

Redirecting an audio file to a SIP call using `/call/inject_sound`

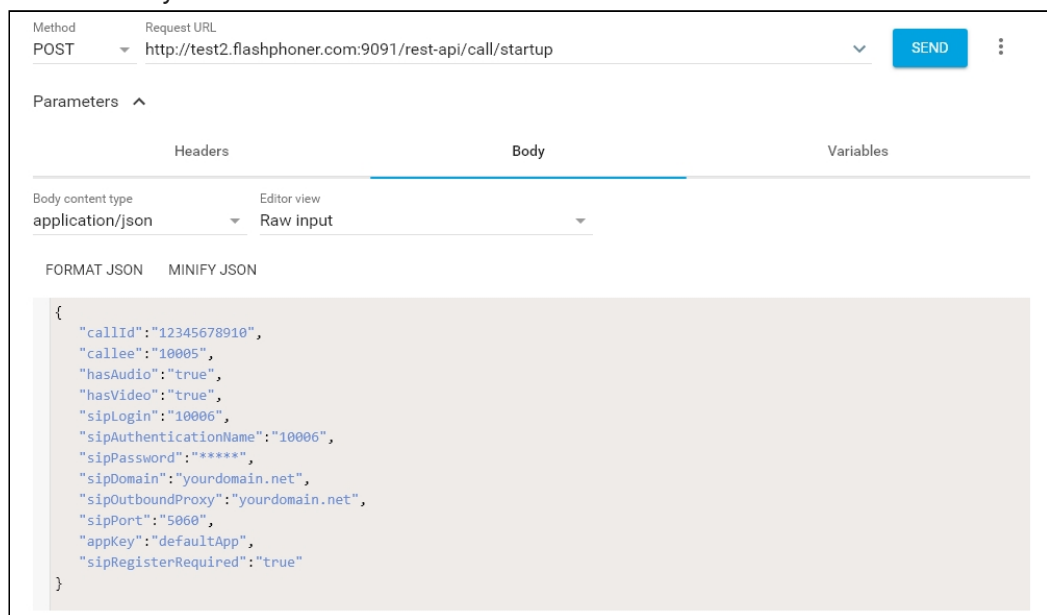
1. For the test we use:

- two SIP accounts;
- a softphone to answer the call;
- the [REST client](#) in the Chrome browser.

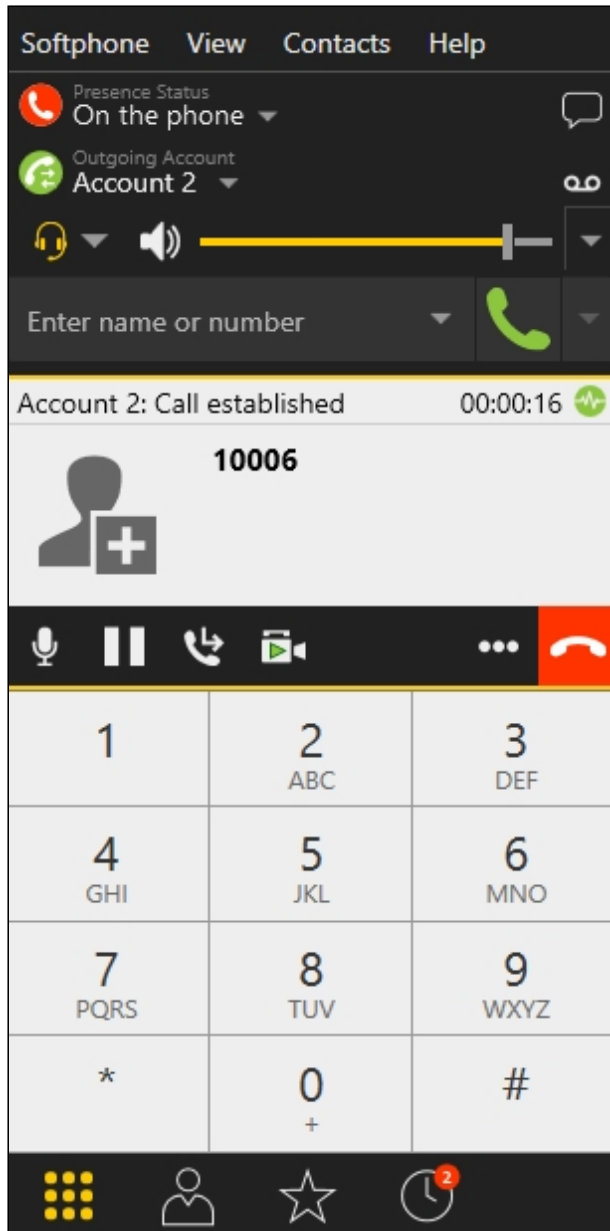
2. On the WCS server create a directory: `/usr/local/FlashphonerWebCallServer/media`. Put a file in the RIFF WAV format there, for example `test.wav`.

