Integrated Networking Solutions

IP PHONE

VP-17P

User manual

Firmware version 1.3.1

Username: admin

Password: password

Contents

1 VP-17P description

1.1 Purpose

To provide VoIP services to network subscribers, VP series IP phones have been developed. The devices are aimed at home users and small offices, and are also suitable for organizations with high requirements to transmitted voice data, stability and usability.

VP-17P is an IP phone providing voice services and PC connection to IP network via single cable. The device supports PoE technology and has advanced functionality, high quality and universal style.

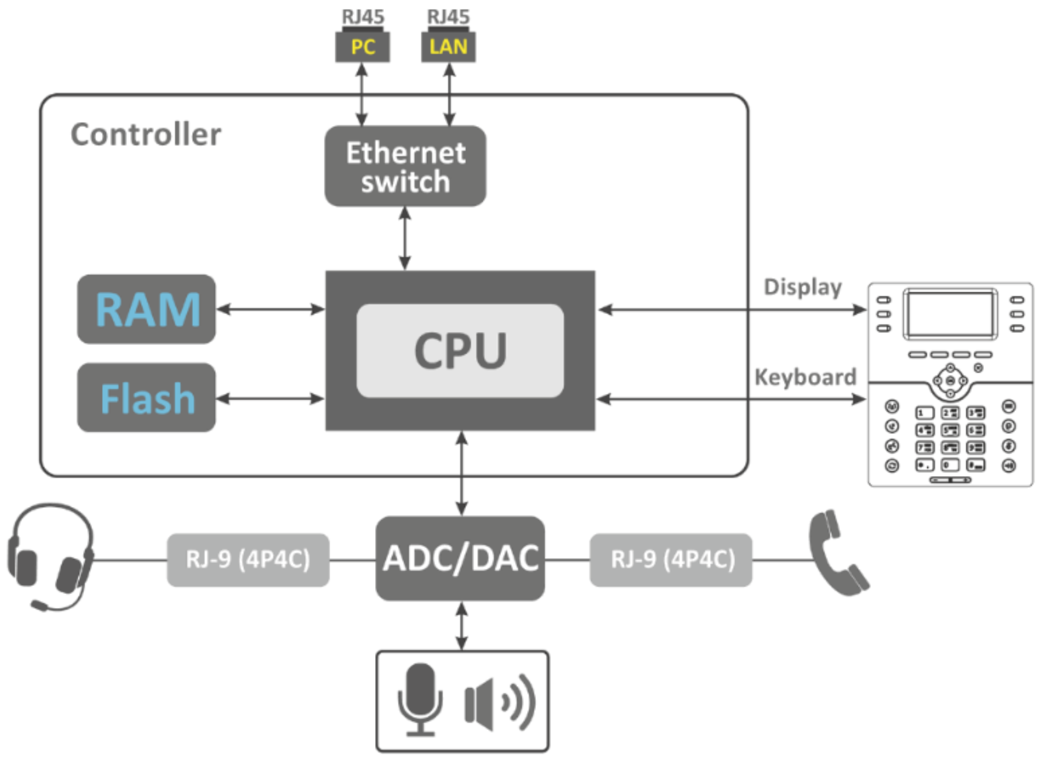
This user manual describes the purpose, main specifications, processes of configuring, monitoring, and changing the software of the VP-17P IP phone.

1.2 Device design and operating principle

VP-17P IP phone includes the following subsystem:

- Controller featuring:
    - highly-integrated System-on-a-Chip (SoC), including a CPU, 1 Gbps switch, hardware L2/L3/L4 acceleration;
    - flash memory — 265 MB;
    - SDRAM — 512 MB;
- Codec (ADC/DAC);
- Liquid crystal display (LCD) with 128 × 64 px resolution;
- Fully-featured digital keyboard with additional function keys;
- 1 × LAN port: RJ-45 10/100/1000BASE-T;
- 1 × PC port: RJ-45 10/100/1000BASE-T;
- 1 × Handset port: RJ-9 (4P4C) for connecting a handset;
- 1 × Headset: RJ-9 (4P4C) for connecting a headset.

Design diagram for the device is depicted in the figure below.



VP-17P design diagram

The device runs under Linux operating system. Basic control functions are performed by the processor which enables IP packet routing and VoIP operation.

1.3 Main specifications

General parameters	
Power supply	• 220 V AC/5 V DC, 2 A power adapter (optional) • PoE support IEEE 802.3af
Maximum power consumption	up to 4 W (max. current consumption is 0.8 A)
Operating temperature range	from +5 to +40 °C
Relative humidity at 25 °C	no more than 80 %
Dimensions (W × H × D)	205 × 210 × 86 mm
Weight	up to 0.8 kg
Lifetime	no less than 5 years
Interfaces	• LAN: 1 port of Ethernet RJ-45 10/100/1000BASE-T • PC: 1 port of Ethernet RJ-45 10/100/1000BASE-T • Handset: 1 RJ-45 (4P4C) port for connecting a handset • Headset: 1 RJ-45 (4P4C) port for connecting a headset

Ethernet LAN interface specification	
Number of ports	1
Electric port	RJ-45
Data transmission rate	10/100/1000 Mbps, autodetection
Standard support	BASE-T
Ethernet PC interface specification	
Number of ports	1
Electric port	RJ-45
Data transmission rate	10/100/1000 Mbps, autodetection
Standard support	BASE-T

Main features and capabilities

VoIP capabilities	
Supported protocols	SIP
Quantity of accounts	2
Key features	• 2 SIP accounts configured independently • Support for up to 3 redundant SIP servers • Flexible dialplan • Operation without SIP server • Caller name and number displaying (CallerID) • Mute • Redial • Different ringtones for accounts, opportunity to upload ringtones • Call History • Local Phonebook for 1000 phone numbers • Remote Phonebook • LDAP Remote Phonebook • Speakerphone mode • Message Waiting Indicator (MWI) • Busy Lamp Field (BLF)
Operation behind NAT	Public IP
Security	• SIP over TLS • SRTP
Voice features	• Acoustic Echo suppression (AES) • Voice Activity Detector (VAD) • DTMF signals detection and generation

DTMF signals detection and generation	• Inband • RFC2833 • SIP INFO
Codecs	• G.711a • G.711u • G.726-24 • G.726-32 • G.729
Supplementary services	• Call Hold • Call Transfer • Call Waiting • Call Forwarding Busy (CFB) • Call Forwarding No Reply (CFNR) • Call Forwarding Unconditional (CFU) • Do Not Disturb mode (DND) • Caller Line Identification Restriction (CLIR) • Hotline/Warmline • Automatic Call Answer • 3-Way Conference • Stop dialing by pressing # • Call Pickup • Remote Call Control
Network features	
Key features	• Opportunity to divide voip and pc-data traffic to different VLANs
Protocols	• Static IP • DHCP • No IP
Support for PPPoE	• PAP, SPAP and CHAP authorization • PPPoE compression
Support for DHCP option	• 1 — Subnet Mask • 3 — Router • 6 — Domain Name Server • 12 — Host Name • 15 — Domain Name • 26 — Interface MTU • 28 — Broadcast Address • 33 — Static Route • 42 — Network Time Protocol Servers • 43 — Vendor-Specific Information • 66 — TFTP ServerName • 67 — Bootfile name • 120 — SIP Servers • 121 — Classless Static Route • 132 — VLAN ID • 133 — Priority of VLAN • 249 — Private/Classless Static Route (Microsoft)
Support for QoS mechanisms	• DSCP • 802.1P
Support for DNS	• Static DNS servers addresses • Obtaining DNS servers addresses via DHCP

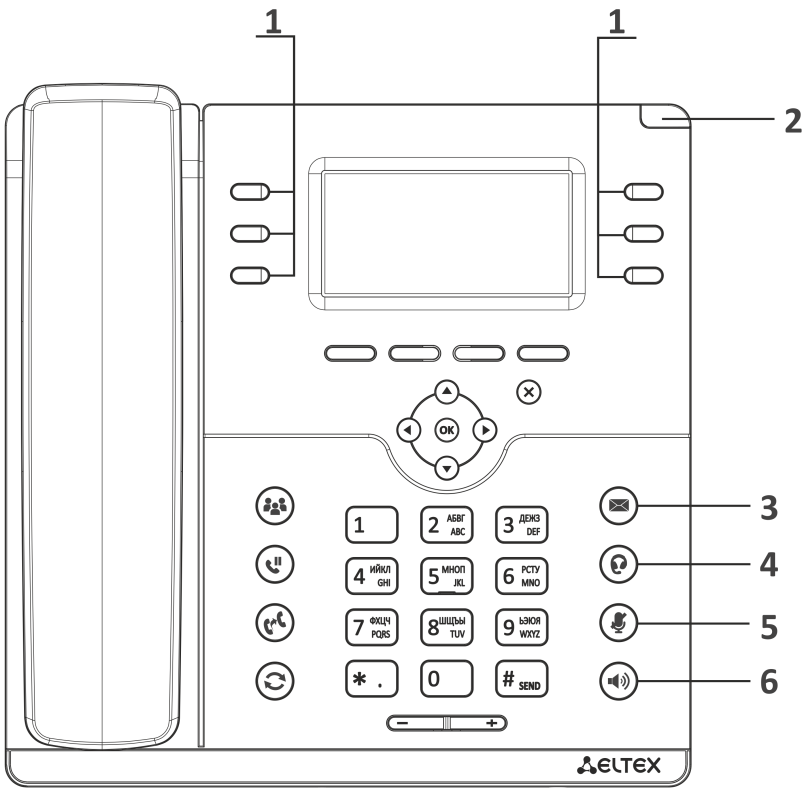
Support for NTP	• Static NTP server address assignment • Obtaining NTP server address via DHCP
Network access limitation	• Firewall • MAC filter
Routing	Routing rules assignment via DHCP (Option 33, 121, 249)
Network discovery	LLDP MED
Management and monitoring	
Key features	Flexible settings for access to display menu
Interfaces	• Web interface • SSH • Telnet • Display menu
Debug information output	• Console • Syslog • Syslog and File • File
Loading/updating of software and configuration	• Autoupdate by schedule • Periodical autoupdate

1.4 Design

VP-17P IP phone is enclosed into 205 × 210 × 86 mm plastic case.

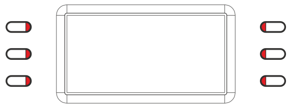
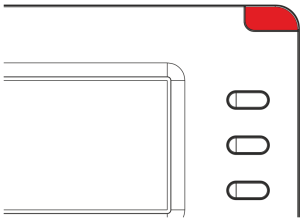
1.4.1 Top panel of the device. Light indication

The figure below shows VP-17P top panel layout.



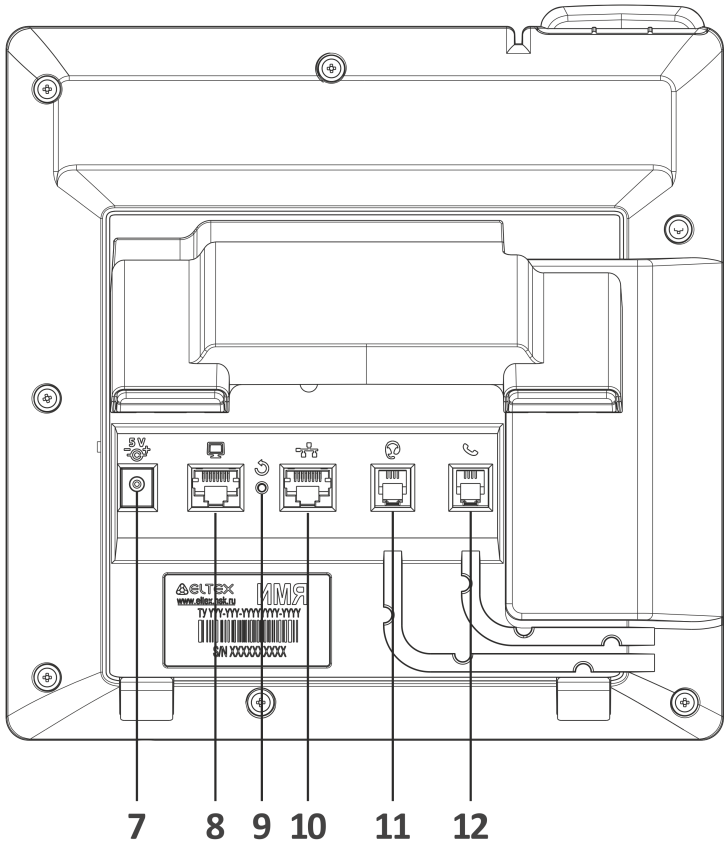
VP-17P top panel layout

VP-17P top panel is equipped with LED indicators:

Top panel element		Description	Description	Device state
1		Programmable keys indicators	Depends on configuration	
2		System indicator	Depends on configuration	
3		New message indicator	Flashes green	There are unread messages
			Off	There are no unread messages
4		Headset mode indicator	Solid green	Headset mode is activated
			Off	Headset mode is not activated
5		Mute mode indicator	Solid green	Mute mode is activated for the current conversation
			Off	Mute mode is not activated
6		Speakerphone mode indicator	Solid green	Speakerphone mode is activated
			Off	Speakerphone mode is not activated

1.4.2 Rear panel of the device

The figure below shows VP-17P rear panel layout.

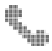


VP-17P rear panel layout

Rear panel layout		**Description**
7	DC	Port for power adapter connection, 5 V, 2 A
8	PC	10/100/1000BASE-T Ethernet port (RJ-45 port) for connection to PC
9	Reset	Device reboot button
10	LAN	10/100/1000BASE-T Ethernet port (RJ-45 port) for connection to LAN
11	Headset	RJ-9 port for connecting a headset
12	Handset	RJ-9 port for connecting a handset

1.5 Status indication on display

Status indication on graphic display

No.	Description
1	Indicator of voice interface:  — handset is off-hooked;  — handset is on-hooked;  — speakerphone is activated.
2	Current date and time.
3	Name of current accounts. If the account does not have name, the phone number is displayed (default account is marked with a filled upper left corner).
4	Actions taken upon pressing soft keys.

1.6 Screensaver

Starting from version 1.3.1, a screensaver has been added to the device display in standby mode. By default, the screensaver is enabled and activated after 3 hours if there is no user activity.

In order to configure the screensaver settings, use the phone's display menu and implement the following:
Menu → 3. Settings → 1. Phone → 3. Display → 2. Screensaver.
In this section, the user can disable the default screensaver and configure timeout for the screensaver activation.

The screensaver is an image of the current time and date that moves every 60 seconds around display perimeter.

1.7 Delivery package

VP-17P standard delivery package includes:

- IP-phone VP-17P;
- Double-position stand;
- Handset and cable for handset connection;
- 220/5 V, 2 A power adapter (optional);
- RJ-45 cable;
- Quick user manual and warranty certificate.

Headphones might be added to delivery package upon a request.

2 Managing via web interface

2.1 Getting started

2.1.1 Pre-starting procedures

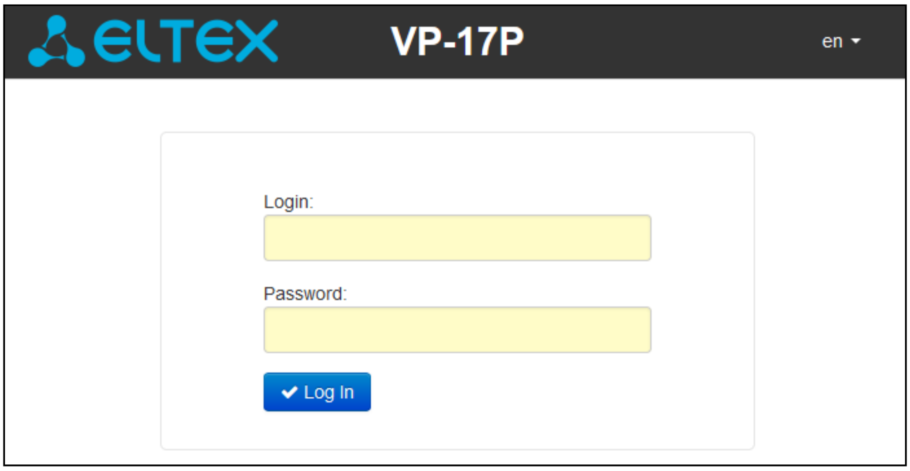
It is recommended to reset the device to factory settings when switching it on for the first time. Use display menu and buttons to reset the device and implement the following:
Menu → 3. Settings → 2. System → 5. Reset settings → Yes
The device will automatically reload.

To start the operation, you should connect the device to PC via LAN interface. Use a web browser:

1. Open web browser, i.e. Firefox, Opera, Chrome.
2. Enter the device IP address in the browser address bar.

By default, IP phone receives an IP address and other network parameters automatically via DHCP.
To get an obtained IP address, implement **Menu → 1. Status → 1. Network** using display menu.

When the device is successfully detected, username and password request page will be shown in the browser window:



By default, username is **admin**, password is **password.**

3. Enter your username into *'Login'* field and password into *'Password'* field.
4. Click *'Log in'* button. Monitoring panel will be shown in the browser.

Before you start, please, upgrade the firmare. See 'Firmware upgrade' submenu.
You can download the up-to-date firmware version on the Downloads page or contact ELTEX technical support. You can find contacts on TECHNICAL SUPPORT page.

2.1.2 Web interface description

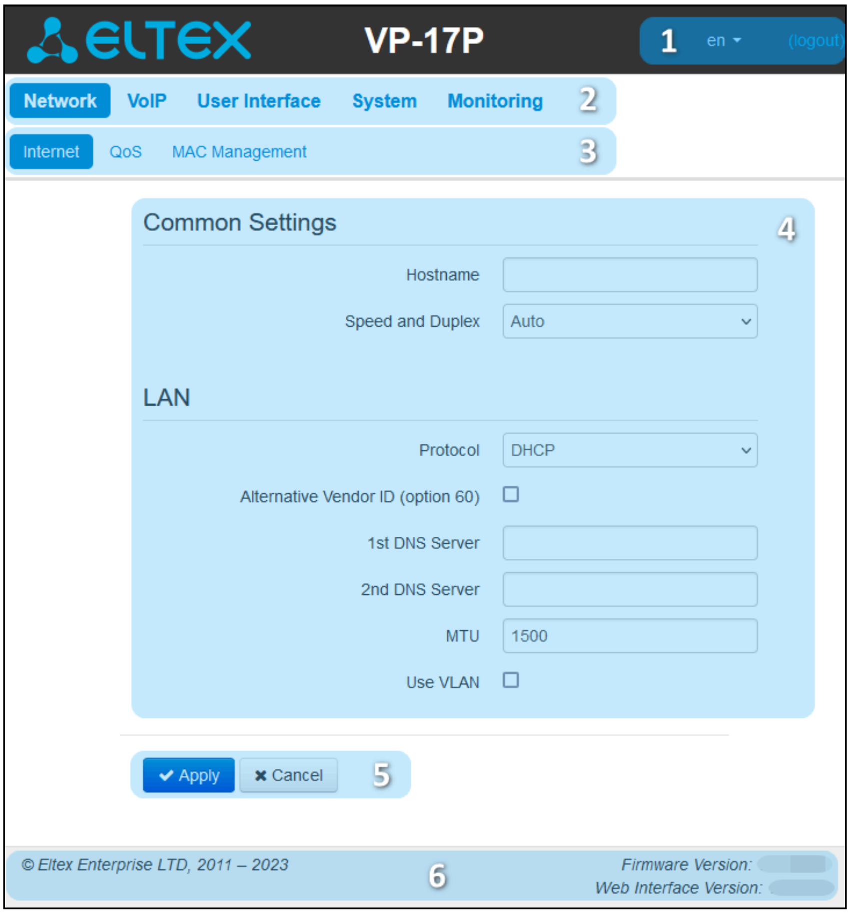
2.1.2.1 Web interface operation modes

Web interface of the VP devices can operate in two modes:

- **Configuration** is a system mode which enables full device configuration.
  The mode has four tabs:
  - Network;
  - VoIP;
  - User Interface;
  - System.
- **Monitoring** is a system monitoring mode which allows viewing various device operation information: Internet connection activity, phone port status, device information, etc.

2.1.2.2 Key elements of the web interface

User interface window is divided into 6 areas (see picture below).



Key elements of the web interface

1. User name for log in, session termination button in the web interface ('logout') for the current user and dropped down-menu for language changing.

2. Menu tabs allow you to select configuration and monitoring categories:

- **Network**;
- **VoIP**;
- **User Interface**;
- **System**;
- **Monitoring**.

3. Submenu tabs allow you to control settings field.

4. Device settings field based on the user selection; allows viewing device settings and entering configuration data.

5. Configuration management buttons. For detailed description see 'Applying configuration' submenu.

   - *Apply* — apply and save the current configuration into flash memory of the the device;
   - *Cancel* — discard changes (effective only until '*Apply*' button is clicked).

6. Informational field showing firmware version and web interface version.

2.1.2.3 Applying configuration

'Apply' button appears as follows: 

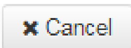
. Click it to save the configuration into the device flash memory and apply new settings. All settings will be accepted without device restart.

See the following table for detailed information on web interface visual indication of the current status of settings application process:

Visual indication of the current status of the setting application process

Appearance	**Status description**
	When you click the '*Apply*' button, settings will be applied and saved into the device memory. This is indicated by the  icon in the tab name and on the '*Apply*' button.
	Successful settings saving and application are indicated by  icon in the tab name.
	If the parameter value being specified contains an error, you will see a message with the reason description and  icon will appear in the tab name, when you click '*Apply*' button.

2.1.2.4 Discarding changes

Discard changes button appears as follows: 

. Click it to restore values currently stored in the device memory.

> Use '*Cancel*' button before clicking '*Apply*' button only. After you click '*Apply*', you will not be able to restore the previous settings.

2.2 Configuring

To move to configuration mode, select one of the following tab 'Network', 'VoIP' or 'System' depending on the configuration goals:

- In the 'Network' menu, the network settings of the device are configured;
- In the 'VoIP' menu, the following is configured: SIP settings, accounts settings, codecs installation, VAS and dialplan settings;
- In the 'User Interface' menu, function keys and sound volume for different device operation modes are configured;
- In the 'System' menu, system, time, access to the device via different protocols are configured, passwords can be changed, firmware can be updated.

Configuration mode elements:

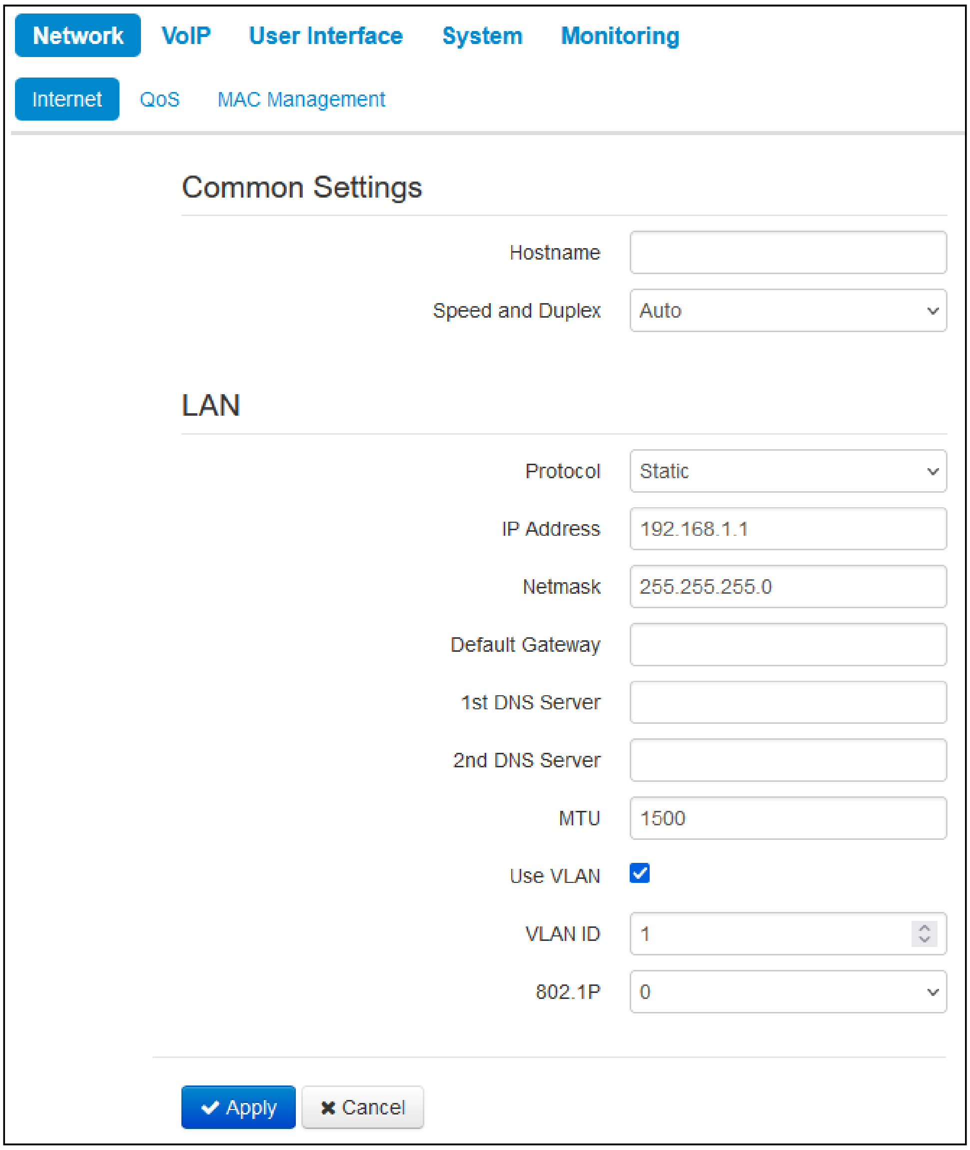
- 'Network' menu
  - 'Internet' submenu
  - 'QoS' submenu
  - 'MAC management' submenu
- 'VoIP' menu
  - 'SIP Accounts' submenu
  - 'Phone Book' submenu
  - 'Call History' submenu
- 'User Interface' menu
  - 'Common Settings' submenu
  - 'Buttons' submenu
  - 'System LED' submenu
  - 'Notifications' submenu
  - 'Ringtones' submenu
  - 'Audio' submenu
- 'System' menu
  - 'Time' submenu
  - 'Access' submenu
  - 'Log' submenu
  - 'Passwords' submenu
  - 'Configuration Management' submenu
  - 'Firmware Upgrade' submenu
  - 'Reboot' submenu
  - 'Autoprovisioning' submenu
  - 'Certificates' submenu
  - 'Advanced' submenu

2.2.1 'Network' menu

In the 'Network' menu, the network settings of the device are configured.

2.2.1.1 'Internet' submenu

In the 'Internet' submenu, you can configure LAN via DHCP, Static and No IP.



2.2.1.1.1 Common settings

- *Hostname* — device network name.
- *Speed and Duplex* — specify data rate and duplex mode for LAN Ethernet port of the device:
  - *Auto* — automatic speed and duplex negotiation;
  - *100 Half* — 100 Mbps data transfer rate with half-duplex mode is supported;
  - *100 Full* — 100 Mbps data transfer rate with duplex mode is supported;
  - *10 Half* — 10 Mbps data transfer rate with half-duplex mode is supported;
  - *10 Full* — 10 Mbps data transfer rate with duplex mode is supported.

2.2.1.1.2 LAN

- *Protocol* — select the protocol that will be used for device LAN interface connection to a data network:
  - *Static* — operation mode where IP address and all the necessary parameters for LAN interface are assigned statically;
  - *DHCP* — operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server;
  - *No IP* — operation mode when IP address is not assigned to the interface.

2.2.1.1.2.1 Static protocol

When 'Static' type is selected, the following parameters will be available for editing:

- *IP Address* — specify the device LAN interface IP address in the data network;
- *Netmask* — external subnet mask;
- *Default gateway* — address that the packet will be sent to, when route for it is not found in the routing table;
- *1st DNS Server, 2nd DNS Server* — domain name server addresses (allow identifying the IP address of the device by its domain name). You can leave these fields empty, if they are not required;
- *MTU* — maximum size of the data unit transmitted on the network.

2.2.1.1.2.2 DHCP protocol

When 'DHCP' type is selected, the following parameters will be available for editing:

- *Alternative Vendor ID (Option 60)* — when selected, the device transmits Vendor ID (Option 60) field value in Option 60 DHCP messages (Vendor class ID). When not selected, a default value is transmitted in Option 60 in the following format:
  - **[VENDOR:** device vendor**][DEVICE:** device type**][HW:** hardware version**][SN:** serial number**][WAN:** WAN interface MAC address**][LAN:** LAN interface MAC address**][VERSION:** firmware version**]**
    Example: [VENDOR:Eltex][DEVICE:VP-17P][HW:2.0][SN:VI23000118] [WAN:A8:F9:4B:03:2A:D0] [LAN:02:20:80:a8:f9:4b][VERSION:#1.3.1].
- *Vendor ID (Option 60)* — option 60 value (Vendor class ID) which is transmitted in DHCP messages. When the field is empty, option 60 is not transmitted in DHCP messages;
- *1st DNS Server, 2nd DNS Server* — domain name server addresses (allow identifying the IP address of the device by its domain name). Addresses, which are specified statically, have the higher priority than addresses obtained via DHCP;
- *MTU* — maximum size of the data unit transmitted on the network.

You can manually assign the list of used DHCP options on each network interface.

2.2.1.1.2.3 No IP protocol

When this mode is selected, IP address will not be assigned to the network interface. This mode is used when IP telephony operates in an allocated VLAN.

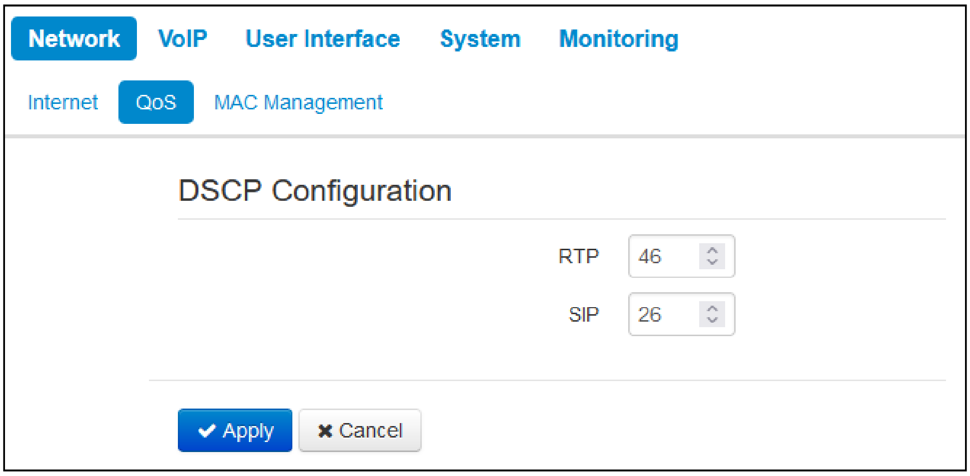
2.2.1.1.3 Use VLAN

VLAN (virtual local area network) is a group of hosts united in a network not depending on the physical location. The devices grouped to a VLAN have the same VLAN identifier (ID).

