

Konfigurieren der sicheren SIP-Signalisierung in Contact Center Enterprise

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Aufgabe 1: Sichere CUBE-Konfiguration](#)

[Aufgabe 2: Sichere CVP-Konfiguration](#)

[Aufgabe 3: Sichere CVVB-Konfiguration](#)

[Aufgabe 4: Sichere CUCM-Konfiguration](#)

[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](#)

[Überprüfung](#)

[Fehlerbehebung](#)

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

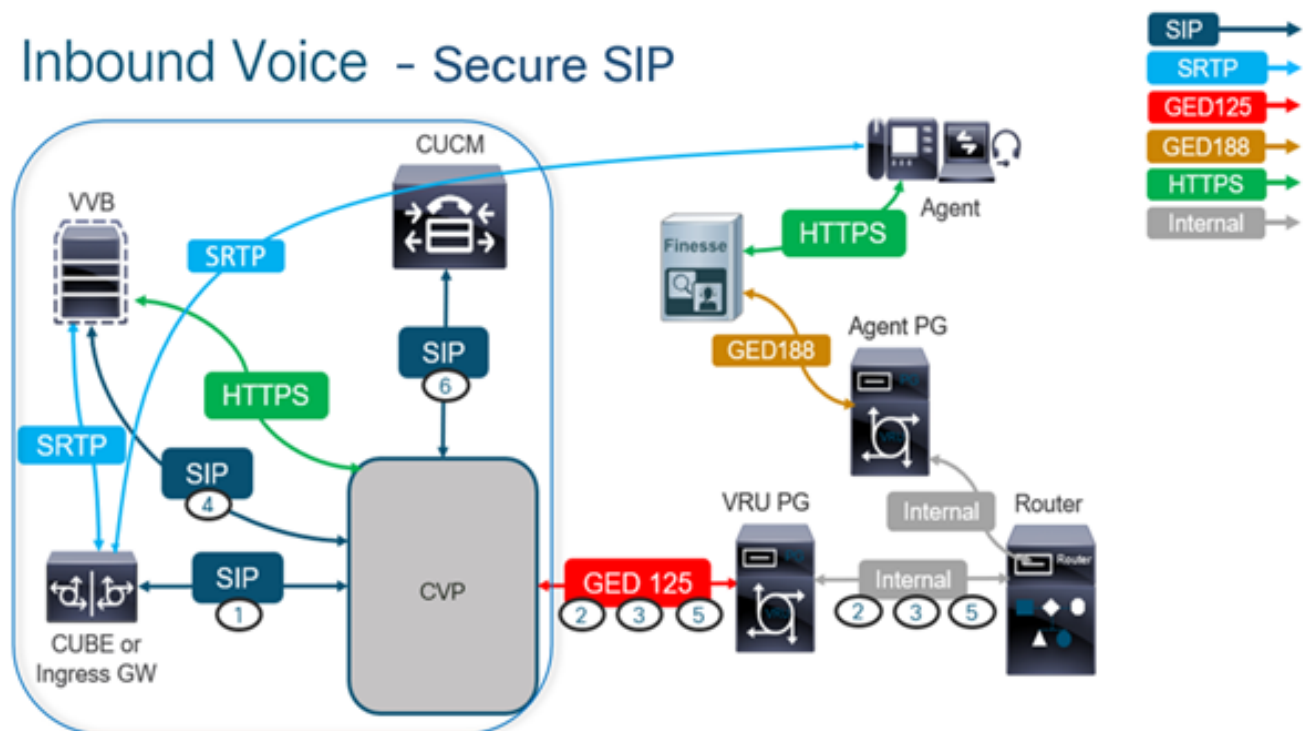
Verwendete Komponenten

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 an UCCE Web Administration.
2. Navigieren Sie zu **Call Settings > Route Settings > SIP Server Group**.

Route Settings

Media Routing Domain Call Type Dialed Number Expanded Call Variables **SIP Server Group**

Properties

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**.

Edit cucm1.dcloud.cisco.com

General

Members

List of Group Members



Hostname/IP	Priority	Weight	Port	SecurePort	Site
198.18.133.3	10	10	5060	5061	Main

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

Edit vvb1.dcloud.cisco.com

General

Members

List of Group Members



Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

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**.

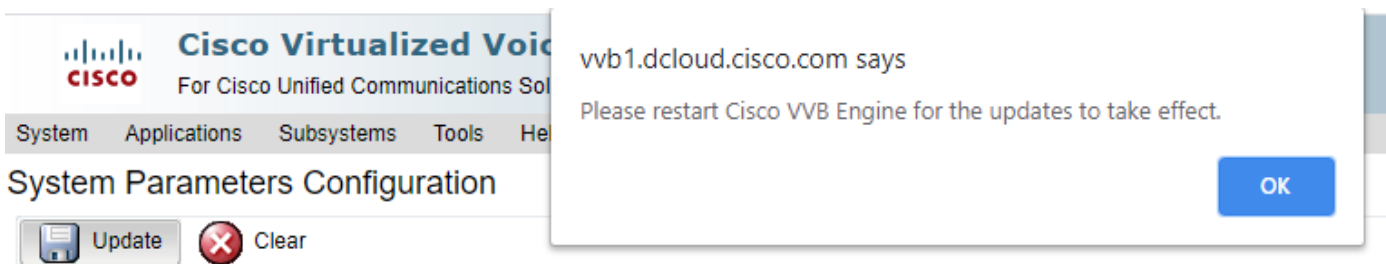
The screenshot shows the Cisco Virtualized Voice Browser Administration interface. At the top, there is a navigation bar with the following items: System, Applications, Subsystems, Tools, and Help. Below this, there is a dropdown menu with 'System Parameters' selected and 'Logout' as an option. The main header area displays the Cisco logo and the text 'Cisco Virtualized Voice Browser Administration For Cisco Unified Communications Solutions'. At the bottom, there is a dark blue banner with the text 'Cisco Virtualized Voice Browser Administration' and 'System version: 12.5.1.10000-24'.

