CUCM と CUC 間のセキュアな統合の設定およびトラブルシューティング

内容

概要

このドキュメントでは、Cisco Unified Communication Manager（CUCM）サーバと Cisco Unity Connection（CUC）サーバの間でのセキュアな接続の設定、検証、およびトラブルシューティングについて説明します。

前提条件

要件

CUCM について十分に理解しておくことをお勧めします。

詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』を参照してください。

注：セキュアな統合を正しく機能させるには、混合モードに設定する必要があります。

Unity Connection 11.5(1) SU3以降では暗号化を有効にする必要があります。

CLIコマンド「utils cuc encryption <enable/disable>」

使用するコンポーネント

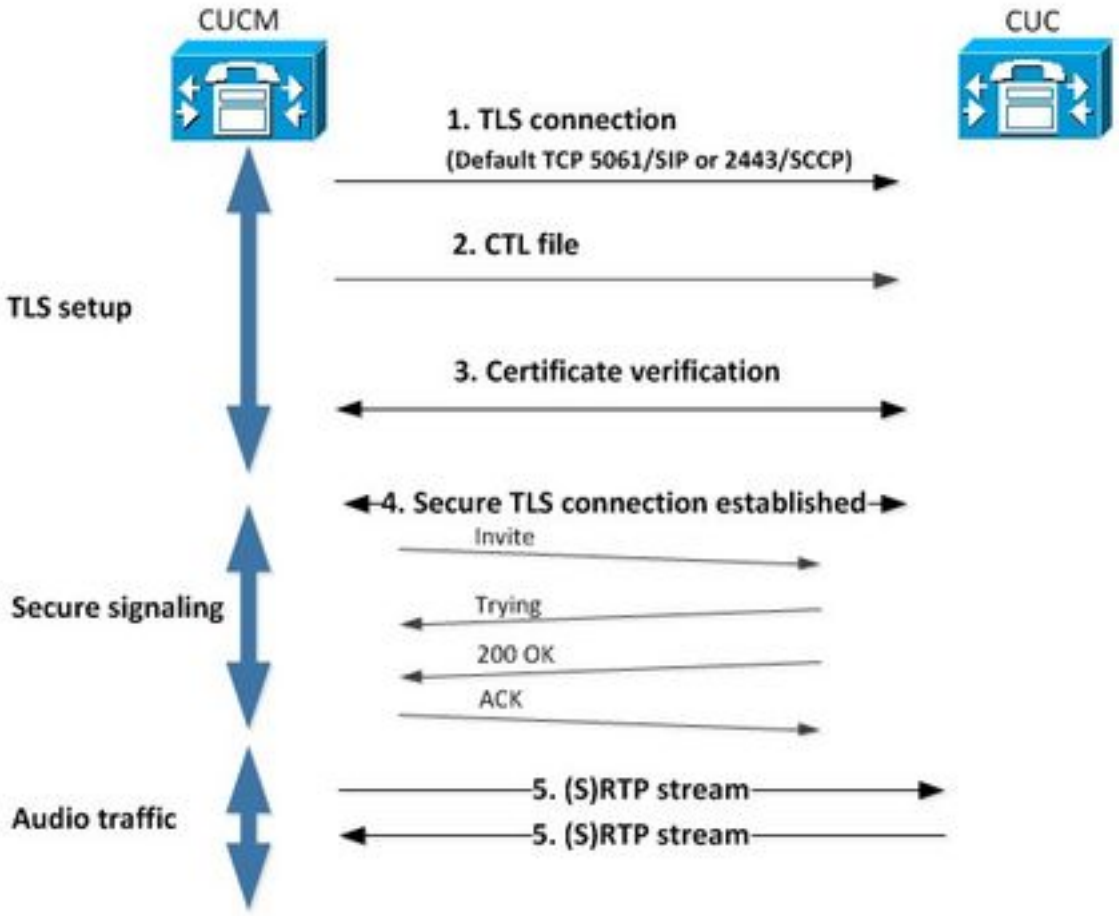
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM バージョン 10.5.2.11900-3
- CUC バージョン 10.5.2.11900-3

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

図

次の図で、CUCM と CUC の間でセキュアな接続を確立するプロセスについて簡単に説明します。



1. Call Managerは、統合に使用されるプロトコルのポート2443 Skinny Call Control Protocol(SCCP)または5061 Session Initiation Protocol(SIP)ベースで、CUCサーバへのセキュアなTransport Layer Security(TLS)接続を設定します。

2. CUCサーバは、TFTPサーバから証明書信頼リスト(CTL)ファイルをダウンロードし（ワンタイムプロセス）、CallManager.pem証明書を抽出して保存します。

3. CUCMサーバは、前の手順で取得したCallManager.pem証明書に対して検証されたCallmanager.pem証明書を提供します。また、CUC 証明書は CUCM に保存されている CUC ルート証明書に対して検証されています。管理者がルート証明書を CUCM にアップロードする必要があります。

4.証明書の検証が成功すると、セキュアなTLS接続が確立されます。この接続は、暗号化されたSCCP シグナリングまたは SIP シグナリングの交換に使用されます。

5.音声トラフィックは、Real-time Transport Protocol(RTP)またはSRTPとして交換することができます。

> **注**：TLS 通信が確立されると、CUCM および CUC は TLS 相互認証を使用します。詳細については、RFC5630 を参照してください。

設定：セキュア SIP トランク

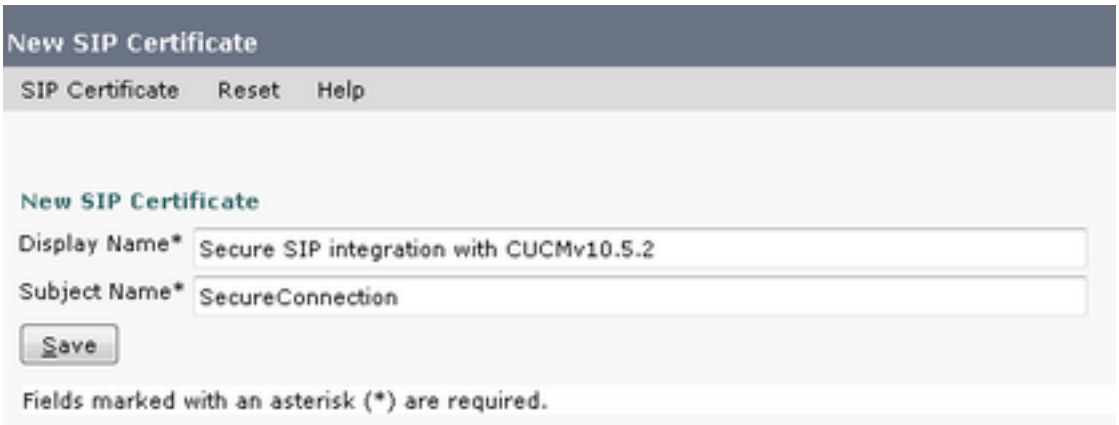
CUC の設定

1. SIP証明書の追加

[CUC Administration] > [Telephony Integrations] > [Security] > [SIP Certificate] > [Add new]に移動します。

- 表示名:<any meaningful name>
- Subject Name:<any name for example, **SecureConnection>**

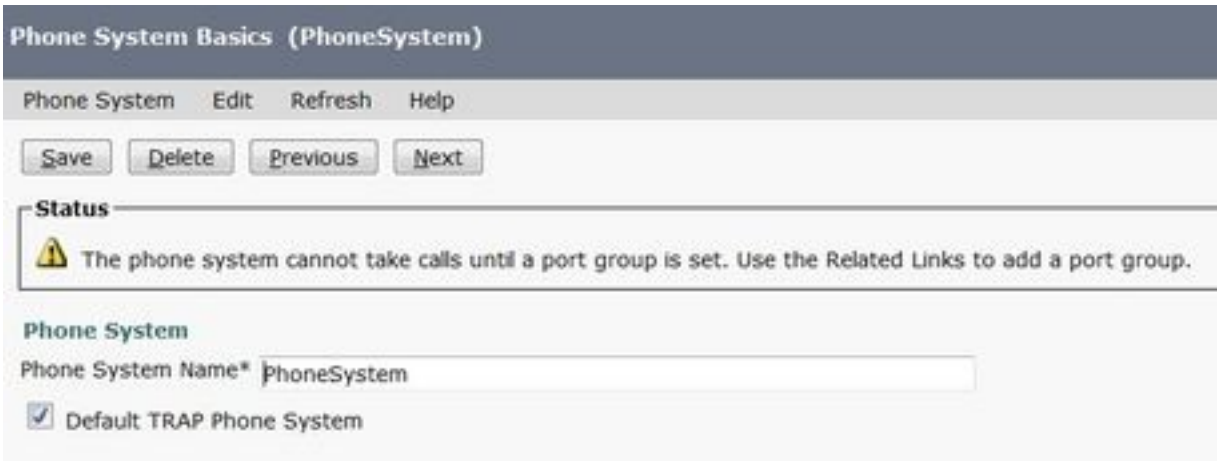
注:[Subject Name]は、SIPトランクセキュリティプロファイルの[X.509 Subject Name]と一致している必要があります（このドキュメントの後のCUCM設定のステップ1で設定）。



注：証明書は、CUC ルート証明書によって生成および署名されます。

2.新しい電話システムの作成またはデフォルトの電話システムの変更

[Telephony Integration] > [Phone System]に移動します。既存の電話システムを使用するか、新しい電話システムを作成することができます。