- *Use VLAN* — when selected, VLAN identifier specified below is used to enter the network:
  - *VLAN ID* — VLAN identifier which is used for the network interface;
  - *802.1P* — 802.1P attribute (also called CoS — Class of Service) attached to egress IP packets from the interface. The value is from 0 (the least priority) to 7 (the highest priority).

2.2.1.2 'QoS' submenu

In the 'QoS' submenu, Quality of Service functions configuring is available.



2.2.1.2.1 DSCP Configuration

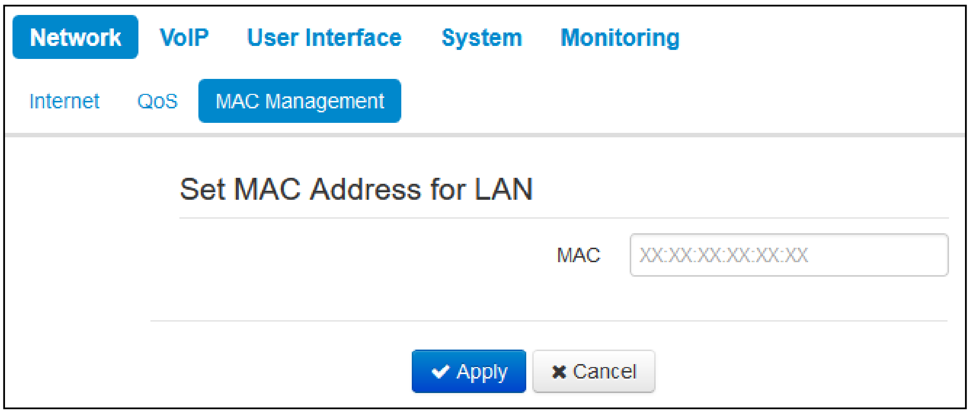
- *RTP* — value of the DSCP field of the IP packet header for voice traffic;
- *SIP* — value of the DSCP field of the IP packet header for SIP signaling traffic.

The setting are common for the first and second accounts.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.1.3 'MAC management' submenu

In the 'MAC management' submenu you can change MAC address of the device LAN interface.



- *MAC* — MAC address that will be assigned to the device network interface.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button

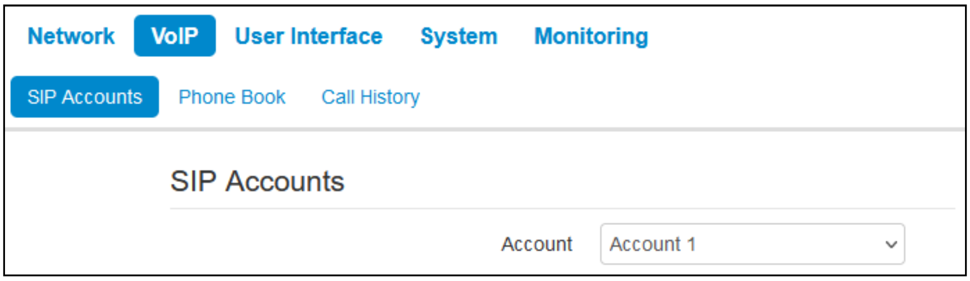
2.2.2 'VoIP' menu

In the 'VoIP' menu you can configure VoIP (Voice over IP):

- Account configuration;
- Codec installation;
- VAS and dialplan configuration.

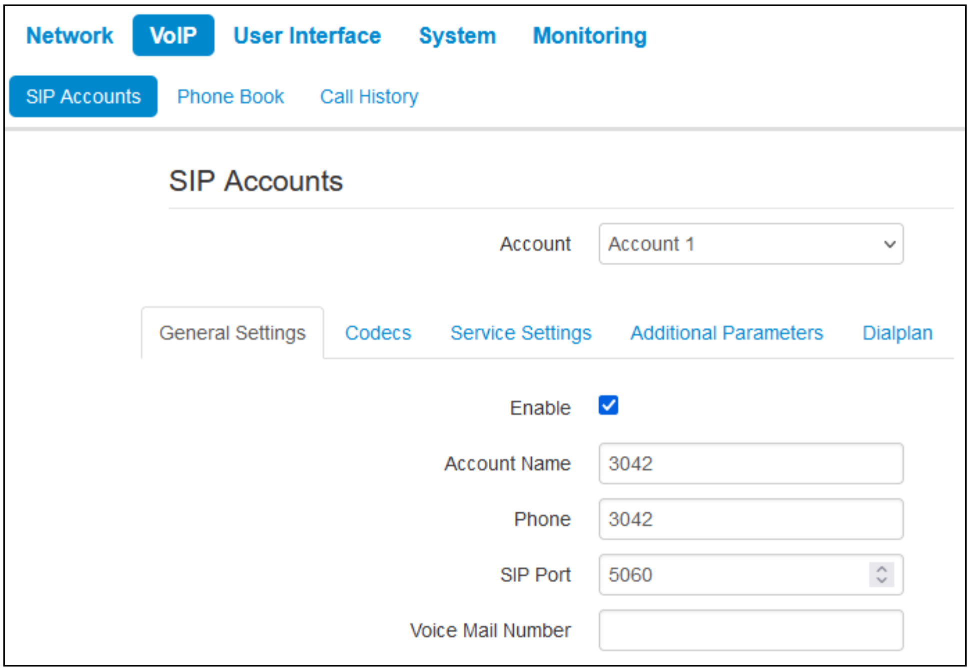
2.2.2.1 'SIP Accounts' submenu

Use drop-down 'Account' menu to select account for editing.



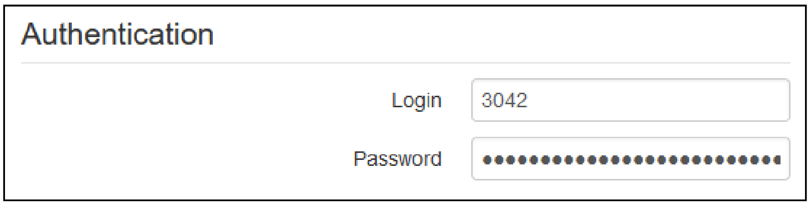
You can assign own SIP server addresses, registration servers, voice codecs, individualized dialing plan and other parameters for each account.

2.2.2.1.1 General settings



- *Enable* — when selected, account is active;
- *Account Name* — an account tag, which will be used for identifying active account or account by default;
- *Phone* — subscriber number assigned to the account;
- *SIP Port* — UDP port for incoming SIP message reception for this account, and for outgoing SIP message transmission from this account. It can take values from 1 to 65535 (default value: 5060);
- *Voice Mail Number* — a number which a call will be established to when subscriber selects 'Call' (to listen voice mail messages) in voice mail menu.

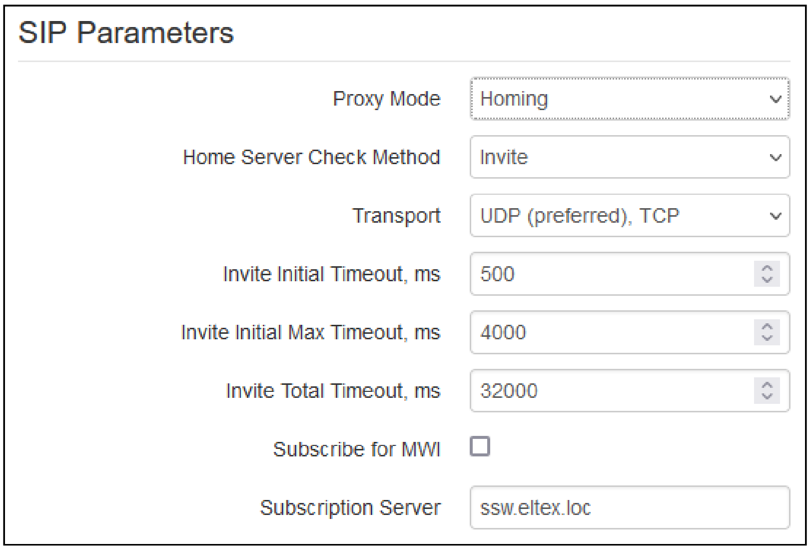
2.2.2.1.1.1 Authentication



- *Login* — user name used for subscriber authentication on SIP server and on registration server;
- *Password* — password used for subscriber authentication on SIP server and on registration server.

2.2.2.1.1.2 SIP parameters

Use '*SIP Parameters*' section to configure SIP parameters of the account.



- *Proxy Mode* — you can select SIP server operation mode in the drop-down list:
  - *Off;*
  - *Parking* — SIP-proxy redundancy mode without main SIP-proxy management;
  - *Homing* — SIP-proxy redundancy mode with main SIP-proxy management.

  The phone can operate with a single main SIP-proxy and up to three redundant SIP-proxies. For exclusive operations with the main SIP-proxy, *'Parking'* and *'Homing'* modes are identical. In this case, if the main SIP-proxy fails, it will take time to restore its operational status.

  For operations with redundant SIP-proxies, '*Parking*' and '*Homing*' modes will work as follows:

  > The gateway sends INVITE message to the main SIP-proxy address when performing outgoing call, and REGISTER message when performing registration attempt. If on expiration of '*Invite Total Timeout*' there is no response from the main SIP-proxy or response 408 or 503 is received, the phone sends INVITE (or REGISTER) message to the first redundant SIP-proxy address. If it is not available, the request is forwarded to the next redundant SIP-proxy and so forth. When available redundant SIP-proxy is found, registration will be renewed on that SIP-proxy.

  Next, the following actions will be available depending on the selected redundancy mode:

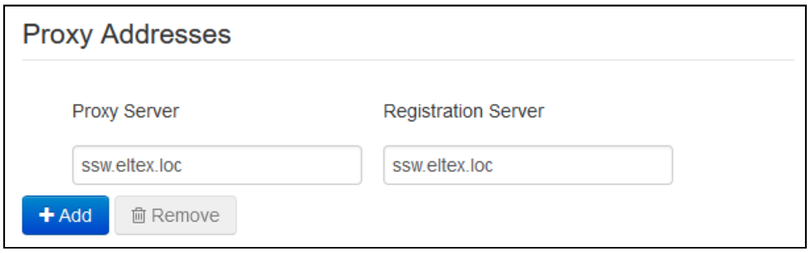
  > In the '*Parking*' mode, the main SIP-proxy management is absent, and the phone will continue operation with the redundant SIP-proxy even when the main proxy operation is restored. If the connection to the current SIP-proxy is lost, querying of the subsequent SIP-proxies will be continued using the algorithm described above. If the last redundant SIP-proxy is not available, the querying will continue in a cycle, beginning from the main SIP-proxy.

In the '*Homing*' mode, three types of the main SIP-proxy management are available: periodic transmission of OPTIONS messages to its address, periodic transmission of REGISTER messages to its address, or transmission of INVITE request when performing outgoing call. First of all, INVITE request is sent to the main SIP-proxy, and if it is unavailable, then the next redundant one, etc. Regardless of the management type, when the main SIP-proxy operation is restored, the gateway will use it to renew its registration. The gateway will begin operation with the main SIP-proxy.

- *Home Server Check Method* — select availability control method for the primary SIP server in *'Homing'* mode:
  - *Invite* — control via transmission of INVITE request to its address when performing an outgoing call;
  - *Register* — control via periodic transmission of REGISTER messages to its address;
  - *Options* — control via periodic transmission of OPTIONS messages to its address.
- *Home Server Keepalive Timeout* — periodic message transmission interval in seconds; used for home SIP server availability check.
- *Transport* — select protocol for SIP messages transport;
- *Invite Initial Timeout, ms* — a time interval between first INVITE transmission and the second one in case there is no answer on the first INVITE (ms). For the following INVITE requests (third, forth, etc.) the interval will be increased twice (i.e. if the value is 300 ms, the second INVITE will be sent in 300 ms, the third — in 600 ms, the forth — in 1200 ms, etc.);
- *Invite Initial Max Timeout, ms* — the maximum time interval for retransmitting non-INVITE requests and responses on INVITE requests;
- *Invite Total Timeout, ms* — common timeout of INVITE requests transmissition (ms). When the timeout is expired, it is defined that the route is not available. INVITE requests retranslation is limited for availability definition as well;
- *Subscribe for MWI* — when selected, the subscription request on 'message-summary' events is sent. After obtaining such request, subscription server will notify the device on new voice messages through sending NOTIFY requsts;
- *Subscriprion Server* — a network address, to which SUBSCRIBE requests are sent for subscription on 'message-summary' and 'dialog' events. It is possible to specify IP address as well as domain name (after colon, specify a UDP port of SIP server, default value is 5060).

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.2.1.1.3 Proxy Addresses



To add the main SIP proxy and registration server, enter the following settings:

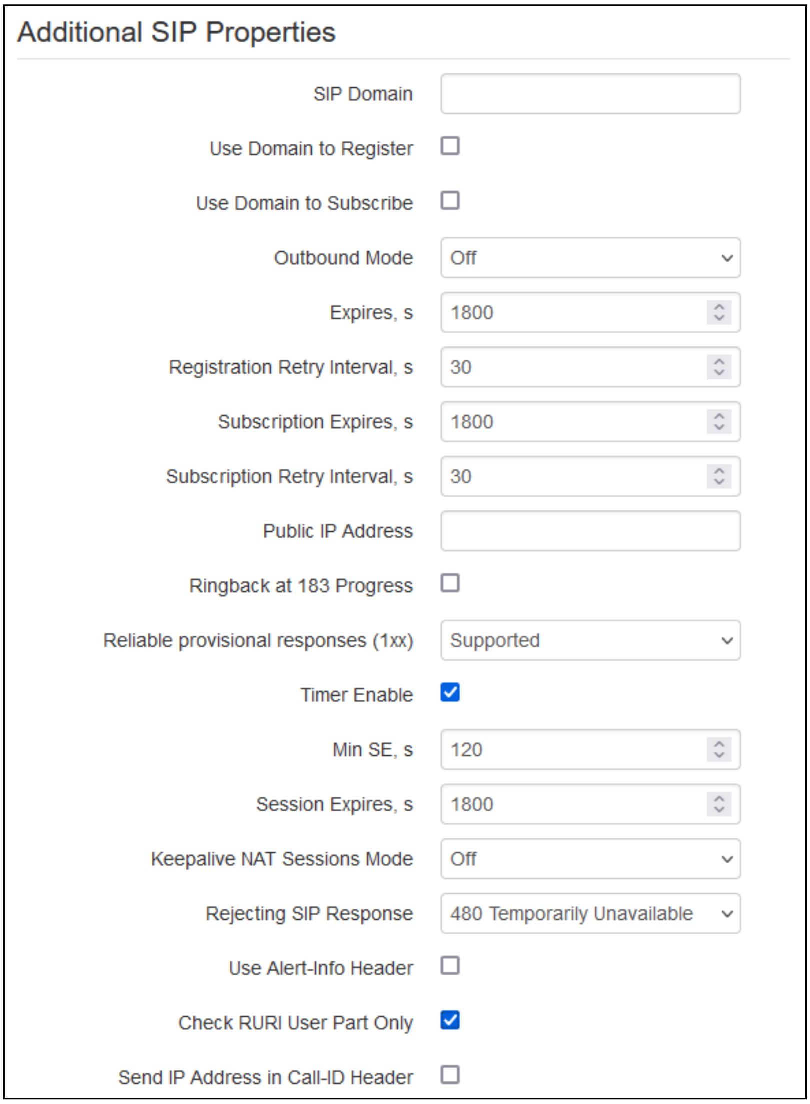
- *Proxy Server* — network address of the main SIP server. You can specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060);
- *Registration Server* — network address of the main registration server (specify UDP port after the colon, default value is 5060). You can specify IP address as well as the domain name.

To add redundant SIP proxy and registration server, click '*Add*' button and enter the following settings:

- *Proxy Server* — network address of redundant SIP server. You can specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060);
- *Registration Server* — network address of redundant registration server (specify UDP port after the colon, default value is 5060). You can specify IP address as well as the domain name. If the '*Proxy Server*' checkbox is selected, the redundant server registration is enabled.

To delete the redundant SIP proxy and registration server, select the checkbox next to the specified address and click '*Remove*' button.

2.2.2.1.1.4 Additional SIP Properties



- *SIP Domain* — domain where the device is located (fill in, if needed);
- *Use Domain to Register* — when selected, apply SIP domain for registration (SIP domain will be inserted into the 'Request-Line' of REGISTER requests);
- *Use Domain to Subscribe* — when selected, apply SIP domain for subscription (SIP domain will be inserted into the 'Request-Line' of SUBSCRIBE requests);
- *Outbound Mode*:
  - *Off* — calls will be routed according to the dialplan;
  - *Outbound* — dialplan is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, PBX response will be sent to the subscriber in order to enable subscriber service management (VAS management);
  - *Outbound with Busy* — dialplan is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, VoIP will be unavailable — error tone will be transmitted to the phone headset.
- *Expires, s* — valid time of account registration on SIP server. At the average, account registration renewal will be performed after 2/3 of the specified period;
- *Registration Retry Interval, s* — time interval between unsucceful attempt of SIP server registration and the next try;
- *Subscription Expires, s* — valid time of subscription on events. The subscription renewal is usually performed in 2/3 of the specified period;

- *Subscription Retry Interval, s* — time interval between unsucceful attempt of subscription on events and the next try;
- *Public IP Address* — this parameter is used as an external address of the device when it operates behind the NAT (gateway). As a public address, you can specify an external interface address (WAN) of a gateway (NAT) that the IP Phone operates through. At that, on the gateway (NAT), you should forward the corresponding SIP and RTP ports used by the device;
- *Ringback at 183 Progress* — when selected, 'ringback' tone will be sent upon receiving '183 Progress' message (w/o enclosed SDP);
- *Reliable provisional responses (1xx) (100rel)* — use reliable provisional responses (RFC3262):
    - *Supported* — reliable provisional responses are supported;
    - *Required* — reliable provisional responses are required;
    - *Off* — reliable provisional responses are disabled.

SIP protocol defines two types of responses for connection initiating requests (INVITE) — provisional and final. 2xx, 3xx, 4xx, 5xx and 6xx-class responses are final and their transfer is reliable, with ACK message confirmation. 1xx-class responses, except for *100 Trying* response, are provisional and transferred unreliable, without confirmation (RFC3261). These responses contain information on the current INVITE request processing step, therefore loss of these responses is unacceptable. Utilization of reliable provisional responses is also stated in SIP (RFC3262) protocol and defined by *100rel* tag presence in the initiating request. In this case, provisional responses are confirmed with PRACK message.

100rel setting operation for outgoing communications:

- *Supported* — send the following tag in INVITE request — *supported: 100rel*. In this case, communicating gateway can transfer provisional responses reliably or unreliably — as it deems fit;
- *Required* — send the following tags in INVITE request — *supported: 100rel* and *required: 100rel*. In this case, communicating gateway should perform reliable transfer of provisional replies. If communicating gateway does not support reliable provisional responses, it should reject the request with message 420 and provide the following tag — *unsupported: 100rel*. In this case, the second INVITE request will be sent without the following tag — *required: 100rel*;
- *Off* — do not send any of the following tags in INVITE request — *supported: 100rel* and *required: 100rel*. In this case, communicating gateway will perform unreliable transfer of provisional replies.

100rel setting operation for incoming communications:

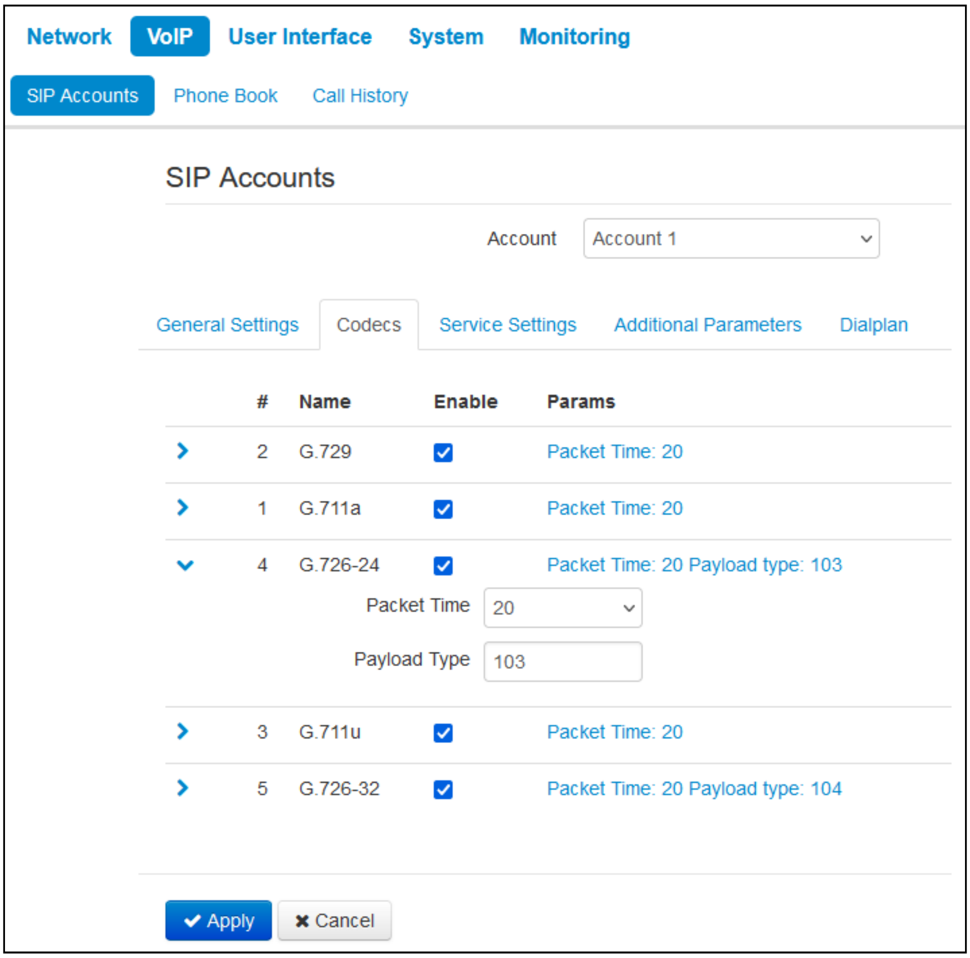
- *Supported, Required* — when the following tag is received in INVITE request — *supported: 100rel*, or *required: 100rel* — perform reliable transfer of provisional replies. If there is no *supported: 100rel* tag in INVITE request, the gateway will perform unreliable transfer of provisional replies;
- *Off* — when the following tag is received in INVITE request — *required: 100rel*, reject the request with message 420 and provide the following tag — *unsupported: 100rel*. Otherwise, perform unreliable transfer of provisional replies.

- *Timer Enable* — when selected, the 'timer' (RFC 4028) extension support is enabled. When connection is established, and both sides support 'timer' extension, one of them periodically sends re-INVITE requests for connection monitoring purposes (if both sides support UPDATE method, wherefore it should be specified in the 'Allow' header, the session update is performed by periodic transmission of UPDATE messages);
- *Min SE, s* — minimal time interval for connection health checks in seconds (90 to 1800 s, 120 s by default);
- *Session Expires, s* — period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 80000 s, recommended value — 1800 s, 0 — unlimited session);

- *Keepalive NAT Sessions Mode* — select SIP server polling method:
    - *Off* — SIP server will not be polled;
    - *Options* — SIP server polling with OPTIONS message;
    - *Notify* — SIP server polling with NOTIFY message;
    - *CLRF* — SIP server polling with an empty UDP packet.
- *Rejecting SIP Response* — select SIP response on incoming call rejection;
- *Use Alert-Info Header* — process INVITE request *'Alert-Info'* header to send a non-standard ringing to the subscriber port;
- *Check RURI User Part Only* — when selected, only subscriber number (user) will be analyzed, and if the number matches, the call will be assigned to the subscriber port. When cleared, all URI elements (user, host and port — subscriber number, IP address and UDP/TCP port) will be analyzed upon receiving an incoming call. If all URI elements match, the call will be assigned to the subscriber port;
- *Send IP Address in Call_ID Header* — when selected, during outgoing communications, device custom IP address will be used in 'Call-ID' header in 'localid@host' format.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

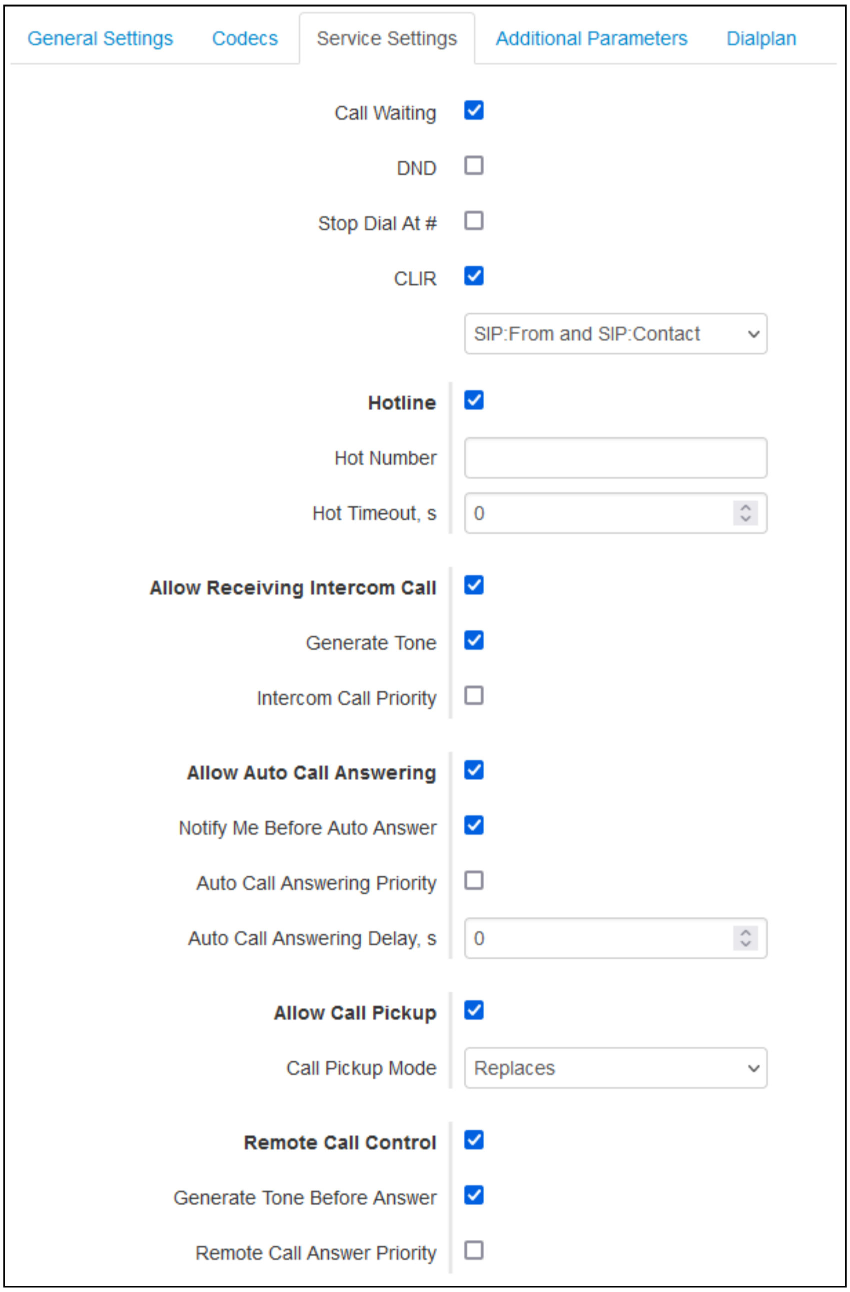
2.2.2.1.2 Codecs



- *Codec 1..5* — you can select codecs and an order of their usage. The highest priority codec should be dragged to the top of the list. For operation, you should select the checkbox '*Enable*' at least for one codec:
  - G.711a — use G.711A codec;
  - G.711u — use G.711U codec;
  - G.729 — use G.729 codec;
  - G.726-24 — use G.726 codec with the rate of 24 kbps;
  - G.726-32 — use G.726 with the rate of 32 kbps.
- *Params*:
  - *Packet Time* — amount of voice data in milliseconds (ms) transmitted in a single RTP packet for the corresponding codec G.711A, G.729, and G.726;
  - *Payload Type* — payload type of G.726-24 or G.726-32 codec (acceptable values are in the range from 96 to 127).

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

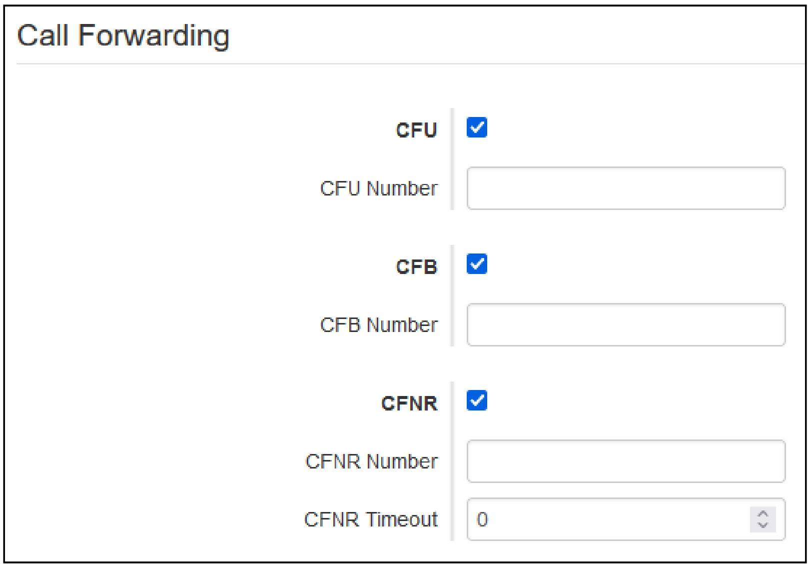
2.2.2.1.3 Service settings



- *Call Waiting* — when selected, the subscriber will accept incoming calls while being in a call state, otherwise '484 Busy here' reply will be sent;
- *DND* — when selected, temporary restriction is placed for incoming calls (DND service — Do Not Disturb);
- *Stop Dial At #* — when selected, use '#' button on the phone unit to end the dialing, otherwise '#' will be recognized as a part of the number;
- *CLIR* — when selected, limitation of caller number identification:
  - *SIP:From — Anonymous sip: anonymous@unknown.host* will be transmitted in the *'From'* header of SIP messages*;*
  - SIP:From and SIP:Contact — *Anonymous sip:anonymous@unknown.host* will be transmitted in the *'From'* and *'Contact'* headers of SIP messages.

