

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

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[タスク 1.CUBEセキュア設定](#)

[タスク 2.CVPセキュア設定](#)

[タスク 3.CVVBセキュア設定](#)

[タスク 4.CUCMセキュア設定](#)

[CUCMセキュリティモードを混合モードに設定する](#)

[CUBEおよびCVPのSIPトランクセキュリティプロファイルの設定](#)

[各SIPトランクへのSIPトランクセキュリティプロファイルの関連付け](#)

[CUCMとのセキュアエージェントのデバイス通信](#)

[確認](#)

[トラブルシューティング](#)

概要

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

前提条件

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

要件

次の項目に関する知識があることが推奨されます。

- CCE
- CVP
- CUBE
- CUCM
- CVVB

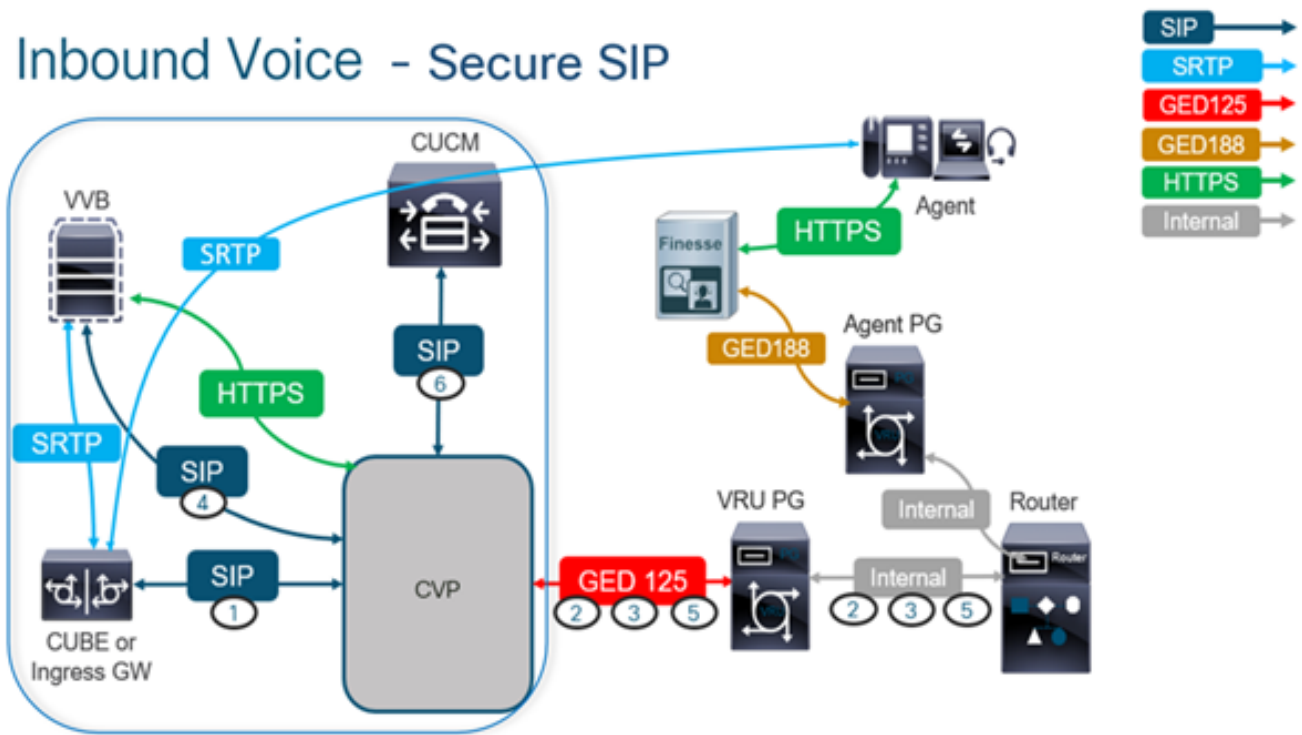
使用するコンポーネント

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

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



タスク 1.CUBEセキュア設定

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

必要な設定：

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

手順：

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

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

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

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

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

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

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

タスク 2.CVPセキュア設定

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

手順：

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

Route Settings

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

Properties

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

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

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

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

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

タスク 3.CVVBセキュア設定

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

手順 :

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



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

version as TLSv1.2.

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

The screenshot shows the Cisco Virtualized Voice Administration interface. A notification dialog box is displayed over the configuration page, stating: "wb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect." The dialog has an "OK" button. In the background, the "System Parameters Configuration" page is visible, with an "Update" button highlighted.

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

The screenshot shows the navigation menu of the Cisco VVB Administration interface. The "Cisco VVB Administration" dropdown menu is open, showing the following options: "Cisco VVB Administration", "Cisco Unified Serviceability", "Cisco VVB Serviceability" (highlighted), and "Cisco Unified OS Administration". A "Go" button is visible to the right of the menu.

