

Configurare SIP TLS Trunk in Communications Manager con un certificato firmato dalla CA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Utilizzare la CA pubblica o la CA configurata in Windows Server 2003](#)

[Passaggio 2. Verificare nome host e impostazioni](#)

[Passaggio 3. Generare e scaricare la richiesta di firma del certificato \(CSR\)](#)

[Passaggio 4. Firmare CSR con Microsoft Windows 2003 Certificate Authority](#)

[Passaggio 5. Ottenere il certificato radice dalla CA](#)

[Passaggio 6. Caricare il certificato radice CA come attendibilità di CallManager](#)

[Passaggio 7. Caricare il certificato CSR CallManager firmato dalla CA come certificato CallManager.](#)

[Passaggio 8. Creazione di profili di sicurezza trunk SIP](#)

[Passaggio 9. Creazione di trunk SIP](#)

[Passaggio 10. Creazione di serie di cicli di lavorazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Raccogli acquisizione pacchetti su CUCM](#)

[Raccogli tracce CUCM](#)

Introduzione

In questo documento viene descritto un processo dettagliato per configurare il trunk TLS (Transport Layer Security) SIP (Session Initiation Protocol) su Communications Manager con un certificato firmato da un'autorità di certificazione (CA).

Dopo aver seguito questo documento, i messaggi SIP tra due cluster verranno crittografati tramite TLS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di:

- Cisco Unified Communications Manager (CUCM)
- SIP

Componenti usati

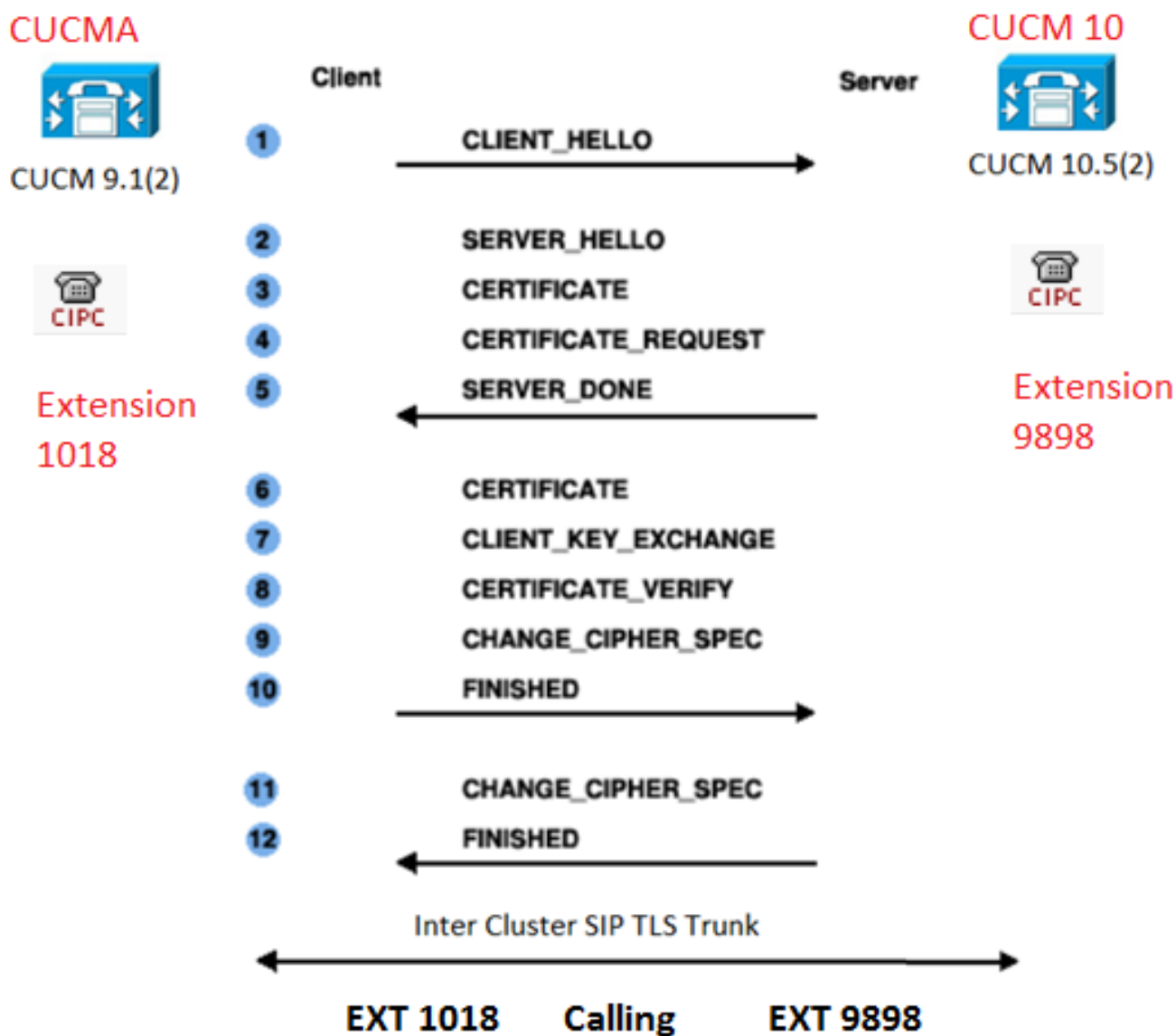
Le informazioni di questo documento si basano sulle seguenti versioni software:

- CUCM versione 9.1(2)
- CUCM versione 10.5(2)
- Microsoft Windows Server 2003 come CA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Come illustrato in questa immagine, Handshake SSL con certificati.



Passaggio 1. Utilizzare la CA pubblica o la CA configurata in Windows Server 2003

Fare riferimento al collegamento: [Configura CA su Windows 2003 Server](#)

Passaggio 2. Verificare nome host e impostazioni

I certificati sono basati sui nomi. Assicurarsi che i nomi siano corretti prima di iniziare.

```
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
```

Per modificare il nome dell'host, fare riferimento al collegamento: [Modifica nome host in CUCM](#)

Passaggio 3. Generare e scaricare la richiesta di firma del certificato (CSR)

CUCM 9.1(2)

Per generare il CSR, selezionare **Amministratore sistema operativo > Sicurezza > Gestione certificati > Genera CSR**

Nel campo **Nome certificato**, selezionare l'opzione **CallManager** dall'elenco a discesa.

The screenshot shows a 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 *" with "CallManager" selected. This dropdown menu is highlighted with a red rectangular box. At the bottom of the dialog, there are two buttons: "Generate CSR" (highlighted with a red rectangular box) and "Close".

