Vodafone MachineLink

Watchdogs Configuration Guide

Document History

This guide covers the following products:

- Vodafone MachineLink 3G (NWL-10)
- Vodafone MachineLink 3G Plus (NWL-12)
- Vodafone MachineLink 4G (NWL-22)

Ver.	Document Description	Date
v. 1.0	Initial document release.	March 2013
v. 2.0	Revised content based on current firmware.	September 2016

Table i - Document revision history

Note – Before performing the instructions in this guide, please ensure that you have the latest firmware version installed on your router.

Visit http://vodafone.netcommwireless.com to download the latest firmware.

Note – The functions described in this document require that the router is assigned with a publicly routable IP address.

Please ensure that your mobile carrier has provided you with a publicly routable IP address before performing the instructions in this document.

Copyright

Note – This document is subject to change without notice.

Contents

Notation

The following symbols are used in this user guide:

⚠ The following note requires attention.

⚡ The following note provides a warning.

ℹ The following note provides useful information.

Introduction

The Vodafone MachineLink includes multiple layers of watchdogs to ensure that you always have a way to access your devices remotely in the case that the unit is not physically accessible.

There are multiple layers of hardware and software watchdogs which all work in conjunction to provide a reliable and stable service. The user configurable watchdog features on the unit are the Ping watchdog and SMS diagnostics.

Internal watchdogs

Hardware watchdog

The CPU has an independent process with a counter which starts at 15 seconds and counts down to 0. If the counter ever reaches zero it will perform a reboot of the device.

When the system powers up, the boot loader executes code before the Linux kernel starts, sending a signal to reset the counter to 15. This avoids the possibility of the system becoming stuck in boot loader mode. The Linux kernel then boots and sets the counter to 2 seconds and sends a signal to reset the counter every second. This means if the kernel ever crashes (panics) it will be detected in 2 seconds and the system will reboot. After the kernel has loaded the user space loads and sends the signal to the kernel to reset the timer. If the kernel does not receive the signal it will perform the reboot.

If the system ever reboots the kernel messages will show whether it was caused by the watchdog, reset via hardware button or a power cycle.

Software watchdog

Phone module

The device’s phone module produces a heartbeat (signal) which is received by the kernel from the CNS port connected to the module and writes a variable into the RDB manager. If this variable is not written, the kernel will detect if the module is not responding and perform a power cycle on the module.

Connection manager

There is a connection manager which monitors the WAN connection. It detects if there is an active PDP session and reconnects if the device is rebooted.

