

Demonstreer IP-telefoonmigratie van beveiligde naar niet-beveiligde CUCM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft een van de best practices voor het migreren van telefoons van beveiligde Cisco Unified Communications Manager (CUCM) naar een niet-beveiligde CUCM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM
- IP-telefoon 7811

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- CUCM-versies - 12.5.1.16065-1 en 12.5.1.14900-63
- IP-telefoon model - 8865 en versie - 12.8(1)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdigram

IP_telefoon > Cisco Switch > Cisco router > Cisco Switch > CUCM Cluster

Configuraties

Deze scenario's verklaren de telefoonmigratie van veilig naar niet-veilig CUCM-cluster. Tijdens elke fase wordt de status van CTL-bestanden (Certificate Trust List) en ITL-bestanden (Identity Trust List) op de telefoon gedocumenteerd.

1. Registreer een telefoon naar een niet-beveiligde CUCM-cluster.
2. Converteer een niet-beveiligde cluster naar een beveiligd CUCM-cluster.
3. Terug naar niet-beveiligde cluster converteren vanuit beveiligd
4. Migreer de telefoon naar een nieuwe niet-beveiligde CUCM-cluster.

1. Registreer een telefoon naar een niet-beveiligde CUCM-cluster.

Dit is de informatie over het niet-beveiligde broncluster.

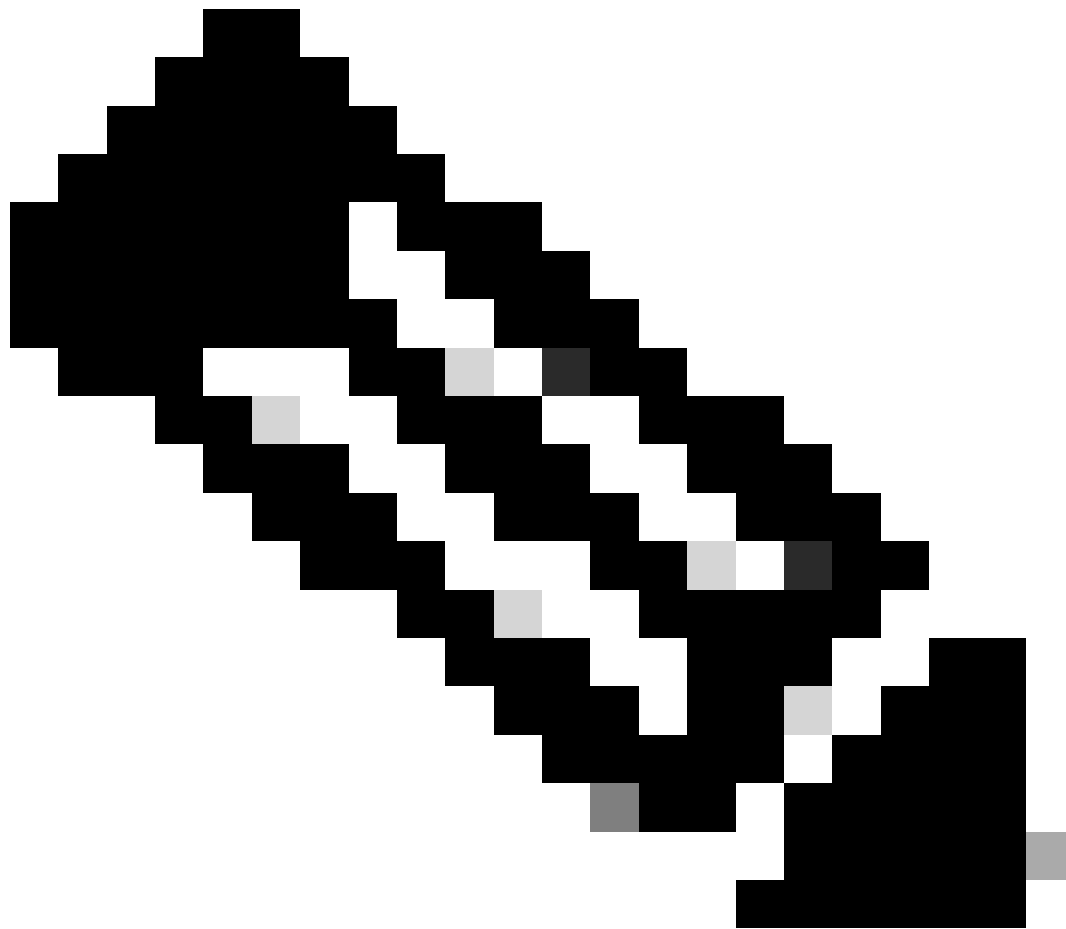
- IP-adres - 10.201.251.171
- FQDN - cucm1052.domain.com
- Versie: 12.5.1.16065-1

Registreer een telefoon naar een niet-beveiligde CUCM-cluster. Hiervoor configureer je Dynamic Host Configuration Protocol (DHCP) optie 150/66 om naar het Trivial File Transfer Protocol (TFTP) IP-adres te wijzen (dit zou de CUCM-knooppunt zijn waar de TFTP-service is ingeschakeld).

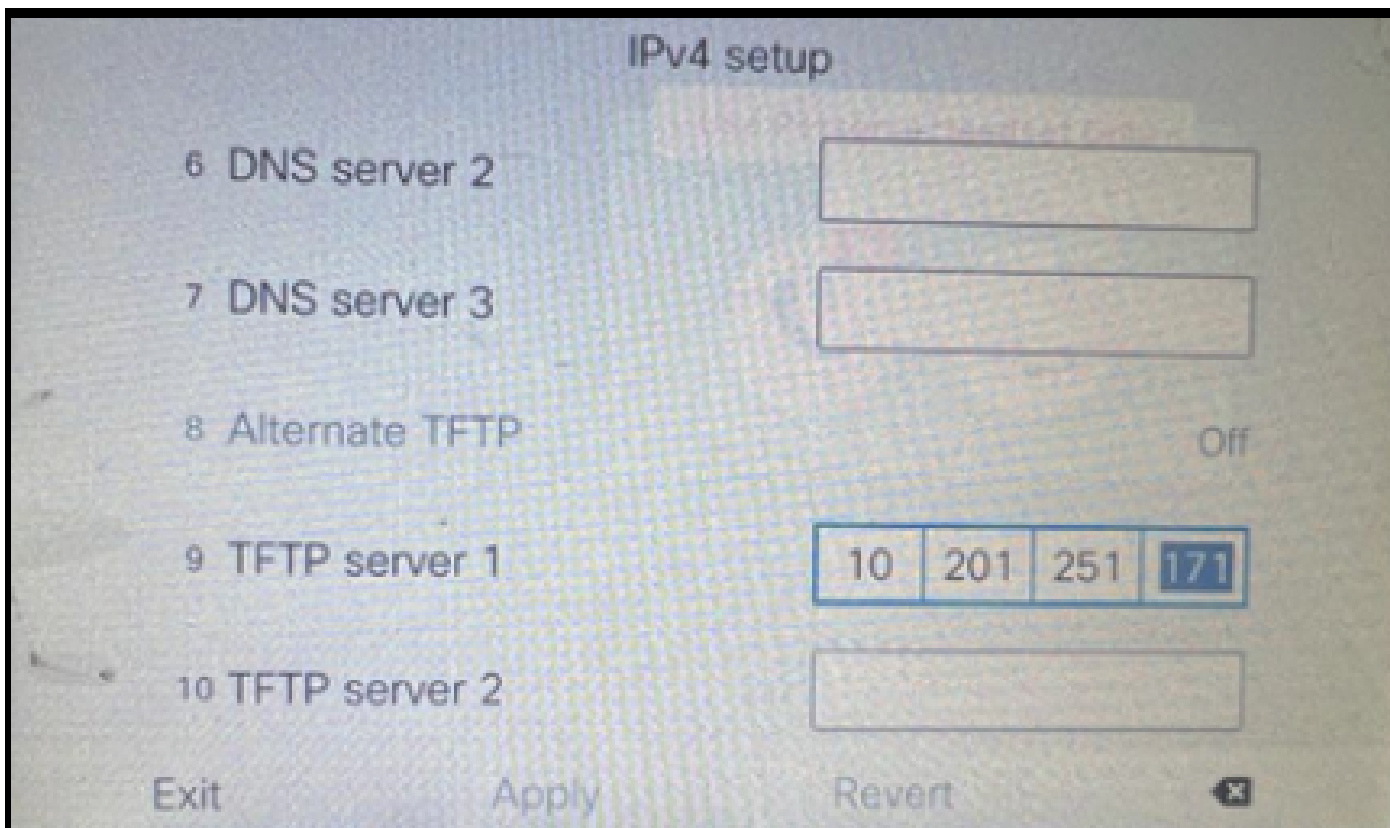
Voor de infrastructuur waar u niet de DHCP-servers hebt, moet u TFTP IP handmatig op de fysieke telefoon configureren.