Per scaricare il CSR, selezionare **Amministratore del sistema operativo > Sicurezza > Gestione certificati > Scarica CSR**

Nel campo **Nome certificato**, selezionare l'opzione **CallManager** dall'elenco a discesa.

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)


Per generare il CSR, selezionare **Amministratore sistema operativo > Sicurezza > Gestione certificati > Genera CSR**

1. Nel campo **Scopo certificato**, selezionare **CallManager** dall'elenco a discesa.
2. Nel campo **Lunghezza chiave**, selezionare **1024** dall'elenco a discesa.
3. Nel campo **Hash Algorithm**, selezionare **SHA1** dall'elenco a discesa.

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* CallManager

Distribution* CUCM10

Common Name* CUCM10

Subject Alternate Names (SANs)

Parent Domain

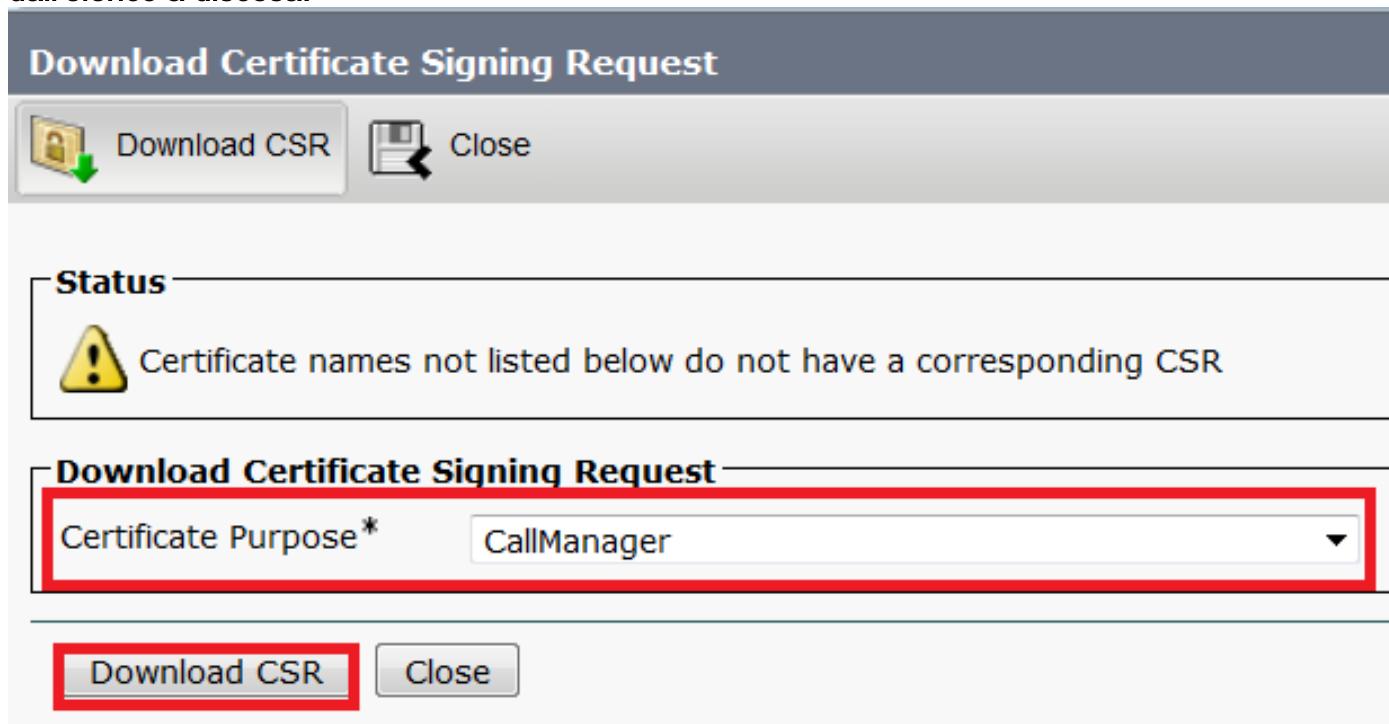
Key Length* 1024

Hash Algorithm* SHA1

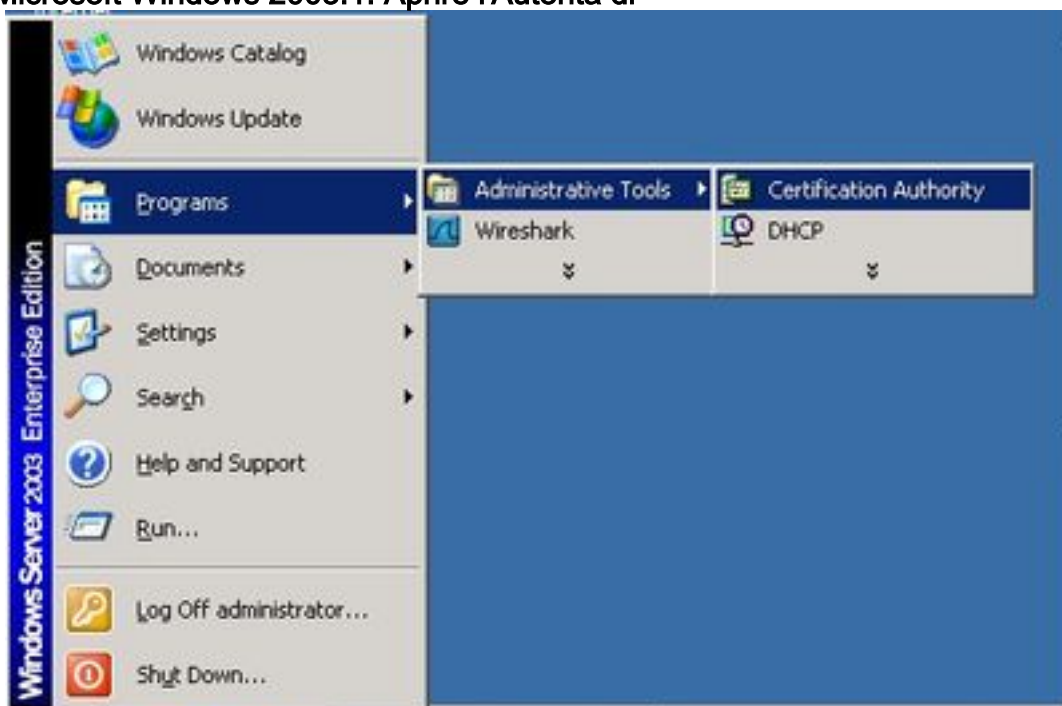
Generate Close

Per scaricare il CSR, selezionare **Amministratore del sistema operativo > Sicurezza > Gestione certificati > Scarica CSR** Nel campo **Scopo certificato**, selezionare l'opzione **CallManager**

