CLIQ® Web Manager

Guide de l'utilisateur

IKON
ASSA ABLOY

assaabloy.com

Experience a safer
and more open world

ASSA ABLOY is committed to operating in compliance with data laws globally across its various divisions. The EU General Data Protection Regulation ("GDPR") requires us to meet principles of fairness, accountability and transparency in handling personal data.

ASSA ABLOY has a focused, structural and systemic approach to data protection and privacy. Our globally applicable ASSA ABLOY Data Protection Compliance Program has been developed to protect the integrity of the personal data of our employees, customers and partners worldwide. ASSA ABLOY has dedicated resources across the Group whose continual focus is the compliance with data laws globally including the GDPR.

We keep personal data secure using equipment operating in accordance with recognized security standards. In cases where the rights of individuals are at risk, we conduct impact assessments in accordance with our standard methodology.

We recognize that data laws are continuously evolving. ASSA ABLOY has invested considerable resources in raising awareness and rolling out training in relation to its Data Protection Compliance Program. We continuously monitor data protection developments to ensure our policies, processes and procedures are relevant and adequate.

We are committed to ensuring good data governance and are invested in data trust and security for the long-term.

ASSA ABLOY
Sicherheitstechnik GmbH

Attilastrasse 61-67
12105 Berlin
ALLEMAGNE
Tél. : + 49 30 8106-0
Télécopie : + 49 30 8106-26 00
berlin@assaabloy.com

www.assaabloy.de

Program version: V 2025.1
Main document number: D001583864
Date published: 2025-05-22
Language: fr-FR

1 Présentation

1.1 Introduction

CLIQ Web Manager (CWM) est un système logiciel Web de gestion et de commande de CLIQ, un système de fermeture électromécanique prenant en charge le contrôle total des autorisations d'accès et des activités des utilisateurs de clé. Le système CLIQ offre une solution permettant d'assurer la fiabilité des clés et des cylindres mécaniques tout en garantissant la sécurité et la flexibilité inhérentes aux serrures électroniques.

1.2 Principales caractéristiques

- **Installation aisée** - CLIQ est un système hors ligne économique ne nécessitant aucun câblage électrique ou batterie pour cylindre.
- **Journaux des événements** - CLIQ offre un accès direct aux données de journal des événements de tous les cylindres et clés du système de fermeture.
- **Clés individuelles** - Protégée par une clé de chiffrement forte, chaque clé est conçue pour être utilisée par un utilisateur unique. Si la clé est perdue, elle est simplement rendue obsolète et une nouvelle clé est générée à sa place.
- **Permission selon horaire** - L'accès est autorisé uniquement pendant les créneaux horaires du planning.
- **Gestion des clés** - CLIQ Web Manager assure le suivi des problèmes de clés pour les différents possesseurs de clés.
- **Annulation électronique de clé** - Les clés peuvent être annulées sans la présence physique de la clé.
- **Revalidation des autorisations** - Renforce la sécurité du système de fermeture en obligeant les possesseurs de clés à effectuer des mises à jour de permission depuis un boîtier de programmation proche. Elle permet également de s'assurer que le journal des événements est chargé sur le serveur et mis à disposition des administrateurs du système de fermeture.
- **Fonctions de groupement** pour une administration facilitée. CLIQ Web Manager permet de réserver l'accès à des groupes de cylindres et des groupes de personnes en fonction, par exemple, de leur situation géographique ou de leur rôle dans l'organisation.

1.3 À propos de ce Guide

Table des matières du guide
Ce guide comprend les parties suivantes, destinées à différents groupes cibles :

Chapitre	Pour les administrateurs	Pour les super administrateurs	Description
1 Présentation	✓	✓	Introduction rapide à CLIQ et à ce guide.
2 Réglages des clients CWM	✓	✓	Décrit comment installer un client CWM.
3 Démarrer avec CWM	✓	✓	Décrit comment commencer à travailler avec CWM pour la première fois.
4 Utiliser CWM	✓	✓	Détaille comment exécuter l'ensemble des tâches pertinentes pour les administrateurs dans le cadre de l'utilisation d'un système de fermeture.
5 Réglages de systèmes de fermeture		✓	Décrit comment installer un nouveau système de fermeture.
6 Configuration des systèmes de fermeture		✓	Décrit comment configurer différents paramètres d'un système de fermeture.
7 Matériel CLIQ	✓	✓	Décrit l'architecture de CLIQ et ses composantes.
8 Concepts et caractéristiques CLIQ	✓	✓	Décrit le fonctionnement des autorisations et les notions de fonctions CWM. Certaines notions sont très techniques et exclusivement destinées aux super administrateurs.
9 Annexe	✓	✓	Contient des informations de référence.

Terminologie
Pour la définition des termes et abréviations utilisés dans ce guide, voir *Chapitre 9.1.1 "Termes", page 198* et *Chapitre 9.1.2 "Abréviations", page 199*.

Les options de menu apparaissent dans CWM comme **Menu principal » Option de menu**.

Les noms de clé suivants diffèrent des noms utilisés dans CWM ainsi que dans ce guide :

Nom de clé	Nom dans CWM et dans ce guide
E1	Clé normale
E2	Clé standard
E3	Clé dynamique

2 Réglages des clients CWM

2.1 Présentation de la configuration des clients CWM

1) Installez le programmateur local.

   Voir *Chapitre 2.2 "Installation des programmateurs à distance", page 13*.

2) Installer CLIQ Connect PC.

   Voir *Chapitre 2.3 "Installation de CLIQ Connect PC", page 13*.

3) Configurer CLIQ Connect PC.

   Voir *Chapitre 2.4 "Configuration de CLIQ Connect PC", page 14*.

2.2 Installation des programmateurs à distance

1) Vérifiez que le compte utilisateur Windows actuellement connecté dispose de droits d'accès Administrateur.
2) Connectez le câble USB du programmateur local au PC.
3) Vérifiez que les pilotes sont téléchargés et installés automatiquement.

> **REMARQUE !**
> Notez le port COM attribué affiché dans la zone de notification. Lorsque vous vous connectez à CLIQ Express ou à CLIQ Go App, sélectionnez le port COM attribué si le port COM n'est pas trouvé automatiquement.
>
> Exemple : `STMicroelectronics Virtual Port COM (COM7)`.

4) Si les pilotes ne sont pas installés automatiquement, contactez le support technique.

2.3 Installation de CLIQ Connect PC

CLIQ Connect PC est un logiciel qui gère la communication entre le boîtier de programmation local et CLIQ Web Manager et génère également les certificats de clé de programmation.

Conditions préalables :

- Le compte utilisateur Windows actuellement connecté dispose de droits d'accès Administrateur
- La clé de programmation a déjà été remise et l'utilisateur a reçu un e-mail de CLIQ Web Manager.

1) Téléchargez et lancez le fichier d'installation de CLIQ Connect PC.

   Vous trouverez le lien vers le fichier aux emplacements suivants :

   - L'e-mail de CLIQ Web Manager
   - La page d'identification CWM
   - La page d'accueil pour l'enregistrement

2) Une fois le programme d'installation téléchargé, sélectionnez **langue** et cliquez sur **OK**.

   L'assistant d'installation de CLIQ Connect s'ouvre.

3) Cliquez sur **Suivant**.

4) Lisez les conditions d'utilisation. Si vous acceptez ces conditions, cochez le bouton radio **J'accepte l'accord** (cette action est nécessaire pour permettre à l'assistant d'installation de poursuivre la procédure) puis cliquez sur **Suivant**.

   REMARQUE !
   Lisez l'**Accord de licence** avec attention.

5) Exécutez l'une des opérations suivantes :

   - Pour installer CLIQ Connect PC pour la première fois : Sélectionnez directement la destination et cliquez sur **Suivant**.
   - Pour mettre à jour une installation existante : Sélectionnez **Oui** pour mettre à jour l'installation existante ou **Non** pour installer dans un répertoire différent. Puis cliquez sur **Suivant** pour continuer.

6) Définissez les services externes suivants :

   - **Activer les mises à jour automatiques** permet à CLIQ Connect PC de télécharger et d'installer automatiquement la dernière version du logiciel CLIQ Connect PC.
   - Désélectionnez **CLIQ Go** et sélectionnez **CLIQ Web Manager (Clé de programmation)**.

   REMARQUE !
   Les deux paramètres ci-dessus ne peuvent pas être modifiés après le processus d'installation ou de mise à jour.

   - **Intégration au Directory Service** permet à CLIQ Connect PC d'obtenir automatiquement les détails de la connexion à CLIQ Remote à partir du serveur Service Directory. Si le CLIQ Connect PC ne doit se connecter à aucun service externe, désélectionnez **Intégration au Directory Service**. Dans ce cas, **URL CLIQ Remote** et **URL CLIQ Enrolment** doivent être spécifiés manuellement.

7) Cliquez sur **Suivant** pour continuer.

8) Pour installer CLIQ Connect PC pour la première fois :

   Sélectionnez ou créez un **Dossier de menu de démarrage** pour placer les raccourcis de programme et cliquez sur **Suivant** pour continuer.

9) Patientez pendant l'extraction et l'installation des fichiers.

10) Choisissez d'exécuter le programme ou ne de pas l'exécuter à la fin de la configuration.

11) Cliquez sur **Terminer** pour quitter la configuration.

2.4 Configuration de CLIQ Connect PC

2.4.1 Configuration de CLIQ Connect PC COM Sélecteur

1) Cliquez à droite sur l'icône **CLIQ Connect** de la barre d'état système.
2) Cliquez sur **Sélecteur COM**.
3) Sélectionnez le port COM où le programmateur local est connecté ou cliquez sur **Auto** (défaut) pour la sélection automatique du port COM.

