Configuring Secure SRST for SCCP and SIP

The Secure SRST adds security functionality to the Unified SRST.

Contents

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

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 248.
- 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 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 236.

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).
- It is mandatory to configure **security-policy secure** under **voice register global** configuration mode. Non-Secure endpoints cannot register when security-policy secure is configured. As such, mixed deployments of secure and non-secure endpoints is not possible.

Information About Configuring Secure SRST

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 238.

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 235.

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
- 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 270.

- 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

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)*.

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:

```
Router(config-cm-fallback)#transport-tcp-tls ?
  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 in tact, 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
```

Certificates Operation on Secure SRST

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 299 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 IP Phone 7940	Cisco Unified IP Phone 7960	Cisco Unified IP Phone 7970
The phone receives locally significant certificate (LSC) from Certificate Authority Proxy Function (CAPF) in Distinguished Encoding Rules (DER) format. • 59fe77ccd.0 The filename may change based on the CAPF certificate subject name and the CAPF certificate issuer. If Cisco Unified Communications Manager is using a third-party certificate provider, there can be multiple .0 files (from two to ten). Each .0 certificate file must be imported individually during the configuration. Manual enrollment supported only.	The phone receives locally significant certificate (LSC) from Certificate Authority Proxy Function (CAPF) in Distinguished Encoding Rules (DER) format. • 59fe77ccd.0 The filename may change based on the CAPF certificate subject name and the CAPF certificate issuer. If Cisco Unified Communications Manager is using a third-party certificate provider, there can be multiple .0 files (from two to ten). Each .0 certificate file must be imported individually during the configuration. Manual enrollment supported only.	The phone contains a manufacturing installed certificate (MIC) used for device authentication. If the Cisco 7970 implements MIC, two public certificate files are needed: • CiscoCA.pem (Cisco Root CA, used to authenticate the certificate.) **Note** The name of the manufacturing certificate can vary depending on your configuration. • a69d2e04.0, in Privacy Enhanced Mail (PEM) format If Cisco Unified Communications Manager is using a third-party certificate provider, there can be multiple .0 files (from two to ten). Each .0 certificate file must be imported individually during the configuration. Manual enrollment supported only.

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 248
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 255
- Configuring SRST Fallback on Cisco Unified Communications Manager, page 266

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 265.

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 257.

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

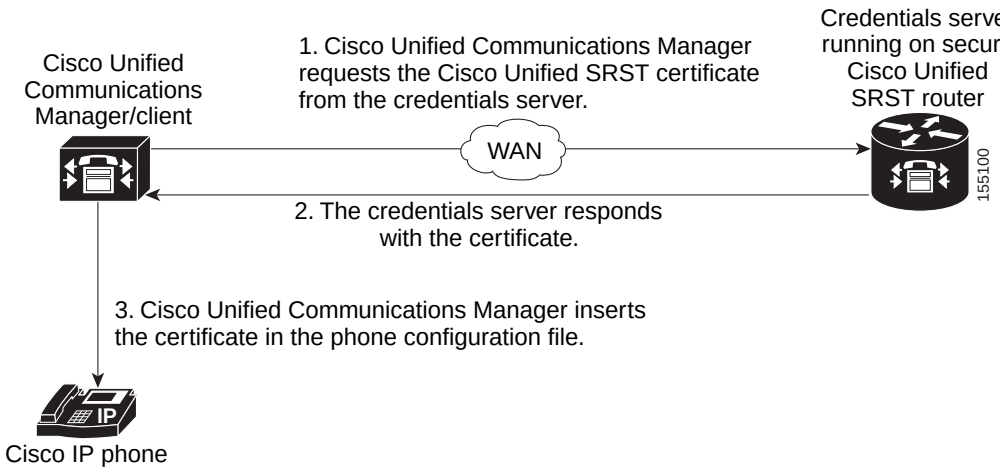


Table 9-2 Establishing Secure SRST

Mode	Process	Description or Detail
Regular Mode	The Cisco Unified IP Phone configures DHCP and gets the TFTP server address.	—
	The Cisco Unified IP Phone retrieves a CTL file from the TFTP server.	The CTL file contains the certificates that the phone should trust.
	The Cisco IP Phone opens a Transport Layer Security (TLS) protocol channel and registers to Cisco Unified Communications Manager.	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.
	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.	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.

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.

Figure 9-2 Secure Cisco Unified SRST Authentication and Encryption

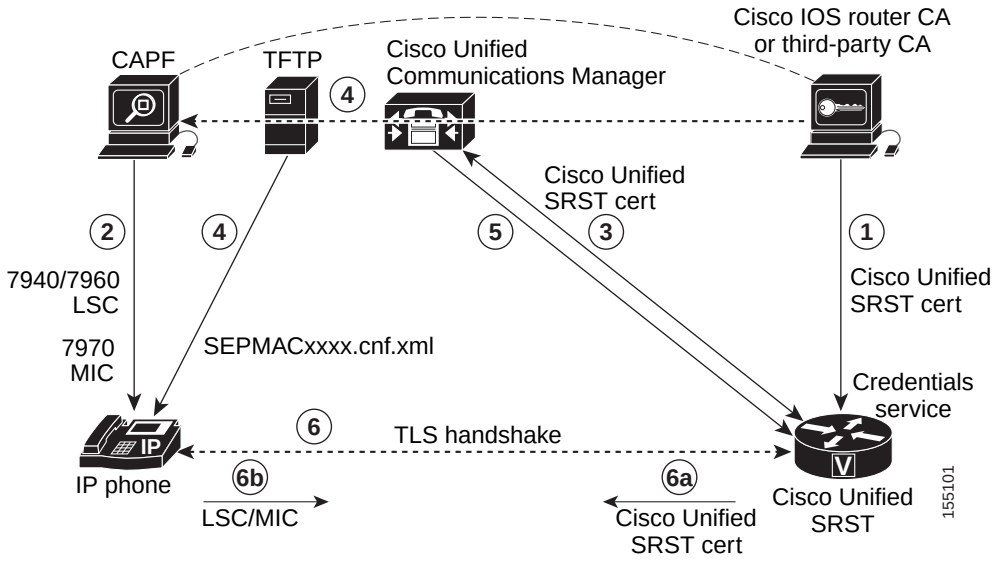


Table 9-3 Overview of the Process of Secure SRST Authentication and Encryption

Process Steps	Description or Detail
1.	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 *Cisco Communications Manager Security Guide*.
2.	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.
3.	Cisco Unified Communications Manager requests the SRST certificate from credentials server, and the credentials server responds with the certificate.

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

Process Steps	Description or Detail
4.	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.
5.	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 241 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.
6.	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.
a.	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.
b.	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.

Note The media is encrypted automatically after the phone and router certificates are exchanged and the TLS connection is established with the SRST router.

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 246
- Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router, page 265
- Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 268
- Configuring Secure SCCP SRST, page 270
- Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 284g

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 246 (optional)
- Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 248 (required)
- Disabling Automatic Certificate Enrollment, page 252 (required)
- Verifying Certificate Enrollment, page 253 (optional)
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 255 (required)
- Troubleshooting Credential Settings, page 257
- Importing Phone Certificate Files in PEM Format to the Secure SRST Router, page 257

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto pki server** *cs-label* **Example:** `Router (config)# crypto pki server srstcaserver`	Enables the certificate server and enters certificate server configuration mode. **Note** If you manually generated an RSA key pair, the *cs-label* argument must match the name of the key pair. For more information on the certificate server, see the *Cisco IOS Certificate Server* documentation.
Step 2	**database level** {**minimal** | **names** | **complete**} **Example:** `Router (cs-server)# database level complete`	Controls what type of data is stored in the certificate enrollment database. • **minimal**: Enough information is stored only to continue issuing new certificates without conflict; this is the default. • **names**: In addition to the information given in the minimal level, the serial number and subject name of each certificate are stored. • **complete**: In addition to the information given in the minimal and names levels, each issued certificate is written to the database. **Note** 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.
Step 3	**database url** *root-url* **Example:** `Router (cs-server)# database url nvram`	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. • The default location for the database entries to be written is flash; however, NVRAM is recommended for this task.
Step 4	**issuer-name** *DN-string* **Example:** `Router (cs-server)# issuer-name CN=srstcaserver`	Sets the CA issuer name to the specified distinguished name (DN-string). The default value is as follows: **issuer-name CN**=*cs-label*.

	Command or Action	Purpose

Step 5	`grant auto`
	
	Example:
	`Router (cs-server)# grant auto`
		Allows an automatic certificate to be issued to any requestor.
		• This command is used only during enrollment and will be removed in the "Disabling Automatic Certificate Enrollment" section on page 252.

