Grandstream Networks, Inc.

UCM6XXX WebRTC Demo Guide

Table of Contents

Table of Figures

OVERVIEW

The UCM6xxx supports HTTP & WebSocket for web browser to register to the UCM and establish calls with other endpoints in real time via webRTC. This document describes how to set up an easy WebRTC connection through UCM6xxx webUI User Portal.

Note: UCM6xxx series include UCM6100 series (UCM6102, UCM6104, UCM6108 and UCM6116), UCM6200 series (UCM6202, UCM6204 and UCM6208) and UCM6510.

CONFIGURING HTTP & WEBSOCKET

On the UCM6xxx web UI, the users need firstly configure HTTP and WebSocket in order for the webRTC client to establish connection with the UCM.

1. Log in UCM6xxx webUI and navigate to **PBX**->**Value-added Features**->**HTTP & WebSocket**.
2. Select the checkbox for “Enable HTTP”.
3. Enter the **UCM IP address** in “HTTP Bind Address” field, e.g., 192.168.40.214.
4. Enter the port number for “HTTP Bind Port”. The default “HTTP Bind Port” is 8088. Once configured, the UCM6xxx will listen on HTTP connection through port 8088.
5. If the users would like to use TLS for security purpose, select the checkbox for “TLS Enable”. Then enter the “TLS Bind Address” of the UCM IP Address with port number, e.g., 192.168.40.214:8445. The default port number is 8445.

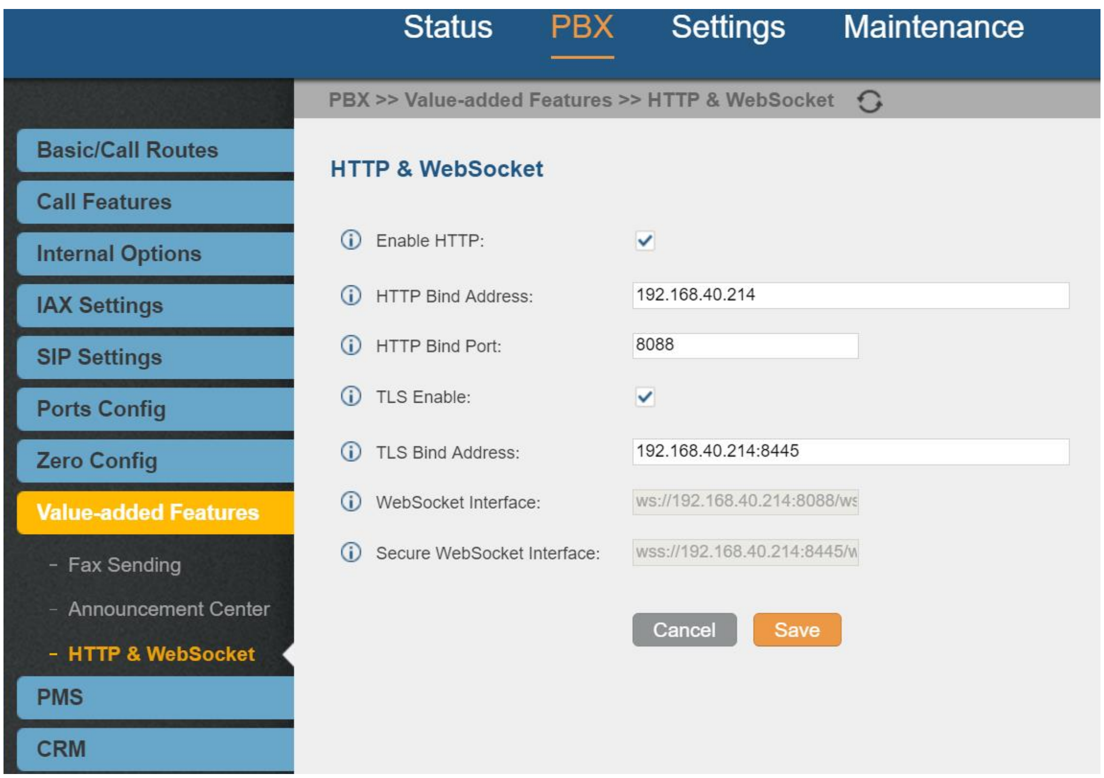

Figure 1: HTTP & WebSocket

6. Once the above are configured, the WebSocket Interface and Secure WebSocket Interface will be automatically filled up.
   For example:
   WebSocket Interface: *ws://192.168.40.214:8088/ws*
   Secure WebSocket Interface: *wss://192.168.40.214:8445/ws*
7. Save and apply the change.

