Multitel

iO GATEWAY

USER MANUAL

Document Name:	UM_iO Gateway_1.4
Issue:	4
Date (MM/DD/YYYY):	09/20/2021

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:

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 Protocol SSH added	L. Methot
4	07/27/2021	iO Gateway v1.4	L. Methot

TABLE OF CONTENTS

FIGURES

TABLES

TECHNICAL 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.

1. FIRST TIME CONNECTION

1.1 ETHERNET CONNECTION

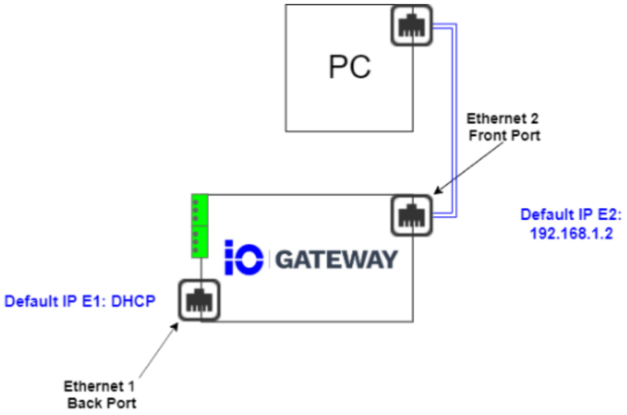
iO Gateway interfaces need to be accessed in a web browser. iO Gateway can either be accessed by the front or the back Ethernet port. However, for the first connection, the front Ethernet port needs to be used because the backport doesn’t have a static IP address (DHCP). The following table shows the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

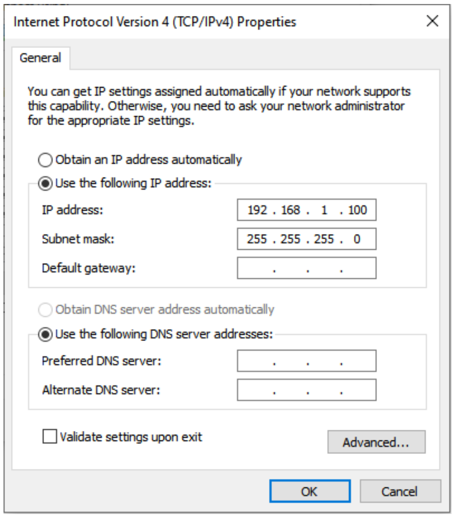


To create a LAN between a PC and the iO Gateway. The user needs to change the ethernet port adapter proprieties. This can be done by on a Windows machine by:

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


Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

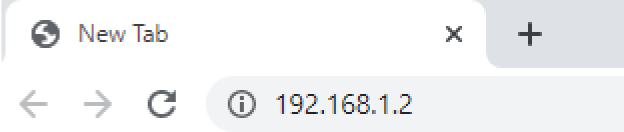
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

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


192.168.1.2

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.

