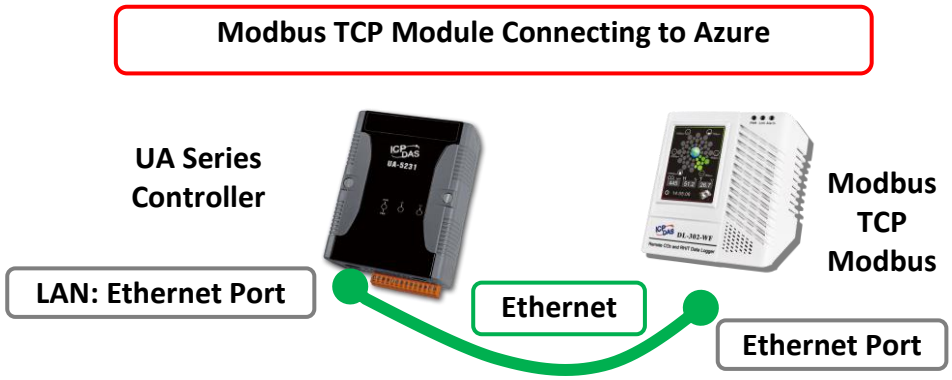
FAQ-AZR-01: UA Web UI Function Wizard – Module Connecting to Azure - How to Connect Modbus TCP <=> Azure ? (Use DL-302)

This FAQ introduces the settings of the **[Modbus TCP <=> Azure], using the DL-302 module of ICP DAS** (see the Wiring Diagram below). The UA series provides the MQTT function for the module to **connect to the Microsoft Azure platform** and allows the user to publish messages to Azure and receive messages from Azure. When the UA series connecting with a Modbus TCP module needs to read/write the I/O data through the MQTT Service and transmit them to the Microsoft Azure cloud platform, the user can use the **[Modbus TCP <=> Azure]** function.

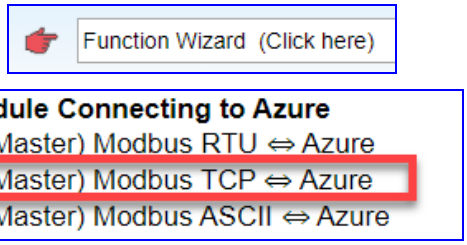
When **setting the UA and Azure connection**, the user needs to upload the **Root CA (Step 2)** and enter the **SAS Token (Step 3) that applied from Microsoft Azure**. The description (See "**Azure side settings**") is placed between Step 2 and Step 3, there are many setting steps, users can refer to it first.

- **Wiring Diagram of Modbus TCP Module Connecting to Azure:**

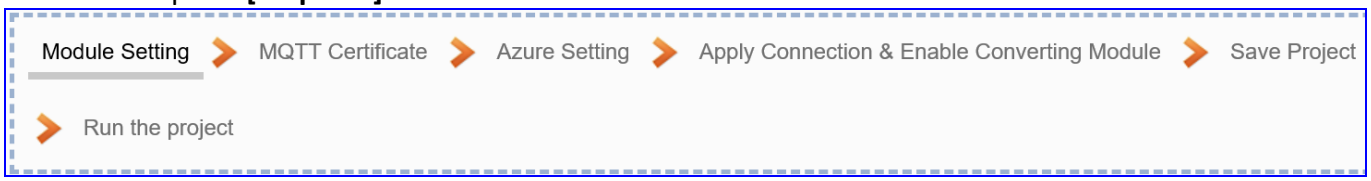


Note: The hardware/network connection methods please see the UA manual Chapter 2 .

First click the item [**Modbus TCP <=> Azure**] of the "Module Connecting to Azure" in the Function Wizard.

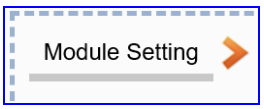


Then show up the **[Step Box]:**



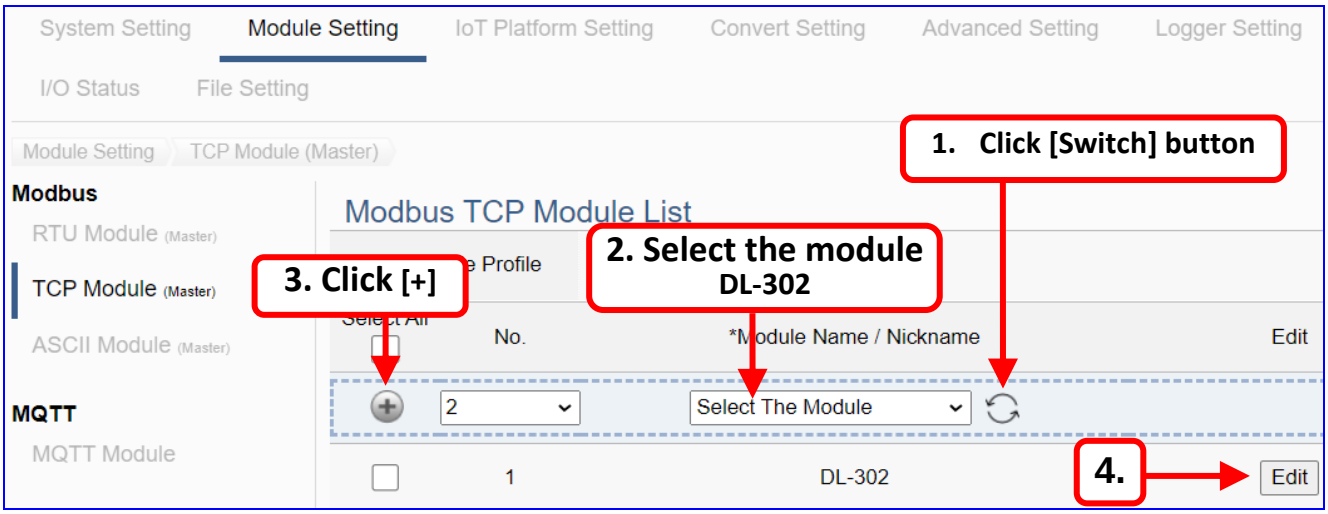
When enabling the Step Box, it auto enters the first step setting page (The step with a bold underline means it is the current step.). The user only needs to follow the "Step Box" step-by-step and then can complete the project quickly and correctly.

Step 1. Module Setting

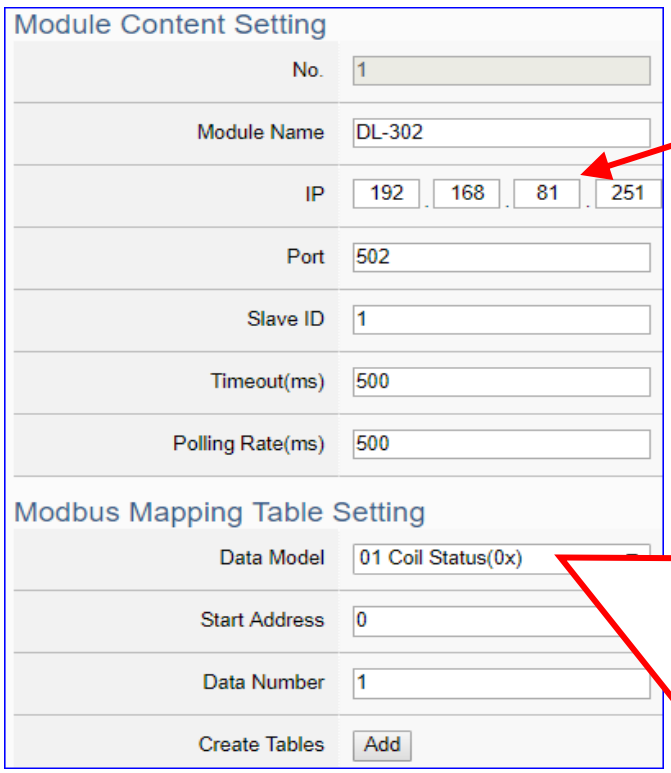


This step is mainly to set the module connected to the UA controller.

1. Click the [Switch] button to change to the [Select The Module] mode.
2. Select the DL-302 module of the DL series
3. Click the [⊕] button to add the module.



4. Click [Edit] button of the DL-302 module to enter the [Module Content Setting] page.

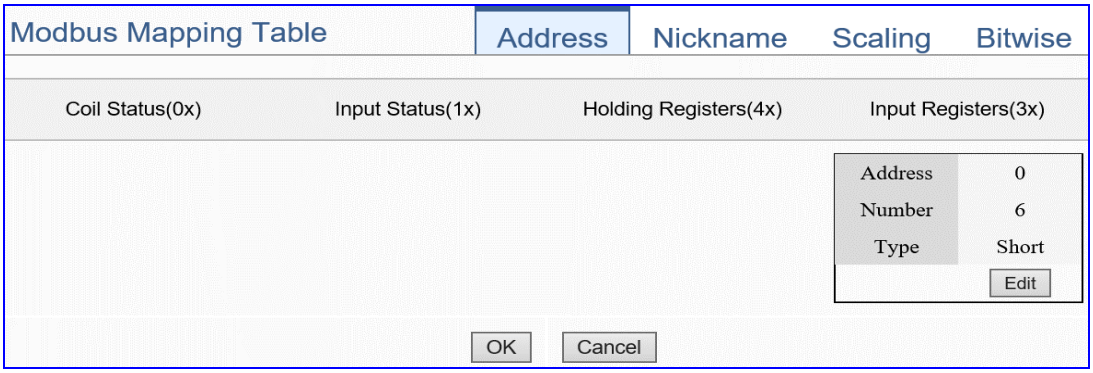


The user fills in the actual connected IP address

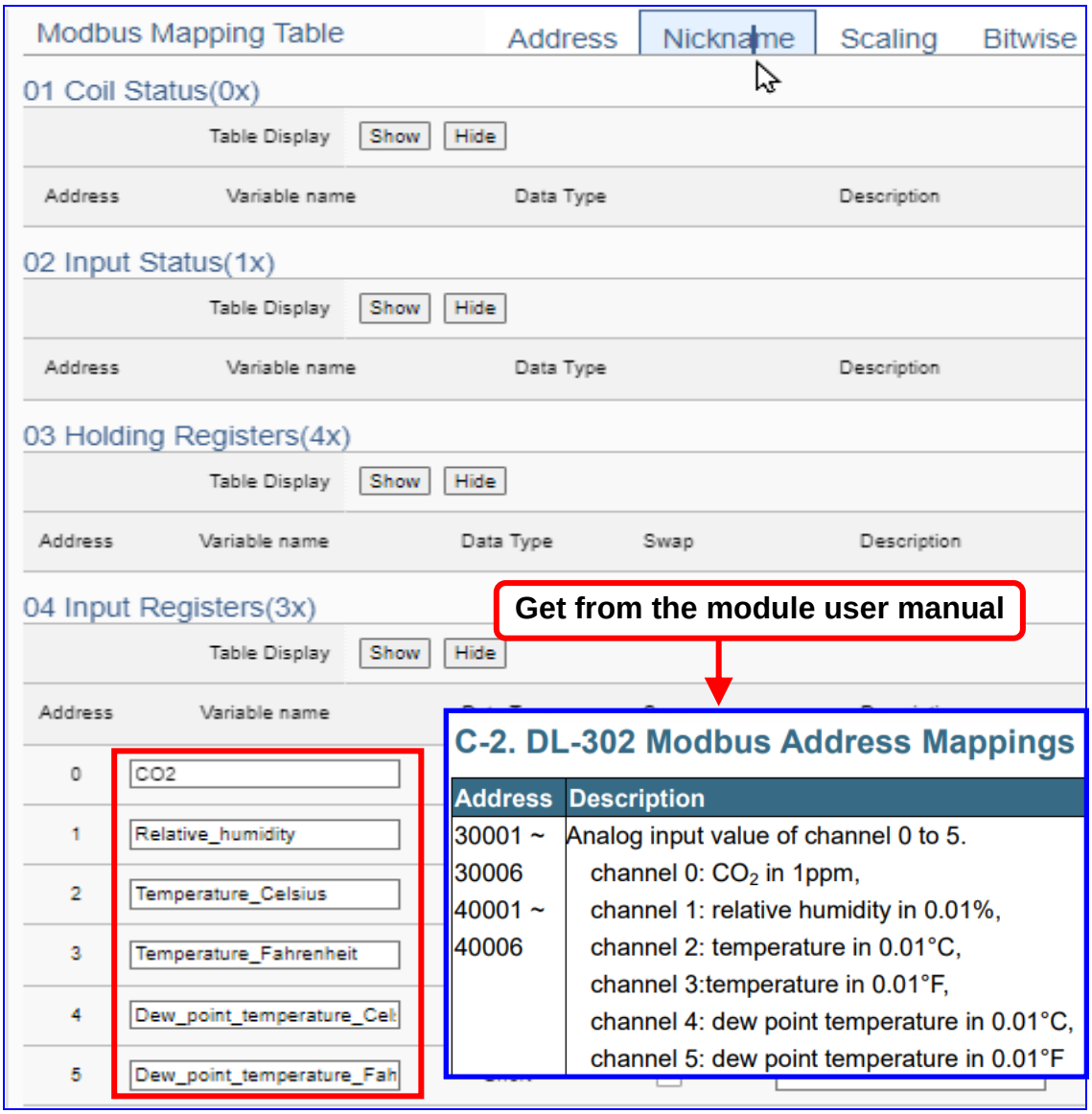
[Modbus Mapping Table Setting]
If use the ICP DAS module, system will auto-set the module's Modbus mapping table.

