

Konfigurieren des SIP-TLS-Trunks im Communications Manager mit einem von der Zertifizierungsstelle signierten Zertifikat

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Verwenden Sie die öffentliche CA oder die Einrichtungs-CA auf Windows Server 2003.](#)

[Schritt 2: Hostname und Einstellungen überprüfen](#)

[Schritt 3: Erstellen und Herunterladen der Zertifikatsanforderung \(Certificate Signing Request, CSR\)](#)

[Schritt 4: Signieren Sie den CSR mit der Microsoft Windows 2003-Zertifizierungsstelle.](#)

[Schritt 5: Abruf des Root-Zertifikats von der CA](#)

[Schritt 6: CA-Stammzertifikat als CallManager Trust hochladen](#)

[Schritt 7: Laden Sie das CallManager CSR-Zertifikat für das CA-Zeichen als CallManager-Zertifikat hoch.](#)

[Schritt 8: Erstellen von SIP-Trunk-Sicherheitsprofilen](#)

[Schritt 9: SIP-Trunks erstellen](#)

[Schritt 10: Erstellen von Routenmustern](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Paketerfassung auf CUCM erfassen](#)

[Erfassung von CUCM-Ablaufverfolgungen](#)

Einführung

Dieses Dokument beschreibt einen Schritt-für-Schritt-Prozess zur Konfiguration des SIP-Trunks (Session Initiation Protocol) Transport Layer Security (TLS) auf Communications Manager mit einem Zertifikat der Zertifizierungsstelle (Certificate Authority, CA).

Nach Befolgen dieses Dokuments werden SIP-Nachrichten zwischen zwei Clustern mithilfe des TLS verschlüsselt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager (CUCM)
- SIP

Verwendete Komponenten

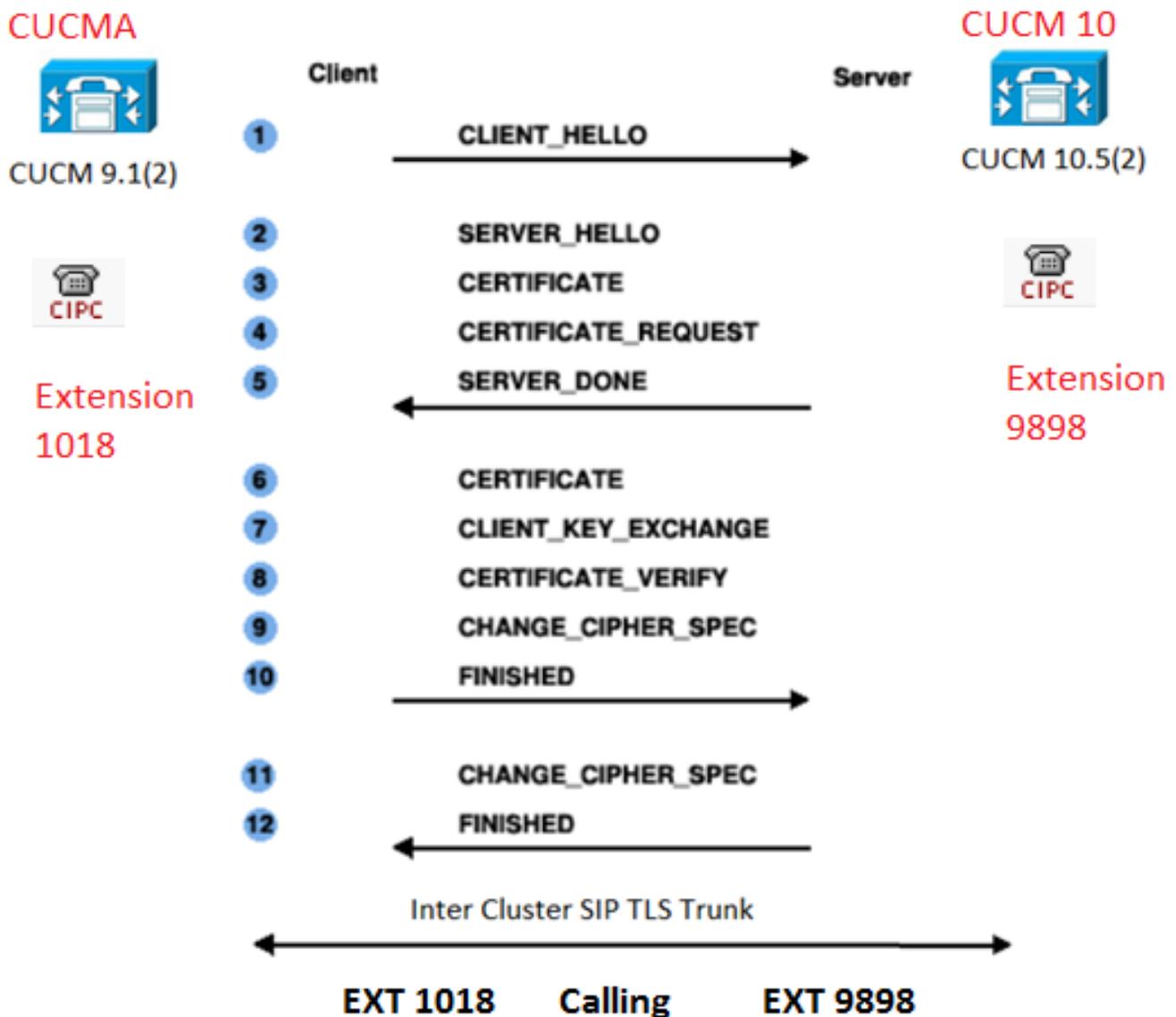
Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- CUCM-Version 9.1(2)
- CUCM-Version 10.5(2)
- Microsoft Windows Server 2003 als CA

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

Hintergrundinformationen

Wie in diesem Bild gezeigt, SSL-Handshake mit Zertifikaten.



Konfigurieren

Schritt 1: Verwenden Sie die öffentliche CA oder die Einrichtungs-CA auf Windows Server 2003.

Weitere Informationen finden Sie unter: [Einrichten der CA auf einem Windows 2003-Server](#)

Schritt 2: Hostname und Einstellungen überprüfen

Zertifikate basieren auf Namen. Stellen Sie sicher, dass die Namen korrekt sind, bevor Sie beginnen.

```
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
```

Um den Hostnamen zu ändern, klicken Sie auf den folgenden Link: [Ändern des Hostnamens in CUCM](#)

Schritt 3: Erstellen und Herunterladen der Zertifikatsanforderung (Certificate Signing Request, CSR)

CUCM 9.1(2)

Um den CSR zu generieren, navigieren Sie zu **OS Admin > Security > Certificate Management > Generate CSR**.

