次世代 暗号化（NGE）に基づいて CUCM と CUC 間のセキュア SIP 統合のための設定例

目次

概要

この資料は次世代 暗号化を使用して Cisco Unified 通信マネージャ（CUCM）および Cisco Unity Connection（CUC）サーバ間のセキュア SIP 接続の設定および確認を記述したものです。

SIP インターフェイス上の次世代 の セキュリティは TLS 1.2、SHA-2 および AES256 基づいてスイート B 暗号を使用するために SIP インターフェイスをプロトコルに制限します。 それは RSA または ECDSA 暗号の優先順位に基づいて暗号のさまざまな組み合わせを割り当てます。 Unity Connection と Cisco Unified CM 間の通信の間に、暗号およびサード パーティ 認証は両方両端に確認されます。 次世代 暗号化サポートのための設定は下記にあります。

使用するために計画すればサード パーティ 認証局（CA）が署名する認証はにコンフィギュレーションセクション（設定署名する認証から-開始しま EC キーによって基づく認証にサード パーティ CA によって署名します）の終わり

前提条件

要件

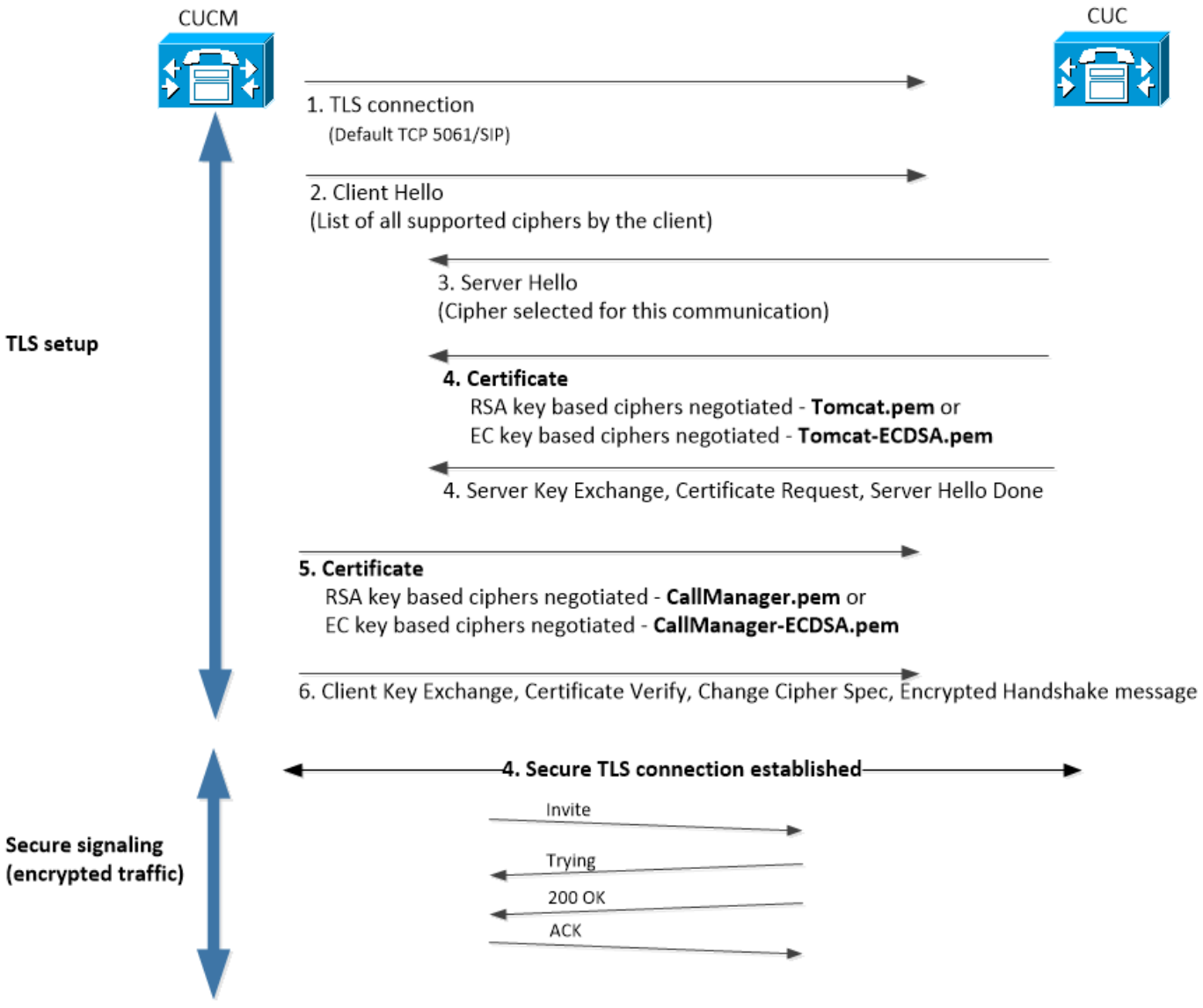
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

ミックス モードの CUCM バージョン 11.x および それ 以降
CUC バージョン 11.x および それ 以降

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

ネットワーク図

このダイアグラムは簡潔に一度次世代 暗号化サポートが有効に なることをヘルプが CUCM と CUC 間の信頼できる接続を確立することプロセスを説明します:



認証必要条件

これらは次世代 暗号化サポートが有効に された on Cisco Unity Connection なら認証交換必要条件です。

使用される自己署名証明書:

- Unity 接続
  認証をアップロードする必要無し。 Unity Connection サーバは TLS ネゴシエーションの間に設定および信頼 CallManager.pem の間に及び CallManagerEC.pem 規定 された TFTPサーバから自動的に ITLfile をダウンロードします。

- Cisco Unified CM
  CUCM の CallManager 信頼ストアに Unity connetion の Tomcat.pem 及び TomcatEC.pem をアップロードして下さい

使用されるサード パーティ CA証明:

