IoT Catalyst
Edge Gateway

Table of contents

Preliminary notes

The following document illustrates the Edge Manager application's IoT Catalyst Gateway device configuration procedure.

IoT Catalyst Edge Gateway configuration

Before powering up the system, be sure to:

- have read the datasheet and viewed the schematics
- have inserted the SIM in the gateway and connected all the peripherals of the kit.

When the IoT Catalyst Edge Gateway starts, it activates a hot spot WiFi for management activities. For security reason, if nobody joins the local WiFi network, the hot spot is activated in 5 minutes.

To configure the IoT Catalyst Edge Gateway, connect to it via WiFi using a smartphone, tablet, or PC.

To connect to the IoT Catalyst Edge's hot spot:

- Go to the Wi-Fi configuration section of the device (smartphone, tablet, laptops, etc.)
- Search for the network with an SSID equal to the MAC address of the gateway (MAC address is printed on the label on the back of the IoT Edge Gateway)

The credentials to connect via Wi-Fi with the gateway are:

- Wi-Fi password: fwdedgext001

The gateway configuration through Edge Manager is done using a browser and opening the page that appears at the following address:

- IoT Edge Gateway URL: http://172.24.1.1:9090/

The IoT Catalyst Edge Manager login page will come, where you will be able to log in with the following credentials:

User: catalyst
Password: Fwd0012k18

Alternatively, you can access IoT Catalyst Edge Manager via a wired network, as follows:

- Connect the pc to the gateway using a LAN cable and set the network card of your pc to the same subnet as the gateway.

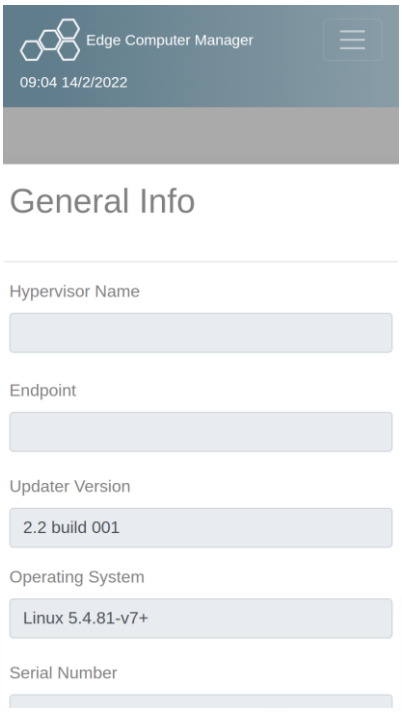
The address set on the gateway's LAN1 port is default 192.168.1.199.

- Access via the following URL: http://192.168.1.199:9090/

If the address of the IoT Catalyst Edge Manager is different, you need to change the URL above, replacing the default address with the actual IP address, as follows:

http:// gateway_ip_address: 9090 /

Once authenticated on the web app, the following page will appear:

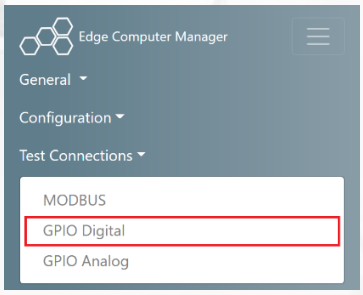


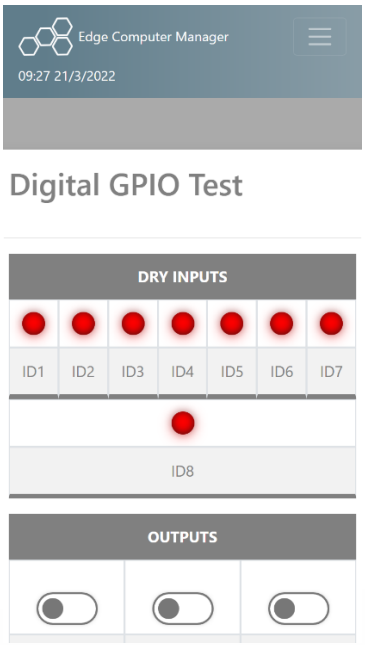
Local test of signals

This section describes how to test the I / O using the Edge Manager application

Digital Signals

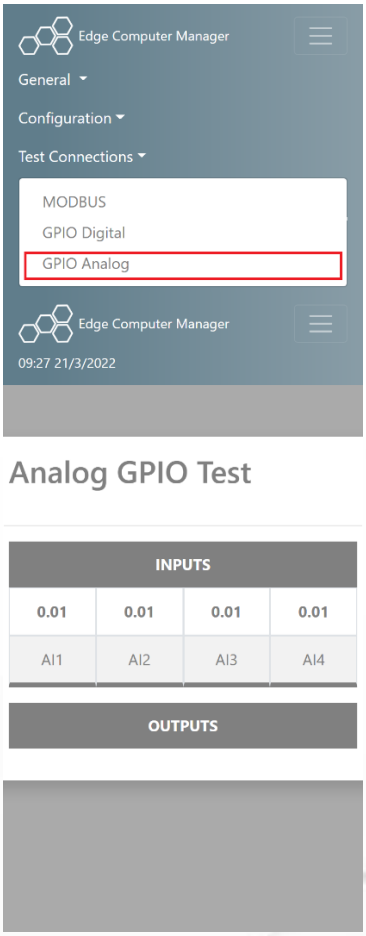
- Click on GPIO Digital menu item to test digital signals.





By changing the status of the input signals, you will have to see the LED turn green, while by changing the status of the output signal, you will have to check the effect of the status change in the field (it depends on what you have connected to the output signal you are testing).

Analog Signals

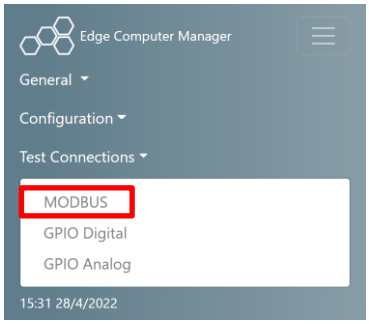


By modifying the state of the collected input signals from connected external sensors/probes, the corresponding values of the analog inputs must vary.

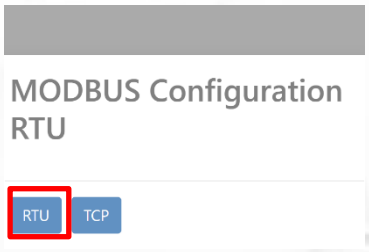
MODBUS

This section shows how to perform a Modbus test through the appropriate area of the Edge Manager.

- Open the Test Connections menu and select MODBUS.



- Choose the Modbus protocol of the device you want to test; unless otherwise indicated, select RTU.



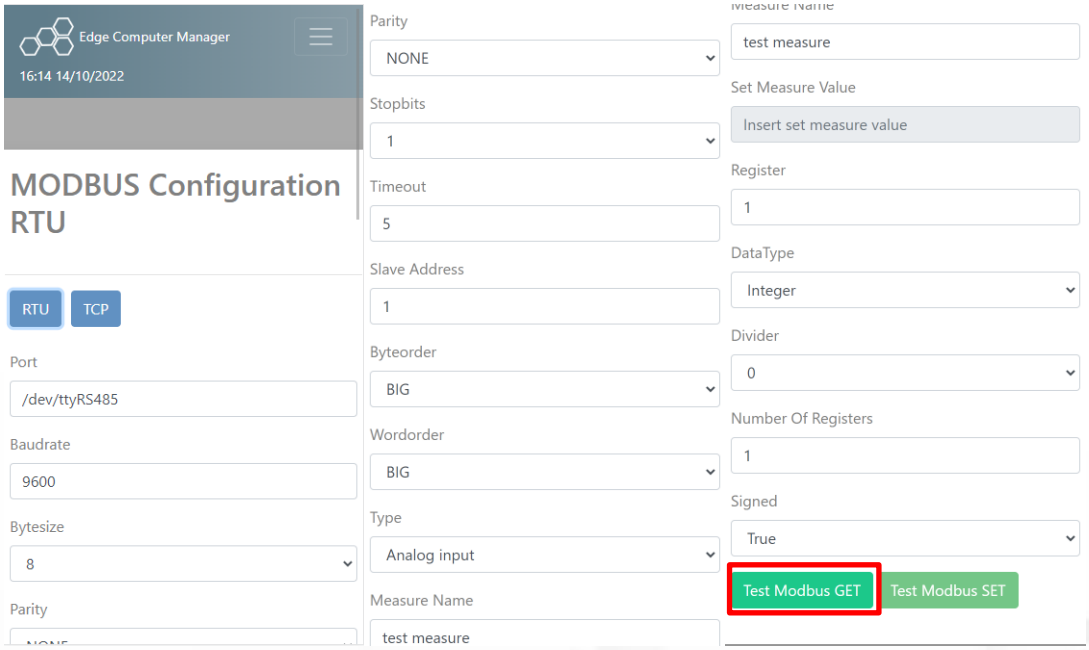
The following example shows how to read the temperature value from a Modbus RS485 temperature/humidity probe.

