

Demonstre a migração do telefone IP de CUCM seguro para não seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve uma das melhores práticas para migrar telefones do Cisco Unified Communication Manager (CUCM) protegido para um CUCM não seguro.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CUCM
- Telefone IP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Versões do CUCM - 12.5.1.16065-1 e 12.5.1.14900-63
- Modelo do telefone IP - 8865 e versão - 12.8(1)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede

Telefone_IP > Switch Cisco > Roteador Cisco > Switch Cisco > Cluster CUCM

Configurações

Esses cenários explicam a migração do telefone de um cluster do CUCM seguro para um não seguro. Durante cada estágio, o status dos arquivos CTL (Certificate Trust List) e ITL (Identity Trust List) no telefone são documentados.

1. Registre um telefone em um cluster não seguro do CUCM.
2. Converta o cluster não seguro em cluster CUCM seguro.
3. Converta de volta para um cluster não seguro a partir de um
4. Migre o telefone para um novo cluster não seguro do CUCM.

1. Registre um telefone em um cluster não seguro do CUCM.

Estas são as informações sobre o cluster de origem não segura.

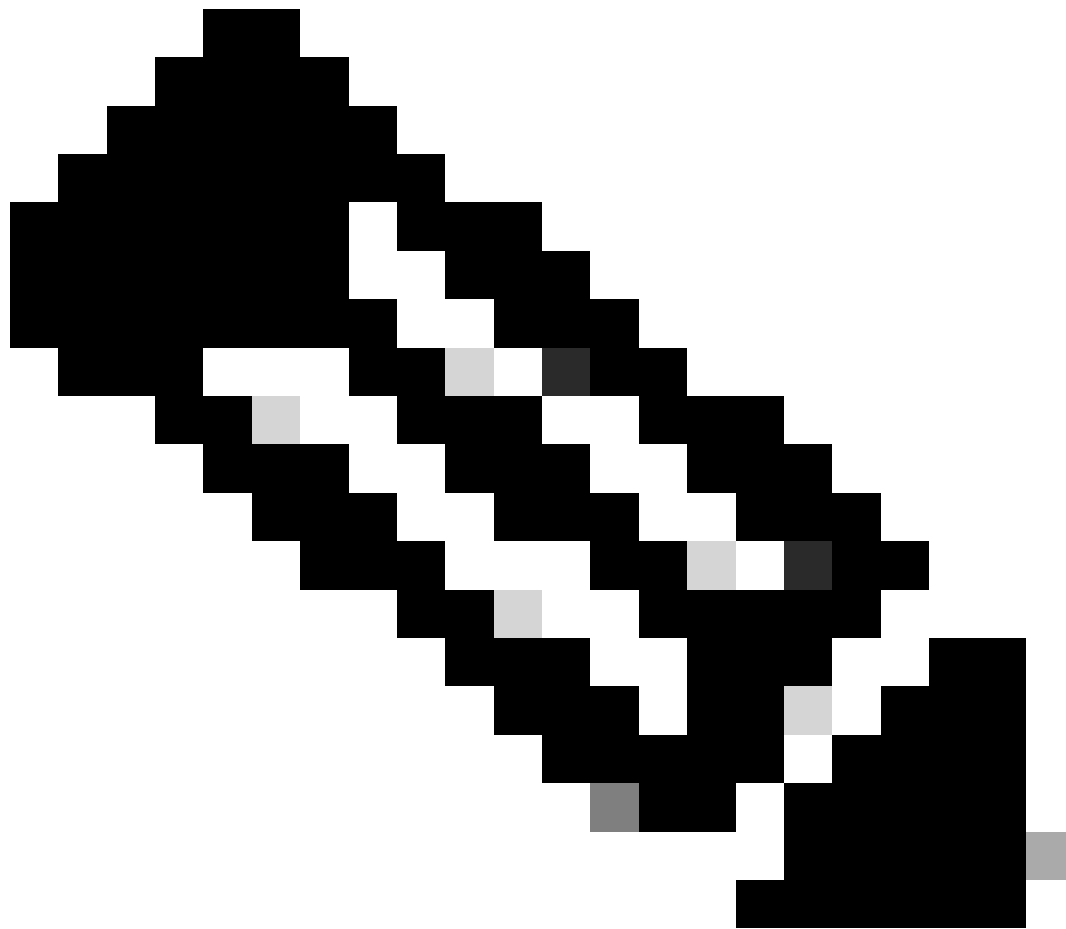
- Endereço IP - 10.201.251.171
- FQDN - cucm1052.domain.com
- Versão: 12.5.1.16065-1

Registre um telefone em um cluster não seguro do CUCM. Para isso, configure a opção 150/66 do Dynamic Host Configuration Protocol (DHCP) para apontar para o endereço IP do Trivial File Transfer Protocol (TFTP) (esse seria o nó CUCM onde o serviço TFTP está ativado).

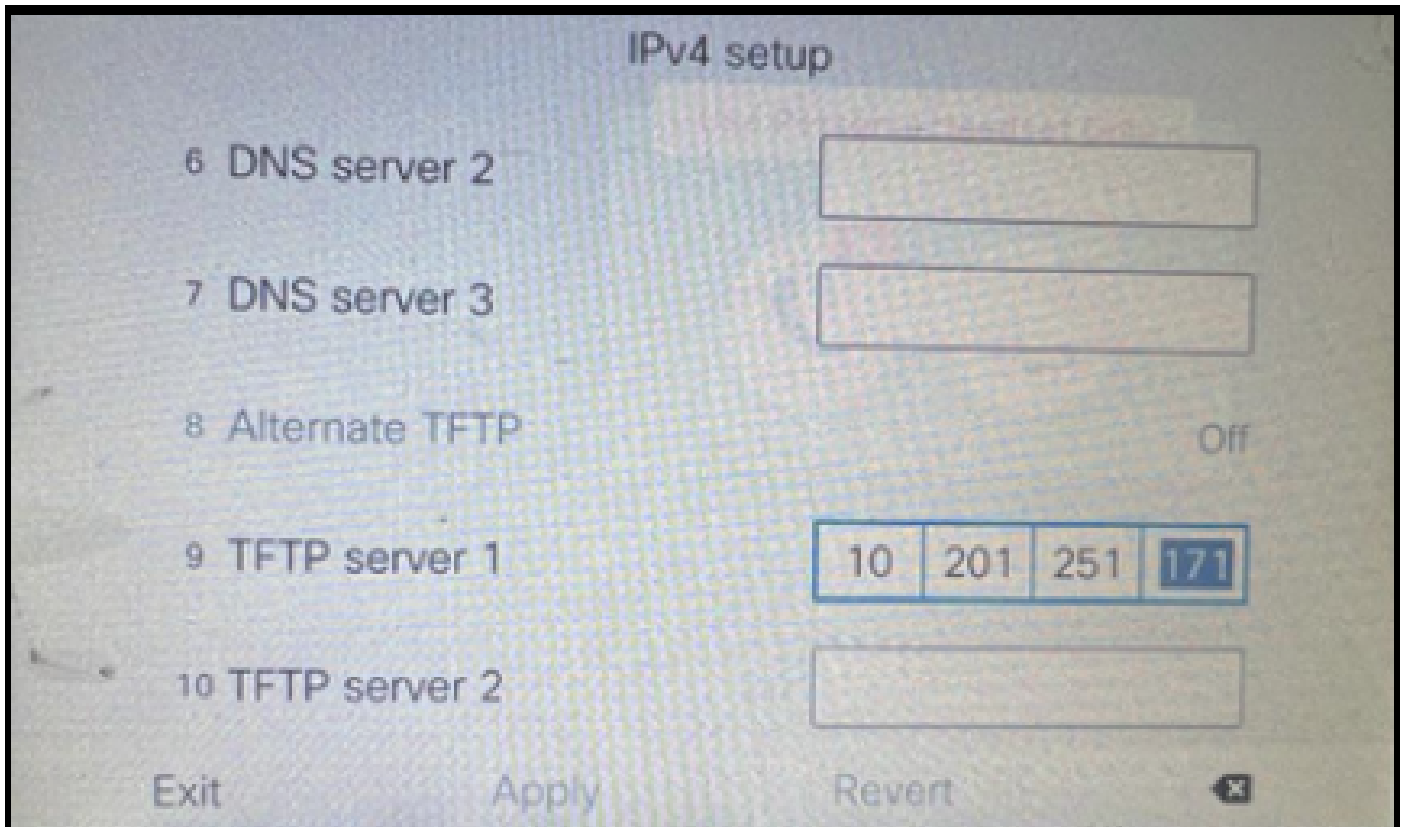
Para a infraestrutura em que você não tem os servidores DHCP, é necessário configurar o IP TFTP manualmente no telefone físico.

