

# SIP-TLS between IOS SIP Gateway and CallManager Configuration Example

Document ID: 98746

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Configure

- Network Diagram
- Configurations
- Download the Cisco CallManager Self-signed Certificate
- Cisco IOS SIP Gateway Configuration
- Upload Cisco IOS SIP Gateway s Certificate to Cisco Unified CallManager
- SIP Trunk Configuration in Cisco CallManager

### Verify

### Troubleshoot

- Debug Commands

### Related Information

---

## Introduction

This document provides a sample configuration for SIP signaling encryption (SIP over Transport Layer Security) between a Cisco IOS<sup>®</sup> Gateway and Cisco Unified CallManager.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Gateway: Cisco 2821, Cisco IOS Software Release 12.4(15)T1 with Advanced Enterprise Services Feature set
- Cisco CallManager 5.1.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

# Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool ( registered customers only) in order to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:



## Configurations

This document uses these configurations:

- Download the Cisco CallManager Self–signed Certificate
- Cisco IOS SIP Gateway Configuration
- Upload the Cisco IOS SIP Gateway Certificate to Cisco Unified CallManager
- SIP Trunk Configuration in Cisco CallManager

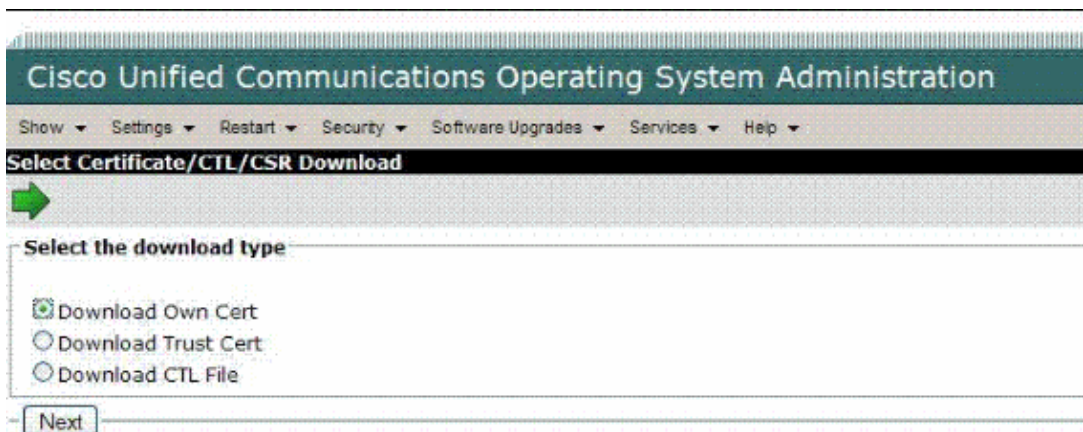
## Download the Cisco CallManager Self–signed Certificate

Complete these steps:

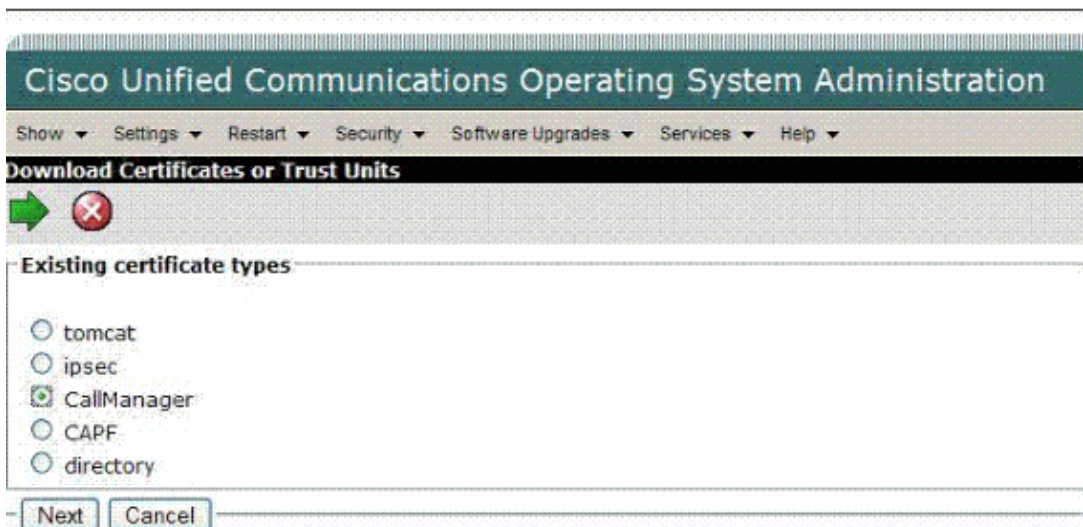
1. Log into the Cisco Unified OS Administration Page in Cisco CallManager at **[https://<ccm ip address>/platform\\_gui/](https://<ccm ip address>/platform_gui/)**, and choose **Security > Certificate Management > Download Certificate/CTL**.