2.4.2 Configuration de CLIQ Connect PC Server Configuration

1) Cliquez à droite sur l'icône **CLIQ Connect** de la barre d'état système.
2) Cliquez sur **Configuration** et trouvez la section **Configuration du serveur** .
3) Si l'intégration du serveur Service Directory est activée :
   a) Sélectionnez **Automatiquement**.
   b) Entrez le **Répertoire URL**.
4) Si l'intégration du serveur Service Directory n'est **pas** activée :
   a) Sélectionnez **Manuelle**.
   b) Entrez **URL CLIQ Remote** et **URL CLIQ Enrolment**.
5) Cliquez sur **OK** pour enregistrer et quitter.

2.4.3 Configuration des réglages proxy CLIQ Connect PC

1) Cliquez à droite sur l'icône **CLIQ Connect** de la barre d'état système.
2) Cliquez sur **Configuration**.
3) Pour **Proxy**, sélectionnez **Activer**.
4) Entrez les informations requises et cliquez sur **OK**.

3 Démarrer avec CWM

3.1 Présentation du démarrage avec CWM

Pour les nouveaux administrateurs : Exécutez les étapes suivantes pour pouvoir utiliser CWM.

Conditions préalables :

- CWM est installé et configuré.
- Une clé de programmation, un certificat de clé de programmation et le code PIN de la clé de programmation sont disponibles.

1) Installez le certificat de la clé de programmation.

   Voir *Chapitre 3.2 "Enregistrement et installation des certificats de la clé de programmation", page 16*.

2) Connectez-vous à CWM.

   Voir *Chapitre 3.3 "Connexion", page 18*.

3) Définissez la langue de CWM.

   Voir *Chapitre 3.4 "Réglage de la langue CWM", page 19*.

4) Lisez la *Chapitre 3.5 "Introduction à l'interface utilisateur de CWM", page 19*.

Les tâches les plus courantes lorsque vous travaillez avec CWM sont listées dans *Chapitre 3.6 "Tâches courantes", page 23*.

3.2 Enregistrement et installation des certificats de la clé de programmation

Pour utiliser une clé de programmation avec CWM, un certificat unique doit être installé sur le client CWM.

La procédure d'installation d'un certificat diffère selon que vous utilisez ou non **l'intégration DCS**.

Installation de certificat avec Intégration DCS
La clé de programmation est enregistrée et son certificat est généré directement dans le navigateur Internet. Il n'est pas nécessaire d'obtenir le certificat séparément.

Pour plus d'informations, consultez *Chapitre 3.2.1 "Enregistrement du certificat de la clé de programmation via CLIQ Connect PC", page 17*.

Installation manuelle du certificat
Pour installer le certificat de clé de programmation manuellement, vous devez disposer d'un fichier de certificat.

Pour plus d'informations, consultez *Chapitre 3.2.2 "Installation manuelle du certificat de clé de programmation", page 17*.

3.2.1 Enregistrement du certificat de la clé de programmation via CLIQ Connect PC

Conditions préalables :

- Le boîtier de programmation local est installé.
- Le logiciel CLIQ Connect PC est installé sur l'ordinateur.

  Voir *Chapitre 2.3 "Installation de CLIQ Connect PC", page 13*.
- La clé de programmation est remise dans CWM.
- L'enregistrement de la clé de programmation est autorisé.

  Normalement, une clé de programmation ne peut être enregistrée qu'une fois, mais ce réglage peut être modifié par un administrateur disposant des autorisations adéquates. Pour plus d'informations, consultez *Chapitre 6.11.4 "Modification des informations de clé de programmation", page 137*.
- La clé de programmation et le code PIN de la clé de programmation sont disponibles.

1) Insérez la clé de programmation dans la fente gauche du boîtier de programmation local.
2) Faites un clic droit sur l'icône CLIQ Connect dans la barre d'état système et sélectionnez **Démarrer l'enregistrement du certificat**.
3) Saisissez le code PIN de la clé de programmation et cliquez sur **Suivant**.

   Si le code PIN saisi est vérifié, le mot de passe temporaire est envoyé à l'adresse e-mail de l'utilisateur de la clé de programmation.
4) Entrez le mot de passe temporaire et cliquez sur **Suivant**.

   Le certificat de la clé de programmation est créé et ajouté automatiquement aux navigateurs Internet.
5) Cliquez sur **Effectué** pour terminer l'enregistrement de la clé de programmation.

3.2.2 Installation manuelle du certificat de clé de programmation

Condition préalable :

- Un fichier **.p12** pour la clé de programmation et un mot de passe ont été obtenus.

1) Effectuez un double-clic sur le fichier **.p12**.

   L'**Assistant d'importation de certificat** s'affiche.
2) Sélectionnez **Utilisateur actuel** et cliquez sur **Suivant**.
3) Vérifiez si le bon certificat est sélectionné et cliquez sur **Suivant**.
4) Entrez le mot de passe fourni avec le fichier **.p12** et cliquez sur **Suivant**.
5) Sélectionnez **Stockez tous les certificats dans l'emplacement suivant** et cliquez sur **Parcourir**.
6) Dans la fenêtre pop-up, sélectionnez **Personnel** et cliquez sur **Suivant**.
7) Confirmez le réglage et cliquez sur **Terminer**.

   Le certificat de la clé de programmation est installé dans les navigateurs Web pris en charge.

REMARQUE !
Le certificat de la clé de programmation doit être réinstallé si le mot de passe du compte utilisateur Windows est modifié par un administrateur. Cela n'est pas nécessaire lorsque les utilisateurs changent leur propre mot de passe.

3.2.3 Renouvellement de certificat de clé de programmation

Lorsque le délai d'expiration du certificat de la clé de programmation est inférieur ou égal à 60 jours, un message d'avertissement s'affiche après la connexion.

- **Avec l'intégration DCS activée** :

  Un e-mail contenant une brève description du mode de renouvellement du certificat est envoyé à l'utilisateur de la clé de programmation.

  Le certificat est renouvelé avec CLIQ Connect PC et le processus est le même que celui de l'enregistrement. Pour des informations détaillées, consultez *Chapitre 3.2.1 "Enregistrement du certificat de la clé de programmation via CLIQ Connect PC", page 17*.
- **Sans intégration DCS** :

  Le nouveau certificat est généré dans DCS et remis à l'utilisateur de la clé de programmation.

  Pour installer le nouveau certificat, voir *Chapitre 3.2.2 "Installation manuelle du certificat de clé de programmation", page 17*.

Conseil
Il est recommandé de supprimer l'ancien certificat du navigateur.

3.3 Connexion

Conditions préalables :

- Le boîtier de programmation local est installé. Voir *Chapitre 2.2 "Installation des programmateurs à distance", page 13*.
- Un navigateur Internet pris en charge est disponible. Voir *Chapitre 9.8 "PC client - Configuration requise", page 215*.
- Le logiciel CLIQ Connect est installé et en cours d'exécution sur l'ordinateur.

  Voir *Chapitre 2.3 "Installation de CLIQ Connect PC", page 13*.
- Le logiciel CLIQ Connect est configuré et connecté à CWM.

  Voir *Chapitre 2.4 "Configuration de CLIQ Connect PC", page 14*.

- Une clé de programmation avec son code PIN est disponible. La clé de programmation doit être également remise à un employé dans CWM.

  REMARQUE !
  Pour les systèmes avec authentification unique (SSO), une fois le certificat C-Key installé, la connexion peut se faire sans clé pour certaines opérations. Pour plus d'informations, consultez *Chapitre 8.10 "Authentification unique (SSO)", page 194*.

- Un certificat valide pour la clé de programmation est installé. Voir *Chapitre 3.2 "Enregistrement et installation des certificats de la clé de programmation", page 16*.
- Une URL vers CWM est disponible.

3.3.1 Connexion avec la clé de programmation

1) Insérez la clé de programmation dans la fente gauche du boîtier de programmation local.
2) Rendez-vous sur la page de démarrage CWM.
3) Sélectionnez le certificat de la clé de programmation.

   La page de connexion CWM est affichée.
4) Cliquez sur **Identification**.
5) Saisissez le code PIN de la clé de programmation.

   CLIQ Connect PC demande de confirmer l'utilisation de la clé.
6) Cliquez sur **Confirmation**.

3.3.2 Connexion sans la clé de programmation

1) Rendez-vous sur la page de démarrage CWM.
2) Sélectionnez le certificat de la clé de programmation.

   La page d'identification CWM est affichée.
3) Cliquez sur **Identification SSO**.

   Dans la plupart des cas, l'authentification automatique se produit lorsque votre navigateur est déjà connecté avec les identifiants du domaine de l'entreprise, ce qui permet d'accéder directement à CWM, sans autre action.

   Sinon, la fenêtre de connexion du fournisseur d'identifiants s'affiche.

3.4 Réglage de la langue CWM

1) Sélectionnez **Réglages » Sélectionner langue**.
2) Sélectionnez la langue désirée.

La langue peut aussi être sélectionnée en cliquant sur l'icône drapeau correspondante dans la fenêtre de connexion.

