

Setting the Security Parameters of the RTP Stream

All Mediatrix units

DGW 49.2.2941

2023-08-09

Table of Contents

Secure Real-Time Transport Protocol	3
Basic Tasks	4
Enabling Secure Media (SRTP) on All Endpoints	4
Enabling Secure Media (SRTP) on a Specific Endpoint	5
Allowing Unsecure T.38 with Secure RTP	6
Modifying the SRTP Basic Port	6
Advanced RTP Parameters	8
Advanced SRTP Preferences Configuration for the Mediatrix Gateways	8
Recommended SRTP Preferences for a Typical VoIP Network	9
Recommended SRTP Preferences for Cisco BroadWorks and BroadCloud	10
Recommended SRTP Preferences for Microsoft Teams	10
Recommended SRTP Preferences for Oracle SBC	10
Online Help	11
DGW Documentation	12
Copyright Notice	13

Secure Real-Time Transport Protocol

Secure Real-time Transport Protocol (SRTP) is a profile of Real-time Transport Protocol (RTP) that provides encryption, message authentication, and replay attack protection.

SRTP can be enabled on all Mediatrix unit endpoints, or on one or more specific endpoints. However, SRTP encryption and authentication requires more processing therefore, if SRTP is enabled, the number of calls that the Mediatrix unit can handle simultaneously may be reduced, depending of the enabled codecs . (For more details on resources limitations with SRTP and conferences, refer to the [DGW Configuration Guide - Limitations of DGW Platforms](#) document published on the [Media5 Documentation Portal](#)).

To reduce the impact on the number of simultaneous calls a Mediatrix unit can handle, is it possible to disable all voice or data codec, including the T.38 protocol, and keep only the G.711 voice codec enabled.

IMPORTANT: If Secure RTP (SRTP) is enabled on at least one line, it is acceptable to have the secure SIP transport (TLS) disabled for testing purposes. However, this configuration must never be used in a production environment, since an attacker could easily break it. Enabling TLS for SIP Transport is strongly recommended and is usually mandatory for security interoperability with third-party equipments.

The Mediatrix unit supports the MIKEY protocol using pre-shared keys (MIKEY-PS as per RFC 3830) or the SDES protocol for negotiating SRTP keys

Basic Tasks

Enabling Secure Media (SRTP) on All Endpoints

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose **Default**.
- 3) In the **Security** table,
 - a) From the **Mode** drop box, select **Secure** or **Secure with fallback**.
 - b) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDES** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDES** protocol will add the `a=crypto` line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the `a=key-mgmt:mikey` line within the SDP Session Attributes.

- c) From the drop box, select the **AES_CM_128** encryption algorithm.
- d) From the **Allow Unsecure T.38 with Secure RTP** selection, choose if unsecure **T.38** is allowed with RTP.

Note: **T.38** packets will never be encrypted. The setting **Allow Unsecure T.38 with Secure RTP** will make possible to use **T.38**, otherwise it will be rejected. If not using **T.38** for faxing, to avoid an impact on the number of simultaneous calls a Mediatrix unit can handle in SRTP, set the **Allow Unsecure T.38 with Secure RTP** parameter to **No** and refer to the [Standard Fax Configuration](#) document to disable **T.38** Fax Transmission.

- 4) In the **SRTP Preferences** table,
 - a) From the **Crypto Mode When Sending Offer** drop box, select the preferred mode.
 - b) From the **Crypto Mode When Sending Answer** drop box, select the preferred mode.
 - c) From the **Crypto Context Behavior** drop box, select the preferred behavior.

Note: For more information about the recommended **SRTP Preferences**, please refer to [Recommended SRTP Preferences for a Typical VoIP Network](#) section of the [Setting the Security Parameters of the RTP Stream](#) document.

Note: For troubleshooting the SRTP interoperability, please refer to the [SRTP Troubleshooting](#) document.

- 5) Click **Apply**.

