

# Contact Center EnterpriseでのセキュアRTP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のセキュアな設定](#)

[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](#)

[SIPトランクセキュリティプロファイルをそれぞれのSIPトランクに関連付け、SRTPを有効にする](#)

[CUCMとのセキュアエージェントのデバイス通信](#)

[確認](#)

## 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Real-time Transport Protocol(SRTP)トラフィック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)Call Server、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、以前のバージョンにも適用できます。

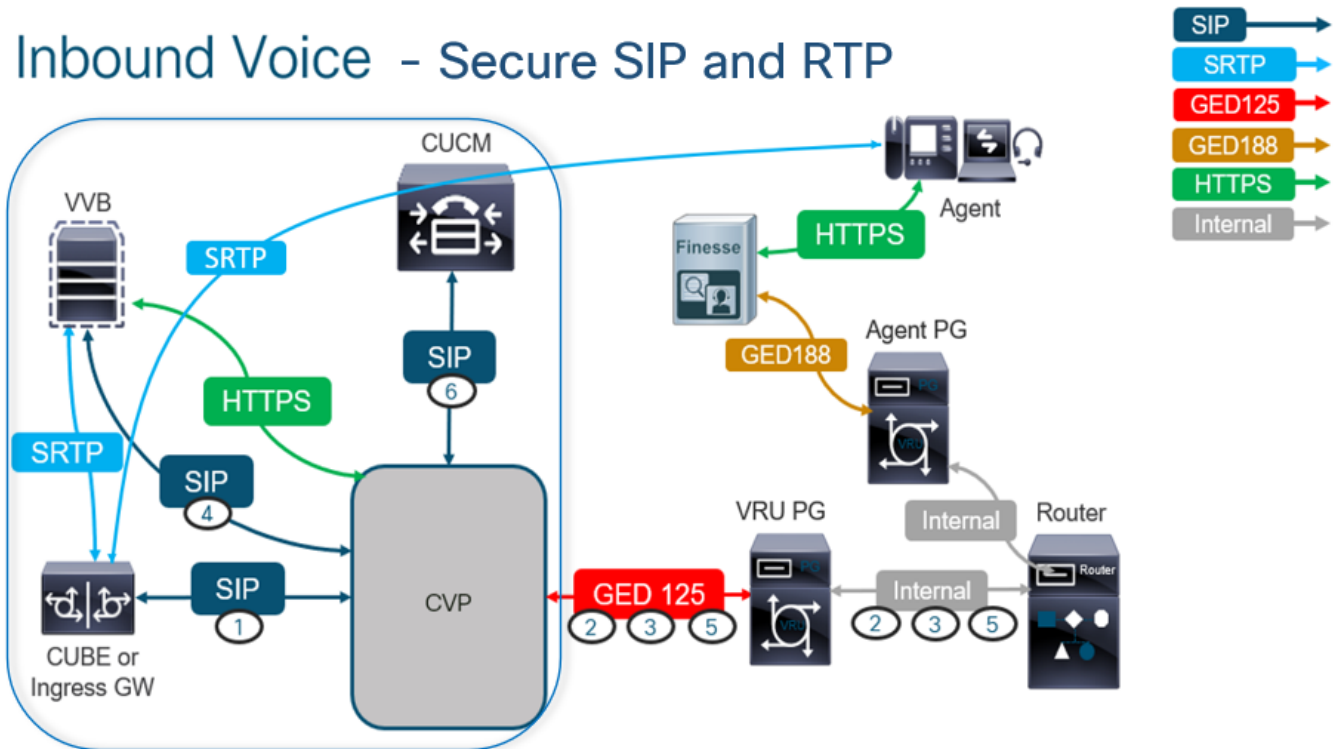
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

注：コンタクトセンターの包括的なコールフローでは、セキュアRTPを有効にするには、セキュアSIP信号を有効にする必要があります。したがって、このドキュメントの設定では、セキュアSIPとSRTPの両方が有効になっています。

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信号とRTPに関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で設定を開始します。次に、CVP、CVVB、およびCUCMを設定します。

### Inbound Voice - Secure SIP and RTP



### タスク1:CUBEのセキュアな設定

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

必要な設定：

- SIP UA のデフォルトのトラストポイントを設定します。
- TLSおよびSRTPを使用するためのダイヤルピアの変更

手順 :