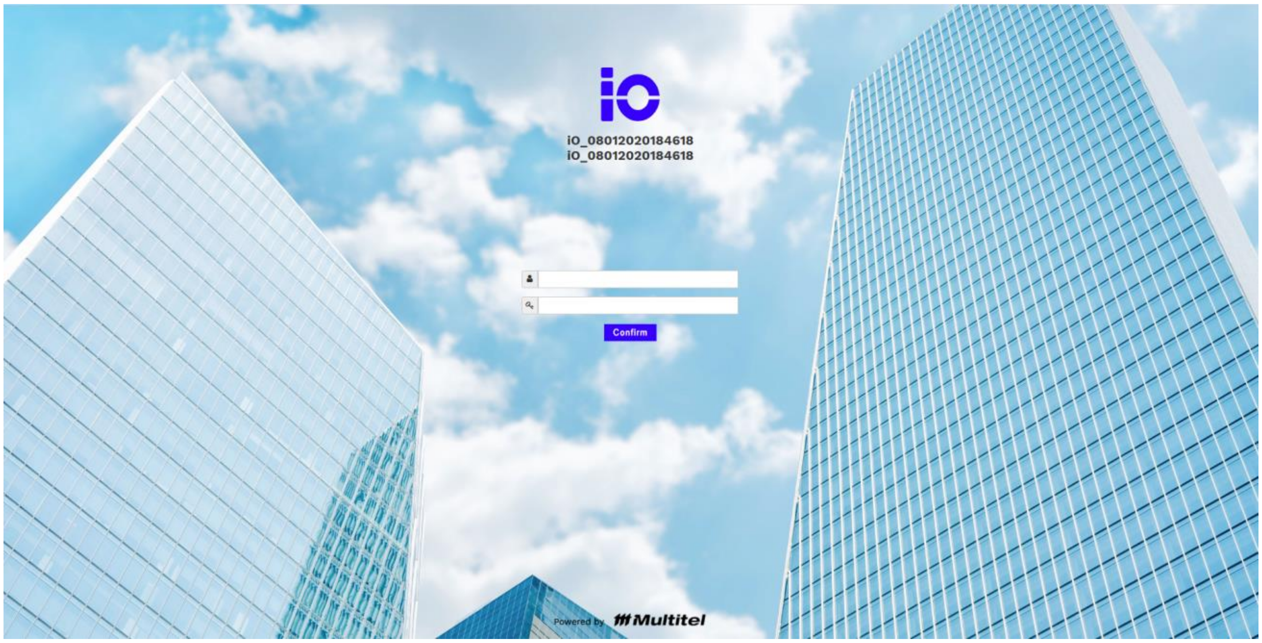
Table 2 – Supported Web Browsers

Web Browsers
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

Administrator	Username	administrator
	Password	admin
User	Username	user
	Password	user
Viewer	Username	viewer
	Password	viewer

1.3 INITIAL CONNECTIONS

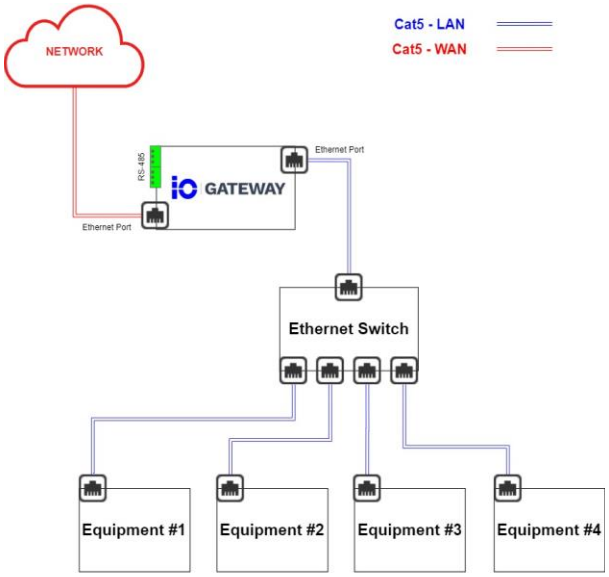
1.3.1 ETHERNET CONNECTION

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

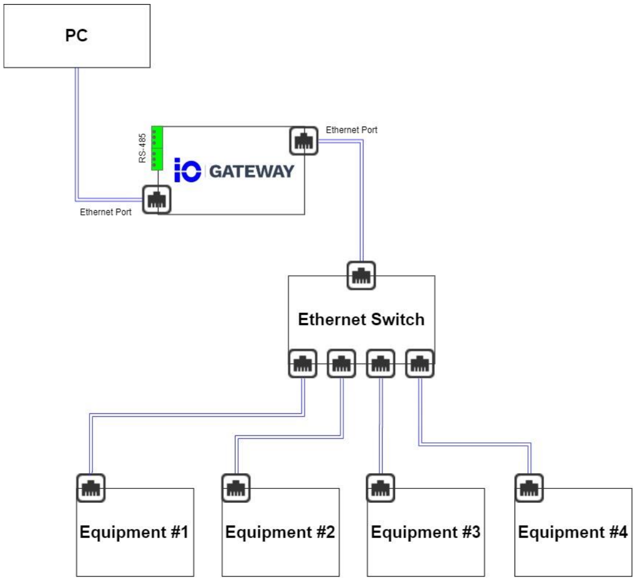


1.3.1.2 Configuring LAN iO device and equipment

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

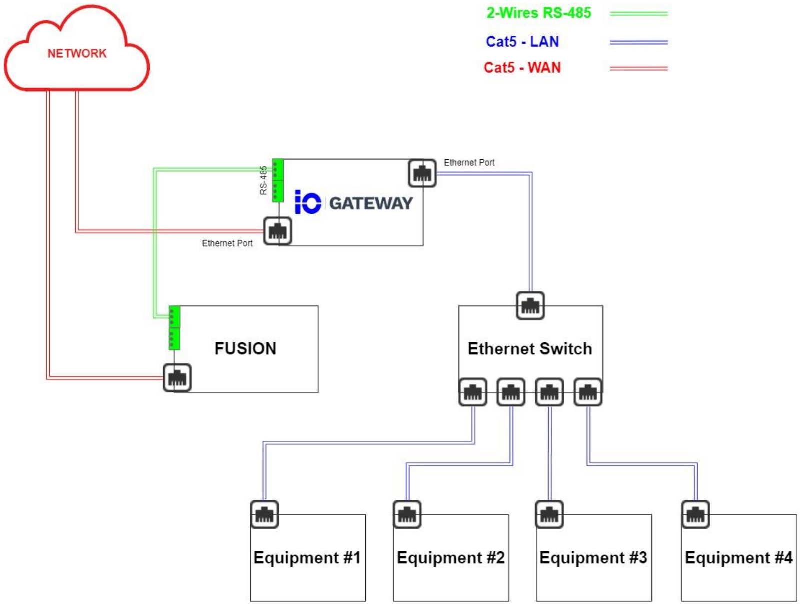
5. Keep MTU at 1500 unless specified otherwise by your network administrator.
6. Keep Speed at Auto unless specified otherwise by your network administrator.
7. Click on Mode to change from DHCP to Static.
8. Enter IPv4 Address, IPv4 Subnet Mask, and iPv4 Gateway. Make sure that every piece of equipment 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