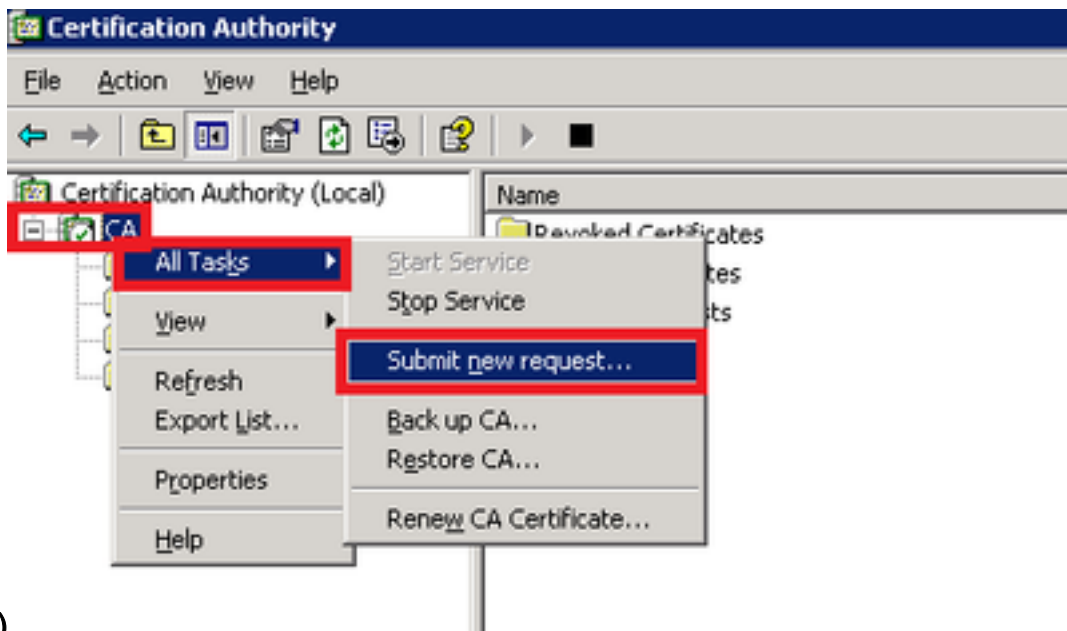
dall'elenco a discesa.



Nota: Il CSR di CallManager viene generato con le chiavi RSA (Rivest-Shamir-Addleman) a 1024 bit. Passaggio 4. Firmare CSR con Microsoft Windows 2003 Certificate Authority. Informazioni facoltative per la firma del CSR con la CA di Microsoft Windows 2003.1. Aprire l'Autorità di



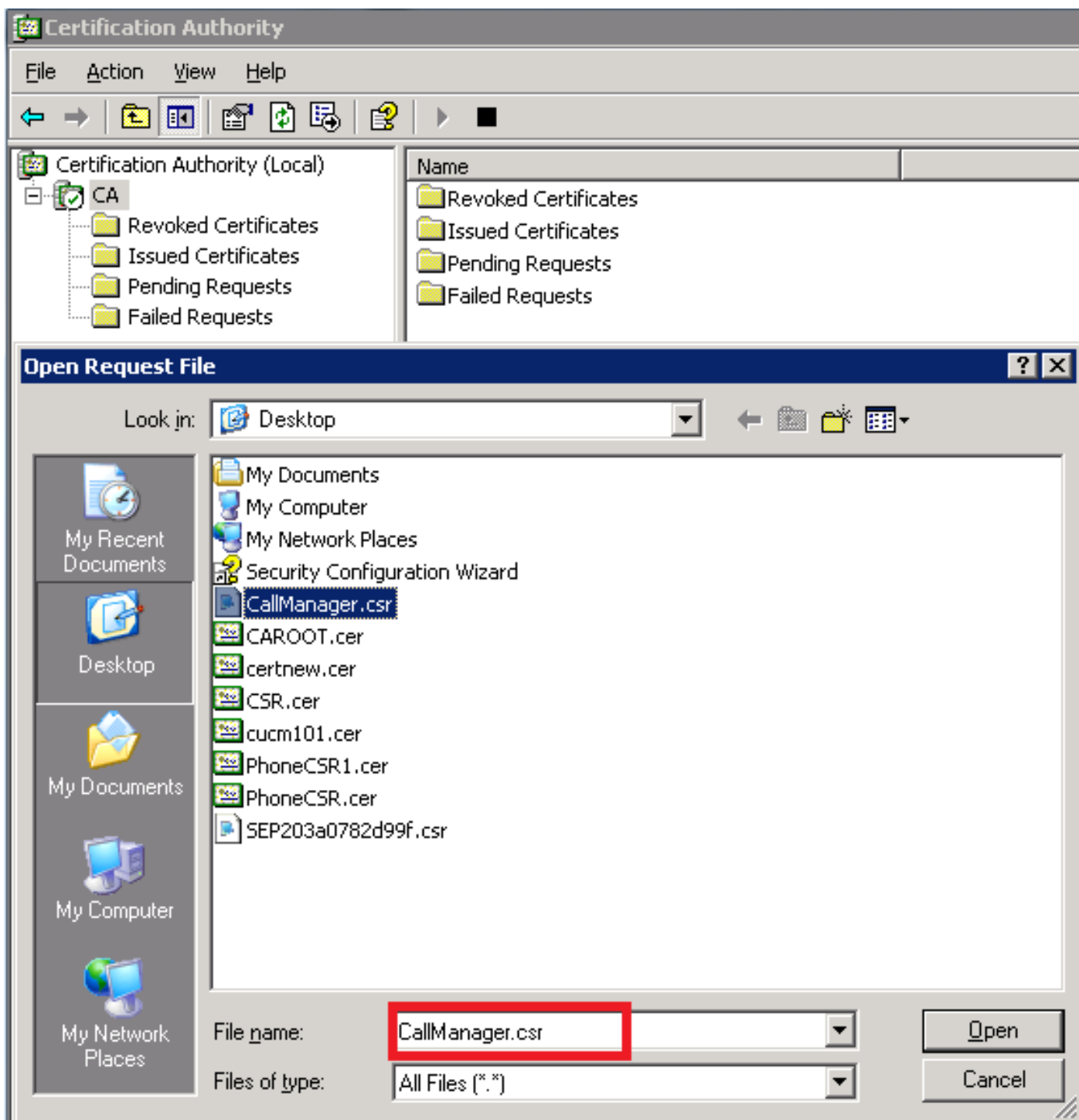
certificazione. 2. Fare clic con il pulsante destro del mouse sull'icona CA e selezionare All Tasks > Submit new request (Tutte le attività > Invia nuova