Wählen Sie im Feld **Zertifikatsname** die Option **CallManager** aus der Dropdown-Liste aus.

The screenshot shows a web-based dialog box titled "Generate Certificate Signing Request". At the top, there are two buttons: "Generate CSR" (with a lock icon) and "Close" (with a document icon). Below this is a "Status" section containing a yellow warning triangle 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 dropdown menu labeled "Certificate Name *". The dropdown menu is currently set to "CallManager". At the bottom of the dialog, there are two buttons: "Generate CSR" and "Close".

Um den CSR herunterzuladen, navigieren Sie zu **OS Admin > Security > Certificate Management > Download CSR (OS-Administrator > Sicherheit > Zertifikatsverwaltung > CSR herunterladen)**.

Wählen Sie im Feld **Zertifikatsname** die Option **CallManager** aus der Dropdown-Liste aus.

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*

CUCM 10.5(2)

Um den CSR zu generieren, wählen Sie **OS Admin > Security > Certificate Management > Generate CSR (Betriebssystemadministrator > Sicherheit > Zertifikatsverwaltung > CSR erstellen)** aus.

1. Wählen Sie im Feld **Certificate Purpose** (Zweck des Zertifikats) in der Dropdown-Liste **CallManager** aus.
2. Wählen Sie im Feld **Schlüssellänge** die Option **1024** aus der Dropdown-Liste aus..
3. Wählen Sie im Feld **Hash Algorithm** die Option **SHA1** aus der Dropdown-Liste aus.

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*

Um den CSR herunterzuladen, navigieren Sie zu OS Admin > Security > Certificate Management > Download CSR (OS-Administrator > Sicherheit > Zertifikatsverwaltung > CSR herunterladen). Wählen Sie im Feld Zertifikatzweck die Option CallManager aus der Dropdown-Liste aus.

Download Certificate Signing Request

Download CSR Close

Status

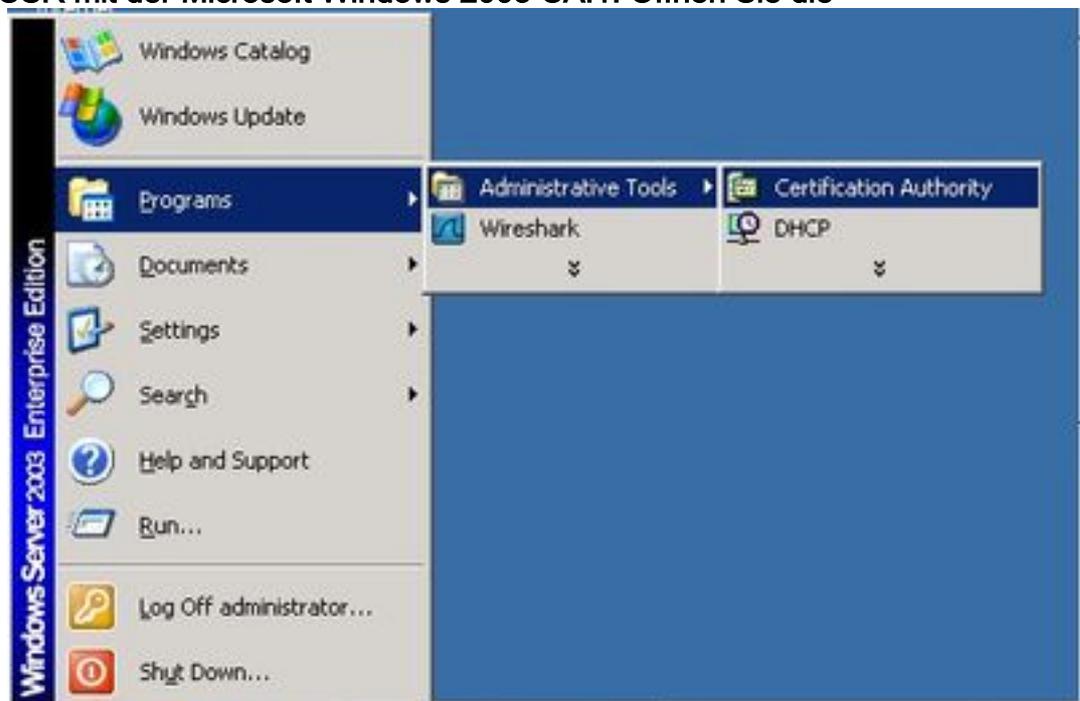
! Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

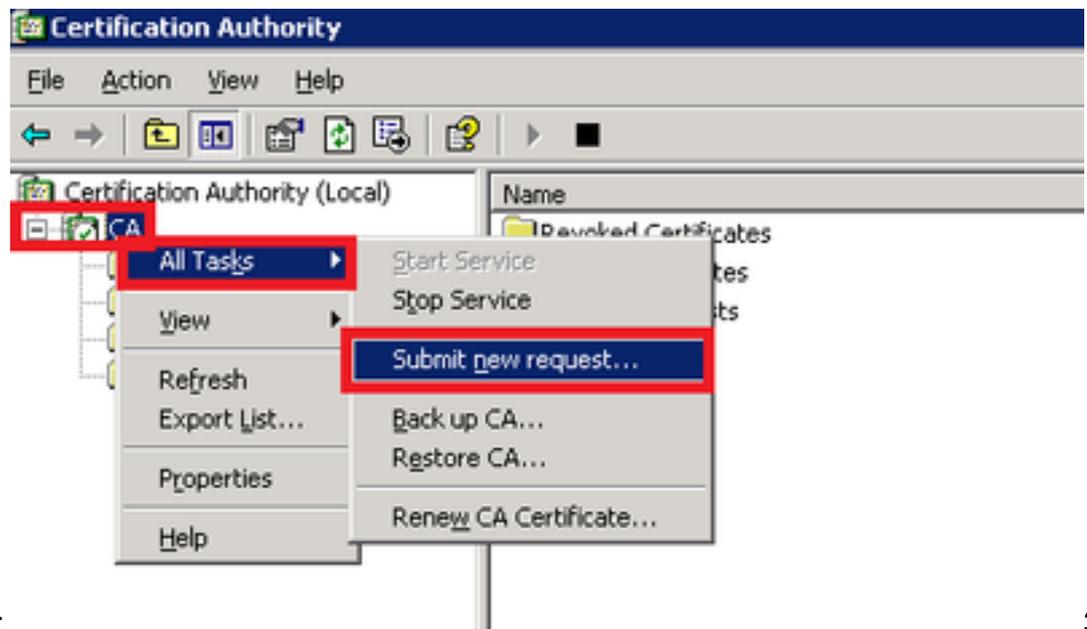
Certificate Purpose* CallManager

Download CSR Close

Hinweis: Der CallManager-CSR wird mit den 1024-Bit-RSA-Schlüsseln (Rivest-Shamir-Addleman) generiert. Schritt 4: Signieren Sie den CSR mit der Microsoft Windows 2003-Zertifizierungsstelle. Dies ist eine optionale Information zum Signieren des CSR mit der Microsoft Windows 2003 CA.1. Öffnen Sie die



