AudioCodes MP202 FXS gateway

Rainbow Hub provisioning guide

Guide version: 1.3

MP202 version: 4.4.9_build_144

Document revisions

Revised on	Version	Description	Revised by
01.09.2020	1.0	Initial version	YM
26.05.2021	1.1	Adopted to reflect TLS 1.2 and SIP proxy requirements	MC
12.12.2021	1.2	Added certificate upload section; refresh with updated screenshots	YM
26.05.2023	1.3	Refresh certificate upload section	CM

Contents

1. General

This document provides overview of AudioCodes MP202 FXS VoIP gateway (ATA), when used for connection of analog device to Rainbow Hub.

Configuration on Rainbow Hub side (user creation, license allocation, obtaining of SIP account password and domain) is not covered by this document.

2. Rainbow integration parameters

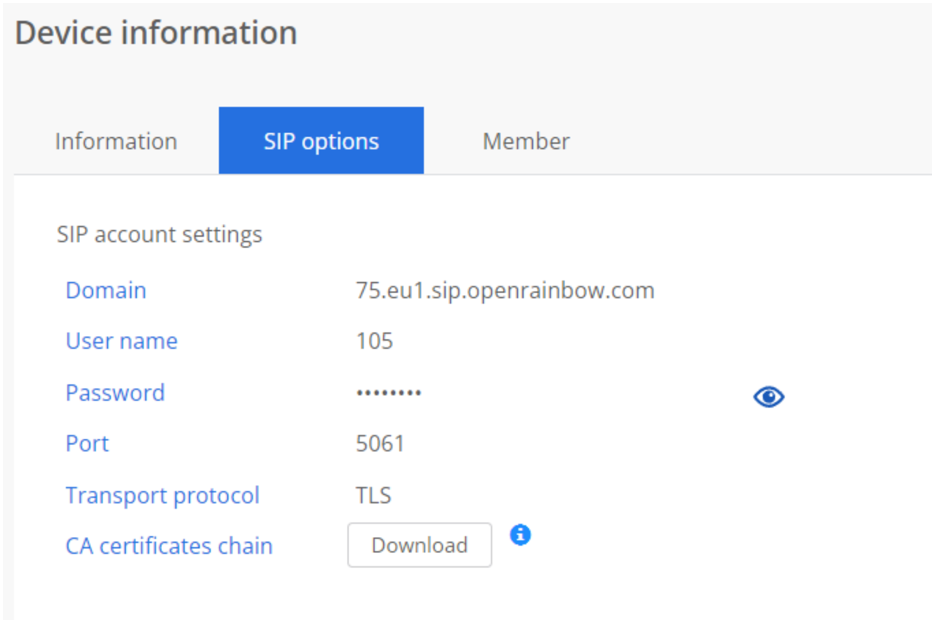
There is a number of provisioning parameters related to Rainbow that need to be configured in the MP202 device. Below information must be obtained per each connected analog device from Rainbow Company Administration interface - under *Communication – Devices – SIP options* prior to MP202 configuration:

- **SIP registrar domain name** (e.g. *75.eu1.sip.openrainbow.com)* and port (e.g. *5061*)
- **SIP proxy domain name** (e.g. *lb02.eu1.sip.openrainbow.com*) and port (e.g. *5061*)
- **SIP User name** (e.g. *105*) – usually equals to extension number
- **SIP Password**
- **CA certificate chain** (download a *.pem file)

  Note: you may need to split the downloaded certificate *.pem file into three separate certificates, using any text editor (e.g. Notepad).

  Rainbow SIP certificates are signed by an official authority (The USERTRUST Network) that might be already trusted by some equipment. In that case there is no need to upload any certificates. Rainbow certificates are already accepted by the equipment firmware.

