

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## WeOS 5.29.0 Release Notes

### Contents

1	Summary of Changes . . . . .	5
1.1	News in 5.29.0 . . . . .	5
1.1.1	Linux Kernel 6.12 . . . . .	5
1.1.2	System Information - Added CPU Architecture . . . . .	5
1.1.3	Logging . . . . .	5
1.1.4	Logging - FQDN . . . . .	5
1.1.5	DNS . . . . .	6
1.1.6	Interface - ARP Watch . . . . .	6
1.1.7	SNMP . . . . .	6
1.1.8	Gratuitous ARP Improvements . . . . .	7
1.1.9	Policy Filtering - Updated Counter Behaviour . . . . .	7
1.1.10	Boot Configuration Improvements . . . . .	7
2	Fixed Issues . . . . .	8
2.1	WeOS 5.29.0 . . . . .	8
3	Known Limitations . . . . .	10
3.1	Ring Coupling version 2 not supported . . . . .	10
3.2	Port Access Control . . . . .	10
3.3	RMON . . . . .	10
3.4	Login . . . . .	10
3.5	Setting Date Manually . . . . .	11
3.6	Available ports for boot specific functionality . . . . .	11
3.7	Routing Hardware Offloading . . . . .	11
3.8	Redundancy protocols on Relay ports . . . . .	12
3.9	FRNT . . . . .	12
3.10	RSTP . . . . .	12
3.11	IEC 61375 . . . . .	12
3.12	Custom TRDP telegrams . . . . .	13
3.13	LLDP . . . . .	13

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

3.14	Port Monitoring . . . . .	14
3.14.1	Cross switch core limitation . . . . .	14
3.15	Media Redundancy Protocol (MRP) . . . . .	14
3.16	10G SFP Ports . . . . .	14
3.17	Search function in User Guide . . . . .	15
3.18	RedBox PTP Boundary Clock . . . . .	15
3.19	Ingress rate limiting . . . . .	15
3.20	Static unicast MAC filters for link aggregates . . . . .	15
4	Known Issues . . . . .	16
4.1	List of known issues . . . . .	16
4.2	#20888 & #20868 Redfox and Lynx 5000 1Gbps SFP issues . . . . .	19
4.3	#18163: Work-around for OSPF NSSAs convergence issue . . . . .	19
5	Quick Start Guide . . . . .	21
5.1	Default User and Password . . . . .	21
5.2	General . . . . .	21
5.3	CLI . . . . .	22
6	Firmware Upgrade . . . . .	24
6.1	WeOS Image . . . . .	24
6.2	Boot Loader . . . . .	25
7	Significant differences between WeOS 4 and WeOS 5 . . . . .	26



Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## Legal Information

The contents of this document are provided “as is”. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy and reliability or contents of this document. Westermo reserves the right to revise this document or withdraw it at any time without prior notice. Under no circumstances shall Westermo be responsible for any loss of data or income or any special, incidental, and consequential or indirect damages howsoever caused.

More information about Westermo at <http://www.westermo.com>

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## Important User Information

This section details important user information, directed in particular to new users of WeOS 5:

For help with getting started using WeOS 5, refer to the Quick Start Guide in section 5.

### User Guide

In WeOS 5, the primary user documentation is referred to as the *WeOS 5 User Guide*. Compared to the *WeOS 4 Management Guide*, the User Guide is a web first publication focusing on use-cases, documented in stand-alone “HowTo:s”, and configuration guides for all supported sub-systems.

The User Guide is included in the release Zip file in the sub-directory: `doc/weos/user-guide/`. To access the documentation, open the following file in your web browser:

`file://Downloads/WeOS-5.29.0/doc/weos/user-guide/index.html`

The *User Guide* is also available online at <https://docs.westermo.com/weos/weos-5/>.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 1 Summary of Changes

This section details new features added in this minor release.

Users new to WeOS 5 are recommended to read section 7 carefully, as it highlights some of the major differences between WeOS 4 and WeOS 5.

### 1.1 News in 5.29.0

The subsection below describe news in WeOS 5.29. In addition, section 2.1 includes information on fixed issues.

#### 1.1.1 Linux Kernel 6.12

This release of WeOS includes an upgrade of the Linux kernel from 5.17 to 6.12, a modern LTS release of the kernel that also includes functionality to support our upcoming hardware platforms. With the new kernel, our Viper family of products now run a 64-bit version of WeOS.

#### 1.1.2 System Information - Added CPU Architecture

Added CPU Architecture to system information in CLI and WEB. The mapping from product family to CPU Architecture is shown below.