The Modbus port of the gateway is / dev / ttyRS485
The parameters of the temperature probe used in the example are as follows:

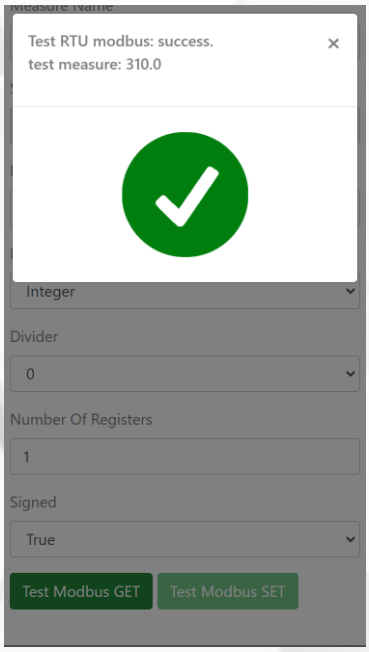
- Probe Modbus configuration (default)
    - Slave Address: 1
    - Baudrate: 9600
    - Bytesize: 8
    - Parity: NONE
    - Stopbits: 1

  Modbus register to be interrogated to read the temperature value
    - Byteorder: BIG
    - Wordorder: BIG
    - Type: Analog Input
    - Register: 1
    - Datatype: Integer

- Divider: 0
- Number of Registers: 1
- Signed: True



Once inserted the parameters in the respective fields, click the "Test Modbus GET" button.
If the connection and communication have been established correctly, you will have a response like the following:



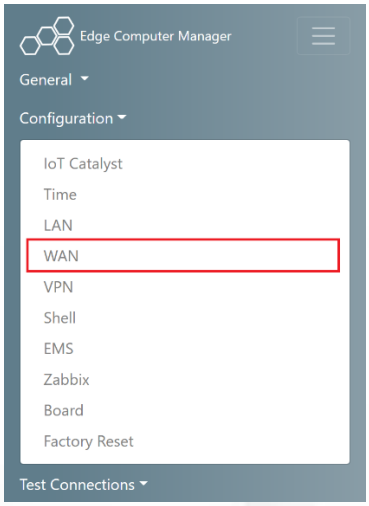
(Temperature is expressed here in tenth of a degree)

IoT Catalyst Edge Configuration

The configuration operations to be carried out are the following in order of execution.

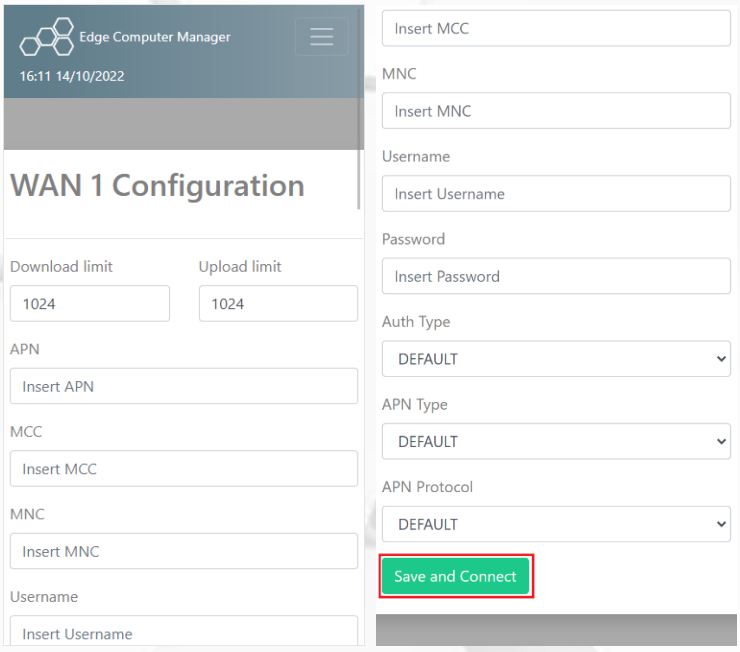
APN configuration

Click on WAN



The following page will appear with the WAN 1 and WAN 2 settings.

Move to the WAN 1 box. In the APN field, enter the APN of the sim used, then click on the Save and Connect button.

