

**iO | GATEWAY**  
**USER MANUAL**

**Document Name:** UM\_iO Gateway\_1.3

**Issue:** 3.1

**Date (MM/DD/YYYY):** 01/04/2021

**PROPRIETARY INFORMATION**

The information contained in this document is the property of **MULTITEL INC.** Except as specifically authorized in writing by **MULTITEL INC.**, the holder of this document shall:

1. Keep all information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to all third parties and;

## CONTROL SHEET

Issue	Date MM/DD/YYYY	Description	Revised by
1	06/06/2020	iO Gateway v1.0, v1.1	S.Boivin
2	12/02/2020	iO Gateway v1.2	S.Boivin
3	12/08/2020	iO Gateway v1.3	S. Boivin
3.1	01/04/2021	Security access level adjusted	L. Methot

## TABLE OF CONTENTS

<b>CONTROL SHEET .....</b>	<b>3</b>
<b>TABLE OF CONTENTS .....</b>	<b>4</b>
<b>FIGURES.....</b>	<b>7</b>
<b>TABLES.....</b>	<b>8</b>
<b>CUSTOMER SERVICE CONTACT .....</b>	<b>9</b>
<b>Repair Request.....</b>	<b>9</b>
<b>1. FIRST TIME CONNECTION.....</b>	<b>10</b>
<b>1.1 ETHERNET CONNECTION .....</b>	<b>10</b>
<b>1.2 FIRST TIME LOGIN.....</b>	<b>12</b>
<b>1.3 INITIAL CONNECTIONS.....</b>	<b>13</b>
1.3.1 Ethernet Connection .....	13
1.3.1.1 Configuring WAN iO Device and Network .....	13
1.3.1.2 Configuring LAN iO device and equipment.....	14
1.3.2 RS-485 Connection.....	15
<b>2. SETTINGS.....</b>	<b>17</b>
<b>2.1 GENERAL PARAMETERS.....</b>	<b>17</b>
2.1.1 Site Information .....	17
2.1.2 System Information .....	17
2.1.2.1 System Resources.....	17
2.1.2.2 Power Input .....	17
2.1.2.3 About.....	17
2.1.3 Date and Time.....	18
2.1.3.1 Date and Time .....	18
2.1.3.2 Date and Time Format.....	19
<b>2.2 SECURITY .....</b>	<b>19</b>
<b>2.3 CONNECTIONS.....</b>	<b>20</b>
2.3.1 Ethernet ports .....	20
2.3.2 RS-485 Ports.....	21
<b>2.4 PROTOCOLS.....</b>	<b>21</b>
2.4.1 HTTP/HTTPS .....	21
2.4.2 SNMP Agent.....	21
2.4.3 PING.....	21

2.4.4	Modbus Slave.....	21
<b>2.5</b>	<b>CATEGORIES AND MODELS.....</b>	<b>22</b>
2.5.1	Category.....	22
2.5.2	Model.....	22
<b>2.6</b>	<b>SYSTEM MAINTENANCE.....</b>	<b>23</b>
2.6.1	Configuration File.....	23
2.6.2	Software Update.....	24
2.7.3	Reset Factory.....	24
<b>2.8</b>	<b>LABELS.....</b>	<b>24</b>
<b>2.9</b>	<b>REBOOT.....</b>	<b>25</b>
<b>3.</b>	<b>DATA SOURCE.....</b>	<b>26</b>
<b>3.1</b>	<b>iO DEVICE MONITORING CAPABILITIES.....</b>	<b>26</b>
<b>3.2</b>	<b>GATEWAY MODE.....</b>	<b>26</b>
3.2.1	Standard Mode.....	26
3.2.2	Transparent Mode.....	26
<b>3.3</b>	<b>IO MONITORING ARCHITECTURE.....</b>	<b>27</b>
3.3.1.	Equipment creation.....	27
3.3.1.1.	Communication Protocol: Modbus TCP/IP - Client   Standard mode.....	28
3.3.1.2.	Communication Protocol: Modbus TCP/IP - Client   Transparent mode.....	29
3.3.1.3.	Communication Protocol: Modbus RTU - Master.....	29
3.3.1.4.	Communication Protocol: SNMP Get V1/V2C.....	29
3.3.2.	Data points creation.....	30
3.3.2.1.	Modbus TCP/IP – Standard mode.....	30
3.3.2.2.	Data Points – Modbus TCP/IP – Transparent Mode.....	32
3.3.2.3.	Data Points - SNMP Get v1/v2C/v3.....	33
3.3.3.	Network Management Software.....	35
3.3.3.1.	SNMP Get.....	35
<b>4.</b>	<b>PASSTHROUGH.....</b>	<b>36</b>
<b>4.1</b>	<b>PASSTHROUGH OVERVIEW.....</b>	<b>36</b>
4.1.3.	Fields Description.....	37
4.1.1.1	Protocol Options (mandatory).....	37
4.1.1.2	Source Port Options (mandatory).....	37
4.1.1.3	Destination IP (mandatory).....	37
4.1.1.4	Destination Port (mandatory).....	38

4.1.1.5	Additional Port.....	38
4.1.1.6	Transport Protocol (mandatory).....	38
4.1.1.7	Action.....	39
4.1.1.8	Status .....	39
4.1.1.9	Web Access .....	39
<b>4.2</b>	<b>PASSTHROUGH CONFIGURATION .....</b>	<b>39</b>

## **FIGURES**

Figure 1 – First Time Connection .....	10
Figure 2 – Changing IPv4 Properties on PC .....	11
Figure 3 – IP Address in Web Browser .....	11
Figure 4 – First Time Login .....	12
Figure 5– iO Device LAN/WAN Connection .....	13
Figure 6 – LAN Connection.....	14
Figure 7 – iO Device Network and Serial Connections.....	15
Figure 8 – Settings .....	17
Figure 9 –iO Monitoring Architecture .....	27
Figure 10 – Step 1.....	27
Figure 11– Standard Mode .....	28
Figure 12 –Transparent Mode .....	29
Figure 13 – SNMP GET .....	30
Figure 14– iO Modbus Register – Modbus TCP/IP Transparent .....	32
Figure 15 – iO Gateway mapped to the Network Management Software.....	35
Figure 16– Passthrough Topology.....	36

## TABLES

---

Table 1 -Maximum Distances .....	10
Table 2 – Supported Web Browsers .....	11
Table 3– Factory Credentials .....	12
Table 4 –Access level according to the module .....	19
Table 5 – Protocol description .....	37
Table 6 –Source Port specifications .....	37



## CUSTOMER SERVICE CONTACT

---

Customer Service, Technical Support, Product Repair and Return, and Warranty Service.

For customers in Canada and United States please call 1-888-685-8483 (418-847-2255). This number is staffed from 8:30 am to 5:00 pm Eastern Time (zone 5) Monday through Friday on normal business days.

Services provided include: initiating the spare parts procurement process, ordering documents, product warranty administration and providing other product and service information.

