WESTERMO

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

WeOS 5.25.2
Release Notes

Contents

WESTERMO

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

This page intentionally left blank.

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 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

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-5.25.2/doc/weos/user-guide/index.html`

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

1 Summary of Changes

This section details new features added in this major release.

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

1.1 News in 5.25.0

In the WeOS 5.25 release focus has been to enhance the basic security functionality of WeOS. This effort has led to several improvements and also future functionality preparations. Enhancing product security may impose some limitations on how a device can be accessed and manipulated.

Although the aim has been to minimize user exposure to these changes, certain modifications were necessary and will affect some users.

With all the changes in this release, 5.25.0+ will sadly not function with WeConfig version 1.xx, However, in the near future WeConfig 2.0 will be released where WeOS will be fully supported again moving forward.

It is recommended to review these changes carefully before upgrading any system used in a live environment.

1.1.1 Dagger Platform Support Temporarily Excluded

Support for the Dagger products (RedFox-5000/7000 and Lynx-5000 series) is not included in 5.25.0. Support for Dagger have been resolved in 5.25.1, please see section 1.2.3.

1.1.2 Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol, or SCEP, described in RFC 8894 is a protocol designed to simplify and automate the process of certificate issuance and management within a Public Key Infrastructure (PKI) environment.

SCEP facilitates communication between client devices and a Certificate Authority (RA/CA) to automate the issuance of digital certificates and is popular because it saves time and enables devices to request and renew certificates.

The system supports the rollover of Intermediate-CA certificates. The rollover of Root-CA certificates is not supported. Any new root certificate will overwrite the existing one.

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

Document

Release Notes WeOS 5.25.2

Date

August 26, 2025

Document No

224004-gd84d170

1.1.3 Certificate Revocation List

Static configuration of CRL:s (certificate revocation list) is implemented. If CRL is configured the device will periodically check URL for valid files. Support for using CRL is implemented in OpenVPN, syslog and webgui.

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

1.1.4 Certificate Chaining

When selecting a certificate to use in services like OpenVPN it is now a requirement that the full certificate chain must exist on the device.

For more information see the WeOS User Guide section *Configuration Guides → PKI → Certificates and Keys*.

1.1.5 Secure storage

Secure storage encrypts certificates and private keys when they are written to persistent storage, both on internal or external memory media.

When upgrading to this release, legacy keys from previous releases will not automatically be migrated to secure storage and encrypted. To encrypt legacy keys, they must be removed and re-imported. Both unencrypted legacy keys and newly imported encrypted keys can coexist, but this is not recommended.

The sync command in the media context is used to synchronize configuration files and certificates between specified media. When synchronizing to an external device, the certificates will be encrypted with a device specific ID and cannot be used on another device, it can only be used on the originating device. The configuration files, however, can be moved and used on other devices.

The VFAT filesystem support is deprecated, certificates and keys saved on a USB stick with VFAT will be mounted as read-only.

The secure storage function is not implemented on the Redfox and Lynx 5000.

1.1.6 SSH - Changes

In this release the SSH services daemon from Dropbear to OpenSSH. However, this change results in the devices SSH-keys needing to change structure. After upgrading the old SSH-keys will automatically be converted to the new format. The reformatted keys will automatically be stored into the Secure Storage.

This daemon change also results in WeOS no longer supporting DSS (Digital Signature Standard) keys. The DSS keys have been considered deprecated generally due to security concerns.