Ga op de fysieke telefoon naar Instellingen > Beheerinstellingen > Netwerkinstallatie > Ethernet-instelling > IPv4-installatie.

Schakel DHCP uit en geef statische IP-gegevens over uw netwerk op. Daarna, verstrek niet-beveiligde CUCM IP in TFTP Server 1 sectie zoals getoond in het schermshot.

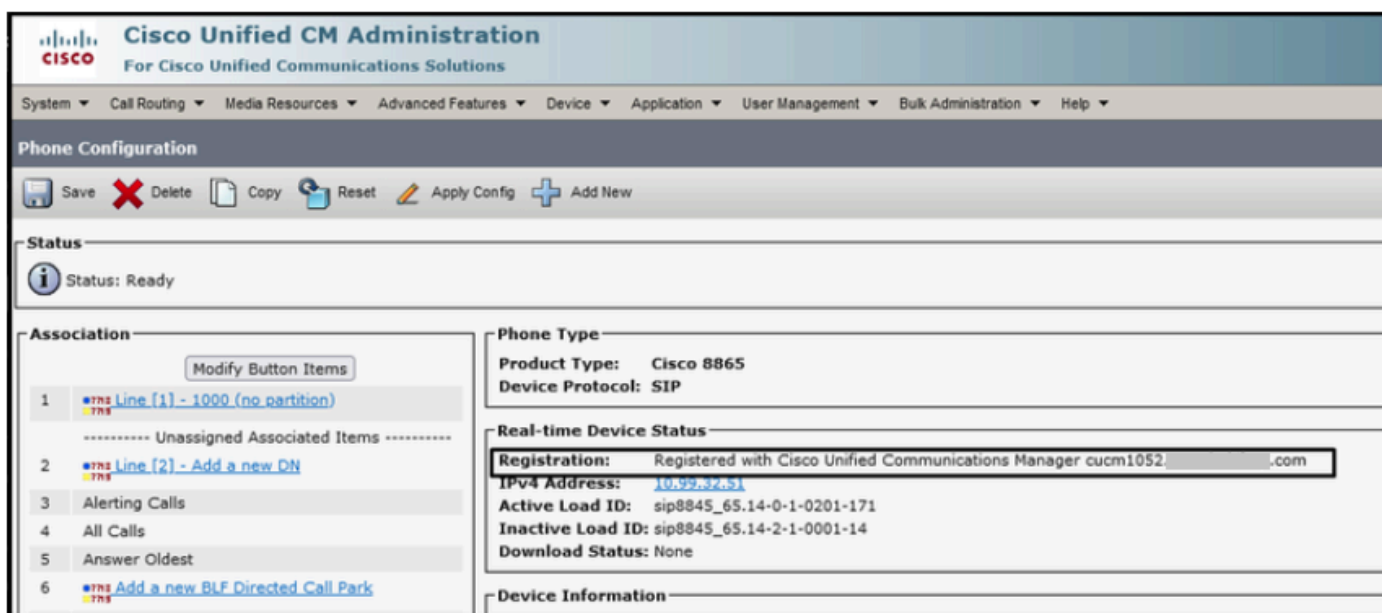


Opmerking: dit proces staat gelijk aan het wijzigen van het TFTP IP in de DHCP-scope - optie 150/66. En als de cluster is geconfigureerd met de domeinnaam, moet u ook de juiste Domain Name System (DNS)-servers instellen in de DHCP-scope.



Configureer TFTP IP op de telefoon

De IP-telefoon krijgt register naar de genoemde niet-beveiligde CUCM-cluster met succes.

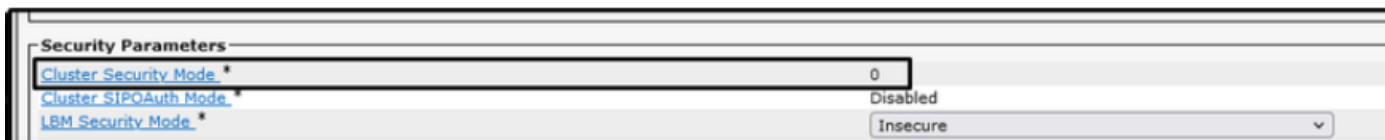


Telefoon geregistreerd bij de CUCM

Meld u aan bij de CUCM-webinterface voor beheer en navigeer naar System > Enterprise Parameters.

Dit zijn de parameters'-waarden die zijn ingesteld onder de Enterprise-parameterpagina van het niet-beveiligde CUCM-cluster.

- Cluster security Mode is ingesteld op 0, dit bevestigt dat het cluster niet veilig is.



De modus Cluster Security is ingesteld op 0

- Bereid Cluster voor op Rollback naar pre 8.0 is ingesteld als False. De inhoud van de ITL & CTL-bestanden blijft dus behouden met de juiste waarden.



Klaarmaken Cluster voor teruggedraaien naar pre 8.0 is ingesteld als onwaar

Aangezien de cluster niet veilig is, is er geen CTL-bestand op de TFTP-server. U kunt dit verifiëren door de opdracht `ctl` op de Secure Shell (SSH)-sessie van de CUCM-knooppunt uit te voeren.

```
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:
```

CTL-bestand is niet aanwezig

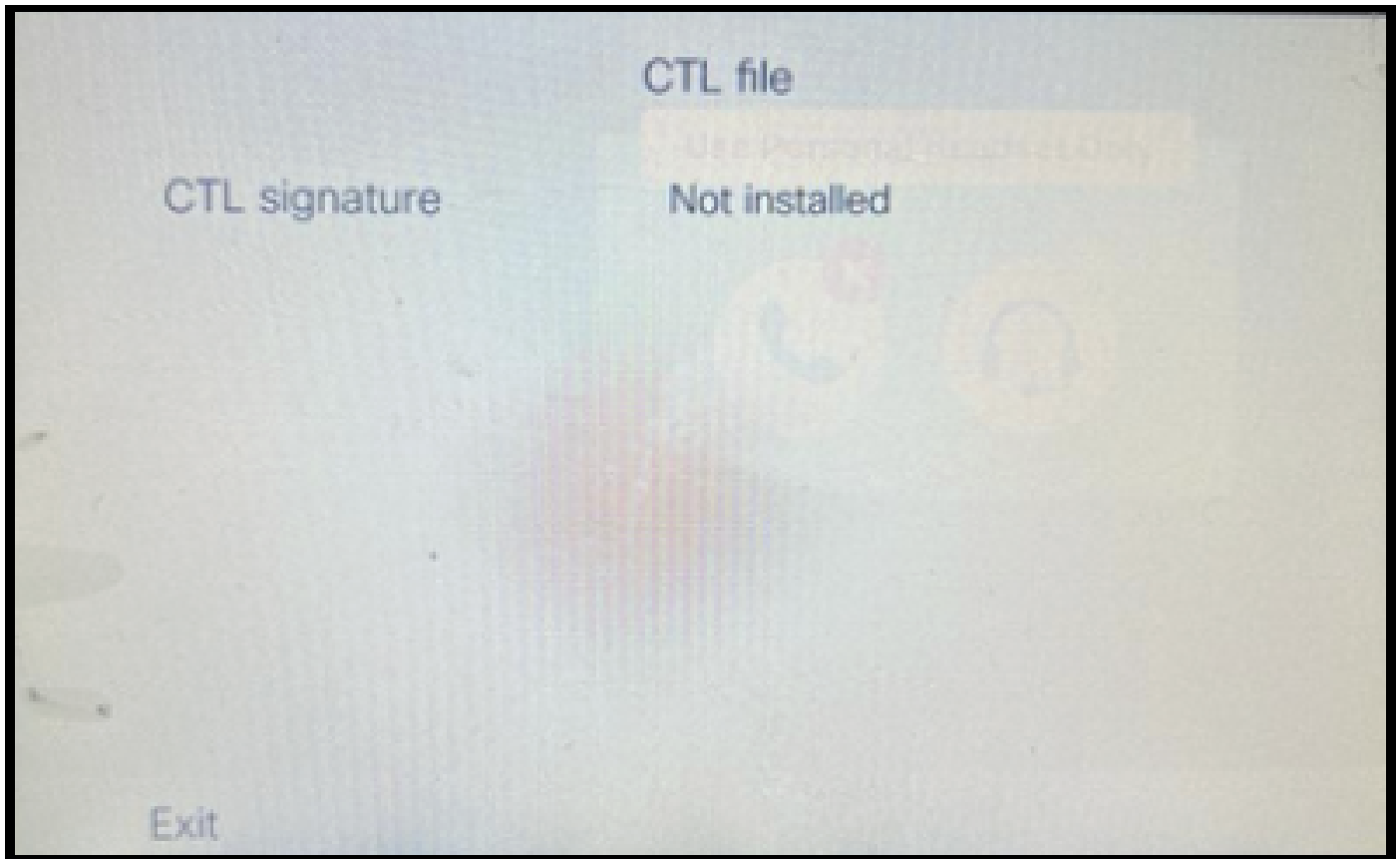
Op de fysieke telefoon, kunt u bevestigen dat er geen CTL-bestand geïnstalleerd is. U ziet echter het ITL-bestand.