- *Hotline* — when selected, 'Hotline' service is enabled. This service enables an outgoing connection automatically without dialing the number after the phone handset is picked up with the defined delay (in seconds). When selected, fill in the following fields:
    - *Hot Number* — phone number that will be used for connection establishment upon '*Hot timeout*' expiration after the phone handset is picked up (in SIP profile being used, a prefix for this direction should be defined in the dilaplan);
    - *Hot Timeout, s* — time interval that will be used for connection establishment with the opposite subscriber, in seconds.
- *Allow Receiving Intercom Call* — when cleared, incoming intercom calls are declined automatically:
    - *Generate Tone* — short sound signal is played before automatic answering to an incoming intercom call;
    - *Intercom Call Priority* — when selected, an incoming intercom call has higher priority than an active call. Before answering to incoming intercom call, an active call is put on hold. When the option is disabled, the function of automatic answering to intercom calls during active call is disabled;
- *Allow Auto Call Answering* — when selected, all incoming calls will be answered automatically:
    - *Notify Me Before Auto Answer* — short audio signal is played before automatic answering;
    - *Auto Call Answering Priority* — when selected, an incoming call has higher priority than an active call. Before answering to incoming call, an active call is put on hold. When the option is disabled, the function of automatic answering to incoming calls during active call is disabled;
    - *Auto Call Answering Delay, s* — time interval in seconds between the incoming call and the automatic answer to it.
- *Allow Call Pickup* — when selected, pressing the BLF key will initiate the interception of the incoming call to the subscriber on which the BLF key is configured;
    - *Call Pickup Mode* — the way the call is intercepted:
        - *Replaces* — call pickup using the Replaces header;
        - *Feature Code* — call pickup using the prefix added to the number of the subscriber on which the BLF key is configured:
            - *Call Pickup Code* — prefix which will be added to the number of the subscriber to which the BLF key is configured;
            - *Sign '#' terminates the number* — adding the '#' symbol when intercepting a call after the number of the subscriber to which the BLF key is configured.
- *Remote Call Control* — when selected, processing of '*Event*' headers in '*SIP Notify*' is allowed in accordance with the *Broadsoft: SIP Access Side Extensions Interface* specification. When receiving the '*event: talk*' header, the phone itself can answer the call, and when receiving the '*event: hold*' header, the phone itself will send a request to hold the call. This is important for the 'line shifting' function, since the phone itself will remove the call on hold;
    - *Generate Tone Before Answer* — short audio signal is played before remote control answering;
    - *Remote Call Answer Priority* — when selected, a new incoming call has higher priority than an active call. The active call will be put on hold before the call is automatically answered. When the option is disabled, automatic call answering will not work when there is an active call.

2.2.2.1.3.1 Forwarding

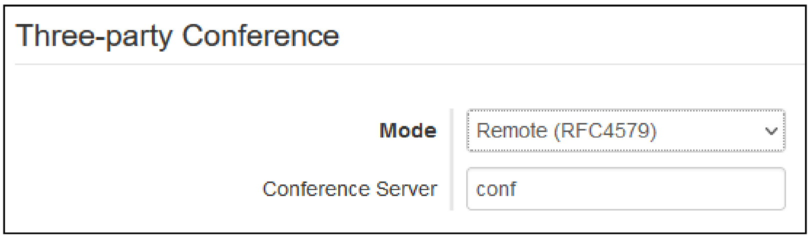


- *CFU* — when selected, CFU (Call Forwarding Unconditional) service is enabled — all incoming calls will be forwarded to the specified *CFU Number*:
  - *CFU Number* — number that all incoming calls will be forwarded to when CFU service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan).
- *CFB* — when selected, CFB (Call Forwarding Busy) service is enabled — call forwarding to the specified *CFNR Number*, when the subscriber is busy:
  - *CFB Number* — number that incoming calls will be forwarded to when the subscriber is busy and CFB service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan).
- *CFNR* — when selected, CFNR (Call Forwarding No Reply) service is enabled — call forwarding, when there is no answer from the subscriber:
  - *CFNR Number* — number that incoming calls will be forwarded to when there is no answer from the subscriber and CFNR service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan);
  - *CFNR Timeout* — time interval that will be used for call forwarding when there is no answer from the subscriber, in seconds.

When multiple services are enabled simultaneously, the priority will be as follows (in the descending order):

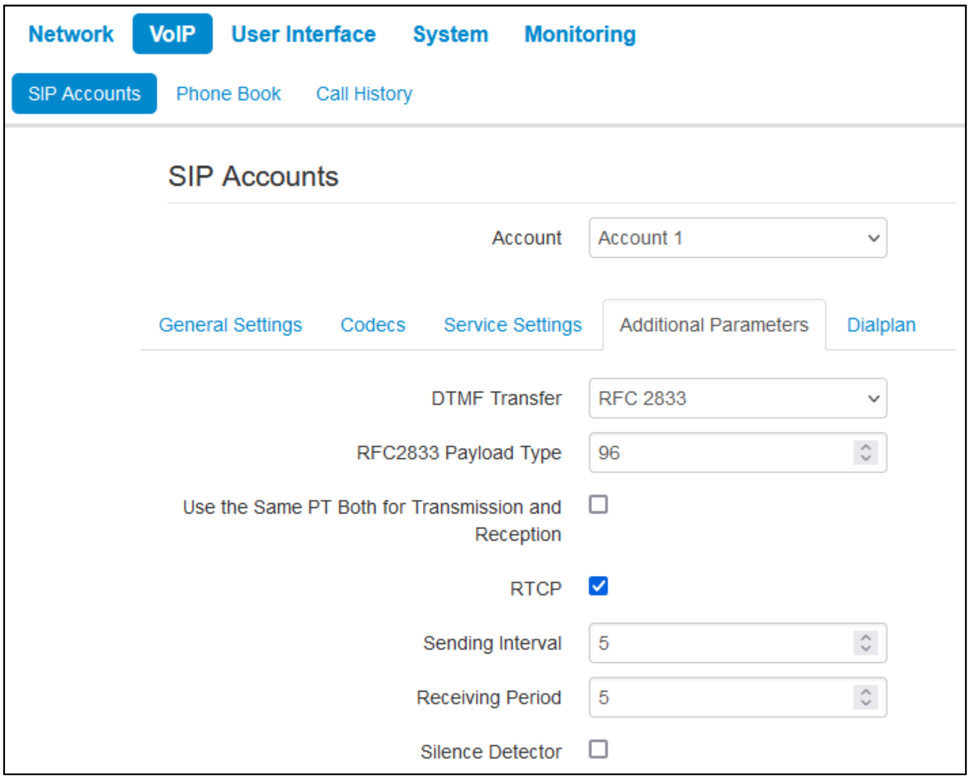
1. CFU;
2. DND;
3. CFB, CFNR.

2.2.2.1.3.2 Three-party conference



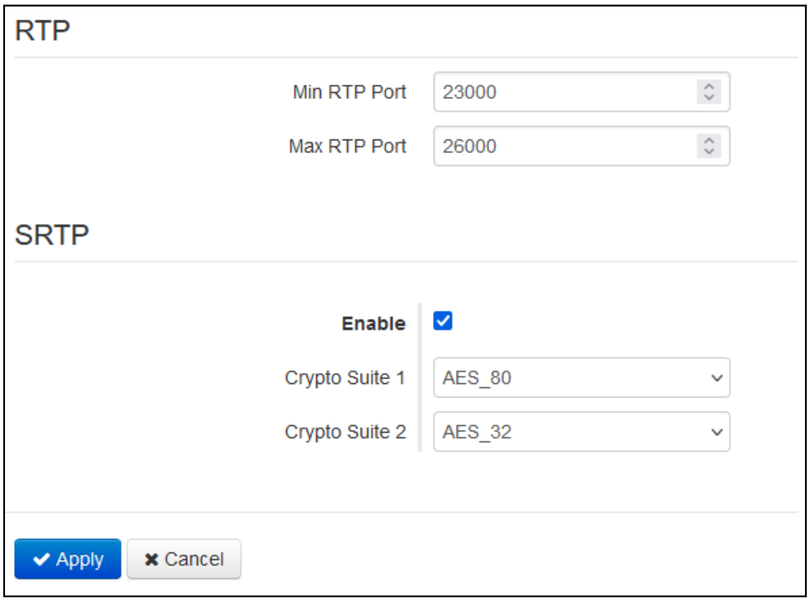
- *Mode* — operation mode of three-party conference. Two modes are possible:
  - *Local* — conference assembly is performed locally by the device after pressing 'CONF' button;
  - *Remote (RFC 4579)* — conference assembly is performed at the remote server; after pressing 'CONF' button, 'Invite' message will be sent to the server using number specified in the 'Conference server' field. In this case, conference operation complies with the algorithm described in RFC 4579.
- *Conference Server* — in general, address of the server that establishes conference using algorithm described in RFC 4579. Address is specified in the following format SIP-URI: user@address:port. You can specify the 'user' URI part only — in this case, 'Invite' message will be sent to the SIP proxy address.

2.2.2.1.4 Additional Parameters



- *DTMF Transfer* — mode of DTMF signal transmission:
  - *Inband* — inband transmission;
  - *RFC2833* — according to RFC2833 recommendation as a dedicated payload in RTP voice packets:
    - *RFC2833 Payload Type* — payload type for packet transmission via RFC2833 (possible values: from 96 to 127);
    - *Use the Same PT Both for Transmission and Reception* — option is used in outgoing calls for payload type negotiation of events sent via RFC2833 (DTMF signals). When selected, event transmission and reception via RFC2833 is performed using the payload from 200Ok message sent by the opposite side. When cleared, event transmission is performed via RFC2833 using the payload from 200Ok being received, and reception — using the payload type from its own configuration (specified in the outgoing *Invite*).
  - *SIP info* — transfer messages via SIP in INFO requests.
- *RTCP* — when selected, use RTCP for voice link monitoring:
  - *Sending Interval* — RTCP packet transmission period, in seconds;
  - *Receiving Period* — RTCP message reception period measured in transmission period units; if there is no single RTCP packet received until the reception period expires, the IP Phone will terminate the connection.
- *Silence Detector* — when selected, enable voice activity detector.

2.2.2.1.4.1 RTP



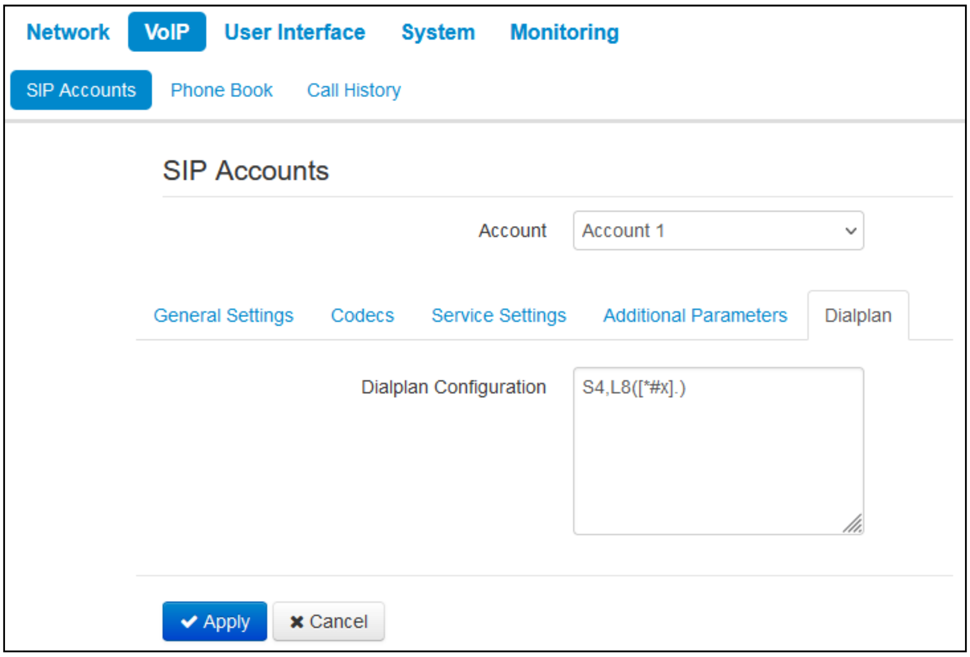
- *Min RTP Port* — lower limit of the RTP ports range used for voice traffic transmission;
- *Max RTP Port* — upper limit of the RTP ports range used for voice traffic transmission.

2.2.2.1.4.2 SRTP

- *Enable* — when selected, RTP flow encryption is used. Thus, the RTP/SAVP profile will be specified in SDP of outgoing INVITE requests. Also, the SDP of incoming requests will be scanned for the RTP/SAVP profile. If the RTP/SAVP profile is not found, the call will be rejected;
  - *Crypto Suite 1-2* — allows to choose encryption and hashing algorithms to be used. A suite with the highest priority should be specified in '*Crypto Suite 1*' field. You have to specify at least one crypto suit:
    - *AES_80* — according to AES_CM_128_HMAC_SHA1_80;
    - *AES_32* — according to AES_CM_128_HMAC_SHA1_32;
    - *Off* – RTP encryption will not be used.

To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

2.2.2.1.5 Dialplan



To define a dialplan, use regular expressions in the '*Dialplan configuration*' field. The structure and format of regular expressions that enable different dialing features are listed below.

Structure of regular expressions:

S xx , L xx (Rule1 | Rule2 | ... | RuleN)

where:

- **xx** — arbitrary values of S and L timers;
- **()** — dialplan margins;
- **|** — delimiter for dialplan rules;
- **Rule1, Rule 2, Rule N** — numbers templates which are allowed or forbidden to be called.

Routing rules structure:

Sxx Lxx prefix@optional(parameters)

where:

- **xx** — arbitrary value of S and L timer. Timers inside rules could be dropped; in this case, global timer values, defined before the parentheses, will be used.
- **prefix** — prefix part of the rule;
- **@optional** — optional part of the rule (might be skipped);
- **(parameters)** — additional options (might be skipped).

2.2.2.1.5.1 Timers

- *Interdigit Long Timer ('L' character in a dialplan record)* — entry timeout for the next digit, if there are no templates that correspond to the dialed combination.
- *Interdigit Short Timer ('S' character in a dialplan record)* — entry timeout for the next digit, if the dialed combination fully matches at least one template and if there is at least one template that requires an extension dialing for the full match.

The timers values might be assigned either for the whole dialplan or for a certain rule. The timers values specified before round brackets are applied for the whole dialplan.

<u>Example:</u> S4 (8XXX.) or S4, L8 (XXX)

If the values of timers are specified in a rule, they are applied to this rule. The value might be located at any position in a template.

<u>Example:</u> (S4 8XXX. | XXX) or ([1-5] XX S0) — an entry requests instant call transmission when 3-digit number dialing; a number should begin with 1,2, … ,5.

2.2.2.1.5.2 Prefix part of the rule

Prefix part might consist of the following elements:

Prefix part elements	**Description**
X or x	Any digit from 0 to 9, equivalent to [0-9] range.
0 - 9	Digits from 0 to 9.
*	Symbol *.
#	Symbol #. The use of # in a dialplan can cause blocking of dial completion with the help of # key!
[ ]	Specify a range (using dash), enumeration (without spaces, comas and other symbols between digits) or combination of range and enumeration. <u>Example of a range:</u> ([1-5]) — any digit from 1 to 5. <u>Example of enumeration :</u> ([1239]) — any digit out of 1, 2, 3 or 9. <u>Example of a range and enumeration combination</u>: ([1-39]) — the same as in the previous example but in another form. The entry corresponds to any digit from 1 to 3 and 9.

Prefix part elements	Description
{a,b}	Specify the number of reiteration of the symbol placed before round brackets, range or *# symbols. The following entries are possible: • {,max} — equal to {0,max}, • {min,} — equal to {min,∞}. Where: • min — minimum number of reiteration, • max — maximum. Example 1: 6{2,5} — 6 might be dialed from 2 to 5 times. The entry equals to the followings: 66 | 666 | 6666 | 66666 Example 2: 8{2,} — 8 might be dialed 2 and more times. The entry equals to the followings: 88 | 888 | 8888 | 88888 | 888888 | ... Example 3: 2{,4} — 2 might be dialed up to 4 times. The entry equals to the followings: 2 | 22 | 222 | 2222.
.	Special symbol 'dot' defines the possibility of reiteration of the previous digit, range or *# symbols from 0 ad infinitum times. It is equal to {0,} entry. Example: 5x.* — x in this rule can either be absent or present as many times as needed. It is equal to 5* | 5x* | 5xx* | 5xxx* | ...
+	Special symbol 'plus' — repeat the previous digit, range or *# symbols from 1 ad infinitum times. It is equal to {1,} entry. Example: 7x+ — x is supposed to present in the rule at least 1 time. It is equal to 7x | 7xx | 7xxx | 7xxxx | ...
<arg1:arg2>	Replace dialed sequence. The dialed sequence (arg1) in SIP request to SIP server is changed to another one (arg2). The modification allows deleting — <xx:>, adding — <:xx>, or replacing — <xx:xx> of digits and symbols. Example 1: (<9:8383>XXXXXXX) — the entry corresponds the following dialed digits 9XXXXXXX, but in the transmitted request to SIP server, 9 digit will be replaced to 8383 sequence. Example 2: (<83812:>XXXXXX) — the entry corresponds the following dialed digits 83812XXXXXX, but the sequence 83812 will be omitted and will not be transmitted to a SIP server.
,	Paste tone to dialing. When ringing to intercity numbers (or to city number using an office phone) usually, you can hear a dial tone. The dial tone can be realized by putting coma at the needed position in a sequence. Example: (8, 770) — while dialing 8770 sequence you will hear a continuous dial tone ('station responce') after dialing 8 digit.

Prefix part elements	Description
!	Forbid number dialing. If you put '!' symbol at the end of the number template, dialing of numbers corresponding to the template will be blocked. Example: (8 10X xxxxxxx ! | 8 xxx xxxxxxx) — expression allows long-distance dialing only and denies outgoing international calls. Prohibition rules must be written first.

2.2.2.1.5.3 Optional part of rules

The optional part of a rule might be omitted. This part might consist the following elements:

Optional part of rules element	Description
@host:[port]	Direct address dialing (IP Dialing). '@' symbol placed after the number defines that the dialed call which will be sent to the subsequent server address. Also, IP Dialing address format can be used for numbers intended for the call forwarding. If *@host:port* is not specified, calls are routed via SIP-proxy. Example: (**1xxxx@192.168.16.13:5062**) — all five-digit dials, beginning with 1, will be routed to 192.168.16.13 IP address to 5062 port.

2.2.2.1.5.4 Additional parameters

Format: **(param1: value1, .., valueN; .. ;paramN: value1, .., valueN)**

- *param* — parameter name; several parameters are semicolon-separated and all parameters are enclosed in parentheses;
- *value* — parameter value; several values of one parameter are comma-separated.

Valid parameters and their values:

Parameter	Description
line	Account. Placing a call via the accont, possible values 0 and 1. The value 0 corresponds to the first account, the value 1 corresponds to the second account. Example: 12x(line:1) — call to 3-digit numbers beginning with 12 will be performed via the second account.

2.2.2.1.5.5 Examples

Example 1: (8 xxx xxxxxxx) — 11-digit number beginning with 8.

Example 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) — 11-digit number beginning with 8; if 7-digit number is dialed, add 8495 to the number being sent.

Example 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) — dialing of emergency call numbers and unusual sets of long-distance numbers.

Example 4: (S0 <:82125551234>) — quickly dial the specified number, similar to 'Hotline' mode.

Example 5: (S5 <:1000> | xxxx) — this dialplan allows you to dial any number that contains digits, and if there was no entry in 5 seconds, dial number '1000' (for example, it belongs to a secretary).

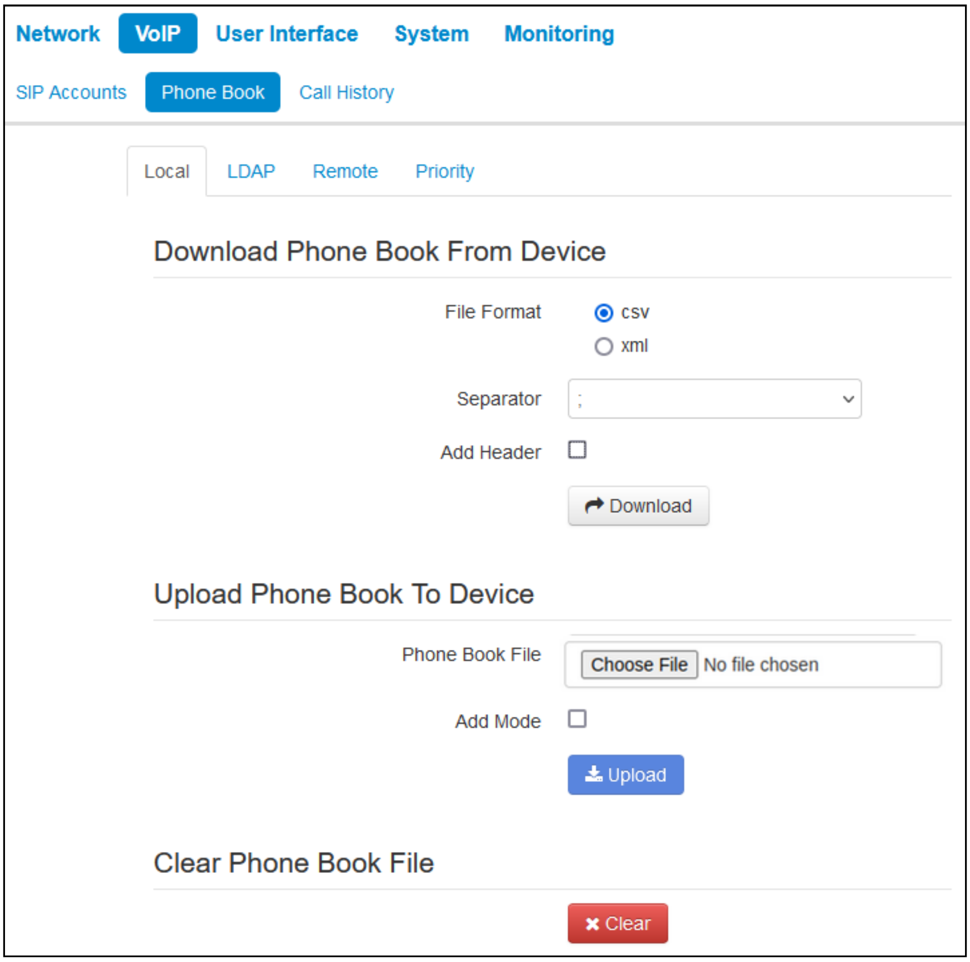
Example 6: (8, 10x.|1xx@10.110.60.51:5060) — this dialplan allows you to dial any number beginning with 810 and containing at least one digit after '810' (after entering '8', 'station reply' tone will be generated) as well as 3-digit numbers beginning with 1. Subscriber calls with 3-digit numbers beginning with 1 will be sent to IP address 10.110.60.51 and port 5060.

Example 7: (S3 *xx#|#xx#|#xx#|*xx*x+#) — managment and usage of VAS.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.2.2 'Phone Book' submenu

2.2.2.2.1 Local phone book management



2.2.2.2.1.1 Download Phone Book From Device

Use the section to download a phone book stored on the device.

- *File Format* — select a format of the file you want to download. The following formats are available:
  - *csv* — text file format where all the conacts are written in the table. The values in the table are separated by the selected separator;
    - *Separator* — the symbol for separating data in the table in csv format;
    - *Add Header* — when selected, downloaded csv file will have a header — the first line.
- *xml* — an eXtensible Markup Language.

2.2.2.2.1.2 Upload Phone Book To Device

This section is used to configure parameters of restoring a phone bool from the backup copy.

- *Phone Book File* — choose file;
- *Add Mode* — when selected, the conacts from the uploaded file will be added to existing ones.

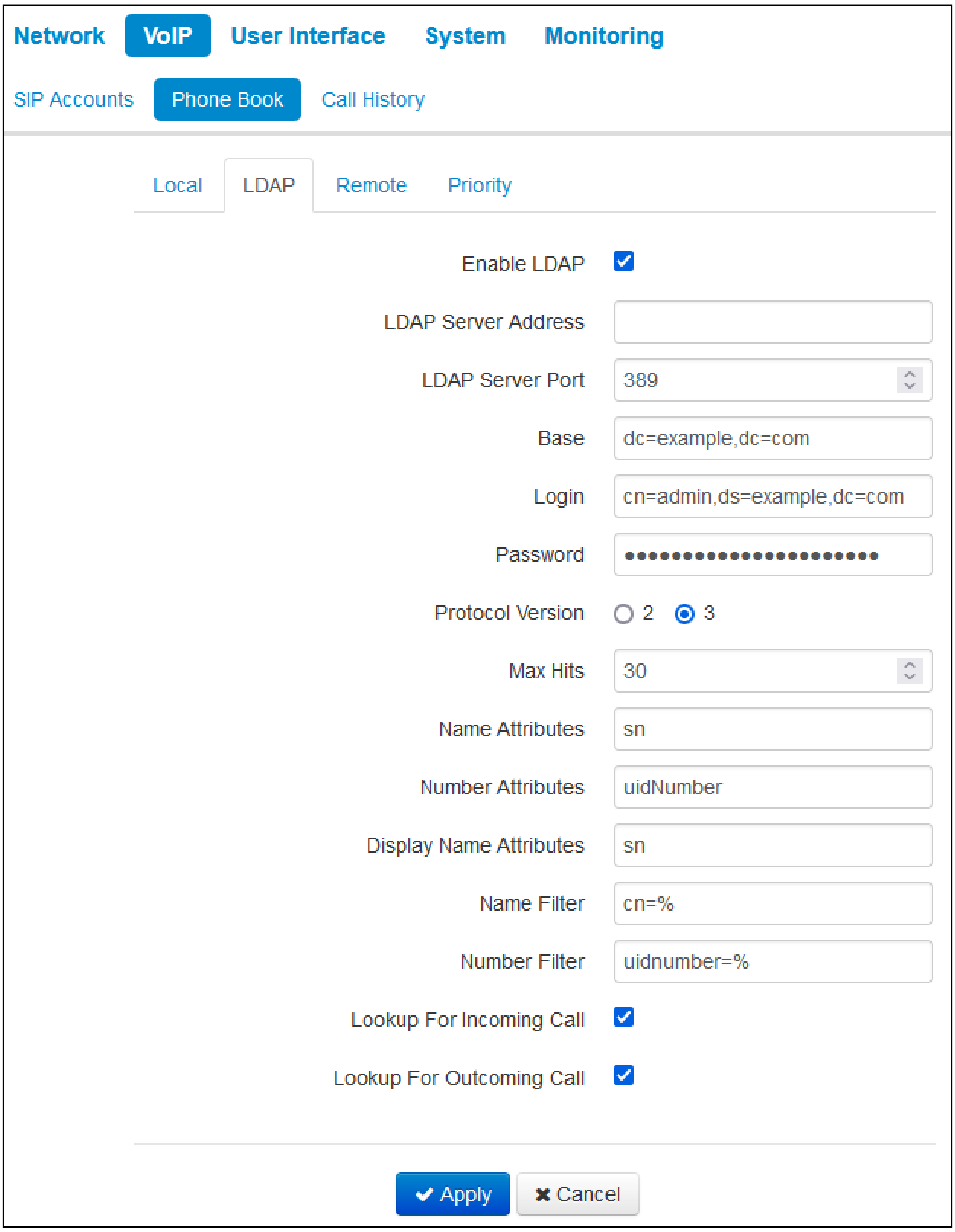
> If 'Add Mode' box is not selected, contacts from the loaded file will replace the existing one.

2.2.2.2.1.3 Clear Phone Book File

To clean the phone book, click '*Clear*' button.

2.2.2.2.2 LDAP Phone Book management

In the 'Phone book' submenu, you can set up the connection to LDAP server and search parameters.



