セキュアから非セキュアCUCMへのIPフォンの移行のデモンストレーション

内容

はじめに

このドキュメントでは、セキュアなCisco Unified Communication Manager(CUCM)から非セキュアなCUCMに電話機を移行するためのベストプラクティスの1つについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CUCM
- IP フォン

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- CUCMバージョン – 12.5.1.16065-1および12.5.1.14900-63
- IP Phoneモデル – 8865およびバージョン – 12.8(1)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図

IP_Phone > Ciscoスイッチ> Ciscoルータ> Ciscoスイッチ> CUCMクラスタ

コンフィギュレーション

次のシナリオでは、セキュアなCUCMクラスタから非セキュアなCUCMクラスタへの電話機の移行について説明します。各段階では、電話機の証明書信頼リスト(CTL)ファイルとID信頼リスト(ITL)ファイルのステータスが文書化されます。

1. 電話機を非セキュアCUCMクラスタに登録します。
2. 非セキュアクラスタをセキュアCUCMクラスタに変換します。
3. セキュリティで保護されていないクラスターに変換し直します
4. 電話機を新しい非セキュアCUCMクラスタに移行します。

1. 非セキュアCUCMクラスタへの電話機の登録

これらは、非セキュアなソースクラスタに関する情報です。

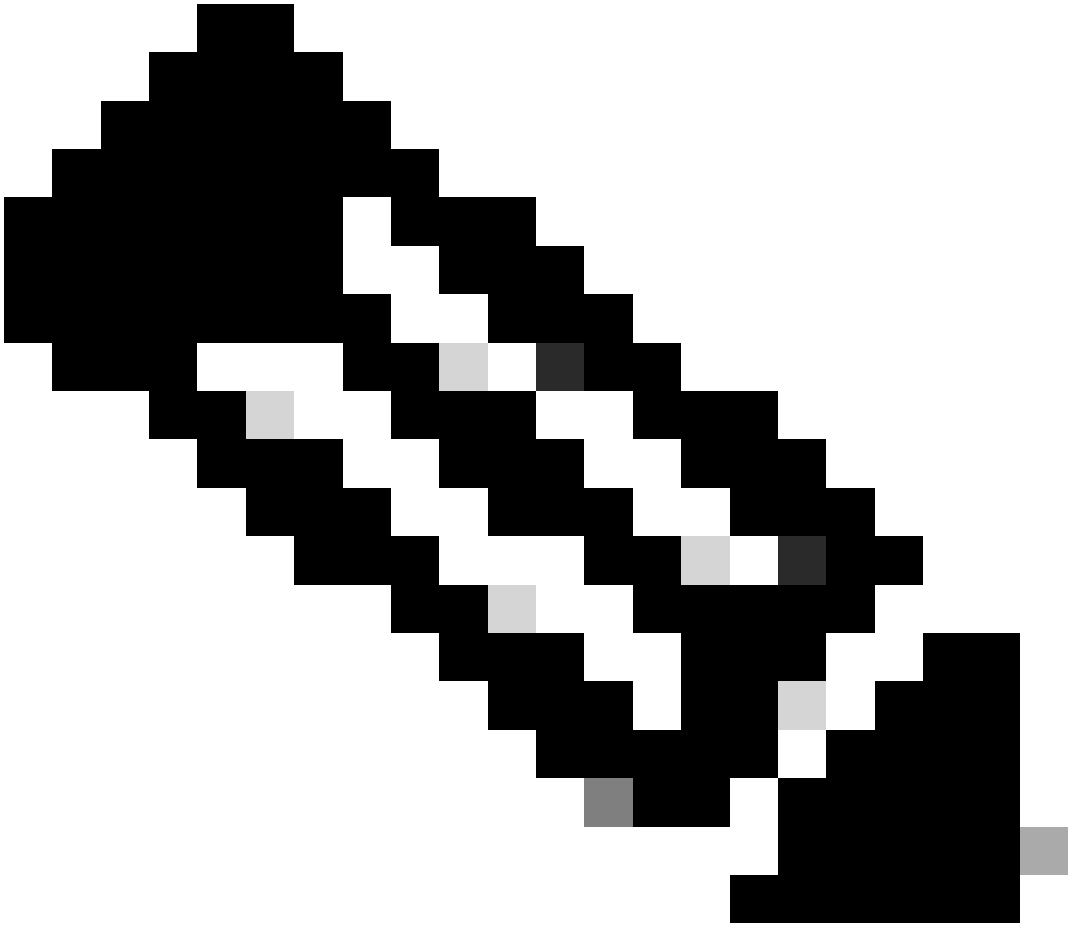
- IPアドレス：10.201.251.171
- FQDN:cucm1052.domain.com
- バージョン：12.5.1.16065-1

電話機を非セキュアCUCMクラスタに登録します。このため、Trivial File Transfer Protocol(TFTP)のIPアドレス（TFTPサービスがオンになっているCUCMノード）を指すようにDynamic Host Configuration Protocol(DHCP)オプション150 / 66を設定します。

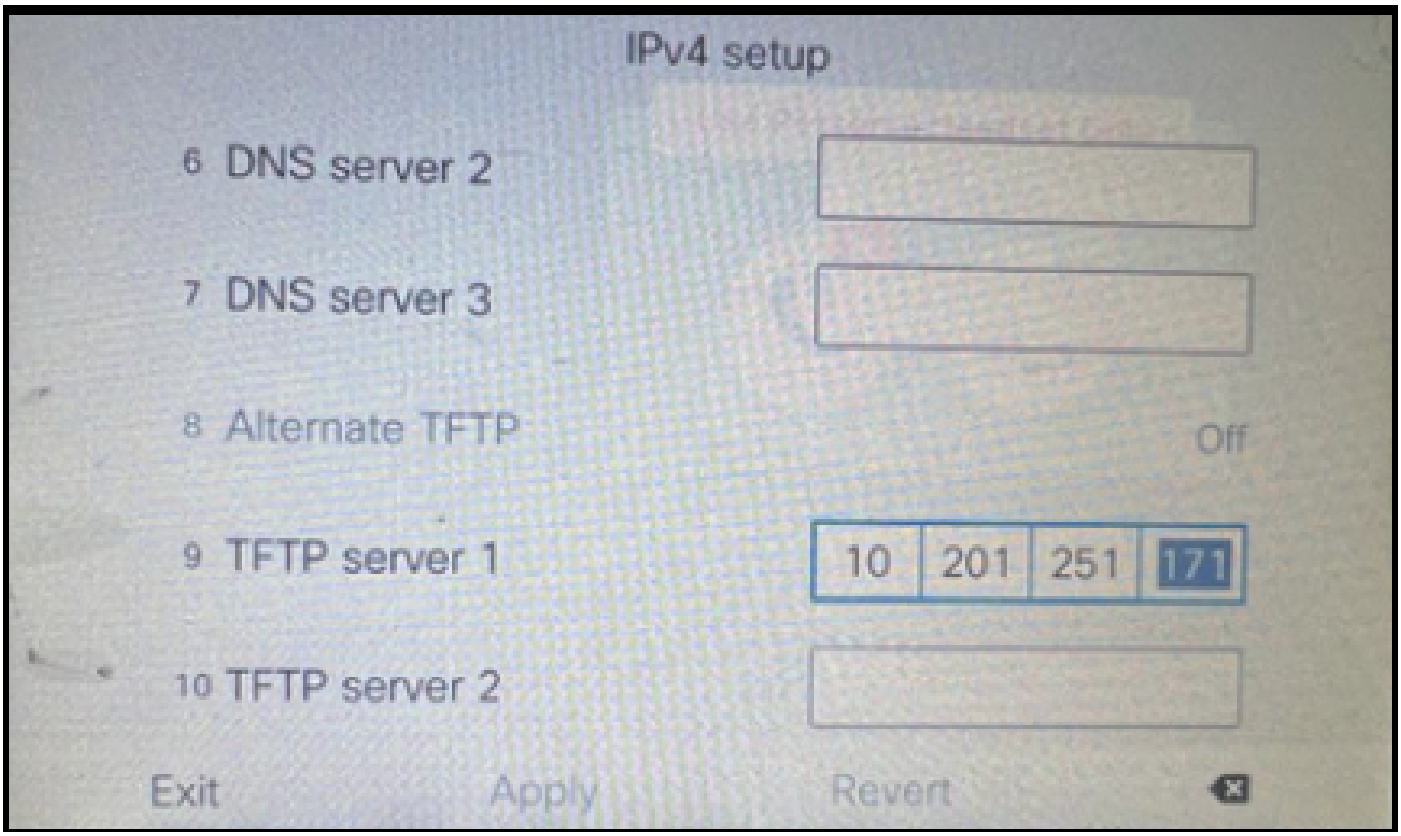
DHCPサーバが存在しないインフラストラクチャでは、物理的な電話機でTFTP IPを手動で設定する必要があります。

物理的な電話機で、Settings > Admin Settings > Network Setup > Ethernet setup > IPv4 setupの順に移動します。

DHCPをオフにし、ネットワークの静的IPの詳細を入力します。その後、スクリーンショットに示すように、TFTPサーバ1セクションに非セキュアCUCM IPを指定します。

