

Sichere Integration zwischen CUCM und CUC konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Diagramm](#)

[Konfigurieren - Sicherer SIP-Trunk](#)

[Konfigurieren von CUC](#)

- [1. SIP-Zertifikat hinzufügen](#)
- [2. Neues Telefonsystem erstellen oder Standard ändern](#)
- [3. Neue Portgruppe hinzufügen](#)
- [4. Server bearbeiten](#)
- [5. Setzen Sie die Portgruppe zurück.](#)
- [6. Voicemail-Ports hinzufügen](#)
- [7. CUC-Stammzertifikat herunterladen](#)

[Konfigurieren von CUCM](#)

- [1. Konfigurieren des SIP-Trunk-Sicherheitsprofils für den Trunk zum CUC](#)
- [2. SIP-Profil konfigurieren](#)
- [3. SIP-Trunk erstellen](#)
- [4. Erstellen eines Routenmusters](#)
- [5. Pilotprogramm für Voicemail erstellen](#)
- [6. Voicemail-Profil erstellen](#)
- [7. Voicemail-Profil den DNS zuweisen](#)
- [8. CUC-Stammzertifikat als CallManager-trust hochladen](#)

[Konfigurieren sicherer SCCP-Ports](#)

[Konfigurieren von CUC](#)

- [1. CUC-Stammzertifikat herunterladen](#)
- [2. Erstellen Sie ein Telefonsystem, und ändern Sie das vorhandene System.](#)
- [3. Neue SCCP-Portgruppe hinzufügen](#)
- [4. Server bearbeiten](#)
- [5. Sichere SCCP-Ports hinzufügen](#)

[Konfigurieren von CUCM](#)

- [1. Ports hinzufügen](#)
- [2. CUC-Stammzertifikat als CallManager-trust hochladen](#)
- [3. Konfigurieren von MWI-Erweiterungen \(Message Waiting Information\)](#)
- [4. Voicemail-Pilot erstellen](#)
- [5. Voicemail-Profil erstellen](#)
- [6. Voicemail-Profil den DNS zuweisen](#)

[7. Erstellen einer Voicemail-Sammelgruppe](#)

[Überprüfen](#)

[Überprüfung der SCCP-Ports](#)

[Überprüfung sicherer SIP-Trunks](#)

[Überprüfung sicherer RTP-Anrufe](#)

[Fehlerbehebung](#)

[1. Allgemeine Tipps zur Fehlerbehebung](#)

[2. Zu sammelnde Ablaufverfolgungen](#)

[Häufige Probleme](#)

[Fall 1: Sichere Verbindung kann nicht hergestellt werden \(Warnung der unbekanntem Zertifizierungsstelle\)](#)

[Fall 2: CTL-Datei kann nicht vom CUCM TFTP heruntergeladen werden.](#)

[Fall 3: Ports sind nicht registriert](#)

[Fehler](#)

Einführung

Dieses Dokument beschreibt die Konfiguration, Verifizierung und Fehlerbehebung für die sichere Verbindung zwischen dem Cisco Unified Communication Manager (CUCM)- und dem Cisco Unity Connection (CUC)-Server.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse von CUCM verfügen.

Weitere Informationen finden Sie im [Cisco Unified Communications Manager Security Guide](#).

Hinweis: Sie muss auf den gemischten Modus gesetzt werden, damit die sichere Integration ordnungsgemäß funktioniert.

Verwendete Komponenten

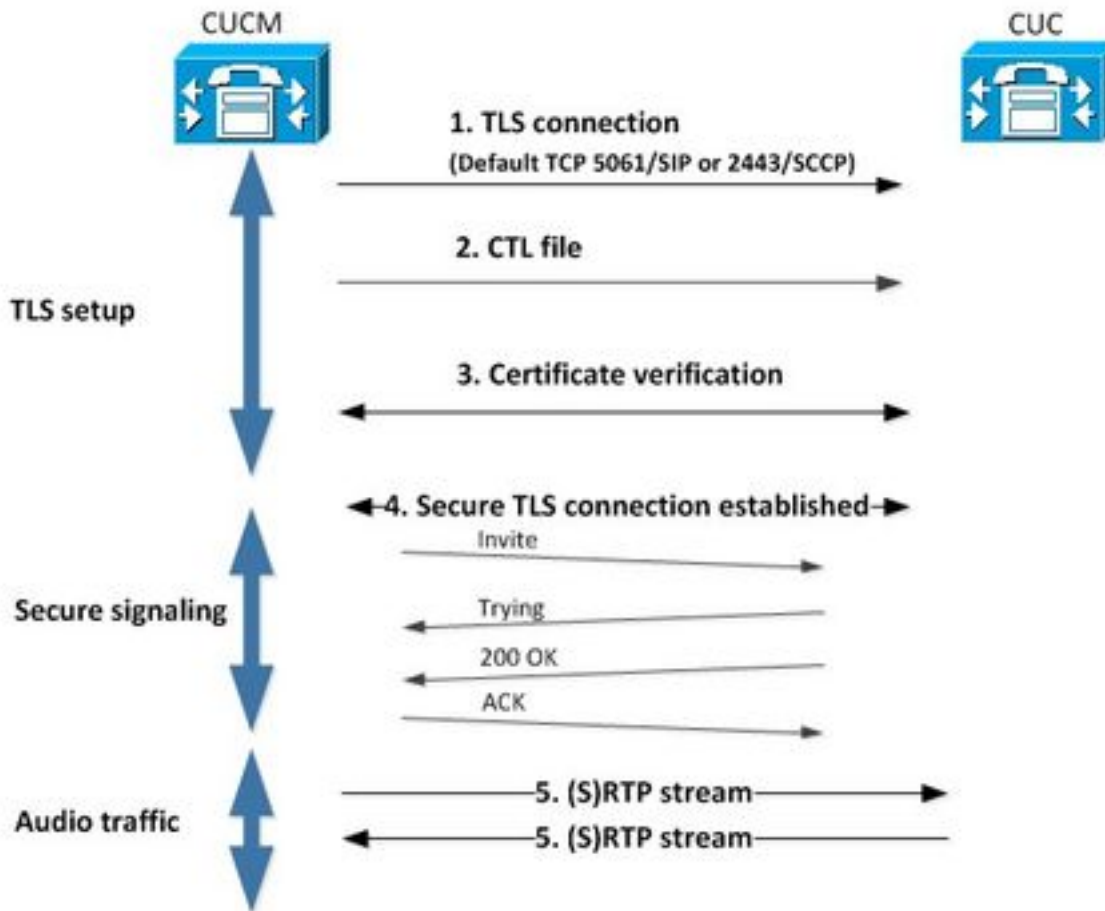
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CUCM-Version 10.5.2.11900-3.
- CUC-Version 10.5.2.11900-3.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Diagramm