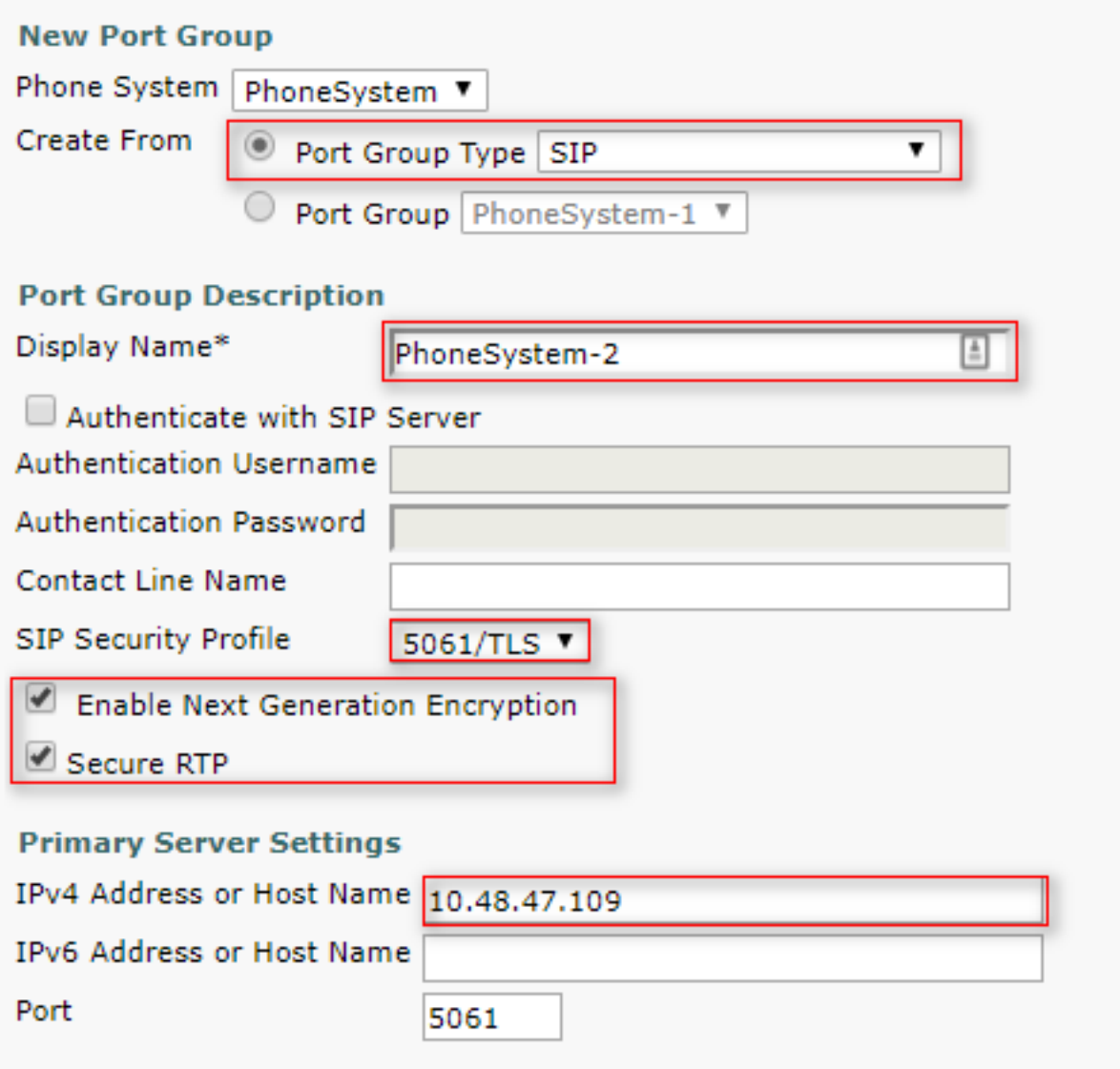
- Unity 接続
  Unity Connection の CallManager 信頼のサード パーティ 認証局 （CA）のルートおよび中間認証をアップロードして下さい。 それの上、
  接続サーバは TLS ネゴシエーションの間に設定および信頼 CallManager.pem の間に及び CallManagerEC.pem 規定 された TFTPサーバから自動的に ITLfile をダウンロードします。

- Cisco Unified CM
  統一された CM の CallManager 信頼のサード パーティ 認証局 （CA）のルートおよび中間認証をアップロードして下さい。

設定- Cisco Unity Connection （CUC）

1. 新しいポートグループを追加して下さい

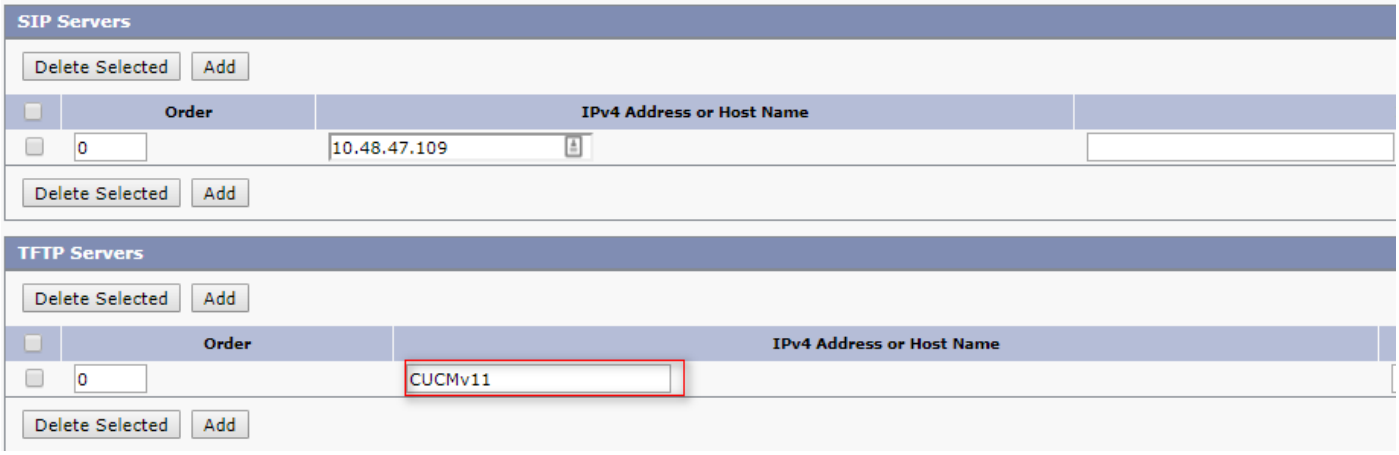
Cisco Unity Connection 管理 ページ > テレフォニー 統合 > ポートグループへのナビゲートはおよび『Add New』 をクリック します。 イネーブル 次世代 暗号化チェックボックスをチェックすることを確かめて下さい。



1. **注:** Unity Connection の Cisco Tomcat 認証は SSL ハンドシェイクの間にイネーブル 次世代暗号化チェックボックスが有効に なれば使用されます。
   • ECDSA によって基づく暗号がそれからネゴシエートされれば EC キー基づいた TomcatECDSA 認証は SSL ハンドシェイクで使用されます。
   • RSA によって基づく暗号がそれからネゴシエートされれば RSA キー基づいた Tomcat 認証は SSL ハンドシェイクで使用されます。