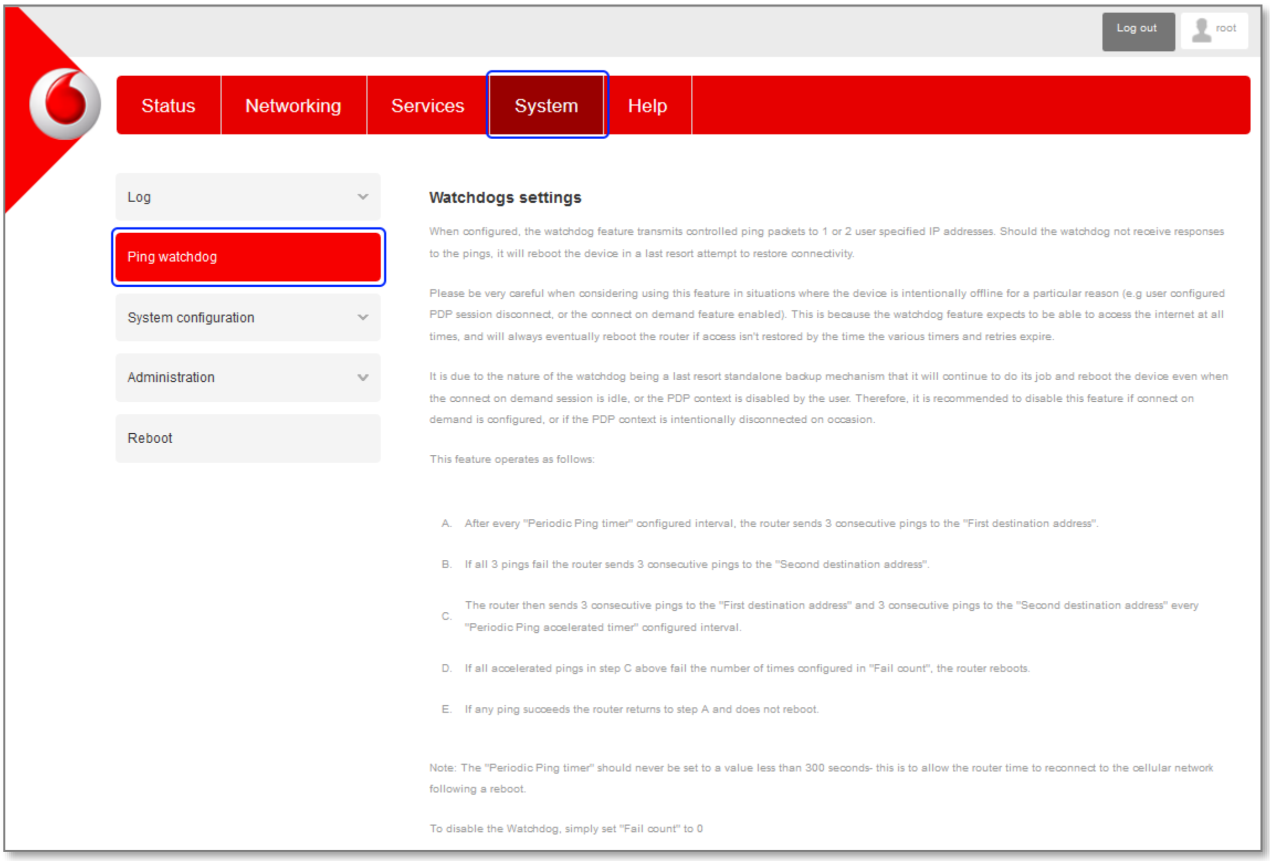
User-configurable watchdogs

Ping watchdog

The ping watchdog is a “keep alive” feature on top of the internal watchdogs. This detects cases where the device has a PDP session but no traffic can be passed through the connection. This situation may occur on the network from time to time. If the ping fails based on the prescribed conditions, the unit will reboot which will allow it to re-establish a valid data connection.

The Ping watchdog configuration page contains a detailed description of how it works. To access the Ping watchdog configuration screen:

Click **System** in the taskbar at the top, then click **Ping watchdog** from its menu on the left.



Watchdogs settings

When configured, the watchdog feature transmits controlled ping packets to 1 or 2 user specified IP addresses. Should the watchdog not receive responses to the pings, it will reboot the device in a last resort attempt to restore connectivity.

Please be very careful when considering using this feature in situations where the device is intentionally offline for a particular reason (e.g user configured PDP session disconnect, or the connect on demand feature enabled). This is because the watchdog feature expects to be able to access the internet at all times, and will always eventually reboot the router if access isn't restored by the time the various timers and retries expire.

It is due to the nature of the watchdog being a last resort standalone backup mechanism that it will continue to do its job and reboot the device even when the connect on demand session is idle, or the PDP context is disabled by the user. Therefore, it is recommended to disable this feature if connect on demand is configured, or if the PDP context is intentionally disconnected on occasion.

This feature operates as follows:

A. After every "Periodic Ping timer" configured interval, the router sends 3 consecutive pings to the "First destination address".

B. If all 3 pings fail the router sends 3 consecutive pings to the "Second destination address".

C. The router then sends 3 consecutive pings to the "First destination address" and 3 consecutive pings to the "Second destination address" every "Periodic Ping accelerated timer" configured interval.