### REPAIR REQUEST

All Multitel equipment is covered by a 24-month warranty.

Please contact us before returning material as a Return Material Authorization is mandatory for product repair. Repair, shipping and handling fees are applicable for repairs no longer under warranty. Administrative fees may apply on equipment returned to Multitel for repair, upon which no trouble was found (NTF).

For a return, send your request at [rma@multitel.com](mailto:rma@multitel.com).

# 1. FIRST TIME CONNECTION

## 1.1 ETHERNET CONNECTION

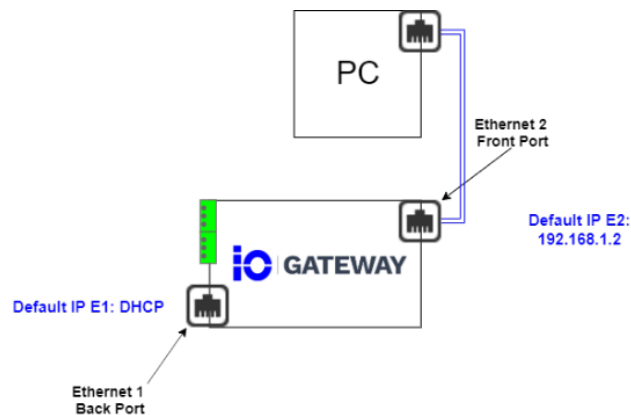
iO Gateway interfaces need to be accessed in a web browser. iO Gateway can either be accessed by the front or the back Ethernet port. However, for the first connection, the front Ethernet port needs to be used because the backport doesn't have a static IP address (DHCP). The following table shows the factory settings for both Ethernet ports.

Table 1 -Maximum Distances

Ethernet Ports	Mode	IPv4 Address
Ethernet 1 - Back	DHCP	N/A
Ethernet 2 - Front	Static	192.168.1.2

A local area network (LAN) needs to be configured between the iO Gateway Ethernet front port and the user's PC.

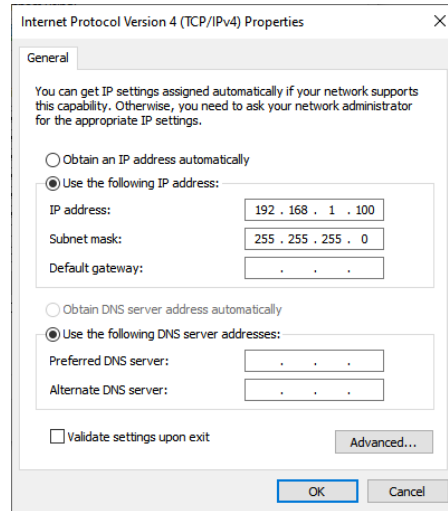
Figure 1 – First Time Connection



To create a LAN between a PC and the iO Gateway. The user needs to change the ethernet port adapter properties. This can be done by on a Windows machine by:

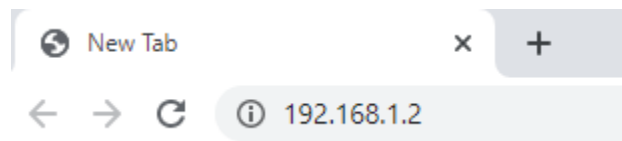
1. Going to control panel
2. Change adapters settings
3. Click on the desired ethernet port
4. Click on properties
5. Click on Internet Protocol Version 4 (TCP/IPv4)
6. Click on properties
7. Change the IP address and subnet mask (ex. 192.168.1.100 & 255.255.255.0).

**Figure 2 –Changing IPv4 Properties on PC**



Once the LAN is configured the user needs to input the default IP address (192.168.1.2) in the address bar of a web browser.

**Figure 3 – IP Address in Web Browser**



Please note that iO Gateway is using a web server version that has been released in 2019 that doesn't support legacy web browsers. Below is a table that shows which web browsers are supported by iO Gateway.

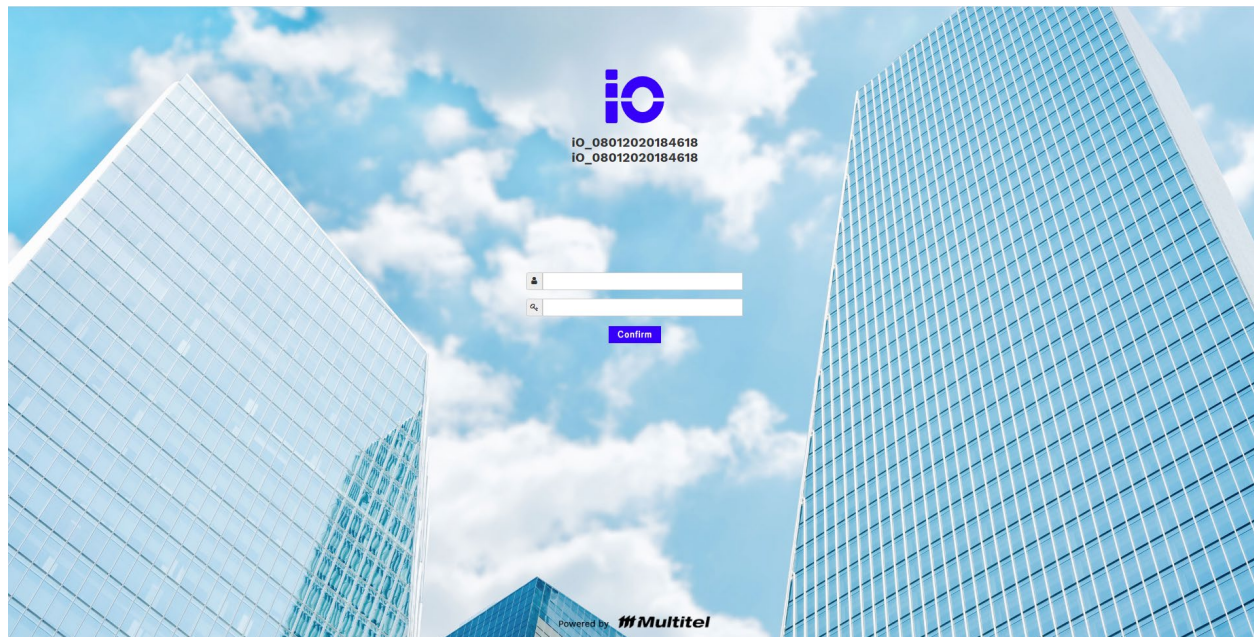
**Table 2 – Supported Web Browsers**

<b>Web Browsers</b>
Chrome
Firefox
EDGE

## 1.2 FIRST TIME LOGIN

Once the default IP address is entered in the address bar and the LAN configuration has been properly done the user will access iO Gateway Login Page.