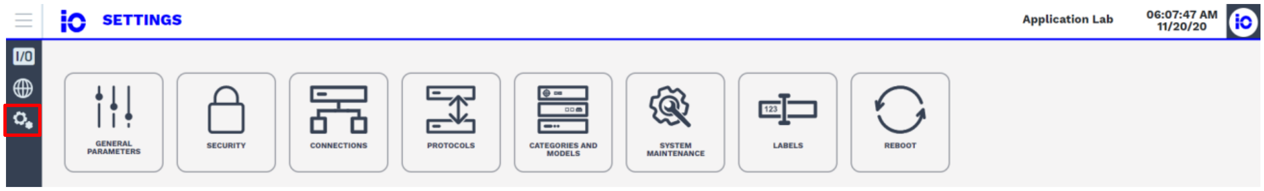
1. Click on *Settings*
2. Click on *Connections*
3. Click on *RS-485 – COM A* tab

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 Information tab

System Resources

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

Power Input

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

About

About section covers several components of the iO device:

- Serial Number
- Model Number
- Batch Number
- Hardware Version
- Software Version
- Memory Max
- Disk Max
- Mac 0
- Mac 1
- Trending Data Point

2.1.2.2 Activation Key

After the installation, at any moment it is possible to update with a superior version the device. An activation key generate by Multitel is required to activate the advanced option.

To request an activation key, please contact your sales representative or the Multitel professional service (support@multitel.com).

Information	Description
Product Version	Refer to the current version used.
Update your Product	Explanation of the update available.

To update a device with the advanced option:

* Even if the update shall not overwrite the configuration before performed an update, Multitel recommends exporting the configuration file. Thus, if there are any unexpected results, the configuration can be restored with the backup configuration.

1. Click on *Settings*, then *General Parameters – System Information*
2. Click on *Activation Key* tab
3. Copy and paste the activation key provide by Multitel in the activation key field
4. Click on *Activate*

Table 4 – Activation key error messages

Message	Issue description
Serial number or MAC addresses does not match with the activation key. Please try again.	The serial number or the MAC is not associated to the activation key.

Activation key has already been used or no longer valid. Please try again	The activation is not active anymore, the activation key has been already used or is expired.
Activation key not valid. Please try again	The activation key is not entered correctly.

4.1.1 DATE AND TIME

Data and Time parameter can be configured from the **Settings** module in the General Parameters section. Date and Time section is used to set the time and date of the iO Gateway. Date and Time can be configurate manually or with a NTP Server.

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.

4.1.1.1 Date and Time Configuration

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

If you using a hostname as a NTP Server, the DNS server of the Ethernet Client must be enabled, otherwise the iO won't be able to reach the NTP Server. To enable the DNS Server, please refer you to the settings - connection section.

5. If needed, enter a second and tertiary NTP Server
6. Click on *Save*

4.1.1.2 Date and Time Format

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

4.2 SECURITY

User and access levels can be view and configured in the **Security** parameter from the **Settings** module.

The iO Gateway support two type of authentification:

- Standard authentification: The standard authentification allows to create unlimited of user and give access level directly to the security parameter of the device.
- LDAP Authentification: The LDAP authentification protocol can be used to connect up to 3 users by using the customer LDAP authenticator. For LDAP users all management action excepted the deletion has to be performed directly from the customer LDAP authenticator.

Table 5 – User Permission

Modules	Groups	Permission
Settings	Supervisor	Edit
	User	Read-only access *User can reboot the iO device
	Viewer	Read-only access to *General Parameters* and *Labels* parameters

Data Sources	Supervisor	Edit
	User	Edit
	Viewer	Read-only access
Passthrough	Supervisor	Edit
	User	Edit
	Viewer	Read-only access
SNMP Trap Forwarding	Supervisor	Edit
	User	Edit
	Viewer	Read-only access * User can export trap log

Table 6 – User informations

Field	Description	Mandatory
Username	Refer to the user's name. The username is used to log in the device.	Mandatory
Email	Refer to the user email.	
Phone	Refer to the user phone number.	
Function	Refer to the user function.	
Groups	Define the user permission	Mandatory
Authentication	Display the user type of authentication	Auto-populated
Password/ Confirm Password	There are no password requirements, but Multitel recommends that password should be at least 8 characters long and include letters (both upper and lower case), digits, and symbols.	Mandatory

To reset a password of a local user:

Only user assign to the supervisor group can reset password of any local user.