No telefone físico, navegue até Settings > Admin Settings > Network Setup > Ethernet setup > IPv4 setup.

Desative o DHCP e forneça detalhes de IP estático da sua rede. Depois disso, forneça o CUCM IP não seguro na seção Servidor TFTP 1 como mostrado na captura de tela.

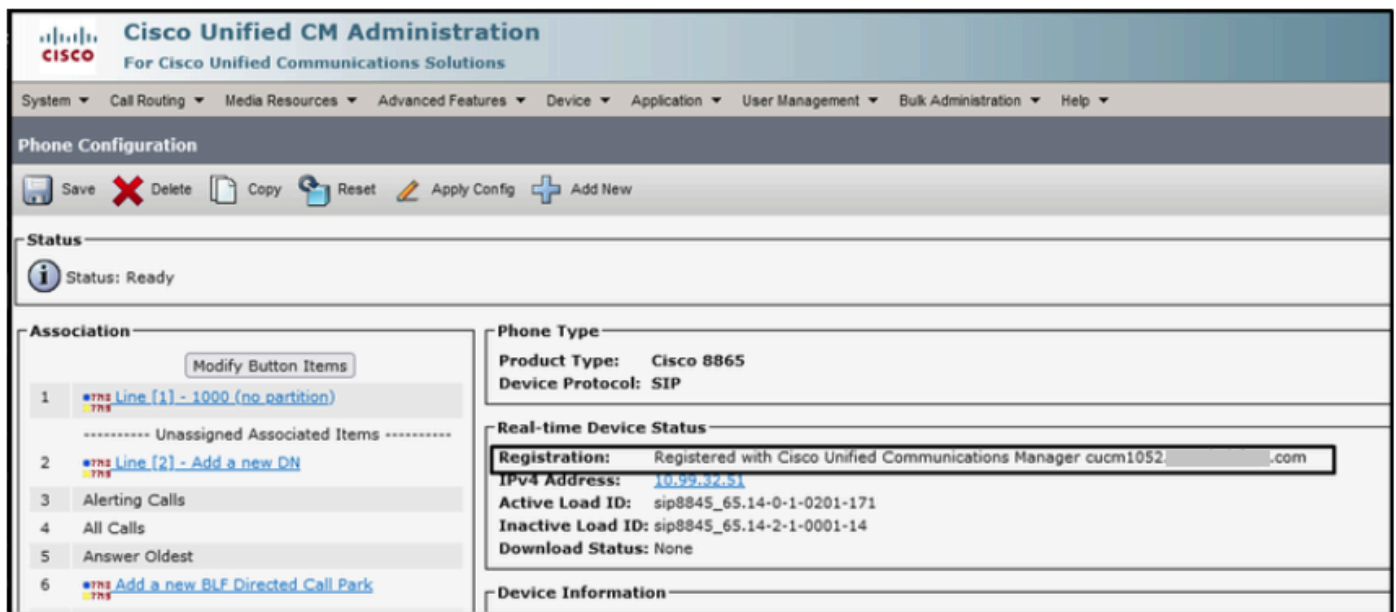


Observação: esse processo é equivalente à alteração do IP TFTP no escopo do DHCP - opção 150 / 66. E se o cluster estiver configurado com o nome de domínio, então você terá que definir os servidores apropriados do Domain Name System (DNS) no escopo do DHCP também.



Configurar o IP TFTP no telefone

O telefone IP é registrado no cluster CUCM não seguro mencionado com êxito.



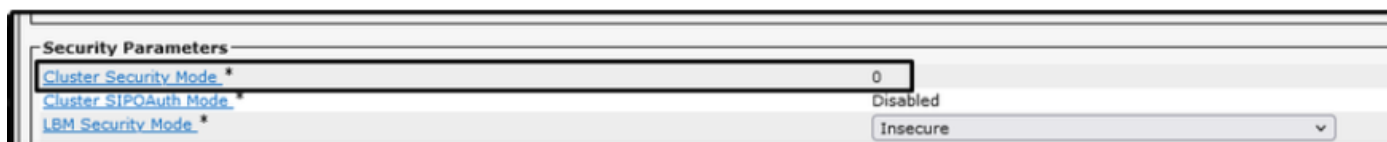
Telefone registrado no CUCM

Faça login na interface da Web de administração do CUCM e navegue até System > Enterprise Parameters.

Esses são os valores dos parâmetros definidos na página Enterprise parameter do cluster CUCM não seguro.

- O Modo de segurança de cluster está definido como 0, isso confirma que o cluster não é

seguro.



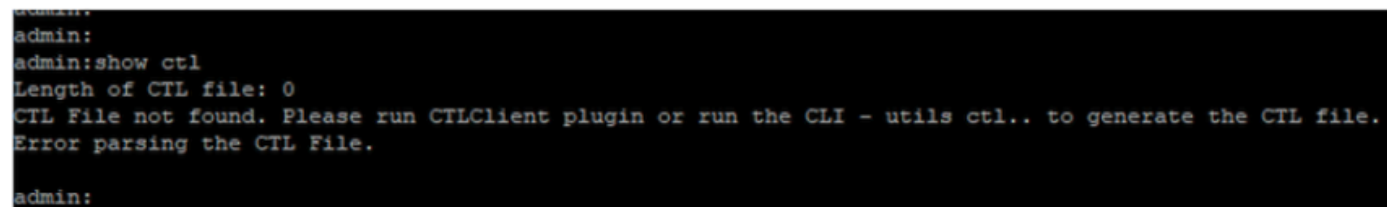
O Modo de Segurança de Cluster está Definido como 0

- Preparar Cluster para Reversão anterior a 8.0 está definido como Falso. Assim, o conteúdo dos arquivos ITL e CTL são mantidos com valores apropriados.



Preparar Cluster para Reversão para versões anteriores à 8.0 está Definido como Falso

Como o cluster não é seguro, não há arquivo CTL no servidor TFTP. Você pode verificar isso executando o comando show ctl na sessão Secure Shell (SSH) do nó CUCM.



O arquivo CTL não está presente

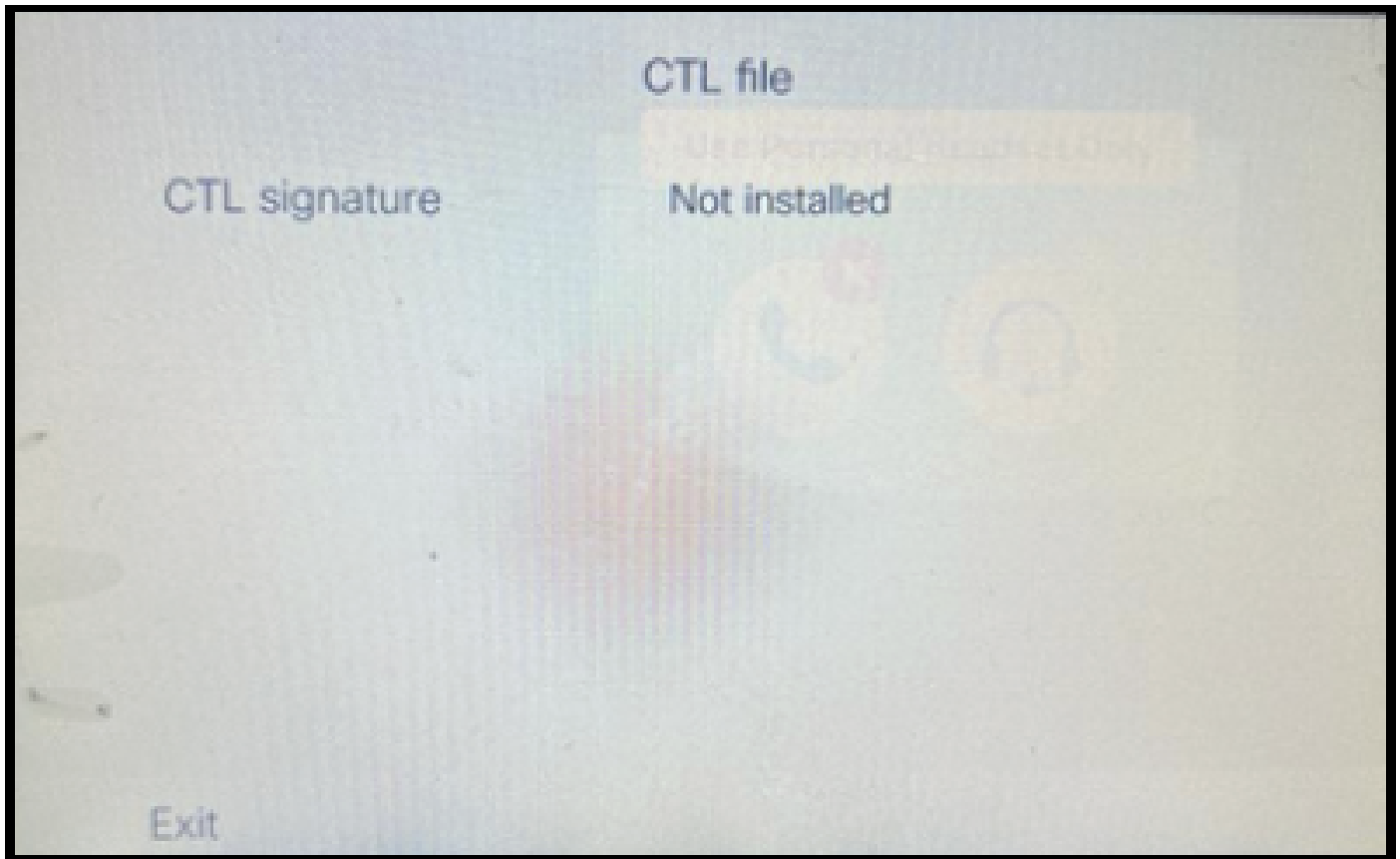
No telefone físico, você pode confirmar que não há nenhum arquivo CTL instalado. No entanto, você verá o arquivo ITL.