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

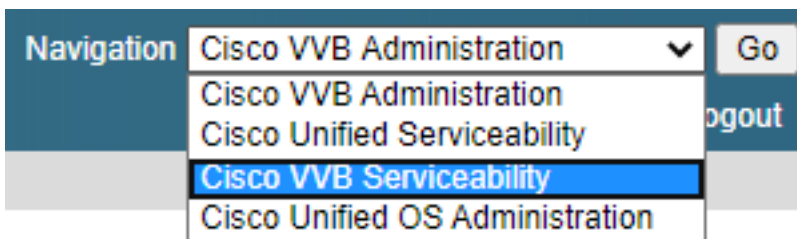
version als TLSv1.2.

Security Parameters		
Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
▶ Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

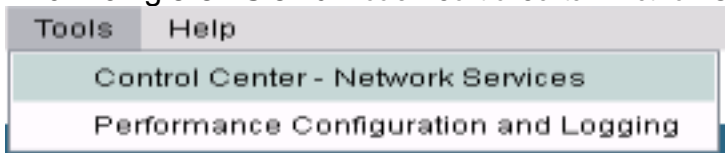
4. Klicken Sie auf **Aktualisieren**. Klicken Sie auf **ok** wenn Sie dazu aufgefordert werden, das CVVB-Modul neu zu starten.



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**.

Control Center - Network Services



Status

 Ready

Select Server

Server *

System Services	
	Service Name
<input type="radio"/>	Perfmon Counter Service
<input type="radio"/>	▼Cluster View Daemon
	▶Manager Manager
<input checked="" type="radio"/>	▼Engine
	▶Manager Manager
	▶Subsystem Manager

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

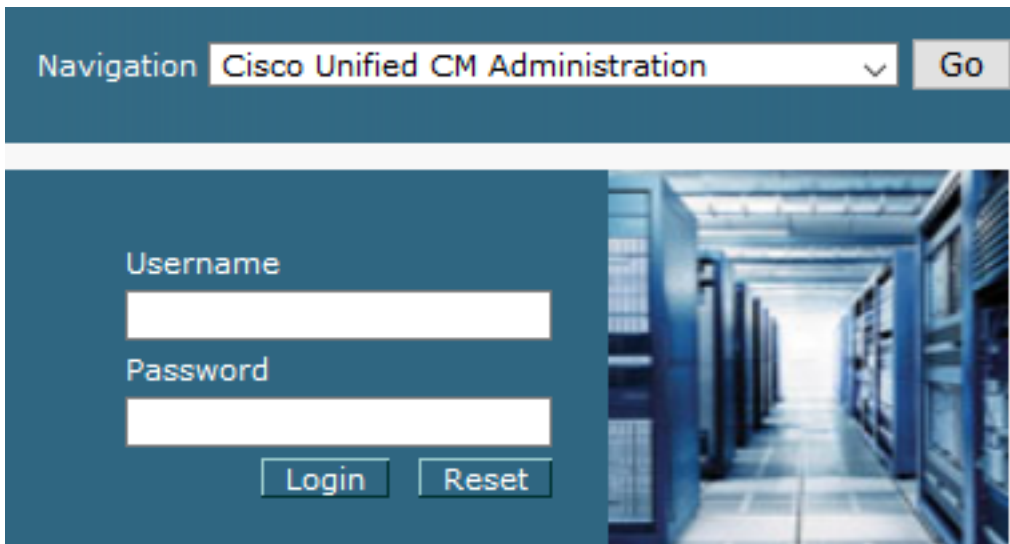
CUCM-Sicherheitsmodus auf "Gemischt" setzen

CUCM unterstützt zwei Sicherheitsmodi:

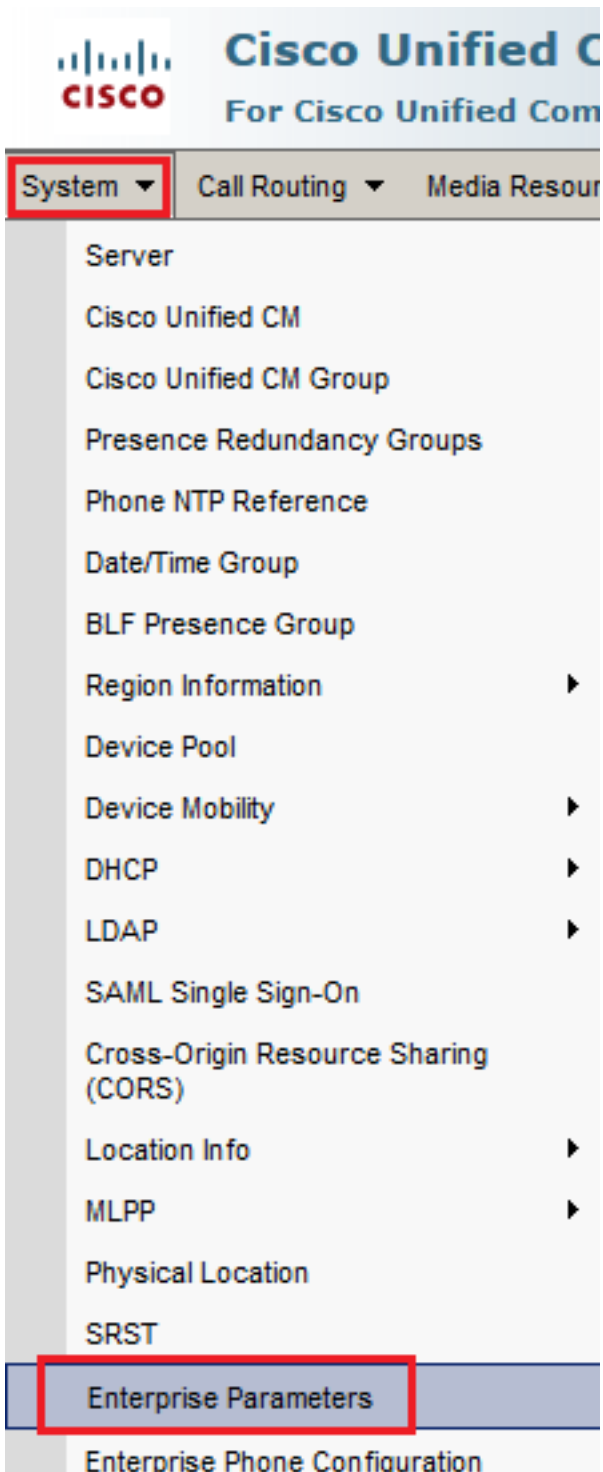
- Nicht sicherer Modus (Standardmodus)
- Gemischter Modus (sicherer Modus)

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.



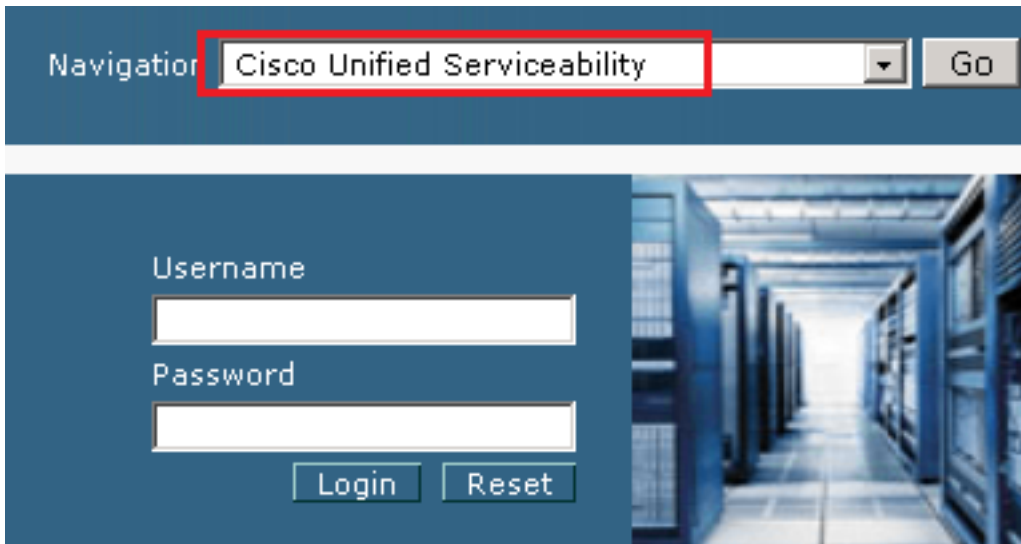
4. Wenn der Clustersicherheitsmodus auf 0 festgelegt ist, bedeutet dies, dass der Clustersicherheitsmodus auf "nicht sicher" festgelegt ist. Sie müssen den gemischten Modus über die CLI aktivieren.
5. Öffnen Sie eine SSH-Sitzung mit dem CUCM.
6. Nachdem Sie sich über SSH erfolgreich beim CUCM angemeldet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