WARNING
If a user with a supervisor access level resets a password or changes the username of another user, the new credentials have to be informed to the user. There is no automatic notification sent to the user.

Users assigned to the user or viewer group can only reset their own password in the user profile interface (to access the user profile interface, on the header bar click on the IO logo and click on *user profile*).

MULTITEL RECOMMANDATION

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

To enable or disable a local 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 local or LDAP user:

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

IMPORTANT NOTE

The default user named Administrator cannot be deleted or disabled.

4.3 CONNECTIONS

The connections parameters can be accessed from **Settings** module.

NOTE

This parameter 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.

4.3.1 ETHERNET PORTS

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

Following fields can be configured:

- MTU
- Speed (Auto, 10Mbs, 100Mbs, 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.

4.3.2 RS-485 PORTS

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

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

4.4 PROTOCOLS

The protocol parameters can be accessed from the **Settings** module.

4.4.1 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.

The default HTTP port is 80; HTTPS port is 443. To change those defaults, enter a port number between 1 to 65 534. To ensure a good communication, those ports number must be unique.

4.4.2 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

   The default port is 161; to change this default, enter a port number between 1 to 65 534.
4. Enabled the SNMP v1/v2c Agent or v3
5. Enter a Read Community Name
6. Click on *Submit*

4.4.3 SNMP - TRAP

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

To configure the SNMP Trap

7. Click on *Settings*
8. Click on *Protocols – SNMP – Trap* tab
9. Enter a Port Number

   The default port is 161; to change this default, enter a port number between 1 to 65 534.
10. Enabled the SNMP v1/v2c
11. Enter a Read Community Name
12. Click on *Submit*

4.4.4 PING

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

4.4.5 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

   The default slave ID is 80; to change this default, enter a port number between 1 to 255.
5. Click on *Submit*

4.4.6 SSH

Configuring the SSH protocol:

1. Click on *Settings*
2. Click on *Protocols - SSH* tab
3. Click on Enable
4. Enter the Port Number

   The default port is 22; to change this default, enter a port number between 1 to 65 534. To ensure a good communication, this port number must be unique.
5. Click on *Submit*

4.5 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.**

4.5.1 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.

4.5.2 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.

4.6 SYSTEM MAINTENANCE

4.6.1 CONFIGURATION FILE

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

*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* tab
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 backup configuration.

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.

Error Messages

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

6. As need, reboot the device to apply changes by clicking on the *Reboot* button in the header

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.

MULITEL RECOMMENDATION

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.

4.6.2 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.

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.

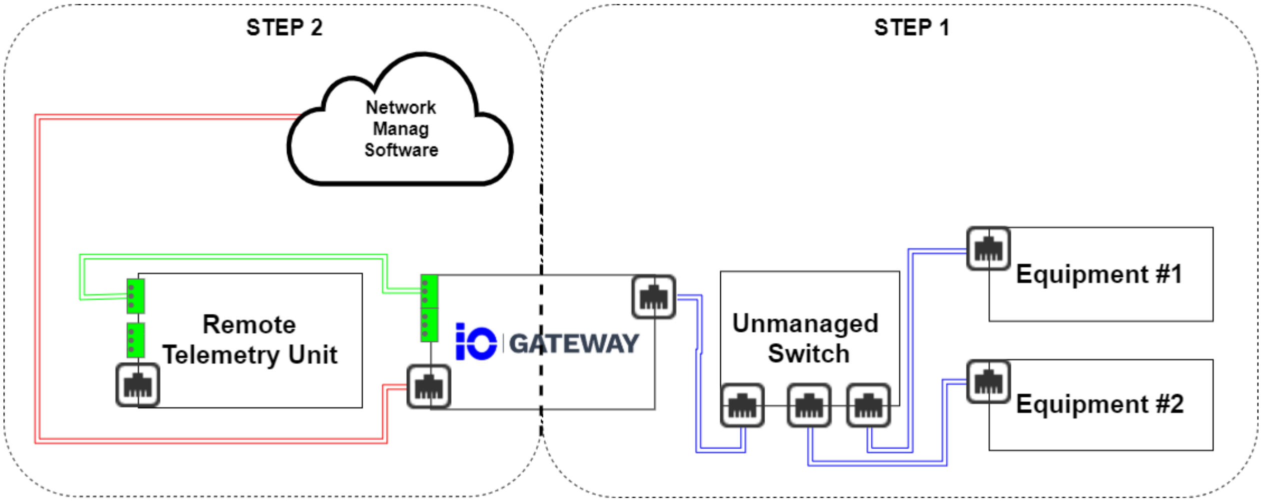
iO Modbus registers need to be mapped manually but iO OIDs are mapped automatically in the iO MIB which include two tables: Analog Input and Binary Input.