O ITL está presente devido ao recurso Segurança por padrão (SBD) no CUCM. Para obter mais informações sobre o SBD, clique [aqui](#) .

No telefone físico, navegue até Settings > Admin settings > Security setup > Trust list.

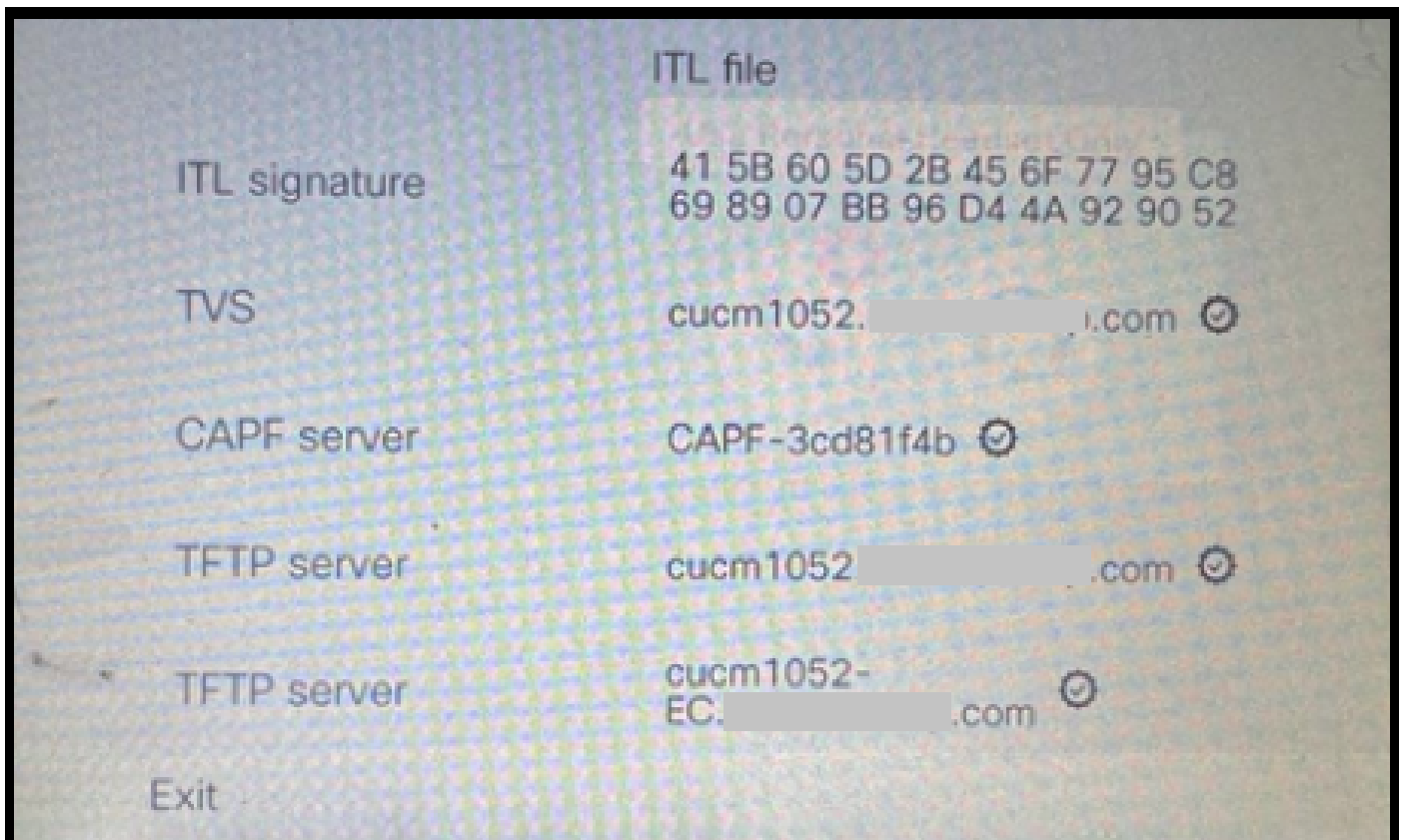
Aqui você pode encontrar o status dos arquivos CTL e ITL.

O CTI não está instalado no telefone.



Arquivo CTL no telefone

O telefone tem o arquivo ITL.



Arquivo ITL no telefone

2. Converta um cluster não seguro em um cluster CUCM seguro.

Ative o modo misto executando o comando `utils ctl set-cluster mixed-mode` na Interface de Linha de Comando (CLI) do Editor do CUCM. Isso converte o cluster de não seguro em seguro.

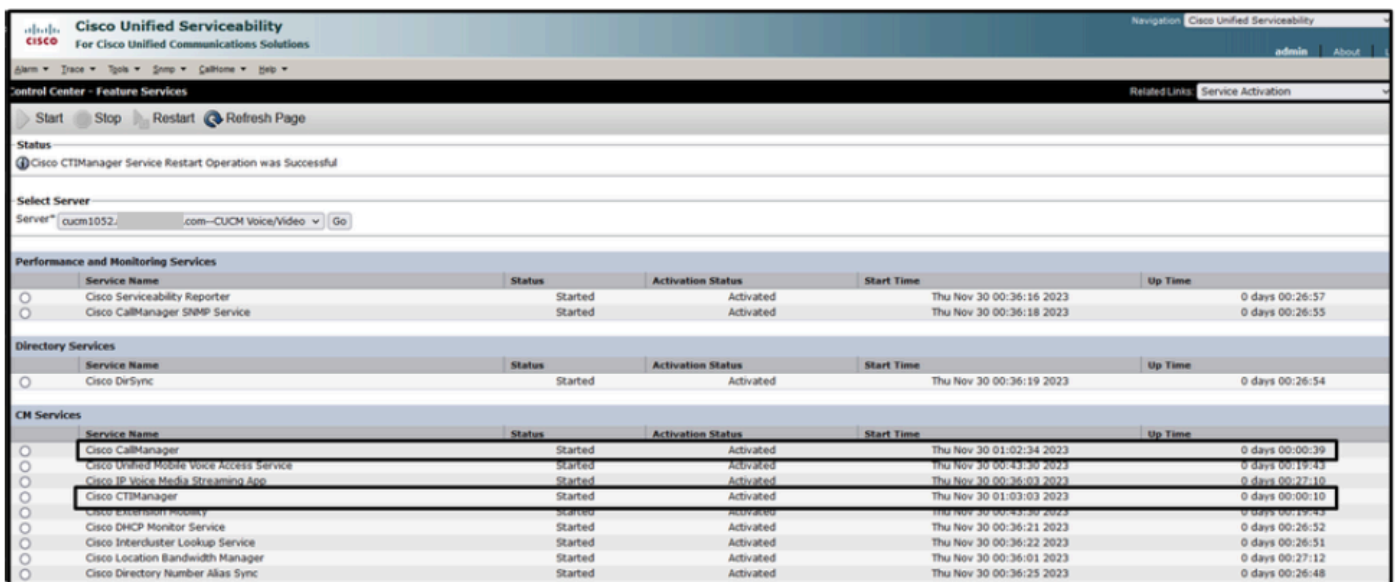
```
admin:
admin:
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y

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:
```

Converter em um cluster seguro

Após executar o comando, reinicie os serviços Cisco CallManager (CCM) e Cisco CTIManager (CTI) em todos os nós no cluster.