Step 6	`no shutdown`
	
	Example:
	`Router (cs-server)# no shutdown`
		Enables the Cisco IOS certificate server.
		• You should issue this command only after you have completely configured your certificate server.

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 251.

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

	Command or Action	Purpose
Step 1	**crypto pki trustpoint** *name* **Example:** `Router(config)# crypto pki trustpoint srstca`	Declares the CA that your router should use and enters ca-trustpoint configuration mode. • The name provided will be the same as the trustpoint name that will be declared in the "Enabling Credentials Service on the Secure Cisco Unified SRST Router" section on page 255.
Step 2	**rsakeypair** *keypair-label* **Example:** `Router(config-trustp)# rsakeypair srstcakey 2048`	To specify a named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint, use the **rsakeypair** command in trustpoint configuration mode. • For TLS 1.2 version, the RSA key length is set to 2048 bits.
Step 3	**enrollment url** *url* **Example:** `Router(ca-trustpoint)# enrollment url http://10.1.1.22`	Specifies the enrollment parameters of your CA. • **url** *url*: Specifies the URL of the CA to which your router should send certificate requests. • If you are using Cisco proprietary SCEP for enrollment, *url* must be in the form http://*CA_name*, where *CA_name* is the host Domain Name System (DNS) name or IP address of the Cisco IOS CA. • If you used the procedure documented in the "Configuring a Certificate Authority Server on a Cisco IOS Certificate Server" section on page 246, the URL is the IP address of the certificate server router configured in Step 1. If a third-party CA was used, the IP address is to an external CA.
Step 4	**revocation-check** *method1* **Example:** `Router(ca-trustpoint)# revocation-check none`	Checks the revocation status of a certificate. The argument *method1* is the method used by the router to check the revocation status of the certificate. For this task, the only available method is **none.** The keyword **none** means that a revocation check will not be performed and the certificate will always be accepted. • Using the **none** keyword is mandatory for this task.
Step 5	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**crypto pki authenticate** *name* **Example:** `Router(config)# crypto pki authenticate srstca`	Authenticates the CA (by getting the certificate from the CA). • Takes the name of the CA as the argument.
Step 7	**crypto pki enroll** *name* **Example:** `Router(config)# crypto pki enroll srstca`	Obtains the SRST router certificate from the CA. • Takes the name of the CA as the argument.

