https://wiki.teltonika-networks.com/view/RUTX08_Administration

RUTX08 Administration

The information in this page is updated in accordance with firmware version **RUTX_R_00.07.04.5**.

□

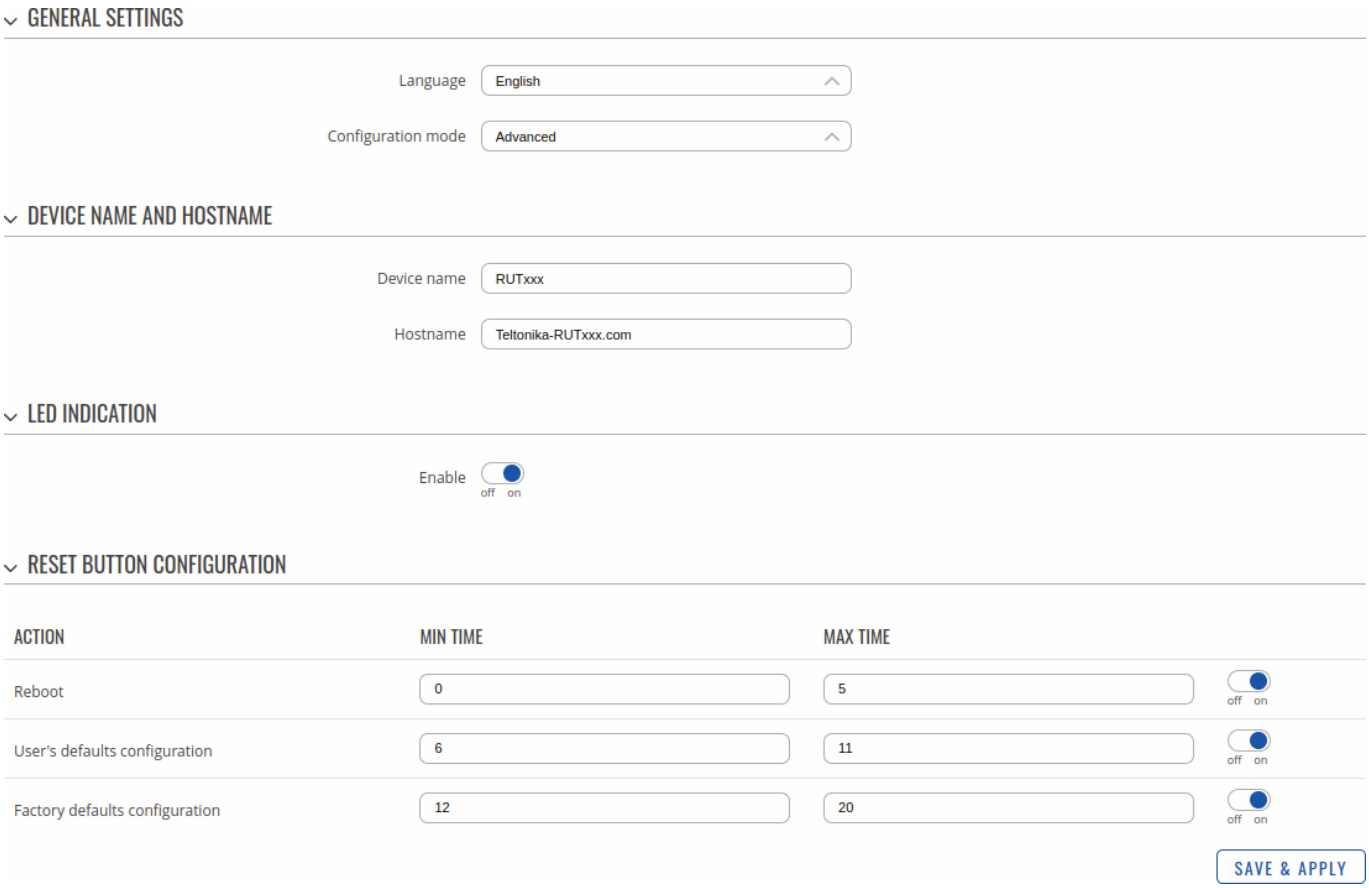
Contents

Summary

This page is an overview of the **Administration** section of RUTX08 devices.

General

The **General** section is used to set up some of device managerial parameters, such as changing device name. For more information on the General section, refer to figure and table below.



Field	Value	Description
General Settings		
Language	English | Turkish* | Spanish* | Portuguese* | German* | Japanese*; default: **English**	Changes the router's WebUI language.
Configuration Mode	Basic | Advanced; default: **Basic**	Mode determines what options and configurations are shown. In Basic mode only the essential configurations are shown. In Advanced mode there is greater freedom to configure and access more options.
Device name and hostname		
Device name	string; default: **RUTX08**	Device model name.
Hostname	string; default: **Teltonika-RUTX08.com**	Device hostname. This can be used for communication with other LAN hosts.
LED Indication		
Enable	off | on; default: **on**	Manages signal strength and connection status indication LEDs.
Reset Button Configuration		
Min time	integer [0..60]; default: **none**	Minimum time (in seconds) the button needs to be held to perform an action.
Max time	integer [1..60]; default: **none**	Maximum time (in seconds) the button can be held to perform an action, after which no action will be performed.

* Different language packages can be downloaded separately from the **Services → Package Manager** page.

Access Control

General

The **Access Control** page is used to manage remote and local access to device.