Figure 4 – First Time Login



The factory credentials are the following:

Table 3– Factory Credentials

	<b>Username</b>	<b>Password</b>
Administrator	Username	administrator
	Password	admin
User	Username	user
	Password	user
Viewer	Username	viewer
	Password	viewer

## 1.3 INITIAL CONNECTIONS

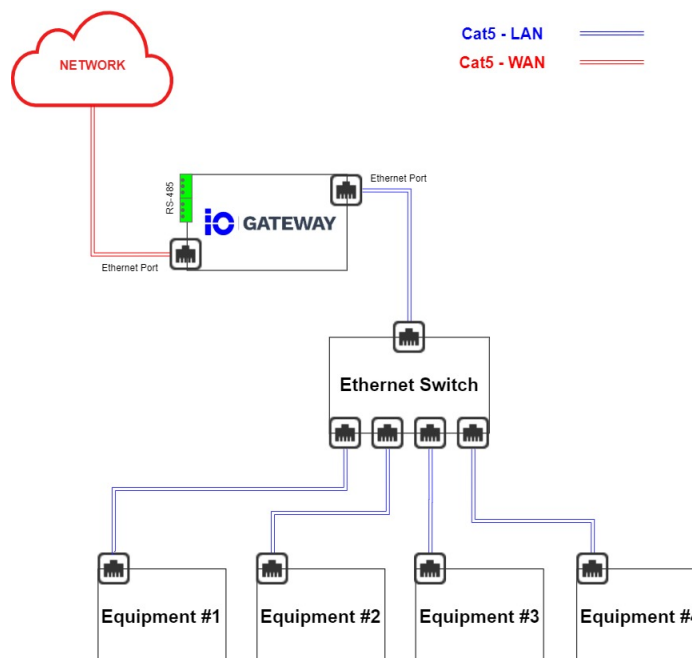
### 1.3.1 ETHERNET CONNECTION

#### 1.3.1.1 Configuring WAN iO Device and Network

The first step consists of configuring the WAN connection between the iO device and the user's network. The user will, therefore, be able to access the iO device web interfaces remotely. The user should get the WAN IP from their IT management team. The WAN will be configured on the back ethernet port which the reader is currently not using. Modifications to the ethernet backport can be done directly on the user's PC.

1. Click on *Settings*
2. Click on *Connections*
3. Click on *Ethernet 1 – Back* tab
4. Keep MTU at 1500 unless specified otherwise by your network administrator.
5. Keep Speed at Auto unless specified otherwise by your network administrator.
6. Click on Mode to change from DHCP to Static.
7. Change IPv4 Address, IPv4 Subnet Mask, and IPv4 Gateway.
8. Click on *Save*
9. Reboot the device

Figure 5– iO Device LAN/WAN Connection

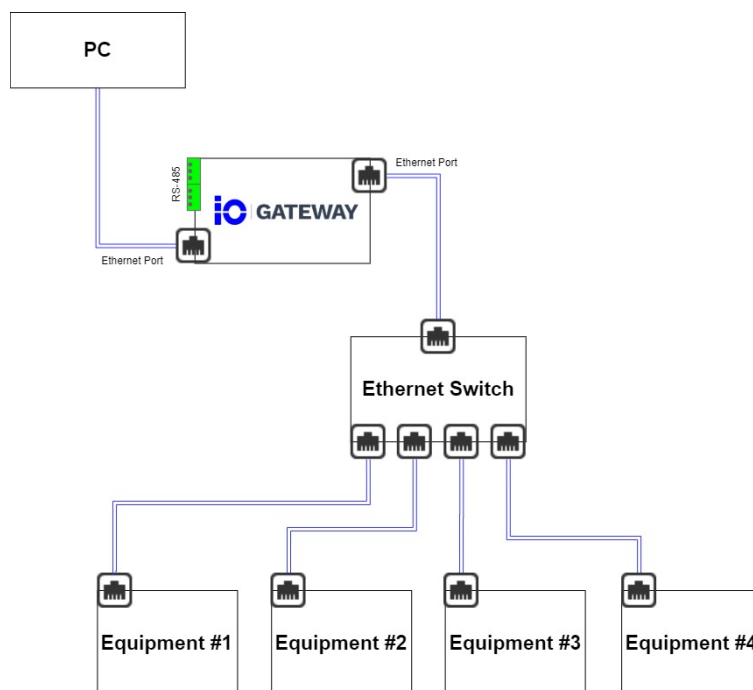


### 1.3.1.2 Configuring LAN iO device and equipment

To connect the iO Gateway to other devices, a new LAN needs to be configured. The iO device is going to use this LAN to monitor the desired pieces of equipment. If the iO device is only intended to monitor a single piece of equipment, the user can create a simple LAN between the iO and the single equipment. In most cases multiple pieces of equipment will be monitored at the same time. In that case, an or several unmanaged ethernet switches will be required. When dealing with multiple equipments, the user needs to make sure that each equipment IP is configured to be on the same network.

In this example, 4x pieces of equipment need to be monitored. A 5-ports unmanaged ethernet switch is selected to create the LAN between the equipment and the iO Gateway. IPs from the equipment are configured on the 10.10.10.X network.

Figure 6 –LAN Connection



A Cat-5 cable will need to be used between the iO Gateway back ethernet port and the unmanaged switch to complete the LAN.

1. Click on *Settings*
2. Click on *Connections*
3. *Ethernet 1 – Front* tab
4. Enabled the port
5. Keep MTU at 1500 unless specified otherwise by your network administrator.

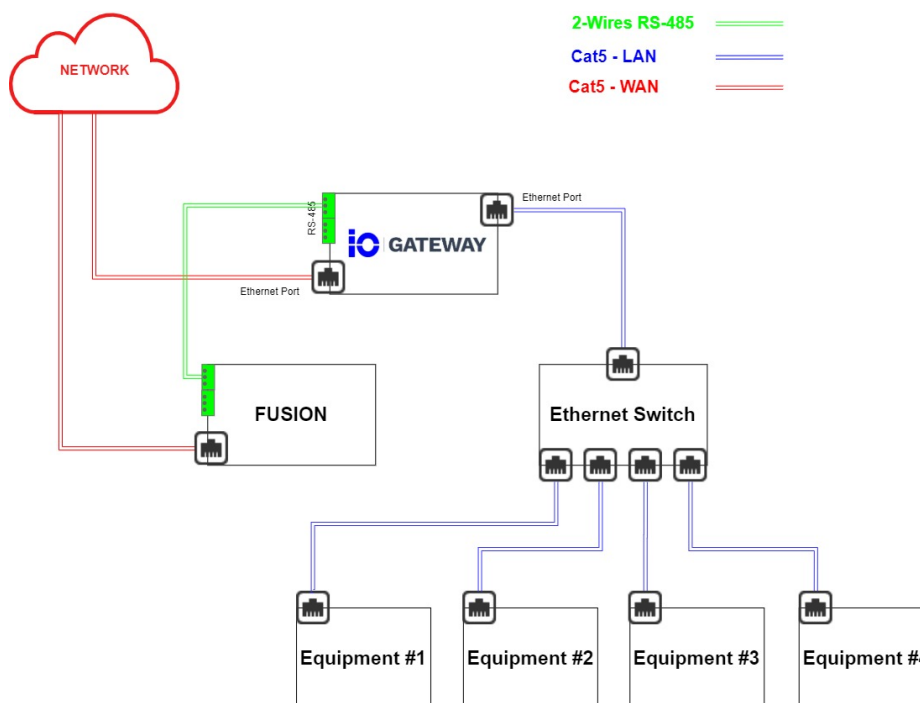
6. Keep Speed at Auto unless specified otherwise by your network administrator.
7. Click on Mode to change from DHCP to Static.
8. Enter IPv4 Address, IPv4 Subnet Mask, and IPv4 Gateway. Make sure that every piece of equipment that you wish to connect to the iO device will be configured to the same IP network.
9. Click on *Save*
10. Reboot the iO Gateway (the reboot button will appear in the header)

Once the iO Gateway is rebooted, the iO Gateway/Equipment LAN will be configured.