Platform	Family	CPU Architecture
Dagger	Lynx 5000	ARMv7
Dagger	RedFox 5000	ARMv7
Envoy	Lynx 3000	ARMv8
Coronet	Viper 3000	PowerPC
Byron	Lynx RB	ARMv5

#### 1.1.3 Logging

Added new configuration option for Remote Log Sources called `use-local-timestamp`. When enabled, all log messages received for that remote source will have their timestamp replaced with the device's local timestamp at the time of reception. By default this option is disabled, preserving the existing behavior of using the timestamp provided by the sender.

For more information see the WeOS User Guide section *Configuration Guides* → *Logging* → *Source Configuration* → *Source Remote Specific* .

#### 1.1.4 Logging - FQDN

The system can now be configured to identify itself using a Fully Qualified Domain Name (FQDN) instead of the hostname when storing log messages locally, and/or sending log messages to a remote log

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

server. This is controlled by the new configuration option `identification` in the WeOS Logging configuration. By default, this option is set to "hostname", and the system will use the hostname as it did previously.

The FQDN is constructed from the statically configured `hostname` and `domain` values, both of which are located in the `system` configuration section. If the `domain` value is not configured, the system will fall back to using the hostname as the identification string, even if the FQDN option is enabled.

## 1.1.5 DNS

The WeOS DNS subsystem has been updated, along with the underlying infrastructure, to support the use of a statically configured domain. While these changes should be transparent to the user, they should result in a more robust and correct DNS implementation.

For more information see the WeOS User Guide sections *Configuration Guides → System Settings* and *Configuration Guides → DNS*.

## 1.1.6 Interface - ARP Watch

Some additions have been made to the existing ARP Watch functionality that can be enabled or disabled on an interface. Currently, this is a simple enable/disable that will log a number of selected events to the system audit log.

This configuration has been extended to allow selection of which specific events to report; this also includes support for a number of additional events that were not previously available for reporting.

Further, the ARP Watch functionality now also supports reporting detected events as SNMP notifications (traps/informs). Both of the currently available reporting methods can be individually enabled or disabled.

For more information see the WeOS User Guide section *Configuration Guides → Interface → Configuration*.

See the MIB file *WESTERMO-ARPIFNO-MIB.my* for more information on the available SNMP notifications.

## 1.1.7 SNMP

Support for specifying destination ports for SNMP trap host configurations has been added, by allowing the port to be provided as part of the trap host address, e.g. `192.168.1.1:1620`. If no port is specified, the default SNMP trap port (162) will be used, same as the current behavior.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 1.1.8 Gratuitous ARP Improvements

Improvements have been made to the handling of gratuitous ARP. Gratuitous ARP frames should now, if enabled (default is enabled) on an interface, be sent in the following cases:

- When an interface comes up. Note that if the interface is a VLAN interface, the first underlying device to come up will trigger the sending of gratuitous ARP frames for the VLAN interface. Therefore, when any subsequent underlying device comes up, it will not trigger additional gratuitous ARP frames for the VLAN interface.
- When the IP address of an interface changes, due to manual configuration changes.
- When an IP address is dynamically assigned to an interface, e.g. via DHCP.
- If the MAC address is reconfigured on an interface.

These adjustments should also resolve some known issues with gratuitous ARP, such as issue #20040.

## 1.1.9 Policy Filtering - Updated Counter Behaviour

In previous versions of WeOS, Policy Filtering only provided packet and byte counters for rules configured with the Accept action. To enable consistent visibility across all action types (Accept, Drop, and Trap) the counter implementation has been updated. As part of this change, the “number of bytes” metric has been removed, and counters now report packet counts only.

## 1.1.10 Boot Configuration Improvements

A *factory* option has been added to the *config-order* and *config-fallback* settings under the boot context. When the system boots using the *factory* option, it will load the factory default configuration, *factory-config*.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 2 Fixed Issues

### 2.1 WeOS 5.29.0

Fixed issues in WeOS 5.29.0 (as relative to 5.28).

