Contact Center Enterpriseでのセキュアシグナリングの設定

内容

概要

このドキュメントでは、Contact Center Enterprise(CCE)の包括的なコールフローでSession Initiation Protocol(SIP)シグナリングを保護する方法について説明します。

前提条件

証明書の生成とインポートについては、このドキュメントでは扱いません。そのため、Cisco Unified Communication Manager(CUCM)、Customer Voice Portal(CVP)コールサーバ、Cisco Virtual Voice Browser(CVVB)、およびCisco Unified Border Element(CUBE)の証明書を作成し、各コンポーネントにインポートする必要があります。自己署名証明書を使用する場合は、異なるコンポーネント間で証明書を交換する必要があります。

要件

次の項目に関する知識があることが推奨されます。

- CCE
- CVP
- CUBE
- CUCM
- CVVB

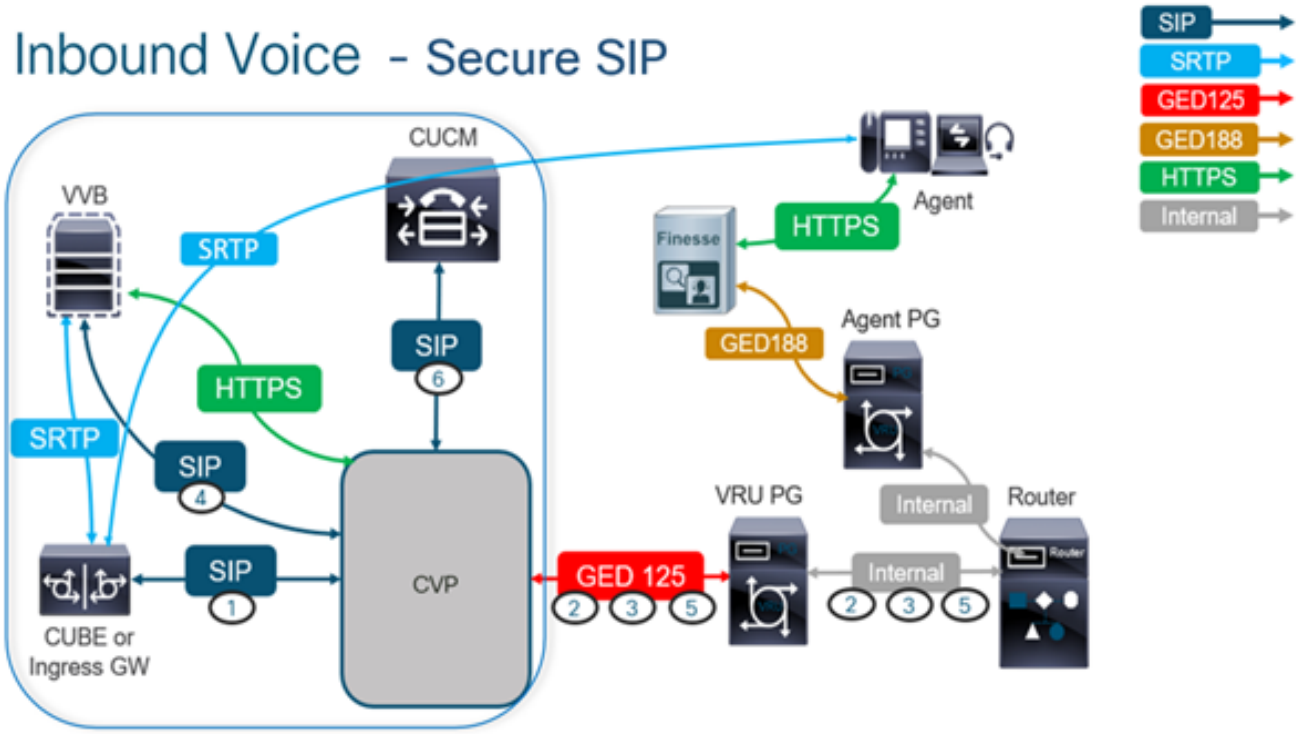
使用するコンポーネント

このドキュメントの情報は、Package Contact Center Enterprise(PCCE)、CVP、CVVB、およびCUCMバージョン12.6に基づいていますが、それ以前のバージョンにも適用できます。

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。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

次の図は、コンタクトセンターの包括的なコールフローでSIPシグナリングに関与するコンポーネントを示しています。システムに音声コールが着信すると、最初に入力ゲートウェイまたはCUBE経由で着信するため、CUBEでセキュアSIP設定を開始します。次に、CVP、CVVB、およびCUCMを設定します。



タスク 1.CUBEセキュア設定

この作業では、SIPプロトコルメッセージを保護するようにCUBEを設定します。

必要な設定：

- SIPユーザエージェント(UA)のデフォルトのトラストポイントの設定
- Transport Layer Security(TLS)を使用するためのダイヤルピアの変更

手順：

1. CUBEへのセキュアシェル(SSH)セッションを開きます。
2. SIPスタックでCUBEの認証局(CA)証明書を使用するには、次のコマンドを実行します。

CUBEは、CUCM(198.18.133.3)およびCVP(198.18.133.13)との間でSIP TLS接続を確立します。

conf t sip-ua transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit

```
CC-VCUBE(config)#sip-ua
CC-VCUBE(config-sip-ua)#transport tcp tls v1.2
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#exit
CC-VCUBE(config)#
```