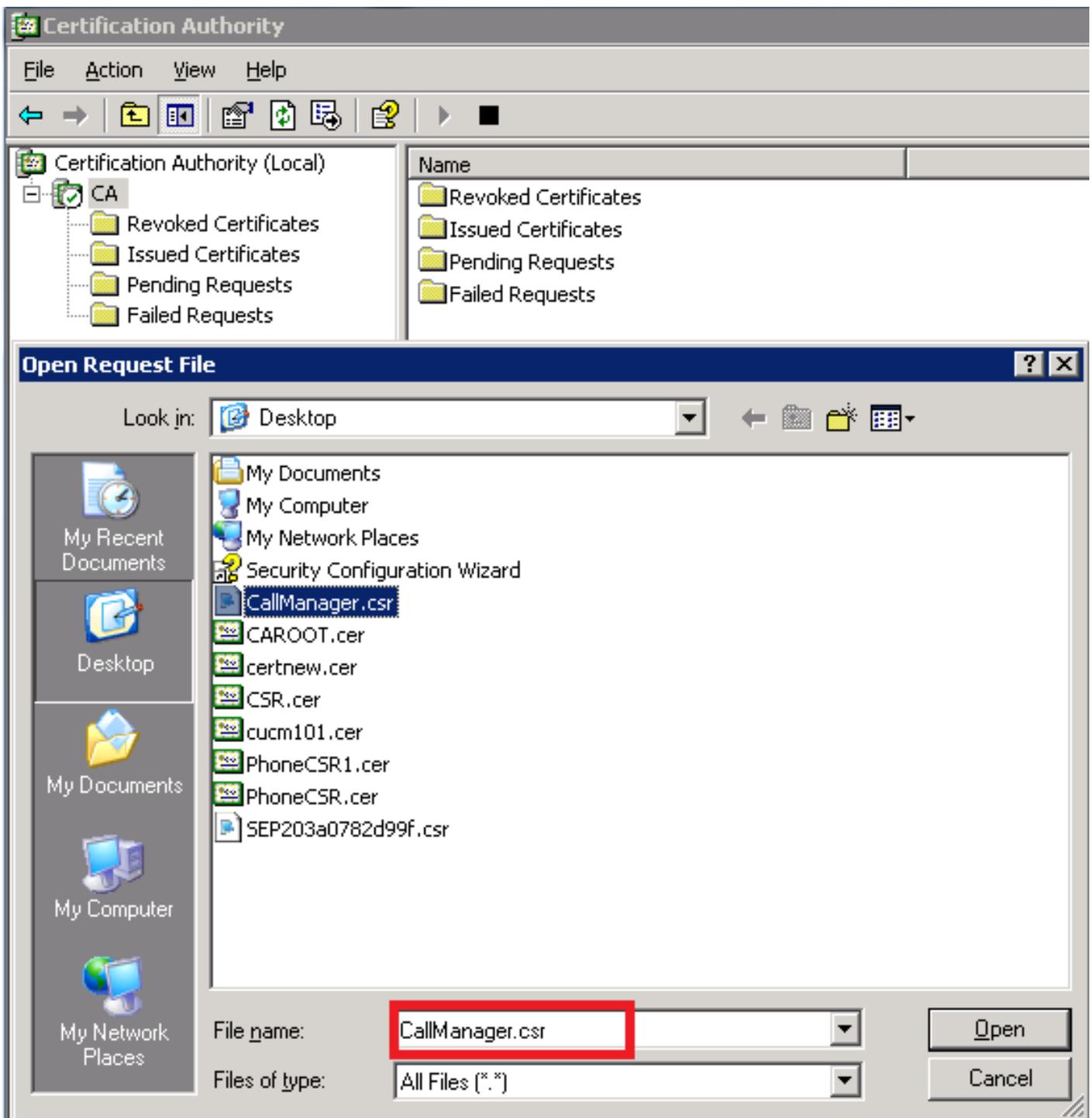
Zertifizierungsstelle. 2. Klicken Sie mit der rechten Maustaste auf das CA-Symbol, und navigieren Sie zu All Tasks >



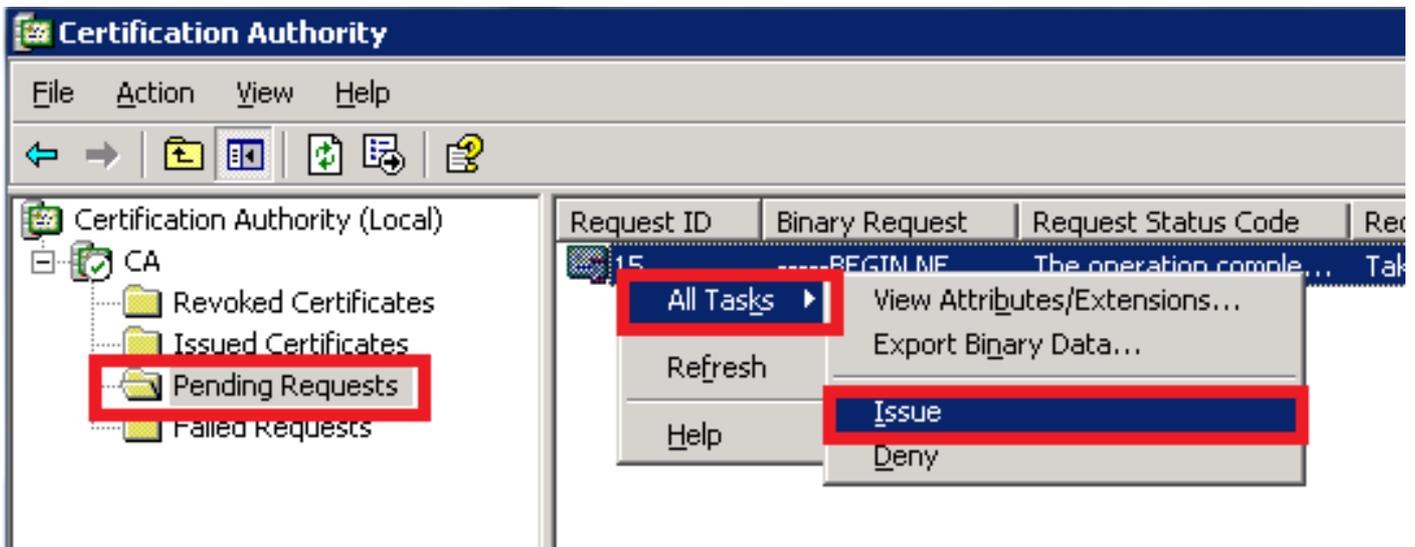
Submit new request.

