



## Firmware for EDR-G9004 Series Release Notes

<b>Version: v3.23</b>	<b>Build: 25123121</b>
<b>Release Date: Jan 09, 2026</b>	

### Applicable Products

EDR-G9004 Series

### Supported Operating Systems

N/A

### New Features

- Added Directed Forwarding.
- Added RX Discard.
- Added Neighbor MAC Change events.
- Added Connection Management.

### Enhancements

- SNMP/SNMP Trap supports SHA-256 and SHA-512 authentication.
- Port Usage Alarm supports SNMP Trap.
- Tech Support File allows users to generate and import files for troubleshooting.
- Ping tool supports selecting source interface.
- WAN Redundancy feature supports configuring domain names as ping hosts for each interface.
- Supports identification of embedded CIP command type (Service Code) in EIP traffic.

### Bugs Fixed

- An error occurs when viewing LLDP entries through the web interface or via SSH.
- Rate limit not working after device reboot.
- Link-up failure after device reboot.
- Failed to import configuration file.
- CPU usage reaches 100% after uploading security package v13.0.28.
- SNMP v3 traffic is blocked, causing devices to be SNMP-unreachable in MXview One.
- Page freezes when Asset Recognition is enabled.
- Trap information for MAC address table changes is incorrect.
- Cannot get up-to-date SNMP OID values through SNMP.
- Web interface not accessible via HTTP after HTTPS is disabled.
- System time incorrect after importing configuration. (Fixed in v3.21.0)
- OpenVPN client configurations occasionally fail to import.

### Changes

- When relay activates, the STATE LED also triggers.

### Notes

N/A



<b>Version: v3.22</b>	<b>Build: 25102916</b>
<b>Release Date: Nov 11, 2025</b>	

### **Applicable Products**

N/A

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Added a CIP Service Code option to the EtherNet/IP (EIP) Protocol Filter Object.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

- This version includes the security fixes from the previous v3.17 release, addressing the following vulnerabilities:
  - CVE-2025-0415
  - CVE-2025-0676



<b>Version: v3.21</b>	<b>Build: 25100115</b>
<b>Release Date: Oct 03, 2025</b>	

### **Applicable Products**

N/A

### **Supported Operating Systems**

N/A

### **New Features**

- Added mechanism to detect syslog server availability.
- Added a notification feature for soon-to-expire licenses.

### **Enhancements**

N/A

### **Bugs Fixed**

- CVE-2025-6892, CVE-2025-6893, CVE-2025-6894, CVE-2025-6949, CVE-2025-6950 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-258121.

### **Changes**

- Changed the behavior of user account password modification.

### **Notes**

N/A



<b>Version: v3.20</b>	<b>Build: 25082113</b>
<b>Release Date: Aug 27, 2025</b>	

### **Applicable Products**

N/A

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

N/A

### **Bugs Fixed**

- IPS function disabled after upgrading the firmware.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v3.19</b>	<b>Build: 25071510</b>
<b>Release Date: Jul 31, 2025</b>	

### **Applicable Products**

N/A

### **Supported Operating Systems**

N/A

### **New Features**

- Added SMTPS support in email settings.
- Added Domain Protection.
- Added Asset Recognition.

### **Enhancements**

N/A

### **Bugs Fixed**

- Unexpected space characters in IPsec VPN Tunnel name settings.
- The local time does not change according to the selected time zone when Daylight Saving Time is enabled.
- State LED UI hint not accurate.
- Navigating to Syslog page causes unexpected sign out.
- Device stops responding to NTP requests from LAN clients.
- Certain characters in passwords cause sign in failures.
- Enabling or disabling a user account required re-entering the password modification.

### **Changes**

- Simplified license management and IPS licensing.

### **Notes**

N/A



<b>Version: v3.14</b>	<b>Build: 24123112</b>
<b>Release Date: Dec 31, 2024</b>	

## Applicable Products

EDR-G9004 Series

## Supported Operating Systems

N/A

## New Features

N/A

## Enhancements

- Added support for "Route Mode" in IPsec Startup Mode. In Route Mode, the VPN tunnel initiates only when routing packets are generated, relying on traffic to trigger the tunnel.
- Added support for CLI commands to configure MXsecurity port settings.
- The "Ping Response" function has been moved from the "User Interface" (MX-ROS v3.12.1 to v3.13) and "Trusted Access" (MX-ROS v3.6) pages to the dedicated "Ping Response" page.
- Added IP display on the Querier Connected Port in the IGMP Snooping Group Table.

## Bugs Fixed

- Routed traffic is not correctly processed according to the configured QoS rules.
- MXview 1.4.1 does not receive encrypted SNMPv3 Trap/Inform packets from the routers.
- Email Settings cannot be disabled.
- CVE-2024-9138, CVE-2024-9140 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-241155.

## Changes

- Changed the QoS DSCP Mapping table to start from 0x0(0) instead of 0x0(1).

## Notes

Due to an issue, using an identical pre-shared key to set up multiple site-to-any IPsec VPN tunnels with IKEv1 mode requires a workaround. Please contact Moxa Technical Support for assistance.