2. TFTPサーバ参照を追加して下さい

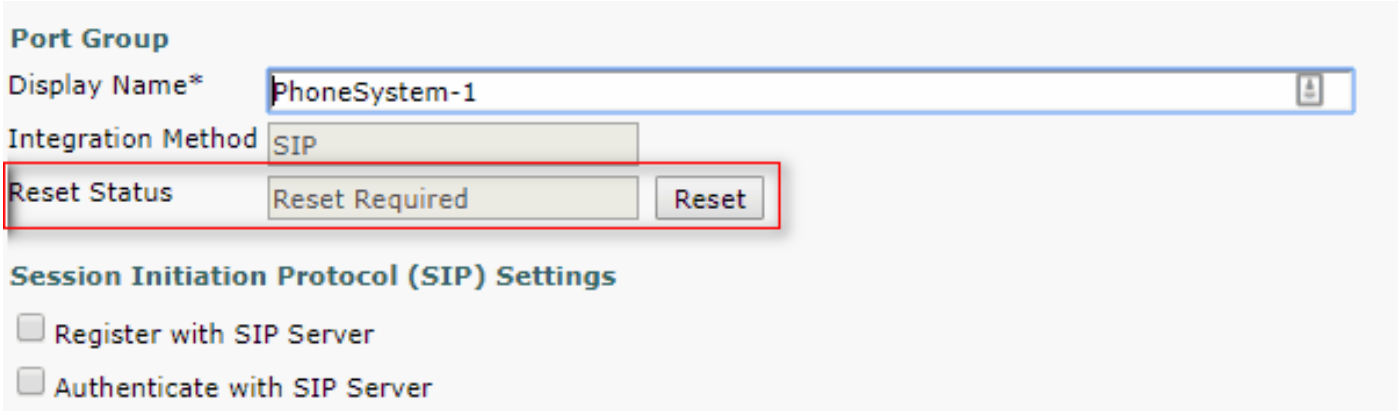
ポートグループ 基本 ページで、> サーバは編集し、CUCM クラスタの TFTPサーバの FQDN を追加するためにナビゲート します。 TFTPサーバの FQDN/ホスト名は CallManager 認証の Common Name （ CN ）を一致する必要があります。 サーバの IP アドレスははたらかないし、ITL ファイルをダウンロードするために失敗に終わります。 DNS名は設定された DNSサーバによって解決可能である必要があります従って。



Cisco Unity Connection サービサビリティ > Tools > Service 管理へのナビゲートによって各ノードの接続メッセージ交換マネージャを再起動して下さい。 これは設定が実施されることができるように必須です。

1. **注:** Unity 接続はセキュア 6972 ポートの https プロトコルを使用して CUCM の TFTP から ITL ファイル（ITLfile.tlv）をダウンロードします（URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv）。 CUCM はミックス モードに CUC が ITL ファイルからの「CCM+TFTP」機能 認証を探して いるのである必要があります。

テレフォニー 統合 > ポートグループ > ポートグループ 基本 設定 ページに戻ってナビゲート し、新たに追加されたポートグループをリセットして下さい。



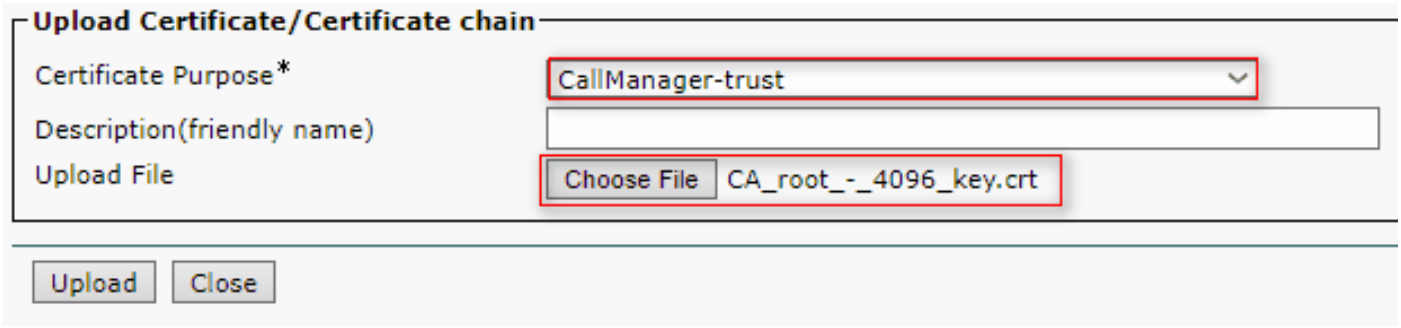
1. **注:** ポートグループがリセットされる度に、CUC サーバは CUCM サーバに接続によってローカルで保存された ITL ファイルをアップデートします。

3. 音声メールポートを追加して下さい

テレフォニー 統合 > ポートに戻ってナビゲート し、新しく作成されたポートグループにポートを追加するために『Add New』 をクリック して下さい。

4. サード パーティ CA の CUCM ルートおよび中間物認証をアップロードして下さい

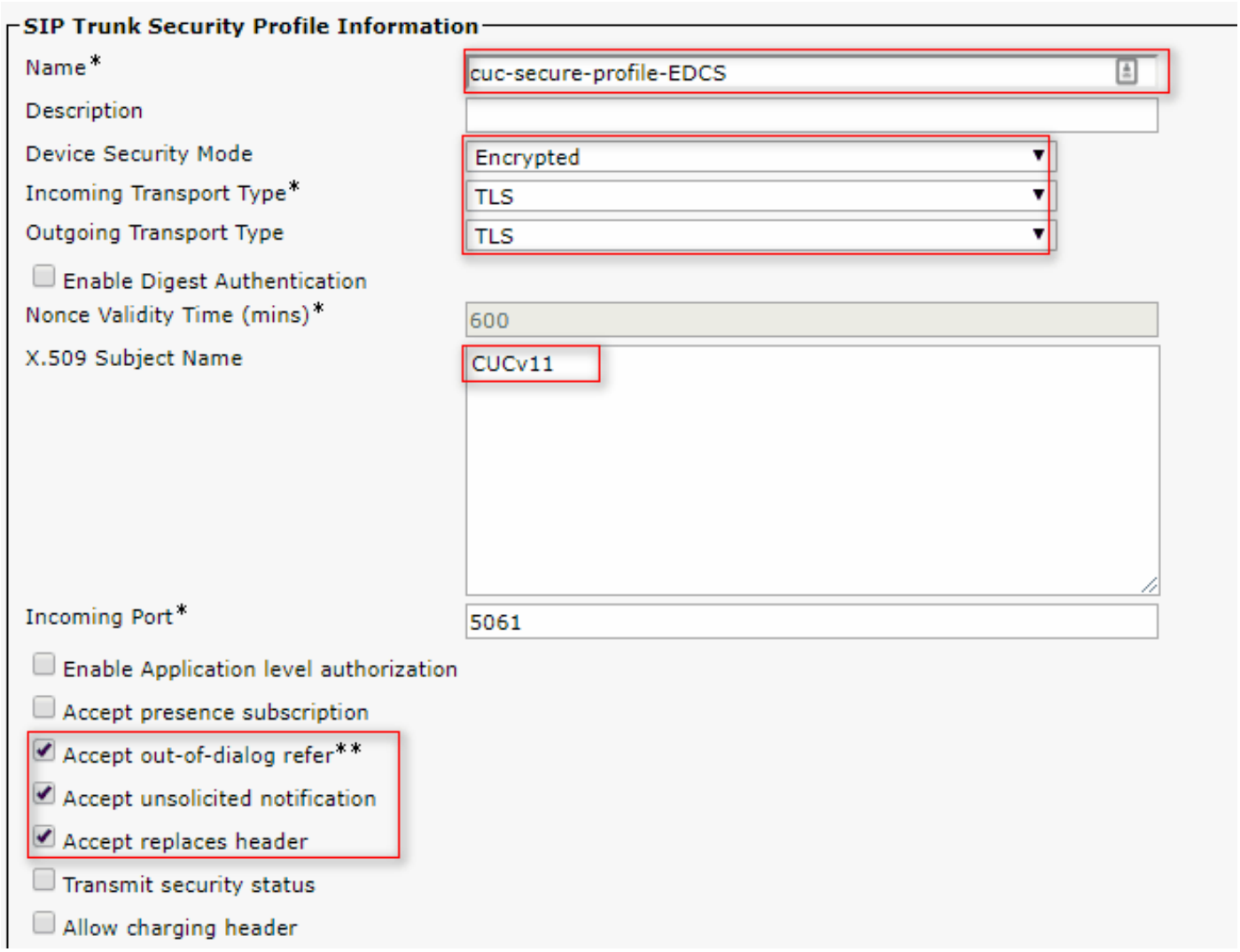
サード パーティ 認証の場合には、Unity Connection の CallManager 信頼のサード パーティ 認証局 （ CA ）のルートおよび中間物認証をアップロードして下さい。 これはサード パーティ CA が Call Manager 認証に署名したときだけ必要とされます。 このアクションを Cisco Unified OS 管理 > Security > Certificate Management へのナビゲートによって行い、認証を『Upload』 をクリック して下さい。