In diesem Diagramm wird kurz erläutert, wie eine sichere Verbindung zwischen CUCM und CUC hergestellt werden kann:



1. Der Call Manager richtet eine sichere TLS-Verbindung (Transport Layer Security) zum CUC-Server ein, entweder über das Skinny Call Control Protocol (SCCP) des Ports 2443 oder über das SIP (Session Initiation Protocol) des 5061.
2. Der CUC-Server lädt die CTL-Datei (Certificate Trust List) vom TFTP-Server herunter (einmaliger Vorgang), extrahiert das CallManager.pem-Zertifikat und speichert es.
3. Der CUCM-Server bietet das Zertifikat "Callmanager.pem" an, das anhand des im vorherigen Schritt erhaltenen Zertifikats "CallManager.pem" verifiziert wird. Darüber hinaus wird das CUC-Zertifikat mit einem im CUCM gespeicherten CUC-Root-Zertifikat verifiziert. Beachten Sie, dass das Stammzertifikat vom Administrator in den CUCM hochgeladen werden muss.
4. Wenn die Überprüfung der Zertifikate erfolgreich ist, wird eine sichere TLS-Verbindung hergestellt. Diese Verbindung wird zum Austausch verschlüsselter SCCP- oder SIP-Signalisierung verwendet.
5. Audiodatenverkehr kann entweder als Real-Time Transport Protocol (RTP) oder SRTP ausgetauscht werden.

Hinweis: Wenn Sie eine TLS-Kommunikation einrichten, verwenden CUCM und CUC die gegenseitige TLS-Authentifizierung. Weitere Informationen finden Sie unter RFC5630.

Konfigurieren - Sicherer SIP-Trunk

Konfigurieren von CUC

1. SIP-Zertifikat hinzufügen

Navigieren Sie zu **CUC Administration > Telephony Integrations > Security > SIP Certificate > Add new**

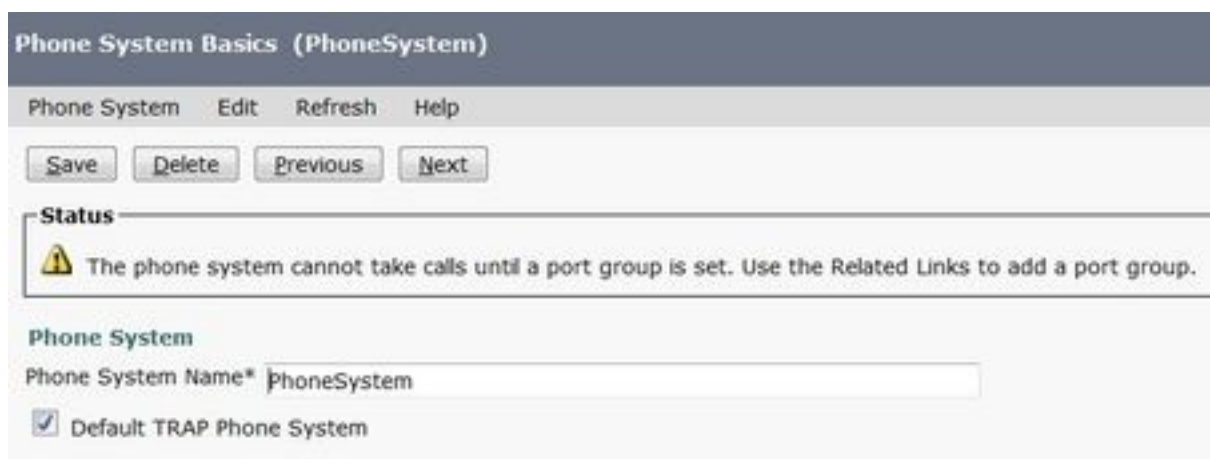
- Anzeigename: <beliebige aussagekräftige Namen>
- Betreffname: <jeder Name, z. B. **SecureConnection**>

Hinweis: Der Betreffname muss mit dem X.509-Betreffnamen im SIP-Trunk-Sicherheitsprofil übereinstimmen (konfiguriert in Schritt 1 der CUCM-Konfiguration weiter unten in diesem Dokument).

Hinweis: Das Zertifikat wird vom CUC-Root-Zertifikat generiert und signiert.

2. Neues Telefonsystem erstellen oder Standard ändern

Navigieren Sie zu **Telefonieintegration > Phone System (Telefonieintegration > Telefonsystem)**. Sie können das bereits vorhandene Telefonsystem verwenden oder ein neues System erstellen.



3. Neue Portgruppe hinzufügen

Wählen Sie auf der Seite Basics (Grundlagen der Telefonsysteme) im Dropdown-Feld Related Links (Zugehörige Links) die Option Add Port Group (Portgruppe hinzufügen) aus, und wählen Sie Go (Los) aus. Geben Sie im Konfigurationsfenster die folgenden Informationen ein:

- Telefonsystem:
- Erstellen von: Port-Gruppen-Typ SIP
- SIP Security Profile: 5061/TLS
- SIP-Zertifikat:
- Sicherheitsmodus: verschlüsselt
- Sicheres RTP: Checked
- IPv4-Adresse oder Hostname:

Drücken Sie Save.

