

# SIP-TLS entre el gateway del SORBO IOS y el ejemplo de la configuración del CallManager

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Descargue el certificado autofirmado del Cisco CallManager](#)

[Configuración de gateway del SORBO del Cisco IOS](#)

[El certificado del gateway del SORBO del Cisco IOS de la carga al Cisco Unified CallManager](#)

[Configuración del tronco del SORBO en el Cisco CallManager](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos de Debug](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento suministra una configuración de ejemplo para el cifrado de la señalización SIP (SIP sobre Transport Layer Security) entre Cisco IOS® Gateway y Cisco Unified CallManager.

## [prerrequisitos](#)

### [Requisitos](#)

No hay requisitos específicos para este documento.

### [Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS Gateway: Cisco 2821, Cisco IOS Software Release 12.4(15)T1 con el conjunto de características avanzado de los Enterprise Service
- Cisco CallManager 5.1.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

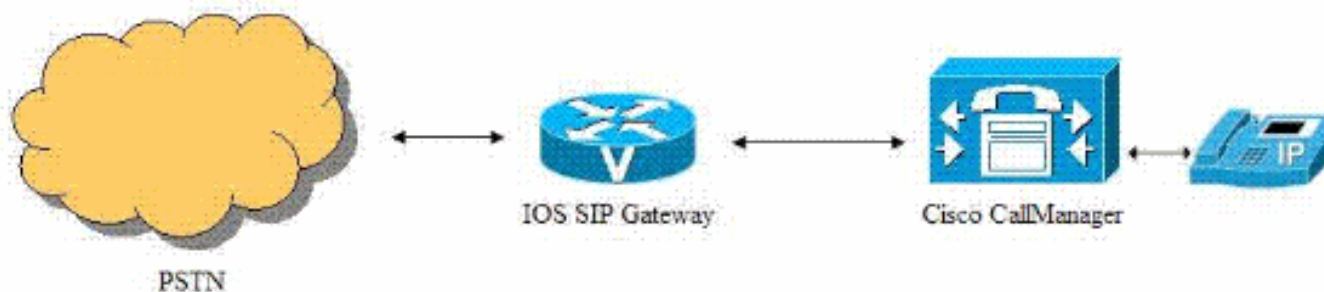
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Note:** Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configuraciones

En este documento, se utilizan estas configuraciones:

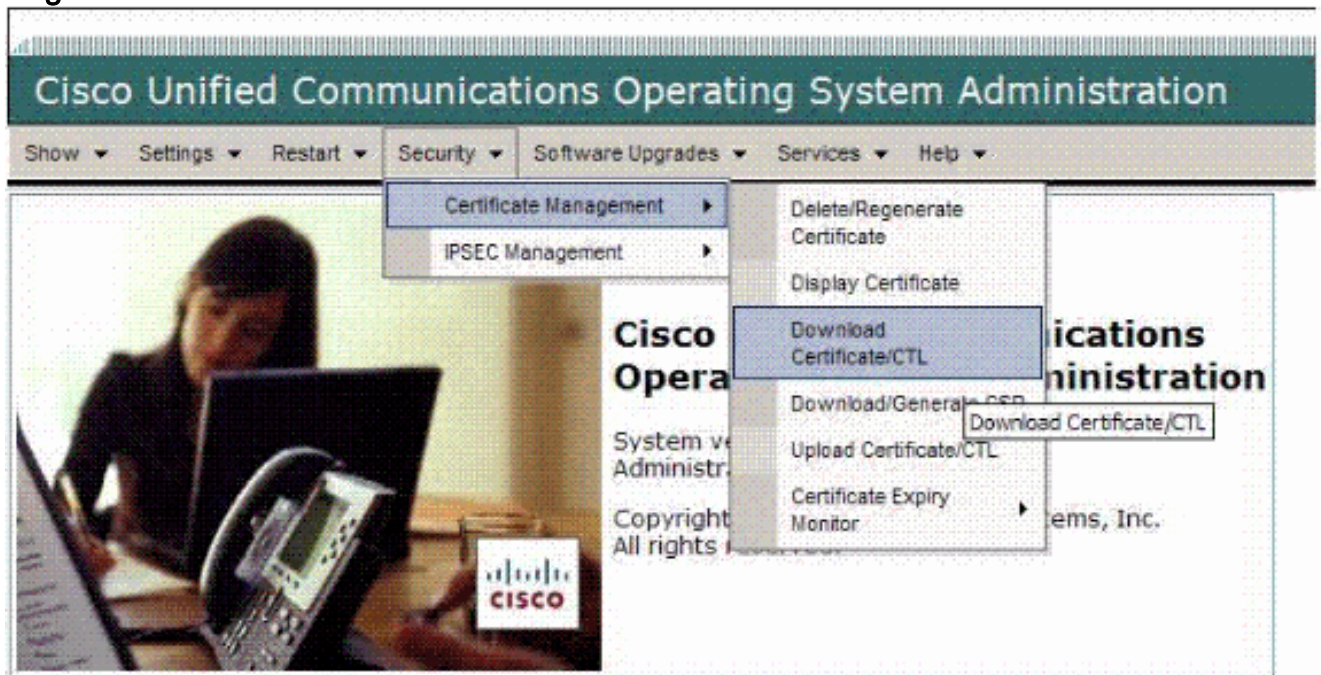
- [Descargue el certificado autofirmado del Cisco CallManager](#)
- [Configuración de gateway del SORBO del Cisco IOS](#)
- [Cargue el certificado del gateway del SORBO del Cisco IOS al Cisco Unified CallManager](#)
- [SORBA la configuración del tronco en el Cisco CallManager](#)