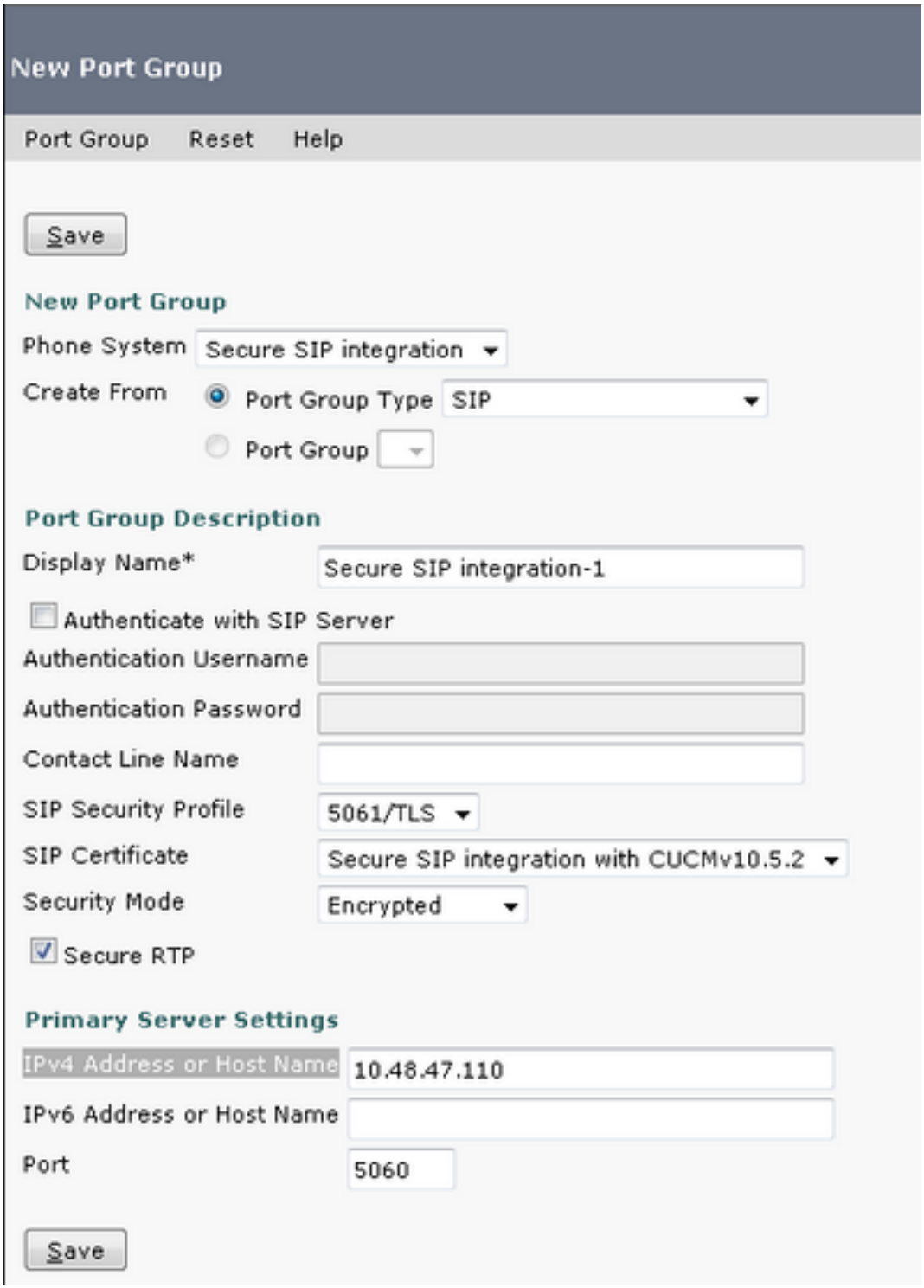


3.新しいポートグループの追加

[Phone System Basics] ページの [Related Links] ドロップダウン ボックスで、[Add Port Group] を選択して、[Go] を選択します。設定ウィンドウで、次の情報を入力します。

- [Phone System]：
- [Create From]：　[Port Group Type SIP]
- [SIP Security Profile]：　[5061/TLS]
- [SIP Certificate]：
- [Security Mode]：　[Encrypted]
- [Secure RTP]：　チェックボックスをオンにします。
- [IPv4 Address or Host Name]：

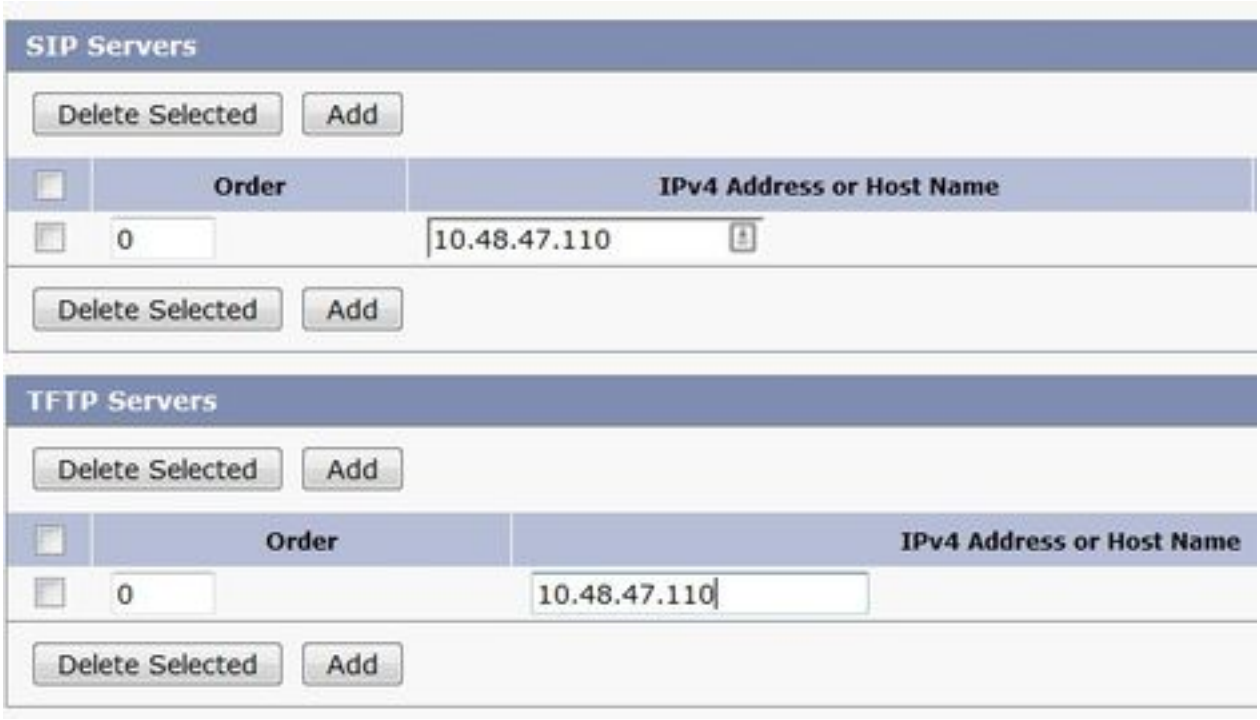
[Save] をクリックします。



4.サーバの編集

次の図に示すように、[Edit] > [Servers]に移動して、CUCM クラスタから TFTP サーバを追加し

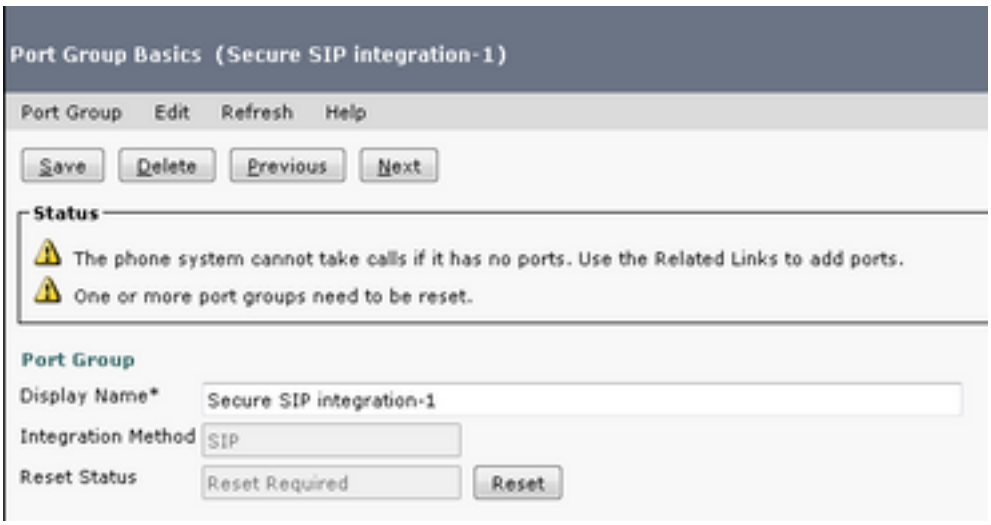
ます。



注：正しい TFTP アドレスを指定することが重要です。CUC サーバは、説明したとおり、この TFTP から CTL ファイルをダウンロードします。

5.ポートグループのリセット

次の図に示すように、[Port Group Basics]に戻り、システムによって促されるとおりにポート グループをリセットします。

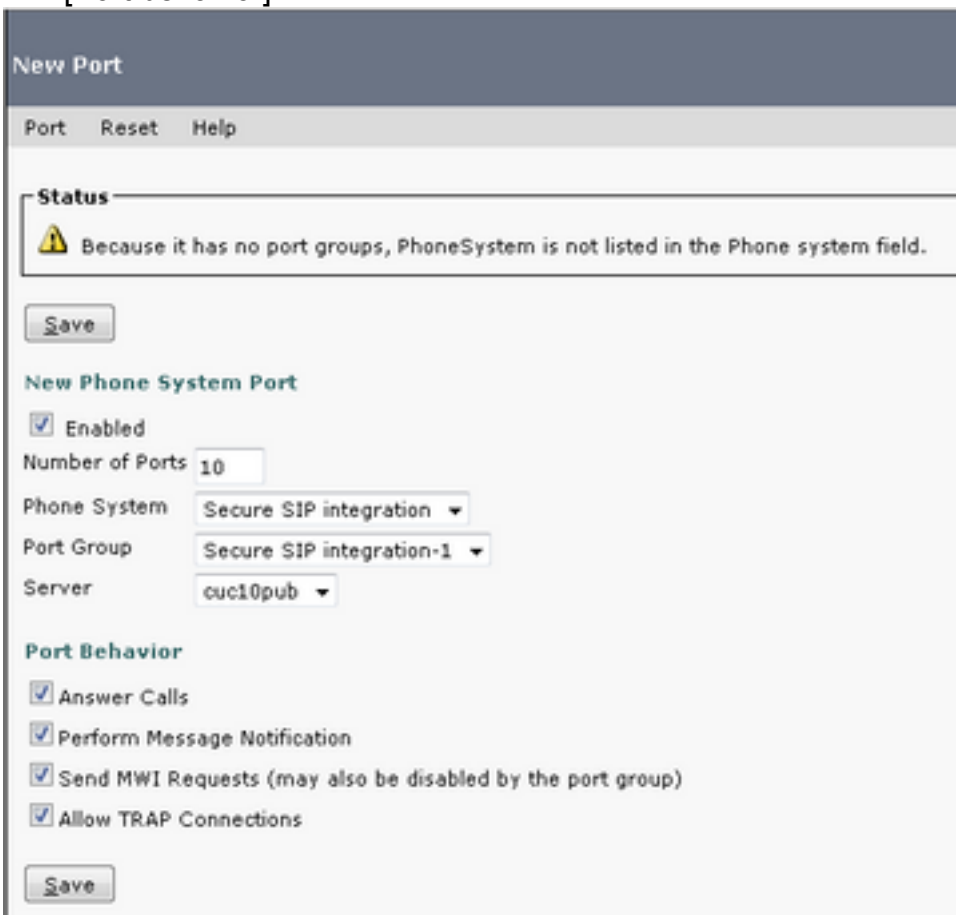


6.ボイスメールポートの追加

[Port Group Basics]ページの[Related Links]ドロップダウンボックスで[**Add Ports**]を選択し、[**Go**]を選択します。設定ウィンドウで、次の情報を入力します。