1. CUBEへのSSHセッションを開きます。
2. SIPスタックでCUBEの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 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)#
```

## 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. Cisco Unified Communications Managerにログインし、 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するタブ。 Set SecurePort から 5061 をクリックし、 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. クリック vvb1.dcloud.cisco.comその後、 Members タブをクリックし、 SecurePort から 5061 をクリックし、 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

### 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)とSRTPを保護するようにCVVBを設定します。

手順：

1. を開きます。 Cisco VVB Admin 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. Cisco Unified Communications Manager Security Parameters セクション、選択 Enable を参照 TLS (SIP) .IPv6アドレスを Supported TLS(SIP) version as TLSv1.2 を選択し、 Enable を参照 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 [Crypto Suite : AES_CM_128_HMAC_SHA1_32]	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

4. クリック Update. クリック Ok cvvbエンジンの再起動を求めるプロンプトが表示されます。

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. 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 をクリックし、 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. 移動先 Tools > Control Center – Network Services.

The screenshot shows the 'Tools' menu with the following items: '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メッセージとRTP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
- SIPトランクセキュリティプロファイルをそれぞれのSIPトランクに関連付け、SRTPを有効にする
- CUCMとのセキュアエージェントのデバイス通信

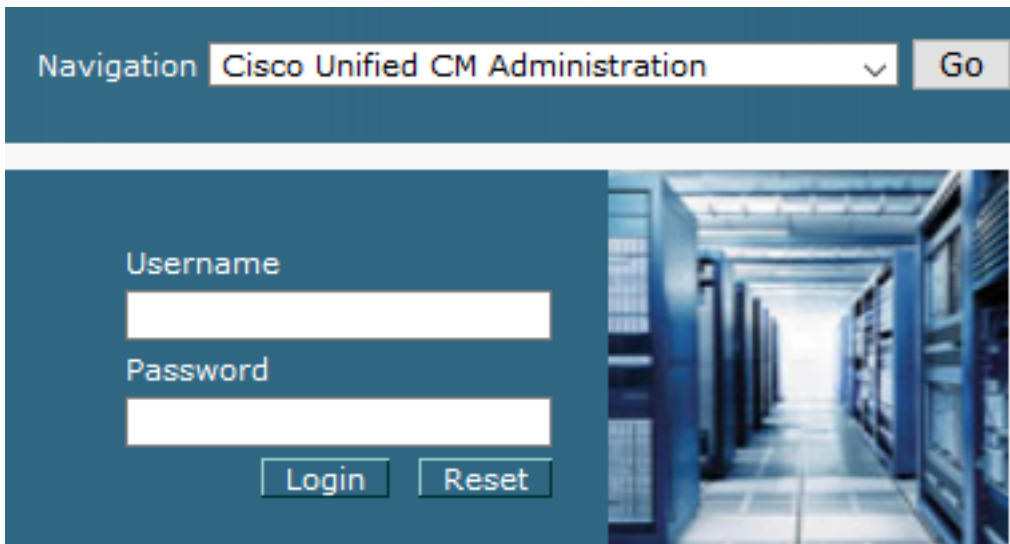
### CUCMセキュリティモードを混合モードに設定する

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。

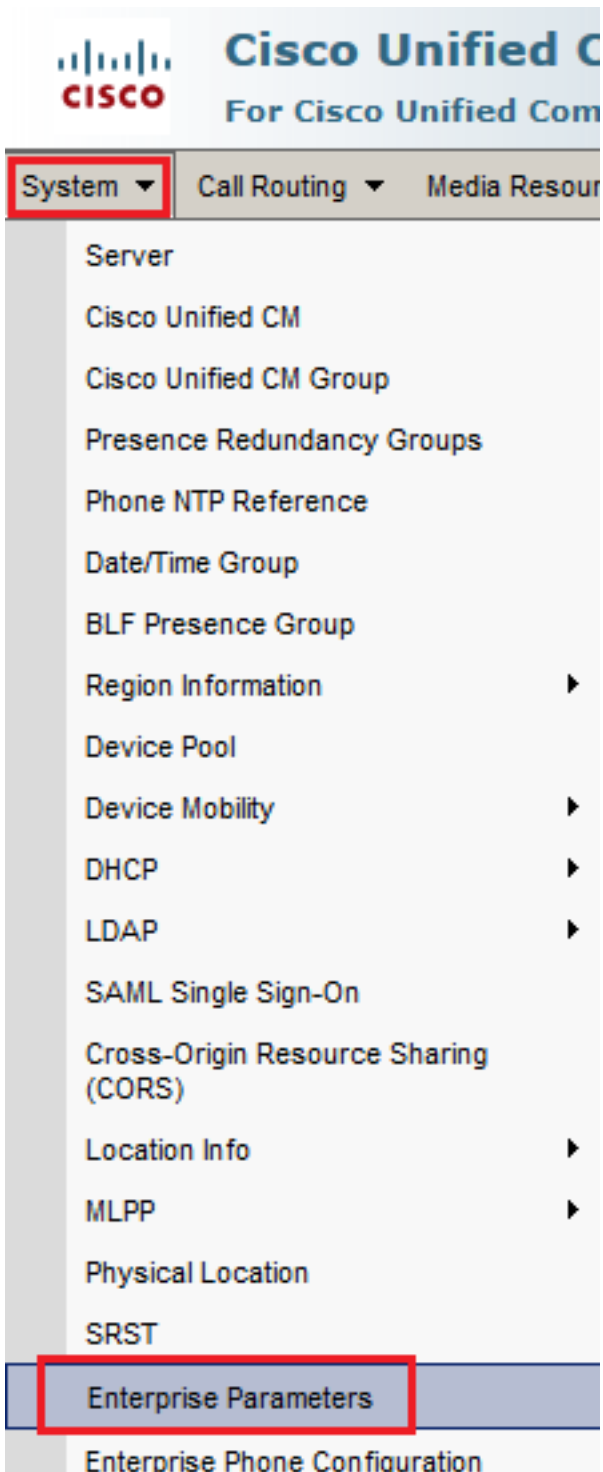
- 非セキュアモード ( デフォルトモード )
- 混合モード ( セキュアモード )

手順：

1. CUCM管理インターフェイスにログインします。



2. CUCMにログインすると、 System > Enterprise Parameters.



3. 下に Security Parameters セクションを参照して、 Cluster Security Mode に設定されている 0.



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。

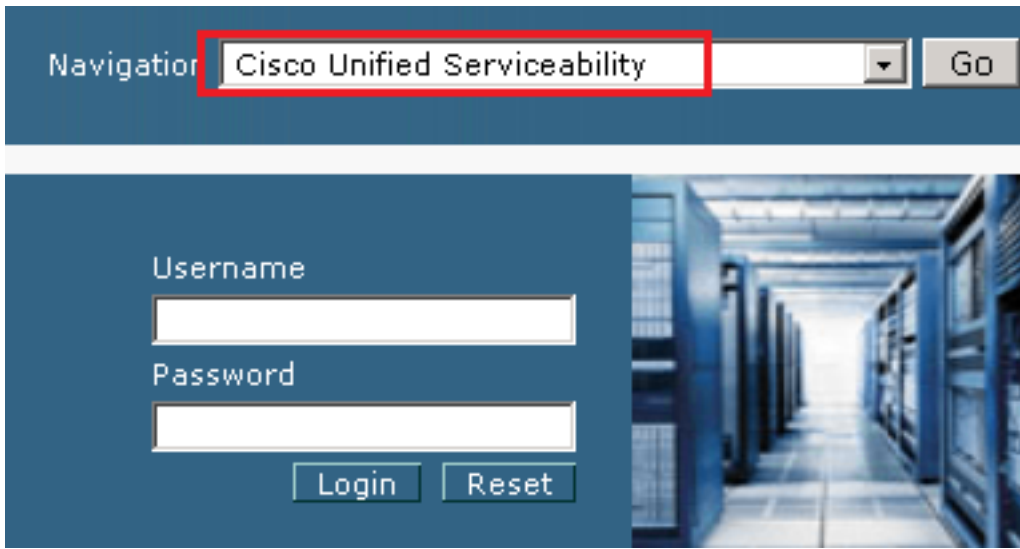
**utils ctl set-cluster mixed-mode**



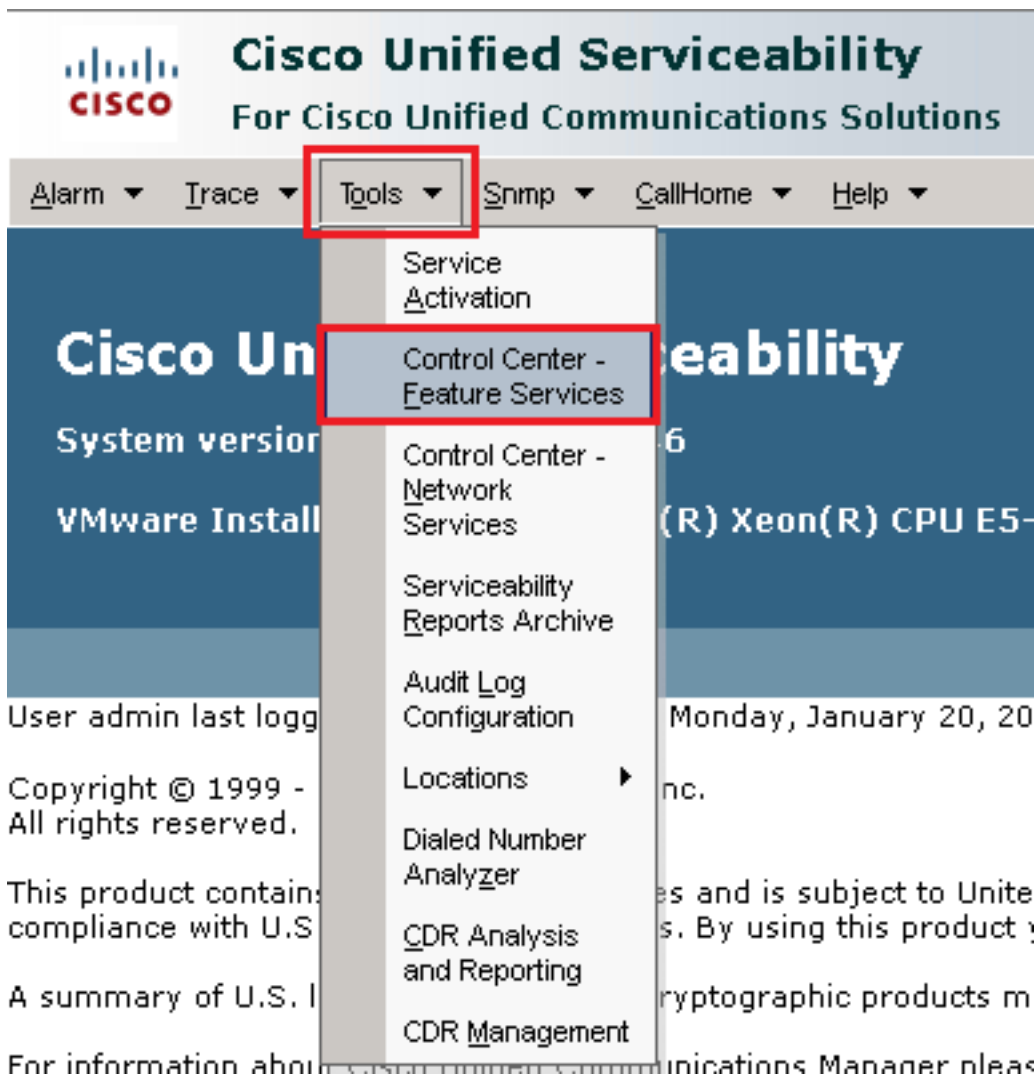
7. Type `y` をクリックし、Enter プロンプトが表示されます。このコマンドは、クラスタセキュリティモードを混合モードに設定します。

