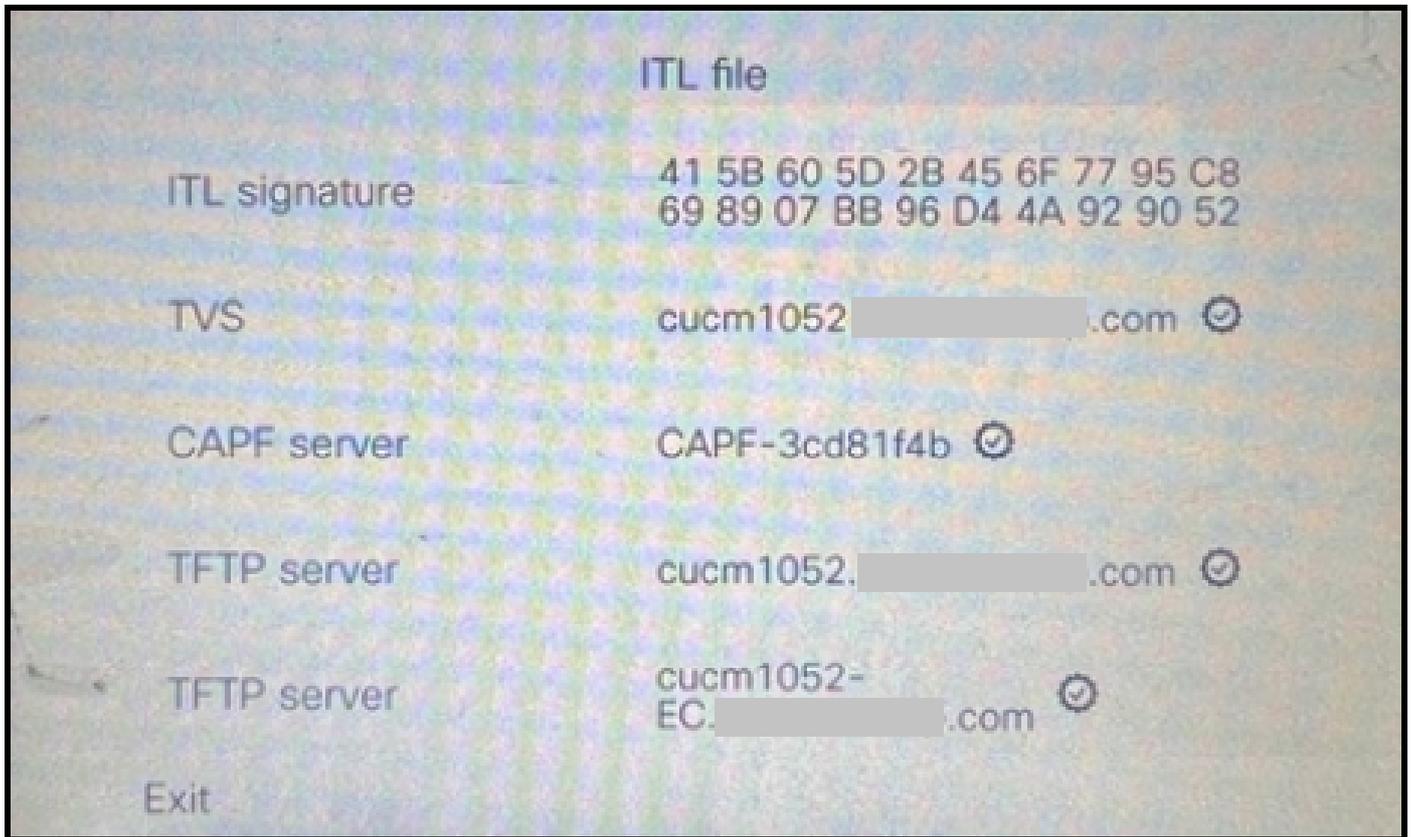
Redémarrez les services CCM et CTI sur tous les noeuds du cluster pour effectuer la modification afin qu'elle s'applique à tous les noeuds du cluster CUCM.

Après avoir converti le cluster en non sécurisé, la CTL ne contient pas les entrées CUCM et TFTP. Le fichier CTL contient uniquement l'entrée CAPF.



Fichier CTL sur le téléphone

Le fichier ITL est resté avec les mêmes entrées.



