

Konfigurieren von sicherem RTP in Contact Center Enterprise

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

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

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

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

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

[CUCM-Sicherheitsmodus auf "Gemischt" setzen](#)

[Konfigurieren von SIP-Trunk-Sicherheitsprofilen für CUBE und CVP](#)

[Zuordnen von SIP-Trunk-Sicherheitsprofilen zu den entsprechenden SIP-Trunks und Aktivieren von SRTP](#)

[Sichere Gerätekommunikation der Agenten mit CUCM](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie der SRTP-Datenverkehr (Real-time Transport Protocol) in Contact Center Enterprise (CCE) abgesichert 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) Call Server, Cisco Virtual Voice Browser (CVVB) 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

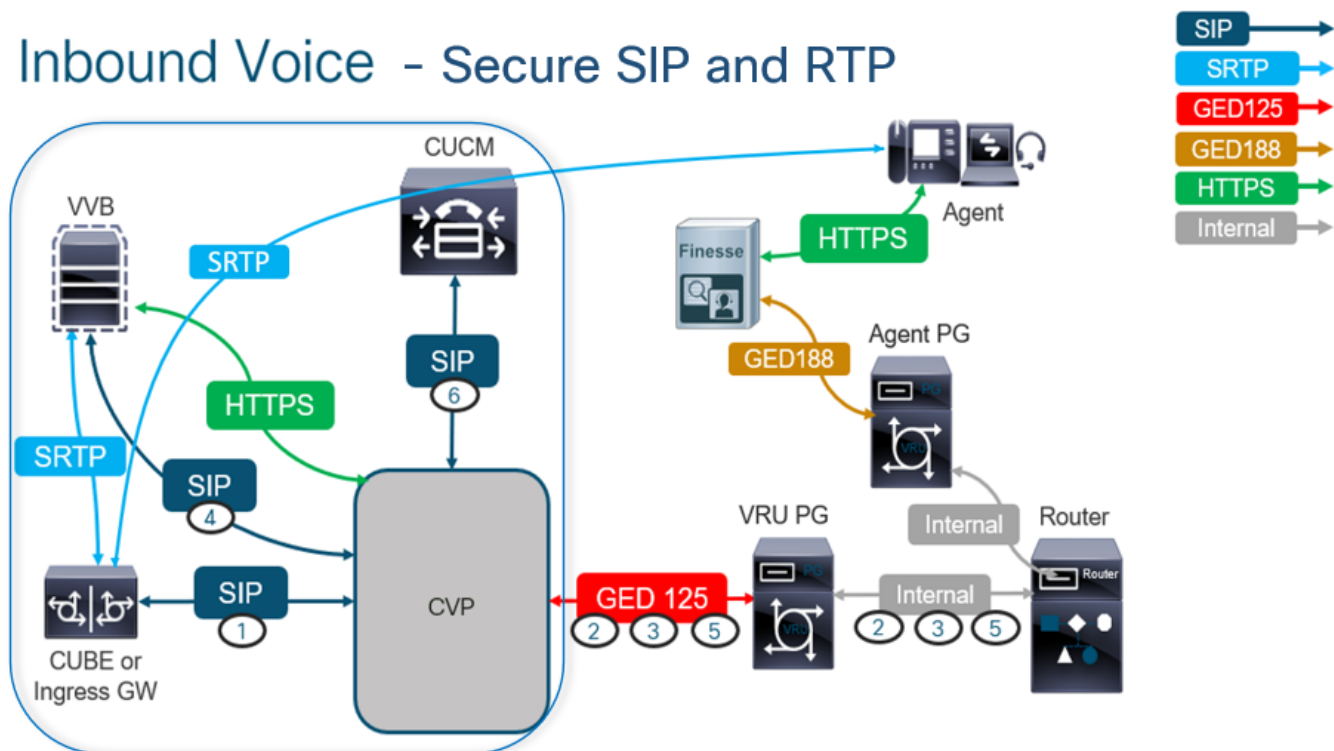
Die Informationen in diesem Dokument basieren auf Package Contact Center Enterprise (PCCE), CVP, CVVB und CUCM Version 12.6, gelten jedoch auch für die Vorgängerversionen.

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

Hinweis: Im Contact Center ist ein umfassender Anruffluss erforderlich. Um sicheres RTP zu aktivieren, müssen sichere SIP-Signale aktiviert sein. Aus diesem Grund ermöglichen die Konfigurationen in diesem Dokument sowohl sicheres SIP als auch SRTP.

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



Schritt 1: Sichere CUBE-Konfiguration

Bei dieser Aufgabe konfigurieren Sie CUBE zum Sichern von SIP-Protokollnachrichten und RTP.

Erforderliche Konfigurationen:

- Konfigurieren eines Standard-Vertrauenspunkts für SIP UA
- Ändern der DFÜ-Peers zur Verwendung von TLS und SRTP

Schritte:

1. Öffnen einer SSH-Sitzung für CUBE
2. Führen Sie diese Befehle aus, damit der SIP-Stack das CA-Zertifikat 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 CVP weiterzuleiten:

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

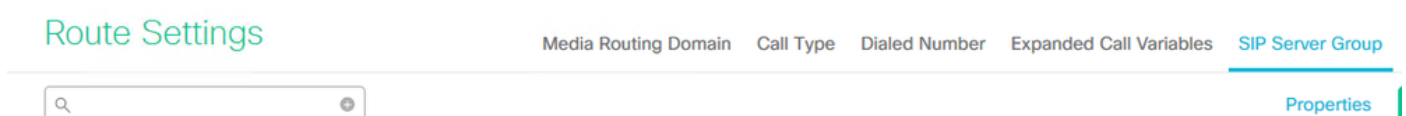
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line. End with CNTL/Z.
CC-VCUBE (config) #dial-peer voice 6000 voip
CC-VCUBE (config-dial-peer) #session target ipv4:198.18.133.13:5061
CC-VCUBE (config-dial-peer) #session transport tcp tls
CC-VCUBE (config-dial-peer) #SRTP
CC-VCUBE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

Schritt 2: Sichere CVP-Konfiguration

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

Schritte:

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



Basierend auf Ihren Konfigurationen haben Sie SIP-Servergruppen für CUCM, CVVB und CUBE 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` um die Details der SIP-Servergruppenkonfigurationen anzuzeigen. Festlegen `SecurePort` zu `5061` und klicke auf `Save`.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups** [Routing Pattern](#)

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` Registerkarte, legen Sie `SecurePort` zu `5061` und klicke auf `Save`.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups**

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

Schritt 3: Sichere CVVB-Konfiguration

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

Schritte:

1. Öffnen Sie `Cisco VVB Admin` Seite.
2. Navigieren Sie zu `System > System Parameters`.



