

# CA署名付き証明書を使用したCommunications ManagerでのSIP TLSトランクの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ1:Windows Server 2003でパブリックCAまたはセットアップCAを使用する](#)

[ステップ2: ホスト名と設定の確認](#)

[ステップ3: 証明書署名要求 \( CSR \) の生成とダウンロード](#)

[ステップ4: Microsoft Windows 2003 認証機関による CSR の署名](#)

[ステップ5: CA からのルート証明書の取得](#)

[ステップ6: CallManager Trust としての CA ルート証明書のアップロード](#)

[ステップ7: CallManager 証明書としての CA 署名 CallManager CSR 証明書のアップロード](#)

[ステップ8: SIP トランク セキュリティ プロファイルの作成](#)

[ステップ9: SIP トランクの作成](#)

[ステップ10: ルート パターンの作成](#)

[確認](#)

[トラブルシューティング](#)

[CUCM でのパケット キャプチャの収集](#)

[CUCM トレースの収集](#)

## 概要

このドキュメントでは、認証機関 ( CA ) 署名付き証明書を使用して Communications Manager で Session Initiation Protocol ( SIP ) Transport Layer Security ( TLS ) トランクを構成するための順を追ったプロセスについて説明します。

このドキュメントに従った後、2 つのクラスター間の SIP メッセージは、TLS を使用して暗号化されます。

## 前提条件

### 要件

以下について十分に理解しておくことをお勧めします。

- Cisco Unified Communications Manager ( CUCM )
- SIP

## 使用するコンポーネント

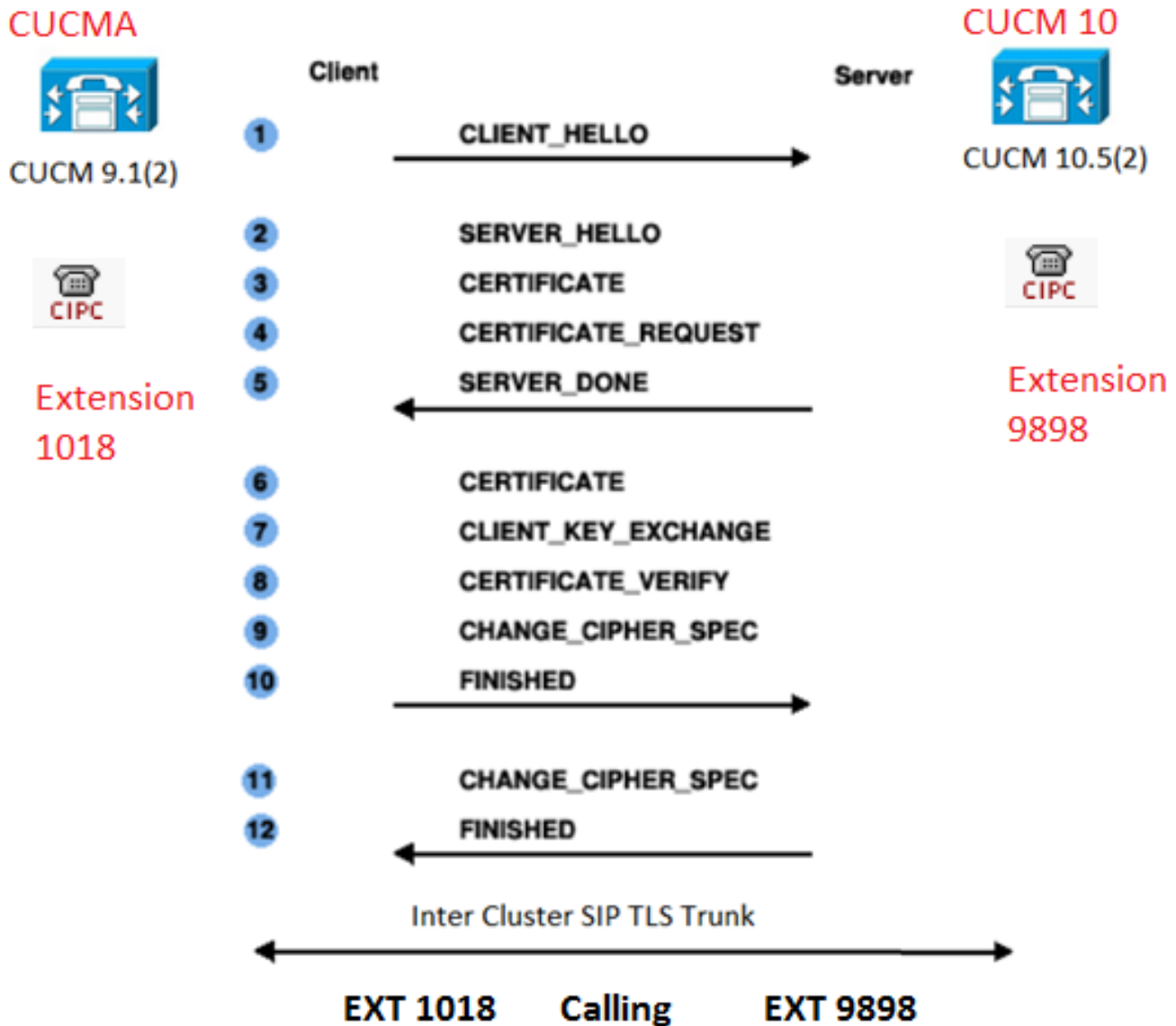
このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- CUCM バージョン 9.1(2)
- CUCM バージョン 10.5(2)
- CA としての Microsoft Windows Server 2003

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。

## 背景説明

証明書を使用する SSL ハンドシェイクについて、以下の図を参照してください。



ステップ1:Windows Server 2003でパブリックCAまたはセットアップCAを使用する

次のリンクを参照してください。 [Windows 2003 Sever での CA のセットアップ](#)

ステップ2：ホスト名と設定の確認

証明書は名前で識別されます。開始する前に、名前が正しいことを確認します。

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

ホスト名を変更するには、次のリンクを参照してください。 [CUCM のホスト名の変更](#)

ステップ3：証明書署名要求 (CSR) の生成とダウンロード

## CUCM 9.1(2)

CSR を生成するには、[OS Admin] > [Security] > [Certificate Management] > [Generate CSR] に移動します。

[Certificate Name] フィールドで、ドロップダウンリストから [CallManager] オプションを選択します。

The screenshot shows a dialog box titled "Generate Certificate Signing Request". At the top, there are two buttons: "Generate CSR" and "Close". Below this is a "Status" section with a warning icon and the text: "Warning: Generating a new CSR will overwrite the existing CSR". The main section is titled "Generate Certificate Signing Request" and contains a "Certificate Name\*" dropdown menu with "CallManager" selected. At the bottom, there are two buttons: "Generate CSR" and "Close".