If not, user needs to check the module I/O & Modbus address via the module user manual.
For example:
Data Model: 04 Input Registers (3x)
Start Address: 0
Data Number: 6
Type: 16-bit Short
⇨ Click [Add]

Address **Address:** Display and edit the Modbus Mapping Table.

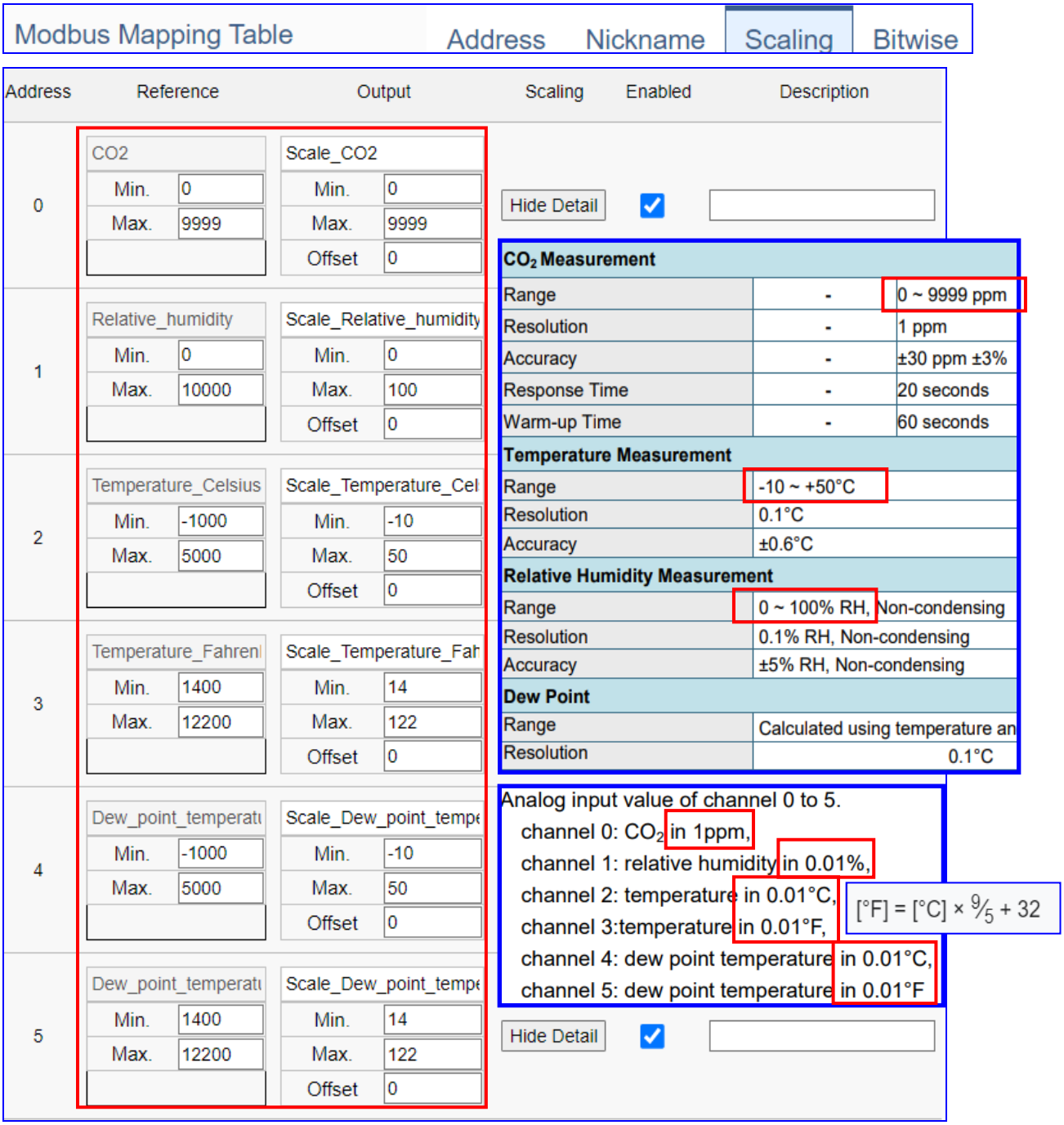


Nickname **Nickname:** Setting the variable nickname and description.



Scaling **Scaling:** Convert/scale the original value to an easily identifiable value.

1. Click the **[Show Detail]** of the variable Show Detail
2. Input **[Min.]** & **[Max.]** in **[Reference]** by the **measure range** value, scaling by the unit (1 or 0.01);
   Input **[Min.]** & **[Max.]** in **[Output]** by the **display range** wanted, and [Offset] value if needed;
   Add a [Description] to make the values more clear.
   (Check the module specifications and Modbus address table..., as same as the figure below)
3. Click the **[Enabled]** box, then the Scaling function will be active when the project restarts.



p.s. Scaling is only available in the AI/AO settings of Modbus RTU/TCP.

Step 2. MQTT Certificate

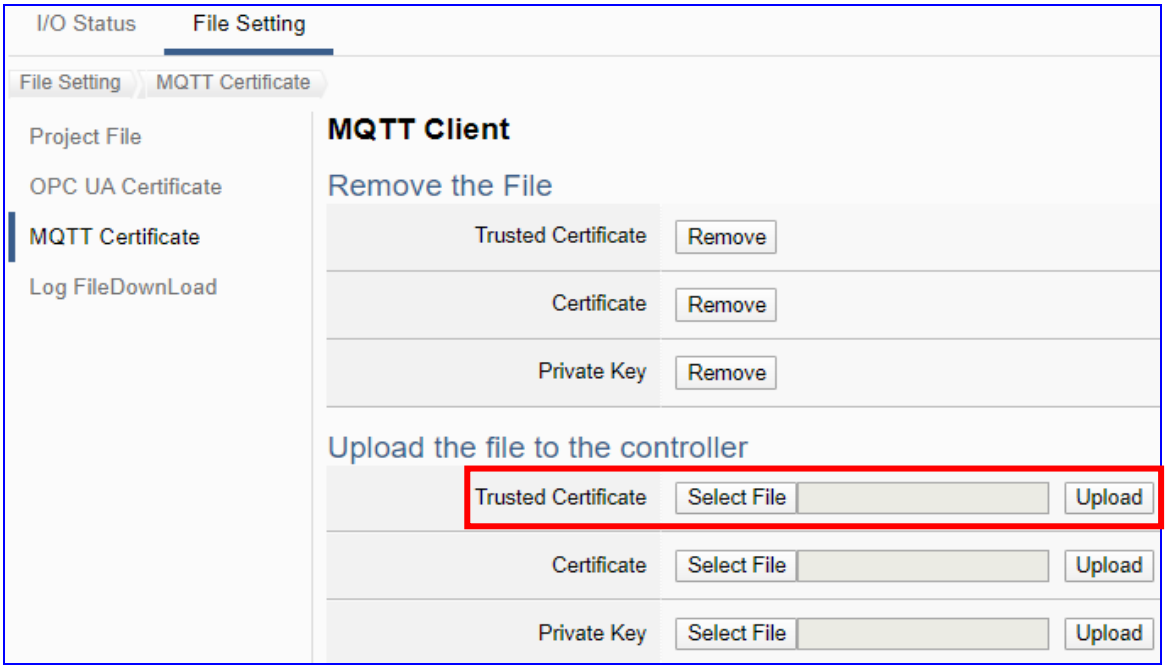
For MQTT communication security to **upload** the **MQTT Certificate**.

To upload the device's certificate, first, you need to obtain the MQTT certificate file for connecting the device and then upload it to the UA controller.

There are 3 types of certificates: Upload certificates according to the **authentication mode**.
To perform **Broker authentication**, you need to upload the **Trusted Certificate**.
To perform **Broker/Client two-way authentication**, you need to upload the **additional Certificate and Private Key**.
You can skip this step if your project does not use certificate transmission security.

For this example, connecting to **Azure** requires **Azure's MQTT Trusted Certificate**, you can **upload it in the [Trust Credential] field**. **(**The MQTT trust certificate **"BaltimoreCyberTrustRoot.crt"** has been **attached to this FAQ,** you can **download it in the FAQ-azr-1.**)

Trusted Certificate	• File format must be **PEM**. Extension name must be ".**pem", ".cer", or ".crt"**. • If select a wrong file, the system will show an error message.



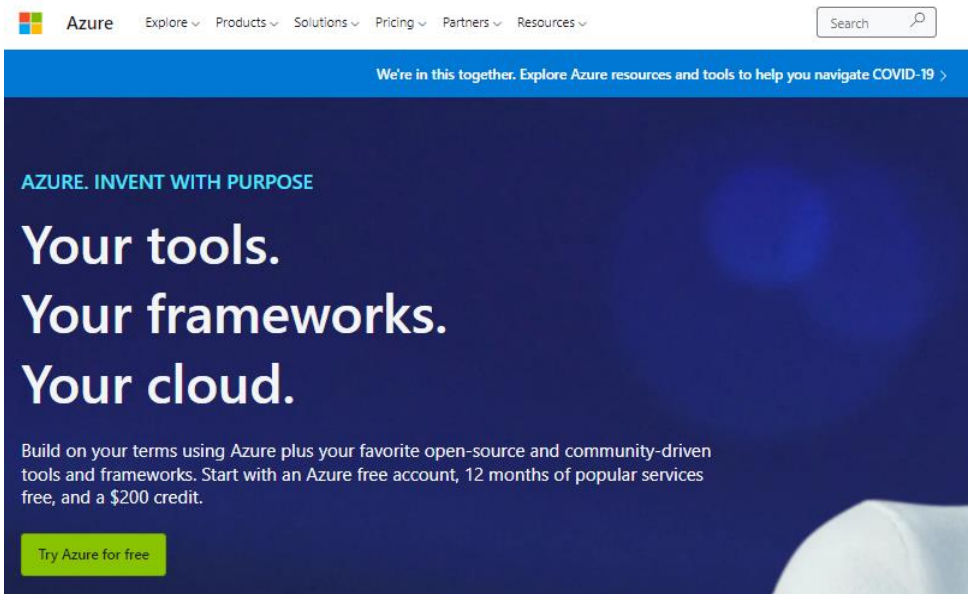
- **Azure Side Settings**

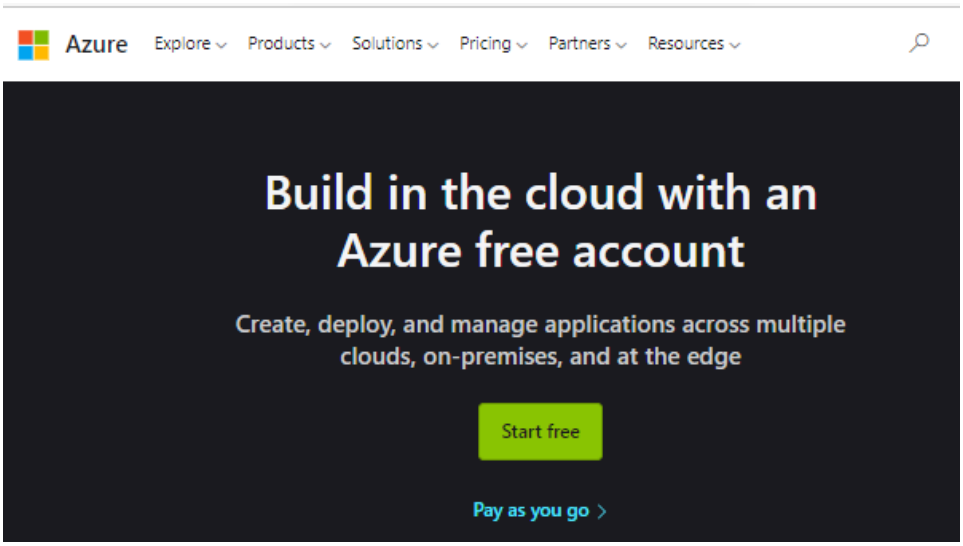
Before setting the next step [Azure Settings], please go to the **Microsoft Azure platform** to obtain Azure-related information, such as connection name, SAS token, etc. This section will explain the steps for getting data on the Azure side (including Azure account application, resource settings, trust credentials, SAS tokens... etc.).