4. Server bearbeiten

Navigieren Sie zu **Bearbeiten > Server**, und fügen Sie den TFTP-Server aus dem CUCM-Cluster hinzu, wie in diesem Bild gezeigt.

The image shows two configuration panels. The top panel is titled 'SIP Servers' and contains a table with one row: Order 0, IPv4 Address or Host Name 10.48.47.110. Below the table are 'Delete Selected' and 'Add' buttons. The bottom panel is titled 'TFTP Servers' and contains a table with one row: Order 0, IPv4 Address or Host Name 10.48.47.110. Below the table are 'Delete Selected' and 'Add' buttons.

Hinweis: Es ist wichtig, die richtige TFTP-Adresse anzugeben. Der CUC-Server lädt die CTL-Datei wie erläutert von diesem TFTP herunter.

5. Setzen Sie die Portgruppe zurück.

Gehen Sie zurück zu **Port Group Basics**, und setzen Sie die Portgruppe zurück, wie im Bild gezeigt.

6. Voicemail-Ports hinzufügen

Wählen Sie auf der Seite Basics (Grundlagen der Portgruppe) im Dropdown-Feld Related Links (Zugehörige Links) die Option **Add Ports (Ports hinzufügen) aus**, und wählen Sie **Go (Los)** aus. Geben Sie im Konfigurationsfenster die folgenden Informationen ein:

- Aktiviert: Aktiviert
- Anzahl der Ports:
- Telefonsystem:
- Portgruppe:
- Server:
- Portverhalten:

7. CUC-Stammzertifikat herunterladen

Navigieren Sie zu **Telefonieintegrationen > Sicherheit > Root Certificate**, klicken Sie mit der rechten Maustaste auf den URL, um das Zertifikat als Datei mit dem Namen <Dateiname>.0 zu speichern (die Dateierweiterung muss 0 sein, nicht .htm)", und drücken Sie die Eingabetaste, wie in diesem Bild gezeigt.



Konfigurieren von CUCM

1. Konfigurieren des SIP-Trunk-Sicherheitsprofils für den Trunk zum CUC

Navigieren Sie zu **CUCM Administration > System > Security > SIP Trunk Security Profile > Add new**

Stellen Sie sicher, dass diese Felder ausgefüllt sind:

- Gerätesicherheitsmodus: verschlüsselt
- X.509-Betreffname: SecureConnection>
- Hinweis zum Abmelden: Aktiviert
- Unerwünschte Benachrichtigung akzeptieren: Aktiviert
- Überschrift akzeptieren: aktiviert

Hinweis: Der X.509-Betreffname muss mit dem Betreffnamen im SIP-Zertifikat des Cisco Unity Connection-Servers übereinstimmen (konfiguriert in Schritt 1 der CUC-Konfiguration).

SIP Trunk Security Profile Information

Name*	Secure_sip_trunk_profile_for_CUC
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	SecureConnection
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" 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

2. SIP-Profil konfigurieren

Navigieren Sie zu **Gerät > Geräteeinstellungen > SIP-Profil**, wenn Sie bestimmte Einstellungen übernehmen möchten. Andernfalls können Sie das Standard-SIP-Profil verwenden.

3. SIP-Trunk erstellen

Gehen Sie zu **Gerät > Trunk > Neu hinzufügen**. Erstellen Sie einen SIP-Trunk, der für die sichere Integration in Unity Connection verwendet wird, wie in diesem Bild gezeigt.

Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Geben Sie im Abschnitt Device Information (Geräteinformationen) der Trunk-Konfiguration die folgenden Informationen ein:

- Geräteiname:
- Gerätepool:
- SRTP zugelassen: Checked

Hinweis: Stellen Sie sicher, dass die CallManager-Gruppe (in der Gerätepool-Konfiguration) alle im CUC konfigurierten Server enthält (**Portgruppe > Bearbeiten > Server**).

Geben Sie im Abschnitt "Eingehende Anrufe" der Trunk-Konfiguration folgende Informationen ein:

- Calling Search Space:
- Umleiten der Diversion Header Delivery - Inbound: Checked

The screenshot shows the 'Inbound Calls' configuration section. It includes several dropdown menus and a checkbox:

- Significant Digits*: All
- Connected Line ID Presentation*: Default
- Connected Name Presentation*: Default
- Calling Search Space: AllPhones
- AAR Calling Search Space: < None >
- Prefix DN: (empty text box)
- Redirecting Diversion Header Delivery - Inbound

In Oubound Ruft den Abschnitt der Trunk-Konfiguration auf, geben Sie die folgenden Informationen ein:

- Umleiten der Diversion Header-Bereitstellung - Ausgehend: Aktiviert

The screenshot shows the 'Outbound Calls' configuration section. It includes several dropdown menus and checkboxes:

- Called Party Transformation CSS: < None >
- Use Device Pool Called Party Transformation CSS
- Calling Party Transformation CSS: < None >
- Use Device Pool Calling Party Transformation CSS
- Calling Party Selection*: Originator
- Calling Line ID Presentation*: Default
- Calling Name Presentation*: Default
- Calling and Connected Party Info Format*: Deliver DN only in connected party
- Redirecting Diversion Header Delivery - Outbound
- Redirecting Party Transformation CSS: < None >
- Use Device Pool Redirecting Party Transformation CSS

Geben Sie im Abschnitt SIP Information (SIP-Informationen) der Trunk-Konfiguration folgende Informationen ein:

- Zieladresse:
- SIP-Trunk-Sicherheitsprofil:
- Calling Search Space wird umgeleitet:
- Dialogfeld "Out-of-Dialog" Siehe Calling Search Space:
- SIP-Profil:

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.48.47.124		5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Secure_sip_trunk_profile_for_CUC

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile [View Details](#)

DTMF Signaling Method* No Preference

Passen Sie andere Einstellungen an Ihre Anforderungen an.