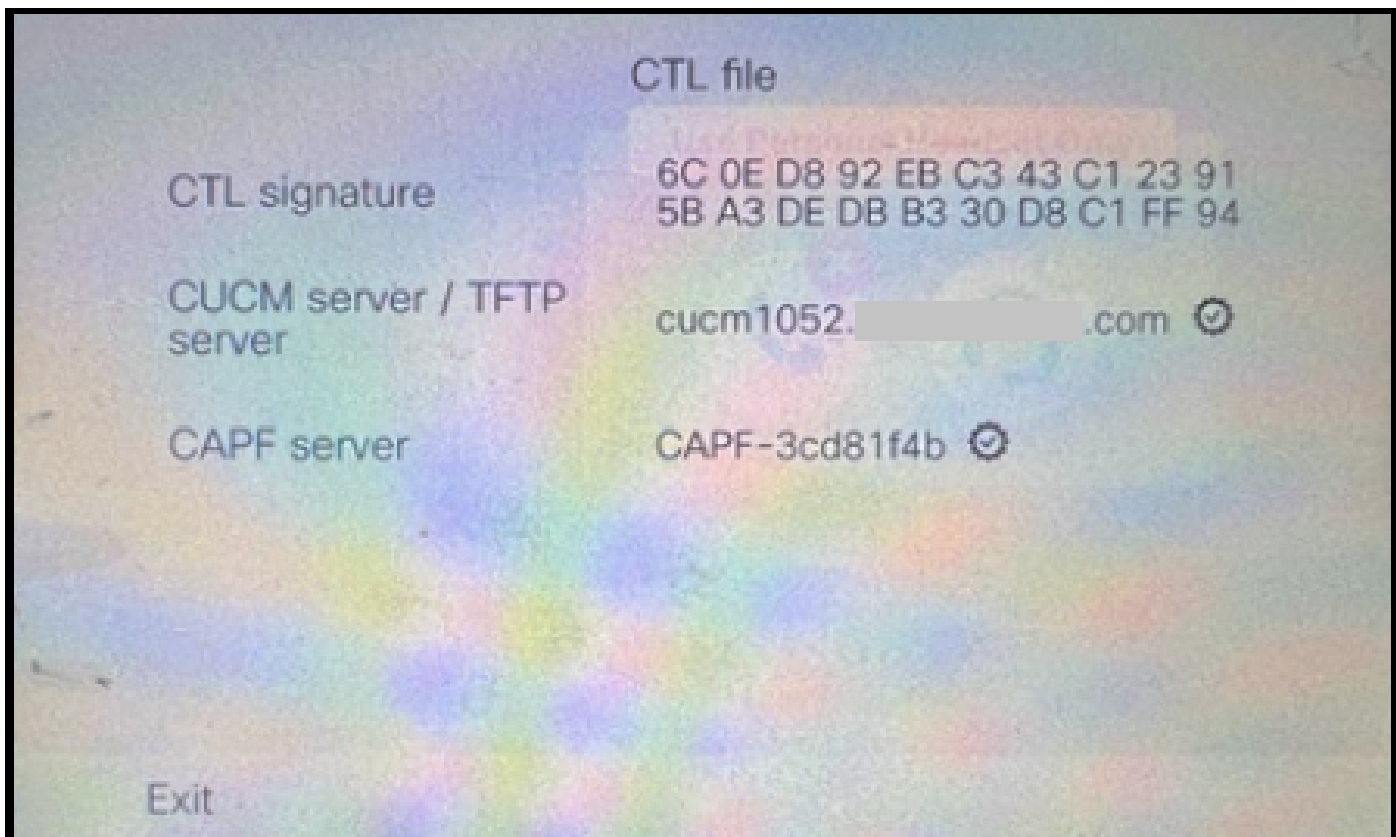


The screenshot shows the Cisco Unified Serviceability Control Center interface. A message indicates that the Cisco CTIManager Service Restart Operation was successful. Below this, there is a 'Select Server' section with a dropdown menu set to 'cucm1052...' and a 'Go' button. The main part of the interface 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 SNMP 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

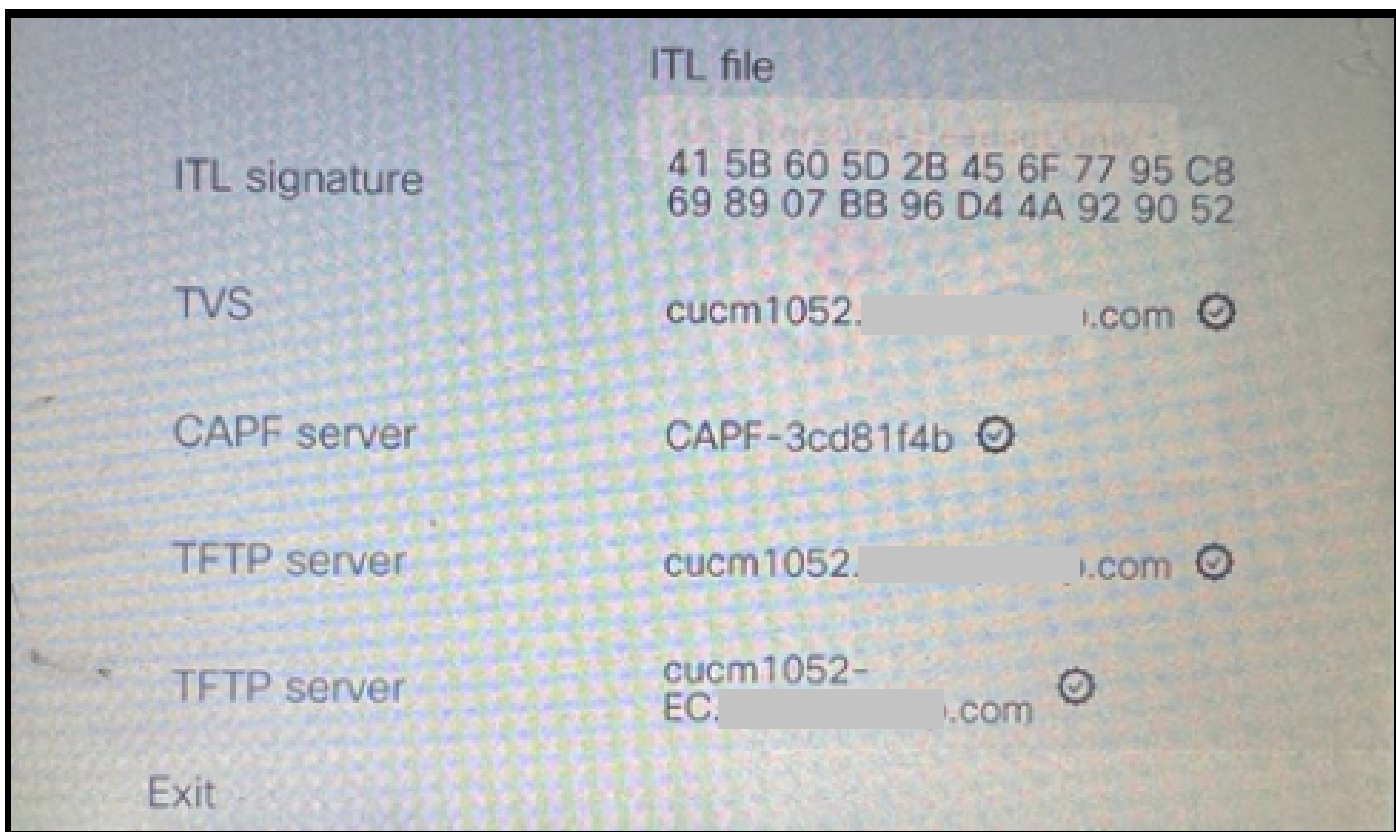
Reinicie os serviços CCM e CTI

Agora, no telefone físico, você pode ver a presença do arquivo CTL.



Arquivo CTL no telefone

O arquivo ITL permaneceu com os mesmos valores.



