dormakaba

Community

Guide d'utilisation

PK3706 2.6 - 08/2026
Document original

FR

dormakaba Canada
105 Marcel-Laurin Blvd
Montréal, Québec, H4N 2M3
Téléphone : +1 866-dormakaba (1-866-367-6252)

www.dormakaba.com

Copyright © dormakaba 2026
Tous droits réservés.

Aucune partie de ce document ne peut être reproduite ou utilisée sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable
de dormakaba Canada.

Tous les noms et logos des produits et services de tiers sont la propriété de leurs détenteurs respectifs. MIFARE, MIFARE Classic, MIFARE Plus et MIFARE Ultralight sont des marques déposées de NXP B.V.

Sous réserve de modifications techniques.

Table des matières

À propos de ce document 8
Bienvenue dans Community 9
Configuration 11
Flux de travail de configuration du site 13
Configurer les paramètres du système 14
En savoir plus sur les paramètres du système 15
Paramètres généraux 19
Paramètres de gestion des résidents 20
Paramètres de sécurité 21
Paramètres de la clé du personnel/prestataire 32
Paramètres des Clés à sécurité intégrée 33
Paramètres d'expiration de la clé 34
Paramètres de configuration de la messagerie électronique 36
Paramètres de sauvegarde de la base de données 37
Paramètres de gestion des visiteurs 41
Paramètres de l'interface du système d'accès 43
API Community 44
Paramètres avancés 46
Paramètres de licence 50
Configurez votre site 51
En savoir plus sur le configurateur de site 52
Ajouter des bâtiments 58
Ajouter des étages 59
Ajouter des unités 62
Ajouter des suites 66
Ajouter des espaces communs pour les résidents 70
Ajouter des espaces communs pour le personnel 76
Ajouter des accès privés 82
Ajouter des ascenseurs 84
Configurer l'accès 88
En savoir plus sur la gestion des accès 89
Ajouter des horaires de libre passage 93
Ajouter des horaires d'accès 95
Ajouter les horaires des clés du personnel 98

Créer des groupes de points d'accès 100
Ajouter des identifiants 102
Attribuer des horaires 106
Configurer les profils d'accès aux espaces communs à accès limité 107
Configurer des périphériques 111
En savoir plus sur la gestion des périphériques 112
Ajouter des encodeurs 114
Programmer des serrures 117
En savoir plus sur la Programmation et audit 118
Programmer des serrures 121
Examiner et personnaliser les rôles 123
En savoir plus sur la gestion des rôles 124
Consulter les rôles prédéfinis 126
Configurer les rôles personnalisés 127
Ajouter des opérateurs 128
En savoir plus sur la gestion du personnel/prestataries 129
Configurer les opérateurs 131
Importer la liste des membres du personnel/prestataires 136
Utilisation Community 138
Gestion des résidents 141
En savoir plus sur la gestion des résidents 142
Ajouter des résidents 150
Importer la liste des résidents 152
Affecter les unités 154
Créer des clés de résidents 161
Modifier l'accès résident 164
Invalider l'accès des résidents 170
Créer des clés pour l'accès aux espaces communs uniquement 180
Créer des clés mobiles pour plusieurs résidents 182
Configurer la gestion des visiteurs pour les résidents 184
Gestion du personnel et des prestataires 186
En savoir plus sur la Gestion du personnel/prestataire et les Clés du personnel/prestataire 187
Ajouter des membres du personnel/prestataires 189
Importer la liste des membres du personnel/prestataires 191
Créer des clés d'urgence 193
Créer une clé du personnel (accès prédéfini) 196

Créer des clés du personnel (accès variable) 199
Créer des clés de prestataire 204
Créer des clés à usage restreint 208
Remplacer les clés du personnel/prestataire 212
Invalider l'accès du personnel/prestataire 214
Configurer la gestion des visiteurs pour les membres du personnel/prestataires 219
Programmation/Audit 220
Reprogrammer des serrures 221
Audit des serrures 223
Auditer les points d'accès en ligne 224
Clés système 225
En savoir plus sur les clés Système 226
Clés de blocage et de déblocage 230
Clés d'annulation 234
Clés de diagnostic 237
Clés de bascule de verrouillage électronique 239
Clés à sécurité intégrée 241
Clés d'annulation 242
Clés de verrouillage et de déverrouillage 244
Clés de programmation primaire et secondaire 246
Clés de reséquence 249
Clés à fonction spéciale 251
Surveillance 253
En savoir plus sur la surveillance 254
Surveiller les clés 255
Surveiller l'utilisation des clés numériques 256
Rapports 258
Rapport d'audit de point d'accès 259
Rapport sur les attributions des identifiants/points d'accès 261
Rapport sur la configuration des ascenseurs 262
Rapport sur les expirations de clés 263
Key/User Assignment Report 264
Rapport sur les opérateurs 265
Rapport sur la configuration du site 266
Rapport sur les rôles et droits 267
Rapport des accès du personnel/prestataire 268

Rapport sur l'activité système 269
Rapport de gestion des visiteurs 271
Les bases de la barre d'outils 272
Naviguer Community 273
Définir les préférences de l'opérateur 275
Installation / Mise à jour du Client Community 277
Sélectionner l'encodeur par défaut 278
Déverrouillage/verrouillage à distance 279
Lire la clé/effacer la clé/rapport de suivi d'accès 281
Afficher les notifications 285
Clés physiques 288
Clés mobiles 290
Gestion des serrures à distance 295
Introduction 296
Activer et configurer la communication en ligne 297
Passerelles et points d'accès assignés 304
Gérer la configuration du périphérique en ligne 305
Passerelles enregistrées et points d'accès assignés 307
Gestion des notifications 312
En savoir plus sur la gestion des notifications 313
Ajouter des groupes de notification 315
Surveillance (à distance) 317
En savoir plus sur la surveillance 318
Afficher les indicateurs 319
Surveiller des opérations en ligne 320
Surveiller les événements en ligne 322
Surveiller l'état des points d'accès 325
Rapports (à distance) 326
Rapport d'état des points d'accès en ligne 327
Rapport d'état de la passerelle en ligne 328
Rapport du point d'accès assigné et en ligne 329
Dépannage 330
Gestionnaire de services 331
Dépannage des encodeurs 335
Dépannage des serrures 339
Données de journal 345

Annexes 346
Glossaire 347
Index 356

À propos de ce document

Validité

Ce document décrit le produit :

Désignation du produit :	Community
Version :	2.6

Public cible

Ce document est destiné à tous les opérateurs Community : Administrateur, configurateur de site, superviseur de maintenance, technicien de maintenance et agent de location.

But et objectif

L'objectif de ce document est de fournir des informations conceptuelles et pédagogiques sur les caractéristiques et les fonctions de Community. Ce document aborde également des sujets de dépannage de base pour les problèmes courants.

Documents supplémentaires

Community Guide d'installation v 2.6 PK3706-FR

Community Notes de mise à jour v 2.6 PK3696

Community Enhanced Key Security 2.6 PK3776

Bienvenue dans Community

Démarrage

Que vous souhaitiez faire une visite auto-guidée de votre nouveau logiciel ou passer directement à la configuration de votre site, le flux de travail Community est le meilleur endroit pour commencer. Le processus opérationnel commence par l'installation, se poursuit par la configuration du site, puis se termine par la mise en service.

Le *Guide d'utilisation Community* est organisé de manière à suivre le flux de travail recommandé et fournit des informations et des instructions à tous les opérateurs de Community.

Un Opérateur est un membre du personnel qui peut se connecter et utiliser Community.

Le guide d'utilisation comprend les sections suivantes :

- « Configuration du site » fournit un flux de travail facile à suivre et des instructions pas à pas pour paramétrer Community.
- « Utiliser Community » fournit des instructions sur l'utilisation au quotidien après la Mise en service et comprend les sujets Utiliser ... qui traitent certaines des situations les plus complexes.
- « Gestion des serrures à distance » fournit des informations relatives à la fonction sous licence Communication en ligne et à toutes les autres fonctions qui nécessitent une communication en ligne.
- « Dépannage » contient des informations sur la résolution de problèmes fournies par les techniciens de terrain de dormakaba.
- Le glossaire définit les termes utilisés dans le produit.
- La table des matières et l'index fournissent des moyens alternatifs pour trouver des informations.

De plus, une aide contextuelle est disponible dans le produit.

Installation

L'installation du serveur Community et du client Community est un processus simple piloté par un assistant. Pour des instructions détaillées, consultez le *Guide d'installation Community* et les *Notes de mise à jour Community*. Pour une assistance, un technicien expérimenté de dormakaba est disponible pour guider le processus et résoudre tout problème.

Configuration du site

La configuration du site est le processus qui consiste à définir les contrôles d'accès pour le site et à créer des profils pour les personnes de votre organisation qui auront accès à Community. Utilisez le flux de travail de configuration du site et les modules suivants pour configurer le site :

- **Paramètres du système** : l'endroit où vous pouvez configurer les options, les paramètres par défaut et les préférences sur l'ensemble du site.
- **Configurateur de site** : l'endroit où vous pouvez créer une représentation virtuelle de votre site dans Community. Ajoutez des bâtiments, des étages, des points d'accès et des ascenseurs.
- **Gestion des accès** : l'endroit où vous pouvez ajouter les identifiants disponibles à encoder sur les clés Systèmes ou les clés du personnel/prestataire. Vous pouvez également configurer des espaces communs à accès restreint et configurer et affecter des horaires aux identifiants et/ou aux points d'accès individuels.
- **Gestion des périphériques** : l'endroit où vous pouvez configurer des encodeurs. Si vous disposez d'une licence pour la communication en ligne, vous pouvez également utiliser des passerelles et des points d'accès assignés.
- **Programmation et audit** : l'endroit où vous pouvez accéder à la fonction de transfert de données requises pour programmer et auditer des serrures. Si la communication en ligne est activée, vous pouvez également réaliser l'audit des points d'accès en ligne.
- **Gestion des notifications** : l'endroit où vous pouvez créer des groupements logiques de notifications auxquels les opérateurs peuvent s'abonner. Le module n'est actif que si vous disposez d'une licence pour la communication en ligne.
- **Gestion des rôles** : l'endroit où vous pouvez créer et configurer des rôles d'opérateur et les droits associés.

- **Gestion du personnel/prestataire** : l'endroit où vous pouvez ajouter des membres du personnel et configurer les opérateurs.

Mise en service

La phase de mise en service commence lorsque la configuration du site est terminée et que vous commencez à effectuer des tâches quotidiennes telles que l'ajout et la création de clés pour le personnel et les résidents. Utilisez les modules Community suivants pour effectuer les tâches quotidiennes :

- **Gestion des résidents** : l'endroit où vous pouvez gérer les résidents, configurer l'accès des résidents et encoder les clés de résidents.
- **Gestion du personnel/prestataire** : l'endroit où vous pouvez créer et gérer les profils du personnel/prestataire, remplacer les clés du personnel/prestataire et annuler les clés du personnel/prestataire.
- **Clés du personnel/prestataire** : l'endroit où vous pouvez créer des clés pour le personnel/les prestataires.
- **Programmation et audit** : l'endroit où vous pouvez reprogrammer et auditer les serrures. Si la communication en ligne est activée, vous pouvez également réaliser l'audit des points d'accès en ligne.
- **Clés Système** : l'endroit où vous pouvez encoder des clés à fonction spéciale.
- **Surveillance** : l'endroit où vous pouvez vérifier l'état de toutes les clés créées dans Community. Si vous disposez d'une licence pour la communication en ligne, vous pouvez également surveiller les opérations, les événements et l'état des points d'accès assignés.
- **Rapports** : l'endroit où vous pouvez générer des rapports actuels et historiques pour chaque aspect de votre site.

Accès aux fonctionnalités Community

Les fonctionnalités et options qui s'affichent dans Community dépendent des droits sélectionnés pour le rôle attribué à l'opérateur actif. Par exemple, si l'opérateur actuellement connecté ne dispose pas des droits d'accès au module Configurateur de site, le module ne s'affiche pas. De même, si le seul droit sélectionné dans la catégorie de droits de clé de bascule *ELO* (verrouillage électronique) est *Créer clé supplémentaire*, la seule fois qu'*ELO* est affiché comme option lors de la sélection de la catégorie d'identifiants est lorsque l'opérateur crée une clé supplémentaire.

Configuration

Cette section comprend les sujets suivants :

- Flux de travail de configuration du site 13
- Configurer les paramètres du système 14
- En savoir plus sur les paramètres du système 15
- Paramètres généraux 19
- Paramètres de gestion des résidents 20
- Paramètres de sécurité 21
- Paramètres de la clé du personnel/prestataire 32
- Paramètres des Clés à sécurité intégrée 33
- Paramètres d'expiration de la clé 34
- Paramètres de configuration de la messagerie électronique 36
- Paramètres de sauvegarde de la base de données 37
- Paramètres de gestion des visiteurs 41
- Paramètres de l'interface du système d'accès 43
- API Community 44
- Paramètres avancés 46
- Paramètres de licence 50
- Configurez votre site 51
- En savoir plus sur le configurateur de site 52
- Ajouter des bâtiments 58
- Ajouter des étages 59
- Ajouter des unités 62
- Ajouter des suites 66
- Ajouter des espaces communs pour les résidents 70
- Ajouter des espaces communs pour le personnel 76
- Ajouter des accès privés 82
- Ajouter des ascenseurs 84

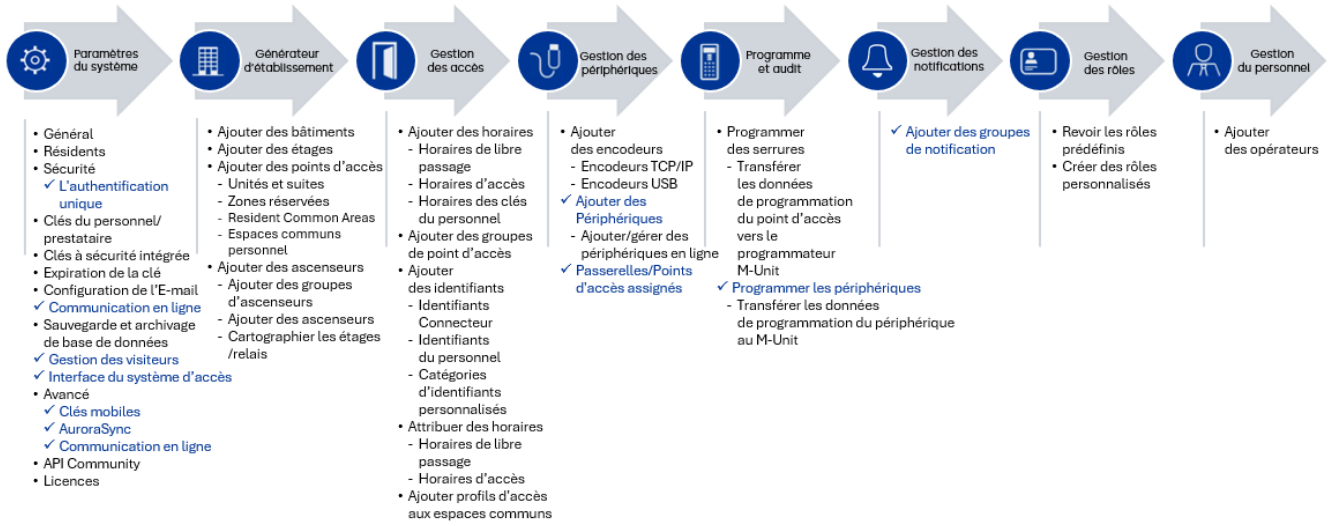
Configurer l'accès 88
En savoir plus sur la gestion des accès 89
Ajouter des horaires de libre passage 93
Ajouter des horaires d'accès 95
Ajouter les horaires des clés du personnel 98
Créer des groupes de points d'accès 100
Ajouter des identifiants 102
Attribuer des horaires 106
Configurer les profils d'accès aux espaces communs à accès limité 107
Configurer des périphériques 111
En savoir plus sur la gestion des périphériques 112
Ajouter des encodeurs 114
Programmer des serrures 117
En savoir plus sur la Programmation et audit 118
Programmer des serrures 121
Examiner et personnaliser les rôles 123
En savoir plus sur la gestion des rôles 124
Consulter les rôles prédéfinis 126
Configurer les rôles personnalisés 127
Ajouter des opérateurs 128
En savoir plus sur la gestion du personnel/prestataries 129
Configurer les opérateurs 131
Importer la liste des membres du personnel/prestataires 136

Flux de travail de configuration du site

Le flux de travail de configuration du site Community fournit un aperçu du processus de configuration du site recommandé. Chaque étape correspond à u module Community. Examinez le processus avant de commencer. Les fonctionnalités sous licence sont indiquées par une coche.

Reportez-vous au *Questionnaire sur la conception du site et la configuration des systèmes* pour connaître les décisions de déploiement consignées par les principales parties prenantes de votre équipe.

Flux de travail de Community



Après la configuration du site, n'oubliez pas de ...

- Accéder à ***Paramètres du système > Sauvegarde de la base de données*** pour configurer les sauvegardes régulièrement programmées et la conservation des données pour la base de données SQL Server Community (et MongoDB pour les systèmes en ligne). Il est recommandé de stocker les sauvegardes dans un emplacement externe sécurisé.
- Accédez à ***Paramètres du système > Clés à sécurité intégrée*** pour créer des clés de rechange.
- Si la licence ne comprend pas le stockage des PPK/SPK, accédez à **Clés Système** pour créer des clés de programmation primaire et secondaire. Conservez les clés dans un endroit sûr.

Étape 1

Configurer les paramètres du système

Cette section comprend les sujets suivants :

En savoir plus sur les paramètres du système 15
Paramètres généraux 19
Paramètres de gestion des résidents 20
Paramètres de sécurité 21
Paramètres de la clé du personnel/prestataire 32
Paramètres des Clés à sécurité intégrée 33
Paramètres d'expiration de la clé 34
Paramètres de configuration de la messagerie électronique 36
Paramètres de sauvegarde de la base de données 37
Paramètres de gestion des visiteurs 41
Paramètres de l'interface du système d'accès 43
API Community 44
Paramètres avancés 46
Paramètres de licence 50

En savoir plus sur les paramètres du système

Paramètres du système est le module Community dans lequel vous pouvez définir les préférences du système et les valeurs par défaut des options globales. Dans certains cas, les options de Paramètres du système contrôlent si des fonctionnalités Community sont activées et leur mode de fonctionnement. Par exemple, si les clés mobiles ne sont pas activées dans les **Paramètres du système**, l'option permettant de créer des clés mobiles n'est pas proposée lors du processus de création des clés.

Configurer les paramètres du système

Pour configurer les paramètres du système :

- Accédez au module **Paramètres du système** et indiquez les paramètres pour chaque catégorie.

Configurer les valeurs par défaut du système et activer les options sous licence. Pour une configuration de site plus efficace, Community renseigne les valeurs recommandées ou modérées pour la plupart des paramètres du système. Bien que ce soit une bonne idée de revoir tous les paramètres du système, vous avez la possibilité d'utiliser les paramètres par défaut du système.

Catégories de paramètres du système

Vous pouvez spécifier des paramètres pour les catégories suivantes.

Général

Définir les informations de base du site et activer l'ouverture forcée pour la validation du numéro de téléphone/téléphone portable. À l'exception du nom du site et de l'image du site, tous les paramètres ont des valeurs par défaut du système. Aucune des options de cette catégorie ne nécessite une attention particulière.

Résidents

Configurez les valeurs par défaut pour le module Gestion des résidents. Tous les paramètres ont des valeurs par défaut du système. Toutefois, si vous prévoyez de contrôler l'accès aux ascenseurs, l'option **Afficher l'accès aux étages** requiert une attention particulière.

Sécurité

Configurer les paramètres relatifs à la sécurité du compte et à l'accès aux serrures, désactiver/activer le mode de sécurité renforcée, obtenir le mot de passe de sécurité du programmateur M-Unit lorsque le mode de sécurité renforcée est activé, activer l'authentification du certificat client API et configurer les options de certificat du navigateur. Les situations suivantes nécessitent une configuration manuelle :

- désactiver l'authentification pour l'Intégration API
- désactiver l'authentification pour les comptes Programmateur M-Unit
- activer la validation du certificat du client pour les requêtes API
- activer/désactiver le mode de sécurité renforcée

Les fonctions sous licence suivantes sont également accessibles :

- Authentification unique – Permet d'activer et de configurer l'authentification unique.

Clés du personnel/prestataire

Configurez le nombre de fois qu'une **Clé à usage restreint** peut être utilisée, désactivez le mode bascule pour les clés d'accès variables des unités, et choisissez d'afficher ou non le menu pour ajouter des espaces communs lors de la création des clés du personnel/prestataire. Vous pouvez également activer les clés d'urgence. Les valeurs par défaut sont renseignées. Toutefois, cette catégorie requiert une attention particulière si vous souhaitez modifier les valeurs par défaut.

Clés à sécurité intégrée

Configurer les valeurs par défaut des options de la clé à sécurité intégrée. Les clés à sécurité intégrée sont des clés de rechange pour les chambres créées à l'avance et conservées en jeux complets à remettre en cas de panne du système ou de courant. Il est recommandé de créer deux jeux de trois clés pour chaque porte d'unité et de suite.

Expiration de la clé

Configurer la date d'expiration de la clé par défaut pour tous les types de catégories d'identifiants et de clés. Lors de la création d'une clé du personnel/prestataire ou d'une clé système, la date d'expiration par défaut est basée sur le calcul utilisant les valeurs spécifiées ici.

E-mail

Configurez les paramètres utilisés pour envoyer des e-mails au personnel. Aucun défaut système n'est renseigné. Cette catégorie requiert une attention particulière afin que Community puisse envoyer des e-mails et des notifications automatiques au personnel.

Configurez les paramètres utilisés pour envoyer des e-mails aux membres du personnel/prestataires. Aucun défaut système n'est renseigné. Cette catégorie requiert une attention particulière afin que Community puisse envoyer des e-mails et des notifications automatiques au personnel/aux prestataires.

Communication en ligne

La communication en ligne est une fonction sous licence qui est désactivée par défaut.

Personnalisez les paramètres de la communication en ligne. Parmi les paramètres que vous pouvez configurer, vous pouvez notamment définir les intervalles de mise à jour pour les passerelles et les intervalles de réveil pour les points d'accès assignés. Vous pouvez également définir si le réseau de passerelle utilise une adresse IP dynamique ou statique pour la communication. Enfin, vous pouvez personnaliser les paramètres qui déclenchent les notifications d'alerte d'intrus et activent Rx-Link.

Sauvegarde de la base de données

dormakaba recommande vivement de programmer des sauvegardes automatiques sur un serveur distant et de conserver les copies de sauvegarde et les données archivées dans un endroit sûr hors site.

Les sauvegardes de base de données constituent la priorité absolue pour la préparation aux catastrophes. En cas de perte ou de corruption des données, les sauvegardes permettent de restaurer entièrement la base de données SQL Server Community et, lorsque la communication en ligne est activée, la base de données MongoDB. Si la base de données SQL Server n'est pas sauvegardée, vous perdez toutes les données Community et devrez reconfigurer l'ensemble du site, y compris recréer les points d'accès et programmer les serrures. Si la base de données MongoDB n'est pas sauvegardée, vous perdez toutes les données relatives à la communication en ligne et devrez reconfigurer l'ensemble de l'environnement en ligne, y compris reconfigurer chaque passerelle et assigner les serrures aux passerelles.

La purge et l'archivage des bases de données permettent de conserver un espace mémoire suffisant sur le serveur Community en supprimant ou en extrayant les enregistrements historiques des tableaux présentant un grand volume de données, tels que le tableau Activité système. Si la purge et l'archivage ne sont pas activés, la base de données va croître jusqu'à la limite du système et l'espace pourrait être indisponible pour le fonctionnement normal. La purge est réalisée comme prévu avant l'archivage. Comme l'archivage se produit comme prévu immédiatement après la sauvegarde, les sauvegardes doivent être configurées avant que l'archivage puisse être activé.

Consultez le tableau suivant pour obtenir des détails sur la sauvegarde/l'archivage.

Protection des	Emplacement de stockage	Option de sauvegarde	Fréquence	Conservation
SQL Server	Répertoire spécifié (local ou distant) Valeur par défaut : C:\Program Files\Microsoft SQL Server\MSSQL16.COMMUNITY\MSSQL\Backup Valeur par défaut pour les mises à niveau : les paramètres existants sont conservés	À la demande	À la demande	Sauvegarde actuelle
		Par horaire	Par horaire	Par réglage
Clé symétrique RGPD	ProgramData\DormaKaba\Community\Backup (local uniquement)	Selon la politique du site		
MongoDB	Dossier MongoDB dans le répertoire spécifié (local uniquement) Valeur par défaut pour les nouvelles installations et les mises à niveau avec SQL Server distant : aucune Valeur par défaut pour les mises à niveau avec SQL Server local : les paramètres existants sont conservés	Par horaire	Par horaire	Dernière sauvegarde
Archive	Répertoire spécifié (local autorisé mais disque dur externe, lecteur réseau ou serveur distant recommandé) Valeur par défaut : C:\Program Files\dormakaba\Community Server\Archive Valeur par défaut pour les mises à niveau : les paramètres existants sont conservés	Par horaire	Par horaire	Indéfini

Conformément au RGPD (Règlement général sur la protection des données), toutes les PII (informations personnelles identifiables) stockées dans la base de données sont cryptées. Lors d'une sauvegarde (à la demande ou programmée), la clé de cryptage spécifique au site est sauvegardée sur le serveur Community dans le répertoire \ProgramData\DormaKaba\Community\Backup. La clé est requise pour restaurer la base de données.

Gestion des visiteurs

La gestion des visiteurs est une fonction gratuite qui fonctionne exclusivement avec AuroraSync et les clés mobiles. La gestion des visiteurs permet aux résidents et au personnel d'étendre tout ou partie de leur accès aux visiteurs sur site. En utilisant l'application BlueSky dormakaba, les résidents et le personnel peuvent générer des codes PIN pour autoriser l'accès au périmètre et aux espaces communs. Les résidents ont également la possibilité d'attribuer aux visiteurs des clés mobiles qui peuvent être utilisées pour les portes communes et l'unité du résident, si souhaité.

- Un code PIN est une séquence à 7 chiffres qui peut être utilisée sur les points d'accès où un clavier numérique est installé.
- Une clé mobile attribuée (ou un code PIN au format clé mobile) permet l'accès à l'aide de l'application BlueSky dormakaba.

Lorsque Gestion des visiteurs est activée dans Paramètres du système pour le personnel/les prestataires, l'attribution de codes PIN peut être activée/désactivée dans l'onglet Gestion des visiteurs des profils du personnel/prestataire. Lorsque Gestion des visiteurs est activée dans Paramètres du système pour les résidents, l'attribution de codes PIN et de clés mobiles peut être activée/désactivée dans l'onglet Gestion des visiteurs des profils de résidents.

Les prérequis sont les suivants :

- AuroraSync doit être activé et configuré.
- Les clés mobiles doivent être activées et configurées.
- Le profil du résident et/ou du membre du personnel doit comporter un numéro de téléphone portable valide.
- L'application BlueSky dormakaba doit être installée et enregistrée sur le périphérique mobile utilisé pour générer le code PIN/la clé mobile.

Avancé

Modifier les paramètres technologiques des clés et activer les espaces communs étendus. Pour plus d'informations, voir « En savoir plus sur le configurateur de site » sur la page d'accueil d'aide.

Les fonctions sous licence suivantes sont également accessibles :

- Clés mobiles — Activer les clés mobiles.
- Communication en ligne — Activer la communication en ligne. Pour plus d'informations, voir « Utilisation de la communication en ligne » sur la page d'accueil d'aide.
- AuroraSync — Pour plus d'informations, voir *Intégration Community Aurora* (PK3768).

Interface du système d'accès

L'interface du système d'accès est une fonction sous licence désactivée par défaut. Activez et configurez un système d'accès tiers pour étendre les options de gestion des accès des résidents. L'interface donne à tout système d'accès tiers la possibilité de s'intégrer à la Gestion des résidents dans Community. OATH (Open Authentication) exige que les tiers fournissent les paramètres requis pour générer un jeton de sécurité.

API Community

Activez et configurez l'API REST Community et la notification de remise de clés. Utilisez l'API REST pour les connexions au Web Service sécurisées avec une authentification par jeton. Pour plus de détails sur l'API, procurez-vous les spécifications *API REST Community* (PK3781) auprès d'un technicien du support dormakaba. La notification de remise de clés envoie une notification distincte pour chaque clé remise à partir de l'interface utilisateur et de l'API REST Community.

Licences

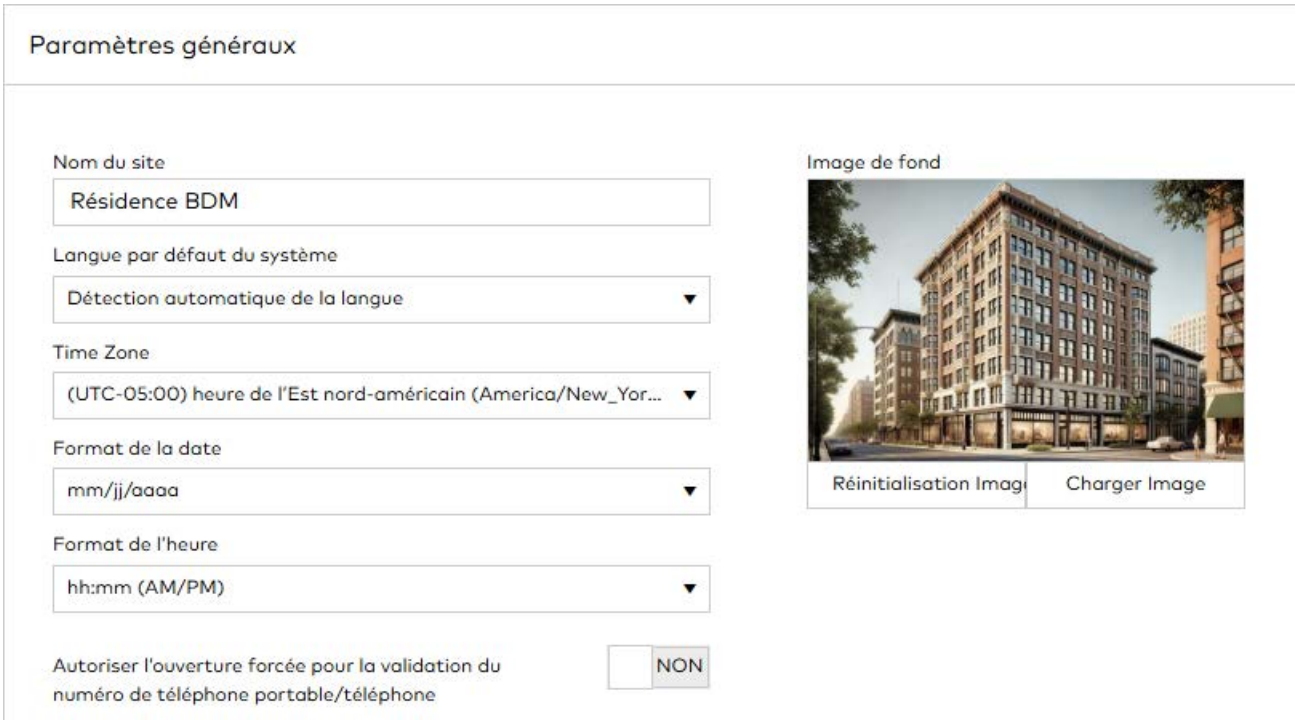
Modifiez la clé d'activation pour activer ou désactiver des fonctionnalités Community. Les fonctionnalités sous licence comprennent :

- Clés mobiles
- Clés d'urgence
- Communication en ligne
- Gestion des visiteurs
- Intégrations de tiers
- Stockage des PPK/SPK — Cette option permet de sauvegarder les PPK/SPK (Clé de programmation primaire/Clé de programmation secondaire) du site en les stockant dans l'application interne sécurisée utilisée pour gérer les licences chez dormakaba. En cas de corruption de la base de données ou d'échec total, la sauvegarde des PPK/SPK peut être utilisée pour reprogrammer les serrures et/ou reconfigurer la base de données Community.
- Authentification unique (SSO)

Paramètres généraux

Configurer des paramètres de site de base.

1. Accédez à ***Paramètres du système > Général***.



2. Pour le **Nom du site**, indiquez le nom du site. Caractères max. : 30. Le nom du site apparaît dans les rapports. Valeur par défaut : Mon site.
3. Pour la **Langue par défaut du système**, sélectionnez la langue par défaut de l'interface utilisateur. La valeur par défaut consiste à détecter la langue du navigateur. L'interface utilisateur s'affiche dans la langue sélectionnée jusqu'à ce qu'une langue préférée soit sélectionnée dans **Préférences**. La langue sélectionnée dans **Préférences**est prioritaire.
4. Pour **Fuseau horaire**, sélectionnez le fuseau horaire à utiliser pour la programmation des serrures et l'encodage des clés. Pour modifier le fuseau horaire, il faut reprogrammer tous les points d'accès et recréer/réémettre toutes les clés. La valeur par défaut correspond au fuseau horaire du serveur Community.
5. Pour le **Format de la date**, sélectionnez le format pour afficher des dates sur l'ensemble du site. Valeur par défaut : jj/mm/aaaa.
6. Pour le **Format de l'heure**, sélectionnez le format pour afficher l'heure sur l'ensemble du site. Valeur par défaut : hh:mm (et si disponible, AM/PM).
7. **Autoriser l'ouverture forcée pour la validation du numéro de téléphone portable/téléphone** — Sélectionnez **OUI** pour autoriser les numéros de téléphone portable/téléphone qui ne sont pas reconnus. Lors de la saisie d'une valeur pour un numéro de téléphone dans les profils des résidents et du personnel/prestataire, vérifiez si la chaîne est conforme aux normes internationales connues. Si la chaîne n'est pas reconnue, la valeur ne peut pas être sauvegardée. (Le problème le plus courant est un indicatif régional non reconnu.) L'option permettant de contourner la validation permet aux opérateurs de sauvegarder des numéros de téléphone qui ne répondent pas aux normes connues Valeur par défaut : NON.
8. Pour l'**Image de fond**, cliquez sur **Charger une image**, accédez à une image, sélectionnez-la, puis cliquez sur **Ouvrir**. Types de fichiers pris en charge : gif, jpg, png. L'image sélectionnée s'affiche sur la page d'accueil de Community.
9. Cliquez sur **(Sauvegarder)**.

Paramètres de gestion des résidents

Configurez les valeurs par défaut pour tout le système pour le module **Gestion des résidents**.

1. Accédez à Paramètres du système.
2. Cliquez sur **Résidents**.



3. Pour le **nombre de clés de résidents par défaut** — Indiquez la valeur par défaut pour le nombre de clés à créer lors de la création de clés d'accès pour les résidents. Valeurs valides : 1-10. Valeur par défaut : 2.
4. Pour l'**expiration de la clé par défaut**, cliquez sur -/+ pour sélectionner le nombre d'années et de jours utilisés pour le calcul de la date d'expiration automatiquement ajoutée lors de la création de la clé. Valeur par défaut : 1 an, 0 jour.
5. Pour **afficher les détails du message**, sélectionnez si vous souhaitez que le système affiche les messages concernant la création des clés pour les résidents. Valeur par défaut : OUI.

   Veuillez procéder avec prudence lorsque vous décidez de ne pas afficher les détails du message. Lorsque des modifications des accès sont effectuées, ces messages affichent la liste des noms des résidents pour lesquels des clés doivent être créées. Ces rappels sont très utiles lorsque des résidents partagent des accès. Si vous ne créez pas les clés comme indiqué par les messages d'avertissement, les clés de résidents peuvent être invalides et empêcher l'accès.

6. Pour **afficher l'accès aux étages**, sélectionnez si vous souhaitez afficher la section ACCÈS AUX ÉTAGES dans les profils des résidents dans Gestion des résidents. Par défaut, les résidents ont accès par ascenseur aux étages sur lesquels des unités leur sont affectées. Lorsque la section ACCÈS AUX ÉTAGES est affichée dans les profils des résidents, des accès à des étages supplémentaires peuvent être activés. Valeur par défaut : NON.
7. Pour **activer l'ouverture forcée du pêne dormant/verrou d'intimité pour les clés des résidents** — Choisissez si les Clés des résidents peuvent forcer l'ouverture du pêne dormant/verrou d'intimité pour les portes d'une unité et d'une unité de suite. Si vous modifiez ce paramètre, les points d'accès devront peut-être être reprogrammés. Valeur par défaut : OUI.
8. Cliquez sur (Sauvegarder).

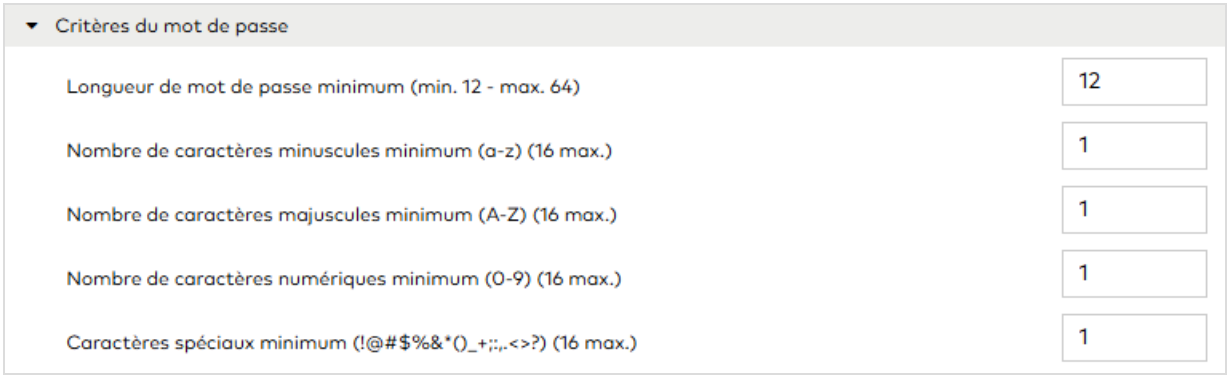
Paramètres de sécurité

Les paramètres de sécurité protègent l'accès au compte. Tous les paramètres de cette catégorie (sauf **PCI-DSS**) sont renseignés avec des valeurs recommandées ou modérées.

Tous les exemples de valeurs sur les figures reflètent les valeurs par défaut du système.

1. Accédez à ***Paramètres du système > Sécurité***.
2. Indiquer les options. Pour en savoir plus, reportez-vous aux sections ci-dessous.
3. Cliquez sur **(Sauvegarder)**.

Critères du mot de passe



- **Longueur de mot de passe minimum** — Indiquez le nombre minimum de caractères dans les mots de passe de compte Community. Valeurs valides : 12-64.
- **Nombre de caractères minuscules minimum** — Indiquez le nombre minimum de caractères en minuscules dans les mots de passe de compte Community. Valeurs permises : a-z (maximum : 16).
- **Nombre de caractères majuscules minimum** — Indiquez le nombre minimum de caractères en majuscules dans les mots de passe de compte Community. Valeurs valides : A-Z (maximum 16).
- **Nombre de caractères numériques minimum** — Indiquez le nombre minimum de caractères numériques dans les mots de passe de compte Community. Valeurs valides : 0-9 (maximum 16).
- **Caractères spéciaux minimum** — Indiquez le nombre minimum de caractères spéciaux dans les mots de passe de compte Community. Valeurs valides : !@#$%&*()_+;:,.<>? (maximum 16).

Expiration du mot de passe



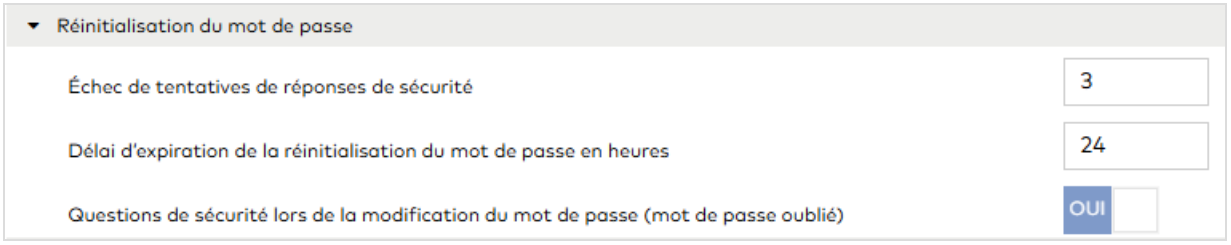
- **Jours avant expiration du mot de passe** — Indiquez le nombre de jours après lesquels le mot de passe pour un compte Opérateur expire. Valeurs valides : 1-90.
- **Activer la notification d'expiration du mot de passe** — Choisissez d'avertir ou non les Opérateurs lorsque leur mot de passe arrive à expiration. Valeur recommandée : OUI.
- **Jours de notification avant expiration** — Indiquez le nombre de jours avant l'expiration d'un mot de passe pour l'affichage d'une notification quotidienne après la connexion de l'Opérateur. Valeurs valides : 5-30.

Historique des mots de passe



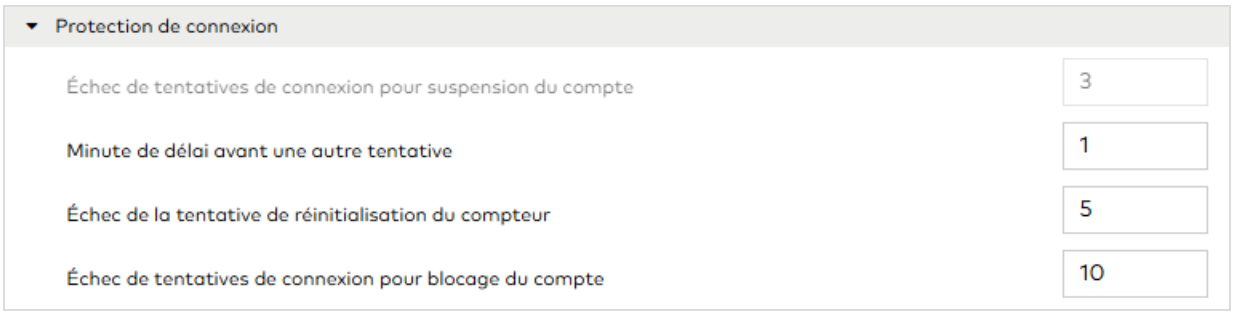
- **Nombre de mots de passe précédents à vérifier**— Indiquez le nombre de mots de passe les plus récents à vérifier lorsqu'un Opérateur crée un nouveau mot de passe. Le nouveau mot de passe ne doit être identique à aucun des mots de passe précédents contrôlés. Valeurs valides : 4-30.

Réinitialisation du mot de passe



- **Échec de tentatives de réponses de sécurité** — Indiquez le nombre de mauvaises réponses d'un Opérateur à la question de sécurité avant que le compte ne soit bloqué. Valeurs valides : 1-10.
- **Délai d'expiration de la réinitialisation du mot de passe en heures** — Indiquez le nombre d'heures de validité d'un lien envoyé en réponse à une demande de réinitialisation du mot de passe. Valeur par défaut : 24. Valeurs valides : 1-24.
- **Questions de sécurité lors de la modification du mot de passe (mot de passe oublié)** — Choisissez d'inviter ou non l'Opérateur à répondre à des questions en cas de demande de réinitialisation du mot de passe. Valeur recommandée : OUI.

Protection de connexion



- **Échec de tentatives de connexion pour suspension du compte** — Indiquez le nombre de tentatives de connexion échouées avant le blocage temporaire du compte Community. Les comptes suspendus sont bloqués pour le nombre de minutes indiquées dans **Minute de délai avant une autre tentative**. Valeurs valides : 3-30.
- **Minute de délai avant une autre tentative**Indiquez le nombre de minutes de suspension d'un compte. Valeurs valides : 1-30.
- **Échec de la tentative de réinitialisation du compteur** — Indiquez le nombre de minutes de suspension d'un compte lorsque le **Échec de tentatives de connexion pour suspension du compte** est atteint. Valeurs valides : 1-30.
- **Échec de tentatives de connexion pour blocage du compte** — Indiquez le nombre de tentatives de connexion échouées avant le verrouillage du compte Community. Lorsque le seuil est atteint, l'Opérateur ne peut plus se connecter sans l'assistance d'un administrateur. Valeurs valides : 1-10.

Inactivité du compte



- **Seuil d'inactivité pour blocage du compte (jours)** — Indiquez le nombre de jours avant le verrouillage d'un compte en cas d'absence de connexion. Lorsque le seuil est atteint, l'Opérateur ne peut plus se connecter sans l'assistance d'un administrateur. Valeurs valides : 1-90.

Inactivité de la session



- **Seuil d'inactivité pour déconnexion de session (en minutes)** — Indiquez le nombre de minutes au bout desquelles une session Community active prend fin pour absence d'activité. Lorsque le seuil est atteint, l'opérateur doit se connecter à nouveau. Valeurs valides : 1-15.

Programmateur M-Unit



- Choisissez de demander ou non une authentification de M-Unit (Programmateur M-Unit). Lorsque l'authentification est activée, les identifiants de M-Unit sont requis pour programmer et auditer des serrures. Configurez les identifiants pour au moins un opérateur dans Gestion du personnel/prestataire. Valeurs par défaut : OUI, 1 jour et 0 heure.
- Indiquez le nombre de jours et d'heures après lesquels les données du programmateur M-Unit ne pourront plus être transférées. Valeur par défaut : 1 jour, 0 heure.

Intégration API

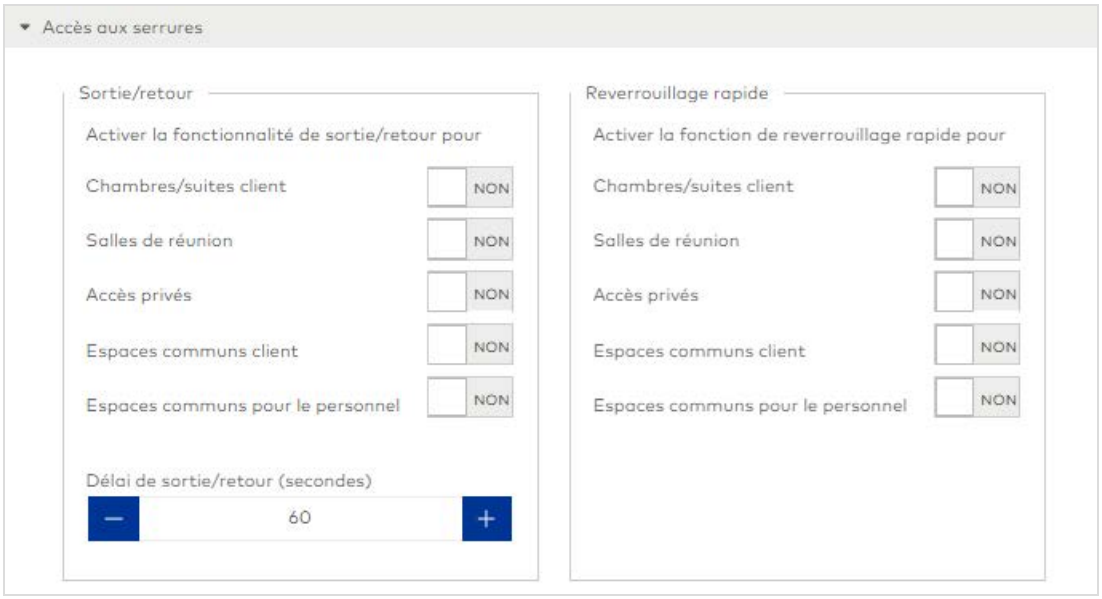


- Choisissez de demander ou non une authentification pour les requêtes API. Lorsque l'authentification est activée, les requêtes API ne sont pas traitées tant que le nom d'utilisateur et le mot de passe indiqués dans la requête n'ont pas été authentifiés en fonction du **nom d'utilisateur et du mot de passe de** connexion à l'API configurés dans **Gestion du personnel/prestataire**. Requis pour le mode de sécurité renforcée. Valeur par défaut : OUI.
- **Valider le certificat client** — Sélectionnez si le certificat du client doit être validé pour chaque requête API (API SOAP Community ou API REST Community). Requis pour la validation de l'expiration du certificat. Lorsque ce paramètre est modifié, Community réinitialise la connexion API. Valeurs par défaut : OUI pour les nouvelles installations ; NON pour les mises à niveau.

- **Valider l'expiration du certificat** — Sélectionnez si l'expiration du certificat doit être validée pour chaque requête API (API SOAP Community ou API REST Community). Si le réglage est OUI et que le certificat est expiré, les requêtes API ne sont pas traitées. **Valider le certificat client** doit être réglé sur OUI. Valeur par défaut : OUI.
- **Générer un nouveau certificat** — (API SOAP Community ou API REST Community) Un certificat est créé automatiquement pour les nouvelles installations. Cliquez pour générer un certificat valable un an. Community génère le certificat indépendamment de la validité ou de l'expiration du certificat actuel. Les certificats sont enregistrés dans les dossiers Personal et Trusted Root Certification Authorities sur la machine locale. Pour plus de détails sur l'exportation/importation du certificat, voir la documentation de l'API.

Accès aux serrures

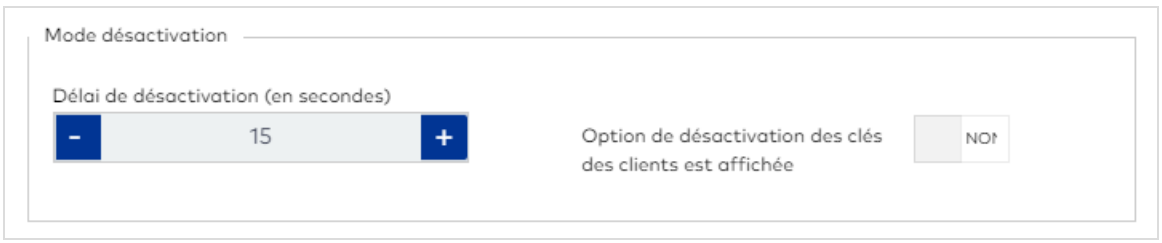
Toute modification des paramètres de cette section peut nécessiter une reprogrammation des points d'accès concernés.



- **Sortie\retour** — Pour chaque type de point d'accès, indiquez si vous souhaitez autoriser une période de grâce pendant laquelle une serrure reste accessible sans clé si la porte est ouverte puis fermée de l'intérieur. Si un point d'accès est activé pour la sortie/retour, spécifiez le nombre de secondes pendant lesquelles la serrure reste accessible. Valeurs par défaut : NON / 60. Valeurs valides : 20-300 (par incréments de 20).
- **Reverrouillage rapide** — Pour chaque type de point d'accès, indiquez si la serrure doit être reverrouillée immédiatement après l'ouverture de la porte. Si le reverrouillage rapide est désactivé, la serrure est reverrouillée 4 secondes après la présentation d'une clé d'accès valide.

Les points d'accès peuvent être programmés à la fois pour la sortie/retour et le reverrouillage rapide. Toutefois, ces paramètres ne sont pas autorisés pour les points d'accès activés en mode bascule.

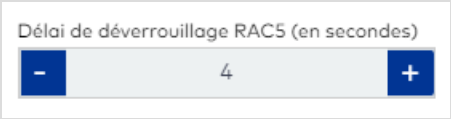
Mode désactivation



- **Délai de désactivation** — Indiquez le nombre de secondes pendant lesquelles le point d'accès doit rester déverrouillé après avoir présenté une clé valide avec l'option de désactivation. Cette option s'applique uniquement lorsque l'option **Afficher la désactivation dans Gestion des résidents** est définie sur **OUI** et que l'option **Activer la désactivation pour les clés de résidents** est sélectionnée lors de la création de clés de résidents. Valeur par défaut : 15. Valeurs valides : 10-60.
- **Afficher l'option de désactivation dans la Gestion des résidents** — Activez ou désactivez l'option permettant d'appliquer le délai de désactivation lors de la création de clés de résidents. Le délai de désactivation ne peut être appliqué aux clés de résidents sans activer cette option. Valeur par défaut : NON.

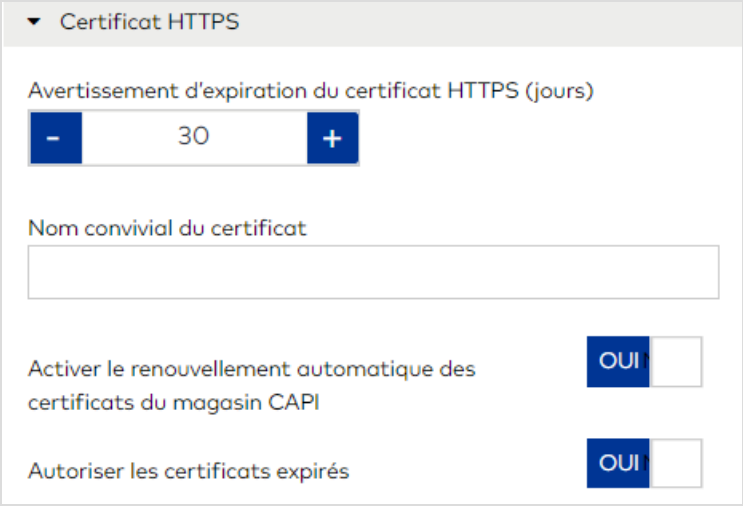
Option RAC5

Les modifications de ce paramètre peuvent nécessiter une reprogrammation des serrures.



- **Délai de déverrouillage** — Indiquez le nombre de secondes pendant lesquelles le point d'accès RAC5 doit rester déverrouillé après avoir présenté une clé valide. Valeur par défaut : 4. Valeurs valides : 4-60.

Certificat HTTPS



Lorsque Community est déployé avec un certificat SSL :

- indiquez le nombre de jours avant l'expiration du certificat pour commencer à recevoir un avertissement quotidien. Valeur par défaut : 30. Valeurs valides : 0-365.

Lorsqu'un certificat du magasin CAPI a été sélectionné lors de l'installation, les options supplémentaires sont disponibles :

- Modifier et sauvegarder le nom convivial du certificat.
- Activer le renouvellement automatique des certificats du magasin CAPI. Lorsque cette option est activée, Community détecte un nouveau certificat basé sur le nom convivial et le lie à nouveau à IIS. La fréquence de détection est d'une heure. La méthode de détection utilise les dates de **début de validité**. Valeur par défaut : NON.
  - Lorsqu'elle est activée, l'option **Ne pas utiliser les certificats expirés** s'affiche. Valeur par défaut : OUI. Lorsqu'il est réglé sur OUI, le certificat du magasin CAPI est ignoré ; lorsqu'il est réglé sur NON, le certificat expiré est utilisé.

Mode de sécurité renforcée

Nouvelles installations

Cette option est désactivée par défaut. Lorsque vous êtes prêt(e), reportez-vous à la section *Activer le mode de sécurité renforcée*.

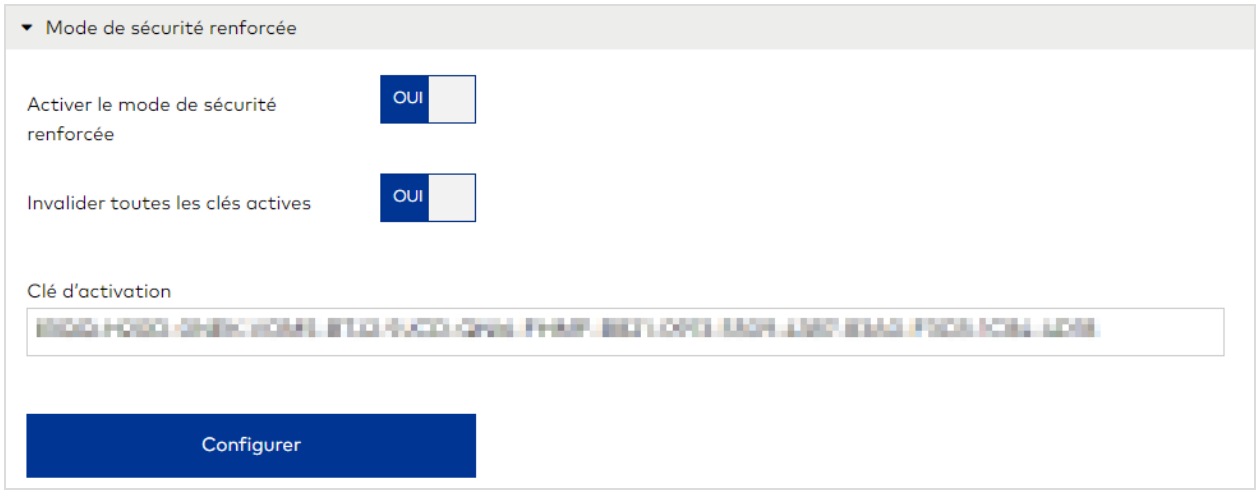
Activation du mode de sécurité renforcée (pour les mises à niveau et lorsqu'il était désactivé auparavant)

Pour obtenir une liste complète des conditions requises et des instructions étape par étape pour activer le mode de sécurité renforcée, reportez-vous à la section *Sécurité renforcée des clés Community* (PK3776).

L'activation de cette option nécessite des encodeurs spécifiques (référence 75720). Au moins un encodeur doit être configuré avant d'activer le mode de sécurité renforcée.

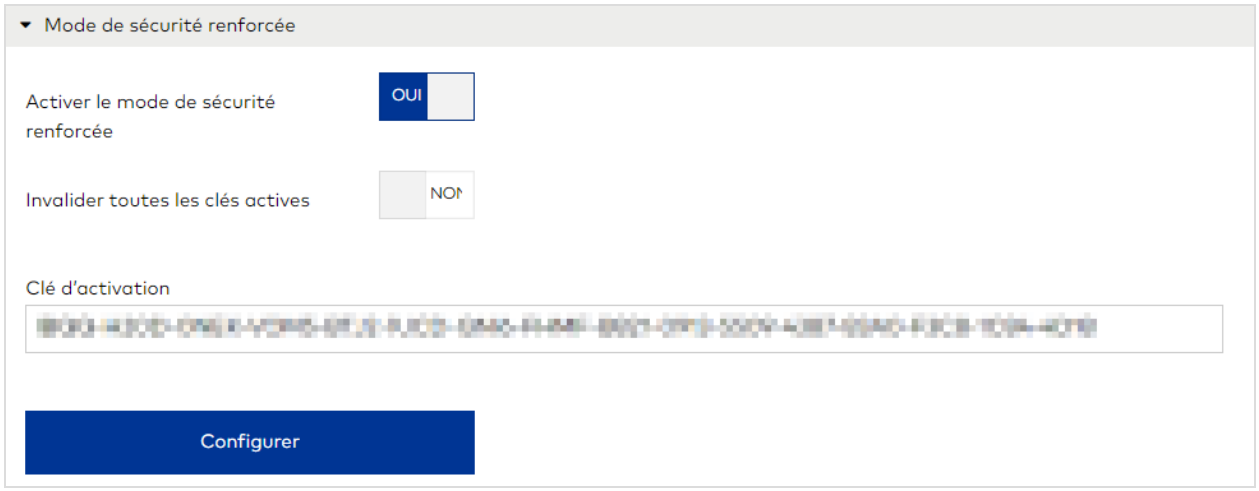
Avant d'activer le mode de sécurité renforcée, obtenez une clé d'activation valide de 64 caractères auprès du support dormakaba. La configuration nécessite que le serveur Community ait accès à l'internet.

1. Placez le commutateur du **Mode de sécurité renforcée** sur **OUI**. Lisez l'avertissement et sélectionnez **OUI** pour continuer.
2. Choisissez d'invalider ou non toutes les clés actives :
   - **OUI** — Vivement recommandé pour Community. Sélectionnez cette option pour commencer à utiliser le mode de sécurité renforcée lors de la reprogrammation des points d'accès.



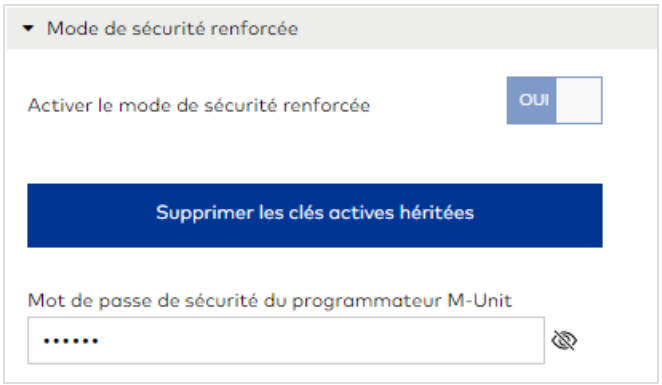
   - **NON** — Sélectionnez cette option pour passer au mode de sécurité renforcée. Les clés actives restent valides jusqu'à ce que la commande de suppression de toutes les clés actives héritées soit émise. dormakaba recommande deux

semaines au maximum pour achever le processus de transition.



3. Indiquez la clé d'activation de 64 caractères.
4. Cliquez sur **Configurer**. Lisez l'avertissement et sélectionnez **OUI** pour continuer. Community configure le site. Le paramètre de mot de passe de sécurité du programmateur M-Unit s'affiche. Si les clés n'ont pas été invalidées à l'étape 2, le bouton **Supprimer les clés actives héritées** s'affiche.

Le mode de sécurité renforcée ne peut pas être désactivé après avoir cliqué sur **Configurer**.



5. Accédez à Clés Système et réencodez les clés à sécurité intégrée.
6. Accédez à Gestion du personnel/prestataire et créez toutes les nouvelles clés RFID pour le personnel/les prestataires actifs.
7. Accédez à Gestion des résidents et créez toutes les nouvelles clés RFID pour les résidents actifs.
8. Accédez à ***Programmation et audit > Programmation*** et reprogrammez les points d'accès. Indiquez le mot de passe de sécurité de M-Unit lorsque vous y êtes invité.
   - Si toutes les clés ont été invalidées à l'étape 2, les serrures n'acceptent que les clés de sécurité renforcée après la reprogrammation.
   - Si les clés n'ont pas été invalidées à l'étape 2, les serrures acceptent les clés de sécurité renforcée et les clés actives héritées après la reprogrammation.
9. Accédez à Gestion du personnel/prestataire et à Gestion des résidents et créez toutes les nouvelles clés BLE pour le personnel/les prestataires et les résidents actifs, respectivement.

Si toutes les clés ont été invalidées à l'étape 2, le processus est terminé. Si les clés n'ont pas été invalidées à l'étape 2, continuez.

10. Lorsque vous êtes prêt à finaliser la transition vers la sécurité renforcée des clés, cliquez sur **Supprimer les clés actives héritées**.
11. Accédez à ***Programmation et audit > Programmation*** et reprogrammez à nouveau les points d'accès. Indiquez le mot de passe de sécurité de M-Unit lorsque vous y êtes invité. Après la reprogrammation, les serrures n'acceptent que les clés de sécurité renforcée.

Authentification unique

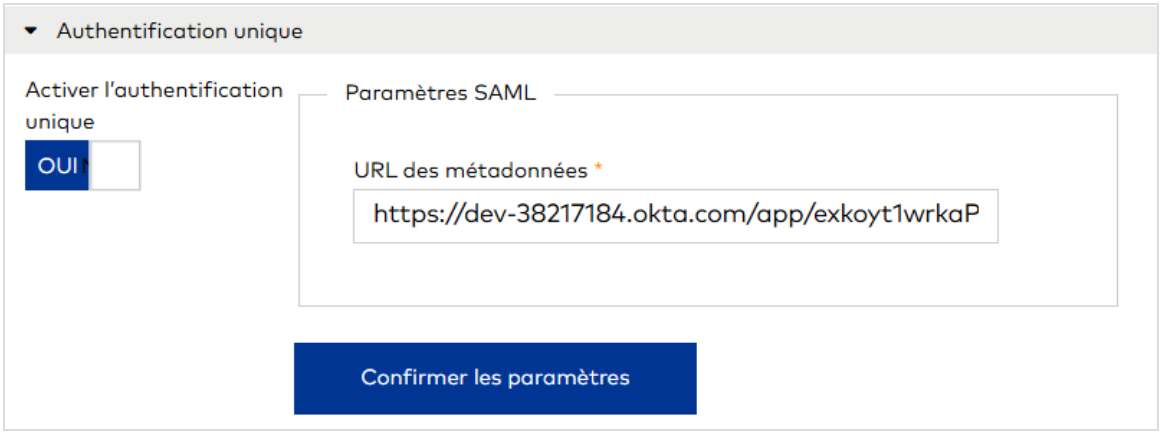
SSO (authentification unique) est une fonction sous licence qui est désactivée par défaut. Certaines valeurs de configuration sont fournies par le support dormakaba. Certaines valeurs, comme indiqué, sont fournies par le fournisseur d'identité.

Activation de SSO

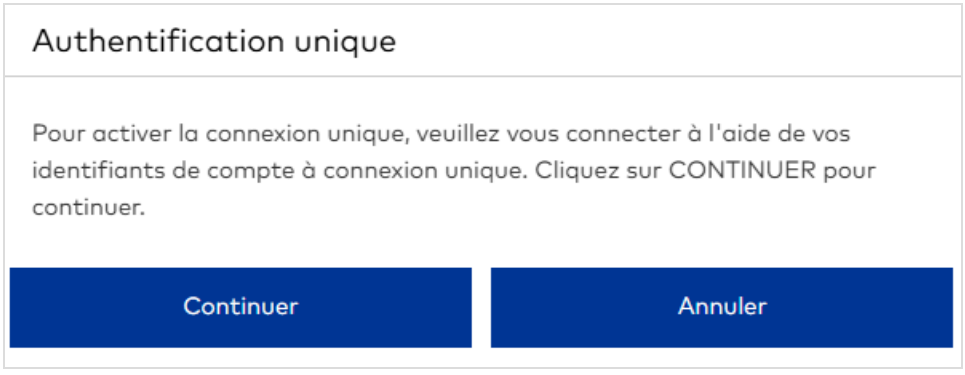
Avant d'activer SSO, il convient d'établir les conditions préalables suivantes :

- Préparez-vous à vous connecter à votre compte SSO pendant le processus de configuration.

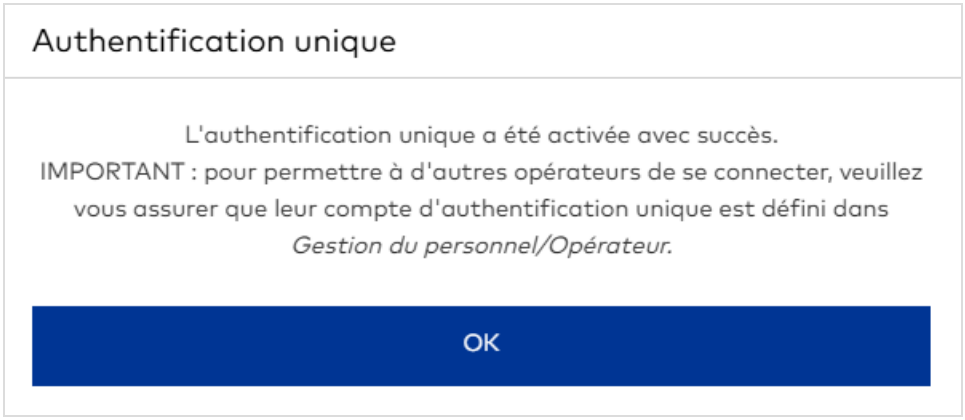
1. Pour activer SSO, placez le commutateur **Activer l'authentification unique** sur **OUI**. Actuellement, seul le protocole d'authentification SAML est pris en charge. SAML utilise le langage XML pour échanger des messages.



2. Pour **URL des métadonnées**, indiquez l'emplacement du document XML contenant des informations de configuration sur le fournisseur d'identité SAML. La valeur est fournie par le fournisseur d'identité.
3. Cliquez sur **Confirmer les paramètres**.



4. Cliquez sur **Continuer**. Community redirige vers la page de connexion du fournisseur d'identité.
5. Connectez-vous à votre compte SSO. L'ID utilisateur pour SSO peut être une adresse e-mail ou un EID (ID d'entreprise). Community sauvegarde les paramètres SSO et met à jour le nom d'utilisateur / l'ID utilisateur de l'opérateur dans Gestion du personnel/prestataire.

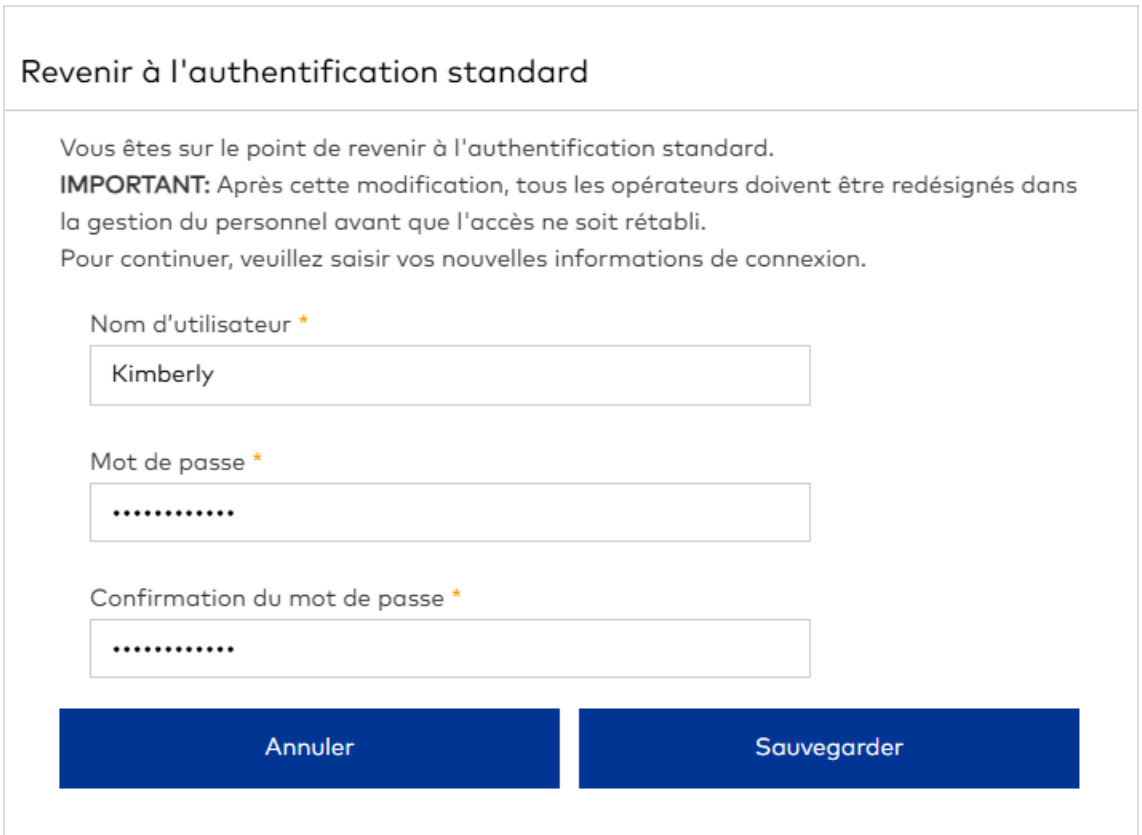


En tant qu'opérateur ayant opté pour SSO, vous êtes désormais le seul opérateur à pouvoir vous connecter à Community. Vous devez maintenant aller dans Gestion du personnel/prestataire et indiquer l'ID utilisateur SSO pour chaque opérateur.

Désactivation de SSO

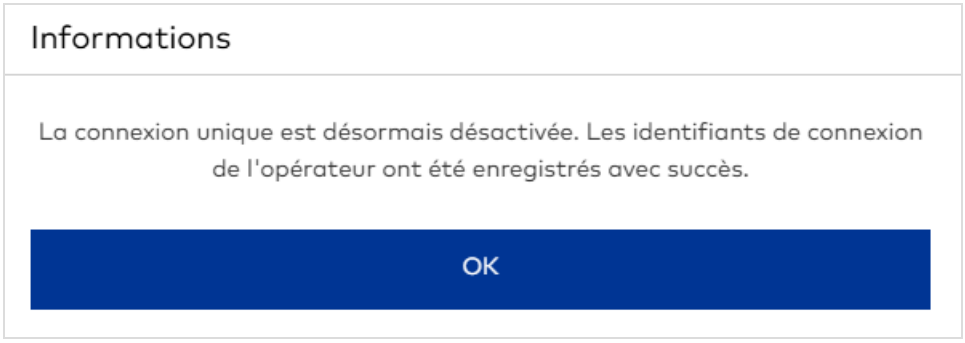
Après avoir pris cette mesure, tous les autres opérateurs perdent leur statut d'opérateur et doivent être redésignés dans Gestion du personnel/prestataire pour rétablir l'accès.

1. Pour désactiver SSO, placez le commutateur **Activer l'authentification unique** sur **NON**.



2. Indiquez un nouveau nom d'utilisateur pour la connexion.
3. Indiquez et confirmez un nouveau mot de passe.

4. Cliquez sur **Sauvegarder**.

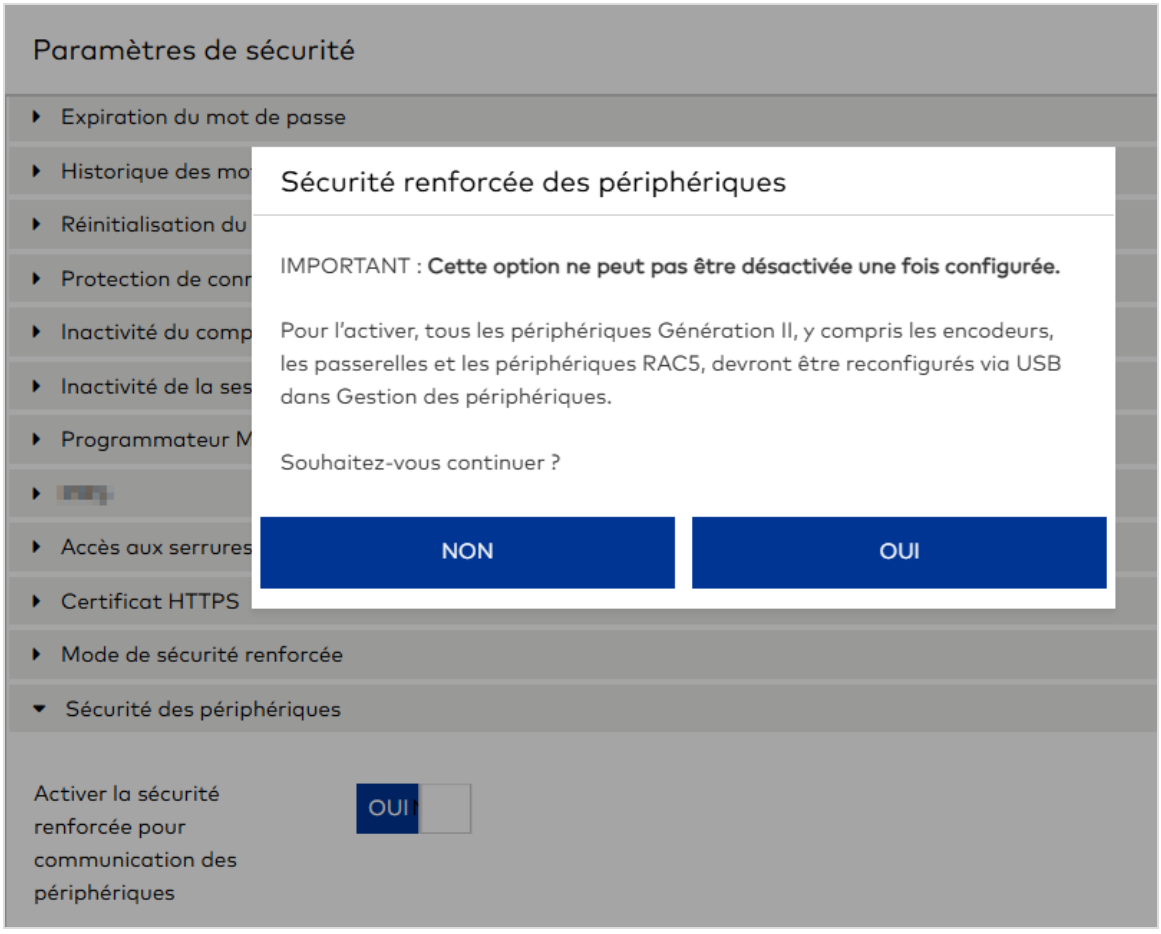


En tant qu'opérateur qui est revenu à l'authentification standard, vous êtes désormais le seul opérateur à pouvoir vous connecter à Community. Vous devez maintenant aller dans Gestion du personnel/prestataire et redésigner les opérateurs.

Sécurité des périphériques

Mises à niveau uniquement. Activez les certificats spécifiques au périphérique pour renforcer la sécurité de la communication entre l'encodeur Gen II et la passerelle Gen II. (L'option est activée par défaut pour les nouvelles installations.)

1. Pour activer la sécurité des périphériques, placez le commutateur **Activer la sécurité renforcée pour la communication des périphériques** sur **OUI**.



2. Lisez le message qui informe que tous les périphériques Génération II, y compris les encodeurs, les passerelles et les périphériques RAC5, doivent être reconfigurés dans **Gestion des périphériques**.
3. Cliquez sur **OUI** pour continuer.

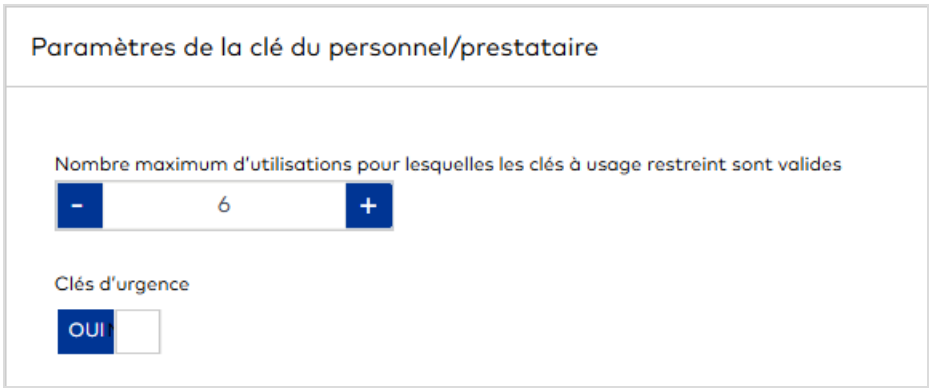
Une fois la sécurité du périphérique activée, Community :

- Génère et stocke les certificats de périphériques IP côté serveur et côté client.
- Désactive définitivement le commutateur **Activer la sécurité renforcée pour la communication des périphériques**.
- Met les périphériques Génération II hors ligne jusqu'à ce qu'ils soient reconfigurés.

Paramètres de la clé du personnel/prestataire

Configurer les valeurs par défaut à l'échelle du système pour les clés du personnel/prestataire.

1. Accédez à ***Paramètres du système > Clés du personnel/prestataire***.



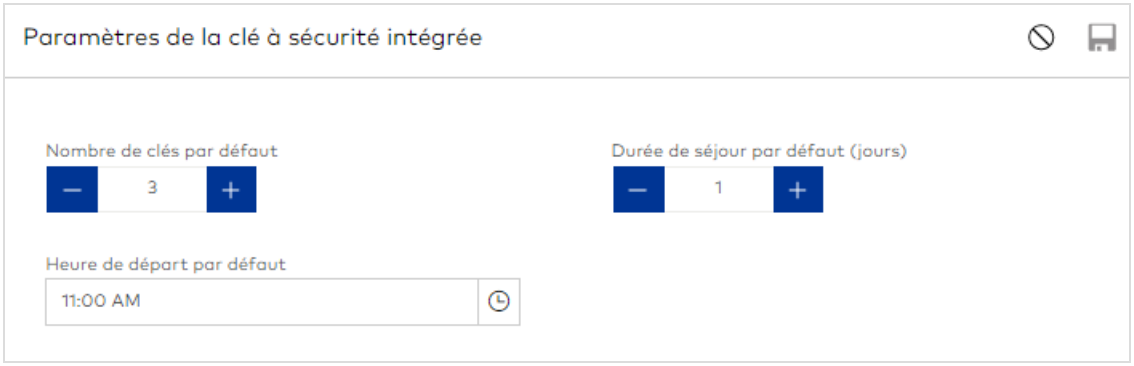
2. Indiquez le nombre de fois qu'une clé à usage restreint peut être utilisée. Valeur par défaut : 6. Valeurs valides : 1-6.
3. Choisissez d'activer ou non les clés d'urgence. Ce paramètre affecte les options disponibles dans **Gestion des rôles**, **Gestion des identifiants** et **Clés du personnel/prestataire**. Lorsque cette option n'est pas activée, aucune clé d'urgence ne peut être créée pour le site. Lorsque les clés d'urgence sont activées :
   - Dans **Gestion des rôles**, la catégorie d'identifiants Urgence est listée et peut être sélectionnée pour les droits de clés.
   - Dans **Gestion des identifiants**, il est possible de créer les identifiants Urgence (ainsi que de les consulter et de les supprimer).
   - Dans **Clés du personnel/prestataire**, les clés peuvent être créées en utilisant la catégorie d'identifiants Urgence.
4. Cliquez sur **(Sauvegarder)** 💾.

Paramètres des Clés à sécurité intégrée

Les clés à sécurité intégrée sont des sauvegardes des clés individuelles des unités qui sont créées à l'avance et conservées en jeux complets à remettre aux résidents en cas de panne du système ou de courant. Il est recommandé de créer et de conserver deux jeux de trois clés pour chaque porte d'unité et de suite. Après qu'un jeu de clés à sécurité intégrée a été émis et utilisé, créez un autre jeu de clés à sécurité intégrée pour remplacer le jeu utilisé. Les serrures n'acceptent que les clés des deux jeux de clés à sécurité intégrée les plus récents.

L'utilisation d'une clé à sécurité intégrée invalide l'accès aux unités, aux portes communes des suites et aux portes des unités de suite par la clé résident précédente.

1. Accédez à ***Paramètres du système > Clés à sécurité intégrée***.



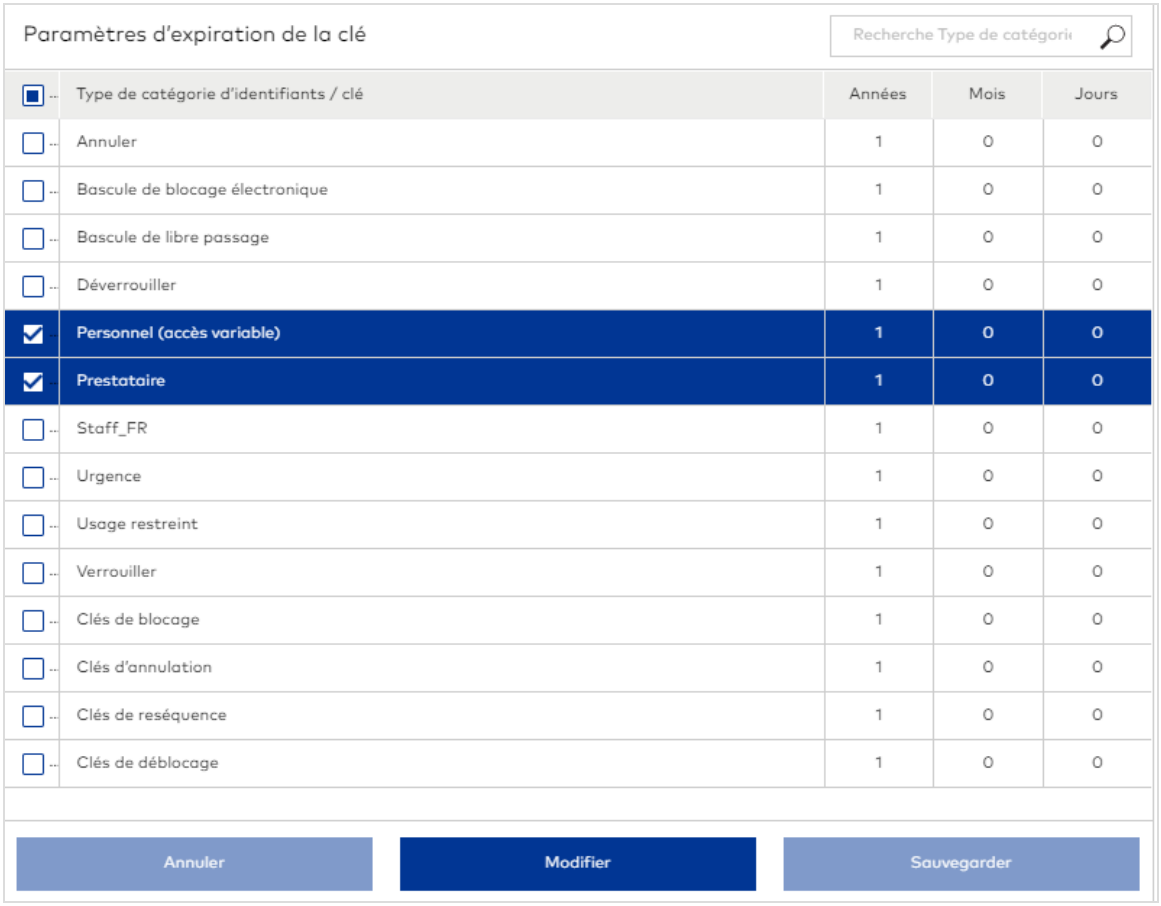
2. Indiquez le nombre de clés à sécurité intégrée par défaut à créer pour chaque point d'accès. Valeur par défaut : 3.
3. Indiquez le nombre de jours de validité des clés à sécurité intégrée. Après une première utilisation, les clés à sécurité intégrée expirent à l'issue du nombre de jours indiqué. Valeur par défaut : 1.
4. Sélectionnez l'heure après laquelle les clés à sécurité intégrée sont invalides le dernier jour du séjour. Valeur par défaut : 11 h du matin.
5. Cliquez sur **(Sauvegarder)**.

Paramètres d'expiration de la clé

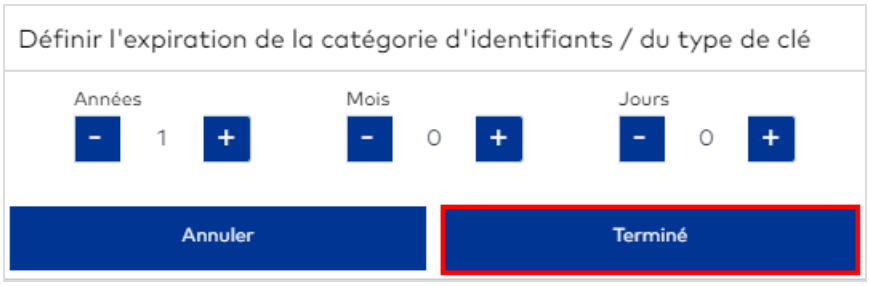
Configurez les dates d'expiration de la clé par défaut pour les catégories d'identifiants et les types de clés.

Les dates d'expiration peuvent toujours être modifiées lors de la création des clés.

1. Accédez à ***Paramètres du système > Expiration de la clé***.



2. Sélectionnez le type de catégorie d'identifiants ou de clé (ou cochez la case adjacente à **Type de catégorie d'identifiants / clé** pour tout sélectionner).
3. Cliquez sur **Modifier**.



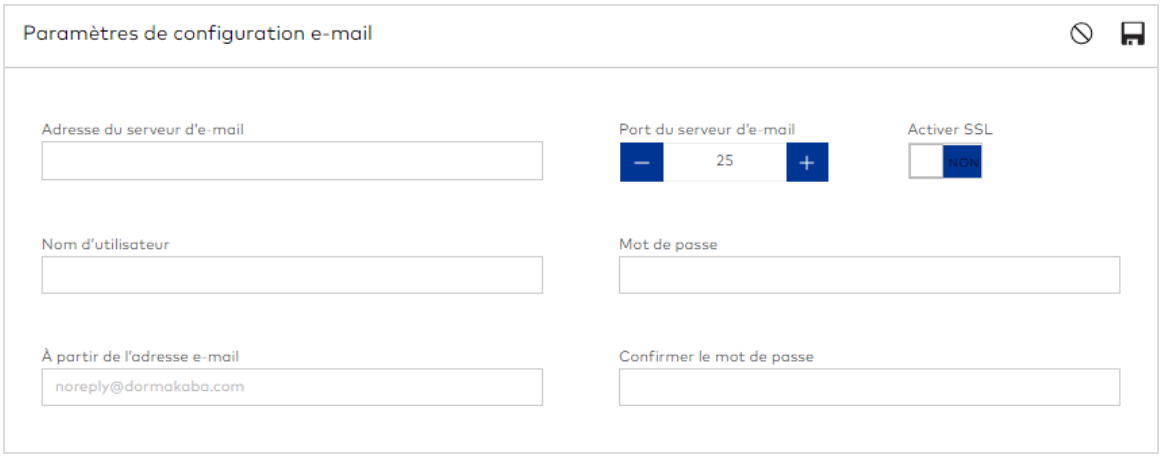
4. Sélectionnez le nombre d'années, de mois et de jours utilisés pour calculer la date d'expiration pour le type de catégorie d'identifiants / clé choisi. Min. : 1 jour, Max. : 9 ans. Valeur par défaut : 1 an.

5. Cliquez sur **Terminé**.
6. Cliquez sur **Sauvegarder**.

Paramètres de configuration de la messagerie électronique

Configurer les paramètres de messagerie électronique utilisés pour envoyer automatiquement des e-mails au personnel/prestataire.

1. Accédez à ***Paramètres du système > E-mail***.



2. Pour l'**Adresse du serveur d'e-mail**, indiquez l'adresse IP ou le nom d'hôte du serveur de messagerie électronique.
3. Indiquez le port de communication sur le serveur de messagerie électronique dédié à l'envoi automatique d'e-mails.
4. Choisissez d'activer ou non SSL (Secure Sockets Layer). Lorsque SSL est activé et que les certificats de sécurité sont valides, toutes les données des e-mails envoyés à partir du serveur de messagerie électronique vers les clients de messagerie électronique sont privées et sécurisées. Valeur par défaut : NON. Valeur recommandée : OUI.
5. Indiquez les identifiants valides du compte utilisé pour l'envoi automatique d'e-mails.
6. Pour **À partir de l'adresse e-mail**, indiquez l'adresse e-mail pour le compte envoyant l'e-mail automatique.
7. Cliquez sur **(Sauvegarder)** .

Paramètres de sauvegarde de la base de données

dormakaba recommande vivement de programmer des sauvegardes automatiques sur un disque dur externe, un disque réseau ou un serveur distant et de conserver les données de sauvegarde dans un endroit sûr hors site.

Consultez le tableau suivant pour obtenir des détails sur la sauvegarde.

Protection des	Emplacement de stockage	Option de sauvegarde	Fréquence	Conservation
SQL Server	Répertoire spécifié (local ou distant) Valeur par défaut : C:\Program Files\Microsoft SQL Server\MSSQL16.COMMUNITY\MSSQL\Backup Valeur par défaut pour les mises à niveau : les paramètres existants sont conservés	À la demande	À la demande	Sauvegarde actuelle
		Par horaire	Par horaire	Par réglage
Clé symétrique RGPD	ProgramData\DormaKaba\Community\backup (local uniquement)	Selon la politique du site		
MongoDB	Dossier MongoDB dans le répertoire spécifié (local uniquement) Valeur par défaut pour les nouvelles installations et les mises à niveau avec SQL Server distant : aucune Valeur par défaut pour les mises à niveau avec SQL Server local : les paramètres existants sont conservés	Par horaire	Par horaire	Dernière sauvegarde
Archive	Répertoire spécifié (local autorisé mais disque dur externe, lecteur réseau ou serveur distant recommandé) Valeur par défaut : C:\Program Files\dormakaba\Community Server\Archive Valeur par défaut pour les mises à niveau : les paramètres existants sont conservés	Par horaire	Par horaire	Indéfini

Conformément au RGPD (Règlement général sur la protection des données), toutes les PII (informations personnelles identifiables) stockées dans la base de données sont cryptées. Une clé de chiffrement spécifique au site, nécessaire pour restaurer la base de données, est enregistrée sur le serveur à l'emplacement \ProgramData\DormaKaba\Community\backup. dormakaba recommande de conserver une copie du fichier de clé dans un emplacement sécurisé distinct.

Stockage des sauvegardes sur un serveur distant

Si vous indiquez un chemin d'accès distant pour les sauvegardes de base de données, vous devez remplir les conditions suivantes :

- Le serveur Community et SQL Server peuvent se trouver sur la même machine ou sur des machines différentes, mais ils doivent se trouver dans le même domaine.
- Le dossier de sauvegarde à distance peut se trouver sur la même machine que SQL Server ou sur une machine différente, mais il n'y a aucune exigence en matière de domaine.
- Le serveur Community doit avoir un accès complet au dossier partagé. Les autorisations sont définies au niveau du dossier sur le serveur distant.

Sur le serveur Community :

1. Créez un dossier de sauvegarde portant le même nom et situé dans le même répertoire que le serveur distant. Par exemple, G:\backup doit exister à la fois sur le serveur Community et sur les serveurs distants.
2. Ouvrez et connectez-vous à SQL Server Management Studio.
3. Accédez à **Sécurité** > **Connexions** > **NT AUTHORITY\SYSTEM**, faites un clic droit et sélectionnez **Propriétés**.

4. Sélectionnez les **Rôles du serveur**.
5. Sélectionnez **sysadmin**.
6. Cliquez sur **OK**.

Sur le serveur distant :

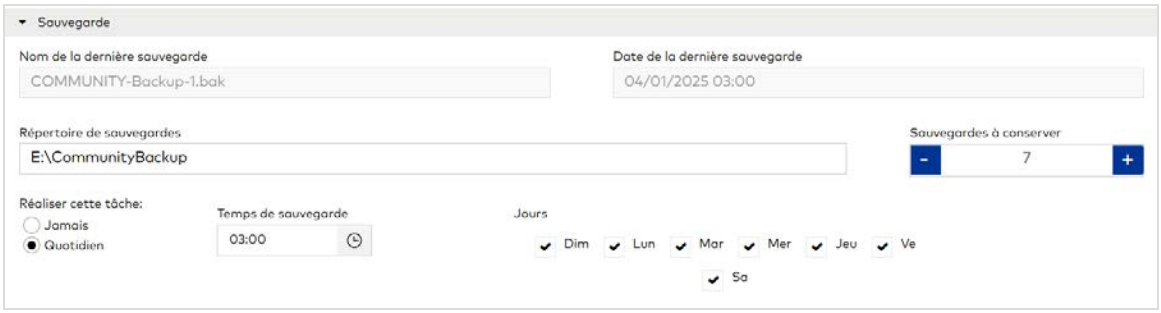
Partagez le dossier de sauvegarde et ajoutez un accès en lecture/écriture pour l'utilisateur du domaine.

Pour vérifier le chemin d'accès au répertoire lors de la spécification d'un serveur distant, cliquez avec le bouton droit de la souris sur le dossier partagé, sélectionnez **Propriétés**, cliquez sur l'onglet **Partage**, puis vérifier la valeur du **Chemin d'accès au réseau**.

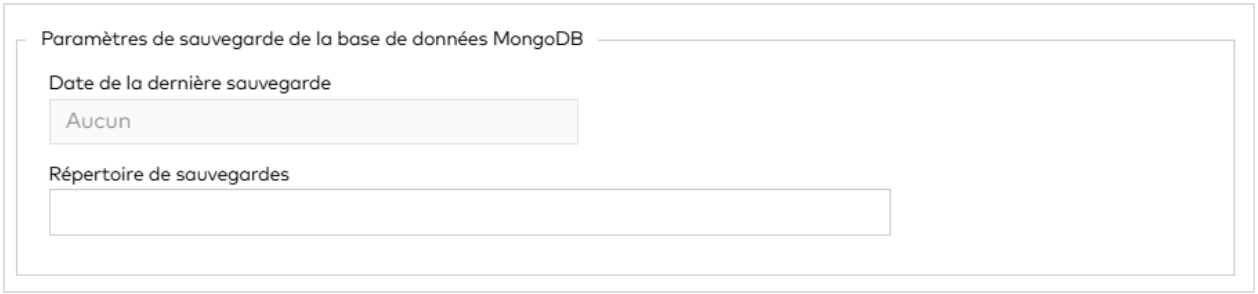
Configurer des sauvegardes

Configurer des sauvegardes de base de données programmées.

1. Accédez à ***Paramètres du système > Sauvegarde de la base de données***.



2. Paramètres de sauvegarde de la base de données SQL Server :
   - **Nom de la sauvegarde** — Champ en lecture seule affichant le nom de la sauvegarde de la base de données SQL Server la plus récente.
   - **Date de la dernière sauvegarde** — Champ en lecture seule affichant la date de la sauvegarde la plus récente. Vierge si elle n'a jamais été sauvegardée.
   - Pour le **Répertoire de sauvegardes**, indiquez où vous souhaitez enregistrer les copies de sauvegarde de la base de données. Vous devez indiquer le chemin complet vers un emplacement accessible par le serveur Community. Bien que vous puissiez indiquer un chemin local, **dormakaba recommande vivement de sauvegarder les sauvegardes sur un lecteur externe, un lecteur réseau ou un serveur distant**. Si vous indiquez le chemin d'accès à un serveur distant, vous devez remplir les conditions requises pour stocker les sauvegardes sur un serveur distant.
   - Pour les **Sauvegardes à conserver**, cliquez sur +/- pour indiquer le nombre de sauvegardes SQL Server à conserver dans le répertoire de sauvegardes. Lorsque le nombre de sauvegardes dépasse le nombre indiqué, la sauvegarde la plus ancienne est supprimée du répertoire de sauvegardes. Valeur par défaut : 7. Maximum : 99.
3. Communication en ligne uniquement. Paramètres de sauvegarde de la base de données MongoDB :



   - **Date de la dernière sauvegarde** — Champ en lecture seule affichant la date de la sauvegarde de la base de données MongoDB la plus récente. Vide si elle n'a jamais été sauvegardée.

- **Répertoire de sauvegardes** — Indiquez où vous souhaitez enregistrer les copies de sauvegarde de la base de données MongoDB sur le serveur local. Les chemins d'accès à distance ne sont pas pris en charge.

> Étant donné que seule la sauvegarde la plus récente de la base de données MongoDB est conservée, établissez un processus externe pour sauvegarder la base de données MongoDB si d'autres sauvegardes que la plus récente sont nécessaires.

4. Paramètres généraux :



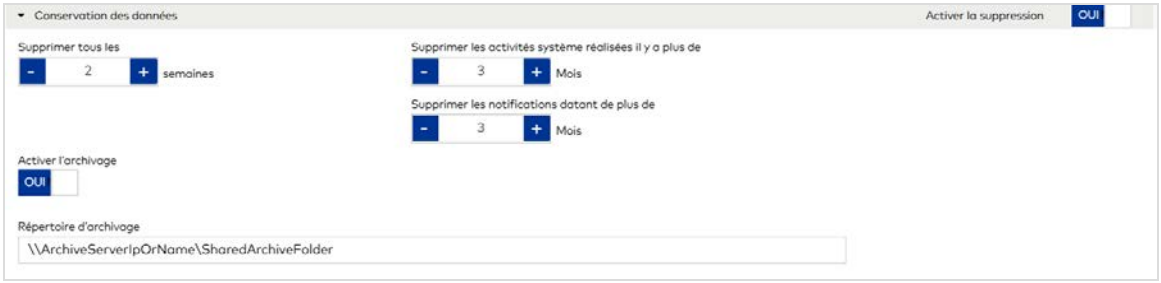
- **Réaliser cette tâche** — Sélectionnez l'une des options suivantes (Par défaut : Quotidien) :
  - **Jamais** — Aucune sauvegarde n'est programmée régulièrement. Vous devez sauvegarder la base de données manuellement ou utiliser un processus externe. Lorsque vous sélectionnez cette option, l'archivage ne peut pas être activé.
  - **Quotidiennement** — Si vous sélectionnez cette option, indiquez quand et lors de quels jours réaliser une sauvegarde programmée.
    - **Temps de sauvegarde** — Cliquez sur (Horloge), puis sélectionnez l'heure de démarrage de la sauvegarde. Valeur par défaut : 03h00 (3 h du matin).
    - **Jours** — Sélectionnez tous les jours de réalisation d'une sauvegarde programmée. Par défaut : tous les jours.

5. Cliquez sur **(Sauvegarder)**. Lors de la sauvegarde des paramètres, Community valide le chemin du répertoire spécifié.

Configurer la conservation des données

Pour configurer la conservation des données :

1. Accédez à ***Paramètres du système > Sauvegarde de la base de données > Conservation des données.***



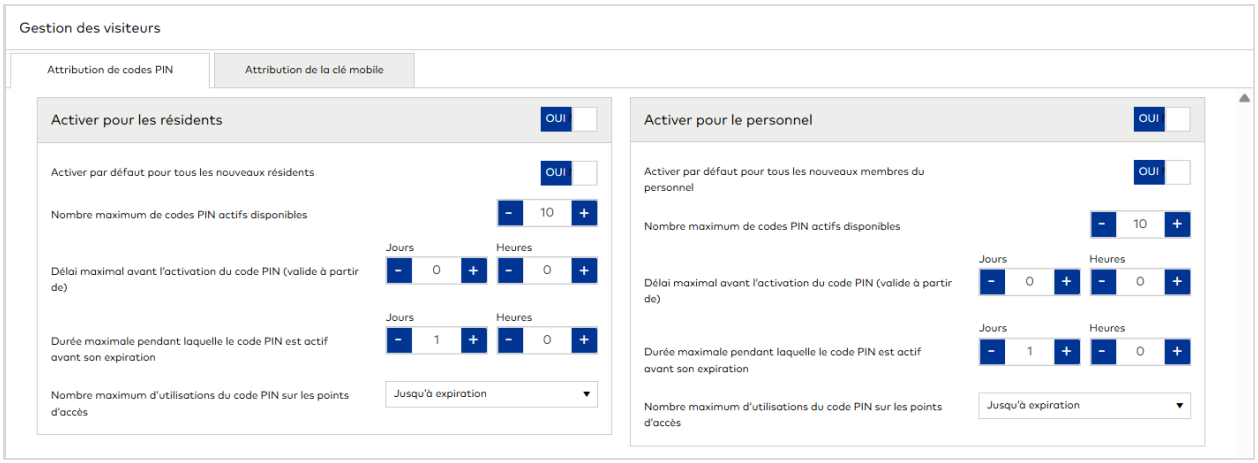
2. Pour **Activer la purge**, sélectionnez si la purge doit être activée ou non. Valeur recommandée : OUI. Si la purge n'est pas activée, la base de données va croître jusqu'à la limite système et l'espace sera indisponible pour le fonctionnement normal.
3. Pour **Purger tou(te)s les**, cliquez sur -/+ pour indiquer la fréquence hebdomadaire pour la purge des données historiques.
4. Pour **Purger les activités système réalisées il y a plus de**, cliquez sur -/+ pour sélectionner le nombre de mois de conservation des dossiers sur les activités système dans la base de données Community. Tous les dossiers sur les activités du système antérieurs à ce seuil sont supprimés. Valeur par défaut : 3.
5. Pour **Supprimer l'historique des opérations/événements en ligne antérieurs à**, sélectionnez le nombre de mois de conservation des enregistrements de la base de données pour les opérations et les événements en ligne. Tous les enregistrements en ligne antérieurs à ce seuil sont supprimés. Valeur par défaut : 3.
6. Pour **Supprimer les notifications datant de plus de**, cliquez sur -/+ pour sélectionner le nombre de mois pendant lesquels les notifications doivent être conservées dans la base de données Community. Tous les enregistrements antérieurs à ce seuil sont supprimés, que la notification ait été lue ou non. Cette option s'affiche uniquement si la communication en ligne est activée dans ***Paramètres du système > Avancés***. Valeur par défaut : 3. Valeurs valides : 1-12.
7. Pour **Activer l'archivage**, choisissez d'activer ou non l'archivage. Valeur par défaut : **NON**. Valeur recommandée : OUI. Si l'archivage n'est pas activé, la base de données va croître jusqu'à la limite système et l'espace sera indisponible pour le fonctionnement normal.
8. Pour le **Répertoire d'archivage**, indiquez le chemin complet vers un emplacement accessible par le serveur Community. **Bien que vous puissiez indiquer un chemin local, dormakaba recommande vivement un disque dur externe, un lecteur réseau ou un serveur distant.** Si vous indiquez un chemin d'accès distant, vous devez remplir les conditions suivantes :
   - Créez et indiquez un dossier partagé sur le serveur à distance.
   - Le serveur Community doit avoir un accès complet au dossier partagé.
9. Cliquez sur **(Sauvegarder)** 💾.

Paramètres de gestion des visiteurs

Configurez les valeurs par défaut pour prendre en charge l'attribution de codes PIN et BLE dans la **Gestion des résidents** et la **Gestion du personnel/prestataire**.

» Accédez à ***Paramètres du système > Gestion des visiteurs***.

Attribution de codes PIN

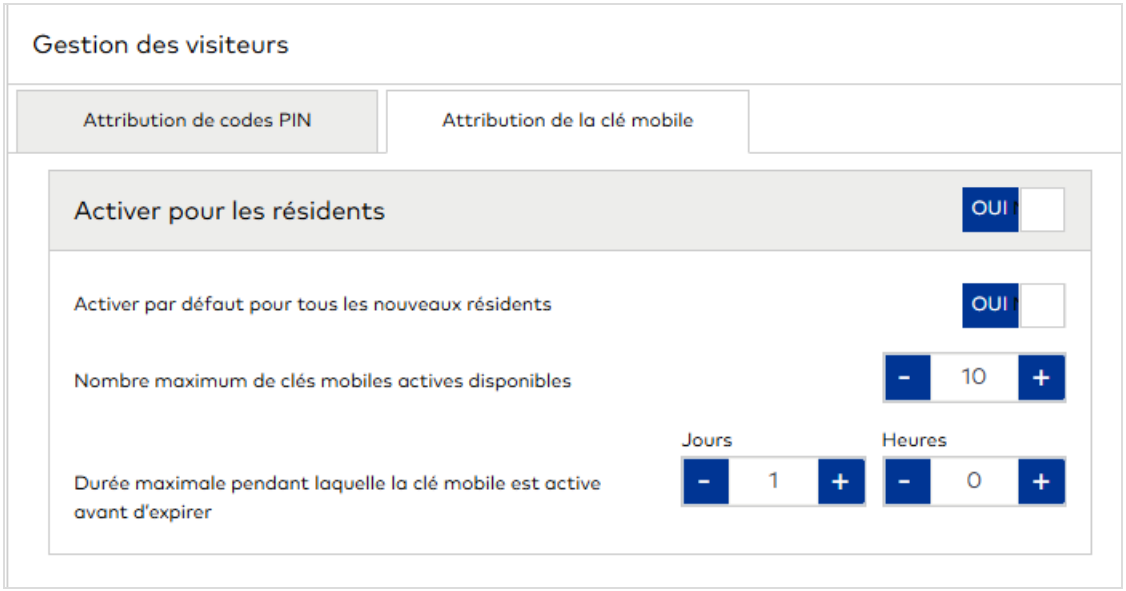


Activer et configurer l'attribution de codes PIN :

- **Activer pour les résidents** — Activer la fonctionnalité PIN de gestion des visiteurs dans **Gestion des résidents**. Valeur par défaut : NON. En sélectionnant **OUI**, une boîte de message vous invite à reconnaître la responsabilité de l'activation de la fonction. Cliquez sur **ACCEPTER** pour continuer.
- **Activer pour le personnel** — Activer la fonctionnalité PIN de gestion des visiteurs dans **Gestion du personnel/prestataire**. Valeur par défaut : NON. En sélectionnant **OUI**, une boîte de message vous invite à reconnaître la responsabilité de l'activation de la fonction. Cliquez sur **ACCEPTER** pour continuer.
- **Activer la valeur par défaut pour tous les nouveaux résidents/membres du personnel** — Activer la fonctionnalité PIN pour tous les nouveaux profils de résidents et de personnel/prestataire. Lorsque cette fonctionnalité est activée, la section PIN s'affiche dans l'onglet Gestion des visiteurs pour tous les nouveaux profils, les paramètres PIN peuvent être personnalisés et mis à jour sur les périphériques mobiles. Valeur par défaut : NON. En sélectionnant **OUI**, une boîte de message vous invite à reconnaître la responsabilité de l'activation de la fonction. Cliquez sur **ACCEPTER** pour continuer.
- **Nombre maximum de PIN actifs disponibles** — Indiquez la valeur par défaut dans les profils des résidents et du personnel/prestataire pour le nombre maximum de codes PIN qui peuvent être actifs. Valeurs valides : 1-50. Valeur par défaut : 10 .
- **Délai maximal avant l'activation du code PIN (valide à partir de)** — Indiquez la valeur par défaut dans les profils des résidents et du personnel/prestataire pour le nombre maximal de jours/heures pendant lesquels un code PIN peut être créé avant que l'accès autorisé par le code PIN ne commence. Plage pour les résidents : 0-15 jours/0-23 heures. Plage pour le personnel : 0-30 jours/0-23 heures. Valeur par défaut : 0 jour/0 heure.
- **Durée maximale pendant laquelle le code PIN est actif avant d'expirer** — Indiquez la valeur par défaut dans les profils de résidents et du personnel/prestataire pour le nombre maximal de jours/heures pendant lesquels un code PIN peut être actif. Plage pour les résidents : 0-15 jours/0-23 heures. Plage pour le personnel : 0-30 jours/0-23 heures. Valeur par défaut : 1 jour/0 heure.
- **Nombre maximum de fois que le code PIN peut être utilisé dans les points d'accès** — Indiquez la valeur par défaut dans les profils de résidents et du personnel/prestataire pour le nombre maximum de fois qu'un code PIN peut être utilisé dans les points d'accès. Valeurs valides : Jusqu'à expiration, 1-5. Valeur par défaut : Jusqu'à expiration.

- **Espaces communs autorisés** — Sélectionnez les espaces communs dont l'accès est activé par défaut dans l'onglet Gestion des visiteurs pour les profils des résidents et du personnel/prestataire.

Attribution de la clé mobile



Activer et configurer l'attribution de clés mobiles :

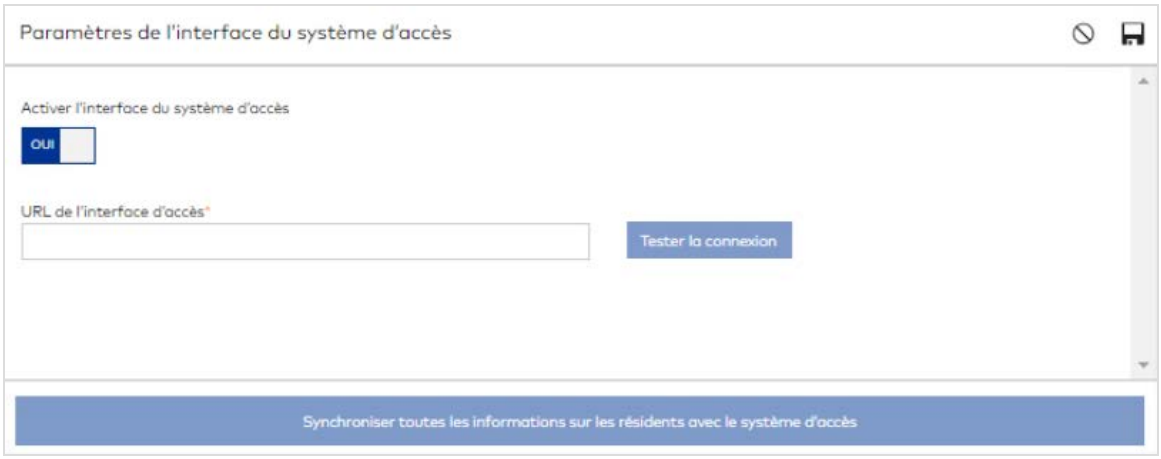
- **Activer pour les résidents** — Activez la fonctionnalité d'attribution des clés mobiles de la Gestion des visiteurs dans **Gestion des résidents**. Valeur par défaut : NON. En sélectionnant **OUI**, une boîte de message vous invite à reconnaître la responsabilité de l'activation de la fonction. Cliquez sur **ACCEPTER** pour continuer.
- **Activer la valeur par défaut de tous les nouveaux résidents** — Activer l'attribution des clés mobiles pour tous les nouveaux profils de résidents. Lorsque cette fonctionnalité est activée, la section d'attribution de clés mobiles s'affiche dans l'onglet Gestion des visiteurs pour tous les nouveaux profils, les paramètres peuvent être personnalisés et mis à jour sur les périphériques mobiles. Valeur par défaut : NON. En sélectionnant **OUI**, une boîte de message vous invite à reconnaître la responsabilité de l'activation de la fonction. Cliquez sur **ACCEPTER** pour continuer.
- **Nombre maximum de clés mobiles actives disponibles** — Indiquez le nombre maximum de clés mobiles attribuées qui peuvent être actives pour le résident. Valeurs valides : 1-50. Valeur par défaut : 10.
- **Durée maximale pendant laquelle la clé mobile est active avant d'expirer** — Indiquez la valeur par défaut dans les profils de résidents pour le nombre maximal de jours/heures pendant lesquels une clé mobile attribuée peut être active. Plage : 0-15 jours/0-23 heures. Valeur par défaut : 1 jour/0 heure.

Paramètres de l'interface du système d'accès

L'interface du système d'accès est une fonction sous licence qui est désactivée par défaut.

Community s'intègre avec des systèmes d'accès tiers pour étendre les options de gestion des accès des résidents. La configuration de l'authentification pour le système d'accès est facultative. Pour les détails de mise en œuvre, obtenez la *Documentation sur l'API RESTful du système d'accès* auprès du support de dormakaba.

1. Accédez à ***Paramètres du système > Interface du système d'accès***.



2. Activer l'interface du système d'accès.
3. Indiquez l'URL du système d'accès tiers. En option, testez la connexion.
4. Options d'authentification — Les valeurs de l'ID client, de la clé secrète, de l'URL d'autorisation, de l'URL de redirection et du code d'autorisation sont fournies par le tiers et sont nécessaires pour générer un jeton.
5. Cliquez sur **Générer un jeton**.
6. Cliquez sur **(Sauvegarder)**.
7. Cliquez sur **Synchroniser toutes les informations sur les résidents avec le système d'accès**. Toutes les informations sur les résidents sont synchronisées avec le système d'accès. Les modifications futures des profils de résidents sont automatiquement synchronisées toutes les deux minutes.

API Community

Pour activer et configurer les paramètres de l'API Module Community : :

1. Accédez à ***Paramètres du système > API Community***.
2. Indiquer les options. Pour en savoir plus, reportez-vous aux sections ci-dessous.
3. Cliquez sur **(Sauvegarder)** .

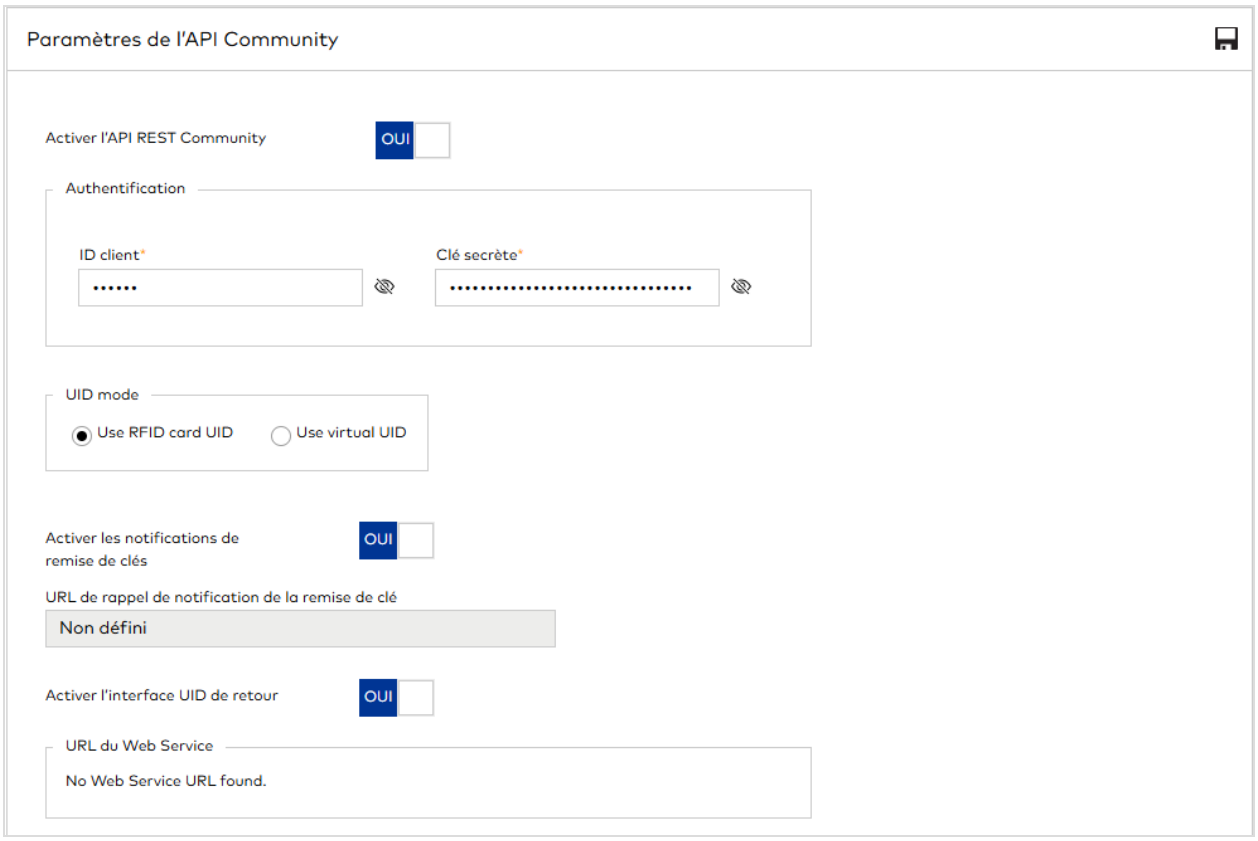
API Community

Activez l'API REST Community et les notifications de remise de clés.

- API REST Community — Les opérateurs peuvent utiliser l'API REST pour créer et gérer pratiquement tous les aspects des clés des résidents/du personnel/des prestataires. L'API prend également en charge les opérations de lecture et d'effacement des clés, ainsi que la liste des informations relatives aux encodeurs, aux audits, aux espaces communs et à l'affectation des unités de résidents. Pour plus de détails sur l'API, procurez-vous les spécifications *API REST Community* auprès d'un technicien du support dormakaba.
- Notifications de remise de clés — Lorsque cette option est activée, des notifications de remise de clés sont envoyées pour chaque clé de résident/personnel/prestataire remise à partir de l'interface utilisateur, de l'API REST Community et de l'API SOAP Community. Les tiers doivent d'abord enregistrer une URL de rappel et un jeton de sécurité facultatif.

Pour activer et configurer l'API REST Community :

1. Accédez à ***Paramètres du système > API Community***.



2. Réglez le commutateur logiciel **Activer l'API REST Community** sur **OUI**.
3. Indiquez l'identifiant et la clé secrète uniques du client utilisés pour obtenir et renouveler un jeton d'authentification. Caractères minimum : 6 ; caractères maximum : 512 (pour les deux paramètres).

4. Sélectionnez **OUI** pour activer les notifications de remise de clés. Community envoie une notification distincte à l'API chaque fois qu'une clé est créée. Les tiers doivent d'abord enregistrer une URL de rappel et un jeton de sécurité facultatif pour recevoir des messages de notification.
   - Paramètre en lecture seule indiqué dans l'API. L'URL de rappel à utiliser pour l'envoi des notifications.
5. Lorsque les notifications de remise de clés sont activées, sélectionnez le mode UID :
   - **UID de la carte RFID** — Lorsque cette option est sélectionnée, la notification inclut l'UID de la carte pour toutes les clés RFID des résidents, du personnel et des prestataires émises à partir de l'interface utilisateur, de l'API REST Community et de l'API SOAP Community. Pour les clés mobiles, l'UID ne figure pas dans le message de notification. Pour les clés de portefeuille émises à partir de l'API REST Community, la notification inclut l'identifiant de la carte de portefeuille.
   - **UID virtuel** — Lorsque cette option est sélectionnée, la notification inclut l'UID virtuel calculé pour toutes les clés mobiles et RFID des résidents, du personnel et des prestataires émises à partir de l'interface utilisateur, de l'API REST Community et de l'API SOAP Community. Pour les clés de portefeuille des résidents, du personnel et des prestataires émises à partir de l'API REST Community, la notification inclut l'identifiant de la carte de portefeuille.
6. Cliquez sur **(Sauvegarder)** .

Paramètres avancés

Pour configurer les paramètres avancés :

1. Accédez aux ***Paramètres du système > Avancés***.
2. Indiquer les options. Pour en savoir plus, reportez-vous aux sections ci-dessous.
3. Cliquez sur **(Sauvegarder)** .

