Konfigurieren der sicheren SIP-Signalisierung in Contact Center Enterprise

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die SIP-Signalisierung (Session Initiation Protocol) in Contact Center Enterprise (CCE) für einen umfassenden Anruffluss gesichert wird.

Voraussetzungen

Die Erstellung und der Import von Zertifikaten werden in diesem Dokument nicht behandelt. Daher müssen Zertifikate für Cisco Unified Communication Manager (CUCM), Customer Voice Portal (CVP)-Anrufserver, Cisco Virtual Voice Browser (CVB) und Cisco Unified Border Element (CUBE) erstellt und in die entsprechenden Komponenten importiert werden. Wenn Sie selbstsignierte Zertifikate verwenden, muss der Zertifikataustausch zwischen verschiedenen Komponenten erfolgen.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CCE
- CVP
- WÜRFEL
- CUCM
- CVB

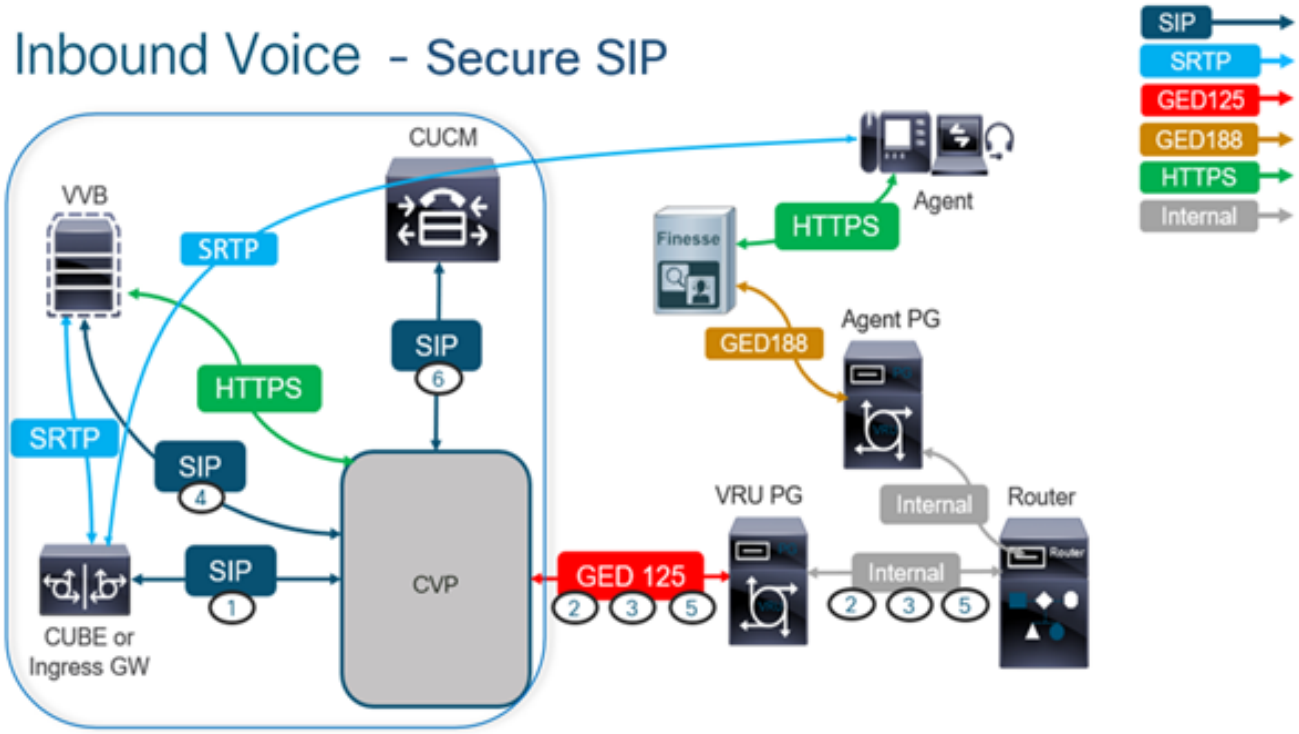
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Package Contact Center Enterprise (PCCE), CVP, CVVB und CUCM Version 12.6. Sie gelten jedoch auch für frühere Versionen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

Das nächste Diagramm zeigt die Komponenten, die an der SIP-Signalisierung im Contact Center beteiligt sind, und einen umfassenden Anrufablauf. Wenn ein Sprachanruf beim System eingeht, erfolgt er zuerst über das Eingangs-Gateway oder CUBE. Starten Sie also sichere SIP-Konfigurationen für CUBE. Konfigurieren Sie anschließend CVP, CVVB und CUCM.



Aufgabe 1: Sichere CUBE-Konfiguration

Konfigurieren Sie in dieser Aufgabe CUBE, um die SIP-Protokollnachrichten zu sichern.

Erforderliche Konfigurationen:

- Konfigurieren eines Standard-Vertrauenspunkts für den SIP-Benutzer-Agenten (UA)
- Ändern der DFÜ-Peers zur Verwendung von TLS (Transport Layer Security)

Schritte:

1. Öffnen Sie eine Secure Shell (SSH)-Sitzung mit CUBE.
2. Führen Sie diese Befehle aus, damit der SIP-Stack das CA-Zertifikat (Certificate Authority)

des CUBE verwendet. CUBE stellt eine SIP-TLS-Verbindung vom/zum CUCM (198.18.133.3) und CVP (198.18.133.13) her.

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. Führen Sie diese Befehle aus, um TLS auf dem ausgehenden DFÜ-Peer für das CVP zu aktivieren. In diesem Beispiel wird das Dial-Peer-Tag 6000 verwendet, um Anrufe an das CVP weiterzuleiten.

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

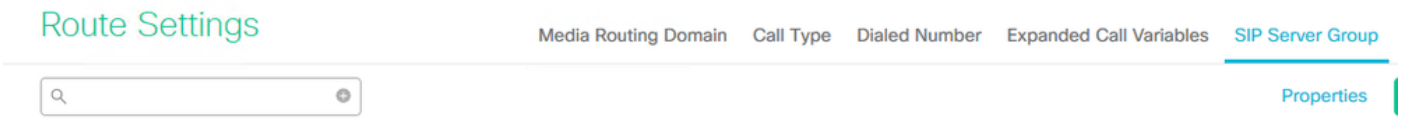
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#
CC-VCUBE(config-dial-peer)#exit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

Aufgabe 2: Sichere CVP-Konfiguration

Konfigurieren Sie bei dieser Aufgabe den CVP-Anrufserver zum Sichern der SIP-Protokollnachrichten (SIP TLS).

Schritte:

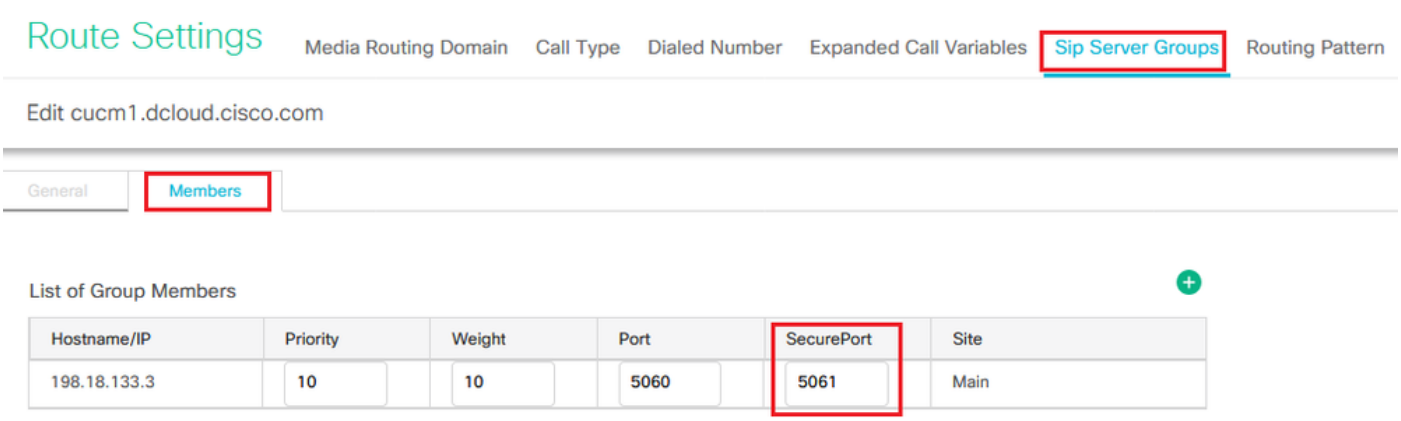
1. Melden Sie sich anUCCE Web Administration.
2. Navigieren Sie zu Call Settings > Route Settings > SIP Server Group.



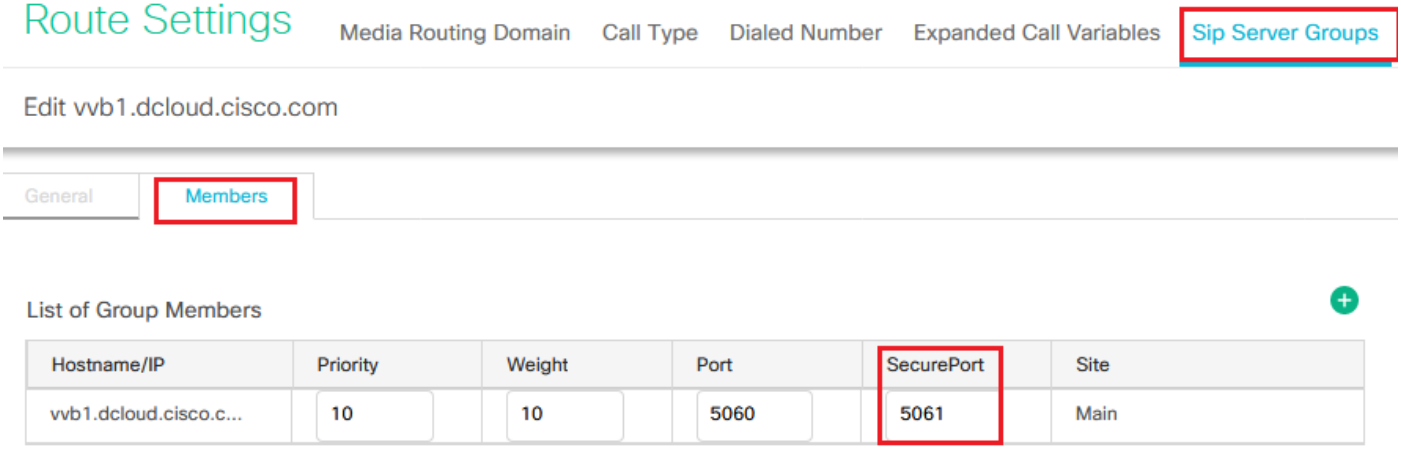
Basierend auf Ihren Konfigurationen sind für CUCM, CVB und CUBE SIP-Servergruppen konfiguriert. Sie müssen für alle SIP-Ports 5061 als sichere Ports festlegen. In diesem Beispiel werden die folgenden SIP-Servergruppen verwendet:

- cucm1.dcloud.cisco.com für CUCM
- vvb1.dcloud.cisco.com für CVVB
- cube1.dcloud.cisco.com für CUBE

3. Klicken Sie auf cucm1.dcloud.cisco.com und dann im **Members** Registerkarte, die die Details der Konfiguration der SIP-Servergruppe anzeigt. Festlegen SecurePort zu 5061 und klicke auf Save .



4. Klicken Sie auf vvb1.dcloud.cisco.com und dann im **Members** aus. Festlegen von SecurePort auf 5061 und klicke auf Save.

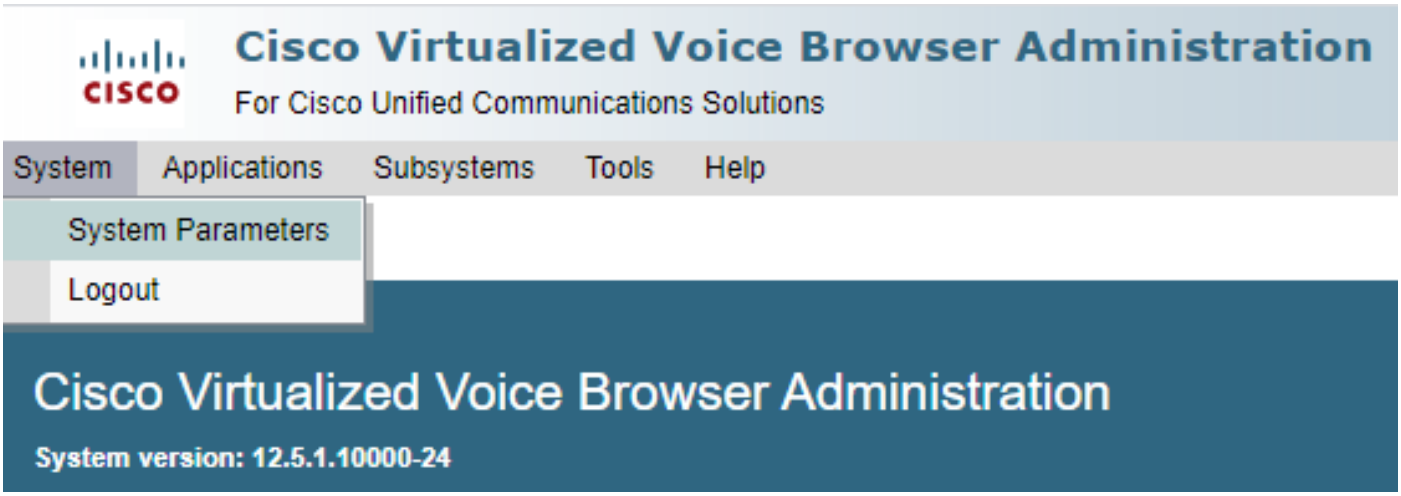


Aufgabe 3: Sichere CVVB-Konfiguration

Konfigurieren Sie bei dieser Aufgabe CVB zum Sichern der SIP-Protokollnachrichten (SIP TLS).