### 1.3.2 RS-485 CONNECTION

The iO device can now reach equipment on the LAN. A serial-based connection can also be configured between the iO device and other devices such as a Remote Telemetry Unit (i.e. RTU). Multitel recommends the use of its own RTU called FUSION.

Figure 7 – iO Device Network and Serial Connections



1. Click on *Settings*
2. Click on *Connections*

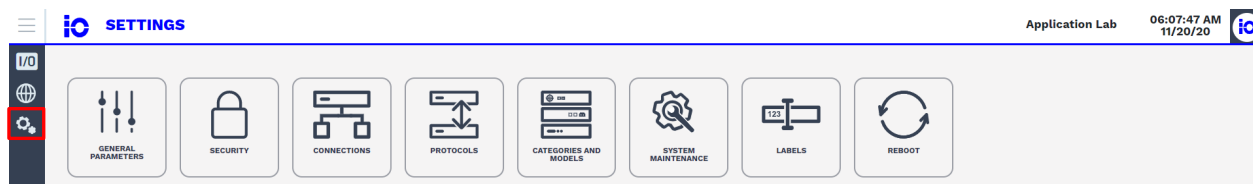
3. Click on *RS-485 – COM A* tab
4. Protocol: Modbus RTU
5. Adjust the Baudrate to the Baudrate of the RTU.
6. Adjust Data Bits to the Data Bits of the RTU.
7. Adjust Stop Bits to the Stop Bits of the RTU.
8. Adjust Parity to the Parity of the RTU.
9. Click on *Save*



## 2. SETTINGS

iO Gateway Settings module can be accessed by clicking on the settings module.

Figure 8 – Settings



### 2.1 GENERAL PARAMETERS

#### 2.1.1 SITE INFORMATION

To configure the site information:

1. Click on *General Parameter – Site Information*
2. Enter Site Name and CLLI number in General Information
3. Enter location information
4. Click on the *Save*

The site name will be displayed in the header for the next login. The site name and CLLI number will be displayed on the Login Page too.

#### 2.1.2 SYSTEM INFORMATION

System information is accessible by clicking on *General Parameters – System Information*

##### 2.1.2.1 System Resources

System resources give an overview of the current CPU load, memory load, and Disk space of the device.

##### 2.1.2.2 Power Input

Power Input gives an overview of the Feed A and Feed B status.

##### 2.1.2.3 About

About section covers several components of the iO device:

- Serial Number
- Model Number
- Batch Number
- Hardware Version

- Software Version
- Mac 1
- Memory Max
- Trending Data Point
- Disk Max
- Mac 0

### 2.1.3 DATE AND TIME

Data and Time can be configured in *General Parameters – Data and Time*.

Date and Time section is used to set the time and date of the iO Gateway. Date and Time will be used for the time-stamping of data therefore, careful considerations need to be taken when configuring the Date and Time.

---

#### IMPORTANT NOTE:

Date and Time will be used for the time-stamping of data therefore, careful considerations need to be taken when configuring the Date and Time. Erroneous Date and Time configuration will impact the data point logging and trends.

---

#### 2.1.3.1 Date and Time

Date and time can be set automatically using NTP Servers or manually.

To set date and time manually

1. Open the setting module
2. Click on General Parameters – Date and Time
3. Choose a time zone (the date and the time will automatically be adjusted according to the time zone selected)
4. If needed, change the time and the date
5. Click on Save

---

#### IMPORTANT NOTE:

iO device doesn't have an internal battery. Manually Date and Time configuration are going to be lost or delayed if any loss of power occurs.

---

To set date and time automatically

1. Click on *Settings* module
2. Click on *General Parameters – Date and Time*
3. Enabled the automatic section
4. Enter a primary NTP Server
5. If needed, enter a second and tertiary NTP Server
6. Click on Save

### 2.1.3.2 Date and Time Format

Date format and time format can be changed in this section.

## 2.2 SECURITY

User and access levels can be view and configured in the **Security** section.

Multitel recommends changing the factory password of the 3 default users to secure access to the iO device. The new password should be at least 8 characters long and include letters (both upper and lower case), digits, and symbols.

Table 4 –Access level according to the module

Modules	Groups	Access level
Settings	Supervisor	Edit
	User	Read-only access *User can reboot the iO device
	Viewer	Access to General Parameters and Labels section (read-only access)
Data Sources	Supervisor	Edit
	User	Edit
	Viewer	Read-only access
Passthrough	Supervisor	Edit
	User	Edit
	Viewer	Read-only access

### **IMPORTANT NOTE:**

Administrator user cannot be deleted or disabled.

To reset a password:

Supervisor user can reset password of all user. Users with user and viewer access level can only reset their own password in the profile page.

1. Enter a new password

2. Click on *Save*

The supervisor user who reset a password to another user must manually send his new credentials by email.

To enable/disable a user:

Disabled a user takes off his access to the iO Gateway interface.

1. Click on the switch in the state column

Blue switch means the user enables  – White switch means the user is disabled 

To delete a user:

1. Select the user needed to be deleted
2. Click on *delete* and *confirm*

## 2.3 CONNECTIONS

The connections section can be accessed in **Settings – Connections**.

---

### **NOTE**

This section required an understanding of network management and serial-based protocols. This user manual will not provide a complete step-by-step process of network and serial communication but is assuming that the reader is educated in both subjects.

---

#### 2.3.1 ETHERNET PORTS

Ethernet ports configuration can be modified in the **Connections – Ethernet 1** and **Connections – Ethernet 2** sections.

Following fields can be configured:

- MTU
- Speed (Auto, 10Mbps, 100Mbps, and 1Gbs)
- Mode (Static, DHCP)
- IPv4 Address
- IPv4 Subnet Mask
- IPv4 Gateway Default Address

A DNS configuration can also be made by providing DNS server addresses.

### 2.3.2 RS-485 PORTS

RS-485 ports configuration can be modified in the **Connections – RS-485 – COM A** and **Connections – RS-485 – COM B** sections.

A single serial protocol can be configured on each RS-485 port.

