Configure Secure SIP SRST on ISR4000

Contents

Introduction

This document describes how to Configure Secure Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) on ISR4000 Series Router and Cisco Unified Communications Manager (CUCM).

Contributed by Ankush Vijay, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

Cisco Unified Communications Manager (CUCM)

Cisco Unified Survivable Remote Site Telephony (SRST)

Transport Layer Security (TLS)

Secure Real-Time Transport Protocol (SRTP)

Real-Time Transport Protocol (RTP)

Session Initiation Protocol (SIP)

User Datagram Protocol (UDP)

Components Used

CUCM: 10.5.2

SIP SRST version - Minimum 12.1 as per SRST Admin Guide

SRST Router: ISR 4451

CA Server: Tested on ISR 2921 and third party CA server.

Phones Tested: 78XX and 88XX

Platform Capacity and firmware requirements as per SRST Compatibility Matrix.

ISRG2 used as an IOS CA server (Same SRST gateway can also be used as an IOS CA server)

> **Caution**: 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, ensure that you understand the potential impact of any command.

Overview on Secure SRST

Cisco Unified Secure SRST provides security features such as authentication, integrity, and media encryption.

Authentication provides assurance to one party that another party is whom it claims to be.

Integrity provides assurance that the given data has not been altered between the entities.

Encryption implies confidentiality; that is, that no one can read the data except the intended recipient. These security features allow privacy for Cisco Unified SRST voice calls and protect against voice security violations and identity theft.

SRST security is achieved when:

- End devices are authenticated through certificates.
- Signaling is authenticated and encrypted through Transport Layer Security (TLS) for TCP.
- A secure media path is encrypted through Secure Real-Time Transport Protocol (SRTP).
- Certificates are generated and distributed by a Certificate Authority(CA)

Background Information

Before this configuration, the CUCM must be tuned into Mix mode with security enable.

Phones must be registered as secure phones.

For Information on how to register phones with CUCM in secure mode, check [IP Phone Security and CTL]

For Secure SIP SRST to be supported on Cisco 4000 Series Integrated Services Routers, enable these technology package licenses on the router:

security **uck9**

Configuration Steps and Example

Step 1. Enable Http on SRST and CA server

ip http server

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#ip http server
Router1(config)#
```

Step 2. Install Certificate from IOS based CA server or Third party CA Server

A) IOS Based CA Server;

- Create Cisco IOS certificate server:

```
1.    crypto pki serverCA-Name
2.    database level{minimal| names | complete}

minimal: Enough information is stored only to continue to issue new certificates without
conflict; this is the default.
names: In addition to the information given in the minimal level, the serial number and subject
name of each certificate are stored.
complete: In addition to the information given in the minimal and names levels, each issued
certificate is written to the database.

3.    database urlroot-url
The default location for the database entries to be written is flash; however, NVRAM is
recommended for this task.
4.    issuer-nameDN-string
      Eg: issuer-name CN= CA-Name
5.    grant auto
6.    no shutdown
```

```
router(config)#crypto pki server srstcaserver
router(cs-server)#databa
router(cs-server)#database level complete
router(cs-server)#database url nvram
% Server database url was changed. You need to move the
% existing database to the new location.
router(cs-server)#issuer-name CN=srstcaserver
router(cs-server)#grant auto
router(cs-server)#no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

% Certificate Server enabled.
router(cs-server)#
```

- Autoenroll and Authenticate the SRST Router to the CA Server:

1. **crypto pki trustpoint** SRST-Trustpoint-Name
2. **enrollment url** url

If the CA is on your router itself url would be http://router-ip-address

3. **revocation-check** none
4. **rsakeypair keypair**-label
5. exit
6. **crypto pki authenticate** SRST-Trustpoint-Name

