



Setting Up Secure SRST

Revised: January 5, 2009

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

Contents

- [Prerequisites for Setting Up Secure SRST, page 151](#)
- [Restrictions for Setting Up Secure SRST, page 152](#)
- [Information About Setting Up Secure SRST, page 153](#)
- [How to Configure Secure SRST, page 159](#)
- [Configuration Examples for Secure SRST, page 185](#)
- [Where to Go Next, page 191](#)

Prerequisites for Setting Up Secure SRST

General

- Secure Cisco Unified IP phones supported in secure SRST must have certificates installed and encryption enabled.
- 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.
- Cisco Unified Communications Manager 4.1(2) or later must be installed and must support security mode (authenticate and encryption mode).
- Certificate trust lists (CTLs) on Cisco Unified Communications Manager must be enabled. For complete instructions, see the “Configuring Secure IP Telephony Calls” procedure in the *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* document.
- Gateway routers that run secure SRST must support voice- and security-enabled Cisco IOS images (a “k9” cryptographic software image). The following two images are supported:
 - Advanced IP Services. This image includes a number of advanced security features.
 - Advanced Enterprise Services. This image includes full Cisco IOS software.

Public Key Infrastructure

- 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.

SRST

- Secure SRST services cannot be enrolled while Cisco Unified SRST is active. Therefore, disable Cisco Unified SRST with the **no call-manager-fallback** 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 [Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#) 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 4.3 Supported Firmware, Platforms, Memory, and Voice Products](#) feature.

Restrictions for Setting Up 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 e-mail 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.

- Secure SRST is supported only within the scope of a single router.

Not Supported in Secure SRST Mode

- Cisco Unified Communications Manager versions prior to 4.1(2)
- Secure music on hold (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 \(HSRP\)](#)

Supported Calls in Secure SRST Mode

Only voice calls are supported in secure 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

Information About Setting Up Secure SRST

To configure secure SRST, you should understand the following concepts:

- [Benefits of Secure SRST, page 153](#)
- [Cisco IP Phones Clear-Text Fallback During SRST, page 154](#)
- [SRST Routers and the TLS Protocol, page 154](#)
- [Cisco Unified SRST Routers and PKI, page 154](#)
- [Secure SRST Authentication and Encryption, page 156](#)
- [Cisco IOS Credentials Server on Secure SRST Routers, page 157](#)
- [Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone, page 158](#)

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 nonsecure. 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.

Cisco IP Phones Clear-Text Fallback During SRST

Cisco Unified SRST versions prior to 12.3(14)T are not capable of supporting secure connections or have security enabled. If an SRST router is not capable of secure 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 the [Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#) for more information on clear-text mode.

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 fallback 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.

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 1](#) shows the secure SRST-supported Cisco Unified IP Phones and the appropriate certificate for each phone. The [“Importing Phone Certificate Files in PEM Format to the Secure SRST Router”](#) section on page 168 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 1 **Supported Cisco Unified IP Phones and Certificates**

Cisco Unified IP Phone 7940	Cisco Unified IP Phone 7960	Cisco Unified IP Phone 7970
<p>The phone receives locally significant certificate (LSC) from Certificate Authority Proxy Function (CAPF) in Distinguished Encoding Rules (DER) format.</p> <ul style="list-style-type: none"> • 59fe77ccd.0 <p>The filename may change based on the CAPF certificate subject name and the CAPF certificate issuer.</p> <p>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.</p> <p>Manual enrollment supported only.</p>	<p>The phone receives locally significant certificate (LSC) from Certificate Authority Proxy Function (CAPF) in Distinguished Encoding Rules (DER) format.</p> <ul style="list-style-type: none"> • 59fe77ccd.0 <p>The filename may change based on the CAPF certificate subject name and the CAPF certificate issuer.</p> <p>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.</p> <p>Manual enrollment supported only.</p>	<p>The phone contains a manufacturing installed certificate (MIC) used for device authentication. If the Cisco 7970 implements MIC, two public certificate files are needed:</p> <ul style="list-style-type: none"> • CiscoCA.pem (Cisco Root CA, used to authenticate the certificate.) <p>Note The name of the manufacturing certificate can vary depending on your configuration.</p> <ul style="list-style-type: none"> • a69d2e04.0, in Privacy Enhanced Mail (PEM) format <p>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.</p> <p>Manual enrollment supported only.</p>