CSR をダウンロードするには、[OS Admin] > [Security] > [Certificate Management] > [Download CSR] に移動します。

[Certificate Name] フィールドで、ドロップダウンリストから [CallManager] オプションを選択します。

**Download Certificate Signing Request**

Download CSR Close

**Status**

! Certificate names not listed below do not have a corresponding CSR

**Download Certificate Signing Request**

Certificate Name\* CallManager



Download CSR Close

## CUCM 10.5(2)

CSR を生成するには、[OS Admin] > [Security] > [Certificate Management] > [Generate CSR] に移動します。

1. [Certificate Purpose]フィールドで、ドロップダウンリストから[CallManager]を選択します。
2. [キーの長さ]フィールドで、ドロップダウンリストから[1024]を選択します。
3. [ハッシュアルゴリズム]フィールドで、ドロップダウンリストから[SHA1]を選択します。

## Generate Certificate Signing Request

 Generate  Close

### Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

### Generate Certificate Signing Request

Certificate Purpose\*

Distribution\*

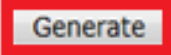
Common Name\*

#### Subject Alternate Names (SANs)

Parent Domain

Key Length\*

Hash Algorithm\*



 Generate

 Close

CSR をダウンロードするには、[OS Admin] > [Security] > [Certificate Management] > [Download CSR] に移動します。

[Certificate Purpose] フィールドで、ドロップダウンリストから [CallManager] オプションを選択します。

## Download Certificate Signing Request

 Download CSR  Close

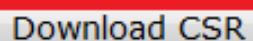
### Status



Certificate names not listed below do not have a corresponding CSR

### Download Certificate Signing Request

Certificate Purpose\*

 Download CSR

 Close

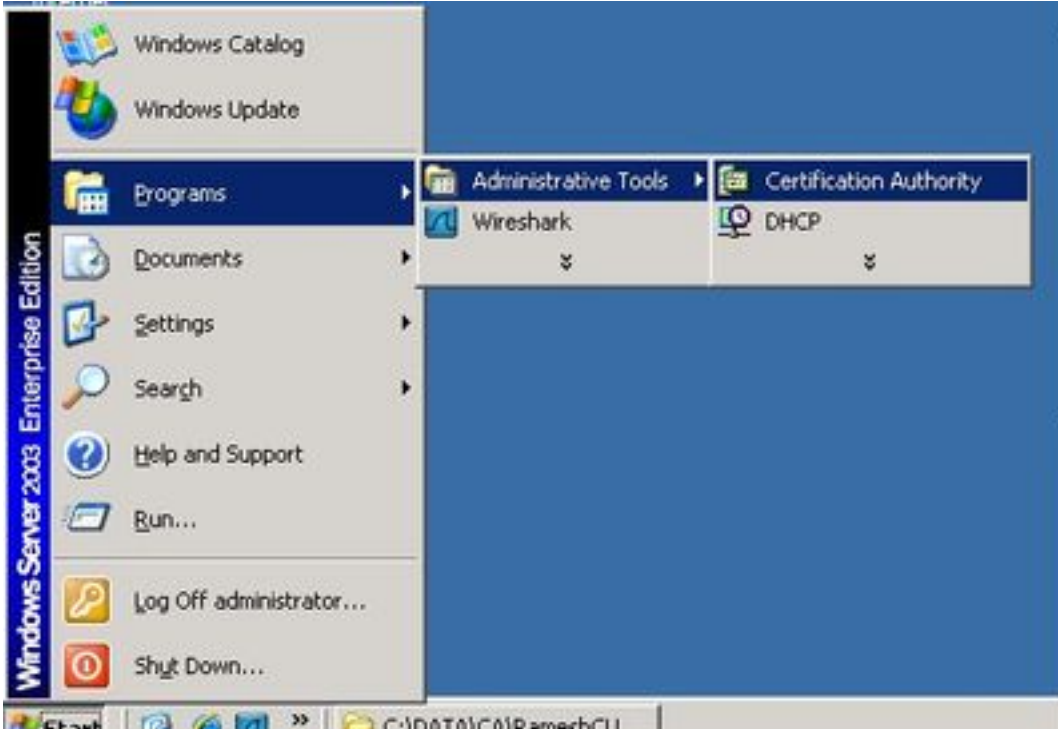
注：CallManager CSR は、1024 ビットの Rivest-Shamir-Addleman ( RSA ) キーを使用し

て生成されます。

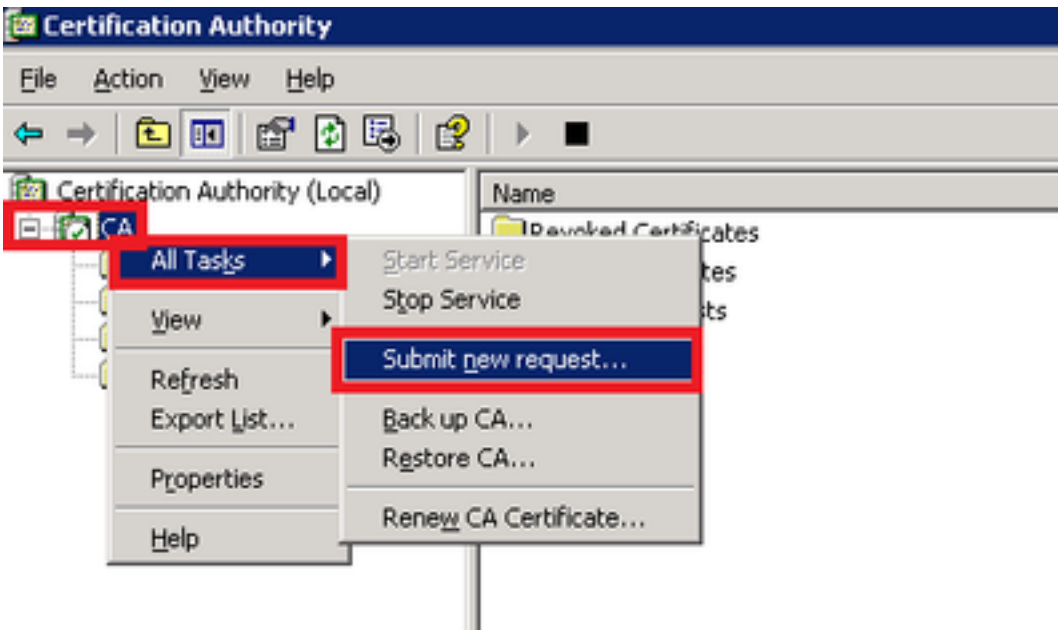
#### ステップ 4 : Microsoft Windows 2003 認証機関による CSR の署名