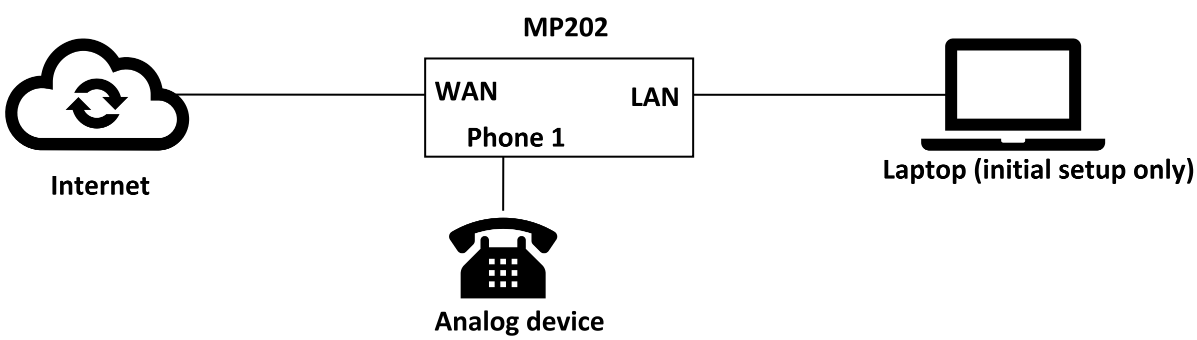
  Only the third certificate (the Root CA) of the chain is mandatory and must be uploaded if not already embedded in the equipment; It expires on 19th January 2038 (fingerprint HA-256: E7 93 C9 B0 2F D8 AA 13 E2 1C 31 22 8A CC B0 81 19 64 3B 74 9C 89 89 64 B1 74 6D 46 C3 D4 CB D2).


Device information
Information
SIP options
Member
SIP account settings
Domain
75.eu1.sip.openrainbow.com
User name
105
Password
••••••••
Port
5061
Transport protocol
TLS
CA certificates chain
Download

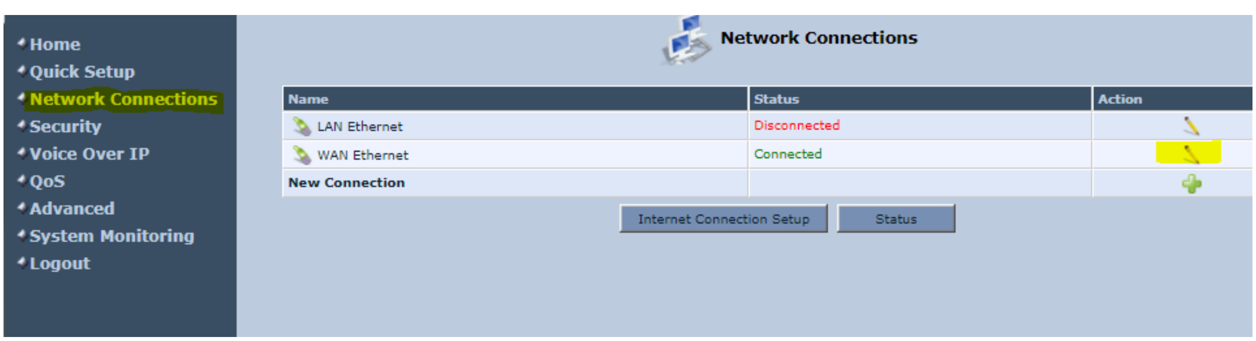
3. IP address configuration

MP202 can provide, in addition to FXS to SIP gateway function, multiple additional functions: firewall, NAT, routing, etc. For the purpose of pure FXS SIP gateway, those functions are not required. To simplify further management of MP202, there are few changes that should be done to the configuration.

Typically, the MP202 will be connected to customer network via WAN Ethernet interface, and LAN interface will be not utilized. However, initial configuration of the MP202 must be done by a PC, connected to the LAN interface. The PC LAN adapter needs to be configured with Automatic IP address assignment – DHCP (MP202 runs DHCP server on LAN interface).