Fichier ITL sur le téléphone



Remarque : la modification du profil de sécurité du périphérique dans la page de configuration du téléphone (dans la page Web d'administration de CUCM) en mode sécurisé ou non sécurisé n'a aucun effet sur les fichiers ITL ou CTL. Ainsi, vous pouvez garder le réglage comme il était avant et pas besoin de les modifier.

---

4. Faites migrer le téléphone vers un nouveau cluster CUCM non sécurisé.



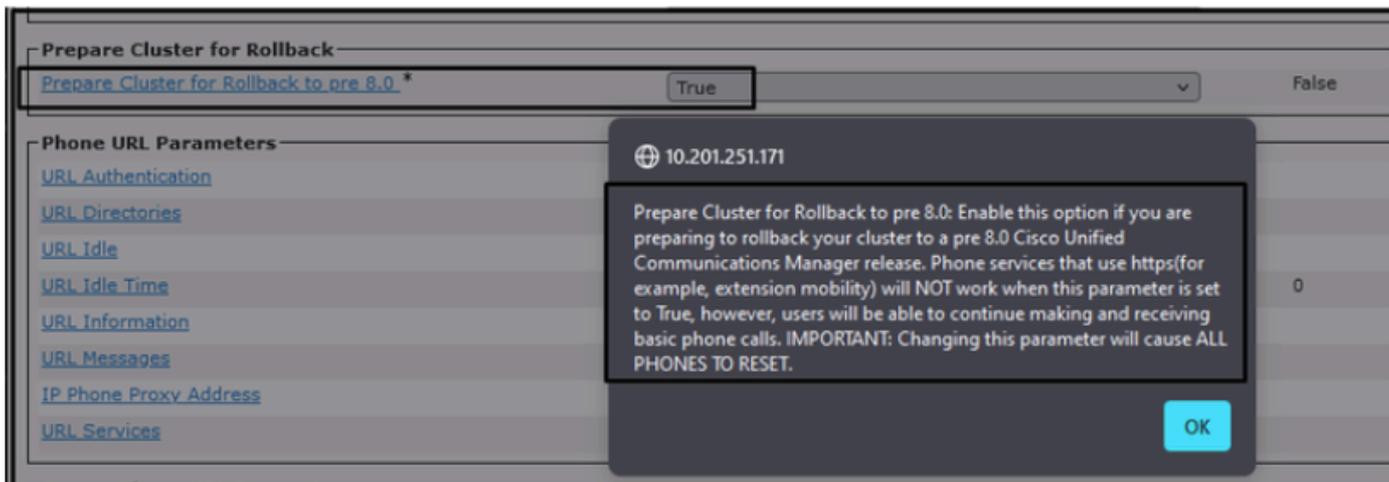
Remarque : avant de poursuivre la migration, il est recommandé de redémarrer le service de vérification de la confiance (TVS) et les services TFTP sur tous les noeuds (uniquement sur ces noeuds activés pour les services) du cluster source. Cela élimine toute session bloquée ou de fuite dans le service TVS / TFTP.

---

Connectez-vous à l'interface Web d'administration de CUCM et accédez à System > Enterprise Parameters.

Définissez la valeur de Prepare Cluster for Rollback sur pre 8.0 sur True. Cliquez ensuite sur les boutons Apply Config et Reset.

La section d'aide de ce paramètre est fournie dans cette capture d'écran.