Arquivo ITL no telefone

3. Converta de volta para um cluster não seguro a partir de um cluster seguro.

Para converter o cluster de seguro para não seguro, você precisa executar o comando `utils ctl set-cluster non-secure-mode` na CLI do Editor do 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

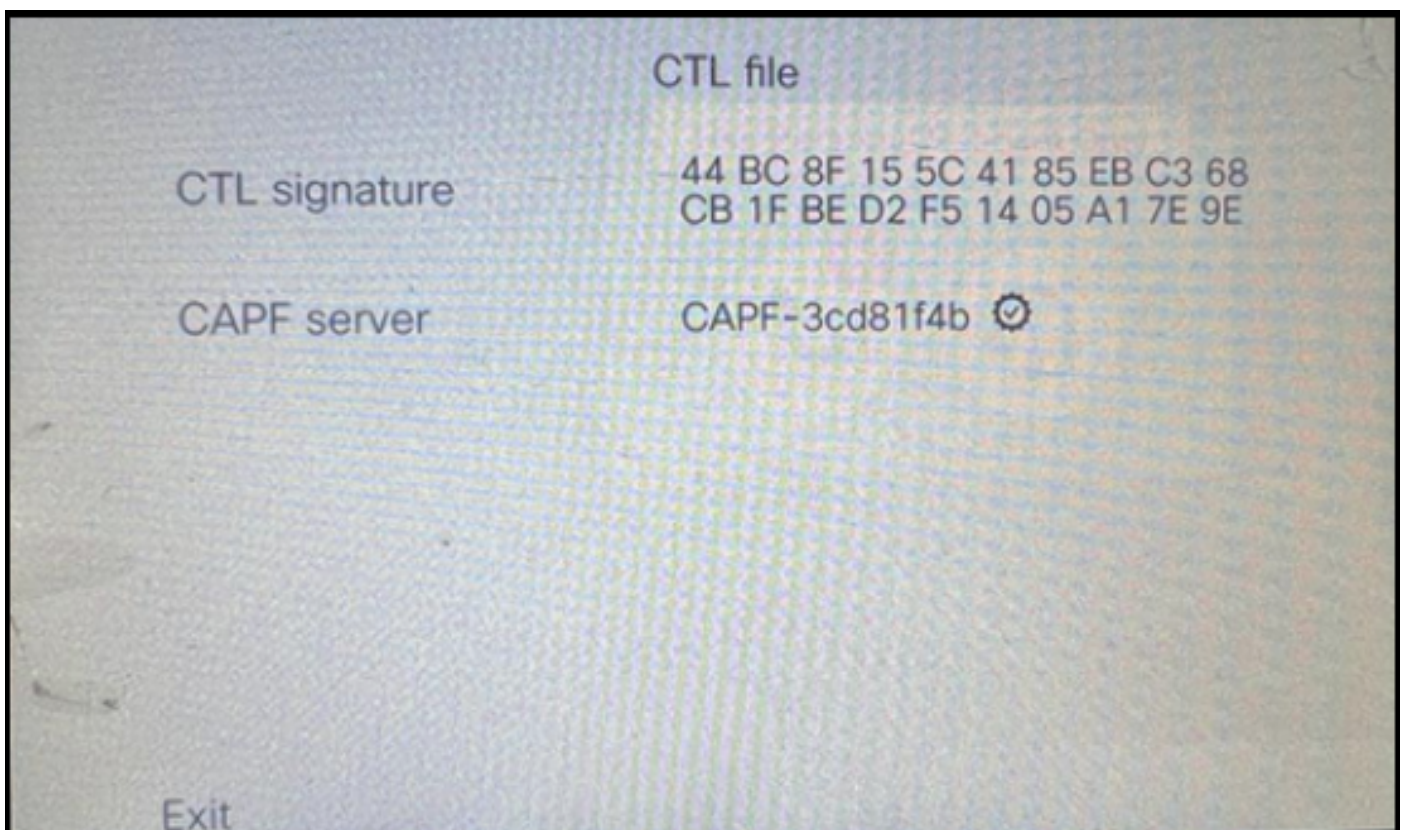
Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.

