



## *NOTICE IPEVIA MANAGER*



## Table des matières

|                                                            |           |
|------------------------------------------------------------|-----------|
| <b>1. Utilisation courante du logiciel</b>                 | <b>5</b>  |
| 1.1. Mode local                                            | 5         |
| Prérequis                                                  | 5         |
| Téléchargement de Ipevia manager                           | 5         |
| Setup.exe                                                  | 6         |
| Créer un compte admin                                      | 8         |
| 1.2. Mode en ligne                                         | 11        |
| <b>2. Assistant de création de site</b>                    | <b>12</b> |
| 2.1. Site                                                  | 12        |
| 2.2. Fonctionnalités                                       | 14        |
| 2.3. Fonctionnalités avancées                              | 16        |
| 2.4. Réseaux                                               | 17        |
| 2.5. Architecture                                          | 19        |
| 2.6. Centrales                                             | 23        |
| 2.7. Portes                                                | 24        |
| 2.8. Ascenseur                                             | 25        |
| Programmation                                              | 26        |
| 2.9. Zones                                                 | 28        |
| 2.10. Profil d'accès                                       | 29        |
| 2.11. Badges                                               | 29        |
| 2.12. Lire/encoder                                         | 31        |
| <b>3. Matériel et paramétrage</b>                          | <b>32</b> |
| 3.1. Paramétrage des emails                                | 33        |
| 3.2. Utilisation de la multisociété                        | 34        |
| Activation de la fonction                                  | 35        |
| Créer une société                                          | 35        |
| Assigner une société aux appareils                         | 35        |
| Assigner une société au profil d'accès et aux utilisateurs | 37        |
| Accès à IPévia manager                                     | 38        |
| 3.3. Réseaux                                               | 41        |
| 3.4 Centrales                                              | 42        |

|                                                  |    |
|--------------------------------------------------|----|
| 3.5. Portes .....                                | 44 |
| 3.6 Lecteurs.....                                | 46 |
| Paramétrage standard .....                       | 47 |
| Lecteur ANPR .....                               | 48 |
| Serrures électroniques sécurisées .....          | 53 |
| Profils de lecteurs .....                        | 56 |
| 3.7. Ascenseurs.....                             | 57 |
| 3.8. Carte ES (entrée/sortie) .....              | 58 |
| 3.9. Entrées .....                               | 59 |
| Option d'adaptation de l'entrée .....            | 60 |
| 3.10 Sorties .....                               | 61 |
| 3.11 Anti-pass back (APB).....                   | 62 |
| Create a counting zone .....                     | 63 |
| 3.13. Horaires & périodes fériées/travaux.....   | 66 |
| Horaires d'accès .....                           | 67 |
| Horaires porte ou sortie.....                    | 67 |
| Horaires lecteur/porte.....                      | 68 |
| Horaires condition/processus .....               | 70 |
| Copier et coller des horaires .....              | 70 |
| Périodes fériées .....                           | 72 |
| 3.14. Serveurs vidéo.....                        | 73 |
| General.....                                     | 73 |
| Synoptique .....                                 | 73 |
| Choisir un logiciel de lecture RTSP .....        | 75 |
| Paramètres .....                                 | 76 |
| 4. Intrusion .....                               | 78 |
| 4.1. Intrusions par contacts secs .....          | 78 |
| Paramètres de zones .....                        | 78 |
| Paramétrage de l'intrusion par zone.....         | 79 |
| 4.2. Elkron/Médéa intrusion .....                | 80 |
| Prérequis .....                                  | 80 |
| Paramétrage général de l'intrusion par zone..... | 81 |
| 4.3. Paramètres communs de l'intrusion.....      | 82 |

|                                                             |            |
|-------------------------------------------------------------|------------|
| Intrusion selon horaire.....                                | 82         |
| Intrusion pour chaque zone.....                             | 83         |
| Profil de lecteurs pour l'intrusion .....                   | 84         |
| Lecteurs pour l'intrusion .....                             | 84         |
| Utilisateurs pilotant l'intrusion (par profil d'accès)..... | 85         |
| Départ tardif .....                                         | 87         |
| Suivi de l'intrusion par les événements .....               | 88         |
| Commandes manuelles de l'intrusion.....                     | 89         |
| <b>5. Profils d'accès et badges .....</b>                   | <b>93</b>  |
| 5.1. Profils d'accès porte .....                            | 93         |
| 5.2. Profil d'accès ascenseur .....                         | 94         |
| 5.3. Personnes sans accès.....                              | 95         |
| 5.4. Utilisateur .....                                      | 95         |
| <b>6. Monitoring .....</b>                                  | <b>99</b>  |
| 6.1 Événements .....                                        | 101        |
| 6.2 Etats réseaux .....                                     | 102        |
| 6.3 Commandes manuelles .....                               | 102        |
| 6.4 Reporting.....                                          | 103        |
| 6.5 Présence zones.....                                     | 105        |
| <b>7. Réservation.....</b>                                  | <b>106</b> |
| 7.1 Pré requis.....                                         | 106        |
| 7.2 Ajouter un bien réservable.....                         | 109        |
| Paramétrage global.....                                     | 109        |
| Paramétrage avancé.....                                     | 111        |
| Restrictions par période .....                              | 113        |
| Personnes.....                                              | 114        |
| Envoi de mails .....                                        | 114        |
| Actions.....                                                | 116        |
| Instructions .....                                          | 117        |
| 7.3 Gestion des réservations .....                          | 118        |
| <b>8. Gestion des visiteurs.....</b>                        | <b>119</b> |
| 8.1 Paramétrage des visiteurs .....                         | 119        |
| 8.2. Gestion des accès visiteurs .....                      | 123        |

|                                                                |     |
|----------------------------------------------------------------|-----|
| 8.2 Créer un profil visiteur.....                              | 125 |
| 8.4. create a visit .....                                      | 125 |
| Planifier une visite.....                                      | 126 |
| Créer une visite instantanée .....                             | 127 |
| 9. Utilisation avancée du logiciel .....                       | 128 |
| 9.1 Outil de modification automatique.....                     | 128 |
| Modification des informations de la centrale.....              | 128 |
| Modification de l'adresse IP de la centrale .....              | 129 |
| Modifications de l'entrée .....                                | 130 |
| Modifications de la sortie.....                                | 133 |
| 9.2 Outil de creation de personnes/de badges automatique ..... | 134 |
| 9.3 Commandes d'urgence.....                                   | 136 |
| 9.4 Relations .....                                            | 137 |
| Qu'est-ce qu'une relation .....                                | 137 |
| Comment configurer une relation .....                          | 137 |
| Limites de relations par IPevia .....                          | 139 |
| Autoriser les utilisateurs à créer des relations .....         | 139 |
| 9.5 message.....                                               | 140 |
| 10. Outils.....                                                | 141 |
| 10.1 Mise à jour firmware .....                                | 142 |
| 10.2 journal .....                                             | 143 |
| 10.3 sauvegarder/restaurer .....                               | 143 |
| 10.4 Restaurer (fichier d'import site).....                    | 144 |
| 10.5 tâches planifiées.....                                    | 145 |
| 10.6 controller detection .....                                | 145 |
| 11. Gestion des opérateurs.....                                | 147 |
| 11.1 Ajouter un groupe d'utilisateur .....                     | 147 |
| 11.2 Ajouter, modifier un opérateur .....                      | 148 |
| 12 Intégration.....                                            | 149 |
| 12.1 Import automatique/import de fichier type .....           | 149 |
| 12.2 Import manuel.....                                        | 151 |
| 12.3 Importer avec une tâche automatique.....                  | 152 |
| 12.4 Importer avec des commandes externes .....                | 153 |

# 1. Utilisation courante du logiciel

Ipévia Manager peut être utilisé soit en mode en ligne, soit en mode local. Le mode local nécessite le téléchargement du fichier .exe sur le site Web d'IPévia. Quant à la version en ligne, elle nécessite uniquement un compte pour se connecter.

## 1.1. Mode local

### Prérequis

La configuration prérequis est :

- Processeur quad-core processor > 3ghz (Intel Core i5 like)
- 8Go de Ram
- Système d'exploitation : Windows 11
- 10Go disponible sur HDD ou SSD
- Carte réseau card 100/1Go
- Connexion internet pour recevoir/envoyer des mails et mettre à jour l'application si nécessaire.

Par défaut, la configuration TCP/IP du contrôleur IPévia est définie sur DHCP. Cela signifie que, lors du démarrage de la centrale, le système demande une adresse au serveur DHCP. Si aucune adresse n'est saisie, le système utilisera les paramètres suivants :

IP Address: 192.168.1.250

Mask: 255.255.255.0

gateway: aucune information renseignée

Lorsque la centrale est correctement connectée au PC ou avec une IP, mais sans serveur DHCP, l'ordinateur doit être configuré comme suit :

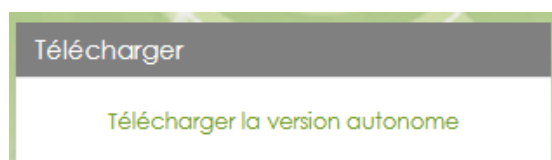
Adresse IP: 192.168.1.1

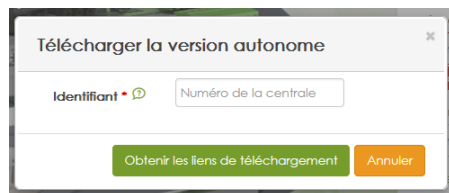
Masque: 255.255.255.0

Gateway: no information provided

### Téléchargement de Ipevia manager

Depuis le site <https://www.ipevia.com>, cliquez sur le bouton « Télécharger la version autonome ».

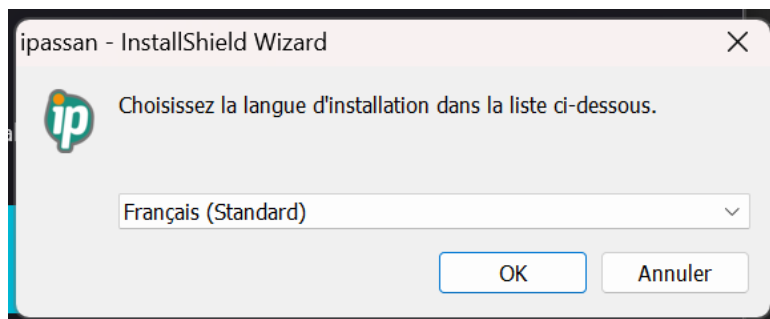




Sur l'écran suivant, saisissez un numéro de contrôleur valide (il commence par 54Cxxxxxx).

Ensuite, le téléchargement de l'exécutable IPévia Manager démarre (le fichier pèse environ 500 Mo). Cliquez dessus une fois terminé pour lancer l'installation.

## Setup.exe



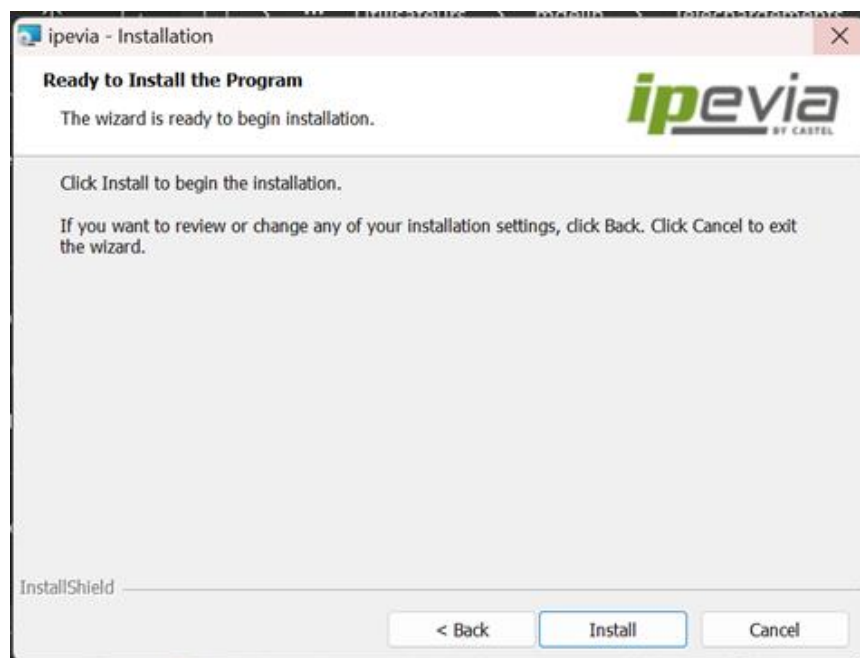
Lancez l'exécutable. Sélectionnez la langue, puis cliquez sur « OK ».



Click on « Next ».



Sélectionnez le répertoire où installer le logiciel et cliquez sur « Suivant ». Puis choisissez « Installer » en bas de la page suivante.



En cliquant sur le bouton « Installer », le système demandera quel navigateur Internet vous souhaitez utiliser pour créer votre compte administrateur. Ce navigateur sera utilisé définitivement pour lancer IPévia Manager, même en mode local.

## Créer un compte admin

Une fois l'installation d'IPévia terminée, l'étape suivante consiste à créer un compte administrateur. Lors du premier lancement d'IPévia Manager, le système demande quel navigateur utiliser pour exécuter IPévia Manager. Il est à noter que le programme fonctionne avec un navigateur Internet même en mode local.

En cliquant sur le navigateur de votre choix, vous serez redirigé vers l'adresse suivante : <https://127.0.0.1:8443/ipevia/?login>. Notez que l'adresse IP « 127.0.0.1 » est l'adresse de boucle locale. Elle est utilisée par l'ordinateur pour se référer à lui-même. Elle est également connue sous le nom de localhost.

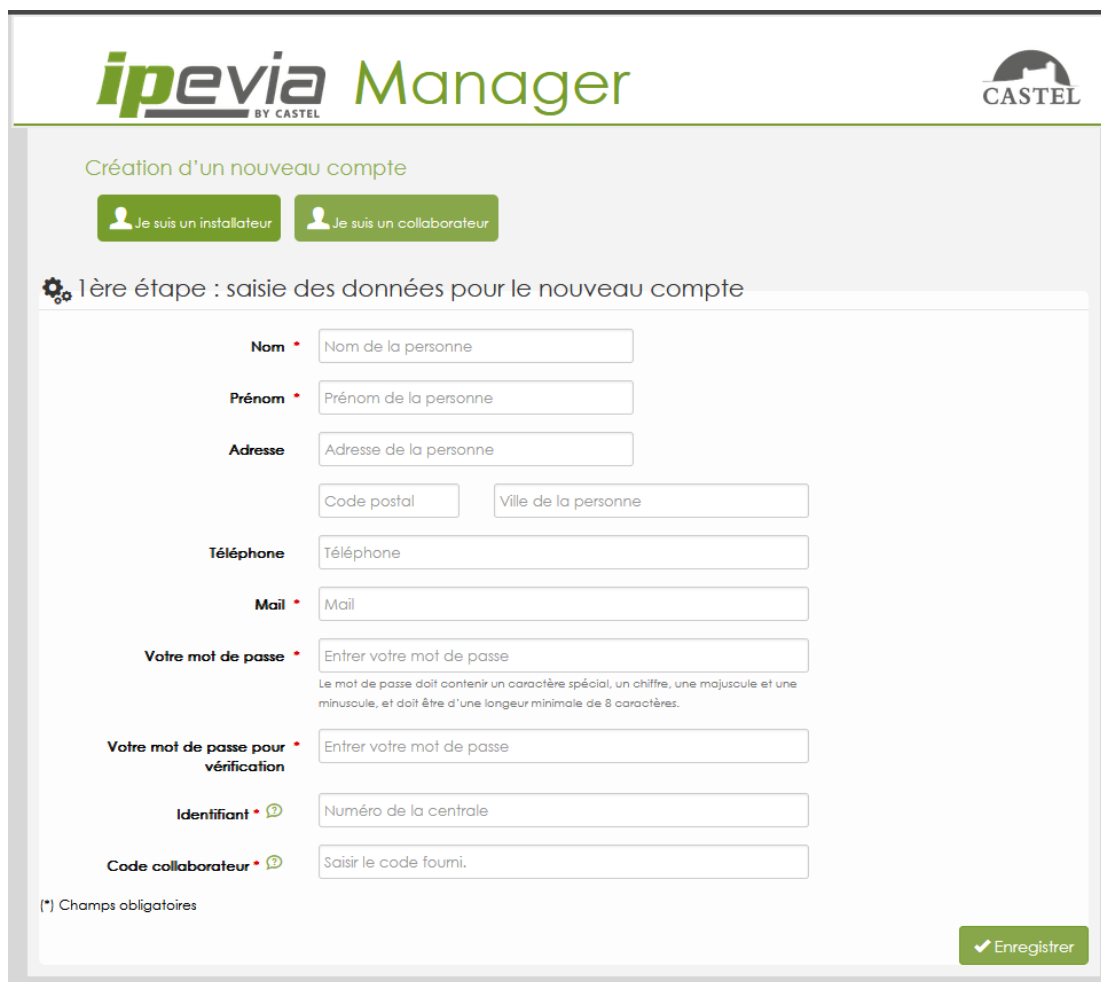


Si vous n'avez pas encore créé de compte, cliquez sur le bouton « Créer un compte ».

Sur l'écran suivant, entrez votre prénom, nom, numéro de téléphone et mot de passe, puis cliquez sur le bouton « Enregistrer ».

Selon que vous soyez installateur ou résident, vous pouvez cliquer sur le bouton en haut de la page. Cela modifie les champs qui peuvent être remplis en dessous.

Voir la capture d'écran ci-dessous si vous cliquez sur le bouton « Je suis un installateur » :



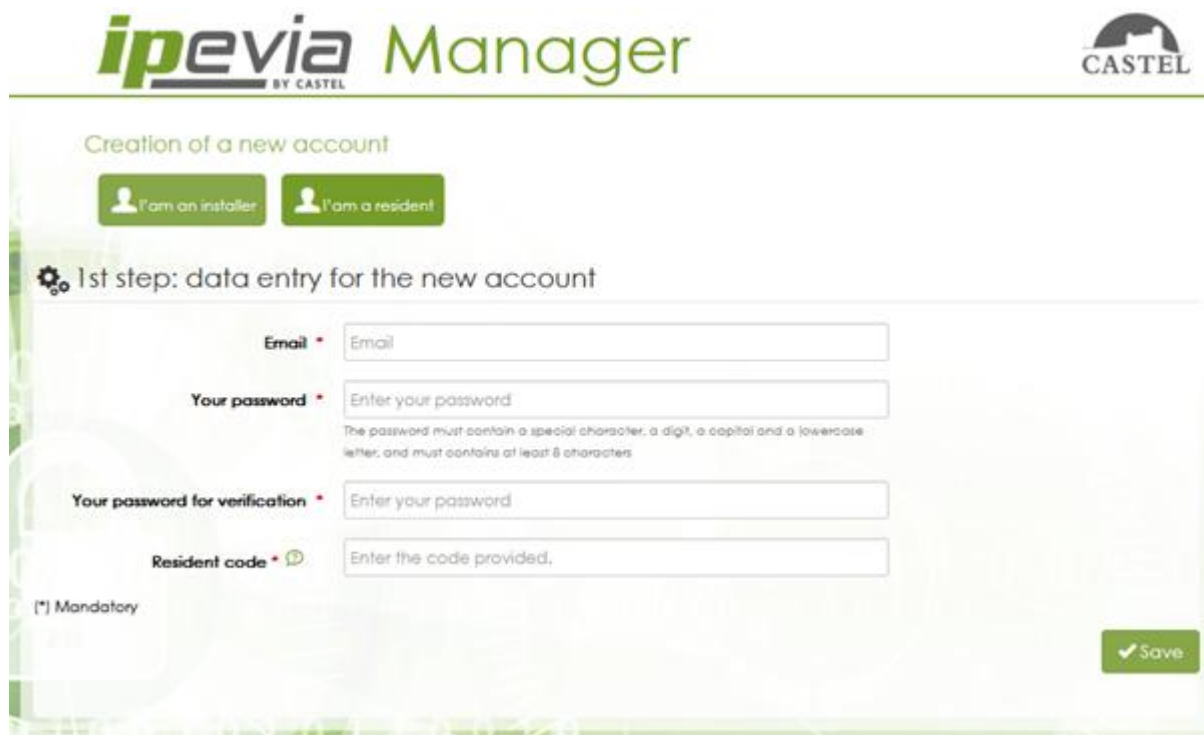
The screenshot shows the 'Création d'un nouveau compte' (Create a new account) page in the Ipevia Manager interface. At the top, there are two buttons: 'Je suis un installateur' (I am an installer) and 'Je suis un collaborateur' (I am a collaborator). Below these, a gear icon indicates the '1ère étape : saisie des données pour le nouveau compte' (1st step: data entry for the new account).

The form contains the following fields:

- Nom \***: Nom de la personne
- Prénom \***: Prénom de la personne
- Adresse**: Adresse de la personne
- Code postal**: Code postal
- Ville de la personne**: Ville de la personne
- Téléphone**: Téléphone
- Mail \***: Mail
- Votre mot de passe \***: Entrer votre mot de passe. A note below states: 'Le mot de passe doit contenir un caractère spécial, un chiffre, une majuscule et une minuscule, et doit être d'une longueur minimale de 8 caractères.'
- Votre mot de passe pour vérification \***: Entrer votre mot de passe
- Identifiant \*** (with a key icon): Numéro de la centrale
- Code collaborateur \*** (with a key icon): Saisir le code fourni.

At the bottom left, a note says '(\*) Champs obligatoires' (Mandatory fields). At the bottom right, there is a green button labeled '✓ Enregistrer' (Save).

Voir la capture d'écran ci-dessous si « Je suis un installateur » est sélectionné.



**ipevia Manager** BY CASTEL

Creation of a new account

1st step: data entry for the new account

Email \*

Your password \*   
The password must contain a special character, a digit, a capital and a lowercase letter, and must contains at least 8 characters

Your password for verification \*

Resident code \*

(\*) Mandatory

Veuillez patienter quelques secondes pendant que le système traite la création du compte administrateur.



**ipevia Manager** BY CASTEL

Création d'un nouveau compte

2ème étape : création de votre base de données

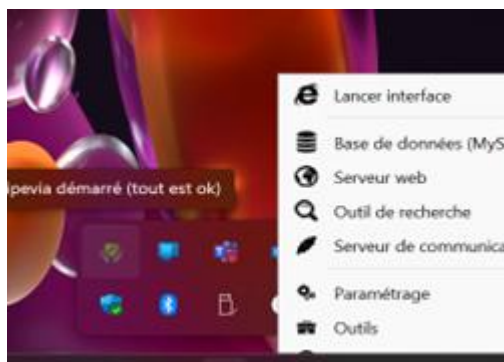
|           |                                                                                            |
|-----------|--------------------------------------------------------------------------------------------|
| Nom       | Maxime                                                                                     |
| Prénom    | GELIN                                                                                      |
| Adresse   | 110 rue Pierre Gilles de Genne<br>49300 Cholet                                             |
| Téléphone |                                                                                            |
| Mail      | fdi.mgelin@gmail.com<br><small>L'adresse email vous servira de login de connexion.</small> |

Votre compte est validé  
 Installation de la base de données  
 Veuillez patienter pendant l'installation.  
 Info : Création de la base de données métier

100 %

Félicitations, IPévia Manager en mode local est installé sur votre ordinateur ! Un icône apparaît maintenant sur votre bureau. Selon le système d'exploitation, cet icône peut être automatiquement nommé « NouveauRaccourci 1 ». N'hésitez pas à le renommer comme bon vous semble.

Vous pouvez lancer le logiciel avec le raccourci en bas à droite de la barre des tâches.



Un clic gauche sur l'icône ouvre le menu.

Sélectionnez « Lancer l'interface » pour ouvrir le logiciel.

Le logiciel est compatible avec Microsoft Edge, Mozilla ou Chrome.

## 1.2. Mode en ligne

Vous pouvez accéder à IPévia Manager avec sa version en ligne. Entrez l'adresse <https://www.ipevia.com> dans votre navigateur web ou recherchez « Ipevia Manager ».



Si vous n'avez pas encore de compte, cliquez sur le bouton « Créer un compte » en haut à droite de la page. Entrez votre identifiant et votre mot de passe pour vous connecter à IPévia Manager.

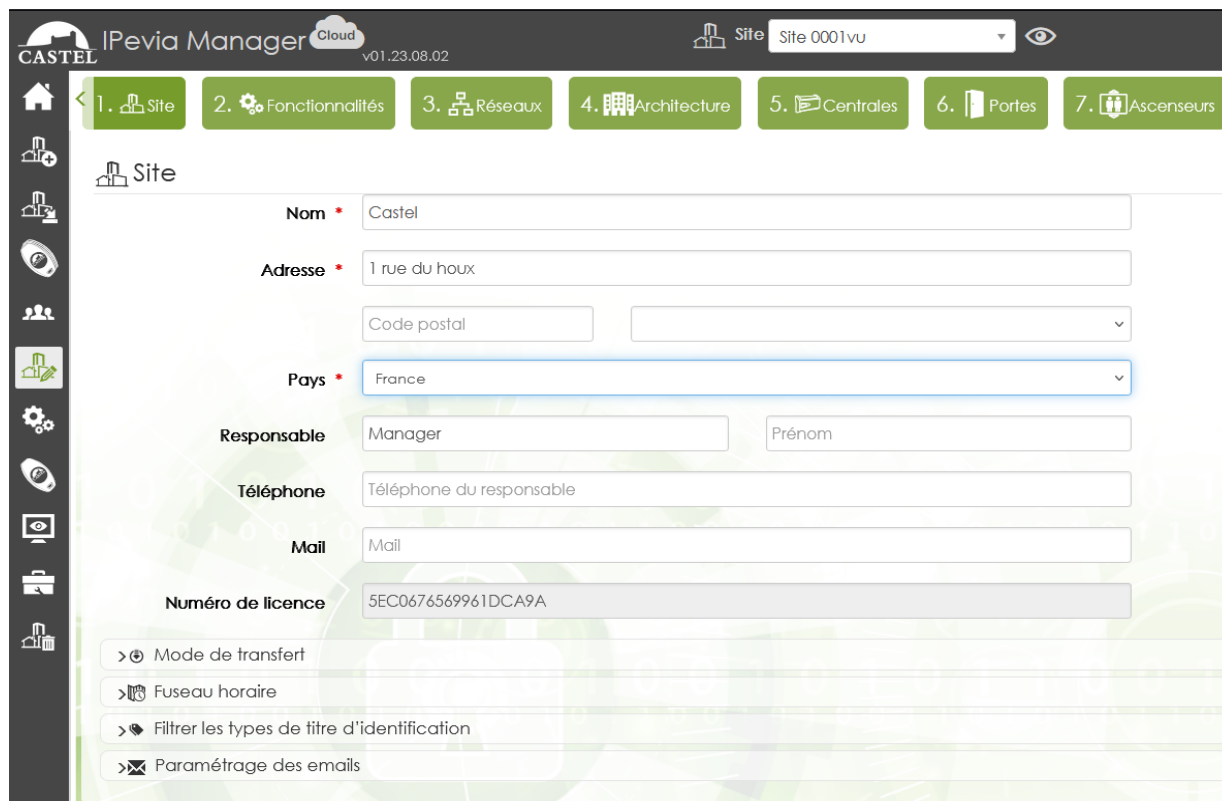
## 2. Assistant de création de site

Cliquez sur le bouton « Créer un nouveau site » sur la page principale. Un assistant vous guidera à travers le processus de création du site étape par étape.

### 2.1. Site

La première étape consiste à définir le site :

- Nom, coordonnées de la personne responsable, etc.
- Fuseau horaire
- Types de clés utilisées
  - o Clé de proximité / télécommande
  - o 13,56 MHz / 125 kHz



CASTEL Ipevia Manager Cloud v01.23.08.02 Site Site 0001vu

1. Site 2. Fonctionnalités 3. Réseaux 4. Architecture 5. Centrales 6. Portes 7. Ascenseurs

Site

Nom \* Castel

Adresse \* 1 rue du houx

Code postal

Pays \* France

Responsable Manager Prénom

Téléphone Téléphone du responsable

Mail Mail

Numéro de licence 5EC0676569961DCA9A

> Mode de transfert

> Fuseau horaire

> Filtrer les types de titre d'identification

> Paramétrage des emails

**Mode de transfert :**

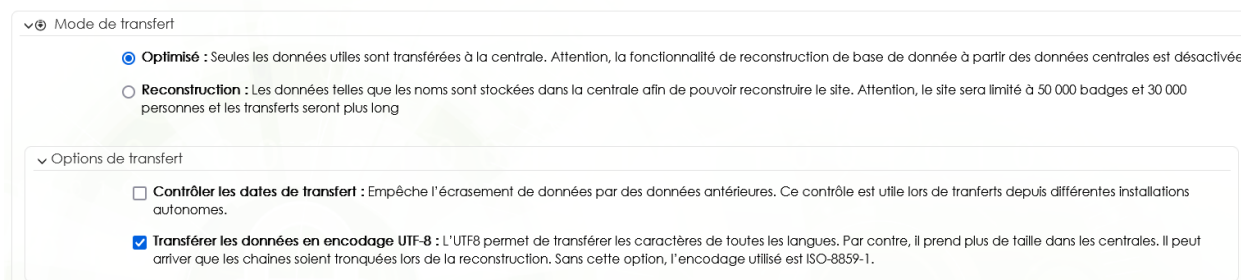
Le logiciel propose deux modes pour l'envoi des données vers les contrôleurs :

- **Optimisé** : le serveur transfère uniquement les données nécessaires au traitement du contrôle d'accès vers les contrôleurs. Le contrôleur ne connaît pas le nom de la porte ni de l'utilisateur, car il n'a pas besoin de ces informations pour autoriser ou refuser l'accès à la porte. Ce mode de transfert est appelé « optimisé » car il est plus rapide. Les données inutiles ne sont pas transmises sur les bus de communication.
- **Reconstruction** : le serveur transfère autant de données que possible vers les contrôleurs. Cela inclut les noms d'utilisateurs, les noms des portes, les profils d'accès, les noms des horaires, etc. Ce mode entraîne des temps de transfert plus longs. En retour, toutes les informations sont disponibles dans les contrôleurs en cas de reconstruction vers le même serveur ou un autre serveur.

Note: The default option for the cloud server is "Optimized," as data backup is natively managed.

In local servers, the default option is "Reconstruction," which allows the site to be rebuilt on another PC in case of theft or destruction of data on the original server.

At any time, it is possible to switch from one mode to another. In this case, a complete transfer of the site's data is required.

**Transfer options**

Mode de transfert

☒ **Optimisé** : Seules les données utiles sont transférées à la centrale. Attention, la fonctionnalité de reconstruction de base de donnée à partir des données centrales est désactivée

☐ **Reconstruction** : Les données telles que les noms sont stockées dans la centrale afin de pouvoir reconstruire le site. Attention, le site sera limité à 50 000 badges et 30 000 personnes et les transferts seront plus long

Options de transfert

☐ **Contrôler les dates de transfert** : Empêche l'écrasement de données par des données antérieures. Ce contrôle est utile lors de transferts depuis différentes installations autonomes.

☒ **Transférer les données en encodage UTF-8** : L'UTF8 permet de transférer les caractères de toutes les langues. Par contre, il prend plus de taille dans les centrales. Il peut arriver que les chaînes soient tronquées lors de la reconstruction. Sans cette option, l'encodage utilisé est ISO-8859-1.

**Vérifier les dates de transfert** : le serveur enregistre systématiquement les dates et heures de la dernière mise à jour dans les contrôleurs. Lorsque cette case est cochée, le serveur compare sa propre date de dernière mise à jour avec celle de chaque contrôleur.

- Si ces dates ne correspondent pas, cela signifie que le serveur a été mis à jour après le contrôleur. Le système proposera alors de forcer la mise à jour du contrôleur.
- Si la date et l'heure de la mise à jour sont plus récentes dans un ou plusieurs contrôleurs que sur le serveur, cela peut indiquer qu'un autre PC/serveur a été utilisé sur le site. Le serveur proposera alors de reconstruire le site à partir des contrôleurs vers le serveur.

**Transférer les données en UTF8** : Cette option est nécessaire lorsque les interphones doivent afficher des caractères spéciaux (par exemple, l'alphabet norvégien).

**Identifiants** : Le logiciel gère plusieurs types d'identifiants (physiques et non physiques).

✓  Filtrer les types de titre d'identification

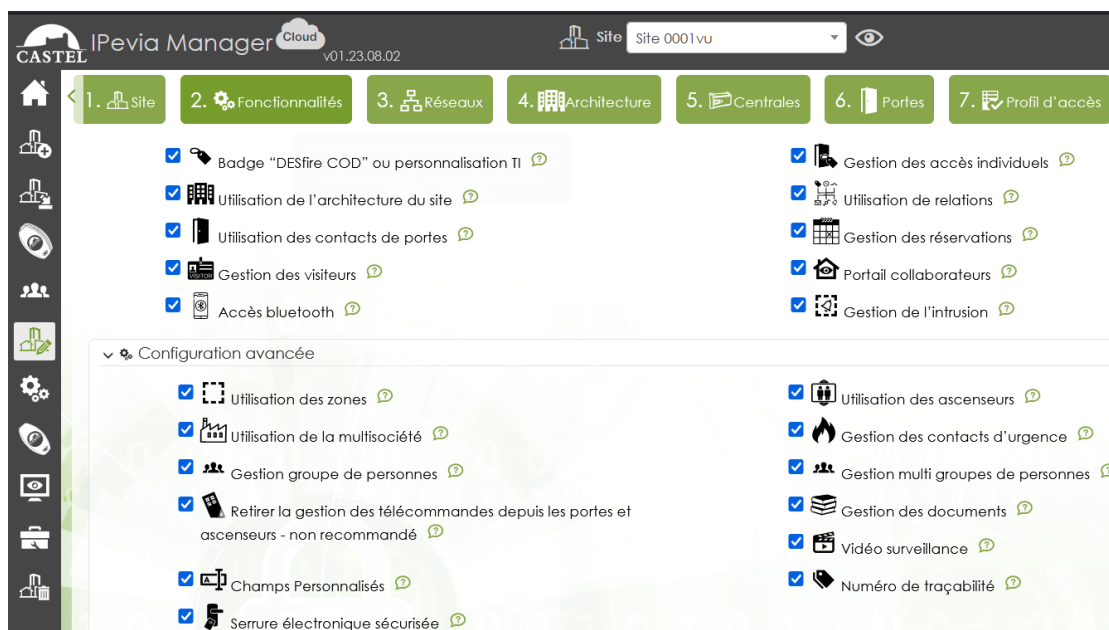
- |                                                                                                                                               |                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/>  Badge 1356 propriétaire | <input type="checkbox"/>  Universel (Hexa)              |
| <input type="checkbox"/>  Universel (Numérique)              | <input type="checkbox"/>  Badge 125 k                   |
| <input type="checkbox"/>  Badge Mifare+                      | <input type="checkbox"/>  Télécommande 1356 - 4 boutons |
| <input type="checkbox"/>  Télécommande 125K - 2/4 boutons    | <input type="checkbox"/>  Télécommande Mifare+ - 4btns  |
| <input type="checkbox"/>  Télécommande 1356 - 2 boutons      | <input type="checkbox"/>  Code clavier                  |
| <input type="checkbox"/>  Plaque d'immatriculation           | <input checked="" type="checkbox"/>  Bluetooth          |
| <input type="checkbox"/>  QRCode                             | <input type="checkbox"/>  Autre (Numérique inversé)     |

- **Clé de proximité 1356** : ce sont des clés 13,56 MHz et des télécommandes avec 8 caractères hexadécimaux.
- **Clé de proximité 125K** : technologie plus ancienne pour les clés et télécommandes. Les clés commencent généralement par 00xxxxxx, et les télécommandes sont gravées en décimal avec 8 chiffres commençant par 9.
- **Télécommande Mifare** : la dernière génération de clés et de télécommandes avec 14 caractères hexadécimaux.
- **Code d'accès** : De 3 à 8 chiffres.
- **Numéro de plaque** : IPévia s'intègre avec les systèmes de reconnaissance de plaques d'immatriculation. Dans ce cas, l'intégration est considérée comme "intelligente" car la caméra ou le logiciel OCR (reconnaissance optique de caractères) communique le numéro de plaque d'immatriculation au contrôleur IPévia en texte intégral. Il ne s'agit pas d'une conversion Wiegand.
- **Autre Hexadécimal ou Décimal** : utile lors de l'utilisation de lecteurs et de clés d'un système de contrôle d'accès précédent. Les badges peuvent être gravés en décimal.
- **Codes QR** : Le logiciel peut générer des codes QR, qui peuvent être utilisés dans la gestion des visiteurs, par exemple.

## 2.2. Fonctionnalités

Dans la deuxième étape, nous sélectionnons les fonctionnalités pertinentes pour ce bâtiment que nous souhaitons configurer à l'aide du logiciel IPévia. Le logiciel est conçu pour être aussi convivial que possible tout en permettant la gestion de fonctionnalités avancées.

Exemple : l'utilisateur qui ne gère pas les zones de comptage ou l'anti-pass back (APB) ne cocherait pas l'option à cette étape. Pour les étapes suivantes, IPévia ne demandera pas à l'utilisateur de saisir les critères liés à cette fonctionnalité.



- **Gestion des accès individuels** : permet d'importer une configuration de badge personnalisée depuis CastelEvoWeb.
- **Badge « desfire COD » ou personnalisation TI** : permet d'exploiter le badge sécurisé DesFire COD sur le site ou permet d'utiliser tout type d'identification personnalisé créé sur la plateforme Castel Evo Web.
- **Utilisation de l'architecture du site** (voir le chapitre Concept d'architecture)
- **Utilisation des contacts de porte** : le contact de porte est natif de l'unité centrale. Il permet de détecter les événements suivants : porte ouverte, porte forcée, porte ouverte trop longtemps...  
Si ces contacts de porte ne sont pas utilisés sur le site, ne cochez pas cette option.
- **Gestion des visiteurs** : les gestionnaires ou les employés peuvent eux-mêmes ajouter un visiteur (ou gérer sa visite) via le portail résident. Ces visiteurs ont accès à la bonne porte ou au bon étage.
- **Accès Bluetooth** : les utilisateurs peuvent accéder aux biens avec leur smartphone. Ils doivent d'abord télécharger l'application « Castel virtual card ». Leur accès Bluetooth doit être saisi dans le logiciel.
- **Utilisation de relations** : un réflexe lie les processus aux conditions. Par exemple, un relais est activé lorsqu'une porte est forcée.
- **Gestion des réservations** : vous pouvez gérer la réservation des biens ou équipements avec le logiciel. Le gestionnaire ou l'employé peut réserver une salle via un portail dédié.
- **Portail collaborateurs** : vos employés ont accès à une version allégée du logiciel. Il est réactif (s'adapte à toutes les tailles d'écran). L'utilisateur peut réserver des biens/équipements, gérer ses visiteurs ou piloter une porte/l'intrusion..
- **Intrusion** : disponible avec la version de firmware fV3230. Le logiciel gère l'intrusion en lien avec les contrôleurs Elkron Medea. En définissant des zones et des lecteurs, le titre d'accès peut désactiver ou activer la gestion de l'intrusion définie dans le contrôleur Medea. Ipévia peut gérer jusqu'à 1 contrôleur Medea par réseau de contrôleur. Ces deux dispositifs doivent être câblés sur le même réseau IP.

## 2.3. Fonctionnalités avancées

**Utilisation des zones:** Les zones du système permettent de gérer le comptage global ou basé sur des groupes. Elles aident également à gérer l'anti-pass back et la présence dans les zones. Si le site n'utilise pas de zones, ne cochez pas cette option.

**Gestion des ascenseurs :** cette option permet de contrôler jusqu'à 110 étages depuis un lecteur. Notez que l'activation de la gestion des ascenseurs active automatiquement l'utilisation de l'architecture (voir le chapitre "Notion d'Architecture").

Ipévia gère les ascenseurs conventionnels (via des contacts secs) ainsi que les ascenseurs intelligents via une communication TCP/IP. Cela inclut deux systèmes du fabricant Kone : le COP (Car Operating Panel) et le DOP (Destination Operating Panel).

- **Dans le COP**, le lecteur est dans la cabine de l'ascenseur et est de la marque FDI. Le panneau de contrôle communique les étages autorisés au contrôleur Kone via une connexion TCP/IP chaque fois qu'un badge valide est présenté.
- **Dans le DOP**, le lecteur est à l'extérieur de l'ascenseur. L'utilisateur badgera et entre ensuite son étage de destination. Le panneau Kone indique quelle cabine d'ascenseur utiliser.  
Dans le système DOP, plusieurs utilisateurs se dirigeant vers le même étage en même temps sont dirigés vers la même cabine. Cela est conçu pour transporter plus de personnes dans le même créneau horaire, consommant ainsi moins d'énergie.

**Utiliser des multi-sociétés :** cette fonctionnalité permet la gestion d'un site occupé par différentes entreprises, où chaque entreprise peut uniquement voir ses propres zones. Seuls les administrateurs du site ont une visibilité complète.

Par exemple, dans un immeuble de bureaux, les portes communes sont utilisées par toutes les entreprises. Chaque opérateur du logiciel gère l'accès à ces zones communes pour ses propres employés, sans voir d'autres utilisateurs, portes ou profils d'accès spécifiques à d'autres entreprises.

**Gestion des contacts d'urgence :** un contact d'urgence permet de déverrouiller une ou plusieurs portes si une entrée est active. Il est généralement déclenché par une alarme incendie.

**Gestion groupe de personnes :** le logiciel propose un tri par défaut des clés et des utilisateurs par profil d'accès. Pour les sites résidentiels, le logiciel offre également une vue par bâtiments, étages et appartements. En plus de ces deux options de tri, IPévia Manager permet la création de groupes d'utilisateurs, tels qu'un département dans une entreprise ou une classe dans une école, etc.

**Gestion multi groupes de personnes :** cette fonctionnalité trouve des applications telles que le partage d'un parking entre plusieurs entités ou la gestion d'un immeuble résidentiel où une partie est supervisée par une société de gestion immobilière et l'autre partie par un bailleur social.

**Retirer la gestion des télécommandes pour les portes et les ascenseurs** : non recommandé.

**Gestion des documents** : Ipévia Manager permet le stockage de documents tels qu'un permis de conduire, un certificat d'assurance, etc.

**Champs personnalisés** : le logiciel gère des champs tels que le nom, le prénom, l'email, etc., pour les utilisateurs. Lorsque l'administrateur nécessite des champs supplémentaires, il a la possibilité de créer ces champs et de définir le type, le format, etc. Ensuite, l'administrateur peut les ajouter au formulaire requis.

**Vidéo surveillance** : Ipévia intègre la vidéosurveillance via le protocole RTSP. Cette intégration permet de lier une ou plusieurs caméras à des portes spécifiques, des entrées, des sorties, des lecteurs, etc. Pour chaque événement (lié à une porte, une sortie, etc.), le logiciel propose un nouveau bouton représentant une caméra. En cliquant dessus, l'opérateur peut visionner la vidéo associée à l'événement. Par exemple, en cas de porte forcée la nuit, Ipévia Manager affichera les images de la caméra liée à la porte à l'heure correspondante.

**Numéro de traçabilité** : cette fonctionnalité permet d'assigner un code supplémentaire à toutes les clés d'un bâtiment ou d'un site.

**Serrure électronique sécurisée** : le logiciel peut gérer jusqu'à 6 serrures électroniques sans fil Assa-Abloy/Aperio par contrôleur. Les appareils sont associés à des hubs radio (DIU AH30 Gen5) qui sont câblés aux contrôleurs via un bus RS485.

## 2.4. Réseaux

Le logiciel est multi-réseaux. Ces réseaux peuvent être de type TCP/IP, RS485 ou mixtes.

**Qu'est-ce qu'un réseau IP ?** Lorsque les équipements sont câblés avec un câble Ethernet (RJ45) ou un câble USB (lorsqu'un ordinateur est physiquement connecté au contrôleur ou au serveur). Dans le cas de plusieurs contrôleurs installés via TCP/IP, ils sont tous connectés à un switch Ethernet, lui-même relié au modem Internet. Un réseau TCP/IP peut prendre en charge jusqu'à 64 centrales communiquant entre eux via IP. Lorsque qu'un site comprend plus de 64 contrôleurs IP, il est nécessaire de créer plusieurs réseaux dans Ipévia Manager.

**Qu'est-ce qu'un réseau RS485 ?** Lorsque les équipements sont câblés en utilisant le RS485. Le premier contrôleur du réseau doit être câblé en RJ45 (TCP/IP) pour avoir accès à Internet. Un réseau RS485 permet une communication entre 32 contrôleurs sur 1 km. Le premier contrôleur du réseau peut communiquer avec le serveur via TCP/IP ou USB.

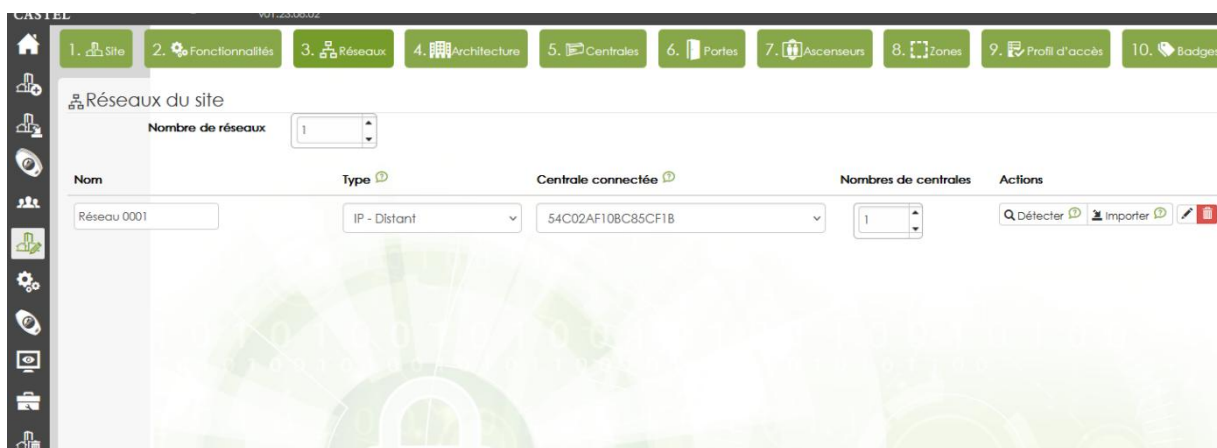
**Qu'est-ce qu'un réseau mixte ?** Cela désigne un réseau contenant des équipements câblés à la fois en RJ45 (TCP/IP) et en RS485. Depuis le serveur de communication, il est possible de câbler d'abord des contrôleurs TCP/IP, suivis de contrôleurs RS485, mais pas l'inverse.

Si un contrôleur est connecté via RS485 au réseau de contrôleurs, il ne peut pas agir comme passerelle IP pour d'autres contrôleurs.

En d'autres termes, un réseau mixte est toujours en TCP/IP du côté du serveur et éventuellement en RS485 par la suite. Cependant, un réseau mixte peut contenir plusieurs branches RS485 (ou plusieurs départs).

Dans Ipévia Manager, entrez le nombre de réseaux et le nombre de contrôleurs par réseau, puis cliquez sur **Suivant** ou utilisez le bouton en forme de **loupe** lorsque le serveur est connecté aux contrôleurs. Dans ce cas, le serveur recherche la présence des contrôleurs sur le réseau.

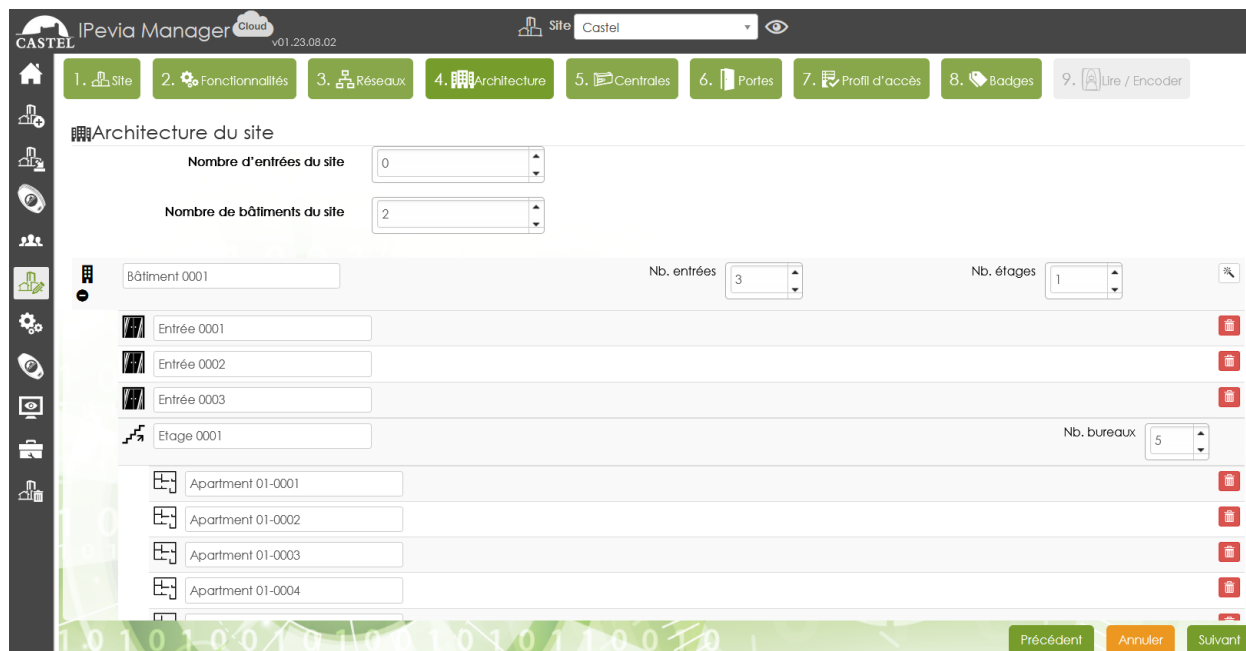
Cette option offre également l'avantage de récupérer automatiquement les numéros de série des contrôleurs, leurs options connectées et la présence de modules d'entrées/sorties, sans aucune intervention de l'utilisateur.



The screenshot shows the 'Réseaux du site' (Site Networks) configuration screen in the IPEVIA Manager software. The interface includes a top navigation bar with 10 tabs: 1. Site, 2. Fonctionnalités, 3. Réseaux (selected), 4. Architecture, 5. Centrales, 6. Portes, 7. Ascenseurs, 8. Zones, 9. Profil d'accès, and 10. Badges. On the left is a vertical toolbar with various icons. The main area is titled 'Réseaux du site' and contains a 'Nombre de réseaux' (Number of networks) dropdown set to '1'. Below this is a table with the following columns: 'Nom' (Name), 'Type' (Type), 'Centrale connectée' (Connected central unit), 'Nombre de centrales' (Number of central units), and 'Actions' (Actions). The table contains one entry: 'Réseau 0001' with 'Type' set to 'IP - Distant', 'Centrale connectée' set to '54C02AF108C85CF1B', and 'Nombre de centrales' set to '1'. The 'Actions' column for this entry contains three buttons: 'Détection' (Detection), 'Importer' (Import), and a red delete icon.

| Nom         | Type         | Centrale connectée | Nombre de centrales | Actions                                                                                                                   |
|-------------|--------------|--------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| Réseau 0001 | IP - Distant | 54C02AF108C85CF1B  | 1                   | <input type="button" value="Détection"/> <input type="button" value="Importer"/> <input type="button" value="Supprimer"/> |

## 2.5. Architecture



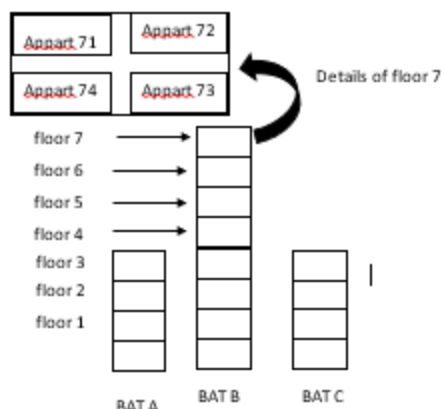
Sur IPévia, le concept d'architecture permet la création de bâtiments, d'étages, d'appartements et de bureaux. Il est ainsi possible de trier les équipements ou les utilisateurs par localisation géographique (plutôt que simplement par profil d'accès ou groupe). Ce concept d'architecture est optionnel pour la gestion du contrôle d'accès aux portes, mais devient obligatoire pour l'accès aux étages.

Cela explique pourquoi, lors de la définition des fonctionnalités, la sélection de "Ascenseur" sélectionne automatiquement "Architecture."

Ce concept simplifie considérablement la gestion du site. L'opérateur logiciel peut retrouver les badges via les bâtiments, étages ou bureaux, plutôt que dans une longue liste de profils d'accès.

De plus, il permet l'attribution automatique de l'accès aux étages pour tous les ascenseurs : par exemple, lorsqu'un opérateur autorise des personnes à accéder à un étage, il peut le faire en une seule action pour tous les ascenseurs desservant cet étage.

Utilisation : les deux vues (par architecture ou par profil d'accès) sont fonctionnelles à tout moment. Une icône en haut de l'arborescence (panneau gauche de l'écran) permet de basculer entre les deux vues.



Exemple de définition d'architecture dans le logiciel et son impact sur la gestion :

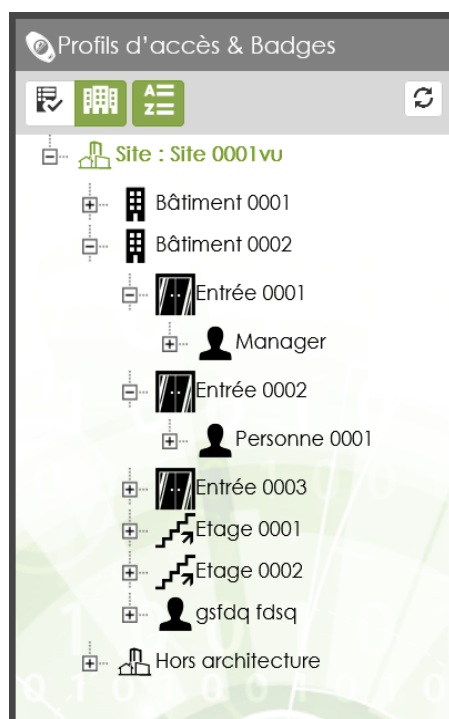
- Un site se compose de trois bâtiments, dont l'un, le bâtiment B, comporte 7 étages.
- Le 7<sup>e</sup> étage dispose de 4 appartements, numérotés de 71 à 74.

## Classic view (category type classification)



Dans la gestion classique, les utilisateurs et leurs clés sont triés dans le logiciel par profil d'accès aux portes ou aux étages.

## View by architecture



Dans cette vue, les utilisateurs et leurs badges sont triés par bâtiment, étage, et bureau ou appartement.

## Setting of the architecture concept

Nombre d'entrées du site

0

Dans l'onglet Architecture (cliquez sur le bouton Assistant de site dans la bannière de gauche, puis sur Architecture en haut), saisissez le nombre d'entrées du site, c'est-à-dire le nombre de portails ou de tourniquets menant au site. Les accès internes aux bâtiments sont définis ultérieurement dans l'outil de création. Ce concept d'entrée de site est optionnel, mais il aide le gestionnaire par la suite en permettant de classer les portes du système en catégories telles qu'extérieur, bâtiments, étages, etc.

Nombre de bâtiments du site

2

Le nombre de bâtiments est requis lorsque les ascenseurs sont gérés dans le logiciel.

Dans l'utilisation quotidienne, lorsque l'opérateur du logiciel accorde des droits à un utilisateur pour l'étage 4, le système autorise tous les niveaux de l'étage 4 de tous les ascenseurs du bâtiment avec la même opération.

Ensuite, vous pouvez entrer le nombre d'étages ou le nombre d'appartements/bureaux. Notez que le concept de "bureau" est optionnel et peut être utilisé plus tard pour trier les personnes et leurs clés.

Notez qu'un bouton avec une icône de baguette magique (voir ci-dessus) permet de créer et de nommer facilement des étages, des appartements et des unités. En cliquant dessus, la fenêtre suivante s'ouvre :

| Test | Floor number | Apartment number | Increment |
|------|--------------|------------------|-----------|
|      | 0            | 1                | 1         |

**Creation title**

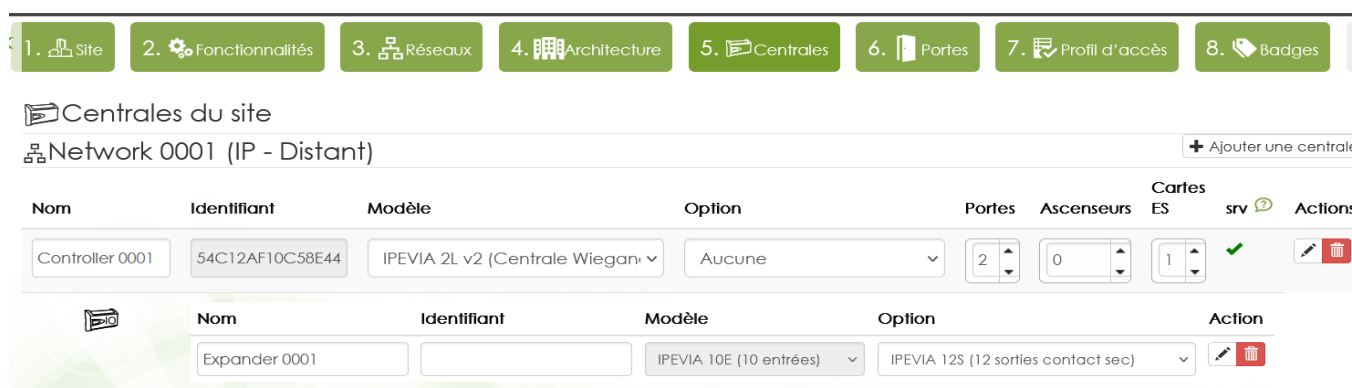
- \$ : Floor number
- \$\$ : floor number with 2 characters
- # : Apartment number
- ## : apartment number with 2 characters
- ### : apartment number with 3 characters
- ...

- Entrez le nombre de sous-sols et d'étages au-dessus du sol. Le logiciel augmentera automatiquement les numéros.
- Cochez la case "Rez-de-chaussée" si l'ascenseur contrôle également le rez-de-chaussée. Sinon, cocher ou décocher la case n'a pas d'importance.
- L'option "Avant/Arrière" s'applique uniquement à l'intégration Kone si les ascenseurs ont à la fois des portes avant et arrière dont l'ouverture est contrôlée par les droits de clé.

- Entrez le nombre d'appartements par étage et fournissez un nom commun, ainsi que le nombre de chiffres pour les numéros d'étage et d'appartement de chaque étage. Par exemple, en entrant "Appartement \$\$##", le logiciel générera "Appartement 0001, 0002, ..., 0501, 0502", etc.

## 2.6. Centrales

Dans l'étape suivante, entrez le nombre de contrôleurs et les options qu'ils prennent en charge en haut ou via le bus RS485. Indiquez également le nombre de portes et d'ascenseurs gérés par chaque contrôleur.



| Nom             | Identifiant     | Modèle                          | Option | Portes | Ascenseurs | Cartes ES | srv | Actions                                                                                                                                                                 |
|-----------------|-----------------|---------------------------------|--------|--------|------------|-----------|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Controller 0001 | 54C12AF10C58E44 | IPEVIA 2L v2 (Centrale Wiegand) | Aucune | 2      | 0          | 1         | ✓   |   |

| Nom           | Identifiant | Modèle                  | Option                              | Action                                                                                                                                                                      |
|---------------|-------------|-------------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Expander 0001 |             | IPEVIA 10E (10 entrées) | IPEVIA 12S (12 sorties contact sec) |   |

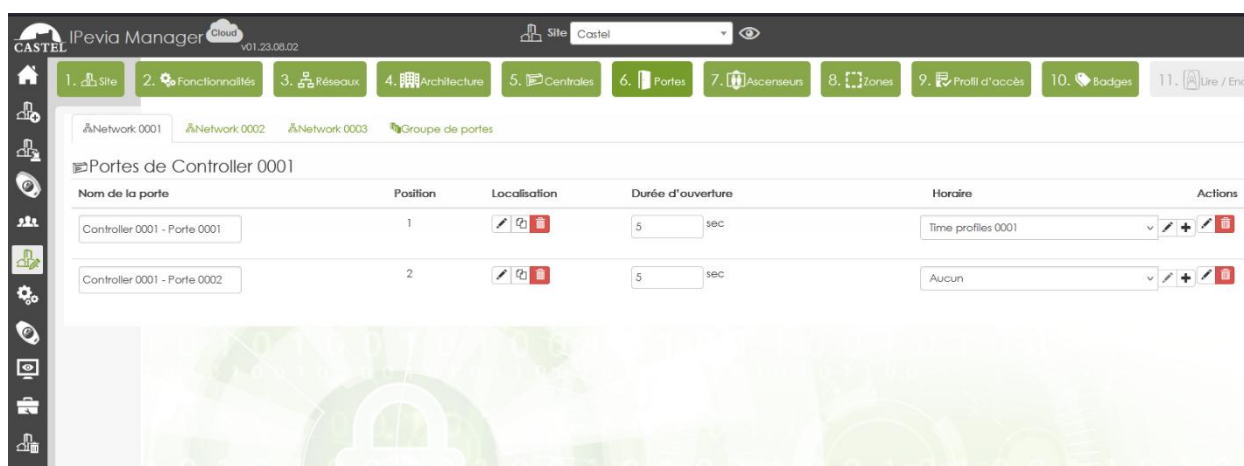
Dans la fenêtre au dessus, remplir les champs comme cela :

- **Nom du contrôleur** : 32 caractères, il s'agit d'un texte libre désignant le contrôleur ou son emplacement.
- **L'identifiant du contrôleur** : c'est celui inscrit sur l'étiquette du contrôleur (ex. 54C01AA000B00C000). Notez que cet identifiant est décomposé comme suit : 54C01 ou 54C02 ou 54C12 ou 54C12 en fonction de la version du contrôleur et de son protocole. AA000B00 correspond à la fin de l'adresse MAC. Le début (00 0E) est commun à tous les contrôleurs, donc l'adresse MAC de ce contrôleur est 00 0E AF 00 0B 00 C000.
- **Option** : un contrôleur peut supporter une carte optionnelle montée sur le dessus du boîtier. Cette carte peut fournir l'une des options suivantes : 4 lecteurs supplémentaires, 12 entrées ou 12 sorties.
- **Portes** : indiquez combien de portes sont gérées par le contrôleur (le nombre maximum de portes par dispositif est de 6).
- **Carte E/S** : chaque contrôleur gère jusqu'à 10 cartes d'entrée/sortie RS485.
- **SRV (server)** : si le contrôleur est connecté au cloud, il affichera une coche verte.