The following table shows the detailed description for all the options in HTTP & WebSocket section.

Enable HTTP	Enable it to allow WebRTC user (such as Chrome or Firefox) to register to UCM6xxx via HTTP.
HTTP Bind Address	Configure IP address for HTTP server on the UCM61xx to bind to. When HTTP Bind Address set to 0.0.0.0, it means UCM6xxx will listen on all the socket connections through HTTP Bind Port.
HTTP Bind Port	Configure the port for the HTTP server on the UCM6xxx that binds to. By default, it is set to 8088.
TLS Enable	Enable it to allow WebRTC user (such as Chrome or Firefox) to securely register to UCM6xxx via HTTPS, by default it is disabled.
TLS Bind Address	Configure IP address for TLS server on the UCM6xxx to bind to. When TLS Bind Address set to 0.0.0.0, it means the UCM6xxx will listen on all the socket connections through the configured port. By default, the port number is set to 8445. Note: By default the TLS Bind address is 0.0.0.0:8445, which means binding to all interfaces via port 8445. CDR API using TLS is using the same port number. To avoid conflict, please manage different port number accordingly when both WebSocket TLS and CDR API TLS feature are enabled.
WebSocket Interface	Indicates WebRTC URL that will be used to connect to UCM6xxx via HTTP. WebSocket Interface is associated with HTTP Bind Address and Port. For example, if HTTP Bind Address and Port set to 192.168.1.2:8088, WebSocket Interface will be ws://192.168.1.2:8088/ws
Secure WebSocket Interface	Indicates secure WebRTC URL that will be used to connect to UCM6xxx with HTTPS. Secure WebSocket Interface is associated with TLS Bind Address. For example, if TLS Bind Address set to 192.168.1.2:8445, Secure WebSocket Interface will be wss://192.168.1.2:8445/ws

8. Check the UCM HTTP & WebSocket status using the following link:

   For HTTP:

   http://UCM_IP_ADDRESS:PORT/httpstatus

   UCM_IP_ADDRESS should be your UCM’s IP address, PORT number is the same as configured in “HTTP Bind Port”. For example, http://192.168.40.214:8088.

If TLS is enabled, use the following link instead:

https://TLS_BIND_ADDRESS/httpstatus

TLS_BIND_ADDRESS should be the same as configured in "TLS Bind Address". For example, https://192.168.40.214:8445.

A warning prompt will pop up for you to confirm the security risk. Once confirmed, the following Asterisk information will be displayed.

Please note: Since UCM6xxx is using self-signed certificate, the WebRTC connection will be dropped by browser by default unless the user confirms the security risk.

Asterisk™ HTTP Status

Server	**Asterisk/13.4.0**
Prefix	
Bind Address	**192.168.40.214**
Bind Port	**8088**
SSL Bind Port	**8445**

Cookie 'jumpMenu'	sip_webrtc.html
Cookie 'locale'	en-US
Cookie 'localeDirection'	ltr
Cookie 'position'	home
Cookie 'first_login'	no
Cookie 'is_strong_password'	0
Cookie 'role'	privilege_0
Cookie 'html'	%7B%22upgrade%22%3A1%2C%22backup%22%3A1%2C%22backup_network%22%3A1%2C%22auto_cleaner email%22%3A1%2C%22webserver%22%3A1%2C%22smtp_settings%22%3A1%2C%22datetime%22%3A1%2C
Cookie 'user_id'	0
Cookie 'username'	admin
Cookie 'session-identify'	sid1985282665-1484355500
Cookie 'TRACKID'	c96cea1303432ff88fcb324a5a207002

Asterisk and Digium are registered trademarks of Digium, Inc.

Figure 2: HTTP & WebSocket Status

ENABLING WEBRTC FOR EXTENSION

Before using the demo in UCM user portal, the users need to enable WebRTC for this extension.

1. Log in UCM6xxx web UI and navigate to **PBX**->**Basic/Call Routes**->**Extensions**.
2. Select the extension to edit and open tab "Features".
3. Select the checkbox for "Enable WebRTC Support".
4. Save and apply the setting.