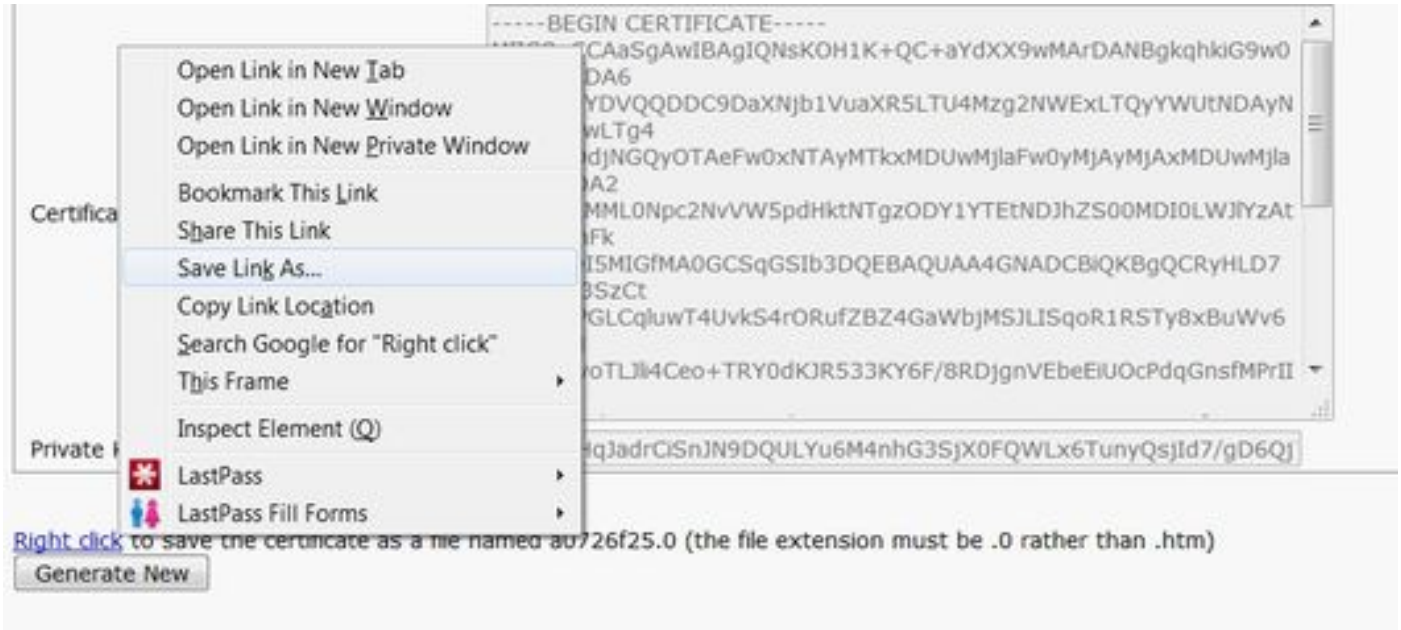
- [Enabled]：チェックボックスをオンにします。
- [Number of Ports]：
- [Phone System]：

- [Port Group]：
- [Server]：
- [Port behavior]：



7. CUCルート証明書のダウンロード

次の図に示すように、[Telephony Integrations] > [Security] > [Root Certificate]に移動し、証明書を <filename>.0 という名前のファイルとして保存するために、URL を右クリックして [save] をクリックします (ファイル拡張子は .htm ではなく .0 にする必要があります)。



CUCM の設定

1. CUCへのトランク用SIPトランクセキュリティプロファイルの設定

[CUCM Administration] > [System] > [Security] > [SIP Trunk Security Profile] > [Add new]に移動します。

次のフィールドを適切に入力してください。

- [Device Security Mode]： [Encrypted]
- [X.509 Subject Name]： [SecureConnection]
- [Accept out-of-dialog refer]： チェックボックスをオンにします。
- [Accept unsolicited notification]： チェックボックスをオンにします。
- [Accept replaces header]： チェックボックスをオンにします。

注：[X.509 Subject Name] は、Cisco Unity Connection サーバの SIP 証明書の [Subject Name] フィールド（CUC 設定のステップ 1 で設定）と一致している必要があります。

2. SIPプロファイルの設定

特定の設定を適用する必要がある場合は、[Device] > [Device Settings] > [SIP Profile]に移動します。そうでない場合は、標準の SIP プロファイルを使用できます。

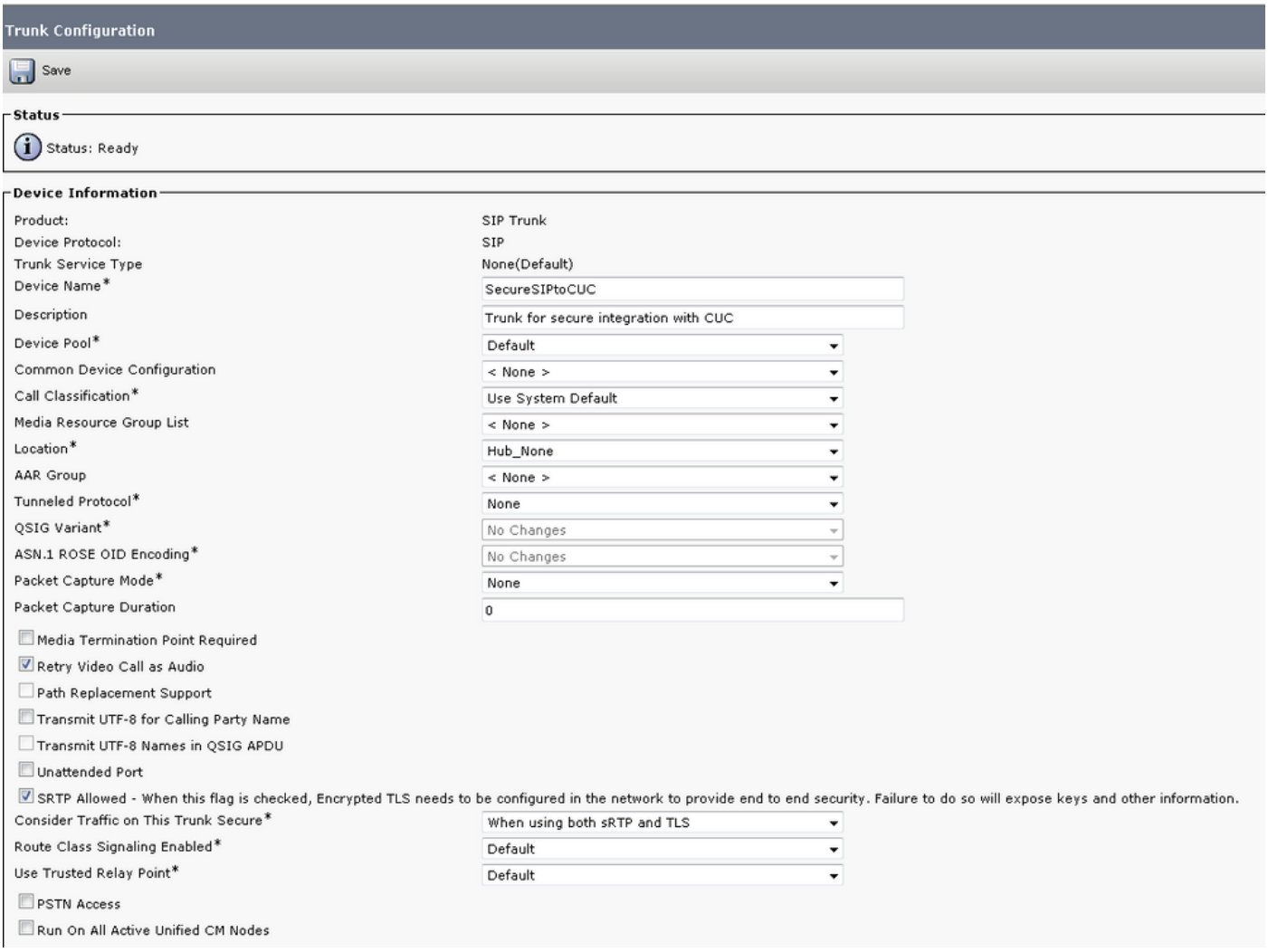
3. SIPトランクの作成

[Device] > [Trunk] > [Add new] に移動します。次の図に示すように、Unity Connectionとのセキュアな統合に使用するSIPトランクを作成します。

トランク設定の [Device Information] セクションで、次の情報を入力します。

- デバイス名:
- [Device pool]：
- [SRTP allowed]：　　チェックボックスをオンにします。

注：CallManager グループ（デバイス プール設定）に CUC で設定されたすべてのサーバが含まれていることを確認します（[Port group] > [Edit] >[Servers]）。

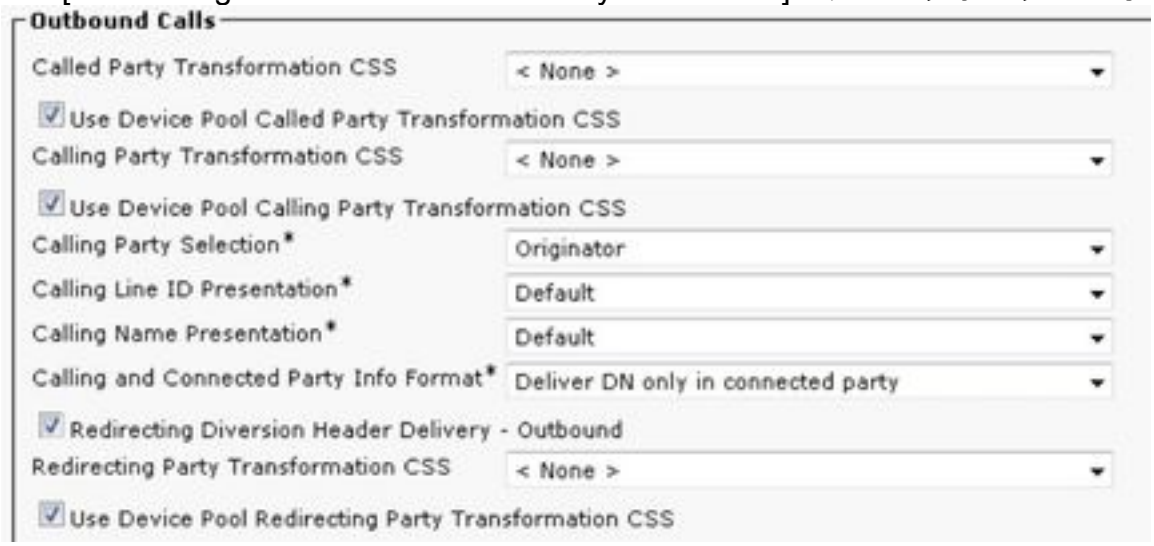


トランク設定の[Inbound Calls] セクションで、次の情報を入力します。

- [Calling Search Space]：
- [Redirecting Diversion Header Delivery - Inbound]：　チェックボックスをオンにします。

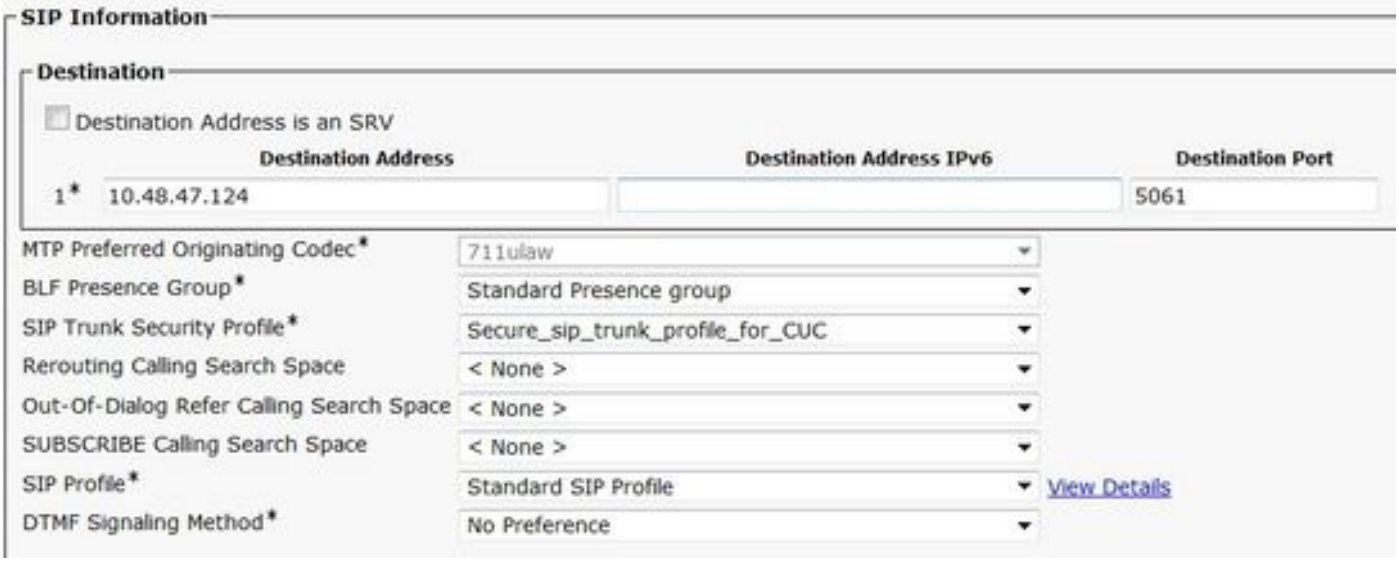
アウトバウンド トランク設定の[Calls]セクションで、次の情報を入力します。