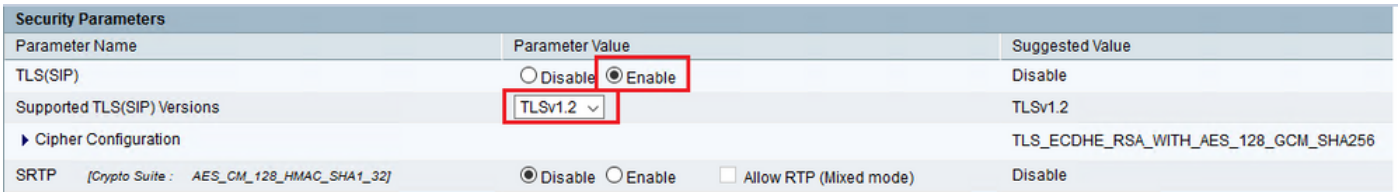
Schritte:

1. Melden Sie sich an **Cisco VVB Administration** Seite.
2. Navigieren Sie zu System > System Parameters.

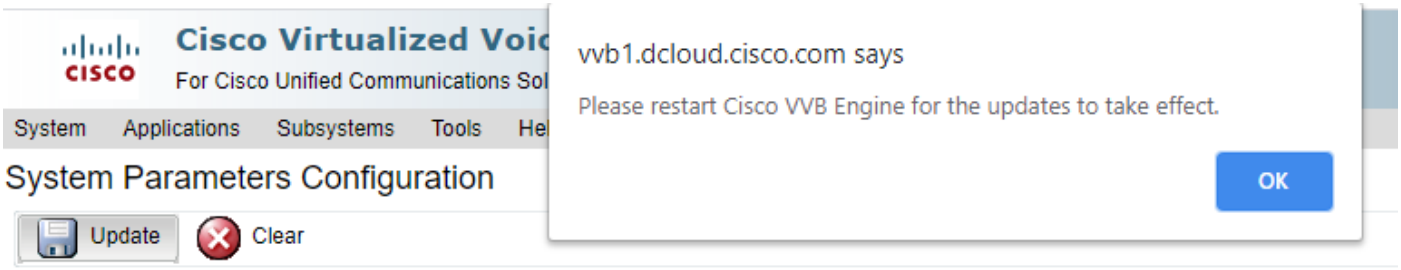


3. Im Security Parameters Abschnitt auswählen Enable für TLS(SIP) . Beibehalten Supported TLS(SIP)

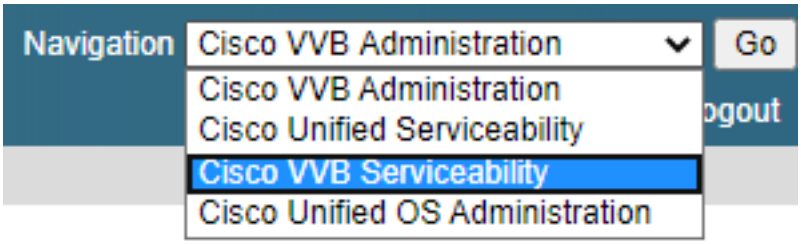
version als TLSv1.2.



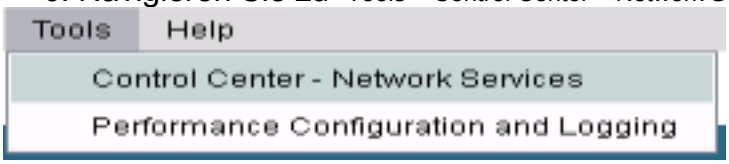
4. Klicken Sie auf **Aktualisieren**. Klicken Sie auf Ok wenn Sie dazu aufgefordert werden, das CVVB-Modul neu zu starten.



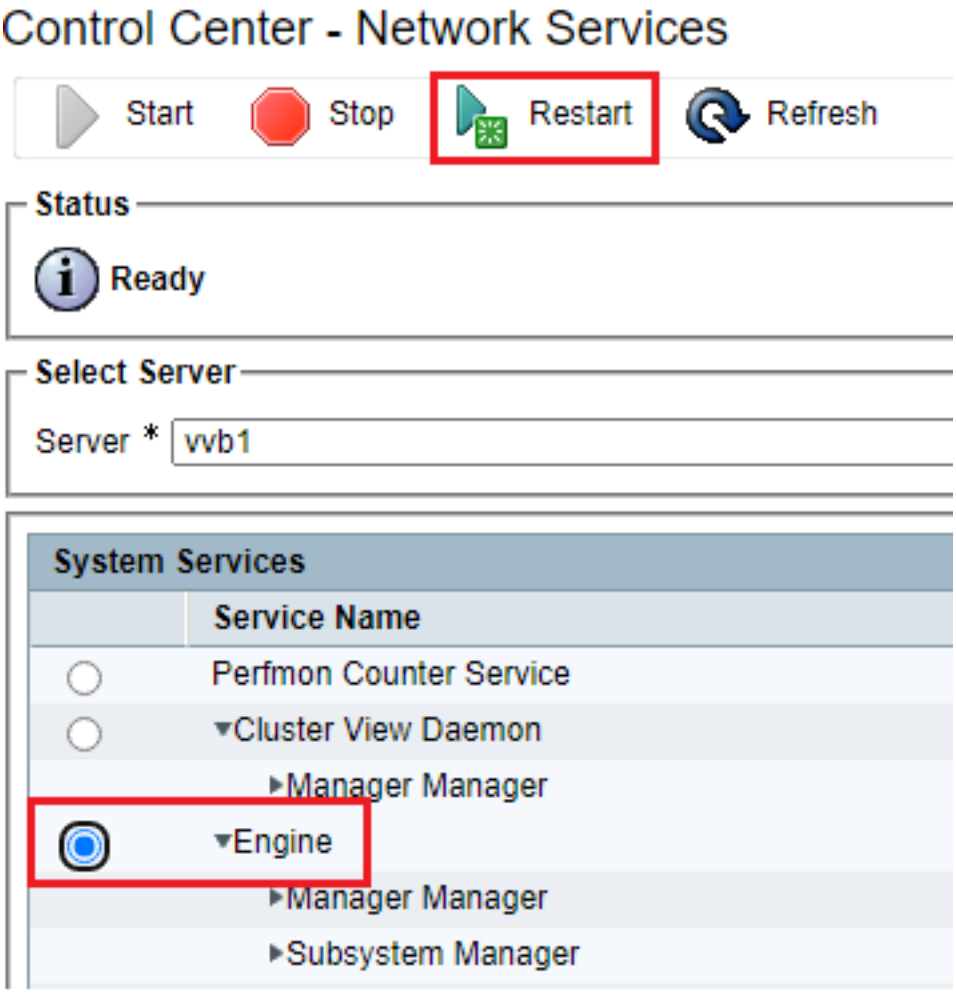
5. Diese Änderungen erfordern einen Neustart der Cisco VB-Engine. Um das VVB-Modul neu zu starten, navigieren Sie zu Cisco VVB Serviceability dann klicken **Go**.



6. Navigieren Sie zu Tools > Control Center – Network Services.



7. Auswählen Engine und klicke auf Restart.



Aufgabe 4: Sichere CUCM-Konfiguration

Führen Sie die folgenden Konfigurationen durch, um SIP-Nachrichten auf dem CUCM zu sichern:

- CUCM-Sicherheitsmodus auf "Gemischt" setzen
- Konfigurieren von SIP-Trunk-Sicherheitsprofilen für CUBE und CVP
- Zuordnen von SIP-Trunk-Sicherheitsprofilen zu entsprechenden SIP-Trunks
- Sichere Gerätekommunikation der Agenten mit CUCM

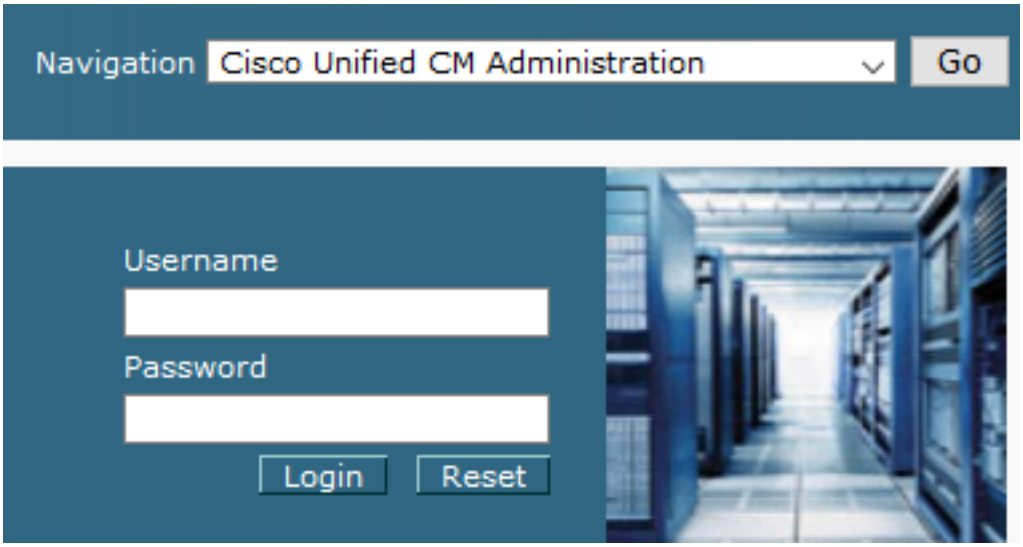
CUCM-Sicherheitsmodus auf "Gemischt" setzen

CUCM unterstützt zwei Sicherheitsmodi:

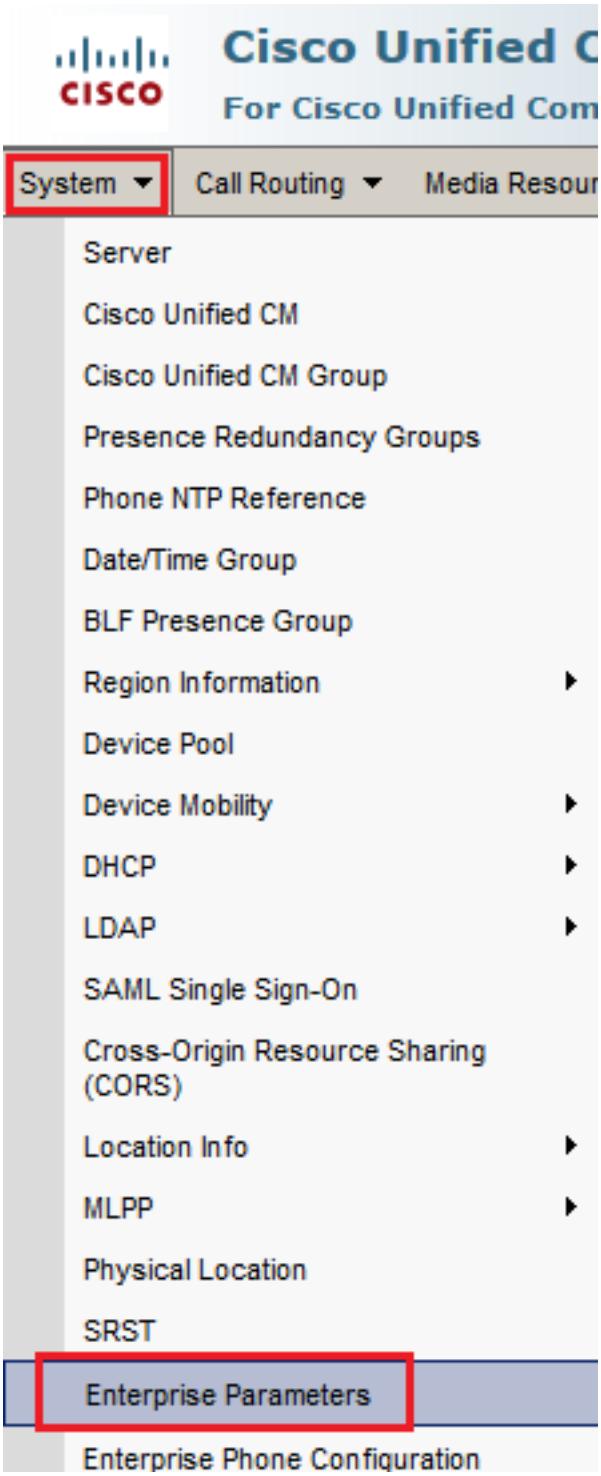
- Nicht sicherer Modus (Standardmodus)
- Gemischter Modus (sicherer Modus)

Schritte:

1. Um den Sicherheitsmodus auf "Gemischter Modus" zu setzen, melden Sie sich an bei Cisco Unified CM Administration Schnittstelle.



