Moxa DLM On-premises User Manual

Version 1.1, July 2026

www.moxa.com/products

Moxa DLM On-premises User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

Overview

Moxa self-hosted DLM service is a centralized platform designed by Moxa to efficiently manage and monitor Moxa devices in the local network. With features for centralized monitoring, software updates, and remote access, the DLM service simplifies operations for IoT applications. By reducing management efforts and ensuring security, the DLM service enhances the efficiency and effectiveness of IoT deployments.

The Moxa self-hosted DLM service will hereafter be referred to as the "DLM service".

System Requirements

Server Hardware

	Minimum (for up to 1,000 devices)	Recommendation (for up to 3,000 devices)
CPU	4 cores (x86 64 bit)	8 cores (x86 64 bit)
Memory	4 GB	16 GB
Storage	100 GB (HDD or SSD)	500 GB (HDD or SSD)
Tested With (specifications)	4 vCPU (Intel® Pentium® G4600) tested on VMware with 1,000 devices	8 vCPU (Intel® Xeon® Silver 4310) tested on VMware with 3,000 devices

Device (client) Hardware

- UC-1200A Series
- UC-2200A Series
- UC-3400A Series
- UC-4400A Series
- UC-8200 Series
- UC-8600A Series

Software

- **DLM Server:** Ubuntu 20.04, 22.04, 24.04
- **DLM Agent:** Moxa Industrial Linux (MIL) version v3.4.1 and higher
- **Docker: docker-ce** ≥ 26.0.0 or **docker.io** ≥ 20.10.24 (either one is required).
  Note: **docker.io** is pre-installed on Ubuntu.

UC Series	MIL 3.4 OS Image Version	MIL 4.x OS Image Version
UC-1200A	v1.4 or later	v1.0 or later
UC-2200A	v1.4 or later	v1.0 or later
UC-3400A	v1.2 or later	v1.0 or later
UC-4400A	v1.3 or later	v1.0 or later
UC-8200	v1.5 or later	v1.0 or later

NOTE

- Actual capacity of DLM depends on factors such as device reporting intervals and the number of scheduled tasks. The specifications listed in the table are tested configurations for reference and sizing.
- DLM has no fixed device limit. Larger deployments may require high-performance hardware (more vCPUs, memory, and storage) to ensure stable operations.

Networking Requirements

1. Public Internet is required for installing DLM software.
2. The cellular and Wi-Fi interfaces on a Moxa computer must be managed by the Moxa Connection Manager (MCM) utility.
3. An NTP server must be reachable to ensure accurate system time synchronization.
4. Accurate time is required for secure communication, log correlation, certificate validation, and DLM agent/server operations.

WARNING

Moxa cannot guarantee the full functionality of the DLM service if the interfaces are managed by other network management software and not the MCM tool.

5. Ports used by the DLM service.

Port	Purpose
TCP 443	DLM web interface
TCP 8883	Secure MQTT connection from DLM Devices (**UC Series**) to DLM server using TLS-RSA
TCP 8884	Secure MQTT connection from DLM Devices (**OnCell** and **EDR Series**) to DLM server using TLS-PSK
UDP 5688	Secure LwM2M connection from **CCG Series** devices to DLM server (using DTLS)
UDP 5788	Secure LwM2M connection from **CCG Series** devices to DLM bootstrap server (using DTLS)
TCP 50001 to 50010	Remote connection service Remote access to the console of the connected devices, enabling interaction with the devices through a command line interface (CLI).

Domain Name: A valid domain name is required to issue certificates between devices and the server.

NOTE

If a specific device is not used in your DLM deployment, its corresponding ports may remain blocked at the firewall to help minimize the system's attack surface.

Email and File Servers

- **SMTP Server for Email Notifications**

  To enable email notifications, Moxa DLM service requires an SMTP server to send messages to users or administrators. The DLM server communicates with the SMTP server to deliver notifications about events such as firmware updates or system alerts. Ensure the DLM server has network connectivity to the SMTP server for reliable operations.

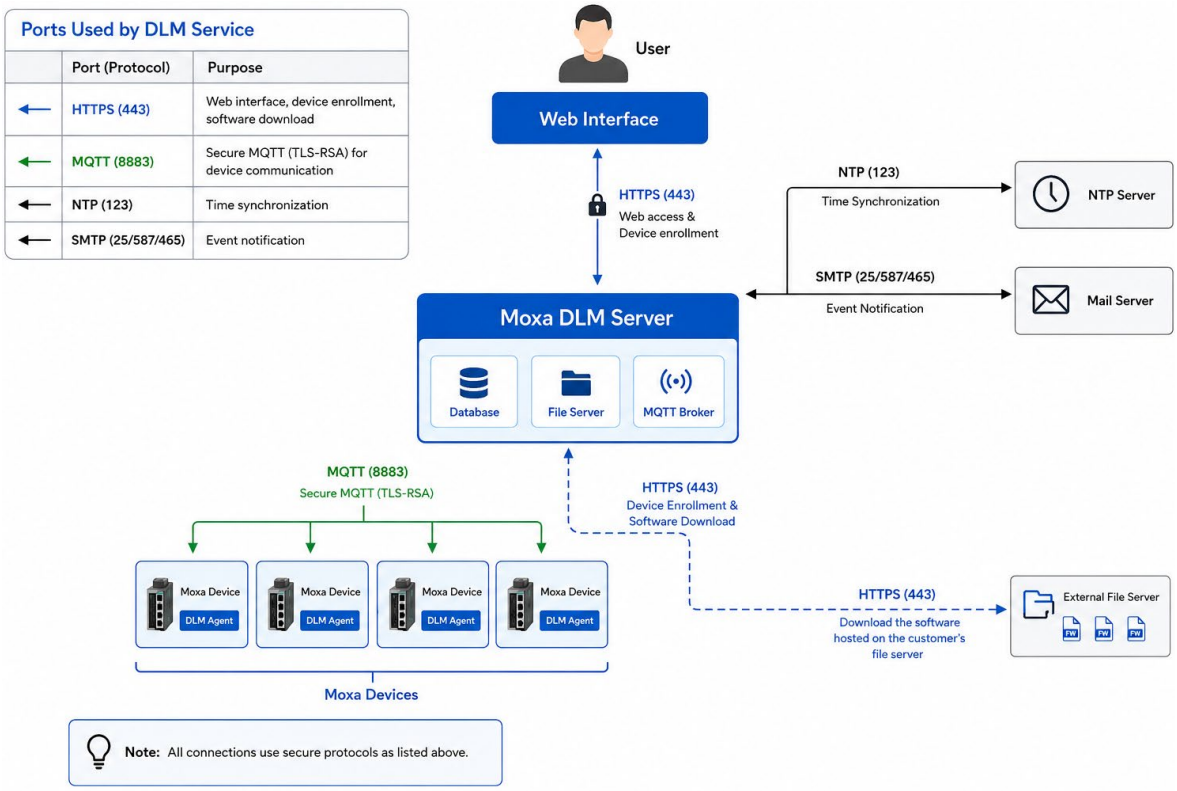
NOTE

The DLM software does **not support email encryption (TLS/SSL)**. When configuring the email server, ensure that encryption is set to **STARTTLS (Optional)** or **None**.

- **File Server for OTA (Over-the-air) Large-scale Software Installation**

  The DLM server allows upload of files through the web GUI, acting as a temporary file server for distribution. For large software files, we recommend using an external file server and update files using **Install Package** or **Run Custom Script** features and embedding the file's HTTPS URL in the script. This approach ensures reliable and efficient delivery of large files to devices.

Architecture



3. Setting Up the DLM Server

Installation and Upgrade

1. Prepare an environment with the required Ubuntu version installed.
   Download the latest DLM On-premise Server software from Moxa website.
2. Open the Ubuntu terminal and run the following command to update the package list and install the DLM service.
   - Replace **${DLM filename}** in the code block with the actual name of the file you receive from Moxa. For example, **dlm-1.1.0-build.63.tar.gz**

```
sudo tar zxvf ${DLM_FILENAME} -C /usr/local

# Add repo to apt sources list
echo "deb [trusted=yes] file:/usr/local/moxa-dlm-local-apt-repo \
jammy/" | sudo tee /etc/apt/sources.list.d/moxa-dlm.list

# Update apt
sudo apt-get update

# Install dlm package
sudo apt-get install dlm
```

NOTE

If the server has previously updated its package list using the **apt-get update** command, the offline installation may face issues with downloading recommended packages. To resolve this, add the **--no-install-recommends** parameter to the **apt-get install dlm** command as follows:
sudo apt-get install dlm --no-install-recommends

WARNING

If the **apt-get** update returns an error related to unsupported architectures (e.g., armhf or i386), remove these architectures before proceeding.

3. The DLM Text User Interface (TUI) will open automatically.
4. A system requirements check list is shown that includes CPU, memory, disk, operating system, packages dependencies, and network.
   - (Info) Meets all recommended requirements.
   - (Warning) Meets only the minimal requirements.
   - (Alert) Not capable of running the system.
5. The installation will start automatically, if the environment meets the **recommended** requirements.
   If the environment does not meet the **recommended** requirements, you can still click Y to install. However, if the **minimum** requirements are not met, the installation will not proceed.
6. If you want to reinstall DLM, you will have to uninstall the current version to avoid the error message:
   Errors were encountered while processing: /usr/local/moxa-dlm-local-apt-repo/jammy/[DLM package name] needrestart is being skipped since dpkg has failed

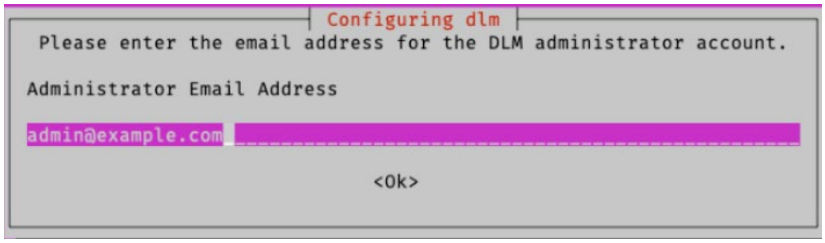
```
sudo apt-get remove dlm
sudo apt-get install dlm
```

7. Specify a fully qualified domain name (FQDN).

NOTE

- We strongly recommend using FQDN instead of an IP address to make it convenient to change the IP address of the DLM service without having to re-register all devices.
- The FQDN is required only during the initial installation of the DLM system. Subsequent upgrades will not require the FQDN information.
- Before installing the DLM server, ensure that the network infrastructure is properly configured, including **server time**, **DNS servers**, **IP address settings**, and **routing**.
  Improper network configuration (for example, incorrect DNS resolution) may prevent devices from connecting to the DLM Server or downloading file updates.

8. Create a default administrator account, the default password is **admin@123**.

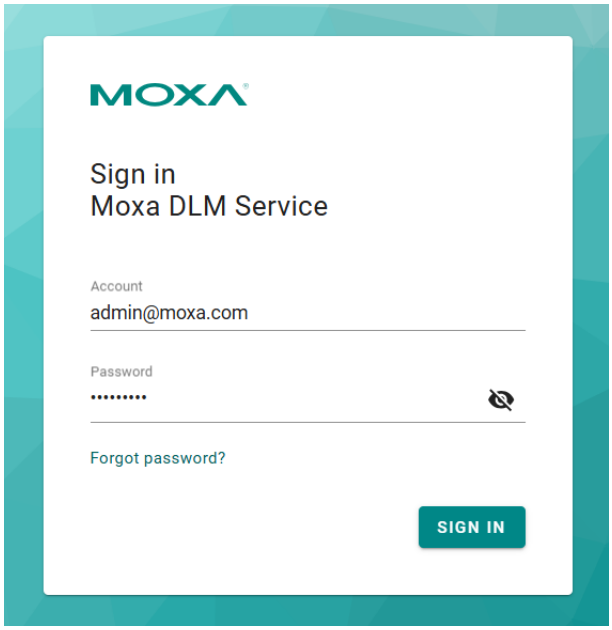


9. After the installation of the DLM service is complete and the devices are registered, you can access the web console of the DLM service via: **https://YOUR_FQDN**.

Accessing the DLM Service Web Console

After the DLM service is installed and the devices are registered, you can access the web console via: https://YOUR_FQDN

1. Log in with the default credentials:
   - Account: **The email address specified during DLM server installation**
   - Password: **admin@123**

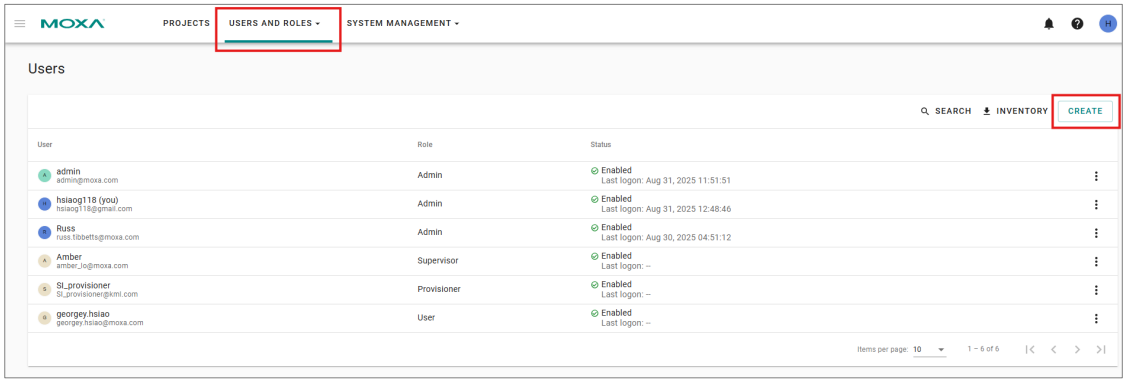


2. You will be asked to change the password for security purpose.
   We highly recommend changing the password after first login.

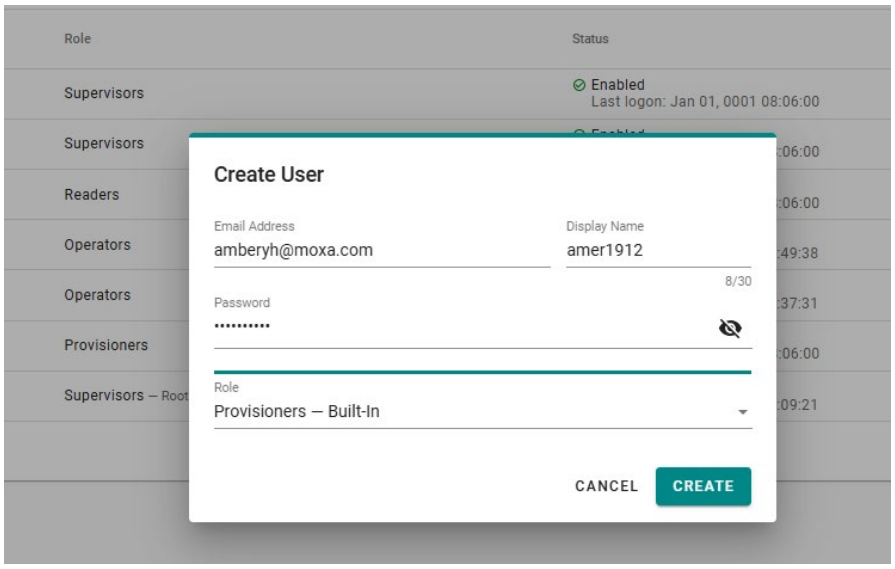
Creating a User-provisioner Role for Device Registration

If you want a user role with restricted access but able to register devices to the DLM server without granting access to the DLM data or web console, create a user with the "Provisioner" role. Users assigned the provisioner role can only registering devices to the DLM server but cannot log in to the DLM web console.

1. Go to **User and Roles** and click **Create**.



2. Create a user with the **Provisioners** role.



3. Click **Create** complete the process.

   You can pass on the **Email Address** and **Password** of the new account to the person responsible for registering Moxa computers on the DLM server.

4. Connecting Moxa Computers to DLM

Installing DLM Agent on UC Computers

The DLM Agent is not pre-installed on UC computers. You must install the DLM Agent and configure the DLM Server to which the devices should connect to.

1. **Download the installer.**

   The DLM Agent installer is available for download from Moxa website using the following command and file name format:

   ```
   dlm_agent_${version}_${supported models}_${MIL version}.zip
   ```

   Example:

   ```
   dlm_agent_1.0.0-1_for_uc-1222a-2222a-3400a-4400a-mil-3.4.zip
   ```

2. **Check the Moxa Industrial Linux Version.**

   Ensure that the UC computer is running MIL version 3.4.1 or later. Run **mx-ver -M** to check the version.

3. **Extract the required files.**

   After extracting the ZIP file, you will find the following contents:

   - **Configuration file:** user.yaml
   - **Installation script:** run
   - **DLM Agent package:** moxa-dlm-*.deb or moxa-dlm-*.tar
   - **User credential:** credentials.yaml
   - **MIL utilities:** The DLM Agent installation may require updating other MIL utilities to newer versions.
     - If an update is required, a folder containing the utility update files will be included.
     - For example, if a Moxa Connection Manager (MCM) update is needed, a folder named **MIL_packages** will be present.
   - **Sample Scripts:** A folder named **Sample Scripts**, which includes useful scripts that can be executed from the DLM web console (for example, scripts to update the DLM agent).

4. **Modify the configuration file (user.yaml)**

   Edit the **user.yaml** file to specify the necessary parameters for the DLM Agent.

   During installation, this configuration file will be copied to **/etc/moxa/moxa-dlm-agent/**. The DLM Agent reads its settings from this location.

