Multitel

IO Platform

GUIDE UTILISATEUR

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

Multitel

TABLE OF CONTENTS

Multitel

Multitel

TABLES

Multitel

FIGURES

Multitel

Multitel

1.PREMIÈRE CONNECTION

1.1 CONNECTION ETHERNET

L'interface du dispositif iO Platform est accessible via un navigateur web. Le dispositif peut être connecté via le port Ethernet ETH-1 ou ETH-2. Cependant, pour la connexion initiale, vous devez utiliser le port ETH-2, car ETH-1 ne dispose pas d'une adresse IP statique et dépend du DHCP. Le tableau ci-dessous montre les paramètres d'usine pour les deux ports Ethernet.

Tableau 1: Paramètres d'usine pour les ports Ethernet

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

Un réseau local (LAN) doit être établi entre le port Ethernet frontal du dispositif iO et le PC de l'utilisateur.

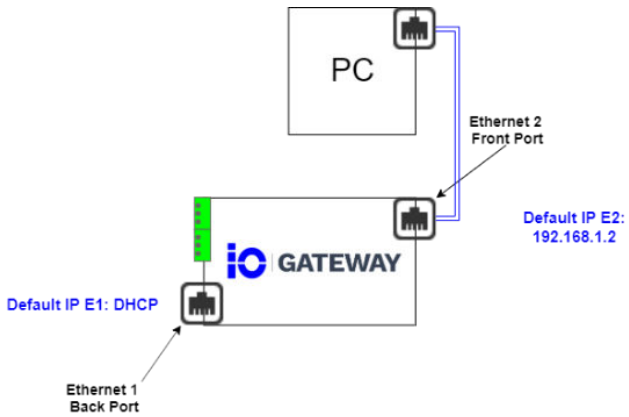


Figure 1: Première Connection

Pour créer un réseau LAN entre un PC et le dispositif iO, l'utilisateur doit modifier les paramètres de l'adaptateur Ethernet. Sur un ordinateur Windows, procéder comme suit :

- Ouvrir le Panneau de configuration.
- Sélectionner Centre Réseau et partage, puis Modifier les paramètres de l'adaptateur.
- Faire un clic droit sur l'adaptateur Ethernet souhaité et sélectionner Propriétés.
- Sélectionner Protocole Internet version 4 (TCP/IPv4).
- Cliquer sur Propriétés.
- Définir l'adresse IP et le masque de sous-réseau (par exemple, 192.168.1.100 et 255.255.255.0).

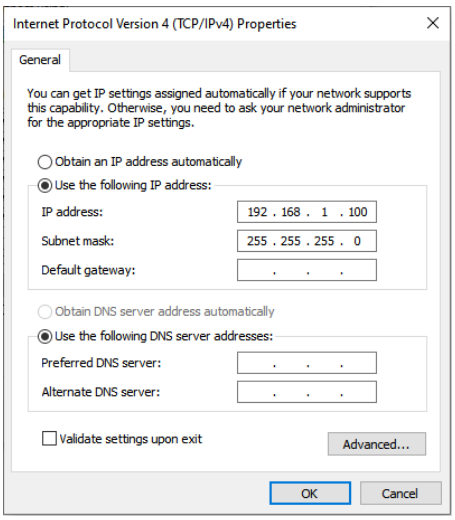


Figure 2: Modifier les propriétés IPv4 sur un PC

Une fois le réseau LAN configuré, l'utilisateur doit saisir l'adresse IP par défaut (192.168.1.2) dans la barre d'adresse du navigateur Web.

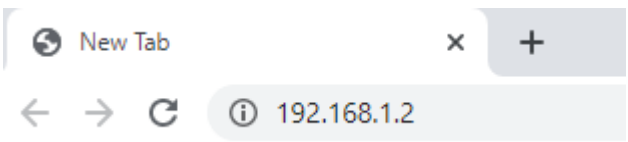


Figure 3: Adresse IP dans le navigateur Web

Veuillez noter que le dispositif iO Platform utilise un serveur Web moderne qui ne prend pas en charge les anciens navigateurs Web. Le tableau ci-dessous répertorie les navigateurs Web pris en charge par le dispositif iO.

Tableau 2: Navigateurs Web pris en charge

Navigateur Web	Version minimale recommandée
Google Chrome	132.0
Mozilla Firefox	121.0
Microsoft Edge	132.0

1.2 PREMIÈRE OUVERTURE DE SESSION

Une fois l'adresse IP par défaut saisie dans la barre d'adresse et le réseau LAN correctement configuré, l'utilisateur sera dirigé vers la page de connexion de la plateforme iO.

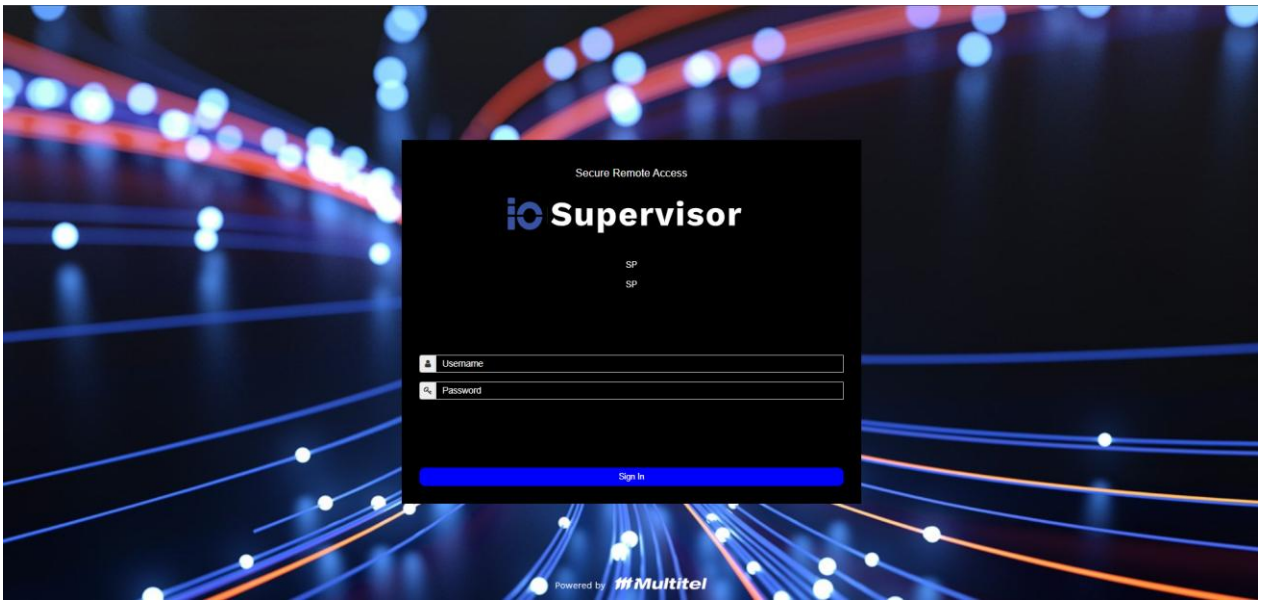


Figure 4: Première ouverture de session

Les identifiants par défaut d'usine sont les suivants :

Tableau 3: Identifiants par défaut

Navigateur web	Utilisateur	Mot de passe
Administrator	administrator	admin
User	user	user
Viewer	viewer	viewer

1.3 CONNEXIONS INITIALES

1.3.1 CONNEXION ETHERNET

1.3.1.1 Configuration de la connexion WAN sur le dispositif iO

Pour activer l'accès à distance à l'interface Web de la plateforme iO, la connexion WAN doit être configurée sur le port Ethernet ETH-1. Ce port est situé à l'arrière du dispositif et n'est pas configuré par défaut. Les modifications de configuration du port arrière ETH-1 peuvent être effectuées directement à partir du PC de l'utilisateur.

⚠ **Note:** Vous devez obtenir une adresse IP statique valide, un masque de sous-réseau et une passerelle auprès de votre administrateur informatique avant de poursuivre.

Suivre les étapes ci-dessous pour configurer la connexion :

- Cliquer sur Settings.
- Cliquer sur Connections.
- Sélectionner l'onglet ETH-1 – 1 Gbps.
- Laisser la valeur MTU à 1500, sauf indication contraire de votre administrateur réseau.
- Laisser le paramètre Speed sur Auto, sauf indication contraire.
- Changer le Mode de DHCP à Static.
- Saisir les valeurs pour IPv4 Address, IPv4 Subnet Mask et IPv4 Gateway.
- Cliquer sur Save.
- Redémarrer le dispositif.

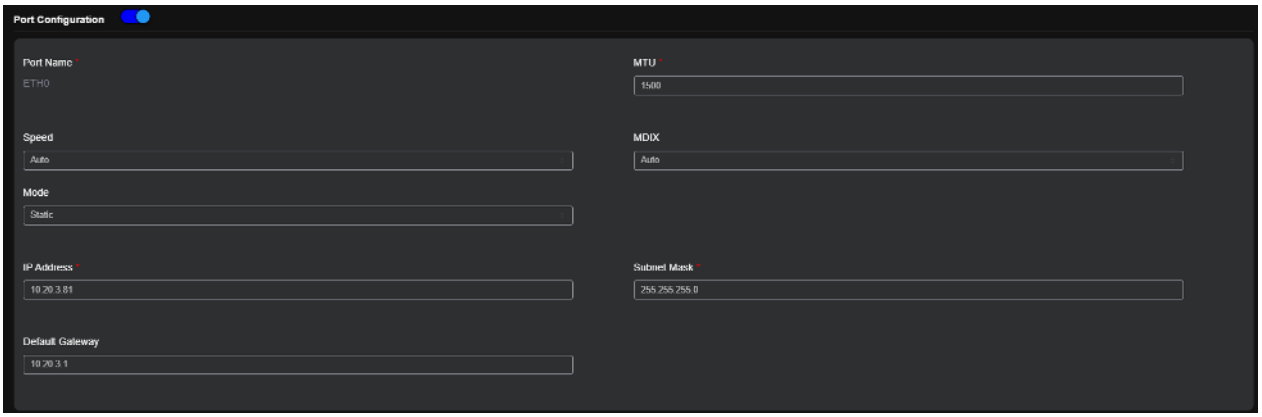


Figure 5: ETH-1 – Configuration 1 Gbps

1.3.1.2 Configuration du dispositive iO et de l'actif LAN

Pour connecter le dispositif iO à d'autres équipements, un nouveau réseau local (LAN) doit être configuré. Le dispositif iO utilise ce LAN pour communiquer avec l'équipement connecté et le surveiller.

Si le dispositif iO est destiné à surveiller un seul équipement, l'utilisateur peut établir une connexion LAN directe entre le dispositif iO et cet équipement. Cependant, dans la plupart des cas, le dispositif iO sera utilisé pour surveiller plusieurs équipements simultanément. Dans ces scénarios, un ou plusieurs commutateurs Ethernet non gérés sont nécessaires pour créer le réseau requis.

Lors de la connexion de plusieurs équipements, s'assurer que chaque équipement se voit attribuer une adresse IP unique et que tous les équipements sont configurés pour fonctionner dans le même sous-réseau.

Dans cet exemple, quatre équipements doivent être surveillés. Un commutateur Ethernet non géré à 5 ports est utilisé pour créer le LAN entre les équipements et le dispositif de la plateforme iO. Les adresses IP des équipements sont configurées sur le réseau 10.10.10.X.

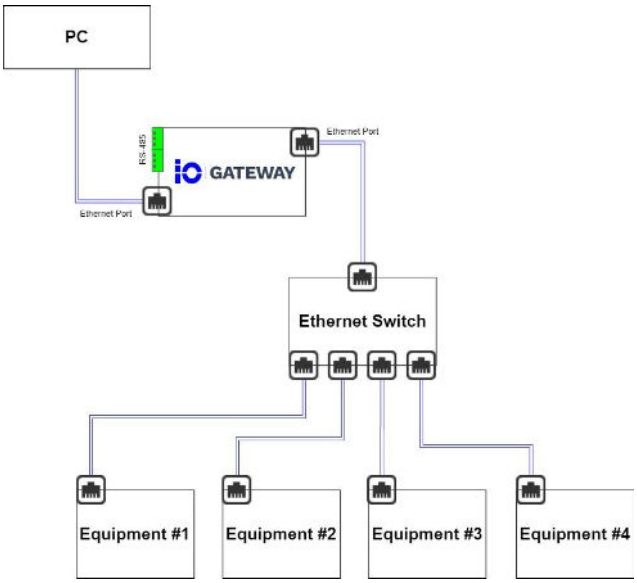


Figure 6: Configuration LAN

Un câble Ethernet doit être utilisé pour connecter le port Ethernet arrière du dispositif iO au unmanaged switch, complétant ainsi la configuration du LAN.

Suivre les étapes ci-dessous pour configurer la connexion :

- Ouvrir l'interface Web de la plateforme iO.
- Cliquer sur Settings.
- Cliquer sur Connections.
- Sélectionner ETH-2 – 100 Mbps.
- Activer le port.
- Laisser la valeur MTU à 1500, sauf indication contraire de votre administrateur réseau.
- Laisser le paramètre de vitesse sur Auto, sauf indication contraire.
- Cliquer sur Mode et le changer de DHCP à Static.
- Saisir les informations réseau suivantes :
    - IPv4 Address
    - IPv4 Subnet Mask
    - IPv4 Gateway.

⚠ **Note:** S'assurer que tous les équipements à connecter au dispositif iO sont configurés dans le même sous-réseau IP.

- Cliquer sur Save.
- Redémarrer le dispositif de la plateforme iO (un bouton Reboot apparaîtra dans l'en-tête supérieur).

2.CONFIGURATION IO

2.1 UTILISATEURS ET NIVEAUX D'ACCÈS

Les comptes utilisateurs et les niveaux d'accès peuvent être consultés et configurés dans la section Security du module Settings.

Le dispositif iO prend en charge deux types d'authentifications :

- **LOCAL** : L'authentification locale permet la création d'utilisateurs et l'attribution de niveaux d'accès directement aux paramètres de sécurité dans le dispositif.
- **LDAP** : Le protocole d'authentification LDAP est utilisé pour authentifier les utilisateurs via l'annuaire LDAP du client. Pour les utilisateurs LDAP, toutes les actions de gestion de compte, à l'exception de la suppression, doivent être effectuées directement dans le système LDAP du client.
- **RADIUS** : Le protocole d'authentification LDAP est utilisé pour authentifier les utilisateurs via l'annuaire Radius du client. Pour les utilisateurs Radius, toutes les actions de gestion de compte, à l'exception de la suppression, doivent être effectuées directement dans le système Radius du client.

2.1.1 INFORMATION D'UTILISATEUR

2.1.1.1 Création d'utilisateur

Cette section explique comment créer de nouveaux comptes utilisateurs sur la plateforme iO. Selon le groupe attribué (par exemple Supervisor, User, Viewer), les utilisateurs disposeront de différents niveaux d'accès aux fonctionnalités de la plateforme. Une configuration correcte des utilisateurs garantit que seules les personnes autorisées peuvent accéder aux paramètres du système ou les modifier, ainsi qu'aux données surveillées.

Suivre les instructions pour créer des utilisateurs, attribuer des rôles et configurer les détails d'authentification de manière sécurisée et efficace.

- Cliquer sur Settings.
- Cliquer sur Security.
- Dans l'onglet Users, cliquer sur + User.
- Compléter les champs selon le tableau ci-dessous.

Multitel

Tableau 4: Information d'utilisateur

Champ	Description	Spécification	Obligatoire
Username	Le nom unique utilisé par l'utilisateur pour se connecter au dispositif.	Alphanumérique, 1-50 caractères	Oui
Email	L'adresse courriel de l'utilisateur.	Format courriel valide (ex. : user@example.com)	Non
Phone	Le numéro de téléphone de l'utilisateur.	Alphanumérique, 1-50 caractères	Non
Function	Le titre d'emploi ou rôle de l'utilisateur (ex. : Technicien, Gestionnaire).	Alphanumérique, 1-50 caractères	Non
Groups	Définit le niveau d'autorisation de l'utilisateur en l'assignant à un groupe. • Supervisor • User • Viewer • Contractor	Sélection unique (liste déroulante)	Oui
Authentication	Indique la méthode d'authentification utilisée par l'utilisateur (ex. : Local ou LDAP)	Généré par le système : Local / LDAP	Automatique
Password	Définit le mot de passe de l'utilisateur.	Le mot de passe doit comporter au moins huit caractères.	

2.1.1.2 *Réinitialisation du mot de passe*

Seuls les utilisateurs assignés au groupe Supervisor peuvent réinitialiser le mot de passe des utilisateurs locaux.

⚠️ Avertissement :
Si un utilisateur disposant d'un accès de niveau Supervisor réinitialise un mot de passe ou modifie le nom d'utilisateur d'un autre utilisateur, les identifiants mis à jour doivent être communiqués manuellement à l'utilisateur concerné. Le système n'envoie aucune notification automatique.

Les utilisateurs assignés aux groupes User ou Viewer peuvent uniquement réinitialiser leur propre mot de passe via l'interface User Profile.

Pour accéder au User Profile :

- Cliquer sur le logo iO dans la barre d'en-tête.
- Sélectionner User Profile.

2.1.1.3 *Statud de l'utilisateur: Activer ou Désactiver*

La désactivation d'un utilisateur supprime son accès à l'interface de la plateforme iO.

Multitel

Pour activer ou désactiver un utilisateur :

- Aller à la page Users.
- Basculer l'interrupteur dans la colonne State.
  - : L'utilisateur est activé
  - : L'utilisateur est désactivé

2.1.1.4 *Statut d'utilisateur: Supprimer un utilisateur*

Pour supprimer un utilisateur :

- Sélectionner l'utilisateur à supprimer.
- Cliquer sur Delete et confirmer l'action.

⚠ Note :
L'utilisateur par défaut Administrator ne peut pas être supprimé ni désactivé.

⚠ Note :
Le délai d'inactivité est fixé à 30 minutes.

2.1.2 LDAP

La plateforme iO prend en charge l'authentification LDAP, permettant une gestion centralisée des accès utilisateurs via les services d'annuaire de votre organisation. Cette section décrit comment configurer les paramètres LDAP sur le dispositif.

Suivre les instructions de cette section pour configurer LDAP :
- Cliquer sur Settings.
- Cliquer sur Security.
- Cliquer sur l'onglet LDAP.
- Activer LDAP en basculant l'interrupteur Global Settings sur ON.

Tableau 5: Configuration LDAP

Champ	Description	Spécification	Obligatoire
Port	Port du serveur LDAP (ex. : 389 pour LDAP, 636 pour LDAPS)	Alphanumérique, 1-50 caractères	Oui
Timeout	Définir le délai d'expiration de la connexion	Liste déroulante : • 5 sec • 10 sec • 30 sec • 1 min	Oui
Login Pattern	Définir la requête de connexion LDAP	Alphanumérique, 1-128 caractères	Non
Secured Connection Type	Choisir entre LDAP et LDAPS	Liste déroulante : • None • LDAPS/SSL	Oui

Trusted Certificate Authority Key	Uniquement pour LDAPS		Oui
User Search Base DN	Le nom distinct de base pour commencer la recherche d'utilisateurs (ex. : ou=users,dc=example,dc=com)		Oui
Username Attribute	L'attribut LDAP utilisé pour la connexion (ex. : uid ou sAMAccountName pour Active Directory)		Oui
Login	Nom distinct (DN) du compte de service		Oui
Password	Mot de passe du compte de service		Oui
Host	Nom d'hôte ou adresse IP du serveur LDAP		Oui
Groups	DN du groupe distant (groupe LDAP)	e.g., cn=contractors, ou=groups, dc=example, dc=com	Oui
First Name	Attributs utilisateur LDAP	e.g., givenName	Non
Last Name	Attributs utilisateur LDAP	e.g., sn	Non
Email	Attributs utilisateur LDAP	e.g., mail	Non
Phone	Attributs utilisateur LDAP	e.g., telephoneNumber	Non

Une fois que tous les champs sont remplis :

- Cliquer sur Save pour appliquer la configuration.
- Vous pouvez aussi utiliser Cancel pour annuler les changements.

Comportement de connexion LDAP :

- Une fois LDAP activé et correctement configuré, les utilisateurs peuvent se connecter en utilisant leurs identifiants de domaine.
- Les droits d'accès sont automatiquement accordés en fonction des correspondances de groupes.
- La gestion des mots de passe est effectuée de manière externe via votre système LDAP.

2.1.3 APERÇU DE RADIUS

RADIUS *(Remote Authentication Dial-In User Service)* est un protocole réseau standardisé utilisé pour l'authentification, l'autorisation et la comptabilisation (AAA).

RADIUS permet une gestion centralisée des accès pour des infrastructures telles que :

- les réseaux Wi-Fi (WPA2/WPA3-Enterprise)
- les connexions VPN
- l'accès filaire (802.1X)
- les équipements réseau (routeurs, commutateurs, pare-feu)

Fonctionnement général :

- Authentification – Vérifie l'identité de l'utilisateur (nom d'utilisateur/mot de passe, certificat, jeton, etc.).
- Autorisation – Attribue les droits d'accès (VLAN, politiques, niveaux de privilèges).
- Comptabilisation (Accounting) – Enregistre les informations de session (durée, utilisation du trafic, statut).

Le protocole fonctionne généralement sur UDP (ports 1812 et 1813) et repose sur une clé secrète (*shared secret*) entre le client RADIUS (NAS – Network Access Server) et le serveur RADIUS afin de sécuriser les communications.

2.1.4 CONFIGURATION DE RADIUS

Pour configurer RADIUS :

- Aller dans *Settings*.
- Aller dans *Security*.
- Cliquer sur l'onglet *Radius*.
- Activer Radius en basculant le commutateur sur ON.

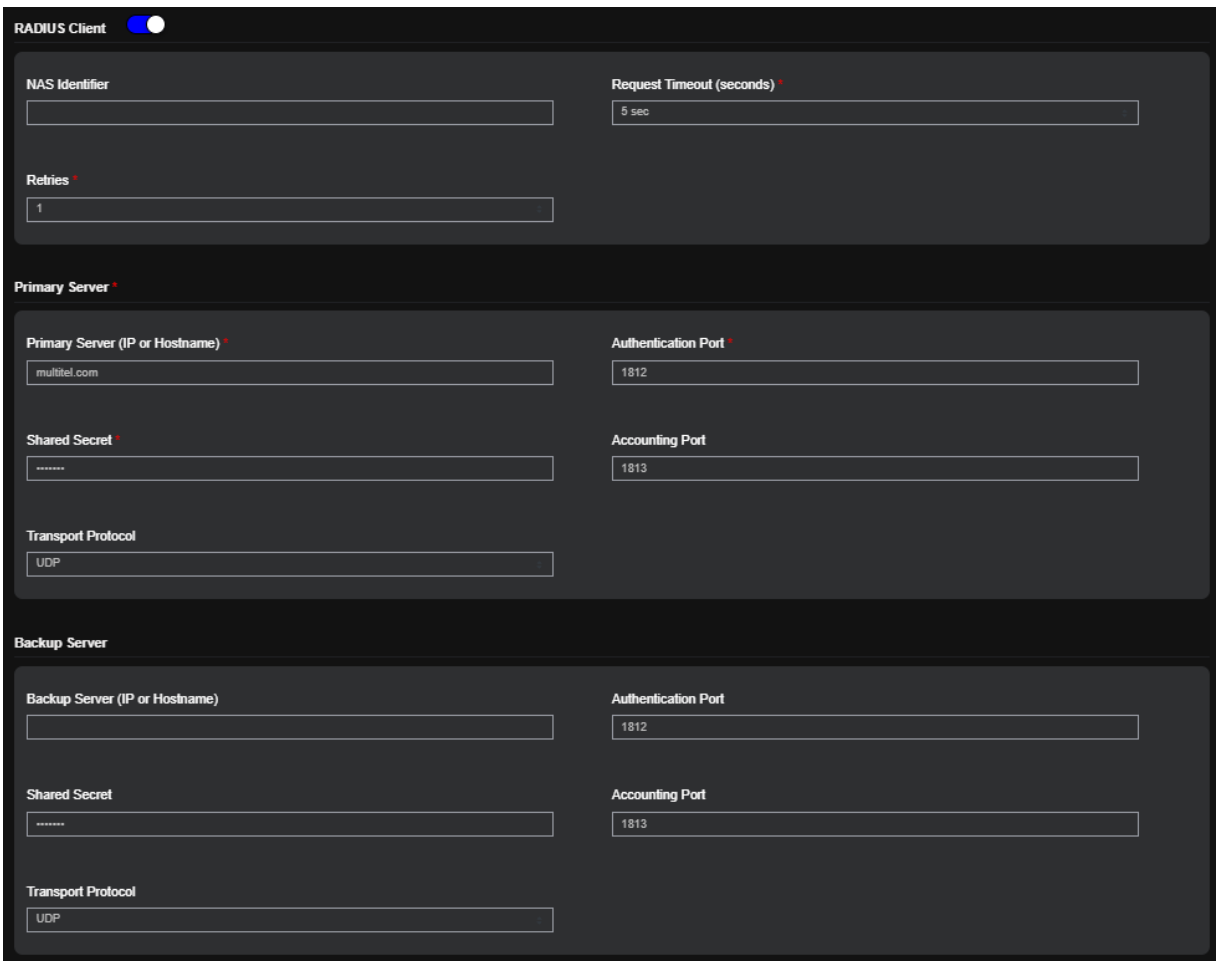


Figure 7: Radius – Configuration

Multitel

Tableau 6: Radius – Configuration

Field	Description	Specification	Required
RADIUS Client State	Permet d'activer ou désactiver un serveur RADIUS externe.	Commutateur	Oui
NAS Identifier	Identifiant unique du client RADIUS (Network Access Server). Cet identifiant est envoyé au serveur RADIUS dans les requêtes d'authentification et de comptabilisation.	1 à 50 caractères	Non
Request Timeout	Temps maximum (en secondes) pendant lequel le système attend une réponse du serveur RADIUS avant que la requête n'expire.	Liste déroulante : • 1 sec • 2 sec • 3 sec (défaut) • 4 sec • 5 sec	Oui
Retries	Nombre de tentatives effectuées si aucune réponse n'est reçue du serveur RADIUS.	Liste déroulante : • 1 • 2 (défaut) • 3 • 4 • 5	Oui
Primary Server (IP or Hostname)	Adresse IP ou nom d'hôte DNS du serveur RADIUS primaire.	0.0.0.0 à 255.255.255.255 ou nom d'hôte	Oui
Primary Authentication Port	Port UDP utilisé pour les requêtes d'authentification RADIUS.	1 à 65535 Défaut : 1812	Oui
Primary Shared Secret	Clé secrète partagée entre le client RADIUS et le serveur.	1 à 50 caractères chiffrés	Oui
Primary Accounting Port	Port UDP utilisé pour les messages de comptabilisation RADIUS (journalisation des sessions).	1 à 65535 Défaut : 1813	Non
Primary Transport Protocol	Protocole utilisé pour communiquer avec le serveur RADIUS.	Liste déroulante : • UDP (défaut)	Oui
Backup Server (IP or Hostname)	Adresse IP ou nom d'hôte DNS du serveur RADIUS secondaire.	0.0.0.0 à 255.255.255.255 ou nom d'hôte	Non
Backup Authentication Port	Port d'authentification du serveur secondaire.	1 to 65535 Défaut : 1812	Non
Backup Shared Secret	Clé secrète partagée avec le serveur secondaire.	1 à 50 caractères chiffrés	Non
Backup Accounting Port	Port de comptabilisation du serveur secondaire.	1 to 65535 Défaut : 1813	Non
Backup Transport Protocol	Protocole utilisé pour communiquer avec le serveur secondaire.	Liste déroulante : • UDP (défaut)	Oui

Pendant la configuration de RADIUS, les connexions des serveurs primaire et de secours peuvent être testées.

Pour tester les connexions des serveurs Radius :

- Saisir le *Username* d'un utilisateur RADIUS.
- Saisir le *Password* de l'utilisateur RADIUS.
- Cliquer sur le bouton *TEST PRIMARY SERVER CONNECTION*.
- Cliquer sur le bouton *TEST BACKUP SERVER CONNECTION* si le serveur secondaire est configuré.

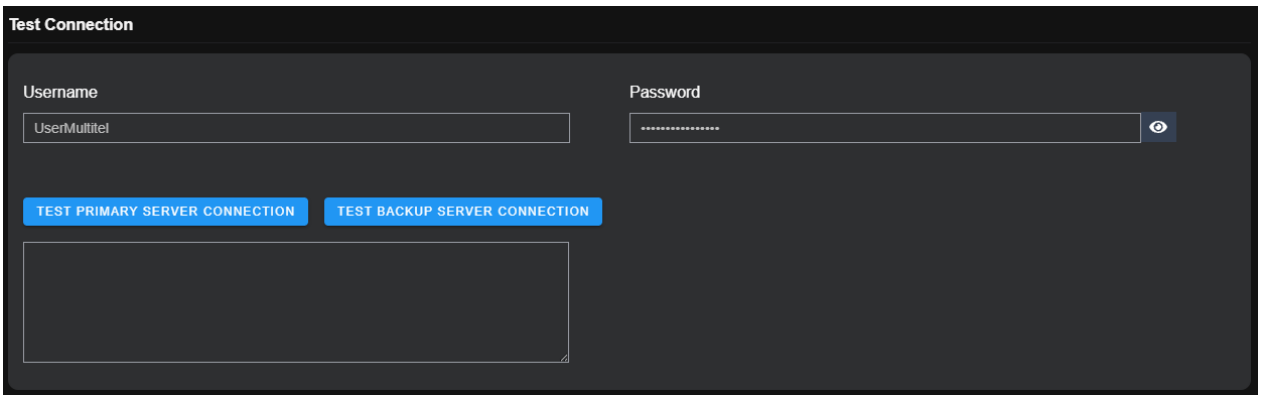


Figure 8: Radius – Tests de connexion

2.1.5 NIVEAU D'ACCÈS

Le tableau ci-dessous présente les permissions d'accès associées à chaque groupe d'utilisateurs pour diverses fonctionnalités de la plateforme iO. Chaque groupe (Supervisor, User, Viewer, Contractor) se voit accorder soit des droits complets de modification, soit un accès en lecture seule, selon son rôle et les fonctionnalités.

Tableau 7: Niveau d'accès

Functionalités	Groupe	Niveau de permission
Settings	Supervisor	Modifier
	User	Lecture seule
	Viewer	Aucun accès
	Contractor	Accès en lecture seule à : – General Parameters – Inventory – Units – Labels – Notifications
Asset	Supervisor	Modifier
	User	Modifier
	Viewer	Lecture seule
	Contractor	Lecture seule
HMI	Supervisor	Modifier
	User	Lecture seule

	Viewer	Lecture seule
	Contractor	Lecture seule
Alarms	Supervisor	Modifier
	User	Lecture seule
	Viewer	Lecture seule
	Contractor	Lecture seule
IO Channels	Supervisor	Modifier
	User	Lecture seule
	Viewer	Lecture seule
	Contractor	Lecture seule
Passthrough	Supervisor	Modifier
	User	Modifier
	Viewer	Lecture seule
	Contractor	Modifier
Trap Forwarding	Supervisor	Modifier
	User	Modifier
	Viewer	Lecture seule
	Contractor	Lecture seule

2.2 PARAMÈTRES GÉNÉRAUX

Les paramètres généraux constituent l'une des premières étapes requises lors de la configuration d'un dispositif iO. Située sous Settings, la section General Parameters est divisée en les sections suivantes :

- Site Information
- System Information
- Date and Time

2.2.1 INFORMATION SUR LE SITE

La section Informations sur le site permet aux utilisateurs de définir et de documenter les détails clés concernant l'emplacement physique où le dispositif iO est déployé. Cela inclut le nom du site, le code CLLI et l'adresse complète de l'emplacement (pays, province/État, ville, code postal et NPA). De plus, les utilisateurs peuvent téléverser une image du site pour une identification visuelle rapide.