## 2.7. Portes

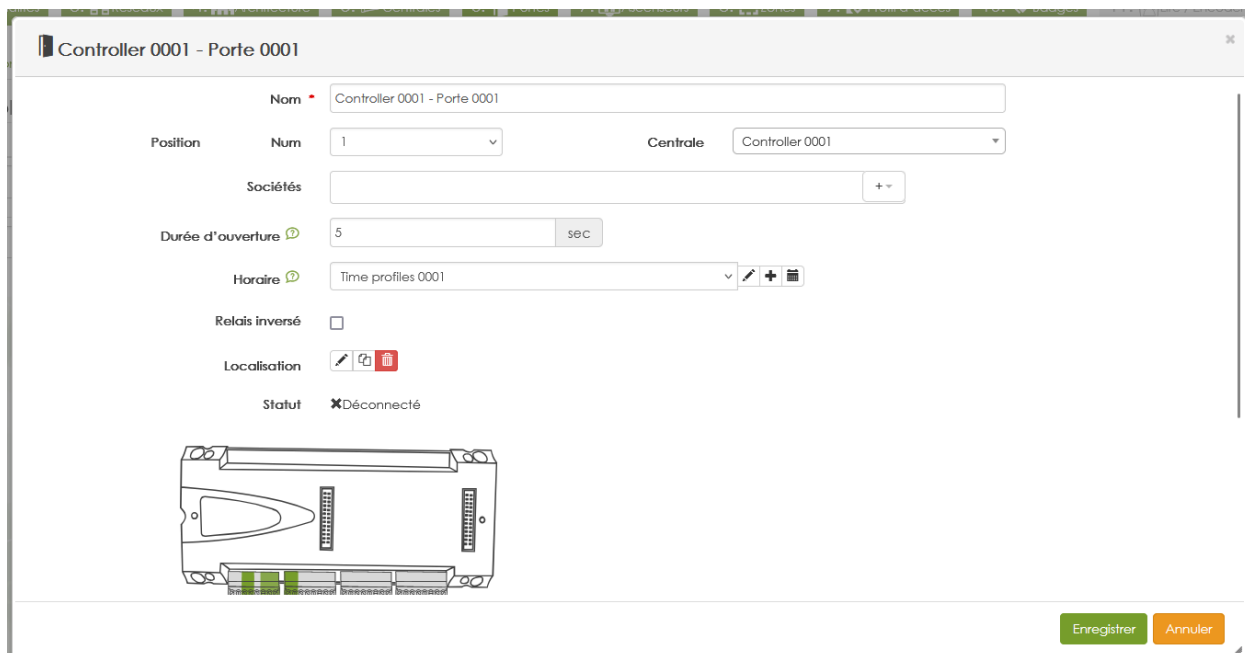
Dans la capture d'écran suivante, vous pouvez modifier les paramètres des portes.

- Changez le nom de chaque porte.
- Ajustez le temps de déverrouillage de la porte si nécessaire (par défaut, 5 secondes).
- Temps de déverrouillage de la porte (+ bouton à gauche) : ajoutez éventuellement des créneaux horaires à la porte pendant lesquels la porte est :
  - Accès libre : la serrure magnétique n'est pas alimentée, et la porte reste déverrouillée. (exemple : pendant les heures de bureau pour permettre l'entrée du service postal).
  - Interdit : même une clé valide ne peut pas l'ouvrir.
  - Normal : une clé valide est requise pour ouvrir la porte.



En cliquant sur le crayon sous la section emplacement, vous pouvez localiser cette porte dans l'architecture de l'installation. Cette option est utile si les paramètres d'architecture ont été activés lors des étapes précédentes.

En cliquant sur le crayon à droite, vous accédez aux paramètres avancés.



## 2.8. Ascenseur

Ipévia gère l'intégration de plusieurs ascenseurs et peut contrôler jusqu'à 110 étages par contrôleur. Dans la plupart des cas, l'intégration de l'ascenseur dans le système de contrôle d'accès se fait par contacts secs. Cependant, Ipévia propose également deux types d'intégration intelligente avec la marque Kone.

Ces deux intégrations, expliquées ci-dessous, reposent sur une communication TCP/IP entre le système de contrôle d'accès et l'ascenseur.

La fonctionnalité de l'ascenseur peut être réutilisée pour gérer des casiers, des boîtes aux lettres ou des coffres de stockage. En effet, pour le même lecteur ou clavier, le système gère jusqu'à 110 relais, qui peuvent être des serrures de casiers ou des contacts de désactivation d'alarme.

### - Ascenseurs traditionnels

Les lecteurs de contrôle d'accès sont installés à l'intérieur des cabines d'ascenseur. L'utilisateur appelle l'ascenseur, entre, présente son badge et appuie sur le bouton de l'étage souhaité. En général, les boutons correspondant à leurs étages autorisés s'allument après la présentation du badge. Pour un résident, seuls les boutons de son étage résidentiel et de l'étage de parking souterrain s'allument, tandis que pour un gardien, l'accès à tous les étages peut être accordé. Le panneau de contrôle fournit un contact sec pour chaque étage et ascenseur. Par exemple, dans un bâtiment de 15 étages avec deux ascenseurs, cela nécessiterait 30 relais.

### - Kone COP (Car operating panel)

Le principe est le même que pour les ascenseurs traditionnels, mais ici, la communication entre le contrôle d'accès et l'ascenseur repose sur le TCP/IP. L'intégration Kone Cop réalise cela sans matériel supplémentaire. La fonctionnalité nécessite une carte d'activation, qui doit être insérée dans le contrôleur. Cette solution simplifie le câblage entre l'ascenseur et le contrôleur. Par exemple, dans une installation utilisant des contacts secs, un bâtiment de 80 étages avec 10 ascenseurs nécessiterait 800 relais du côté du contrôle d'accès et 800 entrées du côté de l'ascenseur, qui devraient toutes être fournies, alimentées et câblées.

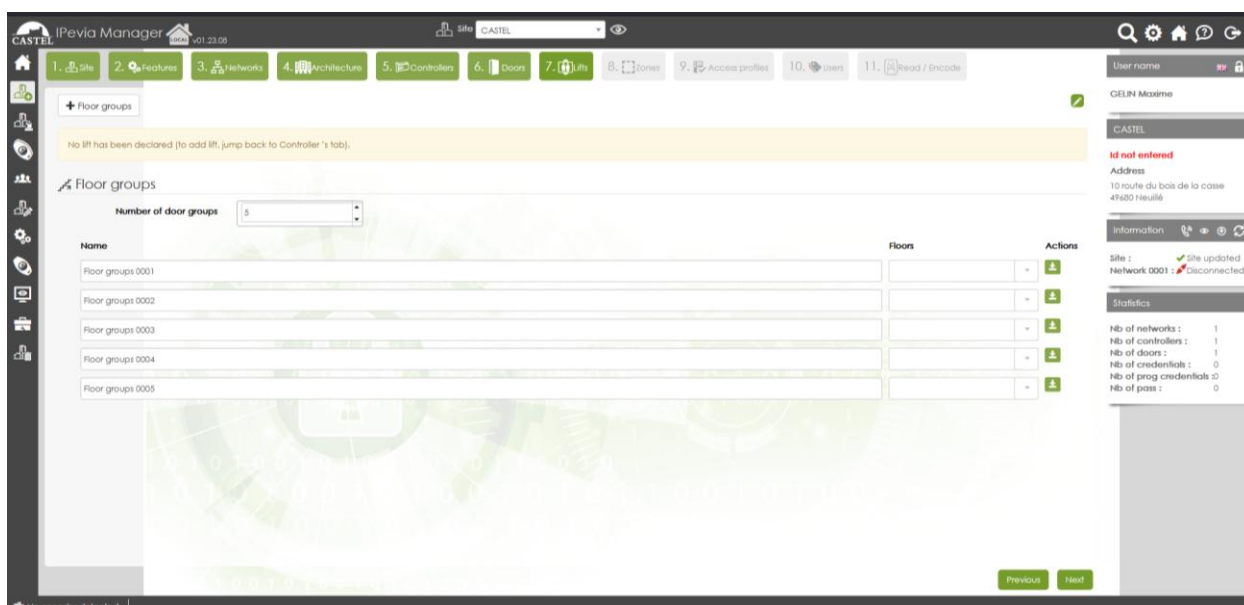
## - Kone DOP (destination operating panel)

L'étage de l'appartement des résidents est programmé dans leur profil d'accès. Lorsqu'ils entrent dans le bâtiment avec leur clé, l'ascenseur est appelé et les amène à l'étage correspondant. Ce système est utile lorsqu'un groupe d'ascenseurs dessert le même étage. À chaque niveau, un terminal permet à l'utilisateur de sélectionner son étage, et l'ascenseur le dirige vers le véhicule approprié. Ce système améliore l'efficacité des ascenseurs en optimisant les trajets, transportant plus de personnes par heure tout en consommant moins d'énergie. L'intégration Kone Dop avec Ipévia est logicielle à logicielle : la configuration de l'ascenseur est effectuée dans Kone Access. Les bases de données de Ipévia Manager et Kone Access sont liées.

## Programmation

Parce que des ascenseurs ont été ajoutés aux contrôleurs lors de l'étape précédente, le logiciel a automatiquement effectué les opérations suivantes :

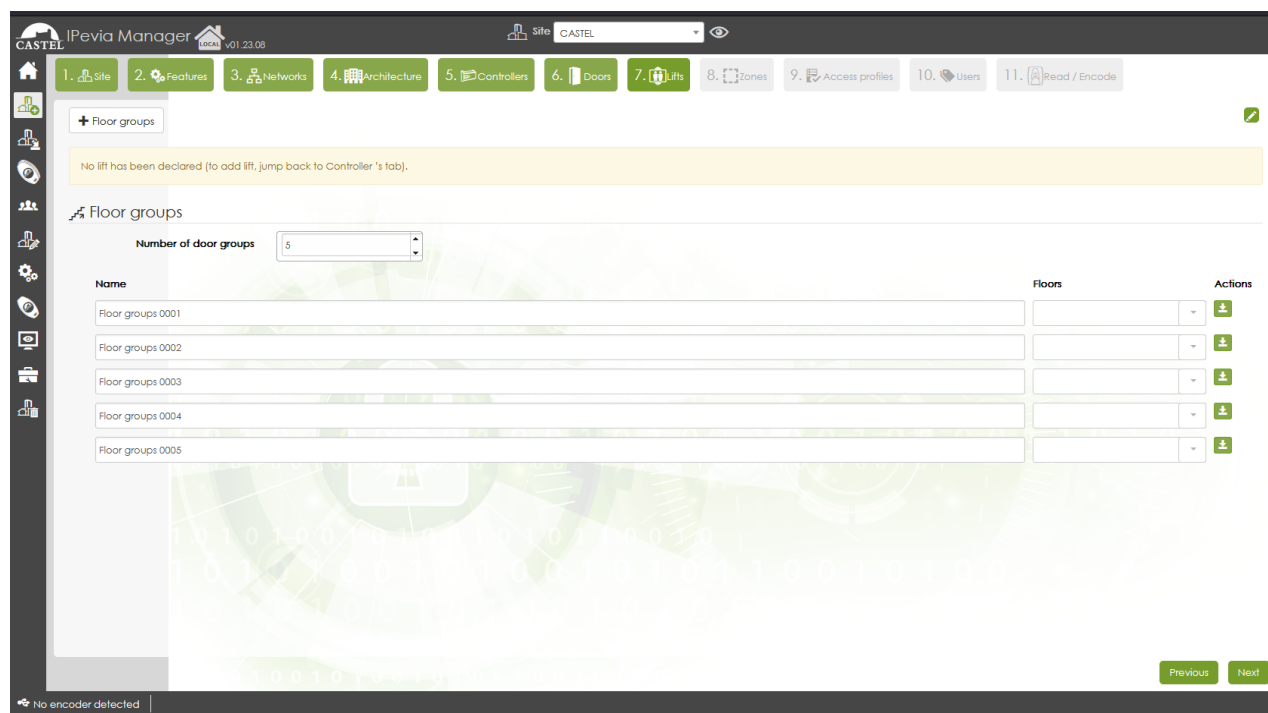
- Attribuer ces ascenseurs à leurs bâtiments respectifs.
- Sélectionner un lecteur inutilisé du contrôleur pour chaque ascenseur.
- Assigner les sorties de relais disponibles aux étages. Pour gérer ces ascenseurs, utilisez l'icône de crayon sous "Bâtiment" ou celle sous "Actions" pour modifier leurs paramètres (voir la deuxième capture d'écran).



Dans la capture d'écran ci-dessous, vous pouvez modifier ou ajouter les paramètres suivants :

- **Ajouter un second lecteur** : lorsqu'une cabine d'ascenseur est équipée de deux lecteurs ou plus, ceux-ci peuvent être ajoutés ici en décochant « lecteur par défaut » et en sélectionnant les lecteurs correspondants.
- **Délai d'activation** : il s'agit du temps entre la présentation de la clé sur le lecteur d'ascenseur et la sélection de l'étage. Les visiteurs, qui n'ont logiquement pas de clé, nécessitent un délai suffisant entre l'autorisation d'accès (accordée par l'hôte) et la sélection de l'étage désiré. C'est pourquoi Ipévia Manager distingue deux délais d'activation différents : le premier en secondes pour les résidents et le second en minutes pour les visiteurs.
- Il est possible d'ajouter un bouton supplémentaire, actionné par l'opérateur du tableau de commande. Ce bouton transmet un contact sec à une entrée de l'Ipévia, ce qui accorde au visiteur les droits de sélectionner et d'accéder à l'étage requis.

Il est possible d'ajouter un bouton supplémentaire, actionné par l'opérateur du tableau de commande. Ce bouton transmet un contact sec à une entrée de l'Ipévia, ce qui accorde au visiteur les droits de sélectionner et d'accéder à l'étage requis.



## 2.9. Zones

Le système permet la gestion des zones de comptage et/ou de l'anti-passback. La fenêtre suivante apparaît lorsque la fonctionnalité "zone" a été activée lors de l'étape précédente (voir chapitre 3.1).

Une zone de comptage permet de :

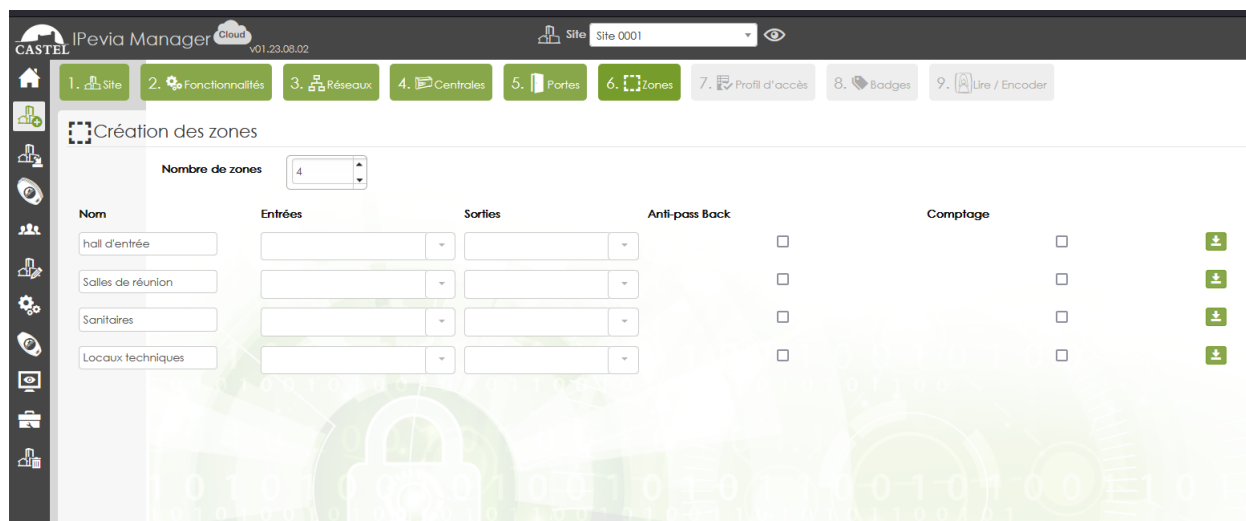
- Savoir en temps réel le nombre de personnes, de voitures, etc., dans une zone
- Limiter le nombre de personnes, de voitures, etc.
- Afficher la zone dans laquelle un utilisateur du contrôle d'accès se trouve

Les options avancées permettent d'assurer l'exactitude du processus de comptage :

- Confirmation de passage : Ipévia peut utiliser le contact de la porte comme confirmation de passage. Cela pourrait être une barrière infrarouge pour un portail de parking, ou un contact fourni par un tourniquet dans le contrôle d'accès piéton.
- Anti-passback : cela peut être lié au comptage pour s'assurer que l'utilisateur A ne prête pas son badge à l'utilisateur B, contournant ainsi les règles.

Notez que l'anti-passback peut également être utilisé sans comptage, selon le scénario.

Dans la fenêtre suivante, entrez le nombre de zone(s), puis, pour chacune, sélectionnez les lecteurs d'entrée et de sortie pour la zone. Cochez les options Anti-pass backLocal et comptage si nécessaire.



| Nom               | Entrées | Sorties | Anti-pass Back           | Comptage                 |                                                                                       |
|-------------------|---------|---------|--------------------------|--------------------------|---------------------------------------------------------------------------------------|
| hall d'entrée     |         |         | <input type="checkbox"/> | <input type="checkbox"/> |  |
| Salles de réunion |         |         | <input type="checkbox"/> | <input type="checkbox"/> |  |
| Sanitaires        |         |         | <input type="checkbox"/> | <input type="checkbox"/> |  |
| Locaux techniques |         |         | <input type="checkbox"/> | <input type="checkbox"/> |  |

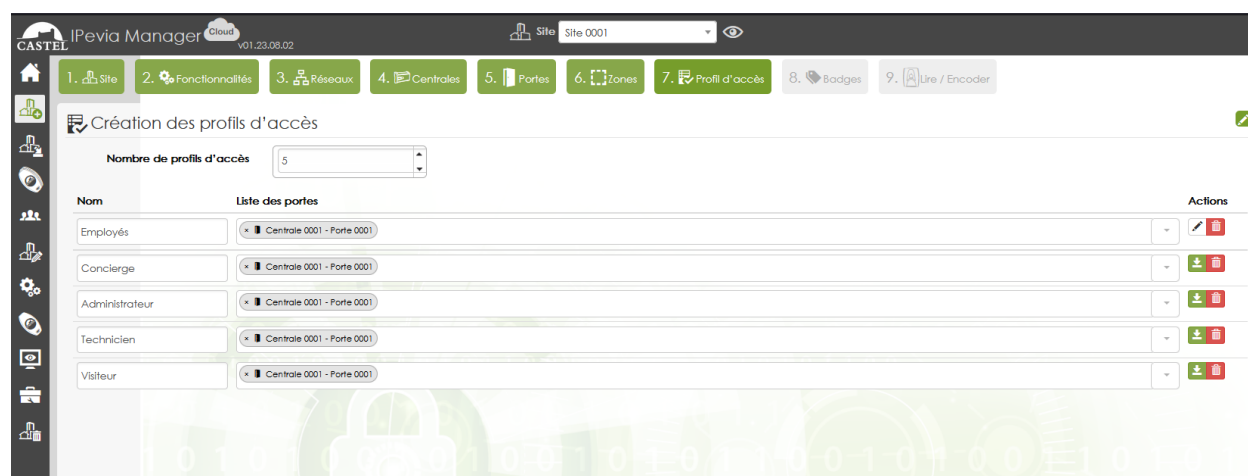
## 2.10. Profil d'accès

Le logiciel fonctionne avec des profils d'accès. Il contient une liste de portes autorisées.

Note : un utilisateur du système possède quatre profils d'accès différents.

- Un profil d'accès permanent aux portes
- Un profil d'accès permanent aux étages
- Un profil d'accès temporaire aux portes
- Un profil d'accès temporaire aux étages
- Un profil temporaire est donc une liste de portes ou d'étages supplémentaires auxquels un utilisateur peut accéder dans un intervalle de temps donné (par exemple, du 04/06 au 15/06, de 03h00 à 18h00).

Lorsqu'un utilisateur a besoin d'un accès à la fois à une zone "bureau" et à une zone "atelier", un profil d'accès doit être créé dans le logiciel, incluant toutes les portes concernées.



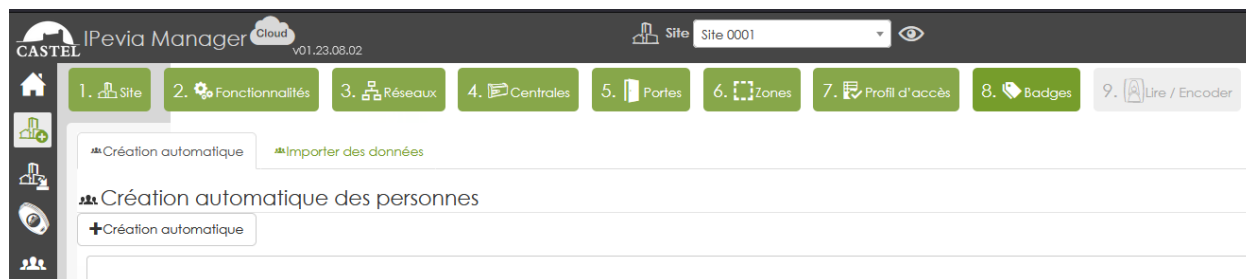
## 2.11. Badges

L'assistant utilisateurs permet de créer automatiquement des individus, leurs clés, codes de clavier, etc.

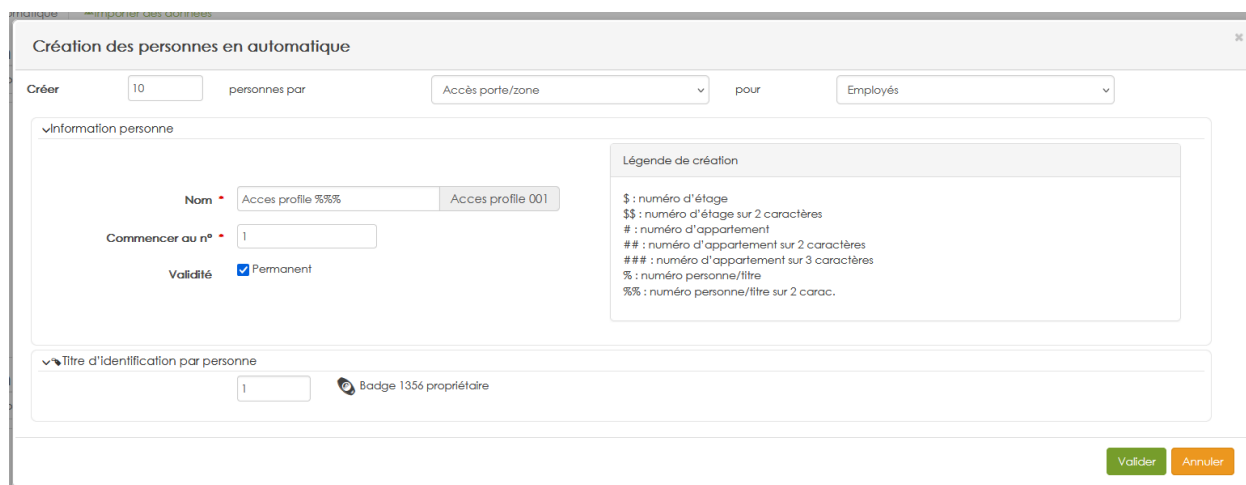
À partir de cette même fenêtre, vous pouvez ajouter plusieurs éléments : par exemple, 20 individus utilisant le même profil d'accès, plus 15 autres utilisant un profil différent. Ces ajouts automatiques s'appliquent aux sites, profils d'accès aux portes ou aux étages, groupes de personnes (par exemple, Ingénierie, Ventes, Administration, etc.) ou éléments architecturaux (par exemple, bâtiments, étages, bureaux).

Cliquez sur le bouton "Création automatique" dans la capture d'écran suivante ; la deuxième capture d'écran montre les détails de l'outil. Dans la fenêtre suivante, entrez le nombre d'individus à créer pour chaque option (accès, bâtiment, étage, etc.). Ensuite, sélectionnez le profil, le bâtiment, l'étage, etc. appropriés.

Dans le champ "Informations sur la personne", entrez un nom et référez-vous à la légende pour gérer les incréments automatiques.



L'exemple suivant montre comment créer 10 individus, ayant le profil d'accès « employé ». Ils seront nommés par incrément, en commençant par « acces profile 001 » puis le deuxième sera nommé « Acces profile 002 ». Ils disposeront tous d'un badge 1356Mhz Castel.

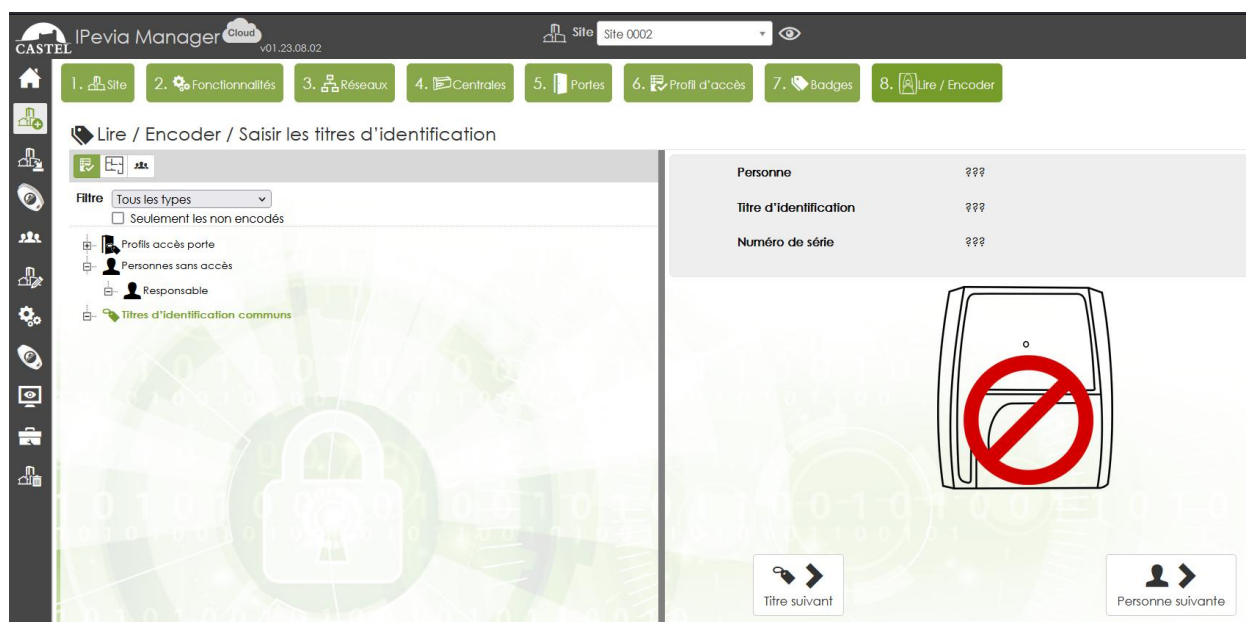


## 2.12. Lire/encoder

À l'étape finale, l'assistant propose de lire les numéros de série des cartes à l'aide du lecteur de bureau et de les associer aux individus créés automatiquement.

Dans le cadre de gauche, vous trouvez toutes les personnes saisies. Vous pouvez les trier par profil d'accès, appartement ou groupe. Vous pouvez les sélectionner manuellement pour les ajouter à un identifiant.

Le cadre de droite indique la personne sélectionnée dont la clé sera encodée. Le cadre de gauche permet de passer directement à un autre profil, groupe, personne, etc. À chaque scan de badge, le logiciel passe automatiquement au suivant. Ainsi, aucune action n'est requise entre chaque présentation de clé au programmeur.



### 3. Matériel et paramétrage



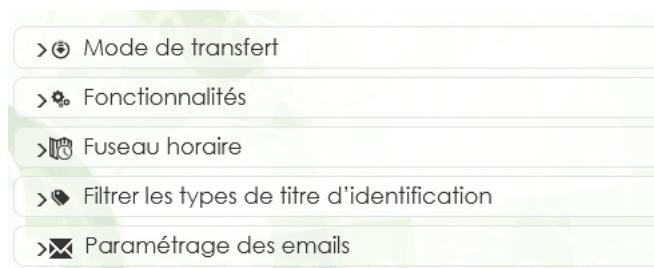
Tous les paramètres du système et du site sont modifiables. En cliquant sur l'icône en forme de roue dentée « Matériel et paramétrages ».

Après avoir cliqué sur l'icône en forme de roue dentée « Équipements et paramètres », puis sur « Site : xxxxxx » dans la structure arborescente, nous accédons aux paramètres principaux du site.

Ce menu inclut toutes les informations saisies lors de la création du site. Pour plus de détails sur les champs présents ici, veuillez consulter le Chapitre 2 : Assistant de création de site.

## 3.1. Paramétrage des emails

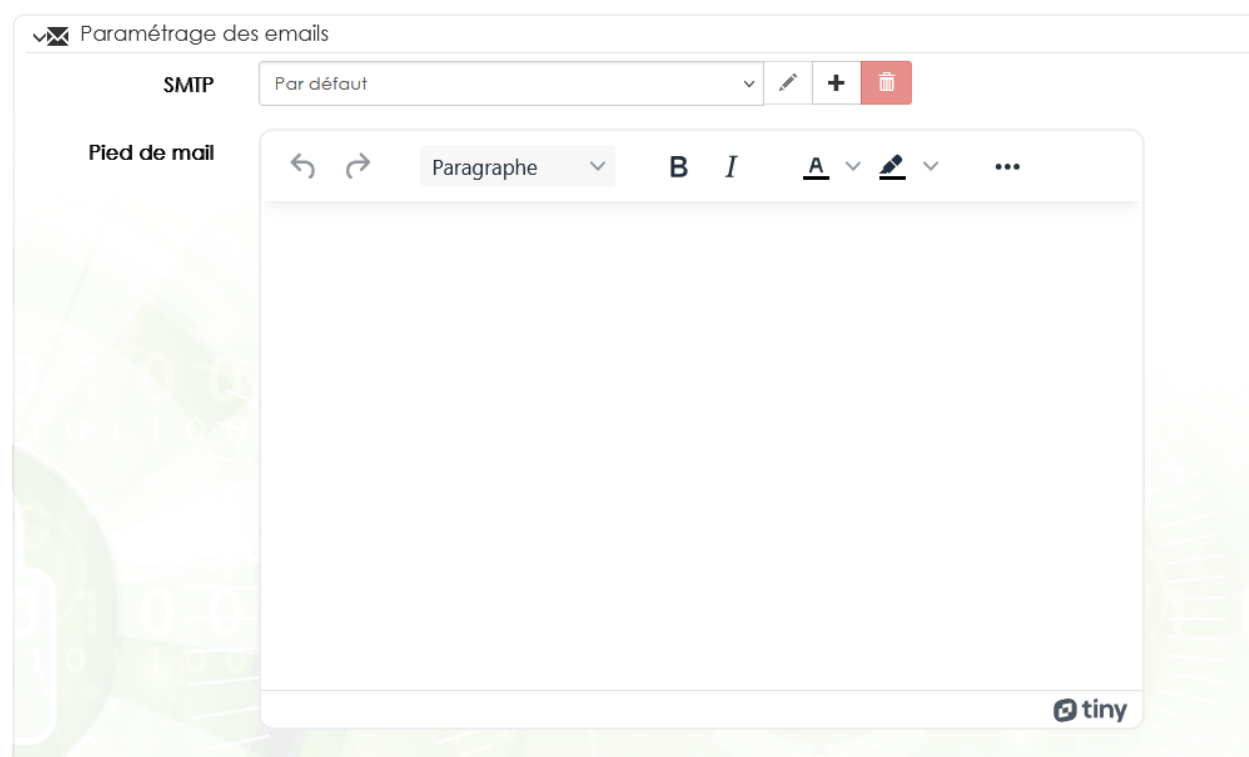
Le logiciel peut envoyer des e-mails soit via des tâches planifiées, soit par des processus. Pour ce faire, il est nécessaire de configurer le compte de messagerie sur le serveur.



Depuis le menu « Équipements et paramètres », cliquez sur le site en haut de l'arborescence.

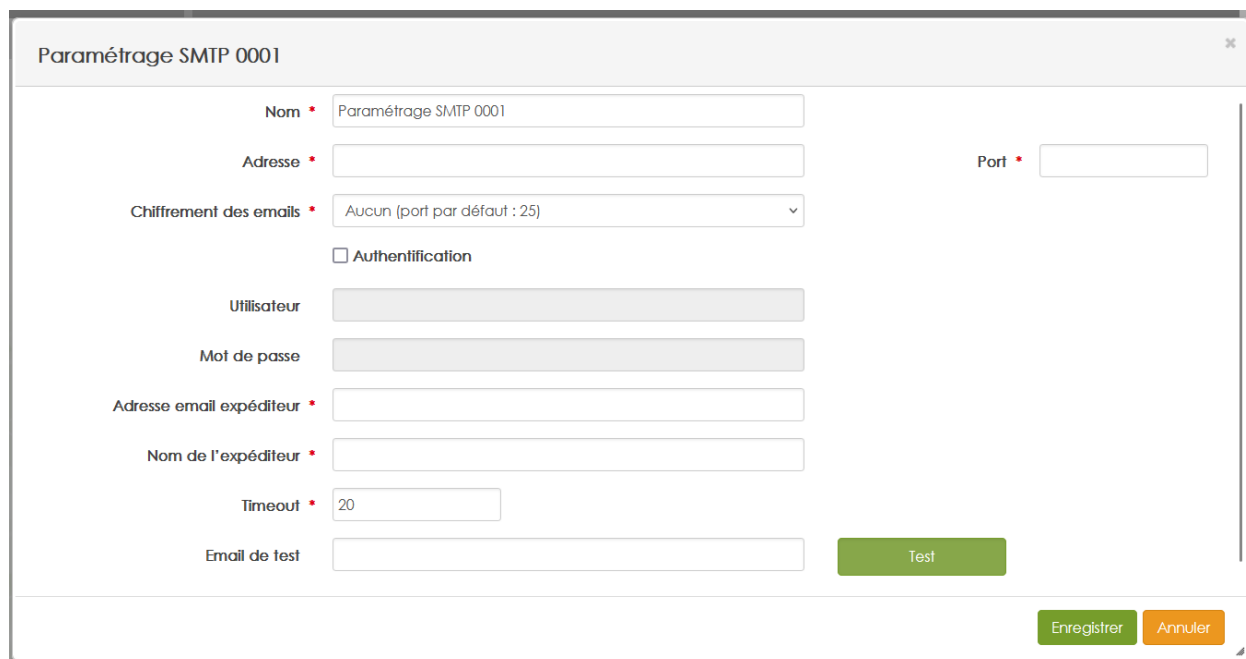
Sous tous les champs de coordonnées du site, et parmi toutes les options disponibles, cliquez sur le bouton « Paramètres de l'email ».

La fenêtre ci-dessous apparaît :



Le pied de mail conçu dans l'encadré ci-dessus, pourra être employé pour diverses usages. Par exemple, lorsqu'un usager réserve une salle de réunion par exemple, il est possible de paramétrer qu'il reçoive ce footer. Il s'agira du pied de page par défaut pour le site.

Un compte e-mail doit avoir été créé. L'ordinateur supportant Ipévia Manager doit avoir accès à ce serveur. Cliquez sur le bouton + à droite du champ « SMTP ».



Ensuite, entrez les champs requis et testez l'envoi du mail en saisissant une adresse et en cliquant sur « Test ».

## 3.2. Utilisation de la multisociété

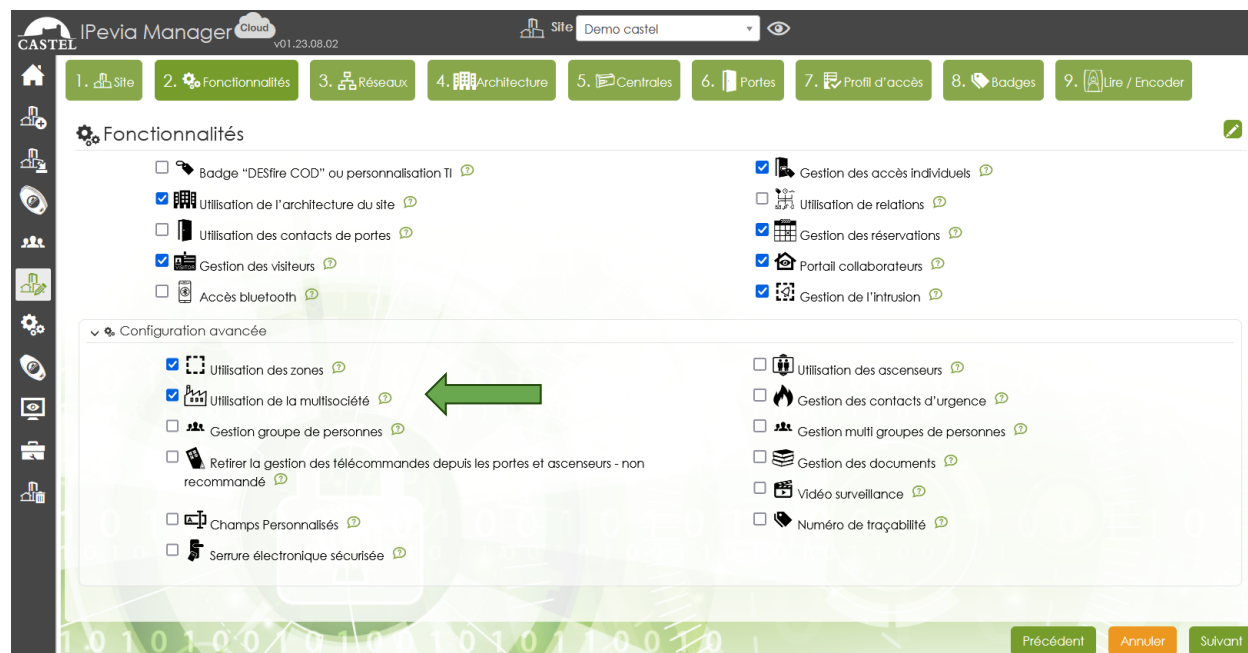
Ipévia Manager propose une gestion multisociétés. Pour un site unique, plusieurs opérateurs peuvent visualiser et gérer leurs propres portes, profils d'accès ou utilisateurs, sans voir ceux des autres opérateurs. Seuls les administrateurs de site ou les opérateurs avec des droits multi-entreprises voient l'ensemble. Cette gestion s'applique, par exemple, à un immeuble de bureaux où des étages sont utilisés par différentes entreprises, mais où toutes utilisent des portes ou ascenseurs communs.

Les opérateurs de l'entreprise A voient leurs propres portes et étages, ainsi que les portes communes. Ils ne voient que leurs profils d'accès et utilisateurs. Dans la gestion des événements, ils ne voient que les portes et/ou utilisateurs autorisés. La gestion multi-entreprises peut être appliquée à d'autres cas d'utilisation, comme les résidences en copropriété : si l'immeuble est occupé par des propriétaires de copropriété à certains niveaux et des logements sociaux à d'autres, les bailleurs et les gestionnaires de copropriété sont considérés comme deux entreprises, et ne voient que leurs propres accès et les zones communes.

La version Cloud d'Ipévia facilite la gestion multi-entreprises, puisqu'il est facile de séparer le site en réseaux et de connecter chaque réseau indépendant au serveur Ipévia.com. Dans ce cas, il n'est pas nécessaire de lier ces réseaux centraux entre eux. Ipévia.com est le lien entre tous.

## Activation de la fonction

Par défaut, la fonction « gestion multi-entreprises » est désactivée. Dans l'assistant de création de site / Fonctionnalités, cochez la case « utiliser la gestion multi-entreprises ».



## Créer une société



Dans l'onglet « équipements et paramètres », ouvrez le nœud « Entreprises », puis cliquez sur le bouton « Ajouter une entreprise » dans la fenêtre droite.

Ensuite, entrez un nom et cochez « adresse identique à celle du site » si cette entreprise est située à l'adresse déjà définie pour le site, ou

décochez-la pour entrer une adresse propre à l'entreprise.

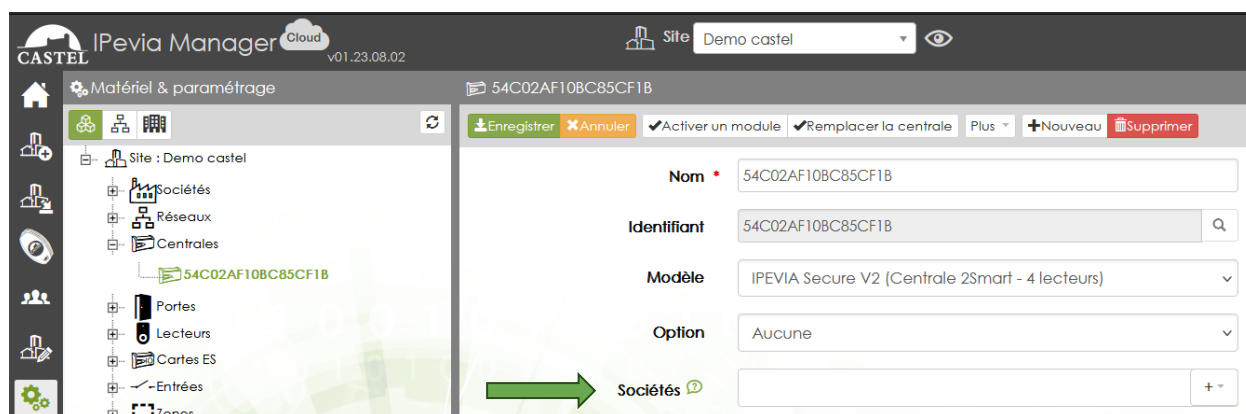
## Assigner une société aux appareils

Chaque paramètre d'équipement ou de site peut être lié à une ou plusieurs entreprises. Par exemple, une porte commune peut être attribuée à plusieurs entreprises, tandis qu'une porte de salle des machines ou de bureau ne peut être utilisée que par une autre entreprise. La sélection de l'entreprise s'applique aux paramètres suivants :

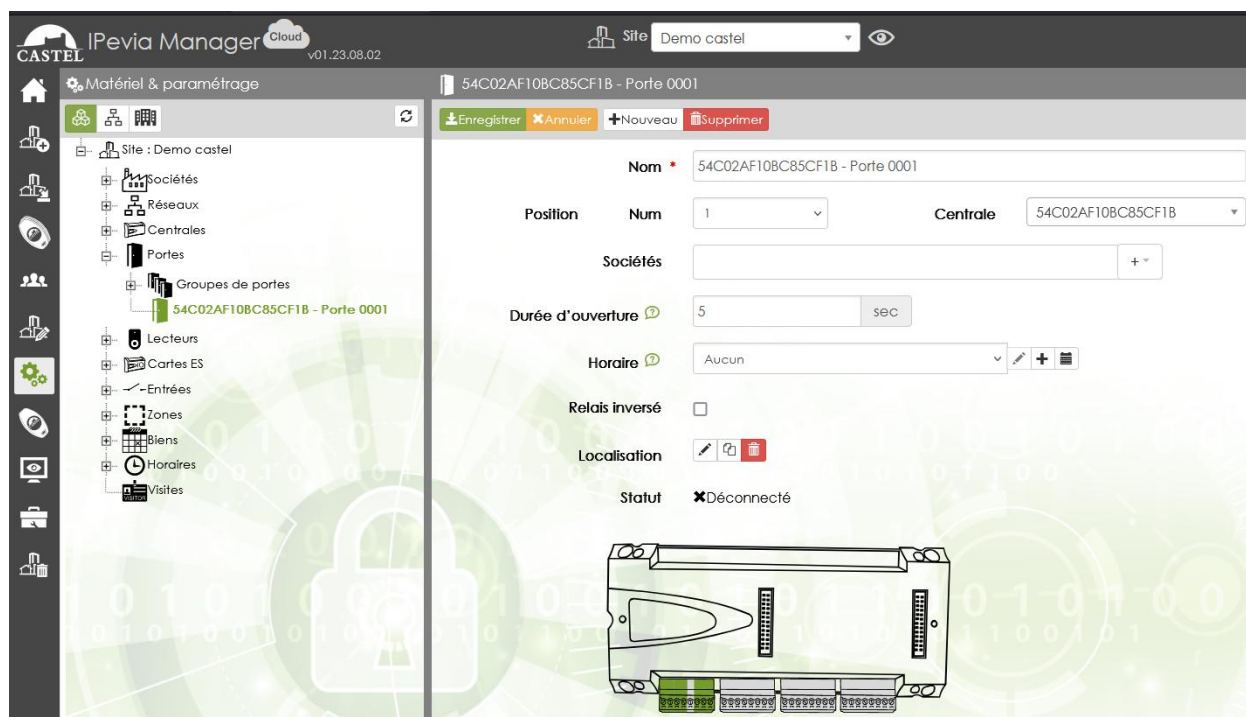
- Contrôleurs
- Lecteurs / portes
- Ascenseurs / étages

- Cartes d'entrée / sortie
- Zones de comptage / anti-pass back
- Profil d'accès
- Plannings (porte, badge, etc.)
- Relations

Exemple pour une centrale:



Exemple pour une porte :



La porte suivante "Porte visiteur" est visible et utilisable par les opérateurs des trois entreprises sélectionnées.

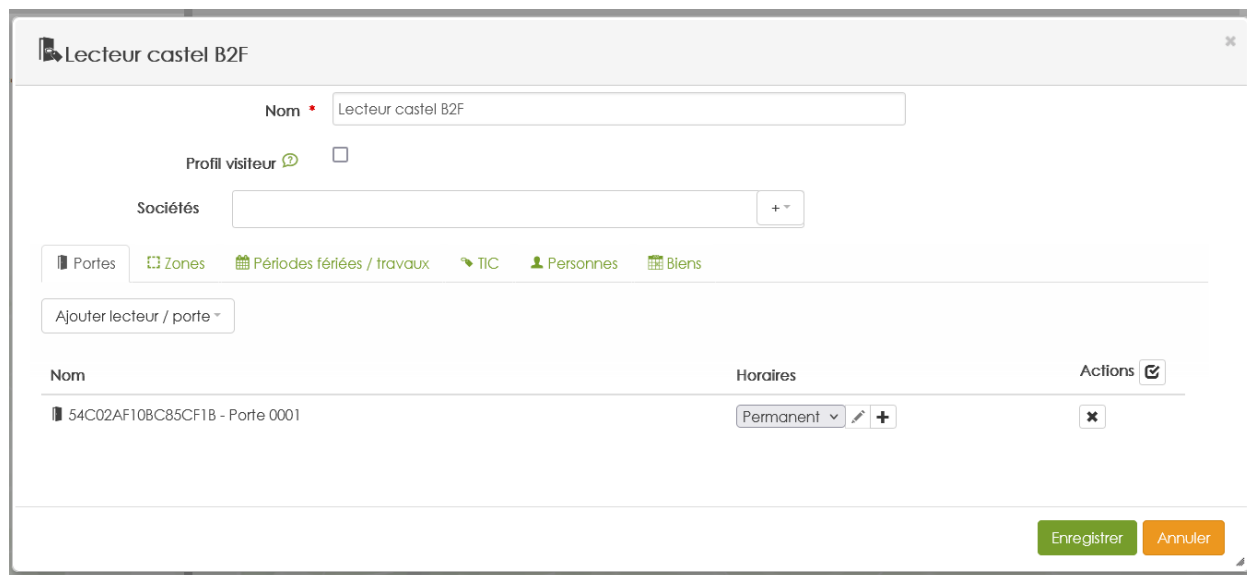
Ces opérateurs peuvent contrôler la porte via des commandes manuelles, la sélectionner pour créer des profils d'accès ou consulter les événements.

Au bas de cette fenêtre, vous pouvez voir un schéma du contrôleur et du port affilié à ce lecteur/porte.

## Assigner une société au profil d'accès et aux utilisateurs

Le système peut gérer un total de 1000 profils d'accès. Pour chaque profil, une ou plusieurs entreprises peuvent être sélectionnées. Par exemple, un profil d'accès "Hall d'entrée" peut être attribué à plusieurs entreprises, tandis que le profil "bureau FDI" peut uniquement être attribué aux opérateurs de l'entreprise "FDI".

E

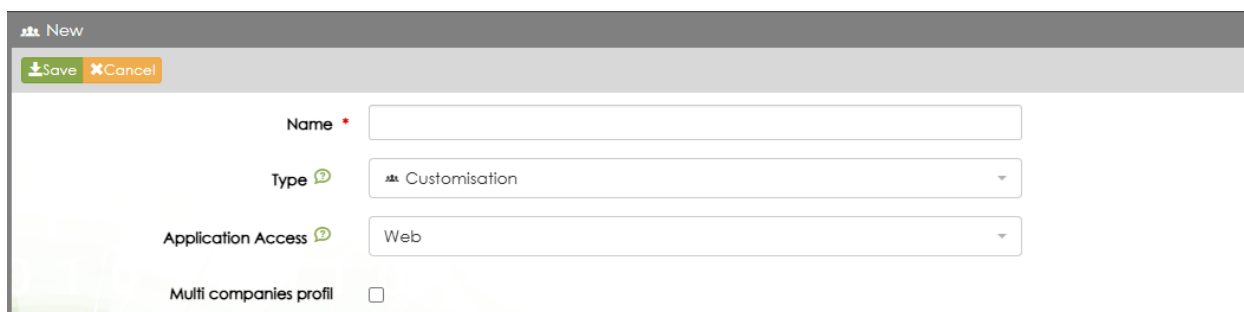


| Nom                            | Horaires  | Actions |
|--------------------------------|-----------|---------|
| 54C02AF10BC85CF1B - Porte 0001 | Permanent | [X]     |

## Accès a IPévia manager

Pour utiliser la gestion multi-entreprises, vous devez également créer des groupes d'opérateurs multi-entreprises et des opérateurs.

Dans la section « Opérateur logiciel », puis « Groupes d'opérateurs et opérateurs », cliquez sur « +Ajouter un groupe d'opérateur s ».

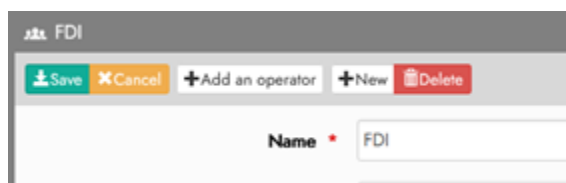


Cette fenêtre apparaît. Entrez un nom pour ce groupe d'opérateurs et cochez « Profil multi-entreprises ». Veuillez noter que si vous cochez cette case, tous les choix liés aux paramètres seront inaccessibles.

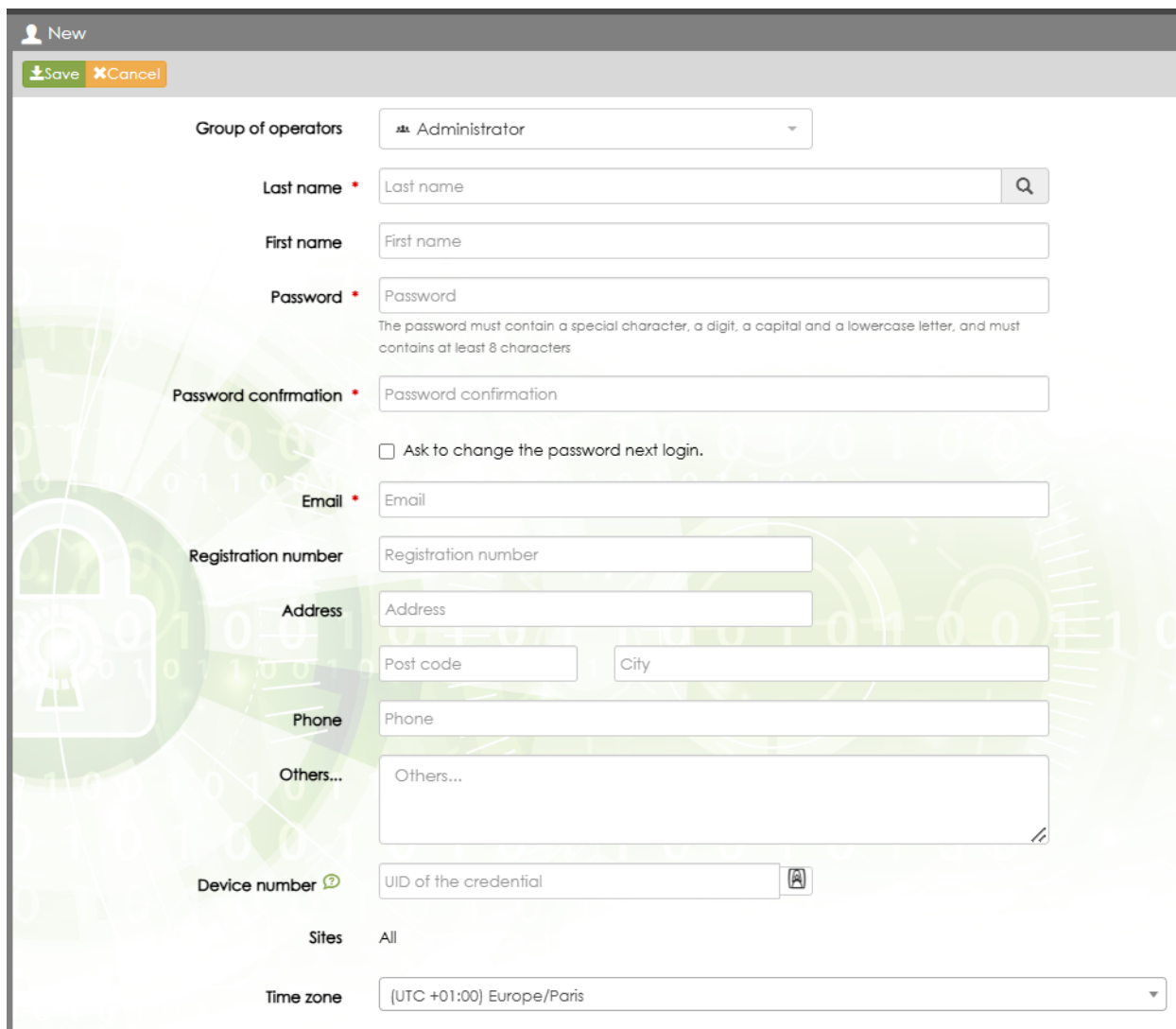
Cependant, toutes les options de gestion des clés et de supervision sont autorisées (voir ci-dessous).

| Rights of the group                                                                                                 |                          |                          |                          |                          |
|---------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Function/Sub-function                                                                                               | View                     | Edit                     | Add                      | Delete                   |
|  <b>General</b>                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| "Multi-site passes"                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Software access                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|  <b>Equipment &amp; Settings</b> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Site                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Network                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Controller                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Architecture                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Zone                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Reflex                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Lift                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Facilities /assets booking                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Wireless locking device                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Control card                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Individual access                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

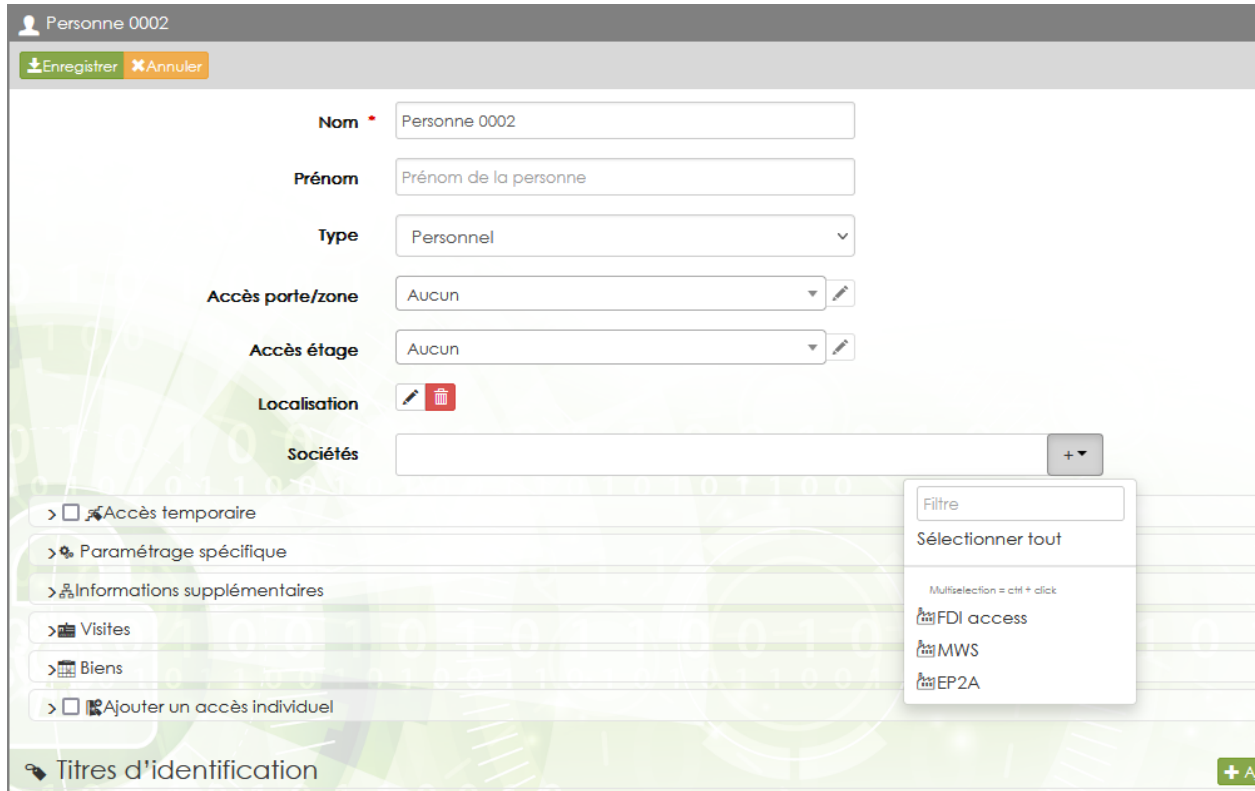
Lorsque le profil d'opérateur multi-entreprises est créé, il est possible de créer les opérateurs.



Sous le profil, cliquez sur « +Ajouter un opérateur ». Cette fenêtre apparaît :



Dans la fenêtre ci-dessous, entrez le nom, le prénom et le mot de passe de l'opérateur comme pour un opérateur traditionnel.



Personne 0002

Enregistrer Annuler

Nom \* Personne 0002

Prénom Prénom de la personne

Type Personnel

Accès porte/zone Aucun

Accès étage Aucun

Localisation

Sociétés

> ☐ Accès temporaire

> ☐ Paramétrage spécifique

> ☐ Informations supplémentaires

> ☐ Visites

> ☐ Biens

> ☐ Ajouter un accès individuel

Titres d'identification

Filtre

Sélectionner tout

Multiselection = ctrl + click

FDI access

MWS

EP2A

Also provide the company(ies) to which this operator will have access.

