

Пример настройки SIP-TLS между шлюзом SIP IOS и CallManager

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Загрузите подписанный сертификат Cisco CallManager](#)

[Конфигурация шлюза SIP Cisco IOS](#)

[Сертификат шлюза SIP Cisco IOS загрузки к Cisco Unified CallManager](#)

[Конфигурация магистрали SIP в Cisco CallManager](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды "debug"](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет пример конфигурации для шифрования сигнализации SIP (SIP по Transport Layer Security) между Cisco IOS[®] Gateway и Cisco Unified CallManager.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Шлюз Cisco IOS: Cisco 2821, программное обеспечение Cisco IOS Release 12.4 (15) T1 с Усовершенствованным Набором функций Корпоративного обслуживания
- Cisco CallManager 5.1.2

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

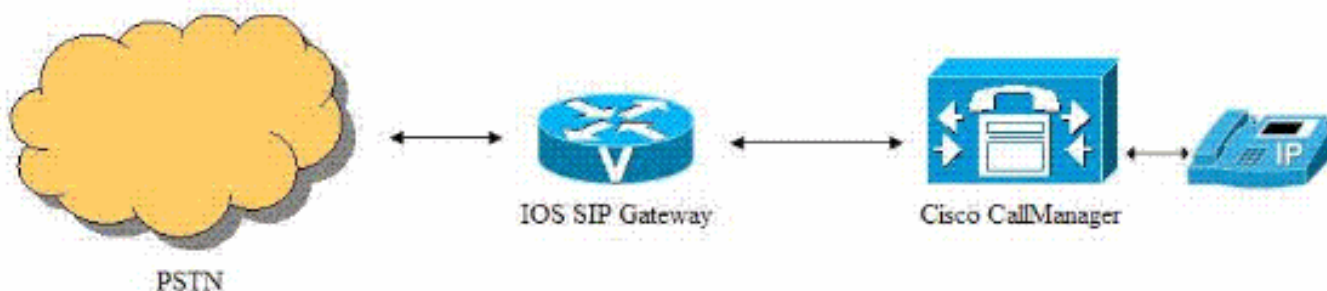
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Эти конфигурации используются в данном документе:

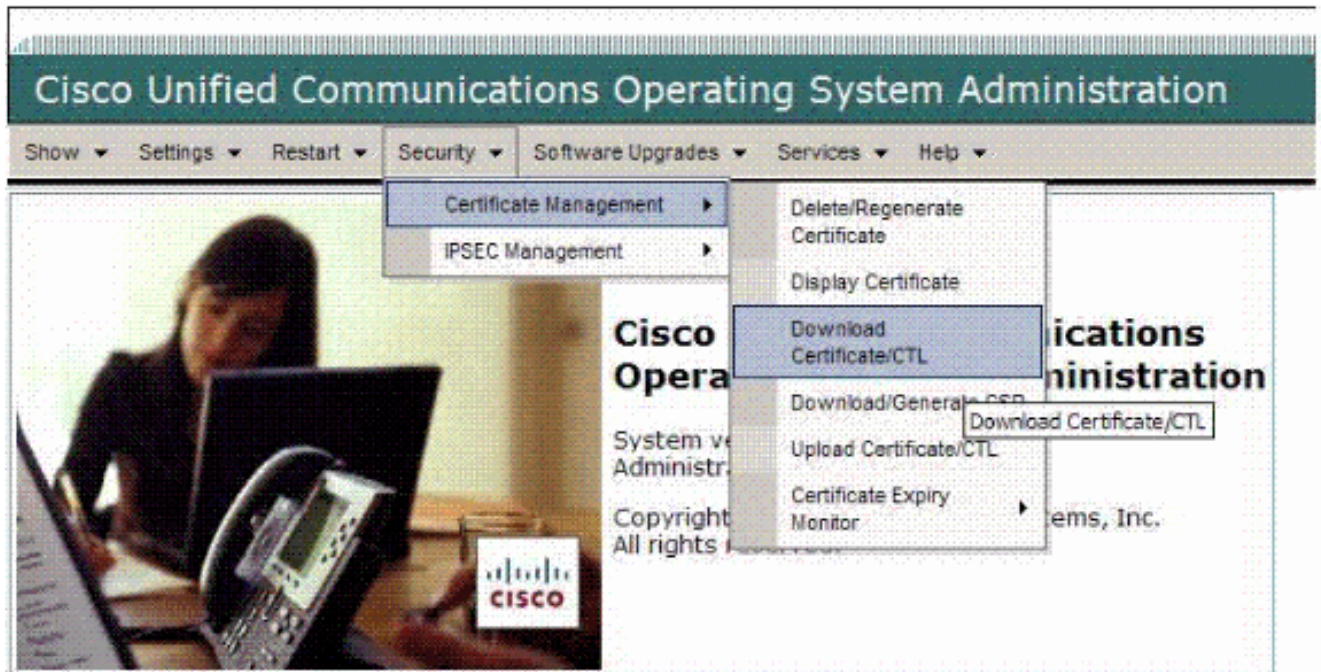
- [Загрузите подписанный сертификат Cisco CallManager](#)
- [Конфигурация шлюза SIP Cisco IOS](#)
- [Загрузите сертификат шлюза SIP Cisco IOS к Cisco Unified CallManager](#)
- [Конфигурация магистрали SIP в Cisco CallManager](#)