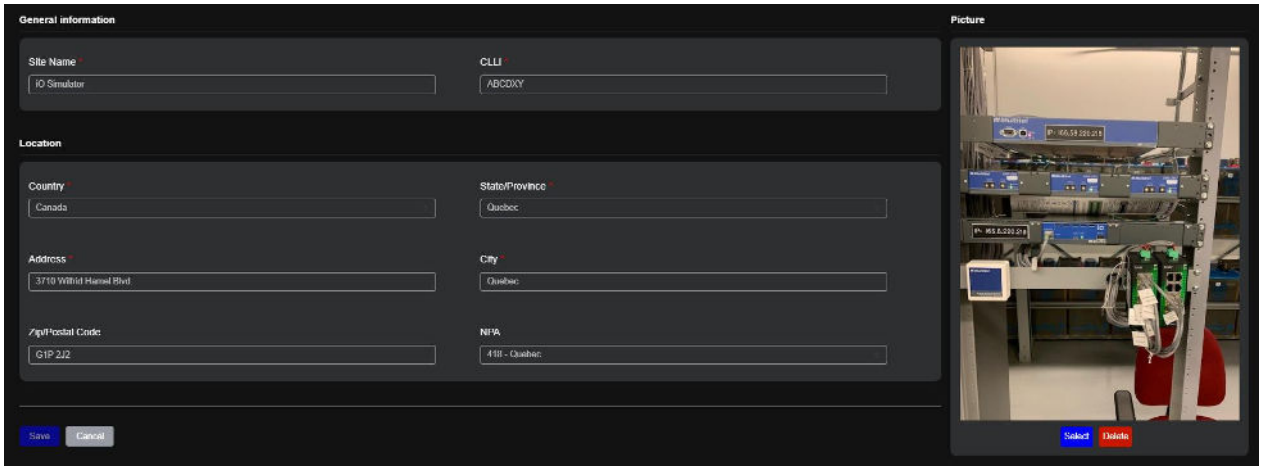


Figure 9: Information sur le site

2.2.1.1 *Information Générale*

Le nom du site configuré dans la section General Information est utilisé pour identifier l'emplacement physique du dispositif iO. Ce nom sera affiché dans l'en-tête de l'interface Web.

Figure 10: Nom du site dans l'en-tête

Le code CLLI peut également être configuré et apparaîtra sur la page de connexion, avec le nom du site.

Figure 11: Nom du site et CLLI dans la page de connexion

2.2.1.2 *Emplacement*

Tableau 8: Emplacement

Champ	Description	Spécification	Obligatoire
Country	Pays où se trouve l'iO	Liste déroulante : • Canada	Oui

		• United States	
State/Province	Liste des États ou province	Liste déroulante	Oui
Address	Adresse du site	Alphanumérique, 1-100 caractères	Oui
City	Ville du site	Alphanumérique, 1-50 caractères	Oui
Zip/Postal Code	Code postal/Zip du site	Format de code postal et Zip valide	Oui
NPA	NPA du site	Liste déroulante	Oui

2.2.2 INFORMATION DU SYSTÈME

2.2.2.1 Ressources du Système

L'information suivante est disponible dans la section System Information :

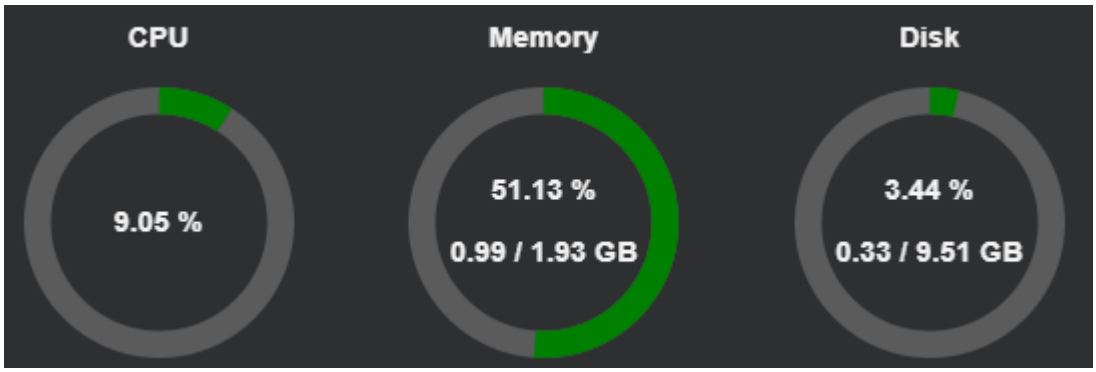


Figure 12: Ressources du système iO

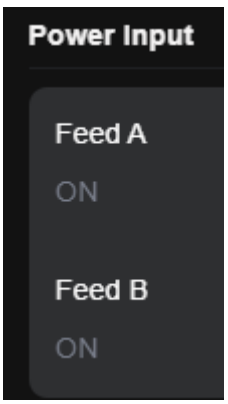


Figure 13: Entrées d'alimentation

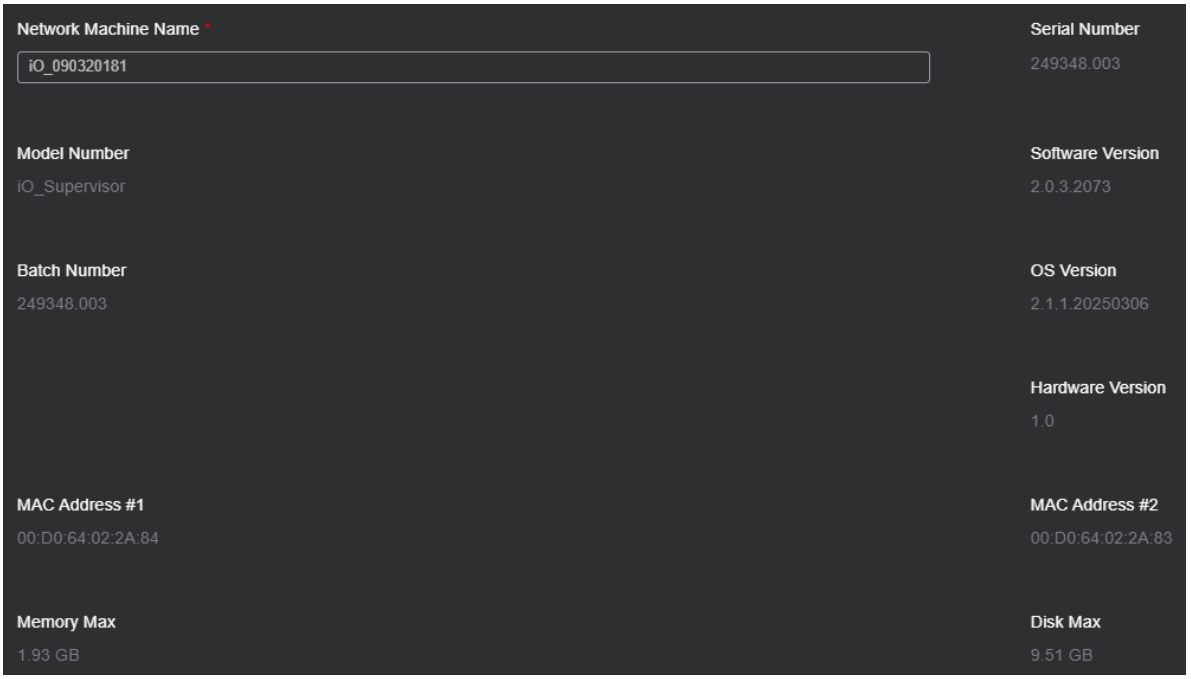


Figure 14: Section À propos

Tableau 9: Détails de la section À propos

Champ	Description
Network Machine Name	Une étiquette unique qui distingue le dispositif des autres présents sur le réseau.
Serial Number	Un identifiant unique attribué par l'équipe de fabrication de Multitel, utilisé pour suivre et identifier l'unité spécifique.
Model Number	Un identifiant indiquant la gamme de produits ou la variante de conception.
Software Version	Une étiquette qui indique la version de publication de la plateforme iO sur le dispositif.
Batch Number	Un identifiant attribué par l'équipe de fabrication de Multitel, utilisé pour suivre et identifier l'unité spécifique.
Hardware Version	Une étiquette qui indique la version matérielle du dispositif.
MAC Address #1	Un identifiant unique pour l'interface réseau ETH-1.
MAC Address #2	Un identifiant unique pour l'interface réseau ETH-2.
Memory Max	La quantité maximale de mémoire (RAM) que le dispositif peut prendre en charge.
Disk Max	La capacité de stockage maximale du dispositif.

2.2.3 DATE ET HEURE

La date et l'heure sont configurées dans la section General Information. La première partie affiche l'heure système actuelle (UTC), tandis que le fuseau horaire de l'unité peut également être configuré.

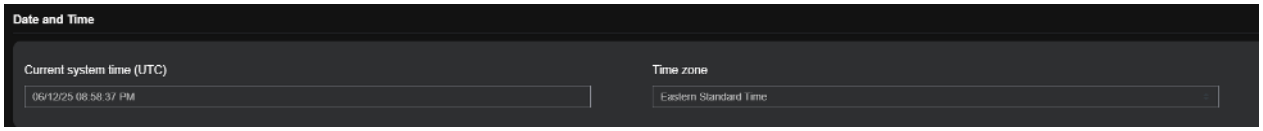


Figure 15: Date and Time

2.2.3.1 NTP

La section NTP est utilisée pour synchroniser automatiquement l'horloge de l'iO à l'aide du Network Time Protocol (NTP). Lorsqu'elle est activée, l'unité met périodiquement à jour son heure système en fonction des serveurs NTP configurés afin de maintenir des horodatages précis pour les journaux, les alarmes et l'historique des données.

Pour activer la synchronisation NTP :

- Aller à Settings
- Aller à General Information
- Dans la section Date and Time, activer Set automatically
- Configurer les serveurs NTP (recommandé : remplir les trois pour la redondance)

Champs du serveur NTP

- Primary NTP server
  o Source de temps principale utilisée par l'iO.

- Secondary NTP server

  o Source de temps de secours utilisée si le serveur primaire n'est pas joignable.

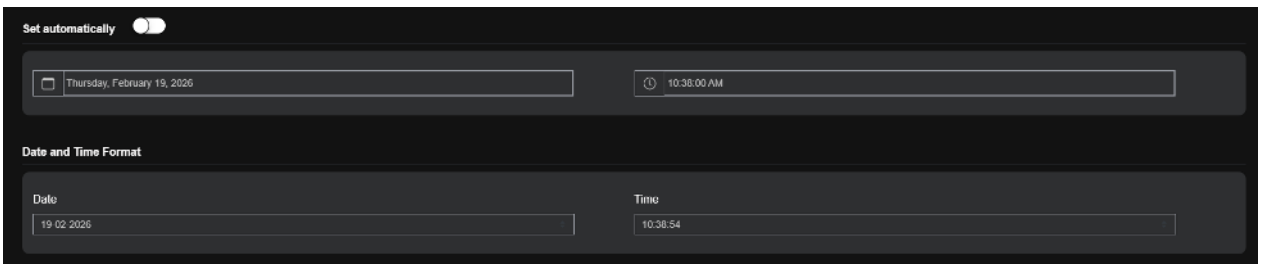
- Tertiary NTP server

  o Source de temps de secours supplémentaire utilisée si les serveurs primaire et secondaire ne sont pas joignables.

Comportement de basculement

Au démarrage, l'iO tente de se synchroniser en utilisant le serveur NTP primaire. Si le serveur primaire ne répond pas, le dispositif tente automatiquement le serveur secondaire, puis le serveur tertiaire.

2.2.3.2 Manuel



La section Manual est utilisée pour configurer la date et l'heure de l'iO sans utiliser NTP.
Pour configurer la date et l'heure manuellement :

• Aller à **Settings**
• Aller à **General Information**
• Dans la section **Date and Time**, désactiver **Set automatically**
• Configurer les valeurs ci-dessous :
  o **Date** : Sélectionner ou entrer la date à l'aide du sélecteur de calendrier
  o **Time** : Entrer l'heure à l'aide du champ horaire

Note : Lorsque Set automatically est désactivé, l'iO ne synchronise plus son horloge avec les serveurs NTP. L'heure manuelle doit être utilisée uniquement lorsque NTP n'est pas disponible ou lorsque le système nécessite une heure fixe pour des tests ou la mise en service. Une date/heure incorrecte peut affecter les journaux, les alarmes et les horodatages des données historiques.

2.2.3.3 Format de la date et l'heure

- Formats de date disponibles
  - MM/DD/YY
  - MM/DD/YYYY
  - DD/MM/YY
  - DD/MM/YYYY

- MM-DD-YY
- MM-DD-YYYY
- DD-MM-YY
- DD-MM-YYYY

- Formats d'heure disponibles
  - HH:MM:SS AM/PM
  - HH:MM:SS
  - HH:MM AM/PM

Note : Lorsque Set automatically est désactivé, l'iO ne synchronise plus son horloge avec les serveurs NTP. L'heure manuelle doit être utilisée uniquement lorsque NTP n'est pas disponible ou lorsque le système nécessite une heure fixe pour des tests ou la mise en service. Une date/heure incorrecte peut affecter les journaux, les alarmes et les horodatages des données historiques.

2.3 CARTES EXP I/O (CARTES HYBRIDES) – POUR IO SUPERVISOR UNIQUEMENT

Tableau 10: Cartes EXP I/O Cards

CARTE PRINCIPALE	Carte auxiliaire	Entrée analogique	Humidité	Entrée binaire	Sortie binaire Forme-C	Sortie binaire Forme-A
EXP1	Aucune	4x Hybride	1	13	3	0
EXP1	EXP2	10x Hybride	1	29	3	3
EXP1	EXP3	4x Hybride	1	45	3	0
EXP1	EXP4	4x Hybride	1	41	3	3
EXP3	Aucune	0	0	32	0	0
EXP3	EXP3	0	0	64	0	0
EXP3	EXP4	0	0	60	0	3
EXP4	Aucune	0	0	28	0	3
EXP4	EXP4	0	0	56	0	6

2.4 POINTS DE DONNÉES D'ENTRÉE ANALOGIQUE

Les points de données d'entrée analogique sont utilisés pour divers types de mesures. Certaines mesures peuvent nécessiter un transducteur spécifique pour convertir un phénomène physique en un signal analogique. D'autres mesures, comme la tension de batterie, ne nécessitent pas de transducteur et peuvent être câblées directement à un point de données d'entrée analogique.

L'iO Supervisor est conçu pour prendre en charge facilement et efficacement une large gamme de mesures grâce à ses canaux d'entrée analogiques hybrides. Pour chaque entrée analogique, la configuration du frontal est sélectionnable par l'utilisateur selon les exigences du signal de mesure.

- ±50 mV pour la mesure du courant continu via shunt
- Temp pour la mesure de température
- 0-65 Vcc pour la mesure de tension CC et ±65 Vcc pour le SMX-24AI
- 23 Vrms pour la mesure de tension CA
- 0-10 Vcc pour la mesure de tension CC et ±10 Vcc pour le SMX-24AI
- 1.4 Vrms pour la mesure de courant CA

Les canaux analogiques se trouvent sur les modules EXP1, EXP2 et SMX-24AI. Ils partagent la même conception électronique et tous les canaux offrent des spécifications techniques identiques ainsi que des paramètres de fonctionnement configurables.
Les seules exceptions sont les suivantes :

- FIAi5, qui est réservé à la mesure d'humidité.
- Les frontaux 65 Vcc et 10 Vcc sur les EXP1 et EXP2 sont unidirectionnels, alors que sur le SMX-24AI ils sont polarisés, c'est-à-dire ±65 Vcc et ±10 Vcc.

⚠ **Note:**
La mesure du niveau d'humidité ambiante est effectuée à l'aide d'un transducteur spécifique disponible auprès de Multitel.

Tableau 11: Front-end du point de données d'entrée analogique

Type de mesure	Front-End	Transducteur	Échelle
Tension CC telle que la tension du système CC, élément de batterie 12 Vcc, batterie de démarrage de générateur, etc.	0-65Vdc	Non applicable – Pour iO seulement	65
	±65Vdc	Non applicable – Pour SMX-24AI seulement	65
Tension CC provenant de cellules de 2 V	0-10Vdc	Non applicable – Pour iO seulement	10
	±10Vdc	Non applicable – Pour SMX-24AI seulement	10
Utilisé pour le signal de sortie 10 V provenant de divers types de transducteurs : niveau de liquide, courant CC ou CA	10Vdc	Divers transducteurs de tierce partie	Transducer value
Courant CC pour la surveillance des circuits de dérivation des alimentations PDF et des distributions CC, courant de charge et de décharge des chaînes individuelles de batteries, etc.	±50mV	Shunts	Shunt Value
	10Vdc For 0-4Vdc CT	Transducteur de courant CC (±50 A)	125
		Transducteur de courant CC (±100 A)	250
		Transducteur de courant CC (±250 A)	625
		Transducteur de courant CC (±500 A)	1250
Tension CA sur des systèmes monophasés 120/240 Vac ou triphasés 208 Vac utilisant le SDTA de Multitel	23Vrms	SDTA-01 (240Vac)	2680
		SDTA-02 (240Vac/600Vac)	2680/6700

Courant CA utilisant un TC fournissant un signal de sortie 0-333 mVrms	1.4Vrms for 0.333mV AC Current CT	Transformateur de courant CA (50 A)	595
		Transformateur de courant CA (100A)	1189
		Transformateur de courant CA (200A)	2378
		Transformateur de courant CA (400A)	4757
		Transformateur de courant CA (600A)	7135
		Transformateur de courant CA (1500A)	17835
		Transformateur de courant CA (2000A)	23783
Températures ambiantes, intérieures, extérieures	Temp	Sondes de temperature (M-4103, M-4107, M-4109, M-4111, M-4115)	120
Humidité relative ambiante	Humidity	Sonde d'humidité (M-4109) – F1Ai5 seulement	100
Courant de charge flottante pour la dérive thermique	±50mV	FCCP-01 (Sonde de courant de charge flottante)	5

2.4.1 FONCTIONNEMENT DE L'ENTRÉE ANALOGIQUE (HYBRIDE)

Chaque point de données d'entrée analogique est câblé au panneau arrière. L'iO Supervisor surveille en continu le niveau de tension entre chaque canal analogique et sa valeur de référence (voir figure ci-dessous). Un ou plusieurs seuils logiciels peuvent être associés à chaque canal afin de générer des alarmes ou d'activer des contrôles.

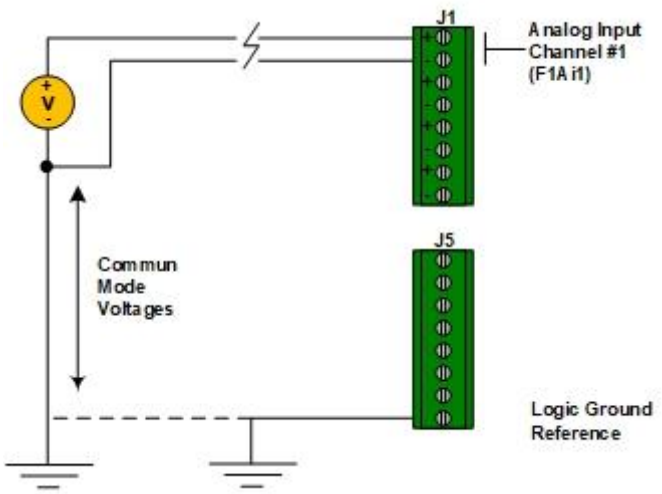


Figure 16: Analog Input – Connection

Multitel

⚠ **Note:**
Respecter la polarité pour chaque point de données d'entrée analogique afin que les valeurs s'affichent correctement. Porter une attention particulière à la mesure de tension -48 Vcc.

2.4.2 CONFIGURATION DE L'ENTRÉE ANALOGIQUE

Les points de données d'entrée analogique sont affichés dans la section IO Channel du menu.

La section des entrées analogiques affiche tous les points de données d'entrée analogique disponibles dans l'iO Supervisor.

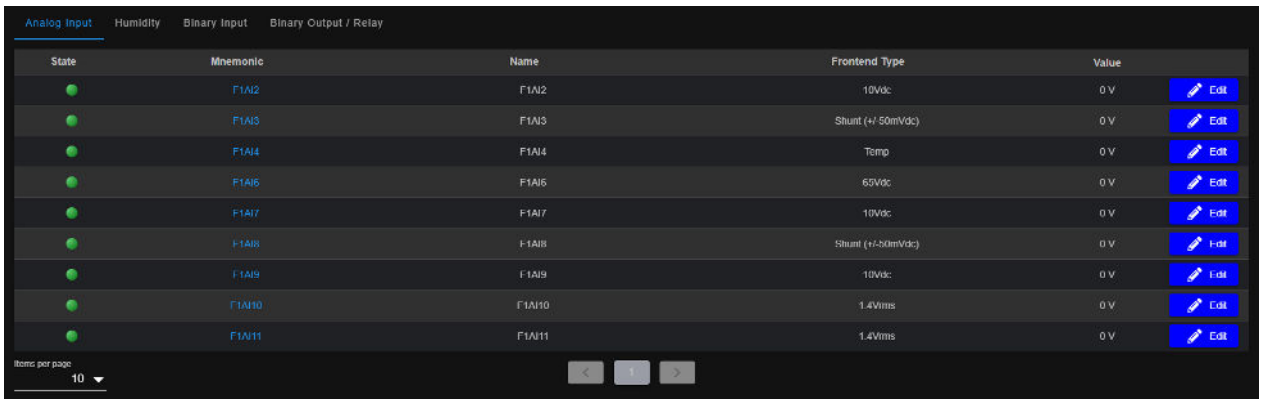
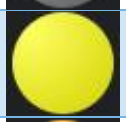


Figure 17: Entrée analogique – Canal IO

La colonne d'état donne à l'utilisateur une représentation visuelle de l'état du point de données.

Tableau 12: État du canal iO

Couleur d'état	État	Description
	Activer	L'acquisition fonctionne.
	Désactiver	Le point de données est désactivé.
	Succès partiel	Applicable au niveau de l'actif : l'erreur d'acquisition des points de données de l'actif est inférieure à 50 %.
	OVL+, OVL-	Surcharge supérieure et inférieure
	Échec partiel	Applicable au niveau de l'actif : l'erreur d'acquisition des points de données de l'actif est supérieure à 50 %.

	Pas encore disponible	La première acquisition du point de données n'est pas terminée. Cela peut être dû à une erreur de communication ou si l'actif est désactivé.
	Statut non disponible	Erreur dans la communication.
	Erreur de configuration du statut	Affiché lorsqu'un point de données ne peut pas obtenir de valeur en raison d'une mauvaise configuration. Cela se produit principalement pour les points de données calculés lorsqu'il y a une erreur dans le script Lua.
	Statut suspendu	Le statut Suspended survient lorsqu'un actif a atteint son Number of Retry configuré, a attendu le Timeout After Retry défini et a complété le Total Iteration Number spécifié sans communication réussie. Lorsque toutes les tentatives de réessai et les délais d'attente configurés ont été épuisés, l'actif est automatiquement placé en statut Suspended pour indiquer que la communication a échoué avec la configuration actuelle.

Le mnémonique est un identifiant unique dans l'iO. Le point de données d'entrée analogique utilise le format suivant :

• F1AIx
• F : Identifiant pour IO Channel.
• 1 : Identifiant pour IO Channel.
• AI : Analog Input.
• x : 1 à 11 (numéro du point de données).

Pour configurer le point de données d'entrée analogique, l'utilisateur peut cliquer sur Edit du côté droit du point de données.

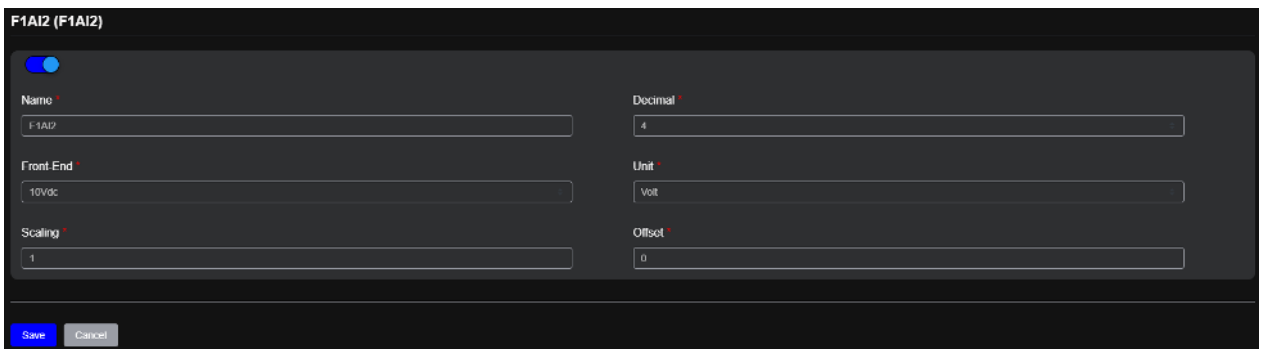


Figure 18: Configuration de l'entrée analogique

Multitel

Une liste des paramètres programmables possibles sera affichée.

Tableau 13: Configuration de l'entrée analogique

Champ	Description	Spécification	Obligatoire
Name	Nom du point de données d'entrée analogique	Alphanumérique, 1-50 caractères	Oui
Decimal	Valeur décimale utilisée pour afficher la valeur du point de données. La décimale arrondira la valeur du point de données.	Liste déroulante	Oui
Front-End	Type de front-end : • Shunt (±50mVdc) • Temp • 65Vdc • 23Vrms • 10Vdc • 1.4Vrms	Liste déroulante Valeur par défaut : Shunt (±50mVdc)	Oui
Unit	Valeur d'unité du point de données. Si le front-end Temp est sélectionné, seulement Celsius ou Fahrenheit est disponible. La valeur de température sera convertie automatiquement.	Liste déroulante	Oui
Scaling	Facteur d'échelle	1 à 65 535 (16bit)	Oui
Offset	Facteur de décalage	±1.79 E+308	Oui

2.4.3 VALEURS QUOTIDIENNES D'ENTRÉE ANALOGIQUE

Les valeurs quotidiennes d'entrée analogique sont des points de données récapitulatifs automatiquement calculés à partir des valeurs d'un point de données au cours d'une journée. Elles sont utilisées pour visualiser le comportement et les tendances quotidiennes sans avoir à analyser l'historique haute fréquence.

2.4.3.1 Accéder à la page des valeurs quotidiennes

Dans la section Analog Input, cliquer sur le mnémonique en bleu (par exemple F1AI1) pour ouvrir la page Data Point Details de l'entrée analogique et afficher ses valeurs quotidiennes.

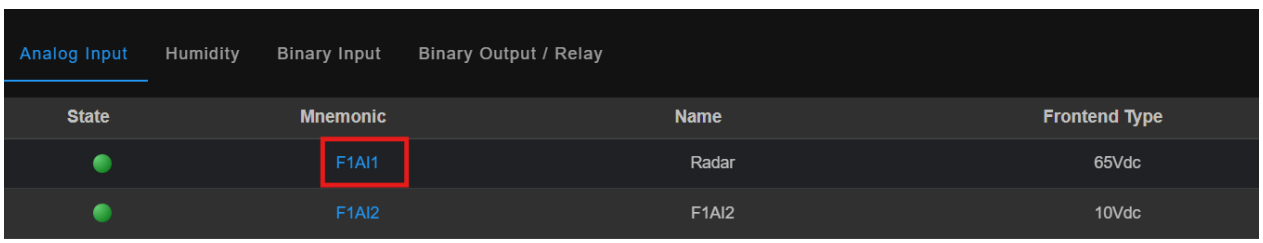


Figure 19: Entrée analogique – Valeurs quotidiennes

Multitel

2.4.3.2 Disponibilité sur l'ensemble de la plateforme

Les valeurs quotidiennes ne sont pas propres aux entrées analogiques F1AIx (IO Channel). Elles sont disponibles pour tous les points de données analogiques de la plateforme, y compris :

• Les points de données internes (calculés)
• Les points de données provenant de protocoles de communication tels que SNMP et Modbus

En d'autres termes, toute mesure analogique prise en charge par la plateforme peut fournir des valeurs quotidiennes, quelle que soit sa source.

2.4.3.3 Page des valeurs quotidiennes

Après avoir cliqué sur le mnémonique en bleu, la plateforme ouvre la page Data Point Details pour le point de données analogique sélectionné.

Cette page fournit des éléments clés :

- **Peaks**: Le tableau Peaks répertorie les valeurs minimales et maximales enregistrées pour la période sélectionnée (jusqu'à 365 jours). Pour chaque valeur extrême, la plateforme affiche également la date et l'heure auxquelles elle s'est produite. Cela permet d'identifier rapidement le moment où la lecture la plus basse ou la plus élevée est survenue.

- **Daily Values Chart**:
  Le graphique affiche les statistiques quotidiennes au fil du temps :
  o Average (valeur moyenne quotidienne)
  o Max (valeur maximale quotidienne)
  o Min (valeur minimale quotidienne)

  En survolant le graphique avec la souris, une info-bulle affiche les valeurs Avg / Max / Min pour la journée sélectionnée, permettant une comparaison rapide jour par jour et une analyse des tendances.