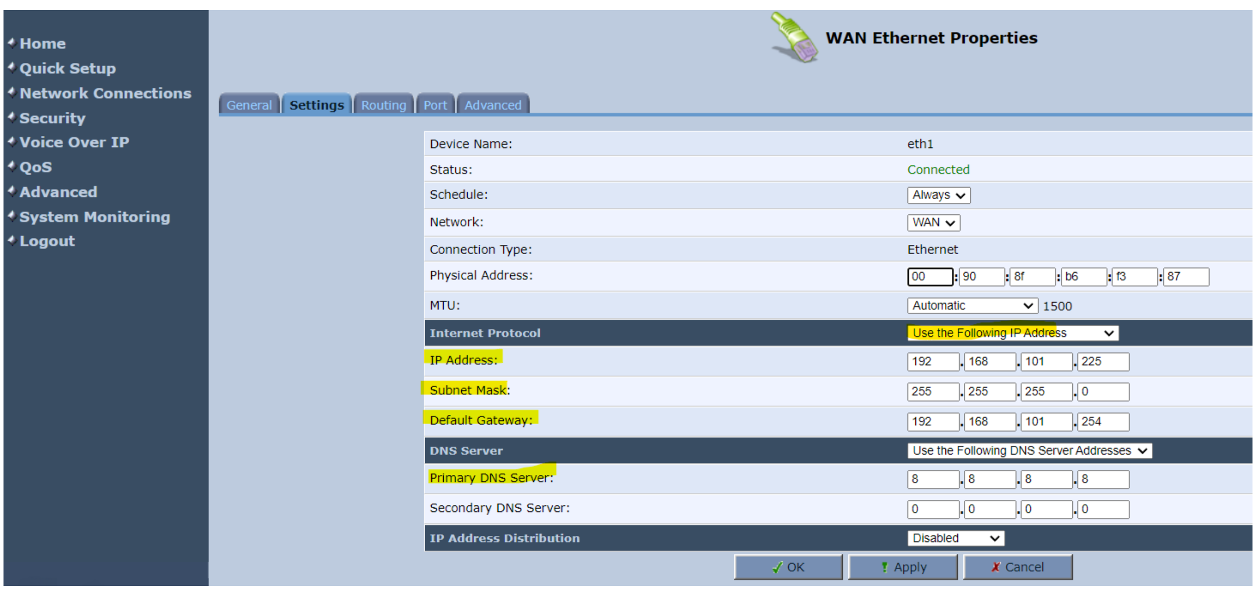


- Connect **WAN** port of MP202 to customer's LAN
- Connect laptop ethernet port to MP202 **LAN** port
- On your PC, verify that the Local Area Connection status is "Connected", by clicking Start > Settings > Network Connections, and then double-clicking the Local Area Connection icon.
- If the LAN status is "Disconnected", click Properties, select 'Internet Protocol (TCP/IP)', and then click Properties; ensure that the 'Obtain an IP address automatically' option is selected.
- Open a Web browser and enter the URL address http://MP20x.home (or http://MP202.home)
- Default username of MP202 is admin; default password is admin. It is recommended to change the password and write it down
- Go to Network Connections menu, and click "edit" icon on the right of WAN Ethernet interface:

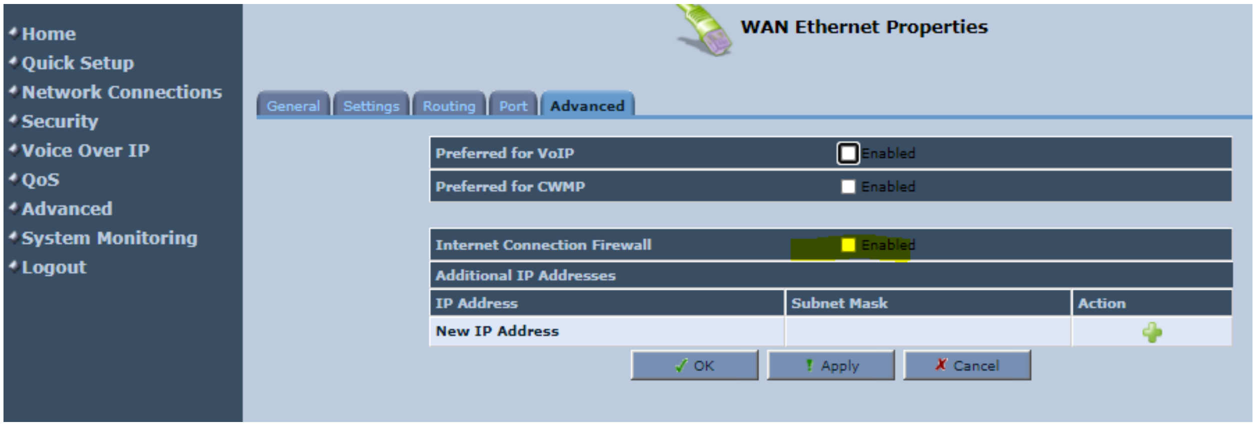


- By default, WAN interface obtains its IP address, mask, default gateway and DNS address from customer's DHCP server. Verify that the parameters obtained from DHCP are correct.

