Multitel

IO Supervisor

USER GUIDE

Multitel

CONTROL SHEET

Issue	Date YYYY/MM/DD	Description	Originator
1	2024-07-26	iO Supervisor	SB
2	2026-02-19	Version 2.1.0	SB
3	2026-03-10	Version 2.2.0	AC
4	2026-04-27	Version 2.2.1	AC

Multitel

TABLE OF CONTENTS

Multitel

Multitel

TABLES

Multitel

FIGURES

Multitel

Multitel

1.FIRST-TIME CONNECTION

1.1 ETHERNET CONNECTION

The iO Platform device interface is accessible through a web browser. The device can be connected via either the ETH-1 or ETH-2 Ethernet port. However, for the initial connection, you must use the ETH-2 port, as ETH-1 does not have a static IP address and relies on DHCP. The table below shows the factory settings for both Ethernet ports.

Table 1: Factory Settings for Ethernet Ports

Ethernet Ports	Mode	IPv4 Address
ETH-1: 1 Gbps	DHCP	N/A
ETH-2: 100 Mbps	Static	192.168.1.2

A local area network (LAN) must be established between the iO device's front Ethernet port and the user's PC.

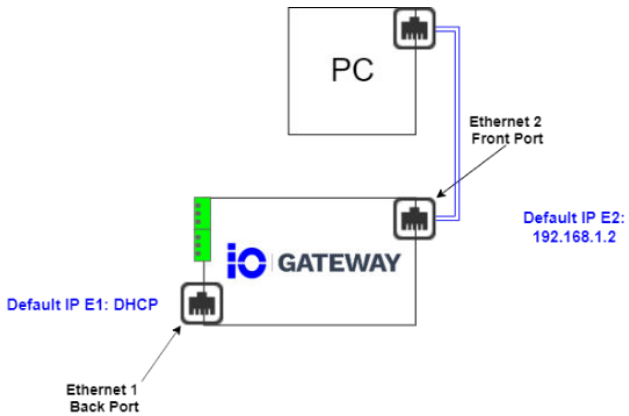


Figure 1: First-Time Connection

To create a LAN between a PC and the iO device, the user must modify the Ethernet adapter settings. On a Windows computer, proceed as such:

- Open the Control Panel.
- Select Network and Sharing Center, then Change adapter settings.
- Right-click the desired Ethernet adapter and select Properties.
- Select Internet Protocol Version 4 (TCP/IPv4).
- Click Properties.
- Set the IP address and Subnet mask (e.g., 192.168.1.100 and 255.255.255.0).

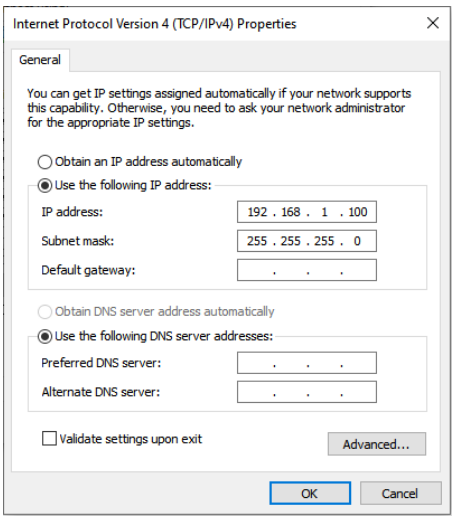


Figure 2: Changing IPv4 Properties on a PC

Once the LAN is configured, the user must enter the default IP address (192.168.1.2) into the web browser's address bar.

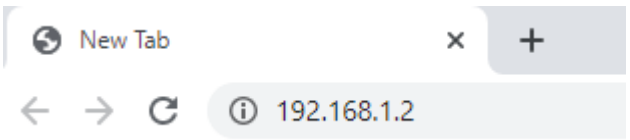


Figure 3: IP Address in Web Browser

Please note that the iO Platform device uses a modern web server that does not support legacy web browsers. The table below lists the web browsers supported by the iO device.

Table 2: Supported Web Browsers

Web Browser	Minimum Recommended Version
Google Chrome	132.0
Mozilla Firefox	121.0
Microsoft Edge	132.0

1.2 FIRST-TIME LOGIN

Once the default IP address is entered in the address bar and the LAN is properly configured, the user will be directed to the iO Platform login page.

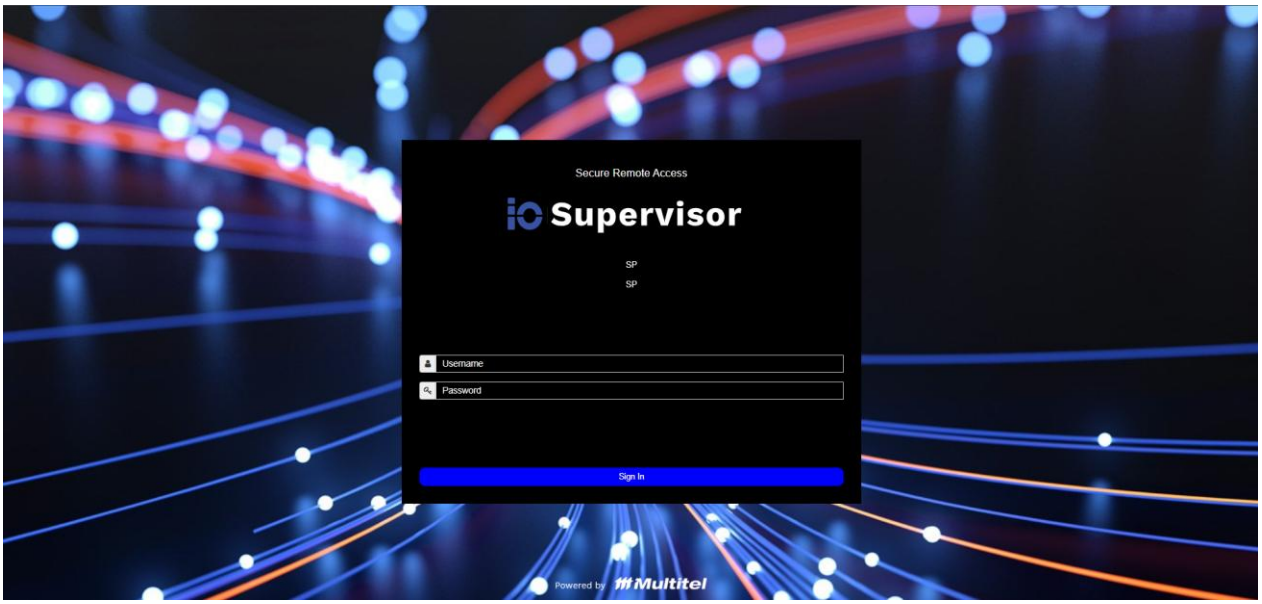


Figure 4: First-Time Login

The factory default credentials are as follows:

Table 3: Factory Credentials

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

1.3 INITIAL CONNECTIONS

1.3.1 ETHERNET CONNECTION

1.3.1.1 Configuring the WAN Connection on the iO Device

To enable remote access to the iO Platform web interface, the WAN connection must be configured on the ETH-1 Ethernet port. This port is located on the rear of the device and is not configured by default. Configuration changes to the rear ETH-1 port can be made directly from the user's PC.

⚠ **Note:** You must obtain a valid static IP address, subnet mask, and gateway from your IT administrator before proceeding.

Follow these steps to configure the connection:

- Click on Settings.
- Click on Connections.
- Select the ETH-1 – 1 Gbps tab.
- Leave the MTU at 1500, unless otherwise specified by your network administrator.
- Leave the Speed setting at Auto, unless otherwise specified.
- Change the Mode from DHCP to Static.
- Enter the values for the IPv4 Address, IPv4 Subnet Mask, and IPv4 Gateway.
- Click Save.
- Reboot the device.

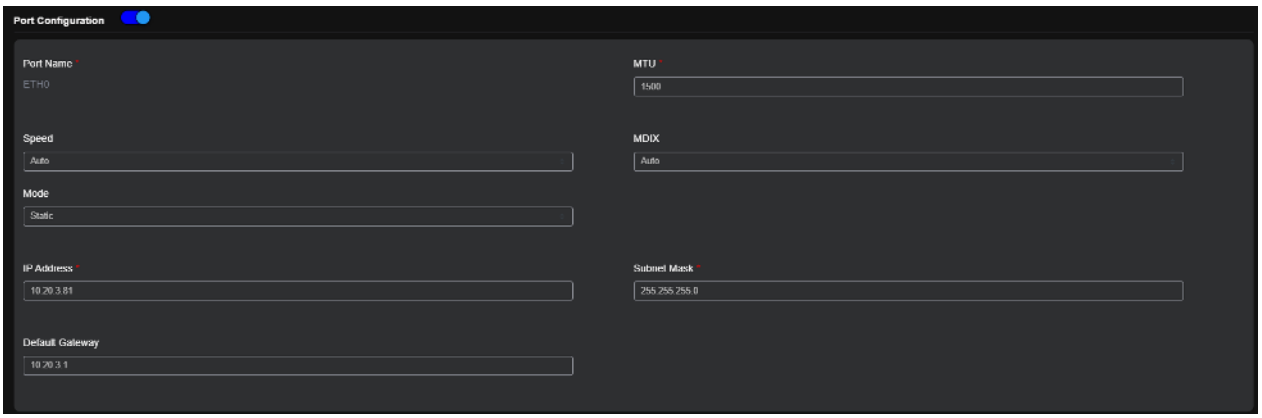


Figure 5: ETH-1 – 1 Gbps Configuration

1.3.1.2 1.3.1.2 Configuring the LAN iO Device and Asset

To connect the iO device to other equipment, a new local area network (LAN) must be configured. The iO device uses this LAN to communicate with and monitor the connected equipment.

If the iO device is intended to monitor only a single piece of equipment, the user may establish a direct LAN connection between the iO device and that equipment. However, in most cases, the iO device will be used to monitor multiple devices simultaneously. In such scenarios, one or more unmanaged Ethernet switches are required to create the necessary network.

When connecting multiple devices, ensure that each device is assigned a unique IP address and that all devices are configured to operate within the same subnet.

In this example, four pieces of equipment are to be monitored. A 5-port unmanaged Ethernet switch is used to create the LAN between the equipment and the iO Platform device. The equipment IPs are configured on the 10.10.10.X network.

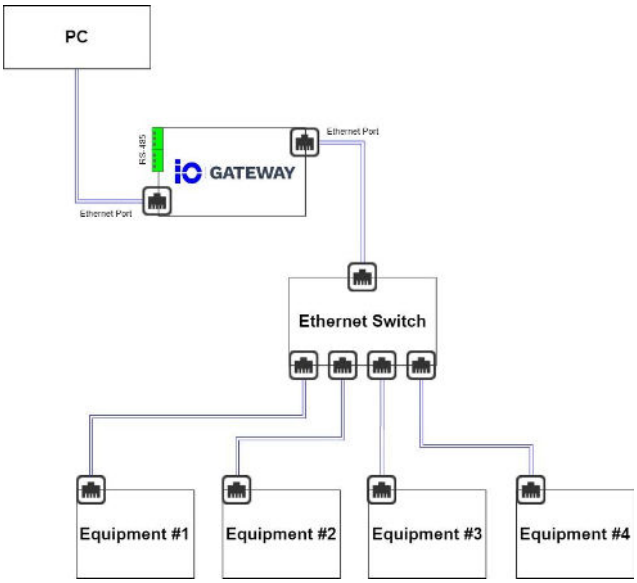


Figure 6: LAN Configuration

An Ethernet cable must be used to connect the rear Ethernet port of the iO device to the unmanaged switch, completing the LAN setup.

Follow these steps to configure the connection:

- Open the iO Platform web interface.
- Click on Settings.
- Click on Connections.
- Select ETH-2 – 100 Mbps.
- Enable the port.
- Leave the MTU at 1500, unless otherwise specified by your network administrator.
- Leave the speed setting at Auto, unless otherwise specified.
- Click on Mode, and change it from DHCP to Static.
- Enter the following network information:
    - IPv4 Address
    - IPv4 Subnet Mask
    - IPv4 Gateway.

⚠️ **Note:** Ensure that all equipment to be connected to the iO device is configured within the same IP subnet.

- Click Save.
- Reboot the iO Platform device (a Reboot button will appear in the top header).

Multitel

2.IO SETUP

2.1 USERS AND ACCESS LEVELS

User accounts and access levels can be viewed and configured under the Security section within the Settings module.

The iO device supports three types of authentications:

- **LOCAL**: The local authentification allows the creation of users and assignment of access levels directly to the security parameters in the device.
- **LDAP**: The LDAP authentication protocol is used to authenticate users via the customer's LDAP directory. For LDAP users, all account management actions, except deletion, must be performed directly through the customer's LDAP system.
- **RADIUS**: The Radius authentication protocol is used to authenticate users via the customer's Radius directory. For Radius users, all account management actions, except deletion, must be performed directly through the customer's Radius system.

2.1.1 USER INFORMATION

2.1.1.1 User Creation

This section explains how to create new user accounts on the iO Platform. Depending on the assigned group (e.g., Supervisor, User, Viewer), users will have different levels of access to the platform's features. Proper user configuration ensures that only authorized personnel can access or modify system settings and monitored data.

Follow the instructions to create users, assign roles, and configure authentication details securely and effectively.

- Click on Settings.
- Click on Security.
- In the Users Tab, click + User.
- Complete the fields according to the table below.

Table 4: User Information

Field	Description	Specification	Required
Username	The unique name used by the user to logging in to the device.	Alphanumeric, 1-50 characters	Yes
Email	The user's email address.	Valid email format (e.g., user@example.com)	No
Phone	The user's phone number.	Alphanumeric, 1-50 characters	No
Function	The user's job title or role (e.g., Technician, Manager).	Alphanumeric, 1-50 characters	No

Groups	Defines the user's permission level by assigning to one group. • Supervisor • User • Viewer • Contractor	Single-Select Dropdown	Yes
Authentication	Indicates the authentication method used by the user (e.g., Local, LDAP or Radius)	System-generated: LOCAL/LDAP/RADIUS	Auto
Password	Defines the user's password.	Password must be at least eight characters long.	

2.1.1.2 Password Reset

Only users assigned to the Supervisor group can reset the password of local users.

⚠ **Warning:**
If a user with Supervisor-level access resets a password or changes another user's username, the updated credentials must be communicated manually to the affected user. The system does not send automatic notifications.

Users assigned to the User or Viewer groups can only reset their own password via the User Profile interface.

To access the User Profile:
- Click the iO logo in the header bar.
- Select User Profile.

2.1.1.3 User Status: Enable or Disable

Disabling a user removes their access to the iO Platform interface.

To enable or disable a user:
- Go to the Users page.
- Toggle the switch in the State column.
  - : User is enabled
  - : User is disabled

2.1.1.4 User Status: Delete

To delete a user:
- Select the user to be deleted.
- Click on Delete and confirm the action.

⚠ **Note:**
The default user Administrator cannot be deleted or disabled.

⚠ **Note:**
The inactive timeout is set to 30 minutes.

2.1.2 LDAP

The iO Platform supports LDAP authentication, allowing centralized user access management through your organization's directory services. This section outlines how to configure the LDAP settings on the device.

To configure LDAP:

- Click on *Settings*.
- Click on *Security*.
- Click on *LDAP* tab.
- Enable LDAP by toggling the Global Settings switch to ON.

Table 5: LDAP Configuration

Field	Description	Specification	Required
Port	LDAP Server Port (e.g., 389 for LDAP, 636 for LDAPS)	Alphanumeric, 1-50 characters	Yes
Timeout	Set the connection timeout	Dropdown: • 5 sec • 10 sec • 30 sec • 1 min	Yes
Login Pattern	Define the LDAP login query	Alphanumeric, 1-128 characters	No
Secured Connection Type	Choose between LDAP and LDAPS	Dropdown • None • LDAPS/SSL	Yes
Trusted Certificate Authority Key	Only for LDAPS		Yes
User Search Base DN	The base distinguished name to start the user search (e.g., ou=users,dc=example,dc=com)		Yes
Username Attribute	The LDAP attribute used for the login (e.g., uid or sAMAccountName for Active Directory)		Yes
Login	Distinguished Name (DN) of the service account		Yes
Password	Password for the service account		Yes
Host	Hostname or IP address of the LDAP server		Yes
Groups	Distant Group DN (LDAP Group)	e.g., cn=contractors, ou=groups,	Yes

		dc=example, dc=com	
First Name	LDAP user attributes	e.g., givenName	No
Last Name	LDAP user attributes	e.g., sn	No
Email	LDAP user attributes	e.g., mail	No
Phone	LDAP user attributes	e.g., telephoneNumber	No

Once all fields are completed:

- Click Save to apply the configuration.
- You may also use Cancel to discard any changes.

LDAP Login Behavior:

- Once LDAP is enabled and configured correctly, users can log in using their domain credentials.
- Access rights are automatically granted based on group mappings.
- Password management is handled externally via your LDAP system.

2.1.3 RADIUS OVERVIEW

RADIUS (Remote Authentication Dial-In User Service) is a standardized networking protocol used for Authentication, Authorization, and Accounting (AAA).

RADIUS enables centralized access management for infrastructure such as:

- Wi-Fi networks (WPA2/WPA3-Enterprise)
- VPN connections
- Wired access (802.1X)
- Network devices (routers, switches, firewalls)

General Operation:

- Authentication – Verifies the user's identity (username/password, certificate, token, etc.).
- Authorization – Assigns access rights (VLAN, policies, privilege levels).
- Accounting – Logs session details (duration, traffic usage, status).

The protocol typically operates over UDP using ports 1812 for authentication and authorization, and 1813 for accounting. It relies on a shared secret between the RADIUS client, also known as the NAS (Network Access Server), and the RADIUS server to secure communications.

2.1.4 RADIUS CONFIGURATION

To configure Radius:

- Go to *Settings*.
- Go to *Security*.
- Click on *Radius* tab.
- Enable Radius by toggling the switch to ON.

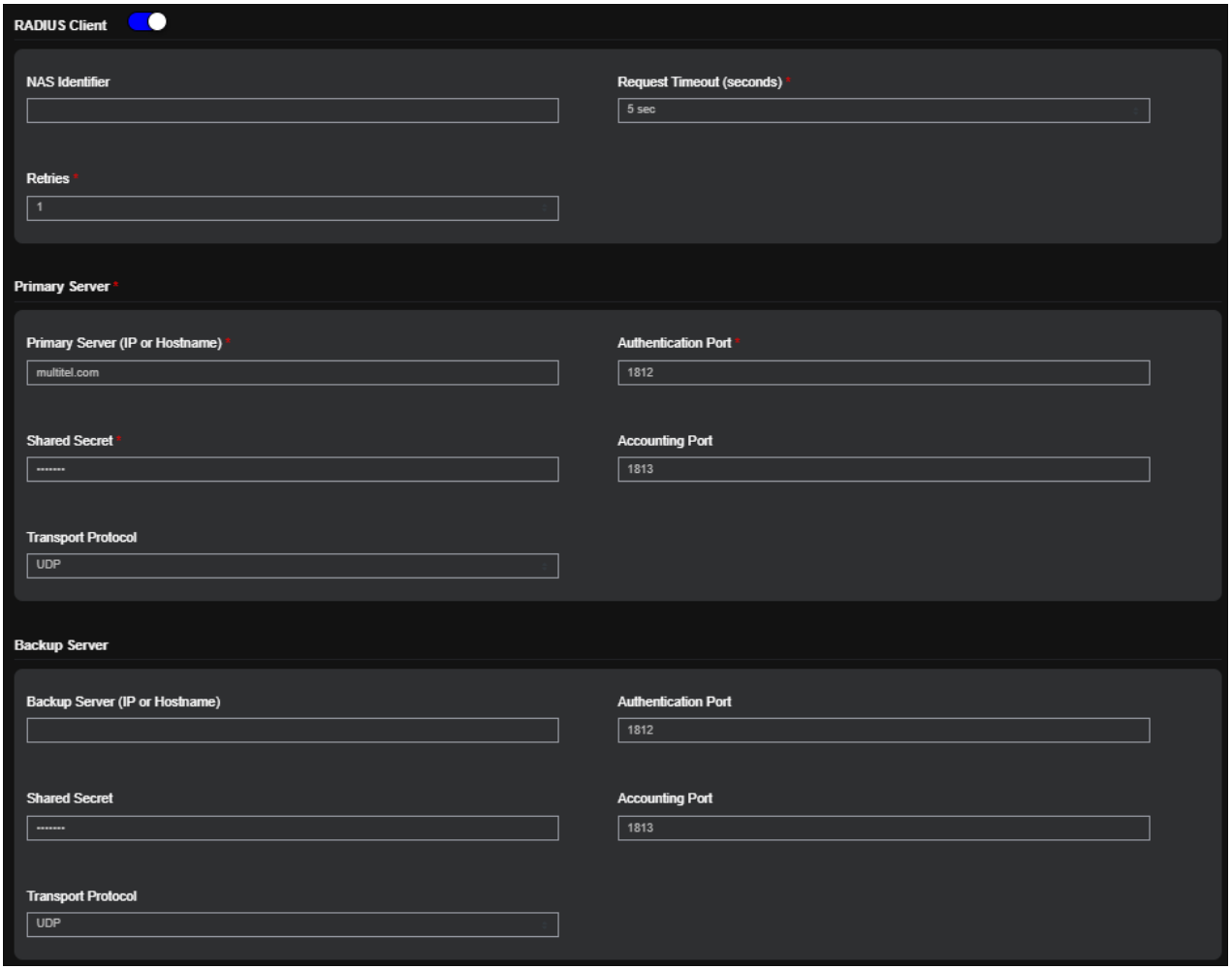


Figure 7: Radius – Configuration

Table 6: Radius – Configuration

Field	Description	Specification	Required
RADIUS Client State	Allows to enable or disable an external RADIUS server.	Switch	Yes
NAS Identifier	Unique identifier of the Radius client (Network Access Server). This identifier is sent to the Radius server in authentication and accounting requests.	1 to 50 characters	No
Request Timeout	Maximum time (in seconds) the system waits for a response from the Radius server before the request times out.	Dropdown: • 1 sec • 2 sec • 3 sec (default) • 4 sec • 5 sec	Yes
Retries	Number of attempts performed if no response is received from the Radius server.	Dropdown: • 1 • 2 (default) • 3	Yes

		• 4 • 5	
Primary Server (IP or Hostname)	IP address or DNS hostname of the primary Radius server.	0.0.0.0 to 255.255.255.255 or hostname	Yes
Primary Authentication Port	UDP port used for Radius authentication requests.	1 to 65535 Default: 1812	Yes
Primary Shared Secret	Shared secret key between the Radius client and the server.	1 to 50 characters encrypted	Yes
Primary Accounting Port	UDP port used for Radius accounting messages (session logging).	1 to 65535 Default: 1813	No
Primary Transport Protocol	Protocol used to communicate with the Radius server.	Dropdown: • UDP (default)	Yes
Backup Server (IP or Hostname)	IP address or DNS hostname of the secondary Radius server.	0.0.1.0 to 255.255.255.255 or hostname	No
Backup Authentication Port	Authentication port of the secondary server.	1 to 65535 Default: 1812	No
Backup Shared Secret	Shared secret key shared with the secondary server.	1 to 50 characters encrypted	No
Backup Accounting Port	Accounting port of the secondary server.	1 to 65535 Default: 1813	No
Backup Transport Protocol	Protocol used to communicate with the secondary server.	Dropdown: • UDP (default)	Yes

During the RADIUS configuration, the primary and backup server connections can be tested.

To test the RADIUS server connections:

- Enter the username of a RADIUS user
- Enter the password of the RADIUS user
- Click the *TEST PRIMARY SERVER CONNECTION* button
- Click the *TEST BACKUP SERVER CONNECTION* button if the Backup server is configured

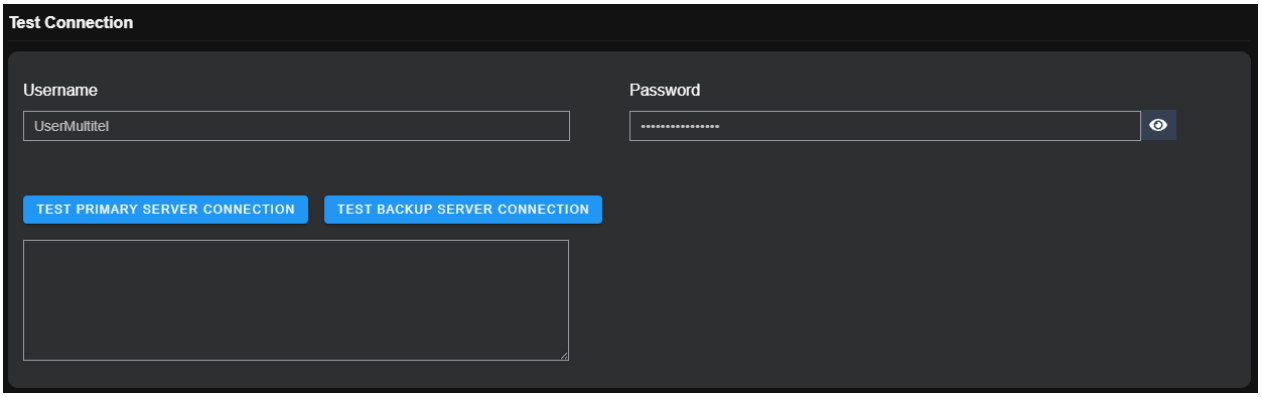


Figure 8: Radius – Test Connection

2.1.5 ACCESS LEVEL

The table below outlines the access permissions associated with each user group for various functionalities of the iO Platform. Each group (Supervisor, User, Viewer, Contractor) is granted either full editing rights or read-only access depending on their role and the functionalities.

Table 7: Access Level

Functionalities	Group	Permission Level
Settings	Supervisor	Edit
	User	Read-only
	Viewer	No access
	Contractor	Read-only access to: – General Parameters – Inventory – Units – Labels – Notifications
Asset	Supervisor	Edit
	User	Edit
	Viewer	Read-only
	Contractor	Read-only
HMI	Supervisor	Edit
	User	Read-only
	Viewer	Read-only
	Contractor	Read-only
Alarms	Supervisor	Edit
	User	Read-only
	Viewer	Read-only
	Contractor	Read-only
IO Channel	Supervisor	Edit
	User	Read-only
	Viewer	Read-only
	Contractor	Read-only
Passthrough	Supervisor	Edit

	User	Edit
	Viewer	Read-only
	Contractor	Edit
Trap Forwarding	Supervisor	Edit
	User	Edit
	Viewer	Read-only
	Contractor	Read-only

2.2 GENERAL PARAMETERS

General Parameters is one of the first steps required when setting up an iO device. Located under Settings, the General Parameters section is divided into the following sections:

- Site Information
- System Information
- Date and Time

2.2.1 SITE INFORMATION

The Site Information section allows users to define and document key details about the physical location where the iO device is deployed. This includes the site name, CLLI code, and the full location address (country, province/state, city, postal code, and NPA). Additionally, users can upload a site picture for quick visual identification.

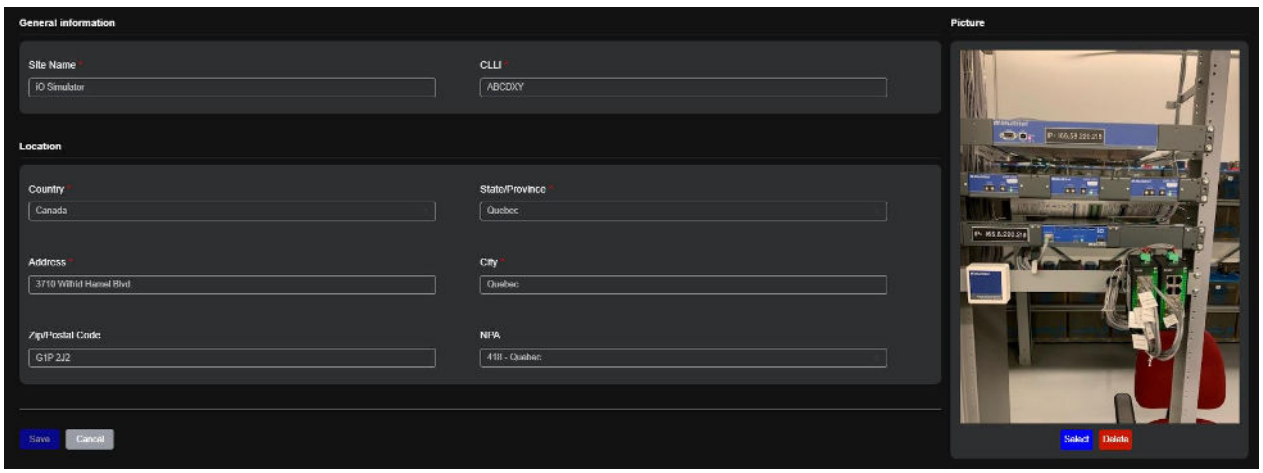


Figure 9: Site Information

2.2.1.1 General Information

The Site Name configured in the General Information section is used to identify the physical location of the iO device. This name will be displayed in the header of the web interface.

Figure 10: Site Name in Header

The CLLI can also be configured and will appear on the login page, along with the Site Name.