Cisco Virtualized Voice Browser Administration

For Cisco Unified Communications Solutions

System Applications Subsystems Tools Help

System Parameters

Logout

Cisco Virtualized Voice Browser Administration

System version: 12.5.1.10000-24

3. Auf dem Security Parameters Abschnitt auswählen Enable für TLS (SIP) . Behalten Sie Supported TLS(SIP) version as TLSv1.2 und wählen Enable für SRTP.

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 <small>[Crypto Suite : AES_CM_128_HMAC_SHA1_32]</small>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

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

The screenshot shows the 'System Parameters Configuration' page with an 'Update' button. A dialog box is displayed over the page, containing the text: 'vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect.' and an 'OK' button.

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

The screenshot shows the navigation menu with the following items: Cisco VVB Administration, Cisco VVB Administration, Cisco Unified Serviceability, Cisco VVB Serviceability (highlighted), and Cisco Unified OS Administration. A 'Go' button is visible next to the first item.

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

The screenshot shows the 'Tools' menu with the following items: Control Center - Network Services and Performance Configuration and Logging.

7. Auswählen Engine und klicke auf Restart.

Control Center - Network Services

The screenshot shows the 'Control Center - Network Services' interface. At the top, there are four buttons: 'Start', 'Stop', 'Restart', and 'Refresh'. The 'Restart' button is highlighted with a red box. Below the buttons, the status is 'Ready' with an information icon. The 'Select Server' section shows 'Server *' with the value 'vvb1'. The 'System Services' section is a table with the following rows:

	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

Schritt 4: Sichere CUCM-Konfiguration

Um SIP-Nachrichten und RTP auf dem CUCM zu sichern, führen Sie die folgenden Konfigurationen durch:

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

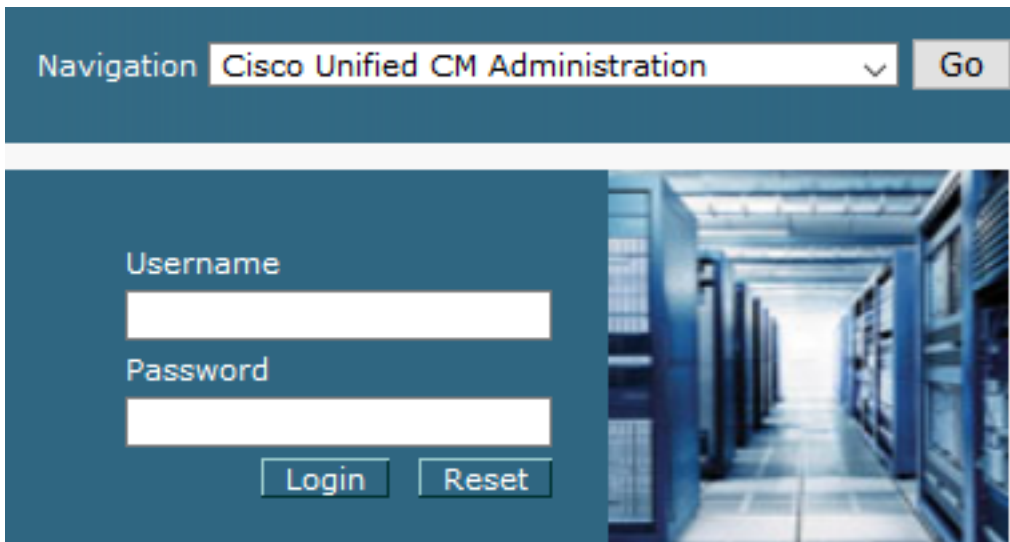
CUCM-Sicherheitsmodus auf "Gemischt" setzen

CUCM unterstützt zwei Sicherheitsmodi:

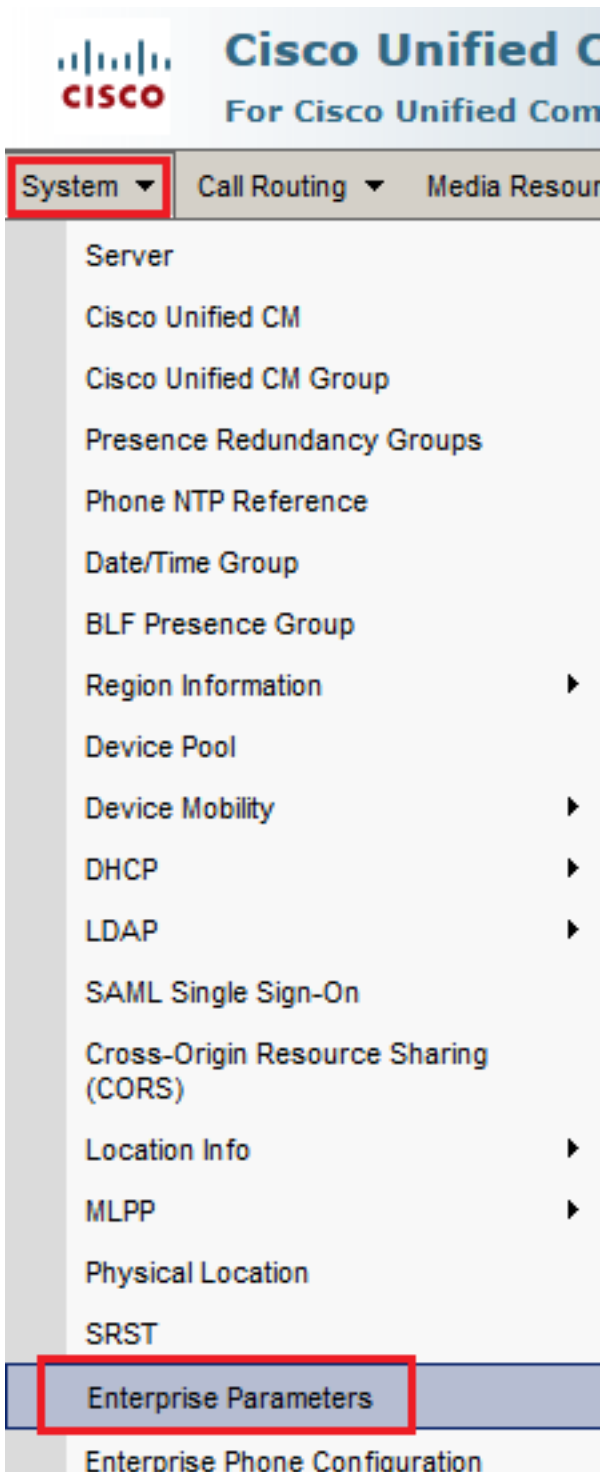
- Nicht sicherer Modus (Standardmodus)
- Gemischter Modus (sicherer Modus)