2. Nachdem Sie sich erfolgreich beim CUCM angemeldet haben, navigieren Sie zu System > Enterprise Parameters.

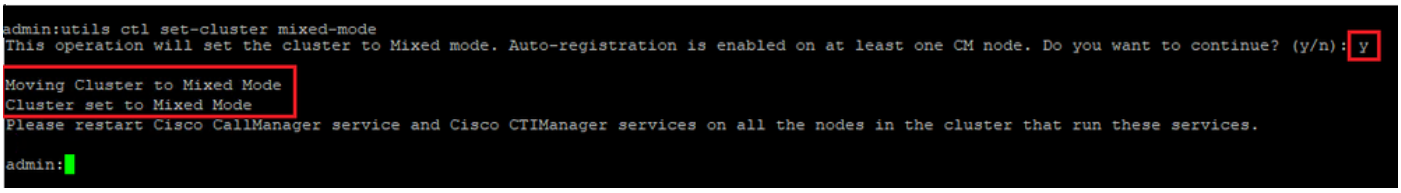


3. Unterhalb des Security Parameters Abschnitt, prüfen, ob Cluster Security Mode ist auf 0.

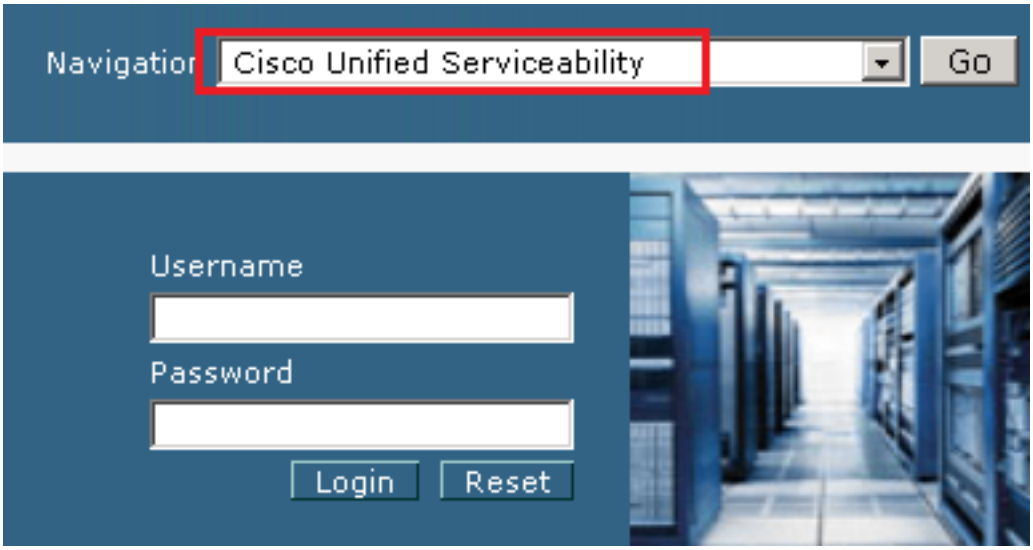
4. Wenn der Clustersicherheitsmodus auf 0 festgelegt ist, bedeutet dies, dass der Clustersicherheitsmodus auf "nicht sicher" festgelegt ist. Sie müssen den gemischten Modus über die CLI aktivieren.
5. Öffnen Sie eine SSH-Sitzung mit dem CUCM.
6. Nachdem Sie sich über SSH erfolgreich beim CUCM angemeldet haben, führen Sie den

folgenden Befehl aus: utils ctl set-cluster mixed-mode

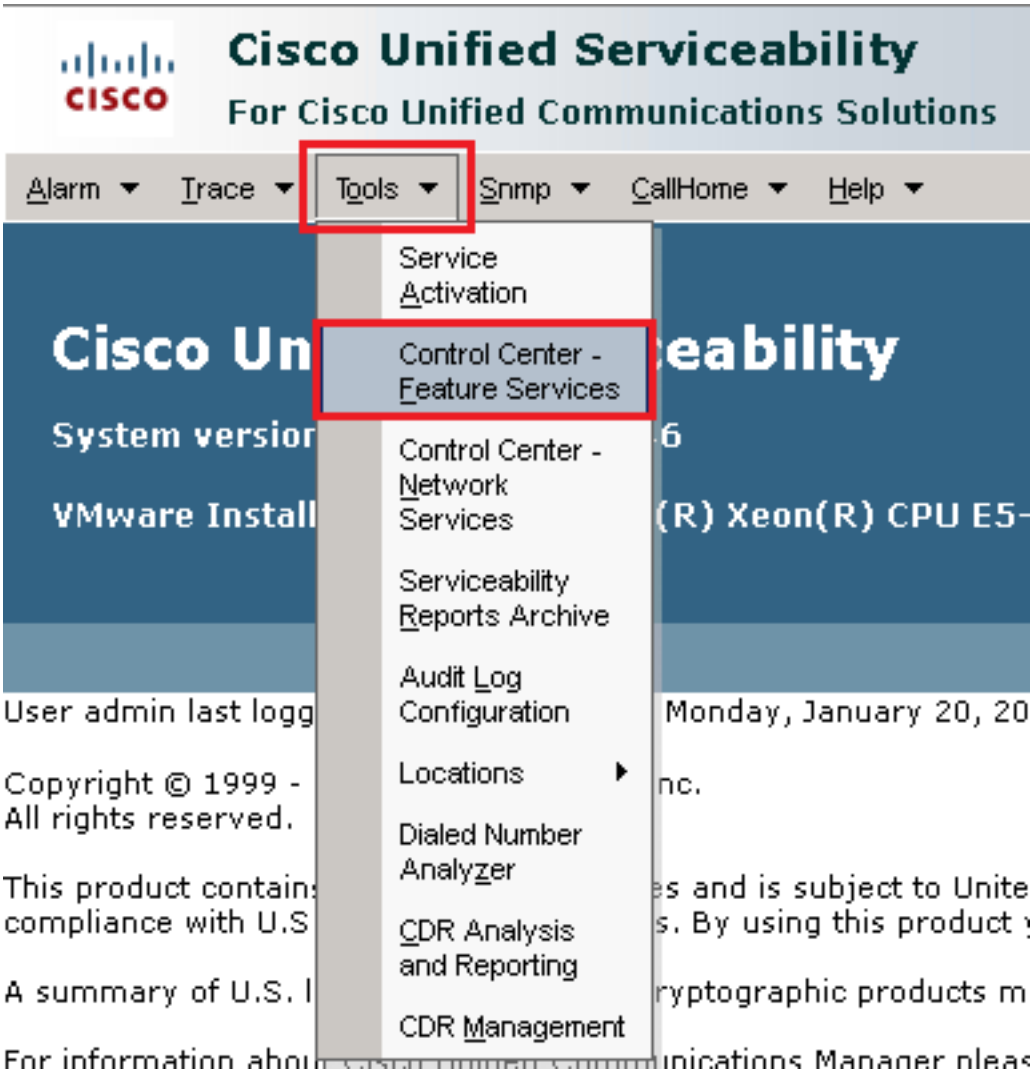
7. Typ y und klicke auf **Eingabe**, wenn du dazu aufgefordert wirst. Mit diesem Befehl wird der Cluster-Sicherheitsmodus auf den gemischten Modus festgelegt.



8. Starten Sie neu, damit die Änderungen wirksam werden. Cisco CallManager und Cisco CTIManager services.
9. Um die Dienste neu zu starten, navigieren Sie zu , und melden Sie sich an unter Cisco Unified Serviceability.

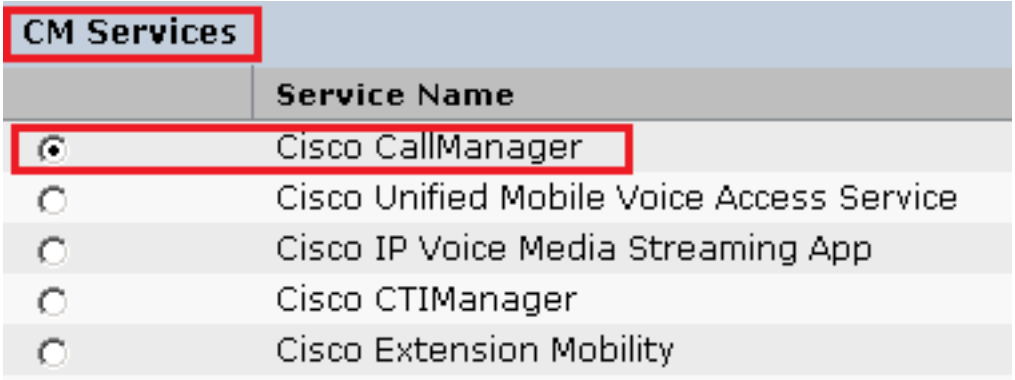


10. Navigieren Sie nach der erfolgreichen Anmeldung zu Tools > Control Center – Feature Services.

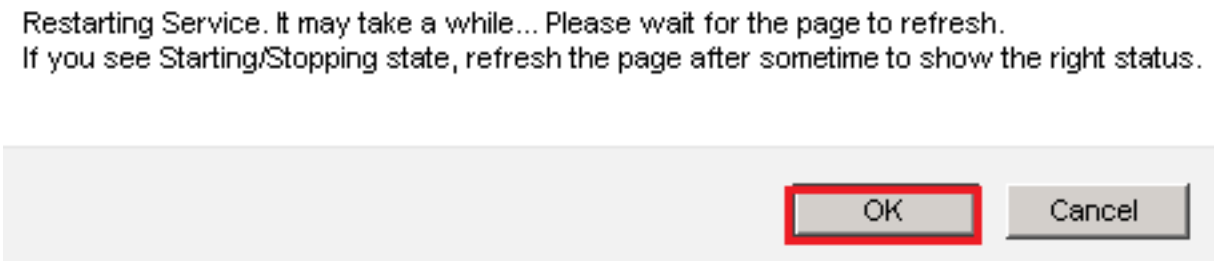


11. Wählen Sie den Server aus, und klicken Sie auf **Go**.

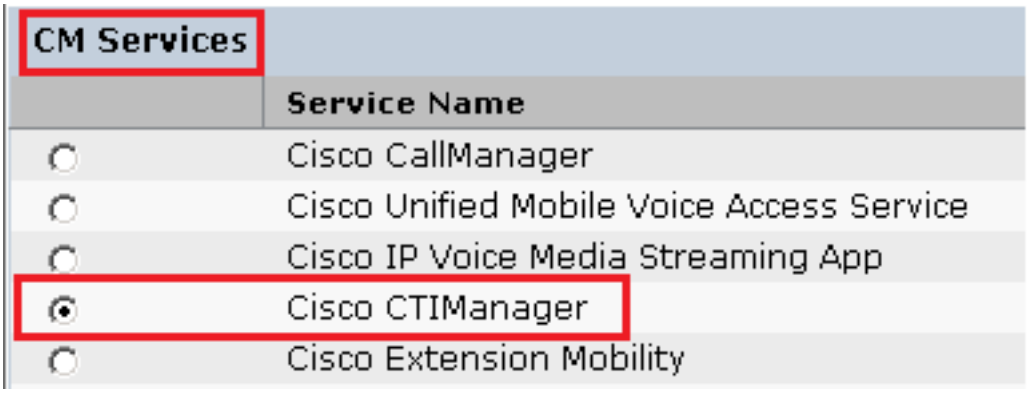
12. Wählen Sie unter den CM-Services Cisco CallManager dann klicken Restart -Taste oben auf der Seite.



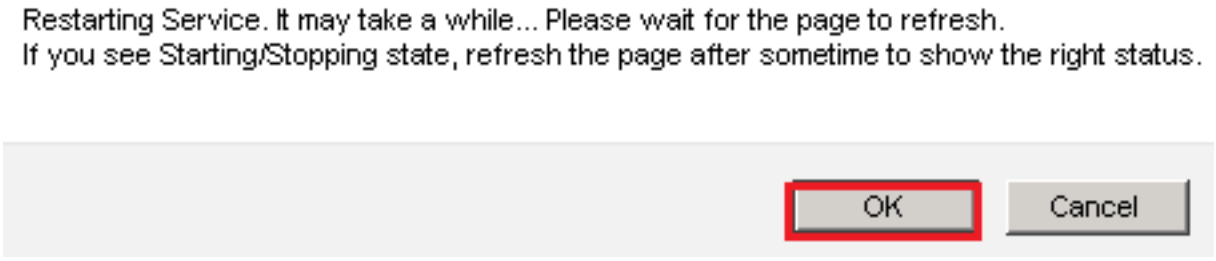
13. Bestätigen Sie die Popup-Meldung, und klicken Sie auf **OK**. Warten Sie, bis der Dienst erfolgreich neu gestartet wurde.



