CHAPTER 9

Configuring Secure SRST for SCCP and SIP

The Secure SRST adds security functionality to the Unified SRST.

**Note**
Unified Secure SRST 12.6 on Cisco IOS XE Gibraltar 16.11.1a Release is not a recommended release version for Unified Secure SCCP SRST call flows and call flows that include stapp configuration.

**Contents**

This chapter describes new Secure SRST security features such as authentication, integrity, and media encryption.

- Prerequisites for Configuring Secure SRST, page 239
- Restrictions for Configuring Secure SRST, page 240
- Information About Configuring Secure SRST, page 242
- How to Configure Secure Unified SRST, page 254
- Additional References, page 308
- Command Reference, page 310
- Feature Information for Secure SCCP and SIP SRST, page 311
- Where to Go Next, page 311

**Prerequisites for Configuring Secure SRST**

**General**

- Secure Cisco Unified IP phones supported in secure SCCP and SIP SRST must have the Certification Authority (CA) or third-party certificates installed, and encryption enabled. For more information on CA server authentication, see Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 257.

- The SRST router must have a certificate; a certificate can be generated by a third party or by the Cisco IOS certificate authority (CA). The Cisco IOS CA can run on the same gateway as Cisco Unified SRST. Over the TLS channel (port 2445), automated certificate exchange happens between
Restrictions for Configuring Secure SRST

the Unified SRST router and the Cisco Unified Communications Manager. However, the phone certificate exchange to Unified SRST through Unified Communications Manager has to be downloaded manually on the Unified SRST router.

- Certificate trust lists (CTLs) on Cisco Unified Communications Manager must be enabled.
- It is mandatory to configure the command `supplementary-service media-renegotiate` under `voice service voip` configuration mode to enable the supplementary features supported on Unified Secure SRST.

Public Key Infrastructure on Secure SRST

- Set the clock, either manually or by using Network Time Protocol (NTP). Setting the clock ensures synchronicity with Cisco Unified Communications Manager.
- Enable the IP HTTP server (Cisco IOS processor) with the `ip http server` command, if not already enabled. For more information on public key infrastructure (PKI) deployment, see the Cisco IOS Certificate Server feature.
- If the certificate server is part of your startup configuration, you may see the following messages during the boot procedure:

```
% Failed to find Certificate Server's trustpoint at startup
% Failed to find Certificate Server's cert.
```

These messages are informational messages and indicate a temporary inability to configure the certificate server because the startup configuration has not been fully parsed yet. The messages are useful for debugging, in case the startup configuration is corrupted.

You can verify the status of the certificate server after the boot procedure using the `show crypto pki server` command.

Supported Cisco Unified IP Phones, Platforms, and Memory Requirements

- For a list of supported Cisco Unified IP Phones, routers, network modules, and codecs for secure SRST, see the Cisco Unified Survivable Remote Site Telephony Compatibility Information feature.
- For the most up-to-date information about the maximum number of Cisco Unified IP Phones, the maximum number of directory numbers (DNs) or virtual voice ports, and memory requirements, see the Cisco Unified SRST 12.3 Supported Firmware, Platforms, Memory, and Voice Products feature.

Restrictions for Configuring Secure SRST

General

- Cryptographic software features (“k9”) are under export controls. This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and, users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at the following URL:

http://www.cisco.com/wwl/export/crypto/tool/

If you require further assistance, please contact us by sending email to export@cisco.com.
• When a Secure Real-Time Transport Protocol (SRTP) encrypted call is made between Cisco Unified IP Phone endpoints or from a Cisco Unified IP Phone to a gateway endpoint, a lock icon is displayed on the IP phones. The lock indicates security only for the IP leg of the call. Security of the PSTN leg is not implied.

**SCCP SRST**

• Secure SCCP SRST is supported only within the scope of a single router.
• Cisco 4000 Series Integrated Services Routers support Secure SCCP SRST only on Unified SRST 12.3 and later releases. For Secure SCCP support on Unified SRST 12.3 Release:
  – Secure Cisco Jabber is not supported.
  – SRTP passthrough is not supported.
  – SDP Passthrough is not supported.
  – Video Calling is not supported.
  – Transcoding is not supported.
  – Hardware Conferencing is not supported (Only Software Conferencing is supported).
  – Secure Multicast MOH is not supported (Multicast MOH stays active, but non-secure).
  – Live MOH is not supported.
  – Secure H.323 is not supported.
  – Hot Standby Routing Protocol (HSRP) is not supported.
  – T.38 Fax Relay and Modem Relay is not supported for Unified Secure SRST.
• For call support on Voice Gateway introduced as part of Unified SRST 12.3 Release:
  – Speed Dial is not supported.
  – For a pure SCCP shared line, Hold and Remote Resume is not supported from an analog phone.
  – Full Blind Transfer mode (Configured with the CLI command `transfer-system full-blind`) is not supported.
  – Consider a call between two Analog Voice Gateways (VG A and VG B) registered on Unified Secure SRST as SCCP endpoints. If a call is already put on hold from the VG B endpoint (could be an SCCP phone too), then VG A (has to be an Analog Voice Gateway) cannot put the same call on hold (double hold). For more information, see CSCvi15203.
  – For three-way software conference related behavior and limitations, see Three-way Software Conferencing for Secure SCCP, Unified SRST Release 12.3, page 244.

**SIP SRST**

• Cisco 4000 Series Integrated Services Router supports Secure SIP SRST only on Unified SRST 12.1 and later releases.
• SRTP passthrough is not supported.
• SDP Passthrough is not supported.
• Video Calling is not supported.
• Transcoding is not supported.
• Hardware Conferencing is not supported (Only BIB Conferencing is supported).
Information About Configuring Secure SRST

- Benefits of Secure SRST, page 242
- Secure SIP SRST Support on Cisco 4000 Series Integrated Services Router, page 242
- Secure SCCP SRST on Cisco 4000 Series Integrated Services Router, page 243
- Cisco IP Phones Clear-Text Fallback During Non-Secure SRST, page 246
- Signaling Security on Unified SRST - TLS, page 246
- Media Security on Unified SRST - SRTP, page 251
- Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone, page 252
- Secure SRST Authentication and Encryption, page 253

Benefits of Secure SRST

Secure Cisco Unified IP phones that are located at remote sites and that are attached to gateway routers can communicate securely with Cisco Unified Communications Manager using the WAN. But if the WAN link or Cisco Unified Communications Manager goes down, all communication through the remote phones becomes non-secure. To overcome this situation, gateway routers can now function in secure SRST mode, which activates when the WAN link or Cisco Unified Communications Manager goes down. When the WAN link or Cisco Unified Communications Manager is restored, Cisco Unified Communications Manager resumes secure call-handling capabilities.

Secure SRST provides new Cisco Unified SRST 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 using certificates.
- Signaling is authenticated and encrypted using Transport Layer Security (TLS) for TCP.
- A secure media path is encrypted using Secure Real-Time Transport Protocol (SRTP).
- Certificates are generated and distributed by a CA.

Secure SIP SRST Support on Cisco 4000 Series Integrated Services Router

For Unified SRST 12.1 and later releases, Secure SIP SRST support is introduced on the Cisco 4000 Series Integrated Services Router. As a part of the Secure SIP SRST feature on Unified SRST Release 12.1, support is provided for calls with the Transport Layer Security protocols (TLS) versions up to 1.2. Also, TLS 1.2 exclusivity is supported as part of Unified SRST Release 12.1.
The Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series is supported on the Unified Secure SIP SRST Release 12.1 configured on Cisco 4000 Series Integrated Services Routers.

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

- security
- uck9

**Note**

For Unified SRST 12.2 and previous releases, only SIP phones are supported on the Cisco 4000 Series Integrated Services Router for Secure SIP SRST. For Unified SRST 12.3 and later releases, a mixed deployment of SIP and SCCP phones are supported on the Cisco 4000 Series Integrated Services Routers.

**Secure Music On Hold for Unified Secure SRST (SIP)**

From Unified SRST Release 12.1, support is introduced for Secure Music On Hold (MOH), as part of the Secure SIP SRST solution on Cisco 4000 Series Integrated Services Router. For a Secure SIP call that is put on hold, playback of Flash-based G.729 and G.711 codec format MOH files are supported. Live MOH and transcoded MOH are not supported as part of Secure MOH feature support.

**Note**

If the CLI command `srtp pass-thru` is configured under the dial peer voice configuration mode, Secure MOH does not work.

**Secure SCCP SRST on Cisco 4000 Series Integrated Services Router**

For Unified SRST 12.3 and later releases, Secure SCCP SRST support is introduced on the Cisco 4000 Series Integrated Services Router. As a part of the Secure SCCP SRST feature on Unified SRST Release 12.3, support is provided for calls with the Transport Layer Security protocols (TLS) versions up to 1.2. Also, TLS 1.2 exclusivity is supported as part of Unified SRST Release 12.3. For more information on the TLS protocol support introduced for Secure SCCP in Unified SRST Release 12.3, see SRST Routers and the TLS Protocol, page 247.

For Secure SCCP SRST to be supported on Cisco 4000 Series Integrated Services Routers, you need to enable the following technology package licenses on the router:

- security
- uck9

The Cisco Unified IP Phone 6961 and Cisco Unified IP Phone 7962G is supported on the Unified Secure SCCP SRST Release 12.3 configured on Cisco 4000 Series Integrated Services Routers. Also, analog phones are supported for analog Voice Gateways as part of Unified Secure SCCP SRST Release 12.3. For more information on support introduced on Voice Gateways, see Secure SCCP SRST for Analog Voice Gateways, page 243.

**Secure SCCP SRST for Analog Voice Gateways**

For Unified SRST 12.3 and later releases on a Cisco 4000 Series Integrated Services Router, Secure SCCP support is introduced for the following Voice Gateways:

- Cisco VG202 Analog Voice Gateway
Information About Configuring Secure SRST

- Cisco VG202XM Analog Voice Gateway
- Cisco VG204 Analog Voice Gateway
- Cisco VG204XM Analog Voice Gateway
- Cisco VG224 Analog Voice Gateway
- Cisco VG310 Analog Voice Gateway
- Cisco VG320 Analog Voice Gateway

As a part of the Secure SCCP SRST feature on Unified SRST Release 12.3, Transport Layer Security protocols (TLS) versions up to 1.2, and TLS 1.2 exclusivity is supported for Cisco VG202XM Analog Voice Gateway, Cisco VG204XM Analog Voice Gateway, Cisco VG310 Analog Voice Gateway, and Cisco VG320 Analog Voice Gateway.

For more information on configuring the Voice Gateways, see Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

Note
Cisco VG202 Analog Voice Gateway, Cisco VG204 Analog Voice Gateway, and Cisco VG224 Analog Voice Gateway only support Transport Layer Security protocols (TLS) version 1.0.

Feature Access Support for Analog Phones on Voice Gateway

For a user in basic call mode on analog phones on a voice gateway, you need to:

- Press hookflash for the first dial tone to dial an extension number to connect to a second call.
- When the second call is established, press hookflash for feature tone and #4 to transfer the call.
- When the second call is established, press hookflash for feature tone and #3 to initiate a three-way conference.
- During a three-party conference, press hookflash to drop the last conferee in Unified Communications Manager. For Unified Secure SRST, press hookflash to get feature tone and dial #2 to drop the last active party in the conference.
- When the second call is established, press hookflash for feature tone and #5 to toggle back to the previous call party.

Secure Music On Hold for Secure Unified SRST (SCCP)

From Unified SRST Release 12.3, support is introduced for Secure Music On Hold (MOH), as part of the Secure SCCP SRST functionality on Cisco 4000 Series Integrated Services Router. For a Secure SCCP call that is put on hold, playback of Flash-based G.729 and G.711 codec format MOH files are supported. Live MOH and transcoded MOH are not supported as part of Secure MOH feature support. Also, Multicast MOH is supported as non-secure on fallback from Cisco Unified Communications Manager to Unified Secure SRST.

Three-way Software Conferencing for Secure SCCP, Unified SRST Release 12.3

From Unified SRST Release 12.3, three-way software conferencing is supported for Secure SCCP endpoints on Cisco 4000 Series Integrated Services Routers. The audio codec supported as part of the three-way software conferencing for Unified SRST 12.3 Release is G.711. The support is introduced for Secure SCCP phones and Secure SCCP endpoints registered on Cisco Analog Voice Gateways.
Three-way software conferencing is supported for a pure SCCP deployment (only involving SCCP endpoints), and a mixed deployment of secure SCCP and SIP phones. The SCCP phones such as Cisco Unified IP Phone 7962, Cisco Unified IP Phone 6961, and Cisco Unified IP Phone 7975 are supported as part of this deployment. For the mixed deployment, the Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series SIP phones are supported. Three-way Software Conference is supported on TDM trunks, for SIP and SCCP endpoints on Unified Secure SRST.

You can set a limit for the maximum number of conferences that are supported. Configure the CLI command `max-conferences` under `call-manager-fallback` configuration mode to set the maximum number of conferences supported. If you do not set the maximum number of supported conferences using the command `max-conferences`, the limit is set to the default value of 8.