Issue	Category	Description
#21186	TCN	Etbnnd memory corruption when consist information is used
#21181	System	Disabling Metrics while HTTPS is disabled generates invalid boot configuration
#21169	Port Access Control	Port-access can not handel Tag in Tunnel-Private-ID for Mac-auth
#21155	WEB	If HTTP is disabled there is sometimes a hidden "0" as port number, making it impossible to save configuration in web
#21129	General	SCEP: interop issue with EJBCA server when SAN is present in the enrollment request
#21118	TCN	etbnnd spam log with timeout entries in some systems running custom TRDP data
#21108	VPN	tunnel.ssl: pki labels (cert, cacert) have broader restrictions than JSON schema
#21092	General	Corruption in the pkcs11 backend (sqlite) for TPM based units
#21038	System	Metrics not showing correct values on Viper 3000 and Lynx 3000
#21015	TCN	If ECSP-ADDR is undefined (auto) then ETBND fails to start
#20973	NTP	Missing some documented NTP log messages
#20964	WEB	Session timeout does not work when using multiple browser tabs
#20953	System	Sending DSCP priority packets from cpu will use Lowest Priority queue (0)
#20935	System	Ingress rate limiting unknown unicast also limits known unicast when routing
#20933	MRP	Device allows configuration of MRP with other incompatible L2 redundancy protocols (e.g. RSTP, FRNT, RiCO)
#20909	Policy	Trap counter in Policy Filtering does not work
#20881	Alarm	Ping alarm peer has bad input validation.
#20831	AAA	IPSec ESP cipher authentication value does not match the CLI/config settings
#20822	Alarm	Configuring RING alarms from WEB results in wrong acvtive mode (condition)
#20733	Firewall	Port forwarding can not handle other protocols than TCP and UDP
#20703	VLAN	Incorrect ARP requests sent when bridging LAGs on Redfox and Lynx 5000
Continued on next page		

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

Continued from previous page		
Issue	Category	Description
#20571	System	Active SSH sessions not closed when a config restore is done via WEB allowing password manipulation in file afterwards
#20102	SNMP	SNMP value for frntStatusVid1/2 show no data in tables
#20040	Any	When IP address is changed from CLI, a gratuitous ARP is send with the old IP instead of new one
#19957	General	Port statistics not available on Redfox and Lynx 5000
#19818	SNMP	Syntax errors in Westermo MIB files for FRNT and EVENT
#19749	VLAN	Able to have policy nest active on a tagged port
#19181	Ports	Port-Priority-mode IP and Offloading broken with DSCP set field
#18967	System	Joins on SSL ports does not lead to the CPU port being added to the ATU

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 3 Known Limitations

This section describes known limitations in WeOS.

### 3.1 Ring Coupling version 2 not supported

Support for FRNT Ring Coupling (RiCo) version 2 was removed in 5.15.0 due to problems with the stability of the function. Most of the use cases for RiCo version 2 can be covered today through the use of FRNTv2 and RiCo v3.

For information around FRNT v2 and RiCo v3 usage please contact local Westermo support.

### 3.2 Port Access Control (IEEE 802.1X and MAC Authentication)

Wake-on-LAN is currently not possible on controlled ports. The reason is that broadcast traffic is not allowed to egress a controlled port until there is at least one MAC address authenticated on the port.

### 3.3 RMON

Some Hardware platforms are unable to provide certain RMON counters due to problems with the hardware chipset.

- RCV Error counter does not work on Viper 3512 and 3520
- FC Received (rx\_pause) does not work on Lynx 5000 and Redfox

### 3.4 Login

Known limitations related to the Login service.

#### Side-effect of disabling console login

When disabling login from console, login via telnet is also prohibited (even when telnet login is enabled).

#### SSH Public Key Lost When Disabling Built-in User

WeOS 5.13.0 introduces support for importing SSH public key for built-in users, as well as the ability to enable/disable a user. When disabling a user, the intention is that the user shall be prohibited from logging in, while other user configuration is till kept in the configuration file.

However, the disabling of a user currently implies that any SSH public key associated with the user is removed and needs to be imported again upon enabling the user.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

### 3.5 Setting Date Manually

Setting a manual date on the WeOS unit before 1 January 2000 will render an error message.

### 3.6 Available ports for boot specific functionality

The boot loader rescue mode only supports regular copper ports, not SFP ports. On RedFox-5528, ports 1-4 are also not supported until the system has booted.

### 3.7 Routing Hardware Offloading

The routing Hardware Offloading support for Viper-TBN introduced in WeOS 5.8 has shown to have instabilities. In particular, when used with dynamic routing, there are issues not yet solved. Therefore hardware offloading has temporarily been Disabled by default.

```
viper:/#> configure
viper:/config/#> ip
viper:/config/ip/#> offload
viper:/config/ip/#> leave
```

When Offloading is Enabled, regular IPv4 forwarding is handled in hardware with some exceptions, see the WeOS 5 User Manual for details (section 'Configuration Guides'/'Routing'/'Offloading').

For Redfox and Lynx-5000 initial Offloading support in 5.23.0. Functionality only cover a very small subset of use cases yet and has a list of restrictions.

The Known limitations for offloading on Redfox and Lynx-5000:

- Routed IPv6 traffic is handled by the CPU
- IP multicast traffic will be routed by the CPU
- Firewall forwarding chain will not impact any routed Unicast traffic
- NAT will not be performed on any routed traffic
- Only VLAN interfaces can be used, usage of Port-interfaces will not perform any traffic forwarding
- Policy-Based Routing will not function
- SSL-tunnel will function to some extent via the CPU but is strongly discouraged from being used in this release

Tracking vrrp instances with mroutes is not supported when offloading is enabled. If this feature is used it is recommended to disable offloading. (opposite steps to the example above).