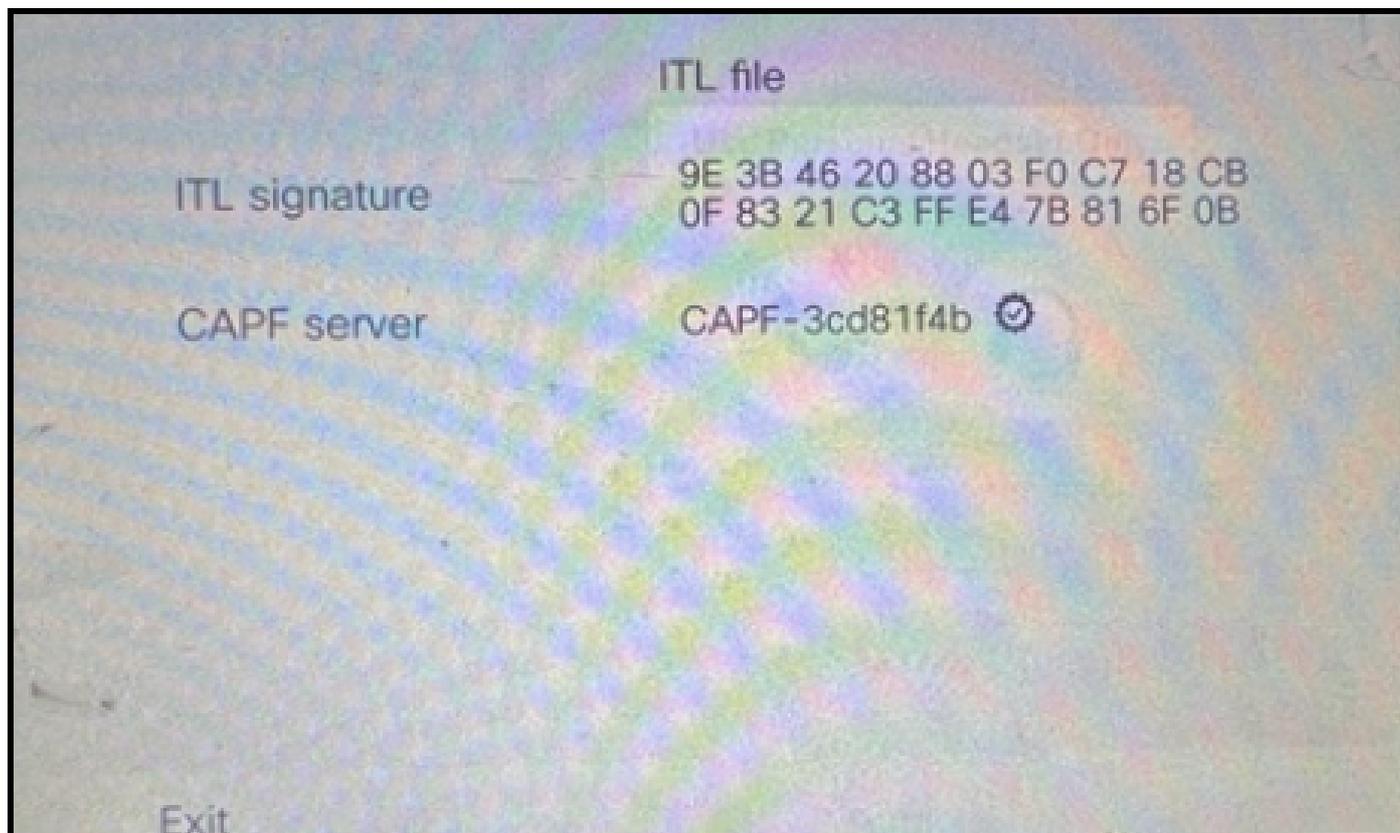


Informations sur le paramètre Préparer le cluster pour la restauration vers la version antérieure à 8.0

Surveillez le nombre d'enregistrements téléphoniques sur le cluster (via l'outil de surveillance en temps réel - RTMT) avant et après la modification de la valeur du paramètre. Cette méthode permet de valider si ces modifications sont appliquées à tous les périphériques du cluster ou non.