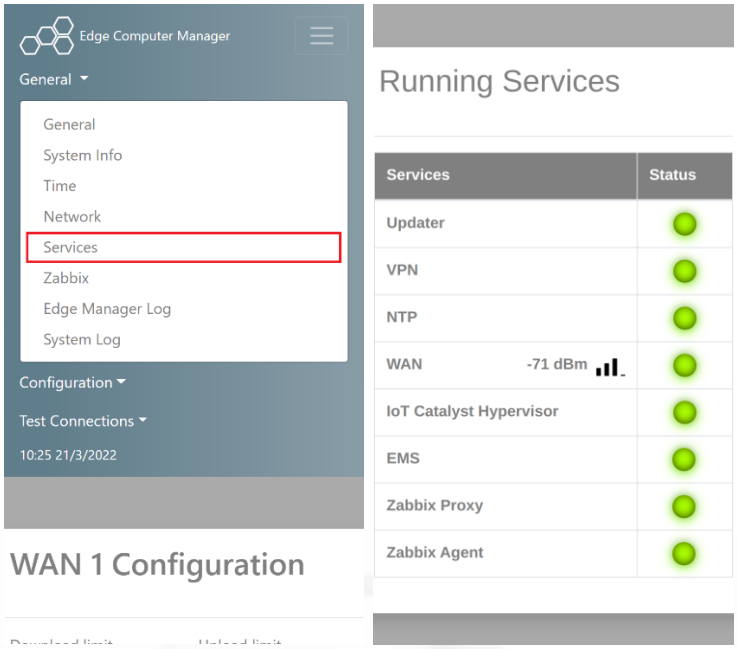


Go to General Services and check that the WAN is active.

Wait a few seconds. If successful, the relative status will have a green dot and the signal

strength indicated.

Please note that sometimes, the signal may not be read, but the system still shows the green dot indicating the connection. To view the actual status of the signal, try reloading the page



The WAN's led must remain steady green; otherwise, please get in touch with the supplier's technical support service.

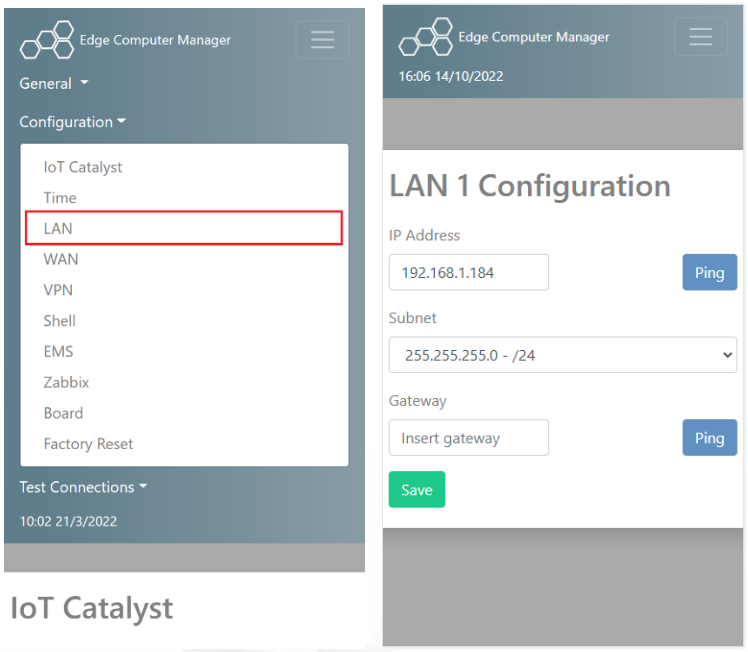
Before activating the WAN, local time could not be in synch (warning triangle next to the time in the navbar); time will align by itself when the connection is active and the NTP service is activated (NTP is active by default).
In this case, you will have to log in again. Just refresh the page to check if you need to log in again.

A triangle next to the time in the navbar, if present, indicates a misalignment between the time of the web client and the gateway.

The gateway time is in UTC, the time of the device used for configuration is usually in UTC + 1 during the solar time period and UTC + 2 during the summertime period.