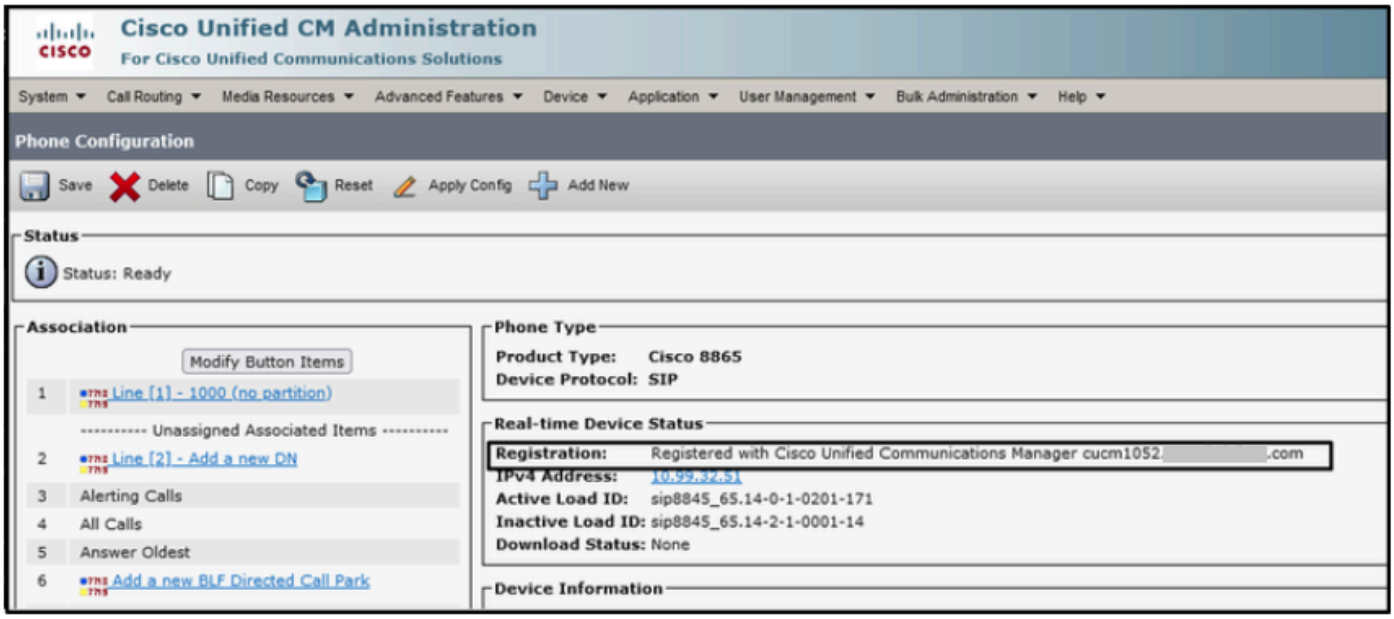


注：このプロセスは、DHCPスコープのTFTP IPを変更するオプション150 / 66と同じです。また、クラスタにドメイン名が設定されている場合は、DHCPスコープでも適切なドメインネームシステム(DNS)サーバを設定する必要があります。



電話機でのTFTP IPの設定

IPフォンは、前述の非セキュアCUCMクラスタに正常に登録されます。



CUCMに登録されている電話機

CUCM Administration Webインターフェイスにログインし、System > Enterprise Parametersの順に移動します。

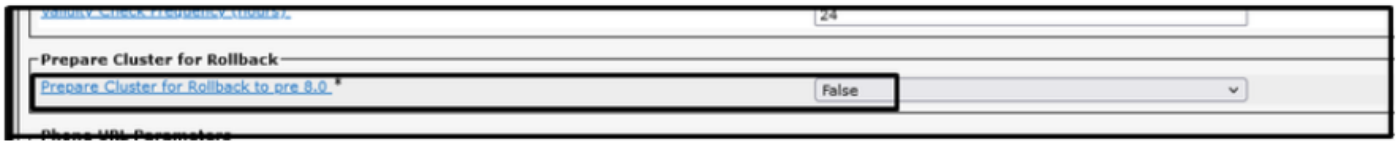
これらは、非セキュアCUCMクラスタのエンタープライズパラメータページで設定されたパラメータの値です。

- クラスタセキュリティモードが0に設定されている場合、クラスタが非セキュアであること

を確認します。

クラスタセキュリティモードが0に設定されている

- Prepare Cluster for Rollback to pre 8.0がFalseに設定されている。したがって、ITLファイルとCTLファイルの内容は適切な値で保持されます。



