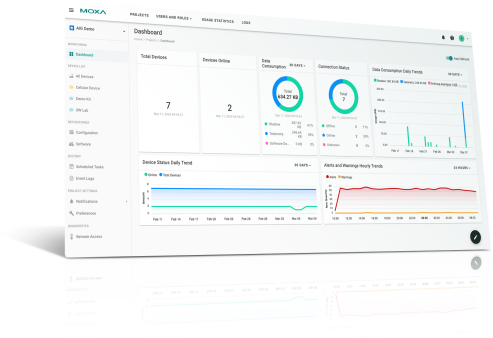
Moxa DLM (on-premises)

Self-hosted DLM that can be install on servers or cloud VMs for full ownership of data along with monitoring and management capabilities

Preliminary



Features and Benefits

- Unified web command center for your device fleet
- Instant visibility into device health
- One-click remote diagnostics and troubleshooting
- Smart connectivity optimization
- Fleet-wide script and software rollout orchestration
- Proactive intelligence on risk management
- Secure access and governance on premises
- Total data sovereignty
- Seamless IT/OT ecosystem integration

Introduction

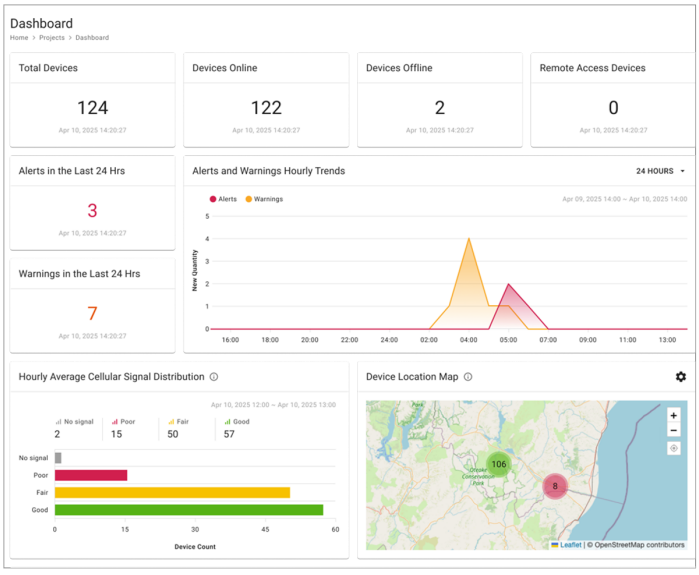
Moxa DLM (on-premises) is a self-hosted device life cycle management platform designed for managing large fleets of Moxa cellular devices deployed across remote and distributed sites. It brings fleet-wide visibility, software distribution, configuration management, and secure remote access together in a single web console.

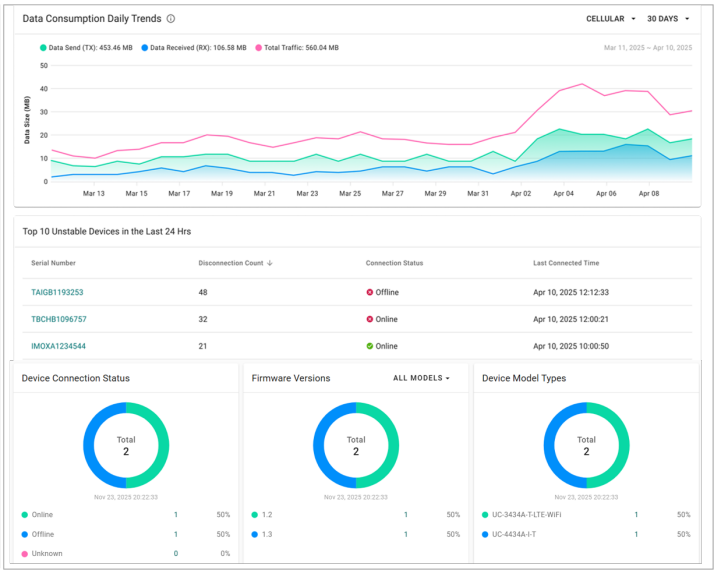
By centralizing daily operations—such as monitoring device health, optimizing cellular connectivity, and automating software rollouts—DLM helps system integrators, asset owners, and service providers reduce site visits, standardize deployments, and keep critical IoT applications running reliably, all this while maintaining full control of data inside their own IT environment.

Real-time Operations Command Center

The DLM dashboard gives operators an overview of their entire deployment in one place.

