Firmware for EDF-G1002-BP Series Release Notes

Version: v3.23	Build: 25123121
Release Date: Jan 12, 2026	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

- Added Neighbor MAC Change events.
- Added Connection Management.

Enhancements

- SNMP/SNMP Trap supports SHA-256 and SHA-512 authentication.
- Tech Support File allows users to generate and import files for troubleshooting.
- Ping tool supports selecting source 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.
- 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)

Changes

- When relay activates, the STATE LED also triggers.

Notes

N/A

Version: v3.21.1	Build: 25102020
Release Date: Oct 27, 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

N/A

Changes

N/A

Notes

N/A

Version: v3.21	Build: 25100115
Release Date: Oct 06, 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

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

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.
- Protocol Filtering was not functioning properly.

Changes

N/A

Notes

N/A

Version: v3.19	Build: 25071510
Release Date: Jul 31, 2025	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

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

Enhancements

• VLAN packet filtering support.

Bugs Fixed

• 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 01, 2025	

Applicable Products

EDF-G1002-BP Series

Supported Operating Systems

N/A

New Features

• Added support for the Traceroute CLI command.
• Added support for the following additional languages for MX-ROS: Traditional/Simplified Chinese, Korean, Japanese.

Enhancements

• 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.
• Added support for Bridge Firewall Filter for Turbo Chain heads/tails.

Bugs Fixed

• Multicast traffic is not filtered correctly, causing forwarding to ports that have not joined the IGMP group.
• 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

N/A

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

Applicable Products

EDF-G1002-BP Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• 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.

Bugs Fixed

• When exporting the configuration, the Object IP Range setting is saved incorrectly, causing importing the configuration to fail.
• MXview 1.4.1 does not receive encrypted SNMPv3 Trap/Inform packets from the firewalls.
• 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

N/A

Notes

• (Known issue) The Bandwidth Utilization widget in Network Statistics does not display correctly, A fix is expected in Q2, 2025.

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

Applicable Products

EDF-G1002-BP Series

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

EDF-G1002-BP Series

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

• Error logs for failed configuration imports now show more details.
• Added support for Modbus DPI protocols in the CLI.

Bugs Fixed

• SNMP OIDs including the "newline" character returns an error.
• Importing configurations containing SNTP/NTP server or SNTP client settings results in an error.
• 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

Changes

• Increased the maximum password and share key length to 64 characters for user accounts, SNMP, IEEE 802.1X, RADIUS server, and TACACS+ server.
• Added support for special characters in passwords and shared keys for user accounts, 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 01, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for the Netflow 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

• Changed the Trusted Access behavior: Trusted Access now applies to the Web UI, CLI, and New Moxa Command interfaces.

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.
• 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

N/A

Notes

N/A

Version: v3.10	Build: 24070315
Release Date: Jul 26, 2024	

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