<b>Version: v3.13.1</b>	<b>Build: 24111415</b>
<b>Release Date: Nov 18, 2024</b>	

### **Applicable Products**

N/A

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

N/A

### **Bugs Fixed**

- ARP Reply packets are incorrectly dropped in Bridge Mode.
- When exporting the configuration, the Object IP Range setting is saved incorrectly, causing importing the configuration to fail.

### **Changes**

N/A

### **Notes**

N/A

<b>Version: v3.13</b>	<b>Build: 24100800</b>
<b>Release Date: Oct 09, 2024</b>	

## Applicable Products

N/A

## Supported Operating Systems

N/A

## New Features

- Added a CPU usage notification to Event Notification.
- Added a port usage notification to Event Notification.
- Added support for new DPI protocols to Advanced Protection: Step7 Comm+, OPC UA, MELSEC.
- Added support for RFC 5424 formatted syslog messages.
- Added a Default Action Log to Layer 3-7 Policy.
- Added support for 2.5G SFP modules.

## Enhancements

- Added Syslog as a Registered Action for the VRRP State Changes event notification.
- Added syslog as a Registered Action for the Fiber Check Warnings event notification.
- Error logs for failed configuration imports now show more details.
- Users can now select multiple inbound interfaces for Static Multicast Routes within same group address.
- Added error logs for the DHCP function.
- Added error logs for the IGMP function.
- Added support for Modbus DPI protocols in the CLI.

## Bugs Fixed

- The port-based DHCP server incorrectly assigns duplicate IP addresses to bridge ports.
- RSTP incorrectly assigns multiple devices as the root.
- Users are only able to configure or import one Static Multicast entry through the CLI.
- SNMP OIDs including the "newline" character returns an error.
- Importing configurations containing SNTP/NTP server or SNTP client settings results in an error.
- The NAT function does not work properly after rebooting the device.
- The PRP traffic function for MTU configuration does not work properly.
- The firewall pop-up window remains visible after the system automatically logs out.
- IEEE 802.1X authentication for the RADIUS server would fail.
- Vulnerability: CVE-2024-9137
- Vulnerability: CVE-2024-9139
- Vulnerability: CVE-2024-1086
- The connection status of the OpenVPN Client function shows incorrectly.

## Changes

- Increased the maximum password and share key length to 64 characters for user accounts, IPsec, L2TP server, SNMP, IEEE 802.1X, RADIUS server, and TACACS+ server.
- Added support for special characters in passwords and shared keys for user accounts, IPsec, L2TP server, SNMP, IEEE 802.1X, RADIUS server, and TACACS+ server.

## Notes

N/A





<b>Version: v3.12.1</b>	<b>Build: 24082116</b>
<b>Release Date: Aug 26, 2024</b>	

### **Applicable Products**

N/A

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

N/A

### **Bugs Fixed**

- Unsupported or unavailable features appear in the web interface.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v3.12</b>	<b>Build: 24073101</b>
<b>Release Date: Aug 02, 2024</b>	

## Applicable Products

N/A

## Supported Operating Systems

N/A

## New Features

- Added support for the Loopback Interface function.
- Added support for the OpenVPN Client function.
- Added support for the Netflow function.
- Added support for event-triggered actions to the VRRP function.
- Added support for UDP-Flood to the DoS Policy function.
- Added SNMP Trap as a Log Destination for the Layer 2 Policy function.
- Added support for additional event log export formats: .pdf, .csv.

## Enhancements

- Enhanced the following IPsec algorithms.
  - Encryption: AES-256-GCM
  - Hash: SHA-512
  - DH Group: DH15 (modp3072), DH16 (modp4096), DH17 (modp6144), DH18 (modp8192), DH22 (modp1024s160), DH23 (modp2048s224), DH24 (modp2048s256), DH31 (curve25519)
  - PRF: PRF SHA-256, PRF SHA-384, PRF SHA-512

## Bugs Fixed

- The "Login Authentication Failure Message" does not save properly.
- Using the newline character (\n) in the 'Login Message' and 'Login Authentication Failure Message' causes abnormalities in the output.
- The system is unable to ping the VRRP virtual IP.
- Users are able to bypass password policy violation warnings by pressing ESC on the keyboard.
- Time zone settings are not saved if GMT is set to 0.
- Vulnerability: CVE-2024-6387.

## Changes

- Changed the IPS license expiration behavior: When the license expires, IPS functionality will now remain enabled, but the IPS patterns will no longer be updated.
- Changed the Trusted Access behavior: Trusted Access now applies to the Web UI, CLI, and New Moxa Command interfaces.
- Changed the Preempt Delay range for the VRRP function from 10 to 300 to 0 to 300

## Notes

N/A



<b>Version: v3.10</b>	<b>Build: 24070315</b>
<b>Release Date: Jul 26, 2024</b>	

**Applicable Products**

N/A

**Supported Operating Systems**

N/A

**New Features**

First release.

**Enhancements**

N/A

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A