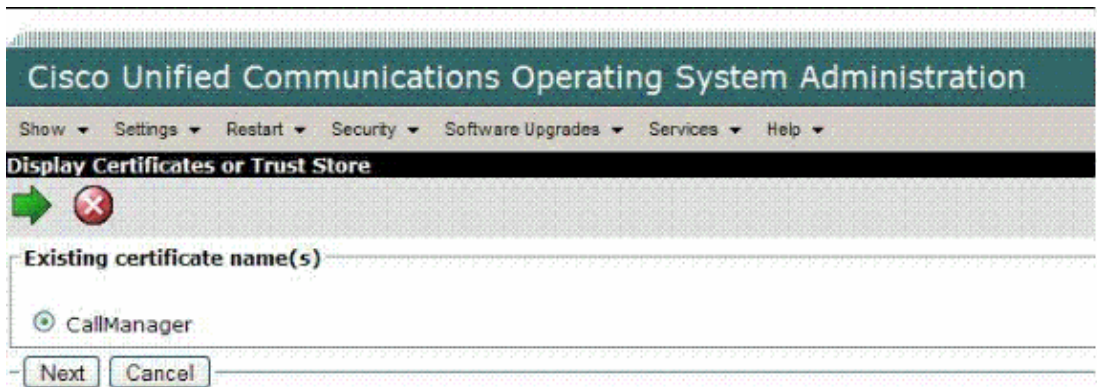
2. Click **Download Own Cert.**



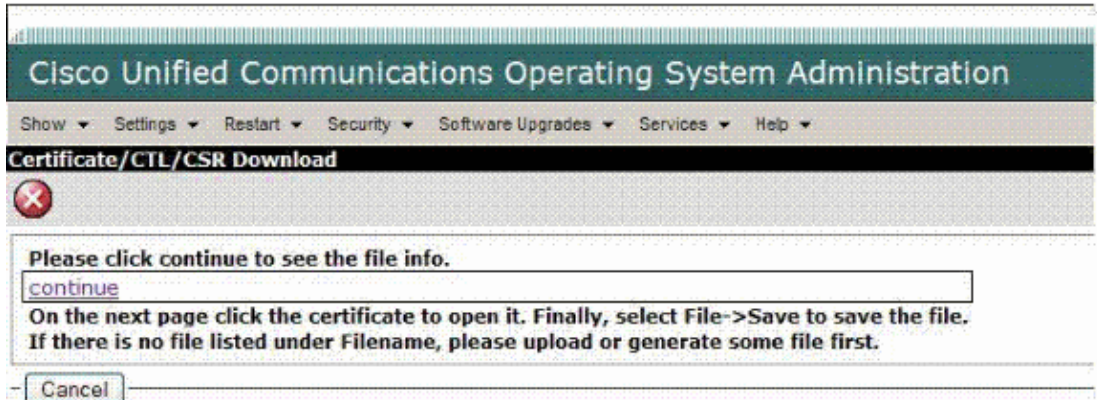
3. Click **CallManager** as the Existing certificate type.