D. If all accelerated pings in step C above fail the number of times configured in "Fail count", the router reboots.

E. If any ping succeeds the router returns to step A and does not reboot.

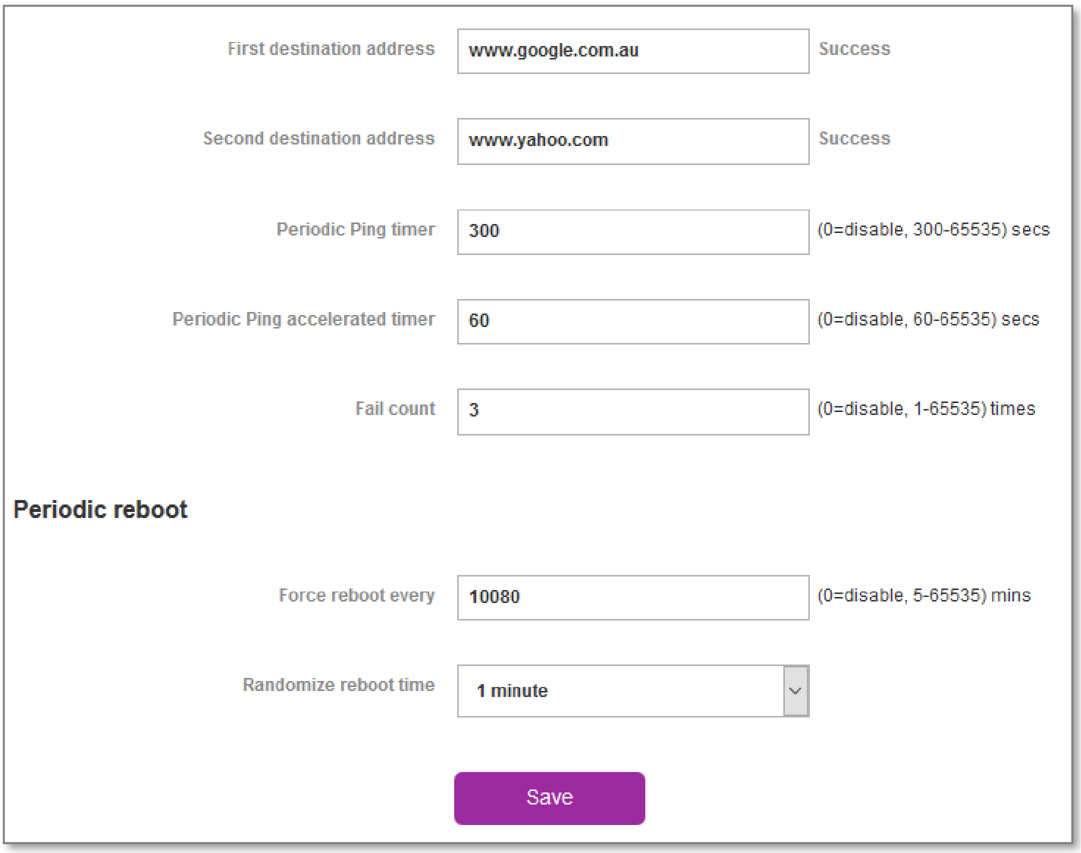
Note: The "Periodic Ping timer" should never be set to a value less than 300 seconds- this is to allow the router time to reconnect to the cellular network following a reboot.

To disable the Watchdog, simply set "Fail count" to 0

Figure 1 – Watchdog settings page

Example watchdog settings

Below is an example configuration of the ping watchdog.



First destination address	www.google.com.au	Success
Second destination address	www.yahoo.com	Success
Periodic Ping timer	300	(0=disable, 300-65535) secs
Periodic Ping accelerated timer	60	(0=disable, 60-65535) secs
Fail count	3	(0=disable, 1-65535) times

Periodic reboot

Force reboot every	10080	(0=disable, 5-65535) mins
Randomize reboot time	1 minute	

Figure 2 – Example Watchdog settings

Note that the above settings are only valid if the device has a connection to the internet. If there is no internet connection, specify IP addresses on the WAN side of the router.

In the above configuration the unit will ping the destination address 3 times every 300 seconds, if they fail it pings the second address 3 times every 300 seconds. If this ping fails, the unit will use the Periodic PING Accelerated Timer and ping every 60 seconds. If the Periodic PING Accelerated Timer ping fails it will be recorded as a failure. After 3 failures the unit performs a software reboot.

For additional information on the Ping watchdog, please refer to the user manual

SMS diagnostics

The SMS feature allows diagnostics and control over the unit by sending an SMS to the SIM card. This allows 3 types of functions.

- **GET** – Retrieve system information e.g. DHCP settings, APN, signal strength, Cell ID
- **SET** – Setting system values e.g. DHCP settings, APN, IP address
- **EXECUTE** – Execute scripts or commands e.g. rebooting the device, enable/disable data connection

In the scenario where the device is unreachable over the packet switched network (3G), it is still possible to reboot the unit via an SMS or perform diagnostic commands. In most scenarios, the device will always be registered to the SGSN. Having this feature enabled allows additional options to access the device.

The SMS diagnostics feature is enabled by default. When using a Vodafone GDSP SIM card with your router, you must use the GDSP web interface to send and receive the SMS messages as the router is pre-configured with security settings to accept SMS messages from the GDSP platform. If using a generic SIM card with your router, the messages must be formatted according to the API.

Here are some examples of SMS diagnostics messages:

Description	Authentication	Input Example
Send SMS to change APN	Not required	set apn1=internet set apn2="access"
	Required	PASSWORD set apn1=internet PASSWORD set apn2=access
Send SMS to change the 3G username	Not required	set username="NetComm"
	Required	PASSWORD set username="NetComm"
Send SMS to check the 3G signal strength	Not required	get rssi
	Required	PASSWORD get rssi
Send SMS to connect the 3G connection	Not required	execute pdpup
	Required	PASSWORD execute pdpup1

Table 3 – Example SMS diagnostic messages

For more SMS diagnostics examples, refer to the Vodafone MachineLink User Guide.