Schritte:

1. Melden Sie sich bei der CUCM-Verwaltungsschnittstelle an.



2. Wenn Sie sich beim CUCM anmelden, können Sie zu **System > Enterprise Parameters**.



3. Im Security Parameters Abschnitt überprüfen, ob die 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.

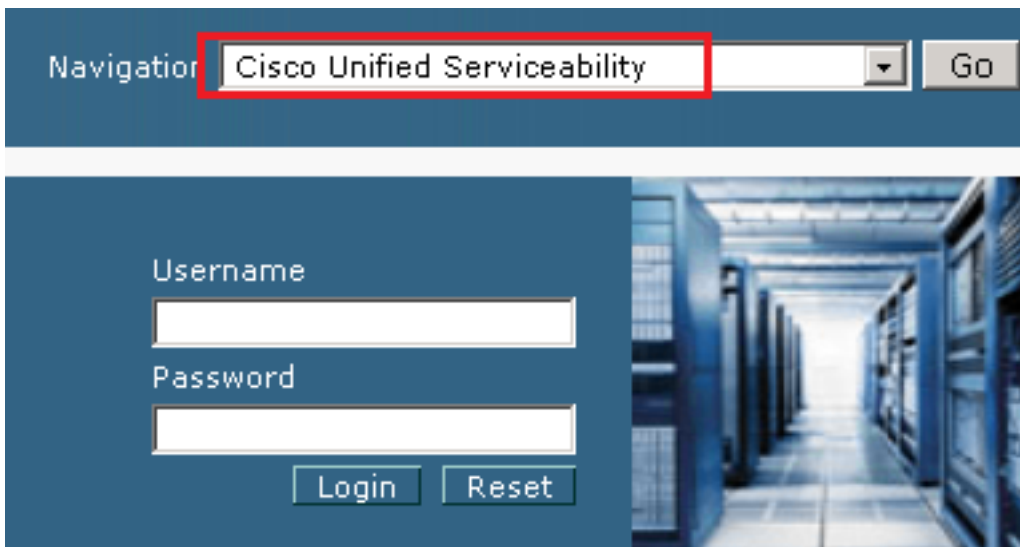
6. Nach erfolgreicher Anmeldung bei CUCM über SSH führen Sie den folgenden Befehl aus:

utils ctl set-cluster mixed-mode

7. Typ `y` und klicke auf `Enter` auf Aufforderung hin. 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. Damit die Änderungen wirksam werden, starten Sie das Cisco CallManager und Cisco CTIManager services.
9. Um die Dienste neu zu starten, navigieren Sie zu `Tools > Control Center – Feature Services`, 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 dann auf Go.

Select Server

Server*

12. Wählen Sie unterhalb der CM-Services die Cisco CallManager, und klicken Sie dann auf 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 dem 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.



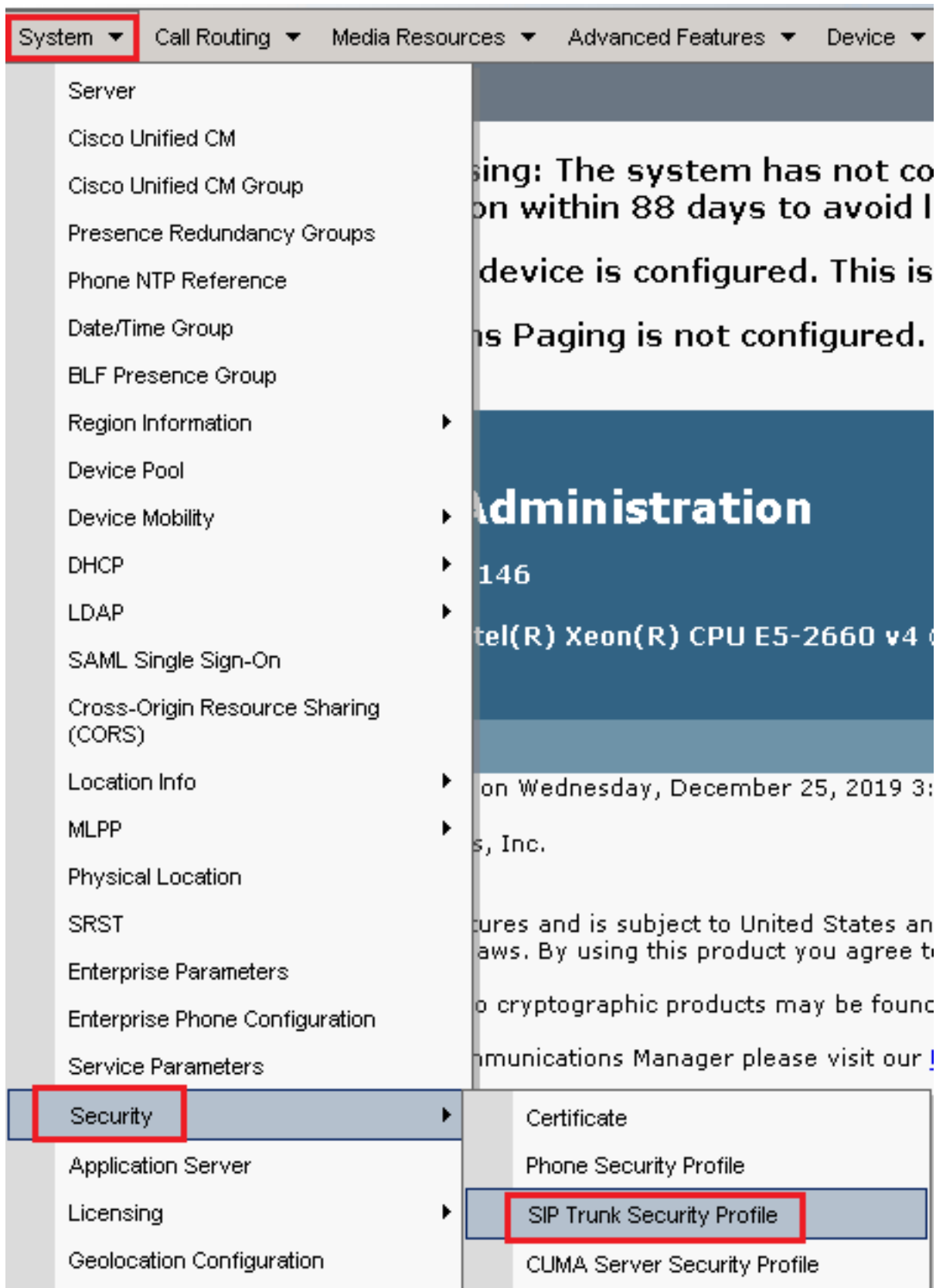
16. Wenn die Dienste erfolgreich neu gestartet wurden, müssen Sie, um zu überprüfen, ob der Cluster-Sicherheitsmodus auf den gemischten Modus gesetzt ist, zur CUCM-Verwaltung navigieren, wie in Schritt 5 beschrieben, und dann die **Cluster Security Mode**. Jetzt muss sie auf **1**.

