SIP Configuration Guide, Cisco IOS XE Release 3S

Revised: January 4, 2016,

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.

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 is supported along with interoperability of SIP support for SRTP on Cisco IOS voice gateways with Cisco Unified Communications Manager. 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.

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.
- 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

- SIP requires that all times be sent in GMT.
- The SIP SRTP TDM-IP Gateway supports only basic calls.

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 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 . 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 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 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** The calls established with SRTP only (and not SIPS) will succeed even if the **srtp fallback** command is not configured.

TLS	SRTP	Description
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
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

Parameter	Default	Recommended Value
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 , 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.
- 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 The calls established with SRTP at one end and SRTP fall back at the other end will succeed even if the **srtp fallback** command is not configured.

When a gateway 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 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 will not generate a new master key after a key has been established for an SRTP session.

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 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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**srtp** **Example:** `Router(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.

	Command or Action	Purpose
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.

Procedure

	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 voip** *tag* **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.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Verifying and Monitoring SIP SRTP Configuration

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show call active voice brief**

Example:

```
Device# show call active voice brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
 LostPacketRate:<%> OutOfOrderRate:<%>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>


Telephony call-legs: 1
SIP call-legs: 1
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
```

```
Total call-legs: 2
11EE : 15 11292320ms.1 (*14:53:43.011 IST Fri Dec 11 2015) +3020 pid:0 Answer 99001 active
 dur 00:02:41 tx:8223/1665909 rx:8225/1671825 dscp:0 media:0 audio tos:0x0 video tos:0x0
 Tele 0/1/0:23 (15) [0/1/0.23] tx:164700/164440/0ms g711ulaw noise:-79 acom:51  i/0:-16/-16 dBm

11EE : 16 11292320ms.2 (*14:53:43.011 IST Fri Dec 11 2015) +3020 pid:102 Originate 99002 active
 dur 00:02:41 tx:8196/1671825 rx:8167/1665909 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 9.45.2.53:16386 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00


Telephony call-legs: 1
SIP call-legs: 1
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Displays active voice brief information.

Step 3 **show sip-ua calls**

Example:

```
Device# show sip-ua calls

Total SIP call legs:1, User Agent Client:1, User Agent Server:0
SIP UAC CALL INFO
Call 1
SIP Call ID                : B4C2B4B5-9F1F11E5-8031F8C8-35DF5EF7@9.45.3.6
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 99001
   Called Number           : 99002
   Called URI              : sip:99002@9.45.2.53:5060
   Bit Flags               : 0xC04018 0x90800100 0x0
   CC Call ID              : 16
   Source IP Address (Sig ): 9.45.3.6
   Destn SIP Req Addr:Port : [9.45.2.53]:5060
   Destn SIP Resp Addr:Port: [9.45.2.53]:5060
   Destination Name        : 9.45.2.53
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 16
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [9.45.3.6]:8014
     Media Dest IP Addr:Port  : [9.45.2.53]:16386
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_32
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_32


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1
```

```
SIP UAS CALL INFO
   Number of SIP User Agent Server(UAS) calls: 0
```

Displays SIP User Agent call information.

Step 4 **show voip fpi calls all**

Example:

```
Device# show voip fpi calls all

Number of Calls : 1
---------------------------------------------------------------------------
VoIP-FPI call entry details:
---------------------------------------------------------------------------
Call Type        :           TDM_IP     confID          :               2
correlator       :                2     call_state      :       ALLOCATED
last_event       :    GET_STATS_RSP     alloc_start_time :       703040335
modify_start_time:                0     delete_start_time:               0
Media Type(SideA):             SRTP
---------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted             :         1
call_create_req_fsm_successful             :         1
call_get_stats_req_fsm_successful          :       329
call_provision_rsp_ok                      :         1
call_provision_rsp_fsm_successful          :         1
call_get_stats_rsp_ok                      :       329
call_get_stats_rsp_fsm_successful          :       329
---------------------------------------------------------------------------------------------
SIDE_A  RTP details    -    gccb=0x7FB2CE41CE58
---------------------------------------------------------------------------------------------
confID           :         2    fpi_user_data    :         2
callID           :        16    dstCallID        :        15    mainstcallID     :         16
srcport          :      8014    dstport          :     16386    DP add_sent      :          1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :          0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :          0
ha_create_sent   :         0    is_video         :         0    media_type       :          0
is dspfarm xcode :        No    is conference    :        No    stream_type      :      VOICE
rtp_type         :  SENDRECV
---------------------------------------------------------------------------------------------
--------- SIDE B DMGR  dmgr=0x7FB2BEE271A0 ---------
---------------------------------------------------------------------------------------------
confID            :         2   sbc_pending_confID:         0   fpi_user_data     :          0
callID            :        15   PeerCallID        :        16   DP add_sent       :          1
DP add_pending    :         0   dp_add_fail       :         0   dp_delete_sent    :          0
DP delete_done    :         0   TDM-TDM hairpin   :         0
---------------------------------------------------------------------------------------------
Detailed Stats from DataPlane:
------------------------------
mgm_handle      : 2
-------------------------------------------------------------------
Call Present in :    FMAN RP   FMAN FP      CPP
                 ----------------------------------------
                         YES       YES       YES
-------------------------------------------------------------------
                      Field                sideA               sideB
-------------------------------------------------------------------
          dtmf_payload_type                    0                   0
   redundant_data_pyld_type                  255                   0
                   tos_mask                  255                   0
                 dtmf_flags                    0                   0
                ucode_flags                    0                   0
                 local_port                 8014                   0
             remote_port_tx                16386                   0
             remote_port_rx                16386                   0
                 session_id           0x50000008         0x        0
  hairpin_prtnr_null(ucode)                 NULL                NULL
       hairpin_prtnr_callid                    0                   0
         dsp_interface_null             NOT NULL                NULL
             dsp_session_id                    8                   0
```

```
      dsp_legOut_stream_id              18799                   0
       dsp_legIn_stream_id              18800                   0
-------------------------------------------------------------------
DSP Resource Used : Yes

DSP Stats:
----------
device-id  : 0
channel_id : 1
core_id    : 0
-------------------------------------------------------------------
                      Field             sideA               sideB
-------------------------------------------------------------------
                 conference                 0                   0
                    proc_id                 0                   0
                   rx_count             16466                   0
                   tx_count             16433                   0
-------------------------------------------------------------------
DSP Session Present in :    FMAN RP   FMAN FP       CPP
                        ---------------------------------
                                YES       YES       YES
------------------------------------------------------------
```

Displays VOIP Forwarding Plane Interface (FPI) call information.

Step 5 **show platform hardware qfp active feature sbc global**

Example:

```
Device# show platform hardware qfp active feature sbc global

SBC Media Forwarder Statistics
------------------------------

  Total packets received                     = 26366
  Total packets forwarded                    = 26446
  Total packets dropped                      = 0
  Total packets punted                       = 0
  Incoming packets diverted to SBC subsystem  = 0
  Outgoing packets inserted by SBC subsystem  = 0

Detailed breakdown of statistics:

Dropped packets:
  No associated flow                         = 0
  Wrong source for flow                      = 0
  Ingress flow receive disabled              = 0
  Egress flow send disabled                  = 0
  Not conforming to flowspec                 = 0
  Badly formed RTP                           = 0
  Badly formed RTCP                          = 0
  Excessive RTCP packet rate                 = 0
  Borrowed for outgoing DTMF                 = 0
  Unknown destination address                = 0
  Misdirected                                = 0
  Feature disabled                           = 0
  Reprocess limit exceeded                   = 0

Punted packets:
  H.248 control packets                      = not implemented
  Packets containing options                 = 0
  Fragmented packets                         = 0
  Unexpected IP protocol                     = 0
  Packets from invalid port range            = 0

Punted packets dropped through rate limiting  = 0
Packets colored with configured DSCP          = 0

Diverted DTMF packets dropped:

  Excessive DTMF packet rate                 = 0
  Bad UDP checksum                           = 0
```

```
  Diverted packet queue full                  = not implemented
  Other                                       = not implemented

Generated event information:
  Number of media UP events                   = 0
  Number of media DOWN events                 = 0
  Number of unexpected source events          = 0

Platform specific statistics:
  Packets learn source address                = 0
  Packets Learn source address timed out      = 0
  Packets conformed                           = 0
  Packets exceed                              = 0
  Packets violate                             = 0
  Packets RTCP receive                        = 107
  RTP drops - bad SSRC                        = 0
  Packet dropped by protocol interworking     = 0
  Packet dropped for SRTP decryption failure  = 0
  Packet dropped for SRTP encryption failure  = 0

  SRTP detailed failure codes:
  Packet dropped for SRTP unspecified failure  = 0
  Packet dropped due to SRTP bad parameter     = 0
  Packet dropped due to SRTP alloc failure     = 0
  Packet dropped due to SRTP dealloc failure   = 0
  Packet dropped due to SRTP init failure      = 0
  Packet dropped due to SRTP auth failure      = 0
  Packet dropped due to SRTP cipher failure    = 0
  Packet dropped due to SRTP replay failure    = 0
  Packet dropped due to SRTP stale packet      = 0
  Packet dropped due to SRTP algorithm failure = 0
  Packet dropped due to no SRTP context        = 0
  Packet dropped due to SRTP validation failure= 0
  Packet dropped due to SRTP key expiry        = 0
  Packet dropped due to other SRTP failure     = 0

SBC Media Forwarder statistics can wrap after a
approximately 18 quintillion packets. For more accurate
statistics on completed calls, please use
show sbc ... dbe media-stats
```

Displays Cisco QuantumFlow Processor (QFP) Session Border Controller (SBC) information.

Step 6 **debug voip fpi all**

Example:

```
Device# debug voip fpi all
```

Enables VOIP FPI debugging.

Step 7 **debug voip ccapi inout**

Example:

```
Device# debug voip ccapi inout
```

Enables trace of the execution path through the call control application programming interface (CCAPI).

Step 8 **debug voip dsmp all**

Example:

```
Device# debug voip dsmp all
```

Enables all Distributed Stream Media Processor (DSMP) debugging.

Step 9 **debug voip dsm all**

Example:

```
Device# debug voip dsm all
```

Displays all DSP stream manager (DSM) debugging messages.

Step 10 **debug voip application session**

Example:
```
Device# debug voip application session
```
Displays debug messages from default session application.

Step 11 **debug voip application states**

Example:
```
Device# debug voip application states
```
Displays debug traces for application states.

Step 12 **debug ccsip all**

Example:
```
Device# debug ccsip all
```
Enables all SIP related debugging.

Step 13 **debug isdn q931**

Example:
```
Device# debug isdn q931
```
Displays information about the call setup and teardown of ISDN network connections (layer 3) between the local router (user side) and the network.

Step 14 **debug platform software dsprm**

Example:
```
Device# debug platform software dsprm
```
Enables Digital Signal Processor Resource Manager (DSPRM) debugging.

Step 15 **debug platform hardware qfp active interface dsp client all**

Example:
```
Device# debug platform hardware qfp active interface dsp client all
```
Enables debug logging for Digital Signal Processor (DSP) client in the Cisco QuantumFlow Processor (QFP).

Step 16 **debug platform hardware qfp active feature sbc dbe client all**

Example:
```
Device# debug platform hardware qfp active feature sbc dbe client all
```
Enables debug logging for signaling border element (SBE) or the data border element (DBE) logs in the Cisco QuantumFlow Processor (QFP).

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*
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 . An account on Cisco.com is not required.

Table 4: Feature Information for Configuring SIP Support for SRTP

Feature Name	Releases	Feature Information
SIP SRTP Support for TDM-IP GW	Cisco IOS XE Release 3.17S	The SIP SRTP Support for TDM-IP GW feature enables SIP SRTP for TDM-IP calls. This feature uses no new or modified commands.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.