14. Nach einem erfolgreichen Neustart von Cisco CallManager, wählen Sie Cisco **CTIManager** dann klicken Restart Taste zum Neustarten Cisco CTIManager Services.



15. Bestätigen Sie die Popup-Meldung, und klicken Sie auf **OK**. Warten Sie, bis der Dienst erfolgreich neu gestartet wurde.

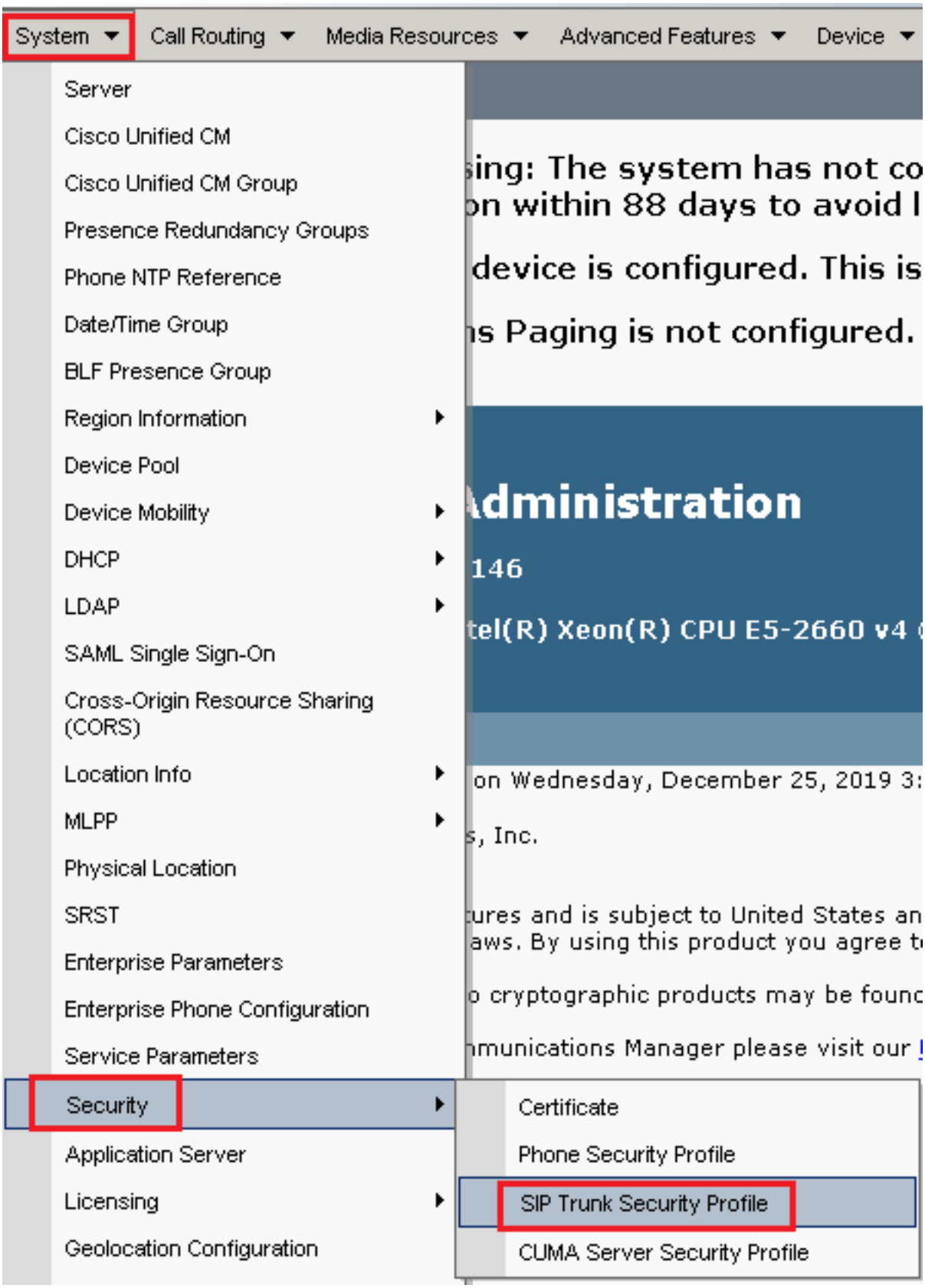


16. Nachdem die Dienste erfolgreich neu gestartet wurden, überprüfen Sie, ob der Cluster-Sicherheitsmodus auf den gemischten Modus gesetzt ist, und navigieren Sie zur CUCM-Verwaltung, wie in Schritt 5 beschrieben. Überprüfen Sie dann die **Cluster Security Mode**. Jetzt muss sie auf **1**.

Konfigurieren von SIP-Trunk-Sicherheitsprofilen für CUBE und CVP

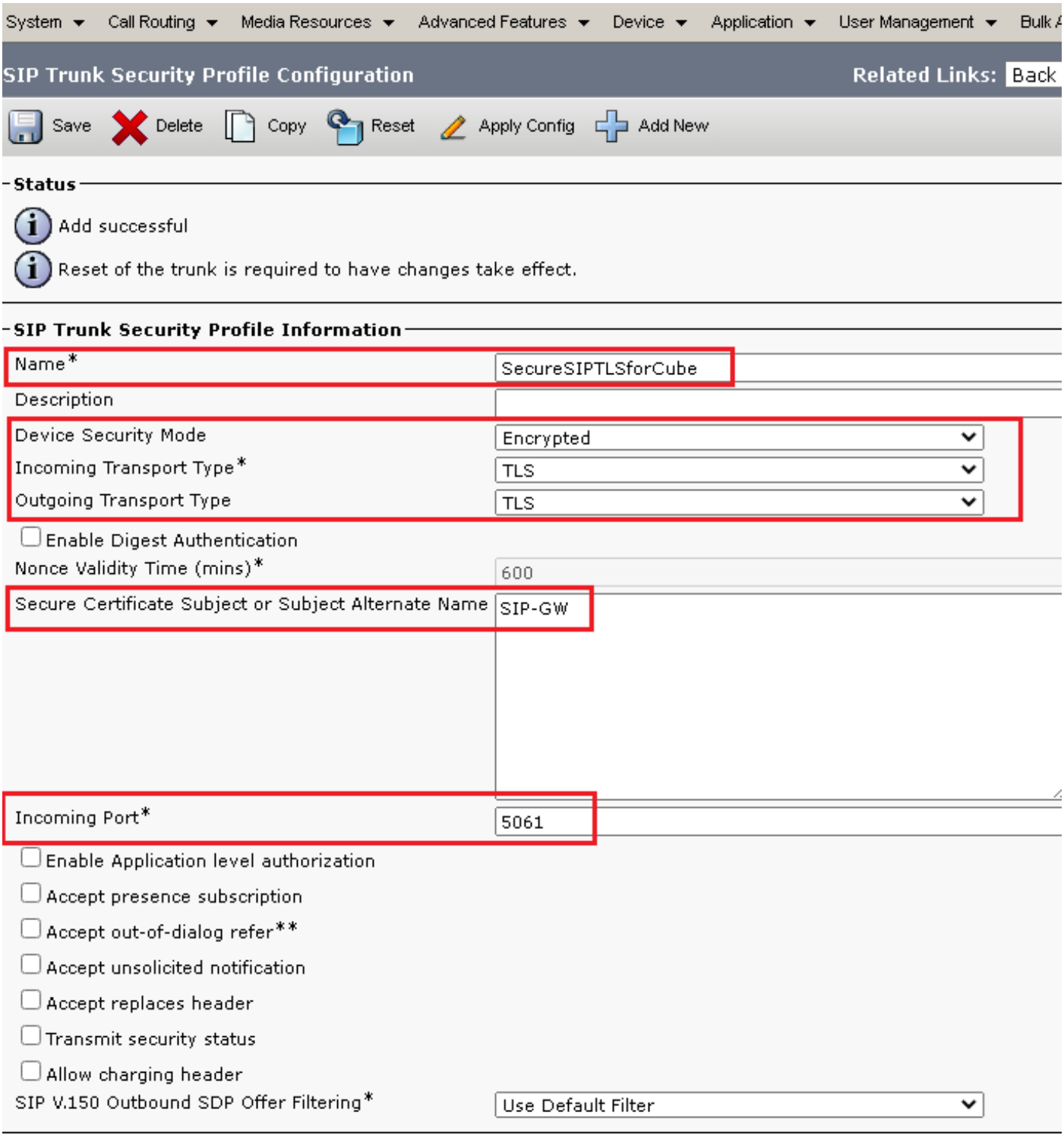
Schritte:

1. Melden Sie sich an CUCM administration Schnittstelle.
2. Navigieren Sie nach der erfolgreichen Anmeldung bei CUCM zu System > Security > SIP Trunk Security Profile um ein Gerätesicherheitsprofil für CUBE zu erstellen.



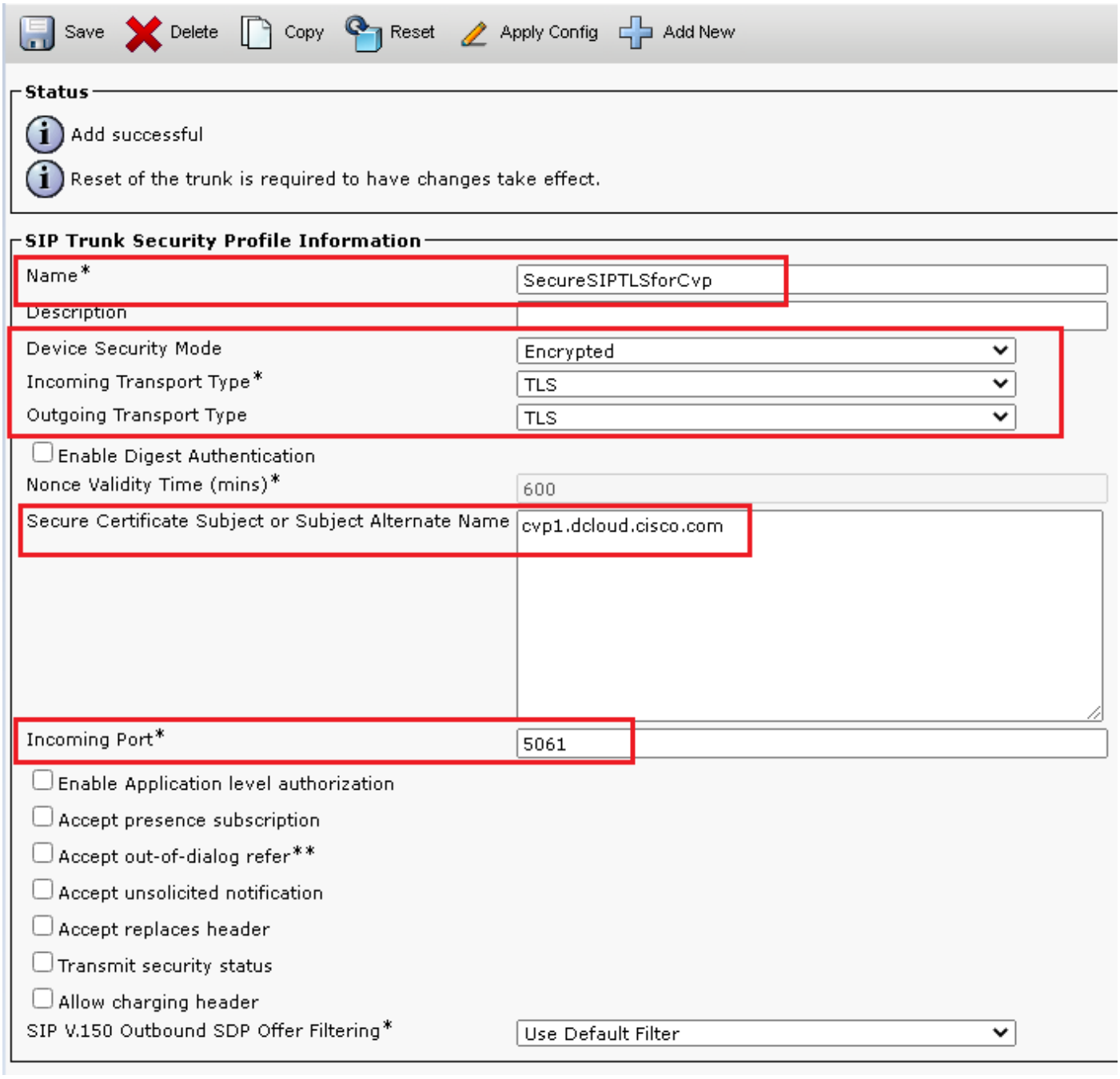
3. Klicken Sie oben links auf Add New um ein neues Profil hinzuzufügen.