- [Redirecting Diversion Header Delivery - Outbound]：チェックボックスをオンにします。



トランク設定の [SIP Information] セクションで、次の情報を入力します。

- 宛先アドレス:
- [SIP Trunk Security Profile]：
- [Rerouting Calling Search Space]：
- [Out-of-Dialog Refer Calling Search Space]：
- [SIP Profile]：

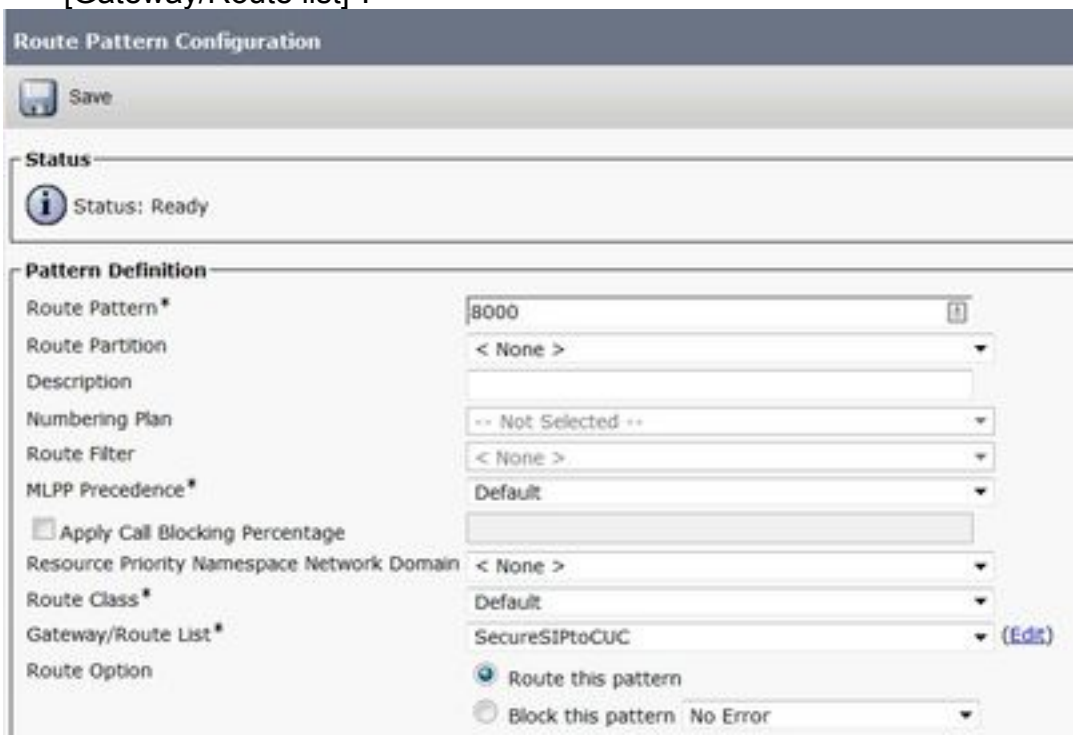


必要に応じて、その他の設定を調整します。

4.ルートパターンの作成

設定済みトランクを示すルート パターンを作成します（ [Call Routing] > [Route/Hunt] > [Route Pattern] ）。 ルート パターン番号として入力された内線番号は、ボイスメール パイロットとして使用できます。次の情報を入力します。

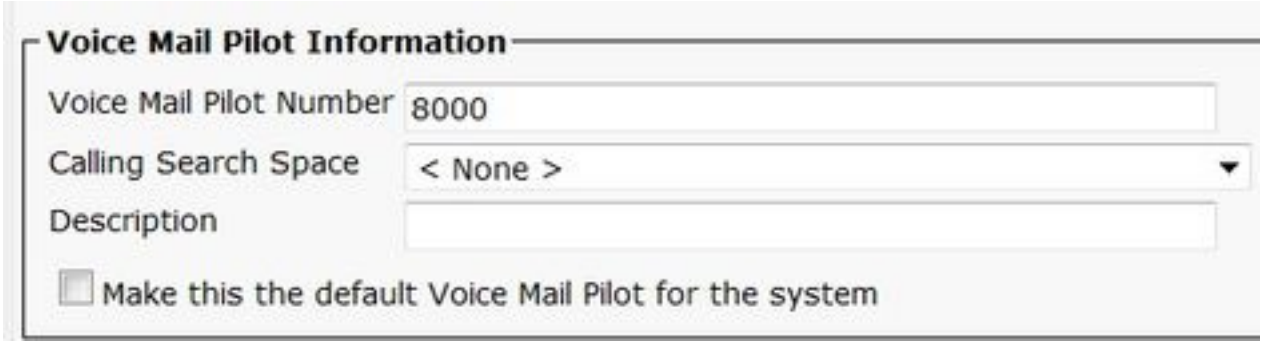
- [Route pattern]：
- [Gateway/Route list]：



5.ボイスメールパイロットの作成

統合用のボイス メール パイロットを作成します（ [Advanced Features] > [Voice Mail] >[Voice Mail Pilot] ）。 次の値を入力してください。

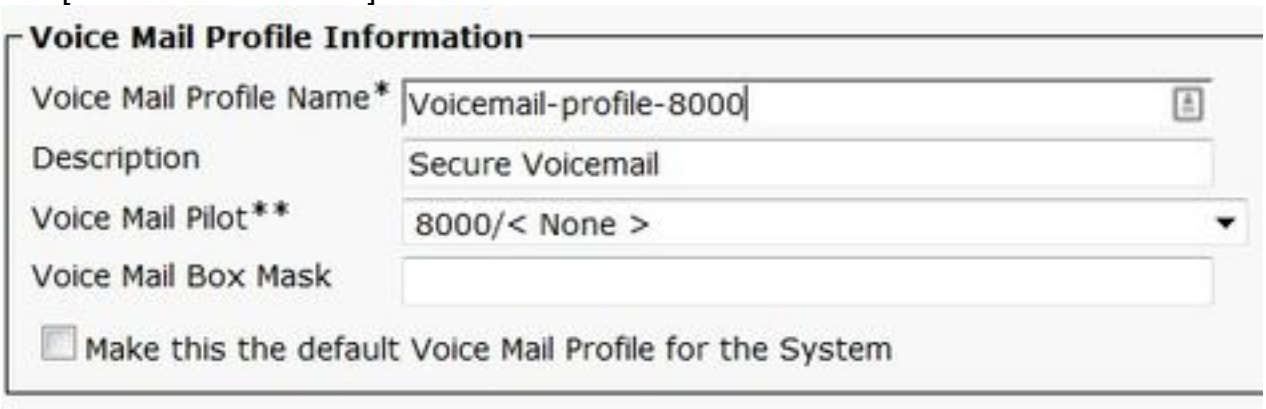
- [Voice Mail Pilot Number]：
- [Calling Search Space]： パイロットとして使用されるルート パターンを含むパーティション が含まれます。



6.ボイスメールプロファイルの作成

ボイス メール プロファイルを作成して、すべての設定をリンクさせます（ **[Advanced Features] > [Voice Mail] > [Voice Mail Profile] ）。** 次の情報を入力します。

- [Voice Mail Pilot]：
- [Voice Mail Box Mask]：

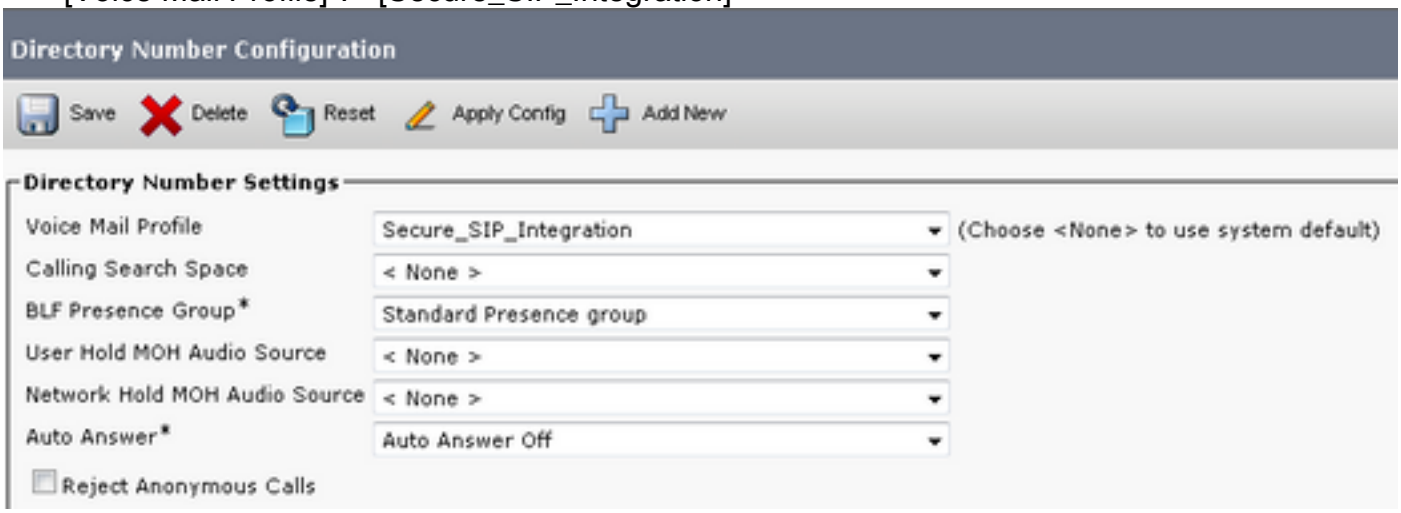


7.ボイスメールプロファイルのDNへの割り当て

セキュアな統合を使用するよう意図されている DN にボイスメール プロファイルを割り当てます。DN 設定を変更したら、忘れずに [Apply Config] ボタンをクリックします。