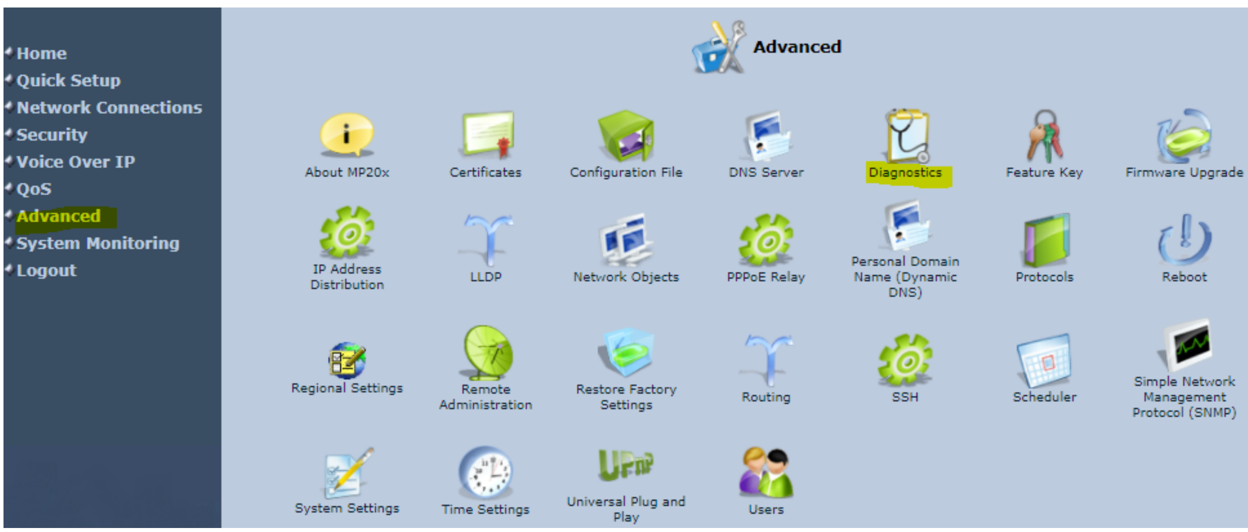
- If needed, the IP parameters can be set statically by going to Settings menu. After configuring **all** parameters, click Apply:

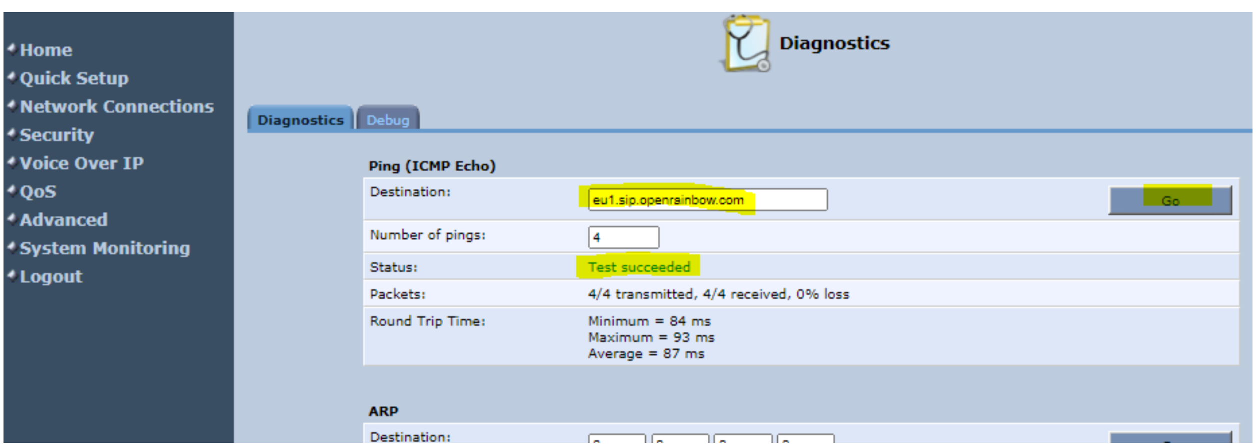


- Go to "Advanced" top menu, and disable Internet Connection Firewall. This will allow you to connect to the MP202 via WAN interface IP address; you will not need the LAN port anymore



- Click “Apply” to save the settings
- Go to Advanced / Diagnostics and check connectivity to *eu1.sip.openrainbow.com*. Both resolving and ping should work