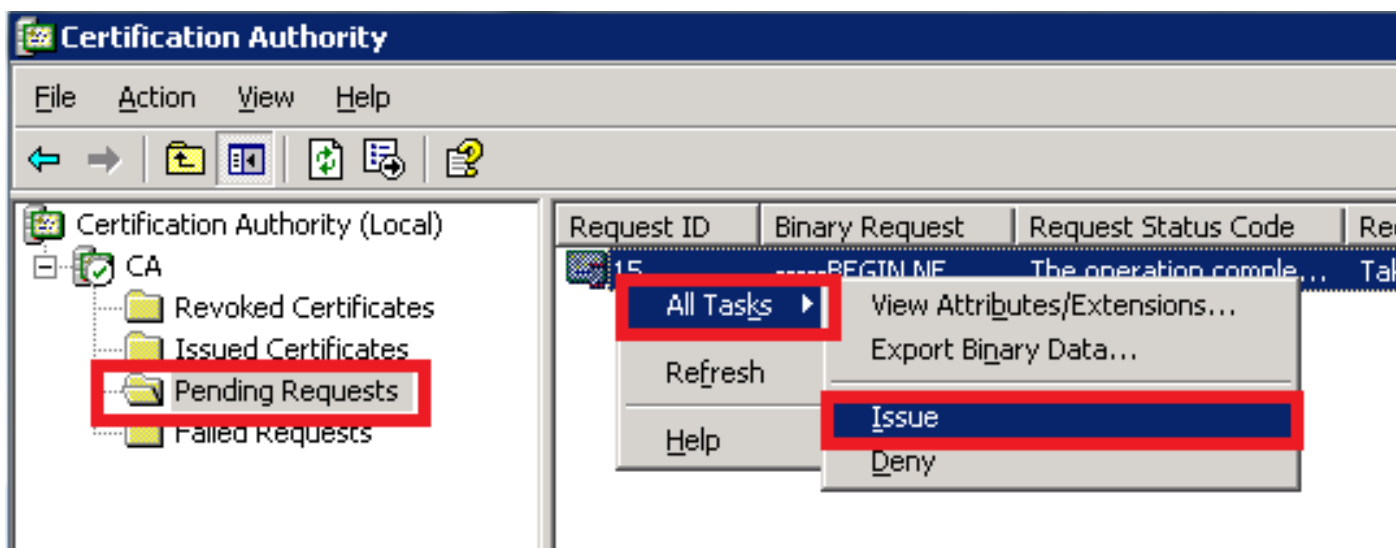
richiesta)

3.

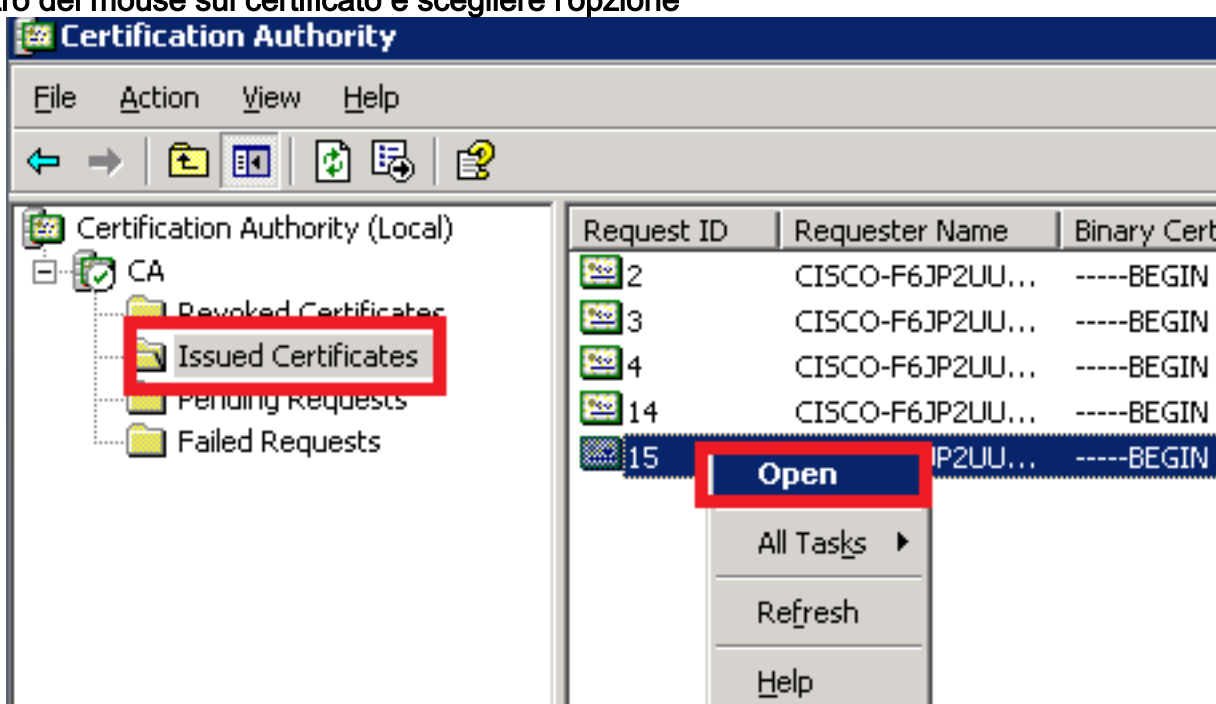
Selezionare il CSR e fare clic sull'opzione Open (applicabile sia al CSR (CUCM 9.1(2) che al CUCM 10.5(2))



4. Tutti i CSR aperti vengono visualizzati nella cartella Richieste in sospeso. Fare clic con il pulsante destro del mouse su ciascun CSR e selezionare All Tasks > Issue per emettere i certificati. (Applicabile sia nel CSR (CUCM 9.1(2) che in CUCM 10.5(2))