Router(config-cm-fallback)#max-conferences ?
<1-16> Maximum conferences to support

For a three-way software conference supported on Secure Unified SRST:

- When a secure SCCP endpoint initiates the conference or the SCCP endpoint is a conference host, the conference is created. The three-way software conference is hosted on a Unified Secure SRST router.
- When a secure SIP endpoint initiates the conference, the three-way software conference is hosted on the SIP phone.
- When the conference host puts the call on hold, the other participants in the three-way software conference will hear Music On Hold until the call is resumed by the host. Multicast MOH is played for an SCCP endpoint, whereas Unicast MOH is played for SIP endpoints.
- When the three-way software conference host is an Analog Voice Gateway endpoint, the host cannot place the conference on hold. The three-way software conference can be put on hold only by SCCP or SIP endpoints.
- When any of the conference participants (apart from the host) put the call on hold, the other participants in the three-way software conference can continue to talk.
- For a three-way software conference on Unified SRST for Secure SCCP endpoints, the conference participants can transfer the call. The conference host cannot transfer the conference call. During an alert transfer, the other two participants can continue to talk without media interruption.
- Conference Cascading is not supported for a three-way software conference on Unified Secure SRST.
- Consider a three-way software conference hosted by an Analog Voice Gateway endpoint, with SCCP A and SCCP B as the second and third conference participants, respectively. In a scenario where SCCP B places the call on hold and the conference host tries to commit the conference using hookflash (followed by FAC), the call with SCCP B is terminated and conference attempt fails.
- Consider a scenario where an Analog Phone (AP 1) registered to the Analog Voice Gateway places a call to SCCP Phone (SCCP 1) registered to Secure SCCP SRST. After placing SCCP 1 on hold, AP 1 places a call to the third participant, SCCP Phone (SCCP 2), that is registered to the same Secure SRST. Three-way Software Conferencing is established. When SCCP 2 tries to perform an alert transfer to a phone (SIP 3 / SCCP 3) and it goes unanswered, the three-way conference is lost and it becomes a one-to-one call between AP 1 and SCCP 1. Any further attempt by AP 1 to establish a three-way software conference with another phone (SCCP 4) is not supported in this scenario.

Note If the failed alert transfer is by SCCP 1, then any further attempt to establish a three-way software conference with another phone will be supported.
Feature Support for Secure SRST (SCCP), Unified SRST Release 12.3

The Secure SCCP SRST on Cisco 4000 Series Integrated Services Routers and the Analog Voice Gateways introduced as part of Unified SRST Release 12.3, offers the following basic and supplementary call processing support. For a list of restrictions for Unified SRST 12.3 and later releases on Cisco Integrated Services Router Generation 2, see Restrictions for Configuring Secure SCCP SRST, page 279.

- Call Forward (Busy, No-answer, All)
- Call Hold or Resume
- Redial
- Secure MOH (Flash Based)
- Speed Dial (Only for Secure SCCP phones on Cisco 4000 Series Integrated Services Router)
- Secure Three-party Software Conference
- SIP trunks (Secure and Non-secure)
- TDM trunks
- Call Transfer (Alert, Consult, and Blind)
- Shared Line (Only for a pure SCCP-to-SCCP shared line. Mixed shared line is not supported.)
- Caller ID
- Call Waiting
- Media Inactivity

The following features are supported for Analog Voice Gateways for Fax and Modem calls on analog FXS ports:

- Fax Passthrough
- Modem Passthrough

Cisco IP Phones Clear-Text Fallback During Non-Secure SRST

- Cisco Unified SRST versions before 12.3(14)T are not capable of supporting secure connections or have security enabled. If an SRST router is not capable of SRST as a fallback mode—that is, it is not capable of completing a TLS handshake with Cisco Unified Communications Manager—its certificate is not added to the configuration file of the Cisco IP phone. The absence of a Cisco Unified SRST router certificate causes the Cisco Unified IP phone to use nonsecure (clear-text) communication when in Cisco Unified SRST fallback mode. The capability to detect and fallback in clear-text mode is built into Cisco Unified IP phone firmware. See Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways for more information on clear-text mode.

Signaling Security on Unified SRST - TLS

- SRST Routers and the TLS Protocol, page 247
- Certificates Operation on Secure SRST, page 249
- Certificates Transport from CUCM to Secure SRST, page 251
SRST Routers and the TLS Protocol

Transport Layer Security (TLS) Version 1.0 provides secure TCP channels between Cisco Unified IP phones, secure Cisco Unified SRST Routers, and Cisco Unified Communications Manager. The TLS process begins with the Cisco Unified IP Phone establishing a TLS connection when registering with Cisco Unified Communications Manager. Assuming that Cisco Unified Communications Manager is configured to fall back to Cisco Unified SRST, the TLS connection between the Cisco Unified IP Phones and the secure Cisco Unified SRST Router is also established. If the WAN link or Cisco Unified Communications Manager fails, call control reverts to the Cisco Unified SRST router.

From Unified Secure SIP SRST Release 12.1, support is introduced for SIP-to-SIP calls with Transport Layer Security up to TLS Version 1.2. For configuring TLS 1.2 exclusivity functionality, you need to configure the command `transport tcp tls v1.2` under `sip-ua` configuration mode. When you configure TLS 1.2 exclusivity on the Secure SIP SRST, any registration attempt by phones using lower versions of TLS (1.0, 1.1) are rejected.

Before Unified SRST Release 12.3, support is available only for TLS 1.0 version with Unified Secure SCCP SRST. For Unified Secure SCCP SRST Release 12.3 and later releases, support is introduced for Transport Layer Security up to TLS version 1.2. To configure a specific TLS version or TLS 1.2 exclusivity for Unified Secure SCCP SRST, you need to configure `transport-tcp-tls` under `call-manager-fallback`. When `transport-tcp-tls` is configured without specifying a version, the default behavior of the CLI command is enabled. In the default form, all the TLS versions (except TLS 1.0) are supported for this CLI command.

For Secure SIP and Secure SCCP endpoints that do not support TLS version 1.2, you need to configure TLS 1.0 for the endpoints to register to Unified Secure SRST 12.3 (Cisco IOS XE Fuji Release 16.9.1). This also means that endpoints which support 1.2 should also use the 1.0 suites.

For TLS 1.0 support on Cisco IOS XE Fuji Release 16.9.1 for SCCP endpoints, you need to specifically configure:

- `transport-tcp-tls v1.0` under `call-manager-fallback` configuration mode

For TLS 1.0 support on Cisco IOS XE Fuji Release 16.9.1 for pure SIP and mixed deployment scenarios, you need to specifically configure:

- `transport-tcp-tls v1.0` under `sip-ua` configuration mode

From Cisco IOS XE Fuji Release 16.9.1 Release, the security certificate exchange between Unified Secure SRST Release 12.3 and Unified Communications Manager does not support TLS version 1.0.

**Note**
Unified Communications Manager Release 11.5.1SU3 is the minimum version required to support security certificate exchange with Unified Secure SRST Release 12.3 (Cisco IOS XE Fuji Release 16.9.1).

For more information on the `transport-tcp-tls` command, see [Cisco Unified SRST Command Reference (All Versions)](Cisco Unified SCCP and SIP SRST System Administrator Guide).

**Note**
SCCP phones and the Analog Voice Gateways VG202, VG204, and VG224 support only TLS version 1.0. For Unified Secure SRST 12.3 Release and later, TLS versions 1.1 and 1.2 are supported only for Cisco Analog Voice Gateways VG202XM, VG204XM, VG310, and VG320.

You can configure `transport-tcp-tls` under `call-manager-fallback` for Unified Secure SCCP SRST as follows:

```bash
Router(config-cm-fallback)#transport-tcp-tls ?
```
Information About Configuring Secure SRST

v1.0  Enable TLS Version 1.0
v1.1  Enable TLS Version 1.1
v1.2  Enable TLS Version 1.2

Note When you configure TLS 1.2 exclusivity on the Secure SCCP SRST, any new connection attempt by phones using lower TLS versions (1.0, 1.1) are rejected. Also, the existing TLS connections will be intact, until the connection is reset.

For Unified Secure SCCP SRST Release 12.3 and later releases, Analog Voice Gateways can register their SCCP endpoints with Transport Layer Security versions up to 1.2 (TLS 1.0, 1.1, and 1.2). For support of a specific TLS version on the analog voice gateways for Unified SRST Release 12.3 and later, you need to configure `stcapp security tls-version` under `stcapp`:

```
   enable
   configure terminal
   stcapp security tls-version ?
   exit
```

```
VG(config)#stcapp security tls-version ?
v1.0  Enable TLS Version 1.0
v1.1  Enable TLS Version 1.1
v1.2  Enable TLS Version 1.2
```

TLS Cipher Support for Secure SRST 12.6 and Later Releases

From Unified Secure SRST 12.6 onwards, the TLS cipher support offered on Secure SRST is modified to enhance security.

TLS Cipher Support for SCCP/TLS (Ports 2443 and 2445)

The following cipher suites are supported (offer and accept):

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_AES_GCM_SHA2

The following cipher suites are not supported:

- TLS_RSA_WITH_NULL_SHA

TLS Cipher Support for SIP/TLS (Port 5061)

The following cipher suites are supported (offer and accept):

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

The following cipher suites are not supported:

- TLS_RSA_WITH_RC4_128_MD5
TLS_DHE_RSA_WITH_AES_128_CBC_SHA1

Certificates Operation on Secure SRST

- Cisco Unified SRST Routers and PKI, page 249
- Cisco IOS Credentials Server on Secure SRST Routers, page 250
- Generating a Certificate for the Credentials Server, page 251

Cisco Unified SRST Routers and PKI

The transfer of certificates between a Cisco Unified SRST router and Cisco Unified Communications Manager is mandatory for secure SRST functionality. Public key infrastructure (PKI) commands are used to generate, import, and export the certificates for secure Cisco Unified SRST. Table 9-1 shows the secure SRST-supported Cisco Unified IP Phones and the appropriate certificate for each phone. The “Additional References” section on page 308 contains information and configurations about generating, importing, and exporting certificates that use PKI commands.

Note
Certificate text can vary depending on your configuration. You may also need CAP-RTP-00X or CAP-SJC-00X for older phones that support manufacturing installed certificate (MIC).

Note
Cisco supports Cisco IP Phones 7900 series phone memory reclamation phones that use MIC or locally significant certificate (LSC) certificates.

Table 9-1    Supported Cisco Unified IP Phones and Certificates
Cisco Unified SCCP and SIP SRST System Administrator Guide

Chapter 9     Configuring Secure SRST for SCCP and SIP

Information About Configuring Secure SRST

Cisco IOS Credentials Server on Secure SRST Routers

Secure SRST introduces a credentials server that runs on a secure SRST router. When the client, Cisco Unified Communications Manager, requests a certificate through the TLS channel, the credentials server provides the SRST router certificate to Cisco Unified Communications Manager.

Cisco Unified Communications Manager inserts the SRST router certificate in the Cisco Unified IP Phone configuration file and downloads the configuration files to the phones. The secure Cisco Unified IP Phone uses the certificate to authenticate the SRST router during fallback operations. The credentials service runs on default TCP port 2445.

Three Cisco IOS commands configure the credentials server in call-manager-fallback mode:

- credentials
- ip source-address (credentials)
- trustpoint (credentials)

Two Cisco IOS commands provide credential server debugging and verification capabilities:

- debug credentials
- show credentials
Generating a Certificate for the Credentials Server

In configuring the credentials server on the Unified Secure SRST, a certificate is required to complete the "trustpoint <trustpoint name>" configuration entry.

To generate the certificate for Credentials Server, perform the following procedures:

- Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 257
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 264
- Configuring SRST Fallback on Cisco Unified Communications Manager, page 275

Once the certificate is generated, fill in the name of the certificate (or the name of the trustpoint in IOS) in the "trustpoint" entry.

This certificate for the Credentials Server on the Secure SRST will be seamlessly exported to the Cisco Unified CM when requested in “Adding an SRST Reference to Cisco Unified Communications Manager” section on page 274.

Certificates Transport from CUCM to Secure SRST

For more information about Certificates Transport from CUCM to Secure SRST, see “Importing Phone Certificate Files in PEM Format to the Secure SRST Router” section on page 266.

Media Security on Unified SRST - SRTP

Media encryption, which uses Secure Real-Time Protocol (SRTP), ensures that only the intended recipient can interpret the media streams between supported devices. Support includes audio streams only.

If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses an RTP connection. SRTP-to-RTP fallback may occur for transfers from a secure device to a non-secure device for music-on-hold (MOH), and so on.

Note

Secure SRST handles media encryption keys differently for different devices and protocols. All phones that are running SCCP get their media encryption keys from SRST, which secures the media encryption key downloads to phones with TLS encrypted signaling channels. Phones that are running SIP generate and store their own media encryption keys. Media encryption keys that are derived by SRST securely get sent through encrypted signaling paths to gateways over IPSec-protected links for H.323.

Warning

Before you configure SRTP or signaling encryption for gateways and trunks, Cisco strongly recommends that you configure IPSec because Cisco H.323 gateways, and H.323/H.245/H.225 trunks rely on IPSec configuration to ensure that security-related information does not get sent in the clear. Cisco Unified SRST does not verify that you configured IPSec correctly. If you do not configure IPSec correctly, security-related information may get exposed.
Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone

Figure 9-1 shows the interworking of the credentials server on the SRST router, Cisco Unified Communications Manager, and the Cisco Unified IP Phone. Table 9-2 describes the establishment of secure SRST to the Cisco Unified IP Phone.