## Descargue el certificado autofirmado del Cisco CallManager

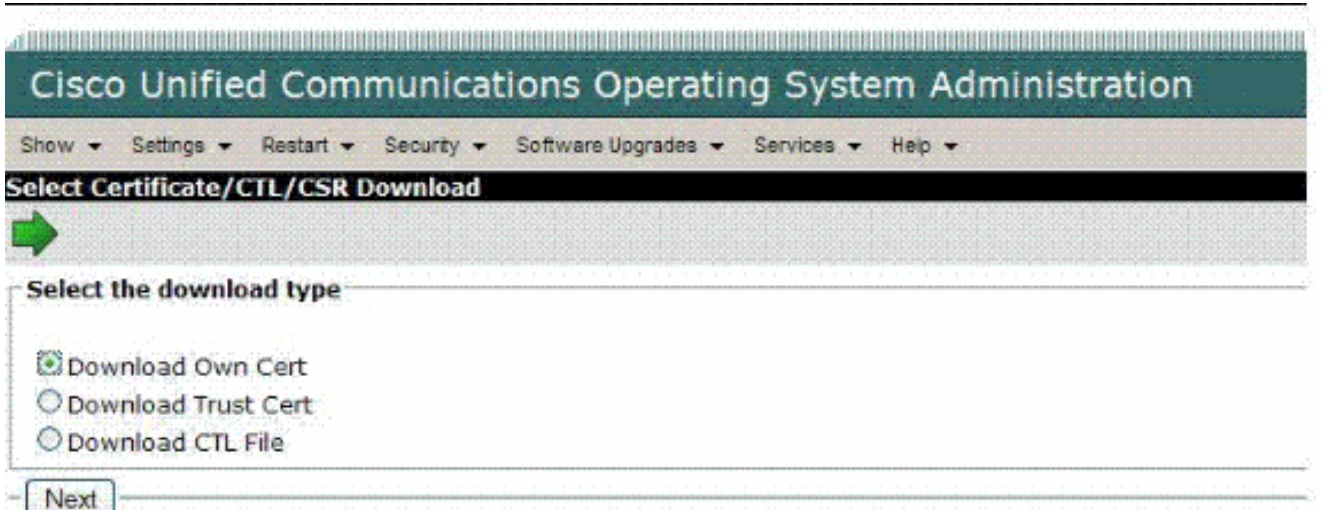
Complete estos pasos:

1. El registro en la página de administración unificada Cisco OS en el Cisco CallManager en el IP Address >/platform\_gui/del <ccm de https://, y elige el Certificate Management