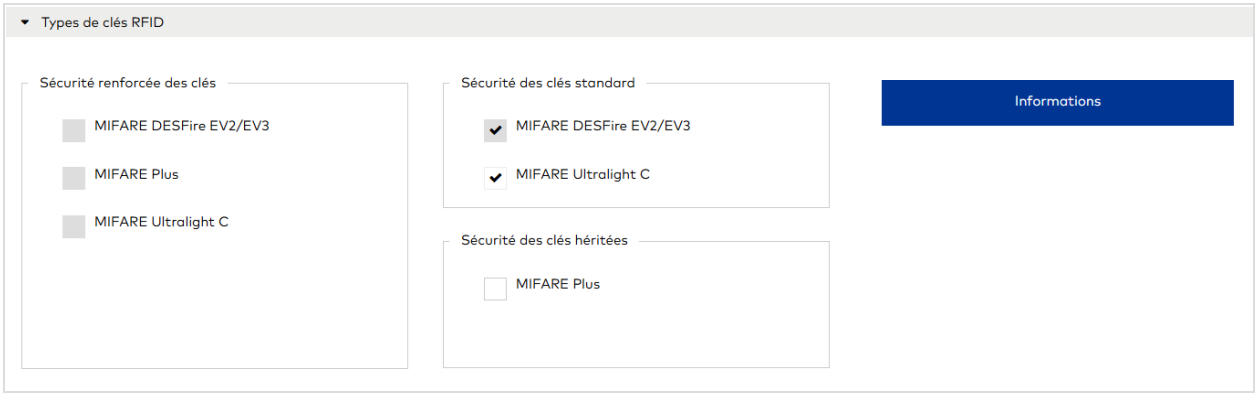
Types de clés RFID

S'il est affiché, cliquez sur le bouton **Informations** dans cette section pour lire les consignes de sécurité.

Sécurité renforcée des clés activée



Sécurité renforcée des clés désactivée



Le changement de type de clé RFID est rare et nécessite la reprogrammation de toutes les serrures.

Pour changer le type de clé RFID, sélectionnez l'option qui s'applique à votre déploiement puis reprogrammez les serrures.

- **Sécurité renforcée des clés** — Uniquement disponible lorsque le mode de sécurité renforcée est activé. Lorsque cette section est activée, les types de clés suivants sont disponibles :

  - **MIFARE DESFire EV2/EV3** — Sélectionné et désactivé par défaut.
  - **MIFARE Plus** — Sélectionné et activé par défaut. Pour les mises à niveau, sélectionné si préalablement sélectionné ou lors de l'activation du mode de sécurité renforcée si préalablement sélectionné dans la sécurité des clés héritées.
  - **MIFARE Ultralight C** — Sélectionné et activé par défaut. Pour les mises à niveau, sélectionné si préalablement sélectionné ou lors de l'activation du mode de sécurité renforcée si préalablement sélectionné dans la sécurité des clés standard.
- **Sécurité des clés standard** — Lorsque cette section est activée, les types de clés suivants sont disponibles :
  - **MIFARE DESFire EV2/EV3** — Sélectionné et désactivé par défaut.
  - **MIFARE Ultralight C** — Sélectionné et activé par défaut.
- **Sécurité des clés héritées** — La sélection d'une option de cette section déclenche un message de rappel de sécurité. Lorsque cette section est activée, les types de clés suivants sont disponibles :
  - **MIFARE Plus** — Désélectionné et activé par défaut.
  - **MIFARE Classic** — Non pris en charge pour les nouvelles installations. Pour les mises à niveau, s'affiche uniquement si préalablement sélectionné. Contactez le support dormakaba.

La technologie de clé sélectionnée contrôle le nombre de points d'accès supplémentaires qui peuvent être encodés sur les clés. De plus, les points d'accès considérés comme *supplémentaires* diffèrent pour les clés résident et personnel/prestataire. (Les espaces communs ne comptent pas comme points d'accès supplémentaires.)

- Clés de résidents — Tous les points d'accès sont considérés comme supplémentaires.
- Clés du personnel/prestataire — Tous les points d'accès ajoutés lors de l'encodage des clés (à l'exception des points d'accès attribués à l'identifiant sélectionné) sont considérés comme supplémentaires.

Limites de la technologie des clés pour les points d'accès supplémentaires :

- MIFARE DESFire EV2/EV3 : 94
- MIFARE Ultralight : 6
- MIFARE Mini : 6
- MIFARE Classic & Plus 1k/2k : 94
- MIFARE Classic & Plus 4k : 542
- Clé mobile : 25

Configuration du site

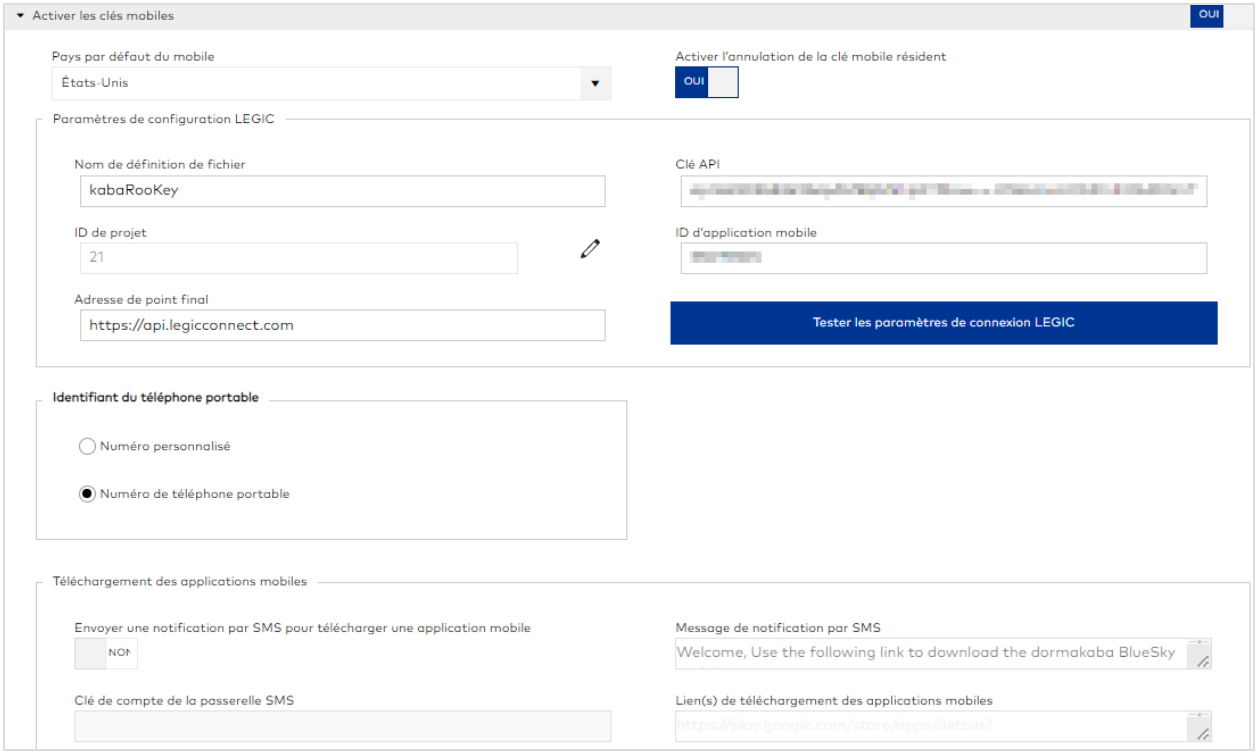


Indiquez si vous souhaitez activer la configuration des espaces communs étendus. L'activation de cette option augmente le nombre d'espaces communs restreints qui peuvent être définis d'un maximum combiné de 12 (pour les espaces communs restreints et les ascenseurs) à un maximum de 256 pour les espaces communs restreints et 80 pour les ascenseurs. Lorsqu'un type quelconque d'espace commun restreint est défini, la modification de cette option nécessite de supprimer puis de recréer tous les espaces communs restreints dans **Configurateur de site**, de reprogrammer les points d'accès concernés et de réencoder toutes les clés (y compris mobiles) sur lesquelles les espaces communs restreints sont encodés. Valeur par défaut : NON. Valeur par défaut : Pour les nouvelles installations et les mises à niveau sans espaces communs restreints : OUI ; pour les mises à niveau avec tout type d'espace commun restreint : NON.

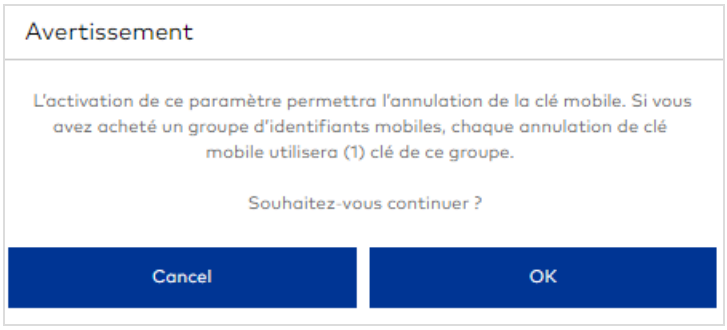
Tous les modèles de serrures, sauf RT et Legacy Confidant, prennent en charge les espaces communs étendus.

Clés mobiles

Les clés mobiles sont une fonction sous licence qui est désactivée par défaut.



1. Positionnez le commutateur **Activer les clés mobiles** sur **OUI**.
2. Pour le **Pays par défaut du mobile**, sélectionnez le pays par défaut pour les numéros de téléphone portable. Le code pays correspondant est extrait pour le numéro de téléphone portable.
3. (*sous conditions, option sous licence*) Pour annuler les clés mobiles remises aux résidents et aux visiteurs, positionnez le commutateur **Activer l'annulation de la clé mobile résident** sur **OUI**. Si des clés mobiles sont activées et si cette option ne l'est pas, vous ne pouvez annuler une clé mobile. À la place, ce sont les détails d'expiration qui déterminent la date d'invalidité de la clé mobile.



4. Pour les **Paramètres de configuration LEGIC/BLE/portefeuille mobile**, un technicien du service client de dormakaba fournit des valeurs valides. La modification des clés de confidentialité, d'authentification et/ou de cryptage nécessite la reprogrammation du point d'accès.
5. Pour **Identifiant du téléphone portable**, sélectionnez l'une des options suivantes :
   - **Numéro personnalisé** — Lorsque les porteurs de clés mobiles utilisent une application tierce intégrée à Community, consultez votre fournisseur de solutions d'intégration pour savoir s'il faut configurer le numéro comme **Numéro de téléphone portable** ou comme **Numéro personnalisé**.
   - **Numéro de téléphone portable** — Sélectionnez le moment où les porteurs de clés mobiles utiliseront l'application dormakaba BlueSky.
6. Uniquement lorsque l'identifiant du téléphone portable est le numéro de téléphone portable. Pour le **Téléchargement des applications mobiles**, choisissez d'envoyer ou non un SMS aux destinataires de clés mobiles pour les informer que leur

périphérique n'est pas enregistré dans l'application mobile. Si vous sélectionnez **OUI**, vous devez également spécifier le texte du message à envoyer et une clé de compte de la passerelle SMS (voir note). Utilisez les liens de téléchargement des applications mobiles pour télécharger dormakaba BlueSky pour les périphériques Android et Apple, respectivement. Cette fonction est disponible pour toutes les clés mobiles (personnel/prestataires,résidents et visiteurs).

Community prend en charge les notifications par SMS en utilisant le service Swift SMS Gateway. Des informations sur ce service tiers sont disponibles à l'adresse suivante : www.swiftsmsgateway.com.

Communication en ligne

La communication en ligne est une fonction sous licence qui est désactivée par défaut.

Si le déploiement de Community est autorisé pour la Gestion des serrures à distance, réglez le commutateur logiciel sur **OUI**. Pour plus d'informations, voir Gestion des serrures à distance.

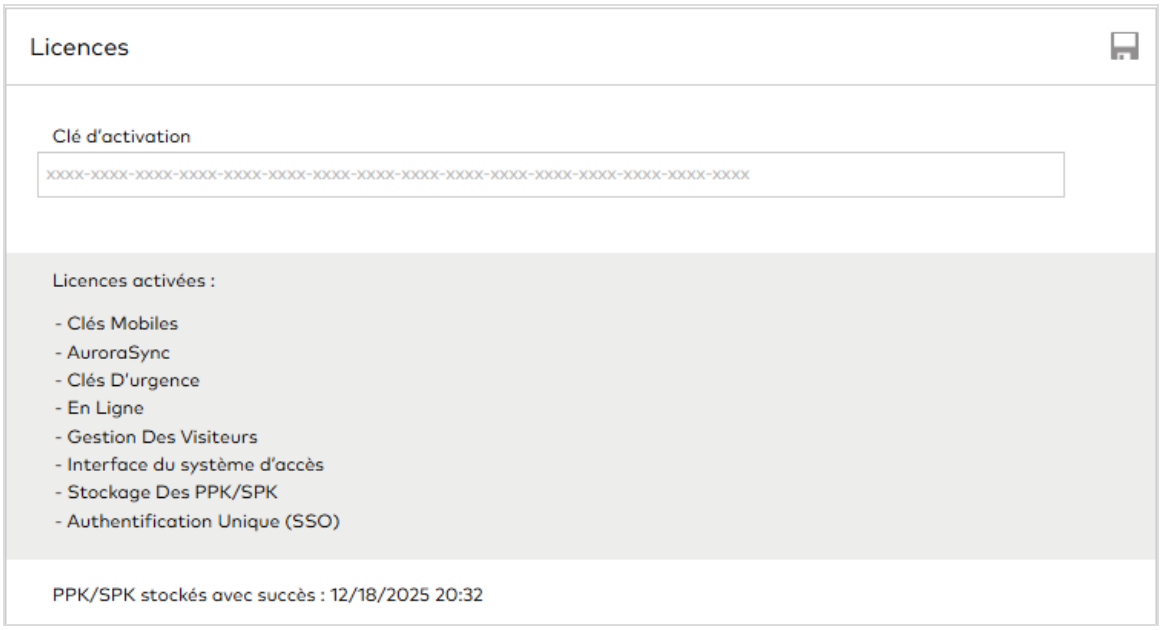
Keyscan Aurora

L'interface AuroraSync est une fonction sous licence qui est désactivée par défaut. Si le déploiement Community se connecte à un serveur Aurora pour prendre en charge les lecteurs Keyscan, réglez le commutateur logiciel sur **OUI**.

Paramètres de licence

Les fonctionnalités du produit sous licence sont activées ou désactivées en fonction de la clé d'activation.

1. Accédez à ***Paramètres du système > Licences***.



2. Indiquez une clé d'activation valide.
3. Cliquez sur **(Sauvegarder)**.

Les licences activées sont affichées.

Si la licence comprend le stockage des PPK/SPK (clé de programmation primaire et clé de programmation secondaire), la date et l'heure d'enregistrement des données est affichée.

Étape 2

Configurez votre site

Cette section comprend les sujets suivants :

En savoir plus sur le configurateur de site 52
Ajouter des bâtiments 58
Ajouter des étages 59
Ajouter des unités 62
Ajouter des suites 66
Ajouter des espaces communs pour les résidents 70
Ajouter des espaces communs pour le personnel 76
Ajouter des accès privés 82
Ajouter des ascenseurs 84

En savoir plus sur le configurateur de site

Configurer votre site dans Community implique la création d'une représentation virtuelle de tous les points d'accès de votre établissement. Les points d'accès représentent des points d'entrée contrôlés par Community. Dans la plupart des cas, un point d'accès correspond à une serrure, par exemple la serrure d'une porte. Cependant, certains points d'accès correspondent à différents types de matériel, comme un lecteur d'ascenseur.

Commencez par ajouter les bâtiments. Ensuite, pour chaque bâtiment, ajoutez tous les étages. Ensuite, ajoutez les unités individuelles, les unités de suites, les espaces communs et les accès privés à chaque étage. Vous pouvez également ajouter des ascenseurs et configurer l'accès aux ascenseurs.

Types de point d'accès

Community prend en charge un maximum de 8 192 points d'accès par site, dont 4 095 peuvent être des points d'accès résidentiels (unités et suites).`

Les types de points d'accès suivants sont créés dans Configurateur de site :

- **Unité** — Point d'accès attribué à un résident lors de l'affectation de l'unité.
- **Suite** — Point d'accès qui est une série d'unités communicantes comprenant une porte commune et un ou plusieurs points d'accès d'unité de suite.
- **Accès privé** — Type de point d'accès réservé au personnel pour un accès à l'arrière de l'établissement. Par exemple, la salle électrique serait un accès privé.
- **Espace commun résident** — Point d'accès où l'accès général est configuré pour les résidents. L'accès peut être illimité ou limité.
- **Espace commun pour le personnel** — Point d'accès où l'accès général est configuré pour le personnel. L'accès peut être illimité (pour le personnel) ou limité.
- **Ascenseur** — Point d'accès qui permet d'accéder aux étages d'un bâtiment. Un groupe d'ascenseurs comprend des ascenseurs qui partagent le même plan d'étage.

Configuration des étages et des points d'accès

Lors de l'ajout d'étages et de points d'accès dans le Configurateur de site, les noms des points d'accès que vous verrez dans Community sont formés. Les conventions de nommage des étages et points d'accès devraient donc être descriptifs et cohérents, de manière à former des noms uniques faciles à identifier lors de la configuration des accès, de la fabrication des clés et de la lecture des rapports.



Les noms des étages et des points d'accès ne doivent pas dépasser 15 caractères, espaces compris. Caractères alphanumériques valides : A-Z, 0-9. Caractères spéciaux valides : -#%=!,.:_()?*'<>/+.

Formats de nom

Tous les noms d'étage sont formatés à l'aide de nombres. Les numéros que vous sélectionnez sont utilisés dans le nom de l'étage. Par exemple, si vous sélectionnez la plage de 1 à 10 lorsque vous ajoutez des étages, alors (en utilisant le préfixe par défaut ÉTAGE), vous ajouterez dix étages appelés Étage1, ..., Étage10.

Les noms des points d'accès sont formés de la même manière, avec une possibilité supplémentaire de formater le nom avec des chiffres ou du texte. Pour certains types de points d'accès tels que les espaces communs, un format de texte est plus adapté, par exemple *Réception*. Si vous utilisez le format chiffré, le numéro de l'étage et le numéro de l'unité sont inclus par défaut dans le nom du point d'accès. Par exemple, si vous sélectionnez la plage de 1 à 1 lorsque vous ajoutez une unité à Étage1, vous ajouterez une unité appelée 101 à Étage1.

Options de formatage avancées

La manière la plus simple de créer des noms d'étages et de points d'accès descriptifs consiste à utiliser les options de formatage avancées. Par exemple, vous pouvez choisir d'exclure le numéro d'étage des noms d'unité et/ou d'ajouter un

préfixe au numéro de l'unité. Comme les noms des points d'accès doivent être uniques, vous ne pouvez sélectionner des numéros ayant été précédemment utilisés que si vous indiquez également un préfixe ou suffixe unique. Les options de formatage avancées ne sont pas disponibles pour le format texte.

Lorsque vous créez des étages ou points d'accès dans le **Configurateur de site**, vous pouvez afficher un échantillon dynamique de vos sélections de formatage dans la zone **Aperçu**.

Création de points d'accès par lots

Pour simplifier la configuration, Community permet la création d'unités et d'accès privés par lots. Vous pouvez ajouter plusieurs points d'accès à plusieurs étages simultanément. Par exemple, si vous sélectionnez la plage 1 à 10 lorsque vous ajoutez des unités à Étage1, ..., Étage10, alors (avec le formatage par défaut), vous ajouterez dix unités à chaque étage (101, ..., 110, 201, ..., 210, 301, ..., 310, et ainsi de suite). Le nombre total de points d'accès est égal à 100.

Inclure dans le fichier de téléchargement des clés mobiles

Lorsque la licence est accordée pour les clés mobiles, l'option **Inclure dans le fichier de téléchargement des clés mobiles** s'affiche lors de la création et de la modification des points d'accès. Cette option permet d'identifier les serrures équipées pour accepter les identifiants de clés mobiles. Sélectionnez l'option permettant d'inclure dans le point d'accès du fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site.

Modèles de serrures

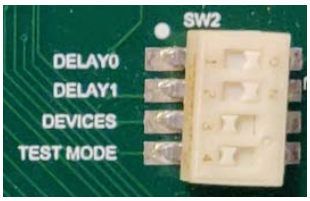
Pour obtenir les informations les plus récentes sur les modèles de serrure, consultez les notes de mise à jour.

Community prend en charge les modèles de serrures suivants :

- **Nova** — Tous les points d'accès programmés avec ce profil de serrure fonctionnent en mode bascule.
- **Saflok Quantum/Saflok Confidant et Confidant NFC/Saflok RT, Saflok RT+/RCU (Remote Controller Unit)/Pixel et Pixel+/Saffire LX (L, M & P)** — Pour ces profils, le mode bascule peut être activé pour les clés de résidents. Ce modèle prend également en charge le mode bascule pour les clés encodées avec un identifiant basé sur une catégorie d'identifiants qui inclut la bascule par défaut ou qui est activée pour inclure la bascule.

  Saflok Confidant et Saflok RT ne prennent pas en charge les espaces communs étendus.

- **Saffire LX (D & I)/Saflok MT** — Pour ces profils, le mode bascule n'est pas pris en charge.
- **RAC5 XT et RAC5 Lite** — Pour ces profils, le mode bascule est pris en charge. RAC5 XT est destiné aux systèmes en ligne ; RAC5 Lite ne prend pas en charge la gestion des serrures à distance. Chaque périphérique RAC5 XT peut être associé à un seul point d'accès ou deux points d'accès différents. Configurer manuellement le nombre de points d'accès à associer en modifiant le commutateur **PÉRIPHÉRIQUES** de chaque périphérique RAC5 XT. Pour plus d'informations, reportez-vous à la documentation RAC5.



Tous les modèles de serrures pour les points d'accès de l'unité, de la porte commune de la suite et de l'unité de suite prennent en charge 255 clés de résidents distinctes actives. Tous les modèles de serrures pour les espaces communs résident peuvent gérer les clés de résidents (pas de touring mode) pour un site déployé avec jusqu'à 8 192 points d'accès (combinaison des points d'accès de l'unité, de la porte commune de la suite et de l'unité de suite).

Mode bascule

La bascule est une fonction qui fait passer l'état d'une serrure de l'état *Verrouillé* à l'état *Déverrouillé* chaque fois qu'une clé valide est présentée. Par exemple, l'état par défaut d'une serrure est *Verrouillé*. La première fois qu'une clé est présentée, la serrure passe à un état *Déverrouillé*. La porte est ouverte et reste accessible jusqu'à ce que la clé soit présentée à nouveau à la serrure ou que le verrou d'intimité intérieur soit sorti.

La bascule est activée de différentes manières selon le type de serrure et la catégorie d'identifiants :

- La bascule peut être une caractéristique mécanique de la serrure. Par exemple, toutes les serrures Nova fonctionnent en mode bascule.
- Pour les identifiants basés sur les catégories Urgence, Personnel, Personnel (accès variable) et Prestataire, la bascule est activée pour les points d'accès d'unités et de suites en sélectionnant l'option **Activer le mode bascule** lors de la création du point d'accès d'unités/suites dans Configurateur de site. Valide pour les profils de serrures suivants : Saflok Quantum, Saflok Confidant, Saflock RT/RT+, RCU, Pixel et Saffire LX, RAC5 XT, RAC5 Lite.
- Pour les identifiants basés sur la catégorie d'usage restreint, le mode bascule n'est pas pris en charge.

Espaces communs pour les résidents

Les espaces communs résident sont des espaces sur votre site qui sont configurés pour un accès général par les résidents et le personnel/les prestataires, tels que les réceptions, le parking et les installations de loisirs. Dans l'industrie hôtelière, nous appelons cela des espaces communs. Lorsque vous créez un point d'accès aux espaces communs pour les résidents, vous pouvez choisir d'activer un accès limité.

Clés du personnel uniquement. L'accès aux espaces communs reste toujours valable jusqu'à l'expiration de la clé. Les nouvelles clés ne peuvent pas invalider l'accès aux espaces communs. Les clés d'annulation ne peuvent invalider l'accès aux espaces communs que si l'état de la clé est Actif.

Espaces communs pour les résidents illimités

Lorsque l'accès limité *n'est pas activé*, l'espace commun est inclus avec toutes les affectations d'unités et autorisé sur toutes les clés de résidents. Les espaces communs résident illimités sont également autorisés sur toutes les clés du personnel/prestataire.

Espaces communs pour les résidents à accès limité

Lorsque l'accès limité est activé, l'accès doit être configuré dans ***Gestion des accès > Accès aux espaces communs***. Essentiellement, des espaces communs résident restreints sont associés aux unités. L'accès des résidents dépend des espaces communs associés aux unités/unités de suites qui leur sont affectées.

Lors de la création de l'espace commun limité, vous devez également sélectionner un identifiant d'espace commun. L'ID est une valeur numérique utilisée par le système pour une synchronisation avec les paramètres API de tiers (interface de programmation d'applications). Lorsque les espaces communs étendus sont activés, le nombre maximum d'identifiants d'espaces communs est de 256 afin de prendre en charge les espaces communs (résident et personnel/prestataire). Sans les espaces communs étendus, la limite est de 12, y compris les identifiants pour les espaces communs limités et les ascenseurs.

L'accès du personnel/prestataire aux espaces communs résident limités est également configuré dans ***Gestion des accès > Accès aux espaces communs***.

Espaces communs pour le personnel

Les espaces communs pour le personnel sont des espaces de votre établissement qui sont configurés pour l'accès du personnel/des prestataires, tels qu'un bureau, un coin cuisine et des placards à fournitures. Lorsque vous créez un point d'accès aux espaces communs pour le personnel, vous pouvez choisir d'activer un accès limité :

L'accès aux espaces communs reste toujours valable jusqu'à l'expiration de la clé. Les nouvelles clés ne peuvent pas invalider l'accès aux espaces communs. Les clés d'annulation ne peuvent invalider l'accès aux espaces communs que si l'état de la clé est Actif.

Espaces communs pour le personnel illimités

Lorsque l'accès limité *n'est pas activé*, l'espace commun figure sur toutes les clés du personnel/des prestataires.

Espaces communs pour le personnel à accès limité

Lorsque l'accès limité est activé, les options suivantes sont disponibles :

- limiter l'accès en fonction de l'identifiant — l'accès doit être configuré dans ***Gestion des accès > Gestion des identifiants***.
- limiter l'accès en fonction du profil d'accès aux espaces communs — l'accès doit être configuré dans ***Gestion des accès > Accès aux espaces communs***.

Lors de la création de l'espace commun limité, vous devez également sélectionner un identifiant d'espace commun. L'ID est une valeur numérique utilisée par le système pour une synchronisation avec les paramètres API de tiers (interface de programmation d'applications).

Lorsque les espaces communs étendus sont activés, le nombre maximum d'identifiants d'espaces communs est de 256 afin de prendre en charge les espaces communs (résident et personnel/prestataire). Sans les espaces communs étendus, la limite est de 12, y compris les identifiants pour les espaces communs limités et les ascenseurs.

Ascenseurs

La configuration des ascenseurs pour contrôler l'accès aux étages du bâtiment implique un technicien d'ascenseur et le Configurateur de site Community. dormakaba fournit le boîtier de contrôle de l'ascenseur et les lecteurs. Le technicien d'ascenseur est responsable de l'installation et du câblage de tous les périphériques. Le Configurateur de site fonctionne dans **Configurateur de site** pour établir les points d'accès aux ascenseurs.

Le processus de base pour le Configurateur de site est le suivant :

1. Ajoutez un ou plusieurs groupes d'ascenseurs.
2. Ajoutez un ou plusieurs ascenseurs.
3. Cartographier l'accès aux étages (pour chaque groupe d'ascenseurs).

Groupes d'ascenseurs

Un groupe d'ascenseurs comprend des ascenseurs qui partagent le même plan d'étage. Les ascenseurs doivent se trouver dans le même bâtiment, mais il n'est pas nécessaire qu'ils soient situés au même endroit. Le Configurateur de site doit obtenir le modèle de boîte de contrôle avant d'ajouter un groupe d'ascenseurs car le modèle affecte le plan d'étage.

Ascenseurs

Les ascenseurs sont ajoutés à un groupe d'ascenseurs. Vous fournissez un nom pour l'ascenseur et un nom pour au moins un lecteur. Les lecteurs sont des périphériques qui interprètent les données de configuration de l'accès aux étages encodées sur une clé et communiquent avec le boîtier de contrôle pour permettre l'accès.

Bien que nous appelions l'ascenseur le point d'accès, c'est en fait le lecteur qui contrôle l'accès.

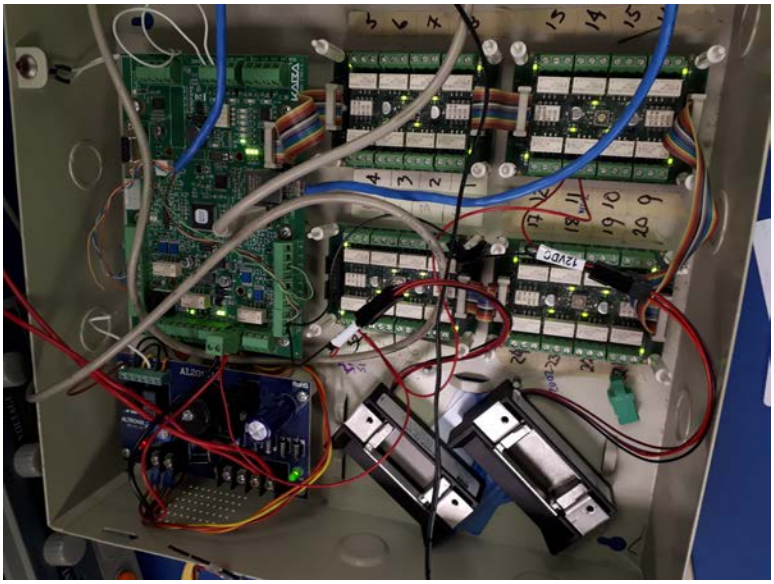
Plan d'étage

Le Configurateur de site cartographie l'accès aux étages pour chaque groupe d'ascenseurs. Bien que tous les plans d'étage fonctionnent de la même manière, le modèle de boîte de contrôle sélectionné lors de l'ajout du groupe d'ascenseurs affecte les options disponibles. En général, plus le nombre d'étages qui doivent être contrôlés indépendamment augmente, plus la taille du boîtier de contrôle augmente.

Un boîtier de contrôle est un périphérique qui contient une ou plusieurs cartes relais électriques avec un ou plusieurs interrupteurs à relais. Votre site utilisera l'un des modèles suivants :

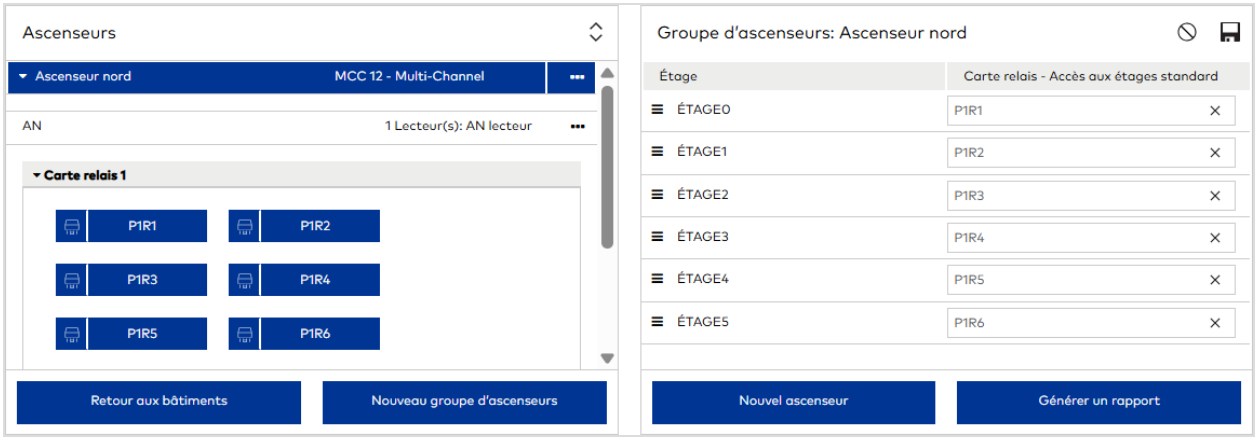
- **EMCC - Contrôleur multicanal étendu** — Huit cartes relais à 16 relais chacune.
- **MCC 12 - Contrôleur multicanal** (Mode hérité pris en charge) — Une carte relais à 12 relais.
- **MCC 8 – Contrôleur multicanal** (Mode hérité pris en charge) — Une carte relais à 8 relais.
- **ECU - Unité de contrôle des ascenseurs** — Une carte relais à un relais.
- **MFC - Contrôleur d'étage multiple** — Quatre cartes relais à huit relais chacune.
- **RAC 5 - Contrôleur d'accès à distance** — (Non MFC) Huit cartes relais à huit relais chacune. Pour les environnements en ligne, les passerelles RAC5 doivent être configurées dans **Gestion des périphériques**.

La figure suivante montre l'intérieur d'un boîtier de contrôle MFC avec quatre cartes relais à huit relais chacune.



Les relais de trois des cartes relais sont étiquetés 1-24. Lors de la cartographie de l'accès aux étages dans Community, les interrupteurs de relais sont cartographiés en fonction des étages.

La figure suivante montre le plan d'étage Community. Les étages 1 à 3 sont reliés au Relais1 (P1R1). Tous les autres étages sont reliés à un relais distinct.



Lorsqu'un porteur de clé présente une clé au lecteur, celui-ci détecte la configuration d'accès encodée sur la clé, communique avec le boîtier de contrôle qui permet d'ouvrir et d'allumer les boutons de la carte relais de l'ascenseur auquel le porteur de clé est autorisé à accéder. Dans certains cas, un lecteur se trouve à l'extérieur de l'ascenseur pour contrôler l'accès aux boutons d'appel de **montée** et de **descente**.

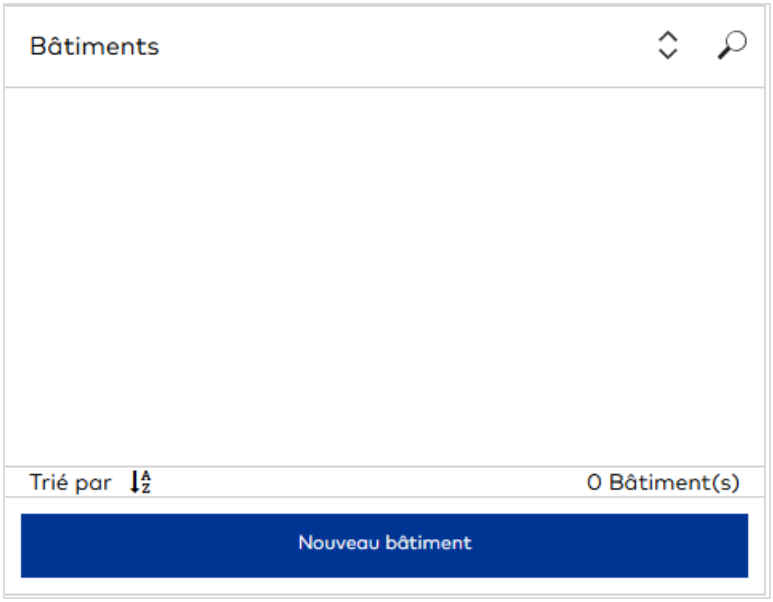
En dehors de la règle de base, *un étage ne peut être relié qu'à un seul relais*, la cartographie des relais-étages est entièrement configurable. Il convient de retenir qu'un signal du lecteur pour ouvrir le relais ouvre l'accès à tous les étages reliés au relais. Par exemple, si les Étages1-3 sont reliés au Relais1 et que l'accès à l'étage encodé sur une clé est autorisé uniquement pour l'Étage1, le porteur de clé pourra accéder aux Étages1-3. Par conséquent, pour un contrôle maximal, il est recommandé d'associer un étage à un relais. Si l'accès à deux ou plusieurs étages est toujours autorisé en même temps, il est possible que vous souhaitiez associer plus d'un étage à un relais.

Ajouter des bâtiments

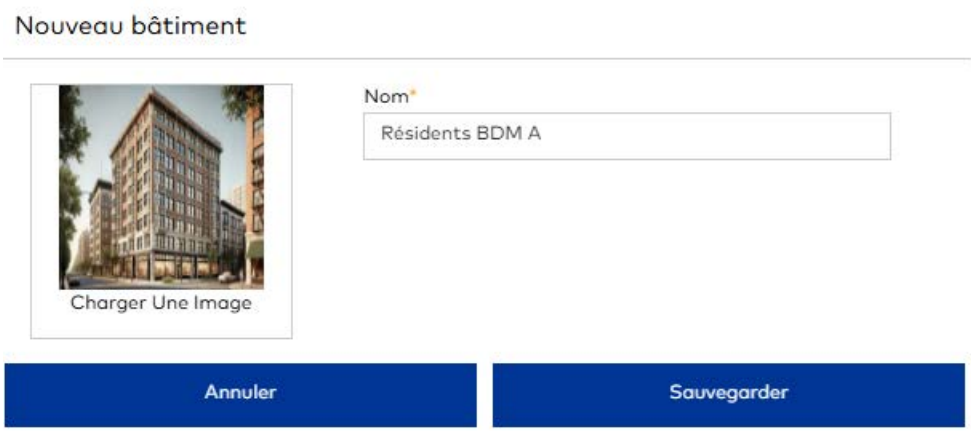
Les bâtiments sont les structures indépendantes de votre site.

Pour ajouter des bâtiments :

1. Ouvrez le **Configurateur de site**.



2. Cliquez sur **Nouveau bâtiment**.



3. Indiquez un nom unique.
4. (*facultatif*) Sélectionnez une image pour représenter votre site. Cliquez sur **Charger une image**, accédez à une image, sélectionnez-la, puis cliquez sur **Ouvrir**. Types de fichiers pris en charge : gif, jpg, png.
5. Cliquez sur **Sauvegarder**. Le bâtiment s'affiche dans la liste.

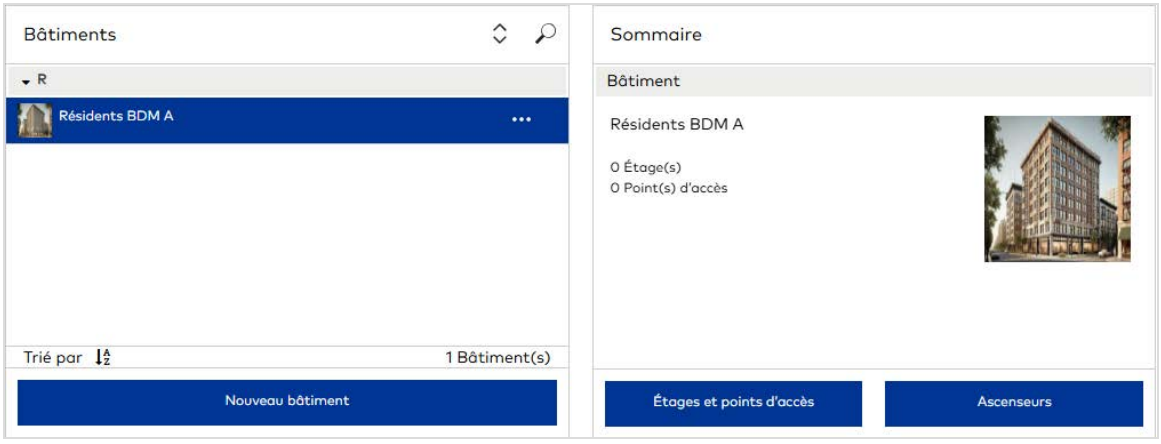


Ajouter des étages

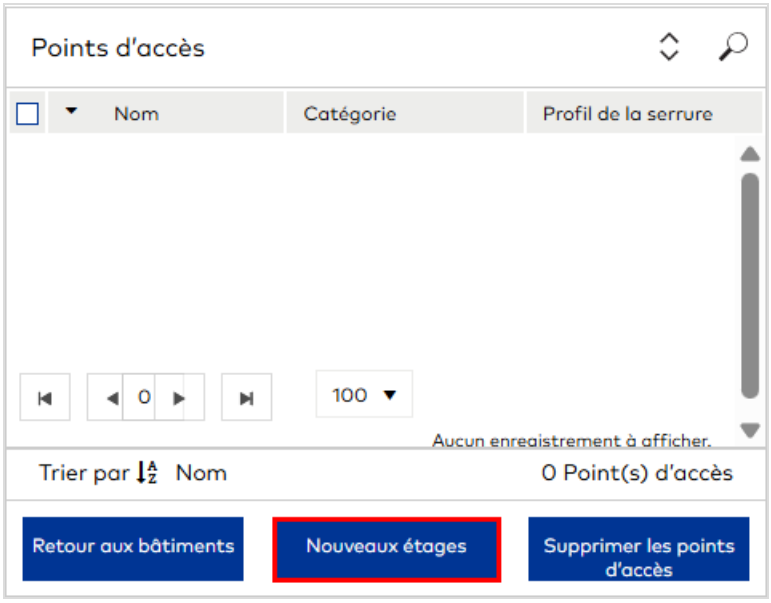
Les étages sont les niveaux d'un bâtiment. Vous devez ajouter des étages avant d'ajouter des points d'accès.

Pour ajouter des étages :

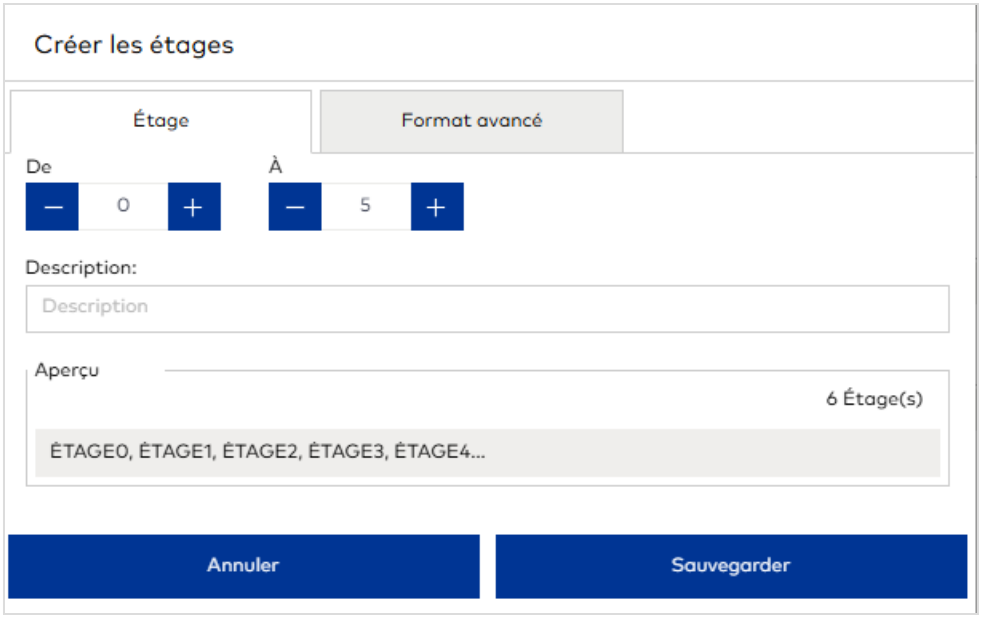
1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.



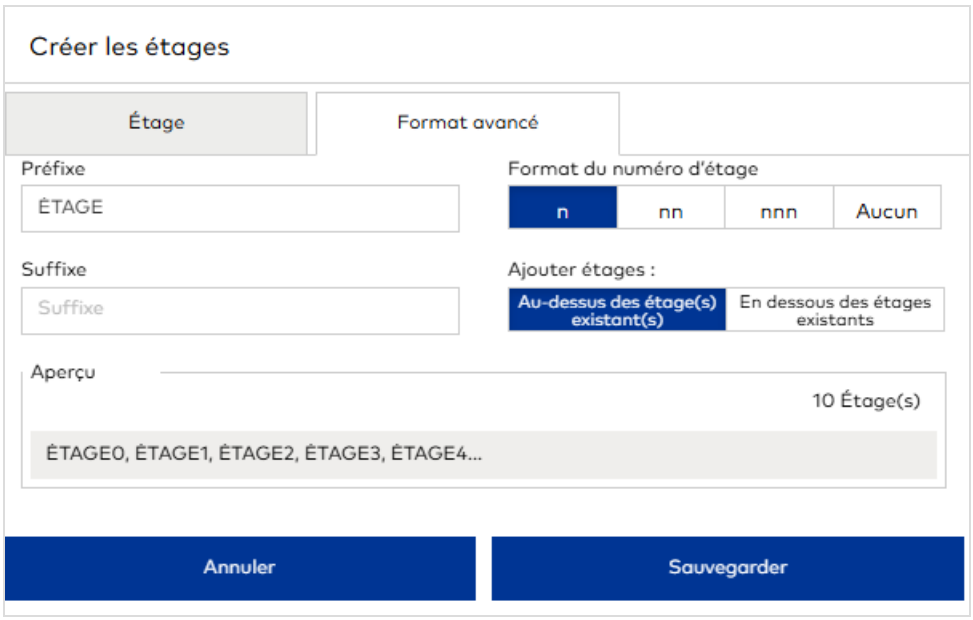
3. Cliquez sur **Étages et points d'accès**.



4. Cliquez sur **Nouveaux étages**.

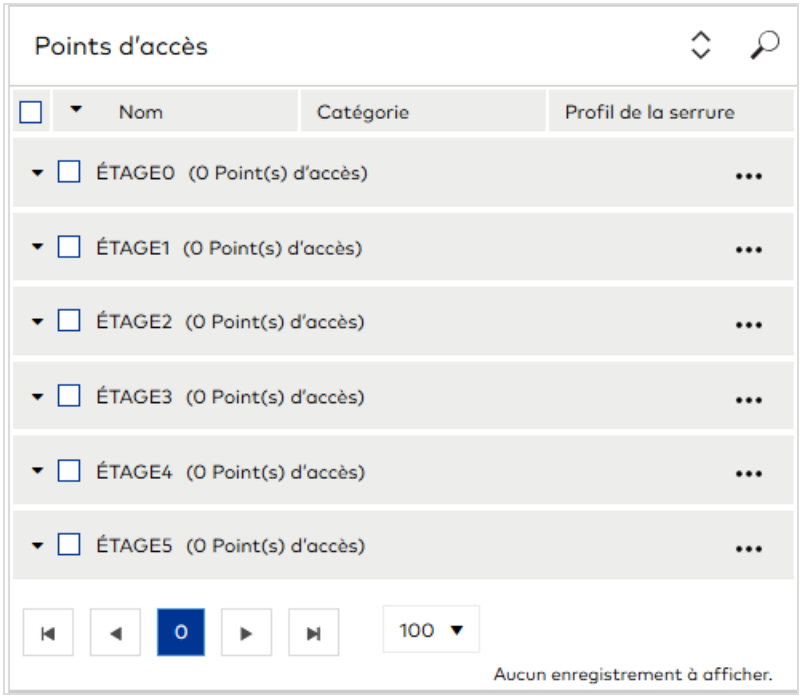


5. Indiquez la plage d'étages à ajouter. Comme le nom des étages doit être unique, vous pouvez sélectionner uniquement des numéros ayant été précédemment utilisés si vous indiquez également un préfixe ou suffixe unique.
6. (*facultatif*) Ajoutez une description pour l'étage ou la plage d'étages.
7. (*facultatif*) Indiquez l'une des options suivantes dans l'onglet **Format avancé** :



- **Préfixe** — Indiquez le texte à afficher avant le numéro d'étage. Ajoutez des espaces, le cas échéant. Valeur par défaut : ÉTAGE.
- **Suffixe** — Indiquez le texte à afficher après le numéro d'étage ou de point d'accès. Ajoutez des espaces, le cas échéant. Valeur par défaut : aucune.
- **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour ÉTAGE 1, **nn** pour ÉTAGE 01 ou **nnn** pour ÉTAGE 001. Pour masquer le numéro d'étage dans le nom, sélectionnez **Aucun**. Valeur par défaut : n.
- **Ajouter un/des étage(s)** — Choisissez d'ajouter ou non les étages à la liste avant ou après les étages existants. Valeur par défaut : Au-dessus de l'étage ou des étages existants.

8. Cliquez sur **Sauvegarder**.

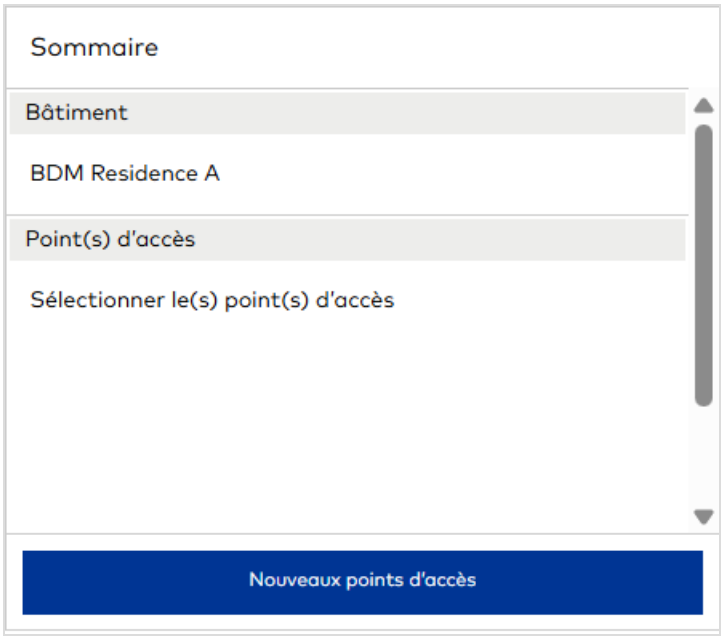


Ajouter des unités

Les unités sont les types de points d'accès attribués aux résidents lors de l'affectation de l'unité.

Pour ajouter des unités :

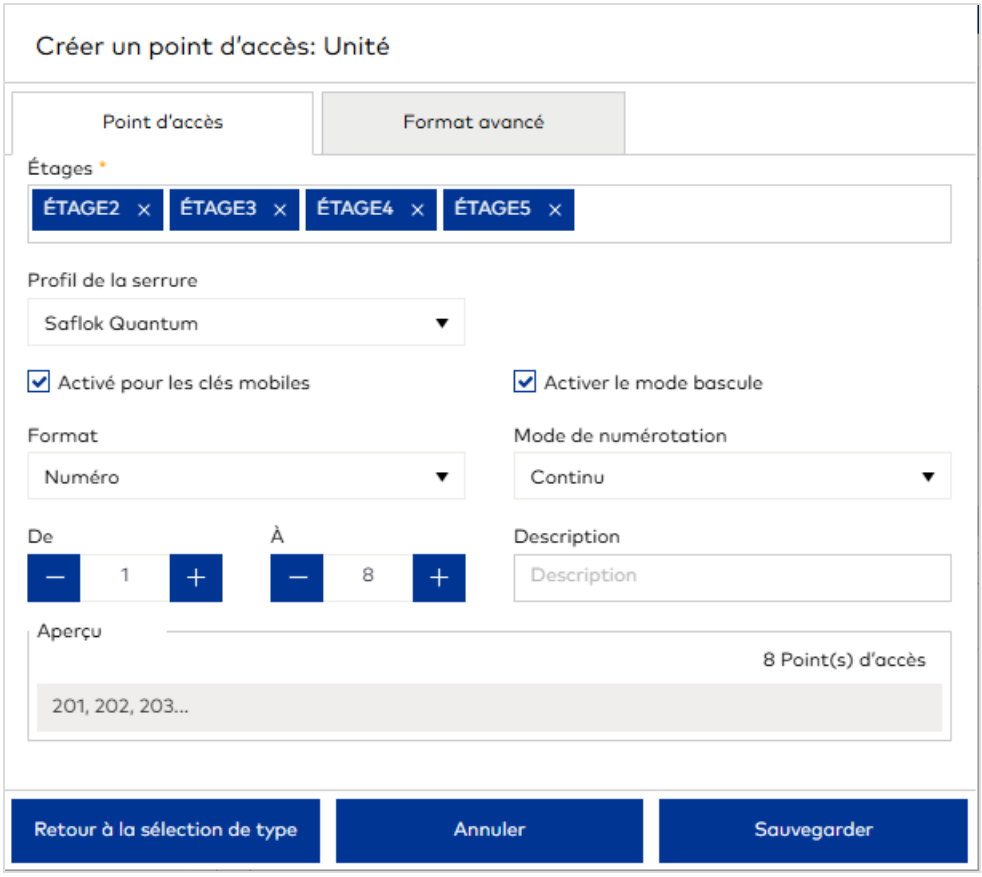
1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Étages et points d'accès**.



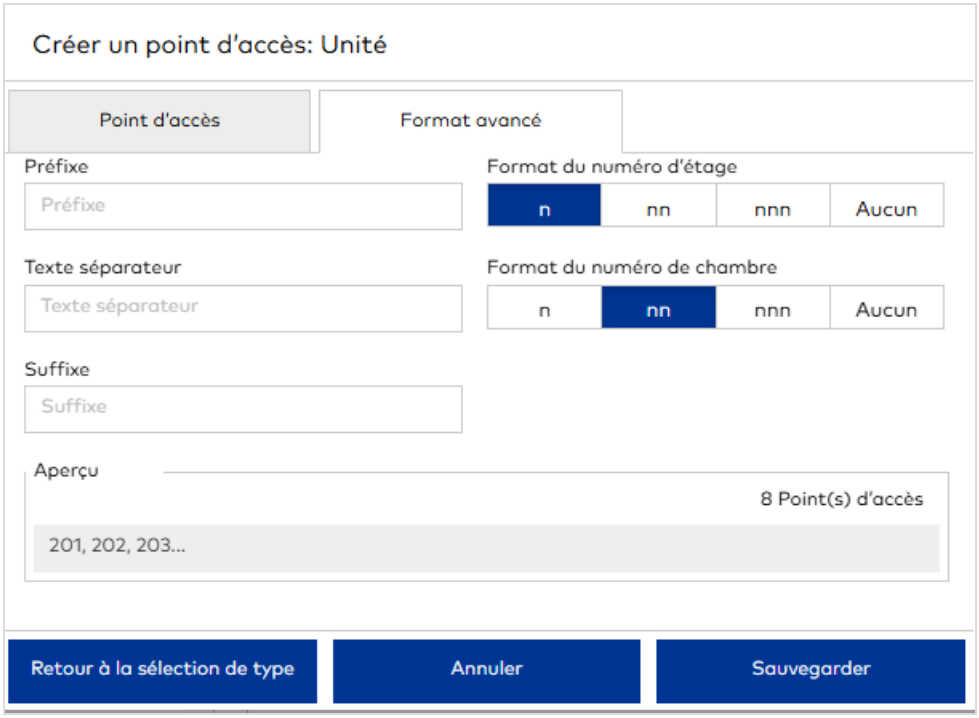
4. Cliquez sur **Nouveaux points d'accès**.



5. Sélectionnez **Unité**, puis cliquez sur **Suivant**.

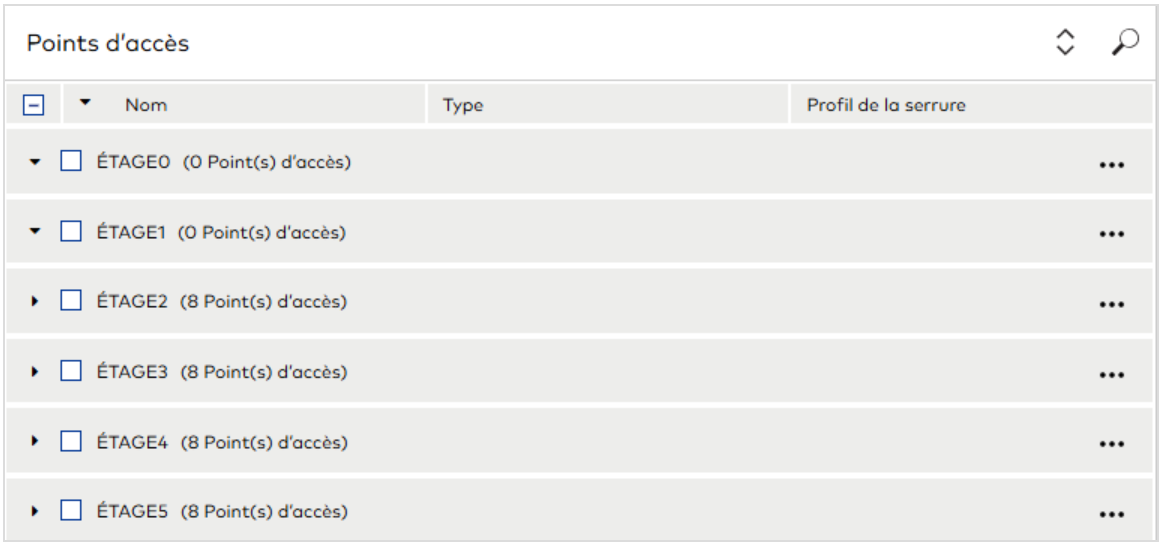


6. Pour les **Étages**, sélectionnez un ou plusieurs étages où vous souhaitez ajouter les points d'accès.
7. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure. Toutes les serrures Nova comprennent la fonction de bascule. Pour tous les autres types de serrures qui prennent en charge la bascule, l'option **Activer le mode bascule** est affichée. Chaque fois qu'une clé valide est présentée à une serrure qui comprend ou est activée pour le mode bascule, l'état de la serrure alterne entre *Verrouillé* et *Déverrouillé*. Par exemple, l'unité 100 est programmée en utilisant un profil de serrure Nova. La serrure est dans un état *Verrouillé* (sécurisé). La première fois que le résident présente une clé, la serrure passe à un état *Déverrouillé*. La porte est ouverte et reste accessible jusqu'à ce que la clé soit présentée à nouveau à la serrure ou que le verrou d'intimité intérieur soit sorti. Lorsque cette option n'est pas sélectionnée, les serrures restent dans un état Verrouillé, sauf pendant la brève période pendant laquelle une clé valide est présentée pour autoriser l'accès.
8. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
9. **Inclure dans le fichier de téléchargement des clés mobiles** — (*(facultatif)* Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
10. Pour le **Format**, indiquez si vous souhaitez identifier les points d'accès à l'aide de numéros ou de texte.
    - Si vous sélectionnez **Numéro**, indiquez la plage de points d'accès à ajouter et, si vous ajoutez plus d'un point d'accès, sélectionnez un mode de numérotation pour l'incrémentation de chiffres.
    - Si vous sélectionnez **Texte**, indiquez un nom de point d'accès unique.
11. (*facultatif*) Ajoutez une description pour le point d'accès ou la plage de points d'accès.
12. (*facultatif*) Si vous avez choisi de formater les noms des points d'accès à l'aide de chiffres, sélectionnez l'une des options suivantes dans l'onglet **Format avancé** :



- **Préfixe** — Indiquez le texte à afficher avant le numéro principal. Ajoutez des espaces, le cas échéant.
- **Texte séparateur** — Indiquez le texte à afficher entre le numéro d'étage et le numéro du point d'accès. Ajoutez des espaces, le cas échéant.
- **Suffixe** — Indiquez le texte à afficher après le numéro principal. Ajoutez des espaces, le cas échéant.
- **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'étage dans le nom du point d'accès, sélectionnez **Aucun**.
- **Format des numéros d'unité** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'unité. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'unité dans le nom du point d'accès, sélectionnez **Aucun**.

13. Cliquez sur **Sauvegarder**.



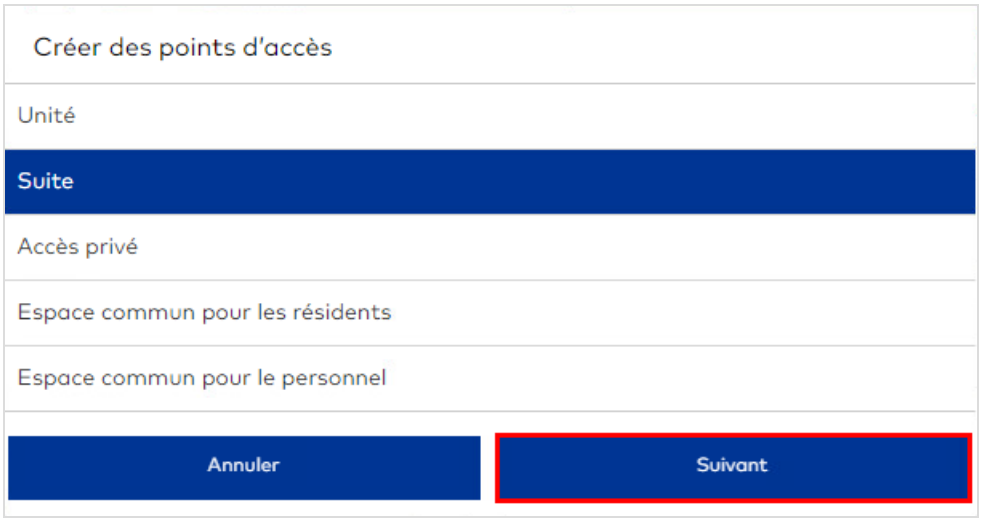
14. Lorsque vous y êtes invité, sélectionnez un profil de la serrure pour les points d'accès.
15. Lorsque vous êtes informé que l'importation est réussie, cliquez sur **OK**. La figure suivante montre l'importation des points d'accès à l'aide du fichier .csv créé dans le bloc-notes.

Ajouter des suites

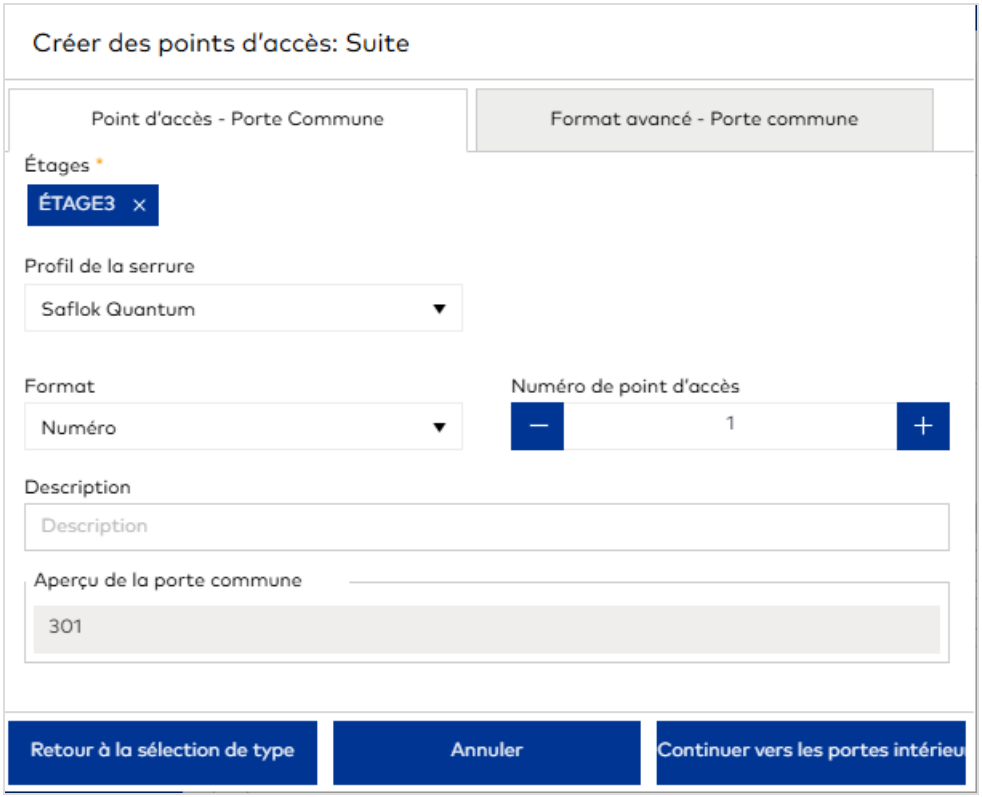
Une suite est une série d'unités communicantes comprenant une porte commune et une ou plusieurs unités de suite.

Pour ajouter des suites :

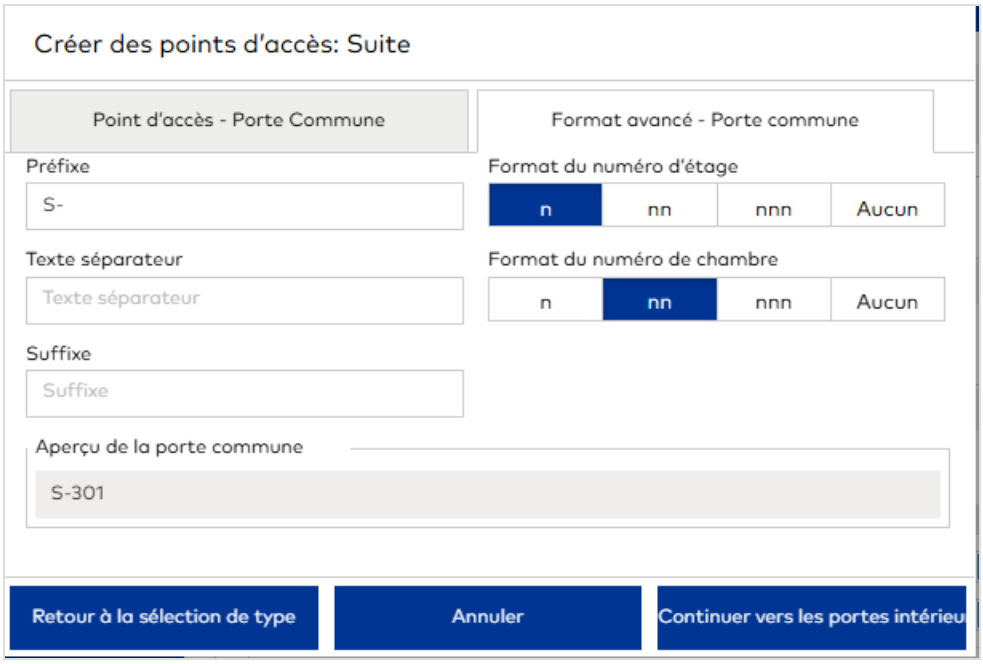
1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Étages et points d'accès**.
4. Cliquez sur **Nouveaux points d'accès**.



5. Sélectionnez **Suite**, puis cliquez sur **Suivant**. Les premières options que vous définissez concernent la porte commune.

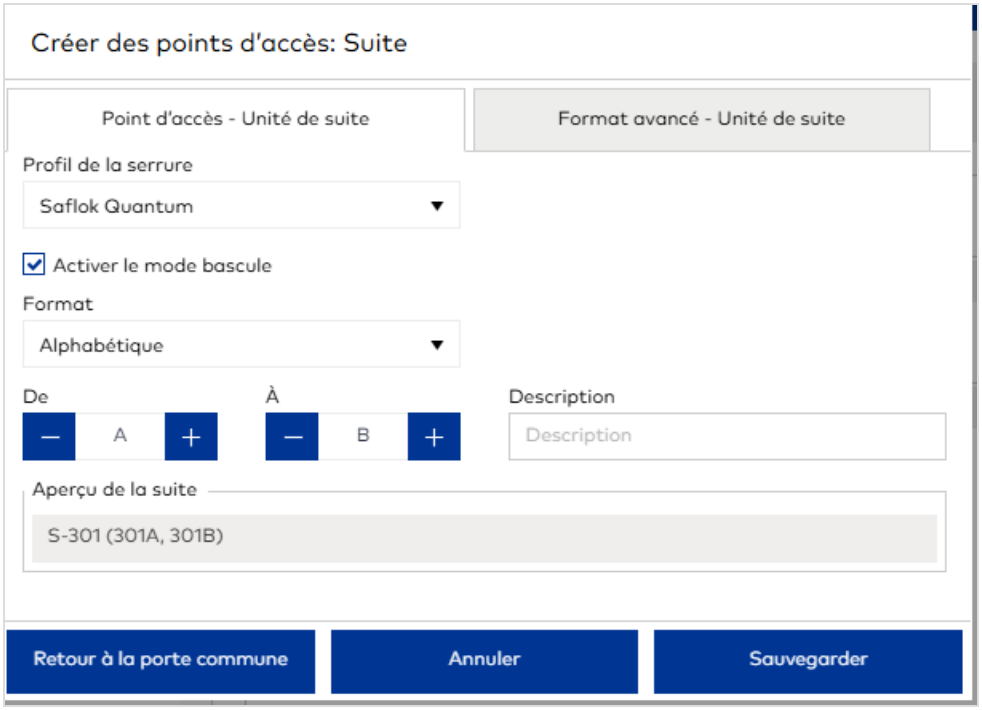


6. Pour les **Étages**, sélectionnez l'étage où vous souhaitez ajouter les points d'accès.
7. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure. Si le modèle de serrure sélectionné n'inclut pas la fonction de bascule intégrée, mais permet d'ajouter cette fonction par programmation, l'option **Activer le mode bascule** s'affiche. Si vous souhaitez que le comportement de la clé alterne entre le verrouillage et le déverrouillage chaque fois que la clé est présentée, sélectionnez **Activer le mode bascule**. Lorsque cette option est désélectionnée, la clé déverrouille uniquement.
8. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
9. **Inclure dans le fichier de téléchargement des clés mobiles** — (*(facultatif)* Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
10. Pour le **Format**, indiquez si vous souhaitez identifier les points d'accès à l'aide de numéros ou de texte.
    - Si vous sélectionnez **Numéro**, indiquez un numéro pour la porte commune.
    - Si vous sélectionnez **Texte**, indiquez un nom de point d'accès unique.
11. (*facultatif*) Ajoutez une description pour le point d'accès ou la plage de points d'accès.
12. (*facultatif*) Si vous avez choisi de formater les noms des points d'accès à l'aide de chiffres, sélectionnez l'une des options suivantes dans l'onglet **Format avancé** :

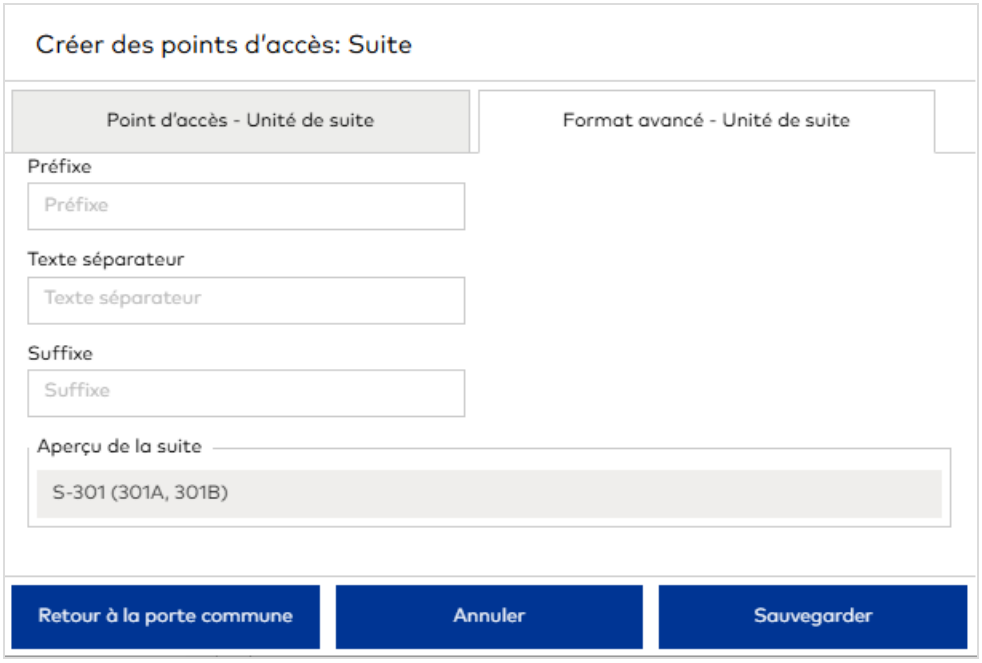


- **Préfixe** — Indiquez le texte à afficher avant le numéro principal. Ajoutez des espaces, le cas échéant.
- **Texte séparateur** — Indiquez le texte à afficher entre le numéro d'étage et le numéro du point d'accès. Ajoutez des espaces, le cas échéant.
- **Suffixe** — Indiquez le texte à afficher après le numéro principal. Ajoutez des espaces, le cas échéant.
- **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'étage dans le nom du point d'accès, sélectionnez **Aucun**.
- **Format des numéros d'unité** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'unité. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'unité dans le nom du point d'accès, sélectionnez **Aucun**.

13. Cliquez sur **Continuer vers les portes intérieures**.

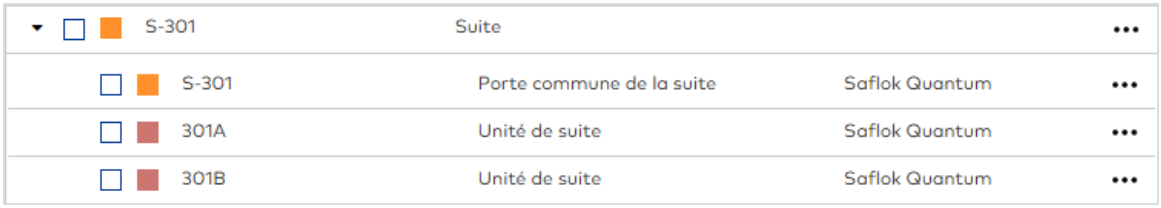


14. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure. Si le modèle de serrure sélectionné ne comprend pas le mode bascule, une option supplémentaire pour activer/désactiver le mode bascule s'affiche. Si vous souhaitez que le comportement de la clé alterne entre le verrouillage et le déverrouillage chaque fois que la clé est présentée, sélectionnez **Activer le mode bascule**. Lorsque cette option est désélectionnée, la clé déverrouille uniquement.
15. **Inclure dans le fichier de téléchargement des clés mobiles** — (*(facultatif)* Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
16. Pour le **Format**, sélectionnez si vous souhaitez identifier les points d'accès à l'aide de caractères alphabétiques, de chiffres ou de texte. Si vous utilisez des lettres ou des chiffres, indiquez la plage de points d'accès à ajouter ; et, si vous ajoutez plusieurs points d'accès, sélectionnez un mode de numérotation pour l'incrémentation de chiffres.
17. (*facultatif*) Ajoutez une description pour le point d'accès ou la plage de points d'accès.
18. (*facultatif*) Si vous avez choisi de formater les noms des points d'accès à l'aide de caractères alphabétiques ou de chiffres, spécifiez l'une des options suivantes dans l'onglet **Format avancé** :



- **Préfixe** — Indiquez le texte à afficher avant le numéro principal. Ajoutez des espaces, le cas échéant.
- **Texte séparateur** — Indiquez le texte à afficher entre le numéro d'étage et le numéro du point d'accès. Ajoutez des espaces, le cas échéant.
- **Suffixe** — Indiquez le texte à afficher après le numéro principal. Ajoutez des espaces, le cas échéant.
- **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'étage dans le nom du point d'accès, sélectionnez **Aucun**.
- **Format des numéros d'unité** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'unité. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'unité dans le nom du point d'accès, sélectionnez **Aucun**.

19. Cliquez sur **Sauvegarder**.



Ajouter des espaces communs pour les résidents

Les espaces communs résident sont des espaces sur votre site qui sont configurés pour un accès général par les résidents et le personnel, tels que les réceptions, le parking et les installations de loisirs. Lorsque vous créez un espace commun, vous avez la possibilité de limiter l'accès.

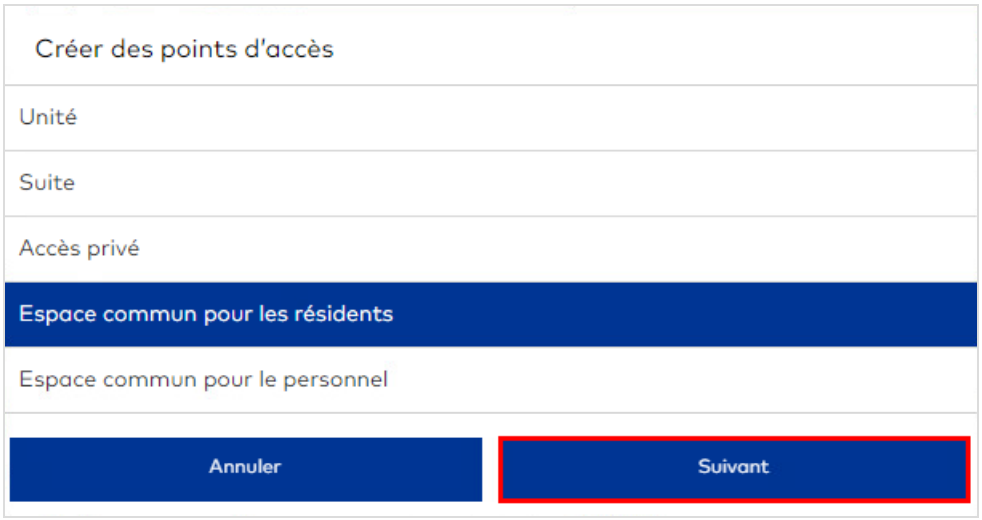
Pour en savoir plus sur les espaces communs et sur la façon dont l'accès limité affecte la configuration, voir Espaces communs résident dans « En savoir plus sur le configurateur de site ».

Cette section fournit des instructions pour ajouter les types suivants de points d'accès aux espaces communs :

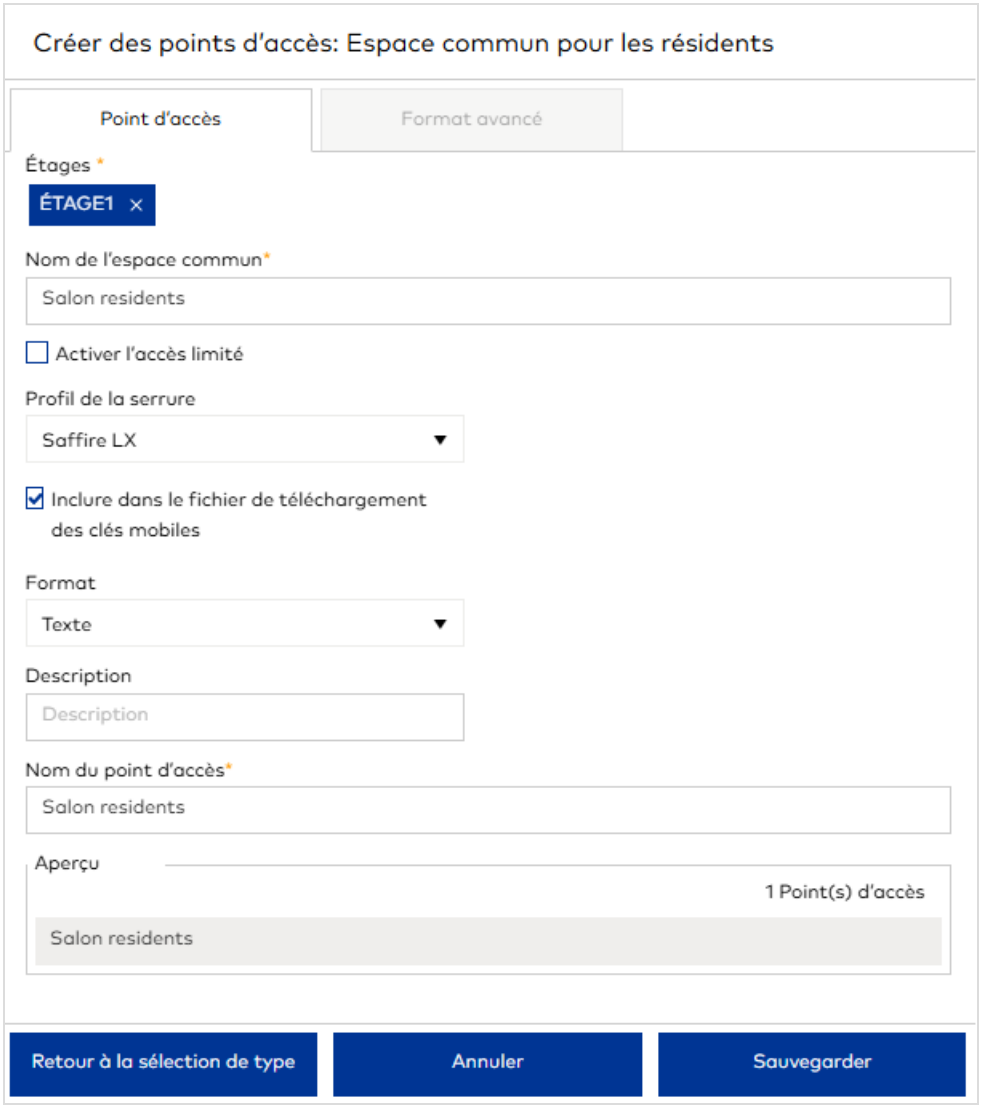
- Ajout des espaces communs résident illimités
- Ajout des espaces communs résident à accès limité
- Ajout d'Espaces Communs aux Groupes d'espaces communs

Ajout des espaces communs résident illimités

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Étages et points d'accès**.
4. Cliquez sur **Nouveaux points d'accès**.



5. Sélectionnez **Espace commun résident**, puis cliquez sur **Suivant**.



6. Pour les **Étages**, sélectionnez l'étage où vous souhaitez ajouter le point d'accès.
7. Pour le **Nom de l'espace commun**, indiquez un nom unique ne dépassant pas 20 caractères. Il s'agit du nom du groupe d'espaces communs. Vous pouvez ajouter des espaces communs supplémentaires au groupe.

   Lorsque l'accès limité n'est pas activé, ces espaces communs et les points d'accès associés sont implicitement accessibles par toutes les clés de résidents.

8. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure.

   Le mode bascule n'est pris en charge que pour les unités et les unités de suite.

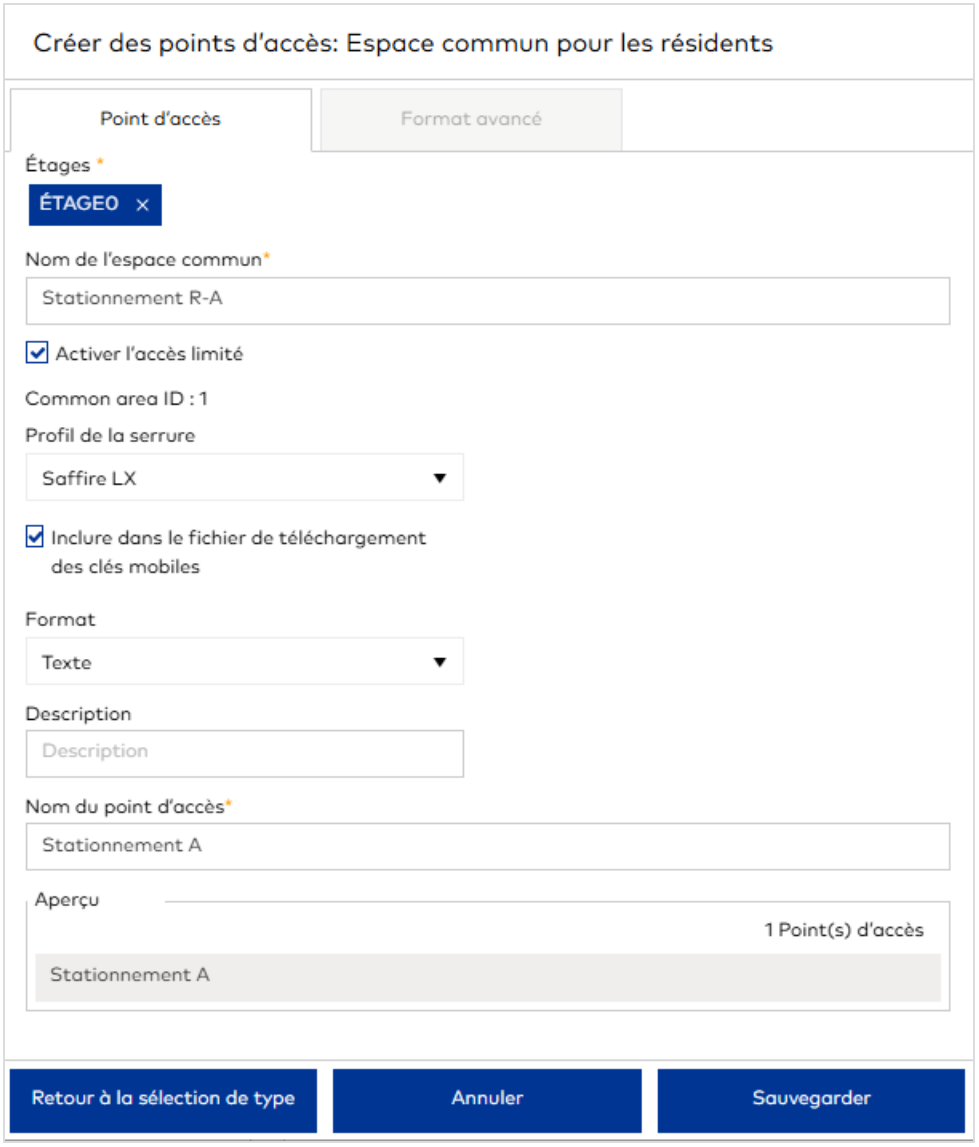
9. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
10. **Inclure dans le fichier de téléchargement des clés mobiles** — (*facultatif*) Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.

11. Pour le **Format**, indiquez si vous souhaitez identifier les points d'accès à l'aide de numéros ou de texte.
    - Si vous sélectionnez **Numéro**, indiquez la plage de points d'accès à ajouter et, si vous ajoutez plus d'un point d'accès, sélectionnez un mode de numérotation pour l'incrémentation de chiffres.
    - Si vous sélectionnez **Texte**, indiquez un nom de point d'accès unique.
12. (*facultatif*) Ajoutez une description pour le point d'accès ou la plage de points d'accès.
13. (*facultatif*) Si vous avez choisi de formater les noms des points d'accès à l'aide de chiffres, sélectionnez l'une des options suivantes dans l'onglet **Format avancé** :
    - **Préfixe** — Indiquez le texte à afficher avant le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Texte séparateur** — Indiquez le texte à afficher entre le numéro d'étage et le numéro du point d'accès. Ajoutez des espaces, le cas échéant.
    - **Suffixe** — Indiquez le texte à afficher après le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'étage dans le nom du point d'accès, sélectionnez **Aucun**.
    - **Format des numéros d'unité** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'unité. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'unité dans le nom du point d'accès, sélectionnez **Aucun**.
14. Cliquez sur **Sauvegarder**.



Ajout des espaces communs résident à accès limité

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Étages et points d'accès**.
4. Cliquez sur **Nouveaux points d'accès**.
5. Sélectionnez **Espace commun résident**, puis cliquez sur **Suivant**.



6. Pour les **Étages**, sélectionnez l'étage où vous souhaitez ajouter le point d'accès.
7. Pour le **Nom de l'espace commun**, indiquez un nom unique ne dépassant pas 20 caractères. Il s'agit du nom du groupe d'espaces communs. Vous pouvez ajouter des espaces communs supplémentaires au groupe.
8. Sélectionnez l'option **Activer l'accès limité**. L'espace commun doit être associé à un profil dans ***Gestion des accès > Accès aux espaces communs*** .
9. Pour **ID d'espace commun**, acceptez la valeur automatiquement que le système remplit automatiquement.
10. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure.

    Le mode bascule n'est pris en charge que pour les unités et les unités de suite.

11. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
12. **Inclure dans le fichier de téléchargement des clés mobiles** — (*facultatif*) Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport

généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.

13. Pour le **Format**, indiquez si vous souhaitez identifier les points d'accès à l'aide de numéros ou de texte.
    - Si vous sélectionnez **Numéro**, indiquez la plage de points d'accès à ajouter et, si vous ajoutez plus d'un point d'accès, sélectionnez un mode de numérotation pour l'incrémentation de chiffres.
    - Si vous sélectionnez **Texte**, indiquez un nom de point d'accès unique.
14. (*facultatif*) Ajoutez une description pour le point d'accès ou la plage de points d'accès.
15. (*facultatif*) Si vous avez choisi de formater les noms des points d'accès à l'aide de chiffres, sélectionnez l'une des options suivantes dans l'onglet **Format avancé** :
    - **Préfixe** — Indiquez le texte à afficher avant le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Texte séparateur** — Indiquez le texte à afficher entre le numéro d'étage et le numéro du point d'accès. Ajoutez des espaces, le cas échéant.
    - **Suffixe** — Indiquez le texte à afficher après le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'étage dans le nom du point d'accès, sélectionnez **Aucun**.
    - **Format des numéros d'unité** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'unité. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'unité dans le nom du point d'accès, sélectionnez **Aucun**.
16. Cliquez sur **Sauvegarder**.



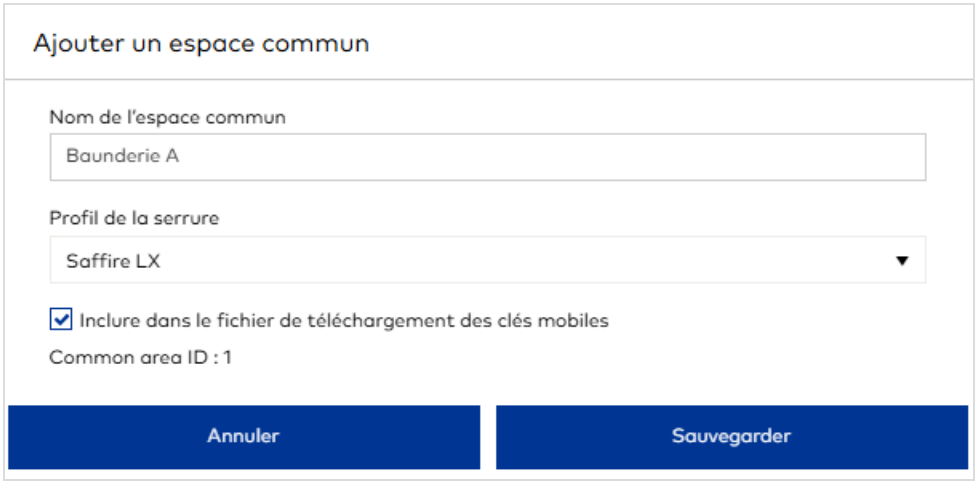
Ajout d'espaces communs aux groupes d'espaces communs

Bien que vous puissiez ajouter plusieurs espaces communs à un même groupe, l'accès est activé au niveau du groupe. Pour ajouter un espace commun à un groupe d'espaces communs :

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez le groupe d'espaces communs dans lequel vous souhaitez ajouter l'espace commun.



3. Cliquez sur ***(Plus) ··· > Ajouter un espace commun***.



4. Indiquez un nom unique pour l'espace commun.
5. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure.

   Le mode bascule n'est pris en charge que pour les unités et les unités de suite.

6. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
7. **Inclure dans le fichier de téléchargement des clés mobiles** — (*(facultatif)* Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
8. Cliquez sur **Sauvegarder**.



Ajouter des espaces communs pour le personnel

Les espaces communs pour le personnel sont le type de points d'accès configurés pour un accès général uniquement par le personnel, tels que les salles de pause, les placards à fournitures. Lorsque vous créez un espace commun, vous avez la possibilité de limiter l'accès.

Pour en savoir plus sur les espaces communs pour le personnel et sur la façon dont l'accès limité affecte la configuration, voir « Espaces communs pour le personnel à accès limité et illimité ».

Cette section fournit des instructions pour ajouter les types suivants de points d'accès aux espaces communs :

- Ajout d'Espaces communs pour le personnel illimités
- Ajout d'Espaces communs pour le personnel à accès limité
- Ajout d'Espaces Communs aux Groupes d'espaces communs

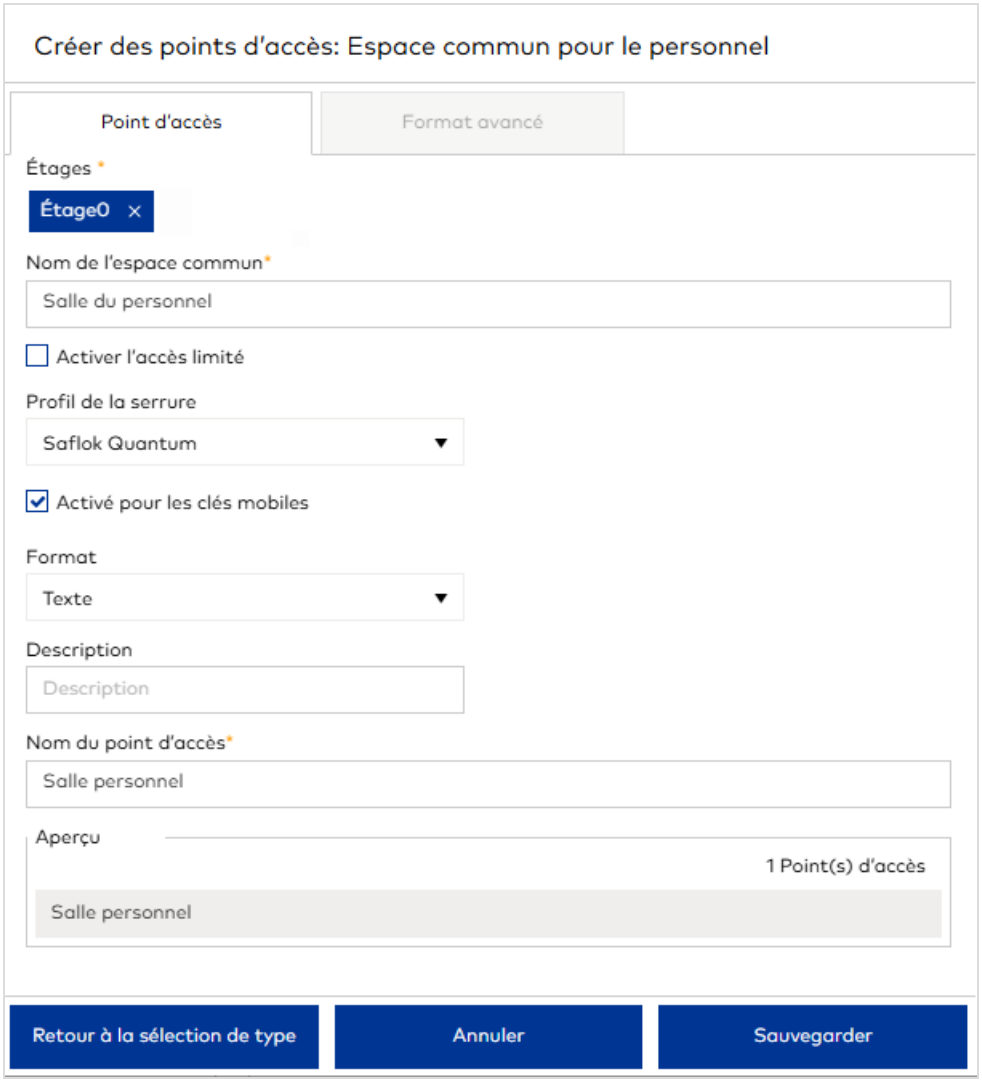
Ajout d'espaces communs pour le personnel illimités

Les espaces communs pour le personnel illimités sont ajoutés à chaque clé du personnel/prestataire.

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Étages et points d'accès**.
4. Cliquez sur **Nouveaux points d'accès**.



5. Sélectionnez **Espace commun pour le personnel**, puis cliquez sur **Suivant**.

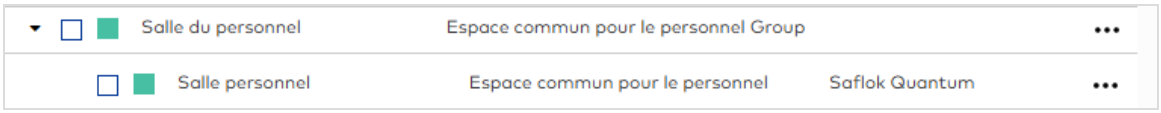


6. Pour les **Étages**, sélectionnez l'étage où vous souhaitez ajouter le point d'accès.
7. Pour le **Nom de l'espace commun**, indiquez un nom unique ne dépassant pas 20 caractères. Il s'agit du nom du groupe d'espaces communs. Vous pouvez ajouter des espaces communs supplémentaires au groupe.
8. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure.

   Le mode bascule n'est pris en charge que pour les unités et les unités de suite.

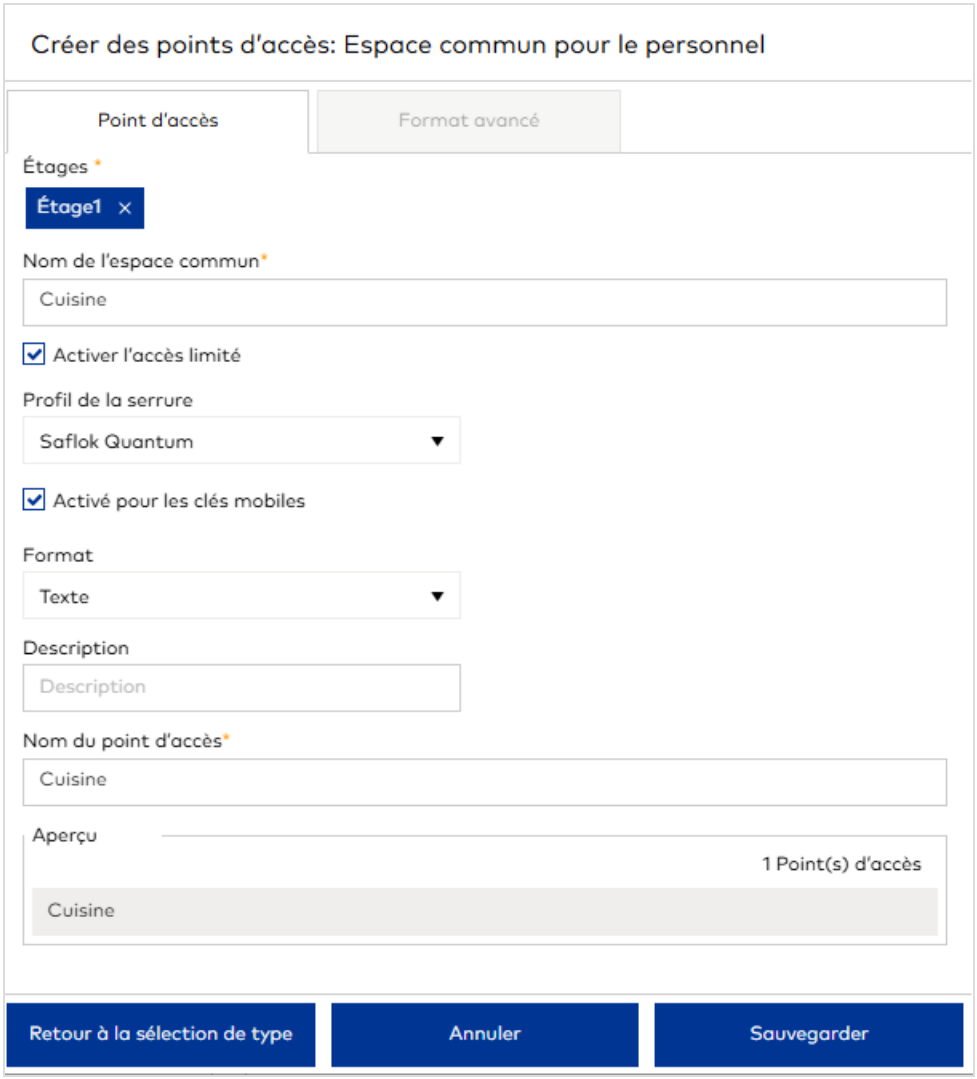
9. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
10. **Inclure dans le fichier de téléchargement des clés mobiles** — (*facultatif*) Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
11. Pour le **Format**, indiquez si vous souhaitez identifier les points d'accès à l'aide de numéros ou de texte.
    - Si vous sélectionnez **Numéro**, indiquez la plage de points d'accès à ajouter et, si vous ajoutez plus d'un point d'accès, sélectionnez un mode de numérotation pour l'incrémentation de chiffres.
    - Si vous sélectionnez **Texte**, indiquez un nom de point d'accès unique.

12. (*facultatif*) Ajoutez une description pour le point d'accès ou la plage de points d'accès.
13. (*facultatif*) Si vous avez choisi de formater les noms des points d'accès à l'aide de chiffres, sélectionnez l'une des options suivantes dans l'onglet **Format avancé** :
    - **Préfixe** — Indiquez le texte à afficher avant le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Texte séparateur** — Indiquez le texte à afficher entre le numéro d'étage et le numéro du point d'accès. Ajoutez des espaces, le cas échéant.
    - **Suffixe** — Indiquez le texte à afficher après le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'étage dans le nom du point d'accès, sélectionnez **Aucun**.
    - **Format des numéros d'unité** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'unité. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'unité dans le nom du point d'accès, sélectionnez **Aucun**.
14. Cliquez sur **Sauvegarder**.



Ajout d'espaces communs pour le personnel à accès limité

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Étages et points d'accès**.
4. Cliquez sur **Nouveaux points d'accès**.
5. Sélectionnez **Espace commun pour le personnel**, puis cliquez sur **Suivant**.



6. Pour les **Étages**, sélectionnez l'étage où vous souhaitez ajouter le point d'accès.
7. Pour le **Nom de l'espace commun**, indiquez un nom unique ne dépassant pas 20 caractères. Il s'agit du nom du groupe d'espaces communs. Vous pouvez ajouter des espaces communs supplémentaires au groupe.
8. Sélectionnez l'option **Activer l'accès limité**.
9. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure.

   Le mode bascule n'est pris en charge que pour les unités et les unités de suite.

10. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
11. **Inclure dans le fichier de téléchargement des clés mobiles** — (*facultatif*) Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
12. Pour le **Format**, indiquez si vous souhaitez identifier les points d'accès à l'aide de numéros ou de texte.
    - Si vous sélectionnez **Numéro**, indiquez la plage de points d'accès à ajouter et, si vous ajoutez plus d'un point d'accès, sélectionnez un mode de numérotation pour l'incrémentation de chiffres.

- Si vous sélectionnez **Texte**, indiquez un nom de point d'accès unique.

13. (*facultatif*) Ajoutez une description pour le point d'accès ou la plage de points d'accès.
14. (*facultatif*) Si vous avez choisi de formater les noms des points d'accès à l'aide de chiffres, sélectionnez l'une des options suivantes dans l'onglet **Format avancé** :
    - **Préfixe** — Indiquez le texte à afficher avant le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Texte séparateur** — Indiquez le texte à afficher entre le numéro d'étage et le numéro du point d'accès. Ajoutez des espaces, le cas échéant.
    - **Suffixe** — Indiquez le texte à afficher après le numéro principal. Ajoutez des espaces, le cas échéant.
    - **Format du numéro d'étage** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'étage. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'étage dans le nom du point d'accès, sélectionnez **Aucun**.
    - **Format des numéros d'unité** — Sélectionnez le nombre de chiffres à afficher pour les numéros d'unité. Des zéros sont antéposés devant le premier chiffre différent de zéro. Par exemple, sélectionnez **n** pour 1, **nn** pour 01, **nnn** pour 001. Pour masquer le numéro d'unité dans le nom du point d'accès, sélectionnez **Aucun**.
15. Cliquez sur **Sauvegarder**.



Avant de remettre au personnel une clé d'accès aux espaces communs pour le personnel à accès limité, vous devez soit ajouter l'espace commun à l'identifiant du personnel attribué, soit associer l'espace commun à l'identifiant du personnel attribué dans ***Gestion des accès > Accès aux espaces communs***.

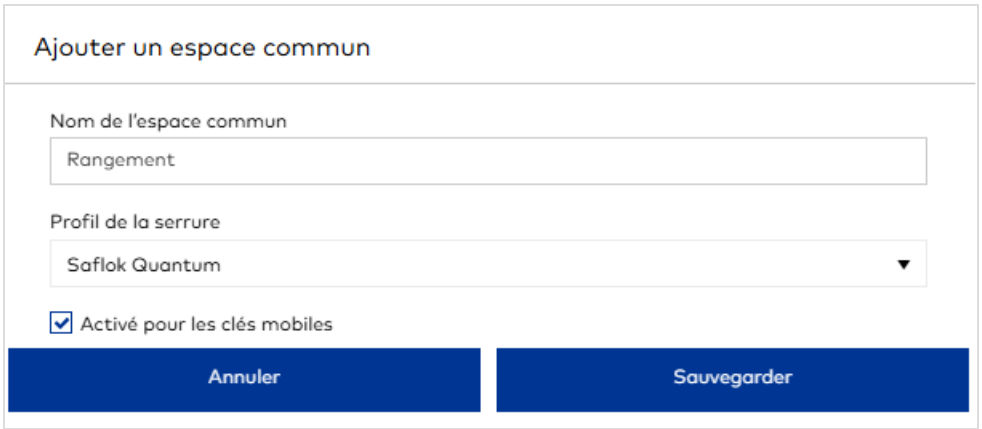
Ajout d'espaces communs aux groupes d'espaces communs

Bien que vous puissiez ajouter plusieurs espaces communs à un même groupe, l'accès est activé au niveau du groupe. Pour ajouter un espace commun à un groupe d'espaces communs :

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez le groupe d'espaces communs dans lequel vous souhaitez ajouter l'espace commun.



3. Cliquez sur ***(Plus) ··· > Ajouter un espace commun***.



4. Indiquez un nom unique pour l'espace commun.
5. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure.

   Le mode bascule n'est pris en charge que pour les unités et les unités de suite.

6. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
7. **Inclure dans le fichier de téléchargement des clés mobiles** — (*facultatif*) Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
8. Cliquez sur **Sauvegarder**.

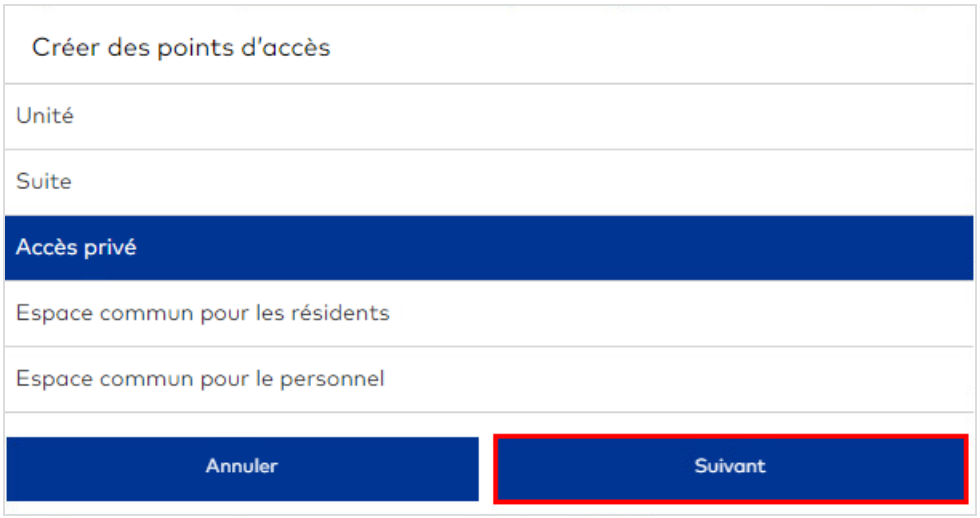


Ajouter des accès privés

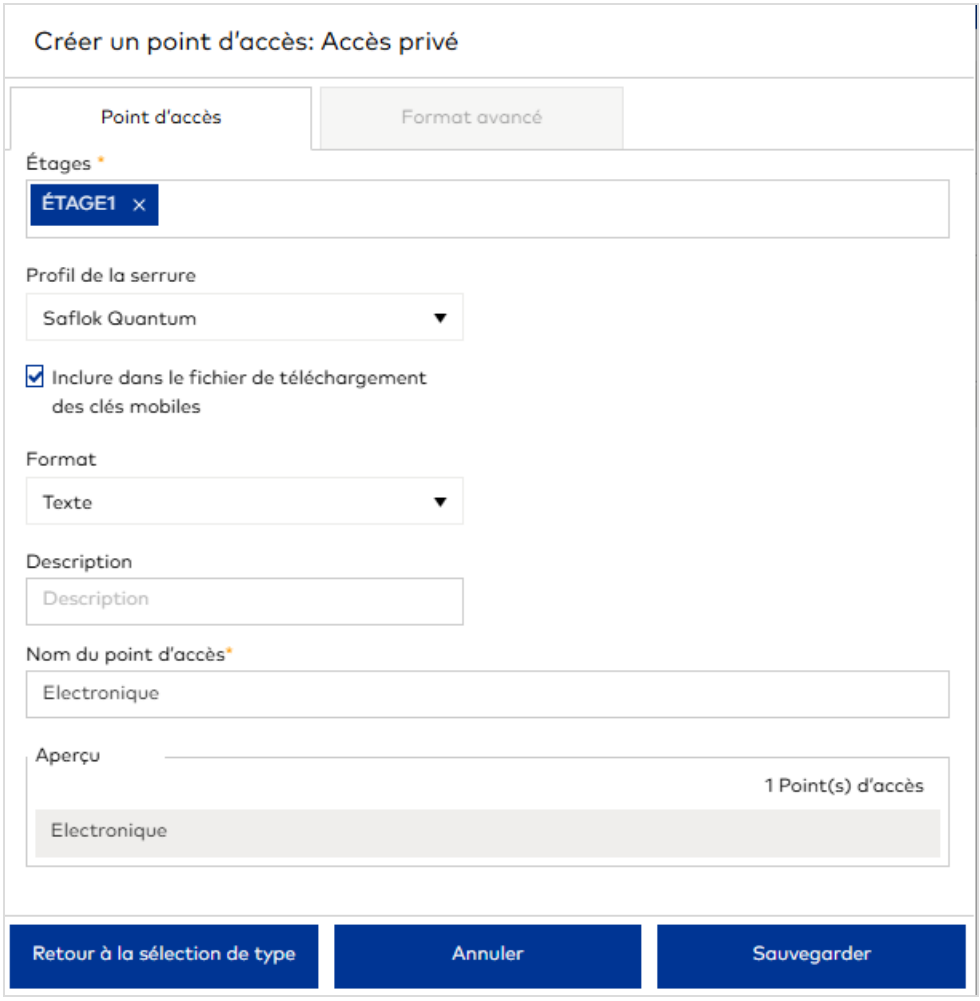
Un accès privé est un type de point d'accès destiné à fournir un accès à l'espace réservé au personnel.

Pour ajouter des accès privés :

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Étages et points d'accès**.
4. Cliquez sur **Nouveaux points d'accès**.



5. Sélectionnez **Accès privé**, puis cliquez sur **Suivant**.



6. Pour les **Étages**, sélectionnez un ou plusieurs étages où vous souhaitez ajouter les points d'accès.
7. Pour le **Profil de la serrure**, sélectionnez le modèle de serrure.

> Le mode bascule n'est pris en charge que pour les unités et les unités de suite.



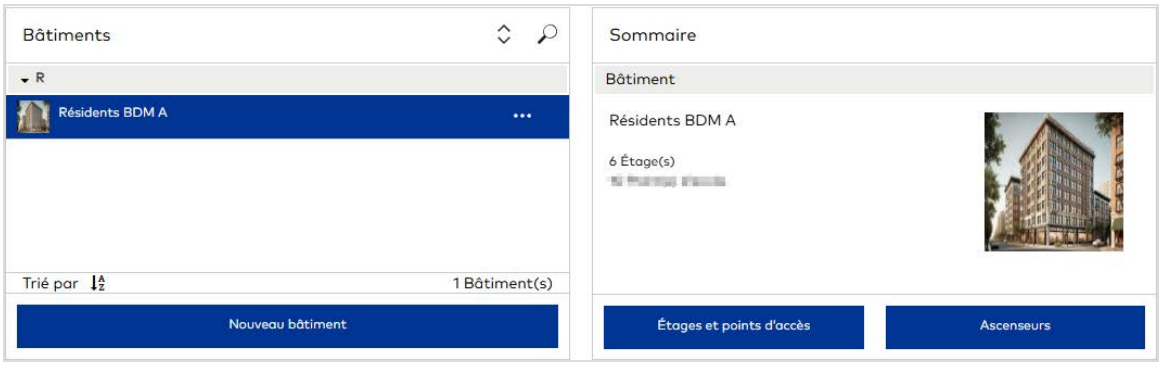
Ajouter des ascenseurs

Le processus de configuration de l'accès aux ascenseurs implique l'ajout d'au moins un groupe d'ascenseurs, l'ajout des ascenseurs pour chaque groupe, puis la cartographie des cartes relais d'ascenseurs aux étages pour chaque groupe d'ascenseurs. Pour en savoir plus sur les ascenseurs, voir « Ascenseurs » dans *En savoir plus sur le configurateur de site*.

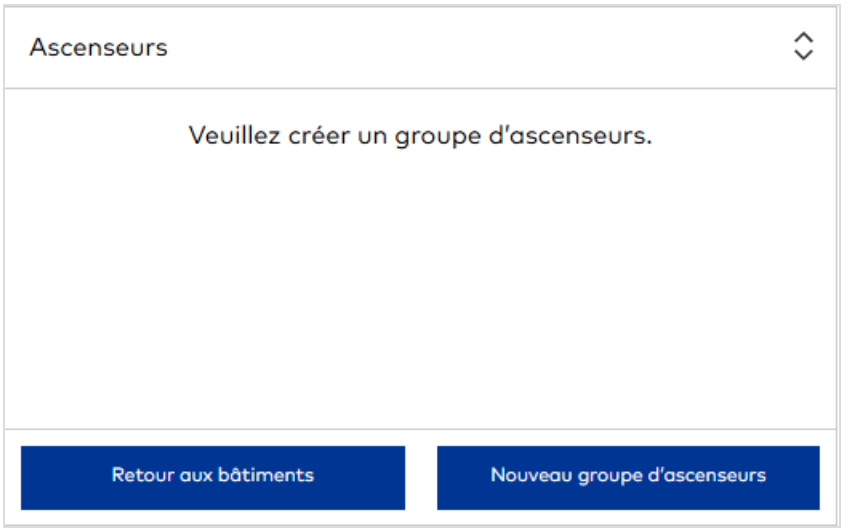
Ajouter des groupes d'ascenseurs

Pour ajouter un groupe d'ascenseurs :

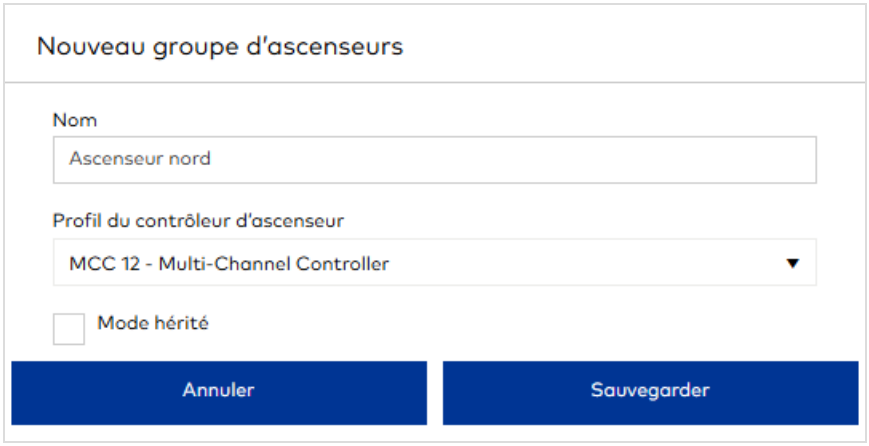
1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.



3. Cliquez sur **Ascenseurs**.



4. Cliquez sur **Nouveau groupe d'ascenseurs**.



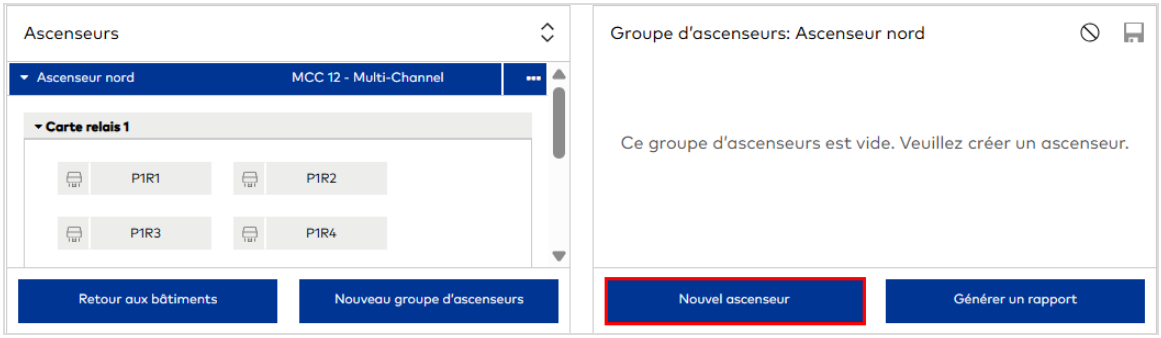
5. Indiquez un nom unique pour le groupe d'ascenseurs.
6. Sélectionnez un profil du contrôleur d'ascenseur. (RAC5 doit être configuré dans **Gestion des périphériques**.)
7. (périphériques RAC5 uniquement) Sélectionnez le niveau sonore des bips audibles lorsque le périphérique est connecté au poste de travail et lorsque des clés sont créées. Valeur par défaut : Élevé.
8. Cliquez sur **Sauvegarder**. Le groupe d'ascenseurs est répertorié dans la liste des ascenseurs, ainsi que le nombre de lignes de cartes relais prises en charge par le profil de la serrure. Les lignes de carte relais sont l'endroit où vous cartographiez l'accès de relais d'un étage à l'autre.



Ajouter des ascenseurs

Pour ajouter un ascenseur :

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Ascenseurs**.



4. Sélectionnez le groupe d'ascenseurs où vous souhaitez ajouter l'ascenseur.
5. Cliquez sur **Nouvel ascenseur**.



6. Indiquez un nom pour l'ascenseur. Pour les contrôleurs RAC 5, indiquez le nom du point d'accès.
7. (*Contrôleurs MFC uniquement*) Sélectionnez l'activation ou non d'une deuxième carte relais de lecteur pour l'ascenseur.
8. (*Contrôleurs MFC uniquement*) Indiquez un nom pour tout lecteur.
9. **Inclure dans le fichier de téléchargement des clés mobiles** — (*(facultatif)* Si vous disposez d'une licence pour les clés mobiles, sélectionnez cette option si la serrure est équipée pour accepter les identifiants de clés mobiles. En sélectionnant cette option, le point d'accès est répertorié dans le fichier de téléchargement des clés mobiles, un rapport généré à partir du menu contextuel Bâtiments dans Configurateur de site. Cette option n'a qu'une valeur informative et n'a aucune incidence sur la fonction de clé mobile.
10. Cliquez sur **Sauvegarder**.

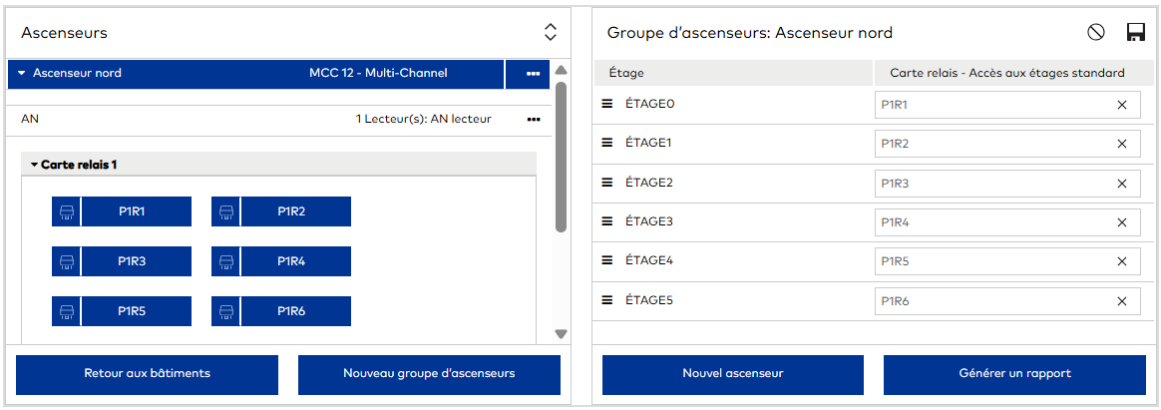
Cartographier l'accès aux étages

La cartographie des relais d'étages contrôle l'accès par ascenseur aux étages du bâtiment. Si vous n'associez pas un étage à un relais, il n'existe aucun accès par ascenseur à l'étage.

Pour cartographier l'accès aux étages :

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Ascenseurs**.
4. Sélectionnez le groupe d'ascenseurs où vous souhaitez cartographier l'accès aux étages. Si le groupe d'ascenseurs contient au moins un ascenseur, la liste des étages du bâtiment est affichée.

5. Sélectionnez une carte relais à configurer.
6. Glissez-déposez des cartes relais (P*n*R*n*) dans la colonne Carte relais de l'étage que vous souhaitez cartographier. Le même relais peut être associé à plusieurs étages, mais chaque étage ne peut être associé qu'à un seul relais.
7. Cliquez sur **(Sauvegarder)**.