4. Konfigurieren SIP Trunk Security Profile wie in diesem Bild dargestellt, und klicken Sie dann auf Save unten links auf der Seite Save IT.



5. Stellen Sie sicher, dass die Secure Certificate Subject or Subject Alternate Name auf den Common Name (CN) des CUBE-Zertifikats, da dieser übereinstimmen muss.

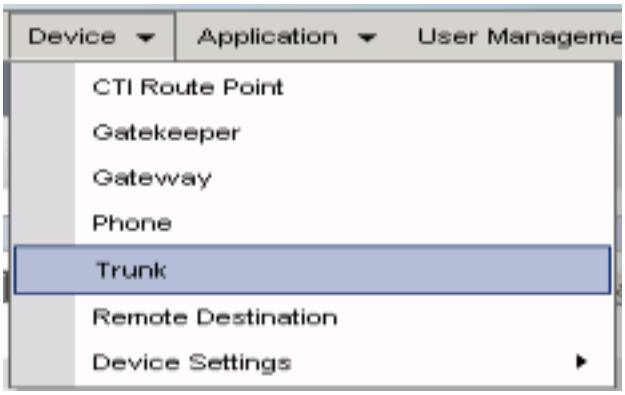
6. Klicken Sie Copy und ändern Sie die Name zu SecureSipTLSforCVP und Secure Certificate Subject auf die CN des CVP-Anrufserverzertifikats, da es übereinstimmen muss. Klicken Sie auf Save -Taste.



Zuordnen von SIP-Trunk-Sicherheitsprofilen zu entsprechenden SIP-Trunks

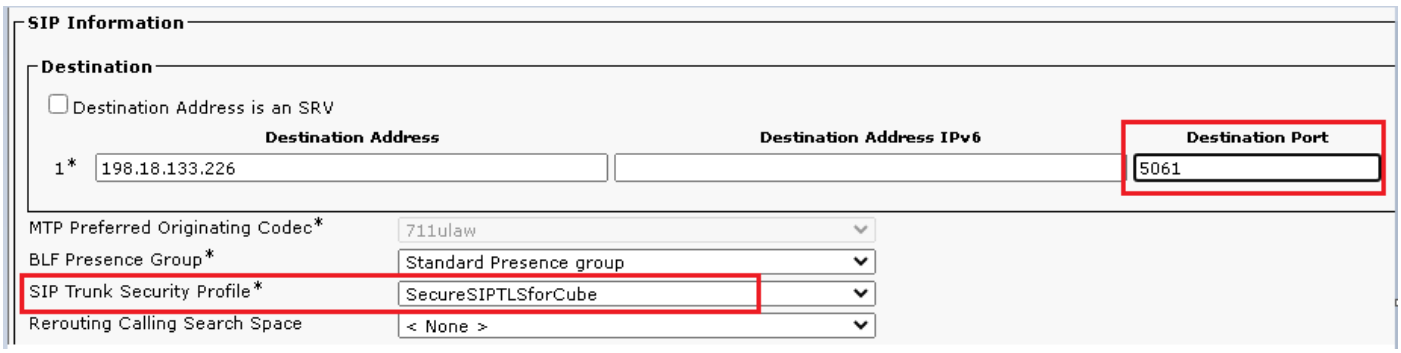
Schritte:

1. Navigieren Sie auf der Seite "CUCM Administration" zu Device > Trunk.

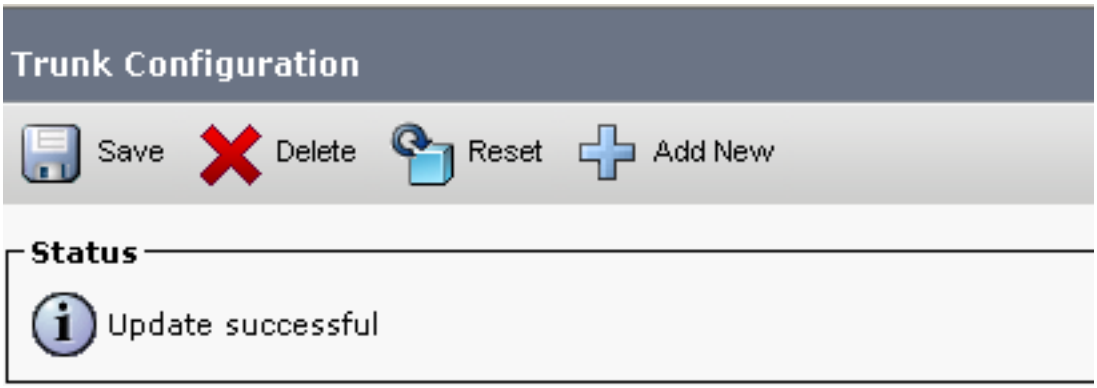


2. Suchen Sie nach CUBE-Trunk. In diesem Beispiel lautet der CUBE-Trunk-Name vCube . Klicken Sie auf **Find**.

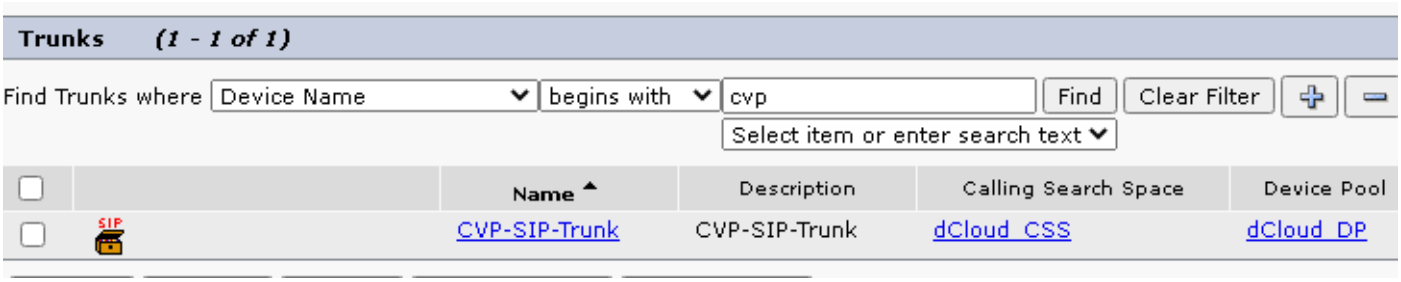
3. Klicken Sie auf vCUBE, um die Konfigurationsseite für vCUBE-Trunks zu öffnen.
4. Blättern Sie nach unten zu SIP Information und ändern Sie den Destination Port zu 5061.
5. Ändern SIP Trunk Security Profile zu SecureSIPTLSForCube.



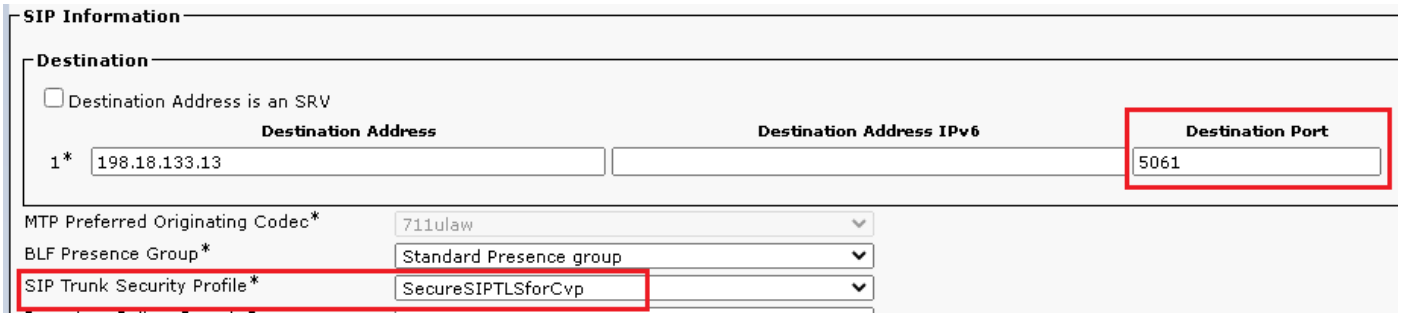
6. Klicken Sie auf Save dann Rest um Save und Änderungen anwenden.



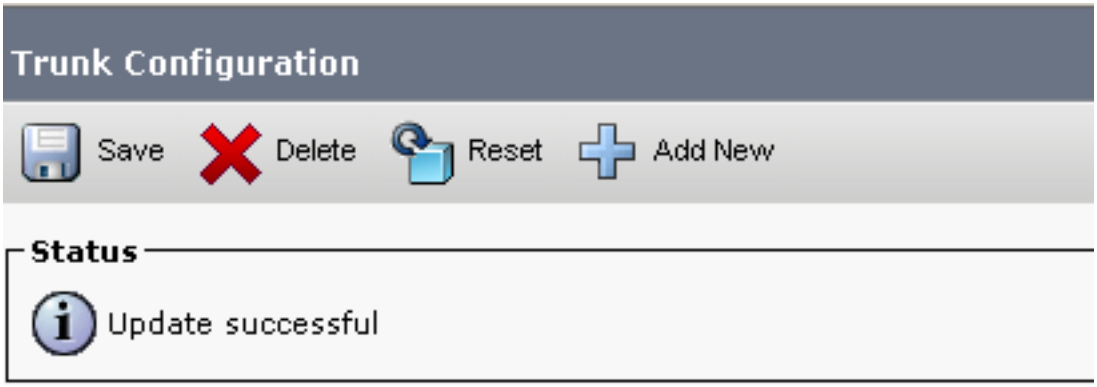
7. Navigieren Sie zu Device > Trunk, und suchen Sie nach CVP-Trunk. In diesem Beispiel lautet der Name des CVP-Trunks cvp-SIP-Trunk . Klicken Sie auf **Find**.



8. Klicken Sie auf CVP-SIP-Trunk , um die Konfigurationsseite für CVP-Trunks zu öffnen.
9. Blättern Sie nach unten zu SIP Information Abschnitt und Änderungen Destination Port zu 5061 .
10. Ändern SIP Trunk Security Profile zu SecureSIPTLSForCvp.



11. Klicken Sie auf Save dann Rest um save und Änderungen anwenden.



Sichere Gerätekommunikation der Agenten mit CUCM

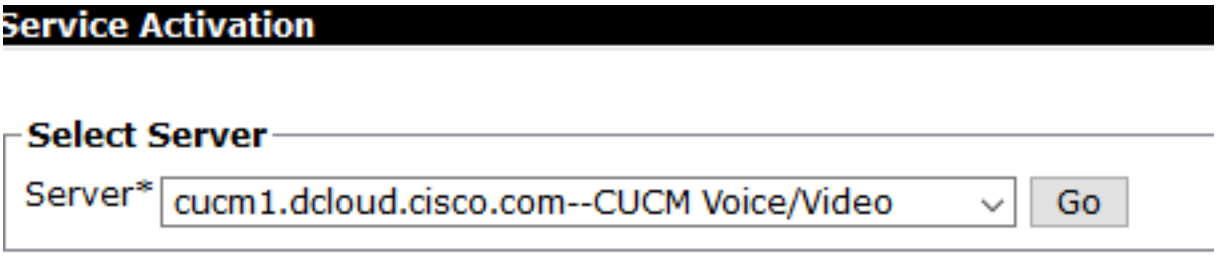
Um Sicherheitsfunktionen für ein Gerät zu aktivieren, müssen Sie ein LSC (Locally Significant

Certificate) installieren und diesem Gerät ein Sicherheitsprofil zuweisen. Das LSC verfügt über den öffentlichen Schlüssel für den Endpunkt, der durch den privaten CAPF-Schlüssel (Certificate Authority Proxy Function) signiert wird. Es ist nicht standardmäßig auf Telefonen installiert.

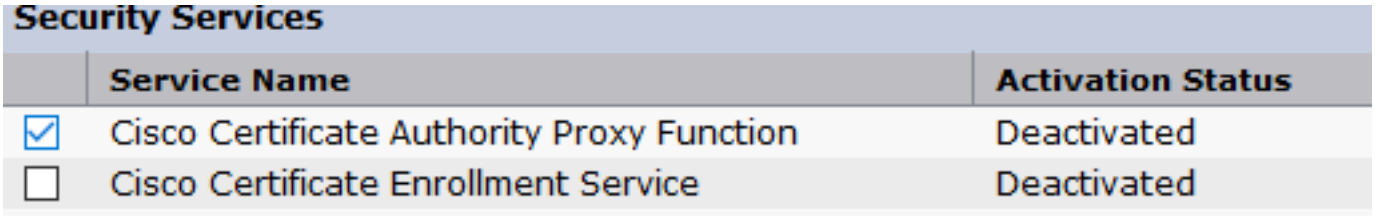
Schritte:

1. Melden Sie sich an Cisco Unified Serviceability Interface.
2. Navigieren Sie zu Tools > Service Activation.

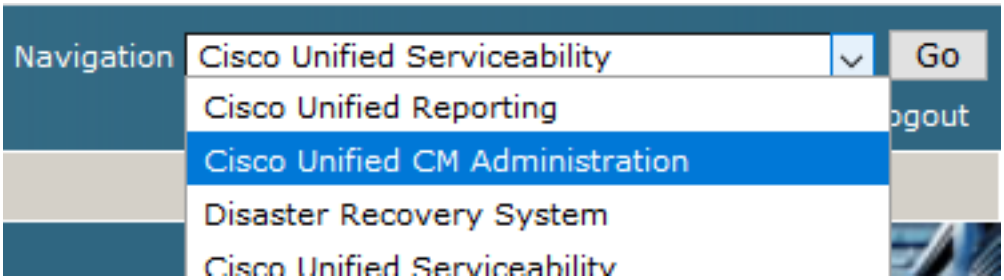
3. Wählen Sie den CUCM-Server aus, und klicken Sie auf Go .