Secure SRST Authentication and Encryption

Figure 1 illustrates the process of secure SRST authentication and encryption, and Table 2 describes the process.

Figure 1 Secure Cisco Unified SRST Authentication and Encryption

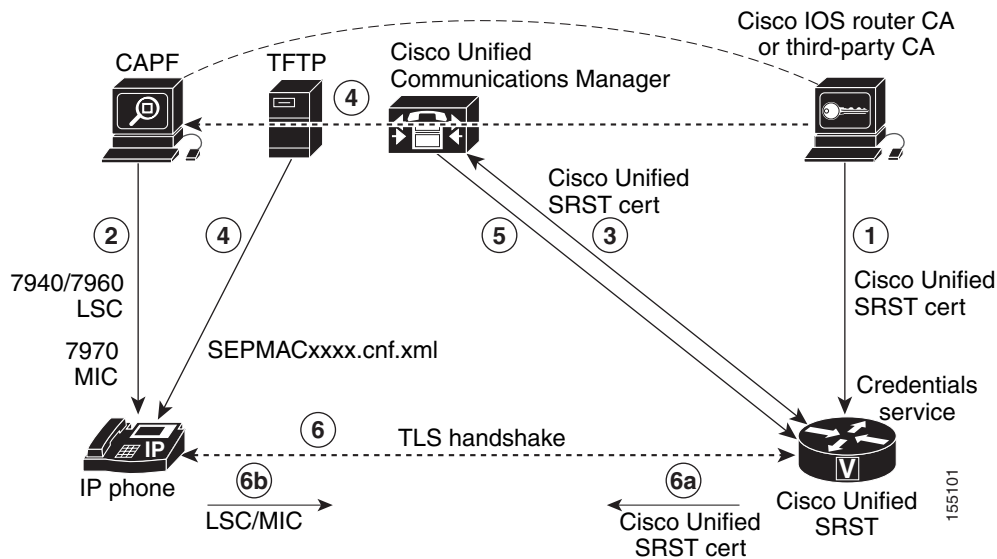


Table 2 Overview of the Process of Secure SRST Authentication and Encryption

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 the 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.
4.	For each device, Cisco Unified Communications Manager uses the TFTP process and inserts the certificate into the SEPMACxxxx.cnf.xml configuration file of the Cisco Unified IP Phone.

Table 2 Overview of the Process of Secure SRST Authentication and Encryption (continued)

Process Steps	Description or Detail
5.	<p>Cisco Unified Communications Manager 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 Unified SRST Routers and PKI, page 154 for more information.</p> <p>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.</p>
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 Communications Manager 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.

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](#)

Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone

Figure 2 and Table 3 show the interworking of the credentials server on the SRST router, Cisco Unified Communications Manager, and the Cisco Unified IP Phone, and describe the establishment of secure SRST to the Cisco Unified IP Phone.

Figure 2 *Interworking of Credentials Server on SRST Router, Cisco Unified Communications Manager, and Cisco Unified IP Phone*