Wählen Sie den CSR aus, und klicken Sie auf die Option Öffnen (gilt sowohl für die CSRs (CUCM 9.1(2) und CUCM 10.5(2))).

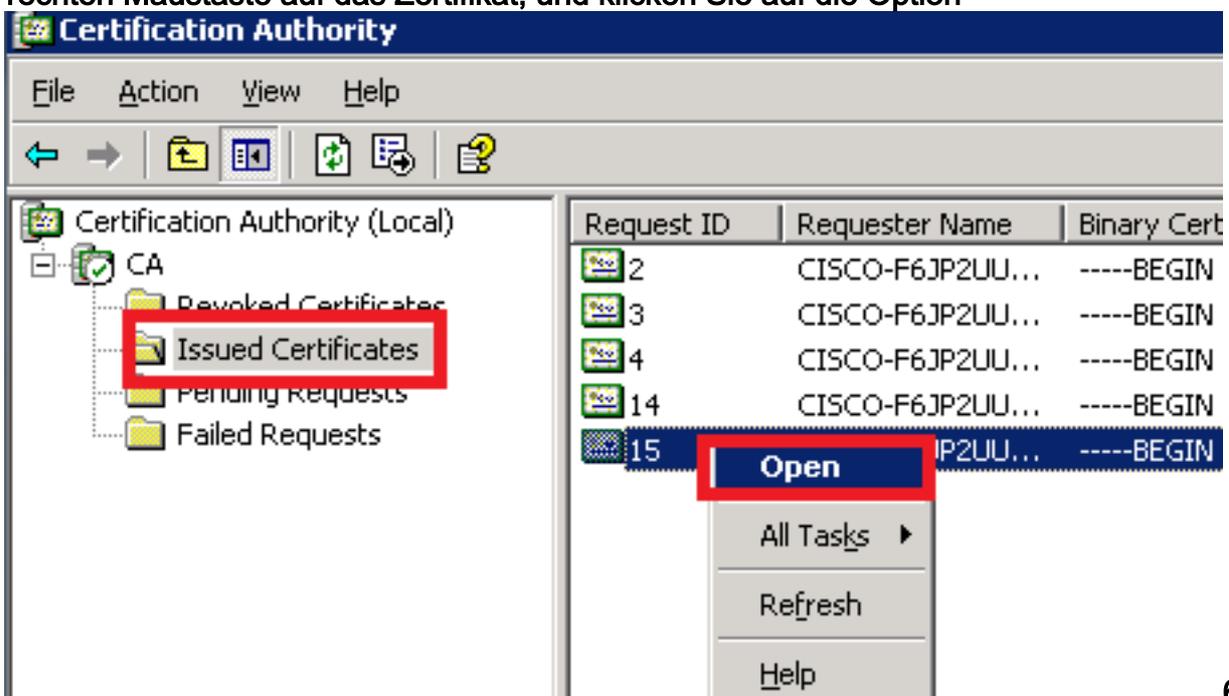
3.



4. Alle geöffneten CSRs werden im Ordner Ausstehende Anfragen angezeigt. Klicken Sie mit der rechten Maustaste auf jeden CSR, und navigieren Sie zu Alle Aufgaben > Ausstellen, um die Zertifikate auszustellen. (Gilt sowohl für CSR (CUCM 9.1(2) und CUCM 10.5(2)))



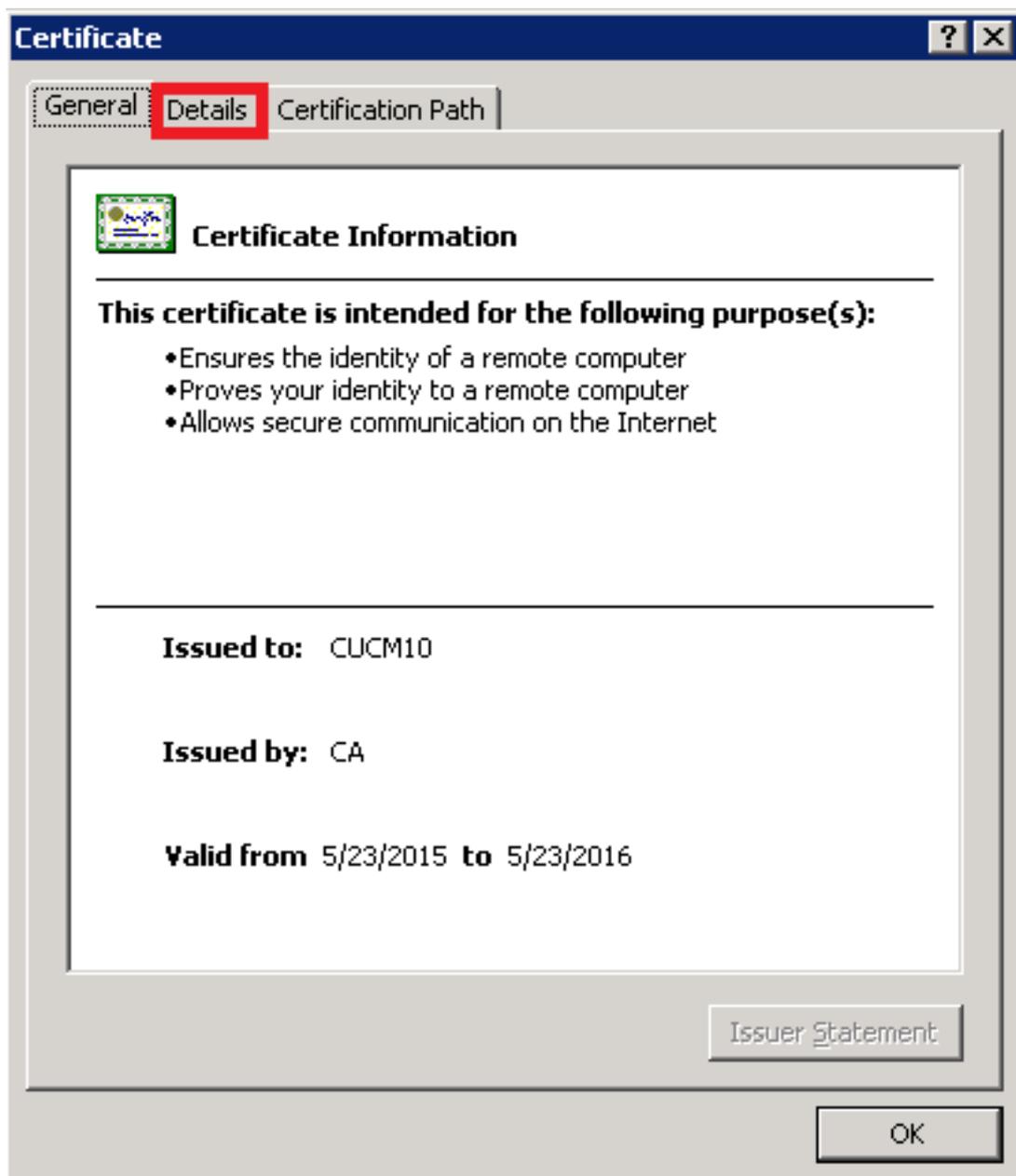
5. Um das Zertifikat herunterzuladen, wählen Sie den Ordner Ausgestellte Zertifikate. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und klicken Sie auf die Option