Examples

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

```
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]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.


Sep 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: 0573FBB2
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 246.

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

	Command or Action	Purpose
Step 1	`crypto pki server` *cs-label* **Example:** `Router (config)# crypto pki server srstcaserver`	Enables the certificate server and enters certificate server configuration mode. **Note** If you manually generated an RSA key pair, the *cs-label* argument must match the name of the key pair.

Step 2	`shutdown`
	
	Example:
	`Router (cs-server)# shutdown`
		Disables the Cisco IOS certificate server.

Step 3	`no grant auto`
	
	Example:
	`Router (cs-server)# no grant auto`
		Disables automatic certificates to be issued to any requestor.
		
		• This command was for use during enrollment only and thus needs to be removed in this task.

Step 4	`no shutdown`
	
	Example:
	`Router (cs-server)# no shutdown`
		Enables the Cisco IOS certificate server.
		
		• You should issue this command only after you have completely configured your certificate server.

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

	Command or Action	Purpose

Step 1	`show running-config`
	
	Example:
	`Router# show running-config`
	`.`
	`.`
	`.`
	`! SRST router device certificate.`
	`crypto pki certificate chain srstca`
	`certificate 02`
	`308201AD 30820116 A0030201 02020102 300D0609`
	`2A864886 F70D0101 04050030`
	`17311530 13060355 0403130C 73727374 63617365`
	`72766572 301E170D 30343034`
	`31323139 35323233 5A170D30 35303431 32313935`
	`3232335A 30343132 300F0603`
	`55040513 08443042 39453739 43301F06 092A8648`
	`86F70D01 09021612 6A61736F`
	`32363931 2E636973 636F2E63 6F6D305C 300D0609`
	`2A864886 F70D0101 01050003`
	`4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2`
	`056E0485 22896D36 6CA70C19`
	`C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3`
	`12946123 E5C1CCD7 A23E6155`
	`FA2ED743 3FB8B902 03010001 A330302E 300B0603`
	`551D0F04 04030205 A0301F06`
	`03551D23 04183016 8014F829 CE97AD60 18D05467`
	`FC293963 C2470691 F9BD300D`
	`06092A86 4886F70D 01010405 00038181 007EB48E`
	`CAE9E1B3 D1E7A185 D7F0D565`
	`CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D`
	`99CBD267 EB8ADF9D 9E43A5F2`
	`FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1`
	`AC518E0B 8657CEBB ED2BDE8E`
	`B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3`
	`1EE43B6E 6CB29EE7 0B8C2752`
	`C3AF4A66 BD007348 D013000A EA3C206D CF`
	`quit`
	`certificate ca 01`
	`30820207 30820170 A0030201 02020101 300D0609`
	`2A864886 F70D0101 04050030`
	`17311530 13060355 0403130C 73727374 63617365`
	`72766572 301E170D 30343034`
	`31323139 34353136 5A170D30 37303431 32313934`
	`3531365A 30173115 30130603`
	`55040313 0C737273 74636173 65727665 7230819F`
	`300D0609 2A864886 F70D0101`
	`01050003 818D0030 81890281 8100C3AF EE1E4BB1`
	`9922A8DA 2BB9DC8E 5B1BD332`
	`1051C9FE 32A971B3 3C336635 74691954 98E765B1`
	`059E24B6 32154E99 105CA989`
	`9619993F CC72C525 7357EBAC E6335A32 2AAF9391`
	`99325BFD 9B8355EB C10F8963`
		Use the **show running-config** command to verify the creation of the CA server (01) and device (02) certificates. This example shows the enrolled certificates.

	Command or Action	Purpose
	9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417 DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04 160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418 30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886 F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805 47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2 C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57 5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3 DEDBAAD7 3780136E B112A6 quit	
Step 2	show crypto pki server **Example:** Router# show crypto pki server Certificate Server srstcaserver: Status: enabled Server's configuration is locked (enter "shut" to unlock it) Issuer name: CN=srstcaserver CA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00 Granting mode is: auto Last certificate issued serial number: 0x2 CA certificate expiration timer: 13:46:57 PST Dec 1 2007 CRL NextUpdate timer: 14:54:57 PST Jan 19 2005 Current storage dir: nvram Database Level: Complete - all issued certs written as <serialnum>.cer	Use the **show crypto pki server** command to verify the status of the CA server after a boot procedure.

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 283.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**credentials** **Example:** `Router(config)# credentials`	Provides the Cisco Unified SRST Router certificate to Cisco Unified Communications Manager and enters credentials configuration mode.
Step 2	**ip source-address** *ip-address* [**port** *port*] **Example:** `Router(config-credentials)# ip source-address 10.1.1.22 port 2445`	Enables the Cisco Unified SRST Router to receive messages from Cisco Unified Communications Manager through the specified IP address and port. • *ip-address*: The IP address is the pre-existing router IP address, typically one of the addresses of the Ethernet port of the router. • **port** *port*: (Optional) The port to which the gateway router connects to receive messages from Cisco Unified Communications Manager. The port number is from 2000 to 9999. The default port number is 2445.
Step 3	**trustpoint** *trustpoint-name* **Example:** `Router(config-credentials)# trustpoint srstca`	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. • The trustpoint name should be the same as the one declared in the "Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server" section on page 248.
Step 4	**exit** **Example:** `Router(config-credentials)# exit`	Exits credentials configuration mode.

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

	Command or Action	Purpose

Step 1	**show credentials**
	
	Example:
	`Router# show credentials`
	
	`Credentials IP: 10.1.1.22`
	`Credentials PORT: 2445`
	`Trustpoint: srstca`
		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.

Step 2	**debug credentials**
	
	Example:
	`Router# debug credentials`
	
	`Credentials server debugging is enabled`
	`Router#`
	`Sep 29 01:01:50.903: Credentials service: Start TLS Handshake 1 10.1.1.13 2187`
	`Sep 29 01:01:50.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr`
	`Sep 29 01:01:51.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr`
	`Sep 29 01:01:52.907: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr`
	`Sep 29 01:01:53.927: Credentials service: TLS Handshake completes.`
		Use the **debug credentials** command to set debugging on the credential settings of the Cisco Unified SRST Router.

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-----".

For certification operation on Cisco Unified Communications Operating System Administration Guide, Release 6.1(1), see http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/6_1_1/cucos/iptpch6.html.

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

	Command or Action	Purpose
Step 1	**crypto pki trustpoint** *name* **Example:** `Router (config)# crypto pki trustpoint CAPF`	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).
Step 2	**revocation-check none** **Example:** `Router(ca-trustpoint)# 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.
Step 3	**enrollment terminal** **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual cut-and-paste certificate enrollment.
Step 4	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration.
Step 5	**crypto pki authenticate** *name* **Example:** `Router(config)# crypto pki authenticate CAPF`	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.

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

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(ca-trustpoint)# 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
MIIDqDCCApCgAwIBAgIQNT+yS9cPFKNGwfOprHJWdTANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMjAe
Fw0wMzEwMTAyMDE4NDlaFw0yMzEwMTAyMDI3MzdaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAyMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEAxCZlBK19w/2NZVVvpjCPrpW1cCY7V1q9lhzI85RZZdnQ
2M4CufgIzNa3zYxGJIAYeFfcRECnMB3f5A+x7xNiEuzE87UPvK+7S80uWCY0Uhtl
AVVf5NQgZ3YDNoNXg5MmONb8lT86F55EZyVac0XGne77TSIbIdejrTgYQXGP2MJx
Qhg+ZQlGFDRzbHfM84Duv2Msez+l+SqmqO80kIckqE9Nr3/XCSj1hXZNNVg8D+mv
Hth2P6KZqAKXAAStGRLSZX3jNbS8tveJ3Gi5+sj9+F6KKK2PD0iDwHcRKkcUHb7g
lI++U/5nswjUDIAph715Ds2rn9ehkMGipGLF8kpuCwIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpIr4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAyL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDIuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMlxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAyLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLNWip2vDRihm
E+DlXdwMS5JaqUtuaSd/m/xzxpcRJm4ZRRwPq6VeaiiQGkjFuZEe5jSKiSAK7eHg
tup4HP/ZfKSwPA40DlsGSYsKNMm3OmVOCQUMH02lPkS/eEQ9sIw6QS7uuHN4y4CJ
NPnRbpFRLw06hnStCZHtGpKEHnY213QOy3h/EWhbnp0MZ+hdr20FujSI6G1+L39l
aRjeD708f2fYoz9wnEpZbtn2Kzse3uhU1Ygq1D1x9yuPq388C18HWdmCj4OVTXux
V6Y47H1yv/GJM8FvdgvKlExbGTFnlHpPiaG9tQ==
quit
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

Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# 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
MIICKDCCAZGgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQDELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRUwEwYDVQQDEwxDQVBGLTdEN0Qw
QzAwHhcNMDQwNzE1MjIzODMyWhcNMTkwNzEyMjIzODMxWjBAMQswCQYDVQQGEwJV
UzEaMBgGA1UEChMRQ2lzY28gU3lzdGVtcyBJbmMxFTATBgNVBAMTDENBUEYtN0Q3
RDBDMDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0hvMOZZ9ENYWme11YGY1
it2rvE3Nk/eqhnv8P9eqB1iqt+fFBeAG0WZ5bO5FetdU+BCmPnddvAeSpsfr3Z+h
x+r58fOEIBRHQLgnDZ+nwYH39uwXcRWWqWwlW147YHjV7M5c/R8T6daCx4B5NBo6
kdQdQNOrV3IP7kQaCShdM/kCAwEAAaMxMC8wDgYDVR0PAQH/BAQDAgKEMB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDBTANBgkqhkiG9w0BAQUFAAOBgQCaNi6x
sL6M5NlDezpSBO3QmUVyXMfrONV2ysrSwcXzHu0gJ9MSJ8TwiQmVaJ47hSTlF5a8
YVYJ0IdifXbXRo+/EEO7kkmFE8MZta5rM7UWj8bAeR42iqA3RzQaDwuJgNWT9Fhh
GgfuNAlo5h1Aikxsvxi vmDlLdZyCMoqJJd7B2Q==
quit
Certificate has the following attributes:
Fingerprint MD5: 4B9636DF 0F3BA6B7 5F54BE72 24762DBC
```

```
Fingerprint SHA1: A9917775 F86BB37A 5C130ED2 3E528BB8 286E8C2D
% 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)# enrollment terminal
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
MIIDqDCCApCgAwIBAgIQdhL5YBU9b59OQiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAe
Fw0wMzAyMDYyMzI3MTNaFw0yMzAyMDYyMzM2MzRaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAxMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEArFW77Rjem4cJ/7yPLVCauDohwZZ/3qf0sJaWlLeAzBlq
Rj2lFlSij0ddkDtfEEo9VKmBOJsvx6xJlWJiuBwUMDhTRbsuJz+npkaGBXPOXJmN
Vd54qlpc/hQDfWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrvlRuz0x3mdbcBEdHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZXmeHjqEgVO3UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxwlANPweufgZMaywIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU6Rexgscfz6ypG270qSac
cK4FoJowbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAxL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDEuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMVxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAxLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAq2T96/YMMtw2Dw4QX+F1+g1XSrUCrNyjx7vtFaRDHyB+kobw
dwkpohfkzfTyYpJELzV1r+kMRoyuZ7oIqqccEroMDnnmeApc+BRGbDJqS1Zzk4OA
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrcxb0UH7IQJ1ogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVVilK17qpqCPllKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxgCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
quit
Certificate has the following attributes:
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 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 MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint 7960:
Issuing CA certificate configured:
Subject Name:
cn=CAPF-508A3754,o=Cisco Systems Inc,c=US
Fingerprint MD5: 6BAE18C2 0BCE391E DAE2FE4C 5810F576
Fingerprint SHA1: B7735A2E 3A5C274F C311D7F1 3BE89942 355102DE
State:
```

```
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint PEM:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-001,o=Cisco Systems
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint srstcaserver:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint srstca:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
Router General Purpose certificate configured:
Subject Name:
serialNumber=F3246544+hostname=c2611XM-sSRST.cisco.com
Fingerprint: 35471295 1C907EC1 45B347BC 7A9C4B86
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

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:

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

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIICKjCCAZOgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQTELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTU4RUFE
MkQyMB4XDTA2MDMwMTIxMjc1MloXDTIxMDIyNTIxMjc1MVowQTELMAkGA1UEBhMC
VVMxGjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTU4
RUFEMkQyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC99KgZT94qhozw4bOB
```

```
f8Z0tYwT2l4L++mC64O3s3AshDi8xe8Y8sN/f/ZKRRhNIxBlK4SWafXnHKJBqKZn
WtSgkRjJ3Dh0XtqcWYt8VS2sC69g8sX09lskKl3m+TpWsr2T/mDXv6CceaKN+mch
gcrrnNo8kamOOIG8OsQc4L6XzQIDAQABozEwLzAOBgNVHQ8BAf8EBAMCAoQwHQYD
quit
Certificate has the following attributes:
Fingerprint MD5: 1951DJ4E 76D79FEB FFB061C6 233C8E33
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(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# 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
MIIDqDCCApCgAwIBAgIQdhL5YBU9b59OQiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAe
Vd54qlpc/hQDfWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrvlRuz0x3mdbcBEdHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZXmeHjqEgVO3UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxwlANPweufgZMaywIBA6OBwzCBwDALBgNVHQ8E
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrcxb0UH7IQJ1ogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVVilK17qpqCPllKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxgCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
quit
Certificate has the following attributes:
Fingerprint MD5: 21956CBR 4B9706DF 0F3BA6B7 7P54AZ72
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(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# 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
MIIE2TCCA8GgAwIBAgIKamlnswAAAAAAAzANBgkqhkiG9w0BAQUFADA1MRYwFAYD
D/g2qgfEMkHFp68dGf/2c5k5WnNnYhM0DR9elXBSZBcG7FNcXNtq6jUAQQIBA6OC
AecwggHjMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFNDFIiarT0Zg7K4F
kcfcWtGwR/dsMAsGA1UdDwQEAwIBhjAQBgkrBgEEAYI3FQEEAwIBADAZBgkrBgEE
AYI3FAIEDB4KAFMAdQBiAEMAQTAfBgNVHSMEGDAWgBQn88gVHm6aAgkWrSugiWBf
2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1
cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEFBQcBAQREMEIwQAYIKwYB
BQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9j
cmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkVAQIAMEMwQQYIKwYBBQUH
I+ii6itvaSN6go4cTAnPpE+rhC836WVg0ZrG2PML9d7QJwBcbx2RvdFOWFEdyeP3
OOfTC9Fovo4ipUsG4eakqjN9GnW6JvNwxmEApcN5JlunGdGTjaubEBEpH6GC/f08
```

```
S25l3JNFBemvM2tnIwcGhiLa69yHz1khQhrpz3B1iOAkPV19TpY4gJfVb/Cbcdi6
YBmlsGGGrd1lZva5J6LuL2GbuqEwYf2+rDUU+bgtlwavw+9tzD0865XpgdOKXrbO
+nmka9eiV2TEP0zJ2+iC7AFm1BCIolblPFft6QKoSJFjB6thJksaE5/k3Npf
quit
Certificate has the following attributes:
Fingerprint MD5: 0F3BA6B7 4B9636DF 5F54BE72 24762SBR
Fingerprint SHA1: L92BB37A S9919925 5C130ED2 3E528UP8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

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

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
quit
Certificate has the following attributes:
Fingerprint MD5: 2G3LZ6B7 2R1995ER 6KE4WE72 3E528BB8
Fingerprint SHA1: M9912245 5C130ED2 24762JBC 3E528VF8 956E8S5H
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% 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 265 (required)
- Configuring SRST Fallback on Cisco Unified Communications Manager, page 266 (required)
- Configuring CAPF on Cisco Unified Communications Manager, page 268 (required)

Adding an SRST Reference to Cisco Unified Communications Manager

The following procedure describes how to add an SRST reference to Cisco Unified Communications Manager.

Before following this procedure, verify that credentials service is running in the Cisco Unified SRST Router. Cisco Unified Communications Manager connects to the Cisco Unified SRST Router for its device certificate. To enable credentials service, see the "Enabling Credentials Service on the Secure Cisco Unified SRST Router" section on page 255.

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: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

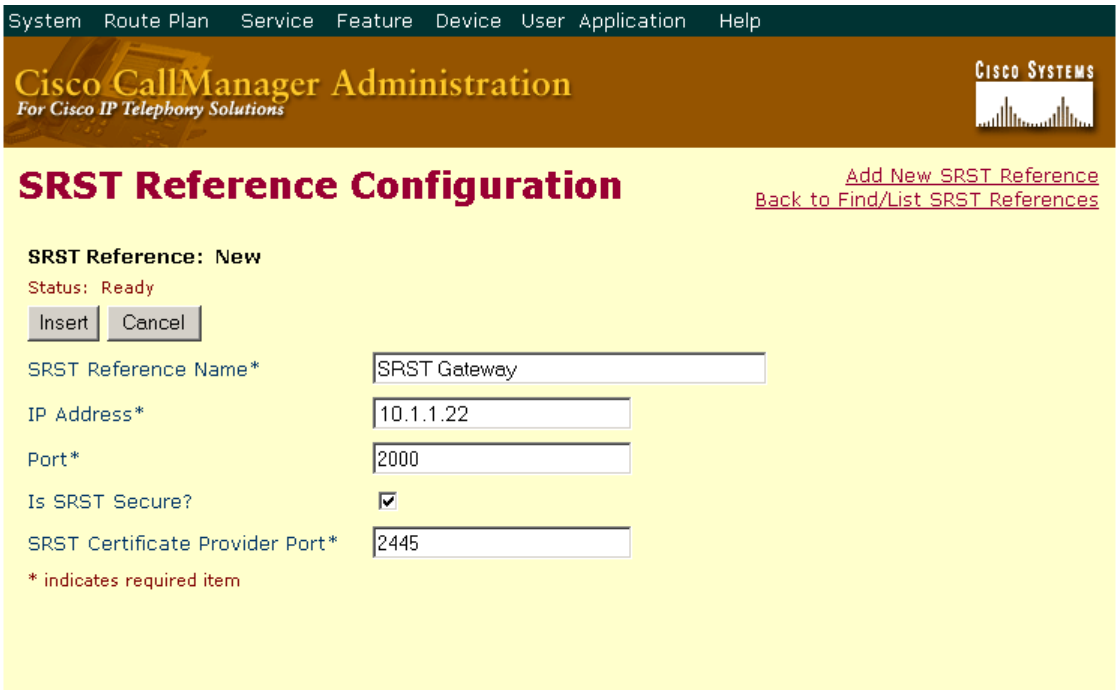
Step 1 In the menu bar in Cisco Unified Communications Manager, choose **CCMAdmin > System > SRST**.

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: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

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

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-ephones** *max-phones*
6. **max-dn** *max-directory-numbers*
7. **transfer-pattern** *transfer-pattern*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-manager-fallback** **Example:** `Router(config)# call-manager-fallback`	Enters call-manager-fallback configuration mode.
Step 2	**secondary-dialtone** *digit-string* **Example:** `Router(config-cm-fallback)# secondary-dialtone 9`	Activates a secondary dial tone when a digit string is dialed.
Step 3	**transfer-system** {**blind** | **full-blind** | **full-consult** | **local-consult**} **Example:** `Router(config-cm-fallback)# transfer-system full-consult`	Defines the call-transfer method for all lines served by the Cisco Unified SRST Router. • **blind**: Calls are transferred without consultation with a single phone line using the Cisco proprietary method. • **full-blind**: Calls are transferred without consultation using H.450.2 standard methods. • **full-consult**: Calls are transferred with consultation using a second phone line if available. The calls fallback to **full-blind** if the second line is unavailable. • **local-consult**: Calls are transferred with local consultation using a second phone line if available. The calls fallback to **blind** for nonlocal consultation or nonlocal transfer target.
Step 4	**ip source-address** *ip-address* [**port** *port*] **Example:** `Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000`	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.
Step 5	**max-ephones** *max-phones* **Example:** `Router(config-cm-fallback)# max-ephones 15`	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 26 for further details.
Step 6	**max-dn** *max-directory-numbers* **Example:** `Router(config-cm-fallback)# max-dn 30`	Sets the maximum number of directory numbers (DNs) or virtual voice ports that can be supported by the router. • *max-directory-numbers:* 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 26 for further details.

	Command or Action	Purpose