Please go to the Microsoft Azure website:

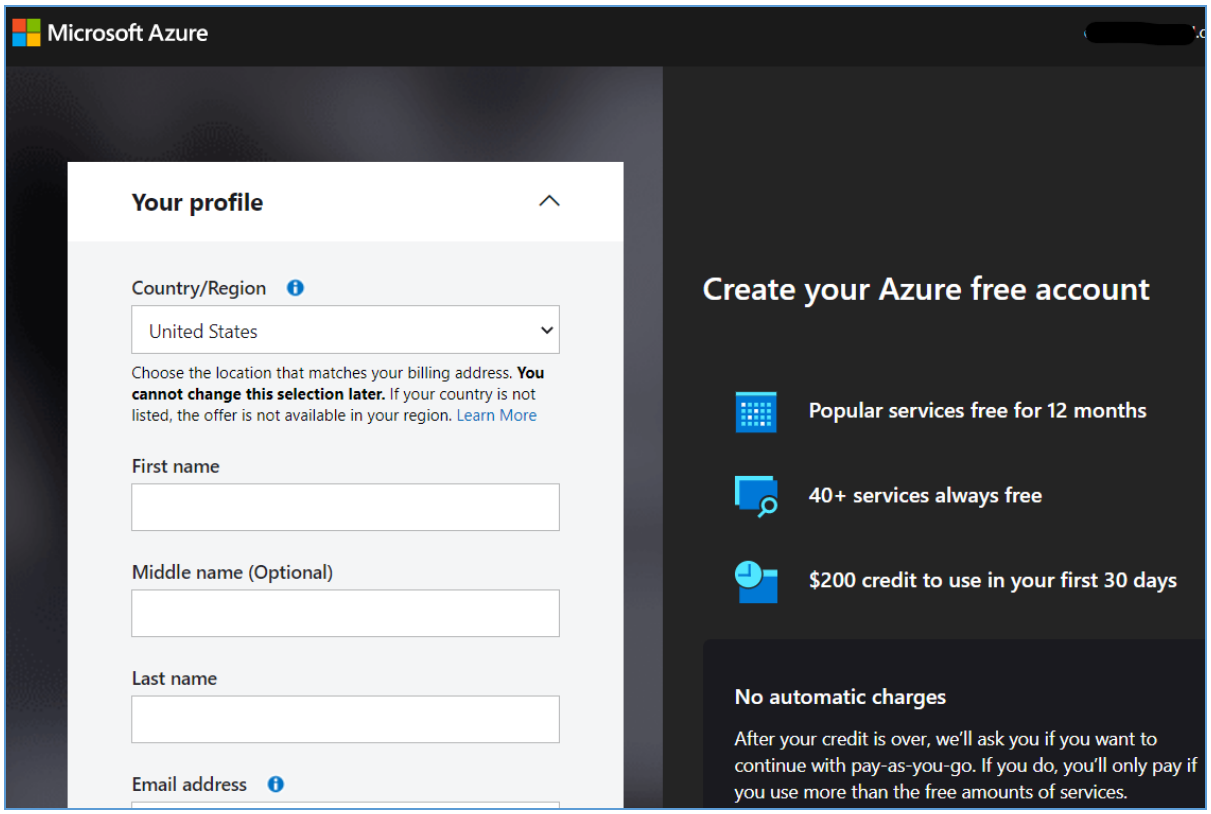
A. Microsoft Azure Account: Create / Sign-in

Using the Azure services, the user needs an Azure account. Microsoft Azure currently (2022/02) provides a free trial activity. Users can create a free account to try Azure for free. And then apply for an appropriate paid account according to the user's needs.
https://azure.microsoft.com/en-us/

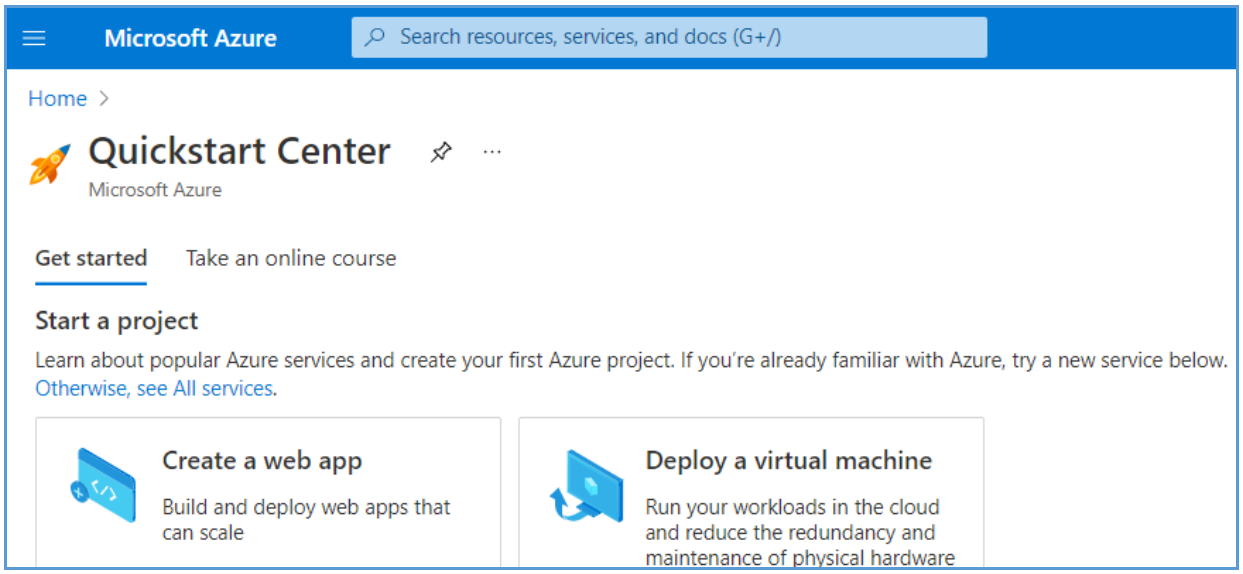




If the user already has an Azure account, please sign in directly. If doesn't has an account, please create one account. Click "Start Free" (see previous page) to create a free account, (or “Pay as you go” by user need), and fill in the registration information, including: Country First Name Last Name, Email Address, Phone number, etc.

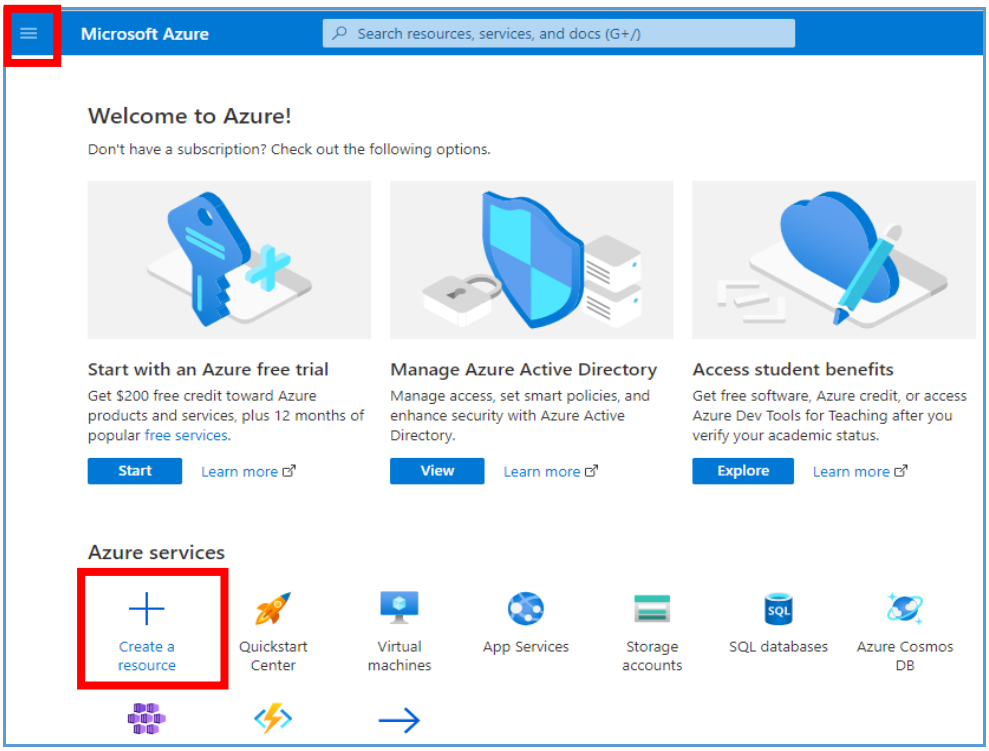


After creating your account, the user can set up the Azure service.

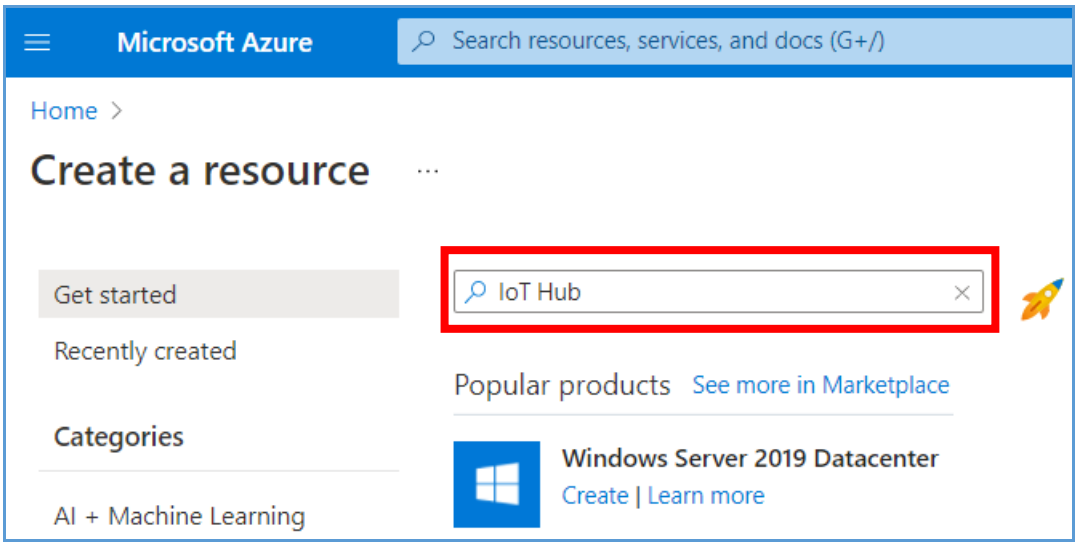


B. Create Azure IoT Service IoT Hub: to get the “Connection string”

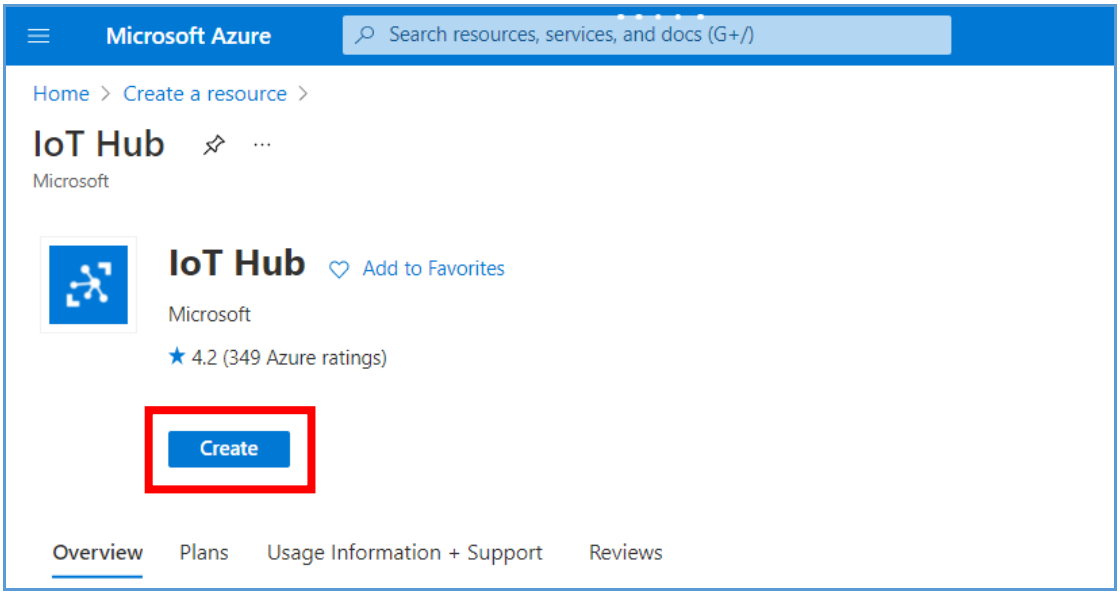
Entering the Azure, click on the menu icon of the upper left corner 【 > Home】to enter the home page (as shown in the figure below, you can view various services of Azure), please click 【Create a resource】 to create and set up the required resources.