ITL is aanwezig vanwege de optie Security by Default (SBD) in de CUCM. Voor meer informatie over SBD, gelieve te klikken [hier](#).

Navigeer op de fysieke telefoon naar Instellingen > Beheer instellingen > Beveiligingsinstellingen > Vertrouwenlijst.

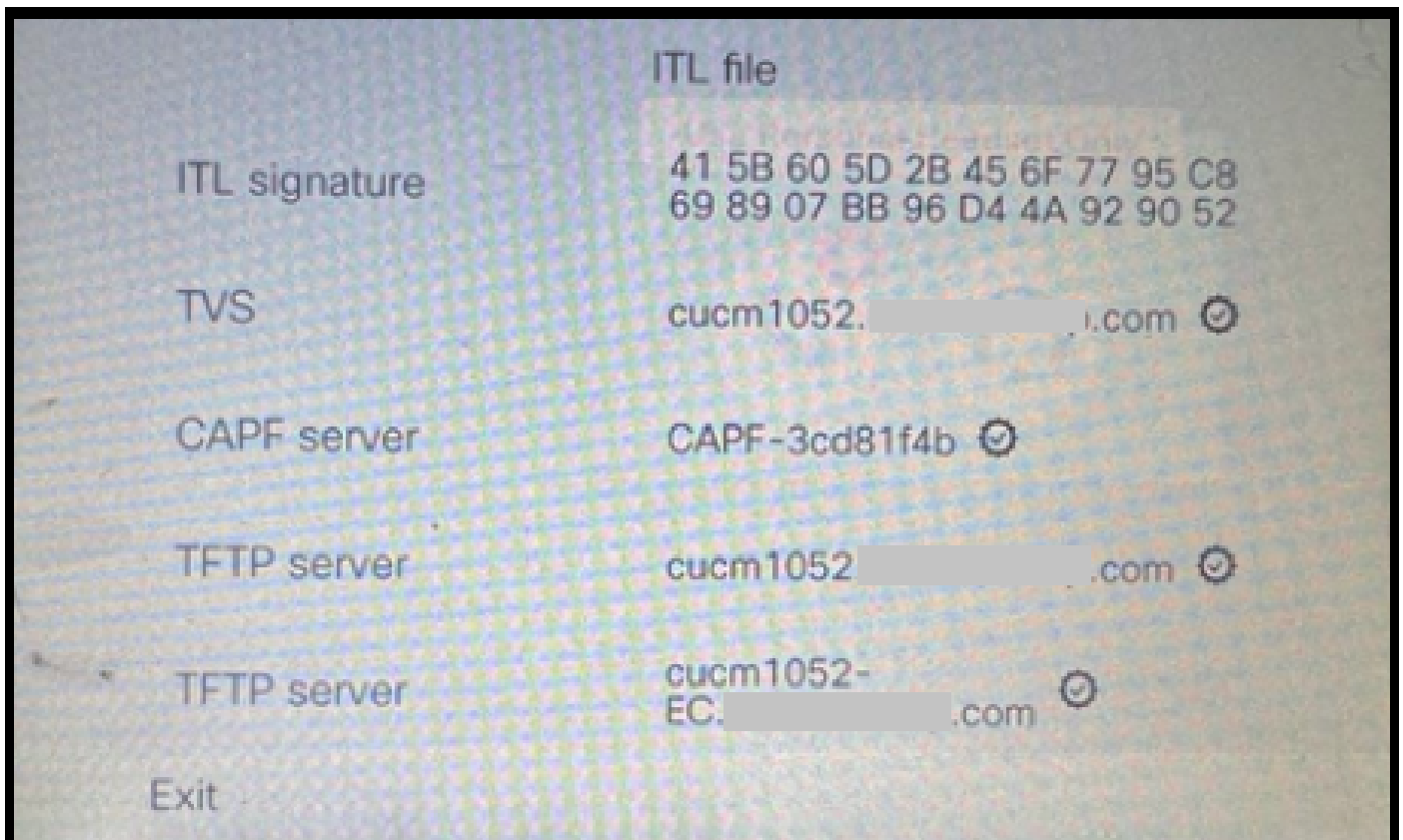
Hier kunt u de status van zowel de CTL- als de ITL-bestanden vinden.

CTI is niet geïnstalleerd op de telefoon.



CTL-bestand op de telefoon

Phone heeft het ITL-bestand.



ITL-bestand op de telefoon

2. Niet-beveiligde cluster converteren naar beveiligde CUCM-cluster.

Schakel de gemengde modus in door de commando tools `ctl set-cluster mixed-mode` op de Command Line Interface (CLI) van de CUCM Publisher uit te voeren. Dit converteert de cluster van niet-veilig naar beveiligd.

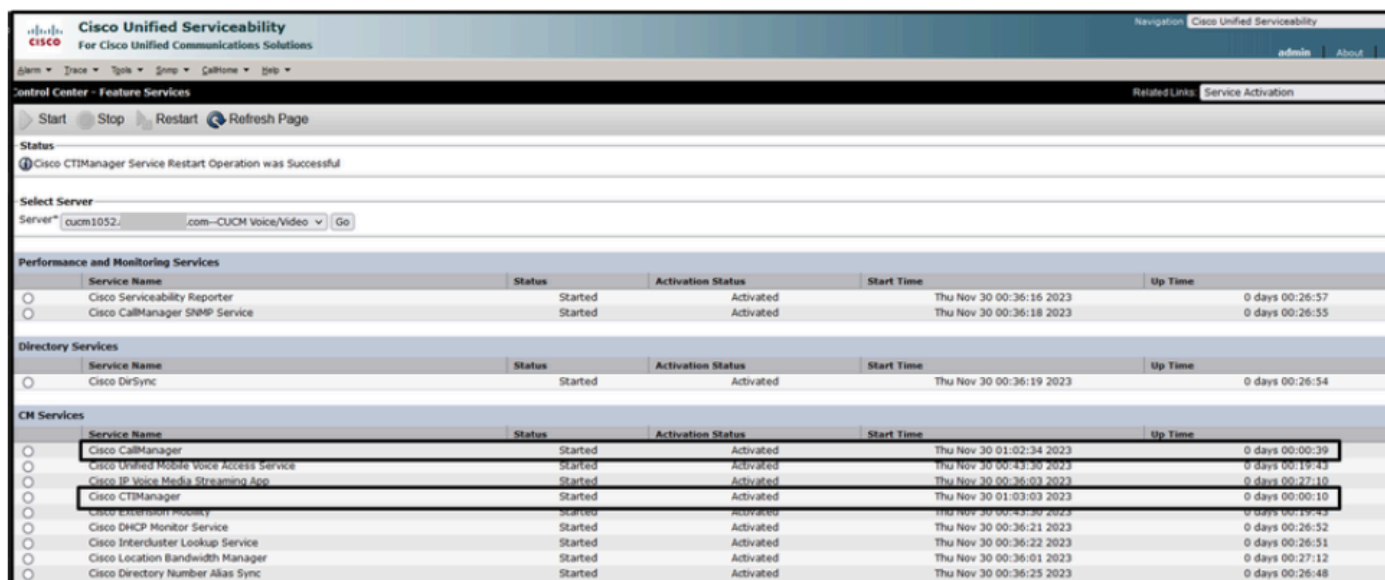
```
admin:
admin:
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y

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:
```

Omzetten in een beveiligd cluster

Nadat u de opdracht hebt uitgevoerd, start u de Cisco CallManager (CCM)- en Cisco CTI Manager (CTI)-services opnieuw op op alle knooppunten in het cluster.