Following fields can be configured:

- Protocol (None, Modbus RTU – Master, Modbus RTU – Slave)
- Baudrate
- Data Bits
- Stop Bits
- Parity

## 2.4 PROTOCOLS

The protocols section can be accessed in **Settings – Protocols**

### 2.4.1 HTTP/HTTPS

It is not recommended to use HTTP and HTTPS at the same time. Both are however enabled as factory settings. One of the two web protocols should be disabled.

### 2.4.2 SNMP AGENT

This section is used to configure the SNMP Agent of the iO device. The SNMP Agent can be used by FIRM Suite/Enterprise Software to gather data from the iO device.

To configure the SNMP Agent

1. Click on *Settings*
2. Click on *Protocols - SNMP Agent* tab
3. Enter a Port Number
4. Enabled the SNMP v1/v2c Agent or v3
5. Enter a Read Community Name
6. Click on *Save*

### 2.4.3 PING

This section is used to enable or disable the iO device PING.

### 2.4.4 MODBUS SLAVE

The Modbus section is used to configure the Modbus RTU Slave ID. This Slave ID is going to be used by the FUSION/RTU to monitor the iO Gateway.

Configuring the Modbus Slave ID:

1. Click on *Settings*
2. Click on *Protocols - Modbus Slave* tab
3. Click on Enable
4. Enter the Slave ID.
5. Click on *Save*

## 2.5 CATEGORIES AND MODELS

Categories and models are used during the equipment creation. This section will cover how categories and models can be created. It can be accessed by clicking on **Settings – Categories and Models**.

### 2.5.1 CATEGORY

To create a new category:

1. Click on *Settings*
2. Click on *Categories and Models*
3. Click on + Category
4. Enter a Category Name
5. Enter a Note
6. Click on *Save*

To edit a category:

Click on the edit icon  of the category.

To delete a category:

Click on the delete icon  of the category.

Deleted a category containing models removes all associated models. The category or model associated with equipment cannot be deleted.

### 2.5.2 MODEL

To create a new model:

1. Click on *Settings*
2. Click on *Categories and Models*

3. Click on + Model
4. Enter a Model Name
5. Enter a Manufacturer
6. Assign the model to a category
7. Click on *Save*

To edit a model:

Click on the edit icon  of the model.

To delete a model:

1. Select a model
2. Click on *Delete*
3. Confirm the deletion

Model associated with an equipment cannot be deleted.

## 2.6 SYSTEM MAINTENANCE

### 2.6.1 CONFIGURATION FILE

This section is used to export and to import configuration files for the iO device.

#### **To import a new configuration:**

\*Before importing a new configuration, be sure that no user is performing manual operations.

1. In the Settings | System Maintenance module, click on the Configuration File
2. Click on *Export*

\*This step is not mandatory but recommended by Multitel. If the new configuration causes some unexpected results, the configuration can be restored with the configuration backup.

3. Click on *Import*
4. Select the new configuration file (must be a CSV. or TEXT. File)
5. Click on *Start Import*

Import a new configuration may take a few minutes to complete the process. A confirmation or error message will be displayed when the process will be finished.

6. As need, reboot the device to apply changes

#### **Error Messages**

Even if there is some error message, the configuration will be uploaded excepted for error lines.

---

### ATTENTION

When you import a configuration file, all existing configuration on the device will be replaced by the new configuration. Imported a configuration file can change critical configuration such as ethernet connection properties which can impact the remote access of the device.

Multitel recommends backup/export the configuration file before importing the new configuration file. To avoid overwriting existing configuration, Multitel also recommends importing only the parameters modified and not the whole configuration file.

---

### 2.6.2 SOFTWARE UPDATE

Software update is used to upload a new version of the software provided by Multitel.

### 2.7.3 RESET FACTORY

Reset factory option allows to restore the device to its original state. Performing factory reset will delete all your data and configuration.

---

### MULTITEL RECOMMENDATION

Multitel recommends backup/export the configuration file before performing a factory reset.

---

Multitel recommends backup/export the configuration file before performing a factory reset.

To restore to factory settings:

1. Click on *Settings – System Maintenance*
2. Click on *Reset Factory* tab
3. As your need, reset Ethernet port by enabling the field
4. Click on *Reset Now*

Your device will reboot instantly and may show the progress screen of the rebooting. The process may take a few minutes.

## 2.8 LABELS

To add a new label:

1. Click on *Settings – Label*
2. Click on + *Label*



3. Enter a One Label and Zero Label
4. As your need, enter a description
5. Click on *Save Label*

To delete a label:

1. Click on *Settings – Label*
2. Select the label you want to delete  
You can select multiple labels at the same time to delete them.
3. Click on *Delete*
4. Confirm the deletion

Label associated with a binary status cannot be deleted.

## 2.9 REBOOT

Reboot button is used to manually reboot the iO device. After confirmation, your device will reboot instantly and may show the progress screen of the rebooting. The process may take a few minutes.

## 3. DATA SOURCE

The data source is the one main module of the iO device and can be accessed by clicking on the Data Source logo on the left side of the iO interfaces



Comprehension of the different ways that the iO device can monitor different types of equipment is fundamental and particular attention needs to be paid to this module.

### 3.1 IO DEVICE MONITORING CAPABILITIES

iO is a multi-protocol gateway capable of dealing with multiple types of equipment at the same time. iO supports a wide range of communication protocols:

- Modbus TCP/IP – Client
- Modbus RTU – Slave
- SNMP GET – v1/v2c/v3
- SNMP Agent – v1/v2c

The goal of the iO is to increase the monitoring capabilities of existing monitoring solutions by enabling them to gather data from devices that they are not able to reach.

### 3.2 GATEWAY MODE

iO supports two different gateway modes. These modes are called: Standard Mode and Transparent Mode. Please note that Modbus TCP/IP is the only protocol that can support the transparent mode.

#### 3.2.1 STANDARD MODE

The standard mode is the only mode that displays actual monitored data points on the interfaces Data Source | Dashboard. The standard mode consists of a mapping process. It requires to map a register or OID from an Equipment to an either an iO Modbus Register or OID.

iO Modbus registers need to be mapped manually but iO OIDs are mapped automatically in the iO MIB which include two tables: Analog Input and Binary Input.