4. Erstellen eines Routenmusters

Erstellen Sie ein Routenmuster, das auf den konfigurierten Trunk zeigt (**Anrufweiterleitung > Route/Hunt > Routenmuster**). Die als Weiterleitungsmuster-Nummer eingegebene Durchwahl kann als Voicemail-Pilot verwendet werden. Geben Sie folgende Informationen ein:

- Routenmuster:
- Gateway/Routenliste:

Route Pattern Configuration

Save

Status

Status: Ready

Pattern Definition

Route Pattern* 8000

Route Partition < None >

Description

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain < None >

Route Class* Default

Gateway/Route List* SecureSIPtoCUC [\(Edt\)](#)

Route Option

Route this pattern

Block this pattern No Error

5. Pilotprogramm für Voicemail erstellen

Erstellen Sie ein Voicemail-Pilot für die Integration (**Erweiterte Funktionen > Voicemail > Voicemail Pilot**). Geben Sie folgende Werte ein:

- Pilotnummer für Voicemail:

- Calling Search Space: Enthält Partitionen, die als Pilot verwendete Routingmuster enthalten>

Voice Mail Pilot Information	
Voice Mail Pilot Number	8000
Calling Search Space	< None >
Description	
<input type="checkbox"/> Make this the default Voice Mail Pilot for the system	

6. Voicemail-Profil erstellen

Erstellen Sie ein Voicemail-Profil, um alle Einstellungen miteinander zu verknüpfen (**Erweiterte Funktionen > Voicemail > Voicemail-Profil**). Geben Sie die folgenden Informationen ein:

- Voicemail-Pilot:
- Voicemail-Box-Maske:

Voice Mail Profile Information	
Voice Mail Profile Name*	Voicemail-profile-8000
Description	Secure Voicemail
Voice Mail Pilot**	8000/< None >
Voice Mail Box Mask	
<input type="checkbox"/> Make this the default Voice Mail Profile for the System	

7. Voicemail-Profil den DN's zuweisen

Weisen Sie das Voicemail-Profil den DN's zu, die eine sichere Integration verwenden sollen. Vergessen Sie nicht, nach dem Ändern der DN-Einstellungen auf die Schaltfläche "Config übernehmen" zu klicken:

Navigieren Sie zu: **Anrufweiterleitung > Verzeichnisnummer** und ändern Sie Folgendes:

- Voicemail Profile: Secure_SIP_Integration

8. CUC-Stammzertifikat als CallManager-trust hochladen

Navigieren Sie zu **OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** und laden Sie das CUC-Stammzertifikat als **CallManager-trust** auf alle Knoten hoch, die für die Kommunikation mit dem CUC-Server konfiguriert sind.

Hinweis: Der Cisco CallManager-Service muss nach dem Hochladen des Zertifikats neu gestartet werden, damit das Zertifikat wirksam wird.

Konfigurieren sicherer SCCP-Ports

Konfigurieren von CUC

1. CUC-Stammzertifikat herunterladen

Navigieren Sie zu **CUC Administration > Telephony Integration > Security > Root Certificate**. Klicken Sie mit der rechten Maustaste auf den URL, um das Zertifikat als Datei mit dem Namen <Dateiname>.0 (Dateierweiterung muss 0 und nicht HTM sein) zu speichern.', und klicken Sie auf **Speichern**:

Root Certificate for Cisco Unified Communications Manager Authentication and Encryption	
Subject	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Issuer	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Valid From	Tue Mar 31 08:59:34 CEST 2015
Valid Until	Fri Apr 01 08:59:34 CEST 2022
Version	2
File Name	57ed0e66.0
Serial Number	f6b8fb3369144dd39f18e064893aec42
Certificate Text	-----BEGIN CERTIFICATE----- MIICPDCCAaWgAwIBAgIRAPa4+zNpFE3TnxjgZ1k67E1wDQYJKoZIhvcNAQEFBQAw OjE4MDYGA1UEAwvQ2lzY29Vbml0eS01ZGFkMzJiY1jYWZlTQ1NTktOTc0ZD01 NmYyYzY4NTBkNDEwHhcNMTUwMzIxMDY1OTM0WWhcNMjIwNDUxOTM0WjA6MTgw NgYDVQDDC9DaxNjb1VuaXR5LTUyYzY2ZGFkMzJiY1jYWZlTQ1NTktOTc0ZD01 Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBOBg/qhBcWQx4S7 Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6euSeMiGbs757WpvtSpKp+ze5DjVm2j4 B1lxG9wM3XgPPwM+3QIMh0NQPLARuJdm9g2/SuiHB6/1k82Po0Wrv2r6Anoragrv MdJordaCB3mG1u2g0GqXj9GChf0CAwEAAaNCMEAwEgYDVR0TAQH/BAgwBgEB/wIB ADAdBgNVHQ4EFgQU438N5JYGHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAgKsMA0G CSqGS1b3DQEBBQUAA4GBAGPhrFt6GH2a0iXV8snKvC12f5t1eTeMD6ZzD62P4C6 RtGM8BWgqUIIAZw1www0nxdetKzZvJX2z2Ksu2ptVUnFPMzSc+xl0jv7vmJq52px Tcd/Ti0efckXlc+vACWlu4wlv20SHxsoto9CiiXqsKQ7o/zyYHu152zTOQeYvAES -----END CERTIFICATE-----
Private Key	Hk2Pzp3YnX3/9ghz1r8v1VgMp5Lr8HZ8XW/VXIL342IudK3G1GwnZ11MVhztq/zEseh2ELON

Right click to save the certificate as a file named 57ed0e66.0 (the file extension must be .0 rather than .htm)

- Open Link in New Tab
- Open Link in New Window
- Open Link in New Private Window
- Bookmark This Link
- Save Link As...
- Copy Link Location
- This Frame
- Inspect Element (Q)

2. Erstellen Sie ein Telefonsystem, und ändern Sie das vorhandene System.


Navigieren Sie zu **Telefonieintegration > Phone System**. Sie können das bereits vorhandene Telefonsystem verwenden oder ein neues System erstellen.