これは Microsoft Windows 2003 CA によって CSR に署名するオプション情報です。

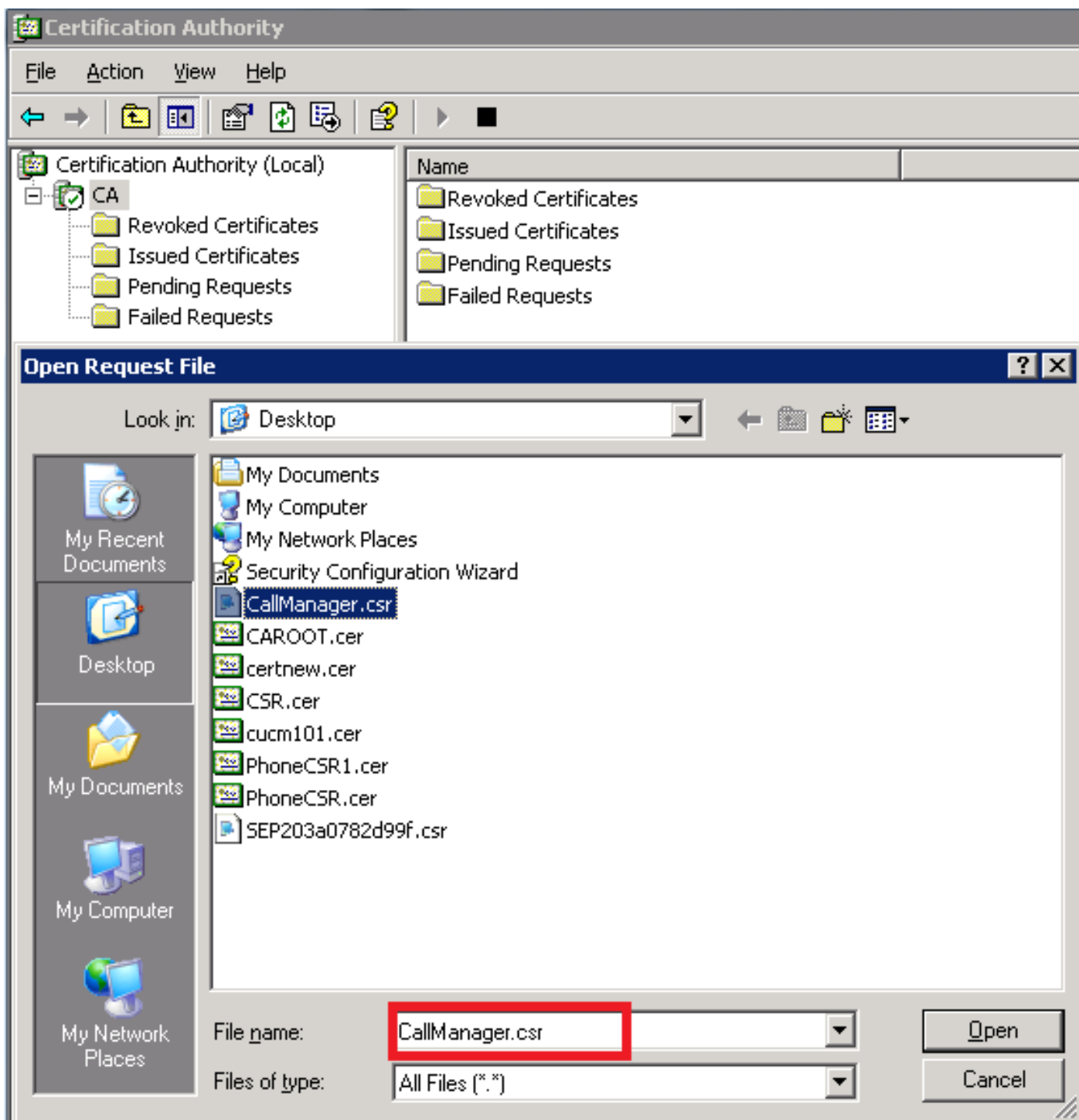
##### 1. 証明機関を開きます。



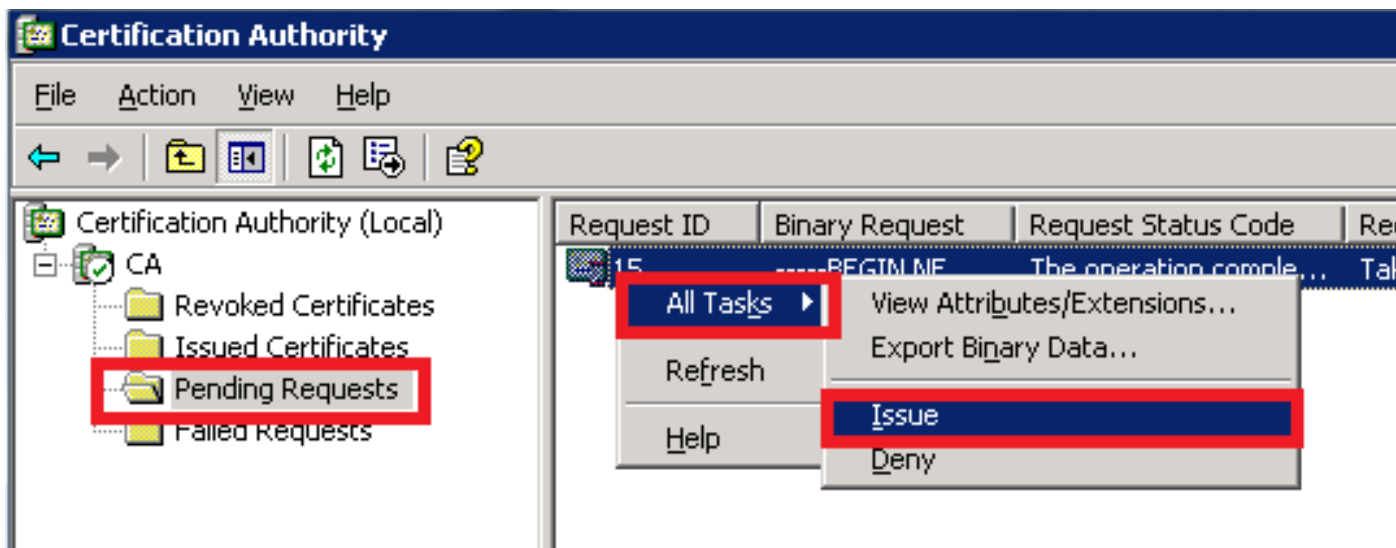
##### 2. CAアイコンを右クリックし、[All Tasks] > [Submit new request]に移動します