```
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 および 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.



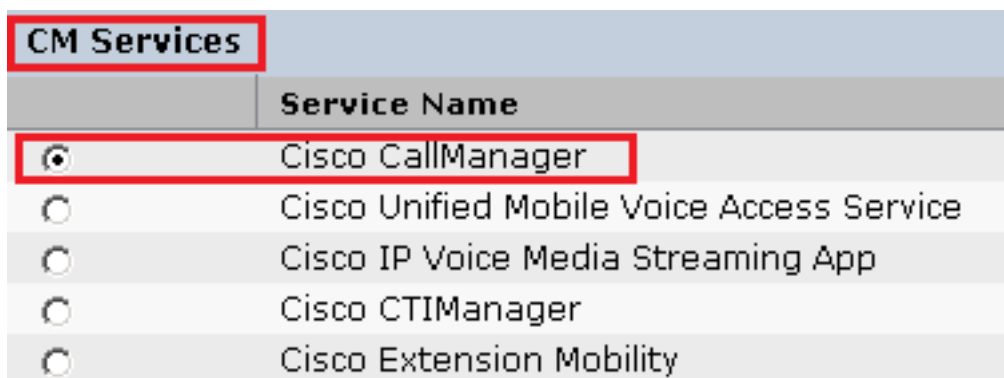
10. ログインに成功したら、に移動します。 Tools > Control Center – Feature Services.