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

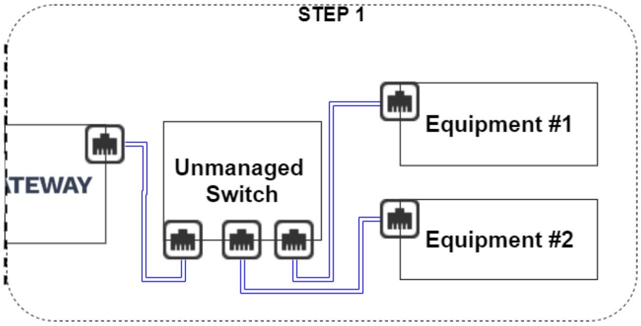
Figure 9 –iO Monitoring Architecture



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

* If the category needed is not created, refer you to the category and model section for instructions.

6. Select Equipment Model

* If the model needed is not created, refer you to the category and model section for instructions.

7. The manufacturer field will be filled automatically based on the equipment model.

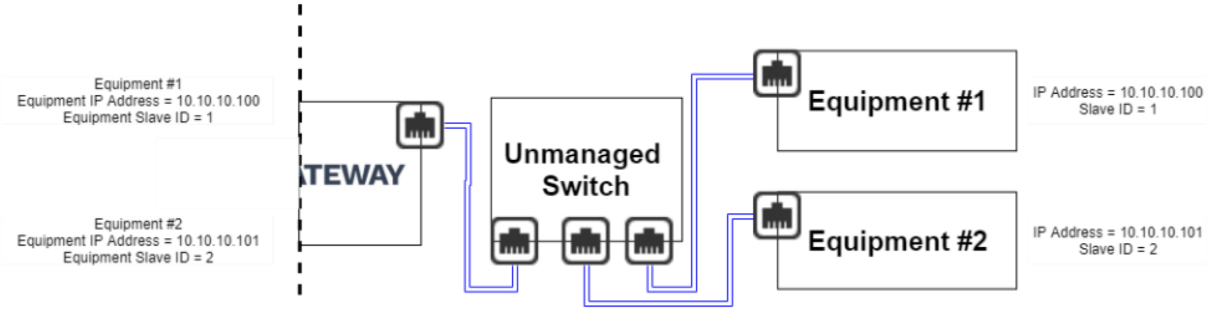
Communication Protocol section

Fields displayed in this section are according to the communication protocol selected.

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)

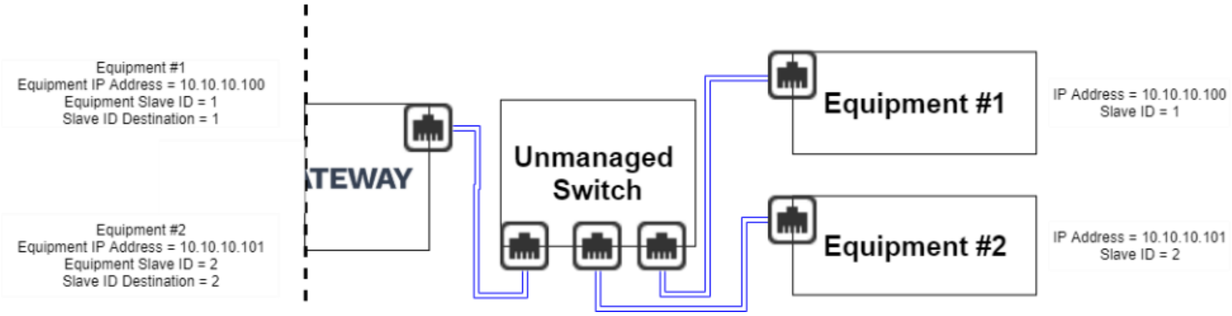
Figure 11– Standard Mode



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. Enter Slave ID Destination

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

3.3.1.4. Communication Protocol: SNMP Get v1/v2c/v3

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. Enter Port Number (161 default value for SNMP GET)