Prepare Cluster for Rollback to pre 8.0がFalseに設定されている

クラスタは非セキュアなので、TFTPサーバにはCTLファイルがありません。このことは、CUCMノードのセキュアシェル(SSH)セッションでコマンドshow ctlを実行することで確認できます。

```
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ファイルがありません

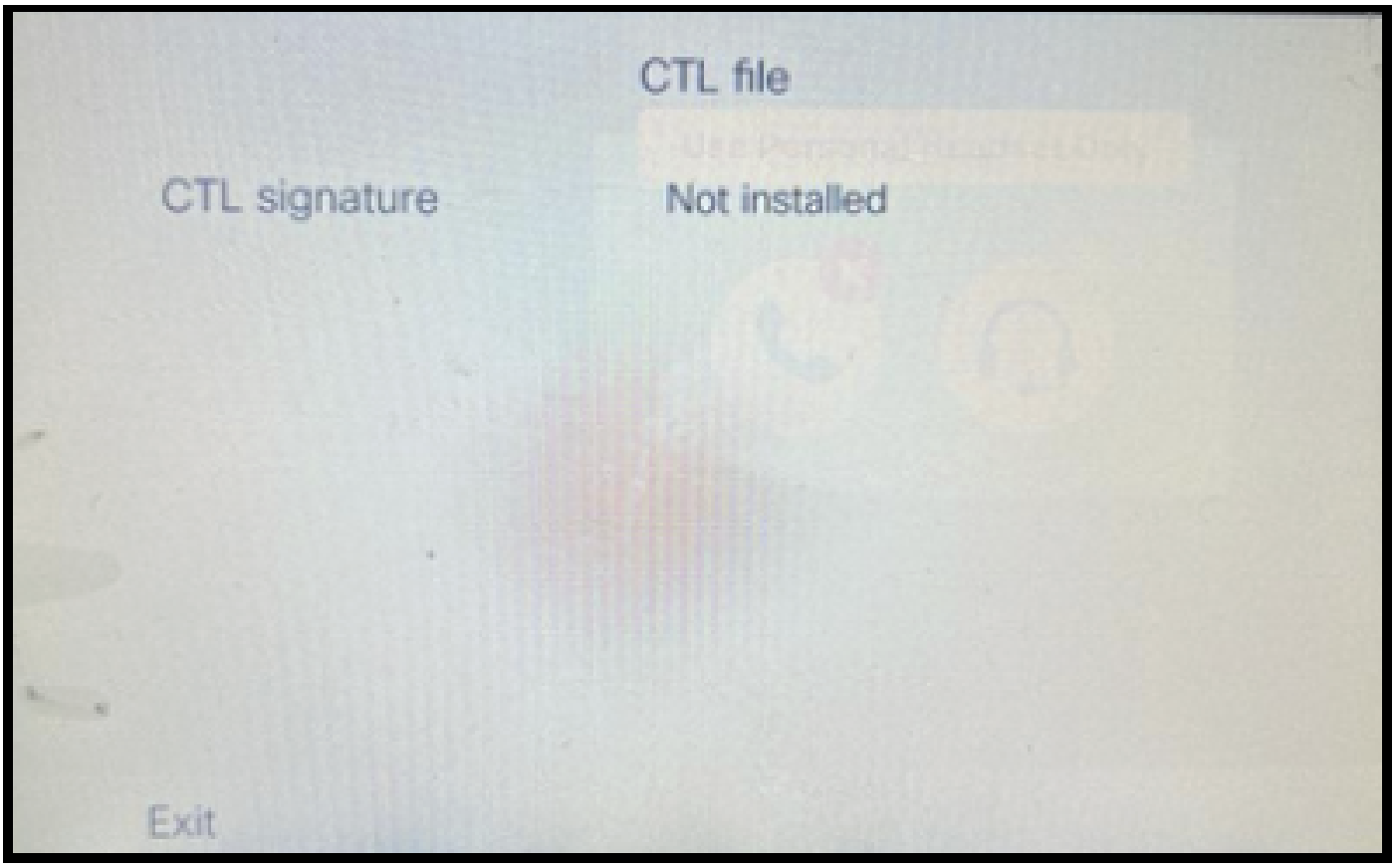
物理的な電話機で、CTLファイルがインストールされていないことを確認できます。ただし、ITLファイルは表示されます。

ITLは、CUCMのデフォルトのセキュリティ(SBD)機能により存在します。SBDの詳細については、ここをクリックしてください。

物理的な電話機で、Settings > Admin settings > Security setup > Trust listの順に移動します。

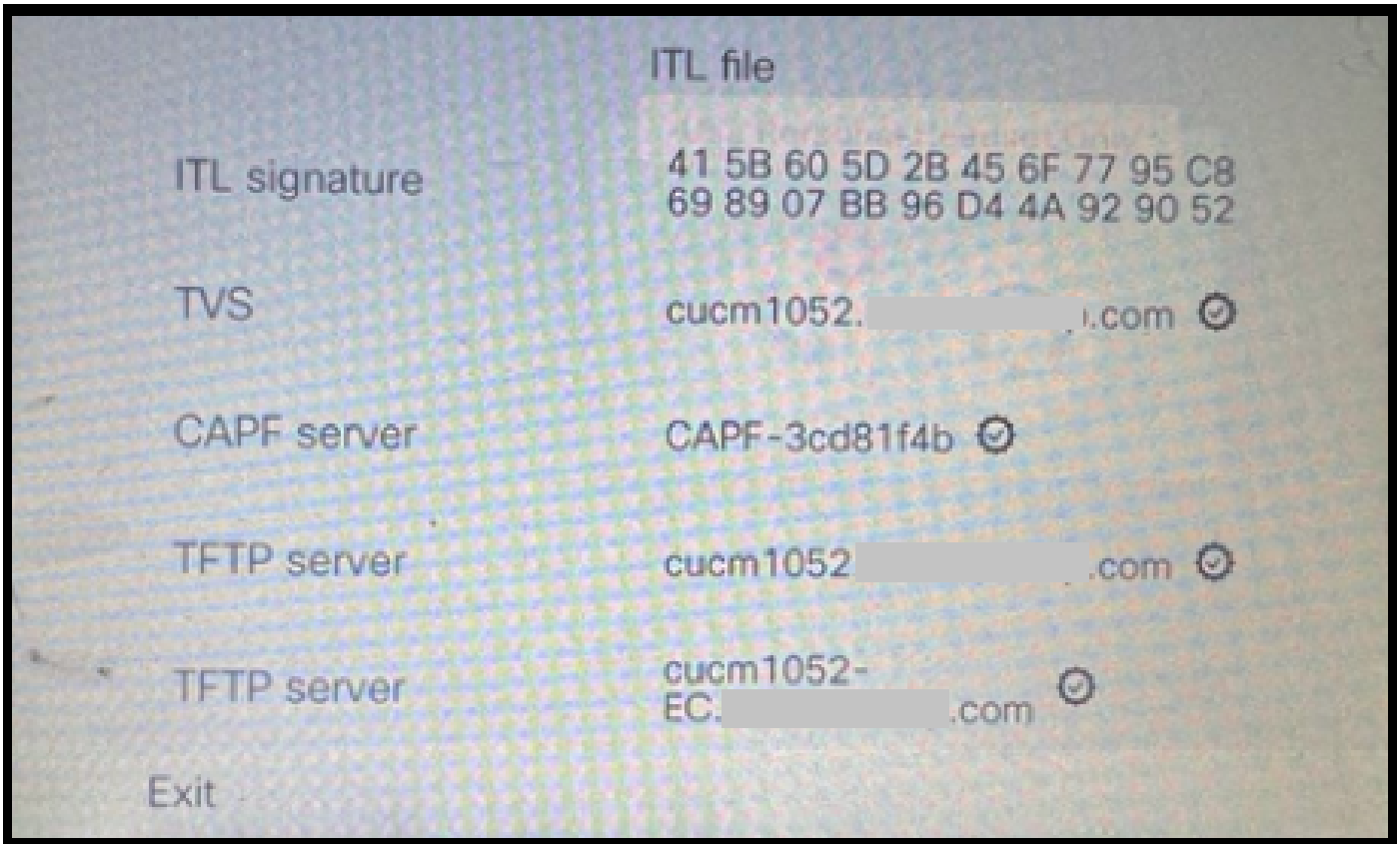
ここでは、CTLファイルとITLファイルの両方のステータスを確認できます。

CTIが電話機にインストールされていない。



電話機のCTLファイル

電話機にITLファイルがある。



電話機のITLファイル

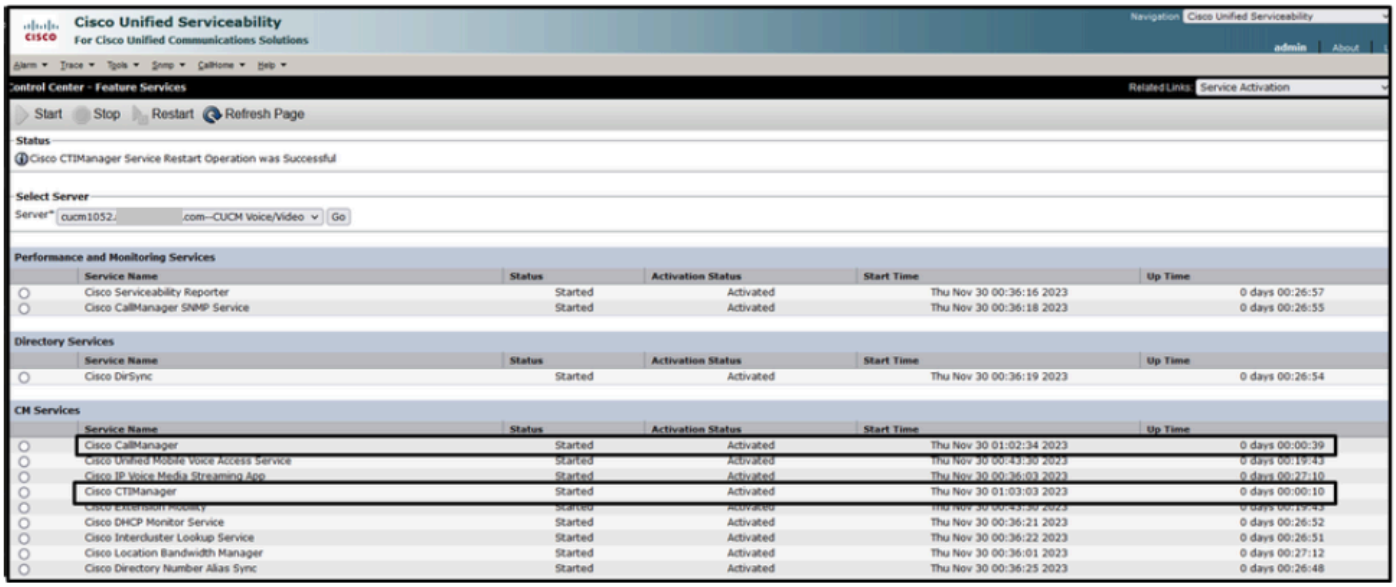
2. 非セキュアクラスタをセキュアCUCMクラスタに変換する。

CUCMパブリッシャのコマンドラインインターフェイス(CLI)でコマンドutils ctl set-cluster mixed-modeを実行して、混合モードを有効にします。これにより、クラスタが非セキュアからセキュアに変換されます。