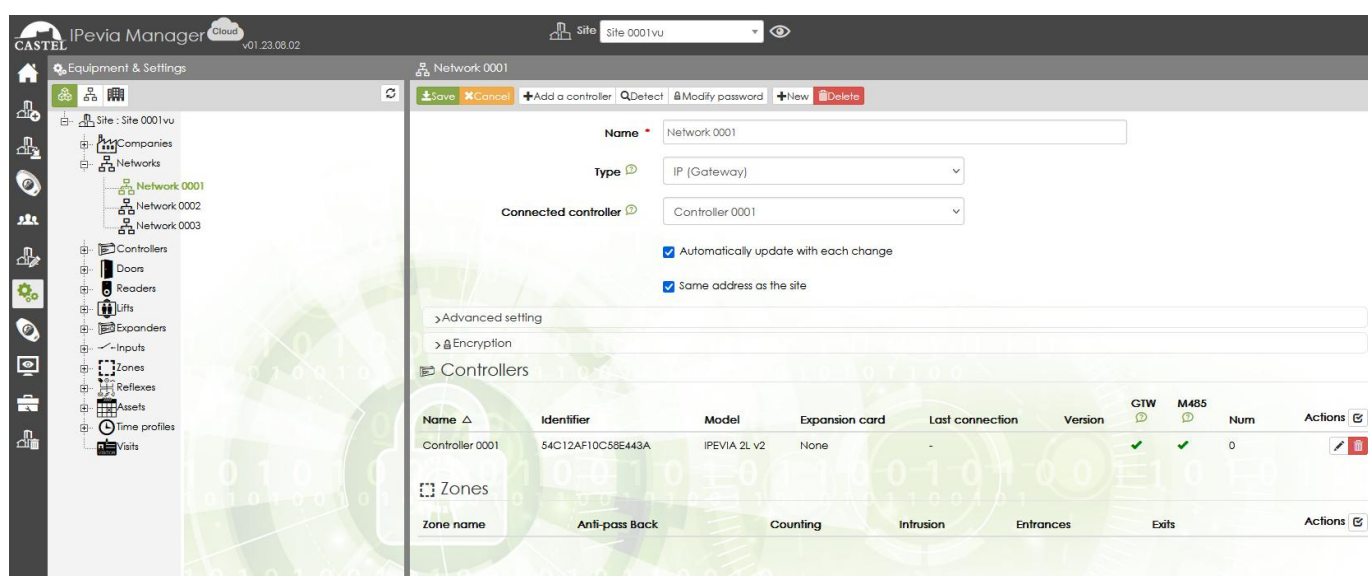
Note that an operator can be authorized by several companies. It is also possible to limit access to the software according to specified dates or times.

### 3.3. Réseaux

Un réseau comprend jusqu'à 64 centrales capables de communiquer entre elles. Au-delà, il est nécessaire de créer un autre réseau.

Si une organisation dispose de sites dans différentes localisations géographiques, des réseaux supplémentaires doivent être créés. Par exemple, une entreprise avec des bureaux à Paris et à Lyon ainsi qu'un site de production correspond à 3 réseaux dans le logiciel.

Ensuite, dans la gestion quotidienne, l'opérateur logiciel ajoute des clés au site sans avoir à gérer spécifiquement les transferts vers un ou plusieurs réseaux.



Un réseau est défini comme suit :

**Connexion** : il s'agit du dialogue entre le serveur et la première unité de contrôle. Cela peut être TCP/IP ou USB. Dans le cas de l'USB, les autres unités de contrôle sont reliées entre elles en TCP/IP via un câble Ethernet.

**Type** : "IP locale" signifie que chaque unité de contrôle du réseau interroge directement le serveur. C'est le choix par défaut pour une installation sur un réseau interne. "IP Distant" fait référence à un réseau géré via Internet. Dans ce cas, une unité de contrôle du réseau agit comme une passerelle pour les autres.

**Port UDP** : Les centrales utilisent des ports UDP (user datagram protocol) pour communiquer entre elles. Ce port peut être modifié si l'équipement réseau utilise déjà ce port.

Cela peut être le cas lorsque le même réseau physique supporte deux réseaux d'unités de contrôle Ipevia.

## 3.4 Centrales

Les centrales regroupent l'intelligence du contrôle d'accès. Ils gèrent la porte en libérant la serrure si la carte présentée est enregistrée dans le logiciel Ipévia.

Pour voir les contrôleurs sur le site, cliquez sur l'icône en forme de roue dentée "équipements et paramètres" à gauche. Tous les appareils apparaissent sous le nœud "contrôleur". En sélectionnant l'un d'eux dans l'arborescence (cadre de gauche), les détails s'affichent à droite. Un contrôleur est défini comme suit :

| Field                    | Description                                                                                                                                                                                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nom                      | Avec 32 caractères                                                                                                                                                                                                                                                                                |
| ID                       | ID de la centrale, marqué sur son étiquette                                                                                                                                                                                                                                                       |
| Modèle de centrale       | Ne peut être modifié                                                                                                                                                                                                                                                                              |
| Options                  | 4 portes Wiegand / option 12 sorties/entrée                                                                                                                                                                                                                                                       |
| Leds                     | Désactiver l'éclairage des LEDs                                                                                                                                                                                                                                                                   |
| Serveur de communication | Désactiver les communications serveur / panneau de contrôle. Cette option est utile lorsque le panneau de contrôle n'est pas encore en service ou ne l'est plus. Le serveur ne tente pas de communiquer avec lui.                                                                                 |
| Configuration TCP/IP     | <ul style="list-style-type: none"> <li>DHCP ou IP fixe</li> <li>Si IP fixe, adresse, masque et passerelle</li> <li>DNS (serveur de noms de domaine), manuel ou automatique. Ces informations doivent être saisies lorsque le panneau de contrôle est géré sur Ipévia.com, par exemple.</li> </ul> |
| Configuration avancée    | La centrale peut redémarrer quotidiennement à une heure spécifiée de la journée.                                                                                                                                                                                                                  |

Notez qu'il est possible de modifier la configuration de plusieurs contrôleurs en une seule opération.

The screenshot displays the IPEVIA Manager web interface. The top navigation bar includes the CASTEL logo, the title 'IPEVIA Manager', a version number 'v01.23.08.02', and a site selector 'Site: Site 0001vu'. The left sidebar shows a tree view of the system hierarchy: Site: Site 0001vu, Companies, Networks, Controllers (with sub-items Controller 0001, Controller 0002, and Controller 0003), Doors, Readers, Lifts, Expanders, Inputs, Zones, Reflexes, Assets, Time profiles, and Visits. The main content area is titled 'Controller 0001' and contains a form for configuration. The form includes fields for Name (Controller 0001), Identifier (54C12AF10C58E443A), Name of the network (Network 0001 (IP (Gateway))), Model (IPEVIA 2L v2 (Wiegand controller v2 - 2 readers)), Expansion card (None), Companies (empty), Location (empty), Activation of leds (checked), Disable communication (unchecked), Reader profiles (None), and Status (Disconnected). Below the form, there are links for '> IP configuration' and '>>> Advanced setting'. At the bottom, a table titled 'Doors' lists the configured doors.

| Name ▲                       | Position | Location | Actions |
|------------------------------|----------|----------|---------|
| Controller 0001 - Porte 0001 | 1        | -        |         |
| Controller 0001 - Porte 0002 | 2        | -        |         |

### 3.5. Portes

D'un point de vue matériel, la porte est :

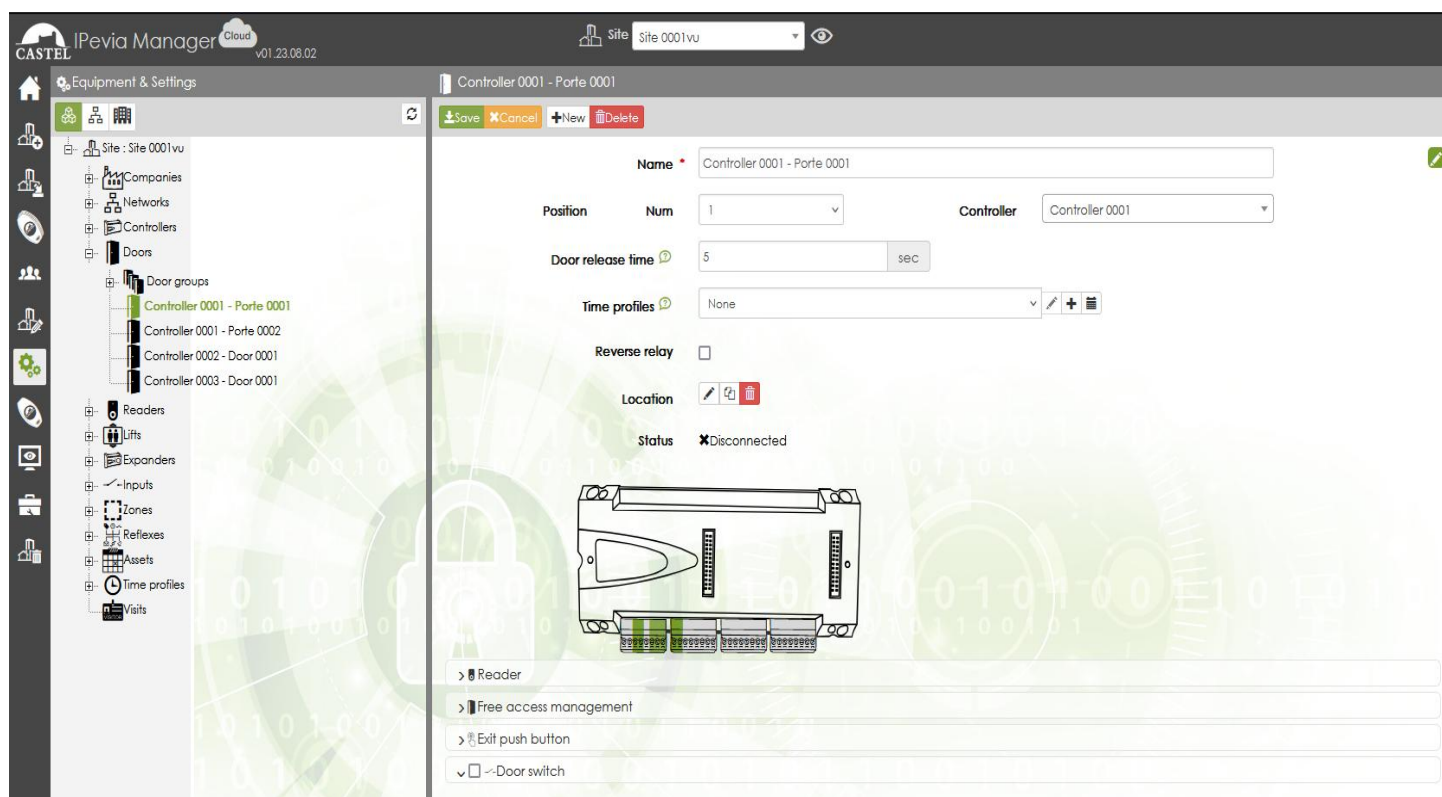
- Une entrée pour un lecteur Wiegand
- Une entrée pour le bouton de sortie
- Une entrée pour le contact de porte
- Un relais pour contrôler la serrure électrique

Dans le logiciel, les paramètres suivants peuvent être personnalisés :

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                       | Avec 32 caractères                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Position of the controller | C'est une fonction utile lorsque qu'un lecteur est relié à un contrôleur mais doit être géré par un autre contrôleur. Dans ce cas, les horaires, la configuration Wiegand ou les informations liées à la sécurité sont également gérées par ce second contrôleur.                                                                                                                                                                          |
| Type                       | Ce champ optionnel est disponible lorsque la fonction « verrous connectés sécurisés » est activée dans les « propriétés du site ». Ce champ précise si la porte est configurée comme « câblée » (configuration standard) ou avec des « verrous connectés sécurisés ». Si cette seconde option est sélectionnée, un nouveau champ est ajouté au formulaire de configuration de la porte.                                                    |
| Schedule profile           | Un planning avec des créneaux horaires d'accès libre (la porte est déverrouillée), des créneaux horaires interdits (même une clé valide ne déverrouille pas la porte), et des créneaux horaires réguliers (une clé valide est nécessaire pour ouvrir la porte).                                                                                                                                                                            |
| Reader                     | <p>Par défaut, la porte 1 est associée à la lecteur 1, la porte 2 avec le lecteur 2. Il est possible de lier deux lecteurs (maximum 6 appareils) à une porte. Cela permet de dédier un lecteur à l'entrée et un autre à la sortie.</p> <p>Il est également possible de lier plusieurs portes à un seul lecteur. Par exemple, un lecteur permet à l'utilisateur A d'ouvrir la porte piétonne et à l'utilisateur B d'ouvrir la barrière.</p> |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Push button  | <p>Par défaut, le bouton-poussoir fonctionne 24h/24 et 7j/7. Vous pouvez appliquer un emploi du temps et restreindre son fonctionnement à des heures spécifiques de la journée. Par exemple, il peut être utilisé pour interdire la sortie par une porte après une certaine heure. Voir le chapitre 4.11.1 pour créer un emploi du temps avec bouton-poussoir.</p> <p>Un mode avancé peut être activé pour gérer le lien entre le bouton-poussoir de sortie et la porte. Par défaut, l'entrée "Push button 1" contrôle la porte 1, "Push button 2" contrôle la porte 2. Cependant, vous pouvez lier deux boutons-poussoirs à une même porte.</p> |
| Door contact | <p>Le contact de porte est une fonction native du contrôleur. Il peut être de différents types : tout ou rien, impédance (la valeur de la résistance de fin de ligne doit être spécifiée), ou contact distant (si des serrures électroniques sont utilisées).</p>                                                                                                                                                                                                                                                                                                                                                                                |

Cochez également "déclencher les événements de sécurité" si vous souhaitez gérer les événements tels que "porte forcée" ou "porte ouverte trop longtemps". Dans ce cas, spécifiez le délai en secondes après lequel la porte est considérée comme ouverte trop longtemps..



## 3.6 Lecteurs

Les lecteurs internes ou externes produits par la société FDI peuvent communiquer avec le système Ipévia via des méthodes câblées ou connectées.

- Lecteurs 2Smart (bus propriétaire 2 fils de FDI avec une portée allant jusqu'à 100 m)
  - Lecteurs Wiegand FDI ou de concurrents (bus universel 8 fils avec une portée allant jusqu'à 100 m)
  - Lecteur RS485 : bus propriétaire 4 fils de FDI avec une portée allant jusqu'à 1000 m
- Ipévia peut intégrer des lecteurs externes, tels que des caméras de reconnaissance de plaques d'immatriculation Dahua ou des poignées connectées Assa Abloy.
- Avec un câble IP logique (par exemple, pour la caméra de reconnaissance de plaques d'immatriculation Dahua)

Par le biais de passerelles industrielles connectées et intégrées au système Ipévia (par exemple, pour les poignées et serrures électroniques) Quel que soit le choix du lecteur ou du câblage, la limite de lecteurs par panneau de contrôle est de 6 appareils.

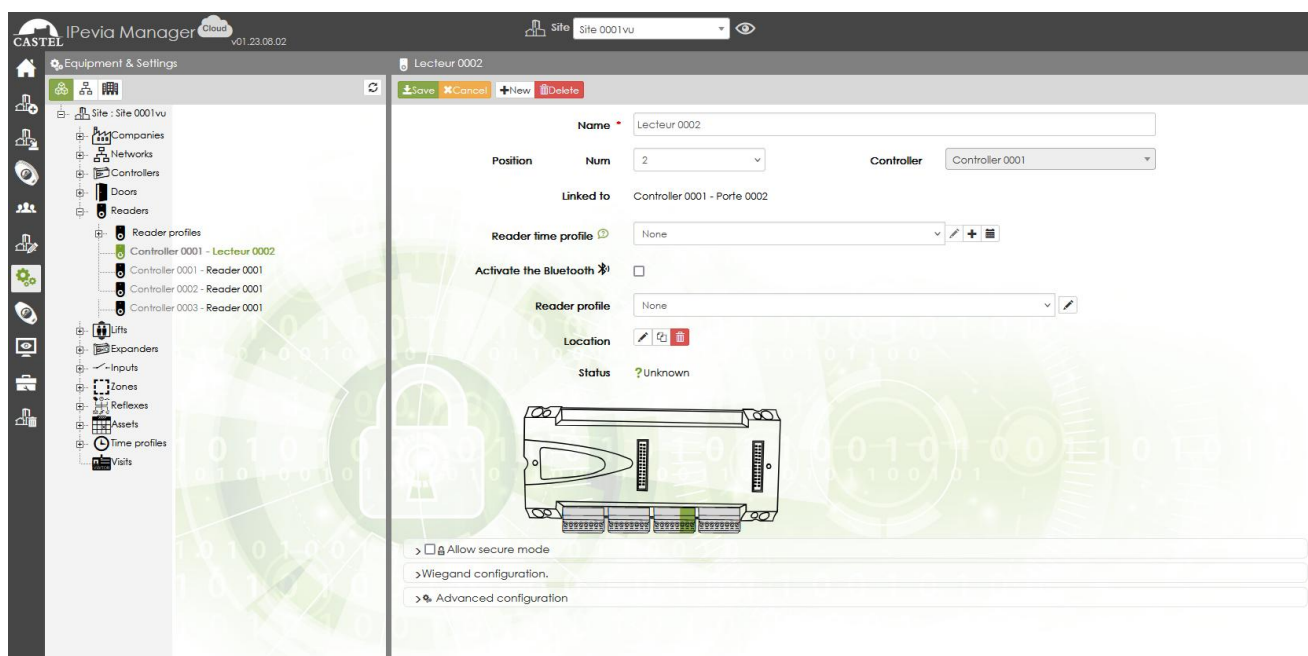
Exemple : l'ajout d'un lecteur ANPR (reconnaissance de plaques d'immatriculation) remplace un lecteur sur le panneau de contrôle.

## Paramétrage standard

Avec Ipévia Manager, les lecteurs sont configurables comme suit :

| field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nom</b>                     | Avec 32 caractères                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Position de la centrale</b> | Fonction utile lorsqu'un lecteur est lié à un contrôleur mais doit être géré par un autre. Dans ce cas, les horaires, la configuration Wiegand ou les informations liées à la sécurité sont également prises en charge par ce second contrôleur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Wiegand configuration</b>   | <p>Par défaut, une seule credential (clé, code clavier, empreinte digitale, etc.) suffit pour avoir accès à une porte. Avec Ipévia Manager, vous pouvez ajouter des conditions temporelles :</p> <ul style="list-style-type: none"> <li>• <b>Double authentification</b> : pendant les heures de travail, une clé suffit pour ouvrir la porte. Lorsque le bureau est fermé, il faut une clé + un code PIN.</li> <li>• <b>Délai en secondes</b> : entre la lecture de la clé et la saisie du code PIN (10 secondes par défaut).</li> <li>• <b>Contact sec</b> : Pour entrer dans un parking, il vous faut une clé ou une télécommande et un véhicule détecté sur une boucle magnétique.</li> <li>• <b>Contact de porte</b> : pour ouvrir la porte B, vous devez d'abord ouvrir la porte A. Ce mode permet de créer un vestibule d'entrée.</li> <li>• <b>Présence du responsable</b> : vous ne pouvez entrer que si le responsable a déjà validé son accès sur le lecteur d'entrée. Par exemple, un employé de production ne peut entrer dans l'usine que si le responsable de production est dans la zone.</li> </ul> |
| <b>Configuration Wiegand</b>   | <p>Configuration Wiegand : par défaut, le contrôleur s'adapte au protocole reçu. Les protocoles de base gérés sont Wiegand 26, 30, 32, 34 bits en hexadécimal.</p> <p>Vous pouvez également choisir le protocole 34 bits décimal pour les claviers Braille.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Exemple de champs configurables dans le menu "lecteur"..



## Lecteur ANPR

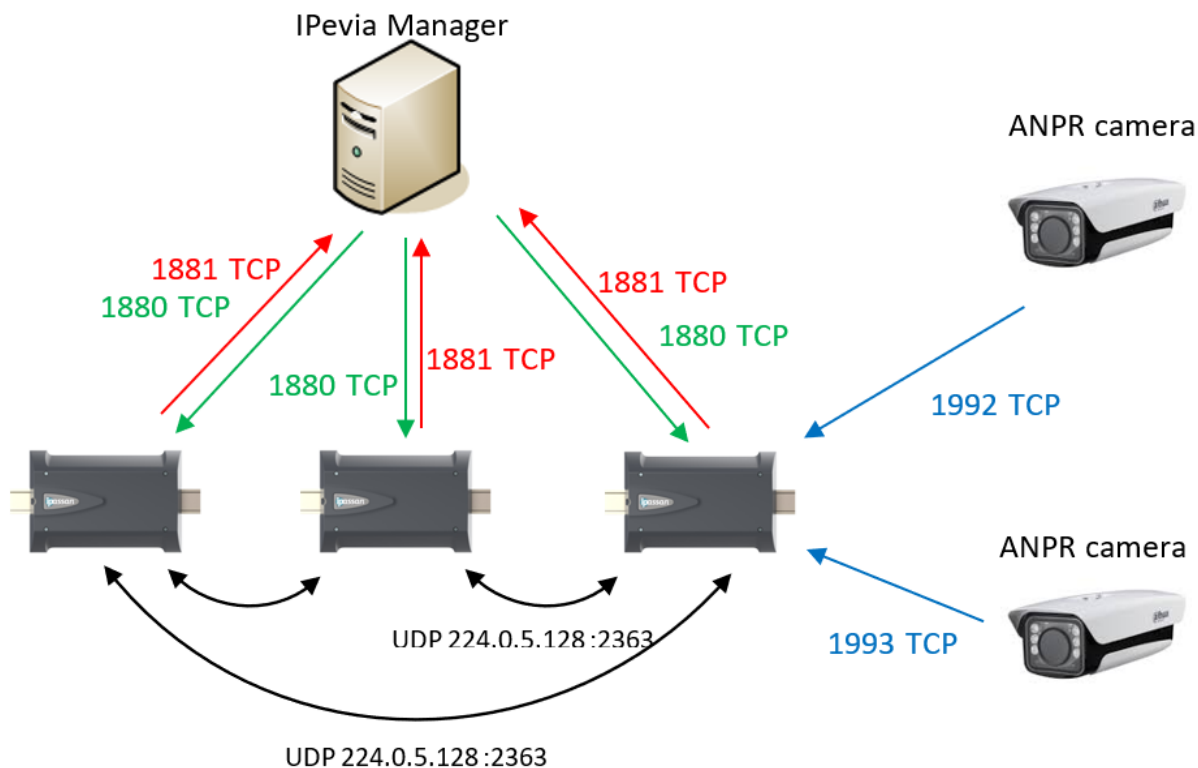
Ipévia permet de connecter jusqu'à 4 caméras de reconnaissance de plaques d'immatriculation (ANPR) par unité centrale. Ces caméras communiquent via IP avec l'unité centrale et transmettent le numéro de la plaque d'immatriculation en texte intégral. Par exemple, la plaque AG-891-CX, programmée dans le logiciel, sera autorisée, contrairement à un équivalent Wiegand. Les événements afficheront également les plaques en texte clair, que les voitures soient autorisées ou non.

**Prérequis :** L'intégration intelligente des ANPR (reconnaissance automatique des plaques d'immatriculation) nécessite une carte d'activation pour chaque unité centrale gérant les caméras.

Il existe deux types d'intégration des caméras ANPR disponibles dans le menu "lecteur" :

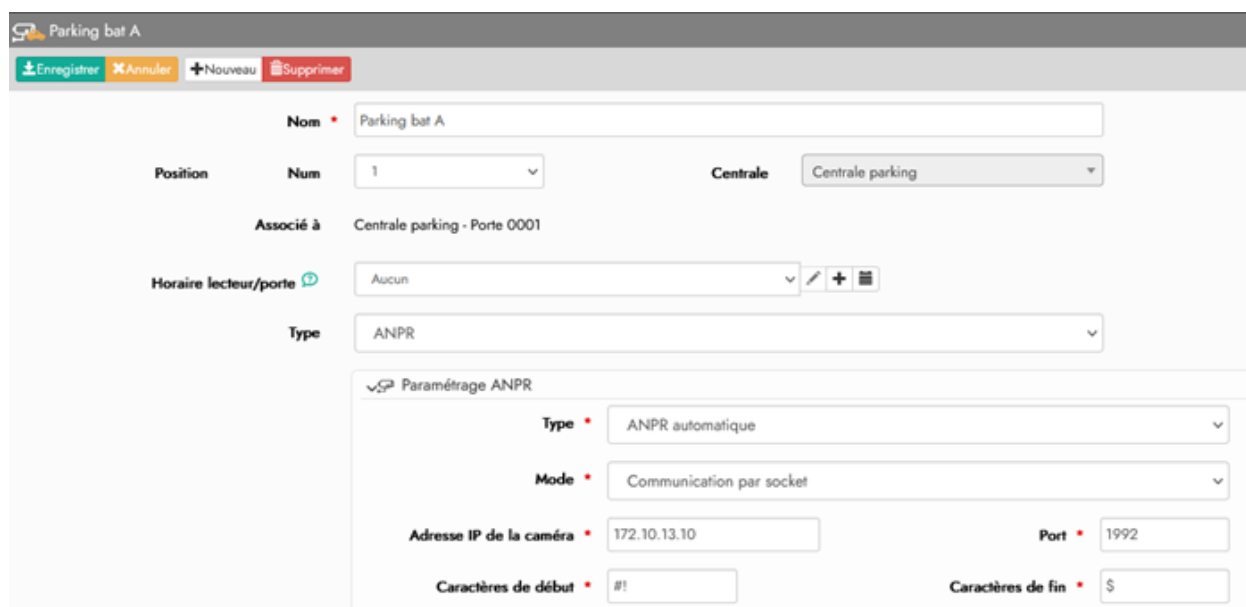
- **Automatique :** Dès qu'une plaque est lue, le système ANPR transmet le numéro à l'unité centrale, qui le traite comme un badge.
- **Avec Trigger :** Lorsqu'un capteur connecté à une entrée détecte un véhicule, l'unité centrale demande au système ANPR de fournir le numéro lu.

Ces caméras intégrées (Dahua et le logiciel OCR Innova) doivent communiquer avec l'unité centrale via TCP. Voir le diagramme ci-dessous.



Après que la carte d'activation ait été validée pour l'unité centrale, vous pouvez choisir le type ANPR dans les paramètres du lecteur.

## Automatic type ANPR

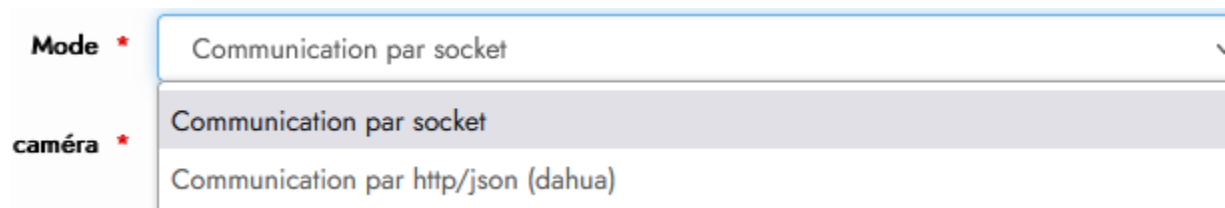


The screenshot shows the configuration page for a parking unit named "Parking bat A". At the top, there are buttons for "Enregistrer", "Annuler", "Nouveau", and "Supprimer". The main form includes fields for "Nom" (Parking bat A), "Position" (Num 1), "Centrale" (Centrale parking), "Associé à" (Centrale parking - Porte 0001), "Horaire lecteur/porte" (Aucun), and "Type" (ANPR). Below these is a section titled "Paramétrage ANPR" which contains:
 

- Type**: ANPR automatique
- Mode**: Communication par socket
- Adresse IP de la caméra**: 172.10.13.10
- Port**: 1992
- Caractères de début**: #!
- Caractères de fin**: \$

Sélectionnez "automatique" dans l'onglet des paramètres ANPR et entrez l'adresse IP et le port utilisés par la caméra.

Pour définir la communication entre l'unité centrale et l'ANPR utilisé, sélectionnez le protocole intégré correspondant au matériel dans le menu "mode".



This close-up shows the "Mode" dropdown menu. The selected option is "Communication par socket". Below it, another option "Communication par http/json (dahua)" is visible, which is highlighted by the mouse cursor.

Communication par socket (lien entre deux programmes) : destinée aux caméras Dahua avec firmware australien (ITC237) et au logiciel OCR Innova dans le scénario 4.

Communication HTTP/JSON : destinée aux caméras Dahua disponibles en 2022 (firmware non australien) telles que ITC 437, ITC 415, ITC 237, ITC 215.

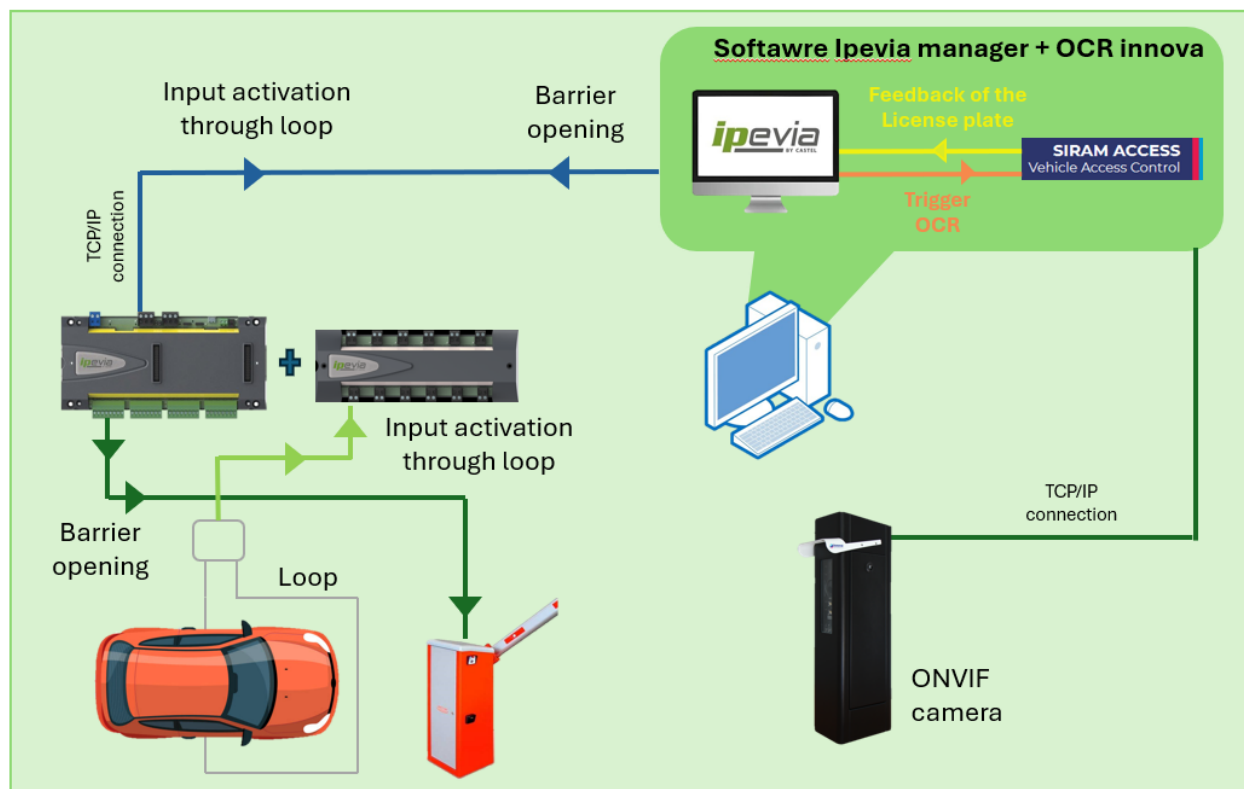
REMARQUE : les caractères de début et de fin sont les caractères par défaut définis dans la communication.

## ANPR on trigger

Cette option est liée aux dispositifs OCR Innova (reconnaissance optique de caractères).

Plus d'informations sur : [www.innovagroupbcn.com](http://www.innovagroupbcn.com)

Cette intégration repose sur la communication TCP/IP.



Lorsque l'entrée connectée au détecteur de véhicule est activée, le contrôleur demande alors à l'OCR (reconnaissance optique de caractères) de transmettre le numéro de plaque d'immatriculation du véhicule détecté. Si le numéro est reconnu, la barrière s'ouvre.

**Parking bat A**

Enregistrer Annuler Nouveau Supprimer

Nom \* Parking bat A

Position Num 1 Centrale Centrale parking

Associé à Centrale parking - Porte 0001

Horaires lecteur/porte Aucun

Type ANPR

Paramétrage ANPR

Type \* ANPR sur déclencheur

Adresse IP de la caméra \* 172.10.13.10 Port \* 22601

Numéro de voie \* 1

Entrée concernée \* Centrale parking - Entrée ...

Timeout \* 5000 ms

Pour cette configuration, les éléments suivants doivent être spécifiés :

- L'adresse IP de l'ordinateur où le logiciel OCR (reconnaissance optique de caractères) Innova est installé.
- Le numéro de canal.
- L'entrée utilisée par le détecteur de véhicule.
- L'ajustement du délai maximum de communication.

L'entrée utilisée doit être configurée comme un type tout-ou-rien (NO normalement ouvert ou NC normalement fermé).

Si 4 caméras sont présentes sur le site, chaque logiciel OCR Innova utilisera son port de communication respectif. Par défaut :

- Le canal 1 utilisera le port 22601.
- Le canal 2 utilisera le port 22602.
- Le canal 3 utilisera le port 22603.
- Le canal 4 utilisera le port 22604.

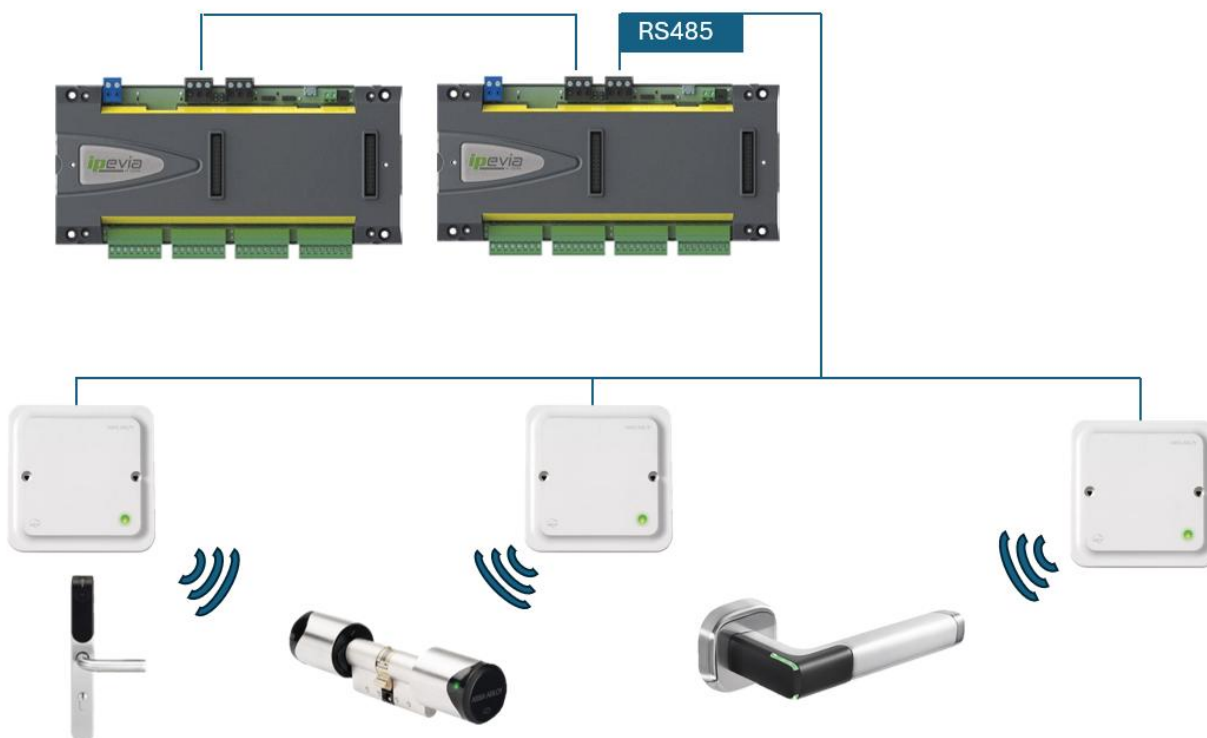


La caméra doit être également configurée.

## Serrures électroniques sécurisées

L'intégration des serrures connectées est disponible en activant l'option dans les fonctionnalités du site (voir chapitre 3.1).

Cette intégration repose sur l'utilisation du bus "RS485 aux" pour connecter les "hubs Apério" reliés aux "lecteurs et serrures Apério" : voir le schéma ci-dessous.



Chaque contrôleur Ipévia peut gérer jusqu'à 6 serrures connectées via 6 hubs (capacité habituelle, quel que soit le type de technologie porte/lecteur).

Il est possible de combiner des lecteurs "standards" et des dispositifs connectés sur le même contrôleur, dans les mêmes limites.

Les serrures intelligentes sont configurées en 5 étapes (de A à E) :

A- Dans les fonctionnalités du site (voir chapitre 3.1) cocher l'option :



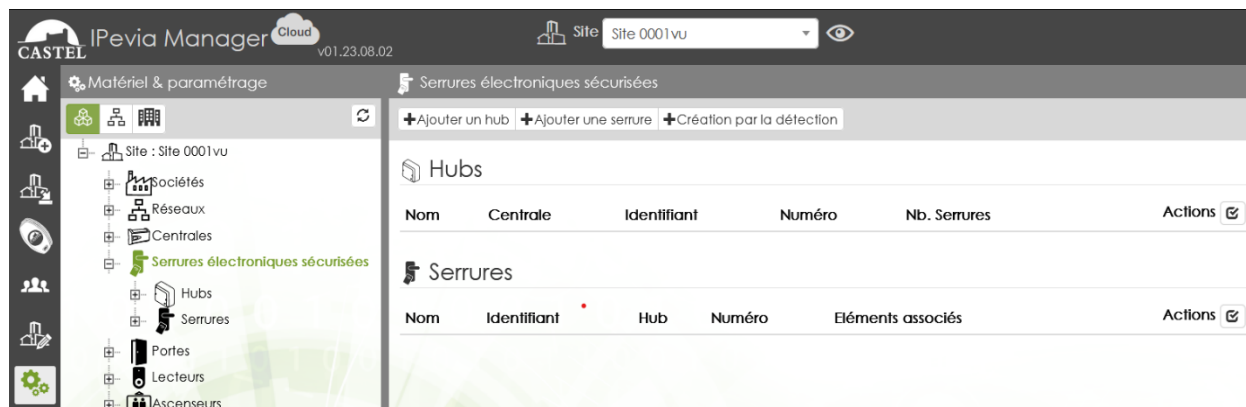
B- Dans la page de configuration des centrales :

- Sélectionner le bus « Apério » dans le champs « type rs485 ».
- Activer la carte module nécessaire. Pour plus d'informations contactez les équipes commerciale de CASTEL



Le "type RS485" peut soit être standard ou Aperio. Modules = N° de la carte d'activation renseignée.

- C- Utiliser le logiciel Aperio afin d'appairer des "hubs" ou serrures (voir le manuel d'utilisateur spécifique à ce logiciel)
- D- Ouvrir le menu d'intégration "serrures électroniques » pour configurer les appareils.



Il existe deux modes : automatique (D1) ou manuel (D2) :

- D1 Sélectionner "création par détection" quand les hubs et serrures sont connectés au bus rs485 de la centrale Ipevia.

Chaque appareil connecté sera affiché dans le tableau :

| Détecter                            |         |                 |      |                     |        |
|-------------------------------------|---------|-----------------|------|---------------------|--------|
| <input checked="" type="checkbox"/> | Module  | Identifiant     | Type | Id                  | Option |
| <input checked="" type="checkbox"/> | Serrure | 1094F3          | -    | RS485_cylinder-2-0  | -      |
| <input checked="" type="checkbox"/> | Serrure | 01EE00          | -    | RS485_cylinder-18-0 | -      |
| <input checked="" type="checkbox"/> | Serrure | 01EE01          | -    | RS485_cylinder-34-0 | -      |
| <input checked="" type="checkbox"/> | Hub     | 00124B0024B27F1 | -    | RS485_gateway-2-0   | -      |

Cochez chaque ligne correspondant aux dispositifs à configurer. Cela enregistrera toutes les données nécessaires pour la configuration globale du matériel (étape D2).

**D-2-** Sélectionner "ajouter un hub" ou "ajouter une serrure ». Ensuite, remplir les champs nécessaires pour finir la configuration.

Hub 0001

[Enregistrer](#)
[Annuler](#)
[Ajouter une serrure](#)
[Nouveau](#)
[Supprimer](#)

Nom \* Hub 0001

Adresse MAC \* 00124B00248F27F1

Localisation   

Paramétrage Apero RS485

Centrale \* Controller 0001

Numéro \* 2

Statut ? Inconnu

Maintenant que la configuration est terminée, ces serrures connectées peuvent être utilisées comme tous les lecteurs sur le site. Vous pouvez consulter les profils d'accès ou visualiser les nouveaux événements liés aux serrures connectées.

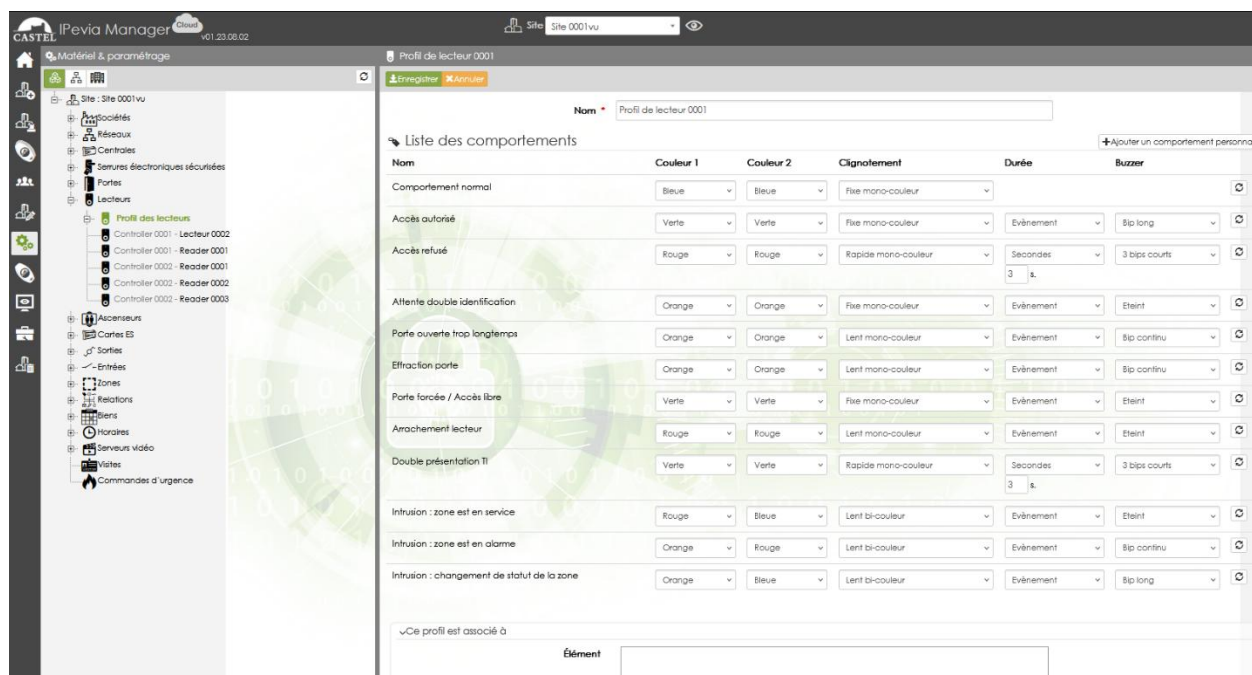
Événements

[Visualisation](#)
[Télécharger](#)
[Archives](#)
[Paramétrage global](#)
[Paramétrage](#)

|                     |                                            |                                                                    |             |                                                                                                                                                                                  |   |
|---------------------|--------------------------------------------|--------------------------------------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 2022-07-28 11:52:36 | Accès autorisé porte simple identification | Controller 0001 - Door 0001<br>Reader 0001<br>Access profiles 0001 | Reader 01   |   7B57485A | 3 |
| 2022-07-28 11:51:57 | Communication OK Hub                       | Hub 0001                                                           | -           | -                                                                                                                                                                                | 3 |
| 2022-07-28 11:51:56 | Niveau Batterie                            | Serrure 0001                                                       | Batterie ok | -                                                                                                                                                                                | 5 |
| 2022-07-28 11:51:55 | Niveau Batterie                            | Serrure 0001                                                       | Batterie ok | -                                                                                                                                                                                | 5 |
| 2022-07-28 11:51:55 | Communication OK Serrure                   | Serrure 0001                                                       | -           | -                                                                                                                                                                                | 3 |
| 2022-07-28 11:51:42 | Communication Ko Hub                       | Hub 0001                                                           | -           | -                                                                                                                                                                                | 6 |
| 2022-07-28 11:50:03 | Communication OK Serrure                   | Serrure 0001                                                       | -           | -                                                                                                                                                                                | 3 |
| 2022-07-28 11:50:03 | Accès refusé : TI non reconnu              | Reader 0001                                                        | -           |  4E3C334A                                                                                   | 4 |

## Profils de lecteurs

Le comportement des lecteurs est défini par le contrôleur. Par défaut, il est configuré comme indiqué ci-dessous :



**Profil de lecteur 0001**

Nom : Profil de lecteur 0001

Liste des comportements

| Nom                                         | Couleur 1 | Couleur 2 | Clignotement        | Durée            | Buzzer        |
|---------------------------------------------|-----------|-----------|---------------------|------------------|---------------|
| Comportement normal                         | Bleue     | Bleue     | Fixe mono-couleur   |                  |               |
| Accès autorisé                              | Verte     | Verte     | Fixe mono-couleur   | Événement        | 8ip long      |
| Accès refusé                                | Rouge     | Rouge     | Rapide mono-couleur | Secondes<br>3 s. | 3 bips courts |
| Attente double identification               | Orange    | Orange    | Fixe mono-couleur   | Événement        | Eteint        |
| Porte ouverte trop longtemps                | Orange    | Orange    | Lent mono-couleur   | Événement        | 8ip continu   |
| Effraction porte                            | Orange    | Orange    | Lent mono-couleur   | Événement        | 8ip continu   |
| Porte forcée / Accès libre                  | Verte     | Verte     | Fixe mono-couleur   | Événement        | Eteint        |
| Arrachement lecteur                         | Rouge     | Rouge     | Lent mono-couleur   | Événement        | Eteint        |
| Double présentation TI                      | Verte     | Verte     | Rapide mono-couleur | Secondes<br>3 s. | 3 bips courts |
| Intrusion : zone est en service             | Rouge     | Bleue     | Lent bi-couleur     | Événement        | Eteint        |
| Intrusion : zone est en alarme              | Orange    | Rouge     | Lent bi-couleur     | Événement        | 8ip continu   |
| Intrusion : changement de statut de la zone | Orange    | Bleue     | Lent bi-couleur     | Événement        | 8ip long      |

✓Ce profil est associé à

Élément

Cependant, les paramètres peuvent être modifiés pour créer un profil de lecteur personnalisé. Vous pouvez les appliquer à un contrôleur spécifique en le sélectionnant sous l'onglet intitulé « Ce profil est associé à ».

## 3.7. Ascenseurs

Un ascenseur dans Ipévia est défini comme suit :

- Un nom de 32 caractères.
- Une position sur le panneau de contrôle et le nom du panneau de contrôle.
- Emplacement : pour utiliser la fonctionnalité ascenseur dans Ipévia, il est nécessaire de créer au moins le bâtiment et les étages lors de l'étape Architecture pendant la création du site (chapitre 3.4).
- Lecteur : le paramètre par défaut est un lecteur par cabine d'ascenseur, mais vous pouvez en ajouter un second en décochant « lecteur par défaut » et en sélectionnant des lecteurs.
- Minuteur d'activation : il existe deux minuteurs différents, l'un en secondes pour les utilisateurs de badge. Ils présentent leur badge au lecteur dans la cabine, puis appuient sur le bouton de leur étage.

Pour les visiteurs, le système gère un délai en minutes. En général, le visiteur appelle depuis le combiné d'interphonie, le standard reçoit l'appel et autorise le visiteur à ouvrir la porte via son interphone.

Grâce à un bouton supplémentaire, le standard fournit un contact sec à une entrée d'Ipévia, autorisant le visiteur à utiliser l'ascenseur pour accéder uniquement à l'étage correct. Dans Ipévia Manager, cochez « Interphonie », saisissez le délai en minutes ainsi que l'entrée du système utilisée pour chaque étage.

**Étage / sortie** : étant donné que le bâtiment a été sélectionné ci-dessus, le logiciel propose la liste correcte des étages.

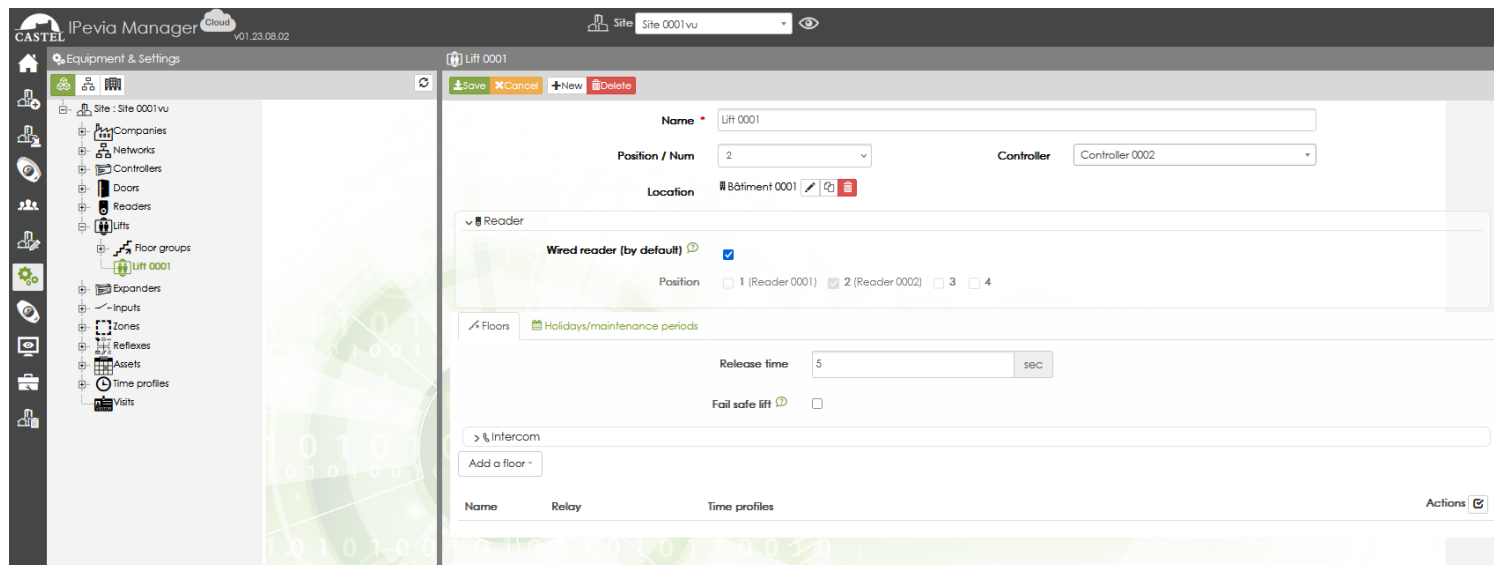
Sélectionnez le relais associé à chaque étage.

**Calendrier** : un calendrier contient des créneaux horaires pendant lesquels l'étage est :

- **Non sécurisé ou accès libre** : le bouton de l'étage peut être sélectionné sans clé.
- **Interdit** : même une clé valide ne permet pas d'accéder à cet étage.
- **Normal** : une clé valide est requise pour accéder à l'étage.

**Interphonie** : lorsque les visiteurs doivent être autorisés à entrer dans les ascenseurs via le système d'interphone, Ipévia utilise des entrées pour récupérer les contacts secs de ces interphones.

**Ajouter un étage** : une fois « contact sec » renseigné dans le champ précédent, sélectionnez l'entrée correspondant à chaque étage.

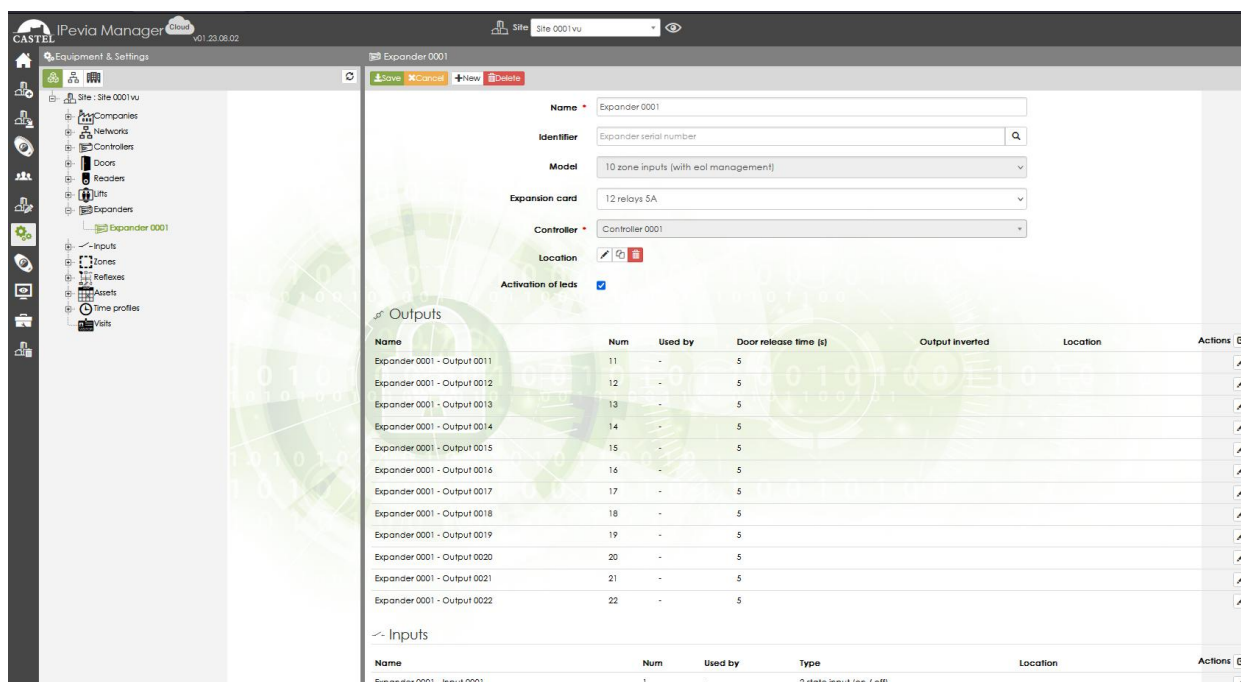


### 3.8. Carte ES (entrée/sortie)

Chaque centrale gère jusqu'à 10 cartes d'entrée/sortie. Ces cartes possèdent un identifiant unique qui doit être saisi dans le logiciel lors de la mise en service.

Une carte est définie dans le logiciel comme suit :

- Un nom en 32 caractères
- Un identifiant unique de type 517xxxx
- Une option : soit une carte 12 entrées ou 12
- La centrale à laquelle cette carte est câblée
- Une société à laquelle cette carte (et ce qui est câblé dessus » et attribuée



**Outputs**

| Name                        | Num | Used by | Door release time (s) | Output inverted | Location | Actions |
|-----------------------------|-----|---------|-----------------------|-----------------|----------|---------|
| Expander 0001 - Output 0011 | 11  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0012 | 12  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0013 | 13  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0014 | 14  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0015 | 15  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0016 | 16  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0017 | 17  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0018 | 18  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0019 | 19  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0020 | 20  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0021 | 21  | -       | 5                     |                 |          | [Edit]  |
| Expander 0001 - Output 0022 | 22  | -       | 5                     |                 |          | [Edit]  |

**Inputs**

| Name                       | Num | Used by | Type                     | Location | Actions |
|----------------------------|-----|---------|--------------------------|----------|---------|
| Expander 0001 - Input 0001 | 1   | -       | 2 state input (on / off) |          | [Edit]  |

### 3.9. Entrées

D'un point de vue matériel, les entrées d'Ipévia sont soit une option de 12 entrées sur le contrôleur, soit une carte distante sur le bus RS485.



Une centrale dont le bus "RS485Aux" est configuré pour communiquer avec le système Aperio ne peut pas communiquer avec les entrées/sorties ou les lecteurs RS485 FDI.

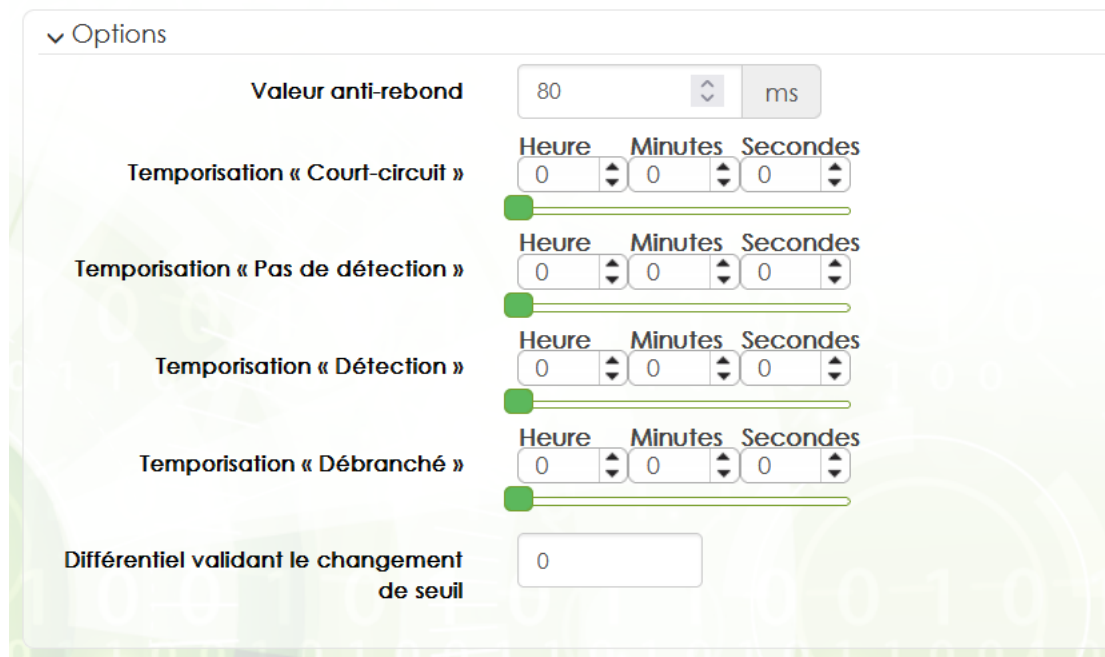
Une entrée est définie comme suit :

| Champ | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nom   | Avec 32 caractères                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Type  | <ul style="list-style-type: none"> <li>- <b>Tout ou rien:</b> l'entrée est soit dans un état actif, soit dans un état inactif. L'entrée peut être configurée comme normalement ouverte (NO) ou normalement fermée (NC).</li> <li>- <b>Impedance (EOL):</b> grâce aux résistances de fin de ligne, l'entrée différencie les circuits ouverts (coupure de câble/sabotage), les courts-circuits (sabotage), l'entrée inactive et l'entrée active. Sélectionnez les valeurs de résistance R1 (en série) et R2 (en parallèle). Par défaut, elle est de type NC (normally closed).</li> <li>- <b>Décimale :</b> l'entrée va analyser le signal qu'elle reçoit. Selon celui-ci, elle va lui attribuer une valeur comprise entre 0 et 4095. Trois seuils peuvent être ensuite définis.</li> </ul> |

|         |                                                                                                                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Société | Permet de relier une entrée (et ce qui est câblé dessus) à une société.<br>Exemple pour un capteur de présence qui serait dans un immeuble de bureaux et qui pointerait uniquement vers les locaux de l'entreprise A. |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Notez qu'une entrée à impédance est toujours de type NC (normalement fermée).

## Option d'adaptation de l'entrée



Options

Valeur anti-rebond: 80 ms

Temporisation « Court-circuit »: 0 Heures, 0 Minutes, 0 Secondes

Temporisation « Pas de détection »: 0 Heures, 0 Minutes, 0 Secondes

Temporisation « Détection »: 0 Heures, 0 Minutes, 0 Secondes

Temporisation « Débranché »: 0 Heures, 0 Minutes, 0 Secondes

Différentiel validant le changement de seuil: 0

Les paramètres individuels de l'entrée permettent d'ajuster le comportement de l'entrée aussi précisément que possible par rapport au signal, ou de définir un délai de commutation avant que l'état de l'entrée ne change dans le contrôleur.

La valeur antirebond consiste à filtrer finement le signal et à ignorer les interférences. Si elle est réglée à 80 m/s, le contrôleur ignorera tout signal s'il se produit moins de 80 m/s après le dernier signal.

« Validation différentielle du seuil de déplacement » est la valeur minimale requise pour passer à un autre statut (plage totale de 0 à 4095).

Pour surveiller l'entrée, le contrôleur peut surveiller la sélection d'impédance ou de TOR (actif/inactif).