Étape 3

Configurer l'accès

Cette section comprend les sujets suivants :

- En savoir plus sur la gestion des accès 89
- Ajouter des horaires de libre passage 93
- Ajouter des horaires d'accès 95
- Ajouter les horaires des clés du personnel 98
- Créer des groupes de points d'accès 100
- Ajouter des identifiants 102
- Attribuer des horaires 106
- Configurer les profils d'accès aux espaces communs à accès limité 107

En savoir plus sur la gestion des accès

Le module de **Gestion des accès** est l'endroit où sont configurés les contrôles d'accès à tous les points d'accès créés dans **Configurateur de site**. Bien que toutes les options de configuration fonctionnent ensemble pour contrôler l'accès, la définition des identifiants et la configuration de l'accès aux espaces communs à accès limité sont les principaux objectifs de la **Gestion des accès**. L'attribution horaire est un élément facultatif. La figure suivante résume toutes les options de configuration d'accès.



Identifiants

Les identifiants sont essentiellement les droits d'accès encodés sur les clés. Au cours du processus d'ajout d'un identifiant, vous sélectionnez les points d'accès que vous souhaitez que l'identifiant autorise. Vous pouvez ajouter des points d'accès individuels et des groupes de points d'accès. Vous pouvez également sélectionner un horaire des clés du personnel pour chaque identifiant.

Structure des identifiants

Tous les identifiants dans Community sont organisés selon trois niveaux de hiérarchie :

Type de catégorie d'identifiants > Catégorie d'identifiants > Identifiant

Les *Types de catégories d'identifiants* sont des définitions fixées dont proviennent toutes les catégories d'identifiants. Les définitions fixées se composent d'une ou plusieurs propriétés persistantes. Par exemple, les clés encodées avec un identifiant basé sur un type de catégorie d'identifiants Urgence disposent toujours de la capacité de forcer l'ouverture d'un pêne dormant projeté ou de contourner un verrou d'intimité. D'autres propriétés déterminent si l'accès est configuré dans **Gestion des accès** ou lors de la création de la clé, si le mode bascule est pris en charge, et le nombre de fois qu'une clé peut être utilisée.

Les catégories d'identifiants servent à transmettre tout établissement défini pour le type de catégorie aux identifiants. La catégorie d'identifiants par défaut pour chaque type de catégorie porte le même nom que le type. Par exemple, la catégorie d'identifiants par défaut pour le type de catégorie d'urgence est *Urgence*.

Les *Identifiants* sont le niveau auquel l'accès est activé. Selon le type de catégorie/la catégorie sélectionné(e), les groupes de points d'accès et les points d'accès sont sélectionnés lors de la définition de l'identifiant ou au moment de la création de la clé.

Catégories d'identifiants par défaut pour les clés du personnel/prestataire

Les catégories d'identifiants utilisées pour créer les clés du personnel/prestataire offrent chacune une combinaison unique de caractéristiques. Le tableau suivant résume les types de catégories d'identifiants et les catégories d'identifiants par défaut utilisées pour créer les clés du personnel/prestataire.

La catégorie d'identifiants Urgence n'est disponible que lorsque les clés d'urgence sont activées dans ***Paramètres du système > Clés du personnel/prestataire***.

Type de catégorie d'identifiants/ Catégorie d'identifiants par défaut	Unique Site	Accès	Bascule	Espaces communs
Urgence	A toujours la priorité sur le pêne dormant/ verrou d'intimité	Prédéfini	Valeur par défaut : N° Pour les types de points d'accès Unité/Suite, peut être activé dans Configurateur de site.	Prédéfini
Usage restreint	L'usage de la clé est limité à un nombre de fois déterminé	Prédéfini	Non	Espace commun Profil d'accès
Personnel	Aucun	Prédéfini	Valeur par défaut : N° Pour les types de points d'accès Unité/Suite, peut être activé dans Configurateur de site.	Espace commun Profil d'accès
Personnel (accès variable)	Aucun	Variable	Valeur par défaut : N° Pour les types de points d'accès Unité/Suite, peut être activé dans Configurateur de site.	Espace commun Profil d'accès
Prestataire	Aucun	Variable	Valeur par défaut : N° Pour les types de points d'accès Unité/Suite, peut être activé dans Configurateur de site.	Espace commun Profil d'accès

En savoir plus sur chaque type de catégorie d'identifiants et les catégories d'identifiants par défaut :

- **Clés d'urgence** — La principale caractéristique de la catégorie Urgence est que les clés forcent toujours l'ouverture des pênes dormants ou des verrous d'intimité actifs projetés. Comme telle, réservez cette catégorie au personnel de secours uniquement, comme les pompiers et les officiers de sécurité. Tous les accès sont prédéfinis (aucun point d'accès ne peut être sélectionné lors de la création des clés). Par défaut, les clés ne permettent pas de basculer l'accès ; toutefois, le mode bascule est pris en charge pour les types de points d'accès d'unités et de suites si l'option **Activer le mode bascule** est sélectionnée lors de la création du point d'accès dans **Configurateur de site**.
- **Clés à usage restreint** — À l'exception de tous les espaces communs, l'accès est prédéfini. Tous les espaces communs illimités et limités pour les résidents et le personnel doivent être associés à un profil *Usage restreint* dans **Accès aux espaces communs** avant d'apparaître lors de la création des clés. Les clés encodées au moyen d'identifiants provenant de cette catégorie ne peuvent pas commuter les accès. La caractéristique particulière permettant de différencier la catégorie « Usage restreint » est que l'accès est limité à un nombre de fois prédéfini. La limite est indiquée dans ***Paramètres du système > Clés du personnel/prestataire***. Par exemple, si la limite est de six, la clé ouvre la serrure les six premières fois consécutives puis arrive à expiration.
- **Clés du personnel** — Les options de la catégorie Personnel sont flexibles pour vous permettre de créer les différents types de clés nécessaires au personnel :
  - **Personnel** — À l'exception de tous les espaces communs, l'accès est prédéfini. Tous les espaces communs illimités et limités pour les résidents et le personnel sont sélectionnés lors de la création des clés ; cependant, les espaces communs doivent d'abord être associés à un profil du *Personnel* dans **Accès aux espaces communs**. Par défaut, les clés ne permettent pas de basculer l'accès ; toutefois, le mode bascule est pris en charge pour les types de points d'accès d'unités et de suites si l'option **Activer le mode bascule** est sélectionnée lors de la création du point d'accès dans **Configurateur de site**.
  - **Personnel (accès variable)** — Tous les accès sont autorisés lors de la création des clés. Tous les espaces communs illimités et limités pour les résidents et le personnel sont sélectionnés lors de la création des clés ; cependant, ils doivent être associés à un profil du *Personnel (accès variable)* dans **Accès aux espaces communs** avant d'apparaître lors de la création des clés. Par défaut, les clés ne permettent pas de basculer l'accès ; toutefois, le mode bascule est pris en charge pour les types de points d'accès d'unités et de suites si l'option **Activer le mode bascule** est sélectionnée lors de la création du point d'accès dans **Configurateur de site**.
- **Clés du prestataire** — Tout accès est autorisé lors de la création des clés. Tous les espaces communs illimités et limités pour les résidents et le personnel sont sélectionnés lors de la création des clés ; cependant, ils doivent être associés à un profil de *Prestataire* dans Accès aux espaces communs avant d'apparaître lors de la création des clés. Par défaut, les

clés ne permettent pas de basculer l'accès ; toutefois, le mode bascule est pris en charge pour les types de points d'accès d'unités et de suites si l'option **Activer le mode bascule** est sélectionnée lors de la création du point d'accès dans **Configurateur de site**.

L'accès supplémentaire aux étages est configuré lors de la création des clés pour toutes les catégories d'identifiants.

Accès prédéfini et variable

L'accès prédéfini et variable fait référence à la façon dont les points d'accès sont autorisés lors de la création des clés du personnel/prestataire. Pour les types de catégories d'identifiants avec accès variable, tout accès est autorisé lors de la création des clés. Pour les types de catégories d'identifiants avec accès prédéfini, les points d'accès sont autorisés par un identifiant défini dans ***Gestion des accès > Gestion des identifiants***. Lors de la création d'une clé avec accès prédéfini, seuls les points d'accès de l'identifiant sélectionné sont autorisés. (Les espaces communs à accès limité sont l'exception car ils peuvent être autorisés lors de la création des clés pour toutes les catégories, sauf la catégorie Urgence.)

Mode bascule

La bascule est une fonction qui fait passer l'état d'une serrure de l'état *Verrouillé* à l'état *Déverrouillé* chaque fois qu'une clé valide est présentée. Par exemple, l'état par défaut d'une serrure est *Verrouillé*. La première fois qu'une clé est présentée, la serrure passe à un état *Déverrouillé*. La porte est ouverte et reste accessible jusqu'à ce que la clé soit présentée à nouveau à la serrure ou que le verrou d'intimité intérieur soit sorti.

La bascule est activée de différentes manières selon le type de serrure et la catégorie d'identifiants :

- La bascule peut être une caractéristique mécanique de la serrure. Par exemple, toutes les serrures Nova fonctionnent en mode bascule.
- Pour les identifiants basés sur les catégories Urgence, Personnel, Personnel (accès variable) et Prestataire, la bascule est activée pour les points d'accès d'unités et de suites en sélectionnant l'option **Activer le mode bascule** lors de la création du point d'accès d'unités/suites dans Configurateur de site. Valide pour les profils de serrures suivants : Saflok Quantum, Saflok Confidant, Saflock RT/RT+, RCU, Pixel et Saffire LX, RAC5 XT, RAC5 Lite.
- Pour les identifiants basés sur la catégorie d'usage restreint, le mode bascule n'est pas pris en charge.

Espaces communs à accès limité

À l'exception des clés encodées avec l'identifiant Urgence, les espaces communs à accès limité doivent être configurés dans ***Gestion des accès > Accès aux espaces communs***. En résumé, vous devez créer un profil d'accès aux espaces communs pour le type d'identifiant sélectionné, puis associer les espaces communs à accès limité soit aux unités/unités de suites (pour l'accès des résidents), soit aux identifiants (pour l'accès du personnel). Lors de la création de la clé, les espaces communs à accès limité sont répertoriés avec la possibilité d'inclure ou d'exclure l'accès sur la clé.

Catégories d'identifiants par défaut pour les clés système

Les types de catégories d'identifiants/catégories par défaut suivants sont utilisés pour créer des identifiants pour les clés système :

- **Verrouillage** — Cette catégorie est utilisée pour créer des identifiants système autorisant des clés de verrouillage.
- **Déverrouillage** — Cette catégorie est utilisée pour créer des identifiants système autorisant des clés de déverrouillage.
- **Bascule de libre passage** — Cette catégorie est utilisée pour créer des identifiants système autorisant des clés de bascule de libre passage.

Identifiants pour les clés de résidents

La catégorie d'identifiants et les identifiants utilisés pour créer des clés pour les résidents sont implicites. En d'autres termes, vous ne sélectionnez pas de catégorie d'identifiants/d'identifiant de résidents. Au contraire, les points d'accès sélectionnés lors de l'affectation des unités, y compris les unités, les suites, les espaces communs et les étages forment l'identifiant qui autorise l'entrée. Seul le module **Rapports** contient une référence à une catégorie d'identifiants de résidents. Lorsque vous sélectionnez des options pour le **Rapport sur les attributions des clés/utilisateurs**, vous pouvez sélectionner la catégorie Résident pour inclure une liste de tous les points d'accès encodés dans les clés affectées aux résidents.

Identifiants créés dans l'API Community

Les identifiants créés à l'aide de l'API Community sont répertoriés dans **Gestion des identifiants** tant que l'identifiant est utilisé sur au moins une clé active. Les identifiants ne peuvent pas être modifiés ou sélectionnés lors de la création d'une clé dans l'interface utilisateur Community.

Espaces communs

Les espaces communs pour les résidents et les espaces communs pour le personnel sont deux types de points d'accès configurés pour un accès général. Cependant, les deux types peuvent être activés pour un accès limité. Lorsque l'accès limité est activé, vous devez configurer l'accès dans ***Gestion des accès > Accès aux espaces communs***.

Accès résident

Les espaces communs résident à accès limité sont associés aux unités/unités de suite. L'accès des résidents dépend des espaces communs associés aux unités/unités de suites qui leur sont affectées.

Accès du personnel

Les espaces communs pour le personnel à accès limité sont associés à un identifiant. L'accès du personnel dépend des espaces communs associés à l'identifiant choisi lors de la création d'une clé de personnel/prestataire.



Les espaces communs ne sont pas configurés dans **Accès aux espaces communs** pour les identifiants créés avec la catégorie d'identifiants Urgence. Au lieu de cela, tous les points d'accès (y compris les espaces communs à accès limité) que vous souhaitez autoriser sur la clé doivent être sélectionnés dans l'identifiant.

Attribution horaire

La fonction d'attribution horaire fournit une autre couche de contrôle d'accès. Les deux types d'horaires suivants sont programmés directement dans les serrures :

- Les horaires de libre passage déterminent à quel moment un point d'accès peut être accessible sans clé, permettant ainsi un accès sans restriction. Les types de points d'accès qui prennent en charge les horaires de libre passage sont les accès privés, tous les espaces communs et les lecteurs d'ascenseurs.
- Les horaires d'accès déterminent à quel moment un point d'accès peut être accessible avec une clé valide. Vous pouvez attribuer un horaire d'accès différent pour chaque catégorie d'identifiants dans laquelle un point d'accès est inclus. Par exemple, si l'espace commun de la buanderie est compris dans un identifiant du personnel (accès variable) et un identifiant du prestataire, vous pouvez attribuer des horaires d'accès différents pour chacun. Les types de points d'accès qui prennent en charge les horaires d'accès sont tous les espaces communs et les lecteurs d'ascenseurs.

Ajouter des horaires de libre passage

Créer et configurer des horaires contrôlant les périodes pendant lesquelles les types de points d'accès suivants permettent un accès sans clé :

- espaces communs
- accès privés

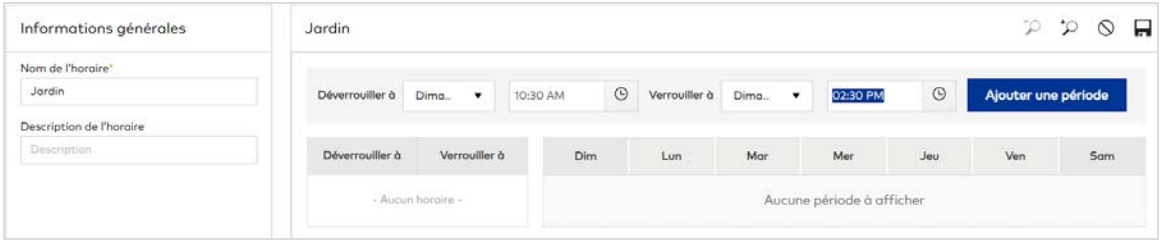
> À chaque fois que vous affectez/désaffectez un horaire ou que vous éditez un horaire, vous devez programmer (ou reprogrammer) les points d'accès affectés.

Pour ajouter un horaire :

1. Accédez à ***Gestion des accès > Horaires de libre passage.***



2. Cliquez sur **Nouvel Horaire**.



3. Indiquez un nom descriptif pour l'horaire.
4. (*facultatif*) Indiquez une description pour l'horaire.
5. Sélectionnez un jour et une heure pour autoriser l'accès sans clé.
6. Sélectionnez un jour et une heure pour rétablir l'accès contrôlé avec une clé valide.
7. Cliquez sur **Ajouter une période**. Vous pouvez ajouter plusieurs périodes par jour, mais les périodes ne peuvent pas se superposer.
8. Cliquez sur **(Sauvegarder)** .



Modifier un horaire

1. Sélectionner l'horaire que vous souhaitez modifier.
2. Cliquez sur **(Modifier)** .
3. Modifier l'horaire :
   - Modifier le nom et/ou la description.
   - Pour modifier une période existante, sélectionnez la période et cliquez sur **Modifier la période**.
   - Pour ajouter une période, sélectionnez les options de jour et d'heure, puis cliquez sur **Ajouter une période**. Vous pouvez ajouter plusieurs périodes par jour, mais les périodes ne peuvent pas se superposer.
   - Pour supprimer une période, cliquez sur **(Supprimer)** directement dans le bloc de période sur l'horaire.
4. Cliquez sur **(Sauvegarder)** .

Supprimer un horaire

1. Sélectionnez un horaire.
2. Cliquez sur **(Supprimer)** .
3. Cliquez sur **OUI** pour confirmer .

Ajouter des horaires d'accès

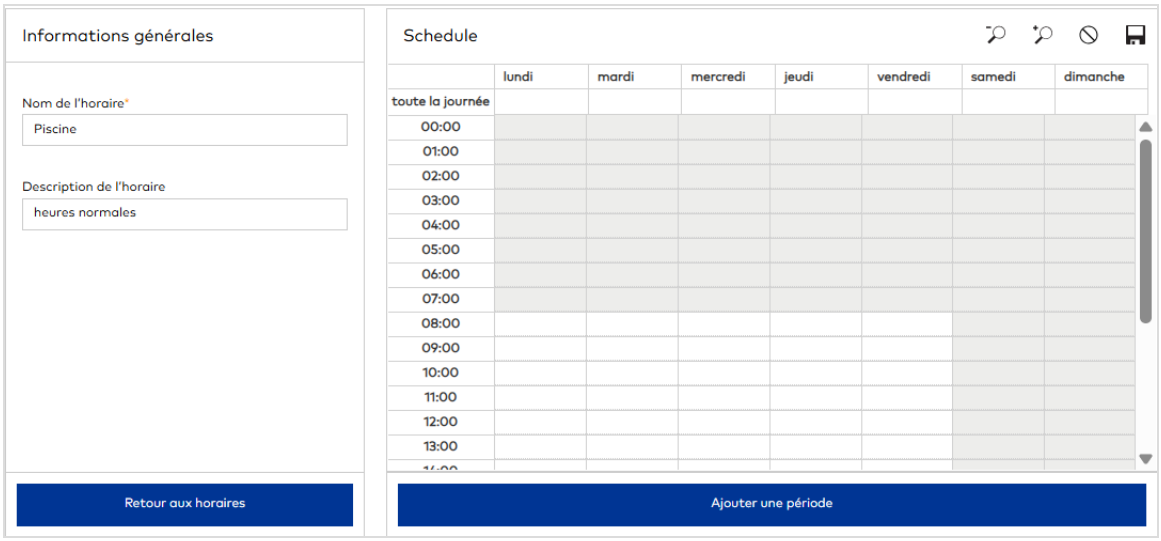
Les horaires d'accès contrôlent les périodes pendant lesquelles les types de points d'accès suivants sont accessibles avec une clé :

- espaces communs
- lecteurs d'ascenseur

> À chaque fois que vous affectez/désaffectez un horaire ou que vous éditez un horaire, vous devez programmer (ou reprogrammer) les points d'accès affectés.

Pour ajouter un horaire :

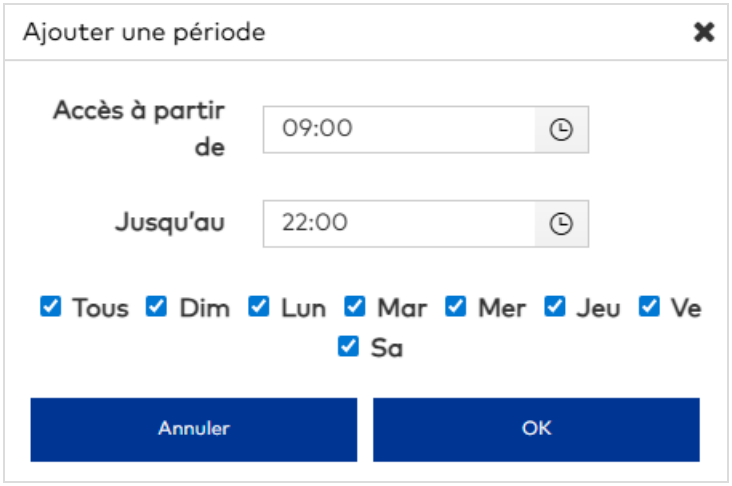
1. Accédez à ***Gestion des accès > Horaires d'accès.***
2. Cliquez sur **(Ajouter)** +.



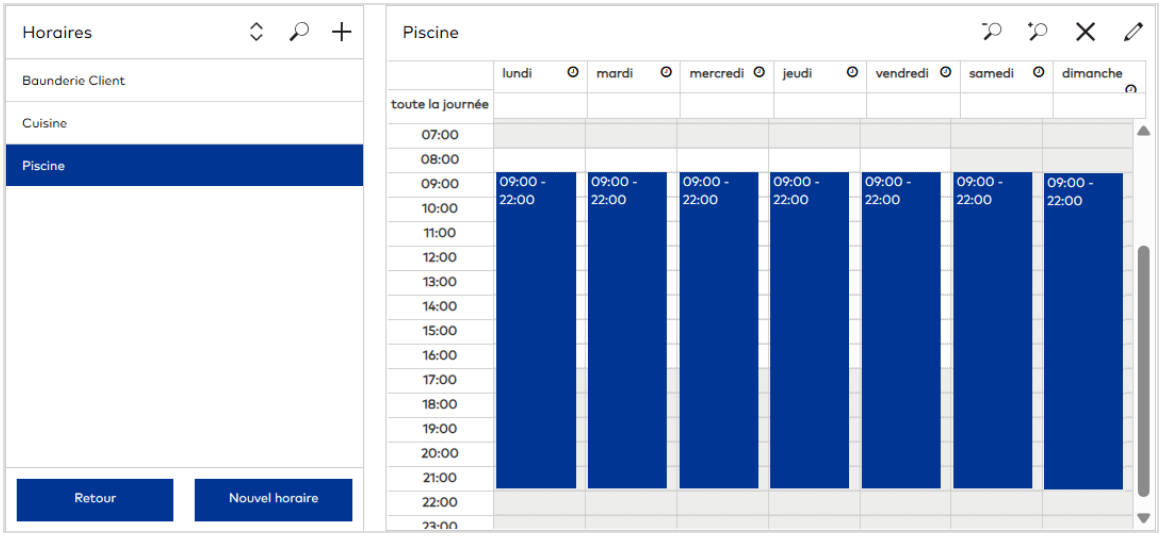
3. Indiquez un nom descriptif pour l'horaire.
4. (*facultatif*) Indiquez une description pour l'horaire.

> Utilisez le glisser-déposer pour ajouter des périodes directement sur le calendrier. Pour ajouter une période qui couvre 24 heures, double-cliquez sur la ligne **toute la journée** (première ligne).

5. Cliquez sur **Ajouter une période**.



6. Sélectionnez l'heure de début d'accès.
7. Sélectionnez l'heure de fin d'accès.
8. Sélectionnez les jours auxquels appliquer les horaires sélectionnés.
9. Cliquez sur **Appliquer**. Vous pouvez ajouter une période par jour.



10. Cliquez sur **(Sauvegarder)**.

Modifier un horaire

1. Sélectionner l'horaire que vous souhaitez modifier.
2. Cliquez sur **(Modifier)** .
3. Modifier l'horaire :
   - Modifier le nom et/ou la description.
   - Pour ajouter une période, cliquez sur **Ajouter une période**, indiquez les paramètres d'horaire, puis cliquez sur **OK**. Vous pouvez ajouter une période par jour.
   - Pour supprimer une période, cliquez sur **(Supprimer)** directement dans le bloc de période sur l'horaire, puis cliquez sur **Supprimer**.
4. Cliquez sur **(Sauvegarder)**.

Supprimer un horaire

1. Sélectionnez un horaire.
2. Cliquez sur **(Supprimer)** ✕.
3. Cliquez sur **OUI** pour confirmer .

Ajouter les horaires des clés du personnel

Créer et configurer des horaires contrôlant les périodes pendant lesquelles les identifiants du personnel peuvent accéder aux types de points d'accès suivants :

- espaces communs
- accès privés

> La période configurée s'applique à tous les jours sélectionnés dans le calendrier.

Pour ajouter un horaire :

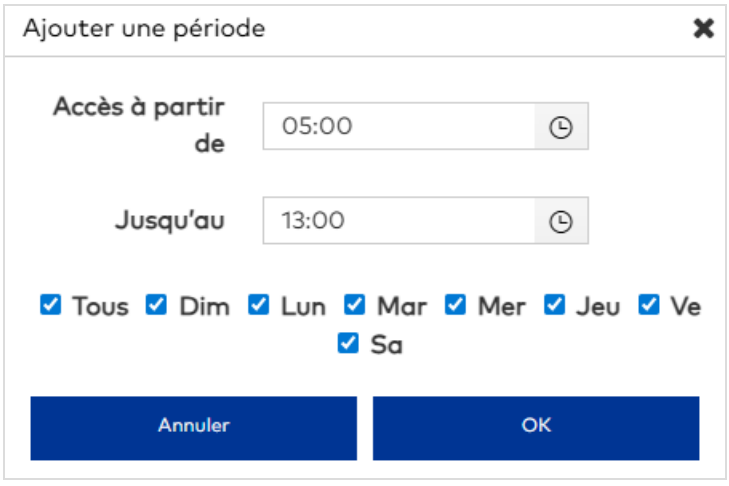
1. Accédez à ***Gestion des accès > Horaires des clés du personnel.***
2. Cliquez sur **(Ajouter)** +.



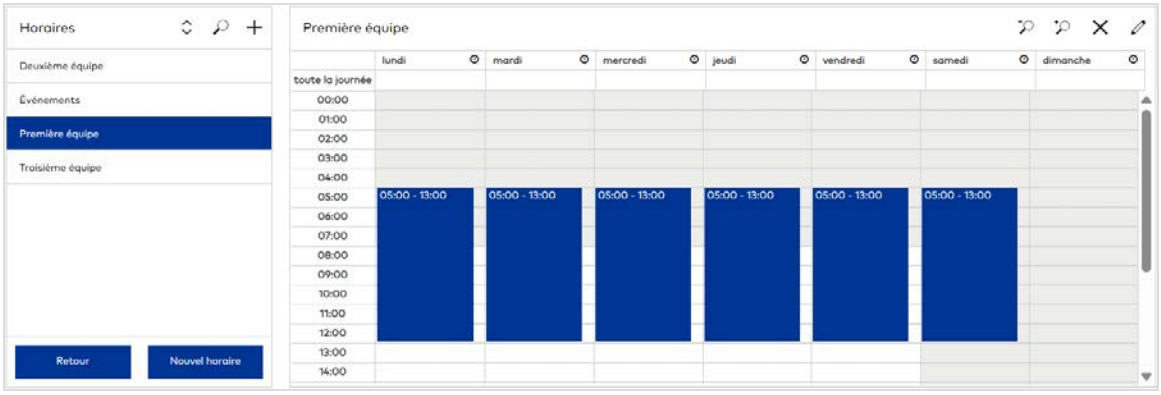
3. Indiquez un nom descriptif pour l'horaire.
4. (*facultatif*) Indiquez une description pour l'horaire.

> Utilisez le glisser-déposer pour ajouter des périodes directement sur le calendrier. Pour ajouter une période qui couvre 24 heures, double-cliquez sur la ligne **toute la journée** (première ligne).

5. Cliquez sur **Ajouter une période**.



6. Sélectionnez l'heure de début d'accès.
7. Sélectionnez l'heure de fin d'accès.
8. Sélectionnez les jours auxquels appliquer les horaires sélectionnés.
9. Cliquez sur **OK**. Vous pouvez ajouter une période par jour.



10. Cliquez sur **(Sauvegarder)**.

Modifier un horaire

1. Sélectionner l'horaire que vous souhaitez modifier.
2. Cliquez sur **(Modifier)** .
3. Modifier l'horaire :
   - Modifier le nom et/ou la description.
   - Pour ajouter une période, cliquez sur **Ajouter une période**, indiquez les paramètres d'horaire, puis cliquez sur **OK**. Vous pouvez ajouter une période par jour.
   - Pour supprimer une période, cliquez sur **(Supprimer)** directement dans le bloc de période sur l'horaire, puis cliquez sur **Supprimer**.
4. Cliquez sur **(Sauvegarder)**.

Supprimer un horaire

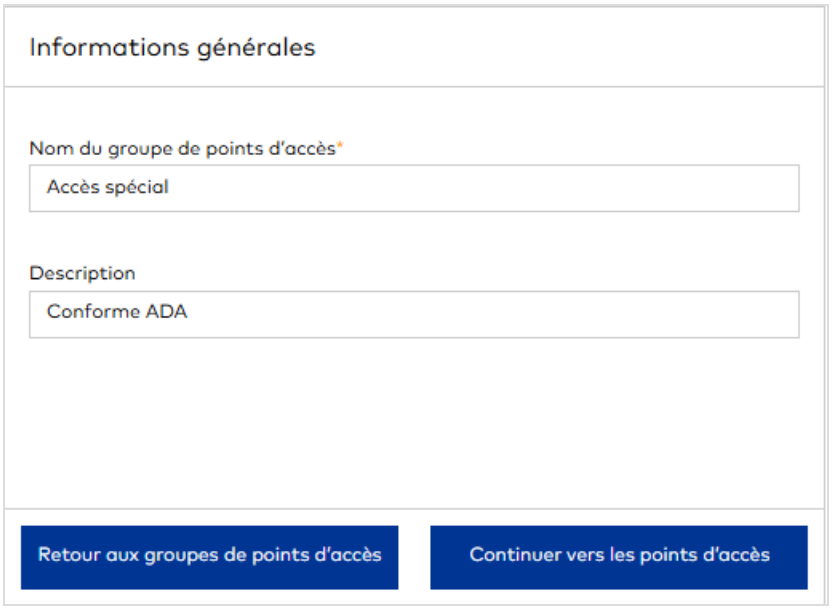
1. Sélectionnez un horaire.
2. Cliquez sur **(Supprimer)**.
3. Cliquez sur **OUI** pour confirmer .

Créer des groupes de points d'accès

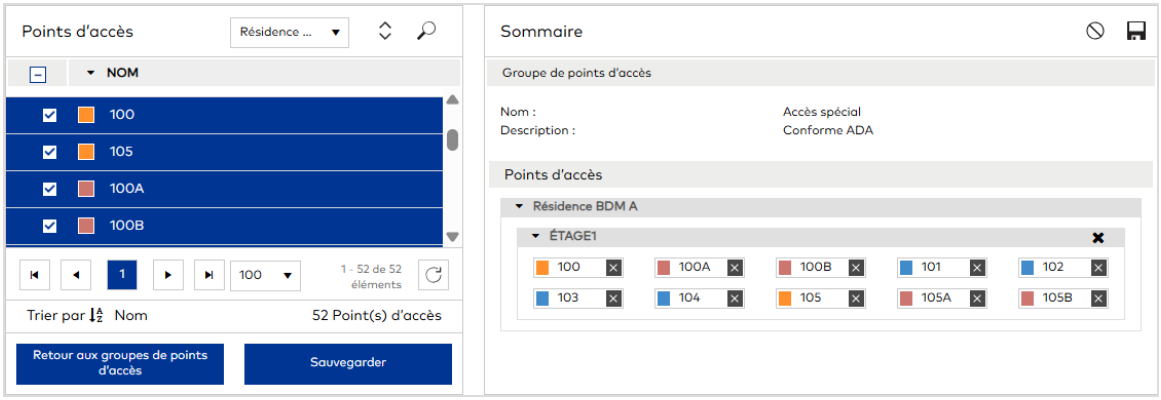
L'organisation des points d'accès en groupes logiques selon leur emplacement ou leur usage prévu facilite l'attribution des identifiants.

Pour ajouter un groupe de points d'accès :

1. Accédez à ***Gestion des accès > Groupes de points d'accès.***
2. Cliquez sur **(Ajouter)** +.



3. Indiquez un nom descriptif pour le groupe.
4. (*facultatif*) Indiquez une description pour le groupe.
5. Cliquez sur **Continuer vers les points d'accès**.



6. Sélectionnez les points d'accès que vous souhaitez attribuer au groupe. Les points d'accès sélectionnés sont ajoutés à la section Sommaire (classés par bâtiment et par étage).
   - Vous pouvez sélectionner des points d'accès de différents bâtiments.
   - Vous ne pouvez pas ajouter d'espaces communs aux groupes de points d'accès.
7. Cliquez sur **Sauvegarder**.

Modifier des groupes de points d'accès

1. Sélectionnez le groupe de points d'accès que vous souhaitez modifier.

> Lorsque vous ajoutez des espaces communs pour le personnel ou des espaces communs résident avec un accès pour le personnel activé à un identifiant du personnel à usage restreint ou à un identifiant maître, vous devez également vous assurer que le même espace commun est également associé à l'identifiant dans ***Gestion des accès > Accès aux espaces communs***.

2. Cliquez sur **(Modifier)** .
3. Modifier le groupe :
   - Modifier le nom et/ou la description du groupe.
   - Pour ajouter ou supprimer des points d'accès, cliquez sur **Continuer vers les points d'accès**. Tous les points d'accès affectés au groupe sont énumérés dans la section **Sommaire**.
     - Sélectionner ou désélectionner les points d'accès. Les points d'accès sélectionnés sont ajoutés au groupe (et listés par bâtiment et par étage à la section **Sommaire**). Les points d'accès désélectionnés sont supprimés du groupe (et supprimés de la section **Sommaire**).
     - Pour supprimer un point d'accès, cliquez sur **(Supprimer)** directement dans le bloc de points d'accès à la section **Sommaire**.
     - Pour supprimer tous les points d'accès d'un étage, cliquez sur **(Supprimer)** dans la ligne de l'étage dans la section **Sommaire**.
4. Cliquez sur **(Sauvegarder)**.

Supprimer un groupe de points d'accès

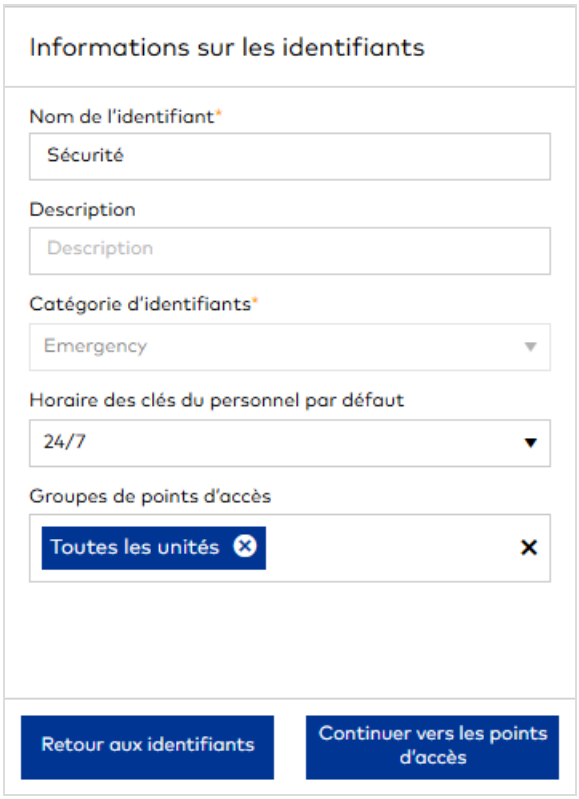
1. Sélectionner un groupe de points d'accès.
2. Cliquez sur **(Supprimer)**.
3. Cliquez sur **OUI** pour confirmer.

Ajouter des identifiants

Les seuls identifiants que vous devez ajouter pendant la configuration du site sont les identifiants de clés du personnel/prestataire.

Pour ajouter un identifiant :

1. Accédez à ***Gestion des accès > Gestion des identifiants.***
2. Cliquez sur **(Ajouter)** +.



3. Indiquez un nom descriptif pour l'identifiant.
4. (*facultatif*) Indiquez une description pour l'identifiant.
5. Sélectionnez une catégorie d'identifiants. Pour une description de chaque catégorie, reportez-vous à « En savoir plus sur la gestion des accès ».

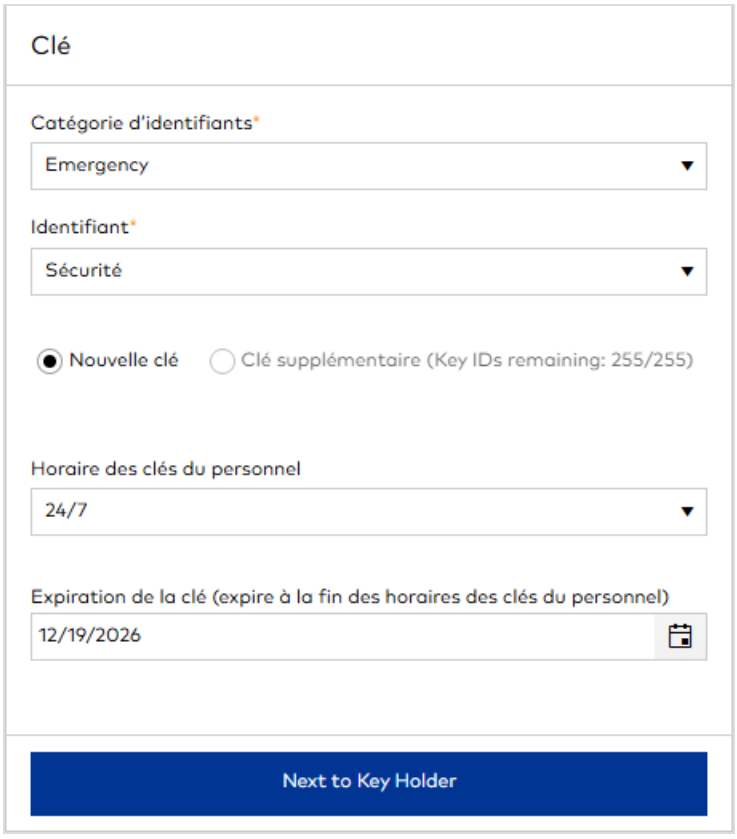
> Vous pouvez également créer une catégorie d'identifiants personnalisée. Pour créer une catégorie d'identifiants personnalisée, sélectionnez **Modifier les catégories d'identifiants** et reportez-vous à « Ajouter des catégories d'identifiants personnalisées ».

6. Sélectionnez un horaire des clés du personnel au cours duquel la clé est valide. Pour permettre un accès 24h/24 et 7j/7, sélectionnez **24/7**. Pour consulter les détails de l'horaire des clés du personnel, accédez à ***Gestion des accès > Horaires des clés du personnel***. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
7. Sélectionnez les groupes de points d'accès que vous souhaitez ajouter à l'identifiant. Cette option n'est pas disponible pour les catégories Personnel (accès variable) ou Prestataire ou une catégorie personnalisée basée sur l'une ou l'autre de ces catégories.
8. L'étape suivante dépend de la catégorie d'identifiants sélectionnée :
   - Pour le Personnel (accès variable), Prestataire ou une catégorie personnalisée basée sur l'une ou l'autre de ces catégories, cliquez sur **Sauvegarder**. L'identifiant est créé. Tous les points d'accès sont sélectionnés lors de la création des clés, mais les espaces communs doivent être configurés dans ***Gestion des accès > Accès aux espaces***

communs.

- Pour la catégorie Urgence, Usage restreint, Personnel ou une catégorie personnalisée basée sur l'une ou l'autre de ces catégories, cliquez sur **Continuer vers les points d'accès**.

9. Sélectionnez les points d'accès que vous souhaitez ajouter à l'identifiant. Vous pouvez ajouter des points d'accès de différents bâtiments. Les points d'accès inclus dans tout groupe de points d'accès sélectionné ne sont pas répertoriés.
   - Pour le type de catégorie **Urgence**, tous les types de points d'accès sont répertoriés, y compris les lecteurs d'ascenseurs.
   - Pour tous les autres types de catégories, tous les types de points d'accès sont répertoriés, à l'exception des espaces communs, qui sont sélectionnés lors de la création de la clé. Toutefois, les espaces communs doivent être configurés dans **Accès aux espaces communs** et associés à l'identifiant sélectionné.
10. Cliquez sur **(Sauvegarder)**. La figure suivante montre l'identifiant Premiers Intervenants qui peut être sélectionné lors de la création d'une clé du personnel.

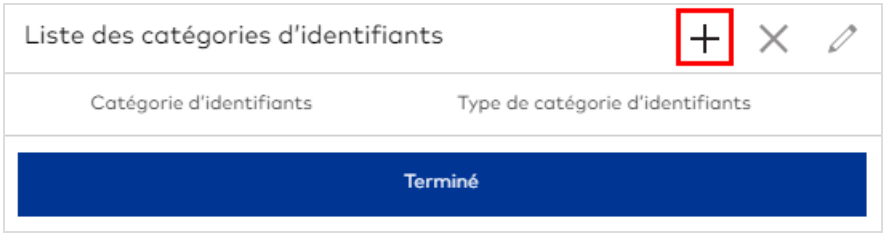


Ajouter des catégories d'identifiants personnalisées

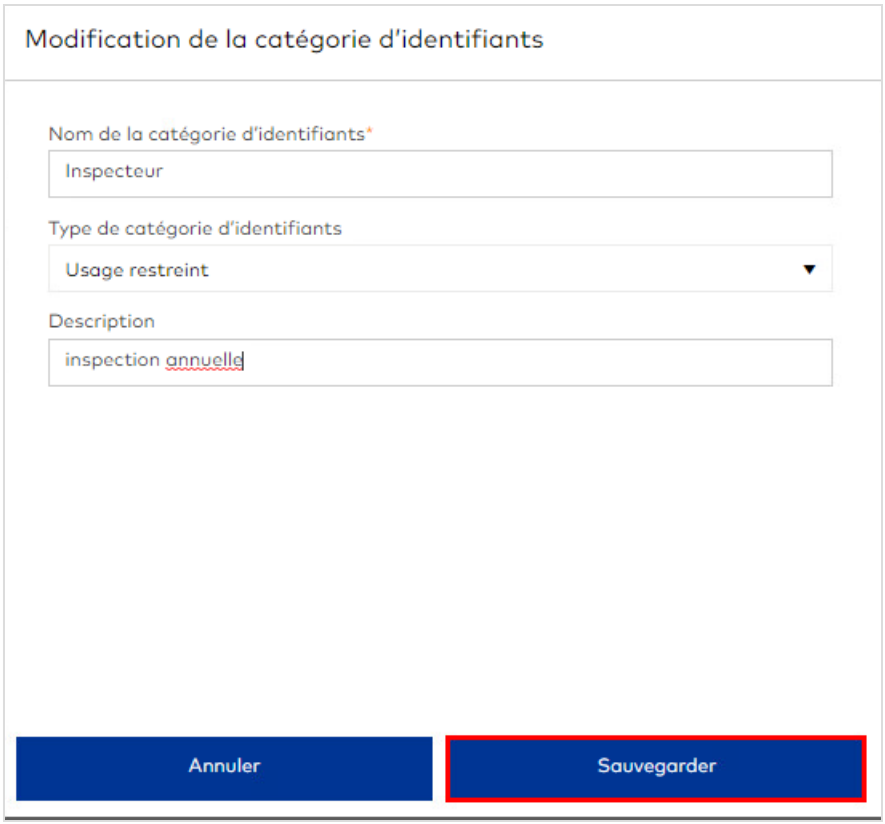
Lors de la sélection d'une catégorie d'identifiants pour un identifiant, il est possible de modifier les catégories d'identifiants. Bien que vous ne puissiez pas modifier ou supprimer les catégories par défaut, il est possible d'ajouter une catégorie basée sur l'une des catégories par défaut.

Pour ajouter des catégories d'identifiants personnalisées :

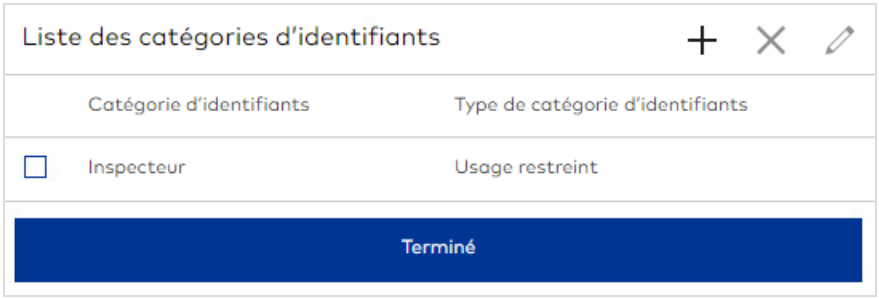
1. Lors de la sélection d'une catégorie d'identifiants pour un nouvel identifiant, sélectionnez **Modifier les catégories d'identifiants**.



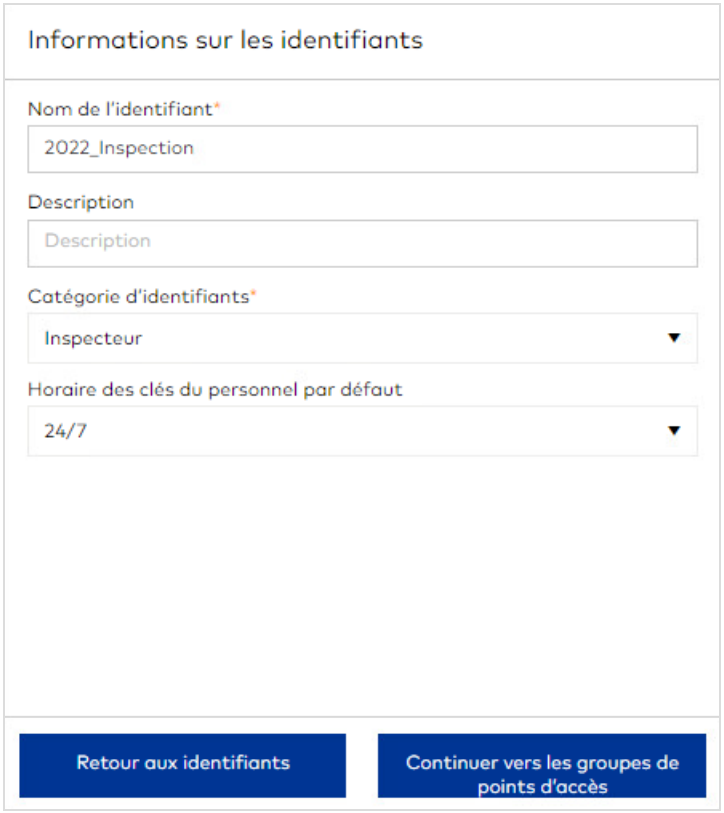
2. Cliquez sur **(Ajouter)**+.



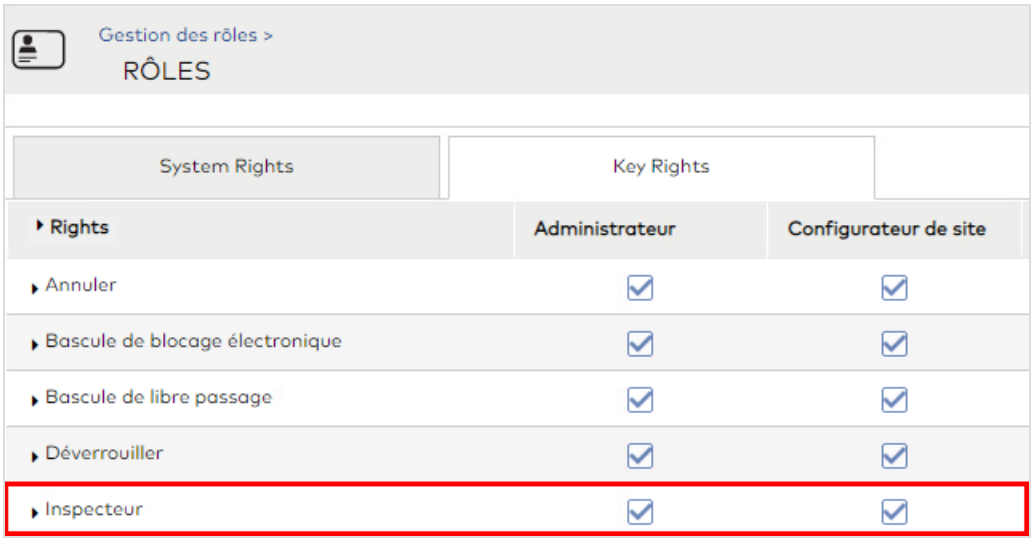
3. Indiquez un nom descriptif pour la catégorie personnalisée.
4. Sélectionnez les types de catégories d'identifiants sur lesquels baser l'identifiant personnalisé.
5. (*facultatif*) Indiquez une description pour la catégorie personnalisée.
6. Cliquez sur **Sauvegarder**.



7. Cliquez sur **Terminé**. Après avoir créé la catégorie personnalisée, vous devez créer un identifiant en utilisant la catégorie personnalisée, puis l'identifiant sera disponible lors de la création d'une clé du personnel/prestataire.



Lorsque vous créez une catégorie d'identifiants personnalisée, tous les opérateurs auxquels est attribué le rôle d'administrateur ou de configurateur de site par défaut disposent des droits nécessaires pour créer des clés à l'aide de la catégorie d'identifiants personnalisée. La figure suivante montre l'accès par défaut dans **Gestion des rôles** pour une catégorie d'identifiants personnalisée.



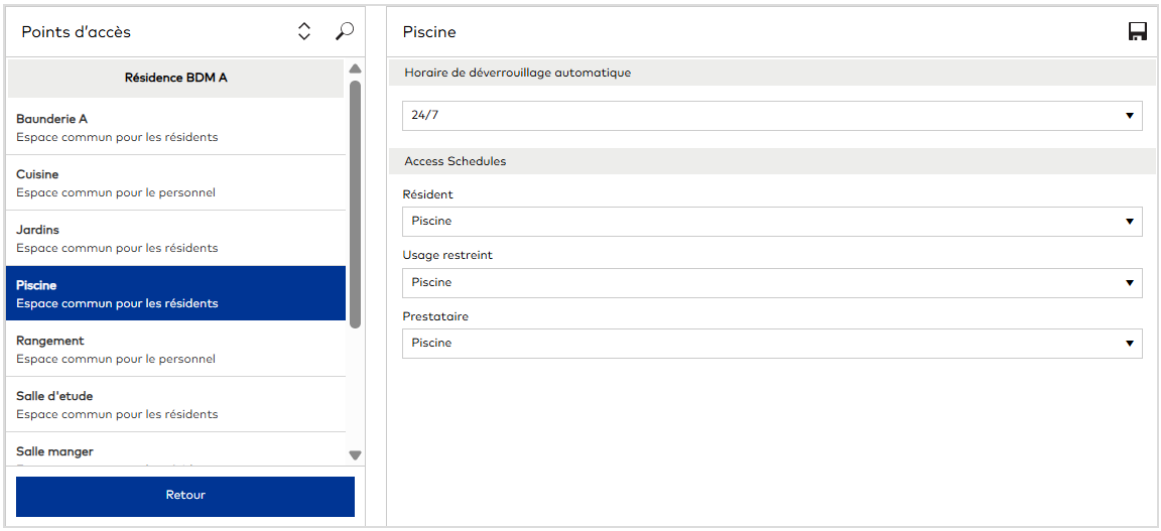
Attribuer des horaires

Les horaires de libre passage peuvent être attribués aux espaces communs accessibles par les résidents/le personnel/les prestataires et aux accès privés.

Étant donné que les points d'accès peuvent être inclus dans plusieurs identifiants, vous pouvez attribuer différents horaires d'accès au même point d'accès pour chacun des types de catégories d'identifiants suivants : Résident, usage restreint et personnel.

Pour attribuer des horaires à un point d'accès :

1. Accédez à ***Gestion des accès > Attribution horaire au point d'accès.***



2. Sélectionnez un point d'accès.
3. Sélectionnez un horaire de libre passage à appliquer au point d'accès. La sélection par défaut (24/7) signifie qu'aucun horaire n'est appliqué.
4. Sélectionnez un horaire d'accès à appliquer au point d'accès. Si le point d'accès est inclus dans plusieurs identifiants, vous pouvez sélectionner un horaire pour chaque catégorie d'identifiants.
5. Cliquez sur **(Sauvegarder)**.

Configurer les profils d'accès aux espaces communs à accès limité

Créer et configurer des profils associant des unités ou des identifiants du personnel/prestataire à des espaces communs à accès limité.

Configurer l'accès du résident aux espaces communs à accès limité

L'accès des résidents aux espaces communs à accès limité peut être configuré dès que toutes les unités, unités de suites et espaces communs à accès limité sont créés dans **Configurateur de site**. Le processus implique l'ajout d'un profil de résident, puis l'association des espaces communs aux unités et aux unités de suites.

Ajouter un profil de résident

1. Accédez à ***Gestion des accès > Accès aux espaces communs.***
2. Cliquez sur **(Ajouter)**+.

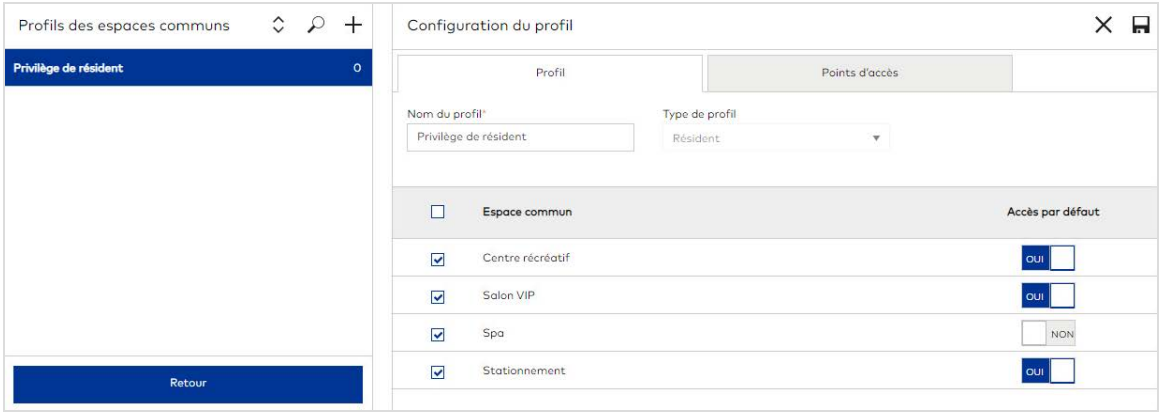


3. Indiquez un nom descriptif pour le profil.
4. Sélectionnez le type de profil Résident.
5. Cliquez sur **Sauvegarder**. Le profil est ajouté à la liste.

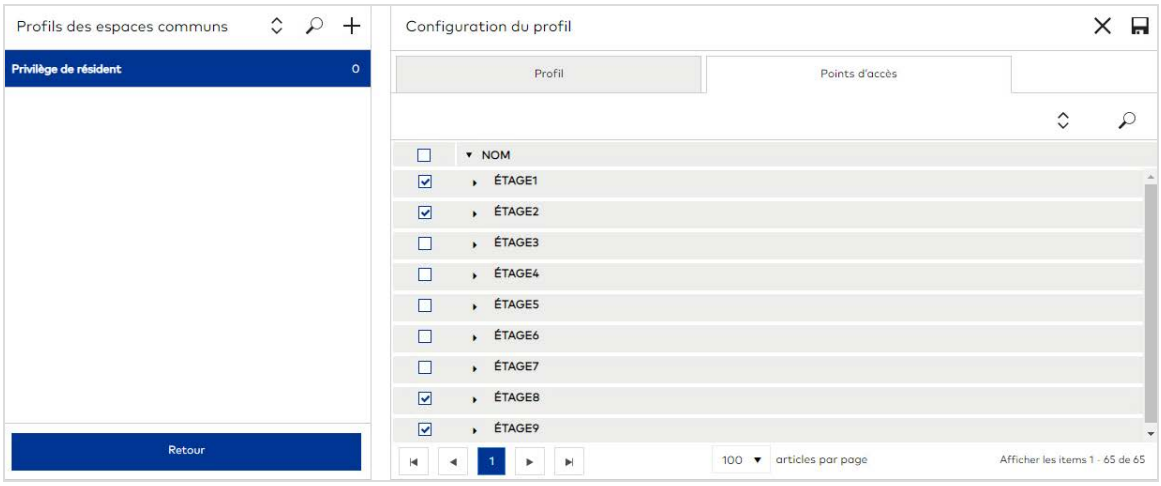
Associer les espaces communs aux unités/unités de suites

Pour associer des unités à des espaces communs :

1. Accédez à ***Gestion des accès > Accès aux espaces communs.***



2. Sélectionnez un profil d'espace commun existant ou ajoutez un nouveau profil.
3. Dans l'onglet **Profil**, sélectionnez les espaces communs que vous souhaitez configurer pour l'accès dans ce profil et choisissez d'activer ou non un accès par défaut pour chaque espace commun que vous sélectionnez. Lorsque l'accès par défaut est activé, l'espace commun est automatiquement ajouté aux affectations d'unités mais peut être désactivé dans les profils de résidents.



4. Dans l'onglet **Points d'accès**, sélectionnez les points d'accès à associer au profil. Vous pouvez ajouter des points d'accès de différents bâtiments.
5. Cliquez sur **(Sauvegarder)**.



Configurer l'accès du personnel/prestataire aux espaces communs à accès limité

L'accès du personnel/prestataire aux espaces communs à accès limité peut être configuré après la définition des identifiants. Le processus implique l'ajout d'un profil du personnel/prestataire, puis l'association des espaces communs aux identifiants.

Ajouter un profil du personnel/prestataire

1. Accédez à ***Gestion des accès > Accès aux espaces communs.***
2. Cliquez sur **(Ajouter)**.

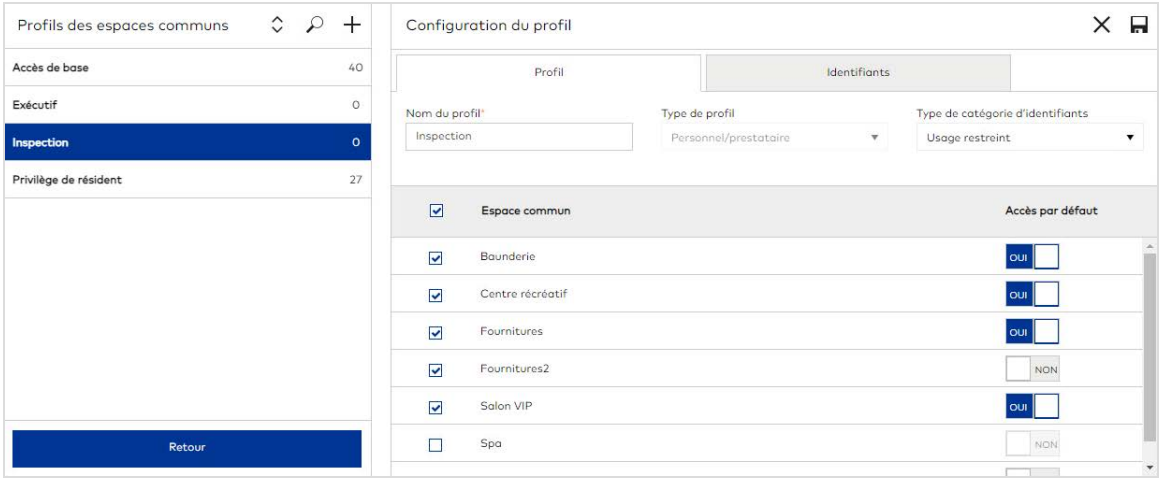


3. Indiquez un nom descriptif pour le profil.
4. Sélectionnez le type de profil du personnel/prestataire.
5. Sélectionnez un type de catégorie d'identifiants. Votre sélection détermine les identifiants que vous pouvez associer aux espaces communs sélectionnés dans l'onglet **Profil**. Vous ne pouvez associer que des identifiants créés à l'aide du même type de catégorie.
6. Cliquez sur **Sauvegarder**. Le profil est ajouté à la liste.

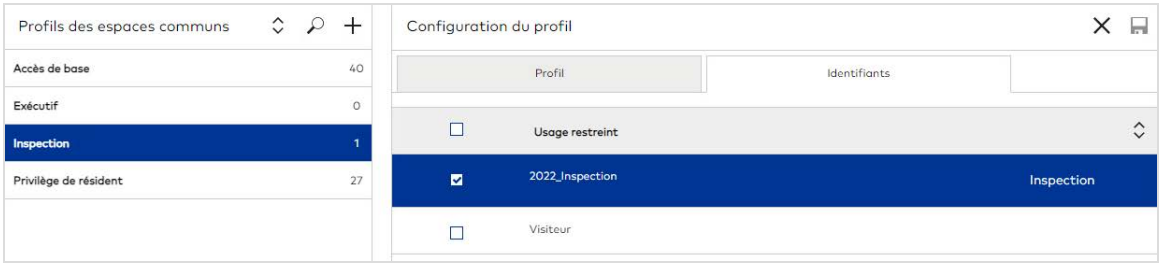
Associer les espaces communs aux identifiants

Pour associer des unités à des espaces communs :

1. Accédez à ***Gestion des accès > Accès aux espaces communs.***
2. Sélectionnez un profil d'espace commun existant ou ajoutez un nouveau profil.



3. Dans l'onglet **Profil**, sélectionnez les espaces communs que vous souhaitez configurer pour l'accès dans ce profil et choisissez d'activer ou non un accès par défaut pour chaque espace commun que vous sélectionnez. L'accès aux espaces communs doit être activé dans ***Paramètres du système > Clés du personnel/prestataire***.



4. Dans l'onglet **Identifiants**, sélectionnez tous les identifiants que vous souhaitez associer aux espaces communs sélectionnés dans l'onglet **Profil**. Vous pouvez ajouter des points d'accès de différents bâtiments.
5. Cliquez sur **(Sauvegarder)** .



Étape 4

Configurer des périphériques

Cette section comprend les sujets suivants :

En savoir plus sur la gestion des périphériques 112

Ajouter des encodeurs 114

En savoir plus sur la gestion des périphériques

Gestion des périphériques est le module Community dans lequel vous configurez les encodeurs.

Lorsque la fonction de communication en ligne sous licence est activée, vous pouvez également configurer les périphériques qui prennent en charge la communication en ligne.

Encodeurs

Un encodeur est un périphérique intégré servant à encoder des clés physiques avec les données de configuration de Community. Avant de pouvoir coder ou lire une clé physique, vous devez connecter et configurer au moins un encodeur. Les encodeurs configurés dans Community sont répertoriés dans la ***Gestion des périphériques > Encodeurs*** avec l'état actuel (hors ligne, en ligne ou configuration non prise en charge), le type de firmware et le mode de communication (TCP/IP ou USB).

Community prend en charge ce qui suit :

- Encodeur RFID I dormakaba — Anciens encodeurs. Configuration non prise en charge pour le mode de sécurité renforcée.
- Encodeur RFID II dormakaba — Requis pour le mode de sécurité renforcée. La référence 75720 s'affiche sur le dessous de l'encodeur.

Pour connaître les dernières versions de firmware prises en charge, reportez-vous aux notes de mise à jour du produit.

Prérequis

Les prérequis suivants sont automatiquement respectés lors de l'installation initiale de Community :

- Le client Community est installé sur le poste de travail.
- Le service client Community est lancé.
- Le fichier de configuration du client Community est automatiquement configuré avec la bonne adresse IP.

Méthode de connexion USB

L'encodeur doit être connecté au poste de travail par un câble USB. Vous devez configurer un encodeur pour chaque poste de travail utilisé pour l'encodage et la lecture des clés physiques. L'encodeur peut être partagé par de multiples postes de travail.

Méthode de connexion TCP/IP

L'encodeur doit être connecté au poste de travail par câble USB pour la configuration initiale.

Les encodeurs TCP/IP communiquent directement par Internet avec le serveur Community (pas avec les postes de travail). Une seule configuration de l'encodeur suffit pour l'utilisation avec des postes de travail multiples. L'encodeur doit être connecté au réseau local pour être en ligne.

Si vous changez la méthode de connexion en TCP/IP après la sauvegarde de la configuration initiale, vous devez réinitialiser l'encodeur (débrancher/rebrancher).

Passerelles enregistrées et points d'accès assignés

Cette section s'affiche lorsque la fonction de communication en ligne sous licence est activée.

Les passerelles sont les périphériques réseau appairés à des points d'accès pour la communication en ligne pour effectuer des opérations à distance et recevoir les événements du point d'accès. Après la mise en service et la connexion des passerelles au serveur Community, les périphériques sont répertoriés dans **Gestion des périphériques**. Lorsque l'état de la passerelle est **En ligne**, les points d'accès peuvent être assignés. Il est possible de connecter plusieurs passerelles à Community, mais chaque point d'accès peut uniquement être assigné à une passerelle.

Programmateur M-Unit

M-Unit (Programmateur M-Unit) est un périphérique intégré portatif utilisé pour transférer des données entre Community et les serrures installées sur les points d'accès. Le périphérique est utilisé pour la programmation et l'audit des serrures.

Les programmateurs M-Unit suivants est pris en charge :

- M-Unit Saflok HH6 NFC – Connexion Wireless prise en charge. Requis pour le mode de sécurité renforcée.
- M-Unit Saflok HH6 – Périphérique existant. Nécessite une connexion câblée.

L'authentification du programmateur M-Unit est activée par défaut, mais peut être désactivée dans ***Paramètres du système > Sécurité***. Si l'authentification est activée, des identifiants du programmateur M-Unit doivent être configurés pour au moins un Opérateur dans **Gestion du personnel/prestataire**.

Lorsque le mode de sécurité renforcée est activé, l'authentification de M-Unit est requise et le mot de passe de sécurité de M-Unit (affiché dans ***Paramètres du système > Sécurité > Mode de sécurité renforcée***) est nécessaire pour programmer les points d'accès. Lorsque le mode de sécurité renforcée est activé, M-Unit est spécifique au site. L'utilisation de M-Unit sur un autre site nécessite une réinitialisation d'usine.

Le type de sonde utilisé pour connecter le programmateur M-Unit aux serrures dépend du modèle de serrure.



Le programmateur M-Unit se connecte au poste de travail à l'aide d'un connecteur sériel.



Pour plus d'informations sur le programmateur M-Unit, reportez-vous à la documentation fournie avec votre périphérique.

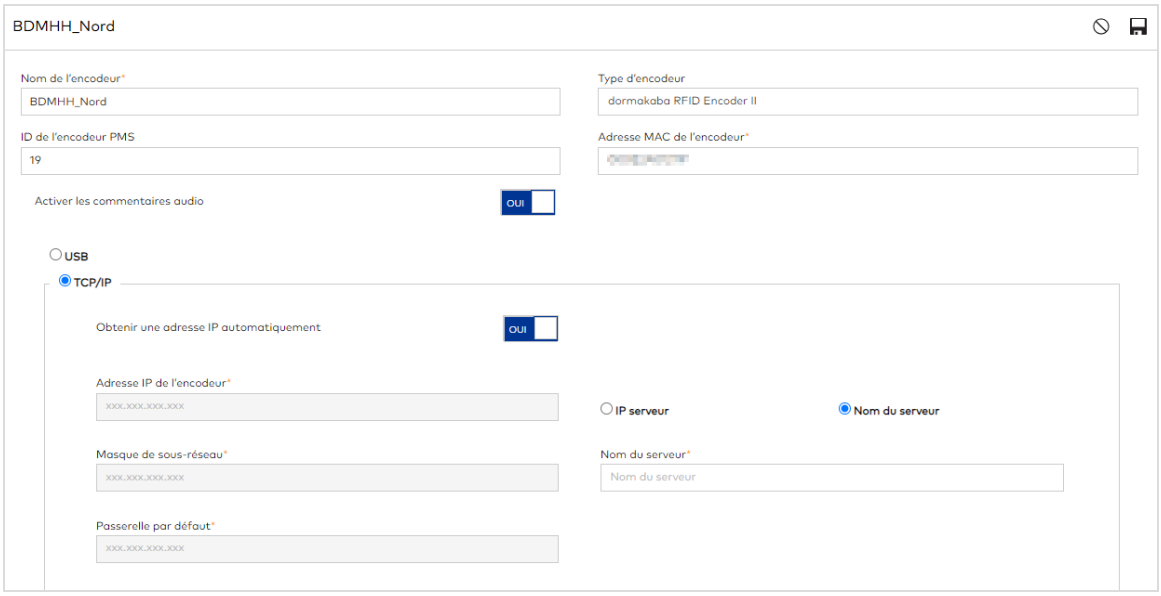
Ajouter des encodeurs

Un encodeur est requis pour l'encodage des clés avec les données de configuration de Community.

Pour les nouvelles installations, le mode de sécurité renforcée est activé par défaut et ne peut pas être désactivé après la configuration d'un encodeur (référence 75720). Vérifiez le réglage du mode de sécurité renforcée dans ***Paramètres du système > Sécurité > Mode de sécurité renforcée***.

Pour ajouter des encodeurs :

1. Connectez l'encodeur via USB au poste de travail. La configuration initiale d'un encodeur nécessite la connexion de l'encodeur au poste de travail Community à l'aide d'un câble USB. Par défaut, le périphérique émet deux bips sonores et un voyant vert clignote pour indiquer une connexion réussie.
2. Accédez à **Gestion des périphériques**. (Si la communication en ligne est activée, cliquez sur **Encodeurs**.)
3. Cliquez sur **Nouvel encodeur**.



4. Pour le **Nom de l'encodeur**, indiquez un nom unique ne dépassant pas 50 caractères. Ce nom s'affiche dans la liste des encodeurs.
5. Le type d'encodeur est détecté en fonction de la version du firmware :
   - **Encodeur RFID I dormakaba** — Anciens encodeurs. Configuration non prise en charge pour le mode de sécurité renforcée.
   - **Encodeur RFID II dormakaba** — Requis pour le mode de sécurité renforcée. La référence 75720 s'affiche sur le dessous de l'encodeur. Configuration non prise en charge pour le mode de sécurité renforcée.
6. (*sous conditions*) Si vous intégrez un API tiers, indiquez un numéro pour identifier l'encodeur. Valeurs valides : 0-99.
7. Sélectionnez l'adresse MAC de l'encodeur. La valeur est détectée automatiquement lorsque vous connectez l'encodeur au poste de travail.
8. Indiquez si l'encodeur émet des bips sonores lorsque la connexion au poste de travail s'établit et lorsque des clés sont créées.
9. **TCP/IP** ou **USB** — Sélectionnez la méthode de connexion de l'encodeur au poste de travail après la configuration initiale. Si vous modifiez le type de connexion pour passer de TCP/IP à USB ou d'USB à TCP/IP, vous devez réinitialiser (débrancher/rebrancher) l'encodeur.

- Renseignez les paramètres TCP/IP pour définir la configuration réseau pour le périphérique encodeur :
  - **Obtenir une adresse IP automatiquement** — Sélectionnez l'une des options suivantes :
    - **Oui** — Il s'agit du paramètre par défaut. Une adresse IP dynamique de l'encodeur, un masque de sous-réseau et une passerelle par défaut sont attribués.
    - **Non** — Consulter votre administrateur réseau pour obtenir les valeurs suivantes : adresse IP de l'encodeur, masque de sous-réseau et passerelle par défaut.
  - Réaliser l'une des configurations suivantes :
    - IP de serveur — Adresse IP du serveur Community.
    - Nom du serveur et adresse DNS IP locale — Nom du serveur Community. Si vous indiquez le nom du serveur, l'encodeur et le serveur doivent se trouver sur le même domaine. Si vous choisissez d'utiliser une adresse IP statique et de spécifier le nom du serveur, l'adresse IP du serveur de noms de domaine local est requise.

10. Cliquez sur **Sauvegarder les modifications**. L'encodeur est ajouté à la liste des encodeurs. Si vous avez sélectionné la méthode de connexion USB, l'encodeur doit rester connecté au poste de travail via USB. Les encodeurs TCP/IP doivent être connectés au réseau avant que l'état passe à **En ligne**.

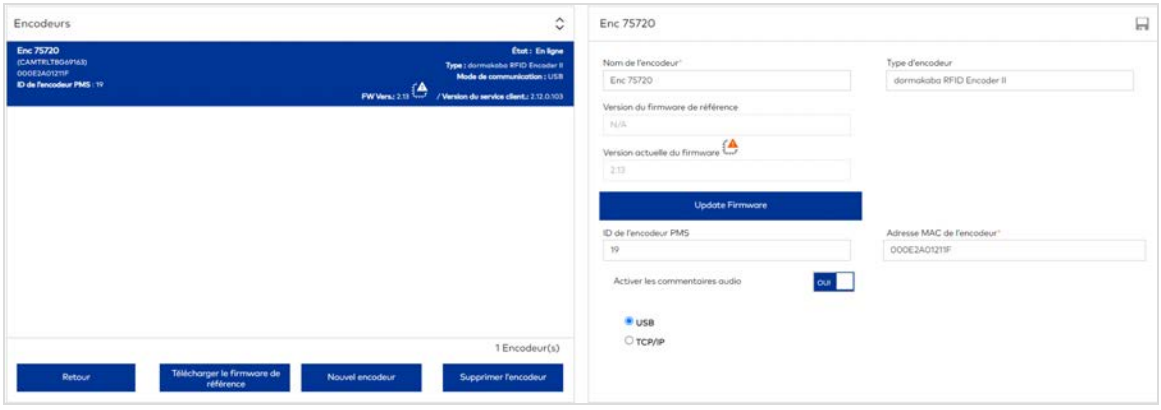


Mettre à jour le firmware de l'encodeur

Les mises à jour du firmware peuvent être effectuées directement sur Community pour l'Encodeur RFID II dormakaba. Lorsque la version du firmware installée sur l'encodeur n'est pas synchronisée avec la dernière version du firmware recommandée dans les notes de mise à jour du produit, demandez le fichier de mise à jour du firmware au support dormakaba.

Avant de suivre les étapes suivantes, obtenez le dernier fichier de la version recommandée du firmware auprès du support dormakaba.

1. Accédez à **Gestion des périphériques**. (Si la communication en ligne est activée, cliquez sur **Encodeurs**.)
2. Cliquez sur **Télécharger le firmware de référence**.
3. Accédez au fichier du firmware (*.enc2), sélectionnez-le, puis cliquez sur **Ouvrir**.
4. Cliquez sur **OK**. La version du firmware apparaît dans le champ **Version du firmware de référence**. Lorsque la version de référence et la version actuelle ne correspondent pas, un symbole d'avertissement ( ) s'affiche à côté du champ **Version actuelle du firmware**.



5. Sélectionnez l'encodeur qui nécessite une mise à jour du firmware.
6. Cliquez sur **Mettre à jour le firmware**.

7. Cliquez sur **OK** pour confirmer que la mise à jour peut prendre plusieurs minutes. Attendez-vous à ce que les voyants LED de l'encodeur clignotent. Lorsque la mise à jour est terminée, l'encodeur redémarre.
8. Après le redémarrage, débranchez puis rebranchez l'encodeur.

Modifier les encodeurs

1. Accédez à **Gestion des périphériques**. (Si la communication en ligne est activée, cliquez sur **Encodeurs**.)
2. Sélectionner l'encodeur que vous souhaitez modifier.
3. Modifiez les paramètres.
4. Cliquez sur **Sauvegarder les modifications**.

Supprimer des encodeurs

1. Accédez à **Gestion des périphériques**. (Si la communication en ligne est activée, cliquez sur **Encodeurs**.)
2. Sélectionnez l'encodeur que vous souhaitez supprimer.
3. Cliquez sur **Supprimer l'encodeur**.
4. Cliquez sur **OUI** pour confirmer.

Étape 5

Programmer des serrures

Cette section comprend les sujets suivants :

En savoir plus sur la Programmation et audit 118

Programmer des serrures 121

En savoir plus sur la Programmation et audit

Programmation et audit est le module Community dans lequel vous pouvez effectuer les transferts de données nécessaires pour programmer et auditer des serrures. M-Unit (Programmateur M-Unit) est le périphérique portable permettant le transfert de données entre le poste de travail Community et les serrures. Pendant la programmation, les données de configuration sont transférées du poste de travail Community à M-Unit puis aux serrures. Pour auditer les serrures, les données d'historique sont transférées des serrures vers M-Unit puis vers le poste de travail Community.

Lorsque la fonction de communication en ligne sous licence est activée, vous pouvez également programmer des périphériques utilisés dans des environnements en ligne.

Le transfert de données de M-Unit vers un poste de travail nécessite le client Community. Téléchargez et installez le client à partir de la barre d'outils principale du module **Programmation et audit** ou **Gestion des périphériques**.

Avec le temps, les serrures connaissent une *dérive temporelle* — un léger retard ou une légère avance — susceptible d'avoir un impact (bien que mineur) sur les paramètres des points d'accès avec une contrainte de temps. Chaque fois que M-Unit transfère des données sur une serrure, l'heure de la serrure est mise à jour, corrigeant ainsi la dérive temporelle. Une bonne pratique consiste à vérifier que M-Unit est connectée à chaque serrure au moins une fois par an.

Avant que les serrures ne soient programmées pour la première fois, les points d'accès sont accessibles à l'aide des clés de construction (ou de zone) distribuées avec le logiciel.

Programmation des serrures

Chaque serrure doit être programmée avec la définition des accès respective configurée dans Community. Le processus consiste à sélectionner les points d'accès que vous souhaitez synchroniser, à transférer les données de configuration du poste de travail Community vers M-Unit, puis à connecter M-Unit à chaque serrure pour la programmation.

Community fournit une fonction de filtrage pour faciliter l'identification des points d'accès qui nécessitent une synchronisation. Bien que tous les points d'accès nécessitent une synchronisation pour la configuration initiale du site, la fonction de filtrage est utile si vous programmez des serrures par lots, ajoutez des points d'accès ou apportez des modifications à la configuration d'accès pour les serrures.

Les codes de couleur suivants identifient les types de points d'accès qui nécessitent une synchronisation.

Coloris	Description
	Unité
	Espace commun pour les résidents
	Porte commune de la suite
	Unité de suite
	Accès privé
	Espace commun pour le personnel
	Lecteurs d'ascenseur

Programmation du point d'accès requise

Les points d'accès doivent être programmés ou reprogrammés après des tâches spécifiques dans les modules suivants :

Configurateur de site

- Après l'ajout ou la modification de la configuration de l'un des types de points d'accès suivants :
  - Unités
  - Unités de suite
  - Accès privés
  - Espaces communs résident
  - Espaces communs pour le personnel
  - Lecteur d'ascenseur
- Après la configuration ou la modification de la cartographie de relais-étages pour les ascenseurs.

Gestion des accès > Horaires de libre passage

- Après la modification d'un Horaire de libre passage.

Gestion des accès > Horaires d'accès

- Après la modification d'un Horaire d'accès.

Gestion des accès > Groupes de points d'accès

- Après l'affectation/la désaffectation de points d'accès à des groupes de points d'accès affectés à des identifiants.

Gestion des accès > Gestion des identifiants

- Après l'affectation/la désaffectation de groupes de points d'accès à des identifiants.
- Après l'affectation/la désaffectation de points d'accès à des identifiants.

Gestion des accès > Attribution horaire au point d'accès

- Après l'affectation/la désaffectation d'un Horaire de libre passage.
- Après l'affectation/la désaffectation d'un Horaire d'accès.

Paramètres du système > Résidents

- Après la modification du paramètre **Activer l'ouverture d'urgence du pêne dormant/du verrou d'intimité pour les clés de résidents**.

Paramètres du système > Sécurité

- Après la modification des paramètres d'accès aux serrures.
- Après l'activation du mode de sécurité renforcée.
- Après la suppression des clés actives héritées en mode de sécurité renforcée.

Paramètres du système > Clés du personnel/prestataire

Après la modification du paramètre **Nombre maximum d'utilisations pour lesquelles les clés à usage restreint sont valides**.

Paramètres du système > Paramètres avancés > Types de clés RFID

- Après la modification d'un des paramètres de types de clés RFID, tous les points d'accès doivent être reprogrammés.

Paramètres du système > Paramètres avancés > Activer les clés mobiles

- Après la modification de l'**ID de projet** dans les paramètres LEGIC, tous les points d'accès pour lesquels une clé mobile a été émise doivent être reprogrammés.

Paramètres du système > Communication en ligne > Rx-Link

- Après avoir activé ou désactivé ce paramètre, tous les points d'accès en ligne doivent être reprogrammés.

Programmation de périphériques

Cette option s'affiche lorsque la fonction de communication en ligne sous licence est activée.

Le périphérique doit d'abord être configuré dans ***Gestion des périphériques > Configuration du périphérique en ligne.*** 240 périphériques au maximum peuvent être programmés simultanément. La programmation des périphériques nécessite une connexion USB. Lors du transfert de données, la date et l'heure de M-Unit sont synchronisées avec le serveur. Lorsque la connexion USB est présente et qu'aucun périphérique n'est sélectionné, l'option de synchronisation de la date et de l'heure sur M-Unit est disponible. Sans connexion USB, l'option de sauvegarde des données de configuration est disponible pour certains types de périphériques.

Audit des serrures

Un audit des serrures permet de récupérer des informations détaillées sur un point d'accès. Les audits permettent de récupérer des données sur le point d'accès (telles que le modèle de serrure et le type de point d'accès), l'état de la serrure (telles que la version du firmware ou le fuseau horaire) et toutes les activités relatives à la serrure. Les données d'audit des deux méthodes sont stockées dans la base de données Community et disponibles lors de la création de Rapports d'audit de point d'accès.

Selon la finalité, les méthodes suivantes sont disponibles pour les audits de serrures :

- **Clé d'audit** — La clé d'audit est une clé système à fonction spéciale qui peut être présentée à une serrure puis lue dans Community.
- **M-Unit** — La procédure M-Unit transfère les données d'audit vers le programmateur M-Unit. Une autre étape est requise pour transférer les fichiers d'interrogation vers Community afin de les consulter. La procédure M-Unit permet de choisir, de stocker et de suivre les données historiques sur l'activité des points d'accès.

Auditer les points d'accès en ligne

Cette option s'affiche lorsque la fonction de communication en ligne sous licence est activée.

Les points d'accès en ligne peuvent être audités directement sur Community.

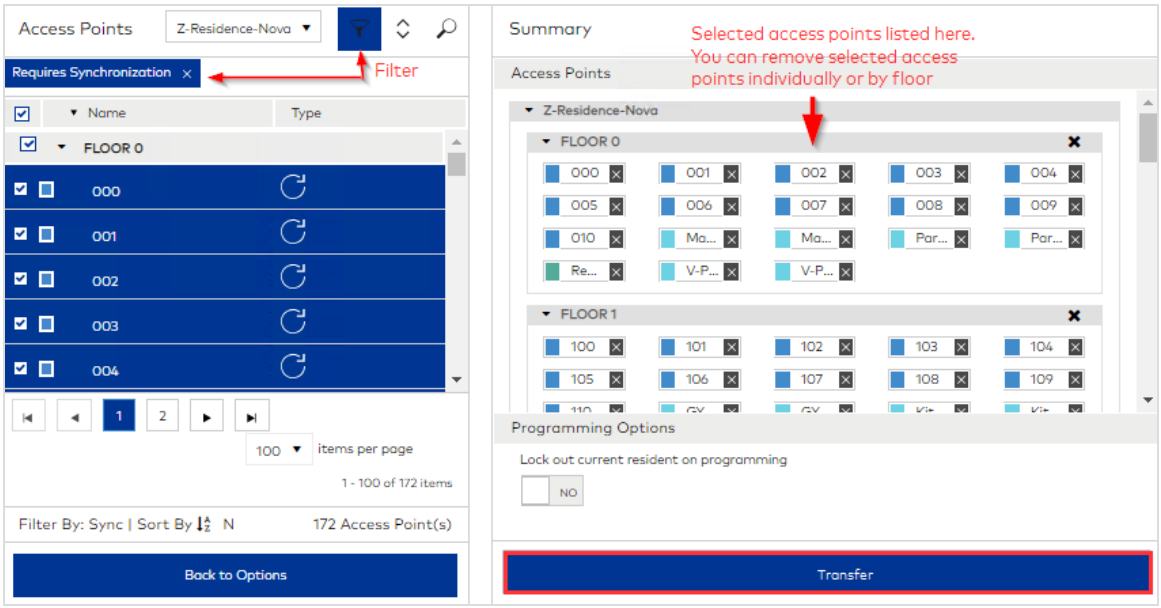
Programmer des serrures

Certaines étapes de programmation sont effectuées sur le M-Unit (Programmateur M-Unit). Pour les instructions officielles, reportez-vous à la documentation fournie avec votre périphérique. Si l'authentification du programmateur M-Unit est activée dans ***Paramètres du système > Sécurité > Programmateur M-Unit***, les identifiants doivent être configurés pour au moins un opérateur dans **Gestion du personnel/prestataire**.

Un problème avec Microsoft empêche le navigateur Edge de détecter/se connecter à un Programmateur M-Unit. Les points d'accès ne peuvent donc pas être programmés ou audités sans intervention. Ouvrez l'Invite de commande et envoyez la commande suivante :
C:\windows\system32\CheckNetIsolation.exe LoopbackExempt –a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe

Pour programmer des serrures :

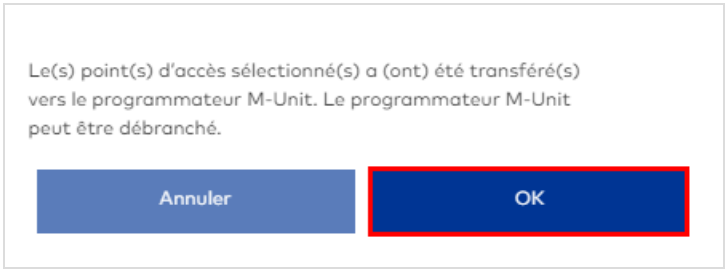
1. Accédez à ***Programmation et audit > Programmation.***



2. Sélectionnez les points d'accès que vous souhaitez synchroniser avec les données de configuration Community. Vous pouvez sélectionner des points d'accès de différents bâtiments et filtrer la liste pour n'afficher que les points d'accès nécessitant une synchronisation. Les points d'accès sélectionnés s'affichent dans la section **Sommaire** organisés par bâtiment et par étage.

   L'option **Bloquer les résidents actuels lors de la programmation** ne s'applique que lorsque les clés ont déjà été créées et remises.

3. Connectez le programmateur M-Unit au poste de travail.
4. Dans Community, cliquez sur **Transfert**. Des messages s'affichent sur le poste de travail et le programmateur M-Unit pour indiquer que le transfert est en cours. Patientez jusqu'à ce que le message s'affichant sur le poste de travail indique que le transfert est terminé et que vous pouvez débrancher le programmateur M-Unit.



5. Cliquez sur **OK**.
6. Déconnectez le programmateur M-Unit du poste de travail. Les étapes restantes sont effectuées sur M-Unit.
7. Si le mode de sécurité renforcée est activé, indiquez le mot de passe de sécurité de M-Unit. Le mot de passe s'affiche dans ***Paramètres du système > Sécurité > Mode de sécurité renforcée***. (Dans certains cas, M-Unit affiche un message avant l'invite de mot de passe indiquant que l'unité n'est pas personnalisée ; il suffit de sélectionner OK.)
8. Si l'authentification de M-Unit est activée, indiquez les identifiants de connexion de M-Unit.
9. Dans le menu du programmateur M-Unit, sélectionnez **SERRURES**.
10. Utilisez les flèches HAUT/BAS pour afficher **1 - Programme** en surbrillance, puis appuyez sur **ENTRÉE**. Les noms des points d'accès s'affichent par groupes de cinq.
11. Sélectionnez le nom du point d'accès pour la serrure, puis appuyez sur **ENTRÉE**. Utilisez les options **PRÉC**, **SUIV** et **RECHERCHER** pour parcourir et affiner la liste des noms.
12. Sélectionnez le type de sonde que vous utilisez pour connecter le programmateur M-Unit à la serrure.
13. Lorsque vous y êtes invité(e), insérez la sonde dans la serrure. La programmation démarre immédiatement. Si la serrure a déjà été programmée, le programmateur M-Unit émet un message demandant confirmation pour remplacer la programmation existante.
14. Lorsqu'un message vous indique que la programmation est terminée, cliquez sur **OK**.

Une bonne pratique consiste à tester les serrures avec des clés valides à l'issue de la programmation.

Si des problèmes surviennent lors de la programmation des serrures, créez et présentez des clés de diagnostic LED dans **Clés Système** et reportez-vous à « Dépannage des serrures ».

Étape 6

Examiner et personnaliser les rôles

Cette section comprend les sujets suivants :

En savoir plus sur la gestion des rôles 124

Consulter les rôles prédéfinis 126

Configurer les rôles personnalisés 127

En savoir plus sur la gestion des rôles

Gestion des rôles est le module Community où sont configurés les rôles qui sont attribués aux opérateurs. Un rôle est un groupement de droits qui autorise l'accès aux caractéristiques et aux fonctions Community. En attribuant un rôle à un opérateur, vous donnez accès à tous les droits sélectionnés pour ce rôle. Les opérateurs ne peuvent voir et utiliser que les caractéristiques et les fonctions autorisées par le rôle qui leur est attribué. Seuls les opérateurs ayant le rôle d'Administrateur ou de Configurateur de site ont accès à la Gestion des rôles.

Rôles prédéfinis et personnalisés

Lorsque vous attribuez des rôles aux opérateurs, vous pouvez utiliser les rôles prédéfinis ou créer des rôles personnalisés. Community comprend les rôles prédéfinis suivants, basés sur des exigences organisationnelles typiques :

- Administrateur
- Configurateur de site
- Agent de location
- Superviseur de maintenance
- Technicien de maintenance

Les droits sélectionnés pour les rôles prédéfinis ne peuvent pas être modifiés.

Les rôles personnalisés sont basés sur l'un des rôles prédéfinis et sont entièrement configurables. Toutefois, aucun rôle personnalisé ne permet d'avoir accès à la Gestion des rôles. Lorsqu'un rôle personnalisé est modifié, les changements s'appliquent à tous les opérateurs qui se voient attribuer le rôle.

Avant de modifier les droits associés à un rôle personnalisé, générez un rapport sur les **Rôles et Droits** afin de déterminer les opérateurs qui pourraient être affectés.

Droits

Il existe deux types de droits dans Community :

- **Les droits système** sont classés par module afin que vous puissiez autoriser un module entier ou des fonctions discrètes au sein d'un module. **Rapports** est une catégorie de droits système. Lorsque la catégorie **Rapports** est autorisée pour un rôle, tout opérateur auquel ce rôle a été attribué peut générer tous les types de rapports.
- Les **Droits de clés** sont classés par type de clé afin que vous puissiez autoriser toutes les commandes pour un type de clé ou des commandes discrètes pour chaque type de clé. **Clés du personnel/prestataire** est une catégorie de droits de clé. Lorsque l'ensemble de la catégorie **Clés du personnel/prestataire** est autorisé pour un rôle, tout opérateur auquel ce rôle a été attribué peut exécuter toutes les fonctions discrètes :

- Créer une clé de rechange
- Créer une clé de déblocage
- Créer une clé de reséquence
- Créer une clé d'annulation
- Créer clé supplémentaire
- Créer une clé de blocage
- Créer une nouvelle clé

Pour les droits système et les droits de clés, l'autorisation peut être activée au niveau de la catégorie ou au niveau du droit individuel. Lorsque la catégorie est sélectionnée, l'accès est autorisé pour tous les droits individuels dans la catégorie.

Affichage de l'interface utilisateur pour le contrôle des rôles

Les fonctionnalités et options qui s'affichent dans Community dépendent des droits sélectionnés pour le rôle attribué à l'opérateur. Par exemple, si l'opérateur actuellement connecté ne dispose pas des droits pour accéder au module

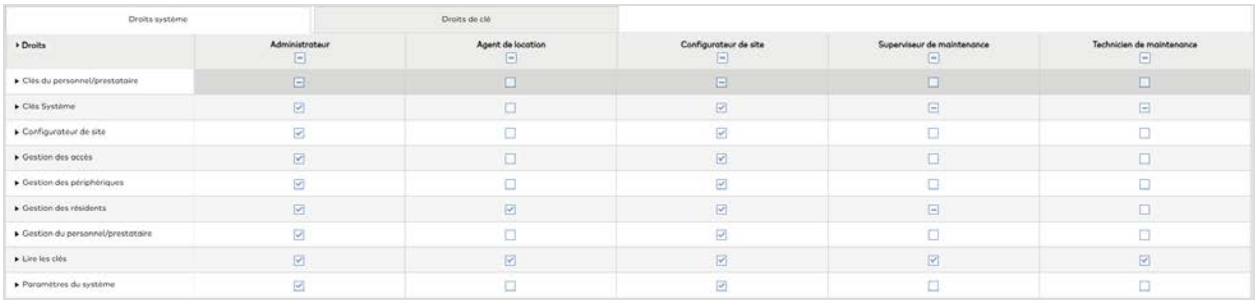
Configurateur de site, le module ne s'affiche pas. De même, si le seul droit sélectionné dans la catégorie de droits de clé ***ELO (verrouillage électronique)*** est *Créer clé supplémentaire*, la seule fois ***qu'ELO*** est affiché comme option lors de la sélection de la catégorie d'identifiants est lorsque l'opérateur crée une clé supplémentaire.

Consulter les rôles prédéfinis

dormakaba recommande de consulter les droits associés aux rôles prédéfinis avant d'attribuer des rôles aux opérateurs ou de créer des rôles personnalisés.

Pour consulter les rôles et droits :

» Accédez à **Gestion des rôles**.



Les rôles sont identifiés dans les en-têtes de colonne. Les droits sont répertoriés dans la liste minimisée de catégories de lignes à gauche. Une case cochée à côté d'un droit ou d'une catégorie de droits indique que les opérateurs auxquels le rôle est affecté peuvent effectuer les fonctionnalités/fonctions liées à ce droit. Les rôles prédéfinis ne peuvent pas être modifiés, mais vous pouvez créer des rôles personnalisés pour permettre un regroupement unique de droits (voir « Configurer des rôles personnalisés »).

Le tableau suivant répertorie les droits associés à chaque rôle prédéfini.

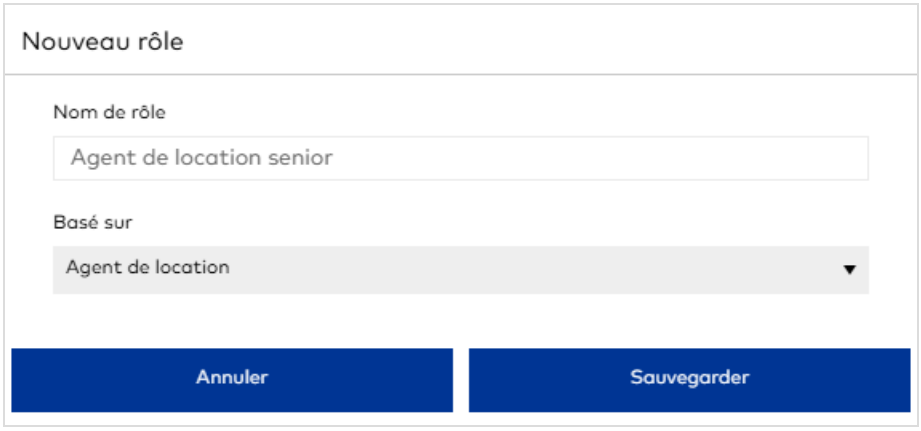
Rôle	Droits système	Droits de clé
Administrateur	Tous	Tous
Configurateur de site	Tous	Tous
Agent de location	▪ Lire les clés ▪ Gestion des résidents	Aucun
Superviseur de maintenance	▪ Programmation et audit ▪ Lire les clés ▪ Gestion des serrures à distance ▪ Gestion des résidents ▪ Rapports ▪ Clés Système > Clés de diagnostic	Aucun
Technicien de maintenance	▪ Programmation et audit ▪ Lire les clés ▪ Rapports ▪ Clés Système > Clés de diagnostic	Aucun

Configurer les rôles personnalisés

Les rôles personnalisés offrent la possibilité d'autoriser toute combinaison de droits système et de droits de clé.

Pour configurer un rôle personnalisé :

1. Accédez à **Gestion des rôles**.
2. Cliquez sur **(Ajouter)** +.



3. Indiquez un nom descriptif pour le rôle.
4. Sélectionnez un rôle existant sur lequel fonder le nouveau rôle. Tous les droits associés au rôle que vous sélectionnez s'appliquent au nouveau rôle, mais peuvent être modifiés après la création du rôle.
5. Cliquez sur **Sauvegarder**.



6. Sélectionnez ou désélectionnez des droits pour le nouveau rôle dans les onglets **Droits système** et **Droits de clé**. Si vous sélectionnez ou désélectionnez une catégorie de droits, tous les droits individuels de la catégorie sont respectivement sélectionnés ou désélectionnés implicitement.
7. Cliquez sur **(Sauvegarder)** 💾.

Étape 7

Ajouter des opérateurs

Cette section comprend les sujets suivants :

En savoir plus sur la gestion du personnel/prestataries 129

Configurer les opérateurs 131

Importer la liste des membres du personnel/prestataires 136

En savoir plus sur la gestion du personnel/prestataries

Le personnel et les prestataires sont les porteurs de clés qui travaillent ou exécutent un service sur l'établissement. La majorité du personnel correspond aux personnes dont les droits sont restreints à l'utilisation des clés qui leur sont remises, par exemple le personnel chargé de la maintenance. Certains membres du personnel, toutefois, nécessitent un accès à Community. Le personnel qui a accès à Community est appelé *Opérateurs*.

Un membre du personnel est désigné comme Opérateur dans le profil du personnel. Le degré d'accès dépend du rôle de l'opérateur sélectionné. Par exemple, un opérateur ayant le rôle prédéfini d'*Administrateur* a accès à toutes les fonctions Community, tandis que les droits d'un opérateur ayant le rôle prédéfini d'*Agent de location* sont limités aux fonctions **Gestion des résidents** et **Lire la clé**.

Vous pouvez ajouter des membres du personnel/prestataires manuellement ou importer une liste.

Profils de personnel/prestataire

Lorsqu'un membre du personnel ou un prestataire est ajouté à Community, un profil est créé avec les onglets suivants :

- **Informations sur le personnel/prestataire** — Cet onglet permet de définir les informations d'identification de base sur les membres du personnel/prestataires et d'activer les notifications. L'option permettant de désigner le membre du personnel comme opérateur se trouve sur cet onglet.
- **Informations sur l'opérateur** — Cet onglet permet de configurer l'accès de l'opérateur. L'onglet n'est actif que si le membre du personnel est désigné comme Opérateur.
- **Clés attribuées** — Cet onglet répertorie les clés actives attribuées au membre du personnel/prestataire. Vous pouvez annuler et/ou remplacer des clés dans la liste.
- **Gestion des visiteurs** — Cet onglet permet d'activer et de configurer l'attribution du code PIN pour le membre du personnel/prestataire.

Pour consulter le profil d'un membre du personnel/prestataire :

» Accédez à **Gestion du personnel/prestataire** et sélectionner un membre du personnel/prestataire.

Vous pouvez filtrer la liste des profils en fonction de l'état (Actif/Désactivé/Opérateurs uniquement).

Importation de membres du personnel/prestataires

Si le droit *Importer une liste* est activé dans la **Gestion des rôles**, vous pouvez créer des profils de personnel/prestataire en important un fichier CSV qui contient des données de base (*prénom/nom/ID*). Toute information supplémentaire, y compris la possibilité de désigner des opérateurs, doit être spécifiée manuellement dans le profil du personnel/prestataire. Le droit *Importer une liste* est activé par défaut pour les rôles Administrateur et Configurateur de site.

Gestion des visiteurs 

La gestion des visiteurs est une fonction gratuite qui fonctionne exclusivement avec AuroraSync et les clés mobiles. La gestion des visiteurs permet aux résidents et au personnel d'étendre tout ou partie de leur accès aux visiteurs sur site. En utilisant l'application BlueSky dormakaba, les résidents et le personnel peuvent générer des codes PIN pour autoriser l'accès au périmètre et aux espaces communs. Les résidents ont également la possibilité d'attribuer aux visiteurs des clés mobiles qui peuvent être utilisées pour les portes communes et l'unité du résident, si souhaité.

Un code PIN est une séquence à 7 chiffres qui peut être utilisée sur les points d'accès où un clavier numérique est installé. Une clé mobile attribuée (ou un code PIN au format clé mobile) permet l'accès à l'aide de l'application BlueSky dormakaba.

Lorsque Gestion des visiteurs est activée dans Paramètres du système pour le personnel/les prestataires, l'attribution de codes PIN peut être activée/désactivée dans l'onglet Gestion des visiteurs des profils du personnel/prestataire. Lorsque Gestion des visiteurs est activée dans Paramètres du système pour les résidents, l'attribution de codes PIN et de clés mobiles peut être activée/désactivée dans l'onglet Gestion des visiteurs des profils de résidents.

Les prérequis sont les suivants :

- AuroraSync doit être activé et configuré.
- Les clés mobiles doivent être activées et configurées.
- Le profil du résident doit comporter un numéro de téléphone portable valide.
- L'application BlueSky dormakaba doit être installée et enregistrée sur le périphérique mobile utilisé pour générer le code PIN/la clé mobile.

Clés du personnel/prestataire

Les clés du personnel/prestataire sont créées et remises aux personnes qui travaillent sur le site, ce qui peut inclure les employés, les sous-traitants et les prestataires. Les clés du personnel/prestataire sont encodées avec un identifiant défini dans ***Gestion des accès > Gestion des identifiants*** qui peut inclure l'accès à tous les types de points d'accès : unités, suites, espaces communs (résidents et personnel) et accès privés.

Les clés du personnel/prestataire sont créées dans le module **Clés du personnel/prestataire**. Les instances de clés sont ensuite gérées dans **Gestion du personnel/prestataire** en sélectionnant le personnel/prestataire à qui la clé (instance) a été attribuée, puis l'onglet **Clés attribuées** dans le profil.

Les clés du personnel/prestataire sont valides dans les espaces communs pour le personnel et les résidents et dans les contrôleurs d'ascenseurs jusqu'à l'expiration de la clé. Notez que les clés du personnel/prestataire ayant le statut Obsolète continuent à permettre l'accès aux espaces communs et aux contrôleurs d'ascenseurs jusqu'à l'expiration de la clé. Pour assurer la sécurité des clés dont l'état est obsolète, créez une clé de blocage pour la séquence de clés. Voir Paramètres du système > Clés de blocage.

Pour plus d'informations sur l'invalidation de l'accès du personnel, voir Invalidation de l'accès du personnel.

Configurer les opérateurs

La première étape de la configuration des opérateurs consiste à ajouter des membres du personnel. Vous pouvez ajouter des membres du personnel manuellement ou, si le droit *Importer la liste du personnel* est activé dans la Gestion des rôles, vous pouvez importer des membres du personnel. L'importation est limitée à la création des profils des membres du personnel avec des données de base : *prénom/nom/ID*.

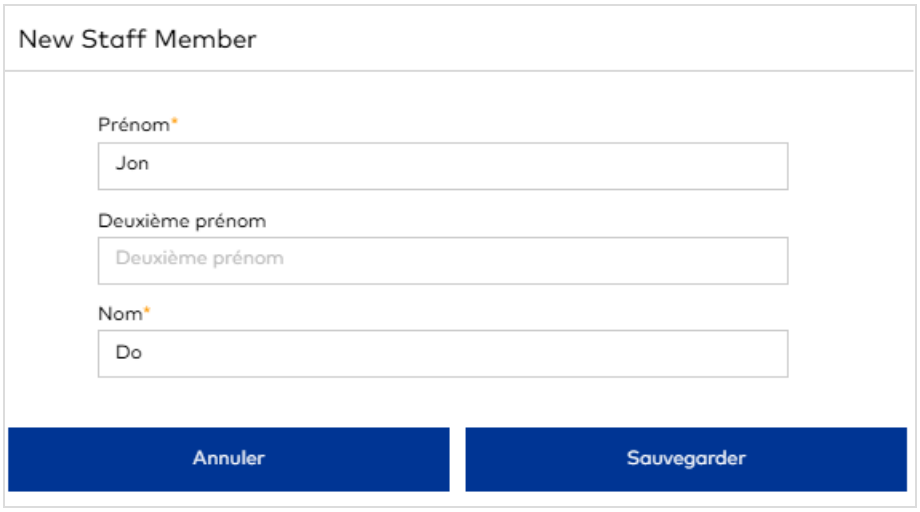
Reportez-vous à l'une des sections suivantes :

- Ajouter un membre du personnel
- Assigner le rôle d'opérateur à un membre du personnel
- Sélectionner / changer la langue par défaut du logiciel pour l'opérateur
- Assigner/modifier le rôle de l'opérateur
- Modifier le mot de passe de connexion de l'opérateur (SSO désactivée uniquement)
- Ajouter/mettre à jour les identifiants du programmateur M-Unit
- Ajouter/mettre à jour les identifiants de connexion à l'API

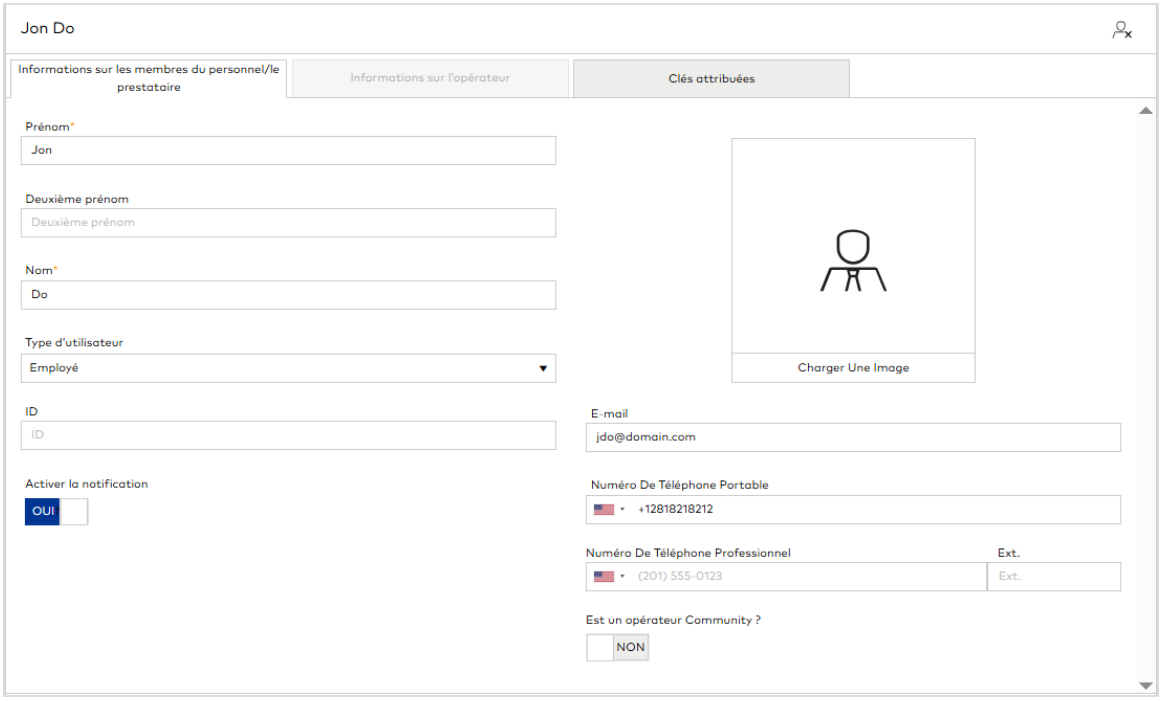
Ajouter un membre du personnel

Pour ajouter un membre du personnel :

1. Accédez à **Gestion du personnel/prestataire**.
2. Cliquez sur **(Ajouter)** .



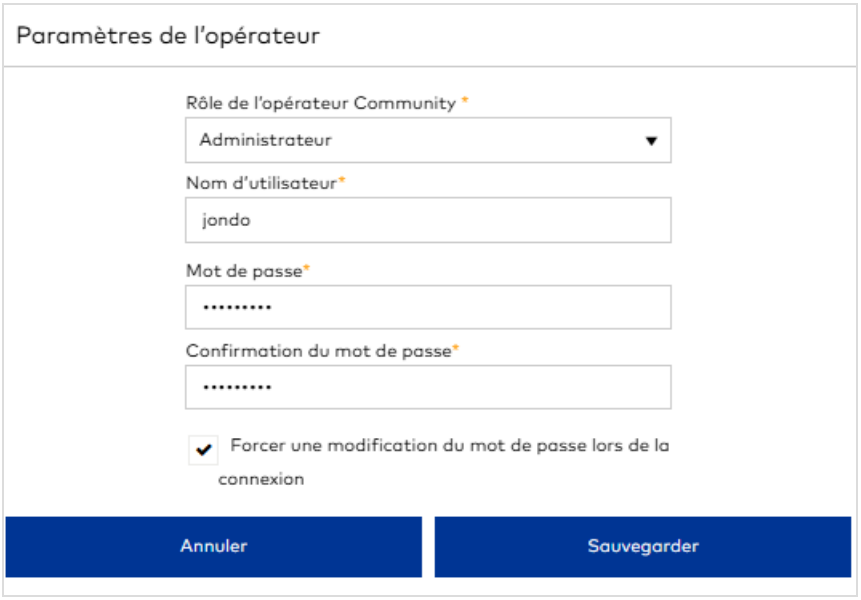
3. Indiquez le nom du membre du personnel. Utilisez le deuxième prénom pour distinguer les membres du personnel ayant le même prénom et le même nom. Nombre maximum de caractères par champ : 25.
4. Cliquez sur **Sauvegarder**. Community crée un profil et affiche l'onglet **d'informations** sur le **Personnel/prestataire**.



5. Indiquez une adresse e-mail valide. Une adresse e-mail est requise pour envoyer des e-mails automatiques concernant l'accès au compte. Les opérateurs peuvent également spécifier ou modifier l'adresse e-mail dans les Préférences du compte après s'être connectés à Community.
6. Cliquez sur **Sauvegarder**.

Assigner le rôle d'opérateur à un membre du personnel

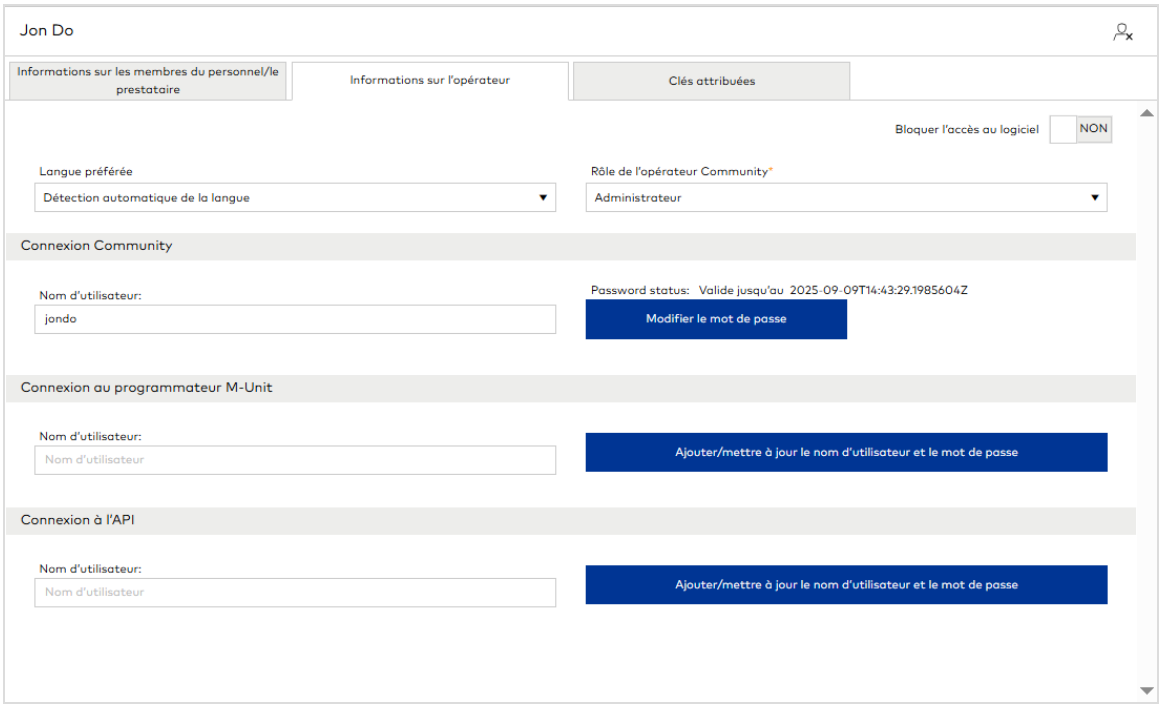
1. Accédez à **Gestion** du **personnel/prestataire** et sélectionner un membre du personnel/prestataire.
2. Dans l'onglet Informations sur le membre du personnel/prestataire, réglez le commutateur **Est u Community vers OUI**.
   - SSO est désactivée.



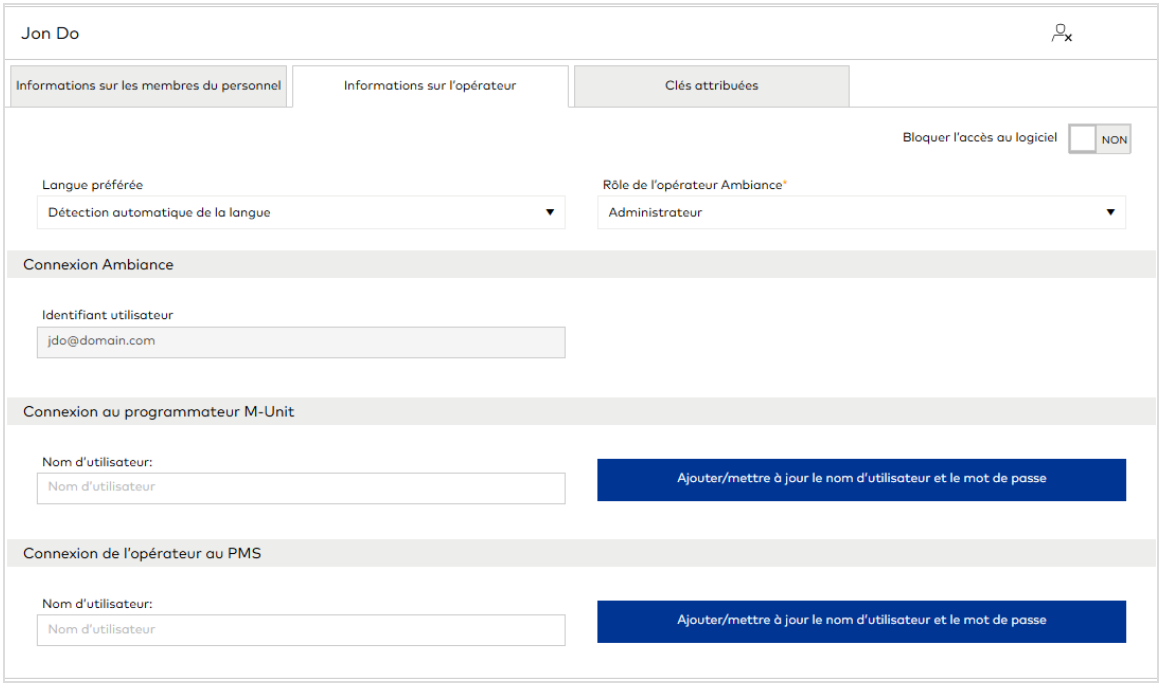
- SSO est activée.

3. Sélectionnez un rôle d'opérateur. La liste des rôles est remplie avec les rôles créés dans le module **Gestion des rôles**.
4. Sélectionnez l'une des options suivantes :
   - SSO est désactivée.
     - Définissez un nom d'utilisateur unique pour l'opérateur.
     - Spécifiez et confirmez un mot de passe pour l'opérateur.
     - (*recommandé*) Pour obliger l'opérateur à modifier le mot de passe lors de la première connexion, sélectionnez **Forcer une modification du mot de passe lors de la connexion**.
   - SSO est activée.
     - Définissez un identifiant utilisateur unique pour l'opérateur. La valeur peut être une adresse e-mail valide ou un EID (ID d'entreprise). L'information est renseignée automatiquement si une valeur est définie pour l'e-mail dans l'onglet contenant les informations du membre du personnel/prestataire.
5. Cliquez sur **Sauvegarder**. L'onglet Informations sur l'opérateur est activé. Référez-vous aux sections suivantes pour configurer des options supplémentaires.

SSO est désactivée :



SSO est activée :



Sélectionner / modifier la langue du logiciel par défaut

1. Accédez à **Gestion** du **personnel/prestataire** et sélectionnez un membre du personnel/prestataire.
2. Cliquez sur l'onglet **Informations sur l'opérateur**.
3. Sélectionnez la langue par défaut du logiciel. L'opérateur peut modifier la langue dans les **Préférences** du compte.
4. Cliquez sur **Sauvegarder**.

Assigner/modifier le rôle de l'opérateur

1. Accédez à **Gestion** du **personnel/prestataire** et sélectionnez un membre du personnel/prestataire.
2. Cliquez sur l'onglet **Informations sur l'opérateur**.
3. Sélectionnez un rôle d'opérateur. La liste des rôles est remplie avec les rôles créés dans le module **Gestion des rôles**.
4. Cliquez sur **Sauvegarder**.

Modifier le mot de passe de connexion de l'opérateur (SSO désactivée uniquement)

Uniquement disponible lorsque SSO est désactivée.

1. Accédez à **Gestion** du **personnel/prestataire** et sélectionner un membre du personnel/prestataire.
2. Cliquez sur l'onglet **Informations sur l'opérateur**.
3. Dans la section Connexion de Community, cliquez sur **Modifier le mot de passe**. Indiquez et confirmez un nouveau mot de passe, puis cliquez sur **Sauvegarder**. Vous devez communiquer les identifiants du compte à l'opérateur.
4. (*recommandé*) Pour forcer l'opérateur à changer le mot de passe lors de la première connexion, sélectionnez **Forcer une modification du mot de passe lors de la connexion**.
5. Cliquez sur **Sauvegarder**.

Ajouter/mettre à jour les identifiants de connexion au programmateur M-Unit

Lorsque l'authentification du programmateur M-Unit (M-Unit) est activée, la section **Connexion au programmateur M-Unit** s'affiche. Les identifiants doivent être configurés pour au moins un opérateur. Pour désactiver l'authentification de M-Unit,

voir « Authentification du programmateur M-Unit ».

1. Accédez à **Gestion** du **personnel/prestataire** et sélectionner un membre du personnel/prestataire.
2. Cliquez sur l'onglet **Informations sur l'opérateur**.
3. Dans la section Connexion du programmateur M-Unit, cliquez sur **Ajouter/mettre à jour le nom d'utilisateur et le mot de passe**.



4. Indiquez un nom d'utilisateur.
5. Indiquez et confirmez un mot de passe.
6. Cliquez sur **Sauvegarder les modifications**.

Ajouter/mettre à jour les identifiants de connexion à l'API

Lorsque l'authentification de connexion à l'API est activée, la section Connexion à l'API s'affiche. Les identifiants doivent être configurés pour au moins un opérateur. Pour désactiver l'authentification API, voir ***Paramètres du système > Sécurité > Intégration API***.

1. Accédez à **Gestion** du **personnel/prestataire** et sélectionnez un membre du personnel/prestataire.
2. Cliquez sur l'onglet Informations sur l'opérateur.
3. Dans la section Connexion à l'API, cliquez sur **Ajouter/mettre à jour le nom d'utilisateur et le mot de passe**.



4. Indiquez un nom d'utilisateur.
5. Indiquez et confirmez un mot de passe.
6. Cliquez sur **Sauvegarder les modifications**.

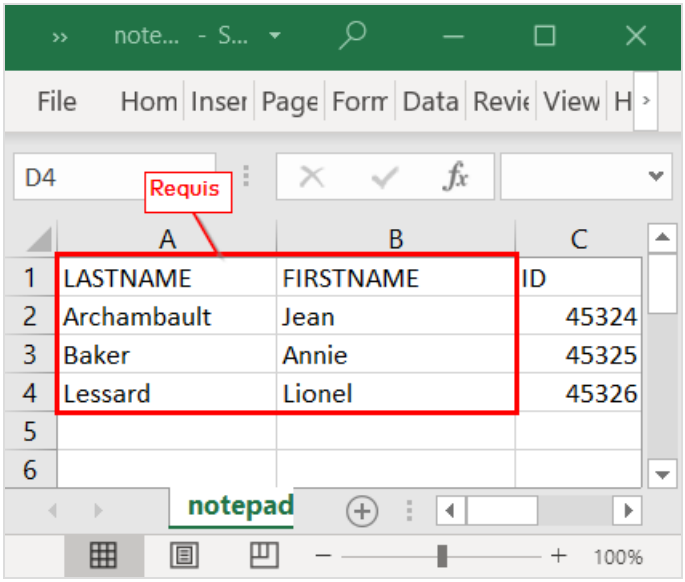
Importer la liste des membres du personnel/prestataires

Pour importer les membres du personnel/prestataires :

1. Accédez à **Gestion du personnel/prestataire**.
2. Cliquez sur ***(Plus)*** **▪▪▪** ***> Importer la liste du personnel***.