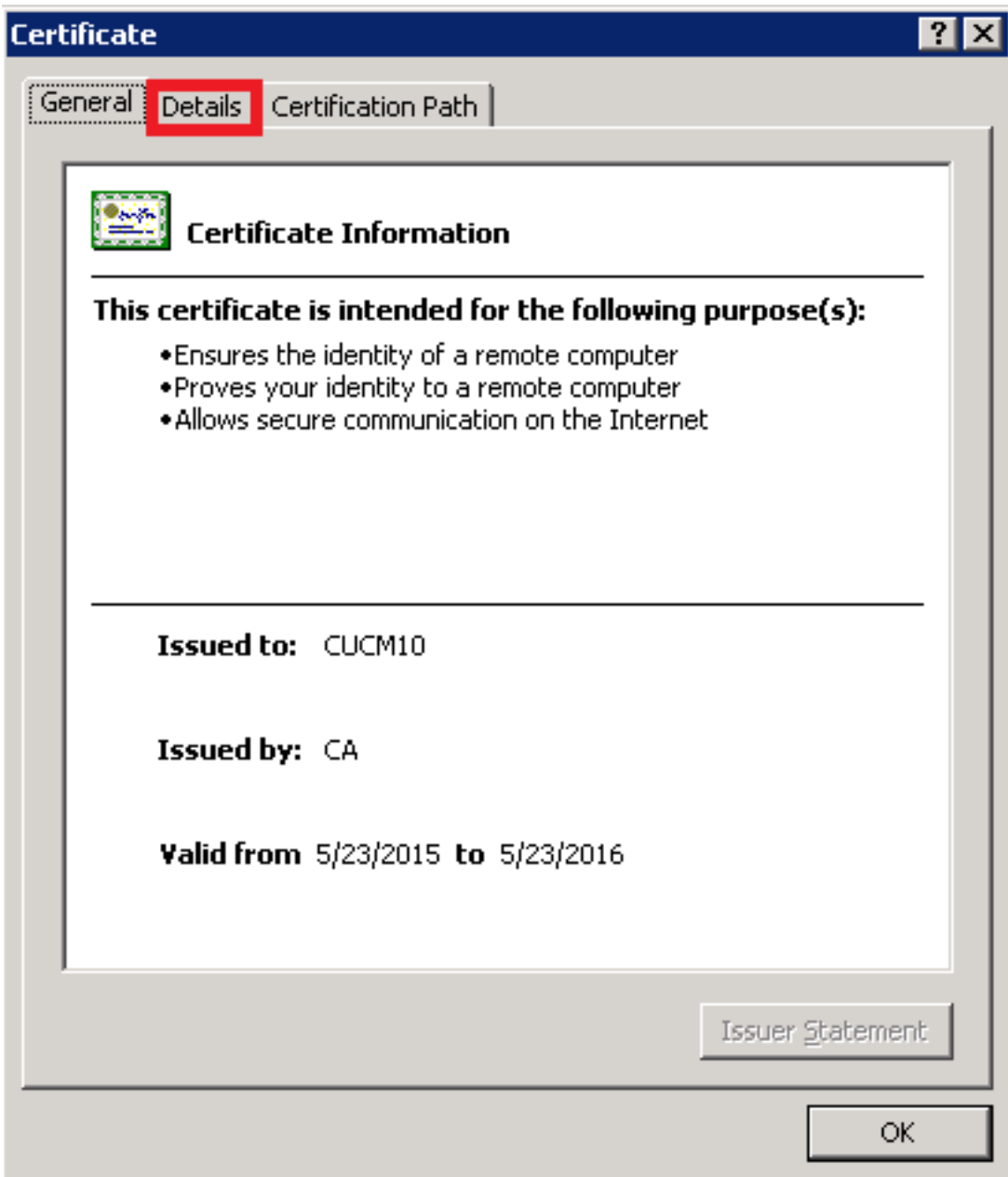
5. Per scaricare il certificato, scegliere la cartella Certificati rilasciati. Fare clic con il pulsante destro del mouse sul certificato e scegliere l'opzione



Apri.

Vengono visualizzati i dettagli del certificato. Per scaricare il certificato, selezionare la scheda Dettagli e fare clic sul pulsante Copia su

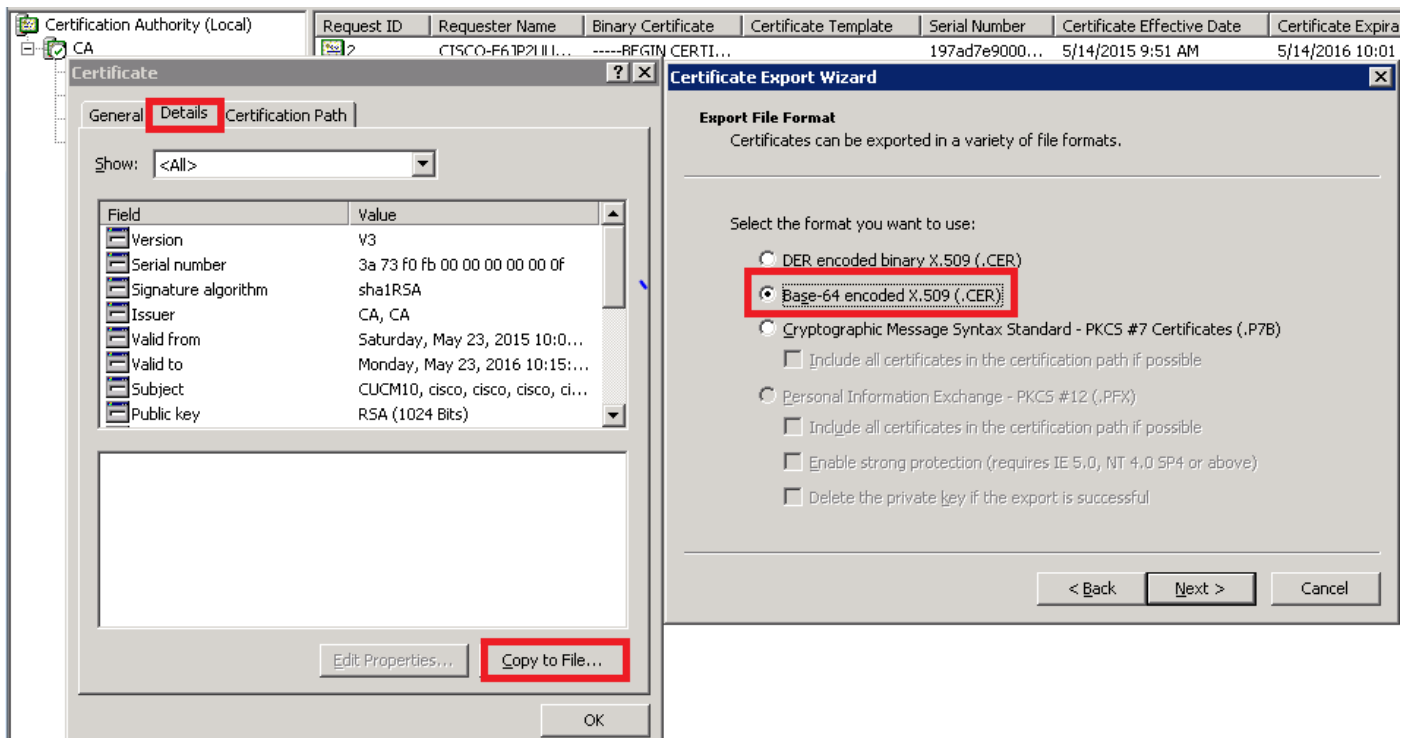
6.