Загрузите подписанный сертификат Cisco CallManager

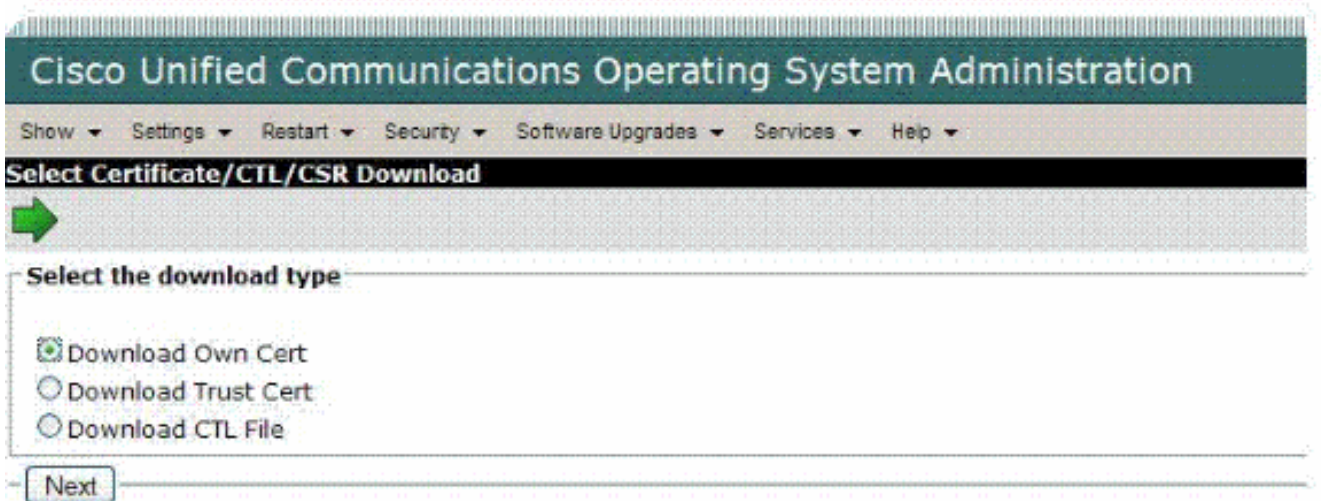
Выполните следующие действия:

1. Войдите в Cisco Унифицированная Страница администрирования операционной системы в Cisco CallManager в https://<IP-адрес ccm>/platform_gui/ и выберите **Security> Certificate Management> Download**