4. Click the **Certificate Name.**



5. Click **Continue**.



6. Right-click the **CallManager.pem** link, and select **Save link as** in order to download the certificate.



## Cisco IOS SIP Gateway Configuration

```

IOS SIP Gateway Configuration

maui-soho-01#

!--- Enable IP TCP MTU Path Discovery.

ip tcp path-mtu-discovery

!--- Configure NTP Server.

ntp server 172.18.108.15

!--- Upload the CCM Certificate to Cisco IOS Gateway.

crypto pki trustpoint CCM-Cert

```

```
enrollment terminal
```

```
revocation-check none
```

```
!--- Download the Cisco CallManager certificate, and paste  
!--- the contents of the certificate, pem format.
```

```
Router(config)#crypto ca authenticate CCM-Cert
```

```
Enter the base 64 encoded CA certificate.
```

```
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
```

```
MIICIjCCAYugAwIBAgIIS4xQN3bIZUowDQYJKoZIhvcNAQEFBQAwFzEVMBMGAlUE  
AxMMUlRQTVMtQ0NNLTUxMB4XDTA3MDcyMzIzMjI0OVoXDTEyMDcyMzIzMjI0OVow  
FzEVMBMGAlUEAxMMUlRQTVMtQ0NNLTUxMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB  
iQKBgQD6HIRcgDXQmO/EWosnaMBaoqjzARIR0erx3luR9W0iaZqsgRY+Am5/E3FG  
n1nJ/4NVmA45z1Q54vK0WULXgMBGANGHnBZFCNiJOiNeBfiEh1LGGMreVTLFqKB/  
lNAMtTppc0AVyYFjAAcJtZfUGxolZCanY5TWfmlwGBMIDhnqQQIDAQABo3cWdTAL  
BgNVHQ8EBAMCARwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMCMCBggrBgEF  
BQCDBTAeBgNVHREEFzAVhhNzaXA6Q049U1RQTVMtQ0NNLTUxMB0GAlUdDgQWBBQr  
pCXbwcRZ09Ak07V0HgHihikpZzANBgkqhkiG9w0BAQUFAA0BgQAuNQAqVKKoZxUD  
HCBIA292qZSsOht859FY3UJkWfGD+kjlGhjgjlxEQcaJOa7pDlorzH+HQIjFpcv6  
lcl0tOdOrs2L6IAGd9e5DQ3qDwWxaB7TIsBPTkv9FLVURnKtJtVHbqjMd+AAtsDl  
/DV5TbDUdre6Orglmm4uaMdrYzt1kQ==
```

```
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
```

```
    Fingerprint MD5: 1EF154E3 70E40379 1C7003B9 B29E111B
```

```
    Fingerprint SHA1: CAFA0F83 B04B2E65 71104B73 64BF6AEB ABE9EED9
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

```
!--- Configure a trustpoint in order to generate the self-signed  
!--- certificate of the Gateway.
```

```
crypto pki trustpoint CCM-SIP-1
```

```
  enrollment selfsigned
```

```
  fqdn none
```

```
  subject-name CN=SIP-GW
```

```
  revocation-check none
```

```
  rsakeypair CCM-SIP-1
```

```
Router(config)#crypto ca enroll CCM-SIP-1
```

```
% The fully-qualified domain name will not be included in the certificate
```

```
% Include the router serial number in the subject name? [yes/no]: no
```

```
% Include an IP address in the subject name? [no]: no
```

```
Generate Self Signed Router Certificate? [yes/no]: yes
```

```
Router Self Signed Certificate successfully created
```

```
! View the certificate in PEM format, and copy the Self-signed CA certificate
```

*!--- (output starting from ----BEGIN to CERTIFICATE---- ) to a file named SIP-GW.pem*

```
Router(config)#crypto pki export CCM-SIP-1 pem terminal
```

```
% Self-signed CA certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZTSVAt  
RlcvHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT  
SVAtRlcvXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW1S/h4CZC  
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8TvJJKwID  
AQABo3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGAlUdEQQVMOCEUYzNDAuMjguMjUt  
MjgwMC0yMB8GAlUdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCKi62MB0GAlUdDgQW  
BBReoJzqaOlWPARY+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhnQS4EKcP6  
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4mlsIMzDAHfsl7dJlB2IOw9Sk  
s980Np7dLJU=
```