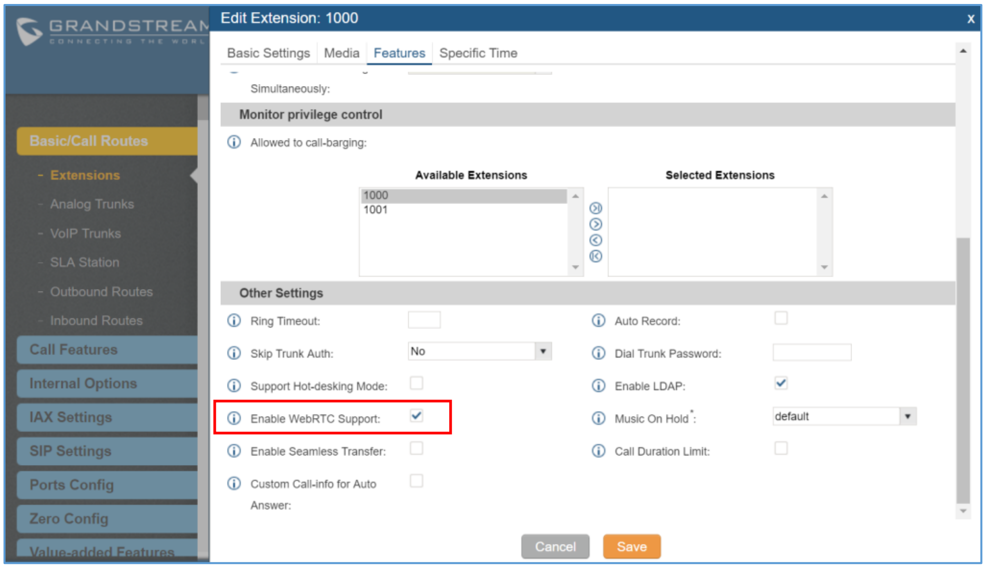

Figure 3: Enable WebRTC Support

5. Check the extension in **PBX**->**Basic/Call Routes**->**Extensions** page. The above extension will have its terminal type shown as "SIP(WebRTC)".

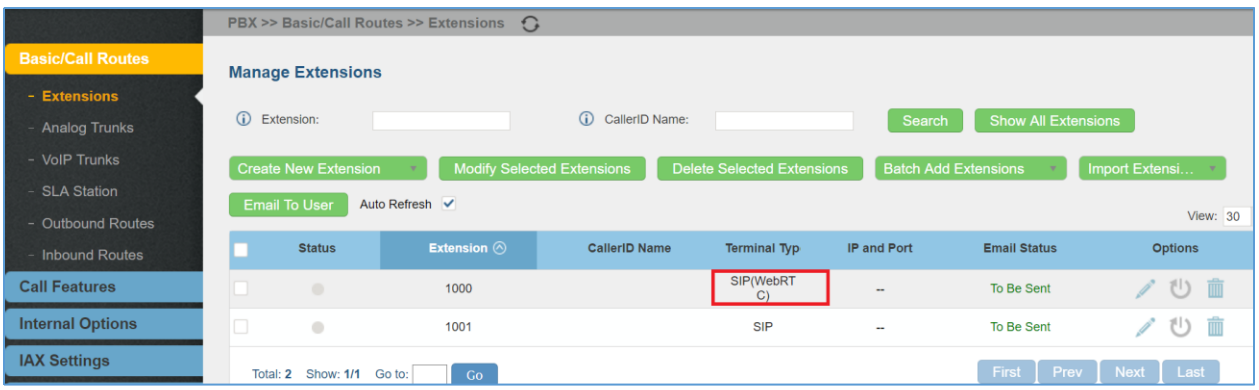

Figure 4: Extension with WebRTC Enabled

USING USER PORTAL DEMO

1. On the UCM6xxx web UI, log in user portal with the extension number the user password.

   Please note the user password for the extension to log in user portal is initially created with admin access under UCM6xxx **web UI**->**PBX**->**Basic/Call Routes**->Edit extension. Please consult with your UCM admin for the user password for your extension to log in user portal.

