

Template:Networking tswos manual maintenance

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



Contents

- [1 Summary](#)
- [2 Auto Reboot](#)
 - [2.1 Summary](#)
 - [2.2 Ping/Wget Reboot](#)
 - [2.3 Reboot Scheduler](#)
- [3 Backup](#)
 - [3.1 Summary](#)
 - [3.2 Create default configuration](#)
 - [3.3 Backup configuration](#)
 - [3.4 Restore configuration](#)
 - [3.4.1 Backup Security Check](#)
 - [3.5 Restore default settings](#)
- [4 Troubleshoot](#)
 - [4.1 Logging Settings](#)
 - [4.2 Troubleshoot](#)
 - [4.2.1 TCP dump](#)
- [5 Events Log](#)
 - [5.1 Summary](#)
 - [5.2 All Events](#)
 - [5.3 General Events](#)
 - [5.4 System Events](#)
 - [5.5 Network Events](#)
 - [5.6 Connections Events](#)
- [6 CLI](#)
 - [6.1 Summary](#)
 - [6.2 CLI](#)

Summary

This page is an overview of the **Maintenance** section of {{{name}}} devices.

Auto Reboot

Summary

Various automatic device reboot scenarios can be configured in the **Auto Reboot** section. Automatic reboots can be used as a prophylactic or precautionary measure that ensures the device will self-correct some unexpected issues, especially related to connection downtime.

This chapter is an overview of the Auto Reboot section of {{{name}}} devices.

Ping/Wget Reboot

The **Ping/Wget Reboot** functions periodically send ICMP or Wget requests to a specified IP address or host and waits for a response. If no response is received, the device will attempt the same action a defined number of times at a defined frequency. If there is still no response, the device will execute the specified action (reboot, by default).

The Ping/Wget Reboot section contains one pre-configured rule by default:



To enable the default rule, use the off/on slider next to it. You can add more rules with the 'Add' button or delete them using the 'Delete' button. If you wish to customize a rule, click the button that looks like a pencil next to it.



Field	Value	Description
Enable	off on; default: off	Turns the rule on or off.
Type	Ping Wget ; default: Ping	Method used for health checking. • Ping - sends ICMP requests to the specified host. • Wget - retrieves the contents of the specified web server.
Action if no echo is received	Device reboot None; default: Device reboot	Action that will be executed if there is no response after the specified amount of retries. If None is selected, only a message to syslog will be logged.
Interval	5 mins 15 mins 30 mins 1 hour 2 hours; default: 5 mins	The frequency at which ping/Wget requests are sent to the specified host.
Interval count	integer [1..9999]; default: 2	Indicates how many additional times the device will try sending requests if the initial one fails.
Timeout (sec)	integer [1..9999]; default: 5	Maximum response time. If no echo is received after the amount of time specified in this field has passed, the ping/wget request is considered to have failed.
URL	url; default: none	URL to which the wget requests will be sent. E.g. http://www.host.com
Packet size	integer [0..1000]; default: 56	ICMP packet size in bytes.
Interface	Automatically selected; default: Automatically selected	Specifies through which interface the pings will be sent. If Automatically selected is set, the pings will go through the main WAN interface.
IP type	IPv4 IPv6; default: IPv4	IP address version of the host to ping.

Host to ping host | ip; default: **8.8.8.8**

Hostname or IP address to which the Ping/Wget requests will be sent.

Reboot Scheduler

The **Reboot Scheduler** is a function that reboots the device at a specified time interval regardless of other circumstances. It can be used as a prophylactic measure, for example, to reboot the device once at the end of every day.

You can add more rules with the 'Add' button or delete them using the 'Delete' button. If you wish to customize a rule, click the button that looks like a pencil next to it.