However, the converted keys will not be recognized by older WeOS versions and after performing a WeOS downgrade the user will be prompted with the following warning the first time they are accessing the device trough SSH.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:[FINGERPRINT].
Please contact your system administrator.
Add correct host key in /home/USER/.ssh/known_hosts to get rid of this
message.
Offending RSA key in /home/USER/.ssh/known_hosts:15
  remove with:
  ssh-keygen -f '/home/USER/.ssh/known_hosts' -R '10.0.0.1'
Host key for 10.0.0.1 has changed and you have requested strict
checking.
Host key verification failed
```

These changes were made to enhance the default security in the software.

- Access to shell over SSH has been restricted but can be re-enabled through Console access.

- File uploading using SCP has been restricted but can be controlled through device management.

It strongly discouraged to leave these settings enabled permanently.

Finally, a minor update have also been made to the SSH client command in the CLI. This includes some improvements to IPv6 address handling, user name providing and non standard port providing. However, the same command format as currently exist should still work as before. Fore more information, refer to the WeOS User Guide section mentioned below.

For more information see the WeOS User Guide section *Configuration Guides → Management Interfaces → SSH*.

1.1.7 Logging

Add a new configuration option *Ignore Hostname Mismatch* for logging configurations using TLS, available both for source and destination. When enabled, the TLS handshake will ignore any mismatch between hostname and subject name in the certificate. By default, this setting is disabled, meaning that the default behaviour is still the same as before.

For more information see the WeOS User Guide section *Configuration Guides → Alarm, LEDs and Logging → Logging*.

1.1.8 Multicast route - VRRP tracking

Multicast route control using VRRP tracking has been added (only routes packets if the VRRP instance is active). There are limitations with regards to overlapping multicast routes and the ability to use this feature, see the user guide for more information.

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

1.1.9 RedBox - PTP Boundary Clock

PTP Boundary Clock has been added. If PTP BC is enabled along with HSR/PRP it will behave as a DABC (Doubly Attached BC) according to 62439-3:2016.

For more information see the WeOS User Guide section *Configuration Guides → Network Services → PTP/1588*.

1.1.10 Increased numbers of VLANs

The number of supported VLANs has been increased from 64 to 255. The maximum number of VLAN interfaces remains 64, if additional VLANs are created on the device no associated VLAN interface is created.

1.1.11 AAA RBAC - Auditor role

A new user role has been added, the Auditor, which has read-only access to audit logs.

For more information see the WeOS User Guide section *Configuration Guides → AAA and User Management → AAA*.

1.1.12 Password Expiration

During user configuration it is now possible to mark passwords as expired to force the user to change it on next login.

For more information see the WeOS User Guide section *Configuration Guides → AAA and User Management → AAA*.

WESTERMO

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	**224004-gd84d170**

1.1.13 Copy command now longer supports URI:s

The copy CLI command no longer supports URI:s. Refer to the file context for more information on how to copy files to and from the device.

1.1.14 File context added to CLI

The CLI now has a file context for general file operations such as show, copy and erase for log files and configuration files.

Within this context it is also possible to perform Imports and Exports of managed files in the system.

For more information see the WeOS User Guide section *Configuration Guides → Generic Maintenance → Filesystem*.

1.1.15 IEC61375 - All Viper 3000 extended

With this release the IEC61375 protocols are now officially supported on all Extended Viper-3000 products.

1.1.16 IEC61375 - CSTINFO data file validation