```
Certificate has the following attributes:
Fingerprint MD5: 4C894B7D 71DBA53F 50C65FD7 75DDBFCA
Fingerprint SHA1: 5C3B6B9E EFA40927 9DF6A826 58DA618A BF39F291
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

```
Router1(config)#crypto pki trustpoint srstca
Router1(ca-trustpoint)#rsakeypair srstcakey 2048
Router1(ca-trustpoint)#enrollment url http://
Router1(ca-trustpoint)#revo
Router1(ca-trustpoint)#revocation-check none
Router1(ca-trustpoint)#exit
Router1(config)#cryp
Router1(config)#crypto pki auth
Router1(config)#crypto pki authenticate srstca
Certificate has the following attributes:
       Fingerprint MD5: AA086E13 EE0E5F61 2A585804 2DA3FB28
      Fingerprint SHA1: DD59741A DB10F1E3 566F6F9E C0AC97C2 9B7116D0

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

7. **crypto pki enroll** *SRST-Trustpoint-Name*

```
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
```

```
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be: router.cisco.com
% The subject name in the certificate will be: router.cisco.com
% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: D0B9E79C
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.


Sep XX 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint MD5: D154FB75
2524A24D 3D1F5C2B 46A7B9E4
Sep XX 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 0573FBB2
98CD1AD0 F37D591A C595252D A17523C1
Sep XX 00:41:57.339: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

```
Router1(config)#crypto pki enroll srstca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: Router1
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: FLM2008W049
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose srstca' commandwill show the fingerprint.
```

B) Third Party CA server

Summary Steps:

1. **crypto key generate rsa general-keys label** *SRST-Trustpoint-Name* modulus 2048

2. Router(config)#**crypto pki trustpoint** srstca

   Router(ca-trustpoint)#**enrollment terminal pem**

   Router(ca-trustpoint)#**subject-name** CN=srstca

   Router(ca-trustpoint)#revocation-check none

   Router(ca-trustpoint)#**rsakeypair** cube

```
Router1#
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#crypto key generate rsa gene
Router1(config)#crypto key generate rsa general-keys label srstca mod
Router1(config)#crypto key generate rsa general-keys label srstca modulus 2048
The name for the keys will be: srstca

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

Router1(config)#
Router1(config)#
Router1(config)#
Router1(config)#
Router1(config)#cryp
Router1(config)#crypto pki tru
Router1(config)#crypto pki trustp
Router1(config)#crypto pki trustpo?
trustpoint  trustpool

Router1(config)#crypto pki trustpoi
Router1(config)#crypto pki trustpoint srstca
Router1(ca-trustpoint)#enr
Router1(ca-trustpoint)#enrollment term
Router1(ca-trustpoint)#enrollment terminal pem
Router1(ca-trustpoint)#subje
Router1(ca-trustpoint)#subject-?
subject-alt-name  subject-name

Router1(ca-trustpoint)#subject-name CN=srstca
Router1(ca-trustpoint)#revo
Router1(ca-trustpoint)#revocation-check non
Router1(ca-trustpoint)#revocation-check none
Router1(ca-trustpoint)#rsa
Router1(ca-trustpoint)#rsakeypair ?
  WORD  RSA keypair label

Router1(ca-trustpoint)#rsakeypair srstca
Router1(ca-trustpoint)#
Router1(ca-trustpoint)#
Router1(ca-trustpoint)#
```