```
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:
```

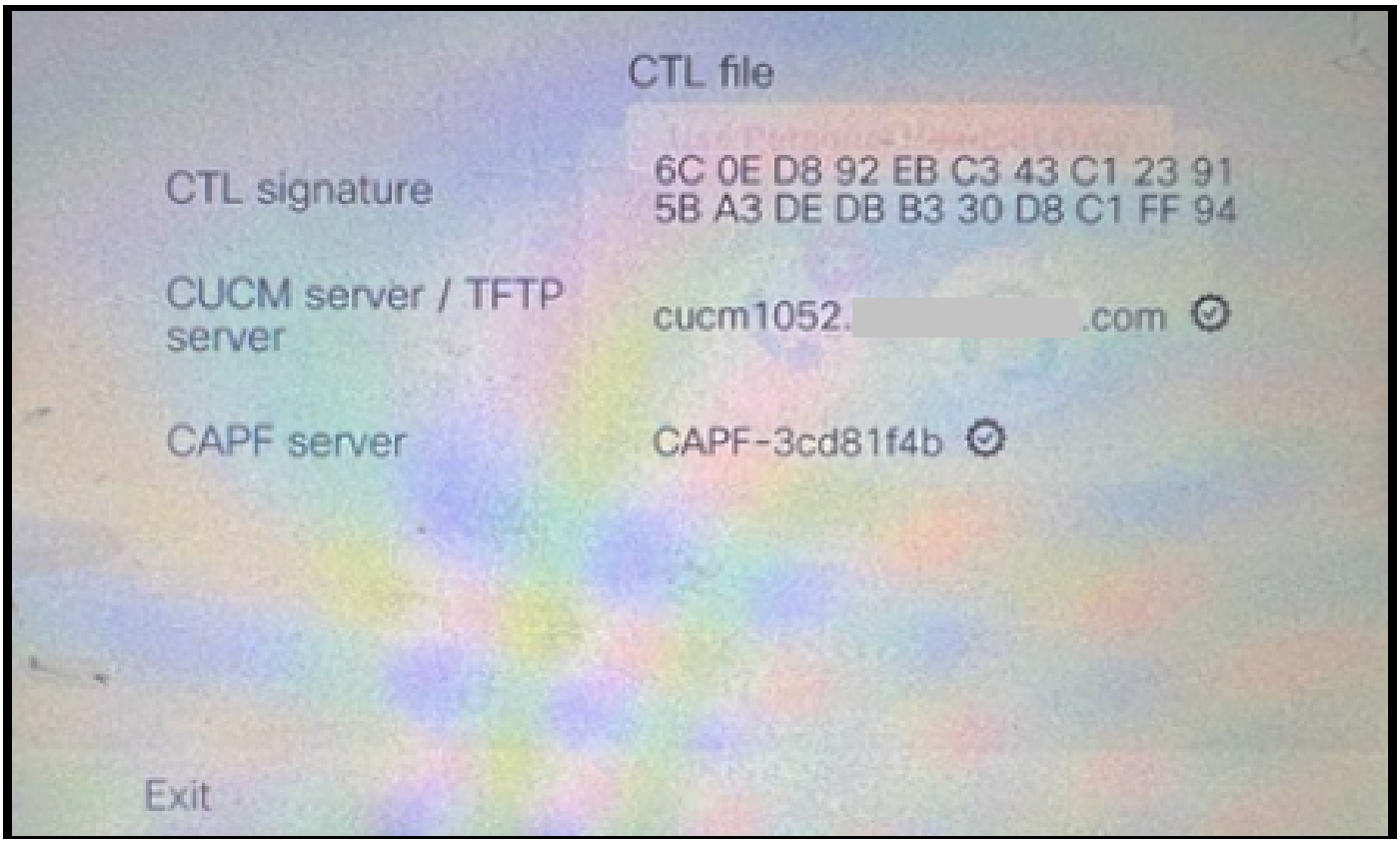
セキュアクラスタへの変換

コマンドを実行した後、クラスタ内のすべてのノードでCisco CallManager(CCM)およびCisco CTIManager(CTI)サービスを再起動します。



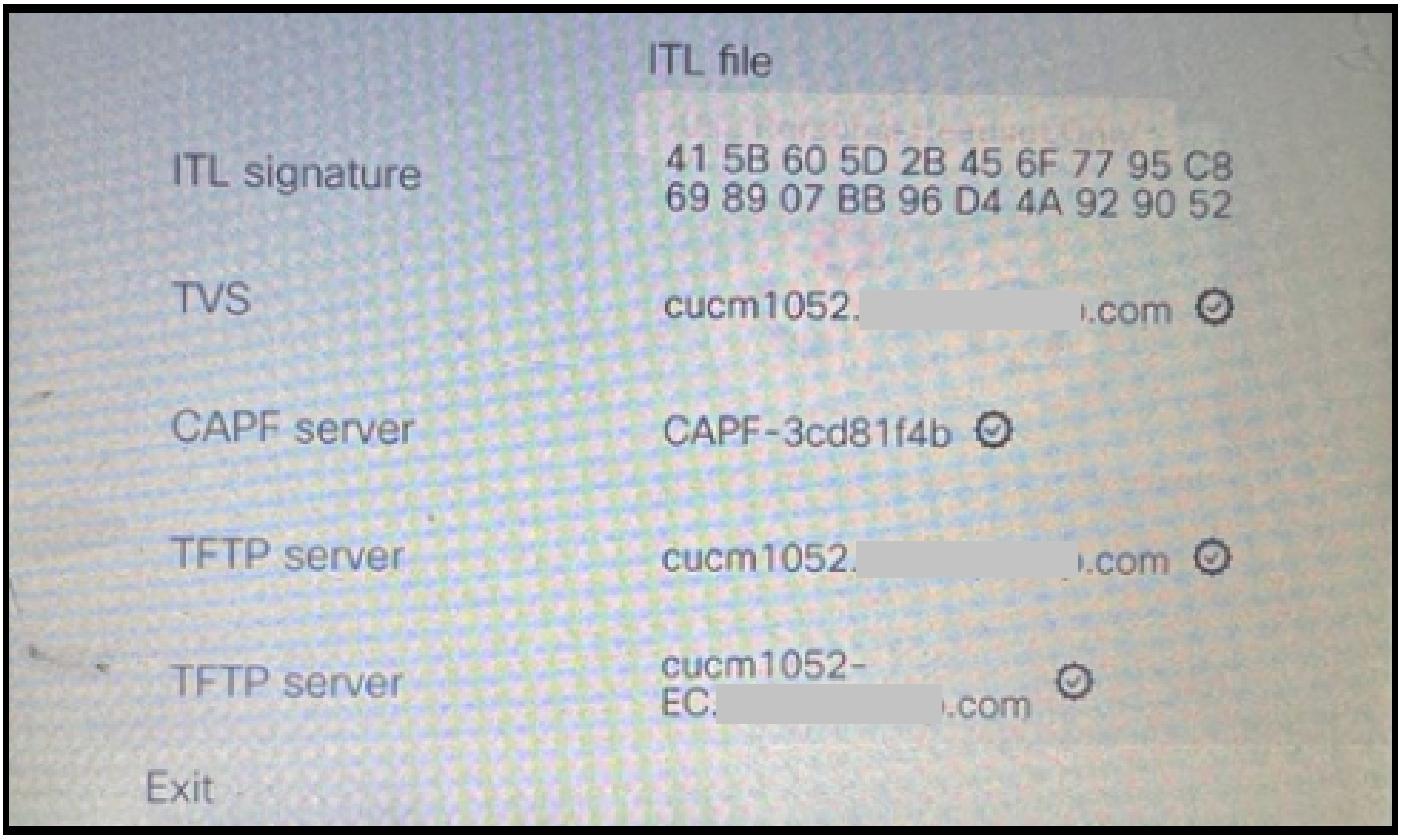
CCMおよびCTIサービスの再起動

ここで、物理的な電話機で、CTLファイルの存在を確認できます。



電話機のCTLファイル

ITLファイルは同じ値のままです。



電話機のITLファイル

3. セキュリティで保護されていないクラスターをセキュリティで保護されたクラスターから保護

されていないクラスターに変換します。

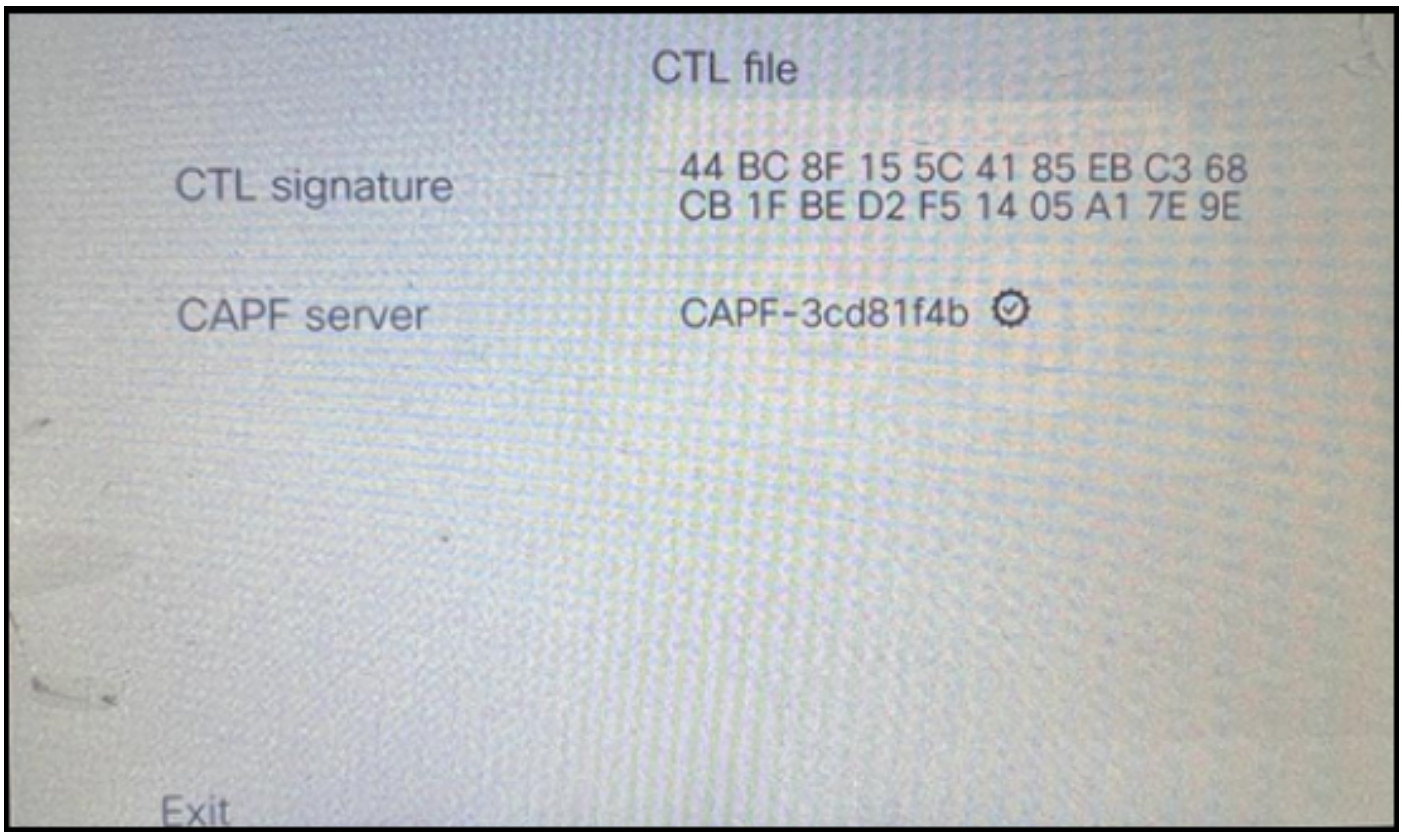
クラスタをセキュアから非セキュアに変換するには、CUCMパブリッシャのCLIでコマンドutils ctl set-cluster non-secure-modeを実行する必要があります。