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

Use of the WeOS Firewall together Hardware Offloading is not supported and the behaviour of doing so is undefined. The exception is when firewall configuration is limited to *filter input* rules.

Hence, if the Firewall is use to configure *filter forwarding* rules, *NAPT* rules or *port forwarding* rules on a Viper-TBN, it is necessary to disable the Hardware Offloading (opposite steps to the example above).

```
viper:/#> configure
viper:/config/#> ip
viper:/config/ip/#> no offload
viper:/config/ip/#> leave
viper:/#>
```

### 3.8 Redundancy protocols on Relay ports

It is only supported to run link-aggregation as the selected option for redundancy on Relay ports. This is due to the fact that any other protocol can end up in very uncertain situations in cases where the bypass-relays are used.

In the future WeOS may refuse enabling these protocols on relay ports.

### 3.9 FRNT

Fastlink must be enabled manually for FRNT (gigabit Ethernet) ring ports.

Fastlink is a unique feature of Westermo products to optimise gigabit Ethernet link-down fail-over times in layer-2 redundancy protocols such as FRNT.

### 3.10 RSTP

WeOS 5 supports RSTP, compliant to IEEE 802.1D-2004. Due to limitations in the WeOS 4 implementation of RSTP, a WeOS 4 unit will keep ports in blocking mode longer than needed when connected to a WeOS 5 node.

Hence, mixing WeOS 4 and WeOS 5 units in RSTP topologies may exhibit relatively long periods with limited connectivity during topology changes, this applies to both link failure and when a link comes up again.

Link aggregate path-cost use the configured port speed value(s) and not the negotiated speed value. This can lead to RSTP making the non-optimal path selection. Work-around this issue by setting a fixed path-cost in the spanning-tree port configuration.

### 3.11 IEC 61375

In this release, not all of the recovery use cases, nor the optional cases, are supported.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

TTDP and non-TTDP multicast can be used simultaneously in this release, but is considered unstable and is strongly recommended to be avoided.

"Automatic Gap Insertions", when several vehicles have the same name, can lead to unexpected behaviour.

When recovery-mode is set to deferred/wait, an ECSC must be running on the configured multicast address. If no ECSC is running and sending data on the configured multicast address, no node will come up at all.

It is strongly recommended to enable inauguration inhibition on all nodes to reduce spurious re-inaugurations and guarantee a stable train communication.

The "ECSP inhibit sync" function should only be enabled in consists with simple or straightforward ECN configurations. In complex configurations with non-symmetric ETBN/ECN connections and/or configurations where different ETBNs are master routers for different ECNs simultaneously, the backup ETBNs will not be able to unambiguously determine which ETBN is the master router/ECSP, which can in turn lead to unexpected behaviour with regards to the local inauguration inhibition value. In these cases, manually setting the local inauguration inhibition values on the backup ETBNs, via the ETBN\_CTRL telegram, should instead be performed.

VRRP virtual IP address ("VIP") is primarily intended to be used as a gateway/router address, and not as a host address. However, using the VIP as a host address, that at any one time belongs to the currently active ECSP is a common use case. When using the VIP in this way, for ECSC-ECSP communication, it is recommended that the "vmac" option in the VRRP configuration be turned off for all VRRP instance whose VIPs are used in this way.

### 3.12 Custom TRDP telegrams

The implementation of Custom TRDP telegrams has some limitations:

- Data from up to 32 device ports can be included across all defined datasets.
- Data from up to 8 VLANs can be included across all defined datasets.
- Data from up to 4 FRNTv2 rings can be included across all defined datasets. FRNTv2 is the only supported ring protocol for which data can be included.

### 3.13 LLDP

When using Link Aggregation, the individual member ports will transmit LLDP frames using the MAC address of the link aggregation interface, i.e. all member links in an aggregate will be using the same MAC address.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 3.14 Port Monitoring

It is not possible to utilise port monitoring directly on a link aggregation port interface. However it is still fully possible to monitor the individual member ports that constitute any given link aggregate.

Therefore, in order to fully monitor an aggregate, monitoring must be configured for each of the aggregate member ports.

### 3.14.1 Cross switch core limitation

It is not possible to use port-monitor where the source and destination ports are split between switchcore 2 and 3 on Viper-120 and Viper-220 products.

Having the source and Destination port on the same switch core or one of the source or destination ports on ports ethX7, ethX8, ethX14 or ethX20 while the other resides on one of the other switchcores is possible.