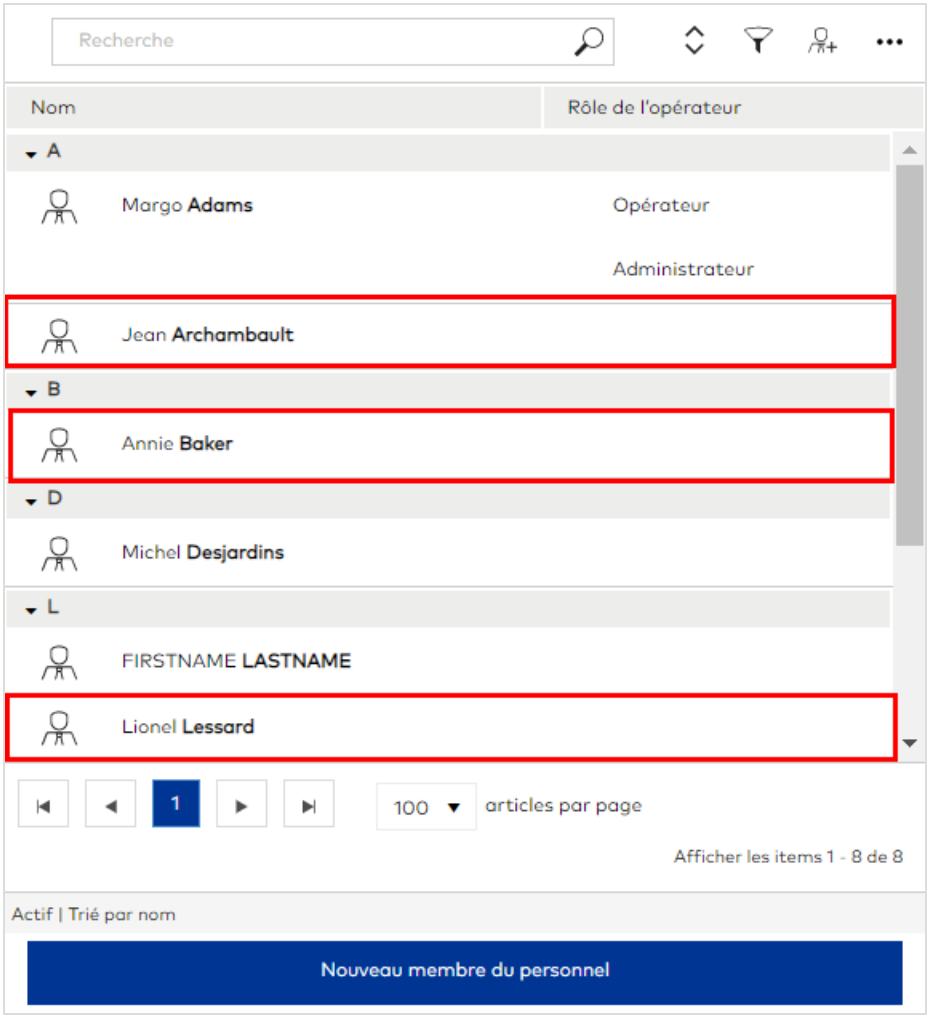


3. Naviguez et sélectionnez le fichier que vous souhaitez importer, puis cliquez sur **Ouvrir**. Type de fichiers pris en charge : csv. La figure suivante montre un exemple de fichier et le format de données requis. Si un champ requis est vide, le membre du personnel/prestataire n'est pas ajouté.



> Si les profils des membres du personnel ont déjà été créés, vous êtes invité à continuer. Cliquez sur **OUI** pour continuer.

4. Lorsque vous êtes informé que l'importation est réussie, cliquez sur **OK**.


Recherche
Nom
Rôle de l'opérateur
A
Margo Adams
Opérateur
Administrateur
Jean Archambault
B
Annie Baker
D
Michel Desjardins
L
FIRSTNAME LASTNAME
Lionel Lessard
1
100
articles par page
Afficher les items 1 - 8 de 8
Actif | Trié par nom
Nouveau membre du personnel

Utilisation Community

Cette section comprend les sujets suivants :

Gestion des résidents 141

En savoir plus sur la gestion des résidents 142

Ajouter des résidents 150

Importer la liste des résidents 152

Affecter les unités 154

Créer des clés de résidents 161

Modifier l'accès résident 164

Invalider l'accès des résidents 170

Créer des clés pour l'accès aux espaces communs uniquement 180

Créer des clés mobiles pour plusieurs résidents 182

Configurer la gestion des visiteurs pour les résidents 184

Gestion du personnel et des prestataires 186

En savoir plus sur la Gestion du personnel/prestataire et les Clés du personnel/prestataire 187

Ajouter des membres du personnel/prestataires 189

Importer la liste des membres du personnel/prestataires 191

Créer des clés d'urgence 193

Créer une clé du personnel (accès prédéfini) 196

Créer des clés du personnel (accès variable) 199

Créer des clés de prestataire 204

Créer des clés à usage restreint 208

Remplacer les clés du personnel/prestataire 212

Invalider l'accès du personnel/prestataire 214

Configurer la gestion des visiteurs pour les membres du personnel/prestataires 219

Programmation/Audit 220

Reprogrammer des serrures 221

Audit des serrures ... 223
Auditer les points d'accès en ligne ... 224
Clés système ... 225
En savoir plus sur les clés Système ... 226
Clés de blocage et de déblocage ... 230
Clés d'annulation ... 234
Clés de diagnostic ... 237
Clés de bascule de verrouillage électronique ... 239
Clés à sécurité intégrée ... 241
Clés d'annulation ... 242
Clés de verrouillage et de déverrouillage ... 244
Clés de programmation primaire et secondaire ... 246
Clés de reséquence ... 249
Clés à fonction spéciale ... 251
Surveillance ... 253
En savoir plus sur la surveillance ... 254
Surveiller les clés ... 255
Surveiller l'utilisation des clés numériques ... 256
Rapports ... 258
Rapport d'audit de point d'accès ... 259
Rapport sur les attributions des identifiants/points d'accès ... 261
Rapport sur la configuration des ascenseurs ... 262
Rapport sur les expirations de clés ... 263
Key/User Assignment Report ... 264
Rapport sur les opérateurs ... 265
Rapport sur la configuration du site ... 266
Rapport sur les rôles et droits ... 267
Rapport des accès du personnel/prestataire ... 268
Rapport sur l'activité système ... 269
Rapport de gestion des visiteurs ... 271
Les bases de la barre d'outils ... 272
Naviguer Community ... 273
Définir les préférences de l'opérateur ... 275
Installation / Mise à jour du Client Community ... 277
Sélectionner l'encodeur par défaut ... 278

Déverrouillage/verrouillage à distance 279
Lire la clé/effacer la clé/rapport de suivi d'accès 281
Afficher les notifications 285
Clés physiques 288
Clés mobiles 290

Résidents

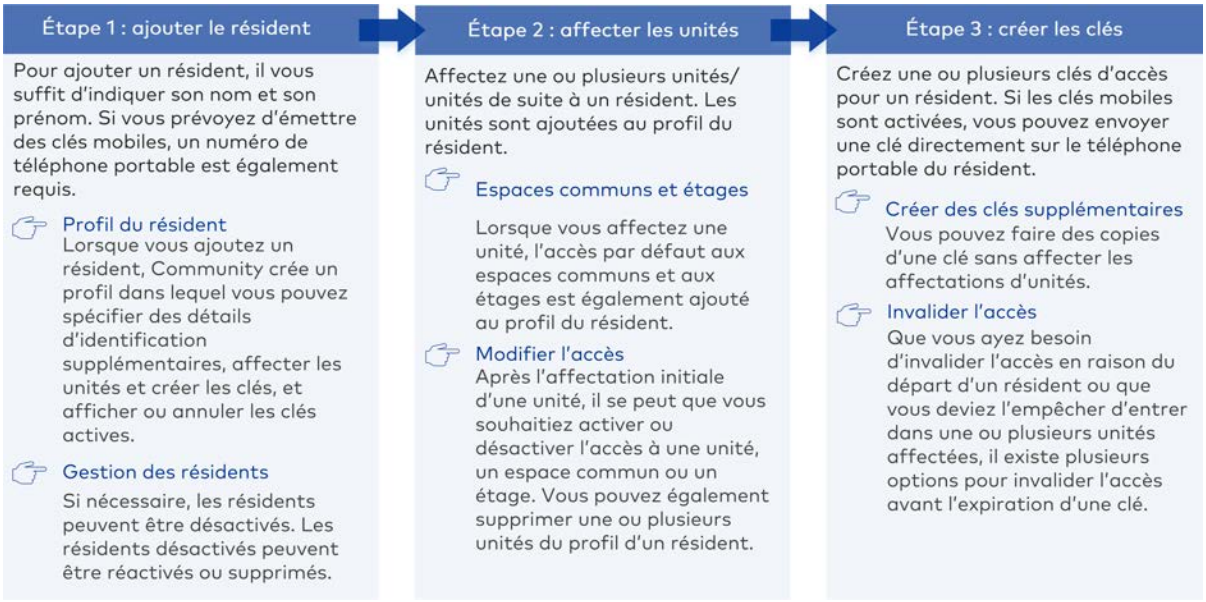
Gestion des résidents

Cette section comprend les sujets suivants :

- En savoir plus sur la gestion des résidents 142
- Ajouter des résidents 150
- Importer la liste des résidents 152
- Affecter les unités 154
- Créer des clés de résidents 161
- Modifier l'accès résident 164
- Invalider l'accès des résidents 170
- Créer des clés pour l'accès aux espaces communs uniquement 180
- Créer des clés mobiles pour plusieurs résidents 182
- Configurer la gestion des visiteurs pour les résidents 184

En savoir plus sur la gestion des résidents

Le module Gestion des résidents permet d'ajouter des résidents à Community, de configurer et gérer l'accès des résidents, et de créer ou d'annuler les clés de résidents. La figure suivante résume les étapes.

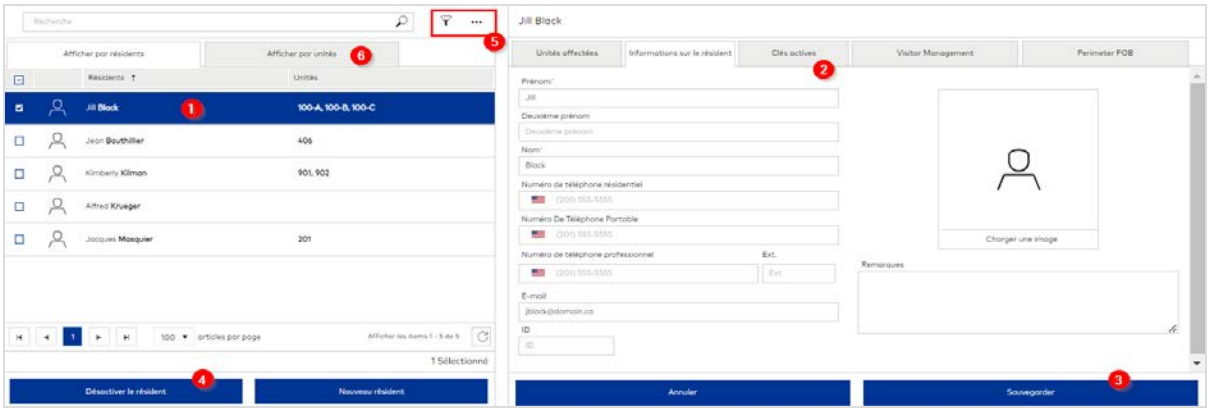


Si Gestion des visiteurs est activée pour les résidents, vous pouvez également configurer les paramètres d'attribution de codes PIN et/ou de clés mobiles pour le résident.

Si Aurora est activé, l'onglet FOB périmétrique s'affiche. Pour plus d'informations, voir *Intégration de Community et Aurora*, PK3769.

Ajouter des résidents

Les résidents peuvent être ajoutés individuellement ou par importation par lots. Une fois les résidents ajoutés, des détails d'identification facultatifs peuvent être spécifiés dans l'onglet **Informations résident**.



Reportez-vous à la figure ci-dessus et à la liste de référence suivante pour en savoir plus sur l'ajout d'un résident et les actions à entreprendre après avoir ajouté un résident.

1 : Un nouveau résident est ajouté à la liste des résidents actifs.

2 : Le profil s'ouvre dans l'onglet **Informations résident**.

3 : Après avoir ajouté d'autres détails, comme un ID, cliquez sur **Sauvegarder**.

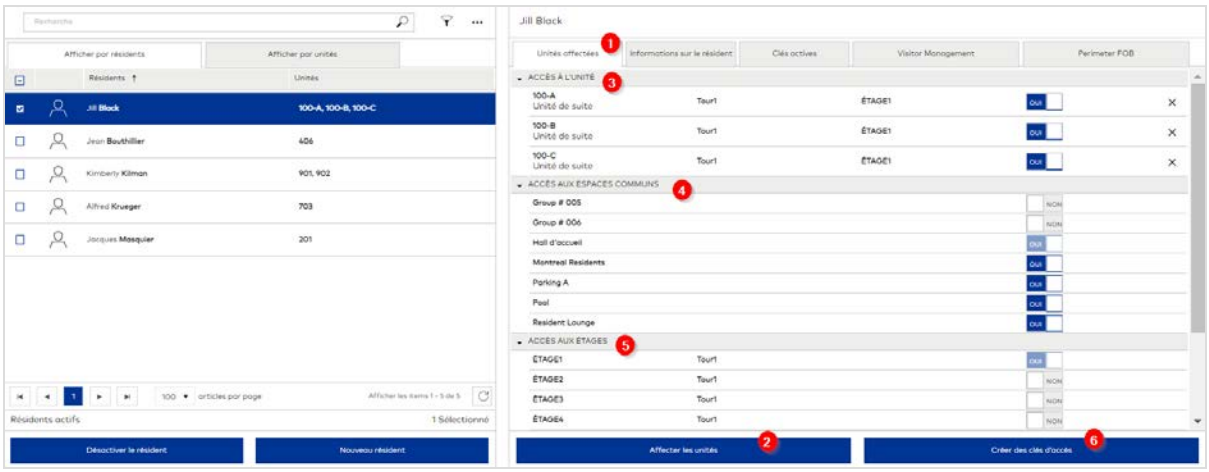
4 : Cliquez sur **Désactiver** pour désactiver les résidents sélectionnés.

5 : Cliquez sur (Filtrer) pour afficher les onglets **Actif** et **Désactivé** . Cliquez sur **(Plus) ...** pour importer une liste de résidents.

6 : Les résidents désactivés sont répertoriés ici ; vous pouvez soit réactiver, soit supprimer les résidents désactivés.

Affecter les unités et créer des clés

La configuration de l'accès pour un résident comprend l'affectation des unités et l'activation ou la désactivation des points d'accès, tels que les espaces communs et les étages. La configuration qui en résulte crée l'identifiant à encoder sur les clés d'accès.



1 : L'accès résident peut être configuré et géré dans l'onglet **Unités affectées** dans le profil de résident. Vous pouvez affecter les unités, modifier l'accès et créer des clés d'accès. Vous pouvez également configurer l'accès aux espaces communs sans affecter d'unité.

2 : Lorsque vous cliquez sur **Affecter les unités**, vous pouvez ajouter une unité au profil du résident. Les options de filtrage montrent où l'unité est située et si elle est occupée ou libre. Vous pouvez affecter une unité occupée à un autre résident, mais les politiques relatives au partage s'appliquent. Pour plus d'informations sur les politiques de partage intégrées, voir Accès résident partagé.

Lorsque des unités sont partagées entre un ou plusieurs résidents, la modification de l'accès pour un résident peut également modifier l'accès pour les résidents qui partagent l'accès. Lorsque des modifications de l'accès se répercutent sur d'autres résidents, le système de messagerie de Community répertorie tous les résidents sur lesquels se répercutent les modifications.

3 : La section **ACCÈS À L'UNITÉ** répertorie les unités affectées. L'accès est activé par défaut. Vous pouvez activer ou désactiver à tout moment l'accès à toute unité du profil.

4 : La section **ACCÈS AUX ESPACES COMMUNS** répertorie tous les espaces communs illimités et restreints. L'accès aux espaces communs illimités est réglé sur **OUI** et ne peut pas être désactivé. L'accès aux espaces communs restreints peut être activé et désactivé. L'accès par défaut dépend de l'affectation ou non d'une unité et, le cas échéant, du profil d'accès aux espaces communs associé aux unités affectées. Si aucune unité n'est affectée, l'accès par défaut aux espaces communs restreints est réglé sur **NON**. Lorsqu'au moins une unité est affectée, les espaces communs restreints activés par défaut dans le profil d'accès aux espaces communs pour les résidents associé aux unités affectées sont activés. Tous les espaces communs restreints précédemment activés (avant l'affectation d'une unité) restent activés après l'affectation d'une unité.

5 : La section **ACCÈS AUX ÉTAGES** répertorie tous les étages pour les bâtiments dans lesquels une unité est affectée à un résident. Par défaut, l'accès est activé pour les étages sur lesquels l'accès résident est activé, mais l'accès à tous les étages dans la liste peut être activé ou désactivé.

La section ACCÈS AUX ÉTAGES affiche seulement si l'option **Accès aux étages** est activée (***Paramètres du système > Résidents***).

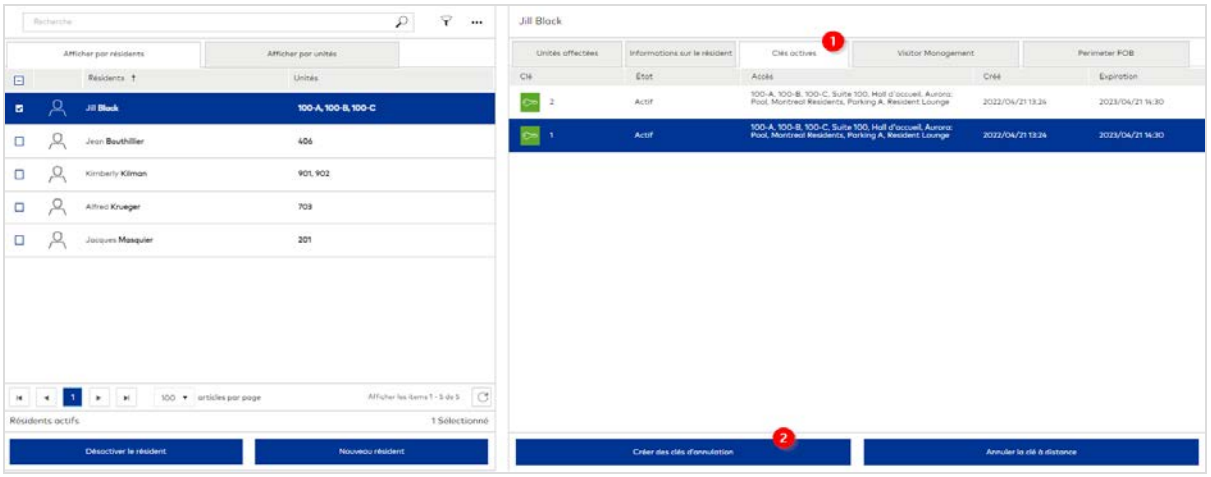
6 : Lorsque vous cliquez sur **Créer des clés d'accès**, vous pouvez créer des clés physiques et/ou des clés mobiles. L'utilisation de clés mobiles est une fonction sous licence qui doit être activée dans **Paramètres du système**.

- Les clés de résidents sont valides dans les espaces communs pour les résidents jusqu'à l'expiration de la clé ou jusqu'à ce qu'une nouvelle clé pour la ou les mêmes unités soit présentée à la ou les serrures respectives.
- Les clés de résidents sont valides dans les contrôleurs d'ascenseur jusqu'à l'expiration de la clé.

Si nécessaire, la clé de blocage peut être utilisée pour invalider l'accès à tous les types de points d'accès. Cependant, après avoir présenté la clé de blocage aux serrures respectives, la clé de déblocage ne rétablira pas l'accès aux espaces communs.

Clés actives

Les clés actives attribuées à un résident sont énumérées dans l'onglet **Clés actives** du profil du résident. Vous pouvez vérifier à tout moment l'état d'une clé ou annuler une clé.

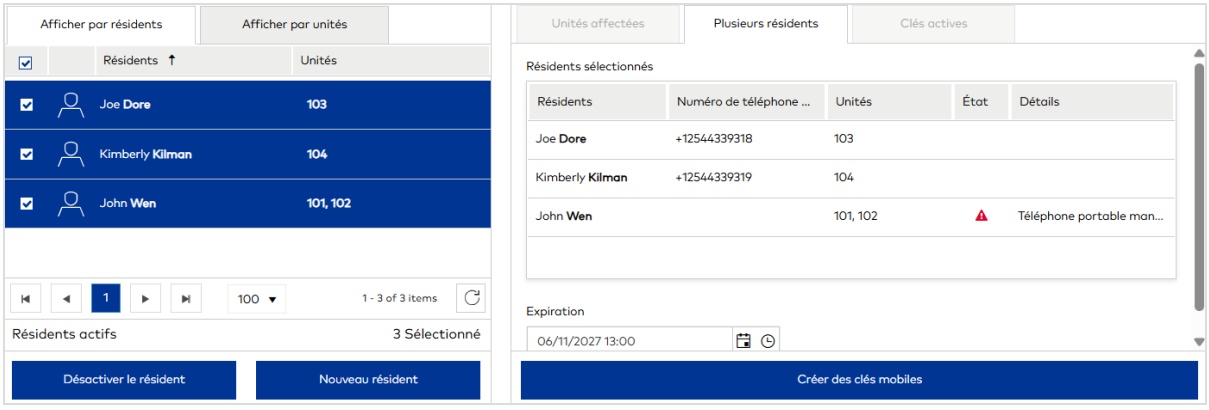


1 : L'onglet **Clés actives** répertorie toutes les clés actives pour le résident sélectionné.

2 : Toutes les clés d'annulation physiques que vous créez pour une instance de clé active doivent être présentées à la serrure installée à chaque point d'accès (unités et espaces communs) avant que l'accès ne soit annulé. Si l'annulation des clés mobiles est activée dans **Paramètres du système**, vous pouvez envoyer la clé d'annulation directement sur le téléphone portable du résident.

Plusieurs résidents

Lorsque deux résidents ou plus sont sélectionnés dans l'onglet Afficher par résidents, l'onglet Plusieurs résidents s'affiche. Créez des clés mobiles pour plusieurs résidents en même temps. Chaque résident doit avoir un numéro de téléphone portable valide et au moins une unité affectée.

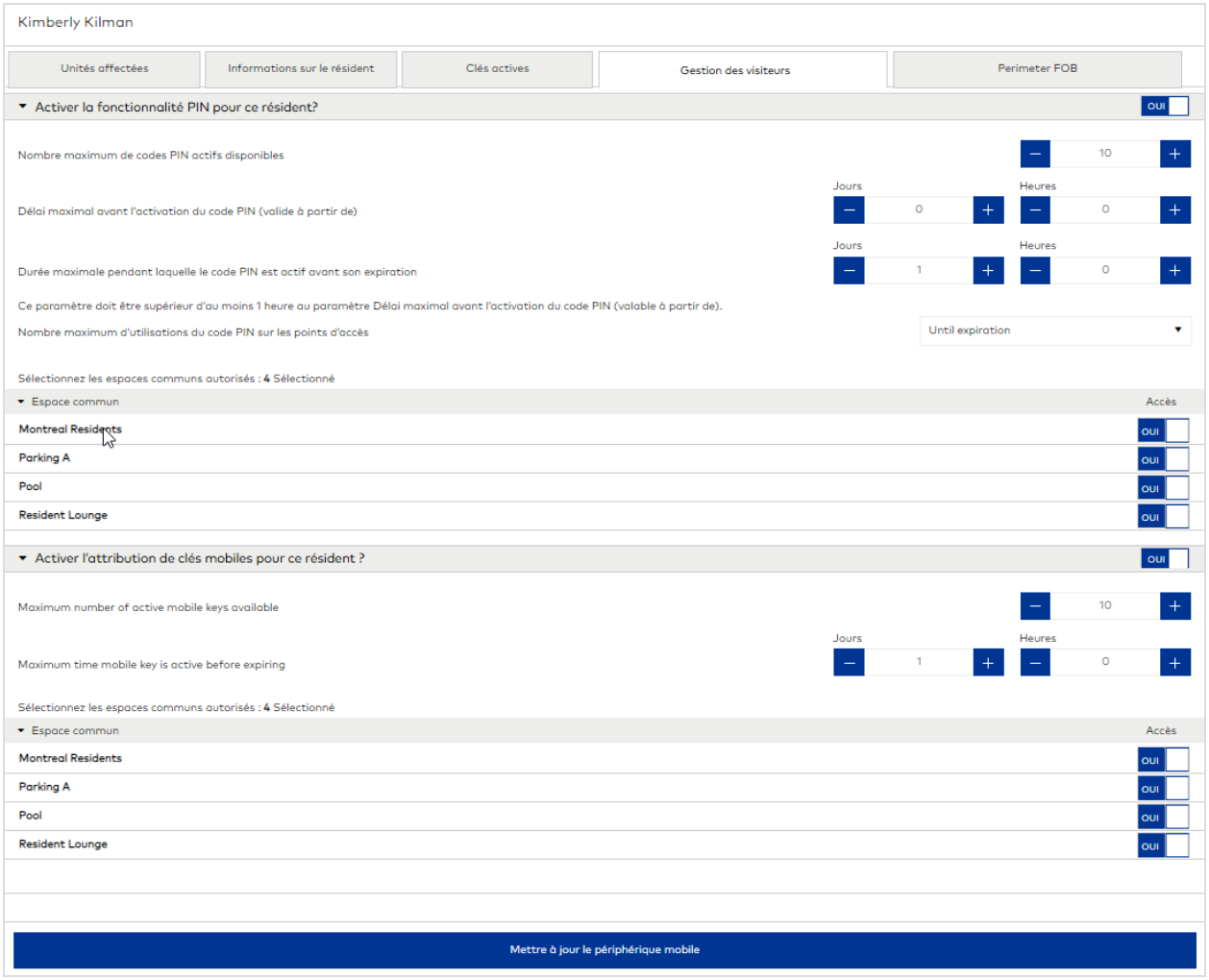


Gestion des visiteurs

La gestion des visiteurs est une fonction gratuite qui fonctionne exclusivement avec AuroraSync et les clés mobiles pour permettre aux résidents d'étendre tout ou partie de leur accès aux visiteurs sur site. En utilisant l'application BlueSky dormakaba, les résidents peuvent générer des codes PIN et des clés mobiles pour autoriser l'accès au périmètre et aux espaces communs.

- Un code PIN est une séquence à 7 chiffres qui peut être utilisée sur les points d'accès où un clavier numérique est installé.
- Une clé mobile attribuée (ou un code PIN au format clé mobile) permet l'accès à l'aide de l'application BlueSky dormakaba.

Lorsque Gestion des visiteurs est activée pour les résidents dans **Paramètres du système**, l'attribution de codes PIN et de clés mobiles peut être activée/désactivée dans l'onglet **Gestion des visiteurs** du profil du résident.

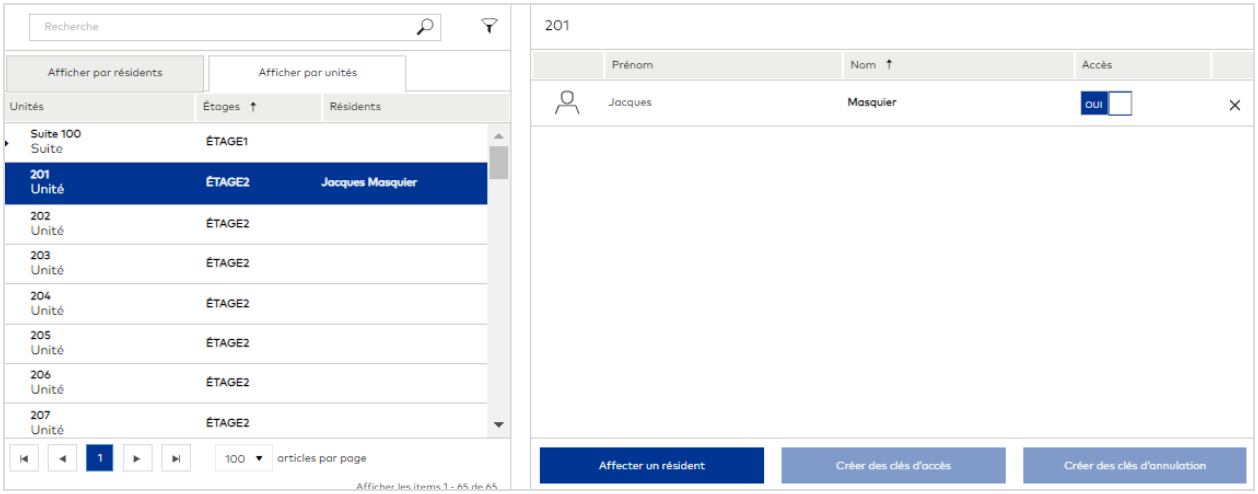


Les prérequis sont les suivants :

- AuroraSync doit être activé et configuré.
- Les clés mobiles doivent être activées et configurées.
- Le profil du résident doit comporter un numéro de téléphone portable valide.
- L'application BlueSky dormakaba doit être installée et enregistrée sur le périphérique mobile utilisé pour générer le code PIN/la clé mobile.

Affichage des unités

Une alternative à la gestion de l'accès des résidents dans le profil du résident est d'afficher une liste de toutes les unités dans l'onglet **Afficher par unités**. Lorsque vous sélectionnez une unité dans la liste, tous les résidents affectés à cette unité sont répertoriés. Vous pouvez affecter un nouveau résident ou un résident existant à l'unité, activer ou désactiver l'accès du résident à l'unité, désaffecter le résident de l'unité, et créer des clés d'accès et d'annulation pour le résident sélectionné.



Accès résident partagé

Le partage Community est basé sur la manière dont les unités sont regroupées. Des groupes d'unités sont créés et fonctionnent en arrière-plan. Lorsqu'une unité libre est affectée à un résident auquel aucune autre unité n'est affectée, un groupe est créé. Lorsqu'une deuxième unité libre est affectée à un autre résident auquel aucune autre unité n'est affectée, un second groupe est créé.

Jean est un nouveau résident. L'unité libre 100 est affectée à Jean. Cette action crée un groupe (GroupeA) avec une unité (100). Lisa est également une nouvelle résidente. L'unité libre 101 est affectée à Lisa. Cette action crée un second groupe (GroupeB).

Étant donné que le scénario par défaut est une unité par résident, la plupart des groupes ne contiennent qu'une unité. Toutefois, lorsque de multiples résidents partagent plus d'une unité, les modifications relatives à l'accès pour un résident peuvent affecter tous les autres résidents qui partagent l'accès.

Il existe trois politiques qui contrôlent le partage :

- Une unité ne peut se trouver que dans un seul groupe.
- Les unités affectées à un résident doivent parvenir d'un seul groupe.
- Si une unité d'un groupe est affectée à un résident, toutes les unités au sein du groupe lui sont affectées ; toutefois, l'accès à chaque unité dans le groupe peut être activé ou désactivé dans les profils de résident individuels.

Community filtre les listes de sélection des résidents et unités pour appliquer les politiques relatives au partage.

Avec l'unité 100 (GroupeA) affectée à Jean et l'unité 101 (GroupeB) affectée à Lisa, Community exclut l'unité 101 dans la liste de sélection lors de l'affectation d'unités à Jean. De même, Community exclut l'unité 100 dans la liste de sélection des unités lors de l'affectation d'unités à Lisa. Les unités se trouvent dans deux groupes différents.

Voyons ce qui est permis et comment s'appliquent les politiques relatives au partage.

Attribuer des unités à un résident

Vous pouvez affecter une unité à un résident lorsque :

- L'unité est libre et aucune autre unité n'est affectée au résident.

L'unité libre 100 est affectée à Jean. Le groupe d'unités GroupeA est créé.

- L'unité est occupée et aucune autre unité n'est affectée au résident.

L'unité 100 est affectée à Marc. Jean et Marc partagent l'unité 100. Une unité du GroupeA est affectée aux deux résidents.

- L'unité est libre et le résident partage l'accès aux autres unités. Dans ce cas, chaque résident auquel est affecté au moins une unité dans un groupe reçoit également l'affectation de toutes les unités dans le groupe.

L'unité 102 est affectée à Marc. Comme Marc partage l'accès avec Jean, les messages Community indiquent que l'unité 102 sera également affectée à Jean. Si vous procédez avec l'opération, l'unité 102 est ajoutée aux profils de résident de Jean et Marc avec l'accès autorisé.

Supprimer l'accès résident

Trois moyens existent pour supprimer l'accès d'un résident à des unités affectées :

- Supprimer l'unité du profil du résident
- Supprimer le résident du profil de l'unité
- Désactiver l'accès à l'unité dans le profil du résident

La méthode correcte pour choisir dépend si vous souhaitez suspendre temporairement ou supprimer définitivement l'accès ; et si l'unité est une parmi au moins deux unités partagées par des résidents multiples.

- Si vous suspendez l'accès temporairement, il est conseillé de désactiver l'accès dans le profil de résident.
- Si vous souhaitez supprimer l'accès définitivement, alors supprimez l'unité du profil de résident (ou supprimez le résident du profil d'unité).

Pour vous aider à décider si vous devez supprimer ou désactiver, comprendre que quand une unité est l'une de deux unités ou plus partagées par des résidents multiples, la suppression d'une unité d'un profil de résident (ou la suppression d'un résident du profil d'unité) supprime l'unité pour tous les résidents qui partagent l'accès.

Jean et Marc partagent les unités 100, 101, 102. La suppression de l'unité 101 du profil de Jean supprime l'unité 101 du profil de Marc.

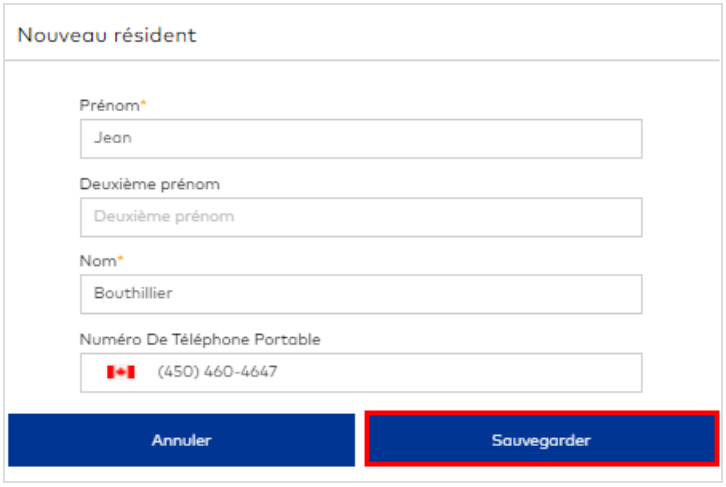
Ajouter des résidents

L'ajout d'un nouveau résident à Community nécessite seulement un prénom et un nom. Si le plan de déploiement comprend la création de clés mobiles, il convient d'indiquer un numéro de téléphone portable. Pour chaque résident ajouté, Community crée un profil de résident. Toutes les données concernant le résident, y compris les détails d'identification, les affectations d'unités et les clés actives, sont configurées et gérées dans le profil de résident. Lors de la définition d'un nouveau résident, le profil s'ouvre dans l'onglet **Informations résident** où les détails facultatifs relatifs au résident peuvent être indiqués.

Pour importer des informations sur les résidents, voir Importer la liste de résidents.

Pour ajouter des résidents :

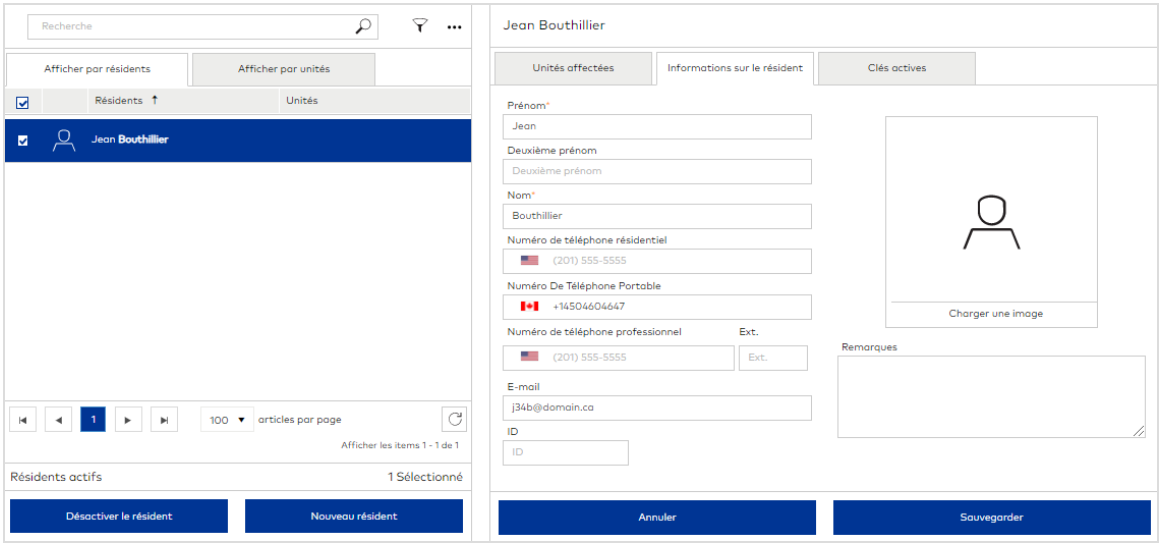
1. Accédez à **Gestion des résidents**.
2. Cliquez sur **Nouveau résident**.



3. Saisissez les nom et prénom. Même si le deuxième prénom est facultatif, utilisez le champ pour distinguer des personnes portant les mêmes nom et prénom. Nombre maximum de caractères par champ : 25.
4. (*sous conditions*) Si vous prévoyez de remettre des clés mobiles, indiquez le numéro de téléphone portable complet, y compris codes pays et région. Le numéro de téléphone portable est obligatoire pour la création de clés mobiles.
5. (*facultatif*) Indiquez des numéros de téléphone supplémentaires, un code d'identification unique (caractères maximum : 100), des remarques (caractères maximum : 2 000) et chargez une image.

Si l'ouverture forcée pour la validation du numéro de téléphone/téléphone portable est activée dans **Paramètres du système**, les opérateurs peuvent autoriser l'utilisation de numéros inconnus.

6. Indiquez une adresse e-mail valide pour le résident.
7. Cliquez sur **Sauvegarder**.

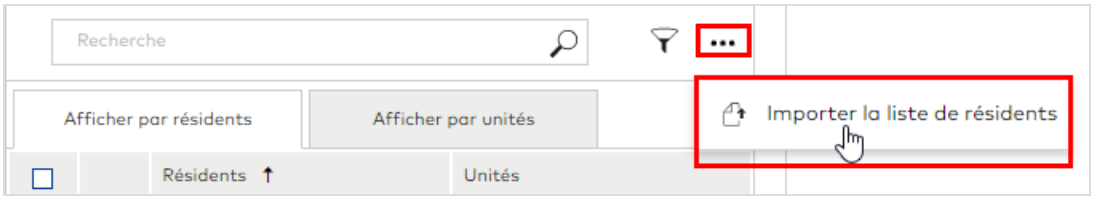

Recherche
Afficher par résidents
Afficher par unités
Résidents
Unités
Jean Bouthillier
100 articles par page
Afficher les items 1 - 1 de 1
Résidents actifs
1 Sélectionné
Désactiver le résident
Nouveau résident
Jean Bouthillier
Unités affectées
Informations sur le résident
Clés actives
Prénom*
Jean
Deuxième prénom
Deuxième prénom
Nom*
Bouthillier
Numéro de téléphone résidentiel
(201) 555-5555
Numéro De Téléphone Portable
+14504604647
Numéro de téléphone professionnel
Ext.
(201) 555-5555
Ext.
E-mail
j34b@domain.ca
ID
ID
Charger une image
Remarques
Annuler
Sauvegarder

Importer la liste des résidents

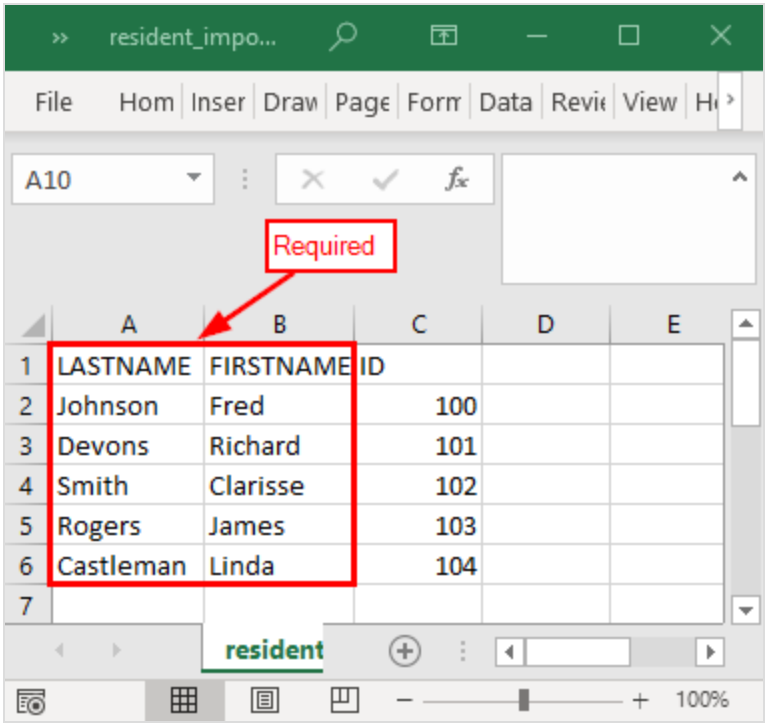
Utilisez le modèle d'importation fourni pour respecter les exigences de format. Téléchargez le modèle à partir de la page d'accueil Aide contextuelle / Gestion des résidents.

Pour importer des résidents :

1. Préparez le fichier d'importation.
2. Accédez à **Gestion des résidents**.
3. Cliquez sur ***(Plus)*** **...** ***> Importer la liste de résidents***.

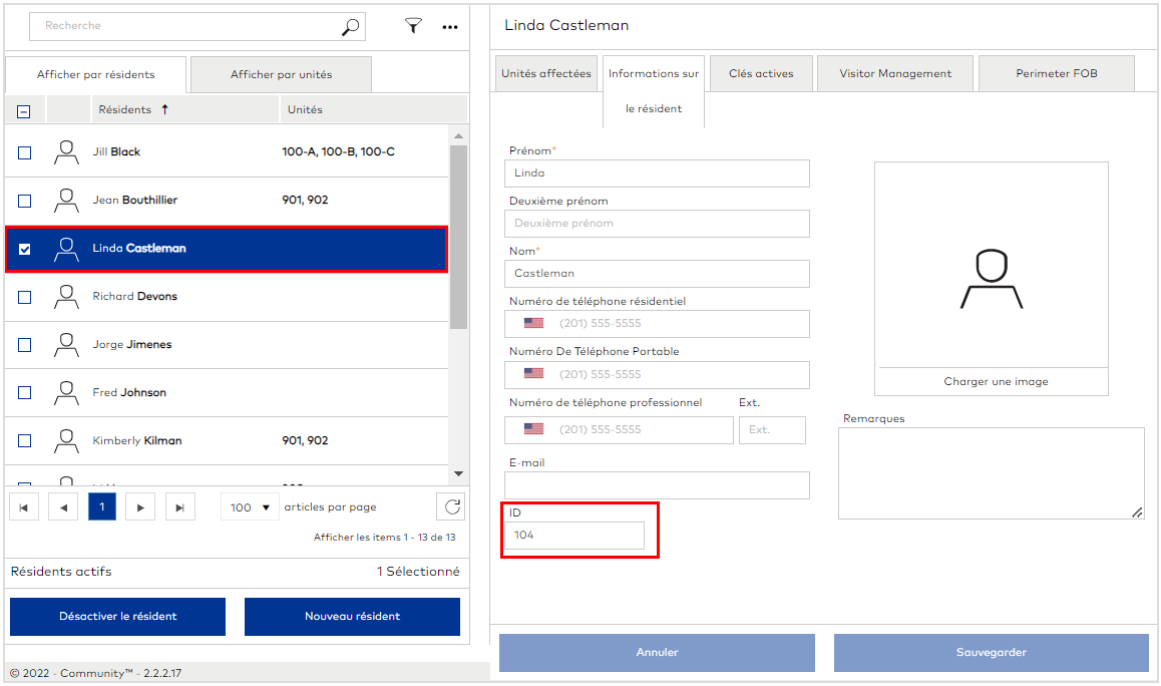


4. Naviguez et sélectionnez le fichier que vous souhaitez importer, puis cliquez sur **Ouvrir**. Type de fichiers pris en charge : csv (.csv UTF-8 pour les langues autres que l'anglais). La figure suivante montre un exemple de fichier et le format de données requis. Si un champ obligatoire est vide, le résident n'est pas ajouté.



Si la paire nom/prénom dans les profils de résidents existants correspond aux données du fichier d'importation, des profils dupliqués sont créés.

5. Lorsque vous êtes informé que l'importation est réussie, cliquez sur **OK**.

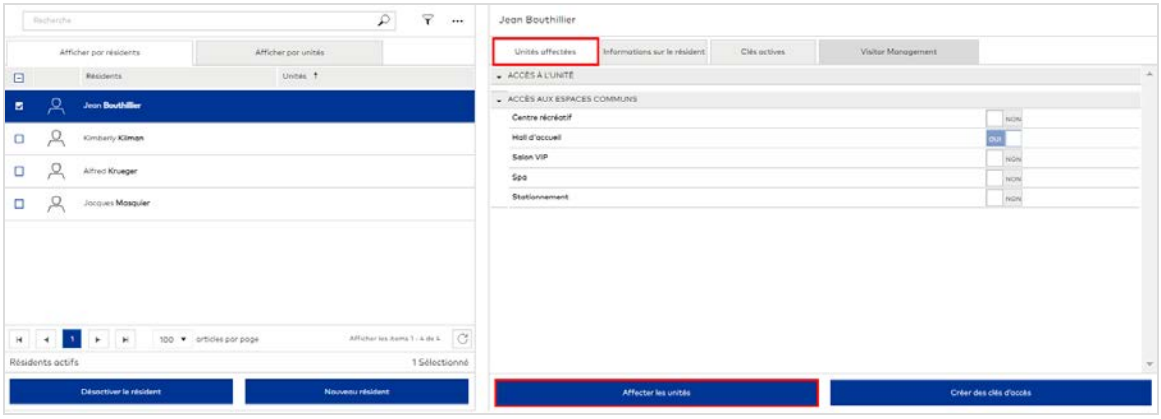

Recherche
Afficher par résidents
Afficher par unités
Résidents
Unités
Jill Black
100-A, 100-B, 100-C
Jean Bouthillier
901, 902
Linda Castleman
Richard Devons
Jorge Jimenes
Fred Johnson
Kimberly Kilman
901, 902
100 articles par page
Afficher les items 1 - 13 de 13
Résidents actifs
1 Sélectionné
Désactiver le résident
Nouveau résident
© 2022 - Community™ - 2.2.2.17
Linda Castleman
Unités affectées
Informations sur le résident
Clés actives
Visitor Management
Perimeter FOB
Prénom*
Linda
Deuxième prénom
Deuxième prénom
Nom*
Castleman
Numéro de téléphone résidentiel
(201) 555-5555
Numéro De Téléphone Portable
(201) 555-5555
Numéro de téléphone professionnel
Ext.
(201) 555-5555
Ext.
E-mail
ID
104
Charger une image
Remarques
Annuler
Sauvegarder

Affecter les unités

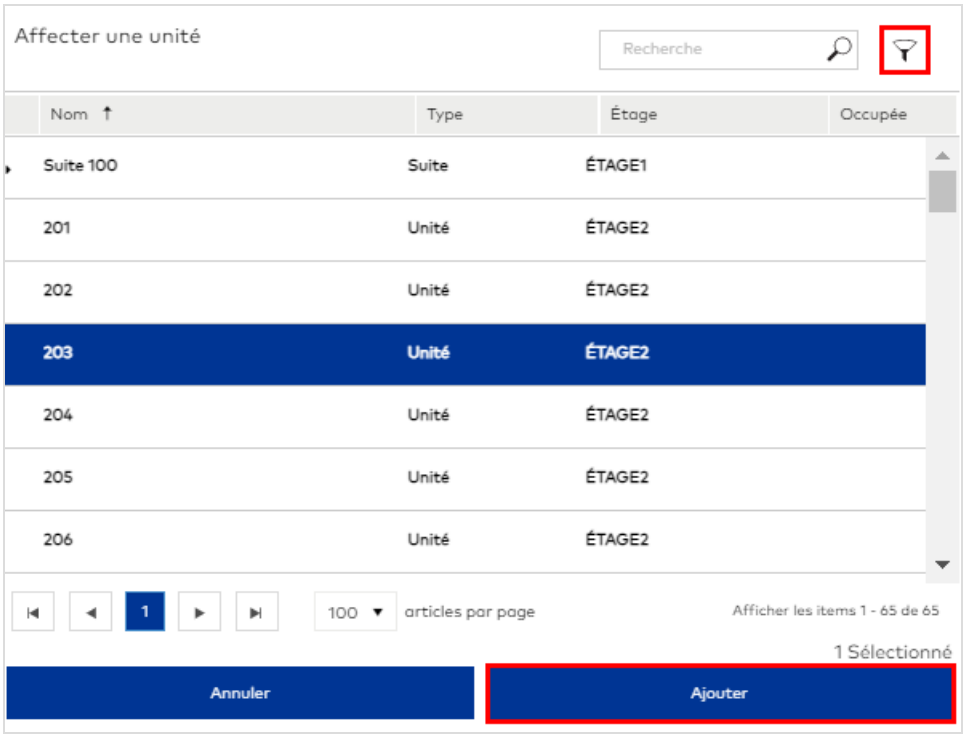
Vous pouvez affecter les unités aux résidents à partir de l'onglet **Afficher par résidents** et affecter des résidents aux unités à partir de l'onglet **Afficher par unités**. Le scénario le plus simple et le plus courant est que chaque résident se voit attribuer une seule et unique unité. Cependant, Community prend en charge l'accès partagé afin qu'un ou plusieurs résidents puissent être affectés à une ou plusieurs unités.

Afficher par résidents

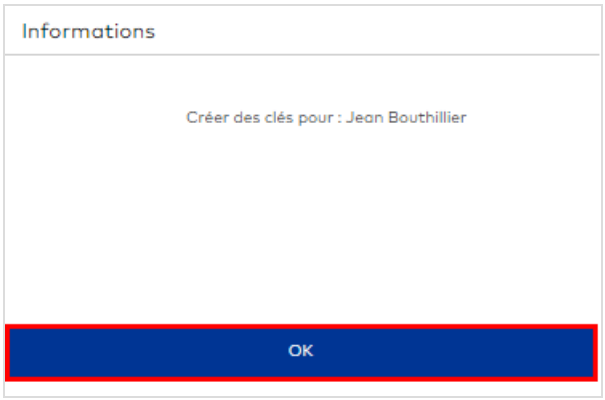
1. Accédez à **Gestion des résidents**.
2. Sélectionnez un résident.
3. Cliquez sur l'onglet **Unités affectées**.



4. Cliquez sur **Affecter les unités**.



5. Sélectionnez une unité.
   - Vous pouvez sélectionner des unités de différents bâtiments.
   - Vous pouvez filtrer la liste par type de chambre, étage et état d'occupation.
6. Cliquez sur **Ajouter**.

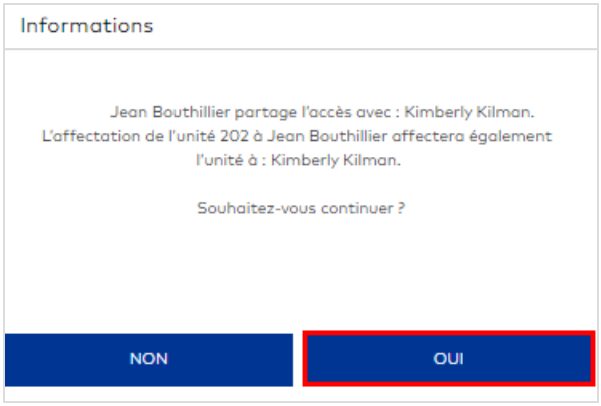


7. Lorsque vous êtes informé des clés que vous devez créer, cliquez sur **OK**.

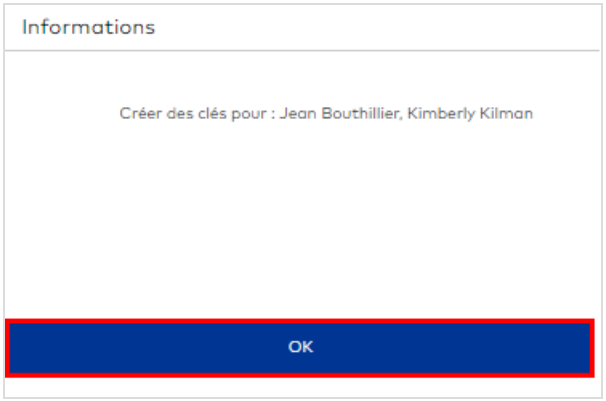
> À chaque fois qu'une modification de l'accès est effectuée, Community affiche un message qui répertorie les noms des résidents pour lesquels des clés doivent être créées. Si ces messages ne s'affichent pas, mettez l'option **Afficher les messages d'avertissement de la clé** dans ***Paramètres du système > Résident*** sur **OUI**.

Affectation des unités lorsque les résidents partagent l'accès

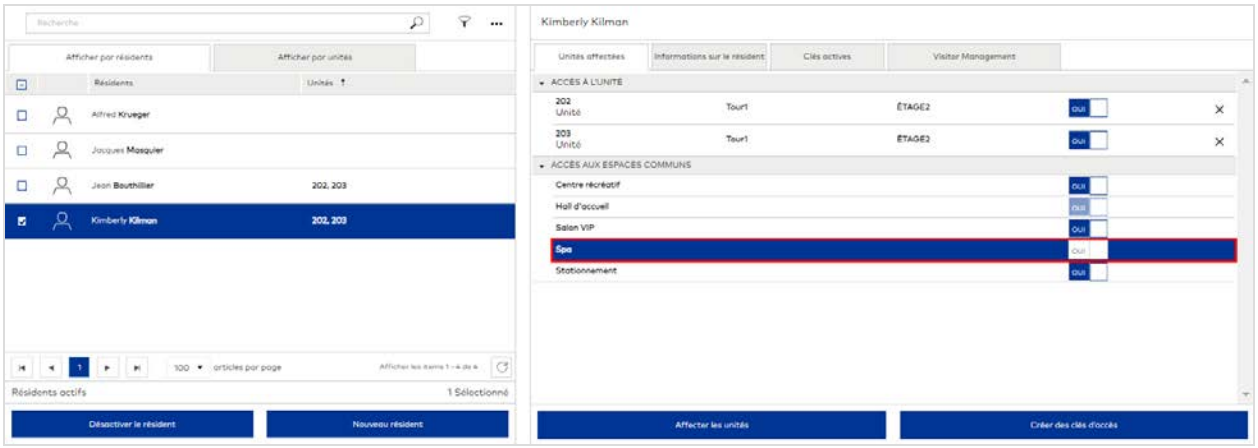
Lorsque vous affectez une unité à un résident qui partage l'accès, vous devez étendre l'accès à tous les résidents qui partagent l'accès.



Lorsque vous sélectionnez **OUI**, Community ajoute l'unité (avec accès activé) aux profils de résidents pour tous les résidents qui partagent l'accès. Community vous informe également des clés que vous devez créer.



Si vous souhaitez que tous les résidents concernés aient accès à l'unité, cliquez sur **OK** et créer des clés pour chaque résident. Cependant, vous pouvez apporter des modifications supplémentaires, telles que l'ajout/la suppression de l'accès aux espaces communs, dans les profils individuels de résidents avant de créer les clés.



Affectation d'unités occupées

Vous ne pouvez affecter des unités occupées qu'aux résidents auxquels aucune autre unité n'a été affectée.

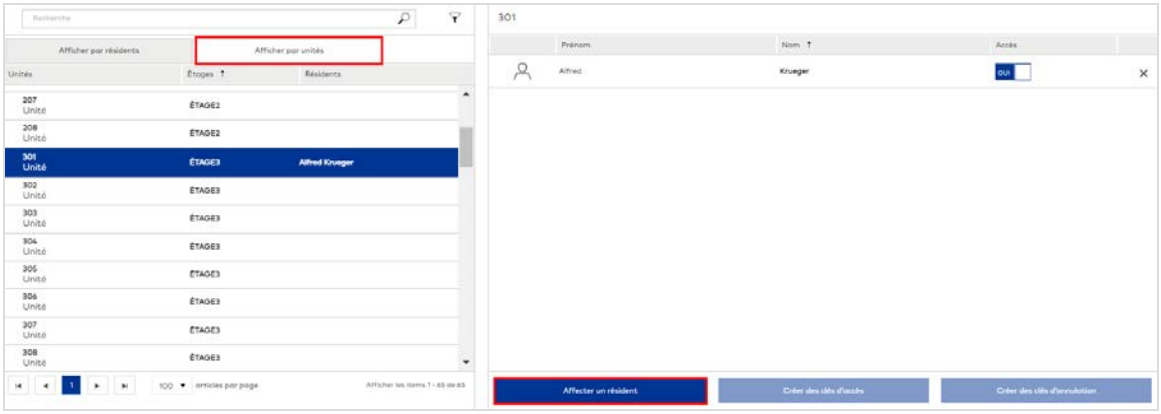
Afficher par unités

Dans Aperçu des unités, vous pouvez ajouter un résident existant ou un nouveau résident à une unité.

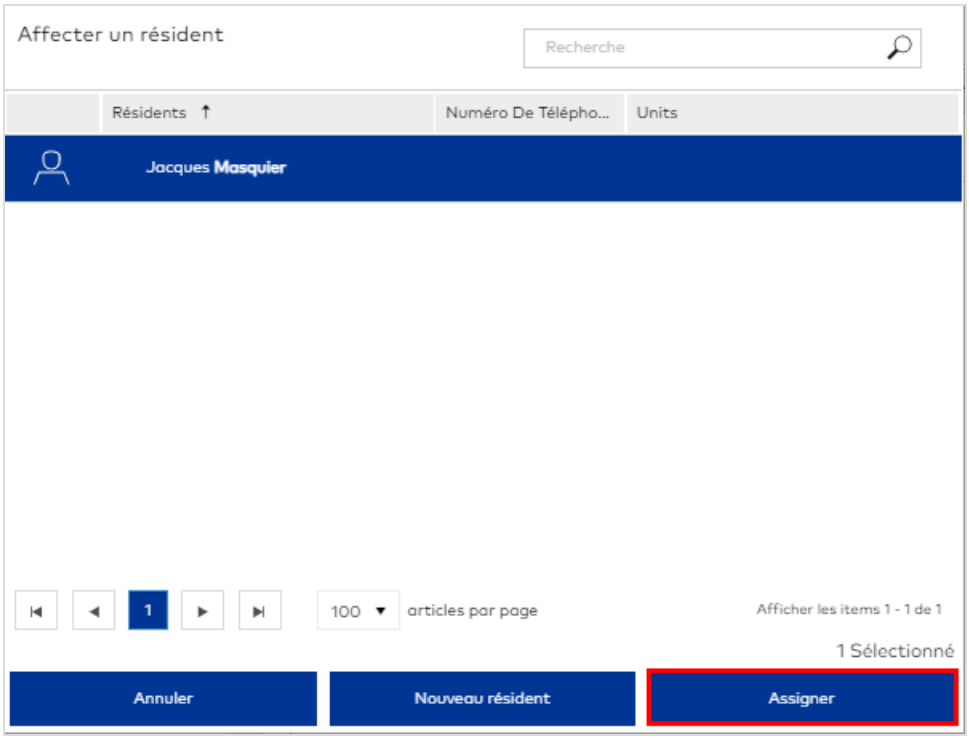
Affecter un résident existant à une unité

Pour ajouter un résident existant à une unité :

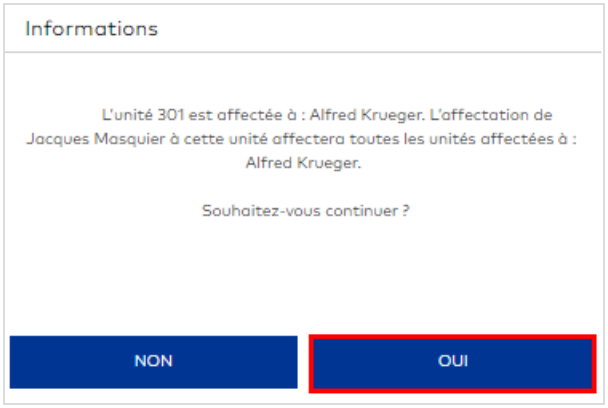
1. Accédez à **Gestion des résidents**.
2. Cliquez sur l'onglet **Afficher par unités**.

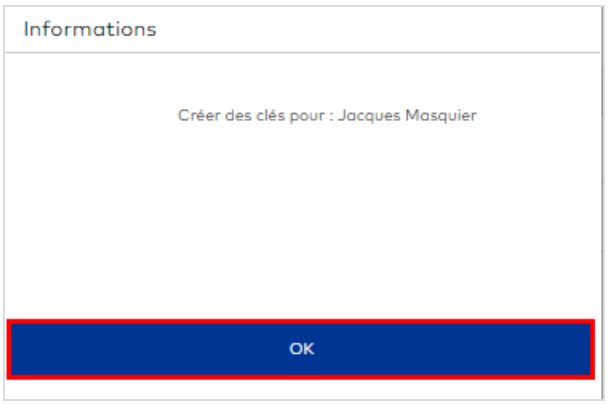


3. Sélectionnez une unité.
4. Cliquez sur **Affecter un résident**.



5. Sélectionnez un résident.
6. Cliquez sur **Affecter**. L'unité que nous avons affectée étant occupée, Community vous demande de confirmer l'affectation de l'unité.



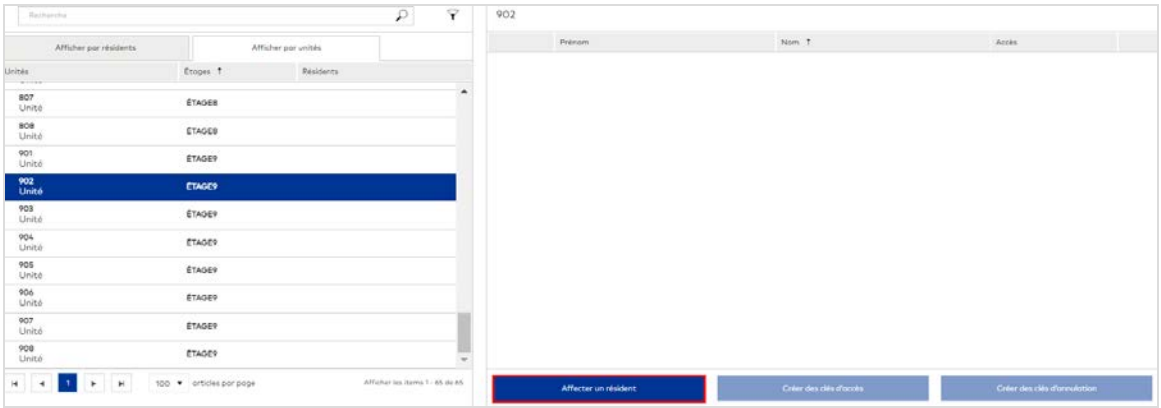


7. Lorsque vous êtes informé des clés que vous devez créer, cliquez sur **OK**.

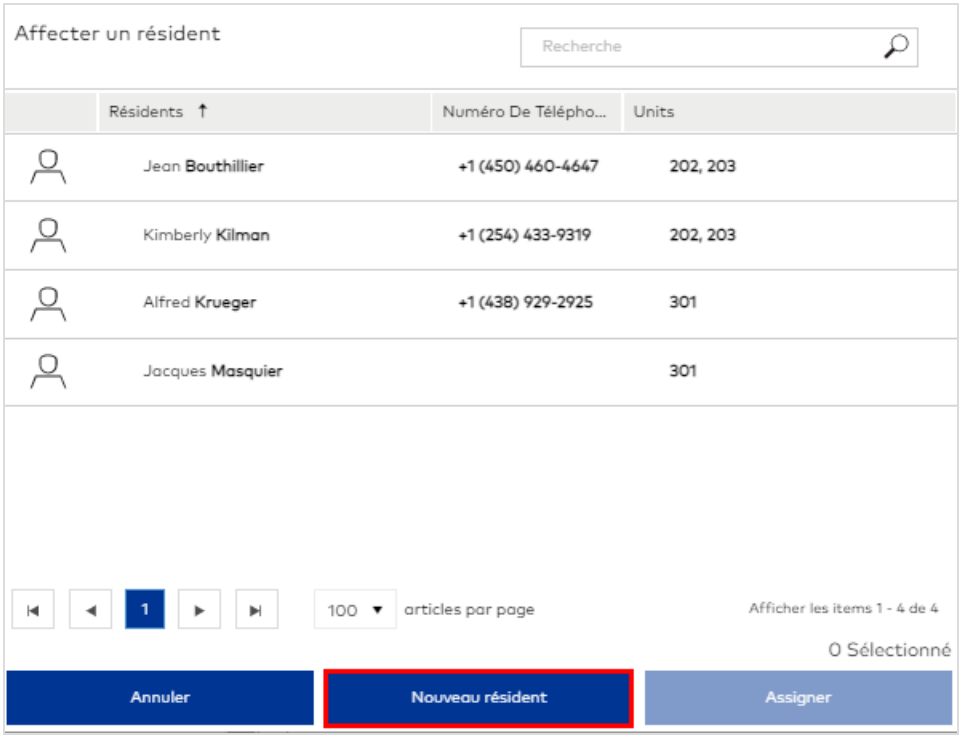


Affecter un nouveau résident à une unité

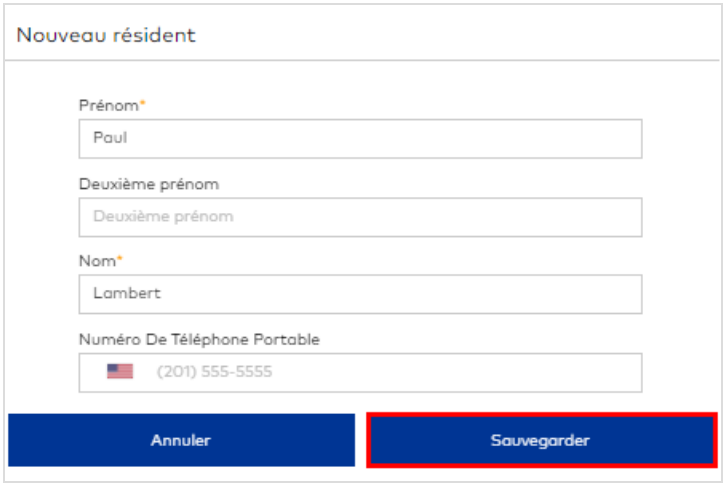
1. Accédez à **Gestion des résidents**.
2. Cliquez sur l'onglet **Afficher par unités**.



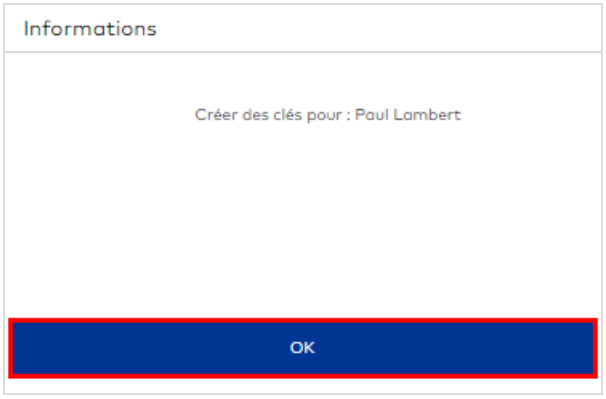
3. Sélectionnez une unité.
4. Cliquez sur **Affecter un résident**.



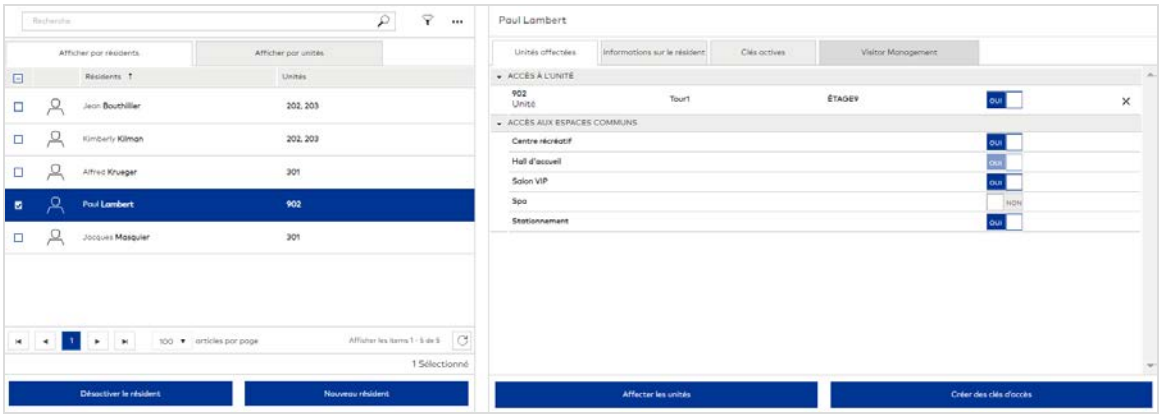
5. Cliquez sur **Nouveau résident**.



6. Indiquez le nom et le prénom du résident et, si vous remettez une clé mobile, le numéro de téléphone portable complet, y compris les codes pays et région.
7. Cliquez sur **Sauvegarder**.



8. Lorsque vous êtes informé des clés que vous devez créer, cliquez sur **OK**. Vous pouvez ouvrir le profil du nouveau résident pour vérifier que l'unité a été affectée ou pour modifier l'accès dans le profil.



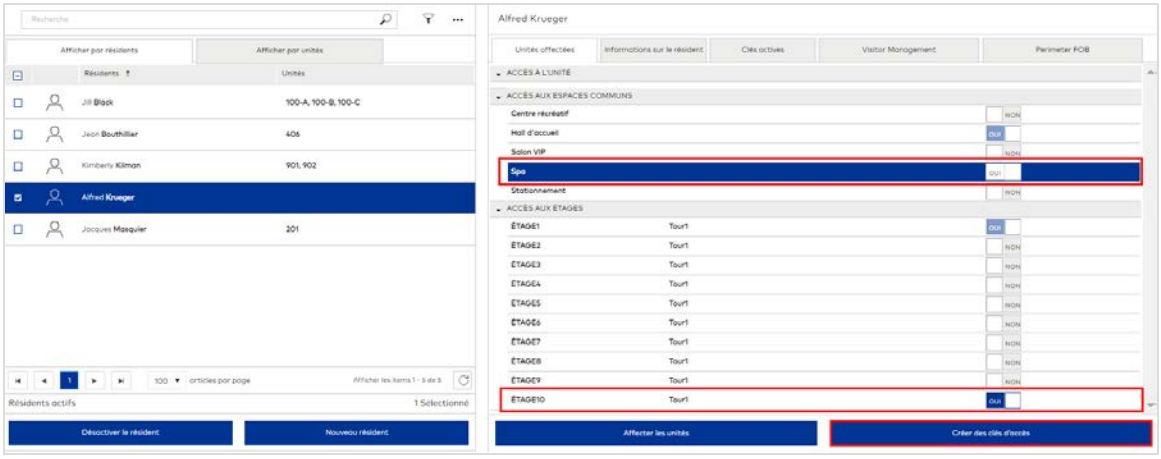
Créer des clés de résidents

Les clés de résidents sont créées et remises aux résidents pour permettre l'accès aux unités affectées et aux espaces communs pour les résidents. Si au moins une unité est affectée, vous pouvez créer des clés de résidents à partir des onglets **Afficher par résidents** et **Afficher par unités**. Si vous créez une clé pour les espaces communs uniquement, vous devez utiliser l'onglet **Afficher par résidents**.

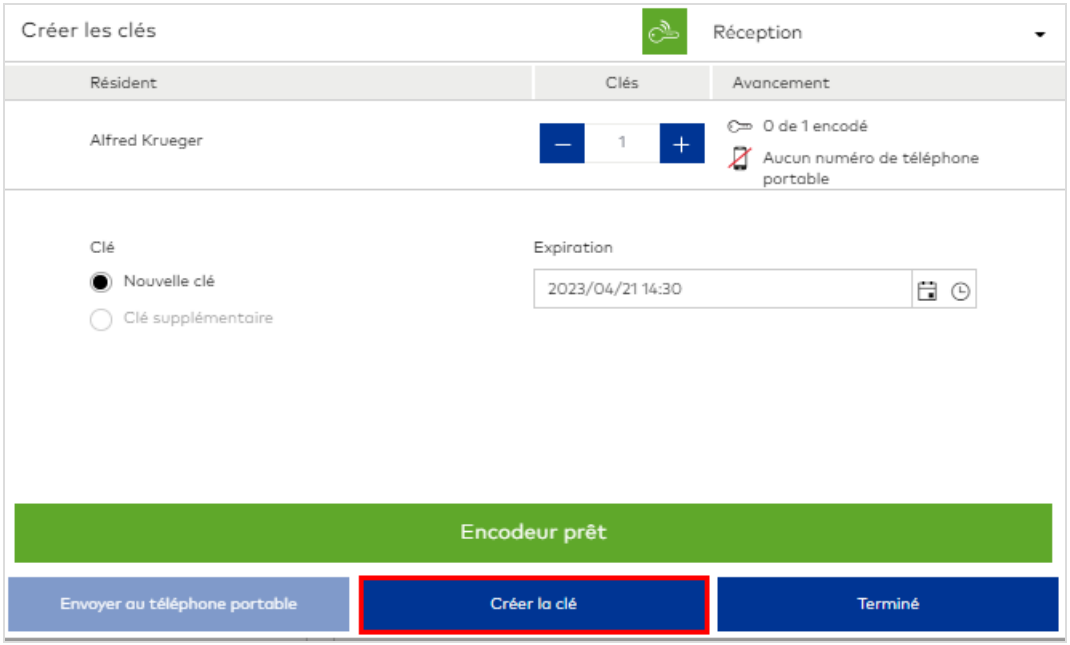
Afficher par résidents

Pour créer des clés de résidents :

1. Accédez à **Gestion des résidents**.
2. Sélectionnez un résident.



3. Cliquez sur **Créer des clés d'accès**.



4. Indiquez le nombre de clés à créer. Si vous créez une clé mobile, sélectionnez **1**.

5. Sélectionnez un mode de la clé. S'il n'y a pas de clé active pour la ou les unités sélectionnées, une **Nouvelle clé** est nécessaire. Si une clé active existe, la création d'une nouvelle clé invalide l'identifiant sélectionné sur toutes les clés actives. La création de clés supplémentaires (copies) n'a pas d'effet sur les clés actives existantes.
6. (*en option*) Spécifiez une date et une heure après lesquelles la clé sera invalide.
7. Sélectionnez si vous souhaitez encoder l'option de désactivation sur les clés de résidents. Cette option n'est disponible que si elle est activée dans ***Paramètres du système > Sécurité > Accès aux serrures > Options RAC5***.
8. Sélectionnez un encodeur en ligne, cliquez sur **Créer la clé** puis présentez les clés à l'encodeur (selon les instructions).

Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

9. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

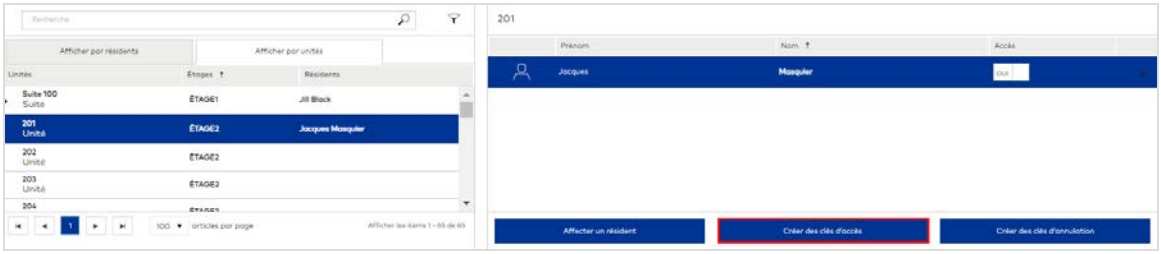


Pour les clés mobiles, vous pouvez cliquer sur l'onglet **Clés actives** dans le profil du résident pour vérifier que la clé a été livrée.

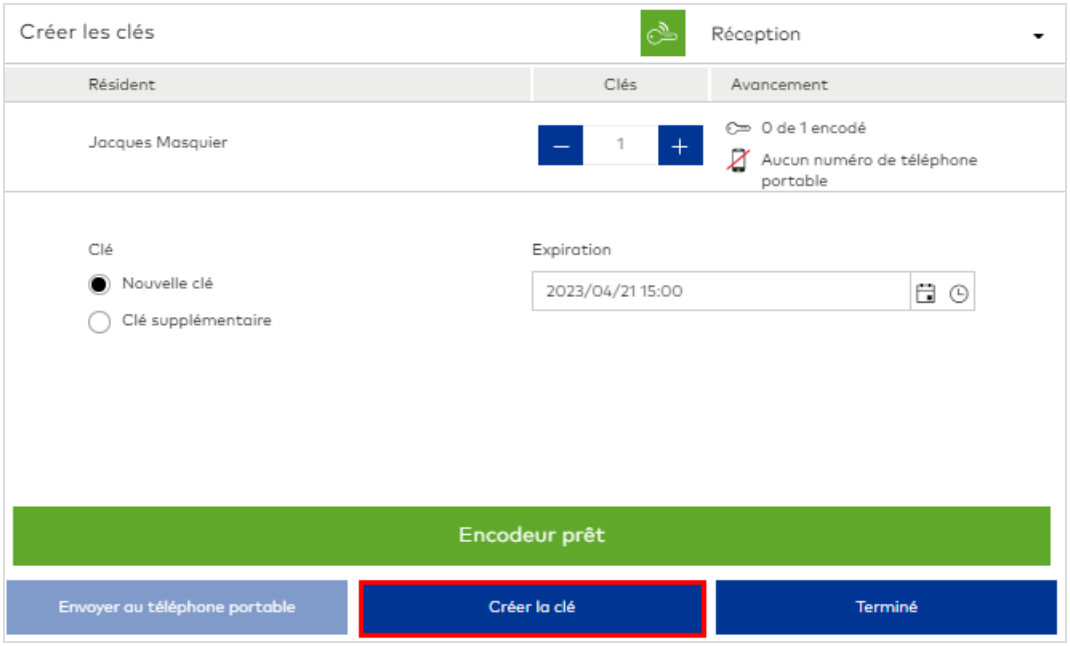
Afficher par unités

Pour créer des clés de résidents

1. Accédez à **Gestion des résidents**.



2. Cliquez sur l'onglet **Afficher par unités**.
3. Sélectionnez une unité.
4. Sélectionnez un résident.
5. Cliquez sur **Créer des clés d'accès**.



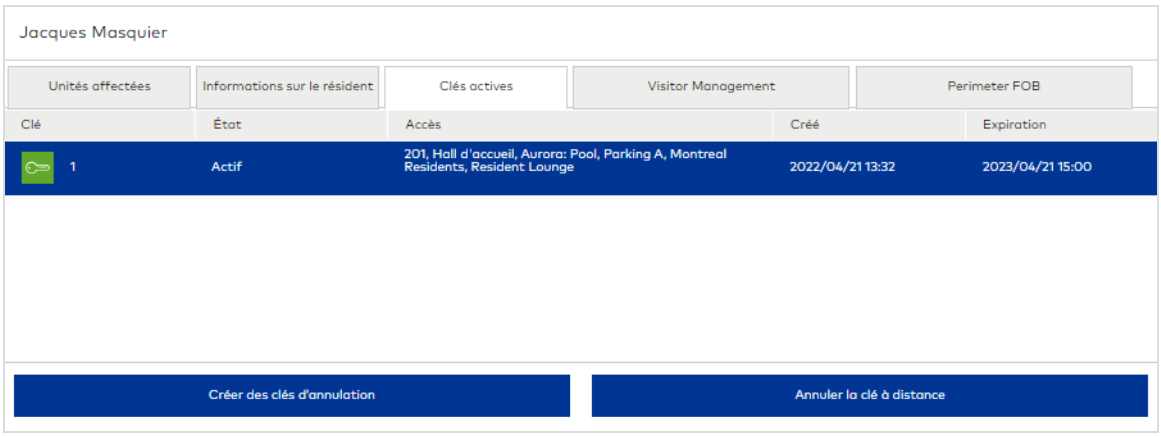
6. Indiquez le nombre de clés à créer.

Pour les clés mobiles, sélectionnez 1.

7. Sélectionnez un mode de la clé. S'il n'y a pas de clé active pour la ou les unités sélectionnées, une **Nouvelle clé** est nécessaire. Si une clé active existe, la création d'une nouvelle clé invalide l'identifiant sélectionné sur toutes les clés actives. La création de clés supplémentaires (copies) n'a pas d'effet sur les clés actives existantes.
8. (*en option*) Spécifiez une date et une heure après lesquelles la clé sera invalide.
9. Sélectionnez si vous souhaitez encoder l'option de désactivation sur les clés de résidents. Cette option n'est disponible que si elle est activée dans ***Paramètres du système > Sécurité > Accès aux serrures > Options RAC5***.
10. Sélectionnez un encodeur en ligne, cliquez sur **Créer la clé** puis présentez les clés à l'encodeur (selon les instructions).

Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

11. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.



Pour les clés mobiles, vous pouvez cliquer sur l'onglet **Clés actives** dans le profil du résident pour vérifier que la clé a été livrée.

Modifier l'accès résident

L'accès résident peut être modifié en activant ou en désactivant l'accès aux unités, aux espaces communs et aux étages qui leur sont affectés, ou en supprimant l'accès aux unités affectées.

Activation/désactivation de l'accès aux unités affectées

Vous pouvez activer et désactiver l'accès résident à partir des onglets **Afficher par résidents** et **Afficher par unités**.

À chaque fois qu'une modification de l'accès est effectuée, Community affiche un message qui répertorie les noms des résidents pour lesquels des clés doivent être créées. Si ces messages ne s'affichent pas, mettez l'option **Afficher les messages d'avertissement de la clé** dans ***Paramètres du système > Résident*** sur **OUI**.

Afficher par résidents

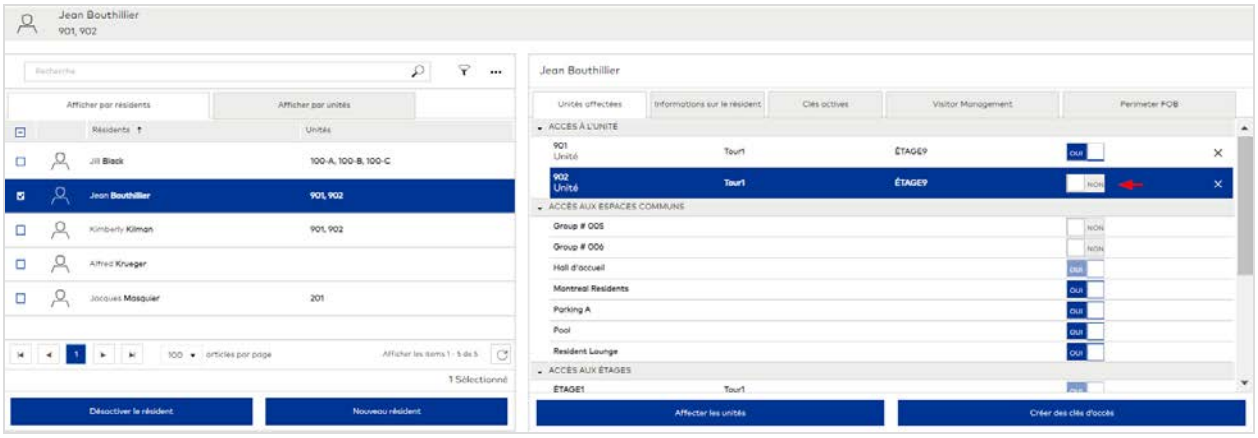
L'onglet **Unités affectées** du profil de résident répertorie toutes les unités affectées au résident, de tous les espaces communs et de tous les étages (pour l'accès aux ascenseurs) dans chacun des bâtiments où le résident a accès à une unité ou à un espace commun.

L'accès aux unités individuelles, aux espaces communs et aux étages peut être activé ou désactivé dans la section correspondante du profil (**ACCÈS À L'UNITÉ**, **ACCÈS AUX ESPACES COMMUNS**, **ACCÈS AUX ÉTAGES**).

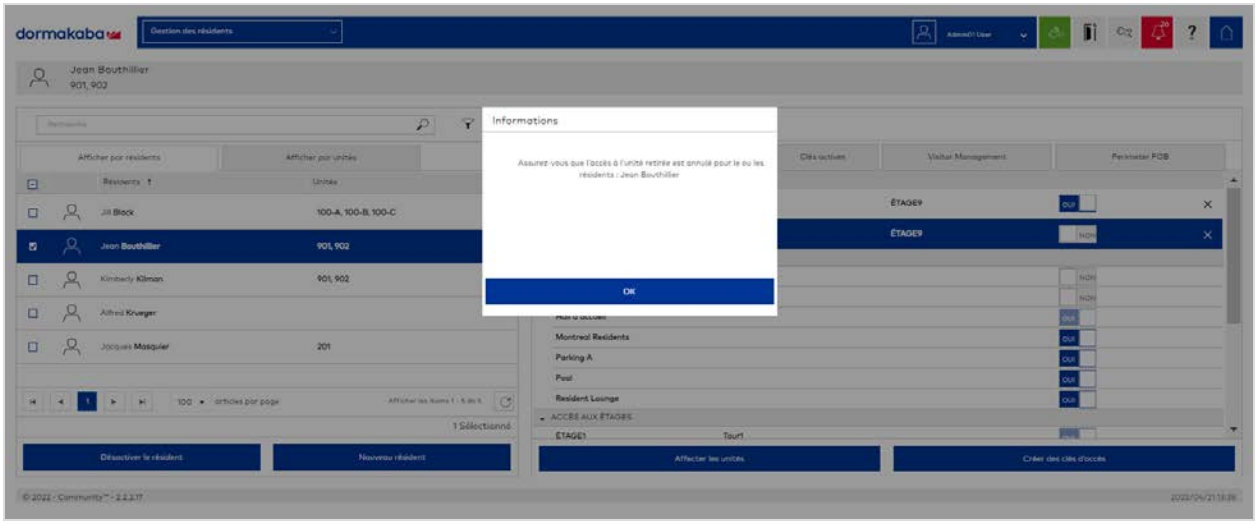
1. Accédez à **Gestion des résidents**.
2. Sélectionnez un résident.
3. Dans l'onglet **Unités affectées** :
   - Pour activer l'accès, déplacez le commutateur Accès sur **OUI**.
   - Pour désactiver l'accès, déplacez le commutateur Accès sur **NON**.

Section ACCÈS À L'UNITÉ

Lorsque vous permettez l'accès à une unité, l'accès est également permis à l'étage où se situe cette unité. De plus, les espaces communs restreints activés par défaut dans le profil d'accès aux espaces communs pour les résidents associé à l'unité sont activés.



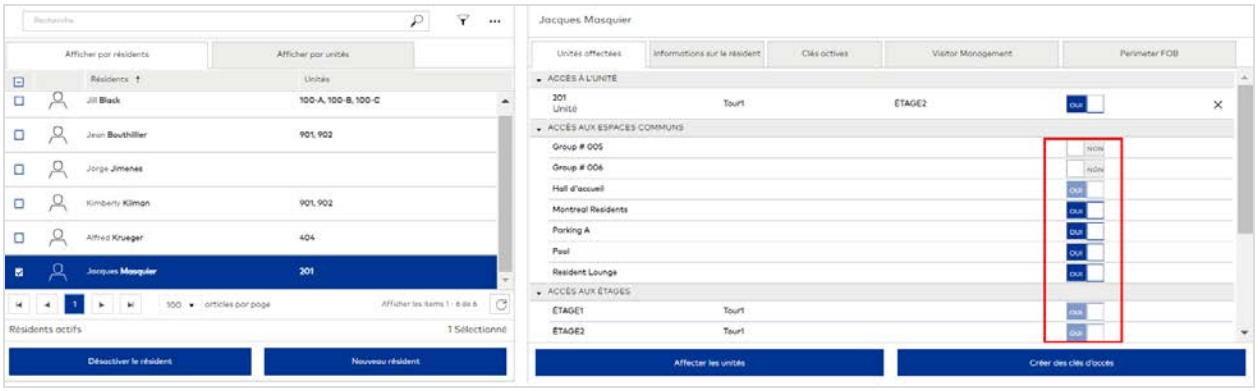
Lorsque vous désactivez l'accès à une unité, l'accès à l'étage où se trouve l'unité est désactivé (si le résident n'a pas accès à d'autres unités ou espaces communs du même étage). L'accès aux espaces communs restreints associés exclusivement à l'unité dans le profil d'accès aux espaces communs pour les résidents est désactivé. Community vous informe de toutes les clés que vous devez créer pour les résidents concernés.



Après avoir désactivé l'accès, le commutateur Accès est réglé sur **NON**.

Section ACCÈS AUX ESPACES COMMUNS

Si aucune unité n'est affectée à un résident, tous les espaces communs sont répertoriés. Les espaces communs illimités sont activés et ne peuvent pas être désactivés. Les espaces communs restreints sont désactivés par défaut mais peuvent être activés.

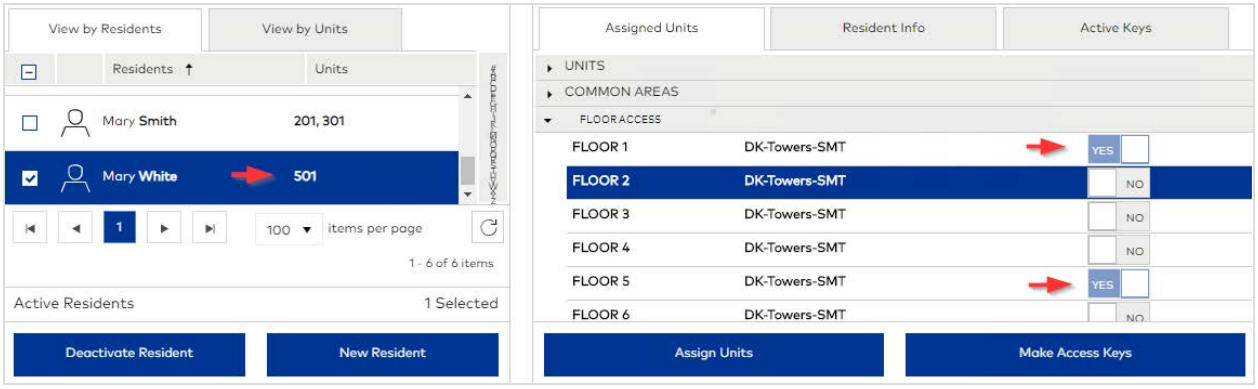


Lorsqu'au moins une unité est affectée à un résident, tous les espaces communs illimités restent activés. Les espaces communs restreints activés sont ceux dont l'accès est activé par défaut dans le profil d'accès aux espaces communs pour les résidents et tous les espaces communs sélectionnés avant l'affectation d'une unité.

Section ACCÈS AUX ÉTAGES

Cette section ne s'affiche que lorsque l'option **Afficher l'accès aux étages** est réglée sur **OUI** dans ***Paramètres du système > Résident***.

Tous les étages pour les bâtiments dans lesquels un résident a accès à une unité ou à un espace commun sont affichés dans la liste **ACCÈS AUX ÉTAGES**. Par défaut, l'accès aux étages est autorisé pour les étages sur lesquels le résident peut accéder à une unité ou à un espace commun. Pour tous les autres étages, l'accès est désactivé par défaut.



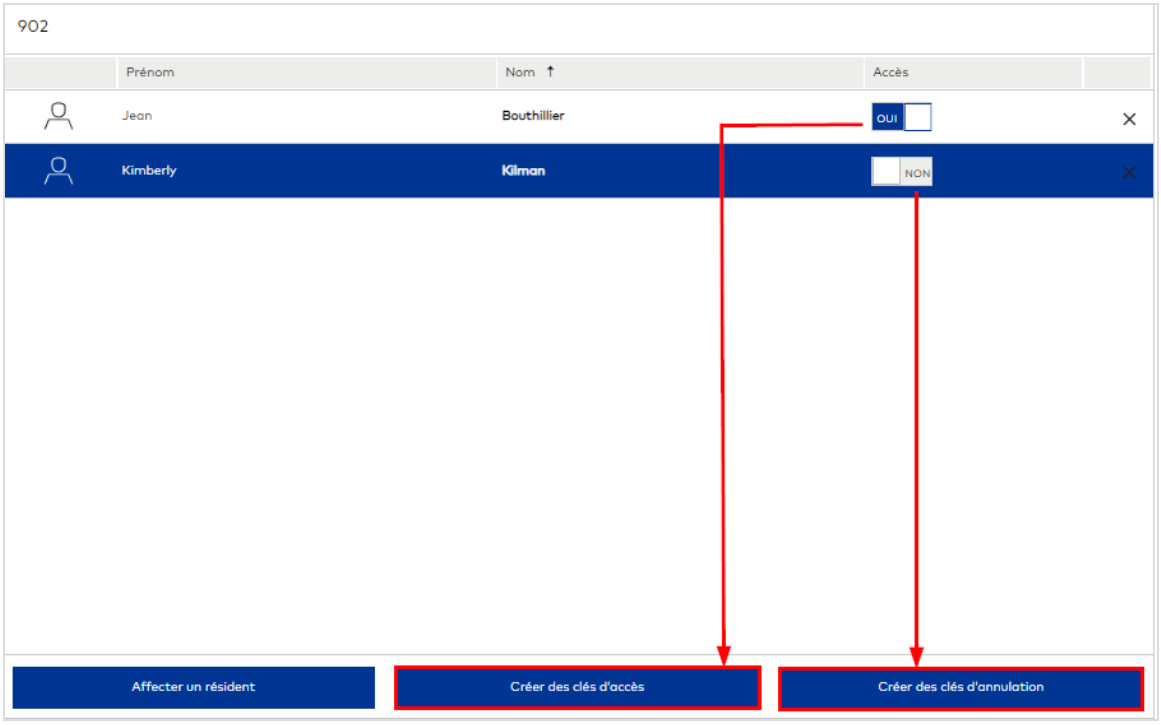
Afficher par unités

Lorsqu'une unité occupée est sélectionnée, vous pouvez activer et désactiver l'accès résident à cette unité.

1. Accédez à **Gestion des résidents**.



2. Cliquez sur l'onglet **Afficher par unités**.
3. Sélectionnez une unité.
4. Pour le(s) résident(s) dont vous souhaitez modifier l'accès :
   - Pour activer l'accès, déplacez le commutateur Accès sur **OUI**. L'unité et tous les espaces communs associés de manière unique avec l'unité sont autorisés. Vous devez créer des clés d'accès pour tout résident dont l'accès a été activé.
   - Pour désactiver l'accès, déplacez le commutateur Accès sur **NON**. L'unité reste dans le profil, mais l'accès à l'unité et aux espaces communs associés de manière unique est refusé. Vous devez créer des clés d'accès pour tout résident dont l'accès a été désactivé.



Désaffectation d'unités

La suppression d'une unité du profil d'un résident supprime l'accès à l'unité et à tous les espaces communs associés exclusivement à l'unité. Si l'unité est partagée avec d'autres résidents, l'unité est également supprimée de leurs profils. Une alternative à la suppression d'une unité d'un profil de résident consiste à désactiver l'accès à l'unité.

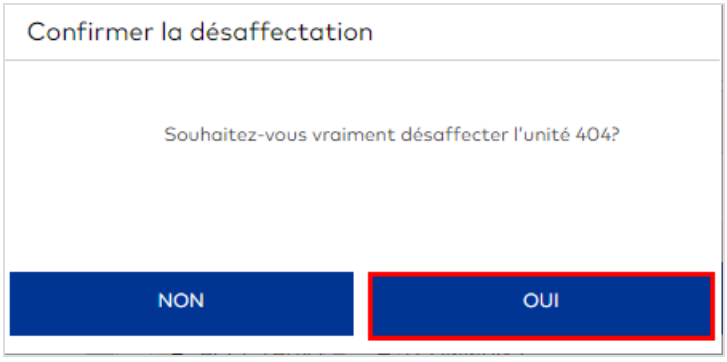
Vous pouvez supprimer l'accès résident à partir des onglets **Afficher par résidents** et **Afficher par unités**.

Afficher par résidents

1. Accédez à **Gestion des résidents**.



2. Sélectionnez un résident.
3. Dans la section **ACCÈS À L'UNITÉ**, cliquez sur **(Supprimer)** ✕ dans la ligne **Unité** .

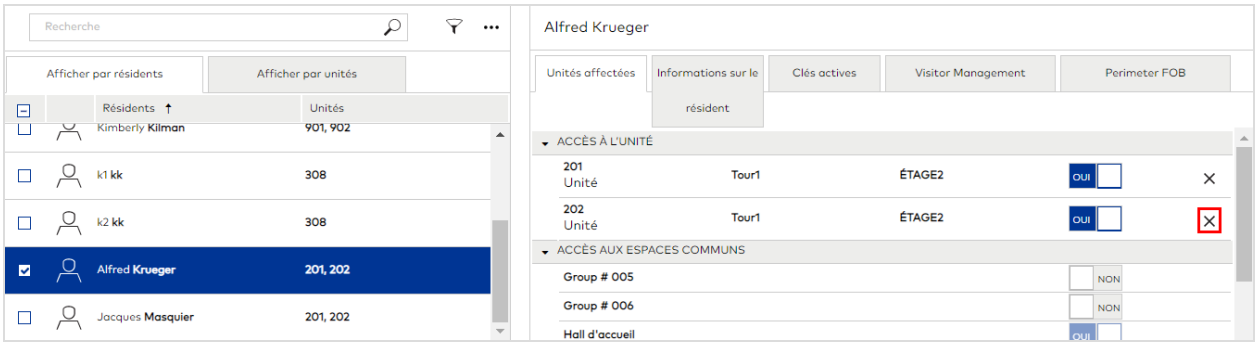


4. Cliquez sur **OUI** pour confirmer.

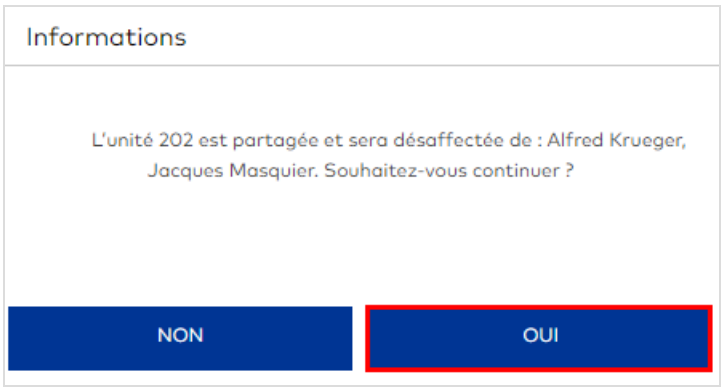
Suppression de l'accès lorsque des résidents partagent l'accès

Lorsque l'accès à une unité est retiré à un résident qui partage l'accès, l'unité est également retirée pour tous les résidents qui partagent l'accès.

La figure suivante montre que l'unité 202 sera supprimée du profil de résident de Jean.



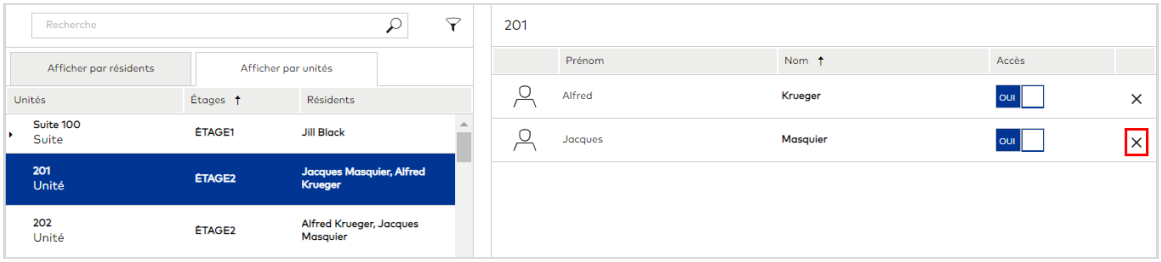
Lorsque vous choisissez de retirer l'unité 202 du profil de Jean, Community vous informe des résidents concernés.



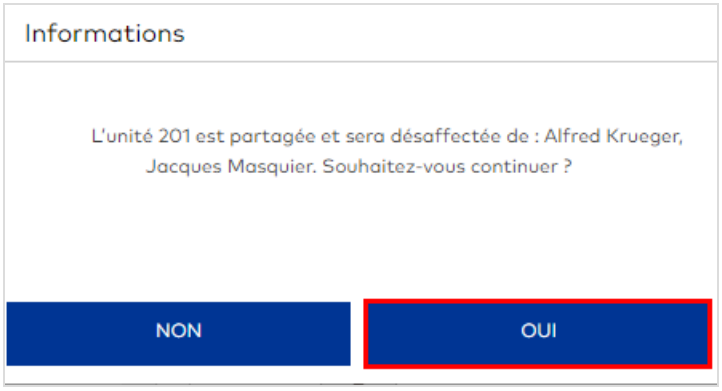
Le message suivant s'affiche.

Afficher par unités

1. Accédez à **Gestion des résidents**.



2. Cliquez sur l'onglet **Afficher par unités**.
3. Sélectionnez une unité.
4. Pour le résident dont vous souhaitez supprimer l'accès, cliquez sur **(Supprimer)** ✕ .



5. Cliquez sur **OUI** pour confirmer.

Invalider l'accès des résidents

Il existe de nombreuses options pour invalider l'accès des résidents avant que la ou les clés arrivent à expiration. La meilleure méthode dépend des modules Community autorisés pour votre compte Opérateur et de la raison pour laquelle vous voulez invalider l'accès.

Voici la situation ...

Trouvez la situation qui vous convient le mieux et examinez l'option recommandée.

Un résident est parti définitivement.	**Créez des clés d'annulation et désactivez le résident** Créez une clé d'annulation pour chaque clé active attribuée au résident, puis désactivez le résident. Vous pouvez éventuellement supprimer le résident après sa désactivation.
Un résident est parti temporairement.	**Créer des clés de blocage OU clés d'annulation** ❑ Si le résident doit retourner dans la même unité assignée, faites des clés de blocage pour suspendre temporairement l'accès. ❑ Si le résident sera assigné à une autre unité, faites les clés d'annulation.
Une clé de résident a été perdue ou volée	**Créer de nouvelles clés ou créer des clés d'annulation** ❑ Si le résident ne partage pas l'accès, créez de nouvelles clés pour le résident. Les nouvelles clés invalident automatiquement les clés précédemment actives. ❑ Si le résident partage l'accès, vous pouvez soit créer de nouvelles clés pour un résident et des clés supplémentaires pour tous les autres résidents qui partagent l'accès, soit créer une clé d'annulation pour la clé perdue puis créer une clé supplémentaire pour le résident.
Vous devez empêcher temporairement tous les résidents d'entrer dans l'une des unités affectées.	**Créer des clés de blocage** Invalide toutes les clés de résident pour la porte de la unité/suite sélectionnée. Si l'intention est de suspendre temporairement l'accès, vous pouvez alors créer des clés de déblocage pour rétablir l'accès.
Vous devez empêcher de façon permanente tous les résidents d'entrer dans une ou plusieurs des unités qui leur sont attribuées.	**Créer des clés d'annulation** Invalide l'accès pour les résidents actuels.
Vous souhaitez annuler l'accès pour un ou plusieurs résidents et réaffecter l'unité/les unités à un autre résident.	**Créer de nouvelles clés** Les nouvelles clés invalident toutes les clés précédemment actives. La création de nouvelles clés vous permet de sauter l'étape d'annulation des clés des résidents d'origine.

N'oubliez pas que l'accès reste valide jusqu'à ce que les clés d'annulation/de blocage/nouvelles clés soient présentées aux serrures.

Outre l'invalidation de l'accès des résidents aux unités, il existe des cas particuliers à prendre en compte.

Annulation de l'accès des résidents aux espaces communs

invalider l'accès aux espaces communs résident sans annuler l'accès du résident aux unités affectées.

Vous souhaitez annuler l'accès d'un résident à un espace commun résident. → Créer des clés d'annulation ou de nouvelles clés

- ❑ Créez une clé d'annulation pour chaque clé active attribuée au résident, puis présentez-la à tout espace commun résident dont vous souhaitez invalider l'accès.
- ❑ Créez une nouvelle clé pour la même affectation d'unité, puis présentez-la à tout espace commun résident dont vous souhaitez invalider l'accès.

Invalidation de l'accès par clé mobile

L'invalidation de l'accès lorsqu'un résident utilise une clé mobile est similaire au processus applicable aux clés physiques.

Vous souhaitez invalider l'accès d'un résident qui possède une clé mobile → Créer des clés d'annulation

Créez une clé d'annulation pour chaque clé mobile active attribuée au résident.

- ❑ Si l'option Activer l'annulation de la clé mobile résident est positionnée sur OUI dans Paramètres du système > Avancés, cliquez sur Envoyer au téléphone portable lorsque vous y êtes invité. Community envoie la commande de suppression de la clé depuis l'application dormakaba BlueSky.
- ❑ Dans tous les autres cas, présentez la clé d'annulation à tous les points d'accès que la clé a autorisés.

Invalidation de l'accès à Keyscan Aurora

Il existe plusieurs façons d'invalider l'accès lorsque Keyscan Aurora est activé

Keyscan Aurora est activé et vous souhaitez invalider l'accès d'un résident → Créer des clés d'annulation/de blocage/des nouvelles clés ou désactiver le résident

Il vous suffit d'encoder l'un de ces types de clés ou de désactiver le résident. Vous n'avez pas besoin de présenter une clé à une serrure Community. Le serveur Aurora communique avec le lecteur Keyscan pour invalider l'accès. La désactivation d'un résident invalide également l'accès automatiquement.

Invalidation de l'accès – Communication en ligne

L'invalidation de l'accès résident, lorsque la communication en ligne est activée, ne nécessite pas de clés physiques.

Vous souhaitez invalider l'accès d'un résident qui part avant l'expiration de sa ou ses clés → Désactiver le résident

Dans la Gestion des résidents, sélectionnez le résident et cliquez sur Désactiver le résident.

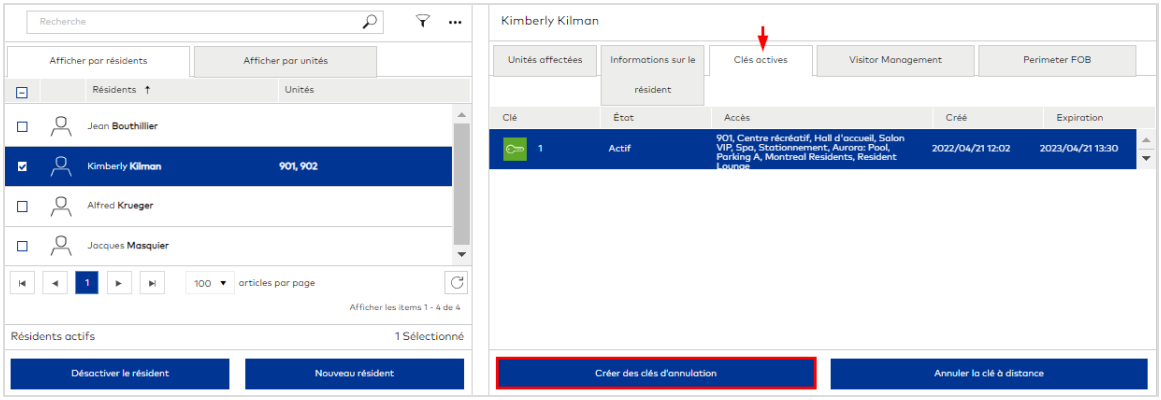
- ❑ Toutes les unités et espaces communs affectés sont supprimés du profil et toutes les clés actives sont annulées. En option, vous pouvez supprimer le résident désactivé.
- ❑ L'accès est également supprimé pour tous les résidents qui partagent l'accès avec le résident désactivé.

Créer des clés d'annulation

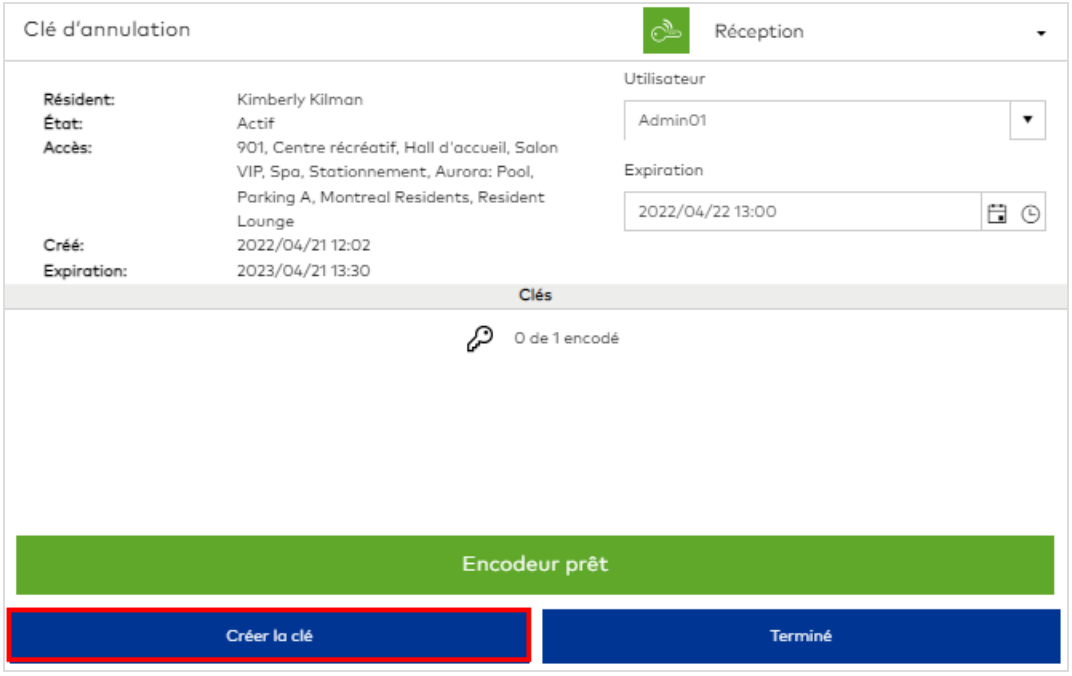
Les clés d'annulation invalident de façon permanente une instance de clé unique et spécifique. Pour annuler des clés physiques, créez une Clé d'annulation physique et présentez la Clé d'annulation à chaque point d'accès autorisé sur la clé d'accès. Pour annuler des clés mobiles, vous pouvez annuler la clé mobile à distance et/ou créer une Clé d'annulation physique.

L'annulation des clés mobiles résident à distance est une fonction sous licence qui doit être activée dans ***Paramètres du système > Avancés > Activer les clés mobiles > Activer l'annulation de la clé mobile résident***.

1. Accédez à **Gestion des résidents**.
2. Sélectionnez un résident.
3. Cliquez sur l'onglet **Clés actives**.



4. Sélectionnez la clé que vous souhaitez annuler.
5. Cliquez sur **Créer des clés d'annulation**.

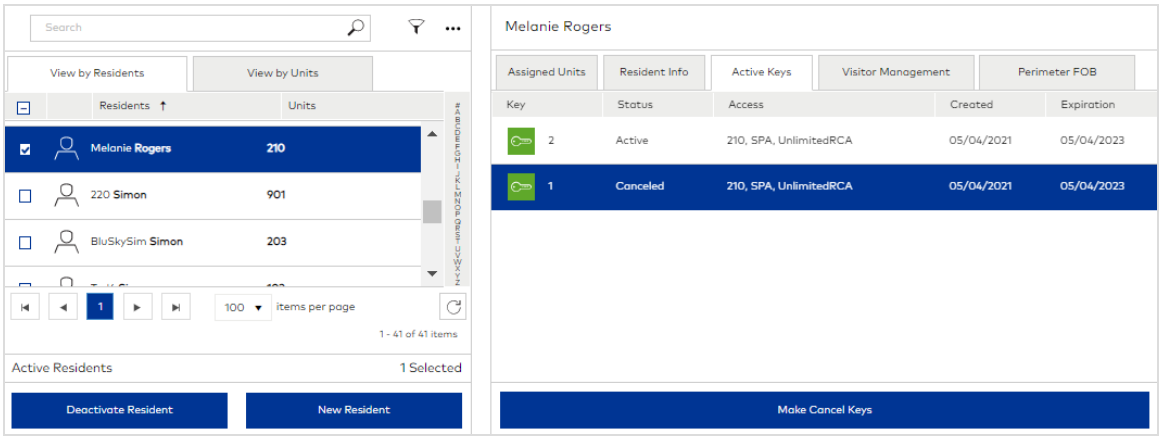


6. (*en option*) Sélectionnez le membre du personnel/prestataire à qui vous souhaitez affecter la Clé d'annulation.
7. (*en option*) Indiquez la date après laquelle la Clé d'annulation est invalide.

8. Sélectionnez un encodeur en ligne, cliquez sur **Créer la clé**, puis présentez une clé à l'encodeur.

Si vous annulez une clé mobile, cliquez sur **Créer la clé** pour créer une Clé d'annulation physique et/ou cliquez sur **Annuler la clé mobile** pour annuler la clé mobile à distance. Les Clés d'annulation physiques doivent être présentées aux points d'accès pour invalider une clé mobile.

9. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**. Vous devez présenter la clé d'annulation aux points d'accès concernés avant que l'accès ne soit annulé.



Bien qu'il soit possible de créer une Clé d'annulation pour annuler une Clé de résident dans le module de **Gestion des résidents**, il n'est pas possible de créer une Clé d'annulation pour annuler une Clé de résident dans le module de **Clés Système**.

Désactiver les résidents

La désactivation d'un résident fonctionne différemment dans les environnements hors ligne et en ligne.

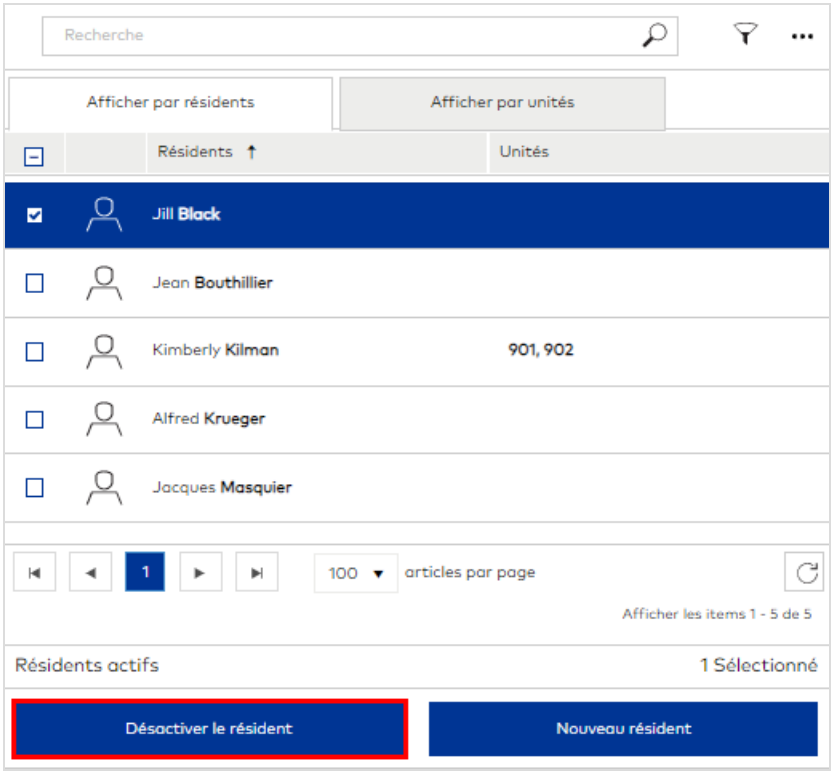
- Dans les environnements hors ligne, vous devez d'abord désaffecter toutes les unités du résident, créer et présenter les clés d'annulation aux serrures concernées, puis désactiver le résident.
- Dans les environnements en ligne, les clés d'annulation sont automatiquement créées et envoyées aux serrures concernées, toutes les affectations d'unités et les clés actives attribuées au résident sont supprimées du profil du résident et le résident n'est plus répertorié dans l'onglet **Afficher par résidents** .

  Si Gestion des visiteurs est activée, tous les codes PIN et clés mobiles attribués actifs sont définitivement annulés.

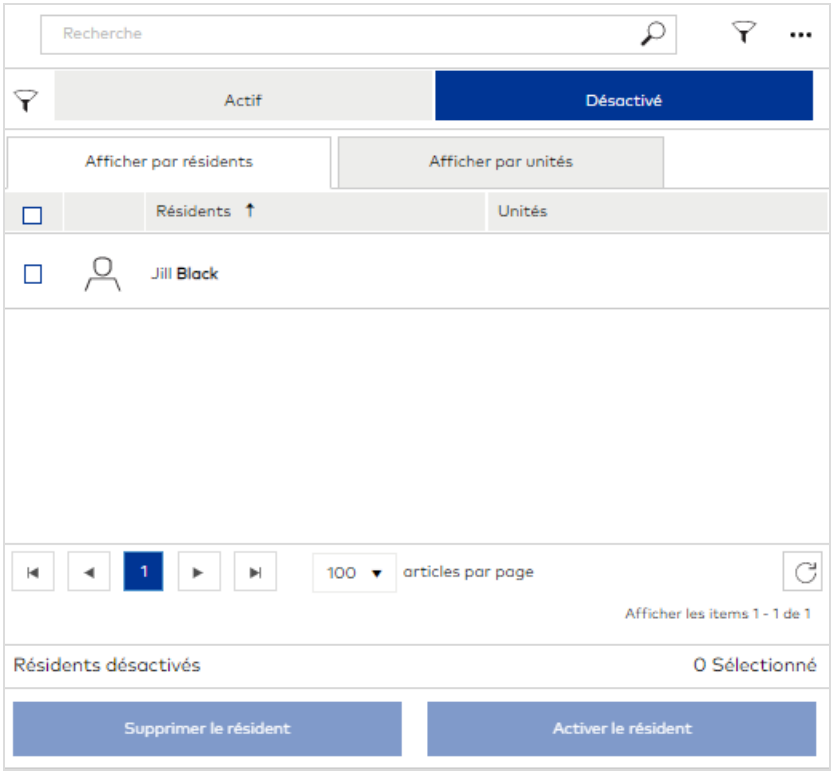
  Vous pouvez supprimer ou (ré)activer un résident qui a été désactivé.

Lorsque la communication en ligne est activée, l'accès est également supprimé pour tous les résidents qui partagent l'accès avec le résident désactivé.

1. Accédez à **Gestion des résidents**.



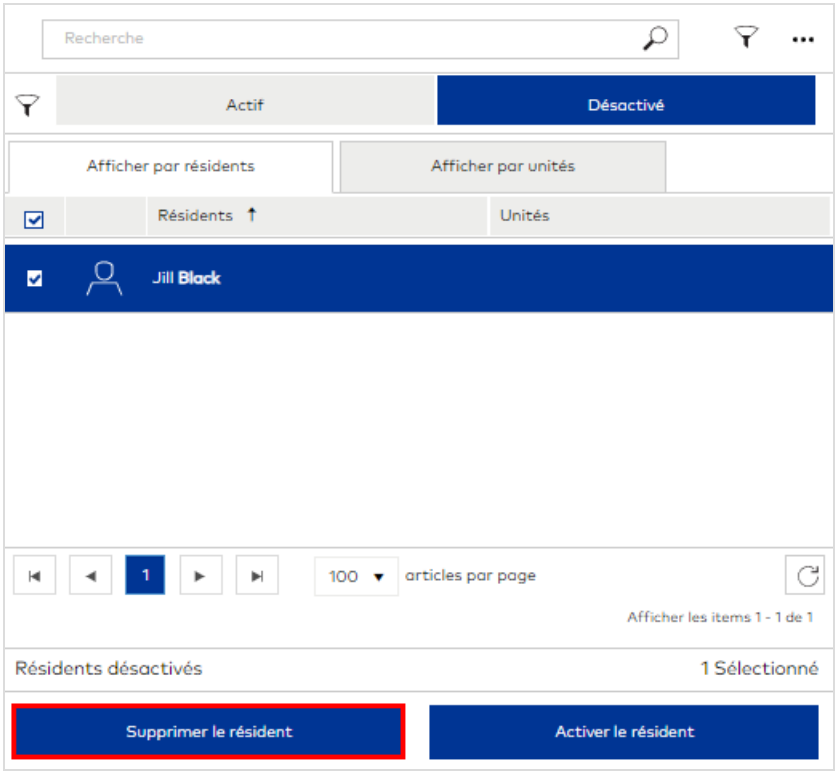
2. Sélectionner un ou plusieurs résidents.
3. Cliquez sur **Désactiver le résident**.
4. Cliquez sur **OUI** pour confirmer. Vous pouvez vérifier que le résident a été désactivé en cliquant sur **(Filtrer)** et en sélectionnant l'onglet **Désactivé** . Le nom du résident est répertorié et le profil montre que l'affectation d'unités et les clés actives ont été supprimées.