Figure 9-1 Interworking of Credentials Server on SRST Router, Cisco Unified Communications Manager, and Cisco Unified IP Phone

Table 9-2 Establishing Secure SRST

<table>
<thead>
<tr>
<th>Mode</th>
<th>Process</th>
<th>Description or Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular Mode</td>
<td>The Cisco Unified IP Phone configures DHCP and gets the TFTP server address.</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Cisco Unified IP Phone retrieves a CTL file from the TFTP server.</td>
<td>The CTL file contains the certificates that the phone should trust.</td>
</tr>
<tr>
<td></td>
<td>The Cisco IP Phone opens a Transport Layer Security (TLS) protocol channel and registers to Cisco Unified Communications Manager.</td>
<td>Cisco Unified Communications Manager exports secure Cisco Unified SRST router information and the Cisco Unified SRST router certificate to the Cisco Unified IP phone. The phone places the certificate into its configuration. Once the phone has the Cisco Unified SRST certificate, the Cisco Unified SRST router is considered secure. See Figure 9-1.</td>
</tr>
<tr>
<td></td>
<td>If the Cisco Unified IP Phone is configured as “authenticated” or “encrypted” and Cisco Unified Communications Manager is configured in mixed mode, the phone looks for an SRST certificate in its configuration file. If it finds an SRST certificate, it opens a standby TLS connection to the default port. The default port is the Cisco Unified IP Phone TCP port plus 443; that is, port 2443 on a Cisco Unified SRST router.</td>
<td>The connection to the SRST router happens automatically, assuming there is not a secondary Cisco Unified Communications Manager and Cisco Unified SRST is configured as the backup device. See Figure 9-1. Cisco Unified Communications Manager should be configured in mixed mode, which is its secure mode.</td>
</tr>
</tbody>
</table>
In case of WAN failure, the Cisco Unified IP Phone starts Cisco Unified SRST registration.

| SRST Mode | The Cisco Unified IP Phone registers with the SRST router at the default port for secure communications. |

## Secure SRST Authentication and Encryption

Figure 9-2 illustrates the process of secure SRST authentication and encryption, and Table 9-3 describes the process.

### Table 9-3 Overview of the Process of Secure SRST Authentication and Encryption

<table>
<thead>
<tr>
<th>Process Steps</th>
<th>Description or Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The CA server, whether it is a Cisco IOS router CA or a third-party CA, issues a device certificate to the SRST gateway, enabling credentials service. Optionally, the certificate can be self-generated by the SRST router using a Cisco IOS CA server. The CA router is the ultimate trustpoint for the Certificate Authority Proxy Function (CAPF). For more information on CAPF, see <em>Cisco Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>2.</td>
<td>The CAPF is a process where supported devices can request a locally significant certificate (LSC). The CAPF utility generates a key pair and certificate that is specific for CAPF, copies this certificate to all Cisco Unified Communications Manager servers in the cluster, and provides the LSC to the Cisco Unified IP Phone. An LSC is required for Cisco Unified IP Phones that do not have a manufacturing installed certificate (MIC). The Cisco 7970 is equipped with a MIC and therefore does not need to go through the CAPF process.</td>
</tr>
<tr>
<td>3.</td>
<td>Cisco Unified Communications Manager requests the SRST certificate from credentials server, and the credentials server responds with the certificate.</td>
</tr>
</tbody>
</table>
How to Configure Secure Unified SRST

The following configuration sections ensure that the secure Cisco Unified SRST Router and the Cisco Unified IP Phones can request mutual authentication during the TLS handshake. The TLS handshake occurs when the phone registers with the Cisco Unified SRST Router, either before or after the WAN link fails.

This section contains the following procedures:

- Preparing the Cisco Unified SRST Router for Secure Communication, page 255
- Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router, page 274
- Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 277
- Configuring Secure SCCP SRST, page 279
- Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 293g

### Table 9-3: Overview of the Process of Secure SRST Authentication and Encryption (continued)

<table>
<thead>
<tr>
<th>Process Steps</th>
<th>Description or Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>For each device, Cisco Unified CM uses the TFTP process and inserts the certificate into the SEPMACxxxx.cnf.xml configuration file of the Cisco Unified IP Phone.</td>
</tr>
<tr>
<td>5.</td>
<td>Cisco Unified CM provides the PEM format files that contain phone certificate information to the Cisco Unified SRST router. Providing the PEM files to the Cisco Unified SRST router is done manually. See “Cisco IOS Credentials Server on Secure SRST Routers” section on page 250 for more information. When the Cisco Unified SRST router has the PEM files, the Cisco Unified SRST Router can authenticate the IP phone and validate the issuer of the IP phones certificate during the TLS handshake.</td>
</tr>
<tr>
<td>6.</td>
<td>The TLS handshake occurs, certificates are exchanged, and mutual authentication and registration occurs between the Cisco Unified IP Phone and the Cisco Unified SRST Router.</td>
</tr>
<tr>
<td>a.</td>
<td>The Cisco Unified SRST Router sends its certificate, and the phone validates the certificate to the certificate that it received from Cisco Unified CM in Step 4.</td>
</tr>
<tr>
<td>b.</td>
<td>The Cisco Unified IP Phone provides the Cisco Unified SRST Router the LSC or MIC, and the router validates the LSC or MIC using the PEM format files that it was provided in Step 5.</td>
</tr>
</tbody>
</table>

Note: The media is encrypted automatically after the phone and router certificates are exchanged and the TLS connection is established with the SRST router.
Preparing the Cisco Unified SRST Router for Secure Communication

The following tasks prepare the Cisco Unified SRST Router to process secure communications.

- Configuring a Certificate Authority Server on a Cisco IOS Certificate Server, page 255 (optional)
- Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 257 (required)
- Disabling Automatic Certificate Enrollment, page 261 (required)
- Verifying Certificate Enrollment, page 262 (optional)
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 264 (required)
- Troubleshooting Credential Settings, page 266
- Importing Phone Certificate Files in PEM Format to the Secure SRST Router, page 266

Configuring a Certificate Authority Server on a Cisco IOS Certificate Server

For Cisco Unified SRST Routers to provide secure communications, there must be a CA server that issues the device certificate in the network. The CA server can be a third-party CA or one generated from a Cisco IOS certificate server.

The Cisco IOS certificate server provides a certificate generation option to users who do not have a third-party CA in their network. The Cisco IOS certificate server can run on the SRST router or on a different Cisco IOS router.

If you do not have a third-party CA, full instructions on enabling and configuring a CA server can be found in the Cisco IOS Certificate Server documentation. A sample configuration is provided below.

SUMMARY STEPS

1. `crypto pki server cs-label`
2. `database level {minimal | names | complete}`
3. `database url root-url`
4. `issuer-name DN-string`
5. `grant auto`
6. `no shutdown`
# How to Configure Secure Unified SRST

## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>crypto pki server cs-label</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router (config)# crypto pki server srstcaserver</td>
</tr>
<tr>
<td>Enables the certificate server and enters certificate server configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>If you manually generated an RSA key pair, the cs-label argument must match the name of the key pair.</td>
</tr>
<tr>
<td>For more information on the certificate server, see the Cisco IOS Certificate Server documentation.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>database level {minimal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router (cs-server)# database level complete</td>
</tr>
<tr>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
<td></td>
</tr>
<tr>
<td>• minimal: Enough information is stored only to continue issuing new certificates without conflict; this is the default.</td>
<td></td>
</tr>
<tr>
<td>• names: In addition to the information given in the minimal level, the serial number and subject name of each certificate are stored.</td>
<td></td>
</tr>
<tr>
<td>• complete: In addition to the information given in the minimal and names levels, each issued certificate is written to the database.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The complete keyword produces a large amount of information; if it is issued, you should also specify an external TFTP server on which to store the data using the database url command.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>database url root-url</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router (cs-server)# database url nvram</td>
</tr>
<tr>
<td>Specifies the location where all database entries for the certificate server will be written. After you create a certificate server using the crypto pki server command, use this command to specify a combined list of all the certificates that have been issued. The root-url argument specifies the location where database entries are written.</td>
<td></td>
</tr>
<tr>
<td>• The default location for the database entries to be written is flash; however, NVRAM is recommended for this task.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>issuer-name DN-string</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router (cs-server)# issuer-name CN=srstcaserver</td>
</tr>
<tr>
<td>Sets the CA issuer name to the specified distinguished name (DN-string). The default value is as follows:</td>
<td></td>
</tr>
<tr>
<td>issuer-name CN=cs-label.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 9      Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

Examples

The following example reflects one way of generating a CA:

Router(config)# crypto pki server srstcaserver
Router(cs-server)# database level complete
Router(cs-server)# database url nvram
Router(cs-server)# issuer-name CN=srstcaserver
Router(cs-server)# grant auto

% This will cause all certificate requests to be automatically granted.
Are you sure you want to do this? [yes/no]: y
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: y
% Generating 1024 bit RSA keys ...[OK]
% Certificate Server enabled.

Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server

The secure Cisco Unified SRST Router needs to define a trustpoint; that is, it must obtain a device certificate from the CA server. The procedure is called certificate enrollment. Once enrolled, the secure Cisco Unified SRST Router can be recognized by Cisco Unified Communications Manager as a secure SRST router.

There are three options to enroll the secure Cisco Unified SRST Router to a CA server: autoenrollment, cut and paste, and TFTP. When the CA server is a Cisco IOS certificate server, autoenrollment can be used. Otherwise, manual enrollment is required. Manual enrollment refers to cut and paste or TFTP.

Use the enrollment url command for autoenrollment and the crypto pki authenticate command to authenticate the SRST router. Full instructions for the commands can be found in the Certification Authority Interoperability Commands documentation. An example of autoenrollment is available in the Certificate Enrollment Enhancements feature. A sample configuration is provided in the “Examples” section on page 260.

SUMMARY STEPS

1. crypto pki trustpoint name
2. rsakeypair keypair-label
3. enrollment url url
4. revocation-check method1
5. exit
6. crypto pki authenticate name
7. crypto pki enroll name
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>crypto pki trustpoint name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# crypto pki trustpoint srstca</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>rsakeypair keypair-label</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-trustp)# rsakeypair srstcakey 2048</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>enrollment url url</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# enrollment url <a href="http://10.1.1.22">http://10.1.1.22</a></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>revocation-check method1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# revocation-check none</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# exit</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `crypto pki authenticate` name | Authenticates the CA (by getting the certificate from the CA).  
  - Takes the name of the CA as the argument. |
| **Example:**            |                                                   |
| Router(config)# `crypto pki authenticate srstca` |                                                   |
| **Step 7**              |                                                   |
| `crypto pki enroll` name | Obtains the SRST router certificate from the CA.  
  - Takes the name of the CA as the argument. |
| **Example:**            |                                                   |
| Router(config)# `crypto pki enroll srstca` |                                                   |

**Examples**

The following example autoenrolls and authenticates the Cisco Unified SRST router:

```plaintext
Router(config)# `crypto pki trustpoint srstca`  
Router(ca-trustpoint)# `enrollment url http://10.1.1.22`  
Router(ca-trustpoint)# `revocation-check none`  
Router(ca-trustpoint)# `exit`  
Router(config)# `crypto pki authenticate srstca`  
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.  
Router(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 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]: n  
% 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 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint MD5: D154FB75  
2524A24D 3D1F5C2B 46A7B9E4  
Sep 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 0573FB82  
98CD1AD0 F37D591A C595252D A17523C1  
Sep 29 00:41:57.339: %PKI-6-CERTRET: Certificate received from Certificate Authority
```
Disabling Automatic Certificate Enrollment

The command `grant auto` allows certificates to be issued and was activated in the optional task documented in the “Configuring a Certificate Authority Server on a Cisco IOS Certificate Server” section on page 255.

| Note | You should disable the `grant auto` command so that certificates cannot be continually granted. |

**SUMMARY STEPS**

1. `crypto pki server cs-label`
2. `shutdown`
3. `no grant auto`
4. `no shutdown`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> crypto pki server <code>cs-label</code></td>
<td>Enables the certificate server and enters certificate server configuration mode. <strong>Note</strong> If you manually generated an RSA key pair, the <code>cs-label</code> argument must match the name of the key pair.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (config)# crypto pki server srstcaserver</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>shutdown</code></td>
<td>Disables the Cisco IOS certificate server.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (cs-server)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>no grant auto</code></td>
<td>Disables automatic certificates to be issued to any requestor. <strong>•</strong> This command was for use during enrollment only and thus needs to be removed in this task.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (cs-server)# no grant auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>no shutdown</code></td>
<td>Enables the Cisco IOS certificate server. <strong>•</strong> You should issue this command only after you have completely configured your certificate server.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router (cs-server)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

**What to Do Next**

For manual enrollment instructions, see the *Manual Certificate Enrollment (TFTP and Cut-and-Paste)* feature.
Verifying Certificate Enrollment

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`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Use the <code>show running-config</code> command to verify the creation of the CA server (01) and device (02) certificates. This example shows the enrolled certificates.</td>
</tr>
</tbody>
</table>