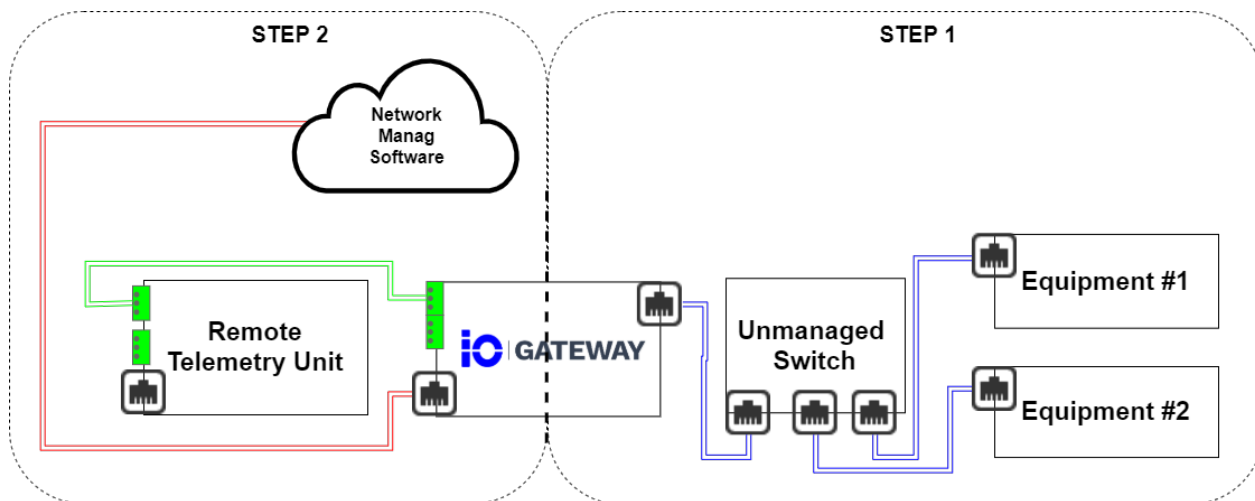
#### 3.2.2 TRANSPARENT MODE

The transparent mode is the easiest way of dealing with Modbus TCP/IP based equipment because it requires no mapping of register or OID between the iO and the equipment. The

transparent mode should preferably be used when dealing with equipment that supports Modbus TCP/IP protocol.

### 3.3 IO MONITORING ARCHITECTURE

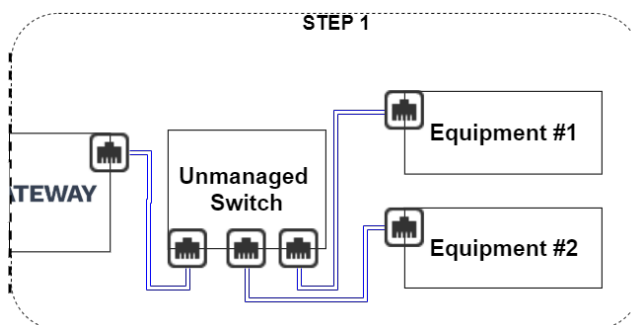
Figure 9 –iO Monitoring Architecture



#### 3.3.1. EQUIPMENT CREATION

This section will cover the equipment and data points creation.

Figure 10 – Step 1



To create an equipment

1. Click on + *Equipment*

### Equipment Creation Section

2. Enter Equipment Name
3. Smart Equipment (Yes)
4. Select Communication Protocol (Modbus TCP/IP – Client, Modbus TCP/IP - Master, SNMP GET)
5. Select Equipment Category
6. Select Equipment Model
7. The manufacturer field will be filled automatically based on the equipment model.

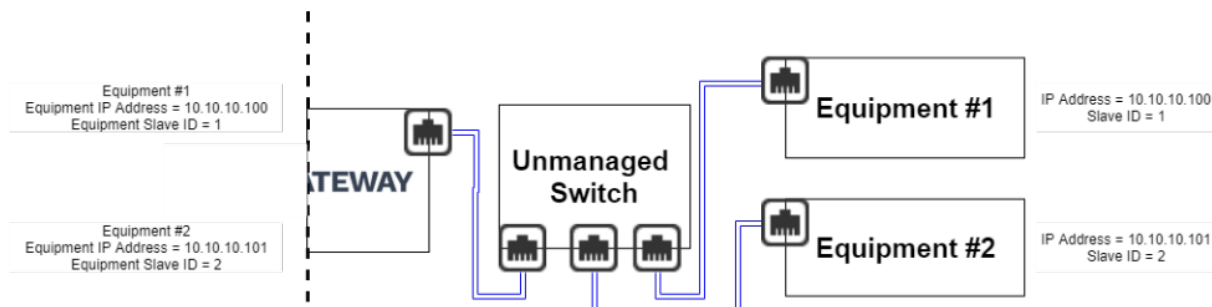
### Communication protocol section

Fields displayed in this section are according to the Communication Protocol selected in the Equipment Creation Section.

#### 3.3.1.1. Communication Protocol: Modbus TCP/IP - Client | Standard mode

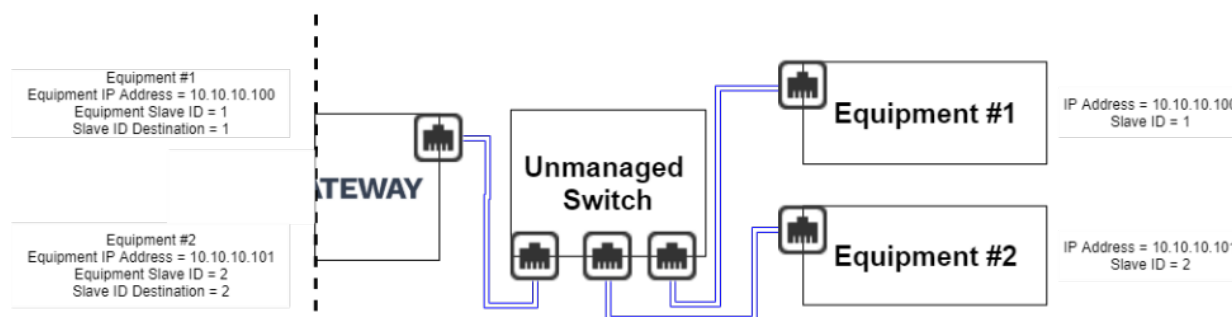
8. Select Gateway mode – Standard Mode
9. Enter Equipment Slave ID
10. Enter Equipment IP Address or Equipment Hostname
11. Enter Port Number (502 default value for Modbus TCP/IP)
12. Select Register Order (Lower Address/Higher Address)
13. Select Register Base Address (Use given address/Substrat 1 from given address)
14. Select Equipment Polling Rate
15. Select Equipment Time Out
16. Click on *Save*

Figure 11– Standard Mode



- 3.3.1.2. Communication Protocol: Modbus TCP/IP - Client | Transparent mode
8. Select Gateway mode – Transparent Mode
  9. Enter Equipment Slave ID
  10. Enter Equipment IP Address
  11. Enter Port Number (502 default value for Modbus TCP/IP)
  12. Select Equipment Polling Rate
  13. Select Equipment Time Out
  14. Enter Slave ID Destination
  15. Click on Save

Figure 12 –Transparent Mode



- 3.3.1.3. Communication Protocol: Modbus RTU - Master
1. Select Serial Port (according to the RS-485 configuration)
  2. Enter Equipment Slave ID
  3. Select Register Order
  4. Select Register Base Address
  5. Select Equipment Polling Rate
  6. Select Equipment Time Out
  7. Click on Save