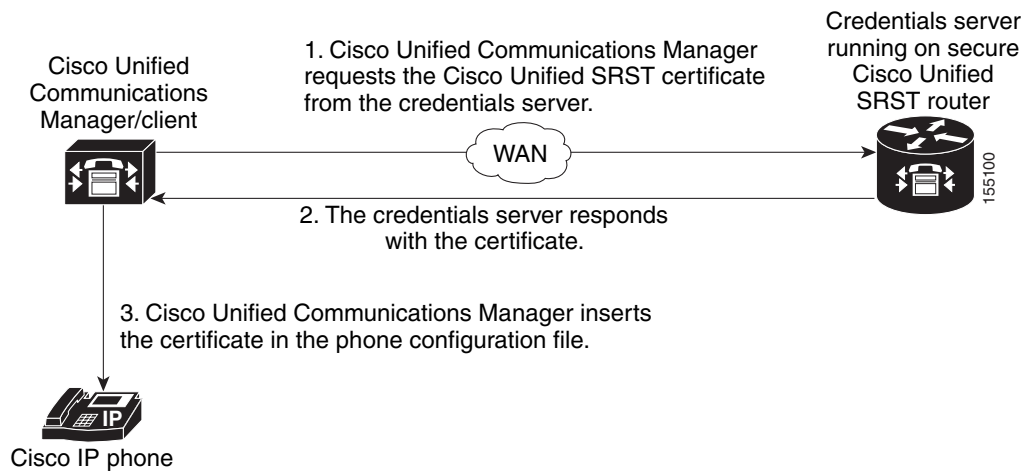


Table 3 *Establishing Secure SRST*

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 2 .
	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 2 . 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.	—
-----------	--	---

How to Configure Secure 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 159](#) (required)
- [Importing Phone Certificate Files in PEM Format to the Secure SRST Router, page 168](#) (required)
- [Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router, page 175](#) (required)
- [Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 179](#) (required)
- [Verifying Phone Status and Registrations, page 181](#) (required)

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 159](#) (optional)
- [Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 161](#) (required)
- [Disabling Automatic Certificate Enrollment, page 164](#) (required)
- [Verifying Certificate Enrollment, page 165](#) (optional)
- [Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 166](#) (required)
- [Troubleshooting Credential Settings, page 167](#) (optional)

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	<pre>crypto pki server cs-label</pre> <p>Example: Router (config)# crypto pki server srstcaserver</p>	<p>Enables the certificate server and enters certificate server configuration mode.</p> <p>Note If you manually generated an RSA key pair, the <i>cs-label</i> argument must match the name of the key pair.</p> <p>For more information on the certificate server, see the Cisco IOS Certificate Server documentation.</p>
Step 2	<pre>database level {minimal names complete}</pre> <p>Example: Router (cs-server)# database level complete</p>	<p>Controls what type of data is stored in the certificate enrollment database.</p> <ul style="list-style-type: none"> • 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. <p>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 via the database url command.</p>
Step 3	<pre>database url root-url</pre> <p>Example: Router (cs-server)# database url nvram</p>	<p>Specifies the location where all database entries for the certificate server will be written. After you create a certificate server via the crypto pki server command, use this command to specify a combined list of all the certificates that have been issued. The <i>root-url</i> argument specifies the location where database entries are written.</p> <ul style="list-style-type: none"> • The default location for the database entries to be written is flash; however, NVRAM is recommended for this task.

	Command or Action	Purpose
Step 4	issuer-name <i>DN-string</i> 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= <i>cs-label</i> .
Step 5	grant auto Example: Router (cs-server)# grant auto	Allows an automatic certificate to be issued to any requestor. <ul style="list-style-type: none"> This command is used only during enrollment and will be removed in the “Disabling Automatic Certificate Enrollment” section on page 164.
Step 6	no shutdown Example: Router (cs-server)# no shutdown	Enables the Cisco IOS certificate server. <ul style="list-style-type: none"> 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 163.

