Configuring SIP Support for SRTP

This module contains information about configuring Session Initiation Protocol (SIP) support for the Secure Real-time Transport Protocol (SRTP). SRTP is an extension of the Real-time Transport Protocol (RTP) Audio/Video Profile (AVP) and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets that provide authentication, encryption, and the integrity of media packets between SIP endpoints.

SIP support for SRTP was introduced in Cisco IOS Release 12.4(15)T.

You can configure the handling of secure RTP calls on both a global level and on an individual dial peer basis on Cisco IOS voice gateways. You can also configure the gateway (or dial peer) either to fall back to (nonsecure) RTP or to reject (fail) the call for cases where an endpoint does not support SRTP.

The option to allow negotiation between SRTP and RTP endpoints was added for Cisco IOS Release 12.4(20)T and later releases, as was interoperability of SIP support for SRTP on Cisco IOS voice gateways with Cisco Unified Communications Manager. In Cisco IOS Release 12.4(22)T and later releases, you can configure SIP support for SRTP on Cisco Unified Border Elements (Cisco UBEs).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring SIP Support for SRTP

- Establish a working IP network and configure VoIP.

Note For information about configuring VoIP, see "Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms".

- Ensure that the gateway has voice functionality configured for SIP.
- Ensure that your Cisco router has adequate memory.
- As necessary, configure the router to use Greenwich Mean Time (GMT). SIP requires that all times be sent in GMT. SIP INVITE messages are sent in GMT. However, the default for routers is to use Coordinated Universal Time (UTC). To configure the router to use GMT, issue the **clock timezone** command in global configuration mode and specify GMT.

Restrictions for Configuring SIP Support for SRTP

- The SIP gateway does not support codecs other than those listed in the table titled “SIP Codec Support by Platform and Cisco IOS Release” in the “Enhanced Codec Support for SIP Using Dynamic Payloads” section of the "Configuring SIP QoS Features" module.
- SIP requires that all times be sent in GMT.

Information About Configuring SIP Support for SRTP

The SIP Support for SRTP features use encryption to secure the media flow between two SIP endpoints. Cisco IOS voice gateways and Cisco Unified Border ElementsCisco Unified Border Elements use the Digest method for user authentication and, typically, they use Transport Layer Security (TLS) for signaling authentication and encryption.

Note To provide more flexibility, TLS signaling encryption is no longer required for SIP support of SRTP in Cisco IOS Release 12.4(22)T and later releases. Secure SIP (SIPS) is still used to establish and determine TLS but TLS is no longer a requirement for SRTP, which means calls established with SIP only (and not SIPS) can still successfully negotiate SRTP without TLS signaling encryption. This also means you could configure encryption using a different protocol, such as IPsec. However, Cisco does not recommend configuring SIP support for SRTP without TLS signaling encryption because doing so compromises the intent of forcing media encryption (SRTP).

When TLS is used, the cryptographic parameters required to successfully negotiate SRTP rely on 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 the Cisco IOS voice gateway or Cisco Unified Border Element is configured to use TLS encryption and sends an invite to an endpoint that

cannot provide TLS support, that endpoint rejects the INVITE message. For cases like these, you can configure the gateway or Cisco Unified Border Elements either to fall back to an RTP-only call or to reject the call.

The SIP support for SRTP features provide the following security benefits:

- Confidentiality of RTP packets--protects packet-payloads from being read by unapproved entities but does so without authorized entities having to enter 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.

The table below describes the security level of SIP INVITE messages according to which of the four possible combinations of TLS and SRTP is configured.

Table 1: TLS-SRTP Combinations

TLS	SRTP	Description
On	On	Signaling and media are secure.
Off	On	Signaling is insecure: • If you use the **srtp fallback** command, the gateway sends an RTP-only SDP. • If you do not configure the **srtp fallback** command, the call fails and the gateway does not send an INVITE message. **Note** In Cisco IOS Release 12.4(20)T and later releases (and, for Cisco UBEs, in Cisco IOS Release 12.4(22)T and later releases), calls established with SRTP only (and not SIPS) will succeed even if the **srtp fallback** command is not configured.
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 (see the table below). Some of these parameters are declarative and apply only 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>]

The table below summarizes the syntax for the cryptographic attribute.

Table 2: Cryptographic Attribute Syntax

Attribute	Optional	Description
tag	No	The tag attribute is 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	The crypto-suite attribute defines the encryption and authentication algorithm. Cisco IOS voice gateways and Cisco UBEs support default suite AES_CM_128_HMAC_SHA1_32 (AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag).
key-params	No	“inline:” <key| |salt> [“|” lifetime] [“|” MKI “:” length] key| | salt is base64 encoded contacted master key and salt.
session-params	Yes	The session-params attribute is specific to a given transport and is optional. The gateway does not generate any session-params in an outgoing INVITE message, nor will the SDP library parse them.

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 DP, which encrypts and decrypts 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 and Recommended SRTP Settings

The table below lists the default and recommended SRTP settings.