4. Überprüfen Cisco Certificate Authority Proxy Function und klicke auf Save um den Service zu aktivieren. Klicken Sie auf Ok zur Bestätigung.

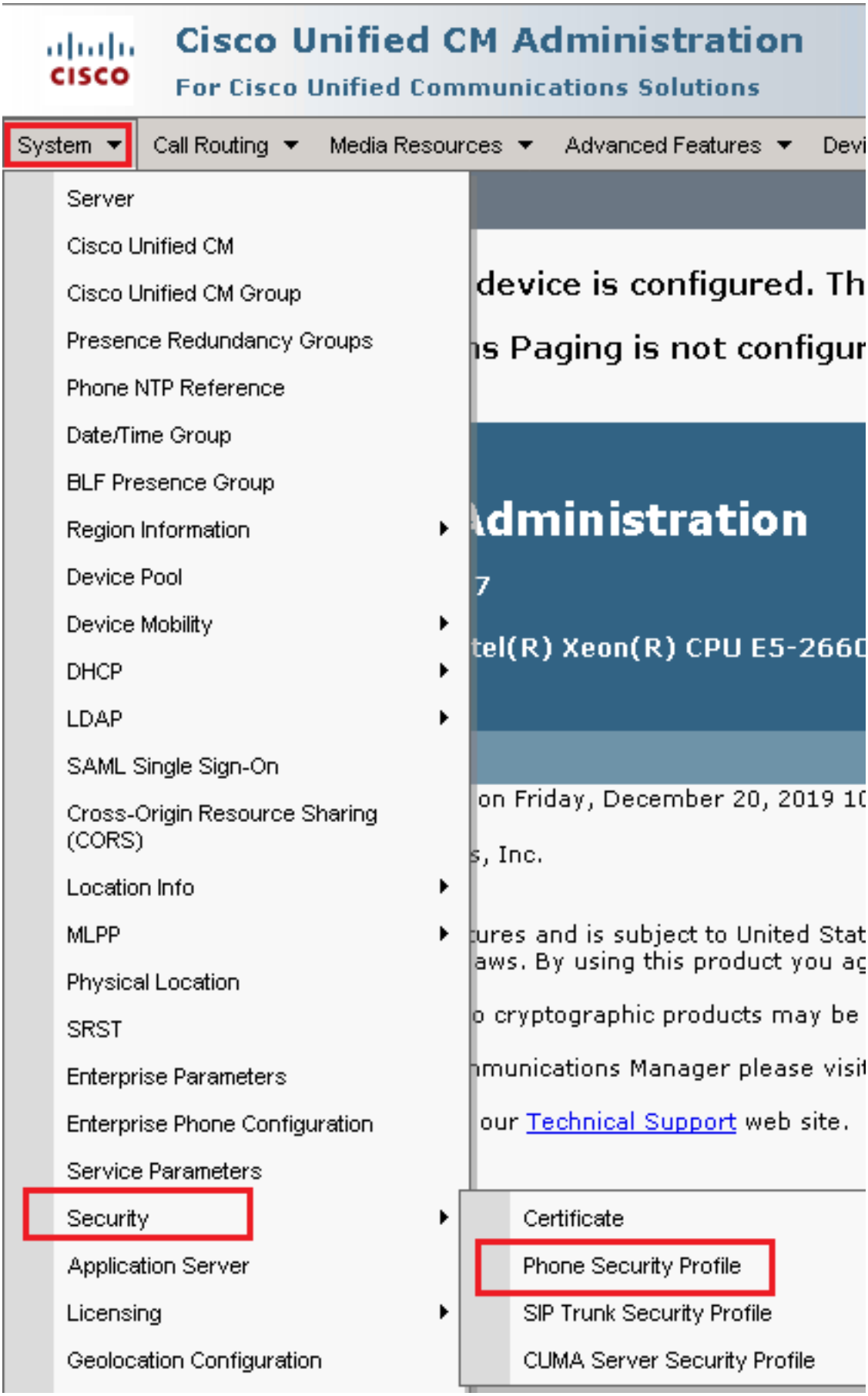


5. Vergewissern Sie sich, dass der Dienst aktiviert ist, und navigieren Sie zu Cisco Unified CM Administration.



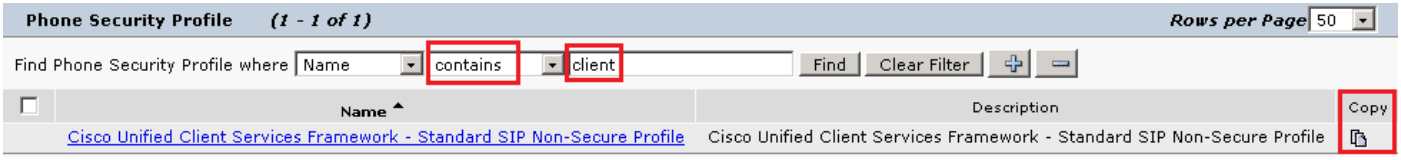
6. Nachdem Sie sich erfolgreich bei der CUCM-Verwaltung angemeldet haben, navigieren Sie

zu System > Security > Phone Security Profile um ein Gerätesicherheitsprofil für das Agentengerät zu erstellen.

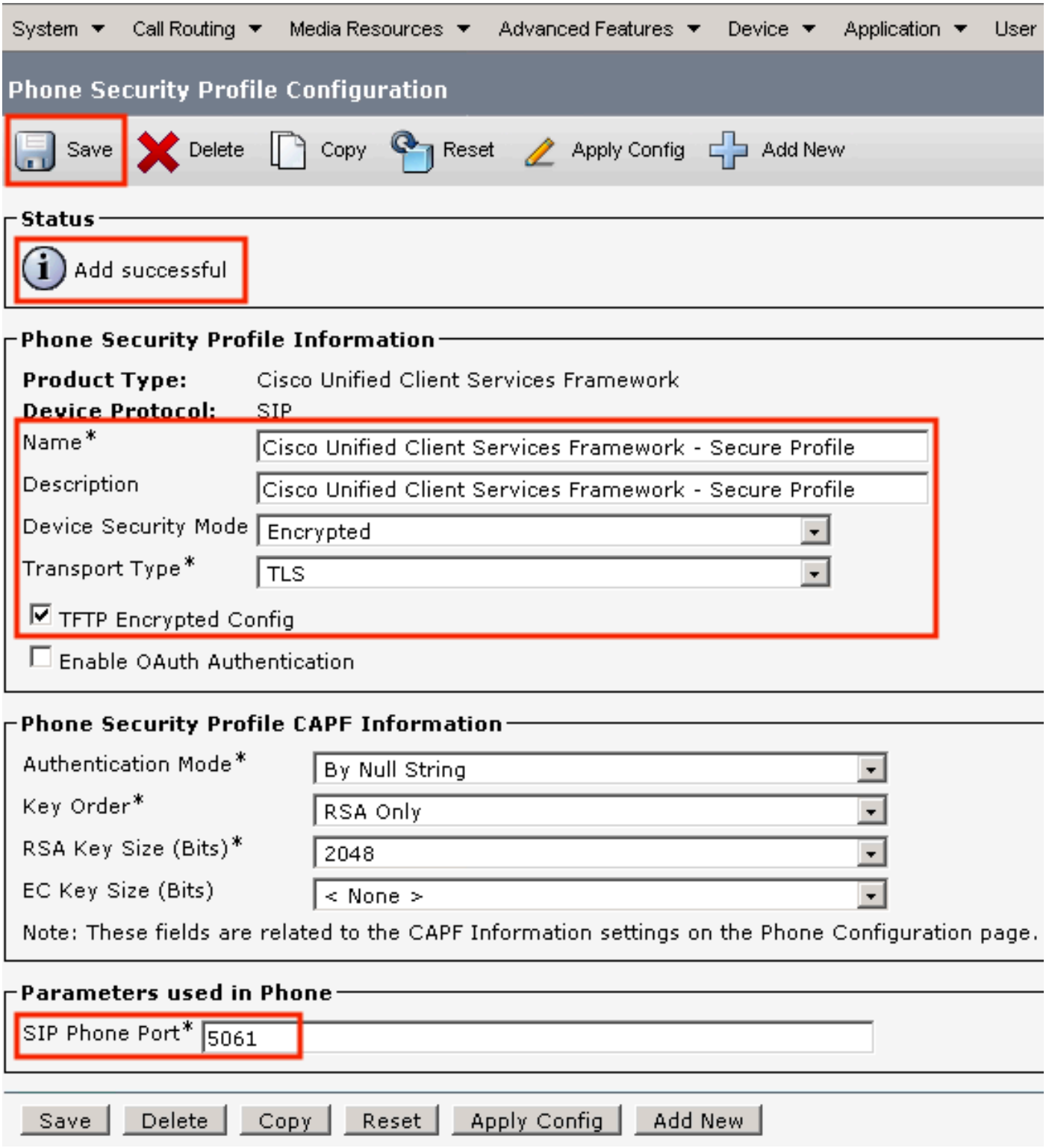


7. Suchen Sie die Sicherheitsprofile für den Gerätetyp Ihres Agenten. In diesem Beispiel wird

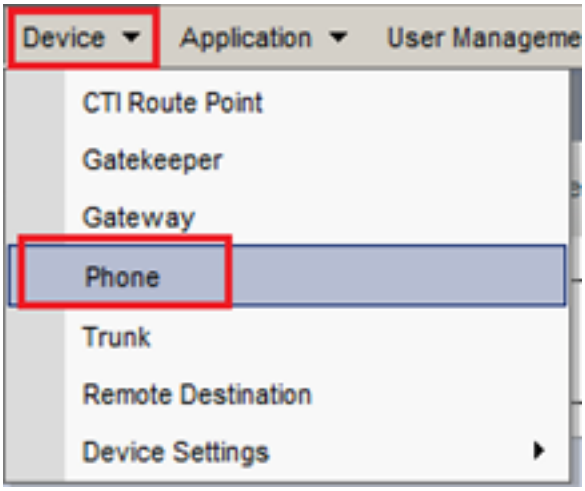
ein Softphone verwendet. Wählen Sie deshalb Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile . Klicken Sie auf Copy um dieses Profil zu kopieren.



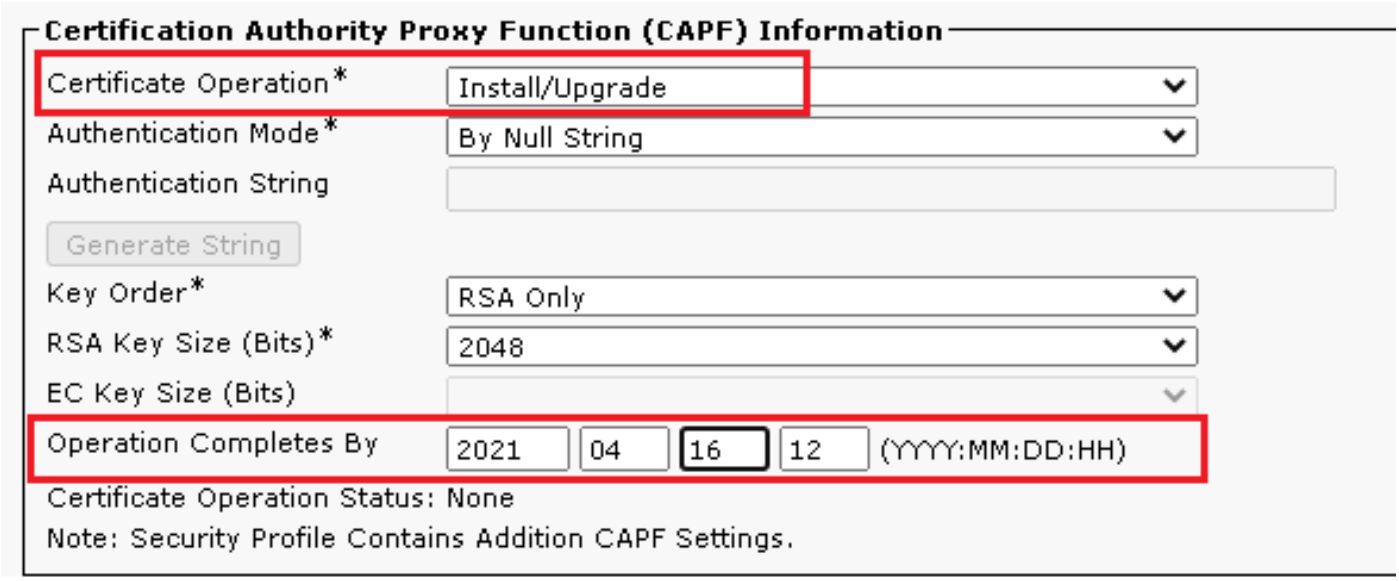
8. Profil umbenennen in Cisco Unified Client Services Framework - Secure Profile, ändern Sie die Parameter wie in diesem Bild dargestellt, und klicken Sie dann auf Save oben links auf der Seite.