Selon la valeur des 2 résistances (R1 et R2), il existe 4 états différents pour chaque entrée :

- Court-circuit
- Aucune détection

- Détection
- Déconnecté

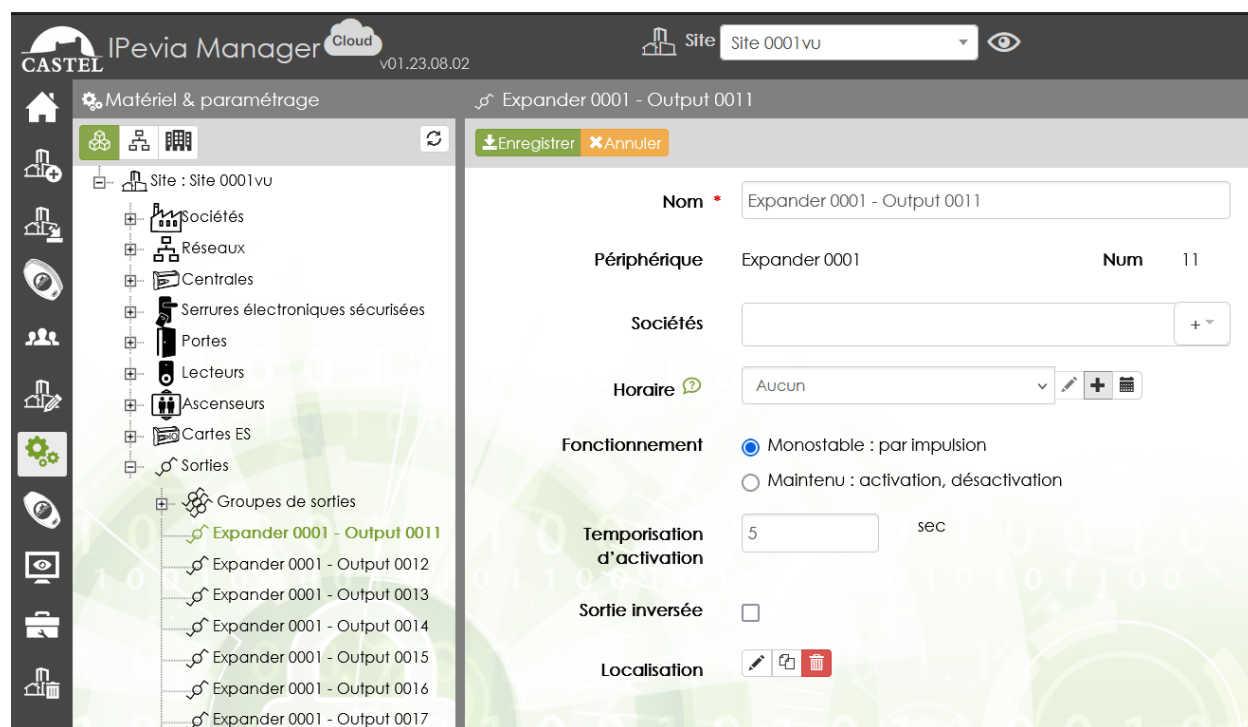
Le transfert de ces informations d'état au contrôleur peut être retardé dans la carte d'entrée en ajoutant un « temporisateur de maintien d'état ». Cela ajoute la fonction d'intégration du signal, améliorant ainsi votre fonctionnement :

Ajouter un délai de 30 secondes à une entrée connectée à un interrupteur de fin de course garantit que la position est atteinte, une fois le mouvement terminé.

## 3.10 Sorties

Les sorties Ipévia sont soit une option de 12 sorties insérée dans l'unité de contrôle, soit la même option insérée dans une carte RS485 de 10 entrées. Une sortie est définie comme suit :

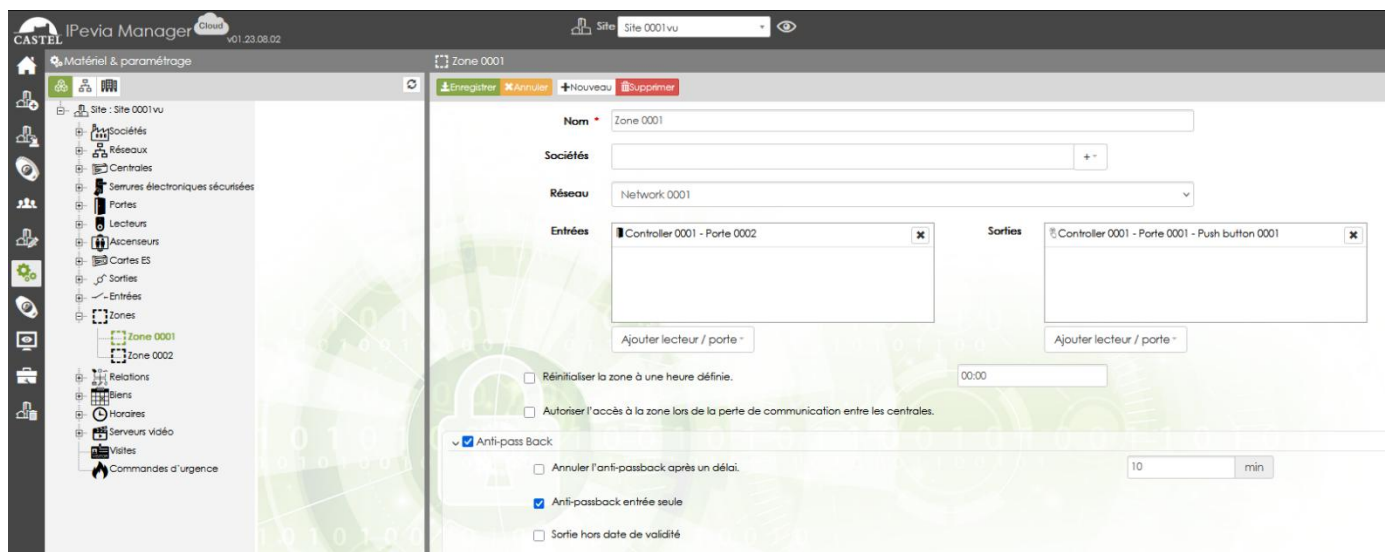
| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nom                        | Nom de 32 caractères                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Horaire                    | Si nécessaire, vous pouvez ajouter un emploi du temps à une entrée. Il contient des créneaux horaires pendant lesquels la sortie est : <ul style="list-style-type: none"> <li>- <b>Accès libre</b> : la sortie reste active, quelles que soient les commandes qu'elle peut recevoir (processus, relation, contrôle de l'ascenseur).</li> <li>- <b>Interdit</b> : la sortie reste inoccupée, quelles que soient les commandes.</li> <li>- <b>Normal</b> : une action (par exemple, un réflexe ou la présentation d'un badge au lecteur d'ascenseur) est requise pour activer la sortie.</li> </ul> |
| Fonctionnement             | <ul style="list-style-type: none"> <li>- « <b>Monostable : par impulsion</b> » : correspond à l'activation pendant le temps programmé.</li> <li>- « <b>Maintenu : activation, désactivation</b> » : correspond à l'activation jusqu'à la prochaine condition de désactivation.</li> </ul>                                                                                                                                                                                                                                                                                                         |
| Temporisation d'activation | Entrez la durée en secondes pendant laquelle la sortie sera activée (cas d'activation / indépendamment de la forçage).                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Sortie inversée            | Sélectionnez le statut du relais en cas de panne de courant. Par exemple, nous souhaitons que la sortie soit fermée au repos, mais ouverte en cas de panne de courant. Nous câblons donc le contact NO, mais définissons la sortie comme inversée.                                                                                                                                                                                                                                                                                                                                                |



### 3.11 Anti-pass back (APB)

Ipevia offre la possibilité de gérer le comptage (anti-pass back). Une zone de comptage est définie par des portes/lecteurs d'entrée et de sortie. Le système sait combien de personnes ou de véhicules se trouvent dans la zone et peut bloquer l'entrée lorsque le seuil est atteint. Cette fonctionnalité est utile pour les parkings, mais peut également être utilisée pour limiter le nombre de personnes dans une zone (piscine, salle commune...). Une option supplémentaire d'Ipevia permet de compter par appartement, groupe de personnes ou entreprise.

Exemples où l'APB est pertinent : **dans un parking commercial**, plusieurs entreprises utilisent le même parking, mais chaque entreprise n'a qu'un nombre prédéfini de places. Les employés de l'entreprise A ont tous des badges, mais seuls un certain nombre peuvent se garer en même temps. Pour que le comptage soit efficace, l'anti-pass back est souvent associé au comptage. L'APB empêche un utilisateur d'entrer dans une zone tant qu'il ne l'a pas quittée. Dans l'onglet « Équipement et paramètres » (dans le cadre gauche), sélectionnez « Zone » dans l'arborescence. Sélectionnez ou créez une zone. En bas de cette fenêtre, cochez la case « Anti-pass back » pour accéder aux autres paramètres.



Comme vous pouvez le voir sur la capture d'écran ci-dessus, Ipévia propose trois types d'anti-pass back.

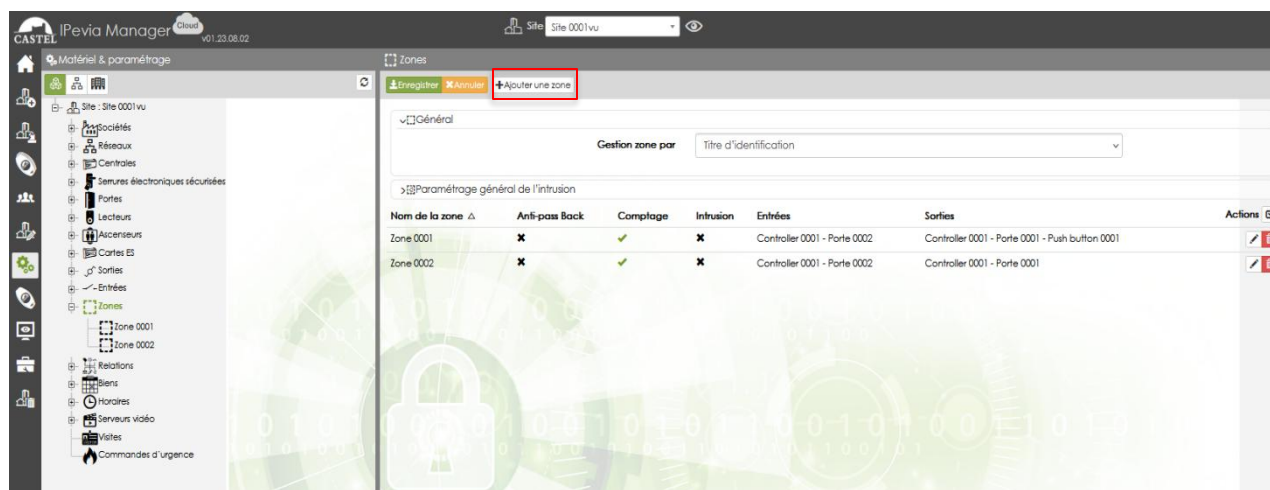
- **Annuler l'anti-pass back après un délai** : l'APB est annulé après un délai programmé.
- **APB entrée seule** : dans ce cas, les utilisateurs sont toujours autorisés à sortir.
- **Sortie hors date de validité (ou Soft APB)** : les utilisateurs peuvent sortir de la zone même après l'expiration de la période de validité. La seule condition pour être autorisé à sortir est d'être présent dans la zone. Cette option est utile pour les visiteurs quittant le parking après la fin de leur visite.

## Create a counting zone

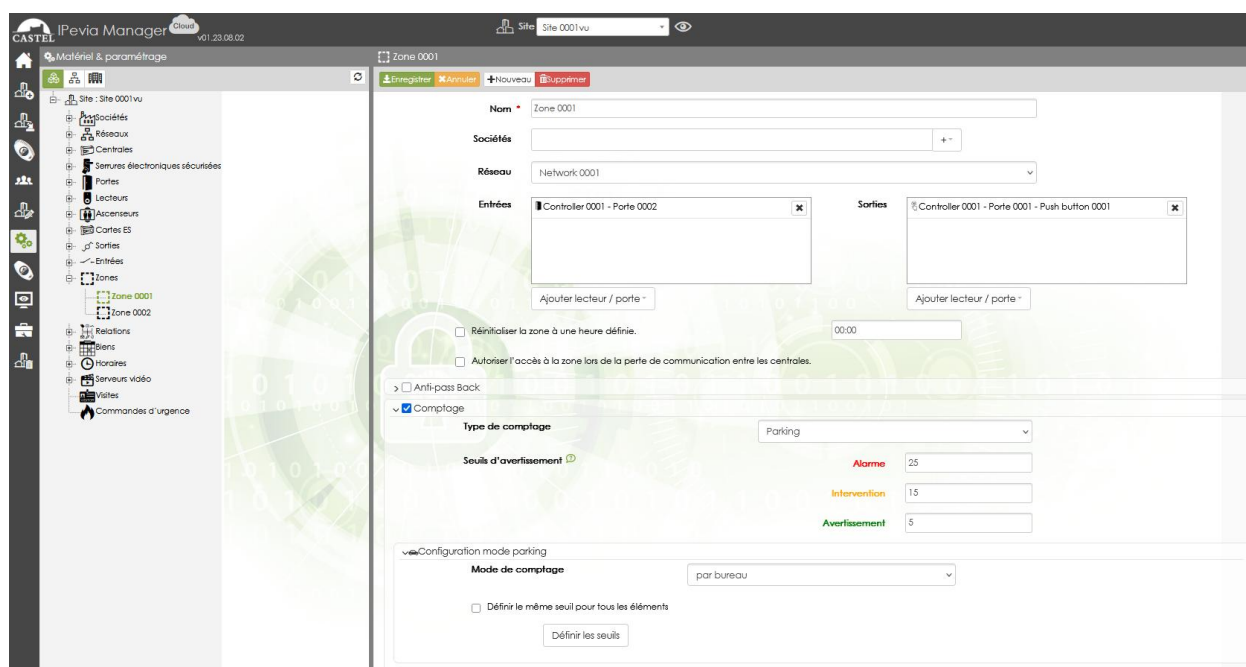
Ipévia gère des zones dans lesquelles vous pouvez activer le comptage global ou par appartement, entreprise ou groupe. L'option APB peut être ajoutée. La case « Utilisation des zones » doit être activée dans les propriétés du site (voir le chapitre 2.2). Ipévia permet de compter par identifiant (clé, empreinte digitale, plaque d'immatriculation) ou par utilisateur.

- **Avec la première option**, un utilisateur entrant dans une zone avec une plaque d'immatriculation doit sortir en utilisant le même identifiant.
- **Avec la deuxième option**, l'utilisateur peut entrer dans une zone avec une plaque d'immatriculation et sortir avec une carte, car la lecture de la plaque d'immatriculation n'aurait pas fonctionné.

Dans l'écran suivant, sélectionnez l'option souhaitée dans la liste à côté de « gérer la zone par ».



Cliquer sur le bouton “ajouter une zone ».



**Une zone est définie comme suit :**

- Un ou plusieurs lecteurs d'entrée dans la section "entrées".
- Un ou plusieurs lecteurs de sortie dans la section "sorties".
- Liste des profils d'accès gérés par la zone.
- Le personnel d'entretien ou les concierges, par exemple, ne sont pas soumis à l'APB et au comptage.
- Trois seuils programmables.
  - Les deux premiers seuils peuvent être utilisés pour contrôler des actions (activation de relais, envoi de message sur écran ou par e-mail).
  - Le troisième seuil (seuil d'alarme), bloque toute nouvelle entrée dans la zone.

## Paramètres avancés :

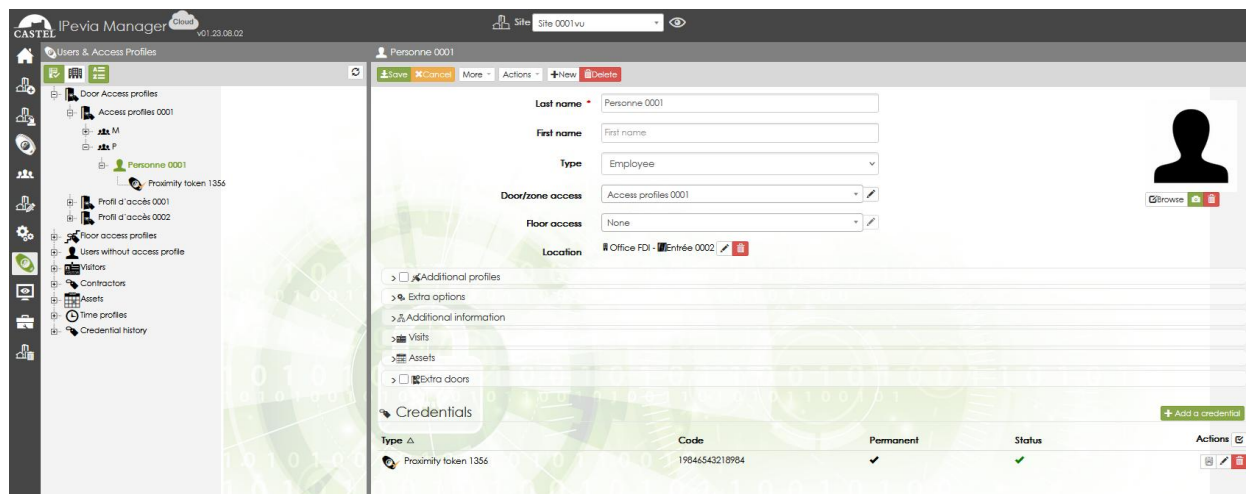
- « **Réinitialiser la zone à une heure définie** » : à une heure définie, le décompte de la zone est réinitialisé par le logiciel.
- « **Autoriser l'accès à la zone lors de la perte de communication entre les centrales** » : si la connexion avec la centrale est perdue, le contrôle d'accès autorise l'entrée dans la zone. Cette option permet d'éviter que les personnes ne restent bloquées dans la zone.

## Compter par bureau:

### 1) Création d'architecture

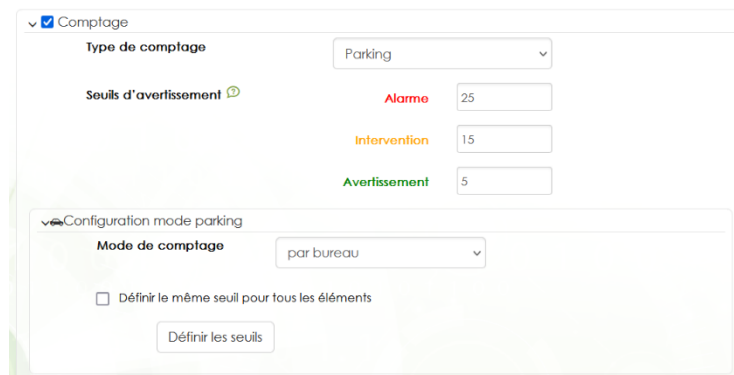
La fonction « architecture » doit avoir été activée dans les propriétés du site (voir le chapitre 2.5 pour plus d'informations).

### 2) Créer les sociétés, utilisateurs et titres dans le logiciel.



3) Sélectionnez la zone de comptage par bureau dans les paramètres de la zone.

Par défaut, le nombre de places de parking est identique pour tous les appartements, mais il est possible de les personnaliser en décochant « définir le même seuil pour tous les éléments ».



où vous pouvez entrer le seuil autorisé pour chaque appartement, entreprise, groupe de personnes, etc.

Une nouvelle fenêtre apparaît alors,

Add a threshold

Default threshold  ☒

| Name                                           | Num | Threshold                       |
|------------------------------------------------|-----|---------------------------------|
| Bâtiment 0001 - Étage 0001 - Apartment 01-0001 | ?   | <input type="text" value="25"/> |
| Bâtiment 0001 - Étage 0001 - Apartment 01-0002 | ?   | <input type="text" value="25"/> |
| Bâtiment 0001 - Étage 0001 - Apartment 01-0003 | ?   | <input type="text" value="25"/> |
| Bâtiment 0001 - Étage 0001 - Apartment 01-0004 | ?   | <input type="text" value="25"/> |
| Bâtiment 0001 - Étage 0001 - Apartment 01-0005 | ?   | <input type="text" value="25"/> |

Au préalable, les sociétés doivent avoir été saisis dans le logiciel.

### 3.13. Horaires & périodes fériées/travaux

Ipévia propose différents types de plannings :

- **Planning d'accès par badge** : un badge ne fonctionne qu'aux horaires autorisés.
- **Planning de porte, sortie ou étage** : la porte ou l'étage est librement accessible, verrouillé ou nécessite un badge pour être contrôlé selon les créneaux horaires.
- **Planning de lecteur** : selon l'heure de la journée, un badge valide suffit, ou une autre condition doit être remplie. Par exemple, un code PIN doit être entré, un contact d'alarme doit être désactivé, etc.
- **Planning de processus** : les processus utilisés dans les réflexes fonctionnent selon des créneaux horaires.
- **Planning d'interphone** : les noms affichés sur les panneaux 2Smart ne sont affichés qu'aux horaires programmés.

Un profil horaire inclut les 7 jours de la semaine plus un jour férié et un jour de travail. Cela signifie qu'une personne peut avoir différents accès selon la période en cours (normale, fériée, travail).

Dans l'exemple ci-dessous (capture du chapitre 4.11.1), en considérant que l'utilisateur utilise le profil bureau à une porte et qu'il s'agit d'un jeudi :

- Il est autorisé de 8h à 17h30 pendant la période normale.
- Il est autorisé de 8h00 à 12h30 pendant les jours fériés.
- Il n'a pas d'accès pendant les périodes de travail.

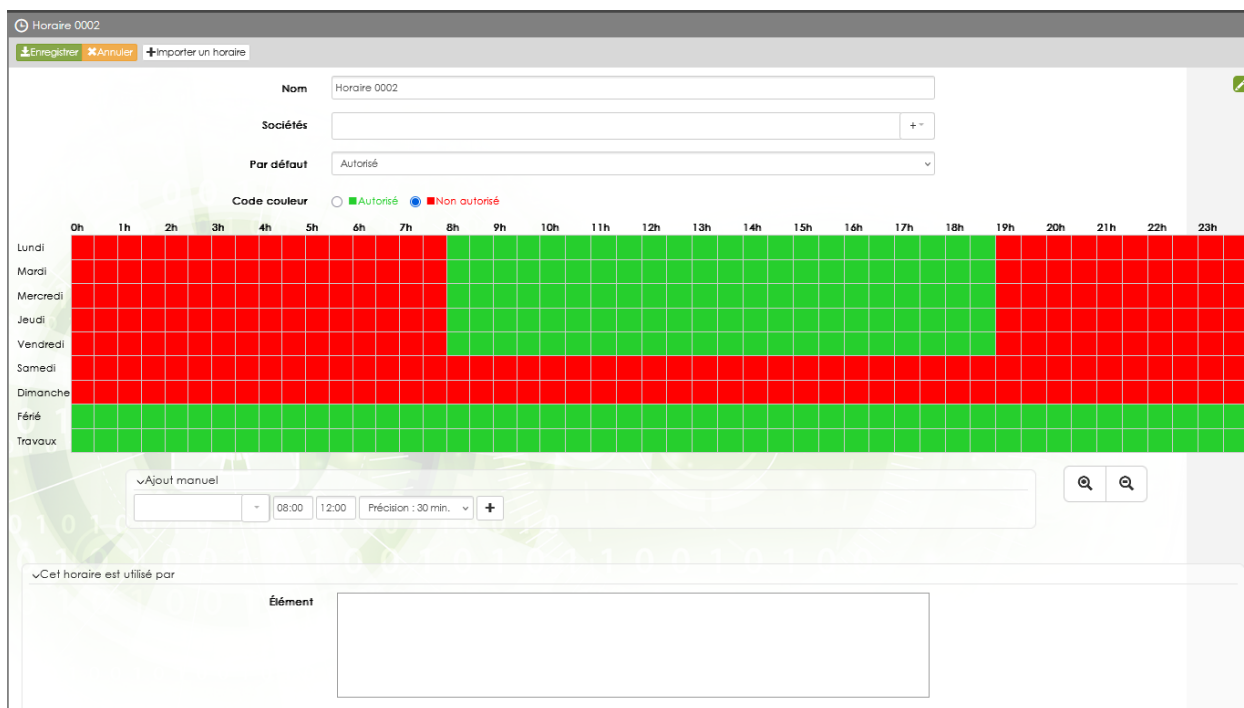
Les jours fériés et les périodes de travail sont déclarés dans le chapitre 3.13.6 et appliqués ensuite aux profils d'accès, portes, sorties, étages ou processus.

Ipévia gère jusqu'à 200 plannings (tous combinés).

## Horaires d'accès

Les plannings d'accès (ou profils horaires) sont utilisés dans les profils d'accès des portes ou des étages. Il y a deux façons de créer des profils horaires d'accès :

- Cliquez sur "matériel et paramétrages » dans le cadre gauche. Sélectionnez une porte dans l'arborescence. Cliquez sur le "+" à droite du champ "profil horaire".
- Cliquez sur "profil d'accès et badges" dans le cadre gauche et cliquez sur le "+" sous la colonne "profils horaires".



Pour le même profil d'accès, les portes ou étages peuvent utiliser différents profils horaires. Par exemple, les utilisateurs ont un accès 24/7 à une porte, de 08h00 à 20h00 à une autre et de 08h00 à 17h00 à une troisième.

Dans la vue suivante, les clés sont autorisées pendant les périodes vertes.

Note : en cliquant sur les boutons "+" ou "-", vous pouvez agrandir la zone et sélectionner des créneaux de 5 minutes.

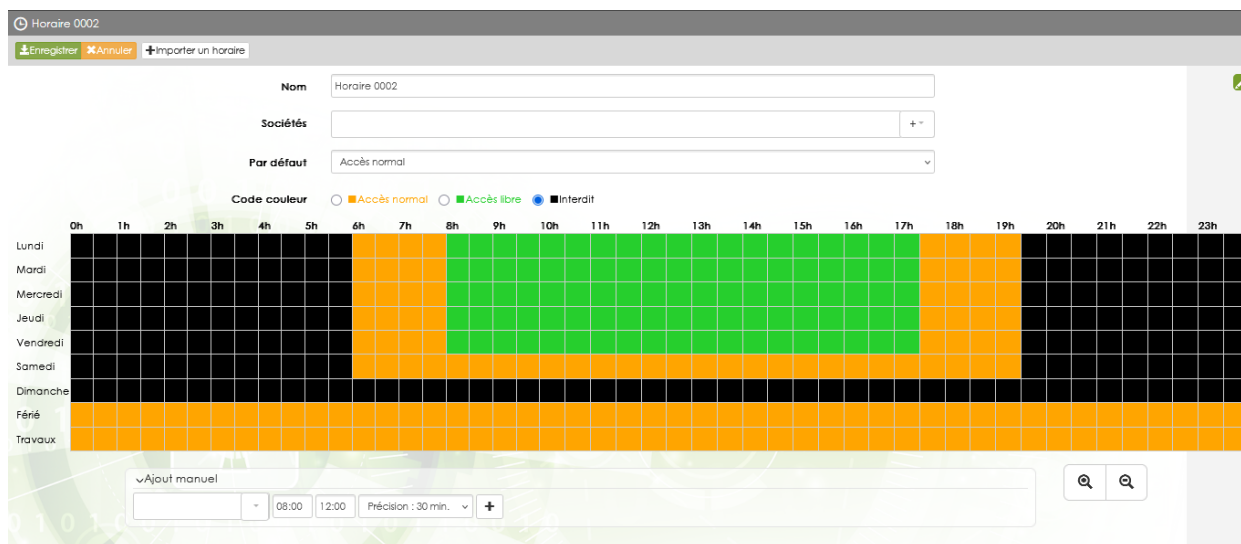
## Horaires porte ou sortie

Les horaires des « relais » ont trois états :

- Bloqué (accès libre) : la porte, la sortie ou l'étage est activé indépendamment de l'opération du badge ou du réflexe.
- Au repos (accès refusé) : même une clé valide ne peut pas ouvrir la porte ou la sortie.
- Normal (accès normal) : les portes, étages ou sorties sont activés selon l'accès ou les réflexes programmés.

Dans l'exemple ci-dessous, les portes et les étages sélectionnés dans le cadre inférieur sont :

- Interdits (relais au repos) aux horaires indiqués en noir (de 19h30 à 6h00 en semaine).
- Accès libre (relais bloqué) entre 8h00 et 17h00.
- Accès normal (accès normal), de 06h00 à 08h00 puis de 17h30 à 19h30 du lundi au vendredi. Le samedi de 06h00 à 19h30.



## Horaires lecteur/porte

Une porte peut être gérée par plusieurs lecteurs. Par exemple, une entrée de bureau peut avoir un lecteur d'entrée et un lecteur de sortie. Dans ce cas, le comportement de ces dispositifs peut être différencié avec une clé + code pour entrer, mais juste une clé pour sortir.

Dans l'exemple suivant, les lecteurs d'entrée du bâtiment fonctionnent comme suit :

- Aucun accès possible la nuit, de 21h00 à 7h30, du lundi au samedi inclus.
- Accès sécurisé (clé + code PIN)
  - Du lundi au vendredi, de 7h30 à 9h00 et de 18h00 à 21h00.
  - Le samedi, de 7h30 à 21h00.
  - Le dimanche, toute la journée.
  - Tous les jours fériés.
- Accès par clé du lundi au vendredi, de 9h00 à...

Time profiles 0002

Name

Time profiles 0002

Default

Normal access

Colour code:

☐ Normal access
 ☒ Secured mode
 ☐ Forbidden

|             |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|-------------|----|----|----|----|----|----|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|             | 0h | 1h | 2h | 3h | 4h | 5h | 6h | 7h | 8h | 9h | 10h | 11h | 12h | 13h | 14h | 15h | 16h | 17h | 18h | 19h | 20h | 21h | 22h | 23h |
| Monday      |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Tuesday     |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Wednesday   |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Thursday    |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Friday      |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Saturday    |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Sunday      |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Holiday     |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Maintenance |    |    |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |

Add manually

08:00

12:00

Precision : 30 min

+

This time profile is used by

Element

Controller 0001 - Porte 0001 - Reader 0001

Controller 0001 - Porte 0002 - Lecteur 0002

Controller 0002 - Door 0001 - Reader 0001

Save

Cancel

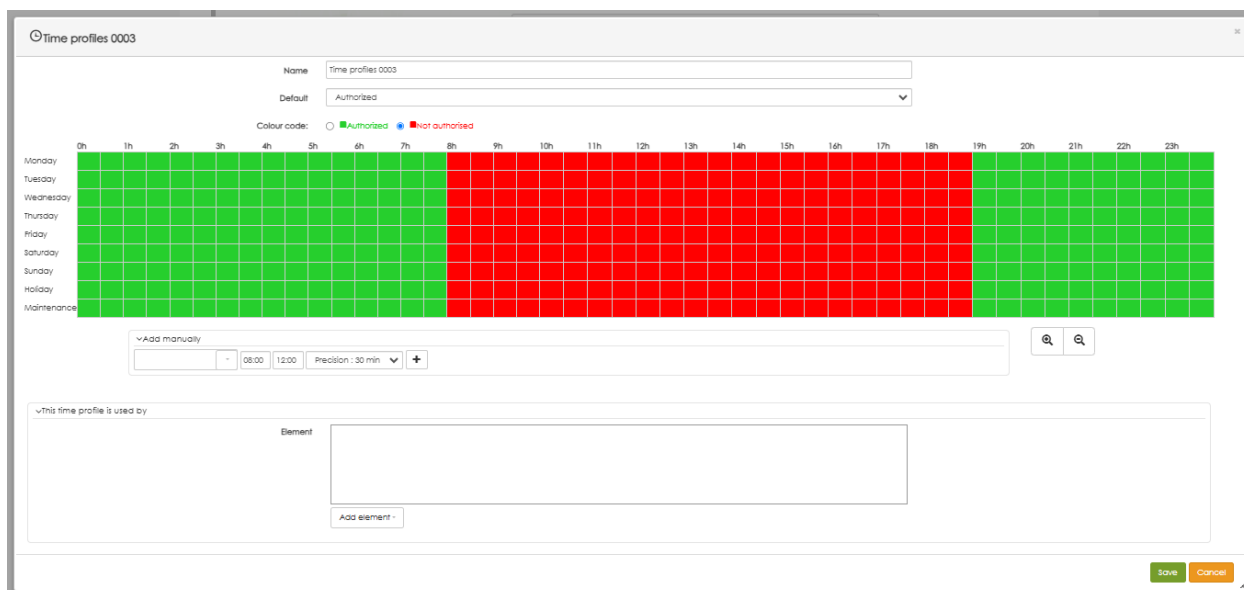
## Horaires condition/processus

IPEvia gère les relations. Il s'agit de la somme de 1 ou plusieurs conditions qui, lorsqu'elles sont "vraies", déclenchent un ou plusieurs processus.

- Un exemple de condition est une porte forcée.
- Un processus pourrait être l'envoi d'un e-mail ou l'activation d'un relais.

IPEvia vous permet de gérer des horaires pour ces processus. Par exemple, pour un événement de "porte forcée", les mêmes personnes peuvent ne pas être averties pendant la journée ou la nuit.

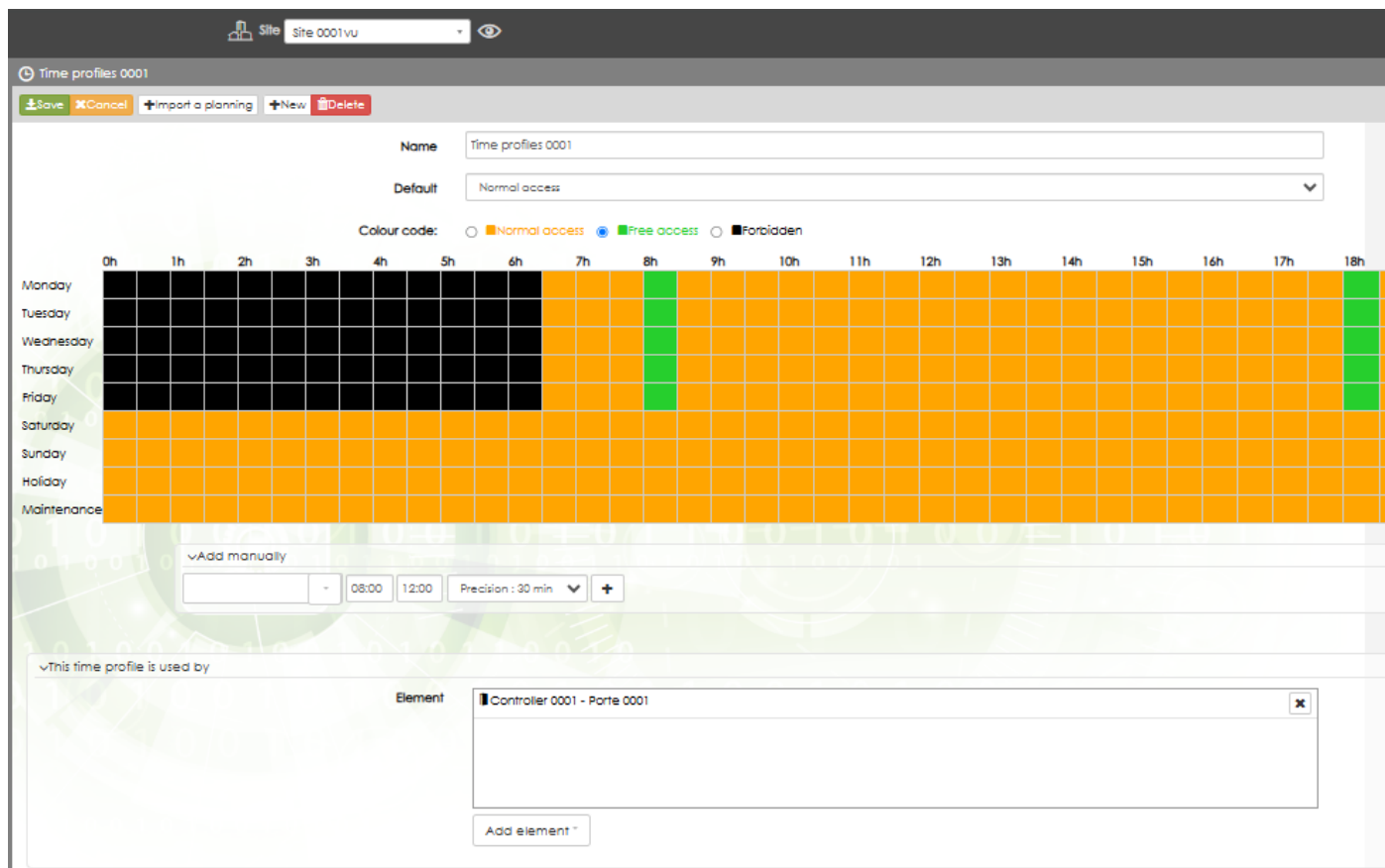
Pour programmer une relation, sélectionnez-le dans le menu "Matériel et paramétrages". Dans le champ "profils horaires", sélectionnez un profil déjà défini. En cliquant sur le bouton "+" à droite, vous pouvez créer un nouveau profil horaire. Dans l'exemple suivant, un processus ne fonctionnera que la nuit.



## Copier et coller des horaires

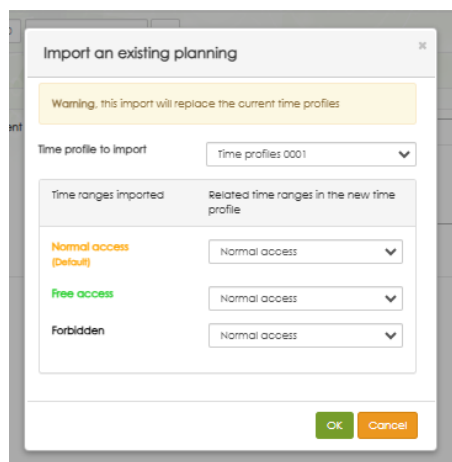
IPEvia Manager contrôle plusieurs profils horaires. Cependant, il peut être utile d'utiliser un planning pour les portes et d'utiliser ce même créneau pour les processus ou les clés.

Pour cela, il est nécessaire de créer un nouveau planning et d'importer le créneau dans le profil d'origine. Lorsque le nouveau planning est créé, cliquez sur le bouton "importer un planning".



The screenshot shows the 'Time profiles 0001' configuration window. At the top, there's a 'Site' dropdown set to 'Site 0001 vu'. Below the title bar, there are buttons: 'Save', 'Cancel', 'Import a planning', 'New', and 'Delete'. The 'Name' field is 'Time profiles 0001' and the 'Default' dropdown is set to 'Normal access'. The 'Colour code' section has three radio buttons: 'Normal access' (selected, orange), 'Free access' (blue), and 'Forbidden' (black). The main area is a grid showing the week from Monday to Sunday, with columns for each hour from 0h to 18h. The grid is mostly orange, indicating 'Normal access', with some black cells indicating 'Forbidden' access. Below the grid, there's an 'Add manually' section with a time range selector (08:00 to 12:00) and a 'Precision: 30 min' dropdown. At the bottom, there's a section 'This time profile is used by' with an 'Element' dropdown set to 'Controller 0001 - Porte 0001' and an 'Add element' button.

The following window appears :



Sélectionnez le planning à dupliquer. Pour chaque option, indiquez le nouveau comportement.

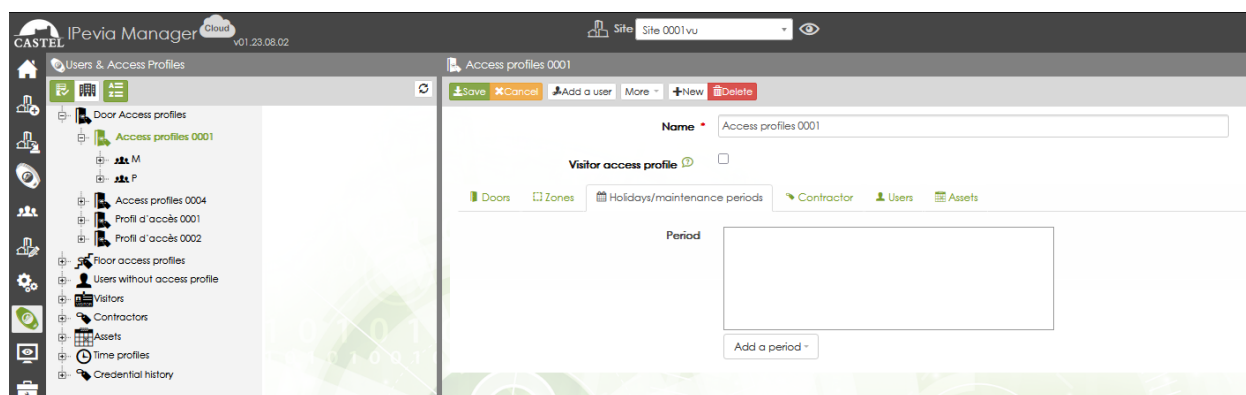
Note : certains plannings peuvent avoir deux statuts différents (autorisé ou refusé) pour une clé ou trois états différents pour un lecteur (refusé, accès avec clé ou clé + code). Cliquez sur « OK » pour confirmer le changement.

## Périodes fériées

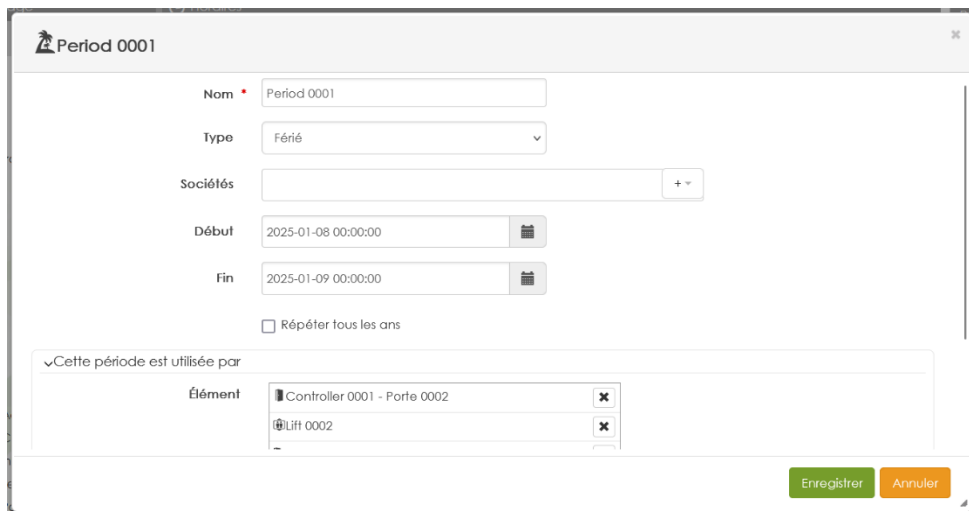
Les jours fériés ou les périodes de travail modifient automatiquement le comportement des portes, des étages, des profils d'accès, etc., en fonction des dates prédéfinies.

La modification peut être plus ou moins sécurisée. Par exemple, un étage est libre le jeudi matin de 8h à 12h mais est sécurisé lorsque le jeudi est un jour férié. Inversement, la porte est libre les dimanches et jours fériés.

Une façon de créer une période de jour férié consiste à cliquer sur le bouton du profil d'accès dans le panneau de gauche. Ensuite, sélectionnez le profil d'accès et l'onglet "périodes de vacances/maintenance". Sélectionnez le bouton "ajouter une période".



L'exemple suivant montre une période de jour férié commençant le 22 décembre à 17h et se terminant le vendredi 2 janvier à 7h. Cette période de vacances est suivie par les portes, les profils d'accès, les étages, les sorties ou les relations.



Une case à cocher « Répéter chaque année » facilite la gestion des dates fixes. Important : si un jour est à la fois un jour férié et un jour de travail, c'est le comportement « travail » qui est prioritaire.

### 3.14. Serveurs vidéo

Ipevia Manager permet d'intégrer la vidéosurveillance via RTSP (real time streaming protocol). Tous les NVR (enregistreurs vidéo) prenant en charge ce protocole peuvent être intégrés à Ipevia, à condition de connaître les liens en direct RTSP et de lecture correspondante.

#### General

En intégrant la vidéosurveillance au contrôle d'accès, un lien est créé entre une caméra et une porte, par exemple.

Ainsi, si une porte est forcée, l'opérateur logiciel visualise l'événement à l'écran et clique sur le bouton vidéo pour voir l'enregistrement de l'effraction.

- Comment cela fonctionne-t-il ?

Dans le logiciel, une caméra est associée à une porte, un lecteur, une entrée ou une sortie, etc. Ainsi, lorsqu'un événement concerne cet élément, une icône représentant une caméra est disponible sur la ligne de l'événement.

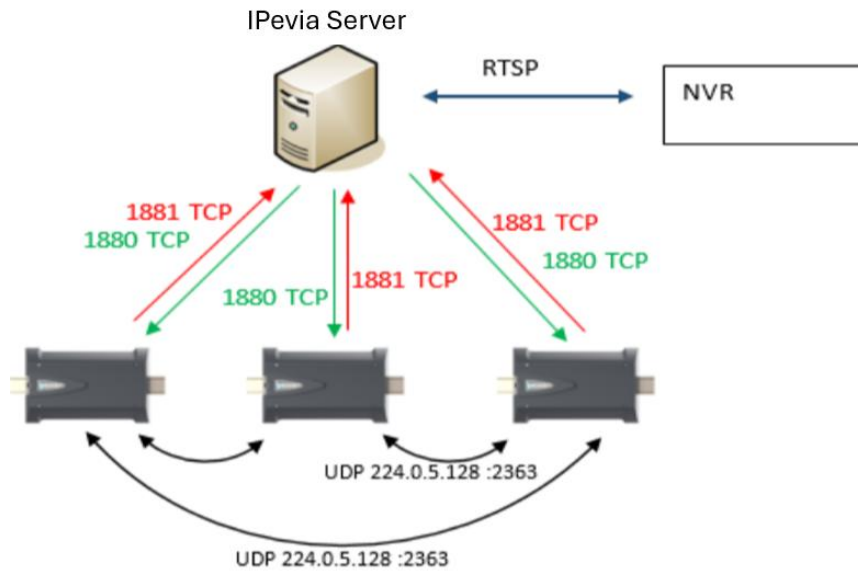
Cette intégration fonctionne à la fois en direct et en rediffusion.

Pour accéder aux serveurs vidéo de la vidéosurveillance, vous devez activer cette fonction dans la configuration du site. Accédez à l'assistant de configuration du site et sélectionnez l'onglet « fonction ». Pour plus d'informations à ce sujet, consultez le chapitre « 2.2 fonctions ».

#### Synoptique

La centrale n'est pas directement impliquée dans cette intégration ; elle enregistre les événements et les transmet au serveur. C'est ce serveur qui maintient le lien entre les caméras et les entrées, portes et lecteurs.

Donc c'est le serveur Ipévia qui communique avec les NVRs.



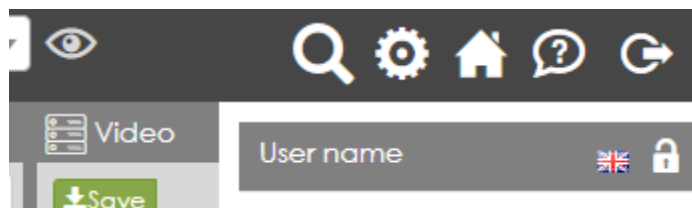
## Choisir un logiciel de lecture RTSP

IPeVia Manager contrôle le lien avec les serveurs vidéo. Cependant, il ne diffuse pas directement le flux RTSP.

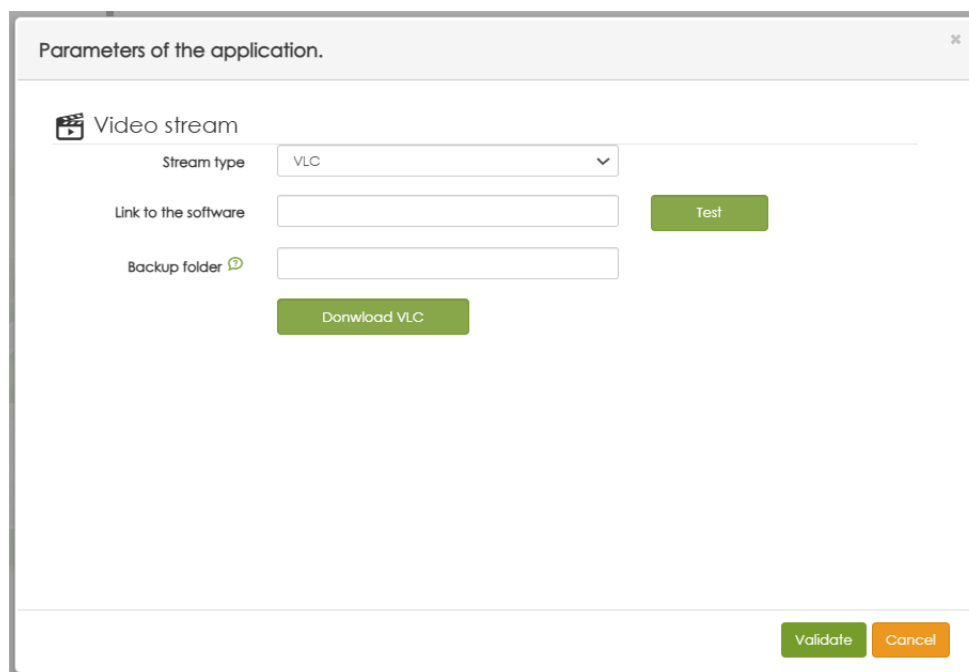
Vous devez sélectionner un lecteur externe (VLC, par exemple).

Sélectionnez le bouton de paramètres de l'application en haut à droite.

Si celui-ci n'apparaît pas, cela signifie que la fonction vidéosurveillance n'a pas été sélectionnée dans la configuration du site. Voir le chapitre 2.2 pour plus d'informations.



Ensuite, la fenêtre suivante apparaît:



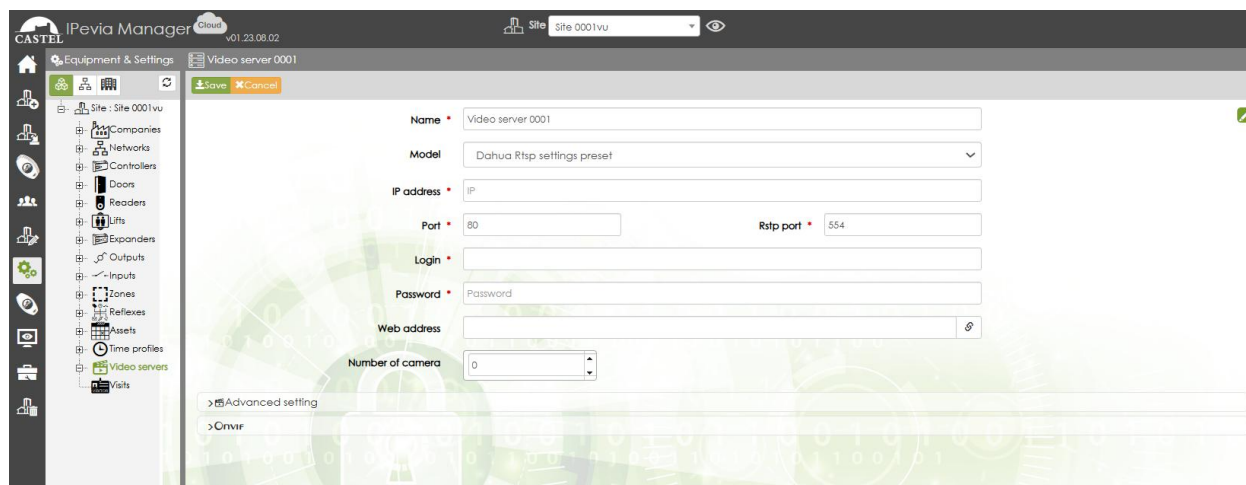
Saisissez le chemin de l'application choisie.

Remarque : VLC est un programme gratuit qui peut lire les flux RTSP. Il peut être sélectionné pour lire les vidéos des NVR.

Saisissez le chemin vers le lecteur ainsi que le répertoire où les vidéos seront enregistrées.

## Paramètres

Notez qu'IPévia Manager peut détecter les appareils ONVIF sur le réseau (un protocole standard pour la communication entre dispositifs de surveillance IP). Le logiciel détectera si les NVR utilisés sur site sont ONVIF pour leur communication avec des équipements tiers, et pas uniquement pour l'intégration de caméras.

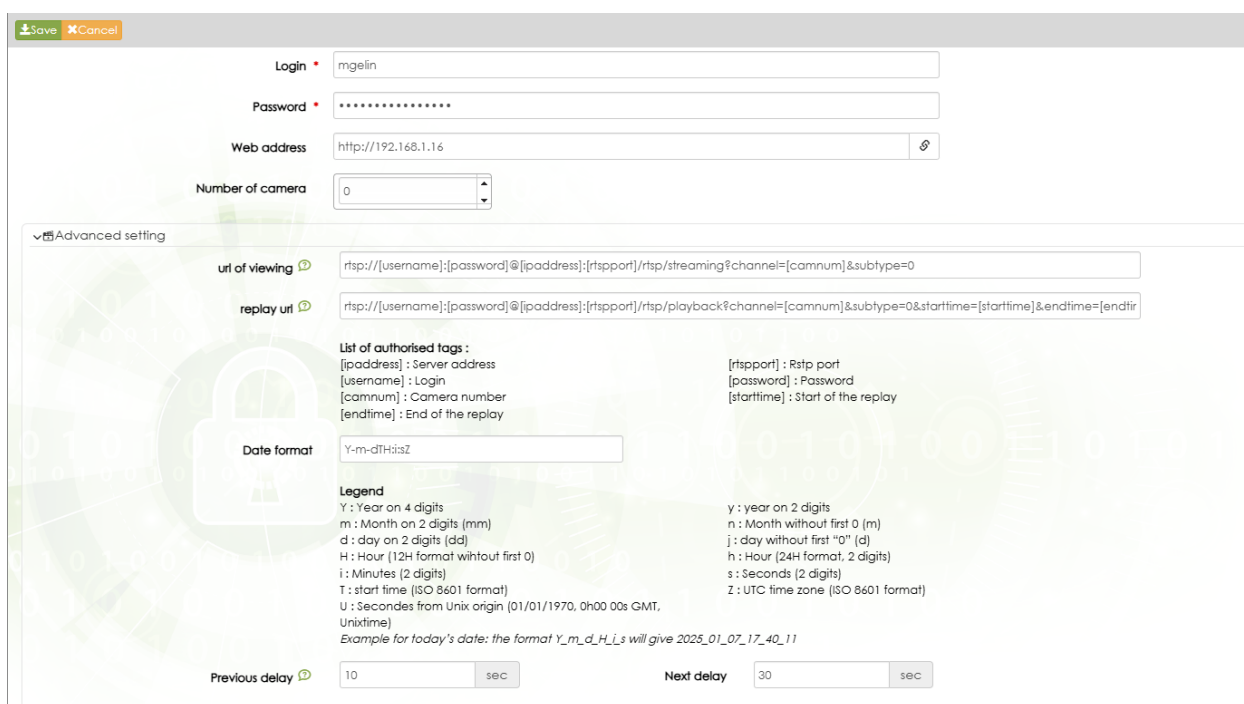


Accédez au menu « matériel et paramétrages » et choisissez « Serveurs vidéo » dans l'arborescence à gauche. Cliquez sur le bouton « Ajouter un serveur vidéo » en haut de la page.

- Saisissez un nom pour le serveur, son adresse IP et les ports de communication RTSP/web.
- Choisissez le modèle approprié dans la liste.
- Entrez le login et le mot de passe, puis cliquez sur Enregistrer.
- Notez que le protocole RTSP est ouvert et partagé par de nombreuses marques d'enregistreurs. Cependant, chaque marque utilise sa propre syntaxe. Exemple de lien RTSP pour le live Urmet :  
`rtsp://[username]:[password]@[ipaddress]:[rtspport]/ch[camnum]/0`. IPévia propose trois pré-réglages : Urmet, Dahua et HIK. Pour intégrer une autre marque, les informations appropriées doivent être saisies manuellement comme indiqué ci-dessous.

### Configuration avancée :

Si le NVR n'est pas l'un des modèles pour lesquels un pré-réglage est disponible, saisissez les chaînes RTSP pour le live et la lecture, puis spécifiez le format date/heure utilisé par le NVR. Deux champs permettent d'entrer le nombre de secondes avant l'événement et le nombre de secondes après l'événement.



Notez que ces deux temps (avant et après l'événement) concernent uniquement l'aperçu dans Ipevia Manager. Il est possible de visualiser plus de caméras ou une période plus large sur le NVR.

Comme montré ci-dessous, pour chaque caméra, sélectionnez les portes, lecteurs, boutons-poussoirs, entrées ou sorties impliqués. Dans la vue de supervision, pour chaque événement concernant ces éléments (entrée, lecteur, etc.), un bouton affichant une caméra sera cliquable.



Notez qu'une caméra peut être liée à plusieurs éléments, et un élément tel qu'une porte peut être lié à plusieurs caméras. Par exemple, une caméra surveille à la fois l'entrée et la sortie d'un parking (deux lecteurs), ou inversement, deux caméras surveillent la même porte d'entrée des visiteurs mais sous deux angles différents.

## 4. Intrusion

Deux concepts d'intrusion sont pris en charge par IPévia

- « Non connectée » : intrusion avec des contacts secs
- « Connectée » avec une centrale Elkron/Médéa

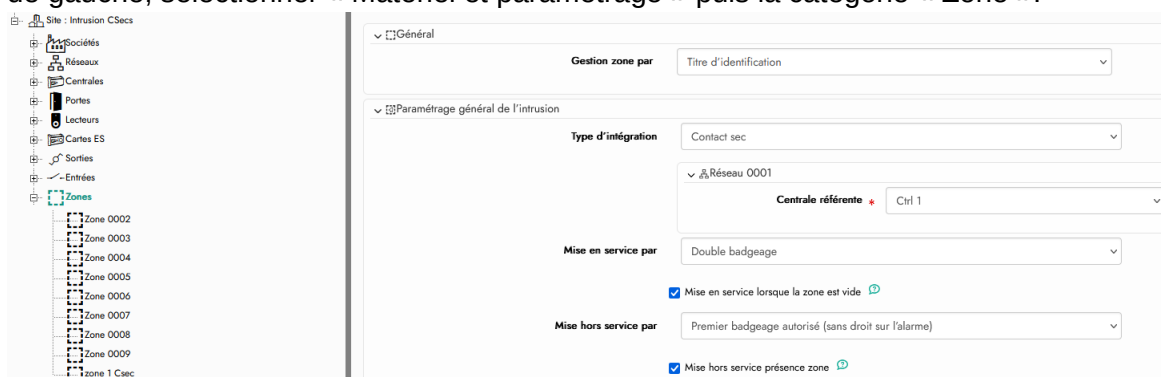
L'intrusion connectée nécessite une carte d'activation, alors que l'intrusion par contact sec est incluse parmi toutes les fonctionnalités de base d'IPévia. Par défaut, lorsque « intrusion » est coché dans les fonctionnalités de site, l'intrusion par contacts secs est sélectionnée par défaut.

Il n'est pas possible de combiner ces deux concepts d'intrusion différents pour une même installation.

### 4.1. Intrusions par contacts secs

#### Paramètres de zones

Les paramètres d'intrusion sont accessibles depuis les paramètres de zones. Dans le bandeau de gauche, sélectionner « Matériel et paramétrage » puis la catégorie « Zone ».



Sélectionnez « contact sec » dans la liste du type d'intégration.

Mise en service par :

- **Double/triple badgeage** : L'armement de la zone n'est possible que par les personnes ayant le droit d'armer/désarmer l'intrusion dans cette zone.
- **Mise en service lorsque la zone est vide** : Ne s'applique qu'aux zones qui gèrent également le comptage.

Mise hors service par :

- **Premier badgeage autorisé (sans droit sur l'alarme)** : le désarmement de la zone est possible par toute personne ayant accès à la zone.
- **Premier badgeage autorisé** : L'alarme n'est désactivée que si l'utilisateur en a le droit.
- **Double / Triple badgeage** : le désarmement de la zone n'est possible que par des personnes ayant le droit de s'armer ou de désarmer en cas d'intrusion dans cette zone.
- **Mise hors service présence zone** : si cette case est cochée, l'alarme sera désarmée dès que la zone comptera au moins une personne.

## Paramétrage de l'intrusion par zone

Pour appliquer l'intrusion à une zone, cochez la case « intrusion (contact sec) ». Ensuite, vous pouvez accéder à de nombreux champs configurables.

▼ ☒ Intrusion (contact sec)

Sortie Mise En Service

Aucun ▼

Sortie Mise Hors Service

Aucun ▼

Report zone en alarme

Aucun ▼

Report Statut de la zone

Aucun ▼

Horaire

Aucun ▼   

☒ Activer la Mise En Service suivant horaire

☒ Activer la Mise Hors Service suivant horaire

Options

☐ Mise en service via une entrée 

Aucun ▼

Pour chaque zone, vous devez définir :

- 2 sorties pour mettre hors service/en service la zone.
- 2 entrées pour connaître l'état d'intrusion de la zone (mise en service ou hors service)
- 1 entrée en option pour contrôler la mise en service de l'intrusion via une commande externe (voir chapitre 5.3 Commandes manuelles).

Vous pouvez appliquer un profil temporel à la mise en service/désactivation de l'alarme.

