

CUCM と CUC 間のセキュアな統合の設定およびトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[図](#)

[設定：セキュア SIP トランク](#)

[CUC の設定](#)

[1. SIP 証明書の追加](#)

[2. 新しい電話システムの作成またはデフォルトの電話システムの変更](#)

[3. 新しいポートグループの追加](#)

[4. サーバの編集](#)

[5. ポートグループのリセット](#)

[6. ボイスメールポートの追加](#)

[7. CUC ルート証明書のダウンロード](#)

[CUCM の設定](#)

[1. CUC へのトランク用 SIP トランクセキュリティプロファイルの設定](#)

[2. SIP プロファイルの設定](#)

[3. SIP トランクの作成](#)

[4. ルートパターンの作成](#)

[5. ボイスメールパイロットの作成](#)

[6. ボイスメールプロファイルの作成](#)

[7. ボイスメールプロファイルの DN への割り当て](#)

[8. CUC ルート証明書を CallManager-trust としてアップロード](#)

[セキュア SCCP ポートの設定](#)

[CUC の設定](#)

[1. CUC ルート証明書のダウンロード](#)

[2. 電話システムの作成/既存の電話システムの変更](#)

[3. 新しい SCCP ポートグループの追加](#)

[4. サーバの編集](#)

[5. セキュア SCCP ポートの追加](#)

[CUCM の設定](#)

[1. ポートの追加](#)

[2. CUC ルート証明書を CallManager-trust としてアップロードする](#)

[3. メッセージ受信情報\(MWI\)のオン/オフの拡張機能の設定](#)

[4. ボイスメールパイロットの作成](#)

[5. ボイスメールプロファイルの作成](#)

[6. ボイスメールプロファイルの DN への割り当て](#)

[7. ボイスメールハントグループの作成](#)

[確認](#)

[SCCP ポートの検証](#)

[セキュア SIP トランクの検証](#)

[セキュア RTP コールの検証](#)

[トラブルシューティング](#)

[1.一般的なトラブルシューティングのヒント](#)

[2.収集するトレース](#)

[一般的な問題](#)

[ケース 1：セキュアな接続を確立できない \(不明な CA アラート\)](#)

[ケース 2：CUCM TFTP から CTL ファイルをダウンロードできない](#)

[ケース 3：ポートが登録されない](#)

[不具合](#)

概要

このドキュメントでは、Cisco Unified Communication Manager (CUCM) サーバと Cisco Unity Connection (CUC) サーバの間でのセキュアな接続の設定、検証、およびトラブルシューティングについて説明します。

前提条件

要件

CUCM について十分に理解しておくことをお勧めします。

詳細については、『[Cisco Unified Communications Manager セキュリティガイド](#)』を参照してください。

注：セキュアな統合を正しく機能させるには、混合モードに設定する必要があります。

Unity Connection 11.5(1) SU3以降では暗号化を有効にする必要があります。

CLIコマンド「`utils cuc encryption <enable/disable>`」

使用するコンポーネント

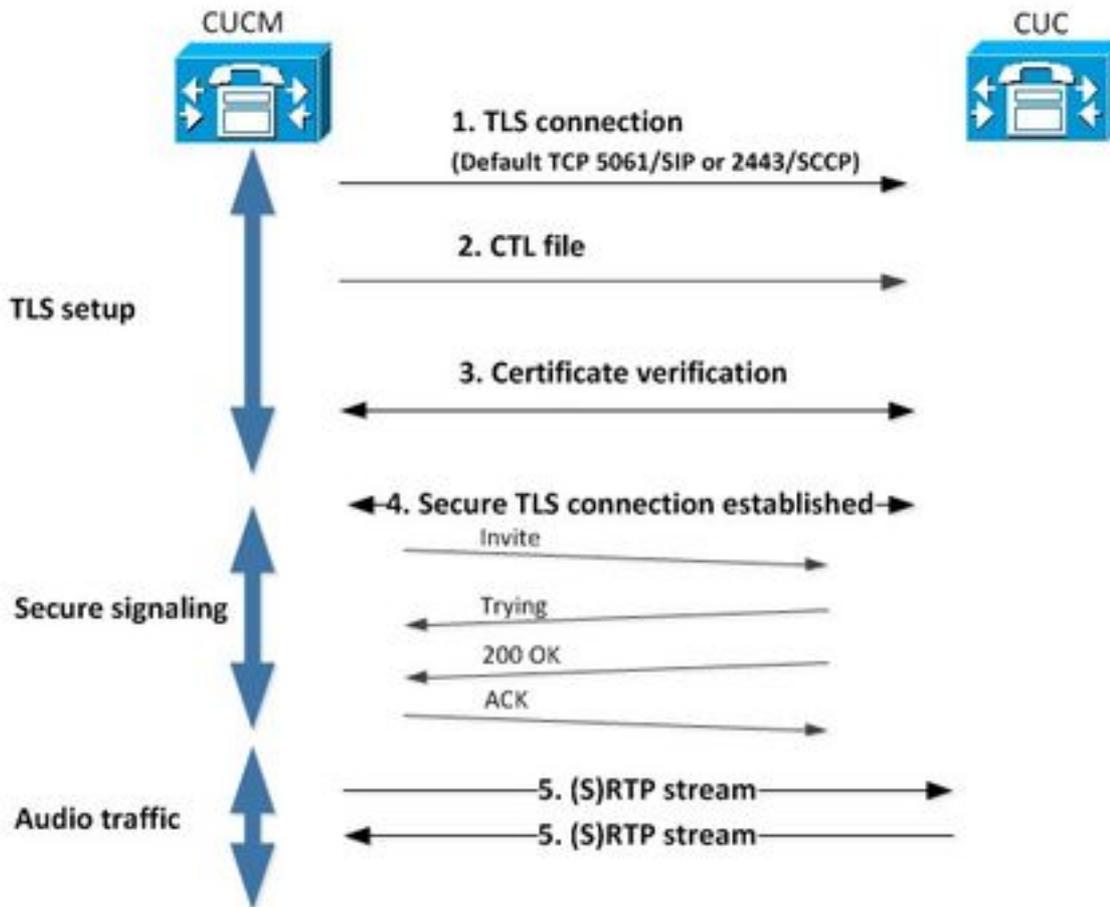
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM バージョン 10.5.2.11900-3
- CUC バージョン 10.5.2.11900-3