The figure below is an example of the Periodic Reboot configuration page and the table below provides information on the fields contained in that page:



Field	Value	Description
Enable	off on; default: off	Turns the rule on or off.
Interval type	Week days Month days; default: Week days	Scheduler instance interval type.
Week days	Monday Tuesday Wednesday Thursday Friday Saturday Sunday; default: Monday	Week day(s) when actions will be executed. This field becomes visible when Interval type is set to Week days.
Month day	integer [1..31]; default: 1	Day of the month on which the reboot will occur. This field becomes visible when Interval type is set to Month days.
Month	month(s) [january..december]; default: none	The month(s) on which the reboot will occur. Leave empty to apply to all months. This field becomes visible when Interval type is set to Month days.
Day time	time [00:00..23:59]; default: none	Exact time of day the reboot will take place
Force last day	off on; default: off	Forces intervals to accept last day of month as a valid option if selected day doesn't exist in the ongoing month. This field becomes visible when Interval type is set to Month days.

Backup

Summary

The **Backup** page is used to generate configuration backup files or upload existing ones to the device. This chapter is an overview of the Backup page in {{{name}}} devices.

Create default configuration

The **Create default configuration** section is used to create or delete a file which stores current device configuration. The default configuration can later be loaded in `[[{{{name}}}]_Maintenance#Backup|Backup]]` page or via reset button.

Click the 'Create' button to generate default configuration file from your current device configuration.



Backup configuration

The **Backup configuration** section is used to generate and download a file which stores the current device configuration. The backup file can later be uploaded to the same device or another device of the same type (product codes must match).

This section contains MD5, SHA256 checksum fields generated from latest downloaded backup file, 'Download' button to generate and download the device configuration backup file.



Restore configuration

The **Restore configuration** section is used to upload a configuration file that was taken from this device or another device of the same type.

Click the 'Browse' button to select a backup file from your computer and click the 'Upload archive' button to apply the selected configuration on to this device.



Important notes:

- Backup files can be uploaded only if they are taken from an identical device (identical Product code (can be checked in the Status → `[[{{{name}}}] System|System]]` page)) with identical or older firmware.
- It is important to remember that the backup file not only changes the device configuration, but also the password. If you are unsure of the backup file's password, you may want to reconsider uploading it because you may lose access to device.

Backup Security Check

After uploading a backup file your device will calculate checksums for uploaded file and display them. If this backup file was the latest downloaded in your device then you can compare these

checksums with the ones in your [Backup configuration](#) section to verify backup's integrity.

If everything is in order click **Proceed** to restore configuration to backup.



Restore default settings

The **Restore default settings** section is used for restoring device's configuration.



Field	Value	Description
Restore to factory defaults	-(interactive button)	Restores device to manufacturer's default settings.
Restore to user's defaults*	-(interactive button)	Restores device to custom configuration set by the user.

* You will not see this button until you have created a `[[{{{name}}}_Maintenance#Create_default_configuration|User's default configuration]]`.

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 on; default: off	Turns TCP dump packets capture on or 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: Any	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.

Events Log

Summary

The **Events Log** page contains information on various device related events. This article is an overview of the Events Log page for {{{name}}} routers.

All Events

The **All Events** page contains a chronological list of various events related to the device. The figure below is an example of the Events Log section:



General Events

The **General Events** page contains a chronological list of general events related to the device. The figure below is an example of the Events Log section:



System Events

The **System Events** page contains a chronological list of system events related to the device. The figure below is an example of the Events Log section:



Network Events

The **Network Events** page contains a chronological list of network events related to the device. The figure below is an example of the Events Log section:



Connections Events

The **Connections Events** page contains a chronological list of connections events related to the device. The figure below is an example of the Events Log section:



CLI

Summary

The **CLI** or **Command-line interface** functionality allows you to enter and execute Linux commands within the device. This manual page provides an overview of the CLI page in {{{name}}} devices.

CLI

The RutOS **CLI** is a console interface similar to the Linux Terminal program. Use the following credentials to log in:

- Username: root
- Password: device's password

If the login was successful, you should be greeted with a window similar to this:



[[Category:{{{name}}} System section]]