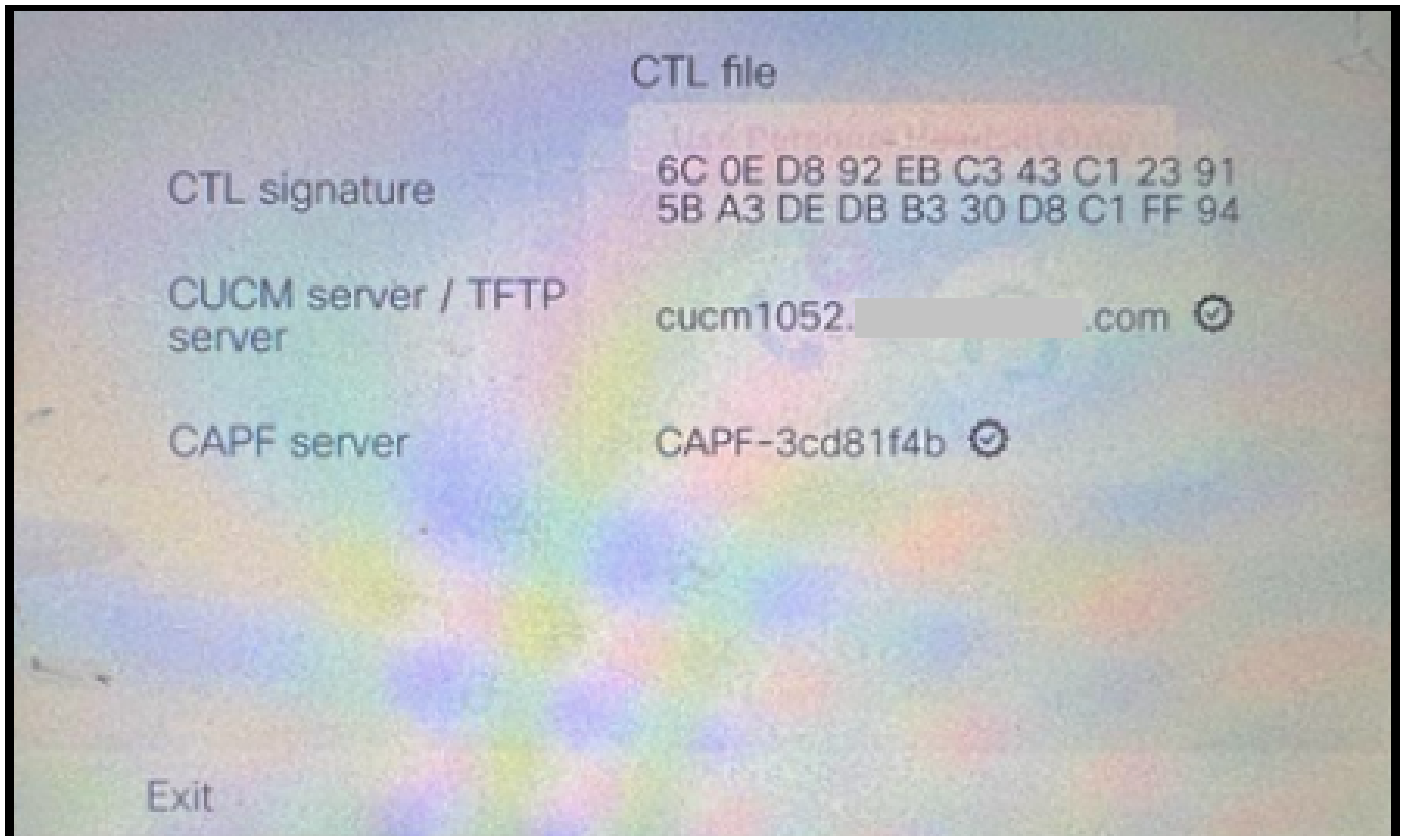


The screenshot shows the Cisco Unified Serviceability Control Center interface. It displays a table of services with columns for Service Name, Status, Activation Status, Start Time, and Up Time. The services are categorized into Performance and Monitoring Services, Directory Services, and CM Services. The CM Services section is highlighted, showing that Cisco CallManager, Cisco Unified Mobile Voice Access Service, Cisco IP Voice Media Streaming App, and Cisco CTIManager are all started and activated.

Service Name	Status	Activation Status	Start Time	Up Time
Cisco Serviceability Reporter	Started	Activated	Thu Nov 30 00:36:16 2023	0 days 00:26:57
Cisco CallManager SRMP Service	Started	Activated	Thu Nov 30 00:36:18 2023	0 days 00:26:55
Cisco DirSync	Started	Activated	Thu Nov 30 00:36:19 2023	0 days 00:26:54
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