##### 3. CSRを選択し、[Open]オプションをクリックします(CSR(CUCM 9.1(2)とCUCM 10.5(2)の両方で適用可能)。

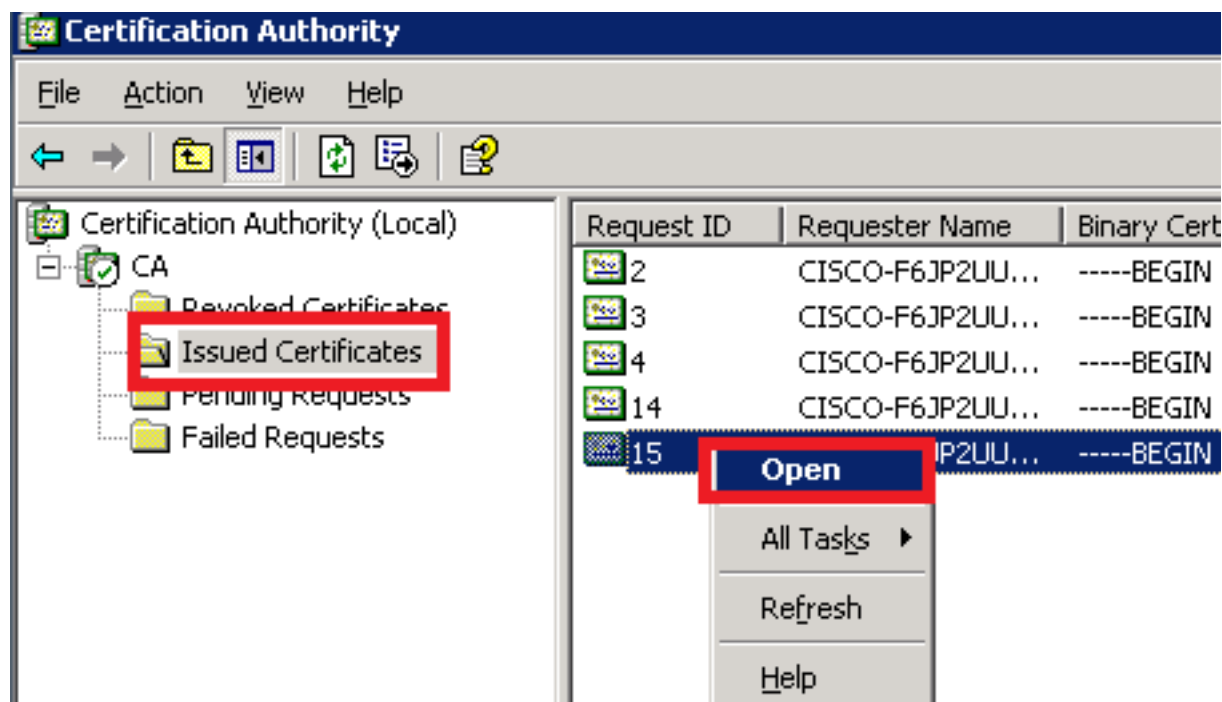


4.開いているすべてのCSRが[Pending Requests]フォルダに表示されます。各 CSR を右クリックし、証明書を発行するために [All Tasks] > [Issue] に移動します。( CSR ( CUCM 9.1(2) と CUCM 10.5(2) ) に適用可能 )



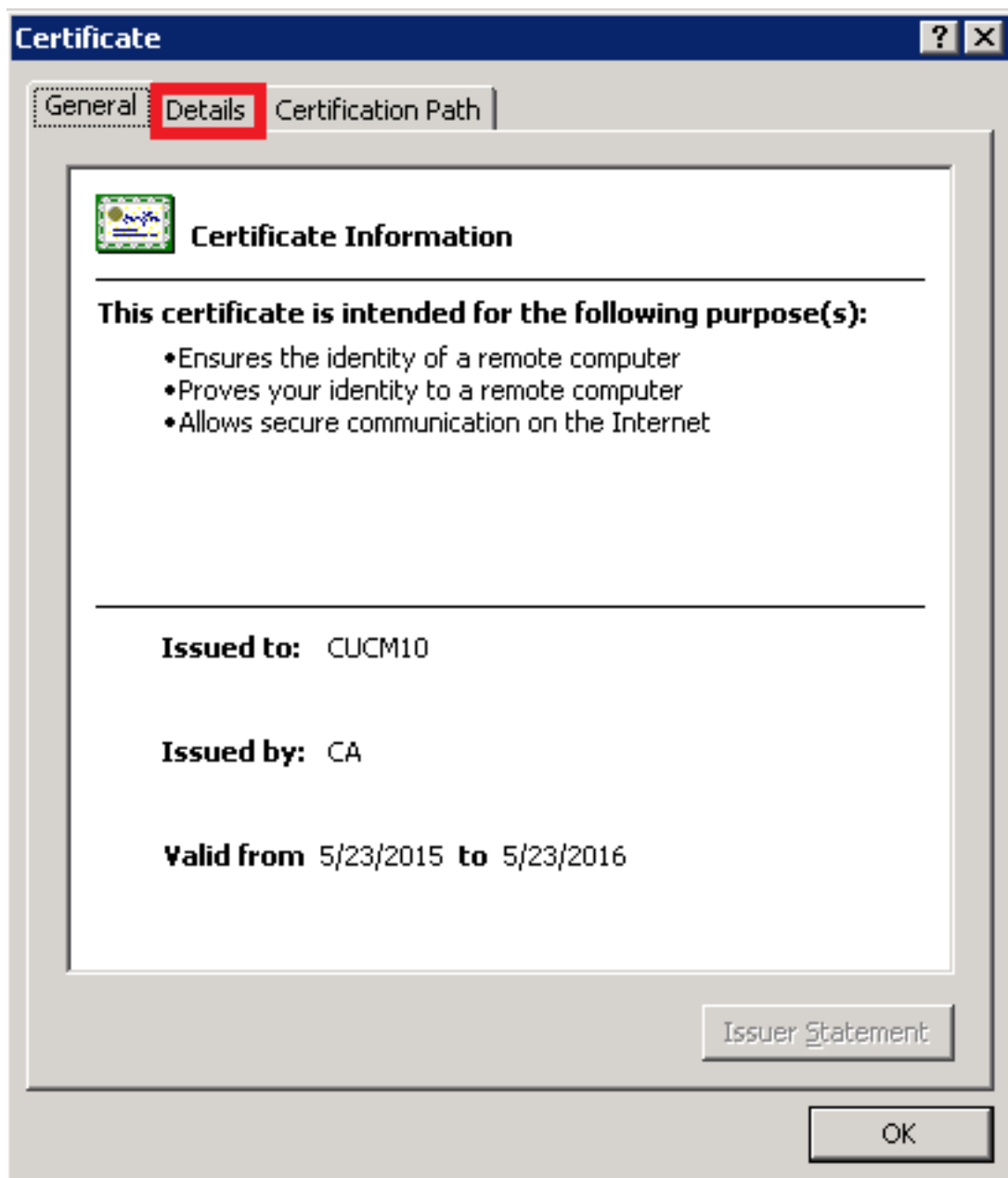
5. 証明書をダウンロードするには、[Issued Certificates] フォルダを選択します。