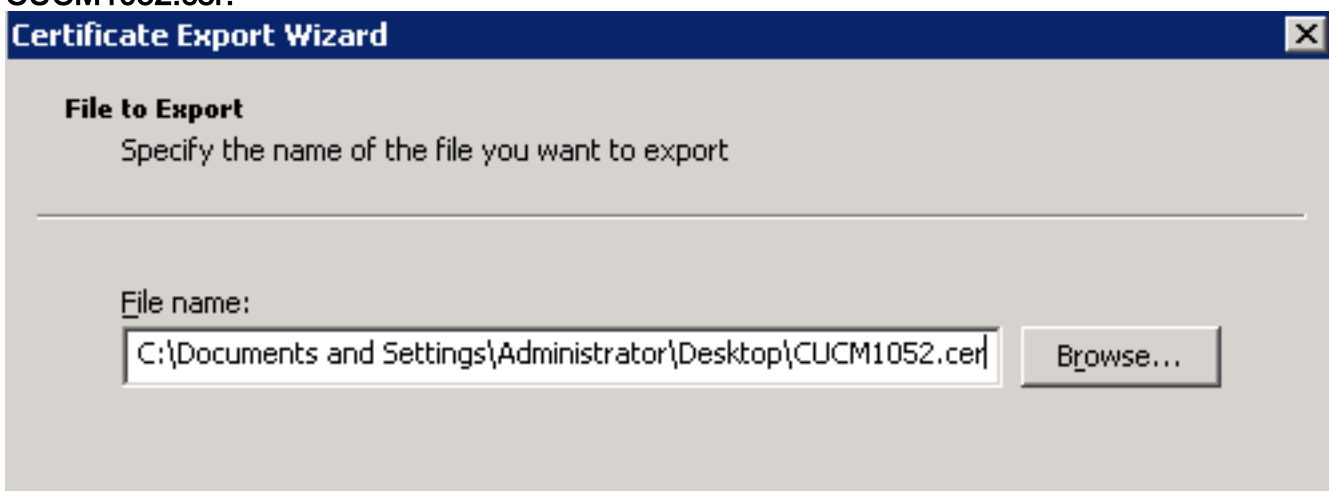
file...

Esportazione guidata certificati, fare clic sul pulsante di opzione X.509(.CER) con codifica Base 64.