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

Konfigurieren von SIP-Trunk-Sicherheitsprofilen für CUBE und CVP

Schritte:

1. Melden Sie sich bei der CUCM-Verwaltungsschnittstelle an.
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 (Neu hinzufügen)**, 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 um dieses Bild anzuzeigen, und klicken Sie dann auf Save unten links auf der Seite.

SIP Trunk Security Profile Configuration

Related Links: [Back](#)

 Save  Delete  Copy  Reset  Apply Config  Add New

- Status -

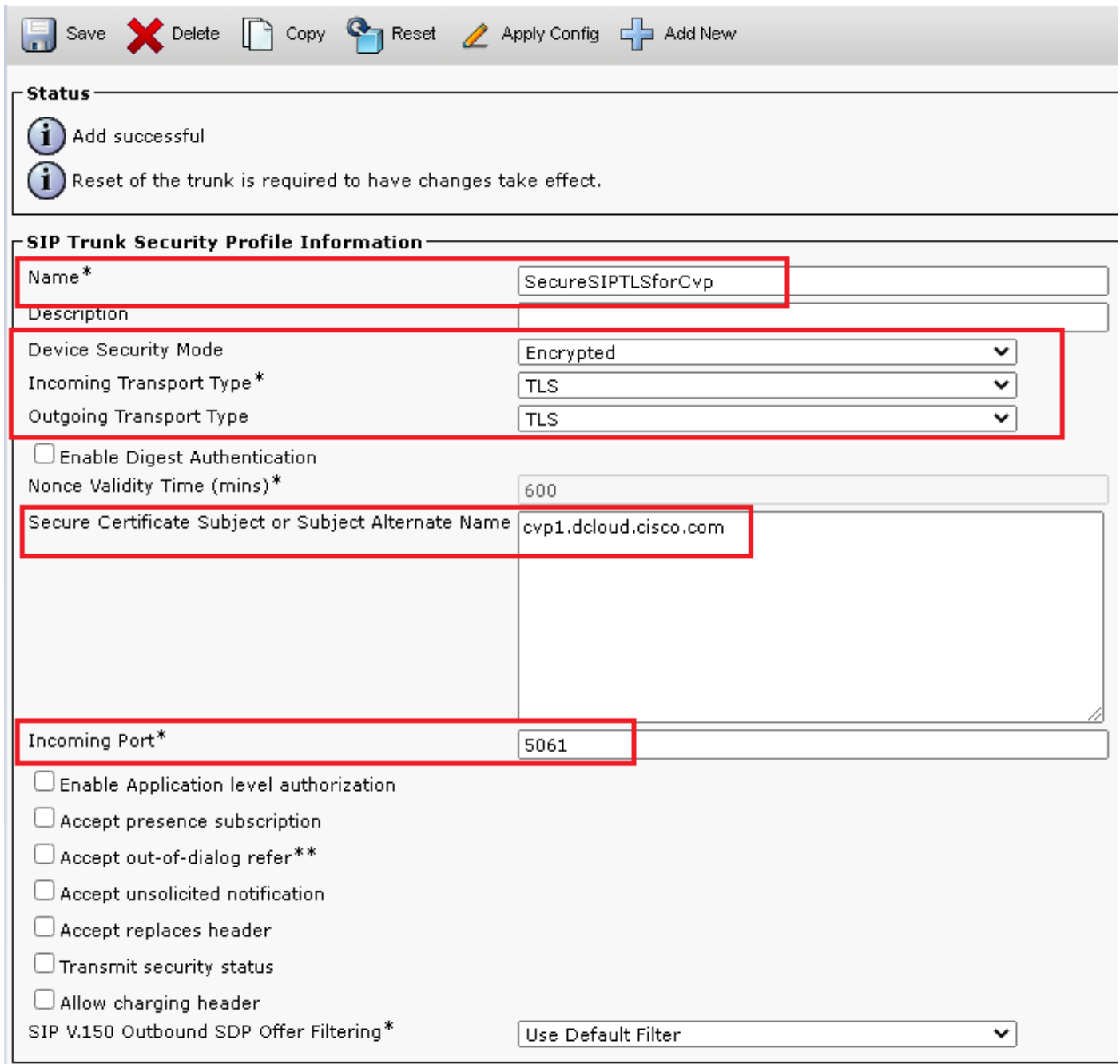
-  Add successful
-  Reset of the trunk is required to have changes take effect.