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。



次の図で、CUCM と CUC の間でセキュアな接続を確立するプロセスについて簡単に説明します。



1. Call Managerは、統合に使用されるプロトコルのポート2443 Skinny Call Control Protocol(SCCP)または5061 Session Initiation Protocol(SIP)ベースで、CUCサーバへのセキュアな Transport Layer Security(TLS)接続を設定します。

2. CUCサーバは、TFTPサーバから証明書信頼リスト(CTL)ファイルをダウンロードし(ワンタイムプロセス)、CallManager.pem証明書を抽出して保存します。

3. CUCMサーバは、前の手順で取得したCallManager.pem証明書に対して検証された Callmanager.pem証明書を提供します。また、CUC 証明書は CUCM に保存されている CUC ルート証明書に対して検証されています。管理者がルート証明書を CUCM にアップロードする必要があります。

4.証明書の検証が成功すると、セキュアなTLS接続が確立されます。この接続は、暗号化された SCCP シグナリングまたは SIP シグナリングの交換に使用されます。

5.音声トラフィックは、Real-time Transport Protocol(RTP)またはSRTPとして交換することができます。

注：TLS 通信が確立されると、CUCM および CUC は TLS 相互認証を使用します。詳細については、RFC5630 を参照してください。

設定：セキュア SIP トランク

CUC の設定

1. SIP証明書の追加

[CUC Administration] > [Telephony Integrations] > [Security] > [SIP Certificate] > [Add new]に移動します。

- 表示名:<any meaningful name>
- Subject Name:<any name for example, **SecureConnection**>

注:[Subject Name]は、SIPトランクセキュリティプロファイルの[X.509 Subject Name]と一致する必要があります(このドキュメントの後のCUCM設定のステップ1で設定)。

注：証明書は、CUC ルート証明書によって生成および署名されます。

2.新しい電話システムの作成またはデフォルトの電話システムの変更

[Telephony Integration] > [Phone System]に移動します。既存の電話システムを使用するか、新しい電話システムを作成することができます。

3.新しいポートグループの追加

[Phone System Basics] ページの [Related Links] ドロップダウン ボックスで、[Add Port Group] を選択して、[Go] を選択します。設定ウィンドウで、次の情報を入力します。

- [Phone System] :
- [Create From] : [Port Group Type SIP]
- [SIP Security Profile] : [5061/TLS]
- [SIP Certificate] :
- [Security Mode] : [Encrypted]
- [Secure RTP] : チェックボックスをオンにします。
- [IPv4 Address or Host Name] :

[Save] をクリックします。

New Port Group

Port Group Reset Help

Save

New Port Group

Phone System Secure SIP integration ▼

Create From Port Group Type SIP ▼
 Port Group ▼

Port Group Description

Display Name* Secure SIP integration-1

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile 5061/TLS ▼

SIP Certificate Secure SIP integration with CUCMv10.5.2 ▼

Security Mode Encrypted ▼

Secure RTP

Primary Server Settings

IPv4 Address or Host Name 10.48.47.110

IPv6 Address or Host Name

Port 5060

Save

4. サーバの編集

次の図に示すように、[Edit] > [Servers]に移動して、CUCM クラスタから TFTP サーバを追加し

ます。

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

注：正しい TFTP アドレスを指定することが重要です。CUC サーバは、説明したとおり、この TFTP から CTL ファイルをダウンロードします。

5.ポートグループのリセット

次の図に示すように、[Port Group Basics]に戻り、システムによって促されるとおりにポートグループをリセットします。

The screenshot shows the 'Port Group Basics (Secure SIP integration-1)' page. It has a menu bar with 'Port Group', 'Edit', 'Refresh', and 'Help'. Below are 'Save', 'Delete', 'Previous', and 'Next' buttons. A 'Status' section contains two warning icons and messages: 'The phone system cannot take calls if it has no ports. Use the Related Links to add ports.' and 'One or more port groups need to be reset.'. The 'Port Group' section shows 'Display Name*' as 'Secure SIP integration-1', 'Integration Method' as 'SIP', and 'Reset Status' as 'Reset Required' with a 'Reset' button.