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

The screenshot shows the navigation menu of the Cisco VVB Administration interface. The "Tools" dropdown menu is open, showing the following options: "Control Center - Network Services" (highlighted) and "Performance Configuration and Logging".

7. 選択 Engine をクリックし、 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

タスク 4.CUCMセキュア設定

CUCMでSIPメッセージを保護するには、次の設定を実行します。

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

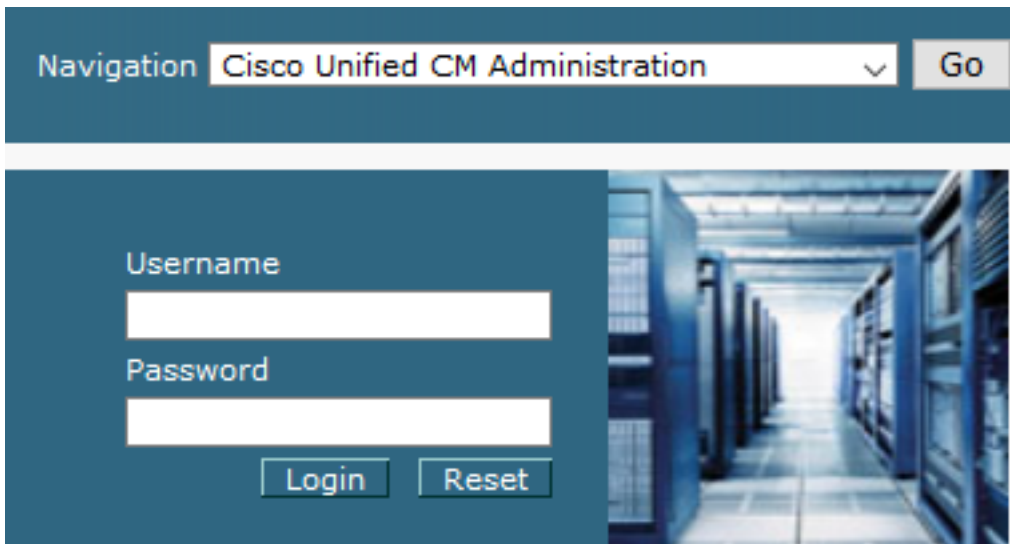
CUCMセキュリティモードを混合モードに設定する

CUCMは、次の2つのセキュリティモードをサポートしています。

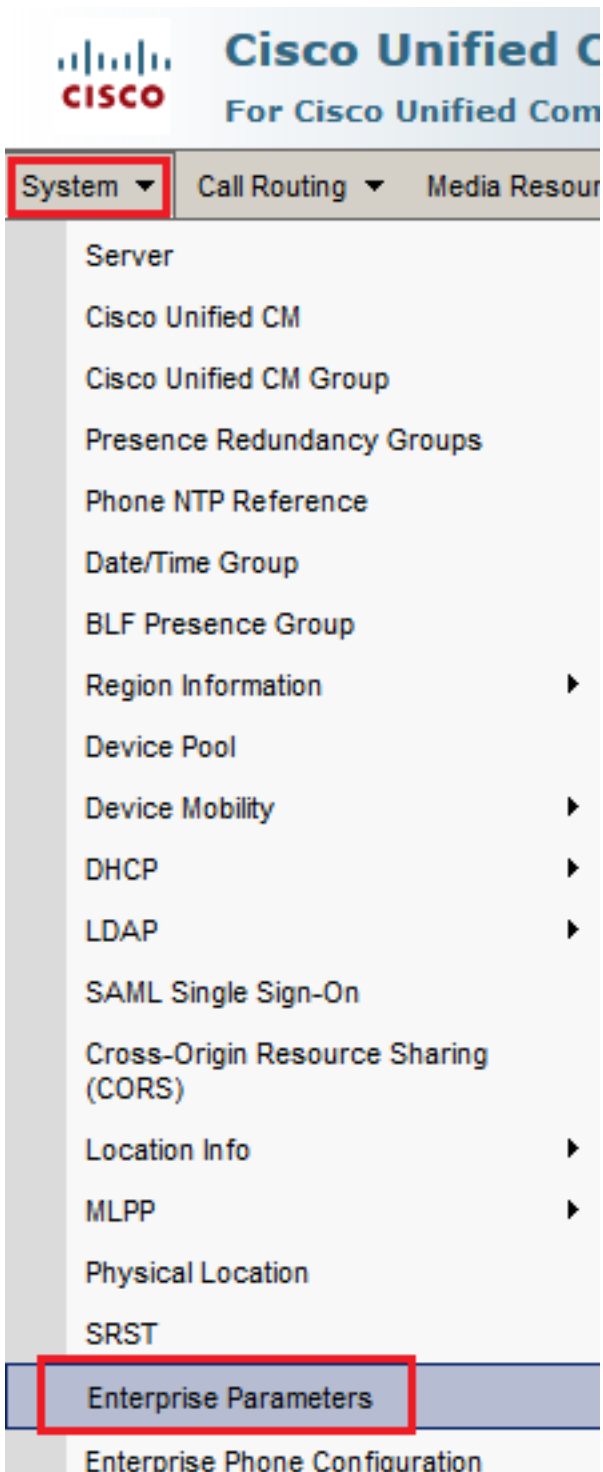
- 非セキュアモード (デフォルトモード)
- 混合モード (セキュアモード)