LAN Configuration

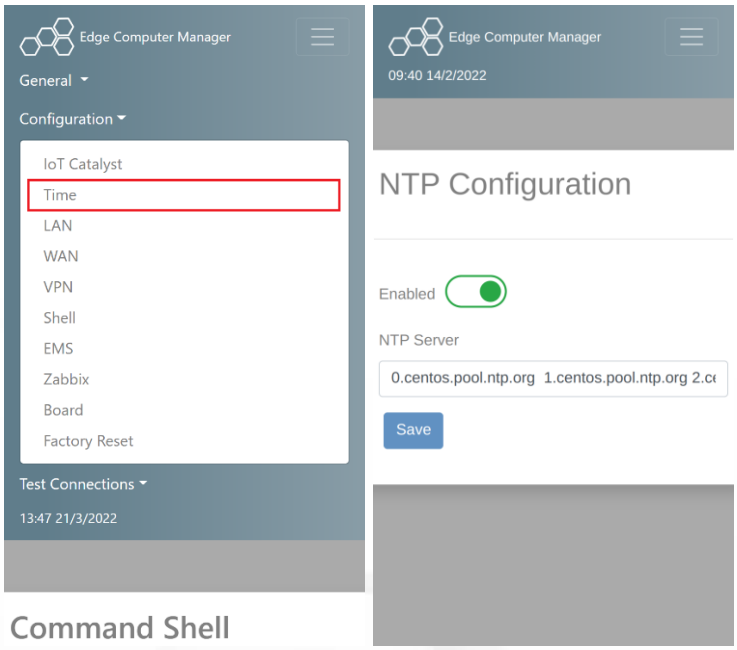
- Click on **LAN**.



- Fill in the IP Address field of the relevant interface with the IP chosen for the IoT Catalyst Edge Gateway
- Leave the Gateway field blank.
- Once edited all the fields, press the **Save** button.

NTP Configuration

The NTP service is active by factory default. Check from the services page that it is active. If it is not happening, open the NTP configuration tab



In the NTP Server field, check the server list entered.

The default list is:

0.centos.pool.ntp.org
1.centos.pool.ntp.org
2.centos.pool.ntp.org
3.centos.pool.ntp.org

In the top navigation bar, there is a datetime, which indicates the system clock. In case of misalignment between the device used to browse the Edge Manager and the IoT Catalyst Edge Gateway, an alarm signal will be displayed that warns the user to set the time or to enable the NTP synchronization service.

You can check that the time is synchronized from the Running Services section.

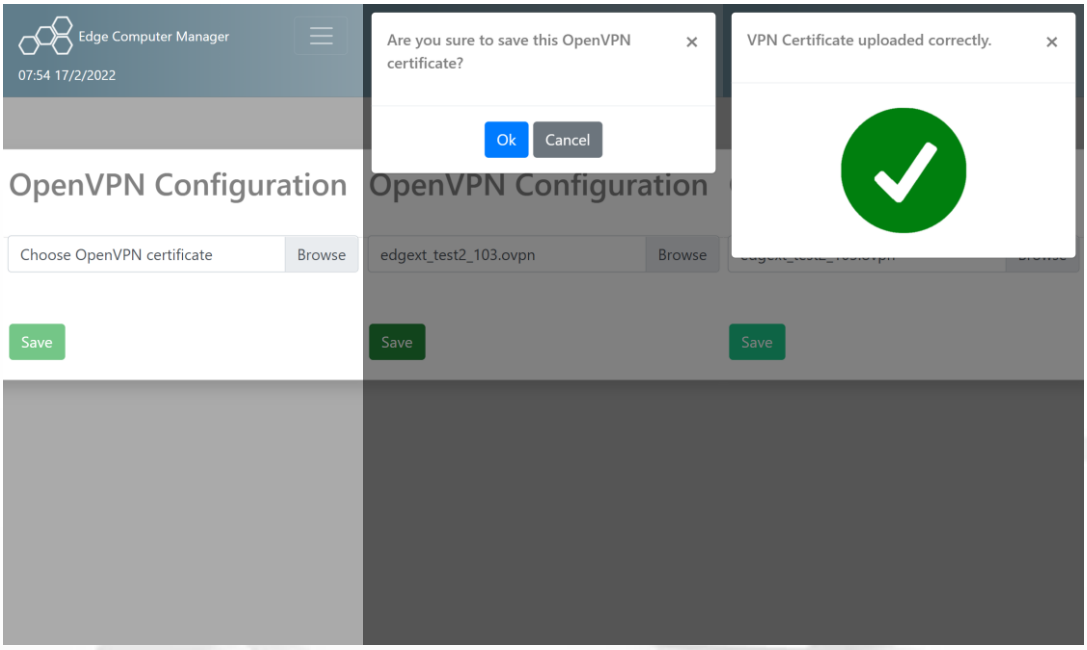
Running Services

Services	Status
Updater	
VPN	
NTP	
WAN -71 dBm	
IoT Catalyst Hypervisor	
EMS	
Zabbix Proxy	
Zabbix Agent	