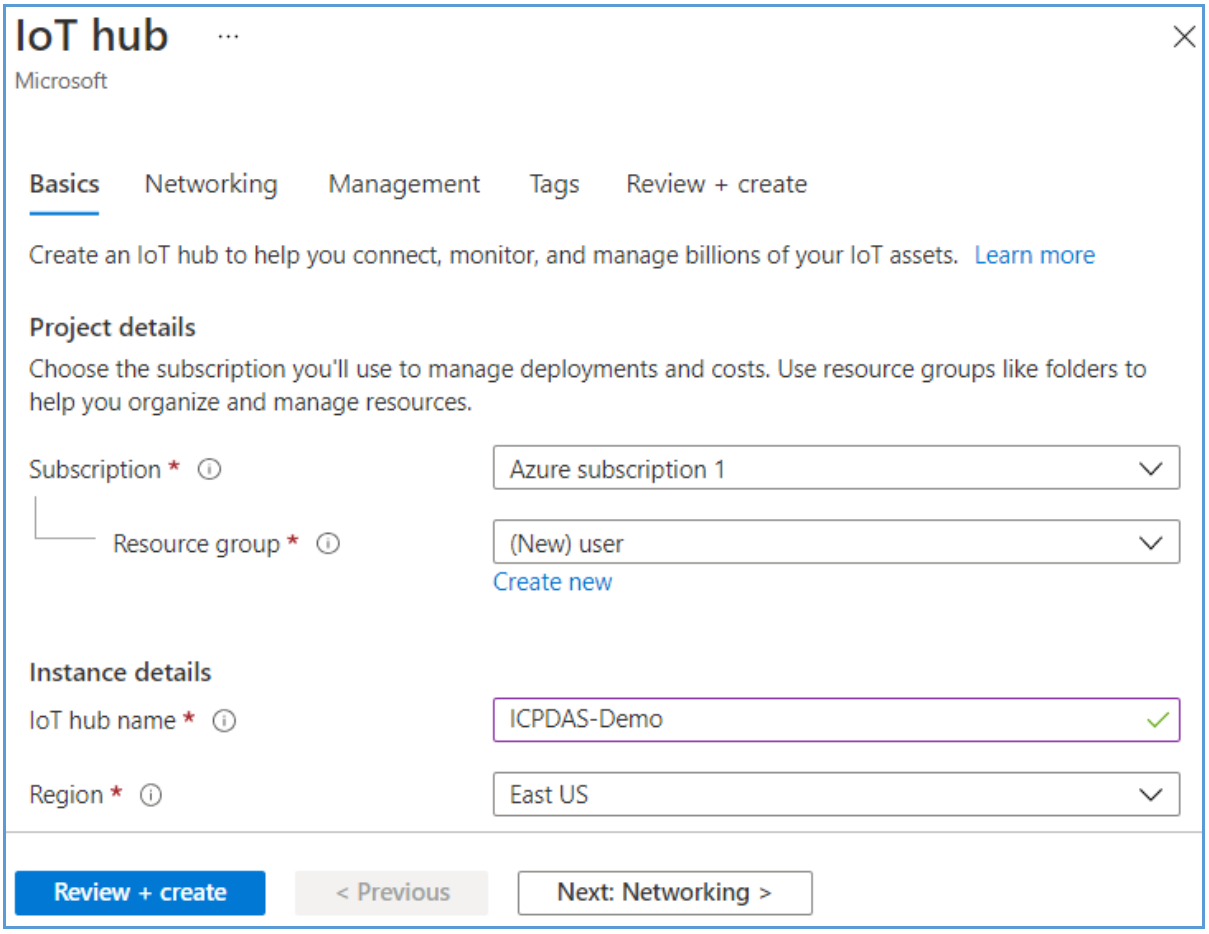
The UA communication server uses Azure's "**IoT Hub**" resource service, please search for "**IoT Hub**" (as shown below).



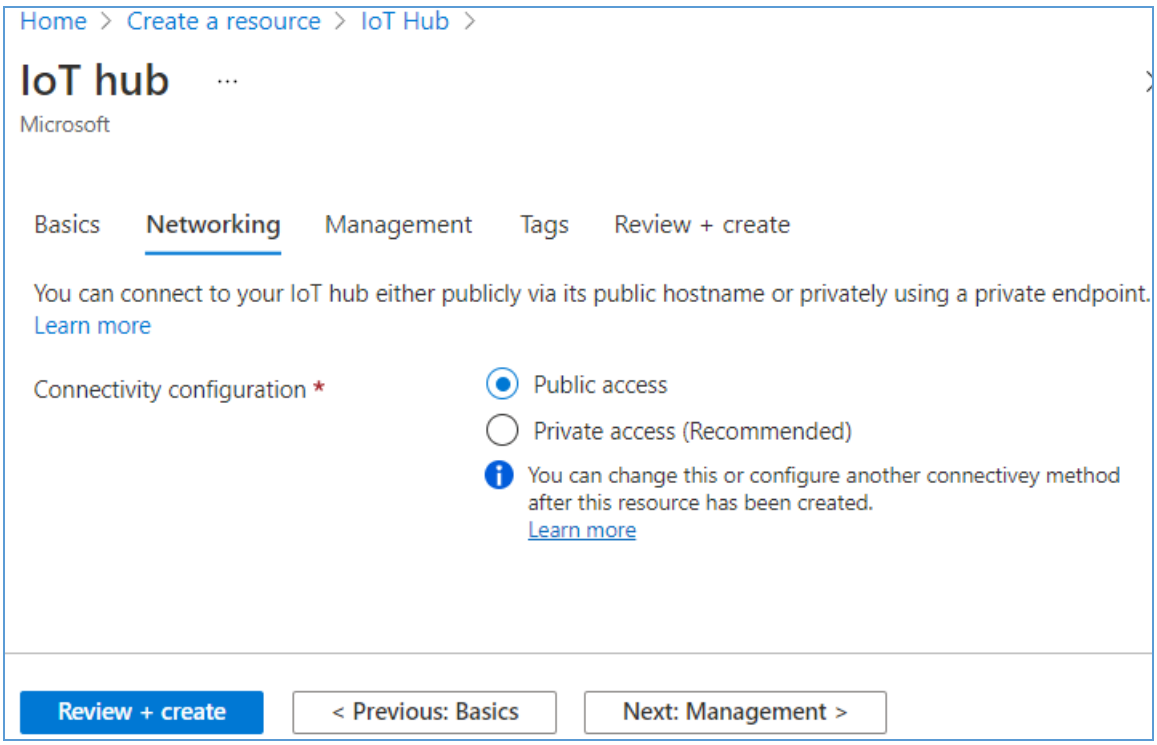
On the “IoT Hub” webpage, click “Create” to create a resource.



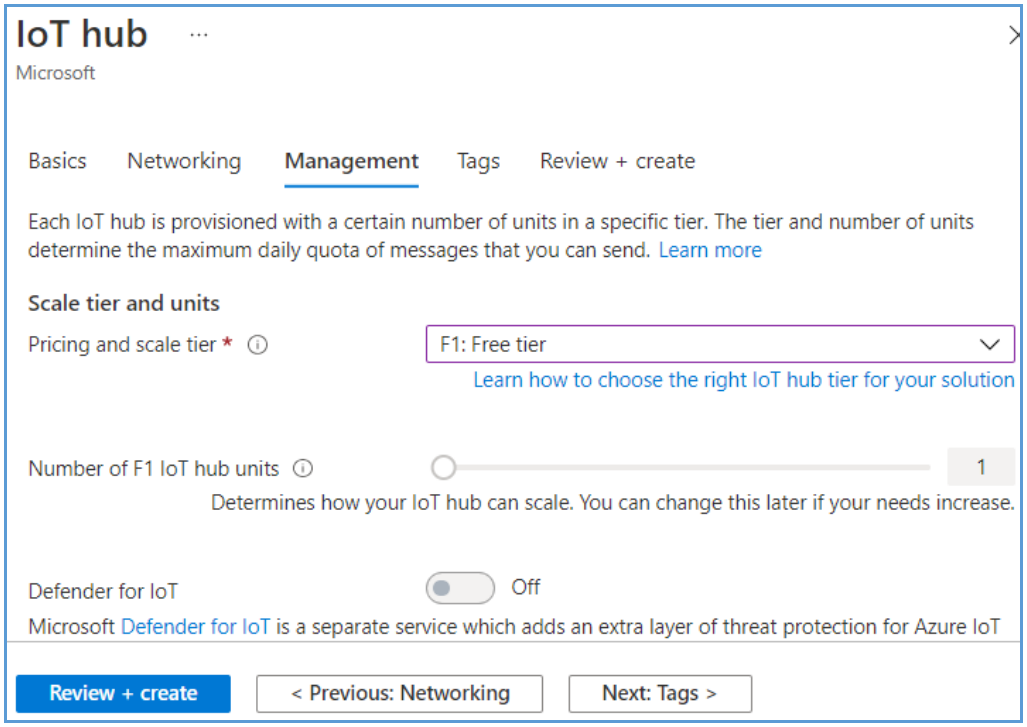
Set up the “**Basics**” data for IoT hub. Click “**Create new**”, give a folder name for **resource group**. Give a name for “**IoT hub name**” and select the region. And click “Next: Networking”.



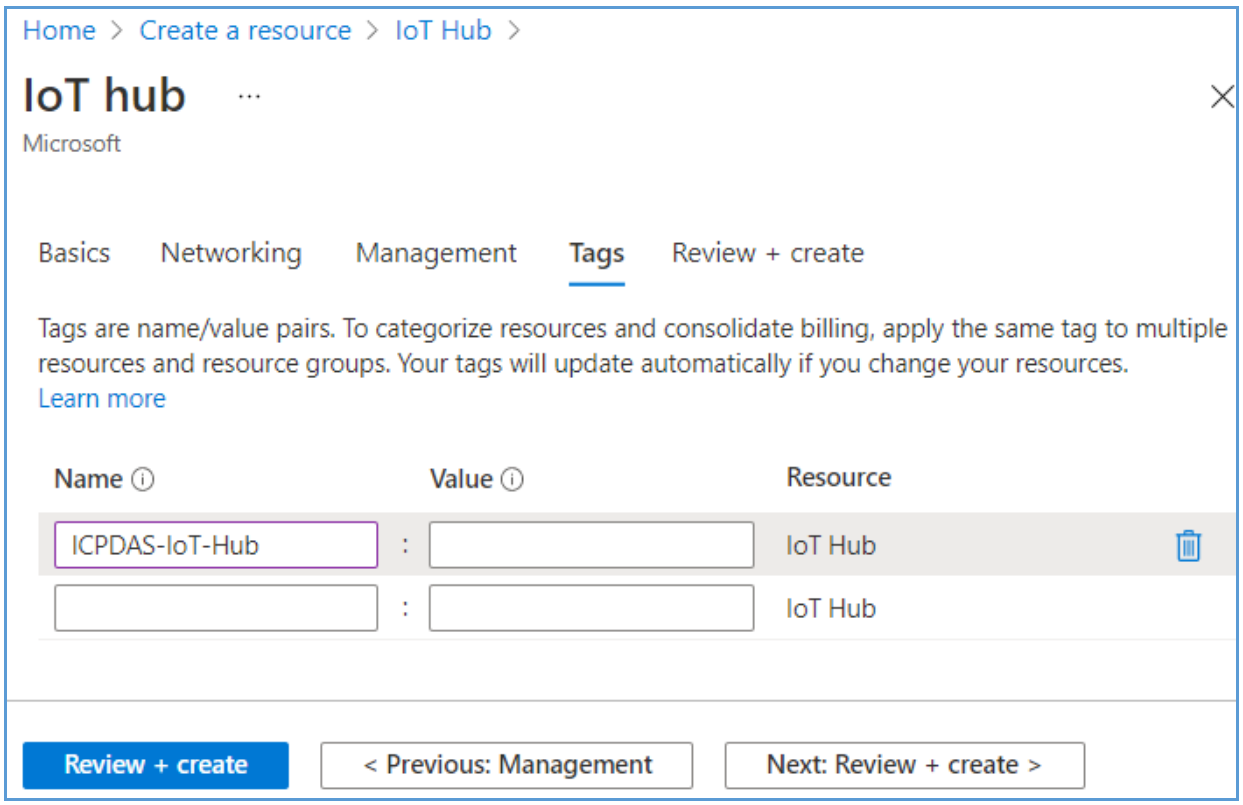
On "**Networking**" page, select "**Public access" or "Private access**" for the IoT hub publicly according to the user project need. Then Click "**Next: Management**".



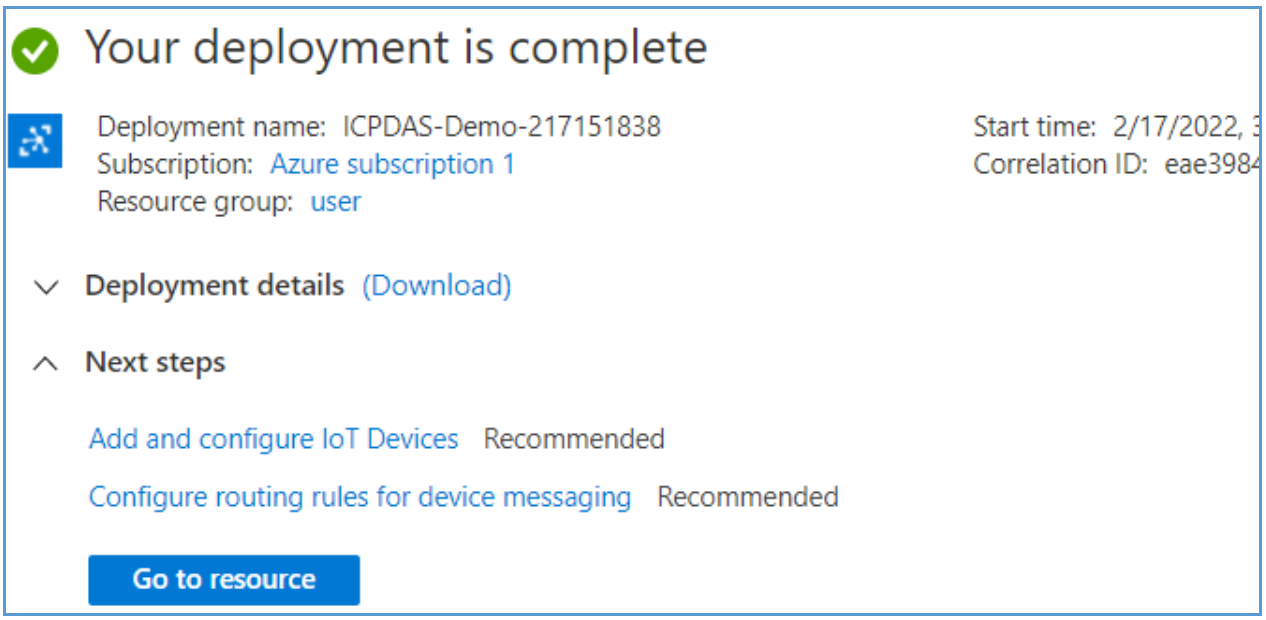
On "**Management**" page, user can select "F1: Free tier" for test, or click the blue text to learn how to choose the right IoT Hub tier for you solution. Then click "Next: Tags".