## 3.15 Media Redundancy Protocol (MRP)

- *MRM not supported for MRP 30 profile:* WeOS 5 units can be configured to operate in MRP 200 or MRP 30 profile. However, for MRP 30 profile, configuring the WeOS 5 unit as MRP Master (MRM) is not supported. A WeOS 5 unit can be used as MRP Client (MRC) with MRP 30 profile with MRMs from other vendors.

More details: When a link comes up between two MRP clients, the clients send *link-up* messages to the MRP master. The MRP 30 ms profile only gives the MRP master 4 ms to block its secondary port from the time the MRP clients send their first *link-up* message. The WeOS 5 MRP Master is not always capable of doing that, resulting in a short transient loop in the MRP ring when the ring is healed.

To avoid this, it is recommended to use the MRP 200 ms profile instead. For link-down scenarios, MRP 200 ms profile conducts failover as fast as the 30 ms profile, given that MRCs in the ring are capable of sending MRP *link-down* messages (WeOS units have this capability).

- *Use of MRP with virtual L2 ports (SSL VPN ports):* MRP is specified for use with Ethernet ports (full duplex, 100 Mbit/s or higher). WeOS enables the use of running MRP over SSL L2 VPNs, but requires the VPN to run over a high-performance network to work well. Furthermore, only the MRP '200 profile' can be used with SSL VPNs.

## 3.16 10G SFP Ports

The 10G SFP ports on RedFox-7528 have the following limitations:

- IEEE 1588/PTP is currently not supported on 10G SFP ports.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

- 10G SFP ports are only to be used for 10G Fiber SFPs or 1G Fiber SFPs, not copper SFPs or 100 Mbit/s Fiber SFPs.
- Status of MDI/MDIX and polarity shows value 'Invalid' ('N/A' or 'Not Applicable' would be more appropriate).

### 3.17 Search function in User Guide

The User Guide included within the release-zip is Web based. The Search function in the User Guide navigation pane only works if you make the pages available via a Web Server. That is, the Search function does not work when opening the User Guide via your local file system.

At <https://docs.westermo.com/weos/weos-5/> you can browse the WeOS 5 User Guide online, with Search function included.

### 3.18 RedBox PTP Boundary Clock

RedBoxes running Boundary Clock in an HSR ring must be connected with all A ports in the same direction. As the BC prioritizes synchronizing from the A port, if two BC are synchronizing towards each other neither of them may end up in a stable state.

Connect devices as shown below:

```
ethA-RB-ethB <-> ethA-RB-ethB <-> ethA-RB-ethB . . . .
```

### 3.19 Ingress rate limiting

On Viper-3000 series and Lynx-3000 series, ingress rate limiting of multicast traffic includes broadcast.

### 3.20 Static unicast MAC filters for link aggregates

Static unicast FDB filters are known to not work as expected when the port associated with the filter is a link aggregate that spans multiple switch cores.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 4 Known Issues

### 4.1 List of known issues

Issue	Category	Description
#21200	Port Monitoring	Not possible to mirror traffic directed to/from the switch
#21198	System	netd generates segfault and cause system to lose default gateway at boot
#21197	System	FW upgrade towards a HTTPS server does not work
#21196	DHCP	DHCP Client not working on Layer 2 Lynx-5000 and Redfox
#21194	IP Multicast	MROUTE tracking maps to interface set as tracking and not input vlan making rule fail on system level
#21193	System	During long term test with link down/up the device lose it's static ip address
#21191	System	Active SSH session remains active after disabling SSH
#21184	System	Installing invalid wmopkg in package context can lead to soft-locked device
#21178	General	Arbitrary command execution through ddns hostname
#21170	CLI	Console lockout when denied upgrade of pkg:s
#21158	Ports	Unable to configure egress rate limit when a LAG exists
#21148	System	system start input validation for system hostname refuse underscore
#21146	VPN	Log spammed with Wireguard messages if no connection to peer
#21141	Alarm	Configuration validation passed files may still break system form storing config making reboot start in safe config
#21140	Alarm	Alarm fails to map to frntv0 service on configuration restore
#21135	AAA	ssh ignores password policy setting 'prevent-reuse: Enabled' when password is expired
#21134	VPN	IPsec: selecting bundle as local-cert might not work
#21123	Offloading	Offloading of multicast fails within 1min after streams start on Viper platform
#21122	Port Access Control	Authorized entries can become black hole in software bridge fdb
#21115	Ports	RedBox: IRQ spam sometimes when SFP is inserted but not in use
#21112	System	SCEP password not stored in product specific GNS3 templates
#21086	System	Show fdb includes unexisted enteries
#21078	System	Setting static speed/duplex works only the first time (Viper 3000)
#21077	TCN	TTDP remote-inhibit flag does not consider both ends simultaneously