3.5 Introduction à l'interface utilisateur de CWM

3.5.1 Menus principaux

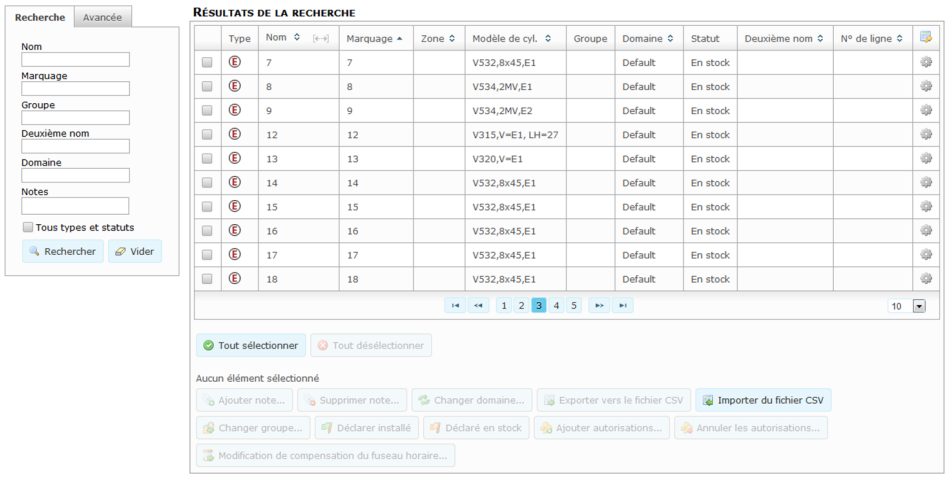
Les options CWM sont divisées en quatre menus principaux :

Tâches	Ce menu comporte les fonctions les plus utilisées quotidiennement.
Informations système	Ce menu comporte les fonctions permettant de gérer les droits d'accès, les informations sur les employés et les visiteurs, les clés, les cylindres et les boîtiers de programmation à distance.
Administration	Ce menu concerne les fonctions permettant de régler et de configurer le système de fermeture.
Réglages	Ce menu comporte les réglages personnels de l'administrateur connecté.

3.5.2 Recherche d'objets

Utilisez d'abord les critères de recherche par défaut
Pour rechercher des objets, tels que des cylindres ou des clés, sélectionnez d'abord l'option correspondante dans le menu, par exemple, **Informations système » Cylindres**.

Le résultat de recherche initialement affiché est basé sur les critères de recherche par défaut.



Ensuite, utilisez les options de recherche suivantes

Critère de recherche	Pour régler le critère de recherche, saisissez un nouveau critère dans la zone de recherche à gauche et cliquez sur **Rechercher**. Dans l'onglet **Avancée** sont proposées des options de recherche moins courantes.
Caractères génériques	Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».
Notes	En tapant **Notes** dans le champ de recherche, toutes les notes correspondantes apparaîtront sous forme d'une liste à sélectionner.
Lignes par page	Utilisez les flèches se trouvant en dessous des résultats de recherche pour naviguer parmi les pages, lorsque les résultats sont nombreux. Le nombre de lignes affichées par page peut être réglé dans la liste déroulante **Lignes par page**.

Trier		Cliquez sur ce symbole pour trier les résultats de recherche en fonction de la colonne correspondante.
		Les résultats de recherche sont triés en fonction de cette colonne (ordre ascendant).
		Les résultats de recherche sont triés en fonction de cette colonne (ordre descendant).
Élargir une colonne		Cliquez sur ce symbole pour élargir les colonnes lorsque des données sont trop longues.

Pour afficher les informations détaillées de l'objet et pour configurer cet objet individuellement, cliquez sur la ligne de l'objet.

3.5.3 Configuration de plusieurs objets simultanément

Certaines opérations peuvent être exécutées sur plusieurs objets en même temps. Les opérations disponibles dépendent du type d'objet.

Pour configurer plusieurs objets simultanément :

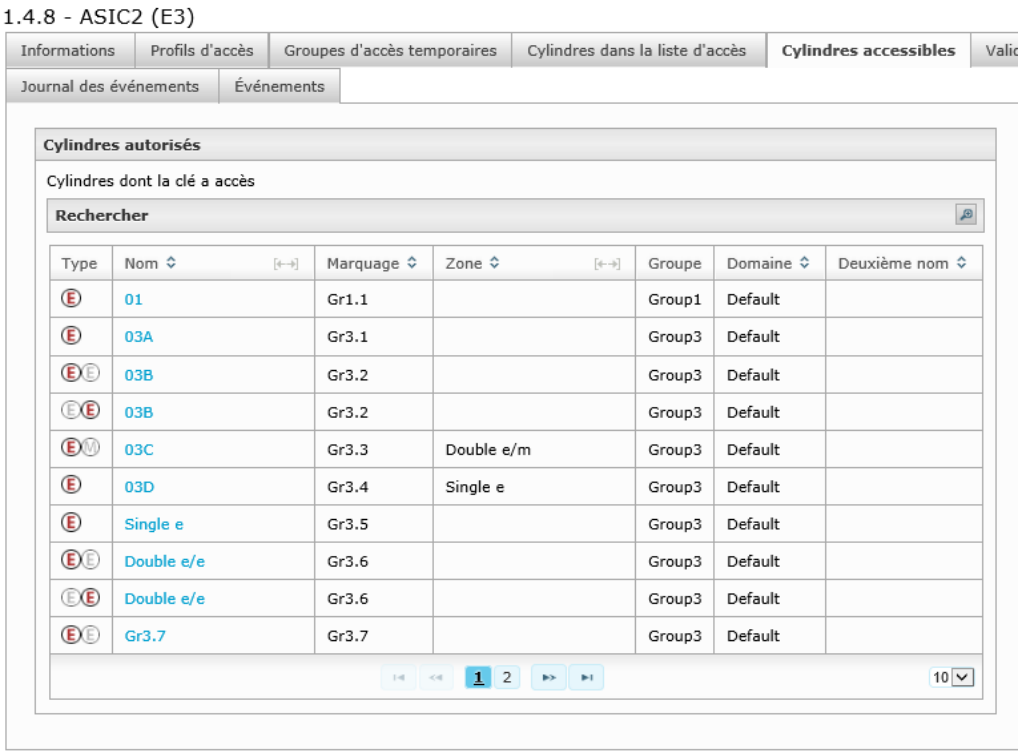
1) Sélectionnez plusieurs objets individuels dans la colonne la plus à gauche d'une ou de plusieurs pages de résultats de la recherche.

   Cliquez **Tout sélectionner** pour sélectionner tous les objets de toutes les pages de résultats de recherche.

2) Cliquez sur le bouton correspondant en bas de la fenêtre de résultats de recherche pour lancer l'opération sur les objets sélectionnés.

3.5.4 Filtrer des listes longues

Dans les aperçus des listes d'accès de cylindres ou de clés par exemple, une bannière **Rechercher** s'affiche. Voir l'exemple ci-dessous.



Cliquer sur le symbole  ouvre une boîte de critères de recherche.

3.5.5 Accessibilité

3.5.5.1 Accessibilité clavier

La navigation au clavier est supportée dans CWM pour les utilisateurs qui ne peuvent pas se servir d'une souris ou d'autres dispositifs de pointage ou qui préfèrent utiliser le clavier.

Interaction	Combinaisons de touches	Remarques
Naviguer entre la plupart des éléments	• **Tab** • **Maj** + **Tab** (reculer)	
Boutons	• **Entrée** ou **Barre Espace**	
Cases à cocher	• **Barre Espace**	Cocher/décocher une case à cocher.
Zones combinées	• **Barre Espace** (Facultatif. Ouvrir la liste des valeurs.) • **Haut**/**Bas** ou **Gauche**/**Droite**	Sélectionner une valeur à l'aide des touches fléchées (**Haut**/**Bas** ou **Gauche**/**Droite**), puis accepter avec **Entrée**.
Tableaux	• **Haut**/**Bas** (Déplacement dans les cellules d'un tableau) • **Entrée** (entrer et afficher les informations détaillées)	Déplacement dans les cellules du tableau avec les touches fléchées (**Haut**/**Bas**).
Boutons radio	• **Haut**/**Bas** ou **Gauche**/**Droite**	Sélectionnez une option à l'aide des touches fléchées (**Haut**/**Bas** ou **Gauche**/**Droite**), puis allez vers l'élément suivant avec **Tab**.
Menu principal	• **Gauche**/**Droite** (Déplacement dans les options du menu principal) • **Haut**/**Bas** (Développer/réduire les options de sous menu) • **Entrée** (Accéder aux options de sous menu)	Déplacement entre les options du menu principal et des sous-menus, avec les touches fléchées (**Haut**/**Bas** ou **Gauche**/**Droite**).
Affichage page	• **Page précédente** et **Page suivante**	Faire défiler la page web vers le haut et vers le bas.
Flux de travail	• **Alt** + **Gauche**/**Droite** • **Alt** + **Q** • **Alt** + **Retour**	Naviguer entre les étapes. Annuler le flux de travail. Confirmer la dernière étape.
Éditeur de texte	• **Alt** + **Q**	Quitter l'éditeur de texte.

3.5.5.2 Modes de visualisation

Mode Contraste élevé
CWM prend en charge le mode de contraste élevé.

Zoom 200 % en résolution 1024x768
Il est possible d'agrandir jusqu'à 200 % dans le navigateur sans perdre les fonctionnalités de l'interface utilisateur.

3.6 Tâches courantes

C'est une liste de certaines des tâches les plus courantes et où trouver les informations correspondantes.