VPN configuration (optional)

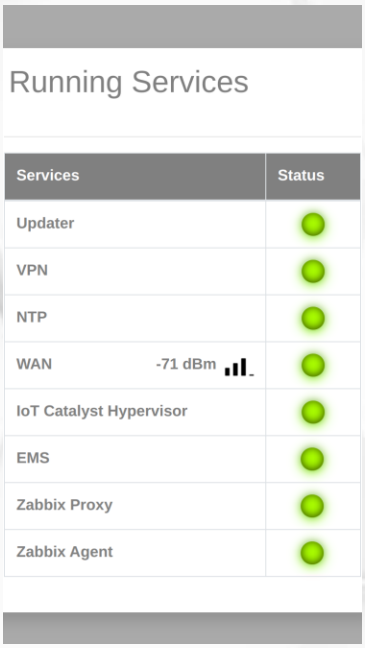
If you want to install a VPN certificate on the Gateway proceed as follows.

- Upload a certificate file: it is possible to upload a certificate file * .ovpn and save it on the system using **Save**. To upload the certificate, use the Browse button to go to the folder of the device (smartphone, tablet, PC) you are using, locate the desired certificate file and select it.



This feature also behaves like the WAN, so it will always take up to five minutes for the service to go live.

To confirm the success of the operation, please check the Running Services section.



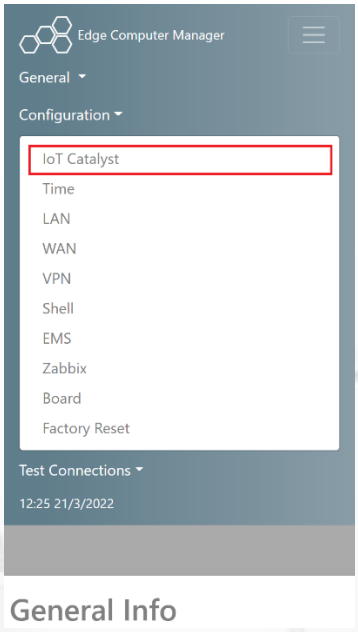
Creation of an IoT Catalyst Hypervisor

The IoT Catalyst Edge Gateway is factory ready to connect to an active instance of IoT Catalyst Studio. The connection is possible after the successful onboarding of the IoT Catalyst Edge Gateway.

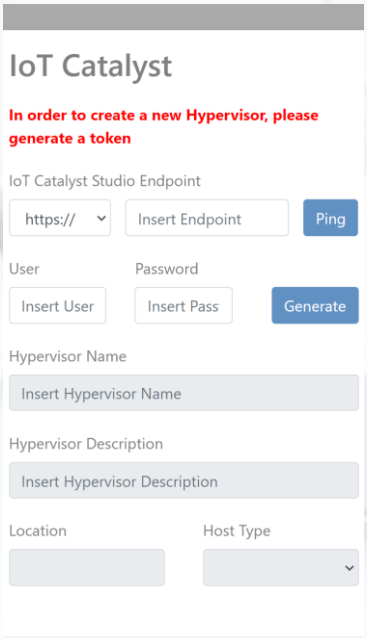
IoT Catalyst is a Low Code/No Code IoT Edge Platform that offers IoT DevOps and IoT Device Management tools to make the IoT simpler, faster and cheaper than it has ever been!. As an IoT Edge Platform, all the business logic is pushed at the edge, and it is managed by a single control plane that works in any web browser: the IoT Catalyst Studio. (https://www.iotcatalyst.com)

To perform the onboarding:

- Click on IoT Catalyst



The following page will appear.