Continued on next page

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

Continued from previous page		
Issue	Category	Description
#21076	System	Flushing fdb can take a long time (Redfox and Lynx 5000)
#21068	Alarm	Alarm instance is not restarted when doing a config restore
#21067	IGMP	IGMP membership reports forwarded on all ports
#21063	SNMP	SNMP commands depend on order they are defined
#21040	VLAN	Creating lots of VLANs can lose LAN settings
#21037	Link Aggregation	"no lag <X>" does not removing lag <X> from "show running configuration"
#21016	Ports	Redfox and Lynx 5000 autoneg to 1Gbps/s may fail and fall back to 100Mbps
#20991	NTP	NTP client may take one full poll interval to start requesting remote server when starting in larger systems
#20957	System	Lynx 5000 and Redfox inconsistent hotswap of External media disk without partitions
#20919	General	certificate store isn't findable by client utilities
#20896	Any	mDNS discovery not working on Redbox
#20891	Kernel	Port priority does not work across switchcores (DSA)
#20888	Ports	Redfox and Lynx 5000 SFP handler can fail to setup the correct low level duplex settings for Gbps SFPs
#20868	System	Ports Eth1-Eth4 on Redfox can become unable to transmit packets after sustained CPU routing overload
#20833	System	Buffer overflow via crafted input leading to denial of service
#20828	System	Deactivating Watchdog in Lynx + RedFox 5000 & 7000 series reboots the unit continuously
#20826	VPN	Dpd timeout treated as constant in schema and not written to strongswan configuration file (only applicable for IKEv1)
#20820	WEB	Web becomes unusable when an upgrade was aborted or done without a reboot
#20771	WEB	WEB page is sporadically not updated after configuration
#20749	TCN	TCN can fail to build TTDB properly in the extremity 2 backup TBN when cstinfo have same cstID and/or vehID
#20748	System	RMON does not show Filtered/Discarded values
#20662	Any	no boot does not reset allow-untrusted/unlock-license
#20627	Port Access Control	Inconsistent and delay in MAC Address Authentication
#20617	VLAN	Packets seen on different VLAN in specific circumstances
#20603	System	Upgrade command can hang device forever in runlevel 9
Continued on next page		

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

Continued from previous page		
Issue	Category	Description
#20578	NTP	RTC may lock at wrong time at power down if backwards time jump has happened
#20574	Logging	Excessive logging during configuration change
#20410	DHCP	Unable to bind IP address when short DHCP leasetime is provided
#20312	AAA	Possible to get locked out if lockout policy is set and no valid connection to Radius server
#20309	System	Firmware upgrade could reset the user password
#20281	System	The error message "Failed to add audit entry to audit daemon" is spammed when applying large configs
#20249	System	Repeated connections via telnet may cause the telnet service to become unresponsive
#20233	HW	RTC: System time might not be stored correctly
#20231	WEB	Fail with restoring config in WEB but no fault messages
#20201	System	Rebooting after disabling offloading will remove all traffic policies
#20150	System	DHCP Reply seems to be offloaded, cannot accept address
#20047	WEB	The user is redirected to the login page when editing firewall rules is tried
#20045	LED	After initiating a 'factory reset' from the web GUI, a device will boot up, but the ON LED will remain RED even when boot is com
#19965	WEB	FRNTv2 is not shown in Status summary page when it is enabled
#19958	Boot Loader	Envoy Barebox uses precompiled ATF
#19928	TCN	Offloading with TCN does not allow for fragmented packets to be forwarded
#19903	System	configuration restore do not clear previous added route from system
#19882	System	Upgrade from ftp sever with DNS name does not work
#19880	WEB	Refreshing page when upgrade of bootloader or secondary restarts the upgrade if it's done
#19878	CLI	Config abort do not work correctly with an in valid configuration
#19870	IGMP	Multicast Snooping Boundary for MLD does not work on Dagger based systems
#19826	System	Large amount of authenticated SSH sessions causes denial-of-service condition
#19777	WEB	Upgrading primary image from web ui does not report flashing done in http response
Continued on next page		