Example:
```
Router# show running-config
.
.
! SRST router device certificate.
crypto pki certificate chain srstca
certificate 02
30B201AD 30B20116 A0030201 02020102 300D0609
2A864886 F70D0101 04050030
17311530 11060355 0403130C 73727374 63617365
72676572 301E170D 30343034
31323139 35323233 5A170D30 35303431 32313935
3232335A 30343132 300F0603
55040513 80443042 39453739 43301F06 092A8648
86F70D01 09021612 6A1736F
32363931 2E636973 6562726E 63617365 72766572 301E170D 30303030 300D0609
2A864886 F70D0101 04050030
4B003048 02410007 0CC354FB 5F7C1AE7 7A25C3F2
056E0485 2286D36 6CA70C19
C98F9BAE AE9D1F9B D4BB7A67 F3251174 193B1A3
12946123 E5C1CCD7 A23E6155
FA2ED743 3F88B902 03010001 A330302E 300B0603
551D0F04 04030205 A0301F06
01551D23 04183016 8014FB29 CB97AD60 1B0D5467
FC293963 C2470691 F9B2000D
0B092A86 4886F70D 01010405 0038B181 007EB48E
CAE9B1B3 D1E7A185 D7F0D565
CB84B17B 1151BD7B B3E9763 59EC650E 49371F6D
99CBDB267 EB8ADF9D 9E43A5F2
FB2B18A0 3A4F6564 11239473 1417ABFC A86E6DA1
AC518EDB 8657CBBB ED2BEB8E
B586FE67 0C358D4 0F0DFD4B 3F421341 C2D331D3
1BE43B6E 6CB29E7 E83C2752
C3AF4A66 BD007348 D013000A EA3C206D CF |
quit

certificate ca 01
30B201AD 30B20116 A0030201 02020102 300D0609
2A864886 F70D0101 04050030
17311530 11060355 0403130C 73727374 63617365
72676572 301E170D 30343034
31323139 35323233 5A170D30 35303431 32313935
3232335A 30343132 300F0603
55040513 80443042 39453739 43301F06 092A8648
86F70D01 09021612 6A1736F
32363931 2E636973 6562726E 63617365 72766572 301E170D 30303030 300D0609
2A864886 F70D0101 04050030
4B003048 02410007 0CC354FB 5F7C1AE7 7A25C3F2
056E0485 2286D36 6CA70C19
C98F9BAE AE9D1F9B D4BB7A67 F3251174 193B1A3
12946123 E5C1CCD7 A23E6155
FA2ED743 3F88B902 03010001 A330302E 300B0603
551D0F04 04030205 A0301F06
01551D23 04183016 8014FB29 CB97AD60 1B0D5467
FC293963 C2470691 F9B2000D
0B092A86 4886F70D 01010405 0038B181 007EB48E
CAE9B1B3 D1E7A185 D7F0D565
CB84B17B 1151BD7B B3E9763 59EC650E 49371F6D
99CBDB267 EB8ADF9D 9E43A5F2
FB2B18A0 3A4F6564 11239473 1417ABFC A86E6DA1
AC518EDB 8657CBBB ED2BEB8E
B586FE67 0C358D4 0F0DFD4B 3F421341 C2D331D3
1BE43B6E 6CB29E7 E83C2752
C3AF4A66 BD007348 D013000A EA3C206D CF |
Chapter 9 Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

Enabling Credentials Service on the Secure Cisco Unified SRST Router

Once the Cisco Unified SRST Router has its own certificate, you need to provide Cisco Unified Communications Manager the certificate. Enabling credentials service allows Cisco Unified Communications Manager to retrieve the secure SRST device certificate and place it in the configuration file of the Cisco Unified IP Phone.

Activate credentials service on all Cisco Unified SRST Routers.

Note

A security best practice is to protect the credentials service port using Control Plane Policing. Control Plane Policing protects the gateway and maintains packet forwarding and protocol states despite a heavy traffic load. For more information on control planes, see the Control Plane Policing documentation. In addition, a sample configuration is given in the “Control Plane Policing: Example” section on page 292.
SUMMARY STEPS

1. credentials
2. ip source-address ip-address [port port]
3. trustpoint trustpoint-name
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> credentials</td>
<td>Provides the Cisco Unified SRST Router certificate to Cisco Unified Communications Manager and enters credentials configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# credentials</td>
</tr>
<tr>
<td><strong>Step 2</strong> ip source-address ip-address [port port]</td>
<td>Enables the Cisco Unified SRST Router to receive messages from Cisco Unified Communications Manager through the specified IP address and port.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-credentials)# ip source-address 10.1.1.22 port 2445</td>
</tr>
<tr>
<td><strong>Step 3</strong> trustpoint trustpoint-name</td>
<td>Specifies the name of the trustpoint that is to be associated with the Cisco Unified SRST Router certificate. The trustpoint-name argument is the name of the trustpoint and corresponds to the SRST device certificate.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-credentials)# trustpoint srstca</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits credentials configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-credentials)# exit</td>
</tr>
</tbody>
</table>

Examples

Router(config)# credentials
Router(config-credentials)# ip source-address 10.1.1.22 port 2445
Router(config-credentials)# trustpoint srstca
Router(config-credentials)# exit
Troubleshooting Credential Settings

The following steps display credential settings or set debugging on the credential settings of the Cisco Unified SRST Router.

SUMMARY STEPS

1. show credentials
2. debug credentials

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 show credentials</td>
<td>Use the show credentials command to display the credential settings on the Cisco Unified SRST Router that are supplied to Cisco Unified Communications Manager for use during secure Cisco Unified SRST fallback.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show credentials</td>
<td></td>
</tr>
<tr>
<td>Credentials IP: 10.1.1.22</td>
<td></td>
</tr>
<tr>
<td>Credentials PORT: 2445</td>
<td></td>
</tr>
<tr>
<td>Trustpoint: srstca</td>
<td></td>
</tr>
<tr>
<td>Step 2 debug credentials</td>
<td>Use the debug credentials command to set debugging on the credential settings of the Cisco Unified SRST Router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# debug credentials</td>
<td></td>
</tr>
<tr>
<td>Credentials server debugging is enabled</td>
<td></td>
</tr>
<tr>
<td>Router# Sep 29 01:01:50.903: Credentials service: Start TLS Handshake 1 10.1.1.13 2187</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:50.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:51.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:52.907: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:53.927: Credentials service: TLS Handshake completes.</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

Use the following commands to show if a certificate cannot be found (you are missing a certificate that you are trying to authenticate) or to show that a particular certificate has matched (so you know what certificate the router used to authenticate a phone):

- debug crypto pki messages
- debug crypto pki transactions

Importing Phone Certificate Files in PEM Format to the Secure SRST Router

This task completes the tasks required for Cisco IP Unified Phones to authenticate secure SRST.
Cisco Unified Communications Manager 4.X.X and Earlier Versions

For systems running Cisco Unified Communications Manager 4.X.X and earlier versions, the secure Cisco Unified SRST Router must retrieve phone certificates so that it can authenticate Cisco Unified IP phones during the TLS handshake. Different certificates are used for different Cisco Unified IP Phones. Table 9-1 lists the certificates needed for each type of phone.

Certificates must be imported manually from Cisco Unified Communications Manager to the Cisco Unified SRST Router. The number of certificates depends on the Cisco Unified Communications Manager configuration. Manual enrollment refers to cut and paste or TFTP. For manual enrollment instructions, see the Manual Certificate Enrollment (TFTP and Cut-and-Paste) feature. Repeat the enrollment procedure for each phone or PEM file.

For Cisco Unified Communications Manager 4.X.X and earlier versions, certificates are found by going to the menu bar in Cisco Unified Communications Manager, choose Program Files > Cisco > Certificates.

Open the .0 files with Windows WordPad or Notepad, and copy and paste the contents to the SRST router console. Then, repeat the procedure with the .pem file. Copy all the contents that appear between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”.


Cisco Unified Communications Manager 5.0 and Later Versions

Systems running Cisco Unified CM 5.0 and later versions require four certificates (CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048) in addition to the requirements listed in Table 9-1, which must be copied and pasted to Cisco Unified SRST Routers.

Note CiscoRootCA is also called CiscoRoot2048CA.

Prerequisites

You must have certificates available when the last configuration command (crypto pki authenticate) issues the following prompt:

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

For Cisco Unified CM 5.0 and later versions, perform the following steps:

---

**Step 1** Login to Cisco Unified Communications Manager.

**Step 2** Go to Security > Certificate Management > Download Certificate/CTL.

**Step 3** Select Download Trust Cert and click Next.

**Step 4** Select CAPF-trust and click Next.

**Step 5** Select CiscoCA and click Next.

**Step 6** Click Continue.

**Step 7** Click the file name.
Step 8  Copy all the contents that appear between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” to a location where you can retrieve it later.

Step 9  Repeat Steps 5 to 8 for CiscoManufactureCA, CiscoRootCA2048, and CAPF.

Cisco Unified Communications Manager 6.0 and Later Versions

From Cisco Unified Communications Operating System Administration, download all certificates listed under CAPF-trust, including 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.

For instructions on downloading certificates, see the “Security” chapter in the appropriate version of Cisco Unified Communications Operating System Administration Guide.

Authenticating the Imported Certificates on the Cisco Unified SRST Router

To authenticate certificates on the Cisco Unified SRST router, perform these steps.

Restrictions

HTTP automatic enrollment from Cisco Unified Communications Manager through a virtual web server is not supported.

SUMMARY STEPS

1. crypto pki trustpoint name
2. revocation-check none
3. enrollment terminal
4. exit
5. crypto pki authenticate name
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** crypto pki trustpoint name | Declares the CA that your router should use and enters ca-trustpoint configuration mode.  
* name: Enter the name of each certificate individually (for example, CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048). |
| Example: Router(config)# crypto pki trustpoint CAPF | |
| **Step 2** revocation-check none | Checks the revocation status of a certificate using the selected method.  
* Using the none keyword is mandatory for this task. The keyword none means that a revocation check is not performed and the certificate is always accepted. |
| Example: Router(ca-trustpoint)# revocation-check none | |
| **Step 3** enrollment terminal | Specifies manual cut-and-paste certificate enrollment. |
| Example: Router(ca-trustpoint)# enrollment terminal | |
| **Step 4** exit | Exits ca-trustpoint configuration mode and returns to global configuration. |
| Example: Router(ca-trustpoint)# exit | |
| **Step 5** crypto pki authenticate name | Authenticates the CA (by getting the certificate from the CA).  
* Enter the same name argument used in the crypto pki trustpoint command in Step 1. |
| Example: Router(config)# crypto pki authenticate CAPF | |

What to Do Next

Update the certificates in Cisco Unified CM. See the “Configuring a Secure Survivable Remote Site Telephony (SRST) Reference” chapter in the appropriate version of Cisco Unified Communications Manager Security Guide.

Examples

This section provides the following:

- Cisco Unified Communications Manager 4.X.X and Earlier Versions: Example, page 270
- Cisco Unified Communications Manager 5.0 and Later Versions Example, page 272
Chapter 9      Configuring Secure SRST for SCCP and SIP

Cisco Unified Communications Manager 4.X.X and Earlier Versions: Example

The following example shows three certificates (Cisco 7970, 7960, PEM) imported to the Cisco Unified SRST Router:

Router(config)# crypto pki trustpoint 7970
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(config)# exit
Router(config)# crypto pki authenticate 7970

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

Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(config)# exit
Router(config)# crypto pki authenticate 7960

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

Certificate has the following attributes:
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Certificate has the following attributes:
Fingerprint MD5: 4B9636DF 0F3BA6B7 5F54BE72 24762DCB
% Certificate successfully imported

Certificate has the following attributes:
Fingerprint MD5: 84BD5F1B 7A8B0FBB 7B2A74E8 1F0A1E80
% Certificate successfully imported

Certificate has the following attributes:
Fingerprint MD5: 84BD5F1B 7A8B0FBB 7B2A74E8 1F0A1E80
% Certificate successfully imported

Certificate has the following attributes:
Fingerprint MD5: 84BD5F1B 7A8B0FBB 7B2A74E8 1F0A1E80
% Certificate successfully imported

Certificate has the following attributes:
Fingerprint MD5: 84BD5F1B 7A8B0FBB 7B2A74E8 1F0A1E80
% Certificate successfully imported

Certificate has the following attributes:
Fingerprint MD5: 84BD5F1B 7A8B0FBB 7B2A74E8 1F0A1E80
% Certificate successfully imported

Certificate has the following attributes:
Fingerprint MD5: 84BD5F1B 7A8B0FBB 7B2A74E8 1F0A1E80
% Certificate successfully imported
How to Configure Secure Unified SRST

Fingerprint SHA1: A9917775 F86B3B7A 5C130ED2 8E8E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint PEM
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate PEM

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

Certificate has the following attributes:
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 44782932 25990732 227631BE
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Use the show crypto pki trustpoint status command to show that enrollment has succeeded and that five CA certificates were granted. The five certificates include the three certificates just entered and the CA server certificate and the SRST router certificate.

Router# show crypto pki trustpoint status

Trustpoint 7970:
Issuing CA certificate configured:
Subject Name: cn=CAP-RTP-002,o=Cisco Systems
Fingerprint SHA1: F7B40B94 5831D2AB 44782932 25990732 227631BE
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
Cisco Unified Communications Manager 5.0 and Later Versions Example

The following example shows the configuration for the four certificates (CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048) that are required for systems running Cisco Unified Communications Manager 5.0:

```bash
Router(config)# crypto pki trustpoint CAPF
Router(config)# crypto pki authenticate CAPF
```
Chapter 9  Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

f8Z0tYwT2l4L++mC64O3s3AshDi8xeY8sN/f/ZKRRhNixBl4SwxfXnHKZBgKZn
WtSkg8K3JdhXtcqWYtB5S2sC69g8aX09xlkKl3m+TpWsr27/mDVx6CeaKE+ch
gcrmmNo8kamoOIG8osQc4LEXzXQDAQAbwEwLzAOBgnNHQ8BAf8BBAMCAqWQYDQ
quit
Certificate has the following attributes:
Certificate fingerprint (MD5): 1951DJ4E 76D79FEB FFB061C6 233C8E33
Certificate fingerprint (SHA1): 222891BE Z7B89B94 447AB8F2 5831D2AB 25990732
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoCA
Router(config)# enrollment terminal
Router(config)# exit
Router(config)# crypto pki authenticate CiscoCA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCCApCgAwIBAgIQdhL5YBU9b59OQiAgMrcjVjAmBqghkiiG9w0BAQUPAD8Au
MRyWyFDVYQDEvKw1DaXnJbyBTEN0Z1wMgQ8BgYDVQDEwtJDQAvUlRQLTwMfTa
Vd54ClqDjHpQdfBrFkCvYhIwsw7vwnPsLuyjKw2l2cF0UXyGhhGlx84qvGqWFo
NnYy7aKj435VD3tzn73n8jv1rU20x3mdbcB6dhBaA825Yo7a8sk12eShM7/YdMm
vyn0pMDNzXmeHuqBegVOSUm6GVCX+K1y1dUUIgqJNYTqLkjq7wqccGjshDhr3a
U+wb1ulg9G8qMoWm6owAo+6hmMx1oANPweufgZMywIBAG6BWzCBwD8LBgNHQ8BE
ce6a7fm5nQRlc5PmUULiDBzKYNbnEjizptaIC5fgB/S9S6C1q0YxPZfnstUjy
WXe2YSpFxc6b0U7H1QJ1oqgCMAUKLoPaZu7tVDSH3hD4+VjmmLyysaULHksGFpr
phszZrsVV11K17qgCPlLkGAS4fSkruq3r/6i/SXp68/gAoIjBJkXPFZ2xqgCU
laU9cURLFP95DOPN1jKB3ips7cVIdcogowPQ==
quit
Certificate has the following attributes:
Certificate fingerprint (MD5): 21956CBR 4B9706DF 0F31A6B7 7P54A272
Certificate fingerprint (SHA1): A9917775 F86BB37A 7H130ED2 3E528BB8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoManufactureCA
Router(config)# enrollment terminal
Router(config)# exit
Router(config)# crypto pki authenticate CiscoManufactureCA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIE2TCCA8gAgAwIBAgIKAmlmewAAAAAAsANGBqghkiiG9w0BAQUPAD8Au
MRvWyFDVQDEvKw1DaXnJbyBTEN0Z1wMgQ8BgYDVQDEwtJDQAvUlRQLTwMfTa
Vd54ClqDjHpQdfBrFkCvYhIwsw7vwnPsLuyjKw2l2cF0UXyGhhGlx84qvGqWFo
NnYy7aKj435VD3tzn73n8jv1rU20x3mdbcB6dhBaA825Yo7a8sk12eShM7/YdMm
vyn0pMDNzXmeHuqBegVOSUm6GVCX+K1y1dUUIgqJNYTqLkjq7wqccGjshDhr3a
U+wb1ulg9G8qMoWm6owAo+6hmMx1oANPweufgZMywIBAG6BWzCBwD8LBgNHQ8BE
ce6a7fm5nQRlc5PmUULiDBzKYNbnEjizptaIC5fgB/S9S6C1q0YxPZfnstUjy
WXe2YSpFxc6b0U7H1QJ1oqgCMAUKLoPaZu7tVDSH3hD4+VjmmLyysaULHksGFpr
phszZrsVV11K17qgCPlLkGAS4fSkruq3r/6i/SXp68/gAoIjBJkXPFZ2xqgCU
laU9cURLFP95DOPN1jKB3ips7cVIdcogowPQ==
quit
Chapter 9  Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

Certificate has the following attributes:
Fingerprint MDS: 0F3BA6B7 4B9636DF 5F54BE72 24762SBR
Fingerprint SHA1: L92BB37A S9919925 5C1103ED2 3E528UF8 286E8C2D
% Do you accept this certificate? [yes/no]: y
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoRootCA2048
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(config)# crypto pki authenticate CiscoRootCA2048

Certificate has the following attributes:
Fingerprint MD5: 0F3BA6B7 4B9636DF 5F54BE72 24762SBR
Fingerprint SHA1: L92BB37A S9919925 5C1103ED2 3E528UF8 286E8C2D
% Do you accept this certificate? [yes/no]: y
% Certificate successfully imported

Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router

The following tasks are performed in Cisco Unified Communications Manager:
• Adding an SRST Reference to Cisco Unified Communications Manager, page 274 (required)
• Configuring SRST Fallback on Cisco Unified Communications Manager, page 275 (required)
• Configuring CAPF on Cisco Unified Communications Manager, page 277 (required)

Adding an SRST Reference to Cisco Unified Communications Manager

The following tasks are performed in Cisco Unified Communications Manager:

Before following this procedure, verify that credentials service is running in the Cisco Unified SRST Router. To enable credentials service, see the “Enabling Credentials Service on the Cisco Unified SRST Router” section on page 264.
For complete information on adding Cisco Unified SRST to Cisco Unified Communications Manager, see the “Survivable Remote Site Telephony Configuration” section for the Cisco Unified Communications Manager version that you are running. All Cisco Unified CM administration guides are at the following URL:

Step 1  In the menu bar in Cisco Unified Communications Manager, choose **CCMAdmin > System > SRST**.

Step 2  Click **Add New SRST Reference**.

Step 3  Enter the appropriate settings. **Figure 9-3** shows the available fields in the SRST Reference Configuration window.

   a. Enter the name of the SRST gateway, the IP address, and the port.
   b. Check the box asking if the SRST gateway is secure.
   c. Enter the certificate provider (credentials service) port number. Credentials service runs on default port 2445.

**Figure 9-3**  **SRST Reference Configuration Window**

Step 4  To add the new SRST reference, click **Insert**. The message “Status: Insert completed” displays.

Step 5  To add more SRST references, repeat Steps 2 to 4.

**Configuring SRST Fallback on Cisco Unified Communications Manager**

The following procedure describes how to configure SRST fallback on Cisco Unified Communications Manager by assigning the Unified SRST reference to a device pool.
For complete information about adding a device pool to Cisco Unified Communications Manager, see the “Device Pool Configuration” section in *Cisco Unified Communications Manager Administration Guide* for the Cisco Unified Communications Manager version that you are running. All Cisco Unified CM administration guides are at the following URL:

**Step 1**
In the menu bar in Cisco Unified Communications Manager, choose **CCMAdmin > System > Device Pool**.

**Step 2**
Use one of the following methods to add a device pool:

- If a device pool already exists with settings that are similar to the one that you want to add, choose the existing device pool to display its settings, click **Copy**, and modify the settings as needed. Continue with **Step 4**.
- To add a device pool without copying an existing one, continue with **Step 3**.

**Step 3**
In the upper, right corner of the window, click the **Add New Device Pool** link. The Device Pool Configuration window displays (see Figure 9-4).

**Figure 9-4 Device Pool Configuration Window**

**Device Pool Configuration**

<table>
<thead>
<tr>
<th>Device Pool: Default (13 members*)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Pool Name</strong>:* Default</td>
</tr>
<tr>
<td><strong>Cisco CallManager Group</strong>:* Default</td>
</tr>
<tr>
<td><strong>Date/Time Group</strong>:* CMLocal</td>
</tr>
<tr>
<td><strong>Region</strong>:* Default</td>
</tr>
<tr>
<td><strong>Softkey Template</strong>:* StandardUser</td>
</tr>
<tr>
<td><strong>SRST Reference</strong>:* jaso2991</td>
</tr>
<tr>
<td><strong>Calling Search Space for Auto-registration</strong>:* NotSelected</td>
</tr>
<tr>
<td><strong>Media Resource Group List</strong>:* Disable</td>
</tr>
<tr>
<td><strong>Network Hold MOH Audio Source</strong>:* jaso2991</td>
</tr>
<tr>
<td><strong>User Hold MOH Audio Source</strong>:* &lt; None &gt;</td>
</tr>
<tr>
<td><strong>Network Location</strong>:*</td>
</tr>
</tbody>
</table>

**Step 4**
Enter the SRST reference.

**Step 5**
Click **Update** to save the device pool information in the database.
Configuring CAPF on Cisco Unified Communications Manager

The Certificate Authority Proxy Function (CAPF) process allows supported devices, such as Cisco Unified IP Phones to request LSC certificates from the CAPF service on Cisco Unified Communications Manager. The CAPF utility generates a key pair and certificate that are specific for CAPF, and the utility copies this certificate to all Cisco Unified Communications Manager servers in the cluster.

For complete instructions on configuring CAPF in Cisco Unified Communications Manager, see the Cisco IP Phone Authentication and Encryption for Cisco Communications Manager documentation.

Enabling SRST Mode on the Secure Cisco Unified SRST Router

To configure secure SRST on the router to support the Cisco Unified IP Phone functions, use the following commands beginning in global configuration mode.

**SUMMARY STEPS**

1. call-manager-fallback
2. secondary-dialtone *digit-string*
3. transfer-system \{blind|full-blind|full-consult|local-consult\}
4. ip source-address *ip-address [port port]*
5. max-phones *max-phones*
6. max-dn *max-directory-numbers*
7. transfer-pattern *transfer-pattern*
8. exit
### How to Configure Secure Unified SRST

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> secondary-dialtone digit-string</td>
<td>Activates a secondary dial tone when a digit string is dialed.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# secondary-dialtone 9</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> transfer-system {blind</td>
<td>full-blind</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# transfer-system full-consult</td>
<td>- <strong>blind</strong>: Calls are transferred without consultation with a single phone line using the Cisco proprietary method.</td>
</tr>
<tr>
<td></td>
<td>- <strong>full-blind</strong>: Calls are transferred without consultation using H.450.2 standard methods.</td>
</tr>
<tr>
<td></td>
<td>- <strong>full-consult</strong>: Calls are transferred with consultation using a second phone line if available. The calls fallback to <strong>full-blind</strong> if the second line is unavailable.</td>
</tr>
<tr>
<td></td>
<td>- <strong>local-consult</strong>: Calls are transferred with local consultation using a second phone line if available. The calls fallback to <strong>blind</strong> for nonlocal consultation or nonlocal transfer target.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip source-address ip-address [port port]</td>
<td>Enables the router to receive messages from the Cisco IP Phones through the specified IP addresses and provides for strict IP address verification. The default port number is 2000.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> max-ephones max-phones</td>
<td>Configures the maximum number of Cisco IP phones that can be supported by the router. The maximum number is platform dependent. The default is 0. See the “Platform and Memory Support” section on page 25 for further details.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# max-ephones 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> max-dn max-directory-numbers</td>
<td>Sets the maximum number of directory numbers (DNs) or virtual voice ports that can be supported by the router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# max-dn 30</td>
<td>- <strong>max-directory-numbers</strong>: Maximum number of directory numbers or virtual voice ports supported by the router. The maximum number is platform dependent. The default is 0. See the “Platform and Memory Support” section on page 25 for further details.</td>
</tr>
</tbody>
</table>
Examples

The following example enables SRST mode on your router:

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# secondary-dialtone 9
Router(config-cm-fallback)# transfer-system full-consult
Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000
Router(config-cm-fallback)# max-ephones 15
Router(config-cm-fallback)# max-dn 30
Router(config-cm-fallback)# transfer-pattern ......
Router(config-cm-fallback)# exit
```

### Configuring Secure SCCP SRST

- **Prerequisites for Configuring Secure SCCP SRST**, page 279
- **Restrictions for Configuring Secure SCCP SRST**, page 279
- **Verifying Phone Status and Registrations**, page 280 (required)
- **Configuration Examples for Secure SCCP SRST**, page 287

#### Prerequisites for Configuring Secure SCCP SRST

- Cisco Unified Communications Manager 4.1(2) or later must be installed and must support security mode (authenticate and encryption mode).
- Unified SRST 12.3 or later releases for Secure SCCP support on Cisco 4000 Series Integrated Services Routers and Cisco Analog Voice Gateways mentioned in the section Secure SCCP SRST for Analog Voice Gateways, page 243. The configuration and behavior of Secure SCCP SRST fallback aligns with the existing support offered on Cisco Integrated Services Router Generation 2, unless specified otherwise.

#### Restrictions for Configuring Secure SCCP SRST

Not Supported in Secure SCCP SRST Mode (For Unified SRST 12.2 and prior releases)
- Cisco Unified Communications Manager versions before 4.1(2).
- Secure MOH; MOH stays active, but reverts to non-secure.
- Secure transcoding or conferencing.
How to Configure Secure Unified SRST

- Secure H.323 or SIP trunks.
- SIP phones interoperability.

Not Supported in Secure SCCP SRST Mode (For Unified SRST 12.3 and later releases)
For information on the restrictions for Secure SCCP SRST support introduced on Unified SRST 12.3, see the section SCCP SRST in Restrictions for Configuring Secure SRST, page 240.