Step 7	**transfer-pattern** *transfer-pattern* **Example:** `Router(config-cm-fallback)# transfer-pattern .....`	Allows transfer of phone calls by Cisco Unified IP Phones to specified phone number patterns. • *transfer-pattern*: String of digits for permitted call transfers. Wildcards are allowed.
Step 8	**exit** **Example:** `Router(config-cm-fallback)# exit`	Exits call-manager-fallback configuration mode.

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

- 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 235. 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.

- Secure H.323 or SIP trunks.
- SIP phones interoperability.
- Hot Standby Routing Protocol (HSRP).

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 232.

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 237.

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 255
- Adding an SRST Reference to Cisco Unified Communications Manager, page 265
- Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 268

SUMMARY STEPS

1. **show ephone**
2. **show ephone offhook**
3. **show voice call status**
4. **debug ephone register**
5. **debug ephone state**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show ephone**
	
	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`
		Use this command to display registered Cisco Unified IP Phones and their capabilities. The **show ephone** 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.

Step 2	**show ephone offhook**
	
	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`
	`: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`
		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.

Command or Action	Purpose
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	

Command or Action	Purpose

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 0x86039700 50/0/2.0 *2010 g711ulaw 20002/20012`
`0x116C 2C0A 0x86119520 50/0/23.0 2034 g711ulaw 20023/20020`
`0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw 20020/20023`
`0x116E 2C0D 0x8608DC20 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 0x860EE8AC 50/0/19.0 *2004 g711ulaw 20019/20016`
`0x117A 2C1F 0x86043FA4 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`
	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.

Command or Action	Purpose
0x117F 2C25 0x85C6BE6C 50/0/1.0 *2006 g711ulaw 20001/20006 0x1180 2C28 0x860ADFF0 50/0/13.0 2029 g711ulaw 20013/20034 0x1181 2C28 0x8618FBBC 50/0/34.0 *2029 g711ulaw 20034/20013 0x1182 2C2B 0x860C3B1C 50/0/15.0 2036 g711ulaw 20015/20005 0x1183 2C2B 0x860590EC 50/0/5.0 *2036 g711ulaw 20005/20015 0x1184 2C2E 0x8617A090 50/0/32.0 2024 g711ulaw 20032/20007 0x1185 2C2E 0x8606E234 50/0/7.0 *2024 g711ulaw 20007/20032 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	
Step 4 debug ephone register **Example:** Router# debug ephone register EPHONE registration debugging is enabled *Jun 29 09:16:02.180: New Skinny socket accepted [2] (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

Step 5 `debug ephone state`
 	
Example:
`Router# debug ephone state`
`*Jan 11 18:33:09.231:%SYS-5-CONFIG_I:Configured from console by console`
`*Jan 11 18:33:11.747:ephone-2[2]:OFFHOOK`
`*Jan 11 18:33:11.747:ephone-2[2]:---SkinnySyncPhoneDnOverlays is onhook`
`*Jan 11 18:33:11.747:ephone-2[2]:SIEZE on activeLine 0 activeChan 1`
`*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 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`
`*Jan 11 18:33:16.039:ephone-2[2]:Skinny-to-Skinny 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 TsProceed`
`*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsRingOut`
`*Jan 11 18:33:16.039:ephone-2[2]::callingNumber 6000`
`*Jan 11 18:33:16.039:ephone-2[2]::callingParty 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`
`*Jan 11 18:33:16.039:ephone-2[2]:Original Called Name 6001`
`*Jan 11 18:33:16.039:ephone-2[2]:6000 calling`
`*Jan 11 18:33:16.039:ephone-2[2]:6001`
`*Jan 11 18:33:16.047:ephone-3[3]:SetCallState line 1 DN 4(4) chan 1 ref 7 TsRingIn`
`*Jan 11 18:33:16.047:ephone-3[3]::callingNumber 6000`
`*Jan 11 18:33:16.047:ephone-3[3]::callingParty 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`
`*Jan 11 18:33:16.047:ephone-3[3]:Ringer Inside Ring On`
	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.

Command or Action	Purpose
*Jan 11 18:33:16.051:dn_tone_control DN=2 chan 1 tonetype=36:DtAlertingTone onoff=1 pid=232 *Jan 11 18:33:20.831:ephone-3[3]:OFFHOOK *Jan 11 18:33:20.831:ephone-3[3]:---SkinnySyncPhoneDnOverlays is onhook *Jan 11 18:33:20.831:ephone-3[3]:Ringer Off *Jan 11 18:33:20.831:ephone-3[3]:ANSWER call *Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsOffHook *Jan 11 18:33:20.831:ephone-3[3][SEP000DEDAB3EBF]:Answer Incoming call from ephone-(2) DN 2 chan 1 *Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsConnected *Jan 11 18:33:20.831:defer_start for DN 2 chan 1 at CONNECTED *Jan 11 18:33:20.831:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsConnected *Jan 11 18:33:20.835:ephone-3[3]::callingNumber 6000 *Jan 11 18:33:20.835:ephone-3[3]::callingParty 6000 *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 *Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000 origcalled 6001 calltype 1 *Jan 11 18:33:20.835:ephone-3[3]:Call Info for chan 1 *Jan 11 18:33:20.835:ephone-3[3]:Original Called Name 6001 *Jan 11 18:33:20.835:ephone-3[3]:6000 calling *Jan 11 18:33:20.835:ephone-3[3]:6001 *Jan 11 18:33:20.835:ephone-2[2]:Security Key Generation ! Ephone 2 generates a security key. *Jan 11 18:33:20.835:ephone-2[2]:OpenReceive DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160 *Jan 11 18:33:20.835:ephone-2[2]:Send Decryption Key ! Ephone 2 sends the decryption key. *Jan 11 18:33:20.835:ephone-3[3]:Security Key Generation !Ephone 3 generates its security key. *Jan 11 18:33:20.835:ephone-3[3]:OpenReceive DN 4 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160 *Jan 11 18:33:20.835:ephone-3[3]:Send Decryption Key ! Ephone 3 sends its decryption key. *Jan 11 18:33:21.087:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232 *Jan 11 18:33:21.087:DN 4 chan 1 Voice_Mode *Jan 11 18:33:21.091:DN 2 chan 1 End Voice_Mode *Jan 11 18:33:21.091:DN 2 chan 1 Voice_Mode *Jan 11 18:33:21.095:ephone-2[2]:OpenReceiveChannelAck:IP 1.1.1.8, port=25552, dn_index=2, dn=2, chan=1	

Command or Action	Purpose
*Jan 11 18:33:21.095:ephone-3[3]:StartMedia 1.1.1.8 port=25552 *Jan 11 18:33:21.095:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160 *Jan 11 18:33:21.095:ephone-3[3]:Send Encryption Key ! Ephone 3 sends its encryption key. *Jan 11 18:33:21.347:ephone-3[3]:OpenReceiveChannelAck:IP 1.1.1.9, port=17520, dn_index=4, dn=4, chan=1 *Jan 11 18:33:21.347:ephone-2[2]:StartMedia 1.1.1.9 port=17520 *Jan 11 18:33:21.347:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160 *Jan 11 18:33:21.347:ephone-2[2]:Send Encryption Key !Ephone 2 sends its encryption key.*Jan 11 18:33:21.851:ephone-2[2]::callingNumber 6000 *Jan 11 18:33:21.851:ephone-2[2]::callingParty 6000 *Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 call state 4 called 6001 calling 6000 origcalled *Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 called 6001 calling 6000 origcalled 6001 calltype 2 *Jan 11 18:33:21.851:ephone-2[2]:Call Info for chan 1 *Jan 11 18:33:21.851:ephone-2[2]:Original Called Name 6001 *Jan 11 18:33:21.851:ephone-2[2]:6000 calling *Jan 11 18:33:21.851:ephone-2[2]:6001	

Configuration Examples for Secure SCCP SRST

This section provides the following configuration examples:

- Secure SCCP SRST: Example, page 278
- Control Plane Policing: Example, page 283

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
```

```
!
! 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
  308201AD 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 35323233 5A170D30 35303431 32313935 3232335A 30343132 300F0603
  55040513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
  32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
  C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
  FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
  03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
  06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
  CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
  FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
  B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
  C3AF4A66 BD007348 D013000A EA3C206D CF
  quit
 certificate ca 01
  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
  55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
  1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
  9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
  9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
  DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
  FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
  160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
  30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
  F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
  47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
  C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
```

```
  5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
  DEDBAAD7 3780136E B112A6
  quit
crypto pki certificate chain srstcaserver
 certificate ca 01
  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
  55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
  1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
  9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
  9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
  DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
  FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