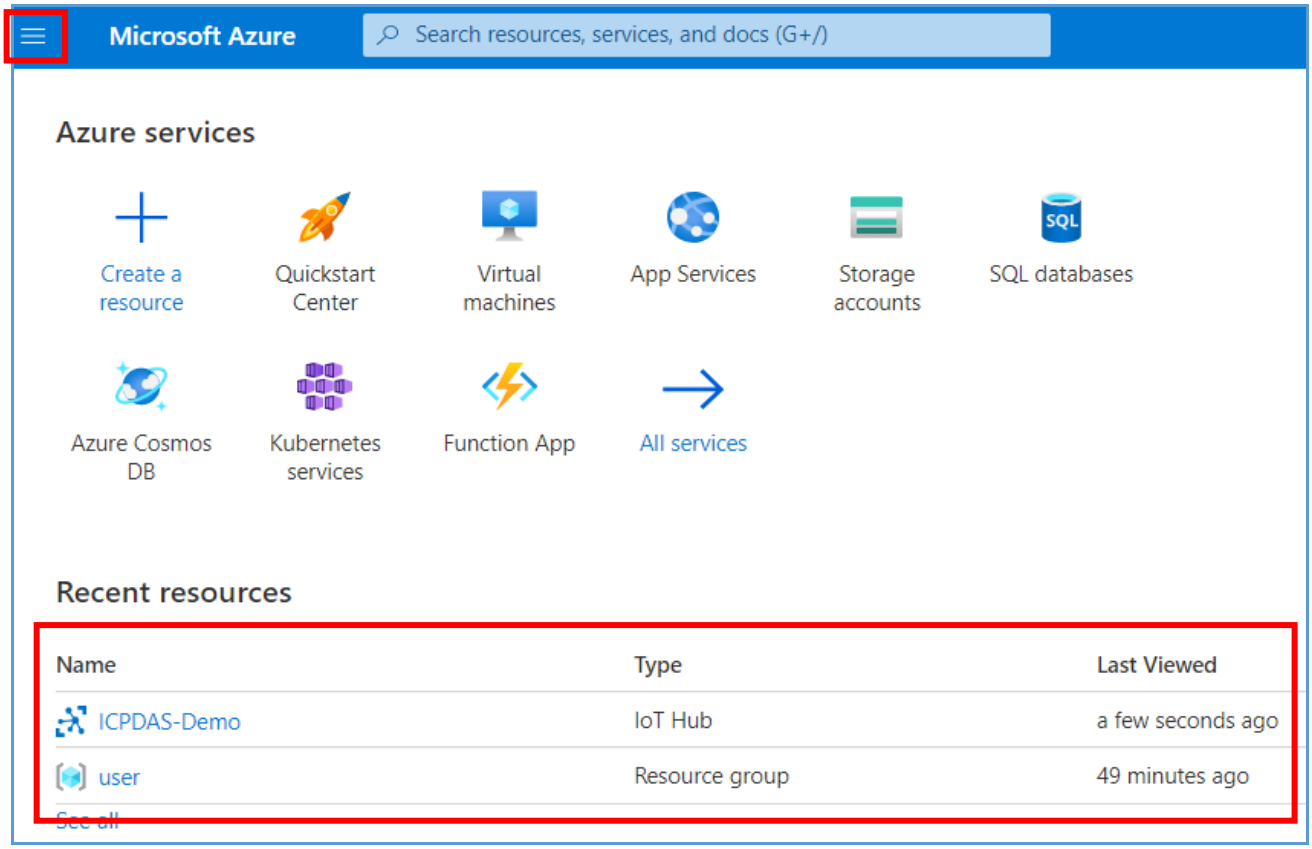
On “**Tags**” page, set the tag name and value of the resource group, for example, ICPDAS-IoT-Hub. Users can apply the same tag to multiple resources and resource group. Then next.



On the “Review + create” page, when the validation passed, click the “**Create**” button to deploy the resource. When showing the following messages, the deployment is complete.



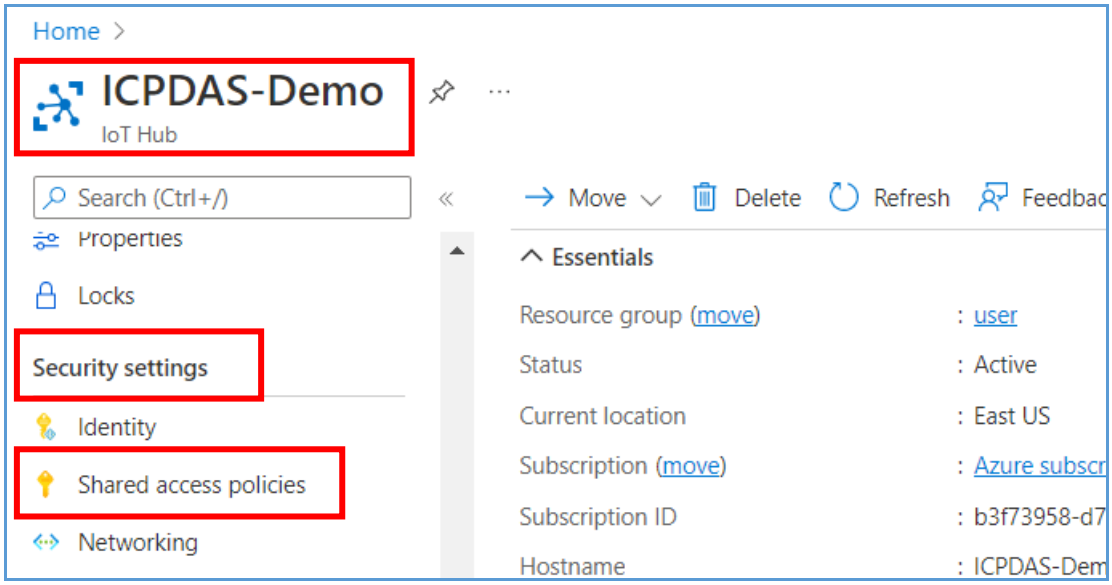
Click the menu button in the upper left corner【 > **Home**】.
The created resouces of "IoT Hub" and "Resource Group" will display in the "Recent resources".

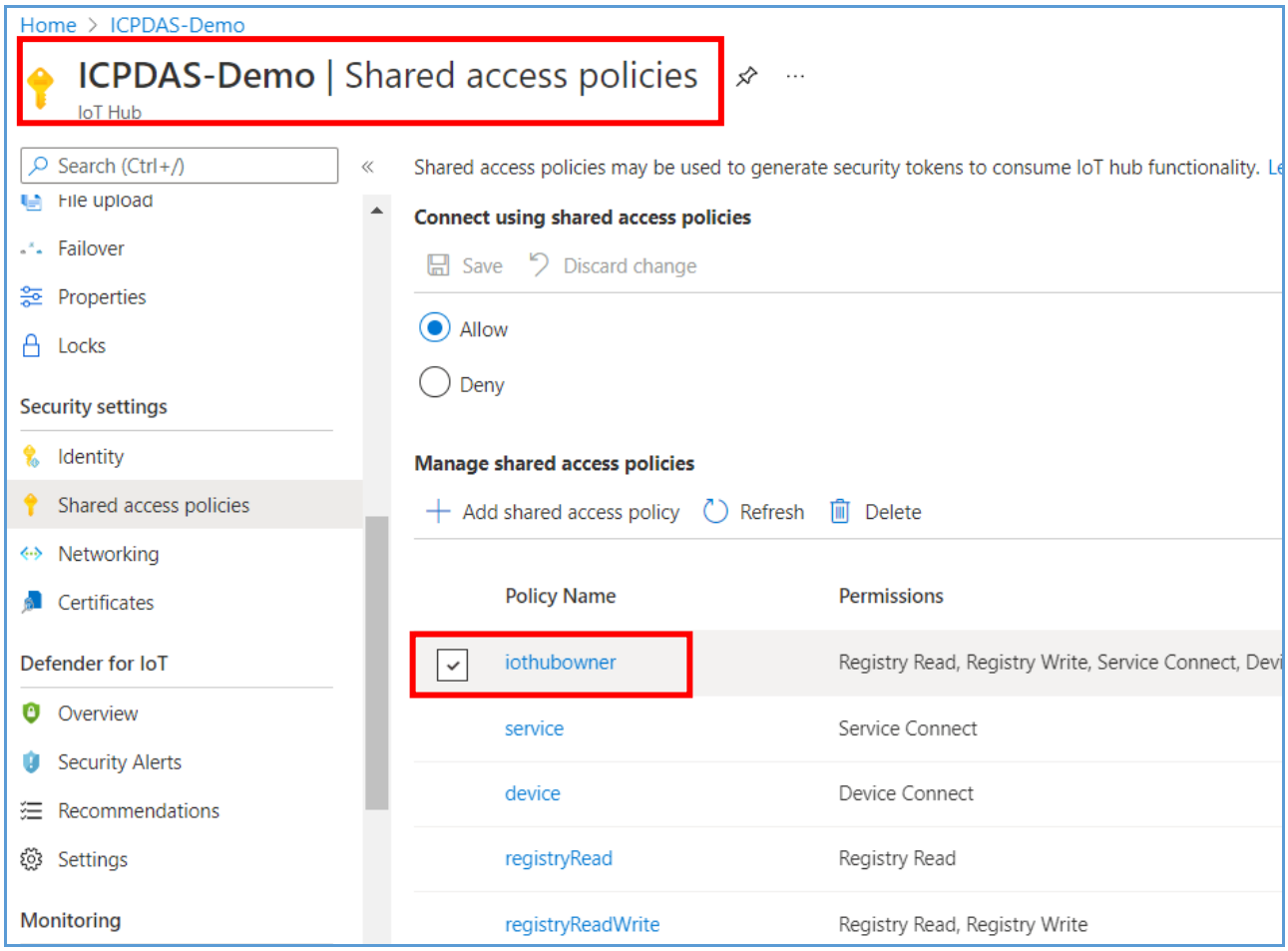


Double click the name of the IoT Hub, this example is “**ICPDAS-Demo**”, enter the setting page of the ICPDAS-Demo.

Enter “**ICPDAS-Demo**” setting page of IoT Hub, scroll left function menu:

1. Find the "**Security Settings**" category and **click the "Shared Access Policies"** function
2. Check the box of "**iothobowner**" in the "Policy Name" column, and click "**iothobowner**".



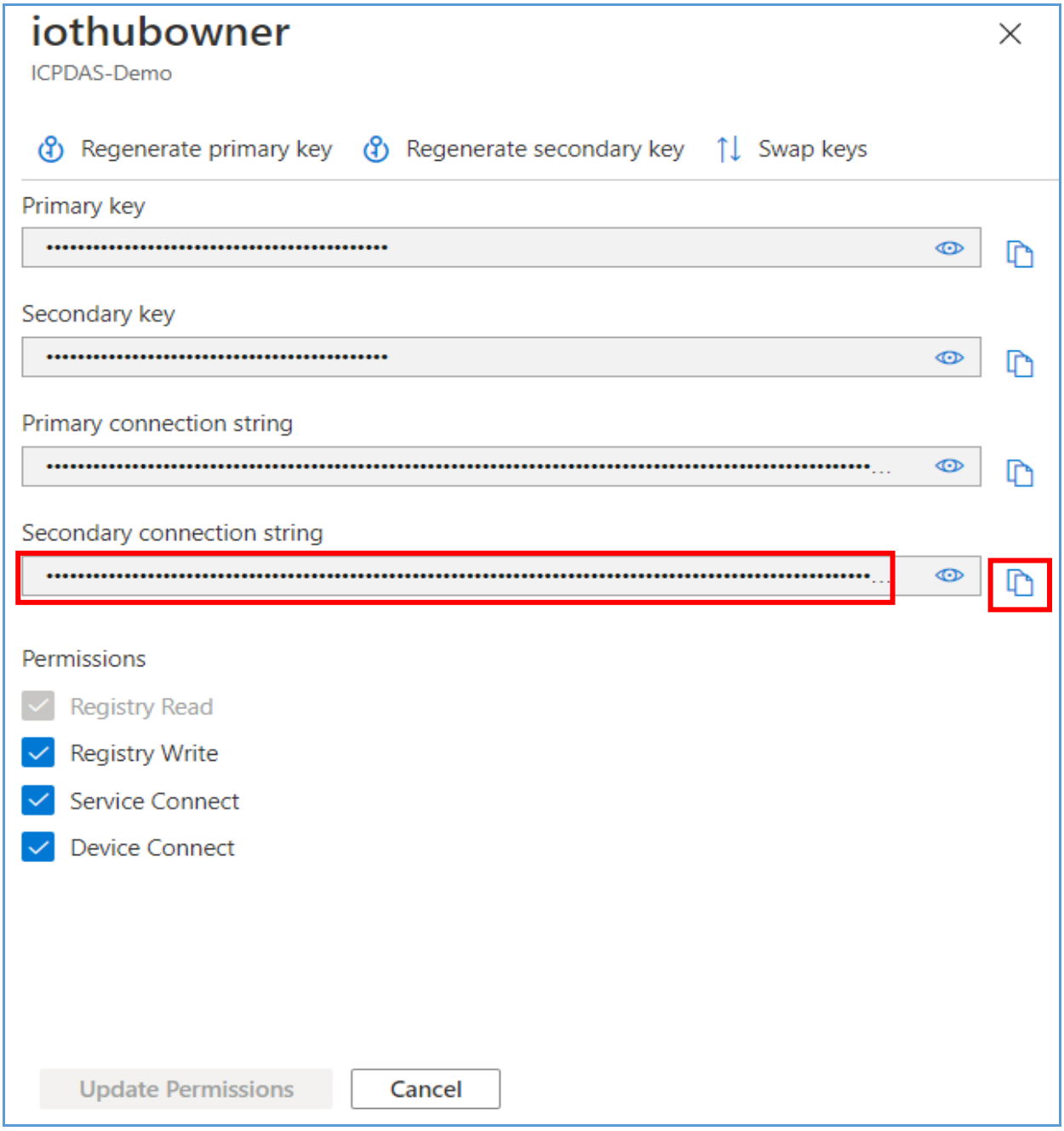


In the "**iothubowner**" page:

1. Click the icon on the right side of "**Secondary connection string**" to copy the string. This string is the **"Connection string"** of the next step for setting **Azure IoT Explorer**.