Result

All new SIP exchanges will contain RTP/SAVP negotiation elements.

Select Endpoint: Default ▾

Security	
RTP	
Mode:	Secure ▾
Key Management Protocol:	Key Management Protocol for SRTP ▾
Encryption:	AES_CM_128 ▾
T.38	
Allow unsecure T.38 with secure RTP:	No ▾

SRTP Preferences	
Crypto Mode When Sending Offer:	Mode when sending SDP offer with SRTP ▾
Crypto Mode When Sending Answer:	Mode when sending SDP answer with SRT ▾
Crypto Context Behavior:	Behavior of the SRTP Context ▾

Enabling Secure Media (SRTP) on a Specific Endpoint

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose an endpoint.

Note: The list of available endpoints will vary depending on the type of unit being used.

- 3) In the **Security** table, from the **Mode** drop box, select **Secure** or **Secure with fallback**.
- 4) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDES** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDES** protocol will add the a=crypto line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the a=key-mgmt:mikey line within the SDP Session Attributes.

- 5) From the drop box, select the **AES_CM_128** encryption algorithm.
- 6) Click **Apply**.

Result

All new SIP exchanges going through the specified endpoint will contain RTP/SAVP negotiation elements.

Select Endpoint: Chosen Endpoint ▾

Security	
RTP	
Endpoint Specific:	Yes ▾
Mode:	Secure ▾
Key Management Protocol:	Key Management Protocol for SRTP ▾
Encryption:	AES_CM_128 ▾

Allowing Unsecure T.38 with Secure RTP

Information

The T.38 protocol must be enabled under **Media/Codec**.

This procedure is required only if SRTP is used and is available provided the **Select Endpoint** selection list is set to **Default**.

Steps

- 1) Go to **Media/Security**.
- 2) In the **Security** table, under the **RTP** section, set the **Mode** selection list to **Secure with fallback**.
- 3) Under the **T.38** section, set the **Allow Unsecure T.38 with Secure RTP** selection list to **Yes**.
- 4) Click **Apply**.

Result

Select Endpoint: Default ▾

Security	
RTP	
Mode:	Secure with fallback ▾
Key Management Protocol:	Key Management Protocol for SRTP ▾
Encryption:	AES_CM_128 ▾
T.38	
Allow unsecure T.38 with secure RTP:	Yes ▾

Modifying the SRTP Basic Port

Steps

- 1) Go to **Media/Misc**.

- 2) In the **Base Ports** table, in the field next to **SRTP**, indicate in the field to first port to use in SRTP.

Result

The first port to be used in SRTP will be the one specified.

Base Ports		
RTP:	5004	
SRTP:	First port to use	
T.38:	6004	

Advanced RTP Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by:

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

- **Mipt.EnforceSymmetricRtpEnable:** to enforce that incoming RTP packets are from the same source as the destination of outgoing RTP packets.
- **Mipt.InteropDtmfRtpInitialPacketQty:** to specify the quantity of packets sent at the beginning and at the ending of an Out-of-Band DTMF using RTP.
- **Mipt.InteropPacketReceptionMode:** to select the mode that control the range of packetisation times (ptime) applied at the reception of RTP packets.

Advanced SRTP Preferences Configuration for the Mediatrix Gateways

Under certain conditions, the **SRTP Preferences** of the Mediatrix gateways can be tweaked, allowing a better interoperability with the SRTP behaviors of different VoIP devices.

Note: For troubleshooting the SRTP interoperability, please refer to the [SRTP Troubleshooting](#) document.

The **Mipt.CryptoModeWhenSendingOffer** and **Mipt.CryptoModeWhenSendingAnswer** parameters affect the behavior of the SRTP elements within the SIP messages.

Note: The **Mipt.CryptoModeWhenSendingOffer** and **Mipt.CryptoModeWhenSendingAnswer** parameters do not apply to SIP session refresh. The session timers in SIP reINVITES or SIP UPDATES will not be affected by the SRTP crypto.