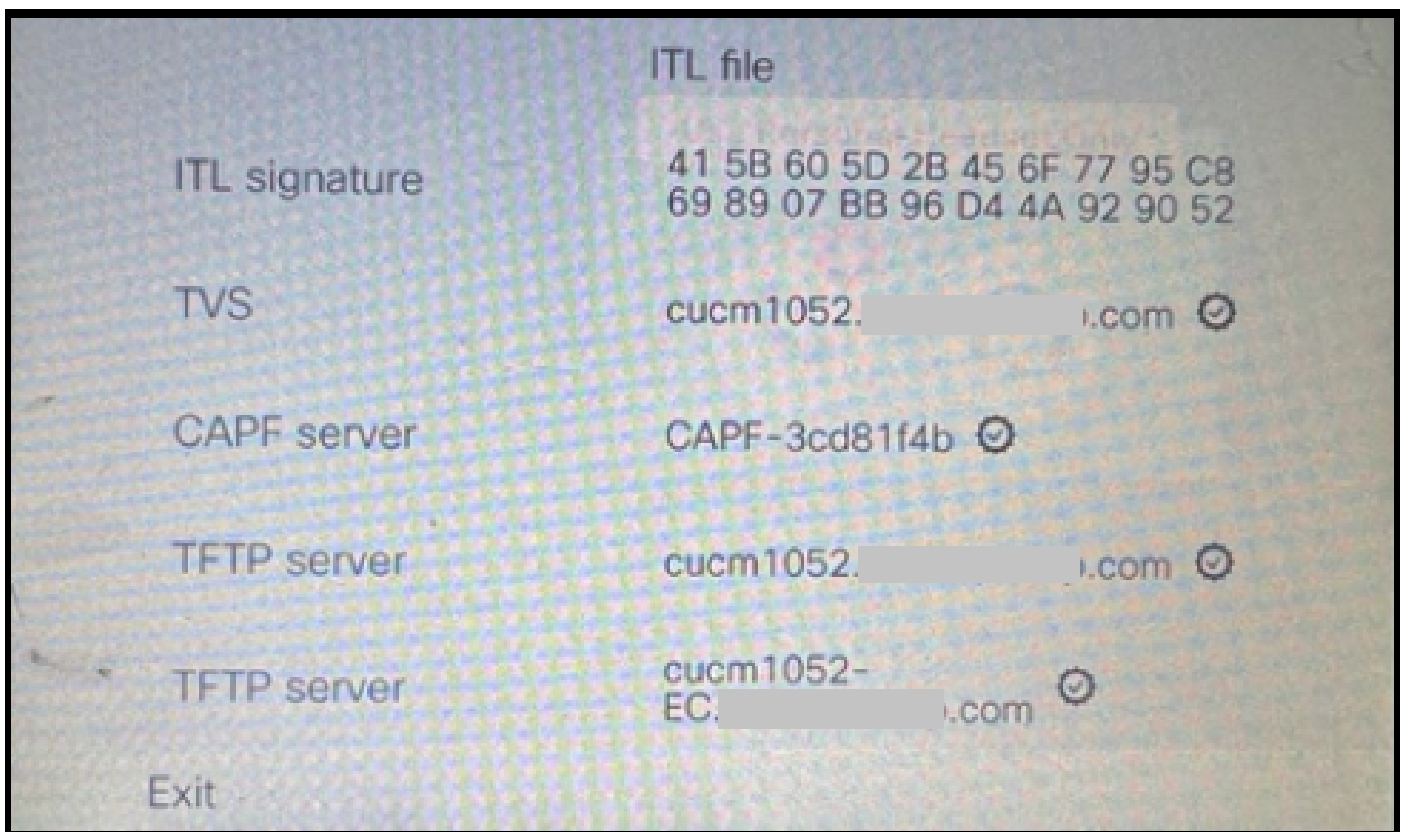
Start de CCM- en CTI-services opnieuw

Op de fysieke telefoon kon je de aanwezigheid van het CTL-bestand zien.



CTL-bestand op de telefoon

Het ITL-bestand bleef met dezelfde waarden.



ITL-bestand op de telefoon

3. Converteer terug naar een niet-beveiligde cluster vanuit een beveiligde verbinding.

Om de cluster van veilig naar niet-veilig te converteren, moet u de commando hulpprogramma's `ctl set-cluster non-secure-mode` op de CLI van de CUCM Publisher uitvoeren.

```
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

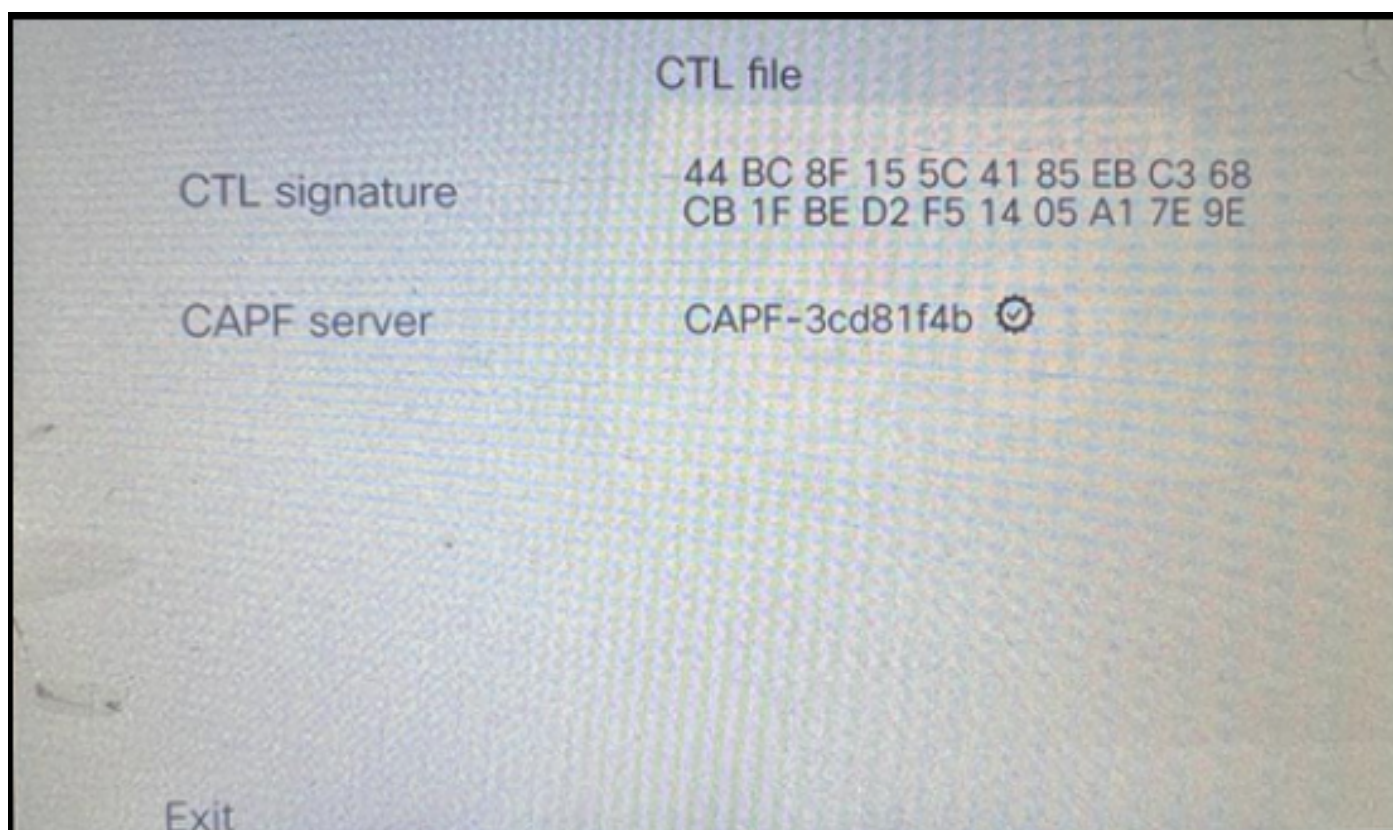
Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.

admin:
admin:
```

Omzetten in een niet-beveiligde cluster

Start de CCM- en CTI-services opnieuw op alle knooppunten in het cluster om de wijziging te laten doorklinken in alle knooppunten in het CUCM-cluster.

Nadat de cluster is geconverteerd naar niet-beveiligd, bevat de CTL de CUCM- en TFTP-vermeldingen niet. Het CTL-bestand bevat alleen de CAPF-ingang.



CTL-bestand op de telefoon

Het ITL-bestand bleef met dezelfde items.

ITL file

ITL signature

41 5B 60 5D 2B 45 6F 77 95 C8
69 89 07 BB 96 D4 4A 92 90 52

TVS

cucm1052-
EC.
.com ☑

CAPF server

CAPF-3cd81f4b ☑

TFTP server

cucm1052-
EC.
.com ☑

TFTP server

cucm1052-
EC.
.com ☑

Exit

ITL-bestand op de telefoon



Opmerking: Het wijzigen van het Apparaatbeveiligingsprofiel in de telefoon configuratie pagina (in de CUCM Administration web pagina) naar ofwel veilig of niet-veilig heeft geen effect op de ITL of CTL bestanden. Je kunt de omgeving dus houden zoals vroeger en je hoeft ze niet te veranderen.

4. Migreer de telefoon naar een nieuwe niet-beveiligde CUCM-cluster.

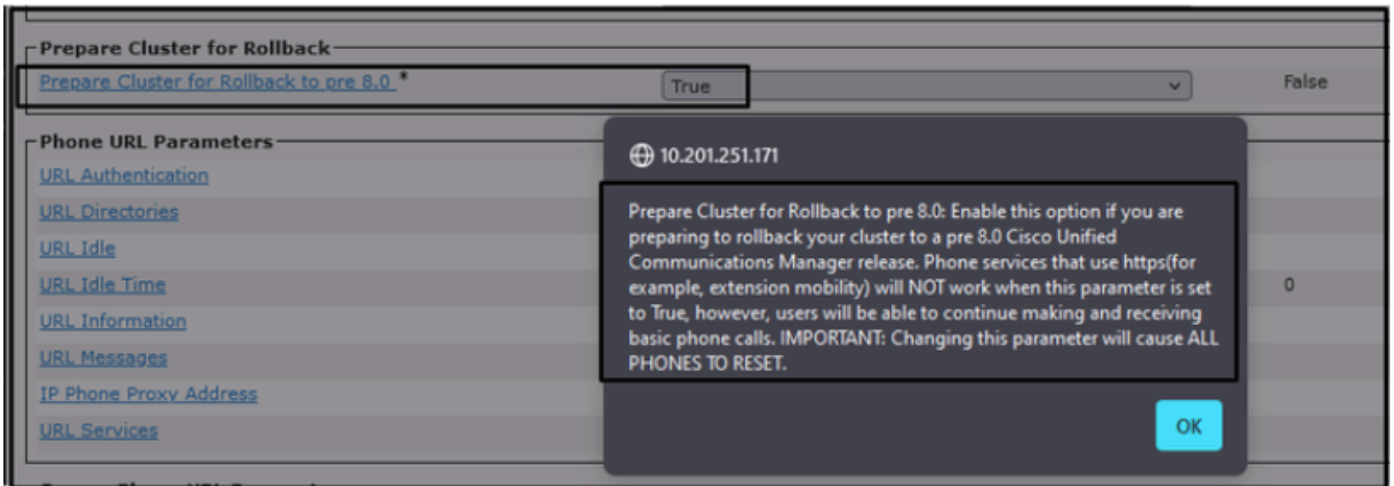


Opmerking: voordat u doorgaat met de migratie, is het een goede praktijk om de Trust Verification Service (TVS) en TFTP-services opnieuw te starten op alle knooppunten (alleen op deze services enabled knooppunten) in het broncluster. Dit elimineert alle hung- of lekkagesessies in de TVS/TFTP-service.