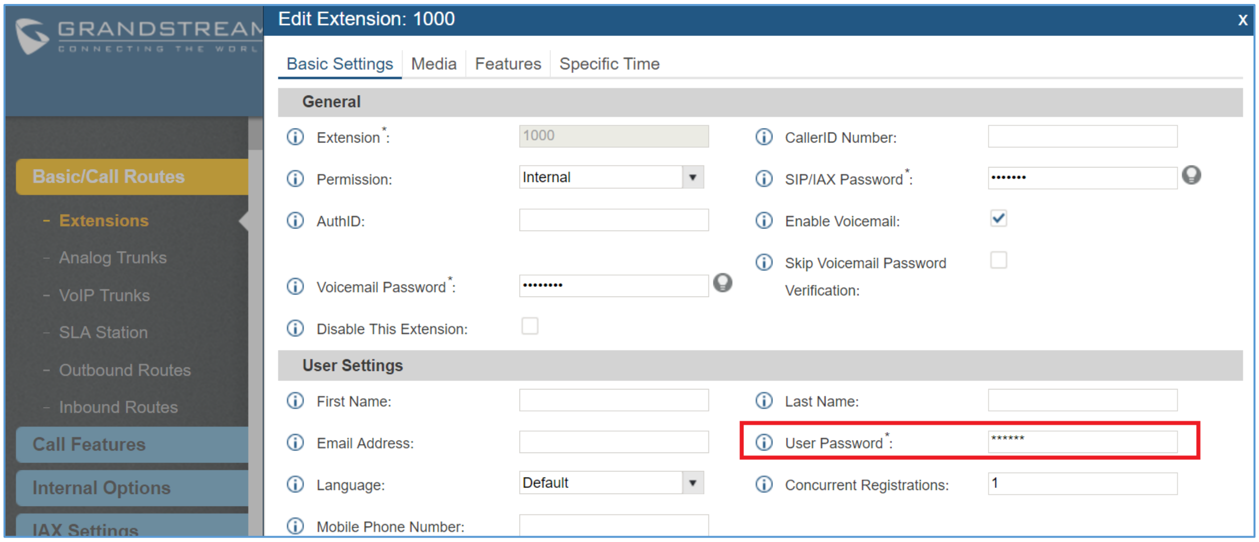

Figure 5: Extension User Portal Password

2. In the user portal web UI**->Value-added Features->WebRTC**, WebRTC settings will be automatically filled up with the previously configured information in above steps.

   Please make sure the password is the one used to register the SIP extension. Also, the WebSocket Server URL is in the format of **ws://192.168.40.214:8088/ws**, or **wss://192.168.40.214:8445/ws** if TLS is enabled.