- *Enable LDAP* — when selected, the phone book is accessible via display menu;
  - *LDAP Server Address* — domain name or IP address of LDAP server;
  - *LDAP Server Port* — port of LDAP server transport protocol;
  - *Base* — indicates the location of base directory, that contains the phone book, and from which the search begins, in the LDAP directory. Specifying this parameter narrows the search and thereby reduces the time it takes to search for a contact;
  - *Login* — username that will be used when authorizing on LDAP server;
  - *Password* — password that will be used when authorizing on LDAP server;
  - *Protocol Version* — LDAP protocol version of formed requests;

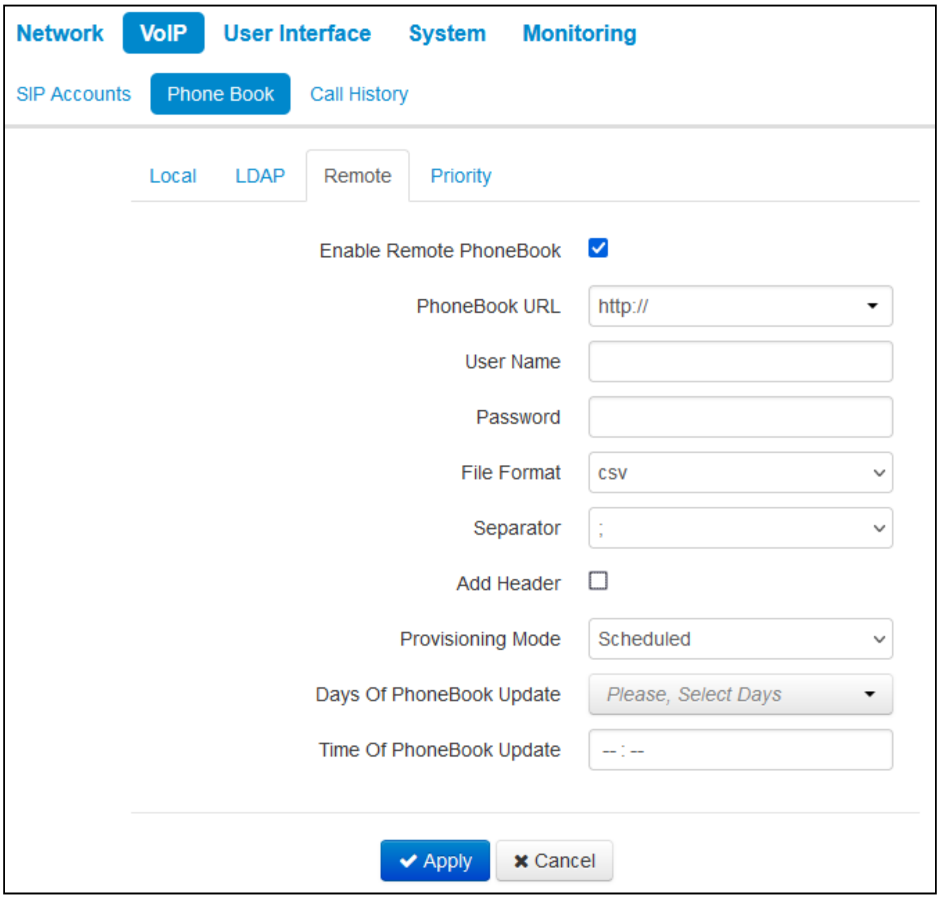
- *Max Hits* — the parameter indicating the maximum amount of search results that will be returned by LDAP server;

> Too big 'Max Hits' value reduces the LDAP search rate, that is why the parameter is to be configured according to the available bandwidth.

- *Name Attributes* — the parameter that indicates the name attribute of each record returned by the LDAP server;
- *Number Attributes* — the parameter that indicates the number attribute of each record returned by the LDAP server;
- *Display Name Attributes* — the parameter that indicates the display name attribute of each record returned by the LDAP server;
- *Name Filter* — the filter used to lookup for the names. The '*' character in the filter indicates any character. The '%' character in the filter indicates the input string used as the filter condition prefix;
- *Number Filter* — the filter used to lookup for the number. The '*' character in the filter indicates any character. The '%' character in the filter indicates the input string used as the filter condition prefix;
- *Lookup For Incoming Call* — when selected, lookup for a name using a number during incoming calls;
- *Lookup For Outcoming Call* — when selected, lookup for a name using a number during outcoming calls.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

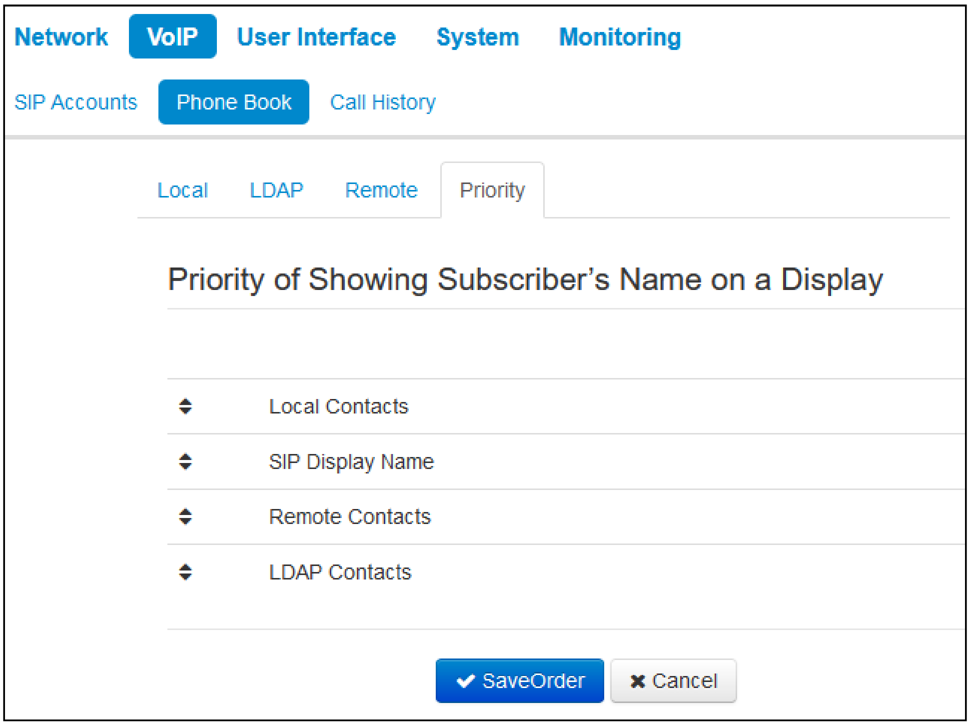
2.2.2.2.3 Remote Phone Book management



- *Enable Remote PhoneBook* — when selected, remote phonebook is loaded automatically;
  - *PhoneBook URL* — a full path to the remote phonebook — is set in URL format (the following protocols are available to be used for phonebook loading through: *TFTP, FTP, HTTP* and *HTTPS*);
  - *User Name* — a name which is used for authentication on FTP/HTTP/HTTPS server for phonebook loading;
  - *Password* — a password which is used for authentication on FTP/HTTP/HTTPS server for phonebook loading;
  - *File Format* — select a format of the file you want to download. The following formats are available:
    - *csv* — text file format where all the conacts are written in the table. The values in the table are separated by the selected separator;
      - *Separator* — the symbol for separating data in the table in csv format;
      - *Add Header* — when selected, downloaded csv file will have a header — the first line.
  - *xml* — an eXtensible Markup Language.
  - *Provisioning Mode* — select a mode for phonebook loading:
    - *Periodically* — the device phone book will be automatically updated after defined period of time;
      - *PhoneBook Update Interval, s* — time interval between phonebook updates. If the parameter is set to 0, the phonebook is updated once — right after device loading.
    - *Scheduled* — the device phone book will be automatically updated at specific time and on specific days:
      - *Days Of PhoneBook Update* — weekdays when the phonebook will be automatically updated;
      - *Time Of PhoneBook Update* — time in 24-hours format, when the phonebook will be automatically updated.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.2.2.4 Phone Book Priority management



In the 'Priority' submenu, you can configure the priority for displaying the subscriber's name on the display.

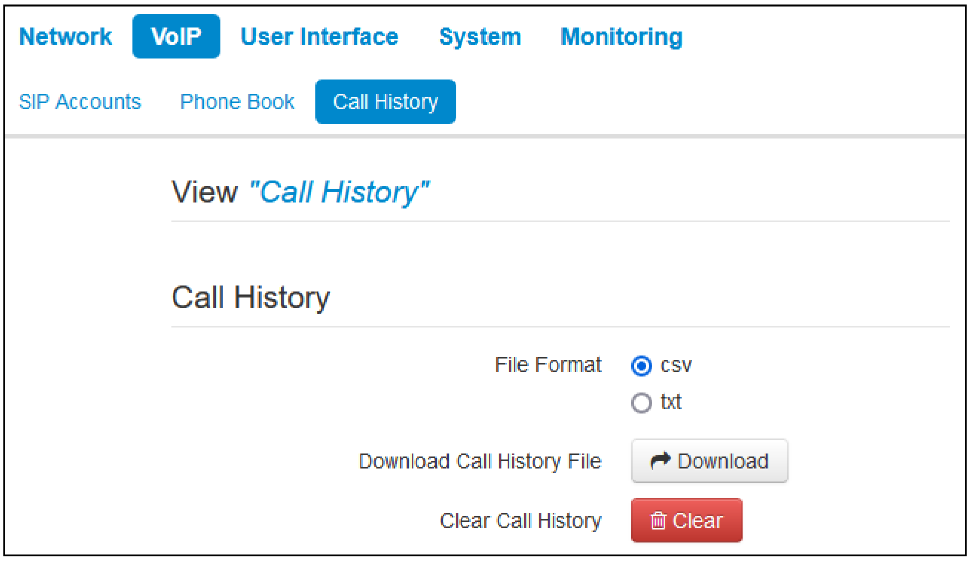
- *Local Contacts* — displaying of names from local pnonebook;
- *SIP Display Name* — displaying of names received via SIP protocol;
- *Remote Contacts* — displaying of names from remote pnonebook;
- *LDAP Contracts* — displaying of names from LDAP pnonebook.

The caller's name will be displayed according to the selected priority. For example, in this case, if the local phone book has the name of the caller, the display will show the name from the local phone book, if not — the name designated in the SIP protocol. If the name is not designated in the SIP protocol, it will be displayed from the remote phone book, etc.

To apply a new configuration and store settings into the non-volatile memory, click *'SaveOrder'* button. To discard changes, click *'Cancel'* button.

2.2.2.3 'Call History' submenu

In the 'Call History' submenu you can configure call history logging.



- *File Format* — select a format of the file you want to download. The following formats are available:
  - *csv* — text file format where call history is written in a table. The values in the table are separated by the selected separator;
  - *txt* — text file format that contains call history organized by lines.
- *Download Call History File* — to save 'voip_history' file on a local PC, click 'Download' button;
- *Clear Call History* — to clear call history, click *'Clear'* button.

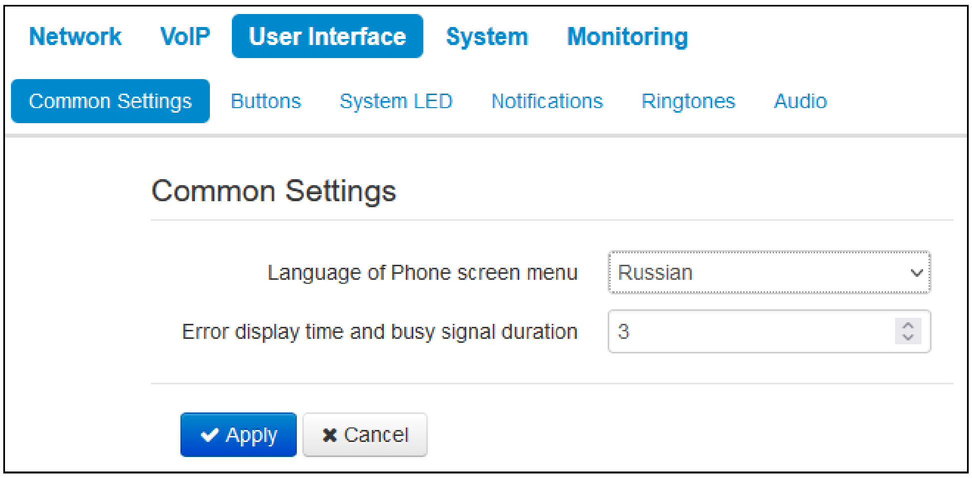
To view the call history, follow the *View 'Call History'* link. For parameter monitoring description, see section 'View call history'.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.3 'User Interface' menu

2.2.3.1 'Common Settings' submenu

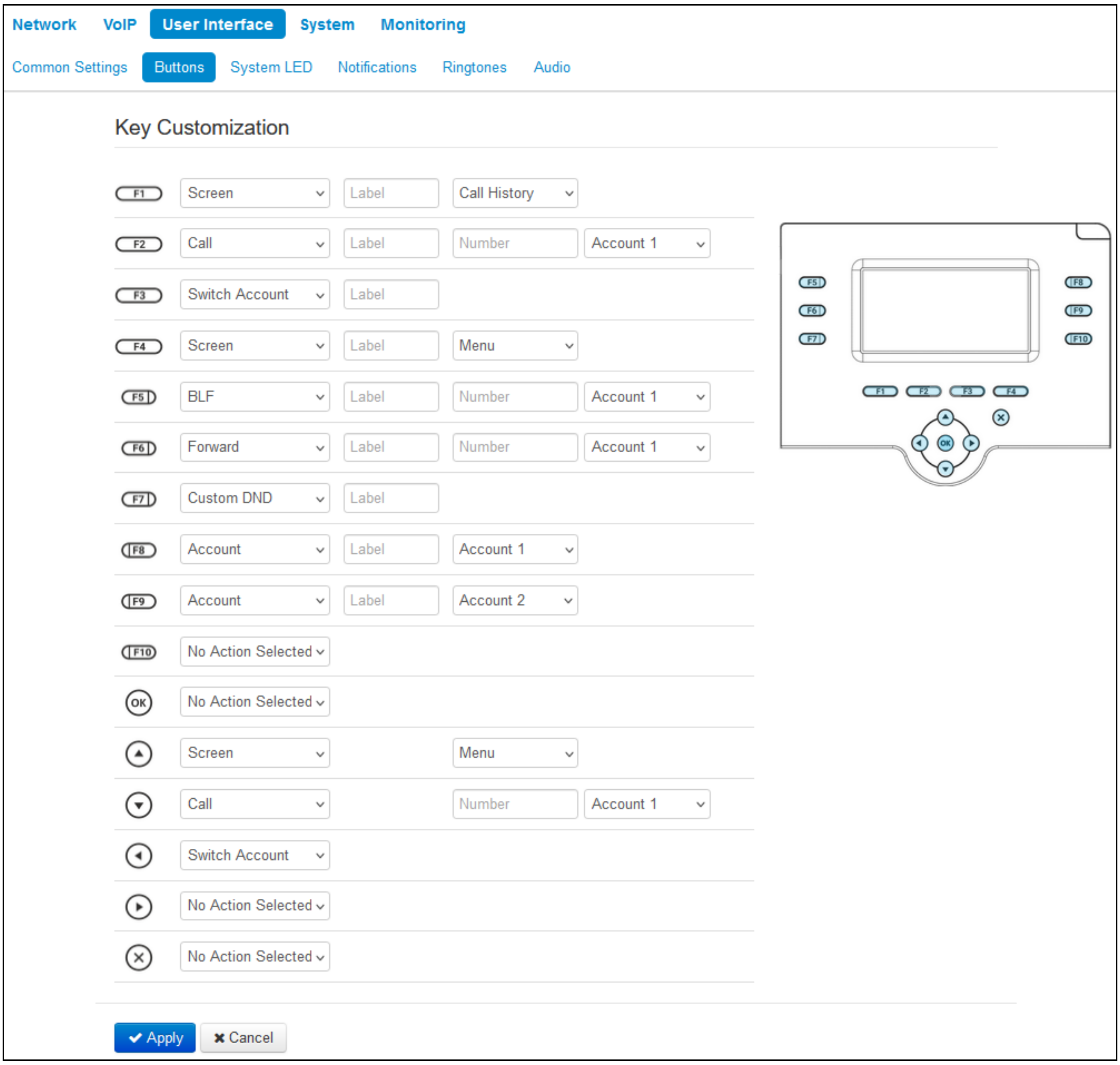
In the 'Common Settings' submenu you can change phone user settings.



- *Language of Phone screen menu* — select screen menu language: *Russian* or *English*;
- *Error display time and busy signal duration* — the option is used to define the time interval in seconds during which an error will be displayed and a busy signal will be played.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.3.2 'Buttons' submenu



You can choose actions for each button to be performed on pressing. The settings are presented as a table with the following columns:

1. *Button*;
2. *Action* — select action to be performed on the button pressing. The followings are available:
    a. *No Action Selected* — pressing this button will not be processed;
    b. *Screen* — open a screen selected in the additional parameters;
    c. *Call* — call the number selected in the additional parameters;
    d. *Switch Account* — change the account by default;

e. *BLF* — pressing the button in stand-by mode initiates a call. In conversation mode, pressing the button redirects the call to the selected subscriber.

> BLF — only for buttons with LED indicator. LED indicates line status of the subscriber selected in the additional settings.

> To activate BLF function, you should specify subscription server in SIP account settings.

f. *Account* — open the dialer for the specified account;
g. *Forward* — activate forwarding to a specified number;
h. *DND* — temporary ban on incoming calls for all accounts;
i. *Custom DND* — temporary ban on incoming calls for the specified account.

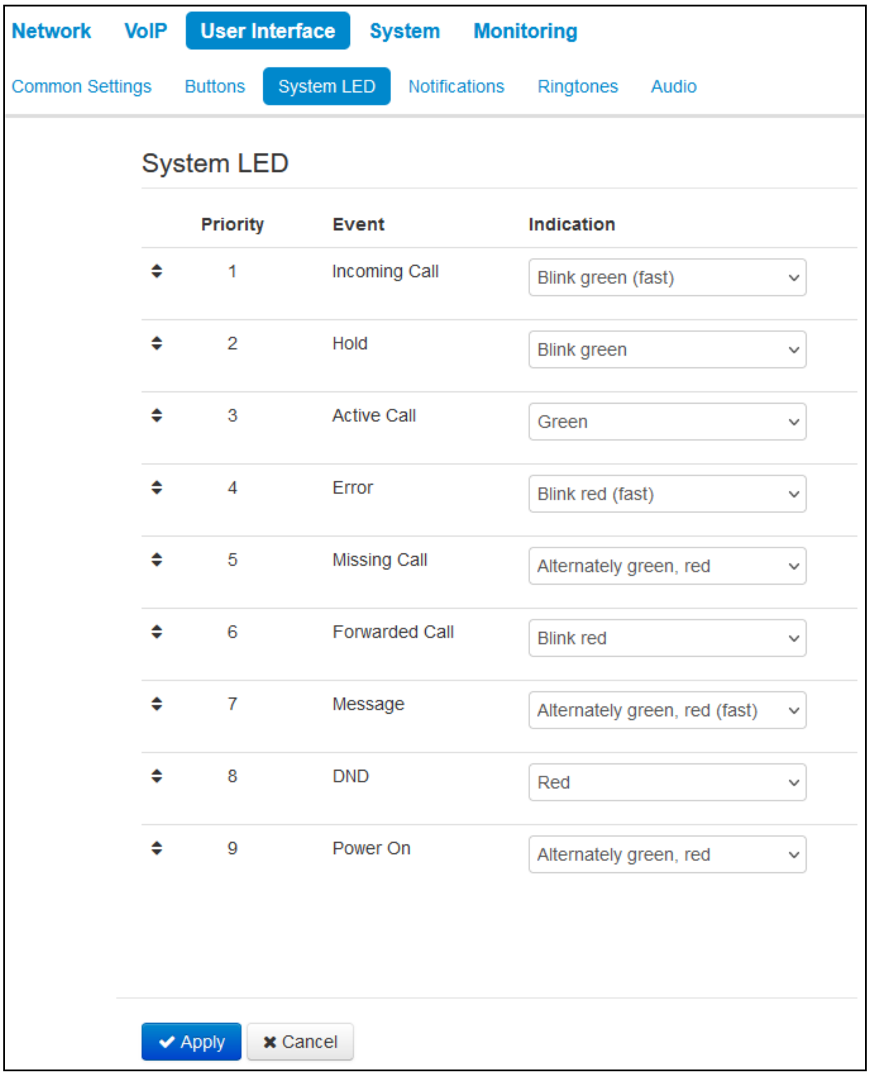
3. *Label* — button label, which is displayed on the screen next to the button;
4. *Additional parameters*— select additional parameters for the button (options depend on the action selected).

To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

2.2.3.3 'System LED' submenu

> ⚠ The system indicator is the LED located on the IP phone case in the upper right corner.

In the 'System LED' submenu you can configure the operation of the system indicator and the priority for possible events. The indicator first displays the signal of the event that is placed higher in the priority table than the others. In the screenshot below, the highest priority event is '*Incoming Call*', the lowest priority event is '*Power On*'.



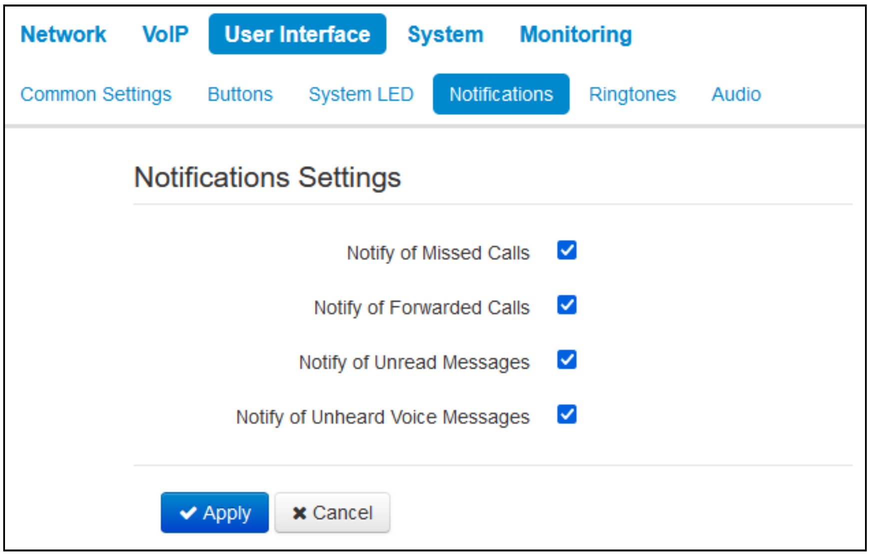
Possible indicator modes:

- *Disabled;*
- *Green;*
- *Red;*
- *Blink green;*
- *Blink red;*
- *Blink green (fast);*
- *Blink red (fast);*
- *Alternately green, red;*
- *Alternately green, red (fast).*

To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

2.2.3.4 'Notifications' submenu

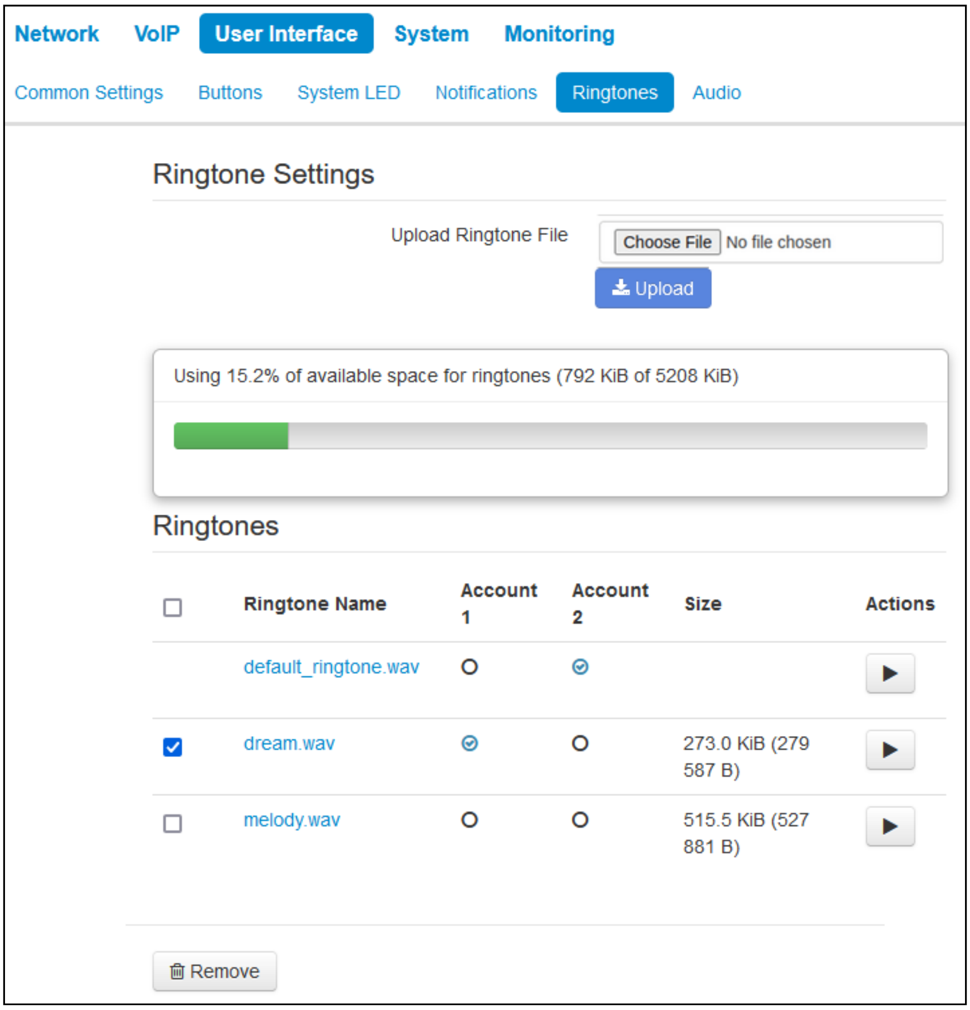
In the 'Notifications' submenu you can manage the notifications that are displayed on the device screen.



- *Notify of Missed Calls* — when selected, the display shows notifications of missed calls;
- *Notify of Forwarded Calls* — when selected, the display shows notifications of forwarded calls;
- *Notify of Unread Messages* — when selected, the display shows notifications of unread text messages;
- *Notify of Unheard Voice Messages* — when selected, the display shows notifications of unheard voice messages.

2.2.3.5 'Ringtones' submenu

In 'Ringtones' submenu, you can upload audio file and set it as ringtone. You can assign different ringtones for accounts.



This tab consists of 3 parts:

- a block for audio file uploading;
- drive free space indicator and total drive memory size for audio files storage;
- list of uploaded audio files.

Before being upload to the storage, audio files are compressed. The indicator shows the size of compressed files.

The list of uploaded audio files is shown in a table with the following columns:

- *Ringtone Name* — name of the audio file;
- *Account 1* — assignment of the ringtone to the Account 1;
- *Account 2* — assignment of the ringtone to the Account 2;
- *Size* — the size of the file before being compressing;
- *Actions* — a button to play/pause audio file on the device. When the key is pressed, the audio file will be played.

Check and uncheck audio files in the list to select the necessary files and click *'Remove'* button below the table to delete them from the storage.

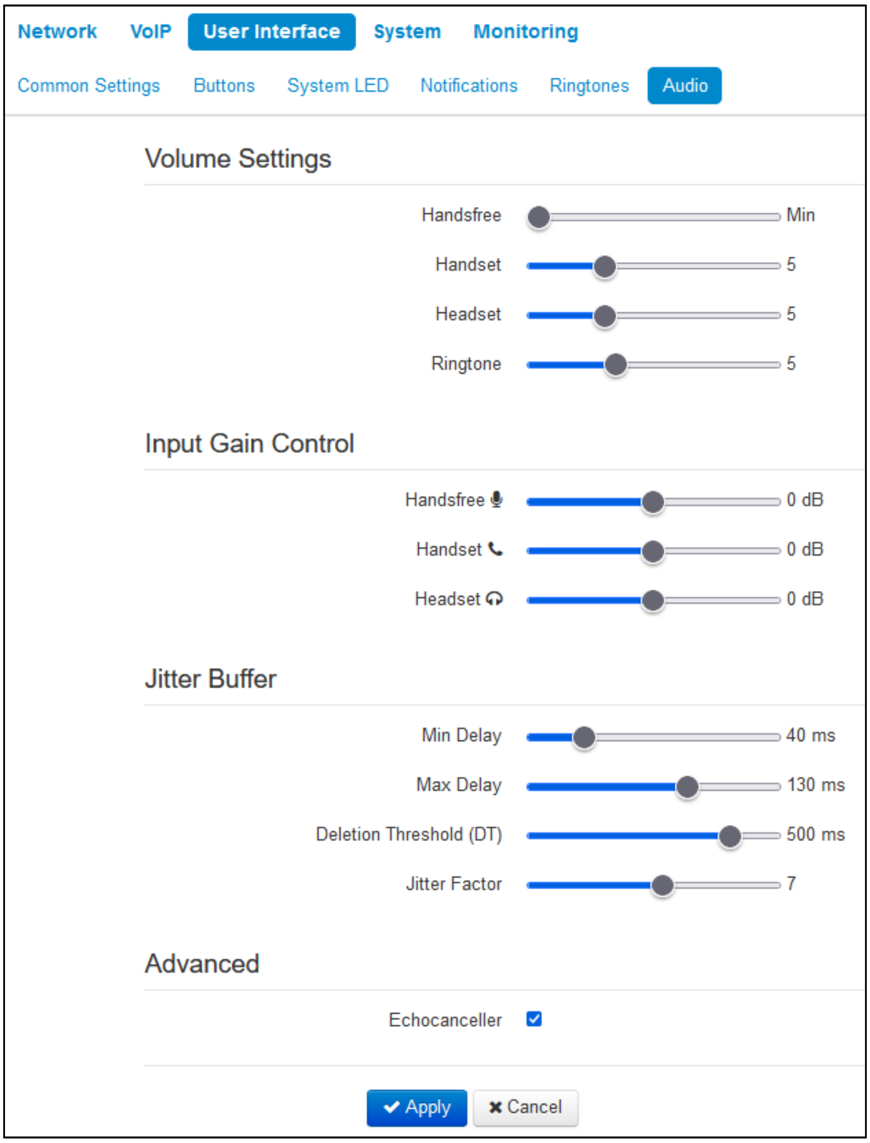
An audio file should meet the following requirements to be played correctly:

1. Sampling frequency — 8000 Hz;
2. Number of channels — 1 (Mono);
3. Code size — 8 bit;
4. Codec — A-Law.

The example of preparing an audio file is presented in the application 'Prepairing an audio file to be uploaded as a ringtone'.

2.2.3.6 'Audio' submenu

In the 'Audio' submenu you can configure the volume in various device operation modes.



Volume Settings

- *Handsfree* — speakerphone volume during conversation;
- *Handset* — handset volume during conversation;
- *Headset* — headset volume during conversation;
- *Ringtone* — ringtone volume.

Input Gain Control

- *Handsfree* — specifies the value by which a signal from the speakerphone will be amplified (valid values -9, … 9 dB, at a pitch of 1.5 dB);
- *Handset* — specifies the value by which a signal from the handset will be amplified (valid values -9, … 9 dB, at a pitch of 1.5 dB);
- *Headset* — specifies the value by which a signal from the headset will be amplified (valid values -9, … 9 dB, at a pitch of 1.5 dB).

Jitter Buffer

Jitter is a deviation of time periods dedicated to packet delivery. Packet delivery delay and jitter are measured in milliseconds. Jitter value is of great importance for real time data transfers (e.g. voice or video data).

