https://wiki.teltonika-networks.com/view/RUT850_Administration

RUT850 Administration

Main Page > RUT Routers > RUT850 > RUT850 Manual > RUT850 WebUI > RUT850 Services section > **RUT850 Administration**
□

Contents

Summary

This page is an overview of the **Administration** section of RUT850 routers.

The information in this page is updated in accordance with the **RUT850_R_00.01.03.4** firmware version.

General

The **General** section is used to set up some of the router's managerial parameters, such as password, name, language, etc. For more information on the General section, refer to figure and table below.

Field	Value	Description
Router name	string; default: **RUT850**	The router's model name.
Host name	string; default: **Teltonika-RUT850.com**	The router's hostname. This can be used instead of the IP address to reach the router's WebUI from the local network.
New password	string; default: **none**	A new password for the router. The password must be comprised of 8-32 characters, including at least one upper case letter, one lower case letter and one digit.

Confirm new password	string; default: **none**	Repeat the new password for confirmation. (Must match the password entered in the "New password" field.)
Language	English | Deutsch | Français | Turkish; default: **English**	Selects the router's WebUI language.
Enable sleep mode*	yes | no; default: **no**	Turns sleep mode on or off.
Show mobile info at login page	yes | no; default: **no**	Shows mobile data connection information (signal strength, state, service mode) at login page.
Show WAN IP at login page	yes | no; default: **no**	Shows the router's WAN IP address at login page.
LEDs Indication	yes | no; default: **yes**	Turns the router's LED indications on or off.
Restore to default	-(interactive button)	Restores the router to it's default state (factory settings).

* more information on sleep mode in the next section.

Sleep mode

Sleep mode is a function that automatically puts the rotuer into standby mode after a user specified delay.

Field	Value	Description
Enable sleep mode	yes | no; default: **no**	Turns sleep mode on or off.
Sleep delay	5 min. | 10 min. | 15 min. | 30 min.; default: **5 min.**	A delay after which the router will enter sleep mode. The delay begins countdown after the sleep mode condition is met.
Sleep condition	Ignition | Votlage | Ignition & Voltage; default: **Ignition & Voltage**	Specifies which type of condition will make the router enter sleep mode.
Set minimum voltage	voltage [0..49,5]; default: **11.75**	Voltage under which sleep conditions are considered to be met.

Troubleshoot

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

Field	Value	Description

System log level	Debug | Info | Notice | Warning | Error | Critical | Alert | Emergency; default: **debug**	Specifies the information output level of the system log. • **Debug** - contains basic information that is diagnostically helpful to most people (i.e., not just engineers). • **Info** - general useful information (e.g., configuration changes, starts and stops of services, etc.) • **Notice** - conditions that are not error conditions, but that may require special handling. • **Warning** - anything that can potentially cause application oddities, but for which the system is automatically recovering from (e.g., retrying an operation, missing secondary data, etc.) • **Error** - errors that are fatal to the operation, but not the service or application (can't open a required file, missing data, etc.) Solving these types of errors will usually require user intervention. • **Critical** - critical conditions, device errors. • **Alert** - a condition that must be corrected immediately. • **Emergency** - a panic condition, i.e., system is no longer usable.
Save log in	RAM memory | Flash memory; default: **RAM memory**	Specifies which type of memory to use for storing system logs.
Include GSMD information	yes | no; default: **yes**	When checked, includes the router's GSMD information in the log file.
Include PPPD information	yes | no; default: **no**	When checked, includes the router's PPPD information in the log file.
Include chat script information	yes | no; default: **yes**	When checked, includes the router's chat script information in log file.
Include network topology information	yes | no; default: **no**	When checked, includes the router's network topology information in the log file.
System log	- (interactive button)	Displays the contents of the router's 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 router's 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 router's Troubleshoot file. It contains the router's configuration information, logs and some other files. When requesting support, it is recommended to always provide the router's Troubleshoot file to Teltonika engineers for analysis.

Backup

The **Backup** page is used to download or upload configuration backup files to the router. Backup files can be uploaded only from identical devices with identical. Once a backup file is uploaded to a router, that router will have identical configuration as the router from which the backup file originated (was downloaded from).

- **Backup Configuration** - generates and downloads the router's backup file based on the current configuration.
- **Restore Configuration** - uploads a configuration backup file to the router. This can be done in two ways:
  - **Upgrade from file** - uploads a configuration file from your computer.
  - **Upgrade from FOTA** - uploads a configuration file assigned to the device in FOTA.