Connexion
Chapitre 3.3 "Connexion", page 18

Personnel
Ajouter un employé ou un visiteur : *Chapitre 4.1.2 "Ajouter des Employés ou des Visiteurs", page 24*

Clés utilisateur
Remise de clés : *Chapitre 4.2.9 "Remise de clés utilisateur", page 39*

Réception de clés (Retour) : *Chapitre 4.2.10 "Réception de clés utilisateur (Retour)", page 44*

Lorsque des clés sont perdues : *Chapitre 4.2.12.2 "Signalement et blocage d'une clé utilisateur perdue", page 46*

Autorisations
Affichage des clés pouvant accéder à un cylindre ou à un groupe de cylindres : *Chapitre 3.6 "Tâches courantes", page 23*

Affichage des cylindres auxquels une clé ou un groupe de clés a accès : *Chapitre 4.8.2 "Affichage des clés avec accès aux cylindres ou aux groupes de cylindres", page 77*

Changer les autorisations d'une clé : *Chapitre 4.9.1 "Configuration des autorisations dans les clés", page 78*

Changer les autorisations d'un cylindre : *Chapitre 4.9.2 "Configuration des autorisations dans les cylindres", page 81*

Profils d'accès
Associer une clé ou une personne à un profil d'accès : *Chapitre 4.9.5 "Sélection des profils d'accès d'employés ou de visiteurs", page 84*

Changer les autorisations d'un profil d'accès : *Chapitre 4.9.4 "Configurer les autorisations de profil d'accès", page 83*

Journaux des événements
Consulter les clés ayant eu accès à un cylindre : *Chapitre 4.11.3 "Affichage des journaux des événements pour le cylindre", page 93*

Programmation
Programmer les cylindres : *Chapitre 4.4.13 "Programmation des cylindres", page 62*

4 Utiliser CWM

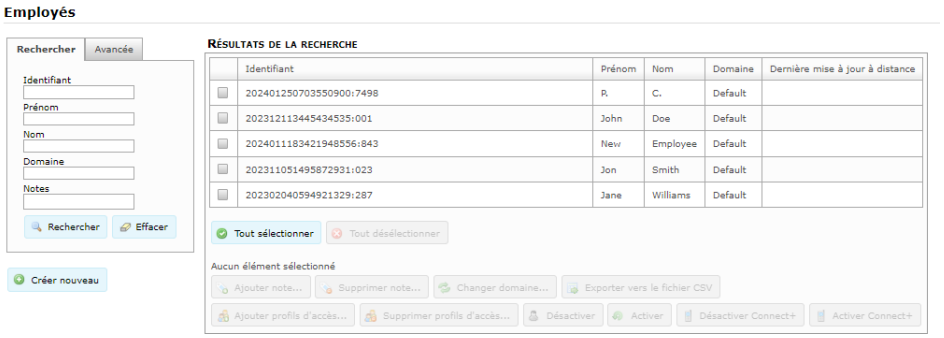
4.1 Gestion des Employés et des Visiteurs

4.1.1 Recherche d'employés ou de visiteurs

1) Sélectionnez **Informations système » Employés** ou **Visiteurs**.

   Une liste de tous les employés ou des visiteurs s'affiche.

   Si l'intégration LDAP est activée, CWM récupère automatiquement les dernières informations depuis le LDAP toutes les 24 heures. La date et l'heure de mise à jour sont affichées et les informations détaillées sont disponibles en cliquant sur **Afficher les détails**. Pour mettre à jour manuellement, cliquez sur **Mise à jour des employés LDAP**. Pour plus d'informations sur l'intégration LDAP, voir *Chapitre 8.12 "Intégration LDAP", page 195*.



2) Sélectionnez l'onglet **Rechercher** ou **Avancée**.

   L'onglet **Avancée** contient d'autres champs de recherche ainsi que la possibilité de rechercher les employés ou visiteurs supprimés ou désactivés, selon la façon dont CWM est configuré pour gérer les personnes supprimées. Voir *Chapitre 8.9 "Suppression des données personnelles et conformité RGPD", page 193* pour plus de détails.

3) Saisissez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

   En tapant **Notes** dans le champ de recherche, toutes les notes correspondantes apparaîtront sous forme d'une liste à sélectionner.

4) Cliquez sur **Rechercher**.

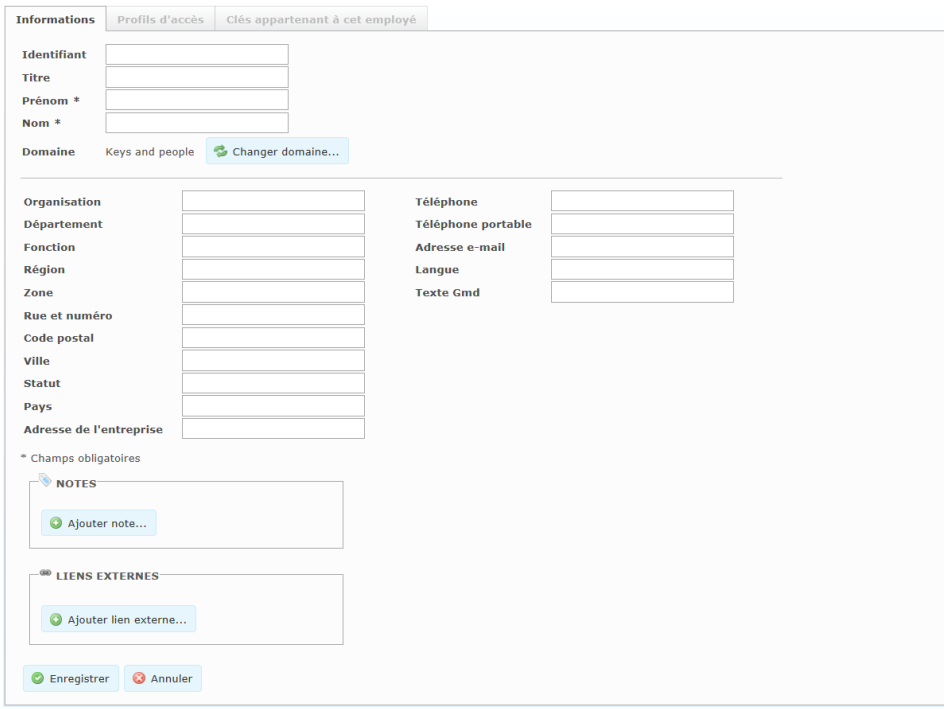
5) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur l'employé ou visiteur correspondant.

4.1.2 Ajouter des Employés ou des Visiteurs

> **REMARQUE !**
> Les informations sur les employés provenant du serveur LDAP sont disponibles en lecture seule. Les employés nouvellement créés dans CWM ne sont pas ajoutés au serveur LDAP.

1) Sélectionnez **Informations système » Employés** ou **Visiteurs**.

2) Cliquez sur **Créer nouveau**.



3) Saisissez les informations.

Prénom et **Nom** sont des champs obligatoires.

L'adresse **Adresse e-mail** est requise pour envoyer les rappels des clés périmées et pour l'utilisation de la fonction d'intégration DCS pour les nouveaux possesseurs de clé de programmation.

Si la fonction CLIQ Connect+ est activée pour le système et si elle est activée pour le nouvel employé ou pour un visiteur, l'adresse e-mail ne doit pas être la même que celle d'un autre utilisateur CLIQ Connect+.

Pour les employés, le champ **Identifiant** est également utilisé. L'identifiant doit être unique. Si le champ n'est pas renseigné, CWM ajoute un identifiant unique au format aaaa-mm-jj:numéro.

4) Pour ajouter une note, cliquez sur **Ajouter note...**. Voir également *Chapitre 4.1.7 "Ajout ou suppression de notes employés ou visiteurs", page 31*.

5) Pour ajouter un lien externe, cliquez sur **Ajouter lien externe...**. Voir également *Chapitre 4.1.8 "Gestion des liens externes employé ou visiteur", page 32*.

6) Cliquez sur **Enregistrer**.

4.1.3 Désactivation ou activation des employés ou des visiteurs

Conditions préalables :

- Pour la désactivation, mais aussi pour la recherche et la réactivation des employés ou des visiteurs désactivés, l'administrateur doit disposer des droits **Utilisateur de clé : Désactiver**.

  Pour plus d'informations sur la gestion des autorisations, voir *Chapitre 6.7 "Gestion des rôles et des autorisations", page 129*.
- Dans **Réglages du système**, **Supprimer de manière permanente** est sélectionné dans la section **Lors de la suppression d'une personne**.

  Pour plus d'informations sur la gestion de **Réglages du système**, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.
- Les employés ou visiteurs suivants ne peuvent pas être désactivés :
  - Employés ou visiteurs disposant de clés remises.
  - Employés intégrés avec le LDAP.
  - Utilisateurs de CLIQ Mobile Manager activés.

1) Sélectionnez **Informations système » Employés** ou **Informations système » Visiteurs**.

   Une liste de tous les employés ou des visiteurs s'affiche.

   Conseil
   Les employés ou visiteurs désactivés ou actifs peuvent être filtrés à l'aide du filtre **Afficher désactivé** de l'onglet **Avancée**.

   Si nécessaire, entrez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

   En tapant **Notes** dans le champ de recherche, toutes les notes correspondantes apparaîtront sous forme d'une liste à sélectionner.

   - Pour activer ou désactiver un employé ou un visiteur, allez à l'*Étape 2*.
   - Pour activer ou désactiver plusieurs employés ou visiteurs, allez à l'*Étape 3*.

2) **Activation ou désactivation d'un employé ou d'un visiteur**

   1. Sélectionnez l'employé ou le visiteur et accédez à ses informations détaillées.
   2. **Pour désactiver un employé ou un visiteur**

      a) Dans la fenêtre des informations, cliquez sur **Désactiver**.

      b) Dans la fenêtre pop-up, cliquez sur **Désactiver**.

      Pour activer un employé ou un visiteur

      a) Dans la fenêtre des informations, cliquez sur **Activer**.

b) Dans la fenêtre pop-up, cliquez sur **OK**.