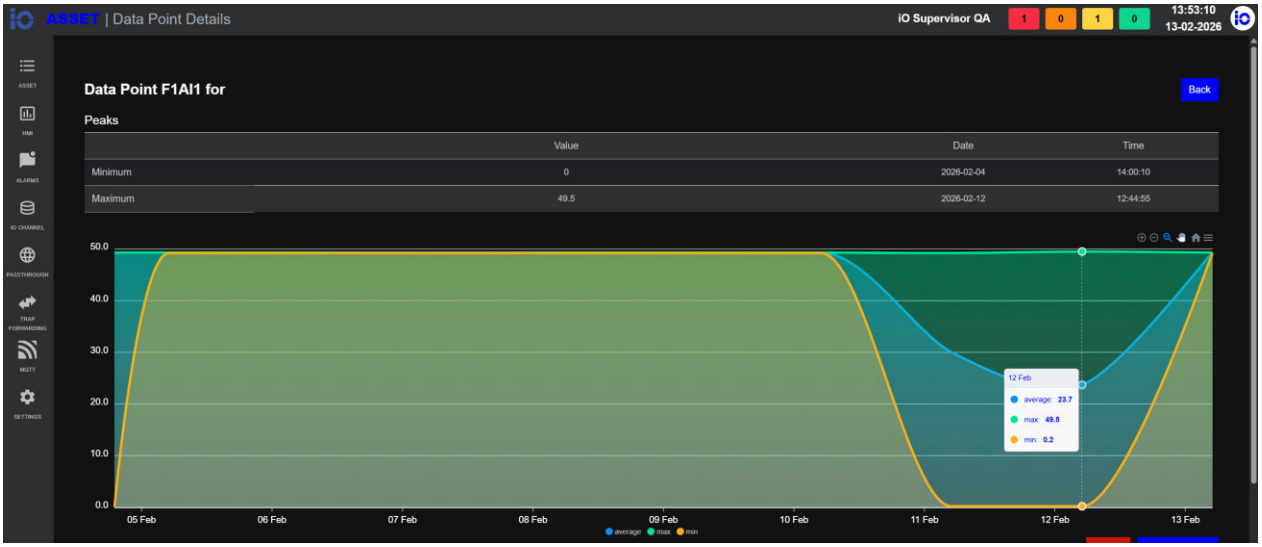


Figure 20: Pics et graphique des valeurs quotidiennes – Entrée analogique

- **Tableau des valeurs quotidiennes**
  Le tableau affiche les statistiques quotidiennes au fil du temps :
  o **Date** : Journée pour laquelle les statistiques ont été calculées.
  o **Average** : Valeur moyenne enregistrée durant la journée.
  o **Delta** : Différence entre la valeur maximale et la valeur minimale quotidiennes (Max − Min). Cela indique la variation du signal durant la journée.
  o **Minimum Value** : Valeur la plus basse enregistrée durant la journée.
  o **Time (Min)** : Heure à laquelle la valeur minimale s'est produite.
  o **Maximum Value** : Valeur la plus élevée enregistrée durant la journée.
  o **Time (Max)** : Heure à laquelle la valeur maximale s'est produite.

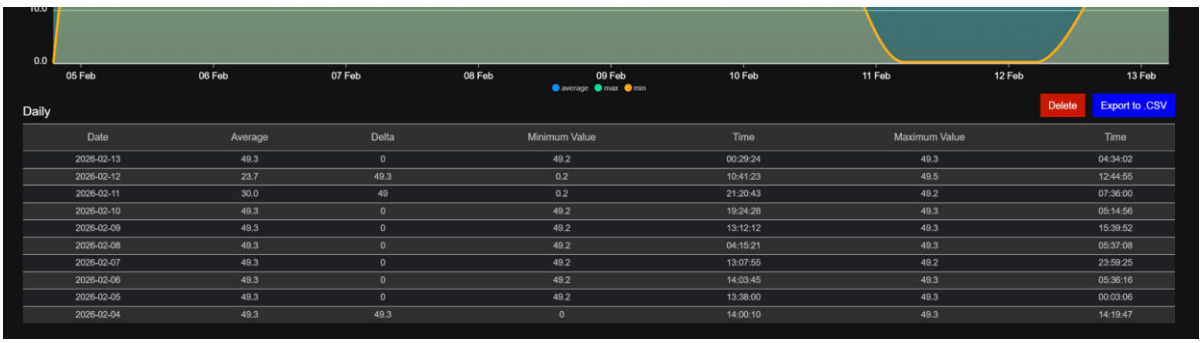


Figure 21: Tableau des valeurs quotidiennes – Entrée analogique

- **Export** : Télécharger la table quotidienne dans un fichier CSV pour création de rapports ou analyse ultérieure (Excel, outils BI, etc.).
- **Delete** : Supprime l'ensemble de l'enregistrement (utile pour le nettoyage après la mise en service/tests ou lorsque des données invalides doivent être supprimées).

⚠ **Note:** La suppression des enregistrements quotidiens affecte le résumé historique quotidien du point de données. À utiliser avec prudence et conformément à votre politique de conservation des données.

2.4.3.4 Information générale des valeurs quotidiennes

- Les valeurs quotidiennes sont calculées en utilisant les paramètres configurés du point de données (unité, facteur d'échelle, décalage, décimales, etc.).
- Les valeurs quotidiennes sont des points de données en lecture seule.
- Au début de chaque journée, les valeurs quotidiennes sont réinitialisées et commencent à accumuler de nouvelles statistiques pour la journée en cours.

⚠ **Note:** Si un point de données est Disabled, en Status-not-available, ou présente une surcharge (OVL+/OVL-), ses valeurs quotidiennes peuvent être incomplètes ou indisponibles pour cette journée.

2.5 POINTS DE DONNÉES D'ENTRÉE BINAIRE (EXP1, EXP2, EXP3, EXP4)

Une terminologie différente est utilisée pour désigner les points de données d'entrée binaire, tels que Dry-C, Discrete, Alarm et Event Channels. Ces canaux sont utilisés pour détecter des changements d'état marche/arrêt (par exemple porte ouverte, défaillance du redresseur, panne CA, HVAC en marche, etc.). La plupart des équipements ou systèmes surveillés peuvent actionner un relais pour générer une alarme par contact sec lorsqu'un changement d'opération survient. Les entrées binaires de l'iO sont utilisées pour détecter les changements dans l'opération de l'équipement ou du système.

Normalement, un contact de relais envoie un signal de mise à la terre à un canal d'entrée binaire spécifique, et l'iO Supervisor détecte ce signal de terre pour déclencher une action selon des conditions préprogrammées. Pour certains types de détections (par exemple fumée/incendie, porte ouverte, présence d'eau, etc.), des transducteurs doivent être utilisés pour effectuer ces tâches. Une grande variété de capteurs, sondes et transducteurs est disponible directement auprès de Multitel.

Chaque entrée binaire est programmable individuellement. Les fonctions de regroupement, les niveaux de sévérité des alarmes, les fichiers d'historique et de nombreuses autres fonctionnalités font de l'iO Supervisor un outil puissant pour la gestion des alarmes d'infrastructure de sites de télécommunication. L'iO Supervisor et les canaux d'entrée binaire SMX-48BI partagent la même conception électronique, les mêmes spécifications techniques et les mêmes paramètres de fonctionnement.

2.5.1 FONCTIONNEMENT DE L'ENTRÉE BINAIRE

L'iO Supervisor surveille en continu le niveau de tension entre chaque point de données d'entrée binaire et la référence Logic Ground. Lorsque la tension se situe dans la « plage de niveau de tension » du « niveau d'activation » sélectionné, l'état du point de données d'entrée binaire changera et sa source de déclenchement correspondante s'activera.

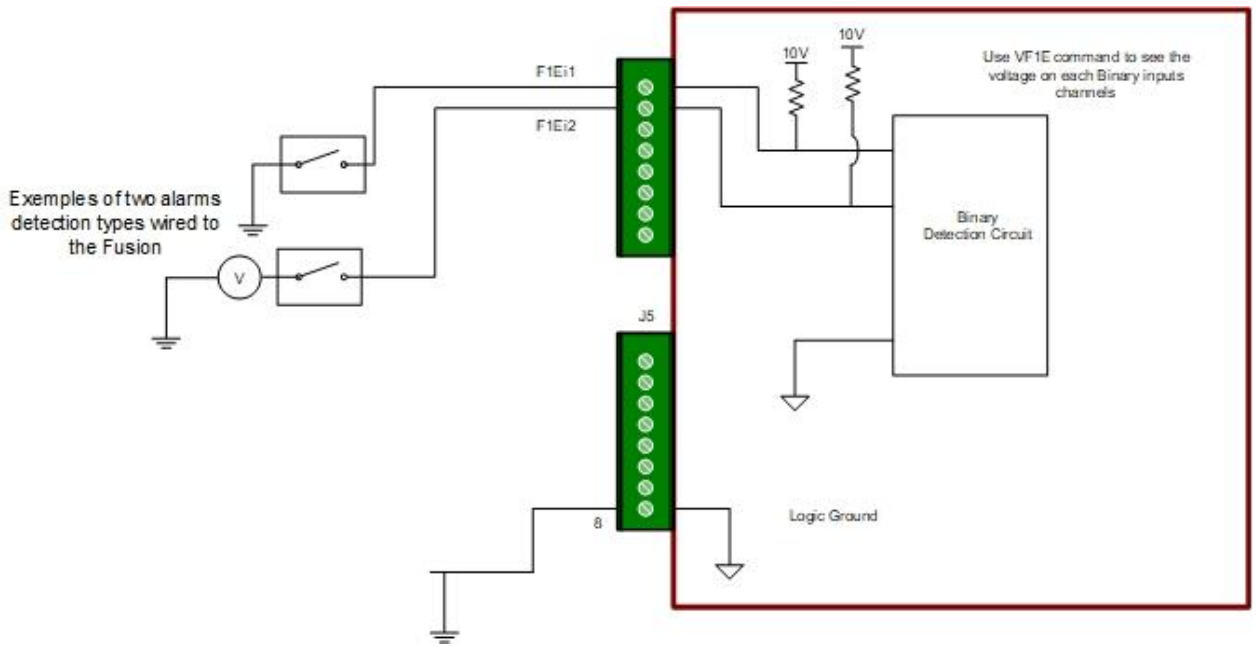


Figure 22: Configuration de l'entrée binaire

L'iO Supervisor fournit entre 13 et 64 points de données d'entrée binaire selon les cartes EXP I/O installées.

Multitel

2.5.2 CONFIGURATION DE L'ENTRÉE BINAIRE

Les points de données d'entrée binaire sont affichés dans la section IO Channel du menu.

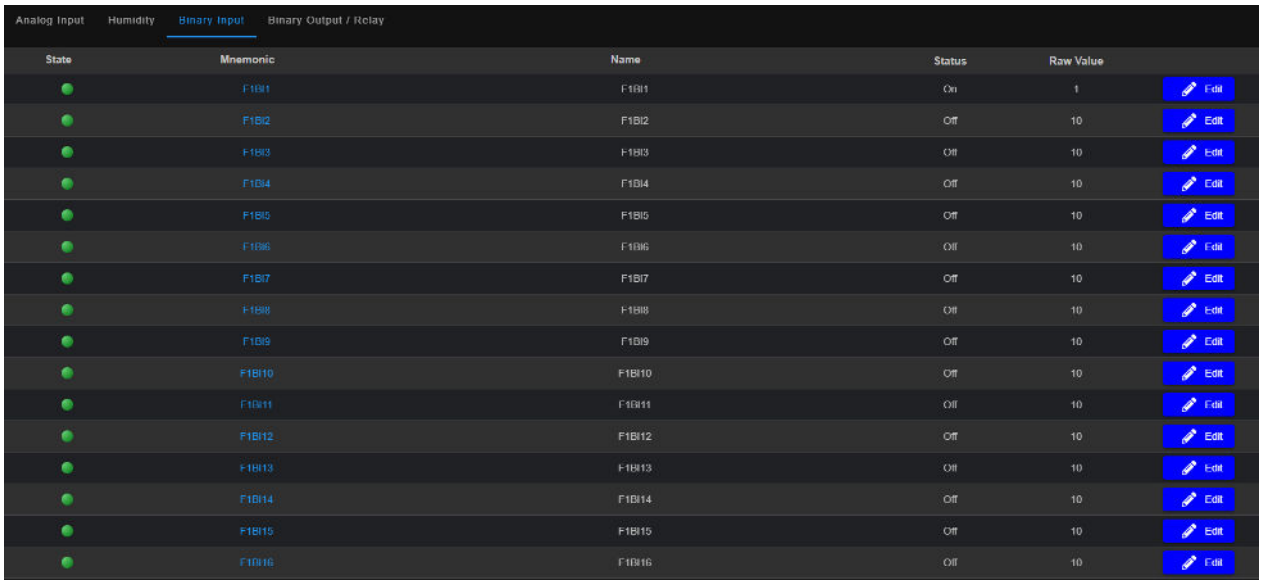


Figure 23: Entrée binaire – Canal IO

Le mnémonique est un identifiant unique dans l'iO. Le point de données d'entrée binaire utilise le format suivant F1Bix :

- F : Identifiant pour IO Channel.
- 1 : Identifiant pour IO Channel.
- BI : Binary Input.
- x : 1 à 64 (numéro du point de données).

Pour configurer le point de données d'entrée binaire, l'utilisateur peut cliquer sur Edit du côté droit du point de données.

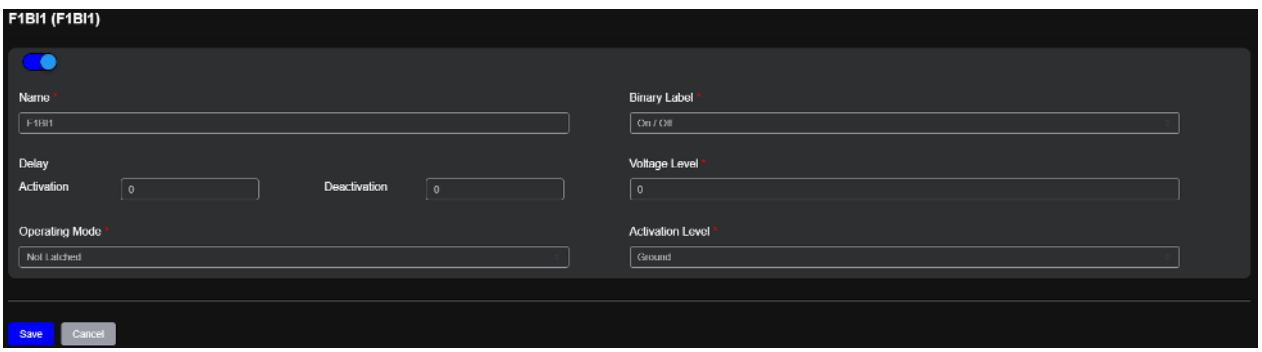


Figure 24: Entrée binaire – Configuration

Multitel

Tableau 14: Entrée binaire - Configuration

Champs	Description	Spécification	Obligatoire
Name	Nom du point de données d'entrée binaire.	Alphanumeric, 1-50 characters	Oui
Binary Label	Étiquette utilisée pour afficher les valeurs true ou false.	Liste déroulante	Oui
Activation Delay	Temps prédéfini utilisé pour retarder l'activation de l'entrée, le comptage commence sur un front montant de l'entrée.	0 à 999 secondes	Oui
Deactivation Delay	Temps prédéfini utilisé pour retarder la désactivation de l'entrée, le comptage commence sur un front descendant de l'entrée.	0 à 999 secondes	Oui
Voltage Level	Niveau de tension d'entrée.	0 à 70V (absolute)	Oui
Operating Mode	Le niveau d'activation permet à l'utilisateur de sélectionner entre les niveaux Ground ou Battery.	Liste déroulante	Oui
Activation Level	Le niveau d'activation permet à l'utilisateur de sélectionner entre les niveaux Ground ou Battery.	Liste déroulante	Oui
Operating Mode	Seul le mode unlatched est disponible.	Liste déroulante	Oui

Marges du niveau d'activation :

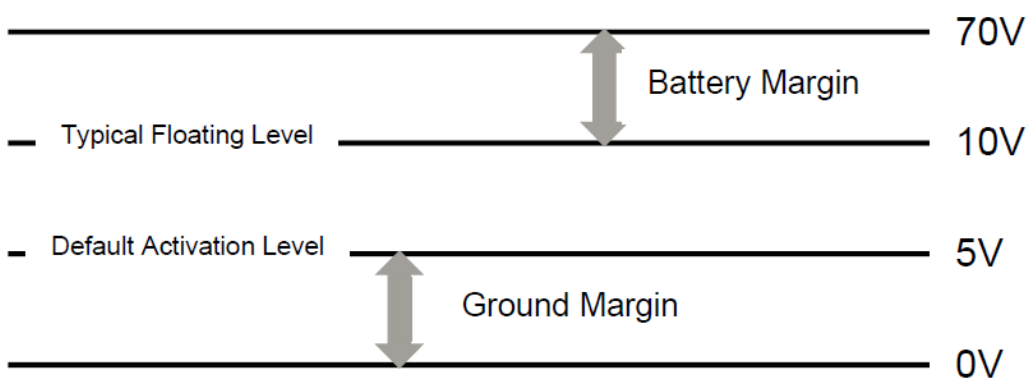


Figure 25: Entrée binaire – Niveau d'activation

Chaque entrée binaire est terminée au panneau arrière de l'iO Supervisor. Une alarme peut être déclenchée lorsque la connexion entre l'équipement ou le capteur et le canal d'entrée binaire de l'iO est ouverte.

Multitel

2.5.3 JOURNAUX D'ENTRÉE BINAIRE

Les journaux d'entrée binaire fournissent une vue historique des transitions d'état (True/False) pour un point de données d'entrée binaire. Ils sont utilisés pour valider l'activité des alarmes, confirmer le moment des événements et dépanner des problèmes intermittents sans dépendre de la surveillance en temps réel.

2.5.3.1 Accéder à la page des journaux d'entrée binaire

Dans la section Binary Input, cliquer sur le mnémonique en bleu (par exemple F1BI2) pour ouvrir la page Data Point Details de l'entrée binaire et afficher ses journaux (Latest Value Changes).

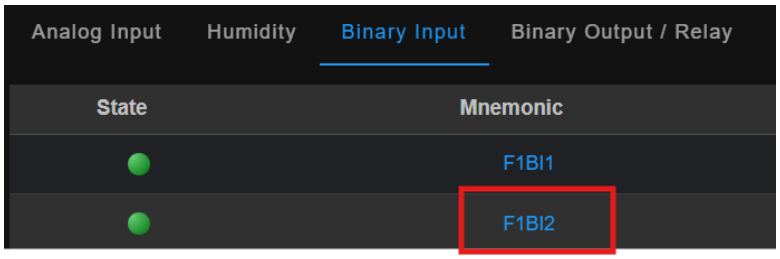


Figure 26: Entrée binaire – Page de journal

2.5.3.2 Disponibilité sur l'ensemble de la plateforme

Les journaux d'entrée binaire ne sont pas propres aux entrées binaires F1BIx (IO Channel). Les vues de journaux/historique sont disponibles pour les points de données binaires sur l'ensemble de la plateforme, y compris :

• Les points de données binaires internes (calculés).
• Les points de données provenant de protocoles de communication tels que SNMP et Modbus (lorsque le point de données est binaire).

En d'autres termes, tout point de données binaire (true/false) pris en charge par la plateforme peut fournir des journaux, quelle que soit sa source.

2.5.3.3 Page de journaux des entrées binaires (Détails de points de données)

Après avoir cliqué sur le mnémonique en bleu, la plateforme ouvre la page Data Point Details pour le point de données d'entrée binaire sélectionné.

Cette page fournit les éléments clés suivants :

• **Latest Value Changes** (table de journal) :
Cette table répertorie les changements d'état les plus récents détectés pour l'entrée binaire. Le journal est une table cyclique qui stocke et affiche les 500 derniers événements. Une fois la limite atteinte, les entrées les plus anciennes sont écrasées.

Chaque entrée inclut :

• **Status** : L'état enregistré (True/False)
• **Date** : Date à laquelle le changement s'est produit
• **Time** : Heure à laquelle le changement s'est produit

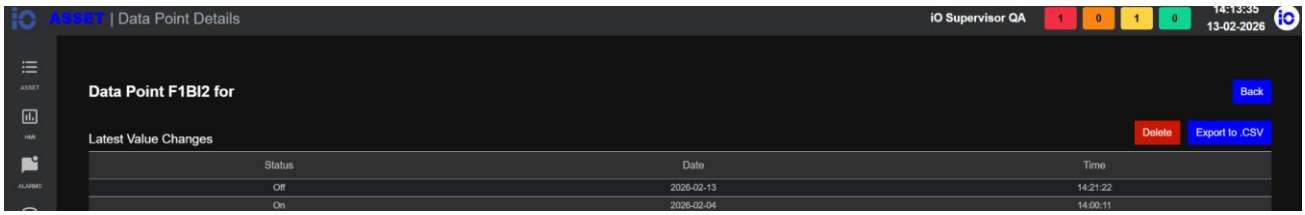


Figure 27: Entrée binaire – Tableau des derniers changements de valeur

- **Export:** Télécharge la table de journal dans un fichier CSV pour création de rapports ou analyse ultérieure (Excel, outils BI, etc.).
- **Delete:** Efface la table de journal (utile pour le nettoyage après la mise en service/tests ou lorsque des événements invalides doivent être supprimés).

⚠️ **Note:** La suppression des enregistrements de journal affecte la traçabilité historique des événements pour le point de données. À utiliser avec prudence et conformément à votre politique de conservation des données.

2.5.3.4 Journaux d'entrées binaires – Information générale

- Les journaux sont des enregistrements en lecture seule générés lorsque l'entrée binaire change d'état.
- Une nouvelle entrée de journal est créée à chaque front montant (False → True) et à chaque front descendant (True → False).
- Si les délais d'activation (Activation Delay) et de désactivation (Deactivation Delay) sont configurés, l'heure enregistrée dans le journal correspond au moment où le changement d'état devient valide après expiration du délai configuré.
- Si une entrée binaire est Disabled ou en Status-not-available, de nouvelles entrées de journal peuvent ne pas être enregistrées.

2.6 POINTS DE DONNÉES DES SORTIES BINAIRES (EXP1, EXP2, EXP3, EXP4)

Selon le modèle d'iO Supervisor, jusqu'à six canaux de sortie binaire (relais) sont inclus. Ces canaux de sortie binaire sont utilisés pour générer des alarmes discrètes ou pour contrôler le fonctionnement de systèmes ou d'équipements (par exemple démarrage/arrêt) à l'aide des contacts de relais internes. Les opérations des relais peuvent être déclenchées manuellement ou au moyen d'une équation de déclenchement programmable par l'utilisateur.

Lorsqu'un relais est utilisé pour des alarmes discrètes, un point de données de sortie binaire est connecté à l'équipement d'alarme local ou de télémétrie. Cela permet aux alarmes générées par l'iO Supervisor d'être communiquées aux centres d'exploitation ou de surveillance des réseaux.

Les points de données de sortie binaire peuvent être utilisés pour démarrer et arrêter d'autres équipements à distance, soit manuellement, soit automatiquement. Les applications varient largement — de la mise en marche ou l'arrêt de redresseurs, convertisseurs ou générateurs, à la déconnexion de charges dans des applications solaires, ou à la régulation de la ventilation et des unités HVAC.

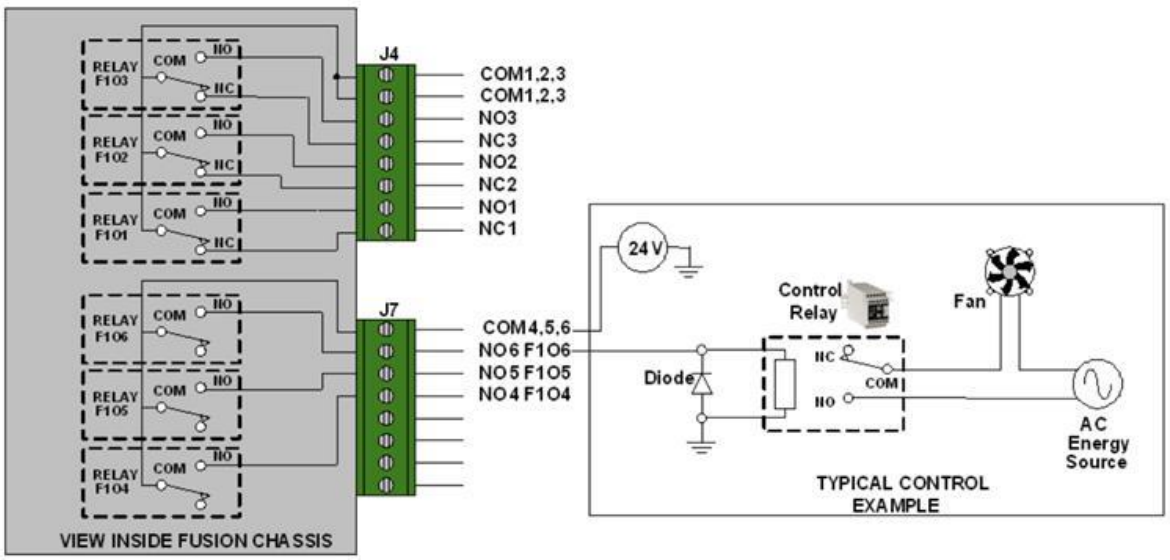


Figure 28: Sortie binaire – Points de données

2.6.1 OPÉRATION DE SORTIE BINAIRE

Les points de données de sortie binaire sont terminés sur le panneau arrière de l'iO Supervisor. Afin de faciliter le câblage des contacts de relais, tous les contacts « communs » des relais sont pontés ensemble à l'interne.

Contacts de relais disponibles :
• 3 relais de type Form "C" : des contacts N.O. et N.C. sont disponibles pour chaque relais
• 3 relais de type Form "A" : seulement des contacts N.O. sont disponibles pour chaque relais

⚠ **Avertissement :**
L'iO Supervisor utilise des micro-relais, qui doivent être protégés avec une diode lorsqu'ils sont connectés à des charges inductives importantes telles que des solénoïdes ou des bobines de relais de commande. Sinon, l'équipement peut se réinitialiser ou subir des dommages.

2.6.2 SORTIE BINAIRE / CONFIGURATION DU RELAY

Les points de données de sortie binaire sont affichés dans la section IO Channel du menu.

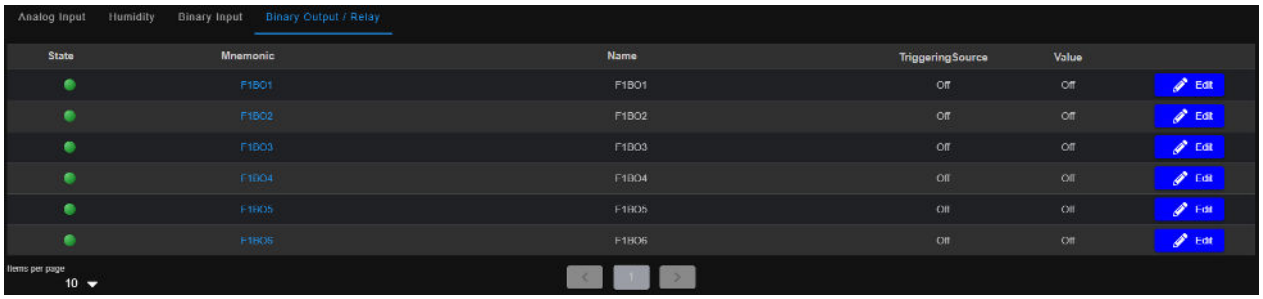


Figure 29: Sortie binaire – Canal IO

Le mnémonique est un identifiant unique dans l'iO. Le point de données de sortie binaire utilise le format suivant F1BOx :

- F : Identifiant pour IO Channel.
- 1 : Identifiant pour IO Channel.
- BO : Binary Output.
- x : 1 à 6 (numéro du point de données).

Pour configurer le point de données d'entrée binaire, l'utilisateur peut cliquer sur Edit du côté droit du point de données.

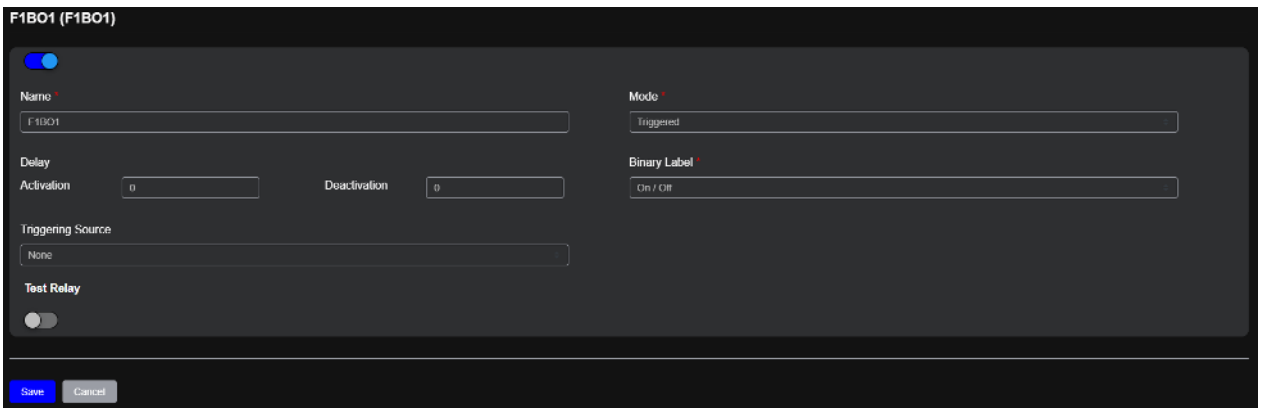


Figure 30: Sortie binaire – Configuration

Une liste des paramètres programmables possibles sera affichée :

Tableau 15: Sortie binaire - Configuration

Champ	Description	Spécification	Obligatoire
Name	Nom du point de données de sortie binaire.	Alphanumérique, 1-50 caractères	Oui
Mode	Le mode de fonctionnement permet à l'utilisateur de sélectionner entre les modes Triggered et Pulsed.	Liste déroulante	Oui

Activation Delay	Temps prédéfini utilisé pour retarder l'activation de la sortie, le comptage commence sur un front montant de l'entrée.	0 à 999 seconds	Oui
Deactivation Delay	Temps prédéfini utilisé pour retarder la désactivation de la sortie, le comptage commence sur un front descendant de l'entrée.	0 à 999 seconds	Oui
Binary Label	Étiquette utilisée pour afficher la valeur true ou false.	Liste déroulante	Oui
Triggering Source	Source de déclenchement utilisée pour activer le point de données de sortie. Tous les points de données binaires à l'intérieur de l'iO peuvent être utilisés comme source de déclenchement.	Liste déroulante	Oui
Test Relay	Utilisé pour tester la fonction de sortie.	Dongle	Oui

2.6.2.1 Mode de déclenchement

Le point de données de sortie devient actif lorsque l'équation ou la source de déclenchement évalue à TRUE (valide). L'activation sera retardée par le temps de délai d'activation configuré et prolongée par le délai de désactivation prédéfini.

Par exemple, si F1BI1 est la source de déclenchement, avec un délai d'activation de 10 secondes et un délai de désactivation de cinq secondes, le signal du canal de sortie F1BO1 se comporterait comme suit :

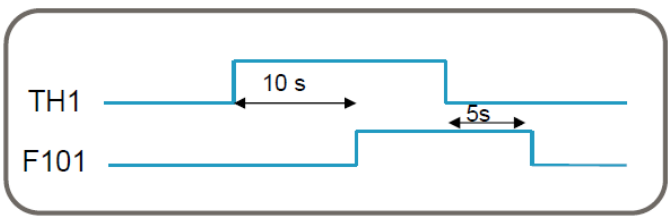


Figure 31: Sortie binaire – Mode de déclenchement

2.6.2.2 Mode pulsé

Le point de données de sortie devient actif lorsque la source de déclenchement est active. Il restera ON tant que la durée d'impulsion prédéfinie n'aura pas expiré. Si la source de déclenchement reste active pendant une période plus courte que la durée de l'impulsion, la sortie restera ON pendant toute la durée d'impulsion prédéfinie.