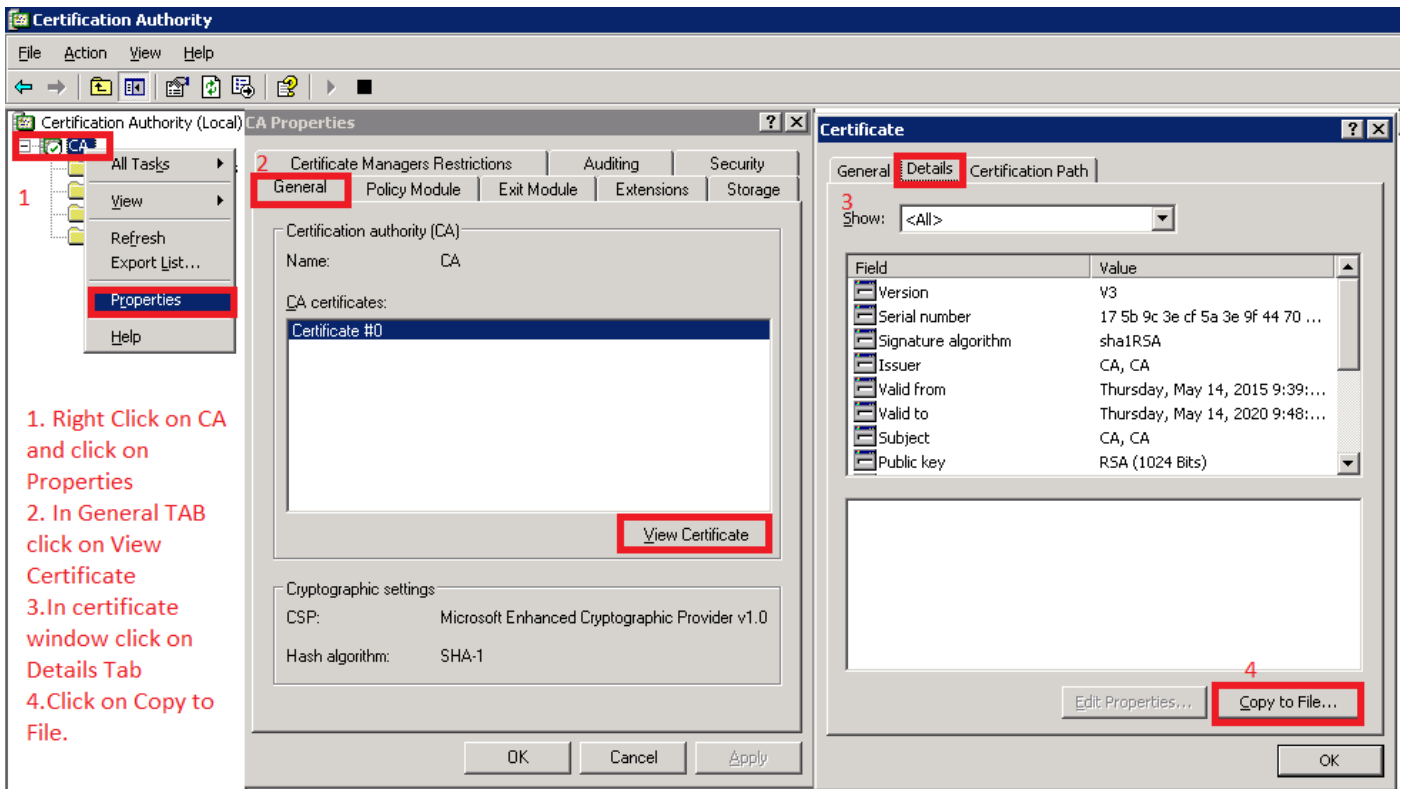
7. Nella finestra



8. Assegnare un nome accurato al file. In questo esempio viene utilizzato il formato CUCM1052.cer.

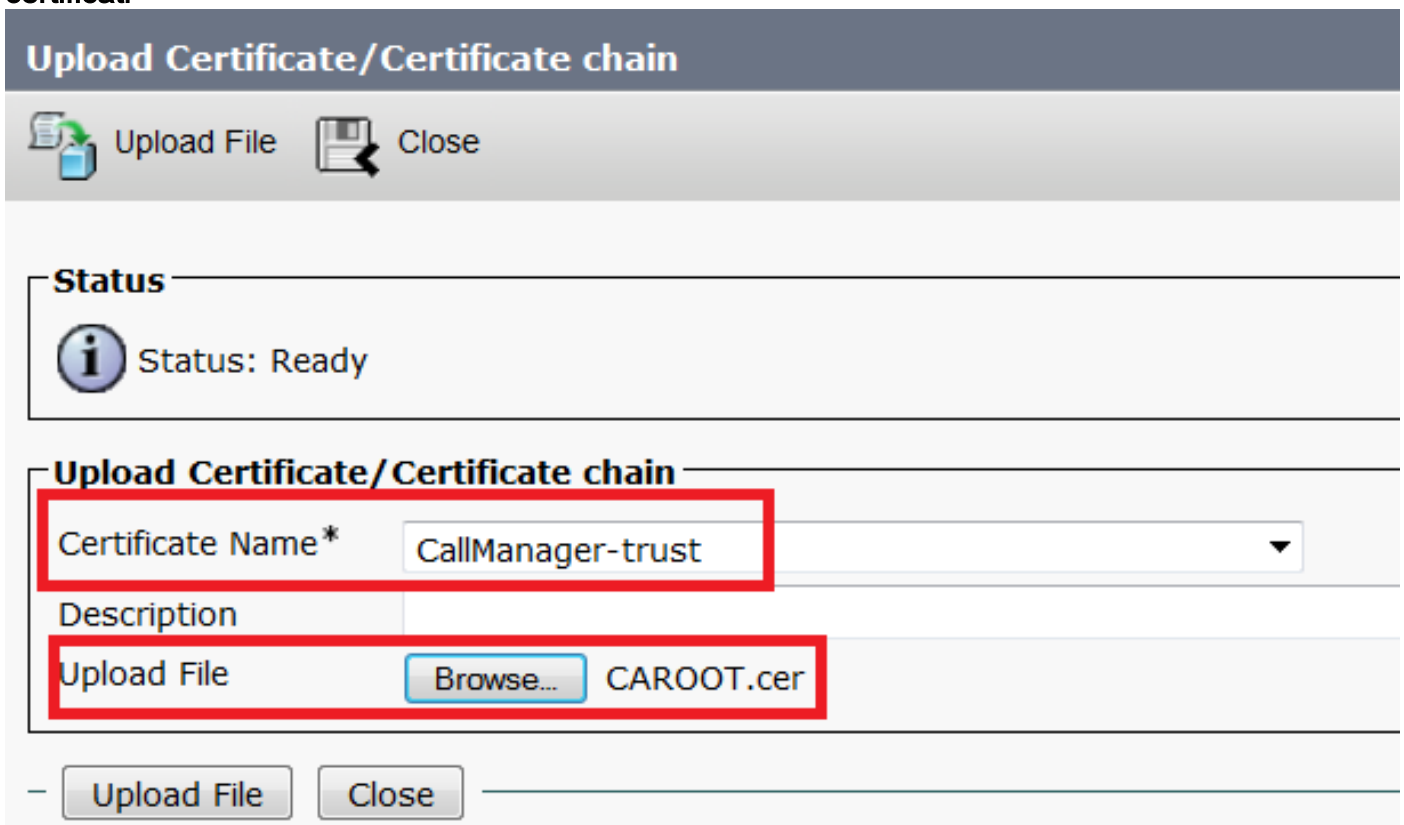


Per CUCM 9.1(2), seguire la stessa procedura. Passaggio 5. Ottenere il certificato radice dalla CA. Aprire la finestra Autorità di certificazione. Per scaricare la CA radice: 1. Fare clic con il pulsante destro del mouse sull'icona della CA e selezionare l'opzione Proprietà. 2. Nella scheda Generale, fare clic su Visualizza certificato. 3. Nella finestra Certificato, fare clic sulla scheda Dettagli. 4. Fare clic su Copia su file...



1. Right Click on CA and click on Properties
2. In General TAB click on View Certificate
3. In certificate window click on Details Tab
4. Click on Copy to File.

Passaggio 6. Caricare il certificato radice CA come attendibilità di CallManager. Per caricare il certificato radice CA, accedere a Amministratore del sistema operativo > Sicurezza > Gestione certificati > Carica certificato/catena di certificati



Nota: Eseguire questi passaggi sia su CUCM (CUCM 9.1(2) che su CUCM 10.5(2)) Passaggio 7. Caricare il certificato CSR CallManager firmato dalla CA come certificato CallManager. Per caricare la firma CA di CallManager CSR, accedere a Amministratore del sistema operativo > Sicurezza > Gestione certificati > Carica certificato/catena di certificati

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

Nota: Eseguire questi passaggi sia su CUCM (CUCM 9.1(2) che su CUCM 10.5(2))
Passaggio 8. Creazione di profili di sicurezza trunk SIP CUCM 9.1(2)

Per creare il profilo di sicurezza trunk SIP, selezionare Sistema > Sicurezza > Profilo di sicurezza trunk SIP. Copiare il profilo trunk SIP non sicuro esistente e assegnargli un nuovo nome.

Nell'esempio, il profilo Trunk SIP non sicuro è stato rinominato con il profilo TLS.

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 Nome soggetto X.509 utilizzare il nome comune (CN) di CUCM 10.5(2) (certificato firmato CA), come mostrato in questa immagine.

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)Passare a Sistema > Sicurezza > Profilo sicurezza trunk SIP.Copiare il profilo trunk SIP non sicuro esistente e assegnargli un nuovo nome. Nell'esempio, il profilo Trunk SIP non sicuro è stato rinominato con il profilo TLS.