- 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**. **Ändern** **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*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

Secure Certificate Subject or Subject Alternate Name

Incoming Port*

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

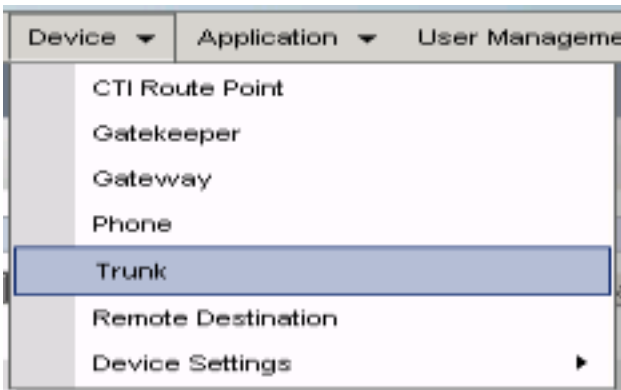
Allow charging header

SIP V.150 Outbound SDP Offer Filtering*

Zuordnen von SIP-Trunk-Sicherheitsprofilen zu den entsprechenden SIP-Trunks und Aktivieren von SRTP

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 , und klicken Sie dann 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. In Device Information Abschnitt überprüfen, SRTP Allowed Kontrollkästchen, um SRTP zu aktivieren.

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information. Consider Traffic on This Trunk Secure*

When using both sRTP and TLS

Route Class Signaling Enabled* Default

Use Trusted Relay Point* Default

5. Blättern Sie nach unten zum SIP Information und ändern Sie den Destination Port ZU 5061.

6. Ändern SIP Trunk Security Profile ZU SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1* Destination Address 198.18.133.226 Destination Address IPv6 Destination Port 5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* SecureSIPTLSforCube


Rerouting Calling Search Space < None >

7. Klicken Sie auf Save dann Rest zu 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

8. Navigieren Sie zu **Device > Trunk**, suchen Sie in diesem Beispiel nach CVP-Trunk-Name: **cvp-SIP-Trunk**. Klicken Sie auf **Find**.

Trunks (1 - 1 of 1)				
Find Trunks where				
<input type="checkbox"/>	Device Name	begins with	cvp	Find
Clear Filter  				
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

9. Klicken Sie auf **CVP-SIP-Trunk**, um die Konfigurationsseite des CVP-Trunks zu öffnen.
10. In **Device Information** Abschnitt, überprüfen **SRTP Allowed** Kontrollkästchen, um SRTP zu aktivieren.

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
Consider Traffic on This Trunk Secure*

Route Class Signaling Enabled*

Use Trusted Relay Point*

11. Blättern Sie nach unten zum **SIP Information** Abschnitt ändern, **Destination Port** zu **5061**.
12. Ändern **SIP Trunk Security Profile** zu **SecureSIPTLSForCvp**.

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text" value="198.18.133.13"/>	<input type="text"/>	<input type="text" value="5061"/>

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

13. Klicken Sie auf **save** dann **Rest** zu **save** und Änderungen anwenden.

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.

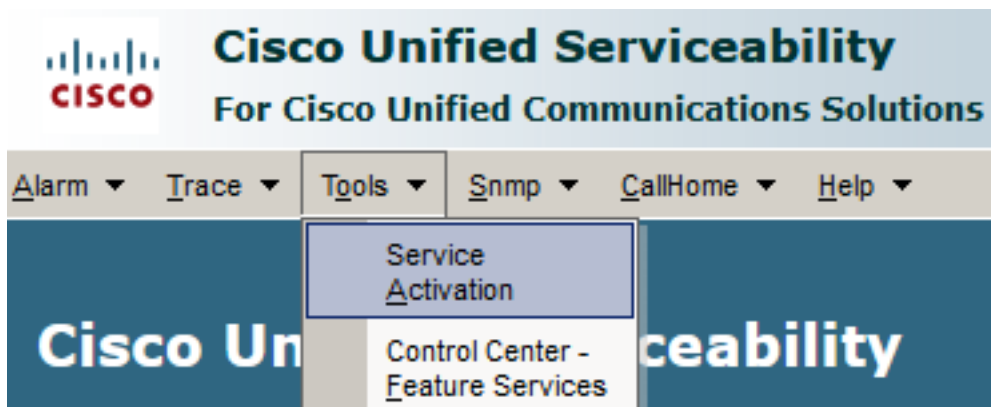
OK

Sichere Gerätekommunikation der Agenten mit CUCM

Um Sicherheitsfunktionen für ein Gerät zu aktivieren, müssen Sie ein LSC (Locally Significant Certificate) installieren und das Sicherheitsprofil diesem Gerät zuweisen. Das LSC verfügt über den öffentlichen Schlüssel für den Endpunkt, der vom privaten CUCM-CAPF-Schlüssel signiert wird. Es ist nicht standardmäßig auf Telefonen installiert.

Schritte:

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



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

Service Activation

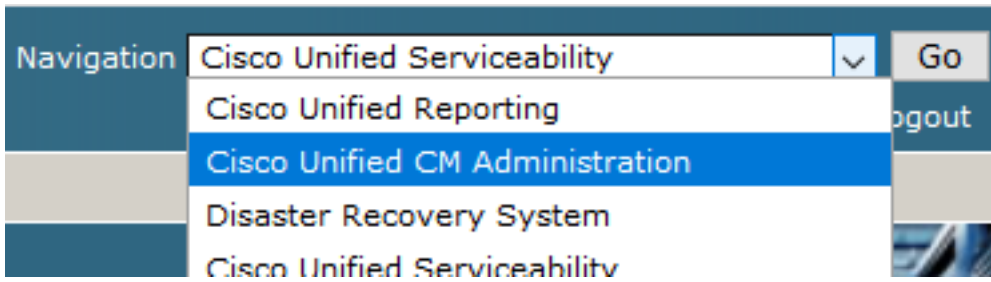
Select Server

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. Stellen Sie sicher, dass der Service aktiviert ist, und navigieren Sie dann zur CUCM-Verwaltung.



6. Navigieren Sie nach der erfolgreichen Anmeldung bei der CUCM-Verwaltung zu `System > Security > Phone Security Profile` um ein Gerätesicherheitsprofil für das Agentengerät zu erstellen.