admin:
admin:
```

Converter em um Cluster Não Seguro

Reinicie os serviços CCM e CTI em todos os nós no cluster para fazer a alteração refletir em todos os nós no cluster CUCM.

Após converter o cluster em não seguro, a lista de certificados confiáveis não contém as entradas de CUCM e TFTP. O arquivo CTL contém somente a entrada CAPF.



Arquivo CTL no telefone

O arquivo ITL permaneceu com as mesmas entradas.

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-██████████.com ☑

CAPF server

CAPF-3cd81f4b ☑

TFTP server

cucm1052-██████████.com ☑

TFTP server

cucm1052-
EC-██████████.com ☑

Exit

Arquivo ITL no telefone



Observação: alterar o Perfil de segurança do dispositivo na página de configuração do telefone (na página da Web Administração do CUCM) para seguro ou não seguro não tem efeito nos arquivos ITL ou CTL. Assim, você pode manter a configuração como era antes e não precisa alterá-los.

4. Migre o telefone para um novo cluster não seguro do CUCM.

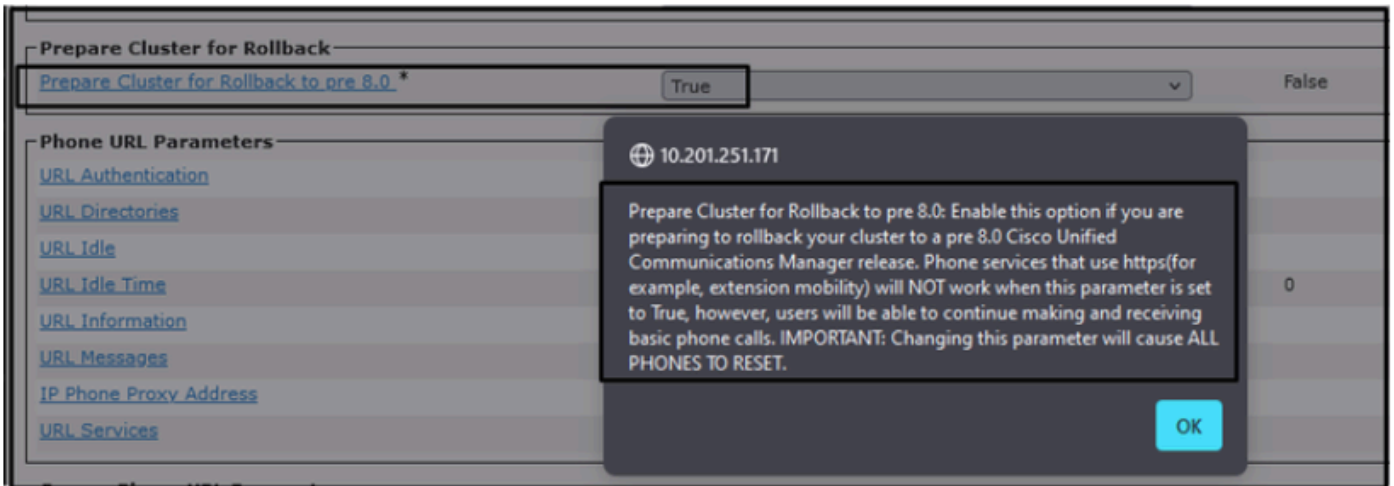


Observação: antes de prosseguir com a migração, é recomendável reiniciar o Serviço de Verificação Confiável (TVS) e os serviços TFTP em todos os nós (somente nesses nós habilitados para serviços) no cluster de origem. Isso elimina qualquer suspensão ou perda de sessões no serviço TVS/TFTP.

Faça login na interface da Web de administração do CUCM e navegue até System > Enterprise Parameters.