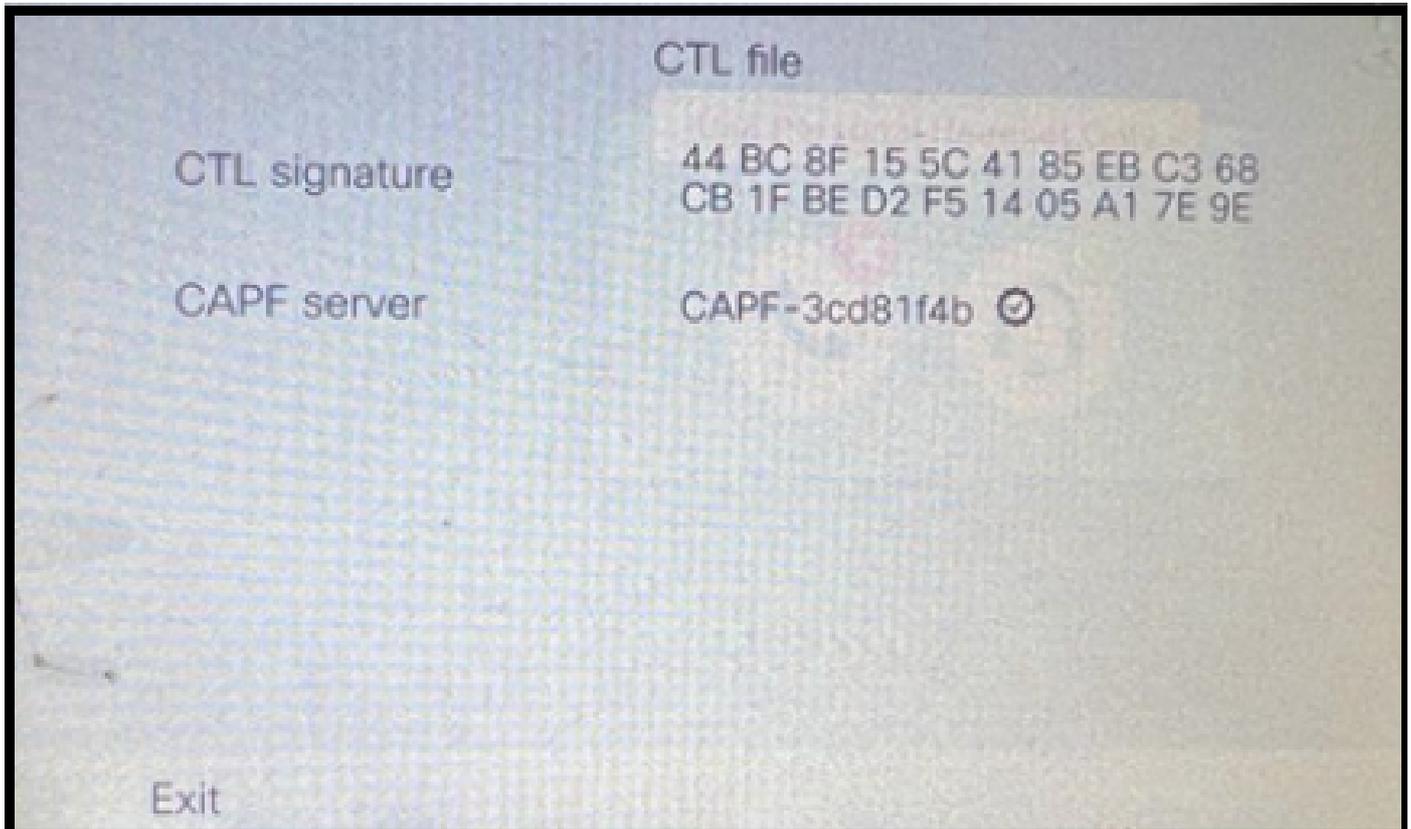
Sur le téléphone physique, seules les entrées CAPF étaient visibles dans les fichiers ITL et CTL. Vous pouvez également l'observer en ouvrant la page Web du téléphone dans le navigateur Web.

Fichier ITL



Fichier ITL sur le téléphone

Fichier CTL



Fichier CTL sur le téléphone

Avant de commencer la migration, il est judicieux de valider les fichiers ITL et CTL sur quelques téléphones pour vérifier que les modifications ont bien été effectuées.

Les téléphones sont maintenant prêts pour la migration.

Migration des téléphones du cluster source vers le cluster de destination. Actuellement, les deux clusters ne sont pas sécurisés.