Phone System Basics (PhoneSystem)

Phone System Edit Refresh Help

Save Delete Previous Next

Status

 The phone system cannot take calls until a port group is set. Use the Related Links to add a port group.

Phone System

Phone System Name* PhoneSystem

Default TRAP Phone System


3. Neue SCCP-Portgruppe hinzufügen


Wählen Sie auf der Seite Basics (Grundlagen des Telefonsystems) im Dropdown-Feld Related Links (Zugehörige Links) die Option **Add Port Group (Portgruppe hinzufügen) aus**, und wählen Sie **Go (Los)** aus. Geben Sie im Konfigurationsfenster die folgenden Informationen ein:

- Telefonsystem:
- Portgruppentyp: SCCP
- Gerätename-Präfix*: CiscoUM1-VI
- MWI On-Erweiterung:
- MWI Off-Erweiterung:

Hinweis: Diese Konfiguration muss mit der CUCM-Konfiguration übereinstimmen.

Status

 The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

 Created Port Group(s)

Port Group

Display Name* Secure-SCCP-1

Integration Method SCCP (Skinny)

Device Name Prefix* CiscoUM1-VI

Reset Status Reset Not Required

Message Waiting Indicator Settings

Enable Message Waiting Indicators

MWI On Extension 999991

MWI Off Extension 999990

Delay between Requests 0 milliseconds

Maximum Concurrent Requests 0

Retries After Successful Attempt 0

Retry Interval After Successful Attempt 5 milliseconds

Save Delete Previous Next

Fields marked with an asterisk (*) are required.

4. Server bearbeiten

Navigieren Sie zu **Bearbeiten > Server**, und fügen Sie den TFTP-Server aus dem CUCM-Cluster hinzu.

The image shows two configuration panels. The top panel is titled 'SIP Servers' and contains a table with one row. The table has columns for a checkbox, 'Order', and 'IPv4 Address or Host Name'. The row contains a checked checkbox, the number '0', and the IP address '10.48.47.110'. Below the table are 'Delete Selected' and 'Add' buttons. The bottom panel is titled 'TFTP Servers' and contains a similar table with one row. The row contains a checked checkbox, the number '0', and the IP address '10.48.47.110'. Below the table are 'Delete Selected' and 'Add' buttons.

<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input checked="" type="checkbox"/>	0	10.48.47.110

<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input checked="" type="checkbox"/>	0	10.48.47.110


Hinweis: Es ist wichtig, die richtige TFTP-Adresse anzugeben. Der CUC-Server lädt die CTL-Datei wie erläutert von diesem TFTP herunter.

5. Sichere SCCP-Ports hinzufügen

Wählen Sie auf der Seite Basics (Grundlagen der Portgruppe) im Dropdown-Feld Related Links (Zugehörige Links) die Option **Add Ports (Ports hinzufügen) aus**, und wählen Sie **Go (Los) aus**. Geben Sie im Konfigurationsfenster die folgenden Informationen ein:

- Aktiviert: Aktiviert
- Anzahl der Ports:
- Telefonsystem:
- Portgruppe:
- Server:
- Portverhalten:
- Sicherheitsmodus: **verschlüsselt**

Status

 Because it has no port groups, PhoneSystem is not listed in the Phone system field.

New Phone System Port

Enabled

Number of Ports

Phone System

Port Group

Server

Port Behavior

Answer Calls

Perform Message Notification

Send MWI Requests (may also be disabled by the port group)

Allow TRAP Connections

Security Mode

Konfigurieren von CUCM

1. Ports hinzufügen

Navigieren zu **CUCM-Administration > Erweiterte Funktionen > Konfiguration des Voicemail-Ports > Neu hinzufügen**.

Konfigurieren Sie die SCCP-Voicemail-Ports wie gewohnt. Der einzige Unterschied besteht im Gerätesicherheitsmodus in der Portkonfiguration, in der die Option Verschlüsselter Voicemail-Port ausgewählt werden muss.

Voice Mail Port Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

Device Information

Registration: Registered with Cisco Unified Communications Manager 10.48.46.182
 IPv4 Address: 10.48.46.184
 Device is trusted
 Port Name* CiscoUM1-VI1
 Description VM-sccp-secure-ports
 Device Pool* Default
 Common Device Configuration < None >
 Calling Search Space < None >
 AAR Calling Search Space < None >
 Location* Hub_None
 Device Security Mode* Encrypted Voice Mail Port
 Use Trusted Relay Point* Default
 Geolocation < None >