```
-----END CERTIFICATE-----
```

```
% General Purpose Certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQDEwZTSVAt  
RlcvHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT  
SVAtRlcvXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW1S/h4CZC  
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8TvJJKwID  
AQABo3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGAlUdEQQVMOCEUYzNDAuMjguMjUt  
MjgwMC0yMB8GAlUdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCKi62MB0GAlUdDgQW  
BBReoJzqaOlWPARY+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhnQS4EKcP6  
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4mlsIMzDAHfsl7dJlB2IOw9Sk  
s980Np7dLJU=
```

```
-----END CERTIFICATE-----
```

*!--- Configure the SIP stack in the Cisco IOS GW to use the self-signed  
!--- certificate of the router in order to establish a SIP TLS connection from/to  
!--- Cisco CallManager.*

```
sip-ua
```

```
crypto signaling remote-addr 172.18.110.84 255.255.255.255 trustpoint CCM-SIP-1 strict-cipher
```

*!--- Configure the T1 PRI.*

```
controller T1 1/0/0  
framing esf  
linecode b8zs  
pri-group timeslots 1-24
```

*!--- Configure the ISDN switch type and incoming-voice under the D-channel  
!--- interface.*

```
interface Serial1/0/0:23  
no ip address  
encapsulation hdlc
```

```
isdn switch-type primary-ni
isdn incoming-voice voice
no cdp enable
```

*!--- Configure a POTS dial-peer that is used as an inbound dial-peer for calls that come in across the T1 PRI line.*

```
dial-peer voice 2 pots
description PSTN PRI Circuit
destination-pattern 9T
incoming called-number .
direct-inward-dial
port 1/0/0:23
```

*!--- Configure an outbound voip dial-peer in order to route calls to the Cisco CallManager.*

```
dial-peer voice 3 voip
destination-pattern 75...
session protocol sipv2
session target ipv4:172.18.110.84:5061
session transport tcp tls
dtmf-relay rtp-nte
codec g711ulaw
```

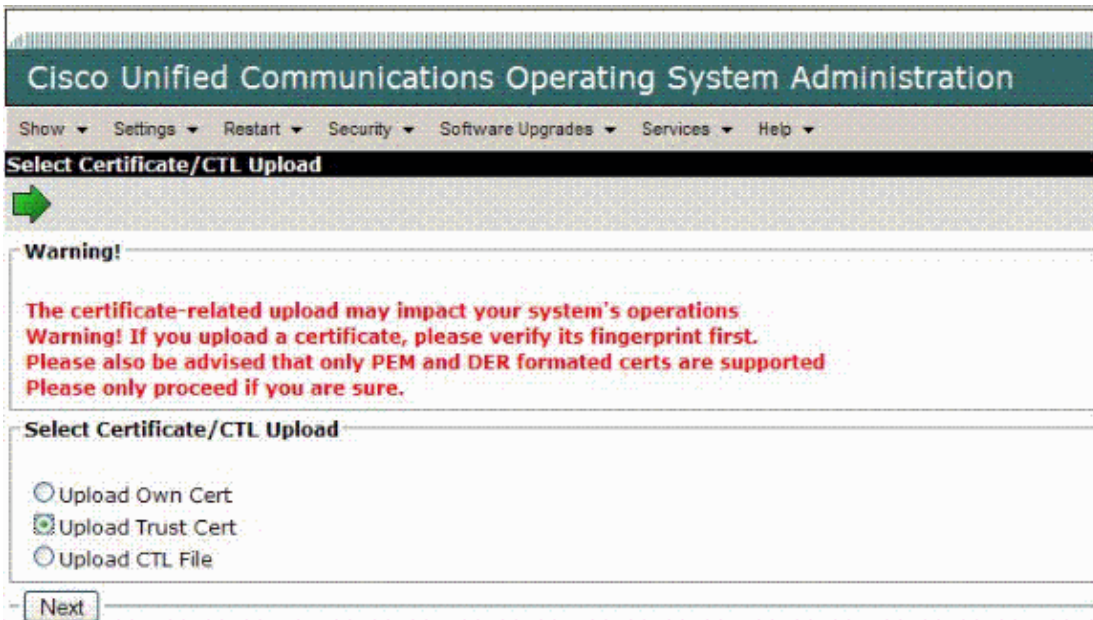
## Upload Cisco IOS SIP Gateway s Certificate to Cisco Unified CallManager

Complete these steps:

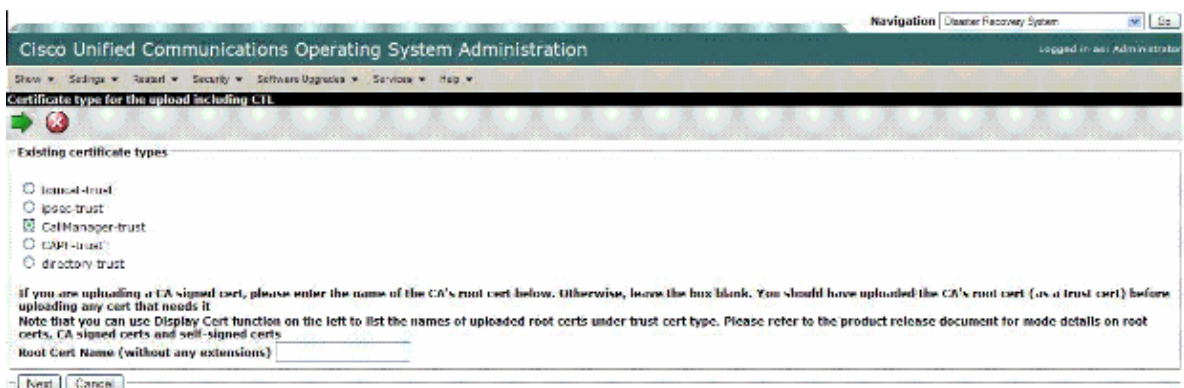
1. Log into the Cisco Unified OS Administration Page in Cisco CallManager at [https://<ccm ip address>/platform\\_gui/](https://<ccm ip address>/platform_gui/), and choose **Security > Certificate Management > Upload Certificate/CTL**.



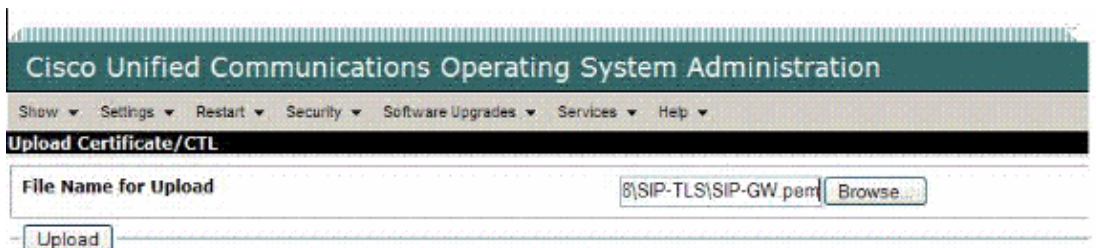
2. Click **Upload Trust Cert.**



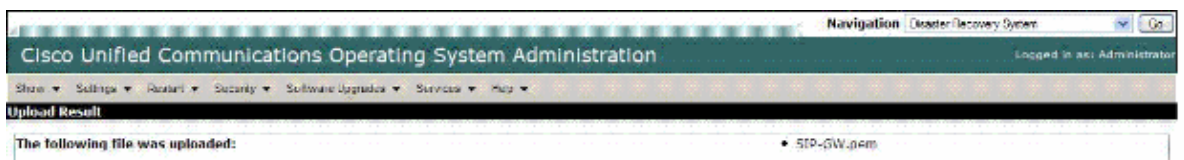
3. Click **CallManager-trust**.



4. Enter or browse to the location of the Cisco IOS Certificate, the **.pem** file, and click **Upload**.



5. Verify the upload result.



## SIP Trunk Configuration in Cisco CallManager

Complete these steps:

1. Log into the Cisco Unified OS Administration Page in CallManager at **https://<ccm ip address>/ccmadmin/**. Configure a SIP Trunk Security Profile:

- a. Choose **System > Security Profile > SIP Trunk Security Profile**.
- b. Click the **Add New** button with the parameters shown in this figure:

**SIP Trunk Security Profile Information**

Name*	IOS-SIP-TLS
Description	
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	SIP-GW
Incoming Port*	5051
<input type="checkbox"/> Enable Application Level Authorization	
<input checked="" type="checkbox"/> Accept Presence Subscription	
<input checked="" type="checkbox"/> Accept Out-of-Dialog REFER	
<input checked="" type="checkbox"/> Accept Unsolicited Notification	
<input checked="" type="checkbox"/> Accept Replaces Header	

\* - indicates required item.

2. Configure a SIP Trunk:

- a. Choose **Device > Trunk**.
- b. Click the **Add New** button.
- c. Select **SIP Trunk** for Trunk Type, as shown:

**Device Information**

Product:	SIP Trunk
Device Protocol:	SIP
Device Name*	IOS-SIP-TLS-Trunk
Description	
Device Pool*	Default
Call Classification*	Use System Default
Media Resource Group List	<None>
Location*	Hub_None
AAR Group	<None>
Packet Capture Mode*	None
Packet Capture Duration	0
<input type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> Unattended Port	

**Multilevel Precedence and Preemption (MLPP) Information**

MLPP Domain	<None>
-------------	--------

\* - indicates required item.

**Call Routing Information**

**Inbound Calls**

Significant Digits\* All

Connected Line ID Presentation\* Default

Connected Name Presentation\* Default

Calling Search Space < None >

ANR Calling Search Space < None >

Prefix DN

Redirecting Diversion Header Delivery - Inbound

**Outbound Calls**

Calling Party Selection\* Originator

Calling Line ID Presentation\* Default

Calling Name Presentation\* Default

Caller ID DN

Caller Name

Redirecting Diversion Header Delivery - Outbound

---

**SIP Information**

Destination Address\* 14.1.103.62

Destination Address is an SRV

Destination Port\* 5061

MTP Preferred Originating Codec\* ITU-T G.711

Presence Group\* Standard Presence group

SIP Trunk Security Profile\* IOS-SIP-TLS

Remoting 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\* RFC 2833

3. Configure a Route pattern:

- a. Choose **Call Routing > Route/Hunt > Route Pattern**.
- b. Click the **Add New** button, as shown:

System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Administration > Help > Log Off

**Route Pattern Configuration** Related Links: [Back To Find/List](#)

**Status**

Update successful

**Pattern Definition**

Route Pattern\* 8XXXXXXX

Route Partition < None >

Description

Numbering Plan - Not Selected -

Route Filter < None >

MLPP Precedence\* Default

Gateway/Route List\* IOS-SIP-TLS-Trunk

Route Option

Route this pattern

Block this pattern No Error

Cell Classification\* OffNet

Allow Device Override  Provide Outside Dial Tone  Allow Overlap Sending  Urgent Priority

Require Prepaid Authorization Code

Authorization Level\* 0

Require Client Matter Code

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Line ID Presentation\* Default

Calling Name Presentation\* Default

**Connected Party Transformations**

Connected Line ID Presentation\* Default

Connected Name Presentation\* Default

## Verify

Use this section in order to confirm that your configuration works properly at the Cisco IOS SIP Gateway.

The Output Interpreter Tool ( registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

- **Show crypto pki certificate verbose CCM-SIP-1**

Router Self-Signed Certificate

Status: Available

Version: 3

Certificate Serial Number: 0x1

Certificate Usage: General Purpose

Issuer:

cn=SIP-GW

Subject:

Name: SIP-GW

cn=SIP-GW

Validity Date:

start date: 16:01:07 EST Sep 5 2007

end date: 20:00:00 EST Dec 31 2019

Subject Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Signature Algorithm: MD5 with RSA Encryption

Fingerprint MD5: 3F9612FB C0E435F1 F445B5C4 0344E6A9

Fingerprint SHA1: E6520255 B799818F C1067042 1A7E2EE9 4DDFD0C8

X509v3 extensions:

X509v3 Subject Key ID: 5EA09CEA 68ED563C 0472F899 B4AFC0DC 422A2EB6

X509v3 Basic Constraints:

CA: TRUE

X509v3 Subject Alternative Name:

F340.28.25-2800-2

X509v3 Authority Key ID: 5EA09CEA 68ED563C 0472F899 B4AFC0DC 422A2EB6

Authority Info Access:

Associated Trustpoints: CCM-SIP-1

- **Show crypto pki certificate verbose CCM-Cert**

CA Certificate

Status: Available

Version: 3

Certificate Serial Number: 0x4B8C503776C8654A

Certificate Usage: General Purpose

Issuer:

cn=RTPMS-CCM-51

Subject:

cn=RTPMS-CCM-51

Validity Date:

start date: 19:22:49 EST Jul 23 2007

end date: 19:22:49 EST Jul 23 2012

Subject Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Signature Algorithm: SHA1 with RSA Encryption

Fingerprint MD5: 1EF154E3 70E40379 1C7003B9 B29E111B

Fingerprint SHA1: CAFA0F83 B04B2E65 71104B73 64BF6AEB ABE9EED9

X509v3 extensions:

X509v3 Key Usage: BC000000

Digital Signature

Key Encipherment

Data Encipherment

Key Agreement

Key Cert Sign

X509v3 Subject Key ID: 2BA425DB C1C459D3 D0243BB5 741E01E2 8622A967

X509v3 Subject Alternative Name:

Authority Info Access:

Associated Trustpoints: CCM-Cert

• **Show sip-ua connection tcp tls detail**

Total active connections	: 2
No. of send failures	: 0
No. of remote closures	: 0
No. of conn. failures	: 2
No. of inactive conn. ageouts	: 0

Max. tls send msg queue size of 0, recorded for 0.0.0.0:0

TLS client handshake failures : 2

TLS server handshake failures : 0

-----Printing Detailed Connection Report-----

Note:

\*\* Tuples with no matching socket entry

- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'  
to overcome this error condition

++ Tuples with mismatched address/port entry

- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>  
id <connid>' to overcome this error condition

Remote-Agent:172.18.110.84, Connections-Count:2

Remote-Port Conn-Id Conn-State WriteQ-Size

=====

5061 1 Established 0

51180 2 Established 0

• Show call active voice brief

11F0 : 7 8990160ms.1 +2670 pid:20001 Answer 7960 active

dur 00:00:10 tx:483/83076 rx:510/81600

Tele 1/0/0:23 (228) [1/0/0.1] tx:9660/9660/0ms g711ulaw noise:0 acom:0 i/0:0/0 dB

11F0 : 8 8990980ms.1 +1840 pid:3 Originate 75001 active

dur 00:00:10 tx:483/1246360336 rx:513/82080

IP 14.50.202.26:28232 SRTP: off rtt:0ms pl:4720/1ms lost:0/0/0 delay:0/0/0ms

g711ulaw TextRelay: off media inactive detected:n media contrl rcvd:n/a

timestamp:n/a long duration call detected:n long duration call

duration:n/a timestamp:n/a

Telephony call-legs: 1

SIP call-legs: 1

H323 call-legs: 0

Call agent controlled call-legs: 0

```
SCCP call-legs: 0
Multicast call-legs: 0
Media call-legs: 0
Total call-legs: 2
```

## Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

### Debug Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

Configure the Cisco IOS Gateway to log the debugs in its logging buffer and disable **logging console**.

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

These are the commands used in order to configure the Gateway to store the debugs in the logging buffer:

- **service timestamps debug datetime msec**
- **service sequence**
- **no logging console**
- **logging buffered 5000000 debug**
- **clear log**

These are the commands used in order to debug the configuration in this document:

- **debug isdn q931**
- **debug voip ccapi inout**
- **debug ccsip all**
- **debug ssl openssl errors**
- **debug ssl openssl msg**
- **debug ssl openssl states**

---

## Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation – Cisco Systems**

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Nov 29, 2007

Document ID: 98746

---