2. Recommend to save this string to a text file for the user easy past it to the other settings.

Note.: This string contains personal account and payment information. Do not provide it to others! The picture will make some mosaic when shown it.

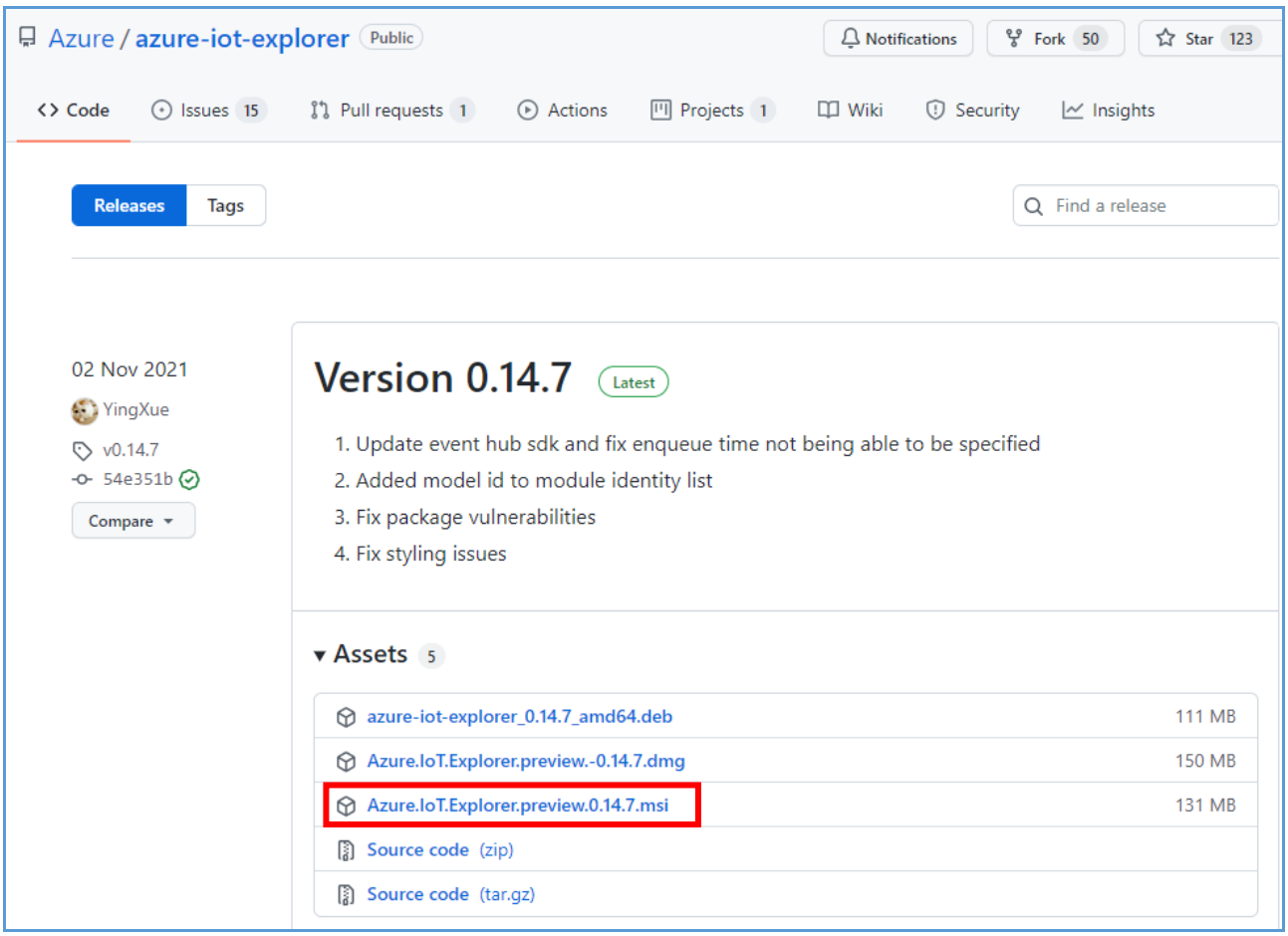


C. Create Azure Connection: PC side Azure IoT Tool "Azure IoT Explorer"

For setting the Azure connection, the user has to set up the IoT Hub and needs to install an Azure IoT management tool, such as **Azure IoT Explorer**, on the PC side.

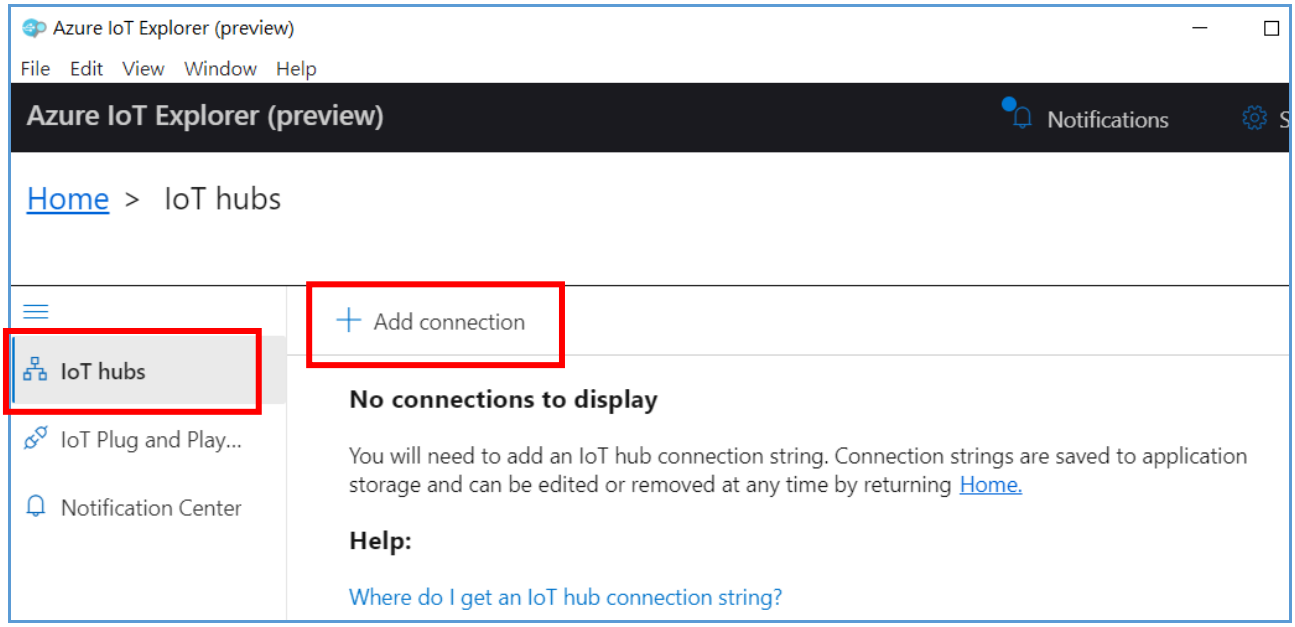
First, download and install the **Azure IoT Explorer** software, and create an Azure IoT management tool on the PC side to set up the device connected with Azure. Click the following link: https://github.com/Azure/azure-iot-explorer/releases

For Windows system, please download the file with the extension **.msi**.

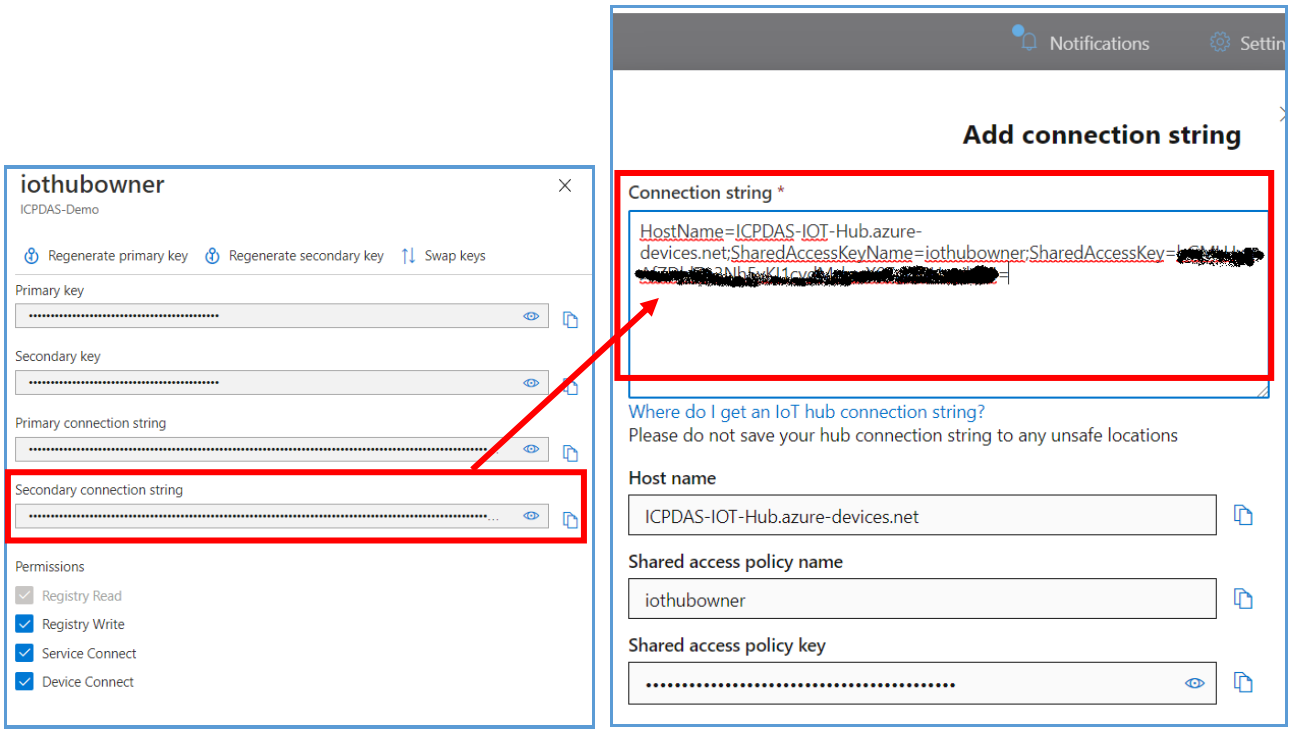


After the download is complete, please install Azure IoT Explorer. And then start and execute the software.

Next, on the Azure IoT Explorer page, switch to the "IoT hubs" item in the left menu, and then click " **+ Add connection**" on the right side to create a new connection, as shown below.



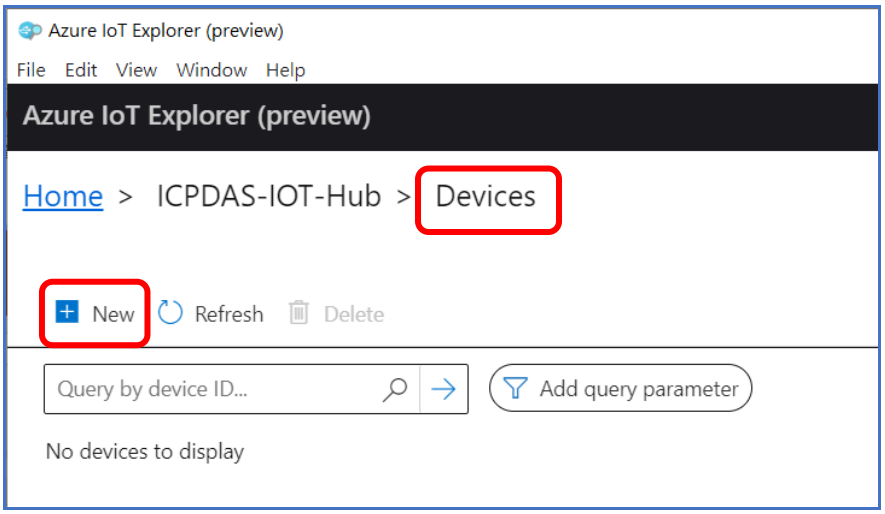
Then copy the connection string obtained in the previous step (C) (as shown on the left image) into the "Connection string" field on this page (as shown on the right image). Note.: This string contains personal account and payment information. Do not provide it to others! The picture will make some mosaic when shown it.