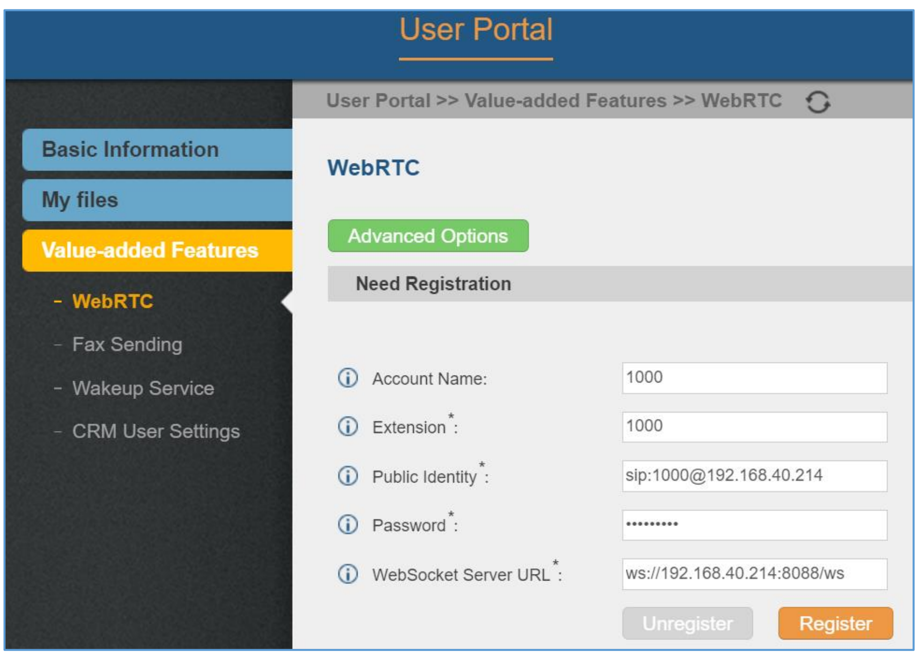

Figure 6: User Portal->Value-added Features: Register

3. Click on "Register" button on the above picture. The connected status will show in a few seconds.

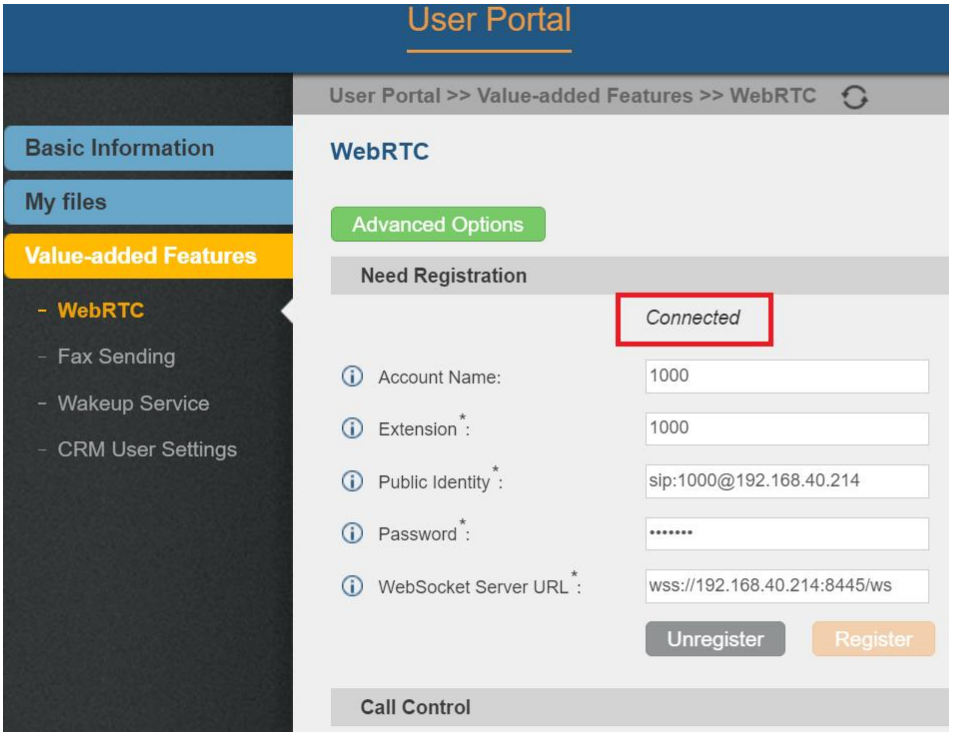

Figure 7: User Portal->Value-added Features: Connected

4. Now the users can make call from the user portal. Enter the number to call and select "Audio" or "Video" call. Call control options are also available once the call is established.