Figure 11: Site Name and CLLI in Login Page

2.2.1.2 Location

Table 8: Location

Field	Description	Specification	Required
Country	Country location of the iO	Dropdown: • Canada • United States	Yes
State/Province	List of states or provinces	Dropdown	Yes
Address	Site Address	Alphanumeric, 1-100 characters	Yes
City	Site City	Alphanumeric, 1-50 characters	Yes
Zip/Postal Code	Site Zip/Postal Code	Valid Postal Code and Zip format	Yes
NPA	Site NPA	Dropdown	Yes

2.2.2 SYSTEM INFORMATION

2.2.2.1 System Resources

The following information is available in the System section:

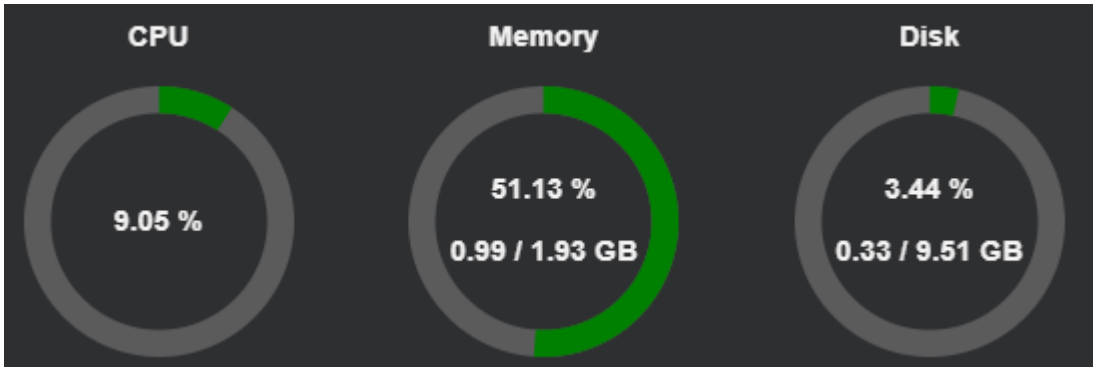


Figure 12: iO System Resources

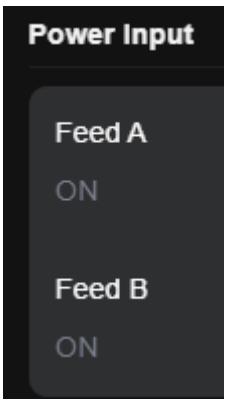


Figure 13: Power Input

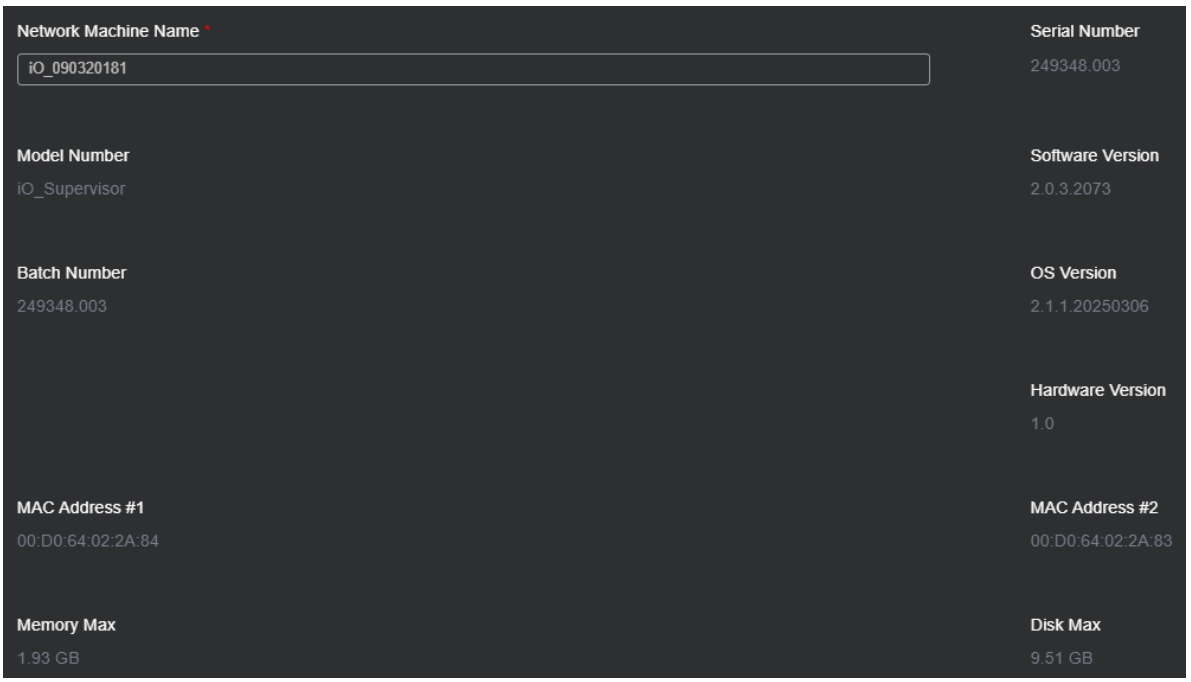


Figure 14: About Section

Table 9: About Section Details

Field	Description
Network Machine Name	A unique label that distinguishes the device from others on the network.
Serial Number	A unique identifier assigned by Multitel manufacturing team used to track and identify the specific unit.
Model Number	An identifier denoting the product line or design variation.
Software Version	A label that indicates the release version of the iO Platform on the device.
Batch Number	An identifier assigned by Multitel manufacturing team used to track and identify the specific unit.
Hardware Version	A label that indicates the hardware version of the device.
MAC Address #1	A unique identifier for the ETH-1 network interface.
MAC Address #2	A unique identifier for the ETH-2 network interface.
Memory Max	The maximum amount of memory (RAM) that the device can support.
Disk Max	The maximum storage capability of the device.

2.2.3 DATE AND TIME

The date and time are configured in the General Information section. The first part displays the current system time (UTC) while the unit's time zone can also be configured.

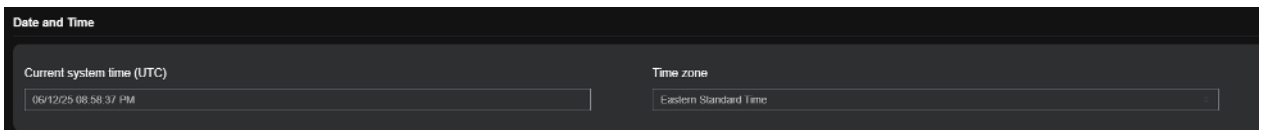


Figure 15: Date and Time

2.2.3.1 NTP

The NTP section is used to automatically synchronize the iO clock using Network Time Protocol (NTP). When enabled, the device periodically updates its system time based on the configured NTP servers to maintain accurate timestamps for logs, alarms, and data history.

To enable NTP synchronization:

- Go to **Settings**
- Go to **General Information**
- In the **Date and Time** section, enable **Set automatically**
- Configure the NTP servers (recommended: fill all three for redundancy)

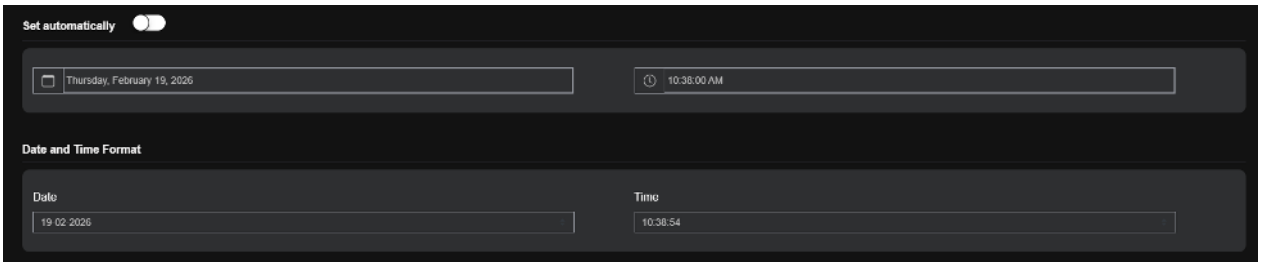
NTP server fields

- Primary NTP server
  - Main time source used by the iO.

- Secondary NTP server
  - Backup time source used if the Primary server is not reachable.
- Tertiary NTP server
  - Additional backup time source used if the Primary and Secondary servers are not reachable.

Failover behavior
Upon power-up, the iO attempts to synchronize using the **Primary NTP server**. If the Primary server does not respond, the device automatically attempts the **Secondary**, followed by the **Tertiary** server.

2.2.3.2 Manual



The Manual section is used to configure the iO date and time without using NTP.
To configure the date and time manually:

- Go to **Settings**
- Go to **General Information**
- In the **Date and Time** section, disable **Set automatically**
- Configure the values below:
  - **Date**: Select or enter the date using the calendar control
  - **Time**: Enter the time using the time field

Note: When Set automatically is disabled, the iO no longer synchronizes its clock with NTP servers. Manual time should be used only when NTP is not available or when the system requires a fixed time for testing or commissioning. An incorrect date/time can impact logs, alarms, and historical data timestamps.

2.2.3.3 Date and Time Format

- Date formats available
  - MM/DD/YY
  - MM/DD/YYYY
  - DD/MM/YY
  - DD/MM/YYYY
  - MM-DD-YY
  - MM-DD-YYYY
  - DD-MM-YY
  - DD-MM-YYYY

- Time formats available
  - HH:MM:SS AM/PM
  - HH:MM:SS
  - HH:MM AM/PM

Note: When Set automatically is disabled, the iO no longer synchronizes its clock with NTP servers. Manual time should be used only when NTP is not available or when the system requires a fixed time for testing or commissioning. An incorrect date/time can impact logs, alarms, and historical data timestamps.

2.3 EXP I/O CARDS (HYBRID CARDS) –FOR IO SUPERVISOR ONLY

Table 10: EXP I/O Cards

Main Card	Aux Card	Analog Input	Humidity	Binary Input	Binary Output Form-C	Binary Output Form-A
EXP1	None	4x Hybrid	1	13	3	0
EXP1	EXP2	10x Hybrid	1	29	3	3
EXP1	EXP3	4x Hybrid	1	45	3	0
EXP1	EXP4	4x Hybrid	1	41	3	3
EXP3	None	0	0	32	0	0
EXP3	EXP3	0	0	64	0	0
EXP3	EXP4	0	0	60	0	3
EXP4	None	0	0	28	0	3
EXP4	EXP4	0	0	56	0	6

2.4 ANALOG INPUT DATA POINTS

Analog input data points are used for various types of measurements. Some measurements may require a specific transducer to convert a physical phenomenon into an analog signal. Other measurements, such as battery voltage, do not require a transducer and can be wired directly to an analog input data point.

The iO Supervisor is designed to easily and efficiently support a wide range of measurements through its hybrid front-end analog input channels. For each analog input, the front-end configuration is user-selectable based on the requirements of the measurement signal.

- ±50mV for shunt DC current measurement
- Temp for temperature measurement
- 0-65Vdc for DC voltage measurement and ±65Vdc for the SMX-24AI
- 23Vrms for AC voltage measurement
- 0-10Vdc for DC voltage measurement and ±10Vdc for the SMX-24AI
- 1.4Vrms for AC current measurement

Analog channels are found on the EXP1, EXP2 and SMX-24AI modules. They share the same electronic design, and all channels provide identical technical specifications and configurable operating parameters.

The only exceptions are as follows:

- FIAi5, which is restricted for humidity measurement.
- 65Vdc and 10Vdc front-end on the EXP1 and EXP2 are unidirectional where on the SMX-24AI are polarized, meaning ±65Vdc and ±10Vdc.

⚠ **Note:**
Ambient humidity level measurement is done using a specific transducer available through Multitel.

Table 11: Analog Input Data Point Front-End

Measurement Type	Front-End	Transducer	Scale
DC voltage such as DC system voltage, 12Vdc battery jar, generator start battery voltage, etc.	0-65Vdc	Not applicable – For iO only	65
	±65Vdc	Not applicable – For SMX-24AI only	65
DC voltage from 2V cells	0-10Vdc	Not applicable – For iO only	10
	±10Vdc	Not applicable – For SMX-24AI only	10
Used for 10V output signal from various types of transducers liquid level, DC or AC Current	10Vdc	Various yhird-party transducers	Transducer value
DC Current for branch circuit monitoring of PDF and DC distribution feeds, individual battery string charging and discharging current, etc.	±50mV	Shunts	Shunt Value
	10Vdc For 0-4Vdc CT	DC Current Transducer (±50A)	125
		DC Current Transducer (±100A)	250
		DC Current Transducer (±250A)	625
		DC Current Transducer (±500A)	1250
AC Voltage on single phase 120/240 Vac or three phase 208 Vac systems using SDTA from Multitel	23Vrms	SDTA-01 (240Vac)	2680
		SDTA-02 (240Vac/600Vac)	2680/6700
AC Current using CT providing 0-333mVrms output signal	1.4Vrms for 0.333mV AC Current CT	AC Current Transformer (50A)	595
		AC Current Transformer (100A)	1189
		AC Current Transformer (200A)	2378
		AC Current Transformer (400A)	4757
		AC Current Transformer (600A)	7135
		AC Current Transformer (1500A)	17835
		AC Current Transformer (2000A)	23783
Ambient, indoor, exterior temperatures	Temp	Temperature Probes (M-4103, M-4107, M-4109, M-4111, M-4115)	120
Ambient relative humidity	Humidity	Humidity Probe (M-4109) – F1Ai5 Only	100

Float Charging Current for thermal runaway	±50mV	FCCP-01 (Float Charging Current Probe)	5

2.4.1 ANALOG INPUT OPERATION (HYBRID)

Each analog input data point is wired to the back panel. The iO Supervisor is continuously monitoring the voltage level between each analog channel and its reference value (see figure below). One or more software thresholds can be associated to each channel in order to generate alarms or enable controls.

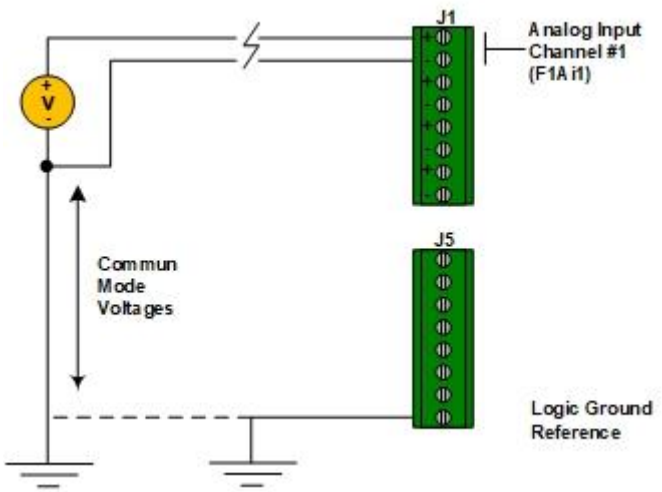


Figure 16: Analog Input – Connection

⚠ Note:
Respect the polarity for each analog input data point for values to display correctly. Pay particular attention to -48Vdc voltage measurement.

2.4.2 ANALOG INPUT CONFIGURATION

The analog input data points are displayed in the IO Channel section of the menu.

The analog input section displays all analog input data points available in the iO Supervisor.

Multitel

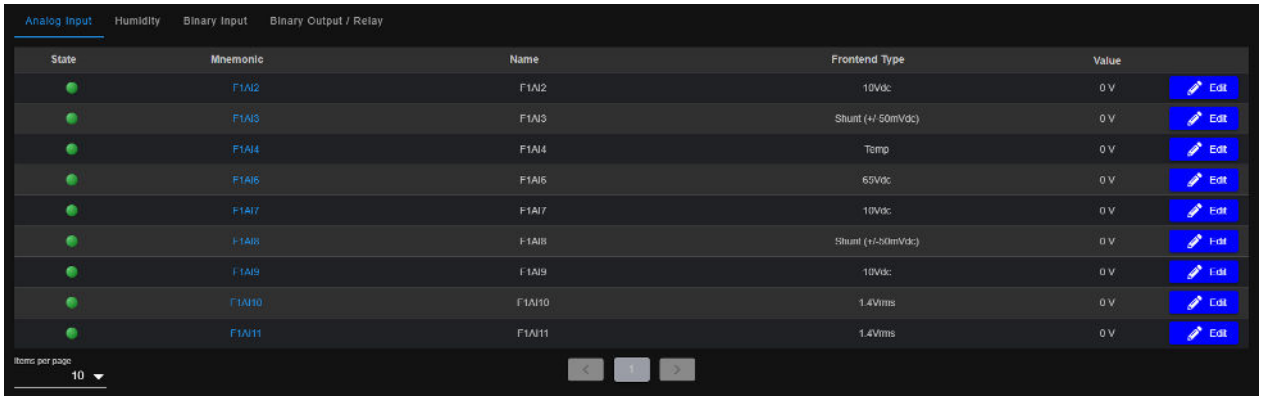
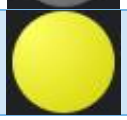


Figure 17: Analog Input – IO Channel

The **state** column gives the user a visual representation of the data point state.

Table 12: IO Channel State

State Color	State	Description
	Enable	Acquisition is working.
	Disable	Data Point is disabled.
	Partial Success	Applicable at the asset level: data points acquisition error of the asset is below 50%.
	OVL+, OVL-	Overload over and under
	Partial Failure	Applicable at the asset level: data points acquisition error of the asset is over 50%.
	Not-yet-available	First acquisition of the data point is not complete. Could be due to a communication error or if the asset is disabled.
	Status-not-available	Error in the communication.
	Status config error	Displayed when a datapoint cannot get a value because of a misconfiguration. Mainly happens to computed datapoints when there is an error in the l=Lua script.
	Status Suspended	The Suspended status occurs when an asset has reached its configured Number of Retry, has waited for the defined Timeout After Retry, and has completed the specified Total Iteration Number without successful communication. When all retry attempts and configured waiting periods have been exhausted, the asset is automatically placed in Suspended status to indicate that

		communication has failed under the current configuration.

The mnemonic is a unique identifier in the iO. The analog input data point uses the following format:

- F1AIx
  - F: Identifier for IO Channel.
  - 1: Identifier for IO Channel.
  - AI: Analog Input.
  - x: 1 to 11 (Data point number).

To configure the analog input data point, the user can click on Edit on the right side of the data point.

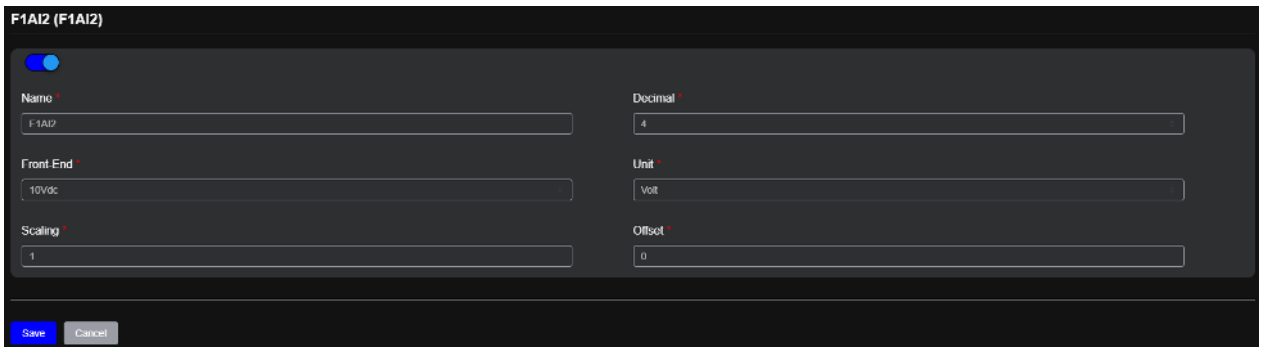


Figure 18: Analog Input – Configuration

A list of possible programmable parameters will be displayed.

Table 13: Analog Input – Configuration

Field	Description	Specification	Required
Name	Analog input data point name	Alphanumeric, 1-50 characters	Yes
Decimal	Decimal value used to display the value of the data point. The decimal will round up the value of the data point.	Dropdown	Yes
Front-End	Front-end type: • Shunt (±50mVdc) • Temp • 65Vdc • 23Vrms • 10Vdc • 1.4Vrms	Dropdown Default value: Shunt (±50mVdc)	Yes
Unit	Unit value of the data point. If Temp front-end is selected, only Celsius or	Dropdown	Yes

	Fahrenheit is available. The temp value will be converted automatically,		
Scaling	Scaling factor	1 to 65 535 (16bit)	Yes
Offset	Offset factor	±1.79 E+308	Yes

2.4.3 ANALOG INPUT DAILY VALUES

Analog Input Daily Values are summary data points automatically calculated from a data point's values over the course of a day. They are used to view daily behavior and trends without having to analyze high-frequency history.

2.4.3.1 Accessing the Daily Values page

In the **Analog Input** section, click the blue mnemonic (for example F1AI1) to open the Data Point Details page for the analog input and to view its Daily Values.

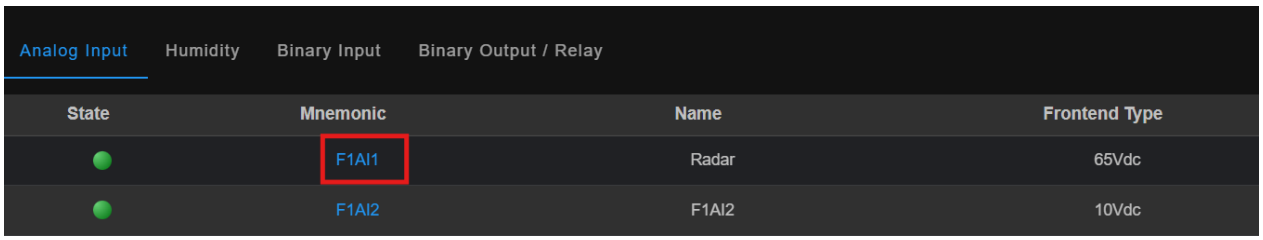


Figure 19: Analog Input – Daily Values

2.4.3.2 Availability across the platform

Daily Values are not unique to F1AIx (IO Channel) analog inputs. They are available for all analog data points in the platform including:

- Internal data points (computed)
- Communication Protocols data points such as SNMP and Modbus

In other words, any analog measurement supported by the platform can provide Daily Values, regardless of its source.

2.4.3.3 Daily Values Page

After clicking the blue mnemonic, the platform opens the Data Point Details page for the selected analog data point.

This page provides key elements:

- **Peaks**: The Peaks table lists the Minimum and Maximum values recorded for the selected period (up to 365 days). For each peak, the platform also shows the date and time when it occurred. This allows for quick identification of when the lowest or highest reading occurred.
- **Daily Values Chart**:

The chart displays the daily statistics over time:

- Average (daily average value)
- Max (daily maximum value)
- Min (daily minimum value)

Hovering your mouse over the chart shows a tooltip with the Avg / Max / Min for the selected day, allowing for quick day-by-day comparison and trend analysis.

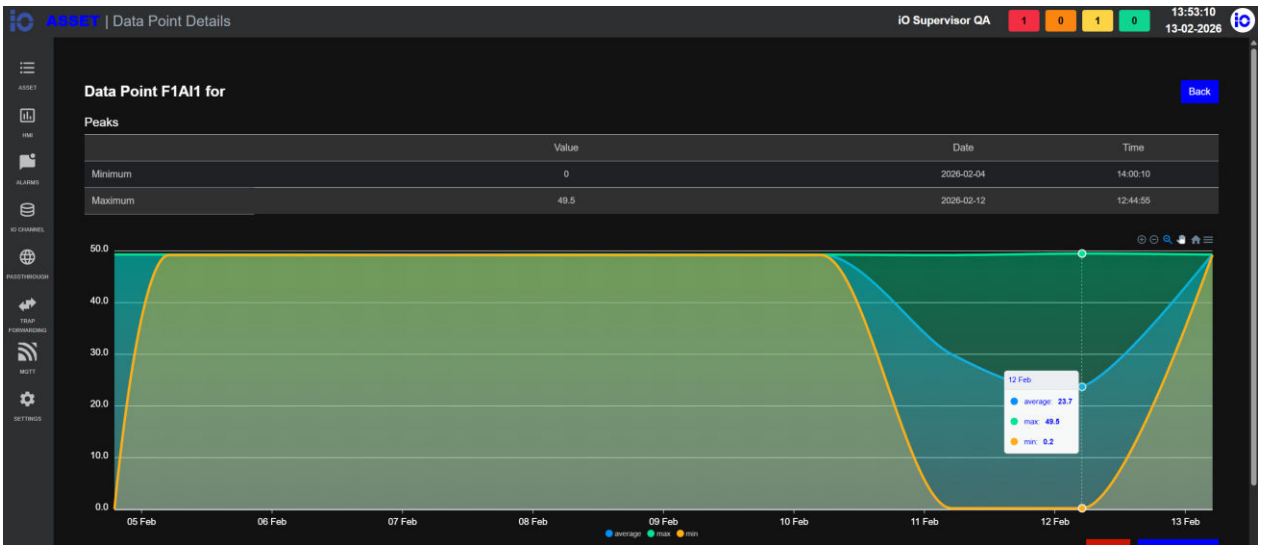


Figure 20: Analog Input – Daily Values Peaks and Chart

- **Daily Values Table**

  The chart displays the daily statistics over time:

  - **Date**: Day for which statistics were calculated.
  - **Average**: Average value recorded during the day.
  - **Delta**: Difference between the daily Maximum Value and Minimum Value (Max − Min). This indicates signal variation during the day.
  - **Minimum Value**: Lowest value recorded during the day.
  - **Time (Min):** Time when the Minimum Value occurred.
  - **Maximum Value:** Highest value recorded during the day.
  - **Time (Max):** Time when the Maximum Value occurred.

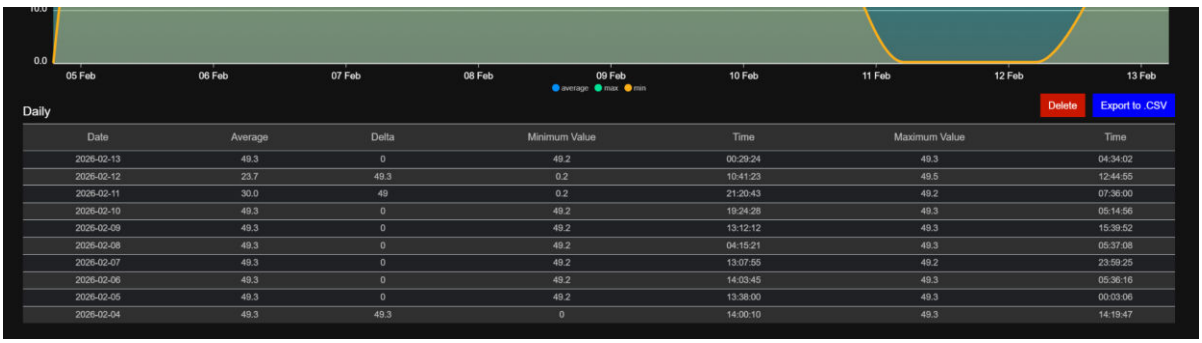


Figure 21: Analog Input – Daily Values Table

- **Export**: Download the Daily table to a CSV file for reporting or further analysis (Excel, BI tools, etc.).
- **Delete**: Removes the entire record (useful for cleanup after commissioning/tests or when invalid data must be discarded).

⚠ **Note:** Deleting daily records impacts the historical daily summary for the data point. Use with caution and according to your data retention policy.

2.4.3.4 Daily Values General Information

- Daily values are calculated using the data point's configured parameters (unit, scaling, offset, decimals, etc.).
- Daily values are read-only data points.
- At the beginning of each day, the daily values are reset and start accumulating new statistics for the current day.

⚠ **Note:** If a data point is Disabled, in Status-not-available, or has overload (OVL+/OVL-), its daily values may be incomplete or unavailable for that day.

2.5 BINARY INPUT DATA POINTS (EXP1, EXP2, EXP3, EXP4)

Different terminology is used to refer to binary input data points, such as Dry-C, Discrete, Alarm, and Event Channels. These channels are used to detect on-off status changes (e.g., door open, rectifier failure, AC outage, HVAC on, etc.). Most monitored equipment or systems can operate a relay to generate a dry contact alarm when a change in operation occurs. The iO's binary inputs are used to detect change in equipment or system operation.

Normally, a relay contact sends a ground signal to a specific binary input channel, and the iO Supervisor detects this ground signal to trigger an action based on pre-programmed conditions. For certain types of detections (e.g., smoke/fire, open door, water presence, etc.), transducers should be used to perform these tasks. A wide variety of sensors, probes, and transducers are available directly from Multitel.

Each binary input is individually programmable. Grouping functions, alarm severity levels, history log files, and many other features make the iO Supervisor a powerful tool for managing telecommunication site infrastructure alarms. The iO Supervisor and the SMX-48BI binary input channels share the same electronic design, technical specifications, and operating parameter setup.

2.5.1 BINARY INPUT OPERATION

The iO Supervisor continuously monitors the voltage level between each Binary Input data point and the Logic Ground reference. When the voltage is within the “voltage level range” of the selected “activation level”, the Binary Input data point state will change and its corresponding triggering source will turn on.

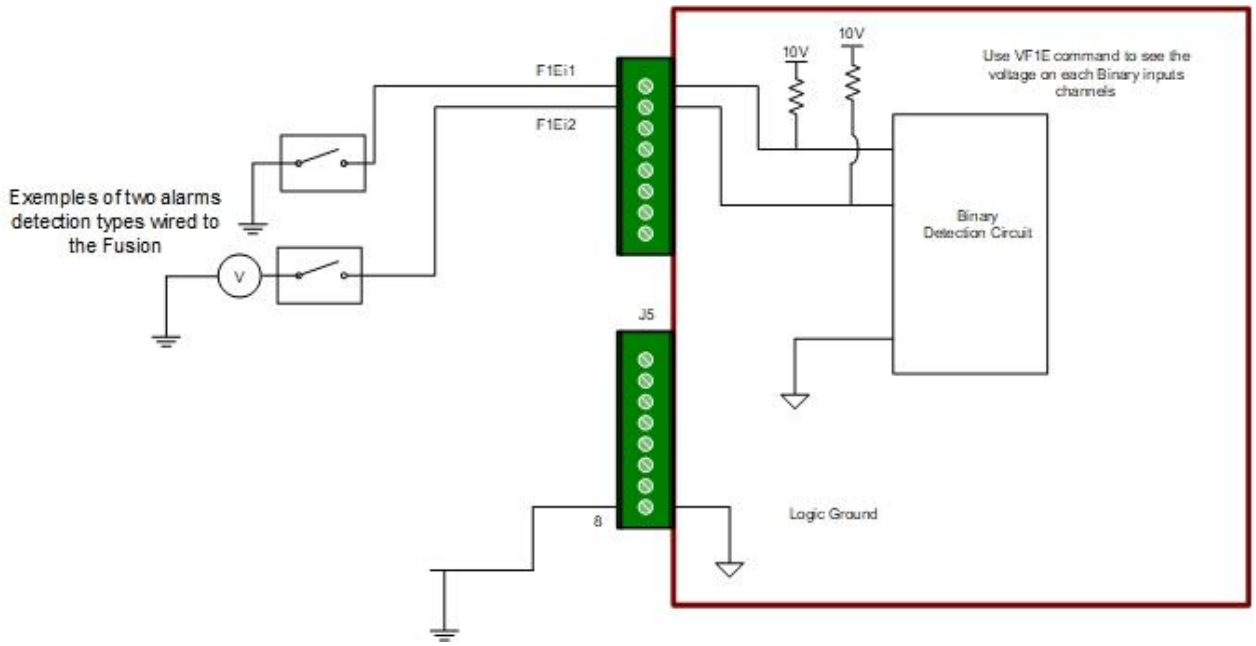


Figure 22: Binary Input – Configuration

The iO Supervisor provides between 13 and 64 binary input data points depending on installed EXP I/O cards.

Multitel

2.5.2 BINARY INPUT CONFIGURATION

The binary input data points are displayed in the IO Channel section of the menu.

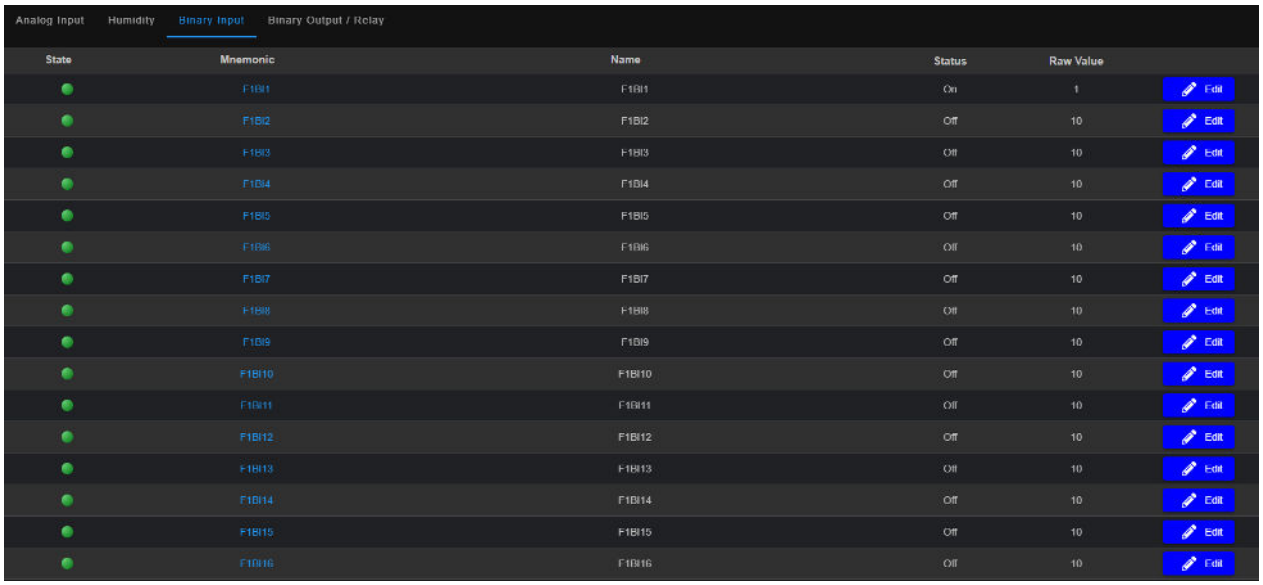


Figure 23: Binary Input – IO Channel

The mnemonic is a unique identifier in the iO. The binary input data point uses the following format of F1Bix:

- F: Identifier for IO Channel.
- 1: Identifier for IO Channel.
- BI: Binary Input.
- x: 1 to 64 (Data point number).