The CSTINFO data file is now validated against a JSON schema. The syntax has also been changed to be stricter. Any previous comm-profile.json files wont be used in this release and a new file with the correct structure must be uploaded before use. The file must now be placed in /cfg/cstinfo.json. The preferred uploading mechanism for this file is through the Web interface.

The schema file is available in the User Guide.

For more information see the WeOS User Guide section *Configuration Guides → Train → IEC 61375-2-3 (Communication Profile)*.

1.1.17 Input validation

As of this release, any configuration that is applied to the system will be validated against a JSON schema. This also includes copying configuration files to running or startup-config. The JSON schema used for validation is available for offline external validation and is included together with the release.

1.1.18 Configuration Integrity

WeOS' configuration files are now secured by the configuration-integrity feature. Any change to systems configuration files is intercepted, verified and logged into the audit log.

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

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

1.1.19 Boot Configuration Integrity

Boot Configuration Integrity ensures that the boot configuration remains unaltered outside of WeOS. If WeOS detects any unauthorized changes, it will trigger an alarm and log the event to the audit log. Additionally, the user will receive a warning message in both the CLI and WEB interface.

Note: During upgrades or downgrades that also involves changes to the boot configuration, verification failures may occur. If the change is intentional, the alarm can be reset using a command in the boot context menu.

The boot integrity function is not implemented on the Redfox and Lynx 5000 series.

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

1.1.20 Updated CA Certificates bundle

Bundled certificates is now updated to https://ftp.debian.org/debian/pool/main/c/ca-certificates/ca-certificates_20250419_all.deb

1.1.21 ID-mem Integrity Verification

WeOS will verify the integrity of the ID-mem when booting and generate an auditble event and syslog message describing the result. This verification check is not configurable and will always be performed. The signed ID-mem integrity verification function is not implemented on the Redfox and Lynx 5000 series.

This verification is only applicable for Secure Boot devices.

1.1.22 IPv6

When IPv6 is enabled the loopback interface will be automatically assigned the IPv6 address ::1/128.

1.1.23 Outgoing multicast routes

The supported number of outgoing multicast routes has been increased to 32, up from the previous limit of 16.

1.2 News in 5.25.1

This release is a bug fix release that aims to remediate critical issue with the previous released version. The primary driver for the release is to fix issues with a to verbose logging and configuration validation issues discovered in WeOS 5.25.0.

The subsections below describe news in WeOS 5.25.1. In addition, section 2.2 includes information on fixed issues.

1.2.1 Sensitive Information in logging removed (as relative to 5.24.0)

Security advisory Westermo-25-08: Sensitive Information in logging, is solved.

1.2.2 Improved configuration validation (as relative to 5.25.0)

JSON schema for configuration validation was too restrictive and have been adjusted.

1.2.3 RedFox-5000/7000 and Lynx-5000 series

The Dagger products (RedFox-5000/7000 and Lynx-5000 series) fully supported (was excluded in 5.25.0).

1.2.4 SNMP RICH-MIB not cached

Caching for WESTERMO-RICH-MIB has been disabled.

1.3 News in 5.25.2

The subsections below describe news in WeOS 5.25.2. In addition, section 2.3 includes information on fixed issues.

1.3.1 VRRP - vmac interface management

This version changes and exposes some VRRP-vmac behaviours as selected interfaces as listening and incoming interfaces.

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

2   Fixed Issues

2.1   WeOS 5.25.0

Fixed issues in WeOS 5.25.0 (as relative to 5.24).

Issue	Category	Description
#20454	SNMP	Memory leak when performing any SNMP read on RiCh MIB (oid: 1.3.6.1.4.1.16177.2.10*)
#20451	SSH	SSH session opened from WeOS do not respect user typed and uses admin
#20412	System	Upgrade options are not handled consistently