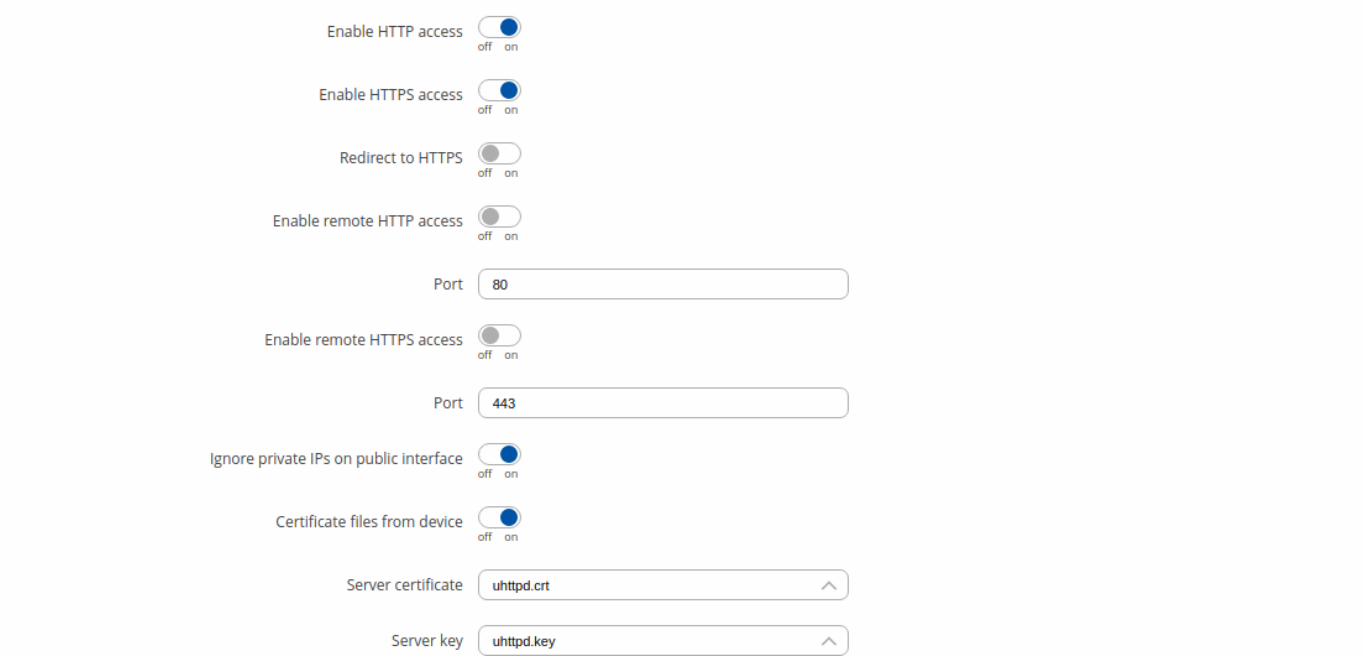
Important: turning on remote access leaves your device vulnerable to external attackers. Make sure you use a strong password.

SSH

Field	Value	Description
Enable SSH access	off | on; default: **on**	Turns SSH access from the local network (LAN) on or off.
Remote SSH access	off	
Port	integer [0..65535]; default: **22**	Selects which port to use for SSH access.
Enable key-based authentication	off | on; default: **off**	Use public keys for authentication.