Cisco Unified CM Administration

For Cisco Unified Communications Solutions

System ▾

Call Routing ▾

Media Resources ▾

Advanced Features ▾

Devi

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information ▶

Device Pool

Device Mobility ▶

DHCP ▶

LDAP ▶

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info ▶

MLPP ▶

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The
as Paging is not configur

Administration

7

tel(R) Xeon(R) CPU E5-2660

on Friday, December 20, 2019 10
s, Inc.

ures and is subject to United Stat
aws. By using this product you ac

o cryptographic products may be

munications Manager please visit


our [Technical Support](#) web site.

Certificate

Phone Security Profile

SIP Trunk Security Profile

CUMA Server Security Profile

7. Suchen Sie das Sicherheitsprofil 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 das Kopiersymbol  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 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*
 Description
 Device Security Mode
 Transport Type*
 TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

Authentication Mode*
 Key Order*
 RSA Key Size (Bits)*
 EC Key Size (Bits)
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

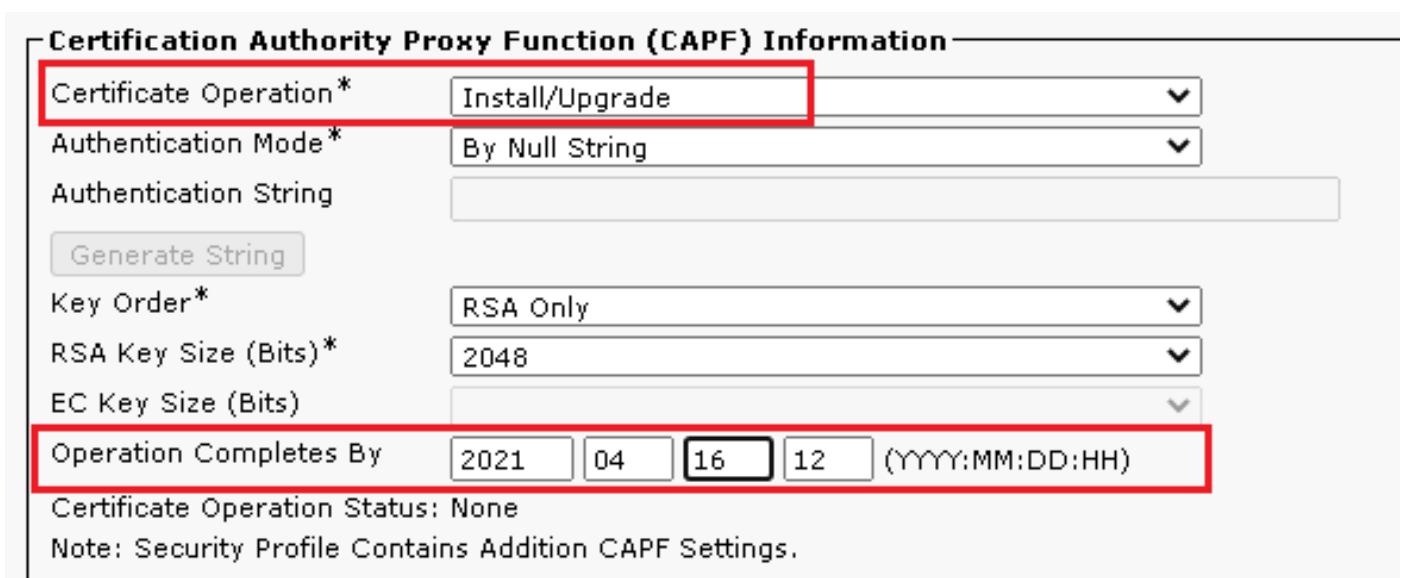
SIP Phone Port*

Save Delete Copy Reset Apply Config Add New

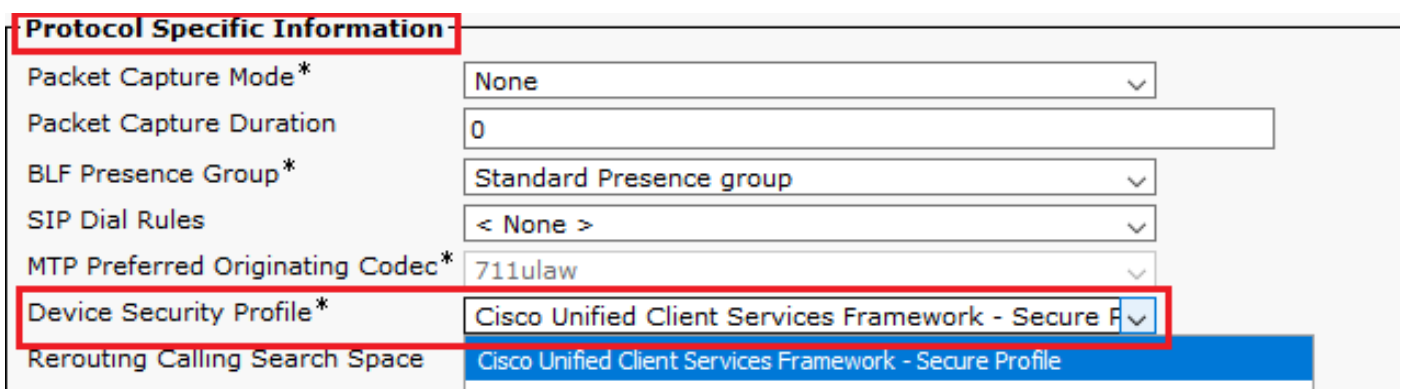
9. Navigieren Sie nach der erfolgreichen Erstellung des Telefongeräteprofils zu Device > Phone.



10. Klicken Sie auf Find um alle verfügbaren Telefone aufzulisten, und klicken Sie dann auf 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.