To configure the binary input data point, the user can click on **Edit** of the right side of the data point.

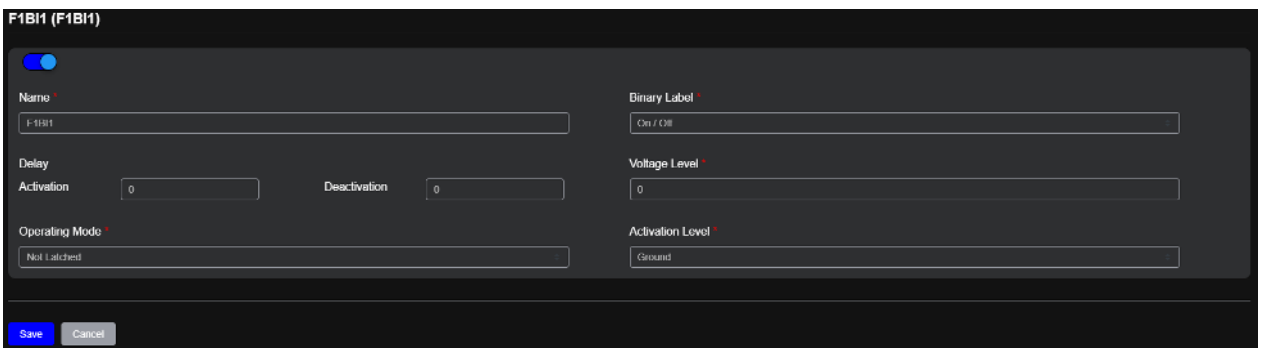


Figure 24: Binary Input – Configuration

A list of possible programmable parameters will be displayed.

Multitel

Table 14: Binary Input - Configuration

Field	Description	Specification	Required
Name	Binary input data point name.	Alphanumeric, 1-50 characters	Yes
Binary Label	Label used to display true or false values.	Dropdown	Yes
Activation Delay	Pre-set time used to delay the input activation, counting starts on a rising edge of the input.	0 to 999 seconds	Yes
Deactivation Delay	Pre-set time used to delay the input de-activation, counting starts on a falling edge of the input.	0 to 999 seconds	Yes
Voltage Level	Voltage input level.	0 to 70V (absolute)	Yes
Operating Mode	The activation level enables the user to select between Ground or Battery levels.	Dropdown	Yes
Activation Level	The activation level enables the user to select between Ground or Battery levels.	Dropdown	Yes
Operating Mode	Only unlatched mode is available.	Dropdown	Yes

Activation level margins:

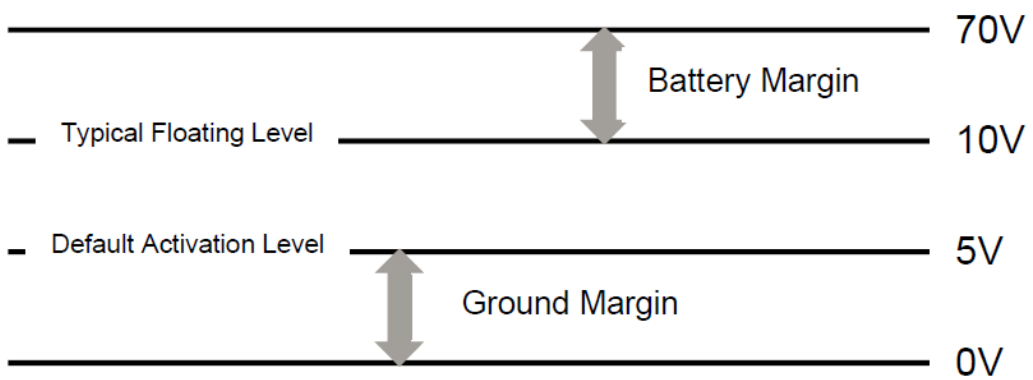


Figure 25: Binary Input – Activation Level

Each binary input is terminated at the rear panel of the iO Supervisor. An alarm can be triggered when the connection between the equipment or sensor and the iO binary input channel is opened.

2.5.3 BINARY INPUT LOGS

Binary Input Logs provide a historical view of state transitions (True/False) for a binary input data point. They are used to validate alarm activity, confirm event timing, and troubleshoot intermittent issues without relying on real-time monitoring.

2.5.3.1 Accessing the Binary Input Logs Page

In the Binary Input section, click the blue mnemonic (fe.g., F1BI2) to open the Data Point Details page for the binary input and view its logs (Latest Value Changes).

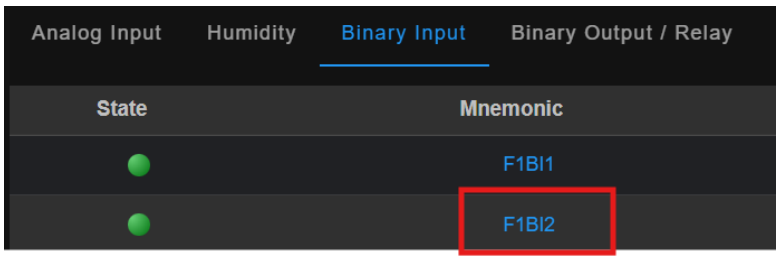


Figure 26: Binary Input – Log Page

2.5.3.2 AvailabilityAcross The Platform

Binary Input Logs are not unique to F1BIx (IO Channel) binary inputs. Log/history views are available for binary status data points across the platform, including:

- Internal binary data points (computed).
- Communication protocol data points such as SNMP and Modbus (when the data point is a binary).

In other words, any binary (true/false) data point supported by the platform can provide logs, regardless of its source.

2.5.3.3 Binary Input Log Page (Data Point Details)

After clicking the blue mnemonic, the platform opens the Data Point Details page for the selected binary input data point.

This page provides the following key elements:

- **Latest Value Changes (log table):**

This table lists the most recent state changes detected for the binary input. The log is a rollover table that stores and displays the last 500 events. Once the limit is reached, the oldest entries are overwritten.

Each entry includes:

- Status: The recorded state (True/False)
- Date: Date when the change occurred
- Time: Time when the change occurred

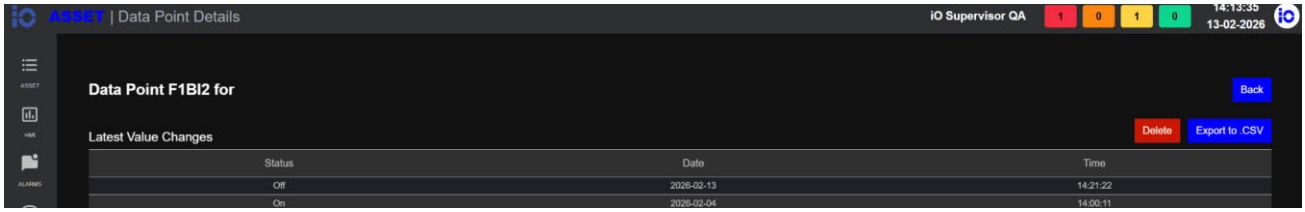


Figure 27: Binary Input – Latest Value Changes Table

- **Export:** Downloads the log table to a CSV file for reporting or further analysis (Excel, BI tools, etc.).
- **Delete:** Clears the log table (useful for cleanup after commissioning/tests or when invalid events must be discarded).

⚠️ **Note:** Deleting log records impacts the historical event traceability for the data point. Use with caution and according to your data retention policy.

2.5.3.4 Binary Input Logs – General Information

- Logs are read-only records generated when the binary input changes state.
- A new log entry is created on each rising edge (False → True) and falling edge (True → False).
- If the Activation Delay and Deactivation Delay are configured, the logged event time reflects the moment the state change becomes valid after the configured delay has elapsed.
- If a binary input is Disabled or in Status-not-available, new log entries may not be recorded.

2.6 BINARY OUTPUT DATA POINTS (EXP1, EXP2, EXP3, EXP4)

Up to six binary output channels (relays) are included, depending on the iO Supervisor model. These binary output channels are used to generate discrete alarms or to control system or equipment operations (e.g., start/stop) using internal relay contact closures. Relay operations can be triggered manually or through a user-programmable triggering equation.

When used for discrete alarms, a Binary Output data point is connected to local alarm or telemetry equipment. This enables alarms generated by the iO Supervisor to be communicated to Network Operations or Surveillance Centers.

Binary Output data points can be used to remotely start and stop other equipment, either manually or automatically. Applications vary widely—from turning on or off rectifiers, converters, or generators, to disconnecting loads in solar applications, or regulating ventilation and HVAC units.

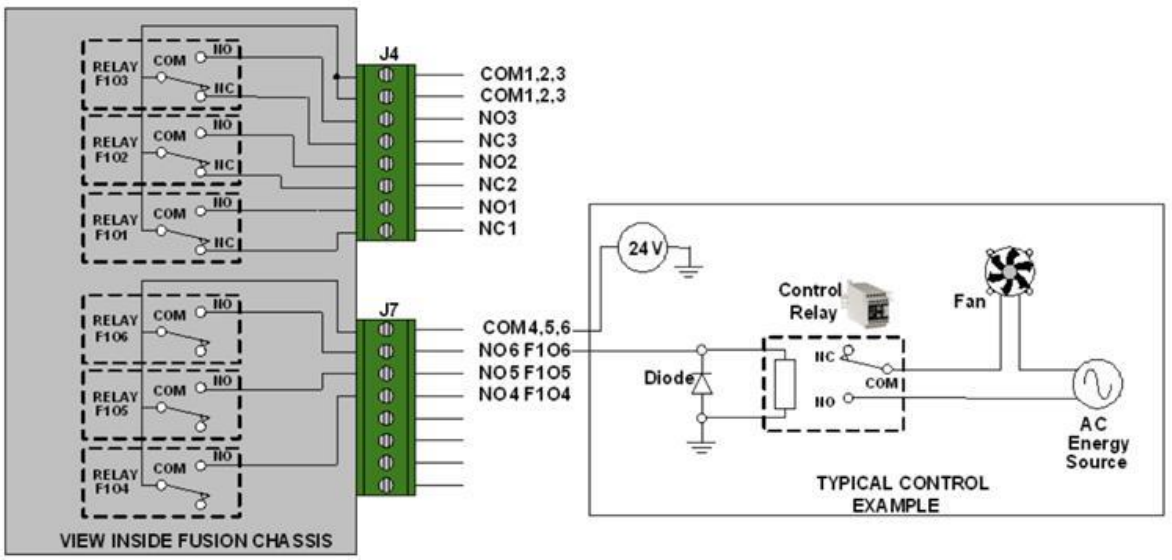


Figure 28: Binary Output – Data Points

2.6.1 BINARY OUTPUT OPERATION

Binary output data points are terminated on the iO Supervisor rear panel. In order to facilitate relay contacts wiring, all relay "common" contacts are bridged together internally.

Available relay contacts:

- 3x Form "C" relays: N.O. and N.C. contacts are available for each relay
- 3x Form "A" relays: only N.O. contacts available for each relay

⚠ **Warning:**
The iO Supervisor uses micro relays, which should be protected with a diode when connected to large inductive loads such as solenoids or control relay coils. Otherwise, the equipment may reset or sustain damage.

2.6.2 BINARY OUTPUT/RELAY CONFIGURATION

The binary output data points are displayed in the IO Channel section of the menu.

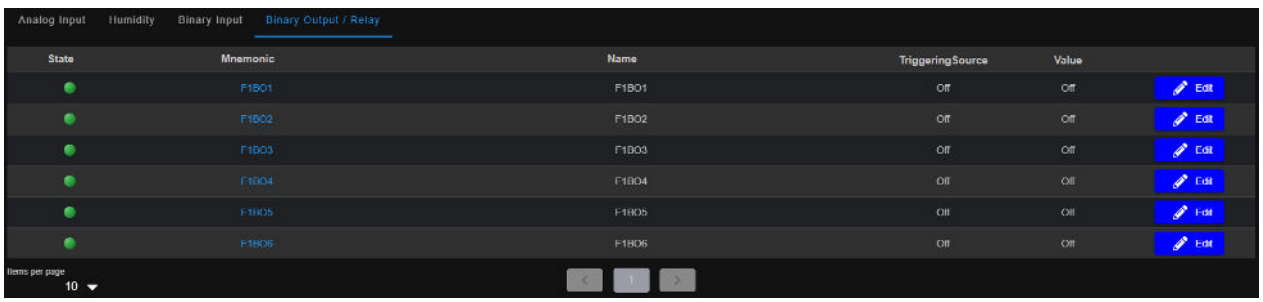


Figure 29: Binary Output – IO Channel

The mnemonic is a unique identifier in the iO. The binary output data point uses the following forma of F1Box:

- F: Identifier for IO Channel.
- 1: Identifier for IO Channel.
- BO: Binary Output.
- x: 1 to 6 (Data point number).

To configure the binary input data point, the user can click on **Edit** of the right side of the data point.

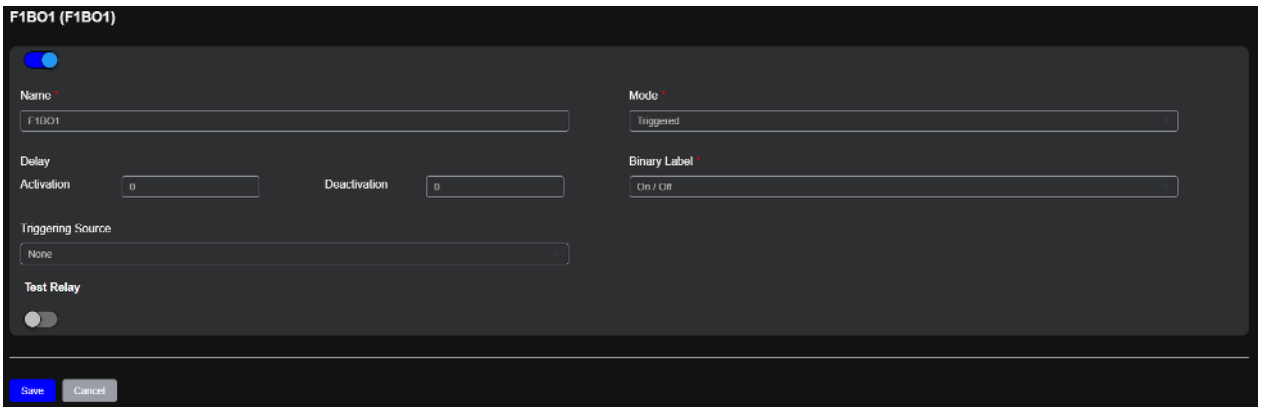


Figure 30: Binary Output – Configuration

A list of possible programmable parameters will be displayed:

Table 15: Binary Output - Configuration

Field	Description	Specification	Required
Name	Binary output data point name.	Alphanumeric, 1-50 characters	Yes
Mode	The operating mode enables the user to select between Triggered and Pulsed operation.	Dropdown	Yes
Activation Delay	Pre-set time used to delay the input activation, it starts counting on a rising edge of the input.	0 to 999 seconds	Yes
Deactivation Delay	Pre-set time used to delay the input de-activation, counting states on a falling edge of the input.	0 to 999 seconds	Yes
Binary Label	Label used to display true or false value.	Dropdown	Yes
Triggering Source	Triggering source used to activate the output data point. All binary data points inside the iO can be used as a triggering source.	Dropdown	Yes
Test Relay	Used to test the output function.	Dongle	Yes

2.6.2.1 Triggering Mode

The output data point becomes active when the triggering equation or source evaluates to TRUE (valid). Activation will be delayed by the configured activation delay time and extended by the pre-set deactivation delay.

For example, if F1BI1 is the triggering source, with an activation delay of 10 seconds and a deactivation delay of fiveseconds, the output channel signal **F1BO1** would behave as follows:

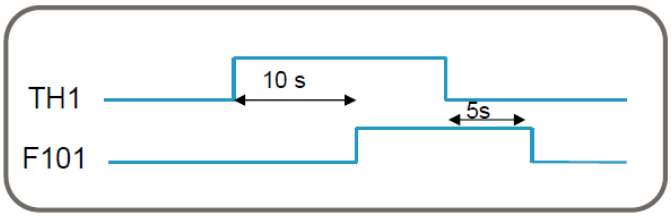


Figure 31: Binary Output – Triggering Mode

2.6.2.2 Pulsed Mode

The output data point becomes active when the triggering source is active. It will remain ON as long as the pre-set pulse duration has not expired. If the triggering source remains active for a shorter period than the pulse duration, the output will remain ON for the full pre-set pulse duration.

For example, if F1BI1 is the triggering source and the pulse duration is 10 seconds, the output channel signal F1BO2 would behave as follows:

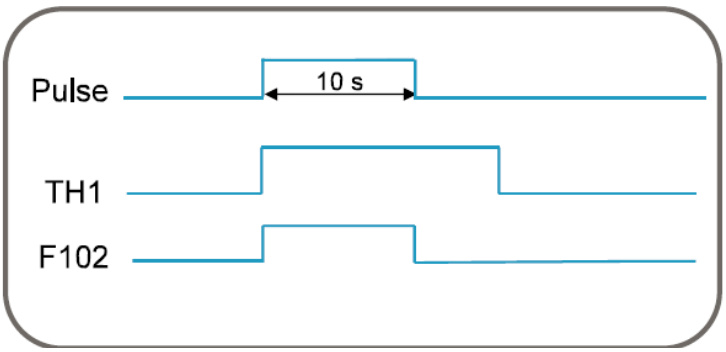


Figure 32: Binary Output – Pulsed Mode

2.6.3 BINARY OUTPUT/RELAY LOGS

Binary Output Logs provide a historical view of state transitions (True/False) for a Binary Output / Relay data point. They are used to confirm when an output was activated or deactivated, validate control behavior, and troubleshoot unexpected relay activity.

Binary Output Logs behave the same way as Binary Input Logs (same log format, rollover behavior, export/delete options, and general event timing rules). For details on how the log table

works, how many records are retained, and how timestamps are recorded, refer to Section 2.5.3 – Binary Input Logs.

Typical use cases:

- Confirm when a relay/output was turned ON or OFF (manual action or triggered logic).
- Validate that a triggering source is correctly driving the output (e.g., alarm-to-relay mapping).
- Troubleshoot relay chatter (frequent ON/OFF changes) or unexpected activations.
- Export the last events for commissioning reports or customer troubleshooting.

⚠ **Note:** If the output is Disabled or in Status-not-available, new log entries may not be recorded. If Activation Delay and Deactivation Delay are configured, logged event times reflect the moment the output state becomes valid after the configured delay has elapsed.

2.7 SMX MODULES

The iO Supervisor is capable of acquiring data from remote devices using the standard Modbus RTU protocol over its RS-485 communication ports. Up to 128 modules can be connected to a single iO Supervisor: a maximum of 64 modules on each of the RS-485 ports.

SMX modules come in two variants: the SMX-48BI and the SMX-24AI. All SMX can be networked together with the iO Supervisor using the open-standard Modbus RTU protocol.

SMX modules do not require any manual Modbus register configuration. Once configured, SMX analog and binary input data points are processed like any other iO Supervisor I/O channels. Thresholds can be set, and statistics and historical data can be recorded.

2.8 ALARM LEVELS

The iO alarms allow the user to quickly identify monitoring and control points in the system. The alarms are located at the top right of the interface. Alarms will be displayed in the header when the user-configured conditions are met. Once an alarm is cleared, it will disappear from the header.

Figure 33: Alarm Levels

To configure alarm levels, see section STATUSES.

Multitel

3.IO UTILIZATION

3.1 ASSET

The Asset module is used to create and manage monitored equipment in the iO Platform. An asset represents a device or system at a site (e.g., DC Plant, Battery (BMS), Generator, HVAC, SMX modules, etc.). Once an asset is created and enabled, the iO device can communicate with the asset using the configured communication protocol and apply the template rules to generate and acquire the related data points.

3.1.1 ASSET OVERVIEW

The Asset module allows users to:

- Create new assets and associate them with a Site.
- Select an Asset Type and a Template.
- Configure the communication protocol required to reach the asset (e.g., SNMP).
- Configure the polling engine behavior (poll rate, timeout, retries).
- Enable or disable asset acquisition.

3.1.2 ASSET CREATION

To create a new asset:

- Click on Asset.
- Click on + Asset (or Create Asset).
- Complete the fields described below.
- Click Save.

The Asset Creation form contains the following main fields.

Main Information

- **Asset Name**
  Name used to identify the asset in the platform.
- **Site**
  Site where the asset will be created.
- **Asset Type**
  Defines the equipment category (e.g., *DC Plant, Battery (BMS), Generator, HVAC*, etc.).
  Asset Type values are managed through the Inventory configuration.
- **Template**
  Defines the monitoring template that will be applied to the asset.
  Templates are managed through the Inventory configuration.
- **Manufacturer**
  Manufacturer associated to the selected asset type/template (typically auto-filled once the type/template is selected).
- **Communication Protocol**
  Selects the protocol used to communicate with the asset (e.g., SNMP Get).

The protocol selection controls which configuration section appears below (SNMP, Modbus, etc.).

- **Smart Asset**
  Indicates whether the asset uses a smart template behavior (displayed as Yes when applicable).

Once the required fields are completed, click on the following:

- Save to create the asset.
- Cancel to discard changes.

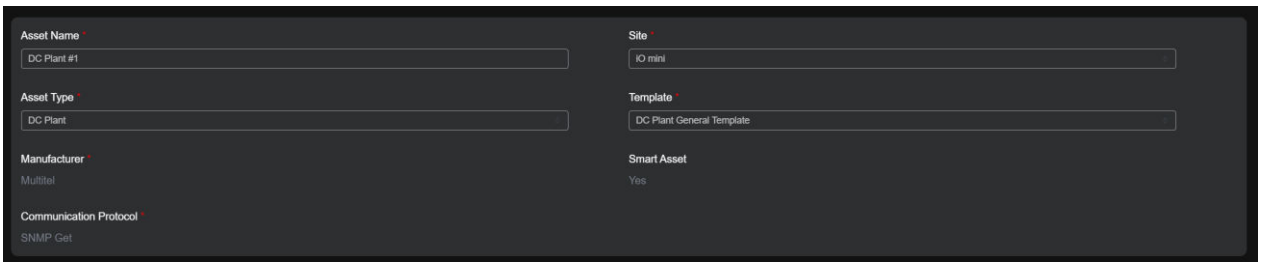


Figure 34: Asset Overview

3.1.3 COMMUNICATION PROTOCOL CONFIGURATION

After selecting a Communication Protocol, the corresponding configuration panel is displayed.

3.1.3.1 Communication Protocol PROTOCOL – SNMP

The SNMP configuration defines how the iO device connects to the remote SNMP agent.

Figure 35: Communication Protocol -- SNMP

- **Asset IP Address**
  IP address of the SNMP device.
- **Asset Hostname**
  Optional hostname field. If used, ensure DNS is configured in the iO connections settings.
- **SNMP Version**
  SNMP version used for polling (example shown: **SNMP v1**).
- **SNMP Device Community Name**
  Community string used for authentication (example shown: *public*).
- **Port Number**
  UDP port used for SNMP polling (typical SNMP default is **161**).

- **Constant Part of OID**
  Optional field used to define a base OID prefix that can be reused by the template/data point definitions.

⚠ **Note:** The exact list of required fields depends on the selected SNMP version and the template rules. Always confirm that the IP addressing, port, and credentials match the monitored device configuration.

3.1.3.2 Communication Protocol – Modbus RTU

When Modbus RTU is selected as the Communication Protocol, the platform displays the serial communication parameters used to reach the Modbus device over RS-485.

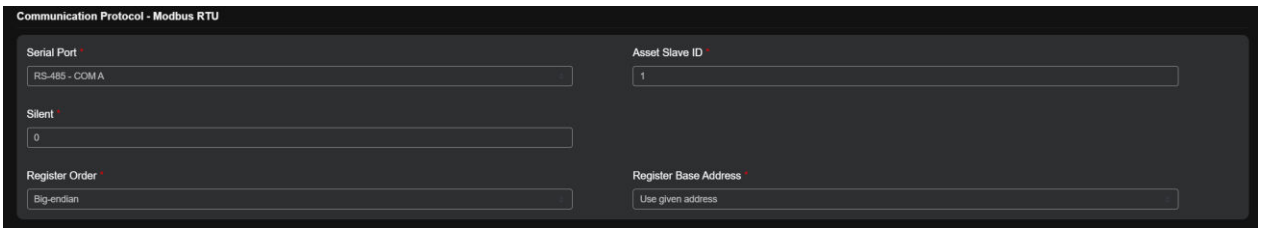


Figure 36: Communication Protocol – Modbus RTU

- **Serial Port**
  Select the RS-485 interface used to communicate with the asset (example: RS-485 – COM A).
- **Asset Slave ID**
  Modbus slave address of the remote device. This value must match the configured slave ID in the monitored equipment.
- **Silent**
  Silent interval (in milliseconds) applied between Modbus frames. This is used to stabilize communications on slower or noisy serial links.
  (Default is typically 0 unless required by the device).
- **Register Order**
  Defines the byte/word order used to interpret multi-register values.
  This must match the manufacturer's Modbus register definition.
- **Register Base Address**
  Defines how register addresses are interpreted by the platform. This setting is used to align the register numbering between the vendor documentation and the configured template.

⚠ **Note:** Modbus RTU requires correct RS-485 wiring (A/B polarity), termination, and device addressing. If values are incorrect or unstable, validate Slave ID, baud rate settings (device side), and register order/base addressing.

3.1.3.3 Communication Protocol – Modbus TCP

When Modbus TCP is selected as the Communication Protocol, the platform uses Ethernet/IP to communicate with the asset through a Modbus TCP server.

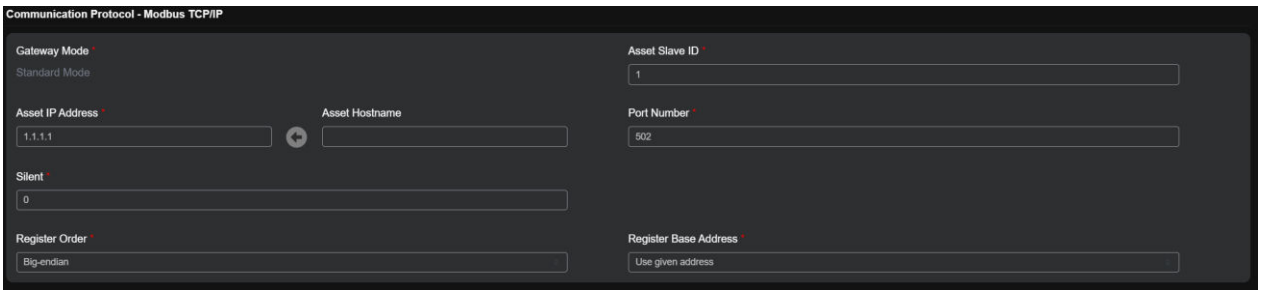


Figure 37: Communication Protocol – Modbus TCP/IP

- **Asset IP Address**
  IP address of the Modbus TCP device.
- **Port Number**
  TCP port used for Modbus communications (default is typically 502 unless the device uses a custom port).
- **Asset Unit ID / Slave ID**
  Unit identifier used by Modbus TCP devices that bridge to Modbus RTU networks, or when a device requires a specific Unit ID.
  (If not required by the device, this is commonly left at 1.)
- **Register Order**
  Defines the byte/word order used to interpret multi-register values (Big-endian / Little-endian depending on device).
- **Register Base Address**
  Defines how register addresses are interpreted (e.g., “Use given address” vs offset behavior).
  This must match the addressing format used by the device documentation and the selected template.

⚠️ **Note:** For Modbus TCP, make sure the device is reachable from the iO network and that the Modbus port is open. If communication fails, validate IP/port and confirm the device is configured as a Modbus TCP server.

3.1.4 POLLING ENGINE CONFIGURATION

The Polling Engine Configuration section defines how often the iO reads values from the asset and how it behaves when communication issues occur.

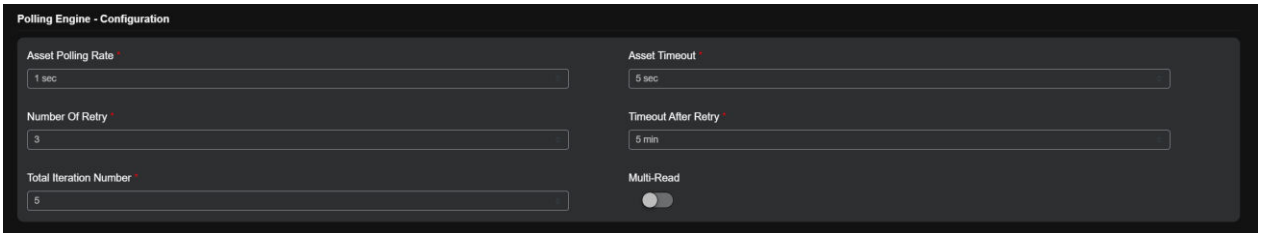


Figure 38: Polling Engine – Configuration

- **Asset Polling Rate**
  Frequency at which the iO polls the asset (e.g., 1 sec). A faster rate increases responsiveness but can increase network and CPU load.
- **Asset Timeout**
  Maximum time allowed for the asset to respond to a polling request (eg., five seconds).
- **Number Of Retry**
  Number of retries performed if a polling attempt fails (e.g., three).
- **Timeout After Retry**
  Waiting period after retries are exhausted before attempting again (example: five minutes).
- **Total Iteration Number**
  Number of consecutive polling iterations used by the acquisition engine for the asset (e.g., 5).
- **Multi-Read**
  Enables/disables multi-read behavior when supported by the protocol/template (toggle).

Best practice: The iO device supports a maximum acquisition rate of 80 data points per second (total across the entire iO). When selecting an Asset Polling Rate, ensure the combined polling load of all assets and templates remains under this limit. Exceeding 80 data points/second can cause the device to become very slow and, in some cases, unresponsive.

3.1.5 ASSET LIST

Once an asset is saved, it becomes visible in the Asset list. This page is used to view existing assets, search/filter, and access actions such as edit or delete.

The Asset list provides:

- A filter to display assets by type.
- A searchable table showing key information for each asset.
- Quick access to asset actions through the Actions menu.