Supprimer des résidents

Vous ne pouvez supprimer que les résidents qui ont été désactivés.

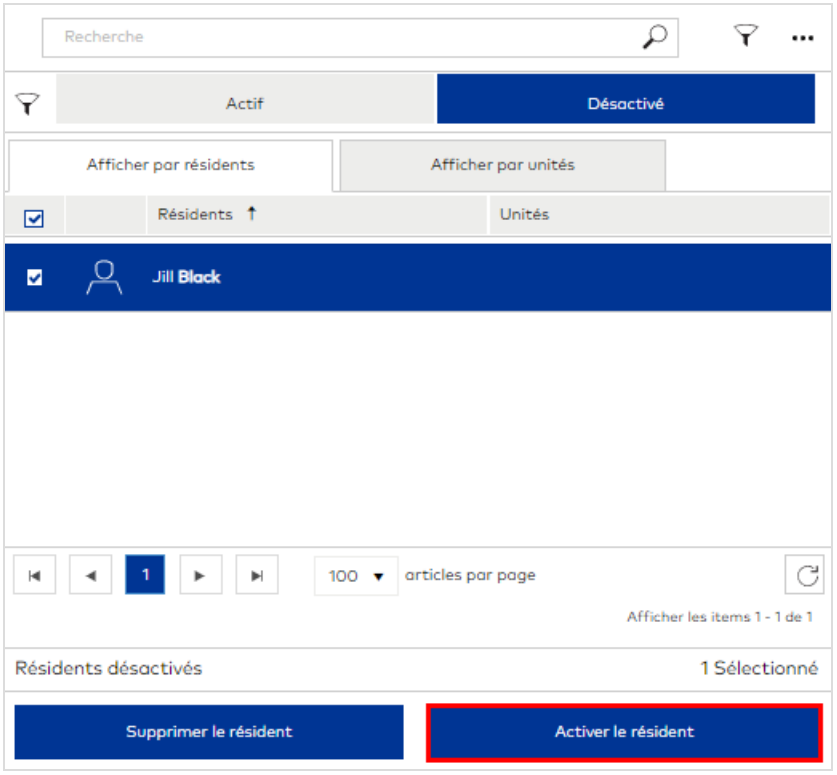
1. Accédez à **Gestion des résidents**.



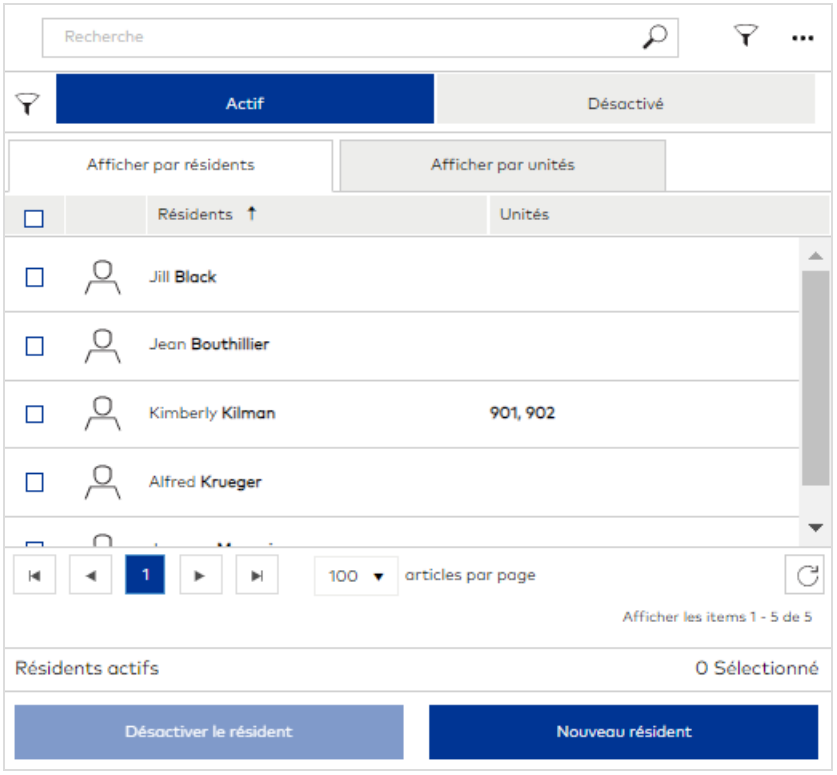
2. Après l'affichage des options (Filtrer) , cliquez sur l'onglet **Désactivé** .
3. Sélectionner un ou plusieurs résidents.
4. Cliquez sur **Supprimer le résident**.
5. Cliquez sur **OUI** pour confirmer.

Activer les résidents

1. Accédez à **Gestion des résidents**.



2. Après l'affichage des options (Filtrer) , cliquez sur l'onglet **Désactivé**.
3. Sélectionner un ou plusieurs résidents.
4. Cliquez sur **Activer le résident**.
5. Cliquez sur **OUI** pour confirmer. Vous pouvez vérifier que le ou les résidents sont activés en cliquant sur l'onglet **Activé** ou en fermant les options de filtre et en recherchant le ou les résidents dans l'onglet **Afficher par résidents**. Une fois les résidents activés, vous pouvez affecter les unités et créer des clés de résidents.



Créer de nouvelles clés

La création d'une nouvelle clé invalide automatiquement l'accès à l'identifiant sélectionné sur toutes les clés précédemment actives. Par exemple, la NouvelleClé1 pour les unités 100 et 101 expire demain à 13 heures. Si vous créez une NouvelleClé2 pour l'unité 100, NouvelleClé1 devient invalide pour l'unité 100 dès que vous présentez NouvelleClé2 à la serrure installée pour l'unité 100. NouvelleClé1 ne reste valide que pour l'unité 101. Pour les instructions, voir Créer des clés de résidents.

Créer des clés de blocage

Les clés de blocage invalident toutes les instances d'un identifiant spécifique. Bien que vous puissiez utiliser la clé de blocage pour invalider l'accès de manière permanente, la clé de blocage est associée à la clé de déblocage pour suspendre puis rétablir l'accès. Par exemple, créez une clé de blocage pour l'unité 100 afin de suspendre tout accès, puis créez une clé de déblocage pour l'unité 100 afin de rétablir l'accès pour toutes les clés actives.

Lorsque vous créez une clé de blocage pour invalider l'accès d'un résident, la catégorie d'identifiants que vous sélectionnez est *Résident*. L'identifiant que vous sélectionnez est l'unité/unité de suite que vous souhaitez bloquer.

Après avoir bloqué l'accès, la clé de déblocage ne débloque pas l'accès aux espaces communs lorsque l'accès est basé sur un profil d'accès aux espaces communs.

Pour les instructions, voir Clés de blocage/déblocage.

Créer des clés d'annulation

Les clés d'annulation sont utilisées pour annuler définitivement l'accès d'un résident actuel. Le plus souvent, les clés d'annulation sont utilisées par le personnel après le départ d'un résident avant l'expiration de la clé. Les clés d'annulation invalident toutes les clés de résidents encodées avec accès à l'unité, même si le pêne dormant ou le verrou d'intimité est actionné.

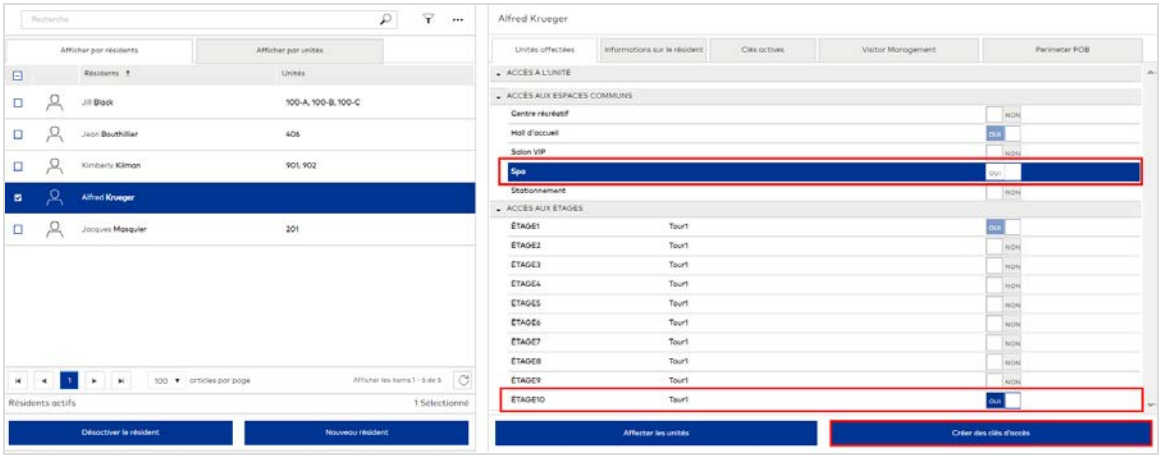
Les clés d'annulation n'invalident pas l'accès aux espaces communs et aux lecteurs d'ascenseurs.

Pour les instructions, voir Clés d'annulation.

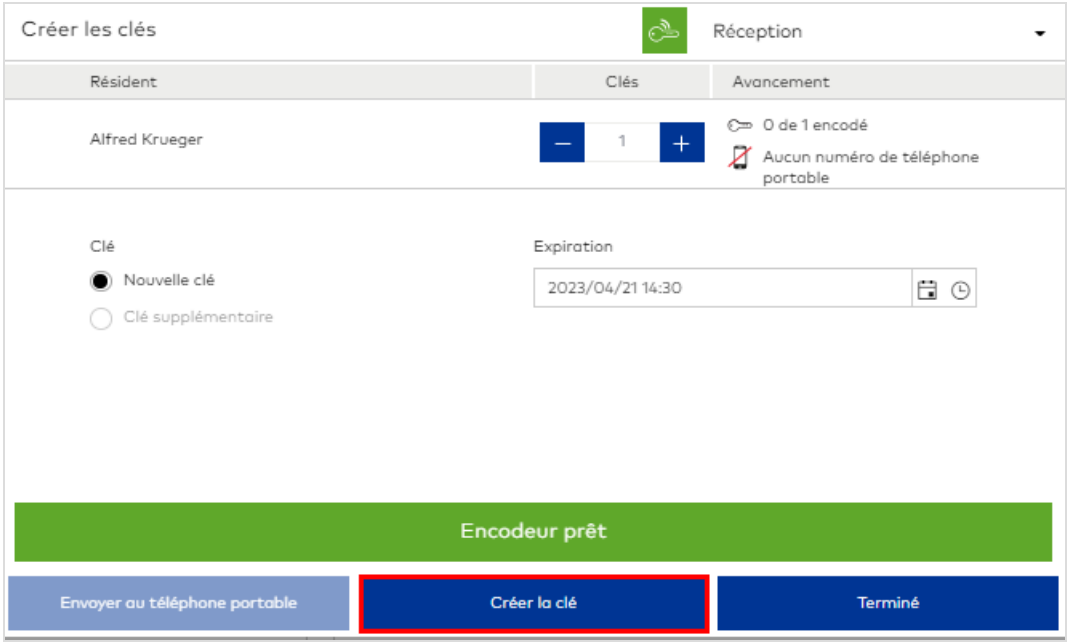
Créer des clés pour l'accès aux espaces communs uniquement

La fonction Community de création de clés d'accès aux espaces communs permet uniquement aux sites d'autoriser un accès spécial à des espaces communs restreints, comme un centre de remise en force, à des personnes qui ne séjournent pas sur le site. Bien que les clés soient remises à des non-résidents, vous devez quand même ajouter un profil de résident pour chaque porteur de clé.

1. Accédez à **Gestion des résidents**.
2. Sélectionnez (ou ajoutez) un résident. Pour ajouter un résident, cliquez sur **Nouveau résident**, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.



3. Dans la section **ACCÈS AUX ESPACES COMMUNS**, sélectionnez les espaces communs restreints que vous souhaitez activer. (Tous les espaces communs illimités sont activés par défaut et ne peuvent pas être désactivés).
4. Cliquez sur **Créer des clés d'accès**.



5. Indiquez le nombre de clés à créer. Si vous créez une clé mobile, sélectionnez **1**.

6. Sélectionnez un mode de la clé. S'il n'y a pas de clé active pour la ou les unités sélectionnées, une **Nouvelle clé** est nécessaire. Si une clé active existe, la création d'une nouvelle clé invalide l'identifiant sélectionné sur toutes les clés actives. La création de clés supplémentaires (copies) n'a pas d'effet sur les clés actives existantes.
7. (*en option*) Spécifiez une date et une heure après lesquelles la clé sera invalide.
8. Sélectionnez si vous souhaitez encoder l'option de désactivation sur les clés de résidents. Cette option n'est disponible que si elle est activée dans ***Paramètres du système > Gestion des résidents***.
9. Sélectionnez un encodeur en ligne, cliquez sur **Créer la clé** puis présentez les clés à l'encodeur (selon les instructions).

Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

10. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.



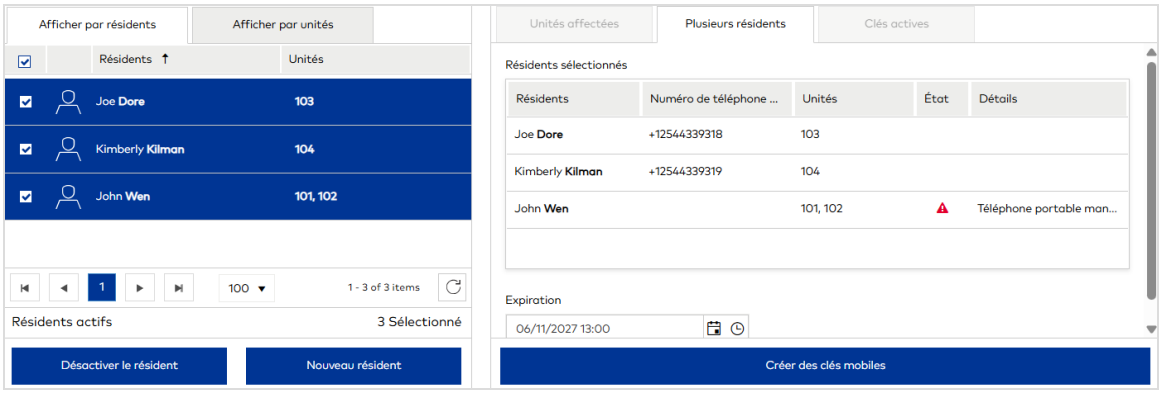
Pour les clés mobiles, vous pouvez cliquer sur l'onglet **Clés actives** dans le profil du résident pour vérifier que la clé a été livrée.

Créer des clés mobiles pour plusieurs résidents

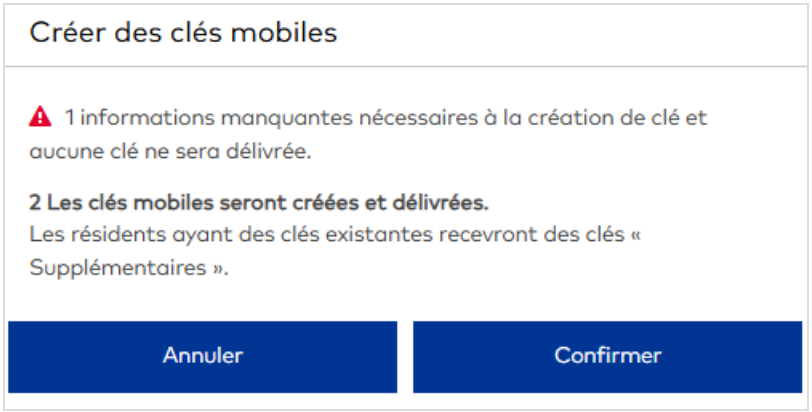
Créer des clés mobiles pour les résidents sélectionnés. Les conditions requises sont les suivantes :

- Un numéro de téléphone portable doit être renseigné dans le profil du résident.
- Au moins une unité doit être affectée au résident.

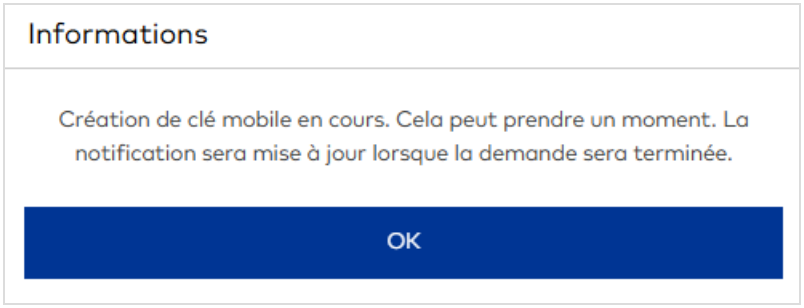
1. Accédez à **Gestion des résidents**.
2. Sélectionnez au moins deux résidents. Des avertissements s'affichent pour tout résident sélectionné dont le numéro de téléphone portable ou l'unité affectée est manquant.



3. Sélectionnez une date d'expiration pour toutes les clés mobiles.
4. Indiquez si l'option d'accessibilité doit être incluse. L'option d'accessibilité (configurée dans Paramètres système/Sécurité) prolonge la durée pendant laquelle une porte reste déverrouillée après la présentation d'une clé valide.
5. Cliquez sur **Créer des clés mobiles**.



6. Vérifiez les informations dans la boîte de dialogue de confirmation, puis cliquez sur **Confirmer**. La boîte de dialogue de confirmation indique le nombre total de clés qui seront créées et le nombre d'avertissements de demande de clé.



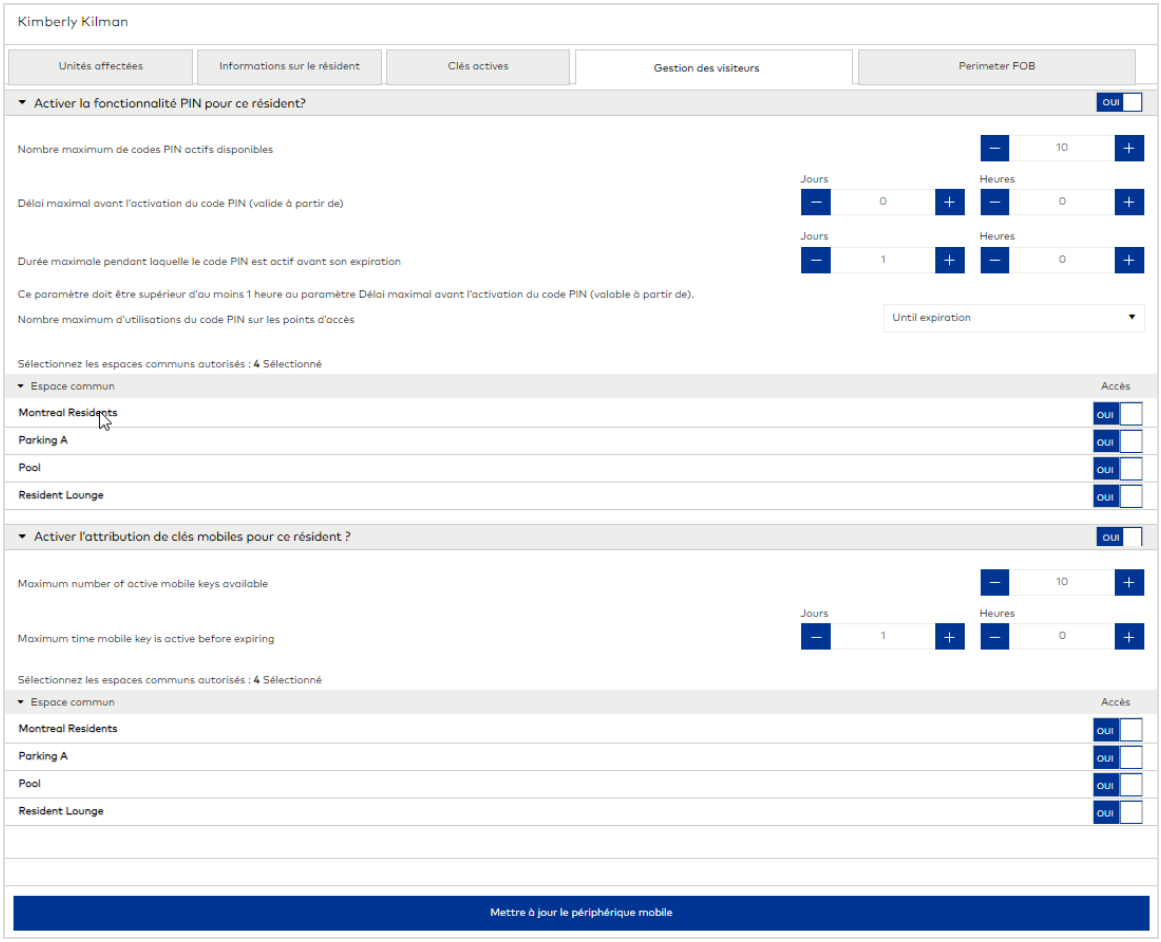
7. Cliquez sur **OK** lorsque vous êtes informé que la création des clés mobiles est en cours. Le nombre de clés demandées et les problèmes potentiels avec les téléphones portables des résidents ont une incidence sur le temps de traitement.

Configurer la gestion des visiteurs pour les résidents

Cet onglet s'affiche lorsque la fonction sous licence de gestion des visiteurs est activée.

Pour configurer l'attribution de codes PIN / clés mobiles pour un résident :

1. Accédez à **Gestion des résidents**.
2. Sélectionnez un résident.
3. Cliquez sur l'onglet **Gestion des visiteurs**.



4. Configurer les options d'attribution de codes PIN :
   - **Activer la fonctionnalité PIN pour ce résident** — Lorsque cette fonctionnalité est activée, la section PIN s'affiche, les paramètres PIN peuvent être personnalisés et mis à jour sur les périphériques mobiles.
   - **Nombre maximum de codes PIN actifs disponibles** — Indiquez le nombre maximum de codes PIN qui peuvent être actifs. Valeurs valides : 1-50.
   - **Délai maximal avant l'activation du code PIN (valide à partir de)** — Indiquez le nombre maximal de jours/heures pendant lesquels le résident peut créer un code PIN avant que l'accès autorisé par code PIN ne commence. Plage : 0-15 jours/0-23 heures.
   - **Durée maximale pendant laquelle le code PIN est actif avant d'expirer** — Indiquez le nombre maximal de jours/heures pendant lesquels un code PIN peut être actif. Plage : 0-15 jours/0-23 heures.

- **Nombre maximum de fois que le code PIN peut être utilisé dans les points d'accès** — Indiquez le nombre maximum de fois qu'un code PIN peut être utilisé dans les points d'accès. Valeurs valides : Jusqu'à expiration, 1-5.
- **Espaces communs autorisés** — Sélectionnez les espaces communs à autoriser sur le code PIN. Au moins un espace commun doit être autorisé.

5. Configurer les options d'attribution de clés mobiles :
   - **Activer l'attribution de la clé mobile pour ce résident** — Lorsque cette fonctionnalité est activée, la section d'attribution de clés mobiles s'affiche, les paramètres peuvent être personnalisés et mis à jour sur les périphériques mobiles.
   - **Nombre maximum de clés mobiles actives disponibles** — Indiquez le nombre maximum de clés mobiles attribuées qui peuvent être actives pour le résident. Valeurs valides : 1-50.
   - **Durée maximale pendant laquelle la clé mobile est active avant d'expirer** — Indiquez le nombre maximal de jours/heures pendant lesquels une clé mobile attribuée peut être active. Plage : 0-15 jours/0-23 heures.
   - **Espaces communs autorisés** — Sélectionnez les espaces communs à autoriser sur la clé mobile attribuée. Au moins un espace commun doit être autorisé.
6. Pour mettre à jour les paramètres sur le périphérique mobile du résident, cliquez sur **Mettre à jour le périphérique mobile**.

Personnel

Gestion du personnel et des prestataires

Cette section comprend les sujets suivants :

En savoir plus sur la Gestion du personnel/prestataire et les Clés du personnel/prestataire 187

Ajouter des membres du personnel/prestataires 189

Importer la liste des membres du personnel/prestataires 191

Créer des clés d'urgence 193

Créer une clé du personnel (accès prédéfini) 196

Créer des clés du personnel (accès variable) 199

Créer des clés de prestataire 204

Créer des clés à usage restreint 208

Remplacer les clés du personnel/prestataire 212

Invalider l'accès du personnel/prestataire 214

Configurer la gestion des visiteurs pour les membres du personnel/prestataires 219

En savoir plus sur la Gestion du personnel/prestataire et les Clés du personnel/prestataire

Le personnel et les prestataires sont les porteurs de clés qui travaillent ou exécutent un service sur l'établissement. La majorité du personnel correspond aux personnes dont les droits sont restreints à l'utilisation des clés qui leur sont remises, par exemple le personnel chargé de la maintenance. Certains membres du personnel, toutefois, nécessitent un accès à Community. Le personnel qui a accès à Community est appelé *Opérateurs*.

Un membre du personnel est désigné comme Opérateur dans le profil du personnel. Le degré d'accès dépend du rôle de l'opérateur sélectionné. Par exemple, un opérateur ayant le rôle prédéfini d'*Administrateur* a accès à toutes les fonctions Community, tandis que les droits d'un opérateur ayant le rôle prédéfini d'*Agent de location* sont limités aux fonctions **Gestion des résidents** et **Lire la clé**.

Vous pouvez ajouter des membres du personnel/prestataires manuellement ou importer une liste.

Profils de personnel/prestataire

Lorsqu'un membre du personnel ou un prestataire est ajouté à Community, un profil est créé avec les onglets suivants :

- **Informations sur le personnel/prestataire** — Cet onglet permet de définir les informations d'identification de base sur les membres du personnel/prestataires et d'activer les notifications. L'option permettant de désigner le membre du personnel comme opérateur se trouve sur cet onglet.
- **Informations sur l'opérateur** — Cet onglet permet de configurer l'accès de l'opérateur. L'onglet n'est actif que si le membre du personnel est désigné comme Opérateur.
- **Clés attribuées** — Cet onglet répertorie les clés actives attribuées au membre du personnel/prestataire. Vous pouvez annuler et/ou remplacer des clés dans la liste.
- **Gestion des visiteurs** — Cet onglet permet d'activer et de configurer l'attribution du code PIN pour le membre du personnel/prestataire.

Pour consulter le profil d'un membre du personnel/prestataire :

» Accédez à **Gestion du personnel/prestataire** et sélectionner un membre du personnel/prestataire.

Vous pouvez filtrer la liste des profils en fonction de l'état (Actif/Désactivé/Opérateurs uniquement).

Importation de membres du personnel/prestataires

Si le droit *Importer une liste* est activé dans la **Gestion des rôles**, vous pouvez créer des profils de personnel/prestataire en important un fichier CSV qui contient des données de base (*prénom/nom/ID*). Toute information supplémentaire, y compris la possibilité de désigner des opérateurs, doit être spécifiée manuellement dans le profil du personnel/prestataire. Le droit *Importer une liste* est activé par défaut pour les rôles Administrateur et Configurateur de site.

Gestion des visiteurs

La gestion des visiteurs est une fonction gratuite qui fonctionne exclusivement avec AuroraSync et les clés mobiles. La gestion des visiteurs permet aux résidents et au personnel d'étendre tout ou partie de leur accès aux visiteurs sur site. En utilisant l'application BlueSky dormakaba, les résidents et le personnel peuvent générer des codes PIN pour autoriser l'accès au périmètre et aux espaces communs. Les résidents ont également la possibilité d'attribuer aux visiteurs des clés mobiles qui peuvent être utilisées pour les portes communes et l'unité du résident, si souhaité.

Un code PIN est une séquence à 7 chiffres qui peut être utilisée sur les points d'accès où un clavier numérique est installé. Une clé mobile attribuée (ou un code PIN au format clé mobile) permet l'accès à l'aide de l'application BlueSky dormakaba.

Lorsque Gestion des visiteurs est activée dans Paramètres du système pour le personnel/les prestataires, l'attribution de codes PIN peut être activée/désactivée dans l'onglet Gestion des visiteurs des profils du personnel/prestataire. Lorsque Gestion des visiteurs est activée dans Paramètres du système pour les résidents, l'attribution de codes PIN et de clés mobiles peut être activée/désactivée dans l'onglet Gestion des visiteurs des profils de résidents.

Les prérequis sont les suivants :

- AuroraSync doit être activé et configuré.
- Les clés mobiles doivent être activées et configurées.
- Le profil du résident doit comporter un numéro de téléphone portable valide.
- L'application BlueSky dormakaba doit être installée et enregistrée sur le périphérique mobile utilisé pour générer le code PIN/la clé mobile.

Clés du personnel/prestataire

Les clés du personnel/prestataire sont créées et remises aux personnes qui travaillent sur le site, ce qui peut inclure les employés, les sous-traitants et les prestataires. Les clés du personnel/prestataire sont encodées avec un identifiant défini dans ***Gestion des accès > Gestion des identifiants*** qui peut inclure l'accès à tous les types de points d'accès : unités, suites, espaces communs (résidents et personnel) et accès privés.

Les clés du personnel/prestataire sont créées dans le module **Clés du personnel/prestataire**. Les instances de clés sont ensuite gérées dans **Gestion du personnel/prestataire** en sélectionnant le personnel/prestataire à qui la clé (instance) a été attribuée, puis l'onglet **Clés attribuées** dans le profil.

Les clés du personnel/prestataire sont valides dans les espaces communs pour le personnel et les résidents et dans les contrôleurs d'ascenseurs jusqu'à l'expiration de la clé. Notez que les clés du personnel/prestataire ayant le statut Obsolète continuent à permettre l'accès aux espaces communs et aux contrôleurs d'ascenseurs jusqu'à l'expiration de la clé. Pour assurer la sécurité des clés dont l'état est obsolète, créez une clé de blocage pour la séquence de clés. Voir Paramètres du système > Clés de blocage.

Pour plus d'informations sur l'invalidation de l'accès du personnel, voir Invalidation de l'accès du personnel.

Ajouter des membres du personnel/prestataires

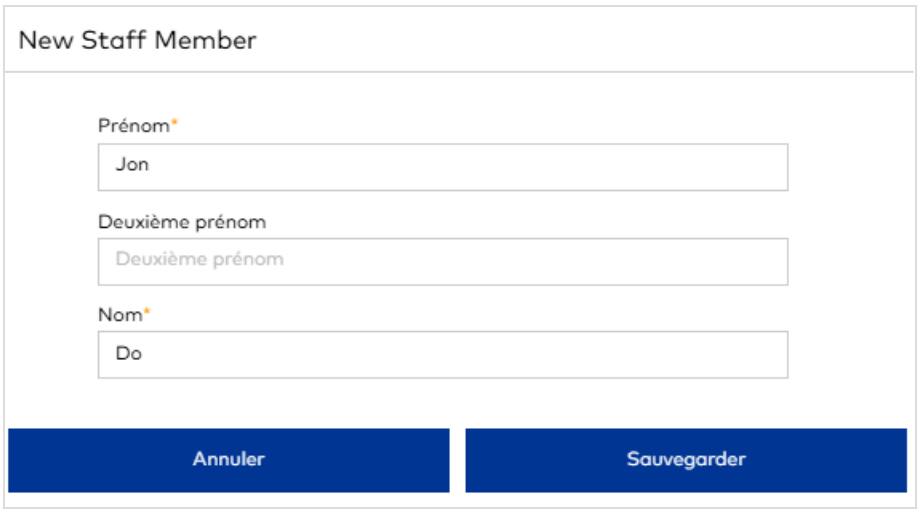
Les membres du personnel sont les porteurs de clés de votre organisation. Les prestataires sont des porteurs de clés extérieurs à votre organisation dont l'accès est limité aux espaces où ils doivent travailler. Vous devez ajouter tous les membres du personnel et prestataires qui recevront une clé.

Vous pouvez ajouter des membres du personnel manuellement ou, si le droit *Importer la liste du personnel* est activé dans la **Gestion des rôles**, vous pouvez importer des membres du personnel. L'importation est limitée à la création des profils des membres du personnel avec des données de base : *prénom*/*nom*/*ID*. Après l'importation, toute information supplémentaire sur un membre du personnel doit être ajoutée manuellement dans son profil du personnel respectif.

Si vous ajoutez un membre du personnel que vous souhaitez désigner comme Opérateur, voir « Configurer des opérateurs » dans *Configuration du site*.

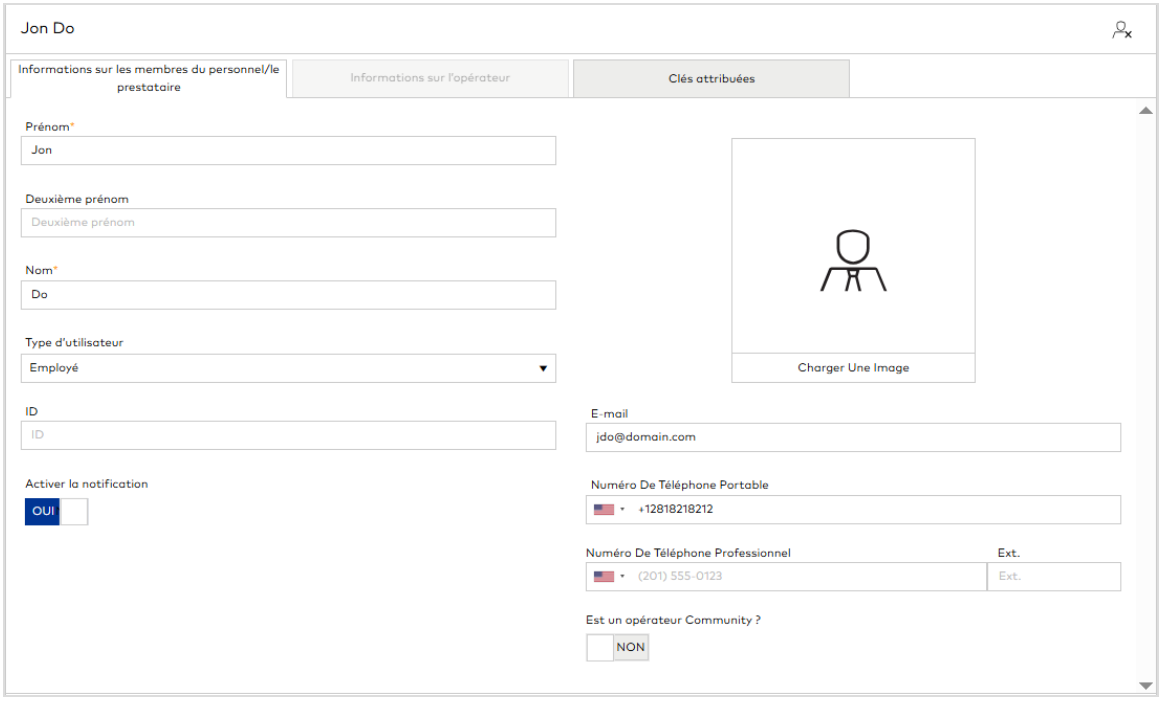
Pour ajouter un membre du personnel ou un prestataire :

1. Accédez à **Gestion du personnel/prestataire**.
2. Cliquez sur **(Ajouter)** .



3. Indiquez le nom du membre du personnel/prestataire. Utilisez le deuxième prénom pour distinguer les membres du personnel ayant le même prénom et le même nom. Nombre maximum de caractères par champ : 25.
4. Cliquez sur **Sauvegarder**. Community crée un profil de membre du personnel/prestataire et affiche l'onglet **Personnel/Prestataire**. Aucune autre option n'est requise, sauf si vous souhaitez envoyer des e-mails automatiques au membre du personnel/prestataire, activer les notifications pour le membre du personnel/prestataire ou désigner le membre du personnel comme Opérateur.

Si l'ouverture forcée pour la validation du numéro de téléphone/téléphone portable est activée dans **Paramètres du système**, les opérateurs peuvent autoriser l'utilisation de numéros inconnus.



5. (*recommandé*) Pour un **e-mail**, indiquez une adresse e-mail valide pour le membre du personnel/prestataire. Une adresse e-mail est nécessaire pour envoyer des e-mails automatiques concernant l'accès au compte et pour envoyer des notifications par e-mail. (Pour les opérateurs, l'adresse e-mail peut être modifiée dans le compte **Préférences**).
6. Choisissez d'activer ou non les notifications et, si elles sont activées, sélectionnez les abonnements aux groupes de notification pour le membre du personnel/prestataire.
7. Cliquez sur **(Sauvegarder)** .

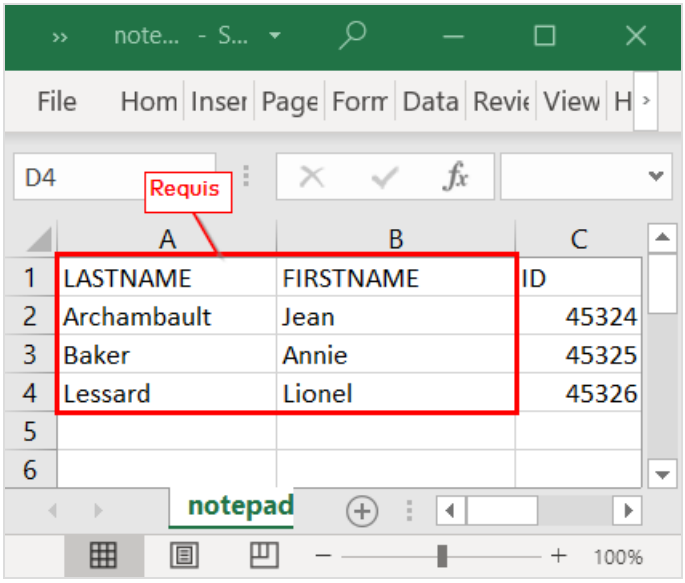
Importer la liste des membres du personnel/prestataires

Pour importer les membres du personnel/prestataires :

1. Accédez à **Gestion du personnel/prestataire**.
2. Cliquez sur ***(Plus)*** **...** ***> Importer la liste du personnel***.

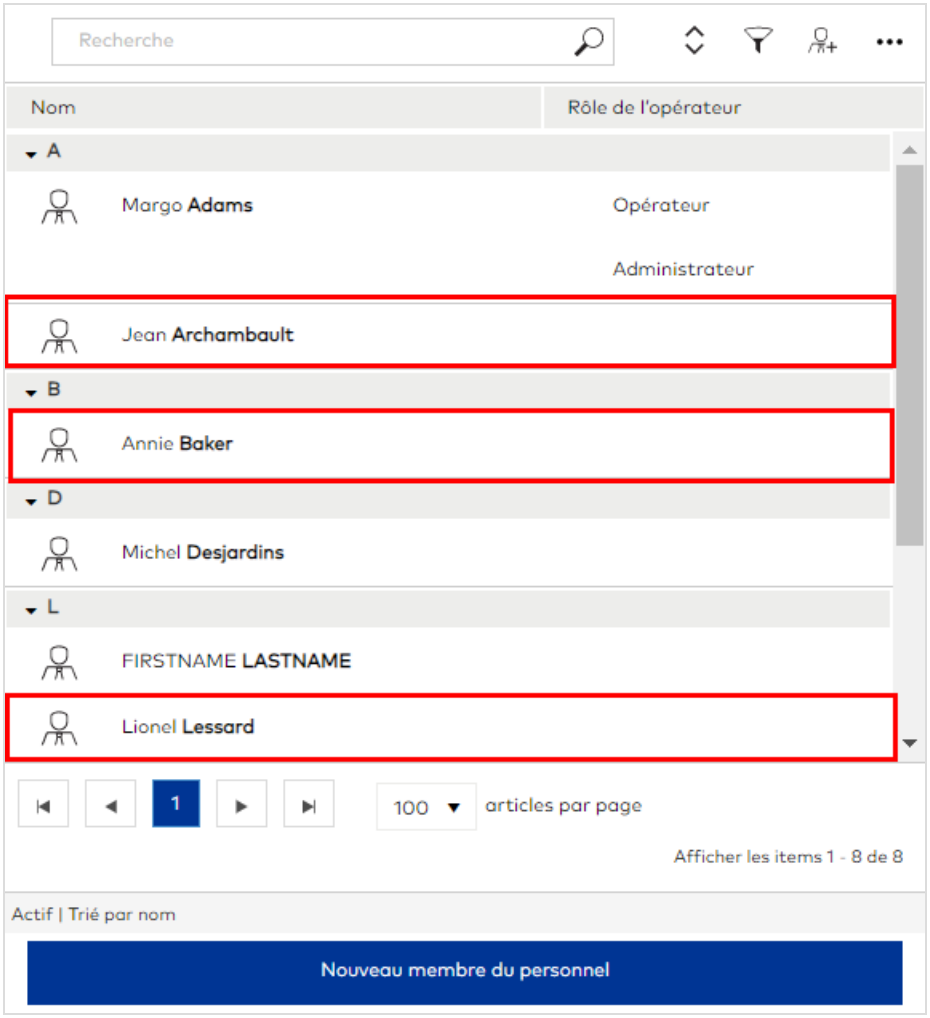


3. Naviguez et sélectionnez le fichier que vous souhaitez importer, puis cliquez sur **Ouvrir**. Type de fichiers pris en charge : csv. La figure suivante montre un exemple de fichier et le format de données requis. Si un champ obligatoire est vide, le membre du personnel/prestataire n'est pas ajouté.



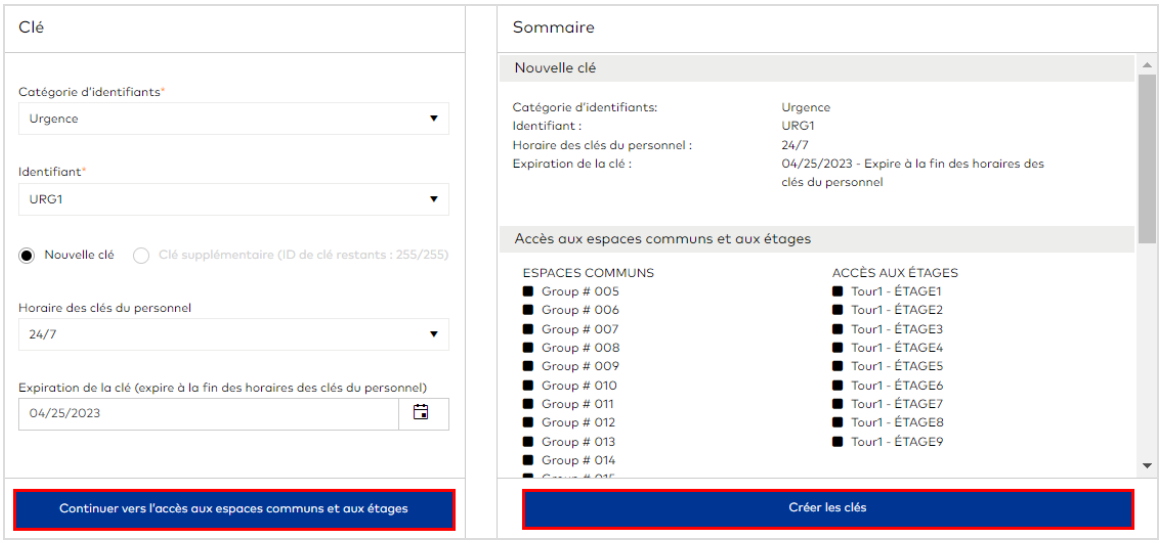
> Si les profils des membres du personnel ont déjà été créés, vous êtes invité à continuer. Cliquez sur **OUI** pour continuer.

4. Lorsque vous êtes informé que l'importation est réussie, cliquez sur **OK**.

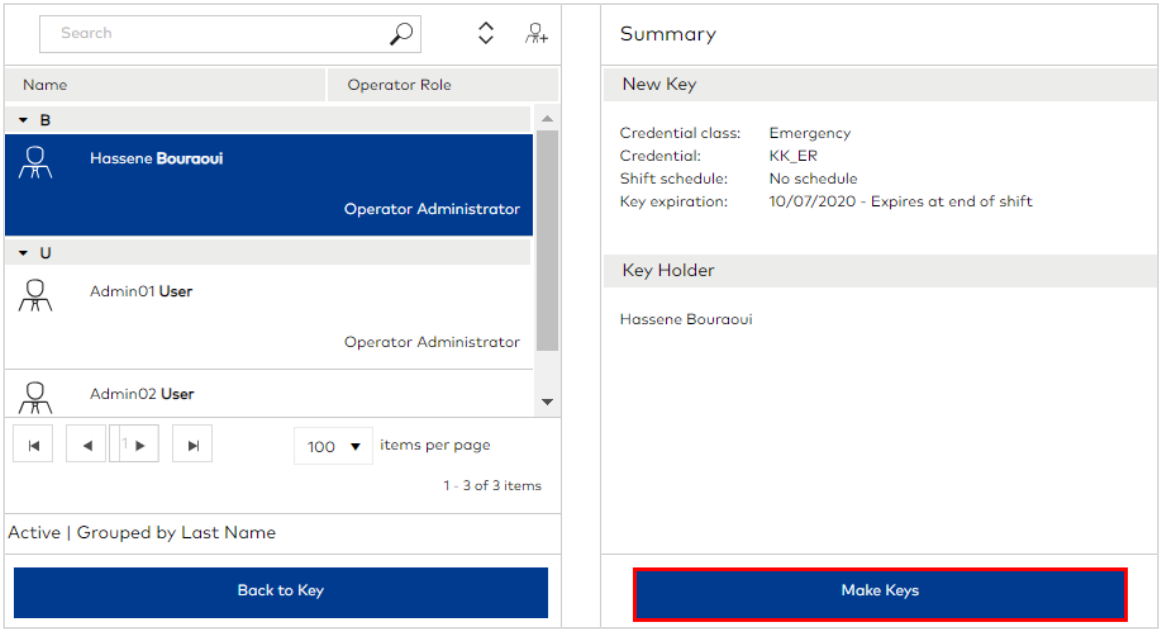

Recherche
Nom
Rôle de l'opérateur
A
Margo Adams
Opérateur
Administrateur
Jean Archambault
B
Annie Baker
D
Michel Desjardins
L
FIRSTNAME LASTNAME
Lionel Lessard
1
100
articles par page
Afficher les items 1 - 8 de 8
Actif | Trié par nom
Nouveau membre du personnel

Créer des clés d'urgence

1. Accédez à **Clés du personnel/prestataire**.



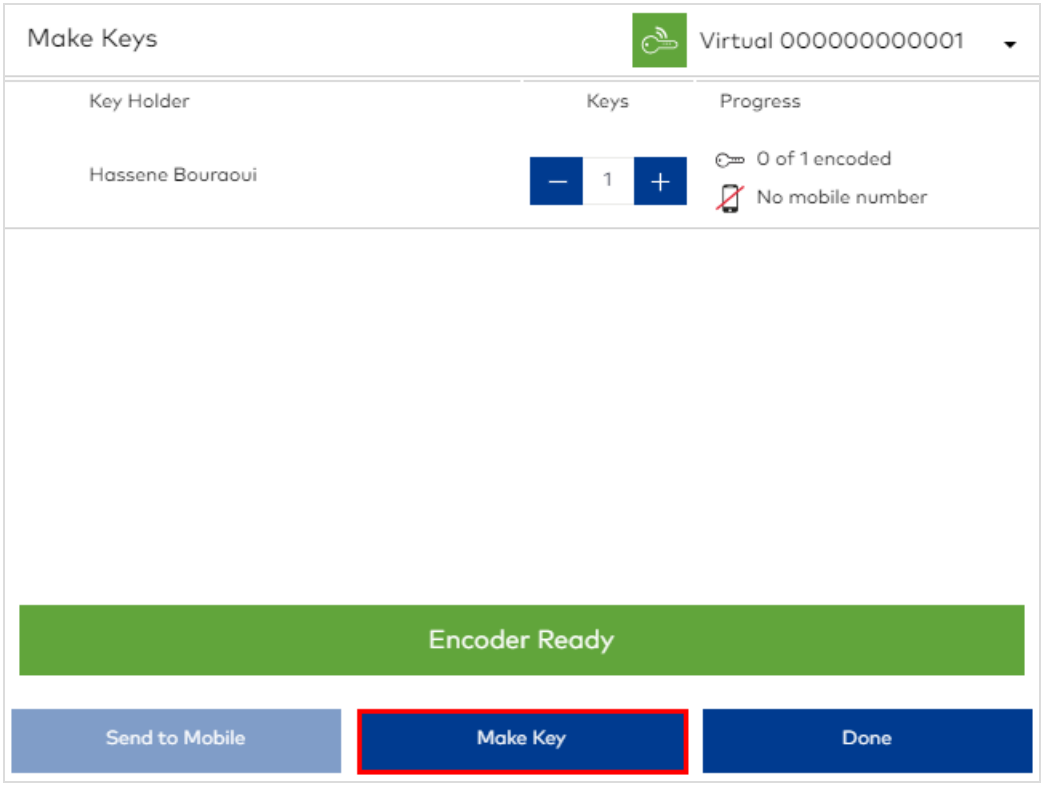
2. Sélectionnez la catégorie d'identifiants **Urgence** ou une catégorie personnalisée basée sur le type de catégorie Urgence. Seules les catégories pour lesquelles les identifiants sont définis figurent dans la liste.
3. Sélectionnez un identifiant. Seuls les identifiants créés à l'aide de la catégorie sélectionnée sont répertoriés.
4. Indiquez si vous souhaitez créer une clé avec le mode **Nouveau** ou **Supplémentaire**. Les nouvelles clés invalident les clés actives existantes pour l'identifiant sélectionné à tous les points d'accès, à l'exception des espaces communs. Les clés supplémentaires (copies) n'ont pas d'effet sur les clés actives existantes.
5. Sélectionnez un horaire des clés du personnel. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
6. Indiquez la date après laquelle la clé est invalide.
7. Cliquez sur **Continuer vers le porteur de clé**, puis sélectionnez le membre du personnel/prestataire auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel/prestataire, cliquez sur **(Ajouter)** , saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.



8. Cliquez sur **Créer les clés**.

Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

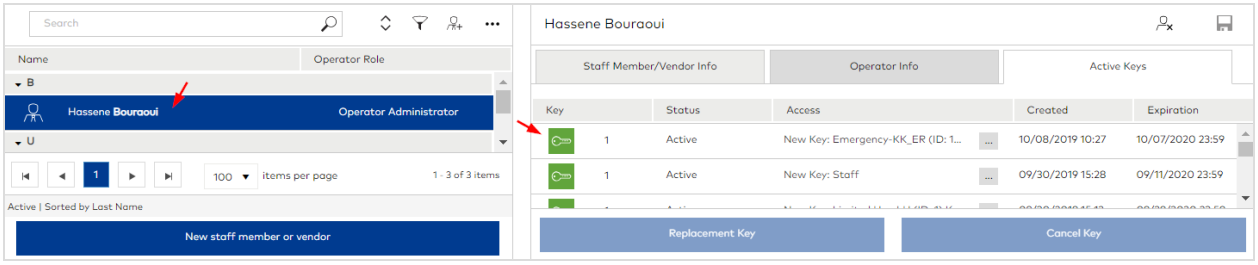
9. Indiquez le nombre de clés à créer.
10. Sélectionnez un encodeur en ligne.
11. Cliquez sur **Créer la clé**.
12. Présentez les clés à l'encodeur (lorsque vous y êtes invité).



Si tous les ID de la clé pour l'identifiant sélectionné sont attribués à des clés actives, un avertissement signale que pour continuer, un ID de la clé existant doit être sélectionné. Pour réutiliser un ID de la clé, cliquez sur **Continuer**, puis sélectionnez l'ID de la clé à réutiliser. Une seule clé peut être créée. La réutilisation des ID de la clé entraîne l'attribution de plusieurs porteurs de clés à une même clé et réduit la traçabilité lors des audits. Les porteurs de clés utilisant le même ID de la clé ne sont pas des porteurs de clés absolus.

13. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

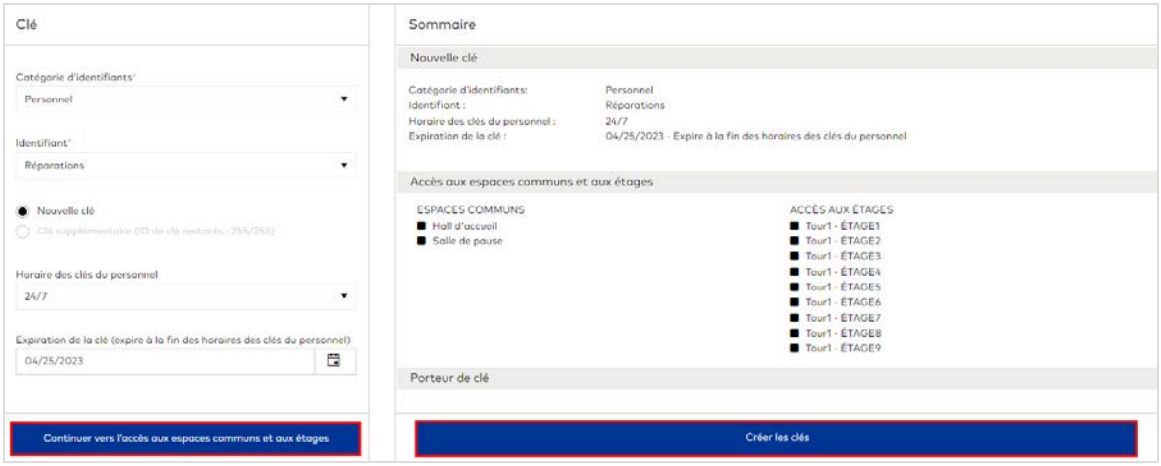
La clé est répertoriée dans l'onglet **Clés attribuées** du profil du membre du personnel/prestataire.



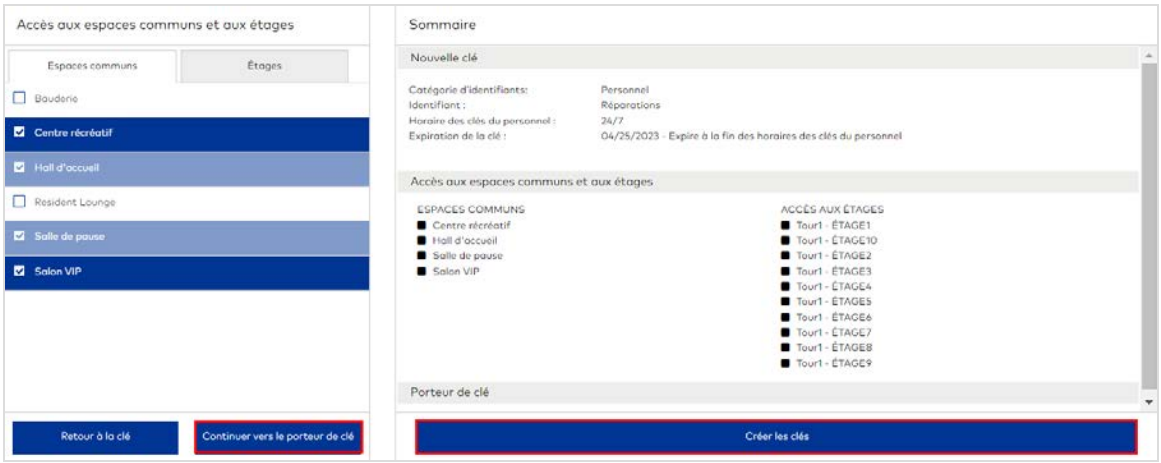
Vous pouvez vérifier qu'une clé mobile a été livrée dans la **Gestion du personnel/prestataire**.

Créer une clé du personnel (accès prédéfini)

1. Accédez à **Clés du personnel/prestataire**.
2. Sélectionnez la catégorie d'identifiants **Personnel** ou une catégorie personnalisée basée sur le même type. Seules les catégories pour lesquelles les identifiants sont définis figurent dans la liste.
3. Sélectionnez un identifiant. Seuls les identifiants créés à l'aide de la catégorie sélectionnée sont répertoriés.



   Lorsque vous sélectionnez un identifiant, les espaces communs illimités et restreints dont l'accès est activé dans le profil d'accès aux espaces communs associé à l'identifiant sont répertoriés. L'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.
4. Indiquez si vous souhaitez créer une clé avec le mode **Nouveau** ou **Supplémentaire**. Les nouvelles clés invalident les clés actives existantes pour l'identifiant sélectionné à tous les points d'accès, à l'exception des espaces communs. Les clés supplémentaires (copies) n'ont pas d'effet sur les clés actives existantes.
5. Sélectionnez un horaire des clés du personnel. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
6. Indiquez la date après laquelle la clé est invalide.
7. Effectuez l'une des actions suivantes :
   - Cliquez sur **Continuer vers les espaces communs**, **Continuer vers les étages**, ou **Continuer vers les espaces communs et les étages** et passez à l'étape suivante.
   - Cliquez sur **Continuer vers le porteur de clé** et passez à l'étape 10.
8. Sélectionnez l'accès aux espaces communs et/ou aux étages à ajouter sur la clé :

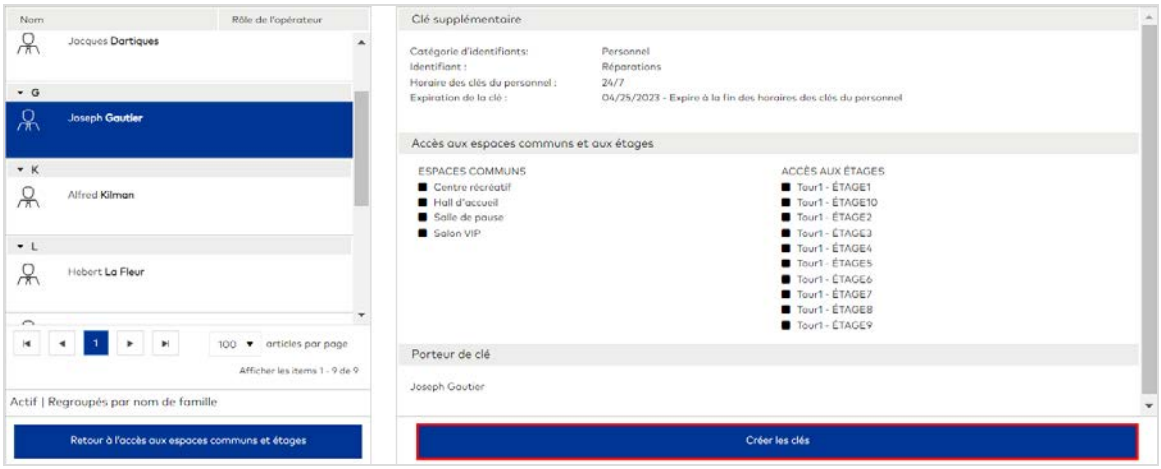


- Lorsque l'onglet **Espaces communs** s'affiche, tous les espaces communs illimités (personnel et résidents) sont sélectionnés par défaut et ne peuvent pas être désélectionnés. Les espaces communs à accès limité (personnel et résidents) sont répertoriés s'ils sont sélectionnés dans un profil d'accès aux espaces communs associé à l'identifiant sélectionné.
- Lorsque l'onglet **Accès aux étages** s'affiche, tous les étages où l'accès aux ascenseurs est configuré sont répertoriés. Par défaut, l'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.

Veillez à ne pas supprimer l'accès aux étages par défaut.

Lorsque vous êtes prêt, cliquez sur **Continuer vers le porteur de clé** et passez à l'étape suivante.

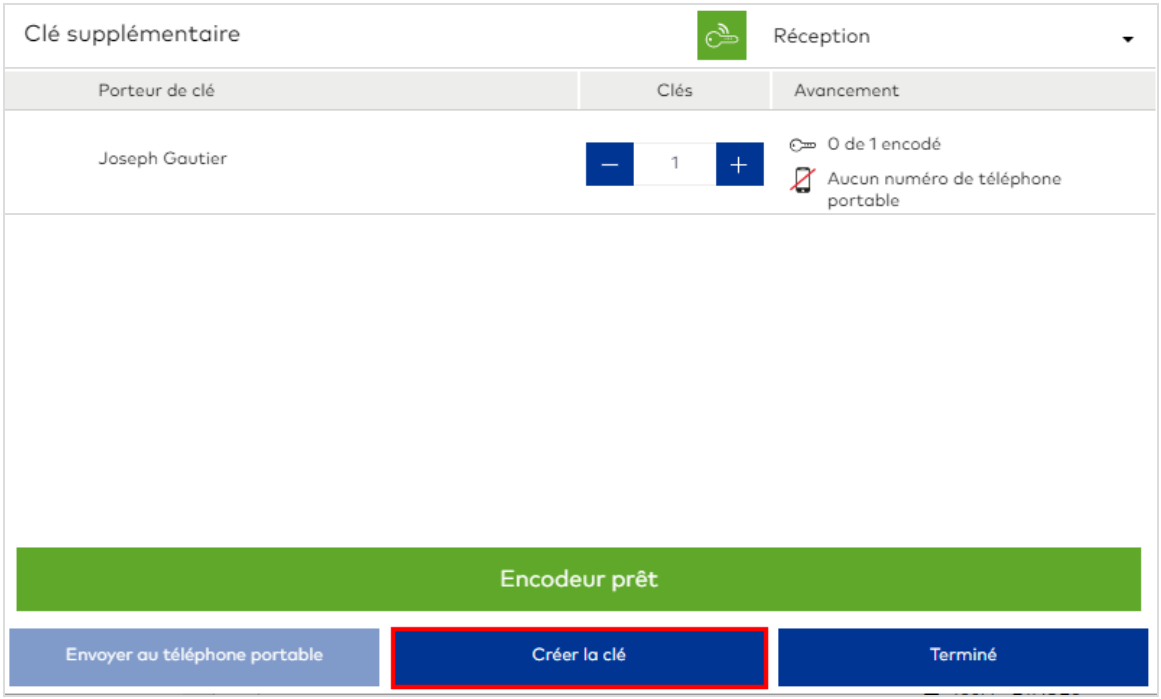
9. Sélectionnez le membre du personnel/prestataire à qui vous souhaitez attribuer la clé. Pour ajouter un membre du personnel/prestataire, cliquez sur (Ajouter) , saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.



10. Cliquez sur **Créer les clés**.

Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

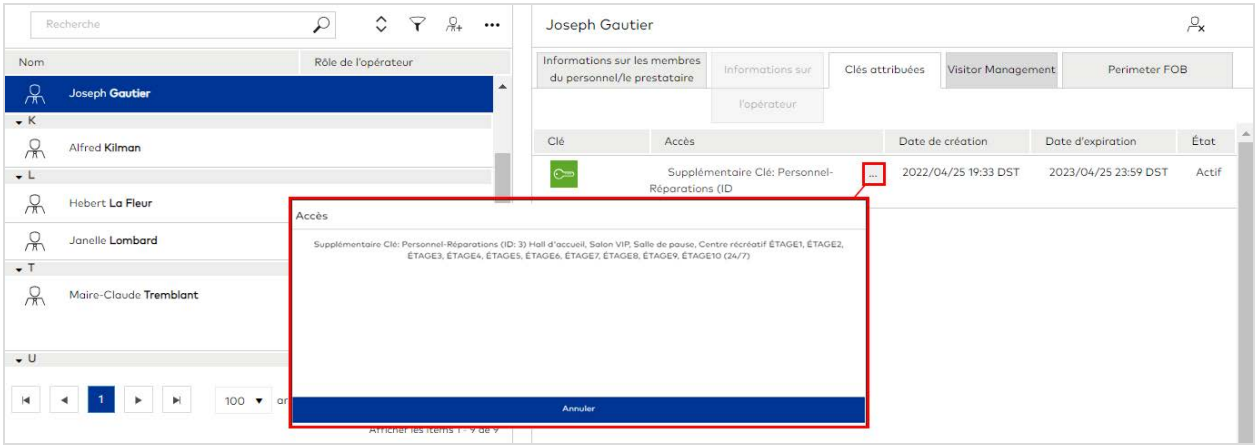
11. Indiquez le nombre de clés à créer.
12. Sélectionnez un encodeur en ligne.
13. Cliquez sur **Créer la clé**.
14. Présentez les clés à l'encodeur (lorsque vous y êtes invité).



Si tous les ID de la clé pour l'identifiant sélectionné sont attribués à des clés actives, un avertissement signale que pour continuer, un ID de la clé existant doit être sélectionné. Pour réutiliser un ID de la clé, cliquez sur **Continuer**, puis sélectionnez l'ID de la clé à réutiliser. Une seule clé peut être créée. La réutilisation des ID de la clé entraîne l'attribution de plusieurs porteurs de clés à une même clé et réduit la traçabilité lors des audits. Les porteurs de clés utilisant le même ID de la clé ne sont pas des porteurs de clés absolus.

15. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

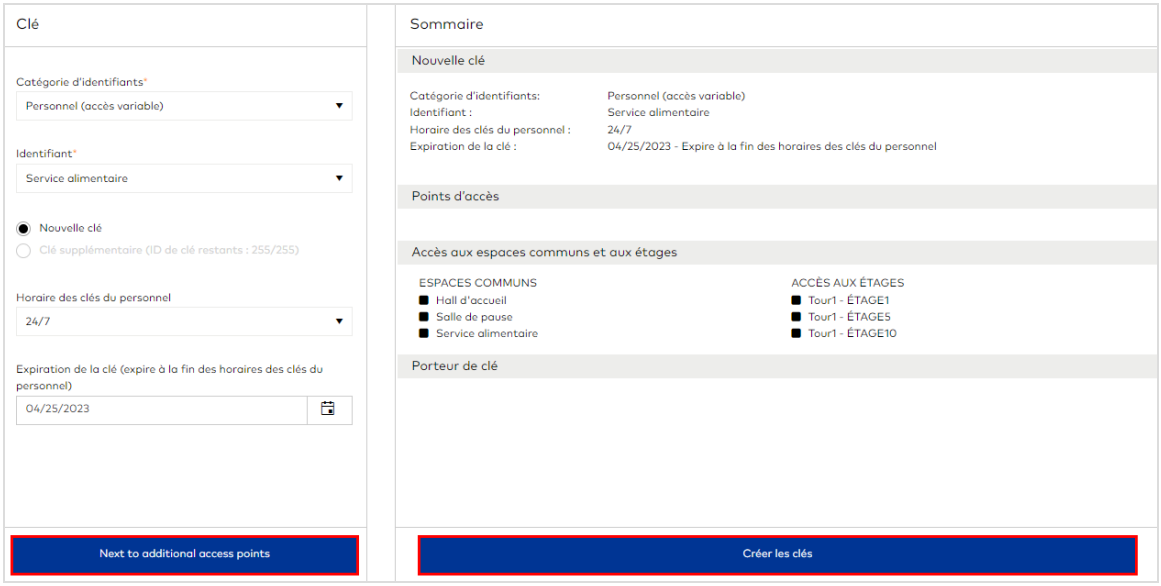
La clé est répertoriée dans l'onglet **Clés attribuées** du profil du membre du personnel/prestataire.



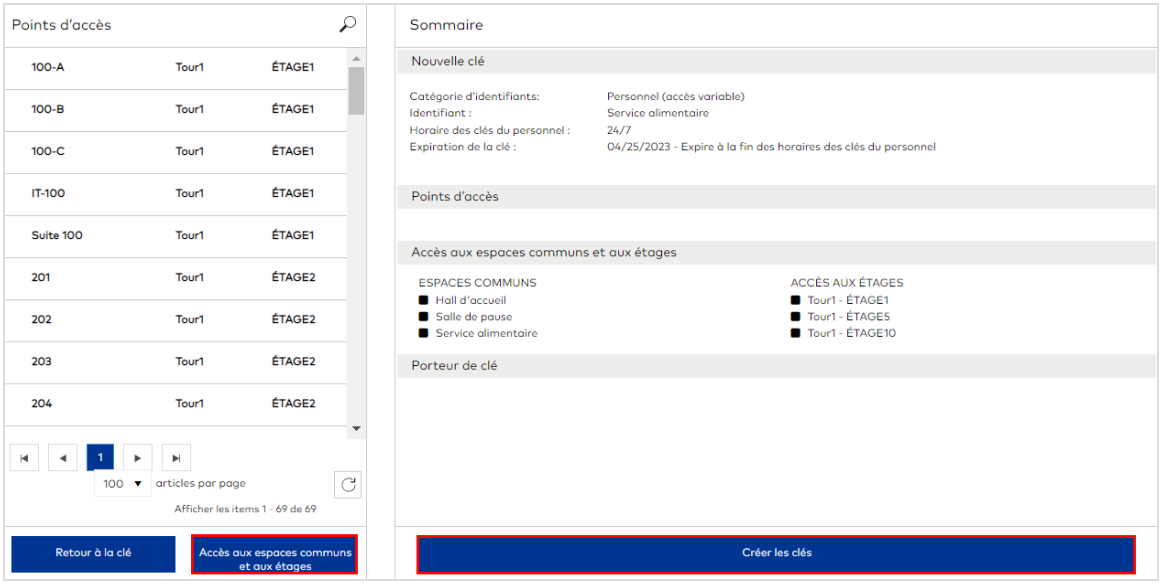
Vous pouvez vérifier qu'une clé mobile a été livrée dans la **Gestion du personnel/prestataire**.

Créer des clés du personnel (accès variable)

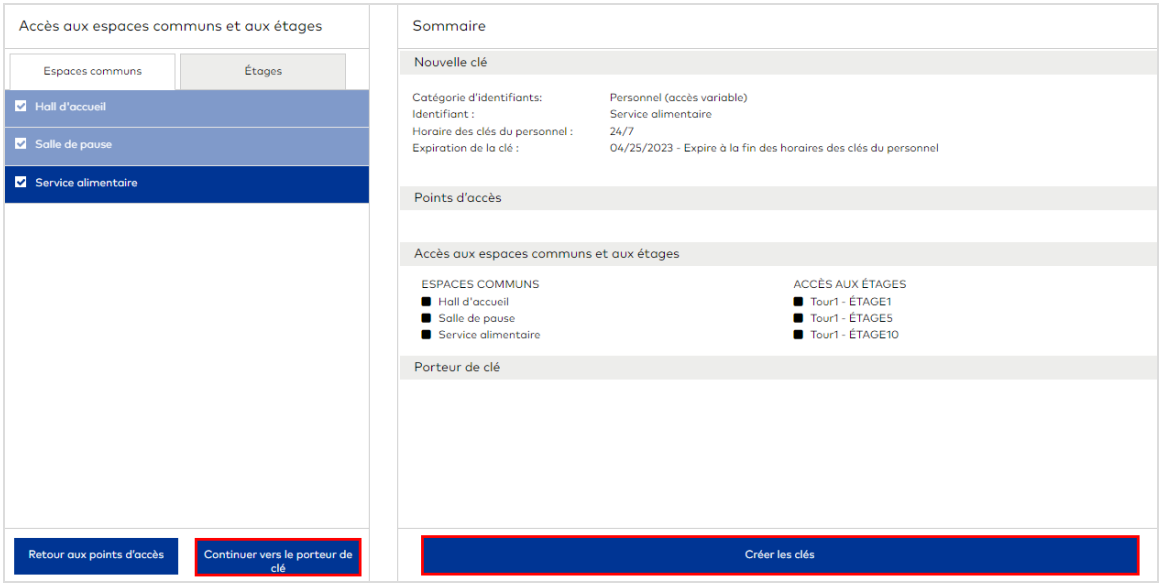
1. Accédez à **Clés du personnel/prestataire**.
2. Sélectionnez la catégorie d'identifiants **Personnel (accès variable)** ou une catégorie personnalisée basée sur le même type. Seules les catégories pour lesquelles les identifiants sont définis figurent dans la liste.
3. Sélectionnez un identifiant. Seuls les identifiants créés à l'aide de la catégorie sélectionnée sont répertoriés.

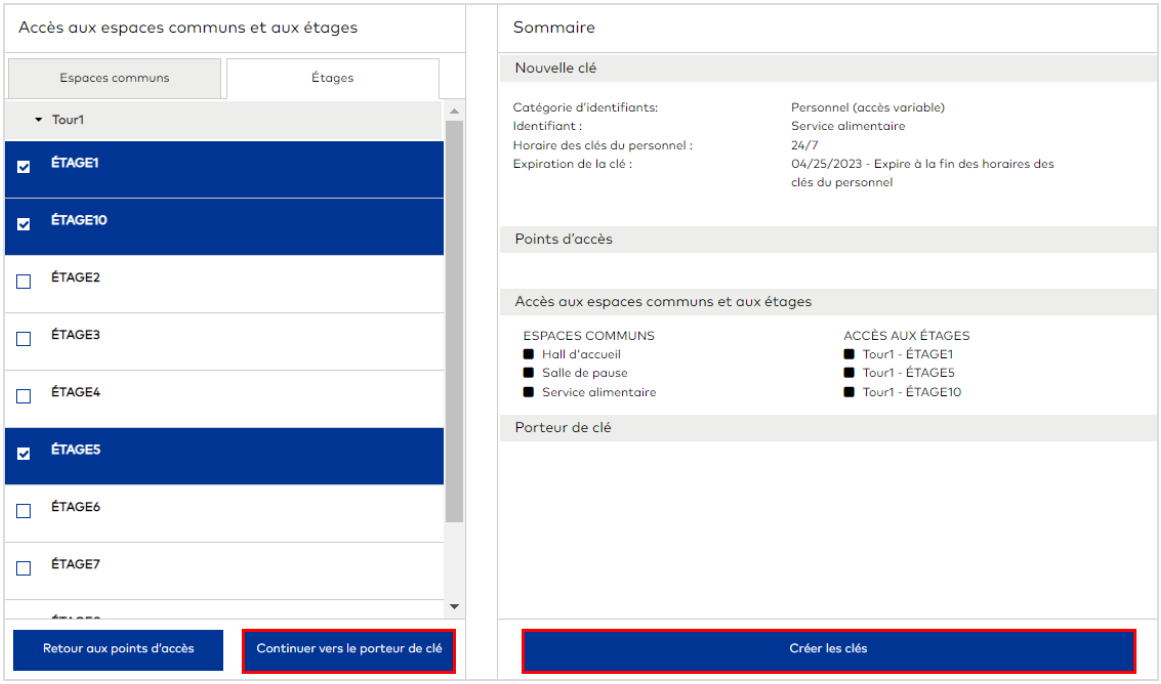


   Lorsque vous sélectionnez un identifiant, les espaces communs illimités et restreints dont l'accès est activé dans le profil d'accès aux espaces communs associé à l'identifiant sont répertoriés. L'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.
4. Indiquez si vous souhaitez créer une clé avec le mode **Nouveau** ou **Supplémentaire**. Les nouvelles clés invalident les clés actives existantes pour l'identifiant sélectionné à tous les points d'accès, à l'exception des espaces communs. Les clés supplémentaires (copies) n'ont pas d'effet sur les clés actives existantes.
5. Sélectionnez un horaire des clés du personnel. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
6. Indiquez la date après laquelle la clé est invalide.
7. Cliquez sur **Continuer vers les Point d'accès**.



8. Sélectionnez les points d'accès à ajouter sur la clé. Types de points d'accès répertoriés : Unités/Unités de suite et accès privés. Vous pouvez sélectionner des points d'accès de différents bâtiments. Les points d'accès maximum que vous pouvez sélectionner sont : 542 (clés 4k), 94 (clés 1k), 25 (clés mobiles). Les points d'accès sélectionnés sont ajoutés à la section **Sommaire** (classés par bâtiment et par étage).
9. Effectuez l'une des actions suivantes :
   - Cliquez sur **Espaces communs et étages**, **Espaces communs**, ou **Accès aux étages** et passez à l'étape suivante.
   - Cliquez sur **Continuer vers le porteur de clé** et passez à l'étape 12.
10. Sélectionnez l'accès aux espaces communs et/ou aux étages à ajouter sur la clé :



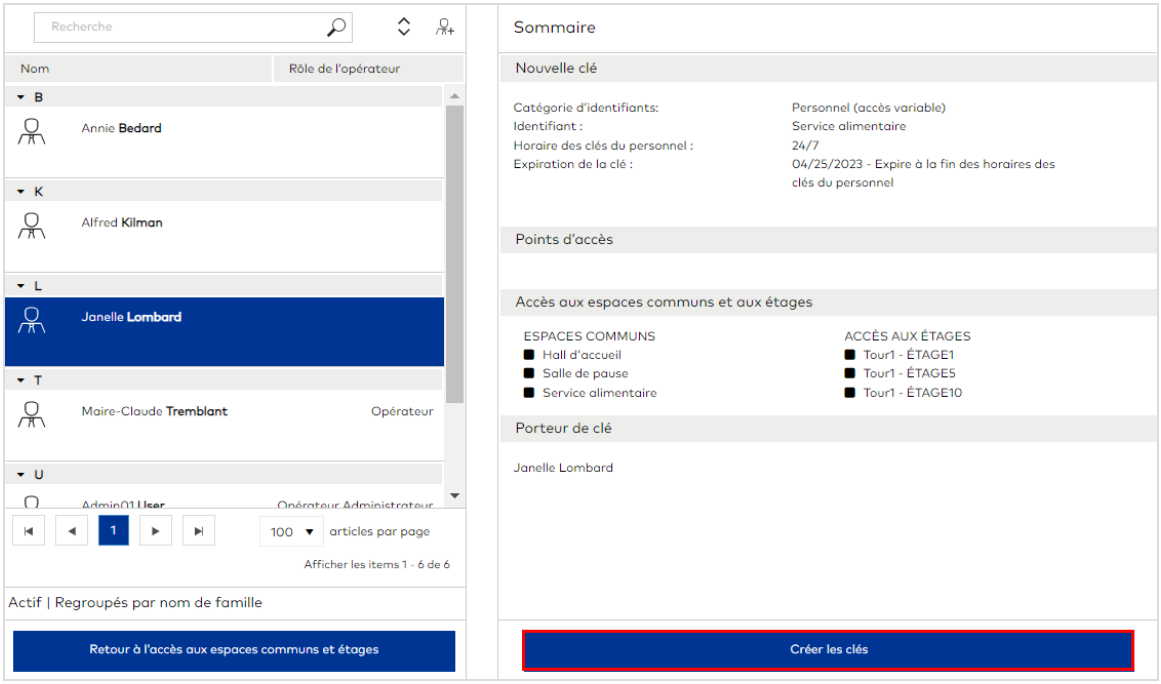


- Lorsque l'onglet **Espaces communs** s'affiche, tous les espaces communs illimités (personnel et résidents) sont sélectionnés par défaut et ne peuvent pas être désélectionnés. Les espaces communs à accès limité (personnel et résidents) sont répertoriés s'ils sont sélectionnés dans un profil d'accès aux espaces communs associé à l'identifiant sélectionné.
- Lorsque l'onglet **Accès aux étages** s'affiche, tous les étages où l'accès aux ascenseurs est configuré sont répertoriés. Par défaut, l'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.

Veillez à ne pas supprimer l'accès aux étages par défaut.

Lorsque vous êtes prêt, cliquez sur **Continuer vers le porteur de clé** et passez à l'étape suivante.

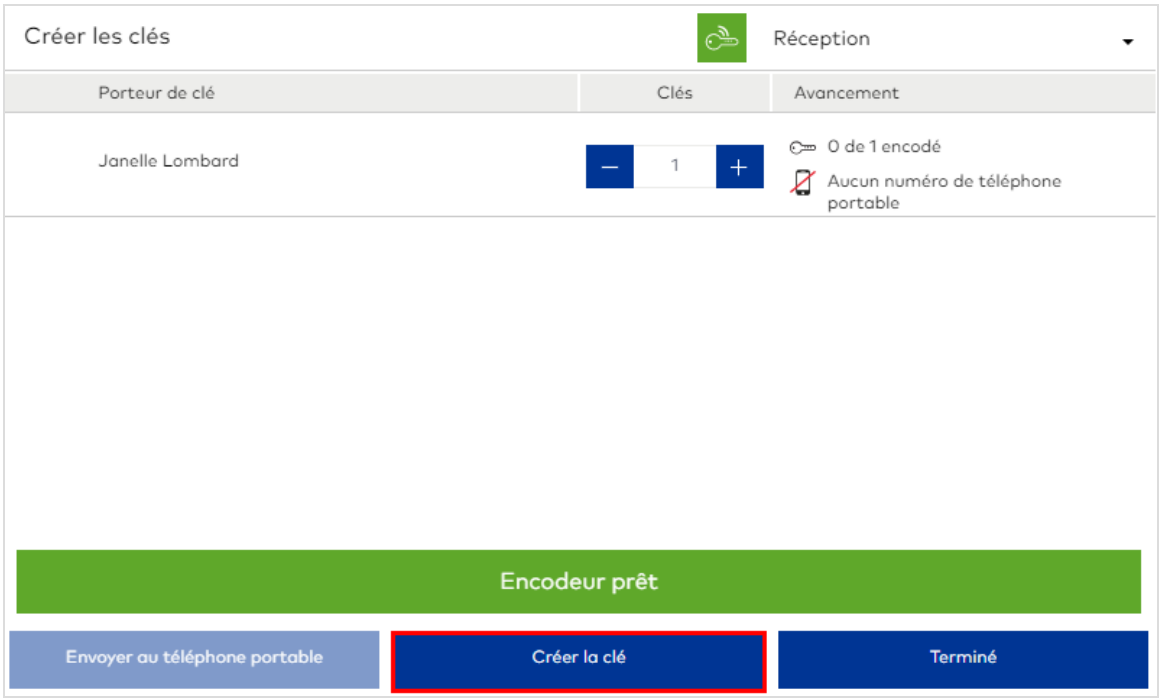
11. Sélectionnez le membre du personnel/prestataire à qui vous souhaitez attribuer la clé. Pour ajouter un membre du personnel/prestataire, cliquez sur (Ajouter) , saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.



12. Cliquez sur **Créer les clés**.

> Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

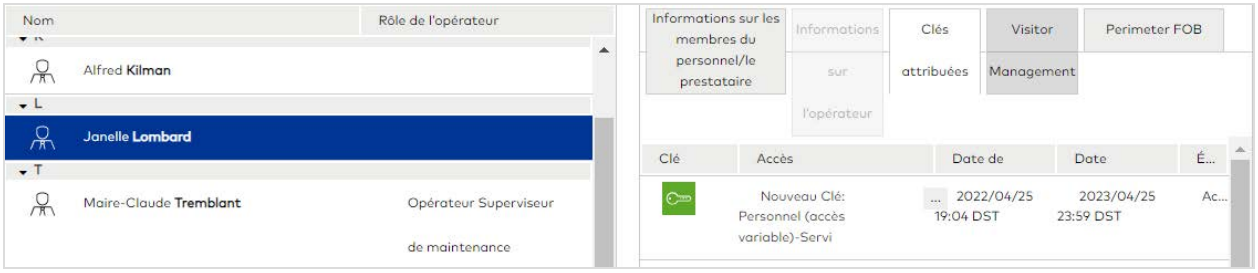
13. Indiquez le nombre de clés à créer.
14. Sélectionnez un encodeur en ligne.
15. Cliquez sur **Créer la clé**.
16. Présentez les clés à l'encodeur (lorsque vous y êtes invité).



Si tous les ID de la clé pour l'identifiant sélectionné sont attribués à des clés actives, un avertissement signale que pour continuer, un ID de la clé existant doit être sélectionné. Pour réutiliser un ID de la clé, cliquez sur **Continuer**, puis sélectionnez l'ID de la clé à réutiliser. Une seule clé peut être créée. La réutilisation des ID de la clé entraîne l'attribution de plusieurs porteurs de clés à une même clé et réduit la traçabilité lors des audits. Les porteurs de clés utilisant le même ID de la clé ne sont pas des porteurs de clés absolus.

17. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

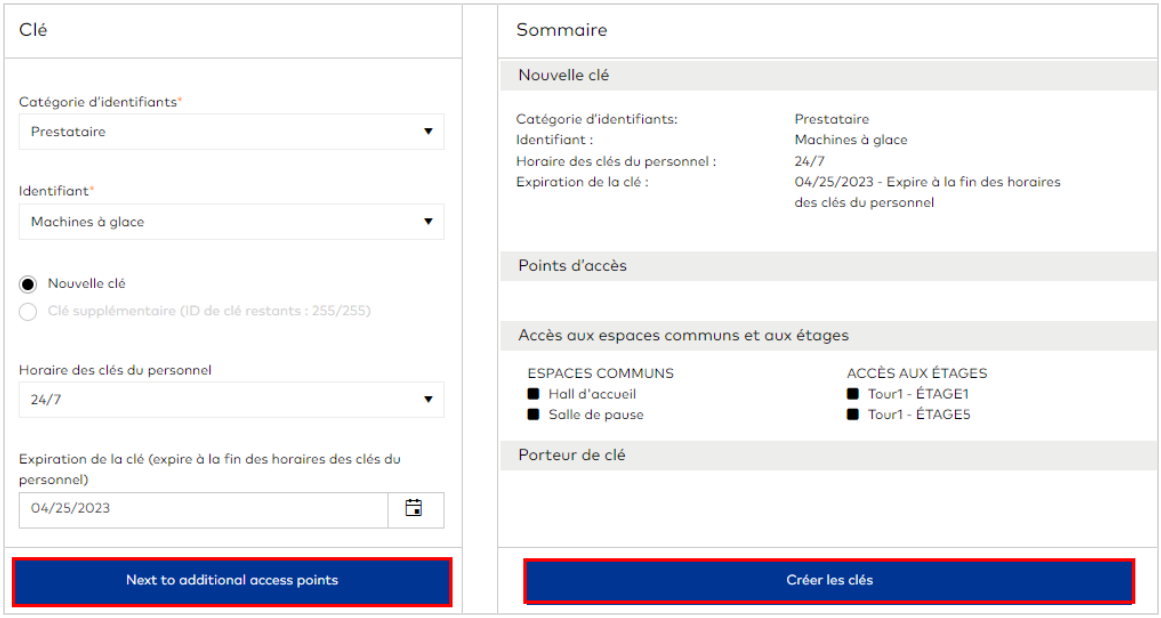
La clé est répertoriée dans l'onglet **Clés attribuées** du profil du membre du personnel/prestataire.



Vous pouvez vérifier qu'une clé mobile a été livrée dans la Gestion du personnel/prestataire.

Créer des clés de prestataire

1. Accédez à **Clés du personnel/prestataire**.
2. Sélectionnez la catégorie d'identifiants **Prestataire** ou une catégorie personnalisée basée sur le même type. Seules les catégories pour lesquelles les identifiants sont définis figurent dans la liste.
3. Sélectionnez un identifiant. Seuls les identifiants créés à l'aide de la catégorie sélectionnée sont répertoriés.

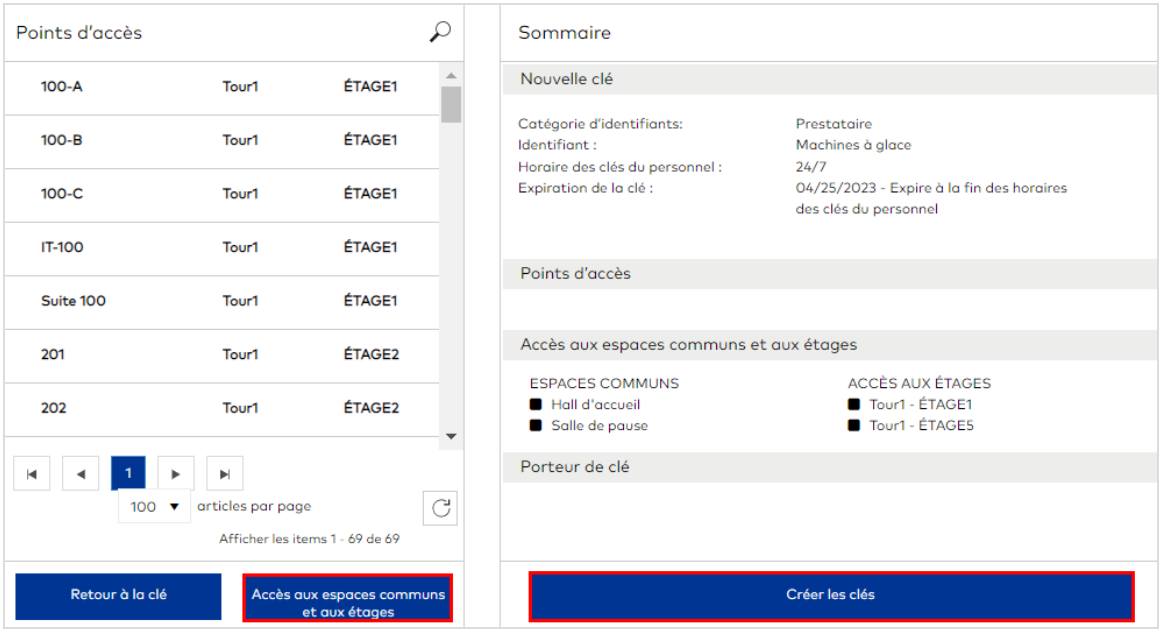


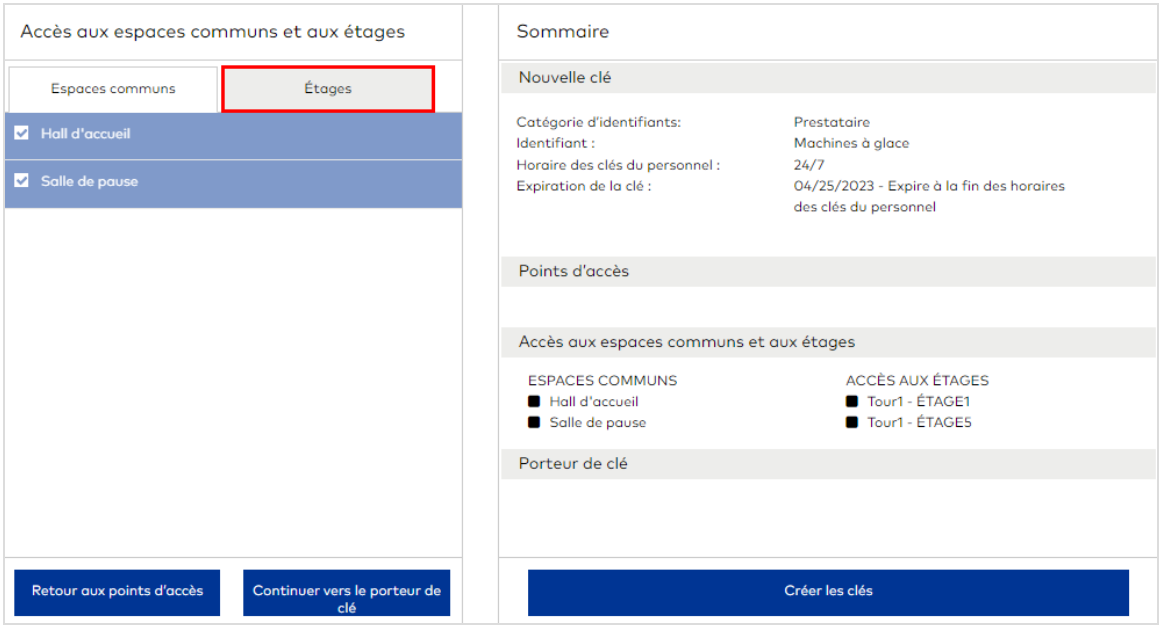
Lorsque vous sélectionnez un identifiant, les espaces communs illimités et restreints dont l'accès est activé dans le profil d'accès aux espaces communs associé à l'identifiant sont répertoriés. L'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.

4. Indiquez si vous souhaitez créer une clé avec le mode **Nouveau** ou **Supplémentaire**. Les nouvelles clés invalident les clés actives existantes pour l'identifiant sélectionné à tous les points d'accès, à l'exception des espaces communs. Les clés supplémentaires (copies) n'ont pas d'effet sur les clés actives existantes.
5. Sélectionnez un horaire des clés du personnel. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
6. Indiquez la date après laquelle la clé est invalide.
7. Cliquez sur **Continuer vers les Point d'accès**.



8. Sélectionnez les points d'accès à ajouter sur la clé. Types de points d'accès répertoriés : Unités/Unités de suite et accès privés. Vous pouvez sélectionner des points d'accès de différents bâtiments. Les points d'accès maximum que vous pouvez sélectionner sont : 542 (clés 4k), 94 (clés 1k), 25 (clés mobiles). Les points d'accès sélectionnés sont ajoutés à la section **Sommaire** (classés par bâtiment et par étage).
9. Effectuez l'une des actions suivantes :
   - Cliquez sur **Espaces communs et étages**, **Espaces communs**, ou **Accès aux étages** et passez à l'étape suivante.
   - Cliquez sur **Continuer vers le porteur de clé** et passez à l'étape 12.
10. Sélectionnez l'accès aux espaces communs et/ou aux étages à ajouter sur la clé :



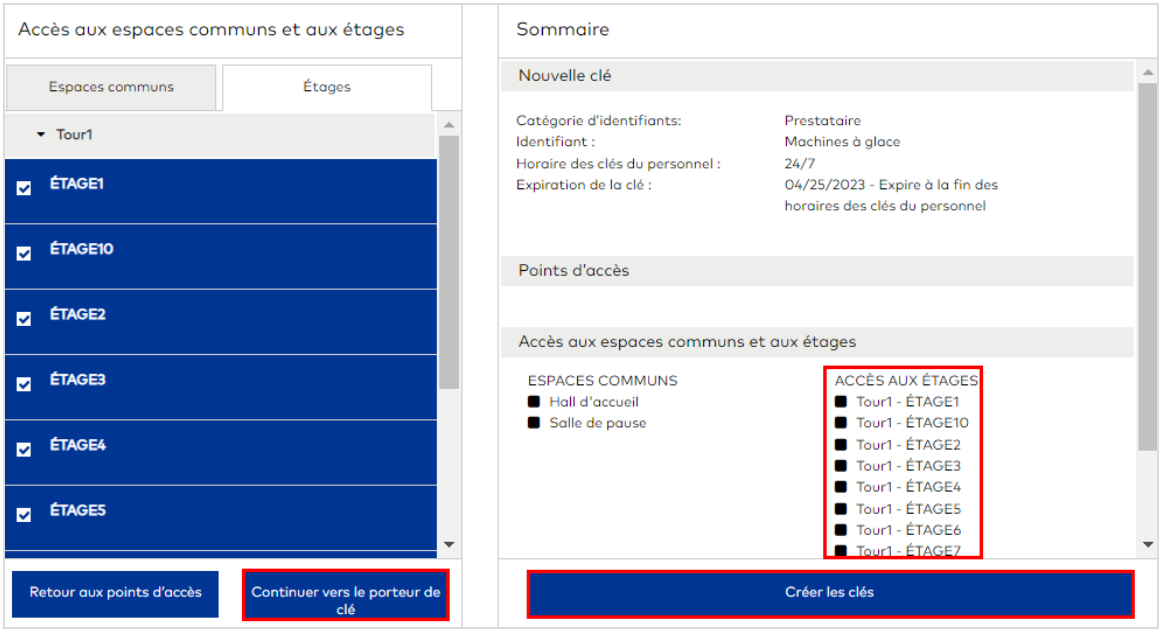


- Lorsque l'onglet **Espaces communs** s'affiche, tous les espaces communs illimités (personnel et résidents) sont sélectionnés par défaut et ne peuvent pas être désélectionnés. Les espaces communs à accès limité (personnel et résidents) sont répertoriés s'ils sont sélectionnés dans un profil d'accès aux espaces communs associé à l'identifiant sélectionné.
- Lorsque l'onglet **Accès aux étages** s'affiche, tous les étages où l'accès aux ascenseurs est configuré sont répertoriés. Par défaut, l'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.

Veillez à ne pas supprimer l'accès aux étages par défaut.

Lorsque vous êtes prêt, cliquez sur **Continuer vers le porteur de clé** et passez à l'étape suivante.

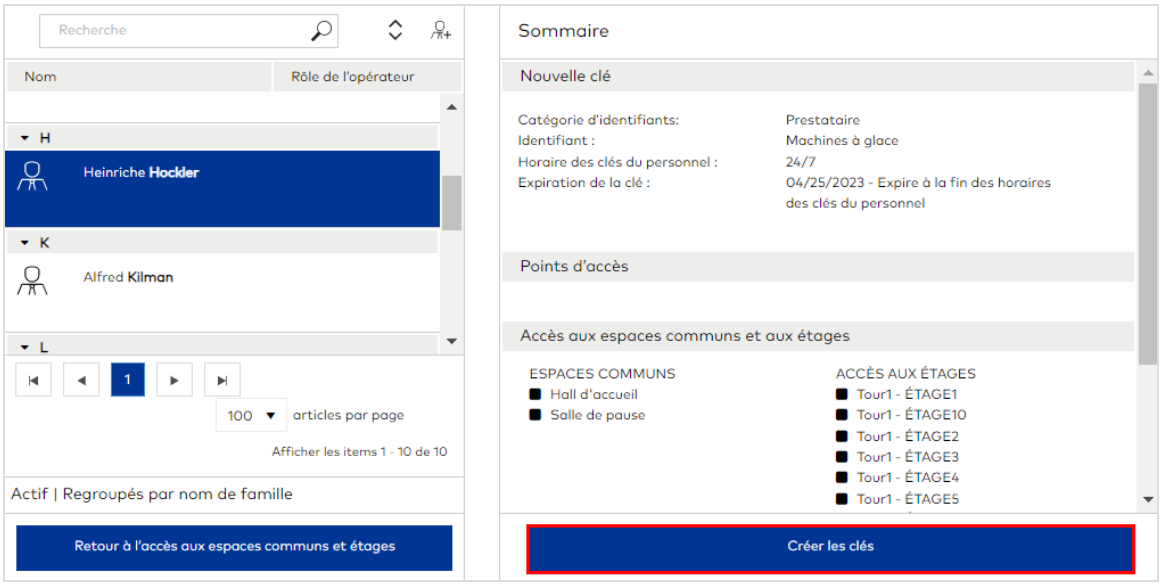
11. Sélectionnez le membre du personnel/prestataire à qui vous souhaitez attribuer la clé. Pour ajouter un membre du personnel/prestataire, cliquez sur (Ajouter) , saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.



12. Cliquez sur **Créer les clés**.

Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

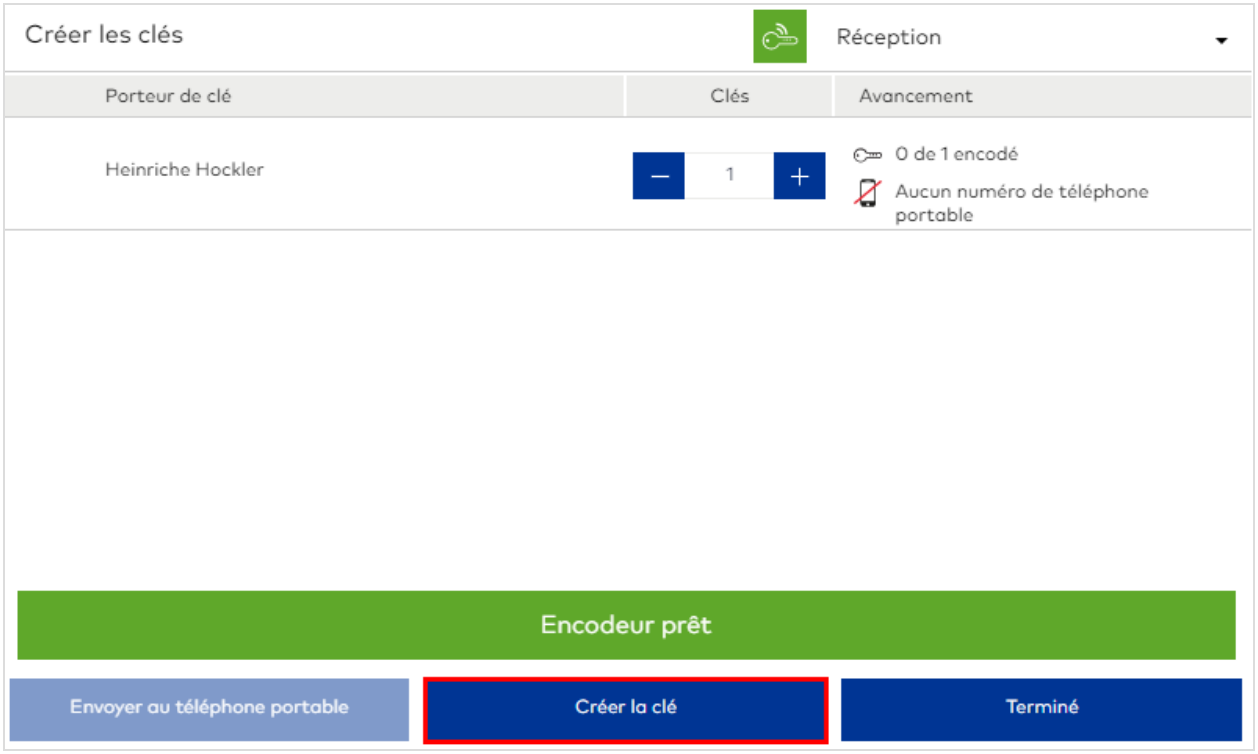
13. Indiquez le nombre de clés à créer.
14. Sélectionnez un encodeur en ligne.
15. Cliquez sur **Créer la clé**.
16. Présentez les clés à l'encodeur (lorsque vous y êtes invité).



Si tous les ID de la clé pour l'identifiant sélectionné sont attribués à des clés actives, un avertissement signale que pour continuer, un ID de la clé existant doit être sélectionné. Pour réutiliser un ID de la clé, cliquez sur **Continuer**, puis sélectionnez l'ID de la clé à réutiliser. Une seule clé peut être créée. La réutilisation des ID de la clé entraîne l'attribution de plusieurs porteurs de clés à une même clé et réduit la traçabilité lors des audits. Les porteurs de clés utilisant le même ID de la clé ne sont pas des porteurs de clés absolus.

17. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

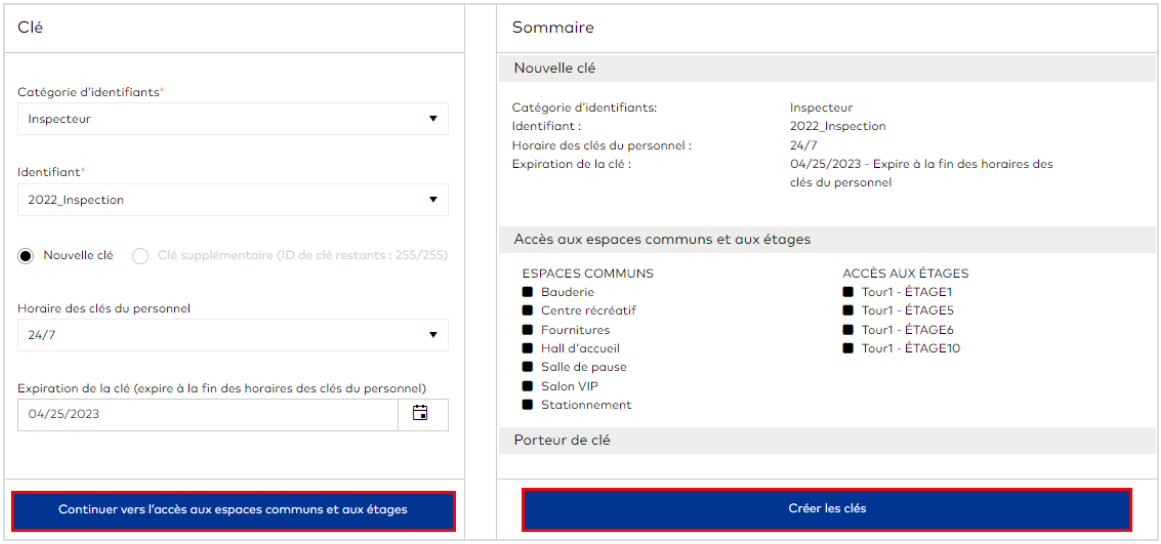
La clé est répertoriée dans l'onglet **Clés attribuées** du profil du membre du personnel/prestataire.



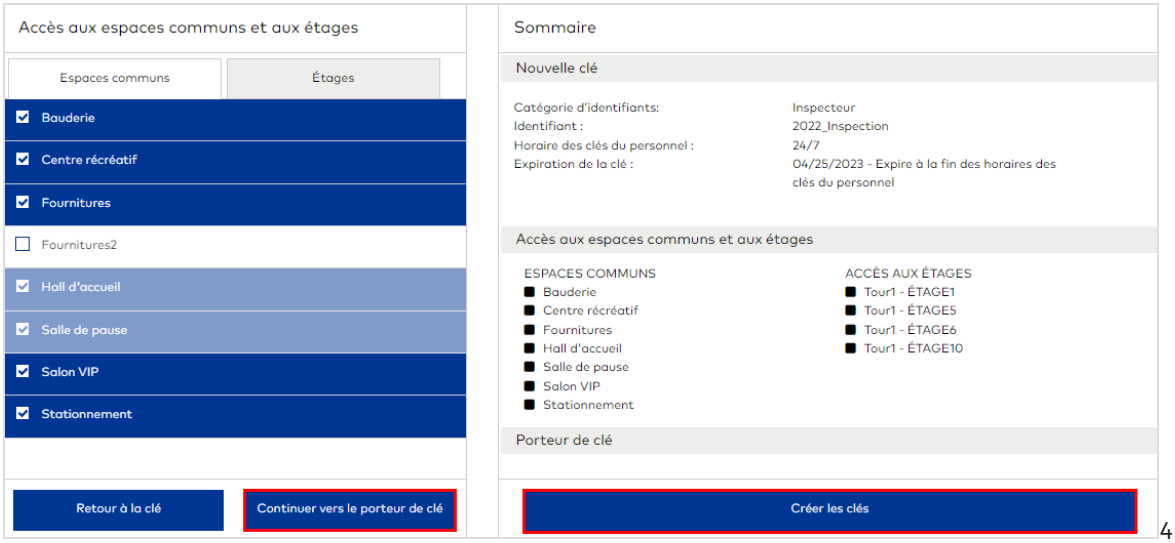
Vous pouvez vérifier qu'une clé mobile a été livrée dans la Gestion du personnel/prestataire.

Créer des clés à usage restreint

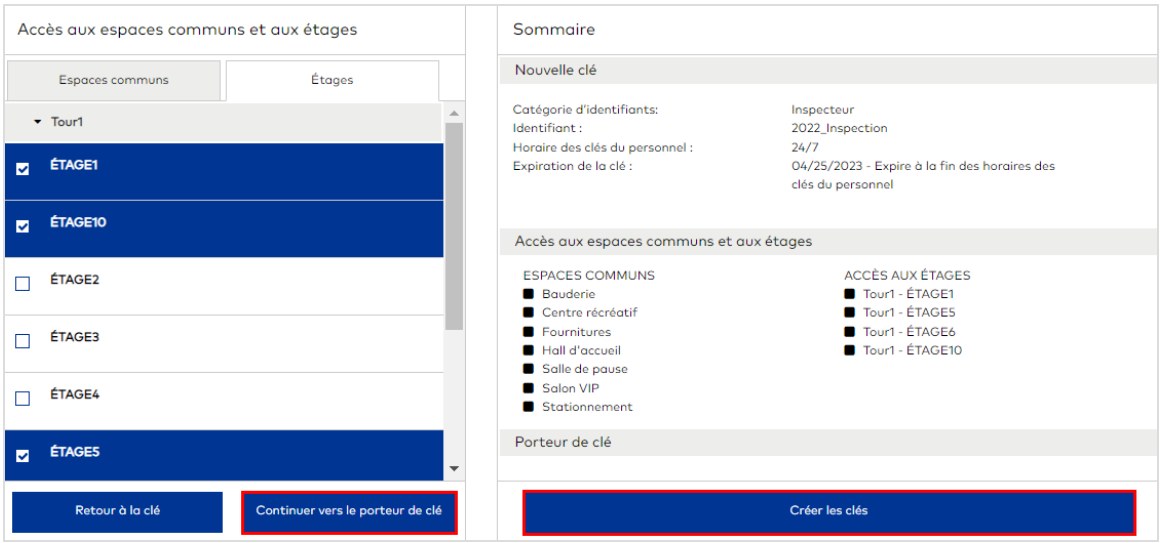
1. Accédez à **Clés du personnel/prestataire**.
2. Sélectionnez la catégorie d'identifiants **Usage restreint** ou une catégorie personnalisée basée sur le type de catégorie Usage restreint. Seules les catégories pour lesquelles les identifiants sont définis figurent dans la liste.
3. Sélectionnez un identifiant. Seuls les identifiants créés à l'aide de la catégorie sélectionnée sont répertoriés.



   Lorsque vous sélectionnez un identifiant, les espaces communs illimités et restreints dont l'accès est activé dans le profil d'accès aux espaces communs associé à l'identifiant sont répertoriés. L'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.
4. Indiquez si vous souhaitez créer une clé avec le mode **Nouveau** ou **Supplémentaire**. Les nouvelles clés invalident les clés actives existantes pour l'identifiant sélectionné à tous les points d'accès, à l'exception des espaces communs. Les clés supplémentaires (copies) n'ont pas d'effet sur les clés actives existantes.
5. Sélectionnez un horaire des clés du personnel. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
6. Indiquez la date après laquelle la clé est invalide.
7. Effectuez l'une des actions suivantes :
   - Cliquez sur **Espaces communs et étages**, **Espaces communs**, ou **Accès aux étages** et passez à l'étape suivante.
   - Cliquez sur **Continuer vers le porteur de clé** et passez à l'étape 10.
8. Sélectionnez les espaces communs et/ou l'accès aux étages à ajouter sur la clé.



4

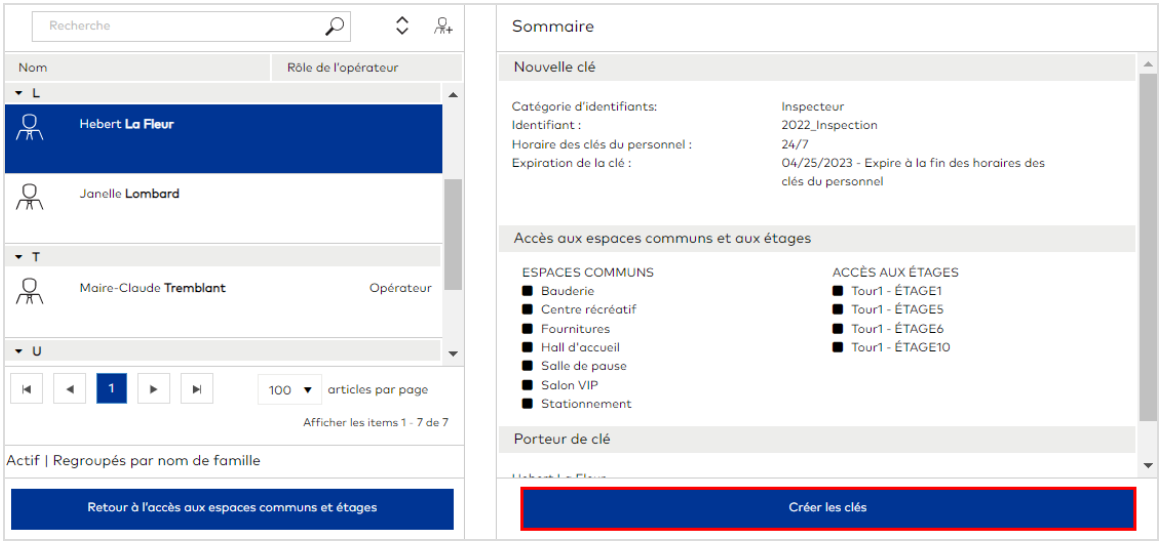


- Lorsque l'onglet **Espaces communs** s'affiche, tous les espaces communs illimités (personnel et résidents) sont sélectionnés par défaut et ne peuvent pas être désélectionnés. Les espaces communs à accès limité (personnel et résidents) sont répertoriés s'ils sont sélectionnés dans un profil d'accès aux espaces communs associé à l'identifiant sélectionné.
- Lorsque l'onglet **Accès aux étages** s'affiche, tous les étages où l'accès aux ascenseurs est configuré sont répertoriés. Par défaut, l'accès aux étages est sélectionné dynamiquement en fonction de l'emplacement des points d'accès à autoriser sur la clé.

Veillez à ne pas supprimer l'accès aux étages par défaut.

Lorsque vous êtes prêt, cliquez sur **Continuer vers le porteur de clé** et passez à l'étape suivante.

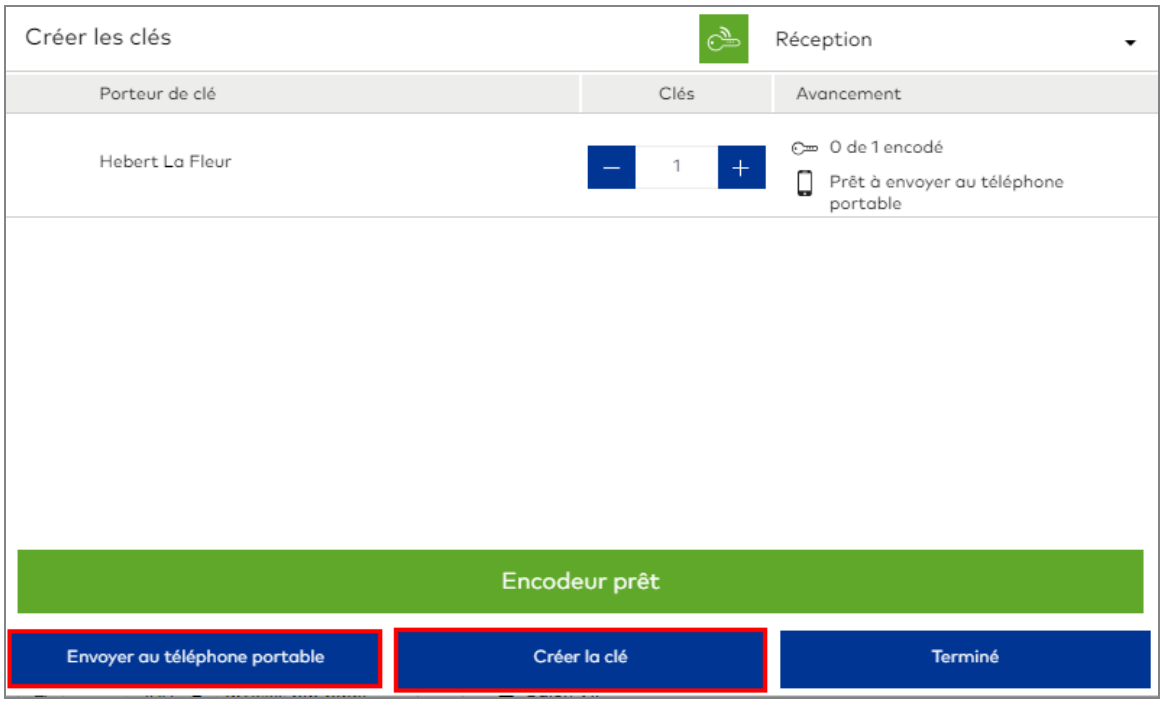
9. Sélectionnez le membre du personnel/prestataire à qui vous souhaitez attribuer la clé. Pour ajouter un membre du personnel/prestataire, cliquez sur **(Ajouter)** , saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.



10. Cliquez sur **Créer les clés**.

> Pour créer une clé mobile, cliquez sur **Envoyer au téléphone portable**.

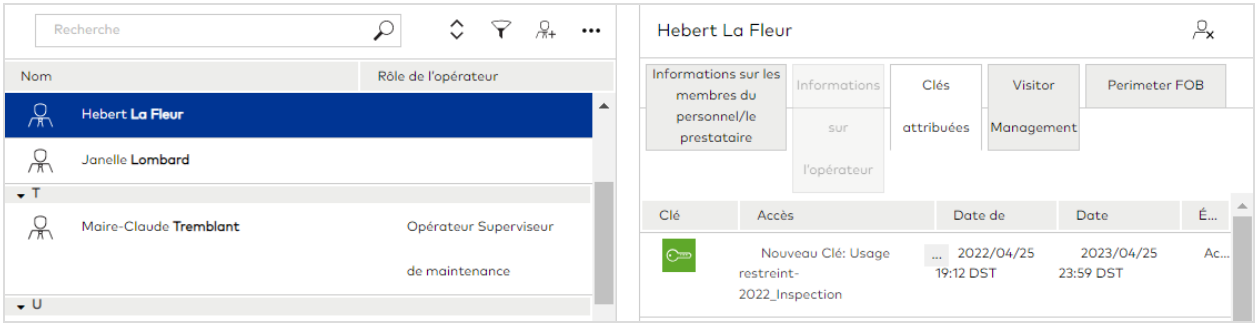
11. Indiquez le nombre de clés à créer.
12. Sélectionnez un encodeur en ligne.
13. Cliquez sur **Créer la clé**.
14. Présentez les clés à l'encodeur (lorsque vous y êtes invité).



Si tous les ID de la clé pour l'identifiant sélectionné sont attribués à des clés actives, un avertissement signale que pour continuer, un ID de la clé existant doit être sélectionné. Pour réutiliser un ID de la clé, cliquez sur **Continuer**, puis sélectionnez l'ID de la clé à réutiliser. Une seule clé peut être créée. La réutilisation des ID de la clé entraîne l'attribution de plusieurs porteurs de clés à une même clé et réduit la traçabilité lors des audits. Les porteurs de clés utilisant le même ID de la clé ne sont pas des porteurs de clés absolus.

15. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

La clé est répertoriée dans l'onglet **Clés attribuées** du profil du membre du personnel/prestataire.



Vous pouvez vérifier qu'une clé mobile a été livrée dans la **Gestion du personnel/prestataire**.

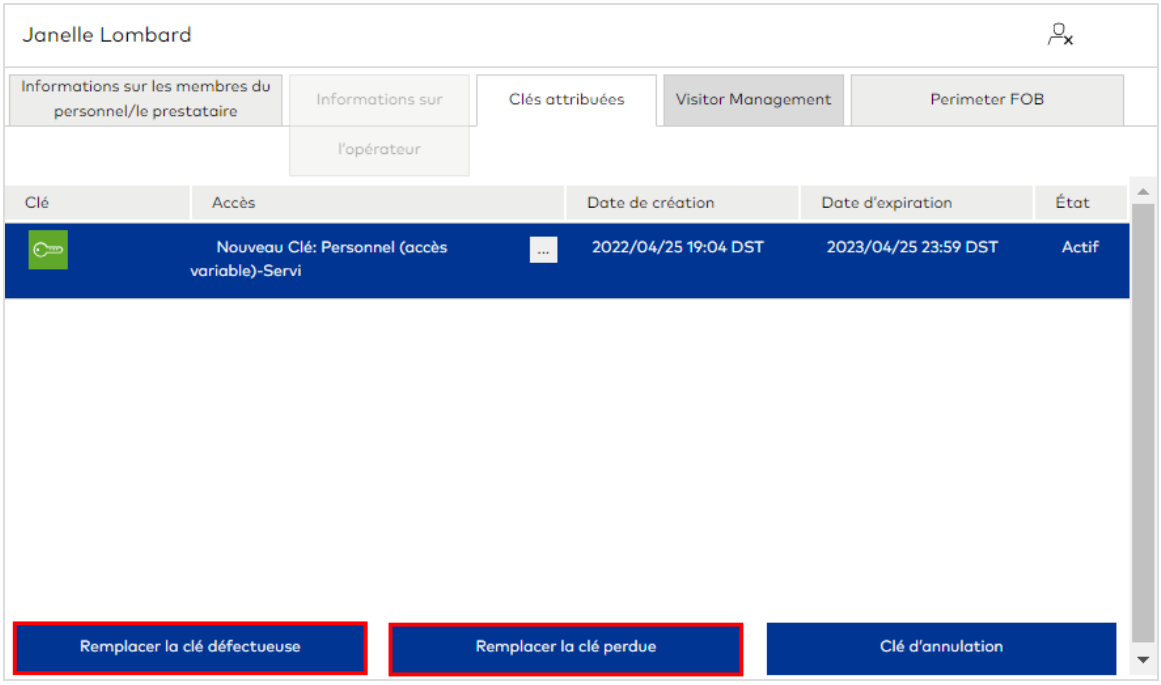
Remplacer les clés du personnel/prestataire

Les clés du personnel/prestataire défectueuses ou perdues peuvent être remplacées.