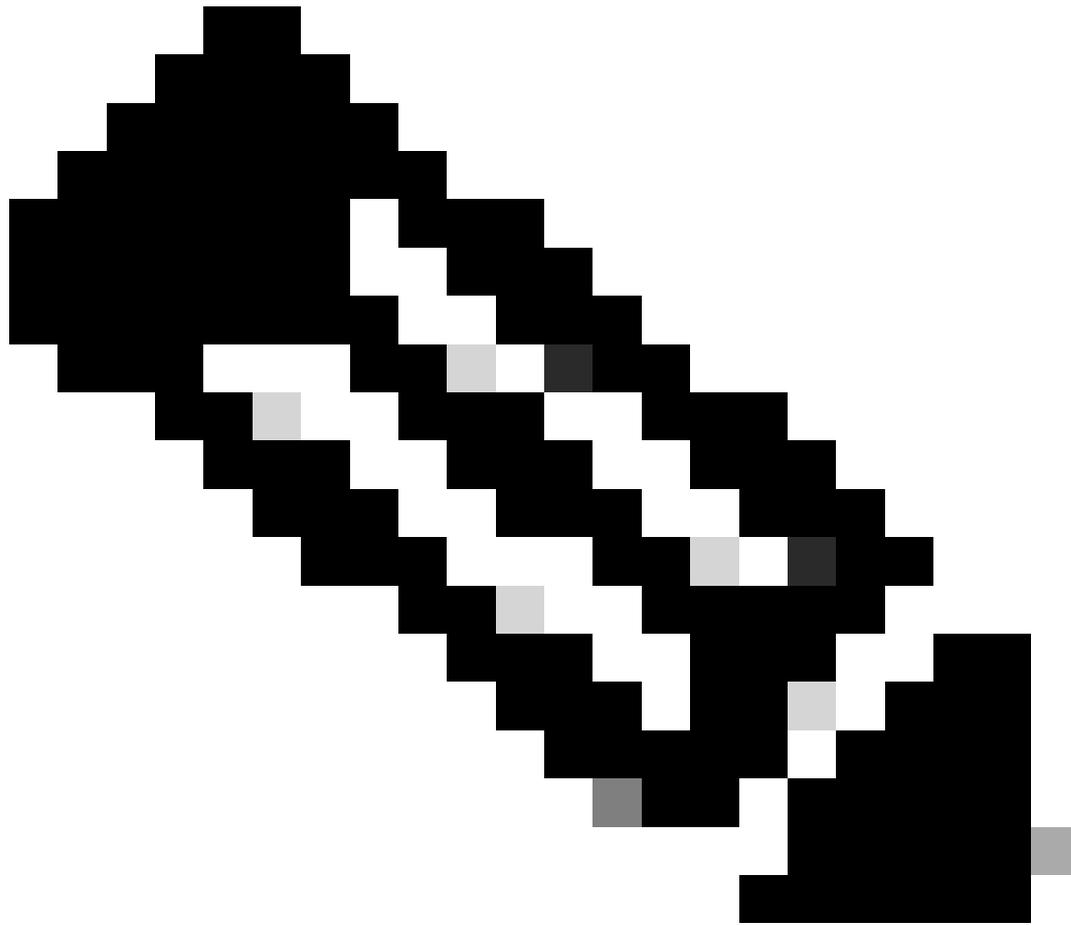
Cluster source :

- Adresse IP : 10.201.251.171
- FQDN - cucm1052.domain.com
- Version : 12.5.1.16065-1

Cluster de destination :