When sending SDP offer in SIP messages and the **Mipt.CryptoModeWhenSendingOffer** parameter is set to:

- *RegenerateAlways*, a different crypto attribute is generated.
- *KeepAlways*, the previously sent crypto attribute is reused.

When sending SDP answer in SIP messages and the **Mipt.CryptoModeWhenSendingAnswer** is set to:

- *RegenerateAlways*, a different crypto attribute is generated.
- *KeepUnlessCryptoChange*, a different crypto attribute is generated if the received offer has a different crypto attribute. Otherwise, the previously sent crypto attribute is reused.
- *KeepAlways*, the previously sent crypto attribute is reused.

The **Mipt.CryptoContextBehavior** parameter affect the behavior of the SRTP cryptographic context. All devices in the VoIP network must have an identical behavior, otherwise this will lead to decryption problems. The possible configurations are:

- *ResetAlways*: Reset the cryptographic context on every SDP renegotiation, even if the crypto key has not changed.
- *ResetOnNewCrypto*: Reset the cryptographic context when the negotiated crypto key has changed.
- *ResetNever*: The cryptographic context is never reset after an SDP renegotiation. The context is updated with the new crypto keys, while the crypto transform parameters keeps its current value.

Note: The SRTP cryptographic context, used for the encryption of the outgoing stream and the decryption of the incoming stream, contains the following transform parameters:

- SSRC identifier
- Sequence number
- Roll Over Counter (ROC) – an internal counter not exchanged between the VoIP devices
- IP address and UDP port number of the media stream

Recommended SRTP Preferences for a Typical VoIP Network

Most of the time, the configuration of those three parameters can be in one of these two cases:

Configurable parameter	Regenerate	Keep
Crypto Mode When Sending Offer	<i>Regenerate Always</i>	<i>Keep Always</i>
Crypto Mode When Sending Answer	<i>Regenerate Always</i>	<i>Keep Always</i>
Crypto Context Behavior	<i>Reset Always</i>	<i>Reset Never</i>

The [Regeneration](#) combination is recommended when:

- the Mediatrix gateway exchanges with VoIP devices which the SRTP behavior is unknown.
- the Mediatrix gateway exchanges with different VoIP devices without centralized VoIP infrastructure.
- the Mediatrix gateway or the Mediatrix Sentinel SBC exchanges with BroadSoft, Cisco or Oracle servers.

The [Keep](#) combination is recommended when:

- the Mediatrix Sentinel SBC interchanges with VoIP devices which the SRTP behavior is unknown.
- the Mediatrix gateway or the Mediatrix Sentinel SBC exchanges with a media relay server which re-encrypt completely the SRTP packets (new crypto keys, different SSRC identifier).
- the Mediatrix gateway or the Mediatrix Sentinel SBC exchanges with Microsoft servers, such as Microsoft Teams.

Recommended SRTP Preferences for Cisco BroadWorks and BroadCloud

```
Mipt.CryptoModeWhenSendingOffer = "RegenerateAlways"  
Mipt.CryptoModeWhenSendingAnswer = "RegenerateAlways"  
Mipt.CryptoContextBehavior = "ResetAlways"
```

Recommended SRTP Preferences for Microsoft Teams

```
Mipt.CryptoModeWhenSendingOffer = "KeepAlways"  
Mipt.CryptoModeWhenSendingAnswer = "KeepAlways"  
Mipt.CryptoContextBehavior = "ResetNever"
```

Recommended SRTP Preferences for Oracle SBC

```
Mipt.CryptoModeWhenSendingOffer = "RegenerateAlways"  
Mipt.CryptoModeWhenSendingAnswer = "RegenerateAlways"  
Mipt.CryptoContextBehavior = "ResetAlways"
```

Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the [Media5 Documentation Portal](#).

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes:** Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes:** These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins:** These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide:** They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide:** The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide:** This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com