11. サーバを選択し、 Go.



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



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. の再起動が成功した後 Cisco CallManagerを選択し、 Cisco 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

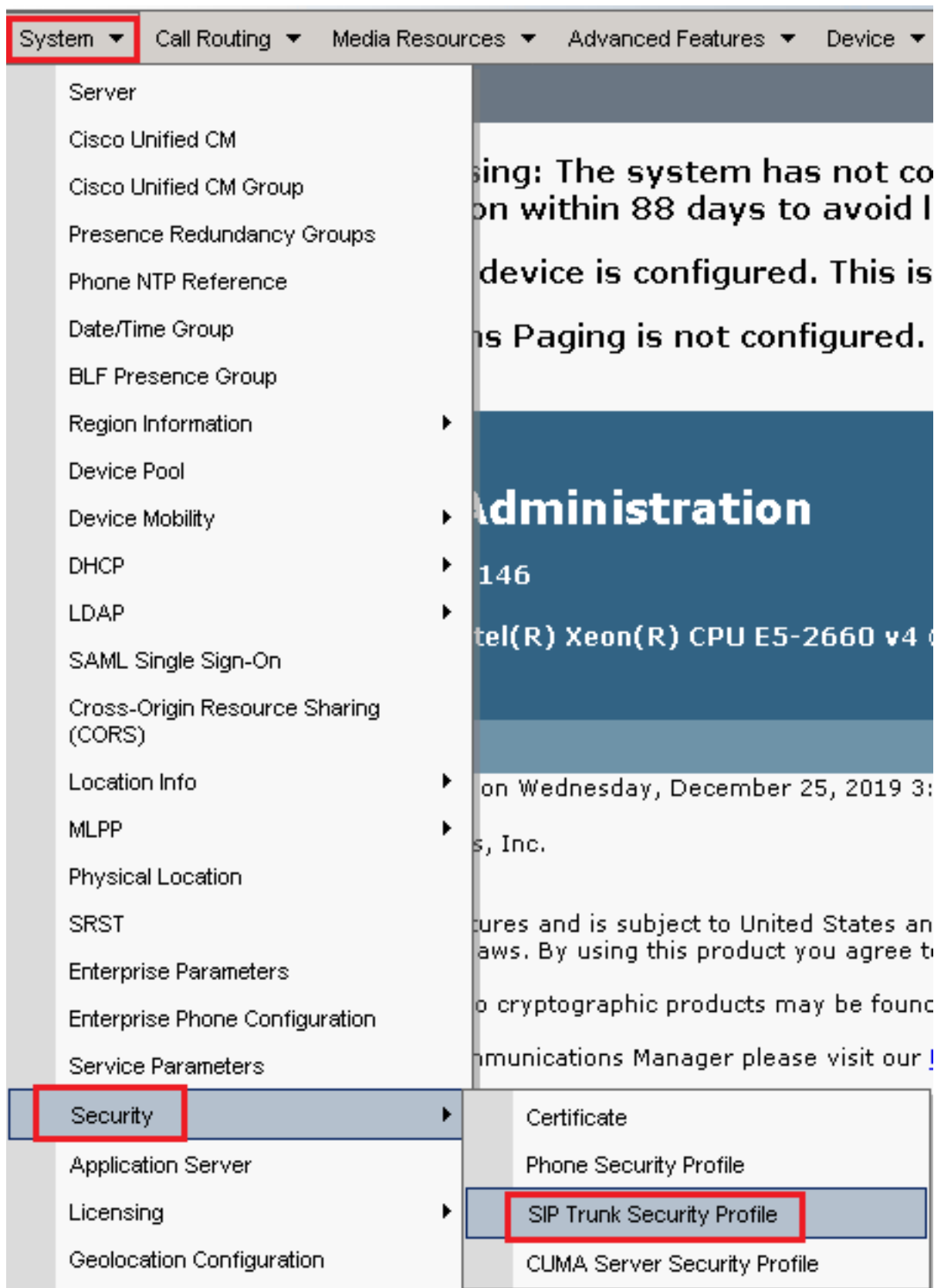
16. サービスが正常に再起動した後、クラスタセキュリティモードが混合モードに設定されていることを確認するには、ステップ5で説明されているようにCUCM管理に移動し、 Cluster Security Mode.次に設定する必要があります。 1.

