

Dear Valued Customer,

We would like to inform you that Moxa Industrial Linux 4.0 (MIL4), based on Debian 13 and Linux kernel 6.12 for the UC-1200A, UC-2200A, UC-3400A, and UC-4400A Series will be available for order through the Configure-to-Order System (CTOS) starting **April 1, 2026**.

Please review the details below to understand how these changes may affect your products and operations.

Impact on Your Current Ordering Method

The release of MIL4 will not replace MIL3. Instead, MIL4 will be offered as an additional OS option.

For example, if you order UC-2222A-T-US, which currently comes preloaded with MIL3, it will continue to ship with MIL3 by default.

If you prefer to receive the system with MIL4, you can select MIL4 as the operating system through the Configure-to-Order System (CTOS). The device will then be shipped with MIL4 preinstalled.

How to order UC Computers with MIL4

To order UC computer series that support MIL4, please select the corresponding CTOS model name listed below. Through the Configure-to-Order System (CTOS), a configuration menu will be available that allows you to choose your preferred MIL version and security type.

- **MIL4 Standard** complies with RED-DA requirements and is JC-STAR Level 1 certified.
- **MIL4 Secure** provides additional security features and complies with IEC 62443-4-2 Security Level 2.

Product Series	Model Name in CTOS
UC-1200A Series	UC-1200A (CTO)
UC-2200A Series	UC-2200A (CTO)
UC-3400A Series	UC-3400A (CTO)
UC-4400A Series	UC-4400A (CTO)

How to upgrade a UC Computer with MIL3 to MIL4

If you would like to upgrade an existing UC computer running MIL3 to MIL4, you can do so using one of the following methods:

1. Reflash using the MIL4 system image

Download the MIL4 image file from the [UC product page](#) and follow the instructions in the MIL4 User Manual

to reflash the system with the MIL4 image through the bootloader menu.

2. Backup and restore from a MIL4 system

Obtain a UC computer that already has MIL4 installed, create a system backup and restore the image to another UC computer of the same model.

Please refer to Chapter 7: Backup, Decommission, and Recovery in the MIL4 User Manual for detailed instructions.

Note:

- Upgrade is supported only between the same security types:
 - MIL3 Standard → MIL4 Standard
 - MIL3 Secure → MIL4 Secure
- Cross-type upgrades between Standard and Secure version are not supported.

For example:

- Devices running MIL3 Standard cannot be upgraded to MIL4 Secure. A new device with MIL4 Secure must be purchased.
- Devices running MIL3 Secure cannot be upgraded to MIL4 Standard. A new device with MIL4 Standard must be purchased.

What Are the Changes in Moxa Industrial Linux 4.0 (MIL4)

This is the first release of MIL4. MIL4 is based on Debian 13 and Linux kernel 6.12. All Moxa proprietary tools remain compatible between MIL3 and MIL4, including major components such as MCM (Moxa Network Manager), MSM (Moxa System Manager), and MCIM (Moxa Computer Interface Manager).

To help you migrate your software from MIL3 (Debian 11, kernel 5.10), the changes listed below are based on a comparison between MIL4 and the latest MIL 3.4 release.

In addition, a MIL3 (Debian 11) to MIL4 (Debian 13) Migration Guide is available in the MIL4 User Manual.

New Features

- Moxa System Manager (MSM)
 - Introduces a file-exclusion feature that allows users to omit specific files from backups (for example, device-unique keys).
- Moxa Connection Manager (MCM)

- Adds support to lock the cellular connection to a specific mobile carrier
- Enables bash auto-completion (tab) for MCM CLI commands.

Enhancements

- Moxa System Manager (MSM)
 - Supports bash-completions so that "mx-system-mgmt" can automatically prompt options, making the tool easier to use.
 - SSH host keys are no longer included in backups by default, ensuring each restored device retains a unique SSH server key.
 - When system-failback is disabled, the existing system replica is now removed to prevent unnecessary storage usage.
- Moxa Connection Manager (MCM)
 - Enhances network failover performance by updating the default WAN failover behavior so that backup WAN interfaces remain connected and periodically ping a configurable target host to proactively verify connectivity and reduce failover time.
 - Ensures device synchronization with gpsd occurs only when the gpsd service is active.
 - Shows 'dummy0' in the routing table only when an interface is managed.
 - Displays 'Unknown' instead of 'Disabled' as the status for unmanaged interfaces to avoid confusion in the MCM CLI.
 - Adds the ability to preserve the local IPv6 address when the Ethernet connection is disconnected.
- Network intrusion detection system
 - Replaced Zeek with Suricata as the default intrusion detection system to provide improved performance, broader protocol detection capabilities, and active community support.

Bugs Fixes:

- Moxa Connection Manager (MCM)
 - GPS toggling did not retry to connect to Telit LE910C4-WWXd modules when no GPS data was received.
 - An issue of the MCM hanging when the service is restarted upon reload timeout.
 - Abnormal DHCP server termination by adding a retry mechanism.
 - An issue whereby cellular time synchronization operates independently of GPS port binding.

Changes:

- Moxa Connection Manager (MCM)
 - MCM no longer manages LAN interfaces (end0) by default. All LAN ports are now consistently managed by NetworkManager, replacing the mixed management behavior in MIL3.
 - Changes default WAN failover behavior: backup WAN interfaces now remain connected and periodically ping a configurable target host to check that the connection is alive.

- Enables 'keep alive (connection.always-keep-alive)' on all WAN interfaces by default
- Changes the default Cellular IP method (ip-method) from ipv4 to ipv4v6.
- Restricts the 'failback.enabled' setting to only the value 'true'.
- Ensures device synchronization with gpsd service occurs only when the service is active.
- Updated LTE cellular signal strength indicator from a 5-level scale to a 4-level scale (None/Very Poor, Poor, Fair, Good) for a unified Moxa product experience.
- Renames the 'Enabled/Managed' field to 'Managed' in the MCM CLI for better readability.
- Renames the bridge interface to 'Bridge-LAN' in the MCM CLI (previously 'LAN').
- Moxa Computer Interface Manager (MCIM)
 - Stops creating symbolic links for serial ports such as ttyM0, ttyM1.
 - Removes deprecated button and DIO management commands from the CLI help menu. These commands were supported to maintain backward compatibility.
- Network Interface Naming
 - Updated network interface naming from legacy eth0 / eth1 to predictable, system-derived names (e.g., end0, end1) in MIL4 (Debian 13).
- Firewall Framework
 - Changed the default firewall management framework to firewalld.
 - The nftables package remains installed but is disabled by default.
- Boot Management Tool
 - Unified boot management tools into a single utility named moxa-boot-manage replaces platform-specific tools (moxa-bootloader-manager and moxa-bios-manager).
- MIL Base System
 - Configured systemd-journald to run in volatile mode (Storage=volatile), keeping logs in memory only to reduce disk usage and slightly improve performance.
 - The /tmp folder is now mounted as a memory-backed tmpfs by default in Debian 13, improving performance and reducing disk usage. Systems requiring a persistent /tmp can disable this behavior.
 - Changed MIL version format from 2-digit (x.y) to 3-digit (x.y.z).
 - Changed APT source configuration from the traditional /etc/apt/sources.list format to DEB822-style source files under /etc/apt/sources.list.d/.
 - Removed legacy Diffie-Hellman-based SSH key exchange algorithms to address CVE-2002-20001 and improve cryptographic security.

If you have any questions, please contact George Hsiao (georgey.hsiao@moxa.com), or contact your regional sales representative.