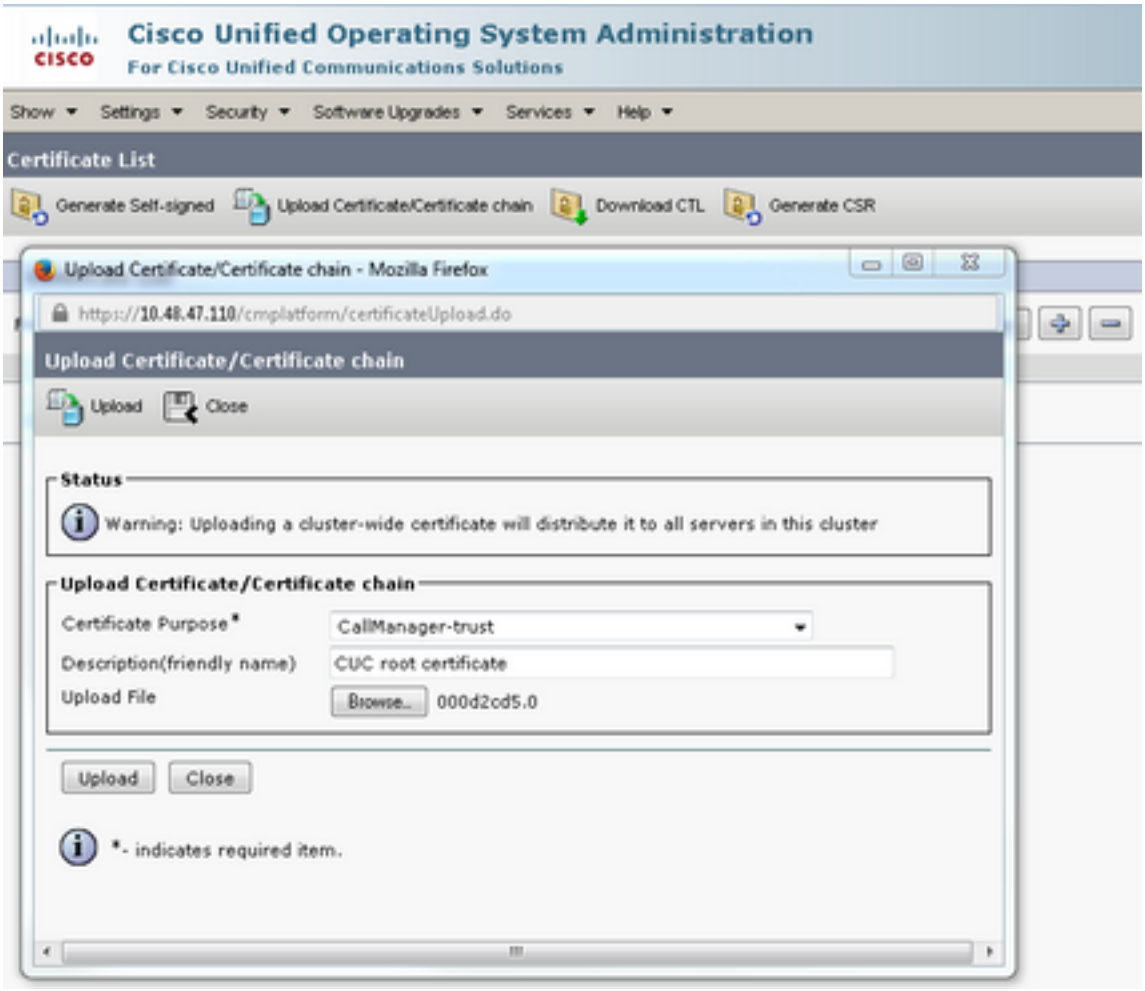
次のとおりに移動します。**[Call Routing] > [Directory number]に移動して、次の項目を変更します。**

- [Voice Mail Profile]： [Secure_SIP_Integration]



8. CUCルート証明書をCallManager-trustとしてアップロード

[OS Administration] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain]に移動し、設定済みのすべてのノードで CUC ルート証明書を **CallManager-trust としてアップロードして、CUC サーバと通信します。**



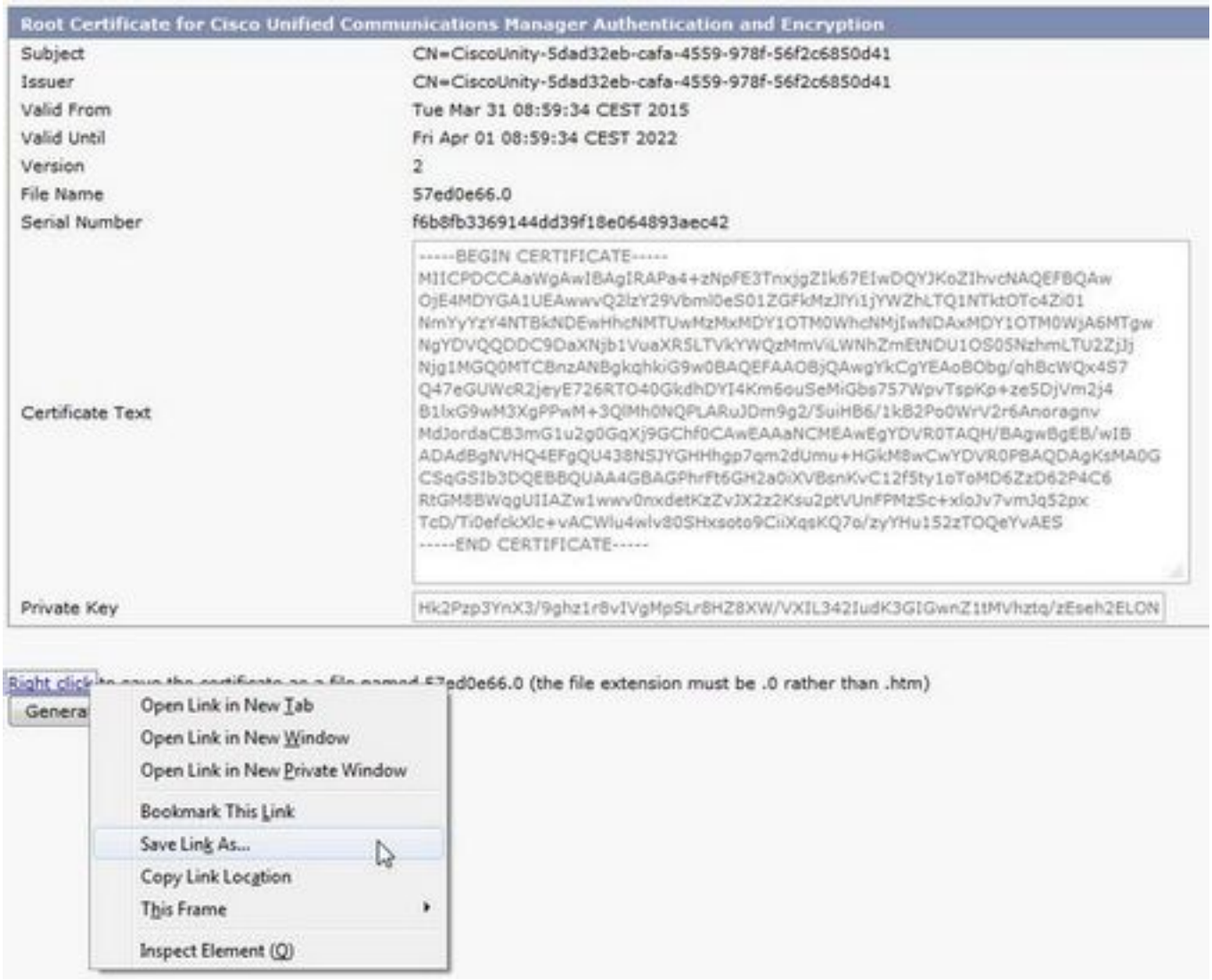
注：証明書を有効にするには、証明書のアップロード後にCisco CallManagerサービスを再起動する必要があります。

セキュア SCCP ポートの設定

CUC の設定

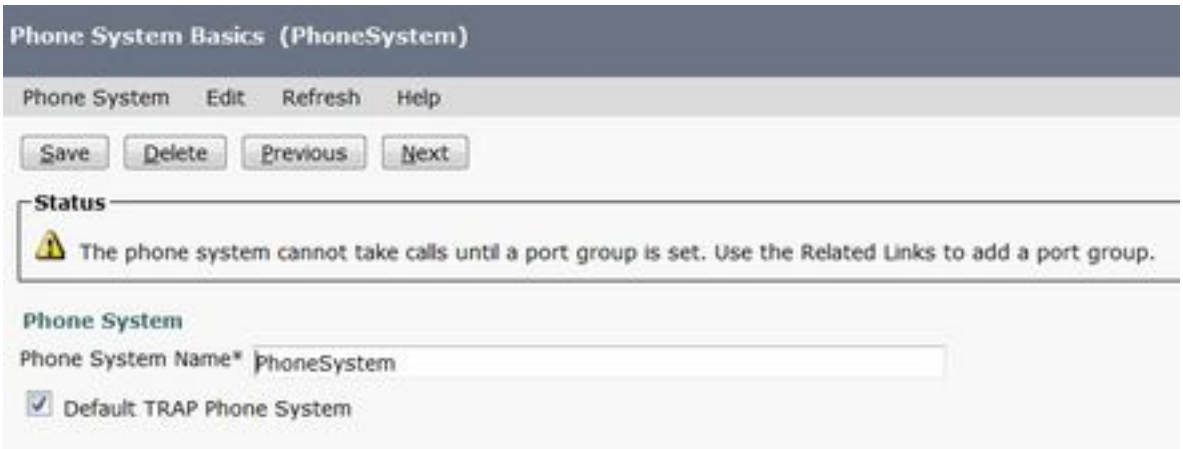
1. CUC ルート証明書のダウンロード

[CUC Administration] > [Telephony Integration] > [Security] > [Root Certificate]に移動します。証明書を <filename>.0 という名前のファイルとして保存するために、URL を右クリックして [Save] をクリックします（ファイル拡張子は .htm ではなく .0 にする必要があります）。



2.電話システムの作成/既存の電話システムの変更

[Telephony Integration] > [Phone System]に移動します。既存の電話システムを使用するか、新しい電話システムを作成することができます。

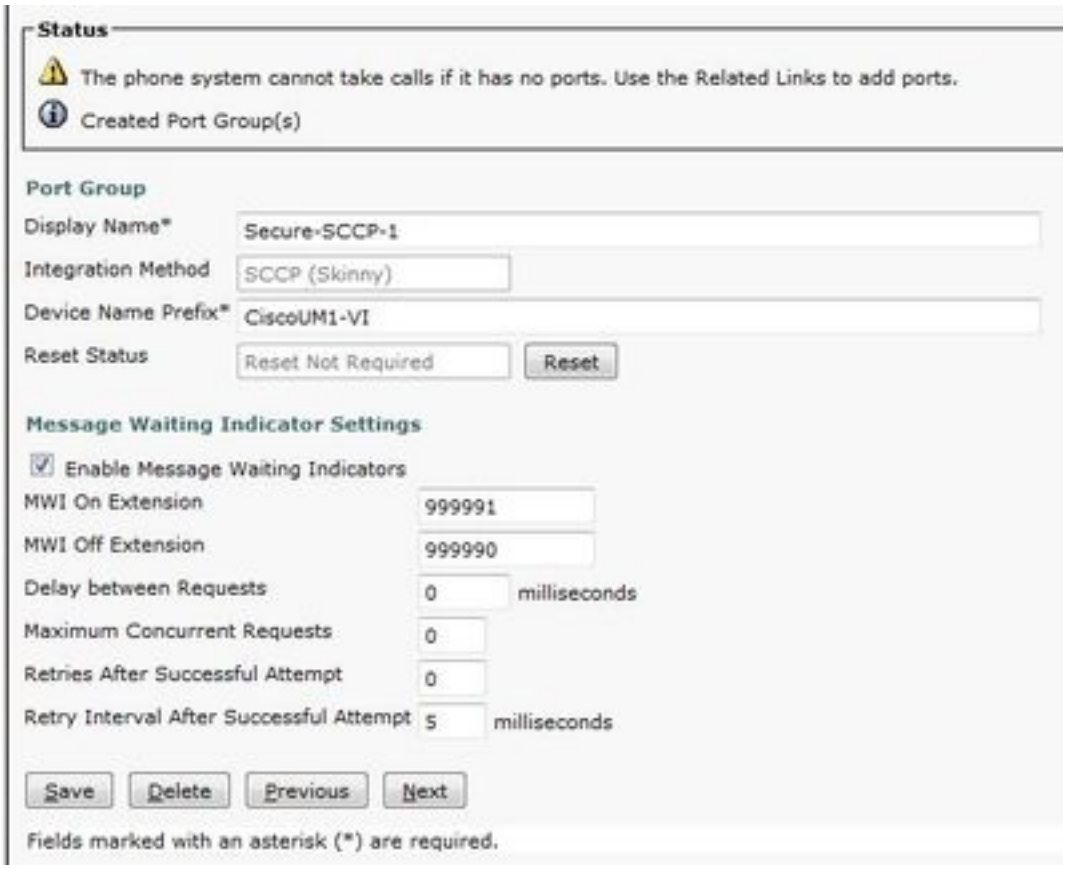


3.新しいSCCPポートグループの追加

[Phone System Basics] ページの [Related Links] ドロップダウン ボックスで、[Add Port Group] を選択して、[Go] を選択します。設定ウィンドウで、次の情報を入力します。