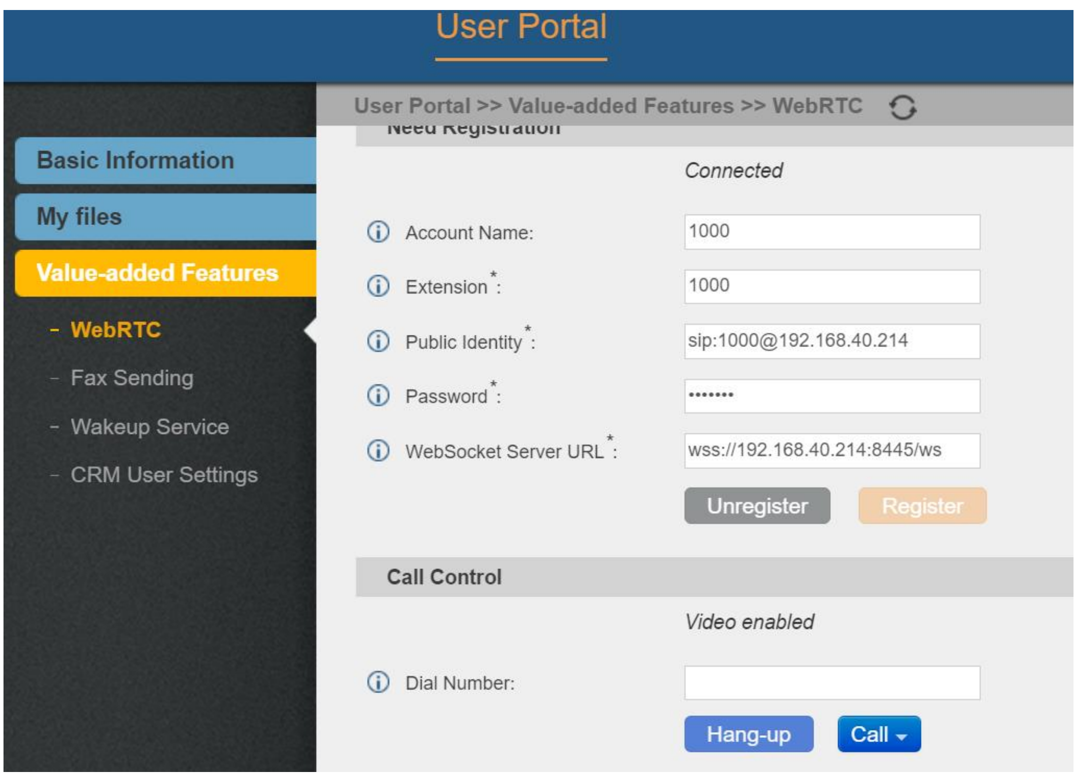

Figure 8: Dial Number

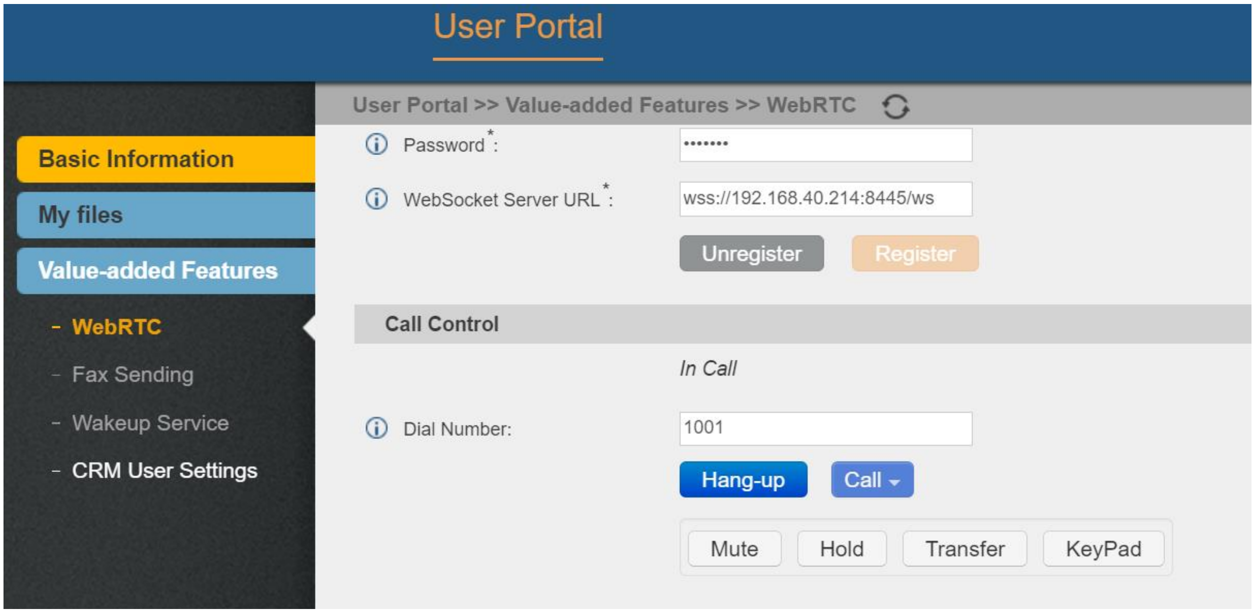

Figure 9: Call Control

Note:

- It is recommended to enable TLS for HTTP & WebSocket because web browser might have security restrictions to use HTTP for webRTC.