   Example configuration file:

   ```
   # Mandatory
   dlmServer:
     host: "demo.dlm.moxa"

   # Optional
   security:
     skipTLSVerify: true

   dataTransmission:
     trafficUsageDebug:
       enabled: false
       interval: "10m0s"
   ```

Category	Field Name	Description
dlmServer	host	Host name of the target DLM server e.g., demo-ka-983e.dlm.dev.moxa.live Make sure the prefix https:// prefix is not included
security	skipTLSVerify	• **false:** validate the DLM server's identify via importing the certificate exported from DLM server to device • **true:**(default) skip the validation
dataTransmission	trafficUsageDebug: enabled	• **enabled:** Device will report the traffic (TX/RX) of each network interface to the DLM server at the frequency (internal) specified (default) • **disabled:**(default) The service won't report any traffic data
	trafficUsageDebug: interval	The minimum interval value is 10s • d = days • h = hours • m = minutes • s = seconds For example, 1h0m0s = 1 hour
	cellularPerformanceDebug: enabled	• **enabled:**(default) Device will report the cellular performance data (signal level, RSRP, RSRQ, SINR, Cell tower's ECI) to DLM server by the frequency (internal) specified. • **disabled:** do not report any cellular performance data.
	cellularPerformanceDebug: interval	The minimum interval value is 10s
Event	cpuTemperature: threshold	CPU temperature threshold used to trigger a CPU Temperature Too High event. • **0 (default):** Uses the device hardware-defined auto-shutdown temperature minus 10°C as the threshold. • **1–150:** Uses the specified temperature value in °C as the threshold. For example, if the value is set to **90**, the device sends a **CPU Temperature Too High** event alert to the DLM server when the CPU temperature reaches **90°C**.

5. **Configure user and password**

   Provide the user and password of the person who is authorized to enroll Moxa computer to DLM.

   Edit the Modify the configuration file **(credentials.yaml)**

   Example configuration file:

```
email: "provisioner@moxa.com"
password:"provisioner@123"
```

WARNING

- The user account for enrolling a device to the DLM server must be created in advance by following the Create New User procedure.
- After the device is enrolled to the DLM server, the **credentials.yaml** file will be encrypted to protect password confidentiality.
- It is strongly recommended to use a user with the **Provisioner** role for enrollment. Unlike the **Admin**, **Supervisor**, and **User** roles, a Provisioner account does not have access to the DLM web console or API, which helps prevent password leakage before the device is enrolled.

6. **Download the DLM Server Certificate**

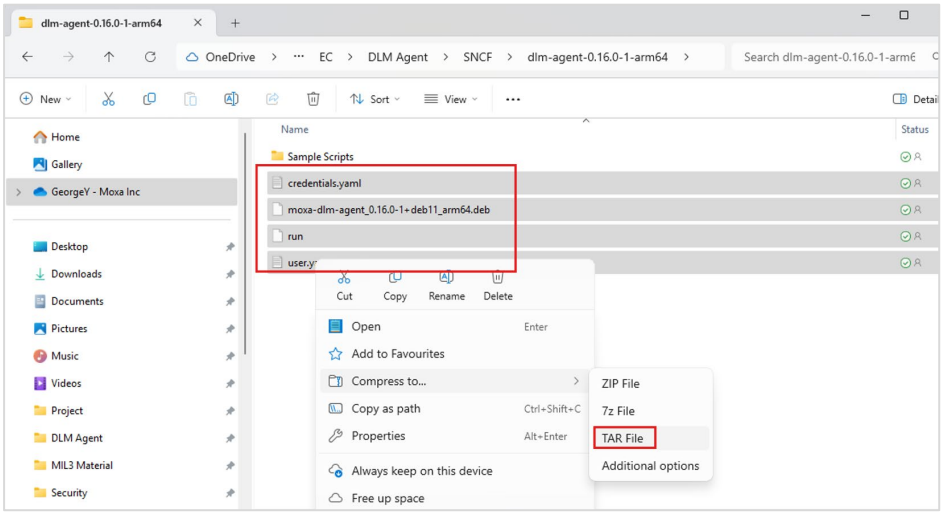
   For improved security, it is recommended that the device validates the DLM Server's identity before registering with the server. To enable this:

   a. In the user.yaml file, set the parameter skipTLSVerify to false.

   b. Download the server certificate from the DLM Server. The certificate is located at:

   /var/lib/dlm/data/certs/root/cert.pem

7. **Pack All Files into a** .tar **Archive**



8. **Install DLM agent on Moxa Computer**

   a. Installing directly from Linux console of Moxa computer

      i. Make sure the Moxa computer can ping the DLM server

      ii. Transfer the `.tar` archive created in previous step to the Moxa computer

      iii. Access the Moxa computer Linux console

      iv. Run the following commands to extract the files and execute the run script:

```
tar -xvf tar -xvf ${name of tar file}
chmod +x run
./run
```

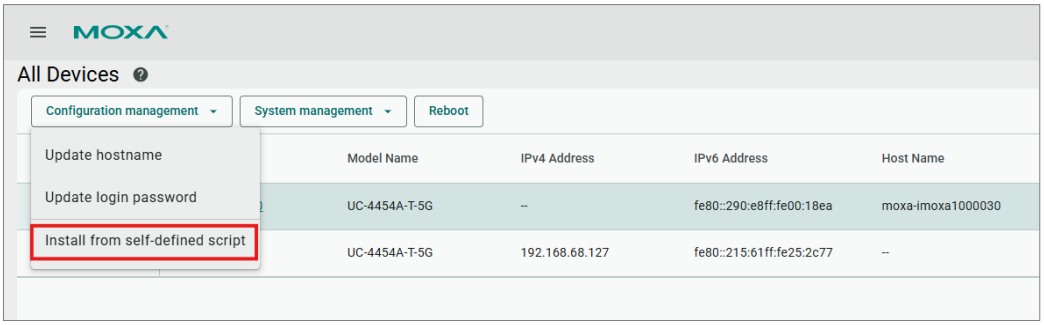
      v. The Moxa computer will begin to register to DLM server, use `mx-dlm-agent status` command to check the connection status.

   b. Install to multiple Moxa Computers using Moxa Swift Utility

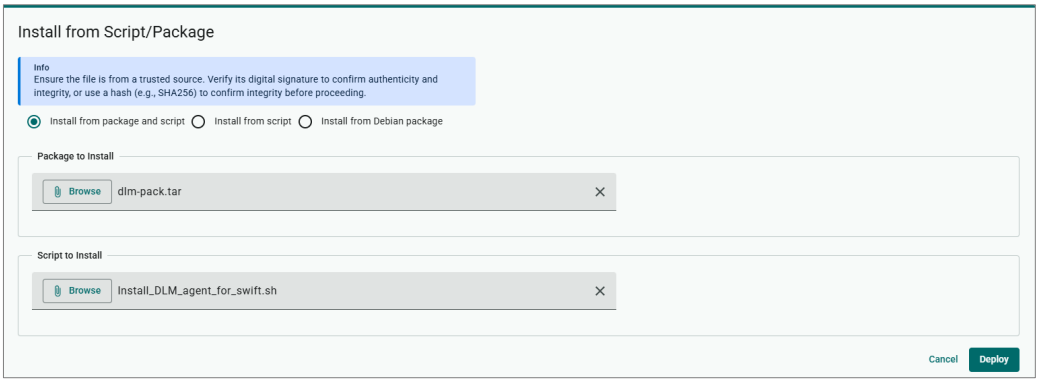
      i. Create a bash script, replace `dlm-pack.tar` with the actually file name created in previous step.

```
#!/bin/bash
set -euo pipefail

# Extract the package
tar -xvf dlm-pack.tar

# Make the installation script executable
chmod +x run

# Execute the installation script
./run
```

ii. From the Swift Web UI, select multiple computers and choose **Install from Self-defined script**.



iii. Upload the dlm agent `.tar` archive, and also the script created.



Checking the DLM Agent Connection Status

Use the command below to check the status of the DLM agent.

```
mx-dlm-agent status
```

Status	Description
init	When the status is init, it indicates that the DLM agent is initializing and ready to enroll with the DLM server. However, if the agent is unable to reach the server, the status will be stuck at "init". It might be due to one of the following reasons: • The DLM server cannot be reached, which could be a network issue. • Internet access is not available, preventing the agent from communicating with the DLM server. • The DLM server URL in the user.yaml configuration file may be incorrect. Please ensure that the URL is properly configured, and remember that the https:// prefix should not be included in the URL.
enroll	The DLM agent has successfully requested enrollment to the DLM server and is waiting for the server to return the enrollment certificate.
pending approval	The DLM agent has successfully obtained the enrollment certificate from the server and has requested registration. The device is now waiting for the DLM admin's approval.
provisioning	The DLM admin has approved the device.
connecting	The device is connecting to the DLM server.
connected	The device is connected to the DLM server.
disconnected	The device is disconnected from the DLM server.
error	An unidentified error occurred during device enrollment or registration.

Updating the DLM Agent

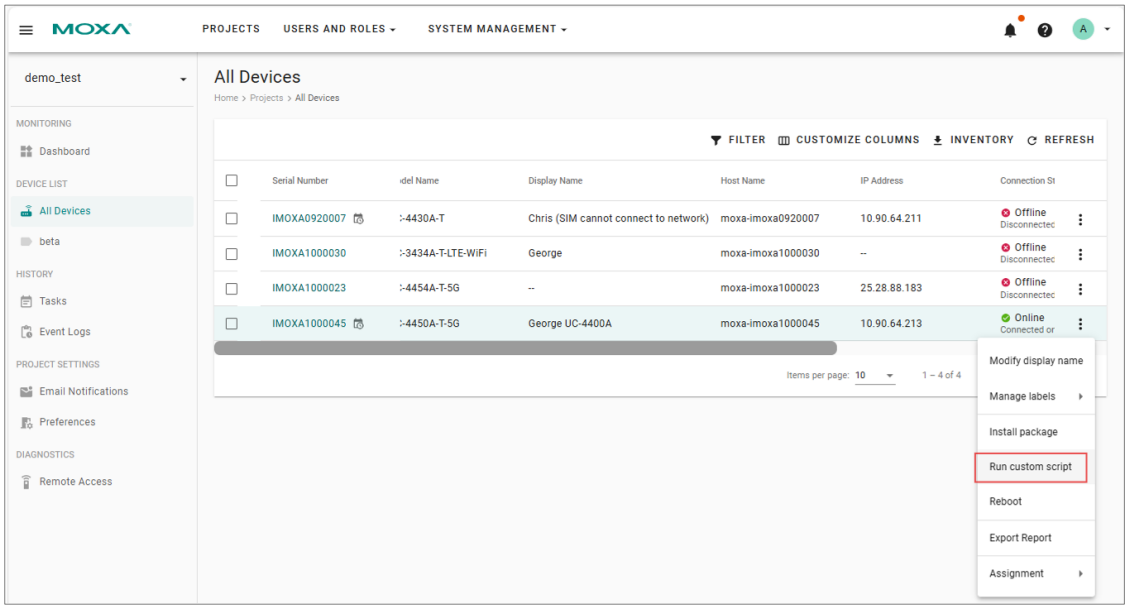
From the DLM Server

If the device is already connected to the DLM server, you can update it directly using the **run custom script** feature.

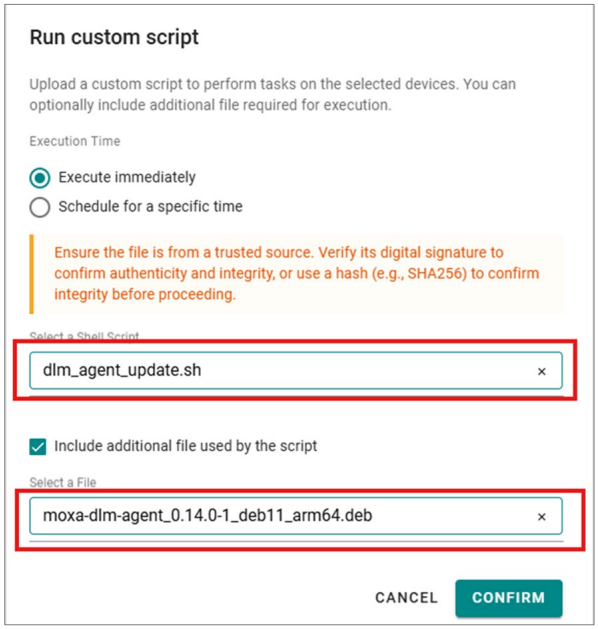
1. A bash script to update DLM agent called `dlm_agent_update.sh` is included in the DLM installer pack released available on the Moxa website.

> **WARNING**
>
> DLM agent updates may include updates for other Moxa Industrial Linux components. Ensure that you run the **`dlm_agent_update.sh`** included in each release as the content might vary.

2. From DLM web UI, select the device(s) you want to update, then click **Run custom script**.



3. Select the script file and the DLM Agent installation file, then start the update.



From the Moxa Computer

If the device is not connected to the DLM Server, you can update it in one of the following ways:

- **Using the Moxa Swift Utility** to perform the update, or
- **Manually:** transfer the `dlm_agent_update.sh` script and the updated DLM Agent package to the Moxa computer, then execute the script from the Linux console.

5. Using the Moxa DLM Service

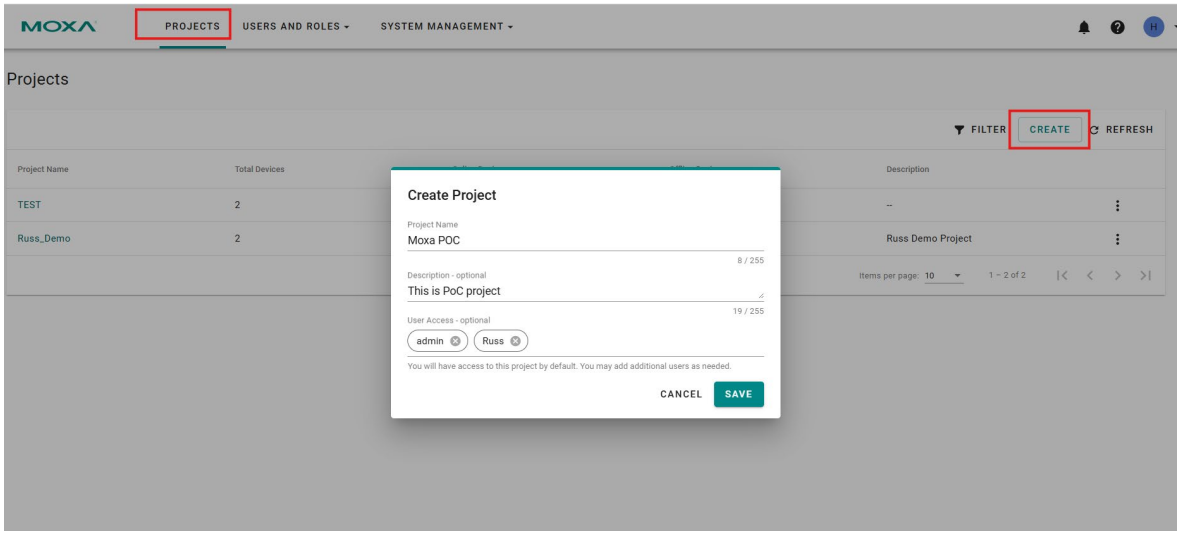
Project Management

All devices registered to the Moxa DLM must be assigned to a project. A device can belong to only one project at a time.

1. In the web console, click **PROJECTS** on the top menu bar.
2. Click **CREATE**.
3. Enter a **project name** and an (optional) **description**.
4. Select which user have access to this project.

> **NOTE**
>
> 1. Users with the **Admin** role automatically have access to all projects.
> 2. It is strongly recommended to limit the number of devices in a single project to fewer than 2,000 in order to maintain optimal UI performance.

5. Click **SAVE** to create the project.



User and Role Management

DLM comes with 4 roles:

- **Admin**

  Full control over the entire DLM system. Administrators can manage all users, configure system settings, manage projects and devices, approve device registrations, and perform device actions.

- **Supervisor**

  Responsible for project and device operations. Supervisors can perform tasks such as rebooting devices, running custom scripts, initiating remote access, and configuring project preferences. They cannot manage projects or users.

- **User**

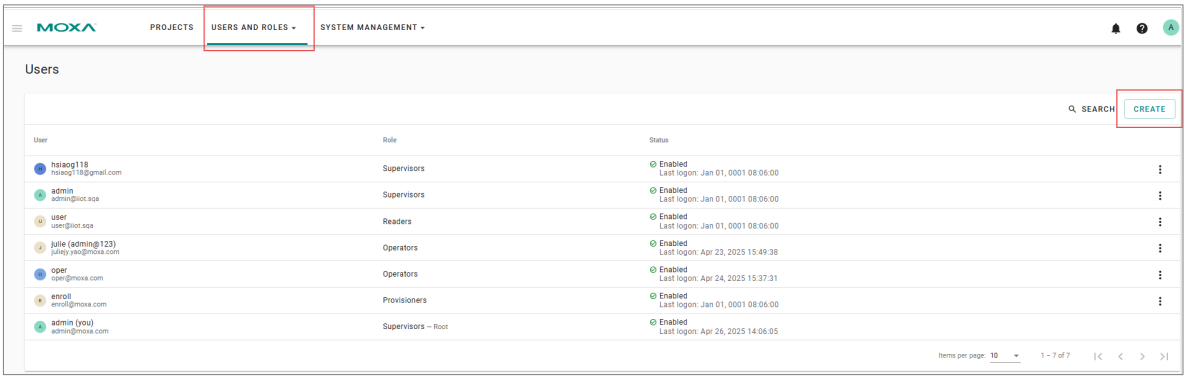
  View-only access. Users can monitor devices, and export reports and logs, but cannot modify device or project configurations.

- **Provisioner**

  Limited to device registration. Provisioners can register devices to the DLM Server but cannot log in to the DLM web console.

Permission Category	Administrator	Supervisor	User	Provisioner
Device Register	✅ Register device to DLM server			
Device Approval	✅ Approve/reject the registered device(s)	❌	❌	❌
Project Management	✅ Create, delete, and modify projects	❌	❌	❌
User Management	✅ Create users and assign roles ✅ Enable/disable **all users** ✅ Modify roles of **all users**	❌	❌	❌
Device Management	✅ Following privileges are provided: • View and configure dashboards and device info • Remove or move devices between projects • Install software packages on devices • Run custom scripts on devices • Reboot devices • Export reports • View and export event logs • Add labels to devices • Create search filters to locate device • Configure email notifications for events	✅ Following privileges are provided: • View and configure dashboards and device info • Remove or move devices between projects • Install software packages on devices • Run custom scripts on devices • Reboot devices • Export reports • View and export event logs • Add labels to devices • Create search filters to locate device • Configure email notifications for events	✅ Following privileges are provided: • View dashboard and device info • View and export event logs • Export report • Apply search filters to locate device	❌
Project Preference	✅ Configure project-level preferences (e.g., auto logout time)	✅ Configure project-level preferences	❌	❌
System Setting	✅ Configure SMTP email server ✅ View and export server system logs	❌	❌	❌

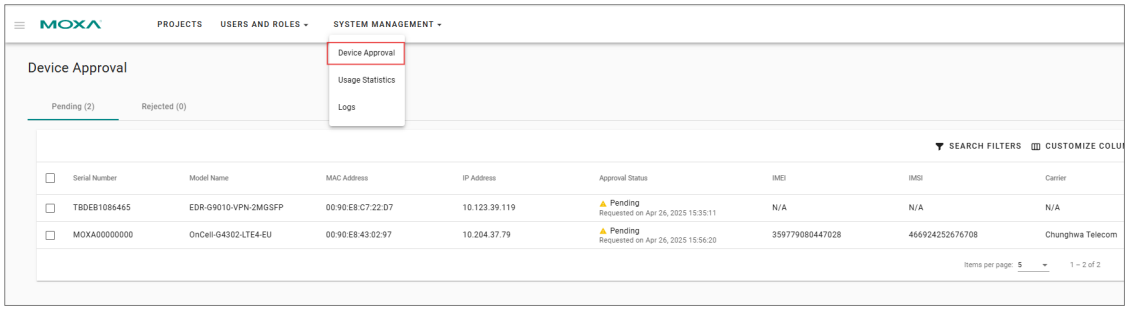
To create a user, go to **User and Roles** and click **Create**. Please note there can be only one user with **Administrator** role.



Reviewing and Approving Device Registrations

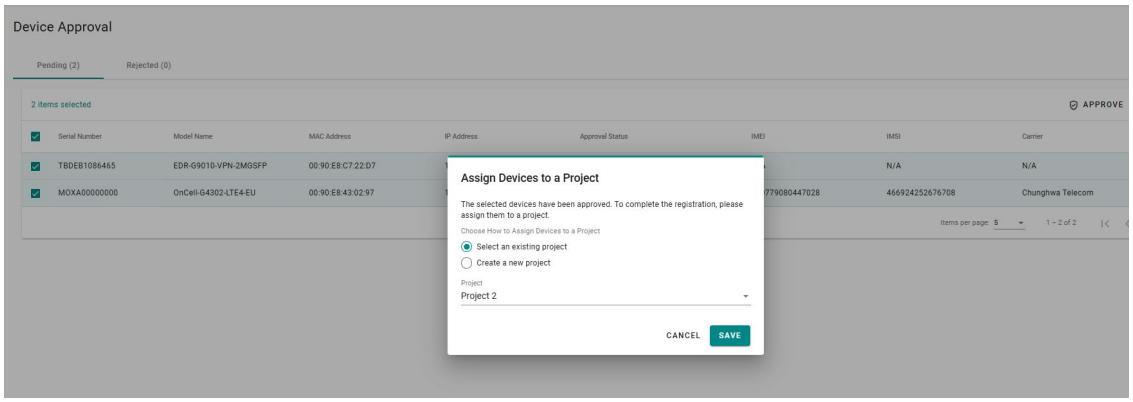
When a device is registered to the DLM server, it requires review and approval by a user with the **Administrator** role. If there are devices pending approval, the system sends a reminder email to all administrators once per day.

1. If you are an **Administrator** or **Supervisor**, go to **System Management > Device Approval** to review and approve devices pending approval.



2. Select the devices you wish to approve, then click **Approve**.

   You will be prompted to assign the approved devices to a project.



3. If you accidentally reject a device, you can navigate to the **Rejected** page and approve it again.

Monitoring—Project Dashboard

Each project has an associated dashboard for monitoring all registered devices and their status.

The dashboard consists of multiple widgets that you can customize as needed.

- To add widgets, click the **edit icon** in the bottom-right corner, then click **Add Widget**, and save your changes by clicking **Save**.
- To adjust widget size and position, click the **edit icon** in the bottom-right corner, make the adjustment and save your changes by clicking **Save**.
- To remove a widget, click the **edit icon**, then press the **delete icon** on the widget you wish to remove.

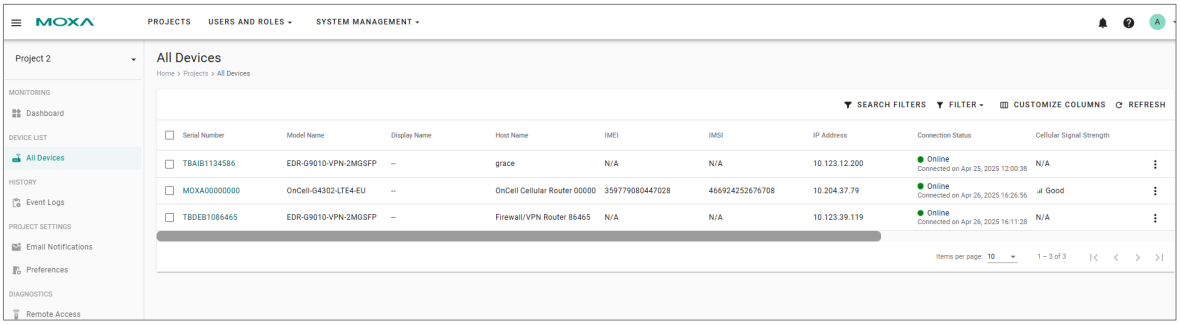
The dashboard widgets include:

Category	Widget Name	Description
Alert & Monitoring	Alerts and Warnings Hourly Trends	Displays the event numbers of Alert and Warning over the past **8, 12, or 24 hours**.
	Alerts in the last 24 hrs	Displays the event numbers of Alert within 24 hours.
	Warnings in the last 24 hrs	Displays the event numbers of Warning within 24 hours.
	Top 10 Unstable Devices in last 24 Hrs	Displays the ten devices with the highest number of connection interruptions or status changes within the past 24 hours. It helps identify devices that may require troubleshooting or further investigation to ensure system stability.
Network & Connectivity	Device Connection Status	Displays the status and the number of the registered devices: • Unknown (device registered and approved, but device has not connected to DLM yet • Offline • Online
	Hourly Average Cellular Signal Distribution	Displays the distribution of cellular signal strength across all devices, averaged over the **last hour**. It provides a snapshot of overall network quality and helps identify devices experiencing weak or unstable connectivity.
	Data Consumption Daily Trend	Shows the daily data usage trend for selected network interfaces, including Wi-Fi, cellular, or Ethernet. Users can choose the interface to monitor and view usage patterns over the past **30, 60, or 90 days**, making it easier to track long-term consumption and identify unusual traffic behavior.
Device Overview	Device Status Daily Trend	Shows the daily count of devices that are **online, offline, and the total registered devices** over a selected time period (past **30, 60, or 90 days**). It helps track connectivity patterns and identify periods of instability across the device fleet.
	Total Devices	Display the total registered devices.
	Devices Online	Display the current number of online devices
	Devices Offline	Display the current number of online devices
	Device Location Map	Displays the geographical locations of all registered devices on a world map. It provides a visual overview of device deployment and distribution, helping users quickly identify where devices are installed and monitor their regional presence.
	Remote Access Devices	Display the number of devices with established remote sessions.
Device Information	Model Types	Displays the breakdown of device models currently registered in the system. It provides an overview of the hardware types deployed and their relative proportions.
	Firmware Version	Shows the distribution of firmware versions across all registered devices. It helps identify which devices are running older versions and track firmware upgrade progress.

Device Management

Device List

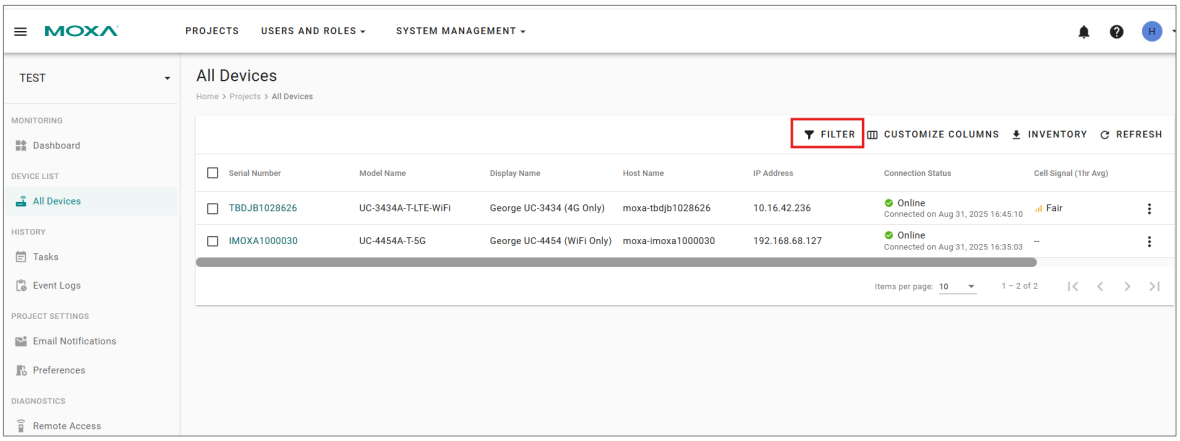
Enter a project and go to "All Devices" to view all devices in the project



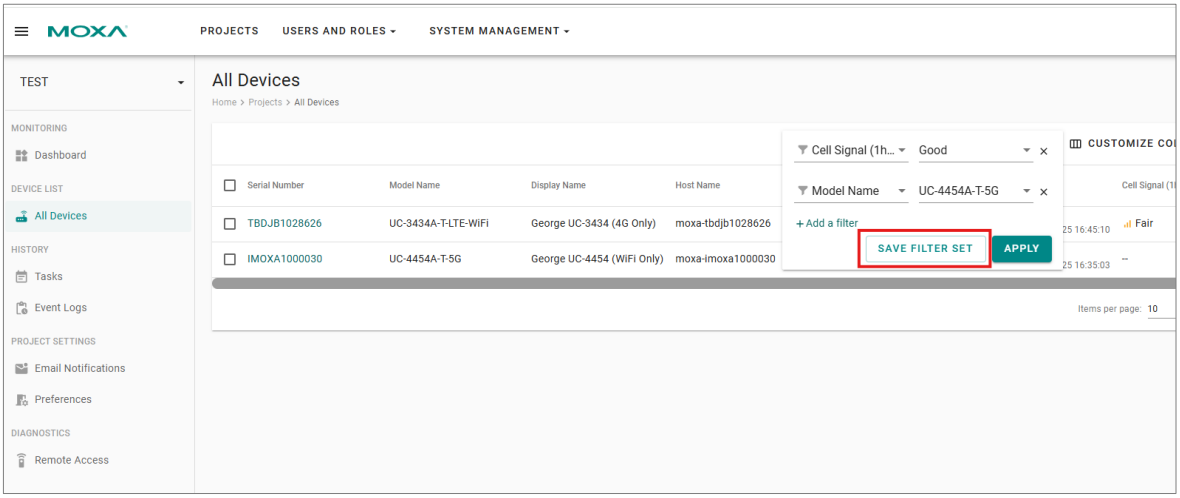
Column Name	Default Visibility	Filter Available	Description
Serial Number	Always Visible	✅	Unique identifier for each device (printed on the back of the device)
Model Name	Visible	✅	Device model name
Display Name	Visible	✅	User-assigned display name
Host Name	Visible	✅	Device hostname, for Moxa computer, this is the host name configured in Linux
IMEI	Hidden by default	–	International Mobile Equipment Identity
IMSI	Hidden by default	–	International Mobile Subscriber Identity
IP Address	Visible	–	Current Default route's IP address of the device
Connection Status	Visible	✅	Online/offline status of the device
Cell Signal (1hr Avg)	Visible	✅	Average cellular signal quality over the past 1 hour
Carrier	Hidden by default	✅	Cellular carrier name
VPN Tunnels	Hidden by default	✅	VPN tunnel information (not applicable to Moxa computers)
Firmware Version	Hidden by default	✅	Device firmware version
Label	Visible	✅	Custom labels assigned to devices

Searching Using Filters

Use the **Filter** function to search and filter devices based on the criteria defined.



Click **SAVE FILTER SET** to save the filter with a specific name.



NOTE

Filter set is saved in the current browser only, not by DLM user account. If you switch browsers or clear browser data, the column settings will not be retained.

Customizing the Columns in the Device List

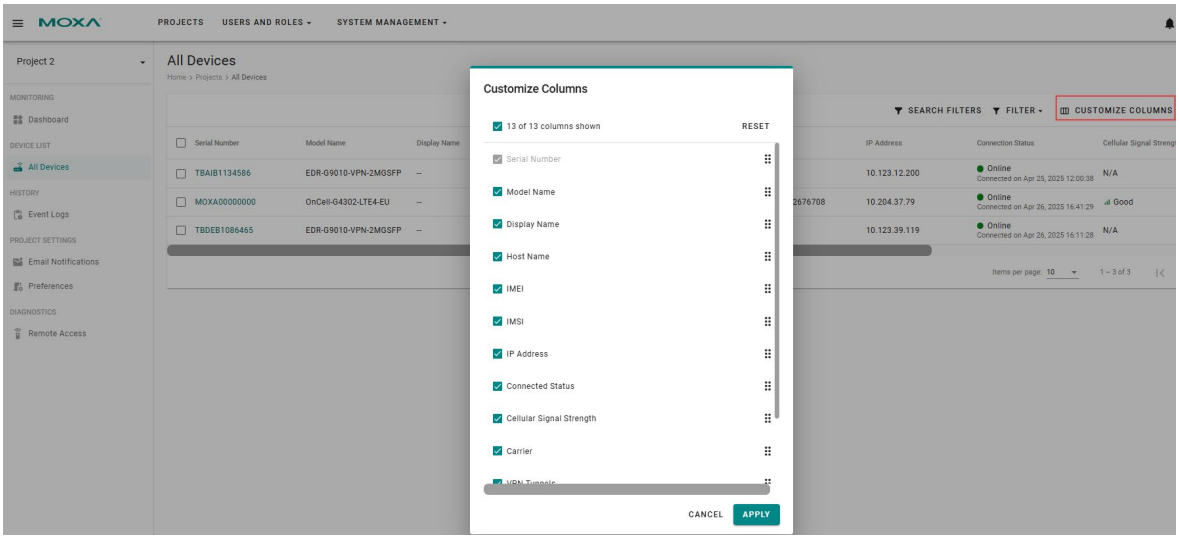
You can use **CUSTOMIZE COLUMNS** to adjust the device list view.

Drag and drop to reorder columns, or check/uncheck to show or hide specific columns.

NOTE

- Column customization is saved in the current browser only, not by DLM user account. If you switch browsers or clear browser data, the column settings will not be retained.
- The Serial Number column is fixed and cannot be hidden, as it serves as the device identifier.

Use the **CUSTOMIZE COLUMNS** to adjust the device list. You can drag and drop the columns in the order you need or check/uncheck the columns to display or hide them in the table. The Serial Number is fixed as the identity of a device.

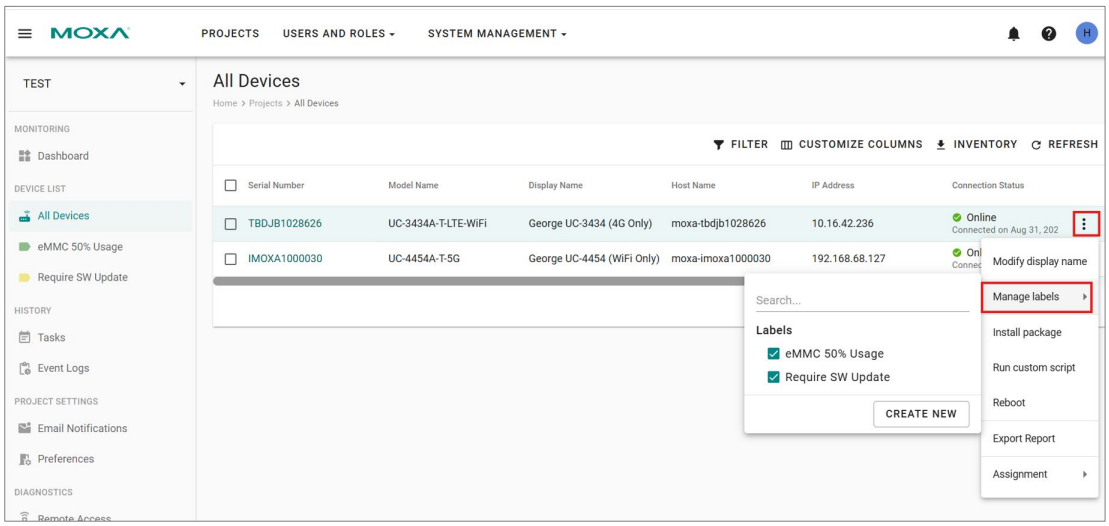


Labeling Devices

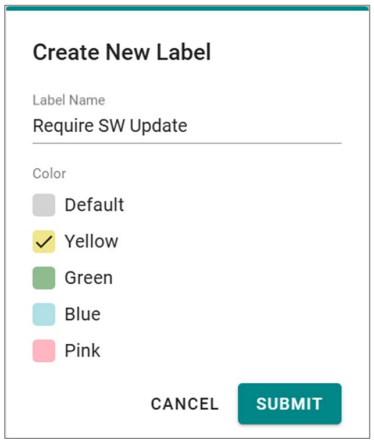
Labelling devices helps to quickly group the devices for a specific purpose.

To add labels to devices, do the following:

1. Select devices from the device list and click on the **LABELS** button shown on the upper-right corner of the page.



2. Search for existing labels to add to the device group or click **CREATE NEW**. You can specify a label name and choose a color for it.

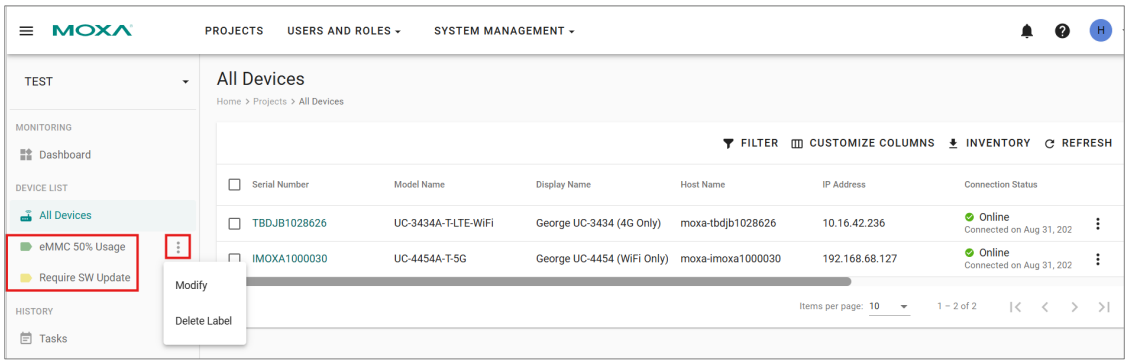


3. Click **SUMBIT**.
4. Using the Label.

   The labels created will appear as shortcuts at the top left of the sidebar.

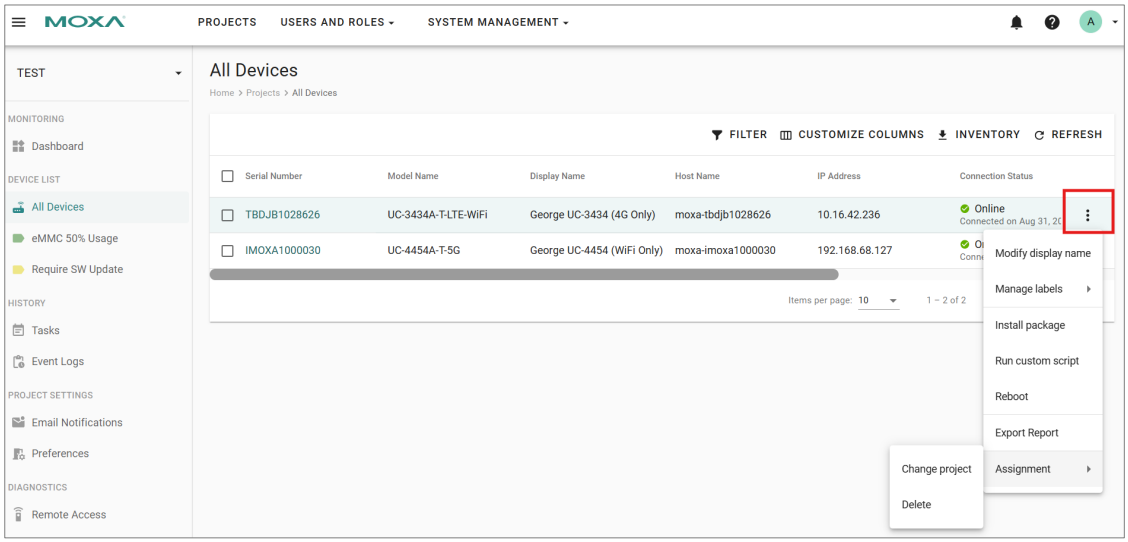
   a. To display all devices associated with a specific label, click the desired label.

   b. To edit or delete a label, click the **More Actions (⋮)** icon next to it.

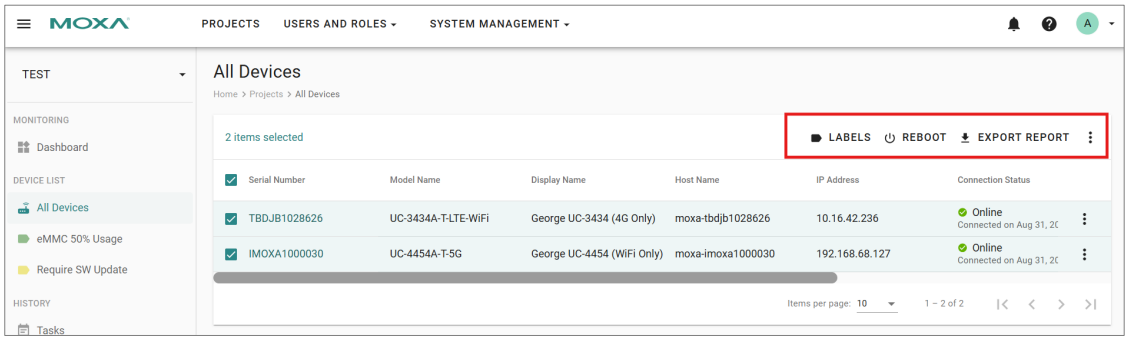


Task Operations

1. Click the More Actions (⋮) icon next to a single device to perform a task.

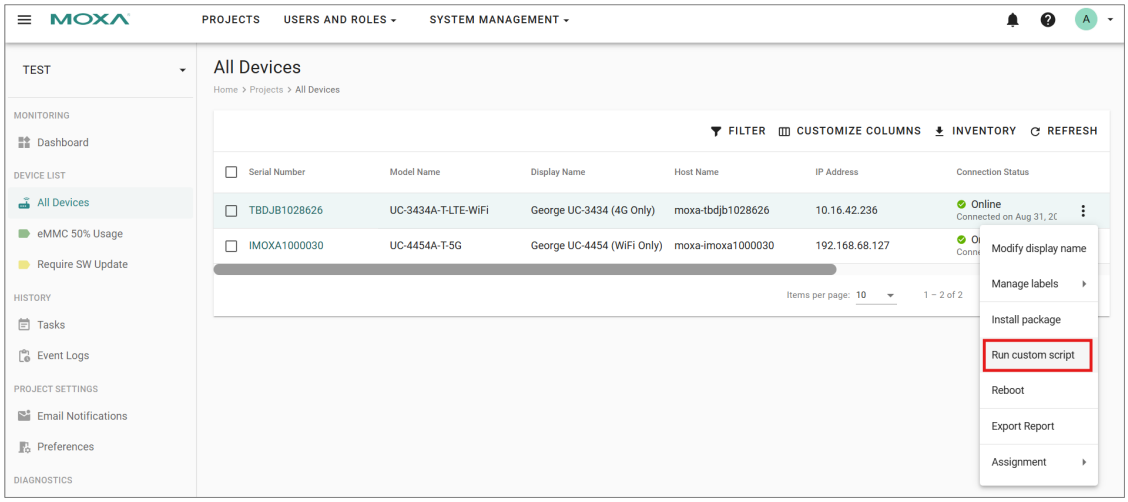


2. Select multiple devices to perform certain tasks in batch.

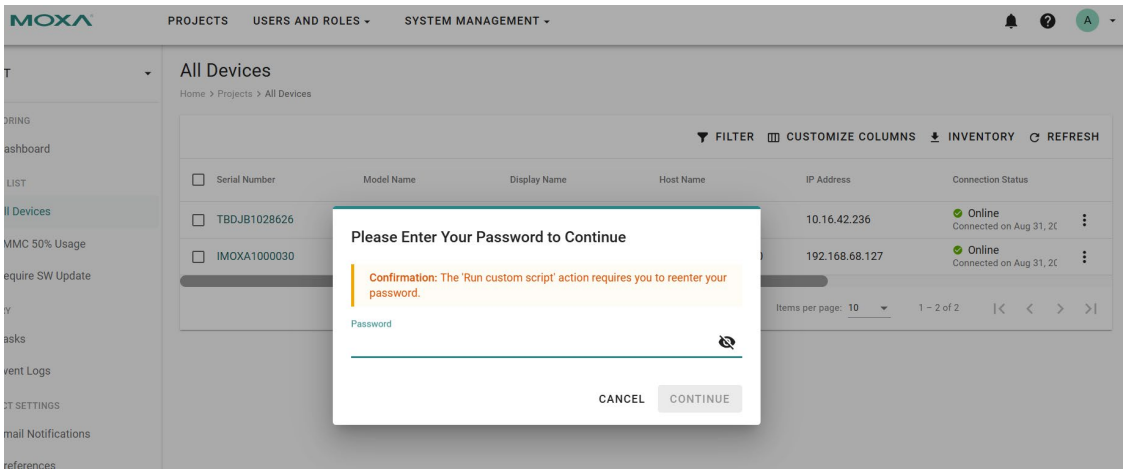


Running Custom Scripts

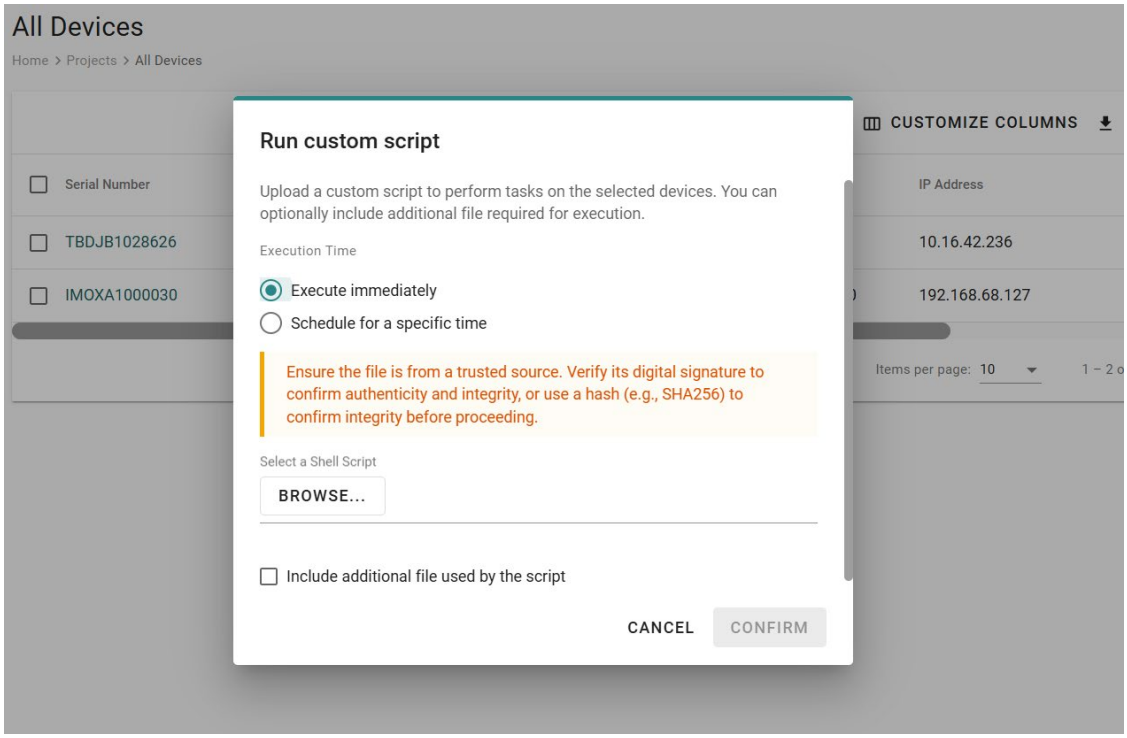
- Select a device, click the **More Actions (⋮)** icon, then select **Run Custom Scripts** to upload the initial configuration file.



- Since this operation will modify the device, you will be prompted to re-enter your password for security purposes.



- Then you can upload your Shell Scripts and run immediately or schedule for a specific time, also you can include additional files used by the scripts.

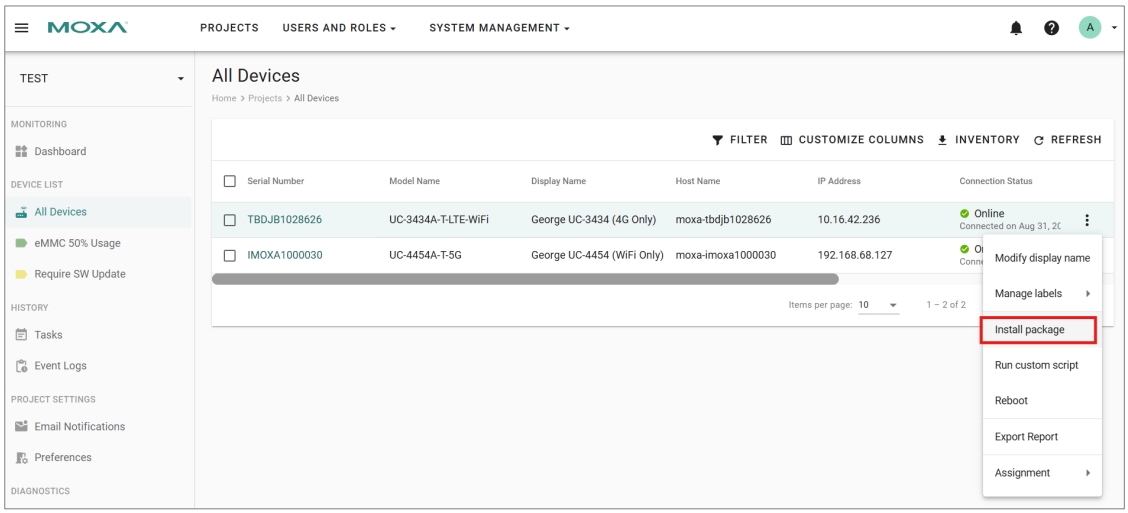


NOTE

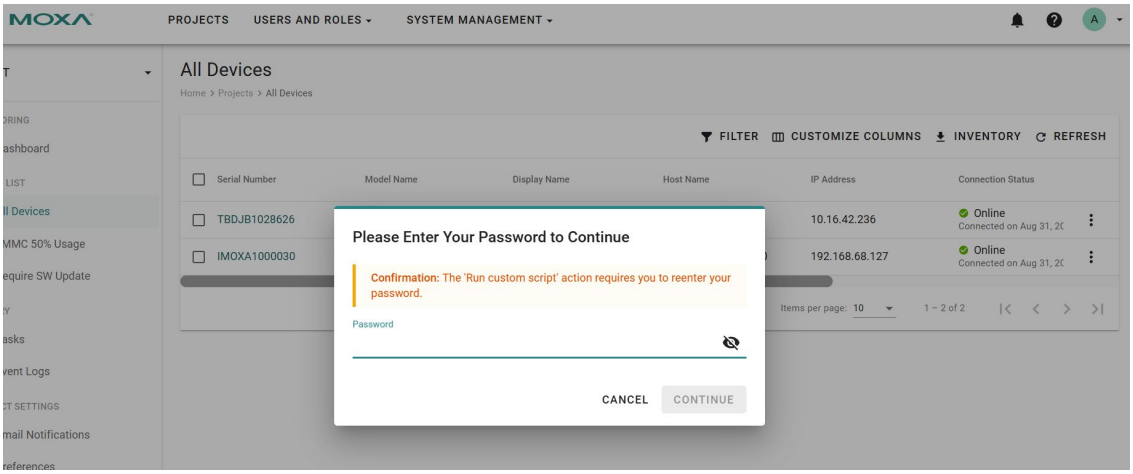
Ensure the script file is from a trusted source with the proper access right. Verify its digital signature to confirm the authenticity and the integrity.

Installing Packages

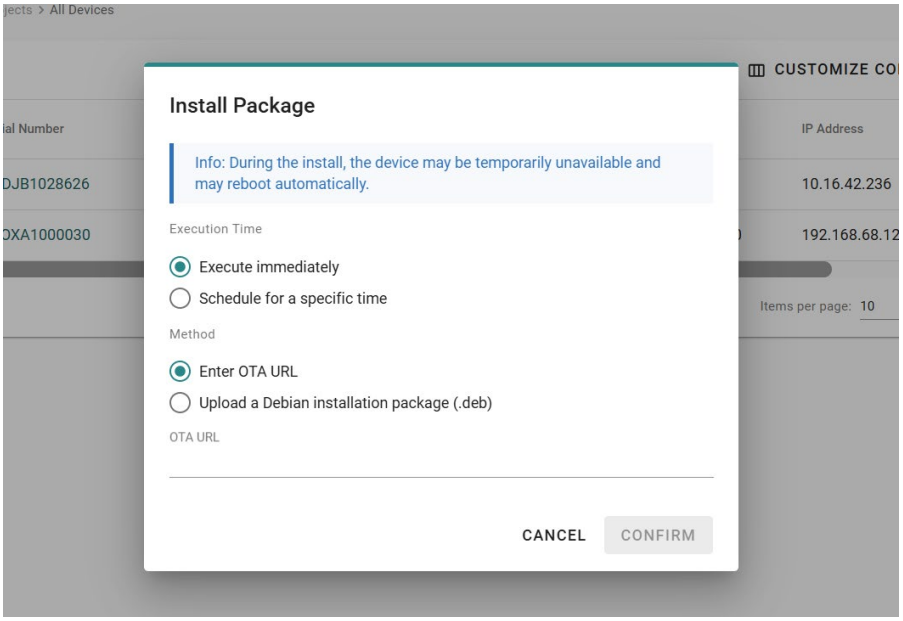
- Select a device, click the **More Actions (⋮)** icon, then select **Install Package**.



- Since this operation will modify the device, you will be prompted to re-enter your password for security purposes.



- Then you can Enter OTA URL or Upload your .deb packages from your computer. You can execute it immediately or schedule for a specific time:

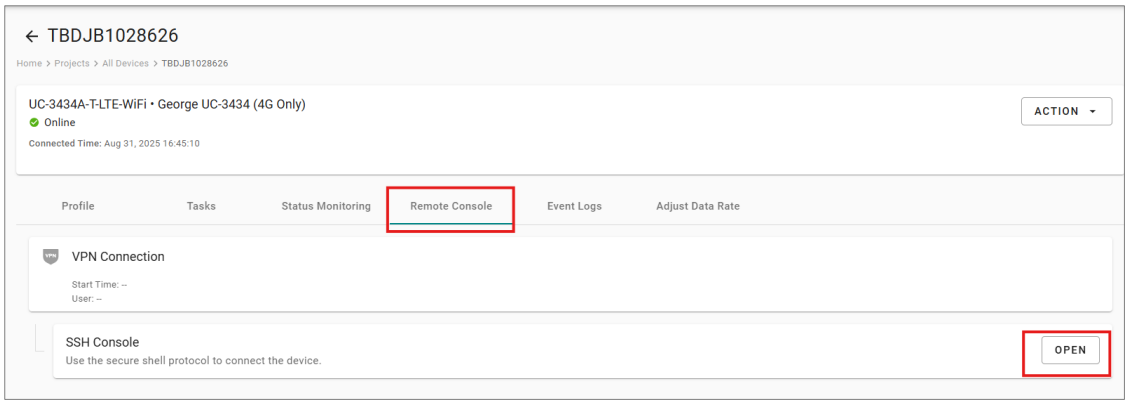


Configuring Remote Access for Troubleshooting

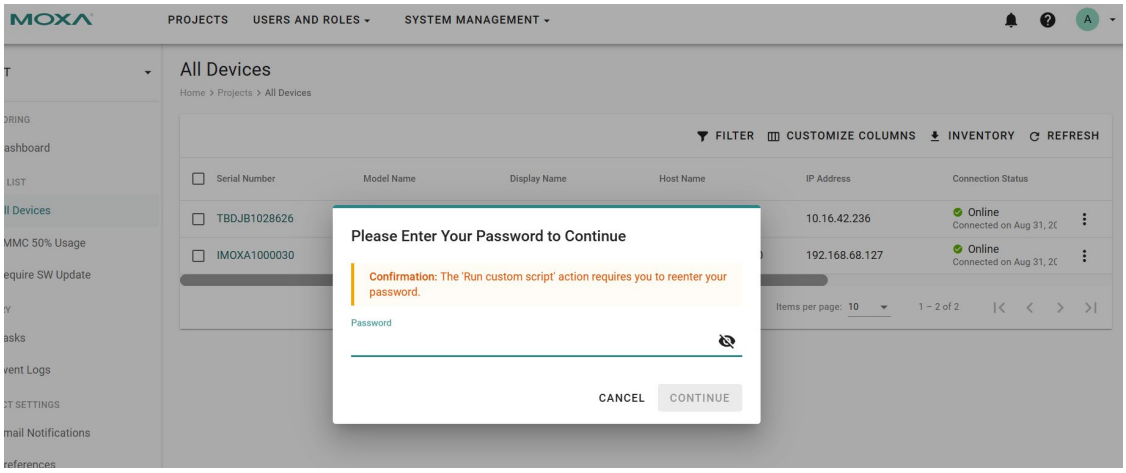
The Remote Console feature allows you to securely access a Moxa computer's Linux system from the DLM web console. By establishing a VPN connection and using the built-in SSH Web Console, you can remotely log into the device as if you were physically on-site.

- **Secure Access –** The connection is protected through an encrypted VPN tunnel and SSH protocol.
- **One-Click Operation –** Simply click **Open** to launch the console. DLM will automatically check the SSH server status and reconnect the VPN if necessary.
- **Full Control –** Once connected, you can execute Linux commands, run diagnostics, and manage the device directly via the browser-based SSH terminal.

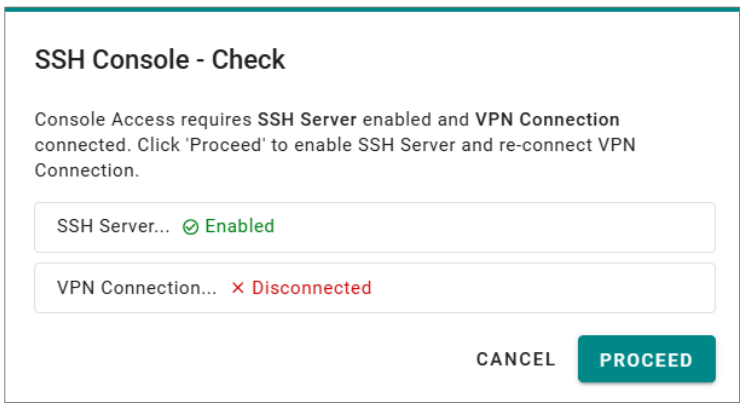
1. Select a device to enter the detail page, click the **Remote Console tab**, then select **open** a SSH console.



2. Since this operation will modify the device, you will be prompted to re-enter your password for security purposes.

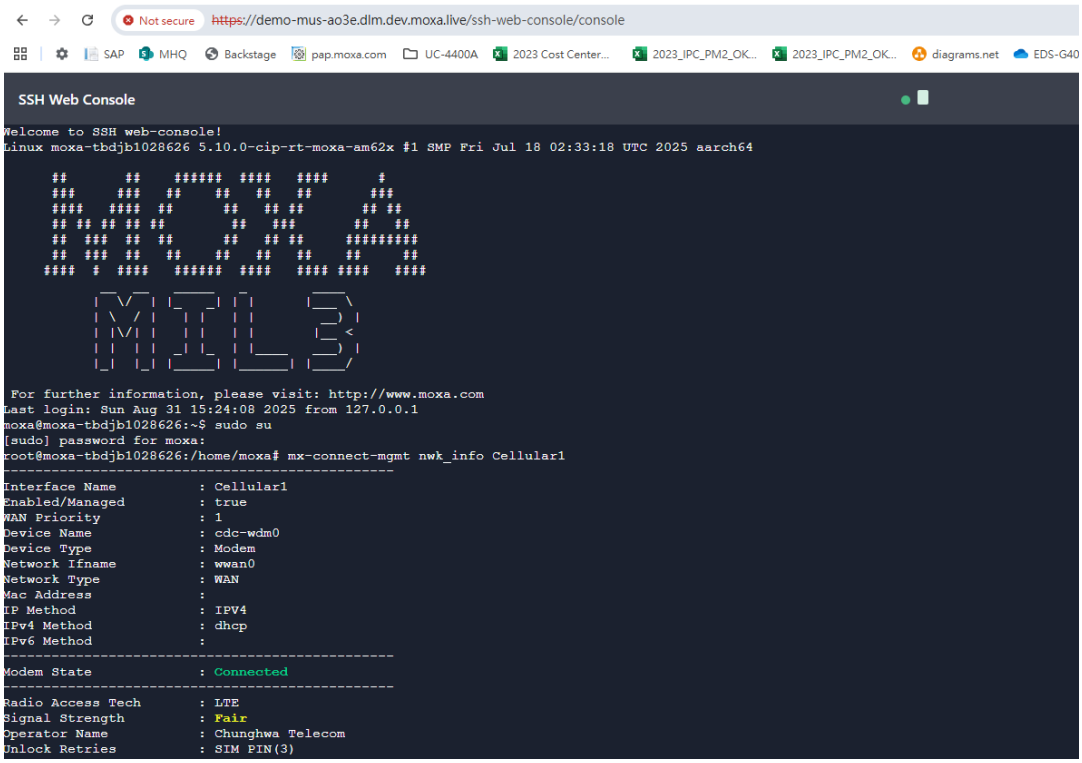


3. A secure VPN connection is established for remote access. Click **PROCEED** to continue.



4. A web console instance will open and you will be asked to enter the username and password of the Moxa computer you are accessing.

5. The interactive Linux console of Moxa computer will open.



Exporting Reports

Report Name	Description
Cellular performance	Exports historical records of a device's signal level, RSRP, RSRQ, SINR, connected cellular tower ECI, eNB, PCI, Cell ID, and EARFCN within the specified time range.
Device Data Consumption	Exports historical daily data consumption records for each network interface within the specified time range.
Device Data Transmission	Exports historical data traffic (TX/RX) records for each network interface within the specified time range.
Device Event Log	Exports historical device event logs within the specified time range.

NOTE

- Records are retained for up to **180 days**.
- Reports are exported in **.csv format**.
- Each **.csv file** can contain a maximum of **10,000 records**.
- The report timestamp and selected date range are based on **UTC**.

Rebooting Devices

You can select multiple devices in the device list and click **REBOOT** on the upper-right corner to reboot the devices. The reboot task can be run immediately or scheduled to run later. To avoid overlapping of scheduled tasks, only one scheduled task per device is run every 15 minutes.

Removing Devices From a Project

Select the device(s) you want to remove, then click **Assignment > Delete** to remove them from the project.

Reassigning a Device to Another Project

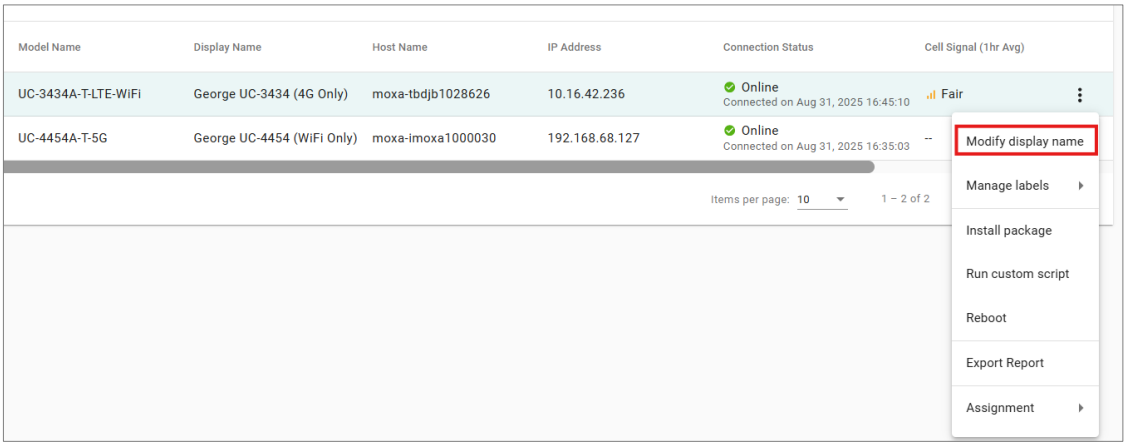
Select the device(s) you want to move, then click **Assignment > Change Project** to transfer them from the current project to the desired project.

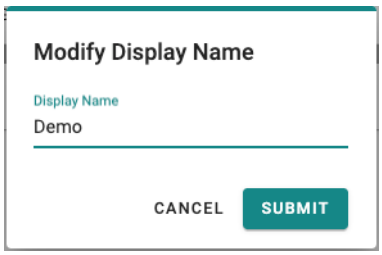
NOTE

If any selected device has a scheduled task, the **Change Project** option will be grayed out. You must cancel the scheduled task before you can change the project assignment.

Modifying the Display Name

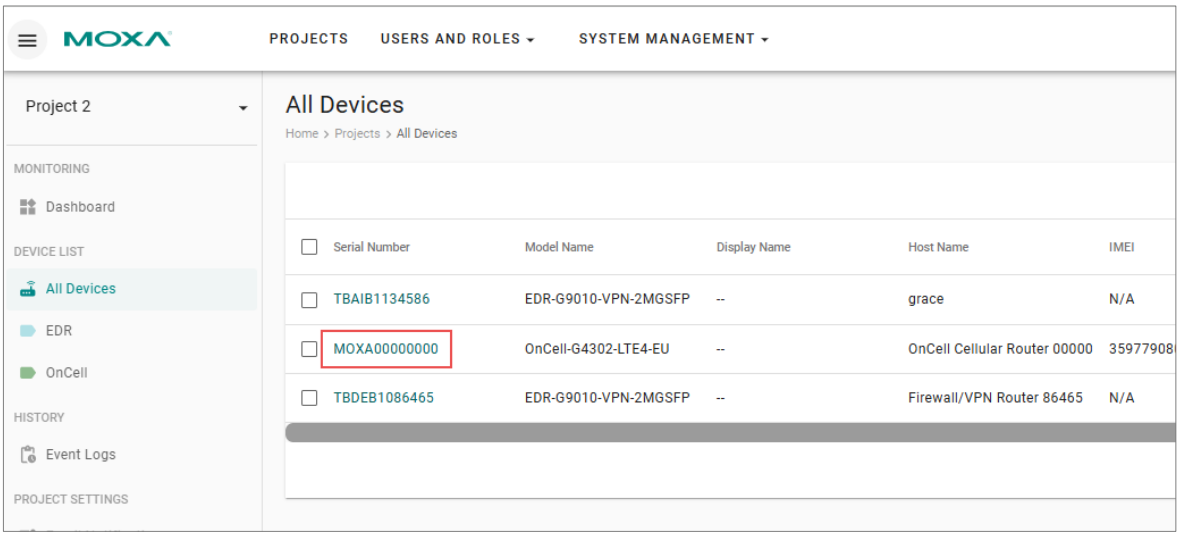
Each device can have a display name customized as needed. Click on the corresponding button , and select **Modify display name**.

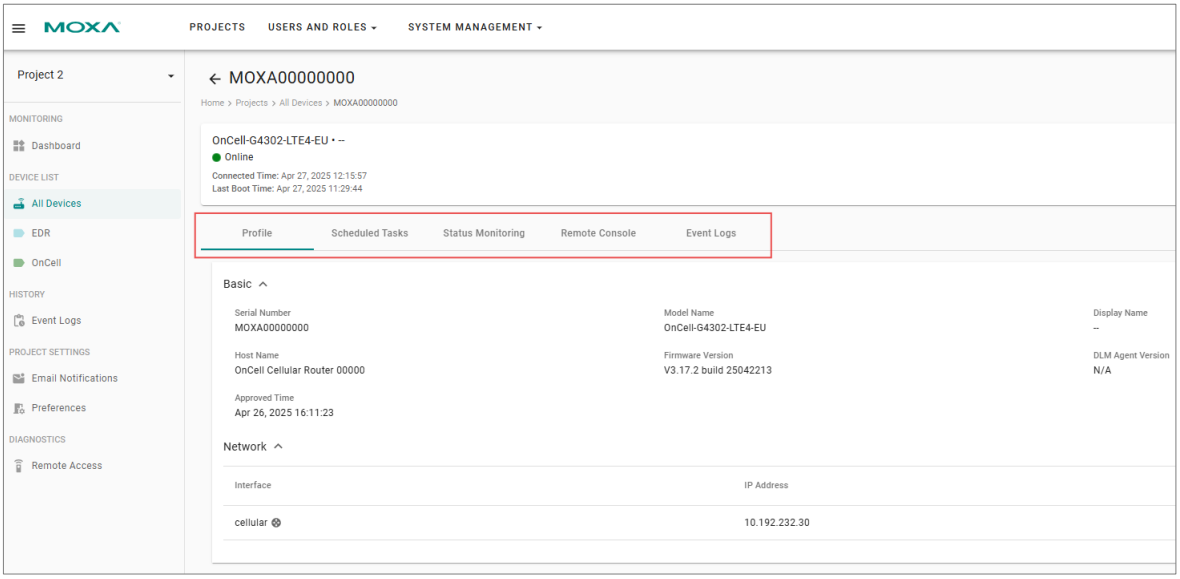




Device Information

To view the current device configuration, click on the device's Serial Number link on the device list.





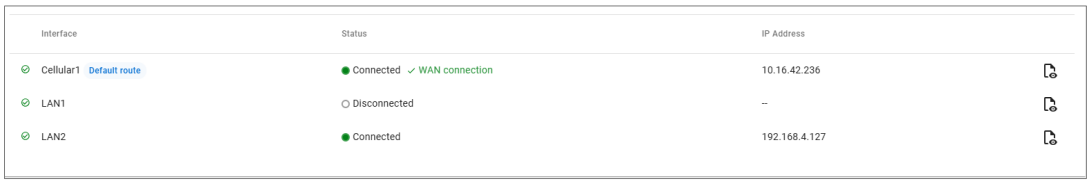
1. Profile

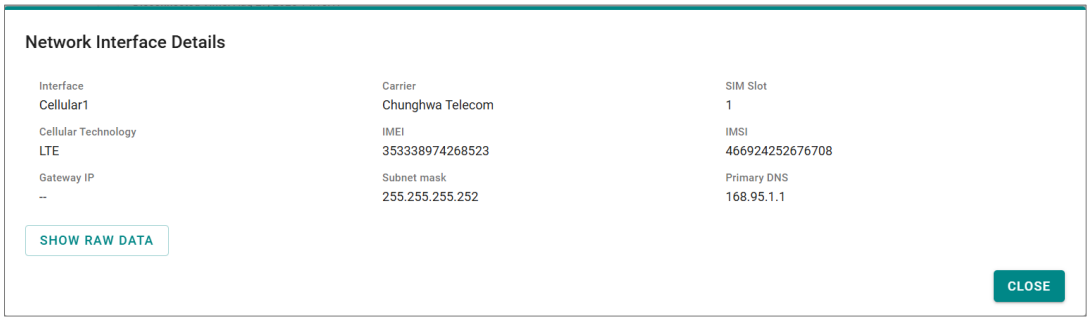
Shows basic information, network interfaces, software status, serial settings, and status of the devices. The details of each product profile are as follows:

- Basic Information
  - Serial number
  - Model name
  - Display name
  - Host name
  - Firmware version

    This is the image version for UC computer
  - DLM agent version
  - Approved time

➢ Network Interfaces





Columns	Values	Description
Interface Name	• **Ethernet:** LAN1, LAN2, LAN3… • **Cellular:** Cellular1, Cellular2… • **WiFi port:** WiFi1, WiFi2…	• The list of network interfaces available on Moxa computer. The name of the interface is the interface name shown in **Moxa Connection Manager (MCM)** utility in Moxa Industrial Linux • If the interface is the default route, it is marked with **Default route** icon
Status	• Connected • Connected (WAN connection) • Disconnected • Disconnected (WAN connection) • Unknown	• For ethernet interface, connected/disconnected status represent physical port link up/down • For Wi-Fi/Cellular interface, the status reflect the connection status reported by **Moxa Connection Manager (MCM)**
IP Address	IPv4/IPv6 address of interface	IP address of interface, if both IPv4 and ipv6 are available, IPv4 will be shown
Details	**Common fields** • Interface Name • Gateway IP • Subnet mask • Primary DNS **Cellular interface specific data** • Carrier • IMEI of Cellular modem • IMSI of SIM card • Cellular technology • The active SIM slot # **Wi-Fi interface specific data** • Operation Mode (client / AP) • SSID • Frequency (e.g., 2.4 GHz, 5 GHz) • Secure mode (e.g., WPA2) **Ethernet interface specific data** • MAC address	Click on icon to view the detail information of each network interface

2. Schedule Tasks

You can view tasks that have already been executed or are scheduled for execution. Only **Install Package, Run Custom Script** and **Reboot** operations can be scheduled. Pending scheduled tasks can be canceled if necessary.

NOTE

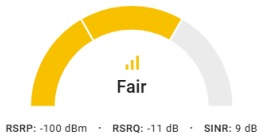
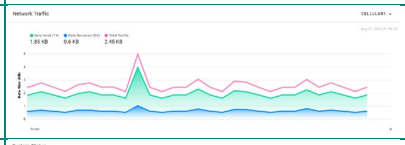
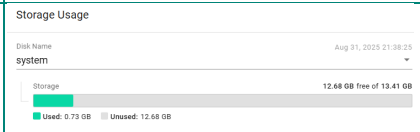
Scheduled tasks can be executed at 00, 15, 30, or 45 minutes past the hour.

To prevent overlap, only one scheduled task per device is allowed every 15 minutes.

3. Status Monitoring

The Status Monitoring tab displays live device data, including location, data consumption, network and telemetry traffic, CPU, memory, storage usage, and cellular signal strength. All information is presented in customizable widgets. You can click the edit icon to add, remove, or adjust widgets as needed.

Device data is refreshed every **10 seconds** while the Status Monitoring tab is open.

Widget Name	Widget	Description
Cellular Signal Strength		Displays the cellular connection signal level (No Signal, Poor, Fair, Good), along with the following metrics: • **RSRP (Reference Signal Received Power):** Indicates the strength of the received reference signal. • **RSRQ (Reference Signal Received Quality):** Represents the quality of the received reference signal, factoring in interference and noise. • **SINR (Signal-to-Interference-plus-Noise Ratio):** Measures overall signal quality compared to background interference and noise.
Cellular Signal Trend		Displays the cellular signal level trend for the past 5 minutes
Network Traffic Trend		Displays the traffic trend of each network interface over the past 5 minutes. Users can select the interface to view
System Status		Displays CPU and memory usage trends over the past 5 minutes
Storage Usage		Displays available storage space and the usage. The calculation excludes the space occupied by the factory-installed Moxa OS.
Device Location		Displays the device's geographical location on an interactive map, allowing users to quickly identify where the device is deployed.

4. Event Log (Device Specific)

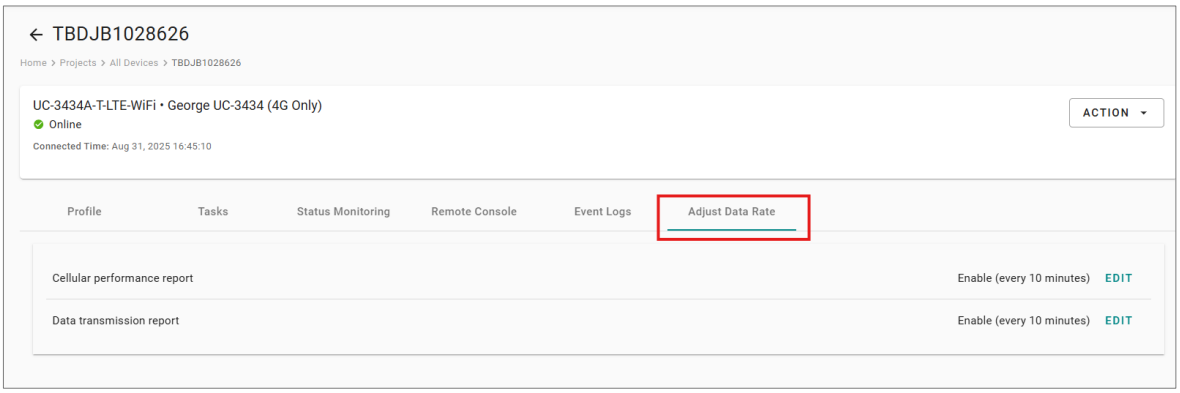
All events related to the selected device are displayed on this page. For detailed log descriptions, refer to **Appendices – Event Log List**.

5. Adjust Data Rate

This configuration allows you to disable or adjust how frequently the device uploads data to the server for the following reports:

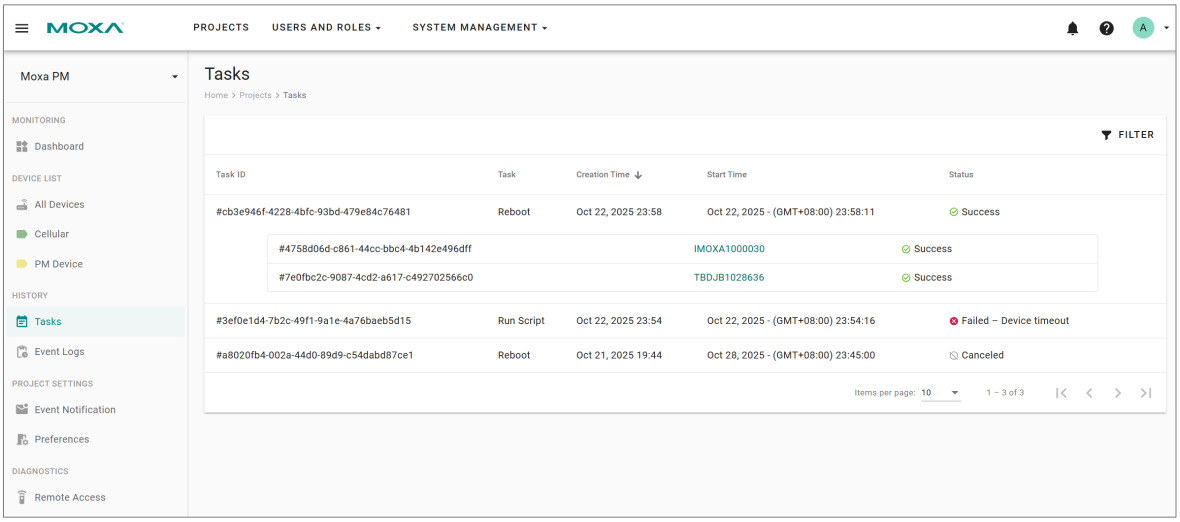
- **Cellular performance data** (signal level, RSRP, RSRQ, SINR, cell tower ECI)
- **Network traffic** (TX/RX) for each network interface

For example, setting the interval to **10 minutes** means the Moxa computer will upload these reports to the DLM server every 10 minutes.



Tasks Monitoring & History

The Task screen provides centralized monitoring and management for actions executed on one or more devices. Users can view a list of tasks, examine individual device outcomes, and diagnose failures quickly.



Task Display Structure

- **Parent Layer:** This shows the task itself, such as "Run Script" or "Reboot," along with the overall status of the task across all selected devices.
- **Child Layer:** When you expand a parent task, each device assigned to the task is listed here with its own execution status.

Parent Layer Status Definitions

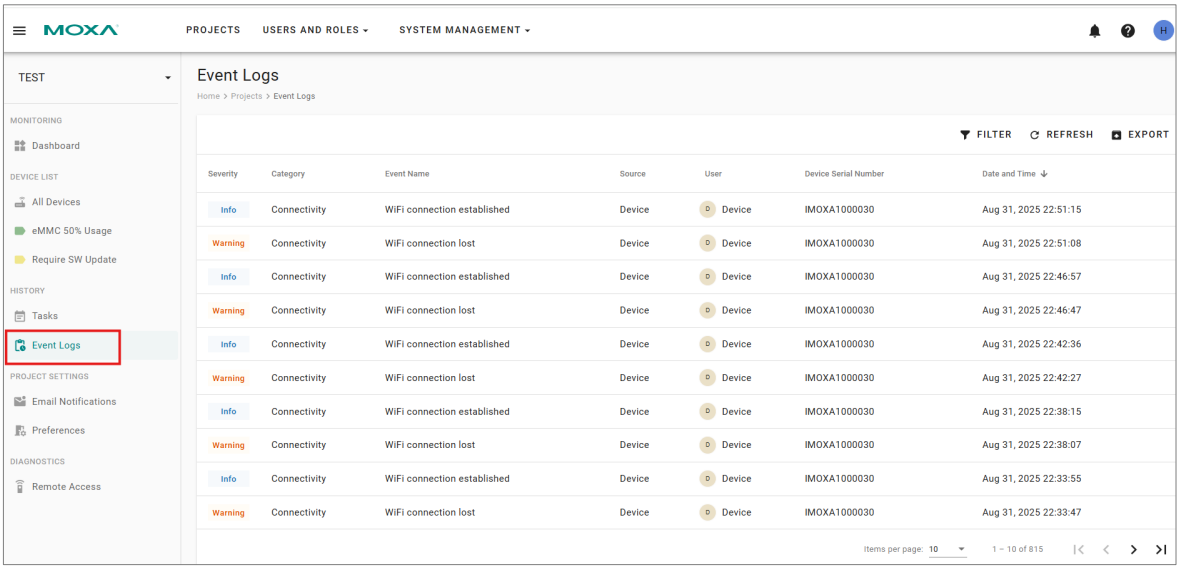
- **Scheduled:** The task is scheduled to run at a future time.
- **In Progress:** Tasks have been dispatched to devices; the system is waiting for device responses.
- **Success:** All devices (except those canceled) have completed the task successfully.
- **Partial Success:** At least one device completed the task successfully.
- **Failed [Reason]:** All devices (except canceled ones) failed the task with the same failure reason. Reasons can be:
  - Error
  - Device Offline
  - Timed Out
- **Failed:** All devices (except canceled ones) failed, but the reasons differ among devices.
- **Canceled:** All device tasks were canceled.

Child Layer Status Definitions

- **Scheduled:** The device's task is scheduled for future execution.
- **In Progress:** Task is currently executing on the device.
- **Success:** The device successfully completed its task.
- **Canceled:** The task was canceled on this device.
- **Failed - Error:** Task failed due to an error reported by the device.
- **Failed - Timed Out:** The device failed to respond within the expected time.
- **Failed - Device Offline:** The device was unreachable or powered off during task execution.

Event Logs

All events related to devices within the project are aggregated and displayed on this page. For detailed log descriptions, refer to **Appendices – Event Log List**.

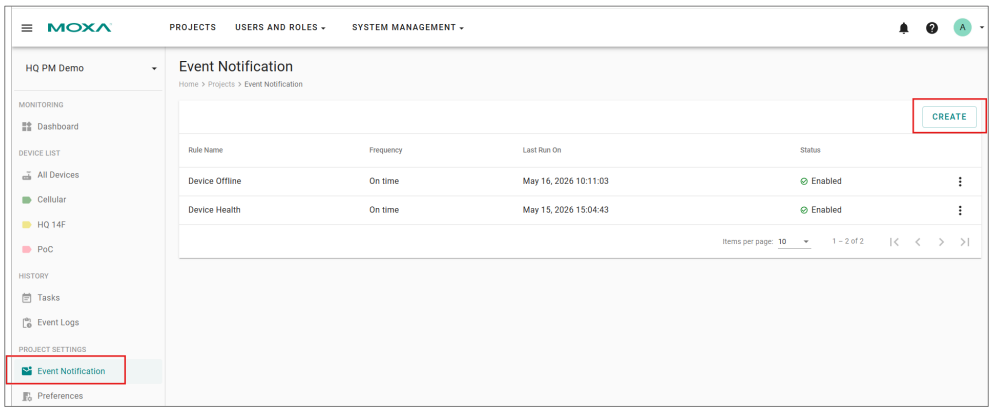


Event-based Email Notifications

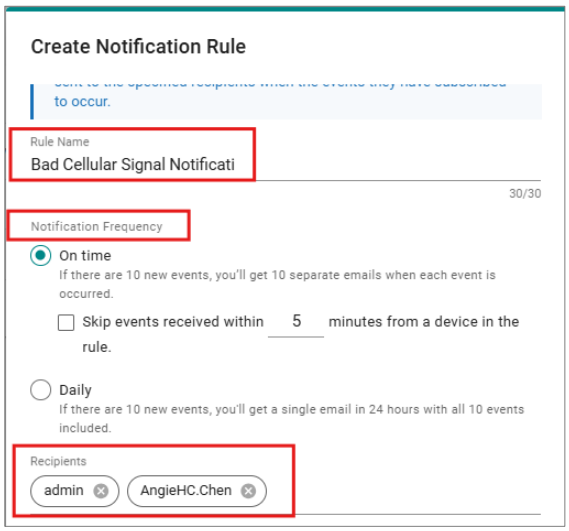
You can create email notifications that are triggered based on the Service and device-related events. NOTE that the SMTP server is required for sending the email notifications. You may refer to Appendices section on **SMTP Installation** for more information. To create an email notification, following the steps below:

Create an Notification Rule

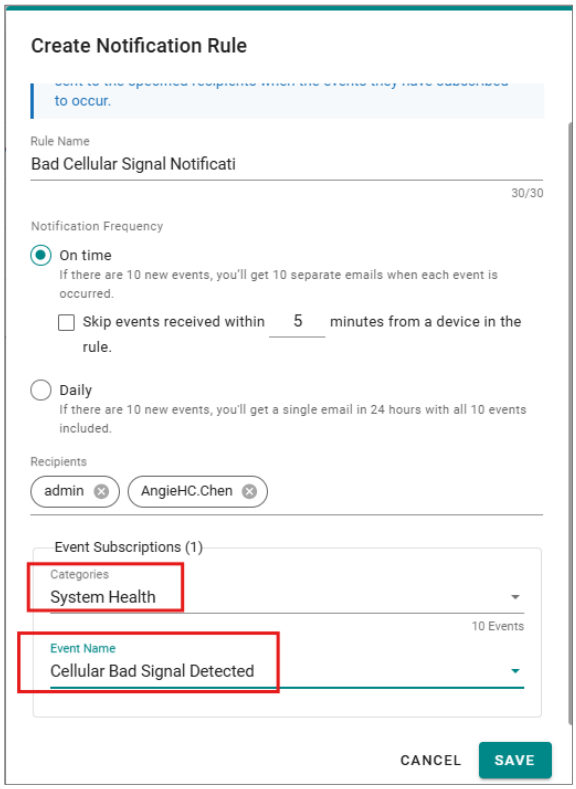
1. Click Email Notifications in the main menu, and click **CREATE**.



2. Specify a **Task Name, Notification Frequency**, and **Recipients**.



3. Select a category, such as System Health, and choose the event name you want to monitor. Click **DONE** to add the event subscription.



4. Click **SAVE**.

Available Events List

Events are grouped by source type:

- **[DLM]** indicates events generated by the DLM server.
- **[Device]** indicates device-specific events reported by devices to the DLM server.

Category	Events
[DLM] Connectivity	• Device online • Device offline
[DLM] Operation	• Request device delete • Cancel scheduled task • Remote connect established • Remote connect establish fail • Failed to send notification ➢ Triggered when DLM cannot send an email notification, for example, due to an unavailable email server.
[Device] Connectivity	• Cellular connection established • Cellular connection lost • Ethernet connection established • Ethernet connection lost • Wi-Fi connection established • Wi-Fi connection lost • Cellular Signal Drop Detected ➢ Triggered when RSRP drops by more than 20 dB from the previous sample.
[Device] Operation	• Install package success • Install package failed • Firmware upgrade success • Firmware upgrade failed • Import configuration success • Import configuration failed • Export configuration success • Export configuration failed • Reboot success • Reboot failed • Script execute success • Script execute failed • SIM card change • Remote access established failed
[Device] Security	• Device login failed • Device login success
[Device] System Health	• Cellular bad signal detected • Unexpected system reboot detected ➢ Triggered when system detected an unexpected reboot, possibly due to power failure or system crash • System reboot ➢ Triggered when the system performs a normal reboot, such as a reboot initiated by a user or program. • Storage near end-of-life (90–100% used) • Storage end-of-life reached (100%+ lifetime used) • Storage usage alarm (85% used) • Storage usage alarm (95% used) • CPU Temperature Too High ➢ Triggered when the CPU temperature reaches the threshold defined in user.yaml.

Notification Email Format

Notification emails use the following subject format:

`[DLM Notification] <Event Name>: <Display Name> (<Project Name>)`

Where:

- **Event Name** indicates the event that triggered the notification, such as **Device offline**.
- **Display Name** is the device name assigned by the DLM user. If no display name is assigned, the device serial number is shown instead.
- **Project Name** is the name of the project that the device belongs to.

For example:

`[DLM Notification] Device offline: Traffic Cabinet Controller-12 (Smart City)`

Preferences

1. **Auto Logout User When Inactive**

   You can specify a duration to automatically log out users after a period of inactivity. Click **EDIT** to set the auto-logout duration.

2. **Auto Logout from Project-Level Dashboard**

   To enable this option, Auto Logout User When Inactive must also be enabled.

   If Auto Logout from Project-Level Dashboard is disabled, the system will not automatically log out users from the project-level dashboard, even if Auto Logout User When Inactive is enabled.

6. System Integration Using RESTful APIs

The DLM Server provides a set of RESTful GET APIs that allow external systems to retrieve operational data from the DLM platform. Using the APIs, you can integrate DLM device information, health metrics, and telemetry into your dashboards, IT/OT systems, or enterprise monitoring tools. See DLM REST API Documentation for more information.

NOTE

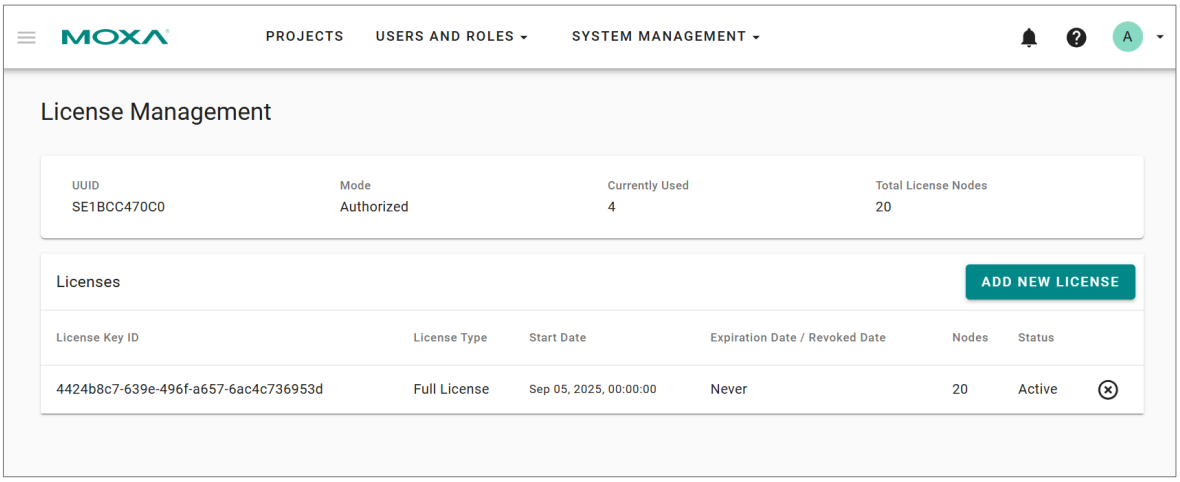
The DLM REST API is read-only. It supports data retrieval but does not allow configuration changes, device control, or management operations.

7. License Management

License Management Overview

The **License** screen displays information about your DLM license, including the number of licensed nodes currently in use. You can also use the **License** screen to add a new license or deactivate an existing license.

To access the **License** management screen, you must have the admin role. Navigate to **SYSTEM MANAGEMENT > License**.

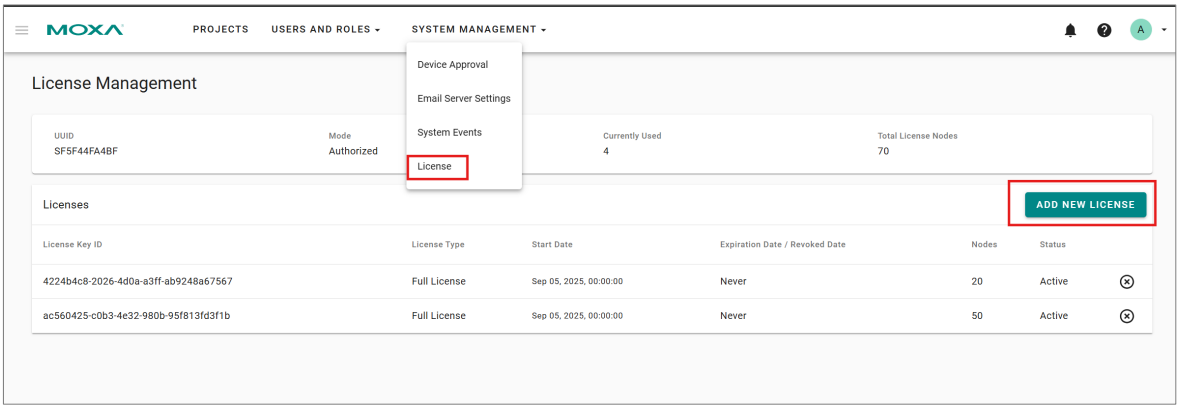


The **License** screen displays the license mode, the number of nodes in use, and the total number of nodes available under the current license.

NOTE

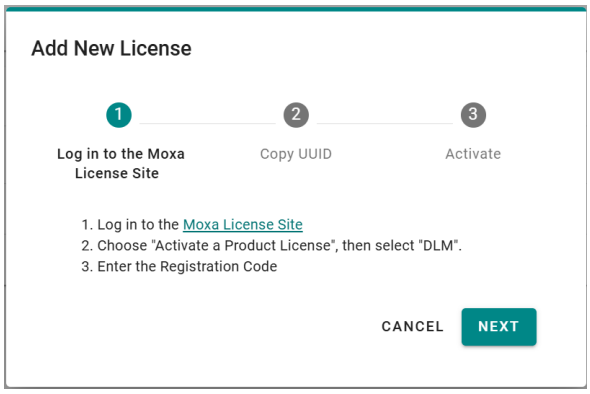
DLM has a built-in trial period of 30 days with max. 5 nodes supported. To extend the trail period of add more nodes, contact the nearest Moxa regional sales office.

Adding a New License

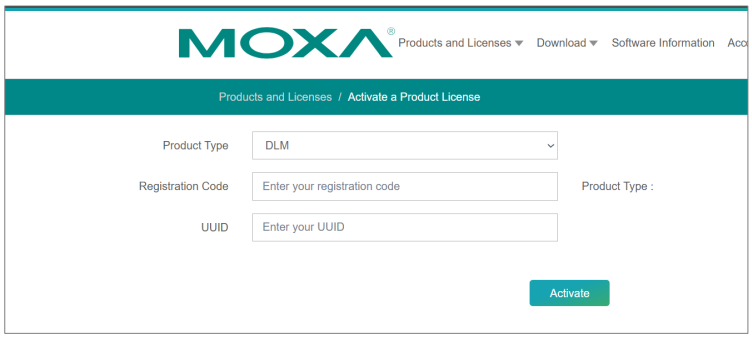


1. Navigate to **SYSTEM MANAGEMENT > License**.
2. Click **Add New License**.

   The **Add New License** screen appears.

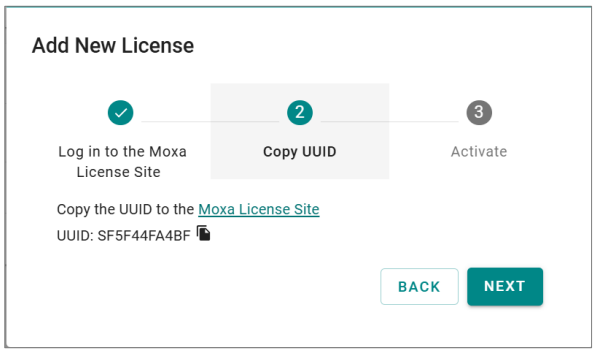


3. Open a web browser and go to Moxa Software License Portal (https://license.moxa.com).
4. Log in using your Moxa account and select **DLM** as Product Type.

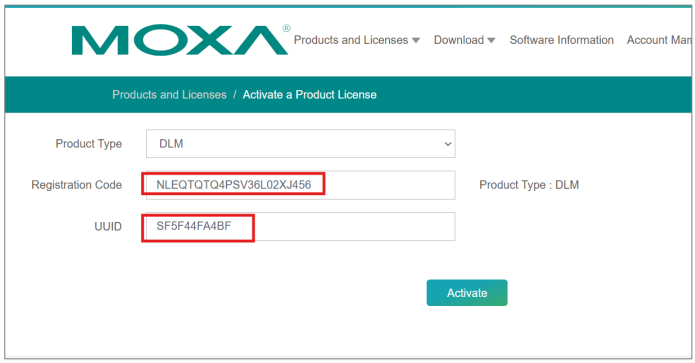


5. Go back to DLM web UI and click **Next** on **Add New License** screen.

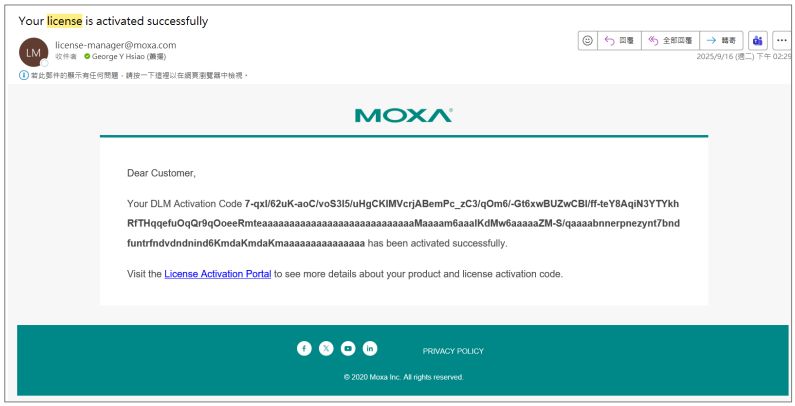
6. Copy the **UUID** shown on screen.



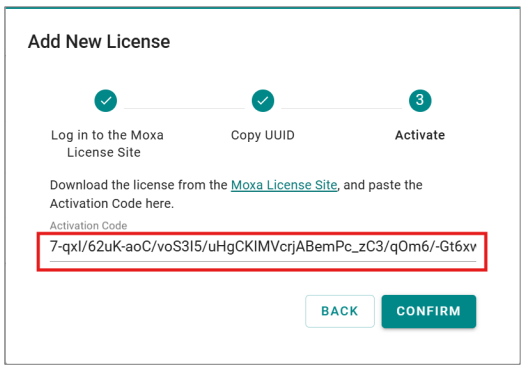
7. Switch to Moxa Software License Portal.
8. Enter the **UUID** and **registration code** you received from license-manager@moxa.com after placing your order.



9. Click **Activate**.
10. You will receive the activation code.



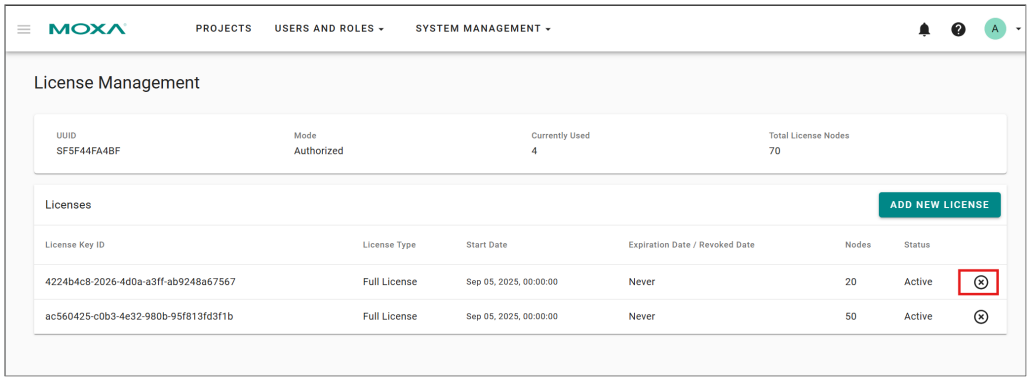
11. Copy and paste the **Activation Code** to DLM web UI and click on **CONFIRM** to complete license activation process.



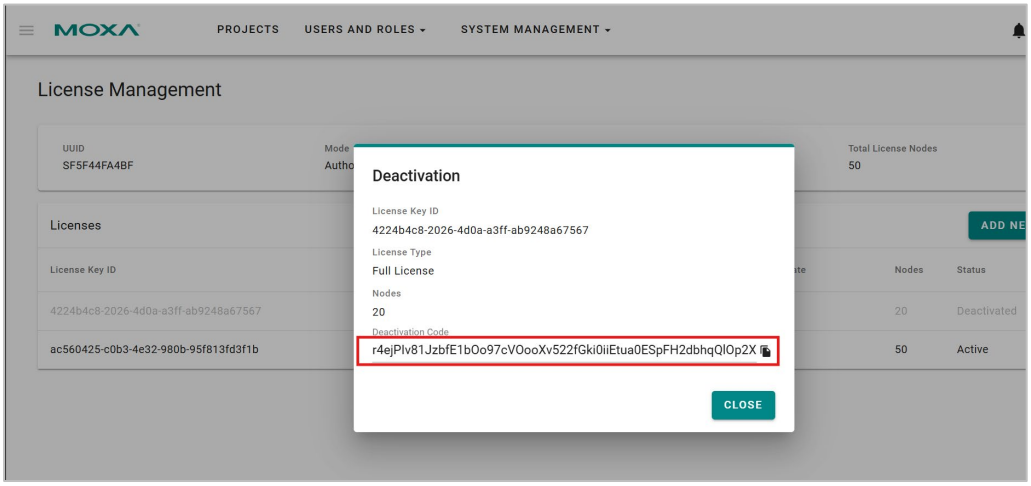
Transferring a License to Another DLM Instance

If you want to transfer a license to a different instance of DLM, the license has to be deactivated first then use the deactivation code to exchange for a new license.

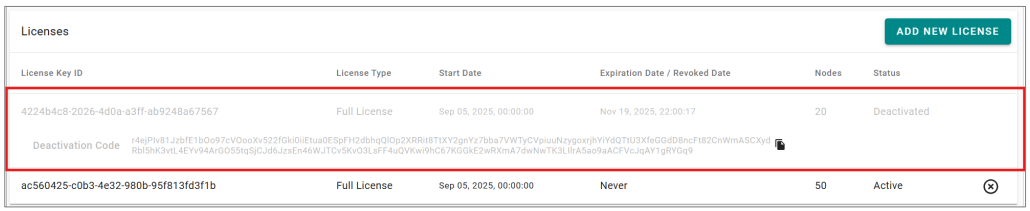
1. Navigate to **SYSTEM MANAGEMENT > License**.
2. Select the license you would like to transfer.
3. Click on the **deactivate** button.



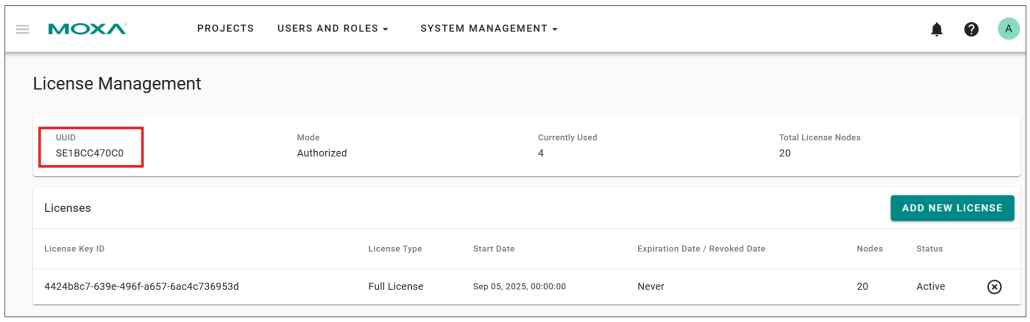
4. After confirmation, you will get a **Deactivation Code**.



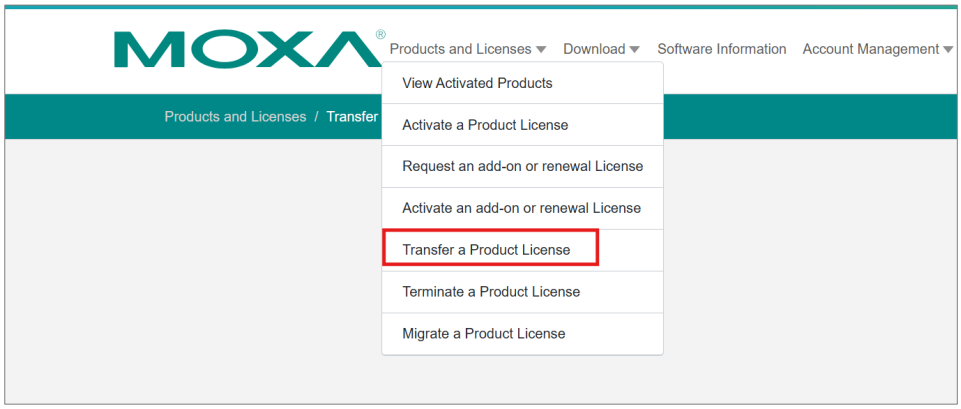
5. The license will now appear deactivated.



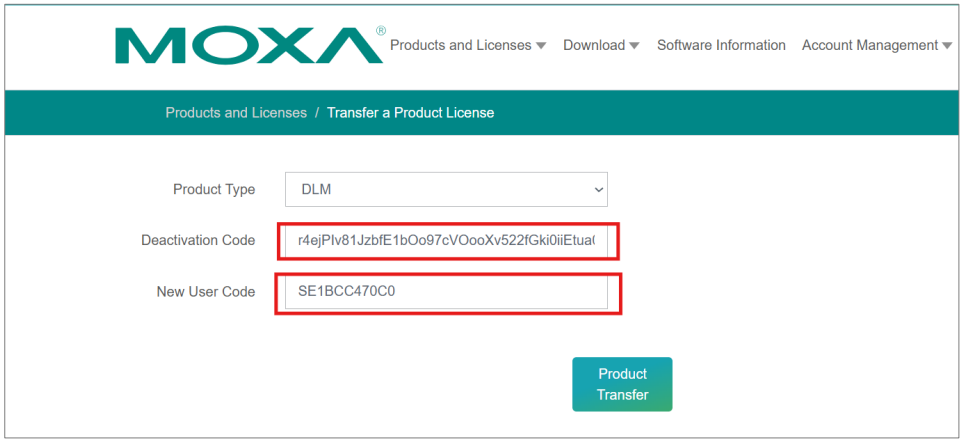
6. Set up a new DLM instance and find the **UUID**.



7. Open a web browser and go to the Moxa Software License Portal. Navigate to **Product and Licenses > Transfer a Product License**.



8. Enter the **Deactivation Code** from the original DLM instance and the **UUID** from the new DLM instance. Click Product Transfer.



9. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license fails to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa Support.
10. Check the email account you used to apply for your moxa account. The new activation code will be sent to this email address.
11. Copy the activation code from the email.
12. Follow **Adding a New License** procedure to activate the license on your new DLM instance with the activation code.

8. Backup and Recovery

To maintain system reliability and ensure data continuity, administrators should implement a regular backup strategy for the DLM Server. Depending on where the DLM Server is hosted, different backup and recovery methods are recommended. This chapter describes three supported scenarios:

- Backup and recovery for on-premises or non-cloud virtualized deployments
- Migrating the DLM Server between cloud providers (e.g., AWS → Azure)
- Backup and recovery for cloud-hosted DLM Servers (e.g., AWS, Azure, GCP)

Each scenario has different requirements and recommendations to ensure successful system continuity.

Scenario 1—Backup and Recovery for Non-cloud or On-premises Installations

For DLM Servers **not hosted on cloud VM infrastructure**, such as:

- On-premises physical servers
- Local virtual machines (VMware, Hyper-V, Proxmox)
- Edge computing environments

Moxa provides a built-in **DLM Database Backup/Restore Tool** using the CLI-based `dlm` command.

Backup Method

1. To back up the DLM database, run **`dlm backup`**
2. This command will:
   - Temporarily stop DLM services
   - Package the internal database
   - Encrypt the backup using a password
   - Generate a file named **`dlm-backup-YYYYMMDDxxxx.tgz.en`**

```
root@ip-172-31-5-167:/mnt/data/backup# dlm backup
DLM service will unavailable during backup. do you want to continue? [y/N] y
Enter password for backup file encryption:
[+] Stopping 7/7
 ✔ Container dlm-nginx            Stopped
 ✔ Container dlm-maf              Stopped
 ✔ Container dlm-api              Stopped
 ✔ Container dlm-host-app         Stopped
 ✔ Container dlm-lwm2m            Stopped
 ✔ Container dlm-ssh-web-console  Stopped
 ✔ Container dlm-emqx             Stopped
Backup file has been created at:
./dlm-backup-202503180321-a4929.tgz.enc
```

3. Validate the integrity of the backup by running `dlm verify-backup ${DLM_BACKUP_FILENAME}`

```
root@ip-172-31-5-167:/mnt/data/backup# dlm verify-backup dlm-backup-202503180321-a4929.tgz.enc
Enter password for backup file decryption:
Backup file is valid.
root@ip-172-31-5-167:/mnt/data/backup#
```

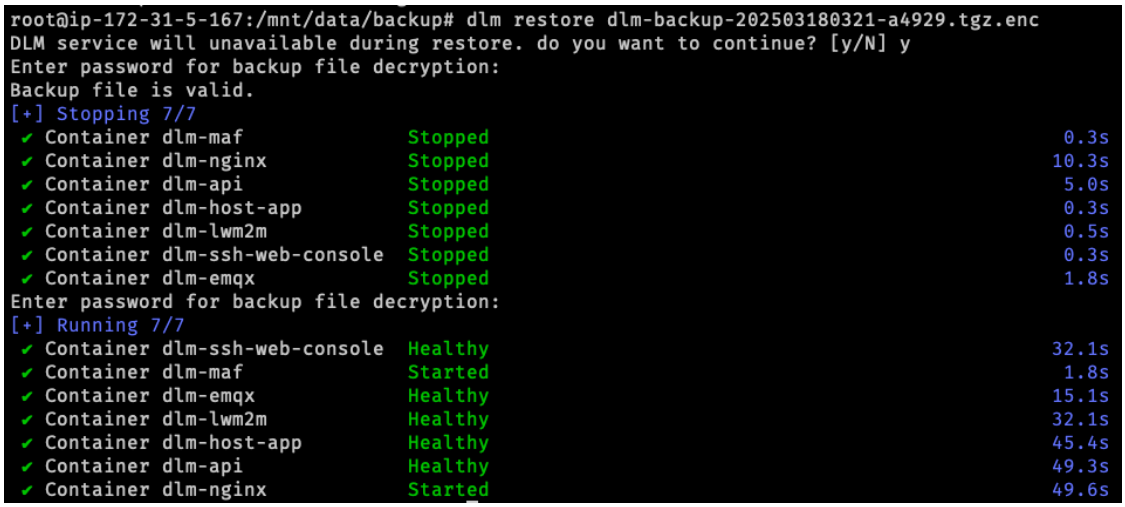
4. Store this file in a secure location offline or on centrally managed storage.

Recovery Method

To restore the DLM database from a backup, run `dlm restore ${DLM_BACKUP_FILENAME}`

Requirements:

- The same version or a newer version of the DLM Server must be installed before performing the restore. For example:
  - A backup created on DLM v1.1.0 may be restored on v1.1.0 or later;
  - A backup created on v1.2.0 cannot be restored on a server running v1.1.0.
- DLM services will be temporarily unavailable during the restore process.
- The system will restart all components after the restore is complete.



When to Use This Method

- The server is deployed outside cloud VM platforms.
- A lightweight backup that does not include OS-level contents is preferred.
- The backup must be transferred to another machine manually.
- Application-level database integrity is required, not a full VM image.

Scenario 2—Migrating DLM Server Between Cloud Providers (e.g., AWS → Azure)

In some cases, you may want to move the DLM Server deployment from one cloud platform to another (e.g., AWS → Azure, Azure → GCP, GCP → AWS). Since VM snapshots are not compatible across cloud vendors, the migration must be performed using DLM's built-in database backup/restore mechanism.

Migration Procedure

1. On the original cloud VM: run `dlm backup` and save the encrypted backup file (`.tgz.enc`).
2. On the new cloud VM (destination): install the same version of the DLM Server and verify it is functional.
3. Restore the database: run **`dlm restore dlm-backup-xxxx.tgz.enc`**, enter the encryption password, and allow the system to process and restart.
4. Confirm migration success: log in to the DLM Web UI and verify that devices, tasks, logs, and settings are intact, and that all services show as Healthy.

NOTE

- Only the DLM database is migrated; OS-level configurations are not transferred.
- The destination VM must match the system requirements of DLM.
- External networking, DNS records, firewall rules, and TLS certificates may need to be updated.
- Device reconnection behavior depends on the server's FQDN: if the new cloud VM uses the same FQDN, devices can typically reconnect automatically. If the FQDN changes — or if devices were configured using an IP address instead of an FQDN — devices must be re-registered with the new DLM Server.

Scenario 3—Backup and Recovery for Cloud VM

Deployments

When the DLM Server is deployed on public cloud platforms such as AWS, GCP, or Microsoft Azure, administrators may use the cloud provider's native VM Snapshot or Image Backup capabilities as part of their backup strategy.

Backup Method

If you choose to use native VM snapshot or image backup capabilities, you should also perform a **DLM database backup** alongside them. Snapshot behavior can vary based on factors such as cloud platform, VM type, disk configuration, and operating system environment. Using cloud snapshots together with the DLM database backup tool provides the most reliable and consistent protection for your system.

Recovery Procedure

Recovery is performed directly through the cloud provider's management console by restoring the VM snapshot or launching a new VM instance from the saved snapshot or image.

After the VM is restored, verify that the DLM Server starts correctly and that all services are operating as expected. If issues occur after restoring a VM snapshot, reinstall the DLM software and use the database restore method described in Scenario 1 to recover the DLM service.

9. Trouble Shooting and FAQ

The following describes how to monitor the status of the DLM system, maintain its services, solve commonly encountered issues, and report issues using commands and tools to help administrators keep the platform running smoothly.

System Monitoring

You can use the `docker stats` command to view system resource usage. It is recommended to regularly monitor the following items:

1. **CPU Usage:** Check whether CPU usage is abnormally high to avoid impacting service performance.
2. **Memory Usage:** Monitor memory usage to ensure it doesn't exceed limits that could interrupt services.
3. **Disk Usage:** Check the host's disk usage to prevent space shortages from affecting log storage or system operation.

Application Monitoring

1. Use the **liveness endpoint** to check whether the DLM application services are functioning properly:
   - URL: **https://{domain}/healthz**
   - If the returned status code is `200` with content 'ok'. the service is operating normally.
   - It is recommended to integrate this into your monitoring system for periodic checks (e.g., once per minute).
2. Log Viewing
   - Use root privileges to execute the command `dlm log` to view logs for each service.
   - Each log file is limited to 5 MB in size by default.
   - Up to 1000 log files are retained.

DLM Server Upgrade

To upgrade the DLM, please refer to the **Installation & Upgrade** section in this DLM User Manual,

WARNING

- You must stop the DLM service by running the **`systemctl stop dlmg2`** command before starting the upgrade.
- It is also strongly recommended that you back up the entire system beforehand in case a system recovery is needed later.

Uninstalling DLM Server

This section guides you through the process of uninstalling the DLM Server software from your system. Follow the steps carefully to ensure a clean removal.

Steps to Uninstall DLM Server

1. Open a terminal on your system.
2. Execute the following command to remove the DLM software:

   ```
   apt remove --purge dlm
   ```

   This command uninstalls the DLM software and removes associated configuration files generated during installation.

Why Configuration and Database Are Not Removed

By default, the `apt remove --purge dlm` command does not delete the following directories:

- /opt/moxa/dlm
- /var/lib/dlm

This is intentional to prevent accidental data loss. These directories contain configuration files and the database used by the DLM Server. Retaining them allows users to reinstall the software later and restore previous settings or data without starting from scratch. However, if you no longer need this data, you can manually remove these directories.

Manually Removing Configuration and Database

If you wish to completely remove the configuration files and database, use the following commands with caution:

To remove the database:

```
rm -rf /var/lib/dlm
```

To remove the log files:

```
rm -rf /var/log/dlm
```

NOTE

These commands permanently delete all data in the specified directories. Ensure you have backed up any important information before proceeding. After completing the above steps, verify that the DLM Server is no longer running. You can reboot your system to ensure all processes are terminated. If you plan to reinstall the software, ensure the directories are either removed or properly backed up as needed.

Reporting Issues

This section explains how to collect diagnostic information and report issues related to the DLM system. The procedures below help administrators gather the necessary data for effective troubleshooting and support.

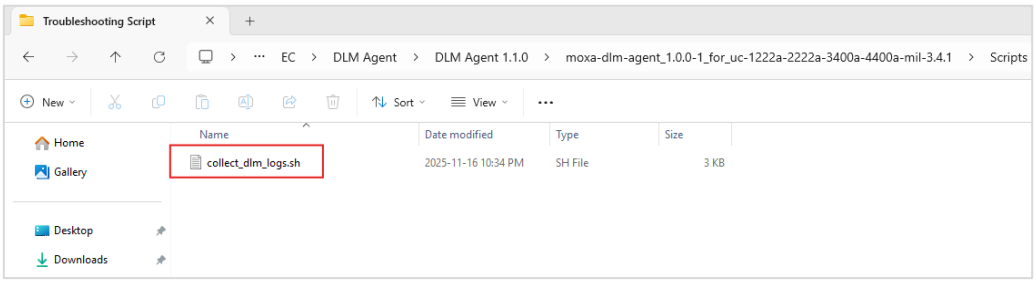
1. **DLM server:**

   Use root privileges to run the command `dlm diagnostic on the Ubuntu OS with DLM server`. The system will generate a `.tar.gz` diagnostic file.

2. **DLM agent:**

   To collect diagnostic information from a DLM agent running on a Moxa computer:

   - Copy the collect_dlm_logs.sh script included in the DLM agent installer (located under scripts/troubleshooting/) to the target device.



   - Execute the script to generate a .tar.gz diagnostic package.

3. Please send this file to Moxa Technical Support for further issue analysis.

FAQs

1. Why does it take a long time for my Moxa computer to reconnect to the DLM server after reboot?

   - If your Moxa computer uses Ethernet with both primary and secondary DNS servers configured, please make sure both DNS servers can resolve the DLM server' s domain name.

     Linux will query the DNS servers in order, but whichever server replies first will be used. If the responding server is misconfigured (e.g., cannot resolve the domain), the system may either fail immediately or wait through long timeouts (often over 30 minutes) before trying the other server.

     To avoid long delays, configure both DNS servers correctly so they can resolve the DLM server's domain name.

2. When installing the DLM server software, installation stops with "E: No packages found / Handler silently failed" error.

   - It is likely that you are not installing the software on x86-64 architecture hardware, which is required. Please verify your system architecture.

3. When running a script that reboots the device or restarts the DLM agent. Why does DLM always show the execution result is failed?

   - If your script breaks the connection (for example, running reboot, power off, or systemctl restart dlm-agent), the DLM agent will have no chance to report the script result back to the server before the connection drops.

     Solution: Add a short delay so the agent can send the result first, then perform the disruptive action.

     Following is an example reboot script

```
#!/bin/bash
#
# delayed-reboot.sh
# Schedule a reboot in 20 seconds using systemd-run

echo "Reboot scheduled in 20 seconds..."
systemd-run --on-active=20 /sbin/reboot
```

     This way the script reports success, waits 20 seconds, then reboots.

4. Authentication token or cookie validation errors.
   - Incorrect system time causes authentication token or cookie validation errors. Enable NTP synchronization to keep the system clock accurate.
5. First-time login: After changing the password, “cookie token is empty” appears
   - This usually happens when the customer is not using a fully qualified domain name (FQDN) or static IP for the DLM URL. If the URL used to access DLM does not match the URL specified during server installation, authentication fails.

     Solution: Access the DLM web interface using the same FQDN or static IP configured during installation.
6. DLM login suddenly stops working even though it shows “Success”
   - This typically occurs when the customer is not using an FQDN, and the **DLM server IP has changed**, causing token validation to fail.

     Solution: Always access DLM using an FQDN so authentication tokens remain valid even if the server IP changes.

10. Appendix

Service Features

Description	Quantity
Max number of devices in project	1,000 for minimum hardware requirement 3,000 for recommended hardware requirement
Max number of projects	100
Event record retention period	180 (days)
Maximum number of records per exported report	10,000 (records)

Event Log List

Event Level	Severity	Category	Source	Event Name
Company	Info	User	DLM	Invite user
Company	Info	User	DLM	Update user
Company	Warning	User	DLM	Delete user
Company	Alert	User	DLM	User login failed
Company	Info	User	DLM	User login success
Company	Info	User	DLM	Export user inventory report
Company	Info	Project	DLM	Create project
Company	Info	Project	DLM	Update project
Company	Info	Project	DLM	Delete project
Company	Info	System	DLM	Update SMTP configuration
Company	Info	System	DLM	System Storage <20 GB
Company	Warning	System	DLM	System Storage <10 GB
Company	Alert	System	DLM	System Storage <5 GB
Project/Device	Info	Operation	DLM	Request device {$jobAction} • firmware upgrade • install package • import configuration • export configuration • run script • reboot • delete • export report
Project/Device	Info	Operation	DLM	Cancel scheduled task
Project/Device	Info	Operation	DLM	Initiated scheduled task {$action} • firmware upgrade • install package • import configuration • export configuration • run script • reboot
Project/Device	Info	Device	DLM	Device enrollment approved
Project/Device	Info	Device	DLM	Device project transfer
Project/Device	Info	Device	DLM	Device project transfer
Project/Device	Info	Connectivity	DLM	Device online
Project/Device	warning	Connectivity	DLM	Device offline
Project	Info	Operation	DLM	Create notification
Project	Info	Operation	DLM	Notification deleted
Project	Info	Operation	DLM	Notification modified
Project	Info	Operation	DLM	Notification disabled
Project	Info	Operation	DLM	Notification enabled
Project/Device	Info	Operation	DLM	Request device remote connect

Event Level	Severity	Category	Source	Event Name
Project/Device	Info	Operation	DLM	Remote connect established
Project/Device	Info	Operation	DLM	Remote connect terminated
Project/Device	Info	Operation	DLM	Remote connect establish fail
Project/Device	Info	Operation	DLM	Remote connect terminate fail
Project/Device	Info	Operation	Device	Remote access connect
Project/Device	Info	Operation	Device	Remote access disconnect
Project/Device	Info	Operation	Device	Remote access established failed
Project/Device	Alert	Operation	Device	Install package failed
Project/Device	Info	Operation	Device	Install package success
Project	Info	Operation	DLM	Failed to send notification
Project/Device	Info	Connectivity	Device	VPN tunnel connected
Project/Device	Alert	Connectivity	Device	VPN tunnel disconnected
Project/Device	Info	Operation	Device	Firmware upgrade success
Project/Device	Alert	Operation	Device/DLM	Firmware upgrade failed
Project/Device	Info	Operation	Device	Import configuration success
Project/Device	Alert	Operation	Device/DLM	Import configuration failed
Project/Device	Info	Operation	Device	Script execute success
Project/Device	Alert	Operation	Device/DLM	Script execute failed
Project/Device	Info	Operation	Device	Reboot success
Project/Device	Warning	Connectivity	Device	Cellular connection lost
Project/Device	Info	Connectivity	Device	Cellular connection established
Project/Device	Warning	Connectivity	Device	Cellular Signal Drop Detected
Project/Device	Info	Connectivity	Device	Ethernet connection established
Project/Device	Warning	Connectivity	Device	Ethernet connection lost
Project/Device	Info	Connectivity	Device	Wi-Fi connection established
Project/Device	Warning	Connectivity	Device	Wi-Fi connection lost
Project/Device	Alert	System health	Device	Unexpected system reboot detected
Project/Device	Warning	System health	Device	System reboot
Project/Device	Warning	System health	Device	Cellular bad signal detected
Project/Device	Alert	System health	Device	CPU Temperature Too High
Project/Device	Warning	System Health	Device	Storage near end-of-life (90-100% used)
Project/Device	Alert	System Health	Device	Storage end-of-life reached (100%+ lifetime used)
Project/Device	Warning	System Health	Device	Storage usage alarm (85% used)
Project/Device	Alert	System Health	Device	Storage usage alarm (95% used)
Project/Device	Alert	Security	Device	SIM card change
Project/Device	Alert	Security	Device	Device login fail
Project/Device	Info	Security	Device	Device login success