3. **Crypto pki enroll** srstca

```
Router1(config)#crypto pki enroll srstca
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=srstca
% The subject name in the certificate will include: Router1
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICjzCCAXcCAQAwKTEPMA0GA1UEAxMGc3JzdGNhMRYwFAYJKoZIhvcNAQkCFgdS
b3V0ZXIxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2rjyhAoTJq2e
//G6iM35Uu5laZPCDV6cFmBWxtOL0Qa2GQKe9odovPBLvV9zSzyw8bxSGkBYS1Qu
n9jgSV2f3IAV79S+oTXf/TEhYlsqWbmf6hm60jdZXjXF0w+4WUidg1wSfAuaI+FY
8Y6jPRUAqYTZeJTnnrp6q/8MfxLhIvyFBX3tzIgxo570sxFtY17rMQsdKfggvRUQ
Up4CFYm7LzFSn4uUM8/NOKcgJzJkihWY3VMsIXOg37d0M0tmAWdrIkIuAftF7pga
3sU5qJuD354Bm8tzkpBOUrf0YshDW93LWP6JZpov9WDfL5qa16pw1WZ3nAiGGINA
2kwitkibjwIDAQABoCEwHwYJKoZIhvcNAQkOMRIwEDAOBgNVHQ8BAf8EBAMCBaAw
DQYJKoZIhvcNAQEFBQADggEBAJDJzAgXRvA5DCxrXe//M7Cwp456pzgSOESLtVeu
OgZhxzis6APYwYsQg6wxzAS821OkyFO0zCIQo2yBWeN7HMhO/UUqvbAF1//PXFkm
vdXRAM1KstDwDMb6EQpArvF23DNWXuVyFPid0uMS/d8xW2OB6+r+B4VGzy1gpZgZ
FHf+gyaemBvwWIWTjX2ZaA+pCeu2Tip3nuvrMnM7jlqFPBtTcTSEw4R8b1WgHZ3W
KSOUvmPS1HJ2Zc0ets2ruInvt5Pz1bOLcBnCY8JkqXcqAhOv282DkPy7G+X8Y59m
opKnAh0gx5L1ANcEQd4a8o09jqqQjj5gz8KMs8MTvT3wrZ8=
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
Router1(config)#
Router1(config)#
Router1(config)#
```

Provide the certificate to Third party CA.

4. CA provides the Signed Certificate as well as the Root CA Certificate and any Intermediate (subordinate) CA certificates if any.

5. Install Root CA cert;

crypto pki authenticate srstca

```
Router1(config)#crypto pki authenticate srstca

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDfTCCAmWgAwIBAgIQT7YJxPVkzYNIGhhGW4aFATANBgkqhkiG9w0BAQsFADBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRowGAYKCZImiZPyLGQBGRYKcmNkbmNvbGxh
YjEeMBwGA1UEAxMVcmNkbmNvbGxhYi1XSU4yMDEyLUNBMB4XDTE4MDYxNDE2MTk1
N1oXDTIzMDYxNDE2Mjk1N1owUTETMBEGCgmSJomT8ixkARkWA2NvbTEaMBgGCgmS
JomT8ixkARkWCnJjZG5jb2xsYWIxHjAcBgNVBAMTFXJjZG5jb2xsYWItV01OMjAx
Mi1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALe03mprczCRg8AY
4cBAgezyjF386xHjwu5K0kNA3zl7xWYmX3s/6vZoDkUFvy50GjwPHzyLxJAvmJ6P
3eaTsSx80JO9PY8NBi4LH0WaWo1zFVjlJO1Fwz1B9LxwBt/KwWnkARrGdBEM5xaT
tMnFK3K6UuWMMWnX1ELvUOKIA7eXFsorSvVrx+KcJLuYowgODPINC7VjBoGBSwun
hnLEIQ3XXIIYbceBEHj0tlo+zoQp9UkLjcp4WgGCr4/rg9h/B/6ppZoMqoyDmBaz
7kNV4C6Nbz9K+XAaRc4MEy0wNjqxIskj3OF0/IK53n1jzGg8JTGw+oqLCUoLYfD0
MKAeM+MCAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYD
VR0OBBYEFCWR/A/DRJ31hAGRFwcgnWrEeAEGMBAGCSsGAQQBgjcVAQQDAgEAMA0G
CSqGSIb3DQEBCwUAA4IBAQCPKhkjEyfKvNK8S2W7SCQao6LWHm6g6ln5CS1zixnv
kG+nY8mhIIhueW7GJ0+n28ufLEA6D6PMqeaL1TzJRwOK4EMq2060Jd6pA34Y6J8s
+teZWPINNvVbyX/eSAVzWeesjjNeI2feQWEhSEyhmyRe5cl7/09k6kyM8bGj86vj
wZ4AFaw+IU/zQ80A+TgBBiPlyz/f90RipPEp+tzfZR2D3xCPrK4jRL7uvDtArdMr
dPH3cVf78iosIFUffDRcubXktfOLFfmqyI+0splwCfEW113IWWuTdbP+UA8FyYJo
DIlRvfK1eVToIROnWJ16U57YB3Ig4/A0TmtTygjLVAjj
quit
Certificate has the following attributes:
       Fingerprint MD5: 4A2FD70E FBC823DA B5AE978B 1B02DEC8
      Fingerprint SHA1: 1F428EAD 360A1944 08F1AB77 CCDF80B5 5F4F8055

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

6. Install Signed cert from CA;

   crypto pki import srstca certificate