- [Phone system]：
- [Port group type]：　SCCP
- [Device Name prefix*]：　[CiscoUM1-VI]
- [MWI On extension]：
- [MWI Off extension]：

注：この設定は CUCM の設定と一致している必要があります。



4.サーバの編集

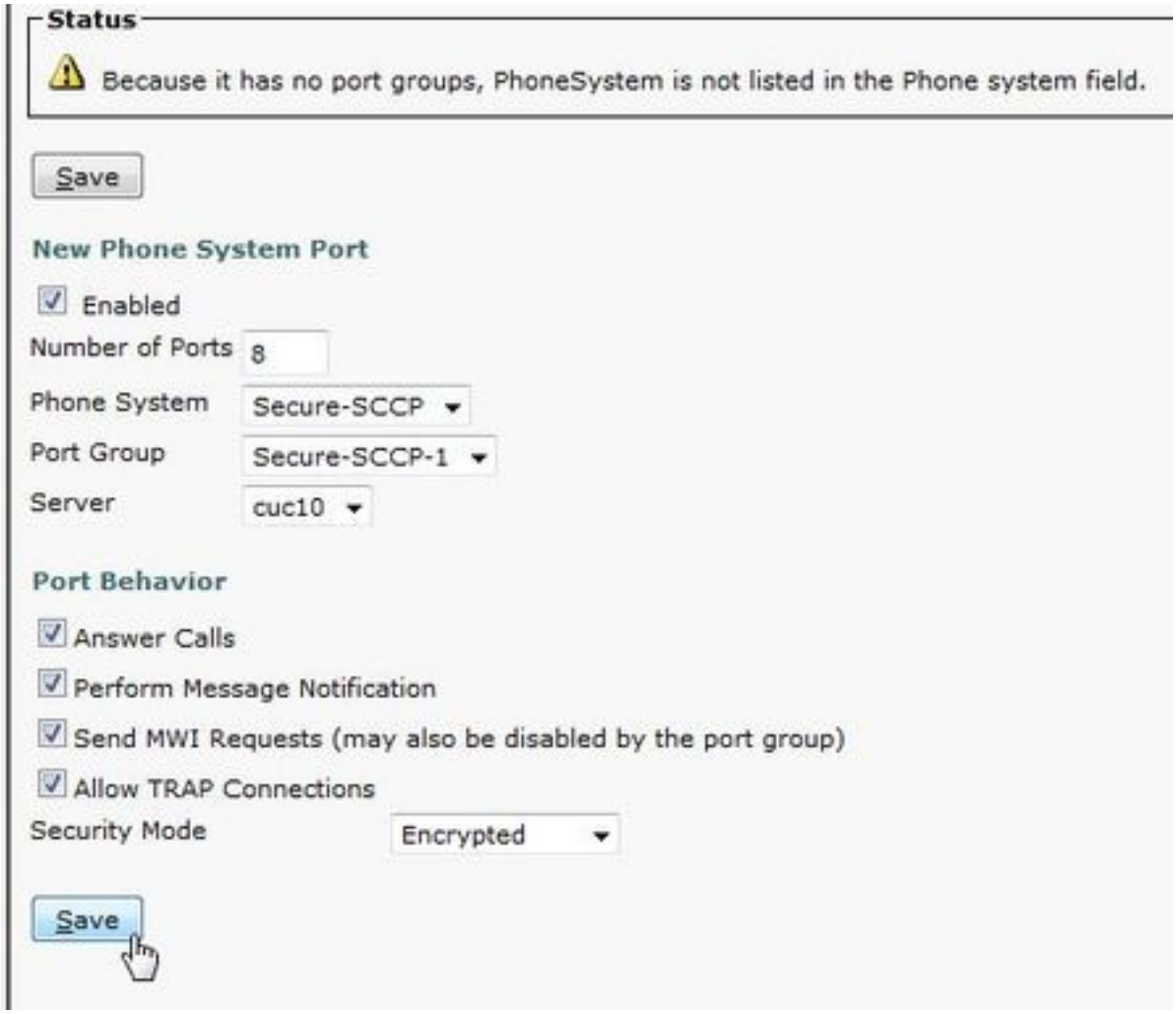
[Edit] > [Servers]に移動して、CUCM クラスタから TFTP サーバを追加します。

注：正しい TFTP アドレスを指定することが重要です。CUC サーバは、説明したとおり、この TFTP から CTL ファイルをダウンロードします。

5.セキュアSCCPポートの追加

[Port Group Basics]ページの[Related Links]ドロップダウンボックスで、**[Add Ports]を選択**し、**[Go]**を選択します。設定ウィンドウで、次の情報を入力します。

- [Enabled]：チェックボックスをオンにします。
- [Number of Ports]：
- [Phone System]：
- [Port Group]：
- [Server]：
- [Port behavior]：
- [Security Mode]：　　**[Encrypted]**