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.
admin:█
```

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`.

Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Alarm ▾ Trace ▾ **Tools ▾** Snmp ▾ CallHome ▾ Help ▾

Service Activation

Control Center - Feature Services

Control Center - Network Services

Serviceability Reports Archive

Audit Log Configuration

Locations ▶

Dialed Number Analyzer

CDR Analysis and Reporting

CDR Management

System version
VMware Install

User admin last logged in
Copyright © 1999 - All rights reserved.
This product contains... compliance with U.S.
A summary of U.S. I...
For information about...

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

Select Server

Server*

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

CM Services	
	Service Name
<input checked="" type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

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

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



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

CM Services	
	Service Name
<input type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input checked="" type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

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

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



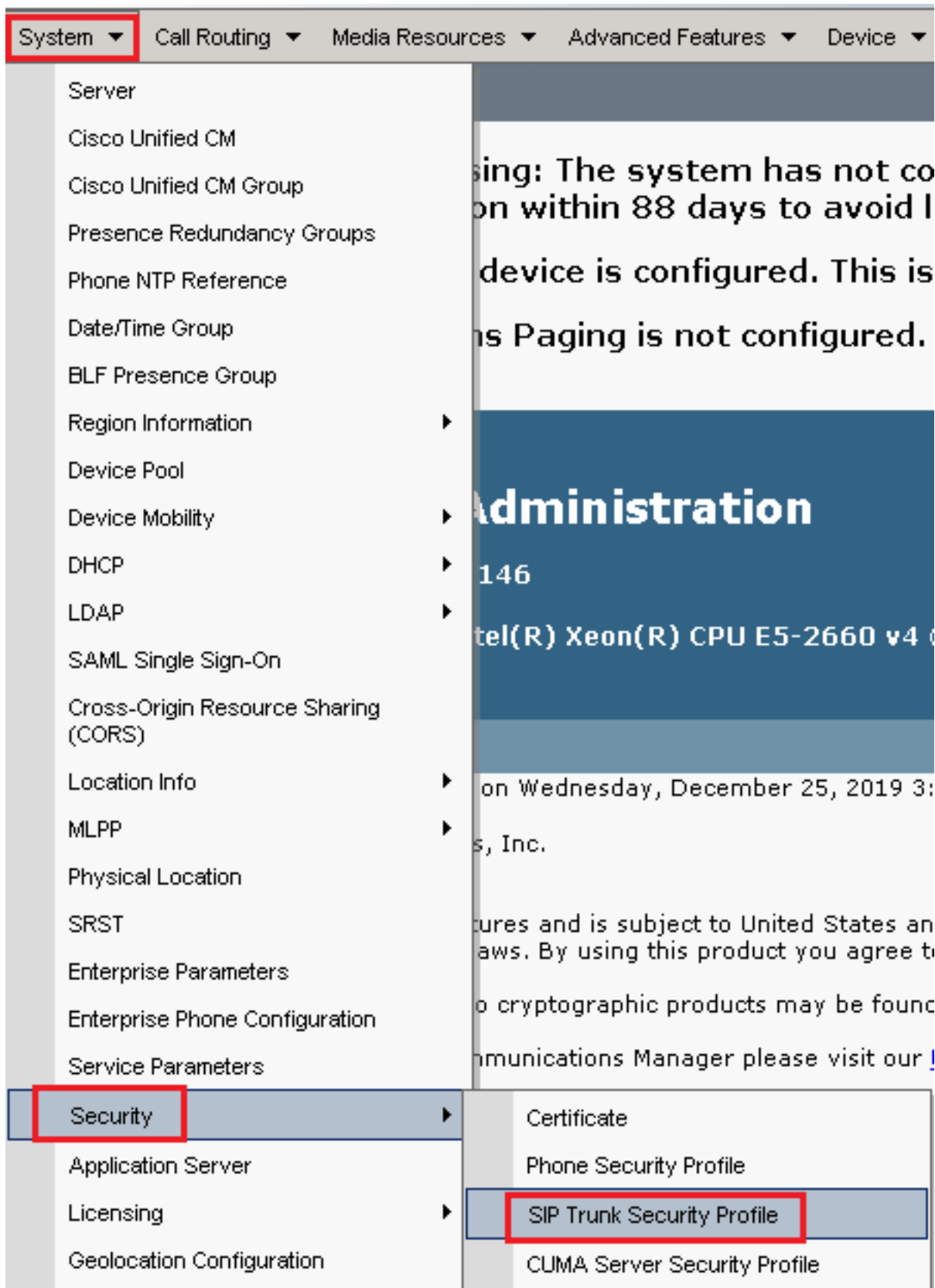
16. Nachdem die Dienste erfolgreich neu gestartet wurden, überprüfen Sie, ob der Cluster-Sicherheitsmodus auf den gemischten Modus gesetzt ist, und navigieren Sie zur CUCM-Verwaltung, wie in Schritt 5 beschrieben. Überprüfen Sie dann die **Cluster Security Mode**. Jetzt muss sie auf 1.

Security Parameters	
Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Disabled

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.

Find and List SIP Trunk Security Profiles

 Add New  Select All  Clear All  Delete Selected



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

SIP Trunk Security Profile Configuration

Related Links: [Back](#)

 Save  Delete  Copy  Reset  Apply Config  Add New

- Status -

-  Add successful
-  Reset of the trunk is required to have changes take effect.

- SIP Trunk Security Profile Information -

Name*	SecureSIPTLSforCube
Description	
Device Security Mode	Encrypted ▾
Incoming Transport Type*	TLS ▾
Outgoing Transport Type	TLS ▾
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SIP-GW
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter ▾

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.

Status

- i** Add successful
- i** Reset of the trunk is required to have changes take effect.

SIP Trunk Security Profile Information