```
Router1(config)#crypto pki import srstca certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIFIzCCBAugAwIBAgITeAAAAAabDPlyI/7cowAAAAAABjANBgkqhkiG9w0BAQsF
ADBRMRMwEQYKCZImiZPyLGQBGRYDY29tMRowGAYKCZImiZPyLGQBGRYKcmNkbmNv
bGxhYjEeMBwGA1UEAxMVcmNkbmNvbGxhYi1XSU4yMDEyLUNBMB4XDTE4MTAwNTE4
MzMwNVoXDTIwMTAwNDE4MzMwNVowETEPMA0GA1UEAxMGc3JzdGNhMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2rjyhAoTJq2e//G6iM35Uu5laZPCDV6c
FmBWxtOL0Qa2GQKe9odovPBLvV9zSzyw8bxSGkBYS1Qun9jgSV2f3IAV79S+oTXf
/TEhYlsqWbmf6hm60jdZXjXF0w+4WUidg1wSfAuaI+FY8Y6jPRUAqYTZeJTnnrp6
q/8MfxLhIvyFBX3tzIgxo570sxFtY17rMQsdKfggvRUQUp4CFYm7LzFSn4uUM8/N
OKcgJzJkihWY3VMsIXOg37d0M0tmAWdrIkIuAftF7pga3sU5qJuD354Bm8tzkpBO
Urf0YshDW93LWP6JZpov9WDfL5qa16pw1WZ3nAiGGINA2kwitkibjwIDAQABo4IC
MjCCAi4wDgYDVR0PAQH/BAQDAgWgMB0GA1UdDgQWBBSK4+gNzQY5gac/9LftIdsd
8z/33zAfBgNVHSMEGDAWgBQlkfwPw0Sd9YQBkRcHIJ1qxHgBBjCB1gYDVR0fBIHO
MIHLMIHIoIHFoIHChoG/bGRhcDovLy9DTj1yY2RuY29sbGFiLVdJTjIwMTItQ0Es
Q049d2luMjAxMixDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1yY2RuY29sbGFiLERDPWNvbT9j
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz
dHJpYnV0aW9uUG9pbnQwgcoGCCsGAQUFBwEBBIG9MIG6MIG3BggrBgEFBQcwAoaB
qmxkYXA6Ly8vQ049cmNkbmNvbGxhYi1XSU4yMDEyLUNBLENOPUFJQSxDTj1QdWJs
aWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9u
LERDPXJjZG5jb2xsYWIsREM9Y29tP2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RD
bGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBl
AGIAUwBlAHIAdgBlAHIwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEL
BQADggEBAC+YzH4UyqXF3dZp5wP3PHvTa64Bhynp8x6EmwGVEcw55EOKZI8x+bR2
cfbailJbs+LVXxjbTHfywtF2a9mg79QF4QEIQbbWoN75doYhYXa4CJfJf2nQahgc
F8cRBejSSs4n+WwGqagWmCe6qq34ZStEVTD62YAogujT3gErSS1rj6hKx8UlC6XV
4yDKSRmRJvIqK4Lkf9R/A6Bb95zHz5euYIiewUpKzHU3nILE7x+vXlCd/rSWesnG
JsUtctJx1a89Wg7OH4fOLZgEfFul3x3nGbL0//lGkOiTUSQcYVaNhgIw+36HVDGY
PW12TrRRnZpAYpplhTmu/4Cp2JOuu4s=
quit
% Router Certificate successfully imported
```

Step 3. Enable Credentials Service on the SRST Router:

SUMMARY STEPS:

1. **credentials**
2. **ip source-address** srst-router-ip port 2445
3. **trustpoint** SRST-trustpoint-name

