# Firmware for EDR-8010 Series Release Notes

| Version: v3.28 | Build: 26070918 |
| --- | --- |
| Release Date: Jul 16, 2026 | |

## Applicable Products

EDR-8010 Series

## Supported Operating Systems

N/A

## New Features

• Added 802.1ad VLAN mode.
• Added VXLAN support.
• Added 2-Factor Authentication.
• Added High Availability redundancy protocol.
• Added LDAP support.
• Supports multicast routing without changing TTL using CLI commands.
- "ip mroute udp-ttl-nochange" (Do not decrement the TTL of UDP multicast routed packets).
- "no ip mroute udp-ttl-nochange" (Decrement the TTL of UDP multicast routed packets [default]).
- "show ip mroute udp-ttl-nochange" (Display the current TTL no-change setting).

## Enhancements

• Add EAP-TLS and PEAP-MSCHAPv2 support for 802.1X Local Authentication Security.
• Added interface option to Trusted Access settings.
• Added granular DoS protection based on destination IP and service port, with configurable thresholds and action modes.
• Added custom threshold configuration and alarm notifications for fiber port TX/RX and temperature to Fiber Check.
• Support restricting primary/secondary/tertiary DNS servers from being set to the same IP address.
• S7comm DPI now converts difficult protocol codes into clear, user-friendly operation names.
• OPC UA provides predefined OPC UA profiles and objects that group required service codes by common operations.
• Added optional Strict Protection mode to DPI-EIP/CIP.

## Bugs Fixed

• MXsecurity fails to backup/restore configuration.
• The configurable System Time year range is different between the Web and CLI.
• Incorrect DHCP pool exhaustion event log may be generated.
• IPS licenses cannot be applied through MXsecurity in some conditions.
• Unexpected Ping Response rules may generate when importing a configuration without Ping Response settings.
• Abnormal OSPF with GRE interface.
• Incorrect user-facing text on session expiration dialog title and button.
• Intermittent failure of SFP fiber link.

## Changes

• USB /ABC-02 function now enabled by default.

## Notes

• CLI usage instructions for multicast routing without changing TTL.

- ip mroute udp-ttl-nochange
  Mode: Global Configuration (config)#
- no ip mroute udp-ttl-nochange
  Mode: Global Configuration (config)#
- show ip mroute udp-ttl-nochange
  Mode: Privileged EXEC #

| Version: v3.24.13 | Build: 26061114 |
| --- | --- |
| Release Date: Jun 17, 2026 | |

## Applicable Products

EDR-8010 Series

## Supported Operating Systems

N/A

## New Features

N/A

## Enhancements

N/A

## Bugs Fixed

• When a bridge interface and NAT N-to-1 are enabled and simultaneously in use in the same environment, connecting a computer to the bridge port causes abnormal router behavior.
• Directed forwarding does not work after a reboot.
• MXsecurity fails to backup/restore configuration.

## Changes

N/A

## Notes

N/A

| Version: v3.24 | Build: 26041517 |
| --- | --- |
| Release Date: Apr 18, 2026 | |

## Applicable Products

EDR-8010 Series

## Supported Operating Systems

N/A

## New Features

• Added relay control actions for firewall events.
• Added support for establishing IPsec connections using domain names.

## Enhancements

• RSA key supports 3072- and 4096-bit key length for Certificate Signing Request function.
• The login message supports comma characters.
• The System Event Summary supports displaying the number of events in the last 24 hours.
• VLAN/LAN number expansion.
• Object Management supports FTP Passive mode.
• Supports creating SNMP accounts.
• Supports Object Grouping.
• Supports identification of embedded CIP command type (Service Code) in EIP traffic.

## Bugs Fixed

• Intermittent ping loss during link-down events.
• TACACS does not work when using FW v3.21 and later.
• MAC-table VLAN sorting non-functional.
• SNMPv3 fails after importing the configuration.
• FTP communication fails using LF newline characters.
• CVE-2026-3867 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-261521.
• CVE-2026-3868 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-261521.

## Changes

• IPSec supports LAN interface connections.

## Notes

N/A

| Version: v3.23 | Build: 25123121 |
| --- | --- |
| Release Date: Jan 09, 2026 | |

## Applicable Products

EDR-8010 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.
- Link-up failure after device reboot.
- Turbo Chain fails after importing the configuration file to the head.
- 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.
- Using the wizard to configure all ports to bridge mode deletes VLAN 1.
- Cannot get up-to-date SNMP OID values through SNMP.
- Unexpected Turbo Ring v2 topology changes.
- 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

| Version: v3.22 | Build: 25102916 |
| --- | --- |
| Release Date: Nov 11, 2025 | |

## 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

• Port Trunking does not work properly.

## Changes

N/A

## Notes

N/A

| Version: v3.21 | Build: 25100115 |
| --- | --- |
| Release Date: Oct 03, 2025 | |

## 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

• Expanded the number of bridge zones to eight sets.