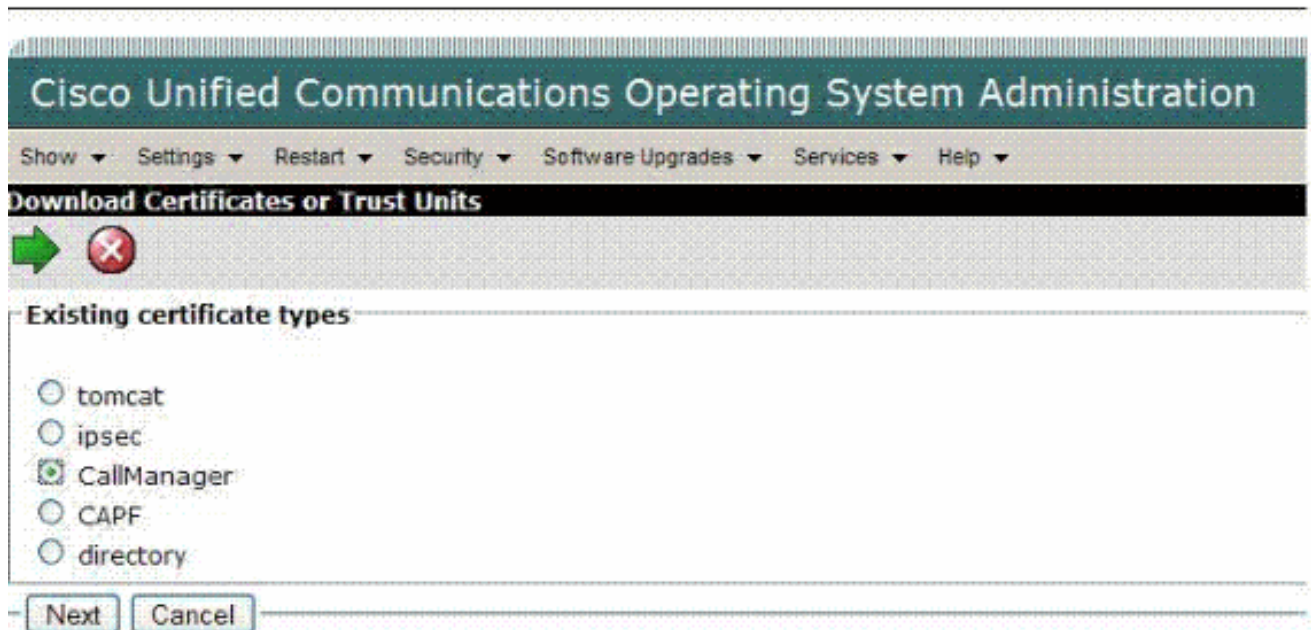
Certificate/CTL.