In RTP, there is a field for precision transmission time tag related to the whole RTP stream. Receiving device uses these time tags to learn when to expect the packet and whether the packet order has been observed. On the basis of this information, the receiving side will learn how to configure its settings in order to evade potential network problems such as delays and jitter. If the expected time for packet delivery from the source to the destination for the whole call period corresponds to the defined value, e.g. 50ms, it is fair to say that there is no jitter in such a network. But packets are delayed in the network frequently, and the delivery time period can fluctuate significantly (in the context of time-critical traffic). If the audio or video recipient application will play packets in the order of their reception time, voice (or video) quality will deteriorate significantly. For example, if the voice data is being transferred, there will be interruptions and interference in the voice.

The device features the following jitter buffer settings:

- *Min Delay, ms* — minimum expected IP package network propagation delay;
- *Max Delay, ms* — maximum expected IP package network propagation delay;
- *Deletion Threshold (DT)* — maximum time for voice package removal from the buffer. The parameter value should be greater or equal to maximum delay;
- *Jitter Factor* — parameter used for jitter buffer size optimization. The recommended value is 0.

Advanced

- *Echocanceller* — when selected, use echocanceller.

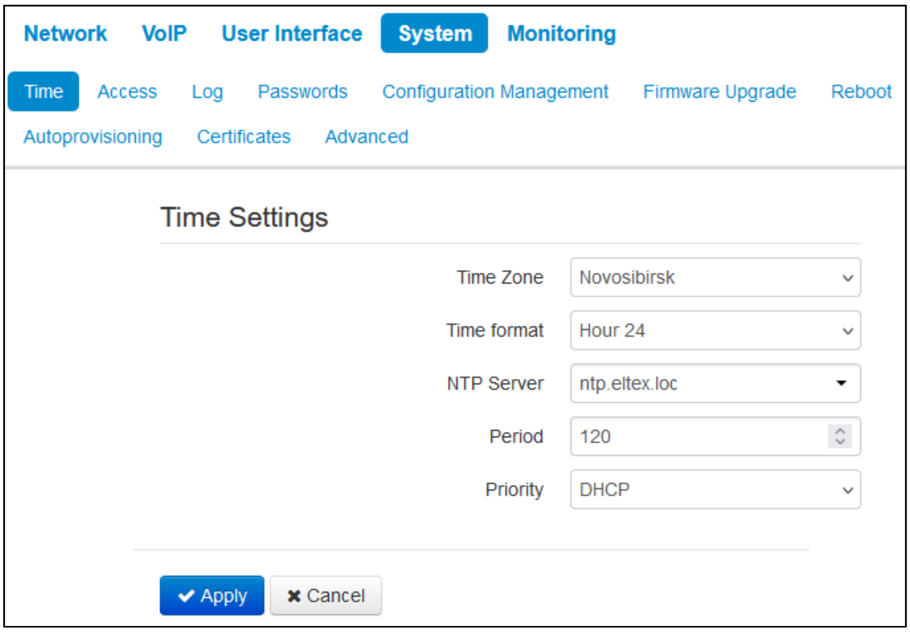
To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

2.2.4 'System' menu

In the 'System' menu you can configure settings for system, time and access to the device via various protocols, change the device password and update the device firmware.

2.2.4.1 'Time' submenu

In the 'Time' submenu you can configure time synchronization protocol (NTP).

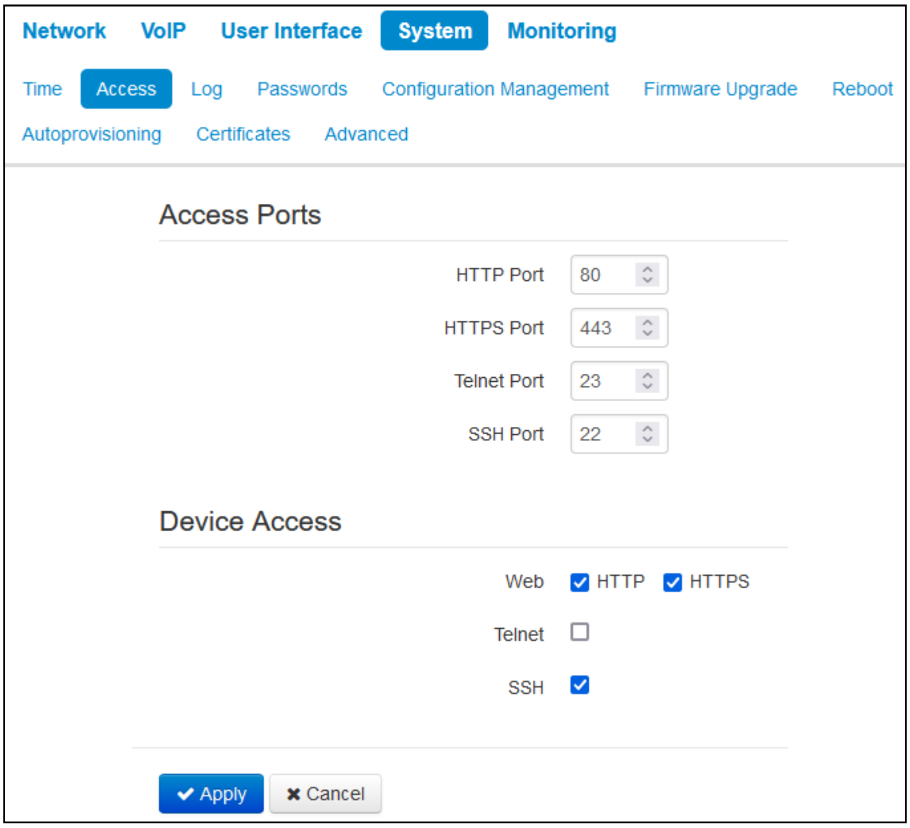


- *Time Zone* — select a timezone from the list according to the nearest city in your region;
- *Time format* — set time format: *Hour 24* or *Hour 12*;
- *NTP Server* — time synchronization server IP address/domain name. Manual entering of server address or selection from a list are available;
- *Period* — the device time will be automatically updated after the specified period of time;
- *Priority* — allows selection of priority of obtaining the NTP server address:
  - *DHCP* — when selected, the device uses the NTP server address from DHCP messages in option 42 (Network Time Protocol Servers). DHCP protocol must be set for the main interface;
  - *Config* — when selected, the device uses the NTP server address from '*NTP Server*' parameter.

To apply a new configuration and store settings into the non-volatile memory, click '*Apply*' button. To discard changes, click '*Cancel*' button.

2.2.4.2 'Access' submenu

In the 'Access' submenu you can configure the device access via web interface, Telnet and SSH protocols.



2.2.4.2.1 Access Ports

In this section you can configure TCP ports for the device access via HTTP, HTTPS, Telnet, and SSH.

- *HTTP port* — number of the port that allows for the device web interface access via HTTP, default value is 80;
- *HTTPS ports* — number of the port that allows for the device web interface access via HTTPS (HTTP secure connection), default value is 443;
- *Telnet port* — number of the port that allows for the device access via Telnet, default value is 23;
- *SSH port* — number of the port that allows for the device access via SSH, default value is 22.

You can use *Telnet* and *SSH* protocols in order to access the command line (Linux console). Username/ password for console connection: **admin/password**.

2.2.4.2.2 Device Access

To get device access from the Internet service interfaces, set the following permissions:

Web

- *HTTP* — when selected, connection to the device web configurator is enabled via HTTP (insecure connection);
- *HTTPS* — when selected, connection to the device web configurator is enabled via HTTPS (secure connection).

Telnet — a protocol that allows you to establish mechanisms of control over the network. Allows you to remotely connect to the gateway from a computer for configuration and management purposes. To enable the device access via Telmet protocol, select the appropriate checkboxes.

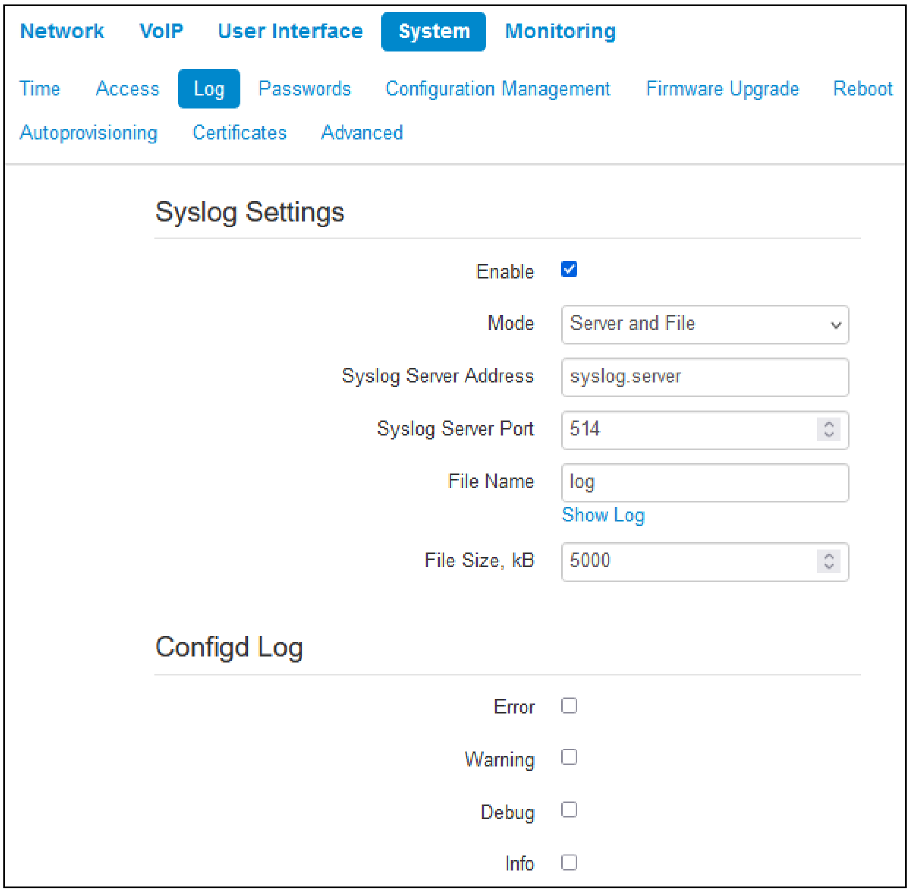
SSH — a secure device remote control protocol. However, as opposed to Telnet, SSH encrypts all traffic, including passwords being transferred. To enable the device access via SSH protocol, select the appropriate checkbox.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.4.3 'Log' submenu

In the 'Log' submenu you can configure output for various debug messages intended for device troubleshooting. Debug information is provided by the following device firmware modules:

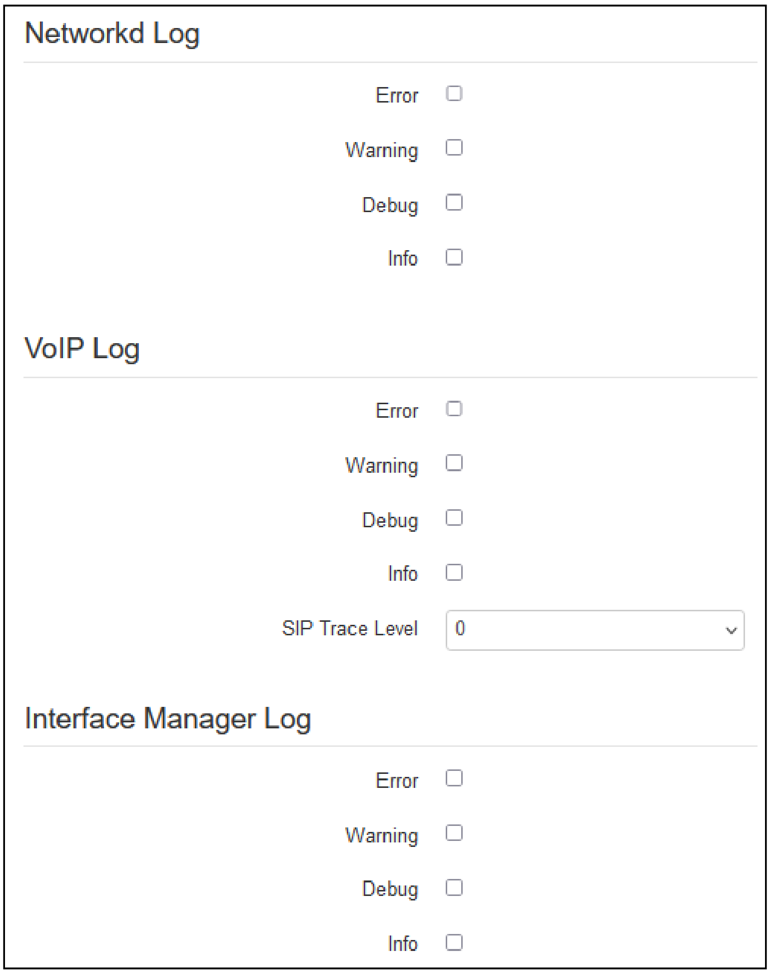
- *Configd Log* — deals with the configuration file operations (config file reads and writes from various sources) and the device monitoring data collection;
- *Networkd Log* — deals with network configuration;
- *VoIP Log* — deals with VoIP functions operation;
- *Interface Manager Log* — deals with the device user interface operation (such as keyboard, display, speaker phone, handset etc.);
- *Auto-update Log* — deals with auto-updating;
- *Remote phone book update log* — deals with LDAP phone book updating.

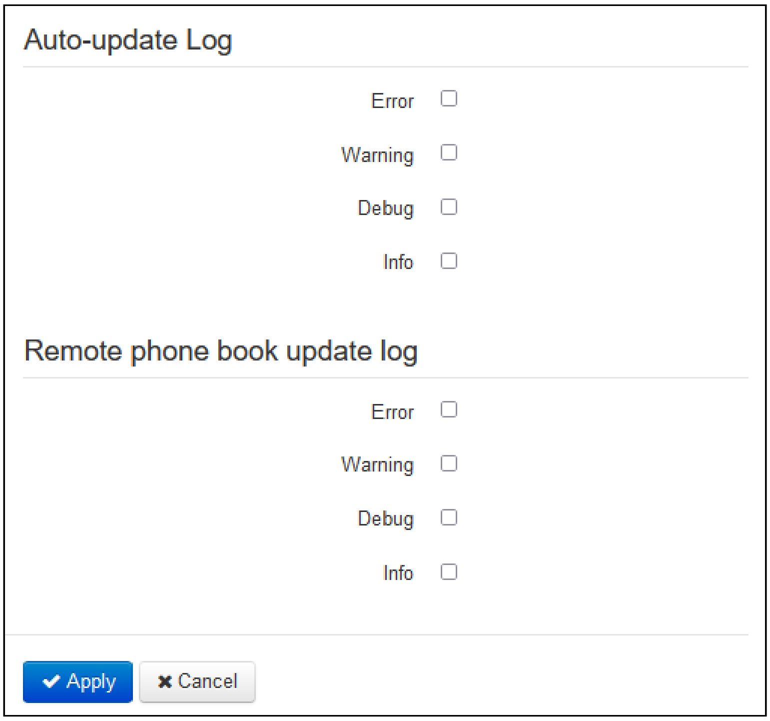


2.2.4.3.1 Syslog Settings

If there is at least a single log is configured for Syslog output, it is necessary to enable Syslog agent that will intercept debug messages from the respective manager and send them to remote server or save them to a local file in Syslog format.

- *Enable* — when selected, user Syslog agent is launched;
- *Mode* — Syslog agent operation mode:
  - *Server* — log information will be sent to the remote Syslog server (this is the 'remote log' mode):
    - *Syslog server address* — Syslog server IP address or domain name (required for 'Server' mode);
    - *Syslog server port* — port for Syslog server incoming messages (default value is 514; required for 'Server' mode).
  - *Local File* — log information will be saved to the local file:
    - *File Name* — name of the file to store log in Syslog format (required for 'Local File' mode);
    - *File Size, kB* — maximum log file size (required for 'Local File' mode).
  - *Server and File* — log information will be sent to the remote Syslog server and saved to the local file;
  - Console — log information will be sent to the device console (connection via a COM port adapter is required).





2.2.4.3.2 Configd Log, Network Log, VoIP Log, Interface Manager Log, Auto-update Log, Remote phone book update log

- *Error* — select this checkbox, if you want to collect 'Error' type messages;
- *Warning* — select this checkbox, if you want to collect 'Warning' type messages;
- *Debug* — select this checkbox, if you want to collect debug messages;
- *Info* — select this checkbox, if you want to collect information messages.
- *SIP trace level* — defines output level of VoIP SIP manager stack messages.

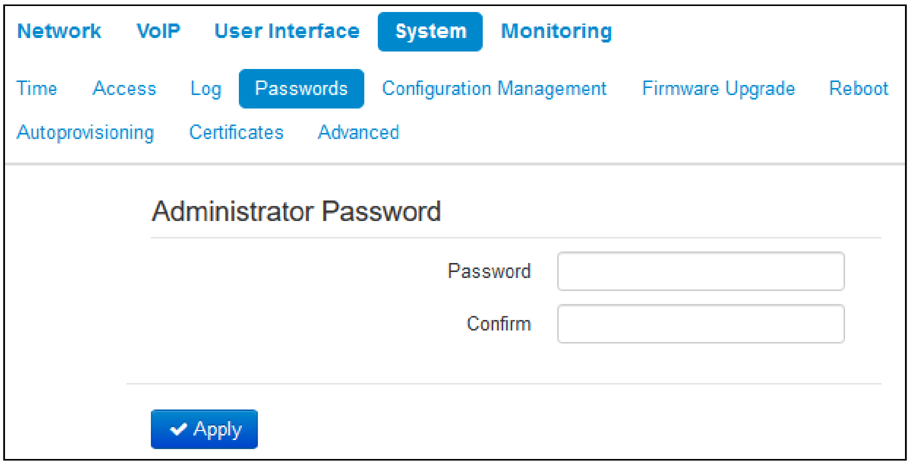
To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.4.4 'Passwords' submenu

In the 'Passwords' submenu you can define passwords for administrator.

When signing into web interface, administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring.

> Administator login: **admin**.

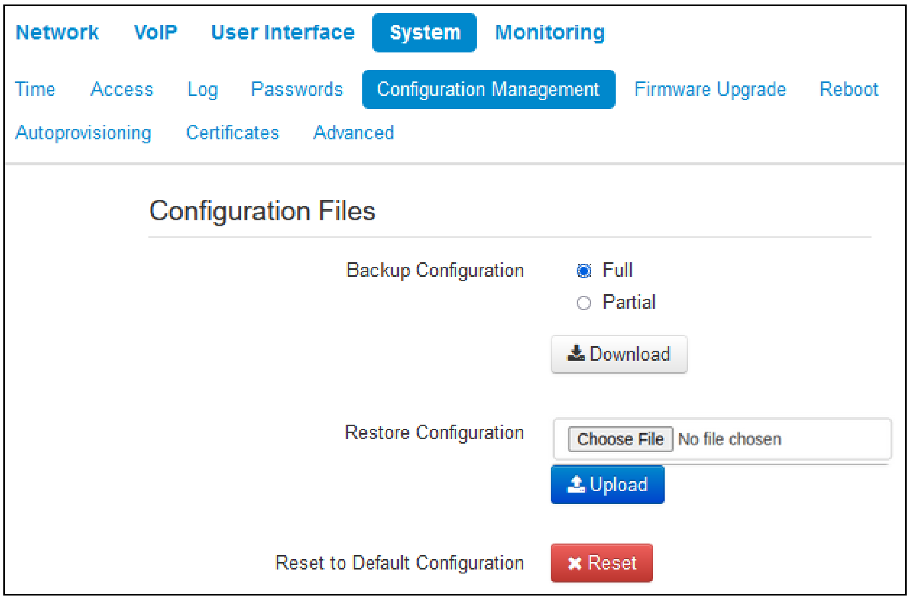


- *Password, Confirm* — enter administrator password in the respective fields and confirm it.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.4.5 'Configuration Management' submenu

In the 'Configuration management' submenu you can save and update the current configuration.



2.2.4.5.1 Backup Configuration

- *Full* — download full device configuration archive;
- *Partial* — download partial device configuration archive, which contains only user configuration.

To save the current device configuration to a local PC, click *'Download'* button.

2.2.4.5.2 Restore Configuration

Select configuration file stored on a local PC. To update the device configuration, click '*Choose File*' button, specify a file (in .tar.gz format) and click '*Upload*' button. Uploaded configuration will be applied automatically without device reboot.

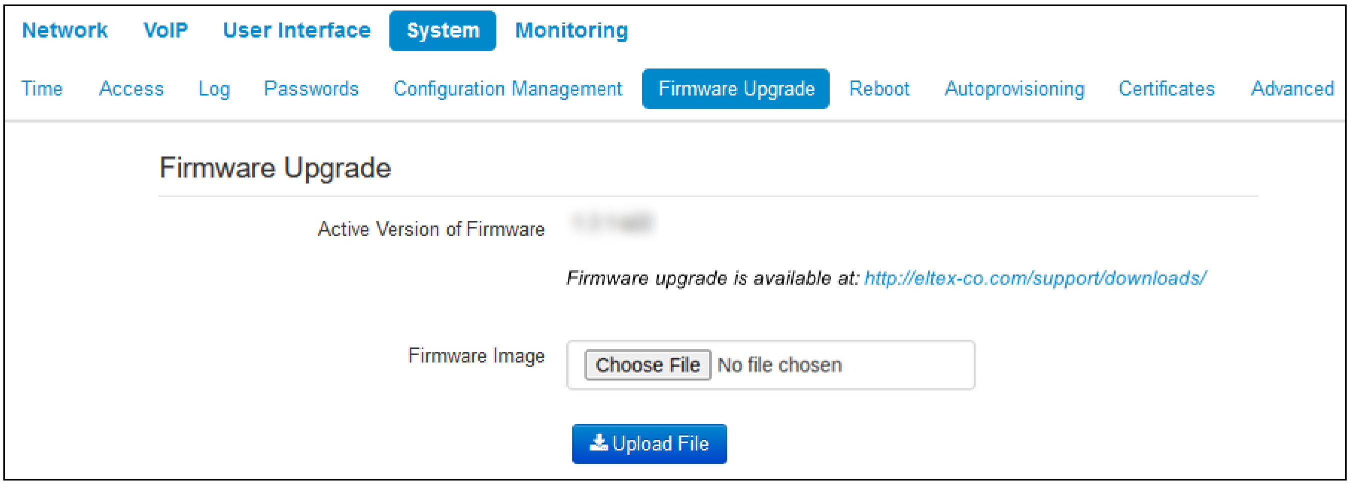
2.2.4.5.3 Reset to Default Configuration

To reset the device to default settings, click '*Reset*' button.

> When you reset the device configuration, the followings will be also reset:
> - contacts;
> - call history;
> - text messages.

2.2.4.6 'Firmware Upgrade' submenu

In 'Firmware upgrade' submenu you can update the firmware of the device.



- *Active Version of Firmware* — installed firmware version;

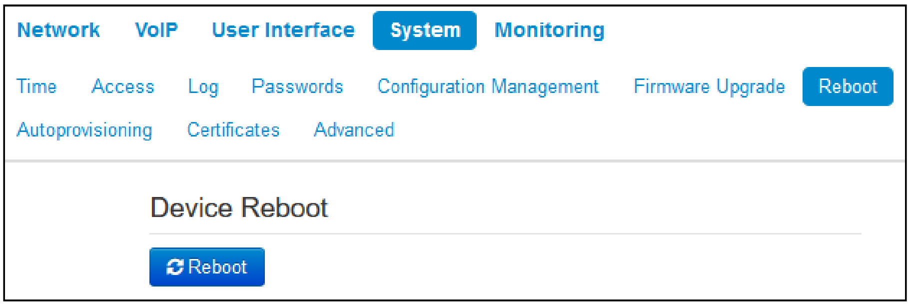
You can upgrade the device firmware manually by downloading the firmware file from the web site https://eltex-co.com/support/downloads/ and saving it on the computer. To do this, click the '*Choose File*' button and specify path to firmware .tar.gz format file.

To launch the update process, click '*Upload file*' button. The process can take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed.

> Do not switch off or reboot the device during the software upgrade.

2.2.4.7 'Reboot' submenu

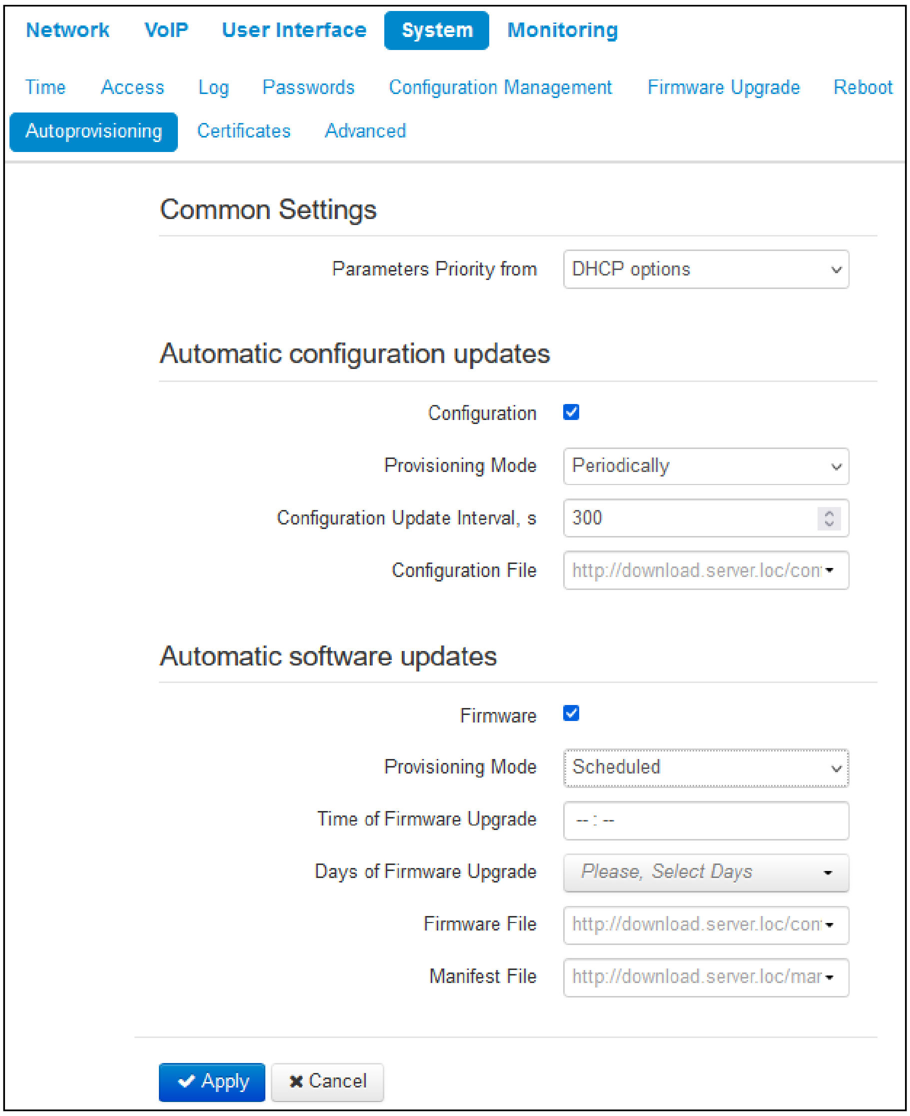
In the 'Reboot' submenu you can reboot the device.



Click the *'Reboot'* button to reboot the device. Device reboot process takes approximately 1 minute to complete.

2.2.4.8 'Autoprovisioning' submenu

In the 'Autoprovisioning' submenu you can configure DHCP-based autoprovisioning algorithm.



2.2.4.8.1 Common Settings

- *Parameters Priority from* — this parameter manages names and locations of configuration and firmware files:
  - *Static settings* — paths to configuration, firmware, and manifest files are defined by the *'Configuration File'* and *'Firmware File', and 'Manifest File'* settings;
  - *DHCP options* — paths to configuration and firmware files are defined by the DHCP Option 43, 66, and 67 (it is necessary to select DHCP for the Internet service).

2.2.4.8.2 Automatic configuration updates

2.2.4.8.2.1 Configuration

- *Provisioning Mode* — to update configuration, you can specify one of the several update modes:
  - *Periodically* — the device configuration will be automatically updated after defined period of time;
    - *Configuration Update Interval, s* — time period in seconds that will be used for periodic device configuration update; if 0 is selected, device will be updated only once — immediately after startup;
  - *Scheduled* — the device configuration will be automatically updated at specific times and on specific days:
    - *Time of Configuration Update* — time on 24-hour format that will be used for configuration autoupdate;
    - *Days of Configuration Update* — week days with defined time that will be used for configuration autoupdate.
- *Configuration File* — full path to configuration file; defined in URL format:
  - http://<server address>/<full path to cfg file>
  - https://<server address>/<full path to cfg file>
  - ftp://<server address>/<full path to cfg file>
  - tftp://<server address>/<full path to cfg file>

where <server address> — HTTP, HTTPS, FTP or TFTP server address (domain name or IPv4),

< full path to cfg file > — full path to configuration file on server.

2.2.4.8.3 Automatic software updates

2.2.4.8.3.1 Firmware

- *Provisioning Mode* — to update firmware, you can separately specify one of the several update modes:
  - *Periodically* — the device firmware will be automatically updated after defined period of time;
    - *Firmware Update Interval, s* — time period in seconds that will be used for periodic device firmware update; if 0 is selected, device will be updated only once — immediately after startup;
  - *Scheduled* — the device firmware will be automatically updated at specific times and on specific days:
    - *Time of Firmware Update* — time on 24-hour format that will be used for firmware autoupdate;
    - *Days of Firmware Update* — week days with defined time that will be used for firmware autoupdate.

- *Firmware File* — full path to firmware file; defined in URL format:
  - http://<server address>/<full path to firmware file>
  - https://<server address>/<full path to firmware file>
  - ftp://<server address>/<full path to firmware file>
  - tftp://<server address>/<full path to firmware file>

where <server address> — HTTP, HTTPS, TFTP or FTP server address (domain name or IPv4),

<full path to firmware file> — full path to firmware file on server.

- *Manifest File* — full path to manifest file; defined in URL format. The use of the manifest file is due to the large size of the firmware file, which is downloaded periodically using the firmware auto-update algorithm. To reduce load on the network in such cases, it is recommended to use the Manifest file. The file structure is a line that specifies the firmware version identifier that is available for downloading and updating.
  For example, the contents of the Manifest file could be as follows: '1.2.0-b100'.