Security Parameters	
<a href="#">Cluster Security Mode</a> *	1
<a href="#">Cluster SIPOAuth Mode</a> *	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. CUCM管理インターフェイスにログインします。
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. 左上の[Add New] をクリックして、新しいプロファイルを追加します。



4. 設定 SIP Trunk Security Profile 次の図のように入力し、 Save ページの左下。

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk A

### 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

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 ▾

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.Change 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。

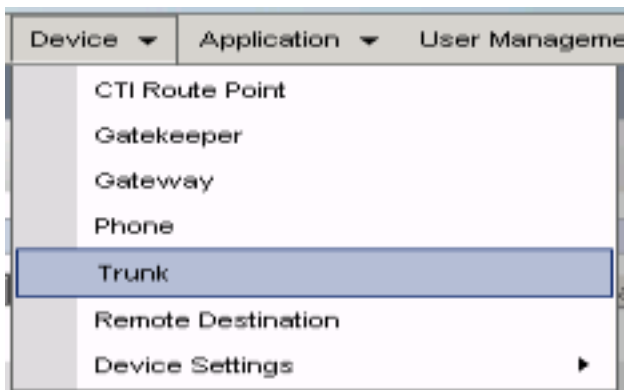
The screenshot displays the configuration page for a SIP Trunk Security Profile. The interface includes a top toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, there is a Status section with two informational messages: "Add successful" and "Reset of the trunk is required to have changes take effect." The main section is titled "SIP Trunk Security Profile Information" and contains the following fields and options:

- Name\*: SecureSIPTLSforCvp
- Description: (empty)
- 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

SIPトランクセキュリティプロファイルをそれぞれのSIPトランクに関連付け、SRTPを有効にする

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 をクリックし、 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_DP	dCloud_DP	cloudcherry_sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. クリック vCUBE をクリックして、vCUBEトランク設定ページを開きます。

4. イン Device Information セクションを確認してください。SRTP Allowed SRTPを有効にします。

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. 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.

6. Change SIP Trunk Security Profile から 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. クリック Save then Rest から 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

8. 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
	Select item or enter search text			
	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

9. クリック CVP-SIP-Trunk CVPトランク設定ページを開きます。
10. イン Device Information セクション、チェック SRTP Allowed SRTPを有効にします。

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\*  When using both sRTP and TLS

Use Trusted Relay Point\*  Default

11. 下にスクロールして、 SIP Information セクションを変更し、 Destination Port から 5061.
12. Change SIP Trunk Security Profile から SecureSIPTLSForCvp.

**SIP Information**

**Destination**

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

13. クリック Save then Rest から 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.

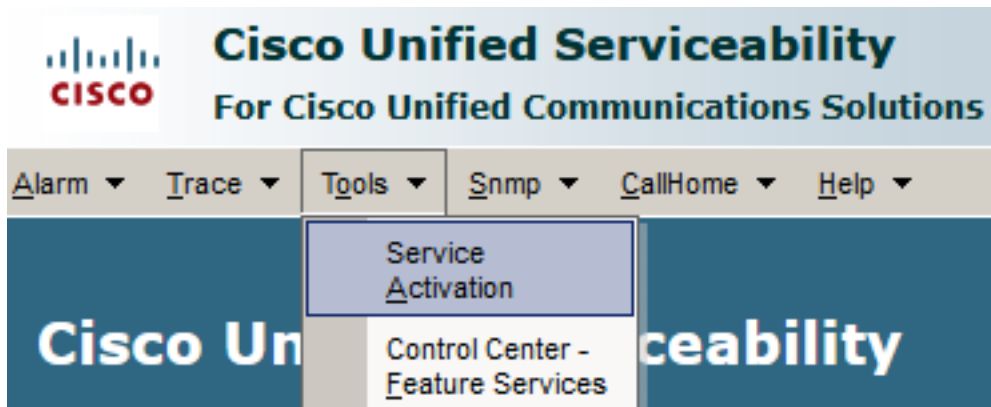
OK

## 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、セキュリティブ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、CUCM CAPF秘密キーで署名されたエンドポイントの公開キーを保持します。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 サポートされていません。
2. 移動先 Tools > Service Activation.