3. CVPへの発信ダイヤルピアでTLSを有効にするには、次のコマンドを実行します。この例では、ダイヤルピアタグ6000を使用してコールをCVPにルーティングします。

Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls exit

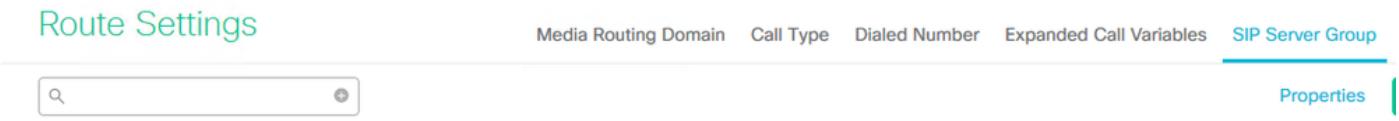
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#
CC-VCUBE(config-dial-peer)#exit
CC-VCUBE(config)#
```

タスク 2.CVPセキュア設定

この作業では、SIPプロトコルメッセージ(SIP TLS)を保護するようにCVPコールサーバを設定します。

手順：

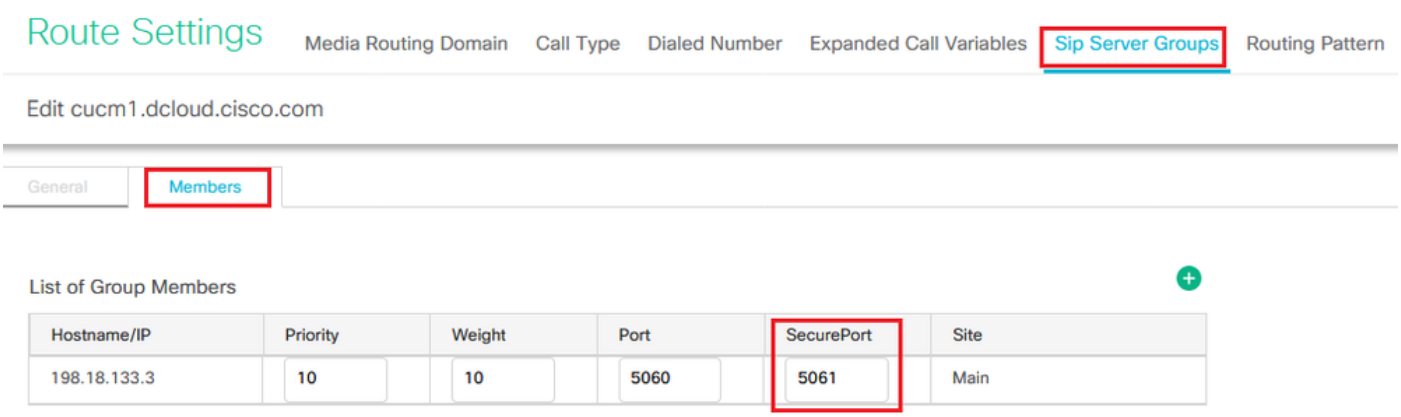
1. ログイン先UCCE Web Administration.
2. 移動先 Call Settings > Route Settings > SIP Server Group.



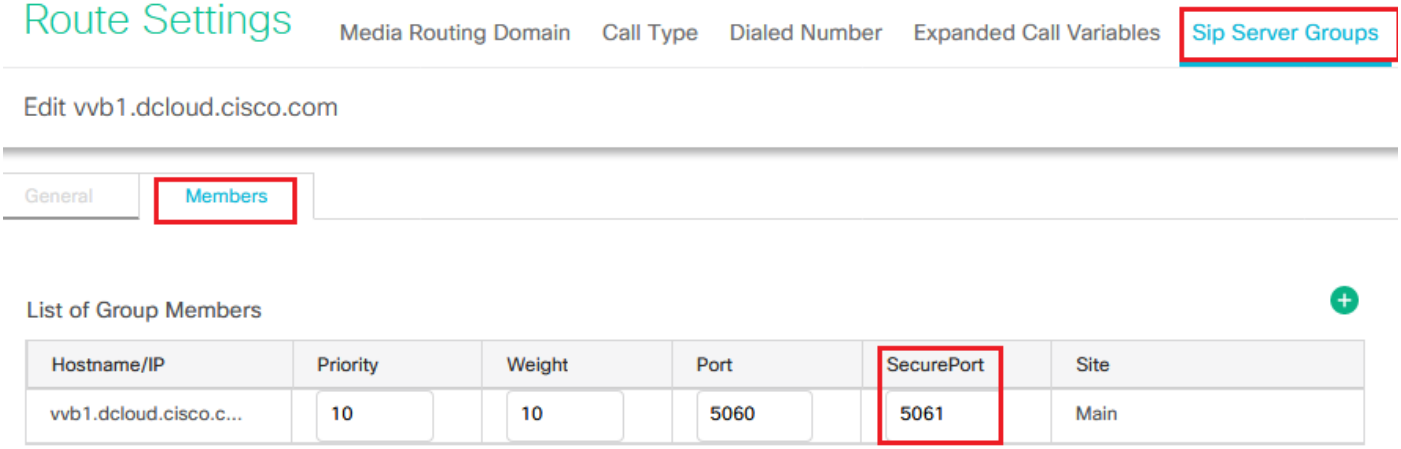
設定に基づいて、CUCM、CVVB、およびCUBEに対してSIPサーバグループが設定されています。これらすべてに対して、セキュアSIPポートを5061に設定する必要があります。この例では、次のSIPサーバグループが使用されます。

- cucm1.dcloud.cisco.com CUCMの場合
- vvb1.dcloud.cisco.com CVVBの場合
- cube1.dcloud.cisco.com CUBE用

3. クリック cucm1.dcloud.cisco.com その後、 **Members** SIPサーバグループ設定の詳細を表示します。Set SecurePort から 5061 をクリックし、 Save .



4. クリック vvb1.dcloud.cisco.com その後、 **Members** tab.SecurePortをに設定 5061 をクリックし、Save.

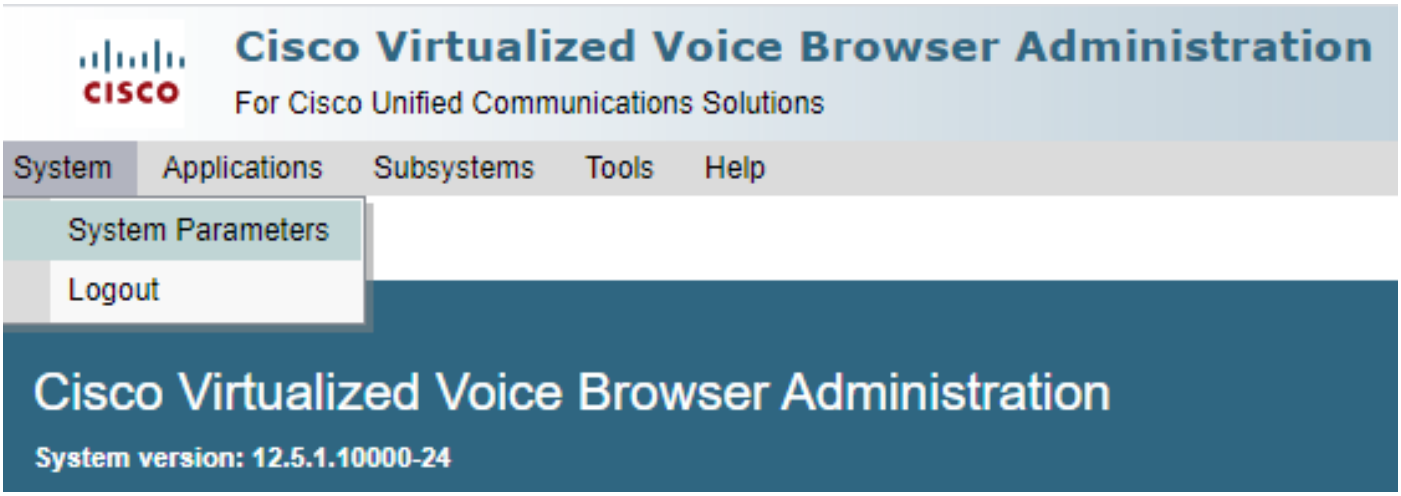


タスク 3.CVVBセキュア設定

この作業では、SIPプロトコルメッセージ(SIP TLS)を保護するようにCVVBを設定します。

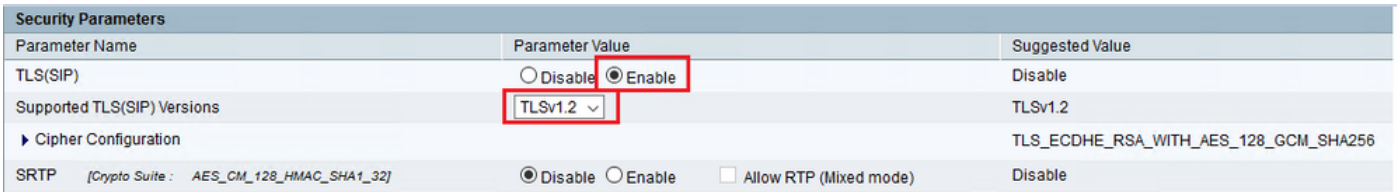
手順：

1. ログイン先 **Cisco VVB Administration** ページを使用します。
2. 移動先 System > System Parameters.

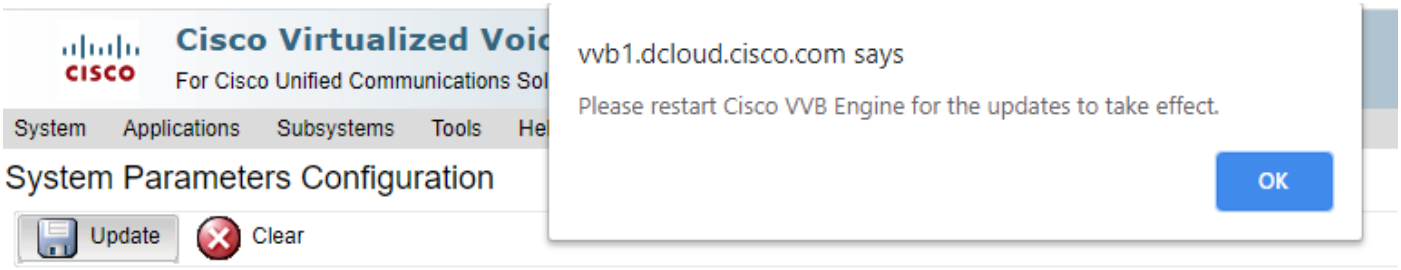


3. 内 Security Parameters セクション、選択 Enable を参照 TLS(SIP)．保持 Supported TLS(SIP)

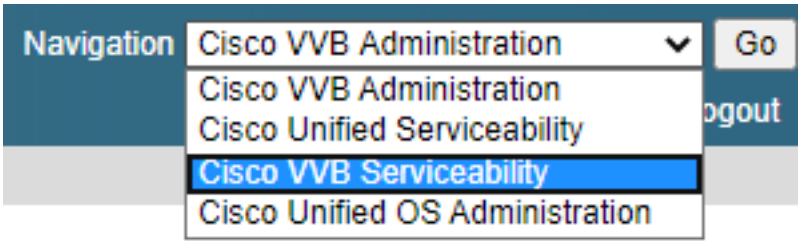
version as TLSv1.2.



4. [Update] をクリックします。クリック Ok CVVBエンジンを再起動するように求めるプロンプトが表示されます。

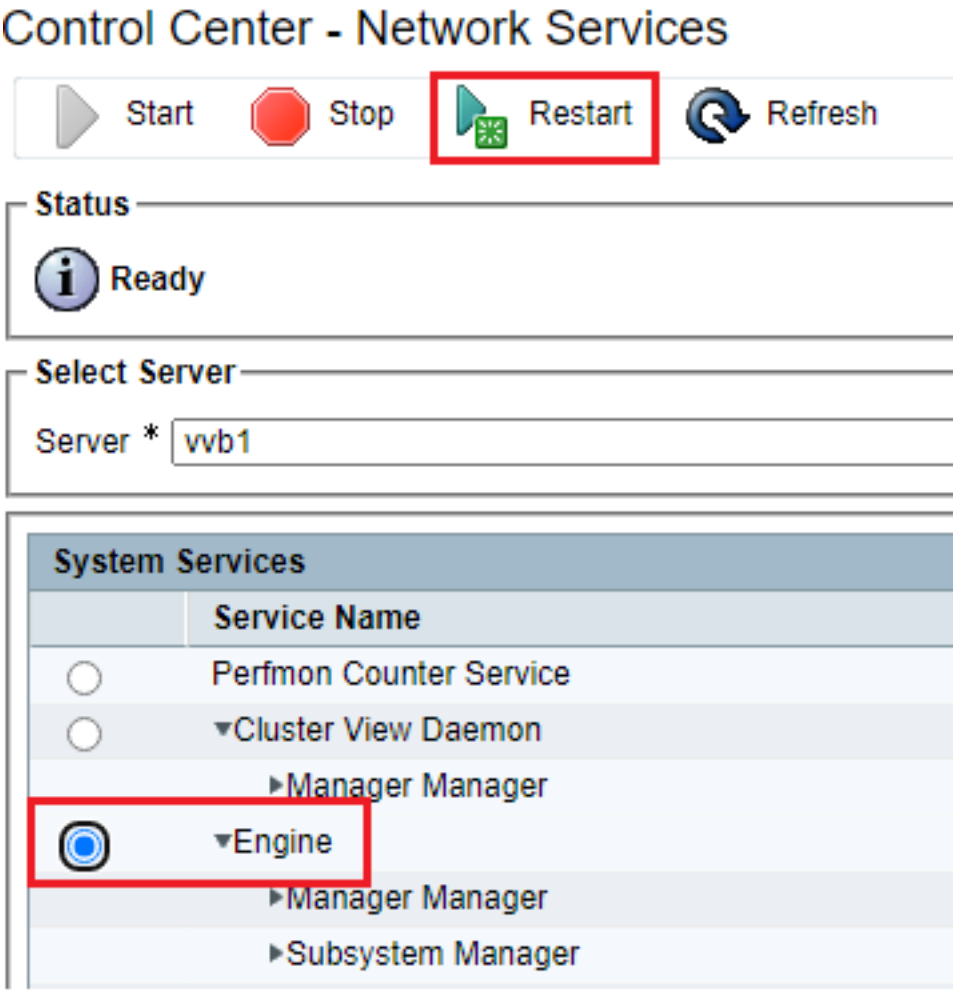


5. これらの変更を行うには、Cisco VVBエンジンを再起動する必要があります。VVBエンジンを再起動するには、 Cisco VVB Serviceability 次に、 **Go**.



6. 移動先 Tools > Control Center – Network Services.

7. 選択 Engine をクリックし、 Restart.



タスク 4.CUCMセキュア設定

CUCMでSIPメッセージを保護するには、次の設定を実行します。

- CUCMセキュリティモードを混合モードに設定する
- CUBEおよびCVPのSIPトランクセキュリティプロファイルの設定
- 各SIPトランクへのSIPトランクセキュリティプロファイルの関連付け
- CUCMとのセキュアエージェントのデバイス通信

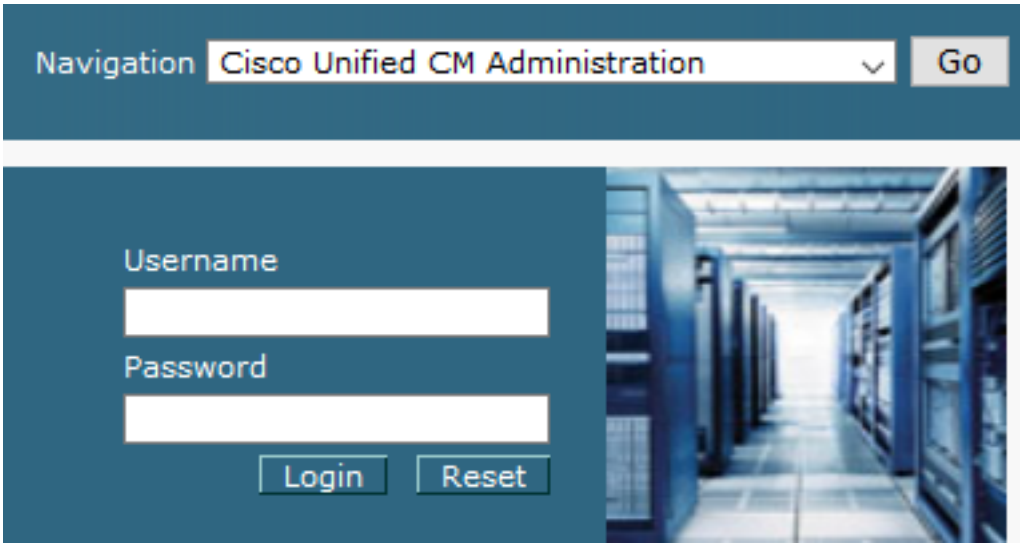
CUCMセキュリティモードを混合モードに設定する

CUCMは、次の2つのセキュリティモードをサポートしています。

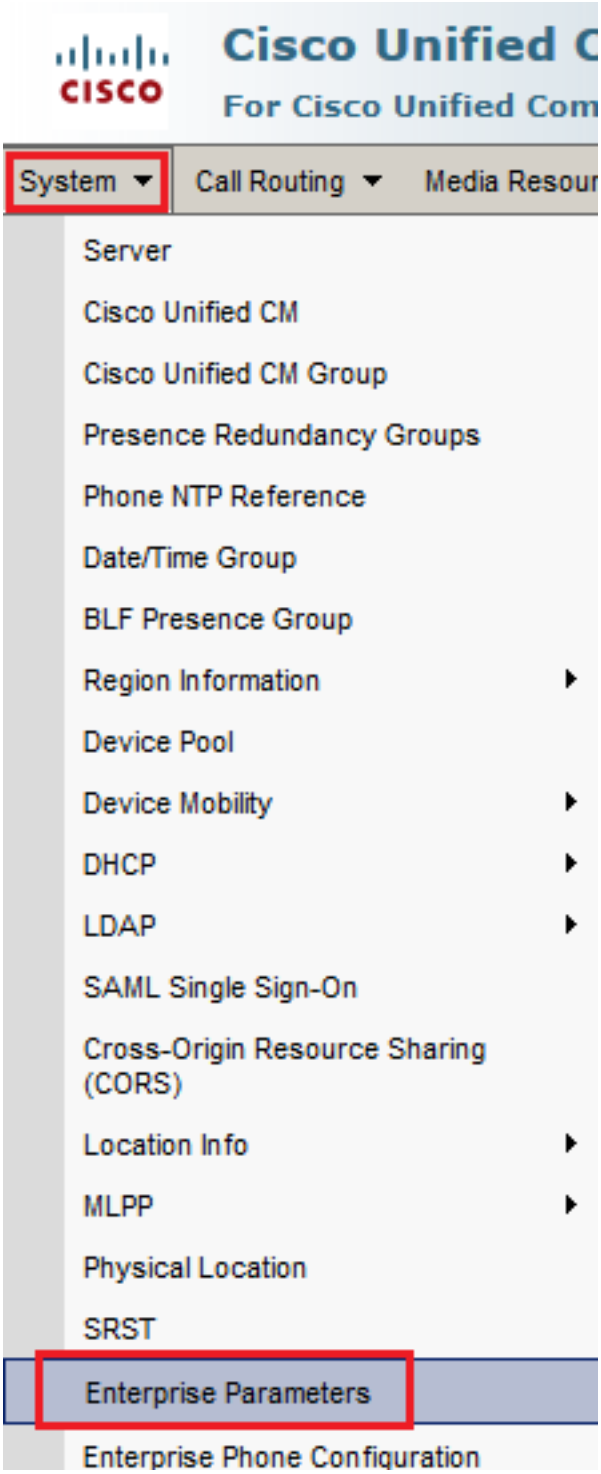
- 非セキュアモード（デフォルトモード）
- 混合モード（セキュアモード）

手順：

1. セキュリティモードを混合モードに設定するには、にログインします Cisco Unified CM Administration サポートされていません。



