



## Configuring SIP Support for SRTP

---

This chapter contains information about the SIP Support for SRTP feature. The Secure Real-Time Transfer protocol (SRTP) is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two SIP endpoints.

You can use the **secure RTP** command to configure secure RTP calls. You can configure the **secure RTP** command on individual dial peer, or globally for all calls entering the gateway. If an endpoint does not support SRTP, you can configure a fallback to RTP, or you can fail the call.

### Feature History for SIP Support for SRTP

Release	Modification
12.4(15)T	This feature was introduced.

## Contents

- [Prerequisites for SIP Support for SRTP, page 483](#)
- [Information About SIP Support for SRTP, page 484](#)
- [How to Configure SIP Support for SRTP, page 489](#)
- [Configuring SIP Support for SRTP on a Dial Peer, page 493](#)
- [Additional References, page 495](#)

## Prerequisites for SIP Support for SRTP

- Establish a working IP network. For information on configuring IP, see the [Cisco IOS IP Configuration Guide](#), Release 12.3.
- Ensure that the gateway has voice functionality that is configurable for SIP.
- Ensure Transport Layer Security (TLS) is configured for secure SIP signaling.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Information About SIP Support for SRTP

The SIP Support for SRTP feature uses SRTP to secure the media flow between two SIP endpoints. The gateway uses the Digest method for user authentication, and Transport Layer Security (TLS) for signaling authentication and encryption. The required cryptographic parameters, for the SRTP to successfully negotiate, use the cryptographic attribute in the Session Description protocol (SDP). To ensure the integrity of cryptographic parameters across a network, SRTP uses the SIPS schema (sips:example.com). If an endpoint cannot provide TLS support, the endpoint rejects an INVITE message from a gateway that is using the sips schema. You can configure a gateway to either fallback to an RTP-only call, or to reject the call.

The SIP Support for SRTP feature supports the following:

- Confidentiality of RTP packets—protects packet-payloads from being read by entities without entering a secret encryption key.
- Message authentication of RTP packets—protects the integrity of the packet against forgery, alteration, or replacement.
- Replay protection—protects the session address against denial of service attacks.

Table 44 summarizes the different combinations when using both TLS and SRTP.

**Table 44**      **TLS-SRTP Combinations**

TLS	SRTP	Description
On	On	Signaling and media are secure.
Off	On	Signaling is insecure. If you use the <b>secure RTP fallback</b> command, the gateway sends an RTP-only SDP. If you do not configure the <b>secure RTP fallback</b> command, the call fails and the gateway does not send an INVITE message.
On	Off	RTP-only call.
Off	Off	Signaling and media are not secure.

## Cryptographic Parameters

RFC 3711 defines the SRTP cryptographic parameters, including valid syntax and values for attribute **a=crypto**. Some of these parameters are declarative and only apply to the send direction of the declarer, while others are negotiable and apply to both send and receive directions.

The following shows the cryptographic attribute syntax:

```
a=crypto:<tag> <crypto-suite> <key-params> [<session-params>]
```

Table 45 summarizes the syntax for the cryptographic attribute.

**Table 45** Cryptographic Attribute Syntax

Attribute	Optional	Description
tag	No	A unique decimal number used as an identifier for a particular cryptographic attribute to determine which of the several offered cryptographic attributes was chosen by the answerer.
crypto-suite	No	Defines the encryption and authentication algorithm. The gateway supports default suite AES_CM_128_HMAC_SHA1_32 which uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag.
key-params	No	“inline:” <keyl  salt> [“l” lifetime] [“l” MKI “:” length] keyl   salt is base64 encoded contacted master key and salt.
session-params	Yes	The session-params are specific to a given transport and is optional. The gateway does not generate session-params in an outgoing INVITE message, nor will the SDP library parse them.

## SDP Negotiation

To operate with endpoints that do not support SRTP, you can configure the gateway to use SRTP only with fallback to the RTP mechanism. If you configure the **securertp fallback** command on a dial peer or globally, the offer SDP in the INVITE message has only one m lines for the RTP/SAVP transport type. If the called endpoint does not support SRTP, the calls fails with a 4xx error. If you configure the **securertp fallback** command, the gateway generates another INVITE message with an RTP-only offer. If you do not configure fallback to RTP, the call fails.