## 4.2. Elkron/Médéa intrusion

### Prérequis

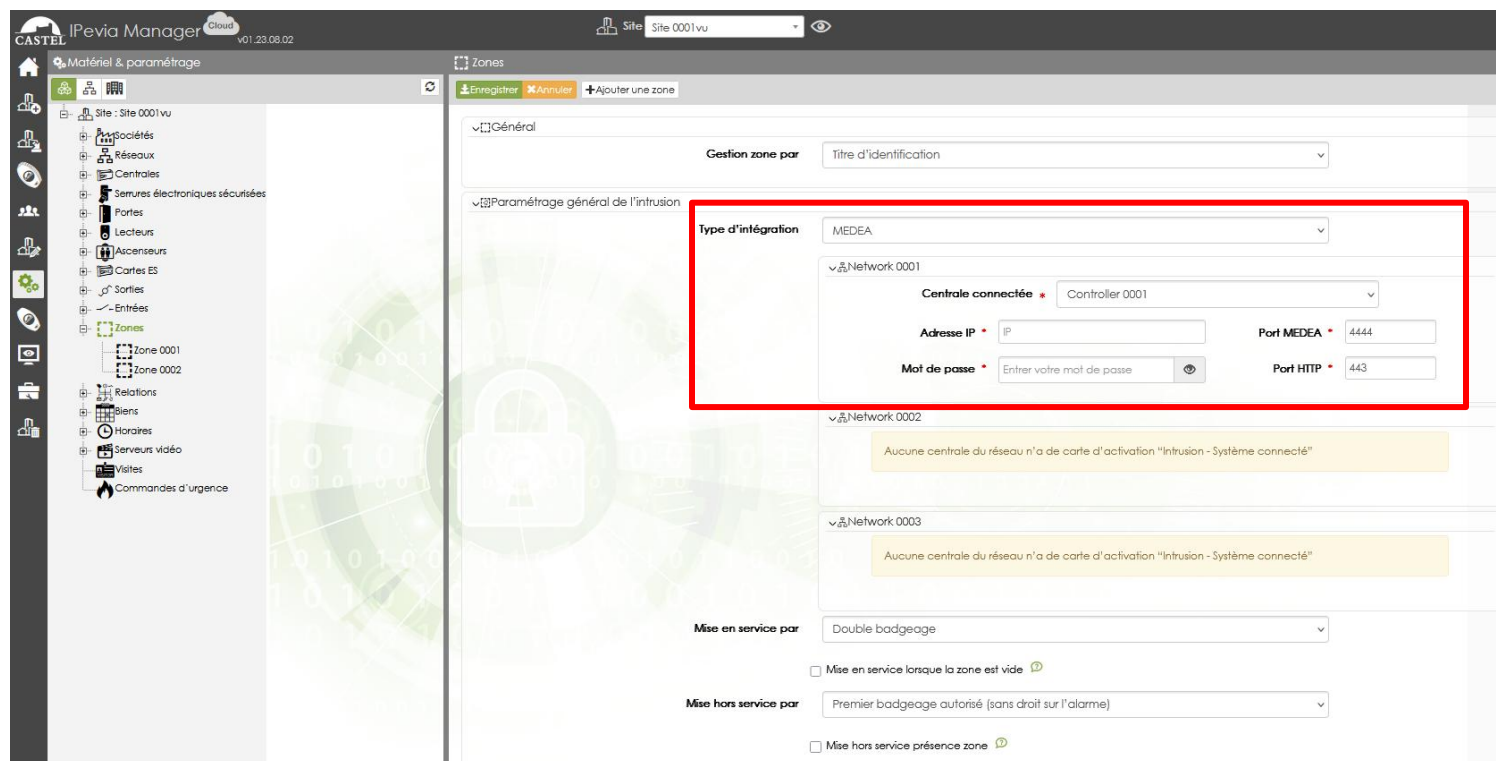
Pour paramétrer la fonctionnalité intrusion en lien avec Elkron/médéa, veuillez au préalable à cocher cette fonction dans l'onglet fonction du wizard de création de site (voir chapitre 2.2).

Vérifier que votre installation suit les prérequis suivants :

- **Logiciel de contrôle d'accès** de version >1.23.06
- **Les centrales V2** ayant un numéro de série x4Cx2DExxxxxyyyy) en version >=**fV3230**.
- **Une carte d'activation** de la fonctionnalité intrusion, référence xx-050-108. A activer en sélectionnant une centrale dans l'onglet "equipments and settings", puis sélectionner le bouton activer un module" en haut de page.
- **Les lecteurs multi technologie** de version >=3071

## Paramétrage général de l'intrusion par zone

La gestion de l'intrusion est définie par secteurs dans la centrale Médéa. Elle est également associée à des zones dans le logiciel de contrôle d'accès. Afin de gérer les paramètres principaux de l'intrusion, sélectionnez "equipments and settings" dans le badeau de gauche puis



cliquez sur la ligne "zone".

Sous l'onglet Paramétrage général de l'intrusion, sélectionner la centrale IPévia connectée au système Médéa. S'il y a plusieurs centrales sur ce site/ce réseau, alors plusieurs appareils vont apparaître dans cette liste. Renseigner l'adresse IP ainsi que le mot de passe de la centrale d'intrusion.

Dans les derniers champs, précisez les modes de mises en service/hors service des zones :

### Mise en service par:

- Double/triple badgeage : armement de la zone possible uniquement par les personnes ayant le droit d'armer/désarmer l'intrusion sur cette zone.
- Mise en service lorsque la zone est vide : ne s'applique uniquement aux zones gérant aussi le comptage

### Mise hors service par:

- **Premier badgeage autorisé** : désarmement de la zone possible par toute personne ayant accès à la zone
- **Double / Triple badgeages** : désarmement de la zone possible uniquement par les personnes ayant le droit d'armer/désarmer l'intrusion sur cette zone

- **Mise hors service « présence zone »** : si cette case est cochée, l'alarme sera désarmée dès que la zone compte au moins une personne.

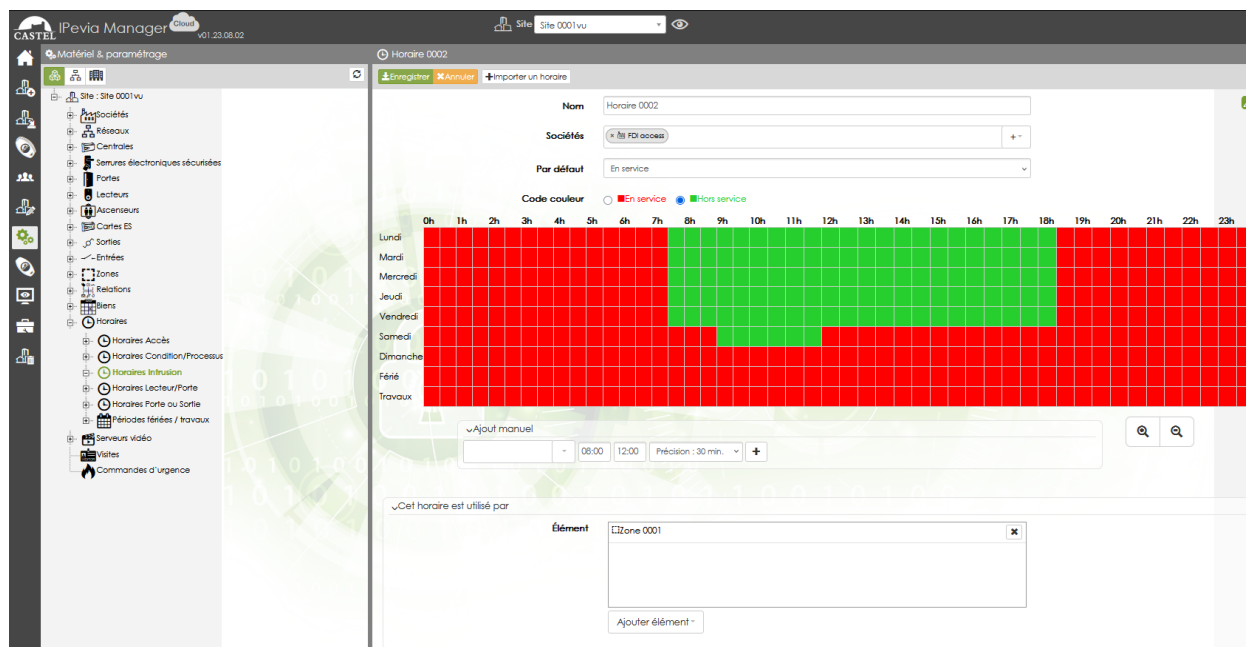
## 4.3. Paramètres communs de l'intrusion

Même si l'intrusion connectée et non connectée fonctionnent différemment, de nombreux paramètres en sont communs.

### Intrusion selon horaire

Depuis le logiciel IPeVIA manager, il est possible de mettre en service/hors service une zone selon des horaires spécifiés.

Dans le menu "Equipment and settings" sous la rubrique "horaires" sélectionner « horaires intrusion ». Cliquez sur le bouton « ajouter un horaire intrusion » en haut de la page si aucun n'a déjà été créé.



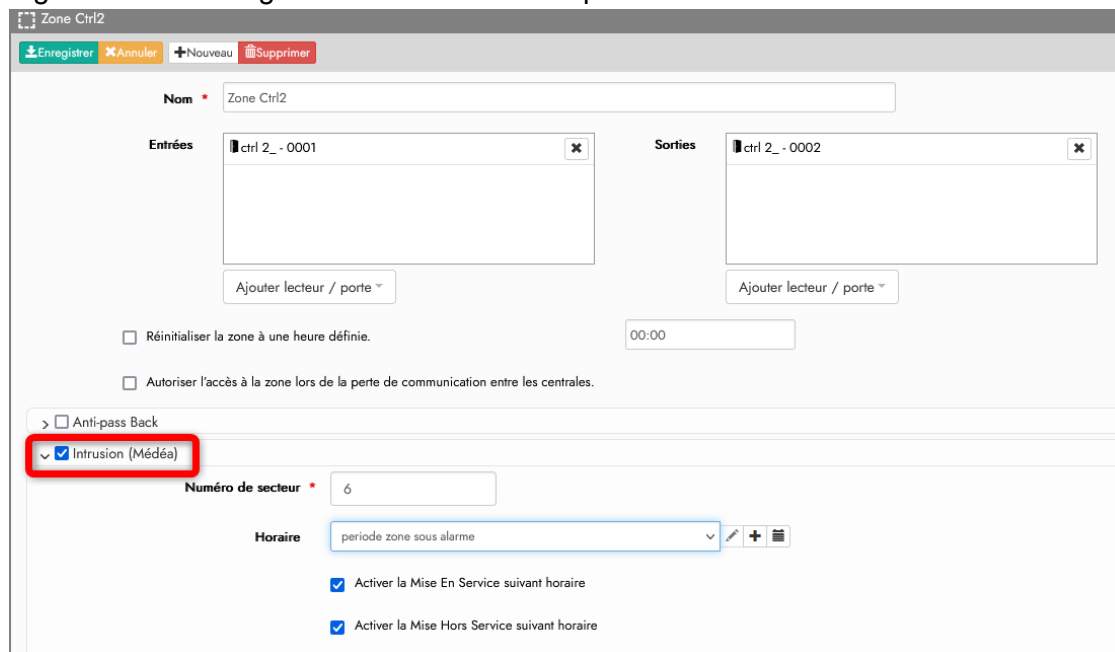
Sélectionner « en service » ou « hors service » afin d'armer/désarmer l'alarme sur des créneaux horaires.

Dans l'exemple du dessus, l'intrusion sera désarmée de 7h30 à 18h du lundi au vendredi. Le samedi elle sera uniquement armée de 8h30 à 11h30.

Une fois l'horaire d'intrusion établi, sélectionner la zone à laquelle il s'applique sous l'onglet « cet horaire est utilisé par ». Un horaire d'intrusion peut être appliqué à plusieurs zones.

## Intrusion pour chaque zone

Pour chaque zone, un onglet supplémentaire “Intrusion médéa” est accessible. Cochez la case à gauche de cet onglet afin d’accéder à ses paramètres.



The screenshot shows the configuration page for 'Zone Ctrl2'. At the top, there are buttons: 'Enregistrer' (green), 'Annuler' (orange), 'Nouveau' (blue), and 'Supprimer' (red). Below these, the 'Nom' field is set to 'Zone Ctrl2'. There are two main sections: 'Entrées' and 'Sorties'. The 'Entrées' section has a list with 'ctrl 2\_ - 0001' and an 'Ajouter lecteur / porte' button. The 'Sorties' section has a list with 'ctrl 2\_ - 0002' and an 'Ajouter lecteur / porte' button. Below these sections, there are two checkboxes: 'Réinitialiser la zone à une heure définie.' (with a time field set to '00:00') and 'Autoriser l'accès à la zone lors de la perte de communication entre les centrales.' Both are unchecked. At the bottom, there is a section for 'Anti-pass Back' with a dropdown menu. The 'Intrusion (Médéa)' option is selected and highlighted with a red box. Below this, the 'Numéro de secteur' is set to '6'. The 'Horaire' section has a dropdown menu set to 'periode zone sous alarme' and two checkboxes: 'Activer la Mise En Service suivant horaire' and 'Activer la Mise Hors Service suivant horaire', both of which are checked.

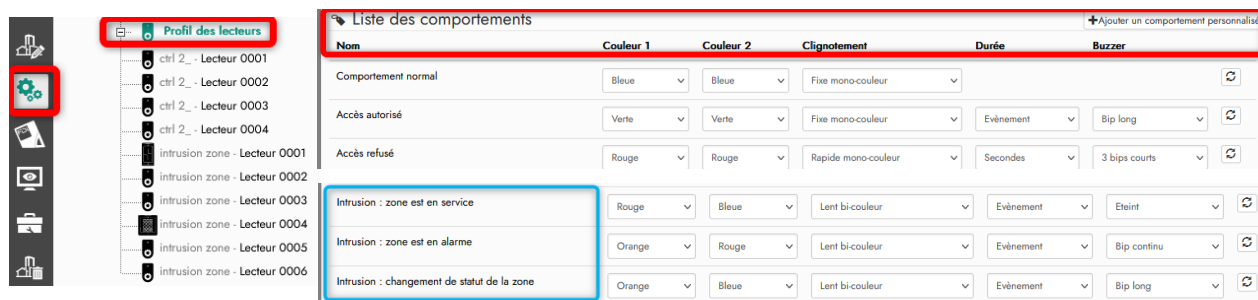
**Numéro de secteur :** Ipevia gère des zones auxquelles sont associées des portes ou des lecteurs. Dans l’interface de Médéa cette notion de zone est appelée « secteurs ». Ces secteurs peuvent regrouper un ou plusieurs capteurs. A noter qu’une centrale Médéa gère jusqu’à 16 secteurs. La définition des secteurs est effectuée sur le logiciel de paramétrage de la centrale d’intrusion Elcron/Médéa.

Dans le réglage d’une zone sur Ipevia, associez la zone au secteur correspondant. Ainsi, si un ou plusieurs lecteurs sont renseignés pour cette zone, leur actionnement peut piloter l’armement ou le désarmement de l’intrusion.

**Activer la mise en service/hors service suivant horaire :** si ces paramètres sont cochés, alors des horaires spécifiques armeront/désarmeront l’intrusion de cette zone. Il est possible d’appliquer des périodes déjà définies ou d’en créer de nouvelles en cliquant sur le « + » à droite du champ.

## Profil de lecteurs pour l'intrusion

Voir le chapitre 3.6 (lecteurs/profils>lecteurs) pour plus d'information sur les profils de lecteurs.



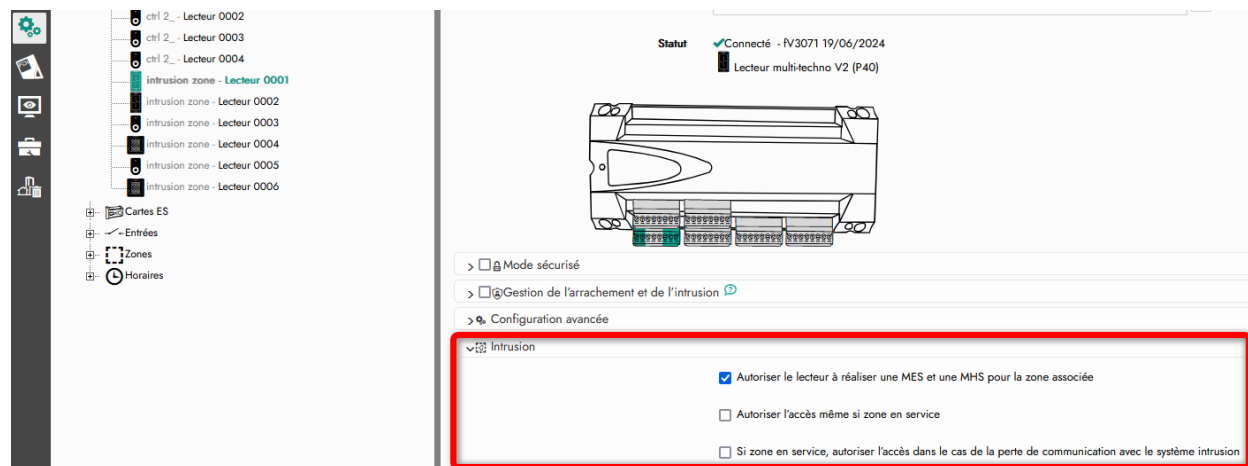
Sélectionnez puis créez un profil de lecteur. Appliquez-le aux lecteurs correspondants.

Dans ses paramètres, vous pouvez définir le comportement des leds du lecteur lorsque :

- **« Intrusion : zone est en service »** : comportement des leds lorsque l'intrusion est armée.
- **« Intrusion : zone est en alarme »** : comportement des leds lorsque l'intrusion est désarmée.
- **« Intrusion : changement de statut de la zone »** : comportement des leds lorsque l'intrusion d'une zone passe du statut armé à désarmé ou inversement.

## Lecteurs pour l'intrusion

Les précédents paramétrages ont ajouté des lignes sous la rubrique « lecteurs » dans le menu « Equipment and settings ». Pour configurer la gestion de l'intrusion par un lecteur, choisir un appareil ayant le préfixe « intrusion zone ».



Si un lecteur devant être associé à de l'intrusion ne dispose pas du préfixe « intrusion zone » alors cela signifie qu'il n'a pas été défini en lecteur d'entrée. Pour cela, reprenez le « paramétrage de l'intrusion pour chaque zone ».

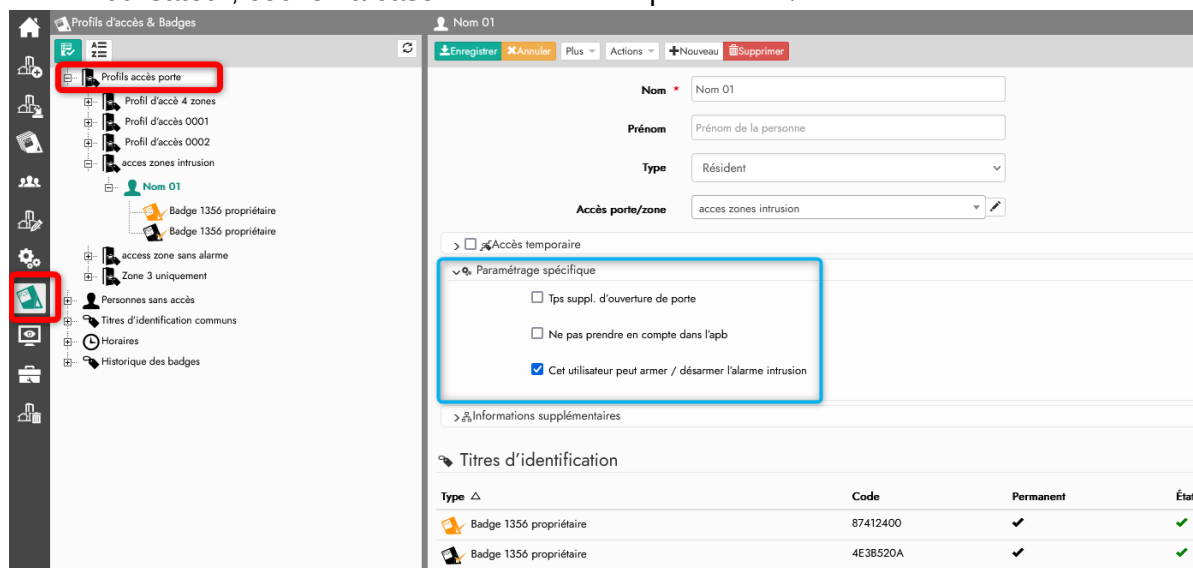
Une fois le bon lecteur sélectionné, cliquer sur l'onglet « intrusion » afin d'en déployer ses paramètres.

- **Autoriser le lecteur à réaliser une MES et une MHS pour la zone associée** : le lecteur peut être utilisé pour mettre en/hors service l'intrusion grâce à un badge autorisé
- **Autoriser l'accès même sur zone en service** : l'accès peut être autorisé même si l'intrusion est armée.
- **Si zone en service, autoriser l'accès dans le cas de la perte de communication avec le système d'intrusion** : lorsque la centrale IPeVia perd sa communication avec la centrale Médéa, autoriser malgré tout l'ouverture de la porte aux badges valides.

## Utilisateurs pilotant l'intrusion (par profil d'accès)

Pour armer/désarmer l'intrusion d'une zone, l'utilisateur devra disposer de :

- Droits d'accès aux zones concernées dans son profil d'accès. Voir chapitre 4 pour paramétrer un profil d'accès
- D'un droit spécifique validé : sous l'onglet « paramétrages spécifiques » de sa fiche utilisateur, cocher la case « cet utilisateur peut armer/désarmer l'alarme intrusion »



The screenshot shows the 'Profil d'accès & Badges' interface for user 'Nom 01'. The left sidebar has a red box around the 'Profil accès porte' icon. The main area has a blue box around the 'Paramétrage spécifique' section, which contains the checkbox 'Cet utilisateur peut armer / désarmer l'alarme intrusion' checked. Below this is a table of identification titles.

| Type                    | Code     | Permanent | État |
|-------------------------|----------|-----------|------|
| Badge 1356 propriétaire | 87412400 | ✓         | ✓    |
| Badge 1356 propriétaire | 4E38520A | ✓         | ✓    |

Il est également possible de permettre à un utilisateur d'armer/désarmer l'intrusion, sans pour autant concéder ce droit à tout son profil d'accès, et donc d'autres utilisateurs du site.

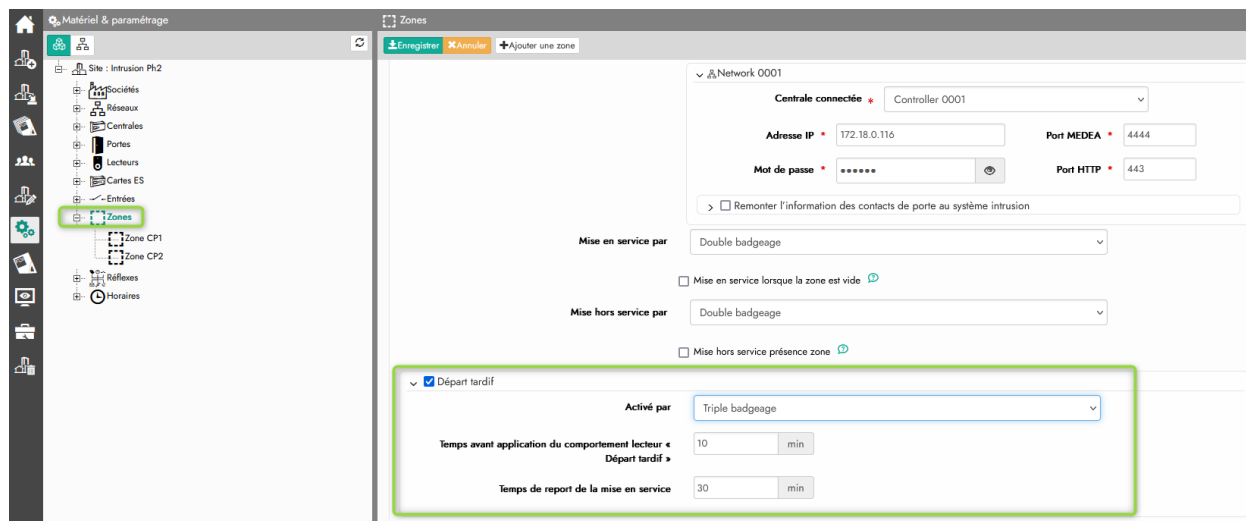
Pour cela accédez à la fiche d'un utilisateur dans le menu « Profil d'accès & badges ». Sélectionnez une personne dans l'arborescence à gauche.

The screenshot displays the Ipevia Manager web application. On the left is a sidebar menu with icons for various functions like 'Profil d'accès & Badges', 'Manager', 'Access profiles', etc. The main area is titled 'Manager' and contains a form for configuring a user. The form includes fields for 'Nom' (Name), 'Prénom' (First name), 'Type' (Personnel), 'Accès porte/zone' (Access door/zone), 'Accès étage' (Access floor), 'Localisation' (Location), 'Sociétés' (Companies), 'Output', and 'Appartenance (groupe)' (Group). Below these fields are several checkboxes under 'Paramétrage spécifique' (Specific configuration), including 'Accès temporaire' (Temporary access), 'Tps suppl. d'ouverture de porte' (Additional door opening time), 'Ne pas prendre en compte dans l'apb' (Do not take into account in the apb), and 'Cet utilisateur peut armer / désarmer l'alarme intrusion' (This user can arm / disarm the intrusion alarm). The last checkbox is checked. At the bottom, there are expandable sections for 'Informations supplémentaires' (Additional information), 'Visites' (Visits), 'Biens' (Assets), 'Documents', and 'Ajouter un accès individuel' (Add individual access).

Sous l'onglet « paramétrage spécifique » cochez « cet utilisateur peut armer / désarmer l'alarme intrusion ».

## Départ tardif

La fonctionnalité « départ tardif » donne la possibilité aux personnes autorisées de décaler l'armement selon un horaire d'une zone. Pour accéder à cette option il faut d'abord l'activer dans les paramètres généraux de l'intrusion.



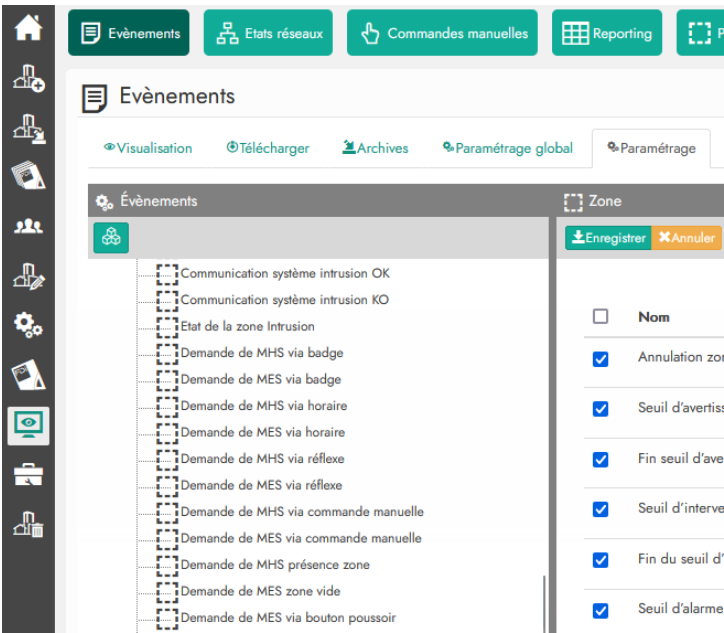
Cliquez sur « Equipment and settings » dans le bandeau de gauche, puis sélectionnez la ligne zones. Cochez la case « départ tardif » afin d'accéder aux paramètres supplémentaires.

- **Activé par** : c'est le comportement qui déclenchera l'activation du départ tardif (exemple, triple badgeage).
- **Temps avant application de comportement lecteur « départ tardif »** : délais avant l'armement horaire de l'intrusion pendant lequel il sera possible de déclencher le départ tardif. Exemple : si l'administrateur renseigne 10 minutes dans ce champ, et qu'une zone s'arme automatiquement à 20h, alors l'utilisateur pourra demander un départ tardif uniquement à partir de 19h50.
- **Temps de report de la mise en service** : c'est le délai pendant lequel l'armement de la zone sera décalé (en minutes). Exemple, si l'admin renseigne 30 minutes dans ce champ et que la zone s'arme automatiquement à 20h. Alors le départ tardif armera l'intrusion de la zone à partir de 20h30.

Suivi de l'intrusion par les événements

Deux menus permettent de surveiller l'intrusion sur un site :

- « **Supervision/Présence zone** » le statut des zones gérant l'intrusion est affiché ainsi que la validité de sa connexion depuis
- « **Supervision/état réseau** » la connexion de la centrale intrusion Elkron/Médéa à la centrale Ipevia.

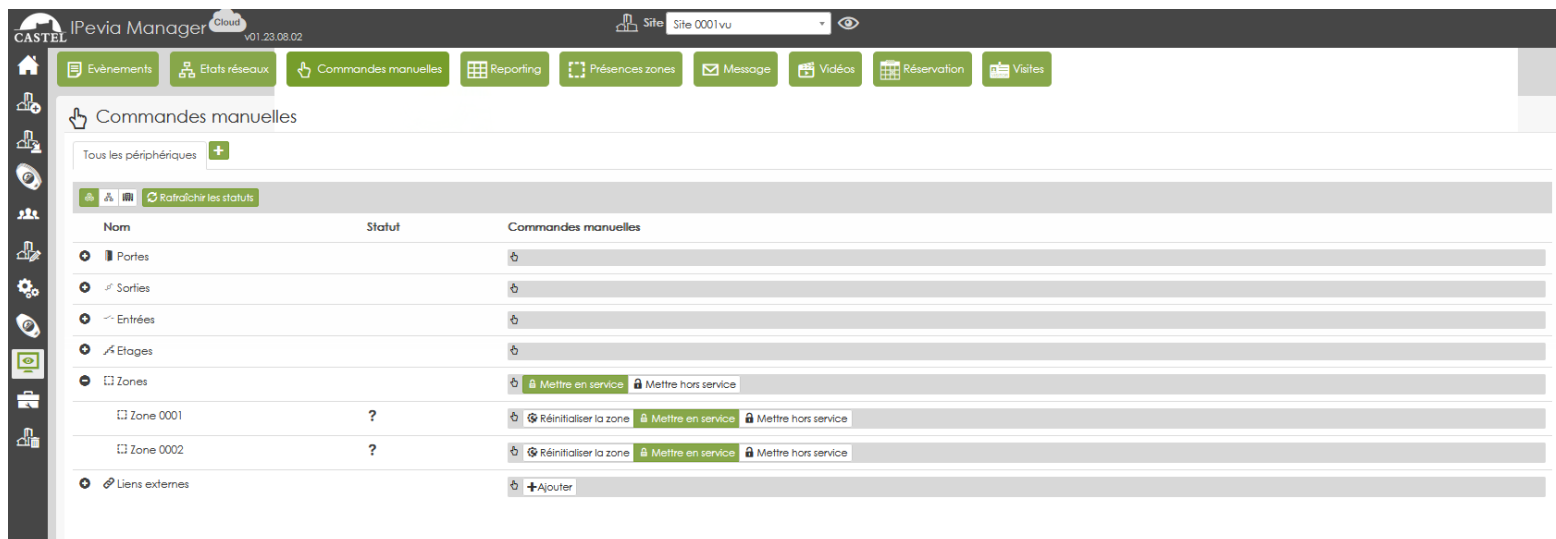


Le journal des événements montre lorsqu'une zone est en statut « armé » ou « désarmé ».

| Date / Hour         | Évènement                                  | Élément                                                              | Informations    | Identifiant |
|---------------------|--------------------------------------------|----------------------------------------------------------------------|-----------------|-------------|
| 2024-10-03 17:21:25 | Etat de la zone Intrusion                  | Hall d'entrée - secteur 1                                            | Etat : Armé     | -           |
| 2024-10-03 17:20:59 | Etat de la zone Intrusion                  | Hall d'entrée - secteur 1                                            | Etat : Non armé | -           |
| 2024-10-03 17:20:52 | Présence sur zone                          | Hall d'entrée - secteur 1                                            | -               | -           |
| 2024-10-03 17:20:52 | Entrée Zone                                | Hall d'entrée - secteur 1                                            | Nom 01          | ✎ 87412400  |
| 2024-10-03 17:20:52 | Accès autorisé porte simple identification | intrusion zone - Porte 0001<br>Lecteur 0001<br>accès zones intrusion | Nom 01          | ✎ 87412400  |
| 2024-10-03 17:20:52 | Demande de MES via badge                   | Hall d'entrée - secteur 1<br>Lecteur 0001                            | Nom 01          | ✎ 87412400  |

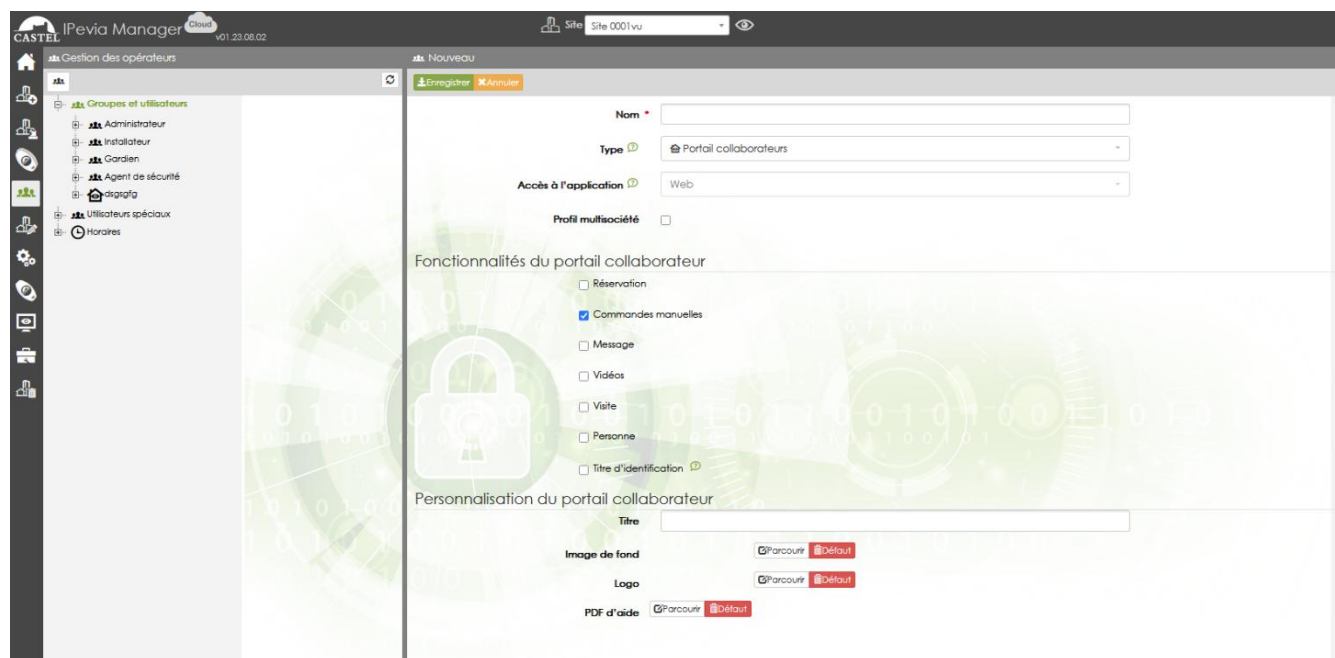
## Commandes manuelles de l'intrusion

Depuis la page « **Supervision/commandes manuelles** » du logiciel, le gestionnaire peut connaître le statut de chaque zone et les modifier par les BP de commandes manuelles



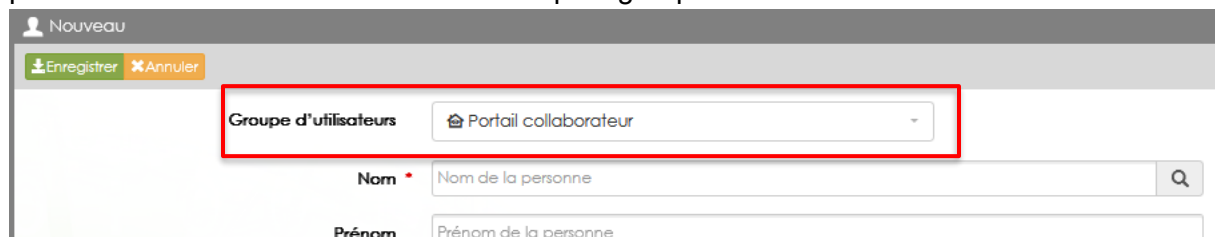
Le gestionnaire de site peut déléguer l'armement/le désarmement à un autre utilisateur.

- **Par un accès au portail résident** : sélectionnez « gestion des opérateurs » dans le bandeau de gauche, puis cliquez sur le bouton « ajouter un groupe d'utilisateur » en haut.

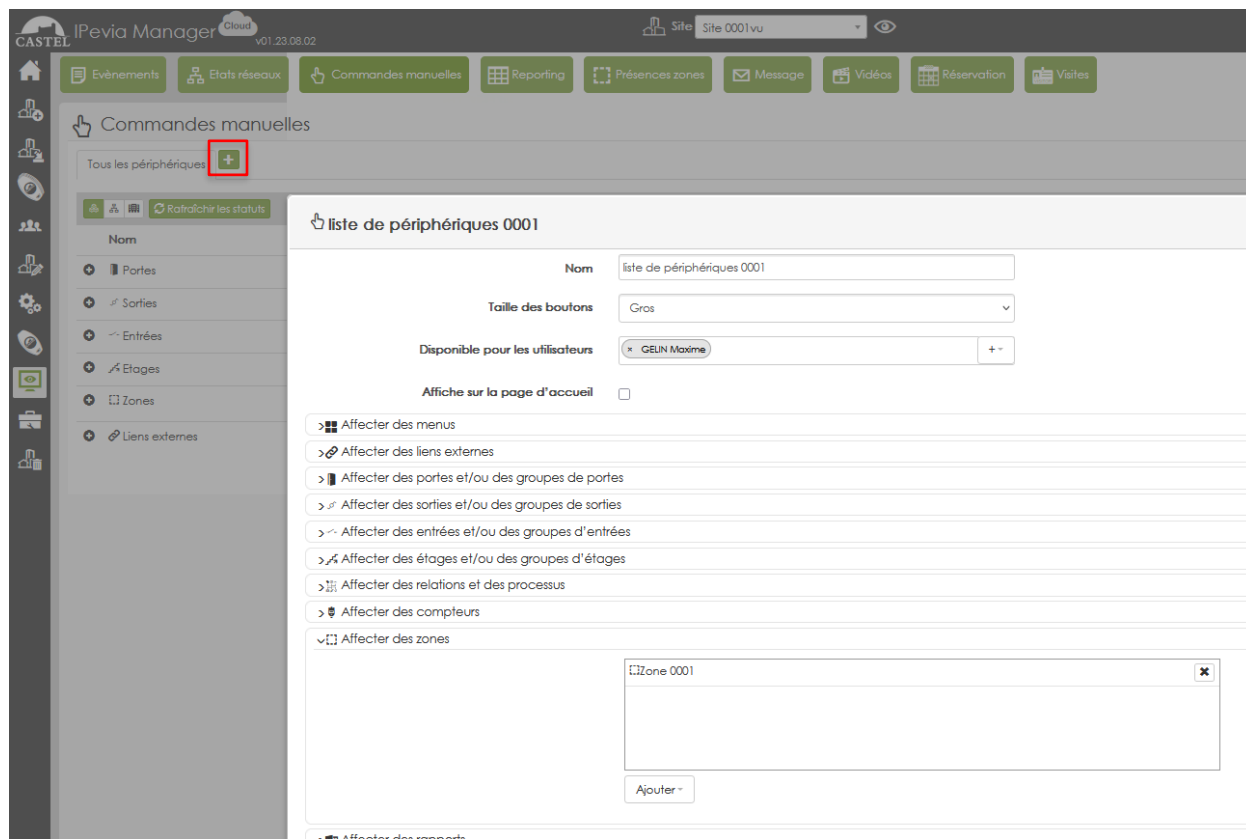


Dans le champ « type », choisir « portail collaborateur ». Parmi les « Fonctionnalités du portail collaborateur », cochez la case « commandes manuelles ». Puis sauvegardez ce nouveau groupe d'utilisateurs.

Ensuite lorsque vous créez un nouvel utilisateur, sélectionnez le portail collaborateur précédemment créé dans la liste du champs « groupe d'utilisateurs ».

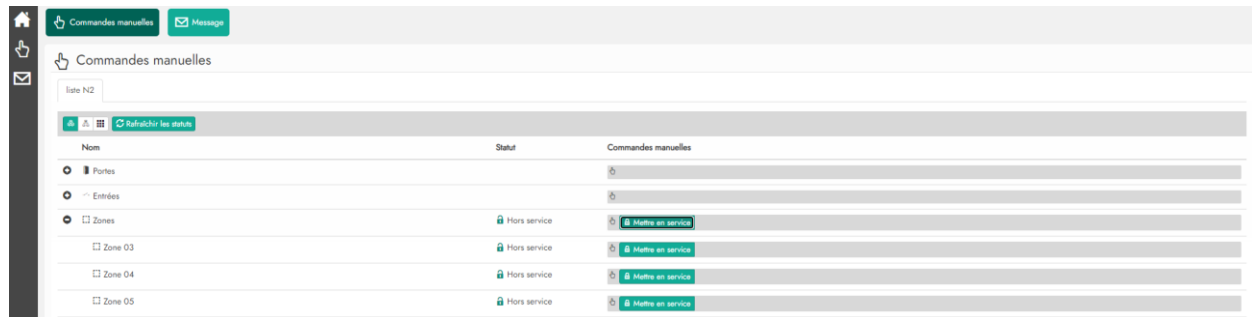


- **Par une page de commande manuelle personnalisée** : depuis le menu « monitoring » puis « commandes manuelles », cliquez sur le bouton « + » en haut de page. La page suivante s'ouvre :



Le champs « disponible pour les utilisateurs » permet de saisir les personnes qui pourront utiliser les commandes manuelles.

L'onglet « affecter des zones » permet de déterminer quelles zones ils pourront piloter.

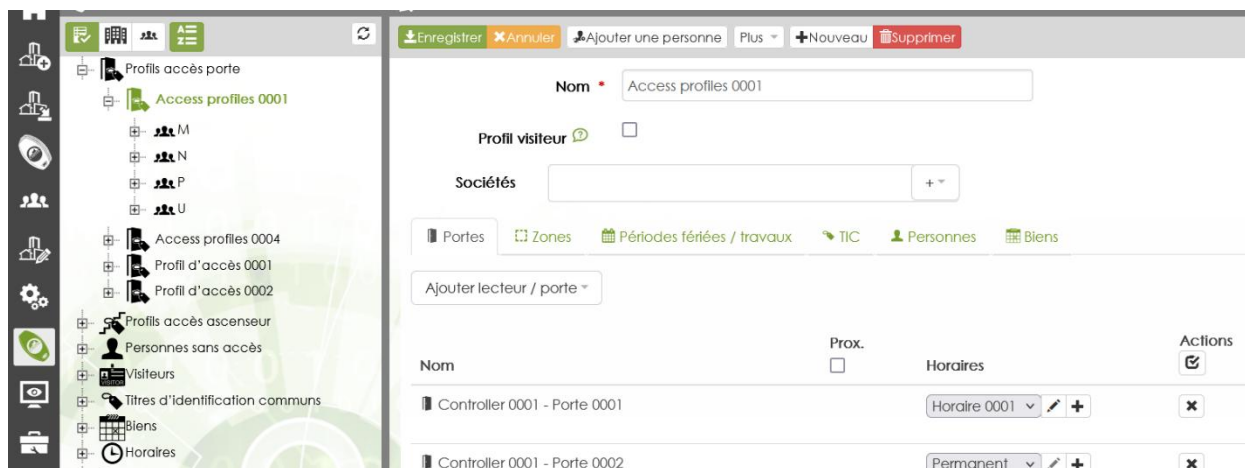


Lorsqu'il se connectera avec son compte, l'utilisateur pourra armer/désarmer la/les zones depuis les commandes manuelles.



## 5. Profils d'accès et badges

La gestion de tous les profils d'accès aux portes/étages est accessible via le bouton en forme de badge dans le cadre gauche. Avec ce menu, vous pouvez également gérer les utilisateurs, les contrats, les actifs et les profils horaires.



### 5.1. Profils d'accès porte

Le profil d'accès à la porte est une liste de portes autorisées avec des horaires spécifiques. Ces profils s'appliquent à des individus et à leurs clés.

Le logiciel gère deux profils d'accès à la porte par utilisateur ainsi que deux profils d'accès aux étages. À chaque fois, qu'il y a un profil permanent et un profil temporaire limité par une date/heure de début et de fin.

Un profil d'accès contient les onglets suivants:

- **Porte** : liste des portes autorisées par ce profil d'accès
- **Zones** : liste des portes considérées comme des entrées de zone
- **Périodes fériées/travaux** : liste des jours fériés ou des périodes de travail que ce profil d'accès suivra
- **TIC (titre d'identification commun)** : il s'agit d'un badge, d'un code de clavier, etc., non attribué à une personne. Cela peut être un code d'accès fourni à différentes personnes ou des badges visiteurs
- **Personnes** : liste des personnes utilisant ce profil d'accès
- **Biens** : tout bien (salle ou matériel par exemple) renseigné dans un profil d'accès sera réservable par les personnes qu'elles incluent (dans l'onglet « personne »)

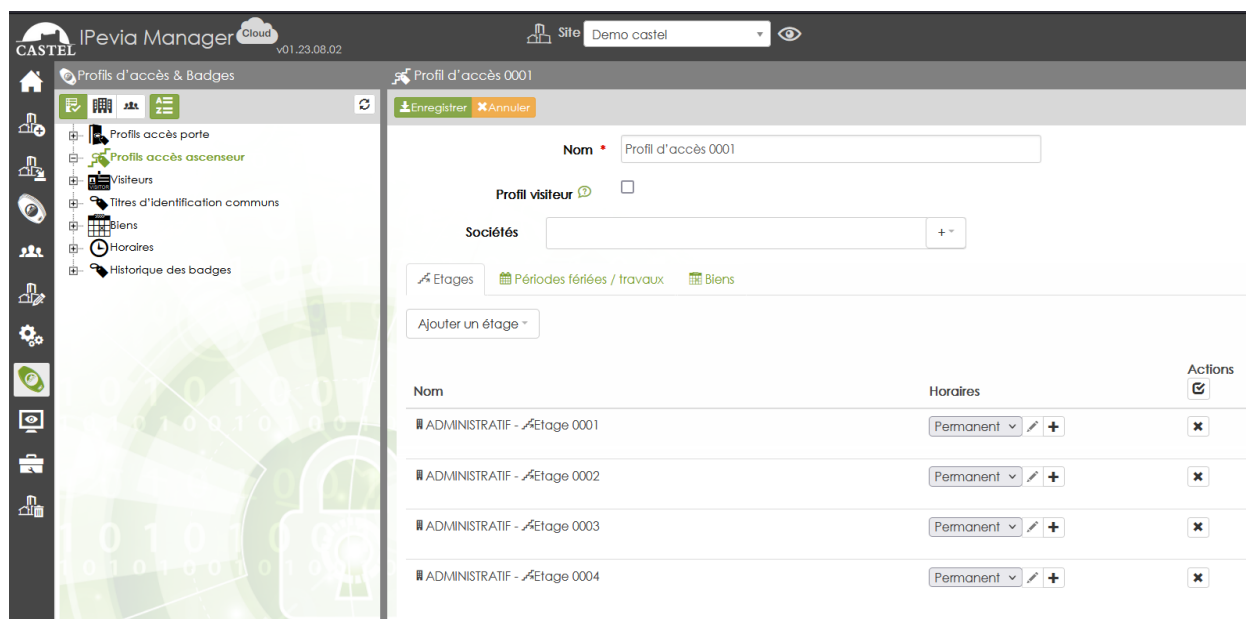
## 5.2. Profil d'accès ascenseur

Le profil d'accès ascenseurs est une liste de bâtiments/étages autorisés à des horaires spécifiques. Ces profils s'appliquent aux personnes et à leurs CLÉS et influencent le comportement des ascenseurs. Si un étage est interdit à un moment donné, les ascenseurs ne pourront jamais atteindre ce niveau.

Un profil d'accès contient les onglets suivants :

- **Etage** : liste des étages autorisés
- **Périodes de vacances / Maintenance** : liste des périodes de vacances ou de travail que ce profil d'accès suivra
- **biens** : vous pouvez appliquer un actif spécifique à un profil d'accès au sol. Pendant le profil horaire d'accès au sol, l'utilisateur peut soit accéder à l'actif, soit se voir interdire l'accès.

L'onglet **Vacances / Travail** est identique à ceux détaillés dans le chapitre 4.1 « Profil d'accès à la porte ».



**Ipevia Manager** Cloud v01.23.08.02 Site Demo castel

Profil d'accès & Badges

Profil d'accès 0001

Enregistrer Annuler

Nom \* Profil d'accès 0001

Profil visiteur ☐

Sociétés  + -

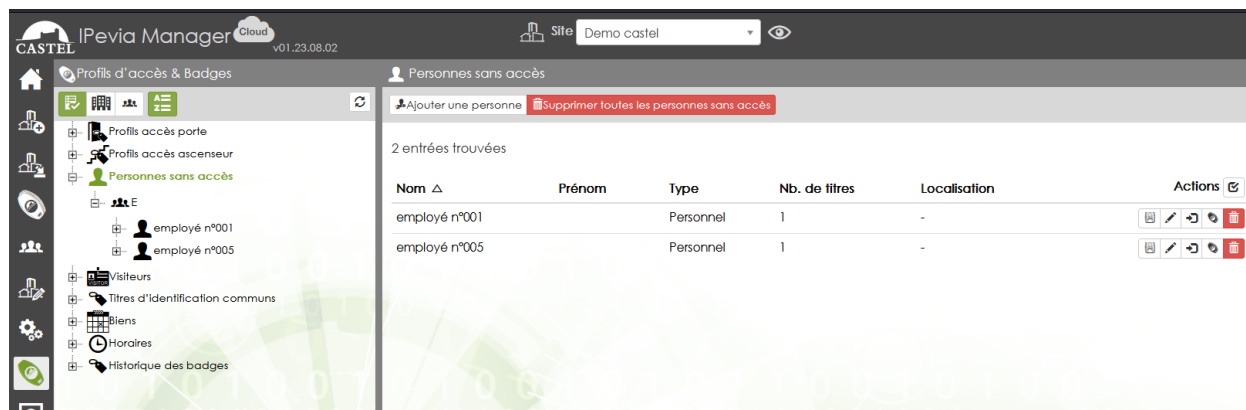
Etages Périodes fériées / travaux Biens

Ajouter un étage

| Nom                        | Horaires                         | Actions                  |
|----------------------------|----------------------------------|--------------------------|
| ADMINISTRATIF - Etage 0001 | Permanent <input type="text"/> + | <input type="checkbox"/> |
| ADMINISTRATIF - Etage 0002 | Permanent <input type="text"/> + | <input type="checkbox"/> |
| ADMINISTRATIF - Etage 0003 | Permanent <input type="text"/> + | <input type="checkbox"/> |
| ADMINISTRATIF - Etage 0004 | Permanent <input type="text"/> + | <input type="checkbox"/> |

## 5.3. Personnes sans accès

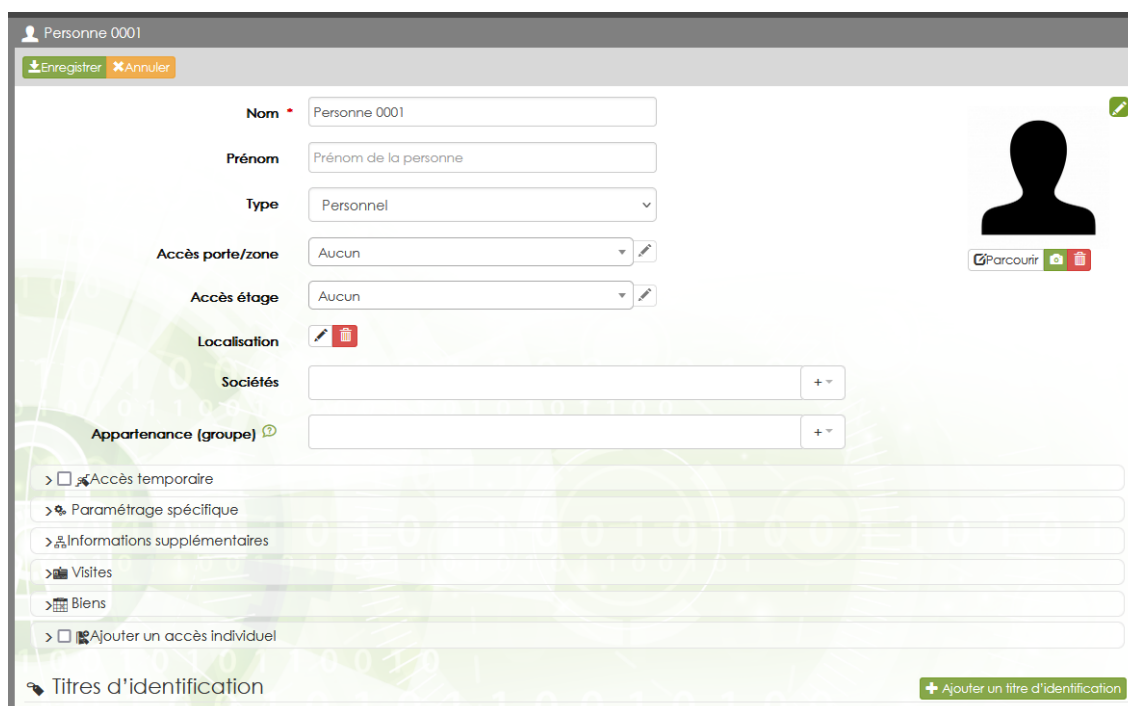
Sous la section « Utilisateurs et profils d'accès », il existe un menu spécifique qui liste les utilisateurs sans profil d'accès assigné.



Il est possible d'assigner plusieurs identifiants (IC) à un utilisateur du contrôle d'accès. Un IC fait référence à un badge, une empreinte digitale, une plaque d'immatriculation, un code de clavier, etc.

## 5.4. Utilisateur

En cliquant sur le bouton "ajouter un utilisateur" en haut de la fenêtre, vous pouvez créer une nouvelle personne et lui attribuer un ou plusieurs IC.



Personne 0001

Enregistrer Annuler

Nom : Personne 0001

Prénom : Prénom de la personne

Type : Personnel

Accès porte/zone : Aucun

Accès étage : Aucun

Localisation : [Edit] [Delete]

Sociétés : [Add] [Remove]

Appartenance (groupe) : [Add] [Remove]

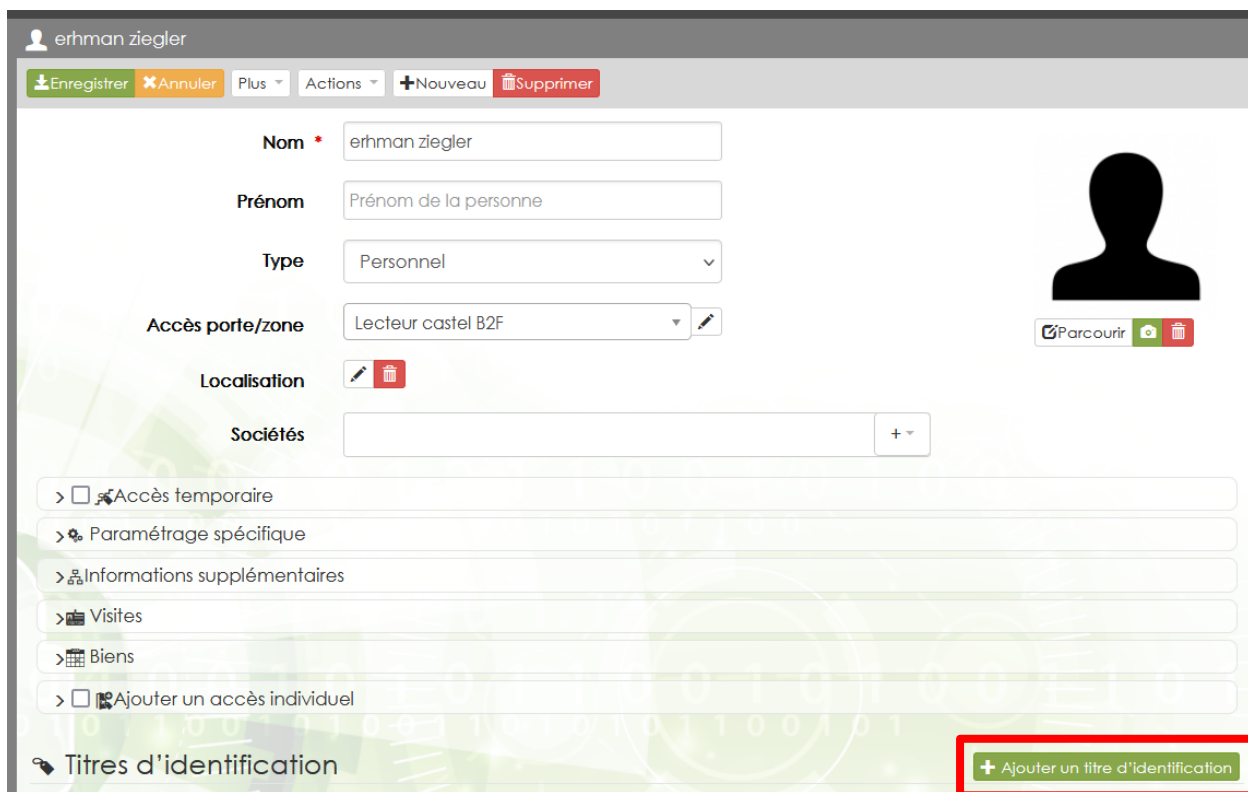
☐ Accès temporaire  
☐ Paramétrage spécifique  
☐ Informations supplémentaires  
☐ Visites  
☐ Biens  
☐ Ajouter un accès individuel

Titres d'identification [Ajouter un titre d'identification]

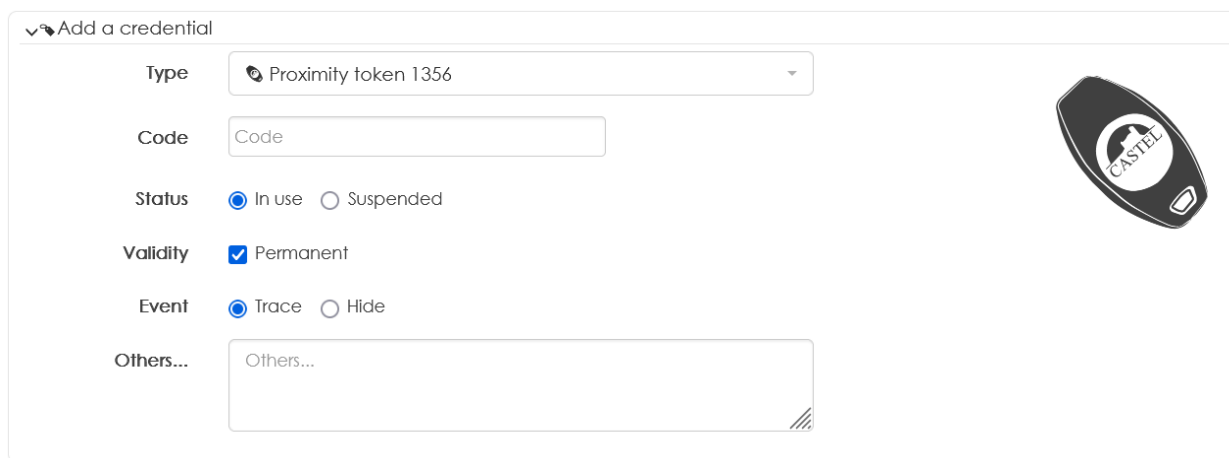
Une personne (ou un utilisateur) dans le système de contrôle d'accès est définie comme suit :

| Champ                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nom</b>                                   | Prénom/nom ou informations supplémentaires (identifiant d'employé, email, adresse, etc...)                                                                                                                                                                                                                                                                                                                                          |
| <b>Accès porte/zone</b>                      | Profil d'accès aux portes/zones auquel l'utilisateur est autorisé avec son ou ses identifiants. Celui-ci est permanent.                                                                                                                                                                                                                                                                                                             |
| <b>Accès étage</b>                           | Profil d'accès aux étages auquel l'utilisateur est autorisé avec son ou ses identifiants. Celui-ci est permanent.                                                                                                                                                                                                                                                                                                                   |
| <b>Localisation</b>                          | Lorsque l'option architecture est cochée (voir le chapitre "2.2 fonctionnalités"), il peut être plus pratique de localiser une personne au sein d'un site et de lui attribuer le profil d'accès requis.                                                                                                                                                                                                                             |
| <b>Accès temporaire</b>                      | Permet de définir un profil d'accès temporaire pour la porte/la zone et un profil d'accès pour le sol. Ils sont limités par des dates/horaires de début et de fin de validité.                                                                                                                                                                                                                                                      |
| <b>Paramétrages spécifiques (onglet)</b>     | <p><b>Temps supplémentaire d'ouverture de porte</b> : si coché, le temps défini ici est ajouté au temps défini pour chaque profil d'accès porte/sol.</p> <p><b>Ne pas prendre en compte dans l'apb</b> : si coché, l'utilisateur ne sera pas affecté par les options APB.</p> <p><b>Cet utilisateur peut armer/désarmer l'alarme intrusée</b> : lié à l'option intrusion, si coché, l'utilisateur peut armer/désarmer l'alarme.</p> |
| <b>Informations supplémentaires (onglet)</b> | Pour entrer d'autres informations d'identité telles qu'un e-mail, un numéro d'enregistrement, une adresse...                                                                                                                                                                                                                                                                                                                        |
| <b>Visites (onglet)</b>                      | Pour voir les visites enregistrées sur le logiciel concernant cet utilisateur.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Biens (onglet)</b>                        | Une liste des biens que cet utilisateur pourra réserver                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Ajouter un accès individuel (tab)</b>     | Pour ajouter une porte spécifique en plus des portes renseignées pour le profil d'accès. Cela est utile afin de créer un contrôle d'accès spécifique pour un utilisateur, indépendamment des paramètres du profil d'accès.                                                                                                                                                                                                          |

Chaque utilisateur dispose d'un nombre illimité d'identifiants d'identification. Des options peuvent être définies pour chaque identifiant (accès par jeton ou Bluetooth). Pour ajouter un nouvel identifiant, cliquez sur le bouton « créer un identifiant » en bas à droite de la fenêtre.