3) **Activation ou désactivation de plusieurs employés ou visiteurs**

1. Sélectionnez les employés ou les visiteurs à activer ou désactiver dans les résultats de recherche en cochant les cases correspondantes.
2. **Pour désactiver des employés ou des visiteurs**

a) Cliquez sur **Désactiver** sous les résultats de recherche.

b) Dans la fenêtre pop-up, cliquez sur **Désactiver**.

Pour activer des employés ou des visiteurs

a) Cliquez sur **Activer** sous les résultats de recherche.

b) Dans la fenêtre pop-up, cliquez sur **OK**.

4.1.4 Suppression ou restauration des employés ou des visiteurs

Dans **Réglages du système**, la suppression d'employés ou de visiteurs peut être configurée sur **Marquer comme supprimé** ou **Supprimer de manière permanente**.

- Une fois que **Marquer comme supprimé** est sélectionné, les employés ou visiteurs supprimés peuvent être restaurés, le cas échéant.
- Lorsque **Supprimer de manière permanente** est sélectionné, les employés ou visiteurs supprimés ne peuvent **pas** être restaurés.

Voir également *Chapitre 6.4 "Modifier les réglages du système", page 100* et *Chapitre 8.9 "Suppression des données personnelles et conformité RGPD", page 193*.

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.

Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

Conseil
Les utilisateurs supprimés peuvent être filtrés à l'aide du filtre **Affichage supprimé** de l'onglet **Avancée**.

2) **Pour supprimer l'employé ou le visiteur :**

REMARQUE !
Les personnes suivantes ne peuvent pas être supprimées :

- Employés ou visiteurs disposant de clés remises.
- Employés intégrés par le LDAP.
- Utilisateurs CLIQ Connect+ activés.

1. Dans la fenêtre des informations détaillées, cliquez sur **Supprimer**.
2. Dans la fenêtre pop-up, cliquez sur **Supprimer**.

Pour restaurer l'employé ou le visiteur :

1. Dans la fenêtre des informations détaillées, cliquez sur **Restaurer**.
2. Dans la fenêtre pop-up, cliquez sur **Restaurer**.

4.1.5 Activation ou désactivation de l'accès à CLIQ Connect+ pour les Employés ou les Visiteurs.

Si CLIQ Connect+ est activé sur le système, les employés et les visiteurs peuvent afficher des informations détaillées sur leur clé dans CLIQ Connect. Pour utiliser cette fonction, l'administrateur doit activer le statut utilisateur CLIQ Connect+.

Il existe deux façons d'activer ou de désactiver le statut utilisateur :

- Pour modifier un seul statut, suivez les instructions en *Chapitre 4.1.5.1 "Configuration individuelle de l'accès à CLIQ Connect+", page 28*.
- Pour activer ou désactiver le statut de plusieurs employés ou visiteurs en même temps, suivez les instructions en *Chapitre 4.1.5.2 "Configurer l'accès à CLIQ Connect+ pour plusieurs employés", page 29*.

Pour plus d'informations sur CLIQ Connect+, voir *Chapitre 8.3.4 "CLIQ Connect et CLIQ Connect+", page 186*.

Conditions préalables :

- L'administrateur a récupéré et installé la licence **CLIQ Connect+**.

  Pour installer la nouvelle licence, voir *Chapitre 6.1.1 "Installation des licences", page 99*.
- L'adresse e-mail de l'employé ou du visiteur ne doit pas être une adresse appartenant à un autre utilisateur CLIQ Connect+.

4.1.5.1 Configuration individuelle de l'accès à CLIQ Connect+

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.

   Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

> **Conseil**
> Les utilisateurs désactivés ou supprimés peuvent être filtrés à l'aide du filtre de l'onglet **Avancée**.

2) Pour activer ou désactiver le statut utilisateur CLIQ Connect+ :

   Pour activer le statut utilisateur CLIQ Connect+ :
   Cliquez sur **Activer Connect+**.

> **REMARQUE !**
> Si l'adresse e-mail n'est pas entrée ou si elle est déjà utilisée par un autre employé ou visiteur ayant activé CLIQ Connect+, le bouton **Activer Connect+** est désactivé.
>
> Cliquez sur **Modifier** et entrez une seule adresse e-mail.

   Un e-mail contenant des informations sur la configuration de CLIQ Connect est envoyé à l'adresse spécifiée.

   L'administrateur peut également envoyer l'e-mail manuellement à un utilisateur CLIQ Connect+ en cliquant sur le bouton **Renvoyer l'e-mail**.

   - Si CLIQ Connect+ n'est pas activé par l'utilisateur de la clé, l'e-mail fournit des informations sur la manière d'activer le compte.

- Si CLIQ Connect+ est activé par l'utilisateur de la clé, l'e-mail contient des informations sur la manière de se connecter au compte.

Pour désactiver le statut utilisateur CLIQ Connect+ :

1. Pour désactiver : Cliquez sur **Désactiver Connect+**.
2. Cliquez sur **Désactiver** dans la fenêtre pop-up.

4.1.5.2 Configurer l'accès à CLIQ Connect+ pour plusieurs employés

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.

Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

Conseil
Les utilisateurs désactivés ou supprimés peuvent être filtrés à l'aide du filtre de l'onglet **Avancée**.

2) Sélectionnez les employés et les visiteurs en cochant les cases.

REMARQUE !
Au maximum, 500 employés ou visiteurs peuvent être sélectionnés à la fois pour la désactivation du statut utilisateur CLIQ Connect+.

3) **Pour activer le statut utilisateur CLIQ Connect+ :**

REMARQUE !
Le statut utilisateur CLIQ Connect+ n'est pas activé pour les employés ou visiteurs suivants :

- n'ont pas d'adresse e-mail enregistrée.
- ont la même adresse e-mail qu'un autre employé ou visiteur ayant activé CLIQ Connect+.
- possèdent déjà un statut utilisateur activé.

1. Cliquez sur **Activer Connect+**.

   La fenêtre d'information s'ouvre.
2. Cliquez sur **Activer** dans la fenêtre pop-up.

   Un e-mail contenant des informations sur la configuration de CLIQ Connect est envoyé à l'adresse spécifiée.

   L'administrateur peut également envoyer l'e-mail manuellement à un utilisateur CLIQ Connect+ via la vue des informations individuelles en cliquant sur le bouton **Renvoyer l'e-mail**.

   – Si CLIQ Connect+ n'est pas activé par l'utilisateur de la clé, l'e-mail fournit des informations sur la manière d'activer le compte.

   – Si CLIQ Connect+ est activé par l'utilisateur de la clé, l'e-mail contient des informations sur la manière de se connecter au compte.

Pour désactiver le statut utilisateur CLIQ Connect+ :

1. Cliquez sur **Désactiver Connect+**.

   La fenêtre d'information s'ouvre.

2. Cliquez sur **Désactiver** dans la fenêtre pop-up.

Le résultat de l'opération est affiché au-dessus du tableau **RÉSULTATS DE LA RECHERCHE**.

4.1.6 Modification des informations sur les Employés ou les Visiteurs

Pour modifier les informations relatives aux employés ou aux visiteurs dans CWM, consultez *Chapitre 4.1.6.2 "Modification des informations sur les Employés ou les Visiteurs dans CWM", page 31*.

Les informations relatives aux employés peuvent également être modifiées en important un fichier CSV actualisé ou via LDAP si le système est intégré à LDAP. Pour davantage d'informations sur la façon d'importer les informations sur les employés, consultez *Chapitre 4.1.11 "Importer les informations Employé", page 34*. Pour plus d'informations sur l'intégration LDAP, voir *Chapitre 8.12 "Intégration LDAP", page 195*.

REMARQUE !
Il existe certaines limitations à la modification ou à la suppression de l'adresse e-mail d'un employé ou d'un visiteur dont le statut utilisateur CLIQ Connect+ est activé. Pour plus d'informations, consultez *Chapitre 4.1.6.1 "Informations importantes sur la modification ou la suppression d'adresses e-mail", page 30*.

4.1.6.1 Informations importantes sur la modification ou la suppression d'adresses e-mail

Lorsque CLIQ Connect+ est activé
Les employés ou les visiteurs dont le statut utilisateur CLIQ Connect+ est activé se connectent à CLIQ Connect avec l'adresse e-mail enregistrée dans CWM. Le fait de modifier ou de supprimer cette adresse va donc bloquer le processus de connexion à CLIQ Connect.

Modification

- Le fait de modifier une adresse e-mail change les informations d'identification de CLIQ Connect.

  Un e-mail contenant des informations sur la configuration de CLIQ Connect est envoyé à l'adresse spécifiée.

  – Si le compte CLIQ Connect+ n'est pas activé par l'utilisateur de la clé, l'e-mail contient le code d'activation du compte.

  – Si le compte CLIQ Connect+ est activé par l'utilisateur de la clé, l'e-mail contient des informations sur la manière de se connecter au compte.

- Dans CWM, il n'est pas autorisé de remplacer une adresse e-mail par une adresse déjà détenue par un autre utilisateur CLIQ Connect+.

  Une telle modification via l'intégration LDAP ou un fichier CSV est ignorée et traitée comme une erreur.

Suppression

- Supprimer une adresse e-mail dans CWM :

La suppression désactive le statut utilisateur CLIQ Connect+.

- Suppression d'une adresse e-mail via l'intégration LDAP ou un fichier CSV :

  Cette suppression n'est pas autorisée si le compte CLIQ Connect+ est activé par l'utilisateur de la clé.