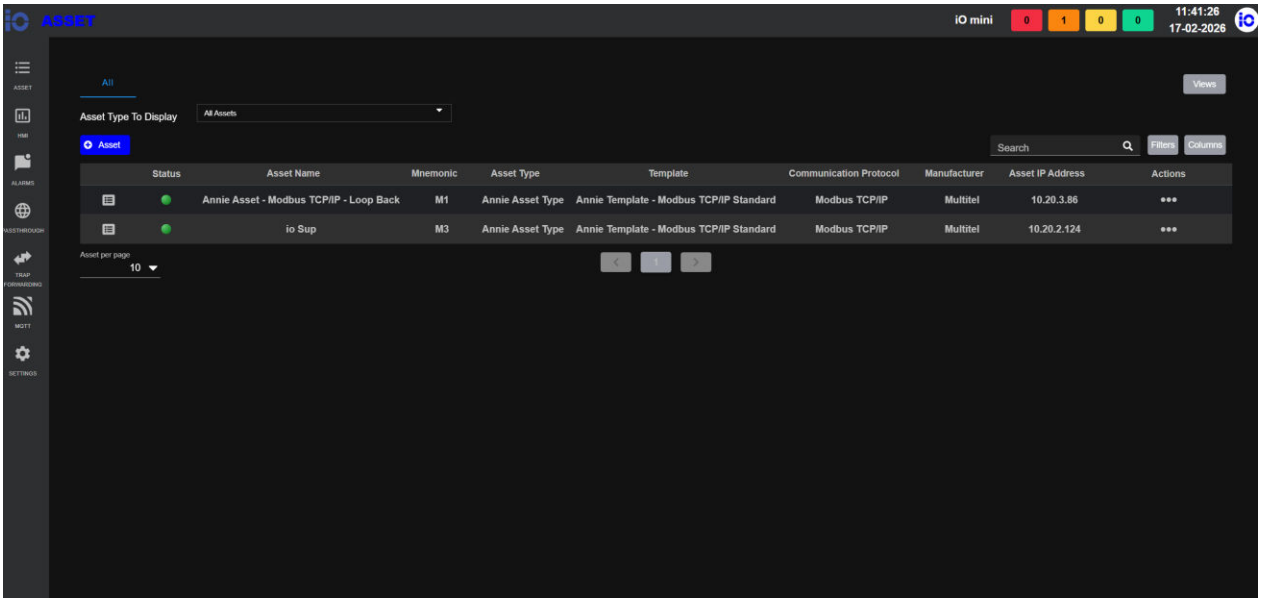


Figure 39: Asset List

3.1.5.1 Accessing The Asset List

To access the asset list:

- Go to Asset.
- The platform displays the list of existing assets for the current site.

3.1.5.2 Filtering And Searching Assets

The following tools are available to locate assets quickly:

- **Asset Type to Display**
  Drop-down filter used to display a subset of assets (e.g., All Assets or a specific asset type).
- **Search**
  Search bar used to find assets by keywords (e.g., asset name, mnemonic, template, protocol, IP address).
- **Filters**
  Opens additional filtering options to narrow down the displayed results.
- **Columns**
  Allows users to show/hide table columns depending on the information needed.
- **Views**
  Provides predefined table views (when configured) to quickly switch between different column/filter layouts.

3.1.5.3 Asset Table Columns

Each row represents an asset. The table includes the following columns:

- **Status**
  Displays the current asset status. A green indicator confirms that the asset is enabled and active.

- **Asset Name**
  Name of the asset.
- **Mnemonic**
  Short identifier used internally and within templates (.e.g., M1, M3).
- **Asset Type**
  Asset category selected during creation (e.g., *Annie Asset Type*).
- **Template**
  Template assigned to the asset (e.g., *Annie Template – Modbus TCP/IP Standard*).
- **Communication Protocol**
  Protocol used for acquisition (e.g., Modbus TCP/IP).
- **Manufacturer**
  Manufacturer associated with the asset (e.g., Multitel).
- **Asset IP Address**
  IP address configured for the asset (when applicable).
- **Actions**
  Opens the actions menu (•••) for the selected asset.

3.1.5.4 Asset Actions

Each asset includes an Actions menu (•••) that provides quick access to common management functions. When selecting an asset action, the platform displays the Asset Options panel.
The following actions are available:

- **Data Points**
  Opens the list of data points associated with the selected asset. This section is used to view the monitored points created by the assigned template and to validate acquisition results.
- **Edit**
  Opens the **Asset Creation** form in edit mode to modify the asset configuration (e.g., name, template, communication parameters, polling configuration).
- **Delete**
  Permanently removes the asset from the system. Once deleted, the asset and its associated data points are no longer available. Use this option with particular care.

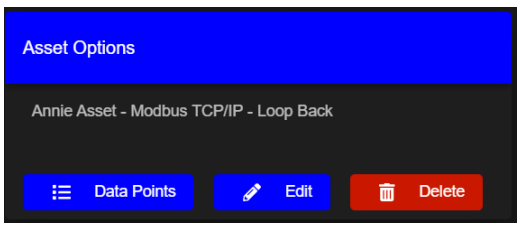


Figure 40: Asset Actions

3.1.5.5 Data Points Asset

When clicking Data Points from the Asset Options menu, the platform opens the Data Points page for the selected asset. This page is used to view and manage the data points associated with the asset template, as well as to validate communication by reading live values.

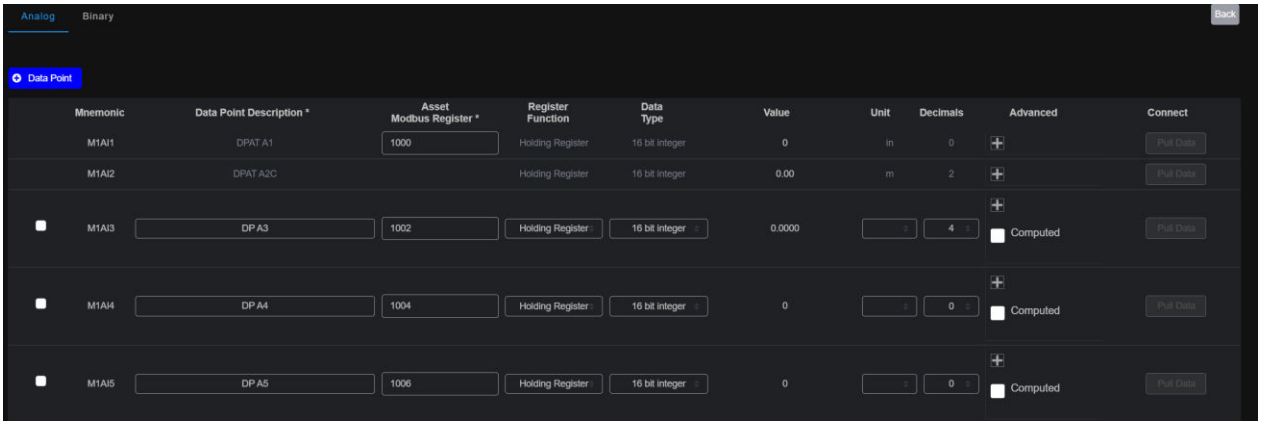


Figure 41: Data Points

The Data Points page is separated into two tabs:

- Analog
- Binary

A Back button is available to return to the Asset list.

3.2 HMI

3.2.1 HMI OVERVIEW

HMI Views files are user defined. They can represent a graphical view of the iO's specific application or any other site application.

The files are selected with the HMI Views dropdown. These images contain telemetry information like analog values with units, binary statuses, On/Off buttons, etc. More than one image file can be loaded into iO.

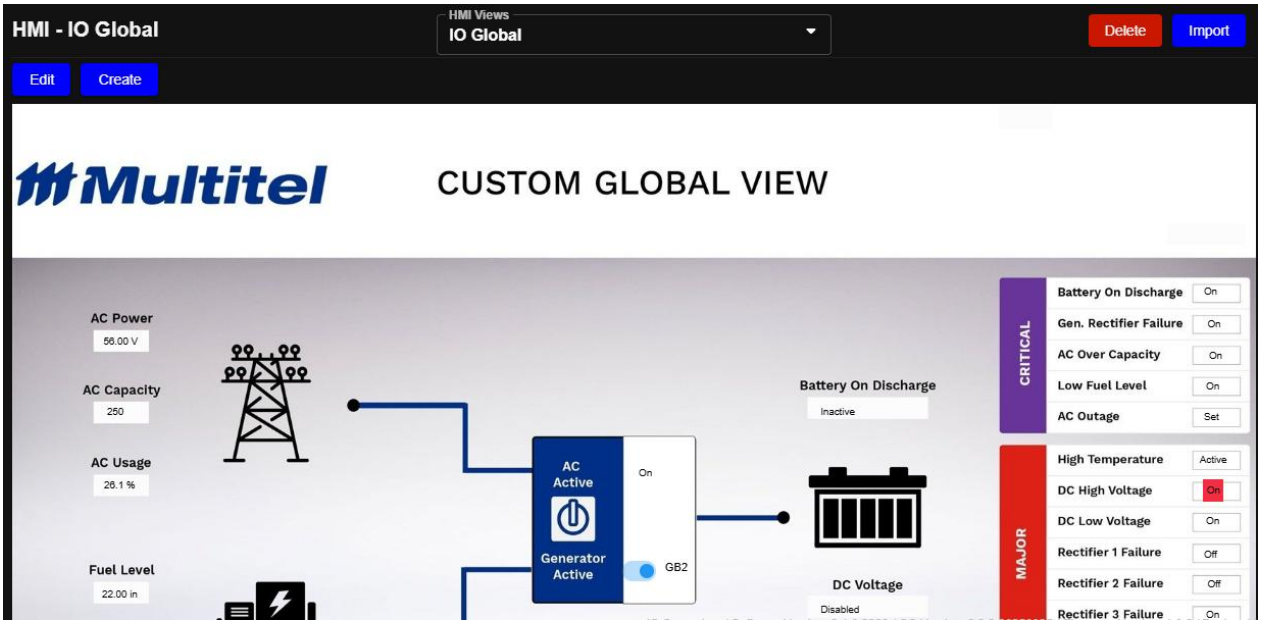


Figure 42: HMI

3.2.2 HMI FUNCTIONS

3.2.2.1 HMI Import

To import an HMI file, this can be done as follows:

- Go to HMI.
- Click on Import button.
- Select an HMI file.

3.2.2.2 HMI Create

To create an HMI file, this can be done as follows:

- Go to HMI.
- Click on Create button.

3.2.2.3 HMI Edit

To edit an HMI file, this can be done as follows:

- Go to HMI.
- Select the HMI file to modify in HMI Views dropdown.
- Click on Edit button.

3.2.2.4 HMI Delete

To delete an HMI file, this can be done as follows:

- Go to HMI.
- Select the HMI file to delete in HMI Views dropdown.
- Click on Delete button.

3.2.3 HMI CONFIGURATION

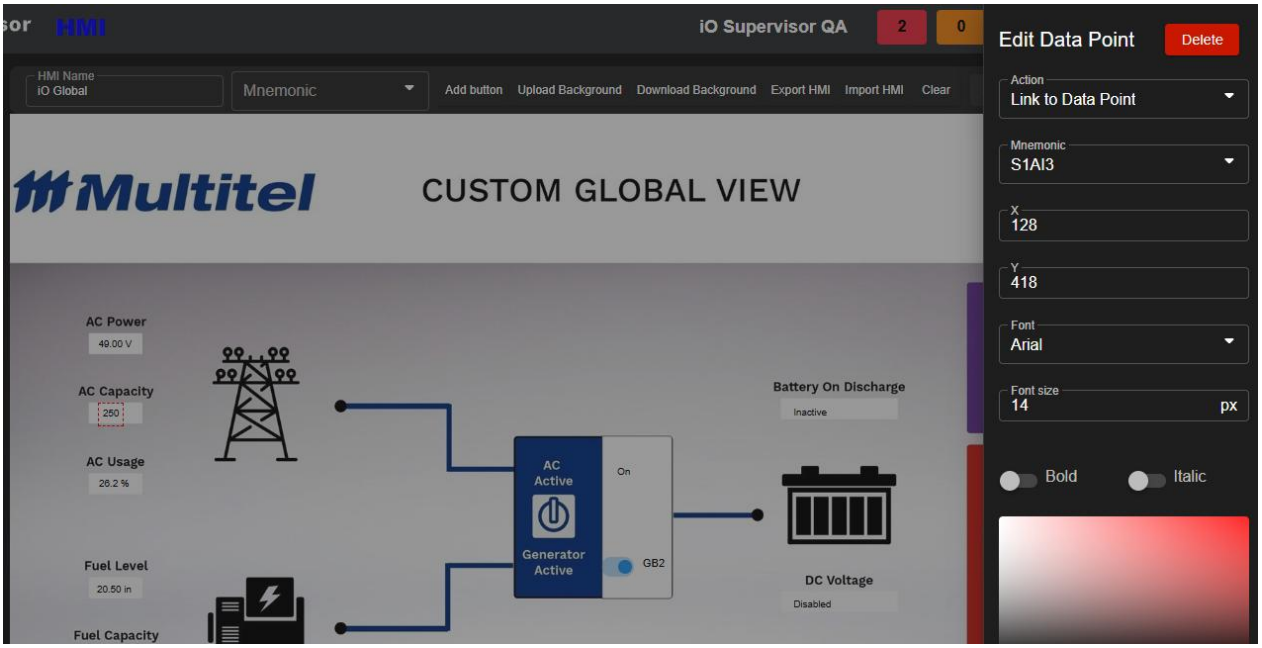


Figure 43: HMI - Configuration

When creating or editing an HMI file, here are the possible actions:

- Rename HMI.
- Manage backgrounds.
- Add data points or buttons.
- Configure display properties.
- Customize graphical styling.
- Export and import HMI views.

3.2.3.1 Rename HMI

The current HMI can be renamed by changing its Name and clicking the Save button.

3.2.3.2 Background Management

Background images can be used to represent technical diagrams (e.g., electrical schematics, layout plans).

The Upload Background button allows to upload a background image.

The Download Background button allows to download the current background.

3.2.3.3 Adding A Data Point

Select a data point from the Mnemonic dropdown and click the Add button.
The new data point will be placed in the center of the HMI by default.

3.2.3.4 Adding A Button

Click the Add button. The new button will be placed in the center of the HMI by default.

3.2.3.5 Editing a Data Point or a Button

Click an existing data point or button to open the Edit Data Point panel (displayed on the right side of the screen).

Here are the options for the Action field for data points and buttons:

- **Link to Data Point**: In visualization mode, clicking on the data point will display the visualization page of the values of the data points containing the data point specified in the Mnemonic field.
- **Link to another HMI:** In visualization mode, clicking on the data point or button will display the specified HMI.

Here are the specific fields for the buttons:

- **Button Label**: Label displayed on the button
- **Width (px)**: button width in pixels
- **Height (px)**: button height in pixels

Here are the possible actions for element positioning for data points and buttons:

- **X**: Horizontal position (left → right)
- **Y**: Vertical position (top → bottom)

Values are expressed in pixels. For precise positioning:

- Manually adjust the X and Y fields or
- Use drag-and-drop

Here are the possible actions for style settings for data points and buttons:

- **Font**: Font family (e.g., Arial)
- **Font size**: Size in pixels
- **Bold**: Enables bold text
- **Italic**: Enables italic text
- **Color Picket**: Select text color

3.2.3.6 Delete a Data Point or a Button

Click an existing data point or button to open the Edit Data Point panel (displayed on the right side of the screen). Click the Delete button in the panel to remove the data point or button from the HMI.

Click the Clear button to remove all data points and buttons from the HMI.

3.2.3.7 Export / Import HMI

An HMI can be imported or exported using the Import HMI and Export HMI buttons.

3.3 PASSTHROUGH

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

3.3.1 PASSTHROUGH OVERVIEW

The Passthrough module uses the client-server model. A client is a program or device that 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) sending a request to a web server to access web pages.
Unlike 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 area network using the iO.

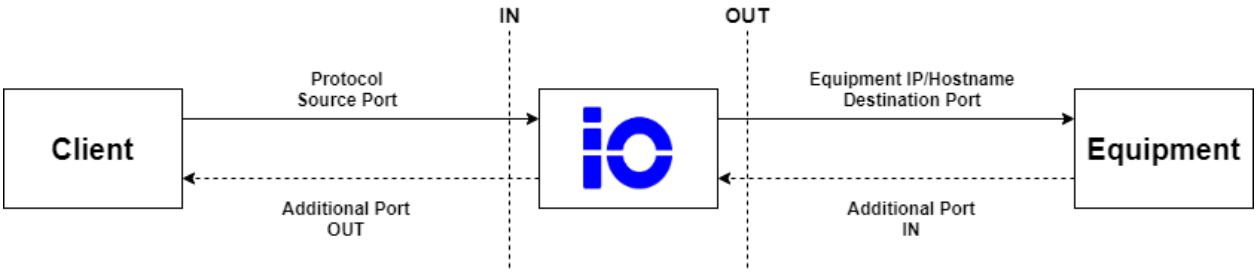


Figure 44: Passthrough Topology

The iO Passthrough topology is divided into two sections:

- Client/iO Platform device
  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 Platform device/equipment
  Once the client is configured, the iO will reroute the client requests to the equipment server.

3.3.2 PASSTHROUGH CONFIGURATION

To configure passthroughs:

- Go to Passthrough.
- Click on Passthrough tab.
- Click on + Passthrough to create a new passthrough.

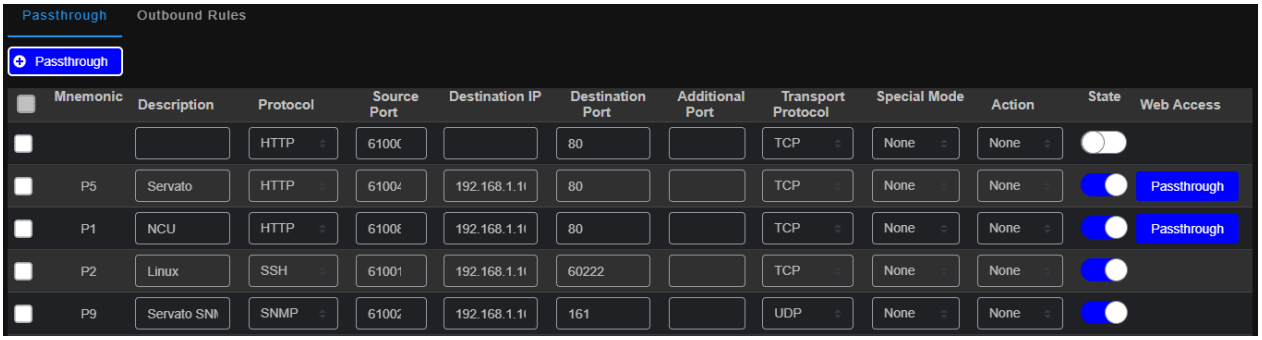


Figure 45: Passthrough – Configuration

The programmable parameters are listed below:

Table 16: Passthrough – Configuration

Field	Description	Specification	Required
Mnemonic	Unique identifier	Pxx – Auto Generate	
Description		1-50 characters	Yes
Protocol		Dropdown: • SNMP • DNS • NTP • HTTP (Default) • FTP • Telnet • Email • HTTPS • SFTP • SSH • SCP • Email-TLS • Email-SSH	Yes
Source Port		1 to 65535	Yes
Destination IP		0.0.2.0 to 255.255.255.255 or hostname	Yes
Destination Port		1 to 65535	Yes
Additional Port	Allows to add more ports to the passthrough	1 to 65 535 (Port interval is accepted)	No
Transport Protocol		Dropdown: • TCP (Default) • UDP • Both	Yes
Special Mode		Dropdown: • None (Default) • PBT WS 8081 • PBT WS 80 • HTTPS Proxy	Yes
Action		Dropdown: • None (Default)	Yes

		• IN • Passthrough	
State	Allows to enable and disable the passthrough	Toggle	Yes
Web Access	Passthrough button is displayed only when the HTTP or HTTPS protocol are enabled. Clicking on the button opens the web interface of the equipment.	Button	

Default values for Port and Transport depend on the selected protocol.

Table 17: Passthrough – Protocols and Ports

Protocol	Description	Default Port	Default Transport
Communication Protocol			
SNMP	Network management protocol.	161	UDP
Insecure Protocol			
HTTP	Hypertext Transfer Protocol is used as an internet communication.	80	TCP
FTP	File Transfer Protocol is used for transferring files to another device.	21	TCP
Telnet	Telecommunication Network is used to log on to one TCP/IP host to access other hosts on the network.	23	TCP
Email	Unencrypted email protocol	25	TCP
Secure Protocol			
HTTPS	Hypertext Transfer Protocol Secure is used as an internet communication.	443	TCP
SFTP	Secure File Transfer Protocol is used for transferring a file to another device with security components.	22	TCP
SSH	Secure Shell is used to execute commands in a remote device and move files from one device to another.	22	TCP
SCP	Secure Copy Protocol is used for transferring files securely from a local to a remote host.	22	TCP
Email-TLS	Secured email transmission using TLS.	587	TCP
Email-SSL	Secured email transmission using SSL.	465	TCP

3.3.2.1 Source Port Options

The sources port is self-generated according to the specifications below. If needed, this can be changed by users. The source port must be unique and between 1 to 65 535.

Table 18: Passthrough – Source Port Options

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
Email	65 000 to 65535

3.3.2.2 *Passthrough Email Forwarding*

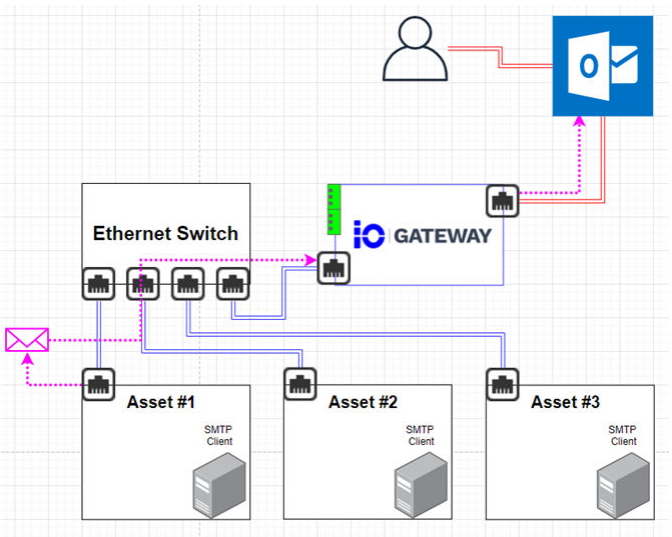
The email can now be forwarded directly through the iO.

The email passthrough feature supports three options:

- Email (unsecured)
- Email-TLS (secured)
- Email-SSL (secured)

The source port is the SMTP server port that needs to be configured in the device. The Destination Port is the port used to send the email to the user SMTP server.

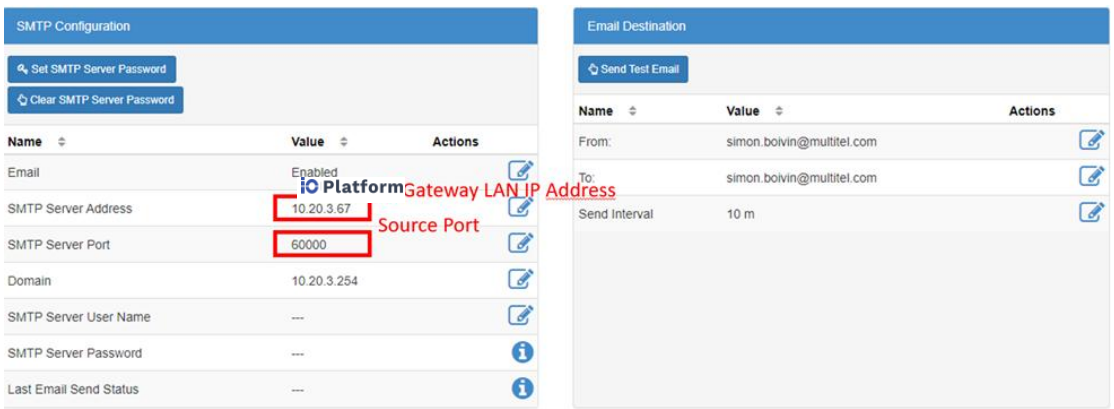
The figure below represents the email forwarding architecture using the passthrough service.



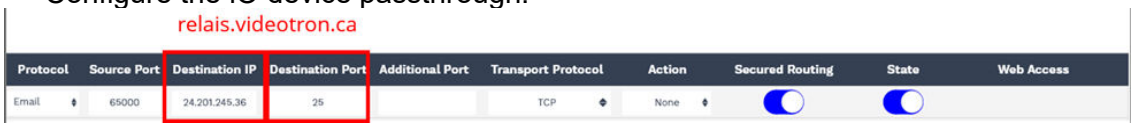
The passthrough only opens ports between the asset and the user SMTP server; there is no manipulation, added security layer, or loggings.

To configure the Passthrough Email Forwarding:

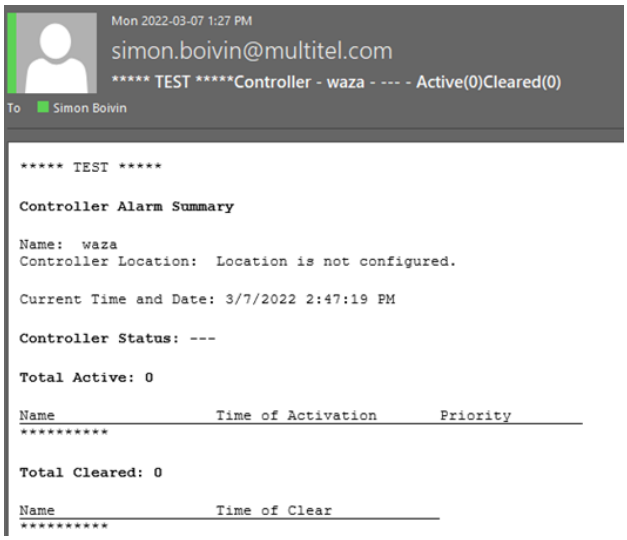
- Configure the SMTP server and server port of the device.



- Configure the iO device passthrough.



- Email received



3.3.3 OUTBOUND RULES OVERVIEW

Outbound rules are part of firewall or network security group configurations. They define the permissions for outgoing connections from a machine or network. These rules specify what types of traffic are allowed to leave a system or infrastructure.

The Traffic Direction of the outbound rules, unlike inbound rules, which control incoming connections, regulates the outgoing traffic from the iO (e.g., a server or a cloud instance) to an external destination.

3.3.4 OUTBOUND RULES CONFIGURATION

To configure passthroughs, follow these steps:

- Go to Passthrough.
- Click on Outbound Rules tab.
- Click on + Outbound Rule to create a new outbound rule.

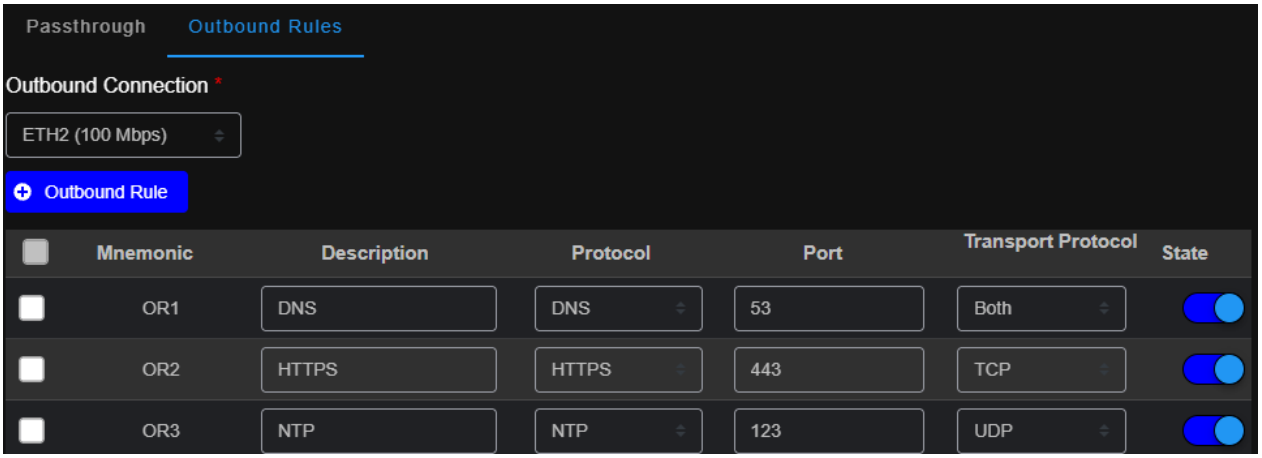


Figure 46: Outbound Rules – Configuration

Table 19: Outbound Rules - Configuration

Field	Description	Specification	Required
Mnemonic	Unique identifier	ORxx – Auto Generate	
Description	Description	1 to 50 characters	Yes
Protocol	Protocol	Dropdown: • SNMP • DNS • NTP • HTTP (Default) • FTP • Telnet • Email • HTTPS • SFTP • SSH • SCP • Email-TLS • Email-SSH	Yes
Port	The port is automatically generated based on the selected protocol. If needed, the user can change it.	1 to 65535	Yes
Transport Protocol	Transport Protocol	Dropdown: • TCP • UDP • Both	Yes
State	Allows to enable and disable the outbound rule.	Dongle	Yes

Default values for Port and Transport depending on the selected protocol.

Multitel

Table 20: Outbound Rules – Protocols and Ports

Protocol	Description	Default Port	Default Transport
Communication Protocol			
SNMP	Network management protocol.	161	UDP
DNS	Domain name resolution protocol.	53	Both
NTP	Network time synchronization protocol.	123	UDP
Insecure Protocol			
HTTP	Hypertext Transfer Protocol is used as an internet communication.	80	TCP
FTP	File Transfer Protocol is used for transferring files to another device.	21	TCP
Telnet	Telecommunication Network is used to log on to one TCP/IP host to access other hosts on the network.	23	TCP
Email	Unencrypted email protocol.	25	TCP
Secure Protocol			
HTTPS	Hypertext Transfer Protocol Secure is used as an internet communication.	443	TCP
SFTP	Secure File Transfer Protocol is used for transferring a file to another device with security components.	22	TCP
SSH	Secure Shell is used to execute commands in a remote device and move files from one device to another.	22	TCP
SCP	Secure Copy Protocol is used for transferring files securely from a local to a remote host.	22	TCP
Email-TLS	Secured email transmission using TLS.	587	TCP
Email-SSL	Secured email transmission using SSL.	465	TCP

3.4 TRAP FORWARDING

3.4.1 TRAP FORWARDING OVERVIEW

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

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

Table 21: Type of SNMP Trap

Type	Description
Trap -- Unacknowledged	The trap will be forwarded and the device will not 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.

3.4.2 TRAP SOURCES OVERVIEW

The trap forwarding sources tab allows users to configure an unlimited number of trap sources and specify their destinations.

NOTE

There is no hard limit on the number of trap forwarding sources but Multitel recommends a limit of 50 sources to optimize performance.

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

3.4.3 TRAP SOURCES CONFIGURATION

To configure trap source, follow these steps:

- Go to Trap Forwarding.
- Click on Sources tab.
- Click on + Source to create a new trap source.

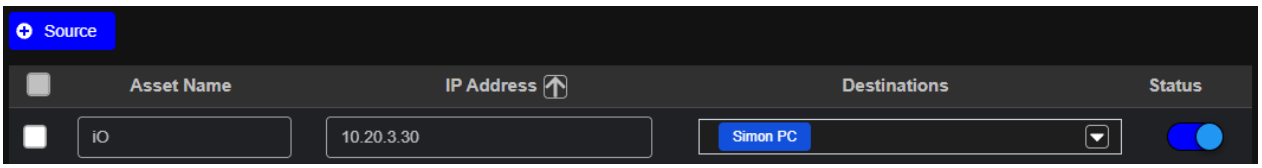


Figure 47: Trap Sources – Configuration

Table 22: Trap Sources – Configuration

Field	Description	Specification	Required
Asset Name	The asset name is use to indicate the source of a trap forwarded.	1 to 50 characters	Yes
IP Address	IP address or domain name of the asset source.	0.0.0.0 to 255.255.255.255	Yes
Destinations	The destination indicates where received traps are to be forwarded. Multiple destinations can be selected.	Dropdown: List of trap destinations	Yes
Status	The status enables or disables a source. A disabled source stops the communication between the source and the iO device.	Dongle	

3.4.4 TRAP DESTINATIONS OVERVIEW

The trap forwarding destination allows users to configure up to ten (10) destinations that the iO device can forward traps received.
Trap destinations are common in notifications and trap forwarding.