手順 :

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



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



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

Security Parameters	
Cluster Security Mode *	0
Cluster SIPOAuth Mode *	Disabled

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

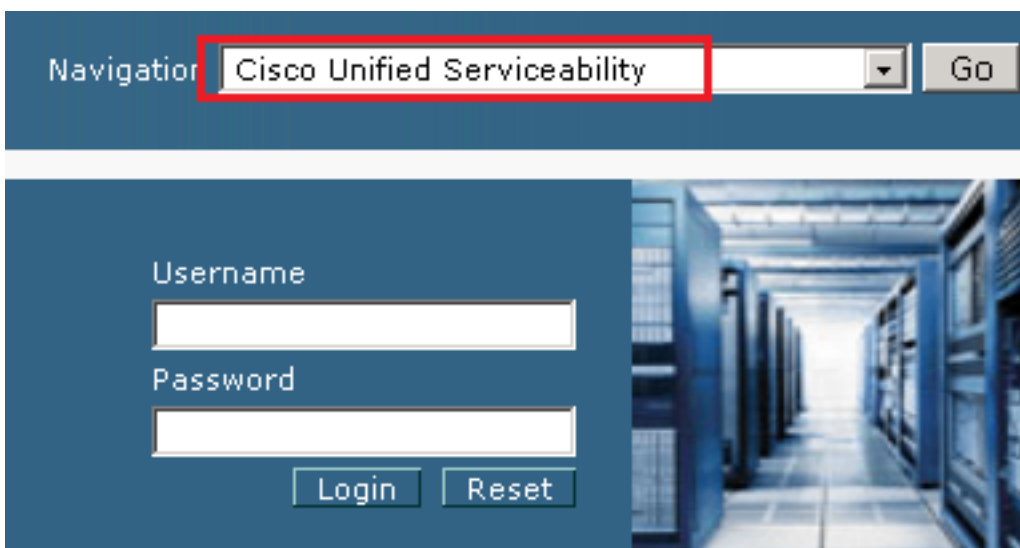
6. SSH経由でCUCMに正常にログインしたら、次のコマンドを実行します。 `utils ctl set-cluster mixed-mode`

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

```
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. 変更を有効にするには、 Cisco CallManager と Cisco CTIManager サービス.

9. サービスを再起動するには、に移動してログインします Cisco Unified Serviceability.



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

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

11. サーバを選択し、 Go.

Select Server

Server*

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

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

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.

OK

Cancel

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

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

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.

OK

Cancel

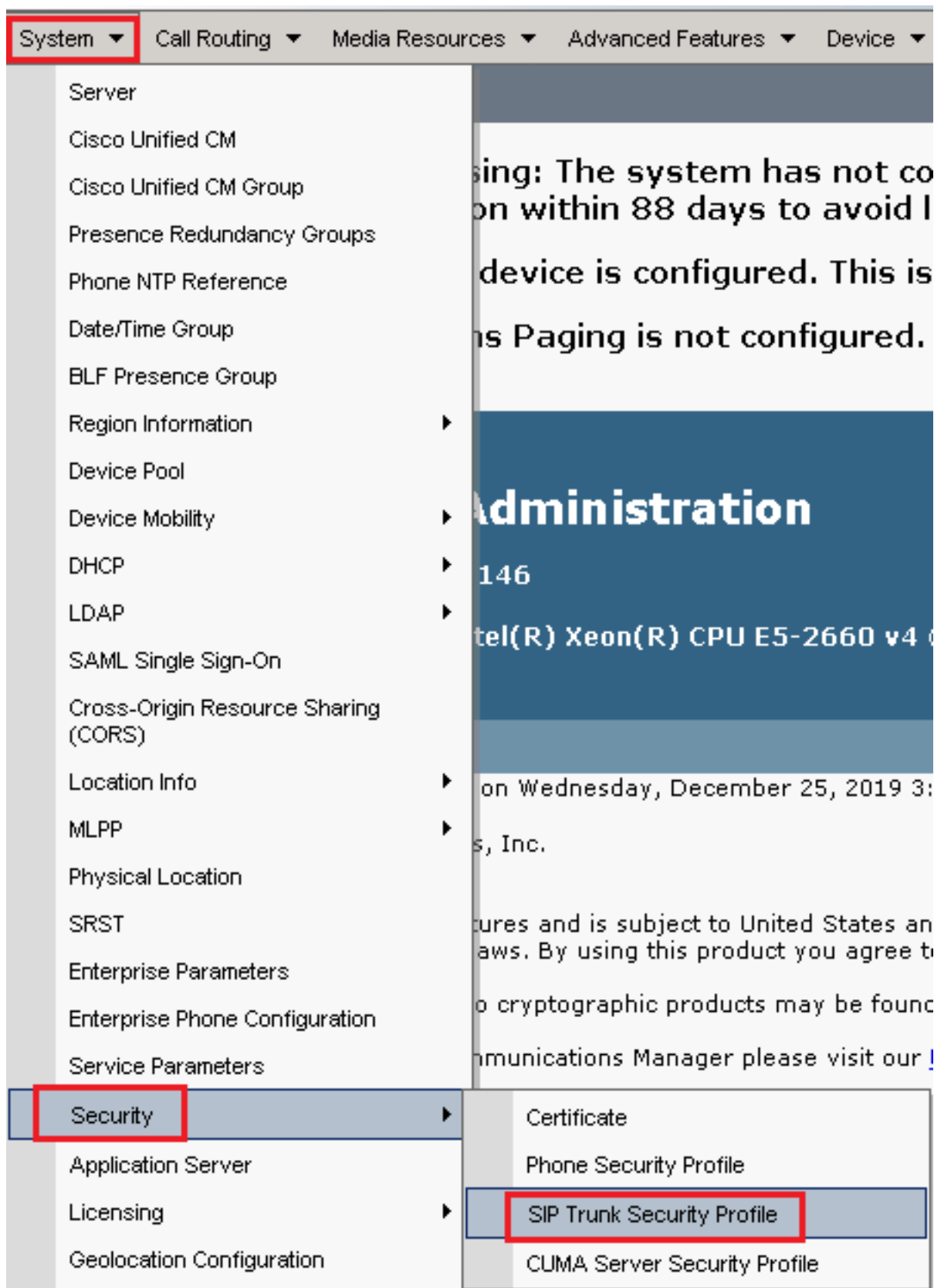
16. サービスが正常に再起動したら、クラスタセキュリティモードが混合モードに設定されていることを確認し、手順5で説明されているようにCUCM管理に移動します。次に、 Cluster Security Mode.次に設定する必要があります。 1.

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

CUBEおよびCVPのSIPトランクセキュリティプロファイルの設定

手順 :

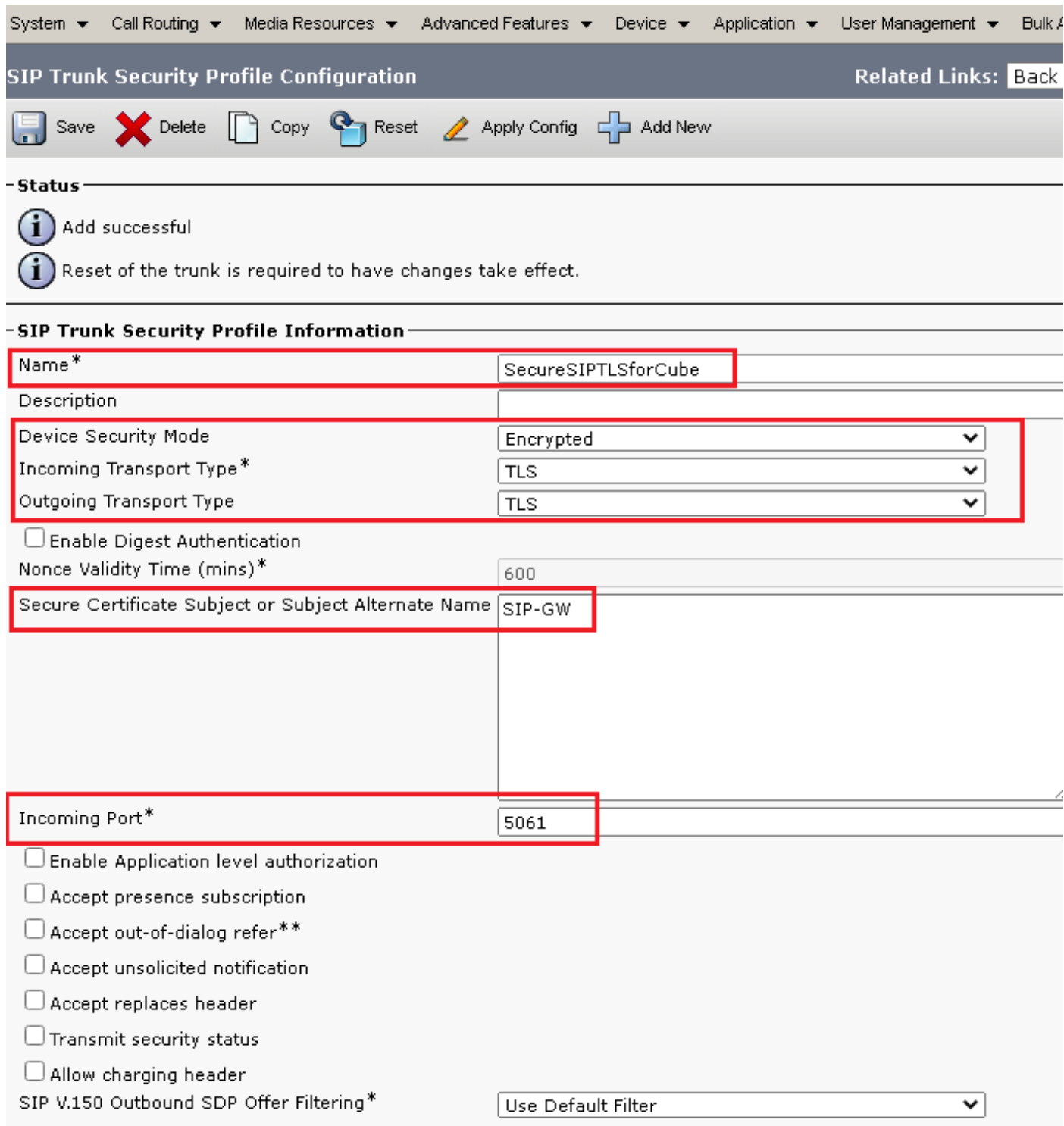
1. ログイン先 CUCM administration サポートされていません。
2. CUCMに正常にログインした後、 System > Security > SIP Trunk Security Profile CUBEのデバイスセキュリティプロファイルを作成します。



3. 左上で、 Add New 新しいプロファイルを追加します。



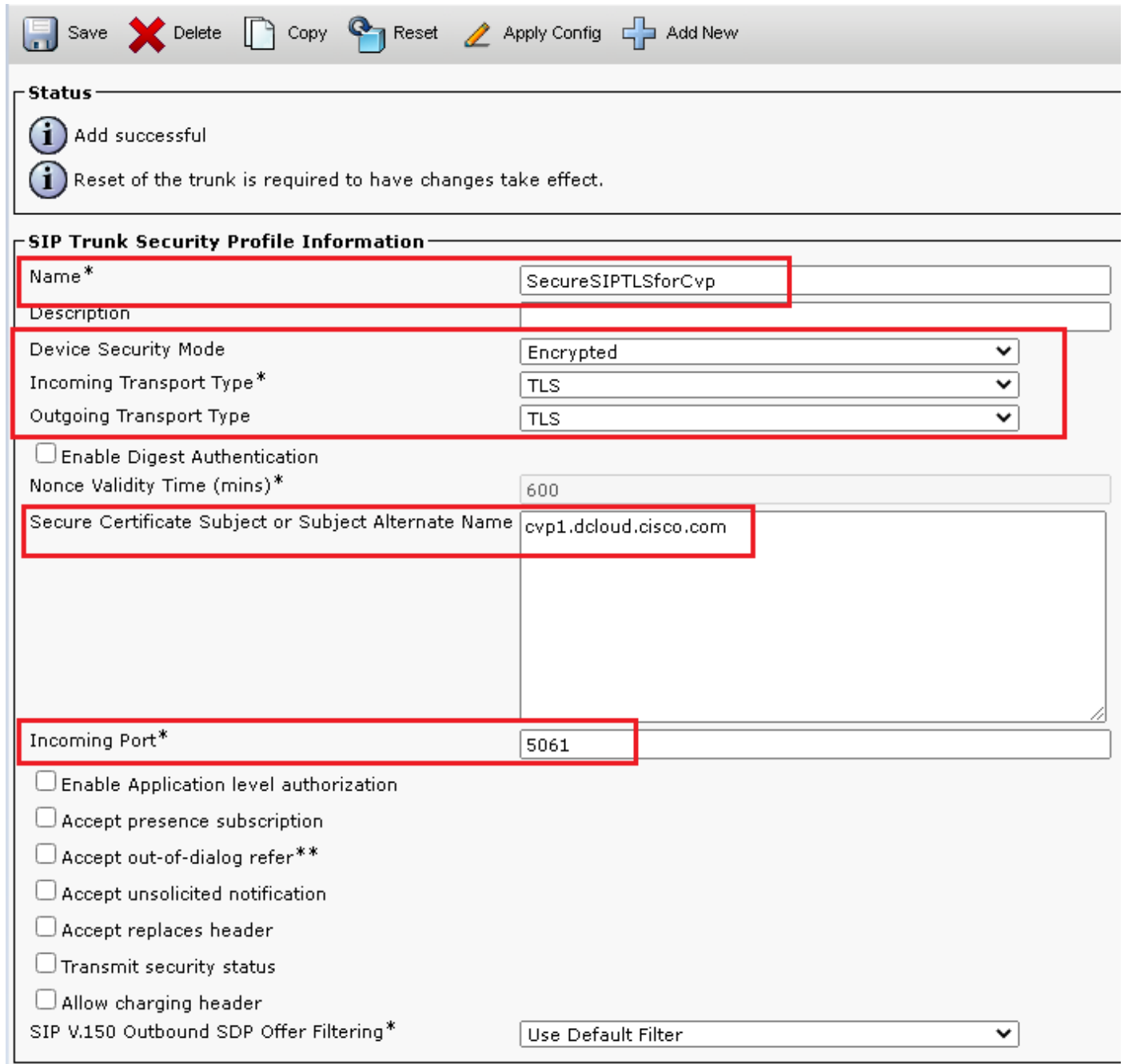
4. 設定 SIP Trunk Security Profile 次の図に示すように、 Save ページの左下で ~する Save IT。



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

必要があります。

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



Status

- Add successful
- 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

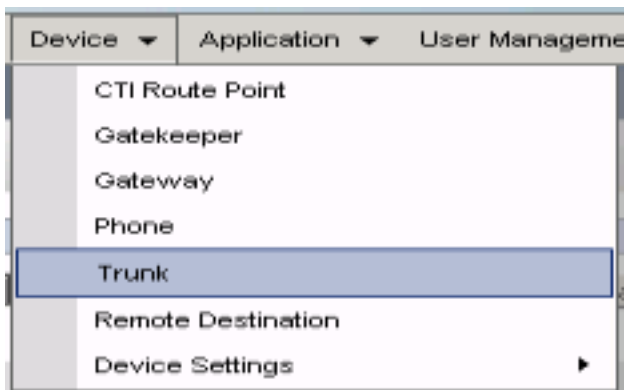
Allow charging header

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

各SIPトランクへのSIPトランクセキュリティプロファイルの関連付け

手順：

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



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

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. [vCUBE]をクリックして、[vCUBEトランク設定(vCUBE trunk configuration)]ページを開きます。

4. 下にスクロールして SIP Information セクションに移動し、 Destination Port から 5061.

5. Change SIP Trunk Security Profile から SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1*

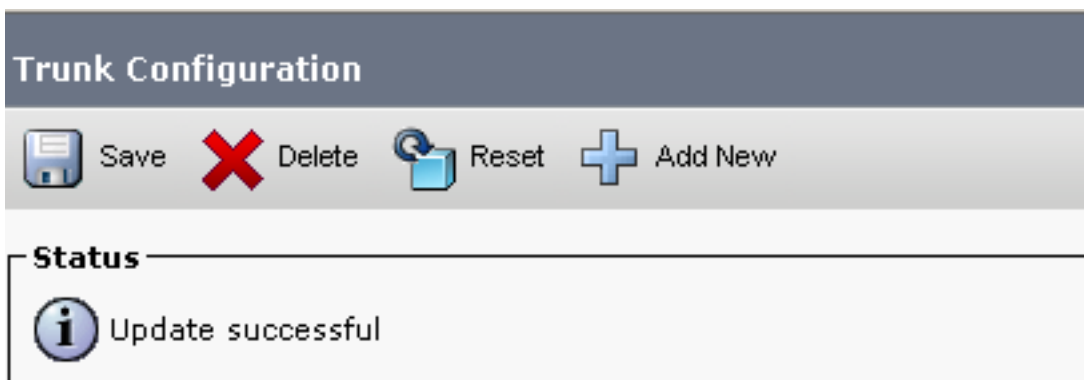
MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space


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



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

Trunks (1 - 1 of 1)				
Find Trunks where				
	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

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

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

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

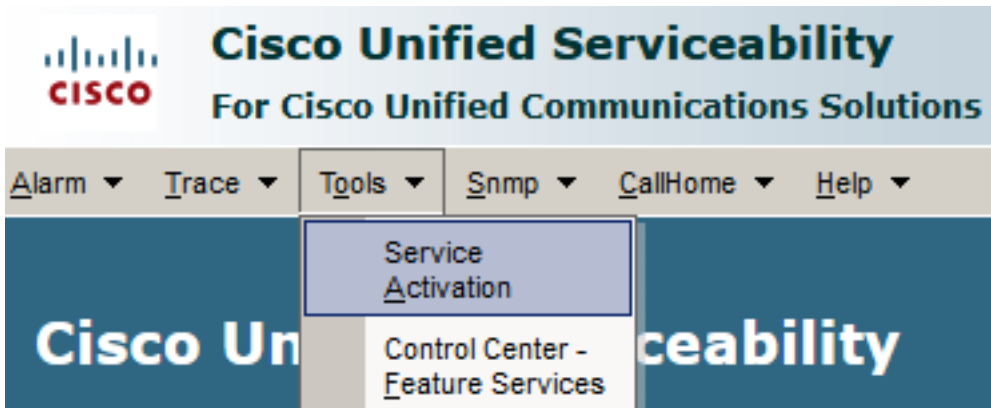
CUCMとのセキュアエージェントのデバイス通信

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

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

手順：

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



3. CUCMサーバを選択し、 Go .

Service Activation

Select Server

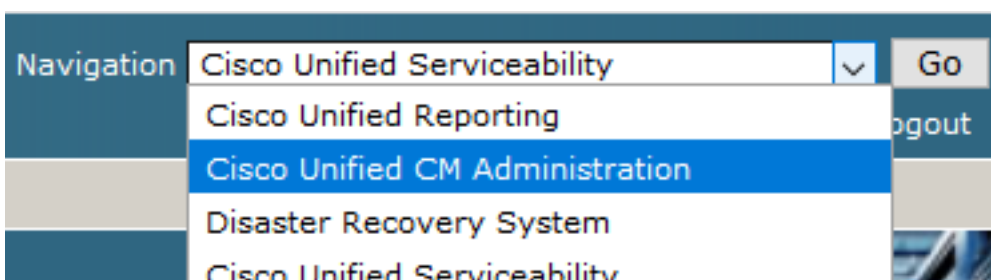
Server*

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

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



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



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

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

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

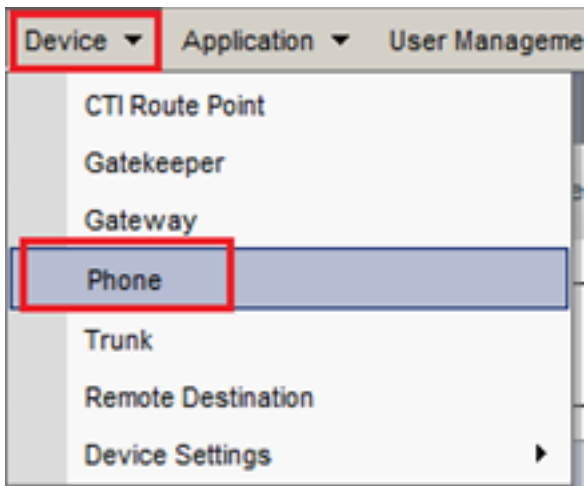
Authentication Mode* By Null String ▾
Key Order* RSA Only ▾
RSA Key Size (Bits)* 2048 ▾
EC Key Size (Bits) < None > ▾
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

Save Delete Copy Reset Apply Config Add New

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



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

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	<input type="text"/>
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

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

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







Protocol Specific Information

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 F
Rerouting Calling Search Space	Cisco Unified Client Services Framework - Secure Profile


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

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ A

Phone Configuration



 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New

Status


 Update successful

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

Device Reset

 Reset
  Restart

Status

 Status: Ready

Reset Information

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

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Order*

RSA Key Size (Bits)*

EC Key Size (Bits)

Operation Completes By (YYYY:MM:DD:HH)

Certificate Operation Status: Upgrade Success

Note: Security Profile Contains Addition CAPF Settings.

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

確認

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

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

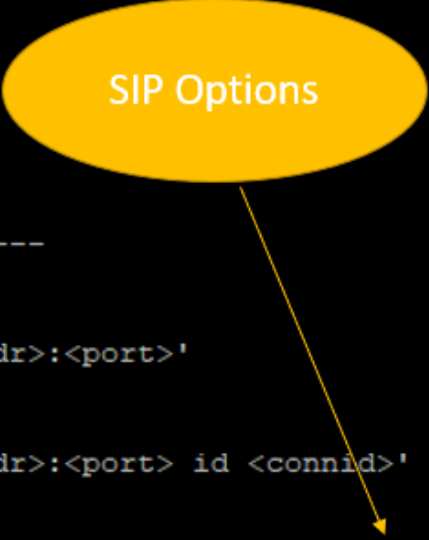
```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 1
No. of send failures         : 0
No. of remote closures       : 34
No. of conn. failures        : 0
No. of inactive conn. ageouts : 12
TLS client handshake failures : 0
TLS server handshake failures : 0