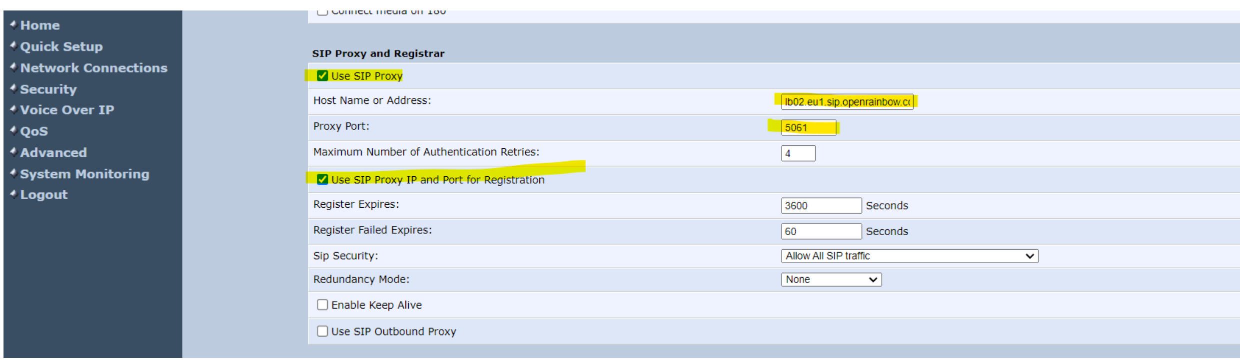




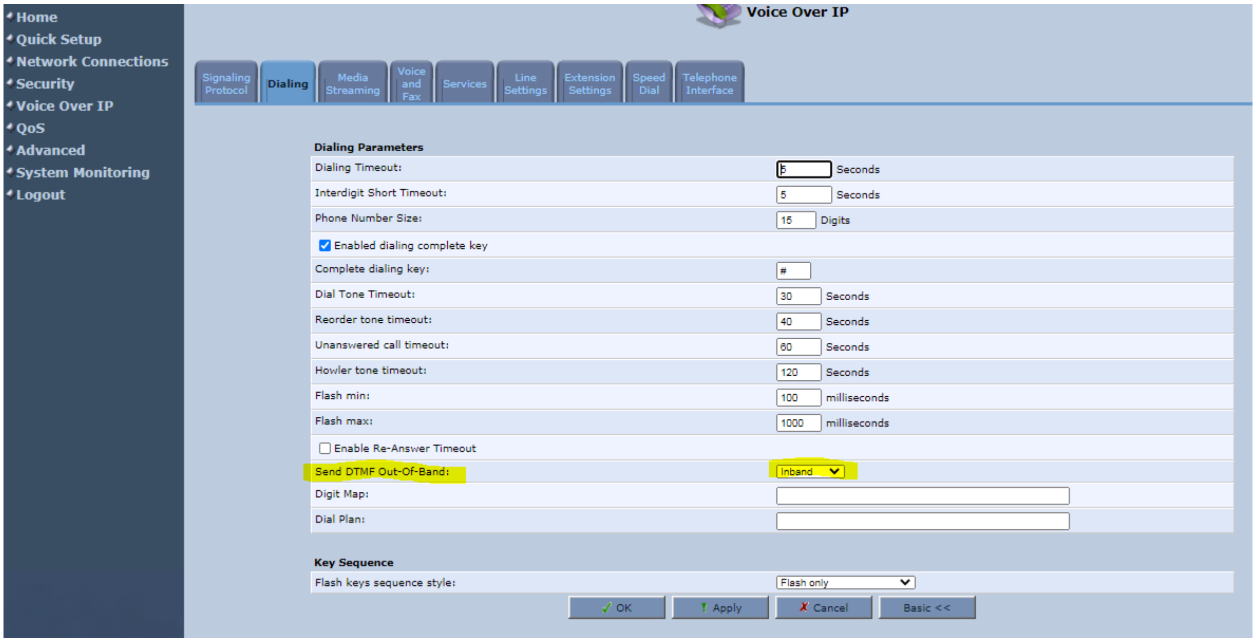
3. Voice over IP configuration

- Go to "Voice over IP" main / Signaling Protocol" menu, click on "Advanced" at the bottom and configure TLS as "SIP Transport Protocol", and "Gateway name – User domain value". Use domain value obtained from Rainbow Provisioning (e.g. *75.eu1.sip.openrainbow.com*):