  160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
  30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
  F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
  47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
  C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
  5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
  DEDBAAD7 3780136E B112A6
  quit
crypto pki certificate chain 7970
 certificate ca 353FB24BD70F14A346C1F3A9AC725675
  308203A8 30820290 A0030201 02021035 3FB24BD7 0F14A346 C1F3A9AC 72567530
  0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
  20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3032301E
  170D3033 31303130 32303138 34395A17 0D323331 30313032 30323733 375A302E
  31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
  03130B43 41502D52 54502D30 30323082 0120300D 06092A86 4886F70D 01010105
  00038201 0D003082 01080282 010100C4 266504AD 7DC3FD8D 65556FA6 308FAE95
  B570263B 575ABD96 1CC8F394 5965D9D0 D8CE02B9 F808CCD6 B7CD8C46 24801878
  57DC4440 A7301DDF E40FB1EF 136212EC C4F3B50F BCAFBB4B CD2E5826 34521B65
  01555FE4 D4206776 03368357 83932638 D6FC953F 3A179E44 67255A73 45C69DEE
  FB4D221B 21D7A3AD 38184171 8FD8C271 42183E65 09461434 736C77CC F380EEBF
  632C7B3F A5F92AA6 A8EF3490 8724A84F 4DAF7FD7 0928F585 764D3558 3C0FE9AF
  1ED8763F A299A802 970004AD 1912D265 7DE335B4 BCB6F789 DC68B9FA C8FDF85E
  8A28AD8F 0F4883C0 77112A47 141DBEE0 948FBE53 FE67B308 D40C8029 87BD790E
  CDAB9FD7 A190C1A2 A462C5F2 4A6E0B02 0103A381 C33081C0 300B0603 551D0F04
  04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  1452922B E288EE2E 098A4E7E 702C56A5 9AB4D49B 96306F06 03551D1F 04683066
  3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30322F43 65727445
  6E726F6C 6C2F4341 502D5254 502D3030 322E6372 6C862F66 696C653A 2F2F5C5C
  6361702D 7274702D 3030325C 43657274 456E726F 6C6C5C43 41502D52 54502D30
  30322E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
  F70D0101 05050003 82010100 56838CEF C4DA3AD1 EA8FBB15 2FFE6EE5 50A1972B
  D4D7AF1F D298892C D5A2A76B C3462866 13E0E55D DC0C4B92 5AA94B6E 69277F9B
  FC73C697 11266E19 451C0FAB A55E6A28 901A48C5 B9911EE6 348A8920 0AEDE1E0
  B6EA781C FFD97CA4 B03C0E34 0E5B0649 8B0A34C9 B73A654E 09050C1F 4DA53E44
  BF78443D B08C3A41 2EEEB873 78CB8089 34F9D16E 91512F0D 3A8674AD 0991ED1A
  92841E76 36D7740E CB787F11 685B9E9D 0C67E85D AF6D05BA 3488E86D 7E2F7F65
  6918DE0F BD3C7F67 D8A33F70 9C4A596E D9F62B3B 1EDEE854 D5882AD4 3D71F72B
  8FAB7F3C 0B5F0759 D9828F83 954D7BB1 57A638EC 7D72BFF1 8933C16F 760BCA94
  4C5B1931 67947A4F 89A1BDB5
  quit
crypto pki certificate chain PEM
 certificate ca 7612F960153D6F9F4E42202032B72356
  308203A8 30820290 A0030201 02021076 12F96015 3D6F9F4E 42202032 B7235630
  0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
  20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3031301E
  170D3033 30323036 32333237 31335A17 0D323330 32303632 33333633 345A302E
  31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
  03130B43 41502D52 54502D30 30313082 0120300D 06092A86 4886F70D 01010105
```

```
  00038201 0D003082 01080282 010100AC 55BBED18 DE9B8709 FFBC8F2D 509AB83A
  21C1967F DEA7F4B0 969694B7 80CC196A 463DA516 54A28F47 5D903B5F 104A3D54
  A981389B 2FC7AC49 956262B8 1C143038 5345BB2E 273FA7A6 46860573 CE5C998D
  55DE78AA 5A5CFE14 037D695B AC816409 C6211F0B 3BBF09CF B0BBB2D4 AC362F67
  0FD145F1 620852B3 1F07E2F1 AA74F150 367632ED A289E374 AF0C5B78 CE7DFB9F
  C8EBBE54 6ECF4C77 99D6DC04 47476C0F 36E58A3B 6BCB24D7 6B6C84C2 7F61D326
  BE7CB4A6 60CD6579 9E1E3A84 8153B750 5527E865 423BE2B5 CB575453 5AA96093
  58B6A2E4 AA3EF081 C7068EC1 DD1EBDDA 53E6F0D6 E2E0486B 109F1316 78C696A3
  CFBA84CC 7094034F C1EB9F81 931ACB02 0103A381 C33081C0 300B0603 551D0F04
  04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E917B1 82C71FCF ACA91B6E F4A9269C 70AE05A0 9A306F06 03551D1F 04683066
  3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30312F43 65727445
  6E726F6C 6C2F4341 502D5254 502D3030 312E6372 6C862F66 696C653A 2F2F5C5C
  6361702D 7274702D 3030315C 43657274 456E726F 6C6C5C43 41502D52 54502D30
  30312E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
  F70D0101 05050003 82010100 AB64FDEB F60C32DC 360F0E10 5FE175FA 0D574AB5
  02ACDCA3 C7BBED15 A4431F20 7E9286F0 770929A2 17E4CDF4 F2629244 2F3575AF
  E90C468C AE67BA08 AAA71C12 BA0C0E79 E6780A5C F814466C 326A4B56 73938380
  73A11AED F9B9DE74 1195C48F 99454B8C 30732980 CD6E7123 8B3A6D68 80B97E00
  7F4BD4BA 0B5AB462 94D9167E 6D8D48F2 597CDE61 25CFADCC 5BD141FB 210275A2
  0A4E3400 1428BA0F 69953BB5 50D21F78 43E3E563 98BCB2B1 A2D4864B 0616BACD
  A61CD9AE C5558A52 B5EEAA6A 08F96528 B1804B87 D26E4AEE AB7AFFE9 2FD2A574
  BAFE0028 96304A8B 13FB656D 8FC60094 D5A53D71 444B3CEF 79343385 3778C193
  74A2A6CE DC56275C A20A303D
  quit
crypto pki certificate chain 7960
 certificate ca F301
  308201F7 30820160 A0030201 020202F3 01300D06 092A8648 86F70D01 01050500
  3041310B 30090603 55040613 02555331 1A301806 0355040A 13114369 73636F20
  53797374 656D7320 496E6331 16301406 03550403 130D4341 50462D33 35453038
  33333230 1E170D30 34303430 39323035 3530325A 170D3139 30343036 32303535
  30315A30 41310B30 09060355 04061302 5553311A 30180603 55040A13 11436973
  636F2053 79737465 6D732049 6E633116 30140603 55040313 0D434150 462D3335
  45303833 33323081 9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
  818100C8 BD9B6035 366B44E8 0F693A47 250FF865 D76C35F7 89B1C4FD 1D122CE0
  F5E5CDFF A4A87EFF 41AD936F E5C93163 3E55D11A AF82A5F6 D563E21C EB89EBFA
  F5271423 C3E875DC E0E07967 6E1AAB4F D3823E12 53547480 23BA1A09 295179B6
  85A0E83A 77DD0633 B9710A88 0890CD4D DB55ADD0 964369BA 489043BB B667E60F
  93954B02 03010001 300D0609 2A864886 F70D0101 05050003 81810056 60FD3AB3
  6F98D2AD 40C309E2 C05B841C 5189271F 01D864E8 98BCE665 2AFBCC8C 54007A84
  8F772C67 E3047A6C C62F6508 B36A6174 B68C1D78 C2228FEA A89ECEFB CC8BA9FC
  0F30E151 431670F9 918514D9 868D1235 18137F1E 50DFD32E 1DC29CB7 95EF4096
  421AF22F 5C1D5804 B83F8E8E 95B04F45 86563BFE DF976C5B FB490A
  quit
!
!
no crypto isakmp enable
!
! Enable IPSec.
crypto isakmp policy 1
 authentication pre-share
 lifetime 28800
crypto isakmp key cisco123 address 10.1.1.13
! The crypto key should match the key configured on Cisco Unified Communications Manager.
!
! The crypto IPSec configuration should match your Cisco Unified Communications Manager
configuration.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
!
crypto map rtp 1 ipsec-isakmp
 set peer 10.1.1.13
 set transform-set rtpset
```

```
 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

- 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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example::** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**srtp** **Example::** `Router(config-voi-serv)# srtp`	Specifies that SRTP be used to enable secure calls.
Step 5	**allow-connections sip to h323** **Example:** `Router(config-voi-serv)# allow-connections sip to h323`	(Optional) Allows connections from SIP endpoints to H.323 endpoints.
Step 6	**allow-connections sip to sip** **Example:** `Router(config-voi-serv)# allow-connections sip to sip`	Allows connections from SIP endpoints to SIP endpoints.
Step 7	**end** **Example:** `Router(conf-voi-serv)# 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**

7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example::** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**sip** **Example:** `Router(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**url sip | sips** **Example:** `Router(conf-serv-sip)# url sips`	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.
Step 6	**srtp negotiate cisco** **Example:** `Router(conf-serv-sip)# srtp negotiate cisco`	Enables a Cisco IOS SIP gateway to negotiate the sending and accepting of RTP profiles in response to SRTP offers.
Step 7	**end** **Example:** `Router(conf-serv-sip)# end`	Ends the current configuration session and returns to privileged EXEC mode.

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

	Command or Action	Purpose

Step 1	`voice register global`
	
	Example:
	`Router(config)# voice register global`
		Enters voice register global configuration mode.

Step 2	`security-policy secure`
	
	Example:
	`Router(config-register-global)# security-policy secure`
		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.
		Note 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.

Step 3	`end`
	
	Example:
	`Router(config-register-global)# end`
		Ends the current configuration session and returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 2	**registrar ipv4**:*destination-address* **expires** *seconds* **Example:** `Router(config-sip-ua)# registrar ipv4:192.168.2.10 expires 3600`	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.
Step 3	**xfer target dial-peer** **Example:** `Router(config-sip-ua)# xfer target dial-peer`	Specifies that SRST should use the dial-peer as a transfer target instead of what is in the message body.
Step 4	**crypto signaling default trustpoint** *string* **[strict-cipher]** **Example:** `Router(config-sip-ua)# crypto signaling default trustpoint 3745-SRST 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.
Step 5	**crypto signaling remote-addr** *{ip address |subnet mask}* **trustpoint** *trustpoint-name* **Example:** `Router(config-sip-ua)# crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk1`	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
Step 6	**end** **Example:** `Router(config-sip-ua)# end`	Ends the current configuration session and returns to privileged EXEC mode.

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 secsrst
```