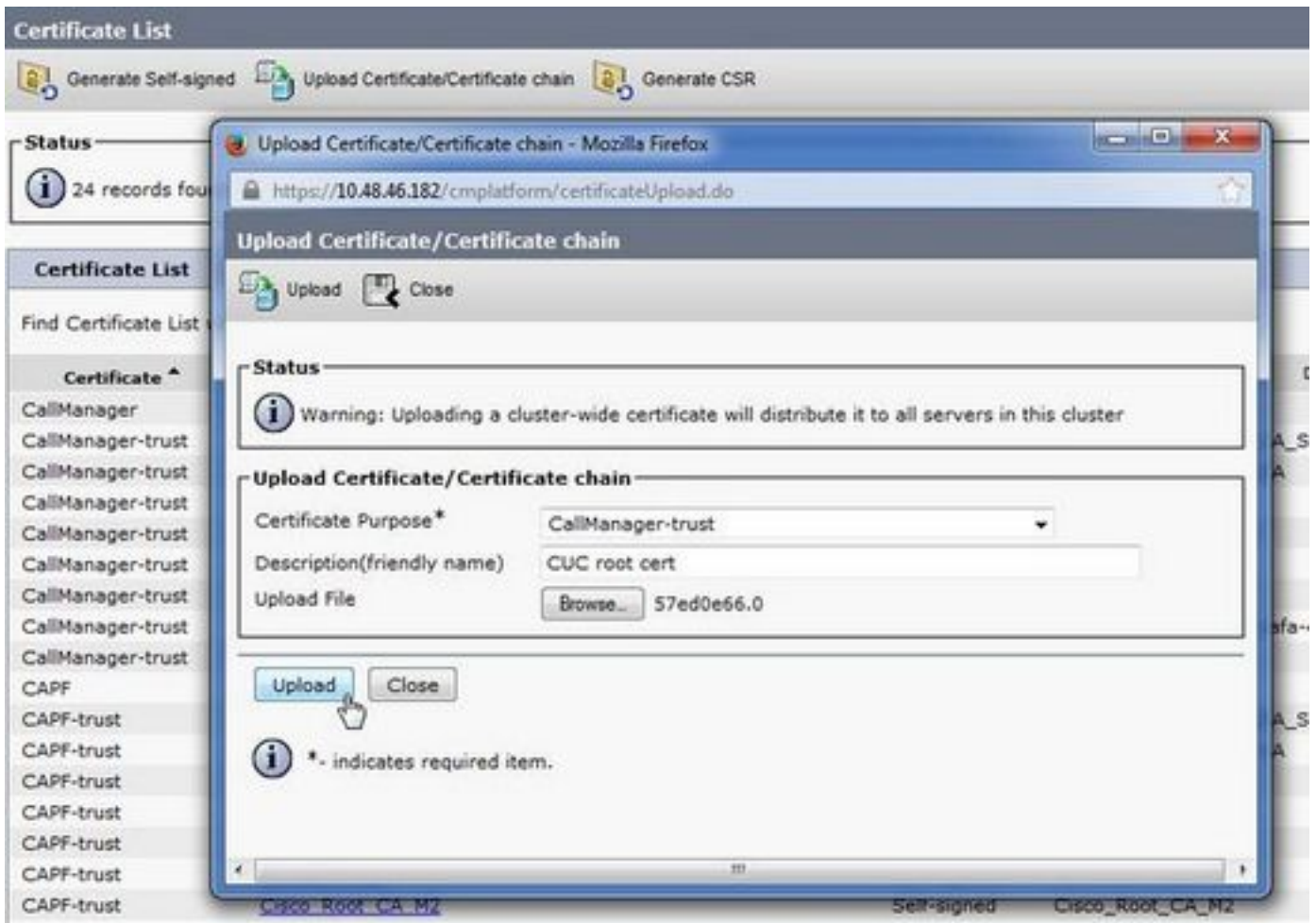
Directory Number Information

Directory Number* 999001
 Partition < None >
 Calling Search Space < None >
 AAR Group < None >
 Internal Caller ID Display VoiceMail
 Internal Caller ID Display (ASCII format) VoiceMail
 External Number Mask

Save Delete Copy Reset Apply Config Add New

2. CUC-Stammzertifikat als CallManager-trust hochladen

Navigieren Sie zu **OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** und laden Sie das CUC-Stammzertifikat als **CallManager-trust** auf alle Knoten hoch, die für die Kommunikation mit dem CUC-Server konfiguriert sind.



Hinweis: Der Cisco CallManager-Service muss nach dem Hochladen des Zertifikats neu gestartet werden, damit das Zertifikat wirksam wird.

3. Konfigurieren von MWI-Erweiterungen (Message Waiting Information)

Navigieren Sie zu **CUCM Administration > Advanced Features > Voicemail Port Configuration** und konfigurieren Sie **MWI On/Off Extensions**. Die MWI-Nummern müssen mit der CUC-Konfiguration übereinstimmen.

Message Waiting Information

Message Waiting Number*

Partition

Description

Message Waiting Indicator* On Off

Calling Search Space

Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* On Off

Calling Search Space < None >

Save

4. Voicemail-Pilot erstellen

Erstellen Sie ein Voicemail-Pilot für die Integration (**Erweiterte Funktionen > Voicemail > Voicemail Pilot**). Geben Sie folgende Werte ein:

- Pilotnummer für Voicemail:
- Calling Search Space: Enthält Partitionen, die als Pilot verwendete Routingmuster enthalten>

Voice Mail Pilot Information

Voice Mail Pilot Number 8000

Calling Search Space < None >

Description

Make this the default Voice Mail Pilot for the system

5. Voicemail-Profil erstellen

Erstellen Sie ein Voicemail-Profil, um alle Einstellungen miteinander zu verknüpfen (**Erweiterte Funktionen > Voicemail > Voicemail-Profil**). Geben Sie folgende Informationen ein:

- Voicemail-Pilot:
- Voicemail-Box-Maske:

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

Make this the default Voice Mail Profile for the System

6. Voicemail-Profil den DN's zuweisen

Weisen Sie das Voicemail-Profil den DN's zu, die eine sichere Integration verwenden möchten. Klicken Sie nach dem Ändern der Verzeichniseinstellungen auf **Config** anwenden:

Navigieren Sie zu **Anrufweiterleitung > Verzeichnisnummer**, und wechseln Sie zu:

- Voicemail Profile: Voicemail-Profil-8000

Directory Number Settings	
Voice Mail Profile	Voicemail-profile-8000 (Choose <None> to use system default)
Calling Search Space	< None >
BLF Presence Group*	Standard Presence group
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
<input type="checkbox"/> Reject Anonymous Calls	

7. Erstellen einer Voicemail-Sammelgruppe

a) Hinzufügen einer neuen **Leitungsgruppe** (Anrufweiterleitung > Route/Hunt > Line Group)

- Line Group Information	
Line Group Name*	voicemail-ig
RNA Reversion Timeout*	10
Distribution Algorithm*	Longest Idle Time

b) Hinzufügen einer neuen **Sammelanschlussliste** für Voicemail (Anrufweiterleitung > Route/Hunt > Sammelanschlussliste)

Hunt List Information	
<input checked="" type="checkbox"/> Device is trusted	
Name*	voicemail-hl
Description	
Cisco Unified Communications Manager Group*	Default
<input checked="" type="checkbox"/> Enable this Hunt List (change effective on Save; no reset required)	
<input checked="" type="checkbox"/> For Voice Mail Usage	