証明書を右クリックし、[Open] オプションをクリックします。

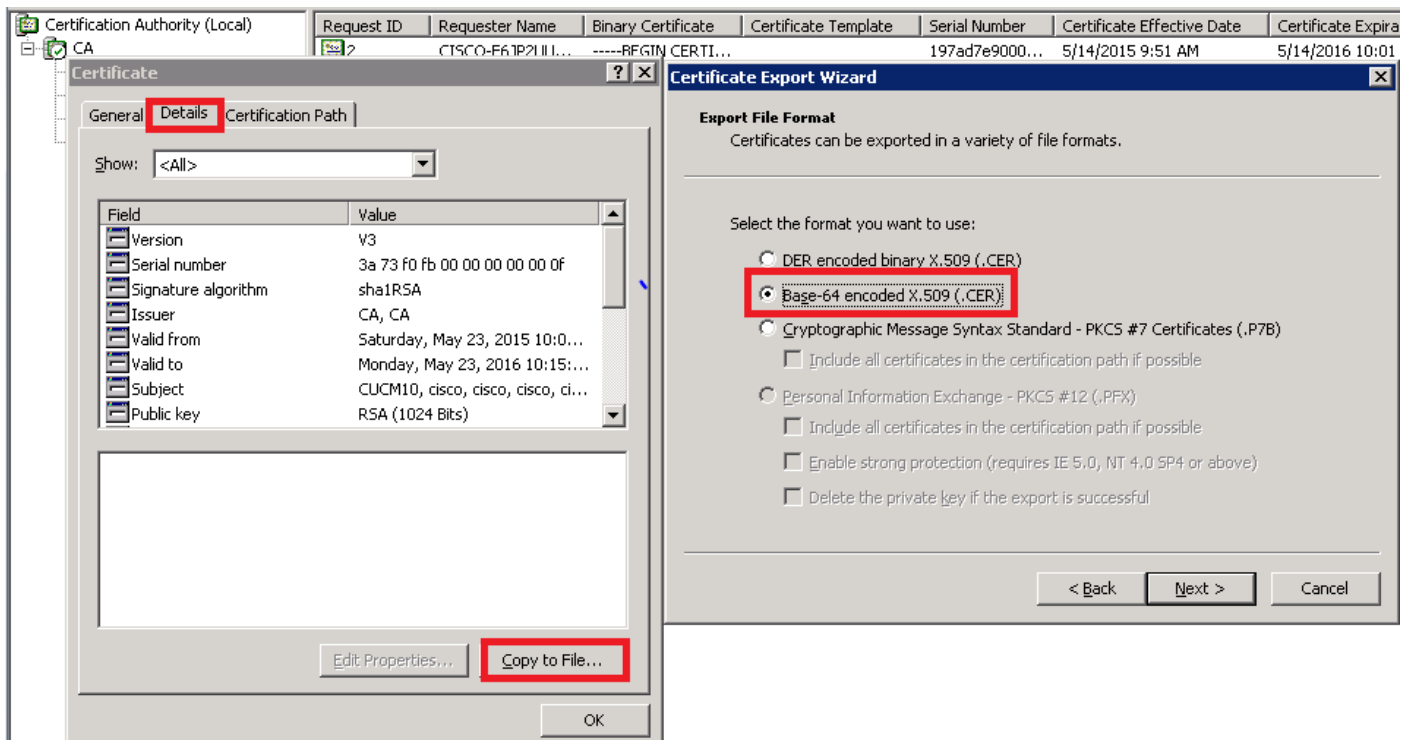


6. 証明書の詳細が表示されます。証明書をダウンロードするには、[Details] タブを選択し、[Copy to File...] ボタンをクリックします。

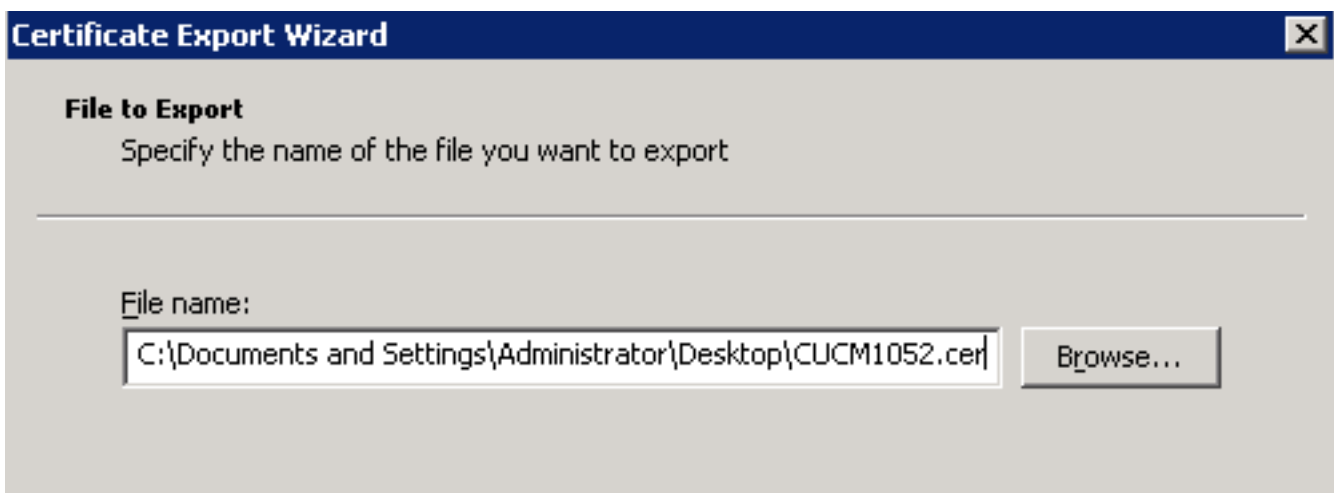




7. [証明書のエクスポートウィザード]ウィンドウで、[Base-64 encoded X.509(.CER)]オプションボタンをクリックします。



8. ファイルに正確な名前を付けます。この例では、**CUCM1052.cer**形式を使用します。



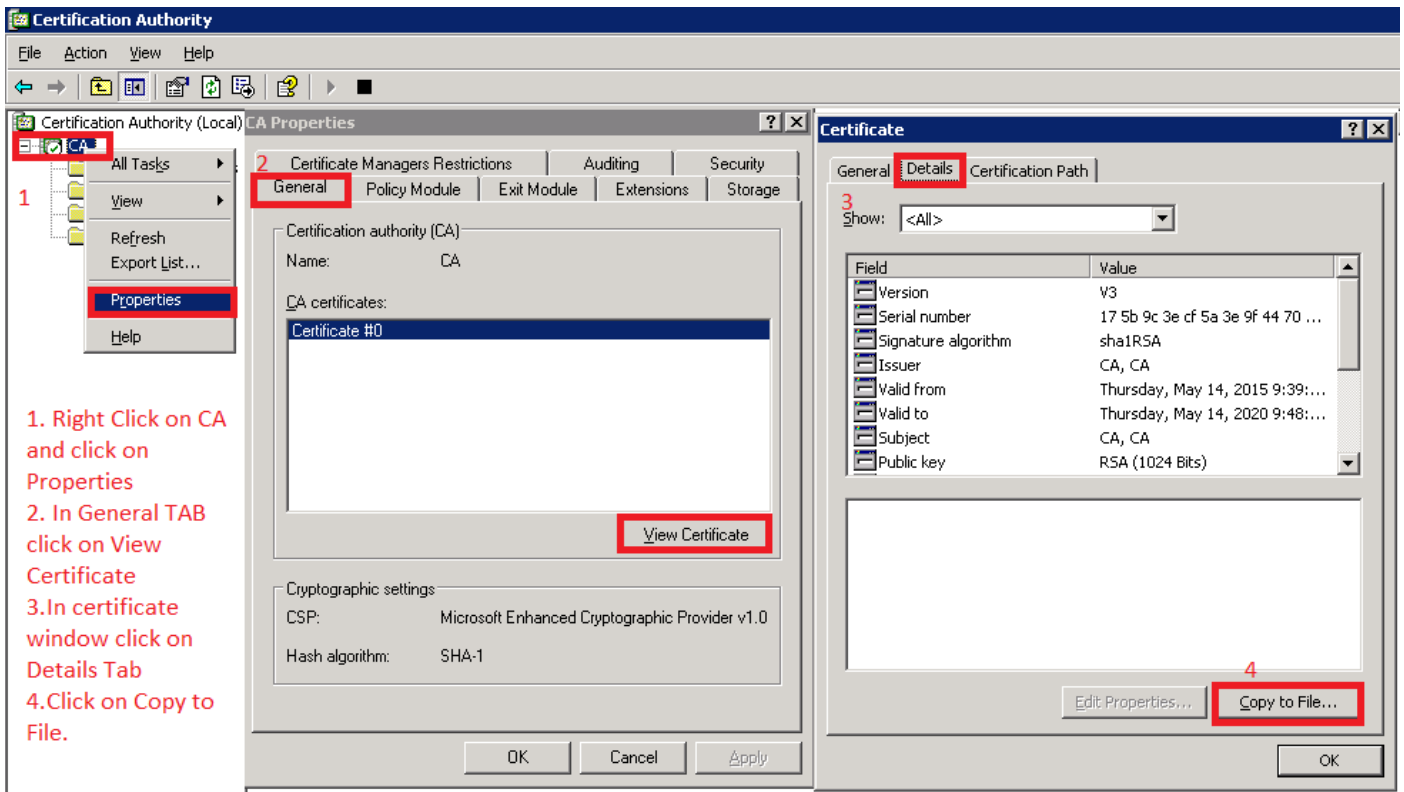
CUCM 9.1(2) で、同じ手順に従います。

ステップ 5 : CA からのルート証明書の取得

[Certification Authority] ウィンドウを開きます。

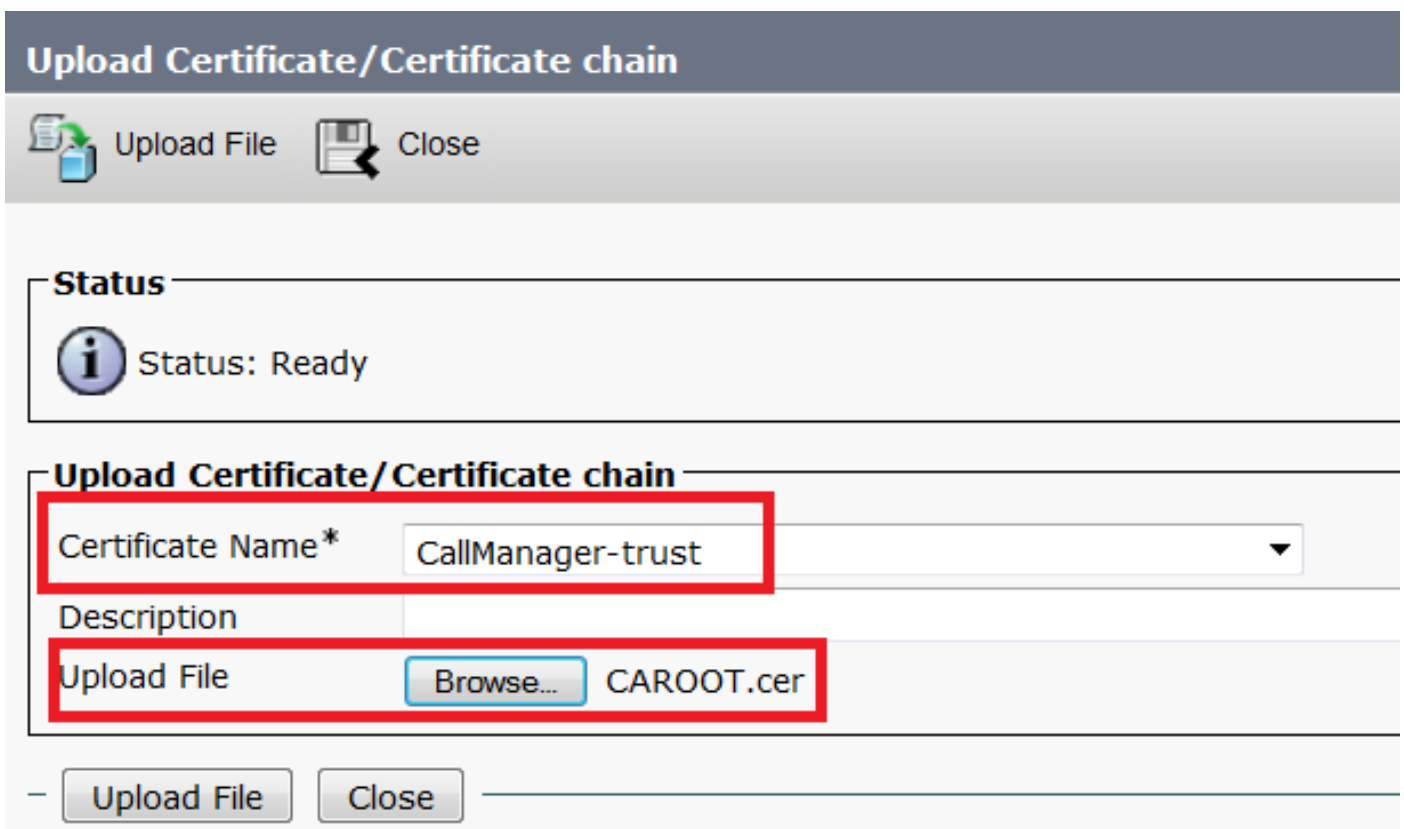
ルート CA をダウンロードするには、次の手順を実行します。

1. CAアイコンを右クリックし、[Properties]オプションをクリックします。
2. [全般]タブで、[証明書の表示]をクリックします。
3. [証明書]ウィンドウで、[詳細]タブをクリックします。
4. 「ファイルにコピー...」をクリックします。



ステップ 6 : CallManager Trust としての CA ルート証明書のアップロード

CA ルート証明書をアップロードするには、[OS Admin] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain] にログインします。



注 : 両方の CUCM ( CUCM 9.1(2) と CUCM 10.5(2) ) でこれらの手順を実行します。

ステップ 7 : CallManager 証明書としての CA 署名 CallManager CSR 証明書のアップロード

CA 署名 CallManager CSR をアップロードするには、[OS Admin] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain] にログインします。

**Upload Certificate/Certificate chain**

Upload File Close

**Status**

**i** Status: Ready

**Upload Certificate/Certificate chain**

Certificate Name\* CallManager

Description Self-signed certificate

Upload File Browse... CUCM9.cer

Upload File Close

注：両方の CUCM ( CUCM 9.1(2) と CUCM 10.5(2) ) でこれらの手順を実行します。

ステップ 8 : SIP トランク セキュリティ プロファイルの作成

### CUCM 9.1(2)

SIP トランク セキュリティ プロファイルを作成するには、[System] > [Security] > [SIP Trunk Security Profile] に移動します。

既存の Non Secure SIP Trunk Profile をコピーし、それに新しい名前を付けます。この例では、Non Secure SIP Trunk Profile が Secure SIP Trunk Profile TLS で名前変更されています。

## SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

### SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS	
Description	Secure SIP Trunk Profile authenticated by null String	
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	CUCM10	This Name should be CN of CUCM 10.5(2)
Incoming Port*	5061	
<input type="checkbox"/> Enable Application level authorization		
<input type="checkbox"/> Accept presence subscription		
<input type="checkbox"/> Accept out-of-dialog refer**		
<input type="checkbox"/> Accept unsolicited notification		
<input type="checkbox"/> Accept replaces header		
<input checked="" type="checkbox"/> Transmit security status		
<input type="checkbox"/> Allow charging header		
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter	

この図に示されているように、[X.509 Subject Name] では、CUCM 10.5(2) ( CA 署名証明書 ) の共通名 ( CN ) を使用します。

## Certificate Settings

Locally Uploaded	23/05/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by CA

## Certificate File Data

```
[
Version: V3
Serial Number: 398B1DA600000000000E
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CA, DC=CA
Validity From: Sat May 23 17:50:42 IST 2015
             To:  Mon May 23 18:00:42 IST 2016
Subject Name: CN=CUCM10, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100bcf093aa206190fe76abe13e3bd3ec45cc8b2afeee86e8393f568e1c9aa0c5fdf3f044eebc
f2d999ed8ac3592220fef3f9dcf2d2e7e939a4b26896152ebb250e407cb65d9e04bf71e8c345633786041e
5c806405160ac42a7133d7d644294226b850810fffd001e5bf2b39829b1fb27f126624e5011f151f0ef07c7
eccb734710203010001
Extensions: 6 present
]
```