6.ボイスメールポートの追加

[Port Group Basics]ページの[Related Links]ドロップダウンボックスで[Add Ports]を選択し、[Go]を選択します。設定ウィンドウで、次の情報を入力します。

- [Enabled] : チェックボックスをオンにします。
- [Number of Ports] :
- [Phone System] :

- [Port Group] :
- [Server] :
- [Port behavior] :

7. CUCルート証明書のダウンロード

次の図に示すように、[Telephony Integrations] > [Security] > [Root Certificate]に移動し、証明書を <filename>.0 という名前のファイルとして保存するために、URL を右クリックして [save] をクリックします (ファイル拡張子は .htm ではなく .0 にする必要があります)。



CUCM の設定

1. CUCへのトランク用SIPトランクセキュリティプロファイルの設定

[CUCM Administration] > [System] > [Security] > [SIP Trunk Security Profile] > [Add new]に移動します。

次のフィールドを適切に入力してください。

- [Device Security Mode] : [Encrypted]
- [X.509 Subject Name] : [SecureConnection]
- [Accept out-of-dialog refer] : チェックボックスをオンにします。
- [Accept unsolicited notification] : チェックボックスをオンにします。
- [Accept replaces header] : チェックボックスをオンにします。

注：[X.509 Subject Name] は、Cisco Unity Connection サーバの SIP 証明書の [Subject Name] フィールド (CUC 設定のステップ 1 で設定) と一致している必要があります。

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

Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name SecureConnection

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

2. SIPプロファイルの設定

特定の設定を適用する必要がある場合は、[Device] > [Device Settings] > [SIP Profile]に移動します。そうでない場合は、標準の SIP プロファイルを使用できます。

3. SIPトランクの作成

[Device] > [Trunk] > [Add new] に移動します。次の図に示すように、Unity Connectionとのセキュアな統合に使用するSIPトランクを作成します。

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

トランク設定の [Device Information] セクションで、次の情報を入力します。

- デバイス名:
- [Device pool] :
- [SRTP allowed] : チェックボックスをオンにします。

注 : CallManager グループ (デバイス プール設定) に CUC で設定されたすべてのサーバが含まれていることを確認します ([Port group] > [Edit] > [Servers]) 。

Trunk Configuration

Save

Status

 Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SecureSIPtoCUC
Description	Trunk for secure integration with CUC
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 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

PSTN Access
 Run On All Active Unified CM Nodes

トランク設定の [Inbound Calls] セクションで、次の情報を入力します。

- [Calling Search Space] :
- [Redirecting Diversion Header Delivery - Inbound] : チェックボックスをオンにします。

Inbound Calls

Significant Digits* All

Connected Line ID Presentation* Default

Connected Name Presentation* Default

Calling Search Space AllPhones

AAR Calling Search Space < None >

Prefix DN

Redirecting Diversion Header Delivery - Inbound

アウトバウンド トランク設定の[Calls]セクションで、次の情報を入力します。

- [Redirecting Diversion Header Delivery - Outbound] : チェックボックスをオンにします。

Outbound Calls

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

トランク設定の [SIP Information] セクションで、次の情報を入力します。

- 宛先アドレス:
- [SIP Trunk Security Profile] :
- [Rerouting Calling Search Space] :
- [Out-of-Dialog Refer Calling Search Space] :
- [SIP Profile] :

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

必要に応じて、その他の設定を調整します。

4. ルートパターンの作成

設定済みトランクを示すルートパターンを作成します ([Call Routing] > [Route/Hunt] > [Route Pattern])。ルートパターン番号として入力された内線番号は、ボイスメールパイロットとして使用できません。次の情報を入力します。

- [Route pattern] :
- [Gateway/Route list] :

The screenshot shows the 'Route Pattern Configuration' window. At the top, there is a 'Save' button. Below it, the 'Status' is 'Ready'. The 'Pattern Definition' section contains the following fields:

Route Pattern *	8000
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence *	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class *	Default
Gateway/Route List *	SecureSIPtoCUC (Eds)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

5. ボイスメールパイロットの作成

統合用のボイス メール パイロットを作成します ([Advanced Features] > [Voice Mail] > [Voice Mail Pilot])。次の値を入力してください。

- [Voice Mail Pilot Number] :
- [Calling Search Space] : パイロットとして使用されるルートパターンを含むパーティションが含まれます。

The screenshot shows the 'Voice Mail Pilot Information' window. It contains the following fields:

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

6. ボイスメールプロファイルの作成

ボイス メール プロファイルを作成して、すべての設定をリンクさせます ([Advanced Features] > [Voice Mail] > [Voice Mail Profile])。次の情報を入力します。

- [Voice Mail Pilot] :
- [Voice Mail Box Mask] :

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

7.ボイスメールプロファイルのDNへの割り当て

セキュアな統合を使用するよう意図されている DN にボイスメール プロファイルを割り当てます。DN 設定を変更したら、忘れずに [Apply Config] ボタンをクリックします。

次のとおりに移動します。[Call Routing] > [Directory number]に移動して、次の項目を変更します。

- [Voice Mail Profile] : [Secure_SIP_Integration]

Directory Number Configuration

Save Delete Reset Apply Config Add New

Directory Number Settings

Voice Mail Profile Secure_SIP_Integration (Choose <None> to use system default)

Calling Search Space < None >

BLF Presence Group* Standard Presence group

User Hold MOH Audio Source < None >

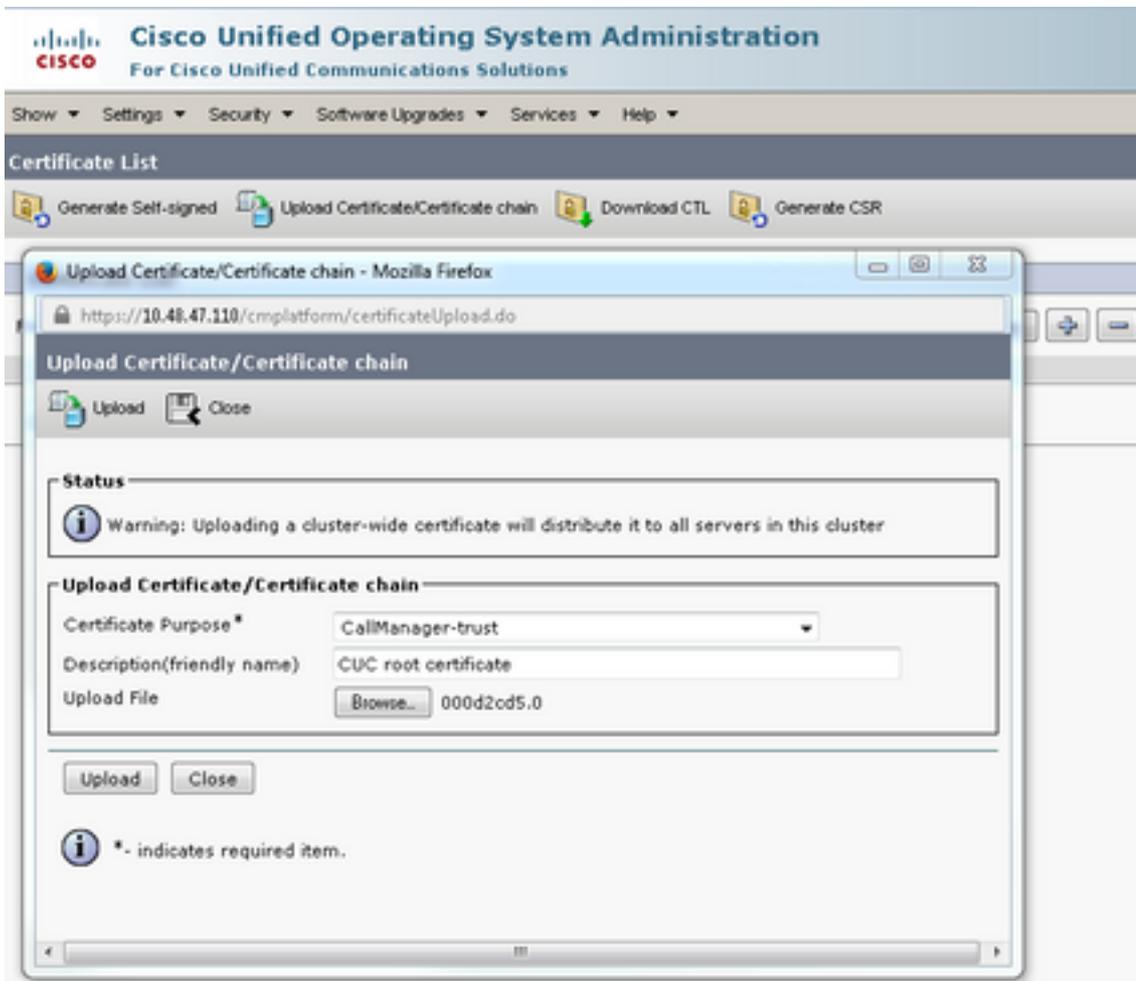
Network Hold MOH Audio Source < None >

Auto Answer* Auto Answer Off

Reject Anonymous Calls

8. CUCルート証明書をCallManager-trustとしてアップロード

[OS Administration] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain]に移動し、設定済みのすべてのノードで CUC ルート証明書を CallManager-trust としてアップロードして、CUC サーバと通信します。



注：証明書を有効にするには、証明書のアップロード後にCisco CallManagerサービスを再起動する必要があります。

セキュア SCCP ポートの設定

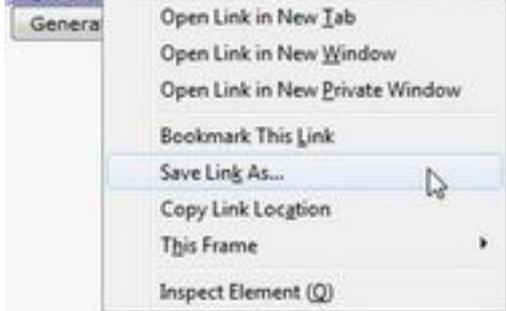
CUC の設定

1. CUC ルート証明書のダウンロード

[CUC Administration] > [Telephony Integration] > [Security] > [Root Certificate]に移動します。証明書を <filename>.0 という名前のファイルとして保存するために、URL を右クリックして [Save] をクリックします (ファイル拡張子は .htm ではなく .0 にする必要があります)。

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	<pre>-----BEGIN CERTIFICATE----- MIICPDCCAaWgAwIBAgIRAPa4+zNpFE3TnxjgZ1k67E1wDQYJKoZIhvcNAQEFBQAw OjE4MDYGA1UEAwwvQ2lyZ29Vbml0eS01ZGFkMzJlYy1jYWZlLnQ1NTktOTc0Zj01 NmYyYzY4NTBkNDEwHhcNMjUwMzE0MDY1OTM0WWhcNMjUwNDAxMDY1OTM0WjA6MTgw NgYDVQQLDDB9DaxNjb1VuaXR5LTkxYVYyZWZlLnQ1NTktOTc0Zj01OS05NzhmLTU2Zj01 Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBOBg/qh8cWQx457 Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6ouSeMiGbs757WpvTspKp+ze5DjVm2j4 B1lxG9wM3XgPPwM+3QIMh0NQFLARuJdm9g2/5uiHB6/1k82Po0Wrv2r6Anoragrv Md3JordaCB3mG1u2g0GqXj9GChf0CAwEAaANCMEEAwEgYDVR0TAQH/BAGwBgEB/wIB ADAdBgNVHQ4EFgQU438N5JYGHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAgKsMA0G CSqGSIb3DQEBBQUAA4GBAGPhrFt6GH2a0iXV8bnKvC12f5ty1eTeMD6ZzD62P4C6 RtGM88WqGU1IAZw1www0nxdetKzZvJX2z2Ksu2ptVUnFPMZSc+xl0jv7vmJq52px TcD/Ti0efckXlc+vACWlu4wlv20SHxsoto9CiiXqsKQ7e/zyYHu152zTOQeYvAES -----END CERTIFICATE-----</pre>
Private Key	Hk2Pzp3YnX3/9ghz1r8v1VgMpSLr8HZ8XW/VXIL342IudK3G1GwnZ1IMvhzta/zEseh2ELON

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



2.電話システムの作成/既存の電話システムの変更

[Telephony Integration] > [Phone System]に移動します。既存の電話システムを使用するか、新しい電話システムを作成することができます。

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*

Default TRAP Phone System

3.新しいSCCPポートグループの追加

[Phone System Basics] ページの [Related Links] ドロップダウン ボックスで、[Add Port Group] を選択して、[Go] を選択します。設定ウィンドウで、次の情報を入力します。

- [Phone system] :
- [Port group type] : SCCP
- [Device Name prefix*] : [CiscoUM1-VI]
- [MWI On extension] :
- [MWI Off extension] :

注：この設定は CUCM の設定と一致している必要があります。

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*

Integration Method

Device Name Prefix*

Reset Status

Message Waiting Indicator Settings

Enable Message Waiting Indicators

MWI On Extension

MWI Off Extension

Delay between Requests milliseconds

Maximum Concurrent Requests

Retries After Successful Attempt

Retry Interval After Successful Attempt milliseconds

Fields marked with an asterisk (*) are required.

4. サーバの編集

[Edit] > [Servers]に移動して、CUCM クラスタから TFTP サーバを追加します。

SIP Servers

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

TFTP Servers

<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input type="checkbox"/>	0	10.48.47.110 <input style="width: 100px;" type="text"/>

注：正しい TFTP アドレスを指定することが重要です。CUC サーバは、説明したとおり、この TFTP から CTL ファイルをダウンロードします。

5.セキュアSCCPポートの追加

[Port Group Basics]ページの[Related Links]ドロップダウンボックスで、[Add Ports]を選択し、[Go]を選択します。設定ウィンドウで、次の情報を入力します。

- [Enabled] : チェックボックスをオンにします。
- [Number of Ports] :
- [Phone System] :
- [Port Group] :
- [Server] :
- [Port behavior] :
- [Security Mode] : **[Encrypted]**

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

CUCM の設定

1.ポートの追加

に移動 [CUCM Administration] > [Advanced features] > [Voice Mail Port Configuration] > [Add New]。

従来どおり SCCP ボイス メール ポートを設定します。唯一の違いは、ポート設定の [Device Security Mode] で [Encrypted Voice Mail Port] オプションを選択する必要があることです。

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 >

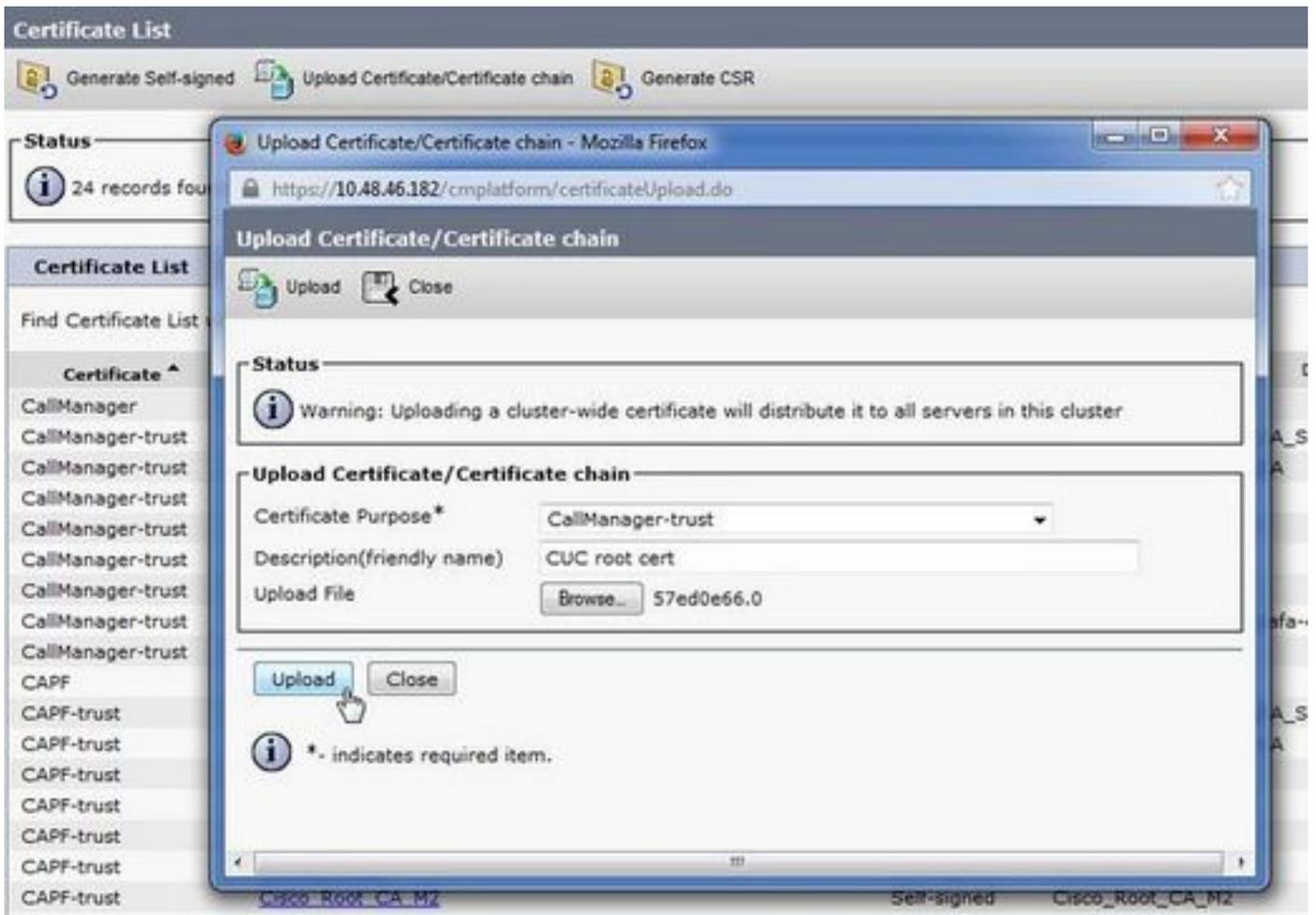
Directory Number Information

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ルート証明書をCallManager-trustとしてアップロードする

[OS Administration] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain]に移動し、設定済みのすべてのノードで CUC ルート証明書を CallManager-trust としてアップロードして、CUC サーバと通信します。



注：証明書を有効にするには、証明書のアップロード後にCisco CallManagerサービスを再起動する必要があります。

を選択します。メッセージ受信情報 (MWI) オン/オフの内線番号

[CUCM Administration] > [Advanced Features] > [Voice Mail Port Configuration]に移動して、[MWI On/Off Extensions] を設定します。MWI 番号は、CUC 設定と一致している必要があります。

Message Waiting Information

Message Waiting Number*	999991
Partition	< None >
Description	MWI on
Message Waiting Indicator*	<input checked="" type="radio"/> On <input type="radio"/> Off
Calling Search Space	< None >

Save

Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* On Off

Calling Search Space < None >

Save

4.ボイスメールパイロットの作成

統合用のボイスメールパイロットを作成します ([Advanced Features] > [Voice Mail] > [Voice Mail Pilot])。次の値を入力してください。

- [Voice Mail Pilot Number] :
- [Calling Search Space] : パイロットとして使用されるルートパターンを含むパーティションが含まれます。

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.ボイスメールプロファイルの作成

ボイスメールプロファイルを作成して、すべての設定をリンクさせます ([Advanced Features] > [Voice Mail] > [Voice Mail Profile])。次の情報を入力します。

- [Voice Mail Pilot] :
- [Voice Mail Box Mask] :

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.ボイスメールプロファイルのDNへの割り当て

セキュアな統合を使用するよう意図されている DN にボイスメールプロファイルを割り当てます。DN 設定を変更したら、[Apply Config] ボタンをクリックします。

[Call Routing] > [Directory number]に移動して、次の項目を変更します。

- [Voice Mail Profile] : [Voicemail-profile-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 >	

Reject Anonymous Calls

7. ボイス メール ハント グループの作成

a)新しい回線グループを追加します([コールルーティング]>[ルート/ハント]>[回線グループ])

- Line Group Information

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

b)新しいボイスメールのハントリストを追加します([Call Routing]>[Route/Hunt]>[Hunt List])

Hunt List Information

Device is trusted

Name*	voicemail-hl
Description	
Cisco Unified Communications Manager Group*	Default

Enable this Hunt List (change effective on Save; no reset required)

For Voice Mail Usage

c)新しいハントパイロットを追加する([コールルーティング]>[ルート/ハント]>[ハントパイロット])

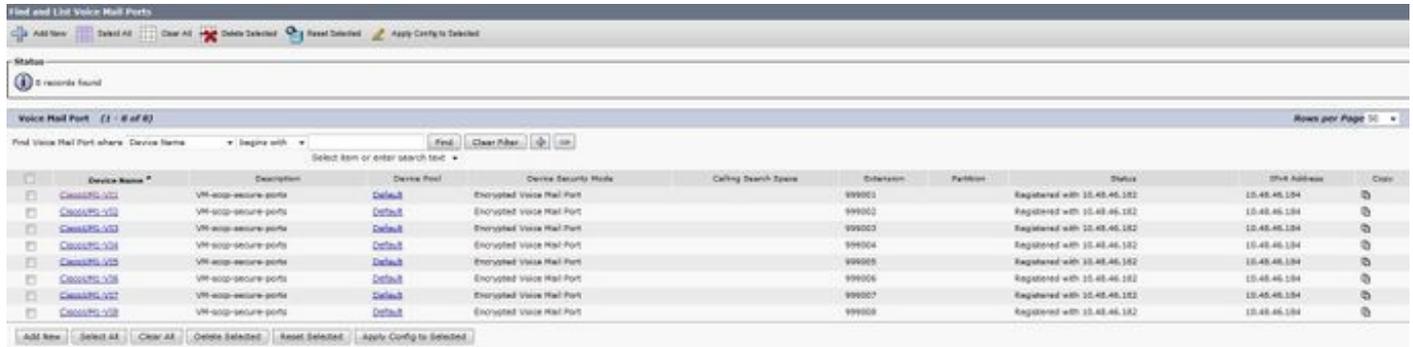
Pattern Definition

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

確認

SCCP ポートの検証

[CUCM Administration] > [Advance Features] > [Voice Mail] > [Voice Mail Ports]に移動して、ポート登録を検証します。



Device Name	Description	Device Pool	Device Security Mode	Calling Search Space	Extension	Partition	Status	IP Address	Class
CiscoUC-V02	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999001		Registered with 10.45.46.182	10.45.46.184	
CiscoUC-V03	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999002		Registered with 10.45.46.182	10.45.46.184	
CiscoUC-V04	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999003		Registered with 10.45.46.182	10.45.46.184	
CiscoUC-V05	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999004		Registered with 10.45.46.182	10.45.46.184	
CiscoUC-V06	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999005		Registered with 10.45.46.182	10.45.46.184	
CiscoUC-V07	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999006		Registered with 10.45.46.182	10.45.46.184	
CiscoUC-V08	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999007		Registered with 10.45.46.182	10.45.46.184	
CiscoUC-V09	VM-ecp-secure-ports	Default	Encrypted Voice Mail Port		999008		Registered with 10.45.46.182	10.45.46.184	

電話の [Voice Mail] ボタンを押して、ボイス メールを送信します。Unity Connection システムでユーザの内線番号が設定されていない場合、オープニング グリーティングを聞く必要があります。

セキュア SIP トランクの検証

電話の [Voice Mail] ボタンを押して、ボイス メールを送信します。Unity Connection システムでユーザの内線番号が設定されていない場合、オープニング グリーティングを聞く必要があります。

または、SIP OPTION のキープアライブを有効にして、SIP トランクのステータスをモニタすることができます。このオプションは、SIP トランクに割り当てられた SIP プロファイルで有効にできます。このオプションを有効にすると、次の図に示すように、[Device] > [Trunk] 経由で SIP トランクのステータスをモニタできます。



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

セキュア RTP コールの検証

鍵マークのアイコンが Unity Connection へのコールに表示されるかどうかを検証します。これは、次の図に示すように、RTP ストリームが暗号化されていることを意味します (機能させるには、デバイス セキュリティ プロファイルがセキュアである必要があります)。



トラブルシュート

1.一般的なトラブルシューティングのヒント

セキュアな統合をトラブルシューティングするには、次の手順を実行します。

- 設定を確認します。
- すべての関連サービスが実行されていることを確認します (CUCM : CallManager、TFTP、CUC : Conversation Manager)。
- サーバ間のセキュアな通信に必要なポート (SCCP 統合用の TCP ポート 2443 および SIP 統合用の TCP 5061) がネットワークで開いていることを確認します。
- これらのすべてが適切な場合、トレース収集に進みます。

2.収集するトレース

次のトレースを収集して、セキュアな統合をトラブルシューティングします。

- CUCM および CUC からのパケット キャプチャ
- CallManager トレース
- Cisco Conversation Manager トレース

詳細については、次の関連資料を参照してください。

CUCM でパケット キャプチャを実行する方法 :

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

CUC サーバでトレースを有効にする方法 :

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

一般的な問題

ケース 1：セキュアな接続を確立できない (不明な CA アラート)

いずれかのサーバからパケット キャプチャを収集すると、TLS セッションが確立されます。

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

クライアントは、サーバから送信された証明書を検証できなかったため、不明な CA の致命的なエラーでサーバにアラートを発行しました。

次の 2 つの可能性が 있습니다。

1) CUCMがアラートを送信する 不明なCA

- 最新の CUC ルート証明書が CUC サーバと通信するサーバにアップロードされていることを確認します。
- CallManager サービスが、対応するサーバで再起動されていることを確認します。

2) CUCが不明CAアラートを送信

- CUC サーバの [Port Group] > [Edit] > [Servers] 設定に TFTP の IP アドレスが正しく入力されていることを確認します。
- 接続サーバから CUCM TFTP サーバに到達できることを確認します。
- CUCM TFTPのCTLファイルが最新であることを確認します (「show ctl」の出力をOS Adminページに表示される証明書と比較します)。最新でなければ、CTLClient を再実行します。
- CUCサーバをリブートするか、ポートグループを削除して再作成し、CUCM TFTPから CTLファイルを再ダウンロードします。

ケース 2：CUCM TFTP から CTL ファイルをダウンロードできない

このエラーは、Conversation Manager のトレースで見られます。

```
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:

ソリューション :

1. [Port group] > [Edit] > [Servers]の設定でTFTPサーバが正しいことを再確認してください。
2. CUCMクラスタがセキュアモードであることを確認します。
3. CTLファイルがCUCM TFTPに存在することを確認します。

ケース 3 : ポートが登録されない

このエラーは、Conversation Manager のトレースで見られます。

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

ソリューション :

1.これは、CUCMとCUCでCTLファイルのmd5チェックサムが再生成された結果として一致していないことが原因である可能性が高いです

考えられます。CUC サーバを再起動して、CTL ファイルを更新します。

シスコ内部情報

または、次のようにルートから CTL ファイルを削除できます。

/tmp/ フォルダから CTL ファイルを削除して、ポート グループをリセットします。
削除する前に、ファイルで md5 チェックサムを実行して

比較することができます。

```
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 ユーザデバイス6120 Feb 5 15:29 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

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

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

さらに、このトラブルシューティング ガイドを参照できます。

不具合

[CSCum48958 : CUCM 10.0 \(IP アドレスの長さが正しくない \)](#)

[CSCtn87264 : セキュア SIP ポートの TLS 接続が失敗する](#)

[CSCur10758 : 取り消された証明書を Unity Connection で消去できない](#)

[CSCur10534 : Unity Connection 10.5 TLS/PKI の相互運用における冗長な CUCM](#)

[CSCve47775:CUCでCUCMのCTLFileを更新および確認する方法の機能要求](#)