IMPULSE

IEC 62443-4-2 Hardening Checklist for MX-NOS / MX-ROS

This guide summarises nine key hardening actions for Moxa MX-NOS and MX-ROS devices to help support IEC 62443-4-2 Security Level 2 alignment.

In industrial networks, switches, routers and other infrastructure devices play a critical role in maintaining secure and reliable communication between systems. If these devices are left with default settings, unnecessary services or weak access controls, they can introduce avoidable security risks into the wider network.

The actions outlined below are designed to reduce unauthorised access, strengthen authentication, improve monitoring, limit insecure services and protect exported configuration data.

1

Change Default Credentials & SNMP Community Strings

Default administrator credentials and SNMP community strings are widely known and should be replaced during device provisioning to prevent easy unauthorised access.

Password: System > Account Management > User Accounts

SNMP: System > Management Interface > SNMP

ACTION Create a new administrator account with a strong password, remove or rename the default account, replace default SNMP community strings, and use SNMPv3 where possible.

2

Configure SNMP Traps or a Syslog Server

Sending event, fault and security logs to a separate monitoring server improves visibility and helps ensure suspicious activity is detected and investigated.

SNMP Trap: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform

Syslog: Diagnostics > Event Logs and Notifications > Syslog

ACTION Configure the device to send SNMP traps and/or Syslog messages to an approved central monitoring or logging server.

3

Enable Trusted Access

Trusted access restricts device management access to approved IP addresses or subnets, reducing the chance of unauthorised systems reaching the management interface.

Enable trusted access: Security > Device Security > Trusted Access

ACTION Define the permitted management hosts or subnets and block access from all other network addresses.

4

Enable Automatic Logout

Automatic logout closes inactive management sessions, reducing the risk of unattended or forgotten sessions being used by unauthorised users.

Enable auto logout: Security > Device Security > Login Policy

ACTION Keep auto logout enabled and set an appropriate inactivity timeout; do not set the timeout value to 0.

IMPULSE

T: +44 (0)1782 337800 **E:** sales@impulse-embedded.co.uk
F: +44 (0)1782 337801 **W:** www.impulse-embedded.co.uk

IMPULSE

IEC 62443-4-2 Hardening Checklist for MX-NOS / MX-ROS

5

Enforce Password Strength & Complexity

Password complexity rules help protect the device against weak passwords and reduce the effectiveness of brute-force and guessing attacks.

Enable password strength and complexity checks: System > Account Management > Password Policy

ACTION Enforce strong password requirements, including a minimum length of 12 characters with uppercase, lowercase, numeric and special characters.

6

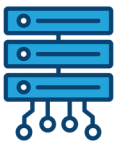
Enable Login Failure Lockout

Login failure lockout limits repeated authentication attempts and helps prevent attackers from making unlimited password guesses.

Enable account login failure lockout period: Security > Device Security > Login Policy

ACTION Configure a lockout policy, such as locking access after three failed login attempts for a defined period, and ensure the device time is correct.

7



Disable Unused & Insecure Services

Unused ports and insecure management services increase the device attack surface and should be disabled unless they are required for operation.

Physical ports: Network Configuration > Ports > Port Settings

Management interfaces: System > Management Interface > User Interface

ACTION Disable unused ports and turn off insecure management interfaces such as HTTP and Telnet, using secure alternatives such as HTTPS and SSH where available.

8

Set a Login Banner Message

A login message informs users that the device is protected, identifies authorised use requirements and provides a clear warning before access.

Set a login message: Security > Device Security > Login Policy

ACTION Configure a login banner stating system ownership, authorised-use conditions and that unauthorised access is prohibited.

9

Enable Configuration File Encryption

Encrypting exported configuration files helps protect sensitive device settings and credentials if a backup file is lost, copied or stolen.

Enable config file encryption: System > System Management > Configuration Backup and Restore

ACTION Enable configuration file encryption and protect exported backups with a strong encryption password.

These hardening actions provide a practical security baseline for MX-NOS & MX-ROS devices.

They should be applied during commissioning and reviewed regularly to help maintain secure operation and continued alignment with IEC 62443-4-2 expectations.

IMPULSE

T: +44 (0)1782 337800 **E:** sales@impulse-embedded.co.uk
F: +44 (0)1782 337801 **W:** www.impulse-embedded.co.uk