Lorsque la connexion SSO est activée
Lorsqu'une clé de programmation est attribuée à un employé, son adresse e-mail associée ne peut plus être modifiée ou supprimée.

4.1.6.2 Modification des informations sur les Employés ou les Visiteurs dans CWM

Cette section explique comment modifier les informations sur les employés ou les visiteurs dans CWM.

Conditions préalables :

- L'employé ou le visiteur à modifier doit être actif.
- L'employé à modifier n'est pas intégré par LDAP.

> **REMARQUE !**
> En cas d'employé intégré par LDAP, seuls les éléments **Domaine** et **NOTES** peuvent être modifiés.

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.

   Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

2) Cliquez sur **Modifier**.
3) Mettez les champs à jour.

   - Pour modifier les notes, voir *Chapitre 4.1.7 "Ajout ou suppression de notes employés ou visiteurs", page 31*.
   - Pour modifier les liens externes, voir *Chapitre 4.1.8 "Gestion des liens externes employé ou visiteur", page 32*.

4) Cliquez sur **Enregistrer**.

> **REMARQUE !**
> Modifier ces informations peut conduire à l'envoi d'une notification par e-mail à l'administrateur du domaine afin qu'il prenne les mesures appropriées. Les notifications seront uniquement envoyées si elles sont activées dans **Réglages du système**.
>
> Voir également *Chapitre 6.4 "Modifier les réglages du système", page 100*.

4.1.7 Ajout ou suppression de notes employés ou visiteurs

Pour des informations sur les notes, voir *Chapitre 8.2.6 "Notes", page 183*.

Condition préalable :

- Les employés ou les visiteurs à modifier doivent être actifs.

1) Sélectionnez **Informations système » Employés** ou **Visiteurs**.

   Une liste de tous les employés ou des visiteurs s'affiche.

- Pour ajouter ou supprimer des notes pour un employé ou un visiteur, allez à l'*Étape 2*.
- Pour ajouter ou supprimer des notes pour plusieurs employés ou visiteurs, allez à l'*Étape 3*.

2) **Ajouter ou supprimer des notes pour un employé ou un visiteur :**

1. Sélectionnez l'employé ou le visiteur et accédez à ses informations détaillées.
2. Cliquez sur **Modifier**.
3. Ajouter ou supprimer une note pour un employé ou un visiteur.

   Pour ajouter une note :

   a) Cliquez sur **Ajouter note...**.
   b) Saisissez un nom pour la note.
   c) Cliquez sur **OK**.

   Pour supprimer une note :
   Cliquez sur la note à supprimer.
4. Cliquez sur **Enregistrer**.

3) **Ajouter ou supprimer des notes pour plusieurs employés ou visiteurs :**

1. Sélectionnez des employés ou des visiteurs dans les résultats de recherche en cochant les cases correspondantes.
2. **Pour ajouter une note :**

   a) Cliquez sur **Ajouter note...**.
   b) Entrez un nom pour la note.
   c) Cliquez sur **OK**.

   Pour supprimer une note :

   a) Cliquez sur **Supprimer note...**.
   b) Entrez un nom pour la note.
   c) Cliquez sur **OK**.

4.1.8 Gestion des liens externes employé ou visiteur

Pour des informations sur les liens externes, voir *Chapitre 8.4 "Liens externes", page 186*.

Condition préalable :

- Les employés ou les visiteurs à modifier doivent être actifs.

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.
   Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.
2) Cliquez sur **Modifier**.
3) **Pour ajouter un lien externe :**

1. Cliquez sur **Ajouter.**

2. Saisissez un **Nom** pour l'URL.
3. Saisissez l'**URL**. L'**URL** doit commencer par un protocole (http:// ou ftp://, par exemple).

   Si une URL racine a été définie dans les **Réglages système** (élément **Liens externes, URL racine**) il suffit d'ajouter la dernière partie de l'URL. Voir également *Chapitre 6.4 "Modifier les réglages du système", page 100*.
4. Cliquez sur **OK**.

Pour modifier un lien externe :

1. Cliquez sur **Modifier** à côté du lien externe à modifier.
2. Mettez les champs à jour.
3. Cliquez sur **OK**.

Pour supprimer un lien externe :
Cliquez sur **Supprimer** à côté du lien externe à supprimer.

4) Cliquez sur **Enregistrer**.

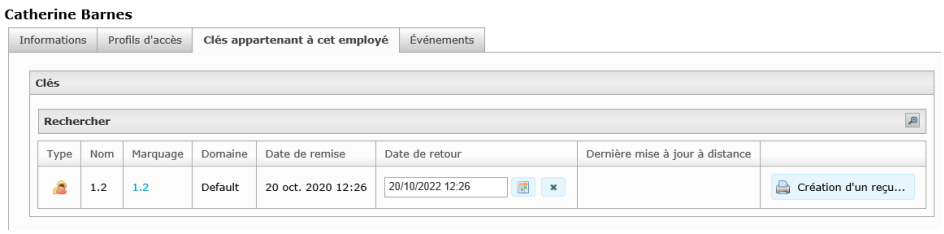
4.1.9 Affichage des clés d'employé ou de visiteur

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.

   Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

2) Sélectionnez l'onglet **Clés appartenant à cet employé** ou **Clés appartenant à ce visiteur**.

   Les clés actuellement remises à l'employé ou au visiteur sont affichées.



3)
   - Pour modifier la date de retour d'une clé, modifiez le champ **Date de retour**.
   - Pour générer un reçu de la remise et du retour de la clé, cliquez sur **Création d'un reçu...**.
   - Pour afficher la fenêtre d'informations détaillées de la clé, cliquez sur le marquage de la clé.

4.1.10 Visualisation des événements d'un employé ou d'un visiteur

L'onglet **Événements** fournit un enregistrement des activités administratives au sein de CWM, y compris des actions telles que la création d'un employé ou d'un visiteur et la mise à jour du statut de CLIQ Connect+. Il enregistre également les événements liés aux clés associées à l'employé ou au visiteur.

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.

   Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

2) Dans la fenêtre d'informations détaillées, sélectionnez l'onglet **Événements**.

La liste des événements employé ou visiteur s'affiche.

4.1.11 Importer les informations Employé

La fonction **Importer des employés** permet l'importation en masse de données nouvelles ou de données mises à jour sur les employés.

> **REMARQUE !**
> Les employés ajoutés par intégration LDAP ne peuvent pas être modifiés via l'importation d'un fichier CSV.

Condition préalable :

- Créez un fichier d'importation CSV en suivant les informations de format en *Chapitre 9.9 "Format du fichier d'importation d'employé", page 215*.

1) Sélectionnez **Administration » Importation d'employés**.
2) Cliquez sur **Sélectionner...**.
3) Sélectionnez le fichier à télécharger et cliquez sur **Ouvrir**.
4) Cliquez sur **Télécharger**.

   Affiche des informations sur le nombre d'entrées valides contenues dans le fichier. Si des entrées ne sont pas valides, cliquez sur **Détails** pour plus d'informations.
5) Cliquez sur **Importer**.

4.1.12 Exportation des informations sur les Employés ou les Visiteurs

1) Localisez les employés ou les visiteurs.

   Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.
2) Dans les résultats de recherche, sélectionnez les employés ou visiteurs dont les informations doivent être exportées.
3) Cliquez sur **Exporter vers le fichier CSV**.

   Les informations concernant les employés ou visiteurs désactivés ne peuvent pas être exportées.

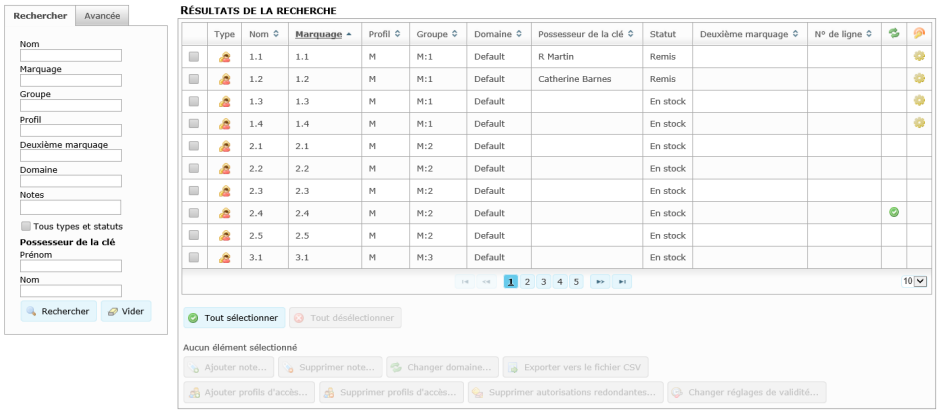
   > **REMARQUE !**
   > Pour pouvoir ouvrir correctement le fichier dans Excel, le délimiteur du fichier doit être défini selon les réglages régionaux. Pour modifier le délimiteur, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.
4) Dans la fenêtre contextuelle de téléchargement de fichier, cliquez sur **Ouvrir** ou sur **Enregistrer**.

4.2 Gestion des clés

4.2.1 Rechercher des clés utilisateur

1) Sélectionnez **Informations système » Clés**.

   Une liste de toutes les clés s'affiche.



Les symboles suivants sont utilisés :

- Clé mécanique
- Clé normale
- Clé standard
- Clé standard CLIQ Connect
- Clé dynamique
- Clé dynamique CLIQ Connect
- Une mise à jour à distance en attente existe pour la clé

2) Sélectionnez l'onglet **Rechercher** ou **Avancée**.

   Par défaut, les clés mécaniques et les clés déclarées perdues ou défectueuses ne s'affichent pas. Pour inclure également toutes ces clés dans les résultats de recherche, sélectionnez **Tous types et statuts**.