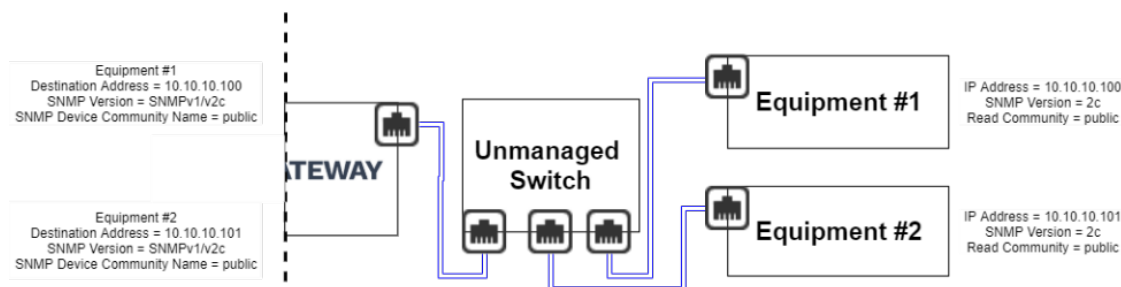
- 3.3.1.4. Communication Protocol: SNMP Get V1/V2C
1. Enter Equipment IP Address or an Equipment Hostname
  2. Select SNMP Version (v1, v2c, v3)
  3. Enter Constant Part of OID (not required)
  4. Enter SNMP Device Community Name

5. Select Equipment Polling Rate
6. Select Equipment Time Out
7. Enter Port Number (161 default value for SNMP GET)

If you selected SNMP v3

8. Enter a Username
9. Select Security Level (No authentication, No privacy/ Authentication, No Privacy/ Authentication, Privacy)
10. Select Authentication Protocol (MD5, SHA1)
11. Enter Authentication Password  
Password Requirement: minimum 8 characters
12. Select Privacy Protocol (DES, AES)
13. Enter Privacy Password  
Password Requirement: minimum 8 characters
14. Click on Save


Figure 13 – SNMP GET



### 3.3.2. DATA POINTS CREATION

#### 3.3.2.1. Modbus TCP/IP – Standard mode

#### **Analog Data Points**

1. Click on the three dots icon  of the equipment
2. Click on *Data Point* option
3. Click on + *Data Point*
4. Enter a Data Point Description
5. Enter the Equipment Modbus Register

6. Select a Register Type

- Holding Register
- Input Register

7. Select a Data Type

- 16-bit integer
- 32-bit integer
- 32-bit float

8. Select the unity and the number of decimals displayed

9. Click on *Pull Data*


The ID of the data point will be created automatically after clicking on *Pull Data*

Advanced section

To access the advanced section of the data point you must click on the plus icon  .

Factor	Multiplication
Offset	Addition
iO Modbus Register	To use the iO device as a gateway for RTU or Network Management Software enter an iO Modbus Register: 0 to 65 565
Polling Rate	Indicates how often the data point is going to be polled. Default value: 15 seconds

**Binary Data Points**

1. Click on the three dots icon  of the equipment
2. Click on *Data Point* option and click on the *Binary* tab
3. Enter a Data Point Description
4. Enter the Equipment SNMP OID
5. Select a Register Type

- Coil RT=1
- Discrete Input RT=2
- Holding Register RT=3
- Input Register RT=4

6. According to the Register Type selection, as needed select a Data Type

- 1-bit DT=0

16-bit integer DT=1

32-bit integer DT=2

7. Select a Mask Type

None MSK\_ST= 0

Bit MSK\_ST= 1

Ranger MSK\_ST= 2

8. According to the Mask Type selection, as needed select a Mask
9. According to the Mask Type selection, as needed select a Value Interpretation
10. Select a Status (status listed are them created in the Settings - Labels section)
11. Click on *Pull Data*

3.3.2.2. Data Points – Modbus TCP/IP – Transparent Mode

**IMPORTANT NOTE:**

There is no data points configuration available in transparent mode.

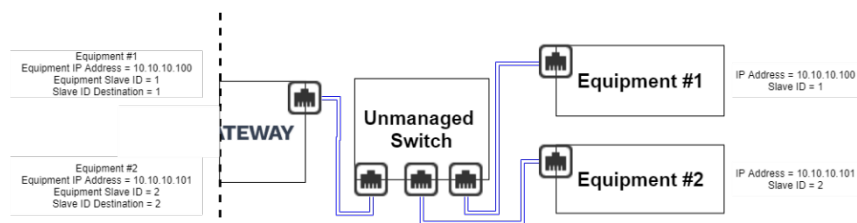
**IO Modbus Register and OID Mapping**

No iO Modbus Register mapping is required when using the transparent mode.

1. Go into RTU web interfaces
2. The RTU needs to use Modbus RTU – Master to get data points from the iO Gateway.
3. Create a module or a device to bind the iO Gateway and the RTU.
4. Enter the Slave ID of the Slave ID destination and not the iO Gateway Slave ID.

In transparent mode, the Slave ID Destination is the Slave ID that the user needs to use in the RTU. Since there is no mapping of Modbus Register, the iO Gateway exposes Modbus register. Since equipment can have the same Modbus registers, the Slave ID destination is used to make a distinction between each Modbus Registers.

Figure 14– iO Modbus Register – Modbus TCP/IP Transparent






5. Create a data point on the RTU
6. Use the Modbus Registers from the list provided in the equipment vendor documentation.

3.3.2.3. Data Points - SNMP Get v1/v2C/v3


**Analog Data Points**

1. Click on three dots icon 
2. Click on *Data Point* option
3. Enter a Data Point Description
4. Constant Part of OID will be automatically displayed in Constant Prefix
5. Enter the Equipment SNMP OID Suffix
6. Select the unity and the number of decimals displayed
7. Click on *Pull Data*

Advanced section

Register Data Type	Option: "16-bit integer", "32-bit integer", "32-bit float"
Register Type	Option: "Holding Register", "Input Register"
iO Modbus Register	To use the iO device as a gateway for RTU or Network Management Software enter an iO Modbus Register: 0 to 65 565
Polling Rate	Indicates how often the data point is going to be polled. Default value: Polling Rate configurated to the equipment
Factor	Multiplication
Offset	Addition

**Binary Data Points**

1. Click on three dots icon 
2. Click on *Data Point* option and select the Binary tab
3. Enter a Data Point Description
4. Constant Part of OID will be automatically displayed in Constant Prefix
5. Enter the Equipment SNMP OID Suffix
6. Select a Syntax Type

Int String                      SYNT=1

Integer SYNT=2

Bit String SYNT=3

7. Select a Data Type

1-bit DT=1

16-bit DT=2

64-bit DT=3

8. Select a Mask Type

None MSK\_ST=0

Bit MSK\_ST=1

Ranger MSK\_ST=2

9. According to the Mask Type selection, as needed select a Mask

16 bit 0 to 15

32 bit 0 to 31

64 bit 0 to 63

10. According to the Mask Type selection, as needed select a Value Interpretation

Reference value for calculating the binary status of a data point without a mask or with a "range" mask. 0 to 65 535 (no-decimal is allowed)