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.

The **show sip-ua status registrar** command in privileged EXEC mode displays all SIP endpoints that are currently registered with the contact address.

```
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-8d301072@192.168.2.1
                  40004
    3029993       192.168.2.103    382           192.168.2.103
    TCP           001bd433-1c840052-655cd596-4e992eed@192.168.2.1
                  40011
    3029982       192.168.2.106    406           192.168.2.106
    UDP           001d452c-dbba0056-0481d321-1f3f848d@192.168.2.1
                  40001
    3029983       192.168.2.106    406           192.168.2.106
    UDP           001d452c-dbba0057-1c69b699-d8dc6625@192.168.2.1
                  40003
    3029992       192.168.2.107    414           192.168.2.107
    TLS           001e7a25-50c9002c-48ef7663-50c71794@192.168.2.1
                  40005
```

The **show voice register global** command in privileged EXEC mode displays all global configuration parameters associated with SIP phones.

```
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
    network-locale[2] US
    network-locale[3] US
    network-locale[4] 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 20000000
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 srstcakey 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
```

```
!
crypto pki trustpoint Cisco_Root_CA_2048
 enrollment terminal
 revocation-check none
!
!
crypto pki certificate chain TRUSTPT-SRST-CA-2
 certificate 02
  3082020B 30820174 A0030201 02020102 300D0609 2A864886 F70D0101 05050030
  14311230 10060355 04031309 53525354 2D43412D 32301E17 0D313730 36303831
  31333131 325A170D 31383036 30383131 33313132 5A303231 30301206 03550405
  130B4647 4C313735 31313150 42301A06 092A8648 86F70D01 0902160D 416E7473
  41726D79 2D343430 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030
  81890281 81009E24 6259A98D A61C1973 45A95DA8 DE83ECAD C2B1B448 741F7E64
  3D753BF1 19BD54FB 9A4D4A8E 7A2BA416 B93C40B3 A63A7C4D 7303498F 098EF07F
  96F26F5F 49AD4E39 EC113DF4 696CB887 607D545A 52A11469 958F4C04 05868DF9
  317456F6 3D23837C D46331FA 69FB29E8 3211E01C A7AB19A3 94DAC09F 97601196
  A08D7073 76210203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
  551D2304 18301680 142110B8 F25BD9BD E1D401EC 9D11DC0E AE52CDB8 2F301D06
  03551D0E 04160414 2110B8F2 5BD9BDE1 D401EC9D 11DC0EAE 52CDB82F 300D0609
  2A864886 F70D0101 05050003 8181003A DC409694 26D08A31 7B4F495F 002D4E57
  B28669A9 10E93C68 A9556659 97D326EC A5508201 C1A86659 B1CDC910 73097FCA
  F6174794 1057DDDE DBA666D6 0BAFC503 96A10BE5 5FCA3B93 5D377ABE BC9B2774
  3732DF01 CE3BF12B 1899AA69 F7EC8726 A1964C5A D6A99A0E E27EE2A0 15A7D364
  793C6C8D 961C77E4 397F9CB4 C6A271
  quit
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 53525354 2D43412D 32301E17 0D313730 36303831
  31323135 305A170D 32303036 30373131 32313530 5A301431 12301006 03550403
  13095352 53542D43 412D3230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 9E246259 A98DA61C 197345A9 5DA8DE83 ECADC2B1 B448741F
  7E643D75 3BF119BD 54FB9A4D 4A8E7A2B A416B93C 40B3A63A 7C4D7303 498F098E
  F07F96F2 6F5F49AD 4E39EC11 3DF4696C B887607D 545A52A1 1469958F 4C040586
  8DF93174 56F63D23 837CD463 31FA69FB 29E83211 E01CA7AB 19A394DA C09F9760
  1196A08D 70737621 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801421
  10B8F25B D9BDE1D4 01EC9D11 DC0EAE52 CDB82F30 1D060355 1D0E0416 04142110
  B8F25BD9 BDE1D401 EC9D11DC 0EAE52CD B82F300D 06092A86 4886F70D 01010405
  00038181 0018859E D39C6A05 63509442 8746D970 BB716DE2 E82BA822 58AA55AD
  AC37260F 36BFDFE6 F2D0E489 A8D23690 791AD903 F19AC857 5002E621 A5927ACC
  DCB759C0 B126ACAB C53BF054 1F62D895 A895C50A E3AE83E3 EC68F346 50B88D39
  BB053EE9 5D466AE4 C6B4593D 7EFA7A78 213C0766 7307A051 78FED92E 5A34AAB6
  98D2A59C 31
  quit
crypto pki certificate chain SRST-CA-2
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 53525354 2D43412D 32301E17 0D313730 36303831
  31323135 305A170D 32303036 30373131 32313530 5A301431 12301006 03550403
  13095352 53542D43 412D3230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 9E246259 A98DA61C 197345A9 5DA8DE83 ECADC2B1 B448741F
  7E643D75 3BF119BD 54FB9A4D 4A8E7A2B A416B93C 40B3A63A 7C4D7303 498F098E
  F07F96F2 6F5F49AD 4E39EC11 3DF4696C B887607D 545A52A1 1469958F 4C040586
  8DF93174 56F63D23 837CD463 31FA69FB 29E83211 E01CA7AB 19A394DA C09F9760
  1196A08D 70737621 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801421
  10B8F25B D9BDE1D4 01EC9D11 DC0EAE52 CDB82F30 1D060355 1D0E0416 04142110
  B8F25BD9 BDE1D401 EC9D11DC 0EAE52CD B82F300D 06092A86 4886F70D 01010405
  00038181 0018859E D39C6A05 63509442 8746D970 BB716DE2 E82BA822 58AA55AD
  AC37260F 36BFDFE6 F2D0E489 A8D23690 791AD903 F19AC857 5002E621 A5927ACC
  DCB759C0 B126ACAB C53BF054 1F62D895 A895C50A E3AE83E3 EC68F346 50B88D39
  BB053EE9 5D466AE4 C6B4593D 7EFA7A78 213C0766 7307A051 78FED92E 5A34AAB6
  98D2A59C 31
```

```
  quit
crypto pki certificate chain Cisco_Manufacturing_CA
 certificate ca 6A6967B3000000000003
  308204D9 308203C1 A0030201 02020A6A 6967B300 00000000 03300D06 092A8648
  86F70D01 01050500 30353116 30140603 55040A13 0D436973 636F2053 79737465
  6D73311B 30190603 55040313 12436973 636F2052 6F6F7420 43412032 30343830
  1E170D30 35303631 30323231 3630315A 170D3239 30353134 32303235 34325A30
  39311630 14060355 040A130D 43697363 6F205379 7374656D 73311F30 1D060355
  04031316 43697363 6F204D61 6E756661 63747572 696E6720 43413082 0120300D
  06092A86 4886F70D 01010105 00038201 0D003082 01080282 010100A0 C5F7DC96
  943515F1 F4994EBB 9B41E17D DB791691 BBF354F2 414A9432 6262C923 F79AE7BB
  9B79E807 294E30F5 AE1BC521 5646B0F8 F4E68E81 B816CCA8 9B85D242 81DB7CCB
  94A91161 121C5CEA 33201C9A 16A77DDB 99066AE2 36AFECF8 0AFF9867 07F430EE
  A5F8881A AAE8C73C 1CCEEE48 FDCD5C37 F186939E 3D71757D 34EE4B14 A9C0297B
  0510EF87 9E693130 F548363F D8ABCE15 E2E8589F 3E627104 8726A415 620125AA
  D5DFC9C9 5BB8C9A1 077BBE68 92939320 A86CBD15 75D3445D 454BECA8 DA60C7D8
  C8D5C8ED 41E1F55F 578E5332 9349D5D9 0FF836AA 07C43241 C5A7AF1D 19FFF673
  99395A73 67621334 0D1F5E95 70526417 06EC535C 5CDB6AEA 35004102 0103A382
  01E73082 01E33012 0603551D 130101FF 04083006 0101FF02 0100301D 0603551D
  0E041604 14D0C522 26AB4F46 60ECAE05 91C7DC5A D1B047F7 6C300B06 03551D0F
  04040302 01863010 06092B06 01040182 37150104 03020100 30190609 2B060104
  01823714 02040C1E 0A005300 75006200 43004130 1F060355 1D230418 30168014
  27F3C815 1E6E9A02 0916AD2B A089605F DA7B2FAA 30430603 551D1F04 3C303A30
  38A036A0 34863268 7474703A 2F2F7777 772E6369 73636F2E 636F6D2F 73656375
  72697479 2F706B69 2F63726C 2F637263 61323034 382E6372 6C305006 082B0601
  05050701 01044430 42304006 082B0601 05050730 02863468 7474703A 2F2F7777
  772E6369 73636F2E 636F6D2F 73656375 72697479 2F706B69 2F636572 74732F63
  72636132 3034382E 63657230 5C060355 1D200455 30533051 060A2B06 01040109