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

Continued from previous page		
Issue	Category	Description
#19756	VRRP	The vmac of VRRP causes strange log messages and VRRP not to work properly
#19711	WEB	Cannot access help in some menus in webGUI when browser tree menu has gone past the bottom of the screen
#19517	Logging	When PoE-chip goes repetitively down many Kernel logs is generated and stored
#19498	IGMP	Duplicate multicast packets over link-aggregates when changing router timeout (Dagger)
#19410	IGMP	Mismatch between MDB and ATU for mc group 239.193.0.1 when etbn is acting as router, sender and consumer of data
#19323	FRNT	FRNT Focal point Topology Counter rush with LACP links (Dagger)
#19262	Ports	Traffic not handled on Envoy ports using Copper SFPs
#19251	PoE	Lynx 3510 PoE leds continuously blinking in case of LV supply
#18675	Link Aggregation	Long failover time (aggregate member link up/down) in link-aggregate interoperability case (WeOS5 'Dagger' vs WeOS4)
#18163	OSPF	Routes to 'redistributed connected E1 routes' lost within NSSA areas upon topology change
#18151	Logging	Long-running programs log events to syslog with the wrong time stamp on timezone changes
#18076	MRP	Probing MRP status (30 ms profile) during heavy load may cause reboot (Viper-TBN)
#18069	QoS	ARP packets treated with lowest priority and may be missed/dropped under load
#17995	System	Service discovery not available in safe-config

## 4.2 #20888 & #20868 Redfox and Lynx 5000 1Gbps SFP issues

The port will operate in half-duplex mode when using a 1 Gigabit SFP module that is hot plugged into a gigabit SFP slot on Redfox 5000 or Lynx 5000 or when a 1 Gigabit SFP module is used in any SFP+ slot on Redfox 7000. Also note that the port may become unable to transmit frames over that port after sustained device overload until the port is reset.

## 4.3 #18163: Work-around for OSPF NSSAs convergence issue

When using OSPF Not-So-Stubby Areas (NSSAs), failover when a router goes down may take a lot longer time than expected. There are two possible work-arounds until this bug is fixed:

- Alternative 1: Let each router get an address on its loopback interface, and include them in the

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

OSPF area, e.g., use OSPF setting “network 192.168.1.5/32 area 1” for a router in (NSSA) area 1 with address 192.168.1.5/32 assigned to its loopback interface (lo).

- Alternative 2: Use 'regular' OSPF areas instead of NSSA areas.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 5 Quick Start Guide

WeOS 5 devices are intended to be usable out-of-the-box as a switch. All access ports are assigned to the same VLAN (untagged) and the device tries to acquire a management IP address via DHCP. It also acquires a link-local address (in the 169.254.x.x range). These addresses are advertised with mDNS (Linux/Apple), SSDP (Windows), and LLDP.

### 5.1 Default User and Password

**user:** admin

**password:** admin

### 5.2 General

Apple, Linux, and Windows users with mDNS installed, can either use an mDNS client to find the device's IP address, or connect using a web browser:

- <http://weos.local>
- <http://redfox-4d-3b-20.local>

The first example is not available if there are many WeOS devices on the same LAN. The latter, and more reliable address, is a combination of the hostname and the last three octets of the device's MAC address in that LAN. In this example the hostname is `redfox` and the MAC address is `00:07:7c:4d:3b:20`.

Windows users without mDNS have SSDP to discover WeOS devices. In Windows 7 there is the *Network and Sharing Center* where a clickable icon for each discovered WeOS device should appear under *Network Infrastructure*. The PC must, however, be in the same subnet (DHCP or link-local) for this to work. Windows users also have the Westermo WeConfig tool to manage their WeOS devices.

Expert users can also use `nmap`, a port scanner, to scan the network for the device. Be aware though that this might be frowned upon should your device be located on a shared network.



Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

```
redfox-4d-3b-20:/config/#> iface vlan2
```

To show or change the interface and VLAN properties the user enters the command: `iface vlan2` and `vlan 2`, respectively, with an optional “show” as prefix. E.g. `show iface vlan2`.

```
redfox-4d-3b-20:/config/iface-vlan2#> help inet
```

The help command is always available. Use it stand-alone or with a context-specific setting to get more detailed help.

To leave a level use the command `end` to save or `abort` (or Control-D) to cancel. To save and exit all levels, and go back to admin-exec, use `leave` (or Control-Z).

```
redfox-4d-3b-20:/config/iface-vlan2#> leave
```

Applying configuration.

Configuration activated. Remember "copy run start" to save to flash (NVRAM).

The CLI, unlike the WebUI and WeConfig, has a concept of a running configuration. This is an activated but volatile (RAM only) file that must be saved to built-in flash (non-volatile storage) before rebooting. Many separate config files can be saved, but only one can be the selected startup-config. For details, see the built-in help text for the admin-exec copy and show commands.

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 6 Firmware Upgrade

Firmware upgrade is supported from the CLI, WebUI, and WeConfig tool. The CLI only supports FTP/TFTP upgrade but the WebUI and WeConfig tool can also upgrade via CGI upload – making them the ultimate choice if you have no FTP/TFTP server available or do not care to set one up.