Name* SecureSIPTLSforCvp

Description

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)* 600

Secure Certificate Subject or Subject Alternate Name cvp1.dcloud.cisco.com

Incoming Port* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

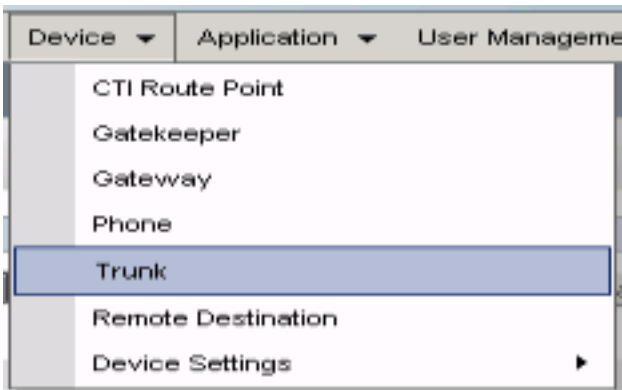
Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

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.

Trunks (1 - 5 of 5)

Find Trunks where Device Name begins with vCube Find Clear Filter

	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

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.

SIP Information

Destination

Destination Address is an SRV

Destination Address: 1* 198.18.133.226

Destination Address IPv6: [Empty]

Destination Port: 5061

MTP Preferred Originating Codec*: 711ulaw

BLF Presence Group*: Standard Presence group

SIP Trunk Security Profile*: SecureSIPTLSforCube

Rerouting Calling Search Space: < None >

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

Trunk Configuration

Save Delete Reset Add New


Status

Update successful

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

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**.

Trunks (1 - 1 of 1)				
Find Trunks where				
<input type="checkbox"/>	Device Name	begins with	cvp	<input type="button" value="Find"/>
<input type="button" value="Clear Filter"/> <input type="button" value="+"/> <input type="button" value="-"/>				
Select item or enter search text				
<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	 CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP


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**.

SIP Information		
Destination		
<input type="checkbox"/> Destination Address is an SRV		
Destination Address	Destination Address IPv6	Destination Port
1* 198.18.133.13		5061
MTP Preferred Originating Codec*	711ulaw	
BLF Presence Group*	Standard Presence group	
SIP Trunk Security Profile*	SecureSIPTLSforCvp	

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

Trunk Configuration	
<input type="button" value="Save"/>	<input type="button" value="Delete"/>
<input type="button" value="Reset"/>	<input type="button" value="Add New"/>
Status	
 Update successful	

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

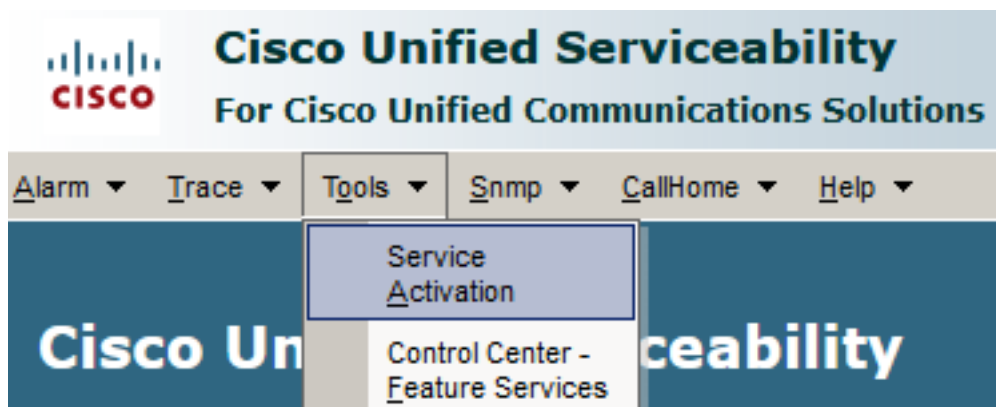
Sichere Gerätekommunikation der Agenten mit CUCM

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**.

Service Activation

Select Server

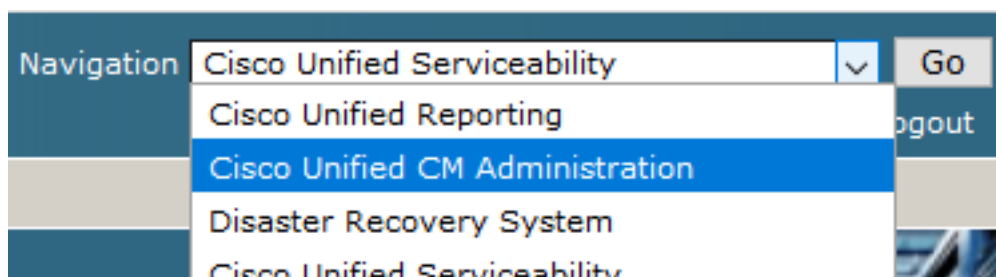
Server*

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

Security Services

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Deactivated
<input type="checkbox"/>	Cisco Certificate Enrollment Service	Deactivated