Supported Calls in Secure SCCP SRST Mode (For Unified SRST 12.2 and prior releases)
Only voice calls are supported in secure SCCP SRST mode. Specifically, the following voice calls are supported:
- Basic call
- Call transfer (consult and blind)
- Call forward (busy, no-answer, all)
- Shared line (IP phones)
- Hold and resume

For information on the features supported on Unified SRST 12.3 and later releases, see Feature Support for Secure SRST (SCCP), Unified SRST Release 12.3, page 246.

Verifying Phone Status and Registrations

To verify or troubleshoot Cisco Unified IP Phone status and registration, complete the following steps beginning in privileged EXEC mode.

Note You can verify Phone Status and Registrations in secure SCCP SRST after you have performed the following steps:
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 264
- Adding an SRST Reference to Cisco Unified Communications Manager, page 274
- Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 277

SUMMARY STEPS

1. show ephone
2. show ephone offhook
3. show voice call status
4. debug ephone register
5. debug ephone state
## Chapter 9  Configuring Secure SRST for SCCP and SIP

### How to Configure Secure Unified SRST

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ephone</strong></td>
<td>Use this command to display registered Cisco Unified IP Phones and their capabilities. The <code>show ephone</code> command also displays authentication and encryption status when used for secure SCCP SRST. In this example, authentication and encryption status is active with a TLS connection.</td>
<td></td>
</tr>
</tbody>
</table>

*Example:*

Router# `show ephone`

```
ephone-1 Mac:1000.1111.0002 TCP socket:[5]
activeLine:0 REGISTERED in SCCP ver 5
  + Authentication + Encryption with TLS connection
mediaActive:0 offhook:0 ringing:0 reset:0
reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32626 7970 keepalive 390 max_line 8
button 1: dn 14 number 2002 CM Fallback CH1 IDLE

ephone-2 Mac:1000.1111.000B TCP socket:[12]
activeLine:0 REGISTERED in SCCP ver 5
  + Authentication + Encryption with TLS connection
mediaActive:0 offhook:0 ringing:0 reset:0
reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32718 7970 keepalive 390 max_line 8
button 1: dn 21 number 2011 CM Fallback CH1 IDLE

ephone-3 Mac:1000.1111.000A TCP socket:[16]
activeLine:0 REGISTERED in SCCP ver 5
  + Authentication + Encryption with TLS connection
mediaActive:0 offhook:0 ringing:0 reset:0
reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32862 7970 keepalive 390 max_line 8
button 1: dn 2 number 2010 CM Fallback CH1 IDLE
```

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ephone offhook</strong></td>
<td>Use this command to display Cisco IP Phone status and quality for all phones that are off hook. In this example, authentication and encryption status is active with a TLS connection, and there is an active secure call.</td>
<td></td>
</tr>
</tbody>
</table>

*Example:*

Router# `show ephone offhook`

```
ephone-1 Mac:1000.1111.0002 TCP socket:[5]
activeLine:1 REGISTERED in SCCP ver 5
  + Authentication + Encryption with TLS connection
mediaActive:1 offhook:1 ringing:0 reset:0
reset_sent:0 paging 0
IP:10.1.1.40 32626 7970 keepalive 391 max_line 8
button 1: dn 14 number 2002 CM Fallback CH1 CONNECTED
Active Secure Call on DN 14 chan 1 :2002 10.1.1.40 29632 to 10.1.1.40 25616 via 10.1.1.40
G711Ulaw64k 160 bytes no vad
Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0
Jitter 0 Latency 0 callingDn 22 calledDn -1

ephone-2 Mac:1000.1111.000B TCP socket:[12]
activeLine:1 REGISTERED in SCCP ver 5
  + Authentication + Encryption with TLS connection
mediaActive:1 offhook:1 ringing:0 reset:0
reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32718 7970 keepalive 391 max_line 8
```
## How to Configure Secure Unified SRST

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>button 1: dn 21 number 2011 CM Fallback CH1 CONNECTED Active Secure Call on DN 21 chan 1 :2011 10.1.1.40 16382 to 10.1.1.40 16382 via 10.1.1.40 G711Ulaw64k 160 bytes no vad Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0 Jitter 0 Latency 0 callingDn -1 calledDn 11</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 3**

`show voice call status`

#### Example:
```
CallID CID ccVdb Port DSP/Ch Called # Codec
Dial-peers
0x1164 2BFE 0x8619A460 50/0/35.0 2014 g711ulaw 20035/20027
0x1165 2BFE 0x86144B78 50/0/27.0 *2014 g711ulaw 20027/20035
0x1166 2C01 0x861043D8 50/0/21.0 2012 g711ulaw 20021/20011
0x1168 2C01 0x860984C4 50/0/11.0 *2012 g711ulaw 20011/20021
0x1167 2C04 0x8610EC7C 50/0/22.0 2002 g711ulaw 20022/20014
0x1169 2C04 0x860B8894 50/0/14.0 *2002 g711ulaw 20014/20022
0x116A 2C07 0x860A374C 50/0/12.0 2010 g711ulaw 20012/20002
0x116B 2C07 0x860A374C 50/0/10.0 2010 g711ulaw 20002/20002
0x116C 2C0A 0x86119520 50/0/23.0 2034 g711ulaw 20023/20020
0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw 20020/20023
0x116E 2C0D 0x860BDC20 50/0/10.0 2022 g711ulaw 20010/20008
0x116F 2C0D 0x86078AD8 50/0/8.0 *2022 g711ulaw 20008/20010
0x1170 2C10 0x861398F0 50/0/26.0 2016 g711ulaw 20026/20028
0x1171 2C10 0x8614F41C 50/0/28.0 *2016 g711ulaw 20028/20026
0x1172 2C13 0x86159CC0 50/0/29.0 2018 g711ulaw 20029/20004
0x1173 2C13 0x8604E848 50/0/4.0 *2018 g711ulaw 20004/20029
0x1174 2C16 0x8612F04C 50/0/25.0 2026 g711ulaw 20025/20030
0x1175 2C16 0x86164F48 50/0/30.0 2026 g711ulaw 20030/20025
0x1176 2C19 0x860D8C64 50/0/17.0 2032 g711ulaw 20017/20018
0x1177 2C19 0x860E4008 50/0/18.0 *2032 g711ulaw 20018/20017
0x1178 2C1C 0x860CE3C0 50/0/16.0 2004 g711ulaw 20016/20019
0x1179 2C1C 0x860E88AC 50/0/19.0 *2004 g711ulaw 20019/20016
0x117A 2C1F 0x86043F4A 50/0/3.0 2008 g711ulaw 20003/20024
0x117B 2C1F 0x861247A8 50/0/24.0 *2008 g711ulaw 20024/20003
0x117C 2C22 0x8608337C 50/0/9.0 2020 g711ulaw 20009/20031
0x117D 2C22 0x8616F7EC 50/0/31.0 *2020 g711ulaw 20031/20009
0x117E 2C25 0x86063990 50/0/6.0 2006 g711ulaw 20006/20001
```

**Purpose:**
Use this command to show the call status for all voice ports on the Cisco Unified SRST router. This command is not applicable for calls between two POTS dial peers.
## How to Configure Secure Unified SRST

### Step 4: debug ephone register

**Example:**

```
Router# debug ephone register
EPHONE registration debugging is enabled
(0 active)
*Jun 29 09:16:02.180: sin_family 2, sin_port 51617, in_addr 10.5.43.177
*Jun 29 09:16:02.180: skinny_socket_process: secure skinny sessions = 1
*Jun 29 09:16:02.180: add_skinny_secure_socket: pid =155, new_sock=0, ip address = 10.5.43.177
*Jun 29 09:16:02.180: skinny_secure_handshake: pid =155, sock=0, args->pid=155, ip address = 10.5.43.177
*Jun 29 09:16:02.184: Start TLS Handshake 0 10.5.43.177 51617
*Jun 29 09:16:02.184: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:03.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:04.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:05.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:06.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:07.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:08.188: CRYPTO_PKI_OPSSL - Verifying 1 Certs
*Jun 29 09:16:08.212: TLS Handshake completes
```

Use this command to debug the process of Cisco IP phone registration.

### Command or Action | Purpose
--- | ---
0x117F 2C25 0x85C6BB6C 50/0/1.0 *2006 g711ulaw 20001/20006 |  | 20034/20034 | 0x1180 2C28 0x860ADFF0 50/0/13.0 2029 g711ulaw 20034/20034 | 0x1181 2C28 0x8618FBBC 50/0/34.0 *2029 g711ulaw 20005/20005 | 0x1182 2C28 0x860C3B1C 50/0/15.0 2036 g711ulaw 20005/20005 | 0x1183 2C2B 0x860590EC 50/0/5.0 *2036 g711ulaw 20005/20005 | 0x1184 2C2B 0x8617A090 50/0/32.0 2024 g711ulaw 20032/20007 | 0x1185 2C2E 0x8606E234 50/0/7.0 *2024 g711ulaw 20007/20006 | 0x1186 2C31 0x861A56E8 50/0/36.0 2030 g711ulaw 20036/20033 | 0x1187 2C31 0x86185318 50/0/33.0 *2030 g711ulaw 20033/20036 | 18 active calls found
How to Configure Secure Unified SRST

Step 5

**Example:**

Router# debug ephone state
*Jan 11 18:33:11.747:ephone-2[2]:---SkinnySyncPhoneDnOverlay s is onhook
*Jan 11 18:33:11.747:ephone-2[2]:SIEZE on activeLine 0
*Jan 11 18:33:11.747:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsoffHook
*Jan 11 18:33:11.747:ephone-2[2]:Check Plar Number
*Jan 11 18:33:11.751:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:11.751:dn_tone_control DN=2 chan 1
*Jan 11 18:33:11.751:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:11.751:dn_tone_control DN=2 chan 1
tonetype=33:DtInsideDialTone onoff=1 pid=232
*Jan 11 18:33:15.031:dn_tone_control DN=2 chan 1
tonetype=0:DtSilence onoff=0 pid=232
call DN 2 chan 1 to DN 4 chan 1 instance 1
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1
DN 2(-1) chan 1 ref 6 TpsProceed
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1
DN 2(-1) chan 1 ref 6 TpRingOut
*Jan 11 18:33:16.039:ephone-2[2]:callingNumber 6000
*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line
1 ref 6 call state 1 called 6001 calling 6000
origcalled
*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line
1 ref 6 called 6001 calling 6000 origcalled 6001
calltype 2
*Jan 11 18:33:16.039:ephone-2[2]:Call Info for chan 1
Name 6001
*Jan 11 18:33:16.039:ephone-2[2]:6000 calling
*Jan 11 18:33:16.047:ephone-3[3]:SetCallState line 1
DN 4(4) chan 1 ref 7 TpRingIn
*Jan 11 18:33:16.047:ephone-3[3]:callingNumber 6000
*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line
1 ref 7 call state 7 called 6001 calling 6000
origcalled
*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line
1 ref 7 called 6001 calling 6000 origcalled 6001
calltype 1
*Jan 11 18:33:16.047:ephone-3[3]:Call Info for chan 1
*Jan 11 18:33:16.047:ephone-3[3]:Original Called
Name 6001
*Jan 11 18:33:16.047:ephone-3[3]:6000 calling
*Jan 11 18:33:16.047:ephone-3[3]:6001

Use this command to review call setup between two secure Cisco Unified IP Phones. The debug ephone state trace shows the generation and distribution of encryption and decryption keys between the two phones.
### How to Configure Secure Unified SRST

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 11 18:33:16.051:dn_tone_control DN=2 chan 1 tonetype=36:DtAlertingTone onoff=1 pid=232</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:OFFHOOK</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:---SkinnySyncPhoneDnOverlay is onhook</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:Ringer Off</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:ANSWER call</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsOffHook</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsConnected</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:Answer Incoming call from ephone-(2) DN 2 chan 1</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsConnected</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:callingNumber 6000</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:callingParty 6000</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 call state 4 called 6001 calling 6000 origcalled</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000 origcalled 601 calltype 1</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Call Info for chan 1</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Original Called Name 6001</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:6000 calling</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:6001</td>
<td></td>
</tr>
<tr>
<td>Ephone 2 generates a security key.</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-2[2]:OpenReceive DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Security Key Generation</td>
<td></td>
</tr>
<tr>
<td>Ephone 3 generates its security key.</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:OpenReceive DN 4 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:21.087:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:21.095:ephone-2[2]:OpenReceiveChannelAck::IP 1.1.1.8, port=25552, dn_index=2, dn=2, chan=1</td>
<td></td>
</tr>
</tbody>
</table>
### How to Configure Secure Unified SRST

**Configuration Examples for Secure SCCP SRST**

This section provides the following configuration examples:

- Secure SCCP SRST: Example, page 287
- Control Plane Policing: Example, page 292

**Note**

IP addresses and hostnames in examples are fictitious.