#20411	WEB	RMON values in WEB do not show right values, many show '0' and other unreasonably high count
#20390	SNMP	SNMPv3 user with both auth and encrypt can be accessed with only auth in snmpwalk
#20382	SNMP	Not possible to set OIDTREE for a user in CLI.
#20332	CLI	Possible to telnet into daemon and make changes from CLI
#20330	QoS	Redfox and Lynx 5000 ingress rate limiting mode 'u-uni' (unknown unicast) also limits known unicast
#20303	CLI	Running 'package import' in not properly sanitized in CLI
#20300	CLI	No ttdp causes issues with vlan ports
#20296	WEB	Config TTDP mroute in WEB without a netmast yields a /0 route this should be a /32 route
#20290	System	No sanity check for media names
#20377	SNMP	Not possible to set listen interface for SNMP from the web
#20273	VPN	IPsec Peer command accepts invalid IP addresses
#20271	Port Access Control	Redfox and Lynx 5000 fdb becomes out of sync and ageing time is negative
#20263	PTP	"show ptp network" doesn't show non-WeOS clocks
#20248	Alarm	At reconfiguration SNMP traps may not become active
#20228	SNMP	SNMP ifIndex-Persistence not respected in Q-Bridge MIB entries
#20224	WEB	It is possible to restart device via web while running an upgrade in CLI
#20214	PTP	Running PTP on many ports caused synchronization to fail. TC should never lose synchronization. For Lynx 5000 and RedFox
#20207	WEB	Broken drop down menu for speed-duplex
#20199	VLAN	Communication loss when changes to VLAN configuration
#20136	SNMP	Strange SNMP behaviour with multiple inform hosts (targets)
		Continued on next page

Document	
Release Notes WeOS 5.25.2	
Date	**Document No**
August 26, 2025	224004-gd84d170

		Continued from previous page
Issue	**Category**	**Description**
#20132	NTP	NTP restart command is treated as process crash, gives up after 10 times
#20131	SNMP	SNMP Inform not sent out when RiCh gets uncoupled to single consist
#20092	NTP	Incorrect NTP DSCP Value
#20052	WEB	redirect_url users (e.g. Config/System/Date&Time -> Set time and Tools/Ping) are broken
#19996	General	Log messages indicating problems with ptp4l/ts2phc config files
#19978	QoS	Ingress-rate-limit for broadcast does not limit ARP
#19940	WEB	Broken JavaScript on "Edit IPSec Tunnel X" page
#19832	NTP	NTP client chrony Poll-Interval not correctly mapped as it uses $2\hat{x}$ and not decimal steps as documented
#19569	PTP	Long residence times introducing inaccuracy. Residence times now significantly lower. For Lynx55xx and RedFox.
#19336	Ports	RMON values for filtered/discarded column are wrong on a Viper 3000

2.2 WeOS 5.25.1

Fixed issues in WeOS 5.25.1 (as relative to 5.25.0).

Please see section 1.2.

2.3 WeOS 5.25.2

Fixed issues in WeOS 5.25.2 (as relative to 5.25.1).

Issue	**Category**	**Description**
#20681	AAA	Authentication of user with only remote Radius (no local fallback) gives the user role null
#20532	SNMP	SNMPv3 get-request are answered with wrong engineID since the MAC address on iface chan0 is wrong
#20530	System	Removing HSR/PRP interfaces fails config apply
#20529	System	Failed validation of AAA Remote server hostname
#20524	SNMP	WESTERMO-RICH-MIB does not follow the TruthValue for richTopoCntValid
#20512	RSTP	Configuration changes restarts RSTP which causes communication loss
		Continued on next page

		Continued from previous page
Issue	**Category**	**Description**
#20552	SNMP	Lockup/Hanging caused by SNMP Traps/Informs
#20502	SNMP	Security advisory Westermo-25-08
#19812	VRRP	VRRP Name greater than 10 characters creates results in VMAC interface name too long error in syslog

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 Firewall

When using VRRP and firewall it is required to disable vmac on the VRRP instance to allow for the firewall rules to match according to in IFACE vlan.

It is still possible to use IP-Address matching on traffic. This current limitation is restricted to rules matching on incoming interfaces.

3.4 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

3.5 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.

3.6 Setting Date Manually

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

3.7 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.

3.8 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).

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:/#>
```