If you selected SNMP v3

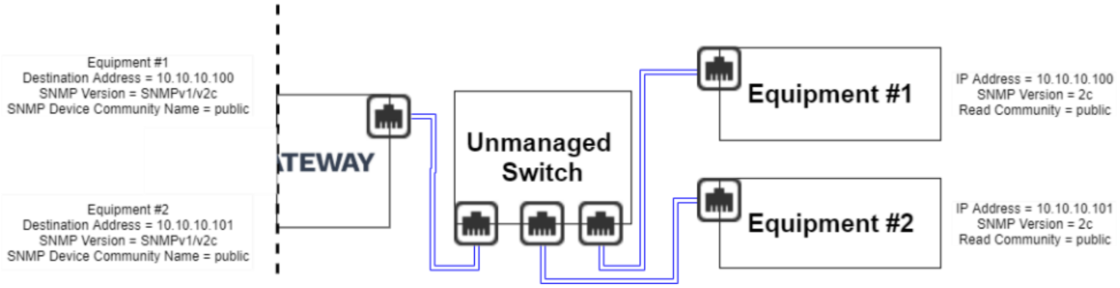
8. Enter a Username

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. Select Equipment Polling Rate (1 sec, 15 sec, 30 sec, 1 min, 5 min, 15 min, 30 min, 60 min, 4 hrs, 12 hrs, 24 hrs)
15. Select Equipment Time Out (1 sec, 2 sec, 3 sec, 4 sec, 5 sec)
16. Select Number of Retry (1 to 10)
17. Select Time Out after Retry (5 min, 15 min, 30 min, 60 min, 4 hrs, 12 hrs, 24 hrs)
18. Select Total Iteration Number (1 to 10)

Figure 13 – SNMP GET


Equipment #1
Destination Address = 10.10.10.100
SNMP Version = SNMPv1/v2c
SNMP Device Community Name = public
Equipment #2
Destination Address = 10.10.10.101
SNMP Version = SNMPv1/v2c
SNMP Device Community Name = public
ATEWAY
Unmanaged Switch
Equipment #1
IP Address = 10.10.10.100
SNMP Version = 2c
Read Community = public
Equipment #2
IP Address = 10.10.10.101
SNMP Version = 2c
Read Community = public

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*
3. Click on *+ Data Point*
4. Enter a Data Point Description

5. Enter an Equipment Modbus Register, a Register Type and a Data Type
6. Select a unit and the number of decimals displayed
7. Click on *Pull Data*

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

Advanced options

To access the advanced section of the data point you must click on the plus icon ✚. All advanced options are optional.

Table 7 – Advanced information SNMP analog data point

Factor	To multiplicate the value
Offset	To addition the value
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
Number of Retry	The number of retry indicates how many time the device will retry to get a reading from a data point. Once the value of the number of retry is reached, the data will be disabled.
Timeout after Retry	The timeout after retry indicates how long the device needs to wait to retry getting a value from the disabled data point.
Total Iteration Number	The total iteration number indicates how many cycle the device shall done before disabled the datapoint permanently.

Binary Data Points

1. Click on the three dots icon ••• of the equipment
2. Click on *Data Point* and click on the *Binary* tab
3. Enter a Data Point Description
4. Enter the Register

5. Select a Register Type, Data Type, Mask Type, Mask, Value Interpretation
6. Select a Status

*Status listed are them created in the Settings - Labels section. If the label desired is not available, refer you to the Label section for instruction.

7. Click on *Pull Data*

Advanced options

To access the advanced section of the data point you must click on the plus icon ➕. All advanced options are optional.

Table 8 – Advanced information SNMP binary data point

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
Number of Retry	The number of retry indicates how many time the device will retry to get a reading from a data point. Once the value of the number of retry is reached, the data will be disabled.
Timeout after Retry	The timeout after retry indicates how long the device needs to wait to retry getting a value from the disabled data point.
Total Iteration Number	The total iteration number indicates how many cycle the device shall done before disabled the datapoint permanently.

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

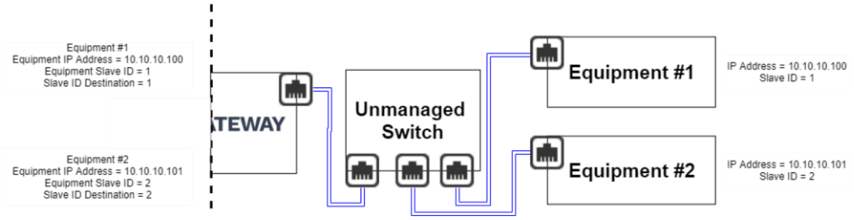
No iO Modbus Register mapping is required when using the transparent mode.

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 unit and the number of decimals displayed
7. Click on *Pull Data*

Advanced section

Table 9 – Advanced information Modbus analog data point

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
Number of Retry	The number of retry indicates how many time the device will retry to get a reading from a data point. Once the value of the number of retry is reached, the data will be disabled.
Timeout after Retry	The timeout after retry indicates how long the device needs to wait to retry getting a value from the disabled data point.
Total Iteration Number	The total iteration number indicates how many cycle the device shall done before disabled the datapoint permanently.

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
7. Select a Data Type
8. Select a Mask Type
9. According to the Mask Type selection, as needed select a Mask
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. If the label desired is not available, refer you to the Label section for instruction.