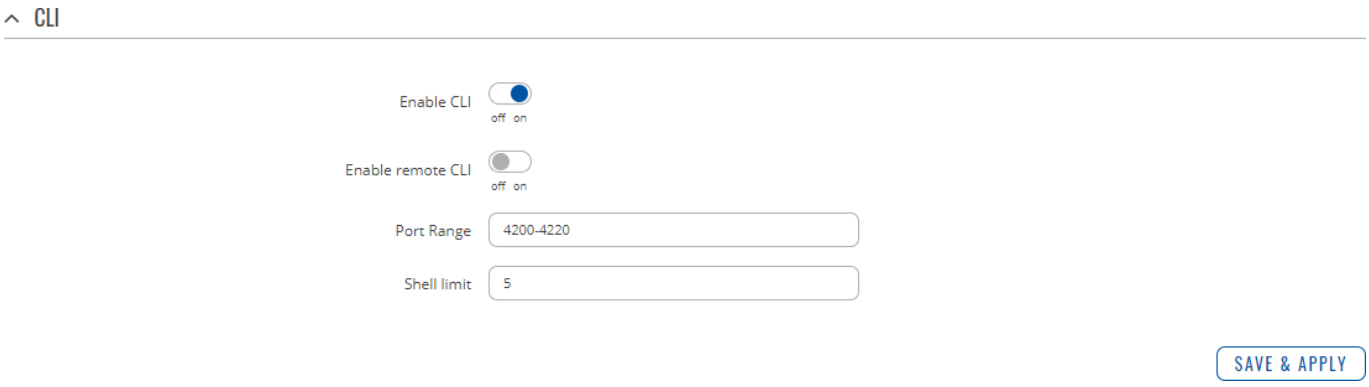
WebUI

WEBUI



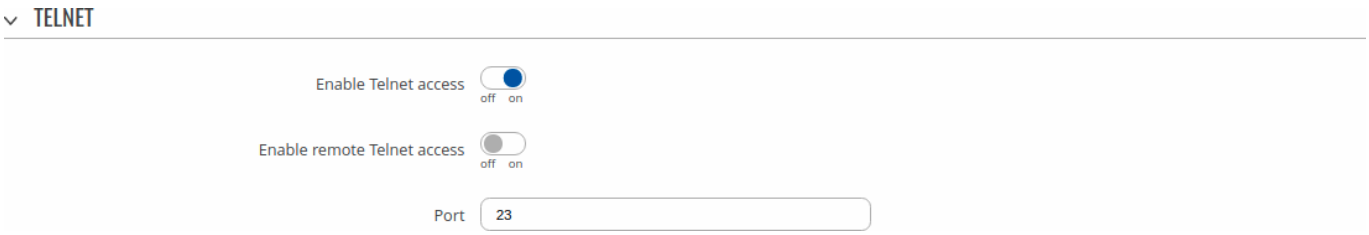
Field	Value	Description
Enable HTTP access	off | on; default: **on**	Turns HTTP access from the local network (LAN) to the device WebUI on or off.
Enable HTTPS access	off | on; default: **on**	Turns HTTPS access from the local network (LAN) to the device WebUI on or off.
Redirect to HTTPS	off | on; default: **off**	Redirects connection attempts from HTTP to HTTPS.
Enable remote HTTP access	off	
Port	integer [0..65535]; default: **80**	Selects which port to use for HTTP access.
Enable remote HTTPS access	off	
Port	integer [0..65535]; default: **443**	Selects which port to use for HTTPS access.
Ignore private IPs on public interface	off	
Certificate files from device	off	
Server certificate	.crt; default: **uhttpd.crt**	Server certificate file.
Server key	.key; default: **uhttpd.key**	Server key file.

CLI



Field	Value	Description
Enable CLI	off | on; default: **on**	Turns CLI access from the local network (LAN) on or off.
Enable remote CLI	off	
Port range	range of integers [0..65534]-[1..65535]; default: **4200-4220**	Selects which ports to use for CLI access.
Shell limit	integer [1..10]; default: **5**	Maximum number of active CLI connections.

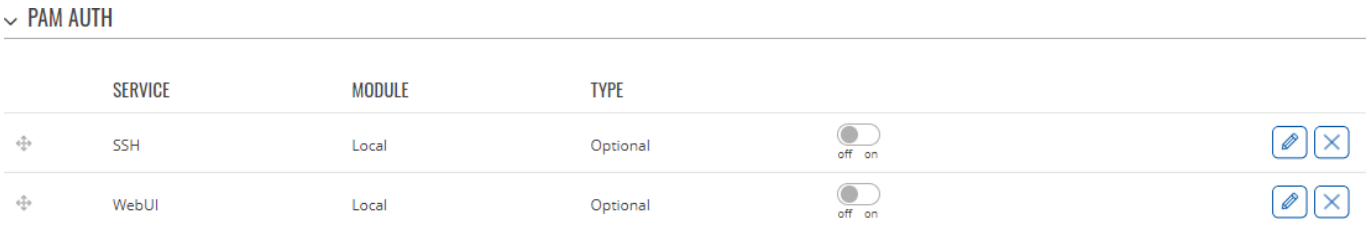
Telnet



Field	Value	Description
Enable Telnet access	off | on; default: **on**	Turns Telnet access from the local network (LAN) on or off.
Enable remote Telnet access	off | on; default: **off**	Turns Telnet access from remote networks (WAN) on or off.
Port range	integer [0..65535]; default: **23**	Selects which port to use for Telnet access.

PAM

Note: PAM is additional software that can be installed from the **Services → Package Manager** page.



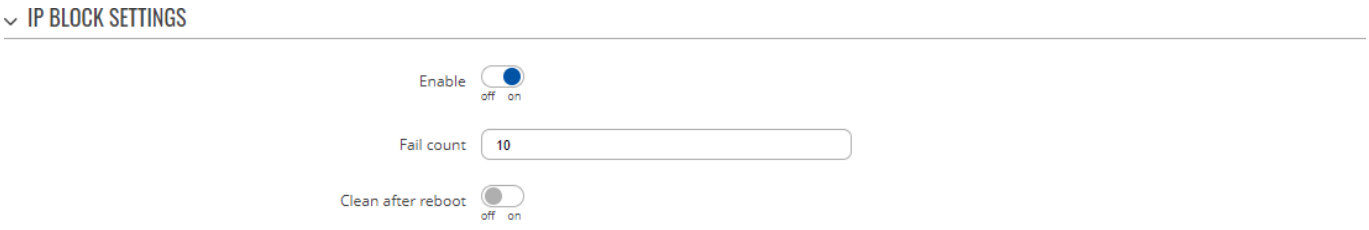
Modify PAM Auth

Field	Value	Description
Enable	off | on; default: **on**	Turns the PAM auth on or off.
Module	TACACS+ | Radius | Local; default: **Local**	Specifies the PAM module that implements the service.
Type	Required | Requisite | Sufficient | Optional; default: **Required**	Determines the continuation or failure behavior for the module
TACACS+/Radius: Server	ip4 | ip6; default: **none**	The IP address of the RADIUS server
TACACS+/Radius: Secret	string; default: **none**	RADIUS shared secret
Radius: Port	integer [0..65535]; default: **1812**	RADIUS server authentication port
Radius: Timeout	integer [3..10]; default: **3**	Timeout in seconds waiting for RADIUS server reply.

Security

The **Security** tab provides the possibility to enable/disable blocking IP's service and delete blocked devices from the list.

IP Block Settings



Field	Value	Description
Enable	off | on; default: **on**	Enable or disable blocking IP's if they have reached the set amount of failed times.
Fail count	integer [1..1000]; default: **10**	An amount of times IP address can try to access SSH or WebUI before being blocked.
Clean after reboot	off | on; default: **off**	If enabled, blocked loging attempts list will be cleared on device reboot.

Login Attempts

Field	Value	Description
Source address	IP address	Shows the IP address from which the connection failed.
Device port	Port number	Shows the port number from which the connection failed.
Destination address	IP address	Shows yours device IP adress
Protocol	Connection protocol	Displays the connection protocol used for connection.
Failed atempts	Number	Shows the number of failed attempts to connect to device.
Status	- | Blocked	Indicates whether the source address is blocked or not.
Reset	Check box	Allows you to select multiple IP addresses.
Unblock all	-(interactive button)	Unblocks all source adresses from the list.
Unblock selected	-(interactive button)	Unblocks selected source adresses from the list.