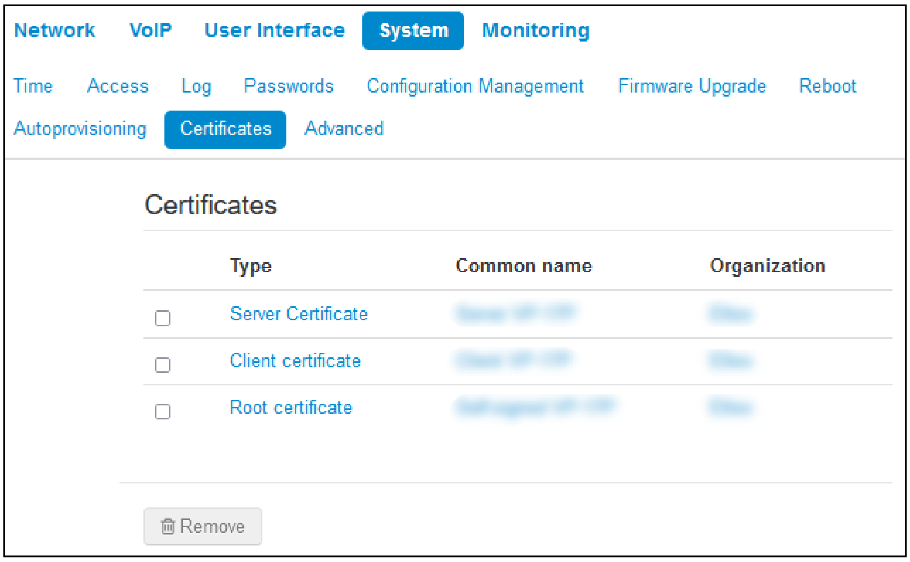
There is an optional ability to control the data integrity of the Manifest file, which consists of adding a line with an MD5 checksum to the file. If the Manifest file is specified, but an error occurs during network transmission and an incorrect checksum is received, then after a timeout specified in the configuration, an attempt will be made to obtain the Manifest file again. In this case, the contents of the Manifest file could be as follows:

```
1.2.0-b1
d969205dcc37c9c856fa43863e8c75ff
```

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

2.2.4.9 'Certificates' submenu

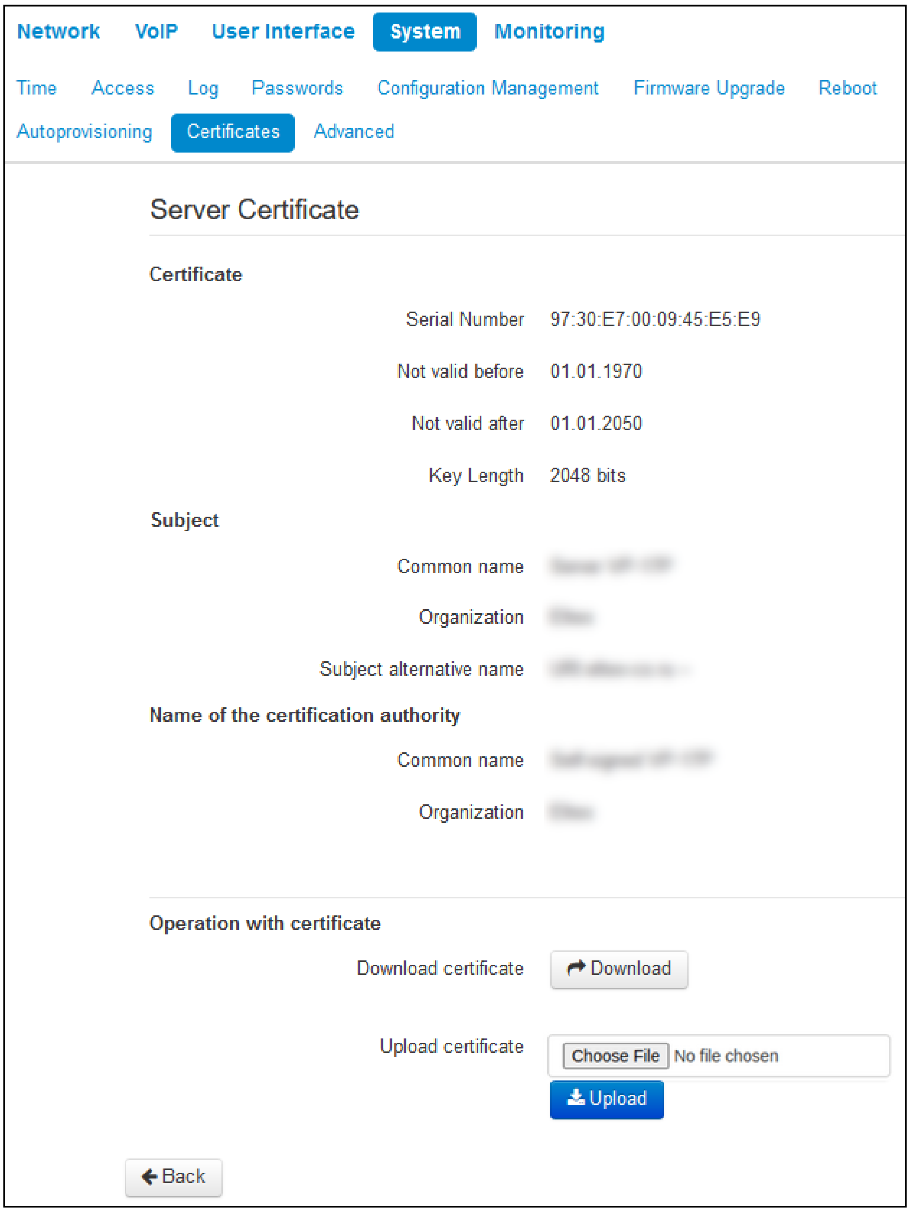
'Certificates' submenu allows to view, download and upload certificates for using in protected TLS connections. To configure a certificate, click the needed certificate type.



Select the certificate and click *'Remove'* button below the table to delete it.

2.2.4.9.1 Server certificate

Server certificate is used when accessing to the device web configurator via HTTPS.

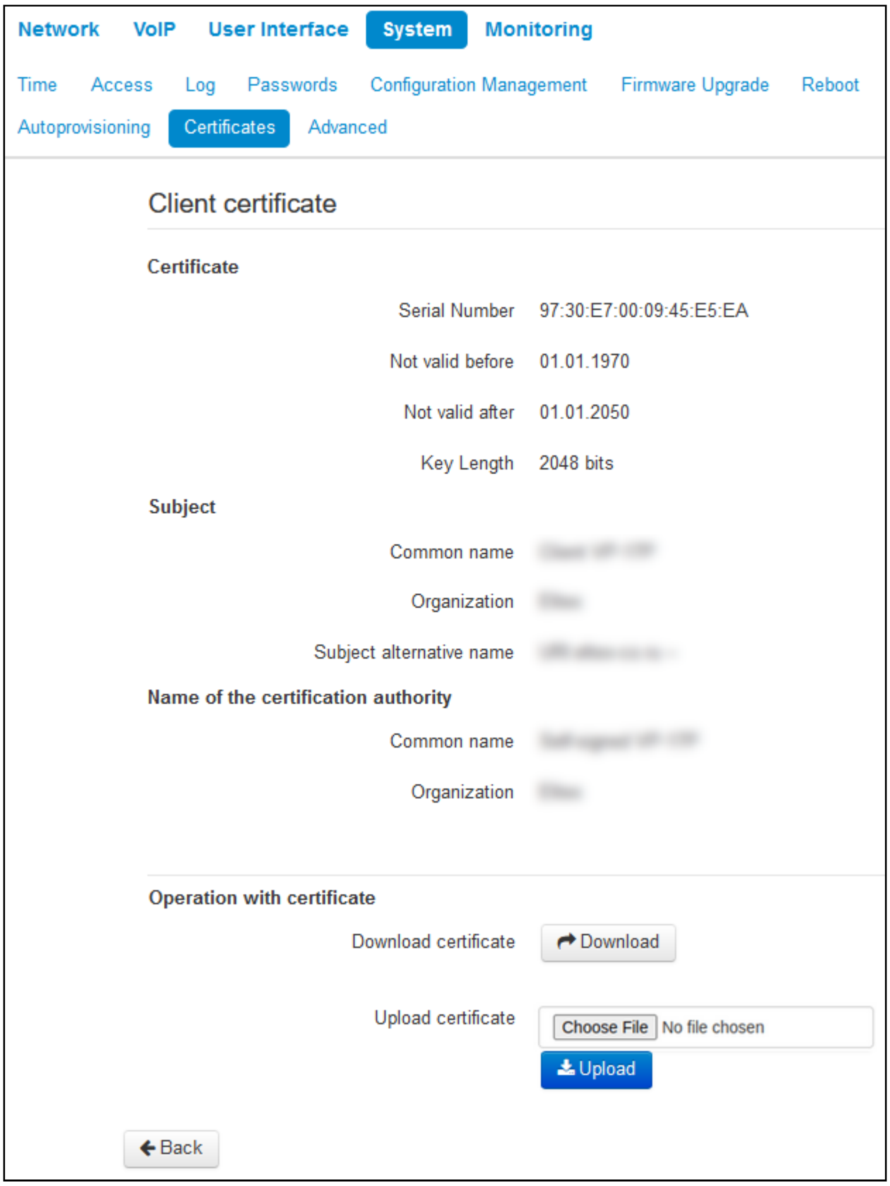


- *Certificate* — information about certificate:
  - *Serial Number* — serial number of the selected certificate;
  - *Not valid before* — valid-from date;
  - *Not valid after* — valid-to date;
  - *Key Length* — amount of encryption symbols in bits.
- *Subject* — information about the certificate recipient (*Common name, Organization, Subject alternative name*);
- *Name of the certification authority* — information about the certification authority (*Common name, Organization*);
- *Operation with certificate* — possible actions to be done with the certificate:
  - *Download certificate* — to save the certificate click *'Download'* button;
  - *Upload certificate* — to update the current certificate choose the file by clicking '*Choose File*' and then click *'Upload'*.

Click *'Back'* button to return to the list of certificates.

2.2.4.9.2 Client certificate

Client certificate is used with outbound connections via SIP with use of TLS.

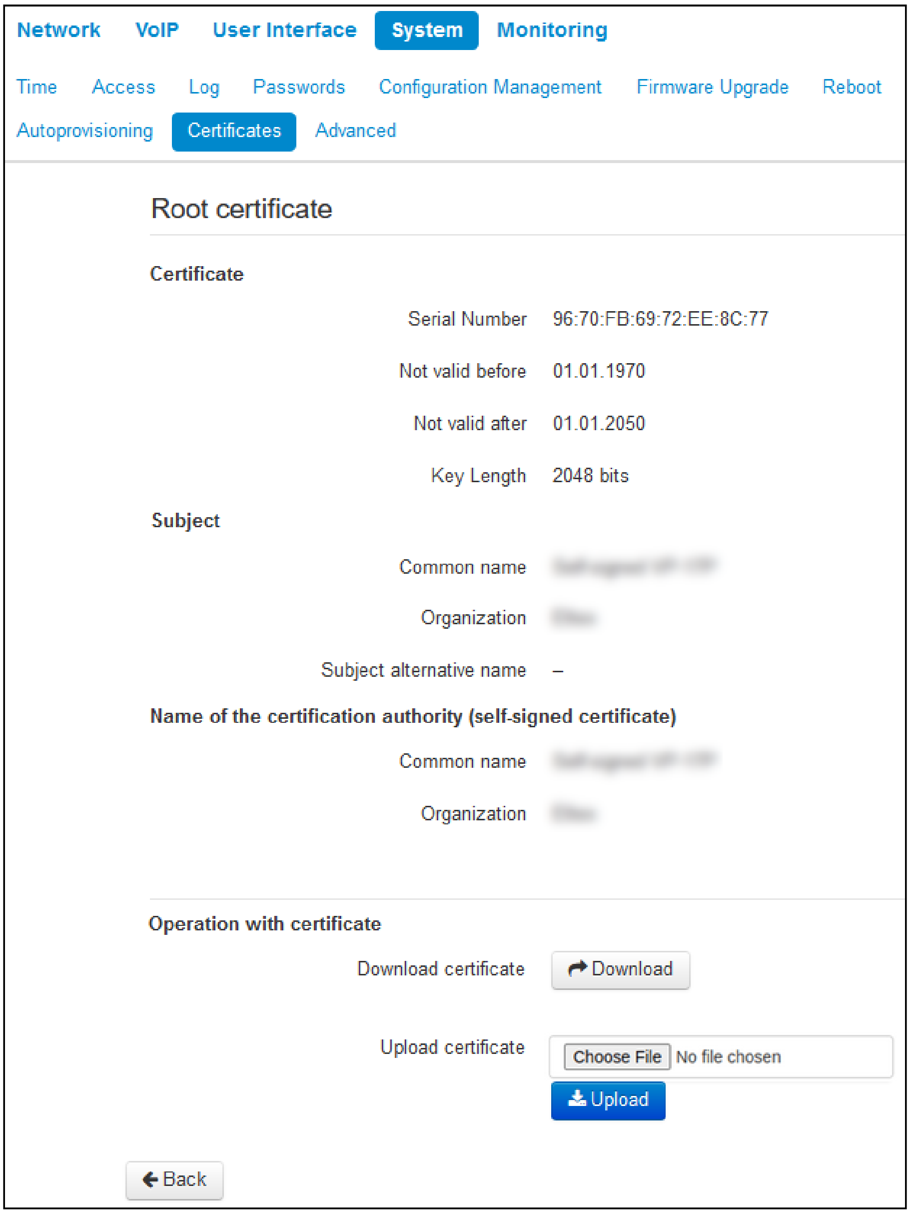


- *Certificate* — information about certificate:
  - *Serial Number* — serial number of the selected certificate;
  - *Not valid before* — valid-from date;
  - *Not valid after* — valid-to date;
  - *Key Length* — amount of encryption symbols in bits.
- *Subject* — information about the certificate recipient (*Common name, Organization, Subject alternative name*);
- *Name of the certification authority* — information about the certification authority (*Common name, Organization*);
- *Operation with certificate* — possible actions to be done with the certificate:
  - *Download certificate* — to save the certificate click '*Download*' button;
  - *Upload certificate* — to update the current certificate choose the file by clicking '*Choose File*' and then click '*Upload*'.

Click '*Back*' button to return to the list of certificates.

2.2.4.9.3 Root certificate

Root certificate is used to authenticate certificates with incoming connections. This certificate must be signed by the certification authority.

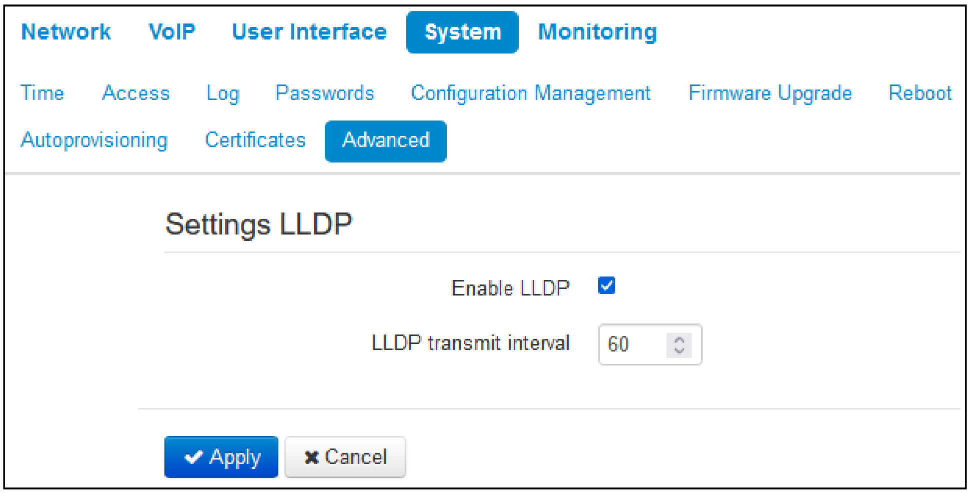


- *Certificate* — information about certificate:
  - *Serial Number* — serial number of the selected certificate;
  - *Not valid before* — valid-from date;
  - *Not valid after* — valid-to date;
  - *Key Length* — amount of encryption symbols in bits.
- *Subject* — information about the certificate recipient (*Common name, Organization, Subject alternative name*);
- *Name of the certification authority* — information about the certification authority (*Common name, Organization*);
- *Operation with certificate* — possible actions to be done with the certificate:
  - *Download certificate* — to save the certificate click *'Download'* button;
  - *Upload certificate* — to update the current certificate choose the file by clicking '*Choose File*' and then click *'Upload'*.

Click *'Back'* button to return to the list of certificates.

2.2.4.10 'Advanced' submenu

Use the menu to configure additional device settings.



2.2.4.10.1 Settings LLDP

- *Enable LLDP* — use LLDP when selected;
- *LLDP transmit interval* — time interval for messages transmission through LLDP. Default value is 60 seconds.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

2.3 Monitoring

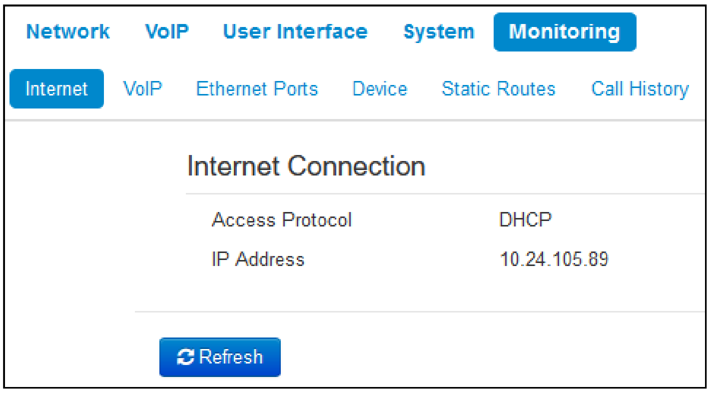
- Network parameters monitoring
- VoIP connection monitoring
    - Status of VoIP Network Interface
    - SIP Accounts Status
    - Actual Calls
- Ethernet ports monitoring
- Viewing information on the device
- Viewing the route table
- Viewing Call History

To enter the system monitoring mode, select 'Monitoring' tab from the panel.

> Some pages do not feature automatic update of the device monitoring data. To obtain the current information from the device, click Refresh button.

2.3.1 Network parameters monitoring

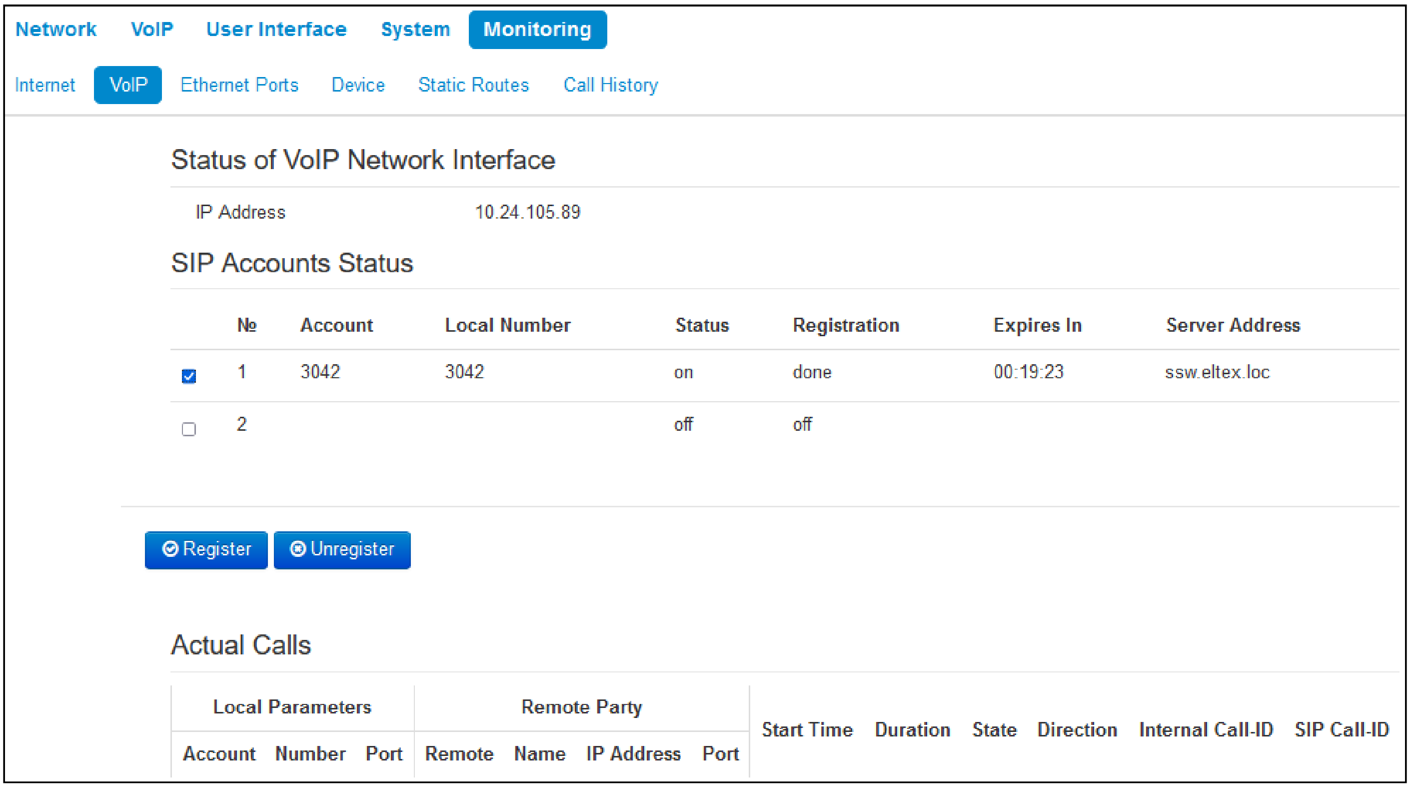
In the 'Internet' submenu you can view basic network settings of the device.



- *Access protocol* — protocol used for LAN access.
- *IP Address* — device IP address in the external network.

2.3.2 VoIP connection monitoring

In 'VoIP' submenu you can view VoIP network interface status and monitor accounts.



2.3.2.1 Status of VoIP Network Interface

- *IP Address* — IP address of VoIP network interface.

2.3.2.2 SIP Accounts Status

- *№* — number of account;
- *Account* — name of account;
- *Local Number* — subscriber phone number assigned to the current account;
- *Status* — account status:
  - *on*;
  - *off*.
- *Registration* — state of registration on proxy server for the group phone number:
  - *off* — SIP server registration function is disabled in SIP profile settings;
  - *error* — registration was unsuccessful;
  - *done*— registration on SIP server successfully completed.
- *Expires In* — expiration time of account registration on SIP server;
- *Server Address* — address of the server on which the subscriber line has been registered at the last time.

Buttons for forced registration '*Register*' or unregistration '*Unregister*' of selected accounts are located under the table 'SIP Accounts Status'.

2.3.2.3 Actual Calls

Actual Calls

Local Parameters			Remote Party				Start Time	Duration	State	Direction	Internal Call-ID	SIP Call-ID
Account	Number	Port	Remote	Name	IP Address	Port						
3042	3042	23000	3043	-	10.80.0.10	12978	14:31:35 03.05.2024	00:01:10	holded	outgoing	1	ae407000-83fc-123d-95a2-6813e2091653
3042	3042	23004	3035	-	10.80.0.11	12318	14:31:41 03.05.2024	00:01:04	talking	outgoing	2	b251e0f9-83fc-123d-95a2-6813e2091653

Local Parameters

- *Account* — name of account through which a call is implemented or on which the call was received;
- *Number* — phone number assigned on the account;
- *Port* — RTP stream local port.

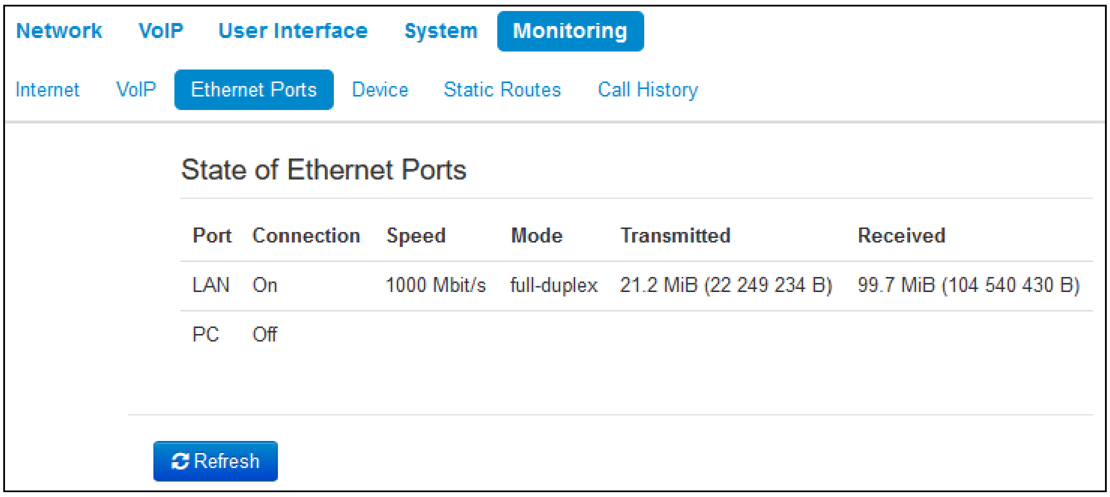
Remote Party

- *Number* — phone number of opposite party;
- *Name* — opposite party name;
- *IP address* — IP address of opposite party used for RTP;
- *Port* — UDP port of opposite party used for RTP stream.

Common parameters

- *Start Time* — call start time;
- *Duration* — call duration;
- *State* — call state. Call might be in the following states:
  - *call* — ringback tone is issued (during outcoming call);
  - *incoming call* — ring tone is issued (during incoming call);
  - *talking;*
  - *holded;*
  - *conference.*
- *Direction* — call type:
  - *incoming;*
  - *outgoing.*
- *Internal Call-ID;*
- *SIP Call-ID.*

2.3.3 Ethernet ports monitoring

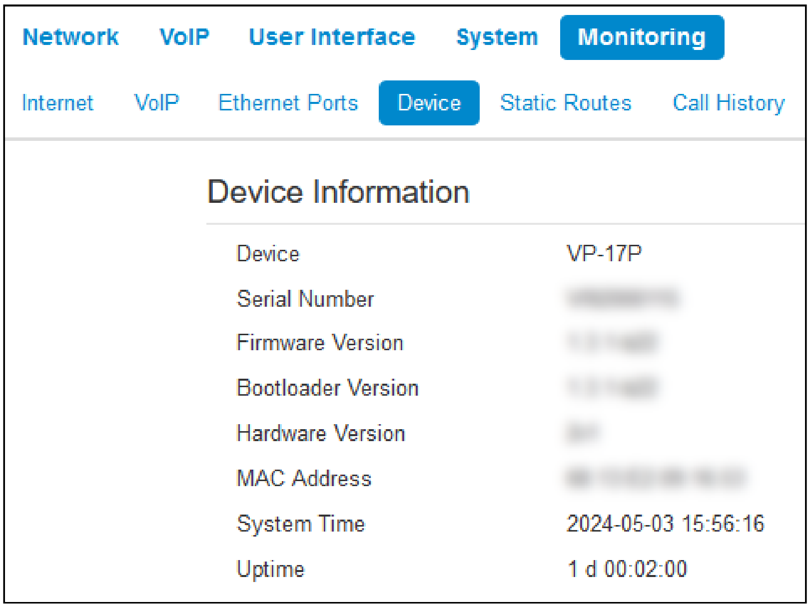


- *Port* — port name:
  - *LAN* — external network port;
  - *PC* — port for PC connection.
- *Connection* — state of the connection to the port:
  - *On* — a network device is connected to the port (active link);
  - *Off* — network device is not connected to the port (inactive link).
- *Speed* — data rate of the external network device connected to the port (10/100/1000 Mbit/s);
- *Mode* — data transfer mode:
  - *Full-duplex*;
  - *Half-duplex*.
- *Transmitted* — quantity of bytes sent from the port;
- *Received* — quantity of bytes received by the port.

To obtain the current information on Ethernet ports and updating the values and transmitted bytes, click Refresh button .

2.3.4 Viewing information on the device

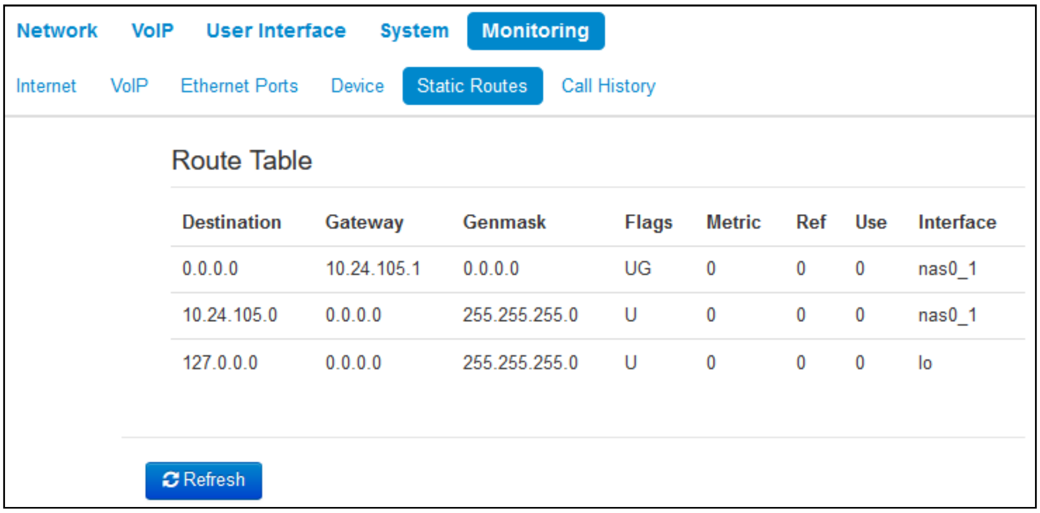
In the 'Device' submenu you can find general device information.



- *Device* — device model name;
- *Serial Number* — device serial number defined by the manufacturer;
- *Firmware Version* — device firmware version;
- *Bootloader Version* — software version of the device bootstrap;
- *Hardware Version* — device revision;
- *MAC Address* — device MAC address defined by the manufacturer;
- *System Time* — current date and time defined in the system;
- *Uptime* — time of operation since the last startup or reboot of the device.

2.3.5 Viewing the route table

In the 'Static Routes' submenu you can view the device route table.



Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	10.24.105.1	0.0.0.0	UG	0	0	0	nas0_1
10.24.105.0	0.0.0.0	255.255.255.0	U	0	0	0	nas0_1
127.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	lo

- *Destination* — IP address of destination host or subnet that the route is established to;
- *Gateway* — gateway IP address that allows for the access to the 'Destination';
- *Genmask* — subnet mask;
- *Flags* — specific route attributes. The following flag values exist:
  - **U** — means that the route is created and passable;
  - **H** — identifies the route to the specific host;
  - **G** — means that the route lies through the external gateway. System network interface provides routes in the network with direct connection. All other routes lie through the external gateways. 'G' flag is user for all routes except for the routes in the direct connection networks;
  - **R** — means that the route most likely was created by a dynamic routing protocol running on a local system with the 'reinstate' parameter;
  - **D** — means that the route was added on reception of the ICMP Redirect Message. When the system learns the route from the ICMP Redirect message, the route will be added into the routing table in order to exclude redirection of the following packets intended for the same destination. Such routes are marked with the 'D' flag;
  - **M** — means that the route was modified — likely by a dynamic routing protocol running on a local system with the 'mod' parameter applied;
  - **A** — means buffered route with corresponding record in the ARP table;
  - **C** — means that the route source in the core routing buffer;
  - **L** — means that the route destination is an address of this PC. Such 'local routes' exist in the routing buffer only;
  - **B** — means that the route destination is a broadcasting address. Such 'broadcast routes' exist in the routing buffer only;
  - **I** — means that the route is related to the loopback interface. Such 'internal routes' exist in the routing buffer only;
  - **!** — means that datagrams sent to this address will be rejected by the system.
- *Metric* — defines route cost. Metrics allows you to sort the duplicate routes, if they exist in the table;
- *Ref* — identified number of references to the route for connection establishment (not used by the system);
- *Use* — number of route detections performed by IP protocol;
- *Interface* — name of the network interface that the route lies through.

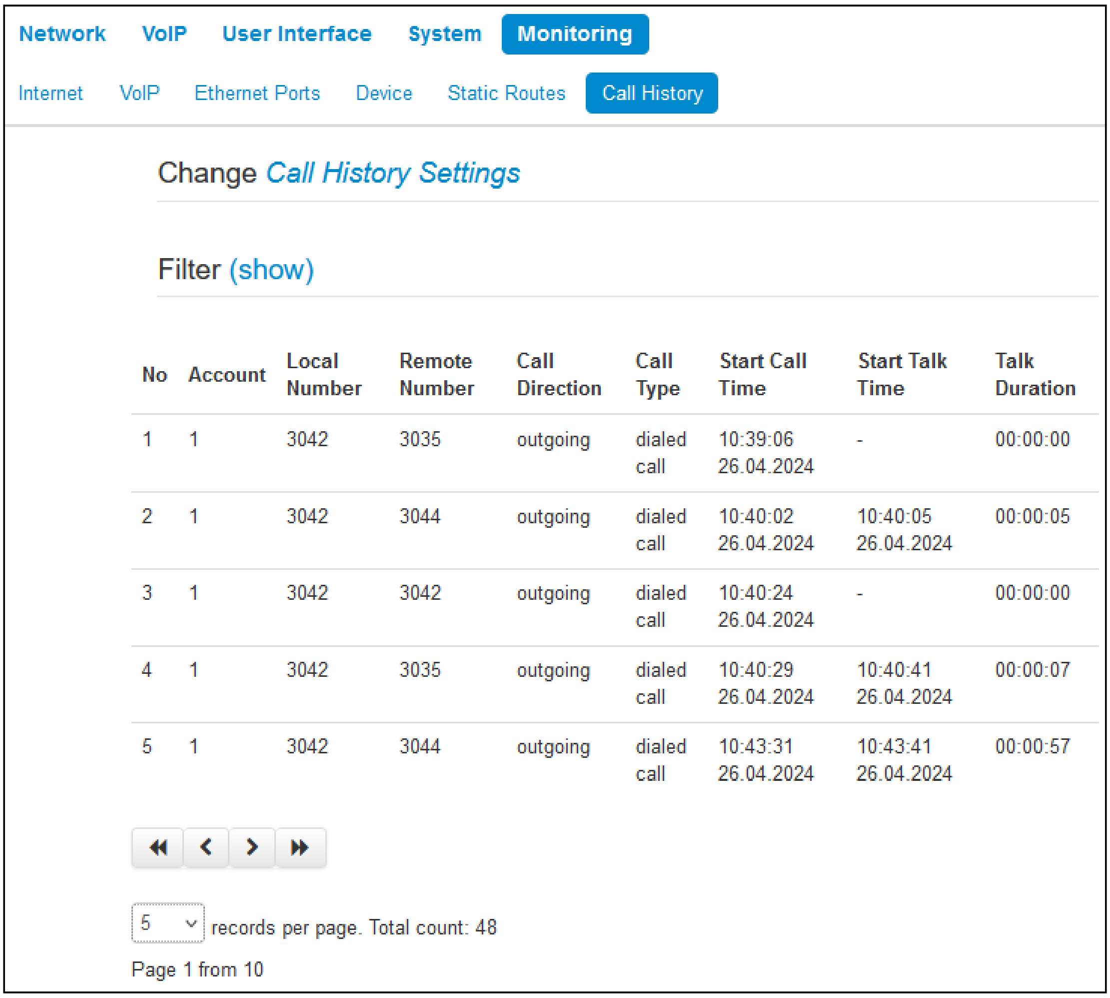
To obtain the current information from the device, click Refresh button.

2.3.6 Viewing Call History

In the 'Call History' submenu you can view the list of phone calls and the summary for each call.

The device RAM can store up to 100 records for performed calls. If the record number exceeds 100 the oldest records (at the top of the table) will be removed, and new ones will be added at the end of the file.

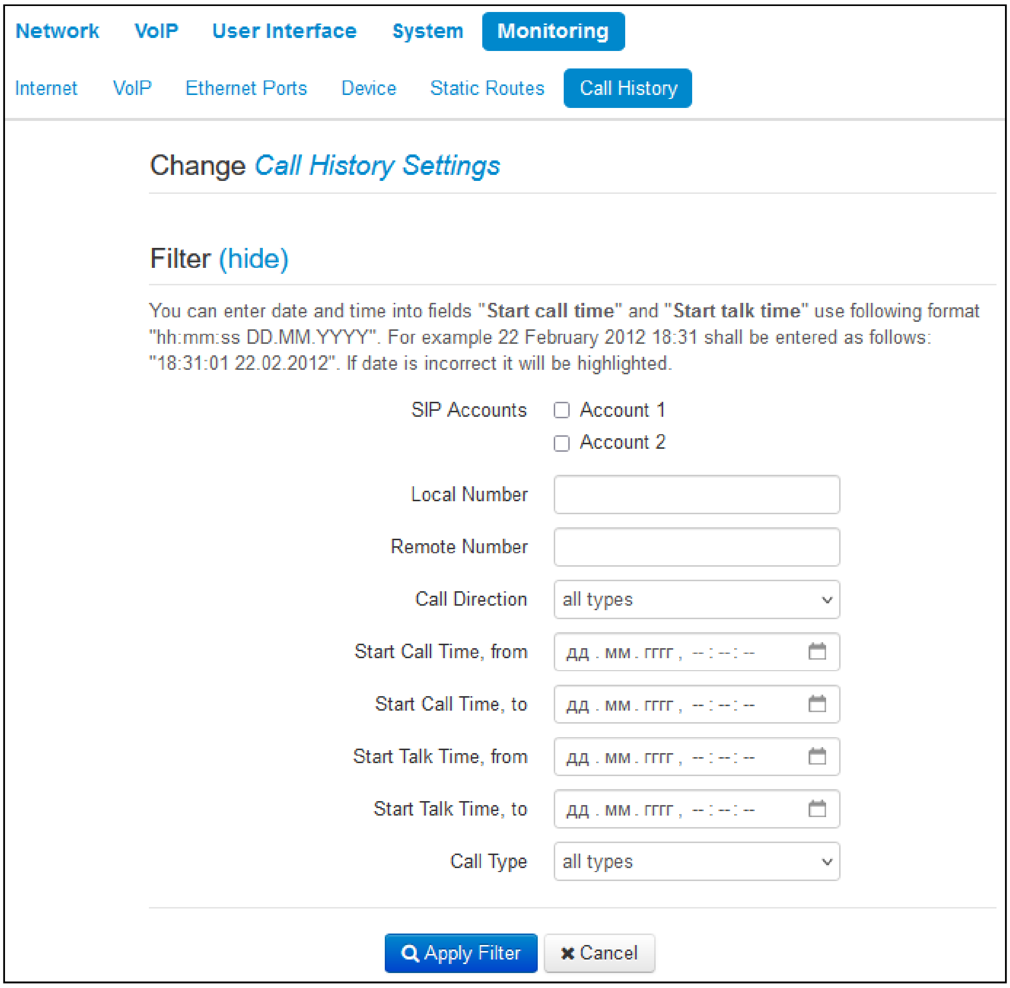
Call log statistics will not be collected, when the history size is zero.



No	Account	Local Number	Remote Number	Call Direction	Call Type	Start Call Time	Start Talk Time	Talk Duration
1	1	3042	3035	outgoing	dialed call	10:39:06 26.04.2024	-	00:00:00
2	1	3042	3044	outgoing	dialed call	10:40:02 26.04.2024	10:40:05 26.04.2024	00:00:05
3	1	3042	3042	outgoing	dialed call	10:40:24 26.04.2024	-	00:00:00
4	1	3042	3035	outgoing	dialed call	10:40:29 26.04.2024	10:40:41 26.04.2024	00:00:07
5	1	3042	3044	outgoing	dialed call	10:43:31 26.04.2024	10:43:41 26.04.2024	00:00:57

'Call history' table field description:

- *No* — sequence number of the record in the table;
- *Account* — device subscriber port number;
- *Local Number* — subscriber number assigned to the current subscriber port;
- *Remote Number* — remote subscriber number that the phone connection has been established with;
- *Call Direction* — *outgoing* or *incoming*;
- *Call Type* — *dialed, missed* or *answered*;
- *Start Call Time* — call received/performed time and date;
- *Start Talk Time* — call start time and date;
- *Talk Duration* — call duration in seconds.



In the call history table you can search records by different parameters; to do this, click the Filter '*(show)*' link. Filtering can be performed by account, local or remote number, call direction, start call time, call talk time, and call type. For filtering parameter description, see call history table field description above.

- *Start Call Time from/to* or *Start Talk Time from/to* — call received/performed time period or call start time period in the 'dd.mm.yyyy hh:mm:ss' format.

To hide the table record filtration parameter settings, click the Filter '*(hide)'* link.

To configure call history parameters, click '*Change Call History Settings*' link. For detailed parameter configuration description, see 'Phonebook' submenu.

Click button to proceed to the table showing the first record.

Click button to proceed to the previous page with the call history table.

Click button to proceed to the next page with the call history table.

Click button to proceed to the table showing the last record.

You can select the number of displayed records at the bottom of the page.

3 Example of device configuration

1. Open web browser such as Firefox, Opera or Chrome on the PC.

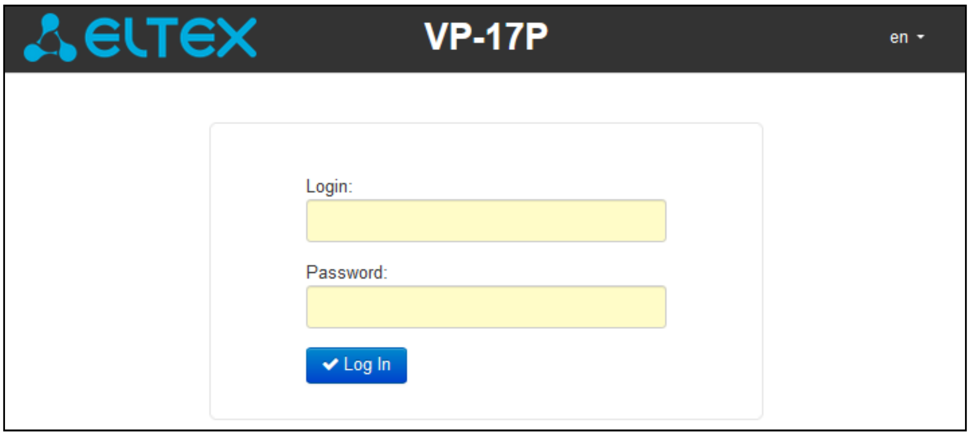
2. Enter the device IP address in an address line of a browser.

By default, the device receives IP address and other network parameters via DHCP. For further work, you should know IP address received by IP phone from DHCP server. To do it, use display menu:

1. Press 'Menu' soft key.
2. Check the IP address assigned to the phone in 'State' → 'Network' section.

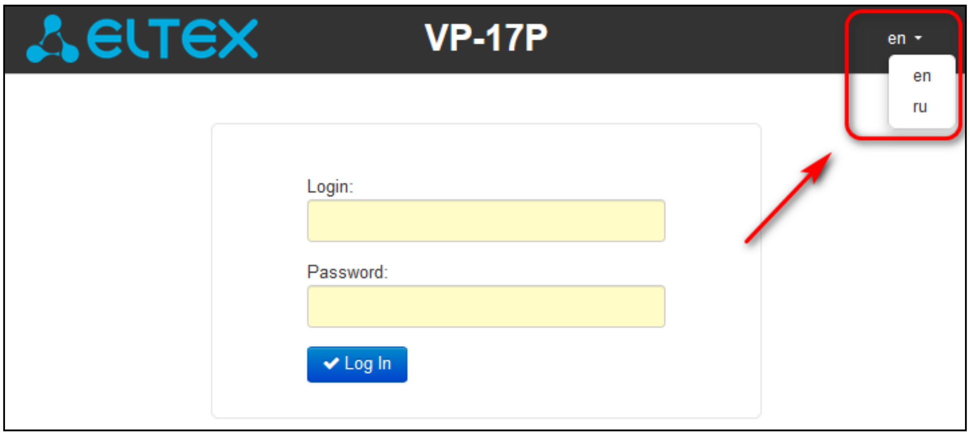
If IP address is 0.0.0.0, it means IP phone has not received IP address from DHCP server. In this case, you should manually configure network parameters by using display menu.

If the device is successfully connected, you will see a pop-up window with login and password. Fill in the following fields and click '*Log in*' button.

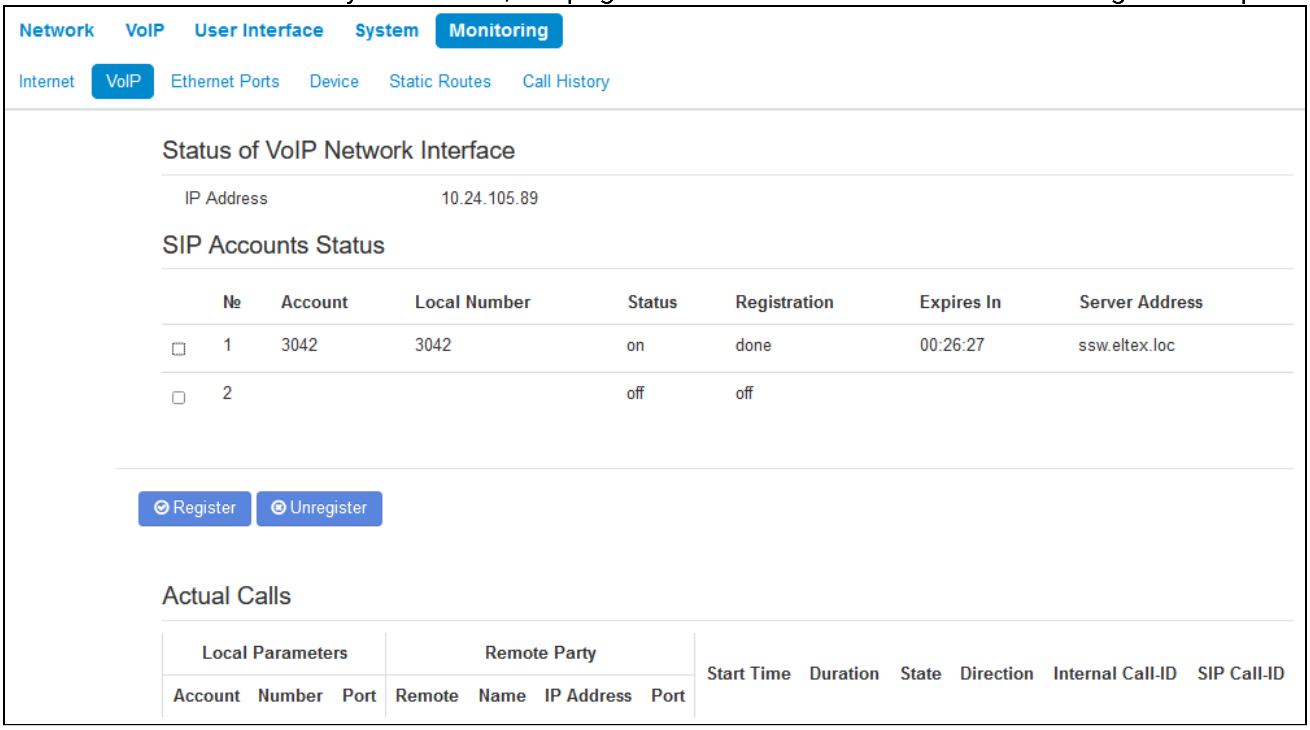


By default, login: **admin**, password: **password**.

You can change web interface language at the top right corner, see below:



If the device has been successfully authorized, the page of the device current state monitoring will be opened:

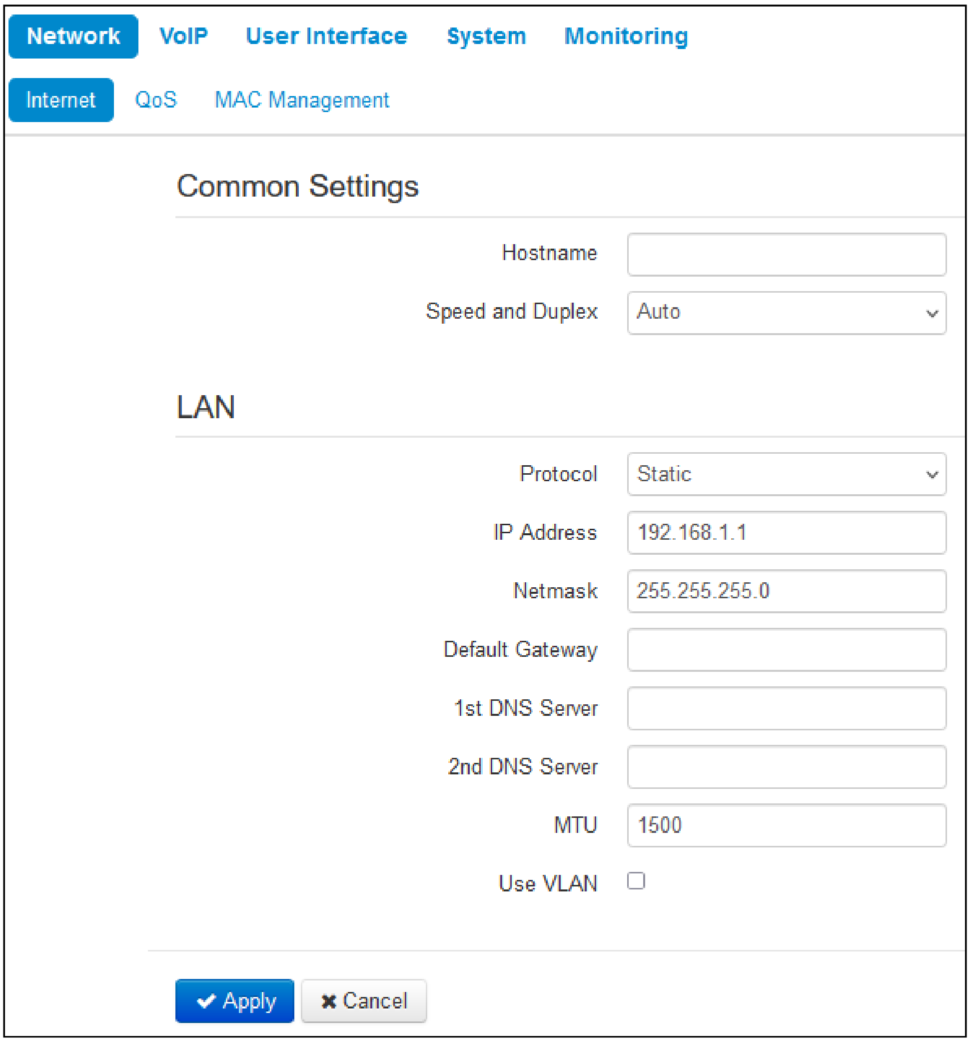


3. To change the device network settings go to 'Network' → 'Internet' section.

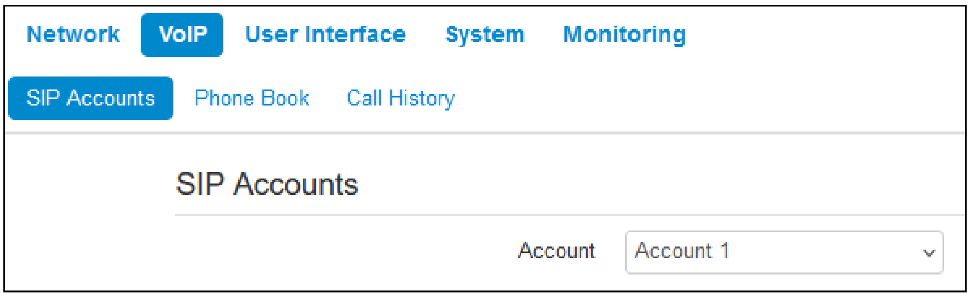
   Select protocol used by your Internet provider in '*Protocol*' field and enter necessary data according to provider guidelines. If static settings are used for connection to a provider network, select '*Static*' value in the '*Protocol*' field and fill in *'IP address*', '*Netmask*', '*Default gateway*', '*1st DNS Server*' and '*2nd DNS Server*' fields (parameter values are given by service provider).

   To save and apply settings, click 

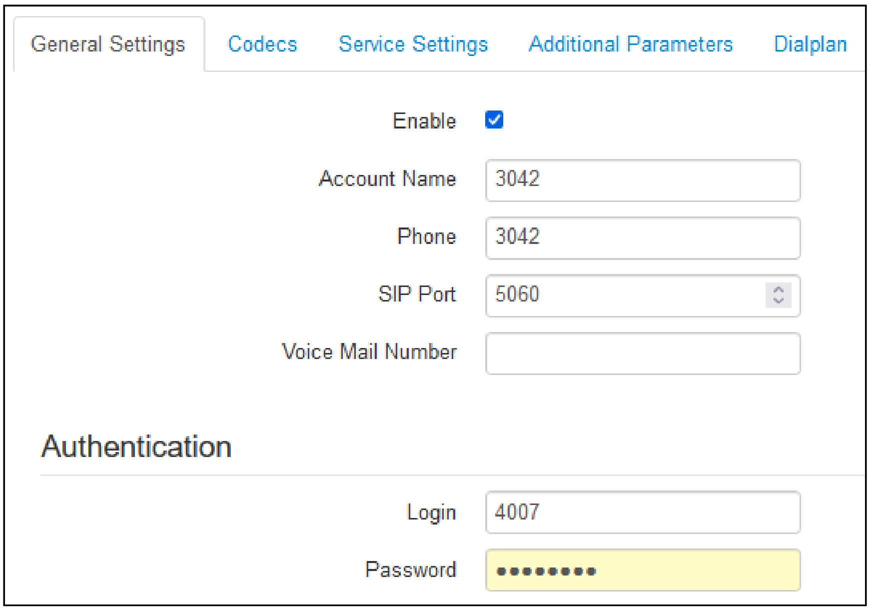
.



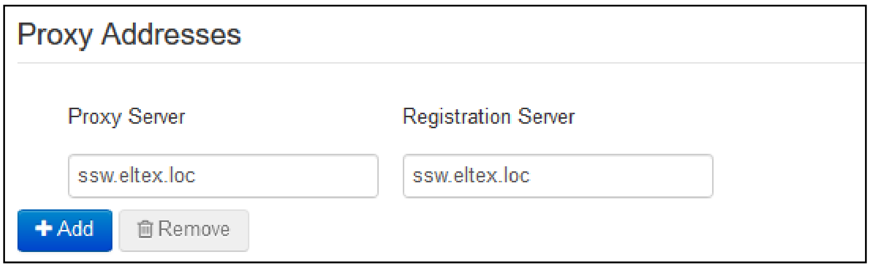
   Use 'VoIP' → 'SIP Accounts' tab to configure accounts for operation via SIP. To do it, select '*Account*' required for configuring in the drop-down list.



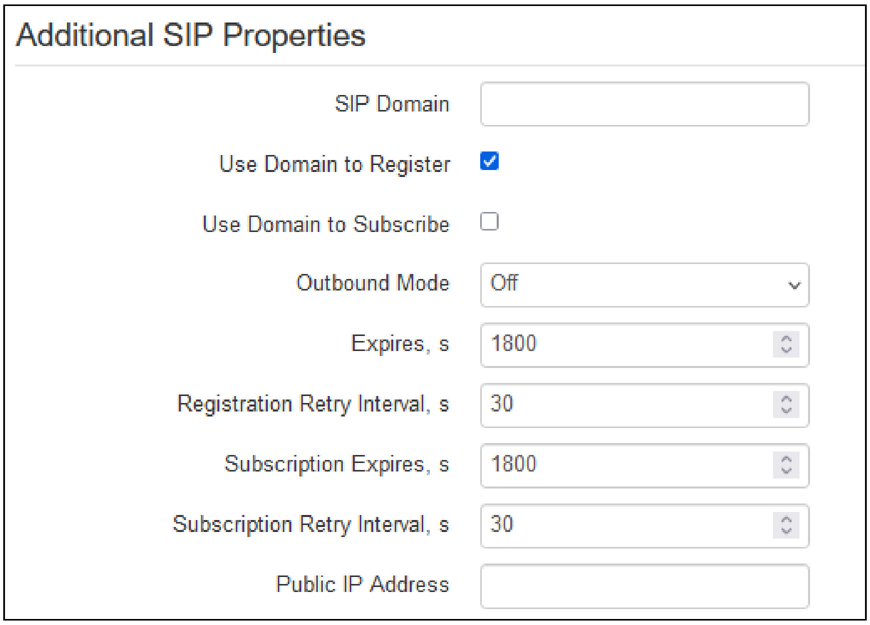
Select '*Enable*' checkbox, enter phone number assigned to the current account and specify login and password for SIP server authorization.



Specify IP address or SIP server domain name and registration servers (if required) in relevant fields in section 'Proxy Addresses'. If port numbers used on servers are different than 5060, you should specify alternative port colon separated.



Specify SIP domain (if required) in relevant field in the tab below. If it is required to use domain to register set the relevant flag in 'Additional SIP Properties' section.

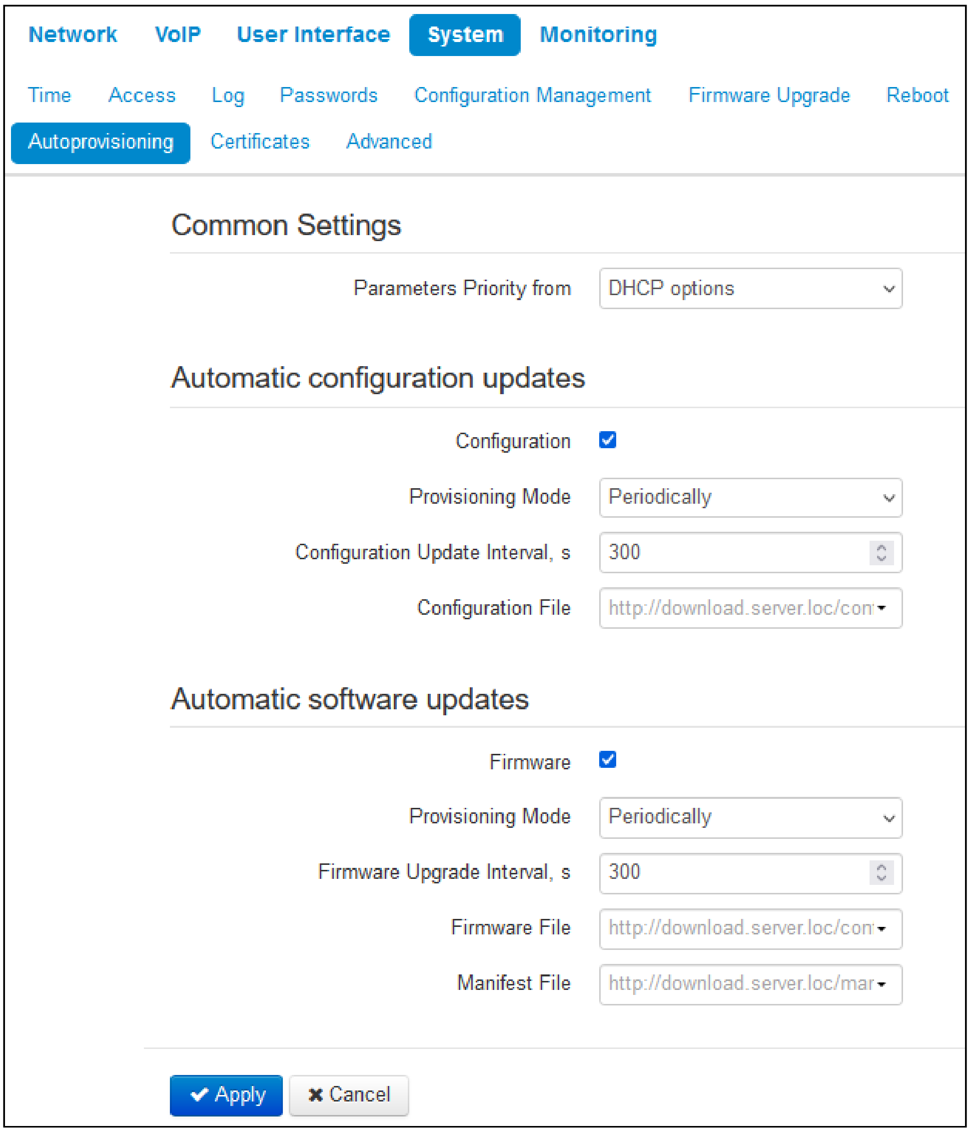


To save and apply settings click 

button.