Öffnen.

Die Zertifikatdetails werden angezeigt. Um das Zertifikat herunterzuladen, wählen Sie die Registerkarte Details aus und klicken auf die Schaltfläche In Datei

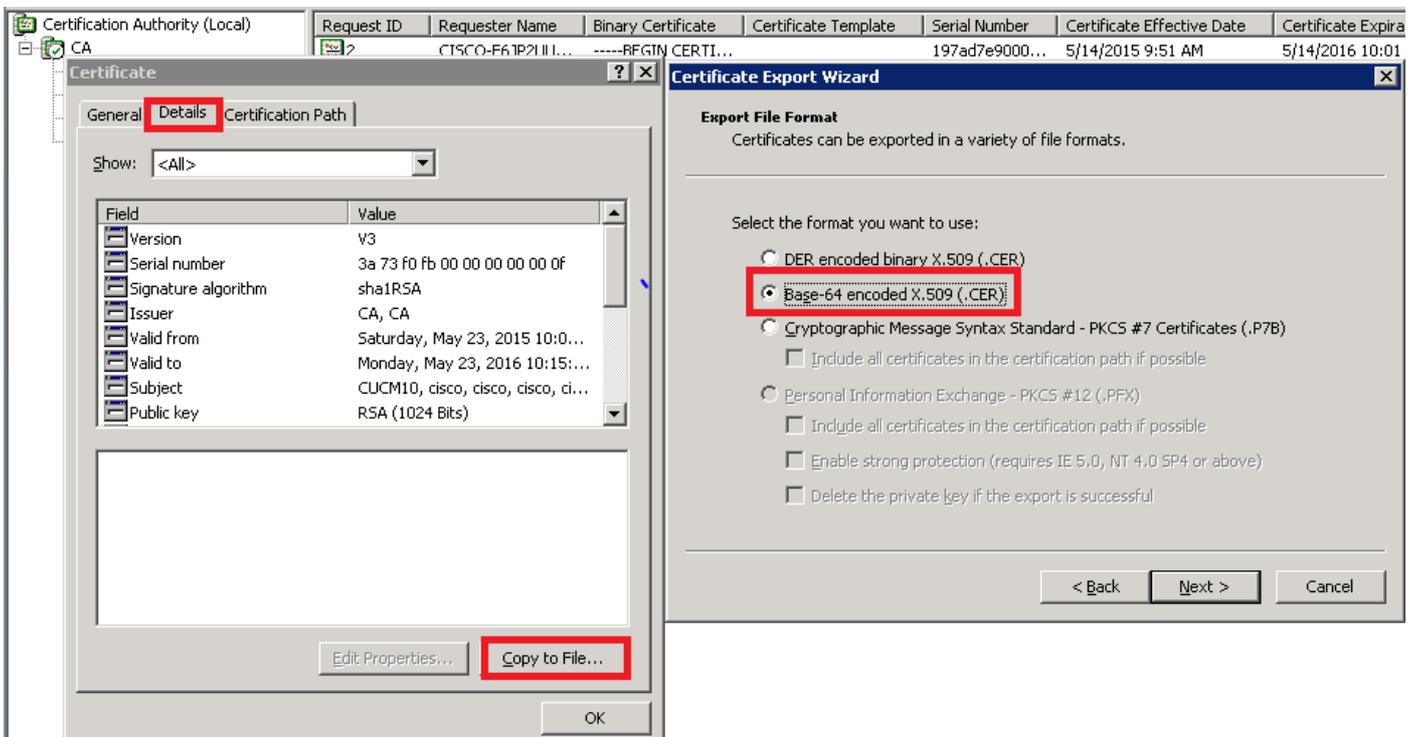
6.



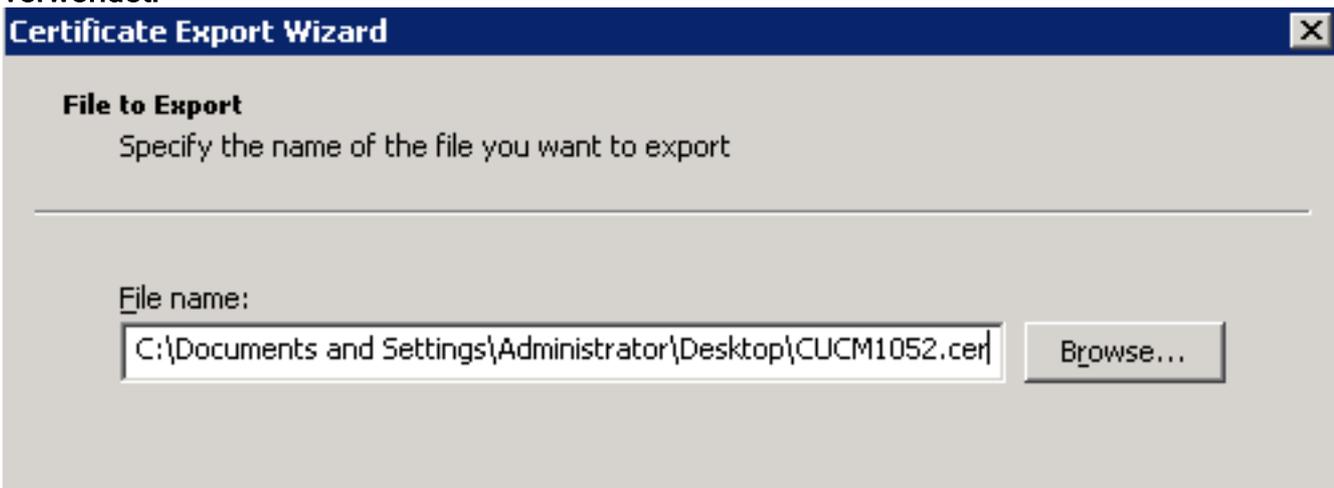
kopieren...