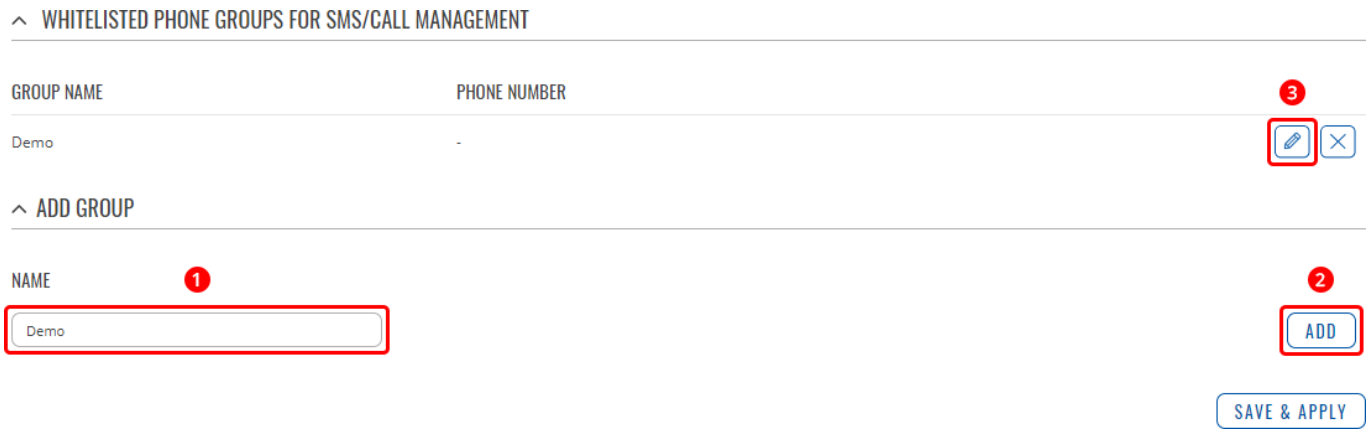
Recipients

The **Recipients** section is used to configure phone groups and email users, which can later be used along with SMS or email related services, such as Events Reporting.

Phone Groups

A **Phone Group** is a collection of phone numbers that can be used as the recipient in SMS & call related services instead of specifying every number individually. The phone group list is empty by default thus, you must first add at least one new group before you can add phone numbers to it. To create and begin editing a phone group, follow these steps:

1. Enter a custom name for the phone group into the 'Name' field.
2. Click the 'Add' button.
3. Click the 'Edit' button next to the newly added phone group.



After clicking 'Edit' you should be redirected to that phone group's configuration page where you can start adding phone numbers to it.

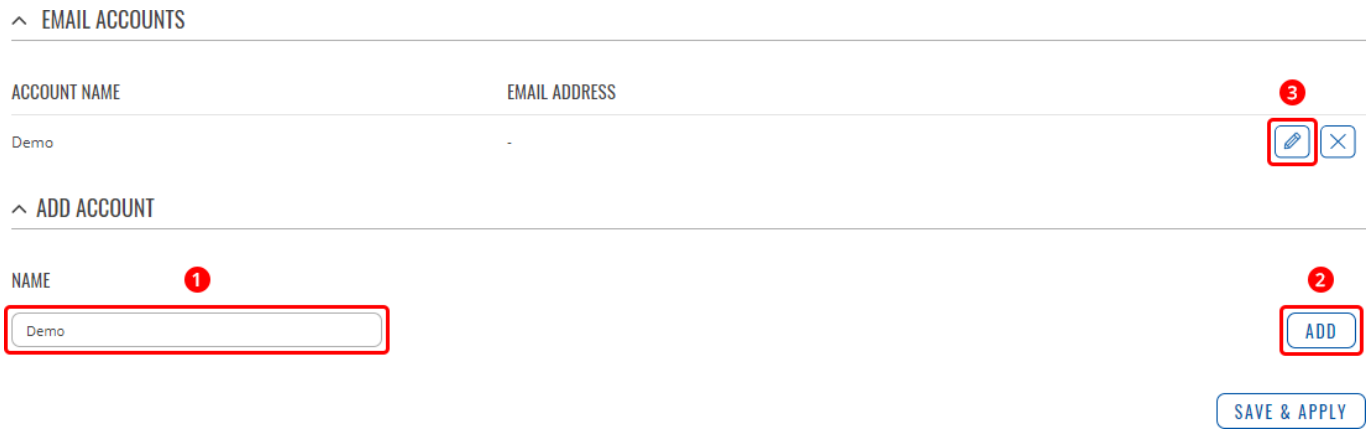
Field	Value	Description
Group name	string; default: **none**	Name of this phone numbers group.
Phone number	string; default: **none**	A phone number entry for this group. Numbers that consist of *0-9*+#* characters are accepted. Click the plus symbol to add more entries.

Email Accounts

When email related services (such as Events Reporting) are used, the device logs in to the specified email account and reads the inbox (e.g., Email to SMS) or sends out a message (e.g., SMS to Email) depending on the configured service. In this context, an **Email Account** is an configuration instance that contains the necessary data required in order to log into an email account.

The email accounts list is empty by default thus, you must first add at least one new account before you can configure it. To create and begin editing an email account, follow these steps:

1. Enter a custom name for the email account into the 'Name' field.
2. Click the 'Add' button.
3. Click the 'Edit' button next to the newly added email account.



After clicking 'Edit' you should be redirected to that email account's settings page where you can start configuring the account.