2. CUCMに正常にログインした後、 System > Enterprise Parameters.

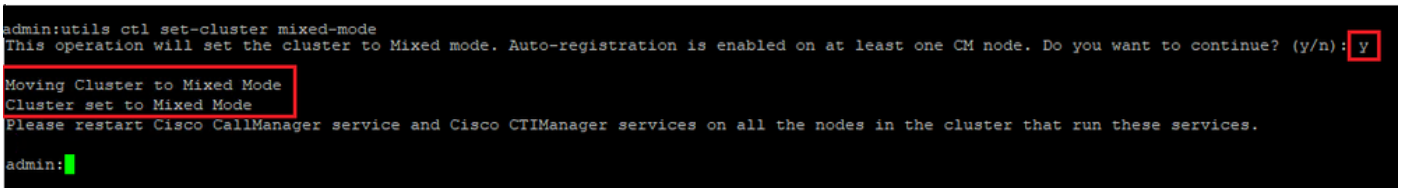


3. その下に Security Parameters セクションをチェックします。 Cluster Security Mode に設定されている 0.

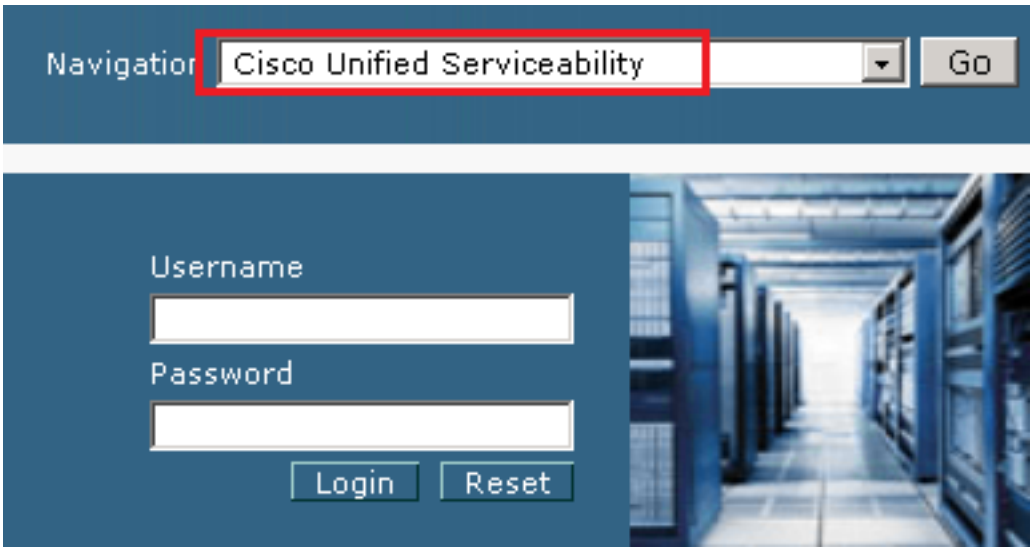
4. [クラスタセキュリティモード(Cluster Security Mode)]が0に設定されている場合は、クラスタセキュリティモードが非セキュアに設定されていることを意味します。CLIから混合モードを有効にする必要があります。
5. CUCMへのSSHセッションを開きます。

6. SSH経由でCUCMに正常にログインしたら、次のコマンドを実行します。 utils ctl set-cluster mixed-mode

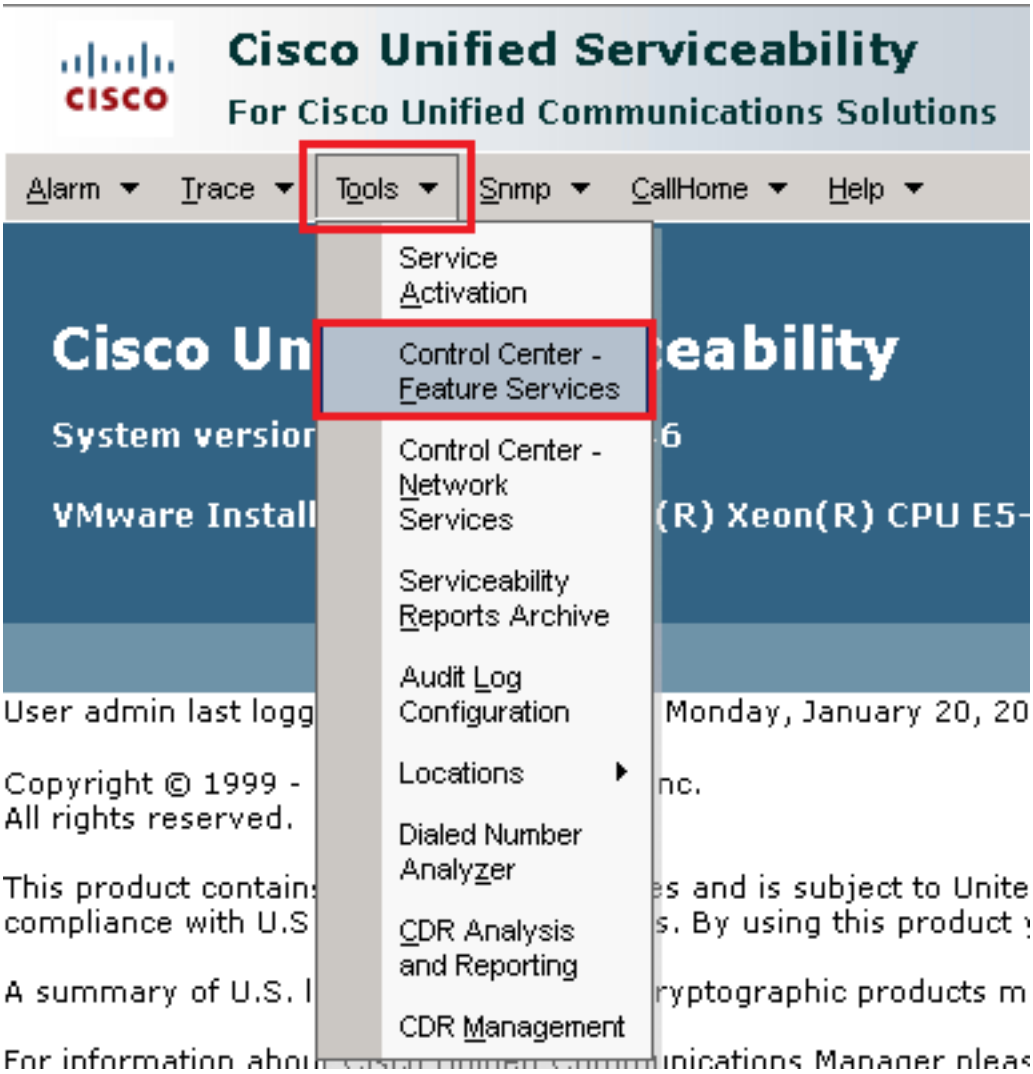
7. Type y プロンプトが表示されたら、**Enter**をクリックします。このコマンドは、クラスタセキュリティモードを混合モードに設定します。



8. 変更を有効にするには、 Cisco CallManager と Cisco CTIManager サービス.
9. サービスを再起動するには、に移動してログインします Cisco Unified Serviceability.

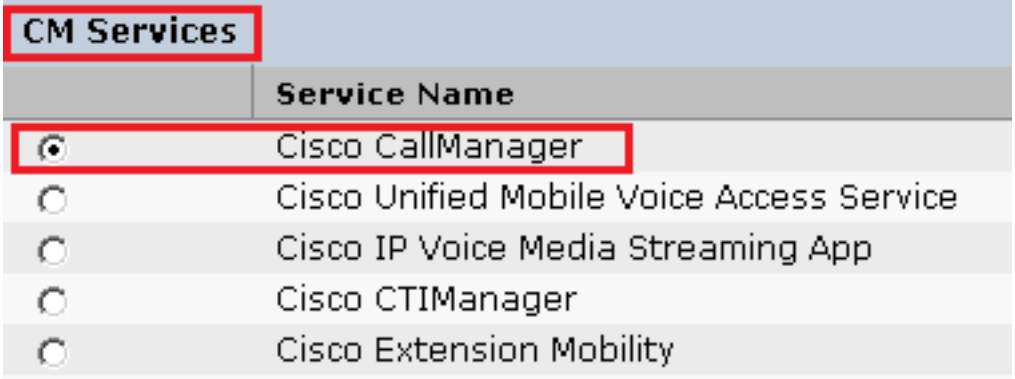


10. 正常にログインしたら、に移動します。 Tools > Control Center – Feature Services.

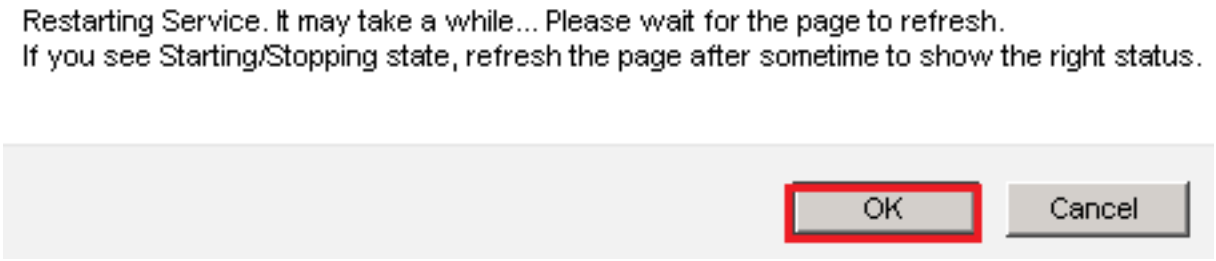


11. サーバを選択し、 Go.

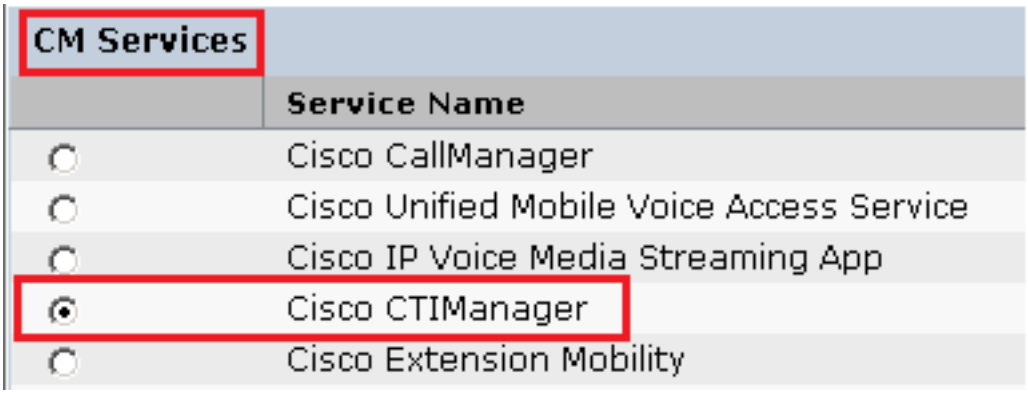
12. CMサービスの下で、 Cisco CallManager 次に、 Restart ボタンをクリックします。



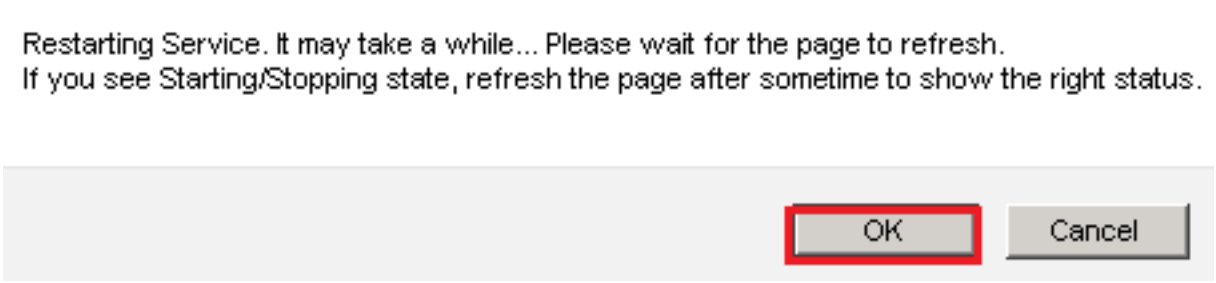
13. ポップアップメッセージを確認し、 OK.サービスが正常に再起動するまで待ちます。



14. 再起動が成功した後 Cisco CallManager[Cisco]を選択します。 **CTIManager** 次に、 Restart 再起動するボタン Cisco CTIManager service .



15. ポップアップメッセージを確認し、 OK.サービスが正常に再起動するまで待ちます。

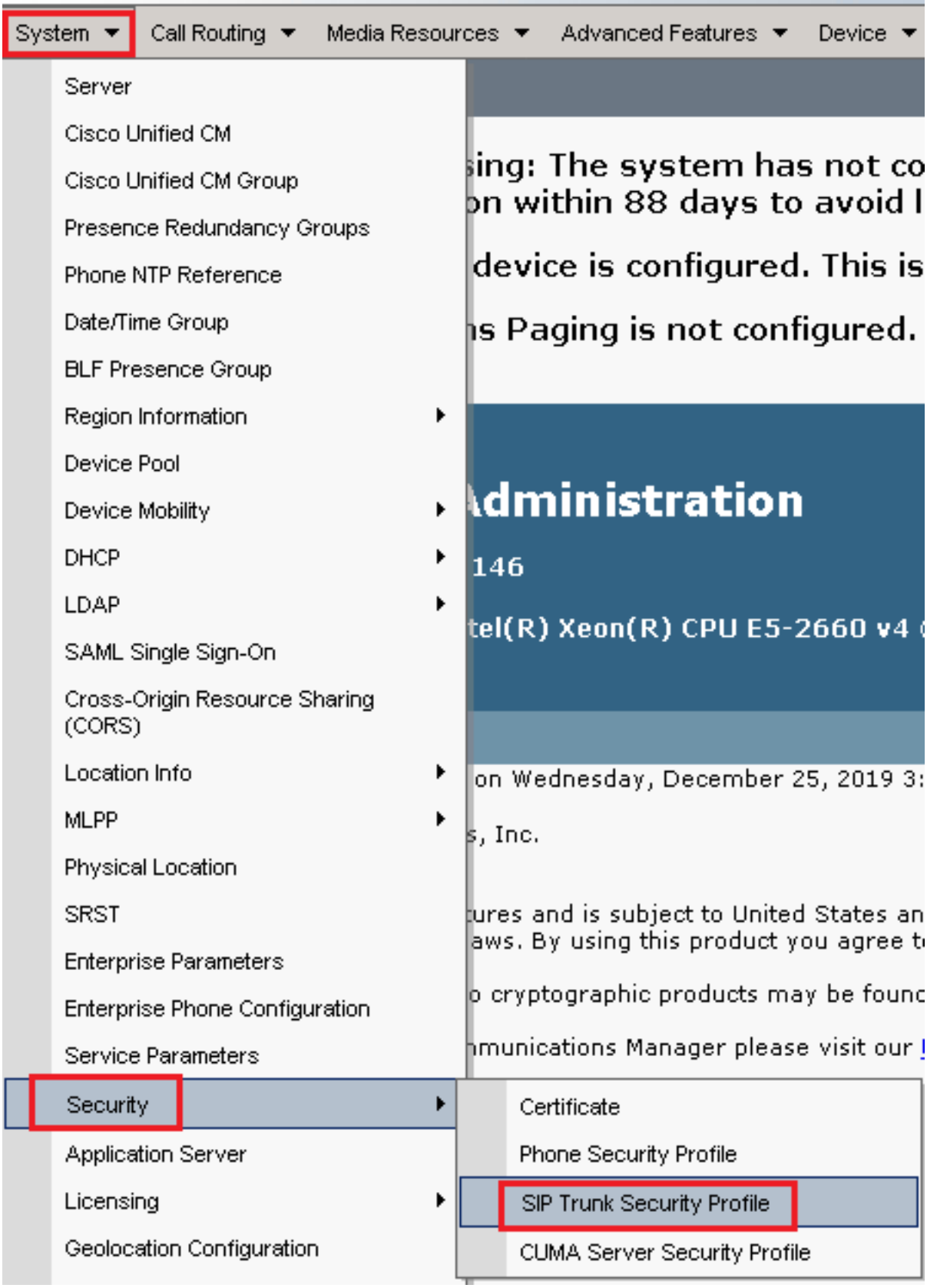


16. サービスが正常に再起動したら、クラスタセキュリティモードが混合モードに設定されていることを確認し、手順5で説明されているようにCUCM管理に移動します。次に、 **Cluster Security Mode**.次に設定する必要があります。 1.

CUBEおよびCVPのSIPトランクセキュリティプロファイルの設定

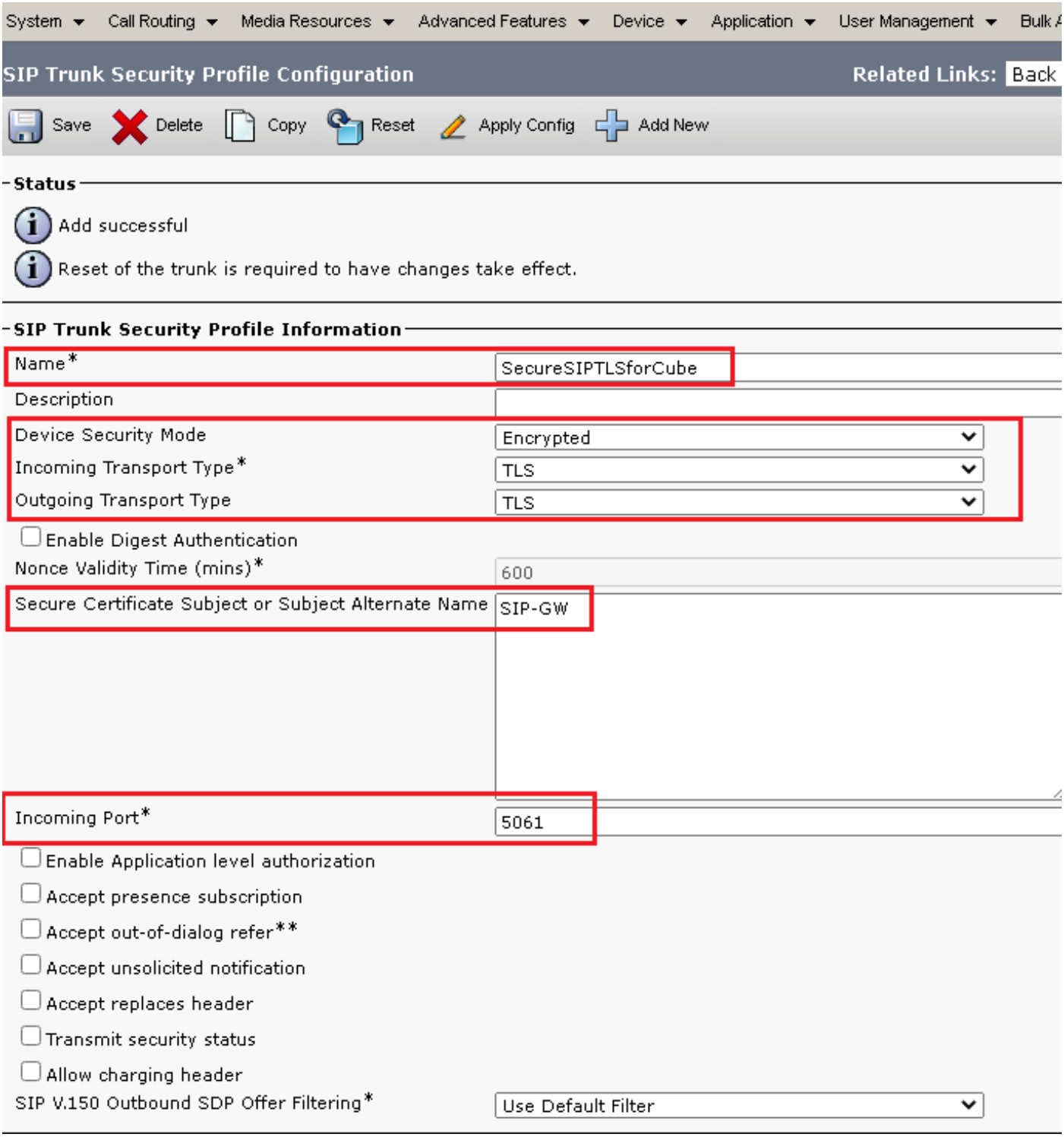
手順：

1. ログイン先 CUCM administration サポートされていません。
2. CUCMに正常にログインした後、 System > Security > SIP Trunk Security Profile CUBEのデバイスセキュリティプロファイルを作成します。



3. 左上で、 Add New 新しいプロファイルを追加します。

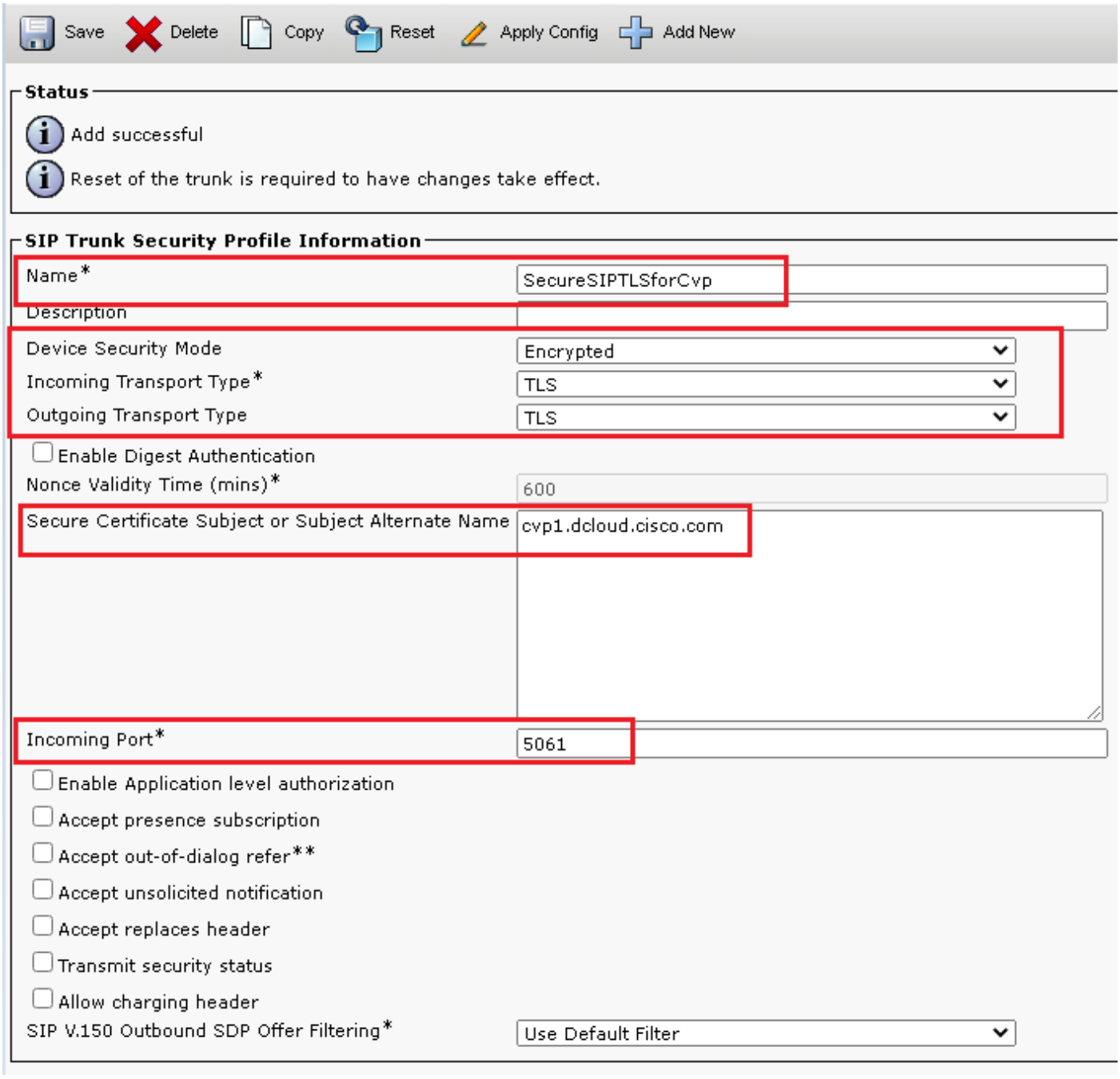
4. 設定 SIP Trunk Security Profile 次の図に示すように、 Save ページの左下で～する Save IT。



5. VLANの設定を Secure Certificate Subject or Subject Alternate Name CUBE証明書の共通名(CN)に一致する

必要があります。

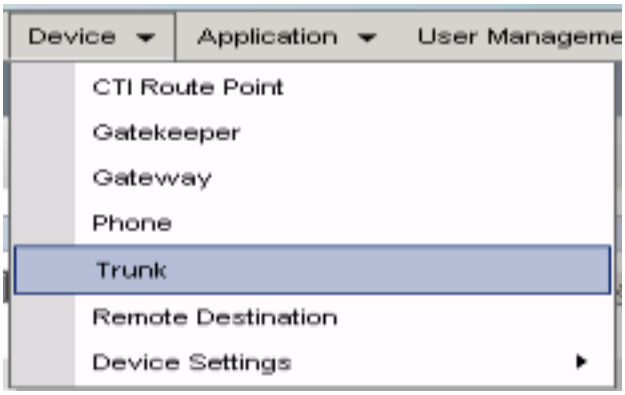
6.クリック Copy ボタンをクリックし、 Name から SecureSipTLSforCVP および Secure Certificate Subject 一致する必要があるCVPコールサーバ証明書のCNに送信します。クリック Save をクリックして、クエリーを実行します。



各SIPトランクへのSIPトランクセキュリティプロファイルの関連付け