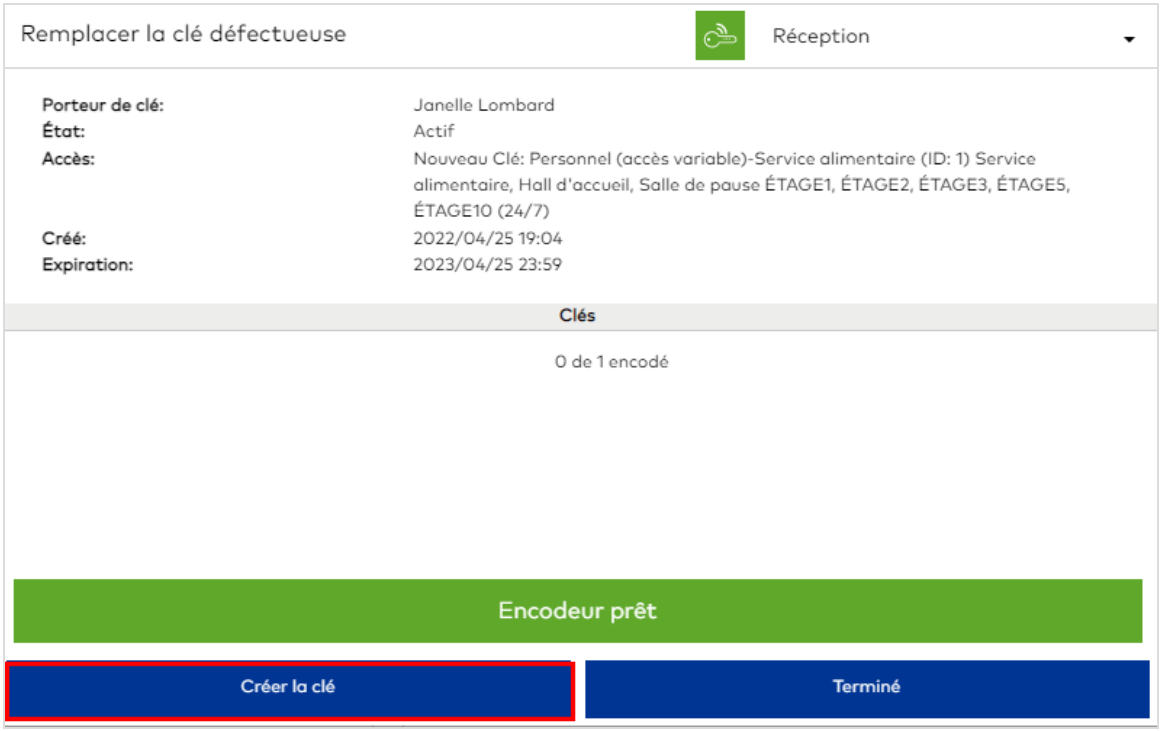
1. Accédez à **Gestion du personnel/prestataire**.



2. Sélectionnez le membre du personnel pour lequel vous souhaitez remplacer la clé.
3. Cliquez sur l'onglet **Clés attribuées**.



4. Sélectionnez la clé que vous souhaitez remplacer.
5. Cliquez sur **Remplacer la clé défectueuse** ou **Remplacer la clé perdue**.

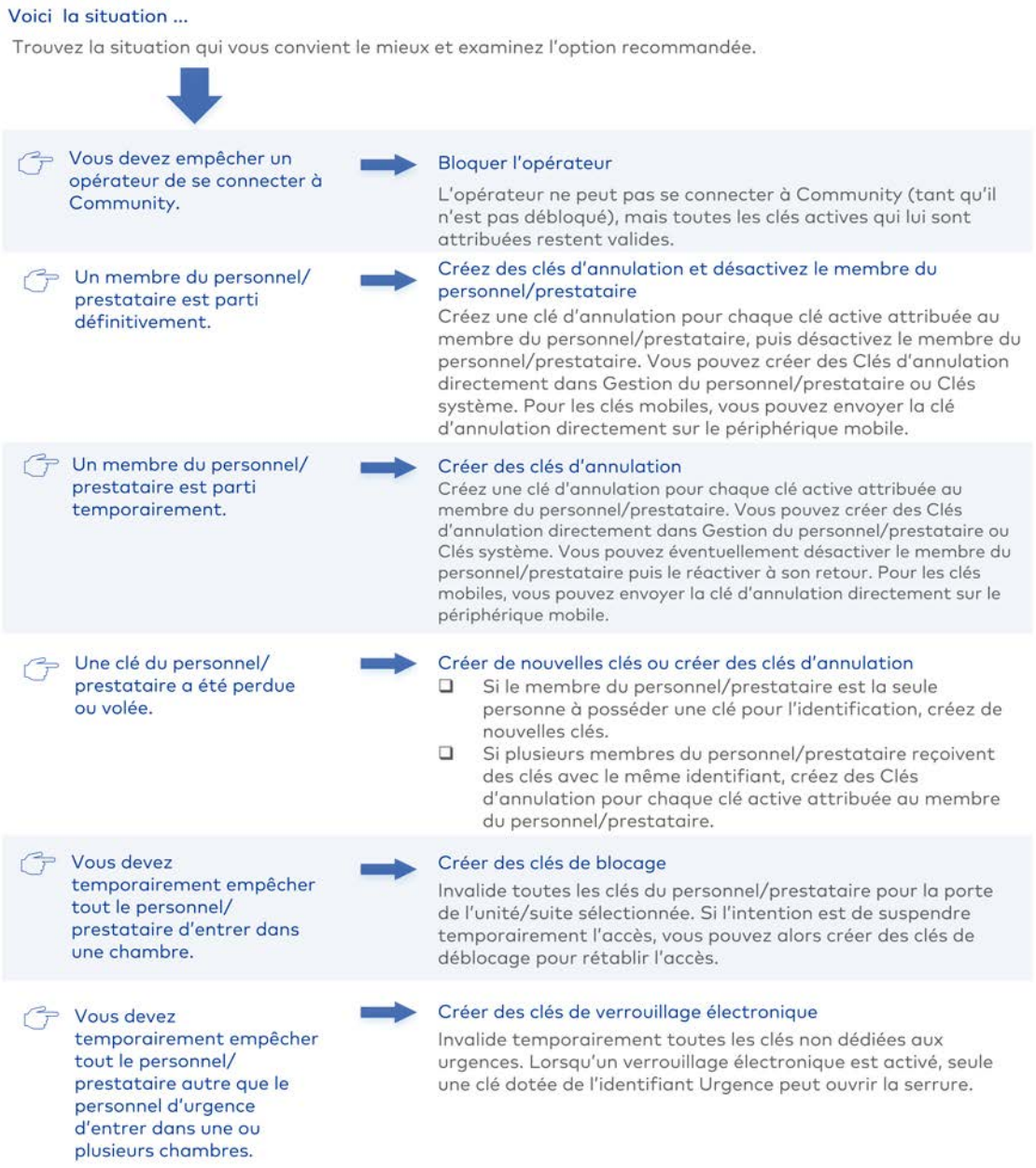


6. (clés perdues uniquement) Cliquez sur **OK** pour confirmer l'opération et reconnaître l'obligation de créer et de présenter une clé d'annulation.
7. Sélectionnez un encodeur en ligne et à disposition du poste de travail.
8. Cliquez sur **Créer la clé**.
9. Présentez une clé à l'encodeur.
10. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Si vous avez remplacé une clé perdue, vous devez également créer une clé d'annulation pour l'instance de clé perdue et la présenter aux points d'accès correspondants.

Invalider l'accès du personnel/prestataire

Il existe de multiples options pour invalider l'accès du personnel/prestataire. La meilleure méthode dépend des modules Community autorisés pour votre compte Opérateur et de la raison pour laquelle vous voulez invalider l'accès.



N'oubliez pas que lorsque vous bloquez l'accès à l'aide d'une clé physique, l'accès reste valide jusqu'à ce que la clé physique d'annulation/blocage/ELO/nouvelle clé est présentée aux verrous concernés.

Bloquer/Débloquer l'accès de l'opérateur

Le blocage d'un opérateur empêche l'opérateur de se connecter à Community. Des opérateurs peuvent être bloqués automatiquement en raison de contrôles de sécurité tels que le dépassement du seuil de connexions échouées ou le non-

renouvellement d'un mot de passe expiré. Si un opérateur est bloqué automatiquement, vous devez rétablir son accès manuellement.

Pour bloquer ou débloquer manuellement l'accès de l'opérateur :

1. Accédez à **Gestion du personnel/prestataire**.
2. Sélectionnez un profil d'opérateur.
3. Cliquez sur l'onglet **Informations sur l'opérateur**.



4. Pour **Bloquer l'accès au logiciel** :
   - Pour bloquer l'accès, déplacez le commutateur sur **OUI**.
   - Pour débloquer l'accès, déplacez le commutateur sur **NON**.
5. Cliquez sur **(Sauvegarder)**.
6. Cliquez sur **OUI** pour confirmer l'action.

Rétrograder l'opérateur

Pour retirer définitivement l'accès opérateur à un membre du personnel/prestataire :

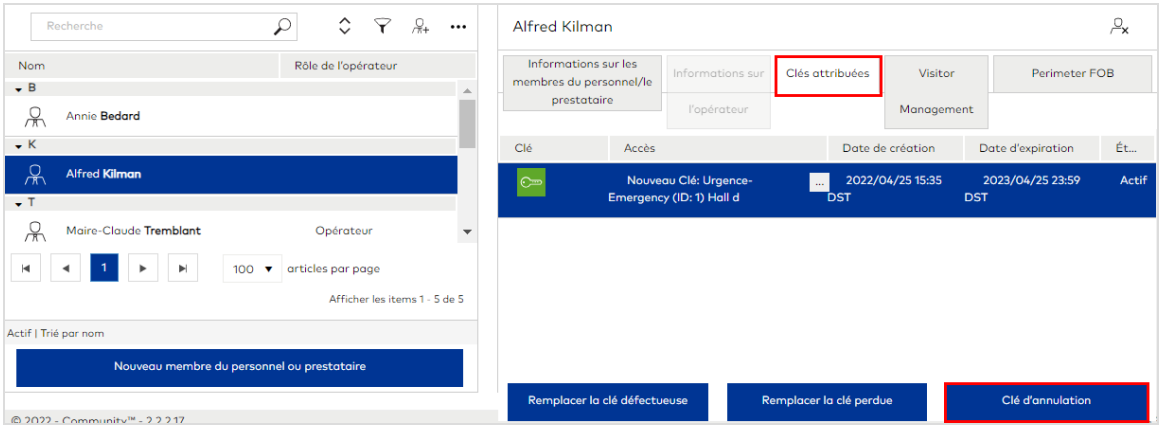
1. Accédez à **Gestion du personnel/prestataire**.
2. Sélectionnez le profil d'opérateur.
3. Dans l'onglet **Informations sur le membre du personnel/prestataire**, basculer le commutateur **Est un opérateur Community ?** vers **NON**.
4. Cliquez sur **(Sauvegarder)**. L'onglet **Informations sur l'opérateur** et l'accès à Community sont bloqués.

Créer des clés d'annulation

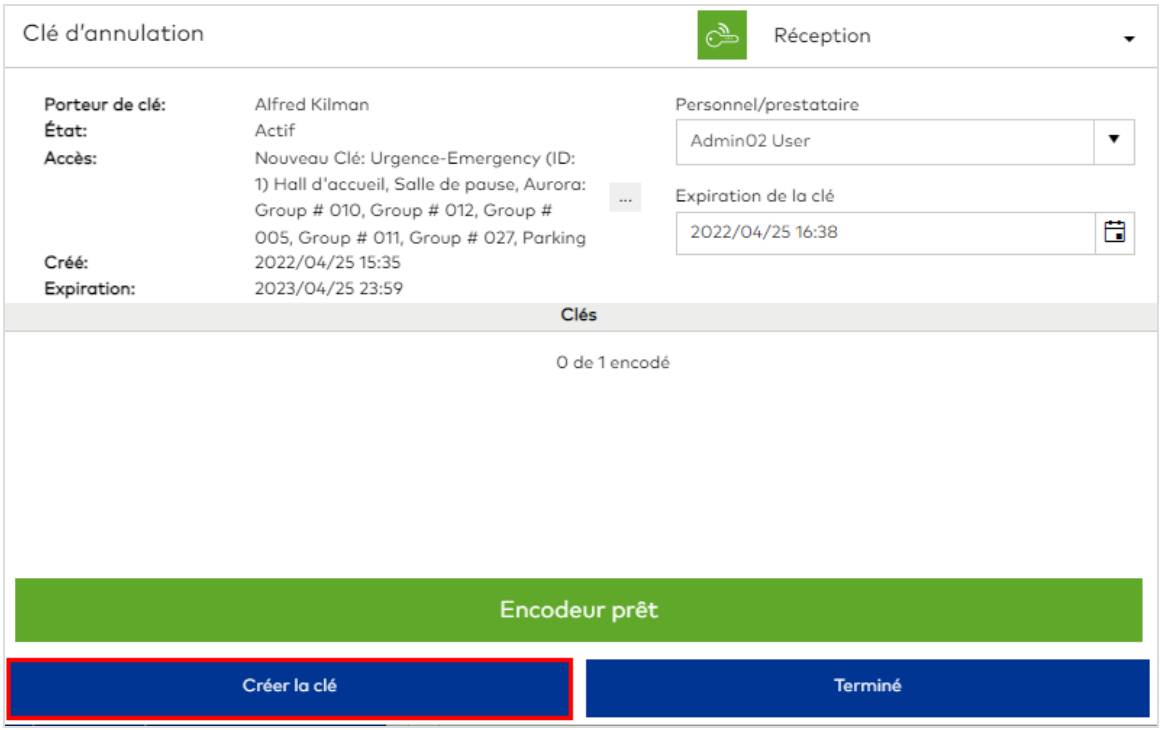
Les clés d'annulation invalident définitivement une seule instance de clé spécifique et doivent être présentées à tous les points d'accès auxquels la clé initiale permet l'accès. Des clés d'annulation peuvent être créées pour annuler les clés du personnel/prestataire dans le module **Gestion du personnel/prestataire** (voir ci-dessous) et dans le module **Clés Système**.

Lors de la création d'une clé d'annulation pour invalider l'accès du personnel/prestataire, vous devez sélectionner la même catégorie d'identifiants/le même identifiant encodé sur la clé que vous souhaitez annuler.

1. Accédez à **Gestion du personnel/prestataire**.
2. Sélectionner un membre du personnel ou un prestataire.
3. Cliquez sur l'onglet **Clés attribuées**.
4. Sélectionnez la clé que vous souhaitez annuler.



5. Cliquez sur **Clé d'annulation**.



6. (*en option/clés physiques uniquement*) Sélectionnez le membre du personnel/prestataire à qui vous souhaitez attribuer la clé.
7. (*en option/clés physiques uniquement*) Définissez la date après laquelle la Clé d'annulation sera invalide.
8. Effectuez l'une des opérations suivantes :
   - Si vous annulez une clé physique, sélectionnez un encodeur en ligne, cliquez sur **Créer la clé** puis présentez la clé à l'encodeur.
   - Si vous annulez une clé mobile, cliquez sur **Créer la clé** pour créer une Clé d'annulation physique et/ou cliquez sur **Annuler la clé mobile** pour annuler la clé mobile à distance. Les Clés d'annulation physiques doivent être présentées aux points d'accès pour invalider une clé mobile.
9. Lorsqu'un message vous indique que la création de la clé est réussie, cliquez sur **Terminé**. Vous pouvez vous assurer que les clés mobiles sont annulées dans l'onglet **Clés attribuées** du profil du membre du personnel/prestataire.

Désactiver le personnel/les prestataires

La désactivation du personnel/des prestataires annule tout accès pour le membre du personnel/prestataire. Si Gestion des visiteurs est activée, tous les codes PIN attribués actifs sont définitivement annulés. De plus, le personnel ayant été promu opérateur ne peut pas se connecter à Community. Des membres du personnel peuvent être désactivés automatiquement en raison de contrôles de sécurité tels que le non-renouvellement d'un mot de passe expiré. En cas de désactivation automatique d'un membre du personnel, vous devez (ré)activer le membre du personnel manuellement.

1. Accédez à **Gestion du personnel/prestataire**.



2. Sélectionnez un profil.
3. Cliquez sur **(Désactiver l'utilisateur)** .
4. Cliquez sur **OUI** pour confirmer.

Activer le personnel/prestataire

1. Accédez à **Gestion du personnel/prestataire**.



2. Cliquez sur **(Filtrer)** .
3. Sélectionnez l'onglet **Désactivé** et éventuellement le filtre pour les opérateurs uniquement.
4. Sélectionnez un profil.
5. Cliquez sur **(Activer l'utilisateur)** .
6. Cliquez sur **OUI** pour confirmer.

Si vous activez un opérateur, vous devrez peut-être aussi débloquer l'opérateur pour permettre la connexion Community.

Créer de nouvelles clés

La création d'une nouvelle clé invalide automatiquement l'accès à l'identifiant sélectionné, à l'exception des espaces communs, sur toutes les clés précédemment actives. Par exemple, la NouvelleClé1 pour les unités 100 et 101 expire demain à 13 heures. Si vous créez une NouvelleClé2 pour l'unité 100, NouvelleClé1 devient invalide pour l'unité 100 dès que vous présentez NouvelleClé2 à la serrure installée dans l'unité 100. NouvelleClé1 ne reste valide que pour l'unité 101.

Les nouvelles clés n'invalident pas l'accès aux espaces communs avec les clés existantes. L'accès aux espaces communs est valide jusqu'à l'expiration de la clé. Si l'identifiant comprend l'accès aux espaces communs, créez des clés d'annulation pour invalider l'accès (au lieu de nouvelles clés).

Créer des clés de blocage/déblocage

Les clés de blocage invalident toutes les instances d'un identifiant spécifique. Bien que vous puissiez utiliser la clé de blocage pour invalider l'accès de manière permanente, la clé de blocage est associée à la clé de déblocage pour suspendre

puis rétablir l'accès. Par exemple, créez une clé de blocage pour *identifiantA* pour suspendre l'accès à tous les points d'accès inclus dans identifiantA ; ensuite, créez une clé de déblocage pour *identifiantA* pour rétablir l'accès pour toutes les clés actives.

Lors de la création d'une clé de blocage pour invalider l'accès du personnel/prestataire, vous devez sélectionner la même catégorie d'identifiants/le même identifiant encodé sur la clé que vous souhaitez bloquer.

Après avoir bloqué l'accès, la clé de déblocage ne débloque pas l'accès aux espaces communs lorsque l'accès est basé sur un profil d'accès aux espaces communs.

Pour les instructions, voir Clés de blocage/déblocage.

Créer des clés ELO

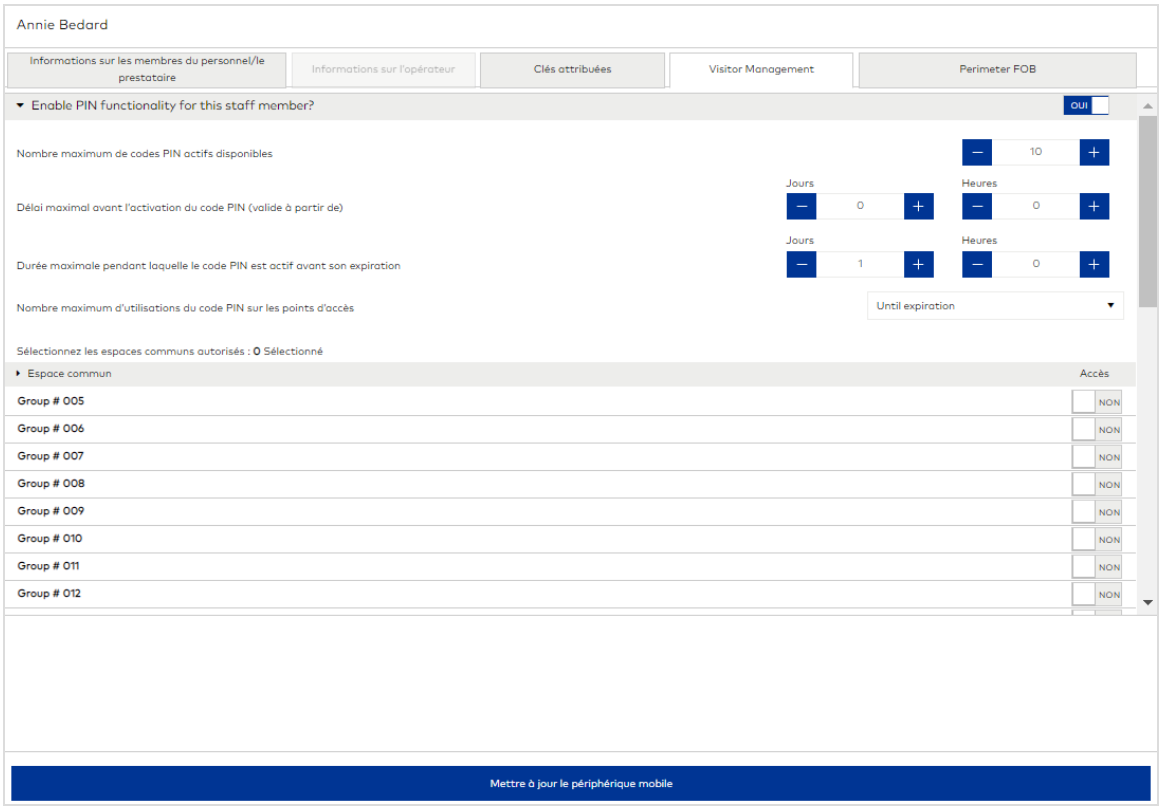
Les clés de blocage électronique (ELO) invalident temporairement toutes les clés non dédiées aux urgences en verrouillant à double tour la porte de l'extérieur (activer le commutateur d'intimité ou le pêne dormant). Lorsqu'un blocage électronique est activé, seule une clé dotée de l'identifiant Urgence peut ouvrir la serrure. Lorsque le blocage électronique est désactivé, l'accès par clé standard est rétabli.

Pour les instructions, voir Clés de blocage électronique.

Configurer la gestion des visiteurs pour les membres du personnel/prestataires

Pour configurer la fonctionnalité PIN pour un membre du personnel ou un prestataire :

1. Accédez à **Gestion du personnel/prestataire**.
2. Sélectionnez le profil d'un membre du personnel/prestataire.
3. Cliquez sur l'onglet **Gestion des visiteurs**.



4. Configurer les options d'attribution de codes PIN :
   - **Activer la fonctionnalité PIN pour ce membre du personnel** — Lorsque cette fonctionnalité est activée, la section PIN s'affiche, les paramètres PIN peuvent être personnalisés et mis à jour sur les périphériques mobiles.
   - **Nombre maximum de codes PIN actifs disponibles** — Indiquez le nombre maximum de codes PIN qui peuvent être actifs. Valeurs valides : 1-50.
   - **Délai maximal avant l'activation de la clé mobile (valide à partir de)** — Indiquez le nombre maximal de jours/heures pendant lesquels le membre du personnel peut créer un code PIN avant que l'accès autorisé par code PIN ne commence. Plage : 0-30 jours/0-23 heures.
   - **Durée maximale pendant laquelle le code PIN est actif avant d'expirer** — Indiquez le nombre maximal de jours/heures pendant lesquels un code PIN peut être actif. Plage : 0-30 jours/0-23 heures.
   - **Nombre maximum de fois que le code PIN peut être utilisé dans les points d'accès** — Indiquez le nombre maximum de fois qu'un code PIN peut être utilisé dans les points d'accès. Valeurs valides : Jusqu'à expiration, 1-5.
   - **Espaces communs autorisés** — Sélectionnez les espaces communs dont l'accès est autorisé par le code PIN. Au moins un espace commun doit être sélectionné.
5. Cliquez sur **Sauvegarder**.
6. Pour mettre à jour les paramètres sur le périphérique mobile du membre du personnel/prestataire, cliquez sur **Mettre à jour le périphérique mobile**.

Programmation/Audit

Cette section comprend les sujets suivants :

Reprogrammer des serrures 221
Audit des serrures 223
Auditer les points d'accès en ligne 224

Pour en savoir plus, voir « En savoir plus sur la Programmation et audit » dans **Configuration du site**.

Reprogrammer des serrures

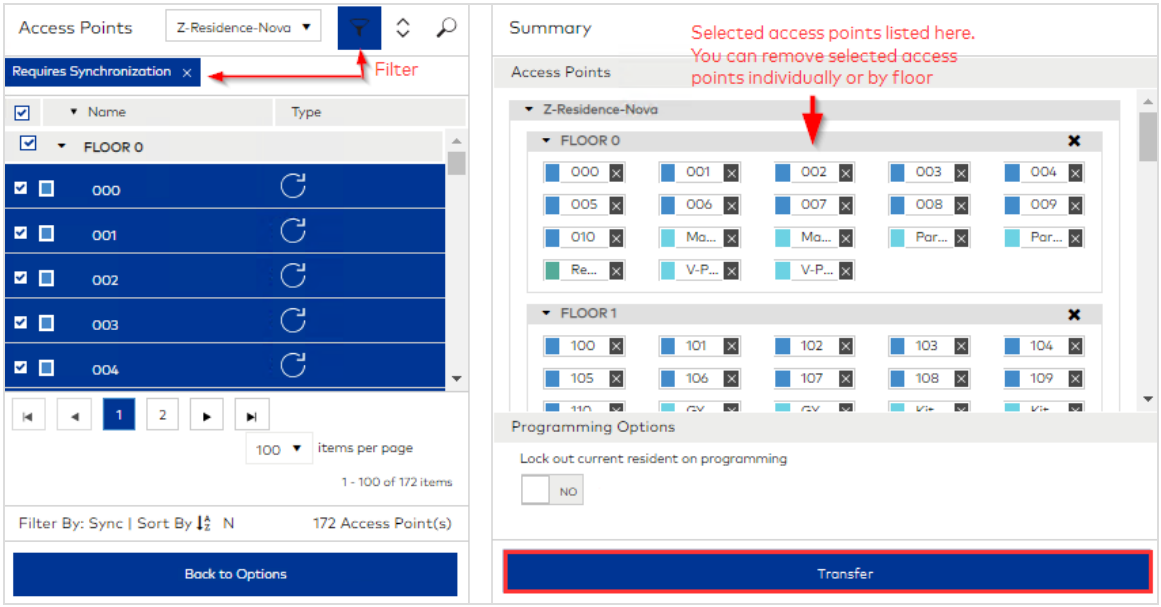
Les serrures doivent être reprogrammées chaque fois que les données de configuration affectant le point d'accès sont modifiées dans Community. Pour obtenir une liste des points d'accès (serrures) à reprogrammer, voir « Programmation du point d'accès requise ».

Certaines étapes de programmation sont effectuées sur le M-Unit (Programmateur M-Unit). Pour les instructions officielles, reportez-vous à la documentation fournie avec votre périphérique. Si l'authentification du programmateur M-Unit est activée dans ***Paramètres du système > Sécurité > Programmateur M-Unit***, les identifiants doivent être configurés pour au moins un opérateur dans **Gestion du personnel/prestataire**.

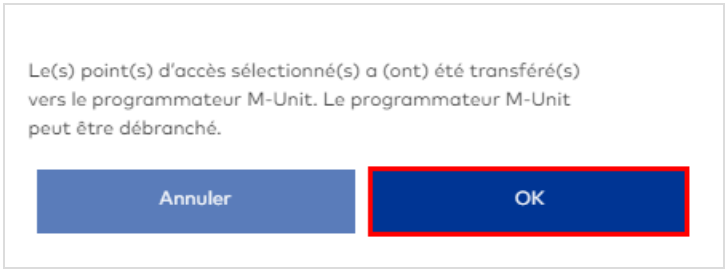
Un problème avec Microsoft empêche le navigateur Edge de détecter/se connecter à un Programmateur M-Unit. Les points d'accès ne peuvent donc pas être programmés ou audités sans intervention. Ouvrez l'Invite de commande et envoyez la commande suivante :
C:\windows\system32\CheckNetIsolation.exe LoopbackExempt –a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe

Pour reprogrammer des serrures :

1. Accédez à ***Programmation et audit > Programmation***.



2. Sélectionnez les points d'accès que vous souhaitez synchroniser avec les données de configuration Community. Vous pouvez sélectionner des points d'accès de différents bâtiments et filtrer la liste pour n'afficher que les points d'accès nécessitant une synchronisation. Les points d'accès sélectionnés s'affichent dans la section **Sommaire** organisés par bâtiment et par étage.
3. Pour **Bloquer les résidents actuels lors de la programmation**, indiquez si vous souhaitez invalider toutes les clés actives affectées aux résidents après la programmation de la serrure. Si vous sélectionnez **Oui**, de nouvelles clés (résident) doivent être créées et remises après la programmation des serrures.
4. Connectez le programmateur M-Unit au poste de travail.
5. Dans Community, cliquez sur **Transfert**. Des messages s'affichent sur le poste de travail et le programmateur M-Unit pour indiquer que le transfert est en cours. Patientez jusqu'à ce que le message s'affichant sur le poste de travail indique que le transfert est terminé et que vous pouvez débrancher le programmateur M-Unit.



6. Cliquez sur **OK**.
7. Déconnectez le programmateur M-Unit du poste de travail. Les étapes restantes sont effectuées sur M-Unit.
8. Si le mode de sécurité renforcée est activé, indiquez le mot de passe de sécurité de M-Unit. Le mot de passe s'affiche dans ***Paramètres du système > Sécurité > Mode de sécurité renforcée***. (Dans certains cas, M-Unit affiche un message avant l'invite de mot de passe indiquant que l'unité n'est pas personnalisée ; il suffit de sélectionner OK.)
9. Si l'authentification de M-Unit est activée, indiquez les identifiants de connexion de M-Unit.
10. Dans le menu du programmateur M-Unit, sélectionnez **SERRURES**.
11. Utilisez les flèches HAUT/BAS pour afficher **1 - Programme** en surbrillance, puis appuyez sur **ENTRÉE**. Les noms des points d'accès s'affichent par groupes de cinq.
12. Sélectionnez le nom du point d'accès pour la serrure, puis appuyez sur **ENTRÉE**. Utilisez les options **PRÉC**, **SUIV** et **RECHERCHER** pour parcourir et affiner la liste des noms.
13. Sélectionnez le type de sonde que vous utilisez pour connecter le programmateur M-Unit à la serrure.
14. Lorsque vous y êtes invité(e), insérez la sonde dans la serrure. La programmation démarre immédiatement. Si la serrure a déjà été programmée, le programmateur M-Unit émet un message demandant confirmation pour remplacer la programmation existante.
15. Lorsqu'un message vous indique que la programmation est terminée, cliquez sur **OK**.

Une bonne pratique consiste à tester les serrures avec des clés valides à l'issue de la programmation.

Audit des serrures

Cette procédure explique comment auditer les serrures à l'aide de la procédure du programmateur M-Unit. Si moins de cinq serrures sont auditées à des fins de dépannage, l'utilisation d'une clé d'audit est une alternative à la procédure du programmateur M-Unit. Veuillez vous reporter à « Clés à fonction spéciale » dans **Clés Système**.

Certaines étapes sont effectuées sur le M-Unit (Programmateur M-Unit). Pour les instructions officielles, reportez-vous à la documentation fournie avec votre périphérique. Si l'authentification du programmateur M-Unit est activée dans ***Paramètres du système > Sécurité > Programmateur M-Unit***, les identifiants doivent être configurés dans **Gestion du personnel/prestataire** pour au moins un opérateur.

Un problème avec Microsoft empêche le navigateur Edge de détecter/se connecter à un Programmateur M-Unit. Les points d'accès ne peuvent donc pas être programmés ou audités sans intervention. Ouvrez l'Invite de commande et envoyez la commande suivante :
C:\windows\system32\CheckNetIsolation.exe LoopbackExempt –a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe

Pour auditer des serrures :

1. Connectez M-Unit à la serrure que vous souhaitez auditer.
2. Dans le menu du programmateur M-Unit, sélectionnez **SERRURES**.
3. Utilisez les flèches HAUT/BAS pour afficher **Sélectionner 3 - Interroger** en surbrillance, puis appuyez sur **ENTRÉE**. M-Unit émet un message indiquant le nombre maximal d'enregistrements d'interrogation.
4. Appuyez sur **ENTRÉE** pour procéder à l'audit.
5. Sélectionnez le type de sonde que vous utilisez pour connecter le programmateur M-Unit à la serrure.
6. Lorsque vous y êtes invité(e), insérez la sonde dans la serrure. L'audit démarre immédiatement. Si un fichier d'interrogation existe déjà pour la serrure, le programmateur M-Unit émet un message demandant confirmation de remplacer le fichier existant. Le programmateur M-Unit émet un message invitant à réaliser des audits supplémentaires.
7. Lorsque tous les audits sont terminés, sélectionnez **NON**.
8. Connectez le programmateur M-Unit au poste de travail Community.
9. Dans Community, accédez à **Programmation et audit**.
10. Cliquez sur **Audit**. Tous les fichiers d'interrogation de points d'accès stockés sur M-Unit sont listés.
11. Sélectionnez les fichiers d'interrogation que vous souhaitez transférer.
12. Choisissez de supprimer ou non l'audit de serrure de M-Unit à l'issue du transfert. Les fichiers d'interrogation sur le programmateur M-Unit peuvent être enregistrés indéfiniment ou supprimés après le transfert du fichier vers Community.
13. Cliquez sur **Transfert**.
14. Lorsqu'un message vous indique que le transfert est terminé, cliquez sur **OK**. Tous les fichiers d'interrogation sont stockés sur le serveur Community et sont accessibles à partir du **Rapport d'audit de point d'accès**.

Auditer les points d'accès en ligne

Cette option s'affiche lorsque la fonction de communication en ligne sous licence est activée.

Si la communication en ligne est activée dans les **Paramètres du système**, les points d'accès en ligne peuvent être audités directement dans Community. Tous les points d'accès en ligne sont répertoriés avec les informations suivantes :

- **Point d'accès** — Le nom du point d'accès.
- **Catégorie** — Le type de point d'accès : Unité, Suite, Accès privé, Espace commun.
- **État** — L'état de connectivité du point d'accès, En ligne/Hors ligne.
- **Date** — La date du dernier audit.

Pour auditer un point d'accès en ligne :

1. Accédez à ***Programmation et audit > Points d'accès en ligne***.
2. Sélectionnez un point d'accès.
3. Cliquez sur **Auditer des points d'accès**.

Une fois l'audit terminé, le fichier est accessible depuis la section **Sommaire**.

Clés système

Cette section comprend les sujets suivants :

- En savoir plus sur les clés Système 226
- Clés de blocage et de déblocage 230
- Clés d'annulation 234
- Clés de diagnostic 237
- Clés de bascule de verrouillage électronique 239
- Clés à sécurité intégrée 241
- Clés d'annulation 242
- Clés de verrouillage et de déverrouillage 244
- Clés de programmation primaire et secondaire 246
- Clés de reséquence 249
- Clés à fonction spéciale 251

En savoir plus sur les clés Système

Le module **Clés Système** sert à encoder des clés pour une intervention immédiate et à effectuer une programmation opérationnelle avancée.

Clés de blocage et déblocage

Créer une clé de blocage pour invalider toutes les instances d'un identifiant spécifique. Par exemple, créez une clé de blocage pour invalider toutes les clés actives pour l'unité 100. Lorsque vous créez une clé de blocage, vous devez sélectionner la catégorie d'identifiants et l'identifiant encodé sur la clé que vous souhaitez bloquer. Si l'intention est de bloquer temporairement l'accès, vous pouvez utiliser une clé de déblocage pour débloquer une clé qui était auparavant bloquée par une clé de blocage.

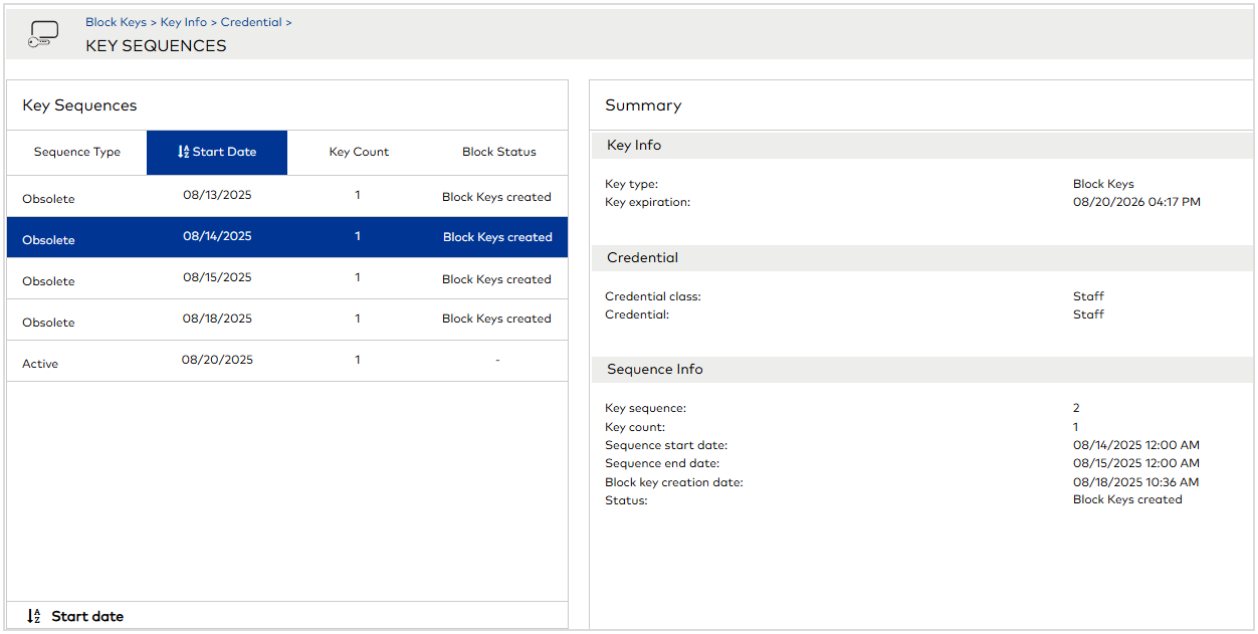
Lorsque la fonction de communication en ligne sous licence est activée, l'opération à distance est prise en charge.

N'oubliez pas que la clé de blocage doit être présentée aux points d'accès avant que l'accès ne soit bloqué.

Blocage des séquences de clés obsolètes

Les clés de blocage peuvent désormais être utilisées pour bloquer des séquences entières de clés obsolètes. Cette option est disponible pour les clés encodées avec un identifiant basé sur la catégorie d'identifiants Personnel, Personnel (accès variable), Prestataire ou Usage restreint.

Les clés peuvent être obsolètes lorsqu'une nouvelle clé avec le même identifiant a été créée et/ou que l'accès a été supprimé avant l'expiration. Les clés obsolètes continuent à permettre l'accès aux espaces communs et aux contrôleurs d'ascenseurs jusqu'à l'expiration de la clé. dormakaba recommande de bloquer les clés obsolètes.



En sélectionnant un identifiant, les séquences de clés s'affichent. Une séquence de clés représente chaque fois qu'une nouvelle clé (et non une clé supplémentaire) a été créée. Chaque fois qu'une nouvelle clé (nouvelle séquence de clés) est créée, la séquence précédente devient obsolète. Le blocage d'une séquence de clés bloque toutes les clés de cette séquence, ainsi que toutes les clés des séquences de clés dont la date de début est antérieure.

La page Séquences de clés contient les informations suivantes :

Séquences des clés :

- **Type de séquence** — État actuel de la séquence de clés : Obsolète ou Actif.
- **Date de début** — Date à laquelle la séquence de clés a été créée. Il s'agit également de la date à laquelle la séquence de clés a été encodée sur la première (nouvelle) clé.
- **Nombre de clés** — Nombre de clés créées à l'aide de la séquence de clés. « 1 » indique que seule la première ou la nouvelle clé a été créée. Toutes les valeurs supérieures à 1 indiquent le nombre de clés supplémentaires (total - 1).
- **État du blocage** — État actuel des clés encodées avec la séquence de clés sélectionnée. L'état indique la méthode de blocage :
  - **Clés de blocage créées** — Une clé de blocage physique a été créée pour la séquence de clés sélectionnée ou une séquence de clés plus récente.
  - **Bloqué** — Lorsque la communication en ligne est activée et que la commande Bloquer des clés à distance est émise pour la séquence de clés sélectionnée ou une séquence plus récente.

  La valeur reflète l'action la plus récente pour bloquer la séquence de clés sélectionnée ou une séquence plus récente. Par exemple, si la séquence de clés active de la figure ci-dessus est bloquée à distance, l'état de toutes les lignes passe à « Bloqué ».

Sommaire :

- **Informations sur la clé**
  - **Type de clé** — Clés de blocage.
  - **Expiration de la clé** — Date et heure sélectionnées pour l'expiration de la clé de blocage.
- **Identifiant**
  - **Catégorie d'identifiants** — Nom de la catégorie d'identifiants.
  - **Identifiant** — Nom de l'identifiant.
- **Informations sur la séquence** — S'affiche uniquement lorsque la catégorie d'identifiants est Personnel, Personnel (accès variable) ou Prestataire, Usage restreint.
  - **Séquence de clés** — Ordre dans lequel la séquence de clés a été créée. Par exemple, la séquence de clés 2 a été créée avant la séquence de clés 3.
  - **Nombre de clés** — Nombre total de clés créées à l'aide de la séquence de clés. « 1 » indique que seule la première ou la nouvelle clé a été créée. Toutes les valeurs supérieures à 1 indiquent la somme de la première nouvelle clé et de toutes les clés supplémentaires créées.
  - **Date de début de la séquence** — Date à laquelle la séquence de clés a été créée. Il s'agit également de la date à laquelle la séquence de clés a été encodée sur la première (nouvelle) clé.
  - **Date de fin de séquence** — Date à laquelle les clés créées à l'aide de la séquence de clés sont devenues obsolètes. Il s'agit également de la date de début de la séquence de clés suivante.
  - **Date de création de la clé de blocage** — Date à laquelle la dernière action de blocage a été effectuée sur la séquence de clés.
  - **État** — État actuel des clés encodées avec cette séquence de clés. L'état indique la méthode de blocage : Clés de blocage créées ou bloquées. La valeur reflète l'action la plus récente pour bloquer cette séquence de clés ou une séquence plus récente. Par exemple, si la séquence de clés active de la figure ci-dessus est bloquée à distance, l'état de toutes les lignes passe à « Bloqué ».

Clés d'annulation

Créez une clé d'annulation pour invalider définitivement une instance de clé spécifique. Lorsque vous créez une clé d'annulation dans Clés Système, vous devez sélectionner la catégorie d'identifiants et l'identifiant encodé sur la clé que vous souhaitez annuler. Une clé d'annulation doit être présentée à tous les points d'accès pour lesquels la clé initiale dispose d'identifiants.



Lorsque la fonction de communication en ligne sous licence est activée, l'opération à distance est prise en charge.

Clés de diagnostic

Les clés de diagnostic interrogent des serrures pour extraire l'état de diverses fonctions de serrures, le plus souvent à des fins de résolution de problèmes et de reporting. Les résultats de l'interrogation sont communiqués par une séquence de clignotements LED.

Clés ELO

Les clés de blocage électronique (ELO) invalident temporairement toutes les clés non dédiées aux urgences en verrouillant à double tour la porte de l'extérieur (activer le commutateur d'intimité ou le pêne dormant). Lorsqu'un blocage électronique est activé, seule une clé dotée de l'identifiant Urgence peut ouvrir la serrure. Lorsque le blocage électronique est désactivé, l'accès par clé standard est rétabli. Les clés ELO sont des clés de commutation. Le comportement de la clé alterne (applique le verrouillage/supprime le verrouillage) à chaque fois qu'elle est présentée à la serrure.

Lorsque la fonction de communication en ligne sous licence est activée, l'opération à distance est prise en charge.

Clés à sécurité intégrée

Les clés à sécurité intégrée sont des clés de rechange de clés d'unités individuelles créées à l'avance et conservées en jeux complets à remettre en cas de défaillance système ou de panne de courant. Toutes les clés à sécurité intégrée sont encodées avec un accès par défaut aux étages et aux espaces communs.

Il est recommandé de créer et de toujours conserver trois jeux de deux clés pour chaque unité et unité de suite. Vous pouvez créer autant de jeux de clés que nécessaire ; cependant, lorsqu'une clé d'un jeu est présentée à la serrure, toutes les clés d'un jeu utilisé précédemment sont invalidées.

Les paramètres par défaut pour les clés à sécurité intégrée sont définis dans ***Paramètres du système > Clés à sécurité intégrée***.

Il est primordial que les clés à sécurité intégrée soient à jour et stockées dans un système d'archivage efficace dans un emplacement sécurisé.

Clés d'annulation

Les clés d'annulation sont utilisées pour annuler définitivement l'accès d'un résident actuel. Le plus souvent, les clés d'annulation sont utilisées par le personnel après le départ d'un résident avant l'expiration de la clé. Les clés d'annulation invalident toutes les clés de résidents encodées avec accès à l'unité, même si le pêne dormant ou le verrou d'intimité est actionné.

Lorsque la fonction de communication en ligne sous licence est activée, l'opération à distance est prise en charge.

Clés de verrouillage, déverrouillage et clés de bascule de libre passage

Les clés de verrouillage désactivent le mode passage. L'accès est restreint aux seules personnes dont les clés sont encodées avec l'identifiant correspondant. Les clés de déverrouillage activent le mode passage. Le mode passage est un état de la serrure au cours duquel les contrôles d'accès programmés dans la serrure sont suspendus afin de permettre un libre accès. Les clés de bascule de libre passage activent et désactivent alternativement le mode passage.

Clés de programmation primaire et secondaire

Les clés de programmation primaire (PPK) mettent la serrure en mode de programmation et sont utilisées conjointement avec les clés d'informations sur la programmation (PI) et les clés d'état de la programmation (PS) pour programmer des serrures et autoriser des fonctions spéciales (voir Créer une clé à fonction spéciale). Elles servent également à reprogrammer la Clé de programmation secondaire (SPK) actuelle ou à réinitialiser une clé SPK différente. Les clés de programmation secondaire (SPK) reprogramment ou resynchronisent la clé de programmation primaire (PPK) actuelle sur des points d'accès et réinitialisent une clé PPK différente sur une serrure. Essentiellement, une clé SPK est une clé de rechange pour la clé PPK mais ne met pas les clés en mode de programmation.

Clés de reséquence

Les clés de reséquence resynchronisent un identifiant d'une clé spécifique sur des points d'accès. La clé de reséquence est utilisée pour actualiser le nombre de séquences stockées dans la mémoire de la serrure lorsque le nombre de nouvelles clés créées mais non utilisées dans la serrure dépasse la plage de séquences programmées pour cette clé.



Lorsque la fonction de communication en ligne sous licence est activée, l'opération à distance est prise en charge.

Clés à fonction spéciale

Les clés à fonction spéciale sont assignées à des clés de programmation primaire pour effectuer des opérations de niveau système sur une serrure.

Clés de blocage et de déblocage

Créez une clé de blocage pour bloquer toutes les instances de clé actives d'un identifiant spécifique. Pour les clés du personnel basées sur la catégorie d'identifiants Personnel, Personnel (accès variable), Prestataire et Usage restreint, vous pouvez également bloquer toutes les instances de clés obsolètes. Avant de créer une clé de blocage, vous devez connaître la catégorie d'identifiants et l'identifiant (ou point d'accès) que vous souhaitez bloquer.

Étant donné que les clés dont l'état est *Obsolète* continuent à donner accès aux espaces communs et aux contrôleurs d'ascenseurs jusqu'à l'expiration de la clé, dormakaba recommande vivement d'utiliser des clés de blocage sur les serrures où les clés sont obsolètes. Lors de la création de la clé de blocage, sélectionnez la séquence de clés. N'oubliez pas de présenter les clés de blocage physiques pour accéder aux espaces communs nécessaires et aux contrôleurs d'ascenseurs.

Avant de bloquer un espace commun, notez que la clé de déblocage ne rétablit pas l'accès aux espaces communs pour la clé lorsque l'accès à l'espace commun est basé sur un profil d'espace commun.

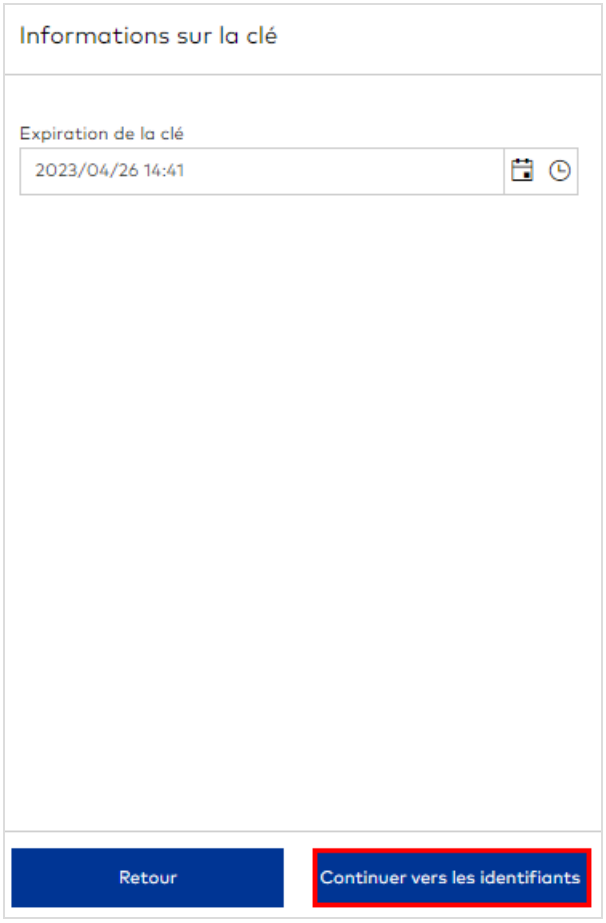
Les clés de blocage peuvent être utilisées pour invalider :

- clés de résidents
- clés du personnel/prestataire
- Clés ELO
- Clés de verrouillage/déverrouillage/clés de bascule de libre passage
- Clés d'annulation

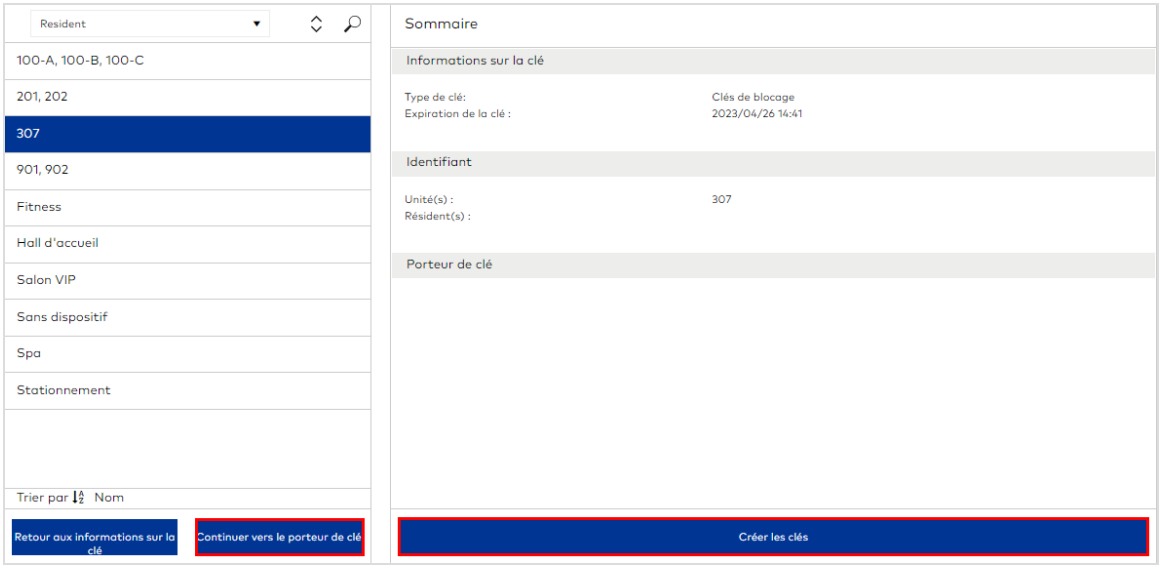
Si l'intention est de bloquer temporairement l'accès, vous pouvez utiliser une clé de déblocage pour débloquer une clé qui était auparavant bloquée par une clé de blocage. Les clés obsolètes ne peuvent pas être débloquées.

Créer des clés de blocage

1. Accédez à ***Clés Système > Clés de blocage***



2. Indiquez les informations d'expiration.
3. Cliquez sur **Continuer vers les identifiants**.



4. Sélectionnez la catégorie d'identifiants dans laquelle l'identifiant que vous souhaitez bloquer est défini.
5. Sélectionnez l'identifiant que vous souhaitez bloquer.

6. Prenez l'une des mesures proposées ou passez à l'étape suivante :
   - Cliquez sur **Continuer vers la séquence de la clé**. Sélectionnez la séquence de clés à bloquer. Vous pouvez bloquer les séquences de clés obsolètes ou actives. Le blocage d'une séquence de clés bloque également toutes les séquences de clés dont la date de début est antérieure. Pour plus de détails sur le blocage des clés obsolètes, reportez-vous à la section En savoir plus sur les clés Système.
   - Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
7. Cliquez sur **Créer les clés**.

> Si la communication en ligne est activée, vous pouvez également cliquer sur **Bloquer des clés à distance**. Cette option est prise en charge lorsque l'identifiant sélectionné est basé sur la catégorie d'identifiants Urgence, Personnel ou Usage restreint. (Les clés ne peuvent pas être bloquées à distance pour les catégories d'identifiants Personnel [accès variable] et Prestataire ou les catégories personnalisées basées sur Personnel (accès variable) et Prestataire.)

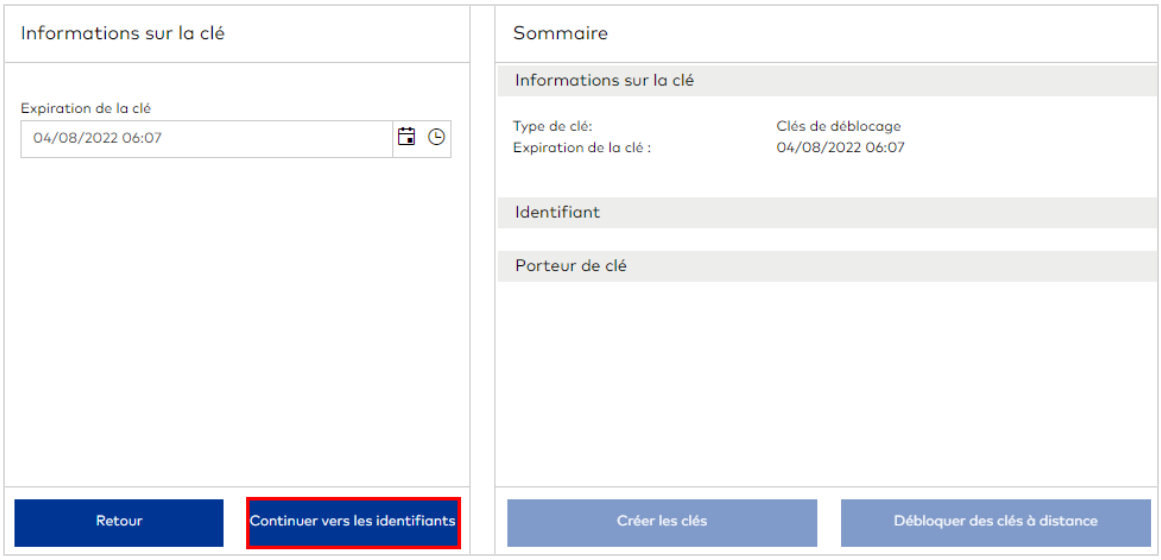
8. Sélectionnez un encodeur en ligne.
9. Présentez une clé à l'encodeur (lorsque vous y êtes invité).
10. Cliquez sur **Démarrer**.
11. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

N'oubliez pas que les clés physiques doivent être présentées aux serrures.

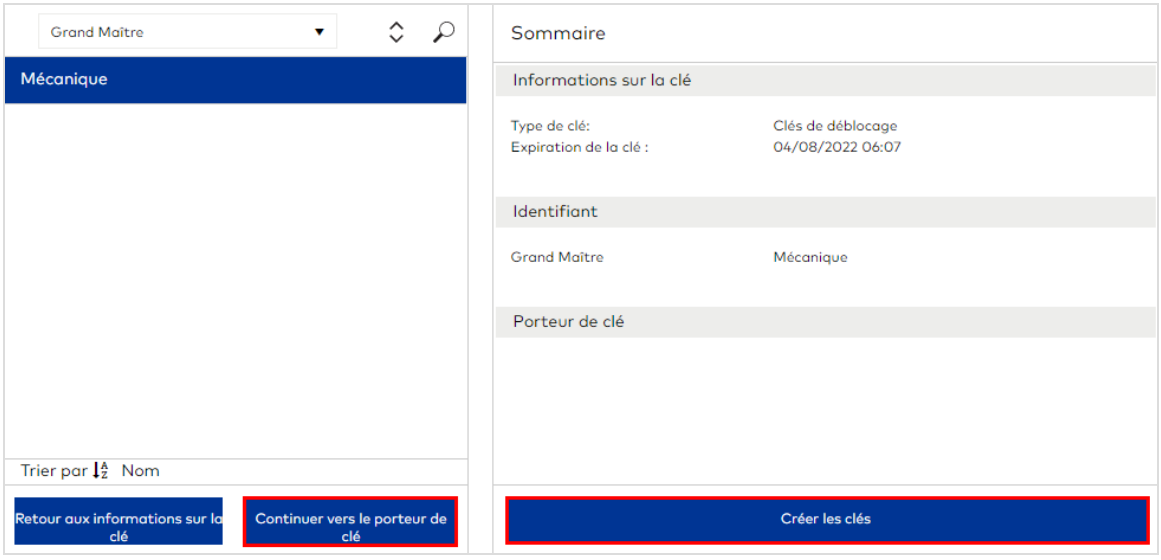
Créer des clés de déblocage

Les clés de déblocage débloquent toutes les instances d'un identifiant spécifique sur des points d'accès ayant été préalablement bloqués à l'aide de la clé de blocage.

1. Accédez à ***Clés Système > Clés de déblocage***.



2. Indiquez les informations d'expiration.
3. Cliquez sur **Continuer vers les identifiants**.



4. Sélectionnez la catégorie d'identifiants pour l'identifiant ou le point d'accès encodé sur la clé que vous souhaitez débloquer. Seules les catégories pour lesquelles des clés actives existent sont affichées dans la liste.
5. Sélectionnez l'identifiant (ou le point d'accès) encodé sur la clé que vous souhaitez débloquer.
6. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
7. Cliquez sur **Créer les clés**.

Si la communication en ligne est activée, vous avez la possibilité de cliquer sur **Débloquer des clés à distance**.

8. Sélectionnez un encodeur en ligne.
9. Présentez une clé à l'encodeur (lorsque vous y êtes invité).
10. Cliquez sur **Démarrer**.
11. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

N'oubliez pas que les clés physiques doivent être présentées aux serrures.

Clés d'annulation

Créez une clé d'annulation pour invalider définitivement une instance de clé spécifique. Avant de créer une clé d'annulation, vous devez connaître la catégorie d'identifiants et l'identifiant que vous souhaitez annuler. Une clé d'annulation doit être présentée à tous les points d'accès pour lesquels la clé initiale dispose d'identifiants.

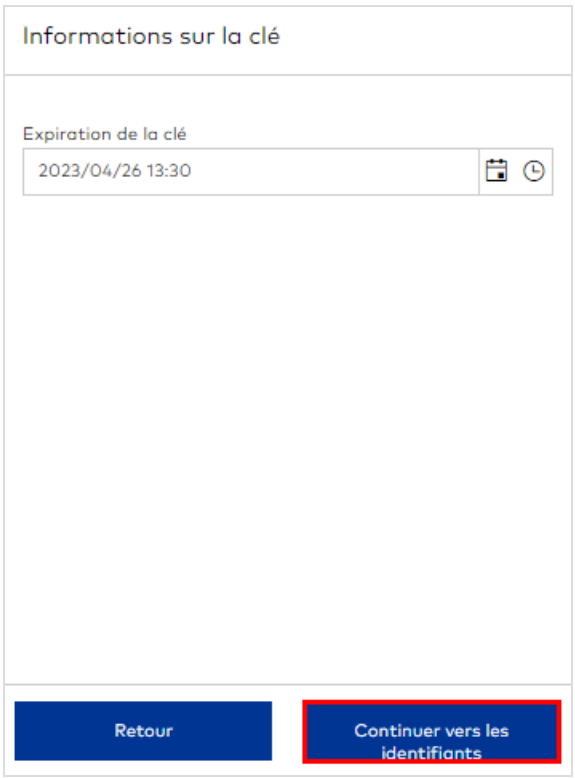
Lorsqu'une clé d'annulation est utilisée pour invalider une clé de personnel/prestataire, l'état de la clé du personnel doit être Actif pour invalider l'accès aux espaces communs. Si l'état de la clé est Obsolète, l'accès aux espaces communs reste valide jusqu'à l'expiration de la clé.

Les clés d'annulation peuvent être utilisées pour invalider :

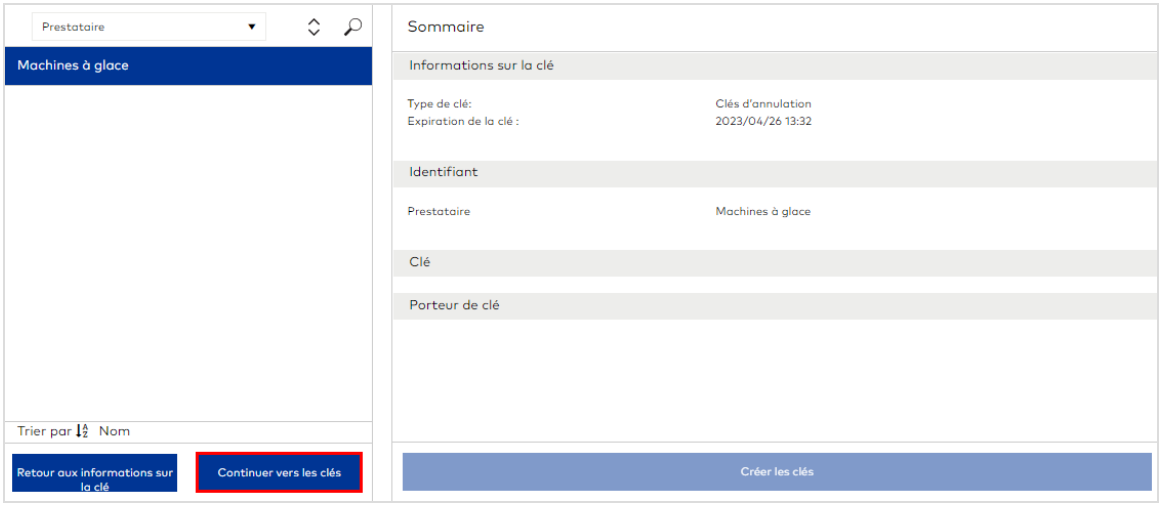
- clés du personnel/prestataire
- Clés ELO
- Clés de verrouillage/déverrouillage/clés de bascule de libre passage
- Clés d'annulation

Pour créer des clés d'annulation :

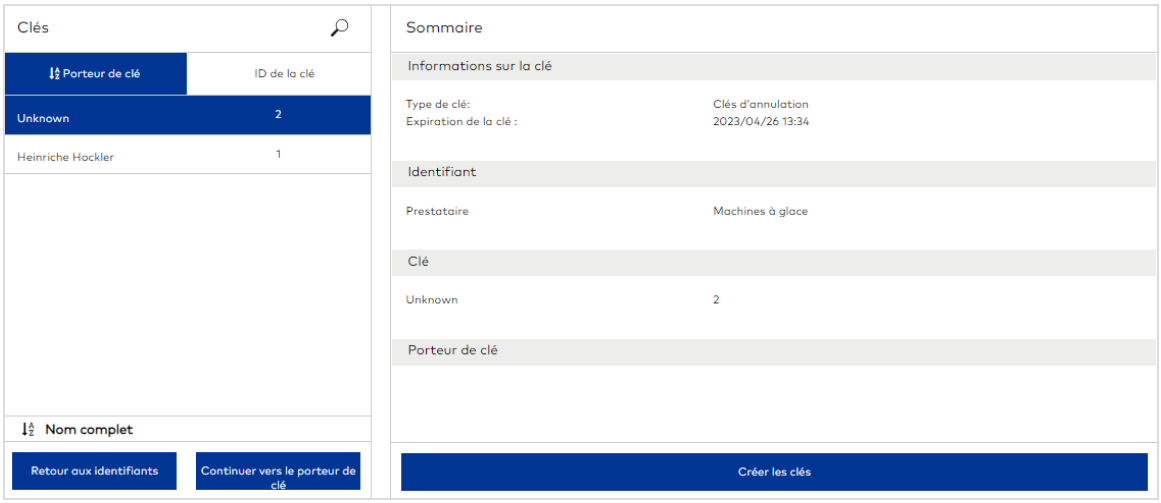
1. Accédez à ***Clés Système > Clés d'annulation***



2. Indiquez les informations d'expiration.
3. Cliquez sur **Continuer vers les identifiants**.



4. Sélectionnez la catégorie d'identifiants dans laquelle l'identifiant que vous souhaitez annuler est défini. Seules les catégories pour lesquelles des clés actives existent sont affichées dans la liste.
5. Sélectionnez l'identifiant ou le point d'accès encodé sur la clé que vous souhaitez annuler.
6. Cliquez sur **Continuer vers les clés**.



7. Sélectionnez la clé que vous souhaitez annuler. Vous pouvez consulter la liste des clés par porteur de clé ou par ID de la clé.
8. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
9. Cliquez sur **Créer les clés**.

Si la communication en ligne est activée, vous pouvez également cliquer sur **Annuler des clés à distance**. Cette option est prise en charge lorsque l'identifiant sélectionné est basé sur la catégorie d'identifiants Urgence, Personnel ou Usage restreint. (Les clés ne peuvent pas être annulées à distance pour les catégories d'identifiants Personnel [accès variable] et Prestataire ou les catégories personnalisées basées sur Personnel (accès variable) et Prestataire.)

10. Sélectionnez un encodeur en ligne.
11. Présentez une clé à l'encodeur (lorsque vous y êtes invité).

12. Cliquez sur **Démarrer**.
13. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Clés de diagnostic

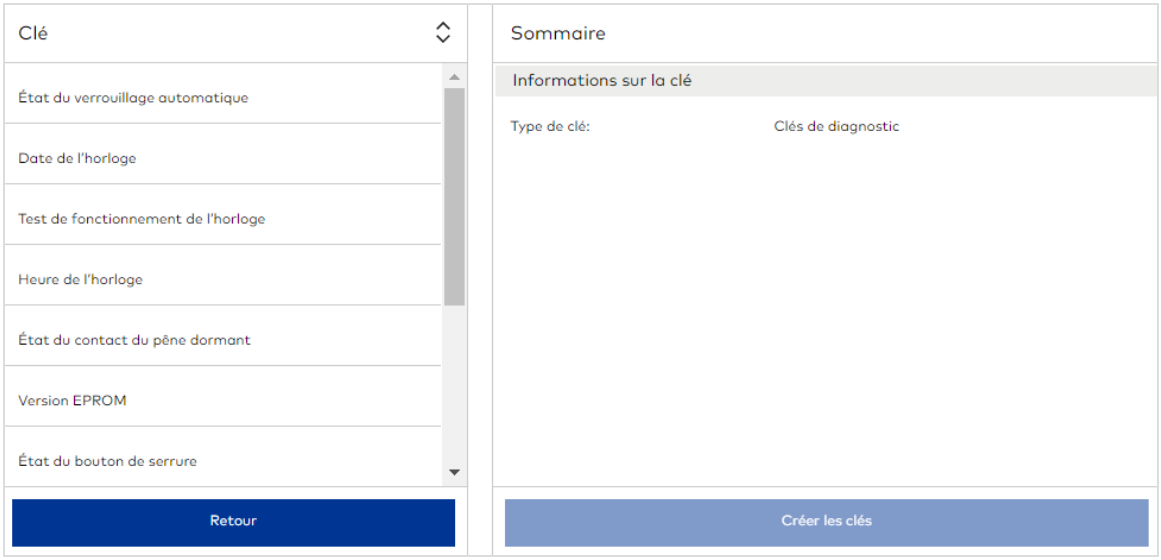
Les clés de diagnostic interrogent des serrures pour extraire l'état de diverses fonctions de serrures, le plus souvent à des fins de résolution de problèmes et de reporting. Les résultats de l'interrogation sont communiqués par une séquence de clignotements LED.

Une alternative plus simple que la création de clés de diagnostic est d'utiliser le M-Unit (Programmateur M-Unit) pour effectuer un diagnostic des serrures. Les résultats de l'enquête sont au format texte lisible au lieu d'une séquence de clignotements LED.

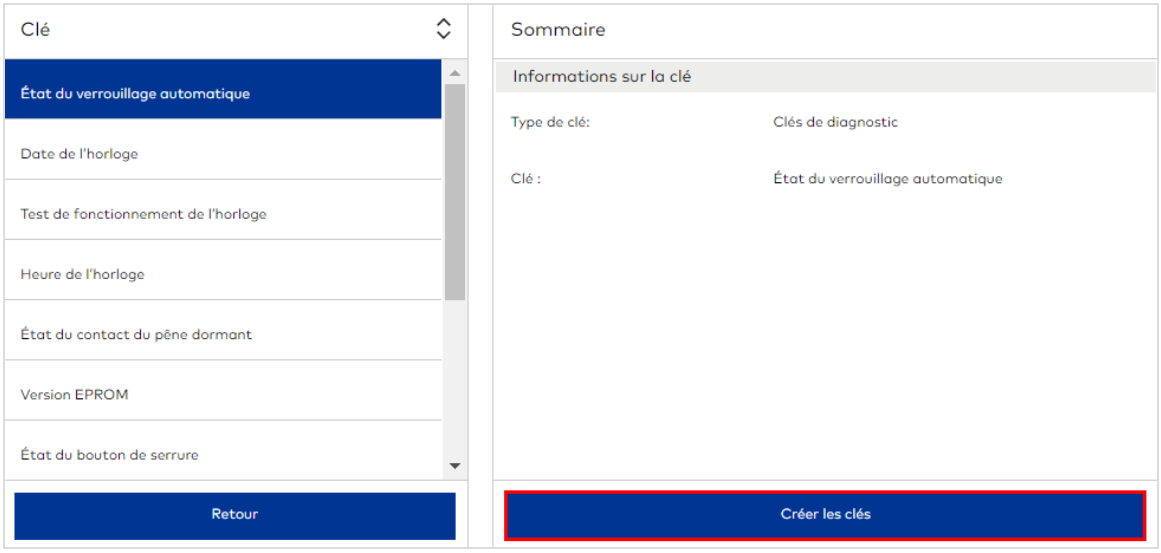
Les clés de diagnostic ne sont pas compatibles avec les nouveaux modèles de serrures NFC : RT+, Sapphire, MT6 et Confidant NFC.

Créer des clés de diagnostic

1. Accédez à ***Clés Système > Clés de diagnostic***.



2. Sélectionnez le type de diagnostic que vous souhaitez exécuter.
   - **État du verrouillage automatique** — Sélectionnez cette option pour interroger la serrure concernant les horaires de verrouillage automatique.
   - **Date de l'horloge** — Sélectionnez cette option pour interroger la serrure concernant la date.
   - **Test de fonctionnement de l'horloge** — Sélectionnez cette option pour tester le fonctionnement de l'horloge de la serrure.
   - **Heure de l'horloge** — Sélectionnez cette option pour interroger la serrure concernant l'heure.
   - **État du contact du pêne dormant** — Sélectionnez cette option pour interroger la serrure concernant l'état projeté ou rétracté du pêne dormant.
   - **Version EPROM** — Sélectionnez cette option pour afficher la version du microcontrôleur dans la serrure.
   - **État du bouton de serrure** — Sélectionnez cette option pour déterminer si la serrure est occupée ou ouverte.
   - **Deux derniers enregistrements LPI** — Sélectionnez cette option pour interroger la serrure concernant les deux erreurs les plus récentes.
   - **Test des voyants LED** — Sélectionnez cette option pour tester la LED de la serrure.
   - **État de batterie faible** — Sélectionnez cette option pour connaître l'état de charge de la batterie de la serrure.
   - **Contact de moteur et état de la serrure** — Sélectionnez cette option pour interroger l'état du moteur de verrouillage et l'état de la serrure.
   - **Version du firmware de la serrure** — Sélectionnez cette option pour interroger la version de firmware de la serrure.



3. Cliquez sur **Créer les clés**.
4. Sélectionnez un encodeur en ligne.
5. Présentez une clé à l'encodeur (lorsque vous y êtes invité).
6. Cliquez sur **Démarrer**.
7. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Résultats de diagnostic

Pour plus d'informations sur l'interprétation d'une séquence de clignotements, voir « Dépannage des serrures ».

Séquence de clignotements LED

Chaque couleur de voyant correspond à une valeur de base différente :

- Vert = 100
- Jaune = 10
- Rouge = 1

Pour interpréter une réponse, multipliez le nombre de clignotements de chaque couleur par la valeur de base. Par exemple, si la séquence de voyants est deux clignotements jaunes suivis de trois clignotements rouges, la valeur de la réponse est 23.

Jaune (10) x 2 + Rouge (1) x 3 = 23

Éléments de diagnostic

Chaque clé de diagnostic fournit plusieurs informations. Chaque information est qualifiée d'élément et vous devez connaître les éléments qui s'afficheront afin de comprendre la réponse.

Par exemple, la clé d'affichage de l'heure de l'horloge vous fournira des informations sur les éléments suivants :

- Problème de date/heure/heure d'été (le cas échéant) (0-4)
- État de l'heure d'été (0-1)
- Heures (au format 24 h) (0-23)
- Minutes (0-59)

Lorsque vous utilisez la carte, la réponse commence et finit par un délimiteur composé de chacun des trois voyants clignotant simultanément. Ce délimiteur sert également à séparer les réponses à chaque élément.

Clés de bascule de verrouillage électronique

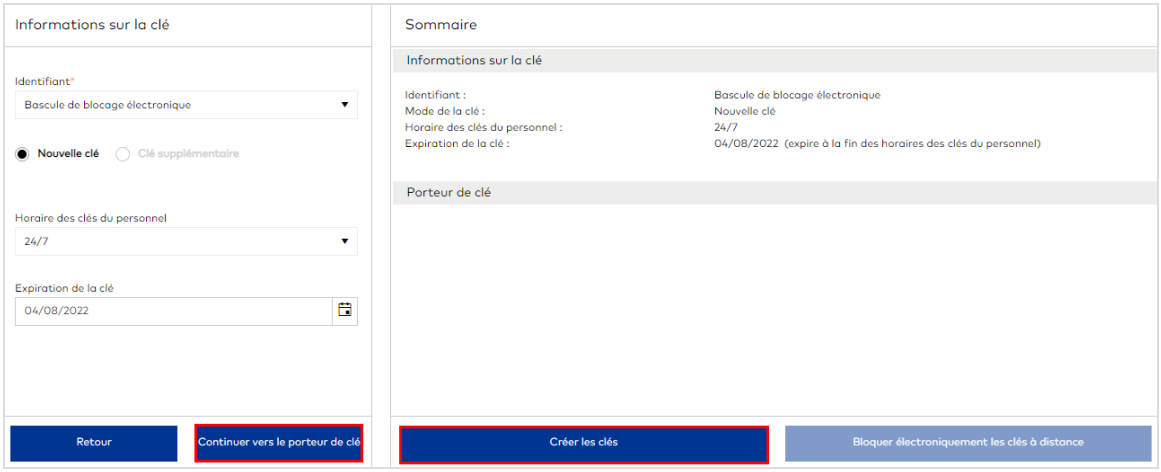
Les clés de bascule de verrouillage électronique (ELO) invalident temporairement toutes les clés non dédiées aux urgences en verrouillant à double tour la porte de l'extérieur (activer le verrou d'intimité ou le pêne dormant). Lorsqu'un blocage électronique est activé, seule une clé dotée de l'identifiant Urgence peut ouvrir la serrure. Lorsque le blocage électronique est désactivé, l'accès par clé standard est rétabli.

Les clés ELO sont des clés de commutation. Le comportement de la clé alterne (applique le verrouillage/supprime le verrouillage) à chaque fois qu'elle est présentée à la serrure.

Pour créer des clés ELO :

L'identifiant sélectionné par défaut (**ELO**) ou un identifiant personnalisé basé sur la catégorie d'identifiants ELO est requis.

1. Accédez à ***Clés Système > Clés de bascule de blocage électronique***. L'identifiant par défaut **ELO** est requis.



2. Indiquez si vous souhaitez créer une Nouvelle clé ou une Clé supplémentaire. Si aucune clé active n'existe, une Nouvelle clé est requise. Si une clé active existe, **Clé supplémentaire** est la valeur par défaut sélectionnée. La création d'une clé supplémentaire (copie) n'a aucun effet sur les clés actives existantes. La création d'une nouvelle clé lorsqu'une clé active existe, invalide la clé précédemment active.
3. Sélectionnez un horaire des clés du personnel. Pour permettre un accès 24h/24 et 7j/7, sélectionnez **24/7**. Pour consulter les détails de l'horaire des clés du personnel, accédez à ***Gestion des accès > Horaires des clés du personnel***. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
4. Indiquez les informations d'expiration.
5. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
6. Cliquez sur **Créer les clés**.

Si la communication en ligne est activée, vous avez la possibilité de cliquer sur **Clés ELO à distance**.

7. Sélectionnez un encodeur en ligne.
8. Présentez une clé à l'encodeur (lorsque vous y êtes invité).
9. Cliquez sur **Démarrer**.
10. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Séquence de clignotements LED des clés de bascule de verrouillage électronique

Pour plus d'informations sur l'interprétation d'une séquence de clignotements, voir « Dépannage des serrures ».

- La séquence de clignotements LED suivante indique l'activation du blocage électronique :
  - Rouge (1) Jaune (12)
- La séquence de clignotements LED suivante indique la désactivation du blocage électronique :
  - Vert (1) Jaune (12)

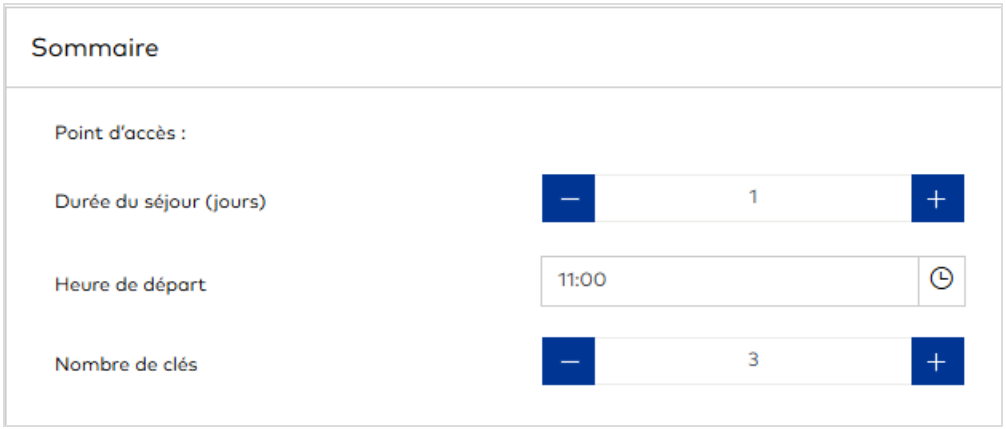
Clés à sécurité intégrée

Les clés à sécurité intégrée sont des sauvegardes des clés individuelles des unités qui sont créées à l'avance et conservées en jeux complets à remettre aux résidents en cas de panne du système ou de courant. Il est recommandé de créer et de conserver deux jeux de trois clés pour chaque porte d'unité et de suite. Après qu'un jeu de clés à sécurité intégrée a été émis et utilisé, créez un autre jeu de clés à sécurité intégrée pour remplacer le jeu utilisé. Les serrures n'acceptent que les clés des deux jeux de clés à sécurité intégrée les plus récents.

L'utilisation d'une clé à sécurité intégrée invalide l'accès aux unités, aux portes communes des suites et aux portes des unités de suite par la clé résident précédente.

Pour créer un jeu de clés à sécurité intégrée :

1. Accédez à ***Clés Système > Clés à sécurité intégrée***.



2. Sélectionnez un point d'accès. Vous pouvez sélectionner un point d'accès à partir de n'importe quel bâtiment du site.
3. Indiquez le nombre de nuits pendant lesquelles l'accès à l'unité est activé.
4. Indiquez l'heure après laquelle la clé devient invalide (la clé reste valide le dernier jour).
5. Indiquez le nombre de clés à créer.
6. Cliquez sur **Créer les clés**.
7. Sélectionnez un encodeur en ligne.
8. Indiquez le nombre de clés à créer.
9. Présentez une clé à l'encodeur (lorsque vous y êtes invité).
10. Cliquez sur **Démarrer**.
11. Lorsqu'un message vous indique que les clés ont bien été créées, cliquez sur **Terminé**.

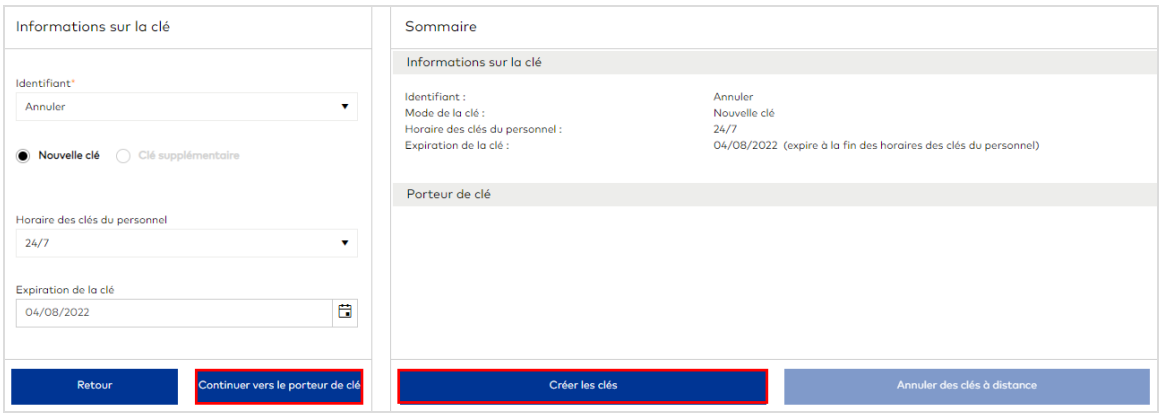
Clés d'annulation

Les clés d'annulation sont utilisées pour annuler définitivement l'accès d'un résident actuel. Le plus souvent, les clés d'annulation sont utilisées par le personnel après le départ d'un résident avant l'expiration de la clé. Les clés d'annulation invalident toutes les clés de résidents encodées avec accès à l'unité, même si le pêne dormant ou le verrou d'intimité est actionné.

Les clés d'annulation n'invalident pas l'accès aux espaces communs et aux lecteurs d'ascenseurs.

Créer des clés d'annulation

1. Accédez à ***Clés Système > Clés d'annulation***. L'identifiant par défaut **Annulation** est requis.



2. Indiquez si vous souhaitez créer une Nouvelle clé ou une Clé supplémentaire. Si aucune clé active n'existe, une Nouvelle clé est requise. Si une clé active existe, **Clé supplémentaire** est la valeur par défaut sélectionnée. La création d'une clé supplémentaire (copie) n'a aucun effet sur les clés actives existantes. La création d'une nouvelle clé lorsqu'une clé active existe, invalide la clé précédemment active.
3. Sélectionnez un horaire des clés du personnel au cours duquel la clé est valide. Pour permettre un accès 24h/24 et 7j/7, sélectionnez **24/7**. Pour consulter les détails de l'horaire des clés du personnel, accédez à ***Gestion des accès > Horaires des clés du personnel***. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
4. Indiquez les informations d'expiration.
5. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
6. Cliquez sur **Créer les clés**.
7. Si la communication en ligne est activée, vous avez la possibilité de cliquer sur **Annuler des clés à distance**. Cette option est prise en charge lorsque l'identifiant sélectionné est basé sur la catégorie d'identifiants Urgence, Personnel ou Usage restreint. (Les clés ne peuvent pas être bloquées à distance pour les catégories d'identifiants Personnel [accès variable] et Prestataire ou les catégories personnalisées basées sur Personnel (accès variable) et Prestataire.)
8. Sélectionnez un encodeur en ligne.
9. Présentez une clé à l'encodeur (lorsque vous y êtes invité).
10. Cliquez sur **Démarrer**.
11. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Séquence de clignotements LED des clés d'annulation

Pour plus d'informations sur l'interprétation d'une séquence de clignotements, voir « Dépannage des serrures ».

- La séquence de clignotements LED suivante s'affiche lorsqu'une clé d'annulation est présentée pour la première fois :
  - Rouge (1) Jaune (12)
- La séquence de clignotements LED suivante s'affiche lorsque la serrure a déjà été inhibée :
  - Jaune (12)

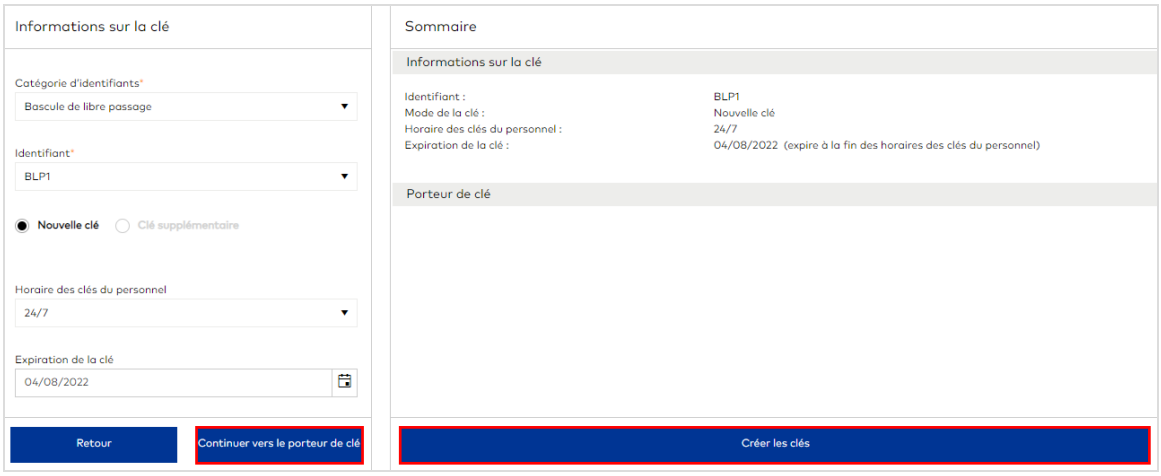
Clés de verrouillage et de déverrouillage

Les clés Système suivantes verrouillent et déverrouillent les serrures :

- **Clés de verrouillage** — Désactiver le mode passage. L'accès est restreint aux seules personnes dont les clés sont encodées avec l'identifiant correspondant.
- **Clés de déverrouillage** — Activer le mode passage. Le mode passage est un état de la serrure au cours duquel les contrôles d'accès programmés dans la serrure sont suspendus afin de permettre un libre accès.
- **Clés de bascule de libre passage** — Activer et désactiver le mode passage. Le mode passage est un état de la serrure au cours duquel les contrôles d'accès programmés dans la serrure sont suspendus afin de permettre un libre accès. Une clé de commutation change de comportement chaque fois que la clé est présentée à la serrure.

Pour créer des clés de verrouillage, déverrouillage et des clés de bascule de libre passage :

1. Accédez à **Clés Système**.
2. Sélectionnez le type de clé à créer :
   - **Clés de verrouillage**
   - **Clés de déverrouillage**
   - **Bascule de libre passage**



3. La catégorie d'identifiants sélectionnée par défaut (**Verrouillage**, **Déverrouillage**, **Bascule de libre passage**) ou une catégorie d'identifiants personnalisée basée sur le type respectif est requise.
4. Sélectionnez l'identifiant pour le verrouillage, le déverrouillage ou la bascule de libre passage.
5. Indiquez si vous souhaitez créer une Nouvelle clé ou une Clé supplémentaire. Si aucune clé active n'existe, une Nouvelle clé est requise. Si une clé active existe, **Clé supplémentaire** est la valeur par défaut sélectionnée. La création d'une clé supplémentaire (copie) n'a aucun effet sur les clés actives existantes. La création d'une nouvelle clé lorsqu'une clé active existe, invalide la clé précédemment active.
6. Sélectionnez un horaire des clés du personnel au cours duquel la clé est valide. Pour permettre un accès 24h/24 et 7j/7, sélectionnez **24/7**. Pour consulter les détails de l'horaire des clés du personnel, accédez à ***Gestion des accès > Horaires des clés du personnel***. L'horaire des clés du personnel sélectionné détermine les jours et heures de validité de la clé.
7. Indiquez les informations d'expiration.
8. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
9. Cliquez sur **Créer les clés**.
10. Sélectionnez un encodeur en ligne.
11. Indiquez le nombre de clés à créer.
12. Présentez une clé à l'encodeur.

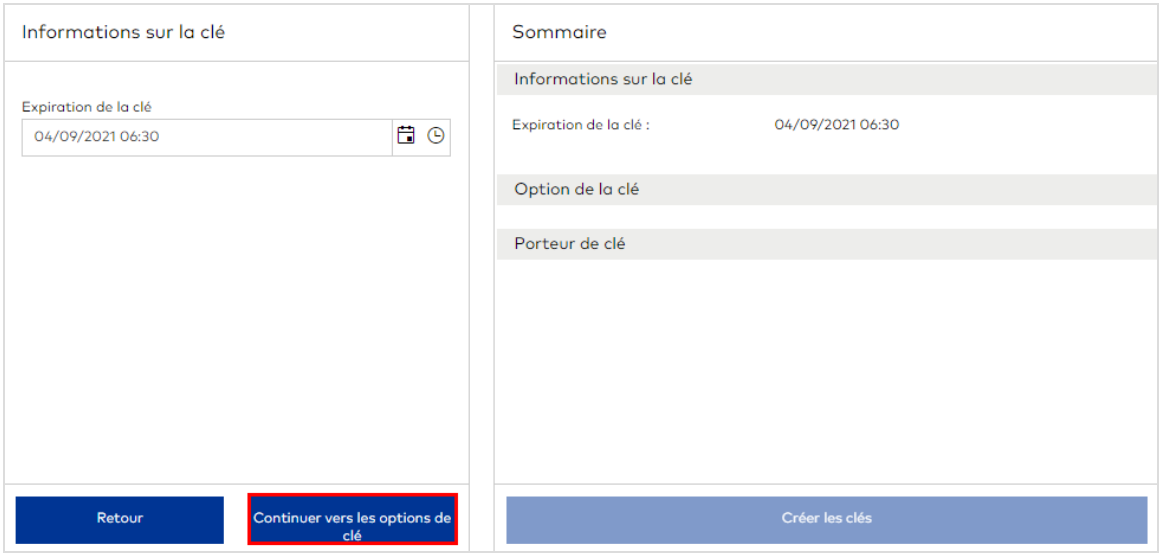
13. Cliquez sur **Démarrer**.
14. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Clés de programmation primaire et secondaire

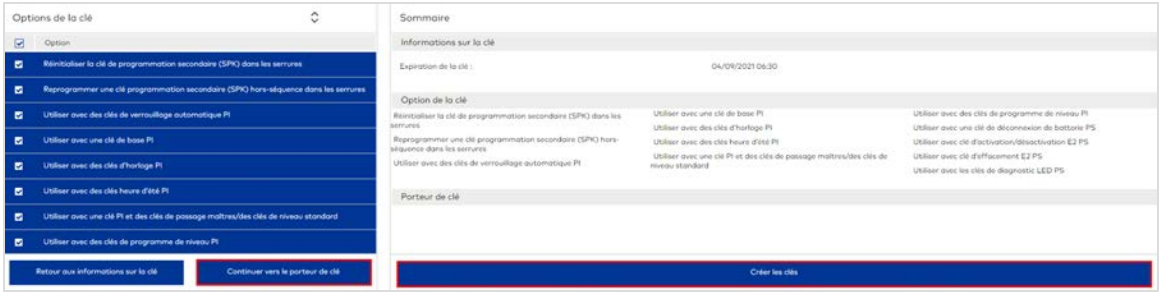
Les clés de programmation primaire mettent la serrure en mode de programmation et sont utilisées conjointement avec les clés d'informations sur la programmation (PI) et les clés d'état de la programmation (PS) pour programmer des serrures et autoriser des fonctions spéciales (voir « Créer une clé à fonction spéciale »). Elles servent également à reprogrammer la clé de programmation secondaire actuelle ou à réinitialiser une clé de programmation secondaire différente.

Créer une clé de programmation primaire

1. Accédez à ***Clés Système > Clés de programmation primaire***.



2. Indiquez les informations d'expiration.
3. Cliquez sur **Continuer vers les options de clé**.



4. Sélectionnez les options à encoder sur la clé. Toutes les options sont sélectionnées par défaut.

> Toutes les options PI demeurent dans le système pour permettre la prise en charge des systèmes hérités. Pour obtenir des conseils sur ces options, veuillez contacter l'assistance technique dormakaba.

- **Réinitialiser la clé de programmation secondaire (SPK) dans les serrures** — Cette option est seulement sélectionnée dans les rares cas où la clé de programmation primaire (PPK) a été endommagée et doit être réinitialisée. Avant de réinitialiser la clé SPK, vous devez utiliser la clé SPK pour réinitialiser une nouvelle clé PPK. Sélectionnez cette option pour encoder une clé PPK autorisant une clé à reprogrammer une clé de programmation secondaire.
- **Reprogrammer une clé programmation secondaire (SPK) hors-séquence dans les serrures** — Cette option est seulement sélectionnée dans de rares cas. Sélectionnez cette option pour encoder une clé PPK autorisant une clé à reprogrammer une clé de programmation secondaire.

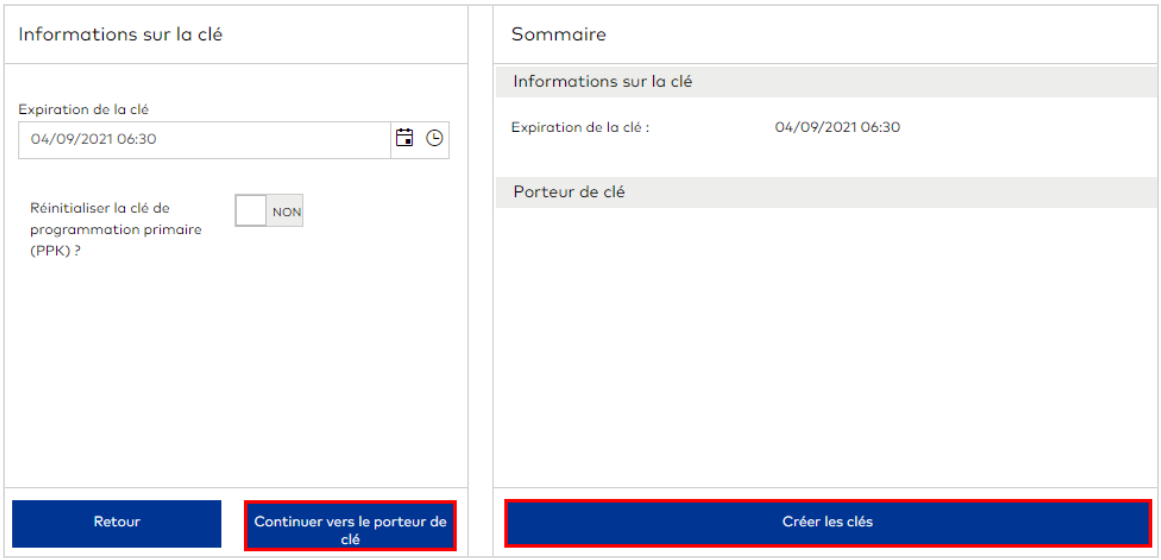
- **Utiliser avec des clés de verrouillage automatique PI** — Sélectionnez cette option pour encoder une clé PPK permettant à une clé de programmer des horaires de verrouillage/déverrouillage automatique dans la serrure.
- **Utiliser avec une clé de base PI**
- **Utiliser avec des clés d'horloge PI** — Sélectionnez cette option pour encoder une clé PPK permettant à une clé de synchroniser l'horloge de la serrure.
- **Utiliser avec des clés heure d'été PI** — Sélectionnez cette option pour encoder une clé PPK permettant à une clé de mettre à jour les réglages d'heure d'été dans la serrure.
- **Utiliser avec une clé PI et des clés de passage maîtres/des clés de niveau standard**
- **Utiliser avec des clés de programme de niveau PI**
- **Utiliser avec une clé de déconnexion de batterie PS** — Sélectionnez cette option pour encoder une clé PPK permettant à une clé de désactiver la serrure avant que la batterie de la serrure ne se déconnecte.

5. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
6. Cliquez sur **Créer les clés**.
7. Sélectionnez un encodeur en ligne.
8. Présentez une clé à l'encodeur.
9. Cliquez sur **Démarrer**.
10. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Créer une clé de programmation secondaire

Pour créer une clé de programmation secondaire :

1. Accédez à ***Clés Système > Clés de programmation secondaire***.



2. Indiquez les informations d'expiration.
3. Choisissez de réinitialiser ou non la clé PPK. La réinitialisation d'une clé PPK est un événement rare et sert à reprogrammer la clé PPK actuelle ou à réinitialiser une clé PPK différente sur une serrure. Cette réinitialisation doit être effectuée uniquement à la demande de l'assistance technique dormakaba. Si vous choisissez de réinitialiser, toutes les clés deviennent invalides et toutes les serrures doivent être reprogrammées.
4. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
5. Cliquez sur **Créer les clés**.

6. Sélectionnez un encodeur en ligne.
7. Présentez une clé à l'encodeur.
8. Cliquez sur **Démarrer**.
9. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Séquence de clignotements LED de la clé de programmation secondaire

Pour plus d'informations sur l'interprétation d'une séquence de clignotements, voir « Dépannage des serrures ».

La séquence de clignotements LED suivante s'affiche lorsqu'une clé SPK est présentée pour la première fois :

Jaune (clignotement lent pendant 20 secondes)

Clés de reséquence

La clé de reséquence est utilisée pour actualiser le nombre de séquences stockées dans la mémoire de la serrure lorsque le nombre de nouvelles clés créées mais non utilisées dans la serrure dépasse la plage de séquences programmées pour cette clé.

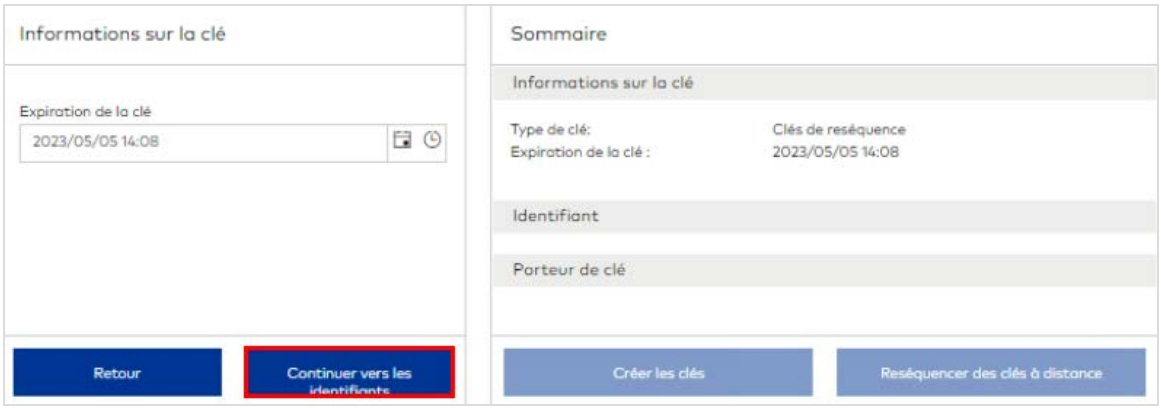
L'utilisation d'une clé de reséquence est rare. Le personnel peut dépanner la serrure pour déterminer si la cause de l'erreur de serrure est un numéro de séquence corrompu.

Les clés de reséquence peuvent être utilisées pour corriger la séquence des :

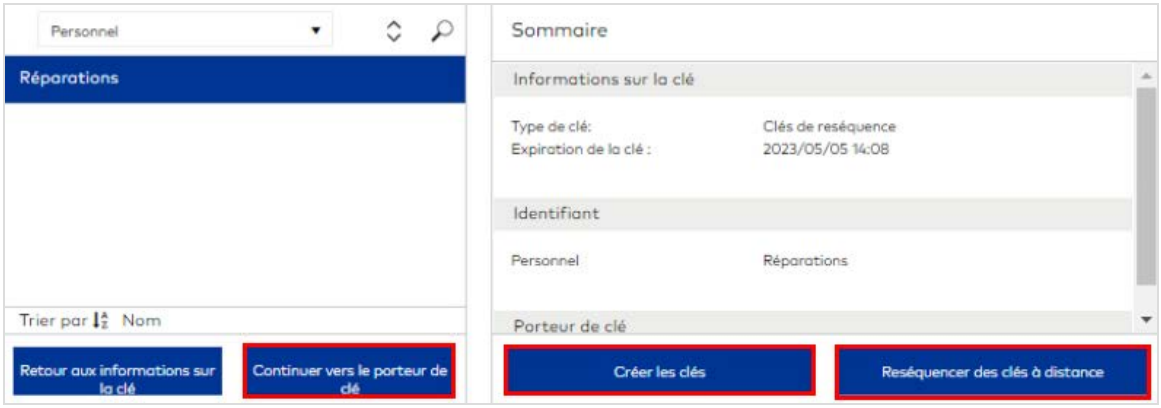
- Clés du personnel/prestataire
- Clés ELO
- Clés de verrouillage/déverrouillage/clés de bascule de libre passage
- Clés d'annulation

Créer des clés de reséquence

1. Accédez à ***Clés Système > Clés de reséquence***.



2. Indiquez les informations d'expiration.
3. Cliquez sur **Continuer vers les identifiants**.



4. Sélectionnez la catégorie d'identifiants. Sélectionnez la catégorie d'identifiants pour l'identifiant ou le point d'accès encodé sur la clé que vous souhaitez reséquencer. Seules les catégories pour lesquelles des clés actives existent sont affichées dans la liste.

5. Sélectionnez l'identifiant. Sélectionnez l'identifiant (ou le point d'accès) encodé sur la clé que vous souhaitez reséquencer. Vous pouvez sélectionner un identifiant à partir de n'importe quel bâtiment.
6. (*facultatif*) Cliquez sur **Continuer vers le porteur de clé** et sélectionnez le membre du personnel auquel vous souhaitez attribuer la clé. Pour ajouter un membre du personnel, cliquez sur **(Ajouter)** +, saisissez les nom et prénom, puis cliquez sur **Sauvegarder**.
7. Cliquez sur **Créer les clés**.

Si la communication en ligne est activée, vous pouvez également cliquer sur **Reséquencer des clés à distance**. Cette option est prise en charge lorsque l'identifiant sélectionné est basé sur la catégorie d'identifiants Urgence, Personnel ou Usage restreint. (Les clés ne peuvent pas être reséquencées à distance pour les catégories d'identifiants Personnel [accès variable] et Prestataire ou les catégories personnalisées basées sur Personnel (accès variable) et Prestataire.)

8. Sélectionnez un encodeur en ligne.
9. Présentez une clé à l'encodeur (lorsque vous y êtes invité).
10. Cliquez sur **Démarrer**.
11. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Séquence de clignotements LED de la clé de reséquence

Pour plus d'informations sur l'interprétation d'une séquence de clignotements, voir « Dépannage des serrures ».

- La séquence de clignotements LED suivante s'affiche lorsqu'une clé de reséquence est présentée pour la première fois :
  - Vert et Jaune (6)
- La séquence de clignotements LED suivante s'affiche lorsqu'une clé de reséquence est présentée à une serrure n'étant pas hors séquence :
  - Jaune (6)

En cas d'utilisation d'une clé de reséquence pour des niveaux résidents, une nouvelle clé résident doit être créée si un clignotement rouge précède les clignotements verts/jaunes.

Clés à fonction spéciale

Les clés à fonction spéciale sont assignées à des clés de programmation primaire pour effectuer des opérations de niveau système sur une serrure.

Les clés à fonction spéciale sont prises en charge pour les systèmes hérités. Une alternative plus simple que la création de clés SFK est d'utiliser le M-Unit (Programmateur M-Unit) pour interroger (auditer) une serrure. Toutes les données pouvant être obtenues par l'utilisation d'une clé SFK sont comprises dans les rapports d'audit.

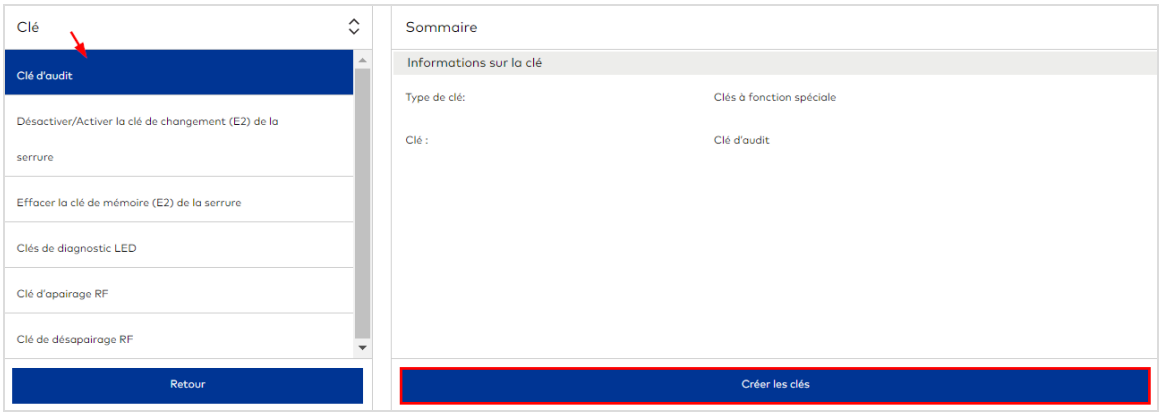
Types de clés à fonction spéciale

Les types suivants de clés à fonction spéciale peuvent être créés dans les Clés Système :

- **Clé d'audit** — Requiert une clé 4k. Sélectionnez cette option pour créer une clé qui audite une serrure pour en obtenir l'état et les données de diagnostic. Une clé d'audit peut contenir au maximum 172 enregistrements. Après avoir audité une serrure au moyen d'une Clé d'audit, présentez la clé à l'encodeur et cliquez sur le bouton Lire la clé dans la barre d'outils Community. Les données de la serrure collectées s'affichent avec la possibilité de générer un rapport. Si vous générez un rapport à partir des résultats de l'action Lire la clé, le rapport se limite aux données collectées par la Clé d'audit. Pour étendre la portée des données du rapport, allez dans le module Rapports et générez un Rapport d'audit de point d'accès.
- **Désactiver/Activer la clé de changement de la serrure** — Sélectionnez cette option pour créer une clé qui désactive toutes les clés et accès de M-Unit à la serrure lorsque la clé est présentée.
- **Effacer la clé de mémoire de la serrure** — Sélectionnez cette option pour créer une clé qui supprime toute programmation stockée dans la mémoire de la serrure.
- **Clés de diagnostic LED** — Sélectionnez cette option pour créer une clé qui effectue des diagnostics des points d'accès.
- **Appairage RF** — Sélectionnez cette option pour créer une clé qui connecte une serrure à la passerelle configurée. Ce type de clé ne s'affiche que si la communication en ligne est activée.
- **Désappairage RF** — Sélectionnez cette option pour créer une clé qui déconnecte une serrure de la passerelle appairée. Ce type de clé ne s'affiche que si la communication en ligne est activée.

Créer des clés à fonction spéciale

1. Accédez à ***Clés Système > Clés à fonction spéciale***.



2. Sélectionnez le type de fonction spéciale que vous souhaitez exécuter.
3. Cliquez sur **Créer les clés**.
4. Sélectionnez un encodeur en ligne.
5. Présentez une clé à l'encodeur.

6. Cliquez sur **Démarrer**.
7. Lorsque vous êtes informé que la demande de clé est terminée, cliquez sur **Terminé**.

Surveiller

Surveillance

Cette section comprend les sujets suivants :

En savoir plus sur la surveillance 254

Surveiller les clés 255

Surveiller l'utilisation des clés numériques 256

En savoir plus sur la surveillance

Le module **Surveillance** fournit des informations sur toutes les clés créées dans Community. Si vous souhaitez savoir à quelle heure et par qui une clé spécifique a été utilisée pour la dernière fois, ces données sont directement disponibles sans générer un rapport.

L'accès aux données du module **Surveillance** est configuré dans **Gestion des rôles**. Par défaut, les rôles Administrateur et Configurateur de site ont un accès complet.



Lorsque la fonction sous licence Clés mobiles est activée, l'onglet Utilisation des clés numériques s'affiche pour contrôler et suivre le nombre de clés numériques (clés mobiles et clés de portefeuille) disponibles/utilisées.

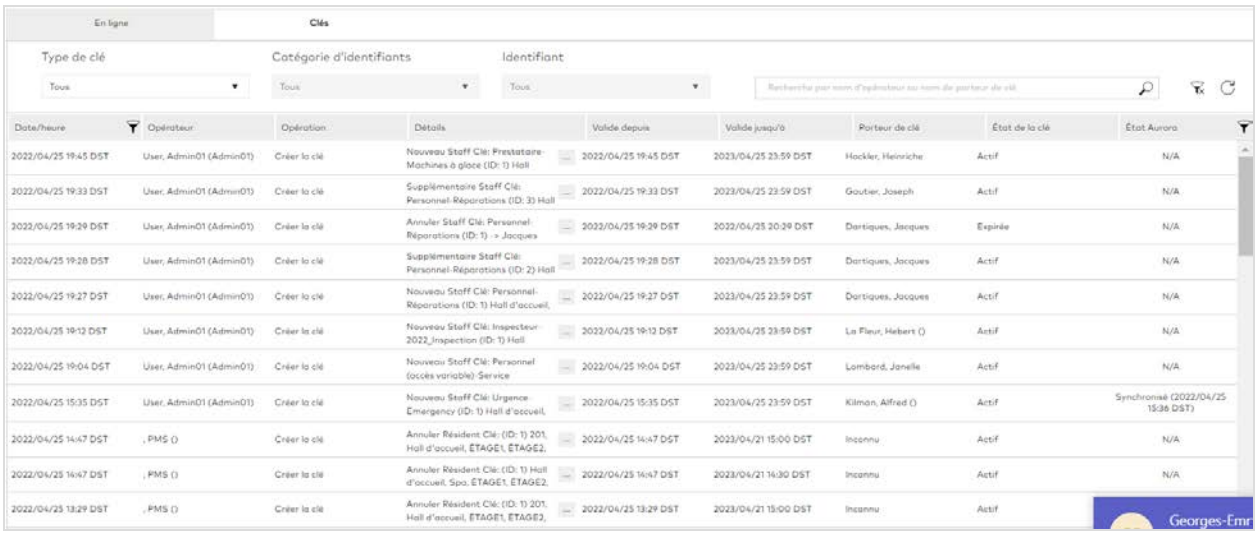


Le module Surveillance comprend des fonctions supplémentaires lorsque la communication en ligne est activée. Voir Surveillance (gestion des serrures à distance).

Surveiller les clés

Le module **Surveillance** vous permet de voir l'état de toutes les clés des résidents, les clés du personnel/prestataire et les clés Système. Vous pouvez filtrer la liste par type de clé, catégorie d'identifiants et identifiant, et rechercher des clés selon le nom de l'Opérateur ou du Porteur de clé.

» Accédez à **Surveillance**. (Si la communication en ligne est activée, cliquez sur l'onglet **Clés**.)



Les informations suivantes s'affichent sous forme de rapport pour chaque clé :

- **Date/Heure** — La date et l'heure d'encodage de la clé. Vous pouvez filtrer la liste selon la date et l'heure. Un maximum de 60 transactions s'affiche.
- **Opérateur** — Le nom complet de l'opérateur qui était connecté lors de l'encodage de la clé. Vous pouvez rechercher des clés qui ont été utilisées par un opérateur spécifique. « API » suivant le nom indique que la clé a été créée en utilisant l'API Community. Si la clé a été créée en utilisant l'API et que l'authentification API est désactivée, seule « API » est répertoriée.
- **Opération** — La commande CRÉER LA CLÉ.
- **Détails** — Le type de clé (résident/personnel/prestataire/système) et les points d'accès encodés sur la clé (y compris les espaces communs). Vous pouvez parcourir la liste de clés en fonction des détails.
- **Valide depuis** — La date de début de validité de la clé.
- **Valide jusqu'à** — La date après laquelle la clé est invalide.
- **Porteur de clé** — Le nom du porteur de clé. Valeurs par défaut : Résident 1 (pour les résidents) et Non attribué (pour les clés du personnel/prestataire ou Système). Vous pouvez rechercher des clés utilisées par un porteur de clé spécifique.
- **État de la clé** — Pour les clés physiques : Active/Expirée/Obsolète/Rendue. Pour les clés mobiles : Livraison en cours/Livrée/Échec/Annulation en cours/Annulée/Expirée/Obsolète.
- **État Aurora** — Lorsqu'Aurora est activé, l'état de la clé dans le système Aurora (Synchronisé/Échec/En attente/Non applicable) et la date/heure à laquelle l'état a été atteint pour la première fois. Vous pouvez filtrer la liste des clés en fonction de l'état Aurora.

Personnaliser l'affichage

- Pour filtrer les données, cliquez sur **(Filtrer)** dans l'en-tête de la colonne, sélectionnez les informations que vous souhaitez afficher, puis cliquez sur **Filtrer**. L'icône **(Filtre appliqué)** indique qu'un filtre est appliqué à la colonne.
- Pour effacer les filtres pour une colonne, cliquez sur ***(Filtre appliqué)*** ***> Effacer***.
- Pour effacer tous les filtres, cliquez sur **(Effacer les filtres)**.
- Cliquez sur n'importe quelle colonne pour trier la liste.
- Pour rafraîchir les données, cliquez sur **(Rafraîchir)**.

Surveiller l'utilisation des clés numériques

Lorsque les clés mobiles sont activées, il est possible de contrôler et de suivre le nombre de clés numériques émises dans l'établissement. Les clés numériques comprennent les clés mobiles et les clés de portefeuille. Les événements suivants nécessitent une clé numérique :

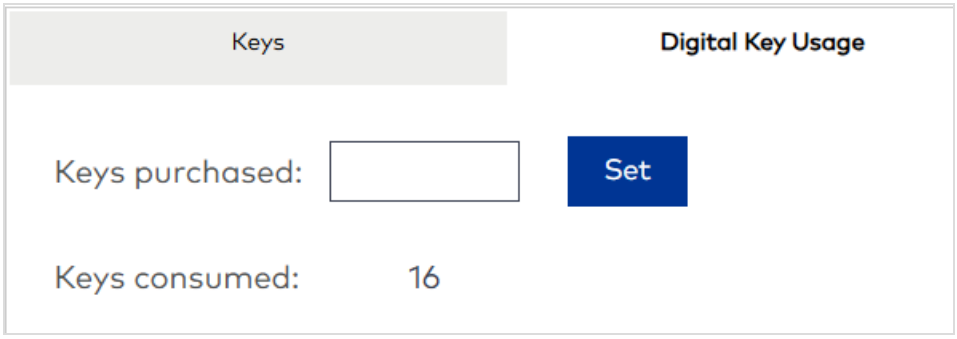
- Création d'une clé
- Mise à jour d'une clé
- Annulation d'une clé

Si le nombre de clés achetées n'est pas spécifié, c'est le nombre de clés utilisées qui s'affiche. Si le nombre de clés achetées est défini, le nombre de clés disponibles s'affiche. Chaque fois qu'un trousseau de clés est acheté (et défini), un enregistrement de l'achat s'affiche. L'enregistrement contient les informations suivantes sur chaque achat de trousseaux :

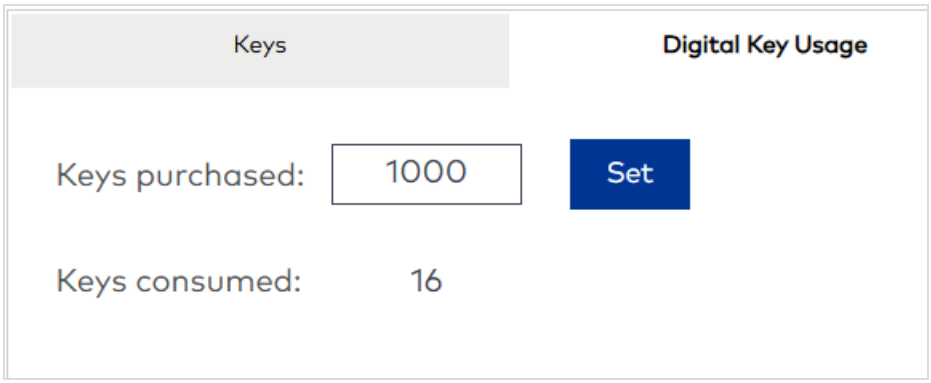
- **Date/Heure** — Date et heure auxquelles le trousseau de clés a été ajouté.
- **Opérateur** — Nom d'utilisateur/identifiant utilisateur de l'opérateur qui a ajouté le trousseau de clés.
- **Opération** — Pour l'instant, la seule opération est Ajouter une clé.
- **Nombre total de clés achetées** — Nombre de clés dans le trousseau. Le nombre augmente à chaque achat.

Ajouter un trousseau de clés

1. Accédez à **Surveillance**.
2. Sélectionnez l'onglet **Utilisation de la clé numérique**.



3. Précisez le nombre de clés achetées.



4. Cliquez sur **Définir**.



Si un autre trousseau de clés est acheté, le nombre de clés augmente. La figure suivante montre le résultat de l'ajout de 100 clés.



Rapports

Rapports

Cette section comprend les sujets suivants :

Rapport d'audit de point d'accès 259
Rapport sur les attributions des identifiants/points d'accès 261
Rapport sur la configuration des ascenseurs 262
Rapport sur les expirations de clés 263
Key/User Assignment Report 264
Rapport sur les opérateurs 265
Rapport sur la configuration du site 266
Rapport sur les rôles et droits 267
Rapport des accès du personnel/prestataire 268
Rapport sur l'activité système 269
Rapport de gestion des visiteurs 271

Rapport d'audit de point d'accès

Ce rapport fournit des détails descriptifs et d'événements sur une serrure. Avant de générer un rapport d'audit de point d'accès, vous devez d'abord auditer la serrure (dans le module **Programmation et audit**). Le processus d'audit transfère des données de la serrure vers Community. Le fichier d'interrogation qui en résulte peut être consulté immédiatement après le transfert ou dans le module **Rapports**. La consultation d'audits de points d'accès dans le module **Rapports** vous permet de sélectionner une plage de dates pour inclure des fichiers d'interrogation historiques.

Le transfert des données d'audit de serrure de M-Unit vers un poste de travail nécessite le client Community. Téléchargez et installez le client à partir de la barre d'outils principale du module **Programmation et audit** ou **Gestion des périphériques**.

Générer un rapport

1. Accédez à ***Rapports > Rapport d'audit de point d'accès***.
2. Sélectionner le point d'accès pour lequel vous souhaitez transférer les données vers Community. Plusieurs fichiers pour le même point d'accès indiquent que la serrure a été auditée à plusieurs reprises. Vérifiez la date pour déterminer l'audit que vous souhaitez consulter.
3. Cliquez sur **Continuer vers la liste d'audit**.
4. Sélectionnez l'audit pour lequel vous souhaitez générer un rapport.
5. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Date d'audit
- Événements d'audit
- Audit importé par
- Méthode d'audit
- Site
- Rapport généré par
- Rapport généré le
- Date/heure du programmateur M-Unit lors de l'audit
- Informations sur le point d'accès
  - Point d'accès
  - Type de point d'accès
  - Description
  - Modèle de serrure
- État de la serrure
  - Version du firmware de la serrure
  - Fuseau horaire
  - L'heure d'été commence le
  - L'heure d'été se termine le
  - État de la batterie
  - Verrouillé (OUI ou NON)
- Séq
- Date de l'événement

- Description de l'événement
- Résultat de l'action

Rapport sur les attributions des identifiants/points d'accès

Générez ce rapport pour afficher les affectations des identifiants/points d'accès. Les listes des catégories d'identifiants/des identifiants que vous pouvez sélectionner pour les inclure dans le rapport contiennent à la fois des catégories/identifiants par défaut et personnalisés. Toutefois, la liste reflète seulement les catégories/identifiants pour lesquels des clés ont été créées. Si la catégorie ou l'identifiant n'a pas encore été affecté(e) et encodé(e) sur une clé, elle/il n'est pas contenu(e) dans la liste.