Par exemple, si F1BI1 est la source de déclenchement et que la durée de l'impulsion est de 10 secondes, le signal du canal de sortie F1BO2 se comporterait comme suit :

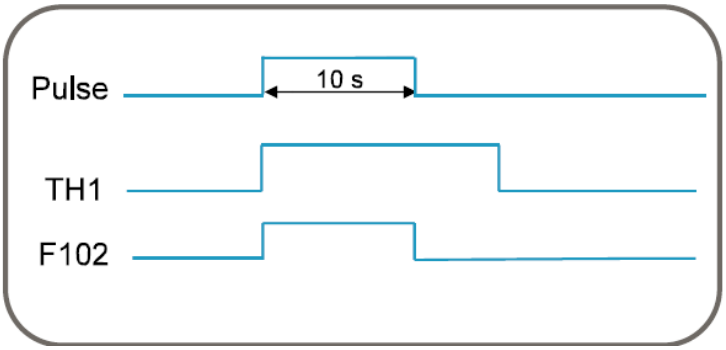


Figure 32: Sortie binaire – Mode pulsé

2.6.3 SORTIE BINAIRE/JOURNAUX DE RELAY

Les journaux de sortie binaire fournissent une vue historique des transitions d'état (True/False) pour un point de données de sortie binaire / relais. Ils sont utilisés pour confirmer quand une sortie a été activée ou désactivée, valider le comportement de commande et dépanner les activations de relais inattendues.

Les journaux de sortie binaire fonctionnent de la même manière que les journaux d'entrée binaire (même format de journal, même comportement cyclique, mêmes options d'exportation/suppression et mêmes règles générales sur le moment des événements). Pour plus de détails sur le fonctionnement de la table de journal, le nombre d'enregistrements conservés et la façon dont les horodatages sont enregistrés, se référer à la section 2.5.3 – Binary Input Logs.

Cas d'utilisation typiques :

- Confirmer quand un relais/une sortie a été mis ON ou OFF (action manuelle ou logique déclenchée).
- Valider qu'une source de déclenchement commande correctement la sortie (p. ex. correspondance alarme-vers-relais).
- Dépanner le cliquetis d'un relais (changements fréquents ON/OFF) ou des activations inattendues.
- Exporter les derniers événements pour les rapports de mise en service ou pour le dépannage client.

⚠ **Note** : Si la sortie est Disabled ou en Status-not-available, de nouvelles entrées de journal peuvent ne pas être enregistrées. Si des délais d'activation (Activation Delay) et de désactivation (Deactivation Delay) sont configurés, les heures enregistrées dans le journal reflètent le moment où l'état de la sortie devient valide après expiration du délai configuré.

2.7 MODULES SMX

L'iO Supervisor est capable d'acquérir des données provenant d'appareils distants en utilisant le protocole standard Modbus RTU via ses ports de communication RS-485. Jusqu'à 128 modules peuvent être connectés à un seul iO Supervisor : un maximum de 64 modules sur chacun des ports RS-485.

Les modules SMX sont disponibles en deux variantes : le SMX-48BI et le SMX-24AI. Tous les modules SMX peuvent être mis en réseau avec l'iO Supervisor en utilisant le protocole ouvert Modbus RTU.

Les modules SMX ne nécessitent aucune configuration manuelle des registres Modbus. Une fois configurés, les points de données analogiques et binaires des SMX sont traités comme n'importe quels autres canaux d'E/S de l'iO Supervisor. Des seuils peuvent être configurés, et des statistiques ainsi que des données historiques peuvent être enregistrées.

2.8 NIVEAUX D'ALARMES

Les alarmes de l'iO permettent à l'utilisateur d'identifier rapidement les points de surveillance et de contrôle dans le système. Les alarmes sont situées en haut à droite de l'interface. Les alarmes seront affichées dans l'en-tête lorsque les conditions configurées par l'utilisateur sont remplies. Une fois qu'une alarme est terminée, elle disparaîtra de l'en-tête.

Figure 33: Niveaux d'alarmes

Pour configurer les niveaux d'alarme, voir la section STATUSES.

Multitel

3. UTILISATION DE L'IO

3.1 ASSET

Le module Asset est utilisé pour créer et gérer les équipements surveillés dans la plateforme iO. Un asset représente un appareil ou un système sur un site (par exemple : DC Plant, Battery (BMS), Generator, HVAC, modules SMX, etc.). Une fois qu'un asset est créé et activé, l'iO peut communiquer avec l'asset en utilisant le protocole de communication configuré et appliquer les règles du gabarit pour générer et acquérir les points de données associés.

3.1.1 APERÇU DE L'ASSET

Le module Asset permet aux utilisateurs de :

- Créer de nouveaux assets et les associer à un site.
- Sélectionner un type d'asset et un gabarit.
- Configurer le protocole de communication nécessaire pour atteindre l'asset (par exemple SNMP).
- Configurer le comportement du moteur de poll (poll rate, timeout, retries).
- Activer ou désactiver l'acquisition de l'asset.

3.1.2 CRÉATION DE L'ASSET

Pour créer un nouvel asset :
• Cliquer sur Asset.
• Cliquer sur + Asset (ou Create Asset).
• Compléter les champs décrits ci-dessous.
• Cliquer sur Save.

Le formulaire de création d'asset contient les champs principaux suivants.

Main Information
• **Asset Name**
Nom utilisé pour identifier l'asset dans la plateforme.
• **Site**
Site où l'asset sera créé.
• **Asset Type**
Définit la catégorie de l'équipement (par exemple : DC Plant, Battery (BMS), Generator, HVAC, etc.).
Les valeurs de Asset Type sont gérées via la configuration Inventory.
• **Template**
Définit le gabarit de surveillance qui sera appliqué à l'asset.
Les gabarits sont gérés via la configuration Inventory.
• **Manufacturer**
Fabricant associé au type/gabarit d'asset sélectionné (généralement rempli automatiquement une fois le type/gabarit sélectionné).

• **Communication Protocol**
Sélectionne le protocole utilisé pour communiquer avec l'asset (par exemple : SNMP Get). La sélection du protocole détermine quelle section de configuration apparaît plus bas (SNMP, Modbus, etc.).
• **Smart Asset**
Indique si l'asset utilise un comportement de gabarit intelligent (affiché comme Yes lorsque applicable).

Une fois les champs requis complétés, cliquer sur :

• **Save** pour créer l'asset.
• **Cancel** pour annuler les changements.

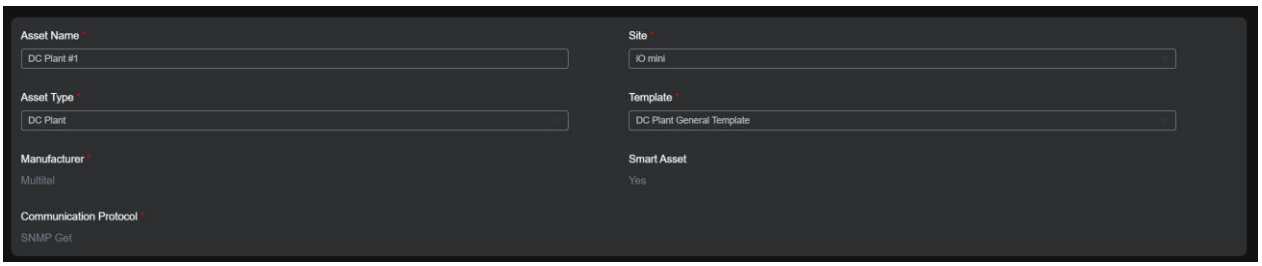


Figure 34: Aperçu de l'asset

3.1.3 CONFIGURATION DU PROTOCOLE DE COMMUNICATION

Après avoir sélectionné un protocole de communication, le panneau de configuration correspondant est affiché.

3.1.3.1 Protocole de communication SNMP

Figure 35: Protocole de communication -- SNMP

- **Asset IP Address**
  Adresse IP du dispositif SNMP.
- **Asset Hostname**
  Champ de nom d'hôte optionnel. S'il est utilisé, s'assurer que le DNS est configuré dans les paramètres de connexions de l'iO.
- **SNMP Version**
  Version SNMP utilisée pour le polling (exemple montré : **SNMP v1**).

- **SNMP Device Community Name**
  Chaîne de communauté utilisée pour l'authentification (exemple montré : public).
- **Port Number**
  Port UDP utilisé pour le polling SNMP (la valeur par défaut typique de SNMP est **161**).
- **Constant Part of OID**
  Champ optionnel utilisé pour définir un préfixe d'OID de base pouvant être réutilisé par les définitions de gabarits/points de données.

⚠️ **Note:** La liste exacte des champs requis dépend de la version SNMP sélectionnée et des règles du gabarit. Toujours confirmer que l'adressage IP, le port et les identifiants correspondent à la configuration du dispositif surveillé.

3.1.3.2 Protocole de communication – Modbus RTU

Lorsque Modbus RTU est sélectionné comme protocole de communication, la plateforme affiche les paramètres de communication série utilisés pour atteindre l'appareil Modbus via RS-485.

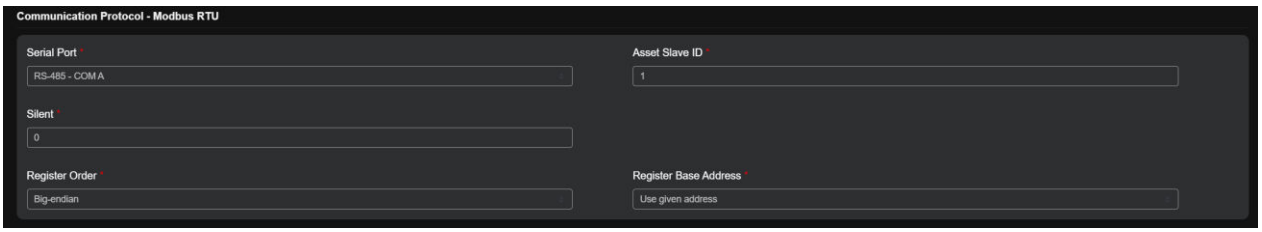


Figure 36: Protocole de communication – Modbus RTU

- **Serial Port**
  Sélectionner l'interface RS-485 utilisée pour communiquer avec l'asset (exemple : RS-485 – COM A).
- **Asset Slave ID**
  Adresse esclave Modbus de l'appareil distant. Cette valeur doit correspondre à l'ID esclave configuré dans l'équipement surveillé.
- **Silent**
  Intervalle silencieux (en millisecondes) appliqué entre les trames Modbus. Ceci est utilisé pour stabiliser les communications sur des liaisons série lentes ou bruyantes.
  (La valeur par défaut est généralement 0 sauf si requise par l'appareil.)
- **Register Order**
  Définit l'ordre des octets/mots utilisé pour interpréter les valeurs multi-registres.
  Cela doit correspondre à la définition des registres Modbus du fabricant.
- **Register Base Address**
  Définit la façon dont les adresses de registres sont interprétées par la plateforme. Ce paramètre est utilisé pour aligner la numérotation des registres entre la documentation du fournisseur et le gabarit configuré.

⚠️ **Note:** Modbus RTU nécessite un câblage RS-485 correct (polarité A/B), une terminaison adéquate et une adresse d'appareil correcte. Si les valeurs sont incorrectes ou instables, valider l'ID esclave, les paramètres de débit (côté appareil) et l'ordre/adressage de base des registres.

3.1.3.3 Protocole de communicationl – Modbus TCP

Lorsque Modbus TCP est sélectionné comme protocole de communication, la plateforme utilise Ethernet/IP pour communiquer avec l'asset via un serveur Modbus TCP.

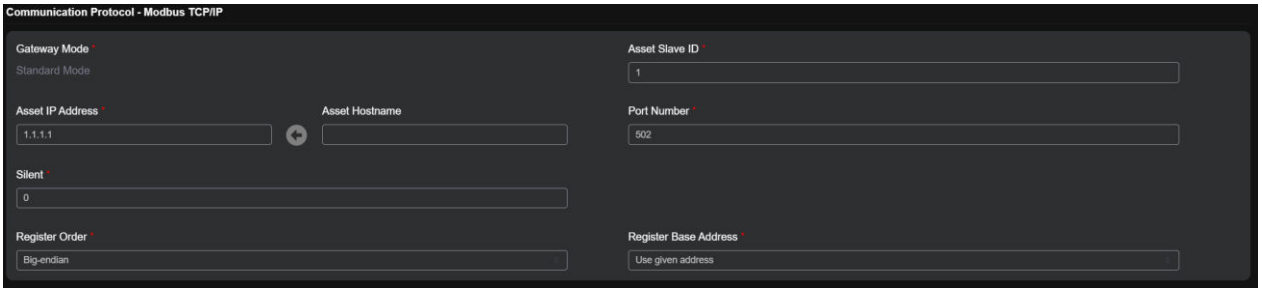


Figure 37: Protocole de communication – Modbus TCP/IP

- **Asset IP Address**
  Adresse IP du dispositif Modbus TCP.
- **Port Number**
  Port TCP utilisé pour les communications Modbus (la valeur par défaut est généralement 502, sauf si l'appareil utilise un port personnalisé).
- **Asset Unit ID / Slave ID**
  Identifiant d'unité utilisé par les appareils Modbus TCP servant de passerelle vers des réseaux Modbus RTU, ou lorsque l'appareil exige un identifiant d'unité spécifique.
  (Si non requis par l'appareil, cette valeur est généralement laissée à 1.)
- **Register Order**
  Définit l'ordre des octets/mots utilisé pour interpréter les valeurs multi-registres (Big-endian / Little-endian selon l'appareil).
- **Register Base Address**
  Définit la manière dont les adresses de registres sont interprétées (par exemple « Use given address » versus comportement d'offset).
  Cela doit correspondre au format d'adressage utilisé par la documentation de l'appareil et le gabarit sélectionné.

⚠️ **Note:** Pour Modbus TCP, s'assurer que l'appareil est atteignable depuis le réseau de l'iO et que le port Modbus est ouvert. Si la communication échoue, valider l'adresse IP/le port et confirmer que l'appareil est configuré comme serveur Modbus TCP.

Multitel

3.1.4 CONFIGURATION DU MOTEUR DU POLLING

La section Polling Engine Configuration définit la fréquence à laquelle l'iO lit les valeurs provenant de l'asset et comment il se comporte lorsque des problèmes de communication surviennent.

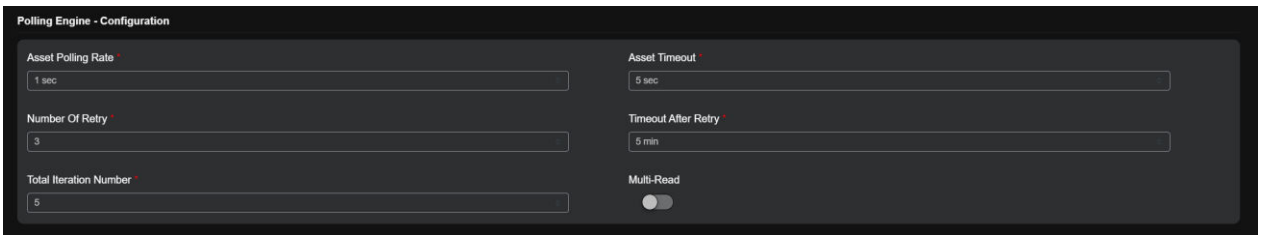


Figure 38: Moteur du polling – Configuration

- **Asset Polling Rate**
  Fréquence à laquelle l'iO effectue le polling de l'asset (par exemple : 1 sec). Un taux plus rapide augmente la réactivité, mais peut augmenter la charge réseau et CPU.
- **Asset Timeout**
  Temps maximal accordé à l'asset pour répondre à une requête de polling (ex. : cinq secondes).
- **Number Of Retry**
  Nombre de tentatives de reprise effectuées si une tentative de polling échoue (ex. : trois).
- **Timeout After Retry**
  Période d'attente après l'épuisement des tentatives avant de réessayer (exemple : cinq minutes).
- **Total Iteration Number**
  Number of consecutive polling iterations used by the acquisition engine for the asset (e.g., 5).
- **Multi-Read**
  Nombre d'itérations de polling consécutives utilisées par le moteur d'acquisition pour l'asset (ex. : 5).

Meilleure pratique: L'appareil iO prend en charge un taux d'acquisition maximal de 80 points de données par seconde (total pour l'ensemble de l'iO). Lors du choix du paramètre **Asset Polling Rate**, s'assurer que la charge de polling combinée de tous les assets et gabarits demeure sous cette limite. Dépasser 80 points de données par seconde peut rendre l'appareil très lent et, dans certains cas, non réactif.

3.1.5 LISTE D'ASSETS

Une fois qu'un asset est enregistré, il devient visible dans la liste des assets. Cette page est utilisée pour afficher les assets existants, effectuer une recherche/un filtrage et accéder aux actions telles que modifier ou supprimer.

La liste des assets fournit :
• Un filtre pour afficher les assets par type.
• Un tableau avec recherche affichant les informations clés pour chaque asset.
• Un accès rapide aux actions de l'asset via le menu Actions.

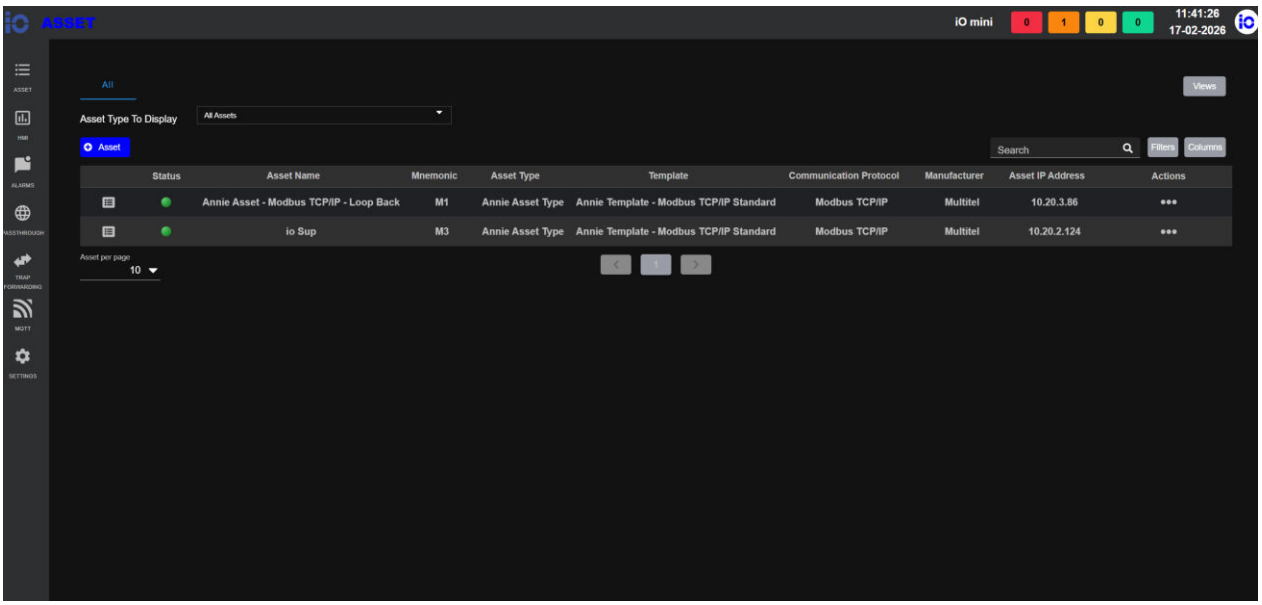


Figure 39: Liste des assets

3.1.5.1 Accéder à la liste des assets

Pour accéder à la liste des assets :

• Aller à Asset.
• La plateforme affiche la liste des assets existants pour le site courant.

3.1.5.2 Filtrer et rechercher des assets

Les outils suivants sont disponibles pour localiser rapidement des assets :

- **Asset Type to Display**
  Filtre déroulant utilisé pour afficher un sous-ensemble d'assets (par exemple : All Assets ou un type d'asset spécifique).
- **Search**
  Barre de recherche utilisée pour trouver des assets par mots-clés (par exemple : nom de l'asset, mnémonique, gabarit, protocole, adresse IP).
- **Filters**
  Ouvre des options de filtrage supplémentaires pour affiner les résultats affichés.
- **Columns**
  Permet d'afficher/masquer des colonnes du tableau selon l'information souhaitée.
- **Views**
  Fournit des vues de tableau prédéfinies (lorsqu'elles sont configurées) pour basculer rapidement entre différents agencements de colonnes/filtres.

3.1.5.3 Colonnes du tableau des assets

Chaque ligne représente un asset. Le tableau inclut les colonnes suivantes :

- **Status**
  Affiche l'état actuel de l'asset. Un indicateur vert confirme que l'asset est activé et actif.
- **Asset Name**
  Nom de l'asset.
- **Mnemonic**
  Identifiant court utilisé en interne et dans les gabarits (par exemple : M1, M3).
- **Asset Type**
  Catégorie d'asset sélectionnée lors de la création (par exemple : Annie Asset Type).
- **Template**
  Gabarit assigné à l'asset (par exemple : Annie Template – Modbus TCP/IP Standard).
- **Communication Protocol**
  Protocole utilisé pour l'acquisition (par exemple : Modbus TCP/IP).
- **Manufacturer**
  Fabricant associé à l'asset (par exemple : Multitel).
- **Asset IP Address**
  Adresse IP configurée pour l'asset (le cas échéant).
- **Actions**
  Ouvre le menu des actions (•••) pour l'asset sélectionné.

3.1.5.4 Actions sur les assets

Chaque asset inclut un menu Actions (•••) qui donne un accès rapide aux fonctions de gestion courantes. Lorsqu'une action d'asset est sélectionnée, la plateforme affiche le panneau Asset Options.

Les actions suivantes sont disponibles :

• **Data Points**
Ouvre la liste des points de données associés à l'asset sélectionné. Cette section est utilisée pour afficher les points surveillés créés par le gabarit assigné et pour valider les résultats d'acquisition.
• **Edit**
Ouvre le formulaire de création d'asset en mode édition afin de modifier la configuration de l'asset (par exemple : nom, gabarit, paramètres de communication, configuration de polling).
• **Delete**
Supprime définitivement l'asset du système. Une fois supprimés, l'asset et ses points de données associés ne sont plus disponibles. Utiliser cette option avec une attention particulière.

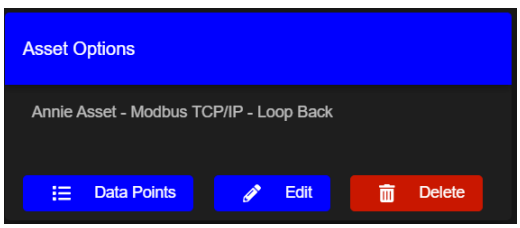


Figure 40: Actions sur les assets

3.1.5.5 Points de données de l'asset

Lorsque l'on clique sur **Data Points** dans le menu Asset Options, la plateforme ouvre la page **Data Points** pour l'asset sélectionné. Cette page est utilisée pour afficher et gérer les points de données associés à l'asset, ainsi que pour valider la communication en lisant les valeurs en temps réel.

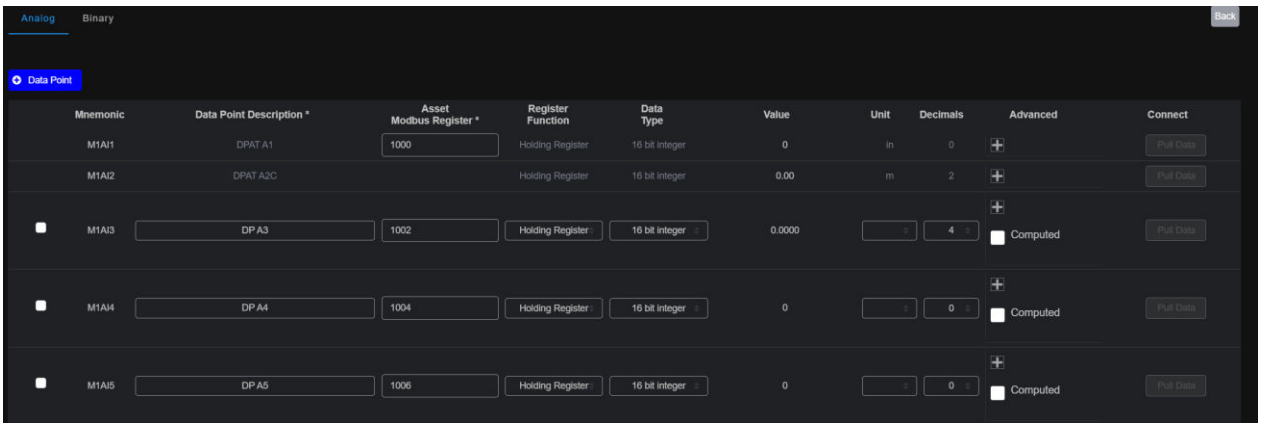


Figure 41: Points de données

La page **Data Points** est séparée en deux onglets :

- Analog
- Binary

Un bouton **Back** est disponible pour revenir à la liste des assets.

3.2 HMI

3.2.1 VUE D'ENSEMBLE HMI

Les fichiers HMI Views sont définis par l'utilisateur. Ils peuvent représenter une vue graphique de l'application spécifique de l'iO ou de toute autre application de site.

Les fichiers sont sélectionnés avec le menu déroulant **HMI Views**. Ces images contiennent des informations de télémétrie comme des valeurs analogiques avec unités, des statuts binaires, des boutons On/Off, etc. Plus d'un fichier image peut être chargé dans l'iO.

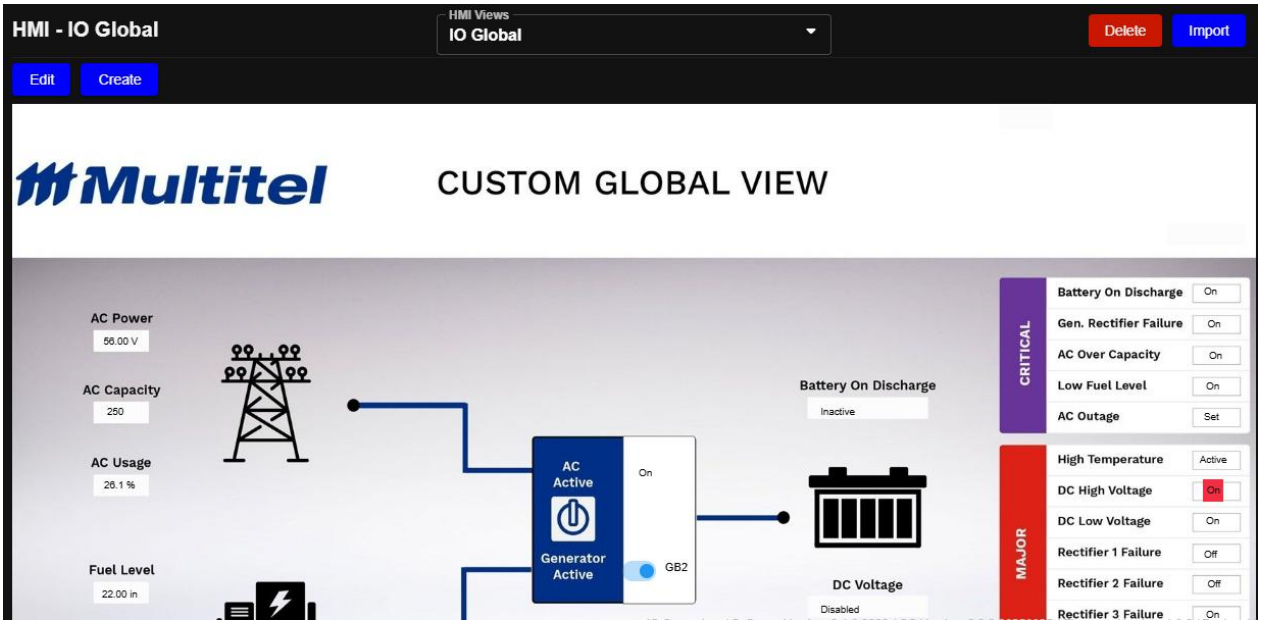


Figure 42: HMI

3.2.2 FONCTIONS HMI

3.2.2.1 Importation HMI

Pour importer un fichier HMI, cela peut être fait comme suit :
• Aller à HMI.
• Cliquer sur le bouton **Import**.
• Sélectionner un fichier HMI.

3.2.2.2 HMI Create

Pour créer un fichier HMI, cela peut être fait comme suit :
• Aller à HMI.
• Cliquer sur le bouton **Create**.

3.2.2.3 HMI Edit

Pour modifier un fichier HMI, cela peut être fait comme suit :
• Aller à HMI.
• Sélectionner le fichier HMI à modifier dans le menu déroulant **HMI Views**.
• Cliquer sur le bouton **Edit**.

3.2.2.4 HMI Delete

Pour supprimer un fichier HMI, cela peut être fait comme suit :
• Aller à HMI.
• Sélectionner le fichier HMI à supprimer dans le menu déroulant **HMI Views**.
• Cliquer sur le bouton **Delete**.

3.2.3 HMI CONFIGURATION

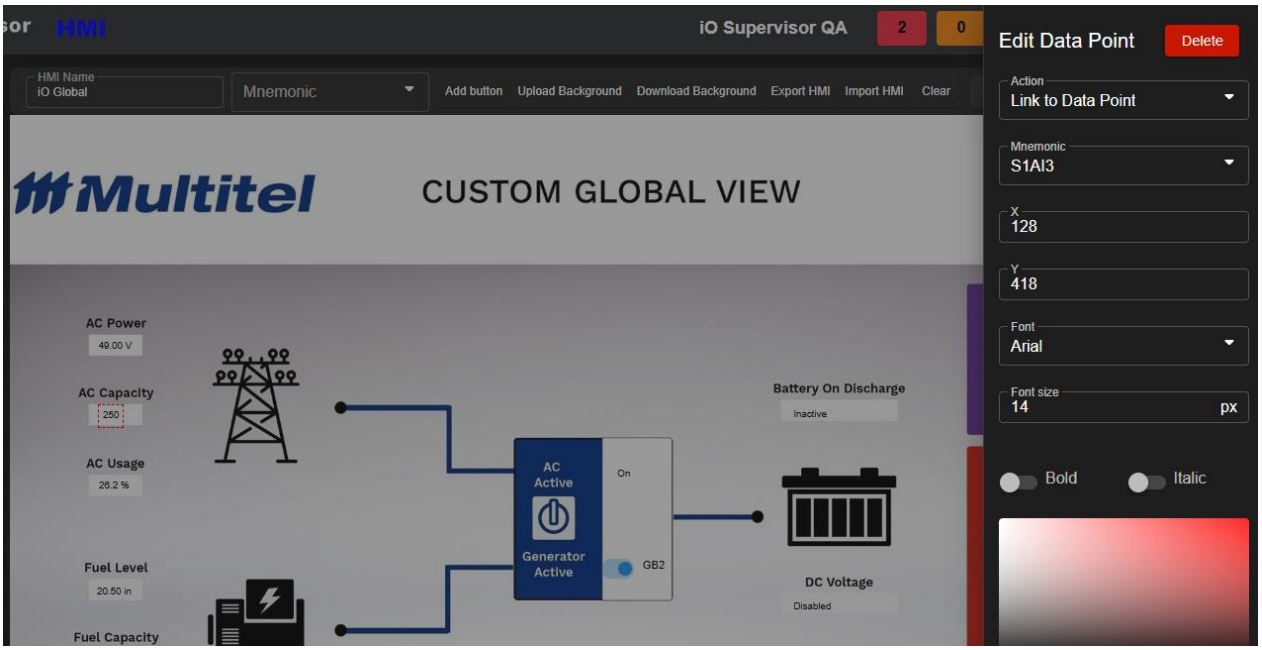


Figure 43: HMI - Configuration

Voici les actions possibles à la création ou à l'édition d'une vue HMI :
• Renommer l'HMI.
• Gérer les arrière-plans.
• Ajouter des points de données ou des boutons.
• Configurer les propriétés d'affichage.
• Personnaliser le style graphique.
• Exporter et importer une vue HMI.