  15010200 30433041 06082B06 01050507 02011635 68747470 3A2F2F77 77772E63
  6973636F 2E636F6D 2F736563 75726974 792F706B 692F706F 6C696369 65732F69
  6E646578 2E68746D 6C305E06 03551D25 04573055 06082B06 01050507 03010608
  2B060105 05070302 06082B06 01050507 03050608 2B060105 05070306 06082B06
  01050507 0307060A 2B060104 0182370A 0301060A 2B060104 01823714 02010609
  2B060104 01823715 06300D06 092A8648 86F70D01 01050500 03820101 0030F330
  2D8CF2CA 374A6499 24290AF2 86AA42D5 23E8A2EA 2B6F6923 7A828E1C 4C09CFA4
  4FAB842F 37E96560 D19AC6D8 F30BF5DE D027005C 6F1D91BD D14E5851 1DC9E3F7
  38E7D30B D168BE8E 22A54B06 E1E6A4AA 337D1A75 BA26F370 C66100A5 C379265B
  A719D193 8DAB9B10 11291FA1 82FDFD3C 4B6E65DC 934505E9 AF336B67 23070686
  22DAEBDC 87CF5921 421AE9CF 707588E0 243D5D7D 4E963880 97D56FF0 9B71D8BA
  6019A5B0 6186ADDD 6566F6B9 27A2EE2F 619BBAA1 3061FDBE AC3514F9 B82D9706
  AFC3EF6D CC3D3CEB 95E981D3 8A5EB6CE FA79A46B D7A25764 C43F4CC9 DBE882EC
  0166D410 88A256E5 3C57EDE9 02A84891 6307AB61 264B1A13 9FE4DCDA 5F
  quit
crypto pki certificate chain CAPF-3a66269a
 certificate ca 583BD5B4844C8BC172B8C4979092A067
  308203C3 308202AB A0030201 02021058 3BD5B484 4C8BC172 B8C49790 92A06730
  0D06092A 864886F7 0D01010B 05003071 310B3009 06035504 06130249 4E310E30
  0C060355 040A0C05 63697363 6F311230 10060355 040B0C09 75637467 2D656467
  65311630 14060355 04030C0D 43415046 2D336136 36323639 61311230 10060355
  04080C09 6B61726E 6174616B 61311230 10060355 04070C09 62616E67 616C6F72
  65301E17 0D313730 35323931 30333631 335A170D 32323035 32383130 33363132
  5A307131 0B300906 03550406 1302494E 310E300C 06035504 0A0C0563 6973636F
  31123010 06035504 0B0C0975 6374672D 65646765 31163014 06035504 030C0D43
  4150462D 33613636 32363961 31123010 06035504 080C096B 61726E61 74616B61
  31123010 06035504 070C0962 616E6761 6C6F7265 30820122 300D0609 2A864886
  F70D0101 01050003 82010F00 3082010A 02820101 00BC774F BAED3986 05BDFFBC
  4EABBFA7 1F73D150 2989EFF2 902502F6 248DA7AB 261E474C 08A4BB6F 35B10449
  0A6A3D94 E2C6EB98 57BECE0C 34F30517 CA6CC9B2 710B511B 8826E0AB 733FF26F
  F7ADC4B9 76118300 6156072C 43F78E5E 3AD7C92B 54CB5BDB 00B53FC8 875100C4
  056BC4A7 0F96CE69 E58B1C22 194CCEC6 968ECF9B 08B7B7B2 0FF0800E 43764BB1
  E6ED36C0 A738F762 81A88F6D E464E2A5 FD74207F 1EC7ACAC 2F63B04D E0E9DA4C
  901A1710 E3D1C069 82EFF77E 0597254D 149C1263 EC67DAE9 305FD8BF C7410B17
  8C6DE9FF 28A37514 86AF828C BC698DD5 F18A3B66 9D8D895A 5562E08D 383F790A
  A5C7F6F6 915CB558 042E5B99 71F7169D B3AFA699 2B020301 0001A357 3055300B
```

```
  0603551D 0F040403 0202A430 13060355 1D25040C 300A0608 2B060105 05070301
  301D0603 551D0E04 16041475 71EC5D35 1A431511 7E8C8462 6E65E570 7C551930
  12060355 1D130101 FF040830 060101FF 02010030 0D06092A 864886F7 0D01010B
  05000382 0101008F 0D3E9F3E 3574100D 97AD876D B4015C21 300A1BD0 59D5C9BF
  41A8448D 597CD278 718A6431 BA94C042 7EC64BA0 71F04501 C33C1664 16484373
  F3C226A7 256363A9 8BE97291 6B25B8B4 E3DB84C3 3DDB63E7 A9D8D577 6B8F37B3
  7CFCE019 D6F09573 946191F7 C4028465 B072DF74 9D6DED45 CA9E6A3B 1401D1A3
  5449EDCE 9FA593E3 2FD71031 C7C7EB9C 045DAAFE C67603BF DAB40EE0 352C009F
  EAAA6816 A11F6D8B 7C406211 1045A0C6 488B34E1 AF968FAF 3705A364 1EE21A1D
  B7080EDC 40D4AA15 E110C5F1 D8A57561 DB2B09F1 0779B855 3998CE22 C471B5CB
  09605E24 99855176 2D1CA40E BEBC2F23 7434CA2B 8D1C5EFB 822147CC 81F98825
  47A1A14F DC5480
  quit
crypto pki certificate chain Cisco_Root_CA_2048
 certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
  30820343 3082022B A0030201 0202105F F87B282B 54DC8D42 A315B568 C9ADFF30
  0D06092A 864886F7 0D010105 05003035 31163014 06035504 0A130D43 6973636F
  20537973 74656D73 311B3019 06035504 03131243 6973636F 20526F6F 74204341
  20323034 38301E17 0D303430 35313432 30313731 325A170D 32393035 31343230
  32353432 5A303531 16301406 0355040A 130D4369 73636F20 53797374 656D7331
  1B301906 03550403 13124369 73636F20 526F6F74 20434120 32303438 30820120
  300D0609 2A864886 F70D0101 01050003 82010D00 30820108 02820101 00B09AB9
  ABA7AF0A 77A7E271 B6B46662 94788847 C6625584 4032BFC0 AB2EA51C 71D6BC6E
  7BA8AABA 6ED21588 48459DA2 FC83D0CC B98CE026 68704A78 DF21179E F46105C9
  15C8CF16 DA356189 9443A884 A8319878 9BB94E6F 2C53126C CD1DAD2B 24BB31C4
  2BFF8344 6FB63D24 7709EABF 2AA81F6A 56F6200F 11549781 75A725CE 596A8265
  EFB7EAE7 E28D758B 6EF2DD4F A65E629C CF100A64 D04E6DCE 2BCC5BF5 60A52747
  8D69F47F CE1B70DE 701B20D6 6ECDA601 A83C12D2 A93FA06B 5EBB8E20 8B7A91E3
  B568EEA0 E7C40174 A8530B2B 4A9A0F65 120E824D 8E63FDEF EB9B1ADB 53A61360
  AFC27DD7 C76C1725 D473FB47 64508180 944CE1BF AE4B1CDF 92ED2E05 DF020103
  A351304F 300B0603 551D0F04 04030201 86300F06 03551D13 0101FF04 05300301
  01FF301D 0603551D 0E041604 1427F3C8 151E6E9A 020916AD 2BA08960 5FDA7B2F
  AA301006 092B0601 04018237 15010403 02010030 0D06092A 864886F7 0D010105
  05000382 0101009D 9D8484A3 41A97C77 0CB753CA 4E445062 EF547CD3 75171CE8
  E0C6484B B6FE4C3A 198156B0 56EE1996 62AA5AA3 64C1F64E 5433C677 FEC51CBA
  E55D25CA F5F0939A 83112EE6 CBF87445 FEE705B8 ABE7DFCB 4BE13784 DAB98B97
  701EF0E2 8BD7B0D8 0E9DB169 D62A917B A9494F7E E68E95D8 83273CD5 68490ED4
  9DF62EEB A7BEEB30 A4AC1F44 FC95AB33 06FB7D60 0ADEB48A 63B09CA9 F2A4B953
  0187D068 A4277FAB FFE9FAC9 40388867 B439C684 6F57C953 DBBA8EEE C043B2F8
  09836EFF 66CF3EEF 17B35818 2509345E E3CBD614 B6ECF292 6F74E42F 812AD592
  91E0E097 3C326805 854BD1F7 57E2521D 931A549F 0570C04A 71601E43 0B601EFE
  A3CE8119 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
 supplementary-service media-renegotiate
 no supplementary-service sip 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 89898
 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
```

```
 negotiation 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-sdp-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
```

```
!
end
```

Additional References

The following sections provide references related to this feature.

Related Documents

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

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
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.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this section. For information about these commands, see the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or *Cisco IOS Master Command List, All Releases* at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **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.

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.

Table 9-4 Feature Information for Secure SIP Call Signaling and SRTP Media with Cisco SRST

Feature Name	Releases	Feature Information
Secure SIP Call Signaling and SRTP Media with Cisco SRST	15.0(1)XA	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**

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 321.

For additional information, see the "Additional References" section on page 30 in the "Cisco Unified SRST Feature Overview" section on page 1 chapter.