3.9   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.

3.10   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.

3.11   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.

3.12   IEC 61375

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

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.

3.13   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.

WESTERMO

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

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 splitt 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.

- 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 Lockup/Hanging caused by SNMP Traps/Informs

SNMP handling in the device hangs after a couple of hundred messages, SNMP Read/Write and Traps/Informs will stop working.

The problem seems to occur when an Alarm Trigger that supports SNMP traps/informs is configured together with an alarm Action that includes generation of SNMP traps/informs. The problem can occur with just Alarm configured, no SNMP Trap Host(s) needs to be configured. When the specific Alarm Event occurs a trap/inform will be attempted to be sent, after a couple of hundred events the sending hangs.

When this happens the only way to get SNMP to function again is to restart the system's alarm handling. This is either a reboot, or a configuration change that affects the Alarm setup. If you do not need SNMP traps/informs, ensure to remove the SNMP from the configured Alarm action.

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

4 Known Issues

4.1 List of known issues

Issue	Category	Description
#20429	SNMP	Lockup/Hanging caused by SNMP Traps/Informs
#20417	VPN	MPTCP in SSL tunnel not starting subflow link in some circumstances
#20416	SNMP	SNMP Read and Write community can not be same as that blocks Write function
#20410	DHCP	Unable to bind IP address when short DHCP leasetime is provided
#20328	TCN	TCN may miss to activate ECSP master state even if the VRRP state is set as Master
#20312	AAA	Possible to get locked out if lockout policy is set and no valid connection to Radius server
#20302	WEB	WEB status for TCN missing most data
#20292	LED	HW-Alarm does not control LED consistently
#20288	PTP	PTP unable to perform timestamping with SFP hotplug
#20281	System	The error message "Failed to add audit entry to audit daemon" is spammed when applying large configs.
#20279	WEB	Error occurs when the user deletes an IPsec tunnel
#20274	Alarm	Entering the severity command with unknown option will crash CLI
#20269	System	When startup-config is missing, the device may not select configured fallback/failover config
#20266	Build/Image/Zip	Upgrade from USB does not work
#20258	DHCP	DHCP relay do not activate at a configuration file restore
#20246	General	Route Monitor doesn't reset the admin distance to the configured value if an alarm triggered
#20245	VPN	IPsec tunnel can be established with wrong PSK in special circumstances
#20233	HW	RTC: System time might not be stored correctly
#20231	WEB	Fail with restoring config in WEB but no fault messages
#20221	DHCP	DHCP snooping not limiting to defined VLAN and snoop up all port 67 request
#20288	PTP	Hotplugged SFP unable to timestamp on Lynx55xx and RedFox
#20058	System	RMON counters not working correctly
#20047	WEB	The user is redirected to the login page when editing firewall rules is tried
		Continued on next page

WESTERMO

Document	
Release Notes WeOS 5.25.2	
Date	**Document No**
August 26, 2025	224004-gd84d170

Issue	Category	Description
#20045	LED	After initiating a 'factory reset' from the web GUI, the ON LED will remain RED after boot
#20042	Kernel	TC get an exception when deleting the TC rules in IGMP context
#19998	General	Metrics for Ports not working on Lynx 5000
#19991	DHCP	Disabling Gateway setting in 'Server-setting' breaks Inherit Gateway in 'Subnet-setting'
#19977	CLI	Custom SNMP engine-id length is not enforced in CLI configuration
#19965	WEB	FRNTv2 is not shown in Status summary page when it is enabled
#19964	LED	The LED indicators for FRNT and RSTP on both Lynx and Redfox do not turn off when the protocol is disabled
#19947	System	IPv6 SCP not working (copy, upgrade)
#19946	System	Upgrade not working using SCP, device also gets soft-locked
#19928	TCN	Offloading with TCN does not allow for fragmented packets to be forwarded
#19924	VRRP	VRRP instance is not restarted when doing a config restore
#19903	System	Configuration restore do not clear previous added route from system
#19902	VPN	IPSec issues with LAN traffic when NAT rule is applied
#19895	Firewall	FTP Alg helpers isn't working when performing FTP file transfers
#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/MLD	Multicast Snooping Boundary for MLD does not work on Lynx-5000 and Redfox-5000/7000
#19856	AAA	MAC Auth reauthentication towards remote-server is delayed after boot
#19850	IEEE1588/PTP	Different link speeds causes higher TC error rate
#19818	SNMP	Syntax errors in Westermo MIB files for FRNT and EVENT
#19783	System	Coronet: Out-of-order problem on Viper-20 remains
#19777	WEB	Upgrading primary image from web gui does not report flashing done in http response
#19721	TCN	Setting port Admin state as "No Enable" not respected on TTDP LAG ports

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

<div align="right">Continued from previous page</div>

Issue	Category	Description
#19711	WEB	Cannot access help in some menus in webGUI when browser tree menu has gone past the bottom of the screen
#19692	Firewall	TCP port 53 listening when DNS server functionality disabled
#19524	WEB	Unable to delete VLAN by WEB when FRNT is enabled (Lynx 3000, 5000 and Redfox)
#19498	IGMP	Duplicate multicast packets over link-aggregates when changing router timeout (Lynx 5000 and Redfox)
#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 (Lynx 5000 and Redfox)
#19288	FRNT	After configuring FRNT2 on Viper 3520, the FRNT LEDs are flashing red
#19262	Ports	Traffic not handled on Lynx 3000 ports using Copper SFPs
#19255	QoS	Priority-mode IP fails when both ingress and egress ports are fiber ports on Lynx 3000
#19181	Ports	Port-Priority-mode IP and Offloading broken with DSCP set field
#19024	Link Aggregation	Using link-aggregates as FRNT ring ports gives long failover times in ring topology changes
#18967	System	Joins on SSL ports does not lead to the CPU port being added to the ATU
#18886	IP Multicast	Static multicast route with wildcard source fails to forward when group first heard on other interface
#18808	Alarm	Link-alarm with multiple ports makes status-relay indicate OK when some port is up and others down
#18675	Link Aggregation	Long failover time (aggregate member link up/down) in link-aggregate interoperability case (WeOS5 'Redfox' vs WeOS4)
#18643	IEEE1588/PTP	RedFox 5528/5728 fiber ports (Eth1-4) have more jitter in the correction field accuracy than the other fiber ports
#18614	TCN	TTDP NAT rules incorrectly modifies packets between local CNs
#18362	TCN	Broken/missing ECSPs in train composition handled incorrectly
#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