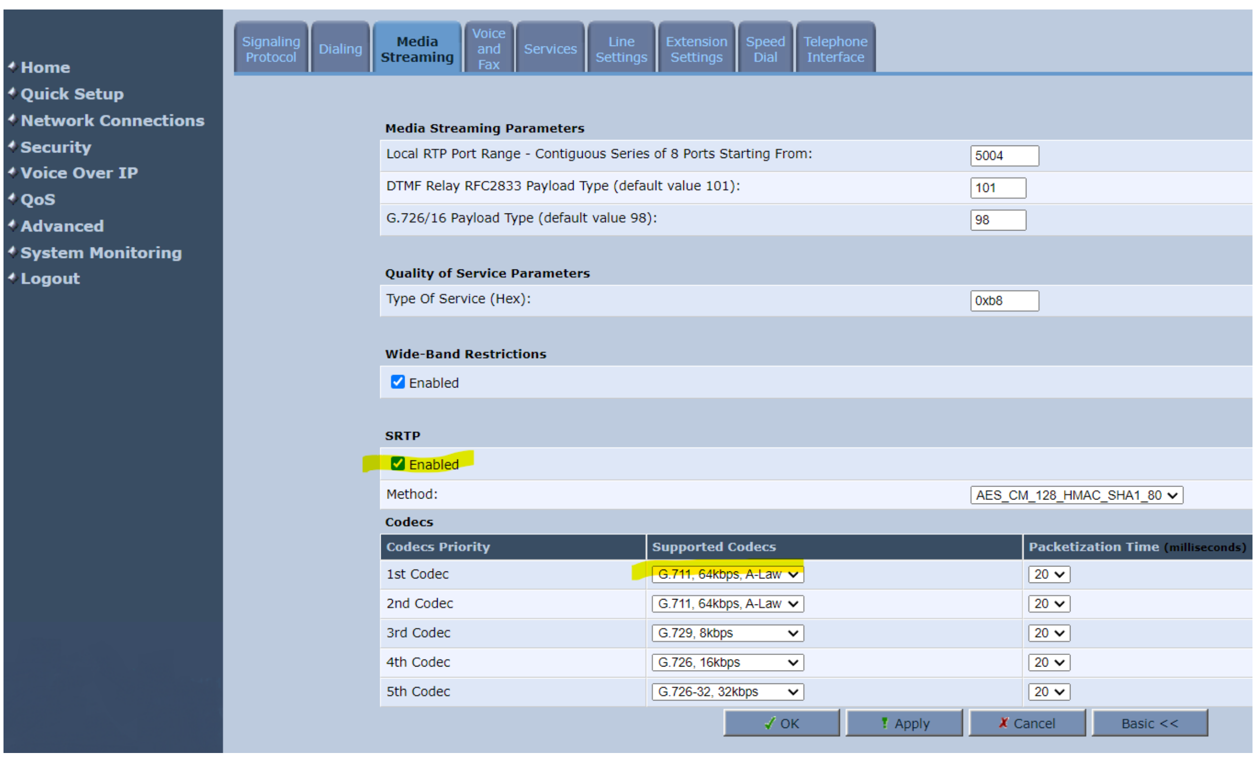
- Enable "Use SIP Proxy" and "Use SIP Proxy IP and Port for Registration". Configure "Host name" and "Proxy Port" with values obtained from Rainbow Provisioning (e.g. *lb02.eu1.sip.openrainbow.com* port *5061*):