When a gateway is the called end, the gateway accepts an offer with an m line with SRTP only, RTP only, or both SRTP and RTP. For calls with two m lines (SRTP and RTP), the negotiation depends on the configuration of the inbound dial peer or global configuration. Only one m line negotiates, and the port number in other m line is set to 0.

Table 46 summarizes the behavior of the gateway during negotiation.

**Table 46** Gateway Behavior During Negotiations

Dial Peer Configuration	INVITE Received with SRTP	INVITE Received with SRTP and RTP	INVITE Received with RTP
SRTP Only	SRTP call	SRTP call, port number in m line of RTP set to 0.	488 (Unacceptable media).
SRTP with fallback	SRTP call	SRTP call, port number in m line of RTP set to 0.	RTP call, port number in m line of SRTP set to 0.
No SRTP	488 (Unacceptable media)	RTP call, port number in m line of SRTP set to 0.	RTP call.

The following example shows an offer SDP with two m lines that use the cryptographic attribute for the RTP/SAVP media transport type.

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 1789 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 51372 RTP/SAVP 0
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHawJSoj|2^20|1:32
```

The following example shows the corresponding answer SDP with SRTP supported:

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 0 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 49170 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
```

## Call Control and Signaling

SIP uses the SRTP library to receive cryptographic keys. If you configure SRTP for the call and cryptographic context is supported, SDP offers the cryptographic parameters. If the cryptographic parameters are negotiated successfully, the parameters are downloaded to the DSP, which encrypts and decrypts of the packets. The sender encrypts the payload by using the AES algorithm and builds an authentication tag which is encapsulated to the RTP packet. The receiver verifies the authentication tag and then decrypts the payload.

## Default SRTP Settings

[Table 47](#) summarizes the recommended SRTP settings.

**Table 47** Recommended SRTP Settings

Parameter	Default	Recommended Value
SRTP cipher	AES_CM	AES_CM
SRTCP cipher	AES_CM	NULL
SRTP authentication	HMAC-SHA1	HMAC-SHA1
SRTCP authentication	HMAC-SHA1	HMAC-SHA1
SRTP HMAC tag length	80	32 (voice)—Supported 80 (other)—Not supported
SRTCP HMAC tag length	80	80
SRTP replay-window size	64	64—Not supported

Parameter	Default	Recommended Value
SRTCP replay-window size	64	64—Not supported
PRF	AES_CM	
Master key length	128 bits	128 bits
Master salt key length	112 bits	112 bits
Session encryption key length	128 bits	128 bits
Session authentication key length	128	128
Session salt key length	112	112
Key derivation rate	0	0—Rekeying is supported
SRTP packets maximum lifetime	2 <sup>48</sup> packets	2 <sup>48</sup> packets
SRTCP packets maximum lifetime	2 <sup>31</sup> packets	2 <sup>31</sup> packets
MKI indicator	0	0
MKI length	0	0

To establish an SRTP session, the following cryptographic information must be exchanged between two endpoints in SDP.

- Crypto suite—crypto algorithm {AES\_CM\_128\_HMAC\_SHA1\_32} and the supported codec list {g711, G729, G729a}. There could be one or more crypto suites. Cisco IOS Release 12.4(6th)T only supports one crypto suite.
- Crypto context—16-byte master key and a 14-byte master salt.

## Generating Master Keys

The SRTP library provides an API, `srtp_generate_master_key`, to generate a random master key. For encryption and authentication purposes, the key length is 128 bits (master key and session keys). The master salt and session salts are 112-bits wide.

## SRTP Offer and Answer Exchange

If you configure the gateway for SRTP (on a dial peer or global configuration level) and end-to-end TLS, an outgoing INVITE message has cryptographic parameters in the SDP.

If you use the **secrtrtp fallback** command and if the called endpoint does not support SRTP (offer is rejected with a 4xx class error response), the gateway sends an RTP-offer SDP in a new INVITE request. If you do not use the **secrtrtp fallback** command to configure fallback, the call fails.