3. Open the [REST client](#). Send the `/call/startup` query to the WCS server and specify in its parameters:

- parameters of your SIP account the call is made from
- the name of your second SIP account the call is made to



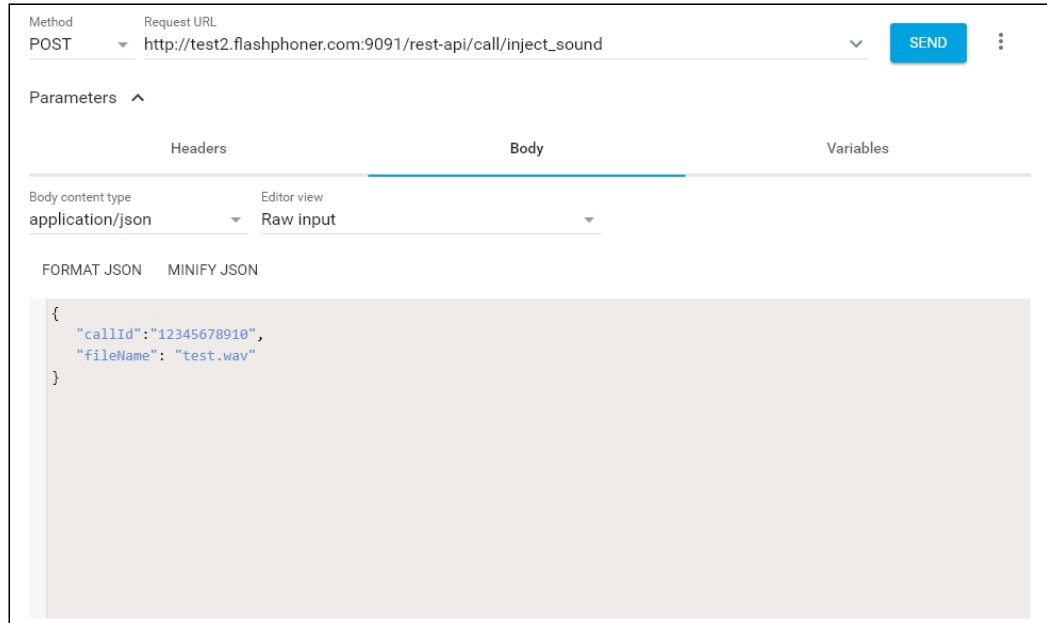
4. Receive the call in the softphone:



5. From the REST-client send the `/call/inject_sound` query to the WCS server and specify in the query's parameters:

- the identifier of the call

- the name of the applied audio file `test.wav`



6. Make sure the softphone plays the test file.
7. To terminate the call, click the corresponding button in the softphone.

Known issues

1. There is no sound when injecting file to a call stream

Symptoms

REST API query was correct with response code 200 OK, but there is no sound from file in the stream.

✓ **Solution**

a) in `flashphoner.properties` file set the following parameter

```
generate_av_for_ua=all
```

b) in softphone settings specify a STUN server address, for example

`stun.l.google.com:19302` on the appropriate page of SIP account settings

The screenshot shows a web interface for SIP account settings. At the top, there are tabs for 'Account', 'Voicemail', 'Topology', 'Presence', 'Transport', and 'Advanced'. The 'Topology' tab is selected and highlighted with a yellow border. Below the tabs, there are two main sections: 'Firewall Traversal' and 'Port Ranges'. The 'Firewall Traversal' section has a title 'Firewall Traversal' and a label 'Firewall traversal method:'. It contains four radio button options: 'Auto-detect firewall traversal method using ICE (recommended)', 'Discover public IP address (STUN)', 'Use media relay (TURN)', and 'None'. The 'Auto-detect' option is selected. Below these options are three input fields: 'Server address:' with the value 'stun.l.google.com:19302', 'User name:', and 'Password:'. The 'Port Ranges' section has a title 'Port Ranges' and two checked checkboxes. The first checkbox is labeled 'Range of ports used for signaling' and has two input fields with the value '0'. The second checkbox is labeled 'Range of ports used for RTP' and has three input fields: 'Audio:' with '0', and 'Video:' with '0'. Each input field is followed by a hyphen and another input field with '0'.