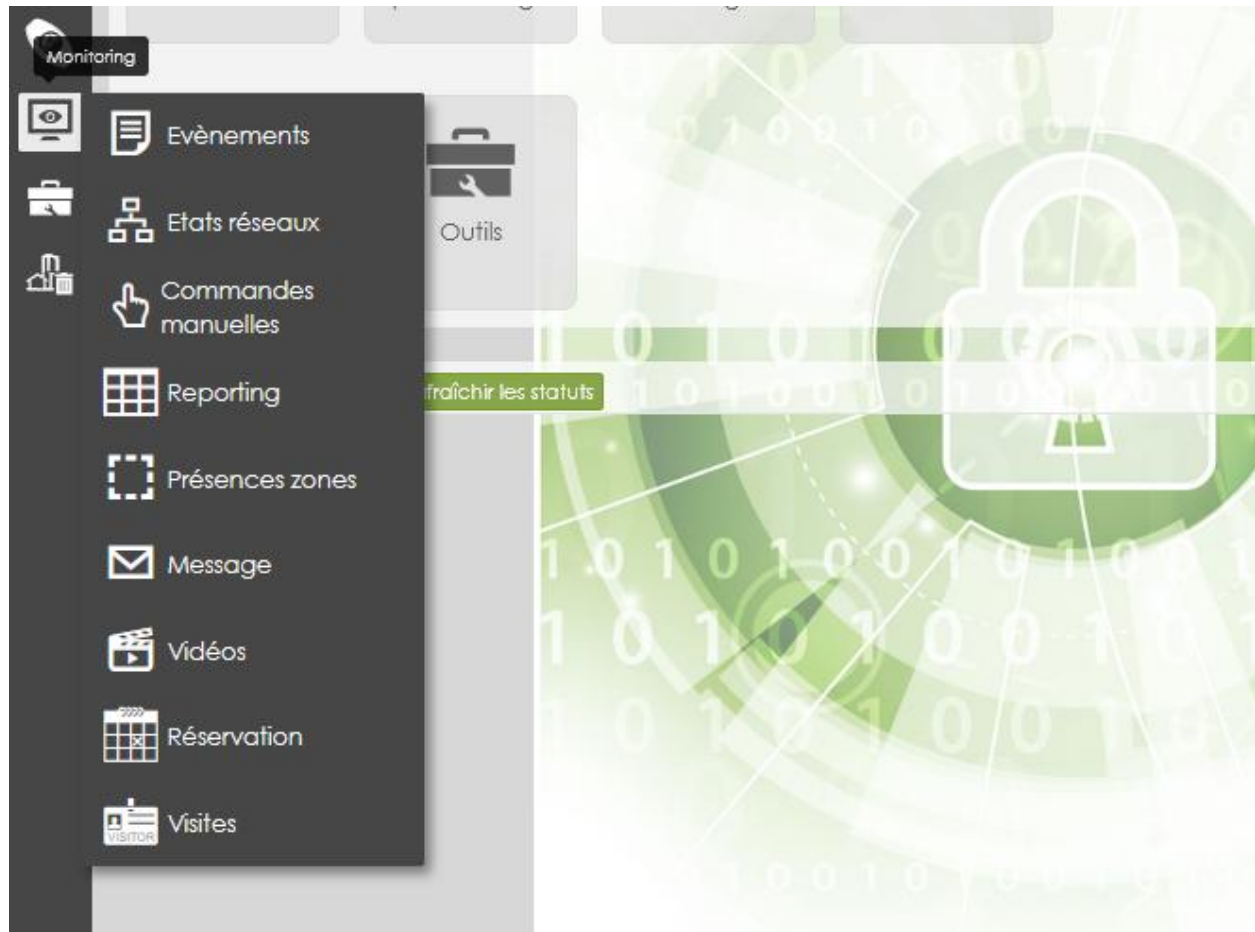
It opens the window below



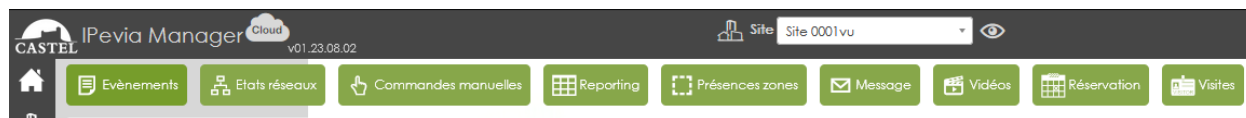
| Field     | Description                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type      | Can be a 13.56 token or a bluetooth access                                                                                                                                                                          |
| Code      | <p>If <b>13.56 Proximity token</b> is set in the previous field, enter Hexa code written on the key</p> <p>If <b>bluetooth</b> is set in the previous field, enter the mobile and email information of the user</p> |
| Status    | <p><b>In use</b> : the token gives access as normal</p> <p><b>Suspended</b> : when the token is lost. If you uncheck this box, the user will regain its access rights</p>                                           |
| Validity  | If "permanent" is unchecked, you can enter validity dates for this credential                                                                                                                                       |
| Event     | <p>Trace : this credential will appear in the event monitoring when used.</p> <p>Hide : it will not appear in the event log when used.</p>                                                                          |
| Others... | To add comments/additional information to this credential                                                                                                                                                           |

## 6. Monitoring

Le menu de supervision, accessible depuis le cadre de gauche, permet d'afficher et de surveiller tout ce qui se passe sur le site.



Lorsque vous cliquez sur l'icône de surveillance, vous pouvez naviguer entre les différents outils en cliquant sur les boutons situés en haut.

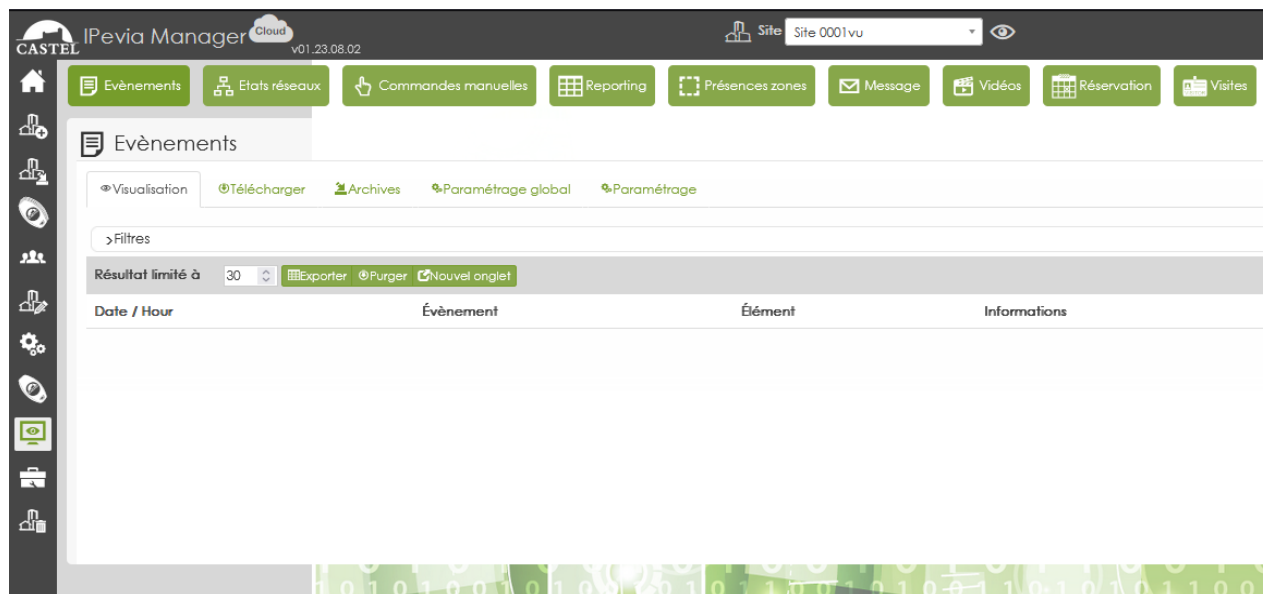


Voici les outils disponibles :

- **Événements** : affiche l'historique du contrôleur avec tous les événements (badge inconnu, accès refusé, accès autorisé, etc.).
- **Etats réseaux** : affiche l'état des centrales et des cartes d'entrées/sorties (connecté oui/non, version du logiciel).
- **Commandes manuelles** : permet de contrôler les portes, étages, sorties avec la possibilité de définir des tableaux de bord personnalisables.
- **Reporting** : génère des exports Excel sur les badges, les personnes, les événements, etc.
- **Présence zones** : affiche la liste des personnes présentes dans chaque zone.
- **Message** : affiche uniquement les événements pour lesquels un affichage spécifique a été programmé. Généralement, il s'agit d'événements de type alerte comme "Porte forcée", etc.
- **Vidéos** : permet de voir les images en direct de la vidéosurveillance.
- **Réservations** : affiche une vue planifiée des réservations d'équipements.
- **Visites** : affiche toutes les visites prévues. Vous pouvez planifier une visite ou en créer une instantanément.

## 6.1 Événements

Les contrôleurs IPévia gèrent jusqu'à 20 000 événements qui sont envoyés aux serveurs en temps réel lorsque la communication serveur/contrôleur est opérationnelle.

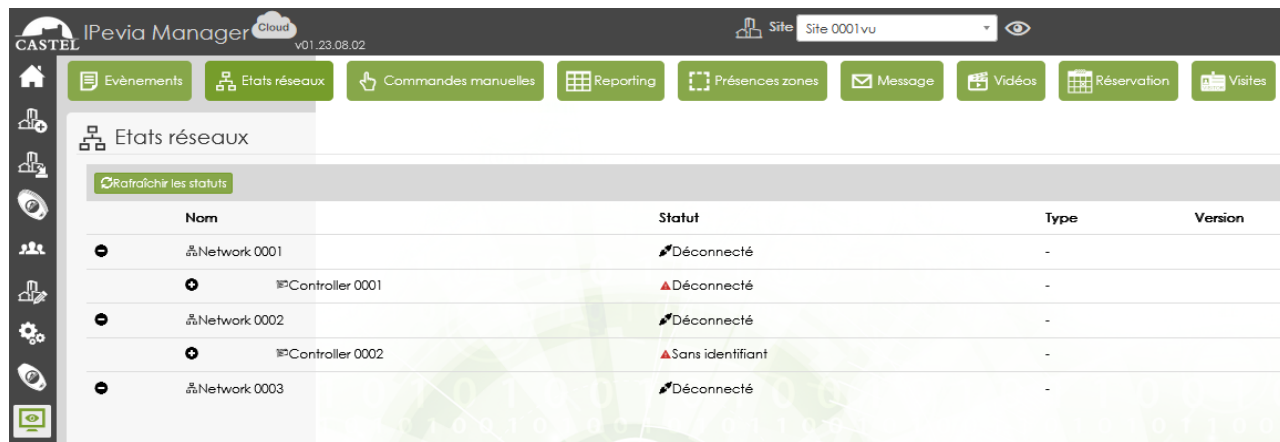


La fonction événement donne accès à d'autres options :

- **Visualisation** : chaque type d'événement a un niveau de priorité de 1 à 9. L'affichage peut être configuré pour ne montrer que les plus importants. Par exemple, l'événement "Porte forcée" a un niveau de priorité de 8, tandis que "Porte ouverte" a un niveau de 2. Avec un niveau de priorité réglé sur 5, l'événement "Porte ouverte" n'apparaîtra pas. Le niveau de priorité de chaque événement est défini dans l'onglet "paramètres". Il est également possible de filtrer l'affichage par type d'événement, par élément (porte, étage, etc.) ou par événement spécifique (ex. : uniquement les accès refusés).
- **Télécharger** : chaque contrôleur gère jusqu'à 20 000 événements. Lors de l'initialisation de la communication avec le serveur, seuls les derniers événements sont récupérés. L'option "Téléchargement" permet de rechercher ces événements manquants dans le contrôleur. Les filtres décrits ci-dessus s'appliquent également lors du téléchargement depuis les unités centrales.
- **Archives** : pour charger des archives dans le logiciel, par exemple un fichier Excel. Comme la limite d'événements par contrôleur est de 20 000, cette option permet d'enregistrer plus de 20 000 événements dans le logiciel.
- **Paramétrage global** : cet onglet permet de définir quels niveaux de priorité sont stockés dans les contrôleurs et quels autres niveaux sont affichés à l'écran.
- **Paramètres** : permet de choisir le niveau de priorité de l'événement (ex. : ouverture du capot) ainsi que la couleur affichée par le lecteur.

## 6.2 Etats réseaux

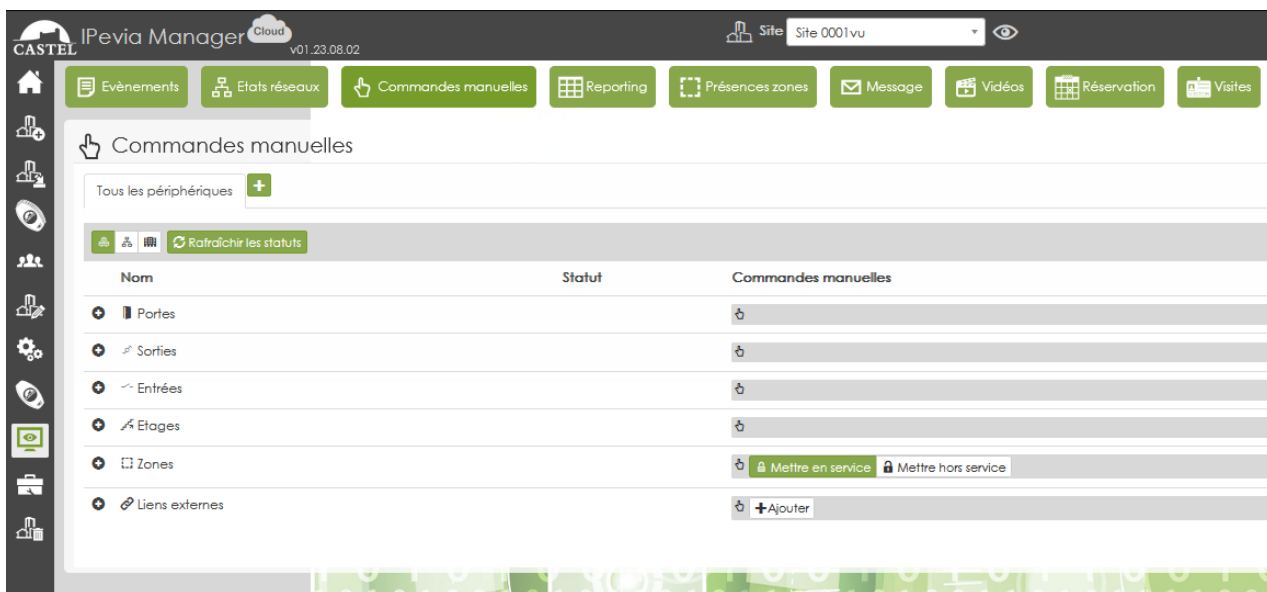
A window shows the status of the controllers (connected / disconnected), their software versions, and the input/output cards connected to each controller.



| Nom             | Statut           | Type | Version |
|-----------------|------------------|------|---------|
| Network 0001    | Déconnecté       | -    |         |
| Controller 0001 | Déconnecté       | -    |         |
| Network 0002    | Déconnecté       | -    |         |
| Controller 0002 | Sans identifiant | -    |         |
| Network 0003    | Déconnecté       | -    |         |

## 6.3 Commandes manuelles

Ce menu permet de contrôler les portes, sorties ou étages depuis le logiciel. Ces commandes peuvent être soit impulsionnelles, soit permanentes. Par exemple, il est possible d'ouvrir une porte pour un visiteur ou de désactiver la sécurité d'un étage jusqu'à ce qu'elle soit réactivée depuis le logiciel.

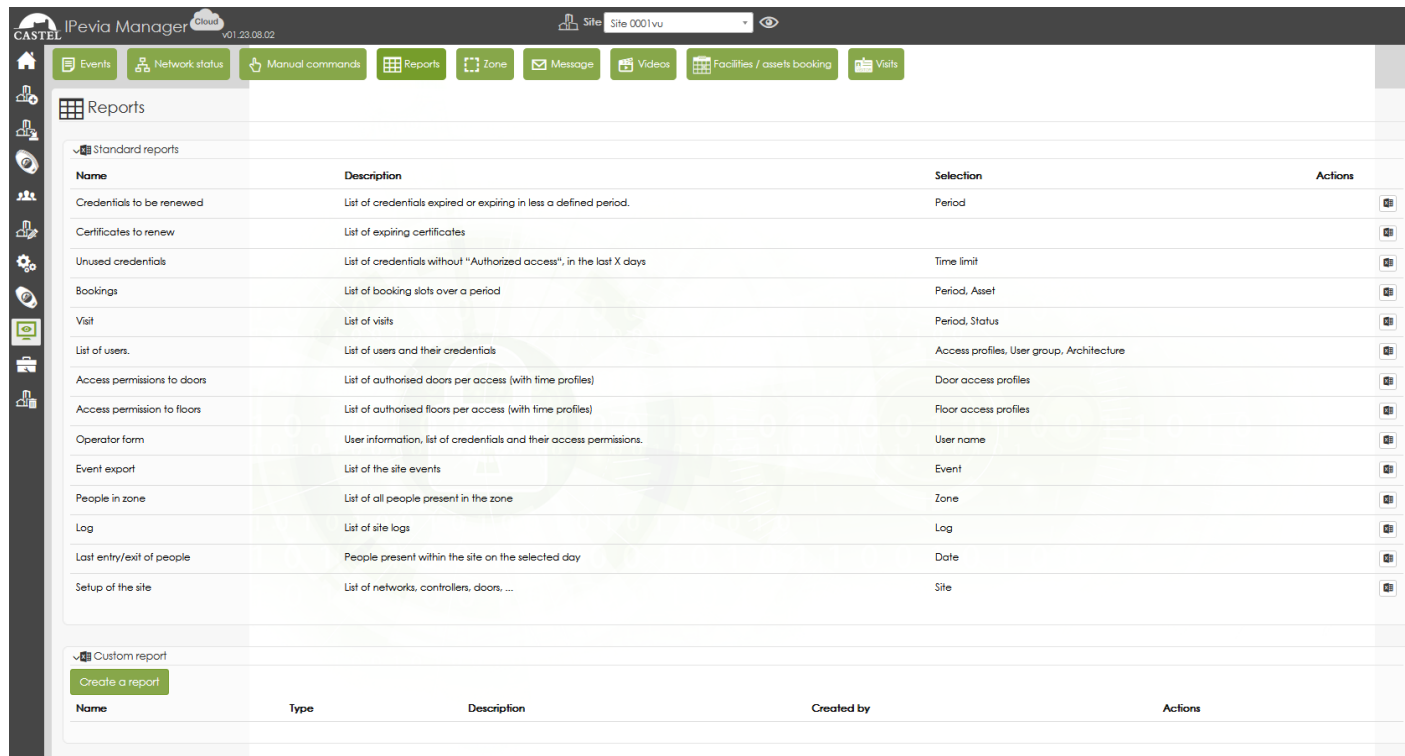


| Nom            | Statut | Commandes manuelles                                                                                 |
|----------------|--------|-----------------------------------------------------------------------------------------------------|
| Portes         |        | <input type="button" value="Ouvrir"/>                                                               |
| Sorties        |        | <input type="button" value="Ouvrir"/>                                                               |
| Entrées        |        | <input type="button" value="Ouvrir"/>                                                               |
| Etages         |        | <input type="button" value="Ouvrir"/>                                                               |
| Zones          |        | <input type="button" value="Mettre en service"/> <input type="button" value="Mettre hors service"/> |
| Liens externes |        | <input type="button" value="Ajouter"/>                                                              |

## 6.4 Reporting

Le logiciel permet de générer des rapports sur les événements, les utilisateurs, les portes, les étages, etc. Un rapport est un fichier Excel et peut être déclenché manuellement, automatiquement ou par un événement. Quatorze rapports sont prédéfinis lors de l'installation du logiciel.

Sélectionnez le rapport dans la liste et cliquez sur le logo Excel à droite.

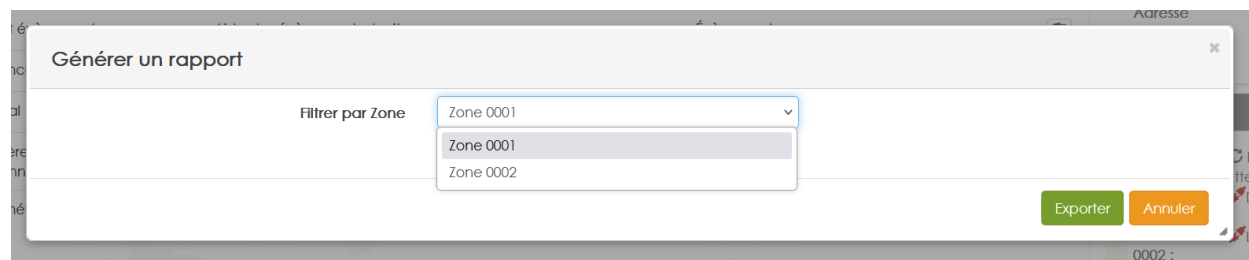


| Name                        | Description                                                         | Selection                                 | Actions |
|-----------------------------|---------------------------------------------------------------------|-------------------------------------------|---------|
| Credentials to be renewed   | List of credentials expired or expiring in less a defined period.   | Period                                    |         |
| Certificates to renew       | List of expiring certificates                                       |                                           |         |
| Unused credentials          | List of credentials without "Authorized access", in the last X days | Time limit                                |         |
| Bookings                    | List of booking slots over a period                                 | Period, Asset                             |         |
| Visit                       | List of visits                                                      | Period, Status                            |         |
| List of users.              | List of users and their credentials                                 | Access profiles, User group, Architecture |         |
| Access permissions to doors | List of authorised doors per access (with time profiles)            | Door access profiles                      |         |
| Access permission to floors | List of authorised floors per access (with time profiles)           | Floor access profiles                     |         |
| Operator form               | User information, list of credentials and their access permissions. | User name                                 |         |
| Event export                | List of the site events                                             | Event                                     |         |
| People in zone              | List of all people present in the zone                              | Zone                                      |         |
| Log                         | List of site logs                                                   | Log                                       |         |
| Last entry/exit of people   | People present within the site on the selected day                  | Date                                      |         |
| Setup of the site           | List of networks, controllers, doors, ...                           | Site                                      |         |

**Custom report**  
 Create a report

| Name | Type | Description | Created by | Actions |
|------|------|-------------|------------|---------|
|      |      |             |            |         |

La fenêtre suivante varie selon le rapport demandé. Ici il s'agit du rapport de présence zone. Saisissez l'élément souhaité puis cliquez sur le bouton « Exporter ».



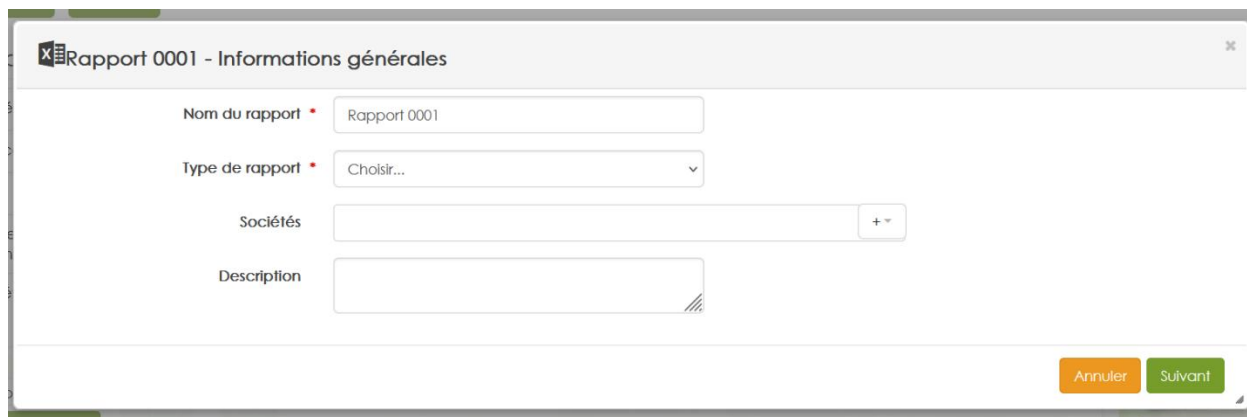
Générer un rapport

Filter by Zone: Zone 0001

Zone 0001  
Zone 0002

Exporter Annuler

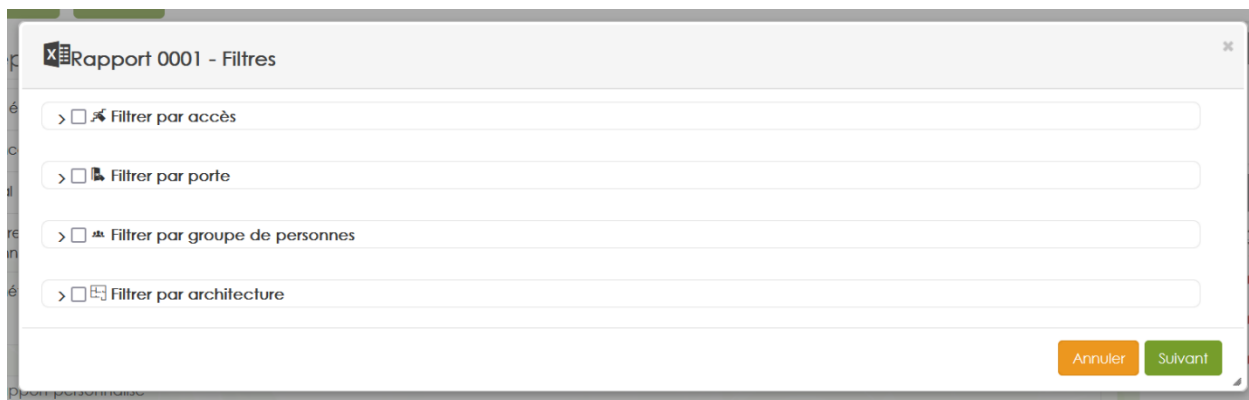
Vous pouvez également créer des rapports personnalisés en tenant compte de critères spécifiques. Cliquez sur le bouton « Créer un rapport » en bas de la page. La fenêtre suivante s'ouvre :



- **Nom du rapport** : attribuez un nom au fichier d'exportation Excel.
- **Type de rapport** : choisissez les informations pertinentes qui apparaîtront dans votre exportation, telles que les événements, les personnes, les zones ou les visites. Ce choix modifiera les champs à remplir lors de l'étape suivante.
- **Sociétés** : vous pouvez choisir d'afficher uniquement les critères en fonction d'une entreprise. En cliquant sur le bouton « + > », vous verrez une liste de toutes les entreprises présentes sur le site.
- **Description** : pour ajouter quelques commentaires sur ce fichier. En cliquant sur le bouton « suivant », vous accédez à plus de paramètres d'exportation. Les champs apparaissant sont définis par le choix effectué dans le champ « type de rapport ». Exemple : si « événement » est sélectionné dans le type de rapport :

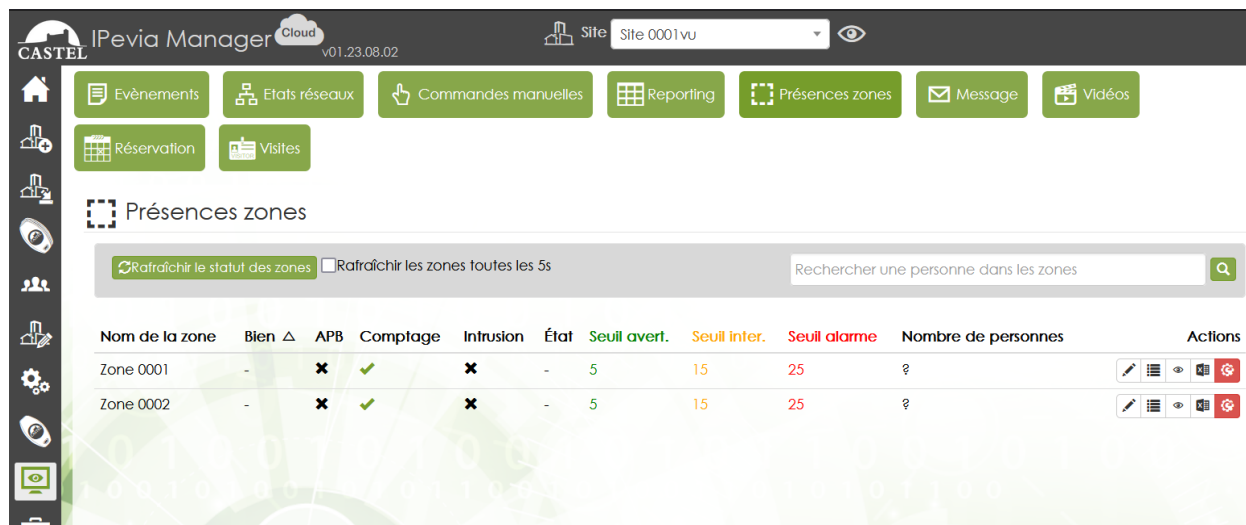
Ensuite cliquez sur le bouton suivant en bas à droite. L'affichage des champs de la prochaine fenêtre sont influencés par l'option choisie dans la case type de rapport :

Exemple si “personne” est renseigné dans le type de rapport :



## 6.5 Présence zones

Lorsque la gestion des zones est activée (voir le chapitre 2.9), l'onglet « Zone » fournit une vue directe des utilisateurs dans chaque zone.



The screenshot shows the Ipevia Manager interface. The top bar includes the CASTEL logo, version v01.23.08.02, and a site selector set to 'Site 0001vu'. The main navigation bar contains buttons for 'Evènements', 'Etats réseaux', 'Commandes manuelles', 'Reporting', 'Présences zones' (selected), 'Message', and 'Vidéos'. The sidebar on the left has icons for home, reservation, visits, and other functions. The main content area is titled 'Présences zones' and features a search bar and two refresh buttons. Below this is a table with the following data:

| Nom de la zone | Bien △ | APB | Comptage | Intrusion | État | Seuil avert. | Seuil inter. | Seuil alarme | Nombre de personnes | Actions                               |
|----------------|--------|-----|----------|-----------|------|--------------|--------------|--------------|---------------------|---------------------------------------|
| Zone 0001      | -      | ✗   | ✓        | ✗         | -    | 5            | 15           | 25           | ?                   | [Edit] [List] [Eye] [Refresh] [Reset] |
| Zone 0002      | -      | ✗   | ✓        | ✗         | -    | 5            | 15           | 25           | ?                   | [Edit] [List] [Eye] [Refresh] [Reset] |

Des boutons supplémentaires sont situés à droite de chaque zone.

- **Edition (crayon)** : afin d'apporter des modifications dans les paramètres de la zone
- **Détails de la zone (liste)** : fonction disponible uniquement si le comptage par société, profil d'accès, profil d'étage... est activé.
- **Personnes dans la zone (œil)** : liste des personnes présentes dans la zone, avec la possibilité d'exporter un fichier Excel.
- **Réinitialiser la zone (cercle rouge)** : remets à zéro le comptage ainsi que la liste des personnes présentes dans la zone.

## 7. Réservation

IPeVia Manager vous permet de gérer les réservations de biens (salle de réunion, espace de coworking, places de parking pour les visiteurs, équipements, etc.).

Lorsqu'une salle est réservée pour une ou plusieurs personnes, ces utilisateurs héritent automatiquement des droits d'accès aux portes et aux étages menant à l'élément concerné (salle de réunion, équipement, etc.).

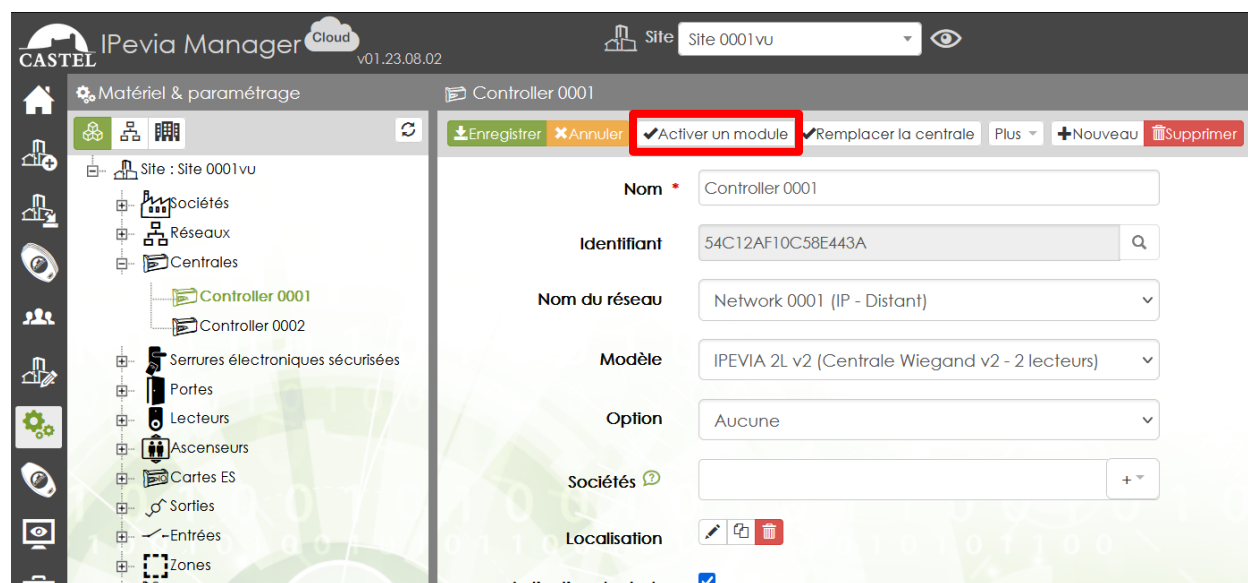
La fonctionnalité de réservation nécessite une licence additionnelle. Elle est accessible via l'activation du logiciel. Voici les étapes suivantes :

### 7.1 Pré requis

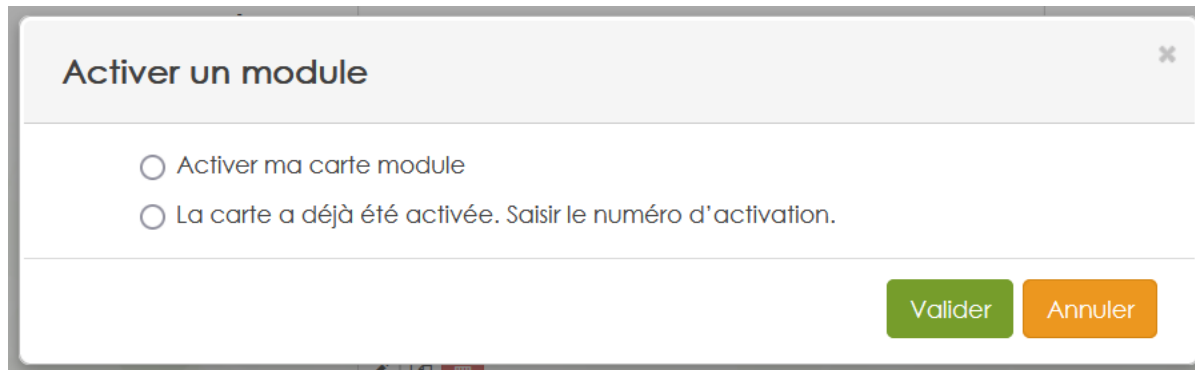
1- La fonction de réservation doit avoir été activée dans les propriétés du site (voir chapitre 2.2 : fonctionnalités).

2- La licence doit être activée.

Dans IPeVia, les licences sont liées aux centrales. Sélectionnez-en une disponible dans le menu "Matériel et paramétrage" et choisissez-en un dans l'arborescence à gauche. Cliquez ensuite sur le bouton "activer le module tiers" (voir capture d'écran ci-dessous).



Ensuite choisissez une des deux options.



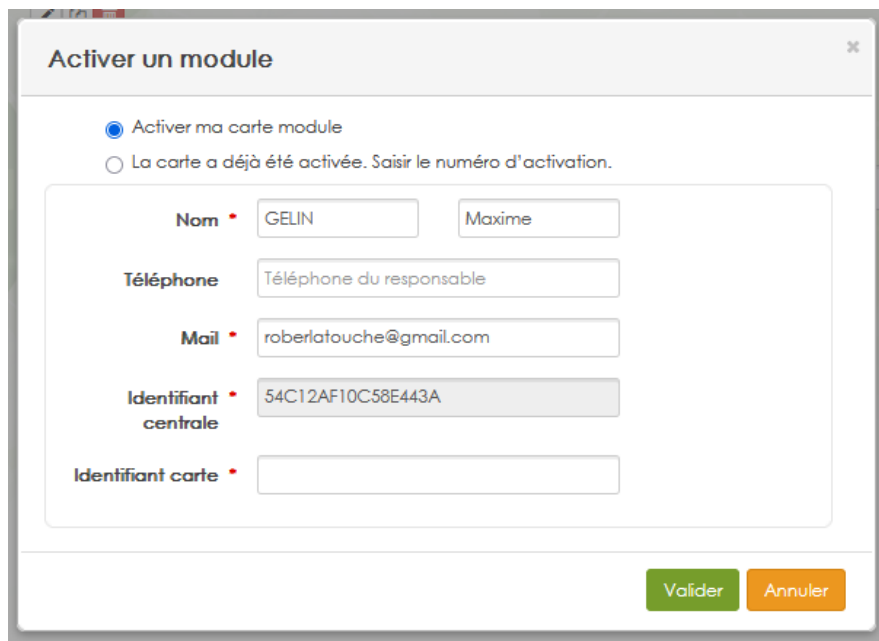
**Activer un module**

☐ Activer ma carte module

☐ La carte a déjà été activée. Saisir le numéro d'activation.

Valider Annuler

Puis renseignez toutes les informations nécessaires dont le numéro unique de la carte d'activation de la fonction réservation.



**Activer un module**

☒ Activer ma carte module

☐ La carte a déjà été activée. Saisir le numéro d'activation.

Nom \* GELIN Maxime

Téléphone Téléphone du responsable

Mail \* roberlatouche@gmail.com

Identifiant \* 54C12AF10C58E443A  
centrale

Identifiant carte \*

Valider Annuler

Afin de vérifier que la carte d'activation à bien été ajoutée à la centrale, celle-ci doit apparaître dans la dans la catégorie « module » en bas du formulaire de la centrale.



Enregistrer Annuler Activer un module Remplacer la centrale Plus + Nouveau Supprimer

**Nom \*** Controller 0001

**Identifiant** 54C12AF10C58E443A

**Nom du réseau** Network 0001 (IP - Distant)

**Modèle** IPEVIA 2L v2 (Centrale Wiegand v2 - 2 lecteurs)

**Option** Aucune

**Sociétés**

**Localisation**

**Activation des leds** ☒

**Désactiver la comm.** ☐

**Profils des lecteurs** Aucun

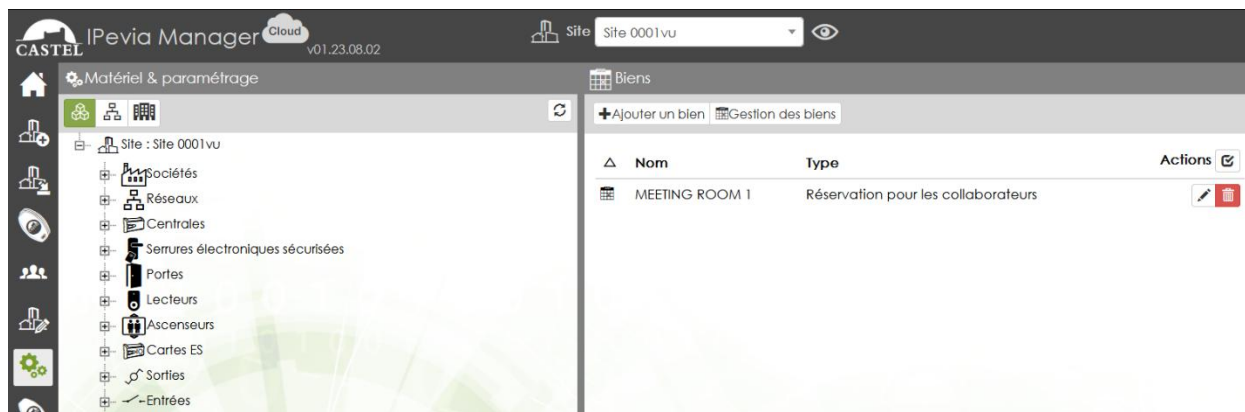
**Statut** ✕ Déconnecté

**Modules**  
Gestion de la réservation  
Identifiant : 5EC19F9B93CA72BF9B  
Intrusion - Système connecté  
Identifiant : 5EC1F1F9F9F1AA3F17F9

## 7.2 Ajouter un bien réservable

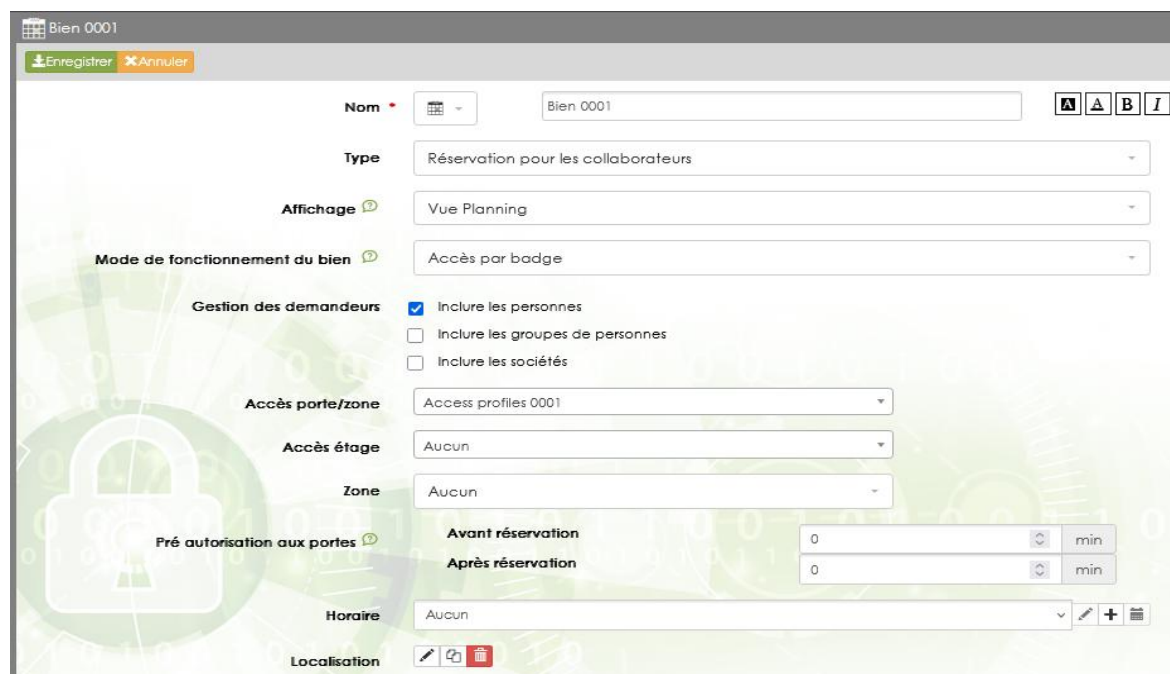
Depuis le menu “Matériels et paramétrages”, sélectionner “biens” dans l’arborescence de gauche.

Cliquer sur le bouton “ajouter un bien » en haut de la page.



## Paramétrage global

Plusieurs informations doivent être renseignées dans le champ des

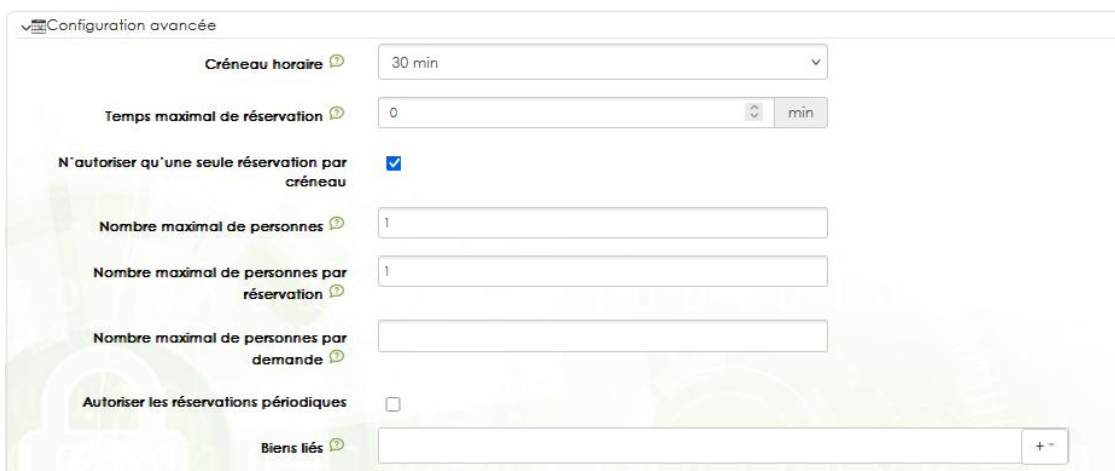


| Champ                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nom</b>                                | Renseigner le nom du bien (salle de réunion, aspirateur...)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Type</b>                               | <p>Le logiciel propose 3 différents types de réservations. Ils peuvent influencer la personne en capacité d'utiliser le bien réservé :</p> <ul style="list-style-type: none"> <li>- <b>Réservation pour les collaborateurs</b> : le gestionnaire de site ou les collaborateurs eux-mêmes, peuvent réserver le bien, pour des collaborateurs enregistrés sur le système de contrôle d'accès. Une fois que la réservation est validée, les usagers autorisés héritent des droits d'accès requis aux portes, étages... afin d'accéder au bien.</li> <li>- <b>Réservation parking pour visiteur</b> : ce mode permet au gestionnaire ou collaborateur de réserver une place de parking pour le visiteur.</li> <li>- <b>Réservation mixte</b> : offre une combinaison des deux configurations précédentes.</li> </ul>                                                                                                                                          |
| <b>Affichage</b>                          | Définissez si la réservation du bien est affichée dans une vue hebdomadaire ou dans une vue planning. Dans le deuxième cas, le bien sera affiché dans un aperçu de la planification de tous équipements du site.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Mode de fonctionnement du bien</b>     | <p>Définissez comment le profil d'accès à la porte autorisera ou non l'ouverture de la porte.</p> <ul style="list-style-type: none"> <li>- <b>Accès par badge</b> : la porte est fermée pendant la réservation, mais tous les utilisateurs autorisés héritent des droits d'accès à cette porte pendant la période réservée. Meilleure option pour les portes équipées de serrures magnétiques.</li> <li>- <b>Accès libre</b> : en fonction des paramètres de la porte sélectionnée (matériel et paramétrages/portes), elle reste déverrouillée pendant toute la période de réservation ou peut être ouverte avec un bouton-poussoir.</li> <li>- <b>Accès libre après badgeage organisateur</b> : si le planificateur accède à l'actif, la porte reste ouverte.</li> <li>- <b>Accès par badge après badgeage organisateur</b> : si le planificateur entre dans la porte de l'actif, les autres utilisateurs pourront y accéder avec leur badge.</li> </ul> |
| <b>Gestion des demandeurs</b>             | <p>Si le planificateur fait partie d'un groupe de personnes ou d'une société, alors il est possible de déléguer l'accès au bien réservé à toutes les personnes qui lui sont affiliées.</p> <p>Exemple : le planificateur travaille dans la société A, tous les employés de cette entreprise auront accès au bien pendant la réservation</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Accès porte/zone &amp; accès étage</b> | Le bien peut avoir un profil d'accès/d'étage spécifique. Ainsi l'utilisateur aura accès à ce profil d'accès pendant la réservation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Zone</b>                               | Si la porte donnant accès au bien est située dans une zone spécifique. Utile pour l'inclure dans du comptage ou de l'anti-pass back.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|                                    |                                                                                                                                |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Pré autorisation aux portes</b> | Délai pendant lequel l'organisateur (ou toute personne si réservation sans organisateur) peut entrer avant l'heure de la résa. |
| <b>Horaire</b>                     | Appliquer ou créer une profil horaire. Ainsi le bien sera réservable seulement pendant des intervalles de temps données.       |

## Paramétrage avancé

Vous pouvez appliquer des paramètres avancés à la réservation d'un bien :

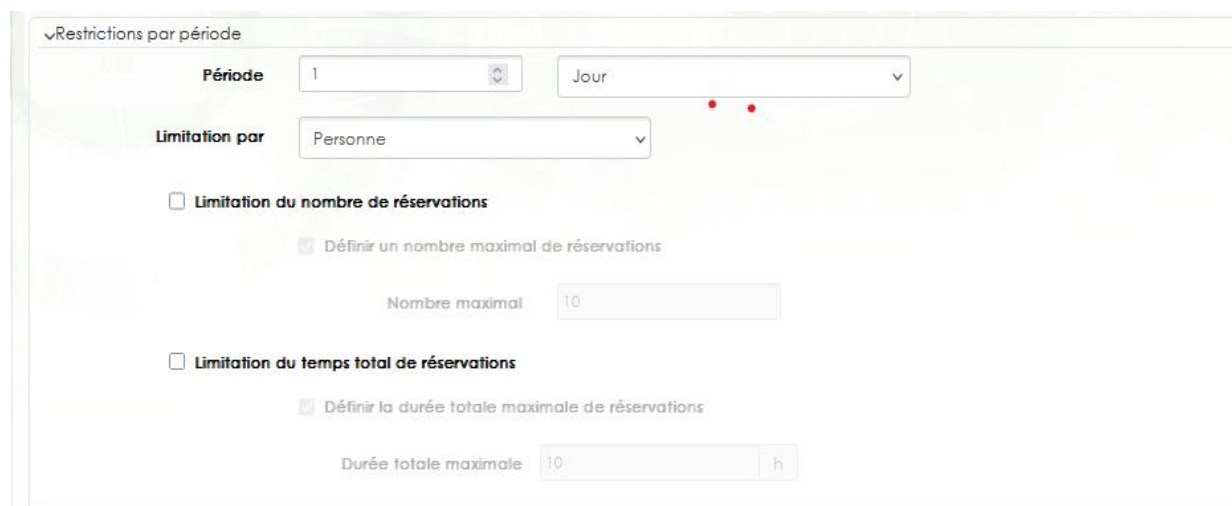


- **Créneau horaire** : c'est le temps minimum de réservation. Le temps de réservation est un multiple de ce critère. (Exemple : si le créneau horaire est défini sur 5 minutes, le temps total du créneau peut être de 5 minutes, 10 ou 15 minutes par exemple).
- **Temps maximal de réservation** : en minutes, c'est le temps maximum que l'équipement ou l'actif peut être réservé. Lorsque ce champ est à 0, il est illimité.
- **N'autoriser qu'une seule réservation par créneau** : la définition de "nombre maximal de personnes" et "nombre maximal de personnes par réservation" (paramètres suivants) peut autoriser plusieurs réservations simultanées (piscine, parking, etc.), mais cette possibilité peut être inhibée en cochant cette case, rendant ainsi la propriété exclusive. NB : cette limitation à une seule réservation par créneau est forcée si la "gestion des candidats" inclut des groupes ou des entreprises. Elle entraîne également l'annulation des paramètres suivants.
- **Nombre maximal de personnes** : il s'agit du nombre maximum de personnes autorisées pour une réservation. Le logiciel gère le nombre de personnes incluses pour la réservation, ainsi que la capacité maximale. Par exemple, si un espace de restauration accepte 30 personnes, il ne pourra pas accepter une réservation de 35 personnes. Mais deux personnes peuvent réserver cet espace si chacune de leurs groupes est composée de 15 personnes (si l'option précédente "autoriser une seule réservation par créneau" est décochée).
- **Nombre maximal de personnes par réservation** : Ipevia Manager peut restreindre le nombre de personnes par réservation. Cela empêche la privatisation de l'actif par un

seul organisateur. Si la capacité du bien est de 30 personnes, vous pouvez limiter à 10 personnes par réservation pour le rendre disponible pour plus d'une réservation.

- **Nombre maximal de personnes par demande** : le logiciel peut limiter le nombre maximum de candidats dans un créneau horaire. Cela empêche les tentatives de privatiser l'actif en dupliquant des candidatures.
- **Autoriser les réservations périodiques** : en cochant cette case, cela permet de réserver l'actif périodiquement. Par exemple, un employé peut réserver la salle chaque lundi de la semaine paire, chaque premier lundi du mois.
- **Biens liés** : pour des raisons organisationnelles et de conception des bâtiments, il est possible de lier plusieurs biens. Cela vise à faciliter la gestion de l'ensemble de l'installation. Exemple : si vous accédez à un gymnase par un hall, vous pouvez lier le hall et le gymnase. De même, par exemple, si des vestiaires sont à côté, réserver le gymnase réservera également les vestiaires.

## Restrictions par période



En plus d'être déterminé par des créneaux horaires, l'accès aux biens définis peut être limité par des périodes.

- **Période** : la période peut être définie en nombre de jour(s)/semaine(s)/mois ou année(s) : il vous faudra également préciser le premier jour calendaire (pour les semaines, définissez le premier jour pris en compte).
- **Limitation par** : choisissez si cette période s'applique à la personne, à la personne, au groupe ou à l'entreprise. Par exemple, vous pouvez définir une période pour la société A et non pour la société B.
- **Limitation du nombre de réservations et définition du nombre maximum de réservations** : pendant la période définie, vous pouvez limiter le nombre de réservations (max 1.000 réservations par période). C'est utile pour un court de tennis par exemple : les membres du club pourront le réserver deux fois par semaine.
- **Limitation de la durée totale des réservations et fixation de la durée totale maximale des réservations** : permet de limiter la durée de la réservation. Exemple : la quantité de cours de tennis réservés par les membres du club est de 4 heures.

## Personnes

 Personnes

Validation par un administrateur ? ☐

Responsable(s) ?

Utilisateurs ? 0 collaborateur(s)  

Ajouter d'autres personnes sur le portail ? ☐

- **Validation par un administrateur** : si coché, le logiciel enverra une demande au gestionnaire. Il peut accepter ou refuser la réservation. Si cette case n'est pas cochée, la réservation sera automatiquement acceptée.
- **Responsable(s)** : les personnes en charge de valider ou non les réservations.
- **Utilisateurs** : saisissez les personnes qui peuvent réserver l'actif.
- **Ajouter d'autres personnes sur le portail** : un candidat peut ajouter un utilisateur à sa réservation, même s'il n'est pas dans la liste des utilisateurs (voir le paramètre précédent).

## Envoi de mails

 Envoi de mail

Envoi des mails de gestion ? ☐

Pied de mail ?

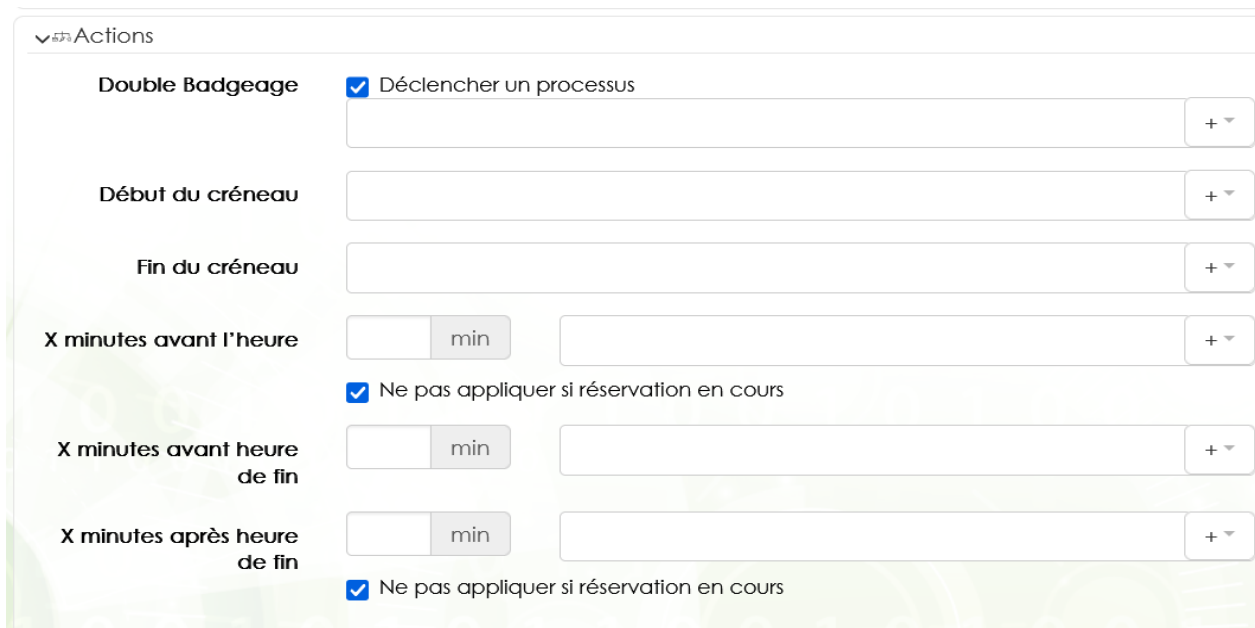
**Envoi d'e-mails de gestion** : il s'agit du paramètre pour l'envoi d'e-mails aux managers et aux candidats. Celui qui sera envoyé au gestionnaire pour l'acceptation ou le refus des réservations. Et l'email de validation/refus au demandeur.

Lorsque la case « envoi d'email de gestion » est cochée, le logiciel envoie automatiquement des e-mails aux résidents pour les informer de l'avancement de la réservation : demande complétée, demande approuvée ou refusée, etc.

**Pied de page de l'email :** vous pouvez personnaliser le pied de page des emails envoyés aux utilisateurs afin de renforcer la communication sur le bien réservé, de faciliter la compréhension du destinataire, etc... Pour ce faire, vous pouvez choisir parmi 4 sélections disponibles dans le champ 'pied de page de l'email' :

- **Aucun** : seules les informations relatives à la réservation seront affichées
- **Site** : les paramètres appliqués seront ceux définis dans « matériel et paramétrage », en voyant le site en haut de l'arborescence et l'onglet « paramètres e-mail ».
- **Société** : les paramètres seront ceux associés aux entreprises configurées dans le menu « Equipement et paramètres » et cliquez sur l'onglet « Paramètres e-mail » après avoir sélectionné une entreprise.
- **Personnalisé** : il ouvre un onglet d'édition dans cette fenêtre.

## Actions



Actions

Double Badgeage ☒ Déclencher un processus

Début du créneau

Fin du créneau

X minutes avant l'heure min

☒ Ne pas appliquer si réservation en cours

X minutes avant heure de fin min

X minutes après heure de fin min

☒ Ne pas appliquer si réservation en cours

Cet onglet "actions" permet de déclencher des processus paramétrés dans le menu « relations ». Ils peuvent être activés automatiquement à la fin/au début de la réservation, à un moment défini par rapport au créneau ou manuellement par badgeage.

**Double badgeage** : lorsqu'un hôte arrive la centrale peut déclencher un processus (activation de relais, par exemple) s'il présente deux fois ce badge. Ce processus doit avoir été créé précédemment (matériel et paramétrages>relations).

**Début du créneau** : au début du créneau, la centrale lance automatiquement un processus (activation de la lumière). Ce processus doit avoir été créé précédemment (matériel et paramétrages>relations).