Each destination can receive SNMP trap forwarding or notifications based on alarm or event activities. The table allows users to configure key parameters for each SNMP receiver, including addressing, protocol version, and notification behavior.

3.4.5 TRAP DESTINATIONS CONFIGURATION

To configure trap destination:

- Go to Trap Forwarding.
- Click on Trap Destinations tab.
- Click on + Destination to create a new trap source.

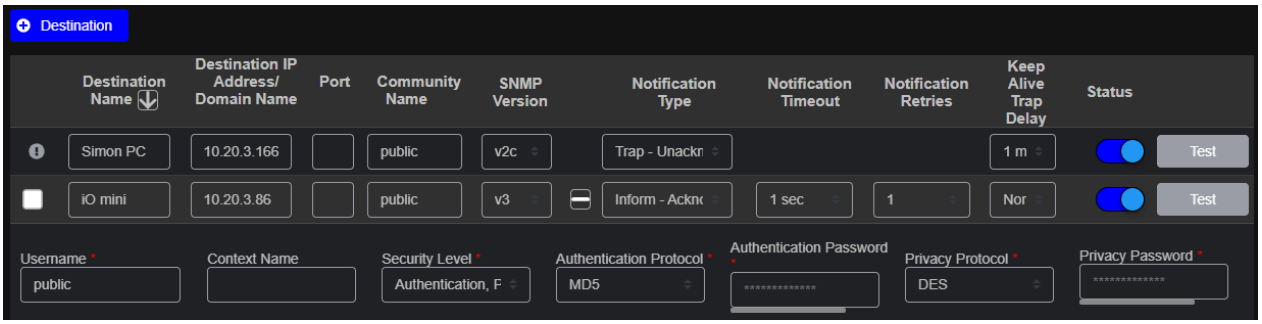


Figure 48: Trap Destinations – Configuration

Each row represents a destination that can receive SNMP trap notifications based on alarm or event activities. The table allows users to configure key parameters for each SNMP receiver, including addressing, protocol version, and notification behavior.

Table 23: Trap Destinations – Configuration

Field	Description	Specification	Required
Destination Name	The asset name is used to indicate the source of a trap forwarded.	1 to 50 characters	Yes
Destination IP Address/ Domain Name	IP address or domain name of the remote SNMP trap receiver.	0.0.0.0 to 255.255.255.255	Yes
Port	The UDP port number used to send SNMP traps.	1 to 65 535 162 (Default)	Yes
Community Name	The SNMP community string used for authentication (applies to SNMP v2c only).	public or private	Yes
SNMP Version	The SNMP protocol version used to communicate with the destination.	Dropdown: • v2c • v3	Yes
Notification Type	**Trap – Unacknowledged**: A basic one-way alert with no confirmation. **Inform – Acknowledged**: A more reliable message type that requires acknowledgment from the receiver.	Dropdown: • Trap • Inform	Yes

Notification Timeout	Time the system waits for acknowledgment before retrying or marking the notification as failed.	Dropdown: • 1 sec • 5 sec • 10 sec • 1 min	Yes
Notification Retries	Number of times the system will retry sending the trap if no acknowledgment is received.	Dropdown: 1 to 5	Yes – Inform
Keep Alive Trap Delay	Optional delay interval to send periodic "keep-alive" traps to confirm connectivity.	Dropdown: • None • 1 min • 15 min • 30 min • 60 min	Yes – Inform
Status	Enable or disable this SNMP trap destination.	Toggle	
SNMP v3			
Username	The username used for authentication.	1 to 50 characters	Yes
Context Name	Name to distinguish a specific agent.	1 to 50 characters	No
Security Level	Security level.	Dropdown: • No authentication, No privacy • Authentication, No privacy • Authentication, Privacy	Yes
Authentication Protocol	Authentication Protocol.	Dropdown: • MD5 • SHA1	No/Yes
Authentication Password	Authentication Password.	String	No/Yes
Privacy Protocol	Privacy Protocol.	Dropdown: • DES • AES	No/Yes
Privacy Password	Privacy Password.	String	No/Yes

3.4.5.1 *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.

3.4.5.2 *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.

3.4.6 LOG

The iO device records all traps received, forwarded and sent by the keep-alive or the test trap button. To reduce unnecessary logs, 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 contained in the log file:

- Date and time of the iO device

The timestamp is based on the date and time configuration of the device. To ensure a proper recording, please configure the date and time accurately.

- The local date and time of the user

The timestamp is based on the date and 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 24: Trap Log Messages

Message Type	Description
Received has been sent	Refers to a trap received by the device.
Forwarded has been sent	Refers to a trap received and forwarded to a destination.
Keep Alive has been sent	Refers to a keep-alive trap.
Test Trap has been sent	Refers to a trap triggered by the *Test trap* button .
Forwarded as inform and received response	Refers to a trap – acknowledge that the destination sends an acknowledgement trap.
Forwarded as inform but received no response	Refers to a trap – acknowledge that the destination does not send an acknowledgement trap.
Error sending test trap: SPECIFIC MESSAGE	Indicates 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.

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

Figure 49: Trap Log – Example

3.4.6.1 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 Gbit

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

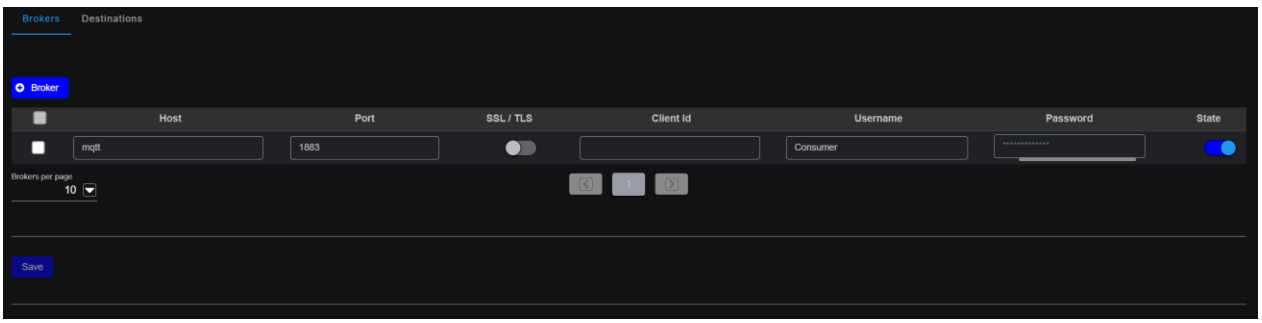
3.5 MQTT

The MQTT module allows the iO device to publish data to an external MQTT broker. The configuration is split into two tabs:

- **Brokers** – Configure the MQTT server connection (host, port, authentication, TLS).
- **Destinations** – Configure where to publish (topic, QoS, asset scope) and define the message payload using a Lua script.

3.5.1 BROKERS

The Brokers tab is used to create and manage MQTT broker connections. Each row represents a broker configuration.



To add or modify a broker, follow these steps:

- Go to Settings.
- Go to MQTT.
- Select the Brokers tab.
- Click + Broker.
- Configure the broker parameters.
- Click Save.

Broker fields

- **Host**
  Hostname or IP address of the broker.
- **Port**
  Broker port (example shown: 1883).
- **SSL / TLS**
  Toggle to enable/disable TLS. When enabled, certificate fields are displayed.
- **Client Id**
  MQTT client identifier used to identify the iO connection for the broker.
- **Username**
  Username used for broker authentication.

- **Password**
  Password used for broker authentication.
- **State**
  Toggle used to enable/disable the broker configuration.

3.5.1.1 TLS Certificate

When SSL/TLS is enabled, additional fields are displayed for certificate configuration:

- **Certificate Authority**
  CA certificate (PEM) used to validate the broker certificate.
- **Client Certificate**
  Client certificate (PEM) used for mutual TLS authentication when required by the broker.
- **Client Key**
  Client private key (PEM) associated with the client certificate.

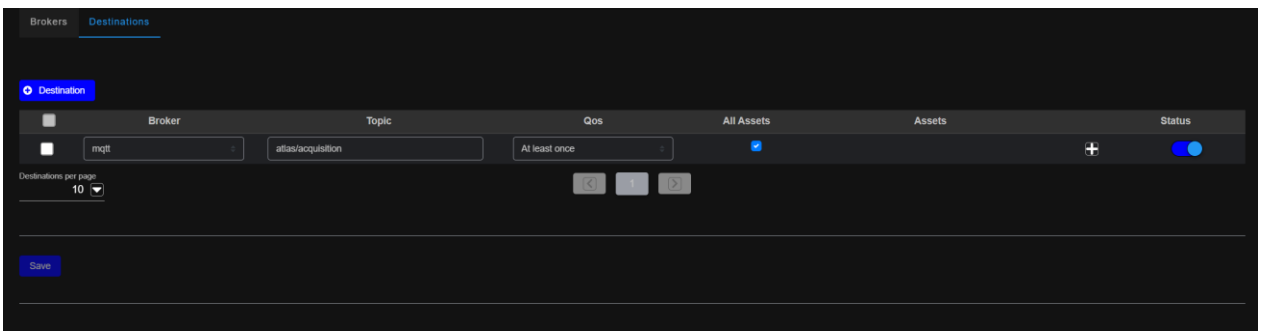
⚠️ **Note:** TLS requirements depend on the broker configuration. Some brokers require only the Certificate Authority, while others require mutual TLS (Client Certificate + Client Key).

3.5.2 DESTINATIONS

The Destinations tab defines the publishing rules: which broker to use, which topic to publish to, the QoS level, and which assets are included.

To add or modify a destination, follow these steps:

- Go to Settings.
- Go to MQTT.
- Select the Destinations tab.
- Click + Destination.
- Configure the destination parameters.
- Click Save.



- **Broker**
  Select the broker configuration to use.
- **Topic**
  MQTT topic used for publishing.
- **QoS**
  Quality of Service level
- **All Assets**
  When enabled, data is published for all assets.

- **Assets**
  Used when All Assets is disabled to select a subset of assets.
- **Status**
  Toggle to enable/disable the destination.

3.5.3 PAYLOAD

Each destination includes a Script area used to generate the payload that will be published to the configured topic. The script typically builds a structured payload (commonly JSON) and returns the final message content.

Script Area

- **Test Mnemonic**
  Field used to select or enter a mnemonic to test the script execution.
- **Run (▶)**
  Executes the script using the selected mnemonic.
- **Reset (↺)**
  Resets the script to its previous/default state (when applicable).
- **Delete (🗑)**
  Clears the current script content (when applicable).

Output Area

- Displays the result of the script execution.
- Includes a CLEAR control to reset the displayed output.

⚠ **Note:** The script must return the content to publish (example: JSON text). If the output is empty or unexpected, validate the mnemonic used for testing and confirm the script syntax.

4.IO SETTINGS

4.1 CONNECTIONS

The Connections parameters can be accessed from the settings module.

Figure 50: Settings – Connections

Multitel

⚠ **Note:**
These parameters require an understanding of network management and serial-based protocols. This user guide does not provide a complete step-by-step guide to network and serial communication, and assumes that the reader is already familiar with both topics.

4.1.1 ETHERNET CONFIGURATION

Depending on the model, the iO device offers one or two Ethernet ports. ETH-1 is a native 1Gbps port and ETH-2 is a 100Mbps.

Both ports can be configured using the following parameters:

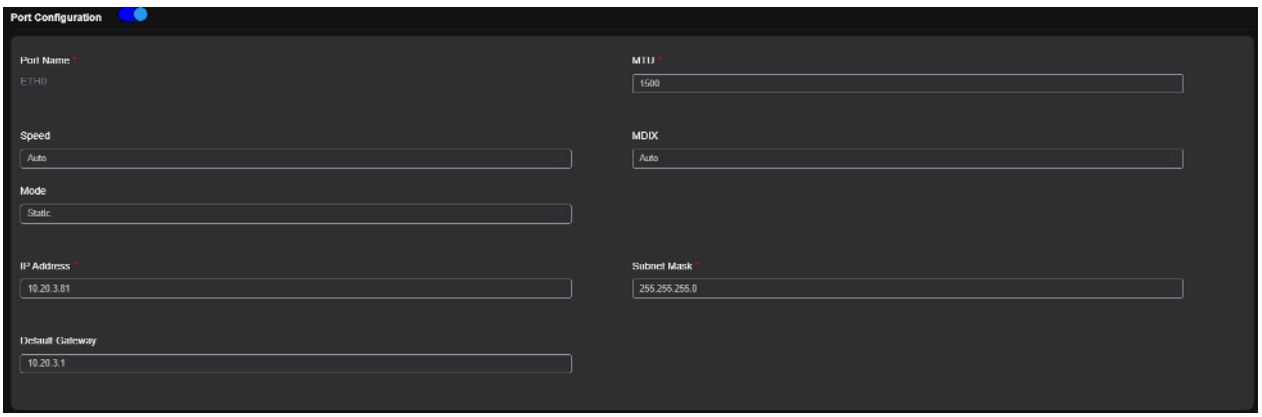


Figure 51: Connections – Ethernet Ports

Table 25: Ethernet Ports -- Configuration

Field	Description	Specification	Required
Port Name	Name of the Ethernet port being configured.	ETH-1: 1Gbps ETH-2: 100Mbps	Yes
MTU	Maximum Transmission Unit – the size of the largest packet that can be sent.	Default: 1500	Yes
Speed	Sets the data rate of the port.	Dropdown: • Auto • 10Mbps • 100Mbps • 1Gbps	Yes
MDIX	Controls automatic crossover of Ethernet cable type.	Dropdown: • Auto • On • Off	Yes
Mode	Defines how the IP address is assigned.	Dropdown: • Static • DHCP	Yes
IP Address	The IP address assigned to the port.	0.0.0.0 to 255.255.255.255	Yes

Subnet Mask	Identifies the network and host portion of the IP address.	0.0.0.0 to 255.255.255.255	Yes
Default Gateway	IP address of the gateway used for external network access.	0.0.0.0 to 255.255.255.255	Yes

DNS servers can also be configured to enable the use of hostnames in certain parameters. The iO allows the configuration of two separate servers to improve redundancy.

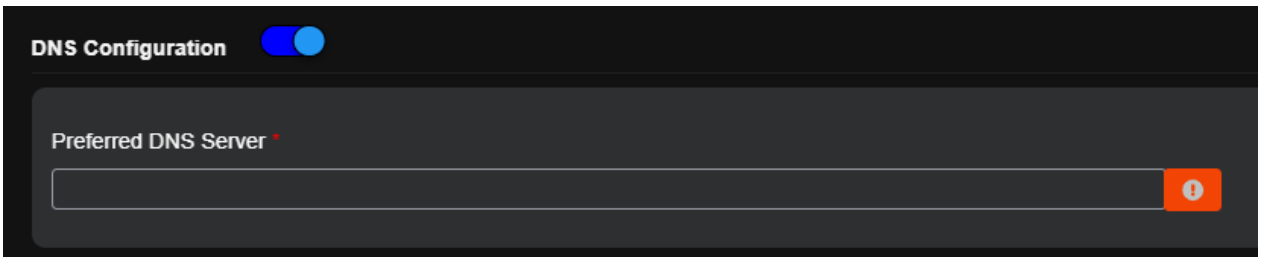


Figure 52: DNS Configuration

4.1.2 RS-485 CONFIGURATION

Depending on the model, the iO device offers one or two RS-485 ports. These ports can be configured using the following parameters:

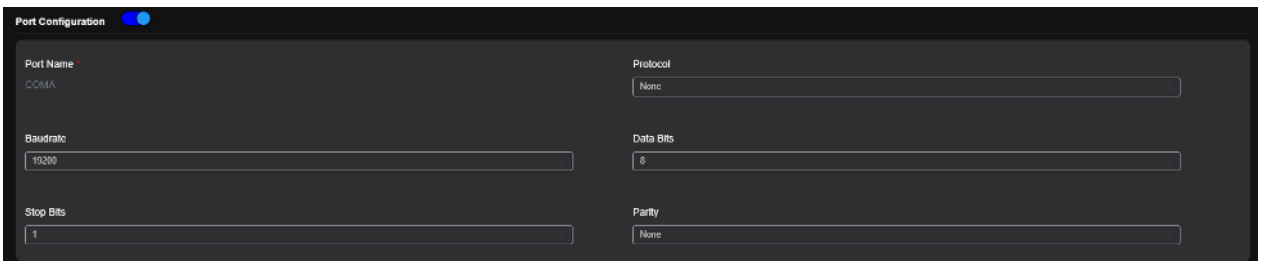


Figure 53: Connections – RS-485

Table 26: RS-485 -- Configuration

Field	Description	Specification	Required
Port Name	Identifier of the serial communication port.	COMA COMB	Yes
Protocol	Communication protocol used over the RS-485.	Dropdown: • None • Modbus RTU – Slave • Modbus RTU - Master	Yes
Baudrate	Speed of communication (in bits per second).	Dropdown: • 300 • 1200 • 2400 • 4800 • 9600 • 19200	Yes

		• 38400 • 57600 • 115200	
Data Bits	Number of data bits in each character/frame.	Dropdown: • 6 • 7 • 8	Yes
Stop Bits	Number of stop bits used to signal the end of a character.	Dropdown: • 1 • 2	Yes
Parity	Method of error checking for transmission.	Dropdown: • None • Odd • Even	Yes

4.2 INVENTORY

The Inventory parameters can be accessed from the settings module.

Figure 54: Settings -- Inventory

4.2.1 SITE CONFIGURATION

Here is a list of the sites configured on the iO. Sites are used to group assets together. The main asset (this device) cannot be deleted, only edited.

⚠ **Note:**
Site configuration should be used only when the iO is acting as an iO Manager, where multiple sites can be created and managed. For a standalone iO device, skip site configuration.

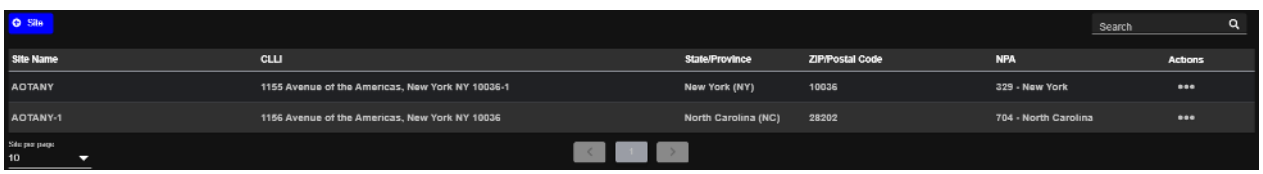


Figure 55: Inventory – Sites

To create a new site, the user needs to click on + Site.

Figure 56: Inventory – Site Creation

The site creation is divided into four sections.

4.2.1.1 Main Information

The Main Information section includes the Site Name and the CLLI code, which uniquely identify each telecommunications network location.

4.2.1.2 Language And Supervisor

This section covers the display language of the iO. Please note that only English is currently supported.

4.2.1.3 Location

This section covers the physical location parameters for the iO.

4.2.1.4 NPA

This section is used to configure the NPA of the iO location.

4.2.2 ASSET TYPE CONFIGURATION

An asset type identifies where data points can be linked. This corresponds to a category of equipment, such as DC plants, batteries, generators, or HVAC systems. The purpose of an asset type is to standardize the data-point nomenclature and configuration while asset types are also used to group templates.

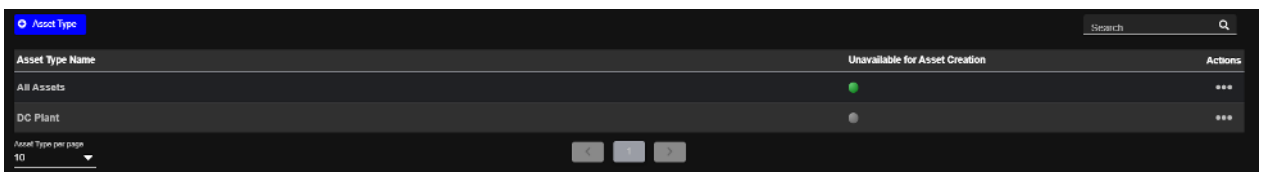


Figure 57: Inventory – Asset Types

4.2.2.1 All Assets

The default asset type available on an iO device is called “All Assets.” It aggregates all other asset types to provide easier visibility in the Asset section. By selecting “All Assets” in the Asset Type to Display dropdown, users can view every asset across all asset types.

Figure 58: Asset Type To Display

There is a special condition for All Assets called “Unavailable for Asset Creation.” It should typically be applied only to All Assets. If this option is enabled, no assets can be created for that asset type.

4.2.2.2 Asset Type Creation

To create a new asset, users should click on + Asset Type.

The Main Information section is where the name of the asset type can be configured. The parent asset type should be set to “All Assets”.

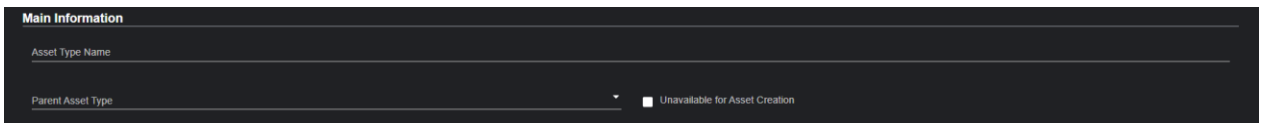


Figure 59: Asset Type – Main Information

The Data Points section defines the data-point structure and is divided into three subsections.

4.2.2.3 Asset Type – Analog Data Point

An analog data point represents a variable physical quantity such as voltage, current, temperature, or pressure. Each analog data point configuration requires a name and a unit. The name should be chosen to standardize data point nomenclature. For example, for a DC plant, the name “DC Plant Voltage” should be used to identify the float voltage of the DC plant. Therefore, even though multiple DC plant models may be used at the same site, the float-voltage value can be easily identified.

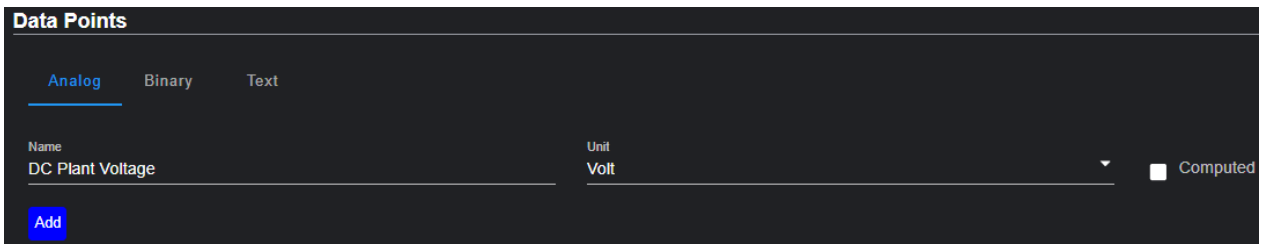


Figure 60: Asset Type – Analog Data Point

The unit can be configured using a dropdown field.

4.2.2.4 Asset Type – Binary Data Point

A binary data point represents a digital or discrete signal that has only two possible states: True or False. These points can also be used as alarm indicators. The name should be used to standardize data point nomenclature.

Figure 61: Asset Type – Binary Data Point

The binary label is configured to display the appropriate text when the value is True or False.

4.2.2.5 Asset Type – Text Data Point

The text data point is used to configured alphanumeric data point typically used in the SNMP protocol. The name should be used to standardize data point nomenclature.

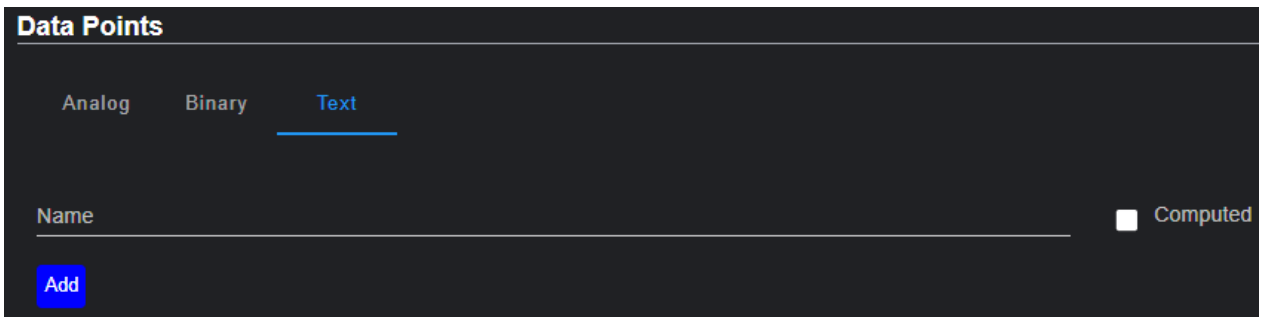


Figure 62: Asset Type – Text Data Point

4.2.3 TEMPLATES CONFIGURATION

A template corresponds to a model of equipment and is linked to an asset type. It is used to configure the communication protocol and the acquisition settings for each data point.

4.2.3.1 Communication Protocol

This section allows you to configure the different communication protocols supported by the iO.

Modbus RTU

The iO supports the Modbus RTU Master protocol, allowing it to poll multiple devices over an RS-485 serial network.

The figure and table below display the various fields required to configure the communication settings for polling a Modbus RTU device. These fields define key parameters such as baud rate,

parity, stop bits, slave ID, and register addresses, ensuring proper communication over the RS-485 network.

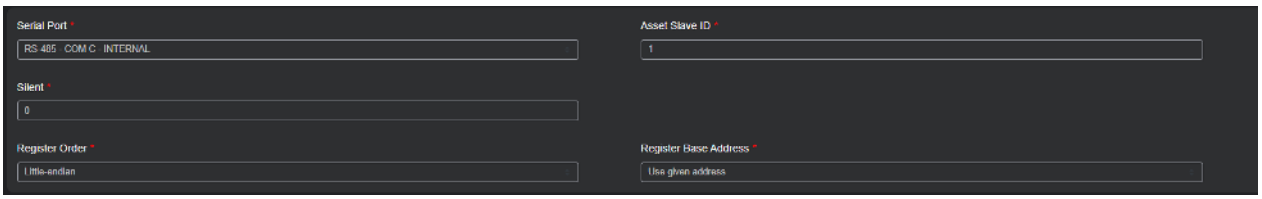


Figure 63: Template Communication Protocol: Modbus RTU

Table 27: Template Communication Protocol Modbus RTU -- Configuration

Field	Description	Specification	Required
Serial Port	Selection of the RS-485 port used for the communication.	Dropdown: • RS-485 – COM A • RS-485 – COM B	Yes
Asset Slave ID	This is where the ID of the device being monitored is configured.	1 to 256	Yes
Silent	The silent mode functionality is used to introduce a timeout in the acquisition loop, giving some legacy equipment "room to breathe" when being polled via serial communication. The silent setting adds the configured delay between each acquisition. For example, if you set a silent period of one second, the iO will wait one second after each acquisition to give the legacy device time to respond. Most of the time, the silent value should be set to zero, but in certain cases, it provides additional flexibility to the user.	0 to 100 seconds	Yes
Register Order	The register order is used when dealing with data types larger than 16 bits (like 32-bit integers and 32-bit float). The Big Endian also called “Most Significant Byte (MSB) First”, the high-order byte or word comes first (lowest address). Example of a 32-bit value split into two 16-bit registers: • Register 40001: 0x1234 • Register 40002: 0x5678 • Combined Result: 0x12345678	Dropdown: • Big-Endian • Little-Endian	Yes

	The Little Endian also called “Least Significant Byte (LSB) First”, the low-order byte or word comes first (lowest address). Example of a 32-bit value split into two 16-bit registers: • Register 40001: 0x5678 • Register 40002: 0x1234 • Combined Result: 0x12345678		
Register Base Address	The field determines how the Modbus register address should be interpreted when polling a device. Use given address: The register address entered by the user is used as-is, with no adjustment. For example, if you enter address 40001, the system will poll exactly that address. Subtract one from given address**:** Some Modbus devices use 1-based addressing (e.g., 40001), while others use 0-based addressing (e.g., zero for the first register). Selecting this option automatically subtracts o**ne** from the entered address to align with devices that use 0-based indexing. For example, entering 40001 will result in polling register 40000**.**	Dropdown: • Use given address • Subtract one from given address	Yes

Modbus TCP/IP

The iO supports the Modbus TCP/IP Client protocol, allowing it to poll multiple devices over an Ethernet network.

The figure and table below display the various fields required to configure the communication settings for polling a Modbus TCP/IP device. These fields define key parameters such as IP address, port number, unit ID, and register addresses, ensuring proper communication over the network using the Modbus TCP/IP protocol.

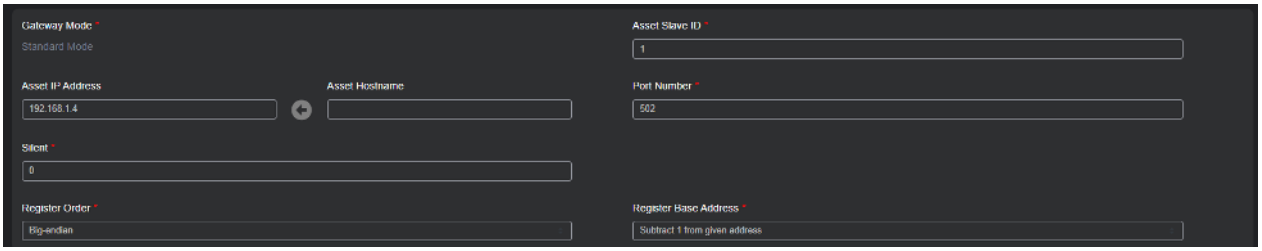


Figure 64: Template Communication Protocol: Modbus TCP/IP

Table 28: Template Communication Protocol Modbus TCP/IP -- Configuration

Field	Description	Specification	Required
Asset IP Address	Specifies the IPv4 address of the target device to be monitored.	0.0.0.0 to 255.255.255.255	Yes
Asset Slave ID	This is where the ID of the device being monitored is configured.	1 to 256	Yes
Port Number	Specifies the TCP port number used to establish communication with the device.	1 to 65 535 (Default: 502)	Yes
Silent	The silent mode functionality is used to introduce a timeout in the acquisition loop, giving some legacy equipment "room to breathe" when being polled via serial communication. The silent setting adds the configured delay between each acquisition. For example, if you set a silent period of one second, the iO will wait one second after each acquisition to give the legacy device time to respond. Most of the time, the silent value should be set to zero, but in certain cases, it provides additional flexibility for the user.	0 to 100 seconds	Yes
Register Order	The register order is used when dealing with data types larger than 16 bits (like 32-bit integers and 32-bit float). The Big Endian also called “Most Significant Byte (MSB) First”, the high-order byte or word comes first (lowest address). Example for a 32-bit value split into two 16-bit registers: • Register 40001: 0x1234 • Register 40002: 0x5678 • Combined Result: 0x12345678	Dropdown: • Big-Endian • Little-Endian	Yes

	The Little Endian also called “Least Significant Byte (LSB) First”, the low-order byte or word comes first (lowest address). Example for a 32-bit value split into two 16-bit registers: • Register 40001: 0x5678 • Register 40002: 0x1234 • Combined Result: 0x12345678		
Register Base Address	The field determines how the Modbus register address should be interpreted when polling a device. Use given address: The register address entered by the user is used as-is, with no adjustment. For example, if you enter address 40001, the system will poll exactly that address. Subtract o**ne** from given address**:** Some Modbus devices use 1-based addressing (e.g., 40001), while others use 0-based addressing (e.g., zero for the first register). Selecting this option automatically subtracts o**ne** from the entered address to align with devices that use 0-based indexing. For example, entering 40001 will result in polling register 40000**.**	Dropdown: • Use given address • Subtract 1 from given address	Yes

SNMP

The iO supports the SNMP protocol (v1, v2c, and v3), allowing it to query multiple devices over an Ethernet network to retrieve performance and status information.