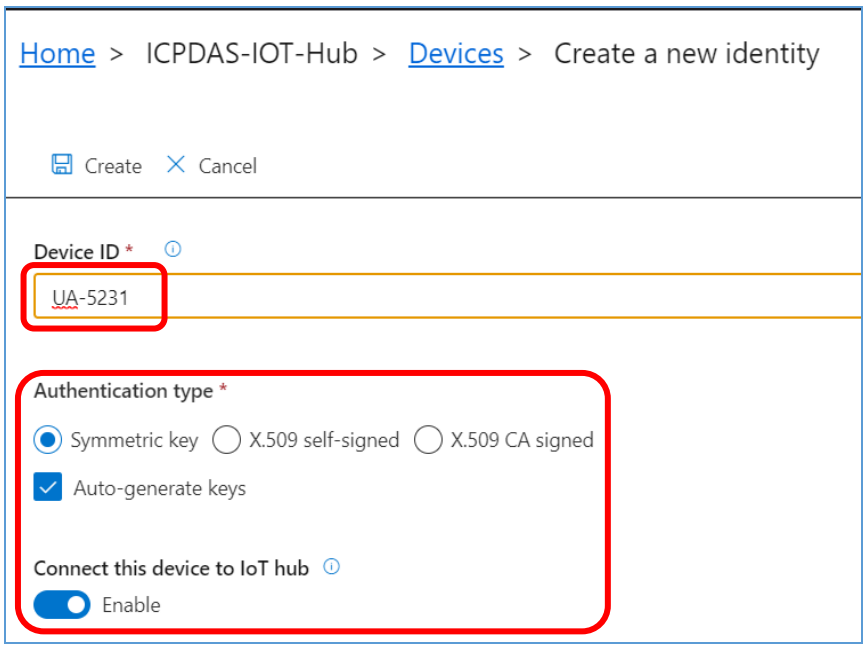
D. Create Connection Devices: Get "SAS Token" for UA Settings

In the Azure IoT Explorer software, enter the "IoT hubs" connection. The next step is to create an UA device connecting with Azure.

In the “Devices” page, click “**+New**” to create a new device.

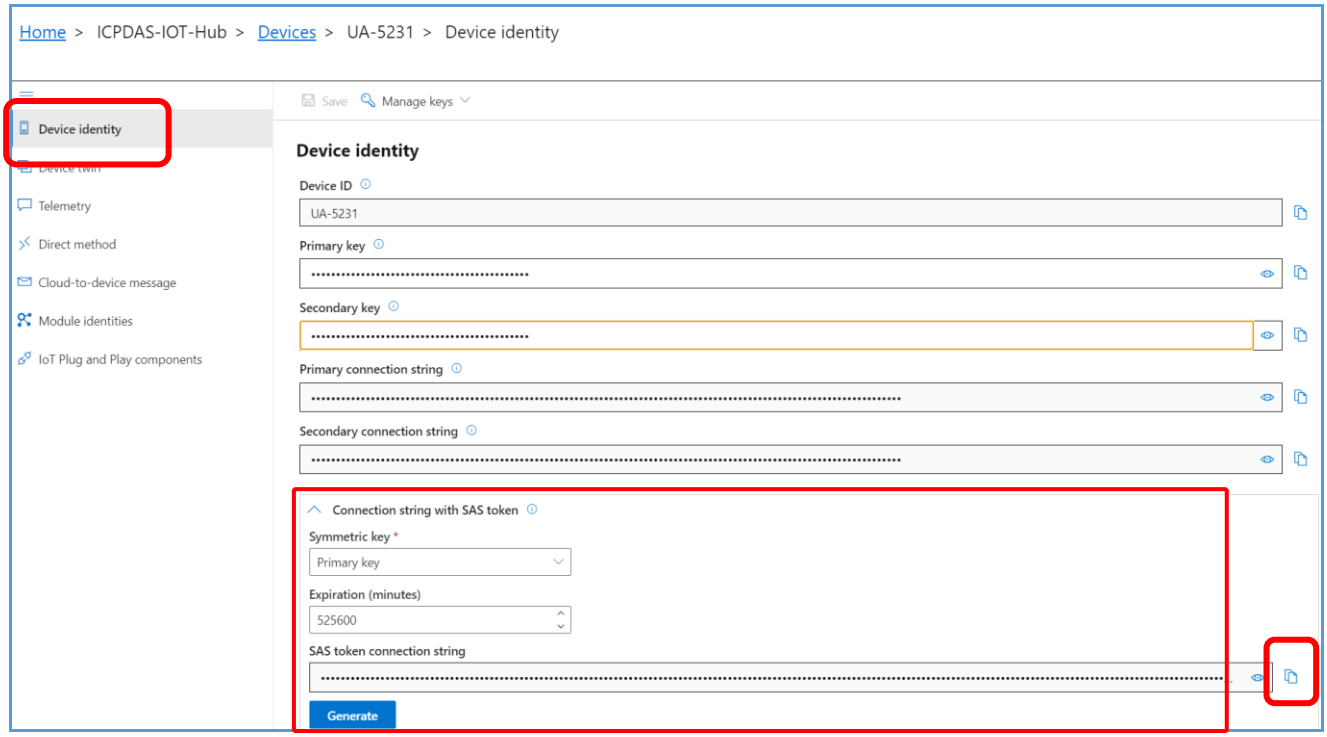


Enter the name of the connecting UA device in the "Device ID" item. Please refer to the figure below for the setting items.



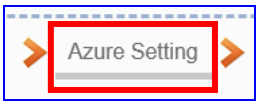
After setting the device, the system will generate the keys and token. Click the left menu "Device identity" and copy the "SAS token connection string" (click the copy icon on the right side of the field) that is the "SAS token" for the UA setting (Used in the next section). Or save this token string to a TXT file to paste in the UA side setting.

Note.: This string contains private information. Do not provide it to others! The picture will make some mosaic when shown it.



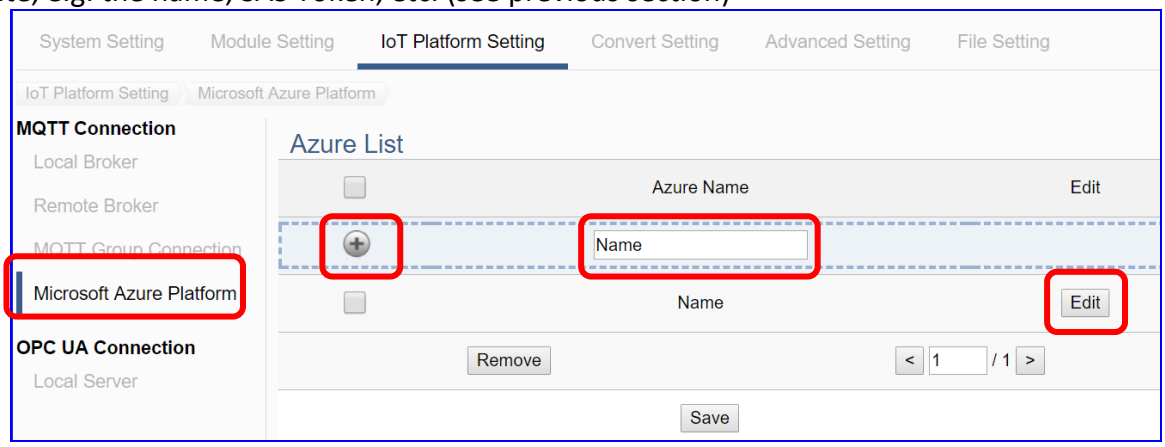
Now, the settings on the Azure side have finished. Next, please go back to the UA web setting interface to fill in the Azure strings applied in this section into the UA settings (see next section: Step 3).

Step 3. Azure Setting

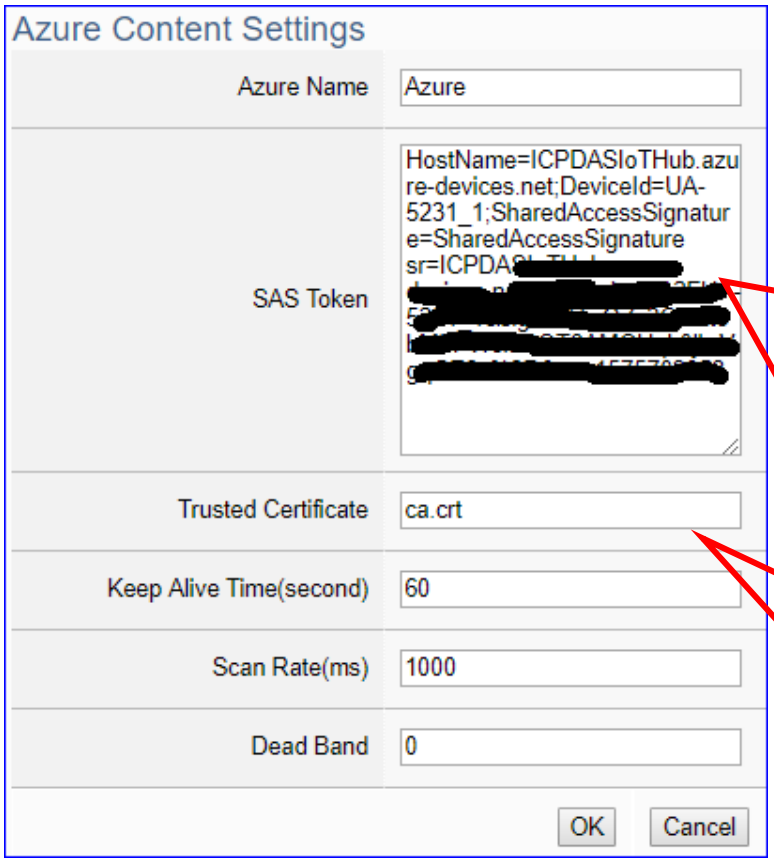


This step is to for setting the information that got from the Azure Platform

Back to the UA web setting interface, click the **Step 3 [Azure Setting]**. Enter the [**MQTT Connection] > [Microsoft Azure Platform**] to set the Azure information that got from the Azure website, e.g. the name, SAS Token, etc. (see previous section)



1. Set up an **Azure Name** for connection
2. Click the "**+**" button to create an Azure connection.
3. Click [**Edit**] button to enter the “Azure Content Settings” page.

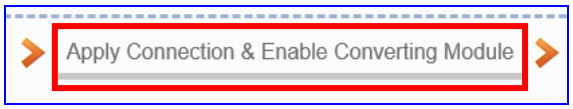


Copy and paste the **SAS Token Connection String** requested from the **Azure platform** that represents this device.

Note.:
This string contains private information. Do not provide it to others! The picture will make some mosaic when shown it.

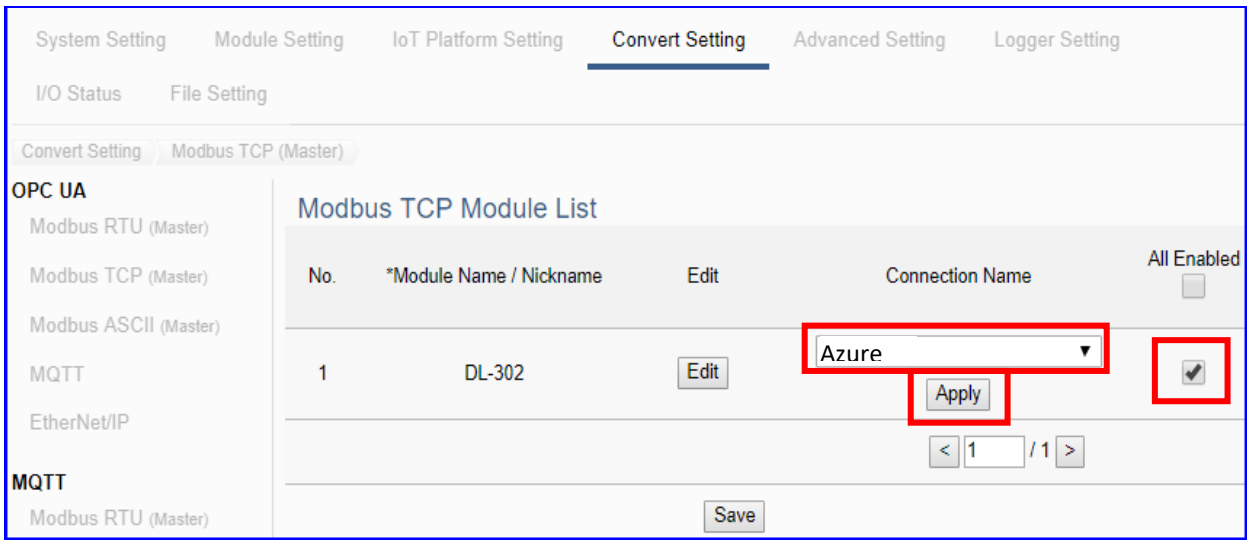
Enter the file name of the Root CA Certificate applied / downloaded from the Microsoft website. It is **attached to this FAQ**.