Meld u aan bij de CUCM-webinterface voor beheer en navigeer naar System > Enterprise Parameters.

Stel de waarde van Prepare Cluster for Rollback in op pre 8.0 to True. Klik vervolgens op de knoppen Apply Config en Reset.

De Help-sectie voor deze parameter is in deze screenshot voorzien.

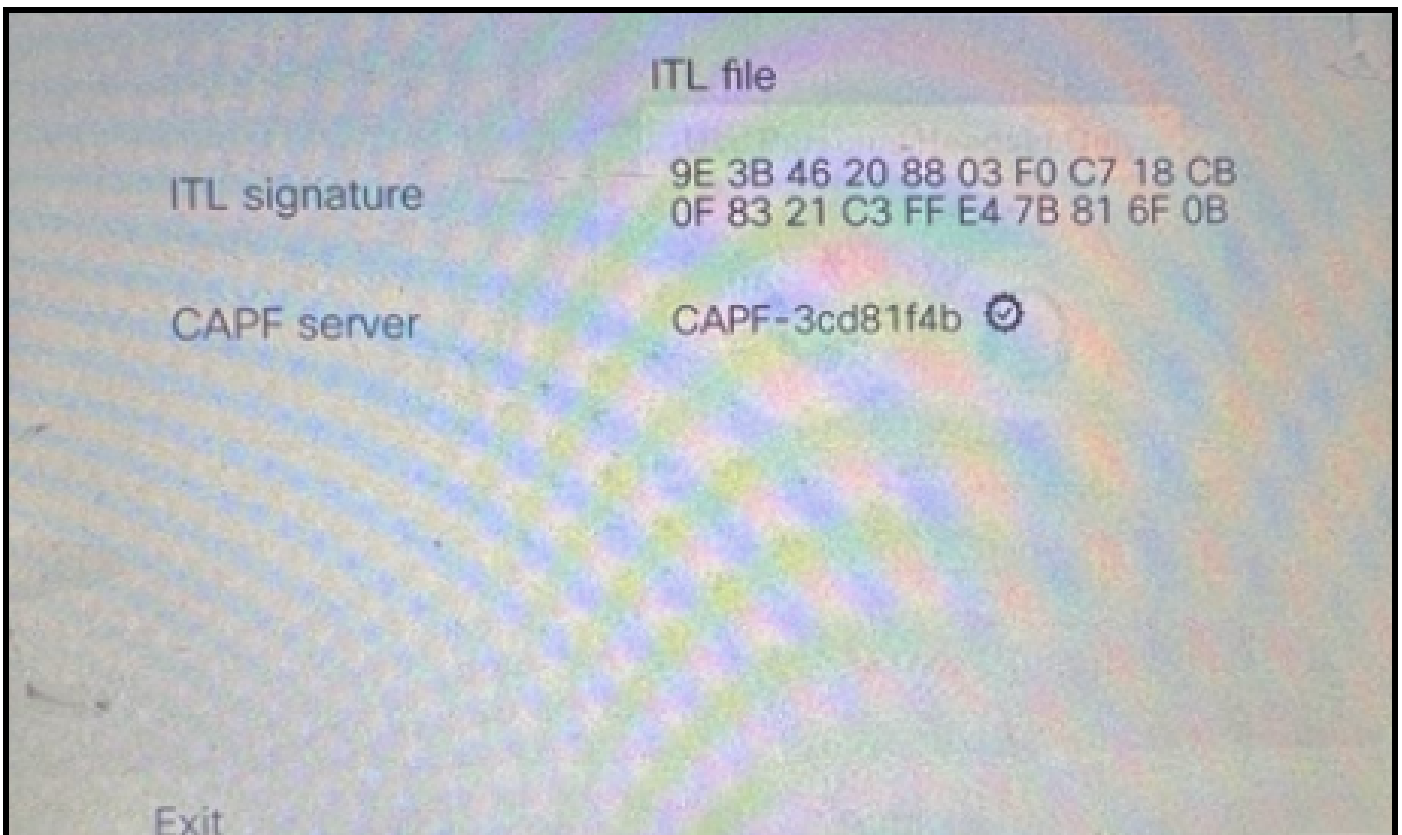


Informatie over het voorbereide cluster voor terugdraaien naar 8.0 Parameter

Monitor de telefoonregistratie telt op het cluster (via Real Time Monitoring Tool - RTMT) voor en na het wijzigen van de parameterwaarde. Op deze manier kan worden gevalideerd of deze wijzigingen al dan niet worden toegepast op alle apparaten in het cluster.

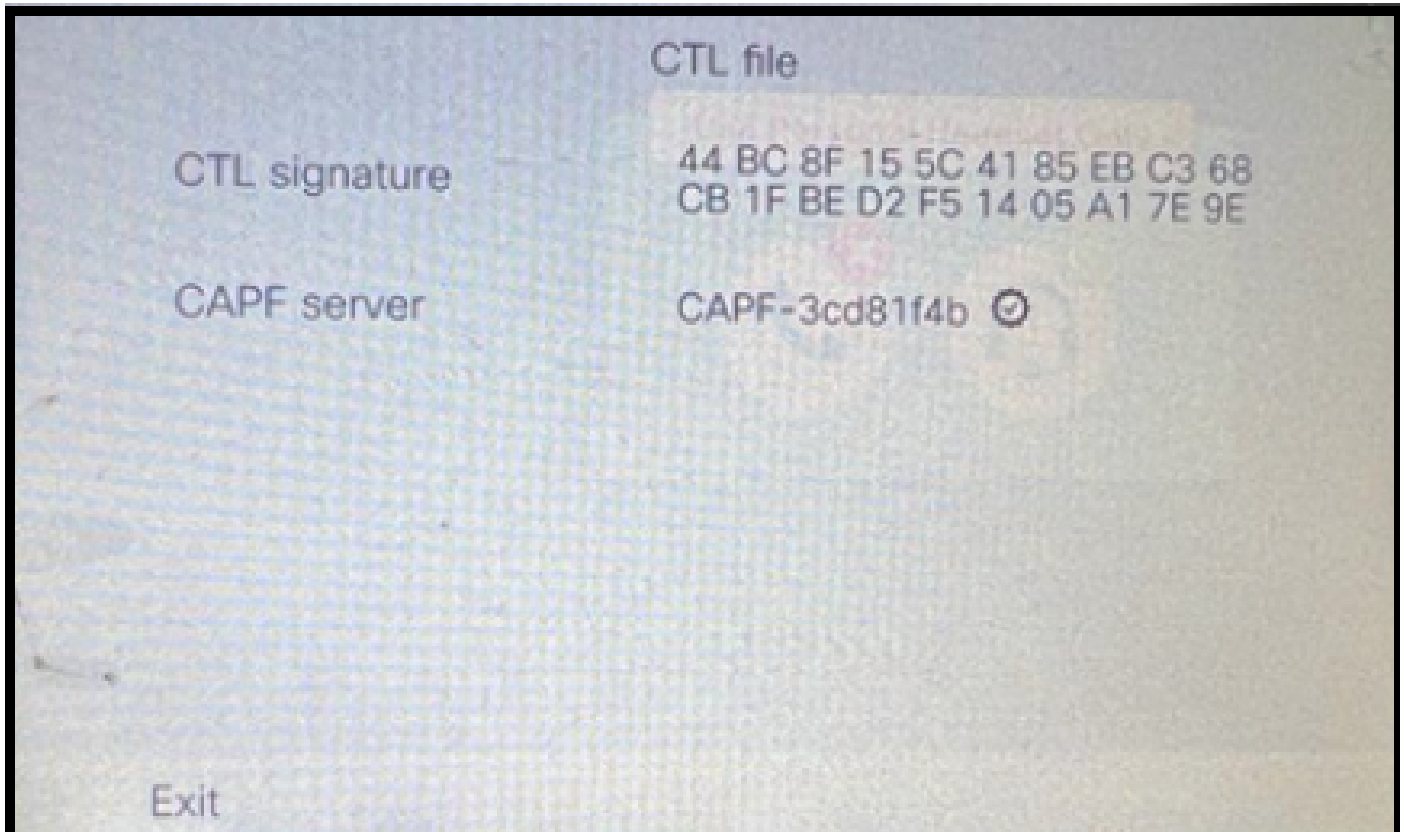
Op de fysieke telefoon, kon u slechts de CAPF ingangen in zowel de ITL & CTL- dossiers zien. U kunt dit ook waarnemen door telefoon webpagina te openen in de webbrowser.