12. Click on *Pull Data*

Advanced section

Table 10 – Advanced information Modbus binary data point

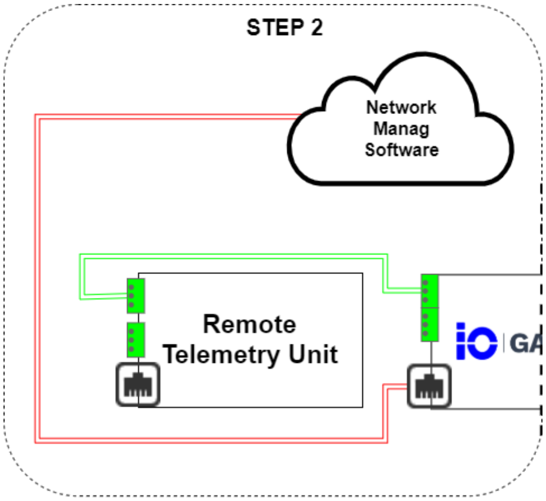
Register Data Type	Option: ‘’16-bit integer’’, ‘’32-bit integer’’, ‘’32-bit float’’
Register Type	Option: ‘’Holding Register’’, ‘’Input Register’’
iO Modbus Register	To use the iO device as a gateway for RTU or Network Management Software enter an iO Modbus Register: 0 to 65 565
Polling Rate	Indicates how often the data point is going to be polled. Default value: Polling Rate configurated to the equipment
Number of Retry	The number of retry indicates how many time the device will retry to get a reading from a data point. Once the value of the number of retry is reached, the data will be disabled.
Timeout after Retry	The timeout after retry indicates how long the device needs to wait to retry getting a value from the disabled data point.
Total Iteration Number	The total iteration number indicates how many cycle the device shall done before disabled the datapoint permanently.

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

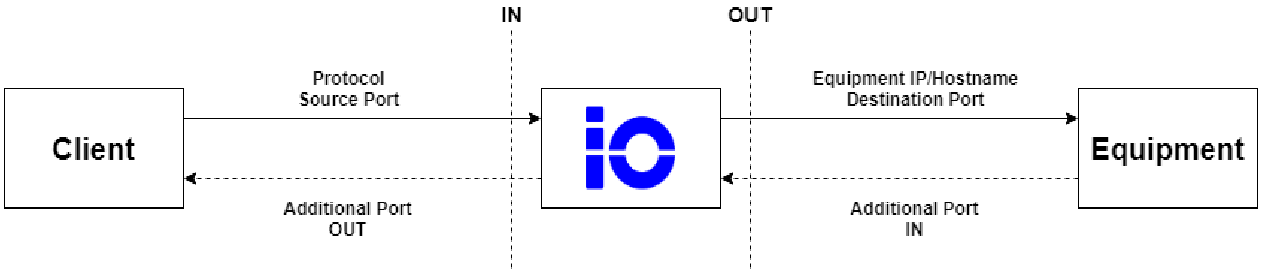
Passthrough is a standalone iO module enabling IP-based communication between a WAN and a LAN. Using this module, the iO can be configured as a router.

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 11 – 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 12 –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 enabled.

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

5. TRAP FORWARDING

5.1 TRAP FORWARDING OVERVIEW

The SNMP Trap Forwarding module allows the system receive and forward trap to one or multiple destination.

There are two types of traps supported by the iO device:

Table 13 – Type of SNMP Trap

Type	Description
Trap - Unacknowledged	The trap will be forwarded and the device won’t be informed that the trap was received from the remote application.
Trap – Acknowledged	The trap will be forwarded to the destination and the iO device will wait for a confirmation of the reception. The trap- acknowledge will be sent continually according to the notification settings until the destination sends an acknowledgment to the device or reaches the requested number of retries.

5.2 TRAP FORWARDING CONFIGURATION

You can access to the Trap Forwarding configuration page by clicking on the SNMP Trap module in the menu ⇔.

5.3.1. SOURCES

The trap forwarding sources tab allows to configure unlimited of trap sources and indicate the destination.

NOTE

There is no hard limit on the number of traps forwarding sources but Multitel recommends a limit of 50 sources to avoid any performance issue.

**At least one Trap Forwarding destination have to be created before adding an equipment source. To create a destination, refer you to the Trap Forwarding Destination section below for instruction.

Table 14 – Source information

Field name	Description	Default value
Equipment Name (Mandatory)	The equipment name is use to indicate the source of a trap forwarded. (Max length: 25, characters ; and , are not accepted)	
IP Address (Mandatory)	The IP address or the domain name of the equipment source. (yourbusiness.com or xxx.xxx.xxx.xxx)	
Destinations (Mandatory)	The destination indicates where traps received has to be forwarded. Multiple destination can be selected.	
Status	The status is use to enable or disable a source. Disabled a source stop the communication between the source and the iO device.	