Defina o valor de Prepare Cluster for Rollback para pre 8.0 como True. Em seguida, continue clicando nos botões Apply Config e Reset.

A seção de ajuda para este parâmetro é fornecida nesta captura de tela.

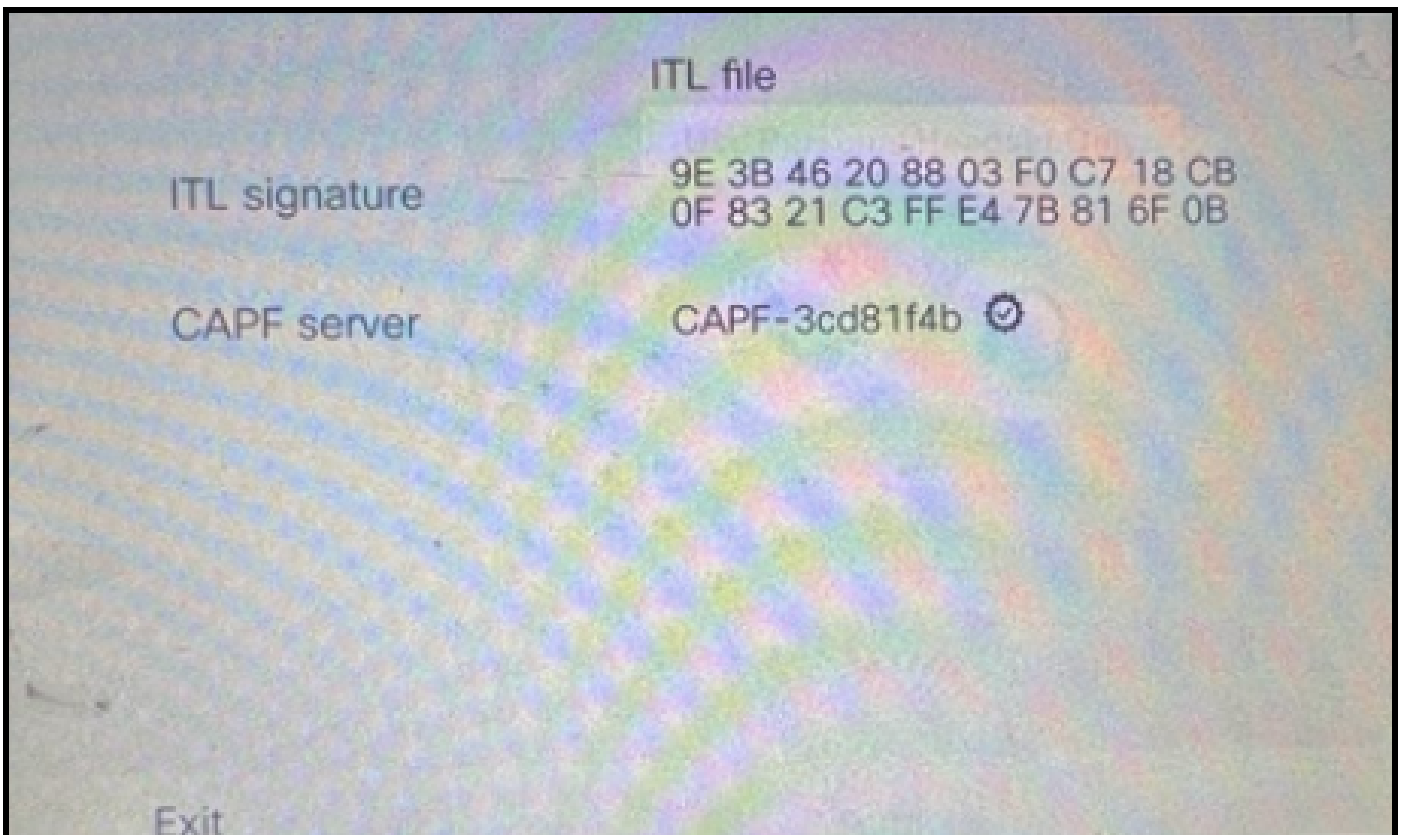


Informações sobre o Parâmetro Preparar Cluster para Reversão para versões anteriores à 8.0

Monitore as contagens de registro de telefone no cluster (via Real Time Monitoring Tool - RTMT) antes e depois de alterar o valor do parâmetro. Dessa forma, é possível validar se essas alterações são aplicadas a todos os dispositivos no cluster ou não.

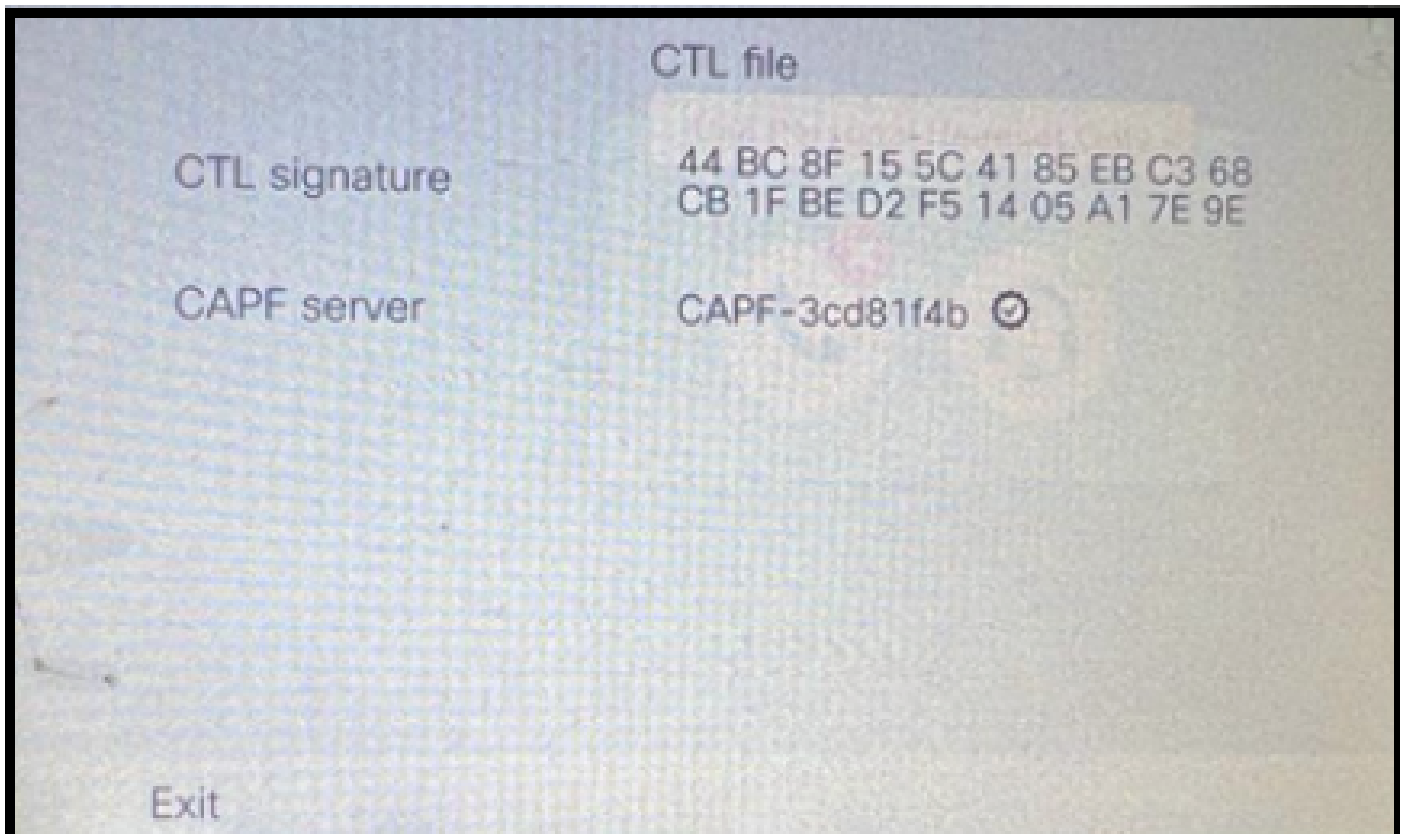
No telefone físico, você pode ver apenas as entradas CAPF nos arquivos ITL e CTL. Você também pode observar isso abrindo a página da Web do telefone no navegador da Web.

Arquivo ITL



Arquivo ITL no telefone

Arquivo CTL



Arquivo CTL no telefone

Antes de iniciar a migração, é recomendável validar os arquivos ITL e CTL em poucos telefones para garantir que as alterações tenham ocorrido.

Agora os telefones estão prontos para a migração.

Migrando os telefones do cluster de origem para o cluster de destino. Atualmente, ambos os clusters não são seguros.

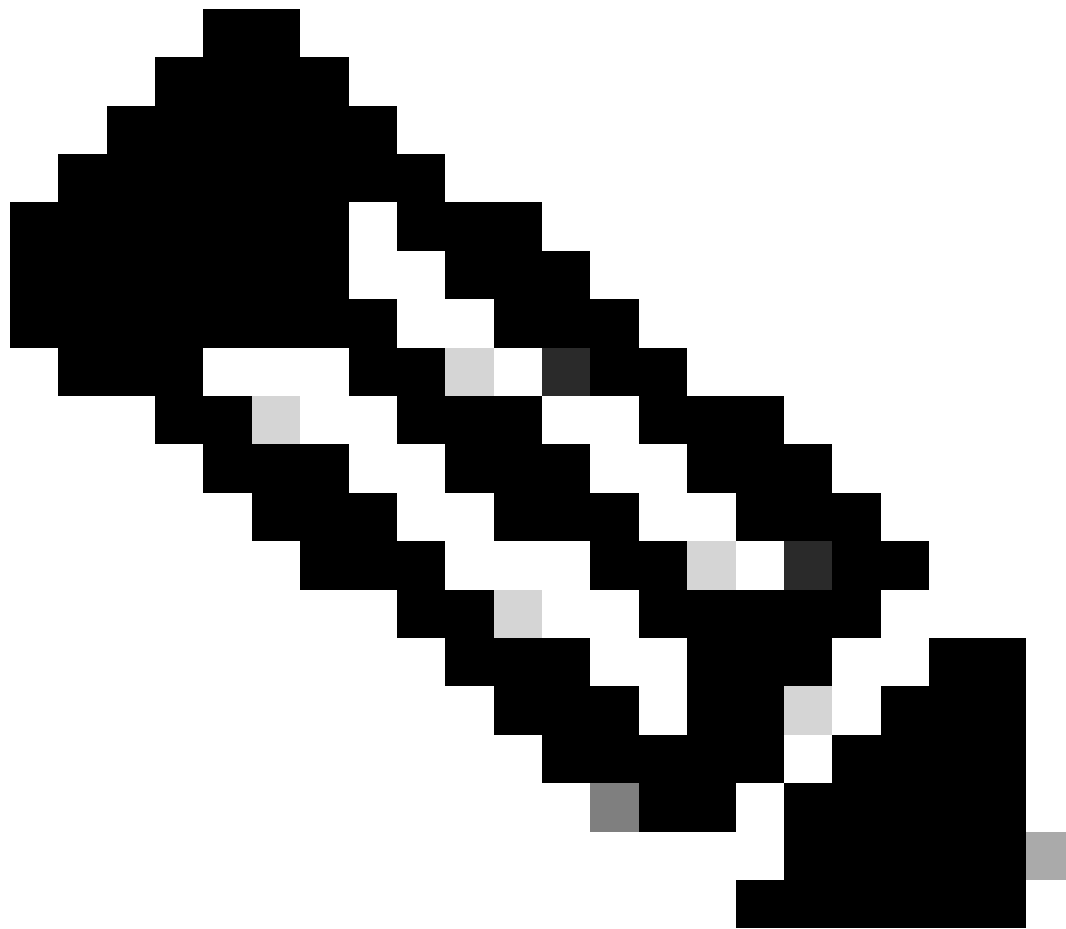
Cluster de origem:

- Endereço IP - 10.201.251.171
- FQDN - cucm1052.domain.com
- Versão: 12.5.1.16065-1