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.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text 'Cisco Unified CM Administration For Cisco Unified Communications Solutions' are visible. Below the header is a navigation bar with several menu items: 'System', 'Call Routing', 'Media Resources', 'Advanced Features', and 'Devices'. The 'System' menu is expanded, showing a list of sub-items. The 'Security' item is highlighted with a red box. A secondary menu is open for 'Security', showing options like 'Certificate', 'Phone Security Profile', 'SIP Trunk Security Profile', and 'CUMA Server Security Profile'. The 'Phone Security Profile' option is also highlighted with a red box. The background of the page shows a blurred view of a device configuration page with some text like 'device is configured. The...', 'Paging is not configur...', and 'Administration'.

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.

Phone Security Profile (1 - 1 of 1) Rows per Page 50







Find Phone Security Profile where Name contains client Find Clear Filter + -

Name	Description	Copy
Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	


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.

System Call Routing Media Resources Advanced Features Device Application User

Phone Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

Status

 Add successful

Phone Security Profile Information

Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Name* Cisco Unified Client Services Framework - Secure Profile
Description Cisco Unified Client Services Framework - Secure Profile
Device Security Mode Encrypted
Transport Type* TLS

TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

Authentication Mode* By Null String
Key Order* RSA Only
RSA Key Size (Bits)* 2048
EC Key Size (Bits) < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

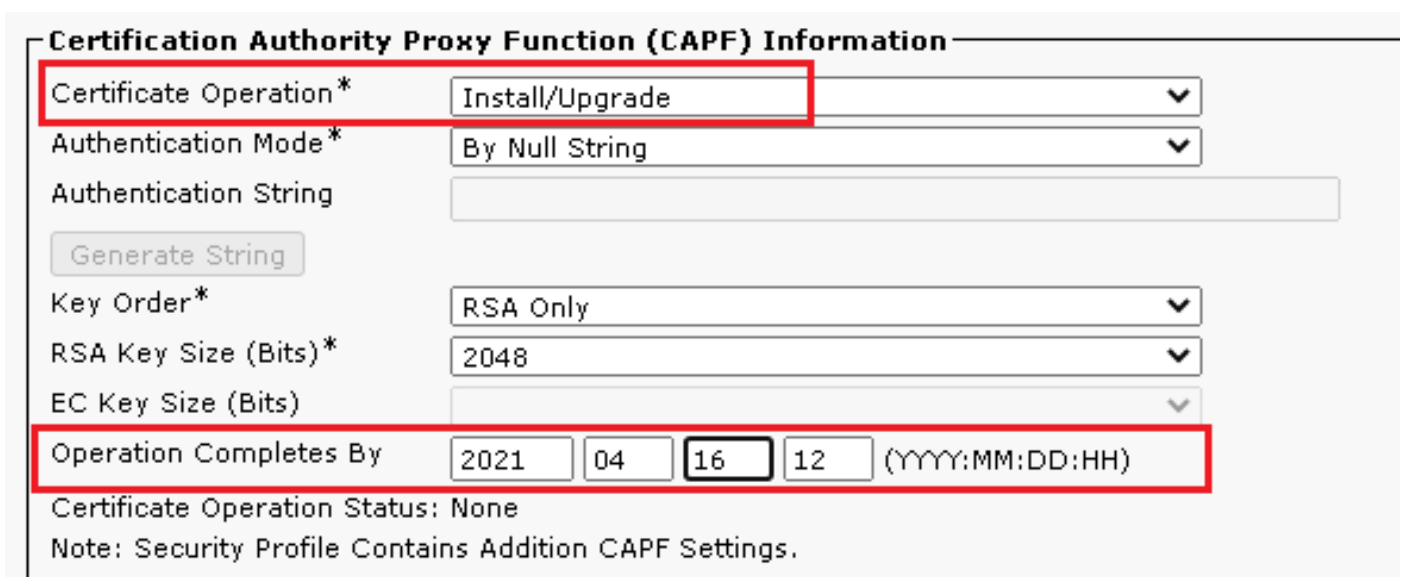
Save Delete Copy Reset Apply Config Add New

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.

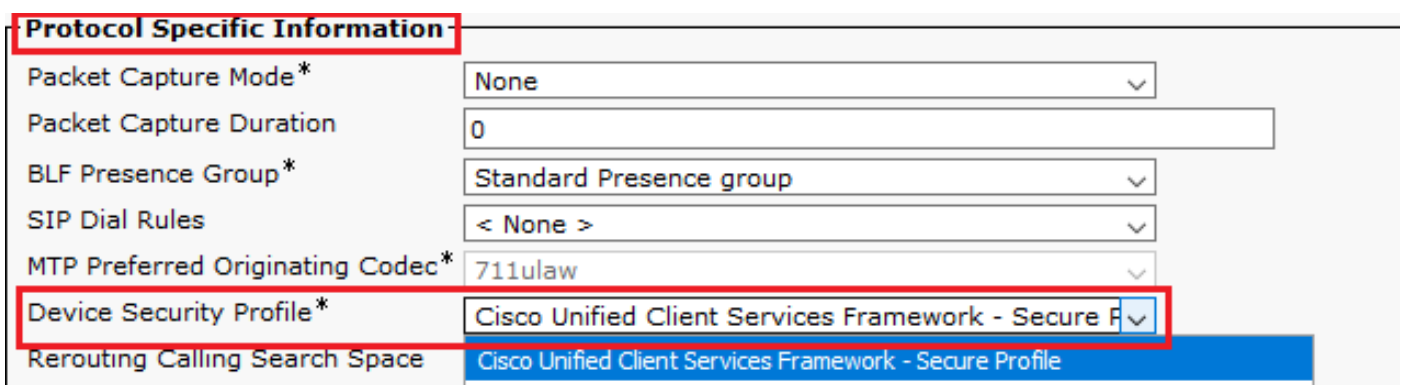
11. Die Konfigurationsseite für Agententelefone wird geöffnet. Suchen **Certification Authority Proxy Function (CAPF) Information** Abschnitt. Um LSC zu installieren, stellen Sie **Certificate Operation** zu **Install/Upgrade** und **Operation Completes by** auf einen beliebigen Zeitpunkt in der Zukunft ändern.



Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None
Note: Security Profile Contains Addition CAPF Settings.

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



Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Unified Client Services Framework - Secure Profile