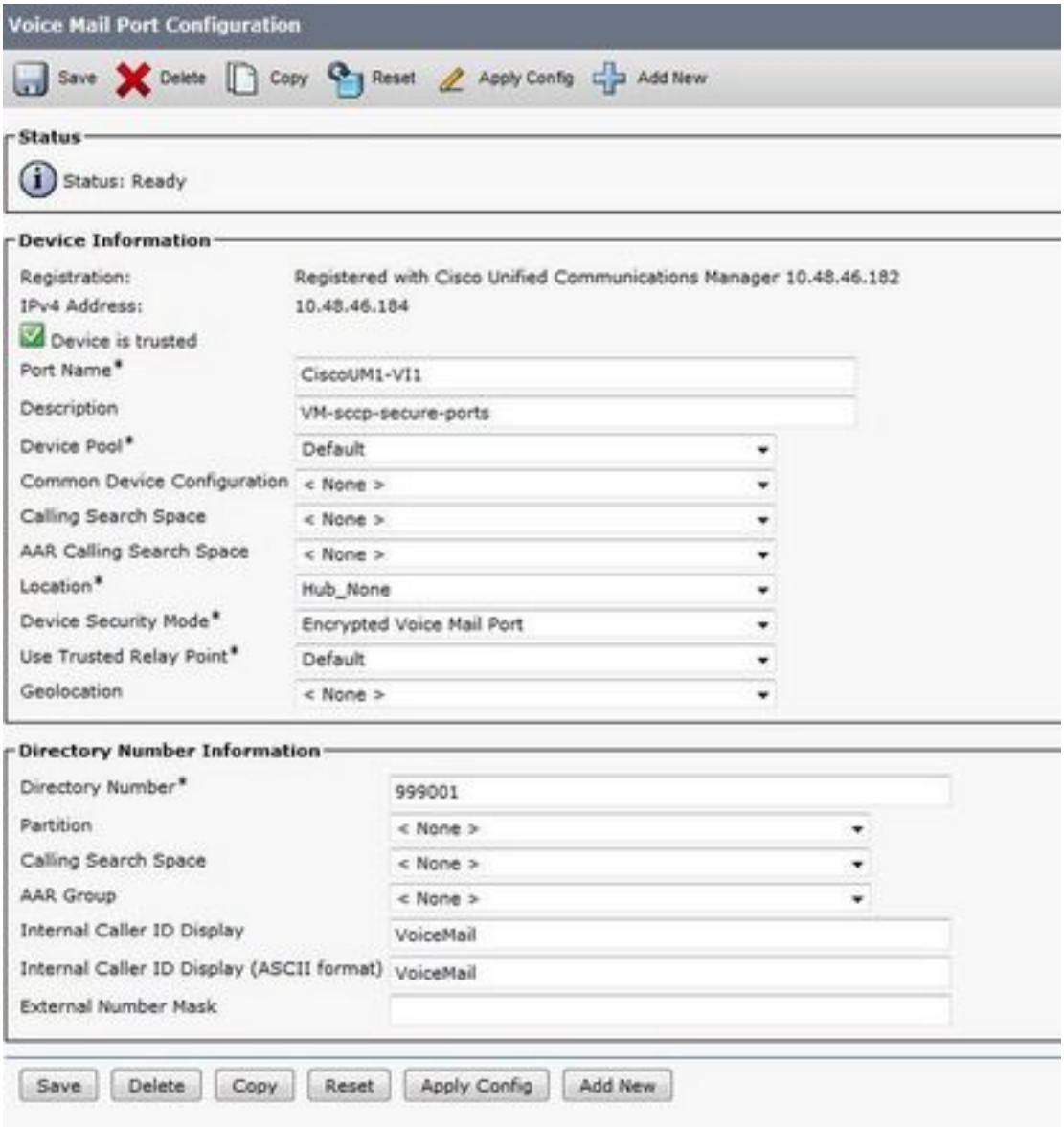


CUCM の設定

1.ポートの追加

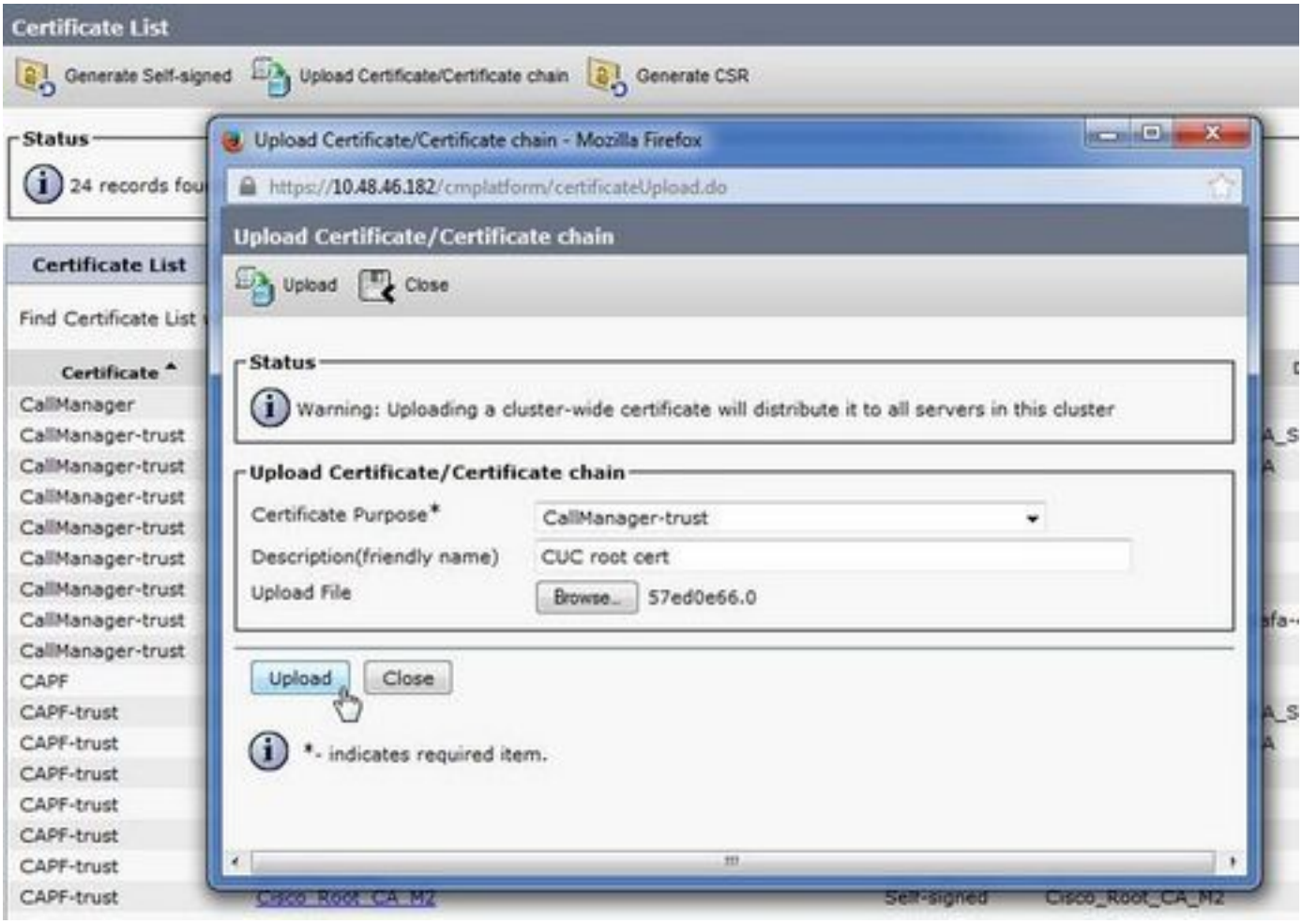
に移動 [CUCM Administration] > [Advanced features] > [Voice Mail Port Configuration] > [Add New]。

従来どおり SCCP ボイス メール ポートを設定します。唯一の違いは、ポート設定の [Device Security Mode] で [Encrypted Voice Mail Port] オプションを選択する必要があることです。



2. CUCルート証明書をCallManager-trustとしてアップロードする

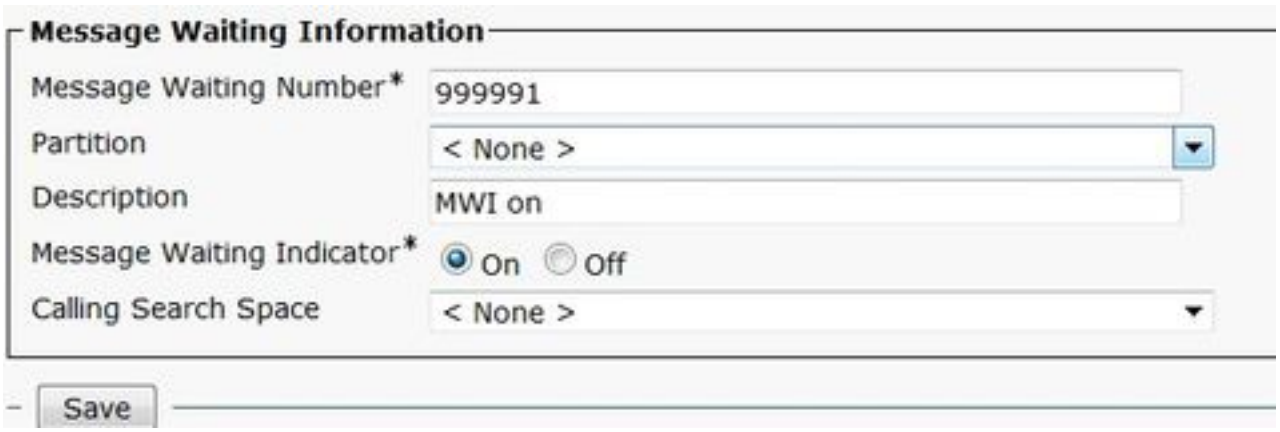
[OS Administration] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain]に移動し、設定済みのすべてのノードで CUC ルート証明書を **CallManager-trust としてアップロードして、CUC サーバと通信します。**

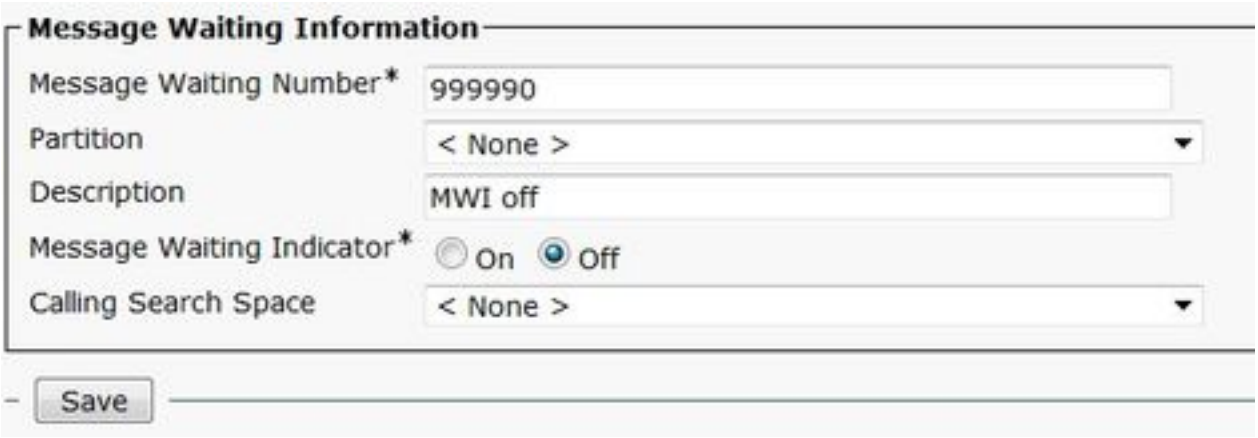


注：証明書を有効にするには、証明書のアップロード後にCisco CallManagerサービスを再起動する必要があります。

を選択します。 メッセージ受信情報（MWI）オン/オフの内線番号

[CUCM Administration] > [Advanced Features] > [Voice Mail Port Configuration]に移動して、[MWI On/Off Extensions] **を設定します。**MWI 番号は、CUC 設定と一致している必要があります。

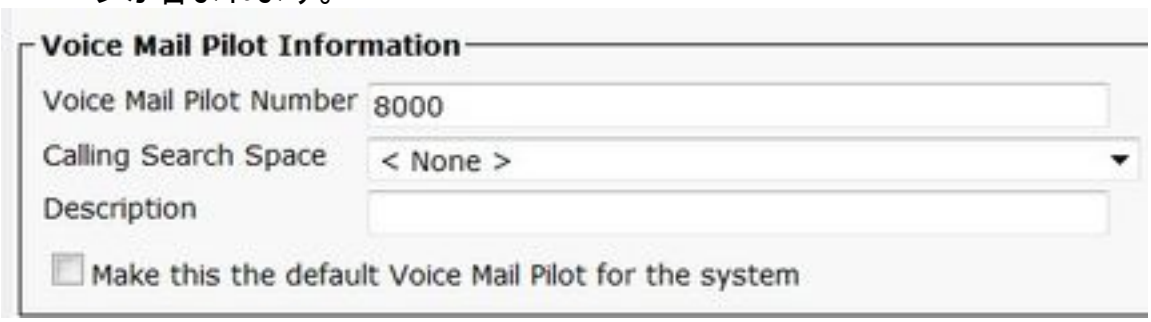




4.ボイスメールパイロットの作成

統合用のボイス メール パイロットを作成します（ [Advanced Features] > [Voice Mail] >[Voice Mail Pilot]）。 次の値を入力してください。

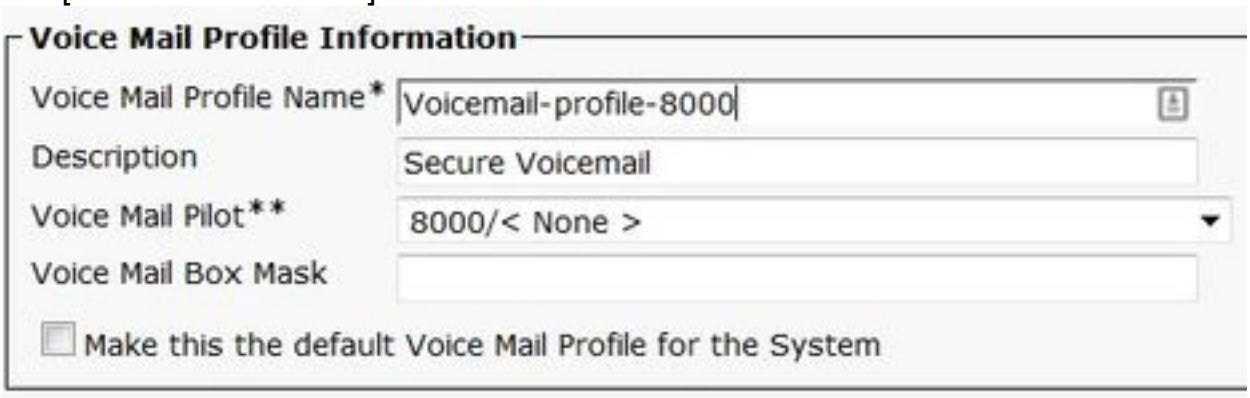
- [Voice Mail Pilot Number]：
- [Calling Search Space]： パイロットとして使用されるルート パターンを含むパーティションが含まれます。



5.ボイスメールプロファイルの作成

ボイス メール プロファイルを作成して、すべての設定をリンクさせます（ **[Advanced Features] > [Voice Mail] > [Voice Mail Profile] ）。** 次の情報を入力します。

- [Voice Mail Pilot]：
- [Voice Mail Box Mask]：

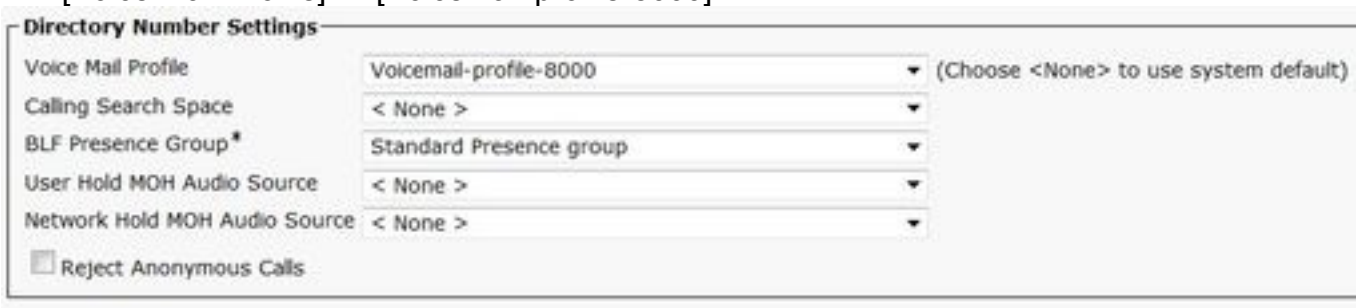


6.ボイスメールプロファイルのDNへの割り当て

セキュアな統合を使用するよう意図されている DN にボイス メール プロファイルを割り当てます。DN 設定を変更したら、[Apply Config]ボタンをクリックします。