The figure and table below display the various fields required to configure the communication settings for polling an SNMP-compatible device. These fields define key parameters such as IP address, SNMP version, community string (for v1/v2c), security credentials (for v3), and Constant Part of OID (Object Identifier), ensuring reliable communication and data acquisition from SNMP-enabled devices.

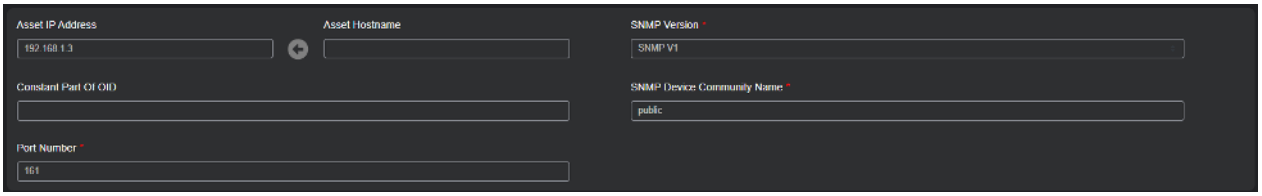


Figure 65: Template Communication Protocol: Modbus TCP/IP

Table 29: Template Communication Protocol Modbus TCP/IP – Configuration

Field	Description	Specification	Required
Asset IP Address	Specifies the IPv4 address of the target device to be monitored.	0.0.0.0 to 255.255.255.255	Yes
Asset Hostname	Optional field used to define a DNS-resolvable name for the device.	Alphanumeric hostname	No
SNMP Version	Select the version of SNMP to be used for communication.	Dropdown: • SNMP v1 • SNMP v2c • SNMP v3	Yes
SNMP Device Community Name	Text string that acts as a password for SNMP v1/v2c communication. Common values include public or private.	Alphanumeric string	Yes
Port Number	Port number used for SNMP polling. The default SNMP port is 161.	1 to 65 535 (Default: 161)	Yes
Constant Part of OID	Base Object Identifier (OID) used to define the SNMP MIB structure to be queried. Data points are typically appended to this base OID.	Dot-separated OID format (e.g., 1.3.6.1.4.1.x.x)	No
Username (SNMPv3)	Username used for SNMPv3 authentication.	Alphanumeric	Yes (v3 only)
Security Level (SNMPv3)	Defines the authentication and privacy level for SNMPv3.	Dropdown: • No Auth, No Priv • Auth, No Priv • Auth, Priv	Yes (v3 only)
Default Context Name	Optional SNMPv3 context name, used when accessing specific MIB views on the agent.	Alphanumeric string	No (v3 only)
Authentication Protocol	Defines the hashing algorithm used for SNMPv3 authentication.	Dropdown: • MD5 • SHA	Required if Auth is enabled
Authentication Password	Password used for SNMPv3 authentication.	Minimum length varies by device policy	Required if Auth is enabled
Privacy Protocol	Defines the encryption method used to protect SNMPv3 payloads.	Dropdown: • DES • AES	Required if Privacy is enabled
Privacy Password	Password used for SNMPv3 privacy encryption.	Minimum length varies by device policy	Required if Privacy is enabled

4.2.3.2 Polling Engine

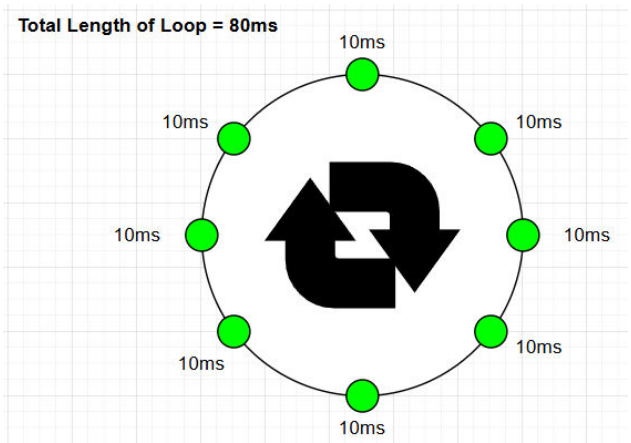
The polling engine is responsible for managing how the iO communicates with external devices to collect data. This section allows users to fine-tune the behavior of the polling mechanism, including the frequency, timeout behavior, retry attempts, and the overall polling duration. These settings are critical for optimizing performance, especially in environments with devices that have varying response times or reliability.

The polling engine uses an acquisition loop to handle requests for retrieving information from various devices. There are two distinct loops: one for Modbus RTU and Modbus TCP/IP, and another for SNMP. This means that performance may vary depending on the number of devices being polled.

Let's take the example of a single device being polled using SNMP with eight data points.

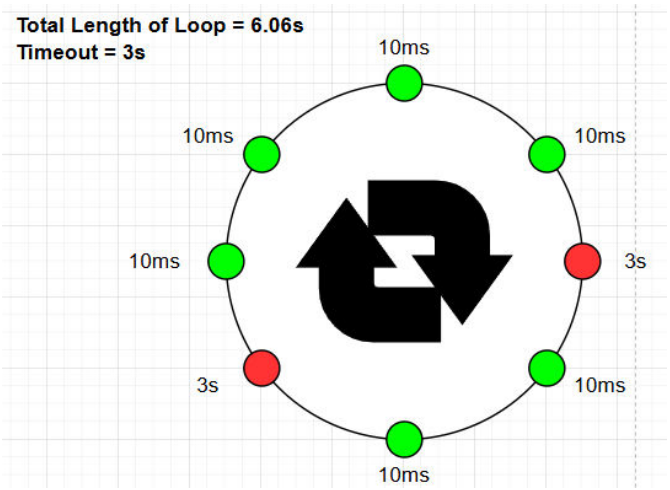
If all data points are configured with a polling rate of one second, the iO will send a request to the device every second to retrieve the data. The request/response cycle is usually fast, especially with SNMP.

Here is a visual representation of the acquisition loop:



In this example, the total duration of the loop is 80 ms, so the one-second polling rate will be easily met.

In the next example, we use the same device but introduce data points that are not responding. When a data point fails to respond, the timeout mechanism is triggered. The timeout acts as a delay between the request and the expected response. The iO sends the request and waits for the configured timeout duration before moving on to the next data point. If the data point is in error or unresponsive, the iO will wait the full timeout period before continuing.



In this example, the total duration of the loop is 6.06 seconds with a timeout of three seconds, so the one-second polling rate will not be met.

As indicated previously, all acquisitions from Modbus RTU, Modbus TCP/IP, and SNMP devices are handled within the same loop. Therefore, it is important to consider that enabling a large number of devices with data points in error can introduce latency across the entire system. Fully functional devices may be negatively impacted by others that are not responding correctly.

⚠ **Warning:**
Enabling a large number of devices with data points in error can introduce latency across the entire system.

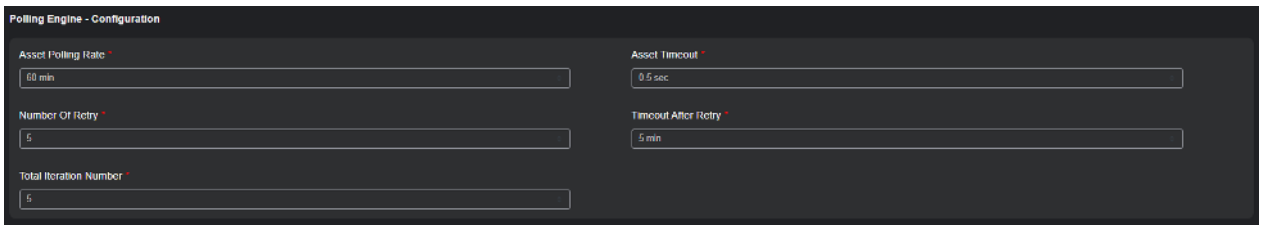


Figure 66: Template Polling Engine

Table 30: Template Polling Engine - Configuration

Field	Description	Specification	Required
Asset Polling Rate	Defines how often the system polls the device. This determines the interval between each acquisition cycle.	Dropdown	Yes
Asset Timeout	Maximum time to wait for a device response before considering the request as failed.	Dropdown	Yes
Number of Retry	Number of retry attempts after a polling failure before triggering the retry timeout period.	Dropdown	Yes

Timeout After Retry	Time the polling engine waits before restarting polling for a device after all retry attempts have failed.	Dropdown	Yes
Total Iteration Number	Total number of polling loops to execute for the given device or configuration. Used to limit the polling sequence duration.	Dropdown	Yes

4.3 UNITS

The Units parameters can be accessed from the settings module.

Figure 67: Settings -- Units

Units are used in analog data points to provide a visual representation of the physical measurement. They serve purely as display elements and do not perform any conversion or scaling of the actual data. For example, changing the unit from VA to kVA will not apply any scaling to the data point value. If scaling is required, the "factor" functionality should be used instead.

The only exception is for temperature units (°C and °F) in the I/O Channels section. When the front-end type is set to Temp, users can toggle between °C and °F, and the conversion will be automatic.

The Units section covers the Unit ID, which is a unique identifier for the unit label. The Unit Name is the full name of the physical unit, and the Abbreviation is what is actually displayed in the iO. Please note that units are preloaded in the iO, and users cannot add custom units themselves.

Units Id	Unit Name	Abbreviation
—	Apparent Power	
27	Volt-ampere	VA Master Unit
28	Kilovolt-ampere	kVA
29	Megavolt-ampere	MVA

Figure 68: Units

4.4 PROTOCOLS

The Protocols parameters can be accessed from the settings module.

Figure 69: Settings – Protocols

4.4.1 HTTP/HTTPS

Using HTTP and HTTPS simultaneously are not recommended. However, both protocols are enabled by default from the factory. It is recommended to disable one of the two.

The default port for HTTP is 80 and 43 for HTTPS. To change these defaults, enter a port number between 1 and 65 534. To ensure proper communication, each protocol must be assigned a unique port number.

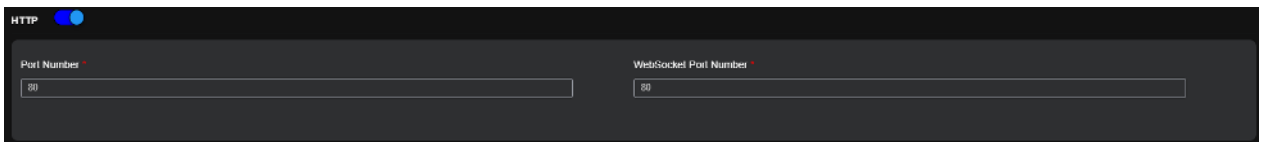


Figure 70: Settings – HTTP

Table 31: HTTP -- Configuration

Field	Description	Specification	Required
HTTP Enabled	Toggles HTTP access to the device.	Enabled (default)	Yes
Port Number	Port used for standard HTTP access. Default is 80.	1 to 65 535 (Default: 80)	Yes
WebSocket Port Number	Port used for WebSocket communication over HTTP.	1 to 65 535 (Default: 80)	Yes

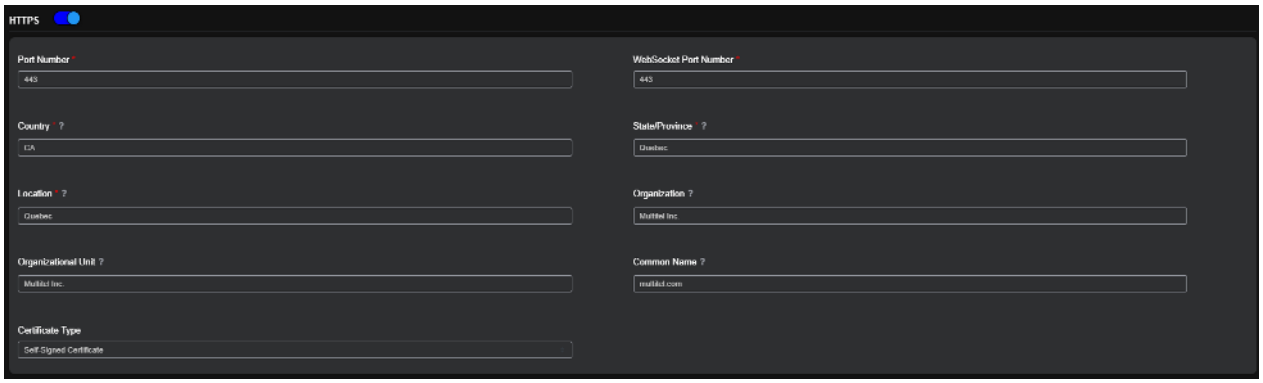


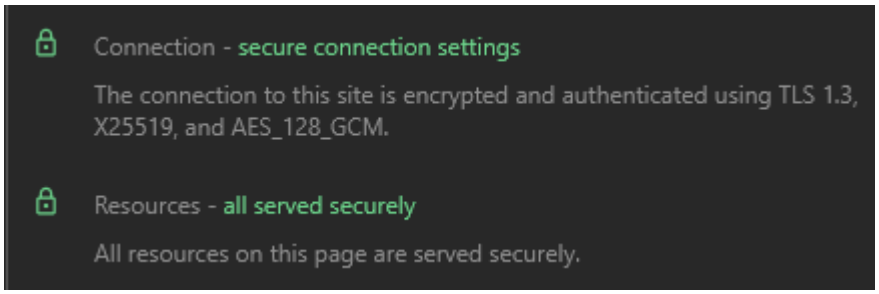
Figure 71: Settings – HTTPS

Table 32: HTTPS – Configuration

Field	Description	Specification	Required
HTTPS Enabled	Toggles HTTPS access to the device.	Enabled (default)	Yes
Port Number	Port used for standard HTTPS access. Default is 80.	1 to 65 535 (Default: 80)	Yes
WebSocket Port Number	Port used for WebSocket communication over HTTPS.	1 to 65 535 (Default: 80)	Yes
Country	Country code used in the SSL certificate generation.		Yes
State/Province	State or province name used in the SSL certificate.		Yes
Location	City or locality for SSL certificate.		Yes
Organization	Legal name of the organization used in the SSL certificate.		Yes
Organizational Unit	Department or unit within the organization. Used in the SSL certificate.		Yes
Common Name	Fully qualified domain name (FQDN) of the device. Must		Yes

	match the access URL for HTTPS to work properly.		
Certificate Type	Type of SSL certificate used. This can be a self-signed certificate or a CA-issued certificate.		Yes

⚠ **Note:**
The HTTPS version supports encryption and authentication using TLS 1.3, X25519, and AES_128_GCM:



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 Atlas to gather data from the iO device.

To configure the SNMP Agent:
- Click on Settings.
- Click on Protocols -- SNMP Agent tab.
- Enter a Port Number.
- The default port is 161. To change this default, enter a port number between 1 to 65 534.
- Enable the SNMP v1/v2c Agent or v3.
- Enter a Read Community Name.
- Click on Submit.

4.4.3 SNMP – TRAP

This section is used to configure the SNMP Trap Receiver on the iO device. It is part of the Trap Forwarding feature.

To configure the SNMP Trap:
- Click on Settings.
- Click on Protocols – SNMP – Trap tab.

- Enter a Port Number.
    - The default port is 161. To change this default, enter a port number between 1 to 65 534.
- Enable the SNMP v1/v2c .
- Enter a Read Community Name.
- Click on Submit.

4.4.4 SSH

This section is used to configure the SSH console.

- Click on Settings.
- Click on Protocols – SSH tab.
- Enter a Port Number
    - The default port is 22. To change this default, enter a port number between 1 to 65 534.
- Enable the SSH .
- Click on Submit.

4.4.5 PING

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

4.4.6 MODBUS

The Modbus section is used to configure the Modbus RTU Server ID. This Server ID will be used by the RTU to monitor the iO device.

To configure the Modbus Server ID:

- Click on Settings.
- Click on Protocols -- Modbus Server tab.
- Click on Enable.
- Enter the Server ID
    - The default server ID is 80. To change this default, enter a port number between 1 to 255.
- Click on Submit.

4.4.7 DNP3 OUTSTATION

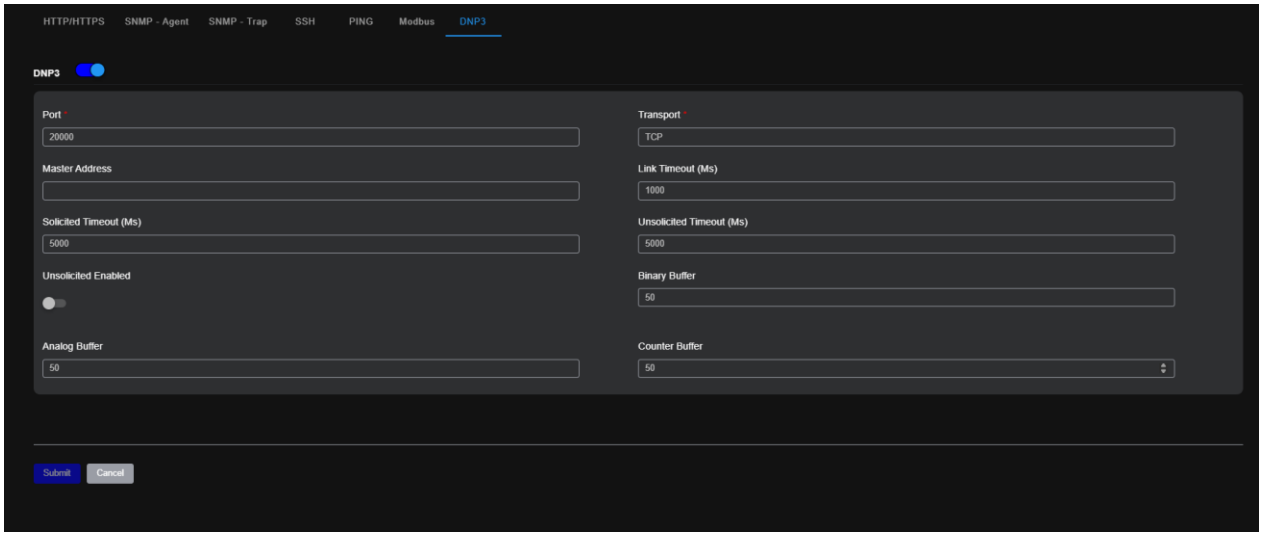


Figure 72: DNP3 Outstation Configuration

The DNP3 module allows the iO platform to operate as a DNP3 Outstation over TCP, enabling communication with a DNP3 Master. This section describes how to configure the transport, communication parameters, and event buffering.

4.4.7.1 Overview

When enabled, the iO acts as a DNP3 Outstation, responding to requests from a Master and optionally sending unsolicited events.

Typical use cases include:

- SCADA integration
- Protocol translation (SNMP/Modbus → DNP3)
- Remote monitoring of power and environmental assets

4.4.7.2 Enabling DNP3

- Toggle DNP3 to ON to activate the Outstation.
- When disabled, no DNP3 communication is performed.

4.4.7.3 Configuration Parameters

Table 33: DNP3 Outstation – Configuration

Field	Description	Specification	Required
DNP3 Enable	Enables or disables the DNP3 Outstation functionality	Toggle (On/Off)	Yes
Port	TCP port used by the DNP3 Outstation to listen for incoming Master connections	1–65535 Default: 20000	Yes
Transport	Communication transport protocol used for DNP3 communication	1 – TCP/IP	Yes
Master Address	Logical address of the DNP3 Master used at the link layer for communication	Integer (0–65535)	Yes
Link Timeout (ms)	Maximum time to wait before considering the link-layer communication failed	Numeric (ms) Default: 1000	Yes
Solicited Timeout (ms)	Maximum time allowed to respond to a Master request (polling)	Numeric (ms) Default: 5000	Yes
Analog Buffer	Maximum number of analog input events stored before transmission	1 to x Default: 50	Yes
Binary Buffer	Maximum number of binary input events stored before transmission	1 to x Default: 50	Yes
Counter Buffer	Maximum number of counter events stored before transmission	1 to x Default: 50	Yes
Unsolicited Enabled	Enables unsolicited messaging where the Outstation sends events without polling	Toggle (On/Off)	No
Unsolicited Timeout (ms)	Timeout waiting for acknowledgment of unsolicited messages	Default: 5000	No

4.4.7.4 Operational Behavior

Solicited Mode (Polling)

- The Master sends requests (e.g., integrity poll, class poll).
- The Outstation responds with current or event data.
- This is the default and most common mode.

Unsolicited Mode

- When enabled, the Outstation sends events automatically.
- Requires Master support and proper configuration.
- Reduces polling traffic but increases complexity.

4.5 NOTIFICATIONS

The Notifications parameters can be accessed from the settings module.

Figure 73: Settings -- Notifications

4.5.1 CONFIGURATIONS

This section is used to configure the notifications for a binary data point.

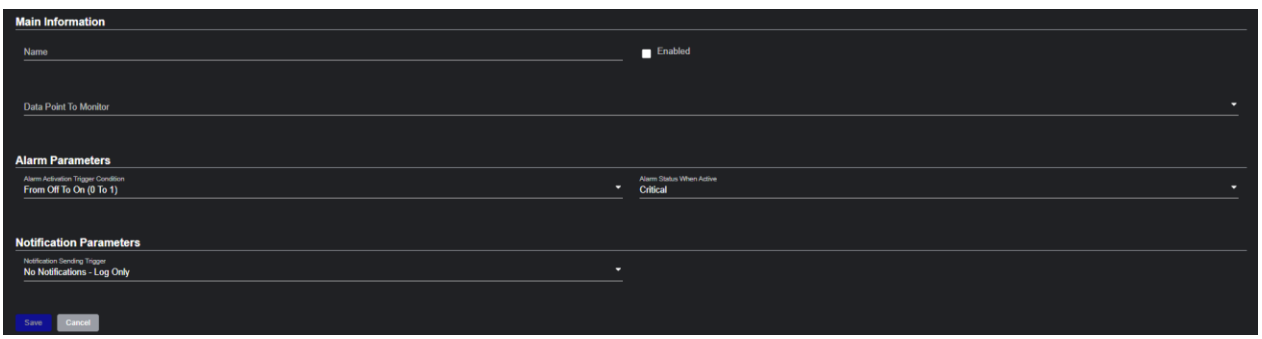


Figure 74: Settings -- Notifications

This section allows users to configure alarm conditions on specific monitored data points. When the configured trigger condition is met, the iO device logs the alarm event and, depending on configuration, may also generate notifications.

The alarm configuration consists of three parts:

- **Main Information** – Defines basic parameters such as name, status, and the data point to be monitored.
- **Alarm Parameters** – Specifies the condition that triggers the alarm and the severity level.
- **Notification Parameters** – Determines whether a notification is generated when the alarm is triggered.

Every binary data point in the iO can be used to trigger a notification. This includes binary data points from physical I/O channels, Modbus, SNMP, and computed data points.

The trigger condition is based on the value of binary data points. There are two different triggering conditions:

- **From Off to On (0 to 1):** The notification will be triggered when the condition of the data point goes from False to True.
- **From On to Off (1 to 0):** The notification will be triggered when the condition of the data point goes from True to False

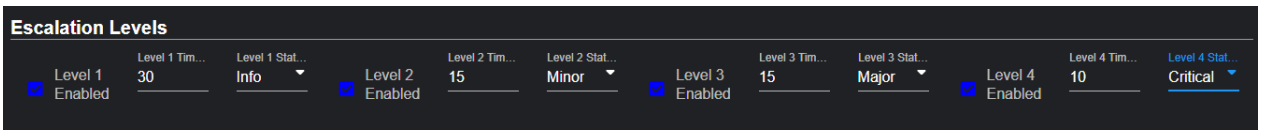


Figure 75: Settings -- Notifications –- Escalation Levels

The Escalation Levels section allows the user to automatically increase (escalate) the alarm severity over time when the alarm condition remains active. This is useful to differentiate a short transient alarm from a persistent issue that requires more attention.

When the trigger condition becomes active, the iO device starts the escalation timer. If the alarm is still active after the configured delay, the alarm severity is updated to the next escalation level. Here is the key behavior:

- Escalation is applied only while the alarm remains active.
- Escalation levels are processed in order (Level 1 → Level 4).
- Each level becomes active after its configured delay.
- The selected status for each level must match a configured alarm level.

Configuration Fields

For each level (Level 1 to Level 4), the following parameters are available:

- **Enabled** (checkbox)
  Enables or disables the escalation level.
- **Time (s)**
  The delay (in seconds) before the level is applied *after the alarm becomes active*.
- **Status** (drop-down)
  The severity level to apply when this escalation level is reached (e.g., Info, Minor, Major, Critical).

Example
If Level 1 is configured as Info after 30s, Level 2 as Minor after 15s, Level 3 as Major after 15s, and Level 4 as Critical after 10s:

- The alarm starts at the Default Alarm Status when it becomes active.
- After 30 seconds, it escalates to Info (Level 1).
- After an additional 15 seconds, it escalates to Minor (Level 2).
- After an additional 15 seconds, it escalates to Major (Level 3).
- After an additional 10 seconds, it escalates to Critical (Level 4), until the alarm clears.

How to Configure Escalation Levels

1. Go to Settings.
2. Select Notifications.
3. Open an existing notification configuration or create a new one.
4. In Escalation Levels, enable the desired levels.
5. For each enabled level, set:
    - Time (s)
    - Status
6. Click Save.

Notes/Best Practices

- Keep escalation delays aligned with your operational process (e.g., short delays for critical infrastructure, longer delays for noisy signals).
- If you want a fixed severity with no escalation, disable all levels and rely only on Default Alarm Status.
- Make sure the Status options (Info/Minor/Major/Critical) are defined and ordered correctly in STATUSES so escalation matches your priority rules.

When the triggered condition is valid, the notification parameters will be applied:

- **No Notifications – Log Only**: The event is logged internally, but no notification is sent.
- **Notification When the Alarm Become Active**: A notification is sent when the alarm is triggered.
- **Notification When the Alarm Becomes Active and When It Comes Back to Normal:** A notification is sent when the alarm is triggered, and a separate "clear" notification is sent when the condition returns to normal.

4.5.2 TRAP DESTINATIONS

Please refer to the following sections in this guide:

- TRAP DESTINATIONS OVERVIEW
- TRAP DESTINATIONS CONFIGURATION

4.5.3 STATUSES

To configure alarm levels, this can be done by following these steps:

- Go to Settings.
- Go to Notifications.
- Click on Status tab.
- Click on + Status.

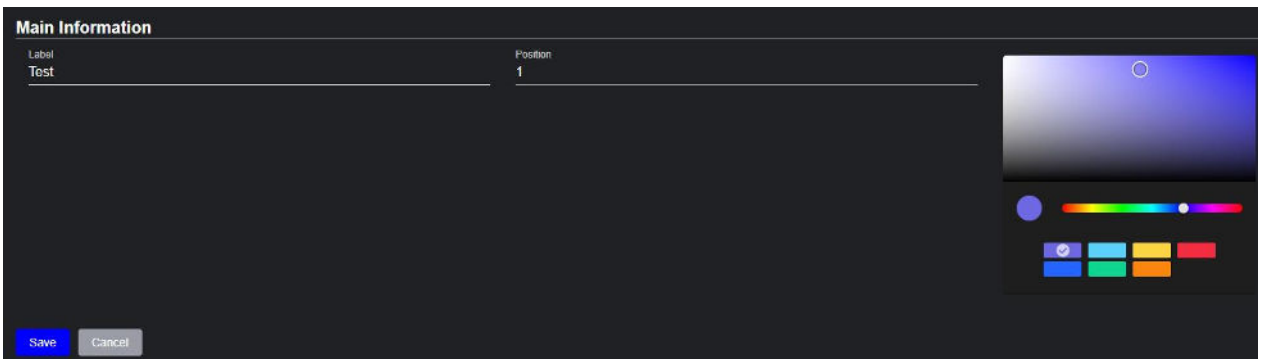


Figure 76: Alarm Level Creation

The position is used to prioritize the alarm level. The position should be configured in the following way:

- Position #1: Critical Alarm
- Position #2: Major Alarm
- Position #3: Minor Alarm
- Position #4: Informational Alarm

Figure 77: Alarm Priority Level

4.6 LABELS

4.6.1 BINARY LABELS OVERVIEW

Binary Labels are used in binary data points.

The defined labels are used to display the value of a binary data point. If the data point has the value *True*, the One Label will be displayed, and if it has the value *False*, the Zero Label will be displayed.

A binary label used in an asset or asset type cannot be deleted.

4.6.2 BINARY LABEL CONFIGURATION

To configure binary labels:

- Go to Settings.
- Go to Labels.
- Click on Binary Labels tab.
- Click on + Label to create a new binary label.
- Click on Save Label to save a new binary label or to make changes to an existing one.

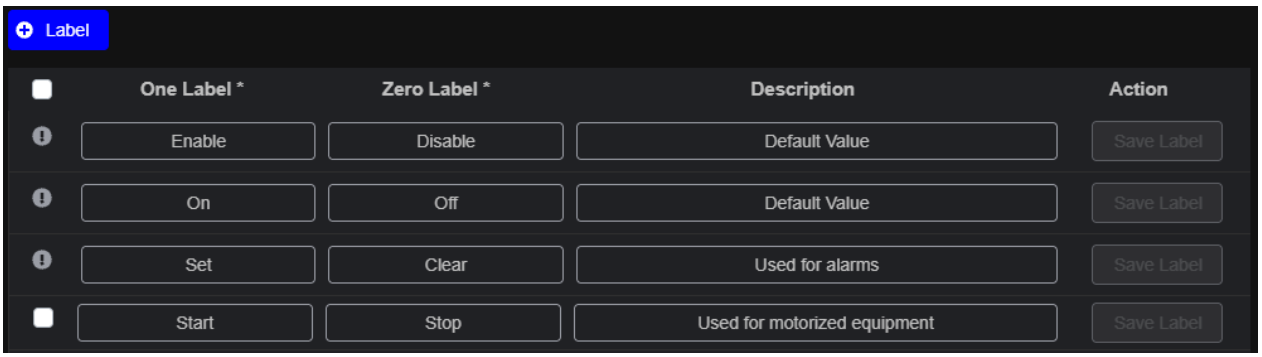


Figure 78: Binary Labels – Configuration

Table 34: Binary Labels – Configuration

Field	Description	Specification	Required
One Label	Label displayed if the data point value is *True*. All One Label must be unique.	1 to 50 characters	Yes
Zero Label	Label displayed if the data point value is *False*. All Zero Label must be unique.	1 to 50 characters	Yes
Description	Allows to explain the use of the binary label. It is only visible on the binary labels page.	1 to 250 characters	No
Action	Allows to save the changes of the binary label.	Button	

4.7 LOGS

The Logs module is used to export diagnostic information from the iO device. These logs help track configuration changes and provide sampling data for troubleshooting acquisition issues.