Sie im Fenster Certificate Export Wizard (Assistent für den Zertifikatsexport) auf das Optionsfeld Base-64-codierte X.509(.CER).

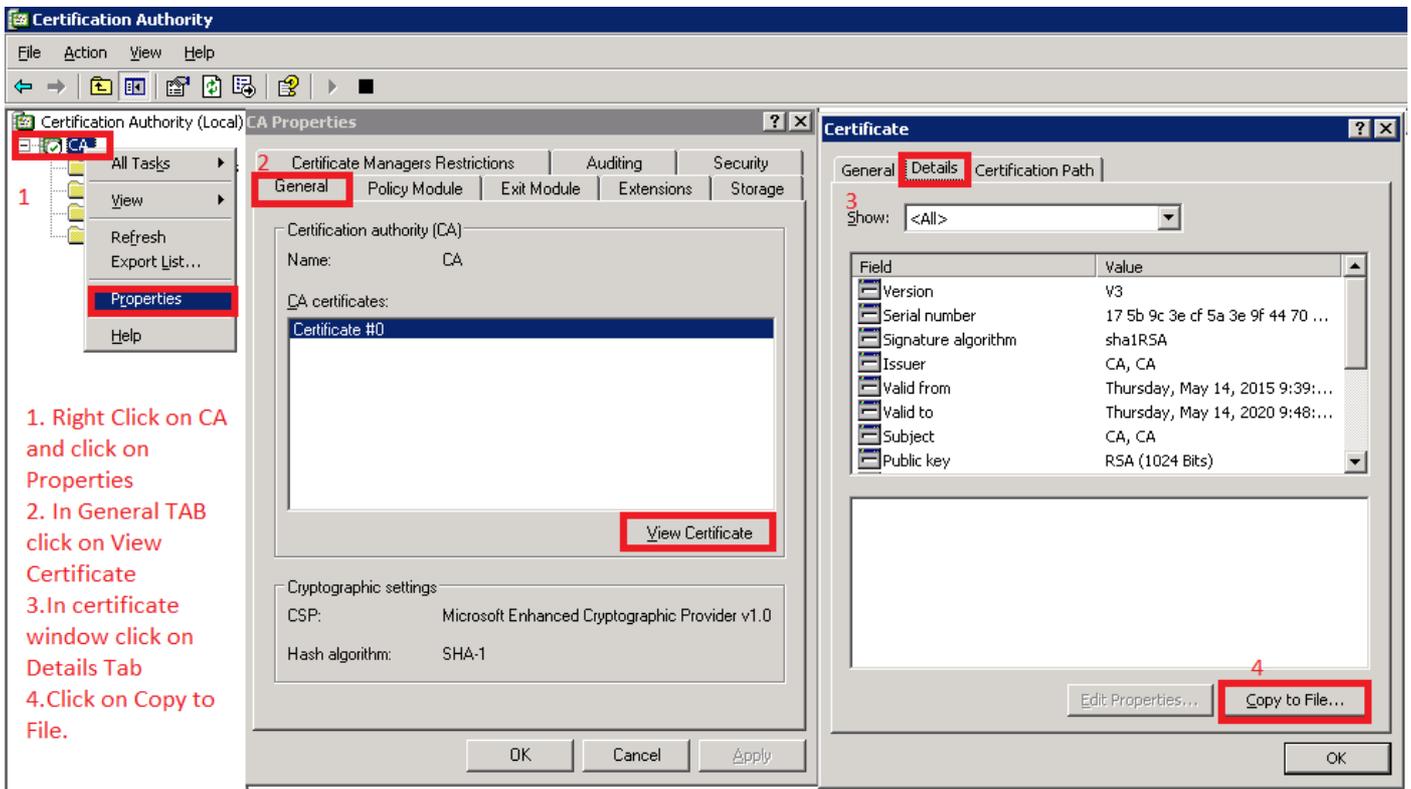
7. Klicken



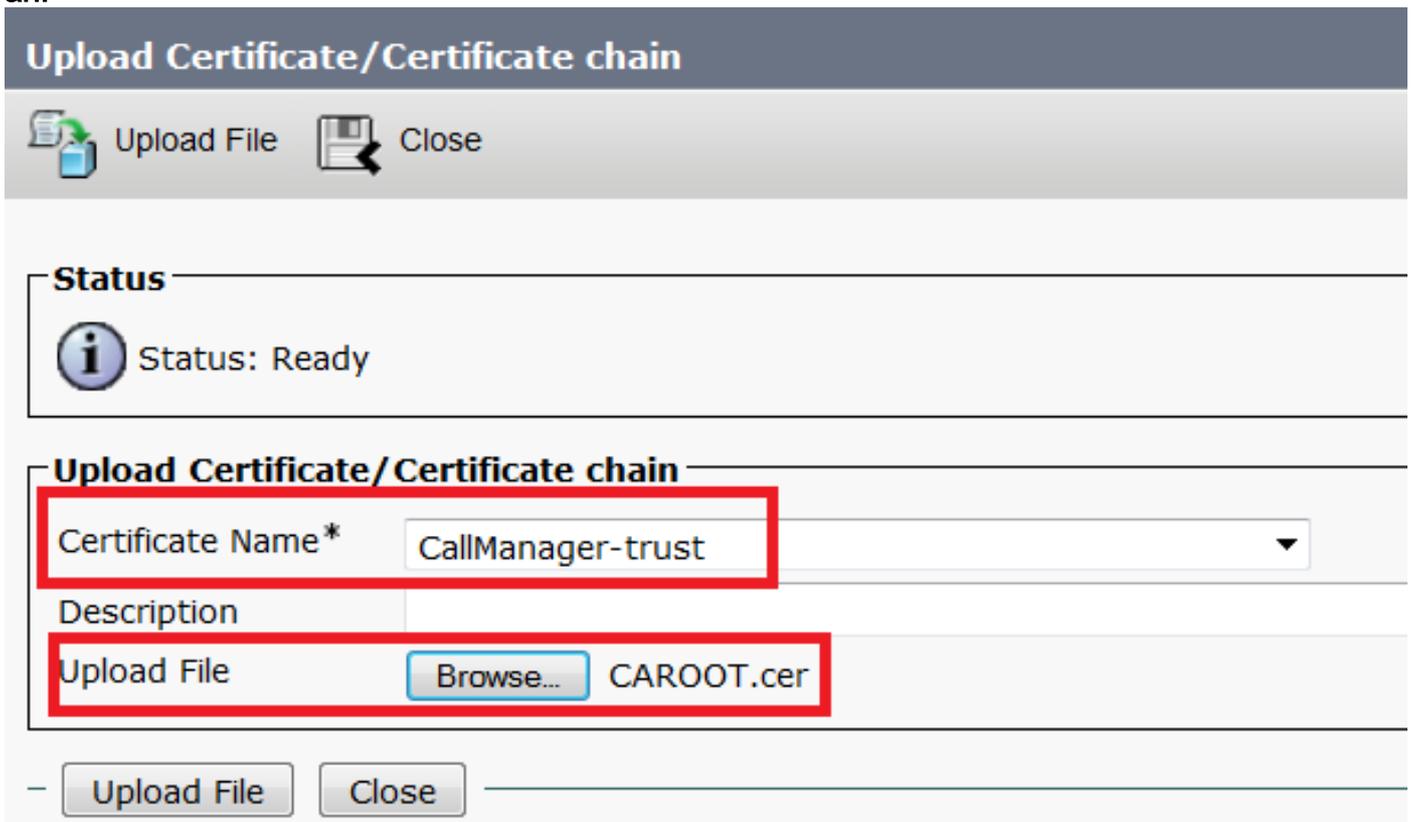
8. Geben Sie der Datei einen korrekten Namen. In diesem Beispiel wird das Format CUCM1052.cer verwendet.



Für CUCM 9.1(2) ist das gleiche Verfahren anzuwenden. Schritt 5: Abruf des Root-Zertifikats von der CA Öffnen Sie das Fenster Zertifizierungsstelle. So laden Sie die Root-CA herunter 1. Klicken Sie mit der rechten Maustaste auf das CA-Symbol, und klicken Sie auf die Option Eigenschaften. 2. Klicken Sie in der Regel auf Zertifikat anzeigen. 3. Klicken Sie im Fenster Zertifikat auf die TAB mit den Details. 4. Klicken Sie auf In Datei kopieren...



Schritt 6: CA-Stammzertifikat als CallManager Trust hochladen. Melden Sie sich zum Hochladen des CA-Stammzertifikats bei OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain an.



Hinweis: Führen Sie diese Schritte für die CUCMs (CUCM 9.1(2) und CUCM 10.5(2)) aus. Schritt 7: Laden Sie das CallManager CSR-Zertifikat für das CA-Zeichen als CallManager-Zertifikat hoch. Melden Sie sich für das Hochladen des CA-Zeichens CallManager CSR an bei OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain.

Upload Certificate/Certificate chain



Upload File



Close

Status



Status: Ready

Upload Certificate/Certificate chain