設定- Cisco Unified CM （ CUCM ）

1. SIP トランク セキュリティプロファイルを作成して下さい

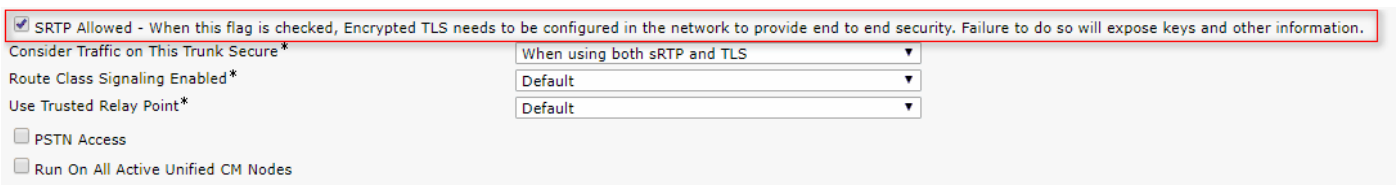
CUCM Administration > システム > Security > SIP トランク セキュリティプロファイルにナビゲート し、新しいプロファイルを追加して下さい。 X.509 サブジェクト名は CUC サーバの FQDN を一致する必要があります。

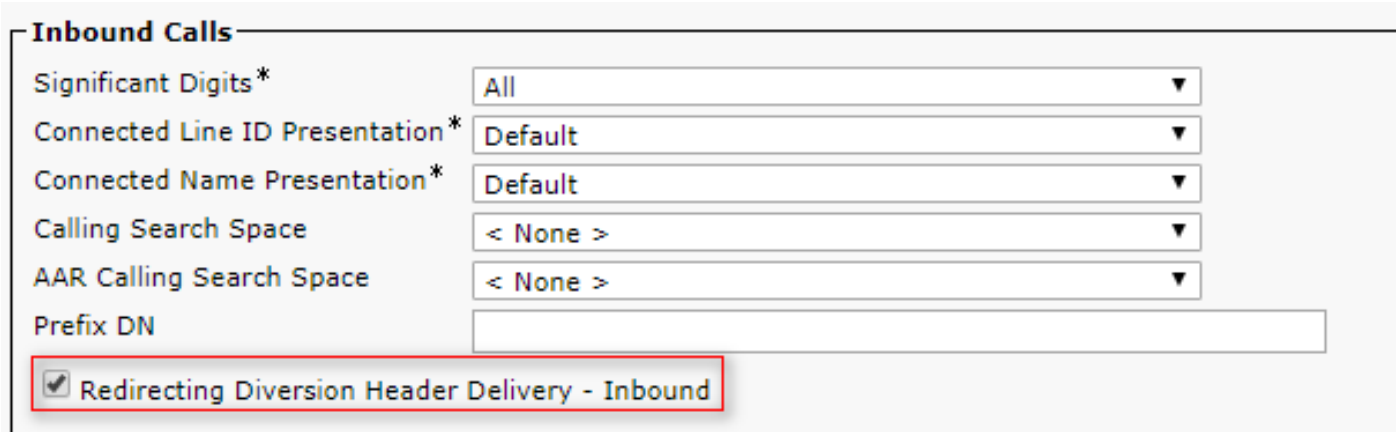


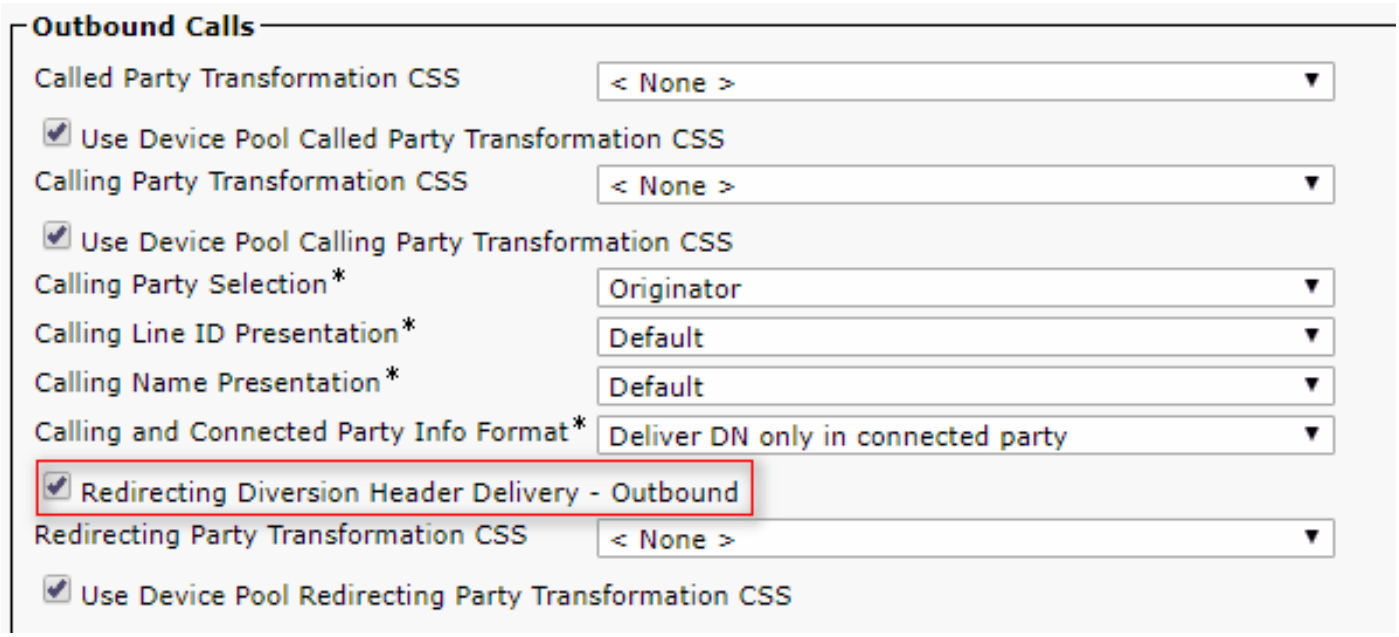
1. **注:** CLI コマンドは「CERT が Tomcat/tomcat.pem」を所有するために Unity Connection の RSA キーによって基づく Tomcat 認証を表示することができることを示します。 それは CN CUCM で設定される X.509 サブジェクト名を一致する必要がありますです。 CN はユニティサーバの FQDN/ホスト名と等しいです。 EC キーによって基づく認証は-認証対象代替名（SAN）フィールドの… FQDN/hostname が含まれています。

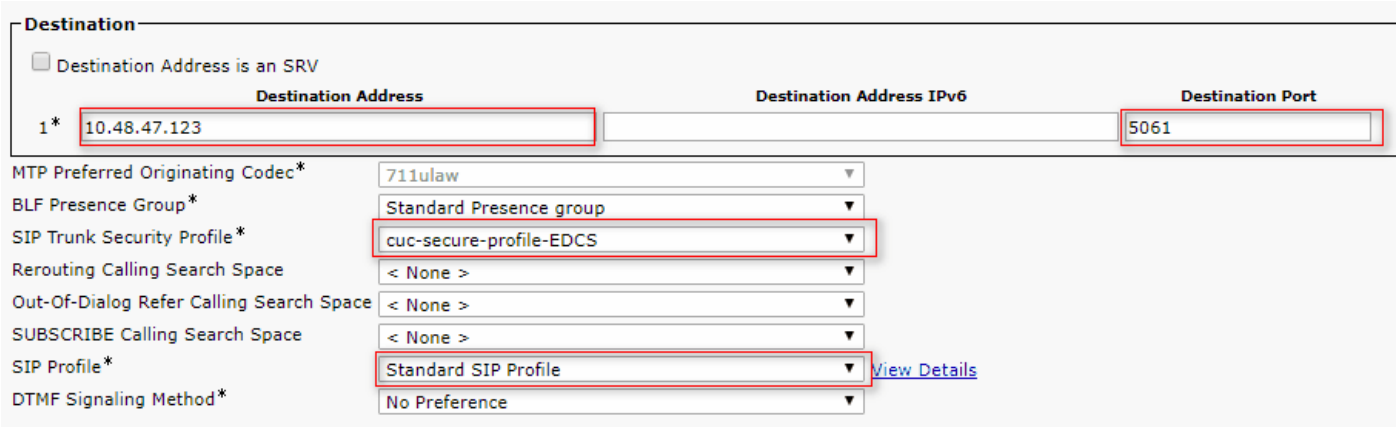
2. セキュア SIP トランクを作成して下さい

デバイス > トランクに > クリックし、追加し、新しい作成します Unity Connection とセキュア統合のために使用される標準 SIP トランクをナビゲート して下さい。