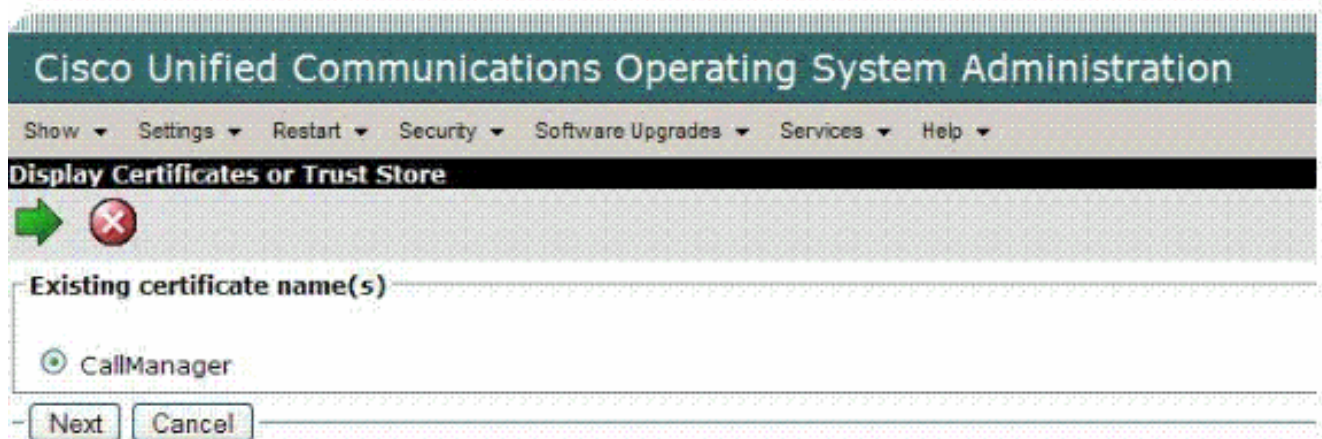
2. Нажмите **Download Own Cert.**



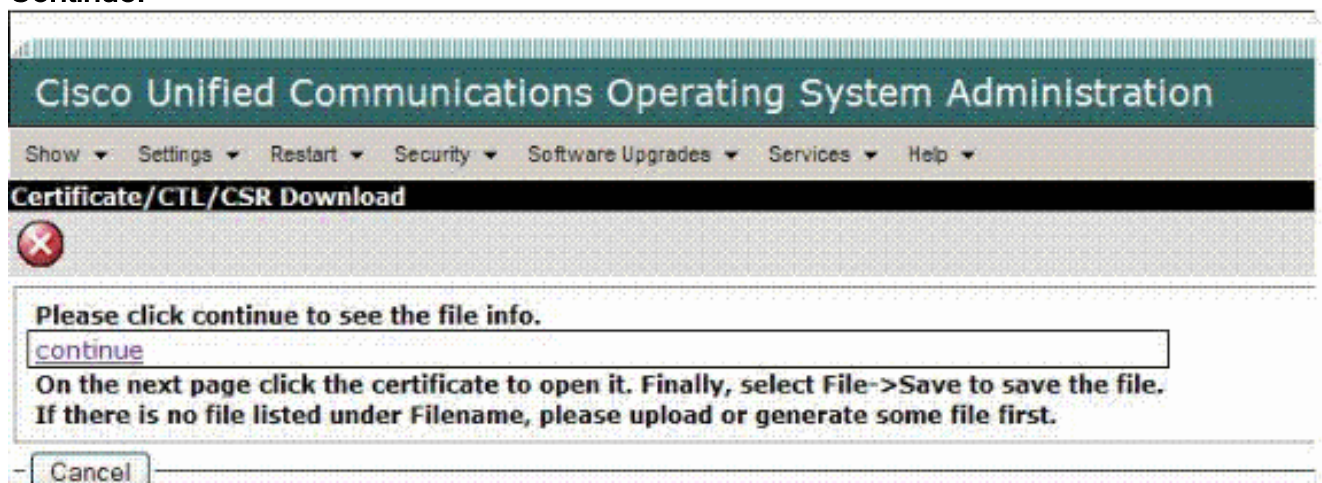
3. Нажмите **CallManager** как тип Существующего сертификата.



4. Нажмите название сертификата.



5. Нажмите кнопку Continue.



6. Щелкните правой кнопкой мыши ссылку **CallManager.pem** и выберите ссылку **Save** как, для загрузки сертификата.

Directory Listing For /downloads/certs/CallManager/ - Up To /downloads/certs

| Filename | Size |
|---------------------------------|--------|
| CallManager.pem | 0.7 kb |

Apache Tomcat/5.0

[Конфигурация шлюза SIP Cisco IOS](#)