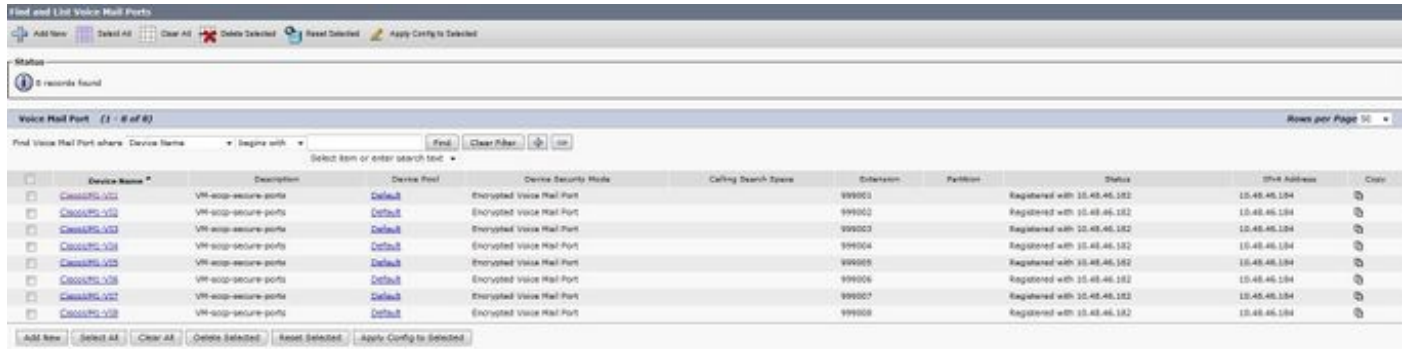
c) Hinzufügen eines neuen **Hunt-Pilotprogramms** (Anrufweiterleitung > Route/Hunt > Hunt Pilot)

Pattern Definition	
Hunt Pilot*	8000
Route Partition	< None >
Description	
Numbering Plan	< None >
Route Filter	< None >
MLPP Precedence*	Default
Hunt List*	voicemail-hl (Edit)
Call Pickup Group	< None >
Alerting Name	
ASCII Alerting Name	
Route Option	<input checked="" type="radio"/> Route this pattern
	<input type="radio"/> Block this pattern No Error

Überprüfen

Überprüfung der SCCP-Ports

Navigieren Sie zu **CUCM Administration > Advance Features > Voicemail > Voicemail Ports**, und überprüfen Sie die Port-Registrierung.



Device Name	Description	Device Pool	Device Security Mode	Calling Search Space	Extension	Partition	Status	IP Address	Class
CiscoPS-102	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999001		Registered with 10.45.46.182	10.45.46.184	
CiscoPS-103	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999002		Registered with 10.45.46.182	10.45.46.184	
CiscoPS-104	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999003		Registered with 10.45.46.182	10.45.46.184	
CiscoPS-105	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999004		Registered with 10.45.46.182	10.45.46.184	
CiscoPS-106	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999005		Registered with 10.45.46.182	10.45.46.184	
CiscoPS-107	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999006		Registered with 10.45.46.182	10.45.46.184	
CiscoPS-108	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999007		Registered with 10.45.46.182	10.45.46.184	
CiscoPS-109	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999008		Registered with 10.45.46.182	10.45.46.184	

Drücken Sie die **Voicemail**-Taste am Telefon, um Voicemail-Nachrichten anzurufen. Sie sollten die Begrüßung hören, wenn die Durchwahl des Benutzers nicht auf dem Unity Connection-System konfiguriert ist.

Überprüfung sicherer SIP-Trunks

Drücken Sie die **Voicemail**-Taste am Telefon, um Voicemail-Nachrichten anzurufen. Sie sollten die Begrüßung hören, wenn die Durchwahl des Benutzers nicht im Unity Connection-System konfiguriert ist.

Alternativ können Sie die Keepalive-Funktion von SIP OPTIONS aktivieren, um den SIP-Trunk-Status zu überwachen. Diese Option kann im SIP-Profil aktiviert werden, das dem SIP-Trunk zugewiesen ist. Wenn diese Funktion aktiviert ist, können Sie den SIP-Trunk-Status über **Gerät > Trunk** überwachen, wie in diesem Bild gezeigt.



Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
SecureSIPtoCUC			Default					SIP Trunk	No Service	Time not in Full Service: 0 day 0 hour 0 minute

Überprüfung sicherer RTP-Anrufe

Überprüfen Sie, ob das Schlosssymbol bei Anrufen von Unity Connection vorhanden ist. Dies bedeutet, dass der RTP-Stream verschlüsselt ist (das Gerätesicherheitsprofil muss sicher sein, damit es funktioniert), wie in diesem Bild gezeigt.



Fehlerbehebung

1. Allgemeine Tipps zur Fehlerbehebung

Führen Sie die folgenden Schritte aus, um eine Fehlerbehebung für die sichere Integration durchzuführen:

- Überprüfen Sie die Konfiguration.
- Stellen Sie sicher, dass alle zugehörigen Services ausgeführt werden. (CUCM - CallManager, TFTP, CUC - Conversation Manager)
- Stellen Sie sicher, dass die Ports, die für die sichere Kommunikation zwischen Servern erforderlich sind, im Netzwerk offen sind (TCP-Port 2443 für SCCP-Integration und TCP 5061 für SIP-Integration).
- Wenn all dies korrekt ist, fahren Sie mit der Erfassung von Traces fort.

2. Zu sammelnde Ablaufverfolgungen

Erfassen Sie diese Ablaufverfolgungen, um Fehler bei der sicheren Integration zu beheben.