Field	Value	Description
Secure connection	off | on; default: **off**	Use if your SMTP server supports TLS or SSL encryption.
SMTP server	string; default: **none**	Name of the email service provider's SMTP server.
SMTP server port	integer [0..65535]; default: **none**	Port of the email service provider's SMTP server.
Credentials	off | on; default: **off**	This options allows you to set username and password of email account.
Username	string; default: **none**	Username used to authenticate to the email service.
Password	string; default: **none**	Password used to authenticate to the email service..
Sender's email address	string; default: **none**	Configured SMTP server user's email address.
Send test email	- (interactive button)	Sends an email based on the current configuration. This is used to test whether the configuration works as intended.

Certificates

The **Certificates** page is used for convenient TLS certificate and key generation and management. Generated files can be exported and used on other machines or locally on this device with functions that use TLS/SSL, such as MQTT, OpenVPN, IPsec and others.

Certificate Generation

The **Certificate Generation** tab provides the possibility to generate TLS certificates required for secure authentication and communication encryption used by some of the devices services.

There are five distinct generation methods (denoted by the selected 'File Type').

1. **Simple** - generates and signs a set of 2048 bit certificate and key files that include:

- Certificate Authority (CA)
- Server certificate & key
- Client certificate & key
- DH Parameters

The CA file generated with this option automatically signs the certificates. In short, this option is used for convenience as it doesn't let the user set any additional parameters for the certificate files. Therefore, it should be used only when no other specific requirements are expected.

2. **CA** - generates a Certificate Authority (CA) file. A CA is a type of certificate file that certifies the ownership of a public key by the named subject of the certificate. In other words, it assures clients that they are connecting to a trusted server and vice versa.
3. **Server** - generates a server certificate and key. A server certificate validates a server's identity to connecting clients, while a key is responsible for encryption.
4. **Client** - generates a client certificate and key. A client certificate validates a client's identity to the server that it's connecting to, while a key is responsible for encryption.
5. **DH Parameters** - generates a Diffie-Hellman (DH) parameters file. DH parameters are used in symmetric encryption to protect and define how OpenSSL key exchange is performed.

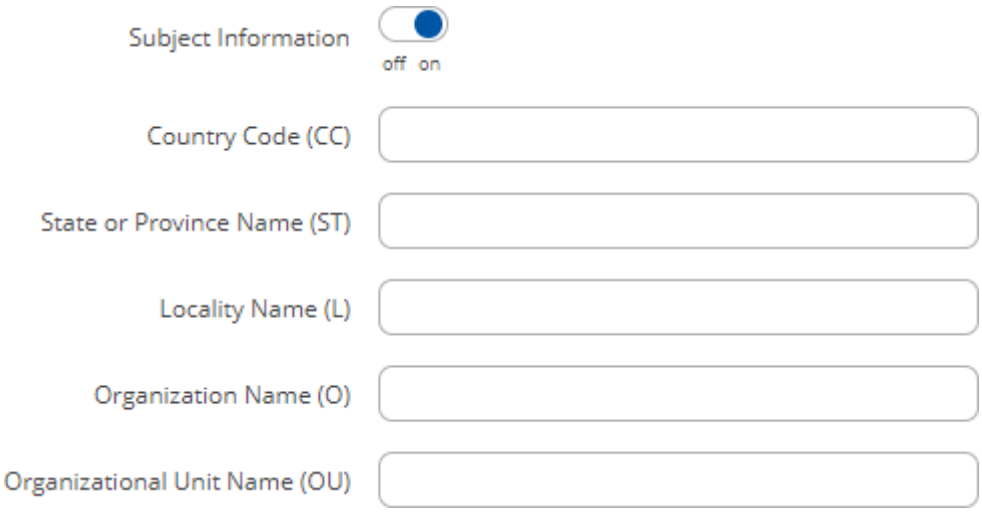
Generation Parameters

Generating each type of file (excluding 'Simple') requires setting some parameters. This section provides an overview for parameters used in TLS certificate generation.

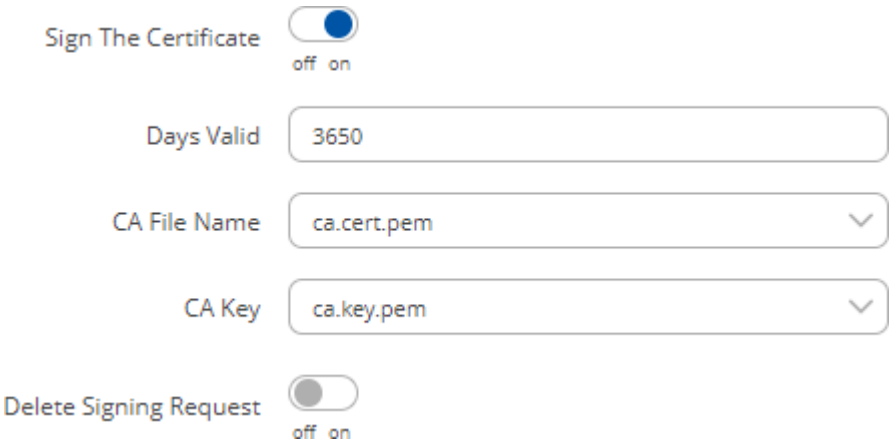
Core parameters or simply parameters that apply to each file type are the size and common name of the generated file(s).

Field	Value	Description
Key Size	integer; default: **2048**	Generated key size in bits. Larger keys provide more security but take longer to generate. A 2048 bit is the preferred option.
Name (CN)	string; default: **cert**	Common Name (CN), aka Fully Qualified Domain Name (FQDN) is a parameter that defines the name of the certificate. It should be chosen with care as it is not only used for easier management. For example, the Common Name should typically hostname of the server. It may also be used to differentiate clients in order to apply client-specific settings.