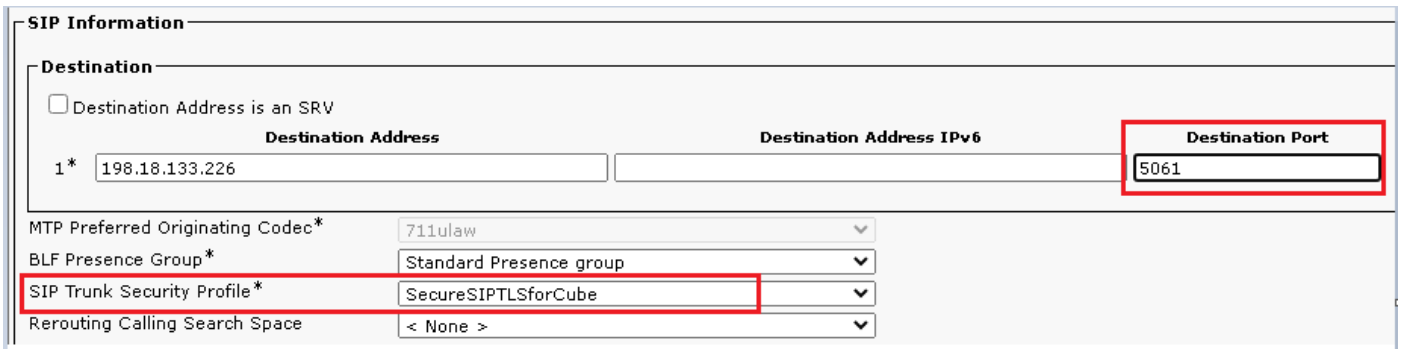
手順：

1. [CUCM Administration]ページで、 Device > Trunk.

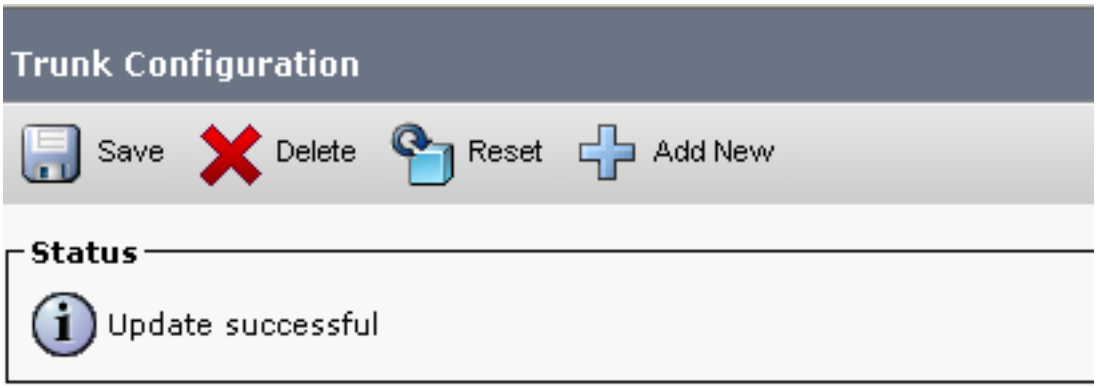


2. CUBEトランクを検索します。この例では、CUBEトランク名は vCube . クリック **Find**.

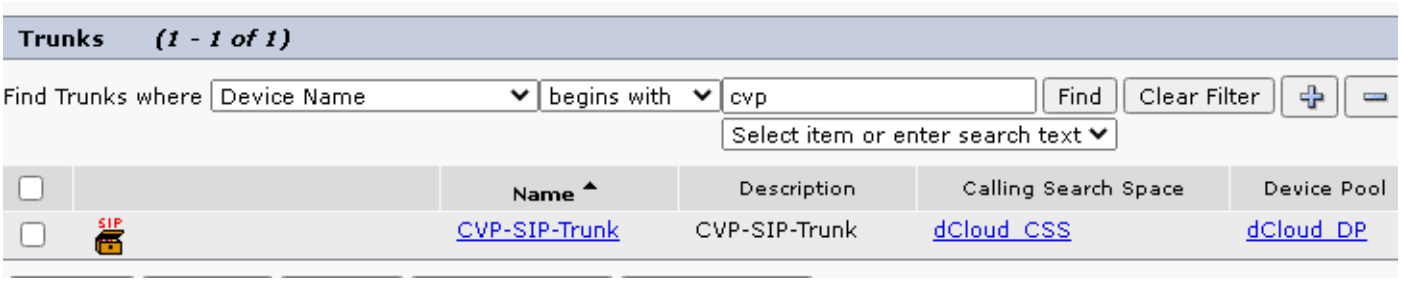
3. [vCUBE]をクリックして、[vCUBEトランク設定(vCUBE trunk configuration)]ページを開きます。
4. 下にスクロールして SIP Information セクションに移動し、 Destination Port から 5061.
5. Change SIP Trunk Security Profile から SecureSIPTLSForCube.



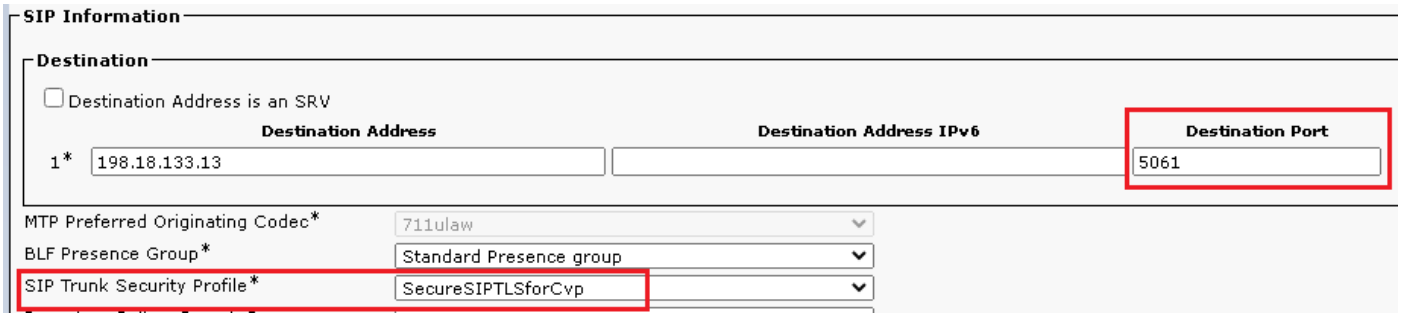
6. クリック Save then Rest ～するために Save 変更を適用します



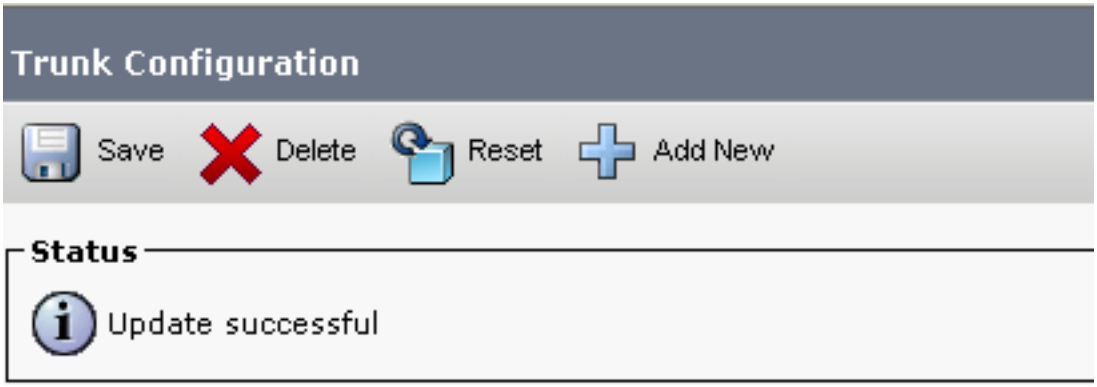
7. 移動先 Device > Trunk、CVPトランクを検索します。この例では、CVPトランク名は cvp-SIP-Trunk . クリック **Find**.



8. クリック CVP-SIP-Trunk CVPトランク設定ページを開きます。
9. 下にスクロールして SIP Information セクション、および変更 Destination Port から 5061 .
10. Change SIP Trunk Security Profile から SecureSIPTLSForCvp.



11. クリック Save then Rest ～するために save 変更を適用します



CUCMとのセキュアエージェントのデバイス通信

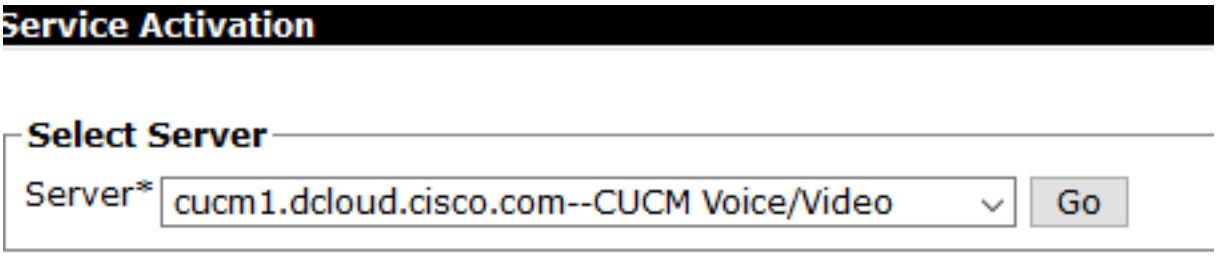
デバイスのセキュリティ機能を有効にするには、ローカルで有効な証明書(LSC)をインストール

し、セキュリティプロファイルをそのデバイスに割り当てる必要があります。LSCは、エンドポイントの公開キーを所有します。この公開キーは、Certificate Authority Proxy Function(CAPF)秘密キーによって署名されています。デフォルトでは、電話機にはインストールされません。

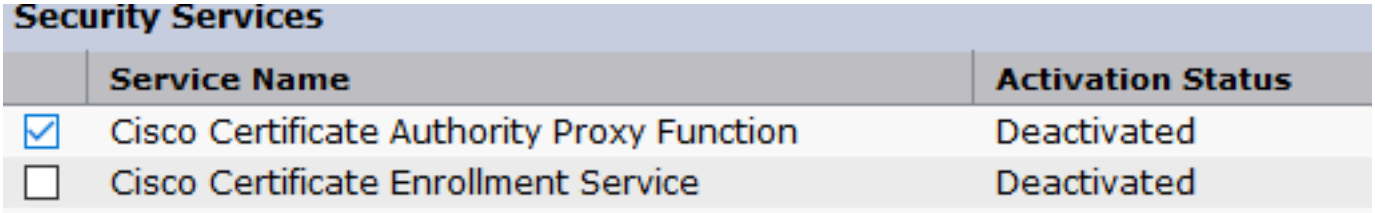
手順：

1. ログイン先 Cisco Unified Serviceability Interface.
2. 移動先 Tools > Service Activation.

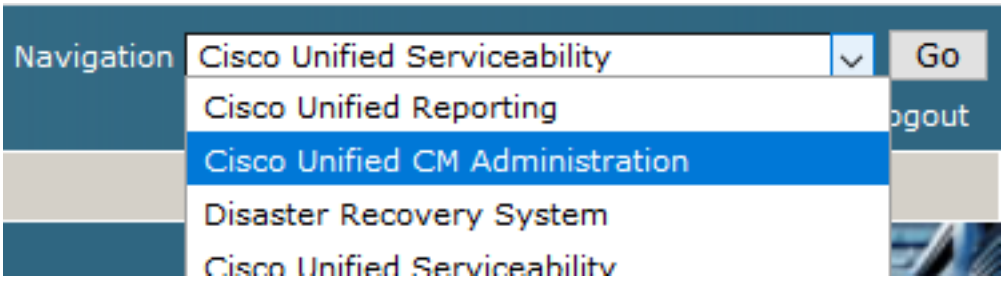
3. CUCMサーバを選択し、 Go .



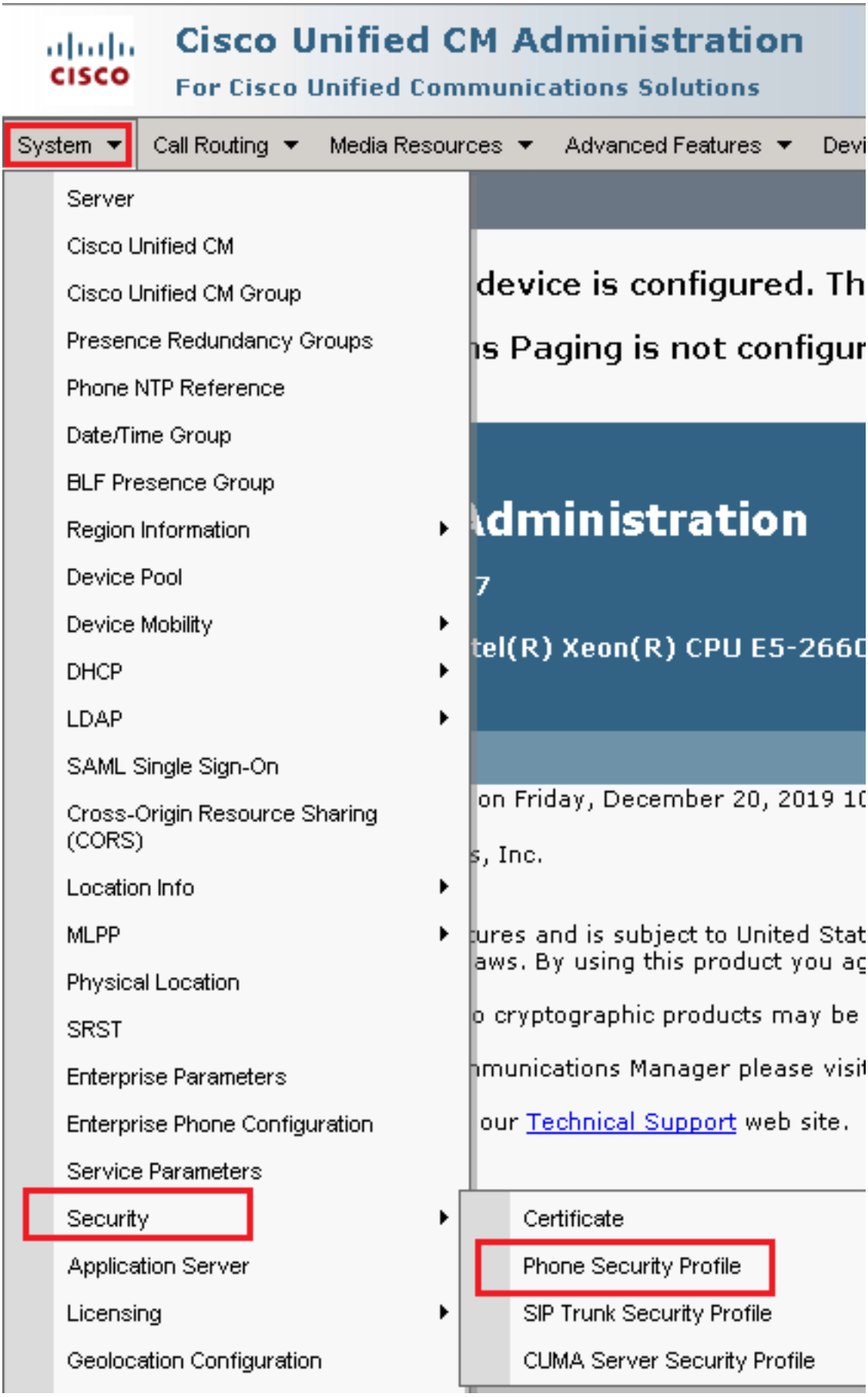
4. オン Cisco Certificate Authority Proxy Function をクリックし、 Save サービスをアクティブ化します。クリック Ok をクリックします。



5. サービスがアクティブになっていることを確認してから、 Cisco Unified CM Administration.

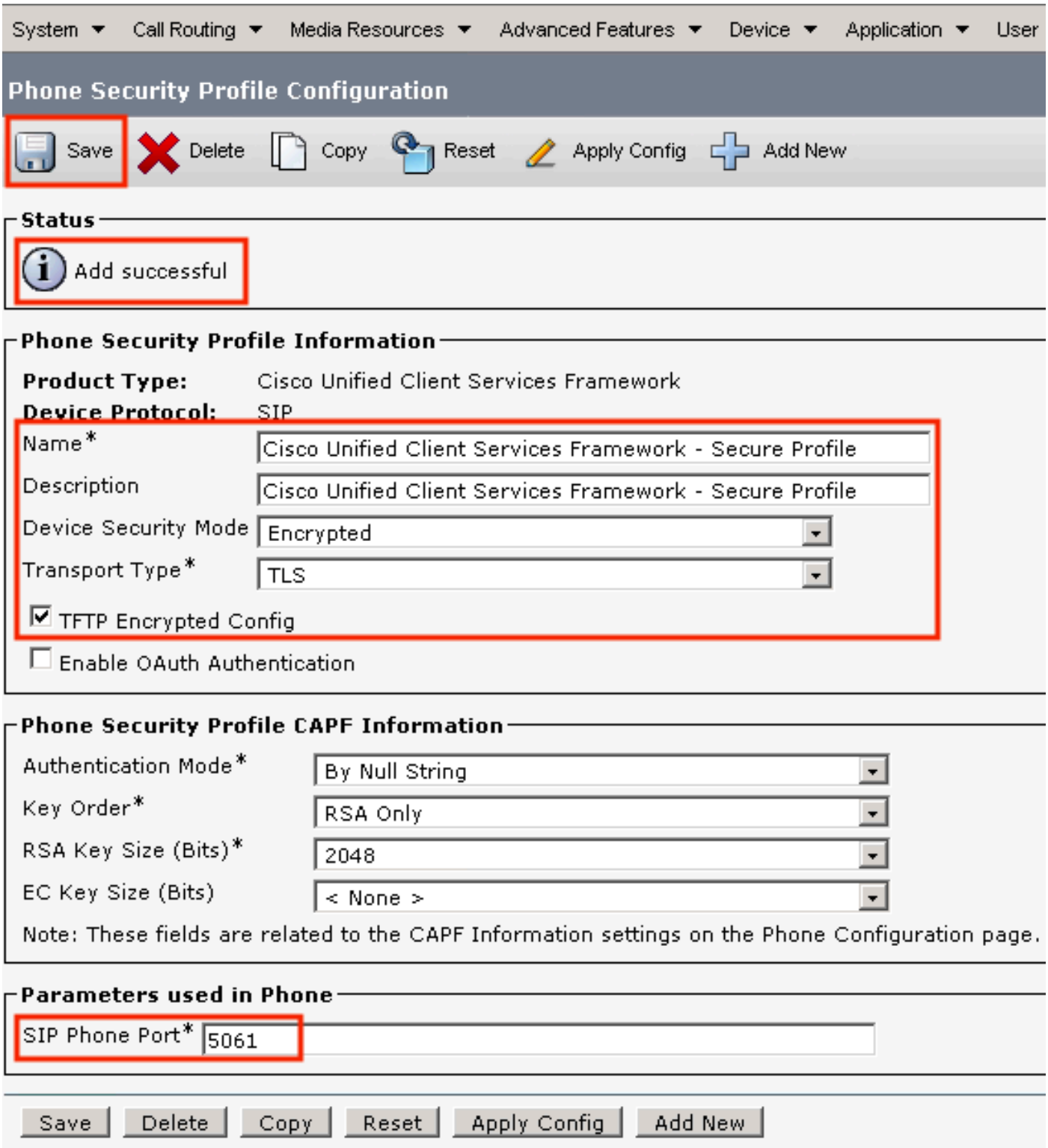


6. CUCM管理に正常にログインしたら、に移動します。 System > Security > Phone Security Profile エージェントデバイスのデバイスセキュリティプロファイルを作成します。

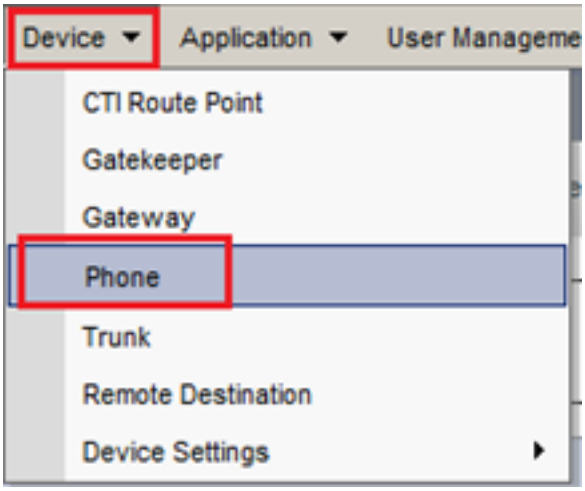


7. 使用しているエージェントデバイスタイプに対応するセキュリティプロファイルを見つけます。この例では、ソフトフォンが使用されているため、 Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile . クリック Copy このプロファイルをコピーします。

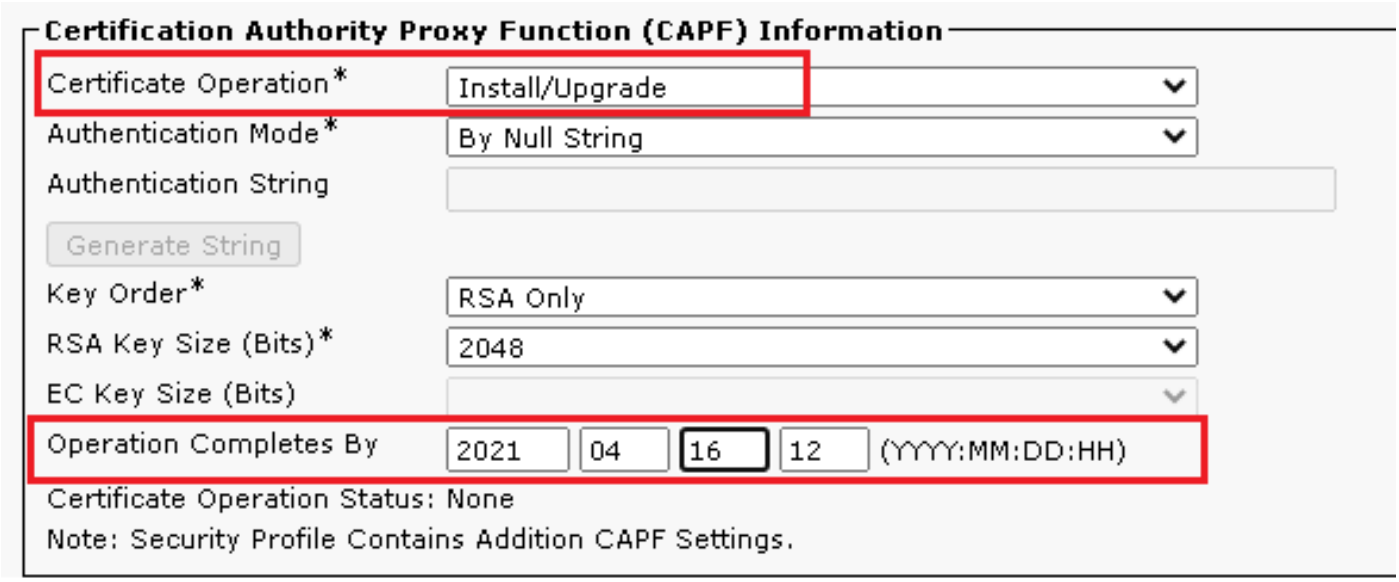
8. プロファイルの名前をに変更 Cisco Unified Client Services Framework - Secure Profileをクリックし、次の図に示すようにパラメータを変更して、 Save ページの左上に表示されます。



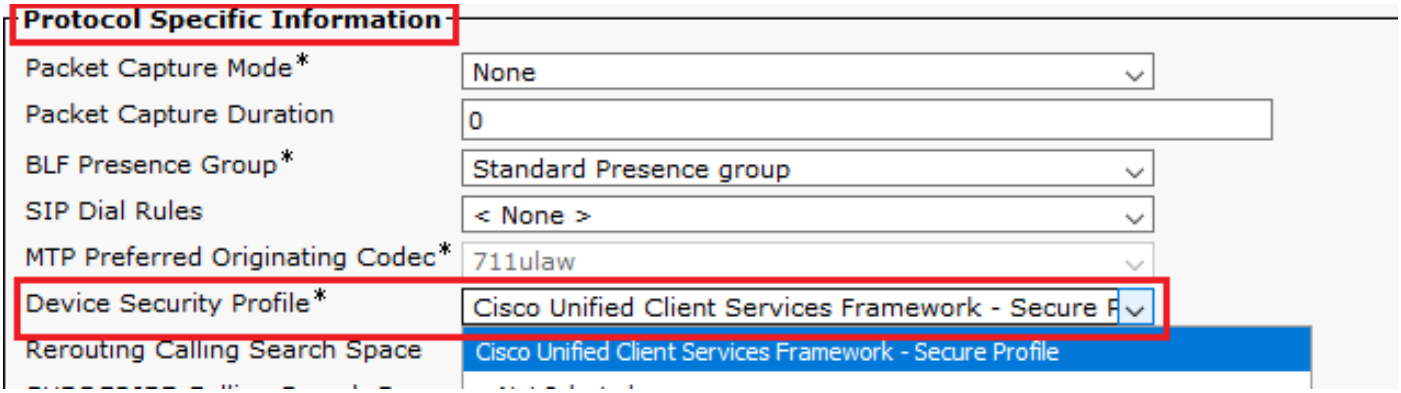