Générer un rapport

1. Accédez à ***Rapports > Rapport sur les attributions des identifiants/points d'accès***.
2. Sélectionnez l'une des options d'index suivantes :
   - **Point d'accès**
   - **Identifiant**
3. Cliquez sur **Continuer vers les catégories d'identifiants**.
   Toutes les catégories étant sélectionnées par défaut, désélectionnez toute catégorie que vous souhaitez exclure du rapport.
4. Cliquez sur **Générer**.

Afficher les détails du rapport (point d'accès)

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Affiché par
  - Point d'accès
- Nombre total de clés
- Site
- Rapport généré par
- Rapport généré le
- Catégorie(s) d'identifiants
- Point d'accès
- Catégorie d'identifiants
- Identifiant

Afficher les détails du rapport (identifiant)

- Affiché par
  - Identifiant
- Nombre total de clés
- Site
- Rapport généré par
- Rapport généré le
- Catégorie(s) d'identifiants
- Catégorie d'identifiants
- Identifiant
- Point d'accès

Rapport sur la configuration des ascenseurs

Générez ce rapport pour consulter les informations sur la configuration d'un groupe d'ascenseurs. Le rapport affiche la cartographie des relais d'étages pour chaque panneau du groupe et liste les détails des ascenseurs.

Générer un rapport

1. Accédez à ***Rapports > Rapport sur la configuration des ascenseurs***.
2. Sélectionnez un groupe d'ascenseurs.
3. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Bâtiment
- Site
- Rapport généré le
- Rapport généré par
- Groupe d'ascenseurs
- Ascenseurs
- Profil
- Carte relais
- Relais
- Étage

Rapport sur les expirations de clés

Générez ce rapport pour identifier les clés sur le point d'expirer. Les listes des catégories d'identifiants/des identifiants que vous pouvez sélectionner pour les inclure dans le rapport contiennent à la fois des catégories/identifiants par défaut et personnalisés. Toutefois, la liste reflète seulement les catégories/identifiants pour lesquels des clés ont été créées. Si la catégorie ou l'identifiant n'a pas encore été affecté(e) et encodé(e) sur une clé, elle/il n'est pas contenu(e) dans la liste.

Générer un rapport

1. Accédez à ***Rapports > Rapport sur les expirations de clés***.
2. Toutes les catégories étant sélectionnées par défaut, désélectionnez toute catégorie que vous souhaitez exclure du rapport.
3. Cliquez sur **Continuer vers les identifiants**.
4. Tous les identifiants étant sélectionnés par défaut, désélectionnez tout identifiant que vous souhaitez exclure du rapport.
5. Cliquez sur **Continuer vers la plage de dates**.
6. Définir la période à inclure dans le rapport.
7. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

Le rapport affiche les détails suivants pour toutes les clés actuelles et expirées pour les options sélectionnées.

- Plage de dates
- Nombre total de clés attribuées
- Site
- Rapport généré par
- Rapport généré le
- Identifiants
- Catégorie d'identifiants
- Identifiant (ID de la clé)
- Accès/Espaces communs supplémentaires
- Date de création
- Date d'expiration
- Porteur de clé
- État — Pour les clés physiques : Active/Expirée/Obsolète/Rendue. Pour les clés mobiles : Livraison en cours/Livrée/Échec/Annulation en cours/Annulée/Expirée/Obsolète.

Key/User Assignment Report

Generate this report to identify the keys assigned to staff/vendors. The report includes a list of all access points encoded on each assigned key.

Generate Report

1. Go to ***Reports > Key/User Assignment Report***.
2. Select whether to include active keys, inactive keys, or both in the report. (All keys with a status other than "Active" are considered inactive.)
3. Select whether to index the report by staff member/vendor name or key credential.
4. Click **Next to Credential Classes**.
5. Because all classes are selected by default, deselect any class that you want to exclude from the report.
6. Click **Generate**.

View Report Details (Staff/Vendor)

- Displayed by
- Total keys assigned
- Site
- Report generated by
- Report generated on
- Key Holder
- Credential Class
- Credential (key ID)
- Additional Access/Common Areas
- Status
- Creation Date
- Expiration Date

Rapport sur les opérateurs

Générez ce rapport pour consulter une liste d'opérateurs, les rôles qui leur sont attribués et les droits associés à chaque rôle.

Générer un rapport

1. Accédez à ***Rapports > Rapport sur les opérateurs***.
2. Tous les types d'état de l'opérateur étant sélectionnés par défaut, désélectionnez tout type d'état que vous souhaitez exclure du rapport :
   - **Actif** — Lorsque cette option est sélectionnée, le rapport inclut tous les opérateurs actifs.
   - **Désactivé** — Lorsque cette option est sélectionnée, le rapport inclut tous les opérateurs qui sont désactivés.
   - **Bloqué** — Lorsque cette option est sélectionnée, le rapport inclut tous les opérateurs bloqués par le logiciel Community.
3. Cliquez sur **Continuer vers les rôles de l'opérateur**.
   Tous les rôles étant sélectionnés par défaut, désélectionnez tout rôle que vous souhaitez exclure du rapport.
4. Cliquez sur **Générer**.

Afficher les détails du rapport



La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- État de l'opérateur
- Rôles de l'opérateur
- Nombre total d'opérateurs
- Site
- Rapport généré par
- Rapport généré le
- Nom de l'opérateur
- Nom d'utilisateur
- Rôle
- Date d'attribution
- État
  - Actif
  - Désactivé
  - Bloqué

Rapport sur la configuration du site

Générez ce rapport pour consulter la configuration des points d'accès de votre site.

Générer un rapport

1. Accédez à ***Rapports > Rapport sur la configuration du site***.
2. Sélectionnez un bâtiment.
3. Cliquez sur **Continuer vers les étages**.
4. Sélectionnez les étages que vous souhaitez inclure dans le rapport.
5. Cliquez sur **Continuer vers les types de points d'accès**.
   Tous les types de points d'accès étant sélectionnés par défaut, désélectionnez tout type que vous souhaitez exclure du rapport.
6. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Nombre total de points d'accès
- Rapport généré par
- Rapport généré le
- Bâtiments
- Étages
- Séquence (Séq)
- Point d'accès
- Type de point d'accès
- Modèle de serrure/périphérique
- Nom du bâtiment
- Nom de l'étage

Rapport sur les rôles et droits

Générez ce rapport pour afficher une liste de rôles définis dans le module **Gestion des rôles** et les fonctions Community pour lesquelles chaque rôle possède des droits.

Générer un rapport

1. Accédez à ***Rapports > Rapport sur les rôles et droits***.
2. Indiquez si vous souhaitez générer un rapport qui montre les rôles autorisés pour les droits système ou les droits de clés.
3. Choisissez d'inclure ou non des opérateurs. Si vous choisissez d'inclure les opérateurs, sélectionnez les types d'état de l'opérateur pour inclure :
   - **Actif** — Lorsque cette option est sélectionnée, le rapport inclut tous les opérateurs actifs.
   - **Désactivé** — Lorsque cette option est sélectionnée, le rapport inclut tous les opérateurs qui sont désactivés.
   - **Bloqué** — Lorsque cette option est sélectionnée, le rapport inclut tous les opérateurs bloqués par le logiciel Community.
4. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Intégrer les opérateurs
- Nombre total de rôles
- Site
- Rapport généré par
- Rapport généré le
- Rôles (y compris liste des opérateurs auxquels le rôle est attribué)
- Droits système / Droits de clé

Rapport des accès du personnel/prestataire

Générer ce rapport pour afficher les informations historiques concernant l'accès du personnel/prestataire.

Avant de générer ce rapport, vous devez obtenir et lire la clé physique attribuée aux membres du personnel/prestataires. Le rapport peut être consulté immédiatement après la lecture de la clé ou dans le module **Rapports**. La consultation de données sur les accès du personnel dans le module **Rapports** vous permet de sélectionner une plage de dates pour inclure des données historiques.

Générer un rapport

1. Accédez à ***Rapports > Rapport des accès du personnel/prestataire***.
2. Sélectionnez un nom.
3. Cliquez sur **Continuer vers la liste de clés**.
4. Sélectionnez les identifiants de clés que vous souhaitez inclure dans le rapport.
5. Cliquez sur **Continuer vers la plage de dates**.
6. Sélectionner des dates de début et de fin.
7. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Plage de dates
- Événements d'accès
- Site
- Rapport généré par
- Rapport généré le
- Identifiant
- Expire dans les serrures
- Horaire des clés du personnel
- État de la clé — Pour les clés physiques : Active/Expirée/Obsolète/Rendue. Pour les clés mobiles : Livraison en cours/Livrée/Échec/Annulation en cours/Annulée/Expirée/Obsolète.
- Séq
- Date de l'événement
- Point d'accès
- Accès autorisé
- Heure définie
- Verrouillé avec pêne dormant
- Batterie faible
- Problème de serrure ?
- Serrure verrouillée
- Nouvelle clé

Rapport sur l'activité système

Générez ce rapport pour consulter l'historique des transactions des opérateurs sélectionnés.

Générer un rapport

1. Indiquez si vous souhaitez générer un rapport qui inclut l'activité système liée aux événements de clés ou aux événements du système.
   - Si vous sélectionnez **Clé**, sélectionnez les options pour inclure les clés de résidents (clés physiques/clés mobiles), les clés du personnel/prestataire (clés physiques/clés mobiles) et les clés Système, puis cliquez sur **Continuer vers les catégories d'identifiants** et désélectionnez les catégories à exclure du rapport.
2. Cliquez sur **Continuer vers les opérateurs**.
3. Sélectionnez les opérateurs que vous souhaitez inclure dans le rapport.
4. Cliquez sur **Continuer vers la plage de dates**.
5. Définir la période pour le rapport.
6. Cliquez sur **Générer**.

Afficher les détails du rapport (clé)

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Plage de dates
- Nombre de transactions
- Site
- Rapport généré par
- Rapport généré le
- Catégories d'identifiants
- Opérateurs — Le nom complet de l'opérateur qui était connecté lors de l'encodage de la clé. « API » suivant le nom indique que la clé a été créée en utilisant l'API Community. Si la clé a été créée en utilisant l'API et que l'authentification API est désactivée, seule « API » est répertoriée.
- Date de la demande de clé
- Opérateur
- Identifiant
- Type de clé
  - Résident (physique)
  - Résident (mobile)
  - Personnel/prestataire (physique)
  - Personnel/prestataire (mobile)
  - Système
- Mode de la clé
  - Supplémentaire
  - Nouveau
- État — Pour les clés physiques : Active/Expirée/Obsolète/Rendue. Pour les clés mobiles : Livraison en cours/Livrée/Échec/Annulation en cours/Annulée/Expirée/Obsolète.
- Numéro de téléphone portable
- Porteur de clé
- Accès/Espaces communs supplémentaires

Afficher les détails du rapport (système)

- Plage de dates
- Nombre de transactions
- Site
- Rapport généré par
- Rapport généré le
- Opérateurs
- Date de la transaction
- Opérateur — Le nom complet de l'opérateur qui était connecté lors de l'encodage de la clé. « API » suivant le nom indique que la clé a été créée en utilisant l'API Community. Si la clé a été créée en utilisant l'API et que l'authentification API est désactivée, seule « API » est répertoriée.
- Opération
- Détails
- État de la transaction

Rapport de gestion des visiteurs

Ce rapport est disponible si vous disposez d'une licence pour la gestion des visiteurs.

Générer ce rapport pour afficher une liste des codes PIN et des clés mobiles attribués. Les opérateurs affectés au rôle d'Administrateur ou de Configurateur de site ont un accès par défaut pour générer ce rapport. Pour tous les autres opérateurs, le droit doit être activé pour le rôle attribué dans **Gestion des rôles**.

Générer un rapport

1. Accédez à ***Rapports > Rapport de gestion des visiteurs***.
2. Indiquez si vous souhaitez inclure les données de gestion des visiteurs pour les résidents ou le personnel. Pour le personnel, sélectionnez l'état du code PIN à inclure dans le rapport. (Les rapports pour les résidents comprennent tous les types d'état.)
3. Cliquez sur **Continuer vers les résidents** ou **Continuer vers les membres du personnel**.
4. Sélectionnez les résidents ou les membres du personnel à inclure dans le rapport.
5. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Type d'utilisateur (résident ou membre du personnel)
- Site
- Rapport généré par
- Rapport généré le
- Délégant — Le résident ou le membre du personnel qui a attribué le code PIN ou la clé mobile.
- Opération — Le type d'attribution, code PIN ou clé mobile.
- Attribué — Date et heure auxquelles le code PIN/la clé mobile a été attribué(e).
- Accès — Pour le code PIN : le code PIN, les espaces communs, le nombre d'utilisations restantes jusqu'à expiration. Pour la clé mobile : espaces communs.
- Valide du — La date/heure à laquelle l'accès à l'aide du code PIN/de la clé mobile commence.
- Valide jusqu'à — La date/heure à laquelle l'accès à l'aide du code PIN/de la clé mobile termine.
- Porteur de clé/code PIN — Nom du visiteur pour lequel le code PIN/la clé mobile a été remis(e).
- État — Actif/Annulé/Expiré. Les rapports pour les résidents comprennent tous les états. Les rapports pour le personnel ne comprennent que les états sélectionnés.

Barre d'outils

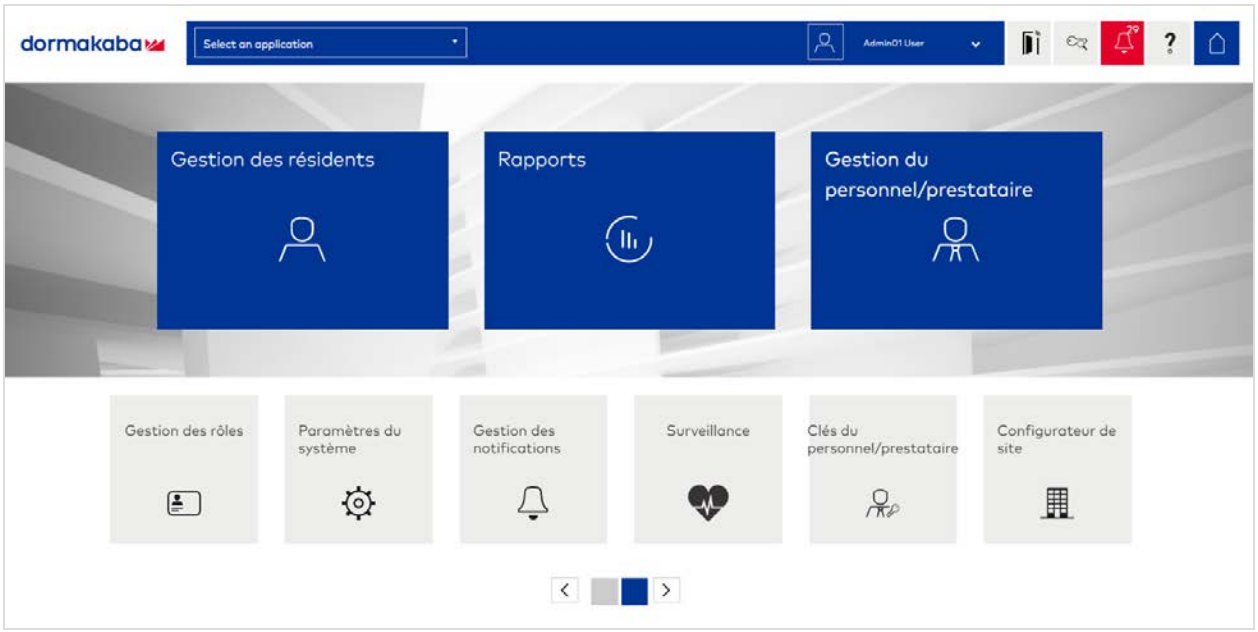
Les bases de la barre d'outils

Cette section comprend les sujets suivants :

Naviguer Community 273
Définir les préférences de l'opérateur 275
Installation / Mise à jour du Client Community 277
Sélectionner l'encodeur par défaut 278
Déverrouillage/verrouillage à distance 279
Lire la clé/effacer la clé/rapport de suivi d'accès 281
Afficher les notifications 285
Clés physiques 288
Clés mobiles 290

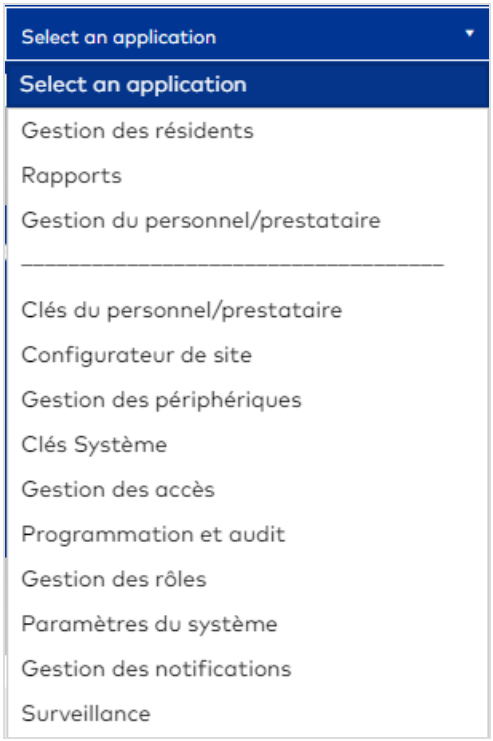
Naviguer Community

Les modules Community sont accessibles quel que soit l'endroit du produit où vous vous trouvez. Lors de votre première connexion, la page d'accueil utilise des tuiles pour permettre l'accès aux modules. La section supérieure est conçue pour afficher les favoris (les modules que vous utilisez le plus souvent). Les tuiles pour tous les autres modules se trouvent dans la section inférieure. Il peut être nécessaire de faire défiler pour afficher la tuile pour un module. Vous pouvez glisser-déposer les tuiles de la section inférieure vers la section des favoris pour personnaliser votre page d'accueil.



Sélecteur de module

À partir de n'importe quel module, vous pouvez passer rapidement à un autre module en utilisant la liste de sélection des modules dans la barre d'outils Community. Les trois premiers éléments de la liste affichent les favoris. Tous les autres modules sont affichés par ordre alphabétique.



Pour naviguer dans les modules Community :

- Depuis la page d'accueil, cliquez sur une tuile de module. Il peut être nécessaire de faire défiler la partie inférieure pour afficher la tuile d'un module.
- Sur toutes les autres pages, sélectionnez un module dans la liste de sélection des modules dans la barre d'outils Community.

Aller à la page d'accueil ou fermer la session

- Pour vous rendre sur la page d'accueil Community, cliquez sur **(Accueil)** .
- Pour fermer la session Community, cliquez sur le ***nom d'utilisateur du compte*** > **Fermer la session**.

Définir les préférences de l'opérateur

Pour définir les préférences de l'opérateur :



1. Dans la barre d'outils principale, cliquez sur ***nom d'utilisateur*** de l'***opérateur*** > **Préférences**.
2. Modifiez les paramètres ci-dessous.
3. Cliquez sur **Sauvegarder**. Après avoir enregistré les préférences, l'écran est rafraîchi avec la langue sélectionnée.

Section GÉNÉRAL



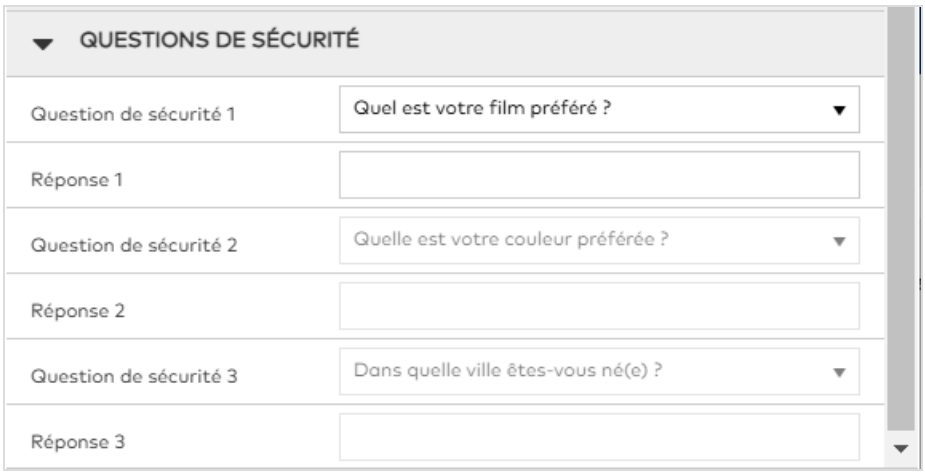
- Le nom d'utilisateur est une option en lecture seule affichant le nom d'utilisateur de l'opérateur.
- L'état du mot de passe est une option en lecture seule affichant les informations sur l'expiration du mot de passe du compte Community.
- Sélectionnez la langue préférée pour le détenteur du compte. Par défaut, l'interface utilisateur est détectée et affichée dans la langue du navigateur. Pour que Community détecte et affiche l'interface utilisateur dans la langue du navigateur, le paramètre de langue dans ***Paramètres du système > Général*** et **Préférences** doit être Détection automatique de la langue.
- Pour E-mail, indiquez une adresse e-mail à associer au compte pour les notifications. Community envoie des e-mails automatiques concernant l'état du compte. L'adresse e-mail indiquée dans le profil de l'opérateur est liée à l'adresse e-mail dans les préférences du compte.

Section MOT DE PASSE



Modifier le mot de passe du compte Community. Pour voir les valeurs, cliquez sur . Exigences par défauts pour les mots de passe : au moins huit caractères comprenant au moins l'un des caractères suivants : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux. Les critères de validité et d'expiration du mot de passe sont basés sur les paramètres sous ***Paramètres du système > Sécurité***.

Section QUESTIONS DE SÉCURITÉ



Sélectionnez et fournissez des réponses aux questions de sécurité lorsqu'elles sont requises pour soumettre une demande de récupération ou de réinitialisation du mot de passe.

Installation / Mise à jour du Client Community

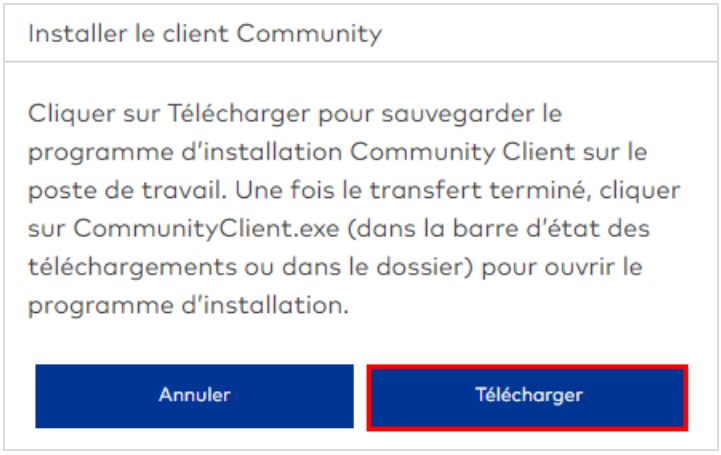
Le client Community est nécessaire pour encoder et lire les clés, ainsi que pour utiliser M-Unit afin de programmer et d'auditer les serrures et les périphériques. Le Client Community et le Serveur Community doivent être de la même version pour garantir des opérations d'encodage de clés appropriées. Lors de la connexion, Community détecte la version du Client et, si elle est antérieure à celle du Serveur, vous invite à télécharger et à installer le Client actuel.

Effectuez l'installation en tant qu'Administrateur local (et non administrateur réseau).

1. Allez dans **Gestion des périphériques** ou **Programmation et audit**.



2. Cliquez sur **(Installer le Client Community)** .



3. Cliquez sur **Télécharger**. Trois fichiers sont nécessaires Community_Client.exe, serverURL.config et token.txt. Le processus de téléchargement peut prendre jusqu'à une minute.
4. Lorsque le téléchargement est terminé, cliquez sur **Client.exe Community**. L'installateur s'ouvre. Si des logiciels anti-virus ou pare-feu sont installés sur le poste de travail, une requête peut apparaître pour permettre l'ouverture de l'installateur.
5. Sur la page de bienvenue, cliquez sur **Suivant** (ou **Réparer** si le client est déjà installé).
   La page **État de l'installation** s'affiche pendant l'installation du client.
6. Sur la page **Mise à jour terminée**, cliquez sur **Terminer**.

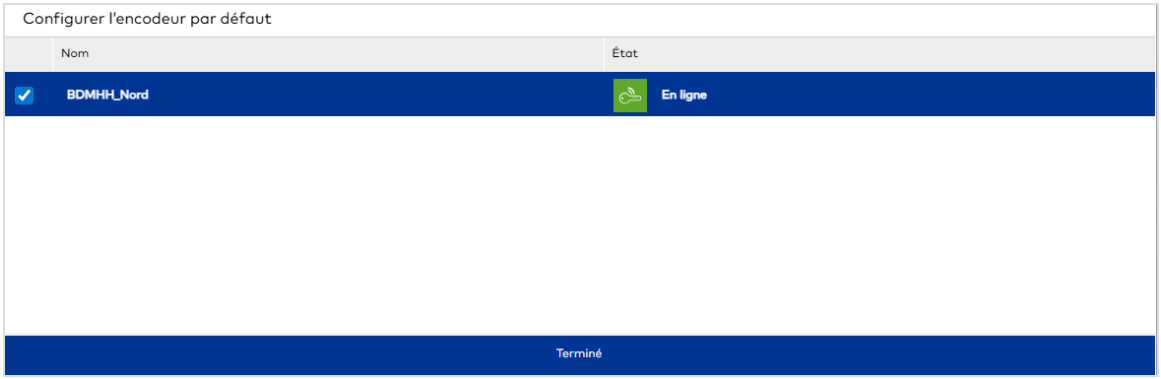
Sélectionner l'encodeur par défaut

Vous pouvez définir l'encodeur par défaut depuis la barre d'outils principale Community dans les modules où les clés sont créées. Lors de la création des clés, vous pouvez toujours sélectionner n'importe quel encodeur en ligne et à disposition du poste de travail.

1. Allez dans n'importe quel module dans lequel les clés sont créées (**Gestion des résidents**, **Gestion du personnel/prestataire**, **Clés du personnel/prestataire**, **Clés Système**).



2. Dans la barre d'outils, cliquez sur **(État de l'encodeur)** .



3. Sélectionnez l'encodeur pour recevoir automatiquement les données lors de la création de clés.
4. Cliquez sur **Terminé.**

Déverrouillage/verrouillage à distance

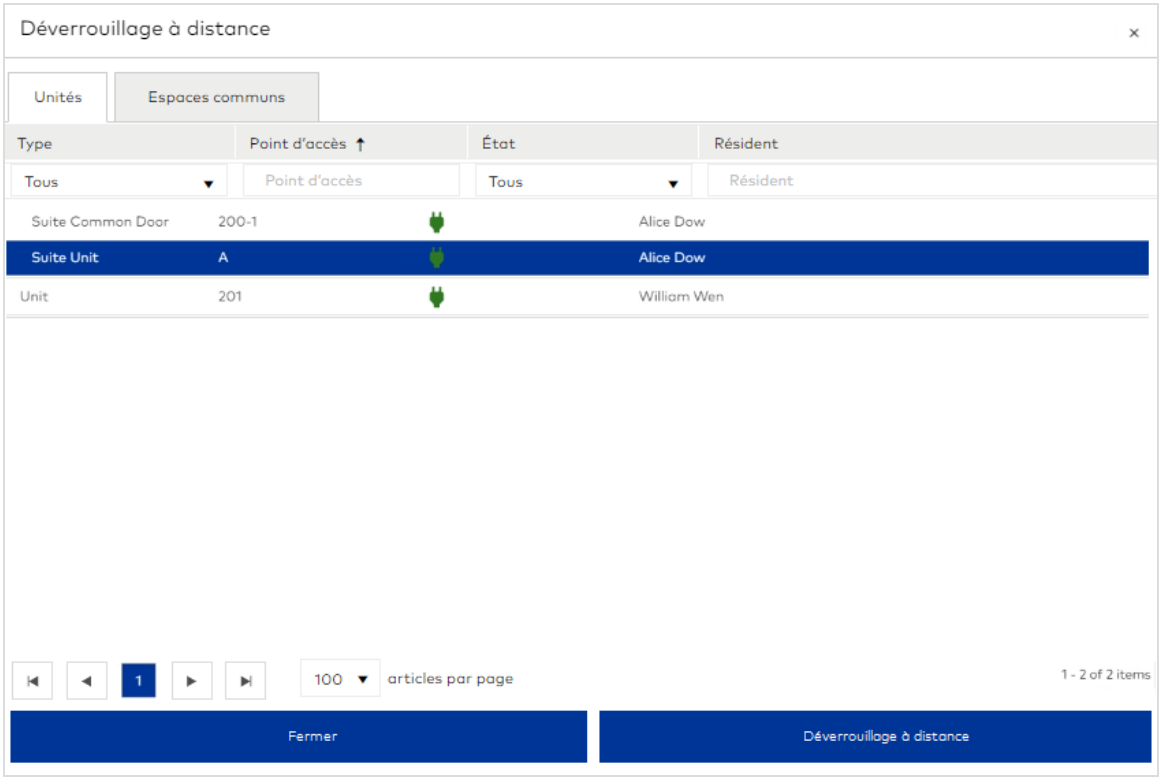
Cette option de la barre d'outils est disponible lorsque la communication en ligne est activée et configurée pour **Passerelle II ; RAC5-MFC/XT ; Rx-Link**. L'opérateur actif doit également se voir affecter un rôle avec le droit du système de **Déverrouillage à distance** activé.

La barre d'outils Community comprend une option permettant de verrouiller et déverrouiller à distance les unités occupées, les suites (porte commune et unité de suite) et les espaces communs pour les résidents. La serrure doit être en ligne pour envoyer une commande.

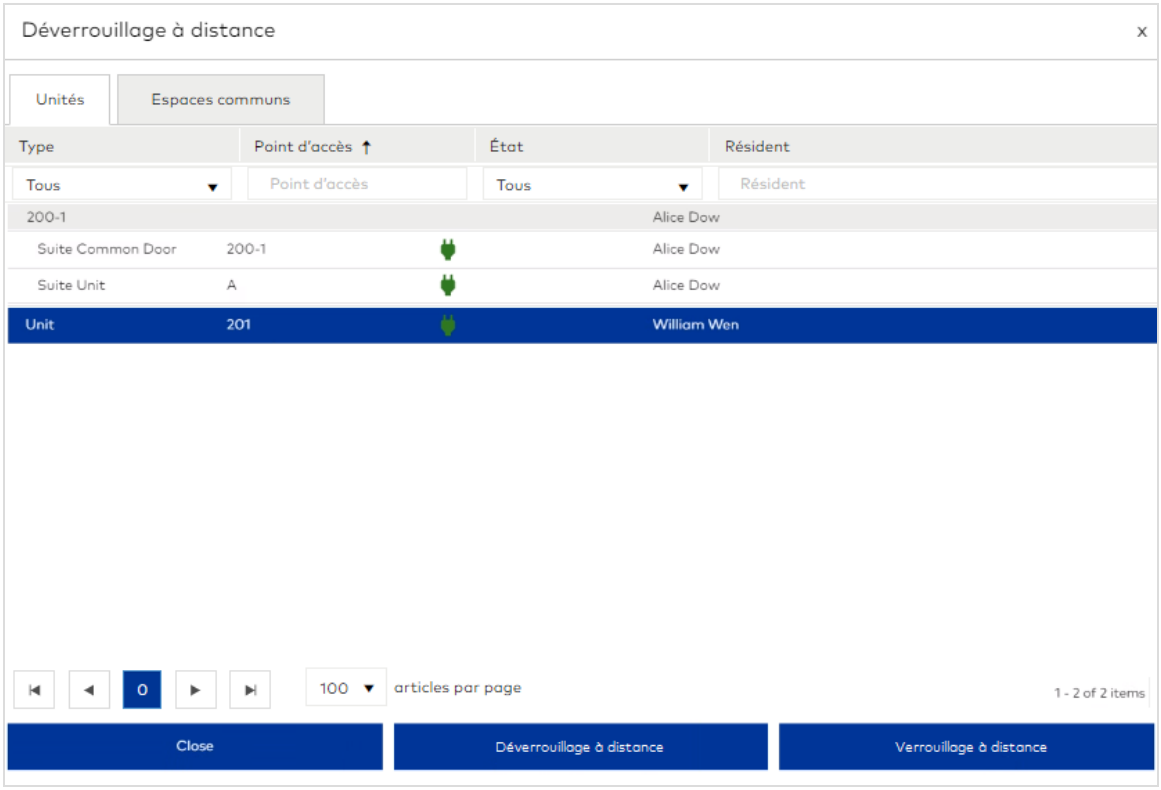


Pour verrouiller ou déverrouiller à distance un point d'accès :

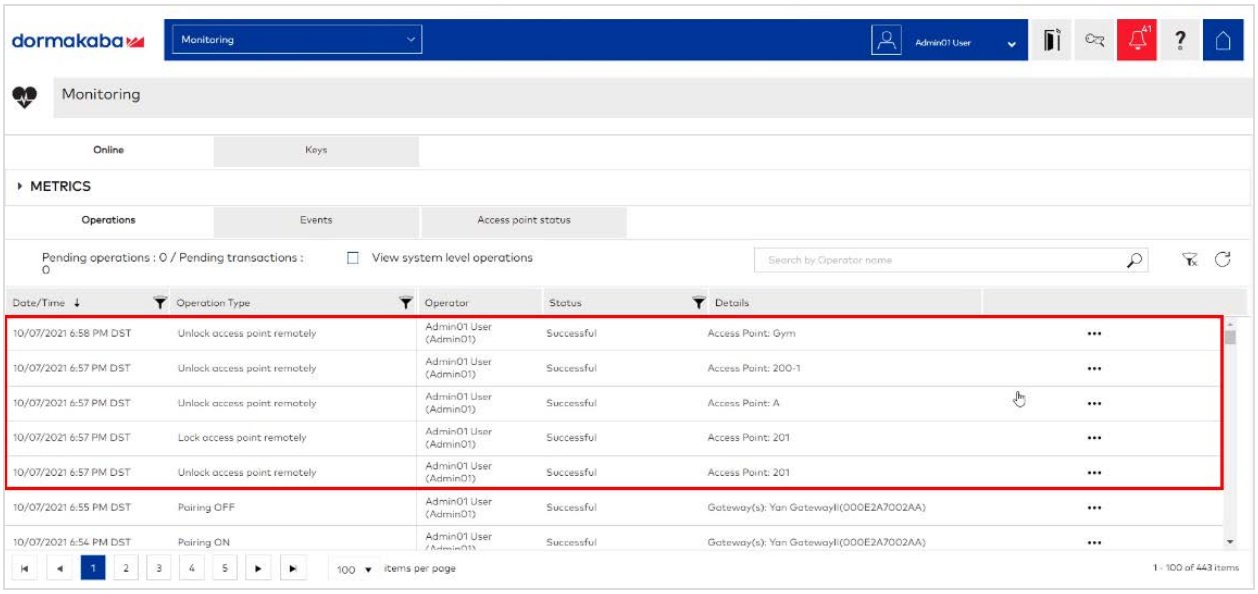
1. Cliquez sur (Déverrouillage à distance) .
2. Sélectionnez le point d'accès que vous souhaitez déverrouiller/verrouiller. Les points d'accès des unités et des suites sont répertoriés dans l'onglet **Unités** . Les espaces communs pour les résidents sont répertoriés dans l'onglet **Espaces communs**. Vous pouvez filtrer la liste par bâtiment, nom de point d'accès et état (en ligne/hors ligne). Pour les unités et les suites, vous pouvez également filtrer par type de point d'accès et par nom de résident.



3. Cliquez sur le bouton correspondant à la commande que vous souhaitez envoyer.
   - Lorsque le mode bascule n'est pas pris en charge, la seule option est de sélectionner **Déverrouillage à distance**.
   - Lorsque le mode bascule est pris en charge, sélectionnez **Déverrouillage à distance** (ou **Verrouillage à distance**). Le point d'accès reste à l'état déverrouillé (ou verrouillé) jusqu'à ce qu'une clé ou une commande valide (de la barre d'outils ou d'un horaire associé) fasse basculer l'état de la serrure.



Afficher les résultats dans le module **Surveillance** .



Lire la clé/effacer la clé/rapport de suivi d'accès

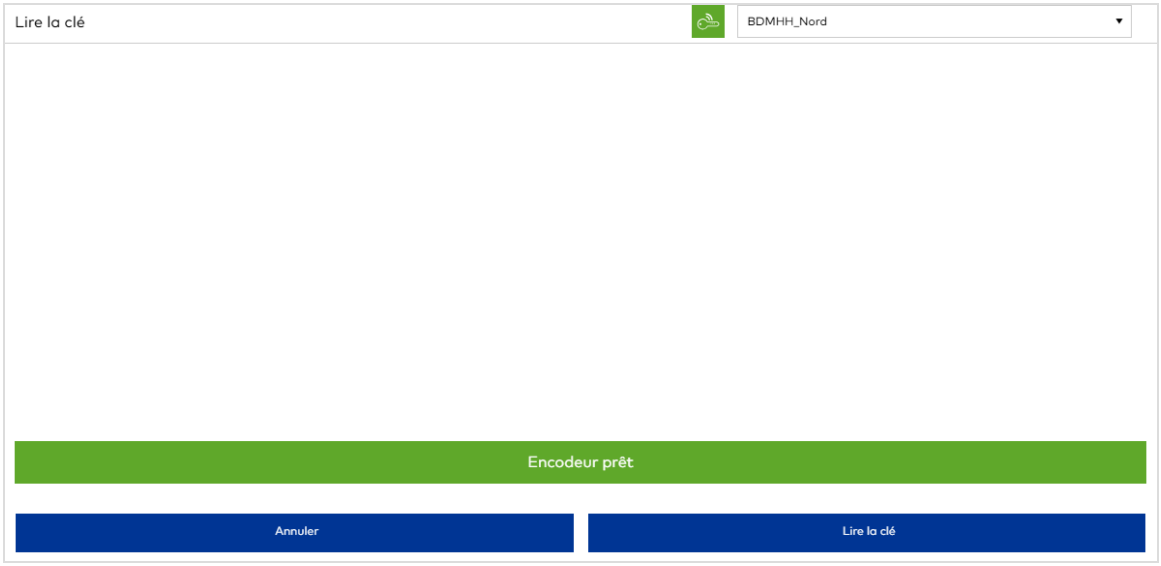
Pour connaître l'état de toute clé, utilisez le lecteur de clés Community accessible depuis la barre d'outils principale. Après la lecture d'une clé, vous pouvez effacer toutes les données de configuration encodées sur la clé et générer un rapport des accès.

Lire la clé

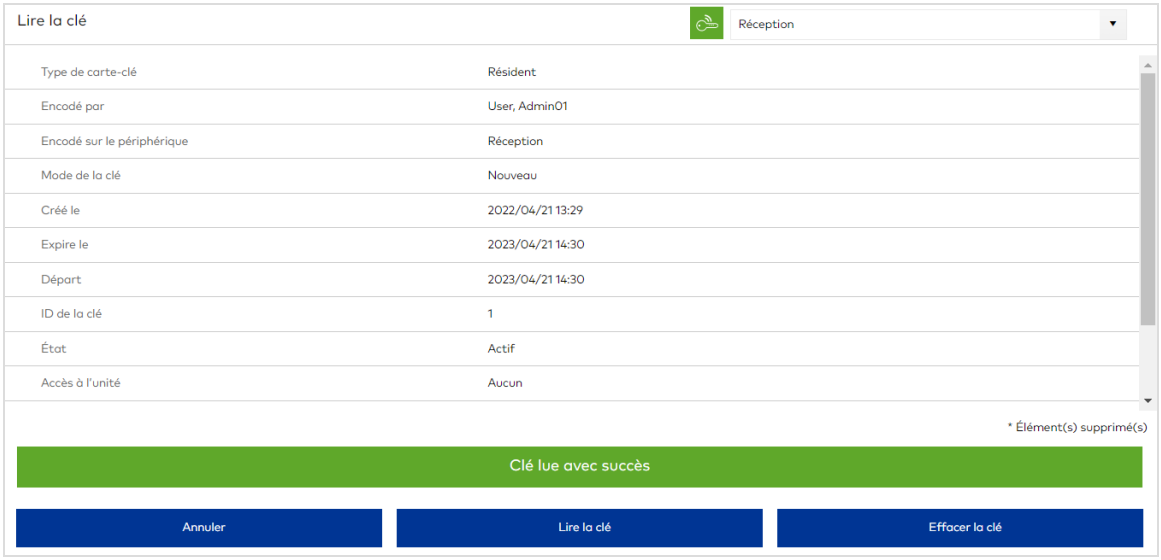
Pour lire une clé :



1. Sur la barre d'outils principale, cliquez sur **(Lire les clés)** .



2. Sélectionnez un encodeur en ligne et à disposition du poste de travail.
3. Présentez une clé à l'encodeur.
4. Cliquez sur **Lire la clé**.



Les informations affichées dépendent du type de clé. Les informations suivantes s'affichent pour les clés de résidents :

- Type de carte-clé
- Encodée par
- Encodée sur le périphérique
- Mode de la clé
- Créée le
- Expire le
- ID de la clé
- État
- Accès à l'unité
- Accès aux espaces communs
- Accès aux étages
- Encodée pour le résident

Les affichages de données supplémentaires pour les clés encodées avec un service tiers dans le secteur 2.

Échecs de lecture des clés

En cas d'échec de lecture de la clé, une fenêtre d'information identifie les problèmes suivants :

- Si la communication entre l'encodeur et le poste de travail échoue.
- Si l'encodeur est hors ligne.
- Si l'encodeur est occupé.
- Si aucune clé n'est présentée à l'encodeur dans le délai prévu.
- Si la clé est endommagée ou corrompue ou qu'elle utilise une technologie non prise en charge.

Effacer la clé

Cette fonction n'est pas prise en charge lorsque le mode de sécurité renforcée est activé. Toutefois, les clés haute sécurité peuvent être encodées de nouveau sur le même site à l'aide de la même base de données Community.

Vous ne pouvez effacer une clé (résident/personnel/prestataire/système) que directement après la lecture de la clé. Effacer une clé supprime toutes les données de configuration encodées sur la clé.

Pour effacer une clé :

1. Une fois que la clé a été lue avec succès, cliquez sur **Effacer la clé**.
2. Cliquez sur **OUI** pour confirmer.
3. Une fois terminé, cliquez sur **OK**.

Les clés effacées apparaissent comme « Rendues » dans les rapports et dans ***Surveillance > Clés***.

Lire le rapport d'accès de la clé

Après la lecture d'une clé, vous pouvez générer une liste détaillée des points d'accès auxquels la clé peut avoir accès. Ce rapport n'est disponible que lorsque les données d'accès sont sur la clé et que l'opérateur actif est autorisé à générer le rapport.

Les rapports d'accès comprennent un maximum de 72 ou 408 événements pour les clés 1k/4k respectivement. Les mini-clés MIFARE ne conservent pas les données de suivi d'accès.

Pour générer un rapport :

1. Une fois que la clé a bien été lue, cliquez sur **Afficher le rapport des accès des résidents**.
2. Une fois que la clé a bien été lue, cliquez sur **Afficher le rapport des accès du personnel/prestataire**.

Détails d'accès

- Plage de dates — Dates et heures auxquelles les événements inclus dans le rapport se sont produits.
- Événements d'accès — Le nombre d'enregistrements dans le rapport.
- Porteur de clé — Le nom du résident.
- Accès — Les points d'accès autorisés pour le porteur de clé.
- Arrivée — La date et l'heure de validité de l'accès.
- Départ — La date et l'heure d'invalidité de l'accès.
- État de la clé — L'état actuel de la clé. Pour les clés physiques : Active/Expirée/Obsolète/Rendue. Pour les clés mobiles : Livraison en cours/Livrée/Échec/Annulation en cours/Annulée/Expirée/Obsolète.
- Séq — L'ordre dans lequel un événement s'est produit.
- Date de l'événement — La date et l'heure de survenance de l'événement.
- Point d'accès — Le point d'accès auquel la clé a été présentée.
- Accès autorisé — Indique si l'accès a été autorisé lorsque la clé a été présentée.
- Heure définie — Indique si l'horloge de la serrure est réglée correctement. Si Non, la date de l'événement signalée peut être incorrecte. La raison la plus courante pour laquelle l'horloge de la serrure n'est pas réglée est le remplacement d'une pile usée. Pour les systèmes en ligne, l'horloge de la serrure se synchronise avec le système en ligne lorsque les piles sont remplacées. Pour les systèmes hors ligne, les membres du personnel peuvent utiliser une M-Unit pour réinitialiser une horloge de serrure.
- Verrouillé avec pêne dormant — Indique si le pêne dormant était sorti au moment de l'événement.
- Batterie faible — Indique si la batterie était faible au moment de l'événement.
- Problème de serrure ? — Indique un problème de serrure au moment de l'événement.
- Serrure verrouillée — Indique si la serrure était verrouillée au moment de l'événement.
- Nouvelle clé — Indique si la clé est nouvelle. Si la clé n'est pas nouvelle, il s'agit d'une clé supplémentaire.

Détails d'accès du personnel/prestataire

- Plage de dates — Dates et heures auxquelles les événements inclus dans le rapport se sont produits.
- Événements d'accès — Le nombre d'enregistrements dans le rapport.
- Identifiant — Le nom de l'identifiant et le mode de la clé (Nouvelle ou Supplémentaire).
- Horaire des clés du personnel — Le nom de tout horaire des clés du personnel attribué à la clé.
- Expiration — La date et l'heure après lesquelles l'accès à la clé est invalide.

- État de la clé — L'état actuel de la clé. Pour les clés physiques : Active/Expirée/Obsolète/Rendue. Pour les clés mobiles : Livraison en cours/Livrée/Échec/Annulation en cours/Annulée/Expirée/Obsolète.
- Séq — L'ordre dans lequel un événement s'est produit.
- Date de l'événement — La date et l'heure de survenance de l'événement.
- Point d'accès — Le point d'accès auquel la clé a été présentée.
- Accès autorisé — Indique si l'accès a été autorisé lorsque la clé a été présentée.
- Heure définie — Indique si l'horloge de la serrure est réglée correctement. Si Non, la date de l'événement signalée peut être incorrecte. La raison la plus courante pour laquelle l'horloge de la serrure n'est pas réglée est le remplacement d'une pile usée. Pour les systèmes en ligne, l'horloge de la serrure se synchronise avec le système en ligne lorsque les piles sont remplacées. Pour les systèmes hors ligne, les membres du personnel peuvent utiliser une M-Unit pour réinitialiser une horloge de serrure.
- Verrouillé avec pêne dormant — Indique si le pêne dormant était sorti au moment de l'événement.
- Batterie faible — Indique si la batterie était faible au moment de l'événement.
- Problème de serrure ? — Indique un problème de serrure au moment de l'événement.
- Serrure verrouillée — Indique si la serrure était verrouillée au moment de l'événement.
- Première utilisation de la clé — Indique si la clé a été utilisée pour accéder à un espace.

Afficher les notifications

Community offre des notifications pour tenir les opérateurs informés des événements du système.

Lorsque la communication en ligne est activée, les notifications tiennent les membres du personnel informés des opérations et des événements liés à la communication en ligne (passerelles et points d'accès assignés). Par exemple, une notification peut signaler qu'une clé est utilisée ou qu'une porte est entrebaillée.



Pour afficher les notifications récentes :

» Cliquez sur **(Notifications)** dans la barre d'outils principale. Les notifications récentes sont affichées dans une liste avec la date, l'heure et le résultat de la commande. Pour supprimer une notification récente, cliquez sur **(Supprimer)** x.

Pour voir toutes les notifications :

» Cliquez sur ***(Notifications)*** ***> VOIR TOUTES LES NOTIFICATIONS*** dans la barre d'outils principale. La liste des notifications inclut les événements sélectionnés dans les groupes de notification auxquels l'Opérateur actuel est abonné.



Les informations suivantes s'affichent pour chaque notification :

- **Notification** — Le texte de la notification/événement en ligne.
- **Catégorie** — Le type de notification : Général ou en ligne.
- **Date/heure** — La date et l'heure de survenance de l'événement.
- **Détails** — Plus d'informations sur l'événement, par exemple commande envoyée et, si applicable, le nom des points d'accès assignés.

Utilisez la barre d'outils de notifications pour rechercher des notifications et effectuer les actions suivantes :

- Supprimer les notifications — Sélectionnez une ou plusieurs notifications puis cliquez sur **(Supprimer)** .
- Effacer les notifications de la Liste des notifications récentes — Sélectionnez une ou plusieurs notifications puis cliquez sur **(Marquer comme lu)** .
- Filtrer les notifications par notification, catégorie et date/heure — Cliquez sur **(Filtre)** , sélectionnez les dates **De** et **À** puis cliquez sur **Filtrer**. Pour effacer un filtre de colonne, cliquez sur **(Filtre appliqué)** puis sur **Effacer**. Pour effacer tous les filtres, cliquez sur **(Réinitialiser les filtres)** .
- Afficher/masquer les types d'événements de notification — Cliquez sur et sélectionnez les catégories d'événements à inclure dans la liste (**Général** et **En ligne**).
- Rafraîchir les données — Cliquez sur **(Rafraîchir)** .

Événements généraux

La fonction de notification de base ne comprend que l'événement suivant :

- **Certains points d'accès doivent être reprogrammés** — Signale qu'il est nécessaire de resynchroniser les données de configuration Community pour les points d'accès répertoriés dans la colonne Détails.

Événements en ligne

- **Point d'accès hors ligne** — Signale qu'il n'y a pas de communication entre la serrure et la passerelle.
- **Point d'accès en ligne** — Signale que la serrure est en ligne et en communication avec la passerelle.
- **Point d'accès assigné** — Signale qu'un point d'accès a été assigné à une passerelle.
- **Porte entrebaillée terminé (porte sécurisée)** — La porte précédemment entrebaillée a été fermée et est sécurisée.
- **Porte entrebaillée générique** — Signale qu'une porte est en état ouvert.
- **Porte entrebaillée résident - long** — Porte entrebaillée au-delà du seuil configuré. L'événement Porte entrebaillée (long) signale qu'une porte a été laissée ouverte pendant un intervalle prolongé, ce qui indique un état inhabituel et une intrusion potentielle.
- **Porte entrebaillée résident - court** — Signale un événement de porte entrebaillée (court), ce qui signifie qu'une porte a été laissée ouverte pendant un bref intervalle, par exemple le temps nécessaire pour libérer une chambre.
- **Porte entrebaillée du personnel/prestataire - long** — Signale qu'une porte entrebaillée (long) a été laissée ouverte par un membre du personnel/prestataire pendant un intervalle prolongé, ce qui indique un état inhabituel et une intrusion potentielle en cours.
- **Porte entrebaillée du personnel/prestataire - court** — La porte entrebaillée (court) signale qu'une porte a été laissée ouverte par un membre du personnel/prestataire pendant un bref intervalle.
- **Porte verrouillée** — Signale qu'une porte est fermée avec la serrure engagée.
- **Porte ouverte** — Le mécanisme anti-crochetage de la serrure est désactivé. Il s'agit de l'état par défaut de la porte.
- **Porte déverrouillée** — Signale que le moteur de la serrure a été désengagé et que la porte peut être ouverte sans clé.
- **Ouverture sans clé (sortie) générique** — La sortie est un événement de porte ouverte.
- **Clé résident utilisée** — Date et heure d'utilisation de la clé sur un point d'accès.
- **Clé résident utilisée (première entrée)** — Signale qu'un résident a accédé à la serrure pour la première fois.
- **Passerelle hors ligne** — La passerelle ne communique pas actuellement avec le serveur Community.
- **Passerelle en ligne** — Affiche toutes les passerelles qui sont en ligne et visibles dans le module Surveillance.
- **Batterie faible** — La batterie est faible et doit être remplacée.
- **Batterie faible terminé (batterie normale)** — La notification de batterie faible a été supprimée ; la batterie a été remplacée ou le problème a été résolu.
- **Ouverture d'urgence avec clé mécanique** — Signale une ouverture forcée de la serrure, un accès à la serrure avec une clé mécanique.
- **Échec de l'opération** — L'opération spécifiée a échoué. Si disponible, la cause est indiquée.
- **Verrou d'intimité désactivée/pêne dormant rétracté** — Signale que l'état du pêne dormant est désengagé.

- **Verrou d'intimité activée/pêne dormant sorti** — Signale que le pêne dormant ou le verrou d'intimité est engagé.
- **Programmation du point d'accès requise** — La serrure peut nécessiter un reséquençage ou une synchronisation avec les données de configuration Community.
- **Clé du personnel utilisée** — Signale qu'une clé du personnel/prestataire a accédé à la serrure.
- **Intrus statique** — Alerte : Possible intrus statique. Plusieurs clés présentées sur un même point d'accès.
- **Clé système utilisée** — Signale qu'une clé système a été présentée à la serrure.
- **Intrus errant** — Alerte : Possible intrus errant. Clé présentée sur plusieurs points d'accès.

Clés physiques

Une clé désigne tout périphérique sur lequel un identifiant est encodé dans le but de contrôler l'accès et/ou d'effectuer des opérations système ou de programmation. Par exemple, cartes-clés et porte-clés.

Sélection d'un mode de la clé (Nouveau/Supplémentaire)

Toutes les clés de résidents ont un mode de la clé : Nouveau ou Supplémentaire. Lorsque vous créez une première clé pour un identifiant (une unité ou une combinaison d'unités), le seul mode que vous pouvez sélectionner est « Nouveau ». Pour toutes les clés suivantes que vous créez pour le même identifiant, l'option permet de sélectionner Nouveau ou Supplémentaire. Si vous souhaitez faire des copies de la même clé, le mode à choisir est le mode Supplémentaire par défaut sélectionné. La création de clés supplémentaires n'a pas d'effet sur les clés actives avec le même identifiant. Toutefois, la création de Nouvelles clés invalide le même identifiant sur toutes les clés précédemment actives avec le même identifiant (une fois que la Nouvelle clé est présentée à une unité ou à un espace commun de l'identifiant). La sélection du mode « Nouvelle clé » peut venir du fait que vous souhaitez remplacer des clés perdues, endommagées ou volées.

Exemple

John et Mark partagent l'accès aux unités 100 et 101. Vous créez une Nouvelle clé avec le même accès pour John. Lorsque John présente la clé à l'unité 100, la clé de Mark est invalide pour l'unité 100. Lorsque John présente la clé à l'unité 101, la clé de Mark est invalide pour l'unité 101.

Créer des clés

La création de clés est le processus d'encodage sur des clés de l'identifiant créé pendant la configuration de l'accès. Vous pouvez créer des clés physiques, des clés mobiles ou les deux pour un résident. Pour créer des clés physiques, vous devez disposer un encodeur en ligne et à disposition du poste de travail.

En cas d'erreur d'encodage ou de lecture de la clé, une fenêtre d'information identifie les problèmes suivants :

- Si la communication entre l'encodeur et le poste de travail échoue.
- Si l'encodeur est hors ligne.
- Si l'encodeur est occupé.
- Si aucune clé n'est présentée à l'encodeur dans le délai prévu.
- Si la clé est endommagée ou corrompue ou qu'elle utilise une technologie non prise en charge.

Pour des raisons de sécurité, dormakaba impose un nombre maximum de clés inutilisées qui peuvent être remises pour un identifiant donné. Par exemple, si plus de 15 clés sont remises mais jamais présentées à la Chambre 100, le point d'accès devient « hors séquence » et refuse l'accès à toutes les clés.

Pour rétablir l'accès aux clés, reprogrammez le point d'accès à l'aide du Programmateur M-Unit ou reséquencez le point d'accès à l'aide de la Clé de reséquence. Une fois reséquencé, le point d'accès accepte la dernière clé remise.

Le nombre maximum de clés inutilisées avant qu'un reséquençage ne soit nécessaire dépend du type de clé :

- Clés de résidents
  - Chambre et suite = 15
- Clés du personnel
  - Toutes les catégories = illimité
- Clés Système
  - Clés à sécurité intégrée, de verrouillage, de déverrouillage, de bascule de libre passage = 15
  - Clés ELO = 3

- Clés d'annulation = 0
- PPK/SPK = 0

État de la clé

Les états suivants s'appliquent aux clés de résidents, aux clés du personnel/prestataire et aux clés Système spécifiques (ELO, annulation, verrouillage, déverrouillage, bascule de libre passage).

Clés physiques uniquement :

- **Active** — Clés qui, selon Community, sont valides et peuvent être utilisées. Cela inclut les clés pour lesquelles une clé de déblocage a été créée et les clés débloquées à distance. L'état des Clés à sécurité intégrée est toujours Actif.
- **Rendue** — Clés qui ont été effacées.

Clés mobiles uniquement :

- **Livraison en cours – Mobile enregistré** — Clés en cours de livraison. Le serveur dormakaba détecte si le périphérique mobile est enregistré avec l'application mobile/dormakaba BlueSky.
- **Livraison en cours - Mobile non enregistré** — Clés en cours de livraison. Le périphérique mobile ne peut être pas détecté.
- **Livrée** — Clés valides pouvant être utilisées et clés invalides car elles ont atteint leur date d'expiration.
- **Annulation en cours** — Clés en cours de suppression du périphérique mobile.
- **Annulée** — Clés qui ont été supprimées du périphérique mobile.
- **Échec** — Clés qui n'ont jamais été livrées au périphérique mobile.

Toutes les clés :

- **Expirée** — Clés invalides car elles ont atteint leur date d'expiration.
- **Obsolète** — Les clés peuvent être obsolètes lorsque : a) une nouvelle clé avec le même identifiant a été créée, b) l'accès a été supprimé avant l'expiration. Les clés obsolètes peuvent comprendre l'un des sous-états suivants :
  - **Obsolète (bloquée)** — Clés pour lesquelles une clé de blocage a été créée et clés pour lesquelles une clé de blocage a été envoyée à distance.
  - **Obsolète (annulée)** — Clés pour lesquelles une clé d'annulation a été créée et clés pour lesquelles une clé d'annulation a été envoyée à distance.

En ce qui concerne les clés du personnel, les clés obsolètes continuent de donner accès aux espaces communs jusqu'à leur expiration. Pour assurer la sécurité, créez des clés de blocage pour les séquences de clés dont l'état est *Obsolète*. Voir Paramètres du système > Clés de blocage.

Clés mobiles

Les clés mobiles fonctionnent avec BlueSky dormakaba pour offrir la commodité d'une clé virtuelle. Généralement, les coûts supplémentaires sont associés à l'utilisation de clés mobiles. Consultez LEGIC ou votre opérateur mobile pour plus de détails.

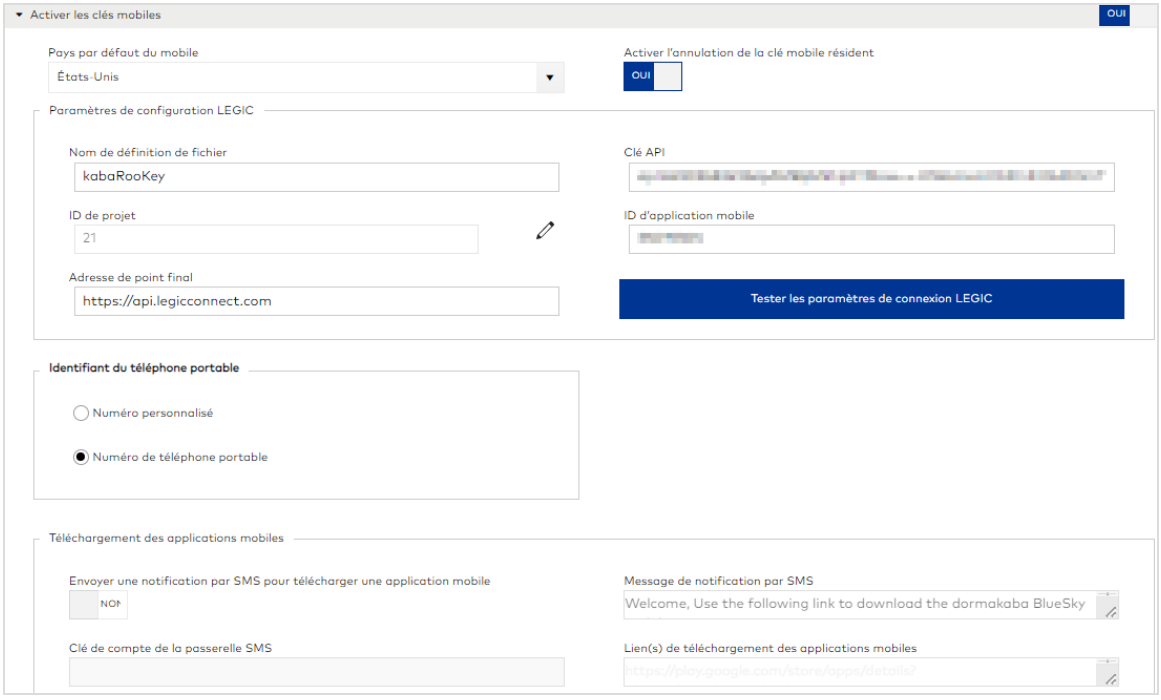
Exigences

- les clés mobiles doivent être activées dans ***Paramètres du système > Paramètres avancés***.
- Le profil du résident et membre du personnel/prestataire doit comporter un numéro de téléphone portable valide ou un numéro personnalisé.
- Les résidents et membres du personnel/prestataires doivent télécharger, installer et enregistrer leur numéro de téléphone portable avec
  BlueSky dormakaba.

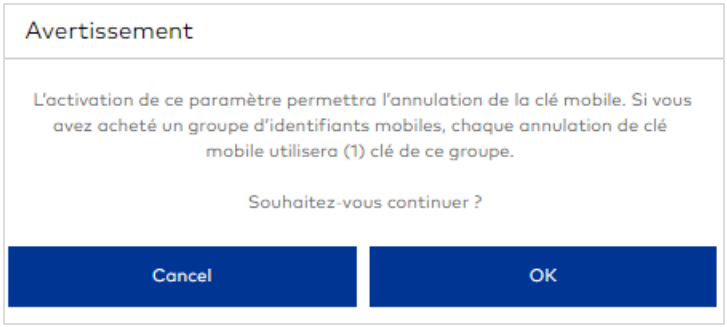
Activer les clés mobiles

Pour activer et configurer les clés mobiles :

1. Accédez aux ***Paramètres du système > Avancés***.



2. Positionnez le commutateur **Activer les clés mobiles** sur **OUI**.
3. Pour le **Pays par défaut du mobile**, sélectionnez le pays par défaut pour les numéros de téléphone portable. Le code pays correspondant est extrait pour le numéro de téléphone portable.
4. Pour annuler les clés mobiles, positionnez le commutateur **Activer l'annulation de la clé mobile résident** sur **OUI**. Si des clés mobiles sont activées et si cette option ne l'est pas, vous ne pouvez annuler une clé mobile. À la place, ce sont les détails d'expiration qui déterminent la date d'invalidité de la clé mobile.



5. Pour les **Paramètres de configuration LEGIC**, un technicien du service client de dormakaba fournit des valeurs valides.
6. Indiquez si vous souhaitez utiliser des numéros de téléphone portable ou des numéros personnalisés. Un numéro personnalisé est un identifiant numérique unique utilisé comme alternative à un numéro de téléphone portable. La génération et l'annulation des clés fonctionnent de la même manière pour les numéros de téléphone portable et les numéros personnalisés. Legic peut reconnaître un porteur de clé sur la base d'un numéro de téléphone portable ou d'un numéro personnalisé.

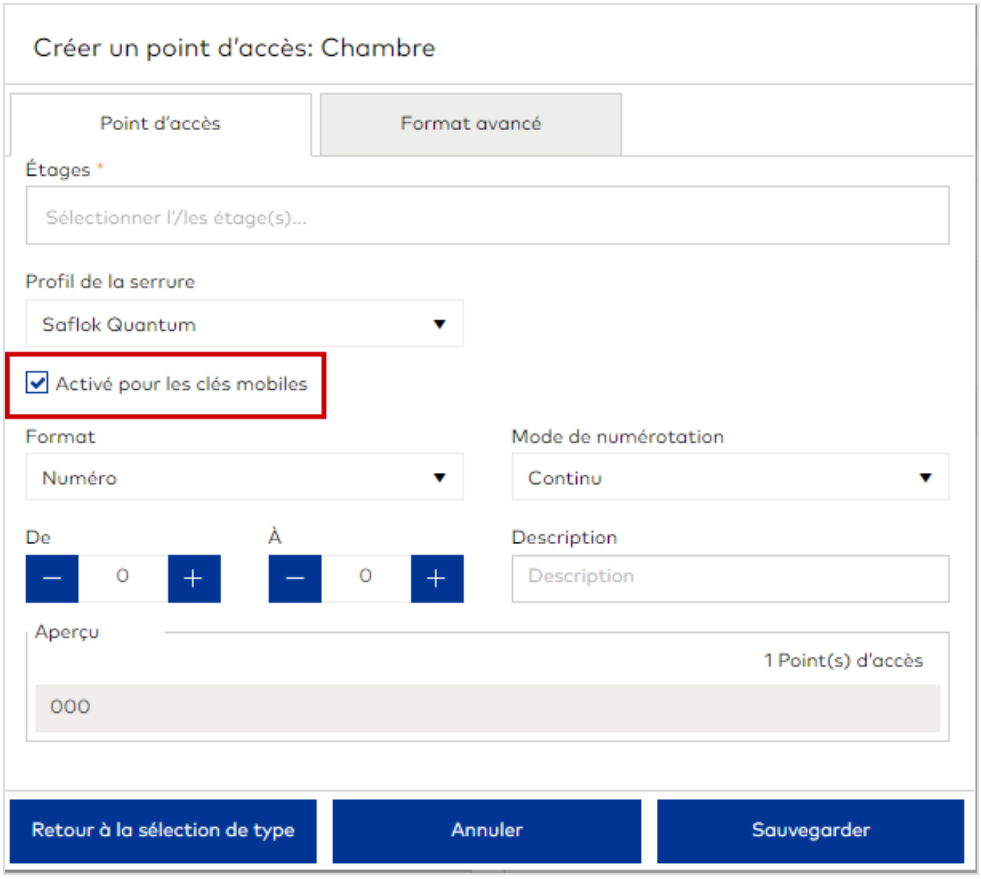
Les numéros personnalisés ne sont pris en charge que lorsque les clés mobiles sont créées/émises depuis le API.

7. Choisissez d'envoyer ou non un SMS aux destinataires de clés mobiles pour les informer que leur périphérique n'est pas enregistré dans BlueSky dormakaba. Si vous sélectionnez **OUI**, vous devez également indiquer le SMS à envoyer, une clé de compte de la passerelle SMS (voir passerelle SMS Swift) et au moins un lien où BlueSky dormakaba peut être téléchargée.

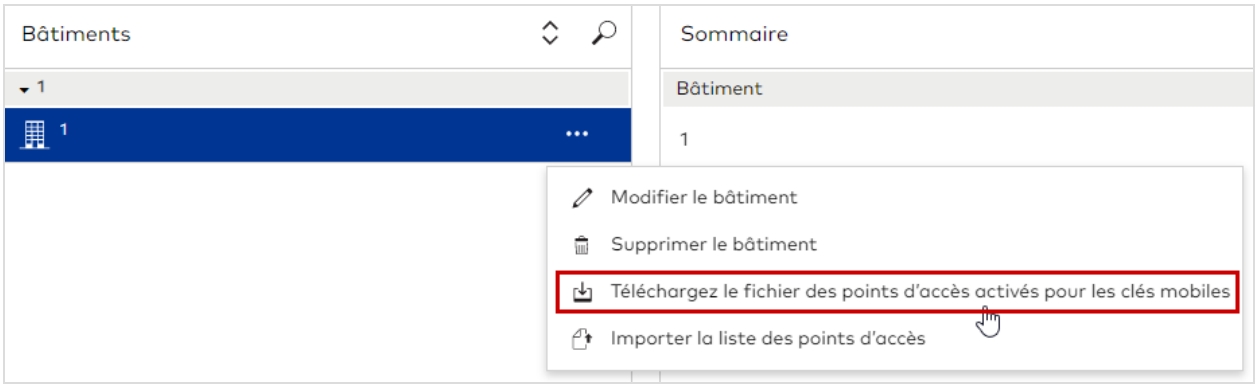
Fichier de téléchargement des clés mobiles

Dans le menu contextuel Bâtiments du Configurateur de site, vous pouvez télécharger un fichier qui répertorie tous les points d'accès configurés avec l'option **Inclure dans le fichier de téléchargement des clés mobiles** sélectionnée. Cette option permet d'identifier les serrures équipées pour accepter les identifiants de clés mobiles.

Les figures suivantes montrent l'option à sélectionner dans le Configurateur de site.



La figure suivante montre où trouver le fichier à télécharger dans Configurateur de site.



Pour télécharger le fichier des points d'accès compatibles avec l'accès mobile :

1. Ouvrez le **Configurateur de site**.
2. Sélectionnez un bâtiment.
3. Cliquez sur ***(Plus)*** ··· ***> Téléchargez le fichier des points d'accès activés pour les clés mobiles***.

Si des clés mobiles sont remises

Après la remise de la clé mobile, Community détecte la connexion du fournisseur de téléphonie mobile et vérifie que BlueSky dormakaba a été téléchargée sur le périphérique mobile. Si aucune connexion n'est détectée, l'échec est signalé dans **Surveillance** > **Clés** et **Rapports** > **Rapport sur l'activité système** (Clés). Si une connexion est détectée mais que BlueSky

dormakaba n'est pas sur le périphérique, un SMS peut être envoyé au périphérique mobile pour inviter l'utilisateur à télécharger l'application.

L'option **Envoyer une notification par SMS pour le téléchargement d'une application mobile** doit être activée dans Paramètres du système > Paramètres avancés > Activer les clés mobiles.

Lorsqu'une connexion est détectée et que BlueSky dormakaba est installée sur le périphérique mobile, l'état dans Community indique si le résident a enregistré son numéro de téléphone portable :

- **Livraison en cours - Mobile enregistré** — Clés en cours de livraison. Community détecte si le périphérique mobile est enregistré avec BlueSky dormakaba.
- **Livraison en cours - Mobile non enregistré** — Clés en cours de livraison. Community ne peut pas détecter le périphérique mobile.

Lorsque la connexion à un téléphone portable n'est pas détectée, Community réessaye toutes les 5 minutes pendant 24 heures.

Pour des raisons de sécurité, dormakaba impose un nombre maximum de clés inutilisées qui peuvent être remises pour un identifiant donné. Par exemple, si plus de 15 clés sont remises mais jamais présentées à la Chambre 100, le point d'accès devient « hors séquence » et refuse l'accès à toutes les clés.

Pour rétablir l'accès aux clés, reprogrammez le point d'accès à l'aide du Programmateur M-Unit ou reséquencez le point d'accès à l'aide de la Clé de reséquence. Une fois reséquencé, le point d'accès accepte la dernière clé remise.

Le nombre maximum de clés inutilisées avant qu'un reséquençage ne soit nécessaire dépend du type de clé :

- Clés de résidents
  - Chambre et suite = 15
- Clés du personnel
  - Toutes les catégories = illimité
- Clés Système
  - Clés à sécurité intégrée, de verrouillage, de déverrouillage, de bascule de libre passage = 15
  - Clés ELO = 3
  - Clés d'annulation = 0
  - PPK/SPK = 0

État de la clé

Les états suivants s'appliquent aux clés de résidents, aux clés du personnel/prestataire et aux clés Système spécifiques (ELO, annulation, verrouillage, déverrouillage, bascule de libre passage).

Clés physiques uniquement :

- **Active** — Clés qui, selon Community, sont valides et peuvent être utilisées. Cela inclut les clés pour lesquelles une clé de déblocage a été créée et les clés débloquées à distance. L'état des Clés à sécurité intégrée est toujours Actif.
- **Rendue** — Clés qui ont été effacées.

Clés mobiles uniquement :

- **Livraison en cours – Mobile enregistré** — Clés en cours de livraison. Le serveur dormakaba détecte si le périphérique mobile est enregistré avec l'application mobile/dormakaba BlueSky.
- **Livraison en cours - Mobile non enregistré** — Clés en cours de livraison. Le périphérique mobile ne peut être pas détecté.

- **Livrée** — Clés valides pouvant être utilisées et clés invalides car elles ont atteint leur date d'expiration.
- **Annulation en cours** — Clés en cours de suppression du périphérique mobile.
- **Annulée** — Clés qui ont été supprimées du périphérique mobile.
- **Échec** — Clés qui n'ont jamais été livrées au périphérique mobile.

Toutes les clés :

- **Expirée** — Clés invalides car elles ont atteint leur date d'expiration.
- **Obsolète** — Les clés peuvent être obsolètes lorsque : a) une nouvelle clé avec le même identifiant a été créée, b) l'accès a été supprimé avant l'expiration. Les clés obsolètes peuvent comprendre l'un des sous-états suivants :
  - **Obsolète (bloquée)** — Clés pour lesquelles une clé de blocage a été créée et clés pour lesquelles une clé de blocage a été envoyée à distance.
  - **Obsolète (annulée)** — Clés pour lesquelles une clé d'annulation a été créée et clés pour lesquelles une clé d'annulation a été envoyée à distance.

En ce qui concerne les clés du personnel, les clés obsolètes continuent de donner accès aux espaces communs jusqu'à leur expiration. Pour assurer la sécurité, créez des clés de blocage pour les séquences de clés dont l'état est *Obsolète*. Voir Paramètres du système > Clés de blocage.

Installation BlueSky dormakaba

L'application BlueSky est gratuite et consomme 34 Mo. Lors de l'installation, les résidents peuvent recevoir les invites suivantes :

- **Permettre les notifications** — La réponse sélectionnée n'affecte pas le fonctionnement des clés mobiles.
- **Mettre les données à la disposition des périphériques Bluetooth** — Les résidents doivent sélectionner **OK** car l'application mobile communique avec les serrures à l'aide de la technologie Bluetooth.
- **Pays** — Les résidents doivent sélectionner le pays associé au numéro de téléphone portable. Le pays est ajouté lors de la sélection.
- **Numéro de téléphone portable** — Les résidents doivent indiquer le numéro de téléphone complet, y compris tous les codes régionaux ou locaux.
- **Conditions d'utilisation** et **Politique de confidentialité** — Les résidents doivent accepter les conditions d'utilisation et la politique de confidentialité.
- **Partager les modèles d'utilisation** — La réponse sélectionnée n'affecte pas le fonctionnement des clés mobiles.

Si un utilisateur de BlueSky supprime l'application, une clé mobile doit être envoyée à nouveau après que l'utilisateur a réinstallé l'application.

Gestion des serrures à

Cette section comprend les sujets suivants :

- Introduction 296
- Activer et configurer la communication en ligne 297

Passerelles et points d'accès assignés 304

- Gérer la configuration du périphérique en ligne 305
- Passerelles enregistrées et points d'accès assignés 307

Gestion des notifications 312

- En savoir plus sur la gestion des notifications 313
- Ajouter des groupes de notification 315

Surveillance (à distance) 317

- En savoir plus sur la surveillance 318
- Afficher les indicateurs 319
- Surveiller des opérations en ligne 320
- Surveiller les événements en ligne 322
- Surveiller l'état des points d'accès 325

Rapports (à distance) 326

- Rapport d'état des points d'accès en ligne 327
- Rapport d'état de la passerelle en ligne 328
- Rapport du point d'accès assigné et en ligne 329

Introduction

Le déploiement de la communication en ligne nécessite la configuration de passerelles pour qu'elles fonctionnent avec le serveur Community. Les passerelles sont les périphériques réseau appairés à des points d'accès pour la communication en ligne (pour effectuer des opérations à distance et recevoir les événements du point d'accès). Lorsqu'une passerelle est répertoriée dans la **Gestion des périphériques** et que l'état de connectivité est En ligne, les points d'accès peuvent être appairés. Il est possible de connecter plusieurs passerelles à Community, mais chaque point d'accès peut uniquement être assigné à une passerelle.

Une fois la configuration terminée, des commandes à distance peuvent être envoyées aux passerelles et aux points d'accès assignés. Toutes les transmissions de demandes et de résultats sont effectuées en temps réel.

Les modules **Gestion des périphériques**, **Surveillance**, **Gestion des notifications** et **Rapports** fournissent tous des moyens de rester informé sur les périphériques et la communication qui permettent la communication en ligne.

Activer et configurer la communication en ligne

Pour activer la communication en ligne :

» Accédez à ***Paramètres du système > Avancés > Activer la communication en ligne*** et réglez le commutateur sur **OUI**.

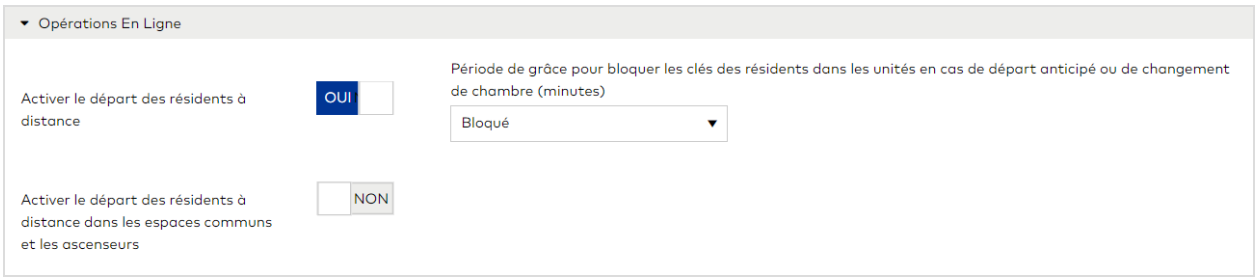


Après avoir activé la communication en ligne, la catégorie **Communication en ligne** s'affiche.

Pour les périphériques Control 4, la seule option pertinente est de s'assurer qu'**Utilisation des périphériques Passerelle I dormakaba** est sélectionnée.

1. Accédez à ***Paramètres du système > Communication en ligne***
2. Configurez les paramètres dans les sections suivantes :
   - Opérations en ligne
   - Paramètres de communication
   - Notifications
   - Rx-Link (si vous l'utilisez)
   - Communication INNCOM (si vous l'utilisez)
3. Cliquez sur (Sauvegarder).

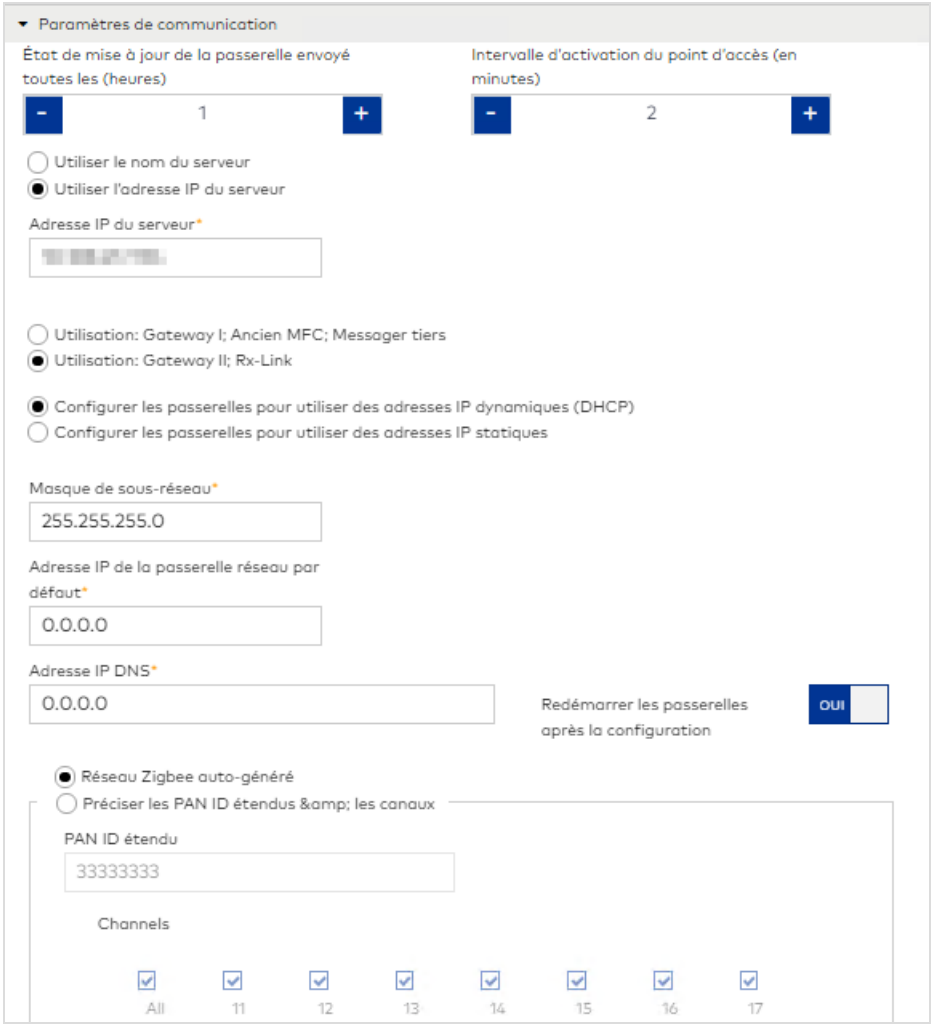
Opérations en ligne



- Réglez l'option **Activer le départ des résidents à distance** sur **OUI** pour activer le départ à distance des unités, des unités de suite et des salles de réunion dans **Gestion des résidents**. Valeur par défaut : OUI.
- Spécifiez le nombre de minutes pendant lesquelles les clés de résidents restent valides après les modifications apportées à l'affectation d'un résident et la mise à jour des clés à distance. Par exemple, si vous avez modifié l'affectation d'un résident pour un résident, l'accès à la nouvelle unité commence dès que les clés sont mises à jour à distance, mais l'accès à l'unité d'origine n'est pas annulé tant que le nombre de minutes spécifié comme période de grâce n'est pas atteint. Valeur par défaut : 5.
- **Activer le départ des résidents à distance dans les espaces communs et les ascenseurs** — Réglez sur **OUI** pour activer le départ à distance des espaces communs résident et des ascenseurs dans Gestion des résidents. Valeur par défaut : NON. Lorsqu'il est désactivé, l'accès (aux espaces communs/ascenseurs) reste valide jusqu'à la date/heure d'expiration de la clé.

L'activation du départ des résidents à distance pour les espaces communs résident et les ascenseurs peut avoir un impact significatif sur le réseau et les performances en ligne.

Paramètres de communication



- **État de mise à jour de la passerelle envoyé toutes les** — Spécifiez la fréquence de mise à jour de l'état de la passerelle. Valeurs valides : 1-255. Valeur par défaut : 1.
- **Intervalle de réveil des points d'accès** — Spécifiez la fréquence à laquelle les points d'accès vérifient si la passerelle appairée a reçu des requêtes d'opération à distance. Valeur par défaut : 2.
- Indiquez s'il faut utiliser un nom de serveur ou une adresse IP statique et précisez les détails. La valeur que vous indiquez remplace toute valeur spécifiée pour le serveur IP/nom du serveur lors de la configuration d'une passerelle dans **Gestion des périphériques**.
- Sélectionnez le type de périphériques utilisés dans le déploiement :
  - **Utilisant : Passerelle I ; anciens MFC ; Messenger tiers** — Sélectionnez cette option si vous utilisez l'un des éléments suivants :
    - Les périphériques Passerelle I
    - L'ancien contrôleur d'ascenseur MFC
    - Messenger tiers (INNCOM, Interel, Telkonet, Control4)
  - **Utilisant : Passerelle II ; Rx-Link** — Sélectionnez cette option si vous utilisez l'un des éléments suivants :
    - Les périphériques Passerelle II
    - Rx-Link

L'option utilisant Passerelle II ; Rx-Link nécessite l'utilisation de l'antenne Zigbee Generation II avec la version minimale du firmware (voir la section Exigences du périphérique dans les Notes de mise à jour) et la reprogrammation de tous les points d'accès en ligne.

RAC5-MFC/XT sont supportés dans les deux modes.

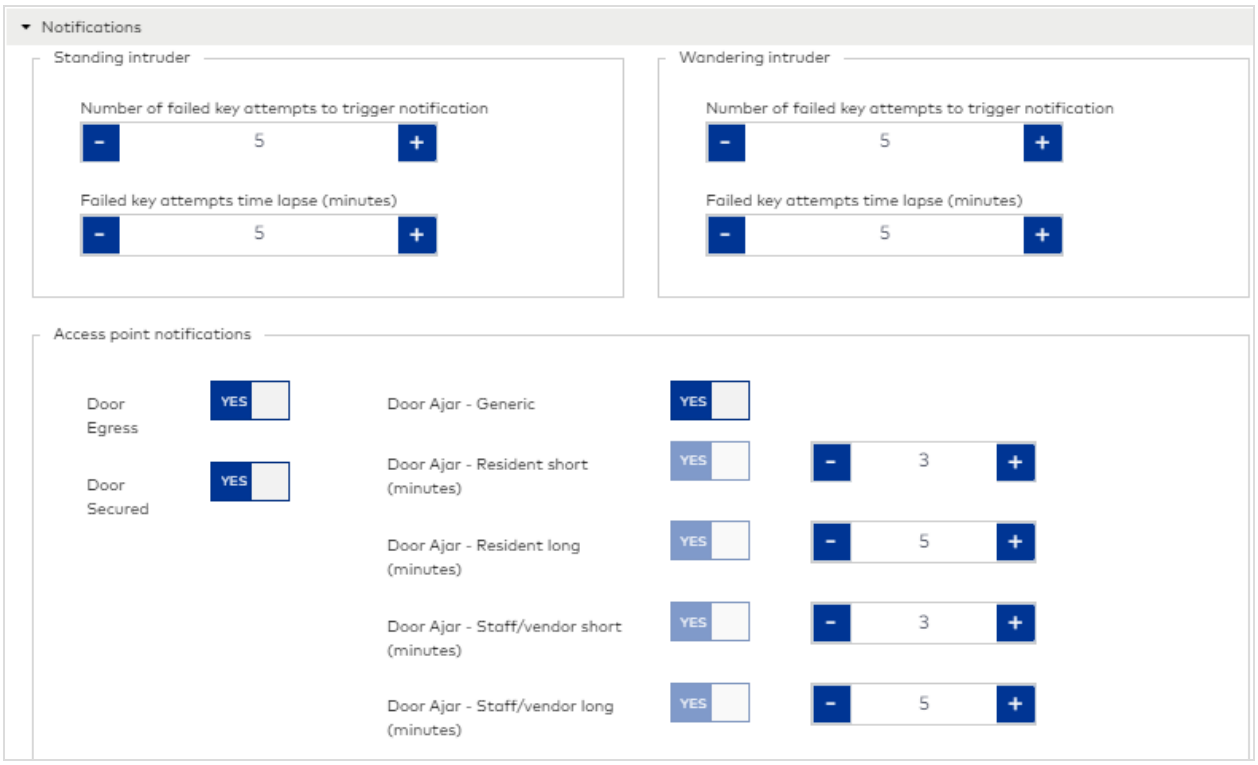
Les périphériques Passerelle II et RAC5 MFC/XT doivent être configurés dans **Gestion des périphériques**.

- Configurer les passerelles pour utiliser des adresses IP dynamiques (DHCP) ou statiques. Si vous utilisez des adresses IP dynamiques, les passerelles résolvent leur propre adresse IP. Un serveur DHCP est requis pour cette option. Si vous utilisez des adresses IP statiques, chaque passerelle doit être configurée avec une adresse IP unique.
- Indiquez si une passerelle redémarre après que la commande **Définir les paramètres de communication** a été envoyée à la passerelle dans *Gestion des périphériques > Passerelles et Points d'accès assignés*.
- Indiquez si vous souhaitez que les passerelles génèrent automatiquement les canaux de communication ZigBee les plus appropriés ou spécifiez un ID PAN (Réseau personnel) étendu unique et sélectionnez les canaux de communication de la passerelle et du point d'accès. Le PAN ID étendu doit comporter huit caractères alphanumériques. Si le PAN ID étendu est défini sur 0 (zéro), le réseau ZigBee génère automatiquement un identifiant. Les canaux 15, 20 et 25 sont recommandés pour réduire au minimum les interférences Wi-Fi.

dormakaba recommande d'utiliser la fonction de génération automatique par défaut pour attribuer automatiquement les canaux requis.

Notifications

Définissez des alertes pour les intrus potentiels et les événements liés aux points d'accès.



Intrus potentiels

Cette section décrit les alertes que vous pouvez définir pour les intrus potentiels. Le comportement qui alerte le système d'un intrus potentiel correspond au nombre d'échecs d'utilisation d'une clé dans une période définie. Le paramètre de

déclenchement des notifications peut être défini pour les intrus statiques ou errants. On parle d'intrus statique lorsque les échecs d'utilisation d'une clé ont lieu sur le même point d'accès, par exemple si une personne a acquis plusieurs clés et les présente l'une après l'autre au même point d'accès. On parle d'intrus errant potentiel si les échecs d'utilisation d'une clé ont lieu sur différents points d'accès, par exemple si quelqu'un a trouvé une clé dans le parking et parcourt le hall en présentant la clé à chaque point d'accès.

- Intrus statique
  - **Nombre d'échecs de tentatives de clés pour déclencher la notification** — Spécifiez le nombre d'échecs d'utilisation d'une clé sur un même point d'accès (dans l'intervalle de temps spécifié) pour déclencher une notification d'alerte d'intrus. Valeur par défaut : 5. Valeurs valides : 3-10.
  - **Échec des tentatives de saisie de clés** — Spécifiez le nombre de minutes pendant lesquelles les échecs d'utilisation de clé (sur le même point d'accès) doivent survenir avant le déclenchement d'une notification. Valeur par défaut : 5. Valeurs valides : 1-10.
- Intrus errant
  - **Nombre d'échecs de tentatives de clés pour déclencher la notification** — Spécifiez le nombre d'échecs d'utilisation d'une clé sur des points d'accès différents (dans l'intervalle de temps spécifié) pour déclencher une notification d'alerte d'intrus. Valeur par défaut : 5. Valeurs valides : 3-10.
  - **Échec des tentatives de saisie de clés** — Spécifiez le nombre de minutes pendant lesquelles les échecs d'utilisation de clé (sur des points d'accès différents) doivent survenir avant le déclenchement d'une notification. Valeur par défaut : 5. Valeurs valides : 1-10.

Notifications des points d'accès

Sélectionnez les événements liés aux points d'accès pour lesquels vous souhaitez recevoir des notifications :

- **Notification d'évènement du point d'accès** — Répertorie les paramètres de porte des points d'accès qui doivent être définis sur **OUI** pour activer les notifications d'état des points d'accès.
- **Sortie** — Sélectionnez **OUI** pour envoyer une notification à propos d'un événement de porte ouverte.
- **Porte sécurisée** — Sélectionnez **OUI** pour envoyer une notification indiquant que la porte est verrouillée et sécurisée.
- **Porte entrebaillée - Générique** — Sélectionnez **OUI** pour envoyer des notifications pour tous les événements Porte entrebaillée. Si NON est sélectionné, activez ou désactivez chaque événement Porte entrebaillée.
- **Porte entrebaillée - Résident court (en minutes)** — Sélectionnez **OUI** pour envoyer une notification indiquant qu'une porte a été laissée ouverte par un résident pendant une brève période (une minute), par exemple le temps nécessaire pour libérer une chambre. Spécifiez le nombre de minutes après lesquelles la notification est envoyée.
- **Porte entrebaillée - Résident long (en minutes)** — Sélectionnez **OUI** pour envoyer une notification indiquant qu'une porte a été laissée ouverte par un résident pendant une période prolongée (deux minutes), ce qui indique un état inhabituel ou une intrusion potentielle. Spécifiez le nombre de minutes après lesquelles la notification est envoyée.
- **Porte entrebaillée - Personnel/prestataire court (en minutes)** — Sélectionnez **OUI** pour envoyer une notification indiquant qu'une porte a été laissée ouverte par un membre du personnel/prestataire pendant une brève période (une minute), par exemple le temps nécessaire pour libérer une chambre. Spécifiez le nombre de minutes après lesquelles la notification est envoyée.
- **Porte entrebaillée - Personnel/prestataire long (en minutes)** — Sélectionnez **OUI** pour envoyer une notification indiquant qu'une porte a été laissée ouverte par un membre du personnel/prestataire pendant une période prolongée (deux minutes), ce qui indique un état inhabituel ou une intrusion potentielle. Spécifiez le nombre de minutes après lesquelles la notification est envoyée.

Les intervalles de temps par défaut pour les notifications d'événements de points d'accès devraient être basés sur les meilleures pratiques en tenant compte de la sécurité.

Rx-Link

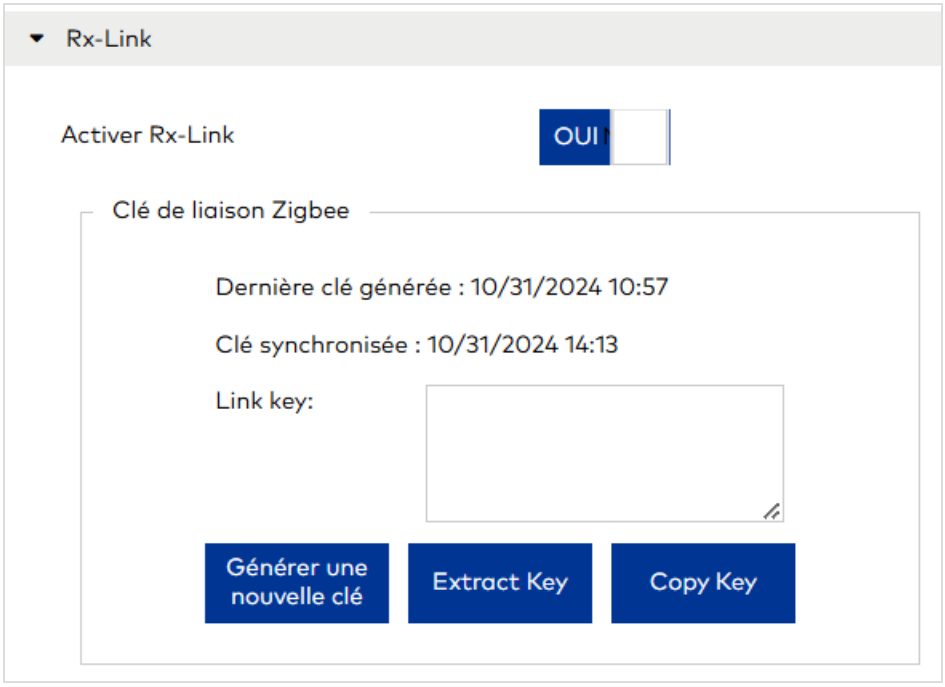
Pour une documentation complète sur Rx-Link, reportez-vous à *CommunityManuel de déploiement et de support Rx-Link* et *Community Spécifications d'intégration des partenaires Rx-Link*.

La section Rx-Link s'affiche lorsque le paramètre de communication **utilisant : Passerelle II ; RAC5-MFC/XT ; Rx-Link** est sélectionné.

Indiquez s'il faut activer Rx-Link ou non. Lorsqu'elle est activée, la Gestion des paramètres Rx-Link dans les Droits du système de gestion des rôles est affichée avec les paramètres par défaut qui autorisent les rôles d'administrateur et de configurateur de site.

Lorsque vous modifiez ce paramètre (activation ou désactivation) ou que vous générez une nouvelle clé de liaison Zigbee tierce, tous les points d'accès doivent être reprogrammés.

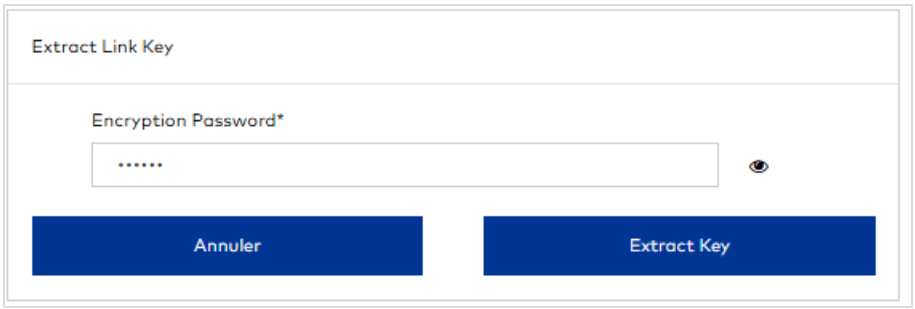
Clé de liaison Zigbee



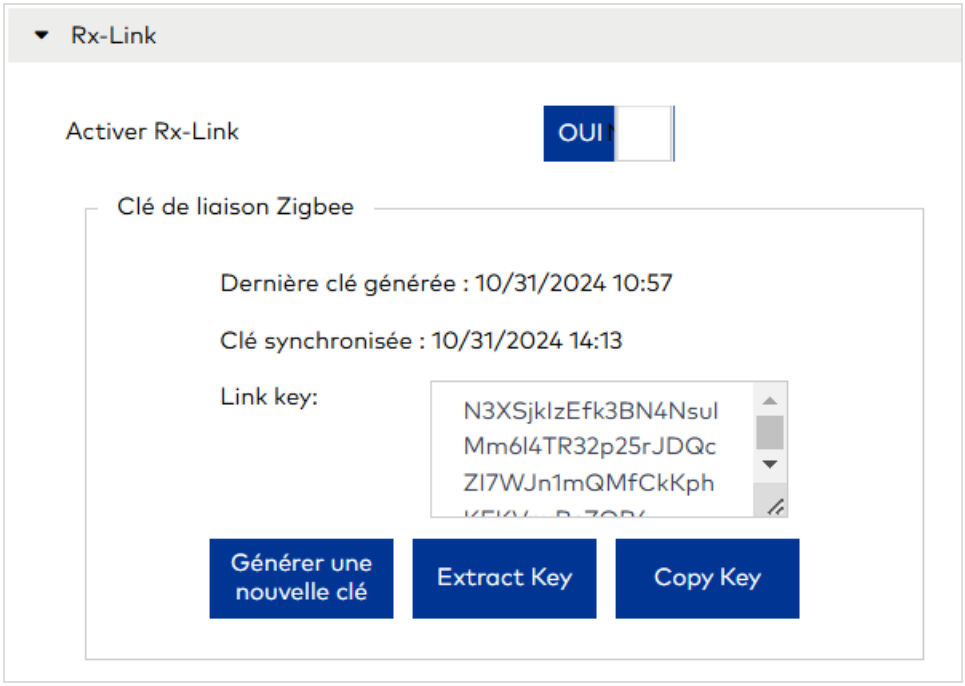
Si vous activez Rx-Link, les informations relatives à la clé de liaison Zigbee sont affichées (la date/heure de la clé la plus récente et la date de synchronisation de la clé). Cliquez sur **Générer une nouvelle clé** pour générer la clé de liaison initiale ou une nouvelle clé de liaison.

Pour les tiers qui exigent que la clé de liaison soit partagée dans un format lisible, extraire la clé de liaison :

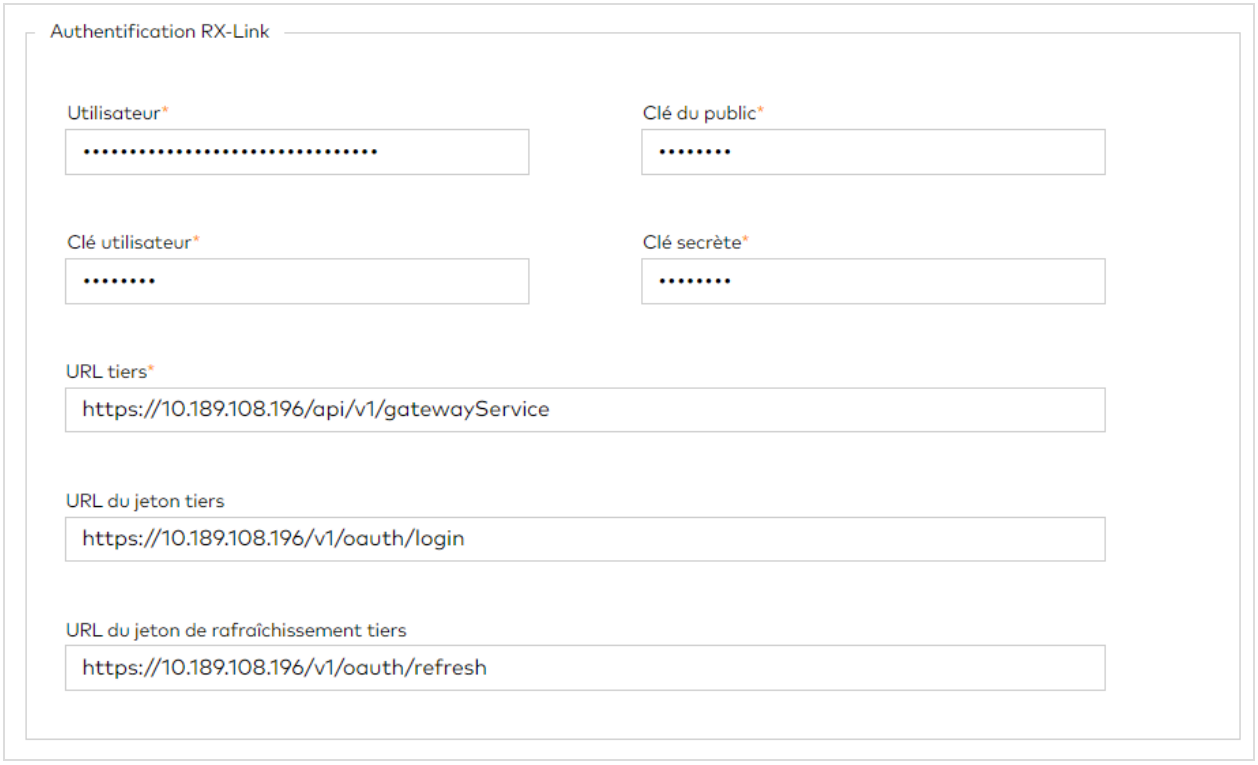
1. Cliquez sur **Extraire la clé**.



2. Indiquez un mot de passe pour la clé. Nombre minimum de caractères : 6.
3. Cliquez sur **Extraire la clé**. La clé de liaison s'affiche dans un format lisible.
4. Cliquez sur **Copier la clé** pour copier la valeur de la clé de liaison dans le presse-papiers.



Authentification Rx-Link



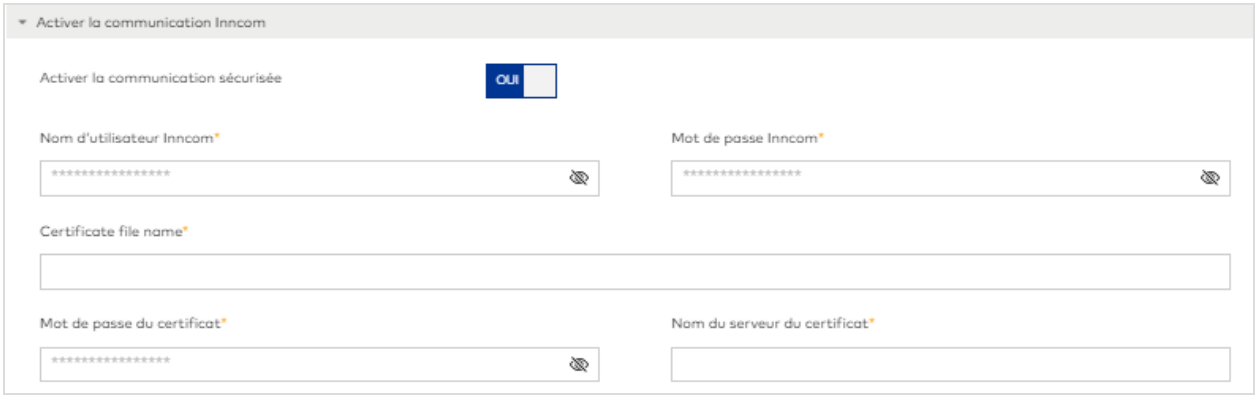
Configurer les options d'authentification :

- **Utilisateur** — L'ID unique fourni par le tiers pour l'authentification afin d'acquérir un jeton. Longueur valide : 1-2 048 caractères. Non requis lors de l'utilisation du protocole WebSocket.

- **Clé utilisateur** — Le mot de passe fourni par le tiers et associé à l'utilisateur. Longueur valide : 1-2 048 caractères. Non requis lors de l'utilisation du protocole WebSocket.
- **Clé du public** — Clé API (associée à la Clé secrète) requise par un tiers pour acquérir un jeton d'authentification auprès du serveur dormakaba. Le jeton élimine le besoin de toujours soumettre les paramètres de la clé Utilisateur/Utilisateur avec chaque requête. Valeur valide : 9b55561a54b94e2db01e15f337e902bb
- **Clé secrète** — Clé API unique (associée à la Clé du public) requise par un tiers pour acquérir un jeton d'authentification auprès du serveur dormakaba. Le jeton élimine le besoin de toujours soumettre les paramètres de la clé Utilisateur/Utilisateur avec chaque requête. Longueur valide : 1-2 048 caractères. Doit avoir une longueur de 64 octets.
- **URL tiers** — Uri du service de pontage tiers pour initier les requêtes Web faites par dormakaba au contrôleur IdO. Représente le point d'extrémité.
- **URL du jeton tiers** — Uri d'un tiers pour demander un jeton.
  Exemple : https://vriot.local-mqtt.video54.local/v1/oauth/login.
- **URL du jeton de rafraîchissement tiers** — L'Uri d'un tiers pour rafraîchir le jeton. Exemple : https://vriot.local-mqtt.video54.local/v1/oauth/refresh.

Communication INNCOM

Pour les intégrations avec INNCOM, réglez le commutateur d'activation sur **OUI**.



Si l'option de sécurisation de la communication est activée, configurez les options suivantes :

- **Nom d'utilisateur/mot de passe INNCOM** — Indiquez les identifiants du compte INNCOM afin que Community puisse se connecter au serveur INNCOM. Longueur de la valeur par réglage : 5-25 caractères.
- **Nom du fichier de certificat/mot de passe** — Spécifiez le chemin d'accès complet au nom du fichier de certificat (par exemple, c:\Program Files\dormakaba\InncomCertificate\Kaba_VHE_Client_cert.pfx) et le mot de passe sur le serveur INNCOM utilisé pour sécuriser la communication entre Community et INNCOM. Longueur de la valeur : illimitée (nom du fichier), 5-25 caractères (mot de passe).
- **Nom du serveur du certificat** — Indiquez l'adresse IP du serveur INNCOM. Longueur de la valeur : 5-25 caractères. Valeur par défaut : inncom.com.

Passerelles et points d'accès assignés

Cette section comprend les sujets suivants :

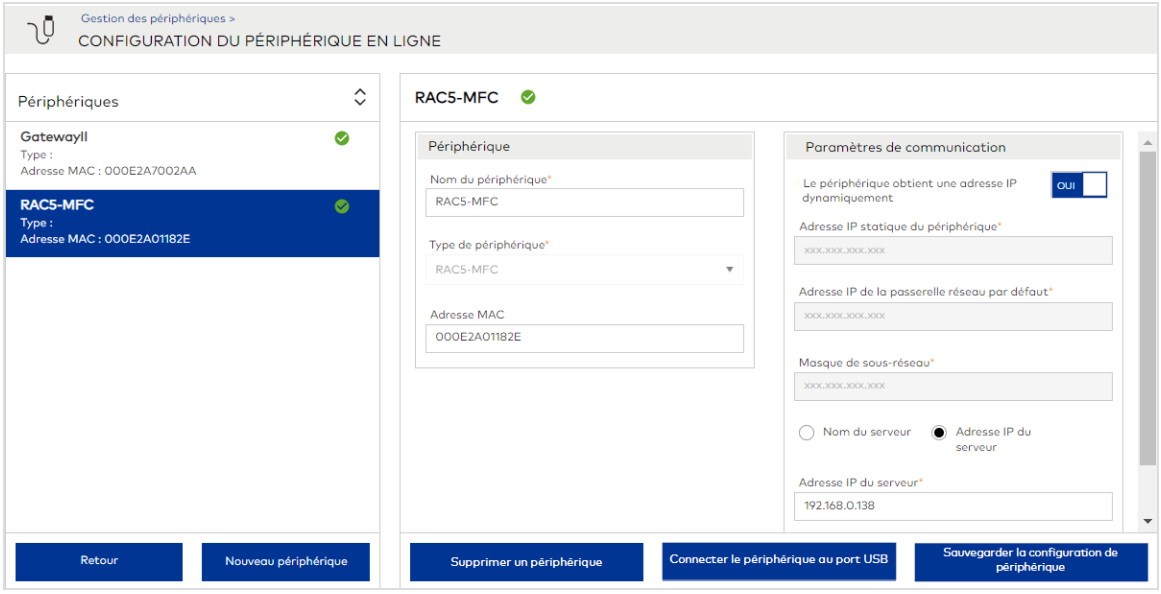
Gérer la configuration du périphérique en ligne 305
Passerelles enregistrées et points d'accès assignés 307

Gérer la configuration du périphérique en ligne

Vous pouvez ajouter, configurer et supprimer des périphériques dans le module **Gestion des périphériques**. Tous les types de périphériques peuvent être configurés dans Gestion des périphériques. Les périphériques RAC5 MFC/XT peuvent également être programmés à l'aide de M-Unit (voir ***Programmation / Audit > Programmation***).

Ajouter des périphériques en ligne

1. Accédez à ***Gestion des périphériques > Configuration du périphérique en ligne***.



2. Cliquez sur **Nouveau périphérique**.
3. Indiquez un nom unique ne dépassant pas 60 caractères. Ce nom s'affiche dans la liste des périphériques.
4. Sélectionnez le type de périphérique : Passerelle II, RAC5-MFC ou RAC5-XT.
5. Sélectionnez l'adresse MAC du périphérique que vous souhaitez configurer. L'adresse MAC du périphérique est automatiquement détectée lorsque le périphérique est connecté au poste de travail.
6. Indiquez si la passerelle obtient une adresse IP automatiquement. Si **NON**, indiquez une adresse IP statique, un numéro de port, un masque de sous-réseau et une adresse IP de passerelle réseau par défaut valides. (La passerelle réseau n'est pas la passerelle dormakaba.)
7. Indiquez si la passerelle communiquera avec le serveur Community en utilisant l'adresse IP ou le nom du serveur. Si vous utilisez le nom du serveur, vous devez également indiquer l'adresse IP ou le nom de domaine du serveur DNS local.

> La valeur IP serveur ou Nom du serveur que vous indiquez doit faire référence au même serveur que celui spécifié dans ***Paramètres du système > Communication en ligne*** >***Paramètres de communication***.

8. Indiquez le numéro de port de la passerelle pour communiquer avec le serveur Community.
9. Effectuez l'une des actions suivantes :
   - Lorsque le périphérique est connecté au poste de travail et que l'adresse MAC est renseignée, cliquez sur **Configurer le périphérique**. La configuration du périphérique est sauvegardée dans la base de données Community. Patientez 20 secondes ou mettez le périphérique de la passerelle hors tension/en marche. Lorsque la passerelle est mise en service, débranchez le périphérique du câble USB et connectez-le à Ethernet (POE ou alimentation externe).
   - Si vous avez l'intention de sauvegarder uniquement les paramètres de configuration du périphérique, cliquez sur **Sauvegarder la configuration du périphérique**.

Modifier la configuration du périphérique

1. Sélectionner un périphérique.
2. Modifier les options.
3. Cliquez sur **Sauvegarder la configuration du périphérique.**

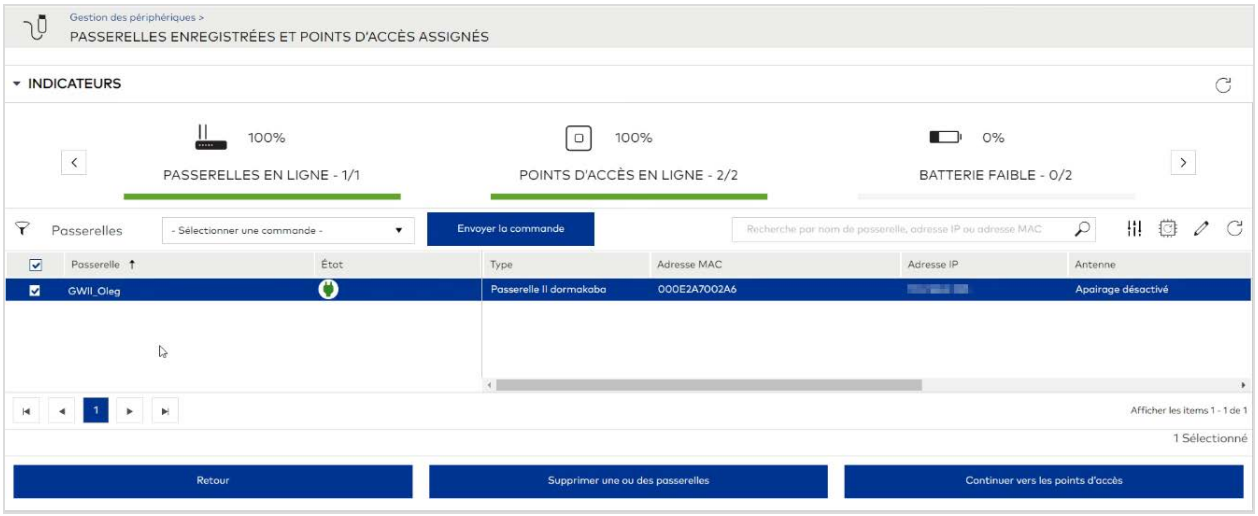
Supprimer un périphérique

1. Sélectionner un périphérique.
2. Cliquez sur **Supprimer un périphérique**.
3. Cliquez sur **OUI** pour confirmer.

Passerelles enregistrées et points d'accès assignés

Pour utiliser des passerelles (et des points d'accès assignés) connectés au serveur Community :

1. Accédez à ***Gestion des périphériques > Passerelles enregistrées et Points d'accès assignés***.



Passerelles enregistrées

Les passerelles et leurs états respectifs sont répertoriés par nom sous la section Indicateurs. Les codes couleur reflètent l'état de chaque passerelle. Le vert indique qu'aucune attention n'est requise. Le jaune indique que la situation peut nécessiter une attention particulière. Le rouge indique que la passerelle est hors ligne ou ne fonctionne pas correctement.

Utilisez la barre d'outils Passerelles pour émettre des commandes, rechercher des passerelles (par nom, adresses IP et MAC) et effectuer les actions suivantes :

- Pour filtrer selon l'état de connectivité, cliquez sur **(Filtre)** et sélectionnez les types d'état (En ligne/Hors ligne) à répertorier.
- Pour afficher/masquer des colonnes, cliquez sur et sélectionnez les informations que vous souhaitez afficher. Les colonnes suivantes peuvent être affichées :
  - **Tous** — Sélectionnez cette option pour afficher toutes les colonnes.
  - **Type** — Le type de passerelle.
  - **Adresse MAC** — Adresse MAC unique pour chaque périphérique.
  - **Adresse IP** — Adresse Ethernet unique pour chaque périphérique. L'adresse IP est dynamique si un DHCP est attribué ; sinon, l'adresse IP est statique.
  - **Antenne** — États des antennes des passerelles (Désactivé/Appairage activé/Appairage désactivé).
  - **Dernier hors ligne** — La date et l'heure de la dernière mise hors ligne de la passerelle.
  - **Dernière communication** — La date et l'heure de la dernière communication réussie avec la passerelle.
  - **Vers. FW Passerelle** — La version actuelle du firmware du périphérique de la passerelle qui fonctionne à tout moment, sauf lors d'une mise à niveau du firmware.
  - **Version FW AVR** — La version du firmware de l'AVR (régulateur de tension automatique) qui fonctionne à tout moment, sauf pendant une mise à niveau du firmware de l'AVR.
  - **Version FW Ember** — Un composant électronique sur la carte RF qui fonctionne à tout moment.
  - **Version FW Boot** — La version du firmware de la passerelle qui fonctionne pendant une mise à niveau du firmware de la passerelle principale.
- Pour rafraîchir les données, cliquez sur **(Rafraîchir)** .

Modifier le nom de la passerelle

1. Sélectionnez une passerelle.
2. Cliquez sur **(Modifier)** .
3. Modifiez le nom.
4. Cliquez sur **Sauvegarder**.

Supprimer une ou plusieurs passerelles

Vous pouvez uniquement supprimer des passerelles qui sont hors ligne.

1. Sélectionnez la ou les passerelles que vous souhaitez supprimer.
2. Cliquez sur **Supprimer une ou des passerelles**.
3. Cliquez sur **OUI** pour confirmer.

Envoyer des commandes aux passerelles

1. Sélectionnez une ou plusieurs passerelles.
2. Sélectionnez l'une des commandes suivantes :
   - **Effacer la mémoire tampon de la passerelle** — Supprime les données de la mémoire tampon de tous les périphériques connectés à la passerelle. La mémoire tampon est automatiquement effacée avant la mise à niveau du firmware. (Non pris en charge pour les périphériques C4.)
   - **Désactiver l'antenne** — Désactive la ou les passerelles sélectionnées du réseau et désactive l'antenne de la passerelle. Lorsque le résultat de la commande est positif, l'état de l'antenne est Désactivé (dans le module **Surveillance**). (Non pris en charge pour les périphériques C4.)
   - **Obtenir l'état des points d'accès** — Demande l'état de connectivité (En ligne/Hors ligne) pour tous les points d'accès assignés.
   - **Obtenir l'état du firmware de la passerelle** — Demande la version du firmware de la passerelle installée sur la passerelle. (Non pris en charge pour les périphériques C4.)
   - **Obtenir l'état de la passerelle** — Demande l'état de connectivité de la passerelle (En ligne/Hors ligne).
   - **Appairage DÉSACTIVÉ** — Désactive le mode Appairage. Lorsque le résultat de la commande est positif, l'état de l'antenne est Appairage désactivé (dans le module **Surveillance**). (Non pris en charge pour les périphériques C4.)
   - **Appairage ACTIVÉ** — Active le mode Appairage. Lorsque le résultat de la commande est positif, l'état de l'antenne est Appairage activé (dans le module **Surveillance**). (Non pris en charge pour les périphériques C4.)

     Important ! Pour éliminer le risque d'assigner des points d'accès à la mauvaise passerelle, dormakaba recommande vivement de placer une seule passerelle à la fois en mode Appairage. Une fois que tous les points d'accès sont assignés à une passerelle, envoyez la commande Appairage DÉSACTIVÉ à la passerelle pour désactiver le mode Appairage. Par mesure de précaution, le mode Appairage ACTIVÉ passe en mode Appairage DÉSACTIVÉ au bout de 15 minutes.

   - **Réinitialiser la passerelle** — Exécute une réinitialisation logicielle sur la ou les passerelles sélectionnées. (Non pris en charge pour les périphériques C4.)
   - **Réglage de l'horloge et du masque d'évènements** — Envoie l'heure du serveur et les paramètres de notification d'évènements de point d'accès (définis dans ***Paramètres du système > Communication en ligne > Notifications***).
   - **Définir les paramètres de communication** — Envoie les paramètres de configuration de communication (définis dans **Paramètres du système > Communication en ligne > Paramètres de communication en ligne > État de mise à jour de la passerelle**, **Réveil du point d'accès**, **État de mise à jour de la passerelle**).
   - **Désappairer tous les points d'accès** — Désapparie tous les points d'accès. (Non pris en charge pour les périphériques C4.)
   - **Mettre à niveau le firmware** — Mettre à jour le logiciel de niveau système installé dans la passerelle. Avant la mise à niveau, vous devez obtenir le fichier requis auprès du support dormakaba. Cette commande s'applique uniquement

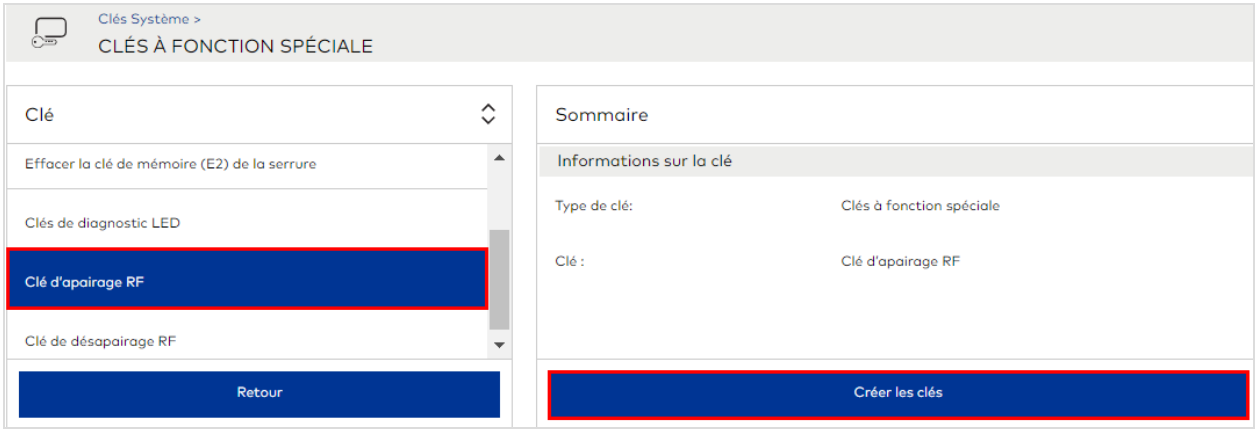
aux périphériques Passerelle II. (Non pris en charge pour les périphériques C4.)
- **Vérifier l'attribution** — Demande l'état de connectivité des points d'accès assignés.