Конфигурация шлюза SIP 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  
AxMMULRQTVMtQ0NNLTUxMB4XDTA3MDcyMzIzMjI0OVoXDTEyMDcyMzIz  
MjI0OVow  
FzEVMBMGA1UEAxMMULRQTVMtQ0NNLTUxMIGfMA0GCSqGSIb3DQEBAQUA  
A4GNADCB  
iQKBgQD6HIRcgDXQmO/EWosnaMBaoqjzARIR0erx31uR9W0iaZqsgRY+  
Am5/E3FG  
nlnJ/4NVmA45z1Q54vK0WULXgMBGANGHnBZFCNiJOiNeBfiEh1LGGMre  
VTLFqKB/  
lNAMtTppc0AVyYfjAAcJtZfUGxolZCanY5TWfmlwGBMIDhnqQQIDAQAB  
o3cWdTAL  
BgNVHQ8EBAMCARwwJwYDVR0lBCAwHgYIKwYBBQUHAWEGCCsGAQUFBwMC  
BggrBgEF  
BQCDBTAeBgNVHREEFzAVhhNzaXA6Q049U1RQTVMtQ0NNLTUxMB0GA1Ud  
DgQWBBQr  
pCxbwczRZ09Ak07V0HgHihikPzZANBgkqhkiG9w0BAQUFAAOBgQAvNQqa  
VKKoZxUD  
HCBIA292qZSsOht859FY3UJkWfGD+kjlgHjgjlxEQcaJOa7pDlorzH+H  
QIjFpcv6  
1cl0tOdOrs2L6IAGd9e5DQ3qDwWxaB7TIsBPTkv9FLVURnKtJtVHbqjM  
d+AAtsDl /DV5TbDUDre6Orglmm4uaMdrYzt1kQ== -----END  
CERTIFICATE----- Certificate has the following  
attributes: Fingerprint MD5: 1EF154E3 70E40379 1C7003B9  
B29E111B Fingerprint SHA1: CAFAF83 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
```

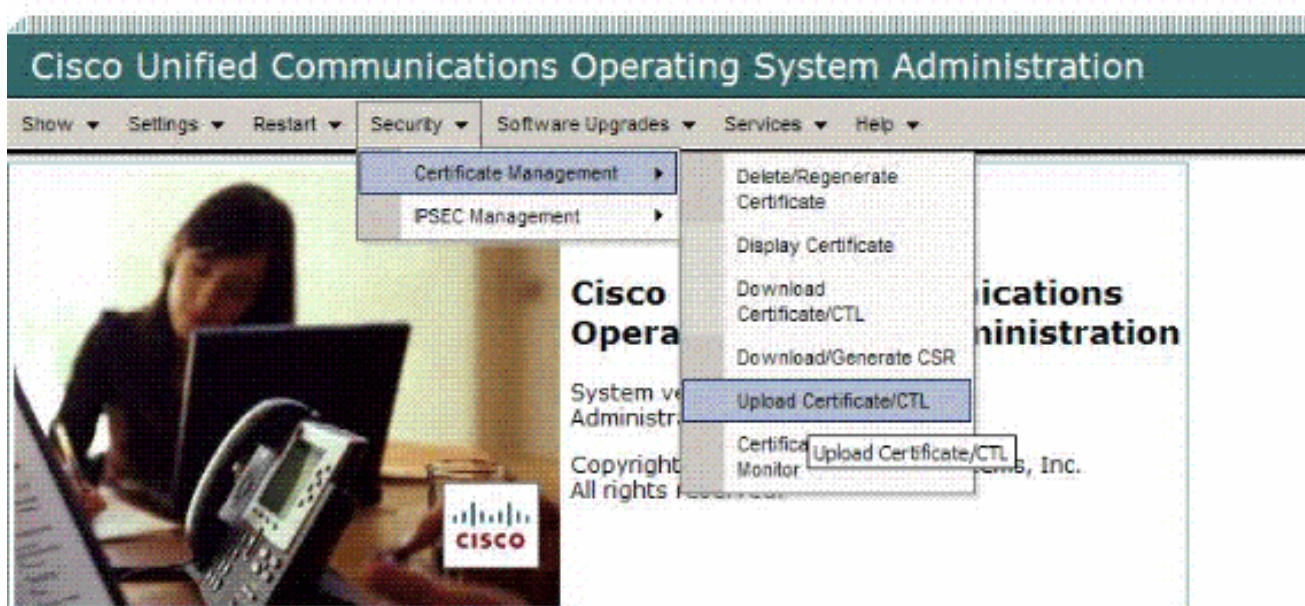
```