ITL-bestand



ITL-bestand op de telefoon

CTL-bestand



CTL-bestand op de telefoon

Voordat u de migratie start, is het goed om de ITL & CTL-bestanden in een paar telefoons te valideren om ervoor te zorgen dat de wijzigingen hebben plaatsgevonden.

Nu zijn de telefoons klaar voor de migratie.

Het migreren van de telefoons van broncluster aan de bestemmingscluster. Op dit moment zijn beide clusters niet veilig.

Broncluster:

- IP-adres - 10.201.251.171
- FQDN - cucm1052.domain.com
- Versie: 12.5.1.16065-1

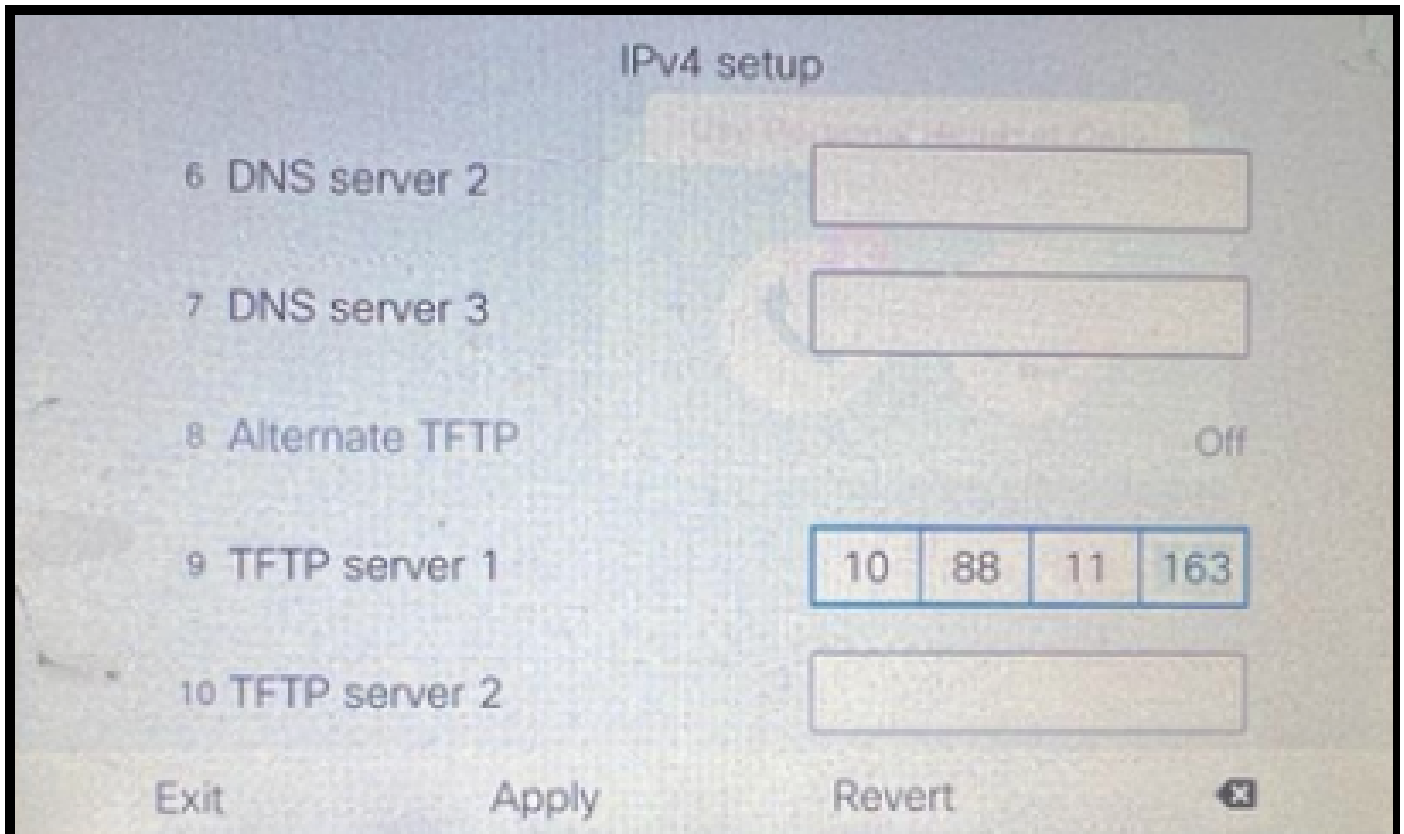
Bestemmingscluster:

- IP-adres - 10.88.11.163
- FQDN - cucmpub.domain.com
- Versie : 12.5.1.14900-63

Stel op de fysieke telefoon de waarde TFTP Server 1 in op het nieuwe IP-adres van het cluster van bestemming en klik op de knop Toepassen.