Table 3: Default and Recommended SRTP Settings

Parameter	Default	Recommended Value
Key derivation rate	0	0--Rekeying is supported
Master key length	128 bits	128 bits
Master salt key length	112 bits	112 bits
MKI indicator	0	0
MKI length	0	0
PRF	AES_CM	128
Session authentication key length	128	128
Session encryption key length	128 bits	128 bits
Session salt key length	112	112

Parameter	Default	Recommended Value
SRTP authentication	HMAC-SHA1	HMAC-SHA1
SRTCP authentication	HMAC-SHA1	HMAC-SHA1
SRTP cipher	AES_CM	AES_CM
SRTCP cipher	AES_CM	NULL
SRTP HMAC tag length	80	32 (voice)--Supported 80 (other)--Not supported
SRTCP HMAC tag length	80	80
SRTP packets maximum lifetime	2^48 packets	2^48 packets
SRTCP packets maximum lifetime	2^31 packets	2^31 packets
SRTP replay-window size	64	64--Not supported
SRTCP replay-window size	64	64--Not supported

Before an SRTP session can be established on a Cisco IOS voice gateway or Cisco UBE, the following cryptographic information must be exchanged in SDP between the two endpoints:

- 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(15)T supports only one crypto suite.
- Crypto context--16-byte master key and a 14-byte master salt.

Generating Master Keys

The SRTP library provides an application program interface (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). Additionally, RFC 3711 introduces “salting keys”--master salts and sessions salts--and strongly recommends the use of a master salt in the key derivation of session keys. The salting keys (salts) are used to fight against pre-computation and time-memory tradeoff attacks.

The master salt (also known as the n-bit SRTP key) prevents off-line key-collision attacks on the key derivation and, when used, must be random (but can be public). The master salt is derived from the master key and is used in the key derivation of session keys. Session salts, in turn, are used in encryption to counter various attacks against additive stream ciphers. All salting keys (master salt and session salts) are 112 bits.

SRTP Offer and Answer Exchange

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

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

Note In Cisco IOS Release 12.4(20)T and later releases (and, for Cisco UBEs, in Cisco IOS Release 12.4(22)T and later releases), calls established with SRTP only (and not SIPS) will succeed even if the **srtp fallback** command is not configured.

When a gateway or Cisco Unified Border Element receives an SRTP offer, negotiation is based on the inbound dial peer if specified and, if not, the global configuration. If multiple cryptographic attributes are offered, the gateway selects an SRTP offer it supports (AES_CM_128_HMAC_SHA1_32). The cryptographic attribute will include 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, the gateway or Cisco Unified Border Element negotiates and the call falls back to (nonsecure) 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. A REINVITE/UPDATE message 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. A new key need only be generated if the offer SDP has a new connection address or port. Because the source connection address and port do not change, the gateway or Cisco Unified Border Element will not generate a new master key after a key has been established for an SRTP session.

Call-Feature Interactions

This section describes call-feature interactions when SIP Support for SRTP features are configured.

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 because 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 **srtp fallback** command to configure the call for RTP with fallback, the INVITE message has an RTP offer. If you do not configure the **srtp fallback** command, the call fails.

Note In Cisco IOS Release 12.4(20)T and later releases (and, for Cisco UBEs, in Cisco IOS Release 12.4(22)T and later releases), calls established with SRTP only (and not SIPS) will succeed even if the **srtp fallback** command is not configured.

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 supported is User Datagram Protocol (UDP). A T.38 call is initiated 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

Before configuring SIP support for SRTP on a gateway or Cisco Unified Border Element, it is strongly recommended you first configure SIPS either globally or on an individual dial peer basis. The configuration on a dial peer overrides the global configuration.

Configuring SIPS Globally

To configure secure SIP (SIPS) globally on a Cisco IOS voice gateway or Cisco Unified Border Element, perform the following 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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service** {**pots** | **voatm** | **vofr** | **voip**} **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**url sips** **Example:** `Router(conf-serv-sip)# url sips`	Specifies generation of URLs in SIPS format for VoIP calls for all dial peers on the voice gateway or Cisco UBE.
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

Configuring SIPS on a Dial Peer

To configure secure SIP (SIPS) on an individual dial peer, perform the following steps.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* {**pots** | **vofr** | **voip**} **Example:** `Router(config)# dial-peer voice 111 voip`	Enters dial peer voice configuration mode.
Step 4	**voice-class sip url sips** **Example:** `Router(config-dial-peer)# voice-class sip url sips`	Specifies configuration of URLs in SIPS format for VoIP calls for a specific dial peer.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring SRTP and SRTP Fallback Globally

To configure SRTP and SRTP fallback behavior globally on a Cisco IOS voice gateway or Cisco Unified Border Element, perform the following steps.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service** {**pots** | **voatm** | **vofr** | **voip**} **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**srtp** **Example:** `Router(conf-voi-serv)# srtp`	Configures secure RTP calls.
Step 5	**srtp fallback** **Example:** `Router(conf-voi-serv)# srtp fallback`	(Optional) Configures a fallback to RTP calls in case secure RTP calls fail due to lack of support from an endpoint.
Step 6	**exit** **Example:** `Router(conf-voi-serv)# exit`	Exits the current mode.