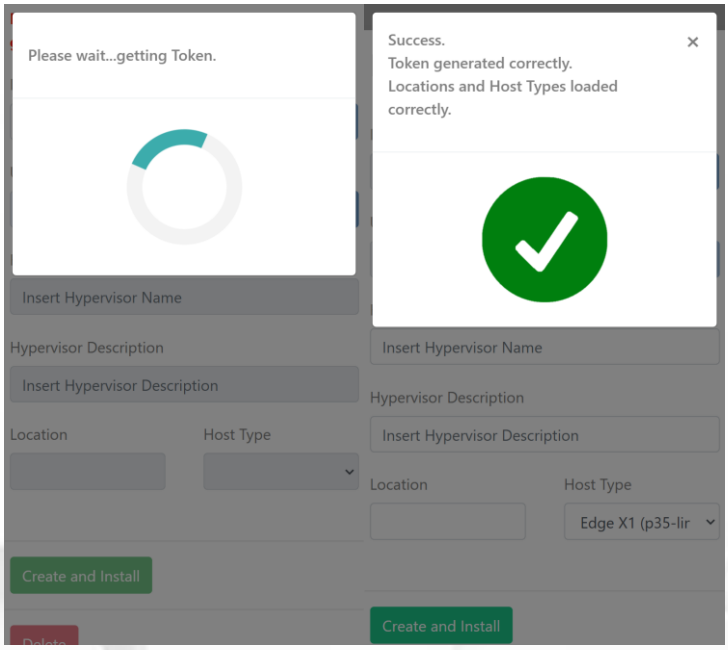


Now, you can create and install an IoT Catalyst Hypervisor on the gateway. This operation requires the request of a valid token issued by an IoT Catalyst Studio instance.

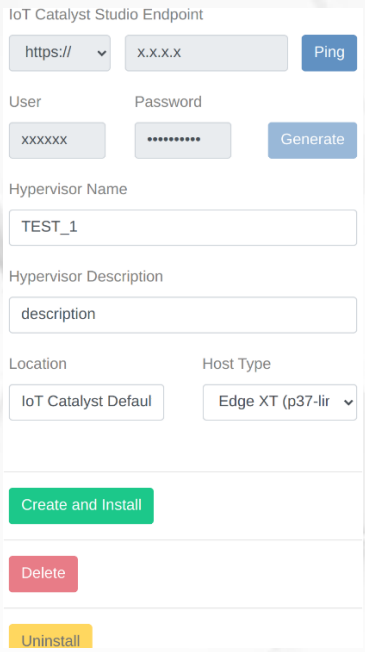
To create the token:

- Select: https: //
- Enter as endpoint: <address of the Catalyst study>
- User: <token creation user>
- Password: <token creation user password>

Then click on **Generate** and wait for the operation to complete

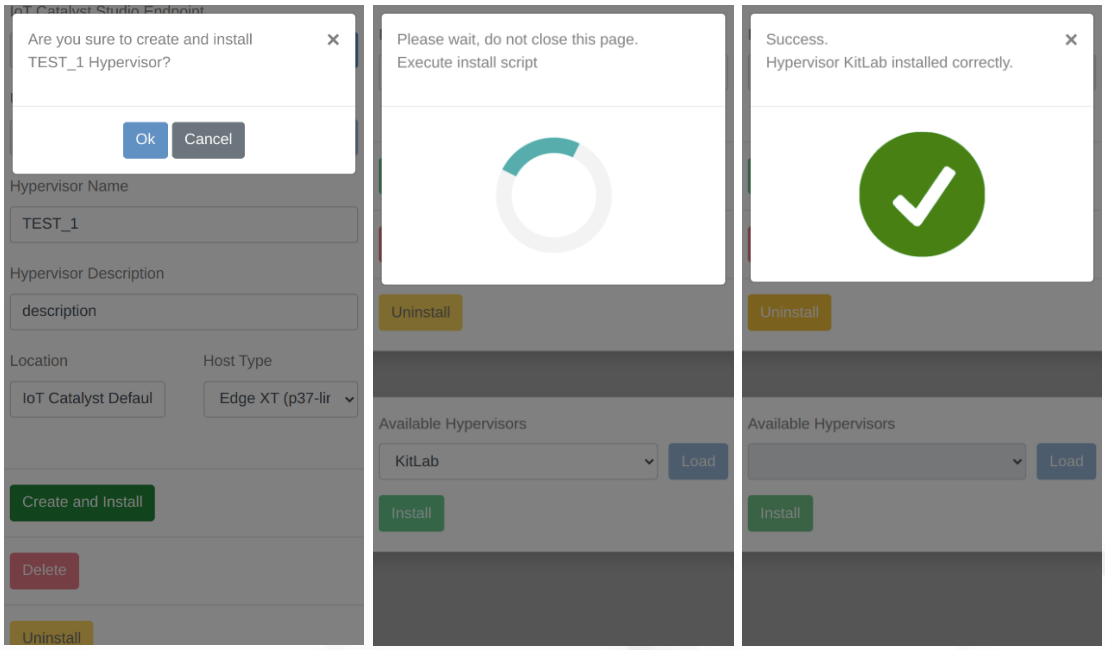


Once a valid token is received, it is possible to create an IoT Catalyst Hypervisor.