SUMMARY STEPS

1. `crypto pki trustpoint name`
2. `enrollment url url`
3. `revocation-check method1`
4. `exit`
5. `crypto pki authenticate name`
6. `crypto pki enroll name`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>crypto pki trustpoint name</code></p> <p>Example: Router(config)# <code>crypto pki trustpoint srstca</code></p>	<p>Declares the CA that your router should use and enters ca-trustpoint configuration mode.</p> <ul style="list-style-type: none"> • 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 166.
Step 2	<p><code>enrollment url url</code></p> <p>Example: Router(ca-trustpoint)# <code>enrollment url http://10.1.1.22</code></p>	<p>Specifies the enrollment parameters of your CA.</p> <ul style="list-style-type: none"> • 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, <i>url</i> must be in the form <code>http://CA_name</code>, where <i>CA_name</i> 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 159, 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 3	<p><code>revocation-check method1</code></p> <p>Example: Router(ca-trustpoint)# <code>revocation-check none</code></p>	<p>Checks the revocation status of a certificate. The argument <i>method1</i> 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.</p> <ul style="list-style-type: none"> • Using the none keyword is mandatory for this task.
Step 4	<p><code>exit</code></p> <p>Example: Router(ca-trustpoint)# <code>exit</code></p>	<p>Exits ca-trustpoint configuration mode and returns to global configuration mode.</p>

	Command or Action	Purpose
Step 5	<code>crypto pki authenticate name</code> Example: Router(config)# <code>crypto pki authenticate srstca</code>	Authenticates the CA (by getting the certificate from the CA). <ul style="list-style-type: none">• Takes the name of the CA as the argument.
Step 6	<code>crypto pki enroll name</code> Example: Router(config)# <code>crypto pki enroll srstca</code>	Obtains the SRST router certificate from the CA. <ul style="list-style-type: none">• 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 159.



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 <i>cs-label</i> Example: Router (config)# <code>crypto pki server srstcaserver</code>	Enables the certificate server and enters certificate server configuration mode. Note If you manually generated an RSA key pair, the <i>cs-label</i> argument must match the name of the key pair.
Step 2	shutdown Example: Router (cs-server)# <code>shutdown</code>	Disables the Cisco IOS certificate server.
Step 3	no grant auto Example: Router (cs-server)# <code>no grant auto</code>	Disables automatic certificates to be issued to any requestor. <ul style="list-style-type: none"> • 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)# <code>no shutdown</code>	Enables the Cisco IOS certificate server. <ul style="list-style-type: none"> • 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

Step 1 **show running-config**

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.

```
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 OCC354FB 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 EFD8D44 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 OFAB0203 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**

Use the **show crypto pki server** command to verify the status of the CA server after a boot procedure.

```
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
```

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 190.

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	Provides the Cisco Unified SRST Router certificate to Cisco Unified Communications Manager and enters credentials configuration mode.
	Example: Router(config)# credentials	

	Command or Action	Purpose
Step 2	<p>ip source-address <i>ip-address</i> [port <i>port</i>]</p> <p>Example: Router(config-credentials)# ip source-address 10.1.1.22 port 2445</p>	<p>Enables the Cisco Unified SRST Router to receive messages from Cisco Unified Communications Manager through the specified IP address and port.</p> <ul style="list-style-type: none"> • <i>ip-address</i>: The IP address is the preexisting 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	<p>trustpoint <i>trustpoint-name</i></p> <p>Example: Router(config-credentials)# trustpoint srstca</p>	<p>Specifies the name of the trustpoint that is to be associated with the Cisco Unified SRST Router certificate. The <i>trustpoint-name</i> argument is the name of the trustpoint and corresponds to the SRST device certificate.</p> <ul style="list-style-type: none"> • 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 161.
Step 4	<p>exit</p> <p>Example: Router(config-credentials)# exit</p>	<p>Exits credentials configuration mode.</p>

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

Step 1 **show credentials**

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.

```
Router# show credentials

Credentials IP: 10.1.1.22
Credentials PORT: 2445
Trustpoint: srstca
```

Step 2 debug credentials

Use the **debug credentials** command to set debugging on the credential settings of the Cisco Unified SRST Router.