```
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:
```

非セキュアクラスタへの変換

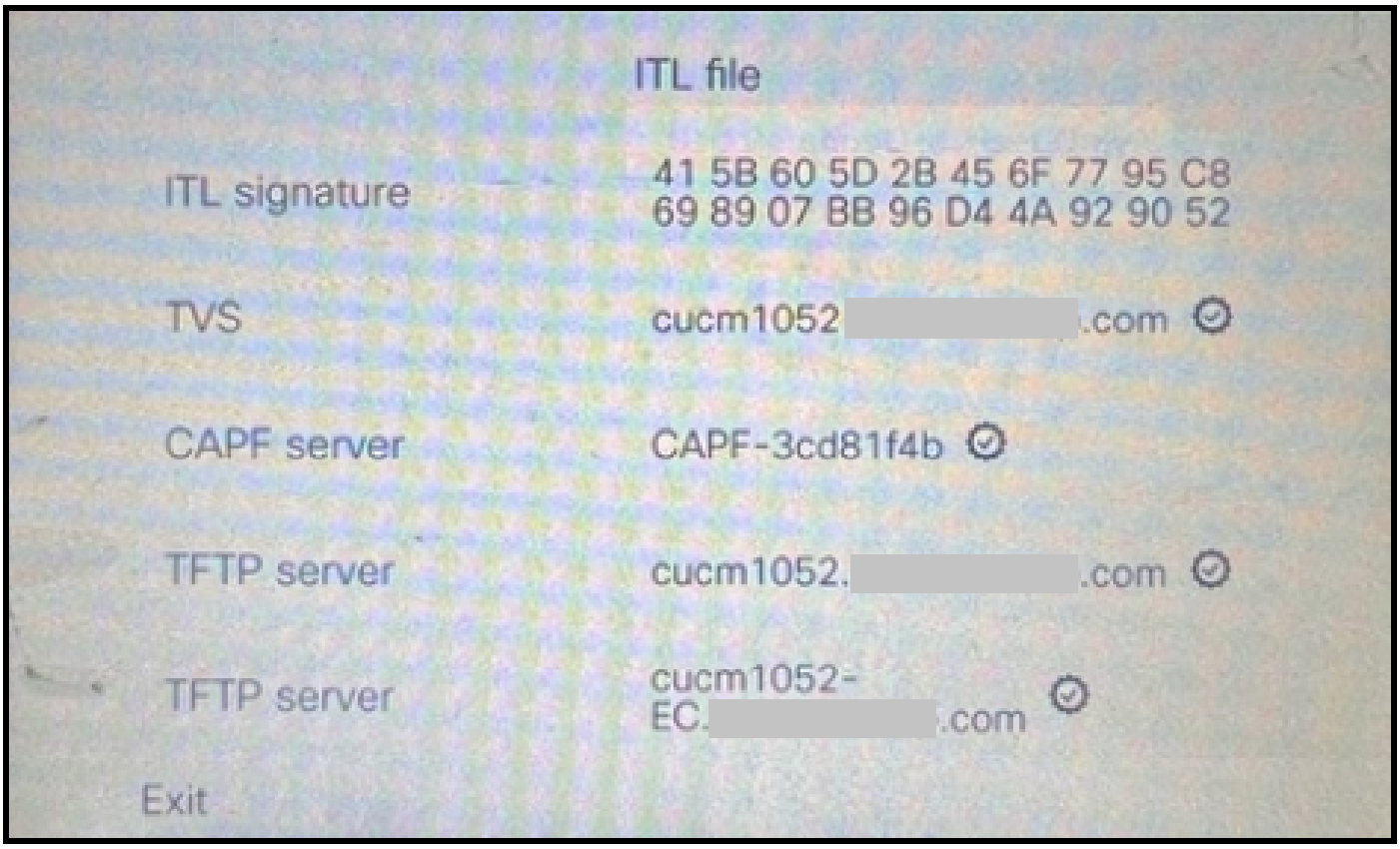
クラスタ内のすべてのノードでCCMサービスとCTIサービスを再起動して、CUCMクラスタ内のすべてのノードに変更を反映させます。

クラスタを非セキュアに変換した後、CTLにはCUCMおよびTFTPエントリは含まれません。CTLファイルにはCAPFエントリだけが含まれています。

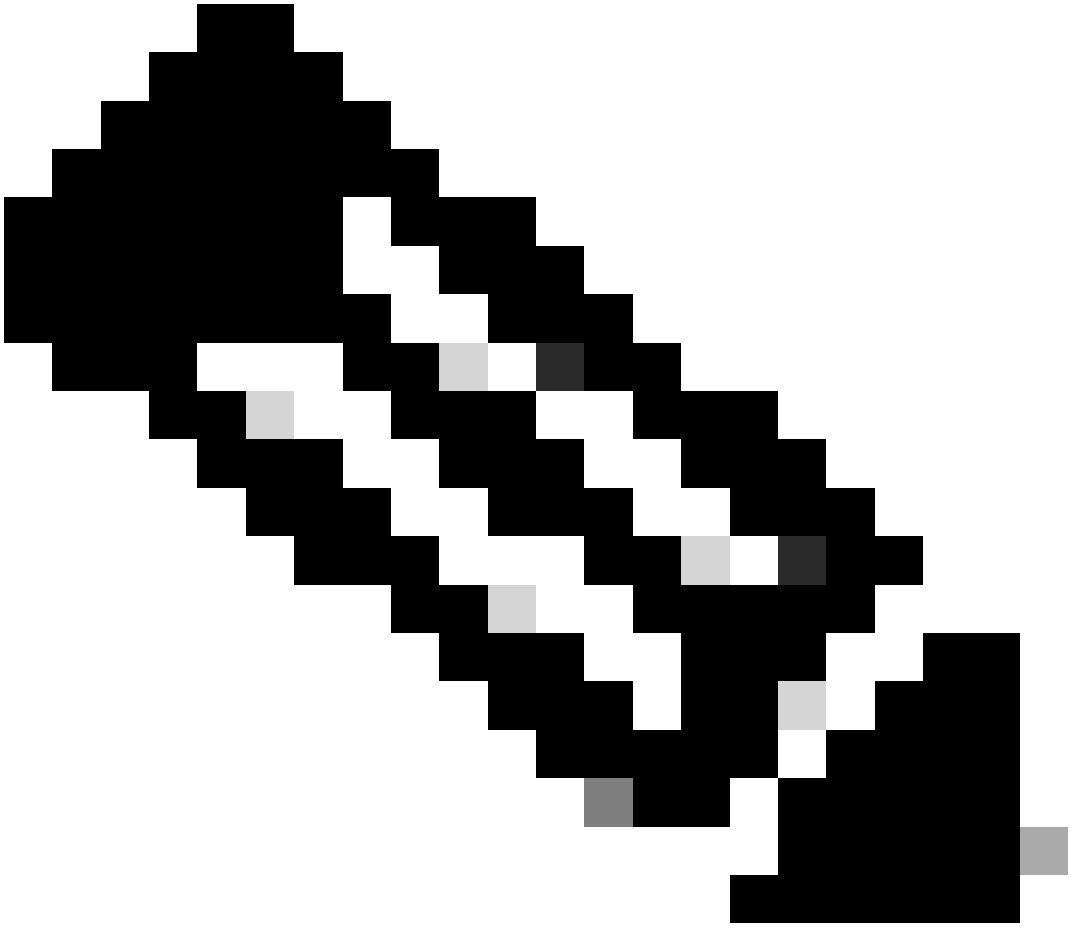


電話機のCTLファイル

ITLファイルは同じエントリのままです。

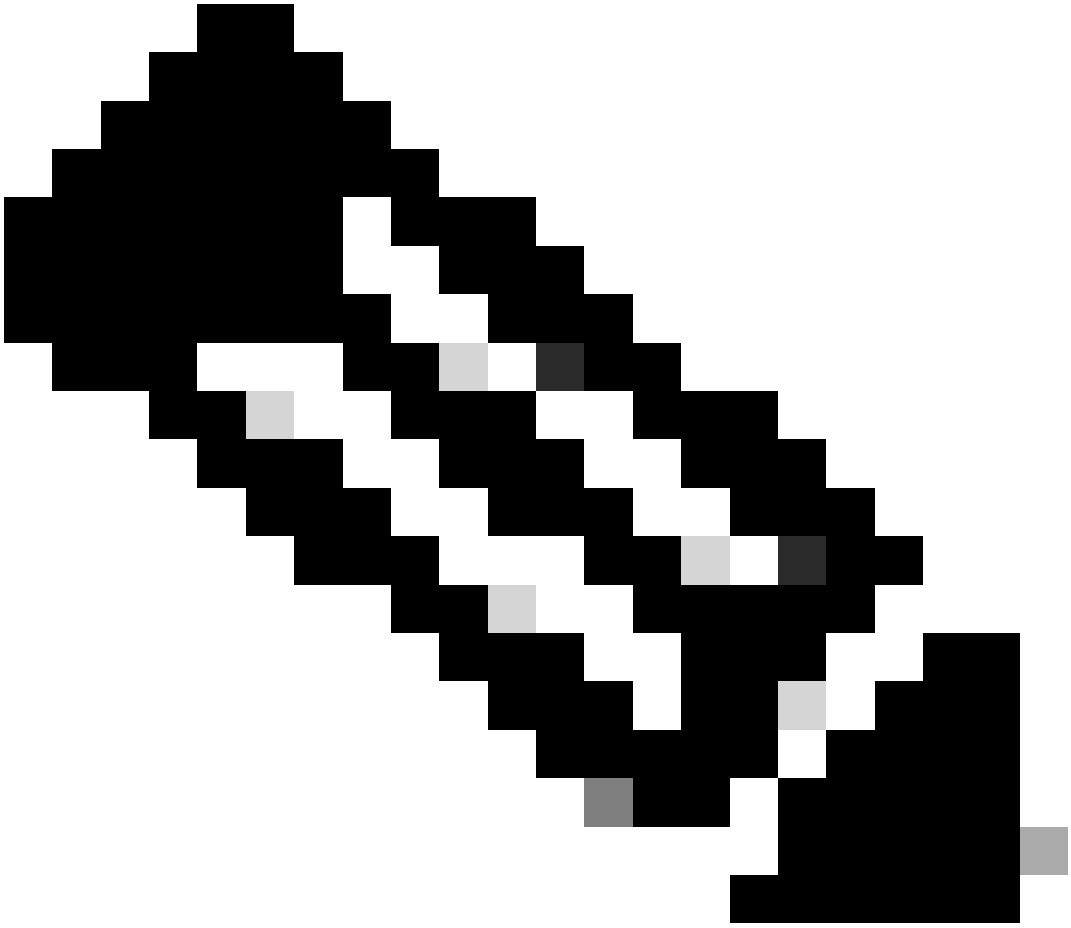


電話機のITLファイル



注：CUCM Administration Webページの電話設定ページでDevice Security ProfileをSecureまたはNon-secureに変更しても、ITLファイルやCTLファイルには影響しません。したがって、以前の設定をそのまま保持し、変更する必要はありません。

4. 電話機を新しい非セキュアCUCMクラスタに移行する。

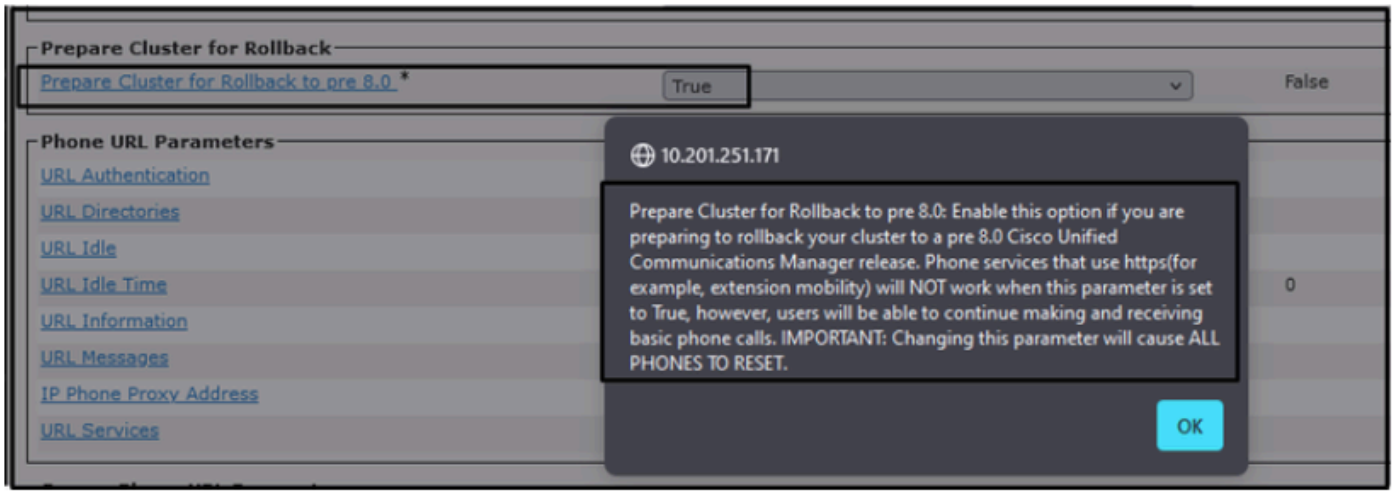