Important: backup files can be uploaded only when taken from a device with an identical **Product code** (can be checked in **Status → Device**) and identical firmware.

Access Control

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

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

General

The **General** section is used to manage SSH, HTTP(S) and CLI access to the router.

SSH

Field	Value	Description
Enable SSH access	yes | no; default: **yes**	Turns SSH access from the local network (LAN) on or off.
Remote SSH access	yes | no; default: **no**	Turns SSH access from remote networks (WAN) on or off.
Port	integer [0..65535]; default: **22**	Selects which port to use for SSH access.

WebUI

Field	Value	Description
Enable HTTP access	yes | no; default: **yes**	Turns HTTP access from the local network (LAN) to the router's WebUI on or off.
Redirect to HTTPS	yes | no; default: **no**	Redirects connection attempts from HTTP to HTTPS.

Enable remote HTTP access	yes | no; default: **no**	Turns HTTP access from remote networks (WAN) to the router's WebUI on or off.
Port	integer [0..65535]; default: **80**	Selects which port to use for HTTP access.
Enable remote HTTPS access	yes | no; default: **no**	Turns HTTPS access from remote networks (WAN) to the router's WebUI on or off.
Port	integer [0..65535]; default: **443**	Selects which port to use for HTTPS access.
RFC1918 Filter	yes | no; default: **yes**	Turns Address Allocation for Private Internets on or off.

Safety

The **Safety** section is used to manage the *List Of Blocked Addresses*. After a user attempts to login to this devices via SSH/HTTP, he will have a limited amount of retries in case of unsuccessful login attempts. This limit is called *Fail count* and is set in this page. After the user exhausts the maximum number of attempts, his IP address will be blocked from making more attempts and added to the *List Of Blocked Addresses*.

Block Unwanted Access

Field	Value	Description
Enable	yes | no; default: **yes**	Turns secure SSH/HTTP access on or off. If this is checked, devices logging in have a limited amount of tries specified in the *Fail count* field to log in to the router via SSH/HTTP.
Clean after reboot	yes | no; default: **no**	If this field is checked, addresses are removed from the *List Of Blocked Addresses* after every router reboot.
Fail count	integer; default: **5**	Maximum login fail count after which the device's address is blocked and addedd to the *List Of Blocked Addresses*.

List Of Blocked Addresses

The screenshot above is of a list that contains one blocked address. If you or someone you know gets blocked accidentally, you can unblock users from this section by deleting their IP address from the list.

Note: the list gets cleared after a factory reset.

Diagnostics

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

Enter an address in the *Host* field and execute one of the following actions:

- **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.

Overview

The **Overview** section is used to select which widgets should be visible in the Status → Overview page.

Simply select the widgets that you would like to view in the Overview page and click the 'Save' button.

RMS

RMS (**Remote Management System**) is a cloud system designed by Teltonika and intended for remote monitoring and management of Teltonika-Networks products.

In order to add a device(s) to RMS, get yourself acquainted by watching this instructional video and register an account by clicking here. **Each unique device receives a free month-long RMS license** when added to RMS for the first time.

The figure below is a screenshot of the RMS section taken from a device which has been connected to RMS:

Field	Value	Description
Connection type	Enabled | Standby | Disabled; default: **Enabled**	Defines how the device will connect to RMS: • **Enabled** - the device attempts to connect to RMS every 2-5 minutes (every 2 minutes the first hour; then every 5 minutes). If it cannot connect for 14 days, it will enter Standby mode. • **Standby** - the device attempts to connect to RMS every 6 hours. • **Disabled** - RMS functionality is disabled.
Hostname	host | ip; default: **rms.teltonika.lt**	Address of the RMS server. If you're using regular RMS, just leave the default address (*rms.teltonika.lt*).
Port	integer [0..65535]; default: **15009**	Port number for connecting to RMS. If you're using regular RMS, just leave the default port (*15009*).

The RMS server waits for incoming connections. Since the device attempts to connect at a fixed interval, it may not connect instantly after you add it to RMS. While it is disconnected, you can check how much time is left until the next connection attempt in the Status section:

To speed up the process by initiating an immediate connection attempt, click the 'Connect' button.

For more information on Teltonika's Remote Management System (RMS) refer to the **RMS Manual** or **RMS FAQ** pages.

Root CA

The **Root CA** section is used to add a root CA certificate file to the router. 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.