## Bugs Fixed

• WAN interface IP address abnormality after reboot in NAT 1-to-1 mode.
• 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.
• System time was incorrect after importing configuration.

## Changes

• Changed the behavior of user account password modification.

## Notes

N/A

| Version: v3.20 | Build: 25082113 |
| --- | --- |
| Release Date: Aug 27, 2025 | |

## 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

| Version: v3.19 | Build: N/A |
| --- | --- |
| Release Date: Jul 31, 2025 | |

## Applicable Products

N/A

## Supported Operating Systems

N/A

## New Features

• Added SMTPS support in email settings.
• Added support for LACP protocol.
• 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

| Version: v3.17 | Build: 25032717 |
| --- | --- |
| Release Date: Apr 02, 2025 | |

## Applicable Products

N/A

## Supported Operating Systems

N/A

## New Features

• Added Traceroute CLI command.
• Introduced multi-language support for MX-ROS, including Traditional/Simplified Chinese, Korean, and Japanese.
• Added GRE interface on Network Interface.

## Enhancements

• Extended Multi-WAN support to accommodate up to 4 WAN connections.
• Added Object types: Secure FTP and SYSLOG (TCP 514) to Object Management.
• Added Offline IDS mode to IPS.
• Added trap and syslog support for IPS/DPI/ADP to Advanced Protection - Configuration.
• Optimized IPsec reconnection time.

## Bugs Fixed

• Bridge topology change packets are not properly bypassed, causing increased Turbo Chain recovery time.
• Web UI fails to disable SFP, leaving link status active.
• Multicast traffic is not filtered correctly, causing forwarding to ports that have not joined the IGMP group.
• IPsec Startup Mode - Initiate Automatically does not function properly.
• “Log Service Ready Log Handler” repeatedly reports messages after enabling notification in System log.
• CVE-2025-0415 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-259491.
• CVE-2025-0676 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-251431.

## Changes

• Supervisor and user accounts are no longer created by default, and must be added manually. Existing accounts are not affected.

## Notes

Small amounts of packet loss may occur when two identical EDR-8010 devices are connected via Static Routes. Instead of using a Static Route, configure the route as a Gateway from WAN settings.

| Version: v3.14 | Build: 24123112 |
| --- | --- |
| Release Date: Dec 31, 2024 | |

## Applicable Products

N/A

## 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.
• ARP Reply packets are being unintentionally dropped in Bridge mode.
• Email Settings cannot be disabled.
• After changing the Management VLAN, the router is unreachable when pinged.
• When configuring Bridge members, the system unintentionally creates two untagged VLANs under the access port.
• 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.

| Version: v3.13.1 | Build: 24111415 |
| --- | --- |
| Release Date: Nov 18, 2024 | |

## 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

| Version: v3.13 | Build: 24100800 |
| --- | --- |
| Release Date: Oct 09, 2024 | |

## 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.

## 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

| Version: v3.12.1 | Build: 24082116 |
| --- | --- |
| Release Date: Aug 26, 2024 | |

## 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

| Version: v3.12 | Build: 24073101 |
| --- | --- |
| Release Date: Aug 02, 2024 | |

## 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 maximum supported number of tunnels shown at the bottom of the IPsec Settings page is incorrect.
• 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

| Version: v3.6 | Build: 24032802 |
| --- | --- |
| Release Date: Apr 03, 2024 | |

## Applicable Products

N/A

## Supported Operating Systems

N/A

## New Features

• Added Turbo Chain support for Layer 2 Redundancy.

## Enhancements

• Modified the DoS policy for Flood Protection to allow independent limit ranges for each interface.

## Bugs Fixed

• Restoring the device configuration may fail under specific circumstances.
• The allowed characters for the Password Policy are shown incorrectly.

## Changes

N/A

## Notes

N/A

| Version: v3.3 | Build: 24010416 |
| --- | --- |
| Release Date: Jan 12, 2024 | |

## Applicable Products

N/A

## Supported Operating Systems

N/A

## New Features

• Added support for TACACS+ authentication.
• Added Port Disable ingress action for Rate Limit function.
• Added support for LAN ID to DHCP option 82 in the DHCP relay agent.
• Added support for Proxy ARP for LAN interfaces.

## Enhancements

• Increased the maximum username length to 32 characters for local account, SNMP, RADIUS, and IEEE 802.1X authentication.
• Increased the maximum length length of passwords, communities, and shared keys to 64 characters for local account, SNMP, RADIUS, and IEEE 802.1X authentication.
• Unified the range of supported special characters for local account, SNMP, RADIUS, and IEEE 802.1X.

## Bugs Fixed

• The STATE LED behaves abnormally when no event notifications have been triggered.
• Users are unable to access the web console if their login passwords includes "$$".
• Units are incorrectly displaying as “packets” on the vertical axis of network statistics.
• Network statistics values are inaccurate when using ports for measurement.

## Changes

N/A

## Notes

N/A

| Version: v3.1 | Build: 23090419 |
| --- | --- |
| Release Date: Sep 20, 2023 | |

## 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