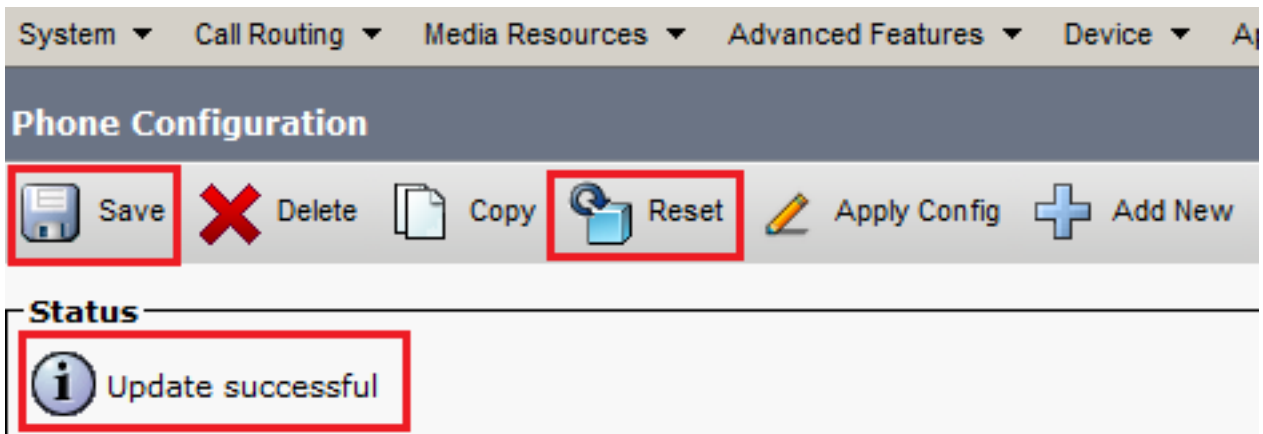


12. Suchen Protocol Specific Information Abschnitt und ändern Sie Device Security Profile zu Cisco Unified Client Services Framework – Secure Profile.

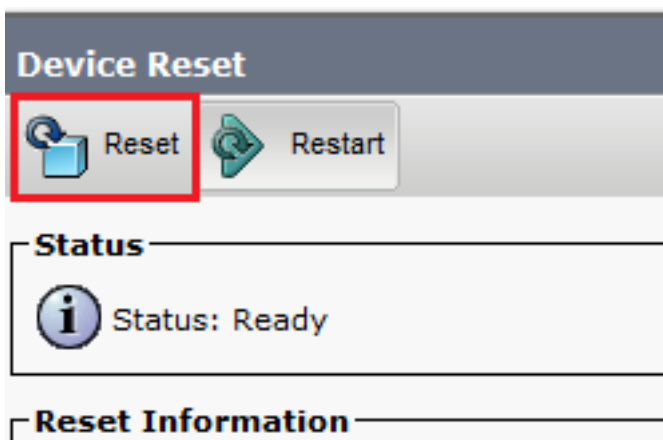


13. Klicken Sie auf save oben links auf der Seite. Stellen Sie sicher, dass die Änderungen

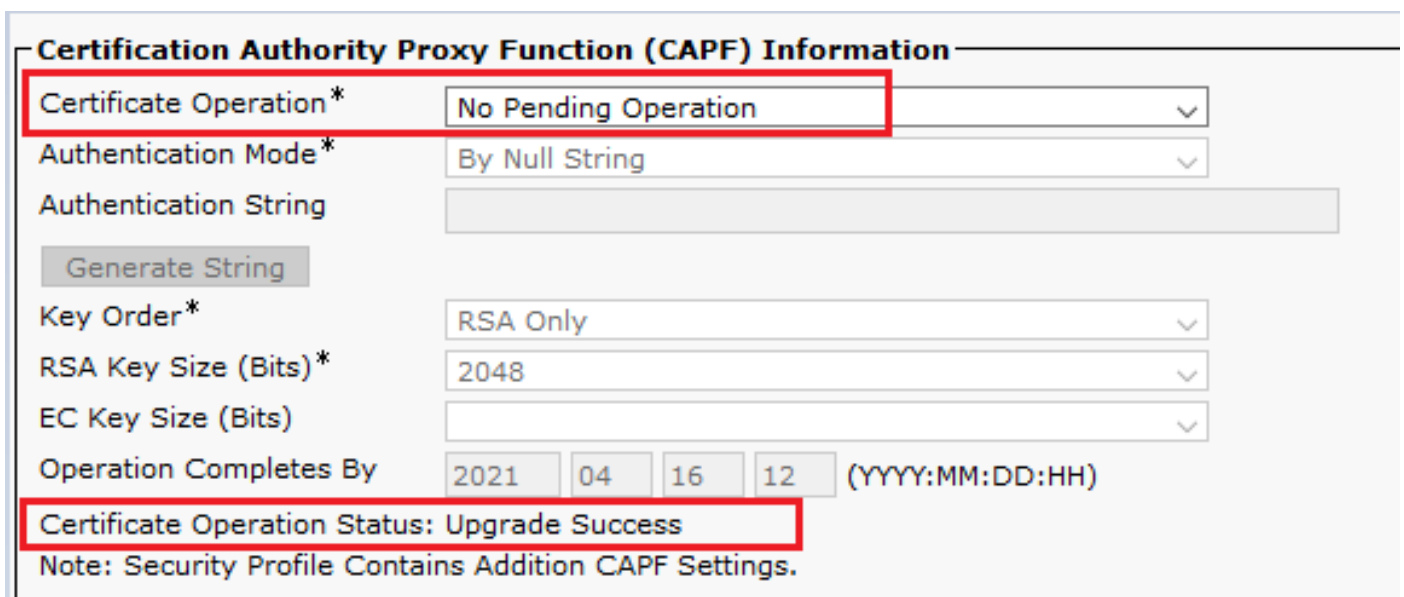
erfolgreich gespeichert wurden, und klicken Sie auf **Reset**.



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



16. Gehen Sie zu den gleichen Schritten wie in Schritt . 7 - 13 zum Sichern der Geräte anderer

Agenten, die Sie mit CUCM sicheres SIP und RTP verwenden möchten.