```
credentials
 ip source-address [illegible] port 2445
 trustpoint srstca
```

Step 4. Import Phone Certificate Files in Privacy Enhanced Mail(PEM) Format to the Secure SRST Router:

On CUCM , navigate to **Cisco unified OS administration >Security > Certificate management**

Download all certificates listed under CAPF-trust, include Cisco_Manufacturing_CA, Cisco_Root_CA_2048, CAP-RTP-001, CAP-RTP-002, CAPF, and CAPF- xxx . Also download any CAPF- xxx certificates that are listed under CallManager-trust and not under CAPF-trust.

CallManager-trust	CAPF-2fbd03a4
CallManager-trust	CAPF-dc3cda68
CallManager-trust	Cisco_Manufacturing_CA
CallManager-trust	CAPF-19a340e5
CallManager-trust	CAP-RTP-002
CallManager-trust	CAPF-851d4452
CallManager-trust	Cisco_Manufacturing_CA_SHA2
CallManager-trust	CAP-RTP-001
CallManager-trust	cm10
CallManager-trust	ACT2_SUDI_CA
CAPF	CAPF-72c7ffbb
CAPF-trust	Cisco_Root_CA_2048
CAPF-trust	CAPF-72c7ffbb
CAPF-trust	Cisco_Root_CA_M2
CAPF-trust	CAPF-2fbd03a4
CAPF-trust	Cisco_Manufacturing_CA
CAPF-trust	CAP-RTP-002
CAPF-trust	CAPF-851d4452
CAPF-trust	Cisco_Manufacturing_CA_SHA2
CAPF-trust	CAP-RTP-001
CAPF-trust	ACT2_SUDI_CA
ipsec	cm10.vipul.com
ipsec-trust	cm10.vipul.com
ITLRecovery	ITLRECOVERY_cm10

Confiure trustpoints for each of them on your SRST router. Ensure to give the trustpoint name same as the .pem.

SUMMARY STEPS:

1. **crypto pki** trustpointname
2. **revocation-check none**
3. **enrollment terminal**
4. **exit**
5. **crypto pki authenticate** name

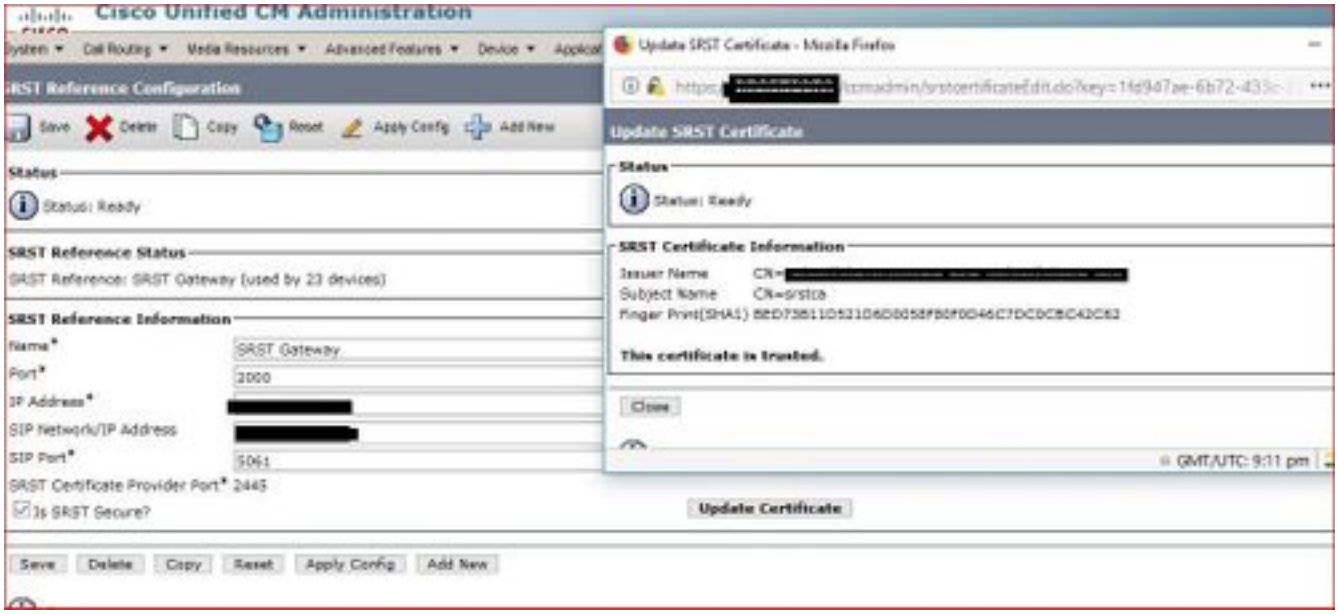
Here copy all of the contents that appear between -----*BEGIN CERTIFICATE*-----and -----*END CERTIFICATE*----- of the corresponding .pem file with a blank line at the end or the word ***quit*** and paste it on the terminal , press enter.