REFERENCES

Users could find reference in below website, which includes live demo as well as source code:

http://www.doubango.org/sipml5/

1. Open the above link and click on "Enjoy our live demo".

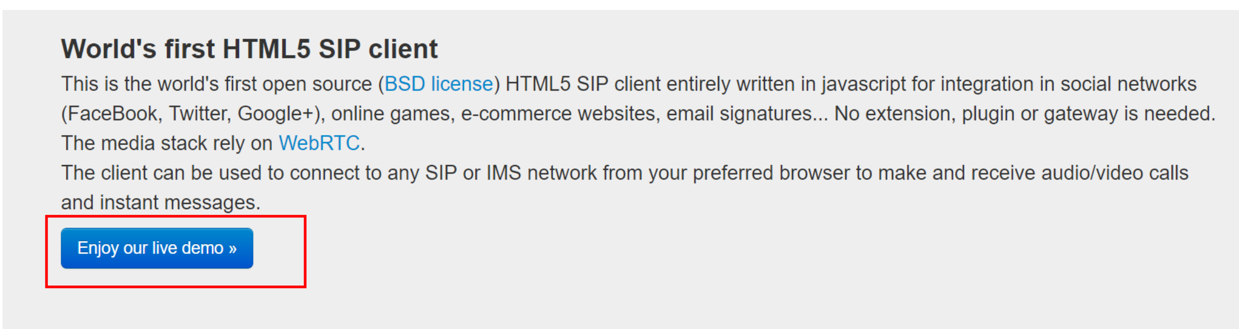

Figure 10: Click on "Enjoy our live demo"

2. Click on "Expert mode".

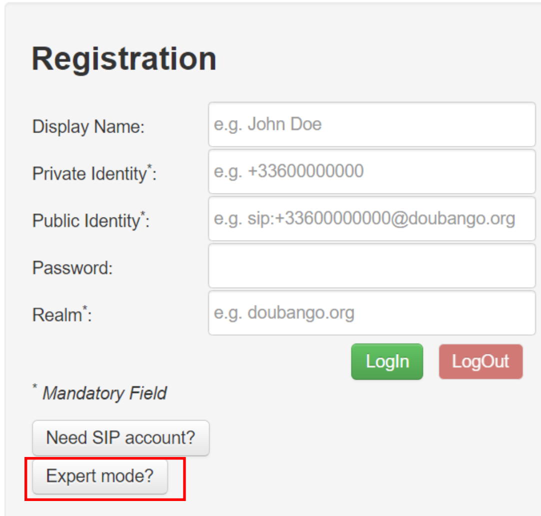

Figure 11: Click on "Expert mode"

3. Enter the WebSocket Server URL to the same one as shown in UCM configuration ***Figure 1: HTTP & WebSocket***. Click on "Save".