11. Select a Status (status listed are them created in the Settings - Labels section)

12. Click on *Pull Data*

Advanced section

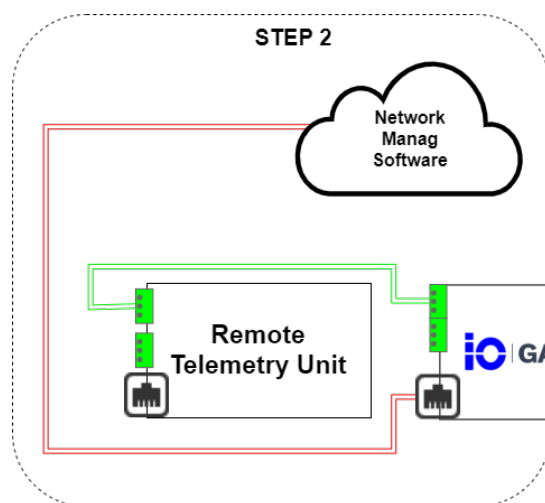
Register Data Type	Option: "16-bit integer", "32-bit integer", "32-bit float"
Register Type	Option: "Holding Register", "Input Register"
iO Modbus Register	To use the iO device as a gateway for RTU or Network Management Software enter an iO Modbus Register: 0 to 65 565
Polling Rate	Indicates how often the data point is going to be polled. Default value: Polling Rate configurated to the equipment
Factor	Multiplication
Offset	Addition

### 3.3.3. NETWORK MANAGEMENT SOFTWARE

#### 3.3.3.1. SNMP Get

No mapping is required when monitoring the iO device using SNMP. The only step required is to download the iO MIB on Multitel websites and enabling the SNMP Agent (see section 2.4.2).

Figure 15 – iO Gateway mapped to the Network Management Software



## 4. PASSTHROUGH

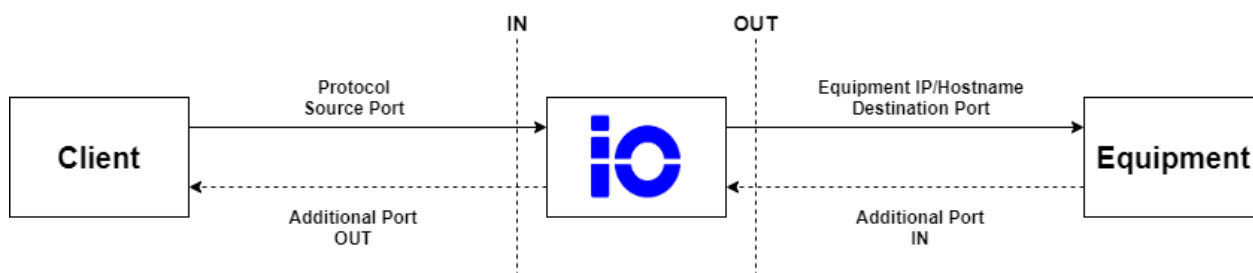
Passthrough is a standalone iO module enabling IP-based communication between a WAN and a LAN. Using this module, the iO can be configured as a router.

### 4.1 PASSTHROUGH OVERVIEW

The Passthrough module uses the client-server model. A client is a program or device which sends a request to another device or program to access a service made available by a server. A typical example is a Web browser (client) that sends a request to a Web server to access Web pages.

Contrary to a client-server model hosted on the same network, the iO passthrough is primarily used to reroute client requests from a WAN to a server on a LAN. Services hosted on a local network can, therefore, be accessed securely on a wide network using the iO.

Figure 16– Passthrough Topology



The iO Passthrough topology is divided into two sections: Client/iO Gateway and iO Gateway/Equipment.

#### Client/iO Gateway

The user can use a client to send a request to the iO by providing the following information:

- iO' IP address
- Server Protocol
- Source Port

#### iO Gateway/Equipment

Once the client is configured, the iO will reroute the client requests to the equipment server.

### 4.1.3. FIELDS DESCRIPTION

#### 4.1.1.1 Protocol Options (mandatory)

Table 5 – Protocol description

Protocol Name	Description
Insecure Protocol	
HTTP	Hypertext Transfer Protocol is used as an internet communication
FTP	File Transfer Protocol is used for transferring file to another device
Telnet	Telecommunication Network is used to log on to one TCP/IP host to access to other hosts on the network
Secure Protocol	
HTTPS	Hypertext Transfer Protocol Secure is used as an internet communication
SFTP	Secure File Transfer Protocol is used for transferring file to another device with security components
SSH	Secure SHell is used to execute commands in a remote device and move file from one device to another
SCP	Secure Copy Protocol is used for transferring files securely form a local to a remote host.

#### 4.1.1.2 Source Port Options (mandatory)

The sources port is self-generated according to the specifications below. If needed, user can change it. The source port must be unique and between 1 to 65 535.

Table 6 –Source Port specifications

Protocol Name	Specifications
HTTP/HTTPS	61 000 to 61 999
FTP/SFTP/SCP	62 000 to 62 999
Telnet/SSH	63 000 to 63 999

#### 4.1.1.3 Destination IP (mandatory)

Destination IP allows you to configure the destination IP or Hostname.

Destination Type	Format accepted
IP	0.0.0.0 to 255.255.255.255
Hostname	1 to 63 long characters 253 ASCII characters 0 to 9 "-" and "."

#### 4.1.1.4 Destination Port (mandatory)

The destination port is self-generated according to the specifications below. If needed, user can change it. The destination port must be between 1 to 65 535.

Protocol	Destination Port
HTTP	80
HTTPS	443
FTP	21
SFTP	21
SSF	22
Telnet	23
SCP	22

#### 4.1.1.5 Additional Port

The additional port allows to add more ports to the passthrough.

Port range accepted: 1 to 65 535 (Port interval is accepted)

#### 4.1.1.6 Transport Protocol (mandatory)

TCP (default option)

UDP



Both

4.1.1.7 Action

- None (default option)
- IN
- Passthrough

4.1.1.8 Status


Allows to enable and disable the passthrough.

Icon	Description
Blue icon 	The passthrough is enabled
White icon 	The passthrough is disabled

4.1.1.9 Web Access

The *Passthrough* button is displayed only when the HTTP or HTTPS protocol are enable. Clicking on the button opens the web interface of the equipment.

## 4.2 PASSTHROUGH CONFIGURATION

You can access to the passthrough configuration page by clicking on the Passthrough module in the menu .

To add a Passthrough:

1. Click on + *Passthrough*
2. Fill the form
3. Enabled the passthrough
4. Click on *Save*

To edit a Passthrough:

1. Modify directly the field needed to be adjusted
2. Click on *Save* to apply the modification

To delete a Passthrough:

1. Select the passthrough needed to be deleted

You can select multiple passthrough at the same time to delete them.

2. Click on *Delete*
3. Confirm the deletion