### Secure SCCP SRST: Example

This section provides a configuration example to match the identified configuration tasks in the previous sections. This example does not include using a third-party CA; it assumes the use of the Cisco IOS certificate server to generate your certificates.

```
Router# show running-config
.
! Define Unified Communications Manager.
ccm-manager fallback-mgcp
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.1.1.13
ccm-manager config
```

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Jan 11 18:33:21.095:ephone-3[3]:StartMedia 1.1.1.8 port=25552</td>
<td><em>Define Unified Communications Manager.</em></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.095:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160</td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.095:ephone-3[3]:Send Encryption Key</td>
<td></td>
</tr>
<tr>
<td><em>Ephone 3 sends its encryption key.</em></td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.347:ephone-3[3]:OpenReceiveChannelAck:IP 1.1.1.9, port=17520, dn_index=4, dn=4, chan=1</td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.347:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160</td>
<td></td>
</tr>
<tr>
<td><em>Ephone 2 sends its encryption key.</em></td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.851:callingNumber 6000</td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.851:Call Info DN 2 line 1 ref 6 call state 4 called 6001 calling 6000 origcalled</td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.851:Call Info DN 2 line 1 ref 6 called 6001 calling 6000 origcalled 6001 calltype 2</td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.851:Call Info for chan 1</td>
<td></td>
</tr>
<tr>
<td>*Jan 11 18:33:21.851:Original Called Name 6001</td>
<td></td>
</tr>
</tbody>
</table>
How to Configure Secure Unified SRST

! Define root CA.
crypto pki server srstcaserver
database level complete
database url nvram
issuer-name CN=srstcaserver
!
crypto pki trustpoint srstca
  enrollment url http://10.1.1.22:80
  revocation-check none
!
crypto pki trustpoint srstcaserver
  revocation-check none
  rsakeypair srstcaserver
!
! Define CTL/7970 trustpoint.
crypto pki trustpoint 7970
  enrollment terminal
  revocation-check none
!
crypto pki trustpoint PEM
  enrollment terminal
  revocation-check none
!
! Define CAPF/7960 trustpoint.
crypto pki trustpoint 7960
  enrollment terminal
  revocation-check none
!
! SRST router device certificate.
crypto pki certificate chain srstca
certificate 02
  3082010D 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050003
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30340304
  31123139 35323233 5A170D30 35303431 32311393 32323335 30341312 300D0603
  55040513 08440102 39457379 43301F06 092A8648 8670F7D0 09021612 6A61736F
  32363931 2E636973 646F6263 66F6D0305 300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 2286FED6 6CA70C19
  C98F9F68 AE9D1F9B D4BB7A67 F1251174 193BB1A3 12946123 E5C1CCD7 A2B6155
  FA2ED743 3FBF8902 03100101 A330302E 300B0603 551D0F04 04030205 A0310F06
  03551D23 04183016 8014F829 CB97AD60 18D05467 FC293963 C2470F91 9FBD0F0D
  06092A86 4886F70D 01010405 00038181 07EB48E C6B9E1B3 D1EA17A5 D7F0D565
  CB8417B7 1151BD78 B3E39763 59EC650E 49371F6D 99CB2D67 E88ADF9D 9E4A5F2F
  PB2B1B80 34AF6F64 11239473 414788FC A868E6A1 ACS18B0B 8657CE8B ED2DB8EE
  B586F6E7 00C358D4 EFDDD84 3F4231A1 C2D313D3 1EE43BE6 6CE289EE 8BC2752
  C3AF4A66 BD007348 D013000A EA3C206D C
quit
certificate ca 01
  30820107 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050003
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30340304
  31123139 34353136 5A170D30 37303431 32311393 3531365A 30173115 30130603
  55040513 08440102 39457379 43301F06 092A8648 8670F7D0 09021612 6A61736F
  32363931 2E636973 646F6263 66F6D0305 300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 2286FED6 6CA70C19
  C98F9F68 AE9D1F9B D4BB7A67 F1251174 193BB1A3 12946123 E5C1CCD7 A2B6155
  FA2ED743 3FBF8902 03100101 A330302E 300B0603 551D0F04 04030205 A0310F06
  03551D23 04183016 8014F829 CB97AD60 18D05467 FC293963 C2470F91 9FBD0F0D
  06092A86 4886F70D 01010405 00038181 07EB48E C6B9E1B3 D1EA17A5 D7F0D565
  CB8417B7 1151BD78 B3E39763 59EC650E 49371F6D 99CB2D67 E88ADF9D 9E4A5F2F
  PB2B1B80 34AF6F64 11239473 414788FC A868E6A1 ACS18B0B 8657CE8B ED2DB8EE
  B586F6E7 00C358D4 EFDDD84 3F4231A1 C2D313D3 1EE43BE6 6CE289EE 8BC2752
  C3AF4A66 BD007348 D013000A EA3C206D C
quit
Chapter 9      Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

00382B01 0D003082 01080282 010100AC 55BBED18 DE9B8709 FFBCB8F2D 509ABB3A
21C1677F DE7F4B0 96694B7 800C196A 463DA516 54A28F47 5D903B5F 104AD5D4
A981B389 2FC7AC9 59262B8 1C143038 5345BB2E 273FA7A6 48660573 CE5C998D
55DE79AA 5A5CCEE1 037D069B AC816409 C6211F0B 3BBF09CF 0BBB2D4 AC362F67
0FD145F1 620852B3 1F07E2F1 AA74F150 367632ED A289E374 AF0C5B78 CE7DFB9F
2C8EBB6E 56ECPF47C 99D6DC04 4747C6CF 36E58A3B 6BCB24D7 6BCB84C2 7F61D326
BE7CB4AE 7CD6579 91E1384A 8153B750 5527E865 423EB285 CB575453 5AA96093
58B6A2E2 AA3EF081 C7068EC1 DD1E8DDB 536F0F6D E2E0486B 109F1316 78C696A3
CBFAABCC 7904304D C189FB10 913ACB02 0103A381 C30081C0 300B0603 551FD0F4
04032001 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
14E917F1 82C71FCF ACA91B6E F4A9269C 70AE05A0 9A306F06 03551D1F 04683066
3064A062 A60862D 68747470 3A2F2F63 61702D72 7402D630 50312F43 65772445
6E7F26F6 6C2F4341 502D2554 502D3030 312E6372 6C862F66 6966536A 2F2F52C5
6361702D 7274702D 3030315C 43667274 456E726F 6C6C5C43 41502D52 54502D30
3012E631 T6C3101 06092806 01040182 37150104 03020100 300D0609 2A86486B
F70D1010 05050003 82010100 AB64FDEB F6C032DC 6F0E01E0 5FE165FA 0D574AB5
02ACDCA3 C7B8ED18 79600100 AF9269C 01040182 37150104 03020100 300D0609
2A86486B quit
crypto pki certificate chain 7960
certificate ca F301
match address 116
!
!
interface FastEthernet0/0
ip address 10.1.1.22 255.255.255.0
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
! Define traffic to be encrypted by IPSec.
access-list 116 permit ip host 10.1.1.22 host 10.1.1.13
!
control-plane
!
!
call application alternate DEFAULT
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/0/2
!
voice-port 1/0/3
!
voice-port 1/1/0
timing hookflash-out 50
!
voice-port 1/1/1
!
voice-port 1/1/2
!
voice-port 1/1/3
!
! Enable MGCP voice protocol.
mgcp
mgcp call-agent 10.1.1.13 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
!
dial-peer voice 81235 pots
  application mgcpapp
  destination-pattern 81235
  port 1/1/0
  forward-digits all
!
dial-peer voice 81234 pots
  application mgcpapp
  destination-pattern 81234
  port 1/0/0
!
dial-peer voice 999100 pots
  application mgcpapp
  port 1/0/0
!
dial-peer voice 999110 pots
  application mgcpapp
  port 1/1/0
!

! Enable credentials service on the gateway.
credentials
  ip source-address 10.1.1.22 port 2445
  trustpoint srstca
!
! Enable SRST mode.
call-manager-fallback
  transport-tcp-tls
  secondary-dialtone 9
  transfer-system full-consult
  ip source-address 10.1.1.22 port 2000
  max-ephones 15
  max-dn 30
  transfer-pattern ......

Control Plane Policing: Example

This section provides a configuration example for the security best practice of protecting the credentials service port using control plane policing. Control plane policing protects the gateway and maintains packet forwarding and protocol states despite a heavy traffic load. For more information on control planes, see the Control Plane Policing documentation.

Router# show running-config

! Allow trusted host traffic.
access-list 140 deny tcp host 10.1.1.11 any eq 2445

! Rate-limit all other traffic.
access-list 140 permit tcp any any eq 2445
access-list 140 deny ip any any

! Define class-map "sccp-class."
class-map match-all sccp-class
match access-group 140

policy-map control-plane-policy
class sccp-class
police 8000 1500 1500 conform-action drop exceed-action drop
! Define aggregate control plane service for the active Route Processor.
control-plane
service-policy input control-plane-policy

Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST

Cisco Unified Survivable Remote Site Telephony (Cisco SRST) provides secure call signaling and Secure Real-time Transport Protocol (SRTP) for media encryption to establish a secure, encrypted connection between Cisco Unified IP Phones and gateway devices.

- Prerequisites for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 293
- Restrictions for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 293
- Information About Cisco Unified SIP SRST Support of Secure SIP Signaling and SRTP Media, page 294
- Configuring Cisco Unified Communications Manager, page 294
- Configuring Phones, page 295
- Configuring SIP options for Secure SIP SRST, page 296
- Configuring SIP SRST Security Policy, page 297 (optional)
- Configuring SIP User Agent for Secure SIP SRST, page 298 (optional)
- Verifying the Configuration, page 300
- Configuration Example for Cisco Unified SIP SRST, page 302

Prerequisites for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST

- Cisco IOS Release 15.0(1)XA and later releases.
- Cisco Unified IP Phone firmware release 8.5(3) or later.
- Complete the prerequisites and necessary tasks found in Prerequisites for Configuring SIP SRST Features Using Back-to-Back User Agent Mode.
- Prepare the Cisco Unified SIP SRST device to use certificates as documented in Preparing the Cisco Unified SRST Router for Secure Communication.

Restrictions for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST

SIP phones may be configured on the Cisco Unified CM with an authenticated device security mode. The Cisco Unified CM ensures integrity and authentication for the phone using a TLS connection with NULL-SHA cipher for signaling. If an authenticated SIP phone fails over to the Cisco Unified SRST device, it will register using TCP instead of TLS/TCP, thus disabling the authenticated mode until the phone fails back to the Cisco Unified CM.

- By default, non-secure TCP SIP phones are permitted to register to the SRST device on failover from the primary call control. Support for TCP SIP phones requires the secure SRST configuration described in this section even if no encrypted phones are deployed. Without the secure SIP SRST configuration, TCP phones will register to the SRST device using UDP for signaling transport.
Information About Cisco Unified SIP SRST Support of Secure SIP Signaling and SRTP Media

Beginning with Cisco IP Phone firmware 8.5(3) and Cisco IOS Release 15.0(1)XA, Cisco SRST supports SIP signaling over UDP, TCP, and TLS connections, providing both RTP and SRTP media connections based on the security settings of the IP phone.

Cisco SRST SIP-to-SIP and SIP-to-PSTN support includes the following features:

- Basic calling
- Hold/resume
- Conference
- Transfer
- Blind transfer
- Call forward

Cisco SRST SIP-to-other (including SIP-to-SCCP) support includes basic calling, although other features may work.

Configuring Cisco Unified Communications Manager

Like SCCP-controlled devices, SIP-controlled devices will use the SRST Reference profile that is listed in their assigned Device Pool. The SRST Reference profile must have the "Is SRST Secure" check box selected if SIP/TLS communication is desired in the event of a WAN failure.

**Note**

All Cisco Unified IP Phones must have their firmware updated to version 8.5(3) or later. Devices with firmware earlier than 8.5(3) will need to have a separate Device Pool and SRST Reference profile created without the "Is SRST Secure" option selected; SIP-controlled devices in this Device Pool will use SIP over UDP to attempt to register to the SRST router.

In Cisco Unified CM Administration, under **System > SRST**:

- For the secure SRST profile, Is SRST Secure? must be checked. The SIP port must be 5061.
- For the non-secure SRST profile, the Is SRST Secure? checkbox should NOT be checked and the SIP port should be 5060.

Under **Device > Phone**:

- Secure phones must belong to the pool that uses the secure SRST profile.
- Non-secure phones must belong to the pool that uses the non-secure SRST profile.

**Note**

SIP phones will use the transport method assigned to them by their Phone Security Profile.
Configuring Phones

This section specifies that SRTP should be used to enable secure calls and allows non-secure calls to "fallback" to using RTP media.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. srtp
5. allow-connections sip to h323
6. allow-connections sip to sip
7. end
## How to Configure Secure Unified SRST

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** voice service voip | Enters voice service configuration mode. |
| **Step 4** srtp | Specifies that SRTP be used to enable secure calls. |
| **Step 5** allow-connections sip to h323 | (Optional) Allows connections from SIP endpoints to H.323 endpoints. |
| **Step 6** allow-connections sip to sip | Allows connections from SIP endpoints to SIP endpoints. |
| **Step 7** end | Ends the current configuration session and returns to privileged EXEC mode. |

### Configuring SIP options for Secure SIP SRST

This section explains how to configure secure SIP SRTP.

### SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. url sip | sips
6. srtp negotiate cisco
### How to Configure Secure Unified SRST

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal |
| **Step 3** voice service voip | Enters voice service configuration mode. |
| **Example:** Router(config)# voice service voip |
| **Step 4** sip | Enters SIP configuration mode. |
| **Example:** Router(config-voi-serv)# sip |
| **Step 5** url sip | To configure secure mode, use the **sips** keyword to generate URLs in SIP secure (SIPS) format for VoIP calls.  
To configure device-default mode, use the **sip** keyword to generate URLs in SIP format for VoIP calls. |
| **Example:** Router(config-serv-sip)# url sips |
| **Step 6** srtp negotiate cisco | Enables a Cisco IOS SIP gateway to negotiate the sending and accepting of RTP profiles in response to SRTP offers. |
| **Example:** Router(config-serv-sip)# srtp negotiate cisco |
| **Step 7** end | Ends the current configuration session and returns to privileged EXEC mode. |
| **Example:** Router(config-serv-sip)# end |

### Configuring SIP SRST Security Policy

This section explains how to secure mode to block registration of non-secure phones to the SRST router.

**SUMMARY STEPS**

1. voice register global
2. security-policy secure | no security-policy
3. end
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> voice register global</td>
<td>Enters voice register global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice register global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> security-policy secure</td>
<td>Configures SIP registration security policy so that only SIP/TLS/TCP connections are allowed. For device-default mode, use the no security-policy command. Device-default mode allows non-secure devices to register without using TLS.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-register-global)# security-policy secure</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>We recommend that security-policy secure is configured for the Secure SRST feature, so that non-secure phones do not fall back on Secure SRST.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-register-global)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring SIP User Agent for Secure SIP SRST

This section explains how the strict-cipher limits the allowed encryption algorithms.

### SUMMARY STEPS

1. sip-ua
2. registrar ipv4:destination-address expires seconds
3. xfer target dial-peer
4. crypto signaling default trustpoint string [strict-cipher]
5. crypto signaling remote-addr {ip address |subnet mask} trustpoint trustpoint-name
6. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**  
  Router(config)# sip-ua | |
| **Step 2** registrar ipv4:destination-address expires seconds | Enables the gateway to register E.164 telephone numbers with primary and secondary external SIP registrars. destination-address is the IP address of the primary SIP registrar server. |
| **Example:**  
  Router(config-sip-ua)# registrar ipv4:192.168.2.10 expires 3600 | |
| **Step 3** xfer target dial-peer | Specifies that SRST should use the dial-peer as a transfer target instead of what is in the message body. |
| **Example:**  
  Router(config-sip-ua)# xfer target dial-peer | |
| **Step 4** crypto signaling default trustpoint string [strict-cipher] | Identifies the trustpoint string keyword and argument used during the TLS handshake. The trustpoint string keyword and argument refer to the gateway’s certificate generated as part of the enrollment process, using Cisco IOS public-key infrastructure (PKI) commands. The strict-cipher keyword restricts support to TLS RSA encryption with the Advanced Encryption Standard-128 (AES-128) cipher-block-chaining (CBC) Secure Hash Algorithm (SHA) (TLS_RSA_WITH_AES_128_CBC_SHA) cipher suite. To configure device-default mode, omit the strict-cipher keyword. |
| **Example:**  
  Router(config-sip-ua)# crypto signaling default trustpoint 3745-SRST strict-cipher | |
| **Step 5** crypto signaling remote-addr {ip address |subnet mask} trustpoint trustpoint-name | The trustpoint label refers to the CUBE’s certificate that is generated with the Cisco IOS PKI commands as part of the enrollment process. Keywords and arguments are as follows:  
  - remote-addr ip address—Associates an IP address to a trustpoint.  
  - trustpoint trustpoint-name—Refers to the SIP gateways certificate generated as part of the enrollment process using Cisco IOS PKI commands |
| **Example:**  
  Router(config-sip-ua)# crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk1 | |
| **Step 6** end | Ends the current configuration session and returns to privileged EXEC mode. |
| **Example:**  
  Router(config-sip-ua)# end | |

#### Multiple Trustpoints

Use the default trustpoint configuration under sip-ua config mode for phones registering to Unified SRST in secure mode. For example, srstca is the default trustpoint for Secure SRST. This default signaling trustpoint is used for all SIP TLS interactions from SIP phones to Unified Secure SRST router.
In a deployment scenario with multiple trustpoints, communication with a service provider over a secure trunk with certificate issued by CA is achieved using the CLI command `crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk1` under `sip-ua config` mode.

**Example**

The following example shows a sample configuration of multiple trustpoints for a Unified SRST deployment. In this example, the `srst-trunk1` trustpoint points to the network with IP address 8.39.0.0, and `srst-trunk2` trustpoint points to the network with IP address 8.41.20.20.

```
sip-ua
crypto signaling remote-addr 8.39.0.0 255.255.0.0 trustpoint srst-trunk1
crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk2
crypto signaling default trustpoint srcestr
```

**Verifying the Configuration**

The following examples show a sample configuration displayed by the `show sip-ua status registrar` command and the `show voice register global` command.

**show sip-ua status registrar**

```
Router# show sip-ua status registrar
                   Line destination expires(sec) contact                  
                    transport call-id                              
                       peer                                      
  ============ =============== ============ =============== ===========
3029991         192.168.2.108    388           192.168.2.108
TLS            00120014-4ae40064-f1a3e9fe-8d3010720192.168.2.1
            40004
3029993         192.168.2.103    382           192.168.2.103
TCP             001bd433-1c840052-655cd596-4e992eed0192.168.2.1
            40011
3029992         192.168.2.106    406           192.168.2.106
UDP             001d452c-dbbab0056-0481d321-1f3f8488d0192.168.2.1
            40001
3029993         192.168.2.106    406           192.168.2.106
UDP             001d452c-dbbab0057-1c69b699-d8dc66250192.168.2.1
            40003
3029992         192.168.2.107    414           192.168.2.107
TLS             001e7a25-50c9002c-48ef7663-50c71794d0192.168.2.1
            40005
```

**show voice register global**

```
Router# show voice register global
CONFIG [Version=8.0]
========================
Version 8.0
Mode is srst
Max-pool is 50
Max-dn is 100
Outbound-proxy is enabled and will use global configured value
Security Policy: DEVICE-DEFAULT
timeout interdigit 10
network-locale[0] US (This is the default network locale for this box)
network-locale[1] US
user-locale[0] US (This is the default user locale for this box)
```
user-locale[1] US
user-locale[2] US
user-locale[3] US
user-locale[4] US
Router#
Configuration Example for Cisco Unified SIP SRST

Current configuration: 15343 bytes

! Last configuration change at 05:34:06 UTC Tue Jun 13 2017
! NVRAM config last updated at 11:57:03 UTC Thu Jun 8 2017

! version 16.7
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core

hostname router

boot-start-marker
boot-end-marker

vrf definition Mgmt-intf

! address-family ipv4
  exit-address-family

! address-family ipv6
  exit-address-family

! card type command needed for slot/bay 0/3
no logging queue-limit
logging buffered 2000000
no logging rate-limit
no logging console
enable password xxxx

no aaa new-model

! subscriber templating

! multilink bundle-name authenticated

crypto pki server SRST-CA-2
  database level complete
  no database archive
  grant auto

! crypto pki trustpoint TRUSTPT-SRST-CA-2
  enrollment url http://10.0.0.1:80
  serial-number
  revocation-check none
  rsakeypair srstcak 2048
  rsakeypair SRST-CA-2

! crypto pki trustpoint SRST-CA-2
  revocation-check crl
  rsakeypair SRST-CA-2

! crypto pki trustpoint Cisco_Manufacturing_CA
  enrollment terminal
  revocation-check none

! crypto pki trustpoint CAPF-3a66269a
  enrollment terminal
  revocation-check none
Chapter 9  Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

crypto pki trustpoint Cisco_Root_CA_2048
  enrollment terminal
  revocation-check none

crypto pki certificate chain TRUSTPT-SRST-CA-2
  certificate ca 01

quit

certificate ca 01

crypto pki certificate chain SRST-CA-3
  certificate ca 01

quit

crypto pki certificate chain SRST-CA-2
  certificate ca 01

quit


cisco pki trustpoint Cisco_Root_CA_2048
  enrollment terminal
  revocation-check none


cisco pki certificate chain TRUSTPT-SRST-CA-2
  certificate ca 01

quit

certificate ca 01

crypto pki certificate chain SRST-CA-3
  certificate ca 01

quit

crypto pki certificate chain SRST-CA-2
  certificate ca 01

quit


cisco pki trustpoint Cisco_Root_CA_2048
  enrollment terminal
  revocation-check none


cisco pki certificate chain TRUSTPT-SRST-CA-2
  certificate ca 01

quit

certificate ca 01

crypto pki certificate chain SRST-CA-3
  certificate ca 01

quit

crypto pki certificate chain SRST-CA-2
  certificate ca 01

quit

Cisco Unified SCCP and SIP SRST System Administrator Guide 9-30
cisco unified SCCP and SIP SRST system administrator guide
How to Configure Secure Unified SRST

0603551D 0F040403 0202A410 13060355 1D25040C 300A0608 2B060105 05070301 101D0603 551D0E04 16041477 71E5C5D5 1A431511 7E8C8462 6E65E570 7C551930 12060355 1D130101 FF040830 060101FF 02010030 0D06092A 864886F7 0D010105 05000382 0101009D 9D8484A3 41A97C77 0CB753CA 4E445062 EF547CD3 75171CE8 E0C6484B B6F643C8 198156B0 0570C04A 71601E43 0B601EFE A3CEB119 E10B35

quit
!

voice service voip
no ip address trusted authenticate
media bulk-stats
media disable-detailed-stats
allow-connections sip to sip srtp
no supplementary-service sip refer
no supplementary-service media-remotegate no supplementary-service media handle-replaces
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none sip

registrar server expires max 120 min 60
!
voice register global
default mode
no allow-hash-in-dn
security-policy secure
max-dn 50
max-pool 40
voice register pool 1
  id network 10.0.0.1 mask 255.255.0.0
dtmf-relay rtp-nte
codec g711ulaw
!
voice hunt-group 1 sequential
  final 99898
  list 1008,2005
  timeout 5
  pilot 1111
!
voice-card 0/1
  no watchdog
!
voice-card 0/2
  no watchdog
!
voice-card 0/3
  no watchdog
!
voice-card 1/0
  no watchdog
!
license udi pid ISR4451-X/K9 sn FOC1743565L
license accept end user agreement
license boot level uck9
license boot level securityk9
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
  mode none
!
interface GigabitEthernet0/0/0
  ip address 10.0.0.1 255.255.0.0
  negotiation auto
!
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/2
  ip address 10.0.0.1 255.0.0.0
  negotiation auto
!
interface GigabitEthernet0/0/3
  no ip address
  negotiation auto
!
interface Service-Engine0/1/0
  shutdown
!
interface Service-Engine0/2/0
  shutdown
!
interface Service-Engine0/3/0
!
interface Service-Engine1/0/0
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
negociation auto
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
control-plane
!
voice-port 0/1/0
!
voice-port 0/1/1
!
voice-port 0/2/0
!
voice-port 0/2/1
!
voice-port 0/2/2
!
voice-port 0/2/3
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-mdp-force disable
!
mgcp profile default
!
sip-ua

crypto signaling default trustpoint TRUSTPT-SRST-CA-2
!
!
credentials
ip source-address 10.0.0.1 port 2445
trustpoint TRUSTPT-SRST-CA-2
!
!
call-manager-fallback
max-conferences 8 gain -6
transfer-system full-consult
max-ephones 50
max-dn 50
call-park system application
fac standard
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 0 0
password xxxx
no login
length 0
transport preferred none
transport input telnet ssh
Additional References

The following sections provide references related to this feature.
### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS voice configuration</td>
<td>• Cisco IOS Voice Configuration Library</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>• Cisco Unified Communications Manager Documentation Guide for Release 8.0(2)</td>
</tr>
<tr>
<td>Documentation Guide for Release 8.0(2)</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified SRST configuration</td>
<td>• Cisco Unified SRST and SIP SRST Command Reference</td>
</tr>
<tr>
<td>Cisco Unified SRST</td>
<td>• Cisco Unified SRST 8.0 Supported Firmware, Platforms, Memory, and Voice Products</td>
</tr>
<tr>
<td>Cisco Unified Communications Operating System</td>
<td>• Security</td>
</tr>
<tr>
<td>Administration Guide, Release 6.1(1)</td>
<td></td>
</tr>
<tr>
<td>Configuring a Secure Survivable Remote Site</td>
<td>• Configuring a Secure Survivable Remote Site Telephony (SRST) Reference</td>
</tr>
<tr>
<td>Telephony (SRST) Reference</td>
<td></td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>---</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>---</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>

Command Reference


- **security-policy**
- **show voice register global**
- **show voice register all**
Feature Information for Secure SCCP and SIP SRST

Table 9-4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure SIP Call Signaling and SRTP Media with Cisco SRST</td>
<td>15.0(1)XA</td>
<td>Adds Session Initiation Protocol/Transport Layer Security/Transmission Control Protocol (SIP/TLS/TCP) support for secure call signaling and Secure Real-time Transport Protocol (SRTP) for media encryption to establish a secure, encrypted connection between Cisco Unified IP Phones and a failover device using Cisco Unified Survivable Remote Site Telephony (Cisco SRST). The following commands were introduced or modified: security-policy, show voice register global, show voice register all</td>
</tr>
</tbody>
</table>

Note
Table 9-4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Where to Go Next

If you require voicemail, see the voice-mail configuration instructions in the “Integrating Voicemail with Cisco Unified SRST” section on page 331.

For additional information, see the “Additional References” section on page 29 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.