- Click the **Create and Install** button and wait for the installation to complete.

Important notice: check that energy saving of the device (PC or smartphone) is disabled to avoid turning off the monitor and the consequent disconnection from the gateway. The disconnection would cause the loss of information on the progress of the installation.

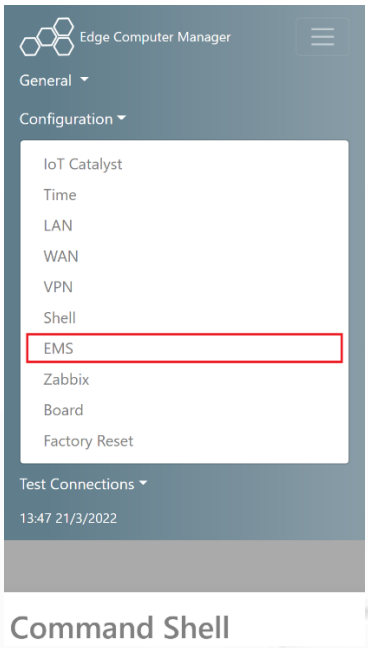


PTC ThingWorx EMS configuration

IoT Catalyst Edge Gateway can communicate natively with the edge service of PTC ThingWorx - The Edge Micro Server (from now on EMS). Some of the features described in this paragraph require an appropriate preliminary configuration of the PTC ThingWorx instance, as installing specific components to release keys and certificates is necessary.

The related service can be enabled and set via the EMS form if the above is satisfied.

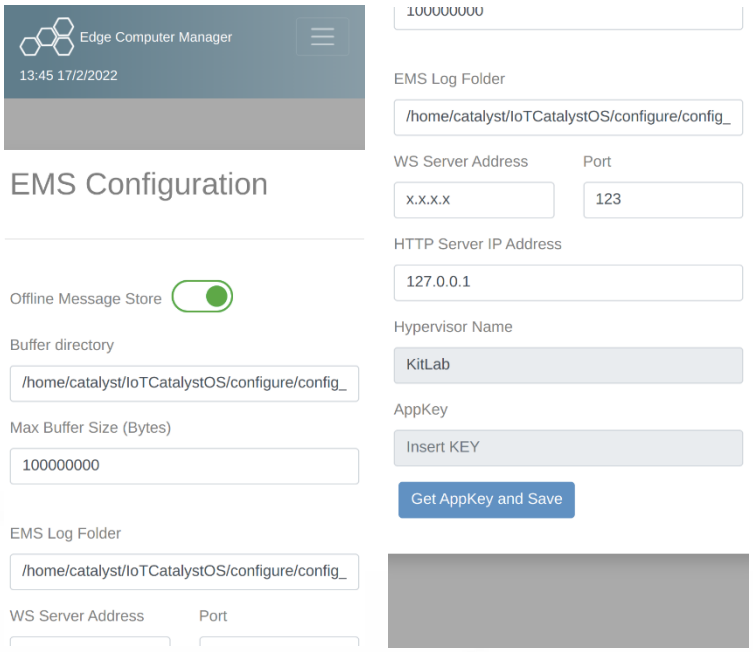
To configure the EMS, you need to navigate -> Configuration -> EMS



Configure the service as follows.

- Enable Offline Message Store (the flag will turn green) (default is enabled)
- Enter the values in the WS Server Address and Port fields and leave the others with the default values.

Setting	Value
WS Server Address	<IP EMS server>
Port	<EMS server port>
Buffer directory	/home/catalyst/IoTCatalystOS/configure/config_files/ems/offline
Max Buffer Size	100000000
EMS Log Folder	/home/catalyst/IoTCatalystOS/configure/config_files/ems/logs/
HTTP Server IP Address	127.0.0.1



- Click on Get AppKey and Save

Appendix

Modbus RTU RS485 parameters

Setting	Value
Baud rate	<IP EMS server>
Byte size	<EMS server port>
Parity	/home/catalyst/IoTCatalystOS/configure/config_files/ems/offline
Stop bits	100000000

Environmental protection

This marking on the product, accessories or literature indicates that the product and its electronic accessories should not be disposed of with other household waste. To prevent possible harm to the environment please separate these items from other types of waste and recycle them responsibly to promote the sustainable reuse of material resources.