注：移行を開始する前に、移行元クラスタ内のすべてのノードで（これらのサービスが有効なノードでのみ）Trust Verification Service(TVS)とTFTPサービスを再起動することを推奨します。これにより、TVS/TFTPサービスでのハングまたはリークのセッションがなくなります。

CUCM Administration Webインターフェイスにログインし、System > Enterprise Parametersの順に移動します。

Prepare Cluster for Rollback to pre 8.0の値をTrueに設定します。続いてApply Configボタンと Resetボタンをクリックします。

このスクリーンショットには、このパラメータのヘルプセクションが示されています。

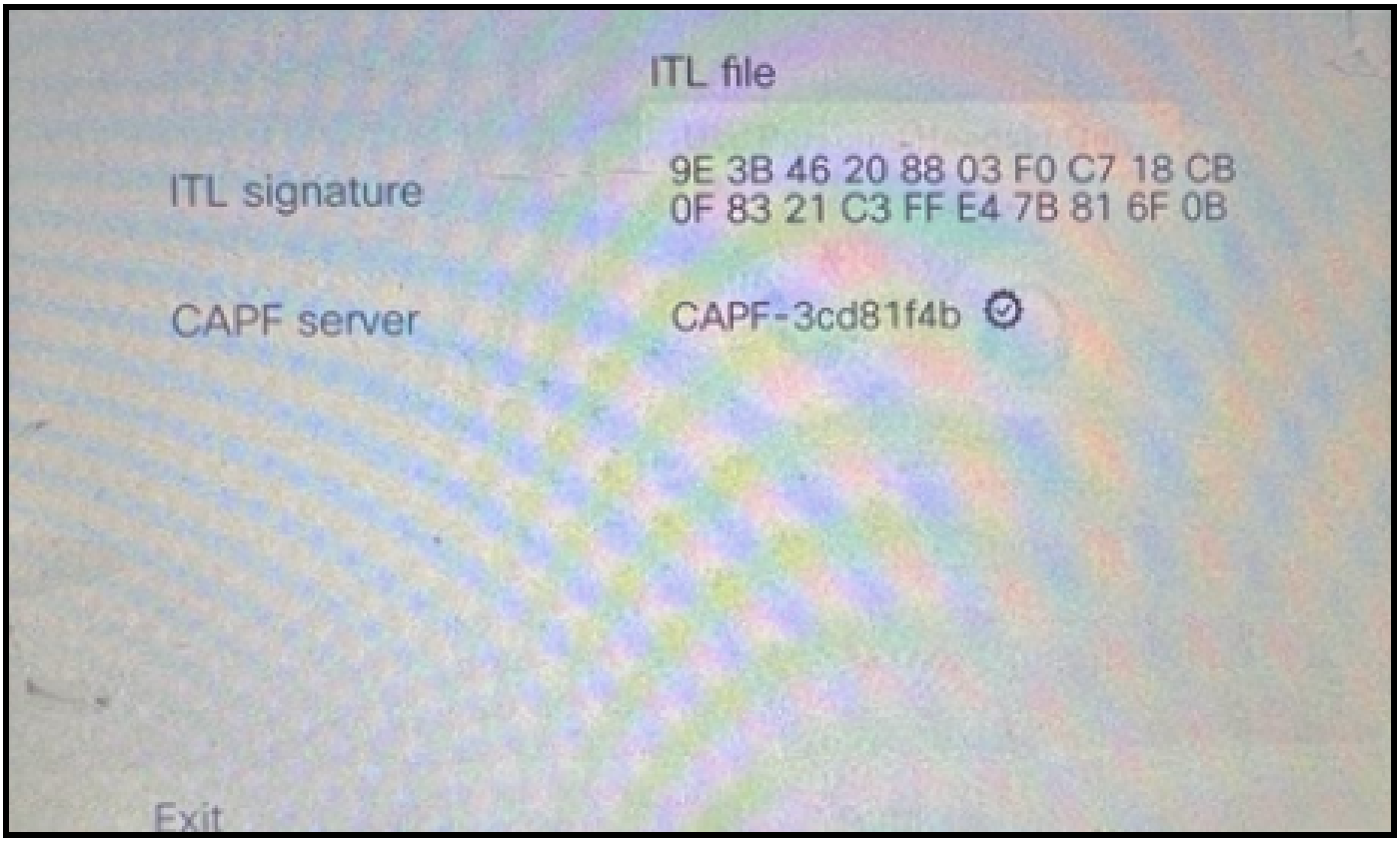


Prepare Cluster for Rollback to pre 8.0パラメータに関する情報

パラメータ値を変更する前後に、クラスタの電話登録数を監視します(Real Time Monitoring Tool(RTMT)を使用)。これにより、これらの変更がクラスタ内のすべてのデバイスに適用されるかどうかを検証できます。

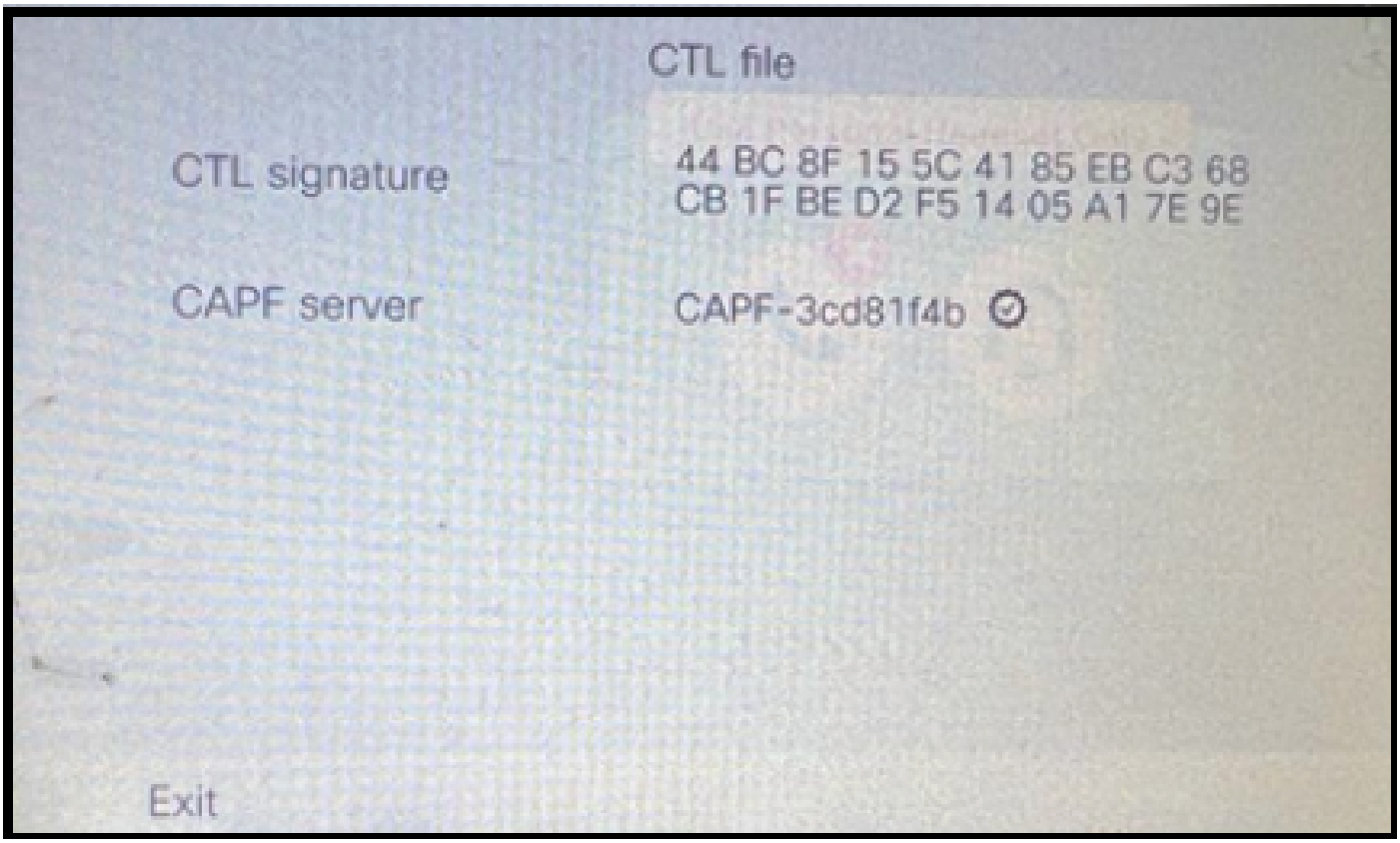