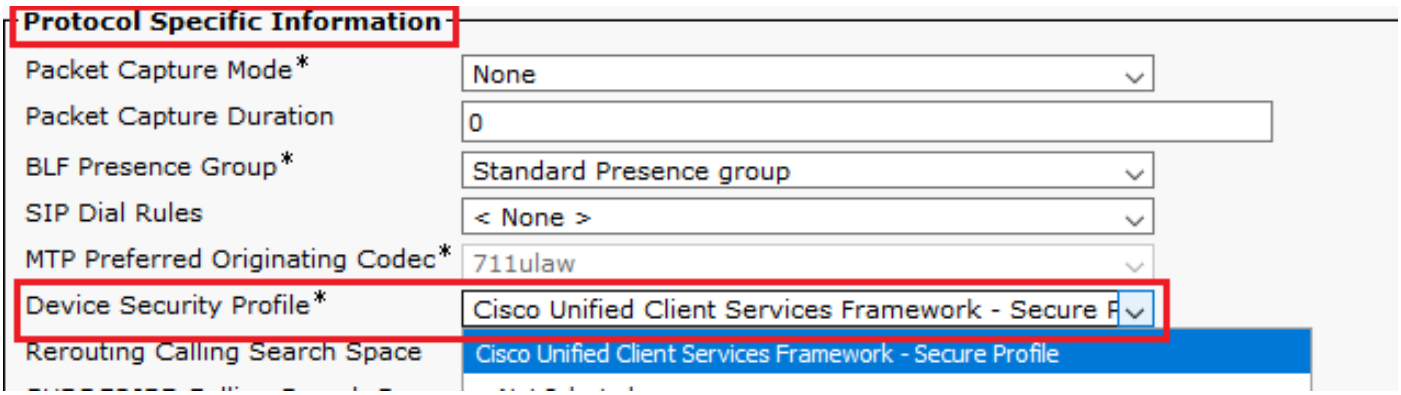
9. Navigieren Sie nach der erfolgreichen Erstellung des Telefongeräteprofils zu Device > Phone.



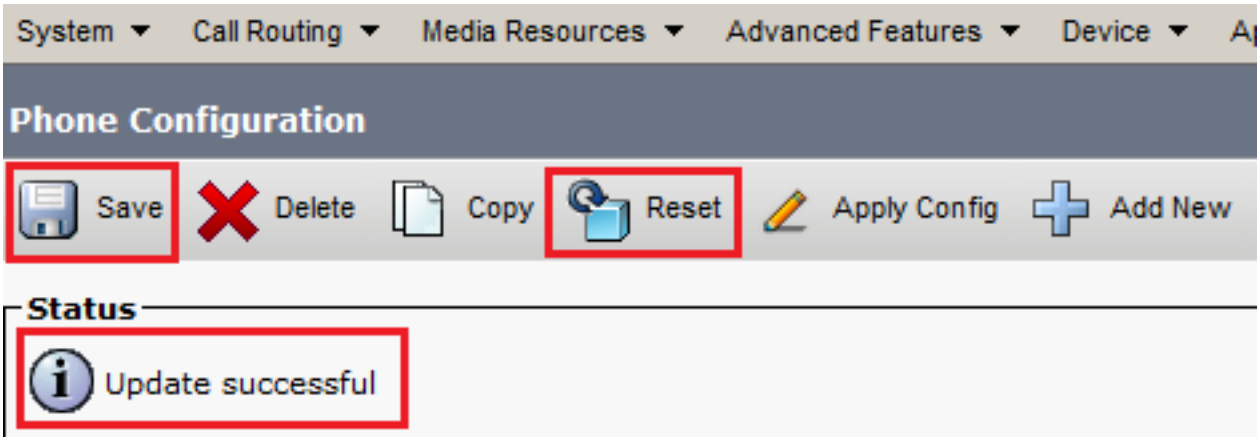
10. Klicken Sie auf Find um alle verfügbaren Telefone aufzulisten, und klicken Sie dann auf das Agententelefon.
11. Die Konfigurationsseite für Agententelefone wird geöffnet. Suchen Certification Authority Proxy Function (CAPF) Information Abschnitt. Um LSC zu installieren, stellen Sie Certificate Operation zu Install/Upgrade und Operation Completes by auf einen beliebigen Zeitpunkt in der Zukunft ändern.



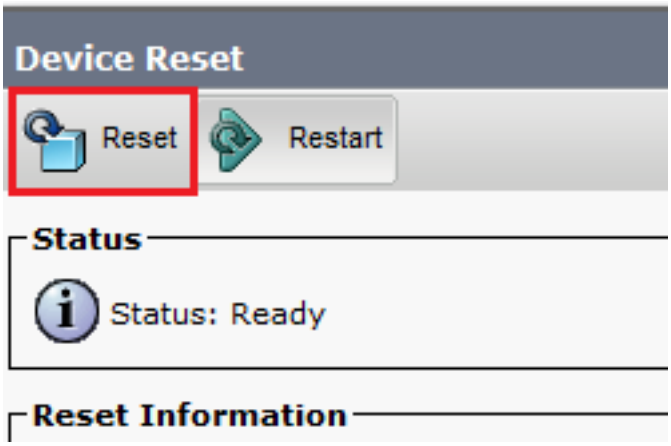
12. Suchen Protocol Specific Information Abschnitt. Ändern Device Security Profile zu Cisco Unified Client Services Framework – Secure Profile.



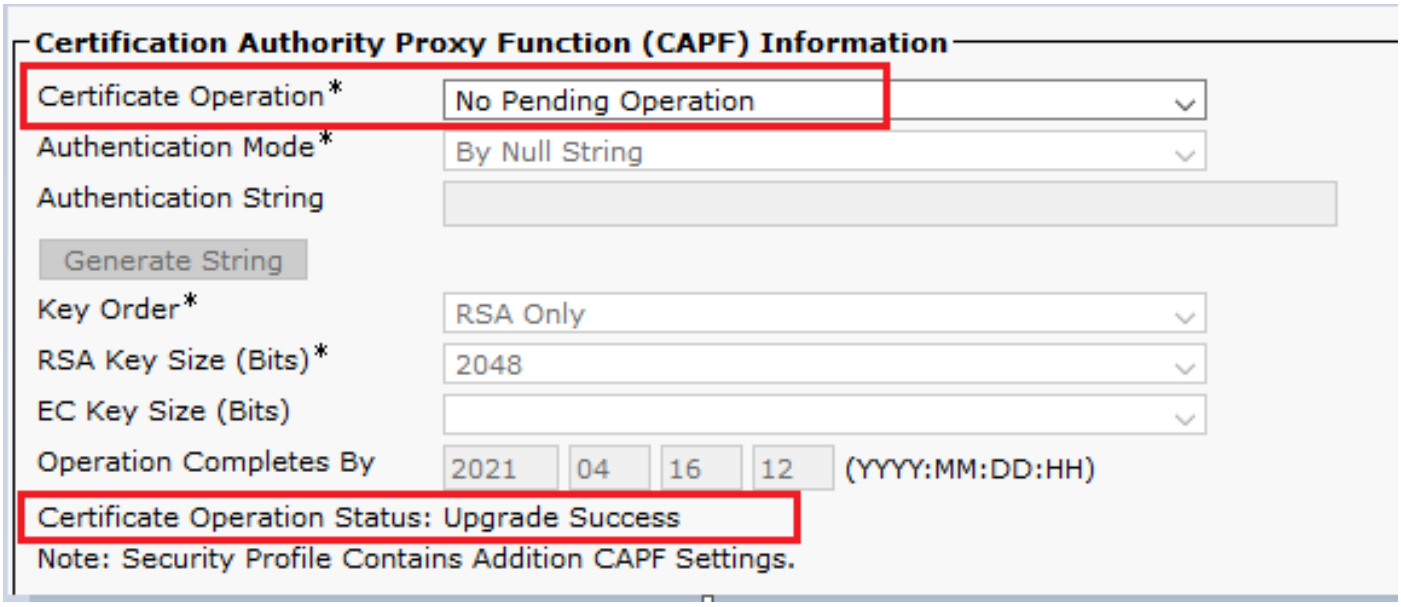
13. Klicken Sie auf Save oben links auf der Seite. Stellen Sie sicher, dass die Änderungen erfolgreich gespeichert wurden, und klicken Sie auf Reset.



14. Ein Popup-Fenster wird geöffnet, und klicken Sie auf Reset um die Aktion zu bestätigen.



15. Nachdem sich das Agent-Gerät erneut beim CUCM registriert hat, aktualisieren Sie die aktuelle Seite, und überprüfen Sie, ob das LSC erfolgreich installiert wurde. Überprüfen Certification Authority Proxy Function (CAPF) Information Abschnitt, Certificate Operation muss auf eingestellt sein No Pending Operationund Certificate Operation Status ist auf Upgrade Success .

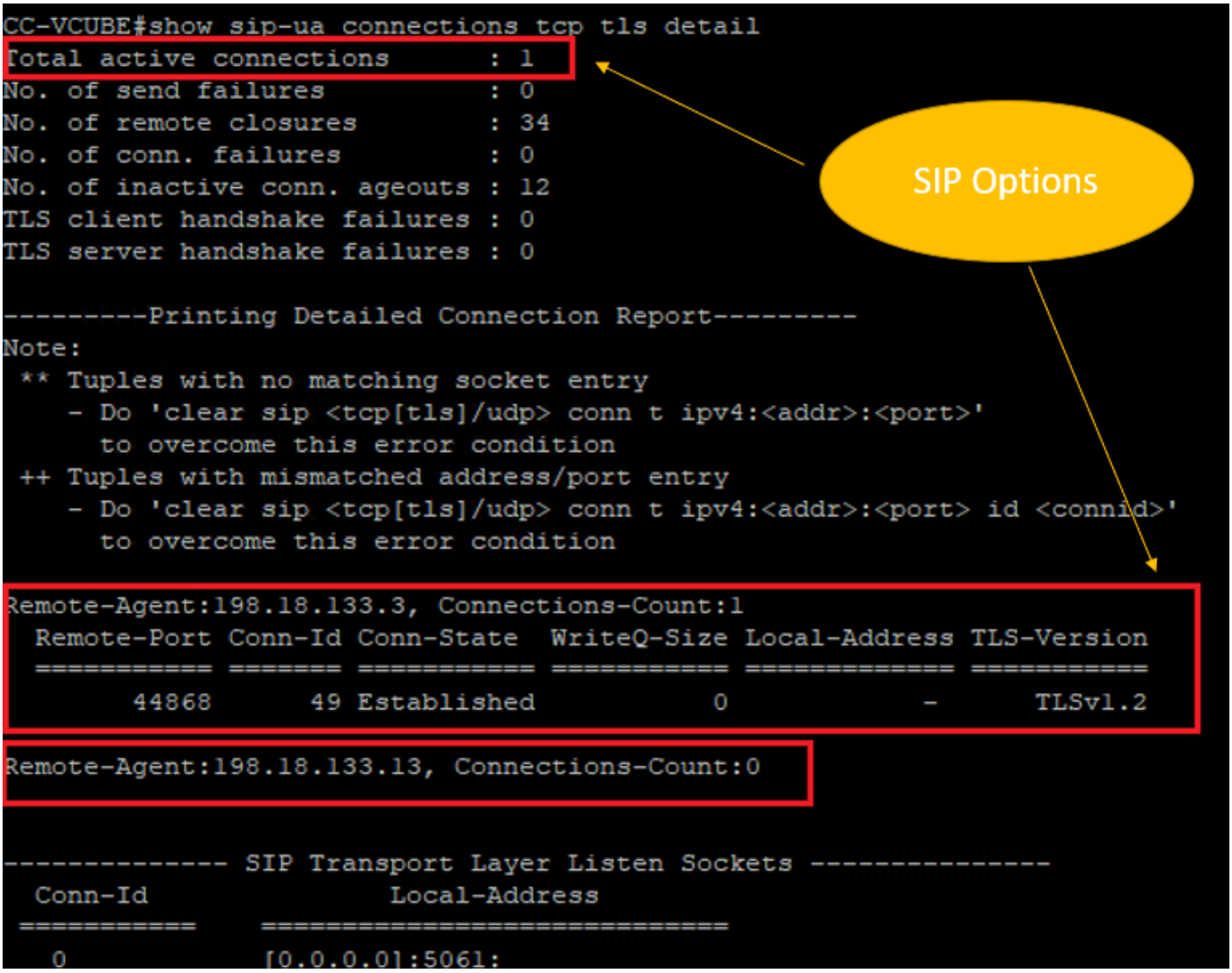


16. Siehe Schritte. 7-13, um andere Agenten und Geräte zu schützen, die Sie zum Sichern von SIP mit CUCM verwenden möchten.