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

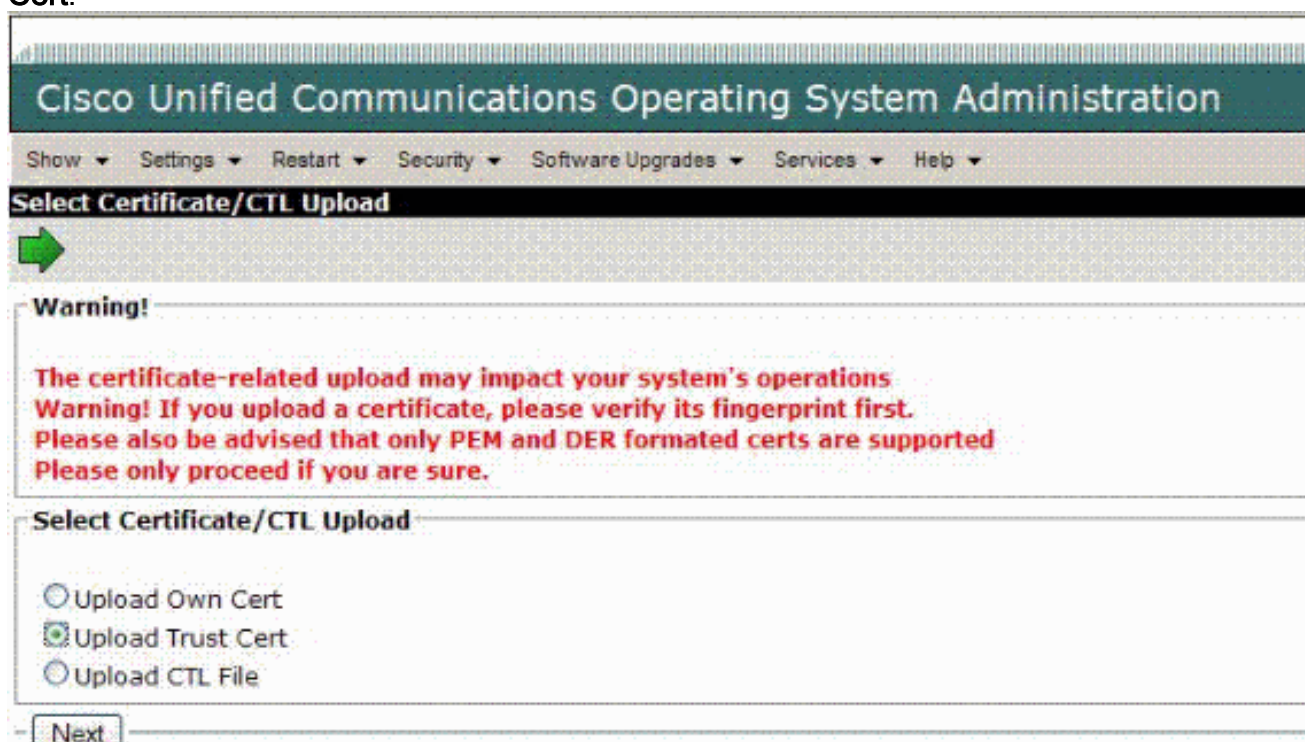
```

Выполните следующие действия:

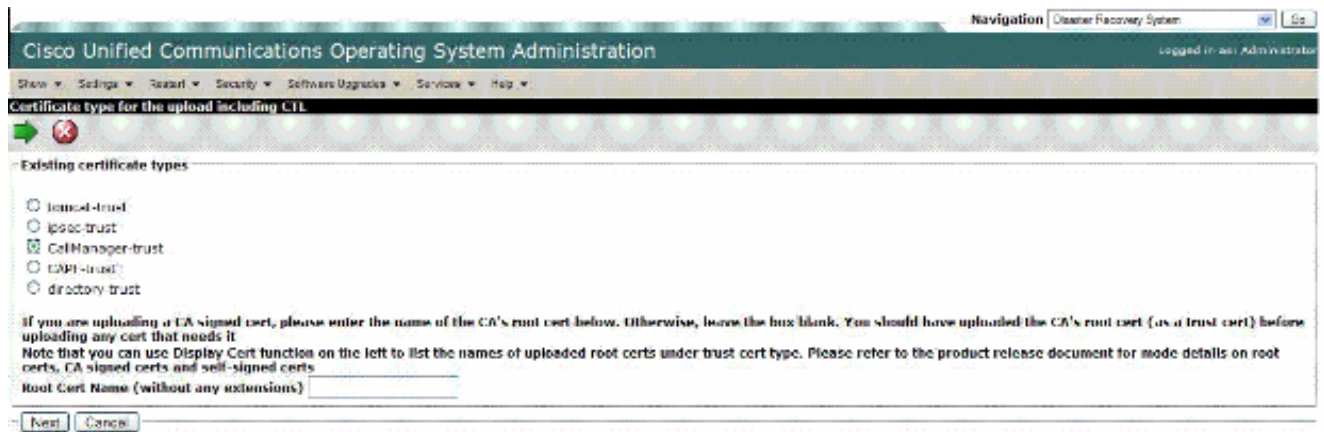
1. Войдите в Cisco Унифицированная Страница администрирования операционной системы в Cisco CallManager в https://<IP-адрес ccm>/platform_gui/ и выберите **Security> Certificate Management> Upload Certificate/CTL**.



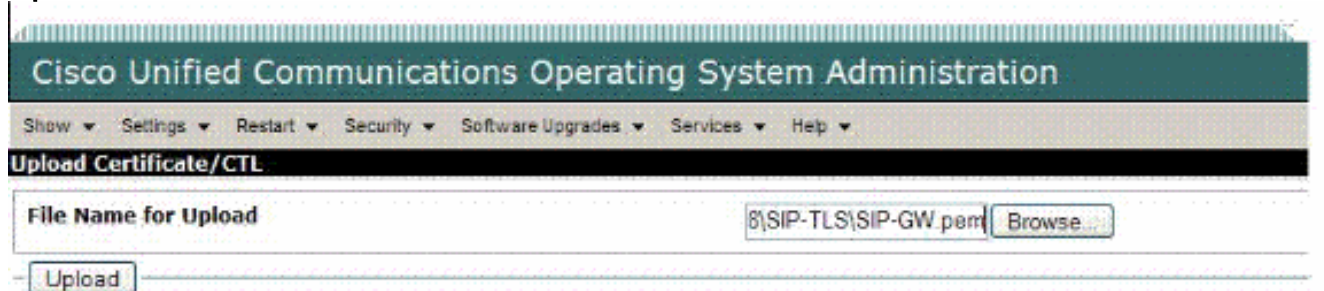
2. Нажмите **Upload Trust Cert**.



3. Нажмите **CallManager-trust**.



4. Войдите или перейдите к местоположению Сертификата Cisco IOS, the.pem файл, и нажмите **Upload**.



5. Проверьте результат загрузки.



[Конфигурация магистрали SIP в Cisco CallManager](#)

Выполните следующие действия:

1. Войдите в Cisco Унифицированная Страница администрирования операционной системы в CallManager в <https://</>/ccmadmin/IP-адреса ccm>. Настройте Профиль безопасности магистрального SIP-канала: Выберите > **Security System Профиль**> **Профиль безопасности магистрального SIP-канала**. Нажмите кнопку Add New с параметрами, показанными на этом рисунке:

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)* 600

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.

2. Настройте магистраль SIP: Выберите **Device** > **Trunk**. Нажмите кнопку **Add New**. Выберите **SIP Trunk for Trunk** Type, как показано:

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. Настройка шаблона маршрута: Выберите маршрутизацию Call > Маршрут/Поиск > Шаблон маршрута. Нажмите кнопку Add New, как показано:

System > Call Routing > Media Resources > Voice Mail > Devices > 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* ORNst

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

Проверка

Используйте этот раздел, чтобы подтвердить, что ваша конфигурация работает должным образом над шлюзом SIP Cisco IOS.

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Используйте OIT для просмотра анализа выходных данных команды show.

- **Покажите крипто-сертификату rki многословный 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

- **Покажите крипто-сертификату rki многословное Свидетельство CCM** 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

• **Покажите подробность tls tcp соединения sip-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

• **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 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

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Команды "debug"

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Используйте OIT для просмотра анализа выходных данных команды show.

Настройте шлюз Cisco IOS, чтобы регистрировать отладки в его буфере журнала и отключить консоль регистрации.

Примечание: Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки".

Это команды, используемые для настройки шлюза для хранения отладок в буфере журнала:

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

Это команды, используемые для отладки конфигурации в этом документе:

- **debug isdn q931**
- **debug voip sccapi inout**
- **debug ccsip all**
- **ошибки debug ssl openssl**
- **сообщение debug ssl openssl**
- **состояния debug ssl openssl**

Дополнительные сведения

- [Поддержка голосовых технологий](#)
- [Поддержка продуктов Голосовой и Унифицированной связи](#)
- [Устранение неполадок в системах IP-телефонии Cisco](#)
- [Cisco Systems – техническая поддержка и документация](#)