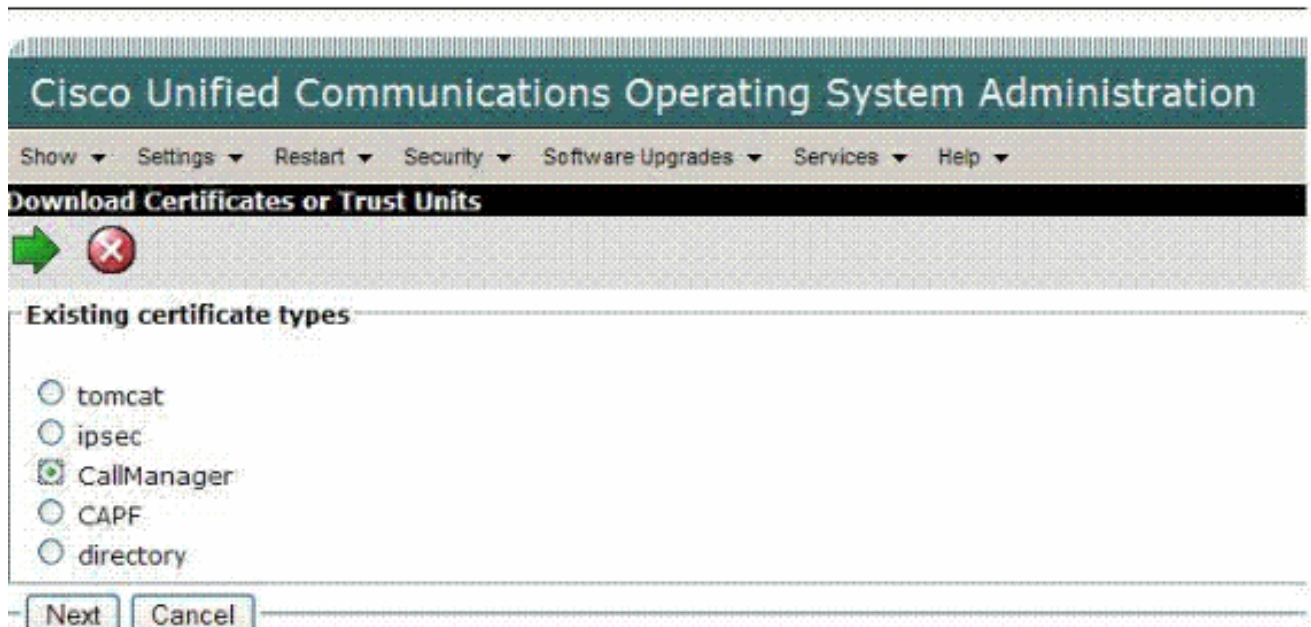
(Administración de certificados) > la **descarga Certificate/CTL de la Seguridad.**



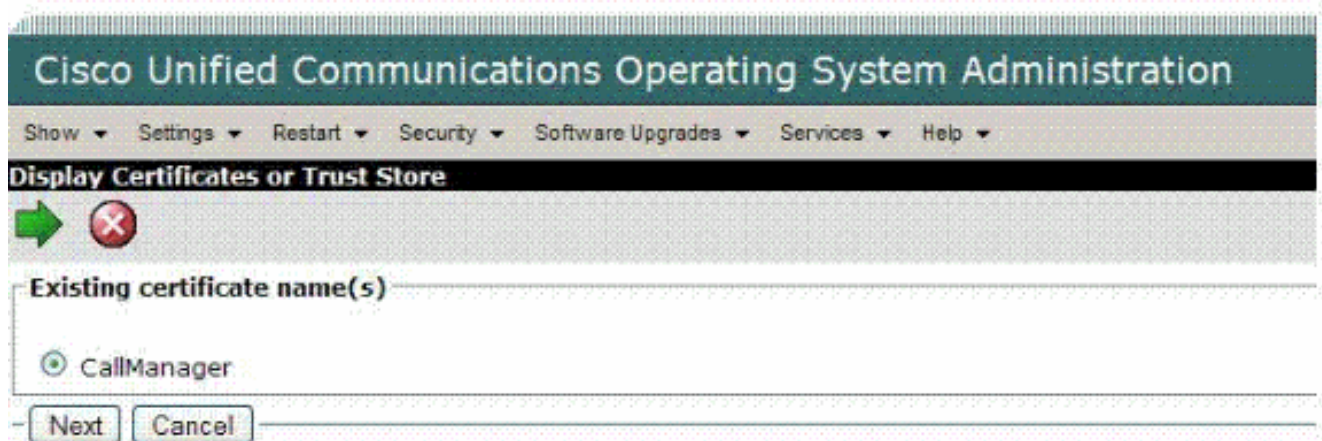
2. La **descarga del teclado** posee el **CERT.**



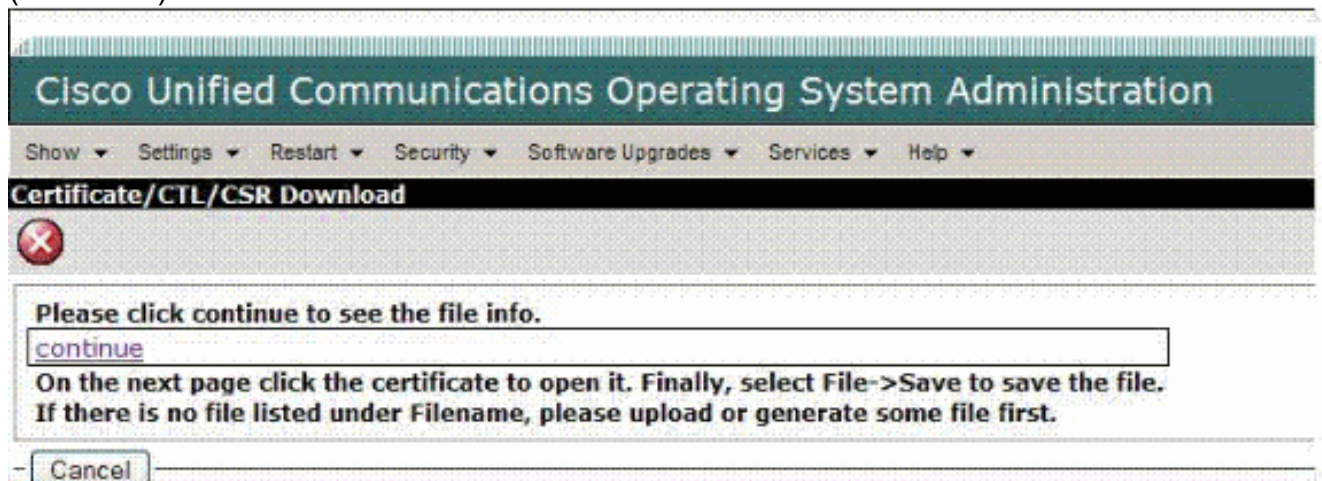
3. **CallManager del teclado** como el tipo del certificado existente.



- Haga clic el nombre del certificado.



- Haga clic en **Continue** (Continuar).



- Haga clic con el botón derecho del ratón el link **CallManager.pem**, y Savelink selecto como **para** descargar el certificado.



Filename	Size
<a href="#">CallManager.pem</a>	0.7 kb

Apache Tomcat/5.0

## [Configuración de gateway del SORBO del Cisco IOS](#)

### Configuración de gateway del SORBO IOS

```

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-----
MIICIjCCAYugAwIBAgIIS4xQN3bIZUowdQYJKoZIhvcNAQEFBQAwFzEV
MBMGA1UE
AxMMU1RQTVMtQ0NNLTUxMB4XDTA3MDcyMzIzMjI0OVoxMDTEyMDcyMzIz
MjI0OVow
FzEVMBMGA1UEAxMMU1RQTVMtQ0NNLTUxMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCB
iQKBgQD6HIRcgDXQmO/EWosnaMBaoqjzARIR0erx31uR9W0iaZqsgRY+
Am5/E3FG
nlnJ/4NVmA45z1Q54vK0WULXgMBGANGHnBZFCNiJOiNeBfiEh1LGGMre
VTLFqKB/
lNAMtTppc0AVyYFjAacJtZfUGxolZCanY5TWfmlwGBMIDhngQQIDAQAB
o3cwtAL
BgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAWEGCCsGAQUFBwMC
BggrBgEF
BQcDBTAeBgNVHREEFzAVhhNzaXA6Q049U1RQTVMtQ0NNLTUxMB0GA1Ud
DgQWBQBQr
pCXbwcRZ09Ak07V0HgHihiKpZzANBgkqhkiG9w0BAQUFAAOBgQAvNQqa
VKKoZxUD
HCBIA292qZSsOht859FY3UJkWfGD+kjlGhjgjlxEQcaJOa7pDlorzH+H
QIjFpcv6
1cl0tOdOrs2L6IAGd9e5DQ3qDwWxaB7TIsBPTkv9FLVURnKtJtVHbqjM
d+AAtdl /DV5TbDUDre6Orglmm4uaMdrYztlkQ== -----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

```

```

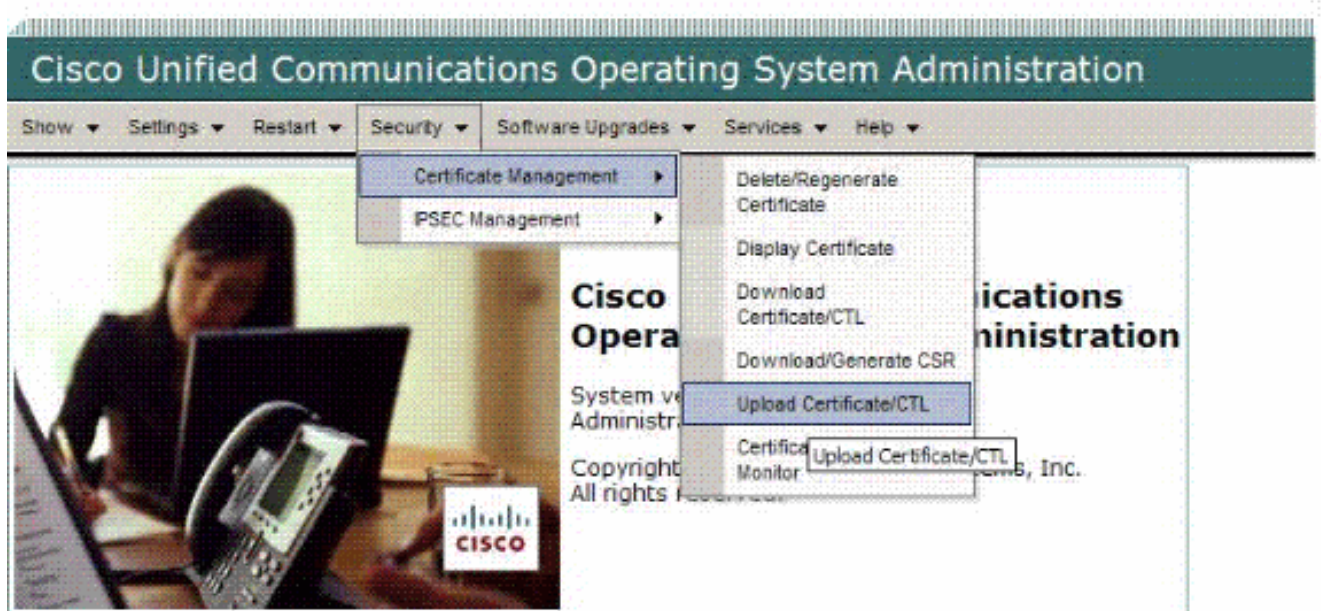
Certificate? [yes/no]: yes Router Self Signed
Certificate successfully created !- View the certificate
in PEM format, and copy the Self-signed CA certificate
!--- (output starting from "----BEGIN" to "CERTIFICATE--
--") to a file named SIP-GW.pem Router(config)#crypto
pki export CCM-SIP-1 pem terminal % Self-signed CA
certificate: -----BEGIN CERTIFICATE-----
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQD
EwZTSVAt
RlcwHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYD
VQQDEwZT
SVAtRlcwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW
1S/h4CZC
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8
TvJJKwID
AQABO3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGA1UdEQQVMBOCEUYzNDAu
MjguMjUt
MjgwMC0yMB8GA1UdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCki62MB0G
A1UdDgQW
BBReoJzqaO1WPARY+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhn
QS4EKcP6
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4m1sIMzDAHfsl7dJl
B2IOw9Sk s980Np7dLJU= -----END CERTIFICATE----- %
General Purpose Certificate: -----BEGIN CERTIFICATE-----
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQD
EwZTSVAt
RlcwHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYD
VQQDEwZT
SVAtRlcwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW
1S/h4CZC
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8
TvJJKwID
AQABO3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGA1UdEQQVMBOCEUYzNDAu
MjguMjUt
MjgwMC0yMB8GA1UdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCki62MB0G
A1UdDgQW
BBReoJzqaO1WPARY+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhn
QS4EKcP6
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4m1sIMzDAHfsl7dJl
B2IOw9Sk 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

```

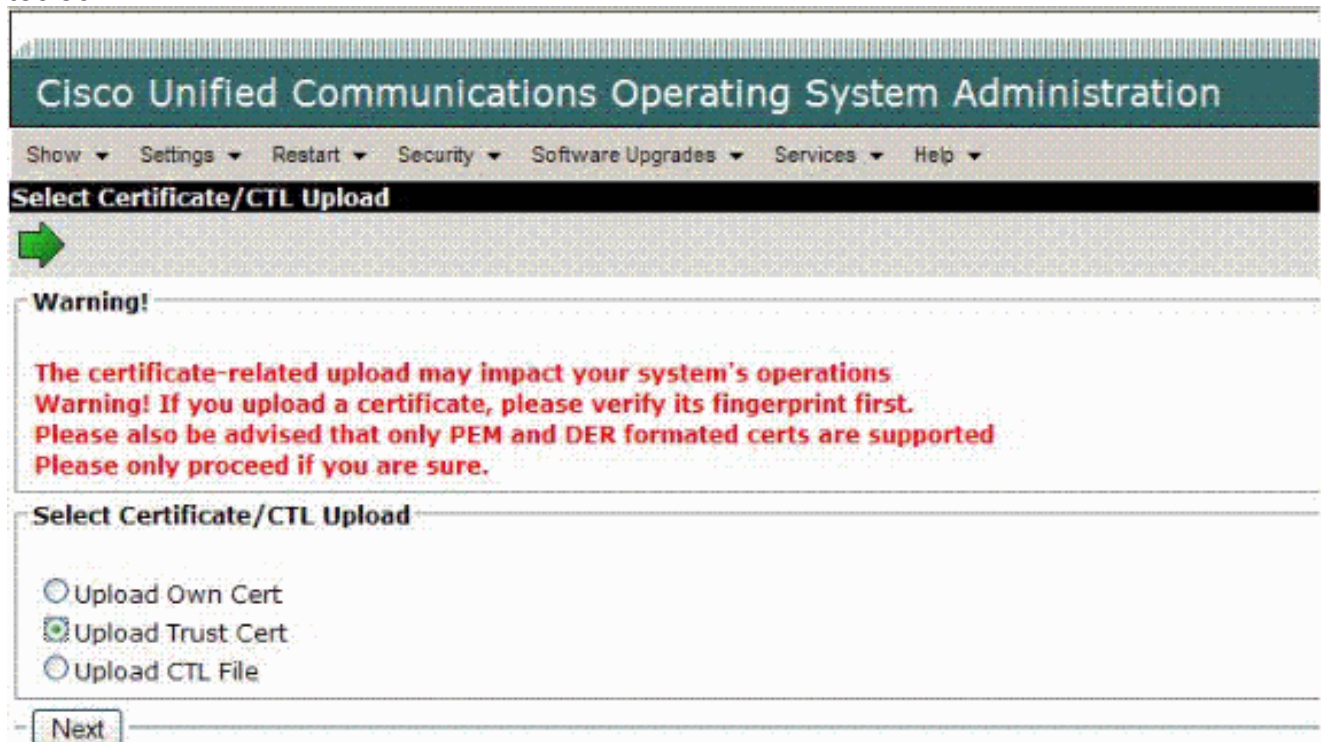
## CallManager

Complete estos pasos:

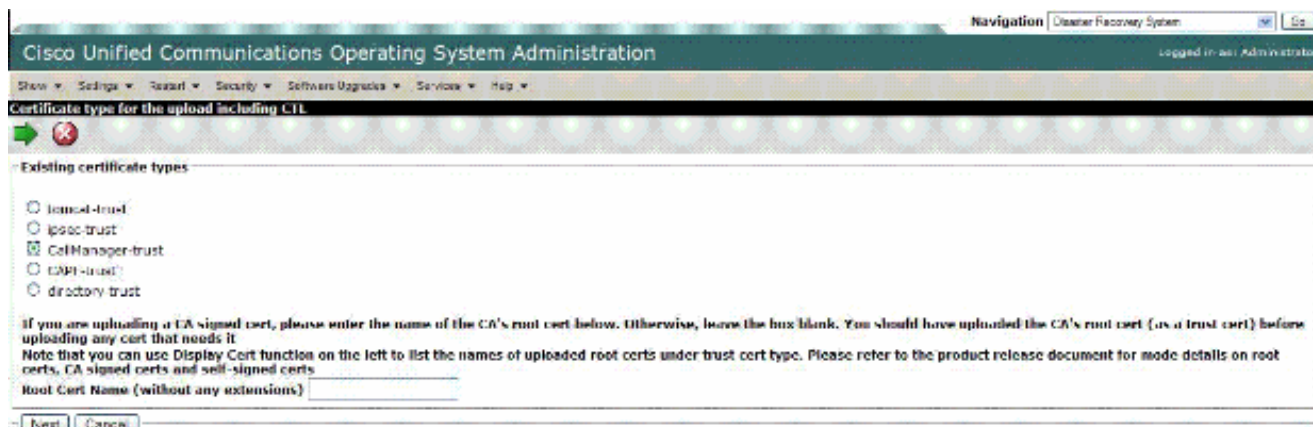
1. El registro en la página de administración unificada Cisco OS en el Cisco CallManager en el **IP Address >/platform\_gui/del <ccm de https://**, y elige el Certificate Management (Administración de certificados) > la carga Certificate/CTL de la Seguridad.



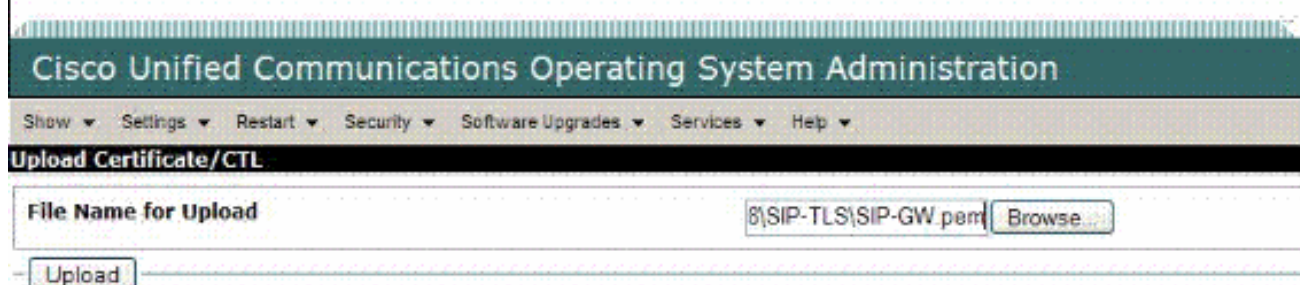
2. CERT de la confianza de la carga del teclado.



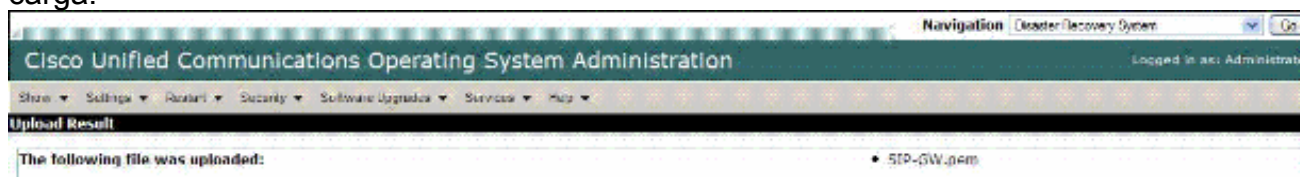
3. CallManager-confianza del teclado.



- Ingrese u hojee a la ubicación del certificado del Cisco IOS, del archivo the.pem, y de la carga del teclado.



- Verifique el resultado de la carga.



## [SORBA la configuración del tronco en el Cisco CallManager](#)

Complete estos pasos:

- El registro en Cisco unificó la página de administración OS en el CallManager en el `>/ccmadmin/del IP Address del <ccm de https://`. Configure un perfil de seguridad del trunk del SORBO: Elija el **perfil de seguridad del perfil del > Security (Seguridad) del sistema > del trunk del SORBO**. Haga clic el nuevo botón del agregar con los parámetros mostrados en esta figura:



Navigation Cisco Unified CallManager Administration [Go](#)

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions Logged in as: CCMAAdministrator

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

SIP Trunk Security Profile Configuration [Related Links](#) [Back To Find/List](#) [Go](#)

**Status**

- Update successful
- Reset of the trunk is required to have changes take effect.

**SIP Trunk Security Profile Information**

Name\* IOS-SIP-TLS

Description

Device Security Mode Encrypted

Incoming Transport Type\* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)\* 300

X.509 Subject Name SIP-GW

Incoming Port\* 5061

Enable Application Level Authorization

Accept Presence Subscription

Accept Out-of-Dialog REFER

Accept Unsolicited Notification

Accept Replaces Header

[Save](#) [Delete](#) [Copy](#) [Reset](#) [Add New](#)

\* indicates required item.

- Configure un trunk del SORBO: Elija el dispositivo > el trunk. Haga clic el nuevo botón del agregar. Seleccione el trunk del SORBO para el tipo de trunk, como se muestra:

Navigation Cisco Unified CallManager Administration [Go](#)

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions Logged in as: CCMAAdministrator

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

Trunk Configuration [Related Links](#) [Back To Find/List](#) [Go](#)

**Status**

- Update successful

**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

AAK Group <None>

Packet Capture Mode\* None

Packet Capture Duration 0

Media Termination Point Required

Retry Video Call as Audio

Transmit UTF-8 for Calling Party Name

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>

AAR 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\* G.711ulaw

Presence Group\* Standard Presence group

SIP Trunk Security Profile\* IOS-SIP-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\* RFC 2833

Save Delete Reset Add New

3. Configure a un patrón de ruta: Elija el ruteo de llamadas > la ruta/la caza > al patrón de ruta. Haga clic el nuevo botón del agregar, como se muestra:

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 Go

Status

Update successful

**Pattern Definition**

Route Pattern\* 80000000

Route Partition <None>

Description

Numbering Plan - Not Selected -

Route Filter <None>

MLPP Precedence\* Default

Gateway/Route List\* IOS-SIP-TLS-Trunk [Edit] [Find]

Route Option

Route this pattern

Block this pattern No Error

Call Classification\* ORNatl

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

Require Forced 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

## Verificación

Utilice esta sección para confirmar que su configuración trabaja correctamente en el gateway del SORBO del Cisco IOS.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice el OIT para ver una análisis de la salida del comando show.

- **Muestre a certificado crypto del pki CCM-SIP-1 prolijo**

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

- **Muestre a certificado crypto del pki el CCM-CERT prolijo**

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

• **Muestre el detalle de los tls tcp de la conexión sorbo-UA**

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

### • Muestre la descripción de la voz activa de la llamada

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 dBm

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
```

## Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

### Comandos de Debug

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice el OIT para ver una análisis de la salida del comando show.

Configure el Cisco IOS Gateway para registrar los debugs en su memoria intermedia de registro y para inhabilitar la **consola de registro**.

**Note:** Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un **comando debug**.

Éstos son los comandos usados para configurar el gateway para salvar los debugs en memoria intermedia de registro:

- **service timestamps debug datetime msec**
- **mantenga la secuencia**
- **ninguna consola de registro**
- **el registro mitigó el debug 5000000**
- **borre el registro**

Éstos son los comandos usados para hacer el debug de la configuración en este documento:

- **debug isdn q931**
- **debug voip ccapi inout**
- **ccsip todo del debug**
- **errores del openssl SSL del debug**
- **msg del openssl SSL del debug**
- **estados del openssl SSL del debug**

## Información Relacionada

- [Soporte de tecnología de voz](#)
- [Soporte de Productos de Voice and Unified Communications](#)
- [Troubleshooting de Cisco IP Telephony](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)