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 Nome soggetto X.509 utilizzare il CN di CUCM 9.1(2) (certificato firmato CA) come evidenziato:

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,
]
```

Entrambi i profili SIP Trunk Security hanno impostato una porta in ingresso di 5061, in cui ciascun cluster resta in ascolto sulla porta TCP 5061 per le nuove chiamate SIP TLS in ingresso. **Passaggio 9.**
Creazione di trunk SIP Dopo aver creato i profili di sicurezza, creare i trunk SIP e apportare le modifiche per il parametro di configurazione riportato di seguito sul trunk SIP. CUCM 9.1(2)

1. Nella finestra SIP Trunk Configuration, selezionare la casella di controllo del parametro di configurazione SRTP Allowed.

In questo modo viene protetto il protocollo RTP (Real-time Transport Protocol) da utilizzare per le chiamate su questo trunk. Questa casella deve essere selezionata solo quando si utilizza il protocollo SIP TLS in quanto le chiavi per il protocollo SRTP (Secure Real-time Transport Protocol) vengono scambiate nel corpo del messaggio SIP. La segnalazione SIP deve essere protetta da TLS, altrimenti chiunque con la segnalazione SIP non protetta potrebbe decrittografare il flusso SRTP corrispondente sul trunk.

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. Nella sezione SIP Information della finestra SIP Trunk Configuration, aggiungere l'indirizzo di destinazione, la porta di destinazione e il profilo SIP Trunk Security.

SIP Information

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. Nella finestra SIP Trunk Configuration, selezionare la casella di controllo del parametro di configurazione SRTP Allowed.

Ciò consente di utilizzare il protocollo SRTP per le chiamate su questo trunk. Questa casella deve essere selezionata solo quando si utilizza SIP TLS, perché le chiavi per SRTP vengono scambiate nel corpo del messaggio SIP. La segnalazione SIP deve essere protetta dal TLS perché chiunque disponga di una segnalazione SIP non protetta può decrittografare il flusso Secure RTP corrispondente sul trunk.

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. Nella sezione SIP Information della finestra SIP Trunk Configuration, aggiungere l'indirizzo IP di destinazione, la porta di destinazione e il profilo di sicurezza.

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

Passaggio 10. Creazione di serie di cicli di lavoroIl metodo più semplice consiste nel creare un modello di percorso su ciascun cluster, che punti direttamente al trunk SIP. È inoltre possibile utilizzare i gruppi di route e gli elenchi di route.CUCM 9.1(2) punta al modello di percorso 9898 attraverso il trunk SIP TLS al modello CUCM

10.5(2)

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

La CUCM 10.5(2) punta al modello di percorso 1018 attraverso il trunk SIP TLS al modello CUCM 9.1(2)

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

Verifica Attualmente non è disponibile una procedura di verifica per questa

configurazione. **Risoluzione dei problemi** È possibile eseguire il debug della chiamata SIP TLS eseguendo la procedura seguente. **Raccogli acquisizione pacchetti su CUCM** Per controllare la connettività tra CUCM 9.1(2) e CUCM 10.5(2), acquisire un pacchetto sui server CUCM e controllare il traffico SIP TLS. Il traffico SIP-TLS viene trasmesso sulla porta TCP 5061 come sip-tls. Nell'esempio seguente viene stabilita una sessione CLI SSH per CUCM 9.1(2). CLI Packet Capture sullo schermo Questa CLI stampa l'output sullo schermo per il traffico SIP TLS.

```
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. Acquisizioni CLI su file Questa CLI acquisisce i pacchetti in base all'host e crea un file denominato packets.

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

Riavviare il trunk SIP su CUCM 9.1(2) ed effettuare la chiamata dall'estensione 1018 (CUCM 9.1(2)) all'estensione 9898 (CUCM 10.5(2)) Per scaricare il file dalla CLI, eseguire questo comando:

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

L'acquisizione viene eseguita nel formato standard .cap. In questo esempio viene utilizzato Wireshark per aprire il file packets.cap, ma è possibile utilizzare qualsiasi strumento di visualizzazione per l'acquisizione dei pacchetti.

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	10.106.95.203	10.106.95.200	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	10.106.95.200	10.106.95.200	TLSv1	1161	Application Data
18:46:11.502380	10.106.95.203	10.106.95.200	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. Transmission Control Protocol (TCP) Synchronize (SYN) per stabilire la comunicazione TCP tra CUCM 9.1(2)(Client) e CUCM 10.5(2)(Server).
2. CUCM 9.1(2) invia al client Hello per avviare la sessione TLS.
3. CUCM 10.5(2) invia a Server Hello, Server Certificate e Certificate Request per avviare il processo di scambio dei certificati.
4. Il certificato inviato dal client CUCM 9.1(2) per completare lo scambio di certificati.
5. I dati dell'applicazione che sono segnali SIP crittografati mostrano che la sessione TLS è stata stabilita.

Verificare ulteriormente se vengono scambiati i certificati corretti. Dopo Server Hello, il server CUCM 10.5(2) invia il proprio certificato al 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

- 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 : 0x398b1da600000000000e
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

Il numero di serie e le informazioni sull'oggetto di cui dispone il server CUCM 10.5(2) vengono presentati al client CUCM 9.1(2). Il numero di serie, l'oggetto, l'emittente e le date di validità vengono confrontati con le informazioni riportate nella pagina Gestione certificati di amministrazione del sistema operativo. Il server CUCM 10.5(2) presenta il proprio certificato per la verifica, ora verifica il certificato del client CUCM 9.1(2). La verifica viene eseguita in entrambe le direzioni.

Filter:	Source	Destination	Protocol	Length	Info
18:40:11.450454	10.106.95.203	10.106.95.200	TCP	66	sip-tls > sip-tls [ACK] Seq=59 Ack=1043 Win=11048 Len=0 TSval=1567010844 TSecr=156
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=988797 TSecr=156
18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Fini
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=988797 TSecr=156

Secure Sockets Layer

- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1559
 - Certificates Length: 1552
 - Certificates (1552 bytes)
 - Certificate Length: 901
 - Certificate (id-at-commonName=CUCM9,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
 - signedCertificate
 - version: v3 (2)
 - serialNumber : 0x197ad7e90000000000002
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

In caso di mancata corrispondenza tra i certificati nell'acquisizione dei pacchetti e i certificati nella pagina Web Amministrazione del sistema operativo, i certificati corretti non vengono caricati. I certificati corretti devono essere caricati nella pagina Admin Cert del sistema operativo. Raccogli tracce CUCM Le tracce CUCM possono inoltre essere utili per determinare quali messaggi vengono scambiati tra i server CUCM 9.1(2) e CUCM 10.5(2) e se la sessione SSL è stabilita correttamente o meno. Nell'esempio sono state raccolte le tracce di CUCM 9.1(2). Flusso di chiamata: Ext 1018 >

CUCM 9.1(2) > SIP TLS TRUNK > CUCM 10.5(2) > Ext 9898++ Analisi cifre

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqc="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 è in uso sulla porta 5061 per questa chiamata.

```
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
```

++ Messaggio SDL (Signal Distribution Layer) SIPCertificateInd fornisce dettagli sul CN soggetto e informazioni sulla connessione.

```
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 =
```