Subject information is not mandatory but can be used as user-friendly way to identify the ownership of certificate files by including such information as the owner's location and company name.



The **Sign the certificate** slider control whether the certificate will be signed automatically or manually after the generation is complete.

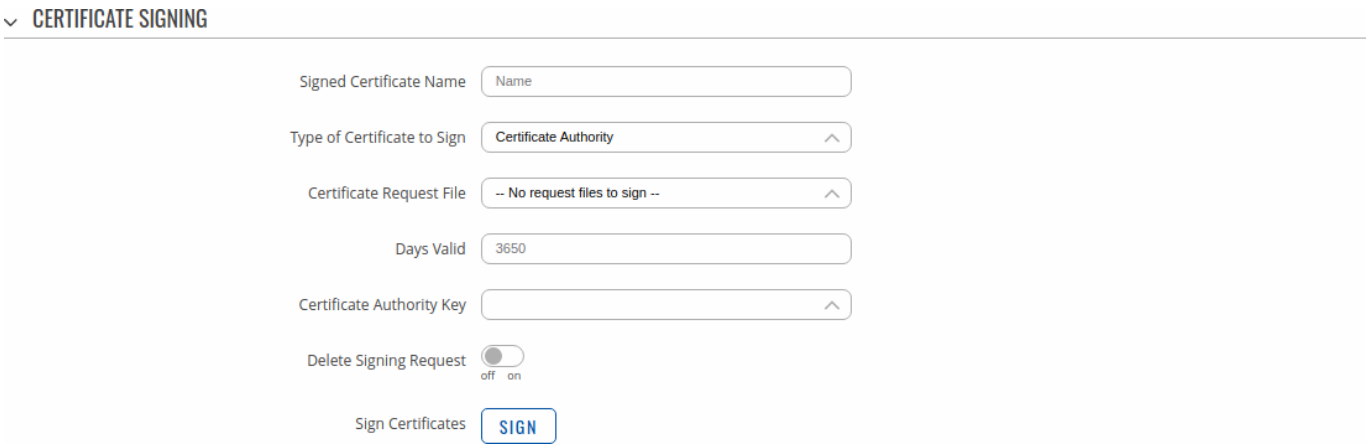


Field	Value	Description
Days Valid	integer; default: **3650**	Length of the signature's validity.
CA File Name	filename; default: **none**	Selects which CA file will be used to sign the generated certificate.
CA key	filename; default: **none**	Selects which CA key file will be used to sign the generated certificate.
Delete Signing Request	off | on; default: **off**	Generation creates additional 'signing request' files (which appear under the Certificate Manager tab) that are later used to sign the generated certificates. When this option is set to 'on', the device deletes the signing request files after the signing process is complete.

A **Private Key Decryption Password** is a parameter used to decrypt private keys protected by a password.

Certificate Signing

The **Certificate Signing** section is used to validate (sign) unsigned certificates.



Field	Value	Description
Signed Certificate Name	string; default: **none**	Name of the signed certificate.
Type of Certificate to Sign	Certificate Authority | Client Certificate | Server Certificate; default: **Certificate Authority**	Specifies what type of file will be signed.
Certificate Request File	file; default: **none**	Specifies the signing request file linked to the certificate.
Days Valid	integer; default: **none**	Length of the signature's validity.
Certificate Authority File	filename; default: **none**	Selects which CA file will be used to sign the generated certificate.
Certificate Authority Key	filename; default: **none**	Selects which CA key file will be used to sign the generated certificate.
Delete Signing Request	off | on; default: **off**	Generation creates additional 'signing request' files (which appear under the Certificate Manager tab) that are later used to sign the generated certificates. When this option is set to 'on', the device deletes the signing request files after the signing process is complete.
Sign	- (interactive button)	Signs the certificate on click.

Certificate Manager

The **Certificate Manager** page displays information on all certificate and key files stored on the device and provides the possibility export these files for use on another machine or import files

generated elsewhere.

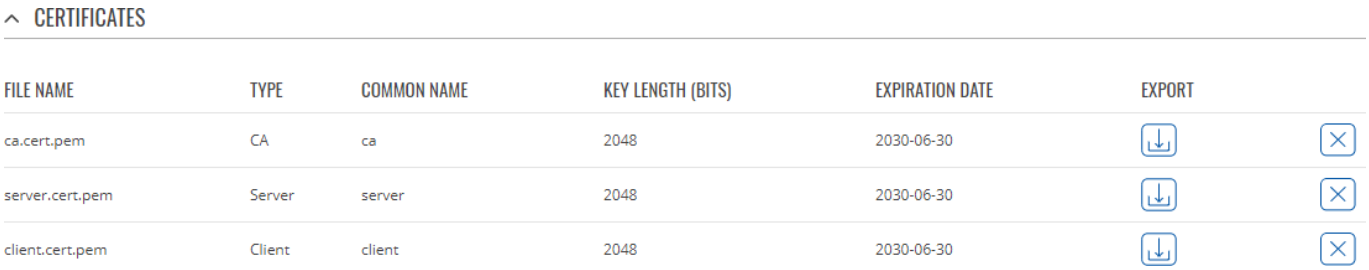
Certificate Import

The **Certificate Import** section provides the possibility to import certificates and files generated on another machine. To upload such a file simply click 'Browse' and locate the file on your computer, it should then start uploading automatically.

Certificates, Keys & Requests

The **Certificates**, **Keys** and Requests section display files generated on or imported to the device along with the most important information related to them.

