

AIG QuickON User Manual

Version 1.0, November 2025

www.moxa.com/products



© 2025 Moxa Inc. All rights reserved.

AIG QuickON 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

© 2025 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

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	4
2. Installing AIG QuickON.....	5
Prerequisites	5
Installing AIG QuickON	7
3. Configuring AIG QuickON	11
AIG QuickON Configuration Modes	11
Configuring By Device	11
Configuring By Plan.....	13
Checking for Updates	21
A. Configuring Services on the AIG.....	22
Configuring the Azure IoT Device/Azure IoT Edge Service.....	22
Configuring the Azure DPS Service.....	23
Configuring the Moxa DLM Service.....	24
Configuring the AWS IoT Core Service.....	25

1. Introduction

AIG QuickON is a powerful utility designed for rapid and efficient deployment of AIG devices. Be it deploying a single device or managing large-scale deployments, AIG QuickON completes setups quickly, saving you valuable time and resources.

Key features include:

- **Security Setting:** Easily configure security parameters to ensure devices are protected according to your needs
- **Software Upgrade:** Automatically detect and upgrade software on AIG devices to ensure they always have the latest features and security enhancements
- **Configuration Import:** Seamlessly import pre-configured settings files into new devices or export current configurations for future use
- **Cloud Enrollment:** Effortlessly register AIG devices to cloud services for remote management and monitoring

AIG QuickON provides a comprehensive and reliable solution to streamline deployment challenges across various scales of AIG device deployments.

The eligible AIG Series products are listed in the following table:

QuickON Version	Supported Model	Note
v1.1.x or prior	AIG-101 AIG-302	
v1.2.0 or later	AIG-101 AIG-301 AIG-302 AIG-501 AIG-502	As required by RED 18031-1, this version is designed to trigger default password modification upon first use.

2. Installing AIG QuickON

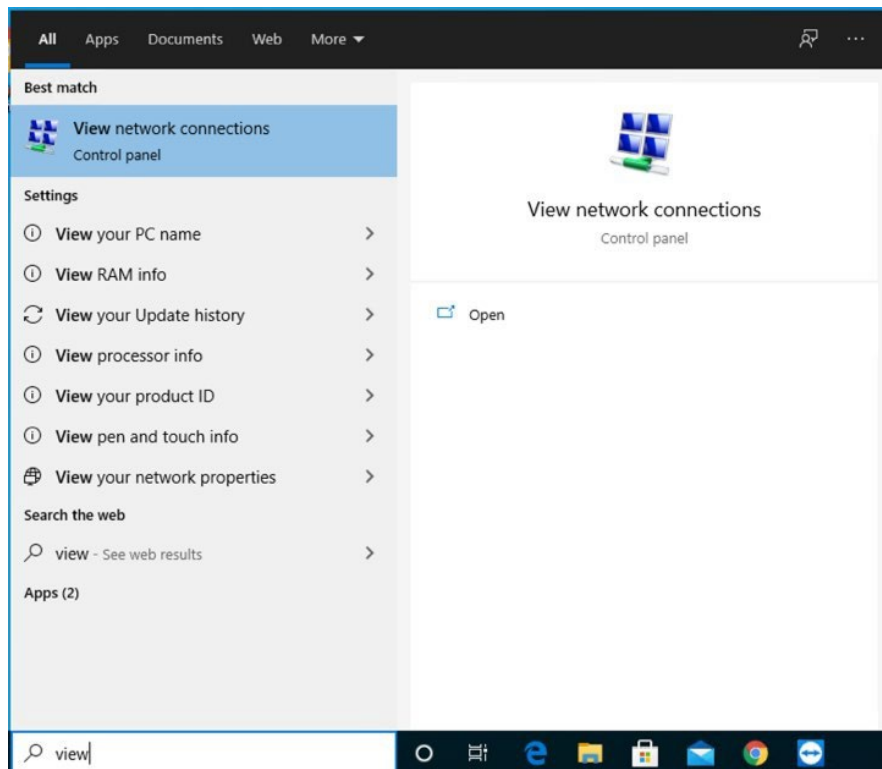
Prerequisites

- Windows 10 OS and Google Chrome browser on the PC.
 - Windows 10 version 1809 or later
 - Google Chrome 86.0.4240.183 (64 bit) or later
- Enable the IPv6 link-local address on the PC.

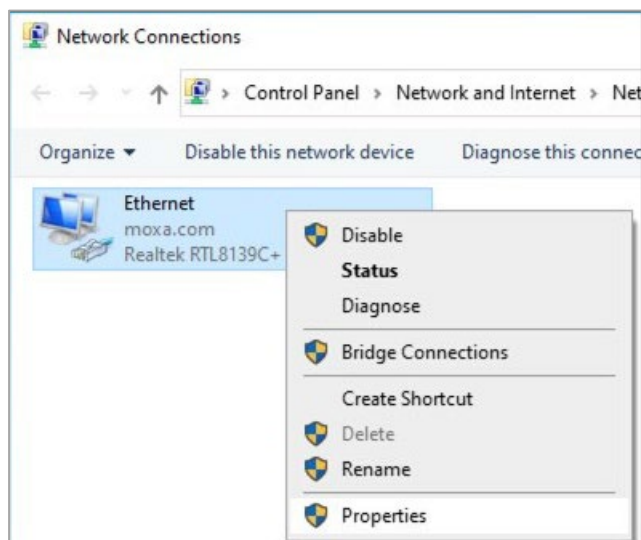
Enabling the IPv6 Link-local Address

To enable the IPv6 link-local address on your PC, do the following:

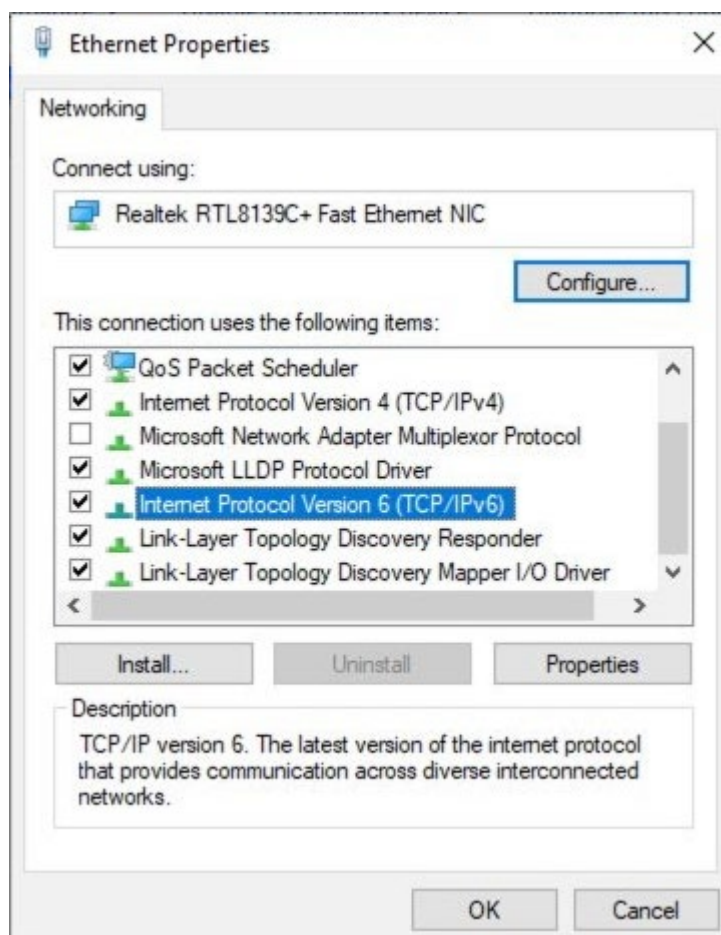
1. In the Windows search box, enter **view network connections** and click on **Open**.



2. Select the network adapter that to use to discover Moxa devices, right-click on the network adapter, and select **Properties**.



3. Select the **Internet Protocol Version 6 (TCP/IPv6)** option.



NOTE

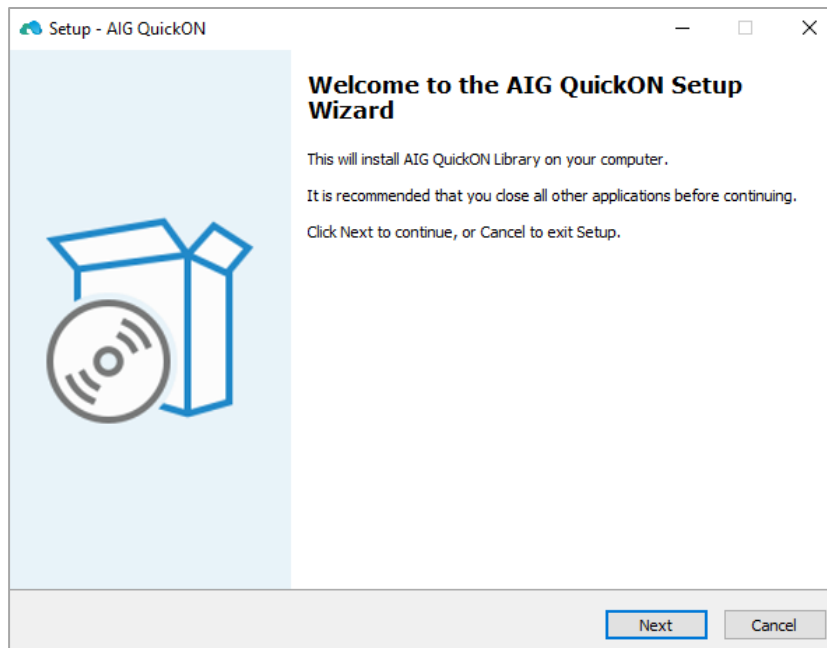
Ensure that the service port 5001 (local host) is available to the AIG QuickON web server.

4. Click **OK** to apply the changes.

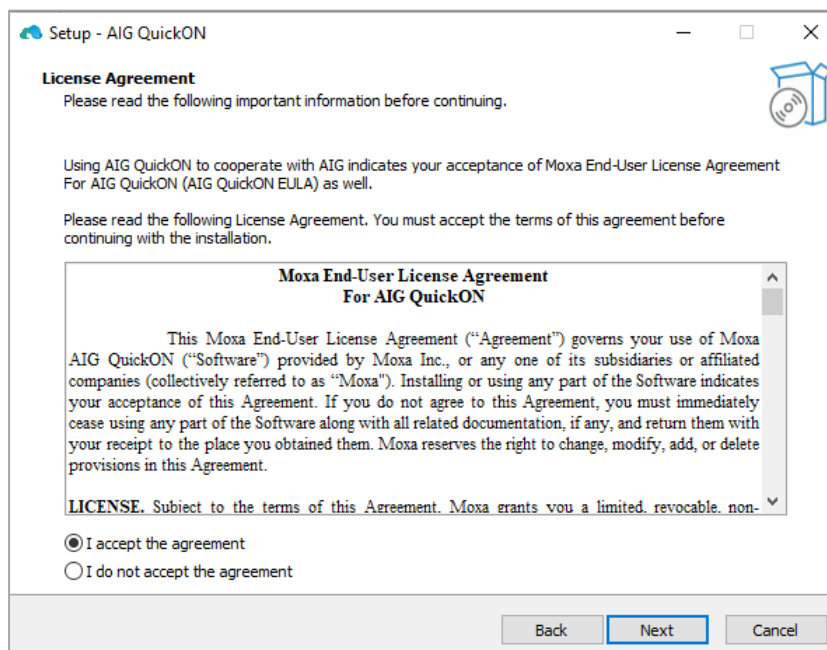
Installing AIG QuickON

To install AIG QuickON, do the following:

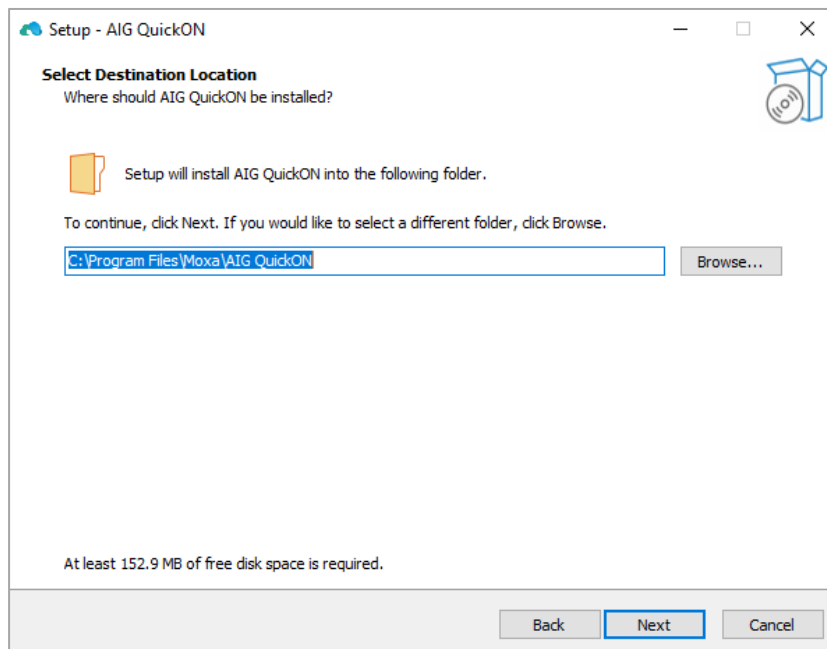
1. Download and run the AIG QuickON installation file **AIG-QuickON-x.x.x-xxxxxxxxxxxxx.exe**.



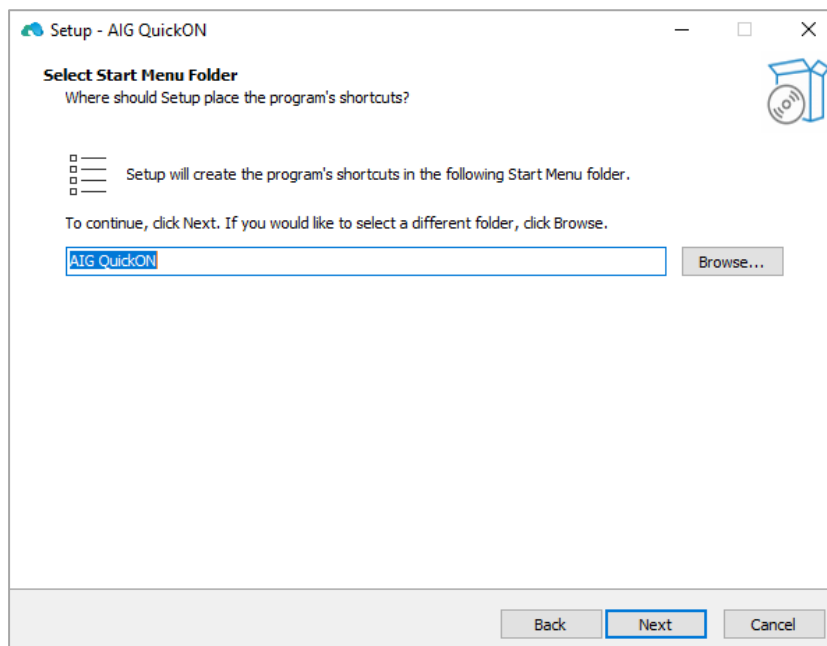
2. Click **Next**.
3. Select the **I accept the agreement** option and click **Next**.



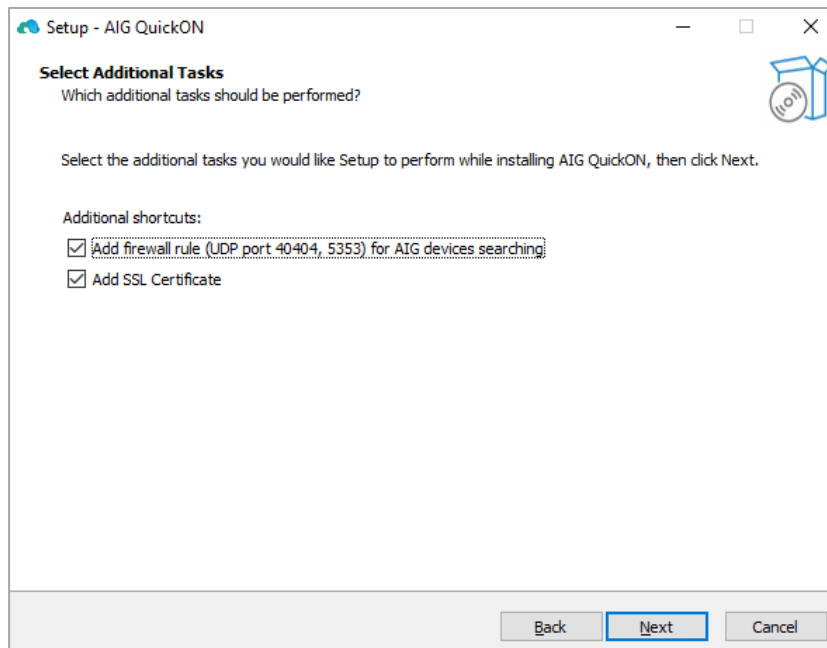
4. Specify the folder to install AIG QuickON in and click **Next**.



5. Specify the folder to create an AIG QuickON shortcut in and click **Next**.



6. Click **Next** again to confirm the installation settings.

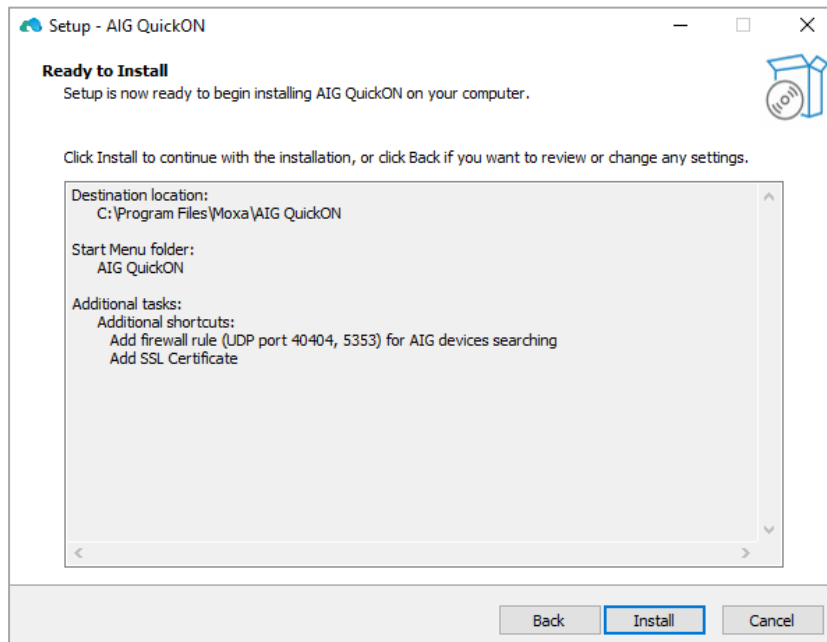


7. Click **Install**.

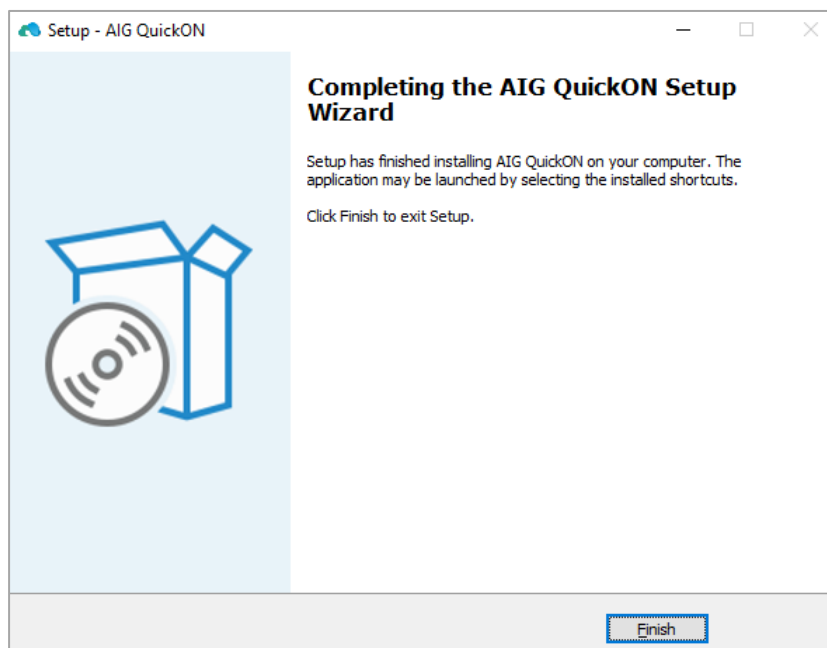


NOTE

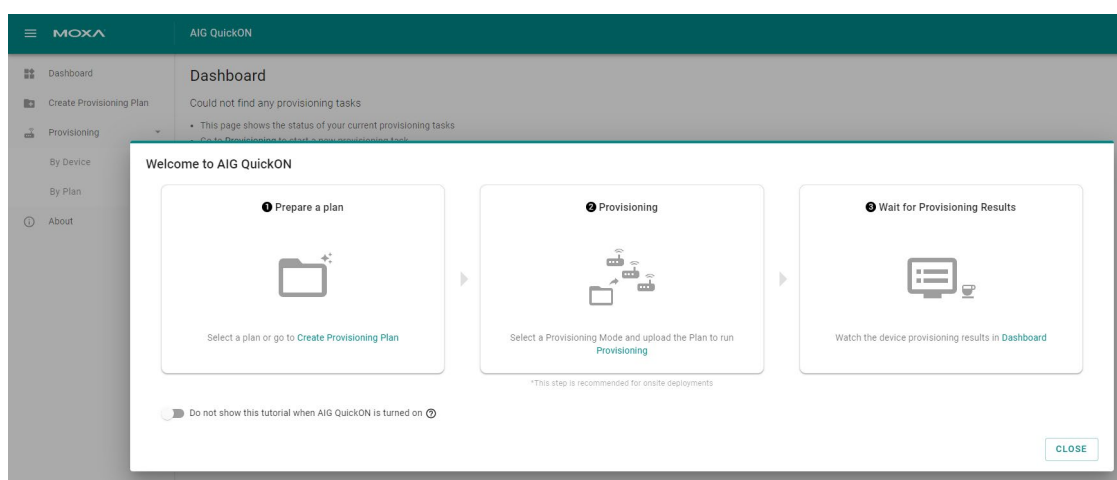
A command line console window (Windows cmd) will open during the installation process. DO NOT close the cmd window.



- After the installation process is complete, click **Finish**.



- Launch the AIG QuickON by Navigating to **Start > AIG QuickON**



3. Configuring AIG QuickON

AIG QuickON Configuration Modes

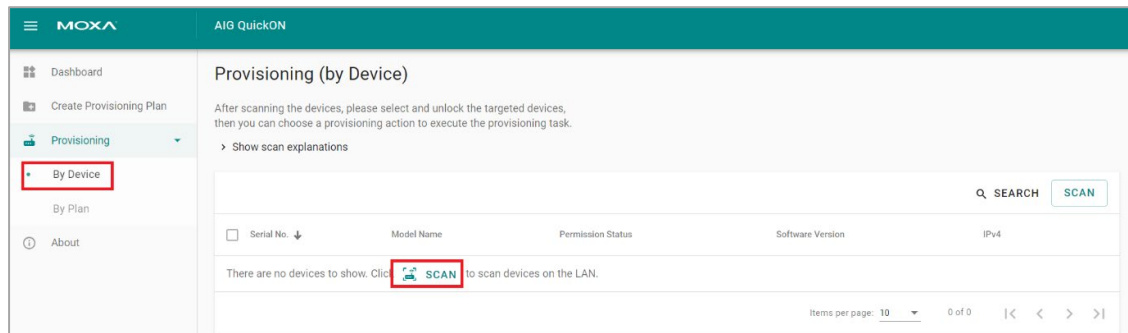
AIG QuickON offers two configuration modes:

- **By Device:** Typically used for running a single task such as software update or configuration import for multiple devices.
- **By Plan:** Typically used for running multiple tasks simultaneously, such as performing software updates and configuration imports at the same time. Aids in performing multiple coordinated tasks across multiple devices.

Select a configuration mode for the AIG QuickON based on your AIG deployment needs.

Configuring By Device

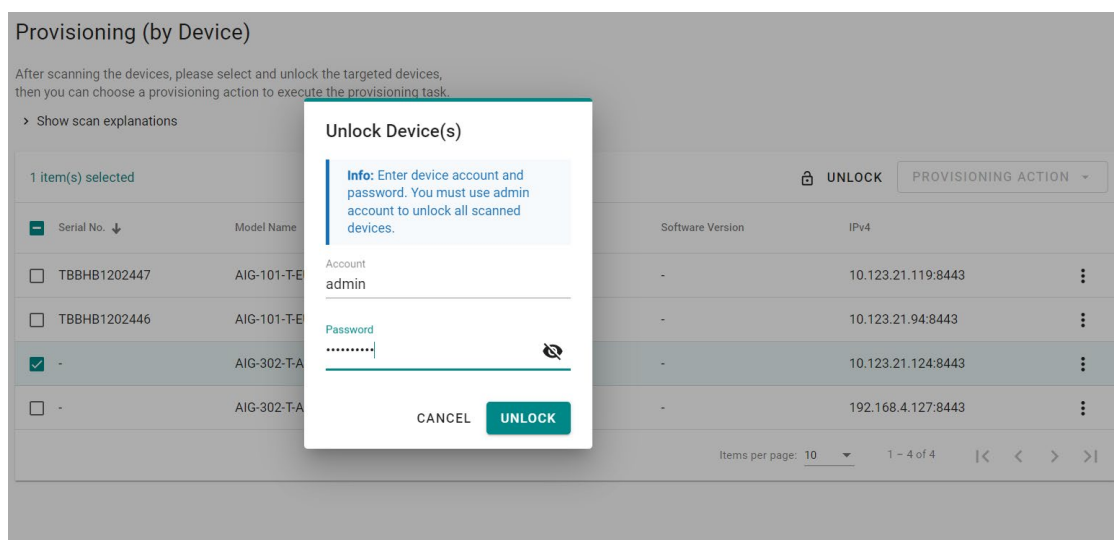
1. Go to **Provisioning (by Device)** page and click **SCAN**.



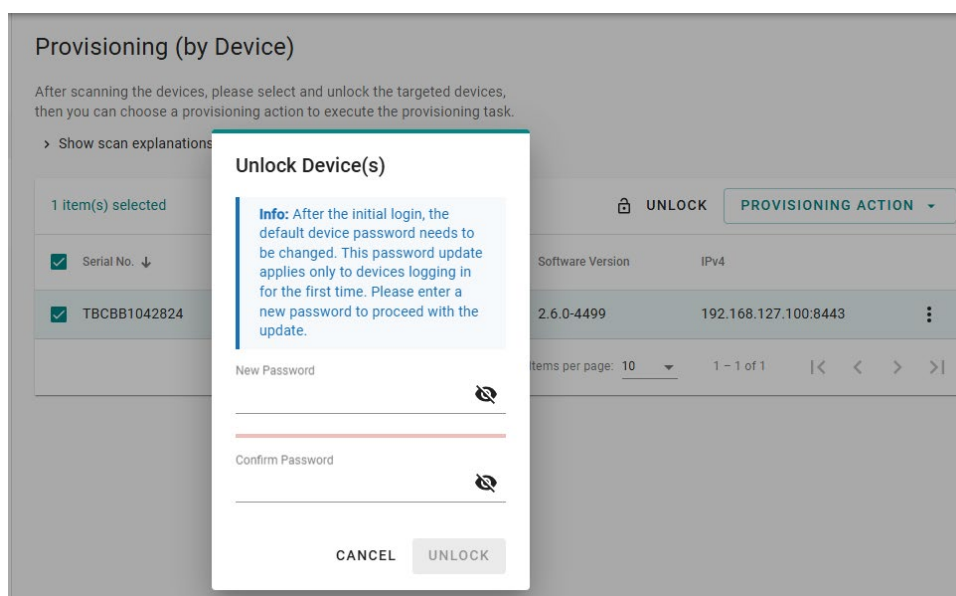
NOTE

AIG QuickON relies on the UDP port 40404 for scanning devices in the same network. Be sure to add UDP ports 40404 and 5353 to the firewall allowed list to enable proper device discovery of AIG devices.

2. Choose the target devices and **Unlock** them by entering the **Account** and **Password**.
The AIG devices are locked using a default account and password for higher security.
For example, AIG-302's default account is **admin** and default password is **admin@123**.



To comply with RED 18031-1 cybersecurity requirements, you must set a new password for the "admin" account and the SSH password for the terminal console.



NOTE

The unlock function is now designed for a device's first use. If the device has been previously used or reset to default configuration, we strongly recommend performing a full factory reset before using QuickON for provisioning; especially the console password reset via the web GUI. This ensures secure and efficient provisioning of a batch of devices in a consistent state.

3. Select tasks under PROVISIONING ACTION and configure them for the selected device(s).

You can configure the following tasks for devices:

- Set Network: Configure the network parameters such as IP address, netmask, and gateway.
- Import Config.: Import and apply a set of configurations to selected device(s).
- Export Config.: Export the configuration of the selected device(s) for backup purposes.
- Upgrade Software: Upload the upgrade pack to upgrade the selected device(s).
- Open Web Console: Access the AIG web console for configuration or troubleshooting.

Provisioning (by Device)

After scanning the devices, please select and unlock the targeted devices, then you can choose a provisioning action to execute the provisioning task.

> Show scan explanations

1 item(s) selected UNLOCK PROVISIONING ACTION

Serial No.	Model Name	Permission Status	Software Version	IPv4
☒ TBCEB1014578	AIG-302-T-AP-AZU-LX	Granted	1.0.1+6856	10.123.2
☐ TBBHB1202447	AIG-101-T-EU	Denied	-	10.123.2
☐ TBBHB1202446	AIG-101-T-EU	Denied	-	10.123.2
☐ -	AIG-302-T-AP-AZU-LX	Denied	-	192.168

Items per page: 10

- Set Network
- Import Config.
- Export Config.
- Upgrade Software
- More Information
- Open Web Console

Configuring By Plan

1. Go to **Create Provisioning Plan** page.
2. Select the target device model and click **START** to edit the plan.

MOXA AIG QuickON

Dashboard

Create Provisioning Plan

Provisioning

About

Create Provisioning Plan

Plan Introduction

Create a plan to provision devices with the time-calibration and predefined settings listed here.

- Software upgrade
- Configuration import
- Cloud Enrollment
- Linux Command
- Security setting

Select target device model

Device Model

AIG-302

START

3. For **Software Upgrade**, you can configure either **Auto** or **Manual** mode.
 - a. **Auto**: The selected devices will be upgraded to the latest software packages.
 - b. **Manual**: Requires the upload of an upgrade pack that you want to install from a local drive.

The screenshot shows the 'Create Provisioning Plan' interface with a sidebar on the left containing steps 1 through 7. Step 1, 'Software Upgrade', is highlighted. The main content area for 'Software Upgrade' includes a toggle switch for 'Add software upgrade pack to plan' which is turned on. Below this is a section titled 'Select upgrade package source' with a dropdown menu for 'Upgrade Mode' set to 'Auto'. A green checkmark icon and the text 'Check for update' are visible, followed by a note: 'The selected devices will be upgraded to the latest software packages.' At the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

4. Enable the **Add configuration settings to plan** slider, browse to the file, and click **NEXT**.

The screenshot shows the 'Create Provisioning Plan' interface with the sidebar step 2, 'Import Configuration', highlighted. The main content area for 'Import Configuration' includes a toggle switch for 'Add configuration settings to plan' which is turned on. Below this is a section titled 'Select the configuration file to upload' with a 'Configuration File' label and a 'BROWSE...' button. At the bottom, there are '< BACK', 'CANCEL', and 'NEXT >' buttons.

5. On the Cloud Enrollment page, click **Manage** and select **Edit** to change the settings.
To add more cloud services, click **+ Add another** and configure the service.

The screenshot shows the 'Create Provisioning Plan' interface with the 'Cloud Enrollment' step selected in the sidebar. The main content area has a toggle 'Add cloud service settings to plan' which is turned on. Below it, the section 'Enroll on to the Cloud Server' shows 'Not selected cloud server' with a 'not completed' status and a 'MANAGE' button. A '+ Add another' link is visible below. The sidebar lists steps: Software Upgrade, Import Configuration, Cloud Enrollment (active), Linux Command, Security Settings, Summary, and Finish. At the bottom are 'BACK', 'CANCEL', and 'NEXT' buttons.

See the following sections for information on adding and configuring specific services:

- [Configuring the Azure IoT Device/Azure IoT Edge Service](#)
 - [Configuring the Azure DPS Service](#)
 - [Configuring the Moxa DLM Service](#)
 - [Configuring the AWS IoT Core Service](#)
6. (optional) You can upload Linux command scripts and deploy them to targeted devices.
The supported file formats include tar.gz, bash, binary executables, and Python3 packages.

The screenshot shows the 'Create Provisioning Plan' interface with the 'Linux Command' step selected in the sidebar. The main content area has a toggle 'Add linux command settings to plan' which is turned on. Below it, the section 'Select the Linux command file to upload' has a 'Linux Command File' label and a 'BROWSE...' button. Further down, there's a section 'Enter your credentials to log in the device's console' with fields for 'Account' and 'Password' (with a toggle for visibility). At the bottom, there's a field for 'Execution Timeout (sec)' with the value '600'. The sidebar lists steps: Software Upgrade, Import Configuration, Cloud Enrollment, Linux Command (active), Security Settings, Summary, and Finish. At the bottom are 'BACK', 'CANCEL', and 'NEXT' buttons.



NOTE

You must provide the terminal credential to remotely access the device via SSH and execute the commands. If the Linux script includes the reboot process, the execution result will display failed due to the timeout seconds reached, but the script is executed.

7. You can select **Disable Provisioning Service** to prevent devices from being discovered after the plan has run or change the current password for cybersecurity reasons.

The screenshot shows a multi-step wizard titled "Create Provisioning Plan". The steps are listed on the left: Software Upgrade, Import Configuration, Cloud Enrollment, Linux Command, Security Settings (highlighted with a '5'), Summary (highlighted with a '6'), and Finish (highlighted with a '7'). The main area is titled "Security Settings" with the subtitle "Configure security settings on devices". It contains two checked options: "Disable Provision Service" (with a note: "Devices will not be discovered by the provisioning tools after enabling the option") and "Change the admin account password" (with a note: "The system mandates altering the default password during initial setup."). Below these are two password input fields: "Password" and "Confirm New Password", both with eye icons for toggling visibility. At the bottom, there are navigation buttons: "< BACK", "CANCEL", and "NEXT >".

8. Click **NEXT** to apply the changes.
9. Review an overview to confirm the current configuration.
Enter a name for the provisioning plan and a password for security purposes.

← Create Provisioning Plan

1 Software Upgrade

2 Import Configuration

3 Cloud Enrollment

4 Linux Command

5 Security Settings

6 Summary

7 Finish

Summary

Plan overview

Upgrade software

Upgrade Mode : Auto

Security Settings

- Enable provisioning service on device
- Disable password change on device

Set security settings for the plan

Plan Name

Password

Confirm New Password

BACK

CANCEL

CREATE

10. Click **CREATE**.
11. Click **DOWNLOAD & FINISH** to download the plan.

The plan will be downloaded as a *.zip file.

← Create Provisioning Plan

1 Software Upgrade

2 Import Configuration

3 Cloud Enrollment

4 Linux Command

5 Security Settings

6 Summary

7 Finish

Finish

Your plan has been created

- Plan Name : Demo
- Software Upgrade Pack: ✓ Completed

← BACK

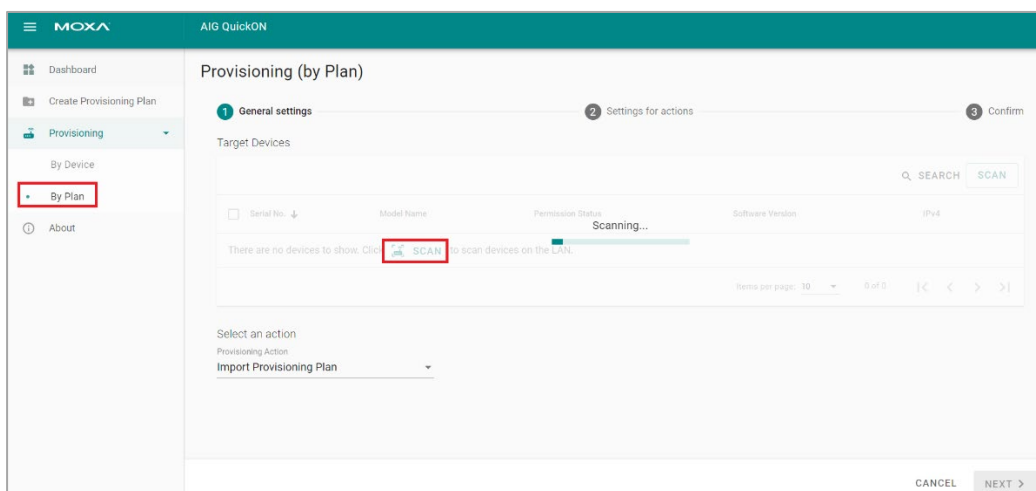
DOWNLOAD & FINISH



NOTE

Store plans in a secure location for use in the workplaces where AIG QuickON is installed.

12. Click **By Plan** and **SCAN** the devices on the LAN.

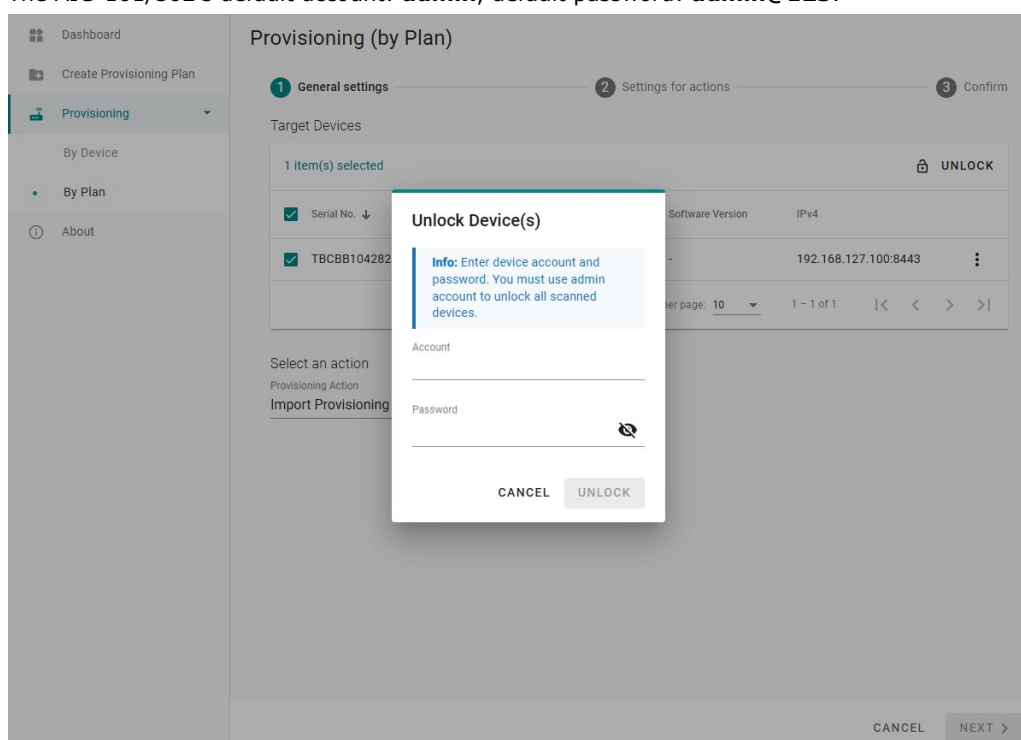


NOTE

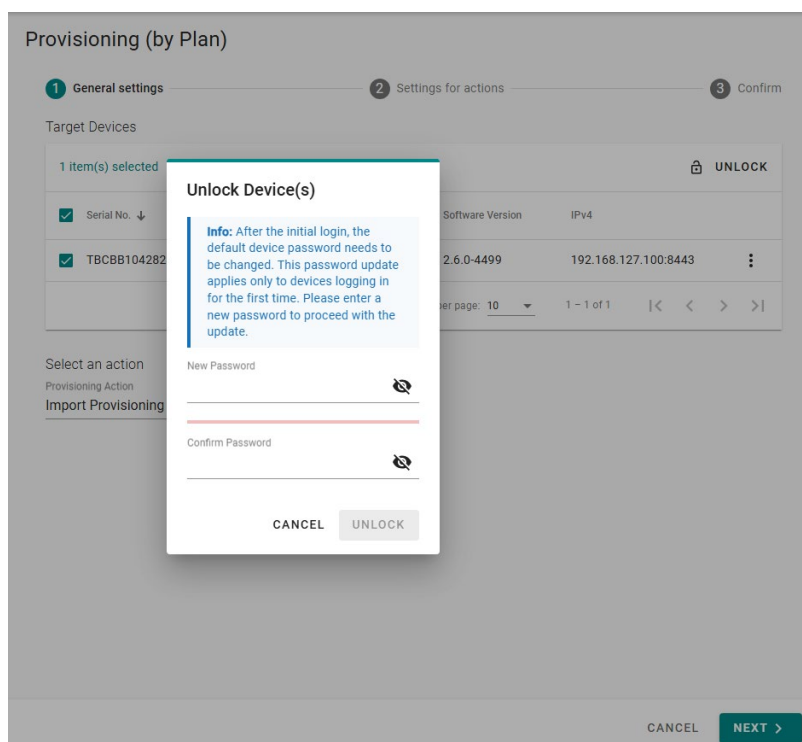
AIG QuickON relies on UDP ports 40404 and 5353 for scanning devices in the same network. Be sure to add UDP ports 40404 and 5353 to the firewall allowed list to enable proper device discovery.

13. Choose the target devices and **Unlock** them by entering the **Account** and **Password**.

The AIG devices are locked using a default account and password for higher security. For example, The AIG-101/302's default account: **admin**, default password: **admin@123**.



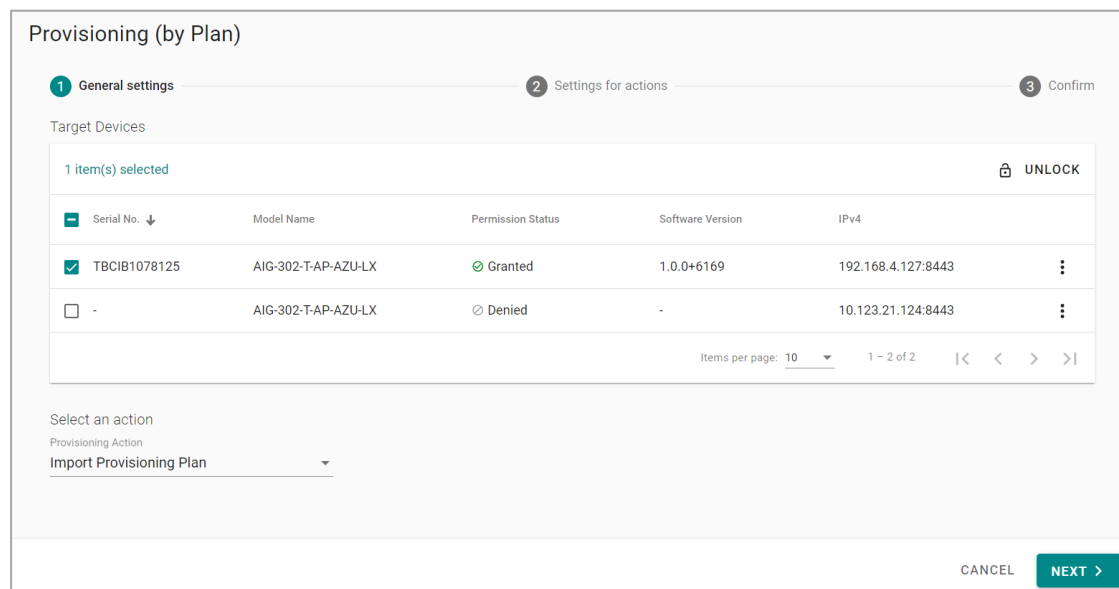
14. To comply with RED 18031-1 cybersecurity requirements, you must set a new password for the "admin" account and the SSH password for the terminal console.



NOTE

The unlock function is now designed for a device's first use. If the device has been previously used or reset to default configuration, we strongly recommend performing a full factory reset before using QuickON for provisioning. This ensures secure and efficient provisioning of a batch of devices in a consistent state..

15. Once the target device's permission status shows **Granted** (meaning device successfully unlocked), click **NEXT**.



16. **Upload** the plan and input the password set for the plan, then Click **NEXT**.

Provisioning (by Plan)

1 General settings
2 Settings for actions
3 Confirm

Select provisioning plan file

☒ **New plan file**
 Select a new provisioning plan file from local.

☐ **Recent plan files**
 Select a used plan file in the history list of plans.

Plan File

Patch_aig-302_1.0.1-20240614.tar X

Plan Password

.....

UPLOAD

Did not have the plan? [Create Provisioning Plan Now !](#)

Provisioning (by Plan)

1 General settings
2 Settings for actions
3 Confirm

Uploaded Plan

Plan File

PoC_188bd49d-5de2-4b70-a219-0263c539cb60.zip X

Plan overview

Upgrade software

Upgrade Mode : Auto

Security Settings

- Enable provisioning service on device
- Disable password change on device

< BACK
CANCEL
NEXT >

17. Click **APPLY** for the mass deployment.

Provisioning (by Plan)

1 General settings
2 Settings for actions
3 Confirm

Confirm plan and device list

PoC
AIG-302 series only - 2 Subtask(s)

DETAIL

Eligible Device (1) Ineligible Device (0)

✔ Device list can be provisioned Q SEARCH

Model Name	Serial No.	Software Version	Message
AIG-302-T-AP-AZU-LX	TBCEB1014578	1.0.1	-

Items per page: 10 1 - 1 of 1 |< < > >|

< BACK
CANCEL
APPLY

Checking for Updates

You can configure AIG QuickON to update automatically.

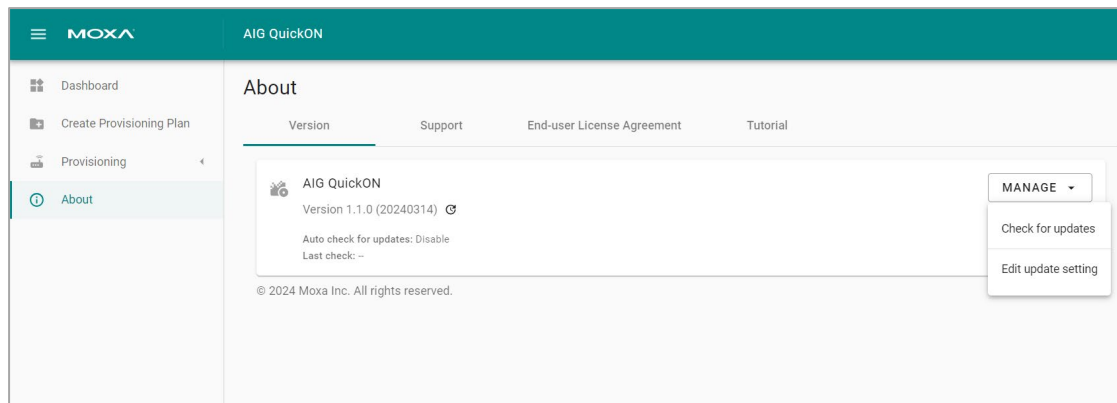


NOTE

Automatic check for updates is disabled by default. You can enable the service by selecting the **Edit update setting** option under **MANAGE**.

To configure auto-updates, do the following:

1. Go to the About page.
2. Click **MANAGE** and select **Check for updates**.



If an updated version is available, the information will be presented.

3. Click **INSTALL** to install the latest version. Please ensure no existing provisioning procedure is running before clicking **INSTALL**.



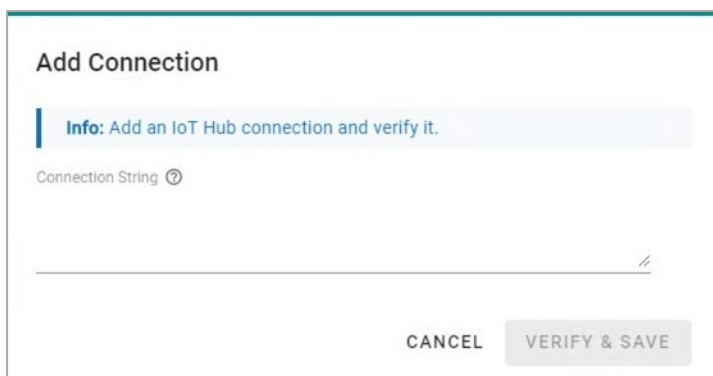
NOTE

The web GUI must be reloaded after the upgrade to ensure the web cache has been cleared.

A. Configuring Services on the AIG

Configuring the Azure IoT Device/Azure IoT Edge Service

1. Select the service type **Azure IoT Device Service** or **Azure IoT Edge Service** under **Cloud Enrollment** of the **Create Provisioning Plan** page.
2. Enter the **Connection String** and click **VERIFY & SAVE**.



3. You can edit the **Connection String** by clicking on **EDIT**.

The Device ID is auto-generated by using the serial number of the device and authenticated via a symmetric key.

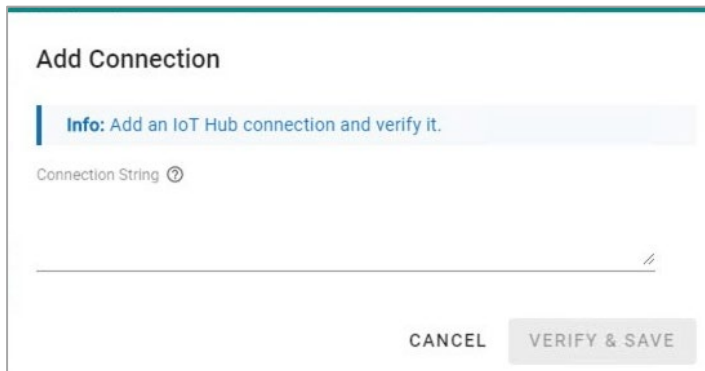


NOTE

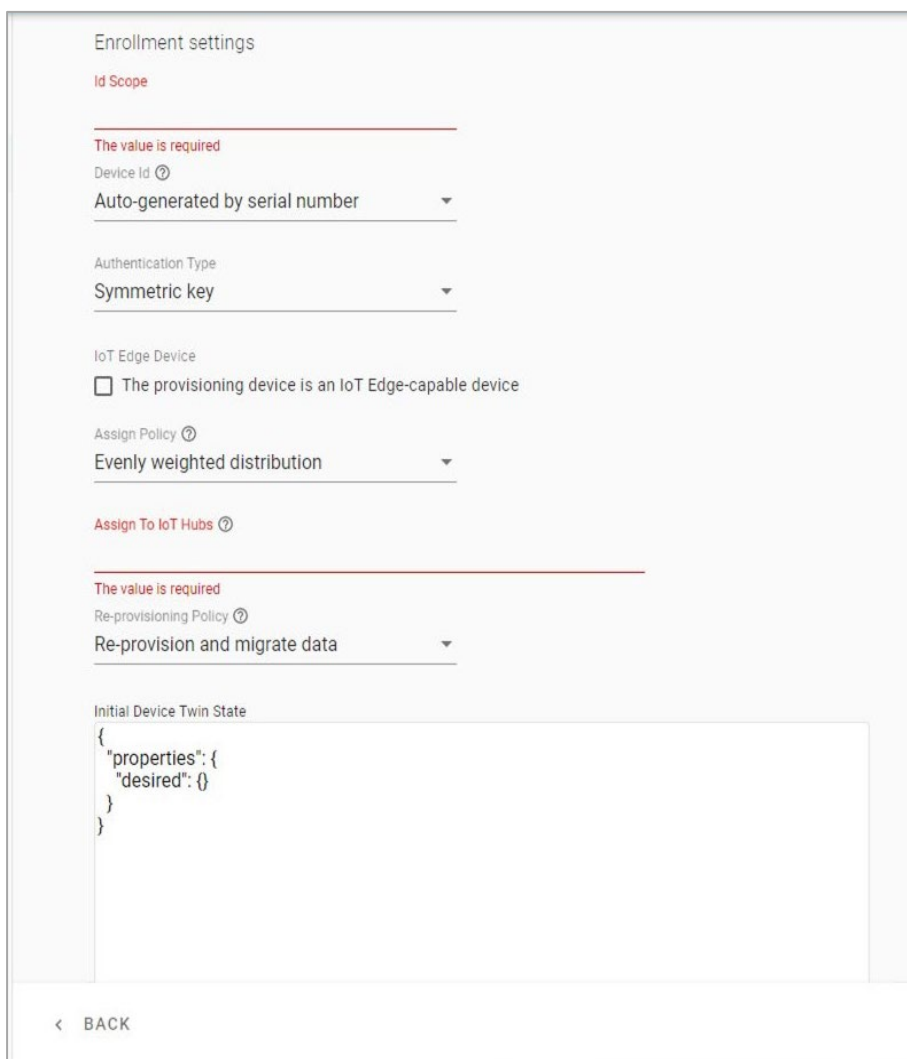
Azure IoT Device Service is only available for AIG-301, AIG-302, AIG-501, and AIG-502 Series.

Configuring the Azure DPS Service

1. Select the service type **Azure DPS Service** under **Cloud Enrollment** of the **Create Provisioning Plan** page.
2. Enter the **Connection String** and click **VERIFY & SAVE**.



3. If you want to edit the Connection String, click **EDIT** and enter the **ID Scope**.
The Device ID is auto generated using the serial number of the device and authenticated via a symmetric key.
4. (optional) Select **The provisioning device is an IoT Edge-capable device**.
5. Select an **Assign Policy**.



6. Enter the name of the **IoT Hubs**.
7. Select a Re-provisioning policy.
8. (optional) Customize the Initial Device Twin State.
9. Click **NEXT**.



NOTE

Azure DPS Service is only available for AIG-301, AIG-302, AIG-501, and AIG-502 Series.

Configuring the Moxa DLM Service

1. Select the service type **Moxa DLM Service** under **Cloud Enrollment** of the **Create Provisioning Plan** page.
2. Enter an **Email** (account) and **Password**.

Add Connection

INFO:: Add a Moxa DLM connection and verify it

Email
aaa@moxa.com

Password



CANCEL

VERIFY & SAVE

3. Select a project name to register devices.

← Edit Cloud Enrollment Setting

Select Server Type

Server Type
Moxa DLM Service

Configure an Moxa DLM Connection

Moxa DLM Connection

Verified

Email : joshua.lin@moxa.com

Password:

EDIT

Enrollment Settings

Project Name *
Site C

Authentication Type
X.509

Connection
☒ Enable Auto Connect

Reconnection Interval (sec) *
10

< BACK CANCEL DONE

- Click **DONE**.

Configuring the AWS IoT Core Service

- Select the service type **AWS IoT Core Service** under **Cloud Enrollment** of the **Create Provisioning Plan** page.
- Enter the **Access Key ID** and **Secret Access Key** and click **VERIFY & SAVE**.

Add Connection

Info: Add an AWS IoT Core connection and verify it.

Access Key ID ?

Secret Access Key ?

CANCEL VERIFY & SAVE

- If you want to edit the **Access Key ID** and **Secret Access Key**, click **EDIT**.
- The Thing Name is auto generated by using the serial number of the device.

← Edit cloud Enrollment Setting

Select server type

Server Type

AWS IoT Core

Configure an AWS IoT Core connection

↔

AWS IoT Core connection

Verified

Access Key ID: AKIATM2PBA27J7E2GFXM

Secret Access Key: *****

EDIT

Enrollment settings

Region *

Asia Pacific (Hong Kong)

Thing Name ⓘ

Auto-generated by serial number

The thing will use "ThingsProEdge-default" as the default policy. Moreover, ThingsPro Proxy will create the policy automatically if it's not existed. The default policy will allow all the resources. We recommend the users should modify the policy with some restrictions later via the AWS portal.



NOTE

AWS IoT Core Service is only available for AIG-101, AIG-301, and AIG-501 Series.