3. CUCMサーバを選択し、 Go.

### Service Activation

Select Server

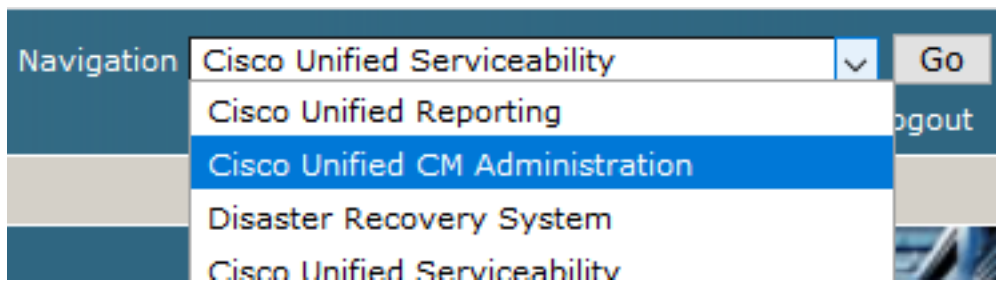
Server\*

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、CUCM administrationに移動します。



6. CUCM管理へのログインに成功したら、に移動します。 System > Security > Phone Security Profile **工**  
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. 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. 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. コピーアイコンをクリックします  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
	Name	Description
	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. C次の図のようにパラメータを変更し、 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**

**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 >

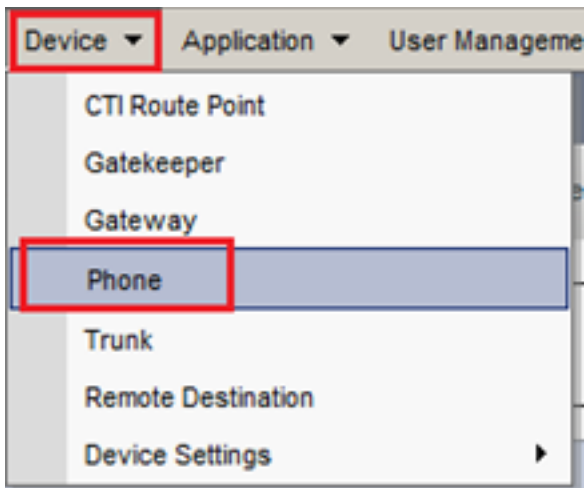
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**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 使用可能なすべての電話機を一覧表示するには、[エージェントの電話機 (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 セクションに移動し、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. 手順と同じ手順を参照してください。7 ~ 13:CUCMでセキュアSIPおよびRTPを使用する他のエージェントのデバイスを保護します。