9. 電話デバイスプロファイルの作成が正常に完了したら、に移動します。 Device > Phone.



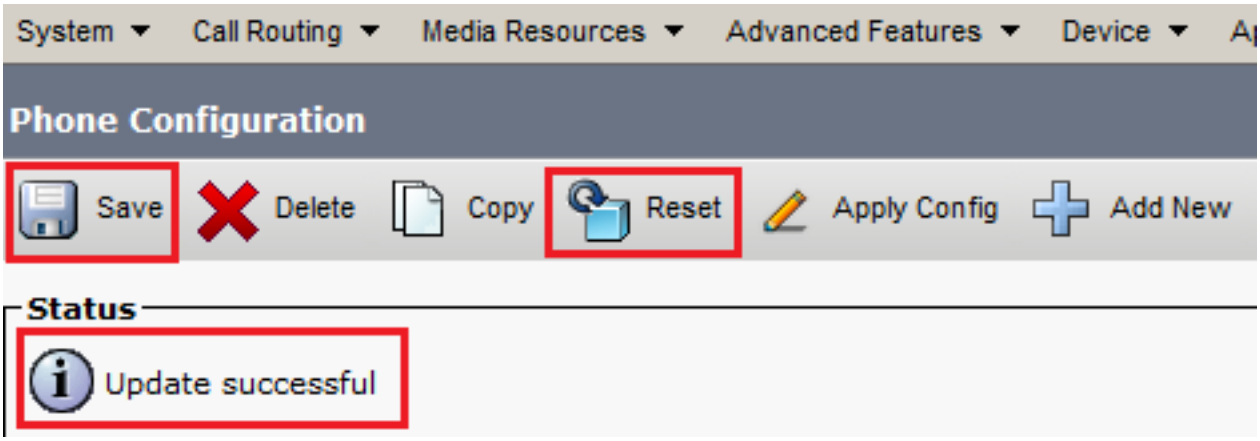
10. クリック Find すべての使用可能な電話機を一覧表示するには、[agent phone]をクリックします。
11. [エージェントの電話機設定(Agent phone configuration)]ページが開きます。検索 Certification Authority Proxy Function (CAPF) Information 。LSCをインストールするには、 Certificate Operation から Install/Upgrade と Operation Completes by 将来の任意の日付に変更します。



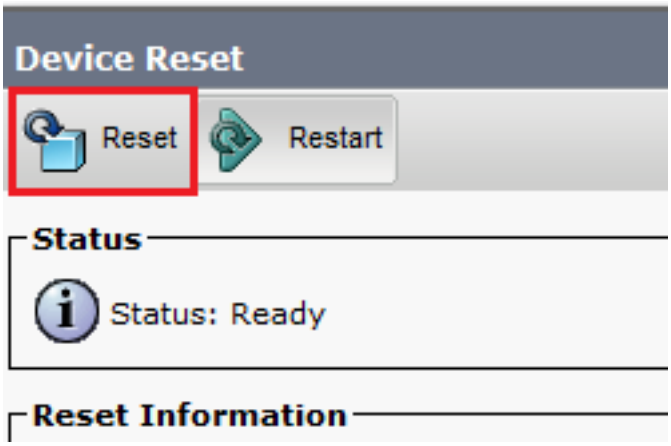
12. 検索 Protocol Specific Information 。Change Device Security Profile から Cisco Unified Client Services Framework – Secure Profile.



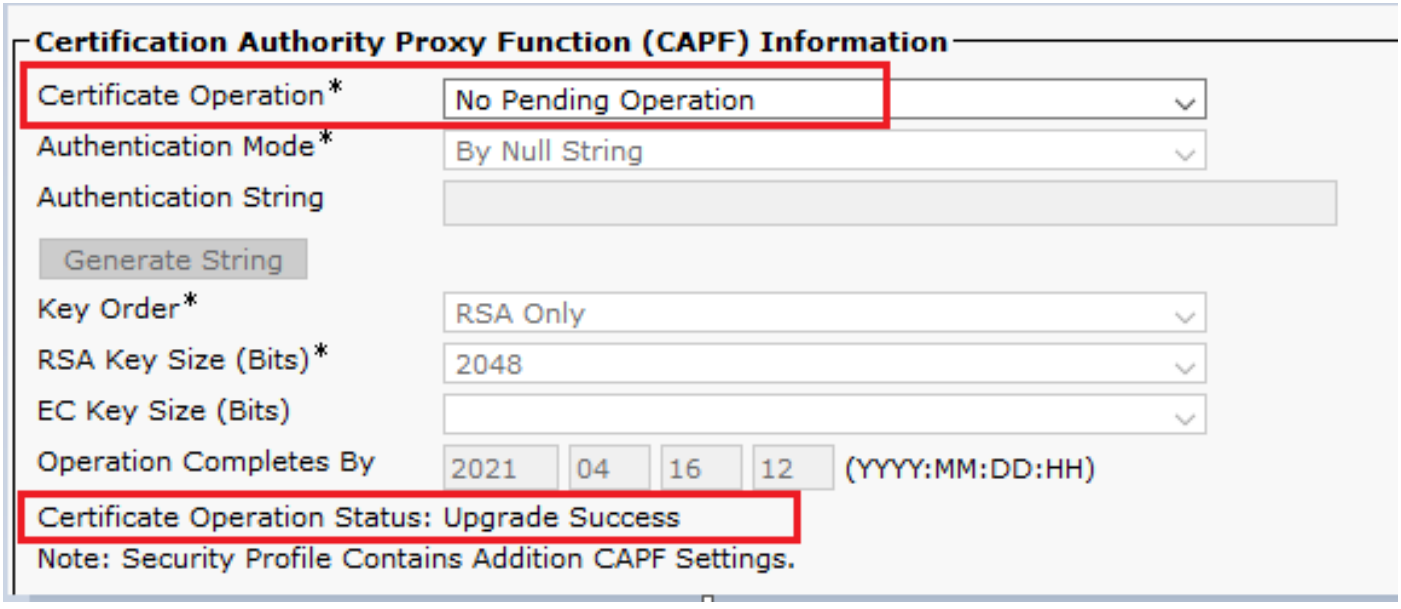
13. クリック Save ページの左上に表示されます。変更が正常に保存されたことを確認し、Reset.



14. ポップアップウィンドウが開き、 Reset をクリックしてアクションを確認します。



15. エージェントデバイスがCUCMに再登録されたら、現在のページを更新し、LSCが正常にインストールされていることを確認します。オン Certification Authority Proxy Function (CAPF) Information section, Certificate Operation に設定する必要があります。 No Pending Operation,と Certificate Operation Status に設定されている Upgrade Success .

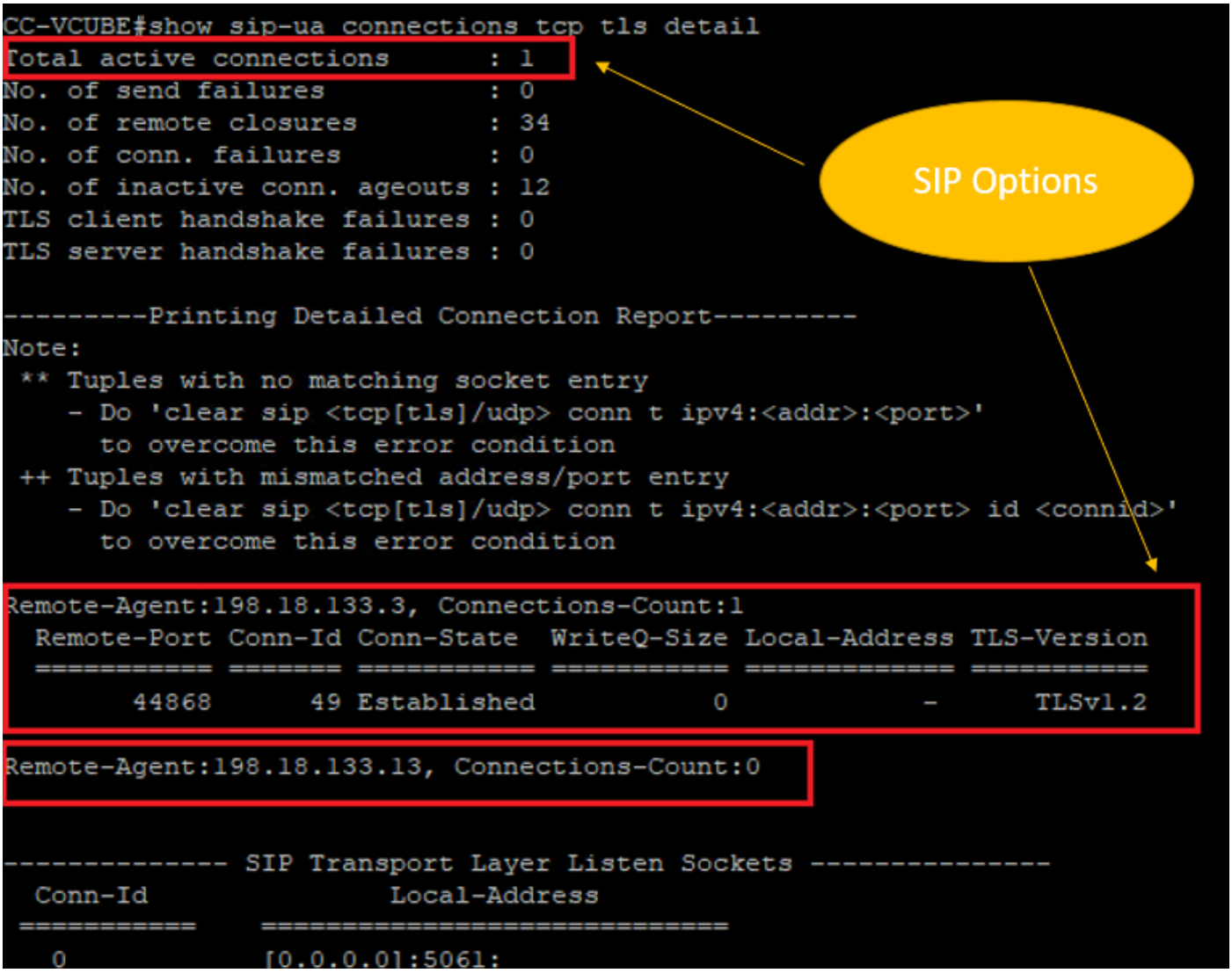


16. 手順を参照してください。7-13:CUCMでSIPを保護するために使用する他のエージェントデバイスを保護するため。

確認

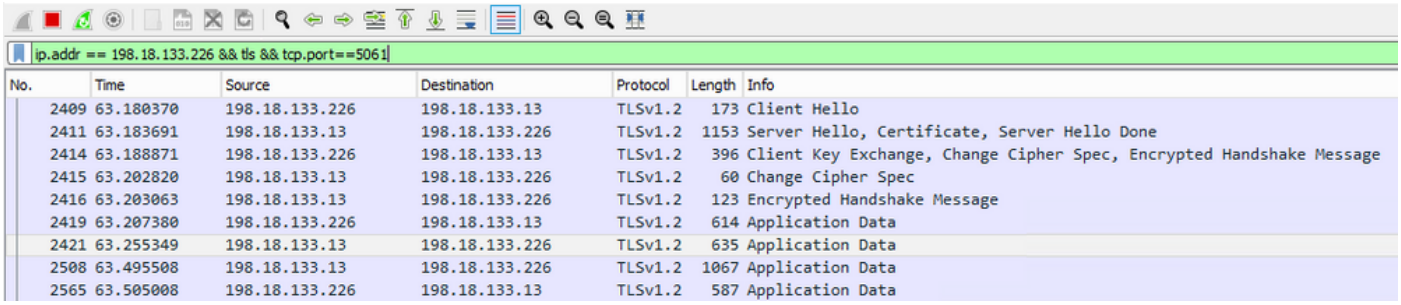
SIPシグナリングが適切に保護されていることを確認するには、次の手順を実行します。

1. vCUBEへのSSHセッションを開き、コマンドを実行します。 show sip-ua connections tcp tls detail 、CVP(198.18.133.13)とのTLS接続が現在確立されていないことを確認します。



注：現時点では、CUCM(198.18.133.3)でSIPオプション用にCUCMとのアクティブなTLSセッションが1つだけ有効になっています。有効なSIPオプションがない場合、SIP TLS接続は存在しません。

2. CVPにログインし、Wiresharkを起動します。
3. コンタクトセンター番号にテストコールを発信します。
4. CVPセッションに移動します。Wiresharkで、CUBEを使用したSIPシグナリングを確認するには、次のフィルタを実行します。
   ip.addr == 198.18.133.226 && tls && tcp.port==5061



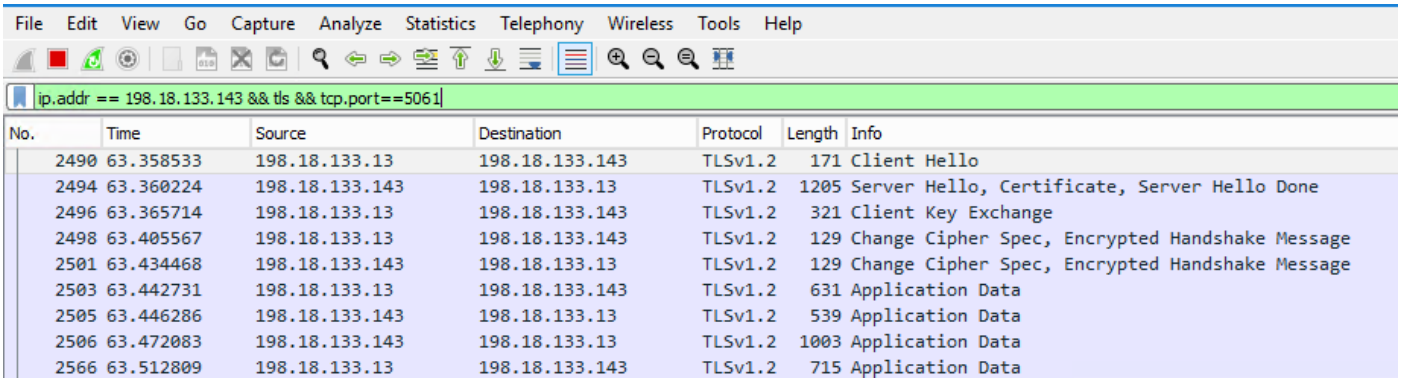
ip.addr == 198.18.133.226 && tls && tcp.port==5061

No.	Time	Source	Destination	Protocol	Length	Info
2409	63.180370	198.18.133.226	198.18.133.13	TLSv1.2	173	Client Hello
2411	63.183691	198.18.133.13	198.18.133.226	TLSv1.2	1153	Server Hello, Certificate, Server Hello Done
2414	63.188871	198.18.133.226	198.18.133.13	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2415	63.202820	198.18.133.13	198.18.133.226	TLSv1.2	60	Change Cipher Spec
2416	63.203063	198.18.133.13	198.18.133.226	TLSv1.2	123	Encrypted Handshake Message