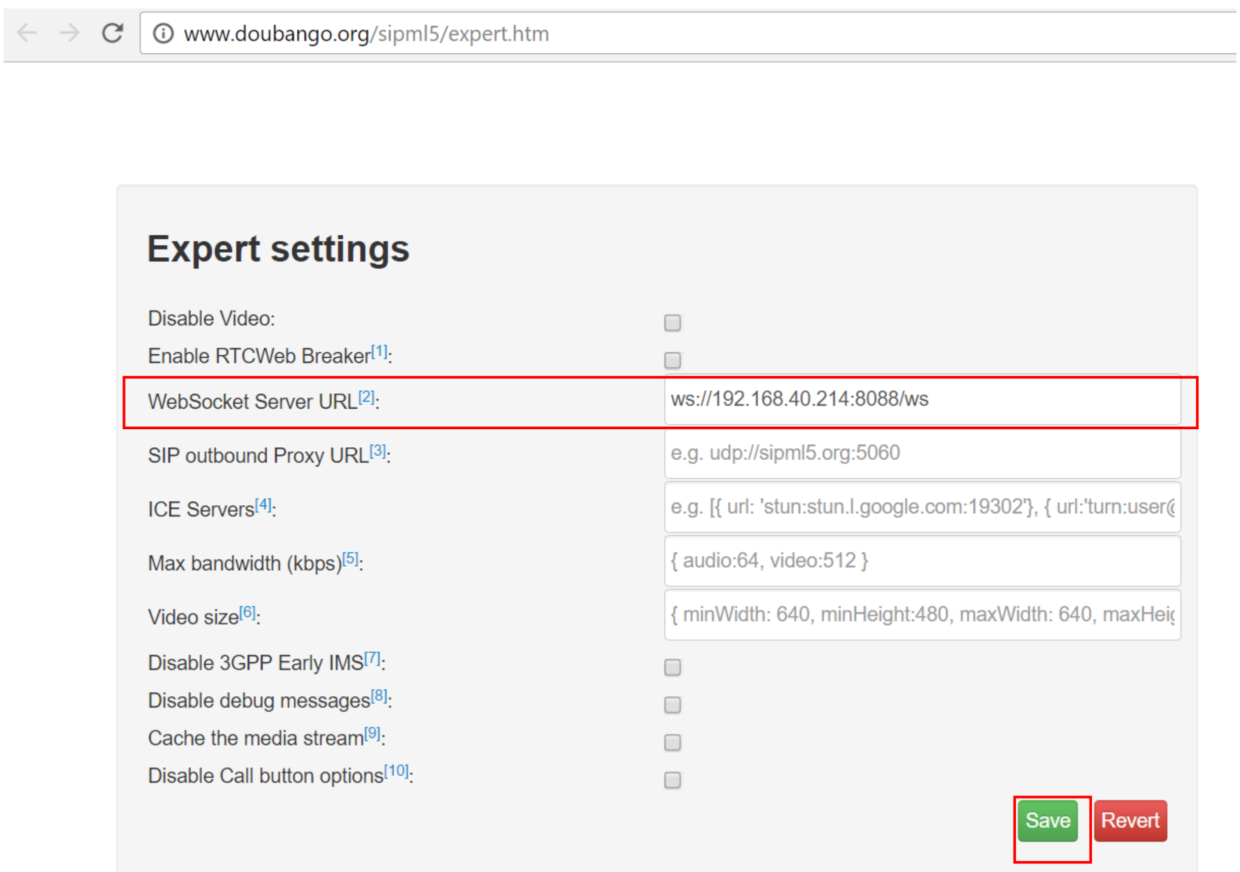

Figure 12: WebSocket Server URL

4. In "Registration" page, fill up "Display Name", "Private Identity", "Public Identity", "Password" and "Realm".

   "Display Name": The name you would like to display when calling the remote party.

   "Private Identity": The SIP User ID on UCM.

   "Public Identity": The SIP URI for this extension, in the format of sip:extension@ucm_ip.

   "Password": This is the password used to register the SIP extension

   "Realm": Enter "Grandstream" here.

5. Click on "Login".
6. Once the extension is successfully logged in, enter the number to call to establish call.
7. Call control options are also available once the call is established.

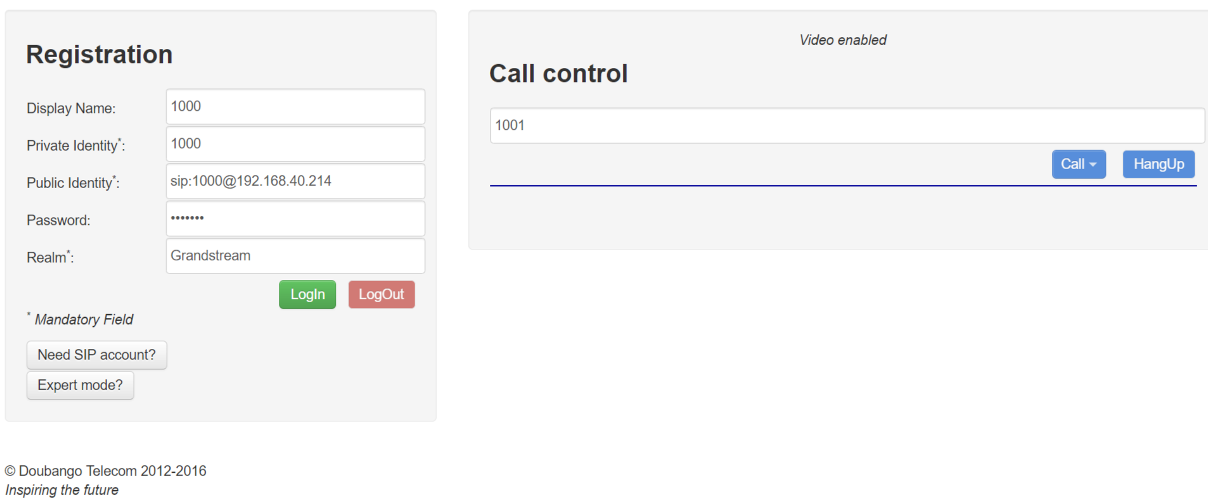

Figure 13: Registration and Call Control