4 Appendixes to VP-17P user manual

4.1 Device automatic update algorithm based on DHCP



Device automatic update algorithm is defined by the '*Parameters Priority from*' value.

If the '*Static settings*' value is selected, then the full path (including access protocol and server address) to configuration file and firmware file will be defined by '*Configuration File*' and '*Firmware File*' parameters. Full path should be specified in URL format:

<protocol>://<server address>/<path to file>, where

- <protocol> — protocol used for downloading corresponding files from the server;
- <server address> — address of the server with a file to be downloaded (domain name or IPv4);
- <path to file> — path to file on the server, the file must be in tar.gz extension.

You may use the following macro in URL (reserved words substituted with the specific values):

- *$MA* – MAC address — this macro in file URL is substituted by the native device MAC address;
- *$SN* – Serial number — this macro in file URL is substituted by the native device serial number;
- *$PN* – Product name — this macro in file URL is substituted by the model name (e.g, VP-12P);
- *$SWVER* — Software version — this macro in file URL is substituted by the firmware version number;
- *$HWVER* — Hardware version — this macro in file URL is substituted by the device hardware version number.

For MAC address, serial number and model name, see 'Device' section on the 'Monitoring' tab.

<u>URL examples:</u>

tftp://download.server.loc/firmware.tar.gz,

http://192.168.25.34/configs/vp-17(p)/mycfg.tar.gz,

tftp://server.tftp/$PN/config/$SN.tar.gz,

http://server.http/$PN/firmware/$MA.tar.gz etc.

If the system is unable to extract the necessary file downloading parameters (protocol, server address or path to file on server) from configuration file or firmware file URL, it will attempt to extract an unknown parameter from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), when address obtaining via DHCP is enabled for the Internet service (DHCP option format and analysis will be provided below). If the system is unable to extract missing parameter from DHCP options, default value will be used:

- protocol: *tftp*;
- server address: *update.local*;
- configuration file name: *$MAC.cfg*;
- firmware file name: *vp17.fw*;
- Manifest file name: *vp17.manifest*.

Thus, if you leave *'Configuration File'* and *'Firmware File'* fields empty, and Options 43 or 66, 67 with file locations are not obtained via DHCP, configuration file URL will be as follows:

tftp://update.local/A8.F9.4B.00.11.22.cfg,

firmware file URL:

tftp://update.local/ vp17.fw;

Manifest file URL:

tftp://update.local/ vp17.manifest.

If '*DHCP options*' value is selected, configuration file and firmware file URLs will be extracted from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), wherefore address obtaining via DHCP should be enabled for the Internet service (DHCP option format and analysis will be provided below). If DHCP options fail to provide some of the URL parameters, default parameter value will be used:

- protocol: *tftp*;
- server address: *update.local*;
- configuration file name: *$MAC.cfg*;
- firmware file name: *vp17.fw*;
- Manifest file name: *vp17.manifest*.

1. Inspite of the filename *$MAC.cfg*, the file format should be in *.tar.gz* extension
2. Inspite of the firmware name *vp17.fw*, the file format should be in *.tar.gz* extension
3. You may upload a text file of configuration, the format of the text file must be *.json*

4.1.1 Option 43 format (Vendor specific info)

TR-069 autoconfiguration is not supported on version 1.3.1. It is recommended to specify suboptions 5, 6, 7, and 9 when using option 43 for the VP-17P device.

1|<acs_url>|2|<pcode>|3|<username>|4|<password>|5|<server_url>|6|<config.file>|7|<firmware.file>|9|<manifest>

1 — TR-069 autoconfiguration server address code;

2 — 'Provisioning code' parameter specification code;

3 — code of the username for TR-069 server authorization;

4 — code of the password for TR-069 server authorization;

5 — server address code; server address URL should be specified in the following format: tftp://address or http://address. The first version represents TFTP server address, the second version – HTTP server address;

6 — configuration file name code;

7 — firmware file name code;

9 — Manifest file name code;

'|' — mandatory separator used between codes and suboption values.

4.1.2 Algorithm of identification for configuration file and firmware file URL parameters from DHCP Options 43 and 66

1. DHCP exchange initialization.
   Device initializes DHCP exchange after the startup.

2. Option 43 analysis.
   When Option 43 is received, codes 5, 6, 7 and 9 suboptions are analyzed in order to identify the server address and the configuration, firmware file, and Minifest file names.

3. Option 66 analysis.
   If Option 43 is not received from DHCP server or it is received but the system fails to extract the server address, Option 66 will be discovered. If the system fails to obtain the firmware file name, Option 67 will be discovered. They are used for TFTP server address and the firmware file path extraction respectively. Next, configuration and firmware files will be downloaded from Option 66 address via TFTP.

4.1.3 Special aspects of configuration updates

Configuration file should be in **.tar.gz** format (this format is used when configuration is saved from the web interface in the 'System' → 'Configuration Management' tab). Configuration downloaded from the server will be applied automatically and does not require device reboot.

4.1.4 Special aspects of firmware updates

Firmware file should be in **.tar.gz** format. When the firmware file is loaded, the device unpacks it and checks its version (using 'version' file in **tar.gz** archive).

If the current firmware version matches the version of the file obtained via DHCP, firmware will not be updated. Update is performed only when firmware versions are mismatched. The process of writing a firmware image to the device’s flash memory is indicated by the appearance of the 'Firmware update in progress...' screen on the phone display.

> Do not power off or reboot the device, when the firmware image is being written into the flash memory. These actions will interrupt the firmware update that will lead to the device boot partition corruption. The device will become inoperable.

4.2 Description of VP-17P configuration file cfg.json (+WEB)

Description of VP-17P configuration file is available at this link.

4.3 Preparing an audio file to be uploaded as a ringtone

An audio file should satisfy the following requirements to be played correctly:

- Sampling frequency — 8000 Hz;
- Number of channels — 1 (Mono);
- Code size — 8 bit;
- Codec — A-Law.

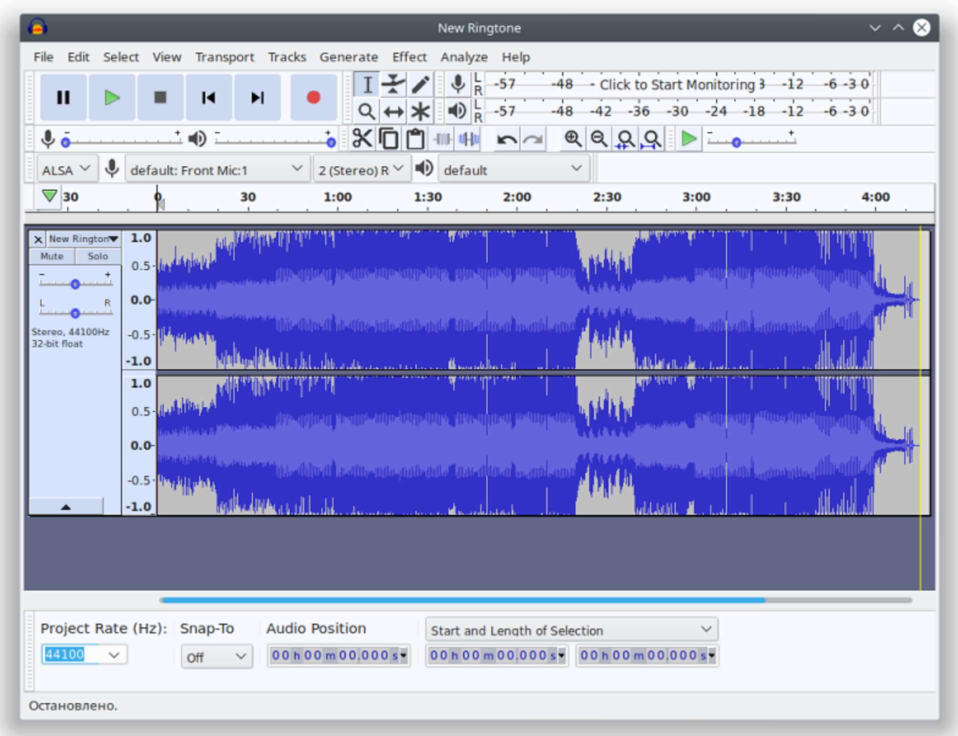
Audio file might be prepared through different methods:

1. Through 'Audacity' audio editing software or its analogue such as 'Sony Sound Forge';
2. Through console utilities (sox, ffmpeg, gstreamer);
3. Through online services.

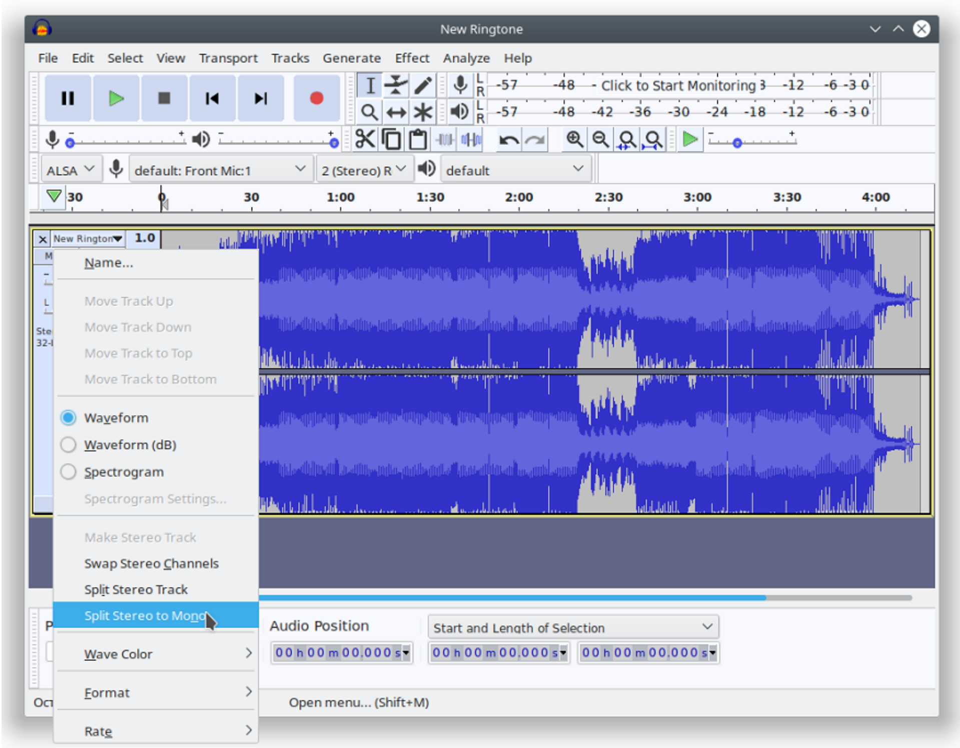
The example of audio file preparation in 'Audacity' audio editing software is shown below.

4.3.1 Preparing an audio file in 'Audacity'

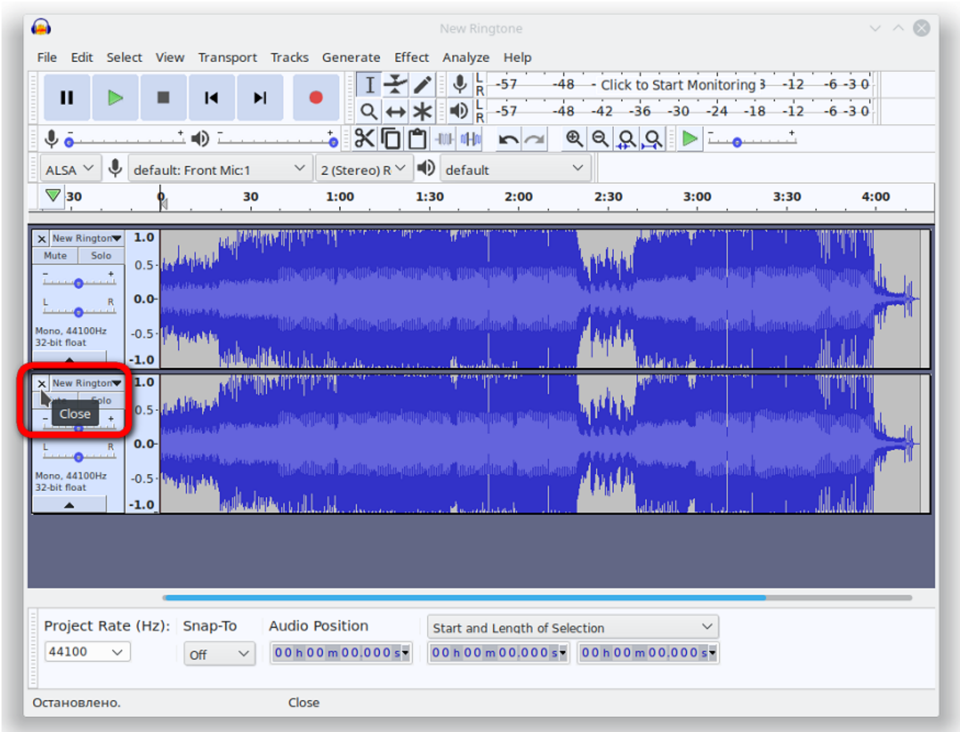
1. Add a file to the project.



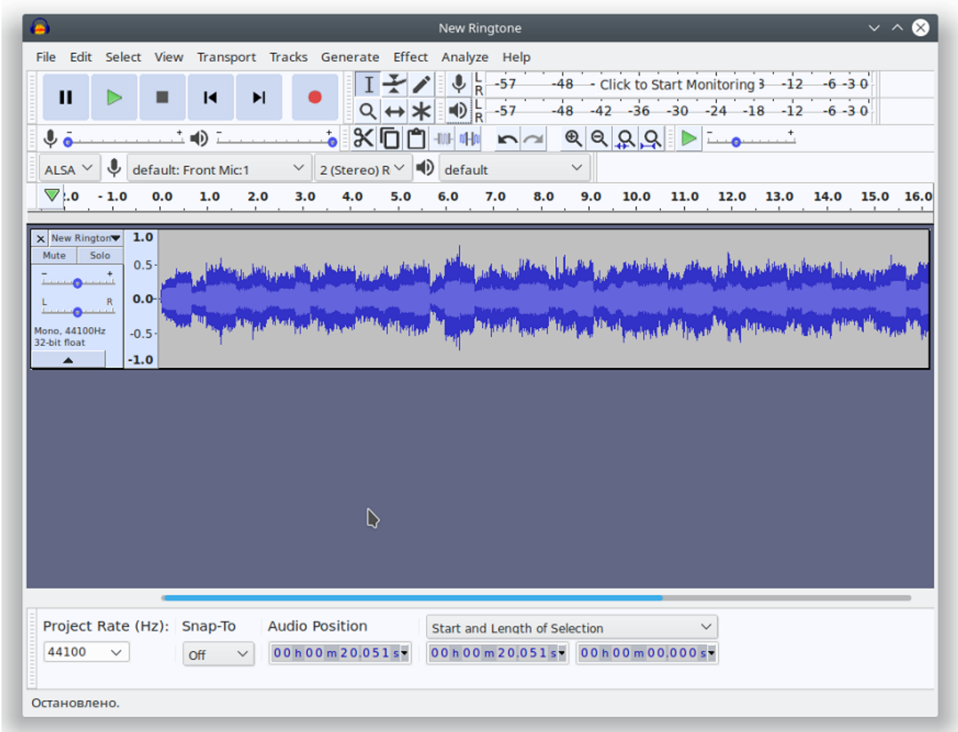
2. Split the track into two (transform it into to monotracks) — select 'Split Stereo to Mono' in the track management menu.



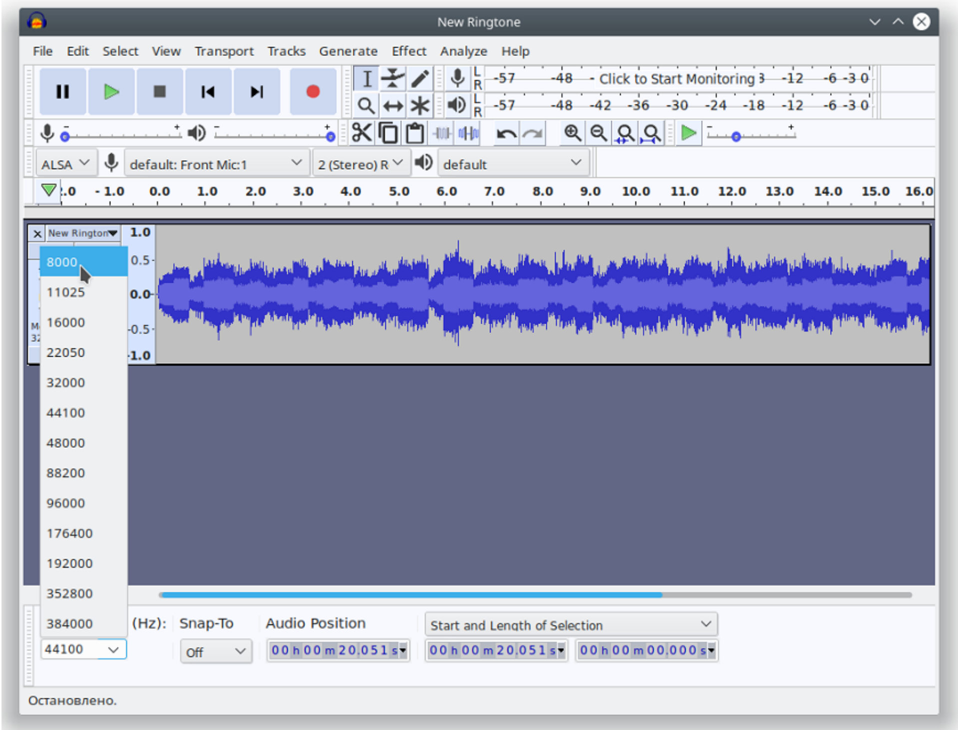
3. Close one of the tracks in the track management menu.



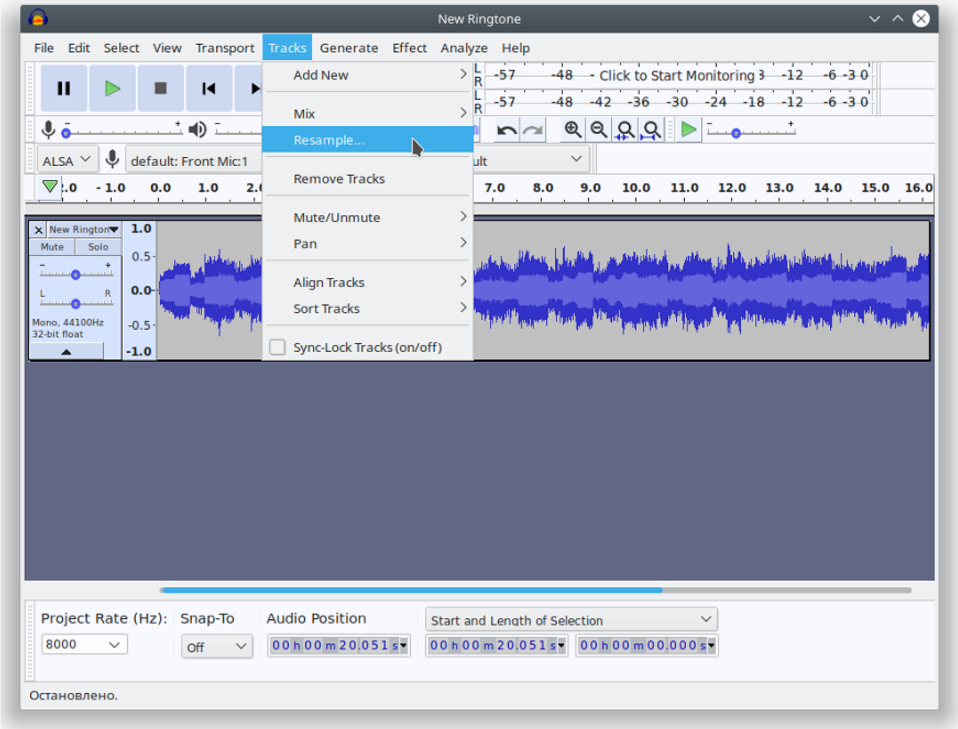
4. If necessary, cut the track to the needed length, you may aslo cut out repeated part. To do this, select unnecessary part and click 'Delete'.

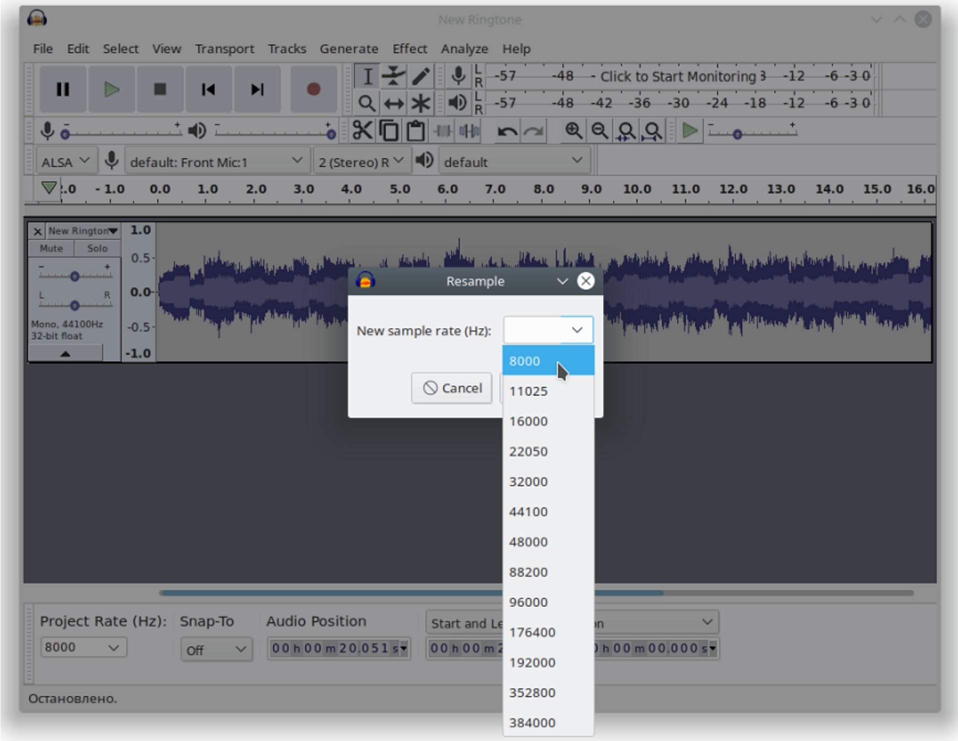


5. Change the project's sampling frequency to 8000 Hz at the bottom of the track management menu.

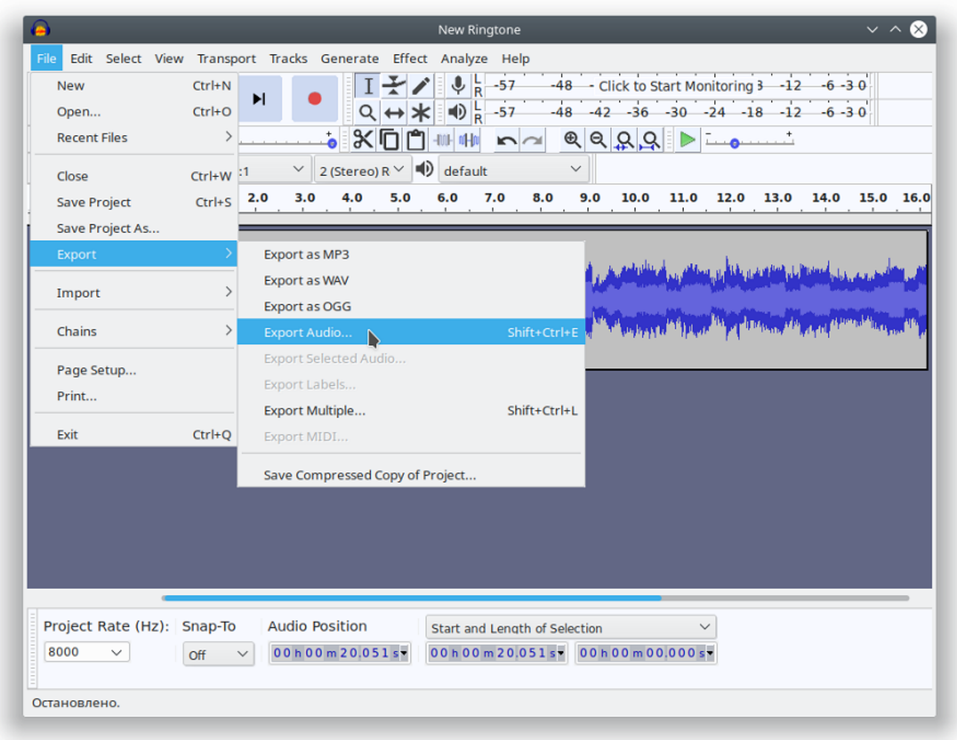


6. Change the track's sampling frequency in the 'Track' menu → 'Change track sampling rate...'.



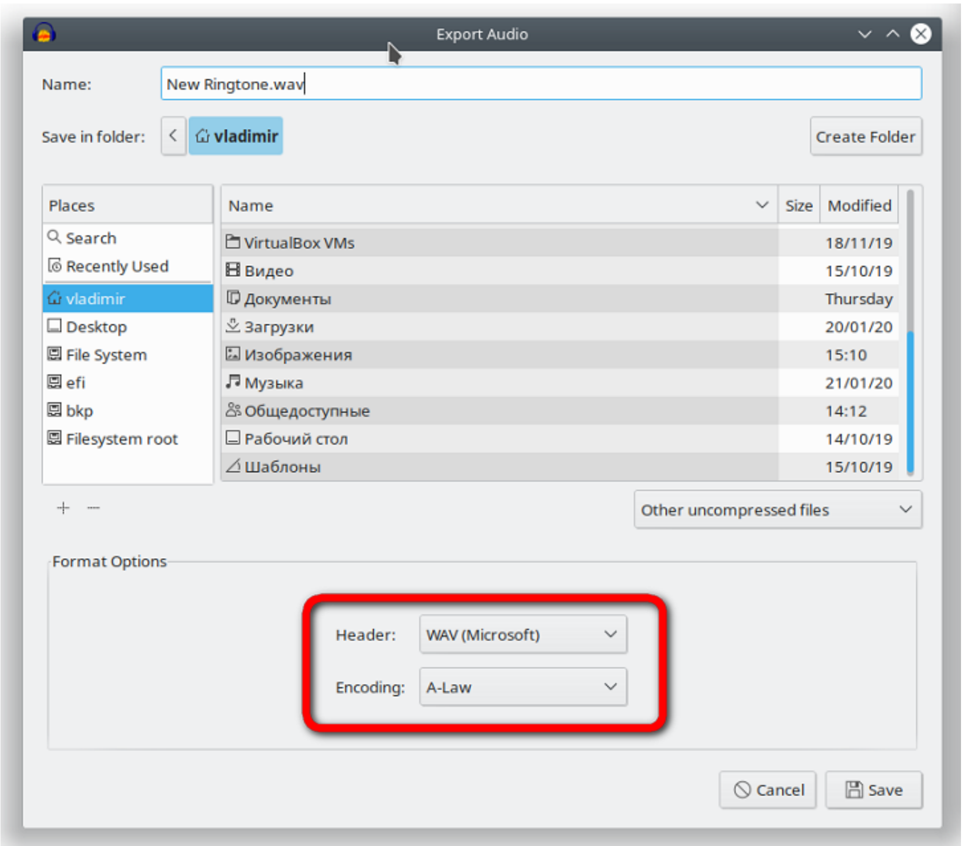


7. Export the audio file: 'File' → 'Export' → 'Export audio'.

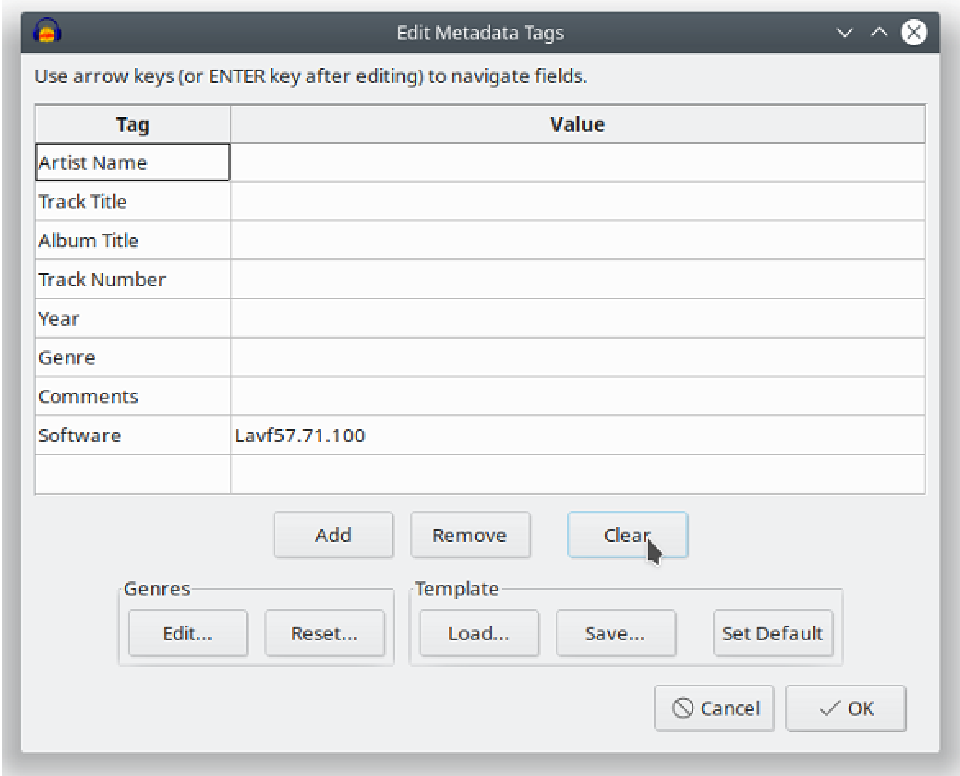


In the displayed window, set:

- Folder in the file system to storage the audio;
- File name;
- WAV title (Microsoft);
- Codec A-Law.



8. Delete tags and finish the export.



The file is ready to be uploaded as a ringtone.

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

https://eltex-co.com/support/

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist.

http://www.eltex-co.com/

http://www.eltex-co.com/support/downloads/