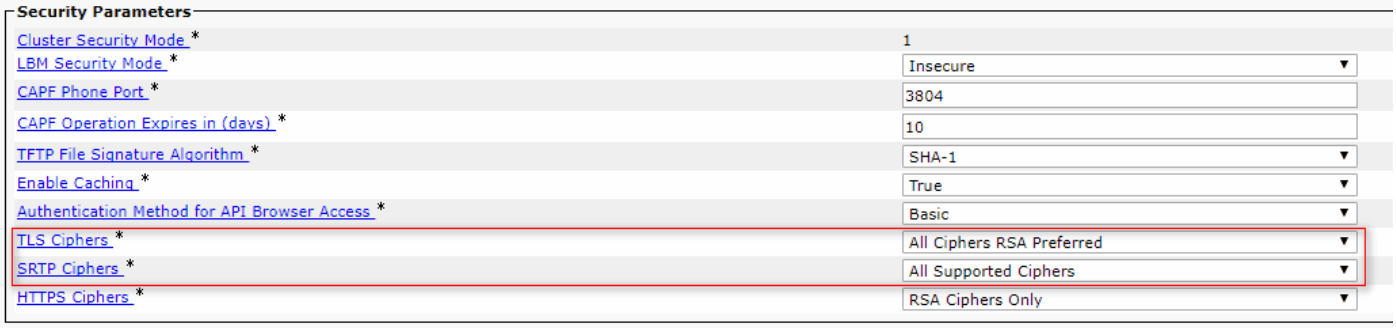




3. TLS および SRTP 暗号を設定して下さい

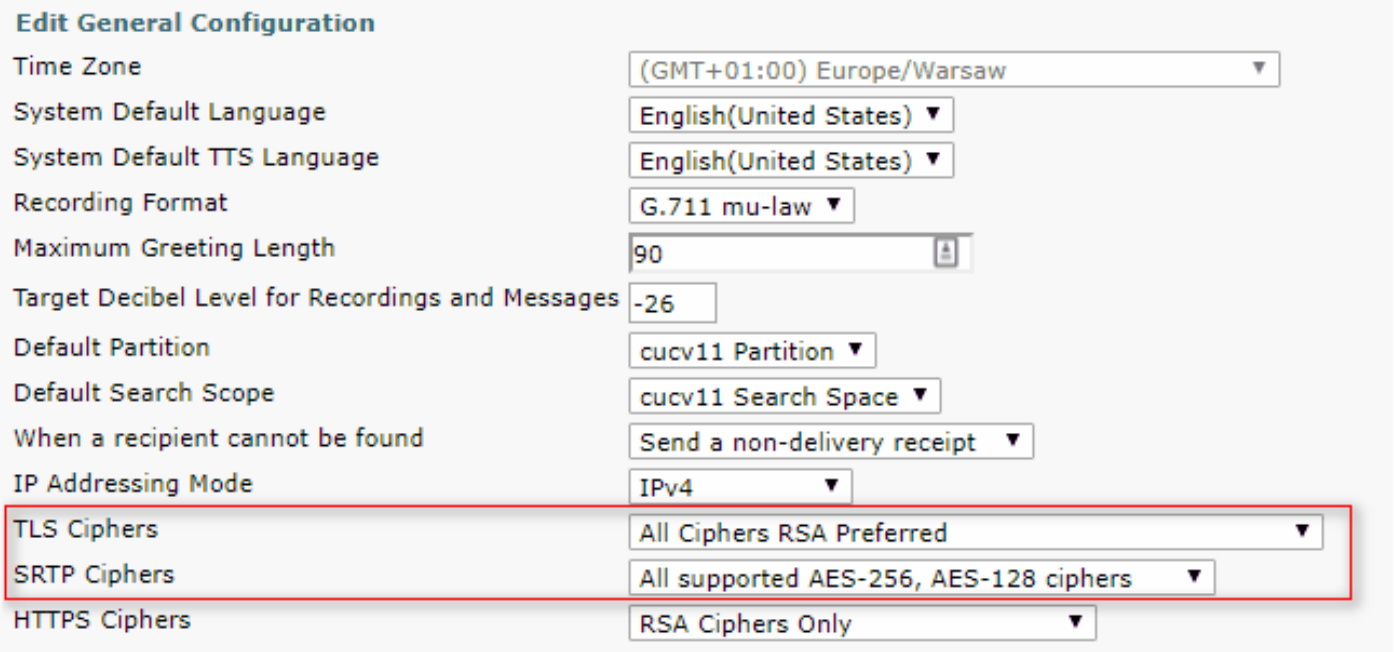
1. **注:** Unity Connection と Cisco Unified Communications Manager 間のネゴシエーションは次の状態の TLS 暗号設定によって決まります: Unity Connection がサーバとして機能するとき、TLS 暗号ネゴシエーションは Cisco Unified CM によって選択されるプリファレンスに基づいています。ECDSA によって基づく暗号がそれからネゴシエートされれば EC キー基づいた TomcatECDSA 認証は SSL ハンドシェイクで使用されます。RSA によって基づく暗号がそれからネゴシエートされれば RSA キー基づいた Tomcat 認証は SSL ハンドシェイクで使用されます。Unity Connection がクライアントとして機能するとき、TLS 暗号ネゴシエーションは Unity Connection によって選択されるプリファレンスに基づいています。

CM > システム > エンタープライズ パラメータは Cisco Unified にナビゲート し、ドロップダウン リストからの TLS および SRTP 暗号から適切な暗号オプションを選択します。



各ノードの Cisco Call Manager サービスを Cisco Unified サービサビリティ ページ、ツール > コントロール センター機能 サービスへのナビゲートによって再開し、CM サービスの下で『Cisco Call Manager』 を選択 して下さい

Cisco Unity Connection 管理 ページ > システム設定 > 一般的 な 設定にナビゲート し、ドロップダウン リストからの TLS および SRTP 暗号から適切な暗号オプションを選択して下さい。



Cisco Unity Connection サービサビリティ > Tools > Service 管理へのナビゲートによって各ノードの接続メッセージ交換マネージャを再起動して下さい。

TLS は優先順位のオプションを暗号化します

TLS 暗号オプション	優先順位の TLS 暗号
最も強い AES-256 SHA-384 だけ: 好まれる RSA	• TLS_ECDHE_RSA_WITH_AES_256_GC M_SH • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384
Strongest-AES-256 SHA-384 だけ: 好まれる ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ 84 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
Medium-AES-256 AES-128 だけ: 好まれる RSA	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SH • TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384

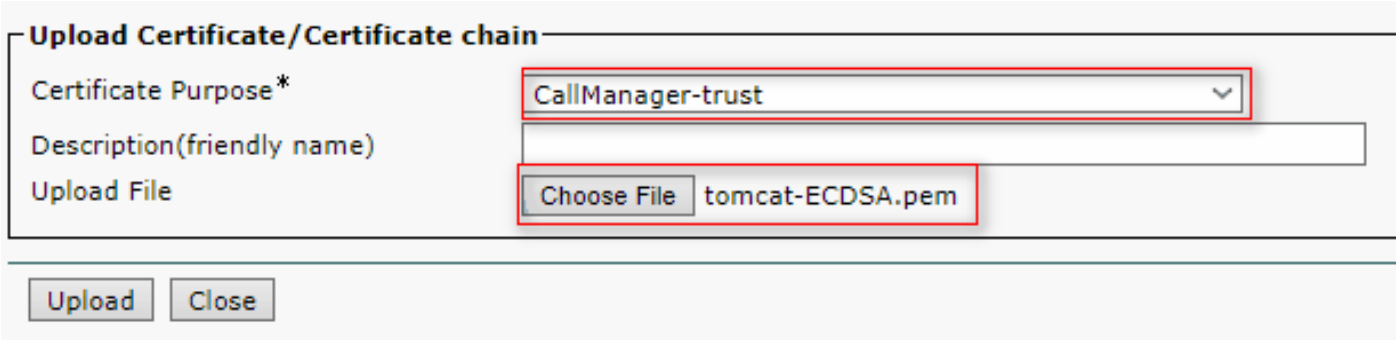
Medium-AES-256 AES-128 だけ: 好まれる ECDSA	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SH • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 56 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ 84 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 56 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ 84
好まれるすべての暗号 RSA （デフォルト）	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SH • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 56 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ 84 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
好まれるすべての暗号 ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ 56 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH • TLS_RSA_WITH_AES_128_CBC_SHA

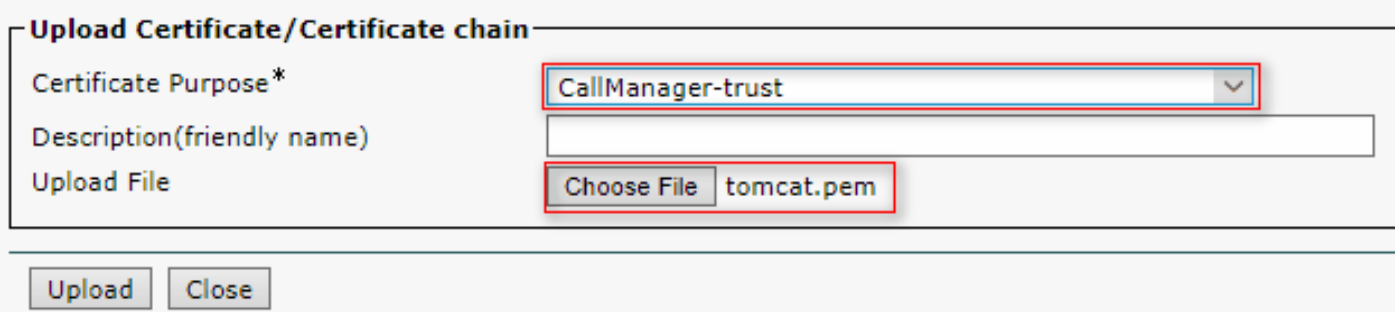
優先順位の SRTP 暗号オプション

SRTP 暗号オプション	優先順位の SRTP
すべては AES-256 を、AES-128 暗号サポートしました	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1 _32
AEAD AES-256、AES-28 GCM ベースの暗号	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
AEAD AES256 GCM ベースの暗号だけ	• AEAD_AES_256_GCM

4. アップロード CUC Tomcat 認証（基づいて RSA 及び EC）

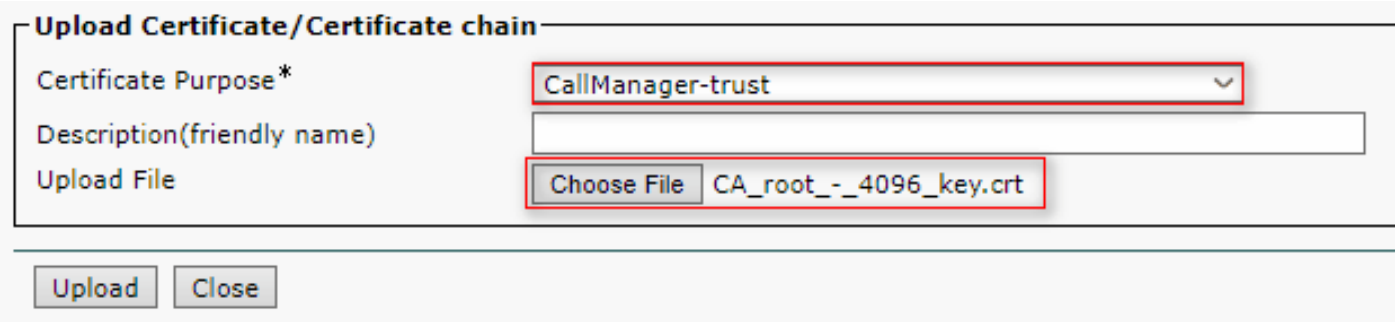
OS 管理 > Security > Certificate Management にナビゲート し、CallManager 信頼ストアに両方の CUC Tomcat 認証を（基づく RSA 及び EC）アップロードして下さい。





1. **注:** 両方の Unity Tomcat 認証をアップロードすることは ECDSA 暗号がただネゴシエートされる場合必須ではないです。 そのようなケース EC によって基づく Tomcat 認証で十分はあります。

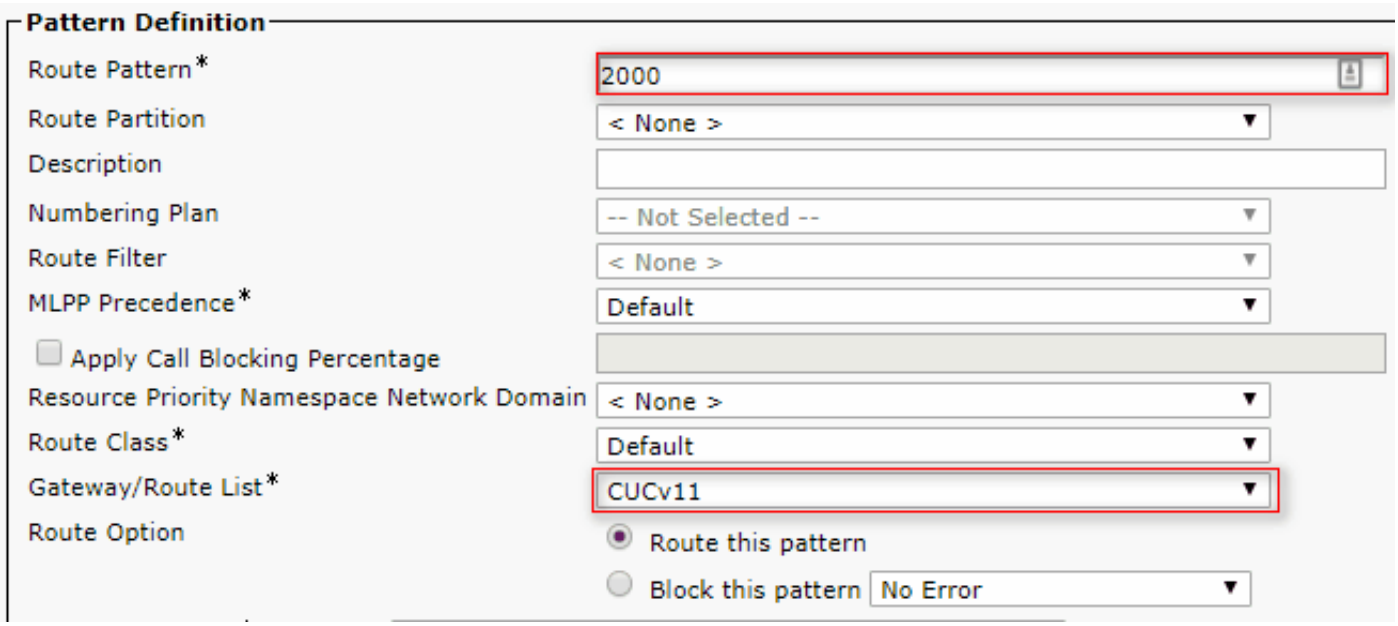
サード パーティ 認証の場合には、サード パーティ 認証局 （ CA ）のルートおよび中間物認証をアップロードして下さい。 これはサード パーティ CA が Unity Tomcat 認証に署名したときだけ必要とされます。



変更を加えるためにすべてのノードの Cisco Call Manager プロセスを再起動して下さい。

5. ルートパターンを作成して下さい

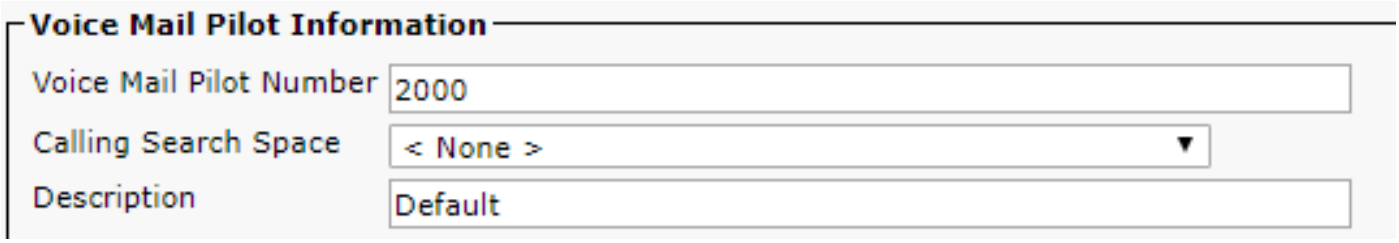
呼ルーティング > ルート/ハントする > ルートパターンへのナビゲートによる設定されたトランクへのポイント ルートパターンを設定して下さい。 ルートパターン数として入力されるエクステンションは音声メール パイロットとして使用することができます。