3.2.3.1 Renommer HMI

La vue HMI actuelle peut être renommée en changeant son **Name** et en cliquant sur le bouton **Save**.

3.2.3.2 Gestion de l'arrière-plan

Des images d'arrière-plan peuvent être utilisées pour représenter des schémas techniques (par exemple schémas électriques, plans d'aménagement).
Le bouton **Upload Background** permet de téléverser une image d'arrière-plan.
Le bouton **Download Background** permet de télécharger l'arrière-plan actuel.

3.2.3.3 Ajouter un point de données

Multitel

Sélectionner un point de données dans le menu déroulant **Mnemonic** et cliquer sur le bouton **Add**.
Le nouveau point de données sera placé au centre de la vue HMI par défaut.

3.2.3.4 Ajouter un bouton

Cliquer sur le bouton **Add Button**. Le nouveau bouton sera placé au centre de la vue HMI par défaut.

3.2.3.5 Modifier un point de données ou un bouton

Cliquer sur un point de données ou un bouton existant pour ouvrir le panneau **Edit Data Point** (affiché sur le côté droit de l'écran).

Options pour le champ **Action** :

- **Link to Data Point** : en mode visualisation, cliquer sur le point de données affichera la page de visualisation des valeurs contenant le point spécifié dans *Mnemonic*.
- **Link to another HMI** : en mode visualisation, cliquer sur l'élément affichera l'HMI spécifiée.

Champs spécifiques aux boutons :
- **Button Label** : étiquette affichée sur le bouton
- **Width (px)** : largeur du bouton en pixels
- **Height (px)** : hauteur du bouton en pixels

Positionnement :

- **X** : position horizontale (gauche → droite)
- **Y** : position verticale (haut → bas)

Valeurs exprimées en pixels.

Position précise :

- Ajuster manuellement **X** et **Y** ou
- Utiliser le glisser-déposer

Style :
- **Font** : famille de police
- **Font size** : taille en pixels
- **Bold** : texte en gras
- **Italic** : texte en italique
- **Color Picket** : couleur du texte

3.2.3.6 Supprimer un point de données ou un bouton

Cliquer sur un point de données ou un bouton existant pour ouvrir le panneau **Edit Data Point**, puis cliquer sur **Delete** pour retirer l'élément de l'HMI.

Cliquer sur **Clear** pour supprimer tous les points de données et boutons de l'HMI.

3.2.3.7 Exporter / Importer une vue HMI

Une vue HMI peut être importée ou exportée en utilisant les boutons **Import HMI** et **Export HMI**.

3.3 PASSTHROUGH

Passthrough est un module iO autonome qui permet la communication basée sur IP entre un WAN et un LAN. À l'aide de ce module, l'iO peut être configuré comme un routeur.

3.3.1 VUE D'ENSEMBLE DU PASSTHROUGH

Le module Passthrough utilise le modèle client-serveur. Un client est un programme ou un appareil qui envoie une requête à un autre appareil ou programme pour accéder à un service mis à disposition par un serveur. Un exemple typique est un navigateur Web (client) envoyant une requête à un serveur Web pour accéder à des pages Web.

Contrairement à un modèle client-serveur hébergé sur le même réseau, le passthrough de l'iO est principalement utilisé pour rediriger des requêtes client d'un WAN vers un serveur sur un LAN. Les services hébergés sur un réseau local peuvent ainsi être accessibles de manière sécurisée sur un réseau étendu à l'aide de l'iO.

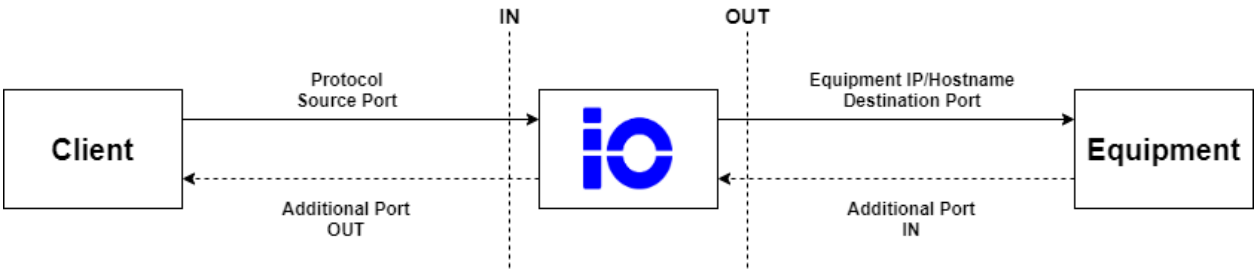


Figure 44: Topologie du passthrough

L'architecture Passthrough de l'iO est divisée en deux sections :

Client / dispositif iO Platform
L'utilisateur peut utiliser un client pour envoyer une requête à l'iO en fournissant les informations suivantes :
o Adresse IP de l'iO
o Protocole du serveur
o Port source

Dispositif iO Platform / équipement
Une fois le client configuré, l'iO redirigera les requêtes du client vers le serveur de l'équipement.

3.3.2 CONFIGURATION DU PASSTHROUGH

Pour configurer des passthroughs :

- Aller à **Passthrough**.
- Cliquer sur l'onglet **Passthrough**.
- Cliquer sur **+ Passthrough** pour créer un nouveau passthrough.

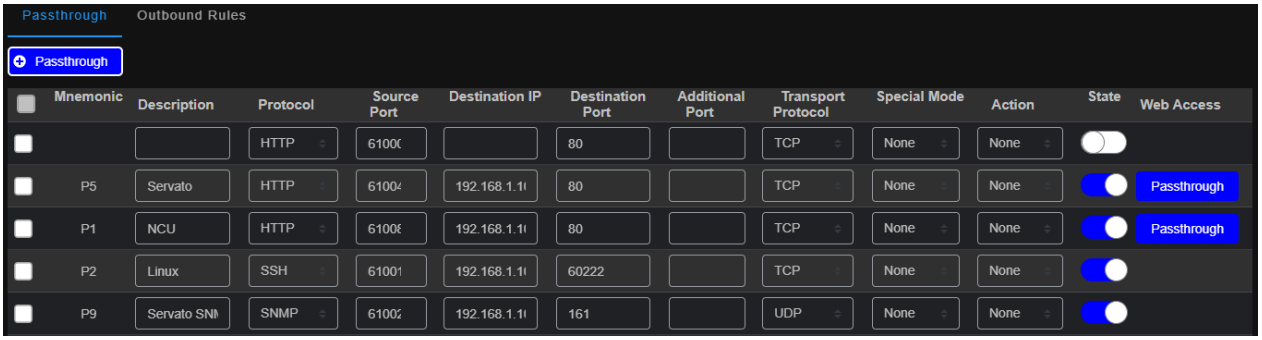


Figure 45: Configuration du passthrough

Les paramètres programmables sont listés ci-dessous :

Tableau 16: Passthrough – Configuration

Champ	Description	Spécification	Obligatoire
Mnemonic	Identifiant unique	Pxx – Auto Générer	
Description		1-50 caractères	Oui
Protocol		Liste déroulante: • SNMP • DNS • NTP • HTTP (Défault) • FTP • Telnet • Email • HTTPS • SFTP • SSH • SCP • Email-TLS • Email-SSH	Oui
Source Port		1 à 65535	Oui
Destination IP		0.0.0.0 à 255.255.255.255 ou hostname	Oui
Destination Port		1 à 65535	Oui
Additional Port	Permet d'ajouter plus de ports au passthrough	1 à 65 535 (Port interval is accepted)	Non
Transport Protocol		Liste déroulante: • TCP (Défault) • UDP	Oui

		• Les deux	
Special Mode		Liste déroulante: • None (Défault) • PBT WS 8081 • PBT WS 80 • HTTPS Proxy	Oui
Action		Liste déroulante: • None (Default) • IN • Passthrough	Oui
State	Permet d'activer et de désactiver le passthrough	Toggle	Oui
Web Access	Le bouton **Passthrough** est affiché uniquement lorsque les protocoles **HTTP** ou **HTTPS** sont activés. Cliquer sur le bouton ouvre l'interface Web de l'équipement.	Bouton	

Les valeurs par défaut pour Port et Transport dépendent du protocole sélectionné.

Tableau 17: Passthrough – Protocoles et Ports

Protocole	Description	Port par défaut	Transport par défaut
Protocole de communication			
SNMP	Protocole de gestion de réseau.	161	UDP
Protocole non sécurisé			
HTTP	Le protocole Hypertext Transfer Protocol est utilisé comme communication Internet.	80	TCP
FTP	Le protocole File Transfer Protocol est utilisé pour transférer des fichiers vers un autre appareil.	21	TCP
Telnet	Le réseau de télécommunication est utilisé pour se connecter à un hôte TCP/IP afin d'accéder à d'autres hôtes sur le réseau.	23	TCP
Email	Protocole de courriel non chiffré	25	TCP
Protocole sécurisé			
HTTPS	Le protocole Hypertext Transfer Protocol Secure est utilisé comme communication Internet.	443	TCP
SFTP	Le protocole Secure File Transfer Protocol est utilisé pour transférer un fichier vers un autre appareil avec des composants de sécurité.	22	TCP
SSH	Le protocole Secure Shell est utilisé pour exécuter des commandes dans un appareil distant et déplacer des fichiers d'un appareil à un autre.	22	TCP
SCP	Le protocole Secure Copy Protocol est utilisé pour transférer des fichiers en toute sécurité d'un hôte local vers un hôte distant.	22	TCP
Email-TLS	Transmission de courriel sécurisée utilisant TLS.	587	TCP
Email-SSL	Transmission de courriel sécurisée utilisant SSL.	465	TCP

3.3.2.1 Options du port source

Le port source est généré automatiquement selon les spécifications ci-dessous. Si nécessaire, cela peut être modifié par les utilisateurs. Le port source doit être unique et compris entre 1 et 65 535.

Tableau 18: Passthrough – Options du port source

Nom du protocole	Spécifications
HTTP/HTTPS	61 000 à 61 999
FTP/SFTP/SCP	62 000 à 62 999
Telnet/SSH	63 000 à 63 999
Email	65 000 à 65535

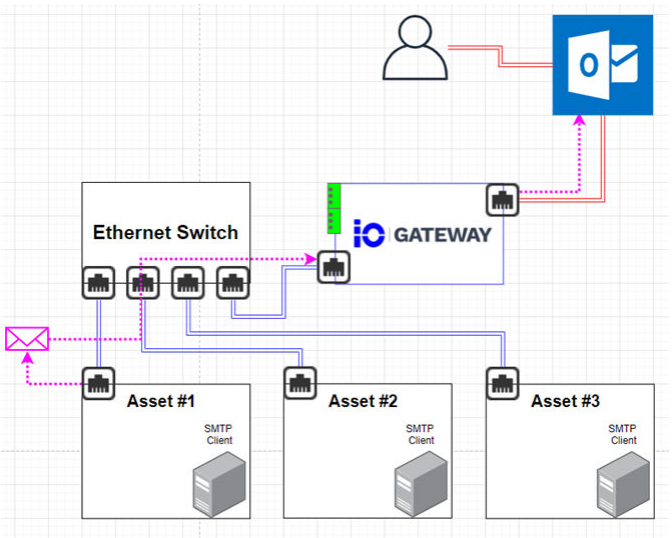
3.3.2.2 *Passthrough Email Forwarding*

L'email peut maintenant être transféré directement via l'iO.

La fonction d'email passthrough prend en charge trois options :

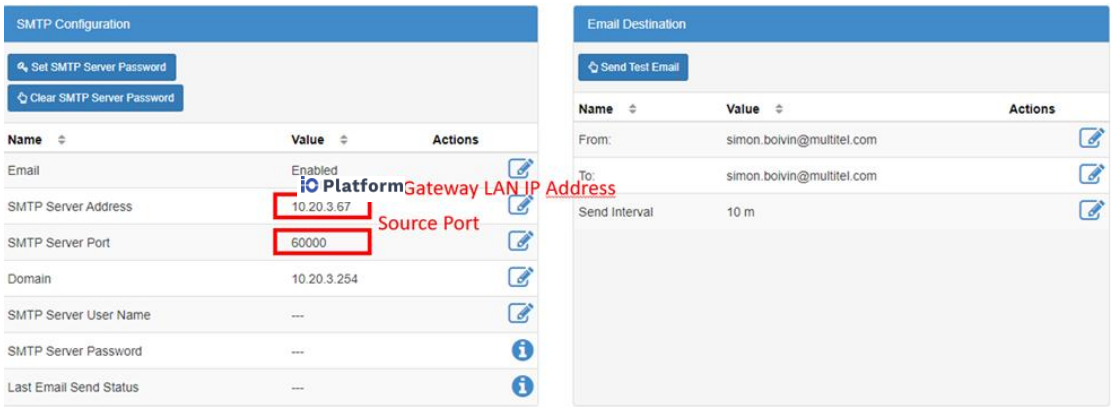
- Email (non sécurisé)
- Email-TLS (sécurisé)
- Email-SSL (sécurisé)

Le **port source** est le port du serveur SMTP qui doit être configuré dans l'appareil. Le **port de destination** est le port utilisé pour envoyer l'email au serveur SMTP de l'utilisateur.
La figure ci-dessous représente l'architecture de transfert d'email utilisant le service passthrough.

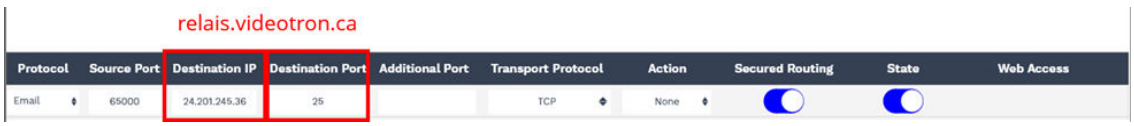


Le passthrough n'ouvre que les ports entre l'asset et le serveur SMTP de l'utilisateur ; il n'y a aucune manipulation, aucune couche de sécurité ajoutée, ni aucun journal.

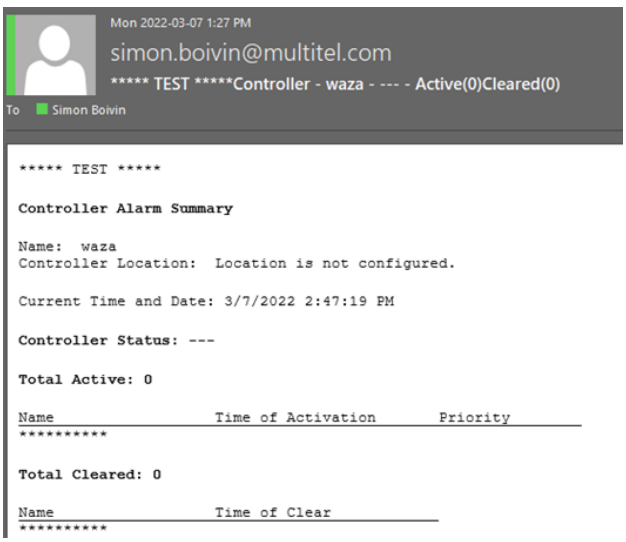
Pour configurer le Passthrough Email Forwarding :
• Configurer le serveur SMTP et le port du serveur de l'appareil.



• Configurer le passthrough de l'appareil iO.



• Courriel reçu



3.3.3 VUE D'ENSEMBLE DES OUTBOUND RULES

Les règles sortantes font partie des configurations de pare-feu ou de groupes de sécurité réseau. Elles définissent les permissions pour les connexions sortantes depuis une machine ou un réseau. Ces règles spécifient quels types de trafic sont autorisés à quitter un système ou une infrastructure.

La **direction du trafic** des règles sortantes, contrairement aux règles entrantes qui contrôlent les connexions entrantes, régule le trafic sortant de l'iO (par exemple, un serveur ou une instance cloud) vers une destination externe.

3.3.4 CONFIGURATION DES OUTBOUND RULES

Pour configurer des passthroughs, suivre les étapes suivantes :

• Aller à **Passthrough**.
• Cliquer sur l'onglet **Outbound Rules**.
• Cliquer sur **+ Outbound Rule** pour créer une nouvelle règle sortante.

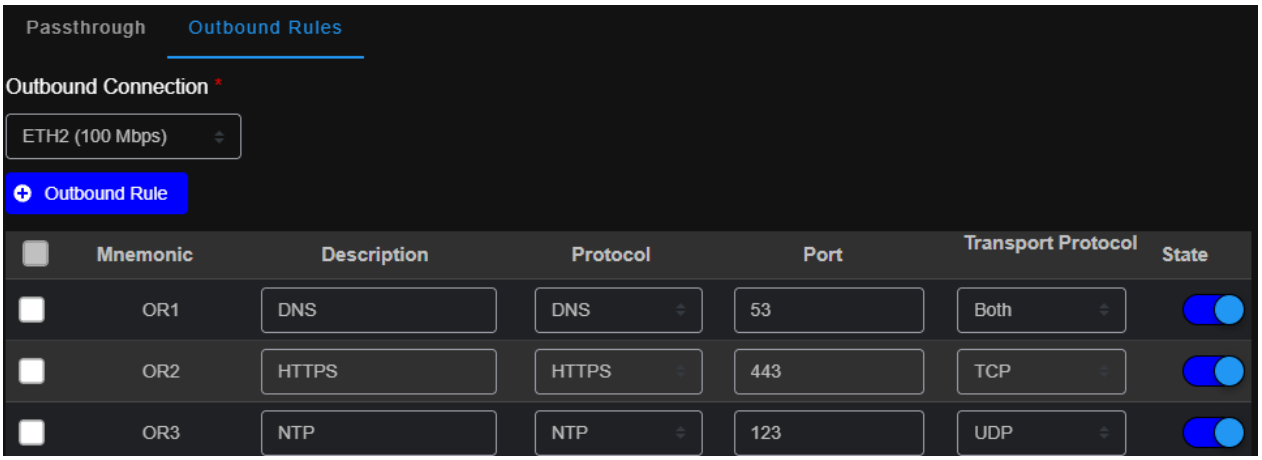


Figure 46: Outbound Rules – Configuration

Tableau 19: Outbound Rules - Configuration

Champs	Description	Spécification	Obligatoire
Mnemonic	Identifiant unique	ORxx – Auto Générer	
Description	Description	1 à 50 caractères	Oui
Protocol	Protocole	Liste déroulante: • SNMP • DNS • NTP • HTTP (Défault) • FTP • Telnet • Email • HTTPS • SFTP • SSH • SCP • Email-TLS • Email-SSH	Oui

Port	Le port est généré automatiquement selon le protocole sélectionné. Si nécessaire, l'utilisateur peut le modifier.	1 à 65535	Oui
Transport Protocol	Protocole de transport	Liste déroulante: • TCP • UDP • Both	Oui
State	Permet d'activer et de désactiver la règle sortante.	Dongle	Oui

Les valeurs par défaut pour Port et Transport dépendent du protocole sélectionné.

Tableau 20: Outbound Rules – Protocols and Ports

Protocole	Description	Port par défaut	Transport par défaut
Protocole de communication			
SNMP	Protocole de gestion de réseau.	161	UDP
DNS	Protocole de résolution de noms de domaine.	53	Both
NTP	Protocole de synchronisation temporelle réseau.	123	UDP
Protocole non sécurisé			
HTTP	Le protocole Hypertext Transfer Protocol est utilisé comme communication Internet.	80	TCP
FTP	Le protocole File Transfer Protocol est utilisé pour transférer des fichiers vers un autre appareil.	21	TCP
Telnet	Le réseau de télécommunication est utilisé pour se connecter à un hôte TCP/IP afin d'accéder à d'autres hôtes sur le réseau.	23	TCP
Email	Protocole de courriel non chiffré.	25	TCP
Protocole sécurisé			
HTTPS	Le protocole Hypertext Transfer Protocol Secure est utilisé comme communication Internet.	443	TCP
SFTP	Le protocole Secure File Transfer Protocol est utilisé pour transférer un fichier vers un autre appareil avec des composants de sécurité.	22	TCP
SSH	Le protocole Secure Shell est utilisé pour exécuter des commandes dans un appareil distant et déplacer des fichiers d'un appareil à un autre.	22	TCP
SCP	Le protocole Secure Copy Protocol est utilisé pour transférer des fichiers en toute sécurité d'un hôte local vers un hôte distant.	22	TCP
Email-TLS	Transmission de courriel sécurisée utilisant TLS.	587	TCP
Email-SSL	Transmission de courriel sécurisée utilisant SSL.	465	TCP

3.4 RENVOI DES TRAPS

3.4.1 VUE D'ENSEMBLE DE RENVOI DES TRAPS

Le module SNMP Trap Forwarding permet au système de recevoir et de transférer des traps vers une ou plusieurs destinations.

Il existe deux types de traps pris en charge par l'iO.

Tableau 21: Type de trap SNMP

Type	Description
Trap -- Unacknowledged	Le trap sera transféré et l'appareil ne sera pas informé que le trap a été reçu par l'application distante.
Trap -- Acknowledged	Le trap sera transféré à la destination et l'appareil iO attendra une confirmation de la réception. Le trap-acknowledge sera envoyé continuellement selon les paramètres de notification jusqu'à ce que la destination envoie un accusé de réception à l'appareil ou que le nombre de tentatives demandé soit atteint.

3.4.2 VUE D'ENSEMBLE DES SOURCES DE TRAP

L'onglet **trap forwarding sources** permet aux utilisateurs de configurer un nombre illimité de sources de trap et de spécifier leurs destinations.

NOTE

Il n'y a pas de limite stricte au nombre de sources de trap forwarding, mais Multitel recommande une limite de **50 sources** pour optimiser la performance.

****Au moins une destination de Trap Forwarding doit être créée avant d'ajouter une source d'équipement. Pour créer une destination, se référer à la section Trap Forwarding Destination ci-dessous.**

3.4.3 CONFIGURATION DES SOURCES TRAP

Pour configurer une source de trap, suivre les étapes suivantes :

- Aller à **Trap Forwarding**.
- Cliquer sur l'onglet **Sources**.
- Cliquer sur **+ Source** pour créer une nouvelle source de trap.

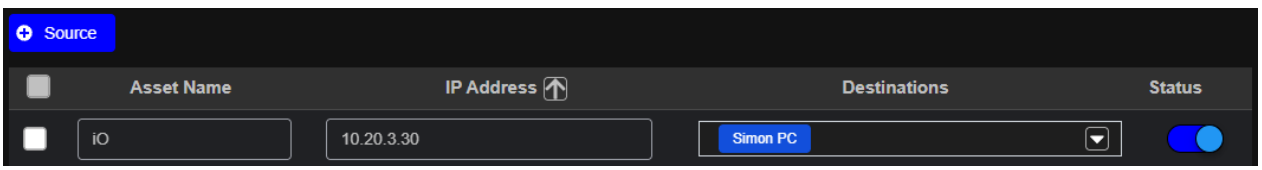


Figure 47: Sources des traps – Configuration

Multitel

Tableau 22: Sources de trap– Configuration

Champ	Description	Spécification	Obligatoire
Asset Name	Le nom de l'asset est utilisé pour indiquer la source d'un trap transféré.	1 à 50 caractères	Oui
IP Address	Adresse IP ou nom de domaine de la source de l'asset.	0.0.0.0 à 255.255.255.255	Oui
Destinations	La destination indique où les traps reçus doivent être transférés. Plusieurs destinations peuvent être sélectionnées.	Dropdown: List of trap destinations	Oui
Status	Le statut permet d'activer ou de désactiver une source. Une source désactivée arrête la communication entre la source et l'appareil iO.	Dongle	

3.4.4 VUE D'ENSEMBLE DES DESTINATIONS DE TRAP

La destination de trap forwarding permet aux utilisateurs de configurer jusqu'à dix (10) destinations vers lesquelles l'appareil iO peut transférer les traps reçus. Les destinations de trap sont communes aux notifications et au trap forwarding.

Chaque destination peut recevoir un transfert de trap SNMP ou des notifications basées sur des activités d'alarmes ou d'événements. Le tableau permet aux utilisateurs de configurer les paramètres clés pour chaque récepteur SNMP, y compris l'adressage, la version du protocole et le comportement de notification.

3.4.5 CONFIGURATION DES DESTINATIONS DE TRAP

Pour configurer une destination de trap :

- Aller à **Trap Forwarding**.
- Cliquer sur l'onglet **Trap Destinations**.
- Cliquer sur **+ Destination** pour créer une nouvelle destination de trap.

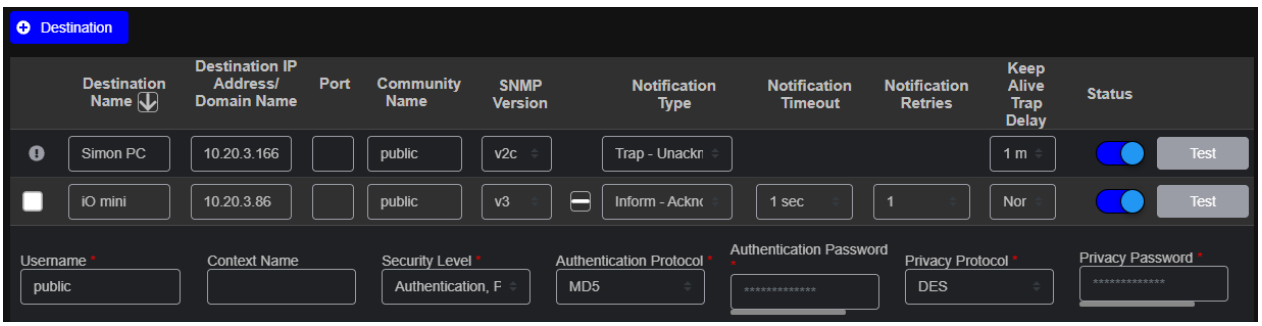


Figure 48: Destinations de trap – Configuration

Multitel

Chaque ligne représente une destination pouvant recevoir des notifications de traps SNMP basées sur des activités d'alarmes ou d'événements. Le tableau permet aux utilisateurs de configurer les paramètres clés pour chaque récepteur SNMP, incluant l'adressage, la version du protocole et le comportement de notification.

Tableau 23: Destinations de trap – Configuration

Champ	Description	Spécification	Obligatoire
Destination Name	Le nom de l'asset est utilisé pour indiquer la source d'un trap transféré.	1 à 50 caractères	Oui
Destination IP Address/ Domain Name	Adresse IP ou nom de domaine du récepteur SNMP trap distant.	0.0.0.0 à 255.255.255.255	Oui
Port	Le numéro de port UDP utilisé pour envoyer des traps SNMP.	1 à 65 535 162 (Défault)	Oui
Community Name	La chaîne de communauté SNMP utilisée pour l'authentification (s'applique uniquement à SNMP v2c).	public ou privé	Oui
SNMP Version	La version du protocole SNMP utilisée pour communiquer avec la destination.	Liste déroulante: • v2c • v3	Oui
Notification Type	**Trap – Unacknowledged**: une alerte unidirectionnelle de base sans confirmation. **Inform – Acknowledged**: un type de message plus fiable qui nécessite un accusé de réception du récepteur.	Liste déroulante: • Trap • Inform	Oui
Notification Timeout	Durée pendant laquelle le système attend un accusé de réception avant de réessayer ou de marquer la notification comme échouée.	Liste déroulante: • 1 sec • 5 sec • 10 sec • 1 min	Oui
Notification Retries	Nombre de fois que le système réessaiera d'envoyer le trap si aucun accusé de réception n'est reçu.	Liste déroulante: 1 à 5	Oui – Inform
Keep Alive Trap Delay	Intervalle de délai optionnel pour envoyer des traps « keep-alive » périodiques afin de confirmer la connectivité.	Liste déroulante: • None • 1 min • 15 min • 30 min • 60 min	Oui – Inform
Status	Activer ou désactiver cette destination SNMP trap.	Toggle	
SNMP v3			
Username	Le nom d'utilisateur utilisé pour l'authentification.	1 à 50 caractères	Oui
Context Name	Nom pour distinguer un agent spécifique.	1 à 50 caractères	Non
Security Level	Niveau de sécurité.	Liste déroulante: • No authentication,	Oui

		No privacy (Aucune authentification, Aucune confidentialité) • Authentication, No privacy (Authentification, Aucune confidentialité) • Authentication, Privacy (Authentification, Confidentialité)	
Authentication Protocol	Protocole d'authentification.	Liste déroulante: • MD5 • SHA1	Non/Oui
Authentication Password	Mot de passe d'authentification.	Chaîne	Non/ Oui
Privacy Protocol	Protocole de confidentialité.	Liste déroulante: • DES • AES	Non/ Oui
Privacy Password	Mot de passe de confidentialité.	Chaîne	Non/ Oui

3.4.5.1 Test d'envoi de trap

Un test d'envoi de trap est utilisé pour envoyer une trap de test à la demande afin de valider la communication entre l'appareil iO et la destination.

3.4.5.2 Trap Keep-Alive

Une trap keep-alive est utilisé pour indiquer à la destination, de manière périodique, que l'appareil iO est toujours actif.

Une trap keep-alive est toujours une trap sans accusé de réception (unacknowledged) et le délai est configuré individuellement pour chaque destination.

3.4.6 JOUNAL DE LOGS

L'appareil iO enregistre toutes les traps reçues, transférées et envoyées par le bouton de trap keep-alive ou de test.

Pour réduire les journaux inutiles, les traps reconnues (Inform) avec plusieurs tentatives seront représentées par une seule ligne dans le fichier de journal.

Le journal des traps peut être exporté uniquement en fichier **.CSV**.

Voici les informations contenues dans le fichier de journal :

- **Date et heure de l'appareil iO**

Le timestamp est basé sur la configuration de date et d'heure de l'appareil. Pour assurer un enregistrement correct, veuillez configurer la date et l'heure avec précision.

- **La date et l'heure locale de l'utilisateur**

Le timestamp est basé sur la configuration de date et d'heure de l'ordinateur de l'utilisateur.

- **Adresse IP de la source ou de la destination**
- **Numéro de port**
- **OID**
- **Community Name**
- **SNMP Version**
- **Trap Type**
- **Message**

Tableau 24: Message du journal des traps

Type de message	Description
Received has been sent	Fait référence à un trap reçu par l'appareil.
Forwarded has been sent	Fait référence à un trap reçu et transféré à une destination.
Keep Alive has been sent	Fait référence à un trap keep-alive.
Test Trap has been sent	Fait référence à un trap déclenché par le bouton Test trap.
Forwarded as inform and received response	Fait référence à un trap – acknowledge lorsque la destination envoie un trap d'accusé de réception.
Forwarded as inform but received no response	Fait référence à un trap – acknowledge lorsque la destination n'envoie pas de trap d'accusé de réception.
Error sending test trap: SPECIFIC MESSAGE	Indique que le trap n'a pas été reçu ou transféré avec succès. Pour aider à diagnostiquer le problème, le message sera ajusté afin de fournir des précisions sur le problème.

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: Journal de traps – Exemple

3.4.6.1 La période des journaux (Log)

Le **period log** est géré automatiquement par l'appareil iO. L'appareil créera automatiquement une nouvelle période si l'une des deux conditions suivantes est remplie :

- S'il y a plus de **25 000 lignes** dans le fichier Excel
- Si la taille du fichier Excel est supérieure à **200 Gbit**

Pour garantir des performances optimales, l'appareil iO ne conservera que l'enregistrement de **quatre (4) périodes**. Si davantage de périodes sont créées, l'appareil supprimera automatiquement la plus ancienne.