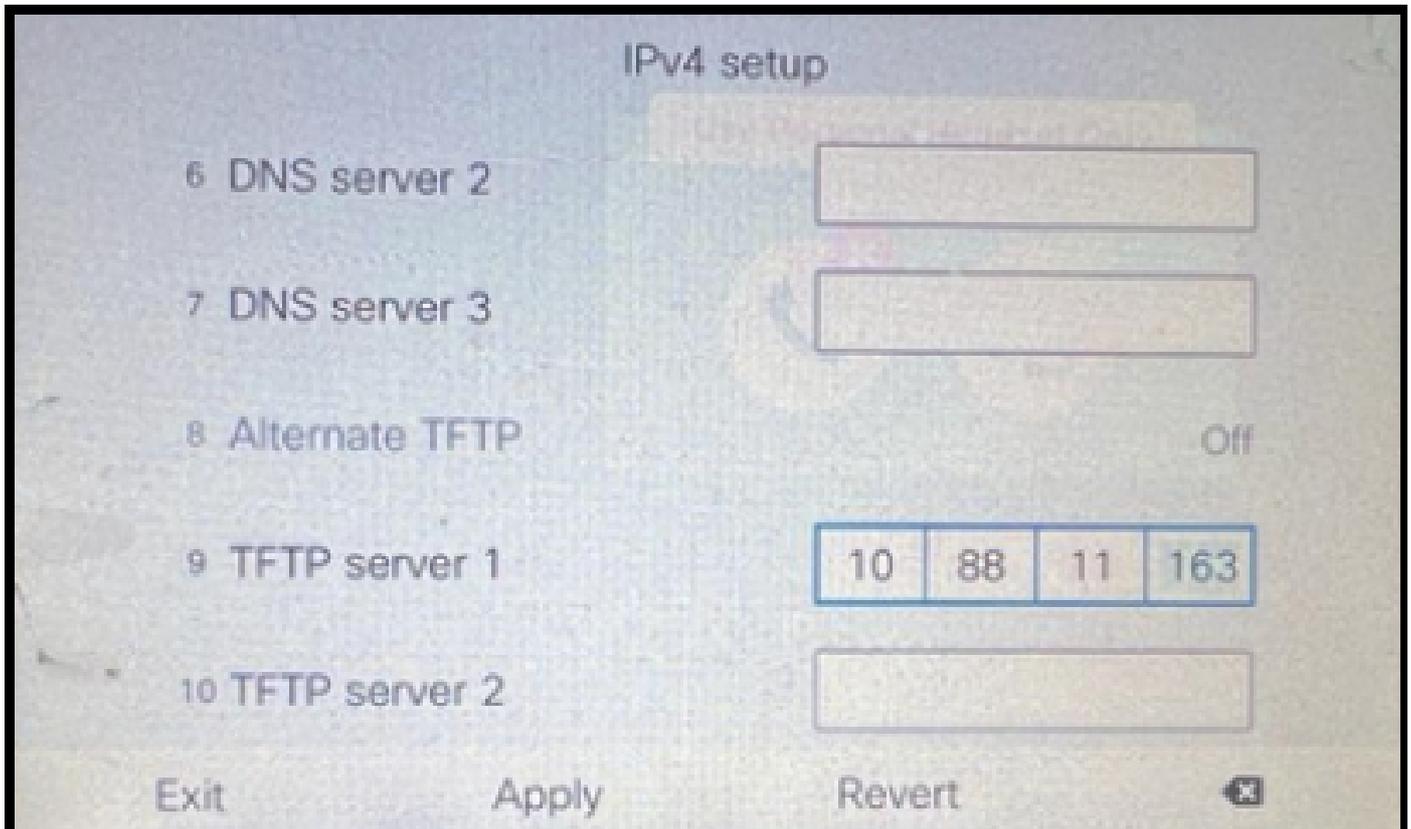
- Adresse IP : 10.88.11.163
- FQDN - cucmpub.domain.com
- Version : 12.5.1.14900-63

Sur le téléphone physique, définissez la valeur TFTP Server 1 sur Destination new cluster IP address et cliquez sur le bouton Apply.