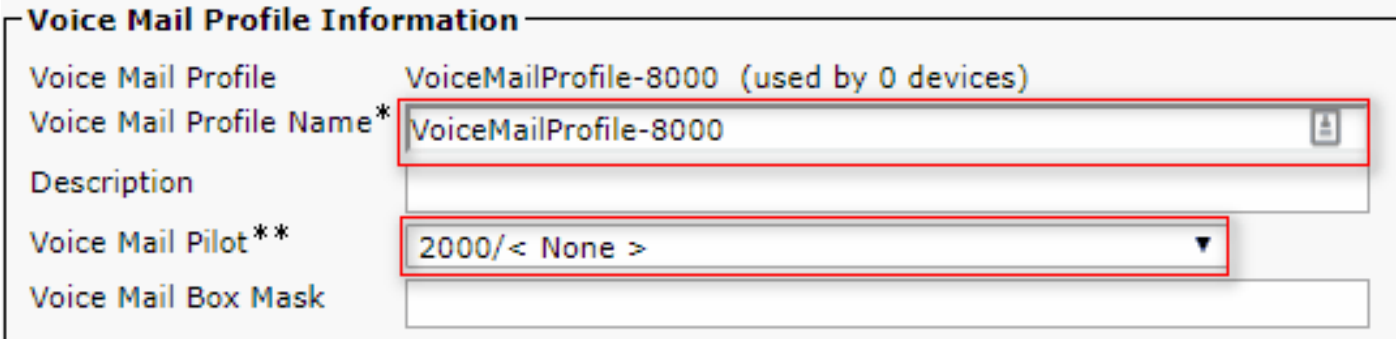
6. 音声メール パイロットを、音声メール プロファイル作成し、DN にそれを割り

当てて下さい

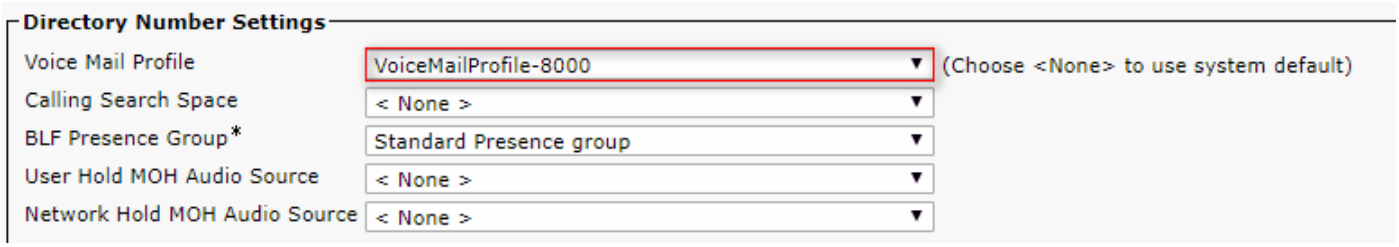
進んだ機能 > 音声メール > 音声メールパイロットへ行くことによって統合のための音声メールパイロットを作成して下さい。



すべての設定進んだ機能 > 音声メール > 音声メール プロファイルをリンクするために音声メールプロファイルを作成して下さい



セキュア統合を使用するように呼ルーティング > ディレクトリ番号へ行くことによって意図されている DN に新しく作成された音声メール プロファイルを割り当てて下さい



設定- EC キーに署名することはサード パーティ CA （オプションの）によって認証を基づかせていました

認証はシステム間のセキュア統合を設定する前のサード パーティ CA によって署名されるかもしれません。 両方のシステムの認証に署名するために次のステップに従って下さい。

Cisco Unity Connection

1. CUC TomcatECDSA のための証明書署名要求（CSR）を生成し、認証をサード パーティ CA によって署名してもらって下さい
2. CA はように続くアップロードする必要がある CA 認証（CA ルート証明）をおよび ID証明（CA 署名入り認証）提供します:
   Tomcat 信頼ストアに CA ルート証明をアップロードして下さい
   Tomcat EDCS ストアに ID証明をアップロードして下さい
3. CUC のメッセージ交換マネージャを再起動して下さい

Cisco Unified CM

1. CUCM CallManagerECDSA のための CSR を生成し、認証をサード パーティ CA によって署名してもらって下さい
2. CA はように続くアップロードする必要がある CA 認証（CA ルート証明）をおよび ID証明（CA 署名入り認証）提供します:
   CallManager 信頼ストアに CA ルート証明をアップロードして下さい
   CallManager EDCS ストアに ID証明をアップロードして下さい
3. Cisco CCM を再起動し、各ノードのサービスを TFTP して下さい

同じプロセスが CSR が CUC Tomcat 認証および CallManager 認証のために生成され、Tomcat ストアおよびそれぞれ CallManager ストアにアップロードされる RSA キーによって基づいた認証に署名するのに使用されます。

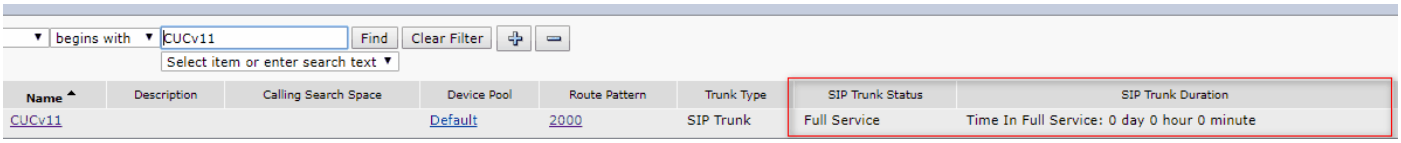
確認

ここでは、設定が正常に動作していることを確認します。

SIP トランク 確認を保護して下さい

音声メールを呼出すために電話の音声メール ボタンを押して下さい。 ユーザの拡張が Unity Connection システムで設定されない場合開始グリーティングを聞くはずです。

また、SIP トランクステータスを監視することを SIP オプション キープアライブが可能に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る SIP プロファイルで有効に することができます。 これが有効に なれば下記に示されているようにデバイス > トランクによって一ロトランクステータスを監視できます:



セキュア RTP コール 確認

パッドロック の アイコンが Unity Connection に呼び出しにあるかどうか確かめて下さい。 それは RTP がこのイメージに示すようにストリーム（デバイスセキュリティ プロファイルははたらくためにそれのためにセキュアである必要があります）暗号化されることを意味します

関連情報

- Cisco Unity Connection リリース 11.x のための SIP 統合ガイド