The Log page contains two main tabs:

- Data Points
- System

4.7.1 DATA POINTS

The Data Points tab provides tools to export information related to binary data points logs and analog data points sampling.

4.7.1.1 Binary Data Points

This section allows users to export the most recent changes applied to binary data points.

To export the latest binary data point changes, follow these steps:

- Go to Logs.
- Select the Data Points tab.
- In Binary Data Points, click Download Latest Binary Data Points Changes.

The exported file includes the following columns:

- **Equipment Name**
  Name of the asset associated with the binary point
- **Data Point Name**
  Display name / description of the binary data point (e.g., *DPAT B1*, *DP B10*, etc.).
- **Mnemonic**
  Unique identifier of the binary point (e.g., *M1BI1*, *M1BI10*).
- **Status**
  The reported state/value at the time of the event (e.g., *Stop, Stopped, Close, Off, Clear, Running*).
  Status values depend on the template and the device mapping.
- **Date**
  Date when the change was recorded (YYYY-MM-DD).

- **Time**
  Time when the change was recorded (HH:MM:SS).

A	B	C	D	E	F
Equipment Name	Data Point Name	Mnemonic	Status	Date	Time
Annie Asset - Modbus TCP/IP - Loop Back	DPAT B1	M1BI1	Stop	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DPAT B1	M1BI1	Stop	2026-02-10	15:35:25
Annie Asset - Modbus TCP/IP - Loop Back	DP B10	M1BI10	Stop	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B10	M1BI10	Stop	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B11	M1BI11	Stopped	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B11	M1BI11	Stopped	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B12	M1BI12	Close	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B12	M1BI12	Close	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B13	M1BI13	Stopped	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B13	M1BI13	Stopped	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B14	M1BI14	Stop	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B14	M1BI14	Stop	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B15	M1BI15	Stop	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B15	M1BI15	Stop	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B16	M1BI16	Off	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B16	M1BI16	Off	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B17	M1BI17	Clear	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B17	M1BI17	Clear	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B18	M1BI18	Off	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B18	M1BI18	Off	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DP B19	M1BI19	Stop	2026-02-10	15:35:24
Annie Asset - Modbus TCP/IP - Loop Back	DP B19	M1BI19	Stop	2026-02-10	15:35:39
Annie Asset - Modbus TCP/IP - Loop Back	DPAT B2C	M1BI2	Running	2026-02-10	15:38:06

Figure 79: Binary Data Points – Log File

4.7.1.2 Data Point Sampling

The Data Point Sampling feature is used to record time-series values of a selected data point into a .CSV file, even when the value does not change.

To export a sampling file, follow these steps:

- Go to Settings.
- Go to Logs.
- Select the Data Points tab.
- In Data Point Sampling, select the desired sampling entry from the drop-down (e.g., *Datapoint sampling for S2AI1*).
- Click Export.

If the sampling file is no longer needed:

- Select the sampling entry.
- Click Delete File.

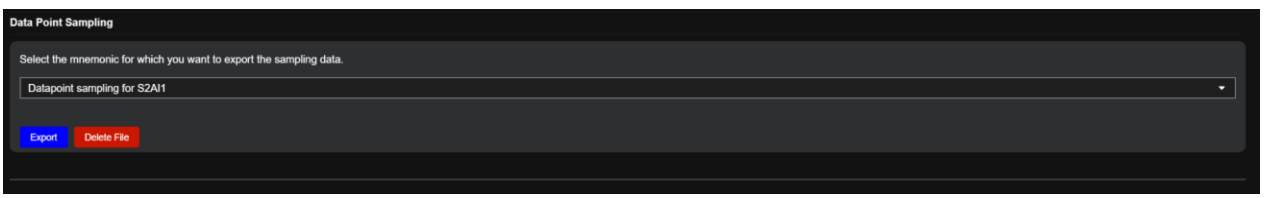


Figure 80: Data Point Sampling

Data point sampling requires a Lua computed data point script that enables sampling for a specific mnemonic. The sampling can be enabled:

- At the Asset Data Point level, or
- At the Asset Type level.

Once enabled by the Lua script, the mnemonic becomes available in the Data Point Sampling drop-down list.

The exported sampling file is generated as a .CSV and typically includes:

- **DateTime**
  Timestamp in UTC format.
- **Local DateTime**
  Timestamp in local time with time zone offset.
- **Value**
  The acquired value recorded at the sampling rate.

DateTime	Local DateTime	Value
2025-11-05T19:23:09Z	2025-11-05T14:23:09-05:00	22
2025-11-05T19:23:10Z	2025-11-05T14:23:10-05:00	22
2025-11-05T19:23:10Z	2025-11-05T14:23:10-05:00	22
2025-11-05T19:23:11Z	2025-11-05T14:23:11-05:00	18.5
2025-11-05T19:23:11Z	2025-11-05T14:23:11-05:00	18.5
2025-11-05T19:23:11Z	2025-11-05T14:23:11-05:00	18.5
2025-11-05T19:23:26Z	2025-11-05T14:23:26-05:00	20
2025-11-05T19:23:40Z	2025-11-05T14:23:40-05:00	21
2025-11-05T19:23:56Z	2025-11-05T14:23:56-05:00	18.5
2025-11-05T19:24:11Z	2025-11-05T14:24:11-05:00	21
2025-11-05T19:24:26Z	2025-11-05T14:24:26-05:00	19.5

Figure 81: Data Point Sampling File

Given the value is written at the configured sampling rate, the file may contain repeated values even when the data point is stable.

To start sampling, use the function below in a Lua computed data point:
enableDatapointSampling('MNEMONIC', 'SamplingDurationUnit', 'SamplingDuration', 'SamplingRate')

This function writes acquired values to a .CSV file at the requested rate, for the configured duration.

Parameters

- **MNEMONIC**
  Mnemonic (identifier) of the data point to sample.
- **SamplingDurationUnit**
  Unit used for the sampling duration. Supported values are:
  - '"s" seconds
  - "m" minutes
  - "h" hours
- **SamplingDuration**
  Duration of the sampling session (used with the unit).
- **SamplingRate**
  Rate (in seconds) at which values are written to the sampling file.
  This overrides the data point's default delay for logging purposes.

⚠ **Note:**

Using multiple data points at a low sampling rate (e.g., < 5 seconds) may impact device performance.

To stop sampling for a data point, use:

disableDatapointSampling('MNEMONIC')

This disables sampling for the specified mnemonic and stops writing values to the .CSV file.

Usage Example:
You have a binary data point (S1BI1) and an analog data point (S1AI1). You want to sample S1AI1 only when S1BI1 is true.

```
asset.autoRefreshWith('S1BI1')  -- Run this script every time S1BI1 acquires a new value
local enabled = asset.getDatapoint('S1BI1')  -- Get the value of S1BI1
if enabled then
   asset.enableDatapointSampling('S1AI1', 'm', 10, 5)  -- Sample for 10 minutes, every 5 seconds
else
   asset.disableDatapointSampling('S1AI1')  -- Stop sampling
end
```

This example:

- Monitors S1BI1.
- Starts sampling S1AI1 for 10 minutes at five-second intervals when S1BI1 is active.
- Stops sampling when S1BI1 becomes inactive.

4.7.2 SYSTEM

The System tab provides exports for security and diagnostic logs generated by the iO device. These files are typically used for troubleshooting, audits, and support investigations.

The System page contains two sections:

- Security
- Diagnostics

A Back button is available to return to the previous page.

4.7.2.1 Security

The Security Logs export provides an audit trail of authentication activity on the iO device. These logs are primarily used to track user sessions, verify who accessed the system, and identify the source IP address of each connection.

To export the security logs:

- Go to Logs.
- Select the System tab.

- In Security, click Download Security Logs.

The exported log is a text-based file where each line represents one event.

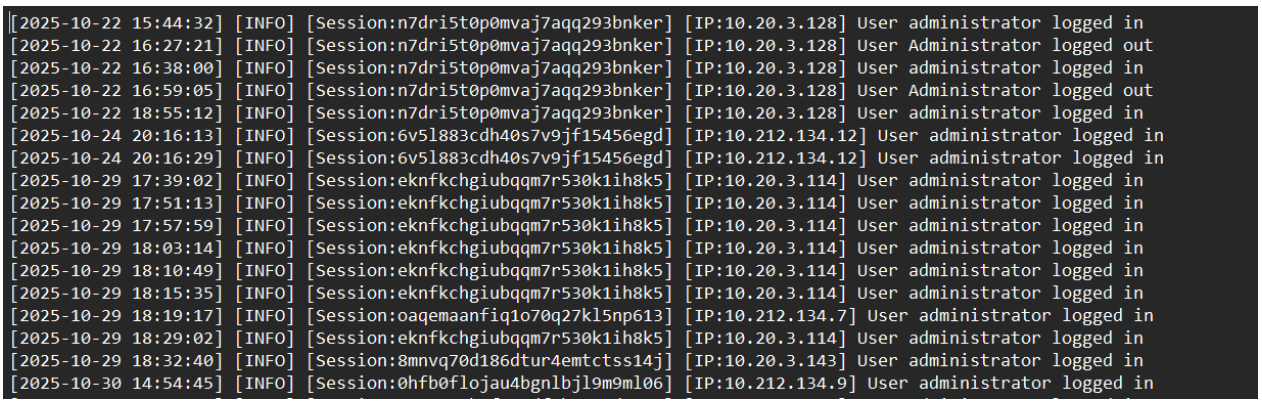


Figure 82: Security – Log File

A typical entry contains:

- **Timestamp**
  Date and time when the event occurred (e.g., 2025-10-22 15:44:32).
- **Severity**
  Log level (e.g., INFO).
- **Session ID**
  Unique identifier for the user session (example: Session:n7dri5t0p0mvaj7aqq293bnker).
- **Source IP Address**
  IP address of the client that connected to the iO device (e.g., IP:10.20.3.128).
- **Event Message**
  Description of the event (e.g., User administrator logged in / User Administrator logged out).

4.7.2.2 Diagnostics

The Diagnostics section is used to export device diagnostic logs. These logs are generally requested for troubleshooting when investigating communication issues, performance problems, or unexpected behavior.

To export diagnostic logs:

- Go to Logs.
- Select the System tab.
- In Diagnostics, click Download All Logs.

4.8 SYSTEM MAINTENANCE

The Inventory parameters can be accessed from the settings module.

Figure 83: Settings – System Maintenance

4.8.1 CONFIGURATION FILE

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

Figure 84: System Maintenance – Configuration File

Before importing a new configuration, make sure no users are performing manual operations.

- In Settings | System Maintenance, click the Configuration File tab.
- Click Export.
    - This step is not mandatory, but it is recommended by Multitel. If the new configuration causes unexpected results, you can restore the device using the backup configuration.
- Click Import.
- Select the new configuration file (CSV or .TXT file).
- Click Start Import.

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

⚠ **Error Messages:**
Even if errors are reported, the configuration will still be imported, except for the lines with errors.

⚠ **Warning:**
When you import a configuration file, all existing device configuration will be replaced by the new configuration. Importing a configuration file may change critical settings (such as Ethernet connection properties), which can impact remote access to the device.

⚠ **Recommendation:**
Multitel recommends backing up or exporting the configuration file before importing a new one. To prevent overwriting existing settings, Multitel also recommends importing only the modified parameters, not the entire configuration file.

4.8.2 SCRIPT TEMPLATES

The Script Templates section is used to load and manage a library of Lua script templates intended for Computed Data Points. These templates provide ready-to-use examples (or starting points) to speed up deployment and standardize calculations across devices (e.g., thresholds with/without hysteresis, averages, chronometers, battery runtime calculations, etc.).

The Script Templates library is accessible from the Settings | System Maintenance menu.

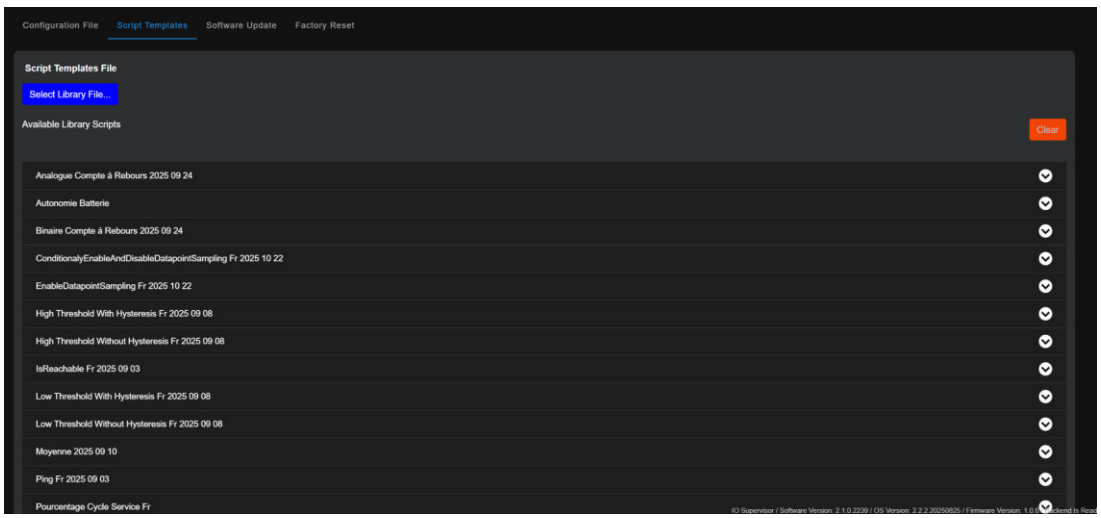


Figure 85: System Maintenance – Script Templates

4.8.2.1 Loading a Script Templates Library

Before loading a new library, make sure no users are performing manual operations.

- In Settings | System Maintenance, click the Script Templates tab.

- Click Select Library File.
- Select the library file provided by Multitel (or your internal library file).
- Once loaded, the templates will appear under Available Library Scripts.

4.8.2.2 *Available Library Scripts*

The Available Library Scripts list displays all templates included in the loaded library.

- Each row represents a script template (template name may include a version or date).
- Click the expand icon (chevron on the right) to display the template details (and its content, if available).
- Use these templates as a reference or starting point when configuring computed data points elsewhere in the platform.

4.8.2.3 *Clearing The Library*

- Click Clear to remove the currently loaded script templates from the page.
- After clearing, the Available Library Scripts list will be emptied until a new library file is loaded.

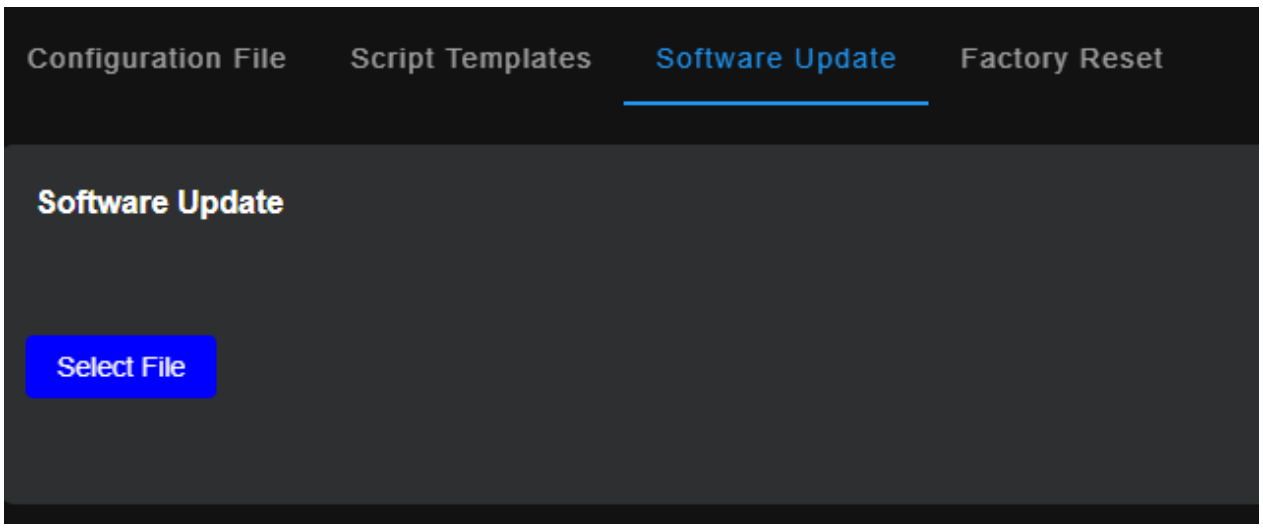
⚠ **Note**: Clearing the library only removes the currently loaded templates from the interface. If you need to restore the templates, reload the library file using Select Library File.

⚠ **Recommendation**: Maintain a controlled, versioned script library (template names including a date/version) to ensure consistent behavior across devices and to simplify troubleshooting and support.

4.8.3 SOFTWARE UPDATE

This section is used to upload a software version to the iO device.

⚠ **Note**: The Software Update process and the OS Update process are the same.



Multitel

Figure 86: System Maintenance – Software Update

Before starting an update, make sure no users are performing manual operations.

- In Settings | System Maintenance, click the Software Update tab.
- Click Select File.
- Select the update file provided by Multitel.
- Start the upload.
- Reboot.

Uploading and installing the update may take a few minutes. The device may reboot during the process. A confirmation or error message will be displayed when the process is complete.

⚠ **Warning:**
Do not power off the device during the update process. Interrupting an update can corrupt the system and may brick the unit, making it unstable, unreachable, or requiring recovery service. The device may also be unreachable for a few minutes during the update, especially if network services restart or the unit reboots.

⚠ **Recommendation:**
Multitel recommends performing updates during a maintenance window and ensuring you have a stable power source. If the device is accessed remotely, plan for a temporary loss of connectivity during the update and ensure you have an alternate access method if needed.

4.8.4 FACTORY RESET

This section is used to perform a factory reset on the iO device.

Figure 87: System Maintenance – Factory Reset

Before performing a factory reset, ensure no users are performing manual operations.

- In Settings | System Maintenance, click the Factory Reset tab.
- Select the reset options as needed:
  - Reset Ethernet (restores Ethernet/network settings to their default values)
  - Reset HMI (restores the HMI configuration)
- Click Reset Now.

The factory reset may take a few minutes. The device may reboot during the process.

⚠ **Warning:**
A factory reset is irreversible. Depending on the selected options, it may restore configuration settings to their default values and can impact remote access to the device (e.g., if network settings are reset).

⚠ Recommendation:
Multitel recommends exporting a backup of the configuration before performing a factory reset. If the device is managed remotely, ensure you have physical access (or an alternate access method) in case network settings are reset.

4.9 REBOOT

The Reboot parameter can be accessed from the settings module.

Figure 88: Settings – Reboot

4.10 GLOBAL PARAMETERS

4.10.1 GLOBAL PARAMETERS OVERVIEW

The Global Parameters page lets you view and manage system-wide settings that apply across the entire device/application (not tied to a specific asset). These parameters are typically used to control common behaviors such as feature toggles, scheduling/automation options, default values, and operational thresholds.

4.10.2 GLOBAL PARAMETERS CONFIGURATION

To configure binary labels:

- Go to Settings.
- Go to Global Parameters.
- Click on + Global Parameter to create a new global parameter.

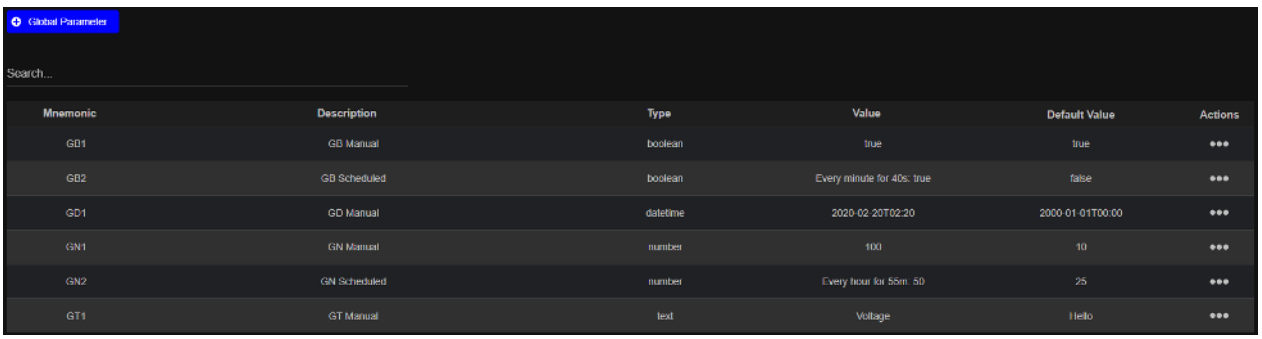


Figure 89: Global Parameters – Configuration

Table 35: Global Parameters – Configuration

Field	Description	Specification	Required
Mnemonic	Unique identifier.	Auto Generate • Boolean: GBxx • Number: GNxx • Text: GTxx • Date: GDxx	
Description	Name explaining what the parameter controls.	1 to 50 characters	Yes
Type	Expected value format.	Dropdown: • Boolean • Number • Text • Date and Time	Yes
Value	Currently active value used by the system.		Yes
Default Value	Original or recommended value for reference.		Yes
Actions	Opens the parameter options menu.	Menu: • Set Value • Edit • Delete	

The Add or Edit Global Parameter screen is used to modify an existing global parameter and define how its value behaves over time. Depending on the parameter type, you can configure a fixed default value or create one or more scheduled rules that automatically apply a value on a recurring basis.

The format of the Default Value and Value fields depends on the selected type:

- **Boolean**: True or False
- **Number**: Number
- **Text**: String
- **Date and Time**: Date and time in format aaaa-mm-jj --:--

4.10.2.1 Add or Edit Global Parameter – Mode Single Value

The Single Value mode is used for global parameters that should keep one constant value at all times (no scheduling). This is the simplest way to configure a parameter such as a text label, a numeric threshold, or a basic on/off setting.

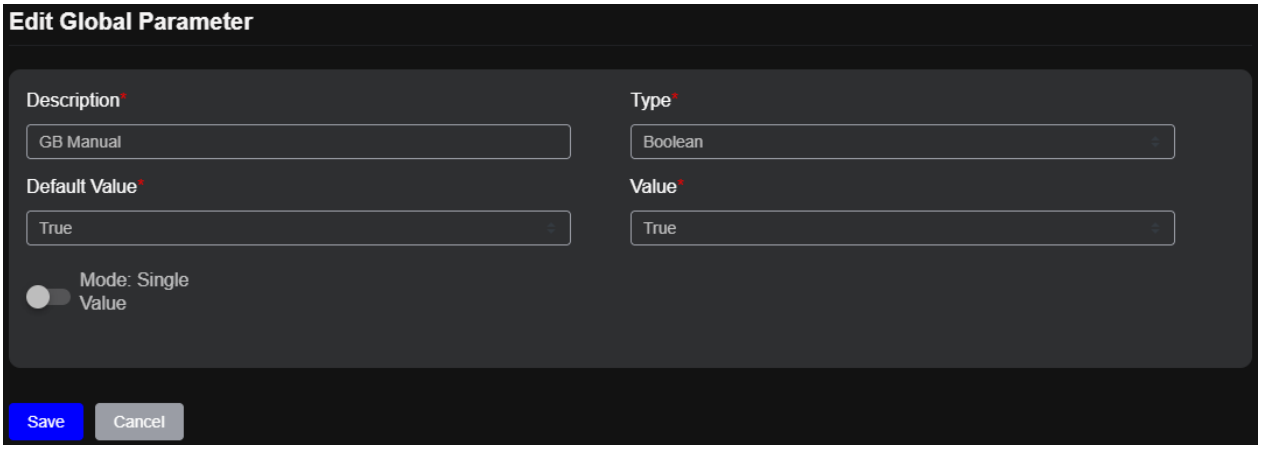


Figure 90: Global Parameters – Mode Single Value

In this case, a value must be entered in the Default Value and Value fields.

- **Default Value**: This is the reference value for this parameter. It can be used as a baseline or reset value, depending on system behavior.
- **Value**: This is the active value currently applied by the system. This is the value that will be used immediately once saved.

4.10.2.2 Add or Edit Global Parameter – Mode Scheduled

The Scheduled mode is used for global parameters that should apply values automatically on a recurring schedule.

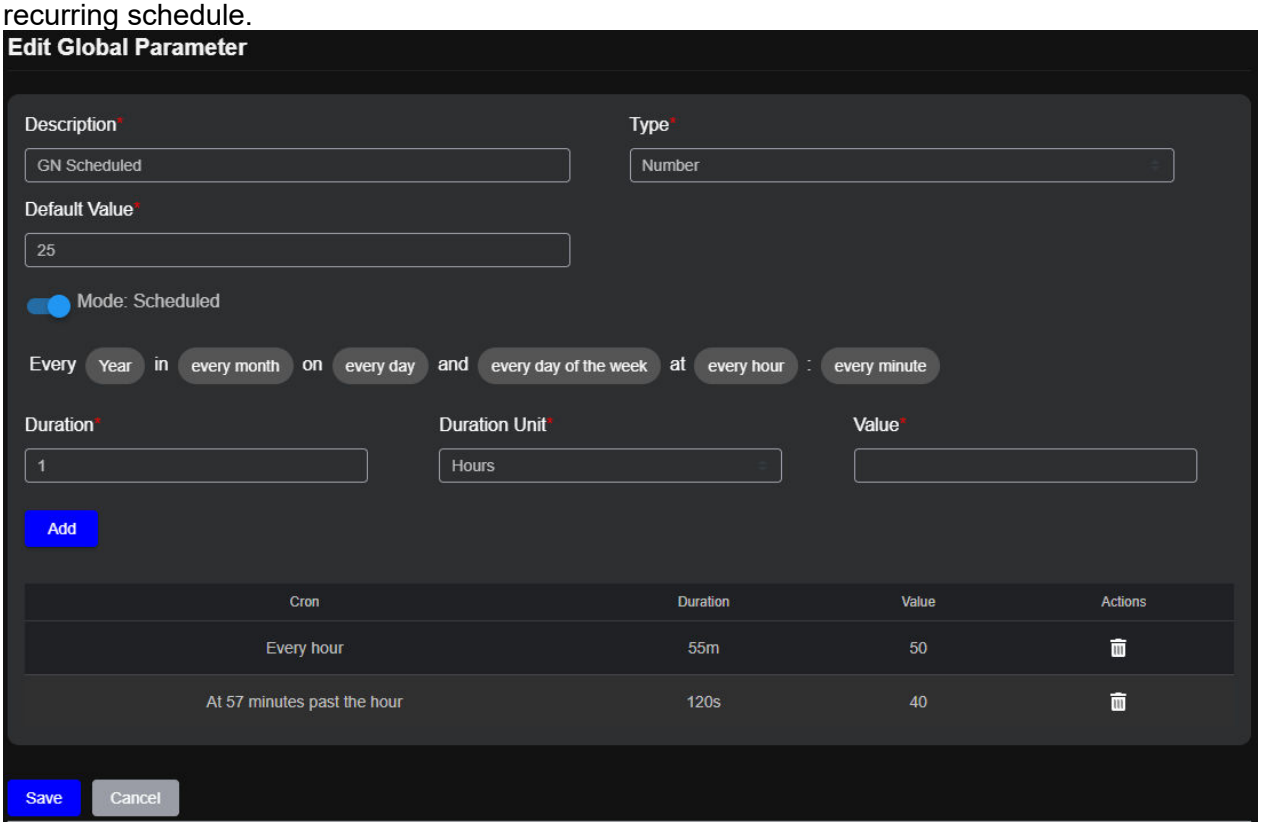


Figure 91: Global Parameters – Mode Scheduled

When scheduled mode is enabled, you can define rules using the following:

- **Every**: Recurrence selector (e.g., every year, month, day, hour, minute).
- **Duration**: How long the rule stays active once it starts.
- **Duration Unit**: Unit for the duration (e.g., hours, minutes, days).
- **Value**: The value to apply during the rule's active window.

Click the Add button to create the rule and insert it into the schedule list.

All created rules appear in a table showing the following:

- **Cron**: The recurrence pattern of the rule.
- **Duration**: How long the rule remains active.
- **Value**: The applied value during that time.
- **Actions**: Remove a rule (trash icon).

Multitel

APPENDIX A: LUA SCRIPT EXAMPLES

A.1 THRESHOLD

This section provides Lua script examples to implement threshold logic on analog data points.

Threshold scripts are typically used to:

- Detect when a value crosses a high or low limit.
- Generate a binary result (e.g., “in alarm” vs “normal”).
- Stabilize alarms using hysteresis to avoid rapid toggling when a value oscillates near the threshold.

Threshold scripts can be used:

- At the asset data point level (computed point associated to a specific asset), or
- At the asset type level (reusable logic applied through templates).

All threshold scripts produce a binary result (e.g., alarm active / alarm normal). For this reason, the computed data point must be configured as a Binary data point in the template or at the asset data point level.

If the computed data point is configured as an Analog type, the threshold output will not be represented correctly in the platform and cannot be used properly for binary alarm logic and notifications.

A.1.1 CONCEPTS

High Threshold
Triggers an alarm condition when the monitored value rises above a configured threshold.

Low Threshold
Triggers an alarm condition when the monitored value drops below a configured threshold.

Hysteresis (Recommended)
Hysteresis introduces a second “return-to-normal” limit so the alarm does not toggle ON/OFF repeatedly when the value is close to the threshold.

- For a High threshold:
  - Alarm becomes Active when value >= HighThreshold
  - Alarm clears when value <= HighThreshold – Hysteresis

- For a Low threshold:
  - Alarm becomes Active when value <= LowThreshold
  - Alarm clears when value >= LowThreshold + Hysteresis
  -

Best Practice: Use hysteresis for signals that can fluctuate (temperature, voltage, current). Without hysteresis, the alarm may oscillate when the signal is near the threshold.

Multitel

A.1.2 SCRIPT INPUTS

Most threshold scripts rely on the following configuration inputs (names can vary depending on your implementation):

- **Source Mnemonic**
  The analog data point to monitor (e.g., S1AI1).
- **Threshold Value**
  The high or low setpoint.
- **Hysteresis Value (optional)**
  The hysteresis band used to clear the alarm.
- **Output Mnemonic / Result**
  A computed result (commonly a binary state or a status) used by notifications, alarms, dashboards, etc.

A.1.3 LOW THRESHOLD WITH HYSTERESIS

Purpose: Prevent alarm toggling when the value hovers near the low threshold.

Behavior:

- Alarm becomes active when value <= LowThreshold.
- Alarm clears when value >= LowThreshold + Hysteresis.

```lua
-- Example structure (generic)
local value = asset.getDatapoint('SOURCE_MNEMONIC')
local low = 10.0         -- LowThreshold
local hyst = 1.0         -- Hysteresis
local clearPoint = low + hyst

-- storedState should be retained (implementation-specific)
local alarmActive = asset.getVar('low_alarm_active') or false

if (not alarmActive) and (value <= low) then
  alarmActive = true
elseif alarmActive and (value >= clearPoint) then
  alarmActive = false
end

asset.setVar('low_alarm_active', alarmActive)
return alarmActive
```

Multitel

A.1.4 HIGH THRESHOLD WITH HYSTERESIS

Purpose: Prevent alarm toggling when the value hovers near the high threshold.