<div align="right">Continued on next page</div>

Document
Release Notes WeOS 5.25.2

Date	Document No
August 26, 2025	224004-gd84d170

		Continued from previous page
Issue	**Category**	**Description**
#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 #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 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.

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.

WESTERMO

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

5.3 CLI

WeOS comes with a Command Line Interface (CLI) that can be accessed via a console port at 115200@8N1, or Secure Shell (SSH). Only SSH protocol version 2 is supported. To gain access to the CLI using SSH you need:

- An SSH client, see below

- The device's IP address or DNS/mDNS name, see above

- The user name and password, default user: admin, password: admin

SSH Clients

There are many of SSH clients available, some of them can even be used to connect to the devices using a (USB) serial console port. A few free clients are listed below. Please follow the directions for installation and usage applicable to your operating system and client.

UNIX, Linux, Apple macOS OpenSSH, `https://www.openssh.com`

Apple macOS Termius, `https://www.termius.com`

Windows PuTTY, `https://www.chiark.greenend.org.uk/~sgtatham/putty/`

CLI Overview

The CLI has two main scopes: admin-exec and configure context. The former is what the user lands in after initial login.

```
redfox-4d-3b-20 login: admin
Password: *****
.--.--.--.-----.-----.------.-----.-.--.--------.-----.
|  |  |  |  | -__|__ --|_    _|  -__|   _|  .  .  |  _  | http://www.westermo.com
 \__/\__/|_____._____|  |__| |_____|__| |__|__|__|_____|        info@westermo.se
   Robust Industrial Data Communications -- Made Easy

\\/ Westermo WeOS v5.3 5.3.x-g7890bde -- Oct 24 19:30 CEST 2018
Type: 'help' for help with commands, 'exit' to logout or leave a context.

redfox-4d-3b-20:/#> help
```

Central concepts in WeOS are: ports, VLANs, and interfaces. To see status of each in admin-exec context, use `show ports`, `show vlans`, and `show ifaces`.

To change settings, enter the configuration context with the command `config`. The same commands as above also apply here, but now display the configured settings. Notice how the CLI prompt changes to show the current scope.

Copyright © 2025 Westermo Network Technologies AB

`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.

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.

```
redfox-4d-3b-20:/#>  upgrade primary <SERVER-ADDRESS> WeOS-5.25.2.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.

6.2   Boot Loader

The boot loader firmware has its own version numbering scheme and is CPU platform specific. Please note, unless the release notes explicitly recommends it, there is usually no need to upgrade the boot loader.

The boot loader firmware is included in the WeOS-5.25.2.pkg.

- Viper-3000 Series (Coronet): Barebox 2024.03.0-2
- RedFox-5000/7000 and Lynx-5000 Series (Dagger): Barebox 2024.03.0-2
- Lynx-3000 Series (Envoy): Barebox 2024.03.0-2
- Lynx-RB (Byron): Uboot 2024.04.0-1

```
redfox-4d-3b-20:/#>  upgrade boot <SERVER-ADDRESS> WeOS-5.25.2.pkg
```

WESTERMO

Document	
Release Notes WeOS 5.25.2	
Date	Document No
August 26, 2025	224004-gd84d170

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[1]. For more information, see the CLI online help text for `help running-config`

---

[1]For more information on jq, a JSON query tool, see https://stedolan.github.io/jq/

This page intentionally left blank.