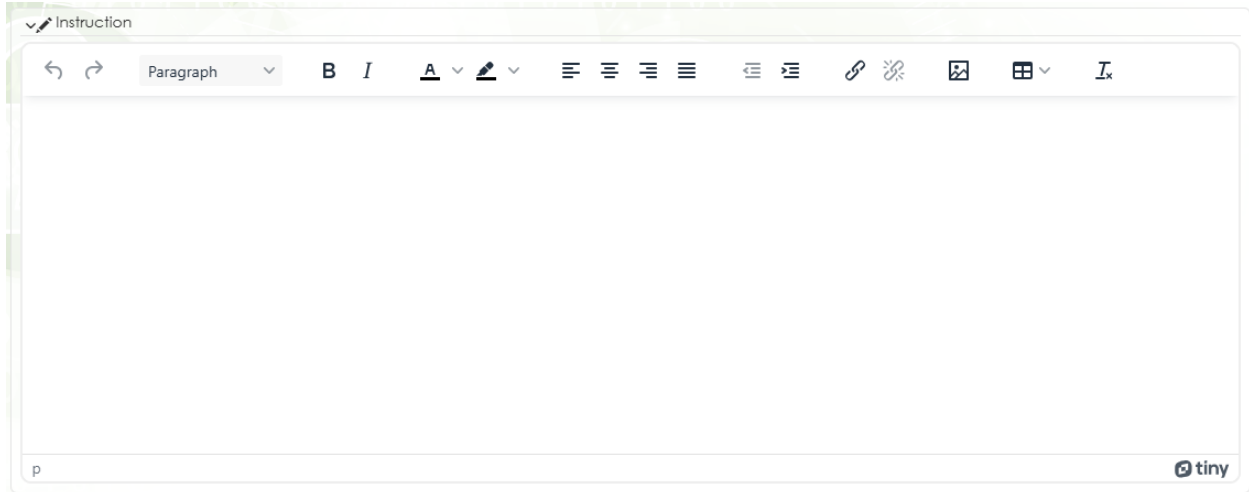
**Fin du créneau** : à la fin de la plage horaire, le contrôleur lance un processus (par exemple pour activer une alarme).

**X minutes avant l'heure** : en fonction de l'heure programmée la centrale démarre un processus (activation du relais de chauffage, par exemple). Ce processus doit avoir été créé précédemment. Si l'option « Ne pas appliquer si réservation en cours » est cochée, le processus ne sera pas déclenché si une autre réservation a lieu juste avant celle-ci.

**X minutes avant l'heure de fin** : en fonction de l'heure programmée, la centrale démarre un processus. Ce processus doit avoir été créé précédemment (matériel et paramétrages>relations).

**X minutes après l'heure de fin** : en fonction de l'heure programmée, la centrale démarre un processus qui doit avoir été créé au préalable. Si l'option « Ne pas appliquer si réservation en cours » est cochée, le processus ne sera pas déclenché si une autre réservation est effectuée juste après celle-ci.

## Instructions



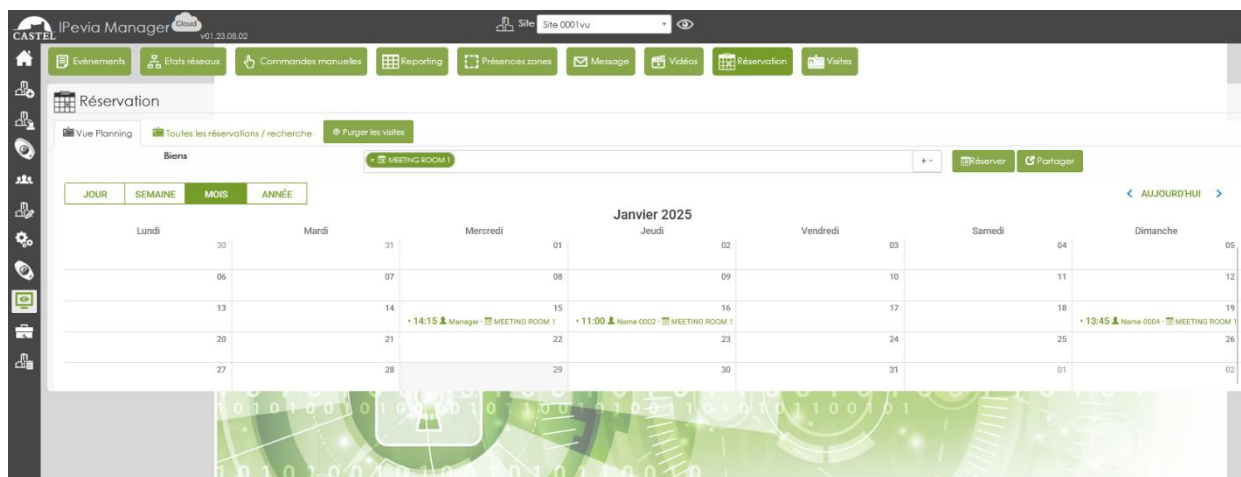
Ce champ libre sert à donner des instructions aux organisateurs. Par exemple:

- Pas de bruit, pas d'alcool
- Laisser la pièce propre
- La télécommande du vidéoprojecteur doit être rangée à un endroit précis

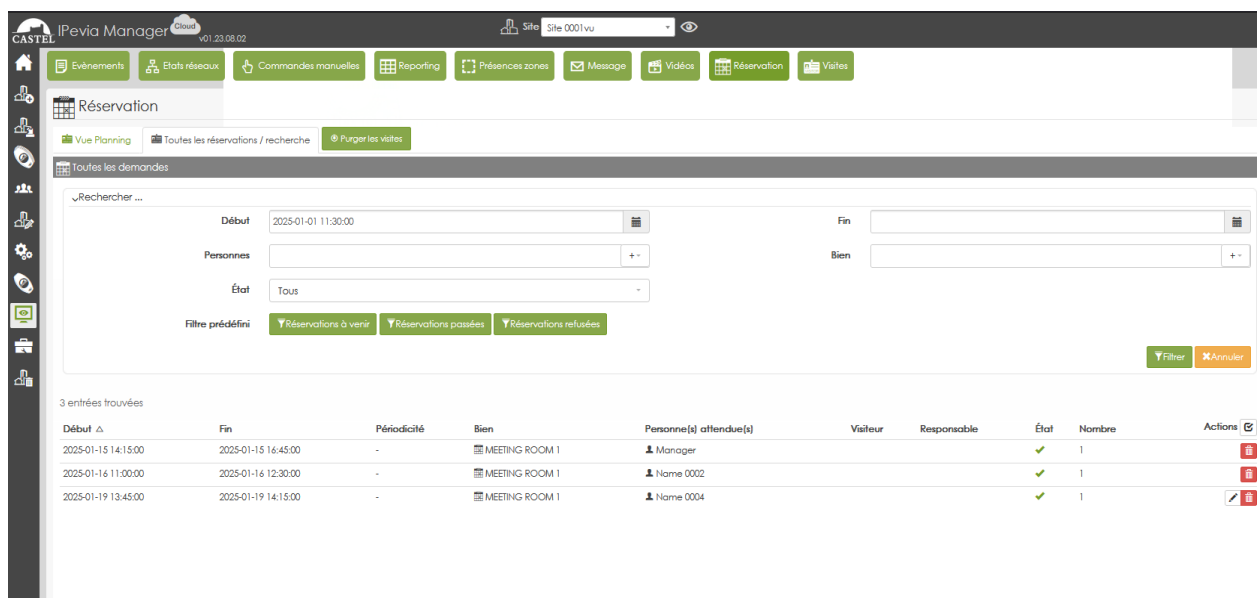
## 7.3 Gestion des réservations

Côté gestionnaire logiciel, via le menu 'Monitoring / Réservation », toutes les réservations apparaissent. Le type d'affichage peut être paramétré en « vue planning » ou en « toutes réservations/recherche ».

Ces deux présentations offrent les mêmes fonctions.

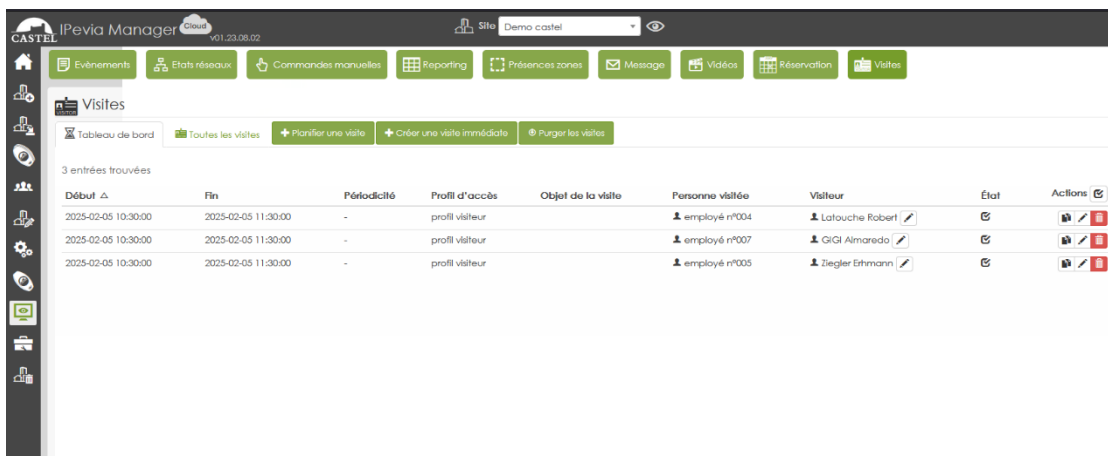


Vous pouvez créer une nouvelle réservation en cliquant sur le bouton « réserver » situé à droite de la liste des biens (vue planning).



## 8. Gestion des visiteurs

IPeVIA Manager dispose d'une interface de gestion des visiteurs. Les administrateurs du logiciel ou les collaborateurs eux-mêmes, planifient les visites. Les visiteurs saisis dans le logiciel héritent des droits d'accès aux portes et aux étages souhaités. La gestion des visiteurs doit avoir été préalablement activée dans les paramètres / fonctionnalités du site (voir chapitre 3.2).

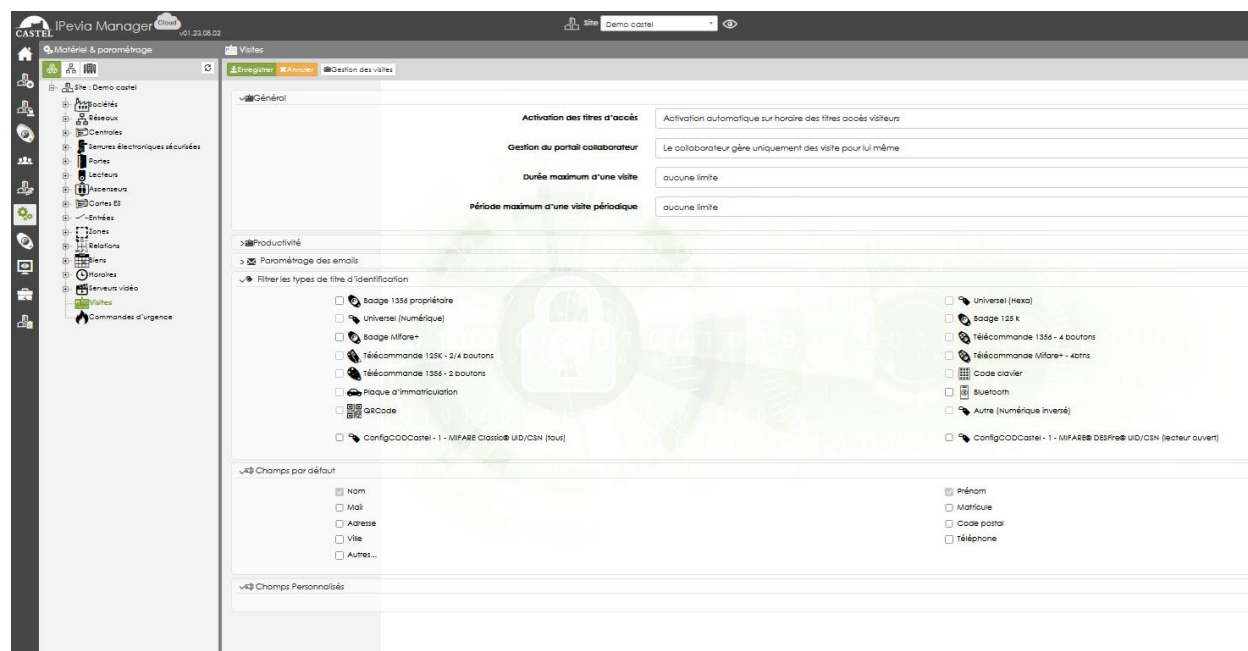


**8.1**

| Début               | Fin                 | Périodicité | Profil d'accès  | Objet de la visite | Personne visitée | Visiteur         | État | Actions |
|---------------------|---------------------|-------------|-----------------|--------------------|------------------|------------------|------|---------|
| 2025-02-05 10:30:00 | 2025-02-05 11:30:00 | -           | profil visiteur |                    | employé n°004    | Lalouché Robert  | ✓    |         |
| 2025-02-05 10:30:00 | 2025-02-05 11:30:00 | -           | profil visiteur |                    | employé n°007    | GIGI Almarado    | ✓    |         |
| 2025-02-05 10:30:00 | 2025-02-05 11:30:00 | -           | profil visiteur |                    | employé n°005    | Stegler Eithmann | ✓    |         |

### Paramétrage des visiteurs

Pour configurer les visites, cliquez sur l'icône « matériel et paramétrage » dans le cadre de gauche. Sélectionnez ensuite « visites » dans l'arborescence.



**Paramétrage des visites**

**Général**

Activation des titres d'accès: Activation automatique sur horaire des titres accès visiteurs

Gestion du portail collaborateur: Le collaborateur gère uniquement des visite pour lui-même

Durée maximum d'une visite: aucune limite

Période maximum d'une visite périodique: aucune limite

**Productivité**

Paramétrage des emails

Filter les types de titre d'identification

- ☐ Sadge 1356 propriétaire
- ☐ Universel (numérique)
- ☐ Sadge Milfire+
- ☐ Télécommande 125K - 2/4 boutons
- ☐ Télécommande 1356 - 2 boutons
- ☐ Plaque d'immatriation
- ☐ QRCode
- ☐ ConfigCODCastel - 1 - MIFARE Classic® UID/CSN [tous]
- ☐ Universel (Hexa)
- ☐ Sadge 125 K
- ☐ Télécommande 1356 - 4 boutons
- ☐ Télécommande Milfire+ - 4cans
- ☐ Code clavier
- ☐ Bluetooth
- ☐ Autre (numérique inversé)
- ☐ ConfigCODCastel - 1 - MIFARE® DESFire® UID/CSN (lecteur ouvert)

**Champs par défaut**

- ☒ Nom
- ☐ Mail
- ☐ Adresse
- ☐ Ville
- ☐ Autres...
- ☒ Prénom
- ☐ Matricule
- ☐ Code postal
- ☐ Téléphone

**Champs Personnalisés**

**Onglet "Général"**

 Général

|                                         |                                                                 |
|-----------------------------------------|-----------------------------------------------------------------|
| Activation des titres d'accès           | Activation automatique sur horaire des titres accès visiteurs ▼ |
| Gestion du portail collaborateur        | Le collaborateur peut ajouter d'autres visités ▼                |
| Durée maximum d'une visite              | aucune limite ▼                                                 |
| Période maximum d'une visite périodique | aucune limite ▼                                                 |

**Activation des titres d'accès** : les titres d'identification (badge, code, QR code, plaque d'immatriculation...) peuvent être actifs automatiquement ou manuellement.

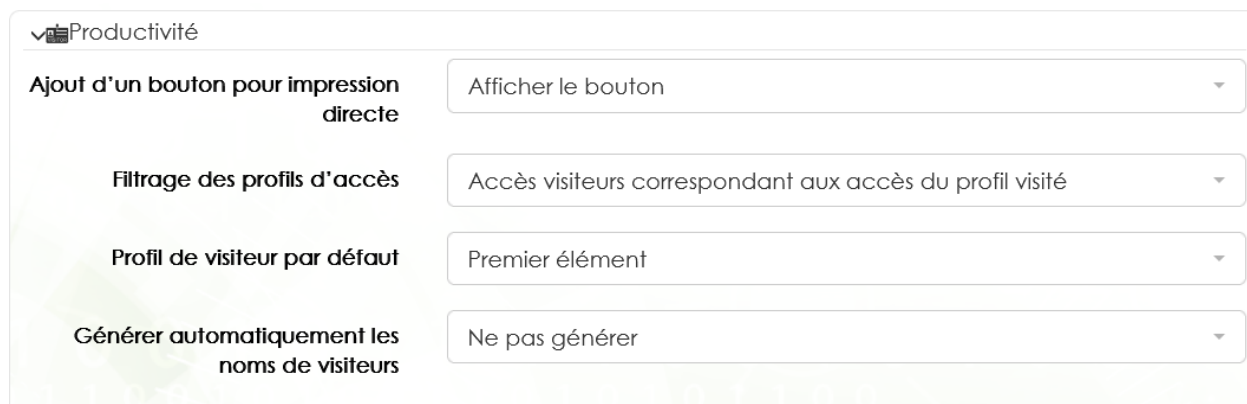
1. **Activation automatique sur horaire des titres accès visiteur** : le titre d'accès est valable pour les portes désignées et dans les heures de visite spécifiées automatiquement.
2. **Activation manuelle des titres accès et des visites (attente, en cours, finie)** : le titre d'identification devient valable lorsqu'un opérateur (par exemple, un réceptionniste) déclare le début et la fin de la visite dans le logiciel Ipévia Manager (monitoring>visites).

**Gestion du portail collaborateur** : via leurs comptes employés IPévia et sur la base des choix configurés par l'administrateur, les utilisateurs peuvent réserver des salles de réunion (voir chapitre 7.3.1.1) ou ajouter des visiteurs. Selon le choix dans ce champs, le résident peut soit uniquement être en mesure de planifier des visites pour lui-même, ou alors il peut être autorisé à ajouter des visiteurs pour d'autres résidents.

**Durée maximum d'une visite** : durée maximale d'une visite.

**Période maximale d'une visite périodique** : les utilisateurs peuvent créer une visite récurrente se produisant tous les jours/mois/semaines.... Vous pouvez choisir d'ajouter une période minimale entre deux visites périodiques. Par exemple 3 semaines, un mois, 3 mois ou 1 an.

### Onglet «*Productivité*»



✓ Productivité

Ajout d'un bouton pour impression directe : Afficher le bouton

Filtrage des profils d'accès : Accès visiteurs correspondant aux accès du profil visité

Profil de visiteur par défaut : Premier élément

Générer automatiquement les noms de visiteurs : Ne pas générer

**Ajouter un bouton pour impression directe** : dans l'aperçu de la visite, le réceptionniste peut accéder à un bouton qui imprime au visiteur son QR code d'accès.

**Filtrage des profils d'accès** : si l'option « Tous les accès visiteurs » est sélectionnée, lorsque la réceptionniste vérifie la visite en cours (monitoring/visites/toutes les visites), chaque visiteur créé apparaîtra dans le champ « visiteur ». Si l'autre option est sélectionnée, la réceptionniste ne verra que les visiteurs saisis pour les visites « en cours ».

**Profil visiteur par défaut** : si vous souhaitez que le droit d'accès du visiteur corresponde à celui de la personne visitée.

- Premier élément : le premier profil d'accès de la liste complète est sélectionné. Il peut être pratique de nommer un profil d'accès visiteur dont le nom commence par un A. Avec cette option, le logiciel choisira automatiquement ce profil d'accès. C'est utile si tous les visiteurs suivent le même chemin ou ont besoin de la même porte d'accès.
- Profil visiteur identique à celui de la personne visitée : le visiteur héritera du même droit d'accès que la personne à laquelle il rend.
- Profil visiteur lié au profil visité : ouvre un nouveau champ personnalisable lors de la création d'une visite pour lier un profil visiteur spécifique à la personne visitée.

**Générer automatiquement des noms de visiteurs** : le logiciel peut nommer les visiteurs par lui-même (exemple « visiteur de [nom de la personne visitée] »).

### Onglet «*paramétrage des emails*»

Vous permet d'appliquer un thème défini. Trois options s'offrent à vous :

- **Aucun** : aucun pied de page n'apparaîtra sur l'email au visiteur
- **Site** : le pied de page sera le même que celui défini dans les paramètres de messagerie du site (Matériel et paramètres/sélectionner le site en haut de l'arborescence/onglet paramétrage des emails)
- **Société** : le pied de page sera le même que celui défini dans les paramètres de messagerie de l'entreprise (matériel et paramétrage/sociétés/paramétrage des emails)

***enable/disable the credential types (prox, fingerprint, etc...) tab***

Cet onglet vous permet de choisir le type d'identifiant qui peut être utilisé pour les visiteurs. Il peut s'agir d'un identifiant tangible (badge, plaque, qr code...) ou virtuel (accès bluetooth, code d'accès...)

***Onglet « champs par défaut »***

Les champs cochés dans la liste apparaîtront sur le formulaire du visiteur pour créer une nouvelle visite.

***Onglet « champs personnalisés »***

Le formulaire d'inscription des visiteurs peut être personnalisé avec l'ajout de champs personnalisés. Pour ce faire, ajoutez d'abord un champ personnalisé.

Cliquez sur le menu « outils »  dans le cadre de gauche et sélectionnez « personnaliser ».

Créez le champ personnalisé requis. Puis dans le menu « matériel et paramètres » , sélectionnez « visites » dans l'arborescence et cochez le champ à ajouter au formulaire en bas de la fenêtre, en dessous de l'onglet « champs personnalisés ». Par exemple, cela a créé le champ nommé « output ».

Une fois le champ personnalisé créé, vous le trouverez sous l'onglet « champs personnalisés ». Cochez la case liée pour qu'elle apparaisse sur le formulaire d'inscription du visiteur.

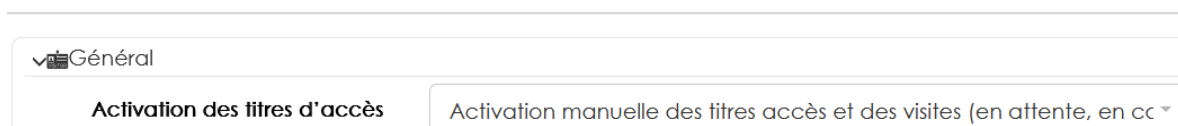


## 8.2. Gestion des accès visiteurs

En ce qui concerne les paramètres configurés dans le menu « Matériel et paramétrage » / « Visites », les identifiants s'activent et se désactivent automatiquement avec une action de l'opérateur.

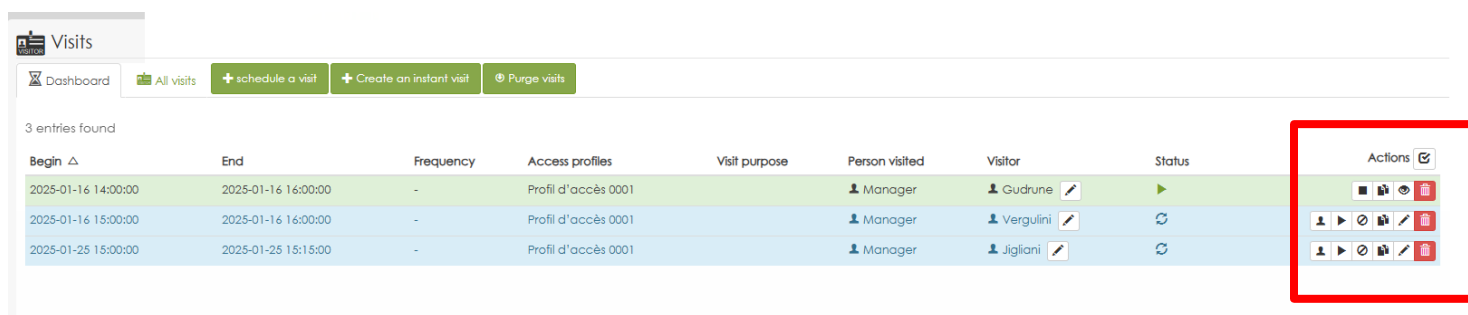
### Activation manuelle des visites

Lorsque l'activation des identifiants d'accès est réglée sur manuelle dans le menu « Matériel et paramétrage » / « Visites » (voir ci-dessous), les titres d'identification ne fonctionnent qu'après l'intervention de l'opérateur.

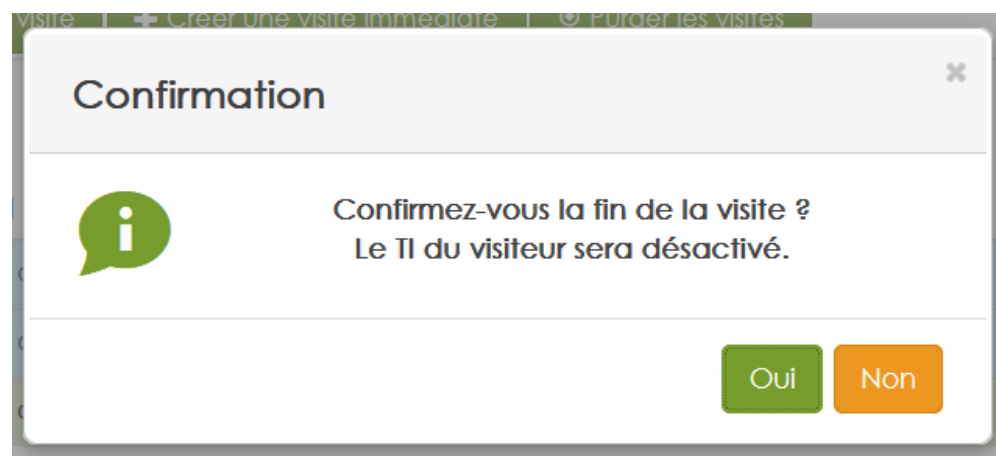


Le début de la visite et donc l'activation du badge ou du code se fait dans la fenêtre Monitoring / Visites / Tableau de bord en cliquant sur le triangle « Play ».

La fin de la visite et donc la désactivation des cartes d'accès se fait dans la fenêtre monitoring / Visites / Tableau de bord en cliquant sur le carré « Fin » comme indiqué ci-dessous.

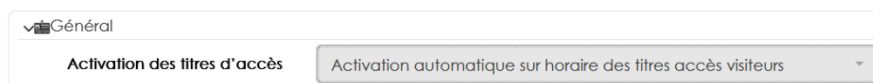


En cas de démarrage ou d'arrêt de la visite, le logiciel affiche une fenêtre de confirmation :



### ***Activation automatique des visites***

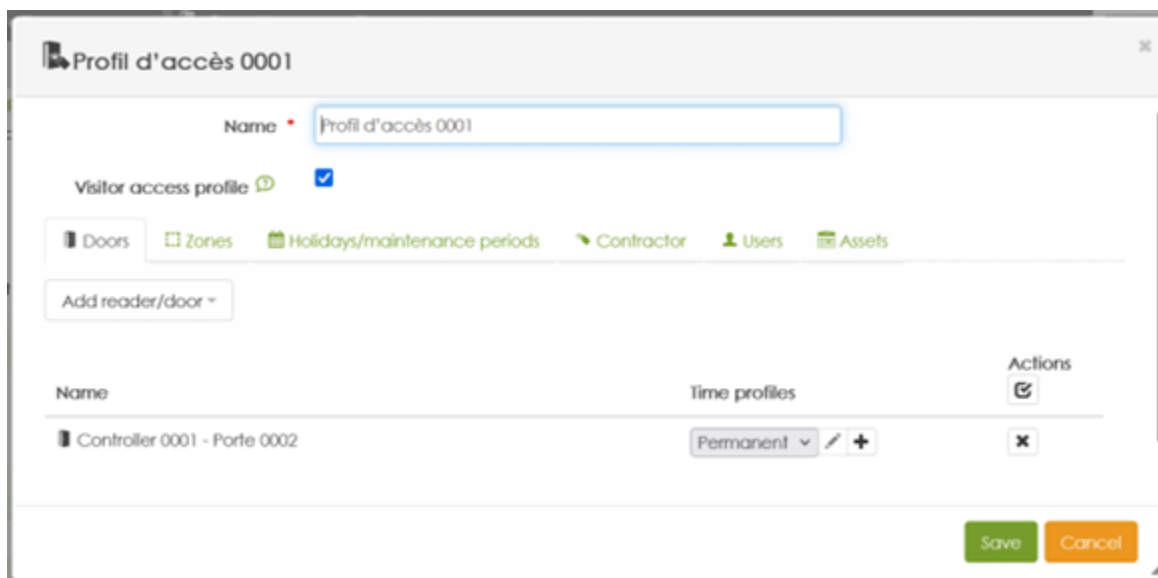
Lorsque l'option d'activation des identifiants est réglée sur « automatique » dans « matériel et paramétrages » / « Visites », les badges et les codes d'accès sont automatiquement valides à la date et à l'heure de la visite.



The screenshot shows a software interface with a tab labeled 'Général' (General) and a dropdown menu titled 'Activation des titres d'accès' (Activation of access titles). The dropdown menu is open, showing the option 'Activation automatique sur horaire des titres accès visiteurs' (Automatic activation on visitor access title schedule).

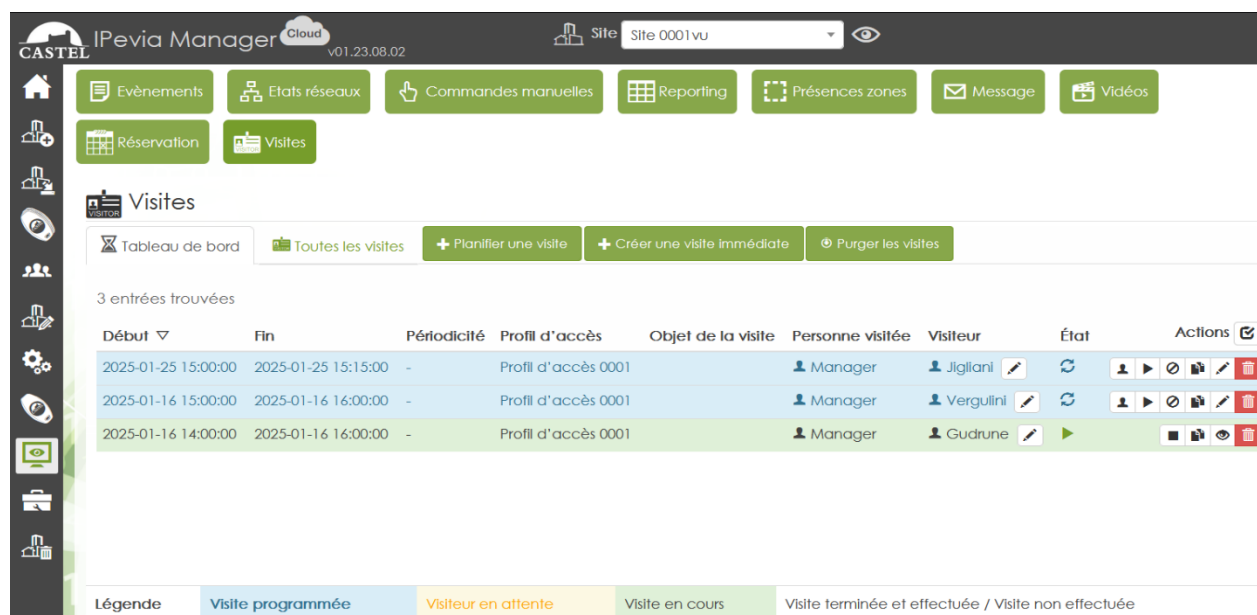
## 8.2 Créer un profil visiteur

Les profils d'accès aux portes et aux étages pris en compte dans le logiciel ne sont pas automatiquement utilisables pour l'accès des visiteurs. Pour qu'ils puissent être sélectionnés lors de la création d'une visite, la case « Profil du visiteur » doit être cochée. Voir la section 4 « Utilisateurs et profils d'accès ».



## 8.4. Ajouter une visite

Pour accéder aux visites en cours ou en créer de nouvelles, cliquez sur «Monitoring» puis «Visite ». La fenêtre suivante apparaîtra :



| Début               | Fin                 | Périodicité | Profil d'accès      | Objet de la visite | Personne visitée | Visiteur  | État | Actions |
|---------------------|---------------------|-------------|---------------------|--------------------|------------------|-----------|------|---------|
| 2025-01-25 15:00:00 | 2025-01-25 15:15:00 | -           | Profil d'accès 0001 |                    | Manager          | Jigliani  |      |         |
| 2025-01-16 15:00:00 | 2025-01-16 16:00:00 | -           | Profil d'accès 0001 |                    | Manager          | Vergulini |      |         |
| 2025-01-16 14:00:00 | 2025-01-16 16:00:00 | -           | Profil d'accès 0001 |                    | Manager          | Gudrone   |      |         |

Légende

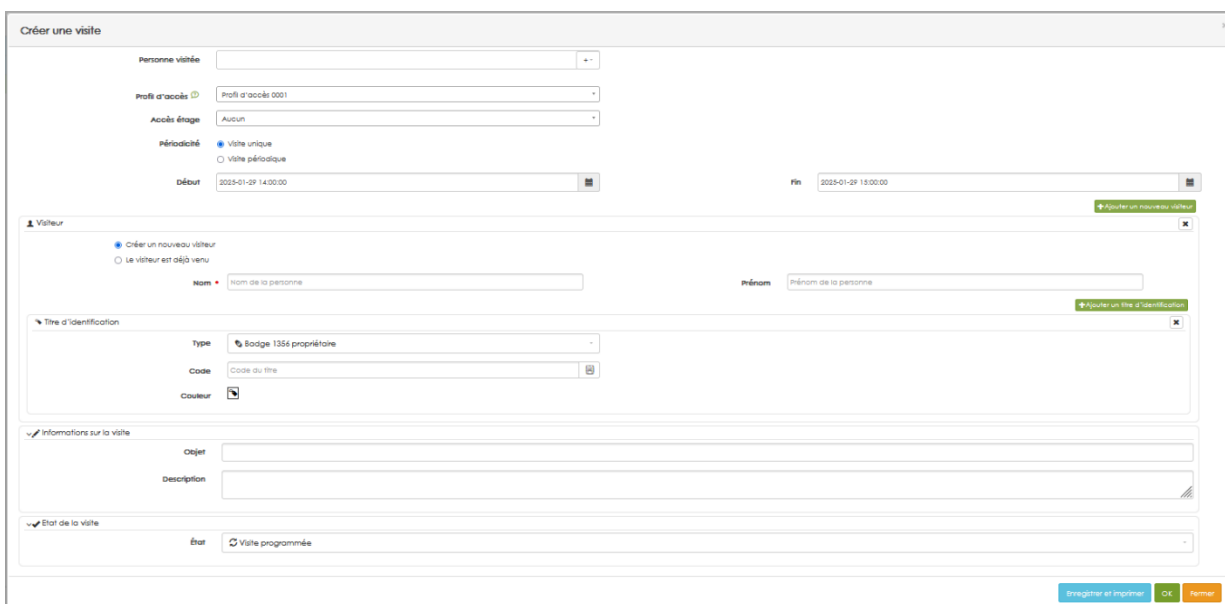
- Visite programmée
- Visiteur en attente
- Visite en cours
- Visite terminée et effectuée / Visite non effectuée

Sous le titre « Visite », il y a deux onglets :

- **Tableau de bord** : seules les visites en cours ou à venir sont affichées (voir capture d'écran ci-dessus).
- **Toutes les visites** : permet d'appliquer des filtres parmi toutes les visites enregistrées (passées, présentes et futures) et de les afficher en fonction de critères spécifiques.

## Planifier une visite

Le logiciel IPEvia vous permet de planifier une visite à l'avance. Dans la fenêtre suivante, entrez le nom de la ou des personnes visitées. Sélectionnez le profil d'accès du visiteur. Seuls les profils sélectionnables pour les visiteurs seront proposés ici.



Rappel : pour rendre sélectionnable un profil d'accès, cochez la case « profil visiteur » dans le formulaire de profil d'accès.

Périodicité ☐ Visite unique ☒ Visite périodique

Périodicité - semaine

Jours ☐ Lundi ☐ Mardi ☐ Mercredi ☐ Jeudi ☐ Vendredi ☐ Samedi ☐ Dimanche

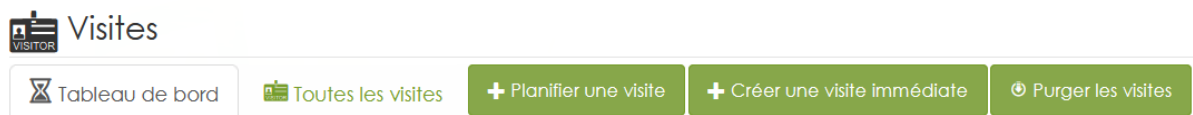
Heure  à

Début  Fin

Entrez la fréquence de la visite : elle peut être ponctuelle ou périodique avec des dates de début et de fin. La capture d'écran ci-dessous montre un exemple de visite périodique.

## Créer une visite instantanée

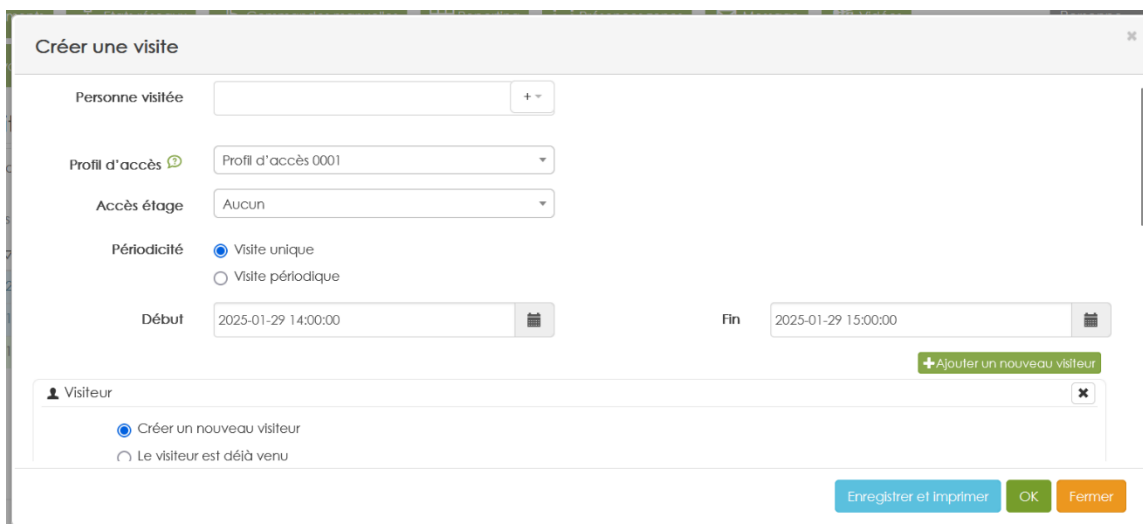
En haut du menu de visite, cliquez sur le bouton « créer une visite immédiate ». Cette option est une version simplifiée de la planification des visites, car elle propose le début de la visite pour



l'heure actuelle.

Ensuite, cette fenêtre s'affiche :

Vous pouvez répéter cette visite. En cliquant sur la case à cocher « visite récurrente », le logiciel



affichera d'autres options, telles que les jours et les heures pour répéter cette visite.

Entrez les informations requises et cliquez sur « OK ».

## 9. Utilisation avancée du logiciel

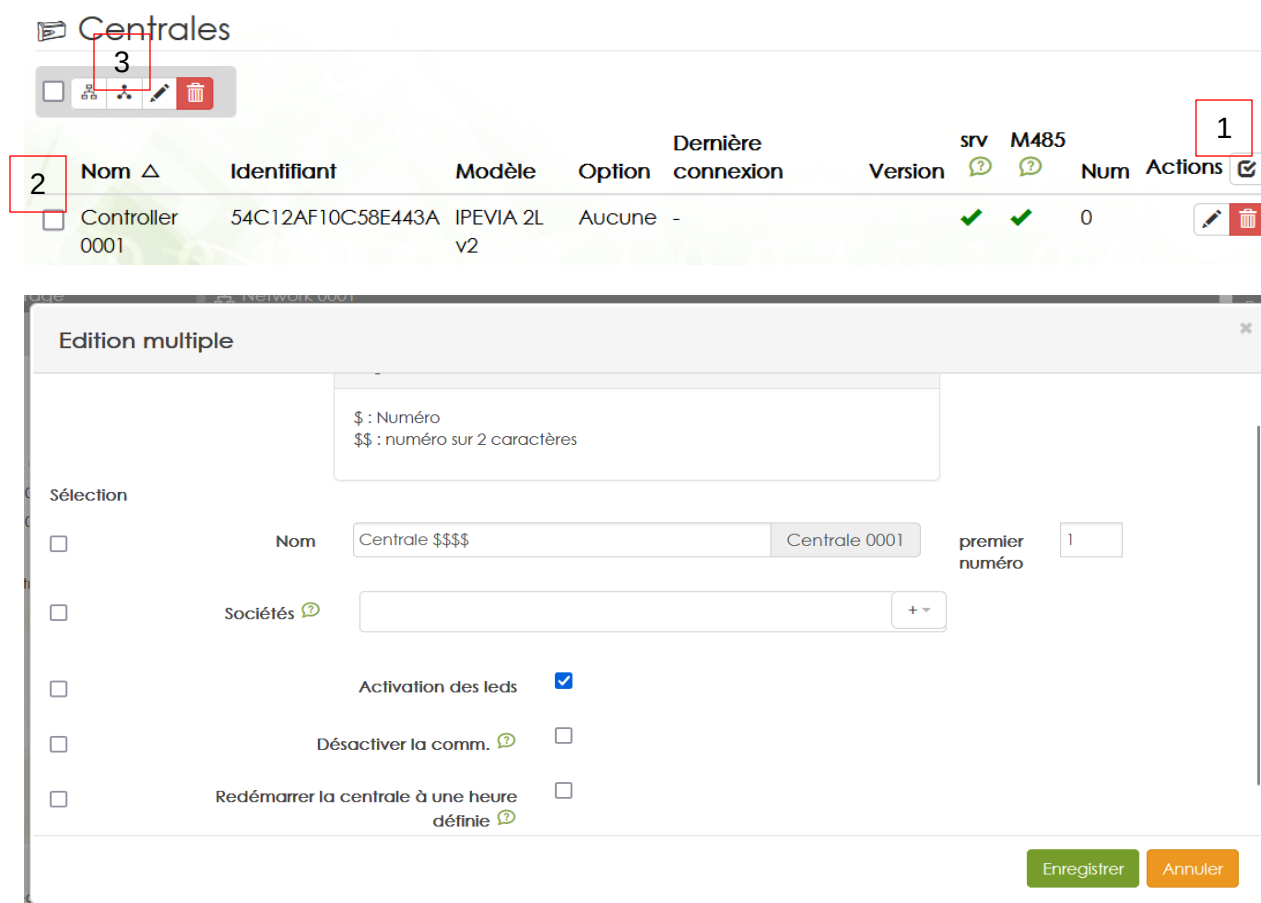
### 9.1 Outil de modification automatique

Différents outils de renommage et/ou de configuration ont été développés afin de simplifier le travail de l'installateur/l'utilisateur. Ces outils sont utilisés sur les panneaux de commande, les entrées, les sorties, les portes et permettent d'appliquer la même modification à plusieurs éléments en une seule opération.

Par exemple, ces outils peuvent être utilisés pour renommer plusieurs sorties en « Sortie 1, Sortie 2, etc. » avec un incrément. Également afin de configurer des résistances de fin de ligne pour les entrées d'impédance en une seule opération.

#### Modification des informations de la centrale

Dans la vue « Réseau » ou « Centrale », cliquez sur le bouton « Actions » (1) à droite, puis cochez les appareils que vous souhaitez modifier dans la première colonne (2). Enfin, cliquez sur le bouton « Réseau » (3).

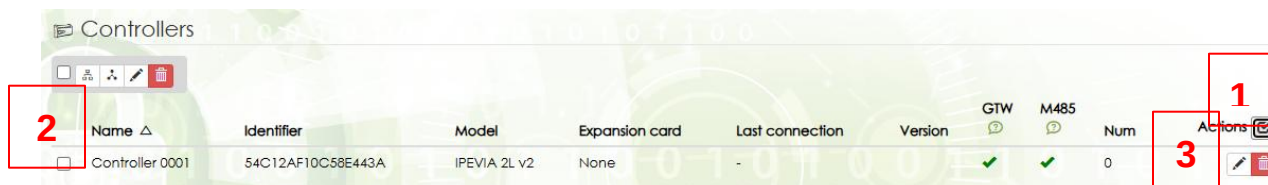


The screenshot shows the 'Centrales' view in the IPEVIA Manager software. At the top, there is a toolbar with icons for selection, addition, modification, and deletion. A red box labeled '3' highlights the 'Actions' button. Below the toolbar is a table of central units. A red box labeled '2' highlights the first column, which contains checkboxes for selecting units. The table has columns for 'Nom', 'Identifiant', 'Modèle', 'Option', 'Dernière connexion', 'Version', 'srv', 'M485', 'Num', and 'Actions'. A red box labeled '1' highlights the 'Actions' column. Below the table, a dialog box titled 'Edition multiple' is open, showing fields for 'Nom', 'Sociétés', 'Activation des leds', 'Désactiver la comm.', and 'Redémarrer la centrale à une heure définie'. The 'Nom' field is set to 'Centrale \$\$\$\$' and 'Centrale 0001'. The 'Sociétés' field is empty. The 'Activation des leds' checkbox is checked. The 'Désactiver la comm.' and 'Redémarrer la centrale à une heure définie' checkboxes are unchecked. The 'premier numéro' field is set to '1'. At the bottom of the dialog box are 'Enregistrer' and 'Annuler' buttons.

|                          | Nom ▲           | Identifiant       | Modèle       | Option | Dernière connexion | Version | srv | M485 | Num | Actions |
|--------------------------|-----------------|-------------------|--------------|--------|--------------------|---------|-----|------|-----|---------|
| <input type="checkbox"/> | Controller 0001 | 54C12AF10C58E443A | IPEVIA 2L v2 | Aucune | -                  |         | ✓   | ✓    | 0   |         |

## Modification de l'adresse IP de la centrale

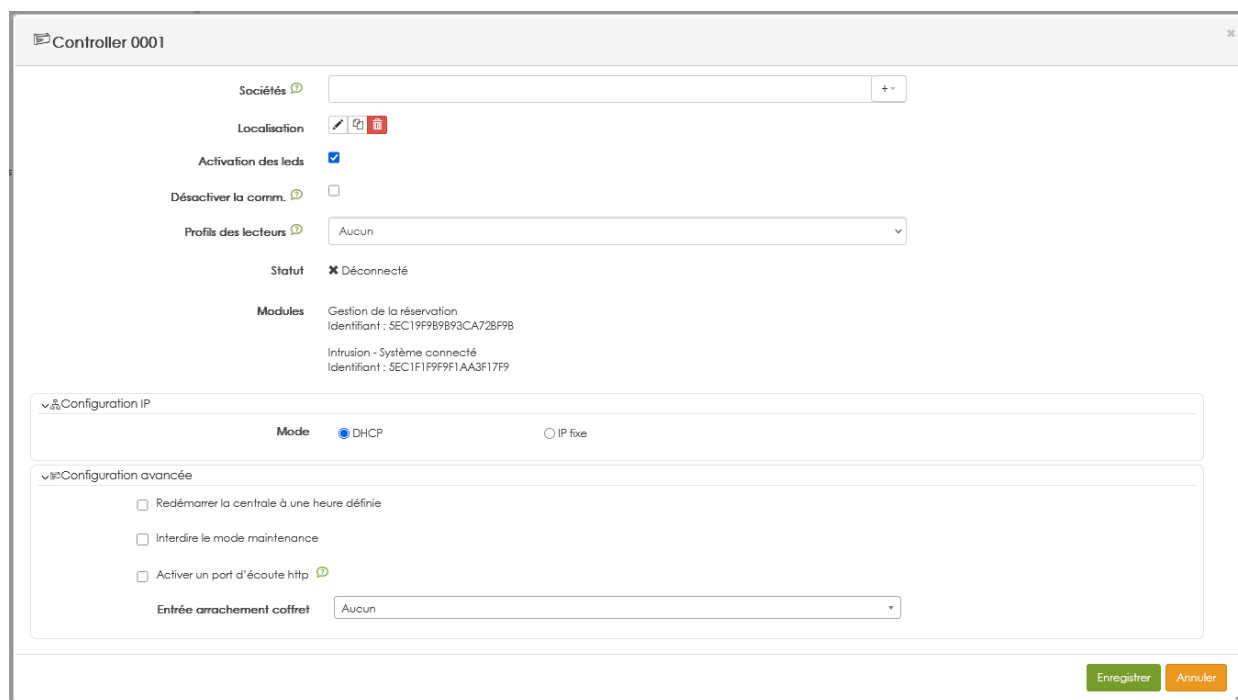
Dans la vue « Réseau » ou « Panneaux de configuration », cliquez sur le bouton « Actions » (1) à droite, puis cochez les panneaux de configuration que vous souhaitez modifier dans la première colonne (2). Enfin, cliquez sur le bouton « crayon » (3) à droite de la manette.



| 2 | Name △          | Identifier        | Model        | Expansion card | Last connection | Version | GTW | M485 | Num | 1<br>3 Actions |
|---|-----------------|-------------------|--------------|----------------|-----------------|---------|-----|------|-----|----------------|
|   | Controller 0001 | 54C12AF10C58E443A | IPEVIA 2L v2 | None           | -               |         | ✓   | ✓    | 0   |                |

Le logiciel affiche la fenêtre suivante :

Cochez la case « IP statique ». Entrez ensuite les informations souhaitées dans les champs. Dans cet exemple, le premier contrôleur sélectionné dans la liste se verra attribuer l'adresse IP 255.255.255.0 et le deuxième contrôleur recevra 255.255.255.1.



Controller 0001

Sociétés

Localisation

Activation des leds

Désactiver la comm.

Profil des lecteurs

Statut

Modules

Configuration IP

Mode

Configuration avancée

Entrée arrachement coffret

Enregistrer

Annuler

## Modifications de l'entrée

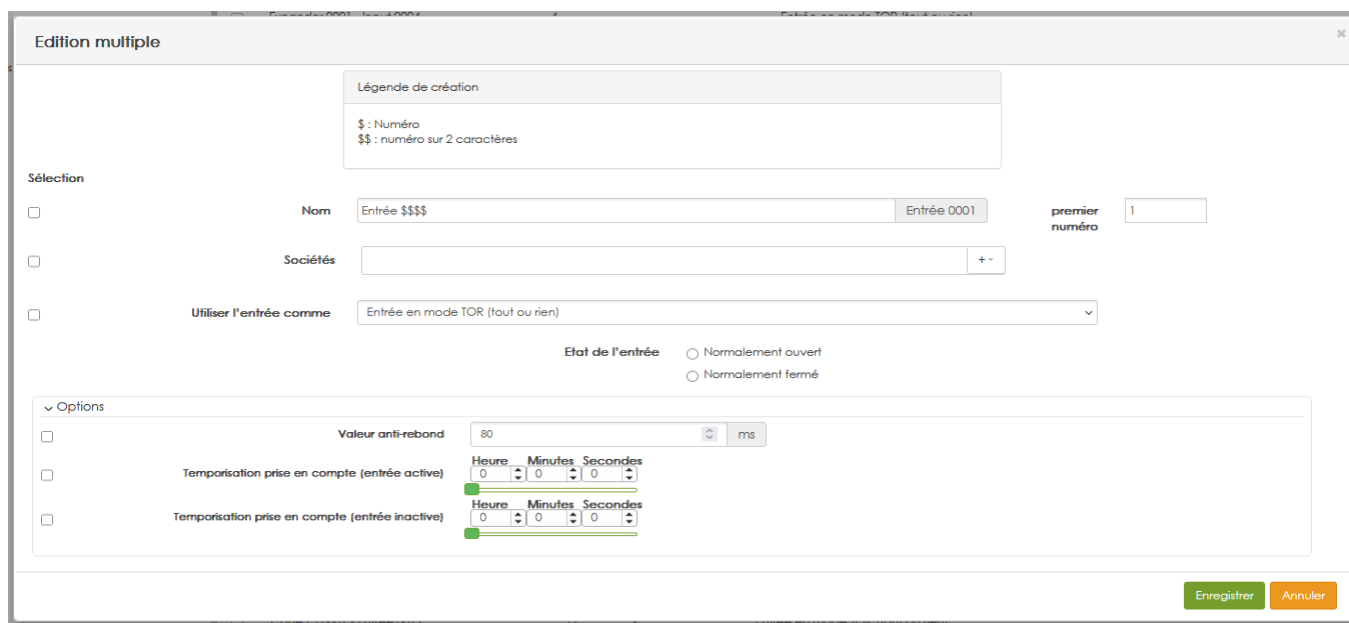
Depuis le menu « matériel et paramètres » puis « entrées », cliquez sur Action (1), puis sélectionnez les entrées à modifier (2), et cliquez sur l'icône du crayon (3). Les cases à cocher situées à gauche du champ vous permettent de modifier uniquement certains champs.



|                          | Nom                        | Num | Utilisé par    | Type                              | Localisation | Actions |
|--------------------------|----------------------------|-----|----------------|-----------------------------------|--------------|---------|
| <input type="checkbox"/> | Expander 0001 - Input 0001 | 1   | Condition 0001 | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0002 | 2   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0003 | 3   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0004 | 4   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0005 | 5   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0006 | 6   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0007 | 7   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0008 | 8   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0009 | 9   | -              | Entrée en mode TOR (tout ou rien) |              |         |
| <input type="checkbox"/> | Expander 0001 - Input 0010 | 10  | -              | Entrée en mode TOR (tout ou rien) |              |         |

La fenêtre suivante s'affiche : pour toutes les entrées sélectionnées, il est possible de modifier le nom en gérant un incrément automatique et de choisir le type d'entrée comme « normalement ouvert » (NO) ou « Normalement fermé ». Exemple pour un interrupteur :

1. En mode NO, l'interrupteur ne conduira pas l'électricité tant qu'il n'est pas activé,
2. En mode NC, l'interrupteur conduira l'électricité jusqu'à ce qu'il soit enfoncé.



**Edition multiple**

Légende de création  
 \$ : Numéro  
 \$\$ : numéro sur 2 caractères

Sélection

☐ Nom Entrée \$\$\$\$ Entrée 0001 premier numéro 1

☐ Sociétés

☐ Utiliser l'entrée comme Entrée en mode TOR (tout ou rien)

Etat de l'entrée  
☐ Normalement ouvert  
☐ Normalement fermé

Options

☐ Valeur anti-rebond 80 ms

☐ Temporisation prise en compte (entrée active)  
 Heure Minutes Secondes  
 0 0 0

☐ Temporisation prise en compte (entrée inactive)  
 Heure Minutes Secondes  
 0 0 0

Enregistrer Annuler

Plusieurs choix sont possible pour le champs « utiliser l'entrée comme ». Ils influencent également les champ apparaissant en bas de la fenêtre (onglet options »

- **Entrée en mode TOR (tout ou rien)** : le signal ne peut avoir que deux états possibles, tels que ON/OFF ou OPEN/CLOSED, ou 0/1. Il existe des paramètres pour empêcher le rebond (voir les informations ci-dessous)

**Valeur anti-rebond (en ms)** : ce réglage est particulièrement utile pour les boutons-poussoirs. Même s'ils sont simples à utiliser, ils sont parfois sujets au rebond : ils ne passent pas directement de l'ouverture à la fermeture. Pendant une très courte période (millisecondes), il basculera plusieurs fois entre ouvert et fermé. Ainsi, le contrôleur comprendra chaque changement d'état comme une pression sur un bouton.

Pour éviter ce phénomène, vous pouvez définir une valeur (en ms), afin que le contrôleur ne prenne pas en compte le changement d'état du bouton-poussoir. Cette valeur doit être suffisamment élevée pour empêcher le contrôleur de comprendre une sollicitation comme deux mais il doit être suffisamment bas pour comprendre deux actions si nécessaire.

**Temps d'activation et de désactivation** : vous pouvez choisir d'appliquer cet anti-rebond uniquement après un certain temps. Alors que les données précédentes sont saisies en millisecondes, vous pouvez choisir d'appliquer un anti-rebond après des heures, des minutes ou des secondes.

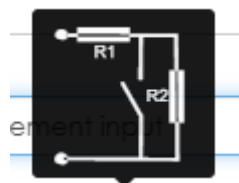
- **Entrée impédant (ou EOL resistance input)**: une résistance de fin de ligne (EOLR) permet de surveiller le câblage en détectant les circuits ouverts ou les courts-circuits. Il permet au contrôleur d'identifier quatre états en fonction des résistances ( $\Omega$ ) et de l'interrupteur. Si les résistances dépassent une valeur définie, le contrôleur détecte l'entrée et peut déclencher une relation par exemple.

End of line resistor1 ⓘ

Default (4.7 k $\Omega$ )

End of line resistor2 ⓘ

Default (10 k $\Omega$ )



Entrez les valeurs de résistance de ligne pour R1 et R2. En fonction de la résistance de courant ( $\Omega$ ) et de l'interrupteur, vous pouvez créer quatre conditions :

**Court-circuit** : l'interrupteur est fermé et le circuit contourne les deux résistances car  $\Omega >$  à R1 et R2.

**Veille (ou non détection) :** l'interrupteur est fermé et  $\Omega$  n'est que  $\geq$  à la valeur R1.

**Actif (ou détection) :** l'interrupteur est fermé et  $\Omega >$  à R1 & R2.

**Circuit ouvert (ou débranché) :** lorsque le circuit est ouvert et que le courant électrique ne dépasse pas les valeurs R1 ou R2.

Avec les paramètres ci-dessus, vous pouvez par exemple, définir que le contrôleur détectera un court-circuit, uniquement s'il s'est produit x secondes après le premier (valeur antirebond). Si deux courts-circuits se produisent en moins de temps que ce réglage, le contrôleur ne détectera qu'un seul court-circuit.

|                                              |                                                                                                                |          |       |         |          |   |   |   |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------|----------|-------|---------|----------|---|---|---|
| Valeur anti-rebond                           | 80                                                                                                             | ms       |       |         |          |   |   |   |
| Temporisation « Court-circuit »              | <table><tr><td>Heure</td><td>Minutes</td><td>Secondes</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table> |          | Heure | Minutes | Secondes | 0 | 0 | 0 |
| Heure                                        | Minutes                                                                                                        | Secondes |       |         |          |   |   |   |
| 0                                            | 0                                                                                                              | 0        |       |         |          |   |   |   |
| Temporisation « Pas de détection »           | <table><tr><td>Heure</td><td>Minutes</td><td>Secondes</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table> |          | Heure | Minutes | Secondes | 0 | 0 | 0 |
| Heure                                        | Minutes                                                                                                        | Secondes |       |         |          |   |   |   |
| 0                                            | 0                                                                                                              | 0        |       |         |          |   |   |   |
| Temporisation « Détection »                  | <table><tr><td>Heure</td><td>Minutes</td><td>Secondes</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table> |          | Heure | Minutes | Secondes | 0 | 0 | 0 |
| Heure                                        | Minutes                                                                                                        | Secondes |       |         |          |   |   |   |
| 0                                            | 0                                                                                                              | 0        |       |         |          |   |   |   |
| Temporisation « Débranché »                  | <table><tr><td>Heure</td><td>Minutes</td><td>Secondes</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table> |          | Heure | Minutes | Secondes | 0 | 0 | 0 |
| Heure                                        | Minutes                                                                                                        | Secondes |       |         |          |   |   |   |
| 0                                            | 0                                                                                                              | 0        |       |         |          |   |   |   |
| Différentiel validant le changement de seuil | 0                                                                                                              |          |       |         |          |   |   |   |

Vous pouvez utiliser la barre coulissante pour définir lorsque la centrale détectera un court-circuit uniquement s'il dure plus de X secondes, X minutes ou X heures.

Le champ « différentiel validant le déplacement du seuil » doit être saisi lorsque d'autres valeurs sont de 4,7 kΩ et 10 kΩ.

- **Entrée décimale** : le contrôleur attribue une valeur au signal qu'il reçoit (comprise entre 0 et 4095). Cette fonction offre la possibilité de gérer 3 seuils dont leur valeur est comprise entre 0 et 4095. En fonction du signal, de sa valeur décimale, et surtout des 3 seuils, le contrôleur peut détecter 4 états différents. Il est utile de gérer le réflexe de porte par exemple

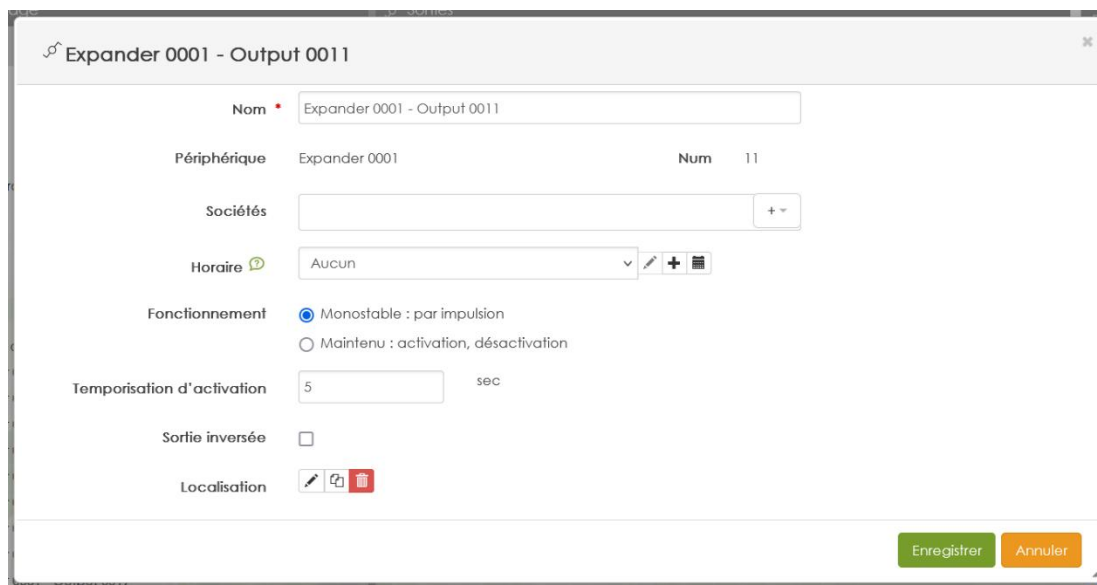
Notez que la valeur du seuil 1 < la valeur du seuil 2 < la valeur du seuil 3.