Step 4. Apply Connection & Enable Converting Module



This step is to apply the connection and enabling the converting module.

① Select the Azure Connection Name and ② Apply it, ③ check the module enabled box.



Step 5. Save Project

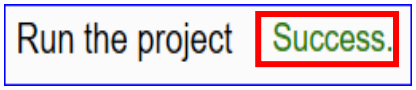
The setting of this example is finished now. Click the next step **[Save Project].**

When the animation vanished, the project is saved completely.

Step 6. Run the Project

This step is to transfer the new project into UA controller, and execute it.

User also can click [**System Setting** > **Controller Service Setting** > **Run Project**] > [**Stop**] & [**Run**] the project.

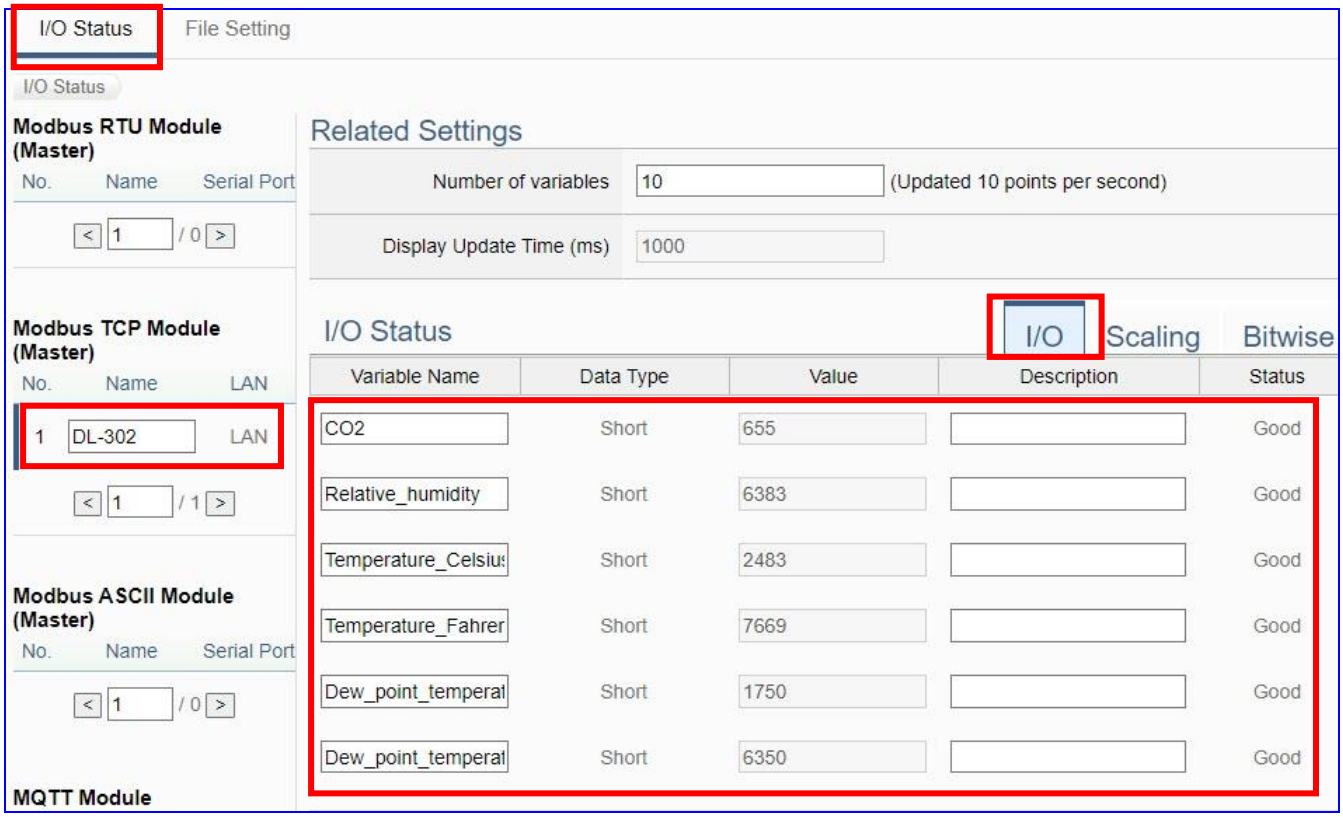


When the words "**Success**" appears, the UA controller is running new project successfully.
Then the **Step Box will disappear** automatically, and back to the first screen view of the Web UI.

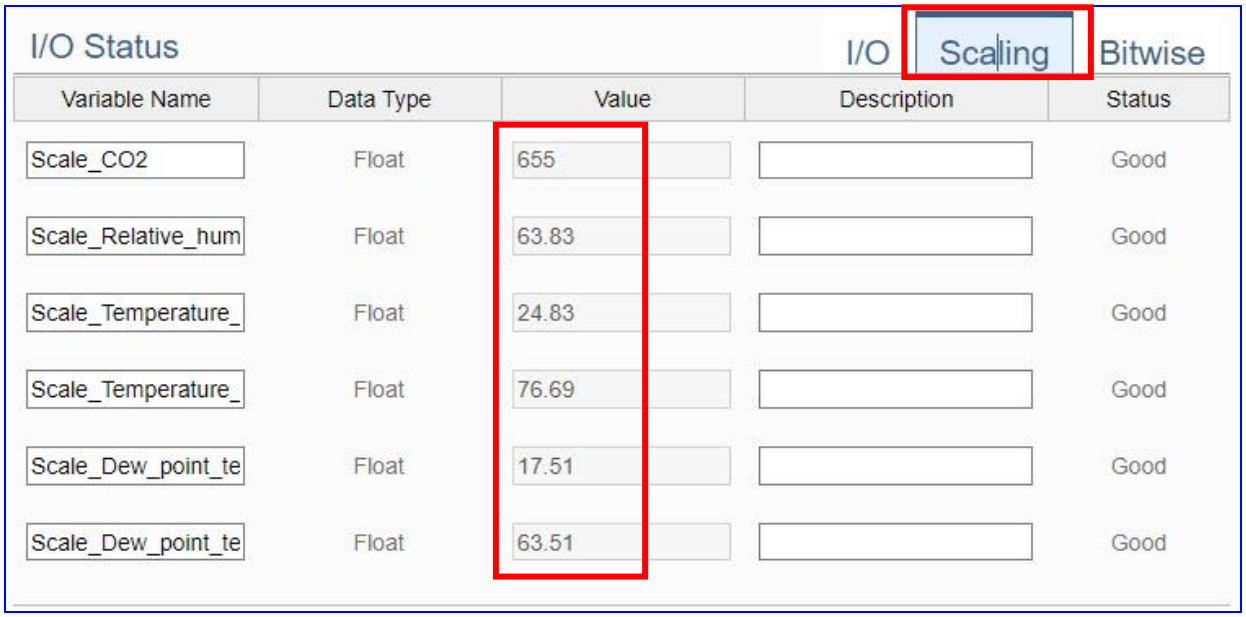
Check I/O Data:

Click the menu **[I/O Status]** > the **module [DL-302]** on the left side to view the real-time I/O status.

[I/O]: Display the I/O status and raw data of DL-302 module.



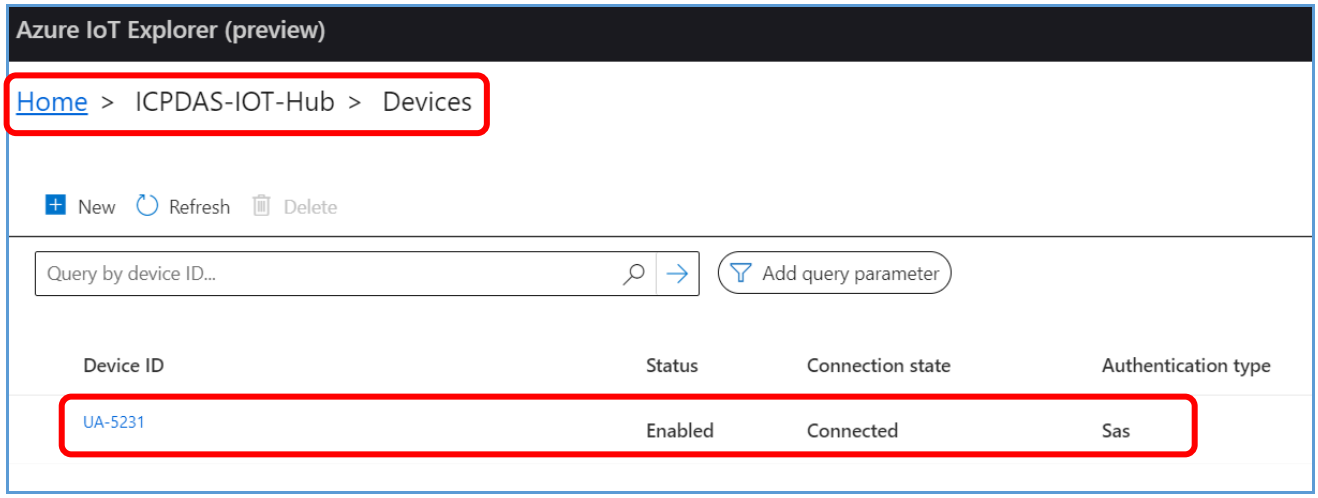
[Scaling]: Displays scaled CO2, relative humidity, Celsius/Fahrenheit temperature and dew point temperature, making the data easier to identify.



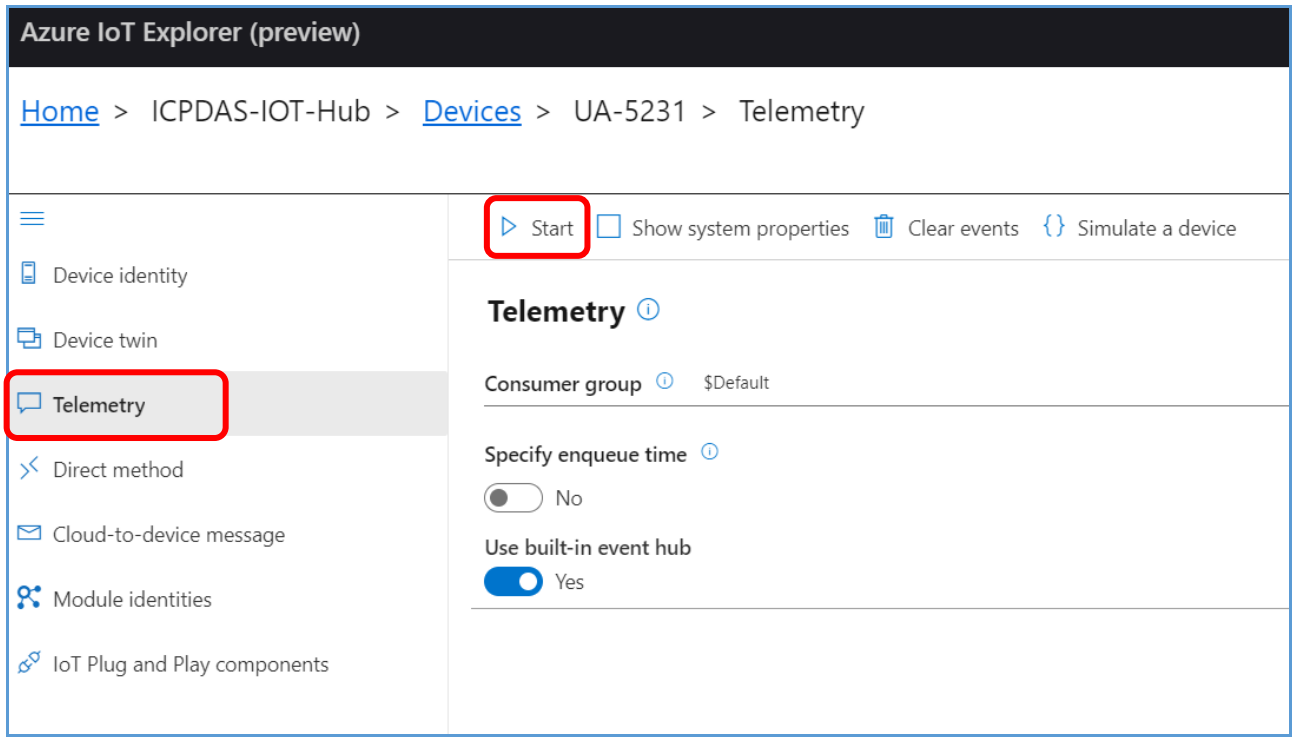
Verify Azure Connection Status

To verify the Azure connection status, you can use the **Azure IoT Explorer** software to test the Azure connection status. For the installation and configuration of Azure IoT Explorer, please refer to steps "C" and "D" of "Azure side Settings" between Steps 2 and 3 of this FAQ.

In the Azure IoT Explorer software, go to 【IoT Hub】>【Devices】, and then click the Device ID to set the connection, for example, Device ID "UA-5231" in this example.



Then click the function item "**Telemetry**" on the left side. And then click "**Start**" on the right side.



After connecting, if the displayed I/O data is correct, as shown in the following I/O point data, it means that the Azure connection status is normal.