Certificate Name*

CallManager

Description

Self-signed certificate

Upload File

Browse...

CUCM9.cer

Upload File

Close

Hinweis: Führen Sie diese Schritte für die CUCMs (CUCM 9.1(2) und CUCM 10.5(2)) aus. Schritt 8:

Erstellen von SIP-Trunk-Sicherheitsprofilen CUCM 9.1(2)

Um das SIP-Trunk-Sicherheitsprofil zu erstellen, navigieren Sie zu System > Security > SIP Trunk Security Profile. Kopieren Sie das vorhandene nicht sichere SIP-Trunk-Profil, und geben Sie ihm einen neuen Namen. Im Beispiel wurde das nicht sichere SIP-Trunk-Profil in das sichere SIP-Trunk-Profil TLS umbenannt.

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 ▼	

In X.509 Subject Name verwenden Sie den Common Name (CN) des CUCM 10.5(2) (Zertifizierungsstellen-signiertes Zertifikat), wie in diesem Bild gezeigt.

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) Navigieren Sie zu System > Security > SIP Trunk Security Profile. Kopieren Sie das vorhandene nicht sichere SIP-Trunk-Profil, und geben Sie ihm einen neuen Namen. Im Beispiel wurde das nicht sichere SIP-Trunk-Profil in das sichere SIP-Trunk-Profil TLS umbenannt.

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 This Name should be CN of CUCM 9.1(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

In X.509 Subject Name verwenden Sie den CN von CUCM 9.1(2) (Zertifizierungsstellen-signiertes Zertifikat), wie hervorgehoben:

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,
```

Beide SIP-Trunk-Sicherheitsprofile legen den eingehenden Port 5061 fest, bei dem jeder Cluster den TCP-Port 5061 für die neuen eingehenden SIP-TLS-Anrufe abhört.Schritt 9: SIP-Trunks

erstellen Erstellen Sie nach der Erstellung der Sicherheitsprofile die SIP-Trunks, und nehmen Sie die Änderungen für die unten stehenden Konfigurationsparameter im SIP-Trunk vor. CUCM 9.1(2)

1. Aktivieren Sie im Fenster "SIP Trunk Configuration" das Kontrollkästchen configuration parameter SRTP Allowed.

Dadurch wird das Real-Time Transport Protocol (RTP) für die Anrufe über diesen Trunk gesichert. Dieses Kontrollkästchen darf nur bei Verwendung von SIP TLS aktiviert werden, da die Schlüssel für Secure Real-Time Transport Protocol (SRTP) im Hauptteil der SIP-Nachricht ausgetauscht werden. Die SIP-Signalisierung muss durch TLS gesichert werden. Andernfalls kann jeder Benutzer mit der nicht sicheren SIP-Signalisierung den entsprechenden SRTP-Stream über den Trunk entschlüsseln.

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. Fügen Sie im Abschnitt SIP-Informationen des Fensters "SIP-Trunk-Konfiguration" die Zieladresse, den Zielport und das SIP-Trunk-Sicherheitsprofil hinzu.

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. Aktivieren Sie im Fenster "SIP Trunk Configuration" das Kontrollkästchen configuration parameter SRTP Allowed.

Auf diese Weise kann SRTP für Anrufe über diesen Trunk verwendet werden. Dieses Kontrollkästchen darf nur bei Verwendung von SIP TLS aktiviert werden, da die SRTP-Schlüssel im Hauptteil der SIP-Nachricht ausgetauscht werden. Die SIP-Signalisierung muss durch das TLS gesichert werden, da jeder mit einer nicht sicheren SIP-Signalisierung den entsprechenden sicheren RTP-Stream über den Trunk entschlüsseln kann.

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. Fügen Sie im Abschnitt SIP-Informationen des Fensters "SIP-Trunk-Konfiguration" die Ziel-IP-Adresse, den Ziel-Port und das Sicherheitsprofil hinzu.

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

Schritt 10: Erstellen von Routenmustern Die einfachste Methode besteht in der Erstellung eines Routenmusters für jeden Cluster, der direkt auf den SIP-Trunk verweist. Routengruppen und Routenlisten können ebenfalls verwendet werden. CUCM 9.1(2) verweist auf das Routenmuster 9898 über den TLS-SIP-Trunk zum CUCM

10.5(2)

Trunks (1 - 1 of 1) Rows per Page 50

Find Trunks where Device Name begins with Find Clear Filter

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

Der CUCM 10.5(2) verweist auf das Routenmuster 1018 über den TLS-SIP-Trunk zum CUCM 9.1(2).

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

Überprüfen Für diese Konfiguration ist derzeit kein Überprüfungsverfahren

verfügbar. **Fehlerbehebung** Der SIP-TLS-Anruf kann mit diesen Schritten gedebuggt werden. **Paketerfassung auf CUCM erfassen** Um die Verbindung zwischen dem CUCM 9.1(2) und dem CUCM 10.5(2) zu überprüfen, führen Sie eine Paketerfassung auf den CUCM-Servern durch, und achten Sie auf den SIP-TLS-Datenverkehr. Der SIP-TLS-Datenverkehr wird über den TCP-Port 5061 übertragen, der als "sip-tls" angesehen wird. Im folgenden Beispiel wird eine SSH-CLI-Sitzung für CUCM 9.1(2) eingerichtet.

1. CLI-Paketerfassung auf dem Bildschirm Diese CLI druckt die Ausgabe für den SIP-TLS-Datenverkehr auf dem Bildschirm.

```
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
6072188 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. CLI-Erfassung in Datei Diese CLI erfasst die Pakete basierend auf dem Host und erstellt eine Datei mit dem Namen Packets.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
Starten Sie den SIP-Trunk auf CUCM 9.1(2) neu, und tätigen Sie den Anruf von der Durchwahl 1018 (CUCM 9.1(2)) zur Durchwahl 9898 (CUCM 10.5(2)). Führen Sie den folgenden Befehl aus, um die Datei von der CLI herunterzuladen:
```

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

Die Erfassung erfolgt im Standard .cap-Format. In diesem Beispiel wird Wireshark verwendet, um die Datei "packages.cap" zu öffnen. Es kann jedoch jedes Anzeigetool für die Paketerfassung verwendet werden.

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. Das Transmission Control Protocol (TCP) Synchronize (SYN) dient zum Herstellen der TCP-Kommunikation zwischen dem CUCM 9.1(2)(Client) und dem CUCM 10.5(2)(Server).
2. Der CUCM 9.1(2) sendet den Client Hello, um die TLS-Sitzung zu starten.
3. Der CUCM 10.5(2) sendet The Server Hello, Server Certificate und Certificate Request, um den Zertifikataustauschprozess zu starten.
4. Das Zertifikat, das der Client CUCM 9.1(2) sendet, um den Zertifikataustausch

abzuschließen.

5. Die verschlüsselten Anwendungsdaten für die SIP-Signalisierung zeigen, dass die TLS-Sitzung eingerichtet wurde.

Überprüfen Sie noch einmal, ob die richtigen Zertifikate ausgetauscht werden. Nach dem ServerHello sendet der Server CUCM 10.5(2) sein Zertifikat an den Client CUCM 9.1(2).

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

- TLSv1 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 : 0x398b1da6000000000000
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

Die Seriennummer und die Fachinformationen, die der Server CUCM 10.5(2) hat, werden dem Client CUCM 9.1(2) präsentiert. Seriennummer, Betreff, Aussteller und Gültigkeitsdatum werden mit den Informationen auf der Seite "OS Admin Certificate Management" (Verwaltung von Betriebssystemzertifikaten) verglichen. Der Server CUCM 10.5(2) stellt ein eigenes Zertifikat zur Überprüfung zur Verfügung, jetzt prüft er das Zertifikat des Clients CUCM 9.1(2). Die Überprüfung findet in beide Richtungen statt.

Filter:	Source	Destination	Protocol	Length	Info
	10.106.95.203	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=59 Ack=1043 Win=11048 Len=0 TSval=1007010644 TSecr=9
	10.106.95.203	10.106.95.200	TCP	1514	[TCP segment of a reassembled PDU]
	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=988797 TSecr=156
	10.106.95.203	10.106.95.200	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Fini
	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=988797 TSecr=156

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 : 0x197ad7e9000000000000
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

Wenn eine Abweichung zwischen den Zertifikaten in der Paketerfassung und den Zertifikaten in der OS Admin-Webseite besteht, werden die richtigen Zertifikate nicht hochgeladen. Die richtigen Zertifikate müssen auf die Seite Betriebssystemadministratorzertifikate hochgeladen werden.

Erfassung von CUCM-Ablaufverfolgungen Die CUCM-Ablaufverfolgungen können auch hilfreich sein, um zu bestimmen, welche Nachrichten zwischen den CUCM 9.1(2)- und den CUCM 10.5(2)-Servern ausgetauscht werden und ob die SSL-Sitzung ordnungsgemäß eingerichtet wurde oder nicht. Im Beispiel wurden die Spuren aus CUCM 9.1(2) gesammelt. Anruffluss: Durchwahl 1018 > CUCM 9.1(2) > SIP TLS TRUNK > CUCM 10.5(2) > Ext 9898++ Ziffernanalyse

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pl="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 wird für diesen Anruf auf dem Port 5061 verwendet.

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)-Nachricht SIPCertificateInd enthält Details zu BetreffCN und
Verbindungsinformationen.

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 =