### 6.1 WeOS Image

WeOS devices run from a built-in flash disk and usually comes with three partitions: primary, secondary, and boot. The latter is for the boot loader (see below) and the primary is the main WeOS image partition. Should this ever get corrupted, e.g. due to power-loss during upgrade, the device will boot using an image from the secondary (or backup) partition. This is a very appreciated, but mostly unknown, robustness feature.

Starting with WeOS 5.28.1, a **boot loader upgrade is required** if you are running Barebox v2024.03.0-3 or earlier to remediate a vulnerability affecting devices with Secure Boot. This means you need to run `upgrade boot` before running `upgrade primary` or `upgrade secondary`. See section 6.2 for details about `upgrade boot`.

Please note that a bug in WeOS versions 5.27.0, 5.27.1 and 5.28.0 will set the device in a state that requires a power cycle if you try to upgrade WeOS without first having upgraded the boot loader. Doing so might also trigger a success or error message that does not accurately reflect the upgrade status.

An alternative is to run `upgrade all` which upgrades all partitions in the correct sequence, not triggering the bug described above, regardless of which WeOS version you are currently running.

To upgrade the primary partition, run:

```
redfox-4d-3b-20: /#> upgrade primary <SERVER-ADDRESS> WeOS-5.29.0.pkg
```

The system must reboot when upgrading the partition image the system started on. This protects against flash corruption issues seen in earlier releases, caused by simultaneous access to the flash during programming or when starting new processes after an upgrade. Also, WeOS warns when one of the partitions has an image with invalid CRC. Attempting to upgrade the partition with the OK CRC is discouraged, upgrade the partition with the invalid CRC first.

As usual, when upgrading from an earlier release, we always recommend backing up your configuration beforehand.

**Note:** The version string listed in the output from the `show system-information` command in the CLI, or the System Details page in the WebUI, is only updated after reboot.

**Note:** Starting with WeOS 5.28.1, if you try to downgrade both WeOS and the boot loader from a WeOS package including a Barebox version older than v2024.03.0-4 by running `upgrade all`,

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

you will in effect only downgrade the secondary partition as the `upgrade all` command installs partitions in the following sequence:

- Secondary
- Boot loader
- Primary

Since it is not possible to downgrade the boot loader to a vulnerable version starting in WeOS 5.28.1, the upgrade process will stop after having downgraded the secondary partition.

## 6.2 Boot Loader

The boot loader firmware has its own version numbering scheme and is CPU platform specific. Unless the release notes explicitly recommend it, there is usually no need to upgrade the boot loader. This and future WeOS releases, however, require a boot loader upgrade if the device is running Barebox v2024.03.0-3 or earlier.

The boot loader firmware is included in the `WeOS-5.29.0.pkg`.

- Viper-3000 Series (Coronet): Barebox 2024.03.0-4
- RedFox-5000/7000 and Lynx-5000 Series (Dagger): Barebox 2024.03.0-4
- Lynx-3000 Series (Envoy): Barebox 2024.03.0-4
- Lynx-RB (Byron): Uboot 2024.04.0-1

```
redfox-4d-3b-20: /#> upgrade boot <SERVER-ADDRESS> WeOS-5.29.0.pkg
```

Document Release Notes WeOS 5.29.0	
Date May 19, 2026	Document No 224004-g7e71e1a

## 7 Significant differences between WeOS 4 and WeOS 5

Some aspects of the CLI are different between WeOS 4 and WeOS 5. Here are some examples:

- Access port names have changed, e.g. `Eth 1` is now `eth1`. Similarly, on products with M12 ports, `Eth X1` is now `ethX1`.
- Port ranges (lists) have changed, e.g. `Eth 1-8` is now `eth1..eth8`
- Server and Internet port settings are now usually input as `ADDR:PORT`
- IGMP settings have been renamed from `igmp-foo` to `multicast-foo` due to the included MLD snooping support. Hidden compatibility aliases exist to ease the transition
- Stateless NAT (NAT 1-to-1) has moved out from the firewall context
- Enabling management services per interface has moved to each specific service
- Configuration of management services have moved to a separate management sub-context
- New discovery services, in addition to LLDP, are mDNS and SSDP. The latter is for discovery on Windows systems, see also section 5
- The DHCP relay agent CLI syntax has changed considerably
- The `show running-config` command now lists an actual file, in JSON format as mentioned previously. An optional keyword now lists the first level JSON object, and more advanced keywords can also be given in `jq` syntax<sup>1</sup>. For more information, see the CLI online help text for `help running-config`

---

<sup>1</sup>For more information on `jq`, a JSON query tool, see <https://stedolan.github.io/jq/>