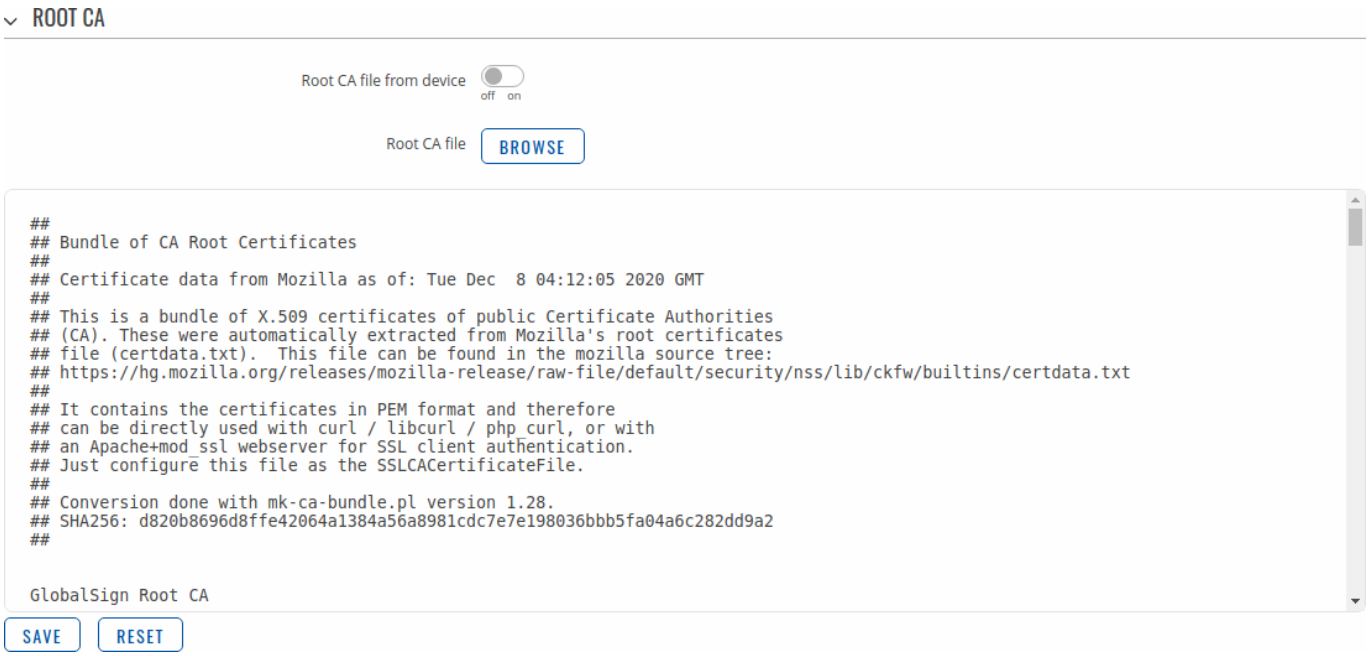
By default, the lists are empty. A set certificates generated using 'Simple' file type would look something like this:



The 'Export' buttons are used to download the files from the device onto your local machine. The 'X' buttons located to the right of each entry are used to delete related files.

Root CA

The **Root CA** section is used to add a root CA certificate file to the device. There is a default file already preloaded on the device which will be overwritten by any uploaded file. The certificates must be in .pem format, maximum file size is 300 KB. These certificates are only needed if you want to use HTTPS for your services and the default file should be sufficient in most cases.



Troubleshoot

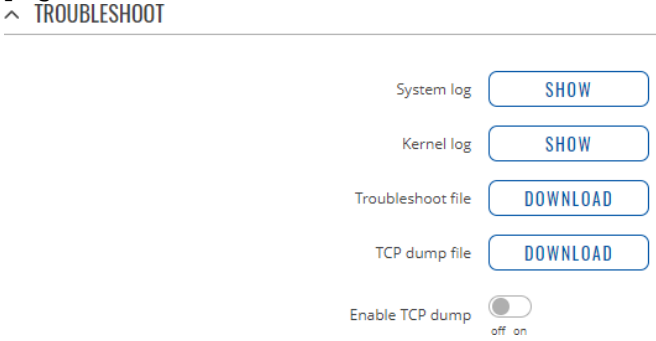
Logging Settings

The **Logging Settings** section is used to configure how and where the device stores system log data. The system log is a file that contains information on various system related events and is useful to engineers for troubleshooting the device.

Field	Value	Description
System log buffer size	integer; default: **128**	System log buffer size in kibibytes (KiB).
External system log server	ip; default: **none**	IP address of an external server that will be used to store device logs.
External system log server port	integer [0..65535]; default: **none**	TCP/UDP port number of the external log server.
External system log server protocol	UDP | TCP; default: **UDP**	Communication protocol used by the external log server.
Save log in	RAM memory | Flash memory; default: **RAM memory**	Specifies which type of memory to use for storing system logs.
System log file size	integer [10..500]; default: **200**	Maximum size (in kilobytes) of a log file. When threshold is reached, log rotation is performed. Can be set to value from 10kB to 500kB. Smaller the file, larger amount of old logs is saved.
Compress	off | on; default: **off**	Compress old rotated logs using GZ format.
Delete	- (interactive button)	Deletes log file from router.
Show hostname	off | on; default: **off**	Show hostname instead of IP address in syslog.

Troubleshoot

The **Troubleshoot** section is used to download various files that contain information used for troubleshooting the device. Refer to the figure and table below for information on the Troubleshoot page.