## CUCM 10.5(2)

[System] > [Security] > [SIP Trunk Security Profile] に移動します。

既存の Non Secure SIP Trunk Profile をコピーし、それに新しい名前を付けます。この例では、Non Secure SIP Trunk Profile が Secure SIP Trunk Profile TLS で名前変更されています。

## SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

### SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS
Description	Secure SIP Trunk Profile authenticated by null String
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	CUCMA <span style="color: red;">This Name should be CN of CUCM 9.1(2)</span>
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input checked="" type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

強調表示されているように、[X.509 Subject Name] では、CUCM 9.1(2) ( CA 署名証明書 ) の CN を使用します。

File Name	CallManager.pem
Certificate Name	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description	Certificate Signed by CA

#### Certificate File Data

```
[
Version: V3
Serial Number: 120325222815121423728642
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CA, DC=CA
Validity From: Thu May 14 09:51:09 IST 2015
To: Sat May 14 10:01:09 IST 2016
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100916c34c9700ebe4fc463671926fa29d5c98896df275ff305f80ee0c7e9dbf6e90e74cd5c44b5b26
be0207bf5446944aef901ee5c3daefdb2cf4cbc870f8e1da5c678bc1629702b2f2bbb8e45de83579f4141ee5c53d
ab8a7af5149194cce07b7ddc101ce0e860dad7fd01cc613fe3f1250203010001
Extensions: 6 present
[
Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
Critical: false
Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
```

どちらの SIP トランク セキュリティ プロファイルも、着信ポートとして 5061 を設定します。その場合、それぞれのクラスターが TCP ポート 5061 で新しいインバウンド SIP TLS 発信をリッスンします。

#### ステップ 9: SIP トランクの作成

セキュリティ プロファイルを作成した後、SIP トランクを作成し、SIP トランクの次の設定パラメータの変更を行います。

#### CUCM 9.1(2)

1. SIP の [Trunk Configuration] ウィンドウで、設定パラメータ [SRTP Allowed] チェックボックスにチェックします。

これにより、このトランクを介した発信で使用される Real-time Transport Protocol ( RTP ) が保護されます。このボックスは、SIP TLS を使用するときだけチェックする必要があります。Secure Real-time Transport Protocol ( SRTP ) のキーは、SIP メッセージの本文で交換されるからです。SIP シグナリングは TLS で保護する必要があります。そうしないと、非セキュア SIP シグナリングを持つどのユーザも、対応する SRTP ストリームをトランクを介して復号できるようになってしまいます。



**Trunk Configuration**

Save Delete Reset Add New

**Status**  
 Status: Ready

**Device Information**

Product: SIP Trunk  
 Device Protocol: SIP  
 Trunk Service Type: None(Default)  
 Device Name\*: CUCM10  
 Description:  
 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

2. SIP の [Trunk Configuration] ウィンドウの [SIP Information] セクションで、[Destination Address]、[Destination Port]、および [SIP Trunk Security Profile] を追加します。

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.200		5061

MTP Preferred Originating Codec\*: 711ulaw  
 BLF Presence Group\*: Standard Presence group  
 SIP Trunk Security Profile\*: Secure SIP Trunk Profile TLS  
 Rerouting Calling Search Space: < None >  
 Out-Of-Dialog Refer Calling Search Space: < None >  
 SUBSCRIBE Calling Search Space: < None >  
 SIP Profile\*: Standard SIP Profile  
 DTMF Signaling Method\*: No Preference

## CUCM 10.5(2)

1. SIP の [Trunk Configuration] ウィンドウで、設定パラメータ [SRTP Allowed] チェックボックスにチェックします。

これにより、このトランクを介した発信で SRTP を使用できるようになります。このボックスは、SIP TLS を使用するときだけチェックする必要があります。SRTP のキーは、SIP メッセージの本文で交換されるからです。SIP シグナリングは TLS で保護する必要があります。そうしないと、非セキュア SIP シグナリングを持つどのユーザも、対応するセキュア RTP ストリームをトランクを介して復号できるようになってしまいます。

**Trunk Configuration**

Save Delete Reset Add New

**SIP Trunk Status**

Service Status: Unknown - OPTIONS Ping not enabled  
Duration: Unknown

**Device Information**

Product: SIP Trunk  
Device Protocol: SIP  
Trunk Service Type: None(Default)  
Device Name\*: CUCMA  
Description:  
Device Pool\*: HQ  
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

2. SIP の [Trunk Configuration] ウィンドウの [SIP Information] セクションで、[Destination IP Address]、[Destination Port]、および [Security Profile] を追加します。

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.203		5061

MTP Preferred Originating Codec\*: 711ulaw  
BLF Presence Group\*: Standard Presence group  
SIP Trunk Security Profile\*: Secure SIP Trunk Profile TLS  
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

#### ステップ 10: ルート パターンの作成

最も簡単な方法は、各クラスタに、SIP トランクを直接指すルート パターンを作成することです。ルート グループとルート リストも使用できます。

CUCM 9.1(2) は、CUCM 10.5(2) への TLS SIP トランクを経由して [Route Pattern] 9898 を指します。

Trunks (1 - 1 of 1)											Rows per Page 50			
Find Trunks where Device Name begins with											Find	Clear Filter	+	-
Select item or enter search text														
Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Security Profile					
CUCM10			Default	9898				SIP Trunk	Secure SIP Trunk Profile TLS					
Add New											Select All	Clear All	Delete Selected	Reset Selected

CUCM 10.5(2) は、CUCM 9.1(2) への TLS SIP トランクを経由して [Route Pattern] 1018 を指します。

Trunks (1 - 1 of 1)											Rows per Page 50			
Find Trunks where Device Name begins with											Find	Clear Filter	+	-
Select item or enter search text														
Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Profile			
CUCMA			HQ	1018				SIP Trunk	Unknown - OPTIONS Ping not enabled		Secure SIP Trunk Profile TLS			
Add New											Select All	Clear All	Delete Selected	Reset Selected

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシューティング

SIP TLS 発信は、次の手順でデバッグできます。

### CUCM でのパケット キャプチャの収集

CUCM 9.1(2) と CUCM 10.5(2) の間の接続を確認するには、CUCM サーバでのパケット キャプチャを使用し、SIP TLS トラフィックを監視します。

SIP TLS トラフィックは TCP ポート 5061 で送信されます ( sip-tls として表示される )。

次の例では、SSH CLI セッションが CUCM 9.1(2) に対して確立されています。

#### 1.画面上のCLIパケットキャプチャ

この CLI は SIP TLS トラフィックの画面上の出力を印刷します。

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
60722188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

#### 2.ファイルへのCLIキャプチャ

この CLI はホストに基づいてパケット キャプチャを行い、packets というファイルを作成します

。

admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200

SIP トランクを CUCM 9.1(2) で再起動し、内線 1018 ( CUCM 9.1(2) ) からの発信を内線 9898 ( CUCM 10.5(2) ) に対して行います。

ファイルを CLI からダウンロードするには、このコマンドを実行します。

admin:file get activelog platform/cli/packets.cap

キャプチャは、標準の .cap 形式で行われます。この例では packets.cap ファイルを開くために Wireshark を使用していますが、任意の packets.cap ファイルを開くことができます。

No.	Time	Source	Destination	Protocol	Length	Info
18:46:11.313121	10.106.95.203	10.106.95.200	TCP	74	33135 > sip-tls [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1	
18:46:11.313230	10.106.95.200	10.106.95.203	TCP	74	sip-tls > 33135 [SYN, ACK] Seq=0 Ack=1 win=14480 Len=0 MSS=1460	
18:46:11.313706	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=1 Ack=1 win=5888 Len=0 TSval=156761672	
18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello	
18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1 Ack=59 win=14592 Len=0 TSval=988679	
18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello	
18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done	
18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 win=8832 Len=0 TSval=15676	
18:46:11.430454	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1643 win=11648 Len=0 TSval=1567	
18:46:11.450926	10.106.95.203	10.106.95.200	TCP	1514	[TCP segment of a reassembled PDU]	
18:46:11.450969	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1507 win=17408 Len=0 TSval=98	
18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Ciph	
18:46:11.451081	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1948 win=20352 Len=0 TSval=98	
18:46:11.461558	10.106.95.200	10.106.95.203	TLSv1	1200	New Session Ticket, Change Cipher Spec, Finished	
18:46:11.463062	10.106.95.203	10.106.95.200	TLSv1	1161	Application Data	
18:46:11.502380	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=2777 Ack=3043 win=23168 Len=0 TSval=98	
18:46:11.784432	10.106.95.200	10.106.95.203	TLSv1	440	Application Data	
18:46:11.824821	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=3151 win=17536 Len=0 TSval=15	
18:46:12.187974	10.106.95.200	10.106.95.203	TLSv1	1024	Application Data	
18:46:12.188452	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=4109 win=20352 Len=0 TSval=15	
18:46:15.288860	10.106.95.200	10.106.95.203	TLSv1	1466	Application Data	
18:46:15.289237	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=5509 win=23296 Len=0 TSval=15	
18:46:15.402901	10.106.95.203	10.106.95.200	TLSv1	770	Application Data	

1. CUCM 9.1(2) (クライアント) と CUCM 10.5(2) (サーバ) の間の TCP 通信を確立するための Transmission Control Protocol (TCP) の同期 (SYN)。
2. CUCM 9.1(2) は、TLS セッションを開始するために Client Hello を送信します。
3. CUCM 10.5(2) は、証明書交換プロセスを開始するために Server Hello, Server Certificate, and Certificate Request を送信します。
4. 証明書の交換を完了するために、クライアント CUCM 9.1(2) が送信する証明書。
5. アプリケーション データは暗号化された SIP シグナリングであり、TLS セッションが確立されていることを示します。

正しい証明書が交換されているかどうかさらにチェックされます。Server Hello の後、サーバ CUCM 10.5(2) はその証明書をクライアント CUCM 9.1(2) に送信します。

No.	Time	Source	Destination	Protocol	Length	Info
4	2015-05-23 18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello
5	2015-05-23 18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1 Ack=59 win=14592 Len=0 TSval=988679
6	2015-05-23 18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello
7	2015-05-23 18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done
8	2015-05-23 18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 win=8832 Len=0 TSval=15676

Secure Sockets Layer

- TLV Record Layer: Handshake Protocol: Certificate
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 1560
- Handshake Protocol: Certificate
  - Handshake Type: Certificate (11)
  - Length: 1556
  - Certificates Length: 1553
  - Certificates (1553 bytes)
    - Certificate Length: 902
      - Certificate (id-at-commonName=CUCM10,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
      - signedCertificate
        - version: v3 (2)
        - serialNumber : 0x398b1da6000000000000e
        - signature (shaWithRSAEncryption)
        - issuer: rdnSequence (0)
        - validity
        - subject: rdnSequence (0)
        - subjectPublicKeyInfo
        - extensions: 6 items

CUCM サーバ 10.5(2) のシリアル番号および情報カテゴリに関する情報は CUCM 9.1(2) に提示さ

れます。シリアル番号、件名、発行者、および利用可能日はすべて [OS Admin Certificate Management] ページの情報と比較されます。

サーバ CUCM 10.5(2) は、検証用の独自の証明書を提示した後に、クライアント CUCM 9.1(2) の証明書をチェックします。検証は両方向で行われます。

The screenshot shows a network traffic capture with the following details:

- Filter: Expression... Clear Apply Save test
- Source: 10.106.95.203, Destination: 10.106.95.200, Protocol: TCP, Length: 1514 [TCP segment of a reassembled PDU]
- Source: 10.106.95.200, Destination: 10.106.95.203, Protocol: TCP, Length: 66 sip-tls > 33135 [ACK] Seq=1643 Ack=1507 win=17408 Len=0 TSval=988797 TSecr=156
- Source: 10.106.95.203, Destination: 10.106.95.200, Protocol: TLSv1, Length: 607 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Finish
- Source: 10.106.95.200, Destination: 10.106.95.203, Protocol: TCP, Length: 66 sip-tls > 33135 [ACK] Seq=1643 Ack=1948 win=20352 Len=0 TSval=988797 TSecr=156

The expanded details for the TLS handshake are as follows:

- Secure Sockets Layer
- TLSv1 Record Layer: Handshake Protocol: Certificate
- Content Type: Handshake (22)
- Version: TLS 1.0 (0x0301)
- Length: 1559
- Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 1555
- Certificates Length: 1552
- Certificates (1552 bytes)
- Certificate Length: 901
- Certificate (id-at-commonName=CUCMA,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
- signedCertificate
- version: v3 (2)
- serialNumber : 0x197ad7e9000000000002
- signature (shaWithRSAEncryption)
- issuer: rdnSequence (0)
- validity
- subject: rdnSequence (0)
- subjectPublicKeyInfo
- extensions: 6 items
- algorithmIdentifier (shaWithRSAEncryption)

パケットキャプチャの証明書と [OS Admin Web] ページの証明書の間で不一致がある場合、正しい証明書はアップロードされません。

正しい証明書を [OS Admin Cert] ページにアップロードする必要があります。

#### CUCM トレースの収集

CUCM トレースは、CUCM 9.1(2) サーバと CUCM 10.5(2) サーバの間で交換されるメッセージの特定、SSL セッションが適切に確立されているかどうかの判断にも役立ちます。

この例では、CUCM 9.1(2) からのトレースが収集されています。

#### コールフロー :

Ext 1018 > CUCM 9.1(2) > SIP TLS TRUNK > CUCM 10.5(2) > Ext 9898

#### ++ デジタル分析

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

++ SIP TLS は、この発信用にポート 5061 で使用されています。

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
```

```
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPtcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

**++ Signal Distribution Layer ( SDL ) メッセージ SIPCertificateInd は、情報カテゴリ CN および接続情報に関する詳細を提供します。**

```
04530218.000 |19:59:21.323 |SdlSig |SIPCertificateInd |wait
|SIPHandler(1,100,72,1) |SIPtcp(1,100,64,1)
|1,100,17,11.3^*^* |[[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig |SIPCertificateInd
|restart0 |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1) |1,100,17,11.3^*^* |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```