```
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.
```

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 1 on page 155](#) 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 of the contents that appear between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”.

Cisco Unified Communications Manager 5.0 and Later Versions

Systems running Cisco Unified Communications Manager 5.0 and later versions require four certificates (CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048) in addition to the requirements listed in [Table 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 Communications Manager 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 of 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 the [Cisco Unified Communications Operating System Administration Guide](#).

Authenticating 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 <i>name</i> Example: Router (config)# crypto pki trustpoint CAPF	Declares the CA that your router should use and enters ca-trustpoint configuration mode. <ul style="list-style-type: none"> • <i>name</i>: 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. <ul style="list-style-type: none"> • 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 <i>name</i> Example: Router(config)# crypto pki authenticate CAPF	Authenticates the CA (by getting the certificate from the CA). <ul style="list-style-type: none"> • Enter the same <i>name</i> argument used in the crypto pki trustpoint command in Step 1.

What to Do Next

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

Examples

This section provides the following:

- [Cisco Unified Communications Manager 4.X.X and Earlier Versions: Example, page 171](#)
- [Cisco Unified Communications Manager 5.0 and Later Versions Example, page 174](#)

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

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

```
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
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtU1RQLTAwMjAe
Fw0wMzEwMTAyMDE4NDIaFw0yMzEwMTAyMDI3MzdaMC4xZjAUBgNVBAoTUDNpc2Nv
IFN5c3R1bXMxPDASBgNVBAMTC0NBUC1SVFAtMDAyMIIBIDANBgkqhkiG9w0BAQEFA
AAOCAQ0AMIIBCAKCAQEACZlBK19w/2NZVVvpjCPrpW1cCY7V1q91hzI85RZZdnQ
2M4CufgIzNa3zYxGJIAYefcRECnMB3f5A+x7xNiEuzE87UPvK+7S80uWCY0Uht1
AVVf5NQgZ3YDN0NXg5MmONb81T86F55EzYVac0XGne77TSIbIdejrTgYQXGP2MJx