-----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:
```



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

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

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

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

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

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

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

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

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

```
show sip-ua connections tcp tls detail
```

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

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

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

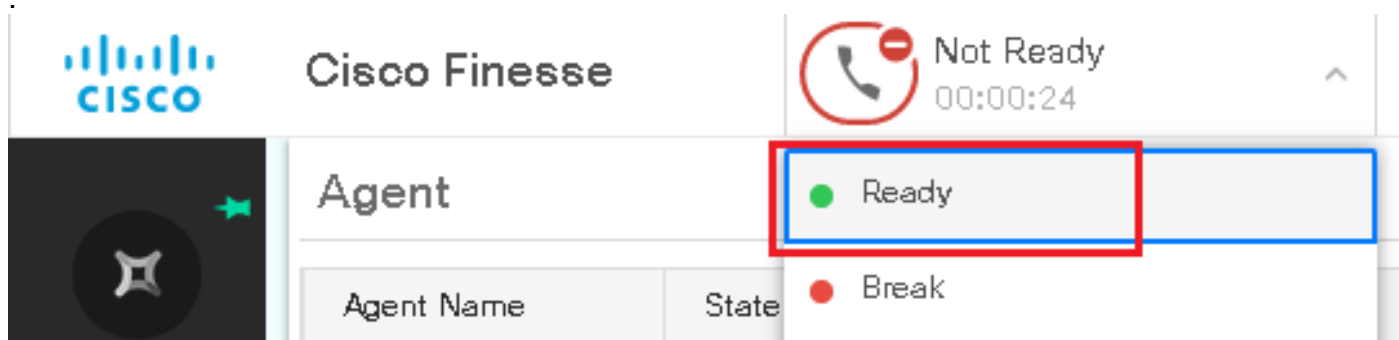
Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address TLS-Version
  =====
      5061      3 Established      0      -      TLSv1.2

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

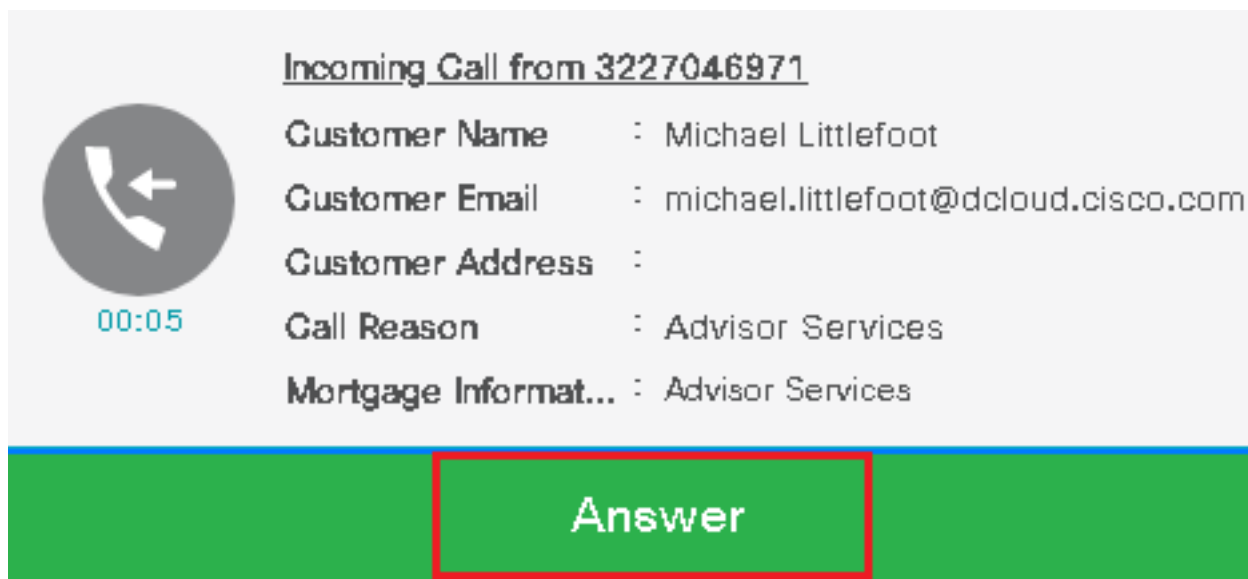
チェック:SIP over TLS接続はCVPと確立されていますか。この場合、出力はCVPとCUBE間のSIP信号がセキュアであることを確認します。

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

8.エージェントがコールに応答できるようにします。



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



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

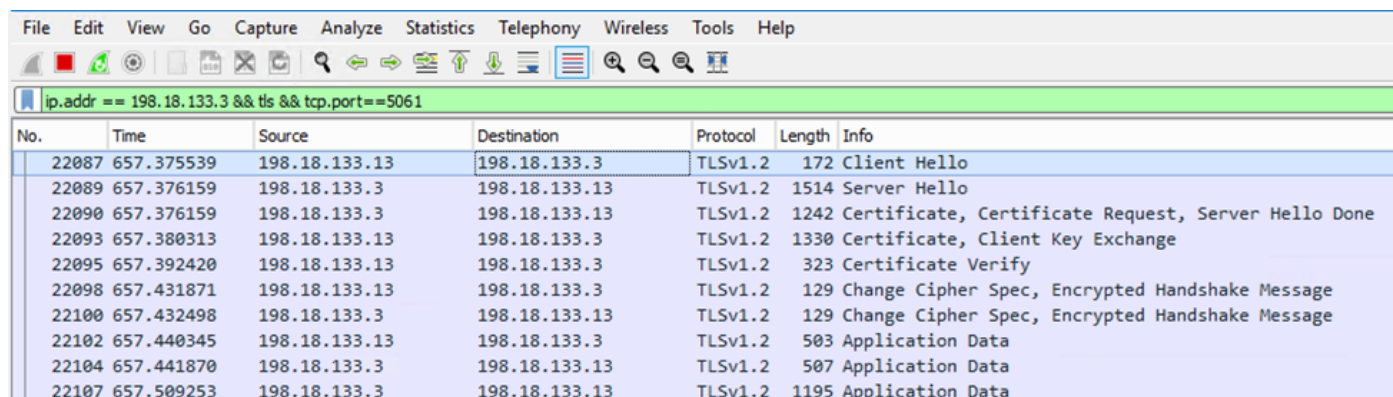
00:05

Answer

10. コールがエージェントに接続します。

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

ip.addr == 198.18.133.3 && tls && tcp.port==5061



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

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

トラブルシューティング

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

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。