Überprüfung

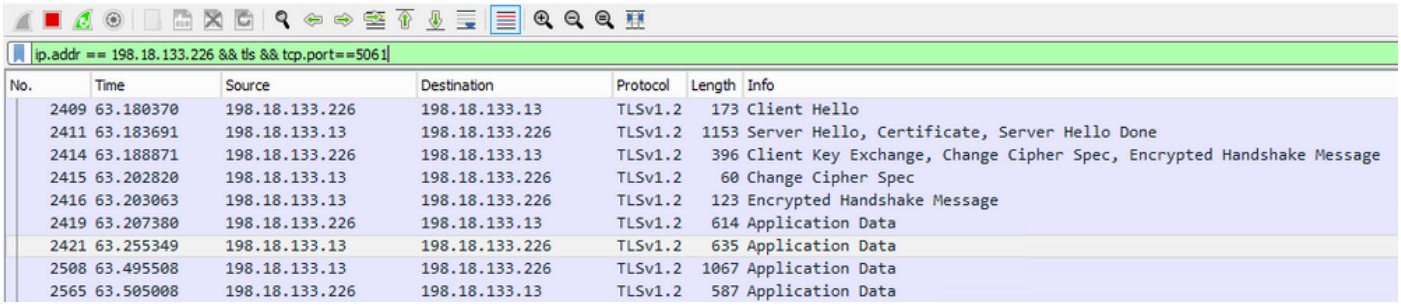
So prüfen Sie, ob die SIP-Signalisierung ordnungsgemäß gesichert ist:

1. Öffnen Sie eine SSH-Sitzung mit vCUBE, und führen Sie den Befehl aus. show sip-ua connections tcp tls detail , und bestätigen Sie, dass derzeit keine TLS-Verbindung mit CVP (198.18.133.13) besteht.



Hinweis: Derzeit ist nur eine aktive TLS-Sitzung mit CUCM für SIP-Optionen auf CUCM aktiviert (198.18.133.3). Wenn keine SIP-Optionen aktiviert sind, besteht keine SIP-TLS-Verbindung.

2. Melden Sie sich bei CVP an, und starten Sie Wireshark.
3. Tätigen Sie einen Testanruf an die Contact Center-Nummer.
4. Navigieren Sie zur CVP-Sitzung. Führen Sie in Wireshark diesen Filter aus, um die SIP-Signalisierung mit CUBE zu überprüfen:
ip.addr == 198.18.133.226 && tls && tcp.port==5061



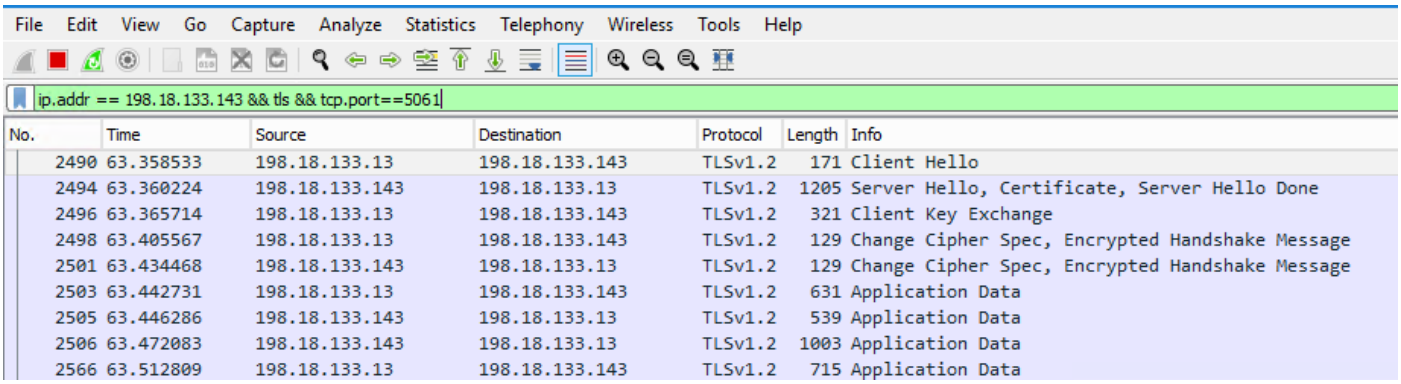
ip.addr == 198.18.133.226 && tls && tcp.port==5061

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

Prüfen: Ist eine SIP-over-TLS-Verbindung hergestellt? Falls ja, bestätigt der Ausgang, dass SIP-Signale zwischen CVP und CUBE gesichert sind.

5. Überprüfen Sie die SIP-TLS-Verbindung zwischen CVP und CVVB. Führen Sie in derselben Wireshark-Sitzung den folgenden Filter aus:

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

Prüfen: Ist eine SIP-over-TLS-Verbindung hergestellt? Falls ja, bestätigt der Ausgang, dass SIP-Signale zwischen CVP und CVVB gesichert sind.

6. Sie können die SIP-TLS-Verbindung mit dem CVP auch von CUBE aus überprüfen. Navigieren Sie zur vCUBE SSH-Sitzung, und führen Sie diesen Befehl aus, um sichere SIP-Signale zu überprüfen:

show sip-ua connections tcp tls detail

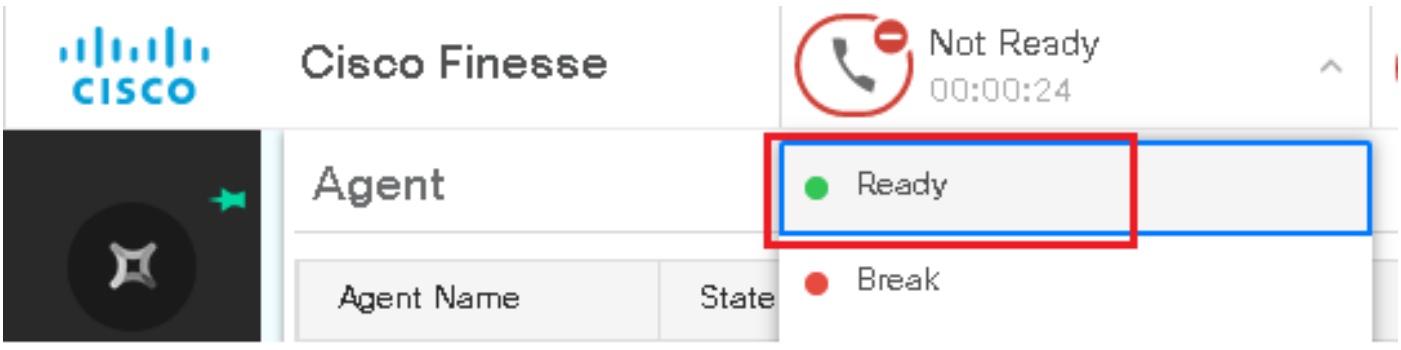
```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------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:
```

Prüfen: Wurde eine SIP-über-TLS-Verbindung mit dem CVP hergestellt? Falls ja, bestätigt der Ausgang, dass SIP-Signale zwischen CVP und CUBE gesichert sind.

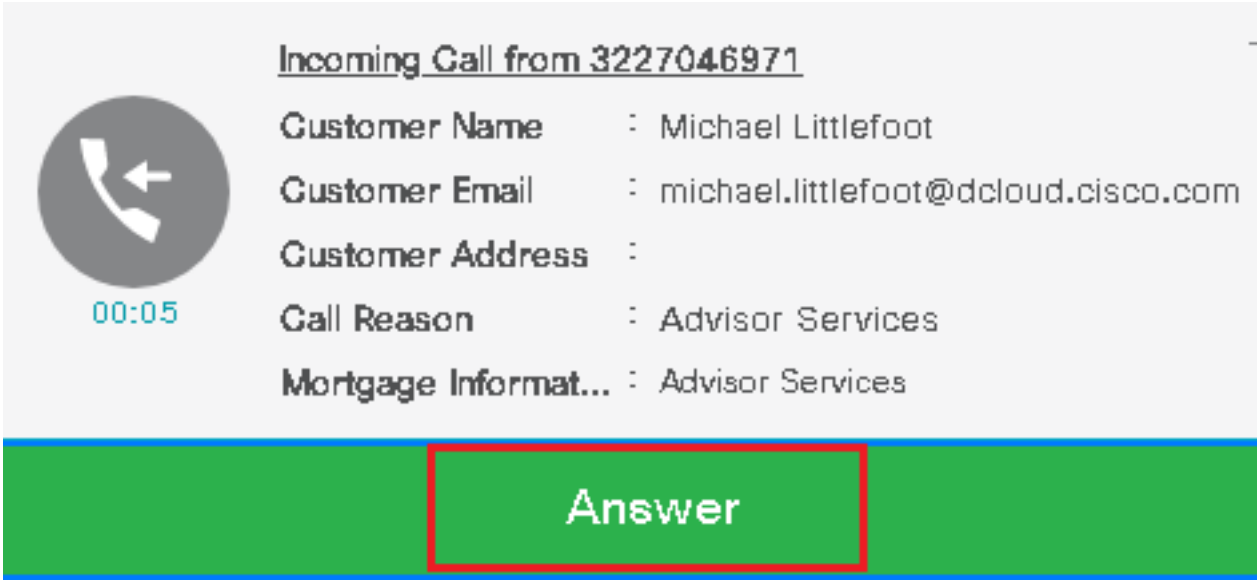
7. Derzeit ist der Anruf aktiv, und Sie hören Warteschleifenmusik, da kein Agent verfügbar ist, um den Anruf zu beantworten.

8. Stellen Sie den Mitarbeiter zur Verfügung, um den Anruf anzunehmen.

.

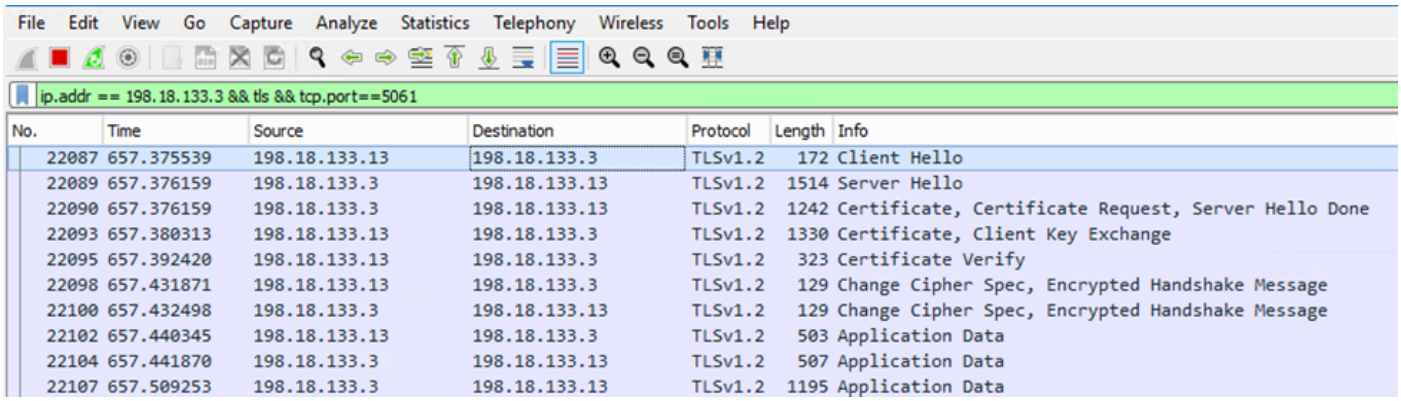


9. Agent wird reserviert und der Anruf wird an ihn/sie weitergeleitet. Klicken Sie auf Answer um den Anruf anzunehmen.



10. Anruf verbindet sich mit dem Agenten.

11. Um SIP-Signale zwischen CVP und CUCM zu überprüfen, navigieren Sie zur CVP-Sitzung, und führen Sie diesen Filter in Wireshark aus:
ip.addr == 198.18.133.3 && tls && tcp.port==5061



> **Prüfen**: Werden alle SIP-Kommunikationen mit CUCM (198.18.133.3) über TLS abgewickelt? Wenn ja, bestätigt der Ausgang, dass SIP-Signale zwischen CVP und CUCM gesichert sind.

Fehlerbehebung

Wenn TLS nicht eingerichtet ist, führen Sie die folgenden Befehle auf CUBE aus, um das Debuggen von TLS zur Fehlerbehebung zu aktivieren:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.