# 確認

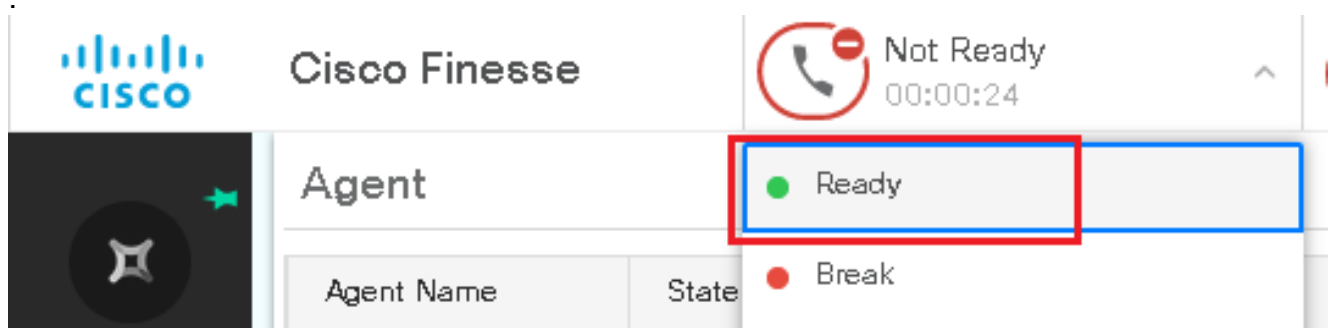
RTPが適切に保護されていることを確認するには、次の手順を実行します。

1. コンタクトセンターにテストコールを発信し、IVRプロンプトを聞きます。
2. 同時に、vCUBEへのSSHセッションを開き、次のコマンドを実行します。  
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:
```

ヒント:SRTPが on CUBEとVVB間(198.18.133.143)。この場合、CUBEとVVBの間のRTPトラフィックが安全であることを確認します。

3. エージェントがコールに応答できるようにします。

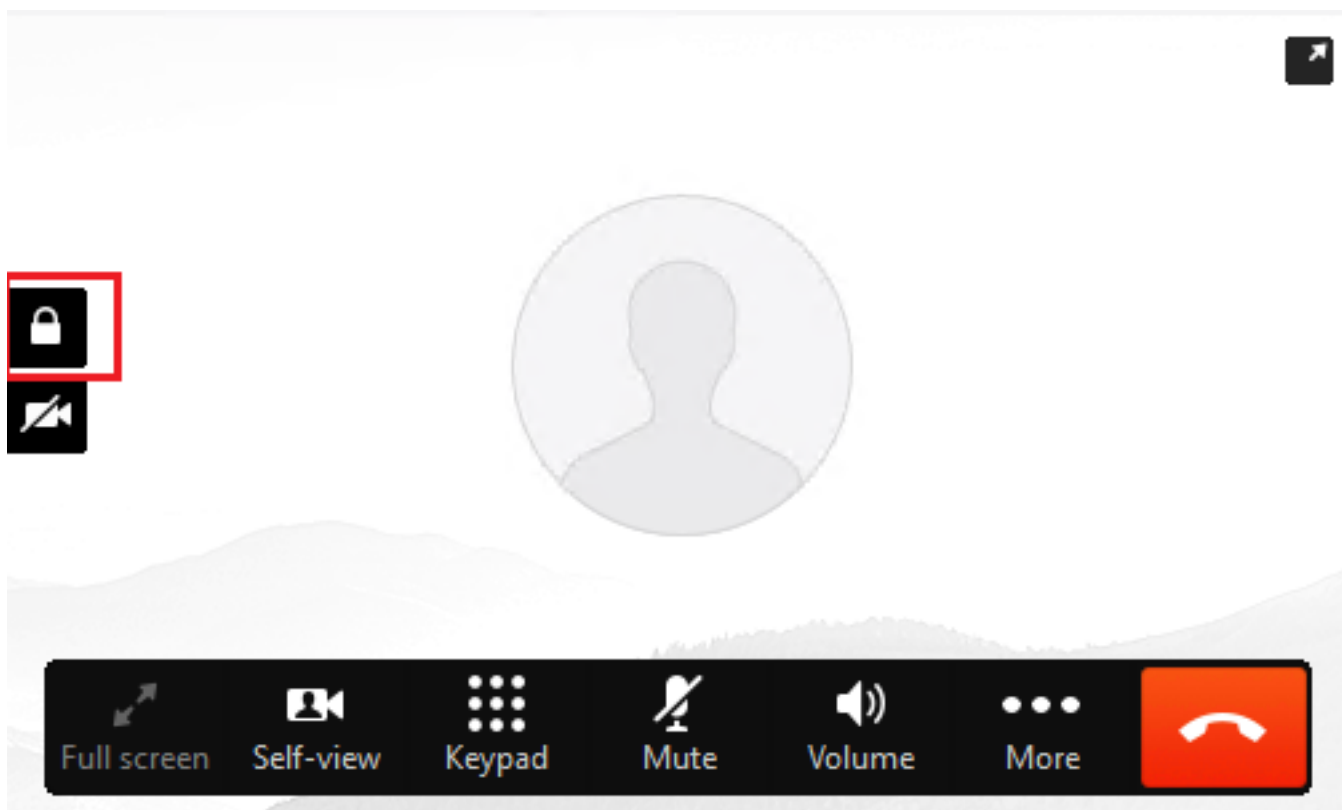


4. エージェントが予約され、コールがエージェントにルーティングされます。通話に応答します。
5. コールがエージェントに接続されます。vCUBE SSHセッションに戻り、次のコマンドを実行します。  
show call active voice brief

```
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:
```

ヒント:SRTPが on CUBEとエージェントの電話(198.18.133.75)の間で行われます。「はい」の場合、CUBEとエージェント間のRTPトラフィックが安全であることを確認します。

6. また、コールが接続されると、エージェントデバイスにセキュリティロックが表示されます。これにより、RTPトラフィックが安全であることも確認できます。



SIP信号が適切に保護されていることを検証するには、「[セキュアSIPシグナリングの設定](#)」の記事を参照してください。



## 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。