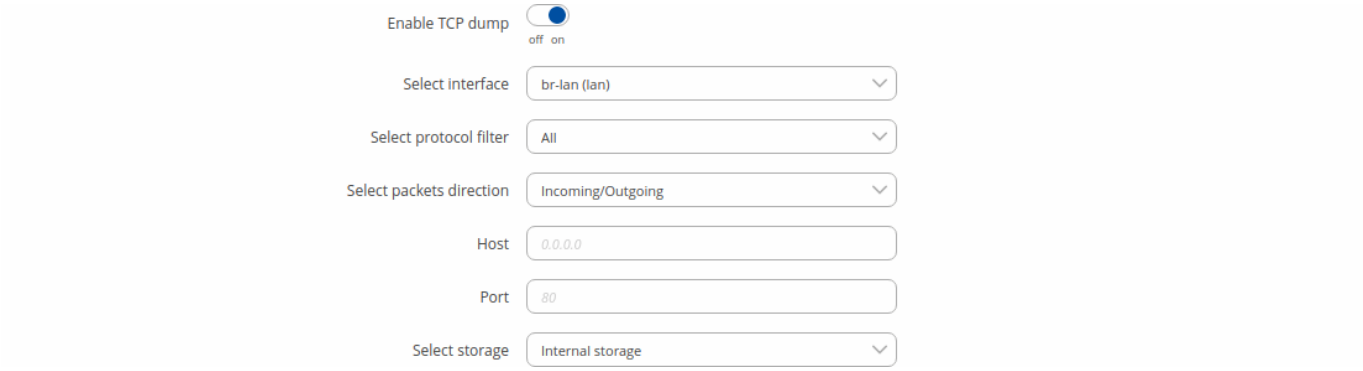


Field	Value	Description
System log	- (interactive button)	Displays the contents of the device system log file. The system log contains records of various system related events, such as starts/stops of various services, errors, reboots, etc.
Kernel log	- (interactive button)	Displays the contents of the device kernel log file. The kernel log contains records of various events related to the processes of the operating system (OS).
Troubleshoot file	- (interactive button)	Downloads the device Troubleshoot file. It contains the device configuration information, logs and some other files. When requesting support, it is recommended to always provide the device Troubleshoot file to Teltonika engineers for analysis.
TCP dump file	- (interactive button)	Downloads the device TCP dump file. TCP dump is a program used to capture packets moving through network interfaces. By default, the device does not store TCP dump information. You must enable TCP dump and save the changes before you can download the file.
Enable TCP dump	off	

TCP dump

TCP dump is used to capture packets moving through network interfaces. By default, the device does not store TCP dump information. You must enable TCP dump and save the changes before you can download the file.

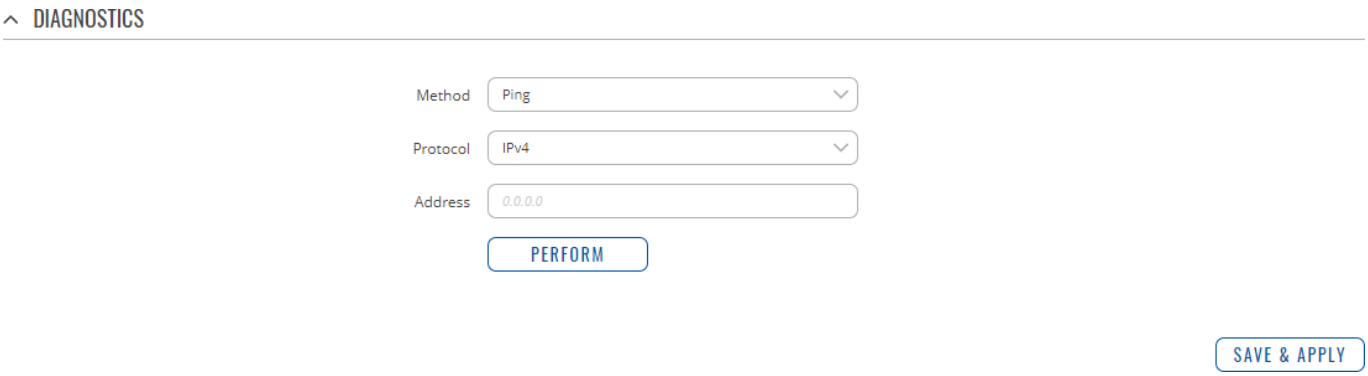
If you enable TCP dump, you will notice additional configuration fields appear. Refer to the figure and table below for realted information.



Field	Value	Description
Enable TCP dump	off | on; default: **off**	Turns TCP dump packet capture on or off.
Select interface	network interface; default: **br-lan**	Only captures packets that move through the specified network interface.
Select protocol filter	All | ICMP | TCP | UDP | ARP; default: **All**	Only captures packets that match the specified protocol.
Select packets direction	Incoming/Outgoing | Incoming | Outgoing; default: **Incoming/Outgoing**	Only captures packets coming from the specified direction.
Host	ip | host; default: **none**	Only captures packets related to the specified host.
Port	integer [0..65335]; default: **none**	Only captures packets related to the specified communication port.
Select storage	RAM memory; default: **RAM memory**	Specifies where the TCP dump file will be stored.

Diagnostics

The **Diagnostics** section is used to execute simple network diagnostic tests, including *ping*, *traceroute* and *nslookup*.



Field	Value	Description
Method	Ping | Traceroute | Nslookup; default: **Ping**	Selects diagnostic method. • **Ping** - sends ICMP requests to the specified address. • **Traceroute** - displays the path that packets have to take in order to reach the specified address. • **Nslookup** - obtains domain name address and IP address mapping information.

Protocol IPv4 | IPv6; default: **IPv4**	Selects IP address family for diagnostic test.
Address ip | host; default: **none**	IP address or hostname on which the diagnostic test will be performed.
Perform -(interactive button)	Performs diagnostic test when clicked.