```
Router1(config)#crypto pki tru
Router1(config)#crypto pki trustpoi
Router1(config)#crypto pki trustpoint Cisco_Manufacturing_CA
Router1(ca-trustpoint)#revocat
Router1(ca-trustpoint)#revocation-check none
Router1(ca-trustpoint)#enroll
Router1(ca-trustpoint)#enrollment termi
Router1(ca-trustpoint)#enrollment terminal
Router1(ca-trustpoint)#exit
Router1(config)#crypto pki auth
Router1(config)#crypto pki authenticate Cisco_Manufacturing_CA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIE2TCCA8GgAwIBAgIKamlnswAAAAAAAzANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMDUwNjEwMjIxNjAxWhcNMjkwNTE0MjAyNTQyWjA5MRYwFAYDVQQKEw1DaXNj
byBTeXN0ZW1zMR8wHQYDVQQDExZDaXNjbyBNYW51ZmFjdHVyaW5nIENBMIIBIDAN
BgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEAoMX33JaUNRXx9J1Ou5tB4X3beRaR
u/NU8kFK1DJiYskj95rnu5t56AcpTjD1rhvFIVZGsPj05o6BuBbMqJuF0kKB23zL
1KkRYRIcXOozIByaFqd925kGauI2r+z4Cv+YZwf0MO61+IgaqujHPBzO7kj9zVw3
8YaTnj1xdX007ksUqcApewUQ74eeaTEw9Ug2P9irzhXi6FifPmJxBIcmpBViASWq
1d/JyVu4yaEHe75okpOTIKhsvRV100RdRUvsqNpgx9jI1cjtQeH1X1eOUzKTSdXZ
D/g2qgfEMkHFp68dGf/2c5k5WnNnYhM0DR9elXBSZBcG7FNcXNtq6jUAQQIBA6OC
AecwggHjMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFNDFIiarT0Zg7K4F
kcfcWtGwR/dsMAsGA1UdDwQEAwIBhjAQBgkrBgEEAYI3FQEEAwIBADAZBgkrBgEE
AYI3FAIEDB4KAFMAdQBiAEMAQTAfBgNVHSMEGDAWgBQn88gVHm6aAgkWrSugiWBf
2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3LmNpc2NvImNvbS9zZWN1
cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEFBQcBAQREMEIwQAYIKwYB
BQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3N1Y3VyaXR5L3Bra9jZXJ0cy9j
cmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkVAQIAMEMwQQYIKwYBBQUH
AgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3N1Y3VyaXR5L3Bra9wb2xpY211cy9p
bmRleC5odG1sMF4GA1UdJQRXMFUGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUH
AwUGCCsGAQUFBwMGBggrBgEFBQcDBwYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJ
KwYBBAGCNxUGMA0GCSqGSIb3DQEBBQUAA4IBAQAw8zAtjPLKN0pkmSQpCvKGqkLV
I+ii6itvaSN6go4cTAnPpE+rhC836WVg0ZrG2PML9d7QJwBcbx2RvdFOWFEdyeP3
OOfTC9Fovo4ipUsG4eakqjN9GnW6JvNwxmEApcN5J1unGdGTjaubEBEpH6GC/f08
S2513JNFBemvM2tnIwcGhiLa69yHz1khQhrpz3B1iOAkFV19TpY4gJfVb/Cbcdi6
YBmlsGGGrd11Zva5J6LuL2GbuqEwYf2+rDUU+bgtlwavw+9tzD0865XpgdOKXrbO
+nmka9eiV2TEP0zJ2+iC7AFm1BCIolblPFft6QKoSJFjB6thJksaE5/k3Npf
quit
Certificate has the following attributes:
       Fingerprint MD5: 6EA241F5 AC9A1148 CC8B4B43 C7C13025
      Fingerprint SHA1: E3E783D3 CC9C30AE DEFFCDEB 5ECFEE08 FF0F1684
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported

Router1(config)#
```

REPEAT this for all the trustpoints

Step 5. CUCM CONFIGS:

1. Add your ***SRST reference*** under system
2. Select the check box of ***Is SRST Secure***?
3. For SIP Secure-SRST , don't forget to change the port in your SRST reference as ***5061.***
4. Create a security profile for your phone under ***System>Security>Phone security profile***. Add this security profile to your phone under ***Device security profile***.
5. Select Update Certificate to verify the srst cert got populated on CUCM;



Step 6. SRST specific configs for your SRST router

A). Configure SIP SRTP for Encrypted Phones

SUMMARY STEPS:

```
1.    crypto pki trustpointname
2.    revocation-check none
3.    enrollment terminal
4.    exit
5.    crypto pki authenticate name
```

Note: Use srtp fallback if you want non srtp calls to work.

B). Configure SIP SRST Security Policy

SUMMARY STEPS:

```
1.    crypto pki trustpointname
2.    revocation-check none
3.    enrollment terminal
4.    exit
5.    crypto pki authenticate name
```

Sample Config

```
1.    crypto pki trustpointname
2.    revocation-check none
3.    enrollment terminal
4.    exit
5.    crypto pki authenticate name
```

Verify

Use this section to confirm that your configuration works properly.

If you used the Cisco IOS certificate server as your CA, use the **show running-config** command to verify certificate enrollment or the **show crypto pki server** command to verify the status of the CA server.

Summary Steps

1. show running-config

2. show crypto pki server

```
Router# show crypto pki server
Certificate Server srstcaserver:
Status: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: CN=srstcaserver
CA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00
Granting mode is: auto
Last certificate issued serial number: 0x2
CA certificate expiration timer: 13:46:57 PST Dec 1 2021
CRL NextUpdate timer: 14:54:57 PST Jan 19 2019
Current storage dir: nvram
Database Level: Complete - all issued certs written as <serialnum>.cer
```

Use **show sip-ua status registrar** to verify registration

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **SRST Admin Guide**
- **Technical Support & Documentation - Cisco Systems**