3.5 MQTT

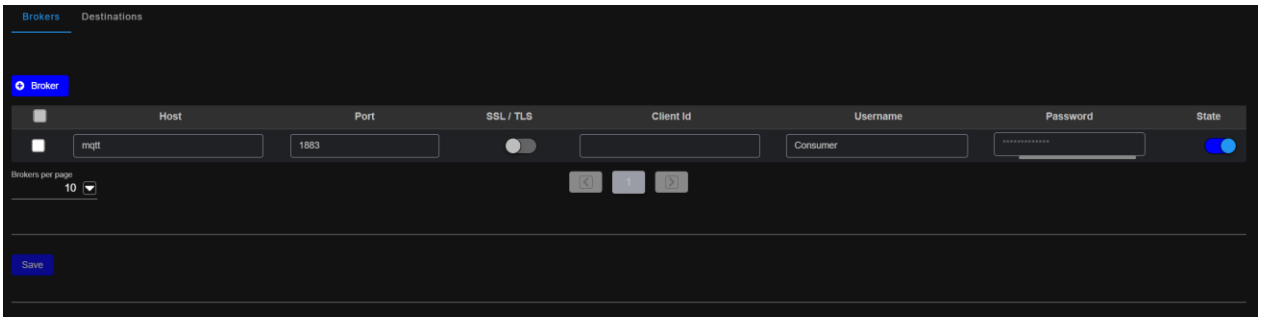
Multitel

Le module MQTT permet à l'appareil iO de publier des données vers un broker MQTT externe. La configuration est divisée en deux onglets :

- **Brokers** – Configurer la connexion au serveur MQTT (hôte, port, authentification, TLS).
- **Destinations** – Configurer l'emplacement de publication (topic, QoS, périmètre de l'asset) et définir le contenu du message à l'aide d'un script Lua.

3.5.1 BROKERS

L'onglet **Brokers** est utilisé pour créer et gérer les connexions aux brokers MQTT. Chaque ligne représente une configuration de broker.



Pour ajouter ou modifier un broker, suivre les étapes suivantes :

- Aller à **Settings**.
- Aller à **MQTT**.
- Sélectionner l'onglet **Brokers**.
- Cliquer sur **+ Broker**.
- Configurer les paramètres du broker.
- Cliquer sur **Save**.

Champs du broker

- **Host**
  Nom d'hôte ou adresse IP du broker.
- **Port**
  Port du broker (exemple montré : 1883).
- **SSL / TLS**
  Bascule pour activer/désactiver TLS. Lorsqu'il est activé, les champs de certificats sont affichés.
- **Client Id**
  Identifiant client MQTT utilisé pour identifier la connexion de l'iO auprès du broker.
- **Username**
  Nom d'utilisateur utilisé pour l'authentification auprès du broker.
- **Password**
  Mot de passe utilisé pour l'authentification auprès du broker.
- **State**
  Bascule utilisée pour activer/désactiver la configuration du broker.

3.5.1.1 *Certificat TLS*

Lorsque SSL/TLS est activé, des champs supplémentaires sont affichés pour la configuration des certificats :

- **Certificate Authority**
  Certificat CA (PEM) utilisé pour valider le certificat du broker.
- **Client Certificate**
  Certificat client (PEM) utilisé pour l'authentification TLS mutuelle lorsque requis par le broker.
- **Client Key**
  Clé privée du client (PEM) associée au certificat client.

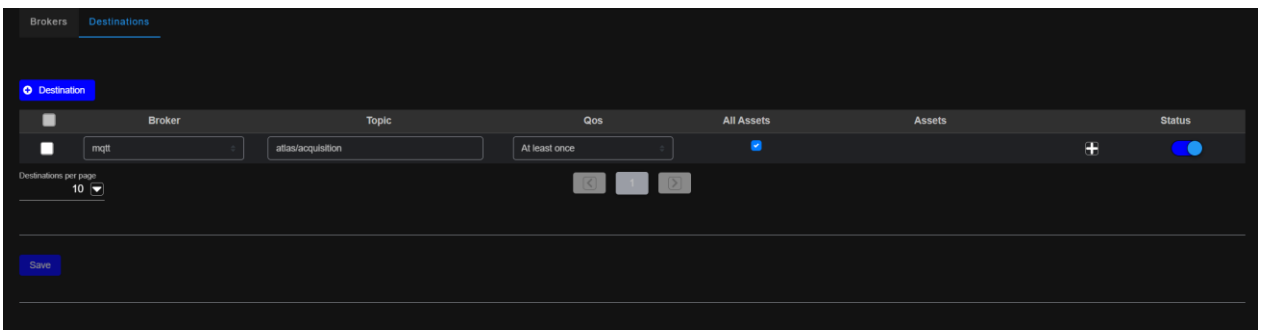
⚠️ **Note:** Les exigences TLS dépendent de la configuration du broker. Certains brokers requièrent uniquement le Certificate Authority, alors que d'autres exigent un TLS mutuel (Client Certificate + Client Key).

3.5.2 DESTINATIONS

L'onglet **Destinations** définit les règles de publication : quel broker utiliser, quel topic publier, le niveau QoS, et quels assets sont inclus.

Pour ajouter ou modifier une destination, suivre les étapes suivantes :

- Aller à **Settings**.
- Aller à **MQTT**.
- Sélectionner l'onglet **Destinations**.
- Cliquer sur **+ Destination**.
- Configurer les paramètres de la destination.
- Cliquer sur **Save**.



- **Broker**
  Sélectionner la configuration du broker à utiliser.
- **Topic**
  Topic MQTT utilisé pour la publication.
- **QoS**
  Niveau de Quality of Service

- **All Assets**
  Lorsqu'il est activé, les données sont publiées pour tous les assets.
- **Assets**
  Utilisé lorsque *All Assets* est désactivé pour sélectionner un sous-ensemble d'assets.
- **Status**
  Bascule pour activer/désactiver la destination.

3.5.3 PAYLOAD

Chaque destination inclut une zone **Script** utilisée pour générer le payload qui sera publié sur le topic configuré.

Le script construit généralement un payload structuré (souvent JSON) et retourne le contenu final du message.

Script Area

- **Test Mnemonic**
  Champ utilisé pour sélectionner ou saisir un mnémonique afin de tester l'exécution du script.
- **Run (▶)**
  Exécute le script en utilisant le mnémonique sélectionné.
- **Reset (↺)**
  Réinitialise le script à son état précédent/par défaut (lorsque applicable).
- **Delete (🗑)**
  Efface le contenu actuel du script (lorsque applicable).

Output Area

- Affiche le résultat de l'exécution du script.
- Inclut un contrôle **CLEAR** pour réinitialiser l'affichage du résultat.

⚠ **Note:** Le script doit retourner le contenu à publier (exemple : texte JSON).
Si la sortie est vide ou inattendue, valider le mnémonique utilisé pour le test et confirmer la syntaxe du script.

4. PARAMÈTRES IO

4.1 CONNEXIONS

La page Connections est accessible depuis le module Settings.

Figure 50: Paramètres – Connexions

⚠ **Note:**
Ces paramètres nécessitent une compréhension de la gestion de réseau et des protocoles basés sur série. Ce guide d'utilisateur ne fournit pas un guide complet étape par étape pour la communication réseau et série, et suppose que le lecteur est déjà familier avec ces deux sujets.

4.1.1 ETHERNET CONFIGURATION

Selon le modèle, l'appareil iO offre un ou deux ports Ethernet. **ETH-1** est un port natif **1 Gbps** et **ETH-2** est un **100 Mbps**.
Les deux ports peuvent être configurés à l'aide des paramètres suivants :

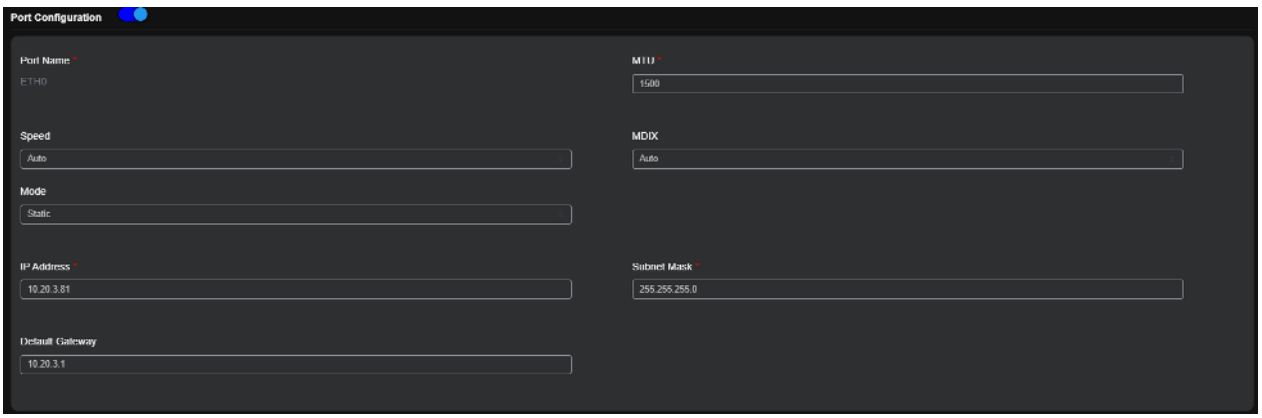


Figure 51: Connexions – Ports ethernet

Tableau 25: Ports ethernet -- Configuration

Champ	Description	Spécification	Obligatoire
Port Name	**Nom du port Ethernet en cours de configuration.**	ETH-1: 1Gbps ETH-2: 100Mbps	Oui
MTU	**Maximum Transmission Unit – la taille du plus grand paquet pouvant être envoyé.**	Défaut: 1500	Oui
Speed	**Définit le débit de données du port.**	Liste déroulante:	Oui

		• Auto • 10Mbps • 100Mbps • 1Gbps	
MDIX	**Contrôle l'inversion automatique du type de câble Ethernet.**	Liste déroulante: • Auto • On • Off	Oui
Mode	**Définit la façon dont l'adresse IP est attribuée.**	Liste déroulante: • Static • DHCP	Oui
IP Address	**L'adresse IP attribuée au port.**	0.0.0.0 à 255.255.255.255	Oui
Subnet Mask	**Identifie la partie réseau et la partie hôte de l'adresse IP.**	0.0.0.0 à 255.255.255.255	Oui
Default Gateway	**Adresse IP de la passerelle utilisée pour l'accès au réseau externe.**	0.0.0.0 à 255.255.255.255	Oui

Les serveurs DNS peuvent également être configurés pour permettre l'utilisation de noms d'hôte dans certains paramètres. L'iO permet la configuration de deux serveurs distincts afin d'améliorer la redondance.

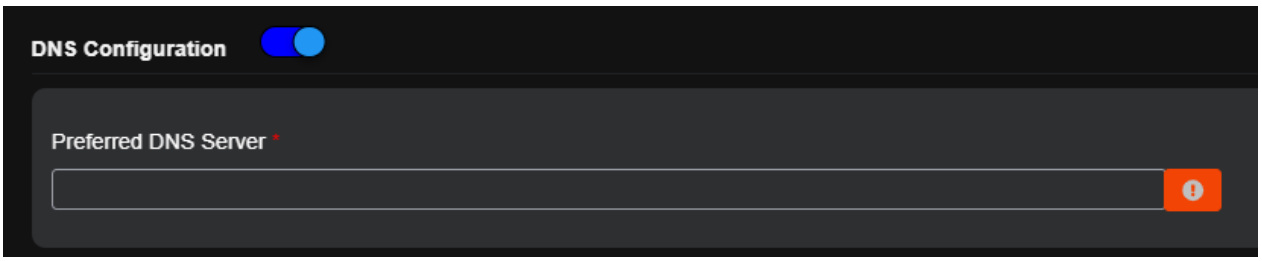


Figure 52: Configuration DNS

4.1.2 CONFIGURATION PORT RS-485

Selon le modèle, l'appareil iO offre un ou deux ports RS-485. Ces ports peuvent être configurés à l'aide des paramètres suivants :

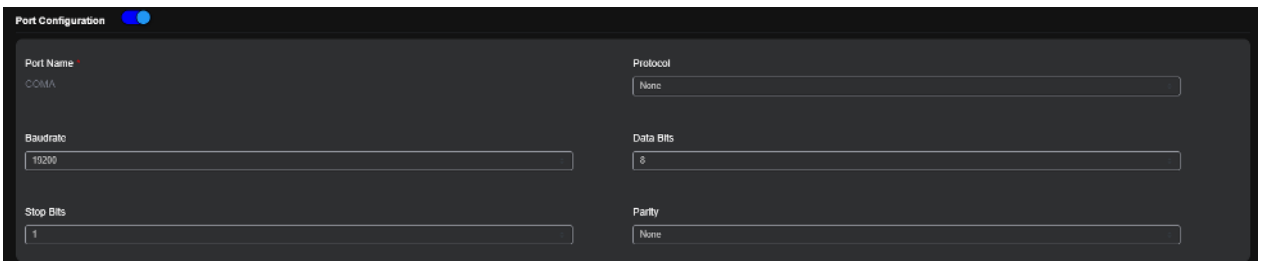


Figure 53: Connexions – RS-485

Multitel

Tableau 26: RS-485 -- Configuration

Champ	Description	Spécification	Obligatoire
Port Name	**Identifiant du port de communication série.**	COMA COMB	Oui
Protocol	**Protocole de communication utilisé sur le RS-485.**	Liste déroulante: • None (Aucun) • Modbus RTU – Slave • Modbus RTU - Master	Oui
Baudrate	**Vitesse de communication (en bits par seconde).**	Liste déroulante: • 300 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 115200	Oui
Data Bits	**Nombre de bits de données dans chaque caractère/trame.**	Liste déroulante: • 6 • 7 • 8	Oui
Stop Bits	**Nombre de bits d'arrêt utilisés pour signaler la fin d'un caractère.**	Liste déroulante: • 1 • 2	Oui
Parity	**Méthode de vérification d'erreur pour la transmission.**	Liste déroulante: • None • Odd • Even	Oui

4.2 INVENTAIRE

Les paramètres Inventory sont accessibles depuis le module Settings.

Figure 54: Paramètres -- Inventaire

4.2.1 CONFIGURATION DU SITE

Voici une liste des sites configurés sur l'iO. Les sites sont utilisés pour regrouper des assets. L'asset principal (cet appareil) ne peut pas être supprimé, seulement modifié.

⚠ **Note:**
La configuration des sites doit être utilisée uniquement lorsque l'iO agit comme un **iO Manager**, où plusieurs sites peuvent être créés et gérés. Pour un appareil iO autonome, sauter la configuration des sites.

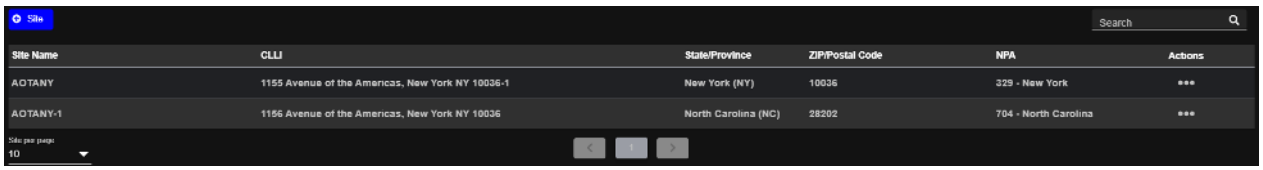


Figure 55: Inventaire – Sites

Pour créer un nouveau site, l'utilisateur doit cliquer sur + Site.

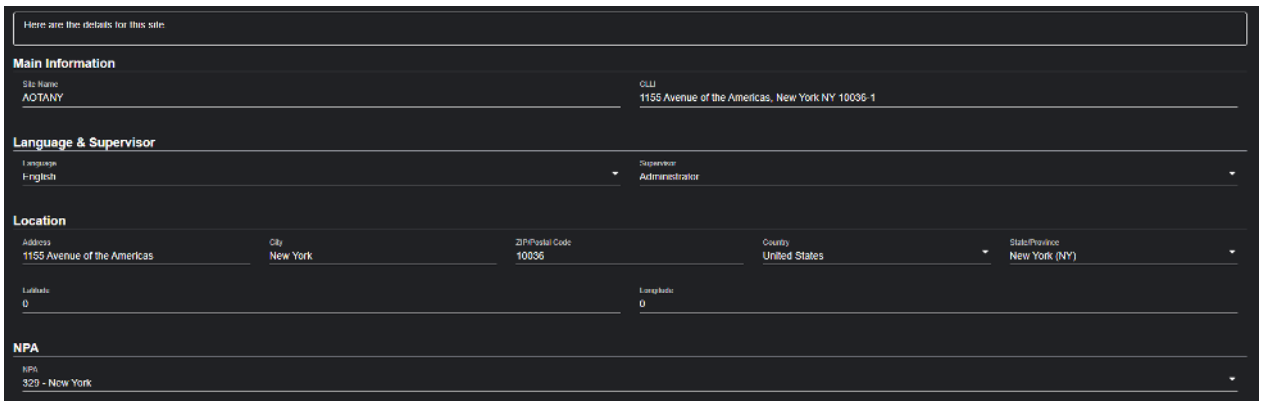


Figure 56: Inventaire – Création du site

La création d'un site est divisée en quatre sections.

4.2.1.1 *Information principale*

La section **Main Information** inclut le **Site Name** et le **code CLLI**, qui identifient de manière unique chaque emplacement du réseau de télécommunications.

4.2.1.2 *Language And Supervisor*

Cette section couvre la langue d'affichage de l'iO. Veuillez noter que seule l'anglais est actuellement pris en charge.

4.2.1.3 *Location*

Cette section couvre les paramètres de localisation physique pour l'iO.

4.2.1.4 NPA

Cette section est utilisée pour configurer le **NPA** de l'emplacement de l'iO.

4.2.2 CONFIGURATION DU TYPE D'ASSET

Un type d'asset identifie l'endroit où les points de données peuvent être liés. Cela correspond à une catégorie d'équipement, telle que les systèmes DC, les batteries, les générateurs ou les systèmes CVC (HVAC). L'objectif d'un type d'asset est de normaliser la nomenclature et la configuration des points de données, tandis que les types d'asset sont également utilisés pour regrouper les gabarits (templates).

Figure 57: Inventaire – Types d'asset

4.2.2.1 Tous les assets

Le type d'asset par défaut disponible sur un appareil iO s'appelle **« All Assets »**. Il regroupe tous les autres types d'assets afin de faciliter la visibilité dans la section Asset. En sélectionnant **« All Assets »** dans le menu déroulant **Asset Type to Display**, les utilisateurs peuvent voir chaque asset à travers tous les types d'assets.

Figure 58: Asset Type To Display

Il existe une condition spéciale pour **All Assets** appelée **«Unavailable for Asset Creation»**. Elle doit généralement être appliquée uniquement à **All Assets**. Si cette option est activée, aucun asset ne peut être créé pour ce type d'asset.

4.2.2.2 Création du type d'asset

Pour créer un nouveau type d'asset, les utilisateurs doivent cliquer sur **+ Asset Type**.

La section **Main Information** est l'endroit où le nom du type d'asset peut être configuré. Le type d'asset parent doit être défini sur **« All Assets »**.

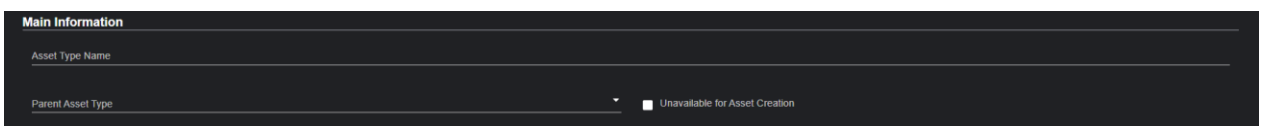


Figure 59: Type d'asset – Information principale

La section **Data Points** définit la structure des points de données et est divisée en trois sous-sections.

4.2.2.3 Type d'asset Type – Point de données analogue

Un point de données analogique représente une quantité physique variable telle que la tension, le courant, la température ou la pression. Chaque configuration de point de données analogique nécessite un nom et une unité.

Le nom doit être choisi pour standardiser la nomenclature des points de données.
Par exemple, pour un DC plant, le nom **« DC Plant Voltage »** doit être utilisé pour identifier la tension de float du DC plant. Ainsi, même si plusieurs modèles de DC plant sont utilisés sur un même site, la valeur de la tension de float peut être facilement identifiée.

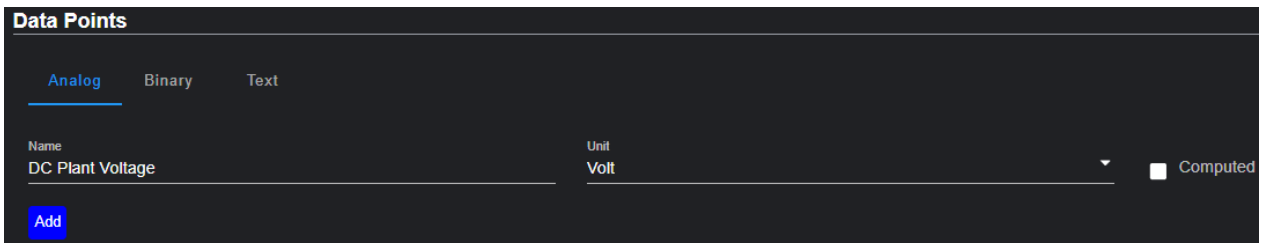


Figure 60: Type d'asset – Point de données analogique

The unit can be configured using a dropdown field.

4.2.2.4 *Type d'asset – Points de données binaires*

Un point de donnée binaire représente un signal numérique ou discret qui n'a que deux états possibles : True ou False. Ces points peuvent également être utilisés comme indicateurs d'alarme. Le nom doit être utilisé pour normaliser la nomenclature des points de données.

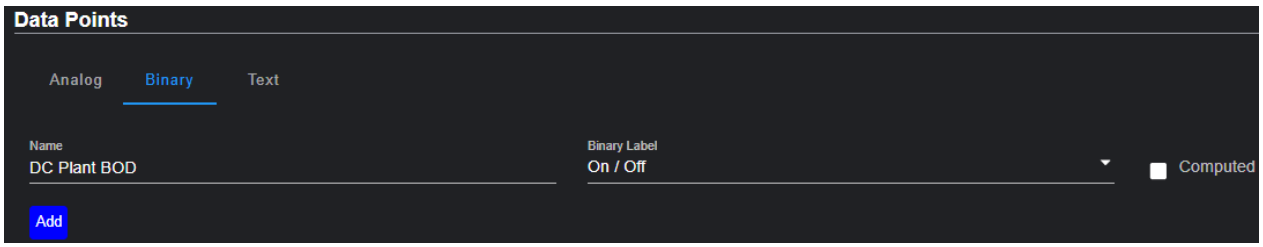


Figure 61: Type d'asset – Points de données binaires

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.

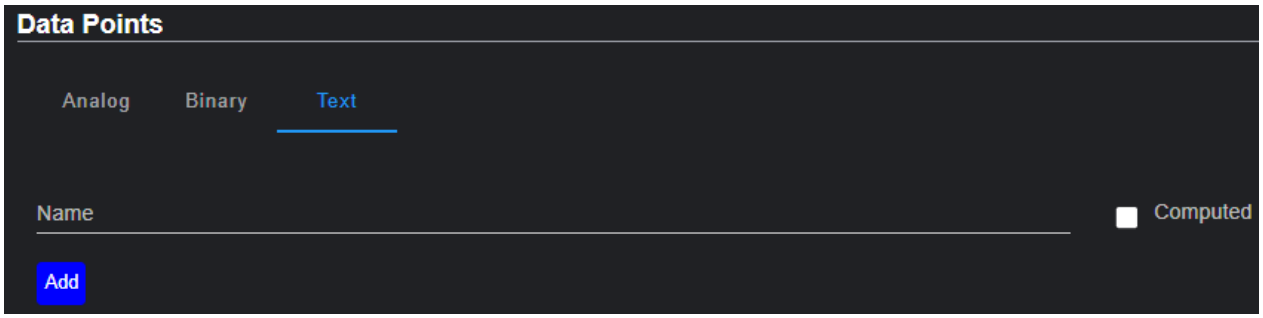


Figure 62: Type d'asset – Point de donné texte

4.2.3 TEMPLATES CONFIGURATION

Le point de donnée texte est utilisé pour configurer un point de donnée alphanumérique généralement utilisé dans le protocole SNMP. Le nom doit être utilisé pour normaliser la nomenclature des points de données.

4.2.3.1 *Protocol de communication*

Cette section vous permet de configurer les différents protocoles de communication pris en charge par l'iO.

Modbus RTU

L'iO prend en charge le protocole Modbus RTU Master, lui permettant d'interroger plusieurs dispositifs sur un réseau série RS-485.

La figure et le tableau ci-dessous affichent les différents champs requis pour configurer les paramètres de communication pour l'interrogation d'un dispositif Modbus RTU. Ces champs définissent des paramètres clés tels que le débit (baud rate), la parité, les bits d'arrêt, l'identifiant esclave (slave ID) et les adresses de registre, assurant une communication correcte sur le réseau RS-485.

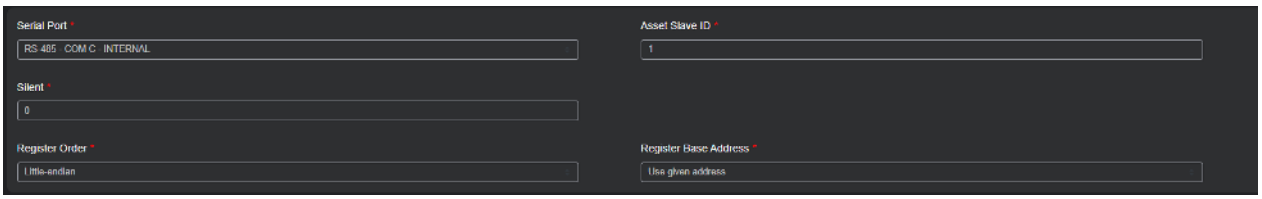


Figure 63: Gabarit du protocole de communication: Modbus RTU

Tableau 27: Gabarit du protocole de communication Modbus RTU -- Configuration

Champ	Description	Spécification	Obligatoire
Serial Port	**Sélection du port RS-485 utilisé pour la communication.**	Liste déroulante: • RS-485 – COM A • RS-485 – COM B	Oui
Asset Slave ID	C'est à cet endroit que l'ID du dispositif surveillé est configuré.	1 à 256	Oui
Silent	La fonctionnalité *silent mode* est utilisée pour introduire un délai dans la boucle d'acquisition, donnant à certains équipements plus anciens un « temps de respiration » lorsqu'ils sont interrogés via une communication série. Le paramètre *silent* ajoute le délai configuré entre chaque acquisition. Par exemple, si vous configurez une période *silent* d'une seconde, l'iO attendra une seconde après chaque acquisition pour laisser le dispositif ancien répondre. La plupart du temps, la valeur *silent* doit être réglée à zéro, mais dans certains cas, elle offre une flexibilité supplémentaire à l'utilisateur.	0 à 100 seconds	Oui
Register Order	L'ordre des registres est utilisé lorsqu'on traite des types de données plus grands que 16 bits (comme les entiers 32 bits et les flottants 32 bits).	Liste déroulante: • Big-Endian • Little-Endian	Oui

	Le **Big Endian** aussi appelé « Most Significant Byte (MSB) First », l'octet ou le mot de poids fort vient en premier (adresse la plus basse). Exemple d'une valeur 32 bits divisée en deux registres 16 bits : • Registre 40001 : 0x1234 • Registre 40002 : 0x5678 • Résultat combiné : 0x12345678 Le **Little Endian** aussi appelé « Least Significant Byte (LSB) First », l'octet ou le mot de poids faible vient en premier (adresse la plus basse). Exemple d'une valeur 32 bits divisée en deux registres 16 bits : • Registre 40001 : 0x5678 • Registre 40002 : 0x1234 • Résultat combiné : 0x12345678		
Register Base Address	Le champ détermine comment l'adresse du registre Modbus doit être interprétée lors de l'interrogation d'un dispositif. Use given address : L'adresse de registre entrée par l'utilisateur est utilisée telle quelle, sans ajustement. Par exemple, si vous entrez l'adresse 40001, le système interrogera exactement cette adresse. Subtract one from given address : Certains dispositifs Modbus utilisent un adressage basé sur 1 (par exemple, 40001), tandis que d'autres utilisent un adressage basé sur 0 (par exemple, zéro pour le premier registre). La sélection de cette option soustrait automatiquement un de l'adresse entrée pour s'aligner avec les dispositifs qui utilisent un index basé sur 0. Par exemple, entrer 40001 entraînera l'interrogation du registre 40000.	Liste déroulante: • Use given address (utiliser l'adresse assignée) • Subtract one from given address (déduire un de l'adresse assignée)	Oui

Multitel

Modbus TCP/IP

L'iO prend en charge le protocole Modbus TCP/IP Client, lui permettant d'interroger plusieurs dispositifs sur un réseau Ethernet.

La figure et le tableau ci-dessous affichent les différents champs requis pour configurer les paramètres de communication pour l'interrogation d'un dispositif Modbus TCP/IP. Ces champs définissent des paramètres clés tels que l'adresse IP, le numéro de port, l'unité ID et les adresses de registre, assurant une communication correcte sur le réseau en utilisant le protocole Modbus TCP/IP.