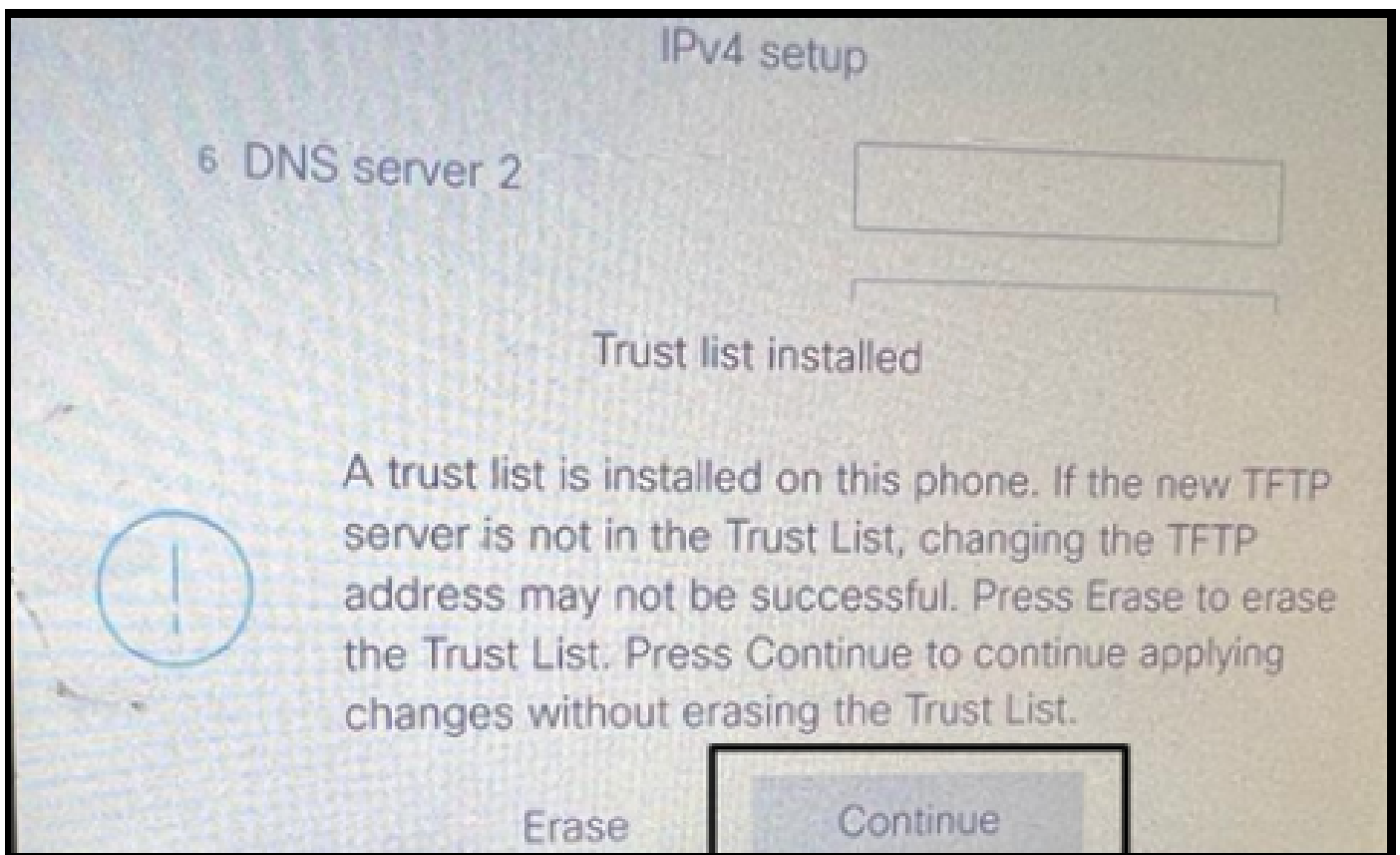


Opmerking: dit proces staat gelijk aan het wijzigen van de TFTP-ip in de DHCP-scope - optie 150/66. Als het doelcluster in het andere domein zit, moet u ook de juiste DNS-servers in de DHCP-scope instellen.



Configureer TFTP IP op de telefoon

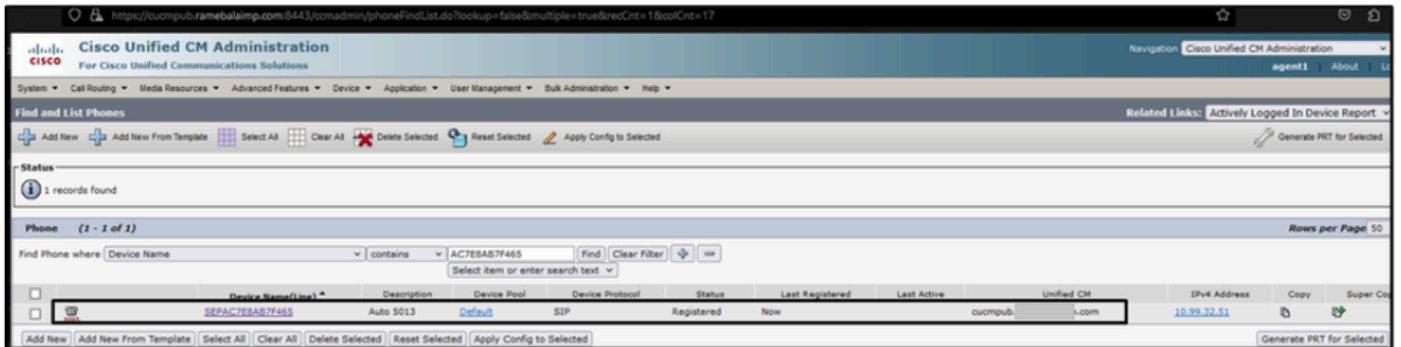
Klik op de knop Doorgaan, hierdoor blijven de oude CTL- en ITL-bestanden (die alleen de CAPF-ingang bevatten) uit het broncluster behouden.



Door op de knop Doorgaan te drukken, kunnen de oude CTL- en ITL-bestanden behouden blijven

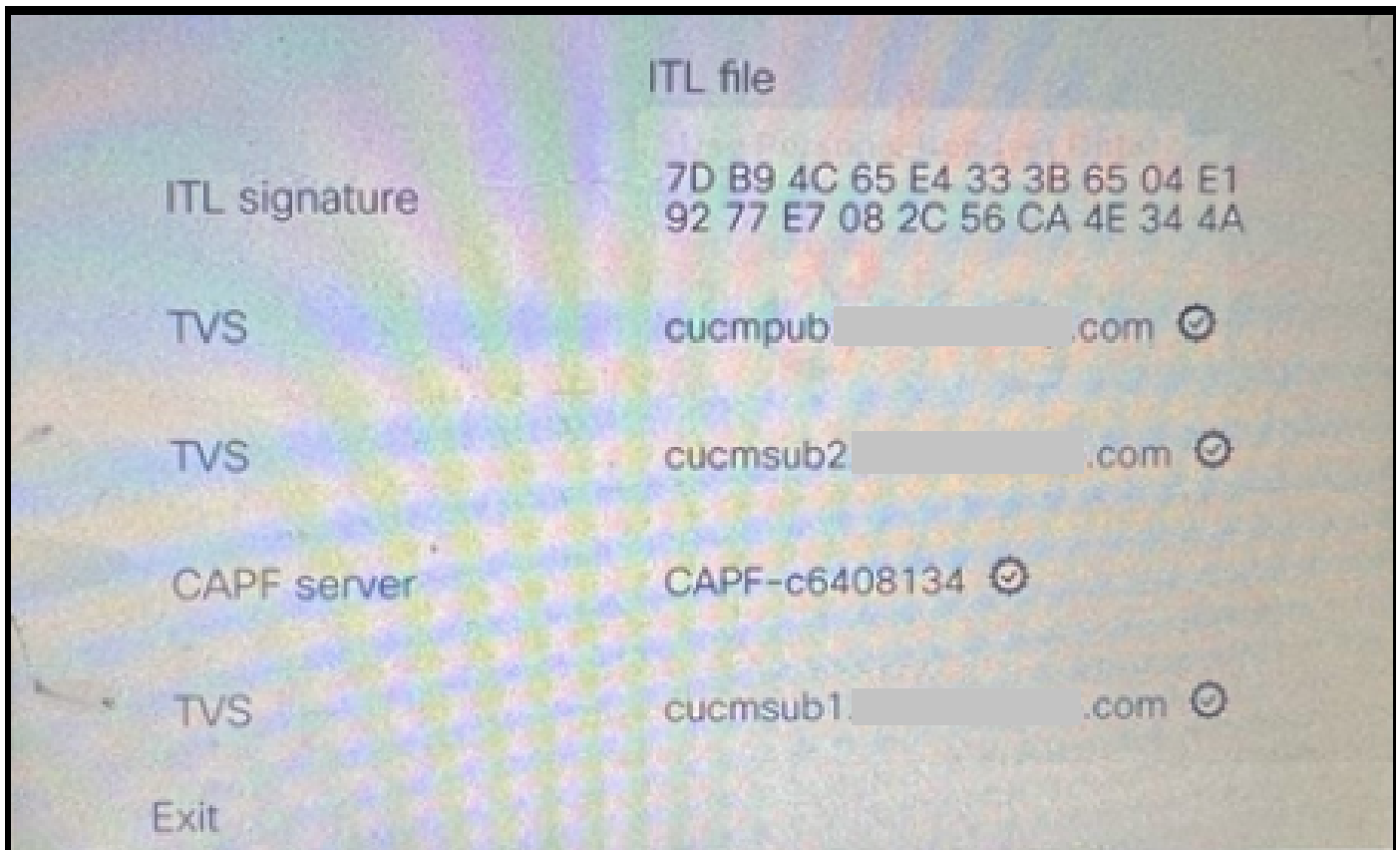
Verifiëren

De telefoon wordt met succes geregistreerd in het doelcluster.



Telefoon geregistreerd bij de CUCM

De telefoon bevat de bestemmingen cluster Vertrouwen lijst ingangen.



ITL-bestand op de telefoon

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Standaard CUCM-beveiliging en ITL-werking en probleemoplossing begrijpen](#)
- [CUCM Mixed Mode met Tokenless CTL](#)
- [Security Guide voor Cisco Unified Communications Manager, release 12.5\(1\)](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.