2419	63.207380	198.18.133.226	198.18.133.13	TLSv1.2	614	Application Data
2421	63.255349	198.18.133.13	198.18.133.226	TLSv1.2	635	Application Data
2508	63.495508	198.18.133.13	198.18.133.226	TLSv1.2	1067	Application Data
2565	63.505008	198.18.133.226	198.18.133.13	TLSv1.2	587	Application Data

チェック:SIP over TLS接続は確立されていますか。この場合、出力はCVPとCUBE間のSIP信号がセキュアであることを確認します。

5. CVPとCVVBの間のSIP TLS接続を確認します。同じWiresharkセッションで、次のフィルタを実行します。

ip.addr == 198.18.133.143 && tls && tcp.port==5061



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 198.18.133.143 && tls && tcp.port==5061

No.	Time	Source	Destination	Protocol	Length	Info
2490	63.358533	198.18.133.13	198.18.133.143	TLSv1.2	171	Client Hello
2494	63.360224	198.18.133.143	198.18.133.13	TLSv1.2	1205	Server Hello, Certificate, Server Hello Done
2496	63.365714	198.18.133.13	198.18.133.143	TLSv1.2	321	Client Key Exchange
2498	63.405567	198.18.133.13	198.18.133.143	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2501	63.434468	198.18.133.143	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2503	63.442731	198.18.133.13	198.18.133.143	TLSv1.2	631	Application Data
2505	63.446286	198.18.133.143	198.18.133.13	TLSv1.2	539	Application Data
2506	63.472083	198.18.133.143	198.18.133.13	TLSv1.2	1003	Application Data
2566	63.512809	198.18.133.13	198.18.133.143	TLSv1.2	715	Application Data

チェック:SIP over TLS接続は確立されていますか。この場合、出力はCVPとCVVBの間のSIP信号が保護されていることを確認します。

6. CUBEからCVPとのSIP TLS接続を確認することもできます。vCUBE SSHセッションに移動し、次のコマンドを実行してセキュアなsip信号を確認します。

show sip-ua connections tcp tls detail

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= =========== =========== ============= ===========
        38896       2 Established           0             -      TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= =========== =========== ============= ===========
         5061       3 Established           0             -      TLSv1.2


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id                Local-Address
 ===========    ==============================
   0             [0.0.0.0]:5061:
```