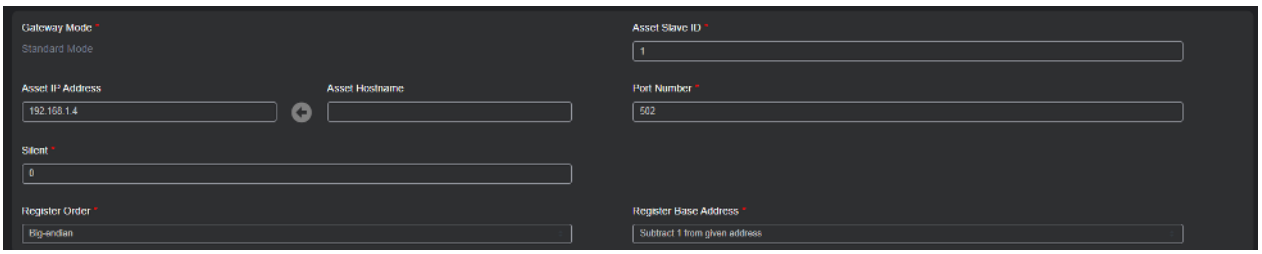


Figure 64: Gabarit de protocole de communication: Modbus TCP/IP

Tableau 28: Gabarit de protocole de communication Modbus TCP/IP -- Configuration

Champ	Description	Spécification	Obligatoire
Asset IP Address	Spécifie l'adresse IPv4 du dispositif cible à surveiller.	0.0.0.0 to 255.255.255.255	Oui
Asset Slave ID	C'est à cet endroit que l'ID du dispositif surveillé est configuré.	1 to 256	Oui
Port Number	Spécifie le numéro de port TCP utilisé pour établir la communication avec le dispositif.	1 to 65 535 (Default: 502)	Oui
Silent	La fonctionnalité silent mode est utilisée pour introduire un délai dans la boucle d'acquisition, donnant à certains équipements plus anciens « room to breathe » lorsqu'ils sont interrogés via une communication série. Le paramètre silent ajoute le délai configuré entre chaque acquisition. Par exemple, si vous définissez une période silent d'une seconde, l'iO attendra une seconde après chaque acquisition pour laisser le dispositif ancien répondre. La plupart du temps, la valeur silent doit être réglée à zéro, mais dans certains cas, elle fournit une flexibilité supplémentaire pour l'utilisateur.	0 to 100 seconds	Oui

Register Order	L'ordre des registres est utilisé lorsqu'on traite des types de données plus grands que 16 bits (comme les entiers 32 bits et les flottants 32 bits). Le **Big Endian** aussi appelé « Most Significant Byte (MSB) First », l'octet ou le mot de poids fort vient en premier (adresse la plus basse). Exemple pour une valeur 32 bits divisée en deux registres 16 bits : • Registre 40001 : 0x1234 • Registre 40002 : 0x5678 • Résultat combiné : 0x12345678 Le **Little Endian** aussi appelé « Least Significant Byte (LSB) First », l'octet ou le mot de poids faible vient en premier (adresse la plus basse). Exemple pour une valeur 32 bits divisée en deux registres 16 bits : • Registre 40001 : 0x5678 • Registre 40002 : 0x1234 • Résultat combiné : 0x12345678	Liste déroulante: • Big-Endian • Little-Endian	Oui
Register Base Address	Le champ détermine comment l'adresse du registre Modbus doit être interprétée lors de l'interrogation d'un dispositif. Use given address : L'adresse de registre entrée par l'utilisateur est utilisée telle quelle, sans ajustement. Par exemple, si vous entrez l'adresse 40001, le système interrogera exactement cette adresse. Subtract one from given address : Certains dispositifs Modbus utilisent un adressage basé sur 1 (par exemple, 40001), tandis que d'autres utilisent un adressage basé sur 0 (par exemple, zéro pour le premier registre). La sélection de cette option soustrait automatiquement un de l'adresse entrée pour s'aligner avec les dispositifs qui utilisent un index basé sur 0.	Liste déroulante: • Use given address • Subtract 1 from given address	Oui

	Par exemple, entrer 40001 entraînera l'interrogation du registre 40000.		

SNMP

L'iO prend en charge le protocole SNMP (v1, v2c et v3), lui permettant d'interroger plusieurs dispositifs sur un réseau Ethernet afin de récupérer des informations de performance et d'état.

La figure et le tableau ci-dessous affichent les différents champs requis pour configurer les paramètres de communication pour l'interrogation d'un dispositif compatible SNMP. Ces champs définissent des paramètres clés tels que l'adresse IP, la version SNMP, la chaîne de communauté (pour v1/v2c), les informations d'authentification (pour v3) et la partie constante de l'OID (Object Identifier), assurant une communication fiable et une acquisition de données à partir des dispositifs compatibles SNMP.

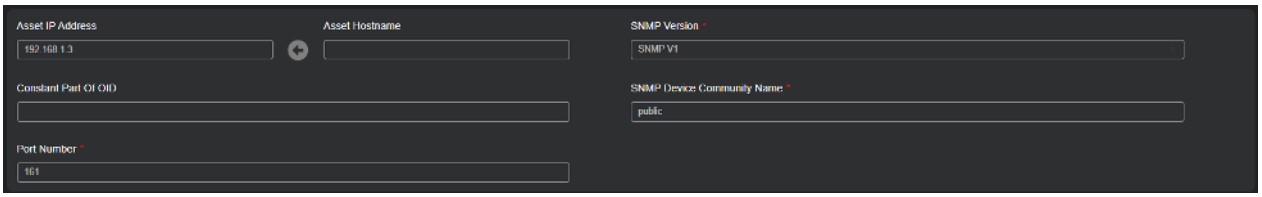


Figure 65: Gabarit du protocole de communication: Modbus TCP/IP

Tableau 29: Gabarit du protocole de communication Modbus TCP/IP – Configuration

Champ	Description	Spécification	Obligatoire
Asset IP Address	Spécifie l'adresse IPv4 du dispositif cible à surveiller.	0.0.0.0 à 255.255.255.255	Oui
Asset Hostname	Champ optionnel utilisé pour définir un nom résolvable par DNS pour le dispositif.	Nom d'hôte alphanumérique	Non
SNMP Version	Sélectionner la version de SNMP à utiliser pour la communication.	Liste déroulante: • SNMP v1 • SNMP v2c • SNMP v3	Oui
SNMP Device Community Name	Chaîne de texte qui agit comme un mot de passe pour la communication SNMP v1/v2c. Les valeurs courantes incluent public ou private.	Chaîne alphanumérique	Oui
Port Number	Numéro de port utilisé pour l'interrogation SNMP. Le port SNMP par défaut est 161.	1 à 65 535 (Défaut: 161)	Oui
Constant Part of OID	Object Identifier (OID) de base utilisé pour définir la structure MIB SNMP à interroger. Les points de données sont généralement ajoutés à cet OID de base.	Format OID séparé par des points (par ex. 1.3.6.1.4.1.x.x)	Non

Username (SNMPv3)	Nom d'utilisateur utilisé pour l'authentification SNMPv3.	Alfanumérique	Oui (v3 seulement)
Security Level (SNMPv3)	Définit le niveau d'authentification et de confidentialité pour SNMPv3.	Liste déroulante: • No Auth, No Priv • Auth, No Priv • Auth, Priv	Oui (v3 seulement)
Default Context Name	Nom de contexte SNMPv3 optionnel, utilisé lors de l'accès à des vues MIB spécifiques sur l'agent.	Chaîne alphanumérique	Oui (v3 seulement)
Authentication Protocol	Définit l'algorithme de hachage utilisé pour l'authentification SNMPv3.	Liste déroulante: • MD5 • SHA	Requis si Auth est activé
Authentication Password	Mot de passe utilisé pour l'authentification SNMPv3.	La longueur minimale varie selon la politique du dispositif	Requis si Auth est activé
Privacy Protocol	Définit la méthode de chiffrement utilisée pour protéger les charges utiles SNMPv3.	Liste déroulante: • DES • AES	Requis si Privacy est activé
Privacy Password	Mot de passe utilisé pour le chiffrement de confidentialité SNMPv3.	La longueur minimale varie selon la politique du dispositif	Requis si Privacy est activé

4.2.3.2 Polling Engine

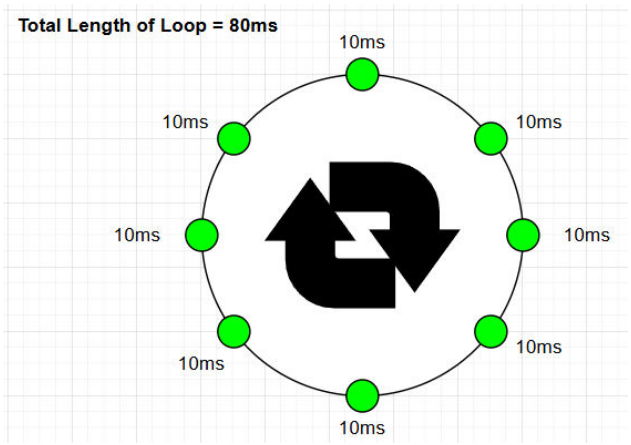
Le polling engine est responsable de la gestion de la manière dont l'iO communique avec les dispositifs externes pour collecter les données. Cette section permet aux utilisateurs d'affiner le comportement du mécanisme de polling, y compris la fréquence, le comportement de timeout, les tentatives de reprise, et la durée globale du polling. Ces paramètres sont essentiels pour optimiser les performances, en particulier dans les environnements où les dispositifs ont des temps de réponse ou une fiabilité variable.

Le polling engine utilise une boucle d'acquisition pour gérer les requêtes permettant de récupérer des informations auprès de divers dispositifs. Il existe deux boucles distinctes : une pour Modbus RTU et Modbus TCP/IP, et une autre pour SNMP. Cela signifie que les performances peuvent varier selon le nombre de dispositifs interrogés.

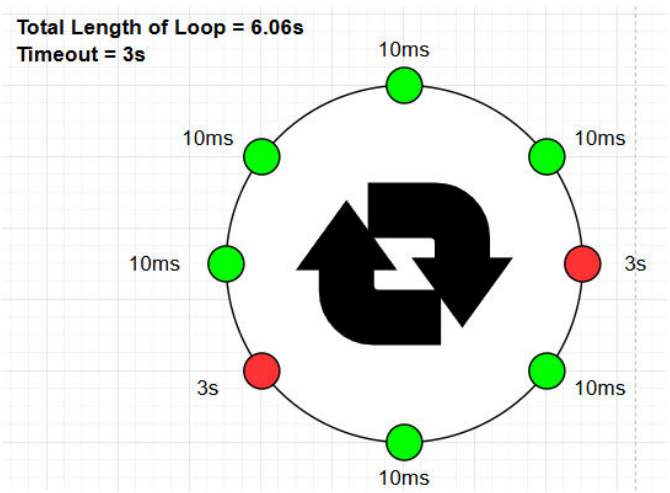
Prenons l'exemple d'un seul dispositif interrogé à l'aide de SNMP avec huit points de données. Si tous les points de données sont configurés avec un taux de polling d'une seconde, l'iO enverra une requête au dispositif chaque seconde pour récupérer les données. Le cycle requête/réponse est généralement rapide, surtout avec SNMP.

Voici une représentation visuelle de la boucle d'acquisition :

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.



Dans cet exemple, la durée totale de la boucle est de 80 ms, donc le taux de polling d'une seconde sera facilement respecté.
Dans l'exemple suivant, nous utilisons le même dispositif mais introduisons des points de données qui ne répondent pas. Lorsqu'un point de donnée ne répond pas, le mécanisme de timeout est déclenché. Le timeout agit comme un délai entre la requête et la réponse attendue. L'iO envoie la requête et attend la durée de timeout configurée avant de passer au point de donnée suivant. Si le point de donnée est en erreur ou ne répond pas, l'iO attendra toute la période de timeout avant de continuer.



Dans cet exemple, la durée totale de la boucle est de 6,06 secondes avec un timeout de trois secondes, donc le taux de polling d'une seconde ne sera pas respecté.
Comme indiqué précédemment, toutes les acquisitions provenant des dispositifs Modbus RTU, Modbus TCP/IP et SNMP sont gérées dans la même boucle. Il est donc important de considérer que l'activation d'un grand nombre de dispositifs avec des points de données en erreur peut introduire de la latence dans l'ensemble du système. Les dispositifs entièrement fonctionnels peuvent être négativement impactés par d'autres qui ne répondent pas correctement.

⚠ **Avertissement :**
L'activation d'un grand nombre de dispositifs avec des points de données en erreur peut introduire de la latence dans l'ensemble du système.

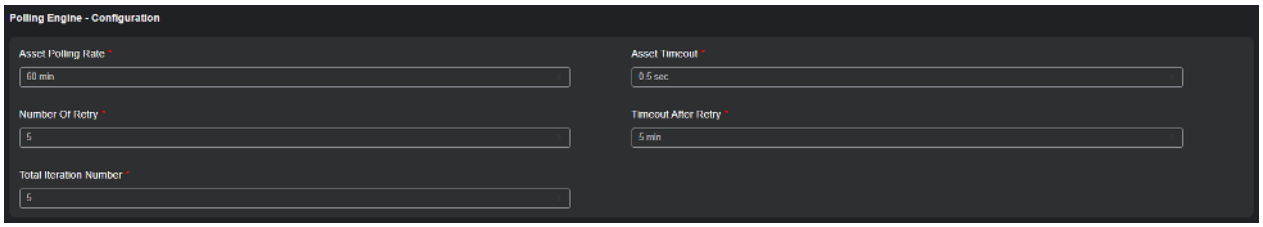


Figure 66: Gabarit de la polling engine

Tableau 30: Gabarit de la polling engine - Configuration

Champ	Description	Spécification	Obligatoire
Asset Polling Rate	Définit la fréquence à laquelle le système interroge le dispositif. Cela détermine l'intervalle entre chaque cycle d'acquisition.	Liste déroulante	Yes
Asset Timeout	Temps maximal d'attente pour une réponse du dispositif avant de considérer la requête comme échouée.	Liste déroulante	Yes
Number of Retry	Nombre de tentatives de reprise après un échec de polling avant de déclencher la période de retry timeout.	Liste déroulante	Yes
Timeout After Retry	Temps que le polling engine attend avant de redémarrer le polling pour un dispositif après l'échec de toutes les tentatives de reprise.	Liste déroulante	Yes
Total Iteration Number	Nombre total de boucles de polling à exécuter pour le dispositif ou la configuration donnée. Utilisé pour limiter la durée de la séquence de polling.	Liste déroulante	Yes

4.3 UNITS

Les paramètres Units sont accessibles à partir du module Settings.

Figure 67: Configuration -- Units

Les unités sont utilisées dans les points de données analogiques pour fournir une représentation visuelle de la mesure physique. Elles servent uniquement d'éléments d'affichage et n'effectuent aucune conversion ou mise à l'échelle des données réelles. Par exemple, changer l'unité de VA à kVA n'appliquera aucune mise à l'échelle à la valeur du point de donnée. Si une mise à l'échelle est requise, la fonctionnalité « factor » doit être utilisée à la place.

La seule exception concerne les unités de température (°C et °F) dans la section I/O Channels. Lorsque le type front-end est défini sur Temp, les utilisateurs peuvent basculer entre °C et °F, et la conversion sera automatique.

La section Units couvre l'ID de l'unité, qui est un identifiant unique pour le libellé de l'unité. Le Unit Name est le nom complet de l'unité physique, et l'Abbreviation est ce qui est réellement affiché dans l'iO. Veuillez noter que les unités sont préchargées dans l'iO, et les utilisateurs ne peuvent pas ajouter leurs propres unités.

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 (PROTOCOLES)

Les paramètres Protocols peuvent être accessibles à partir du module Settings.

Figure 69: Paramètres – Protocols

4.4.1 HTTP/HTTPS

L'utilisation simultanée de HTTP et HTTPS n'est pas recommandée. Cependant, les deux protocoles sont activés par défaut en sortie d'usine. Il est recommandé de désactiver l'un des deux.

Le port par défaut pour HTTP est 80 et 443 pour HTTPS. Pour modifier ces valeurs par défaut, saisissez un numéro de port entre 1 et 65 534. Pour assurer une communication correcte, chaque protocole doit être assigné à un numéro de port unique.

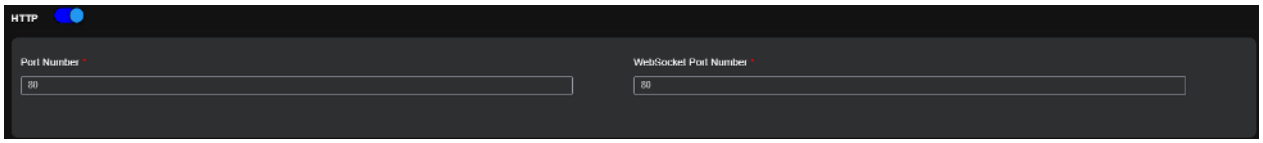


Figure 70: Paramètres – HTTP

Tableau 31: HTTP -- Configuration

Champ	Description	Spécification	Obligatoire
HTTP Enabled	Active ou désactive l'accès HTTP au dispositif.	Activé (défaut)	Oui
Port Number	Port utilisé pour l'accès HTTP standard. La valeur par défaut est 80.	1 à 65 535 (Défaut: 80)	Oui
WebSocket Port Number	Port utilisé pour la communication WebSocket sur HTTP.	1 à 65 535 (Défaut: 80)	Oui

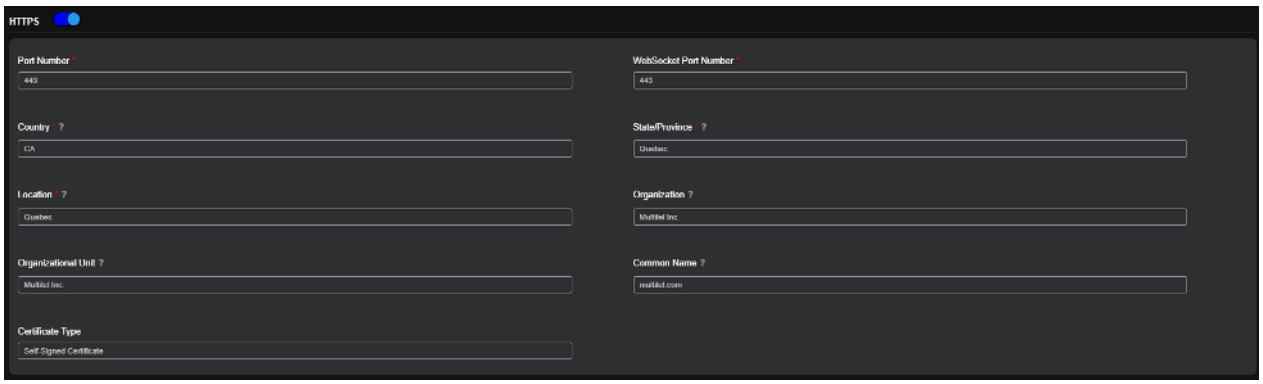


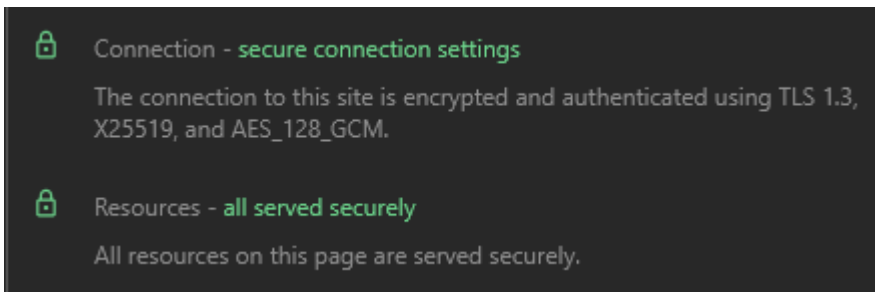
Figure 71: Paramètres – HTTPS

Multitel

Tableau 32: HTTPS – Configuration

Champ	Description	Spécification	Obligatoire
HTTPS Enabled	Active ou désactive l'accès HTTPS au dispositif.	Enabled (default)	Oui
Port Number	Port utilisé pour l'accès HTTPS standard. La valeur par défaut est 80.	1 to 65 535 (Default: 80)	Oui
WebSocket Port Number	Port utilisé pour la communication WebSocket sur HTTPS.	1 to 65 535 (Default: 80)	Oui
Country	Code du pays utilisé pour la génération du certificat SSL.		Oui
State/Province	Nom de l'État ou de la province utilisé dans le certificat SSL.		Oui
Location	Ville ou localité pour le certificat SSL.		Oui
Organization	Nom légal de l'organisation utilisé dans le certificat SSL.		Oui
Organizational Unit	Département ou unité au sein de l'organisation. Utilisé dans le certificat SSL.		Oui
Common Name	Nom de domaine pleinement qualifié (FQDN) du dispositif. Doit correspondre à l'URL d'accès pour que HTTPS fonctionne correctement.		Oui
Certificate Type	Type de certificat SSL utilisé. Il peut s'agir d'un certificat auto-signé ou d'un certificat émis par une autorité de certification (CA).		Oui

⚠ **Note:**
La version HTTPS prend en charge le chiffrement et l'authentification utilisant TLS 1.3, X25519 et AES_128_GCM :



Multitel

4.4.2 SNMP – AGENT

Cette section est utilisée pour configurer le SNMP Agent du dispositif iO. Le SNMP Agent peut être utilisé par Atlas pour collecter des données depuis le dispositif iO.

Pour configurer le SNMP Agent :

- Cliquez sur Settings.
- Cliquez sur Protocols — onglet SNMP Agent.
- Entrez un numéro de port.
- Le port par défaut est 161. Pour modifier cette valeur par défaut, entrez un numéro de port entre 1 et 65 534.
- Activez le SNMP v1/v2c Agent ou v3.
- Entrez un Read Community Name.
- Cliquez sur Submit.

4.4.3 SNMP – TRAP

Cette section est utilisée pour configurer le SNMP Trap Receiver sur le dispositif iO. Elle fait partie de la fonctionnalité Trap Forwarding.

Pour configurer le SNMP Trap :

- Cliquez sur Settings.
- Cliquez sur Protocols – SNMP – onglet Trap.
- Entrez un numéro de port.
    - Le port par défaut est 161. Pour modifier cette valeur par défaut, entrez un numéro de port entre 1 et 65 534.

- Activez le SNMP v1/v2c.
- Entrez un Read Community Name.
- Cliquez sur Submit.

4.4.4 SSH

Cette section est utilisée pour configurer la console SSH.

- Cliquez sur Settings.
- Cliquez sur Protocols – onglet SSH.
- Entrez un numéro de port.
    - Le port par défaut est 22. Pour modifier cette valeur par défaut, entrez un numéro de port entre 1 et 65 534.

- Activez le SSH.
- Cliquez sur Submit.

4.4.5 PING

Cette section est utilisée pour activer ou désactiver le PING du dispositif iO.

4.4.6 MODBUS

La section Modbus est utilisée pour configurer le Modbus RTU Server ID. Cet ID serveur sera utilisé par le RTU pour surveiller le dispositif iO.

Pour configurer le Modbus Server ID :

- Cliquez sur Settings.
- Cliquez sur Protocols — onglet Modbus Server.
- Cliquez sur Enable.
- Entrez le Server ID.
    - Le Server ID par défaut est 80. Pour modifier cette valeur par défaut, entrez un numéro entre 1 et 255.

- Cliquez sur Submit.

4.5 NOTIFICATIONS

Les paramètres Notifications peuvent être accessibles à partir du module Settings.

Figure 72: Paramètres -- Notifications

4.5.1 CONFIGURATIONS

Cette section est utilisée pour configurer les notifications pour un point de donnée binaire.

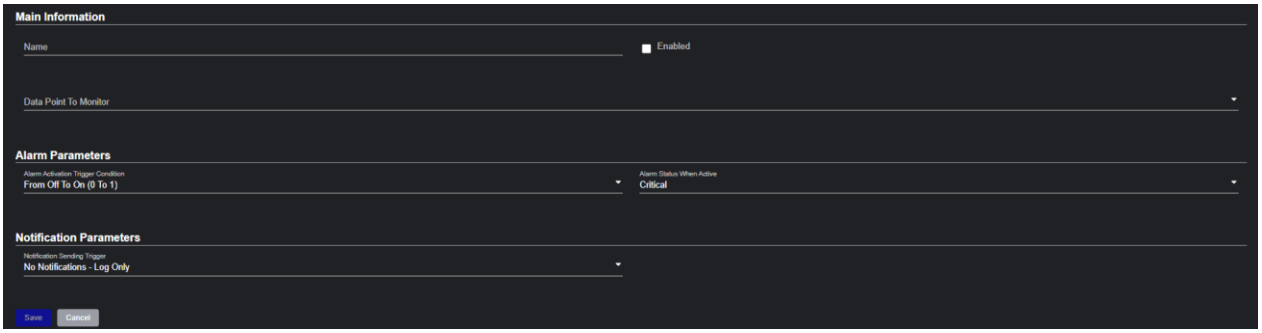


Figure 73: Paramètres -- Notifications

Cette section permet aux utilisateurs de configurer les conditions d'alarme sur des points de données surveillés spécifiques. Lorsque la condition de déclenchement configurée est atteinte, le dispositif iO enregistre l'événement d'alarme et, selon la configuration, peut également générer des notifications.

La configuration de l'alarme est composée de trois parties :

• **Main Information** – Définit les paramètres de base tels que le nom, l'état et le point de donnée à surveiller.
• **Alarm Parameters** – Spécifie la condition qui déclenche l'alarme et le niveau de sévérité.
• **Notification Parameters** – Détermine si une notification est générée lorsque l'alarme est déclenchée.

Chaque point de donnée binaire dans l'iO peut être utilisé pour déclencher une notification. Cela inclut les points de données binaires provenant des canaux I/O physiques, de Modbus, de SNMP et des points de données calculés.

La condition de déclenchement est basée sur la valeur des points de données binaires. Il existe deux conditions de déclenchement différentes :

• **From Off to On (0 to 1)** : La notification sera déclenchée lorsque la condition du point de donnée passe de False à True.
• **From On to Off (1 to 0)** : La notification sera déclenchée lorsque la condition du point de donnée passe de True à False.

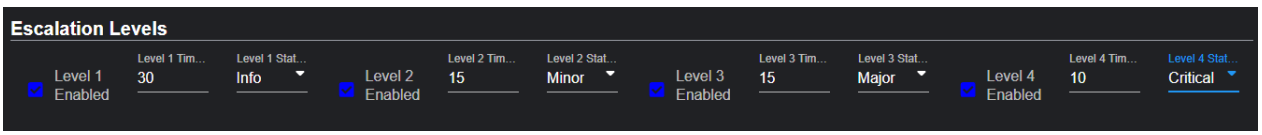


Figure 74: Paramètres -- Notifications –- Escalation Levels (niveaux d'escalation)

La section Escalation Levels permet à l'utilisateur d'augmenter automatiquement (escalader) la sévérité de l'alarme au fil du temps lorsque la condition d'alarme reste active. Cela est utile pour différencier une alarme transitoire courte d'un problème persistant nécessitant plus d'attention.

Multitel

Lorsque la condition de déclenchement devient active, le dispositif iO démarre le minuteur d'escalade. Si l'alarme est toujours active après le délai configuré, la sévérité de l'alarme est mise à jour au prochain niveau d'escalade.

Voici le comportement clé :

- L'escalade est appliquée uniquement tant que l'alarme reste active.
- Les niveaux d'escalade sont traités dans l'ordre (Level 1 → Level 4).
- Chaque niveau devient actif après son délai configuré.
- Le statut sélectionné pour chaque niveau doit correspondre à un niveau d'alarme configuré.

Configuration Fields

Pour chaque niveau (Level 1 à Level 4), les paramètres suivants sont disponibles :

- **Enabled (checkbox)**
  Active ou désactive le niveau d'escalade.
- **Time (s)**
  Le délai (en secondes) avant que le niveau ne soit appliqué après que l'alarme devient active.
- **Status (drop-down)**
  Le niveau de sévérité à appliquer lorsque ce niveau d'escalade est atteint (ex. : Info, Minor, Major, Critical).

Exemple
Si Level 1 est configuré comme Info après 30 s, Level 2 comme Minor après 15 s, Level 3 comme Major après 15 s, et Level 4 comme Critical après 10 s :

- L'alarme commence au Default Alarm Status lorsqu'elle devient active.
- Après 30 secondes, elle escalade à Info (Level 1).
- Après 15 secondes supplémentaires, elle escalade à Minor (Level 2).
- Après 15 secondes supplémentaires, elle escalade à Major (Level 3).
- Après 10 secondes supplémentaires, elle escalade à Critical (Level 4), jusqu'à ce que l'alarme soit rétablie.

Comment configure les Escalation Levels

1. Aller dans Settings.
2. Sélectionner Notifications.
3. Ouvrir une configuration de notification existante ou en créer une nouvelle.
4. Dans Escalation Levels, activer les niveaux souhaités.
5. Pour chaque niveau activé, définir :
   - Time (s)
   - Status
6. Cliquer sur Save.

Notes/Best Practices

- Garder les délais d'escalade alignés avec votre processus opérationnel (ex. : délais courts pour les infrastructures critiques, délais plus longs pour les signaux bruyants).
- Si vous souhaitez une sévérité fixe sans escalade, désactivez tous les niveaux et utilisez uniquement le Default Alarm Status.
- S'assurer que les options Status (Info/Minor/Major/Critical) sont définies et ordonnées correctement dans STATUSES afin que l'escalade corresponde à vos règles de priorité.

Lorsque la condition déclenchée est valide, les paramètres de notification seront appliqués :

- **No Notifications – Log Only** : L'événement est enregistré en interne, mais aucune notification n'est envoyée.
- **Notification When the Alarm Becomes Active** : Une notification est envoyée lorsque l'alarme est déclenchée.
- **Notification When the Alarm Becomes Active and When It Comes Back to Normal** : Une notification est envoyée lorsque l'alarme est déclenchée, et une notification « clear » séparée est envoyée lorsque la condition revient à la normale.

4.5.2 TRAP DESTINATIONS

Veuillez vous référer aux sections suivantes dans ce guide :

- VUE D'ENSEMBLE DESTINATIONS
- CONFIGURATION DE DESTINATIONS DE TRAP

4.5.3 STATUSES

Pour configurer les niveaux d'alarme, cela peut être fait en suivant ces étapes :

• Aller dans Settings.
• Aller dans Notifications.
• Cliquer sur l'onglet Status.
• Cliquer sur + Status.

Figure 75: Création niveau d'alarme

La position est utilisée pour prioriser le niveau d'alarme. La position doit être configurée de la manière suivante :

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

Figure 76: Niveau de priorité d'alarme

4.6 LABELS

4.6.1 VUE D'ENSEMBLE DES LABELS BINAIRES

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

Pour configurer les binary labels, cela peut être fait en suivant ces étapes :

- Aller dans Settings.
- Aller dans Labels.

• Cliquer sur l'onglet Binary Labels.
• Cliquer sur + Label pour créer un nouveau binary label.
• Cliquer sur Save Label pour enregistrer un nouveau binary label ou pour apporter des modifications à un existant.

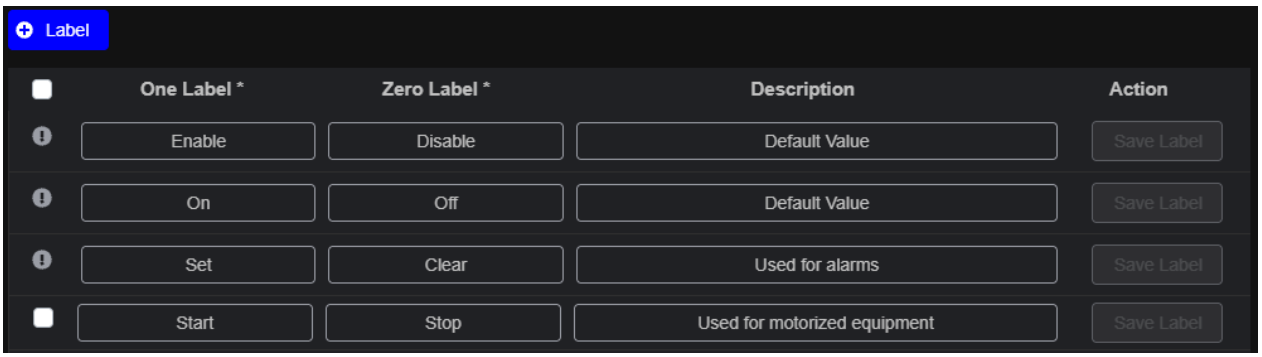


Figure 77: Labels binaires – Configuration

Tableau 33: Labels binaires – Configuration

Champ	Description	Spécification	Obligatoire
One Label	Label affiché si la valeur du point de donnée est True. Tous les One Label doivent être uniques.	1 à 50 caractères	Oui
Zero Label	Label affiché si la valeur du point de donnée est False. Tous les Zero Label doivent être uniques.	1 à 50 caractères	Oui
Description	Permet d'expliquer l'utilisation du binary label. Il est seulement visible sur la page des binary labels.	1 à 250 caractères	Non
Action	Permet d'enregistrer les modifications du binary label.	Bouton	

4.7 LOGS

Le module Logs est utilisé pour exporter des informations de diagnostic depuis le dispositif iO. Ces logs aident à suivre les changements de configuration et fournissent des données d'échantillonnage pour le dépannage des problèmes d'acquisition.
La page Log contient deux onglets principaux :
• **Data Points**
• **System**

4.7.1 DATA POINTS (POINTS DE DONNÉES)

L'onglet Data Points fournit des outils pour exporter des informations liées aux logs des points de données binaires et à l'échantillonnage des points de données analogiques.

