

SRTP Troubleshooting

All Mediatrix Units

DGW 49.2.2941

2023-08-09

Table of Contents

SRTP Troubleshooting	3
Preparing Information for Troubleshooting	4
Required Information to Report a Problem	4
Additional Information to Report a Problem with Secured Media	4
Investigating SRTP Interoperability Issues	6
What to Observe	6
SRTP Test Protocol	6
Result table	9
How to Interpret the Result of the Test Protocol	11

SRTP Troubleshooting

This document provides general tips on how to troubleshoot SRTP issues. Different scenarios are analysed and suggestion of possible solutions using the **SRTP Preferences** are proposed.

Note: For more information about the **SRTP Preferences**, please refer to the [Advanced SRTP Preferences Configuration for the Mediatrix Gateways](#) section of the [Setting the Security Parameters of the RTP Stream](#) document.

Preparing Information for Troubleshooting

Please refer to the [Preparing Information for Troubleshooting](#) document about collecting diagnostic traces (syslogs) and network packets.

Required Information to Report a Problem

When reporting a problem and to make sure that all the relevant information is given to the Mediatrix support team at once, the following information is required.

Required information	Checkmark
Mediatrix product name, release and build number.	
Profile name	
Serial number of the Mediatrix unit if a hardware problem is suspected.	
Name/manufacturer/type of other VoIP devices along with their IP addresses.	
Name/manufacturer/software version of the Proxy server (SIP).	
Whenever possible, a diagram of the network or wiring setup.	
Call flow/call scenario to reproduce the problem.	
Is the call going through a NAT, Firewall, Bridge, VPN, Router, Soft switch, etc?	
Export the complete configuration script of the Mediatrix device. Refer to the Exporting a Configuration Script to Your PC instructions.	

Additional Information to Report a Problem with Secured Media

When reporting a problem with audio using secured media, the following additional information are demanded.

Additional information	Checkmark
Is the problem also observed when the media is unsecured?	
Is the problem observed at the beginning of the call?	
How long is the call before the problem is observed?	
Can the problem be easily reproduced? If yes, how is it reproduced?	
Is the problem present during the complete call?	
Are session timers used with SIP reINVITE or SIP UPDATE messages?	
Was the call put on hold prior to the problem been observed?	
Is music on hold present during the call prior to the problem been observed?	
Is the problem be reproduced when calling different VoIP devices?	
Is the problem be reproduced while using other VoIP devices than Mediatrix devices?	

Investigating SRTP Interoperability Issues

What to Observe

During an SRTP interoperability investigation, the following elements must be observed within the exchanged SDP payloads of SIP messages, the diagnostic traces (syslogs), and the header of SRTP packets. Those elements must be captured from the network traffic, as described in the [Preparing Information for Troubleshooting](#) document.

In the SDP payloads, the following information are meaningful to ensure the establishment of both SRTP streams over the VoIP network:

- the advertised address (IP and port) of the media (**c=** and **m=** attributes)
- the advertised crypto attribute (**a=crypto** attribute)

```
v=0
o=MxSIP 688350484195200802 174878181552902651 IN IP4 192.168.121.10
s=-
--> c=IN IP4 192.168.121.10
t=0 0
a=sendrecv
--> m=audio 5004 RTP/SAVP 8
a=rtpmap:8 PCMA/8000
--> a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:f2vJDBzqgo...
```

In the SRTP packet headers, the following information influence the media stream decryption:

- The Synchronization Source (SSRC) identifier
- The Sequence number

```
--> Sequence number: 10142
[Extended sequence number: 75678]
Timestamp: 1026635472
--> Synchronization Source identifier: 0x9ddb426e (2648392302)
SRTP Encrypted Payload: e4cf7a734ea2f70c720849e...
SRTP Auth Tag: 3684164878c1bd5012e8
```

SRTP Test Protocol

Information

The following test protocol gives all the necessary information useful to experiment with the SRTP interoperability between a Mediatrix device and other VoIP devices.

- If no audio issue is observed during SIP calls, this means the SRTP behavior of the Mediatrix device matches with the VoIP network.
- If an audio issue is observed during SIP calls, changing the **SRTP Preferences** parameters may help to resolve the issue.

To help collecting the information during the investigation, the logging table available at the [Result table](#) (p.9) section can be printed twice, one table for the caller's role and another the callee's role. The table is available to download on our documentation portal: [TestProtocol_SRTP.xlsx](#)

Steps

Configuration of the Mediatrix Gateway

IMPORTANT: The following configuration is for testing purpose only and should not be used in a production environment. Once the test results are completed, the unit configuration must be reverted to the original one.

- 1) Configure the [Syslogs in Debug Mode](#) on the Mediatrix device.
- 2) Configure the **SRTP Preferences** parameters. Refer to the [Advanced SRTP Preferences Configuration for the Mediatrix Gateways](#) document for details.
- 3) Force the ptime of the used codecs to the smallest possible value. The smaller the ptime is, the faster the sequence number increases. The following lines are used to configure the minimum and maximum ptime of the G711 codec.

```
Mipt.DefaultCodecG711MulawMinPTime = 10  
Mipt.DefaultCodecG711MulawMaxPTime = 10  
Mipt.DefaultCodecG711AlawMinPTime = 10  
Mipt.DefaultCodecG711AlawMaxPTime = 10
```

- 4) Deactivate the VAD (Voice Activity Detection). This disables the transmission of Comfort Noise packets when there is no voice activity (silence periods), causing the sequence number to increase faster.

```
Mipt.DefaultCodecGenericVoiceActivityDetection = "Disable"
```

- 5) Disable the Session-expires timer. There will be less SIP messages to investigate.

```
SipEp.DefaultSessionTimerEnable = "Disable"
```

- 6) Make one VoIP device the callee and the other the caller for the duration of the test.
- 7) Start a [Remote Packet Capture](#) from your computer.

Call establishment between the VoIP devices

- 8) The caller calls the callee.
 - a) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

Call holding by the callee VoIP device

- 9) The callee puts the call on hold
 - a) Wait 10 seconds and validate if Music-on-Hold is heard on the caller side.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

- 10) The callee resumes the call
 - a) Wait 10 seconds and validate the audio path.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).
- 11) The callee puts the call on hold again
 - a) Wait 10 seconds and validate if Music-on-Hold is heard on the caller side.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).
- 12) The callee resumes the call
 - a) Wait 10 seconds and validate the audio path.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

Call holding by the caller VoIP device

- 13) The caller puts the call on hold
 - a) Wait 10 seconds and validate if Music-on-Hold is heard on the callee side.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).
- 14) The caller resumes the call
 - a) Wait 10 seconds and validate the audio path.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).
- 15) The caller puts the call on hold again
 - a) Wait 10 seconds and validate if Music-on-Hold is heard on the callee side.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).
- 16) The caller resumes the call
 - a) Wait 10 seconds and validate the audio path.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

The sequence number of both SRTP streams must rollover

- 17) Wait until both SRTP streams have their sequence numbers rollover.

The time to wait depends mainly on the ptime used. With a ptime of 10ms, it may take 13 minutes before the rollover happens. With a ptime of 30ms, it may take 40 minutes.
- 18) Once the rollover occurred on both SRTP streams, both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

Call holding by the callee VoIP device

- 19) The callee puts the call on hold
 - a) Wait 10 seconds and, if it applies, validate that the Music-on-Hold is heard on the caller side.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).
- 20) The callee resumes the call
 - a) Wait 10 seconds and validate the audio path.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).
- 21) The callee puts the call on hold again
 - a) Wait 10 seconds and, if it applies, validate that the Music-on-Hold is heard on the caller side.
 - b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

22) The callee resumes the call

- a) Wait 10 seconds and validate the audio path.
- b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

Call holding by the caller VoIP device

23) The caller puts the call on hold

- a) Wait 10 seconds and, if it applies, validate that the Music-on-Hold is heard on the callee side.
- b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

24) The caller resumes the call

- a) Wait 10 seconds and validate the audio path.
- b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

25) The caller puts the call on hold again

- a) Wait 10 seconds and, if it applies, validate that the Music-on-Hold is heard on the callee side.
- b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

26) The caller resumes the call

- a) Wait 10 seconds and validate the audio path.
- b) Both sides must note the [observed SRTP elements](#) and write them down in the [Result table](#).

Result table

The following table is provided to help with the investigation to write in the information relevant to the testing done for a single VoIP device. The table is also available for download on our documentation portal: [TestProtocol_SRTP.xlsx](#)

Device: _____ IP address: _____ Call Role: (Caller) / (Callee)							
Test Protocol step number	Aud hear	TX SSRC	RX SSRC	1st TX Sequence Number	1st RX Sequence Number	TX Key (first 6 characters)	RX Key (first 6 characters)
6	Establish a call						
Call holding by the callee VoIP device							
7	The callee puts the call on hold						
8	The callee resumes the call						
9	The callee puts the call on hold again						
10	The callee resumes the call						
Call holding by the caller VoIP device							
11	The caller puts the call on hold						
12	The caller resumes the call						
13	The caller puts the call on hold again						
14	The caller resumes the call						
The sequence number of both SRTP streams must rollover							
16	Rollover occurred on both SRTP streams						
Call holding by the callee VoIP device							
17	The callee puts the call on hold						
18	The callee resumes the call						
19	The callee puts the call on hold again						

Device: _____ IP address: _____ Call Role: (Caller) / (Callee)								
Test Protocol step number		Aud	TX SSRC	RX SSRC	1st TX Sequence Number	1st RX Sequence Number	TX Key (first 6 characters)	RX Key (first 6 characters)
20	The callee resumes the call							
Call holding by the caller VoIP device								
21	The caller puts the call on hold							
22	The caller resumes the call							
23	The caller puts the call on hold again							
24	The caller resumes the call							

How to Interpret the Result of the Test Protocol

In the SDP payloads, the following information are meaningful to ensure the establishment of both SRTP streams over the VoIP network:

- the advertised address (IP and port) of the media (**c=** and **m=** attributes)
- the advertised crypto attribute (**a=crypto** attribute)

In the SRTP packet headers, the following information influence the media stream decryption:

- The Synchronization Source (SSRC) identifier
- The Sequence number

Following the observations made during the investigation, the following **SRTP Preferences** are recommended:

Observation	Recommended SRTP Preferences configuration
The Mediatrix gateway receives a different crypto key in the SDP offers and answers after a hold/resume scenario.	Mipt.CryptoModeWhenSendingOffer = <i>RegenerateAlways</i> Mipt.CryptoModeWhenSendingAnswer = <i>RegenerateAlways</i>
The Mediatrix gateway always receives the same crypto key in the SDP offers and answers after a hold/resume scenario.	Mipt.CryptoModeWhenSendingOffer = <i>KeepAlways</i> Mipt.CryptoModeWhenSendingAnswer = <i>KeepAlways</i>
The Mediatrix gateway receives a different media address in the SDP offers and answers OR The Mediatrix gateway receives an SRTP stream with different SSRC after a hold/resume scenario.	Mipt.CryptoContextBehavior = <i>ResetAlways</i>
The Mediatrix gateway receives the same media address in the SDP offers and answers AND The Mediatrix gateway receives an SRTP stream with the same SSRC after a hold/resume scenario.	Mipt.CryptoContextBehavior = <i>ResetNever</i>



media5corp.com