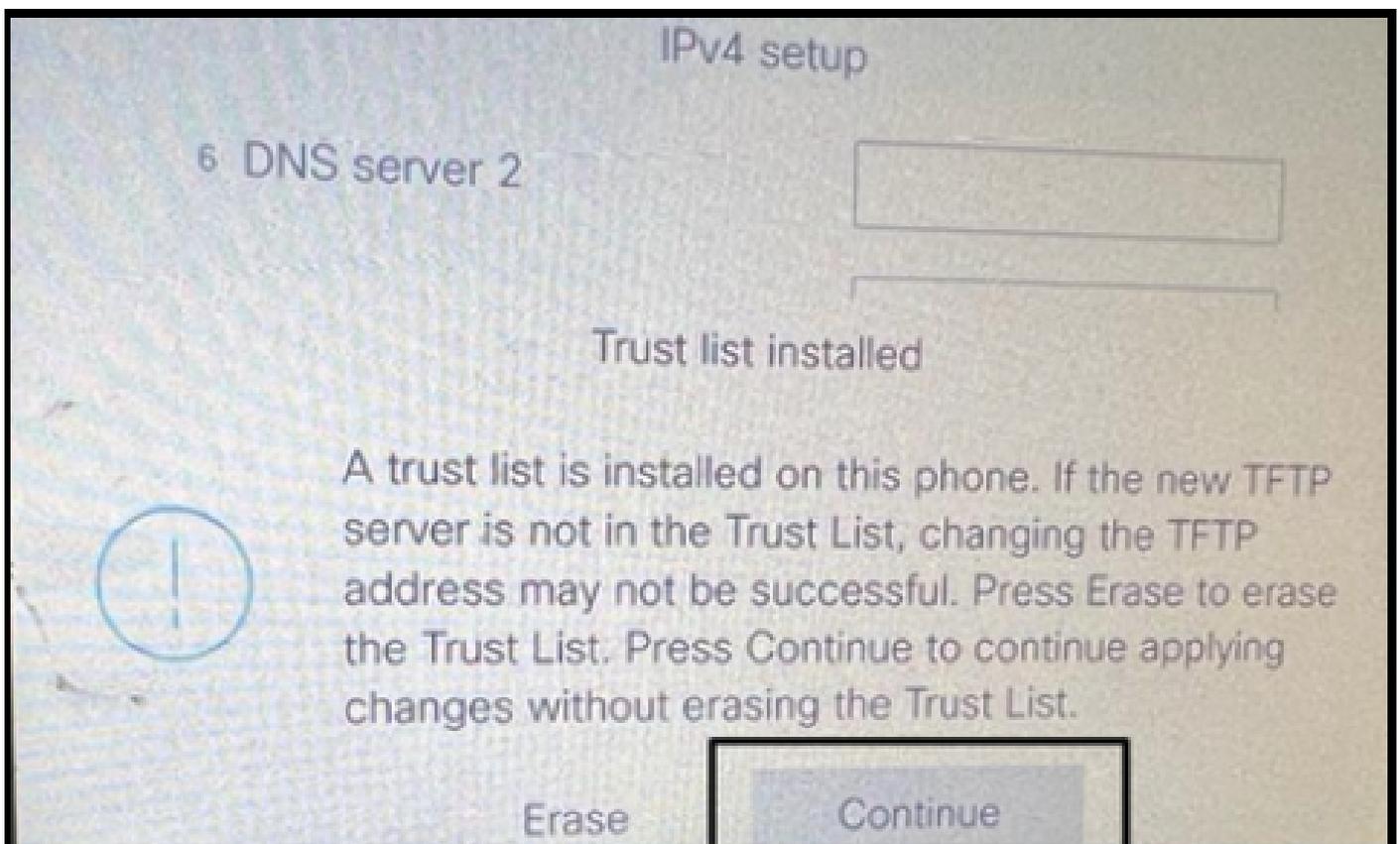
Remarque : ce processus équivaut à modifier l'adresse IP TFTP sur l'étendue DHCP - option 150 / 66. Si le cluster de destination se trouve dans un autre domaine, vous devez également définir les serveurs DNS appropriés dans l'étendue DHCP.

---



Configuration de l'adresse IP TFTP sur le téléphone

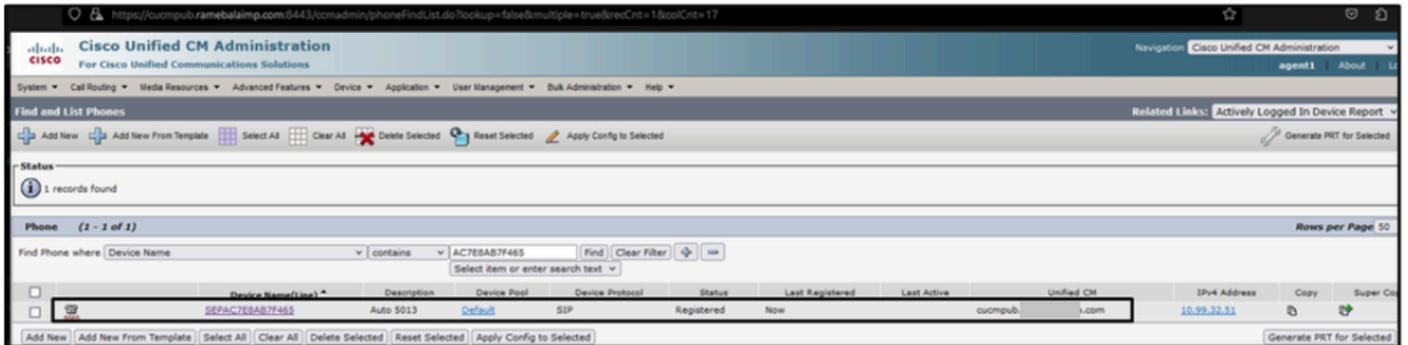
Cliquez sur le bouton Continue, cela conserve les anciens fichiers CTL et ITL (contient uniquement l'entrée CAPF) du cluster source.