4.7.1.1 Points de données binaires

Cette section permet aux utilisateurs d'exporter les changements les plus récents appliqués aux points de données binaires.

Pour exporter les derniers changements des points de données binaires, suivre ces étapes :

- Aller dans Logs.
- Sélectionner l'onglet Data Points.
- Dans Binary Data Points, cliquer sur Download Latest Binary Data Points Changes.

Le fichier exporté comprend les colonnes suivantes :

- **Equipment Name**
  Nom de l'asset associé au point binaire
- **Data Point Name**
  Nom d'affichage / description du point de donnée binaire (par ex., DPAT B1, DP B10, etc.).
- **Mnemonic**
  Identifiant unique du point binaire (par ex., M1BI1, M1BI10).
- **Status**
  L'état / la valeur rapportée au moment de l'événement (par ex., Stop, Stopped, Close, Off, Clear, Running).
  Les valeurs de Status dépendent du template et du mapping du dispositif.
- **Date**
  Date à laquelle le changement a été enregistré (YYYY-MM-DD).
- **Time**
  Heure à laquelle le changement a été enregistré (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 78: Points de données binaires – Fichier du journal

4.7.1.2 Data Point Sampling

La fonctionnalité Data Point Sampling est utilisée pour enregistrer les valeurs en série temporelle d'un point de donnée sélectionné dans un fichier .CSV, même lorsque la valeur ne change pas.

Pour exporter un fichier d'échantillonnage, suivre ces étapes :

- Aller dans Settings.
- Aller dans Logs.
- Sélectionner l'onglet Data Points.
- Dans Data Point Sampling, sélectionner l'entrée d'échantillonnage souhaitée dans le menu déroulant (par ex., Datapoint sampling for S2AI1).
- Cliquer sur Export.

Si le fichier d'échantillonnage n'est plus nécessaire :

- Sélectionner l'entrée d'échantillonnage.
- Cliquer sur Delete File.

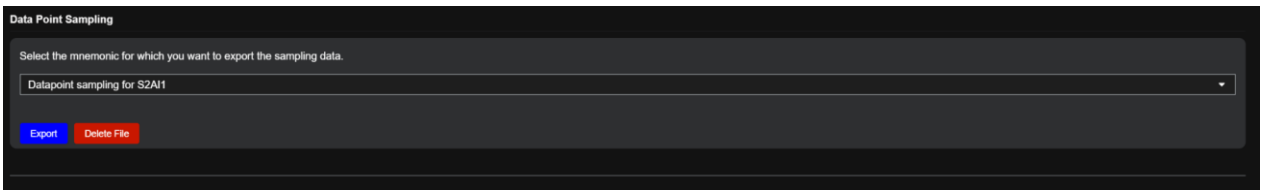


Figure 79: Data Point Sampling

Le Data point sampling nécessite un script Lua computed data point qui active l'échantillonnage pour un mnemonic spécifique. L'échantillonnage peut être activé :

- Au niveau de l'Asset Data Point, ou
- Au niveau de l'Asset Type.

Une fois activé par le script Lua, le mnemonic devient disponible dans la liste déroulante Data Point Sampling.

Le fichier d'échantillonnage exporté est généré en format .CSV et inclut généralement :

- **DateTime**
  Horodatage au format UTC.
- **Local DateTime**
  Horodatage en heure locale avec décalage de fuseau horaire.
- **Value**
  La valeur acquise enregistrée à la fréquence d'échantillonnage.

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 80: Fichier du Data Point Sampling

Étant donné que la valeur est écrite à la fréquence d'échantillonnage configurée, le fichier peut contenir des valeurs répétées même lorsque le point de donnée est stable.

Pour démarrer l'échantillonnage, utilisez la fonction ci-dessous dans un **Lua computed data point** :

enableDatapointSampling('MNEMONIC', 'SamplingDurationUnit', 'SamplingDuration', 'SamplingRate')

Cette fonction écrit les valeurs acquises dans un fichier .CSV à la fréquence demandée, pour la durée configurée.

Paramètres

- **MNEMONIC**
  Mnemonic (identifiant) du point de donnée à échantillonner.
- **SamplingDurationUnit**
  Unité utilisée pour la durée d'échantillonnage. Les valeurs prises en charge sont :
  - **"s"** secondes
  - **"m"** minutes
  - **"h"** heures
- **SamplingDuration**
  Durée de la session d'échantillonnage (utilisée avec l'unité).
- **SamplingRate**
  Fréquence (en secondes) à laquelle les valeurs sont écrites dans le fichier d'échantillonnage. Ceci remplace le délai par défaut du point de donnée à des fins de journalisation.

⚠ **Remarque:**

L'utilisation de plusieurs points de données avec une faible fréquence d'échantillonnage (par ex., < 5 secondes) peut affecter les performances du dispositif.

Pour arrêter l'échantillonnage d'un point de donnée, utilisez :

disableDatapointSampling('MNEMONIC')

Multitel

Cela désactive l'échantillonnage pour le mnemonic spécifié et arrête l'écriture des valeurs dans le fichier .CSV.

Exemple d'utilisation :

Vous avez un point de donnée binaire (S1BI1) et un point de donnée analogique (S1AI1). Vous voulez échantillonner S1AI1 uniquement lorsque S1BI1 est true.

```
asset.autoRefreshWith('S1BI1')  -- Exécuter ce script chaque fois que S1BI1 acquiert une nouvelle valeur
local enabled = asset.getDatapoint('S1BI1')  -- Obtenir la valeur de S1BI1

if enabled then
    asset.enableDatapointSampling('S1AI1', 'm', 10, 5)  -- Échantillonner pendant 10 minutes, toutes les 5 secondes
Échantillonner pendant 10 minutes, toutes les 5 secondes
else
    asset.disableDatapointSampling('S1AI1')  -- Arrêter l'échantillonnage
end
```

Ce exemple:

- Surveille **S1BI1**.
- Démarre l'échantillonage de S1AI1 pendant 10 minutes à des intervalles de cinq seconds lorsque S1BI1 est actif.
- Arrête l'échantillonage lorsque S1BI1 devient inactif.

4.7.2 SYSTEM

L'onglet System fournit des exports pour les logs de sécurité et de diagnostic générés par le dispositif iO. Ces fichiers sont généralement utilisés pour le dépannage, les audits et les enquêtes de support.

La page System contient deux sections :

• **Security**
• **Diagnostics**

Un bouton Back est disponible pour revenir à la page précédente.

4.7.2.1 Security

L'export des Security Logs fournit une piste d'audit de l'activité d'authentification sur le dispositif iO. Ces logs sont principalement utilisés pour suivre les sessions utilisateur, vérifier qui a accédé au système et identifier l'adresse IP source de chaque connexion.

Pour exporter les security logs :

- Aller dans Logs.
- Sélectionner l'onglet System.
- Dans Security, cliquer sur Download Security Logs.

Le log exporté est un fichier textuel où chaque ligne représente un événement.

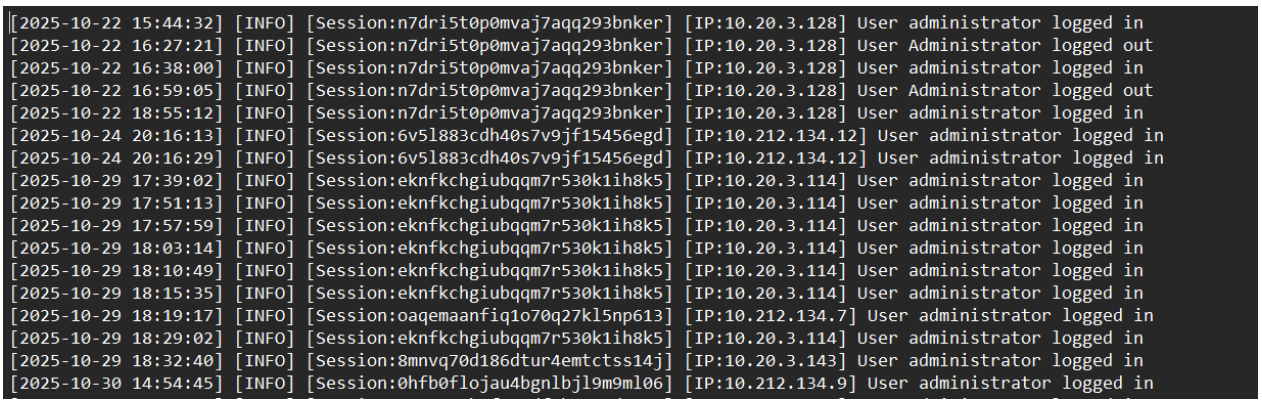


Figure 81: Security – Fichier du journal

Une entrée typique contient :

- **Timestamp**
  Date et heure auxquelles l'événement s'est produit (par ex., 2025-10-22 15:44:32).
- **Severity**
  Niveau du log (par ex., INFO).
- **Session ID**
  Identifiant unique de la session utilisateur (exemple : Session:n7dri5t0p0mvaj7aqq293bnker).
- **Source IP Address**
  Adresse IP du client qui s'est connecté au dispositif iO (par ex., IP:10.20.3.128).
- **Event Message**
  Description de l'événement (par ex., User administrator logged in / User Administrator logged out).

4.7.2.2 Diagnostics

La section Diagnostics est utilisée pour exporter les logs de diagnostic du dispositif. Ces logs sont généralement demandés pour le dépannage lors d'enquêtes sur des problèmes de communication, des problèmes de performance ou un comportement inattendu.

Pour exporter les diagnostics logs :

- Aller dans Logs.
- Sélectionner l'onglet System.
- Dans Diagnostics, cliquer sur Download All Logs.

4.8 SYSTEM MAINTENANCE

Les paramètres Inventory sont accessibles à partir du module Settings.

Figure 82: Paramètres – System Maintenance

4.8.1 CONFIGURATION FILE

Cette section est utilisée pour importer ou exporter des fichiers de configuration pour le dispositif iO.

Figure 83: Maintenance du système – Configuration File

Avant d'importer une nouvelle configuration, assurez-vous qu'aucun utilisateur n'effectue d'opérations manuelles.

- Dans Settings | System Maintenance, cliquer sur l'onglet Configuration File.
- Cliquer sur Export.
    - Cette étape n'est pas obligatoire, mais elle est recommandée par Multitel. Si la nouvelle configuration entraîne des résultats inattendus, vous pourrez restaurer le dispositif en utilisant la configuration de sauvegarde.

- Cliquer sur Import.
- Sélectionner le nouveau fichier de configuration (fichier CSV ou .TXT).
- Cliquer sur Start Import.

L'importation d'une nouvelle configuration peut prendre quelques minutes. Un message de confirmation ou d'erreur sera affiché lorsque le processus sera terminé.

⚠ **Messages d'erreur:**
Même si des erreurs sont signalées, la configuration sera tout de même importée, à l'exception des lignes comportant des erreurs.

⚠ **Avertissement:**
Lorsque vous importez un fichier de configuration, toute la configuration existante du dispositif sera remplacée par la nouvelle configuration. L'importation d'un fichier de configuration peut modifier des paramètres critiques (tels que les propriétés de connexion Ethernet), ce qui peut affecter l'accès à distance au dispositif.

⚠ **Recommendation:**
Multitel recommande de sauvegarder ou d'exporter le fichier de configuration avant d'en importer un nouveau. Pour éviter d'écraser les paramètres existants, Multitel recommande également d'importer uniquement les paramètres modifiés, et non l'intégralité du fichier de configuration.

4.8.2 SCRIPT TEMPLATES

La section Script Templates est utilisée pour charger et gérer une librairie de modèles de scripts Lua destinés aux Computed Data Points. Ces modèles fournissent des exemples prêts à l'emploi (ou des points de départ) pour accélérer le déploiement et standardiser les calculs entre les dispositifs (par ex., seuils avec/sans hystérésis, moyennes, chronomètres, calculs d'autonomie de batterie, etc.).

La librairie Script Templates est accessible depuis le menu Settings | System Maintenance.

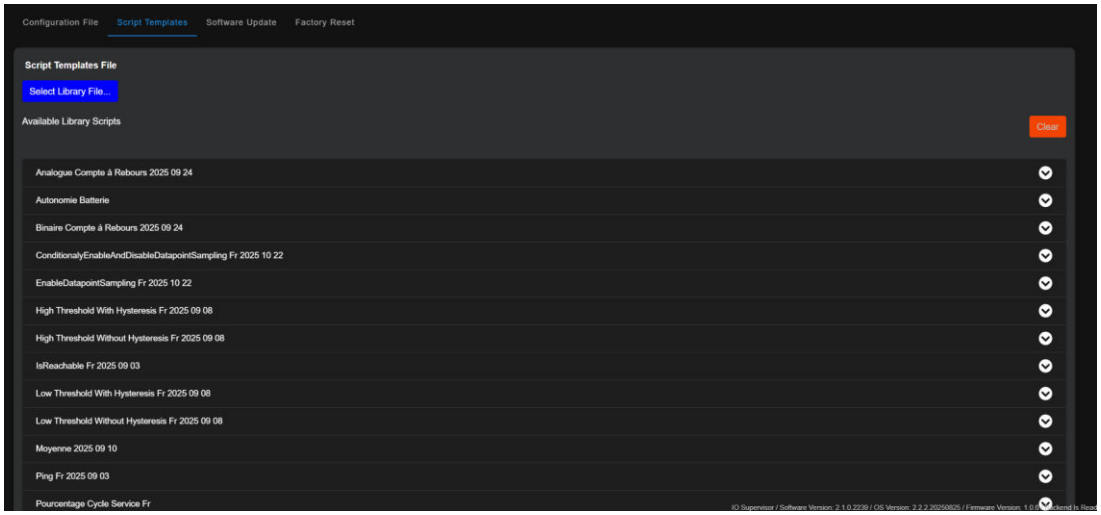


Figure 84: Maintenance du système – Script Templates

4.8.2.1 Charger une nouvelle librairie de Script Templates

Avant de charger une nouvelle librairie, assurez-vous qu'aucun utilisateur n'effectue d'opérations manuelles.

- Dans Settings | System Maintenance, cliquer sur l'onglet Script Templates.
- Cliquer sur Select Library File.
- Sélectionner le fichier de librairie fourni par Multitel (ou votre fichier de librairie interne).
- Une fois chargé, les modèles apparaîtront sous Available Library Scripts.

4.8.2.2 Librairie de Scripts disponibles

La liste Available Library Scripts affiche tous les modèles inclus dans la librairie chargée.

- Chaque ligne représente un modèle de script (le nom du modèle peut inclure une version ou une date).
- Cliquer sur l'icône d'expansion (chevron à droite) pour afficher les détails du modèle (et son contenu, si disponible).
- Utiliser ces modèles comme référence ou point de départ lors de la configuration de computed data points ailleurs dans la plateforme.

4.8.2.3 Nettoyer la Library

- Cliquer sur Clear pour retirer les modèles de scripts actuellement chargés de la page.
- Après l'effacement, la liste Available Library Scripts sera vide jusqu'à ce qu'un nouveau fichier de librairie soit chargé.

⚠ **Note :** L'effacement de la librairie retire uniquement les modèles actuellement chargés de l'interface. Si vous devez restaurer les modèles, rechargez le fichier de librairie en utilisant Select Library File.
⚠ **Recommendation :** Maintenir une librairie de scripts contrôlée et versionnée (avec des noms de modèles incluant une date/une version) pour assurer un comportement cohérent entre les dispositifs et simplifier le dépannage et le support.

4.8.3 SOFTWARE UPDATE

Cette section est utilisée pour téléverser une version logicielle sur le dispositif iO.
⚠ **Note :** Le processus de Software Update et le processus d'OS Update sont identiques.

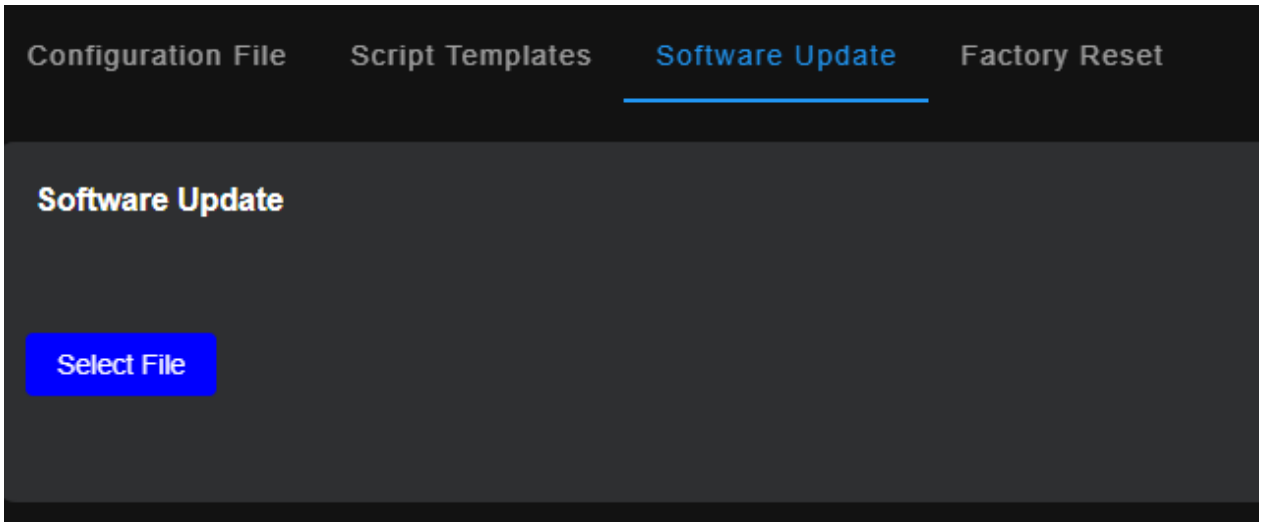


Figure 85: Maintenance du système – Software Update

Avant de commencer une mise à jour, assurez-vous qu'aucun utilisateur n'effectue d'opérations manuelles.

- Dans Settings | System Maintenance, cliquer sur l'onglet Software Update.
- Cliquer sur Select File.
- Sélectionner le fichier de mise à jour fourni par Multitel.
- Démarrer le téléversement.
- Redémarrer.

Le téléversement et l'installation de la mise à jour peuvent prendre quelques minutes. Le dispositif peut redémarrer durant le processus. Un message de confirmation ou d'erreur sera affiché lorsque le processus sera terminé.

⚠ **Avertissement:**
Ne pas éteindre le dispositif pendant le processus de mise à jour. Interrompre une mise à jour peut corrompre le système et peut briser l'unité, la rendant instable, inaccessible ou nécessitant un service de récupération. Le dispositif peut également être

inaccessible pendant quelques minutes durant la mise à jour, en particulier si les services réseau redémarrent ou si l'unité redémarre.

⚠ **Recommandation:**
Multitel recommande d'effectuer les mises à jour durant une fenêtre de maintenance et de s'assurer que vous disposez d'une alimentation stable. Si le dispositif est accessible à distance, prévoyez une perte temporaire de connectivité durant la mise à jour et assurez-vous d'avoir une méthode d'accès alternative si nécessaire.

4.8.4 FACTORY RESET

Cette section est utilisée pour effectuer une réinitialisation usine sur le dispositif iO.

Figure 86: Maintenance du système – Factory Reset

Avant d'effectuer une réinitialisation usine, assurez-vous qu'aucun utilisateur n'effectue d'opérations manuelles.

- Dans Settings | System Maintenance, cliquer sur l'onglet Factory Reset.
- Sélectionner les options de réinitialisation selon les besoins :
  - **Reset Ethernet** (restaure les paramètres Ethernet/réseau à leurs valeurs par défaut)
  - **Reset HMI** (supprime toutes les vues HMI)

- Cliquer sur Reset Now.

La réinitialisation usine peut prendre quelques minutes. Le dispositif peut redémarrer durant le processus.

⚠ **Avertissement:**
Une réinitialisation usine est irréversible. Selon les options sélectionnées, elle peut restaurer les paramètres de configuration à leurs valeurs par défaut et peut affecter l'accès à distance au dispositif (par ex., si les paramètres réseau sont réinitialisés).

⚠ **Recommandation:**
Multitel recommande d'exporter une sauvegarde de la configuration avant d'effectuer une réinitialisation usine. Si le dispositif est géré à distance, assurez-vous d'avoir un accès

physique (ou une méthode d'accès alternative) au cas où les paramètres réseau seraient réinitialisés.

4.9 REBOOT

Le paramètre Reboot est accessible à partir du module Settings.

Figure 87: Paramètres – Reboot

4.10 GLOBAL PARAMETERS

4.10.1 VUE D'ENSEMBLE GLOBAL PARAMETERS

La page Global Parameters permet d'afficher et de gérer les paramètres globaux du système qui s'appliquent à l'ensemble du dispositif/de l'application (et non à un asset spécifique). Ces paramètres sont généralement utilisés pour contrôler des comportements communs tels que les basculements de fonctionnalités, les options de planification/automatisation, les valeurs par défaut et les seuils opérationnels.

4.10.2 CONFIGURATION GLOBAL PARAMETERS

Pour configurer les binary labels :

- Aller dans Settings.
- Aller dans Global Parameters.
- Cliquer sur + Global Parameter pour créer un nouveau global parameter.

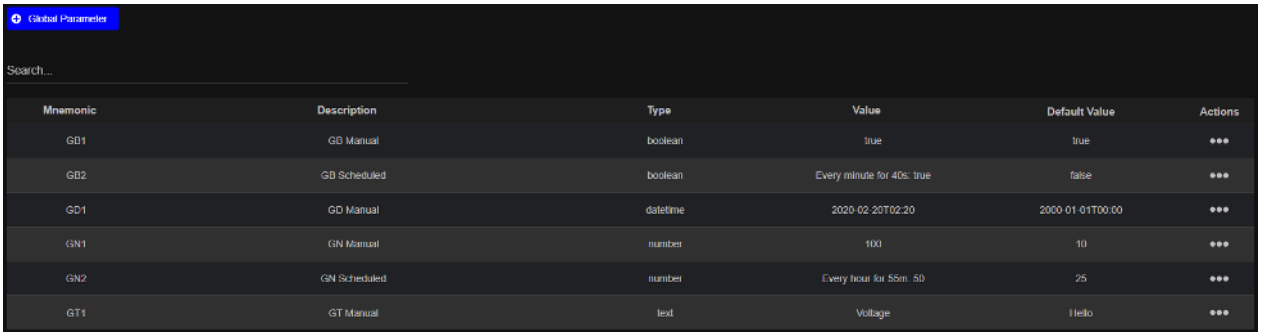


Figure 88: Global Parameters – Configuration

Tableau 34: Global Parameters – Configuration

Champ	Description	Spécification	Obligatoire
Mnemonic	Identifiant unique.	Auto Généré • Boolean: GBxx • Number: GNxx • Text: GTxx • Date: GDxx	
Description	Nom expliquant ce que le paramètre contrôle.	1 à 50 caractères	Oui
Type	Format de valeur attendu.	Lista déroulante: • Boolean • Number • Text • Date and Time	Oui
Value	Valeur actuellement active utilisée par le système.		Oui
Default Value	Valeur originale ou recommandée pour référence.		Oui
Actions	Ouvre le menu des options du paramètre.	Menu: • Set Value • Edit • Delete	

L'écran Add or Edit Global Parameter est utilisé pour modifier un global parameter existant et définir comment sa valeur se comporte dans le temps. Selon le type de paramètre, vous pouvez configurer une valeur par défaut fixe ou créer une ou plusieurs règles programmées qui appliquent automatiquement une valeur de manière récurrente.

Le format des champs Default Value et Value dépend du type sélectionné :

- **Boolean :** True ou False
- **Number :** Number
- **Text :** String
- **Date and Time :** Date et heure au format aaaa-mm-jj --:--

4.10.2.1 Ajouter ou éditer Global Parameter – Mode Single Value

Le mode Single Value est utilisé pour les global parameters qui doivent conserver une valeur constante en tout temps (sans planification). C'est la manière la plus simple de configurer un paramètre tel qu'un libellé texte, un seuil numérique ou un réglage basique on/off.

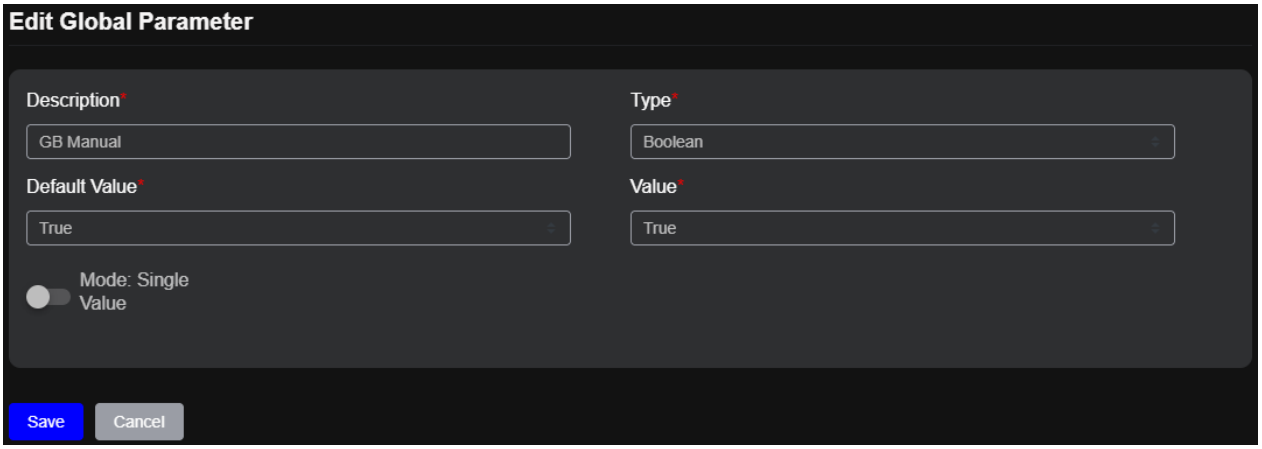


Figure 89: Global Parameters – Mode Single Value

Dans ce cas, une valeur doit être saisie dans les champs Default Value et Value.

- **Default Value :** Il s'agit de la valeur de référence pour ce paramètre. Elle peut être utilisée comme valeur de base ou valeur de réinitialisation, selon le comportement du système.
- **Value :** Il s'agit de la valeur active actuellement appliquée par le système. C'est la valeur qui sera utilisée immédiatement une fois enregistrée.

4.10.2.2 Ajouter ou éditer Global Parameter – Mode Scheduled

Le mode Scheduled est utilisé pour les global parameters qui doivent appliquer des valeurs automatiquement selon une planification récurrente.

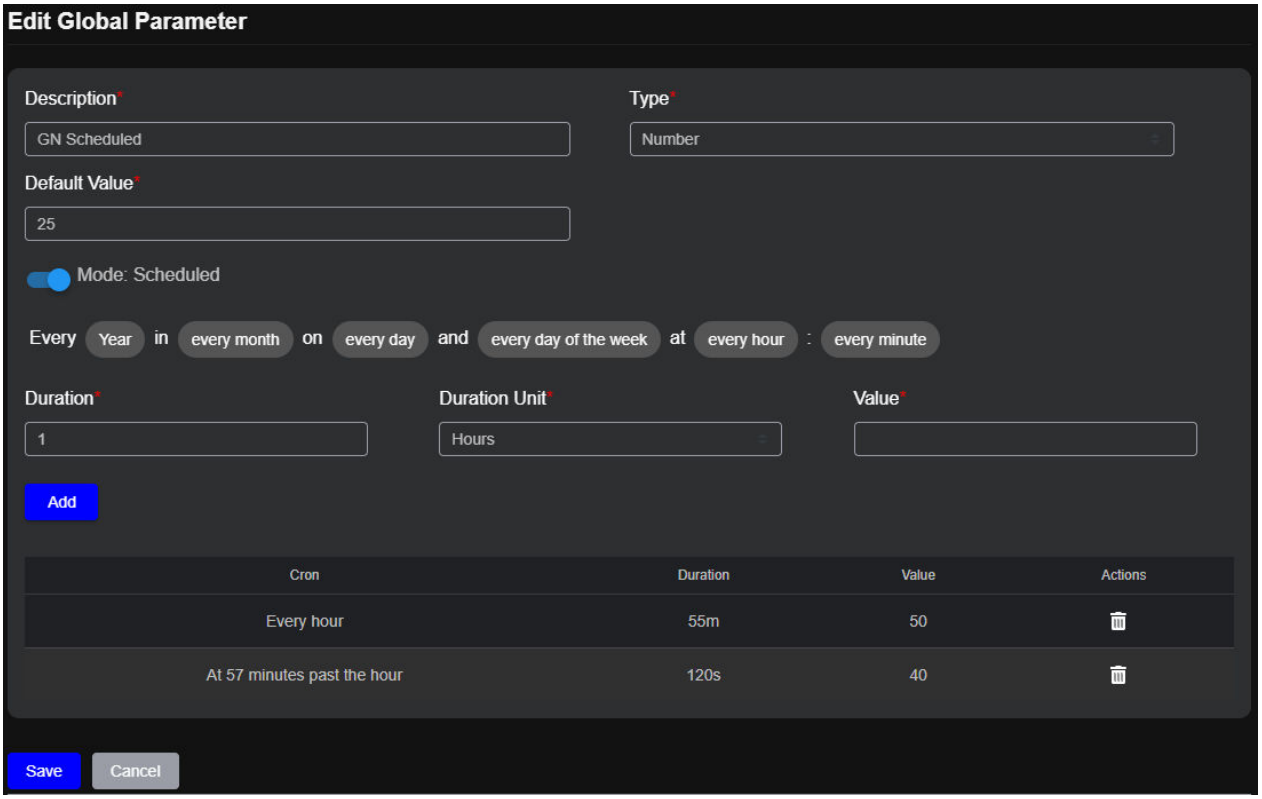


Figure 90: Global Parameters – Mode Scheduled

Lorsque le mode Scheduled est activé, vous pouvez définir des règles en utilisant les éléments suivants :

- **Every :** Sélecteur de récurrence (par ex., every year, month, day, hour, minute).
- **Duration :** Durée pendant laquelle la règle reste active une fois qu'elle commence.
- **Duration Unit :** Unité de durée (par ex., hours, minutes, days).
- **Value :** La valeur à appliquer pendant la période active de la règle.

Cliquer sur le bouton **Add** pour créer la règle et l'ajouter à la liste de planification.

Toutes les règles créées apparaissent dans un tableau affichant les éléments suivants :

- **Cron :** Le modèle de récurrence de la règle.
- **Duration :** La durée pendant laquelle la règle reste active.
- **Value :** La valeur appliquée pendant cette période.
- **Actions :** Supprimer une règle (icône de poubelle).