[Call Routing] > [Directory number]に移動して、次の項目を変更します。

- [Voice Mail Profile]： [Voicemail-profile-8000]

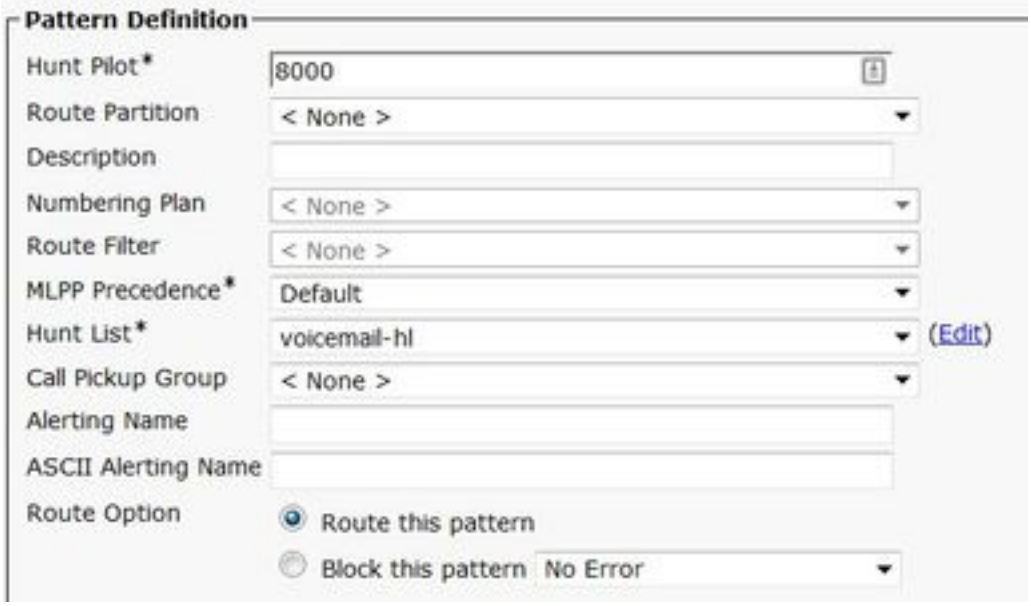


7. ボイス メール ハント グループの作成

a)新しい回線グループ**を追加します**(**[コールルーティング] > [ルート/ハント] > [回線グループ**)

b)新しいボイスメールのハントリ**ストを追加**します(**[Call Routing] > [Route/Hunt] > [Hunt List])**

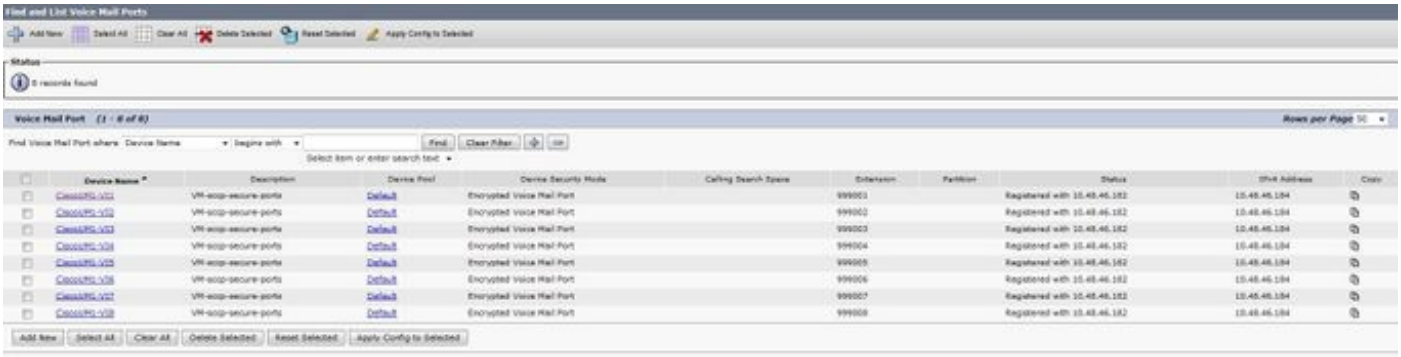
c)新しいハントパイロット**を追加する([コールルーティング] > [ルート/ハント] > [ハントパイロット**])



確認

SCCP ポートの検証

[CUCM Administration] > [Advance Features] > [Voice Mail] > [Voice Mail Ports]に移動して、ポート登録を検証します。



電話の [Voice Mail]ボタンを押して、ボイス メールを送信します。Unity Connection システムでユーザの内線番号が設定されていない場合、オープニング グリーティングを聞く必要があります。

セキュア SIP トランクの検証

電話の [Voice Mail]ボタンを押して、ボイス メールを送信します。Unity Connection システムでユーザの内線番号が設定されていない場合、オープニング グリーティングを聞く必要があります。

または、SIP OPTION のキープアライブを有効にして、SIP トランクのステータスをモニタすることができます。このオプションは、SIP トランクに割り当てられた SIP プロファイルで有効にできます。このオプションを有効にすると、次の図に示すように、[Device] > [Trunk]経由で SIP トランクのステータスをモニタできます。

セキュア RTP コールの検証

鍵マークのアイコンが Unity Connection へのコールに表示されるかどうか検証します。これは、次の図に示すように、RTP ストリームが暗号化されていることを意味します（機能させるには、デバイス セキュリティ プロファイルがセキュアである必要があります）。

トラブルシュート

1.一般的なトラブルシューティングのヒント

セキュアな統合をトラブルシューティングするには、次の手順を実行します。

- 設定を確認します。
- すべての関連サービスが実行されていることを確認します（CUCM：CallManager、TFTP、CUC：Conversation Manager）。
- サーバ間のセキュアな通信に必要なポート（SCCP 統合用の TCP ポート 2443 および SIP 統合用の TCP 5061）がネットワークで開いていることを確認します。
- これらのすべてが適切な場合、トレース収集に進みます。

2.収集するトレース

次のトレースを収集して、セキュアな統合をトラブルシューティングします。

- CUCM および CUC からのパケット キャプチャ
- CallManager トレース
- Cisco Conversation Manager トレース

詳細については、次の関連資料を参照してください。

CUCM でパケット キャプチャを実行する方法：

http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html

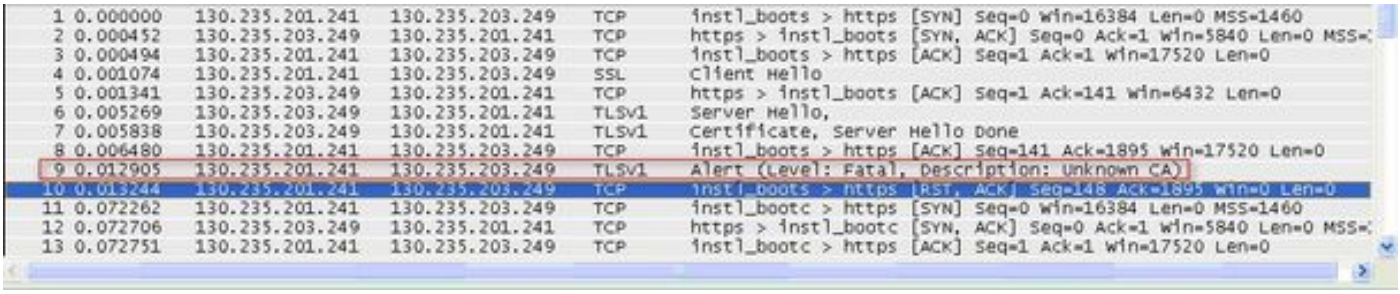
CUC サーバでトレースを有効にする方法：

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/10xcuctsg010.html

一般的な問題

ケース 1：セキュアな接続を確立できない（不明な CA アラート）

いずれかのサーバからパケット キャプチャを収集すると、TLS セッションが確立されます。



クライアントは、サーバから送信された証明書を検証できなかったため、不明な CA の致命的なエラーでサーバにアラートを発行しました。

次の 2 つの可能性があります。

1) CUCMがアラートを送信する 不明なCA

- 最新の CUC ルート証明書が CUC サーバと通信するサーバにアップロードされていることを確認します。
- CallManager サービスが、対応するサーバで再起動されていることを確認します。

2) CUCが不明CAアラートを送信

- CUC サーバの [Port Group] > [Edit] > [Servers] 設定に TFTP の IP アドレスが正しく入力されていることを確認します。
- 接続サーバから CUCM TFTP サーバに到達できることを確認します。
- CUCM TFTPのCTLファイルが最新であることを確認します（「show ctl」の出力をOS Adminページに表示される証明書と比較します）。 最新でなければ、CTLClient を再実行します。
- CUCサーバをリブートするか、ポートグループを削除して再作成し、CUCM TFTPからCTLファイルを再ダウンロードします。

ケース 2：CUCM TFTP から CTL ファイルをダウンロードできない

このエラーは、Conversation Manager のトレースで見られます。

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving
server certificates.
MiuGeneral,25,Error executing tftp command 'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not
found on server)
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving
server certificates.
Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as
ID=1
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
```

```
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

ソリューション：

1. [Port group] > [Edit] > [Servers]の設定でTFTPサーバが正しいことを再確認してください。

2. CUCMクラスタがセキュアモードであることを確認します。

3. CTLファイルがCUCM TFTPに存在することを確認します。

ケース 3：ポートが登録されない

このエラーは、Conversation Manager のトレースで見られます。

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting
retry timer -> 5000 msec
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM
IP Address>' in CTL File
```

ソリューション：

1.これは、CUCMとCUCでCTLファイルのmd5チェックサムが再生成された結果として一致していないことが原因である可能性が高いです

考えられます。CUC サーバを再起動して、CTL ファイルを更新します。

シスコ内部情報

または、次のようにルートから CTL ファイルを削除できます。

/tmp/ フォルダから CTL ファイルを削除して、ポート グループをリセットします。削除する前に、ファイルで md5 チェックサムを実行して

比較することができます。

CUCM： [root@vfrscucm1 trust-certs]# md5sum /usr/local/cm/tftp/CTLFile.tlv

e5bf2ab934a42f4d8e6547dfd8cc82e8 /usr/local/cm/tftp/CTLFile.tlv

CUC： [root@vstscuc1 tmp]# cd /tmp

[root@vstscuc1 tmp]# ls -al *tlv

-rw-rw-r— 1 cucsmgrユーザデバイス6120 Feb 5 15:29 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

[root@vstscuc1 tmp]# md5sum a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

e5bf2ab934a42f4d8e6547dfd8cc82e8 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

さらに、このトラブルシューティング ガイドを参照できます。

不具合

CSCum48958：CUCM 10.0（IP アドレスの長さが正しくない）

CSCtn87264：セキュア SIP ポートの TLS 接続が失敗する

CSCur10758：取り消された証明書を Unity Connection で消去できない

CSCur10534 ：Unity Connection 10.5 TLS/PKI の相互運用における冗長な CUCM

CSCve47775:CUCでCUCMのCTLFileを更新および確認する方法の機能要求