物理的な電話機では、ITLファイルとCTLファイルの両方にCAPFエントリだけが表示されていました。また、Webブラウザで電話機のWebページを開いて、これを確認することもできます。

ITLファイル



電話機のITLファイル

CTLファイル



電話機のCTLファイル

移行を開始する前に、いくつかの電話機でITLおよびCTLファイルを検証して、変更が行われたことを確認することをお勧めします。

これで、電話機は移行の準備が整いました。

電話機を移行元クラスタから移行先クラスタに移行します。現在、両方のクラスタは非セキュアです。

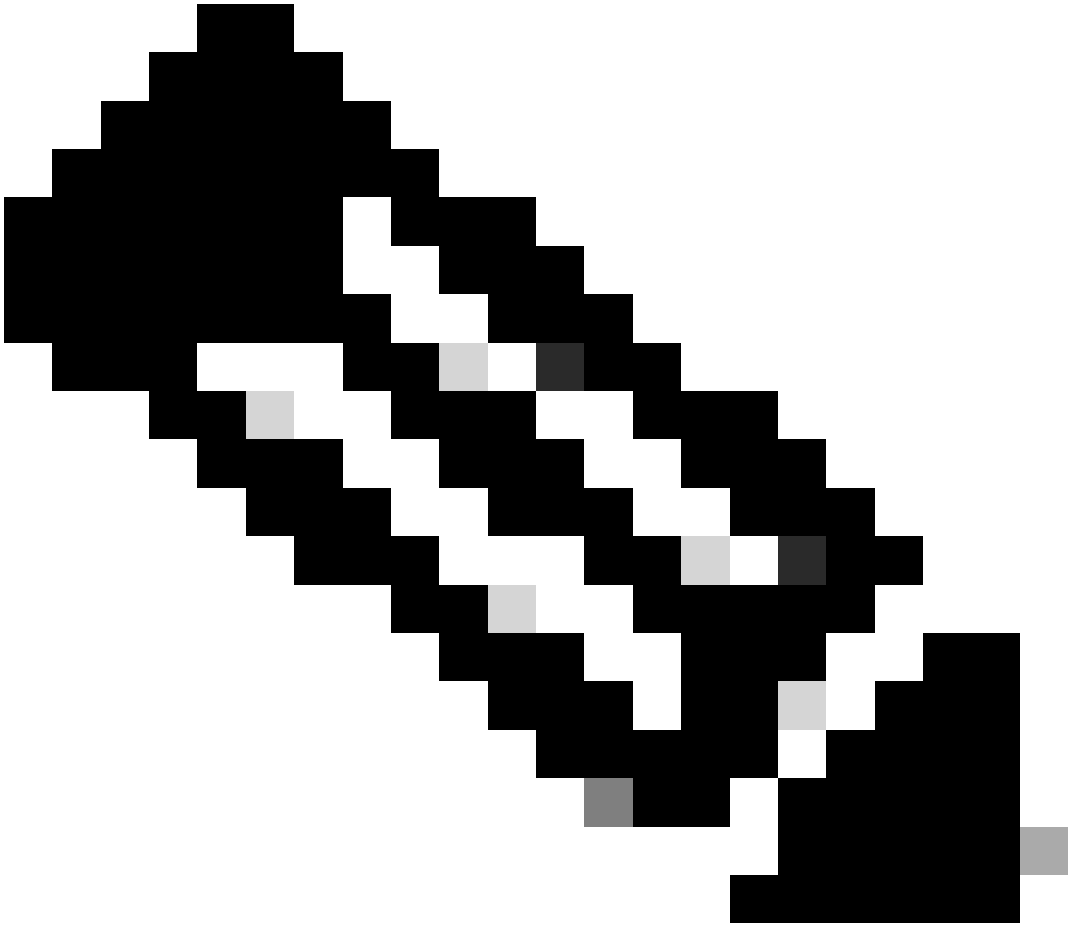
ソースクラスタ：

- IPアドレス：10.201.251.171
- FQDN:cucm1052.domain.com
- バージョン：12.5.1.16065-1

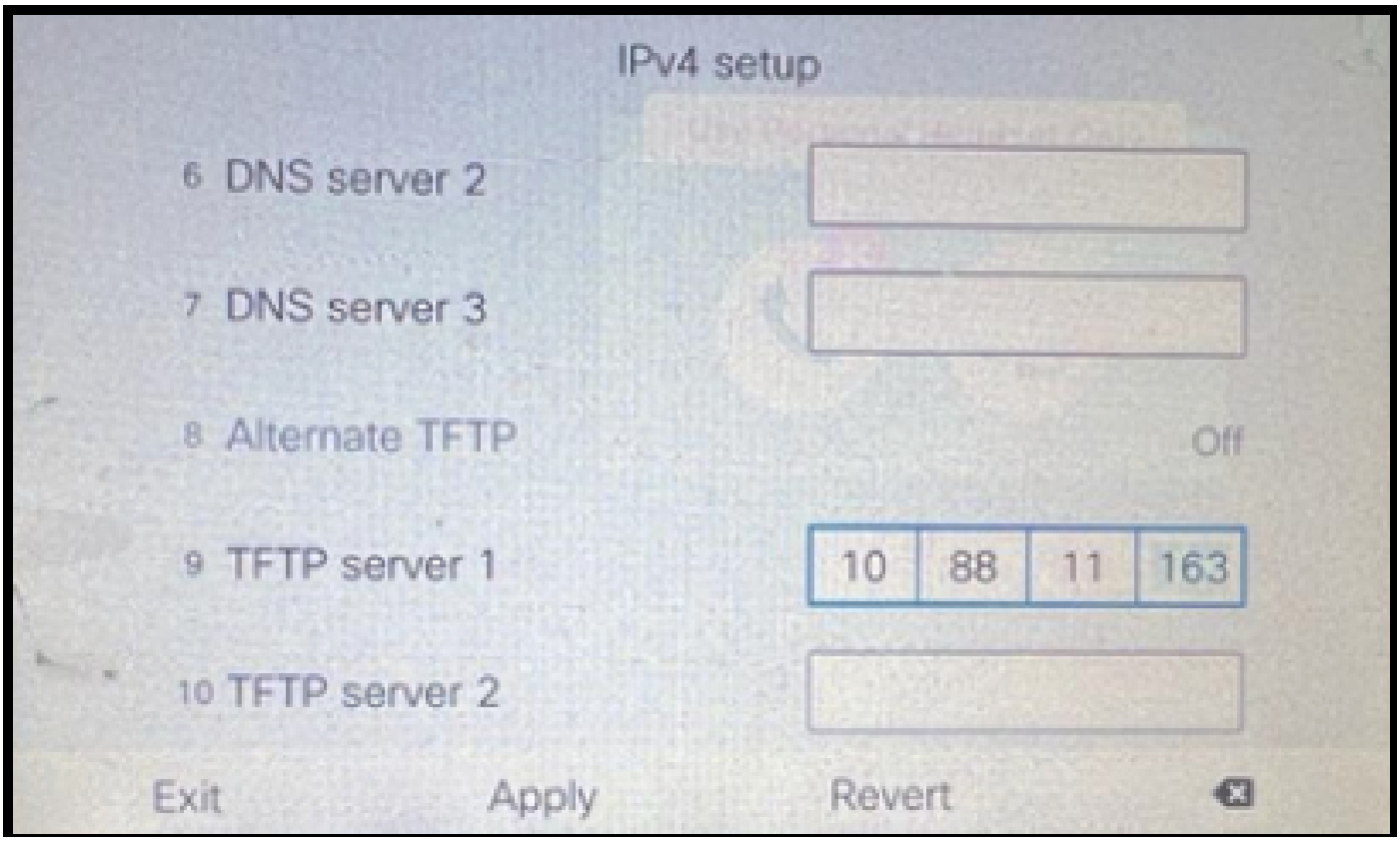
宛先クラスタ：

- IPアドレス：10.88.11.163
- FQDN:cucmpub.domain.com
- バージョン：12.5.1.14900-63

物理的な電話機で、TFTP Server 1の値をDestination new cluster IP addressに設定し、Applyボタンをクリックします。

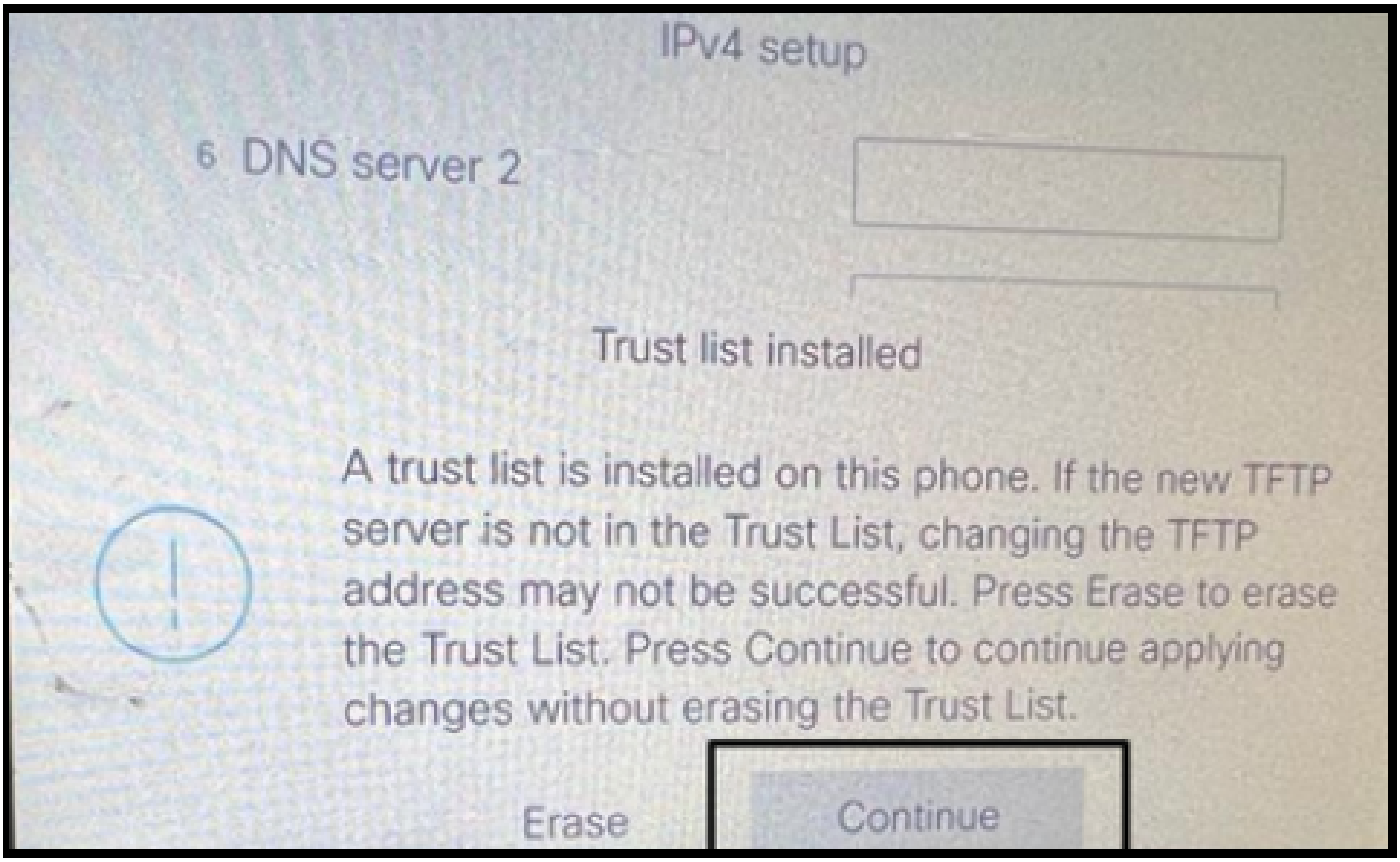