   L'onglet **Avancée** inclut également les champs de recherche Type de clé, Clé CLIQ Connect, Statut inventaire et Statut opérationnel.

3) Saisissez les critères de recherche.

   En tapant **Notes** dans le champ de recherche, toutes les notes correspondantes apparaîtront sous forme d'une liste à sélectionner.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

4) Cliquez sur **Rechercher**.

5) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur la ligne de la clé correspondante.

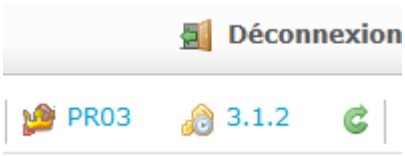
   Pour plus d'informations sur les attributs de clé, voir *Chapitre 9.3.3 "Attributs de clé", page 202*.

4.2.2 Scanner une clé utilisateur

1) Insérez la clé dans la fente droite du boîtier de programmation local.

2) Cliquez sur du coin supérieur droit de la page.

   Les clés du boîtier de programmation local sont affichées sous la barre de navigation.



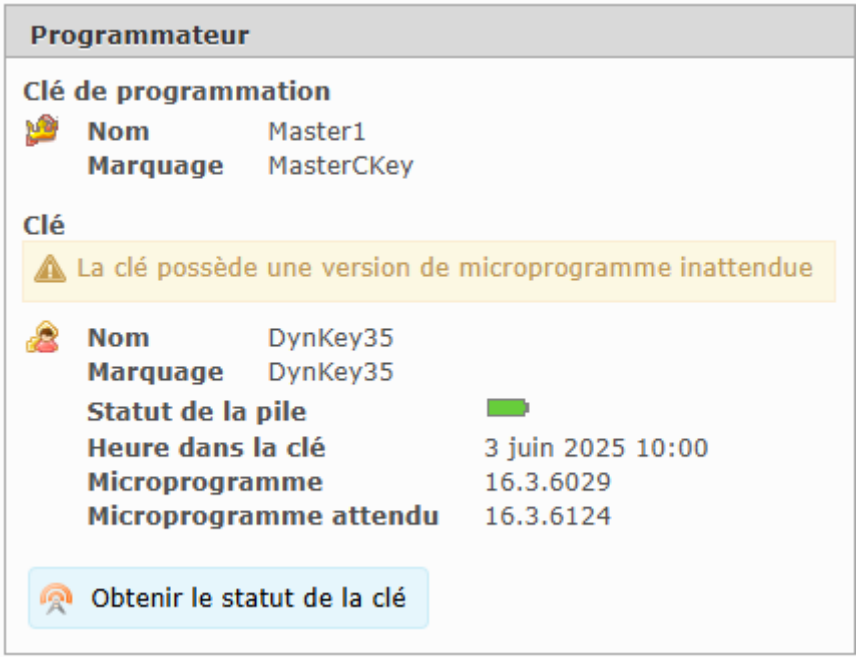
3) Insérez la clé dans la fente droite du boîtier de programmation local.

La vue des informations détaillées de la clé s'affiche, avec le **Nom** et le **Marquage** de la clé dans la partie droite de la page.

4.2.3 Affichage du statut de la clé

1) Scannez la clé. Voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*.
2) Cliquez sur **Obtenir le statut de la clé**.

Les informations de base de la clé s'affichent. Pour plus d'informations sur l'indicateur d'état de la batterie, voir *Chapitre 9.6 "Indications de niveau de batterie", page 213*.



4.2.4 Modifier les informations d'une clé utilisateur

1) Trouvez la clé et accédez à ses informations détaillées.

Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Cliquez sur **Modifier**.
3) Pour modifier le nom de la clé, mettez le champ **Nom** à jour.
4) Pour ajouter une note, cliquez sur **Ajouter note**.

Voir également *Chapitre 4.2.5 "Ajout ou suppression de notes de clé utilisateur", page 37*.

5) Pour ajouter un lien externe, cliquez sur **Ajouter lien externe**.

Voir également *Chapitre 4.2.6 "Gestion des liens externes d'une clé utilisateur", page 37*.

6) Cliquez sur **Enregistrer**.

4.2.5 Ajout ou suppression de notes de clé utilisateur

Pour des informations sur les notes, voir *Chapitre 8.2.6 "Notes", page 183*.

1) Localisez la clé à modifier.

   Pour rechercher une clé, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé située dans le boîtier de programmation local, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*.

2) • Pour ajouter ou supprimer des notes pour une clé, allez à l'*Étape 3*.
   • Pour ajouter ou supprimer des notes pour plusieurs clés, allez à l'*Étape 4*.

3) **Ajouter ou supprimer des notes pour une clé :**

   1. Sélectionnez la clé et accédez à ses informations détaillées.
   2. Cliquez sur **Modifier**.
   3. Ajouter ou supprimer une note pour une clé.

      Pour ajouter une note :

      a) Cliquez sur **Ajouter note...**.
      b) Saisissez un nom pour la note.
      c) Cliquez sur **OK**.

      Pour supprimer une note :
      Cliquez sur la note à supprimer.
   4. Cliquez sur **Enregistrer**.

4) **Ajouter ou supprimer des notes pour plusieurs clés :**

   1. Sélectionnez des clés dans les résultats de recherche en cochant les cases correspondantes.
   2. **Pour ajouter une note :**

      a) Cliquez sur **Ajouter note...**.
      b) Entrez un nom pour la note.
      c) Cliquez sur **OK**.

      Pour supprimer une note :

      a) Cliquez sur **Supprimer note...**.
      b) Entrez un nom pour la note.
      c) Cliquez sur **OK**.

4.2.6 Gestion des liens externes d'une clé utilisateur

Pour des informations sur les liens externes, voir *Chapitre 8.4 "Liens externes", page 186*.

1) Trouvez la clé et accédez à ses informations détaillées.

Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Cliquez sur **Modifier**.
3) Pour ajouter un lien externe :
   a) Cliquez sur **Ajouter**.
   b) Saisissez un **Nom** pour l'URL.
   c) Saisissez l'**URL**. L'**URL** doit commencer par un protocole (http:// ou ftp://, par exemple).

      Si une URL racine a été définie dans les **Réglages système** (élément **Liens externes, URL racine**) il suffit d'ajouter la dernière partie de l'URL. Voir également *Chapitre 6.4 "Modifier les réglages du système", page 100*.
   d) Cliquez sur **OK**.
4) Pour modifier un lien externe :
   a) Cliquez sur **Modifier** à côté du lien externe à modifier.
   b) Mettez les champs à jour.
   c) Cliquez sur **OK**.
5) Pour supprimer un lien externe : Cliquez sur **Supprimer** à côté du lien externe à supprimer.
6) Cliquez sur **Enregistrer**.

4.2.7 Affichage de l'historique des mises à jour de la clé utilisateur

L'onglet **Historique de mise à jour** est utilisé pour la traçabilité de la programmation des clés.

Conditions préalables :

- Le niveau de permission de l'utilisateur doit être **Vue** pour le rôle **Clé : Historique de mise à jour**.

  Pour modifier le niveau d'autorisation, voir *Chapitre 6.7 "Gestion des rôles et des autorisations", page 129*.
-

1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*
2) Sélectionnez l'onglet **Historique de mise à jour**.

   La liste de toutes les mises à jour de clé apparaît.

> **REMARQUE !**
> Par défaut, les mises à jour des clés, à l'exception des mises à jour de microprogrammes, sont supprimées après 3 mois.

Les symboles suivants sont utilisés :

- La tâche de programmation pour un boîtier de programmation local existe, mais n'a pas été commencée
- Une mise à jour à distance en attente existe pour la clé
- La tâche de programmation est terminée
- La tâche de programmation a échoué ou a été annulée
- La tâche de programmation a été remplacée par une nouvelle tâche

3) Pour afficher les détails complémentaires d'une mise à jour spécifique, cliquez sur le lien dans la colonne **Commentaire**.

4.2.8 Affichage des événements d'une clé utilisateur

L'onglet Événements est utilisé pour la traçabilité des opérations administrateur dans CWM, telles que la remise d'une clé, l'association de profils d'accès, la modification des autorisations de clé, etc.

1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Sélectionnez l'onglet **Événements**.

   La liste de tous les événements de clé s'affiche.

4.2.9 Remise de clés utilisateur

Le processus de remise comporte deux phases :

1. **Réglages de la remise de clé**

   Dans cette phase, les réglages de la remise de clé sont configurés dans trois pages différentes : **Général**, **Accès** et **Paramètres d'heure** .

   Il est obligatoire de terminer les réglages de la page **Général**, mais les réglages des autres pages sont facultatifs.

2. **Résumé de la remise**

   Dans cette phase, les détails de la remise sont confirmés et la clé est remise. Si la clé remise est insérée dans le boîtier de programmation, elle sera aussi programmée.