- View how many devices are online/offline, which projects they belong to, and where they are installed
- Review warnings and alerts from the past 24 hours to quickly spot problem areas
- Visualize cellular signal quality, data usage trends, and device distribution so teams can focus on the fleets, sites, or regions that need attention



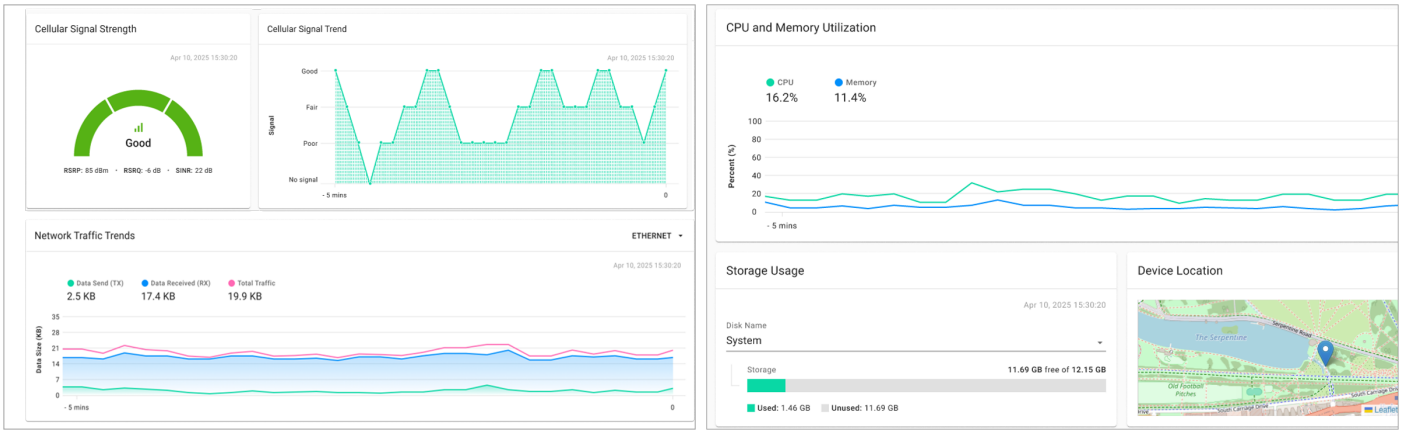


Proactive Device Health Diagnostics

With the DLM Agent running on Moxa cellular devices, key information is continuously reported back to the DLM server, including:

- System health (CPU, memory, disk usage)

- Cellular performance (RSRP, RSRQ, SINR, serving cell information)
- Device configuration and connectivity status



Secure Remote Troubleshooting

DLM provides secure browser-based remote access to registered devices without exposing their services directly to the internet. The highlights include:

- Secure VPN tunnel for one-click, browser-based SSH access
- Diagnose issues, check logs, and fix devices remotely—no site visits
- All remote sessions are fully logged for security and compliance

Intelligent Risk Alert System

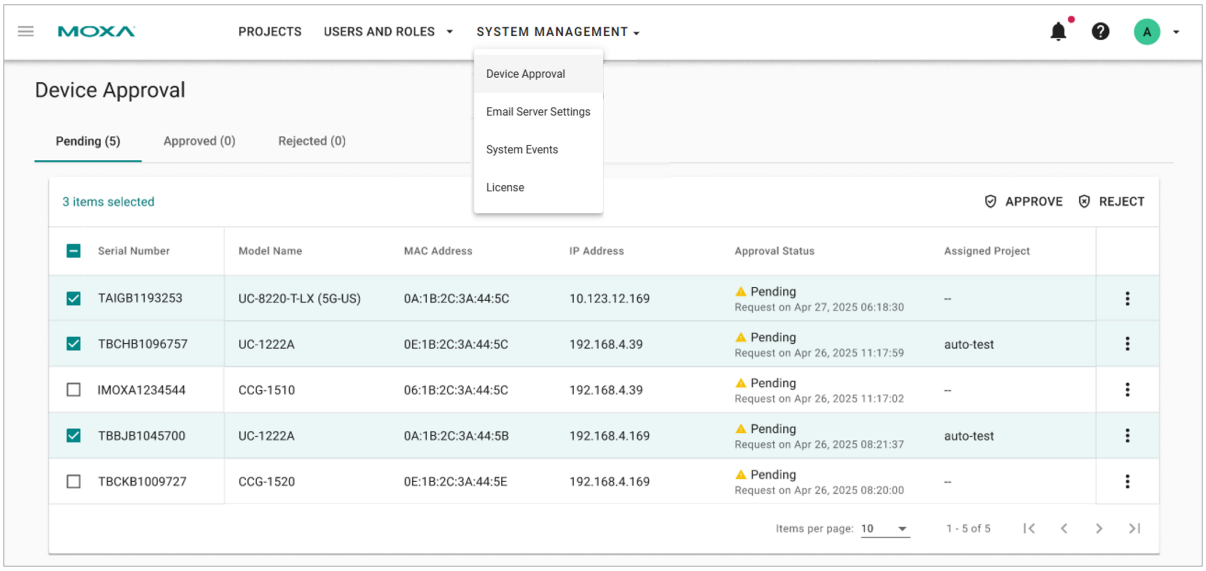
Events generated by the DLM platform or reported by devices are centrally collected and correlated. You can configure who gets notified and how. For example:

- Send email alerts to operations teams when critical thresholds are exceeded (e.g., device offline, weak cellular signal, disk health issues, high disk usage)

Enterprise-grade Security

DLM (on-premises) is built to support secure, controlled management of industrial devices in production environments. Key security capabilities include:

- Per-device X.509 certificates with secure MQTT and HTTPS/TLS communication
- Role-based access control to limit privileges and reduce risks
- Comprehensive audit logs for registrations, approvals, remote access, and changes
- Self-hosted deployment so all telemetry and management data stay under your control



Specifications

Hardware Requirements

CPU	Minimum Requirement: 4 vCPU (Intel® Pentium® G4600) tested on VMware with 1,000 devices Recommended: 8 vCPU (Intel® Xeon® Silver 4310) tested on VMware with 3,000 devices
RAM	4 GB (1,000 devices) 16 GB (3,000 devices)
Hardware Disk Space	100 GB (HDD/SSD, 1,000 devices) 500 GB (HDD/SSD, 3,000 devices)
OS	Ubuntu 20.04 LTS Ubuntu 22.04 LTS (64-bit)

System Requirements

Eligible Devices	UC-1200A / UC-2200A (MIL 3.4.1, image v1.4 or later) UC-3400A (MIL 3.4.1, image v1.2 or later) UC-4400A (MIL 3.4.1, image v1.3 or later) UC-8200 (MIL 3.4.1, image v1.5 or later) UC-8600A Series (MIL 4.0, image v1.0 or later)
Servers	SMTP email server: Supports STARTTLS (optional) or unencrypted SMTP f for sending event notifications File server (optional): External HTTPS file servers are recommended for hosting large OTA packages

Network Requirements

Ports	TCP 443: DLM web interface (HTTPS) TCP 8883: Secure MQTT from UC devices (TLS-RSA) TCP 50001 to 50010: Remote Connect (SSH over VPN, up to 10 sessions)
Internet	Required for installing DLM and accessing external package repositories
Interface Management	Cellular/Wi-Fi interfaces on the devices must be managed by Moxa Connection Manager (MCM) for full functionality
Time Synchronization	NTP DLM server and devices must be able to reach an NTP server to enable accurate time synchronization for TLS, logs, and tokens
Domain Name	FQDN Recommended to ensure certificate and login stability. At a minimum, the DLM server must have a static IP address

Ordering Information

Model Name	License Term	No. of Device Nodes Supported	How to Order
LIC-DLM-ONPREM-NEW-XN-SR	Perpetual	Customizable, minimum 1 node	Qty in one line item is combined (e.g., Qty 2 = one license with 2 nodes). Use separate line items for multiple licenses
LIC-DLM-ONPREM-NEW-XN-SR-50	Perpetual	Customizable, minimum 50 nodes	Qty in one line item is combined (e.g., Qty 2 = one license with 100 nodes). Use separate line items for multiple licenses.
LIC-DLM-ONPREM-NEW-XN-SR-500	Perpetual	Customizable, minimum 500 nodes	Qty in one line item is combined (e.g., Qty 2 = one license with 1,000 nodes). Use separate line items for multiple licenses.
LIC-DLM-ONPREM-NEW-XN-SR-3000	Perpetual	Customizable, minimum 3000 nodes	Qty in one line item is combined (e.g., Qty 2 = one license with 6,000 nodes). Use separate line items for multiple licenses.