注：このプロセスは、DHCPスコープのTFTP IPを変更するオプション150 / 66と同じです。宛先クラスタが異なるドメインにある場合は、DHCPスコープでも適切なDNSサーバを設定する必要があります。



電話機でのTFTP IPの設定

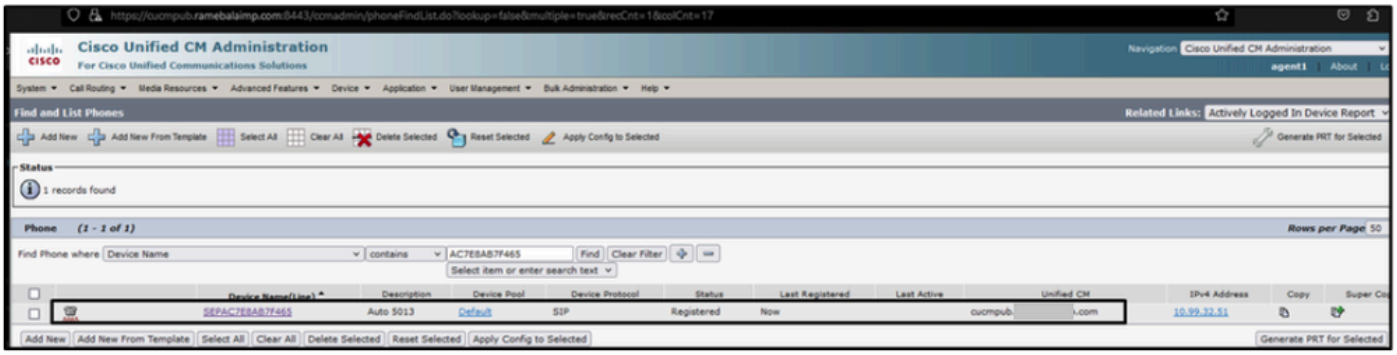
Continueボタンをクリックします。これにより、移行元クラスタの古いCTLファイルとITLファイル（CAPFエントリのみを含む）が保持されます。



Continueボタンを押すと、古いCTLファイルとITLファイルが保持されます

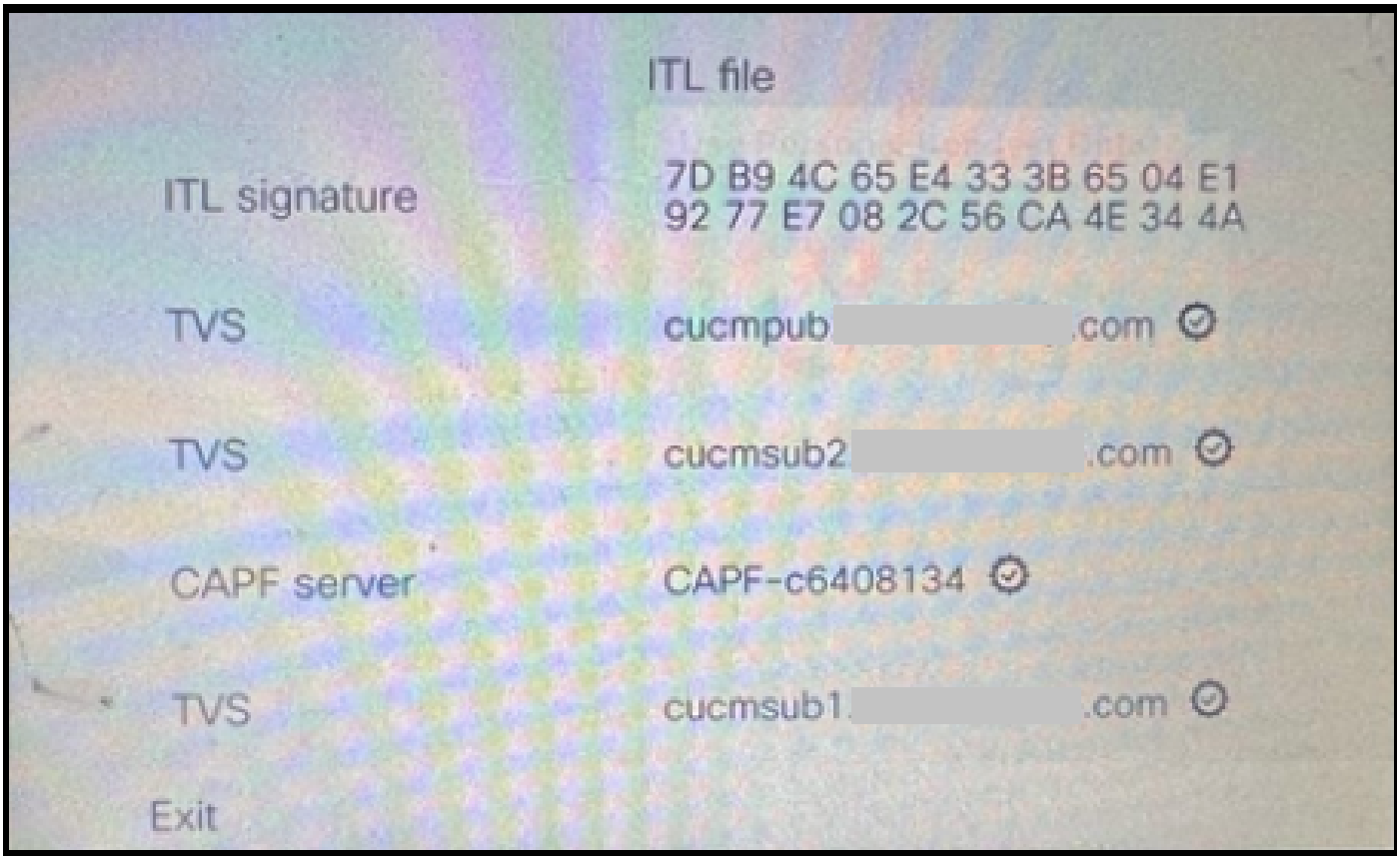
確認

電話機は宛先クラスタに正常に登録されます。



CUCMに登録されている電話機

電話機には、宛先クラスタの信頼リストエントリが含まれています。



電話機のITLファイル

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- デフォルトでのCUCMセキュリティとITLの動作およびトラブルシューティングについて
- トークンレス CTL を使用した CUCM 混合モード
- Cisco Unified Communications Managerセキュリティガイドリリース12.5(1)
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。