- Paketerfassung von CUCM und CUC
- CallManager-Ablaufverfolgungen
- Cisco Conversation Manager verfolgt

Weitere Informationen zu folgenden Themen finden Sie in diesen Ressourcen:

So führen Sie eine Paketerfassung für CUCM durch:

<http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html>

So aktivieren Sie Traces auf dem CUC-Server:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsg/10xcuctsg010.html

Häufige Probleme

Fall 1: Sichere Verbindung kann nicht hergestellt werden (Warnung der unbekanntenen Zertifizierungsstelle)

Nachdem die Paketerfassung von einem der Server übernommen wurde, wird die TLS-Sitzung eingerichtet.

```
1 0.000000 130.235.201.241 130.235.203.249 TCP instl_boots > https [SYN] Seq=0 win=16384 Len=0 MSS=1460
2 0.000452 130.235.203.249 130.235.201.241 TCP https > instl_boots [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=
3 0.000494 130.235.201.241 130.235.203.249 TCP instl_boots > https [ACK] Seq=1 Ack=1 win=17520 Len=0
4 0.001074 130.235.201.241 130.235.203.249 SSL Client Hello
5 0.001341 130.235.203.249 130.235.201.241 TCP https > instl_boots [ACK] Seq=1 Ack=141 win=6432 Len=0
6 0.005269 130.235.203.249 130.235.201.241 TLSv1 Server Hello,
7 0.005838 130.235.203.249 130.235.201.241 TLSv1 Certificate, Server Hello Done
8 0.006480 130.235.201.241 130.235.203.249 TCP instl_boots > https [ACK] Seq=141 Ack=1895 win=17520 Len=0
9 0.012905 130.235.201.241 130.235.203.249 TLSv1 Alert (Level: Fatal, Description: Unknown CA)
10 0.013244 130.235.201.241 130.235.203.249 TCP instl_boots > https [RST, ACK] Seq=148 Ack=1895 win=0 Len=0
11 0.072262 130.235.201.241 130.235.203.249 TCP instl_bootc > https [SYN] Seq=0 win=16384 Len=0 MSS=1460
12 0.072706 130.235.203.249 130.235.201.241 TCP https > instl_bootc [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=
13 0.072751 130.235.201.241 130.235.203.249 TCP instl_bootc > https [ACK] Seq=1 Ack=1 win=17520 Len=0
```

Der Client gab eine Warnmeldung mit dem fatalen Fehler Unknown CA (Unbekannte CA) an den Server aus, nur weil der Client das vom Server gesendete Zertifikat nicht überprüfen konnte.

Es gibt zwei Möglichkeiten:

1) CUCM sendet Warnmeldung Unbekannte CA

- Überprüfen Sie, ob das aktuelle CUC-Root-Zertifikat auf den Server hochgeladen wird, der mit dem CUC-Server kommuniziert.
- Stellen Sie sicher, dass der CallManager-Dienst auf dem entsprechenden Server neu gestartet wird.

2) CUC sendet Warnmeldung Unbekannte CA

- Überprüfen Sie, ob die TFTP-IP-Adresse korrekt in die Konfiguration **Portgruppe > Bearbeiten > Server** auf dem CUC-Server eingegeben wurde.
- Überprüfen Sie, ob der CUCM-TFTP-Server vom Verbindungsserver erreichbar ist.
- Stellen Sie sicher, dass die CTL-Datei auf dem CUCM TFTP aktuell ist. Führen Sie den CTLClient erneut aus, wenn dies nicht der Fall ist.
- Starten Sie den CUC-Server neu, um die CTL-Datei vom CUCM TFTP erneut herunterzuladen.

Fall 2: CTL-Datei kann nicht vom CUCM TFTP heruntergeladen werden.

Dieser Fehler wird in der Conversation Manager Traces angezeigt:

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server certificates.
MiuGeneral,25,Error executing tftp command 'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not found on server)
```

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server certificates.
```

```
Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as ID=1
```

```
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
```

```
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

Lösung:

1. Überprüfen Sie doppelt, ob der TFTP-Server in der Konfiguration **Portgruppe > Bearbeiten > Server** richtig ist.
2. Stellen Sie sicher, dass sich der CUCM-Cluster im gesicherten Modus befindet.
3. Überprüfen Sie, ob die CTL-Datei auf dem CUCM-TFTP vorhanden ist.

Fall 3: Ports sind nicht registriert

Dieser Fehler wird in der Conversation Manager Traces angezeigt:

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
```

```
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting retry timer -> 5000 msec
```

```
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxxx.tlv]
```

```
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM IP Address>' in CTL File
```

Lösung:

1. Dies ist höchstwahrscheinlich auf eine Diskrepanz in der md5-Prüfsumme der CTL-Datei auf CUCM und CUC zurückzuführen, die durch die Regeneration von

Zertifikate. Starten Sie den CUC-Server neu, um die CTL-Datei zu aktualisieren.

Interne Informationen von Cisco

Alternativ können Sie die CTL-Datei wie folgt aus dem Root entfernen:

Löschen Sie die CTL-Datei aus dem Ordner /tmp/, und setzen Sie die Port-Gruppe zurück. Sie können eine md5-Prüfsumme für die Datei erstellen.

und vor dem Löschen vergleichen:

```
CUCM: [root@vfrscucm1 trust-certs]# md5sum /usr/local/cm/tftp/CTLFile.tlv
```

```
e5bf2ab934a42f4d8e6547dfd8cc82e8 /usr/local/cm/tftp/CTLFile.tlv
```

```
CUC: [root@vstscuc1 tmp]# cd /tmp
```

```
[root@vstscuc1 tmp]# ls -al *tlv
```

```
-rw-rw-r-- 1 cucsmgr cuservice 6120 Feb 5 15:29 a31cfe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

```
[root@vstscuc1]# md5sum a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

```
e5bf2ab934a42f4d8e6547dfd8cc82e8 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

Weitere Informationen finden Sie in diesem Handbuch zur Fehlerbehebung:

Fehler

[CSCum48958](#) - CUCM 10.0 (die IP-Adresslänge ist falsch)

[CSCtn87264](#) - TLS-Verbindung schlägt für sichere SIP-Ports fehl

[CSCur10758](#) - Widerrufbare Zertifikate können nicht gelöscht werden Unity Connection

[CSCur10534](#) - Unity Connection 10.5 TLS/PKI-Interop Redundanter CUCM