5.3.2. DESTINATION

The trap forwarding destination allows to configure up to ten (10) destinations that the iO device could forward traps received.

Table 15 – Destination information

Field name	Description	Default value
Destination Name (Mandatory)	The destination name is use to differentiate all destinations. (Max length: 25, characters ; and , are not accepted)	
IP Address/Domain name (Mandatory)	The IP address or the domain name of the destination. (yourbusiness.com or xxx.xxx.xxx.xxx)	
Port Number (Mandatory)	The port number use to make connection with the IP destination to forward trap.	
Community Name (Mandatory)	The community name use to make connection with the IP destination to forward trap.	
SNMP Version (Mandatory)	The SNMP version use to forward traps received to the destination. (Options: v2c or v3)	v2c

Type	The type of trap the device shall forward trap received. (Options: Trap – Unacknowledged; Trap – Acknowledge)	Trap - Unacknowledged
Timeout	Timeout period only apply for trap-acknowledge. The timeout period indicates how long the device needs to wait between each retransmit of the trap, if the device does not get the acknowledgment. (Options: 1s; 5s; 30s; 1m)	
Retries	Retries only apply to trap-acknowledged The number of retries indicates how many time the device shall retransmit the trap, if the device does not get the acknowledgment. (Options: 1 à 5 times)	1
Kee- Alive Trap Delay	The keep-alive trap delay indicates the frequency that the device shall send the trap to the destination. (Options: None; 1min; 15min; 30min; 1hrs)	None
If SNMP v3 is selected		
Username (Mandatory)	The username used for authentication.	
Context Name	Name to distinguished a specific agent.	
Security Level (Mandatory)	Options: No authentication, No Privacy; Authentication; No privacy; Authentication; Privacy	
Authentication Protocol	Options: MD5; SHA1	
Authentication Password	(Minimum 8 characters)	
Privacy Protocol	Options: DES; AES	
Privacy Password	(Minimum 8 characters)	

To delete a Trap Forwarding Destinations:

1. Select the destination need to be deleted

The destination has to be previously unassigned to be deleted. The warning ❗ icon located where the checkbox shall be indicates that the destination is assigned to a source.

2. Click on *Delete*

5.3.2.1 Trap Sender Test

A trap sender test is used to send a trap test on demand in order to validate the communication between the iO device and the destination.

5.3.2.2 Keep-Alive Trap

A keep-alive trap is used to indicate to the destination on a periodic basis that the iO device is still active. A keep-alive trap is always a trap unacknowledged and the delay is configured individually for each destination.

5.3.3. LOG

The iO device records all traps received, forwarded and send by the keep-alive or the test trap button. To reduce unnecessary log, trap acknowledged (Inform) with multiple retries will be represented by one row in the log file.

The trap log can be exported in csv. file only. Here is the information contain in the log file:

- Date and time of the iO device

The timestamp is based on the date & time configuration of the device, to ensure a proper recording please make sure the date & time setup is accurate.

- The local date and time of the user

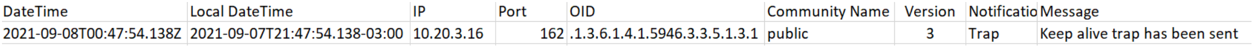
The timestamp is based on the date & time configuration of the user computer.

- IP address of the source or the destination
- Port number
- OID
- Community Name
- SNMP Version
- Trap Type
- Message

Table 16 – SNMP Trap error

Message Type	Description
Received has been sent	Refer to a trap received by the device
Forwarded has been sent	Refer to a trap received and forwarded to a destination
Keep Alive has been sent	Refer to a keep-alive trap
Test Trap has been sent	Refer to a trap triggered by the *Test trap* button
Forwarded as inform and received response	Refer to a trap – acknowledge that the destination sends an acknowledgement trap
Forwarded as inform but received no response	Refer to a trap – acknowledge that the destination does not send an acknowledgement trap
Error sending test trap: SPECIFIC MESSAGE	Indicate that the trap was not received or forwarded successfully. To help diagnose the issue, the message will be adjusted to give precision about the issue.

Trap forwarding log csv. file example



DateTime	Local DateTime	IP	Port	OID	Community Name	Version	Notificatio	Message
2021-09-08T00:47:54.138Z	2021-09-07T21:47:54.138-03:00	10.20.3.16	162	.1.3.6.1.4.1.5946.3.3.5.1.3.1	public	3	Trap	Keep alive trap has been sent

5.3.3.1 Period Log

The period log is automatically managed by the iO device. The device will automatically create a new period if one of these two conditions is met:

- If there are more than 25 000 rows in the excel file
- If the size of the excel file is bigger than 200 000 Mbit

To ensure optimum performance, the iO device will only keep the recording of four (4) periods. If there is more period created, the device will automatically delete the oldest.