When the gateway receives an SRTP offer, negotiation is based on the inbound dial-peer or global configuration. If multiple cryptographic attributes are offered, the gateway selects an STP offer it supports (AES\_CM\_128\_HMAC\_SHA1\_32). The cryptographic attribute in the answer includes the following:

- The tag and same crypto-suite from the accepted cryptographic attribute in the offer
- A unique key the gateway generates from the SRTP library API.
- Any negotiated session parameters and its own set of declarative parameters, if any.

If this cryptographic suite is not in the list of offered attributes, or if none of the attributes are valid, the SRTP negotiation fails. If the INVITE message contains an alternative RTP offer, it negotiates and the call falls back to unsecured-RTP mode. If there is no alternative offer and the SRTP negotiation fails, the INVITE message is rejected with a 488 error (Not Acceptable Media).

## Rekeying Rules

There is no rekeying on an SRTP stream. REINVITE/UPDATE is used in an established SIP call to update media-related information (codec, destination address, and port number) or other features, such as call-hold, and so on. A new key needs to be generated if the offer SDP has a new connection address or port. Because the source connection address and port for the gateway do not change, the gateway will not generate a new master key once a key has been established for an SRTP session.

## Call-Feature Interactions

This section describes call-feature interactions when using the SIP Support for SRTP feature.

### Call Hold

If a gateway receives a call hold REINVITE message after an initial call setup is secured, the gateway places the existing SRTP stream on hold, and its answer in the 200 OK message depends on the offer SDP. If there is a cryptographic attribute in the offer, the gateway responds with a cryptographic attribute in its answer.

### Signaling Forking

A proxy can fork an INVITE message that contains an SRTP offer, which can result in multiple SRTP streams until a 200 OK message is received. Because the gateway always honors the last answer, the gateway deletes previous SRTP streams and creates a new stream to the latest endpoint. Other endpoints might also stream to the gateway, but since the DSP knows only the last streams's cryptographic suite and key, authentication on these packets fails, and the packets are dropped.

### Call Redirection

A gateway redirects a call when an INVITE message, sent to a proxy or redirect server, results in a 3xx response with a list of redirected contact addresses. The gateway handles a 3xx response based on the schema in the contact of a 3xx message. If the message is SIP, and you configure the call for SRTP with fallback, the gateway offers an SRTP-only redirected INVITE message. If you configure for SRTP only, the offer is SRTP only.

If the schema is SIP, and you use the **securertp fallback** command to configure the call for RTP with fallback, the INVITE message has an RTP offer. If you do not configure the **securertp fallback** command, the call fails.

### Call Transfer

The SIP Support for SRTP feature interaction with call transfer depends on your outbound dial peer or global configuration. During a call transfer, the gateway sends an INVITE message to establish the connection to the transfer-target. The gateway includes an SRTP offer in the INVITE message if the outbound dial-peer or global configuration includes the SRTP offer.

## T.38 Fax

The T.38 transport currently supported is UDP. A T.38 call initiates as a voice call, which can be RTP or SRTP, and when it switches to T.38 fax mode, the fax call is not secure. When the fax is switched back to voice, the call returns to its initial voice state.

## Conferencing Calls

For conferencing calls, the incoming INVITE message does not match any inbound dial peer and the message body is sent to the application in a container. The conferencing application performs the necessary negotiation and replies through PROGRESS or CONNECT events.

# How to Configure SIP Support for SRTP

To configure SIP support for SRTP, you must first configure SIPS globally for all calls entering a gateway, or on an individual dial peer basis. You can then configure support for SRTP globally for all call entering a gateway, or on an individual dial peer. The configuration on a dial peer overrides any global configuration.

This section contains the following configurations:

- [Configuring SIPS Globally on a Gateway, page 489](#)
- [Configuring SIPS on a Dial Peer, page 490](#)
- [Configuring SIP Support for SRTP Globally on a Gateway, page 492](#)
- [Configuring SIP Support for SRTP on a Dial Peer, page 493](#)

## Configuring SIPS Globally on a Gateway

To configure SIPS globally on a gateway, follow these steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service { pots | voatm | vofr | voip }**
4. **sip**
5. **url sips**
6. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice service {pots   voatm   vofr   voip}</b>  <b>Example:</b> Router(config)# voice service voip	Enters voice-service voip configuration mode.
Step 4	<b>sip</b>  <b>Example:</b> Router(conf-voi-ser)# sip	Enters SIP configuration mode.
Step 5	<b>url sips</b>  <b>Example:</b> Router(conf-ser-sip)# url sips	Generates URLs in SIPS format for VoIP calls.
Step 6	<b>exit</b>  <b>Example:</b> Router (conf-ser-sip)# exit	Exits the current mode.