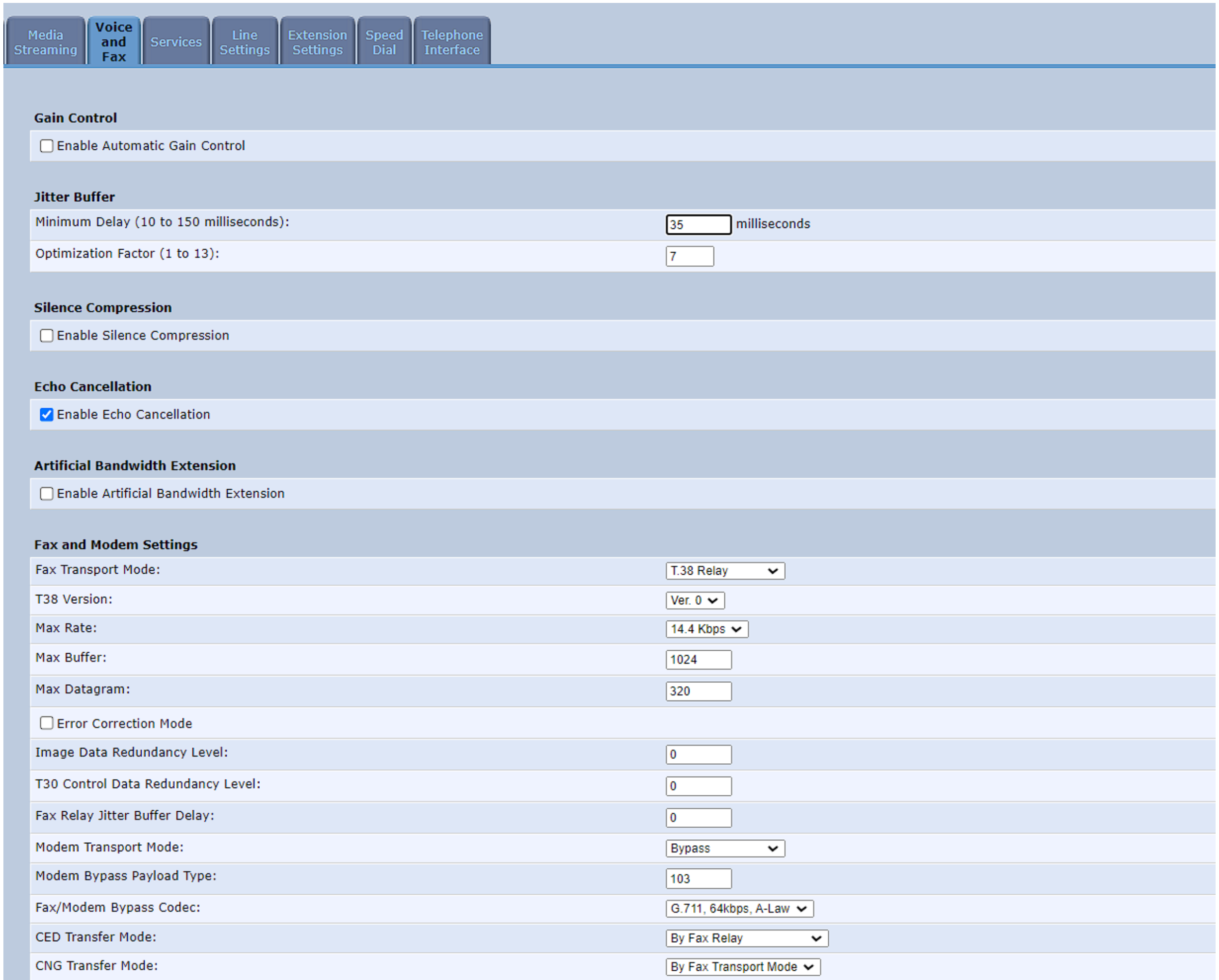
- Click "Apply" to save the changes
- Go to "Dialing" top menu, click on "Advanced" and enable Inband DTMF:



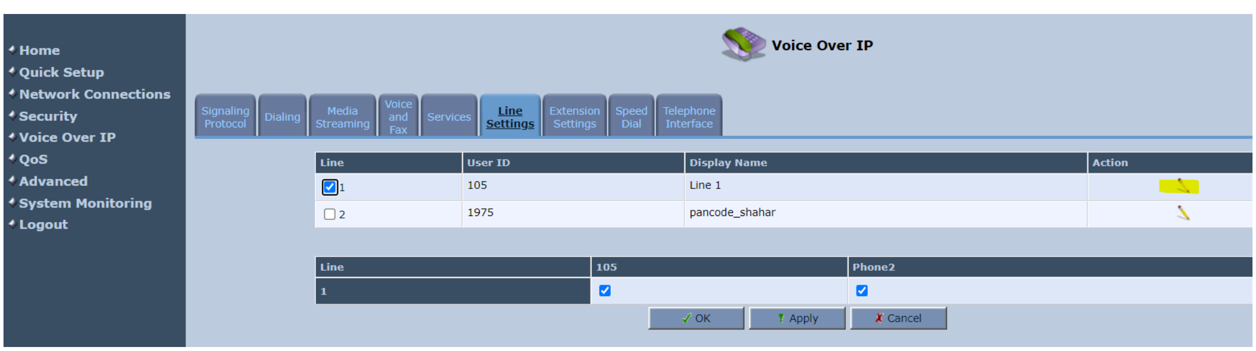
- Click “Apply” to save the changes
- Go to “Media Streaming” top menu and change default 1st codec from u_Law to A-Law; enable SRTP:

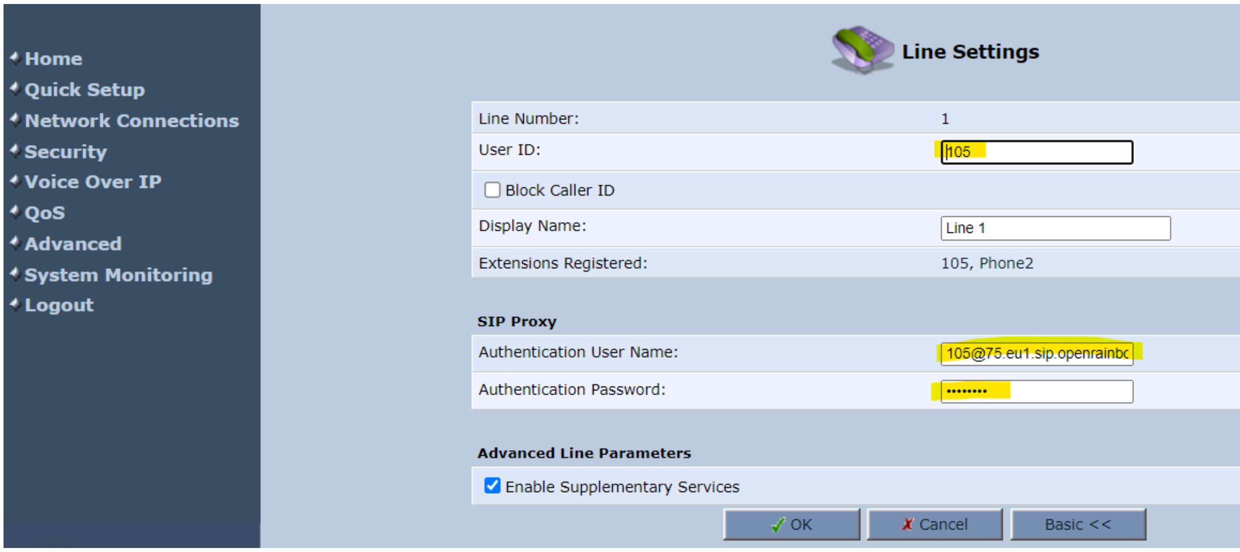


- Click “Apply” to save the changes
- Go to “Voice and Fax” top menu and configure below parameters. Click “Apply” when finished.



- Go to “Line Settings”, and click edit icon to configure SIP parameters for each analog device, connected to the MP202 phone port (SIP parameters should be obtained from Rainbow Provisioning)
  - “User ID” – should be extension number (e.g.105)
  - “Authentication user name” – **SIP user name**; should be in format of <User name>@<SIP Domain name>’ e.g. 105@75.eu1.sip.openrainbow.com
  - “Authentication password” – **SIP password** as obtained from Rainbow provisioning

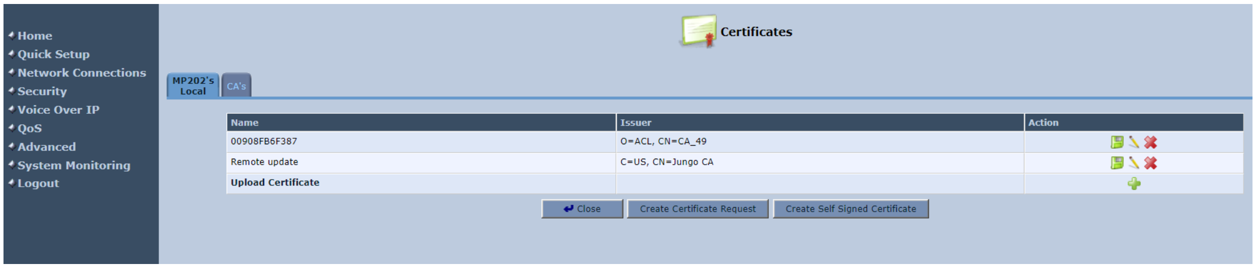




- Click "OK" after configuring above parameters, and" Apply" on "Line settings" screen

4. CA Certificate upload

- Go to Advanced left panel menu – Certificated
- Click on “CA” tab



- Click on “Upload Certificate” and choose the third part of the CA certificates file downloaded from Rainbow provisioning. Verify that certificate is uploaded correctly.
    - Note: the pem file downloaded from Rainbow contains all the certificates chain used by Rainbow. Only the third one must be uploaded, you need to use any text editor to split the downloaded *.pem certificate file into three separate files, and upload it: