



ActiveCloud Board Configuration Manual

Revision 2.0.3

Published 29/09/2026

Application Version 1.4.8

Contents

- Introduction..... 3
- Board Discovery..... 3
- Application Controls and Functions..... 4
 - Configure Ethernet Settings..... 4
 - Configure WiFi Settings 5
 - WiFi Signal Strength..... 7
 - Reset Network Settings 8
 - Reboot 8
 - Reset Cloud Registration 9
 - Firmware Update..... 9
- Machine-to-Machine 11
 - Available Firmware Options 11
 - Standard ActiveCloud 11
 - Enhanced ActiveCloud M2M 13
 - ActiveLAN / HTTP M2M 15
- Density Box..... 17

Introduction

ActiveCloud Board Configuration is a Windows application designed to configure the network settings of the **ActiveCloud** LAN board.

To use ActiveCloud Board Configuration, the PC running the application and the ActiveCloud board, must be connected to the same LAN. Alternatively, the PC can be connected via WiFi to the WiFi network provided by the ActiveCloud board.

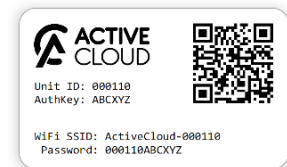
The primary network interface of the ActiveCloud board is Ethernet. By default, the board is factory-configured to obtain an IP address automatically using DHCP. If no Ethernet cable is connected and the board's WiFi network has not yet been configured, the board starts in **Access Point** mode.

In this case, connect the PC to the WiFi network provided by the ActiveCloud board using the following credentials:

- **SSID:** ActiveCloud-#####, where ##### is the board serial number (e.g., ActiveCloud-000101).
- **Password:** the board serial number followed by the authorization key (e.g., 000101ABCXYZ).

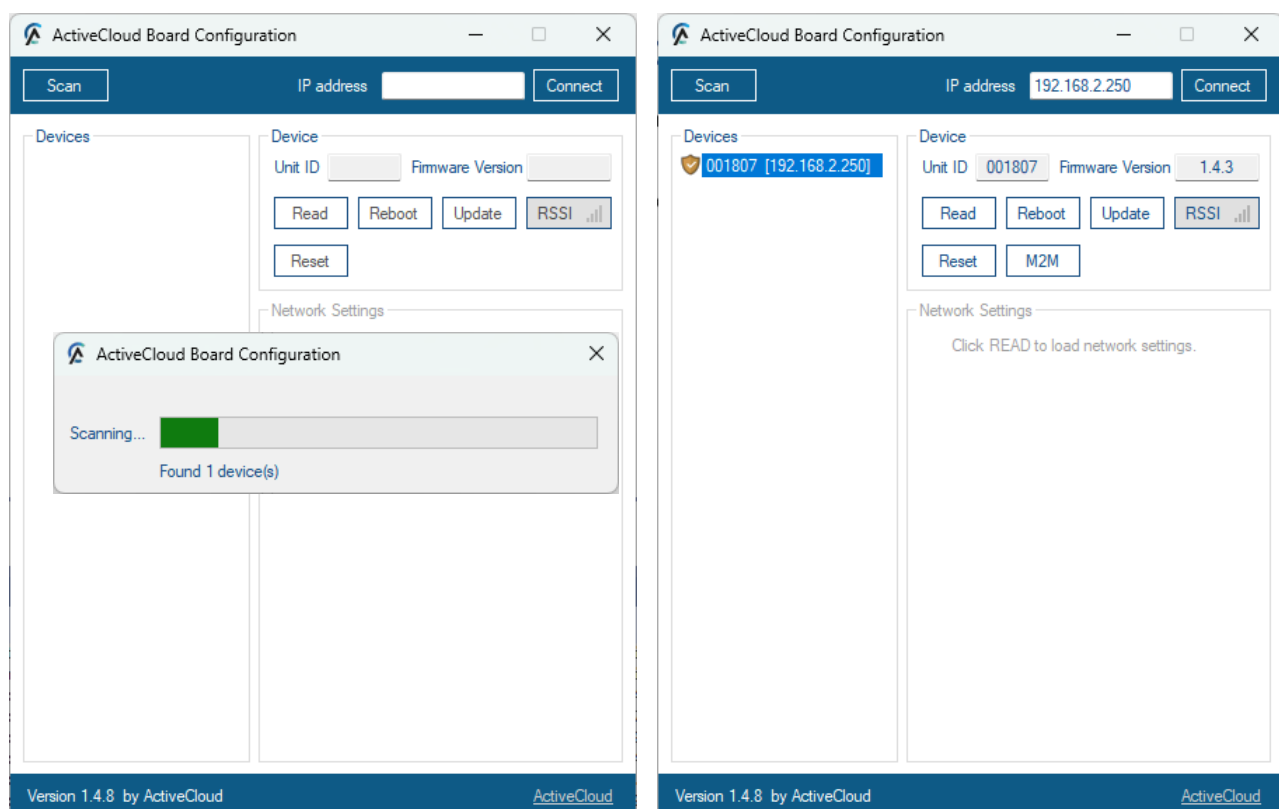
This information is printed on the label attached to the LAN board as **Unit ID** and **AuthKey**.

Once the board and the PC are connected to the same network, LAN or WiFi, run the ActiveCloud Board Configuration application to configure the board.



Board Discovery

When the application starts, it automatically searches the local network for all available ActiveCloud boards. The detected boards are listed in the left panel, identified by their Unit ID and IP address. The right panel displays in the text boxes **Unit ID** and **Firmware Version** of the selected board.



Click **Scan** to perform a new search and refresh the list of detected ActiveCloud boards. While the application is scanning, click the close icon in the scanning window or press ESC to stop the search.

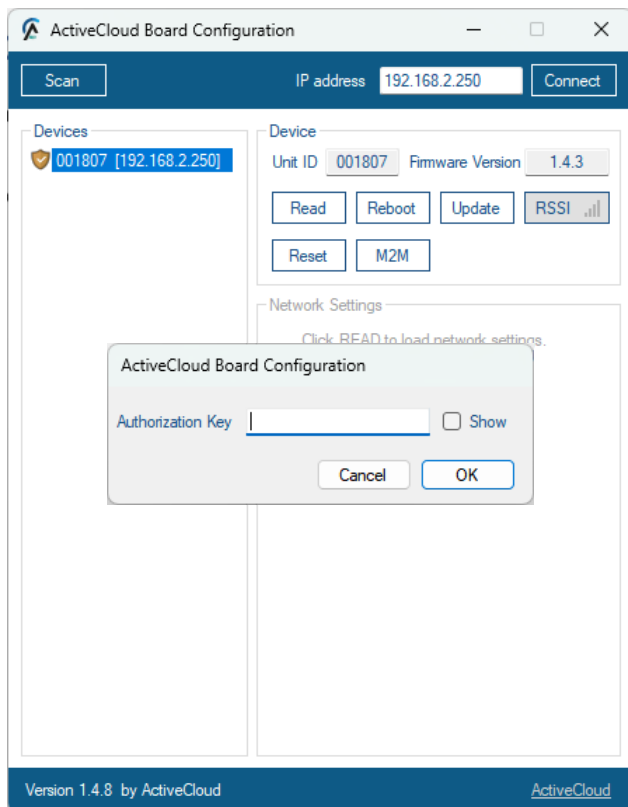
If you already know the IP address of the board, you can enter it in the **IP address** text box in the top-right corner and click **Connect**.

Application Controls and Functions

The following buttons provide access to the corresponding functions on the selected board:

- **Read:** retrieves the network settings of the board (Ethernet and WiFi).
- **Reboot:** requests a firmware reboot.
- **Update:** performs a firmware update.
- **Reset:** clears operative cloud credentials (reset registration).
- **RSSI:** displays the received signal strength indicator (RSSI) of the board's WiFi connection.

To execute any of these functions, enter the board's authorization key (*Auth Key* as printed on the LAN board label) when prompted and click **OK**. The authorization key is required only the first time.

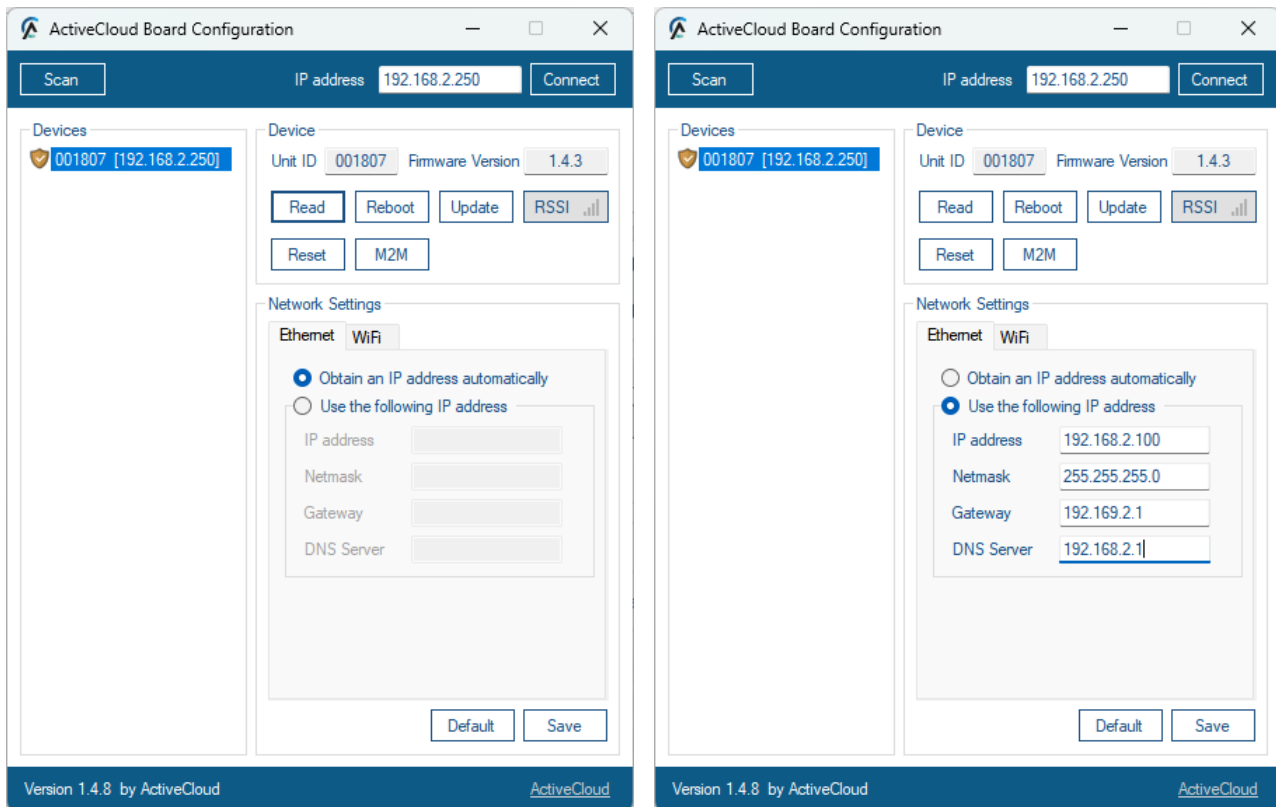


Configure Ethernet Settings

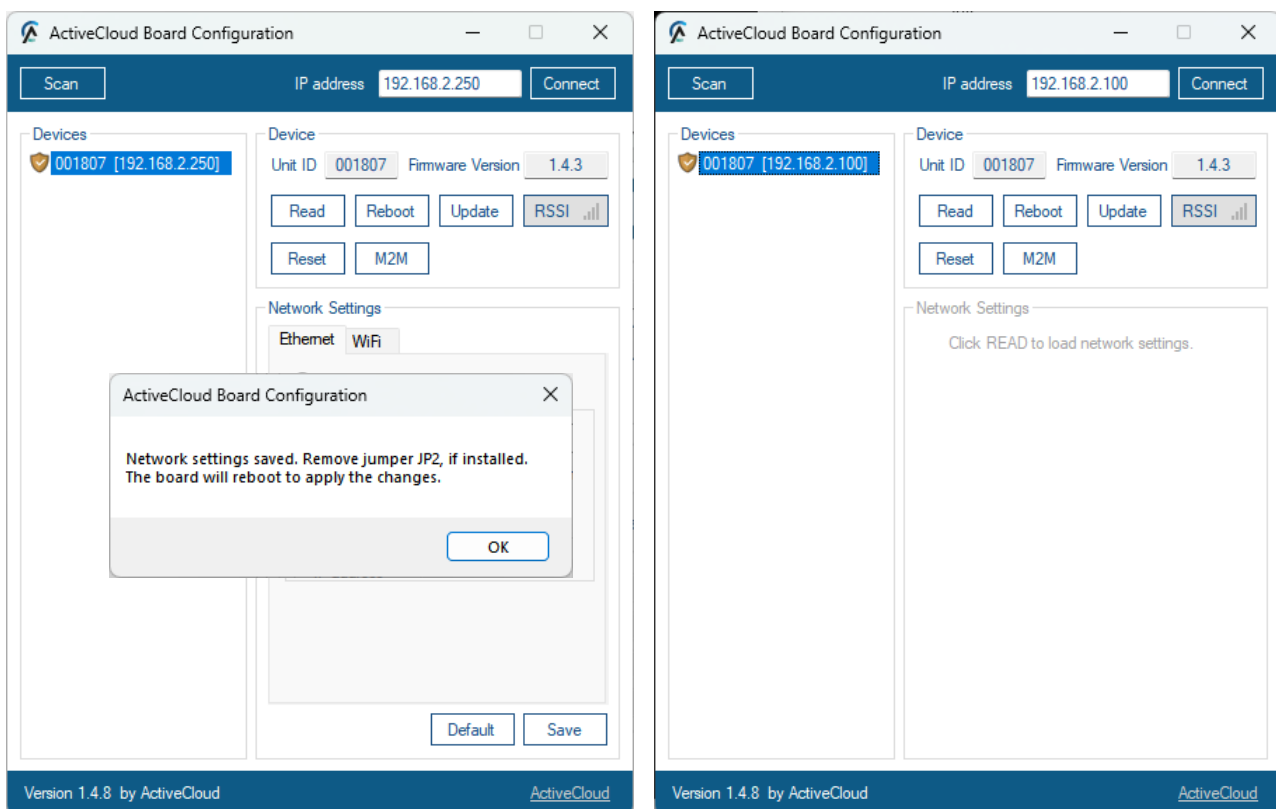
Click **Read** to retrieve the current network settings from the board. Enter the authorization key if required.

Select **Obtain an IP address automatically** (default) to allow the board to obtain an IP address automatically from the router using DHCP.

Select **Use the following IP address** to configure a static IP address for the board. Enter the network **IP address**, **Netmask**, **Gateway**, and **DNS server** in the corresponding text boxes. Then click **Save** to apply the new settings.

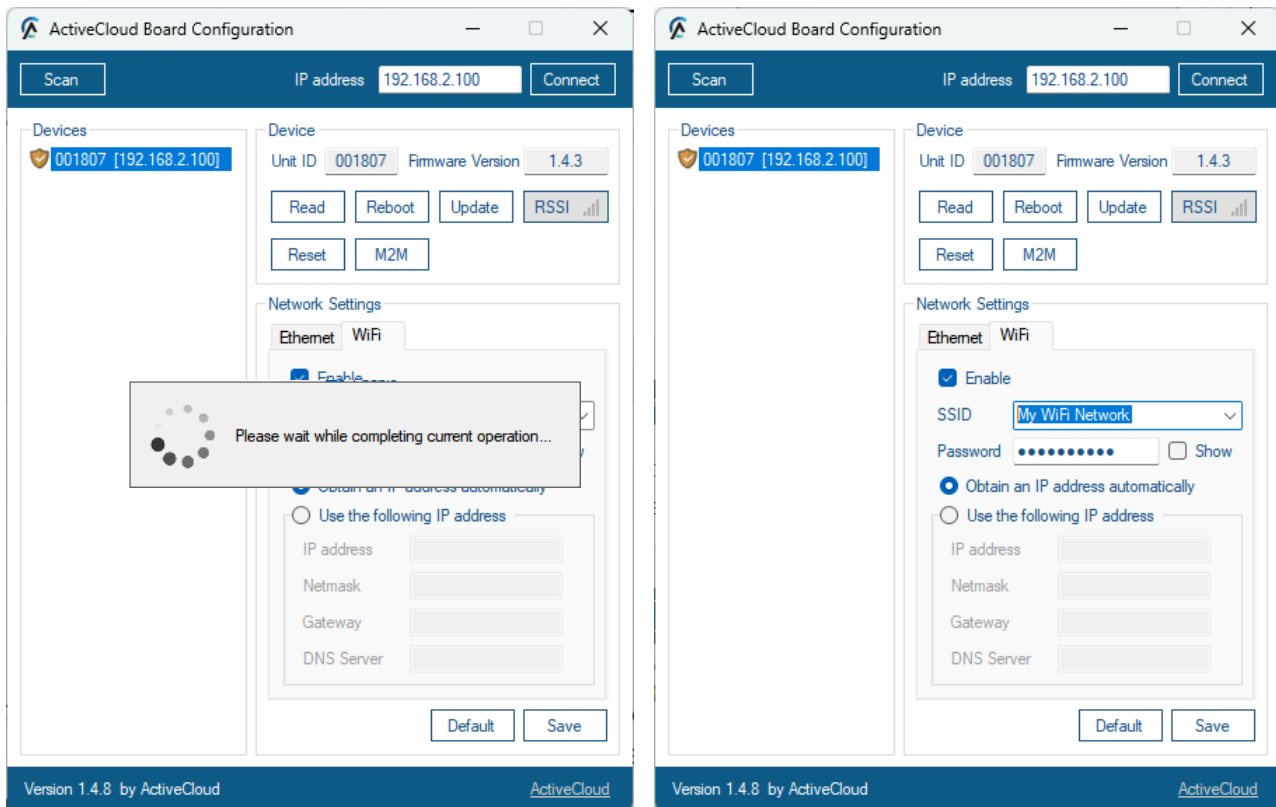


In the confirmation pop-up, click **OK** to confirm: the board will reboot automatically and the application will automatically perform a new scan and reconnect to the board using its new network settings.



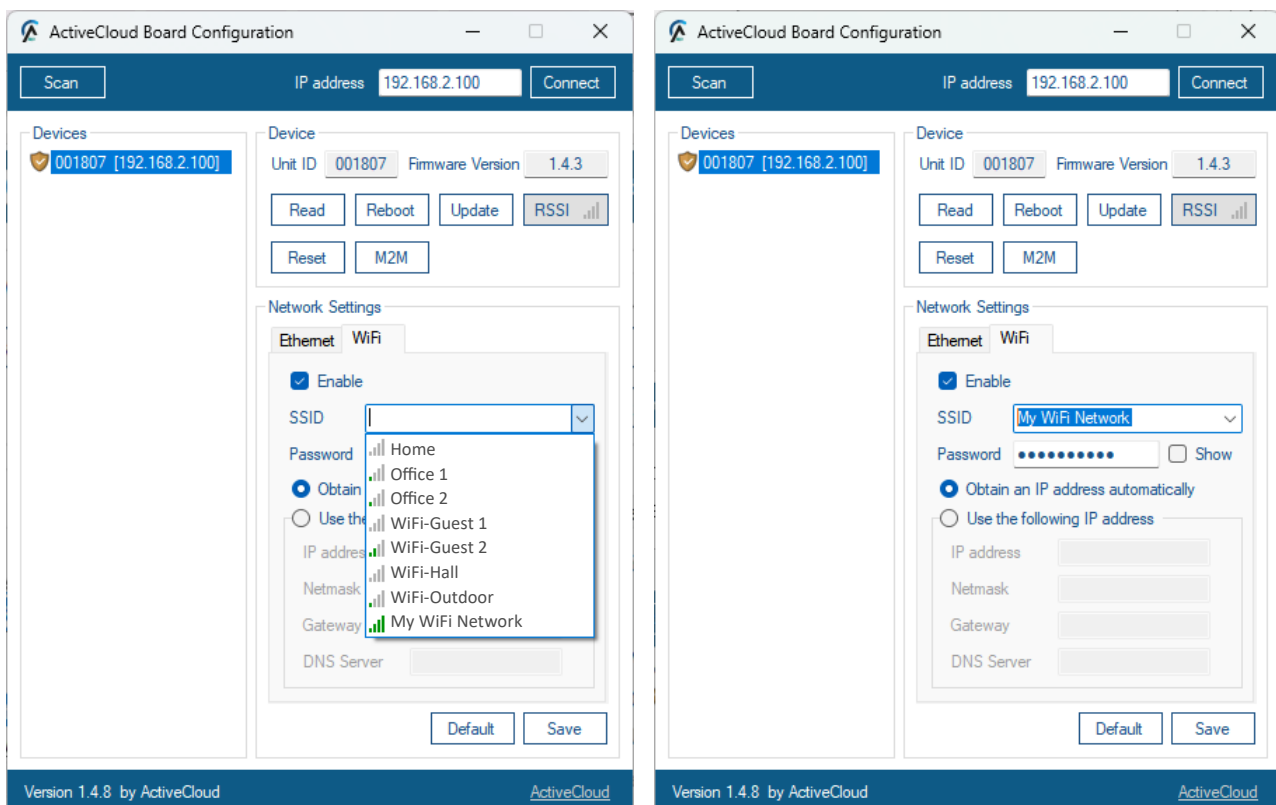
Configure WiFi Settings

After retrieving current network settings, select the **WiFi** tab to view and configure the board's WiFi settings. The board automatically scans for Wi-Fi networks and retrieves the current Wi-Fi settings.



Enter the **SSID** of the WiFi network you want the board to connect to, or select it from the dropdown box, and enter the **Password** of the specified network to configure the new WiFi settings.

Select **Obtain an IP address automatically** to allow the board to obtain an IP address from the router using DHCP. Alternatively select **Use the following IP address** to configure a static IP address. Enter the network **IP address**, **Netmask**, **Gateway**, and **DNS server** in the corresponding text boxes.

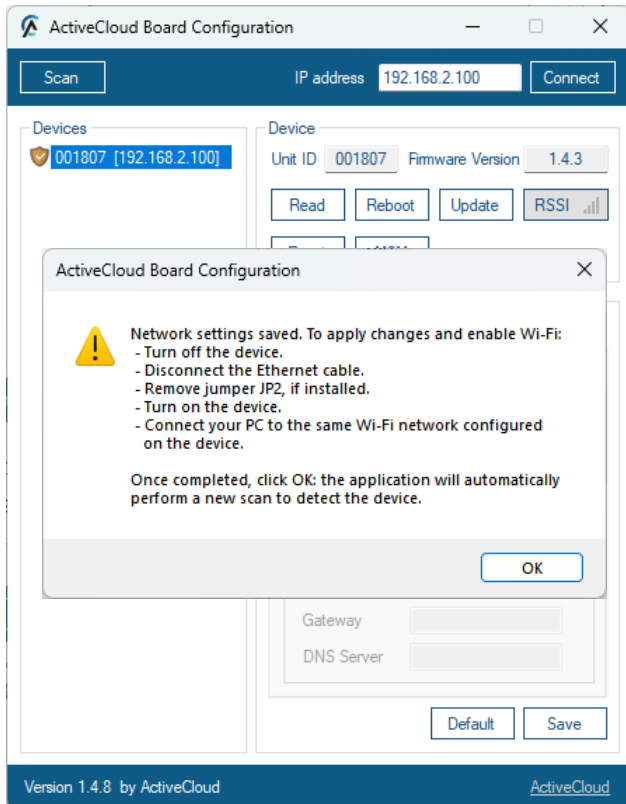


Please note: to completely disable the board's WiFi interface, deselect the **Enable** checkbox.

Click **Save** to apply the settings, then follow instructions in the popup window:

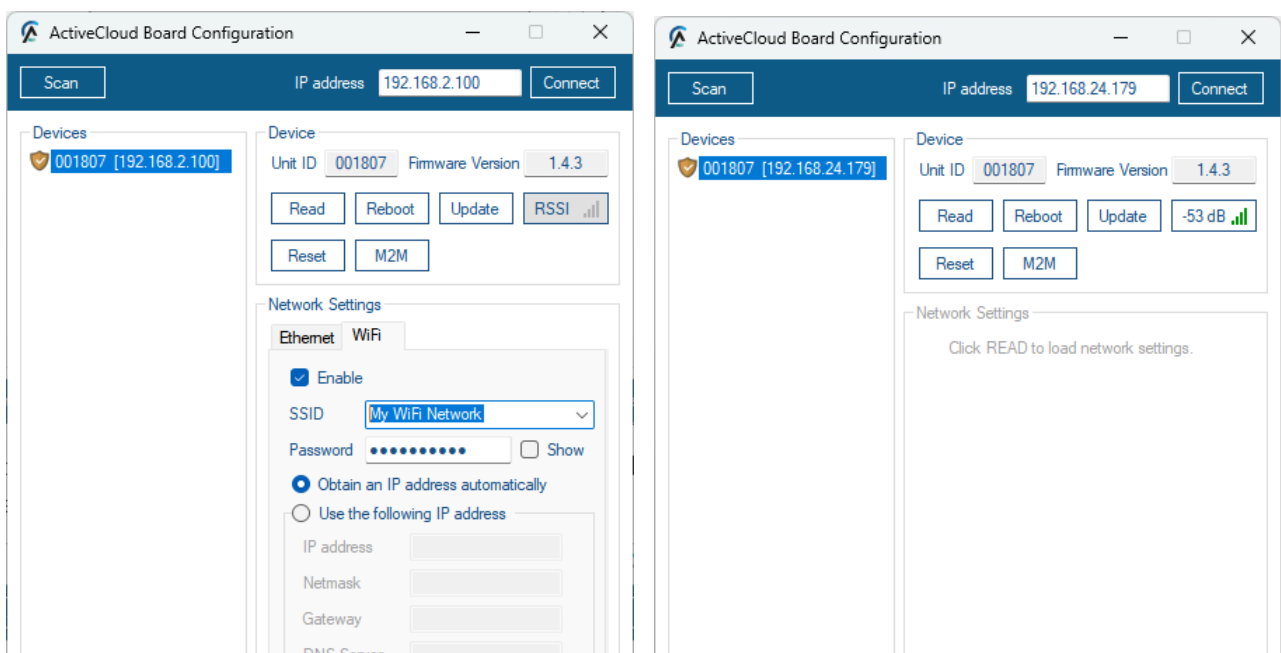
- turn off the device.
- Disconnect the Ethernet cable as an active Ethernet connection prevents WiFi from starting;
- Turn on the device;

Make sure that both the PC and the board are connected to the same WiFi network, then click **OK**. The application will automatically perform a new scan and reconnect to the board using the new WiFi settings



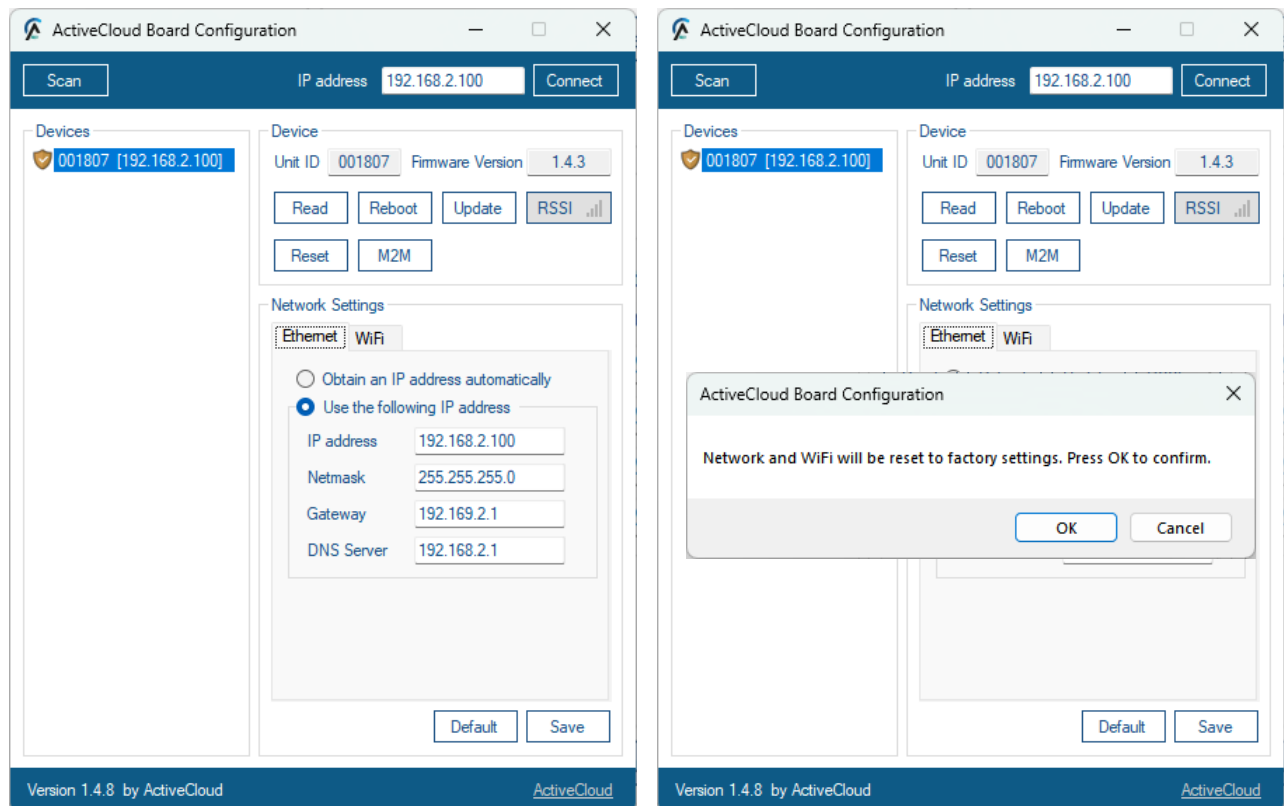
WiFi Signal Strength

Click **RSSI** to display the signal strength of the board's WiFi connection. The RSSI value is displayed on the **RSSI** button and updated in real time. Click the button again to stop the update.



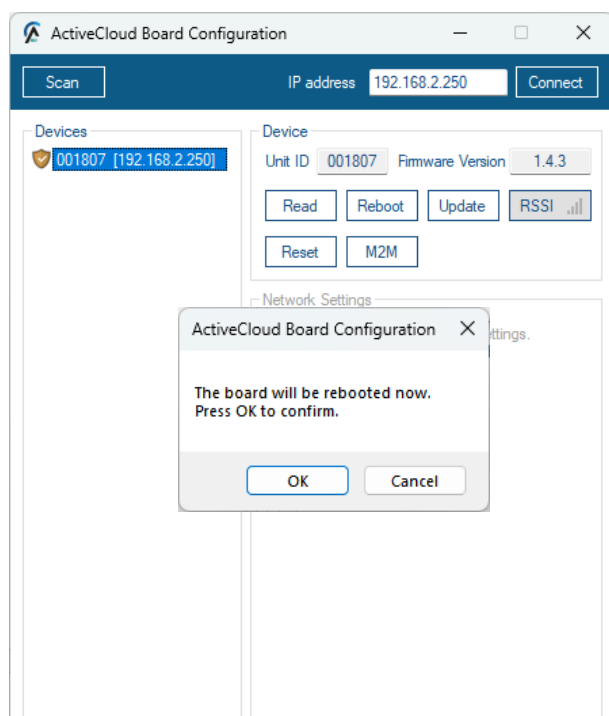
Reset Network Settings

Click **Default** in the network settings panel to reset Ethernet and WiFi settings to default values: obtain an IP address automatically for Ethernet, and WiFi not configured but enabled. Click **OK** in the pop-up window: the application will automatically perform a new scan and reconnect to the board using its default settings.



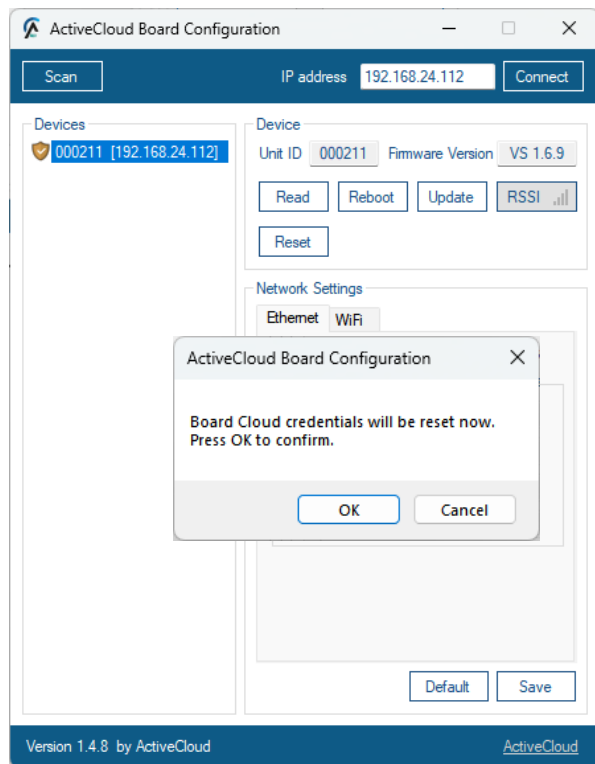
Reboot

Click **Reboot** and press **OK** in the pop-up window to confirm the board reboot. Wait for the application to automatically scan for available devices and establish a new connection with the board.



Reset Cloud Registration

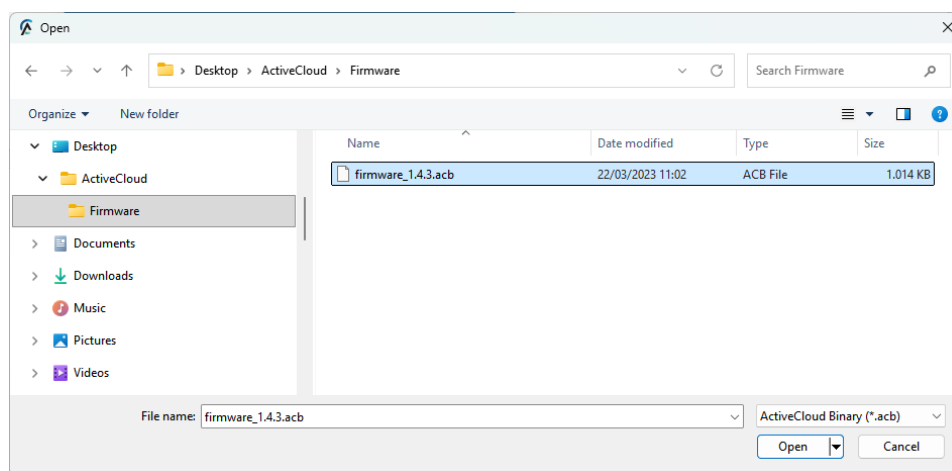
Click **Reset** and press **OK** in the pop-up window to confirm the reset of the Cloud registration. This function is available only for firmware version **1.2.3 or later**. If the board is registered to the Cloud, this command removes its Cloud credentials and after rebooting, the board is ready to be registered again.



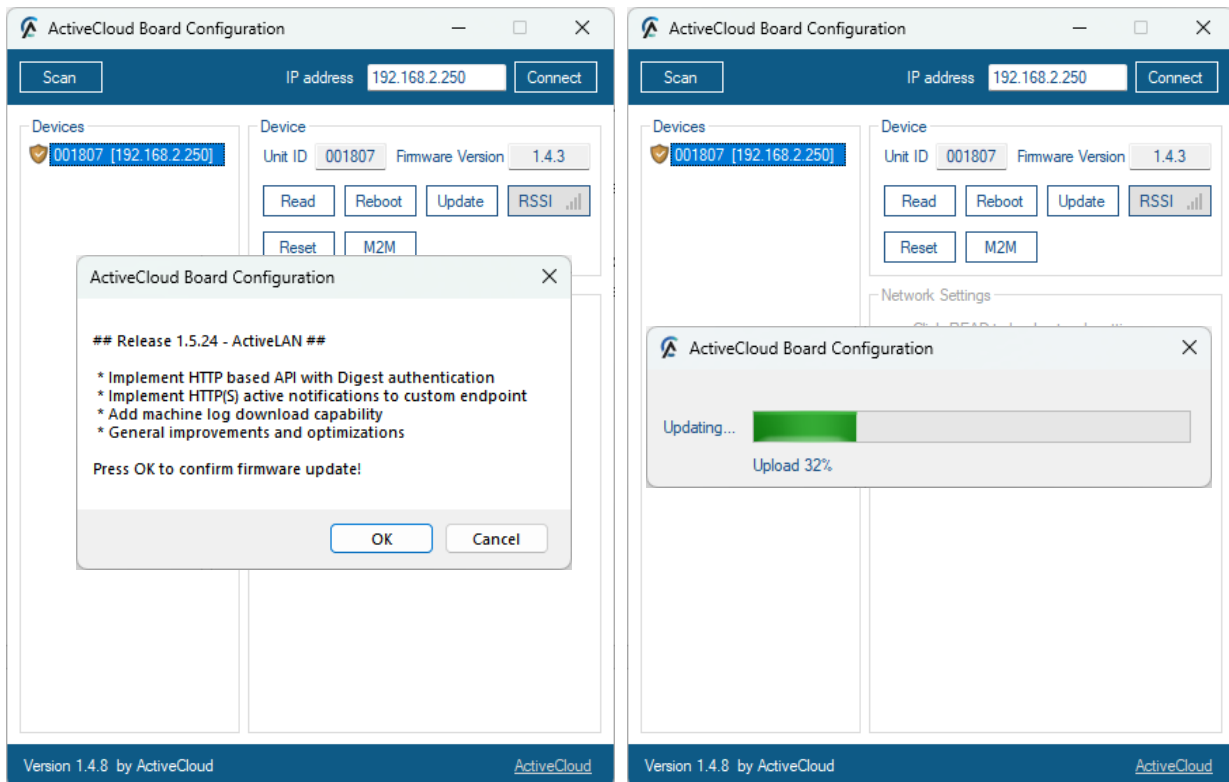
Please note: this command only affects the board and does **not** unregister it from the Cloud. Before registering the board again, you must first remove it from the Cloud.

Firmware Update

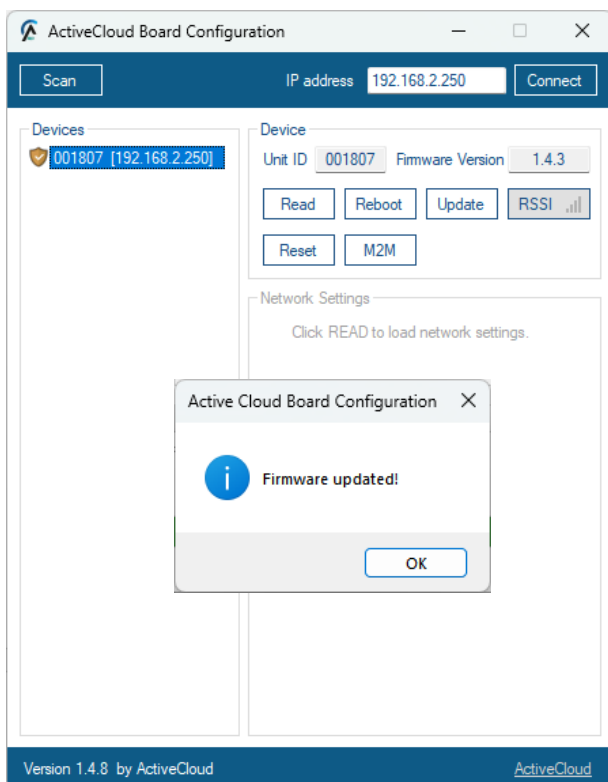
Click **Update** to update the firmware of the ActiveCloud board. In the dialog box, browse to the firmware file on your PC (using the **“.acb”** format for official release or optionally in **“.bin”** format for unofficial/hotfix release), select it and click **Open**.



A pop-up window displays the official release notes (only for **“.acb”** format) for the new firmware version. Click **OK** to confirm the firmware update and wait for the firmware to be uploaded. A progress bar shows the upload progress as a percentage.



At the end, click **OK** in the result pop-up window to complete the update process.



Please note: sometimes, the update process may end with an error message indicating that the transfer was not completed successfully, even though the progress bar has reached 100%.

Perform a new device scan and check whether the firmware version has been updated. If the displayed version is still the same as before the update, repeat the update procedure. Using a wired network connection or a fast and stable wireless connection may improve the success rate of the update procedure.

Machine-to-Machine

Available Firmware Options

By default, the ActiveCloud board is factory-configured to connect the fogging machine to the **ActiveCloud** platform, which provides the Cloud services required to manage the machine remotely, including registration, status monitoring, and command execution.

However, the ActiveCloud board can also be used with other management systems. Depending on the firmware installed on the board, the machine can communicate with an external system using different communication methods and protocols. These **Machine-to-Machine (M2M)** firmware variants are intended to allow the fogging machine to be integrated into third-party or customer-specific systems without necessarily relying on the ActiveCloud management platform.

In addition to the standard firmware, the ActiveCloud board supports three main firmware variants, introduced from version 1.5, each providing a different way of managing and communicating:

- **Standard ActiveCloud:** connects the machine to the **ActiveCloud** server and allows it to be managed through the ActiveCloud platform. The firmware uses **MQTT** over **TLS** for communication. It can also be configured to communicate with another server implementing the same MQTT protocol and registration and operative mechanisms.
- **Enhanced ActiveCloud M2M:** is intended for integration with an external management system using the MQTT protocol. It provides enhanced configuration options than the standard firmware.
- **ActiveLAN / HTTP M2M:** is intended for integration with an external management system using the HTTP protocol and can optionally provide push notifications.
- **ActiveServer:** provides a web-based interface that allows the machine to be managed directly from a browser by a PC or smart device on the same LAN. It is also compatible with the **ActiveServer Manager** application for Windows.

Firmware variants are identified by their prefix to the firmware version:

- Standard ActiveCloud firmware has no prefix (e.g., **1.4.3**).
- Machine-to-Machine MQTT firmware uses the **MM** prefix (e.g., **MM-1.5.27**).
- Machine-to-Machine HTTP firmware uses the **HT** prefix (e.g., **HT-1.5.24**).
- ActiveServer firmware uses the **WI** prefix (e.g., **WI-1.5.19**).

The following sections describe the characteristics and configuration options of each firmware variant in more detail, except for the WI - ActiveServer firmware, that supports the HTTP protocol and does not have additional configuration settings for the Machine-to-Machine.

Standard ActiveCloud

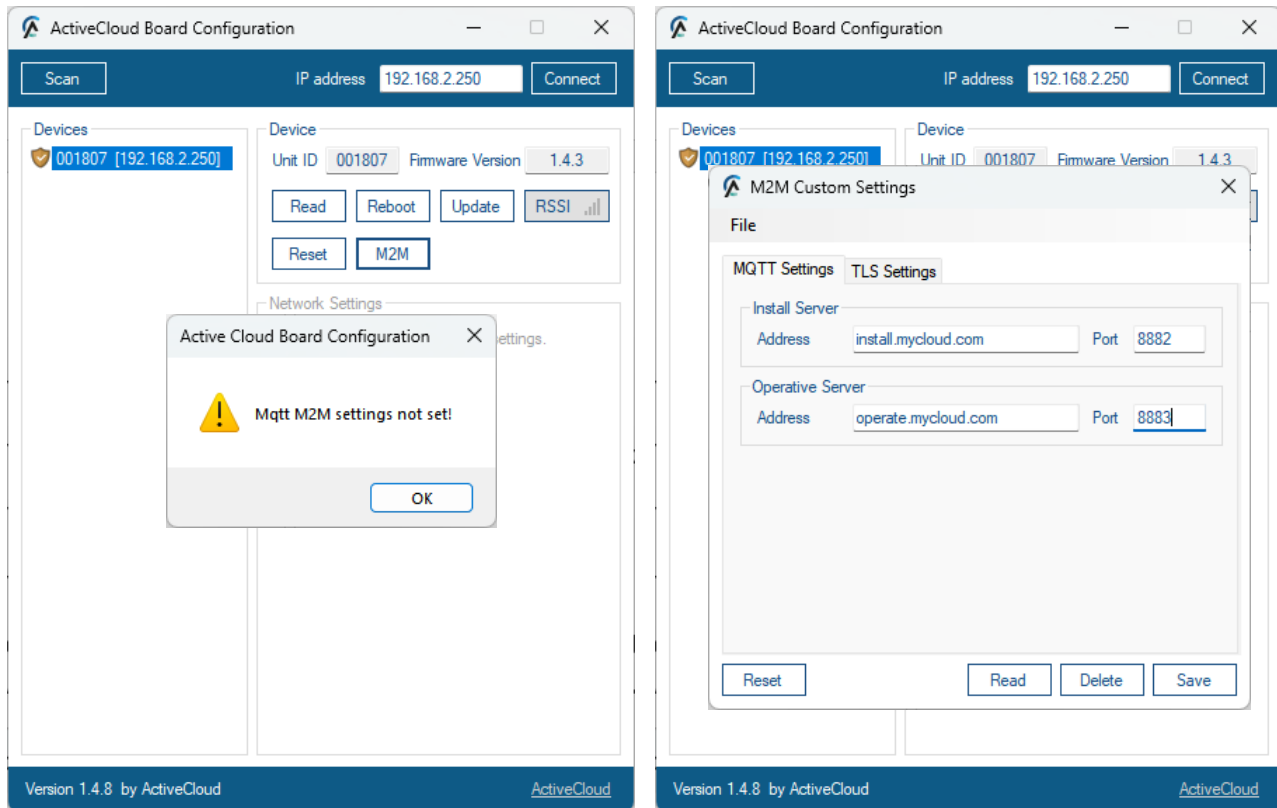
The communication protocol used by the standard firmware is based on **MQTT** with **TLS** security. On supported firmware versions, the standard firmware can be reconfigured to use a different MQTT server, provided that the server implements the same protocol and registration mechanism as the ActiveCloud server. Refer to the **ActiveCloud MQTT Protocol** document for detailed information on the MQTT protocol, as well as the installation and operating procedures.

The standard ActiveCloud firmware provides the following MQTT configuration options:

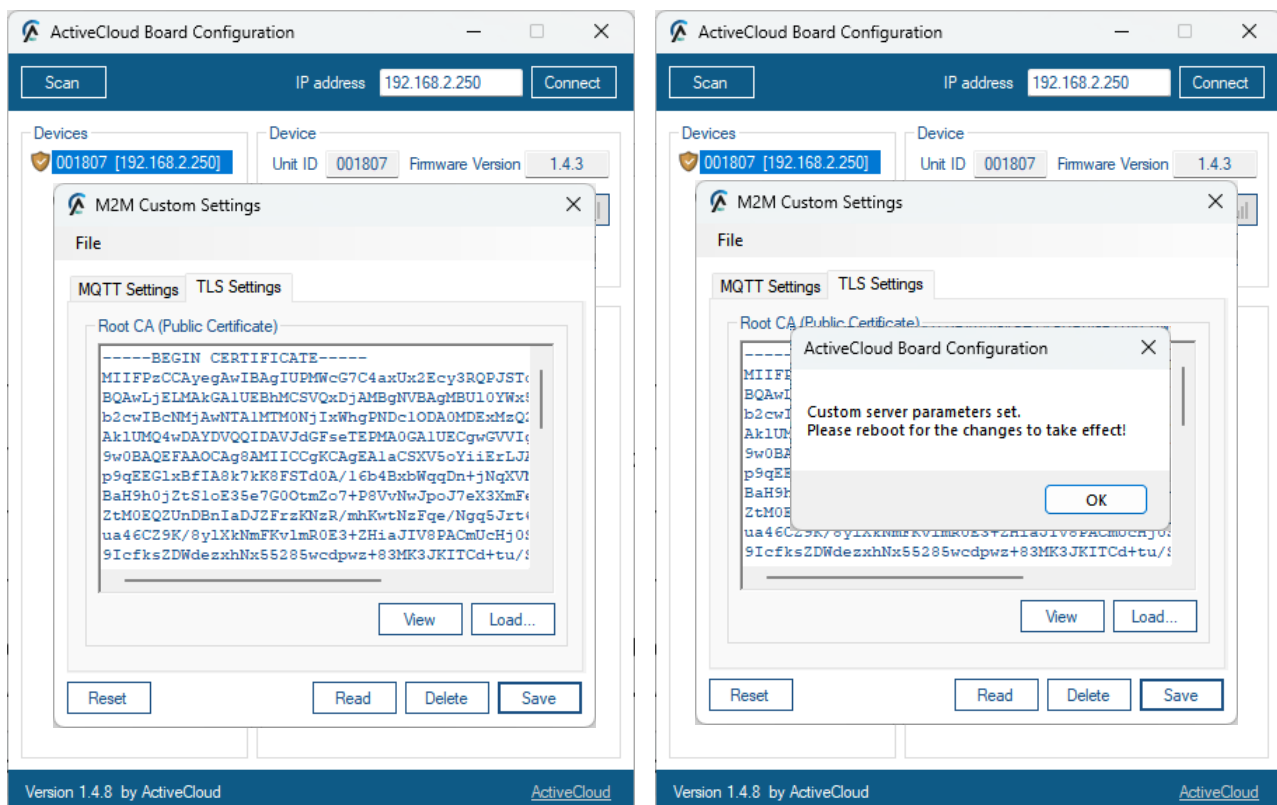
- MQTT install server address and port.
- MQTT operative server address and port.
- Root CA certificate used to validate the secure connection.

Click **M2M** to open the **M2M Custom Settings** window. If the board has not yet been configured, click **OK** in the pop-up window indicating that the settings are not configured.

Enter the **Install Server address and port** and **Operative Server address and ports** of your servers.

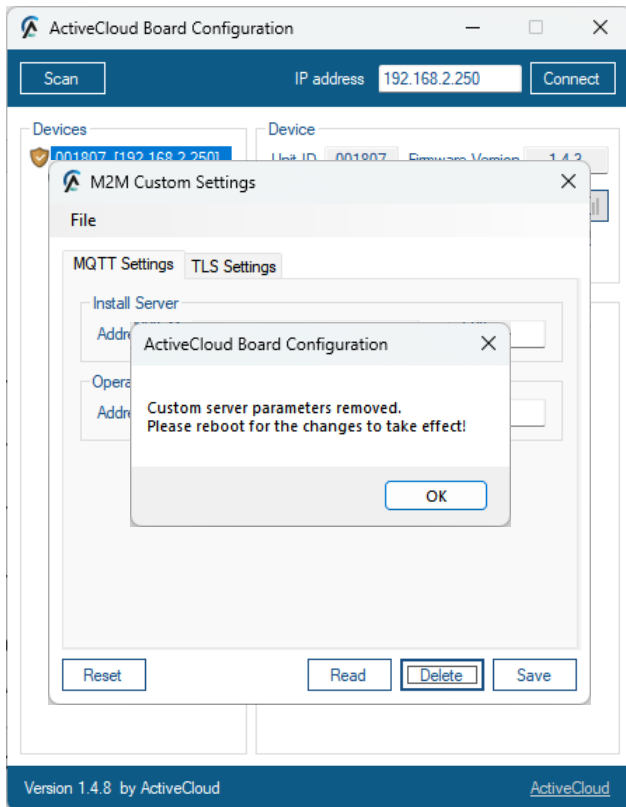


Open the **TLS Settings** tab and click **Load** to upload the server certificate from your PC. Click **Save** to save the new settings. In the confirmation pop-up, click **OK** then reboot the board for the changes to take effect.



In the **M2M Custom Settings** window:

- Click **Read** to retrieve or refresh the M2M settings from the board.
- Click **Reset** to clear the settings displayed in the text boxes. This does not delete the M2M settings from the board; it only clears the values currently displayed in the window.
- Click **Delete** to delete the current M2M settings from the board. Click **OK** in the confirmation pop-up, then reboot the board for the changes to take effect.



Enhanced ActiveCloud M2M

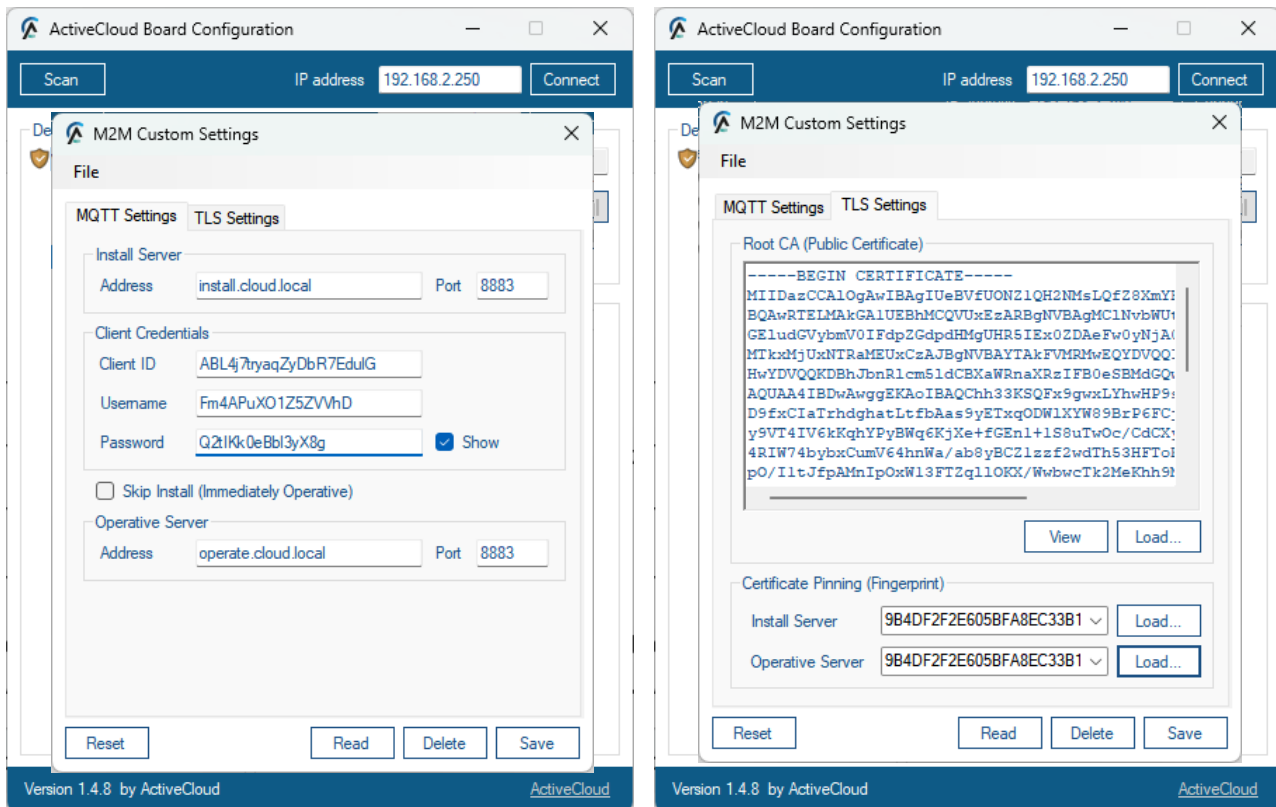
The Machine-to-Machine MQTT firmware provides enhanced configuration options compared with the standard firmware. In particular, it allows you to specify not only the server addresses and ports, but also the MQTT installation credentials (**Client ID**, **Username**, and **Password**), whereas the previous version could only use the factory-programmed credentials provided by the manufacturer.

The new settings also allow the board to skip the registration phase and connect directly to the operational server using the specified MQTT credentials. Another new feature is the option for server certificate pinning: using its unique fingerprint only a server with a matching certificate is allowed to connect, useful when the Root CA can issue other certificates to other entities or for purposes other than the configured MQTT server.

Make sure that prefix of firmware version is **MM** and click **M2M** to open the **M2M Custom Settings** window. If no M2M custom settings are configured, click **OK** in the warning pop-up.

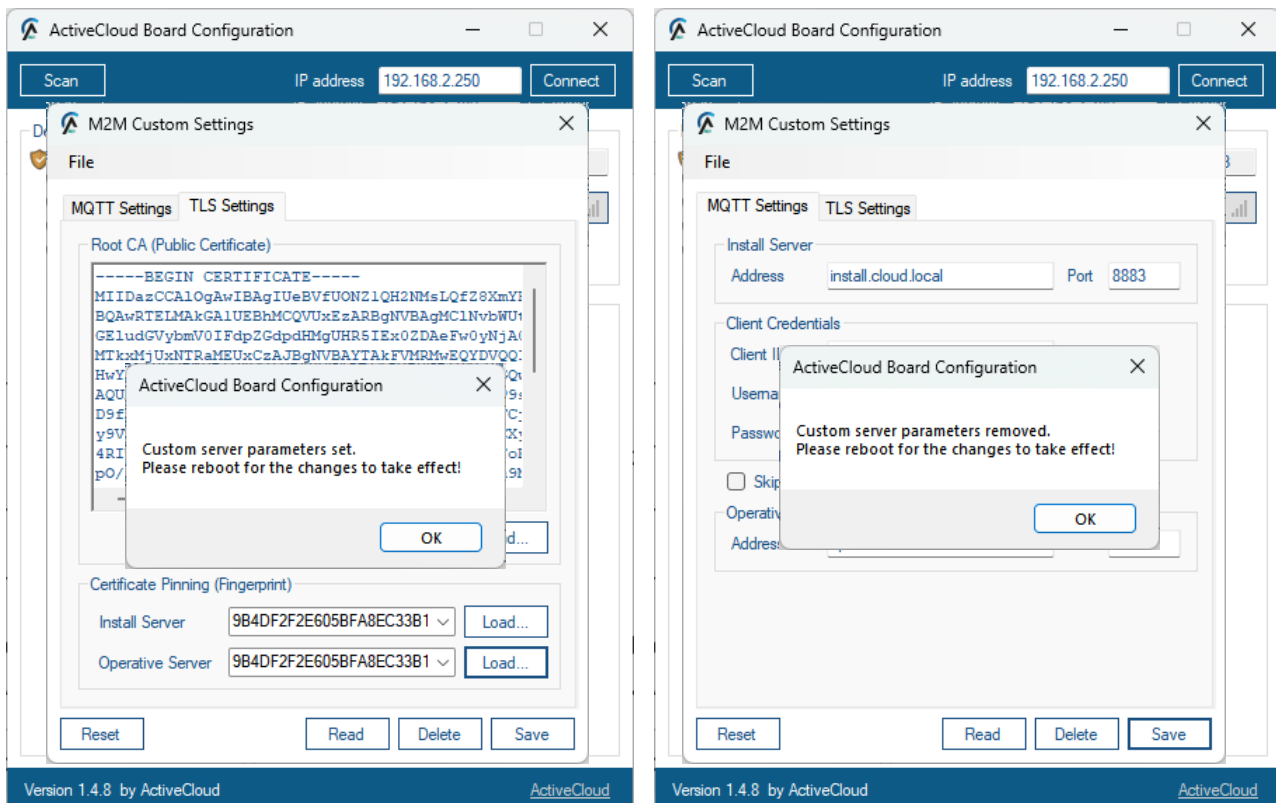
Enter the addresses and ports of your **Install Server** and **Operative Server**. If required by your system configuration, select the **Skip Install** checkbox to allow the board to skip the registration phase and connect directly to the Operative Server using the provided MQTT client credentials.

Open the **TLS Settings** tab and click **Load** upload the server certificate from your PC. Optionally, you can also upload the **Certificate Pinning (fingerprints)** for the **Install Server** and **Operative Server**.



Click **Save** to save the new settings. In the confirmation pop-up click **OK** then reboot the board for the changes to take effect. Please note that after rebooting, the firmware ignores invalid M2M settings.

Click **Read** to retrieve or refresh the M2M settings from the board or **Reset** to clear the settings displayed in the text boxes. Click **Delete** to delete the current M2M settings from the board: click **OK** in the confirmation pop-up, then reboot the board for the changes to take effect.



ActiveLAN / HTTP M2M

The **Machine-to-Machine HTTP** or **ActiveLAN** firmware allows the device to be integrated with an external management system using the HTTP protocol. The integration provides a notification mechanism that allows the fog machine to automatically notify the external management system when its internal status changes.

The fog machine sends a notification whenever one of its internal supported status variables changes. Each notification is sent as an HTTP GET or POST request, depending on the configured settings. Refer to the ActiveCloud MQTT Protocol document for a complete list of supported status variables.

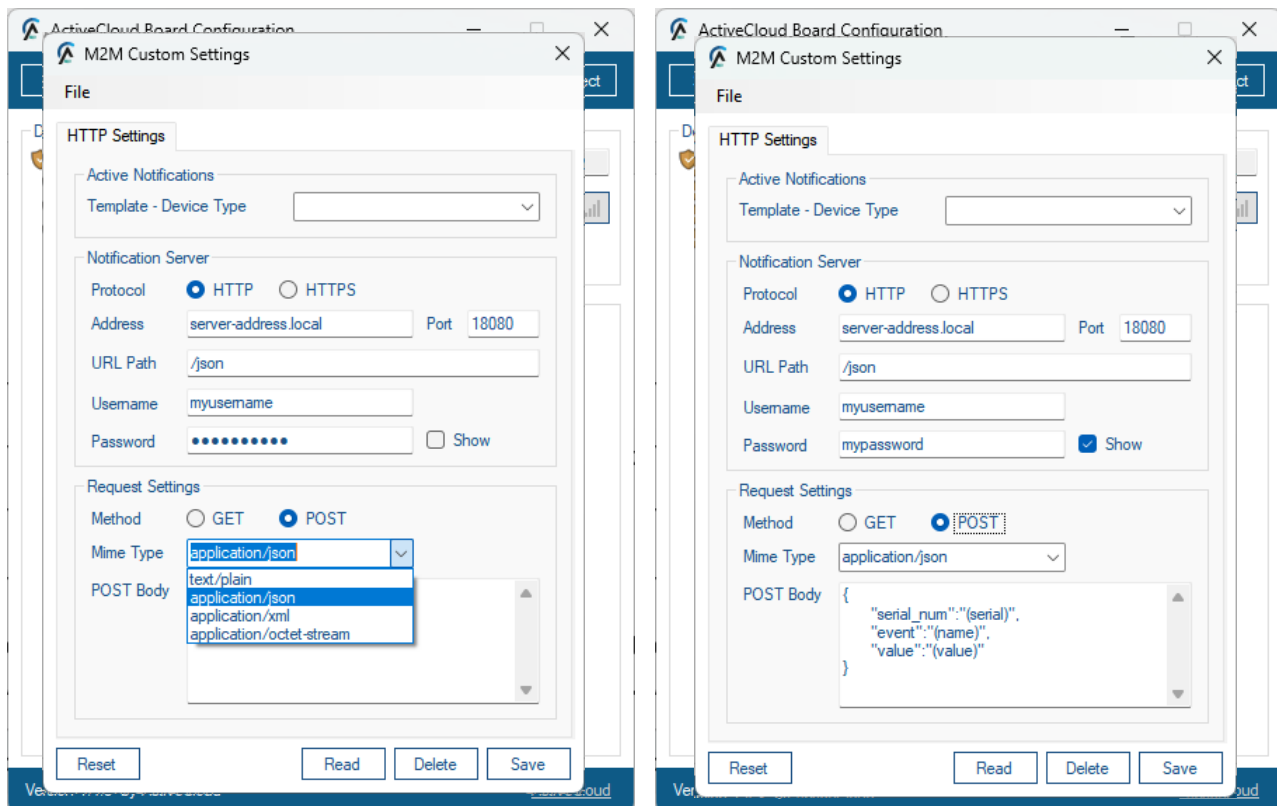
The M2M Custom settings allow you to configure the communication protocol (HTTP or HTTPS), the address and port of the external server, and the username and password for HTTP Basic Authentication, if required. You can also define the request method (GET or POST), the content type (for POST requests) and the request template: the request body for POST requests and the query string for GET requests.

To configure the notification settings, click **M2M** to open the **M2M Custom Settings** window. If the board has not yet been configured, click **OK** in the pop-up window indicating that the settings are not configured.

In the **Notification Server** section select the server protocol (**HTTP** or **HTTPS**), enter the server **address** and **port** and the request **URL**. If required by the server enter the **username** and **password** for the HTTP Basic Authentication (the only authentication supported).

In the **Request Settings** section select the request type (**GET** or **POST**).

For POST requests, select the **content type** from the following options: **text/plain**, **application/json**, **application/xml**, and **application/octet-stream**. You can also specify a custom content type.



In the **POST Body** field, enter a template that matches the selected content type. The template can contain the following special placeholders, enclosed in parentheses:

- **(serial)** : the device serial number.
- **(name)** : the name of the status variable.

- **(value)** : the new value of the status variable.

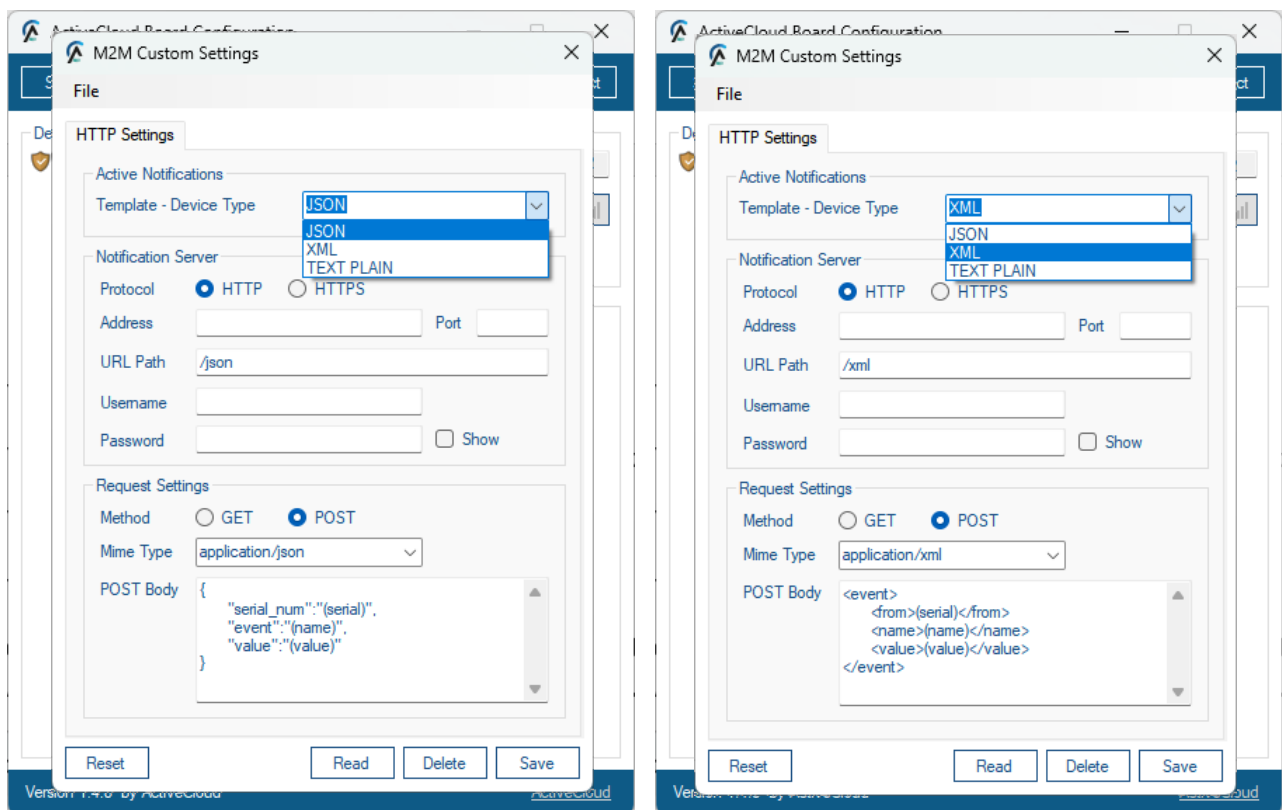
When sending the notification, the device automatically replaces these placeholders. For example, for the **application/json** content type, you can use the following request template:

```
{
  "serial_num": "(serial)",
  "event": "(name)",
  "value": "(value)"
}
```

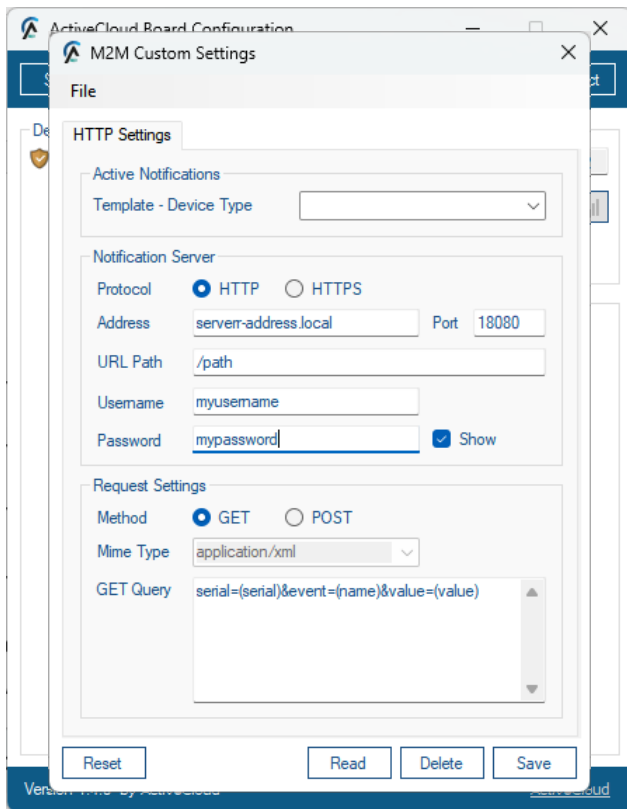
If, for example, the **arm** status variable of the device with serial number **000101** changes from **0** to **1**, the device sends a POST request with the following body:

```
{
  "serial_num": "000101",
  "event": "arm",
  "value": "1"
}
```

Please note: the application provides some predefined type and template for POST requests. From the dropdown list, select a predefined template among **JSON**, **XML** and **TEXT PLAIN**. The application automatically fills in the request method, content type, and request template.



For **GET requests**, enter the request template in the **GET Query** field. The template can contain the same special placeholders used for POST requests. When sending the notification, the device automatically replaces these placeholders with their corresponding values (either strings or numbers).



For example, you can use the following GET request template:

serial=(serial)&event=(name)&value=(value)

If, for example, the **arm** status variable of the device with serial number **000101** changes from **0** to **1**, the device sends a GET request with the following query string:

serial=000101&event=arm&value=1

Density Box

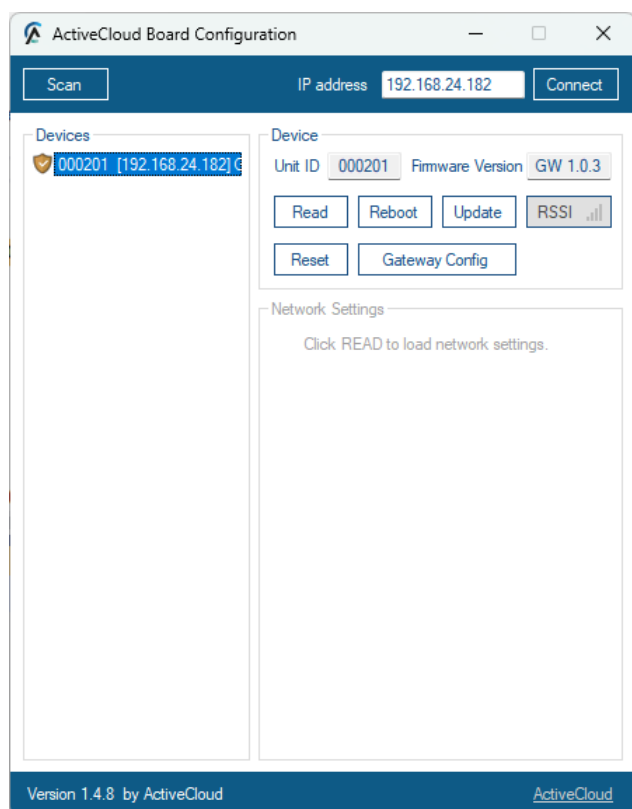
The **ActiveCloud Board Configuration** application also supports the configuration of the **Density Box** LAN board, also called **Density Gateway**. The firmware version of a Density Box is identified by the **GW** prefix (e.g. **GW-1.0.3**).

The Density Box LAN board implements local communication with Density Box BUS boards, also called **Density Bridge**, over **CAN** bus. The fog machines are equipped with a BUS board, acting as a bridge to the local CAN bus, while the LAN board itself act as a gateway from the local CAN bus to the Internet, providing connectivity to the ActiveCloud platform for all the locally connected fog machines.

The Density Box has the same basic configuration options as the ActiveCloud board. The application allows you to setup the Ethernet and WiFi interfaces. It also allows you to reboot the gateway, reset its ActiveCloud registration, display the WiFi signal strength, and update its firmware.

Machine-to-Machine settings are not available for the Density Box firmware. In addition, the Density Box gateway provides further configuration settings for its specific functions.

When the ActiveCloud Board Configuration application detects a Density Box gateway, it displays an additional **Gateway Config** button, which provides access to its specific settings.



Click the **Gateway Config** button to open the **Gateway Configuration** window. Refer to the *Density Box Manual* for detailed information about configuring the Gateway and using the controls available in the Gateway Configuration window.