Behavior:

- Alarm becomes active when value >= HighThreshold.
- Alarm clears when value <= HighThreshold – Hysteresis.

```
-- Example structure (generic)
local value = asset.getDatapoint('SOURCE_MNEMONIC')
local high = 50.0        -- HighThreshold
local hyst = 2.0         -- Hysteresis
local clearPoint = high - hyst

-- storedState should be retained (implementation-specific)
local alarmActive = asset.getVar('high_alarm_active') or false

if (not alarmActive) and (value >= high) then
  alarmActive = true
elseif alarmActive and (value <= clearPoint) then
  alarmActive = false
end

asset.setVar('high_alarm_active', alarmActive)
return alarmActive
```

Multitel

A.2 AVERAGE

This section provides Lua script examples to calculate an average value from one or more analog data points. Average scripts are typically used to:

- Smooth noisy signals (voltage, current, temperature, etc.).
- Build a computed “stable” value for dashboards, trends, or downstream logic.
- Reduce alarm chatter by averaging before applying threshold logic.

Important: The Average script output is a numeric value. The computed data point must therefore be configured as an Analog data point.

A.2.1 CONCEPTS

Instant Value vs Averaged Value

- Instant value reflects the latest acquisition (can fluctuate quickly).
- Averaged value is calculated over a set of samples or a time window to reduce short spikes.

Common averaging methods

- **Rolling/Moving Average (N samples):** average of the last N values.
- **Time-based Average:** average of values collected over a duration (e.g., last 60 seconds).

A.2.2 PREREQUISITES AND CONFIGURATION

- The source data point(s) must be Analog.
- The computed data point that returns the average must be configured as:
  - **Data Type:** Analog.
  - **Unit:** same unit as the source (recommended).
  - **Decimals:** set to desired precision.

Best Practice: Keep averaging logic lightweight. If multiple average scripts run at high frequency, it can add CPU load and contribute to performance issues—especially when overall acquisition approaches the device limit (see polling best practices).

A.2.3 TYPICAL INPUTS

Most average scripts rely on:

- **Source Mnemonic(s):** the analog point(s) to average (e.g., S1AI1)..
- **Window Size/Number of Samples (N):** how many values to include
- **Refresh trigger:** which data point update triggers a recalculation (optional but common).

A.2.4 TYPICAL INPUTS

The following example shows a typical moving average approach.

Multitel

```lua
-- Generic example (moving average)
local source = 'S1AI1'
local N = 10

asset.autoRefreshWith(source)

local v = asset.getDatapoint(source)

-- Retrieve rolling buffer (implementation-specific storage)
local buf = asset.getVar('avg_buf') or {}
table.insert(buf, v)

-- Keep only last N samples
while #buf > N do
  table.remove(buf, 1)
end

-- Compute average
local sum = 0
for _,x in ipairs(buf) do
  sum = sum + x
end

asset.setVar('avg_buf', buf)
return sum / #buf
```

Result: Returns an Analog averaged value.

Multitel

APPENDIX B: CONFIGURATION FILE

B.1 HEADER

Description	ID	Read/Write
Model Number	ModelNumber	Read Only
Serial Number	SerialNumber	Read Only
Batch Number	BatchNumber	Read Only
Software Version	SoftwareVersion	Read Only
OS Version	OsVersion	Read Only
Hardware Version	HardwareVersion	Read Only
MAC Address #1	MAC1	Read Only
MAC Address #2	MAC2	Read Only
Site Name	SiteName	Read Only
Downloaded Time	DownloadedTime	Read Only

B.2 CONNECTIONS: RS-485

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	1 – Connections
Connection Port	CP	1 – RS-485 - COM A 2 – RS-485 - COM B
State	ST	1 – Enabled 0 – Disabled
Protocol	PR	5 – Modbus RTU - Master 15 – Modbus RTU - Slave

Multitel

		255 – None
Baudrate	BR	300
		1200
		2400
		4800
		9600 (Default)
		19200
		38400
		57600
		115200
Data Bits	DB	6
		7
		8 (Default)
Stop Bits	SB	1 (Default)
		2
Parity	PA	0 – None (Default)
		1 – Odd
		1 – Even

B.3 CONNECTIONS: ETHERNET

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	1 – Connections
Connection Port	CP	3 – ETH 1 – 1 Gbps
		4 – ETH 2 – 100 Mbps
State	ST	1 – Enabled
		0 – Disabled
Protocol	PR	255 – None (Ethernet)
MTU	MTU	58 to 1500 (Default: 1500)
Speed	SPD	0 – Auto (Default)
		1 – 10 Mb

		2 – 100 Mb 3 – 1 Gb (Only ETH 1)
Mode	MD	0 – DHCP (Default) 1 – Static
IP Address / IP DHCP Address	IP4	0.0.0.0 to 255.255.255.255
MD = 0		
IP Override Gateway	IP4OG	0.0.0.0 to 255.255.255.255
MD = 1		
Subnet Mask	IP4SM	0.0.0.0 to 255.255.255.255
Default Gateway	IP4G	0.0.0.0 to 255.255.255.255
DNS State	DNS	0 – Disabled 1 – Enabled
Preferred DNS Server	DNSP	0.0.0.0 to 255.255.255.255
Alternate DNS Server	DNSS	0.0.0.0 to 255.255.255.255

B.4 PROTOCOLS: HTTP/HTTPS

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	2 – Protocols
Protocol Type	PT	8 – HTTP
State	ST	0 – Disabled 1 – Enabled
Port Number	PN	1 to 65 535 (Default: 80)
WebSocket Port Number	WP	1 to 65 535 (Default: 80)

Description	ID	Value
Configuration Type	CFGT	2 – Protocols
Protocol Type	PT	9 – HTTPS
State	ST	0 – Disabled

		1 – Enabled
Port Number	PN	1 to 65 535 (Default: 443)
WebSocket Port Number	WP	1 to 65 535 (Default: 443)
Certificate Type	CERT	0 – Self-Signed Certificate 1 – Signed Certificate
CERT = 0		
Country	CT	2-character ISO format country code (US or CA)
State/Province	SP	1 to 50 characters. Do not use special characters (! @ # $ % ^ * ( ) ~ ? > < / \) or abbreviations.
Location	LC	Name of the city where the organization is registered. Do not use abbreviations
Organisation	ORG	Legal name under which your organization is registered. Do not use special characters (! @ # $ % ^ * ( ) ~ ? > < / \) or abbreviations.
Organisation Unit	OU	Trade or DBA name.
Common Name	CN	Fully qualified domain name used for DNS lookups of your server.
CERT = 1		
SSL Private Key File	PKF	Private Key File Base64
SSL Certificate File	CRF	Certificate File Content Base64
Filename.key	PKFN	Private Key Filename
Filename.crt	CRFN	Certificate Filename

B.5 PROTOCOLS: SSH

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	2 – Protocols
Protocol Type	PT	11 – SSH
State	ST	0 – Disabled 1 – Enabled
Port Number	PN	1 to 65 535 (Default: 22)

Multitel

B.6 PROTOCOLS: PING

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	2 – Protocols
Protocol Type	PT	4 – PING
State	ST	0 – Disabled 1 – Enabled

B.7 PROTOCOLS: MODBUS SLAVE

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	2 – Protocols
Protocol Type	PT	15 – Modbus RTU Slave
State	ST	0 – Disabled 1 – Enabled
Slave ID	SID	2 to 65 535 (Default: 80)

B.8 PROTOCOLS: SNMP AGENT

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	2 – Protocols
Protocol Type	PT	1 – SNMP Agent
Port Number	PN	1 to 65 535 (Default: 161)
Read Community	CN	public (Default)
State	ST	0 – Disabled 1 – Enabled
State v3	ST3	0 – Disabled 1 – Enabled

ST3 = 1		
Username	UN	admin (Default)
Context Name	DCN	public (Default)
Security Level	SL	1 – No authentication, No privacy
		2 – Authentication, No privacy
		3 – Authentication, Privacy
Authentication Protocol	AP	1 – MD5
		2 – SHA1
Authentication Password	APWD	8 to 50 characters
Privacy Protocol	PP	1 – DES
		2 – AES
Privacy Password	PPWD	8 to 50 characters

B.9 PROTOCOLS: SNMP TRAP

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	2 – Protocols
Protocol Type	PT	21 – SNMP Trap
Port Number	PN	1 to 65 535 (Default: 162)
State	ST	0 – Disabled
		1 – Enabled
Read Community	CN	public (Default)

B.10 GENERAL PARAMETERS – SITE INFORMATION

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	3 – Site Information
Site Name	SN	1 to 50 characters
CLLI	CLLI	1 to 50 characters
Country	CO	Canada

		United States
State/Province	PROV	Province or State
Address	ADDR	1 to 100 characters
City	CT	1 to 50 characters
Zip/Postal Code	ZC	Valid Zip or Postal Code
NPA	NPA	NPA Code
Picture	PIC	File encoding

B.11 GENERAL PARAMETERS – SYSTEM INFORMATION

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	5 – System Information
Network Machine Name	NMN	1 to 15 alphanumeric characters

B.12 GENERAL PARAMETERS – DATE AND TIME

TYPE: CFG

Description	ID	Value
Configuration Type	CFGT	4 – Date and Time
Date Time DT	DT	Current Date Time
Time Zone	TZ	Time Zone Abbreviation (Default: UTC)
NTP State	NTP	0 – Disabled
		1 – Enabled
Primary NTP Server	NTPS1	Valid IP Address or Domain Name
Secondary NTP Server	NTPS2	Valid IP Address or Domain Name
Tertiary NTP Server	NTPS3	Valid IP Address or Domain Name
Date Format	DF	m/d/y – 06/25/24
		m/d/Y – 06/25/2024
		d/m/y – 25/06/24
		d/m/Y – 25/06/2024

		m-d-y – 06-25-24
		m-d-Y – 06-25-2024
		d-m-y – 25-06-24
		d-m-Y – 25-06-2024
Time Format	TF	g:i:s A – 00:57:43 PM
		G:i:s – 12:57:43
		g:i A – 00:57 PM

B.13 SECURITY – LDAP

TYPE: LDAPCFG

Description	ID	Value
State	ST	0 – Disabled
		1 – Enabled
Port	PORT	1 to 65 535 (Default: 656)
Timeout	TO	1 to 5 – 1 to 5 sec (Default: 5)
Secured Connection Type	SECTY	0 – None
		1 – LDAPS/SSL
Trusted Certificate Authority Key	KEY	Encrypted Key
User Search Base DN	USBDN	
Username Attribute	USUA	displayName
Host	HO	0.0.0.0 to 255.255.255.255
Groups	GR	1 – Supervisor
		2 – User
		3 – Viewer
		5 – Contractor
		{"1":"","2":null,"3":null,"5":null }

User Fields Association	FI	{"Firstname":"","Lastname":"","Email":"","Phone":""}

B.14 SECURITY – RADIUS

TYPE: RADIUSCFG

Description	ID	Value
RADIUS Client State	ENA	0 – Disabled 1 – Enabled
NAS Identifier	NAS	0 to 50 characters
Request Timeout	RT	1 to 5 – 1 to 5 sec (Default: 3 sec)
Retries	RTR	1 to 5 – 1 to 5 (Default: 2)
Primary Server	PHO	0.0.0.0 to 255.255.255.255 or hostname
Primary Transport Protocol	PT	0 – UDP
Primary Authentication Port	PAUTHP	1 to 65 535 (Default: 1812)
Primary Accounting Port	PACCTP	1 to 65 535 (Default: 1813)
Primary Shared Secret	PSS	1 to 50 characters – Encrypted
Backup Server	BHO	0.0.0.0 to 255.255.255.255 or hostname
Backup Transport Protocol	BT	0 – UDP
Backup Authentication Port	BAUTHP	1 to 65 535 (Default: 1812)
Backup Accounting Port	BACCTP	1 to 65 535 (Default: 1813)
Backup Shared Secret	BSS	1 to 50 characters – Encrypted

B.15 SECURITY – USERS

TYPE: USER

Description	ID	Value
UUID	UUID	User UUID
State	ST	0 – Disabled 1 – Enabled
Username	U	1 to 50 characters
Email	E	Email Format
Phone	P	Phone Number Format
Function	F	1 to 50 characters

Groups	G	Supervisor
		User
		Viewer
		Contractor
Authentication	SYSL	1 – LOCAL
Password	PWD	Password

B.16 BINARY LABELS

TYPE: BL

Description	ID	Value
UUID	UUID	Binary Label UUID
One Label	OL	1 to 25 characters
Zero Label	ZL	1 to 25 characters
Description	DES	0 to 250 characters

Multitel

B.17 ASSET TYPES

TYPE: AT

Description	ID	Value
UUID	UUID	Asset Type UUID
Asset Type Name	ATN	1 to 50 characters
Parent Asset Type	PAT	Asset Type UUID (Optional)
Unavailable for Asset Creation	NAAC	0 – Disabled (Default)
		1 – Enabled
Note	N	0 to 250 characters

B.18 DATA POINTS OF ASSET TYPES

TYPE: DPT

Description	ID	Value
UUID	UUID	Data Point UUID
Data Point Type	DPT	1 - Analog
		2 - Binary
		3 - Text
Data Point Name	DPN	1 to 50 characters
Asset Type	PAT	Asset Type UUID
DPT = 1		
Unit	U	Unit UUID
DPT = 2		
Binary Label	BL	Binary Label UUID
Computed	COMPUTED	0 - No
		1 - Yes
COMP = 1		
Script	CODE	Lua Script

B.19 TEMPLATES

Multitel

TYPE: TEMP

Description	ID	Value
UUID	UUID	Template UUID
Template Name	TN	1 to 50 characters
Manufacturer	MAN	1 to 50 characters
Asset Type	AT	Asset Type UUID
Communication Protocol	CP	1 – Modbus TCP/IP – Client 2 – SNMP Get 3 – Modbus RTU - Master
CP = 1		
Gateway Mode	GM	0 – Standard 1 – Transparent
Asset Slave ID	SID	1 to 247
Asset IP Address	IP	0.0.0.0 to 255.255.255.255
Port Number	PN	1 to 65535 502 – Modbus TCP/IP (Default)
Silent	SIL	0 to 100
CP = 1 & GM = 0		
Register Order	RO	1 – Big-endian 2 – Little-endian
Register Base Address	RBA	0 – Use given address 1 – Substract 1 from given address
CP = 1 & GM = 1		
IO Slave ID	IOSID	1 to 247
CP = 2		
Asset IP Address	IP	0.0.0.0 to 255.255.255.255
SNMP Version	V	1 – SNMP V1 (Default) 2 – SNMP V2C 3 – SNMP V3
Constant Part Of OID	OID	

SNMP Device Community Name	CN	1 to 32 characters
Port Number	PN	1 to 65535 161 – SNMP Get (Default)
CP = 2 & V = 3		
Username	UN	1 to 50 characters
Default Context Name	DCN	1 to 50 characters
Security Level	SL	1 – No Authentication, No Privacy 2 – Authentication, No Privacy 3 – Authentication, Privacy
Authentication Protocol	AP	1 – MD5 (Default) 2 – SHA
Authentication Password	APWD	8 to 50 characters
Privacy Protocol	PP	1 – DES 2 - AES
Privacy Password	PPWD	8 to 50 characters
CP = 3		
Serial Port	SP	1 – RS-485 - COM A 2 – RS-485 - COM B
Asset Slave ID	SID	1 to 247
Register Order	RO	1 – Big-endian 2 – Little-endian
Register Base Address	RBA	0 – Use given address 1 – Substract 1 from given address
Asset Polling Rate	PR	1000 – 1s 5000 – 5s 15000 – 15s 30000 – 30s 60000 – 1m

		300000 – 5m
		900000 – 15m
		1800000 – 30m
		3600000 – 60m
		14400000 – 4h
		43200000 – 12h
		86400000 – 24h
Asset Timeout	TO	100 – 0.1s
		250 – 0.25s
		500 – 0.5s
		750 – 0.75s
		1000 – 1s
		2000 – 2s
		3000 – 3s
		4000 – 4s
		5000 – 5s
Number of Retry	NOR	1 to 10
Timeout After Retry	TAR	300 – 5m
		900 – 15m
		1800 – 30m
		3600 – 60m
		14400 – 4h
		43200 – 12h
		86400 – 24h
Total Iteration Number	TIN	1 to 10

B.20 DATA POINTS OF TEMPLATES

TYPE: DP

Description	ID	Value
UUID	UUID	Data Point UUID

Parent Data Point	DP	Data Point UUID of Asset Type
Template	TEMP	Template UUID
Data Point Type	DPT	1 - Analog
		2 - Binary
		3 - Text
Description	DES	1 to 50 characters
Polling Rate	PR	1000 – 1s
		15 000 – 15s
		30 000 – 30s
		60 000 – 1m
		300 000 – 5m
		900 000 – 15m
		1 800 000 – 30m
		3 600 000 – 60m
		14 400 000 – 4h
		43 200 000 – 12h
		86 400 000 – 24h
Number of Retry	NOR	1 to 10
Timeout After Retry	TAR	300 – 5m
		900 – 15m
		1800 – 30m
		3600 – 60m
		14400 – 4h
		43200 – 12h
		86400 – 24h
Total Iteration Number	TIN	1 to 10
DPT = 1		
Factor	F	Numeric with decimal (Default: 1)
Offset	O	Numeric with decimal (Default: 0)
Decimal	D	0 to 4 (Default: 0)
DPT = 2		

Mask Type	MSK_ST	1 – none 2 – bit 3 – range
Mask	MSK	1 to 100 (Default: 1)
Mask Value	MSK_V	1 to 100 (Default: 1)
DPT = 3		
Display String	DS	0 – No (Default) 1 – Yes
CP = 1 ou CP = 3		
Modbus Register Address	RA	1 to 65535 (Must be unique)
Register Type	RT	1 – Discrete Input 2 – Coil 3 – Holding Register 4 – Input Register
Data Type	DT	1 – 16 bit integer 2 – 32 bit integer 3 – 32 bit float 4 – 1 bit
CP = 2		
SNMP OID	OID	OID
Syntax Type	SYNT	2 – Int String 3 – Integer 4 – Bit String
Data Type	DPTS	1 – 16 bit 2 – 32 bit 4 – 64 bit
IO Modbus Register	IOMBR	1 to 65535 (Optional)
Register Type	RT	0 – None 1 – Discrete Input 2 – Coil

		3 – Holding Register
		4 – Input Register
Register Data Type	DT	0 – None
		1 – 16 bit integer
		2 – 32 bit integer
		3 – 32 bit float

B.21 SITES

TYPE: INVSITE

Description	ID	Value
UUID	UUID	Site UUID
Site Name	N	1 to 50 characters
CLLI	CLLI	1 to 50 characters
Language	SLID	1 - English
		2 - French
Supervisor	SUPID	User ID
Address	ADD	1 to 100 characters
City	C	1 to 50 characters
Zip/Postal Code	Z	Valid Zip or Postal Code
Country	SCID	1 - Canada
		2 - United States
State/Province	SPID	1 - Alberta
		2 - British Columbia
		3 - Manitoba
		4 - New Brunswick
		5 - Newfoundland and Labrador
		6 - North West Territories
		7 - Nova Scotia
		8 - Nunavut
		9 - Ontario
		10 - Prince Edward Island

Multitel

		11 - Quebec 12 - Saskatchewan 13 - Yukon 14 - Alabama (AL) 15 - Alaska (AK) 16 - Arizona (AZ) 17 - Arkansas (AR) 18 - California (CA) 19 - Colorado (CO) 20 - Connecticut (CT) 21 - Delaware (DE) 22 - District of Columbia (DC) 23 - Florida (FL) 24 - Georgia (GA) 25 - Hawaii (HI) 26 - Idaho (ID) 27 - Illinois (IL) 28 - Indiana (IN) 29 - Iowa (IA) 30 - Kansas (KS) 31 - Kentucky (KY) 32 - Louisiana (LA) 33 - Maine (ME) 34 - Maryland (MD) 35 - Massachusetts (MA) 36 - Michigan (MI) 37 - Minnesota (MN) 38 - Mississippi (MS) 39 - Missouri (MO) 40 - Montana (MT) 41 - Nebraska (NE) 42 - Nevada (NV) 43 - New Hampshire (NH)

		44 - New Jersey (NJ) 45 - New Mexico (NM) 46 - New York (NY) 47 - North Carolina (NC) 48 - North Dakota (ND) 49 - Ohio (OH) 50 - Oklahoma (OK) 51 - Oregon (OR) 52 - Other (NA) 53 - Pennsylvania (PA) 54 - Rhode Island (RI) 55 - South Carolina (SC) 56 - South Dakota (SD) 57 - Tennessee (TN) 58 - Texas (TX) 59 - Utah (UT) 60 - Vermont (VT) 61 - Virginia (VA) 62 - Washington (WA) 63 - West Virginia (WV) 64 - Wisconsin (WI) 65 - Wyoming (WY)
Latitude	LAT	Decimal between -90 to 90
Longitude	LONG	Decimal between -180 to 180
NPA	SNID	NPA ID

B.22 ASSETS

TYPE: EQU

Description	ID	Value
State	ST	0 – Disabled 1 – Enabled (Default)

Asset Name	EN	1 to 50 characters
Site	SITE	Site UUID
Template	MN	Template Name
Smart Asset	ET	1 – Yes (Default)
Communication Protocol	CP	1 – Modbus TCP/IP – Client 2 – SNMP Get 3 – Modbus RTU - Master
Mnemonic	MNE	Sx ou Mx - Auto Generate
CP = 1		
Gateway Mode	GM	0 – Standard 1 – Transparent
Asset Slave ID	SID	1 to 247
Asset IP Address	DA	0.0.0.0 to 255.255.255.255
Port Number	PN	1 to 65535 502 – Modbus TCP/IP (Default)
Silent	SIL	0 to 100
CP = 1 & GM = 0		
Register Order	RO	1 – Big-endian 2 – Little-endian
Register Base Address	RBA	0 – Use given address 1 – Substract 1 from given address
CP = 1 & GM =1		
IO Slave ID	IOSID	1 to 247
CP = 2		
Asset IP Address	DA	0.0.0.0 to 255.255.255.255
SNMP Version	V	1 – SNMP V1 (Default) 2 – SNMP V2C 3 – SNMP V3
Constant Part Of OID	OID	
SNMP Device Community Name	CN	1 to 32 characters

Port Number	PN	1 to 65535 161 – SNMP Get (Default)
CP = 2 & V = 3		
Username	UN	1 to 50 characters
Default Context Name	DCN	1 to 50 characters
Security Level	SL	1 – No Authentication, No Privacy 2 – Authentication, No Privacy 3 – Authentication, Privacy
Authentication Protocol	AP	1 – MD5 (Default) 2 – SHA
Authentication Password	APWD	8 to 50 alphanumeric characters
Privacy Protocol	PP	1 – DES 2 - AES
Privacy Password	PPWD	8 to 50 alphanumeric characters
CP = 3		
Serial Port	PP	1 – RS-485 - COM A 2 – RS-485 - COM B
Asset Slave ID	SID	1 to 247
Register Order	RO	1 – Lower address 2 – Higher address
Register Base Address	RBA	1 – Use given address 2 – Substract 1 from given address
Asset Polling Rate	DPR	1000 – 1 sec 5000 – 5 sec 15000 – 15 sec 30000 – 30 sec 60000 – 1 min 300000 – 5 min 900000 – 15 min

		1800000 – 30 min
		3600000 – 60 min
		14400000 – 4 hrs
		43200000 – 12 hrs
		86400000 – 24 hrs
Asset Timeout	TO	100 – 0.1 sec
		250 – 0.25 sec
		500 – 0.5 sec
		750 – 0.75 sec
		1000 – 1 sec
		2000 – 2 sec
		3000 – 3 sec
		4000 – 4 sec
		5000 – 5 sec
Number of Retry	NOR	1 to 10
Timeout After Retry	TAR	300 – 5 min
		900 – 15 min
		1800 – 30 min
		3600 – 60 min
		14400 – 4 hrs
		43200 – 12 hrs
		86400 – 24 hrs
Total Iteration Number	TIN	1 to 10
Multi-Read	MR	0 – Disabled (Default)
		1 – Enabled

B.23 DATA POINTS OF ASSETS

TYPE: DP

Description	ID	Value
State	ST	0 – Disabled

		1 – Enabled
Asset	EN	Asset Name
Data Point Type	DPT	1 – Analog
		2 – Binary
		3 – Text
Mnemonic	MNE	Auto Generate
Data Point Description	DES	1 to 50 characters
Parent Data Point	DPTEMP	Data Point UUID of Template
DPT = 1		
Unit	U	Unit UUID
Decimal	D	0 to 4 (0 = Default)
Factor	F	Numeric with Decimal (Default = 1)
Offset	O	Numeric with Decimal (Default = 0)
DPT = 2		
Binary Label	BL	Label UUID
Mask Type	MSK_ST	1 - none
		2 - bit
		3 - range
Mask	MSK	1 to 1000 (Default = 1)
Mask Value	MSK_V	0 to 1000 (Default = 0)
DPT = 3		
Display String	DS	0 - No
		1 - Yes
CP = 1 ou CP = 3		
Modbus Register Address	RA	1 to 65535
Register Type	RT	1 – Discrete Input
		2 – Coil
		3 – Holding Register
		4 – Input Register
Data Type	DT	1 – 16 bit integer
		2 – 32 bit integer

		3 – 32 bit float
		4 – 1 bit
CP = 2		
SNMP OID	OID	OID
Syntax Type	SYNT	2 – Int String
		3 – Integer
		4 – Bit String
Data Type	DPTS	1 – 16 bit
		2 – 32 bit
		4 – 64 bit
IO Modbus Register	IOMBR	1 to 65535 (Must be unique) (Optional)
Register Type	IORF	0 – None
		1 – Discrete Input
		2 – Coil
		3 – Holding Register
		4 – Input Register
Register Data Type	IORDT	1 – 16 Bits Integer
		2 – 32 Bits Integer
		3 – 32 Bits Floating Point
Polling Rate	PR	1000 – 1s
		5000 – 5s
		15000 – 15s
		30000 – 30s
		60000 – 1m
		300000 – 5m
		900000 – 15m
		1800000 – 30m
		3600000 – 60m
		14400000 – 4h
		43200000 – 12h

		86400000 – 24h
Number of Retry	NOR	1 to 10
Timeout After Retry	TAR	300 – 5m
		900 – 15m
		1800 – 30m
		3600 – 60m
		14400 – 4h
		43200 – 12h
		86400 – 24h
Total Iteration Number	TIN	1 to 10
Computed	Computed	0 - Disabled
		1 - Enabled
Script	Code	Lua Script
STM32 Data Point		
Front-End	FE	0 – Shunt (+/-50mVdc)
		1 – Temp
		2 – 65Vdc
		3 – 23Vms
		4 – 10Vdc
		5 – 1.4Vms
Scaling	SC	Decimal value
Delay Activation	DA	0 to 999
Delay Deactivation	DDA	0 to 999
Voltage Level	VL	0 to 70
Operating Mode	OM	0 – Not Latched
Activation Level	AL	0 – Ground
		1 – Battery
Mode	-	-
Triggering Source	-	-

B.24 PASSTHROUGHS

TYPE: PT

Multitel

Description	ID	Value
Mnemonic	MNE	Pxx – Auto Generate
State	ST	0 – Disabled (Default)
		1 – Enabled
Description	DES	1 to 50 characters
Protocol	P	1 – SNMP
		8 – HTTP
		9 – HTTPS
		10 – Telnet
		11 – SSH
		17 – FTP
		19 – SFTP
		20 – SCP
		22 – Email
		23 – Email-TLS
		24 – Email-SSL
Source Port	SC	1 to 65535
Destination IP	IP	0.0.0.0 to 255.255.255.255
Destination Port	DP	1 to 65535
Additional Port	AP	1 to 65535 (Optional)
Transport Protocol	TP	1 – TCP (Default)
		2 – UDP
		3 – Both
Special Mode	SM	0 – None (Default)
		1 – PBT WS 8081
		2 – PBT WS 80
		10 – HTTPS Proxy
Action	I_O	0 – None (Default)
		1 – IN
		2 – Passthrough

Multitel

B.25 OUTBOUND RULES

TYPE: OR

Description	ID	Value
Mnemonic	MNE	ORxx – Auto Generate
State	ST	0 – Disabled (Default)
		1 – Enabled
Description	DES	1 to 50 characters
Protocol	P	1 – SNMP
		8 – HTTP
		9 – HTTPS
		10 – Telnet
		11 – SSH
		17 – FTP
		19 – SFTP
		20 – SCP
		22 – Email
		23 – Email-TLS
		24 – Email-SSL
		30 – DNS
		31 – NTP
Source Port	SC	1 to 65535
Transport Protocol	TP	1 – TCP (Default)
		2 – UDP
		3 – Both

B.26 TRAP FORWARDING – SOURCES

TYPE: TFS

Description	ID	Value
ID	TSID	Trap Forwarding Source ID
Status	ST	0 – Disabled

		1 – Enabled (Default)
Asset Name	AN	1 to 50 characters
IP Address	IP	0.0.0.0 to 255.255.255.255

B.27 TRAP FORWARDING – DESTINATIONS

TYPE: TFD

Description	ID	Value
ID	TDID	Trap Forwarding Destination ID
Status	ST	0 – Disabled 1 – Enabled (Default)
Destination Name	DN	1 to 50 characters
Destination IP Address / Domain Name	IP	IP Address (0.0.0.0 to 255.255.255.255) or Domain Name (1 to 255 characters)
Port	P	1 to 65535
Community Name	CN	1 to 50 characters
SNMP Version	V	2 – v2c (Default) 3 – v3
Notification Type	NT	1 – Trap - Unacknowledged (Default) 2 – Inform - Acknowledged
NT = 2		
Notification Timeout	T	1000 – 1 sec 5000 – 5 sec 30000 – 30 sec 60000 – 1 min
Notification Retries	R	1 to 5
Keep Alive Trap Delay	KA	0 – None 60 – 1 min 900 – 15 min 1 800 – 30 min 3 600 – 60 min

V = 3		
Username	UN	1 to 50 characters
Context Name	CTN	0 to 50 characters
Security Level	SL	1 – No authentication, No privacy (Default) 2 – Authentication, No privacy 3 – Authentication, Privacy
Authentication Protocol	AP	1 – MD5 (Default) 2 – SHA
Authentication Password	APWD	8 to 50 characters (Scripted)
Privacy Protocol	PP	1 – DES (Default) 2 – AES
Privacy Password	PPWD	8 to 50 characters (Scripted)

B.28 TRAP FORWARDING – SOURCE TO DESTINATION

TYPE: TFS2TFD

Description	ID	Value
Trap Forwarding Source	TSID	Trap Forwarding Source ID
Trap Forwarding Destination	TDID	Trap Forwarding Destination ID

B.29 NOTIFICATIONS - STATUS

TYPE: NOTIFICATION_STATUS

Description	ID	Value
UUID	UUID	Status UUID
Label	LABEL	1 to 50 characters
Color	COLOR	Color Code
Position	POSITION	1 to 1000

B.30 NOTIFICATIONS - CONFIGURATIONS

TYPE: NOTIFICATION_CONFIG

Description	ID	Value
UUID	UUID	Configuration UUID
State	ENBL	0 – Disabled (Default) 1 – Enabled
Name	NAME	1 to 50 characters
Data Point To Monitor	MNE	Data Point Mnemonic
Alarm Activation Trigger Condition	AACOND	BINARY_ZERO_TO_ONE – From Off To On (0 To 1) (Default) BINARY_ONE_TO_ZERO – From On To Off (1 To 0)
Alarm Status When Active	STUUID	Status UUID
Notification Sending Trigger	NSTRG	LOG_ONLY – No Notifications – Log Only (Default) ON_ALARM_ACTIVATION – Notification When The Alarm Become Active ON_BOTH_ALARM_ACTIVATION_ AND_DEACTIVATION – Notification When The Alarm Become Active And When It Comes Back To Normal
Destinations	TFDID	Trap Forwarding Destination ID List

Should include our standard support information (how to contact Multitel).