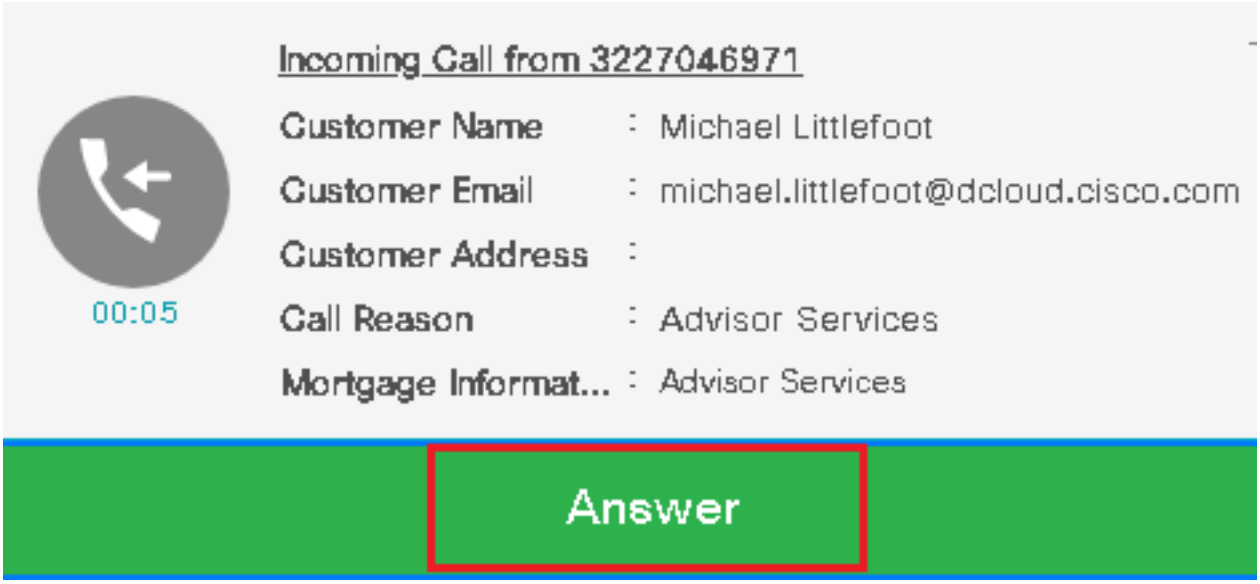
チェック:SIP over TLS接続はCVPと確立されていますか。この場合、出力はCVPとCUBE間のSIP信号がセキュアであることを確認します。