Appuyez sur le bouton Continuer pour conserver les anciens fichiers CTL et ITL

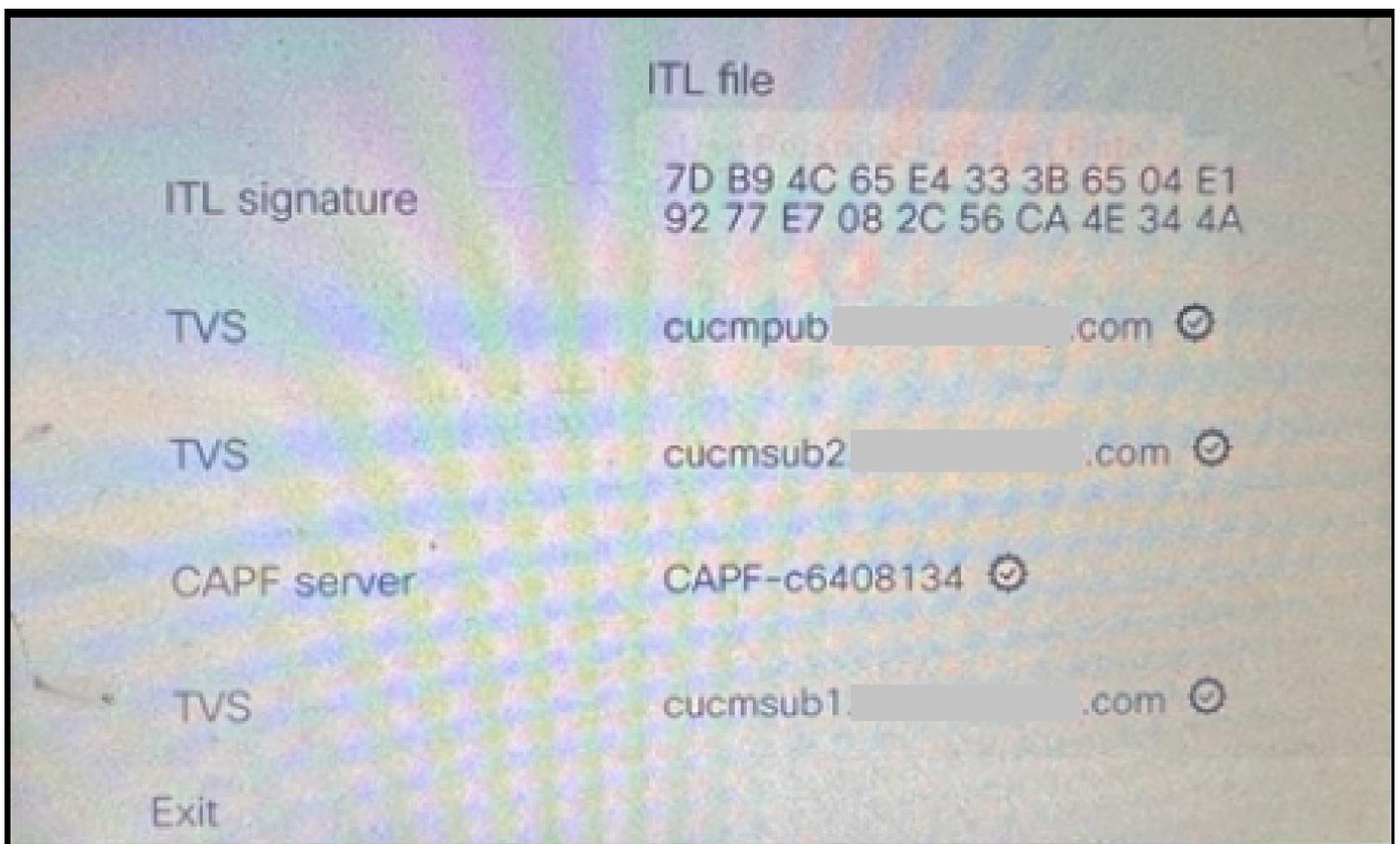
# Vérifier

Le téléphone est correctement enregistré dans le cluster de destination.



Téléphone enregistré auprès du CUCM

Le téléphone contient les entrées de la liste de confiance du cluster de destinations.



Fichier ITL sur le téléphone

# Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

# Informations connexes

- [Comprendre la sécurité CUCM par défaut et le fonctionnement et le dépannage ITL](#)
- [CUCM mode mixte avec CTL sans jeton](#)
- [Guide de sécurité pour Cisco Unified Communications Manager, version 12.5\(1\)](#)
- [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.