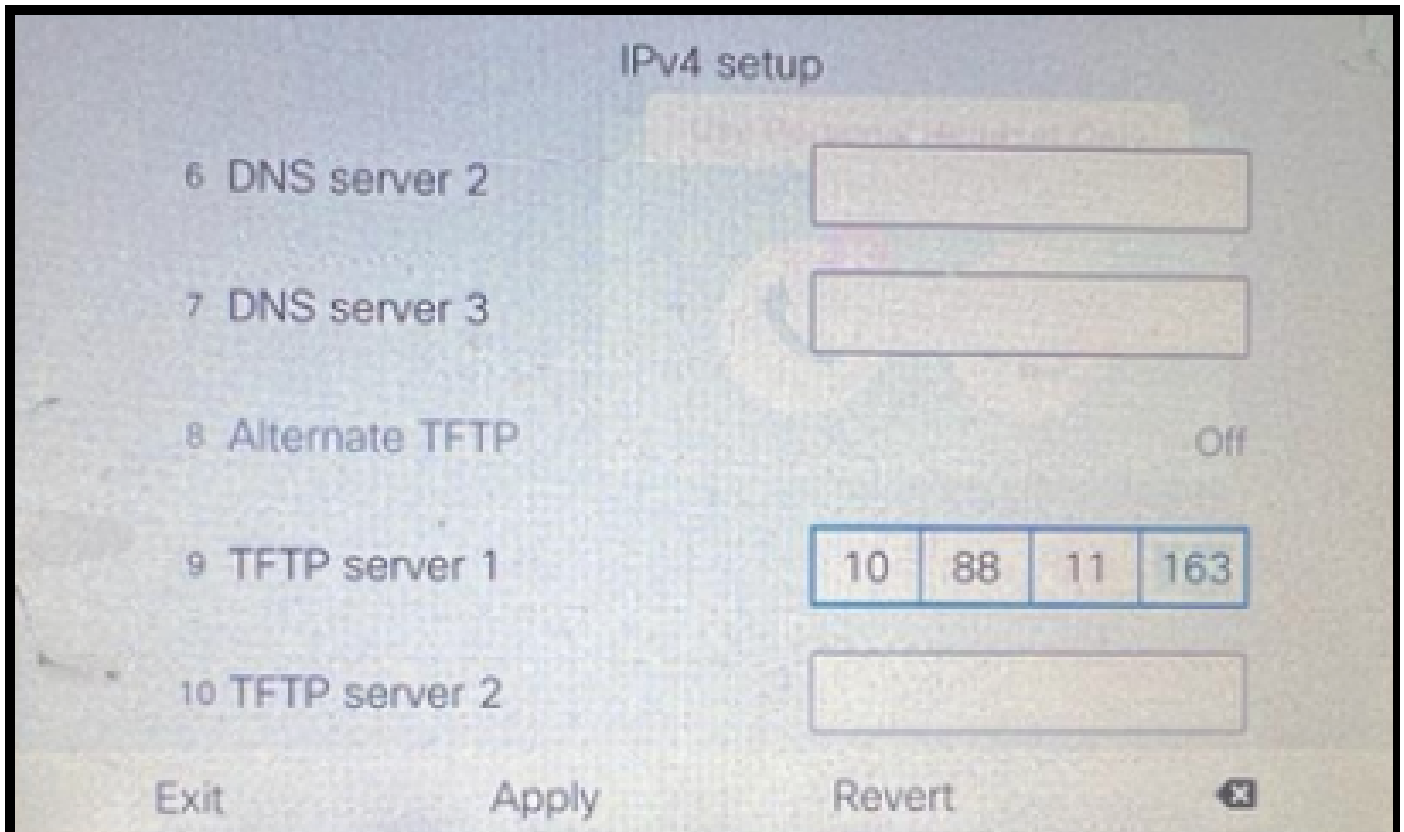
Cluster de destino:

- Endereço IP - 10.88.11.163
- FQDN - cucmpub.domain.com
- Versão: 12.5.1.14900-63

No telefone físico, defina o valor do TFTP Server 1 como o novo endereço IP do cluster de destino e clique no botão Apply.

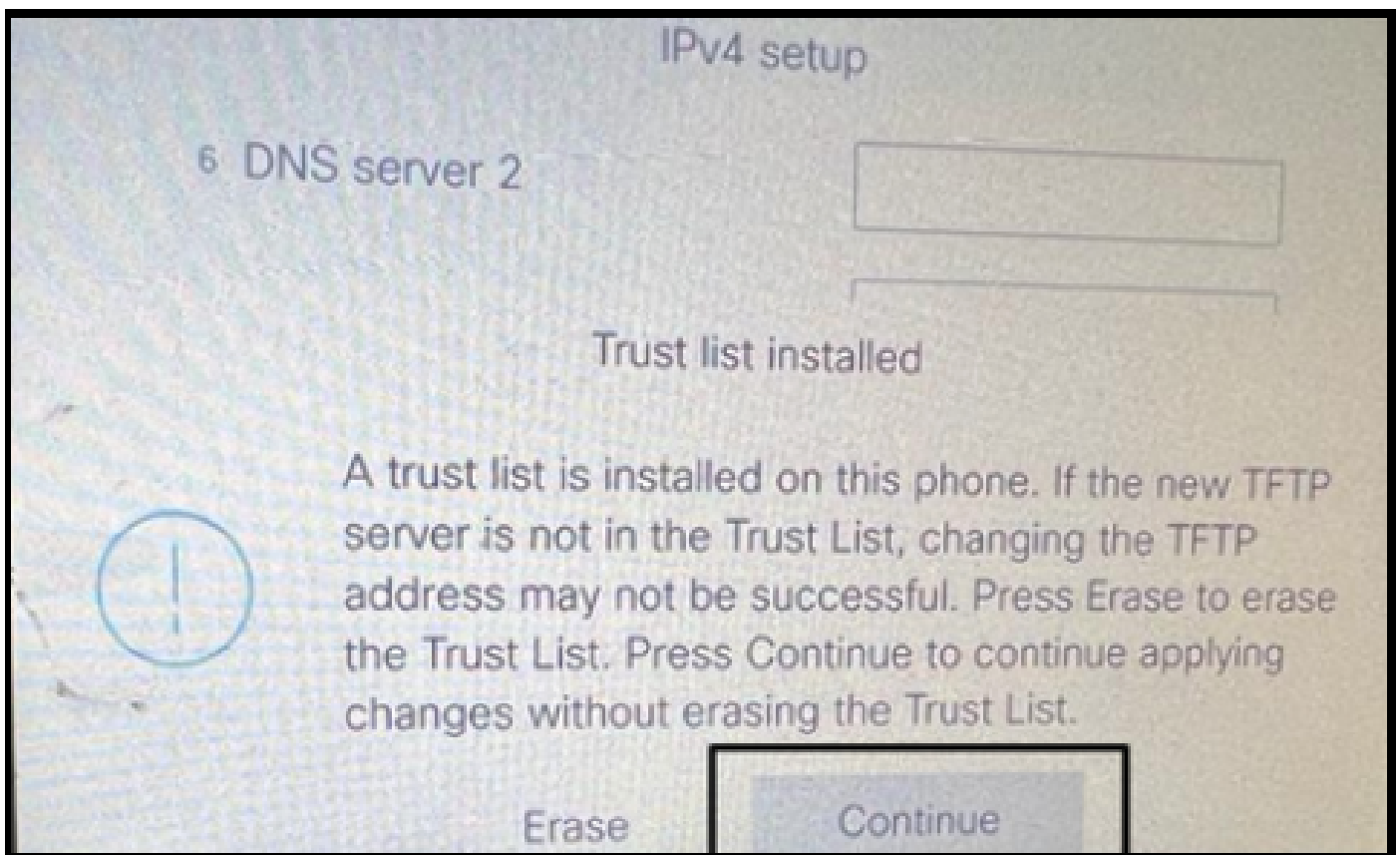


Observação: esse processo é equivalente a alterar o IP do TFTP no escopo do DHCP - opção 150 / 66. Se o cluster de destino estiver em um domínio diferente, você também terá que definir os servidores DNS apropriados no escopo do DHCP.



Configurar o IP TFTP no telefone

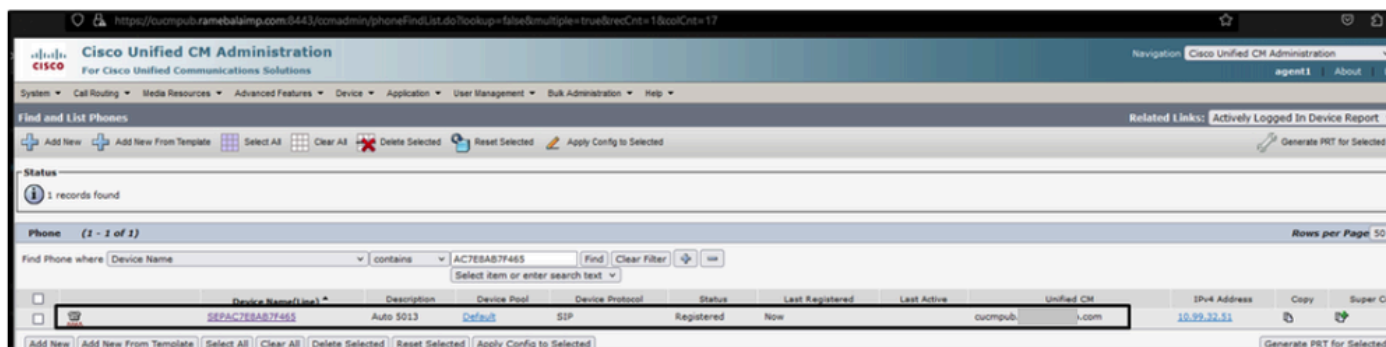
Clique no botão Continuar, que retém os arquivos CTL e ITL antigos (contém somente a entrada CAPF) do cluster de origem.



Pressionar o botão Continuar pode reter os arquivos CTL e ITL antigos

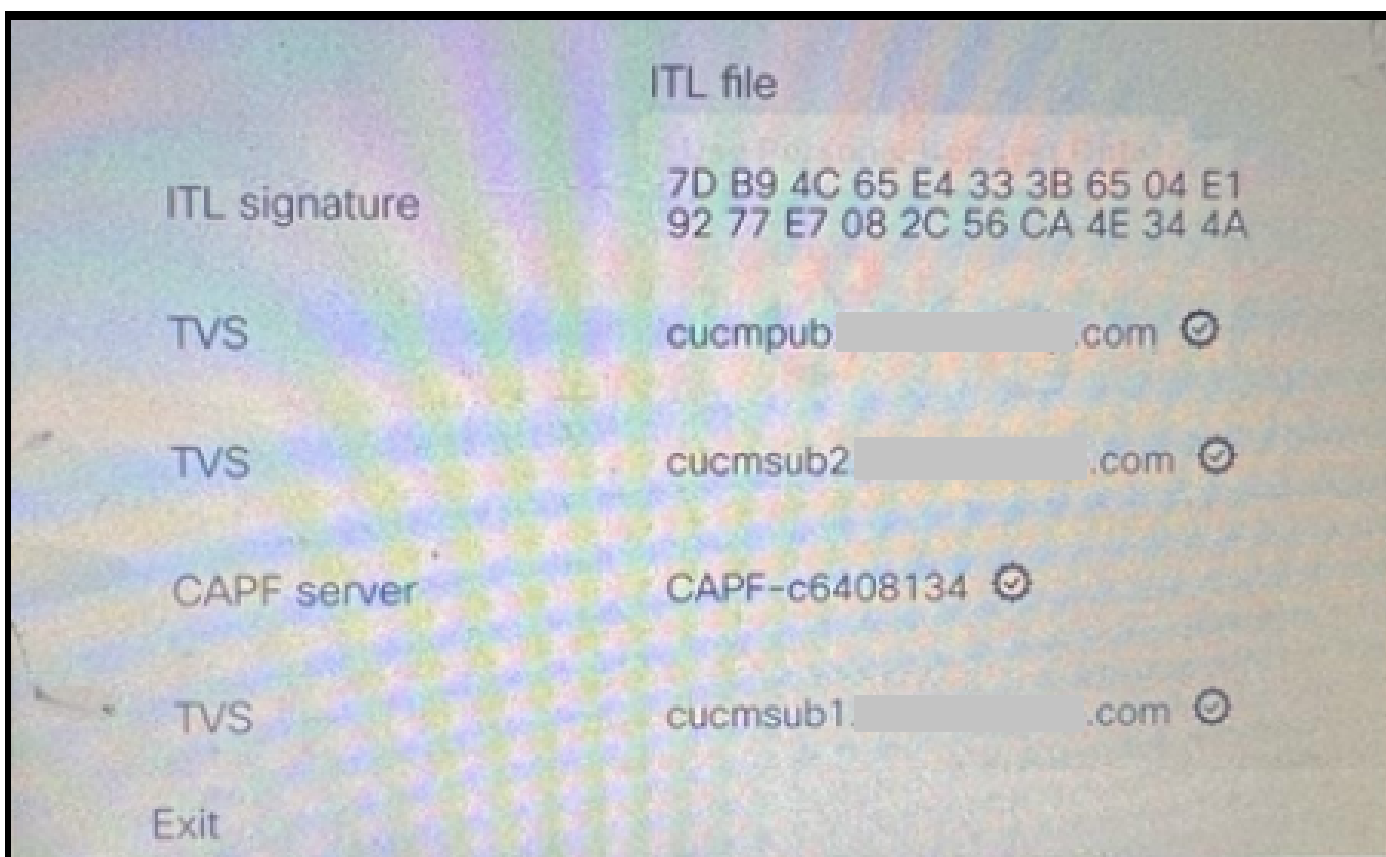
Verificar

O telefone está registrado no cluster de destino com êxito.



Telefone registrado no CUCM

O telefone contém as entradas da lista de confiança do cluster de destinos.



Arquivo ITL no telefone

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Entender a segurança do CUCM por padrão e a operação e solução de problemas do ITL](#)
- [Modo combinado de CUCM com CTL sem token](#)
- [Guia de segurança do Cisco Unified Communications Manager, versão 12.5\(1\)](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.