Überprüfung

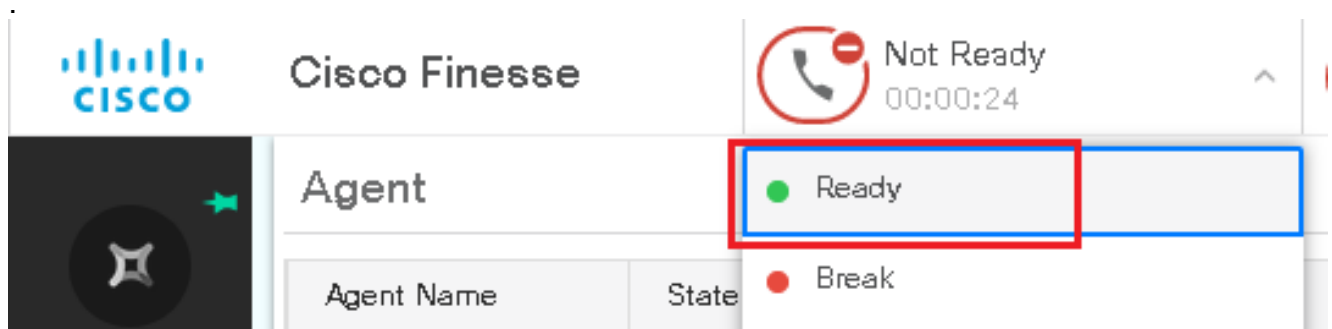
Führen Sie folgende Schritte durch, um zu überprüfen, ob das RTP ordnungsgemäß gesichert ist:

1. Führen Sie einen Testanruf beim Contact Center aus, und hören Sie sich die IVR-Aufforderung an.
2. Öffnen Sie gleichzeitig die SSH-Sitzung zu vCUBE, und führen Sie den folgenden Befehl aus:
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:674ECD1639ED7A710000ABF910000178
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.143:25346 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:674ECD1639ED7A710000ABF910000178
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Tipp: Überprüfen Sie, ob das SRTP on zwischen CUBE und VVB (198.18.133.143) Wenn dies der Fall ist, wird bestätigt, dass der RTP-Verkehr zwischen CUBE und VVB sicher ist.

3. Stellen Sie einen Mitarbeiter zur Verfügung, um den Anruf entgegenzunehmen.

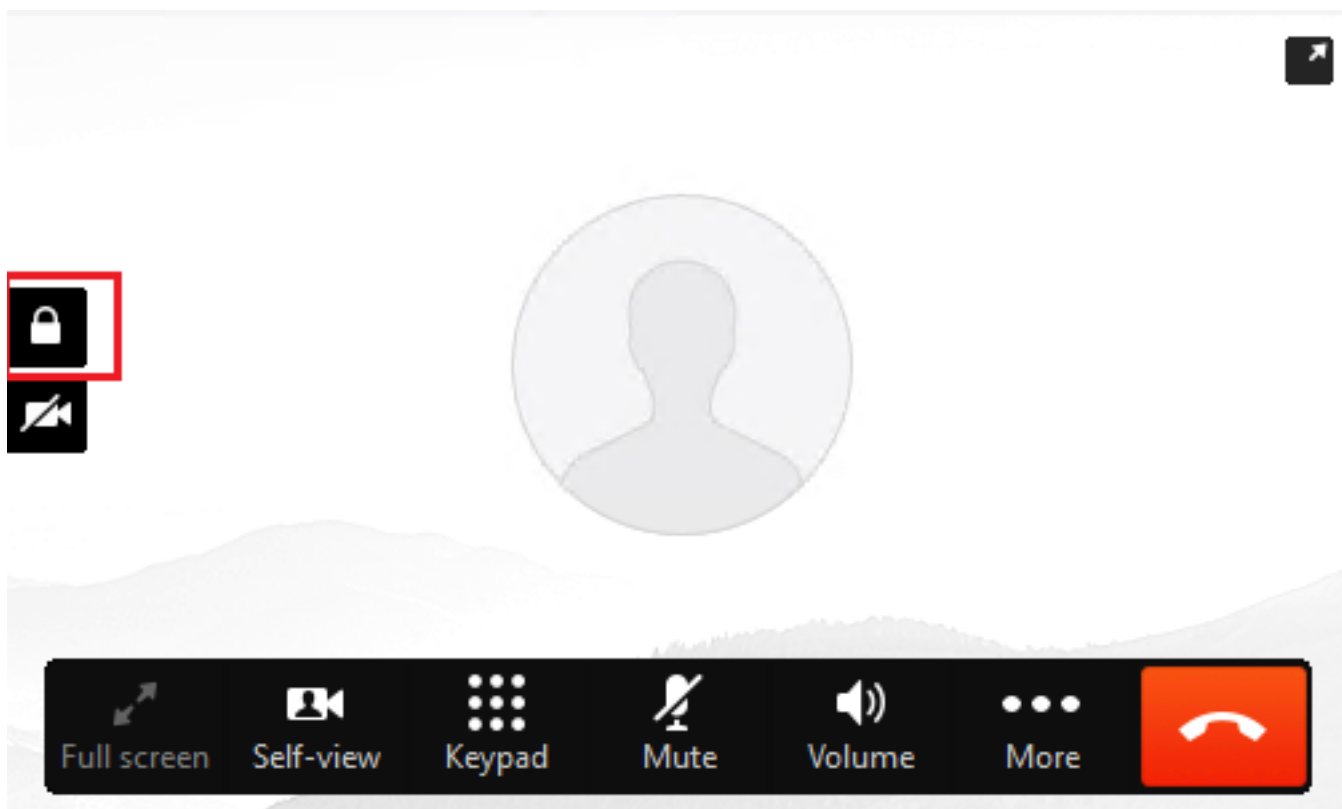


4. Der Agent wird reserviert, und der Anruf wird an den Agent weitergeleitet. Nehmen Sie den Anruf an.
5. Der Anruf wird mit dem Mitarbeiter verbunden. Kehren Sie zur vCUBE SSH-Sitzung zurück, und führen Sie den folgenden Befehl aus:
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:00003e7000105000a000005056a06cb8
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.75:24648 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:00003e7000105000a000005056a06cb8
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Tipp: Überprüfen Sie, ob das SRTP on zwischen CUBE und den Telefonen der Agenten (198.18.133.75). Wenn ja, wird bestätigt, dass der RTP-Verkehr zwischen CUBE und Agent sicher ist.

6. Sobald der Anruf verbunden ist, wird auf dem Agentengerät eine Sicherheitssperre angezeigt.. Dies bestätigt auch, dass der RTP-Verkehr sicher ist.



Weitere Informationen zum Überprüfen der ordnungsgemäßen Sicherung der SIP-Signale finden Sie im Artikel [Configure Secure SIP Signaling](#).

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.