Rerouting Calling Search Space	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**.

The screenshot shows the top navigation bar with tabs for System, Call Routing, Media Resources, Advanced Features, and Device. Below this is the 'Phone Configuration' section. A toolbar contains several icons: a floppy disk for 'Save', a red 'X' for 'Delete', a document for 'Copy', a circular arrow for 'Reset', a pencil for 'Apply Config', and a plus sign for 'Add New'. The 'Save' and 'Reset' buttons are highlighted with red boxes. Below the toolbar is a 'Status' section with a red-bordered box containing an information icon and the text 'Update successful'.

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

The screenshot shows a 'Device Reset' popup window. It has a title bar and two buttons: 'Reset' (with a circular arrow icon) and 'Restart' (with a circular arrow icon). The 'Reset' button is highlighted with a red box. Below the buttons is a 'Status' section with an information icon and the text 'Status: Ready'. At the bottom is a 'Reset Information' section.

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 Operation** und **Certificate Operation Status** ist auf **Upgrade Success** .

The screenshot shows the 'Certification Authority Proxy Function (CAPF) Information' section. It contains several configuration fields: 'Certificate Operation*' is set to 'No Pending Operation' (highlighted with a red box); 'Authentication Mode*' is 'By Null String'; 'Authentication String' is empty; 'Key Order*' is 'RSA Only'; 'RSA Key Size (Bits)*' is '2048'; 'EC Key Size (Bits)' is empty; 'Operation Completes By' is '2021 04 16 12 (YYYY:MM:DD:HH)'. At the bottom, 'Certificate Operation Status: Upgrade Success' is highlighted with a red box. A note below states: 'Note: Security Profile Contains Addition CAPF Settings.'

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.

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 1
No. of send failures         : 0
No. of remote closures       : 34
No. of conn. failures        : 0
No. of inactive conn. ageouts : 12
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
  =====
           44868      49 Established      0             -             TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:0

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



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`

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`

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

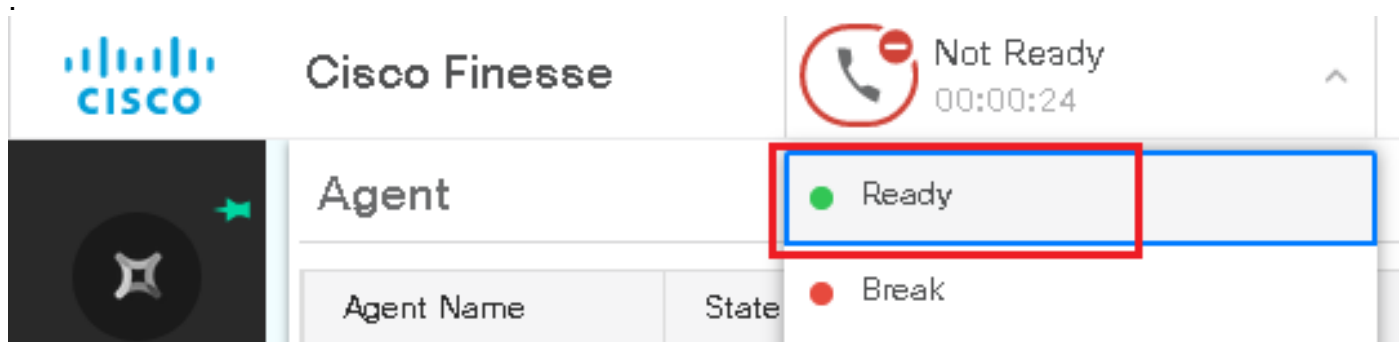
----- SIP Transport Layer Listen Sockets -----
  Conn-Id          Local-Address
  =====
  0                [0.0.0.0]:5061:

```

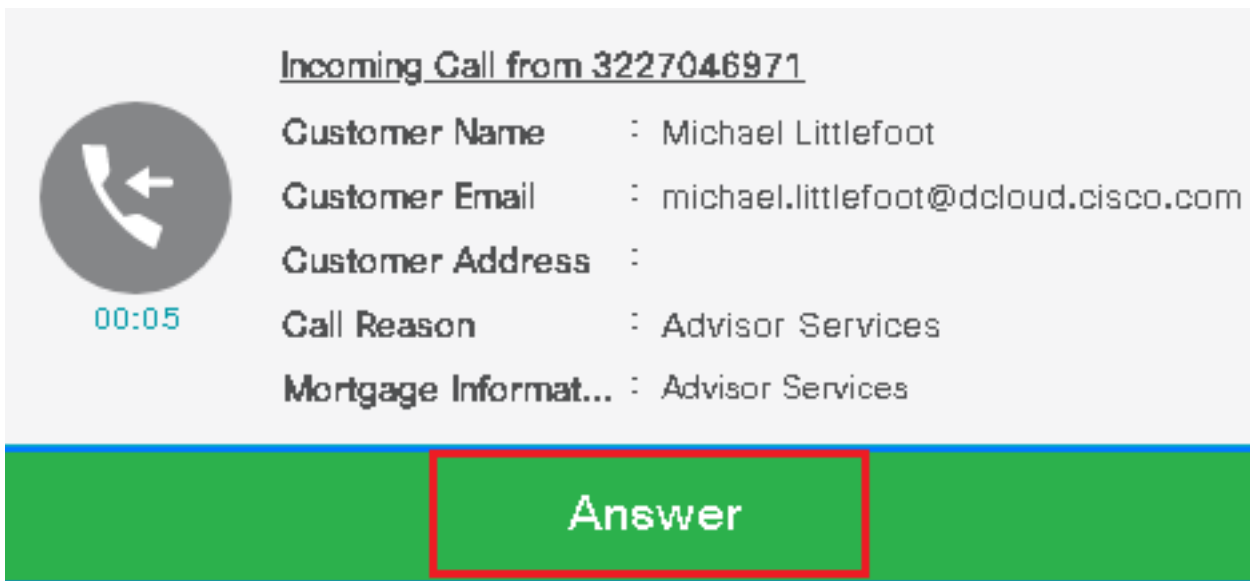
Prüfen: Wurde eine SIP-über-TLS-Verbindung mit dem CVP hergestellt? Falls ja, bestätigt der Ausgang, dass SIP-Signale zwischen CVP und CUBE gesichert sind.

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.



Incoming Call from 3227046971

Customer Name : Michael Littlefoot
Customer Email : michael.littlefoot@dcloud.cisco.com
Customer Address :
Call Reason : Advisor Services
Mortgage Informat... : Advisor Services

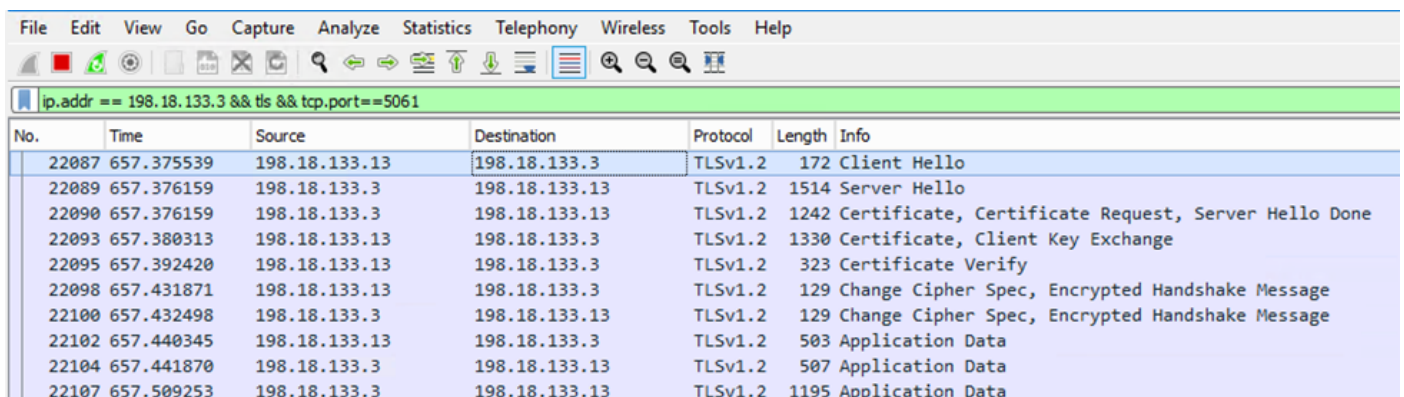
00:05

Answer

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`



No.	Time	Source	Destination	Protocol	Length	Info
22087	657.375539	198.18.133.13	198.18.133.3	TLSv1.2	172	Client Hello
22089	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1514	Server Hello
22090	657.376159	198.18.133.3	198.18.133.13	TLSv1.2	1242	Certificate, Certificate Request, Server Hello Done
22093	657.380313	198.18.133.13	198.18.133.3	TLSv1.2	1330	Certificate, Client Key Exchange
22095	657.392420	198.18.133.13	198.18.133.3	TLSv1.2	323	Certificate Verify
22098	657.431871	198.18.133.13	198.18.133.3	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22100	657.432498	198.18.133.3	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
22102	657.440345	198.18.133.13	198.18.133.3	TLSv1.2	503	Application Data
22104	657.441870	198.18.133.3	198.18.133.13	TLSv1.2	507	Application Data
22107	657.509253	198.18.133.3	198.18.133.13	TLSv1.2	1195	Application Data

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.