## Configuring SIPS on a Dial Peer

To configure SIPS on a dial peer, follow these steps:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice <tag> {pots | vofr | voip}**
4. **voice-class sip**
5. **sip**
6. **url sips**
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>dial-peer voice &lt;tag&gt; {pots   vofr   voip}</b>  <b>Example:</b> Router(config)# dialpeer voice 111 voip	Enters dial-peer voip configuration mode.
Step 4	<b>voice-class sip</b>  <b>Example:</b> Router(conf-dial-peer)# voice-class sip	Enters SIP parameters mode.
Step 5	<b>sip</b>  <b>Example:</b> Router(conf-dial-peer)# sip	Enters SIP configuration mode.
Step 6	<b>url sips</b>  <b>Example:</b> Router(conf-ser-sip)# url sips	Generates URLs in SIPS format for VoIP calls.
Step 7	<b>exit</b>  <b>Example:</b> Router (conf-ser-sip)# exit	Exits the current mode.

## Configuring SIP Support for SRTP Globally on a Gateway

To configure SIP support for SRTP globally on a gateway, follow these steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service { pots | voatm | vofr | voip }**
4. **sip**
5. **securertc**
6. **securertc fallback**
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice service</b> {pots   voatm   vofr   voip}  <b>Example:</b> Router(config)# voice service voip	Enters voice-service voip configuration mode.
Step 4	<b>securertp</b>  <b>Example:</b> Router(conf-voi-ser)# securertp	Configures secure RTP calls.
Step 5	<b>securertp fallback</b>  <b>Example:</b> Router(conf-ser-sip)# securertp fallback	Configures a fallback to RTP calls in case secure RTP calls fail due to lack of support from an endpoint.
Step 6	<b>exit</b>  <b>Example:</b> Router (conf-ser-sip)# exit	Exits the current mode.

## Configuring SIP Support for SRTP on a Dial Peer

To configure SIP support for SRTP on a dial peer, follow these steps:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** <tag> {pots | vofr | voip}
4. **voice-class sip**
5. **securertp**
6. **securertp fallback**
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>dial-peer voice &lt;tag&gt; {pots   vofr   voip}</b>  <b>Example:</b> Router(config)# dialpeer voice 111 voip	Enters dial-peer voip configuration mode.
Step 4	<b>voice-class sip</b>  <b>Example:</b> Router(conf-dial-peer)# voice-class sip	Enters SIP parameters mode.
Step 5	<b>secure RTP</b>  <b>Example:</b> Router(conf-dial-peer)# secure RTP	Configures secure RTP calls.
Step 6	<b>secure RTP fallback</b>  <b>Example:</b> Router(conf-ser-sip)# secure RTP fallback	Configures a fallback to RTP calls in case secure RTP calls fail due to lack of support from an endpoint.
Step 7	<b>exit</b>  <b>Example:</b> Router (conf-ser-sip)# exit	Exits the current mode.

## Configuration Examples for SIP Support for SRTP

The following example shows how to configure for SRTP with fallback to RTP globally on a gateway:

```
gateway> enable
gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)# voice service voip
gateway(conf-voi-serv)# secure RTP
gateway(conf-voi-serv)# secure RTP fallback
gateway(conf-ser-sip)# exit
```

The following example shows how to configure for SRTP with fallback to RTP on a dial peer:

```
gateway> enable
gateway# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)# dial-peer voice 111 voip
```

```

gateway(conf-dial-peer)# voice-class sip
gateway(conf-dial-peer)# securertp
gateway(conf-dial-peer)# securertp fallback
gateway(conf-dial-peer)# exit

```

## Additional References

The following sections provide references related to the SIP Support for SRTP feature.

### RFCs

RFC	
RFC 3711	The Secure Real-Time Transport Protocol (SRTP) draft-ietf-mmusic-sdescriptions-08.txt

### MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