Qhg+ZQ1GFDRzbHfM84Duv2Msez+l+SqmQ080kIckqE9Nr3/XCSj1hXZNNVg8D+mv
Hth2P6KZqAKXAAStGRLSZX3jNbS8tveJ3Gi5+s9+F6KKK2PD0iDwHcRkKcUHb7g
lI++U/5nswjUDIaph715Ds2rn9ehkMGipGLF8kpuCwIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpIr4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2Nhcn1yZHAtdMDAyL0N1cnRF
bnJvbGwvQ0FQLVJUUC0wMDIuY3JshI9maWx1oi8vXFxjYXAtcnRwLTAwM1xDZXJ0
RW5yb2xsXENBUC1SVFAtMDAyLmNyYbDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLNWip2vDRihm
E+DlXdWMS5JaQutuaSd/m/xzxpCRJm4ZRRwPq6VeaiiQGkjFuZEe5jSKiSAK7eHg
tup4HP/ZfKSwPA40D1sGSYsKNMm3OmVOCQUMH021PkS/eEQ9sIw6QS7uuHN4y4CJ
NPnRbpfRLw06hnStCZHtGpKEHnY213QOy3h/EWhbnp0MZ+hdr20FujSI6G1+L391
arjeD708f2fYoz9wnEpZb2bn2Kzse3uhU1Ygq1D1x9yuPq388C18HWdmCj4OVTXux
V6Y47Hlyv/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
GjAYBgNVBAoTEUNpc2NvIFN5c3R1bXMgSW5jMRUwEwYDVQQDEwxDQVBLTDEEN0Qw
QzAwHhcNMDQwNzE1MjIzODMyWhcNMjkwNzEyMjIzODMxWjBAMQswCQYDVQQGEwJV
UzEaMBGGA1UEChMRQ2lyZ28gU3lzdGVTcyBJbMxFTATBgNVBAMTDENBUEYtN0Q3
RDBDMDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA0hvMOZZ9ENYwme11YGY1
it2rvE3Nk/eqhnv8P9eqBliqt+fFBeAG0WZ5b05FetdU+BCmPnddvAeSpsfr3Z+h
x+r58fOEIIBRHQLgmDZ+nwYH39uwXcRWWqWw1W147YHjV7M5c/R8T6daCx4B5NB06
kdQdQNOv3IP7kQaCShdM/kCAwEAAAMxMC8wDgYDVR0PAQH/BAQDAgKEMB0GA1Ud
JQQwMBQGCCsGAQUFBwMBBggrBgEFBQcDBTANBgkqhkiG9w0BAQUFAAOBgQCaNi6x
sL6M5N1DezpSB03QmUVyXmFRONV2ysrSwcXzHu0gJ9MSJ8TwiQmVaJ47hST1F5a8
YVYJ0IdifXbXR0+/EE07kkmFE8MZta5rM7UWj8bAeR42iqA3RzQaDwuJgNWT9Fhh
GgfuaAlo5h1Aikxsxvixvmd1LdZyCMoqJd7B2Q==

```

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
MIIDqDCCApCgAwIBAgIQdhL5YBU9b590QiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZWlzMRRwEgYDVQQDEwtdQVAtU1RQLTAwMTAe
Fw0wMzAyMDYyMzI3MTNaFw0yMzAyMDYyMzI3MzRaMC4xFTJjAUBGNVBAoTDUNpc2Nv
IFN5c3R1bXMxZDAsBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCjQAwGyKCGYEA0hvMOZZ9ENYwme11YGY1it2rvE3Nk/eqhnv8P9eq
Bliqt+fFBeAG0WZ5b05FetdU+BCmPnddvAeSpsfr3Z+hx+r58fOEIIBRHQLgmDZ+
nwYH39uwXcRWWqWw1W147YHjV7M5c/R8T6daCx4B5NB06kdQdQNOv3IP7kQaCShdM/
kCAwEAAAMxMC8wDgYDVR0PAQH/BAQDAgKEMB0GA1UdJQQwMBQGCCsGAQUFBwMBBggr
BgEFBQcDBTANBgkqhkiG9w0BAQUFAAOBgQCaNi6xsL6M5N1DezpSB03QmUVyXmFRONV2
ysrSwcXzHu0gJ9MSJ8TwiQmVaJ47hST1F5a8YVYJ0IdifXbXR0+/EE07kkmFE8MZta5r
M7UWj8bAeR42iqA3RzQaDwuJgNWT9FhhGgfuaAlo5h1Aikxsxvixvmd1LdZyCMoqJd7B2Q
==