Pour simplifier, l'entrée décimale est similaire à celle de type EOL. Cependant, au lieu d'utiliser les trois valeurs prédéfinies, en définir des personnalisées. Les valeurs analogiques mesurées en entrée par la centrale seront converties en une valeur numérique comprise entre 0 et 4095.

Comme pour les autres types d'entrée, vous pouvez définir des paramètres antirebonds, pour empêcher le contrôleur d'interpréter et de prendre en compte les perturbations de changement d'état

## Modifications de la sortie

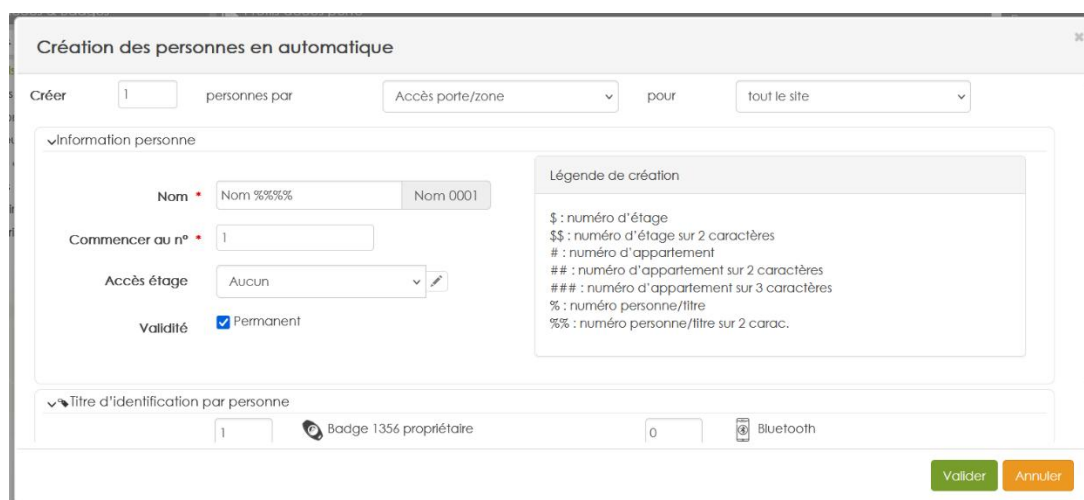
Dans « Matériel et paramétrages », puis « sorties » cliquez sur Action, puis sélectionnez les sorties à modifier, puis cliquez sur l'icône en forme de crayon.



La temporisation d'activation correspond à la période pendant laquelle la centrale enverra une commande. Si elle est réglée sur 5 secondes, le contrôleur via la sortie enverra le message pendant 5 secondes.

## 9.2 Outil de creation de personnes/de badges automatique

Il est possible, dans Ipevia Manager, de créer automatiquement des utilisateurs et leurs clés. Cette fonctionnalité permet la création de x badges (et des informations liées comme le nom). Cet outil est disponible en cliquant sur « utilisateurs et profils d'accès » dans le cadre de gauche. Ensuite, sous la liste « création automatique », sélectionnez « création des personnes en automatique ».

**Créer :** Vous pouvez choisir de créer x utilisateurs par **porte, zone l'étage, groupe d'utilisateurs, bâtiment, étage, bureau** pour **tout le site ou un profil d'accès spécifique**.

**Information personne :** avec des caractères spécifiques (voir la légende à coté pour plus d'informations), vous pouvez créer automatiquement des noms.

**Validité permanent :** si coché, les accès de ces personnes seront valables sans limite de durée. Si cette case est décochée, alors vous pouvez appliquer un calendrier lors duquel ils seront valides.

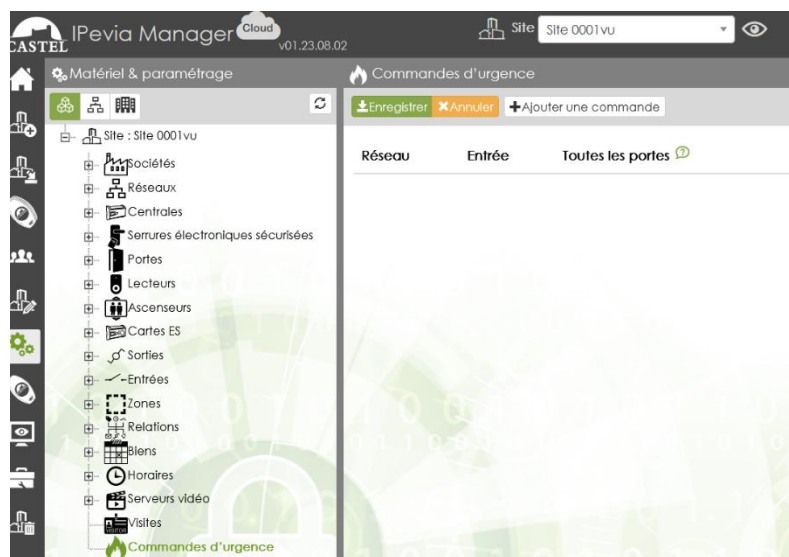
**Titre d'identification par personne :** vous pouvez ajouter un ou plusieurs jetons de proximité/accès Bluetooth pour chaque utilisateur.

## 9.3 Commandes d'urgence

La fonction « Commande d'urgence » permet de libérer des portes ou un groupe de portes si une entrée est active. Par exemple, cette configuration permet de câbler une alarme incendie à une entrée de la centrale IPevia. Lorsque ce contact est actif, il libère les gâches électriques ou les serrures magnétiques, maintenant les portes ouvertes.

Prérequis:

- Cette fonction contrôle un groupe de portes ou toutes les portes du réseau, il est donc nécessaire de créer un ou plusieurs groupes de portes qui seront contrôlés par ces contacts.
- Seules les gâches électriques à rupture ou serrures magnétiques, qui sont alimentées en continu, sont compatibles avec ce mode. Les gâches à émission (verrouillées au repos) ne sont pas conçues pour une alimentation continue et ne conviennent pas à cette option.
- L'entrée utilisée pour cette fonction doit être configurée comme NO (normalement ouverte), NC (normalement fermée) TOR (on/off), ou en impédance.



Pour accéder aux paramètres d'action d'urgence, cliquez sur le bouton « Matériel et paramétrages » dans le cadre de gauche. Sélectionnez l'option « +ajouter une action d'urgence ».

## 9.4 Relations

### Qu'est-ce qu'une relation

Une relation est donc un lien entre une condition et un processus.

- La condition est l'état d'une ou plusieurs entrées, portes, événements, etc.
- Un processus est une somme d'actions (contrôler un relais, déverrouiller un étage ou une porte, envoyer un message au logiciel...).

Les relations sont utiles dans IPévia Manager pour gérer tout ce qui n'est pas prédéfini. Exemples de fonctions réalisables par réflexes :

- Forcer un relais dès qu'une porte est forcée (principe d'une alarme intrusion) & relâcher le relais lorsqu'une clé spécifique est présentée à un lecteur spécifique.
- Activez un relais pour désactiver une alarme, par exemple, lorsqu'une clé d'un profil spécifique est présentée à certains lecteurs.
- Etc...

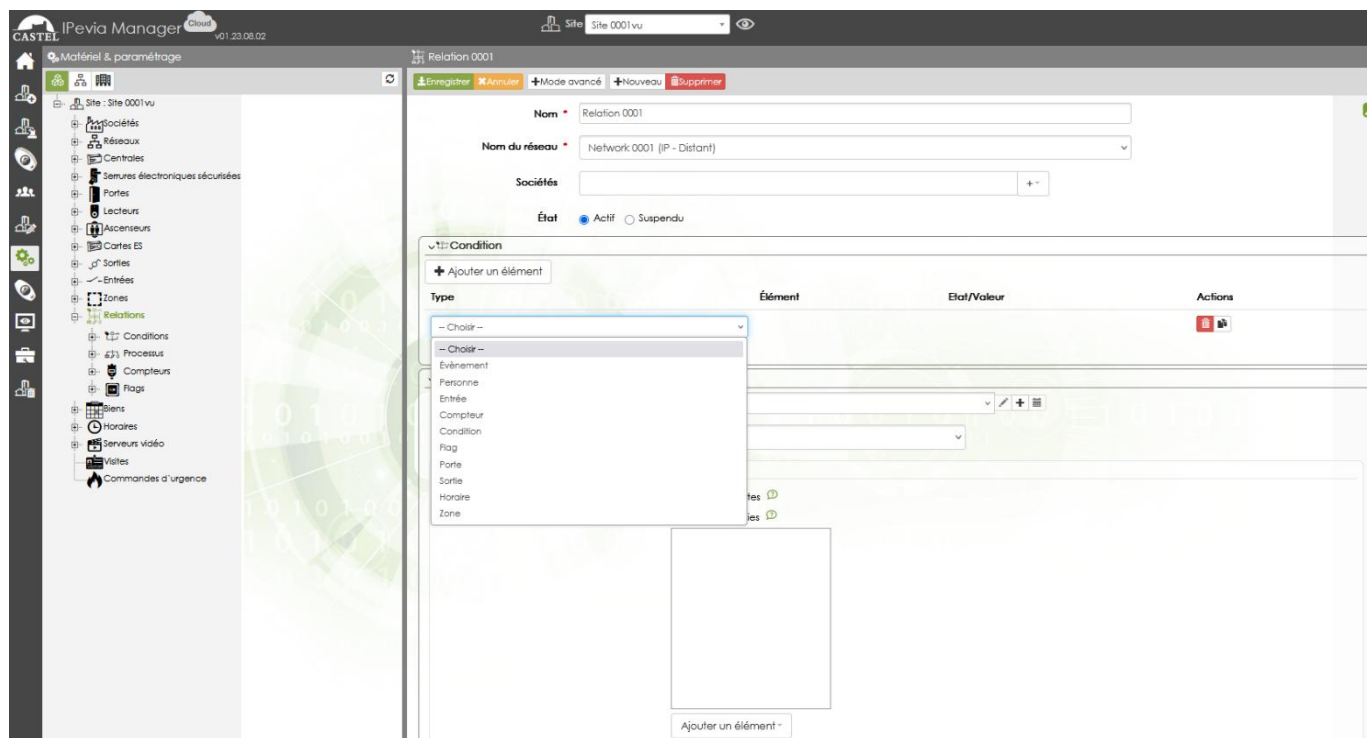
### Comment configurer une relation

Pour configurer une relation dans IPévia, assurez-vous que la fonctionnalité « Relation » est sélectionnée dans les fonctionnalités du site. (voir chapitre 2.2). Pour accéder aux paramètres des relations, allez dans « Matériel et paramétrages » et choisissez « relations » dans l'arborescence.

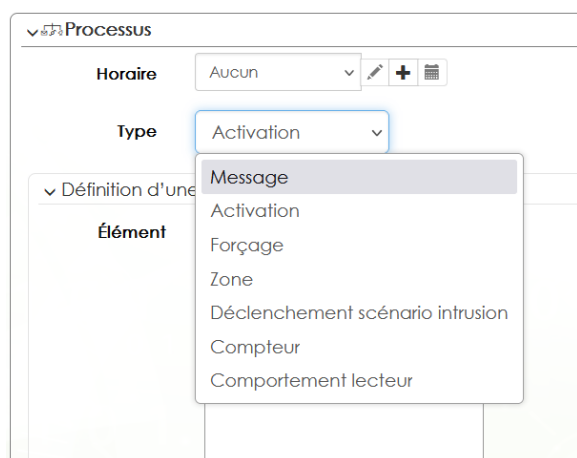
Le logiciel propose deux méthodes de gestion des réflexes :

- **Méthode simple** : dans cette méthode, l'utilisateur sélectionne tous les éléments de la même vue :
  - **Une condition** (parmi 5 événements ou états possibles)
  - **Un processus** (parmi 5 actions disponibles), le logiciel crée ensuite automatiquement la condition, le processus et les assemble afin de former une relation.
- **Méthode avancée** : dans cette méthode, l'utilisateur doit d'abord définir au moins une condition et au moins un processus. Une fois définis, ces conditions et processus peuvent être réutilisés dans d'autres relations, offrant plus de flexibilité et de contrôle sur la configuration.

## Exemple d'une relation simple



Après avoir cliqué sur le bouton « ajouter un élément » sous l'onglet « condition », choisissez le type de condition que vous souhaitez utiliser. Voir la capture d'écran ci-dessus pour voir toutes les options. Ce choix modifie les options sélectionnables sous l'onglet « condition ».

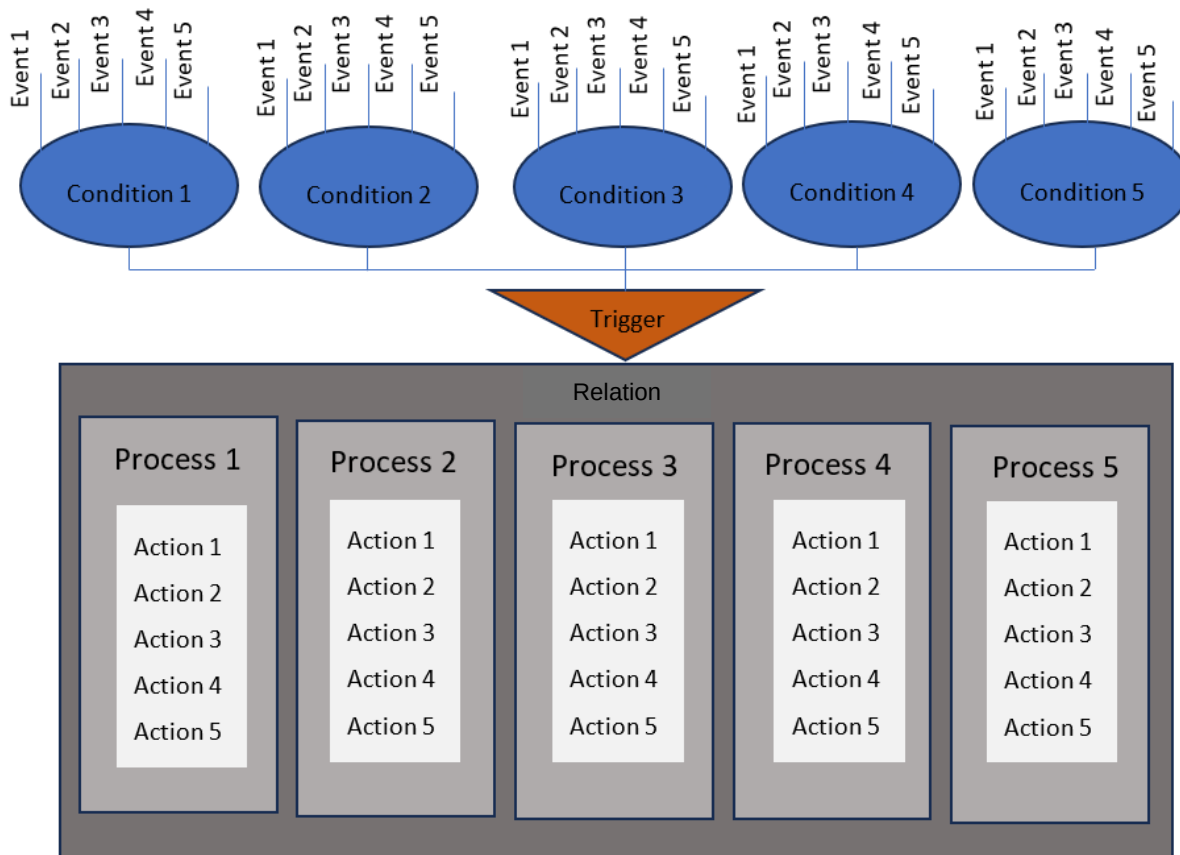


Le processus est la conséquence de la condition ci-dessus. Il existe plusieurs types de processus, comme l'activation d'une porte, une sortie ou l'envoi d'un message. Ce choix affecte les derniers champs.

## Limites de relations par IPevia

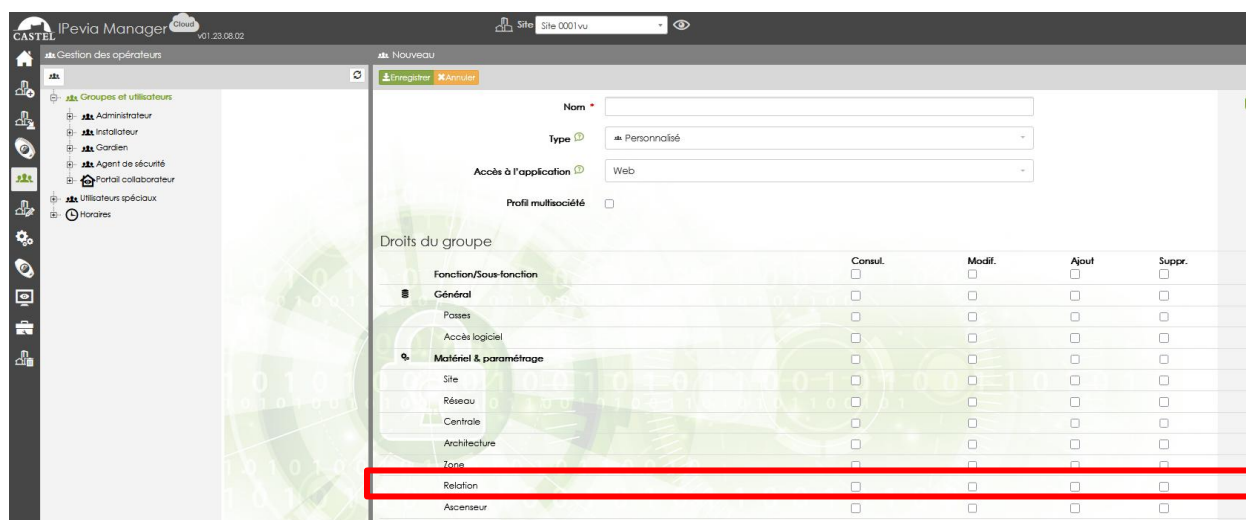
Limites d'IPevia (voir le schéma pour plus d'informations) :

- Une condition comprend jusqu'à 5 événements ou états avec une logique « ET » ou « OU ».
- Un réflexe peut être déclenché par jusqu'à 5 conditions avec une logique « ET » ou « OU ».
- Un processus comprend jusqu'à 5 actions.
- Un réflexe peut lancer jusqu'à 5 processus.



## Autoriser les utilisateurs à créer des relations

Vous pouvez déléguer la création de relations à d'autres utilisateurs du logiciel. Cliquez sur le bouton « gestion des opérateurs » dans le cadre de gauche. Choisissez ensuite le groupe de personnes à qui vous souhaitez laisser créer ou gérer des relations. Cochez ensuite les cases à côté de « relations ». Vous pouvez gérer les privilèges de ce groupe en le laissant consulter, modifier, ajouter ou supprimer une relation.



Il peut être pratique de laisser le droit à l'installateur de créer des relations, sachant qu'il connaît le matériel posé sur site.

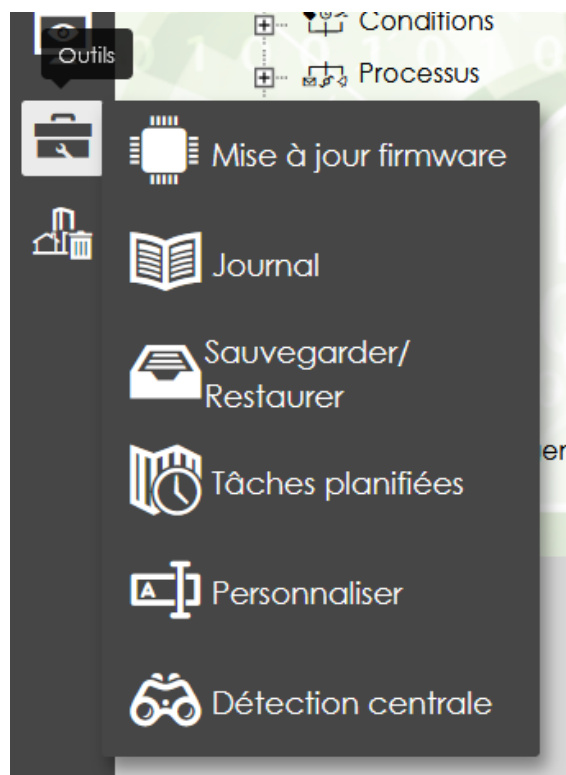
## 9.5 message

La fonctionnalité « **Message** » (accessible depuis l'onglet « **Monitoring** »), affiche des messages d'alerte qui ont été programmés via **des relations**. Ce menu affiche : le message **d'alerte**, la **date**, l'**heure de l'événement**, la **personne** qui a accusé réception (ou ignoré), etc...

Cet outil permet de surveiller et de gérer les alertes en temps réel, ce qui permet aux opérateurs de suivre l'état des événements et de prendre les mesures appropriées.

## 10. Outils

Différents outils, accessibles en cliquant sur la boîte à outils dans la barre d'outils de gauche, sont fournis dans le logiciel et permettent de :



- **Mise à jour firmware** : met à jour le micrologiciel de divers périphériques matériels tels que les contrôleurs et les cartes d'entrée/sortie. Cela permet de s'assurer que les appareils exécutent toujours la dernière version pour des performances et une sécurité optimale.

- **Journal** : affichez des informations en temps réel concernant le site, y compris des événements tels que les journaux d'accès, les alarmes et les activités sur le système. Cet outil permet de surveiller et de suivre les performances du système.

- **Sauvegarder/restaurer** : permet d'importer et d'exporter des sites (par exemple, le transfert d'un site d'un PC à un autre). Cette fonctionnalité est utile pour la migration de données ou la création de copies de sauvegarde des configurations de votre site.

- **Tâches planifiées** : vous permet de forcer des mises à jour sur les contrôleurs, de récupérer des événements et de déclencher des rapports par e-mail. C'est l'idéal pour automatiser les tâches de routine et assurer des mises à jour en temps opportun.

- **Personnaliser** : créez des champs personnalisés et insérez-les dans des formulaires, tels que celui de création de visite. Il permet également d'importer des

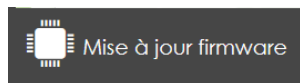
données sur la base de critères spécifiques pour plus de flexibilité et d'intégration.

- **Détection centrale** : détecte automatiquement les appareils sur le réseau, y compris leurs paramètres. Cet outil permet d'identifier et de configurer de nouveaux appareils pour une intégration facile dans le système.

Pour naviguer entre les différents outils, vous pouvez également les sélectionner à partir des boutons supérieurs. Ceux-ci offrent un accès rapide à diverses fonctions et fonctionnalités, vous permettant de passer efficacement d'une tâche à l'autre sans avoir à passer par les menus.



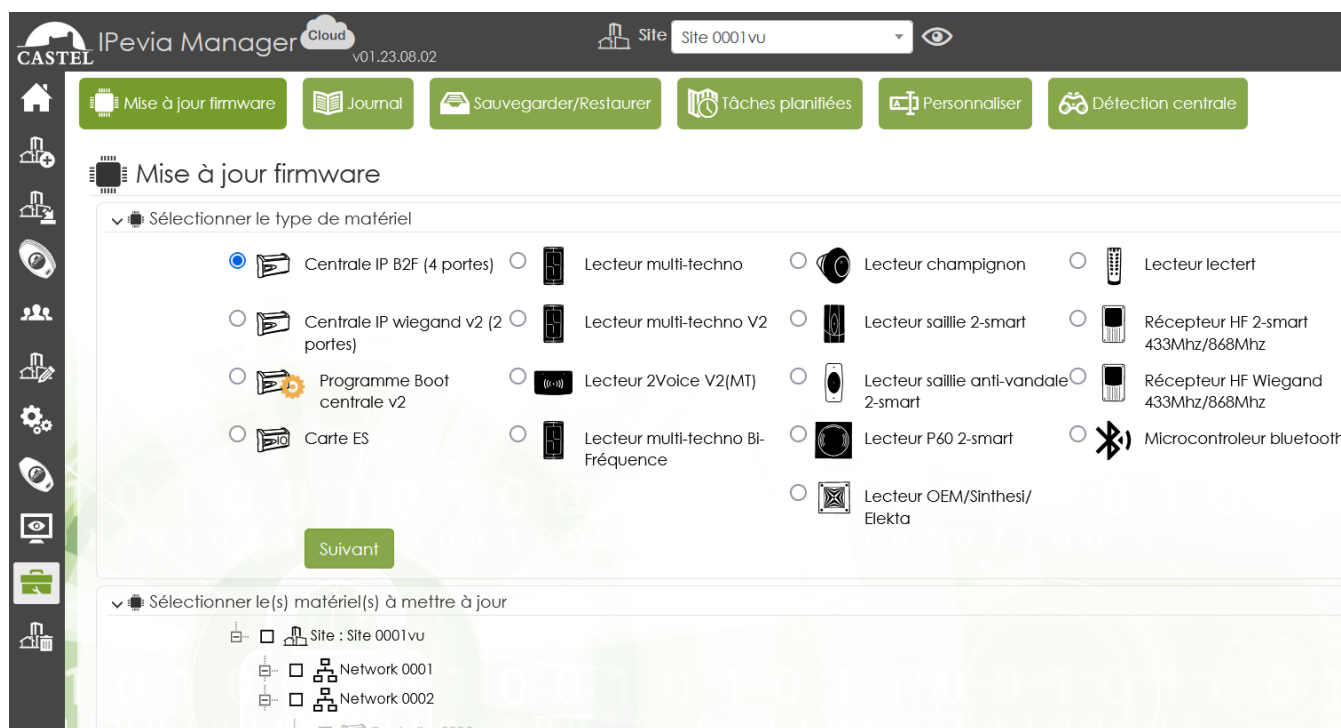
## 10.1 Mise à jour firmware



Dans le menu **Outils**, cliquez sur « **Mise à jour du firmware** ». Le processus de mise à jour matérielle se fait en deux étapes :

- **Sélectionnez le type de matériel** que vous souhaitez mettre à jour.
- **Appliquez la mise à jour au matériel sélectionné** : après avoir sélectionné le matériel, appliquez la mise à jour du micrologiciel à l'appareil choisi en suivant les instructions à l'écran.

Ce processus vous permet de mettre à jour le micrologiciel de divers composants matériels du système, en vous assurant qu'ils exécutent la dernière version pour des performances et une sécurité améliorée.



Ensuite, sélectionnez la version du firmware et cliquez sur le bouton « Mettre à jour le firmware » :

Si le firmware voulu n'est pas spécifié dans le logiciel (et le serveur), un menu vous permet de l'ajouter. En bas de la fenêtre, sous la liste des firmwares, cliquez sur « ajouter un logiciel » et spécifiez un nom pour celui-ci. Il est possible d'ajouter une description. Cliquez sur le bouton « parcourir » pour ajouter le fichier du firmware depuis le répertoire pc.

Une fois le firmware chargé, la page se rafraîchit d'elle-même. Ensuite, il est possible d'envoyer le fichier aux contrôleurs.

## 10.2 journal

Le journal suit les actions de chaque opérateur. Vous pouvez filtrer ces journaux par : utilisateur, dates, sites et autres critères.



Journal

CASTEL Ipevia Manager v01.23.08.02 Site Site 0001vu

Mise à jour firmware Journal Sauvegarder/Restaurer Tâches planifiées Personnaliser Détection centrale

Journal

>Filtres

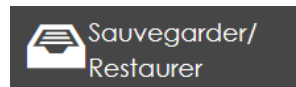
485 entrées trouvées

Résultat base de données journal

Exporter Purger

| Date / Hour         | Personne     | Action                | Type           | Commentaire                                          |
|---------------------|--------------|-----------------------|----------------|------------------------------------------------------|
| 2025-01-29 13:41:40 | GELIN Maxime | Connexion utilisateur | Accès logiciel | Connexion de mgellin@fdi-access.com à l'application. |
| 2025-01-29 09:02:55 | GELIN Maxime | Connexion utilisateur | Accès logiciel | Connexion de mgellin@fdi-access.com à l'application. |
| 2025-01-27 10:18:12 | GELIN Maxime | Modification          | Entrée         | Carte ES 0001 - Entrée 0001                          |
| 2025-01-27 09:53:50 | GELIN Maxime | Ajout                 | Entrée         | Carte ES 0001 - Entrée 0022                          |
| 2025-01-27 09:53:50 | GELIN Maxime | Ajout                 | Entrée         | Carte ES 0001 - Entrée 0021                          |
| 2025-01-27 09:53:50 | GELIN Maxime | Ajout                 | Entrée         | Carte ES 0001 - Entrée 0020                          |
| 2025-01-27 09:53:50 | GELIN Maxime | Ajout                 | Entrée         | Carte ES 0001 - Entrée 0019                          |
| 2025-01-27 09:53:50 | GELIN Maxime | Ajout                 | Entrée         | Carte ES 0001 - Entrée 0018                          |
| 2025-01-27 09:53:50 | GELIN Maxime | Ajout                 | Entrée         | Carte ES 0001 - Entrée 0017                          |

## 10.3 sauvegarder/restaurer



Lors du transfert d'un site d'un serveur à un autre (par exemple, d'Ipevia.com à un serveur local, ou du PC de l'installateur à la base de données du client final), le logiciel permet de créer des fichiers de sauvegarde qui peuvent être directement importés sur l'autre serveur.

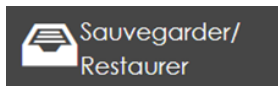
Un fichier de sauvegarde peut inclure plusieurs sites. Pendant la restauration, une boîte de dialogue vous permet de sélectionner les sites à importer.

### Étapes pour exporter des sites :

1. Dans le menu **Outils**, accédez à l'onglet **Sauvegarder/Restaurer**.
2. Cliquez sur le bouton **Ajouter un site à sauvegarder**.
3. Utilisez la **touche Ctrl** pour sélectionner plusieurs sites si nécessaire.
4. Sur le côté droit, cliquez sur **Sauvegarder** pour générer le fichier.
5. En fonction de votre navigateur, une fenêtre vous demandera d'enregistrer le fichier sur votre PC.

**Remarque :** L'exportation d'un site à partir d'une base de données **ne** le supprime pas de la base de données d'origine.

## 10.4 Restaurer (fichier d'import site)



Ce menu vous permet de récupérer un site d'une autre machine (ou du Web) sur le serveur.

Cliquez sur **Outils**, puis sélectionnez le bouton **Sauvegarder/restaurer les données**.

Dans l'option « **restaurer un ou plusieurs sites** », cliquez sur **Parcourir**. Cela ouvre l'explorateur de fichiers Windows.

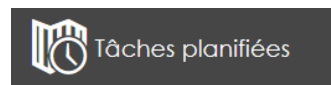
Sélectionnez le fichier de sauvegarde, puis cliquez sur **Restaurer**. La fenêtre suivante s'affiche

A screenshot of a web application dialog box titled 'Restaurer un ou plusieurs sites'. It features a 'Fichier' label, a text input field containing 'Parcourir...' and 'Aucun fichier sélectionné.', and a checkbox labeled 'Supprimer les numéros de séries des centrales lors de la restauration'. A green 'Restaurer' button is located at the bottom right.

:

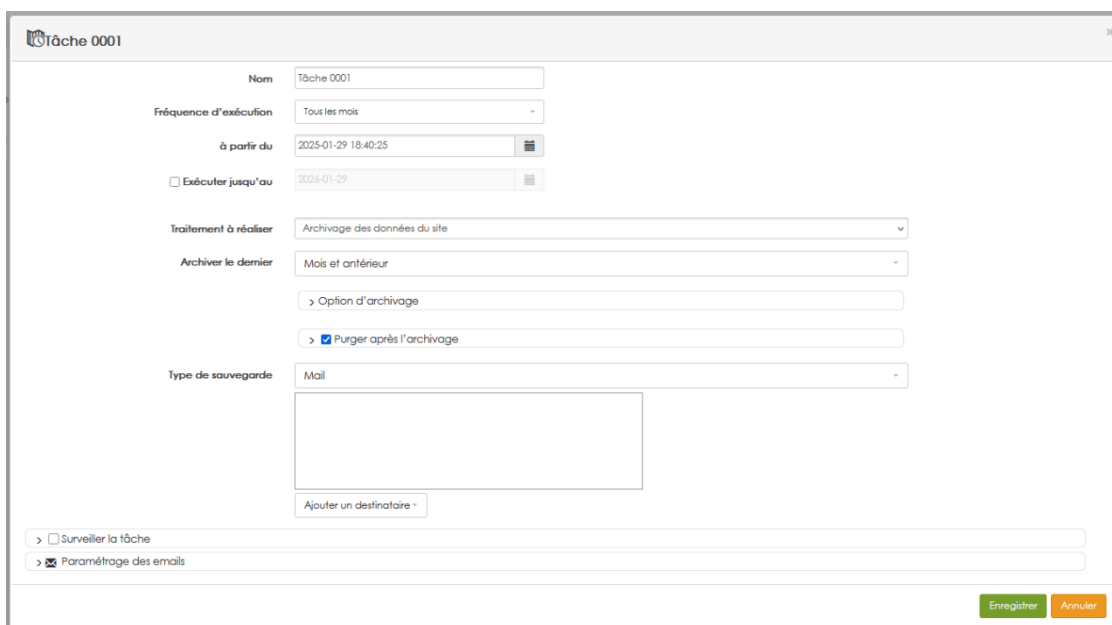
Cliquez sur « **Restaurer** » pour lancer le processus d'importation. Un dernier message confirmera : « **L'importation a réussi** ».

## 10.5 tâches planifiées



Dans IPEvia Manager, il est possible de créer des tâches planifiées. Il s'agit d'actions que la centrale effectuera automatiquement à des dates/heures spécifiées.

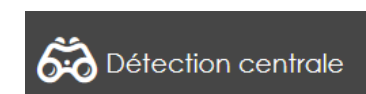
Une tâche planifiée peut impliquer une action sur les centrales, une sauvegarde de base de données ou l'envoi d'un rapport par e-mail.



Note : il est possible d'éviter d'envoyer un rapport s'il est vide en cochant l'option en bas de la fenêtre (sous l'onglet « paramétrage des emails »)

La tâche peut être surveillée, de sorte qu'un ou plusieurs destinataires reçoivent un e-mail les informant de la réussite de la tâche, mais sans recevoir le rapport lui-même.

## 10.6 controller detection



Cet outil permet de détecter les nouveaux contrôleurs sur le réseau, à condition qu'ils n'aient pas déjà été intégrés.

Contrairement au menu « **Monitoring** » et à « **État réseau** » qui affiche tous les contrôleurs du réseau, y compris ceux qui ont déjà

été intégrés au site.

## Détection centrale

Paramétrage de la détection

Recherche par son IP ?

Port

1880



Recherche par identifiant ?



 Recherche des centrales IP/USB en cours...

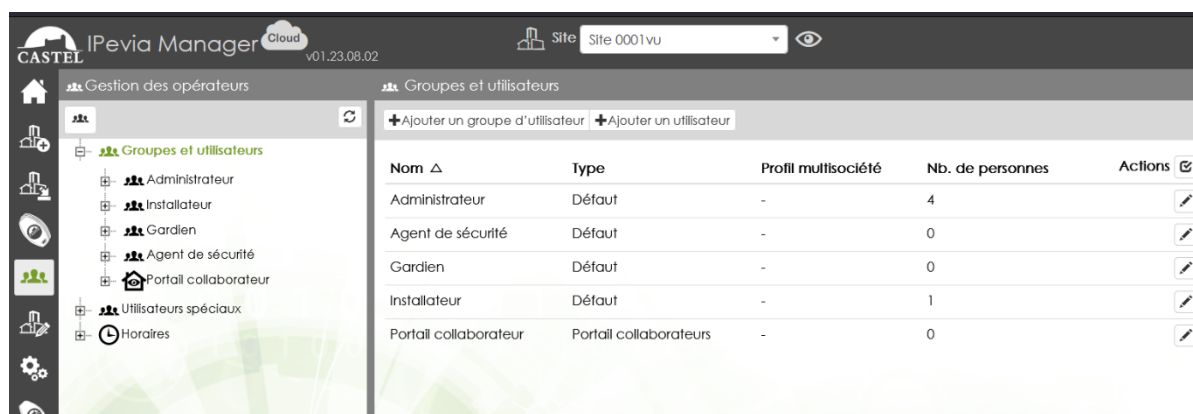
Il est possible d'effectuer une recherche de centrale par son IP ou par son identifiant.

## 11. Gestion des opérateurs

Le logiciel permet la création de profils d'opérateurs limités à des sites et/ou des fonctionnalités logicielles spécifiques.

Par exemple:

- Un **administrateur** dispose de tous les droits sur tous les sites : il a accès à toutes les fonctionnalités et a la possibilité de créer d'autres opérateurs.
- Un opérateur disposant du **profil Installateur** peut effectuer n'importe quelle action sur les sites auxquels il est autorisé à accéder.



Les profils existants, à l'exception de celui d'Administrateur, peuvent être modifiés. Il est également possible de créer une infinité de profils.



Vous pouvez gérer, ajouter ou supprimer un opérateur à l'aide de son onglet spécifique dans le cadre de gauche. Cliquez sur le bouton « Gestion des opérateurs ».

### 11.1 Ajouter un groupe d'utilisateur

Lorsqu'aucun profil existant ne répond aux exigences, il est possible d'en créer d'autres. Cliquez sur « **Groupe et utilisateurs** » à la base de l'arborescence. Cliquez ensuite sur le bouton « **Ajouter un groupe d'utilisateur** ». Définissez le nom de du groupe d'opérateur ainsi que ses privilèges.

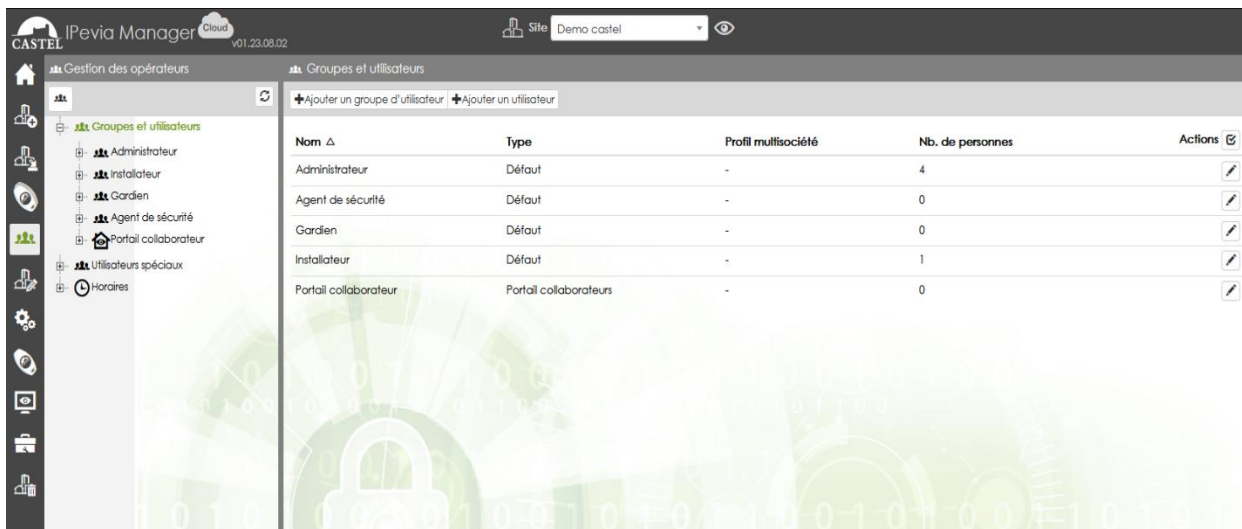
Par exemple:

- Si la ligne relation est cochée à la colonne « **Modifier** » cela signifie que l'opérateur aura le droit d'apporter des modifications aux relations déjà configurés.
- Si « **Ajouter** » est coché, l'opérateur pourra en créer de nouvelles.

## 11.2 Ajouter, modifier un opérateur

Un opérateur est défini par :

- **Nom, prénom, adresse e-mail et mot de passe**
- **Appartenance à un profil d'opérateur (groupe)**
- Données facultatives telles que le numéro d'employé, l'adresse, etc.
- Une liste des sites autorisés. Les droits sont les mêmes pour chaque site.



The screenshot shows the Ipevia Manager interface. The top bar includes the CASTEL logo, the text 'Ipevia Manager Cloud', the version 'v01.23.08.02', and a 'Site' dropdown menu set to 'Demo castel'. The left sidebar has icons for home, users, groups, and settings. The main content area is titled 'Gestion des opérateurs' and 'Groupes et utilisateurs'. It features a table with the following data:

| Nom                   | Type                   | Profil multisociété | Nb. de personnes | Actions |
|-----------------------|------------------------|---------------------|------------------|---------|
| Administrateur        | Défaut                 | -                   | 4                |         |
| Agent de sécurité     | Défaut                 | -                   | 0                |         |
| Gardien               | Défaut                 | -                   | 0                |         |
| Installateur          | Défaut                 | -                   | 1                |         |
| Portail collaborateur | Portail collaborateurs | -                   | 0                |         |

## 12 Intégration

IPeVia Manager offers several data integration options. The easiest method is importing Excel files, which can be automated.

The second option is to create read-only access to the database. A developer can then retrieve, for example, information related to supervision (such as integration with time management systems).

Alternatively, this database access can be set to read/write.

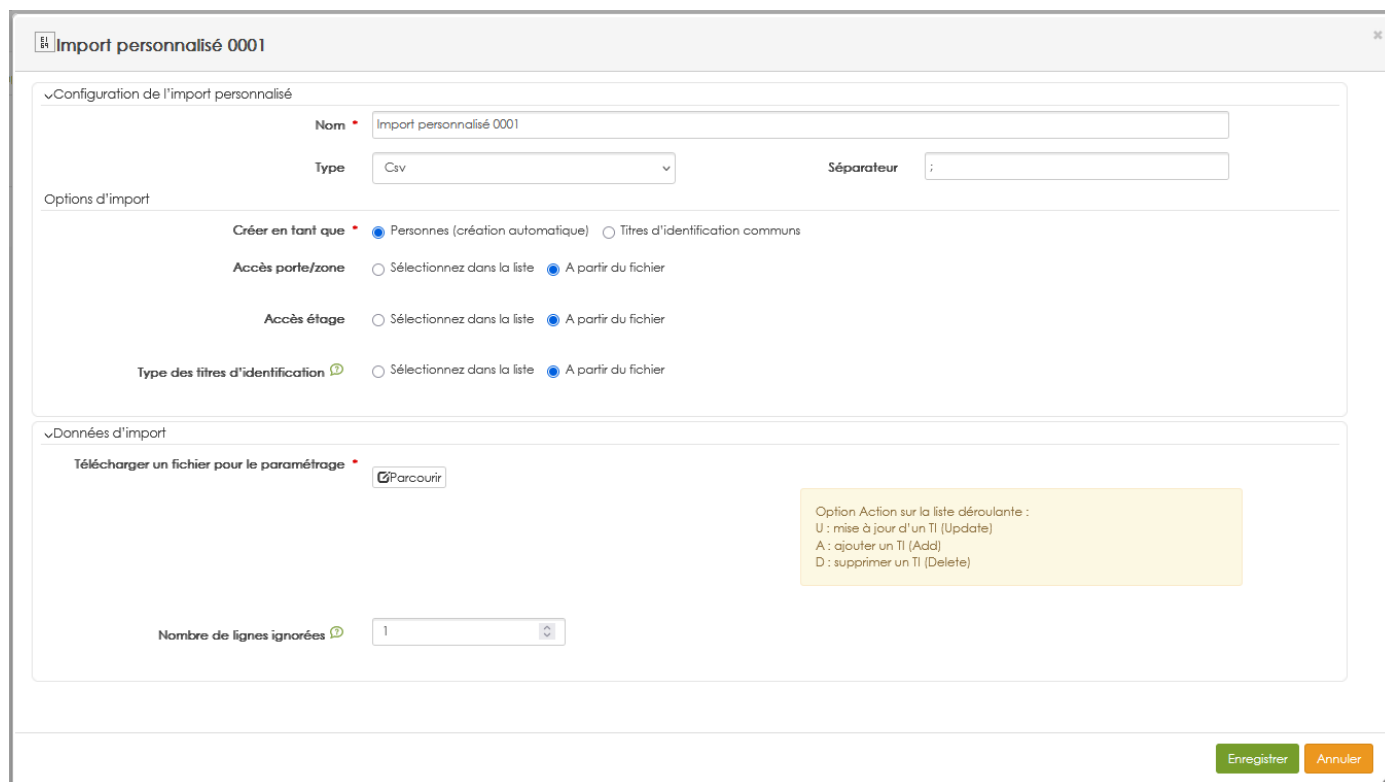
### 12.1 Import automatique/import de fichier type

Il est nécessaire de définir la disposition des colonnes pour le fichier à importer. Ensuite, vous pouvez choisir d'importer manuellement un ou plusieurs fichiers dans le logiciel ou de créer une tâche automatique qui importe les données toutes les heures, tous les jours, etc.

Une dernière option permet de déclencher la tâche à la demande via une URL.



Dans **Outils / Personnaliser**, cliquez sur « **Ajouter un import personnalisé** ».



Tout d'abord, définissez les champs « **Configuration d'Importation Personnalisée** » ainsi que les « **Options d'Importation** » :

Entrez un nom pour ce modèle d'importation de fichiers.

Sélectionnez le type de fichier :

- **Xls**
- **Csv** (le séparateur par défaut est « ; »)
- **Fichier XML**

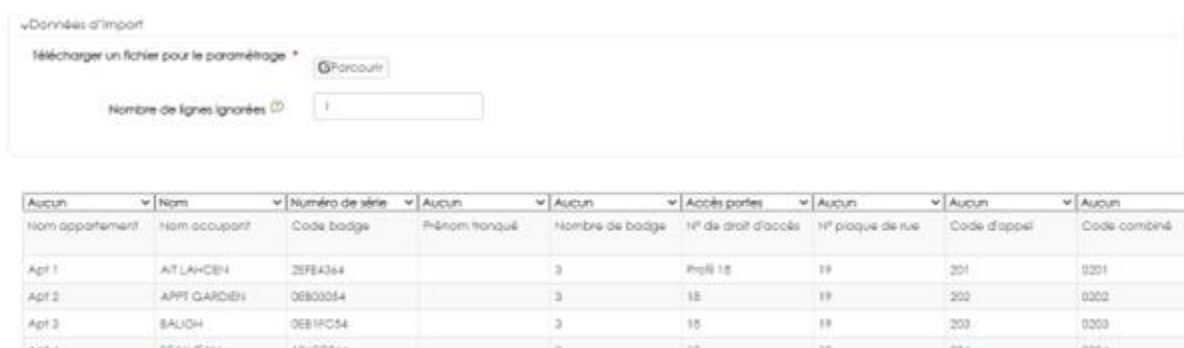
- « **Créer en tant que** » : cette option vous permet de choisir si les badges ajoutés seront catégorisés sous « **Profil d'accès** » ou « **Titre d'identification commun** ».
- « **Accès porte/zone** » : cette option attribue automatiquement un même profil d'accès existant à partir du logiciel. Vous pouvez également récupérer le profil d'accès à la porte à partir du fichier Excel. Dans ce cas, l'utilisateur est ajouté au profil spécifié. Si le profil n'existe pas, il sera automatiquement créé, mais sans sélection de porte.
- « **Type de titre d'identification** » : cette option vous permet de sélectionner le type de titre d'identification à importer dans une liste ou de lire celui renseigné dans le fichier excel.
  - Choisissez « **à partir du fichier** » si cette information est fournie dans la feuille Excel.
  - L' option « **sélectionner dans la liste** » est utile si la feuille Excel ne contient pas le type de titre ou si elle indique un type sans signification pour Ipevia Manager. Cette option force le type d'identification.

Vous pouvez demander que le type de titre d'identification soit lu dans le fichier Excel, mais dans ce cas, les informations renseignées dans la feuille de calcul doivent reprendre celles du logiciel (par exemple, Badge Mifare+, Code du clavier, Télécommande à 4 boutons, Autre hexadécimal, etc.).

Dans la section « **Importer des données** » en bas de la page, vous pouvez importer un fichier à l'aide du bouton **Parcourir**. Cela vous permet de:

- Sauter les **x premières** lignes.
- Définir la colonne du fichier Excel qui contient les données à importer.

**Remarque :** les colonnes peuvent être exclues de l'importation.



Données d'import

Télécharger un fichier pour le paramétrage \*

Parcourir

Nombre de lignes ignorées 1

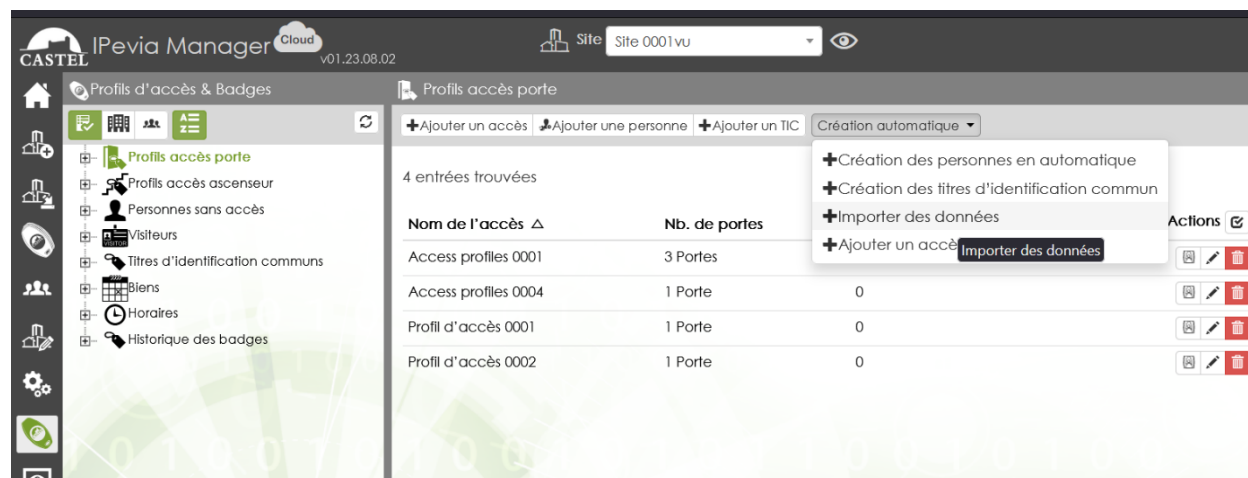
| Aucun           | Nom          | Numéro de série | Aucun          | Aucun           | Accès portes        | Aucun            | Aucun        | Aucun        |
|-----------------|--------------|-----------------|----------------|-----------------|---------------------|------------------|--------------|--------------|
| Nom appartement | Nom occupant | Code badge      | Prénom tronqué | Nombre de badge | N° de droit d'accès | N° plaque de rue | Code d'appel | Code combiné |
| Apt 1           | AIT LAHCEH   | 2EFA4364        |                | 3               | Profil 18           | 19               | 201          | 0201         |
| Apt 2           | APPE GARDIES | 0E800054        |                | 3               | 18                  | 19               | 202          | 0202         |
| Apt 3           | BAUDH        | 0E81FC54        |                | 3               | 15                  | 19               | 203          | 0203         |
| Apt 4           | BEAUJEAN     | 10x50064        |                | 3               | 18                  | 19               | 204          | 0204         |

Click on "save".

## 12.2 Import manuel



Cliquez sur l'icône « Passes » dans le menu de gauche.



Ipevia Manager Cloud v01.23.08.02

Site Site 0001vu

Profil accès porte

+Ajouter un accès +Ajouter une personne +Ajouter un TIC Création automatique

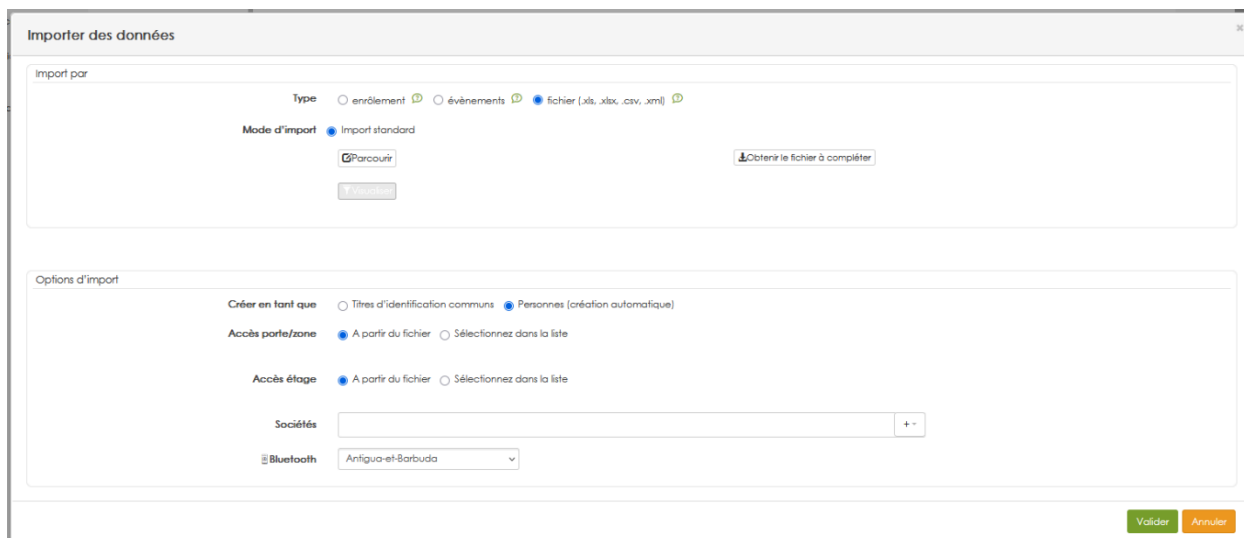
4 entrées trouvées

| Nom de l'accès       | Nb. de portes |   |
|----------------------|---------------|---|
| Access profiles 0001 | 3 Portes      |   |
| Access profiles 0004 | 1 Porte       | 0 |
| Profil d'accès 0001  | 1 Porte       | 0 |
| Profil d'accès 0002  | 1 Porte       | 0 |

+Création des personnes en automatique  
+Création des titres d'identification commun  
+Importer des données  
+Ajouter un accès Importer des données

Actions

Dans la fenêtre suivante, sous la section « Importer par », sélectionnez « Fichier (.xls) ». Utilisez ensuite le bouton « Parcourir » pour sélectionner une importation personnalisée ainsi que le type de fichier à importer.



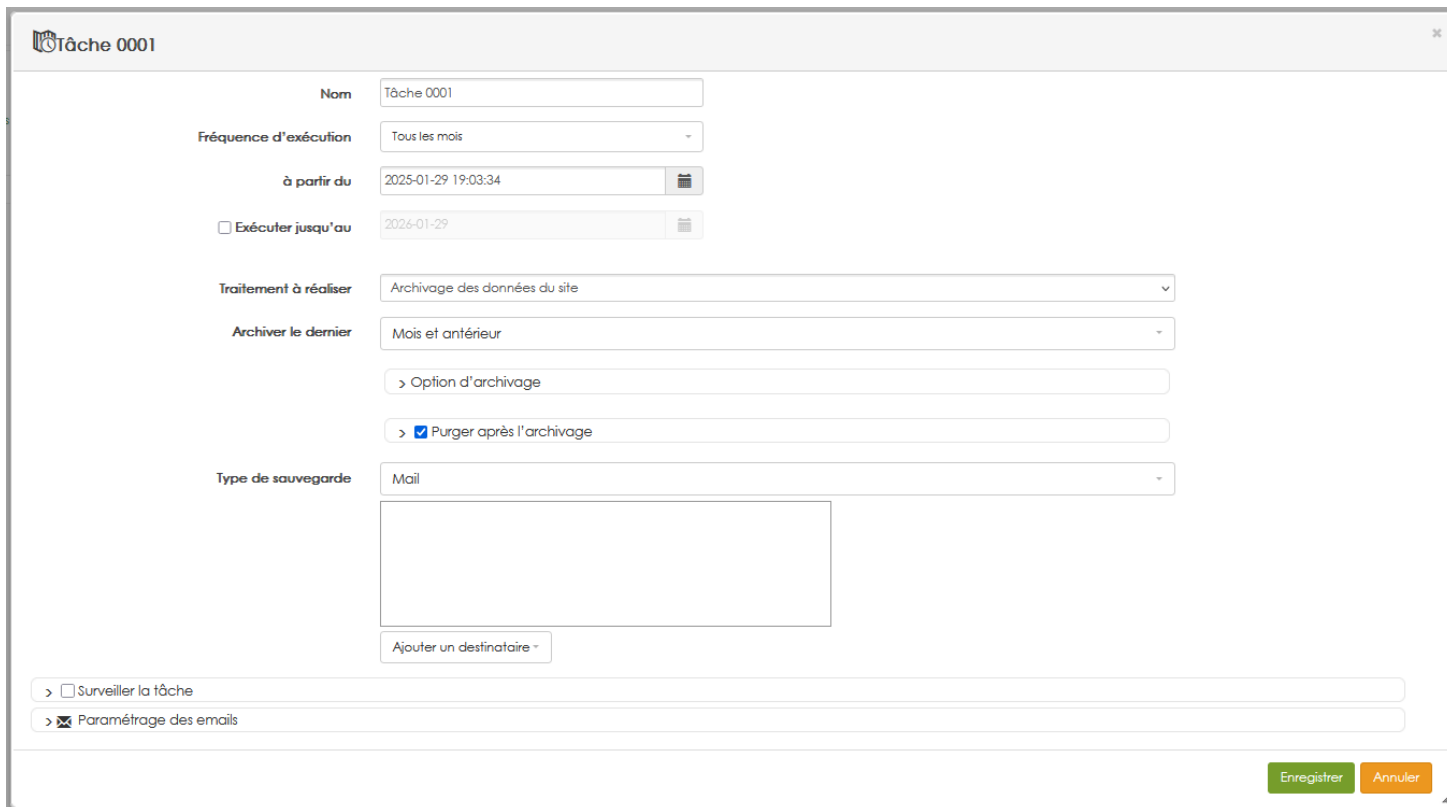
## 12.3 Importer avec une tâche automatique

IPévia Manager permet également l'importation automatique de ces types de fichiers. Des logiciels tiers peuvent régulièrement placer un fichier dans un répertoire désigné, et IPévia Manager l'importera ensuite.

Une fois le fichier traité par IPévia Manager, il est déplacé du répertoire désigné vers **/Backup**.

Si plusieurs fichiers sont placés dans le répertoire, ils seront tous traités.

Dans « **Outils** » / « **Tâches planifiées** », cliquez sur « **Créer une tâche** ».



- Entrez **un nom** pour la tâche et **sélectionnez la fréquence** (par exemple, horaire, quotidienne, hebdomadaire, etc.).
- Choisissez **l'action à effectuer** dans la liste à côté du champ « traitement à faire » (par exemple, importer des personnes via un fichier dans cet exemple). Selon l'option sélectionnée, cela peut affecter les champs suivants ou en ajouter d'autres).
- **Spécifiez le répertoire** dans lequel sont stockés les fichiers à importer.
- Sélectionnez le **type d'importation** (par défaut dans IPévia Manager / personnalisé).
- S'il s'agit d'une importation personnalisée, choisissez le modèle prédéfini. Cliquez sur **Enregistrer** en bas à droite.

## 12.4 Importer avec des commandes externes

Une fois les tâches planifiées configurées, elles peuvent être déclenchées sur le serveur via une URL. La première étape consiste à créer un utilisateur du logiciel autorisé à lancer la tâche. Cliquez sur « Accès au logiciel » dans le menu de gauche. Ensuite, dans l'arborescence, sélectionnez « Utilisateurs spéciaux ».

Entrez un identifiant puis un mot de passe. Sélectionnez l'option « **Lanceur de tâches** » dans le **champ** « Type ».

Choose the task by clicking on the “+”.

Don't forget to **save**.

Le texte suivant apparaît et montre la syntaxe à suivre pour déclencher la tâche via un navigateur web :

**Remarque** : pour exécuter cette tâche à partir d'un autre ordinateur, il suffit de remplacer **127.0.0.1** par l'adresse IP du serveur Ipévia, comme indiqué dans l'exemple ci-dessous :

<https://192.168.0.1:8443/Ipévia/?taskCom=user&login=lanceur&pwd=0000>



- 1 Agence Paris IDF
- 2 Agence Nord
- 3 Agence Est
- 4 Agence Rhône-Alpes
- 5 Agence Paca
- 6 Agence Occitanie
- 7 Agence Sud Ouest
- 8 Agence Nord Ouest
- 9 Agence Bretagne
- 10 Agence Centre



|| **ADMINISTRATION DES VENTES**  
(DÉLAIS, SUIVI DE COMMANDE)  
Tél. 02 41 40 41 40  
info@castel.fr

|| **HOT-LINE**  
Tél. 02 41 40 41 42  
support@castel.fr

|| **SERVICE DEVIS**  
Tél. 02 41 40 41 32  
devis@castel.fr



**Protection de l'environnement :**

Éliminez ce produit conformément aux règlements sur la préservation de l'environnement.