7.この時点では、コールはアクティブで、コールに応答できるエージェントがないため、保留音(MOH)が聞こえます。

8.エージェントがコールに応答できるようにします。

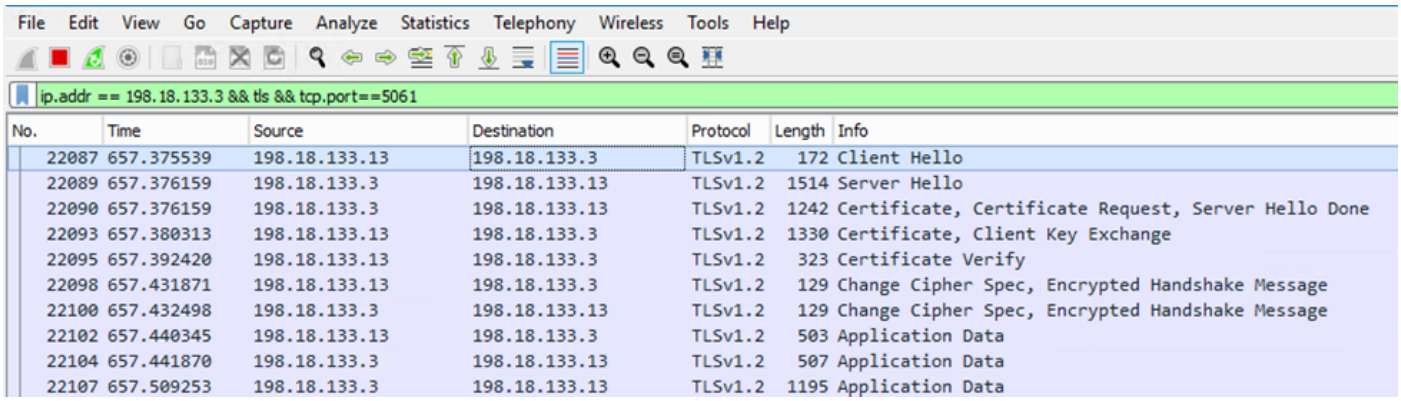
.

9.エージェントが予約され、コールがエージェントにルーティングされます。クリック Answer コールに応答します。



10.コールがエージェントに接続します。

11. CVPとCUCMの間のSIP信号を確認するには、CVPセッションに移動し、Wiresharkで次のフィルタを実行します。
ip.addr == 198.18.133.3 && tls && tcp.port==5061



チェック：CUCM(198.18.133.3)とのSIP通信はすべてTLSを介して行われますか。この場合、出力はCVPとCUCM間のSIP信号がセキュアであることを確認します。

トラブルシュート

TLSが確立されていない場合は、CUBEで次のコマンドを実行し、debug TLSを有効にしてトラブルシューティングを行います。

- Debug ssl openssl errors
- Debug ssl openssl msg
- Debug ssl openssl states

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。