```

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
```


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 166.

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 Communications Manager administration guides are at the following URL:

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

SUMMARY STEPS

1. Choose **SRST** in the Cisco Unified Communications Manager menu bar.
2. Add a new SRST reference.
3. Enter the appropriate settings in the SRST fields.
4. Click **Insert**.
5. Repeat Steps 2 to 4 for additional SRST references.

DETAILED STEPS

-
- 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 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 3 SRST Reference Configuration Window

The screenshot shows the 'SRST Reference Configuration' window in Cisco CallManager Administration. The window has a navigation bar at the top with 'System', 'Route Plan', 'Service', 'Feature', 'Device', 'User', 'Application', and 'Help'. The main content area is yellow and contains the following fields and controls:

- SRST Reference:** New
- Status:** Ready
- Buttons:** Insert, Cancel
- SRST Reference Name*:** SRST Gateway
- IP Address*:** 10.1.1.22
- Port*:** 2000
- Is SRST Secure?**
- SRST Certificate Provider Port*:** 2445
- Footnote:** * indicates required item

Links at the top right include 'Add New SRST Reference' and 'Back to Find/List SRST References'. A vertical ID '127020' is on the right edge.

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 device pool to SRST.

For complete information about adding a device pool to Cisco Unified Communications Manager, see the “Device Pool Configuration” section in the *Cisco Unified Communications Manager Administration Guide* for the Cisco Unified Communications Manager version that you are running. All Cisco Unified Communications Manager administration guides are at the following URL:

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

SUMMARY STEPS

1. Choose **Device Pool** in the Cisco Unified Communications Manager menu bar.
2. Add a device pool.
3. Click **Add New Device Pool**.
4. Enter the SRST reference.
5. Click **Update**.

DETAILED STEPS

- 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 4](#)).

Figure 4 Device Pool Configuration Window

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Device Pool Configuration

[Add new Device Pool](#)
[Back to Find/List Device Pools](#)
[Dependency Records](#)

Device Pool: Default (13 members**)
Status: Ready

Copy Update Delete Reset Devices

Device Pool Settings

Device Pool Name*	Default
Cisco CallManager Group*	Default
Date/Time Group*	CMLocal
Region*	Default
Softkey Template*	Standard User
SRST Reference*	jaso2691
Calling Search Space for Auto-registration	— Not Selected — Disable Use Default Gateway jaso2691
Media Resource Group List	SRST GW
Network Hold MOH Audio Source	
User Hold MOH Audio Source	< None >
Network Locale	< None >

127021

- 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 Communications Manager, to request LSC certificates from Cisco Unified IP Phones. 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 <i>digit-string</i> Example: Router(config-cm-fallback)# secondary-dialtone 9	Activates a secondary dial tone when a digit string is dialed.

	Command or Action	Purpose
Step 3	<p>transfer-system {blind full-blind full-consult local-consult}</p> <p>Example: Router(config-cm-fallback)# transfer-system full-consult</p>	<p>Defines the call-transfer method for all lines served by the Cisco Unified SRST Router.</p> <ul style="list-style-type: none"> • 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	<p>ip source-address <i>ip-address</i> [port <i>port</i>]</p> <p>Example: Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000</p>	<p>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.</p>
Step 5	<p>max-ephones <i>max-phones</i></p> <p>Example: Router(config-cm-fallback)# max-ephones 15</p>	<p>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 37 for further details.</p>
Step 6	<p>max-dn <i>max-directory-numbers</i></p> <p>Example: Router(config-cm-fallback)# max-dn 30</p>	<p>Sets the maximum number of directory numbers (DNs) or virtual voice ports that can be supported by the router.</p> <ul style="list-style-type: none"> • <i>max-directory-numbers:</i> 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 37 for further details.
Step 7	<p>transfer-pattern <i>transfer-pattern</i></p> <p>Example: Router(config-cm-fallback)# transfer-pattern</p>	<p>Allows transfer of telephone calls by Cisco Unified IP Phones to specified phone number patterns.</p> <ul style="list-style-type: none"> • <i>transfer-pattern:</i> String of digits for permitted call transfers. Wildcards are allowed.
Step 8	<p>exit</p> <p>Example: Router(config-cm-fallback)# exit</p>	<p>Exits call-manager-fallback configuration mode.</p>

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
```

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.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show ephone**

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 SRST. In this example, authentication and encryption status is active with a TLS connection.

```
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
```

Step 2 **show ephone offhook**

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.

```
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
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
```

Step 3 show voice call status

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.

```
Router# show voice call status
```

```
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
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

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

```
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

```

Step 5 debug ephone state

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.

```
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
*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

```

```

*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 SRST

This section provides the following configuration examples.

- [Secure SRST: Example, page 185](#)
- [Control Plane Policing: Example, page 190](#)



Note

IP addresses and hostnames in examples are fictitious.

Secure 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 0AED1E10
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 BOBBB2D4 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 98BCE2B1 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
F5E5CDFD 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
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
.
.
.
```

Where to Go Next

If you require voice mail, see the voice-mail configuration instructions in the [“Integrating Voice Mail with Cisco Unified SRST”](#) section on page 191. You may also want to read the [“Monitoring and Maintaining Cisco Unified SRST”](#) section on page 223.