3. Cliquez sur **Envoyer la commande**.
4. Lorsqu'un message vous informe que la commande est envoyée, cliquez sur **OK**.

Appairer les points d'accès

Pour appairer les points d'accès, vous devez créer une Clé d'appairage RF dans les **Clés Système**.

Créer une clé d'appairage RF



1. Accédez à **Clés Système**.
2. Cliquez sur **Clés à fonction spéciale**.
3. Sélectionnez **Clé d'appairage RF**.
4. Cliquez sur **Créer les clés**.
5. Sélectionnez un encodeur en ligne, présentez une clé à l'encodeur, puis cliquez sur **Démarrer**.
6. Lorsqu'un message vous indique que la création de la clé est réussie, cliquez sur **Terminé**.

Appairer les points d'accès

Pour les périphériques Control 4, passez directement à l'étape 6.

1. Accédez à ***Gestion des périphériques > Passerelles enregistrées et Point d'accès assigné***.
2. Sélectionnez la passerelle dans laquelle vous souhaitez appairer des points d'accès.
3. Sélectionnez la commande **Appairage ACTIVÉ** (pour activer l'antenne de la passerelle et placer la passerelle en mode Appairage).
4. Cliquez sur **Envoyer la commande**.
5. Lorsqu'un message vous informe que la commande est envoyée, cliquez sur **OK**.
6. Présentez la Clé d'appairage RF à chaque point d'accès que vous souhaitez assigner à la passerelle.

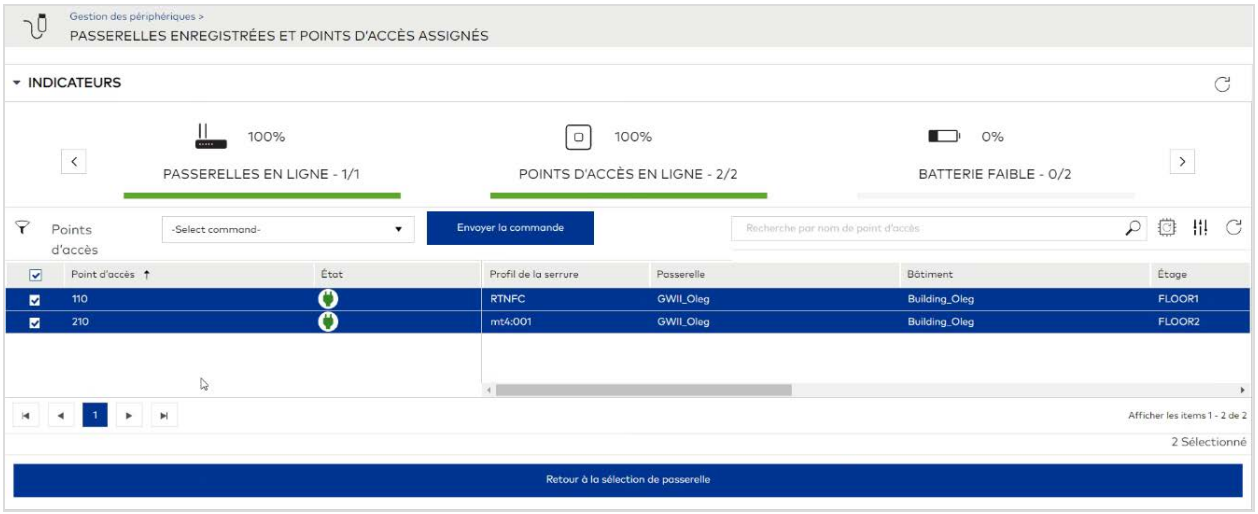
Pour éliminer le risque d'assigner des points d'accès à la mauvaise passerelle, dormakaba recommande vivement de placer une seule passerelle à la fois en mode Appairage. Une fois que tous les points d'accès sont assignés à une passerelle, envoyez la commande **Appairage DÉSACTIVÉ** à la passerelle pour désactiver le mode Appairage. Par mesure de précaution, **Appairage ACTIVÉ** passe automatiquement en **Appairage DÉSACTIVÉ** au bout de 15 minutes.

7. Dans Community, sélectionnez la passerelle en mode **Appairage activé**.
8. Sélectionnez la commande **Appairage DÉSACTIVÉ** (pour désactiver l'antenne et désactiver le mode Appairage).
9. Cliquez sur **Envoyer la commande**.
10. Lorsqu'un message vous informe que la commande est envoyée, cliquez sur **OK**.

Points d'accès assignés

Pour afficher les points d'accès assignés à une passerelle :

1. Accédez à ***Gestion des périphériques > Passerelles enregistrées et Points d'accès assignés***.
2. Sélectionnez la passerelle dans laquelle le ou les points d'accès sont assignés.
3. Cliquez sur **Continuer vers les points d'accès**.



Les points d'accès assignés à la passerelle sélectionnée et leur état respectif sont listés par nom.

> Pour les périphériques RAC5 XT, vous devez déclencher un événement avant que le point d'accès ne s'affiche dans la liste. La façon la plus simple de déclencher un événement est de présenter une clé quelconque (valide ou non) à la serrure.

Utilisez la barre d'outils des points d'accès pour émettre des commandes, rechercher des points d'accès (par nom) et effectuer les actions suivantes :

- Émettez l'une des commandes suivantes :
  - **Obtenir l'état du firmware du point d'accès** — Demande la version actuelle du firmware de la serrure. (Non pris en charge pour les périphériques Control 4.)
  - **Obtenir l'état des points d'accès** — La passerelle demande une mise à jour complète de l'état des points d'accès.
  - **Définition du décalage UTC et du masque d'évènements** — Envoie l'heure du serveur et les paramètres de notification d'évènements de point d'accès (définis dans ***Paramètres du système > Communication en ligne > Notifications***).
  - **Désappairer le point d'accès** — Délier le point d'accès de la passerelle. Cette commande est utile pendant la maintenance de la passerelle, lorsque vous devez assigner un point d'accès à une autre passerelle. (Non pris en charge pour les périphériques Control 4.)

    > Pour associer un point d'accès existant à une nouvelle chambre, vous devez désappairer et supprimer (ou simplement supprimer) le point d'accès existant sur la page Points d'accès en ligne. Ensuite, le « nouveau » point d'accès doit être reprogrammé et assigné à la passerelle.

  - **Mettre à niveau le firmware** — Demander la mise à niveau du firmware. (Non pris en charge pour les périphériques Control 4.)
  - **Vérifier l'attribution** — Demande la passerelle à laquelle les points d'accès sont assignés et l'état de connectivité.
- Pour filtrer selon de l'état de la connectivité, cliquez sur **(Filtrer)** et sélectionnez l'état de la connectivité (En ligne/Hors ligne) ainsi que les états surveillés (Batterie faible/Porte ouverte/Porte entrebaillée/Intimité activée/Déverrouillée) à répertorier.

- Pour afficher/masquer des colonnes, cliquez sur et sélectionnez les informations que vous souhaitez afficher. Les colonnes suivantes peuvent être affichées :
  - **Tous** — Sélectionnez cette option pour afficher toutes les colonnes.
  - **Profil de la serrure** — Le modèle de serrure installé sur le point d'accès.
  - **Passerelle** — La passerelle à laquelle le point d'accès est assigné.
  - **Bâtiment** — Le bâtiment dans lequel le point d'accès est situé.
  - **Étage** — Le niveau du bâtiment dans lequel le point d'accès est situé.
  - **Batterie faible** — Indique si la batterie de la serrure est faible (VRAI=OUI/FAUX=NON). Vous pouvez filtrer la liste pour afficher les points d'accès avec une batterie faible.
  - **Signal RF** — Indique si le signal entre la passerelle et le point d'accès assigné est faible ou normal.
  - **Dernier hors ligne** — La date et l'heure de la dernière mise hors ligne de la passerelle.
  - **Dernière communication** — La date et l'heure de la dernière communication réussie avec la passerelle.
  - **Porte ouverte** — Indique si la porte est ouverte. Vous pouvez filtrer la liste pour afficher les points d'accès avec une porte ouverte.
  - **Porte entrebaillée** — Indique si la porte a été ouverte au-delà d'un seuil prédéfini. Vous pouvez filtrer la liste pour afficher les points d'accès avec une porte entrebaillée.
  - **Porte entrebaillée par** — Indique le type de clé présenté pour ouvrir la porte désormais entrebaillée.
  - **Porte entrebaillée depuis** — Indique la date et l'heure auxquelles la porte a été considérée comme entrebaillée (non ouverte).
  - **Verrou d'intimité activée** — Indique si le pêne dormant ou le verrou d'intimité est activé sur le point d'accès. Vous pouvez filtrer la liste pour afficher les points d'accès avec le verrou d'intimité activée.
  - **Déverrouillé** — Indique si le point d'accès se trouve actuellement en mode Déverrouillé (il permet alors un accès illimité sans clé). Vous pouvez filtrer la liste pour afficher les points d'accès déverrouillés.
  - **Dernière entrée** — La date et l'heure d'entrée la plus récente sur le point d'accès.
  - **Erreur de date/heure** — Indiquez si la date et l'heure doivent être synchronisées.
  - **Vers. FW Serrure (principale) —** La version actuelle du firmware de la serrure qui fonctionne à tout moment, sauf lors d'une mise à niveau du firmware.
  - **Vers. FW Serrure (boot) —** La version actuelle du firmware de la serrure qui fonctionne lors d'une mise à niveau du firmware.
  - **Vers. FW AVR (principal) —** La version du firmware de l'AVR (régulateur de tension automatique) qui fonctionne à tout moment, sauf pendant une mise à niveau du firmware de l'AVR.
  - **Vers. FW AVR (boot) —** La version du firmware de l'AVR (régulateur de tension automatique) qui fonctionne pendant une mise à niveau du firmware de l'AVR.
  - **Vers. FW Ember —** Un composant électronique sur la carte RF qui fonctionne à tout moment.
  - **Vers. FW Quantum** — Version du firmware de la carte RF ZigBee.
- Pour rafraîchir les données, cliquez sur **(Rafraîchir)** .

Notifications

Gestion des notifications

Cette section comprend les sujets suivants :

En savoir plus sur la gestion des notifications 313

Ajouter des groupes de notification 315

En savoir plus sur la gestion des notifications

Les notifications, facilement accessibles depuis la barre d'outils principale Community, tiennent les membres du personnel informés des opérations et des événements en ligne ainsi que de l'état des points d'accès en ligne. Par exemple, une notification peut signaler qu'une clé résident est utilisée ou qu'une porte est entrebaillée. Le module **Gestion des notifications** permet de regrouper différents types de notifications et de les sélectionner ensuite pour les inscrire dans les profils du personnel/prestataire dans la **Gestion du personnel/prestataire**.

Les notifications en ligne suivantes sont disponibles :

- **Point d'accès hors ligne** — Signale qu'il n'y a pas de communication entre la serrure et la passerelle.
- **Point d'accès en ligne** — Signale que la serrure est en communication avec la passerelle et en ligne.
- **Porte entrebaillée terminé (porte sécurisée)** — La porte précédemment entrebaillée a été fermée et est sécurisée.
- **Porte entrebaillée générique** — Signale qu'une porte est en état ouvert.
- **Porte entrebaillée résident - long** — Porte entrebaillée au-delà du seuil configuré. L'événement Porte entrebaillée (long) signale qu'une porte a été laissée ouverte pendant un intervalle prolongé (deux minutes), ce qui indique un état inhabituel ou une intrusion potentielle.
- **Porte entrebaillée résident - court** — Signale un événement de porte entrebaillée (court), ce qui signifie qu'une porte a été laissée ouverte pendant un bref intervalle (une minute), par exemple le temps nécessaire pour libérer une chambre.
- **Porte entrebaillée du personnel/prestataire - long** — Porte entrebaillée au-delà du seuil configuré. L'événement Porte entrebaillée (long) signale qu'une porte a été laissée ouverte pendant un intervalle prolongé (deux minutes), ce qui indique un état inhabituel ou une intrusion potentielle.
- **Porte entrebaillée du personnel/prestataire - court** — Signale un événement de porte entrebaillée (court), ce qui signifie qu'une porte a été laissée ouverte pendant un bref intervalle (une minute), par exemple le temps nécessaire pour libérer une chambre.
- **Porte verrouillée** — Signale qu'une porte est fermée avec la serrure engagée.
- **Porte ouverte** — Signale que le mécanisme anti-crochetage de la serrure est désactivé. Il s'agit de l'état par défaut de la porte.
- **Porte déverrouillée** — Signale que le moteur de la serrure a été désengagé et que la porte peut être ouverte sans clé.
- **Alarme incendie activée** — Notification RAC5 MFC/XT uniquement. Un événement qui signale l'activation de l'alarme incendie du point d'accès.
- **Alarme incendie désactivée** — Notification RAC5 MFC/XT uniquement. Un événement qui signale la désactivation de l'alarme incendie du point d'accès.
- **Mise à jour du code d'erreur de la passerelle** — Signale qu'un code d'erreur a été émis pour une passerelle. La mise à jour peut indiquer que la passerelle est en bon état (code d'erreur=0) ou qu'une erreur s'est produite.
- **Passerelle hors ligne** — Signale qu'une passerelle ne communique pas actuellement avec le serveur Community.
- **Passerelle en ligne** — Signale qu'une passerelle communique avec le serveur Community.
- **Ouverture sans clé (sortie) générique** — Signale qu'un événement d'ouverture de porte s'est produit.
- **Clé résident utilisée** — Signale qu'une clé résident a été présentée à une serrure. Les détails incluent la date/heure auxquelles la clé a été présentée.
- **Clé résident utilisée (première entrée)** — Signale qu'une clé résident a été présentée à une serrure pour la première fois.
- **Batterie faible** — Signale que la batterie est faible et doit être remplacée. Community envoie un(e) seul(e) événement/notification de batterie faible jusqu'à ce que les piles soient remplacées. Une fois les piles remplacées, Community envoie un événement/une notification de **Batterie faible terminé (batterie normale)**.
- **Batterie faible terminé (batterie normale)** — Signale que l'état de batterie faible est terminé. La batterie a été remplacée ou le problème a été résolu.
- **Ouverture d'urgence avec clé mécanique** — Signale une ouverture forcée de la serrure, un accès à la serrure avec une clé mécanique.
- **Échec de l'opération** — Signale que l'opération spécifiée a échoué. Si disponible, la cause est indiquée.
- **Verrou d'intimité désactivée/pêne dormant rétracté** — Signale que l'état du pêne dormant est désengagé.
- **Verrou d'intimité activée/pêne dormant sorti** — Signale que le pêne dormant ou le verrou d'intimité est engagé.

- **Verrouillage à distance** — Commande envoyée depuis la barre d'outils pour verrouiller à distance le point d'accès sélectionné.
- **Déverrouillage à distance** — Commande envoyée depuis la barre d'outils pour déverrouiller à distance le point d'accès sélectionné.
- **Clé du personnel/prestataire utilisée** — Signale qu'une clé du personnel/prestataire a accédé à une serrure.
- **Intrus statique** — Alerte : Possible intrus statique. Plusieurs clés présentées sur un même point d'accès.
- **Clé système utilisée** — Signale qu'une clé système a été présentée à une serrure.
- **Intrus errant** — Alerte : Possible intrus errant. Clé présentée sur plusieurs points d'accès.

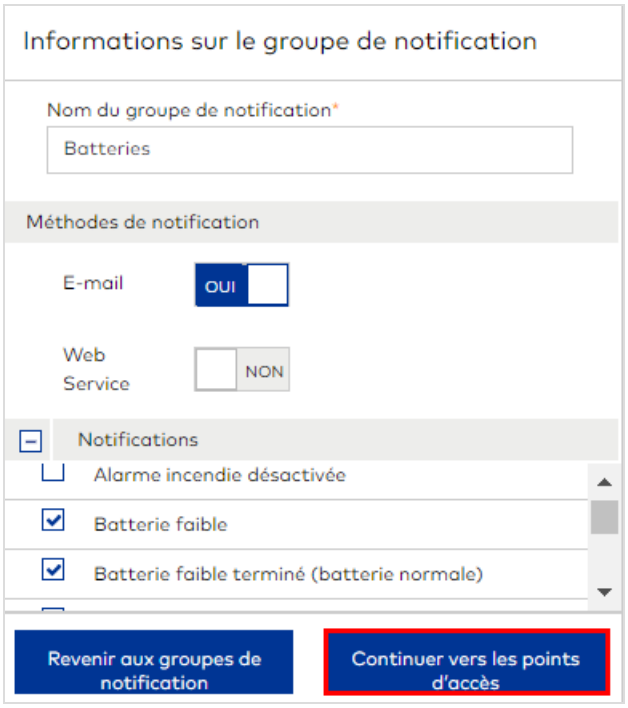


Les notifications par e-mail et par Web Service sont supprimées de la base de données Community une fois qu'elles ont été envoyées avec succès.

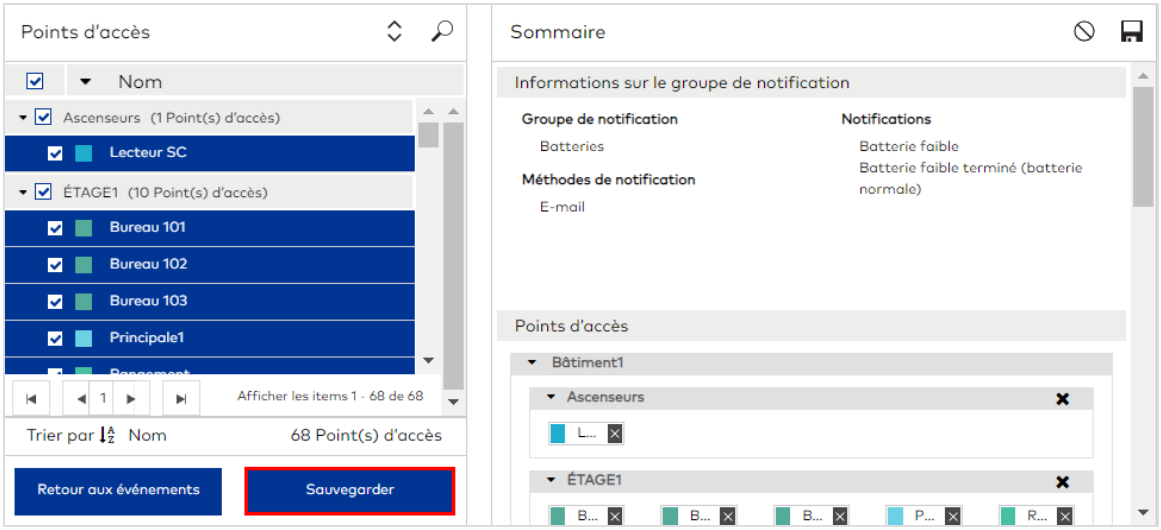
Ajouter des groupes de notification

Pour ajouter des groupes de notification :

1. Accédez à **Gestion des notifications**.

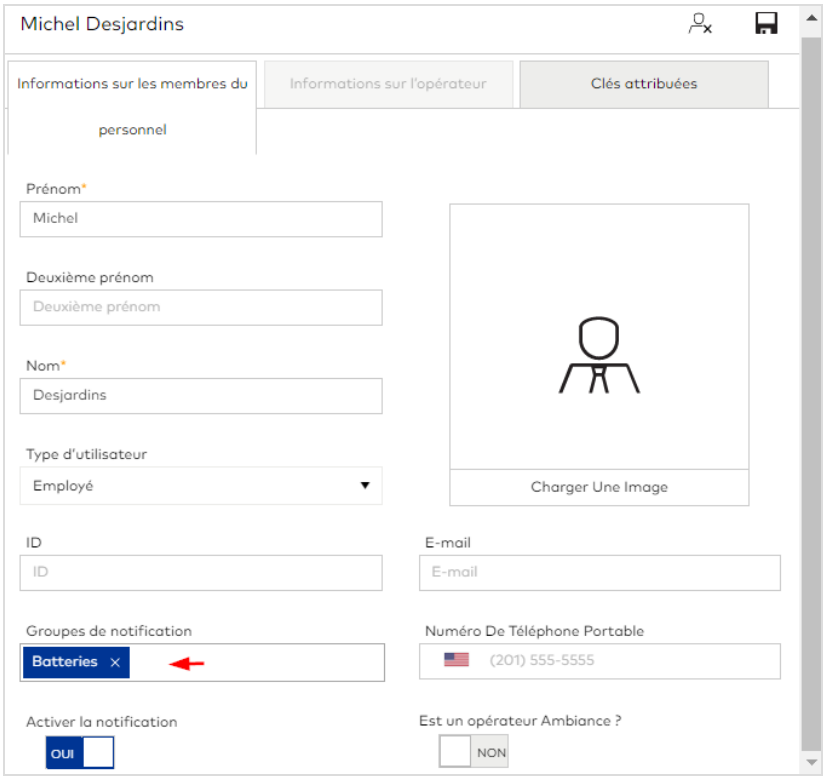


2. Cliquez sur **Nouveau groupe de notification**.
3. Indiquez un nom descriptif pour le groupe.
4. Sélectionnez l'une des méthodes de notification. Si vous ne sélectionnez aucune méthode, seuls les opérateurs possédant les droits pour afficher des notifications verront des notifications lors de leur connexion à Community.
   - **E-mail** — Envoyer des notifications par e-mail. Valeur recommandée : OUI. Nécessite la configuration de l'e-mail dans ***Paramètres du système > E-mail*** et une adresse e-mail définie dans les profils du personnel/prestataire dans **Gestion du personnel/prestataire**.
   - **Web Service** — Envoyer des notifications via le Web Service à l'aide des protocoles SOAP ou REST. Vous devez également spécifier l'URL du Web Service.
5. Sélectionnez les événements que vous souhaitez inclure dans le groupe de notification. Vous pouvez les sélectionner dans les listes **Général** et **En ligne**. Pour inclure toutes les notifications, cochez la case à côté de **Notifications**.
6. Cliquez sur **Continuer vers les points d'accès**.



7. Sélectionnez les points d'accès pour lesquels vous souhaitez recevoir des notifications.
8. Cliquez sur **Sauvegarder**.

Les souscriptions à un ou plusieurs groupes de notification peuvent être sélectionnées dans les profils du personnel/prestataire dans **Gestion du personnel/prestataire**.



Surveillance (à distance)

Cette section comprend les sujets suivants :

- En savoir plus sur la surveillance 318
- Afficher les indicateurs 319
- Surveiller des opérations en ligne 320
- Surveiller les événements en ligne 322
- Surveiller l'état des points d'accès 325

En savoir plus sur la surveillance

Le module **Surveillance** fournit des informations sur toutes les clés créées dans Community. Si vous souhaitez savoir à quelle heure et par qui une clé spécifique a été utilisée pour la dernière fois, ces données sont directement disponibles sans générer un rapport.

Le module Surveillance vous permet également de rester informé de la communication en ligne. La section Indicateurs fournit un aperçu en temps réel des passerelles et des points d'accès d'un site. Par exemple, vous pouvez voir en un coup d'œil si la batterie est faible sur certaines serrures, si des portes sont ouvertes et sur combien de points d'accès le pêne dormant ou le verrou d'intimité sont activés. Sous le sommaire des indicateurs, des listes détaillées indiquent les opérations et événements de serrures à distance et l'état de tous les points d'accès assignés à des passerelles.

L'accès aux données du module **Surveillance** est configuré dans **Gestion des rôles**. Par défaut, les rôles Administrateur et Configurateur de site ont un accès complet.



Lorsque la fonction sous licence Clés mobiles est activée, l'onglet Utilisation des clés numériques s'affiche pour contrôler et suivre le nombre de clés numériques (clés mobiles et clés de portefeuille) disponibles/utilisées.

Afficher les indicateurs

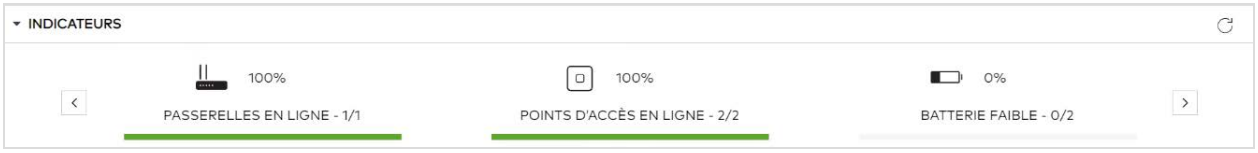
Pour afficher les indicateurs :

Dans **Surveillance** :

» Les indicateurs s'affichent par défaut.

Dans **Gestion des périphériques** :

» Accédez à ***Gestion des périphériques > Passerelles enregistrées et Points d'accès assignés***.



La section **Indicateurs** est développée pour être affichée par défaut. Les codes couleur reflètent l'état des données. Le vert indique qu'aucune attention n'est requise. Le jaune indique que la situation peut nécessiter une attention particulière.

- **PASSERELLES EN LIGNE** — Pourcentage et nombre total de passerelles actuellement en ligne.
- **POINTS D'ACCÈS EN LIGNE** — Pourcentage et nombre total de points d'accès actuellement en ligne.
- **BATTERIE FAIBLE** — Pourcentage et nombre de points d'accès dont la batterie est faible. Zéro pour cent indique qu'aucun point d'accès ne signale une batterie faible.
- **SIGNAL RF FAIBLE** — Indique si le signal entre la passerelle et le point d'accès assigné est faible ou normal.
- **PORTES ENTREBAILLÉES** — Pourcentage et nombre de points d'accès dont la porte est ouverte.
- **VERROU D'INTIMITÉ ACTIVÉE** — Pourcentage et nombre de points d'accès avec pêne dormant ou verrou d'intimité activés.
- **PORTES DÉVERROUILLÉES** — Pourcentage et nombre de points d'accès dont les portes sont fermées mais pour lesquels il existe un accès illimité sans clé. Zéro pour cent indique qu'aucune porte n'est déverrouillée, ce qui signifie qu'une clé est nécessaire pour entrer.

À tout moment, vous pouvez développer ou réduire cette section.

Les codes couleur reflètent l'état des données. Le vert indique qu'aucune attention n'est requise. Le jaune indique que la situation peut nécessiter une attention particulière.

Surveiller des opérations en ligne

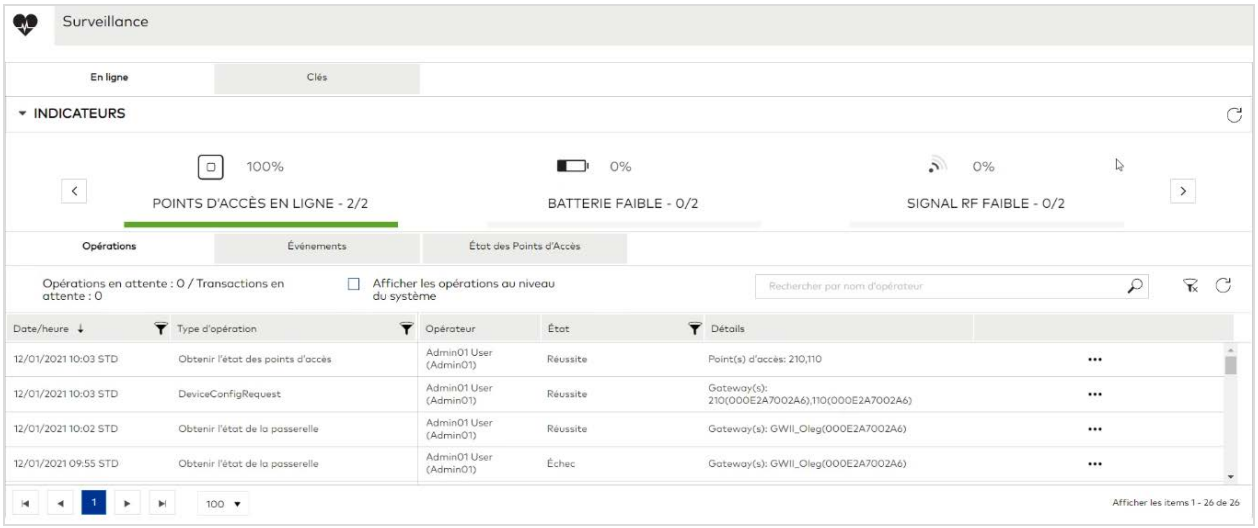
L'onglet Opérations sous la section Indicateurs répertorie les commandes et les détails associés envoyés aux passerelles et aux points d'accès assignés. Les commandes sont envoyées depuis ***Gestion des périphériques > Passerelles enregistrées et Points d'accès assignés***. Les détails de la transaction s'affichent sous forme de rapport pour chaque opération.

Afficher des opérations

Pour surveiller les opérations en ligne :

» Accédez à **Surveillance**. Les opérations s'affichent sous la section **Indicateurs**.

Réduire la section **Indicateurs** pour n'afficher que la liste des opérations.



Les informations suivantes s'affichent sous forme de rapport pour chaque opération :

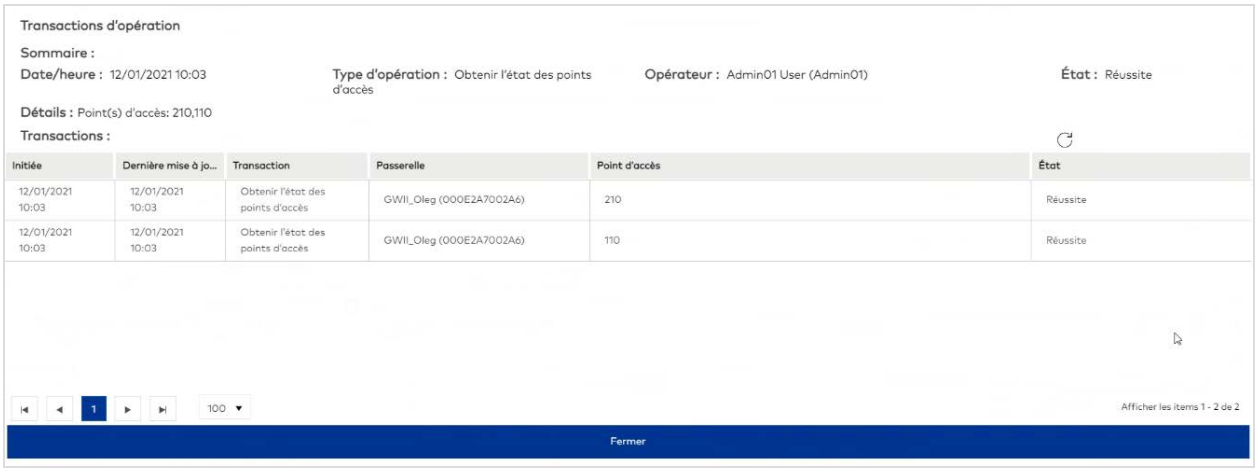
- **Date/heure** — La date et l'heure d'exécution de l'opération. Vous pouvez filtrer la liste selon la date et l'heure.
- **Type d'opération** — Commande envoyée aux passerelles et points d'accès (par exemple, Appairage désactivé/activé/Réglage du masque d'évènements de l'horloge et de verrouillage). Vous pouvez filtrer la liste selon le type d'opération.
- **Opérateur** — Le nom complet de l'opérateur connecté lors de l'exécution de l'opération. Vous pouvez rechercher des commandes envoyées lorsqu'un opérateur spécifique était connecté.
- **État** — Résultat de la commande (par exemple, Échec/Réussite/En attente/Réussite partielle). Si l'état est Échec, une cause est indiquée. Vous pouvez filtrer la liste selon l'état.
- **Détails** — Plus d'informations sur l'opération.

Personnaliser l'affichage

- Pour filtrer les données, cliquez sur **(Filtrer)** dans l'en-tête de la colonne, sélectionnez les informations que vous souhaitez afficher, puis cliquez sur **Filtrer**. L'icône **(Filtre appliqué)** indique qu'un filtre est appliqué à la colonne.
- Pour effacer les filtres pour une colonne, cliquez sur ***(Filtre appliqué)*** ***> Effacer***.
- Pour effacer tous les filtres, cliquez sur **(Effacer les filtres)**.
- Cliquez sur n'importe quelle colonne pour trier la liste.
- Pour rafraîchir les données, cliquez sur **(Rafraîchir)**.

Voir les détails de la transaction

» Sélectionnez une opération et cliquez sur **(Plus)** ▪▪▪.



Outre les informations de la liste des Opérations, les détails suivants sont affichés pour les transactions :

- **Initiée** — La date et l'heure d'envoi de la commande.
- **Dernière mise à jour** — La date et l'heure de mise à jour de l'état (soit réponse soit délai d'expiration).
- **Transaction** — Le type de transaction (par exemple Mise à jour de la clé/Ajouter une clé/Bloquer une clé/Appairage activé/Appairage désactivé).
- **Passerelle** — Le nom et l'adresse MAC de la passerelle.
- **Point d'accès** — Si la transaction implique un point d'accès, le nom du point d'accès ; sinon, le champ est vide.
- **État** — Résultat de la commande (par exemple, Échec/Réussite/En attente/Réussite partielle). Si l'état est Échec, une cause est indiquée.

Personnaliser l'affichage

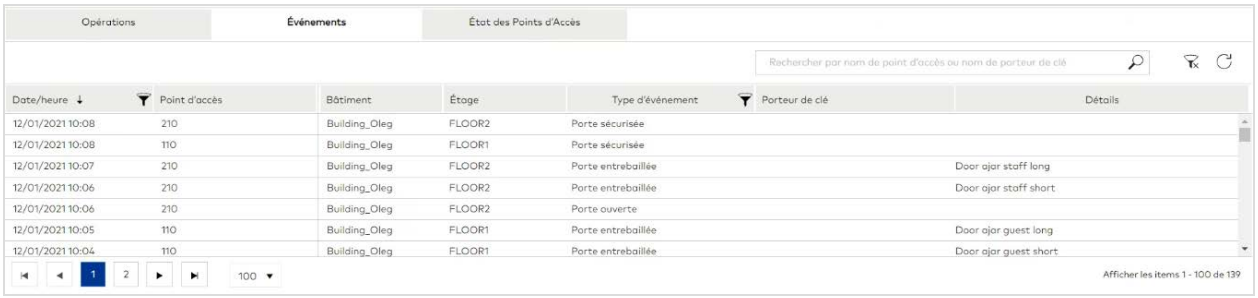
- Cliquez sur n'importe quelle colonne pour trier la liste. Une fois terminé, cliquez sur **Fermer**.

Surveiller les événements en ligne

Les événements liés aux passerelles et aux points d'accès assignés sont affichés dans une liste. Cette liste inclut les événements pour tous les types de clés (clés résident/personnel/prestataire/Système) et les changements d'état des passerelles/points d'accès.

Pour surveiller les événements :

1. Accédez à **Surveillance**.
2. Sous la section **Indicateurs** , cliquez sur l'onglet **Événements**.



Les informations suivantes s'affichent sous forme de rapport pour chaque événement :

- **Date/heure du serveur** — Date et heure auxquelles les événements du point d'accès sont reçus par le serveur. Vous pouvez trier et filtrer la liste en fonction de la date et de l'heure.
- **Date/Heure du point d'accès** — Date et heure auxquelles l'événement s'est produit dans le point d'accès. Vous pouvez filtrer la liste selon la date et l'heure.
- **Point d'accès** — Le nom du point d'accès. Vous pouvez rechercher des événements survenus pour un point d'accès spécifique.
- **Bâtiment** — Le bâtiment dans lequel le point d'accès est situé. Cette colonne s'affiche uniquement si plusieurs bâtiments sont définis.
- **Étage** — L'étage du bâtiment dans lequel le point d'accès est situé.
- **Type d'événement** — Le type d'événement ou type de clé utilisé (par exemple, Porte entrebaillée ou Clé système utilisée). Vous pouvez filtrer la liste selon le type d'événement.
- Porteur de clé — Le nom du porteur de clé. Valeurs par défaut : Résident1 (pour les résidents) et Non attribué (pour les clés du personnel/prestataire ou Système). Vous pouvez rechercher des événements selon le nom du porteur de clé.
- **Possible(s) porteur(s) de clé** — Le nom d'un possible porteur de clé. Valeurs par défaut : Résident1 (pour les résidents) et Non attribué (pour les clés du personnel ou les clés système). Vous pouvez rechercher des événements selon le nom du porteur de clé. Si un ID de la clé est réutilisé, le porteur de clé peut être un parmi plusieurs.
- **Détails** — Plus d'informations sur l'événement (par exemple, Porte entrebâillée/Entrebâillée - court – Résident). Pour tous les types de clés, les détails comprennent le type de clé, la catégorie d'identifiants et l'identifiant. Pour les clés, les détails indiquent si l'accès a été autorisé ou refusé.

Personnaliser l'affichage

- Pour filtrer les données, cliquez sur **(Filtre)** dans l'en-tête de la colonne, sélectionnez les informations que vous souhaitez afficher, puis cliquez sur Filtrer. L'icône **(Filtre appliqué)** indique qu'un filtre est appliqué à la colonne.
- Pour effacer les filtres pour une colonne, cliquez sur **(Filtre appliqué)** puis sur **Effacer**.
- Pour effacer tous les filtres, cliquez sur **(Effacer les filtres)**.
- Cliquez sur n'importe quelle colonne pour trier la liste.
- Pour rafraîchir les données, cliquez sur **(Rafraîchir)**.

Événements

Les événements suivants sont signalés :

- **Point d'accès hors ligne** — Se produit lorsqu'il n'y a pas de communication entre la serrure et la passerelle.
- **Point d'accès en ligne** — Se produit lorsque la serrure est en communication avec la passerelle et en ligne.
- **Porte entrebaillée terminé (porte sécurisée)** — Se produit lorsqu'une porte précédemment entrebaillée est fermée et sécurisée.
- **Porte entrebaillée générique** — Se produit lorsqu'une porte est en état ouvert.
- **Porte entrebaillée résident - long** — Se produit lorsqu'une porte entrebaillée s'étend au-delà du seuil configuré. L'événement Porte entrebaillée (long) se produit lorsqu'une porte a été laissée ouverte pendant un intervalle prolongé (deux minutes), ce qui indique un état inhabituel ou une intrusion potentielle.
- **Porte entrebaillée résident - court** — Se produit lorsqu'une porte a été laissée ouverte pendant un bref intervalle (une minute), par exemple le temps nécessaire pour libérer une chambre.
- **Porte entrebaillée du personnel/prestataire - long** — Se produit lorsqu'une porte entrebaillée s'étend au-delà du seuil configuré. L'événement Porte entrebaillée (long) se produit lorsqu'une porte a été laissée ouverte pendant un intervalle prolongé (deux minutes), ce qui indique un état inhabituel ou une intrusion potentielle.
- **Porte entrebaillée du personnel/prestataire - court** — Se produit lorsqu'une porte a été laissée ouverte pendant un bref intervalle (une minute), par exemple le temps nécessaire pour libérer une chambre.
- **Porte verrouillée** — Se produit lorsqu'une porte est fermée avec la serrure engagée.
- **Porte ouverte** — Se produit lorsque le mécanisme anti-crochetage de la serrure est désactivé. Il s'agit de l'état par défaut de la porte.
- **Porte déverrouillée** — Se produit lorsque le moteur de la serrure a été désengagé et que la porte peut être ouverte sans clé.
- **Alarme incendie activée** — Événement RAC5 MFC/XT uniquement. Se produit lors de l'activation de l'alarme incendie du point d'accès.
- **Alarme incendie désactivée** — Événement RAC5 MFC/XT uniquement. Se produit lors de la désactivation de l'alarme incendie du point d'accès.
- **Mise à jour du code d'erreur de la passerelle** — Se produit lorsqu'un code d'erreur est émis pour une passerelle. La mise à jour peut indiquer que la passerelle est en bon état (code d'erreur=0) ou qu'une erreur s'est produite.
- **Passerelle hors ligne** — Se produit lorsqu'une passerelle passe à l'état Hors ligne. La passerelle ne communique pas avec le serveur Community.
- **Passerelle en ligne** — Se produit lorsqu'une passerelle passe à l'état En ligne. La passerelle communique avec le serveur Community.
- **Ouverture sans clé (sortie) générique** — Se produit lorsqu'une porte s'ouvre.
- **Clé résident utilisée** — Se produit lorsqu'une clé résident est présentée à un point d'accès. Les détails incluent la date/heure auxquelles la clé résident a été présentée à la serrure.
- **Clé résident utilisée (première entrée)** — Se produit lorsqu'un résident a accédé à la serrure pour la première fois.
- **Batterie faible** — Se produit lorsque la batterie passe à l'état de batterie faible. La batterie doit être remplacée. Community envoie un(e) seul(e) événement/notification de batterie faible jusqu'à ce que les piles soient remplacées. Une fois les piles remplacées, Community envoie un événement/une notification de **Batterie faible terminé (batterie normale)**.
- **Batterie faible terminé (batterie normale)** — Se produit lorsque l'état de batterie faible est terminé. La batterie a été remplacée ou le problème a été résolu.
- **Ouverture d'urgence avec clé mécanique** — Se produit lors de l'accès à la serrure avec une clé mécanique (une ouverture forcée de la serrure).
- **Échec de l'opération** — Se produit lorsqu'une opération échoue. Si disponible, la cause est indiquée.
- **Verrou d'intimité désactivée/pêne dormant rétracté** — Se produit lorsque le verrou d'intimité ou le pêne dormant passe à l'état désengagé.
- **Verrou d'intimité activée/pêne dormant sorti** — Se produit lorsque le verrou d'intimité ou le pêne dormant passe à l'état sorti.
- **Verrouillage à distance** — Commande envoyée depuis la barre d'outils pour verrouiller à distance le point d'accès sélectionné.
- **Déverrouillage à distance** — Commande envoyée depuis la barre d'outils pour déverrouiller à distance le point d'accès sélectionné.

- **Clé du personnel/prestataire utilisée** — Se produit lorsqu'une clé du personnel/prestataire accède à une serrure.
- **Intrus statique** — Alerte : Possible intrus statique. Plusieurs clés présentées sur un même point d'accès.
- **Clé système utilisée** — Se produit lorsqu'une clé système est présentée à une serrure.
- **Accès VIP** — Se produit lorsqu'une clé VIP est présentée à une serrure. Les détails peuvent inclure : Accès VIP autorisé, accès VIP refusé, accès refusé (clé VIP inconnue), ou jeton VIP non inséré dans la serrure.
- **Premier accès VIP** — Se produit lorsqu'une clé VIP est présentée à une serrure pour la première fois.
- **Intrus errant** — Alerte : Possible intrus errant. Clé présentée sur plusieurs points d'accès.

Surveiller l'état des points d'accès

L'onglet **État des points d'accès** sous la section **Indicateurs** répertorie l'état des points d'accès assignés.

Pour afficher l'état des points d'accès assignés :

1. Accédez à **Surveillance**.
2. Sous la section **Indicateurs**, cliquez sur l'onglet **État des points d'accès**.



Les informations suivantes s'affichent sous forme de rapport pour chaque point d'accès :

- **Point d'accès** — Nom du point d'accès. Vous pouvez rechercher un point d'accès spécifique dans la liste.
- **État** — L'icône d'état indique l'état de connectivité du point d'accès (vert = en ligne/rouge = hors ligne). Vous pouvez filtrer la liste selon l'état de connectivité.
- **Bâtiment** — Le bâtiment dans lequel le point d'accès est situé.
- **Étage** — L'étage du bâtiment dans lequel le point d'accès est situé.
- **Batterie faible** — Indique si la batterie de la serrure est faible (VRAI=OUI/FAUX=NON). Vous pouvez filtrer la liste pour afficher les points d'accès avec une batterie faible. Community envoie un(e) seul(e) événement/notification de batterie faible jusqu'à ce que les piles soient remplacées. Une fois les piles remplacées, Community envoie un événement/une notification de **Batterie faible terminé (batterie normale)**.
- **Signal RF** — Indique si le signal entre la passerelle et le point d'accès assigné est faible ou normal.
- **Porte ouverte** — Indique si la porte est ouverte. Vous pouvez filtrer la liste pour afficher les points d'accès avec une porte ouverte.
- **Porte entrebaillée** — Indique si la porte a été ouverte au-delà d'un seuil prédéfini. Vous pouvez filtrer la liste pour afficher les points d'accès avec une porte entrebaillée.
- **Porte entrebaillée par** — S'affiche lorsque l'événement Porte entrebaillée se produit. Indique le type de clé présenté pour ouvrir la porte qui est maintenant à l'état Porte entrebaillée.
- **Porte entrebaillée depuis** — S'affiche lorsque l'événement Porte entrebaillée se produit. Indique la date et l'heure auxquelles la porte a été considérée comme entrebaillée (non ouverte).
- **Verrou d'intimité activée** — Indique si le pêne dormant ou le verrou d'intimité est activé sur le point d'accès. Vous pouvez filtrer la liste pour afficher les points d'accès avec le verrou d'intimité activée.
- **Déverrouillé** — Indique si le point d'accès se trouve actuellement en mode Déverrouillé (il permet alors un accès illimité sans clé). Vous pouvez filtrer la liste pour afficher les points d'accès déverrouillés.
- **Dernière entrée** — La date et l'heure d'entrée la plus récente sur le point d'accès.
- **Dernière mise à jour** — La version actuelle du firmware de la serrure.

Personnaliser l'affichage

- Pour filtrer les données, cliquez sur **(Filtre)** puis sélectionnez les informations que vous souhaitez afficher.
- Cliquez sur n'importe quelle colonne pour trier la liste.
- Pour rafraîchir les données, cliquez sur **(Rafraîchir)**.

Rapports (à distance)

Cette section comprend les sujets suivants :

Rapport d'état des points d'accès en ligne 327
Rapport d'état de la passerelle en ligne 328
Rapport du point d'accès assigné et en ligne 329

Rapport d'état des points d'accès en ligne

Générez ce rapport pour afficher l'état des points d'accès en ligne.

Générer un rapport

1. Accédez à ***Rapports > Rapport d'état des points d'accès en ligne***.
2. Sélectionnez si vous souhaitez inclure les passerelles en ligne et/ou hors ligne.
3. Sélectionnez les options d'état à inclure dans le rapport : Tous/Batterie faible/Porte ouverte/Porte entrebaillée/Verrou d'intimité activée/Déverrouillée.
4. Choisissez d'afficher ou non les versions du firmware.
5. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

Ce rapport affiche les détails suivants pour toutes les situations de passerelles et les états des points d'accès actuels en ligne.

- Point d'accès
- Bâtiment
- Étage
- État
- Batterie faible
- Porte ouverte
- Porte entrebaillée
- Verrou d'intimité activée
- Serrure verrouillée
- Dernière entrée
- Dernière mise à jour
- FW Vers Serrures
- FW Vers AVR
- FW Vers Ember
- FW Vers Quantum

Rapport d'état de la passerelle en ligne

Générez ce rapport pour consulter les informations sur l'état de la passerelle.

Générer un rapport

1. Accédez à ***Rapports > Rapport d'état de la passerelle en ligne***.
2. Sélectionnez si vous souhaitez inclure les passerelles en ligne et/ou hors ligne.
3. Indiquez si vous souhaitez inclure les versions du firmware correspondantes.
4. Cliquez sur **Générer**.

Afficher les détails du rapport



La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- État de la communication
- Afficher la version du firmware
- Site
- Rapport généré par
- Rapport généré le
- Passerelle
- Type
- Adresse Mac
- État (En ligne/Hors ligne)
- Antenne
- Dernière mise à jour
- FW Vers de la passerelle
- FW Vers AVR
- FW Vers Ember

Rapport du point d'accès assigné et en ligne

Générez ce rapport pour afficher les points d'accès actuellement assignés à des passerelles.

Générer un rapport

1. Accédez à ***Rapports > Rapport du point d'accès assigné et en ligne***.
2. Indiquez si vous souhaitez inclure les points d'accès hors ligne.
3. Cliquez sur **Générer**.

Afficher les détails du rapport

La barre d'outils « Rapports » est une fonctionnalité pratique que vous pouvez utiliser pour parcourir, télécharger, imprimer et zoomer sur des rapports. Plusieurs formats de téléchargement sont pris en charge.

- Passerelle (Nom)
- Points d'accès assignés
- Points d'accès désappairés

Dépannage

Cette section comprend les sujets suivants :

Gestionnaire de services 331
Dépannage des encodeurs 335
Dépannage des serrures 339
Données de journal 345

Gestionnaire de services

Le Gestionnaire de services fournit un accès pratique aux options de configuration post-installation et au dépannage Les actions suivantes sont disponibles :

- démarrage et arrêt des services de produits
- ouverture des fichiers de configuration pour les services de produits
- installation/renouvellement du certificat SSL après l'installation
- modification de l'adresse IP du serveur
- recueil des informations de support
- ouverture de l'observateur d'événements
- ouverture des services Windows

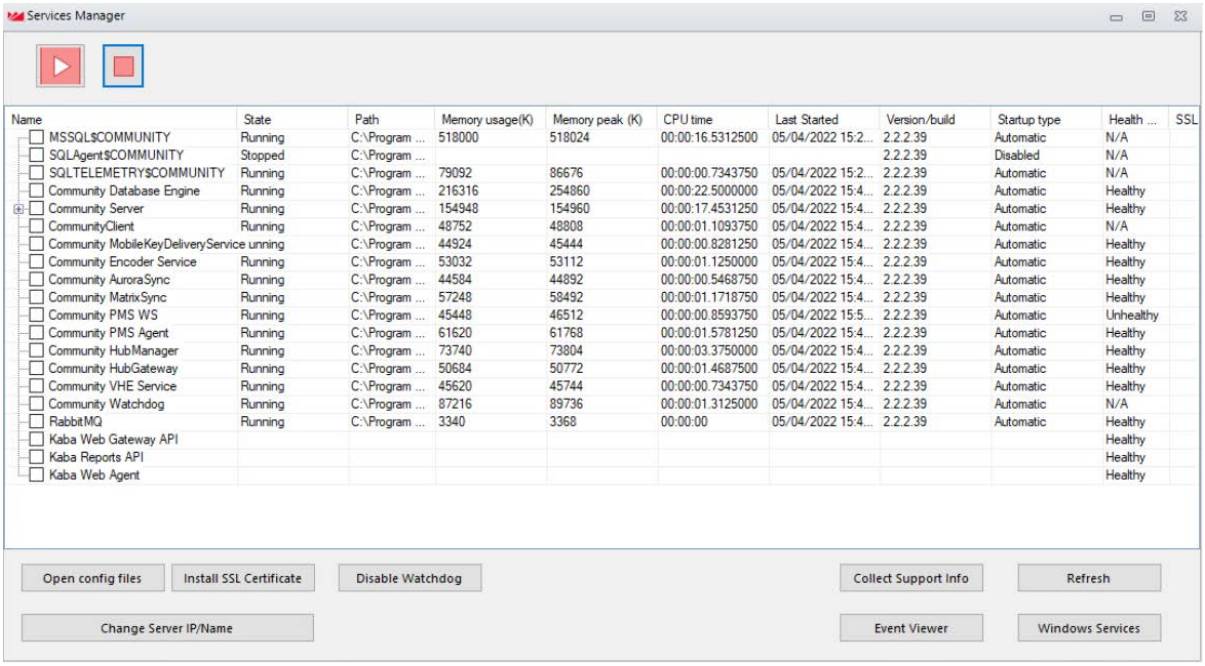
Ouvrir le Gestionnaire de services

Accédez au Gestionnaire de services sur le serveur à partir de l'emplacement par défaut :

C:\Program Files\dormakaba\Community Server\Services\Service Manager\ServiceManager.exe

Accédez au Gestionnaire de services sur le poste de travail à partir de l'emplacement par défaut :

C:\Program Files (x86)\dormakaba\Community Client\Services\ServiceManager\ServiceManager.exe

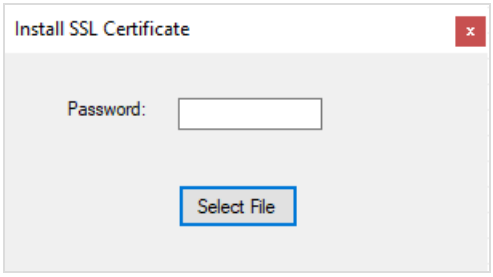


Installer/renouveler le certificat SSL après l'installation

Utilisez le Gestionnaire de services pour installer ou renouveler un certificat SSL sur le serveur Community après l'installation. Chaque poste de travail Community doit être mis à jour pour utiliser le protocole HTTPS.

Serveur

1. Sur le serveur Community, ouvrez le Gestionnaire de services.
2. Cliquez sur Installer le certificat SSL.
3. Ignorez le message d'avertissement et cliquez sur Oui pour continuer.



4. Le cas échéant, indiquez le mot de passe du certificat.
5. Cliquez sur Sélectionner le fichier.
6. Naviguez et sélectionnez le certificat (.pfx).
7. Lorsque vous êtes informé que le certificat a été installé, cliquez sur OK.

Client

Les étapes suivantes doivent être suivies sur chaque poste de travail Community.

1. Ouvrez le Gestionnaire de services.
2. Sélectionnez le service Client Community et cliquez sur  pour arrêter le service.
3. Cliquez sur Ouvrir les fichiers de configuration.
4. Modifiez les valeurs « WebAPIUrl » et « signalrURL » pour rediriger vers **https** :

- De :
  <add key="WebAPIUrl" value="http://<Community Server IP>/WebAPI/" />
  <add key="SERVICE_URL_WITH_PORT" value="http://localhost:40100" />
- À :
  <add key="WebAPIUrl" value="https://< Community Server IP>/WebAPI/" />
  <add key="SERVICE_URL_WITH_PORT" value="https://localhost:40100" />

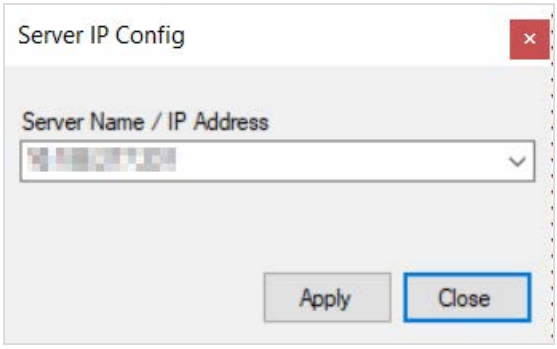
5. Sauvegardez et fermez le fichier de configuration.
6. Cliquez sur  pour redémarrer le service Client Community.

Modifier l'adresse IP / le nom du serveur

Utilisez le Gestionnaire de services pour modifier l'adresse IP du serveur Community après l'installation. La modification de l'adresse IP nécessite que le client Community soit désinstallé et réinstallé sur chaque poste de travail.

Serveur

1. Sur le serveur Community, ouvrez le Gestionnaire de services.
2. Cliquez sur Modifier l'IP/le nom du serveur.
3. Ignorez le message d'avertissement et cliquez sur Oui pour continuer.
4. Indiquez la nouvelle adresse IP ou le nouveau nom, puis cliquez sur Appliquer.



5. Redémarrez le Serveur Community.

Client

Les étapes suivantes doivent être suivies sur chaque poste de travail Community.

1. Ouvrez le Gestionnaire de services.
2. Sélectionnez le service Client Community et cliquez sur  pour arrêter le service.
3. Cliquez sur Ouvrir les fichiers de configuration.
4. Modifiez les valeurs « WebAPIUrl » et « signalrURL » pour rediriger vers la nouvelle adresse IP.

- De :
  <add key="WebAPIUrl" value="https://<Community Server IP>/WebAPI/" />
  <add key="signalrURL" value="https://< Community Server IP>/
  WebAPI/signalr/" />
- À :
  <add key="WebAPIUrl" value="https://< Community NewServer IP>/WebAPI/" />
  <add key="signalrURL" value="https://< Community NewServer IP>/
  WebAPI/signalr/"/>

5. Sauvegardez et fermez le fichier de configuration.
6. Cliquez sur  pour redémarrer le service Client Community.

Ouvrir les fichiers de configuration

Pour ouvrir les fichiers de configuration, sélectionnez les services pour lesquels vous souhaitez consulter les fichiers de configuration correspondants, puis cliquez sur **Ouvrir les fichiers de configuration**. Chaque fichier de configuration s'ouvre dans une fenêtre distincte.

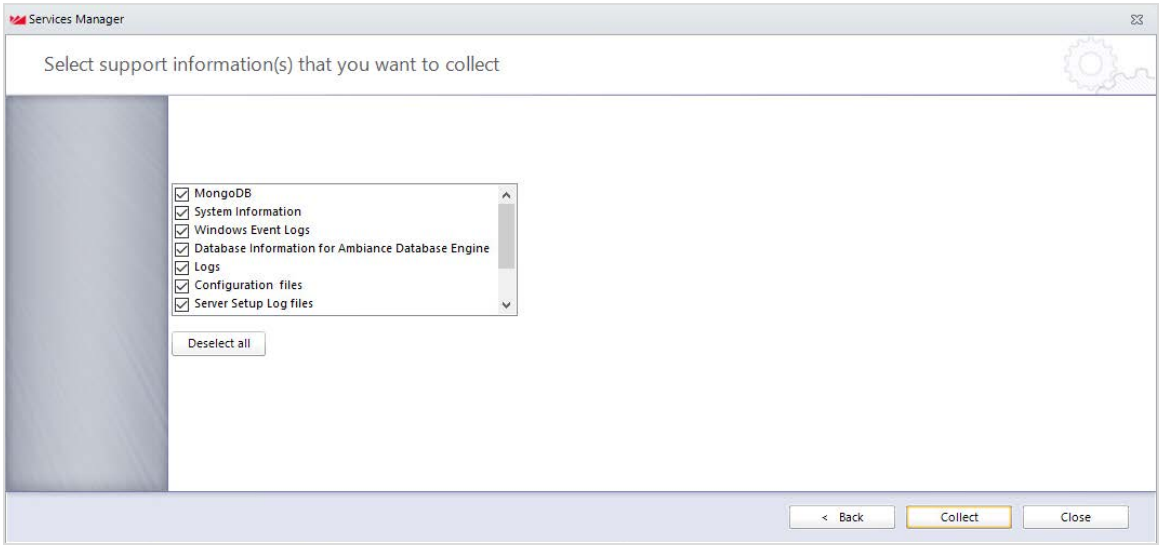
Désactiver/activer la fonction Watchdog

Le Gestionnaire de services comprend une fonction Watchdog qui effectue des contrôles réguliers de l'état du serveur. La fonction Watchdog est activée par défaut. Pour désactiver/activer la fonction Watchdog, ouvrez le Gestionnaire de services et cliquez sur le bouton approprié.

Recueillir les informations de support

Avant de contacter dormakaba pour le support, collectez les informations sur votre système Community. Collectez les informations relatives au serveur et au poste de travail.

1. Ouvrez le Gestionnaire de services, puis cliquez sur **Collecter les informations pour le support**.



2. Sélectionnez le type d'informations pour le support que vous souhaitez collecter.
3. Cliquez sur **Collecter**.
4. Définissez un nom de fichier, puis cliquez sur **Sauvegarder**.

Ouvrir l'observateur d'événements

Pour ouvrir l'application Observateur d'événements Windows, cliquez sur **Observateur d'événements**.

Ouvrir les services Windows

Pour ouvrir l'application Windows Services, cliquez sur **Windows Services**.

Dépannage des encodeurs

En cas d'erreur d'encodage ou de lecture de la clé, une fenêtre d'information identifie les problèmes suivants :

- Si la communication entre l'encodeur et le poste de travail échoue.
- Si l'encodeur est hors ligne.
- Si l'encodeur est occupé.
- Si aucune clé n'est présentée à l'encodeur dans le délai prévu.
- Si la clé est endommagée ou corrompue ou qu'elle utilise une technologie non prise en charge.
- Si la communication échoue au niveau du serveur.

Le Client Community est-il requis/installé ?

Vous devez installer le Client sur chaque poste de travail où un encodeur USB et/ou un programmateur M-Unit est requis. Depuis la page Community, téléchargez le Client. Trois fichiers sont nécessaires :Community_Client.exe, serverURL.config et token.txt.

N'installez pas le Client sur le Serveur Community.

Suivez les instructions pour chacune des pages suivantes de l'assistant.

1. Sur la page de **Bienvenue**, cliquez sur **Suivant**.
2. Sur la page **Contrat de licence**, acceptez les conditions du contrat de licence, puis cliquez sur **Suivant**.
3. Sur la page **Choisissez l'emplacement de destination**, choisissez où installer les fichiers du Client, puis cliquez sur **Suivant**. L'emplacement par défaut est recommandé.
4. Lorsque vous êtes informé que l'installation est réussie, cliquez sur **Terminer**.

L'encodeur est-il connecté au poste de travail et configuré correctement ?

La configuration initiale d'un encodeur nécessite la connexion de l'encodeur au poste de travail Community à l'aide d'un câble USB. Par défaut, le périphérique émet un bip audible et un voyant vert clignote pour indiquer une connexion réussie. Si vous configurez l'encodeur pour une connexion à l'aide d'un câble USB, l'encodeur doit rester connecté au poste de travail.

Configurer un encodeur pour USB

1. Branchez l'encodeur sur le poste de travail.
2. Dans **Gestion des périphériques**, cliquez sur **Nouvel encodeur**.
3. Indiquez un nom unique ne dépassant pas 50 caractères. Ce nom s'affiche dans la liste des encodeurs.
4. Indiquez un numéro pour identifier l'encodeur au PMS (Système de gestion d'établissement). Valeurs valides : 0-99.
5. Sélectionnez l'adresse MAC de l'encodeur. La valeur est détectée automatiquement lorsque vous connectez l'encodeur au poste de travail.
6. Sélectionnez **USB**.
7. Cliquez sur **Sauvegarder**.

Configurer un encodeur pour TCP/IP

Avant de commencer, assurez-vous qu'un port est ouvert pour la communication entrante sur le serveur Community (généralement configuré lors de l'installation initiale du serveur).

1. Branchez l'encodeur sur le poste de travail.
2. Dans **Gestion des périphériques**, cliquez sur **Nouvel encodeur**.
3. Indiquez un nom unique ne dépassant pas 50 caractères. Ce nom s'affiche dans la liste des encodeurs.
4. Indiquez un numéro pour identifier l'encodeur au PMS (Système de gestion d'établissement). Valeurs valides : 0-99.

5. Sélectionnez l'adresse MAC de l'encodeur. La valeur est détectée automatiquement lorsque vous connectez l'encodeur au poste de travail.
6. Sélectionnez TCP/IP.
7. Indiquez si vous souhaitez obtenir une adresse IP automatiquement. Si vous utilisez DHCP, sélectionnez **OUI**.
8. Indiquez si vous souhaitez utiliser le nom du serveur ou l'adresse IP, puis indiquez les informations correctes.
9. Si vous n'utilisez pas DHCP, indiquez l'adresse IP de l'encodeur, y compris le masque de sous-réseau et la passerelle par défaut.
10. Cliquez sur **Sauvegarder**.

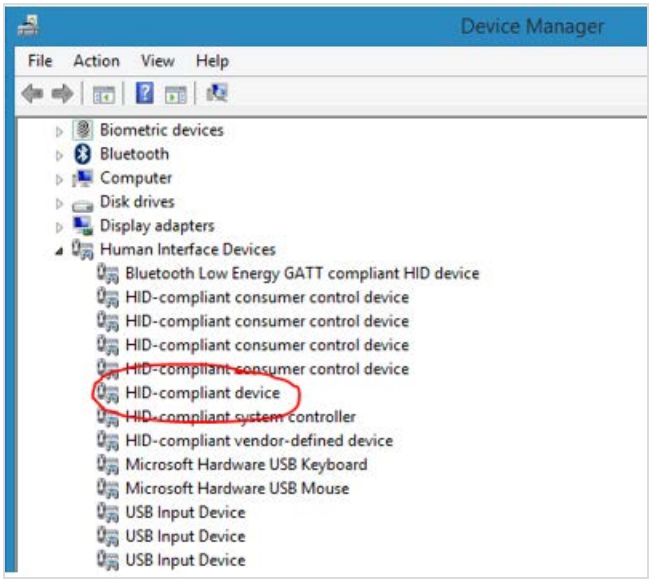
Vous avez toujours un problème d'encodage ou de lecture des clés ?

Pour vous préparer au dépannage, consultez le journal suivant :

C:\ProgramData\dormaKaba\Community\logs\Services\DokaClient.exe.log

Étapes de dépannage :

1. Assurez-vous que le service client Community fonctionne sur le poste de travail. Accédez à Services et vérifiez (ou redémarrez) le service Community.
2. Vérifiez la connexion physique entre l'encodeur et le poste de travail. Débranchez et branchez l'encodeur. Assurez-vous que vous entendez 2 bips et que les voyants sont allumés sous l'encodeur.
3. Vérifiez l'encodeur dans le Gestionnaire de périphériques :
   a. Débranchez l'encodeur du poste de travail.
   b. Ouvrez le Gestionnaire de périphériques.
   c. Branchez l'encodeur.
   d. Assurez-vous qu'un nouveau périphérique conforme au HID apparaît et qu'il n'est pas dans un état d'erreur.

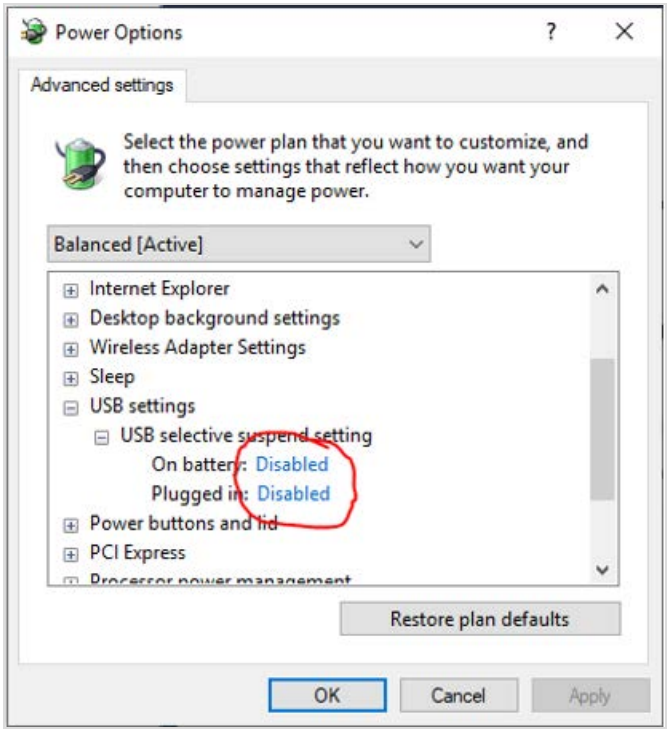


4. Vérifiez l'adresse IP :
   a. Accéder à : C:\Program Files (x86)\dormaKaba\Community Client\Services\ClientServices et ouvrir le fichier **DokaClient.exe.Config** (dans le Bloc-notes).
   b. Assurez-vous que l'adresse IP du serveur est correcte dans les lignes suivantes :
   <add key="WebAPIUrl" value="http://ip_address/WebAPI/" />
   <add key="signalrURL" value="http://ip_address/WebAPI/signalr/" />
5. Dans la Gestion des périphériques, assurez-vous que l'adresse MAC de l'encodeur n'est pas attribuée à un autre poste de travail.



Vous devrez peut-être vérifier qu'un port est ouvert pour la communication entrante sur le serveur Community (généralement configuré lors de l'installation initiale du serveur).

6. Si un encodeur USB cesse de fonctionner, suivez ces étapes sur les postes de travail :
   a. Accédez à Panneau de configuration – Options d'alimentation.
   b. Cliquez sur Modifier les paramètres du plan.
   c. Cliquez sur Modifier les paramètres d'alimentation avancés.
   d. Sélectionnez les paramètres USB.
   e. Sélectionnez le paramètre de suspension sélective USB.
   f. Modifiez les deux paramètres sur Désactivé.



7. L'adresse MAC de l'encodeur ne s'affiche pas après l'installation du client ?
   - Le serveur a été configuré en utilisant soit le nom du serveur, soit l'adresse IP.
   - Installez le client en utilisant le nom du serveur au lieu de l'adresse IP.
   - Effectuez une réinitialisation matérielle de l'encodeur :
     a. Débranchez le câble de l'encodeur.
     b. Appuyez sur le bouton de réinitialisation au dos de l'encodeur et maintenez-le enfoncé.
     c. Insérez le câble d'alimentation de l'encodeur (tout en continuant à appuyer sur le bouton de réinitialisation et à le maintenir enfoncé).
     d. Maintenez le bouton de réinitialisation de l'encodeur enfoncé pendant 2 secondes supplémentaires, puis relâchez-le. Vous devriez entendre 5 bips rapides si la réinitialisation de l'encodeur est réussie.

Si le problème persiste après le dépannage, contactez le support dormakaba.

Dépannage des serrures

Pour des raisons de sécurité, dormakaba impose un nombre maximum de clés inutilisées qui peuvent être remises pour un identifiant donné. Par exemple, si plus de 15 clés sont remises mais jamais présentées à la Chambre 100, le point d'accès devient « hors séquence » et refuse l'accès à toutes les clés.

Pour rétablir l'accès aux clés, reprogrammez le point d'accès à l'aide du Programmateur M-Unit ou reséquencez le point d'accès à l'aide de la Clé de reséquence. Une fois reséquencé, le point d'accès accepte la dernière clé remise.

Le nombre maximum de clés inutilisées avant qu'un reséquençage ne soit nécessaire dépend du type de clé :

- Clés de résidents
  - Chambre et suite = 15
- Clés du personnel
  - Toutes les catégories = illimité
- Clés Système
  - Clés à sécurité intégrée, de verrouillage, de déverrouillage, de bascule de libre passage = 15
  - Clés ELO = 3
  - Clés d'annulation = 0
  - PPK/SPK = 0

Voyants lumineux

Les trois voyants (vert, jaune et rouge) sont situés sur la face de la serrure. Ces voyants fournissent des informations sur l'état de la serrure lorsqu'une clé est insérée dans la serrure et retirée. Lors de l'utilisation d'une serrure RFID, les voyants LED suivants s'affichent lorsqu'une carte RFID est présentée au lecteur de la serrure.

Le cycle d'ouverture par défaut est de quatre secondes, mais il est programmable.

Voyant vert

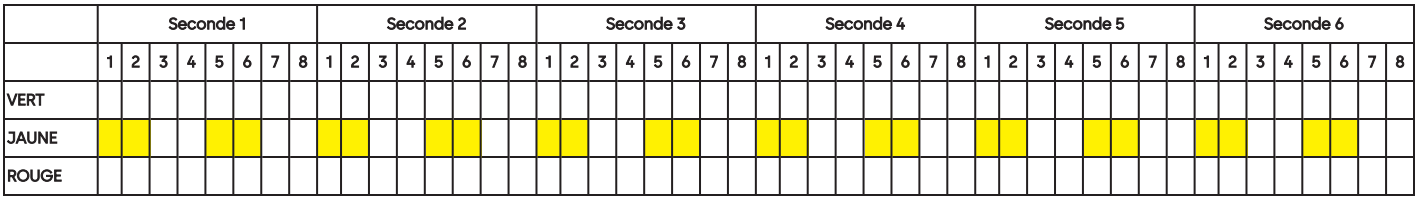
Un voyant vert clignote pendant environ quatre secondes lorsqu'une clé correcte est utilisée.

	Seconde 1								Seconde 2								Seconde 3								Seconde 4								Seconde 5								Seconde 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
VERT	■	■			■	■			■	■			■	■			■	■			■	■			■	■			■	■																		
JAUNE																																																
ROUGE																																																

Cette séquence indique que le mécanisme de verrouillage a été libéré et que l'on peut appuyer sur la poignée pour ouvrir la porte. Si la poignée n'est pas enfoncée pendant que le voyant vert clignote, le mécanisme de verrouillage est sécurisé, et la clé doit alors être réinsérée et retirée de la serrure pour libérer le loquet.

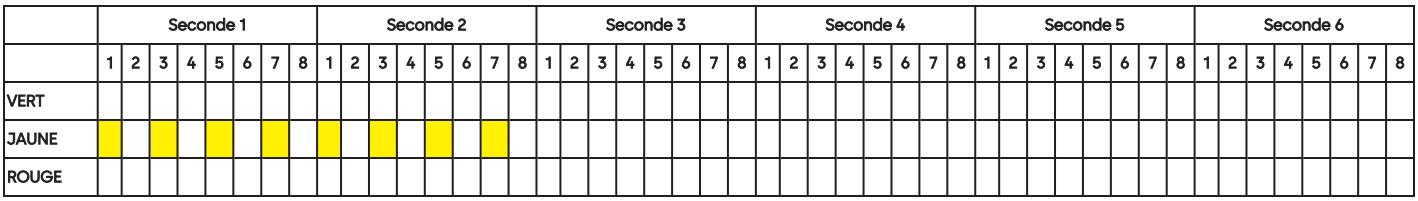
Voyant jaune

Voyant jaune clignotant (12 fois)



Ce voyant jaune clignotant indique qu'une bonne clé a été insérée dans la serrure, mais que le pêne dormant ou le bouton/verrou d'intimité a été réglé de l'intérieur de la chambre.

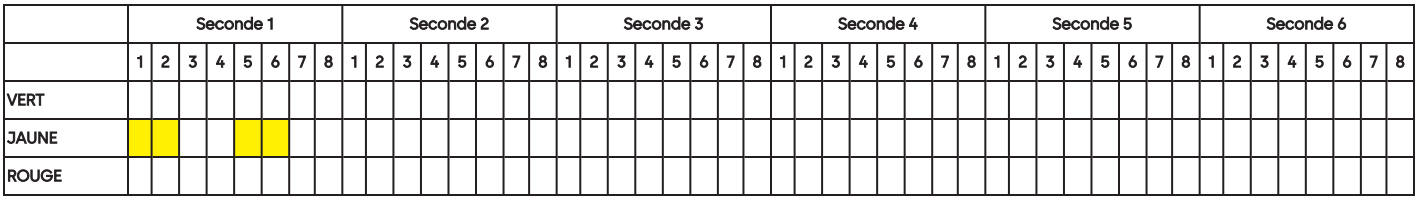
Voyant jaune à clignotement rapide (8 fois)



Ce voyant jaune à clignotement rapide indique qu'une bonne clé a été utilisée dans la serrure, mais que l'entrée est refusée pour l'une des raisons suivantes :

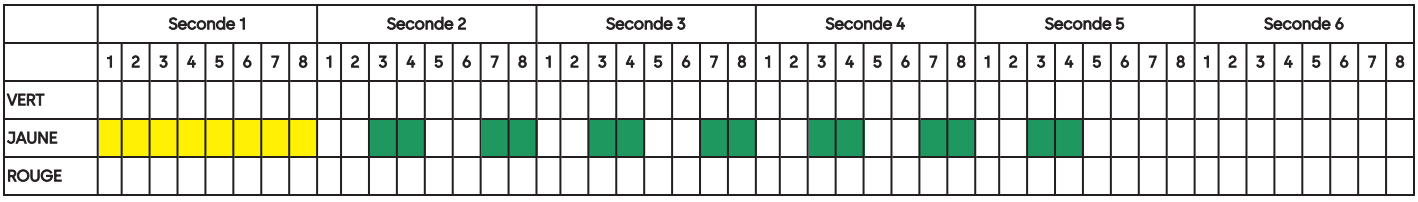
- La porte a été doublement verrouillée électroniquement par une clé de bascule de blocage électronique.
- La clé résident a été automatiquement inhibée, ou la serrure a été inhibée par les clés d'annulation.
- La clé a été programmée avec une date et une heure d'expiration. Le voyant indique que la clé a été utilisée après cette date et cette heure d'expiration.
- La clé maître était programmée pour ne fonctionner que pendant certaines heures de la journée, ou pour ne fonctionner que certains jours de la semaine. Le voyant indique que la clé utilisée n'a pas été programmée pour ce quart ou ce jour.

Deux clignotements jaunes



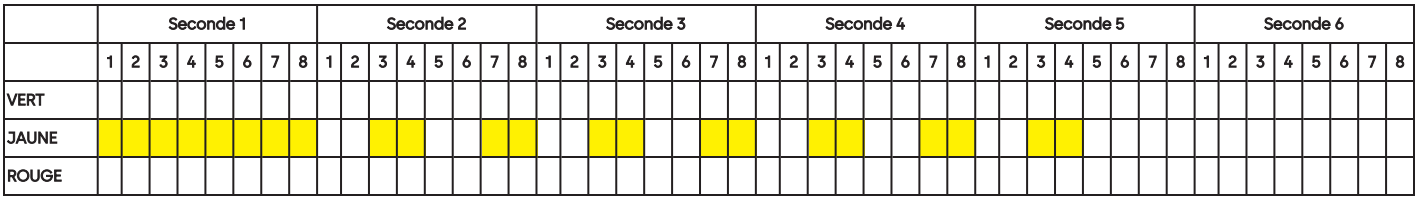
Deux clignotements jaunes indiquent qu'une mauvaise clé a été insérée dans la serrure.

1 clignotement jaune avant 7 clignotements verts



Cette séquence indique que la clé maître est sur le point d'expirer mais que l'accès est autorisé. Ce voyant apparaîtra sept jours avant la date d'expiration.

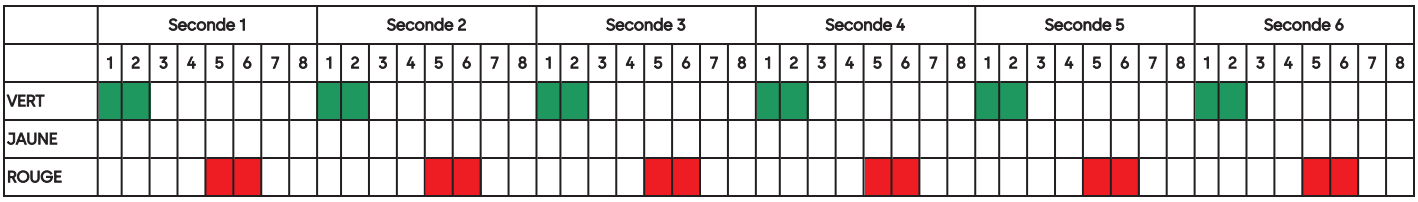
1 clignotement jaune avant 7 clignotements jaunes



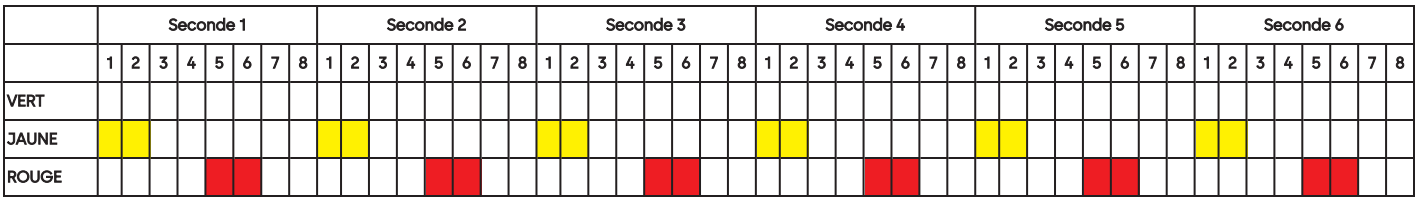
Cette séquence indique que la clé maître est sur le point d'expirer mais que l'accès est refusé (Verrou d'intimité = ACTIVÉ). Ce voyant apparaîtra sept jours avant la date d'expiration.

Voyant rouge

Voyant rouge clignotant en alternance

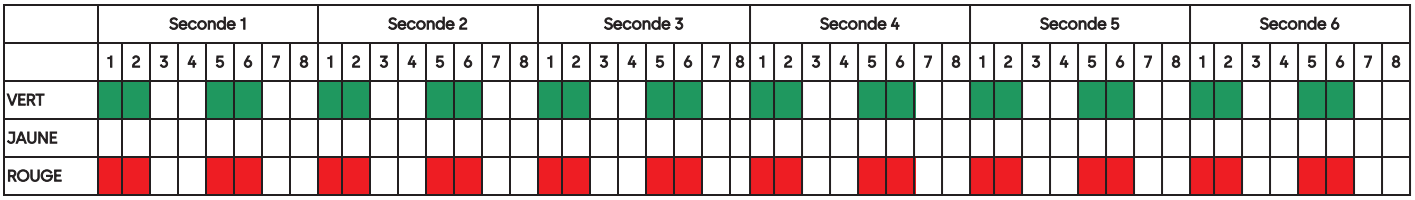


ou

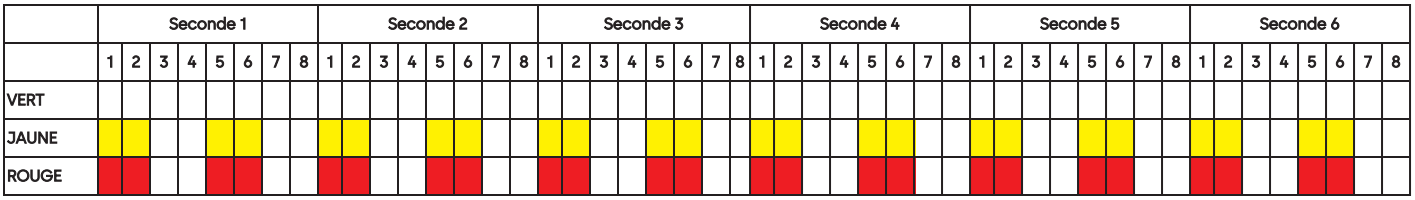


Un voyant rouge clignote en alternance avec un autre voyant lorsque les batteries de la serrure sont faibles.

Voyant rouge clignotant simultanément



ou



Un voyant rouge clignote simultanément avec un autre voyant lorsque l'horloge de la serrure doit être réinitialisée.

Clignotement rouge (1 ou 2 fois)

	Seconde 1								Seconde 2								Seconde 3								Seconde 4								Seconde 5								Seconde 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
VERT																																															
JAUNE																																															
ROUGE																																															

Si un voyant rouge clignote une ou deux fois lorsqu'une clé est insérée dans la serrure, cela signifie que la clé a été utilisée de manière incorrecte (à l'envers ou non retirée). Si un voyant rouge clignote une ou deux fois alors qu'aucune clé n'est insérée, l'interrupteur à clé est bloqué.

Voyants jaunes et rouges

Deux clignotements jaune et rouge.

	Seconde 1								Seconde 2								Seconde 3								Seconde 4								Seconde 5								Seconde 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
VERT																																															
JAUNE																																															
ROUGE																																															

Ces voyants indiquent que la serrure n'a pas pu lire correctement le code de la clé.

Aucun voyant

Si aucun voyant n'apparaît lorsqu'une clé est insérée :

- Une fermeture à clé invalide est en place.
- L'interrupteur à clé est cassé.
- Les batteries de la serrure sont mortes.

Indicateurs de verrouillage et de mode invalides

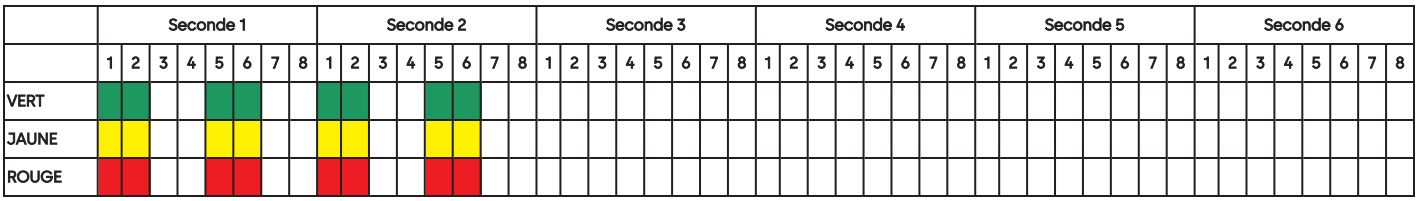
Les serrures sont conçues pour fonctionner en Mode 2 lorsqu'elles sont programmées et qu'elles fonctionnent correctement. Si une serrure ne fonctionne pas en Mode 2 et qu'une clé valide est utilisée, vous verrez l'un des modèles suivants. Ces voyants indiquent qu'il y a un problème physique avec la serrure qui doit être corrigé avant que la serrure ne permette aux clés de fonctionner normalement.

1 vert, 1 jaune, 1 rouge, puis tous les voyants clignotent (4 fois)

	Seconde 1								Seconde 2								Seconde 3								Seconde 4								Seconde 5								Seconde 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
VERT																																															
JAUNE																																															
ROUGE																																															

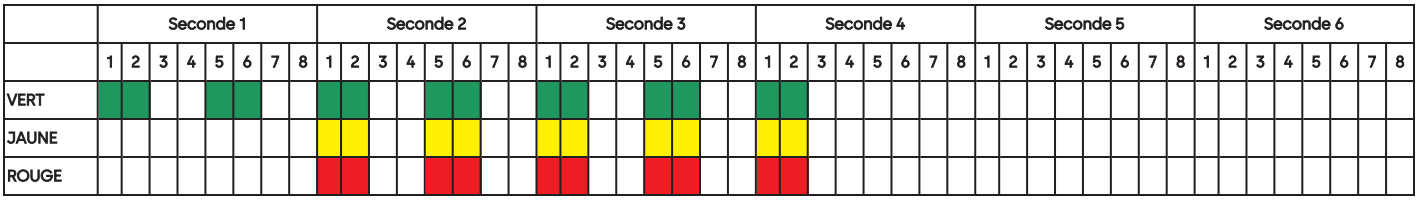
Ces voyants indiquent que la serrure est en Mode test et que la puce de stockage a échoué. Aucune clé ne permet d'ouvrir la serrure et il faut percer la serrure pour accéder à la chambre.

Tous les voyants clignotent (4 fois)



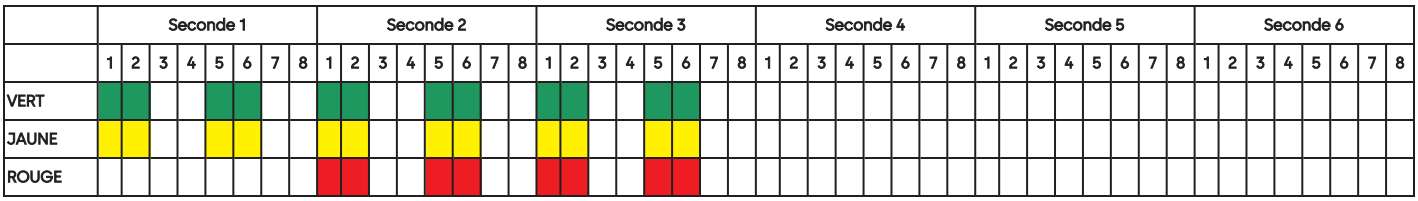
Ces voyants indiquent que le verrouillage est en Mode 0 et qu'il y a un problème avec la carte de circuit. Utilisez la touche d'effacement pour passer en Mode 1 et programmez le verrouillage à l'aide de la sonde et du terminal LPI. Utilisez la nouvelle clé pour ouvrir la porte et remplacer la carte de circuit.

2 clignotements verts. Puis tous les voyants clignotent (4 fois)



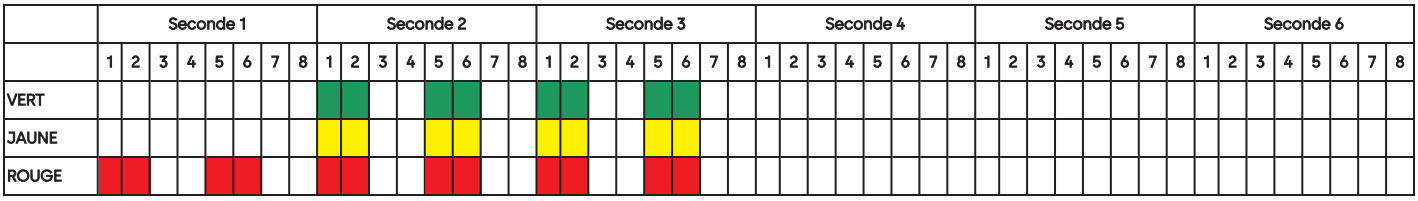
Ces voyants indiquent que la serrure est en Mode 1 et qu'elle n'est pas programmée. Programmez le verrouillage à l'aide de la sonde et du terminal LPI. Utilisez la nouvelle clé pour ouvrir la porte et remplacer la carte de circuit.

2 clignotements verts et jaunes. Puis tous les voyants clignotent (4 fois)



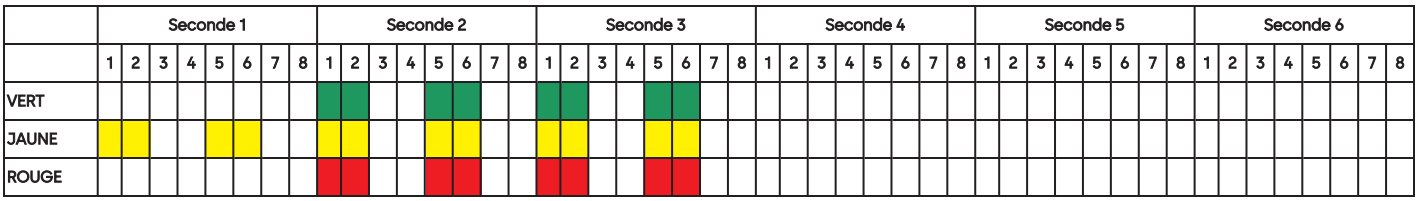
Ces voyants indiquent que la serrure est en Mode 3 et qu'il y a un problème de programmation avec la puce de programmation dans la carte de circuit de la serrure. Ouvrez la porte à l'aide de la clé PPK suivie d'une clé maître valide. Retirez la serrure et remplacez la carte de circuit imprimé.

2 clignotements rouges. Puis tous les voyants clignotent (4 fois)



Ces voyants indiquent que la serrure est en Mode 4 et que la puce de stockage est désactivée. Utilisez la clé PPK suivie de la clé de désactivation/activation pour activer le verrouillage.

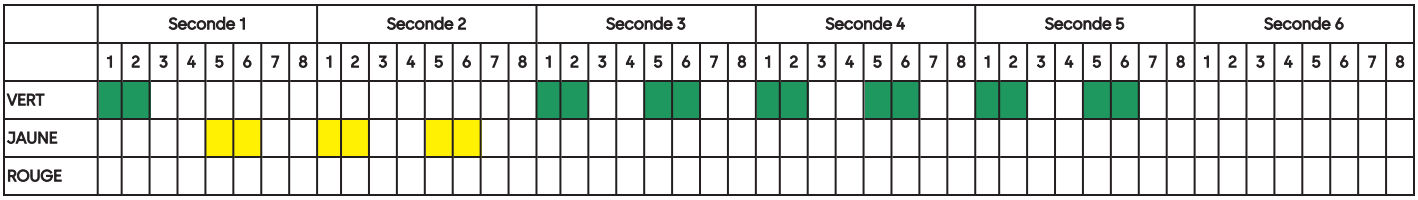
2 clignotements jaunes, puis tous les voyants clignotent (4 fois)



Ces voyants indiquent que la serrure est en Mode 5 et qu'il y a un problème avec le contact de moteur ou que le moteur est bloqué. Ouvrez la porte à l'aide de la clé PPK suivie d'une clé maître valide. Ensuite, retirez la serrure et remplacez la serrure complète.

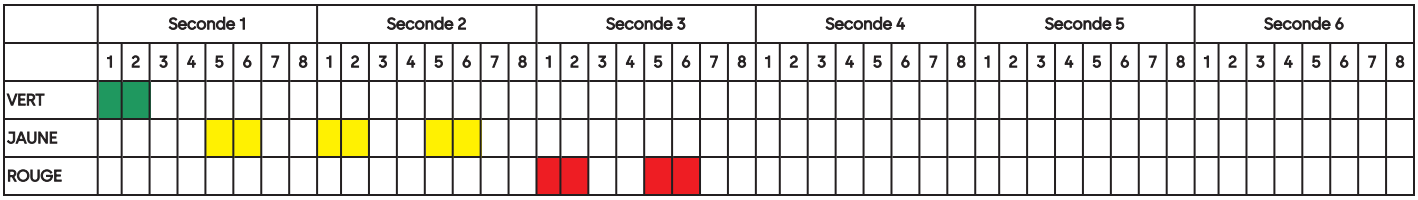
En ligne

1 clignotement vert, quelques clignotements jaunes, 6 clignotements verts.



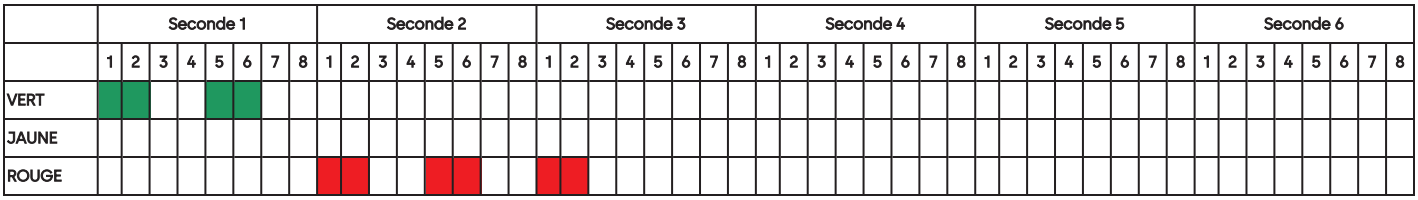
Lors de la présentation d'une clé d'appairage RF et que l'appairage est réussi.

1 clignotement vert, quelques clignotements jaunes, 2 clignotements rouges.



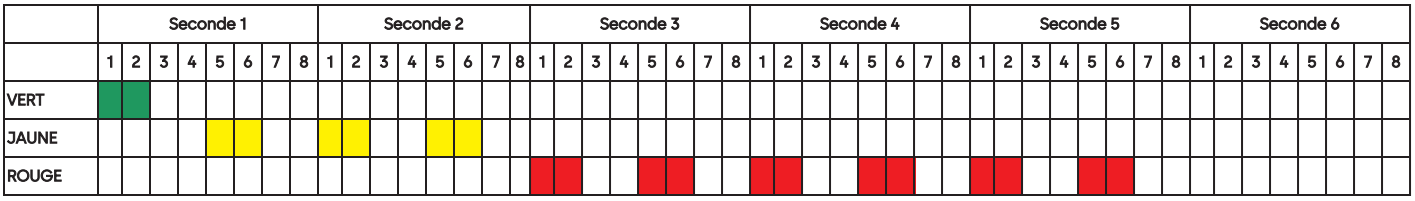
Lors de la présentation d'une clé d'appairage RF et que l'appairage échoue.

2 clignotements verts, 3 clignotements rouges



Lors de la présentation d'une clé de désappairage RF, cette séquence indique que la serrure n'a pas été appairée.

1 clignotement vert, 3 clignotements jaunes, 6 clignotements rouges



Lors de la présentation d'une clé de désappairage RF, cette séquence indique que la serrure était appairée et est maintenant désappairée.

Données de journal

Les journaux Community fournissent des informations détaillées concernant tous les événements et activités système qui ont lieu pendant l'installation (ou la mise à niveau) et l'utilisation du produit. Pour les techniciens du support, les journaux sont la ressource principale pour le dépannage.

Journaux d'installation

Les journaux d'installation suivants se trouvent par défaut sur le serveur à l'adresse : C:\Community Server:

- MongoInstall (pour la communication en ligne)
- SetupServer (journal d'installation primaire)

Le journal d'installation suivant se trouve par défaut sur le poste de travail à l'adresse : C:\Community Server:

- SetupClient.LOG

Journaux produit

De multiples journaux sont enregistrés par défaut à l'adresse : C:\ProgramData\dormaKaba\Community\logs

Le dossier contenant les journaux organise les fichiers journaux comme suit :

- Services — Données relatives aux différents services Windows Community.
- Web
  - reportapi.log.txt — Données relatives à l'API de rapport composants IIS utilisé pour générer des rapports.
  - webApi.log.txt — Données relatives au service Windows Community WebAPI.

Annexes

Cette section comprend les annexes suivantes :

Glossaire

A

Accès aux espaces communs
Sous-module dans Gestion des accès où sont définis les profils d'espace commun pour configurer l'accès aux espaces communs.

Accès prédéfini
Un établissement associé à un type de catégorie d'identifiants qui est caractérisé par la sélection de l'accès lors de la définition de l'identifiant.

Accès privé
Type de point d'accès destiné à l'accès du personnel uniquement.

Accès variable
Un établissement associé à un type de catégorie d'identifiants qui est caractérisé par la sélection de l'accès lors de la création de la clé.

API Community
Ensemble de méthodes API Web permettant d'intégrer la Gestion des résidents et la Gestion du personnel/prestataire avec des systèmes tiers.

Ascenseur
Une structure physique destinée à permettre l'accès aux étages du bâtiment.

Attribution horaire au point d'accès
Sous-module dans Gestion des accès dans lequel vous pouvez affecter les horaires de libre passage et d'accès aux points d'accès.

Audit
Le processus de récupération d'informations historiques à partir d'un point d'accès.

B

Bâtiment
Composante du Configurateur de site qui représente une structure physique sur le site qui contient un ou plusieurs étages et un ou plusieurs points d'accès.

C

Carte relais
Composant électrique dans un boîtier de commande d'ascenseur avec un ou plusieurs interrupteurs de relais. Un relais est un composant électrique associé à des étages spécifiques.

Catégorie d'identifiants
Nom utilisé pour regrouper des identifiants selon le type de catégorie d'identifiants.

Clé
Un support de transport sur lequel un identifiant est encodé dans le but de contrôler l'accès et/ou d'effectuer des opérations système ou de programmation. Par exemple, cartes-clés et porte-clés.

Clé-personnel
Catégorie/type de catégorie d'identifiants. L'accès est prédéfini. Le mode bascule est pris en charge pour les unités/unités de suites en option dans Configurateur de site.

Clé-personnel (accès variable)
Catégorie/type de catégorie d'identifiants. L'accès est variable. Le mode bascule est pris en charge pour les unités/unités de suites en option dans Configurateur de site.

Clé à fonction spéciale
Clé système utilisée pour des opérations de verrouillage avancées.

Clé à sécurité intégrée
Clé de rechange créée à l'avance et conservée en jeux complets à remettre au cas où une défaillance système ou une panne de courant empêche la création de clés.

Clé à usage restreint (Personnel)
1) Catégorie/type de catégorie d'identifiants pour les clés du personnel. 2) Une clé du personnel encodée avec un accès temporaire à un point d'accès pour un nombre de fois prédéfini ou jusqu'à expiration de la clé.

Clé d'annulation
Clé système invalidant définitivement une instance de clé spécifique.

Clé d'urgence (Community)
1) Catégorie/type de catégorie d'identifiants pour l'ouverture forcée du pêne dormant/verrou d'intimité. 2) Un type de clé encodée avec un identifiant basé sur la catégorie Urgence. Le mode bascule est pris en charge pour les unités/suites en option dans Configurateur de site.

Clé de bascule de libre passage
1) Catégorie d'identifiants pour les clés système. 2) Clé système utilisée pour activer et/ou désactiver le mode passage.

Clé de blocage
Clé système qui bloque temporairement toutes les clés encodées avec un identifiant spécifique.

Clé de blocage électronique (ELO)
1) Catégorie d'identifiants pour les clés Système. 2) Clés système invalidant temporairement toutes les clés non dédiées aux urgences.

Clé de déblocage
Clé système débloquant toutes les instances d'un identifiant spécifique sur des points d'accès ayant été préalablement bloqués à l'aide d'une clé de blocage.

Clé de déverrouillage
1) Catégorie d'identifiants pour les clés système. 2) Clé système qui active le mode passage (accès sans restriction) dans la serrure.

Clé de diagnostic
Clé système interrogeant des serrures pour extraire l'état de diverses fonctions de serrures à des fins de résolution de problèmes et de reporting. Les résultats de diagnostic sont communiqués par une séquence de clignotements LED.

Clé de programmation primaire
Clé système autorisant la fonction d'une autre clé système.

Clé de programmation secondaire
Clé système qui reprogramme ou resynchronise la clé de programmation primaire (PPK) actuelle.

Clé de rechange
Une clé supplémentaire créée pour remplacer une clé perdue ou défectueuse.

Clé de reséquence
Clé système resynchronisant un identifiant d'une clé spécifique sur des points d'accès.

Clé de verrouillage
1) Catégorie d'identifiants pour les clés système. 2) Clé système qui désactive le mode passage.

Clé du prestataire
Catégorie/type de catégorie d'identifiants. L'accès est variable. Le mode bascule est pris en charge pour les unités/unités de suites en option dans Configurateur de site.

Clé mobile
Clé virtuelle remise pour un téléphone portable.

Clé supplémentaire
Double des clés. Une nouvelle clé doit être active avant que l'option de créer une clé supplémentaire ne soit activée. Les clés supplémentaires n'affectent pas les clés actives existantes.

Clés d'annulation
1) Catégorie d'identifiants pour les clés Système. 2) Clé système annulant définitivement tous les accès pour un résident actuel.

Clés de construction
Clés qui sécurisent les points d'accès après l'installation mais avant la programmation des serrures. Les clés de construction (ou de zone) sont obsolètes après la programmation des serrures.

Clés du personnel/prestataire
1) Le module où vous créez des clés pour le personnel/les prestataires. 2) Clés encodées avec un identifiant du personnel/du prestataire.

Clés Système
1) Le module où vous créez des clés pour effectuer des opérations de verrouillage ou au niveau du système. 2) Clés créées dans le module Clés Système.

Communication en ligne
Une fonctionnalité sous licence qui fait référence à la communication sans fil entre les points d'accès et Community. La communication à distance est utilisée pour effectuer des opérations en ligne sur les points d'accès et pour recevoir des événements de points d'accès en ligne.

Configurateur de site
Le module où vous créez une représentation virtuelle du site : bâtiments, étages et ascenseurs par bâtiment, et points d'accès.

D

Droits (Gestion des rôles)
Autorisations discrètes pour la fonctionnalité Community.

E

Encodeur
Périphérique intégré servant à encoder des clés.

Espace commun pour le personnel
Type de points d'accès où l'accès général est configuré pour le personnel.

Espace commun pour les résidents
Type de points d'accès où l'accès général est configuré pour les résidents.

Étage
Composante du Configurateur de site qui représente un niveau dans un bâtiment.

État de l'opérateur
État d'un Opérateur.

État de la clé
L'état actuel de la clé.

État des points d'accès
État actuel de la serrure installée pour un point d'accès donné.

F

Firmware
Logiciel d'exploitation pour les périphériques matériels.

G

Gestion des accès
Module qui permet de définir les identifiants pour les clés du personnel et les clés Système, de configurer et d'attribuer les horaires, de configurer l'accès aux espaces communs et de créer des groupements logiques de points d'accès pour faciliter l'attribution des identifiants.

Gestion des identifiants
Sous-module dans Gestion des accès où vous pouvez créer et gérer les identifiants.

Gestion des notifications
Module dans lequel vous pouvez configurer et gérer les groupes de notification qui peuvent être attribués aux membres du personnel.

Gestion des périphériques
Le module où vous ajoutez et configurez des encodeurs. Si la communication en ligne est activée, vous pouvez également configurer des passerelles et des points d'accès assignés. Dans les environnements cloud, vous pouvez également configurer la passerelle cloud si vous disposez d'une licence pour la Passerelle cloud - PMS Bridge.

Gestion des résidents
Module dans lequel vous pouvez gérer tous les accès et clés des résidents.

Gestion des rôles
Module dans lequel vous pouvez configurer les rôles des opérateurs et le système et les droits de clés associés à chaque rôle.

Gestion des visiteurs
Fonction gratuite qui permet d'étendre l'accès aux visiteurs par l'envoi d'un code PIN ou d'une clé mobile attribuée. Nécessite les licences AuroraSync et de la clé mobile.

Gestion du personnel/prestataire
Module dans lequel vous pouvez ajouter des membres du personnel/prestataires, configurer les opérateurs et gérer les clés du personnel/prestataire.

Groupe d'ascenseurs
Groupe d'ascenseurs qui partagent la même configuration de contrôleur d'ascenseur.

Groupe de notification
Regroupement logique d'un ou plusieurs événements de notification configurés dans le module Gestion des notifications aux fins de souscription des opérateurs.

Groupe de points d'accès
Regroupement logique d'un ou de plusieurs points d'accès qui facilite l'attribution d'identifiants à tous les points d'accès du groupe.

H

Horaire d'accès
Les contraintes de jour et d'heure contrôlent lorsqu'un point d'accès est accessible.

Horaire de libre passage
Jour et période permettant le passage sans clés.

Horaire des clés du personnel
Contraintes de jour et d'heure appliquées aux clés du personnel.

I

ID de la clé
Clé spécifique parmi plusieurs clés encodées avec le même identifiant.

Identifiant
1) Configuration qui se compose de groupes de points d'accès et/ou de points d'accès individuels à des fins d'autorisation d'accès du personnel à un espace physique ou à une fonctionnalité de clé système. 2) Code d'identification numérique stocké sur une clé qui autorise l'accès où le code est valide.

L

Lecteur
Périphérique intégré qui lit les données de contrôle d'accès stockées sur des clés.

M

Mode bascule
Fonctionnalité qui alterne l'état d'une serrure pour autoriser/refuser l'accès.

Mode de la clé
Option que vous sélectionnez lors de la création d'une clé : Nouveau ou Supplémentaire.

Mode passage
État de la serrure au cours duquel les contrôles d'accès programmés dans la serrure sont suspendus afin de permettre un libre accès.

N

Notification
Alerte émise aux souscripteurs de la notification.

Nouvelle clé
Clé créée en utilisant le mode Nouvelle. Les nouvelles clés invalident l'accès à l'identifiant sélectionné sur toutes les clés existantes.

O

Opérateur
Membre du personnel auquel est assigné un rôle qui est configuré pour autoriser l'accès aux modules Community et fonctionnalités.

P

Paramètres du système
Le module où sont spécifiées les options, les préférences et les valeurs par défaut pour l'ensemble du site. Certains paramètres contrôlent si des fonctionnalités Community sont activées et leur mode de fonctionnement.

Passerelle
Les passerelles sont les périphériques de réseau appairés à des points d'accès pour la communication en ligne.

PCI-DSS
Norme de sécurité de l'information offrant une protection de connexion supplémentaire.

Période (Horaires)
Un intervalle de temps sélectionné pour les horaires dans la Gestion des accès.

Personnel
Opérateurs et porteurs de clés au sein de votre organisation.

Point d'accès
1) Représentation virtuelle d'un emplacement physique où le passage entre deux espaces est contrôlé par une serrure. 2) Serrure équipée d'un lecteur et encodée avec des données de contrôle d'accès pour autoriser ou refuser l'accès selon des identifiants.

Point d'accès assigné
Dans la communication en ligne, un point d'accès qui est connecté à une passerelle.

Porteur de clé
Une personne autorisée à posséder au moins une clé.

Poste de travail
Ordinateur utilisé par les opérateurs pour accéder au logiciel Community.

Profil d'espace commun (Community)
Configuration définissant les espaces communs accessibles pour les unités et suites sélectionnées ou pour les identifiants du personnel sélectionnés, et si l'accès est inclus par défaut ou doit être sélectionné manuellement.

Profil de la serrure
Modèle de dispositif de verrouillage.

Profil du contrôleur d'ascenseur
La configuration du modèle de groupe d'ascenseurs.

Programmateur M-Unit
Périphérique intégré portatif utilisé pour transférer des données entre Community et des serrures.

Programmation et audit
Module dans lequel vous pouvez effectuer les transferts de données nécessaires pour programmer et auditer des serrures.

R

Rapport d'audit de point d'accès
Informations historiques détaillées sur les événements de verrouillage.

Rapport d'état de la passerelle en ligne
Détails sur les passerelles actuelles.

Rapport d'état du point d'accès en ligne
Détails sur les passerelles actuelles et les points d'accès assignés.

Rapport des accès du personnel
Répertorie les informations historiques sur l'accès du personnel.

Rapport du point d'accès assigné et en ligne
Répertorie les points d'accès assignés à une passerelle.

Rapport sur l'activité système
Détails sur l'historique des transactions du système.

Rapport sur la configuration des ascenseurs
Informations détaillées sur un groupe d'ascenseurs, y compris les ascenseurs et la cartographie des relais-étages pour chaque carte relais.

Rapport sur la configuration du site
Détails sur la configuration du point d'accès pour le site.

Rapport sur les attributions des clés/utilisateurs
Liste des clés actives attribuées à un porteur de clé donné.

Rapport sur les attributions des identifiants/points d'accès
Liste des identifiants et des points d'accès attribués ou une liste des points d'accès et des identifiants attribués.

Rapport sur les expirations de clés
Répertorie la date d'expiration des clés actives.

Rapport sur les opérateurs
Répertorie les opérateurs, les rôles qui leur sont attribués et les droits associés à chaque rôle.

Rapport sur les rôles et droits
Répertorie les rôles définis dans le module Gestion des rôles et les fonctions Community pour lesquelles chaque rôle possède des droits.

Rapports
Module dans lequel vous pouvez suivre, examiner et tenir à jour des dossiers actuels et historiques sur tout aspect de votre site.

Résident
Personne ajoutée dans le module Gestion des résidents aux fins d'affectation des unités et/ou de l'accès aux espaces communs.

RFID
Identification par radiofréquence. Technologie qui prend en charge les clés sans contact.

Rôle
Un groupe de droits attribués à un opérateur.

S

Site
Lieu géographique composé d'un ou de plusieurs bâtiments.

Suite
Une série d'unités communicantes comprenant une porte commune et une ou plusieurs unités de suite.

Surveillance
Module dans lequel vous pouvez visualiser une liste de toutes les clés créées par Community. Lorsque la communication en ligne est activée, vous pouvez également consulter les indicateurs, les opérations, les événements et l'état des points d'accès en ligne.

T

Type d'utilisateur (profil d'opérateur)
Option sélectionnée dans les profils des membres du personnel qui reflète la nature du rapport avec l'établissement.

Type de catégorie d'identifiants
Un ensemble fixe de propriétés d'accès dont proviennent toutes les catégories d'identifiants.

Type de point d'accès (Community)
Classification fonctionnelle d'un point d'accès. Les types de points d'accès dans Community comprennent les unités, les suites, les portes de foyer, les espaces communs pour les résidents et pour le personnel, les accès privés et les lecteurs d'ascenseurs.

U

Unité
Type de points d'accès affecté à un résident.

Index

A

accès aux étages dans les profils des résidents 20
accès aux modules Community 10, 124
accès prédéfini 91, 187
accès privés, ajout 82
accès résident partagé 148
accès résident, partagé 148
accès variable 91, 187
activation des clés mobiles 47, 290
activer
    résidents 176
activer l'accès résident 164
activer le personnel/les prestataires 217
affectation des unités 154, 164
affichage de la langue 19, 275
Affichage des unités 147
ajout
    accès privés 82
    ascenseurs 84
    bâtiments 58
    encodeurs 114
    espaces communs pour le personnel 76
    espaces communs pour les résidents 70
    étages 59
    groupes de notification 315

groupes de points d'accès 100
horaires 93, 95, 98
identifiants 102
opérateurs 131
résidents 150
rôles personnalisés de l'opérateur 127
suites 66
unités 62
ajouter
personnel/prestataires 189
résidents 142
API REST 44
application mobile, BlueSky 294
archivage des données historiques 40
ascenseurs 55, 84, 262
attribution d'horaires 106
attribution de l'accès aux visiteurs 146
attribution des clés mobiles 146
attribution du code PIN 146
audit des serrures 120, 223
Aurora, Keyscan 49
Authentification API 23
authentification unique 28

B

base de données, sauvegarde 37
bâtiments 58
Bloquer/Débloquer l'accès de l'opérateur 214
BlueSky, dormakaba 294

C

catégories d'identifiants 89, 187, 193, 196, 199, 204, 208
clé d'activation 50

Clé d'appairage RF 251
clé d'audit 251
Clé de désappairage RF 251
clé, activation 50
clés
accès aux espaces communs uniquement 180
Annulation 242
bascule 91
Blocage/Déblocage 230
Clés d'annulation 234
Diagnostic 237
effacement 281-282
état 289, 291, 293
Fonction spéciale 251
invalider l'accès des résidents 170
invalider l'accès du personnel/prestataire 214
lecture 281
messages d'avertissement 20
mobiles 290
mode de la clé 288
option d'ouverture forcée du pêne dormant pour les résidents 20
perdues 170
personnel/prestataire 129
physiques 288
Programmation primaire/secondaire 246
rapport sur les expirations 263
remplacement de la clé du personnel/prestataire 212
Reséquence 249
résident 20, 145, 161
Sécurité intégrée 33
Système 226
type RFID 46
Utilisation maximale pour les clés à usage restreint 32
Verrouillage électronique 239, 241
Verrouillage/déverrouillage 244

Clés à fonction spéciale 251
Clés à sécurité intégrée 33
Clés d'annulation 234, 242
Clés d'annulation (accès résident) 172
Clés de bascule de verrouillage électronique 239, 241
Clés de blocage/déblocage 230
Clés de diagnostic 237
Clés de programmation primaire 246
Clés de programmation secondaire 246
Clés de reséquence 249
clés de résidents perdues 170
Clés de verrouillage/déverrouillage 244
clés ELO 239, 241
clés mobiles 47, 145, 290
clés obsolètes 226
clés physiques 288
clés supplémentaires 288
Clés Système 226
clés, réutilisation des ID 195, 198, 203, 207, 211
client, Community 277, 279
codes de couleur, points d'accès 118
common areas, limited access 182
communication en ligne 49, 251, 296
Configurateur de site 52
  rapports 262, 266
configuration
  accès aux espaces communs 107
  encodeurs 114
  Opérateurs 131
  rôles personnalisés de l'opérateur 127
configuration du site 13
création de clés mobiles pour plusieurs résidents 145
création de lots de points d'accès 52

D

dérive temporelle 118
désactivation
    personnel/prestataires 217
    résidents 173
désactiver l'accès résident 164
droits de clé 124
droits système 124

E

échecs, lecture et encodage de clés 282
effacer les clés 282
encodeurs 112, 114, 278, 335
espaces communs à accès limité 92, 107, 180
espaces communs étendus 47
espaces communs pour le personnel
    ajout 76
espaces communs pour les résidents 54
Espaces communs pour les résidents
    ajout 70
espaces communs, accès limité 91-92, 107, 180
espaces communs, étendus 47
étages, ajout 59
état, clés 289, 293

F

Favoris de la page d'accueil 273
flux de travail, configuration du site 13
format de l'heure 19
format de la date 19
fuseau horaire 19

G

Gestion des accès 89
Gestion des périphériques 112
Gestion des résidents 142
Gestion des rôles 124, 126
gestion des visiteurs
  personnel 129, 187, 219
  résidents 146, 184
Gestion du personnel/prestataire 129
Grand Maître (types de catégories d'identifiants/catégories) 193, 196, 199, 204, 208
groupement de points d'accès 100
groupes de notification 313

H

horaires
  accès 95
  attribution aux points d'accès 106
  clés du personnel 98
  libre passage 93
Horaires d'accès 95
horaires d'accès 106
horaires de libre passage 93, 106
horaires des clés du personnel 98

I

identifiants
  ajout 102
  catégorie d'identifiants résident 91
  catégories clé système 91
  catégories personnel/prestataire 89
  en savoir plus 89
  groupes de points d'accès 100

horaires des clés du personnel 98
rapport sur les attributions 261
importation des membres du personnel/prestataires 136, 191
importation des profils de résidents 152
invalider l'accès 230, 234, 239, 241-242
personnel/prestataires 214
résidents 170

J

Journaux 345

K

Key/User Assignment Report 264
keys
common area access only 182
user assignment report 264
Keyscan Aurora 49

L

LEGIC 47, 290
licences 50
limited access common areas 182
Lire la clé 281

M

Maître (types de catégories d'identifiants/catégories) 193, 196, 199, 204, 208
Mifare (Classic/Plus) 47
mise à jour du client Community 277, 279
mise à jour du firmware de l'encodeur 115
mise à jour du firmware, encodeur 115
mode bascule 91
mode passage 93, 244

modules de navigation 273
mot de passe
  changement 275
  paramètres de sécurité 21

N

noms des points d'accès 52
Nouvelles clés 288

O

Opérateurs
  bloquer/débloquer l'accès 214
  configuration 131
  rôles 124
option d'ouverture forcée du pêne dormant pour les clés de résidents 20
ouverture forcée pour la validation du numéro de téléphone portable/téléphone 19
ouverture forcée pour la validation, numéro de téléphone portable/téléphone 19

P

paramètres de sécurité 21
Paramètres du système 15
personnel
  création de clés 193, 196, 199, 204, 208
  e-mail automatique 313
Personnel (types de catégories d'identifiants/catégories) 90, 187
Personnel à usage restreint (types de catégories d'identifiants/catégories) 193, 196, 199, 204, 208
personnel/prestataires
  activer 217
  ajouter des profils 189
  clés 129
  désactiver 217
  e-mail automatique 36
  gestion des visiteurs 129, 187, 219

horaires des clés du personnel 98
importation 136, 191
invalider l'accès 214
remplacement de la clé 212
plan d'étage, ascenseur 55
plusieurs clés mobiles 145
point d'accès
attribution horaire 106
groupes 100
rapport compatible accès mobile 291
types 52
possible(s) porteur(s) de clé 195, 198, 203, 207, 211
poste de travail, Community 277, 279
préférences de l'utilisateur 275
préférences du compte 275
Prestataire (types de catégories d'identifiants/catégories) 90
profil
accès aux espaces communs 107
Opérateur 129
personnel/prestataire 129
résident 142
profil de l'opérateur 131
Programmateur M-Unit 23, 121, 221, 223
programmation de périphériques 120
programmation de serrures 121, 221
programmation des serrures 118

R

Rapport d'audit 259
Rapport d'audit de point d'accès 259
rapport des accès des résidents 283
Rapport des accès du personnel/prestataire 268
rapport des accès du personnel/prestataire 283
rapport des accès, résidents/personnel/prestataires 283

Rapport sur l'activité système 269
Rapport sur la configuration des ascenseurs 262
Rapport sur la configuration du site 266
Rapport sur les attributions des identifiants/points d'accès 261
Rapport sur les expirations de clés 263
Rapport sur les opérateurs 265
Rapport sur les rôles et droits 267
Rapports
Accès du personnel/prestataire 268
Accès résident/personnel/prestataire 283
Activité système 269
Attribution des identifiants/points d'accès 261
Audit de point d'accès 259
Configuration du site 266
État de la passerelle en ligne 328
État des points d'accès assignés et en ligne 329
Opérateur 265
points d'accès compatibles accès mobile 291
Rapport sur la configuration des ascenseurs 262
Rapport sur les expirations de clés 263
Rôles (Opérateur) et droits 267
rapports en ligne 328-329
remplacement de la clé du personnel/prestataire 212
Reports
Key/User Assignment 264
résidents
accès partagé 155
activer 176
affectation des unités 154
affecter les unités 142
ajout 150
ajouter 142
création de clés 161
créer des clés 142
désactivation 173

gestion des visiteurs 146, 184
importation des profils 152
invalider l'accès 142, 170
modifier l'accès 164
supprimer 175
réutilisation des ID de la clé 195, 198, 203, 207, 211
rôle d'administrateur 124
rôle d'agent de location 124
rôle de configurateur de site 124
rôle de l'administrateur 126
Rôle de l'agent de location 126
rôle de superviseur de maintenance 124
rôle de technicien de maintenance 124
rôle du configurateur de site 126
Rôle du superviseur de maintenance 126
Rôle du technicien de maintenance 126
rôles de l'opérateur
personnalisé 127
rôles des opérateurs
prédéfini 126
rôles personnalisés de l'opérateur 127
Rôles, Opérateur 127

S

sauvegarde de la base de données 37
sauvegardes du serveur distant 37
séquence de clés 226
séquence de clignotement LED (serrures) 339
serrures
audit 223
dépannage 237, 339
programmation 118
séquences de clignotement LED 339
suites, ajout 66

suivre les clés numériques 256
supprimer des résidents 175
supprimer l'accès résident 164
surveiller les clés 255-256
suspendre l'accès 230
système d'accès, tiers 43

T

téléchargement de fichiers sur les points d'accès compatibles accès mobile 291
types de catégories d'identifiants 89, 187, 193, 196, 199, 204, 208
types de clés RFID 46
types, point d'accès 52

U

Ultralight C 47
unités
  affectation aux résidents 147, 154
  modifier l'accès résident 164
unités, ajout 62
Urgence (types de catégories d'identifiants/catégories) 90, 187, 193, 196, 199, 204, 208
Usage restreint (types de catégories d'identifiants/catégories) 90, 187

PK3706-FR 2.6 - 08/2026
Copyright © dormakaba 2026

www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montréal, Québec, H4N 2M3
Canada
T: +1 877 468-3555

www.dormakaba.com