Configuring SRTP and SRTP Fallback on a Dial Peer

To configure SRTP and SRTP fallback behavior on an individual dial peer that overrides the global SRTP configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**pots** | **vofr** | **voip** }
4. **srtp**
5. **srtp fallback**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* {**pots** | **vofr** | **voip** } **Example:** `Router(config)# dial-peer voice 111 voip`	Enters dial peer voice configuration mode.
Step 4	**srtp** **Example:** `Router(config-dial-peer)# srtp`	Configures secure RTP calls.
Step 5	**srtp fallback** **Example:** `Router(config-dial-peer)# srtp fallback`	(Optional) Configures a fallback to RTP calls in case secure RTP calls fail due to lack of support from an endpoint.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuration Examples for Configuring SIP Support for SRTP

The following example shows how to configure SIPS globally on a Cisco IOS voice gateway or Cisco Unified Border Element:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# url sips
Router(conf-serv-sip)# exit
```

The following example shows how to configure SIPS on dial peer 111:

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

```
Router(config-dial-peer)# voice-class sip url sips
Router(config-dial-peer)# exit
```

The following example shows how to configure for SRTP with fallback to RTP globally on a Cisco IOS voice gateway or Cisco Unified Border Element:

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

The following example shows how to configure for SRTP with fallback to RTP on dial peer 111:

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

Additional References

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

Related Documents

Related Topic	Document Title
Cisco IOS dial peer overview	"Dial Peer Overview"
Cisco IOS dial technologies command information	*Cisco IOS Dial Technologies Command Reference*
Cisco IOS SIP overview and related documents	"Overview of SIP"
Cisco IOS software configuration guides	• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS SIP Configuration Guide* **Note** To locate the configuration guide specific to your Cisco IOS software release, choose the **Cisco IOS and NX-OS Software** category on the Product Support page and navigate according to your release (http://www.cisco.com/web/psa/products/index.html) .
Cisco IOS voice command information	*Cisco IOS Voice Command Reference*
Cisco IOS voice configuration information	*Cisco IOS Voice Configuration Library*

Related Topic	Document Title
Cisco Unified Border Element configuration information	*Cisco Unified Border Element Configuration Guide*
Cisco Unified CME command information	*Cisco Unified Communications Manager Express Command Reference*
Cisco Unified CME configuration information	Cisco Unified CME Support Documentation Home Page

RFCs

RFC	
draft-ietf-mmusic-sdescriptions-08.txt	Session Description Protocol Security Descriptions for Media Streams
RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3711	The Secure Real-time Transport Protocol (SRTP)

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: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring SIP Support for SRTP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Configuring SIP Support for SRTP

Feature Name	Releases	Feature Information
SIP Support for SRTP	12.4(15)T	This feature introduces SIP support for supplementary services features, such as call hold, call transfer, call waiting, and call conference (3WC) using hook flash (HF) for FXS phones on Cisco IOS voice gateways. The following commands were introduced or modified: **srtp**, **srtp fallback**.
SIP SRTP Fallback to Nonsecure RTP	12.4(15)XY 12.4(20)T	This feature extends the existing SRTP to RTP fallback on Cisco IOS voice gateways to support a delayed offer and adds support for SRTP over SIP. The following commands were introduced or modified: **srtp negotiate**, **voice-class sip srtp negotiate**.
Interworking of Secure RTP calls for SIP and H323	12.4(20)T	This feature provides an option for a Secure RTP (SRTP) call to be connected from H323 to SIP and from SIP to SIP. Additionally, this feature extends SRTP fallback support from the Cisco IOS voice gateway to the Cisco Unified Border Element. This feature uses no new or modified commands.
SIP SRTP Fallback to Nonsecure RTP for Cisco Unified Border Elements	12.4(22)T	This feature adds support for both SRTP to RTP fallback with a delayed offer and SRTP over SIP to the Cisco Unified Border Element. This feature uses no new or modified commands.
Cisco Unified Border Element Support for SRTP-RTP Internetworking	12.4(22)YB	This feature provides the ability to support interworking between SRTP on one IP leg and RTP on another IP leg of a Cisco Unified Border Element. The following command was introduced or modified: **tls**.

Glossary

AVP --Audio/Video Profile.

CAC --Call Admission Control.

CME --Communications Manager Express.

CVP --Customer Voice Portal.

GW --gateway.

ISDN --Integrated Services Digital Network.

MIME --Multipurpose Internet Mail Extensions.

m line --The media-level section of an SDP session begins and ends with an "m" line that confines the information about the media stream.

MOH --music on hold.

OGW --originating gateway (ingress gateway).

PBX --Private Branch Exchange.

PINX --private integrated services network exchange.

PISN --private integrated services network.

QoS --quality of service.

QSIG --Q Signaling protocol.

RSVP --Resource Reservation Protocol.

RTP --Real-time Transport Protocol.

SDP --Session Description Protocol.

SIP --Session Initiation Protocol.

SRTP --Secure Real-time Transport Protocol.

TDM --time-division multiplexing.

TGW --terminating gateway (egress gateway).

UA --user agent.

UDP --User Datagram Protocol.

URI --uniform resource identifier.