1) Il existe deux moyens pour lancer le processus de remise :

   - Sélectionnez **Tâches » Remise d'une clé » à un employé** ou **à un visiteur**.
   - Sur la vue des informations détaillées de l'employé ou du visiteur :

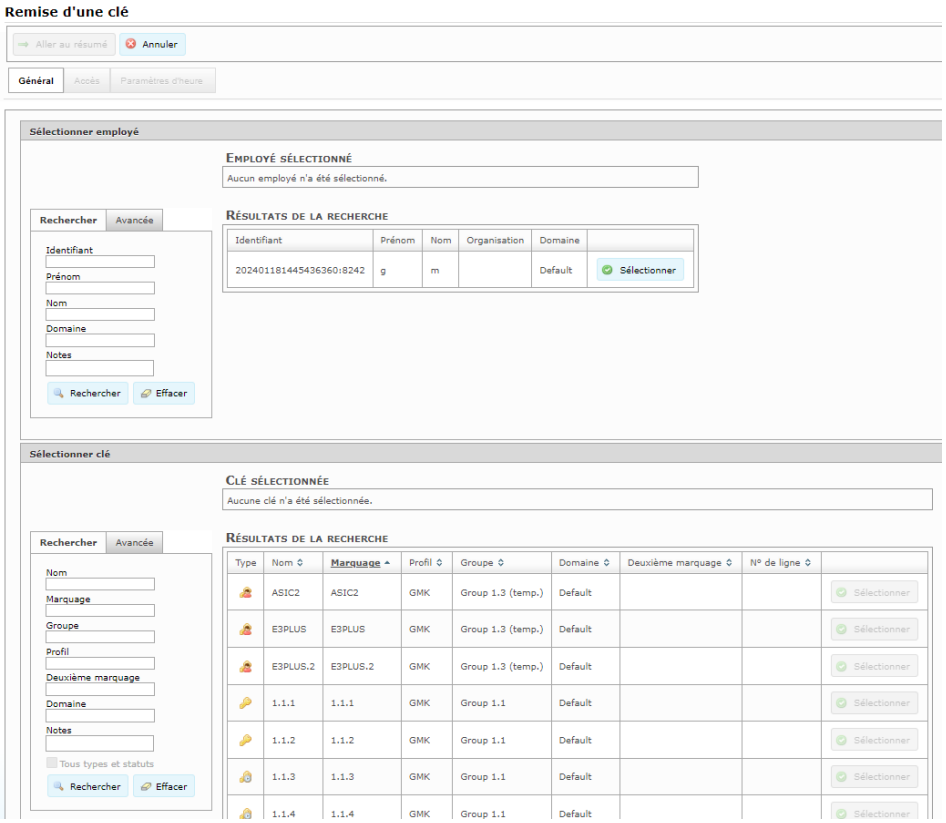
     a) Trouvez la clé et accédez à ses informations détaillées.

     Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

     Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

b) Cliquez sur **Remise d'une clé**.

La page **Remise d'une clé**, **Général** est ouverte.



2) S'il n'y a pas d'employé ou d'invité sélectionné dans la section **Sélectionner employé** ou **Sélectionner visiteur**, trouvez la personne et cliquez sur **Sélectionner**.

   Pour rechercher un employé ou un visiteur spécifique, voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

3) Sélectionnez la clé à remettre de l'une des manières suivantes :

- Si la clé à remettre est disponible :

  a) Insérez la clé dans la fente droite du boîtier de programmation local.

  b) Cliquez sur dans le coin supérieur droit de la page pour scanner la clé.

  c) Dans la boîte de dialogue **Clé utilisateur dans le boîtier de programmation**, cliquez sur **Sélectionner**.

  Il est recommandé d'utiliser la fonction Scanner pour la remise de clés dans la plupart des cas, car la nouvelle configuration est alors immédiatement programmée sur la clé. Ceci est particulièrement important pour les systèmes non distants.

- Si la clé à remettre n'est pas disponible :

  a) Trouvez la clé à remettre dans l'une des listes suivantes et cliquez sur **Sélectionner**.

- La liste **CLÉ PRÉ-ATTRIBUÉE**

  S'il existe des clés pré-attribuées pour la personne sélectionnée, la liste des clés pré-attribuées est affichée dans la vue de sélection des clés.

  > **Conseil**
  > Une clé pré-attribuée est une clé qui est associée à une personne particulière lorsque la clé est attribuée.
  >
  > Relier la clé à la personne concernée aide les administrateurs à choisir la bonne clé pour la personne sélectionnée pendant le processus de remise.
  >
  > Le statut de la clé reste **En stock** après l'importation de la clé dans le système, que la clé physique ait été livrée ou non par le distributeur CLIQ.
  >
  > La clé peut être remise à n'importe qui, et perd la caractéristique de pré-attribution une fois remise.

- La liste **RÉSULTATS DE LA RECHERCHE**

  Pour réduire la liste, entrez les critères de recherche et cliquez sur **Rechercher**. Voir également *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

4) Si nécessaire, définissez les détails dans les pages **Accès** et **Paramètres d'heure** .

   Sinon, passez à *Étape 5*.

   > **REMARQUE !**
   > Les réglages suivants sont applicables aux clés dynamiques pour les systèmes avec fonctionnalités de mise à jour à distance et groupes de cylindres. Certains réglages ne sont pas accessibles pour les autres types et configurations de clé.

   La page Accès

   - **Sélectionner les profils d'accès**

     Sélectionnez les profils d'accès dans la liste.

     Par défaut, les profils d'accès des employés ou des visiteurs sont sélectionnés.

   - **Sélectionner des groupes de cylindres**

     Sélectionnez les groupes de cylindres auxquels les clés doivent avoir accès.

   - **Sélectionner les cylindres**

     Sélectionnez les cylindres auxquels les clés doivent avoir accès.

La page Paramètres d'heure

- **Régler la validité de la clé**

  – **SÉLECTIONNEZ LES DATES DE REMISE ET DE RETOUR**

  Entrez la date de remise (**Date de remise**) et la date de retour (**Date de retour**) :

  Si la date de remise de la clé n'est pas encore déterminée, cliquez sur **X**.

  – **RÉGLER LA VALIDITÉ DE LA CLÉ**

  Définissez les réglages suivants pour la validité de la clé.

  - Sélectionnez les paramètres d'activation parmi **Inactive**, **Active entre les dates sélectionnées** et **Toujours active**.

    Si l'option **Active entre les dates sélectionnées** est sélectionnée, réglez les dates **Clé active à partir du** et **Clé active jusqu'au**.

    Si la date **Clé active jusqu'au** n'est pas encore déterminée, cliquez sur **X**.
  - Pour utiliser la revalidation, cochez la case **Utiliser la revalidation** et définissez l'intervalle de temps.

    Lorsqu'elle est définie, la clé doit être mise à jour à la fréquence spécifiée pour rester active.
  - **Clés CLIQ Connect uniquement** :

    Pour utiliser l'option **Validation du code PIN**, cochez la case et définissez l'intervalle de temps.

    Lorsqu'il est défini, pour rester active, la clé doit être validée selon la fréquence spécifiée par un code PIN à l'aide de CLIQ Connect.

  Pour plus d'informations sur la validité des clés, voir *Chapitre 8.1.4 "Validité de la clé", page 169*.

- **Sélectionner le planning horaire de la clé**

  PLANNING DE CLÉ

  Définissez le planning horaire de la clé comme suit :

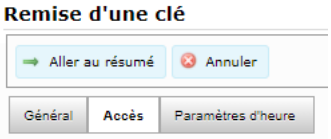
  a) S'il existe un modèle de planning horaire à utiliser, sélectionnez-le dans la liste déroulante et cliquez sur **Appliquer**.

  b) Cliquez sur **Ajouter période** pour ajouter une plage horaire au modèle sélectionné ou pour personnaliser le planning horaire.

  c) Cliquez sur **Ajouter cylindre** pour définir une Plage horaire spécifique pour un cylindre.

  Sélectionnez un cylindre dans la liste affichée, et cliquez sur **Ajouter période** pour définir la période.

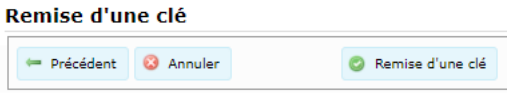
5) Cliquez sur **Aller au résumé**.



Un résumé des droits d'accès et des réglages horaires s'affiche.

6) Vérifiez les réglages.

Pour modifier les réglages, cliquez sur **Précédent** afin de revenir aux pages des réglages.



7)
- Si la clé remise est dans le boîtier de programmation local, cliquez sur **Programmer et enregistrer**.

  La clé est directement programmée dans le boîtier de programmation.
- Si la clé remise n'est pas dans le boîtier de programmation local, cliquez sur **Remise d'une clé**.

  Une tâche de mise à jour à distance est créée dans les systèmes distants.

8) Facultatif : Créez un reçu.

Les reçus sont créés au format PDF et peuvent être imprimés et enregistrés.

Pour créer ou modifier des modèles de reçus, reportez-vous à *Chapitre 6.9 "Gestion des modèles de reçu", page 132*.

a) Cliquez sur **Création d'un reçu...**.

La fenêtre **Sélection d'un reçu** s'ouvre.

b) Choisissez la langue appropriée dans la liste déroulante.

c) Choisissez le modèle approprié dans la liste déroulante.

Dans la liste déroulante, tous les modèles de reçus de remise de clés dans la langue sélectionnée sont affichés.

d) Cliquez sur **Créer un reçu** ou **Télécharger**.

9) Facultatif : Émettez un code QR pour configurer l'URL du serveur CLIQ Remote et remettez ce code avec la clé.

Si l'utilisateur de la clé compte utiliser CLIQ Connect et que le système CWM n'est pas intégré à DCS, il doit entrer manuellement l'URL du serveur CLIQ Remote dans CLIQ Connect. Générer un code QR pour l'URL du serveur CLIQ Remote et le remettre au possesseur de la clé simplifie le processus de configuration de l'application.

a) Ouvrez n'importe quel type de générateur de code QR en ligne.

b) Entrez les informations dans cet ordre : `<Code de la société d'exploitation ASSA ABLOY>,<Nom MKS>,<URL>`

Exemple:
`3,CLIQConnectTeam,https://app-team-remote.cliqapps.aa.st:443/CLIQRemote`

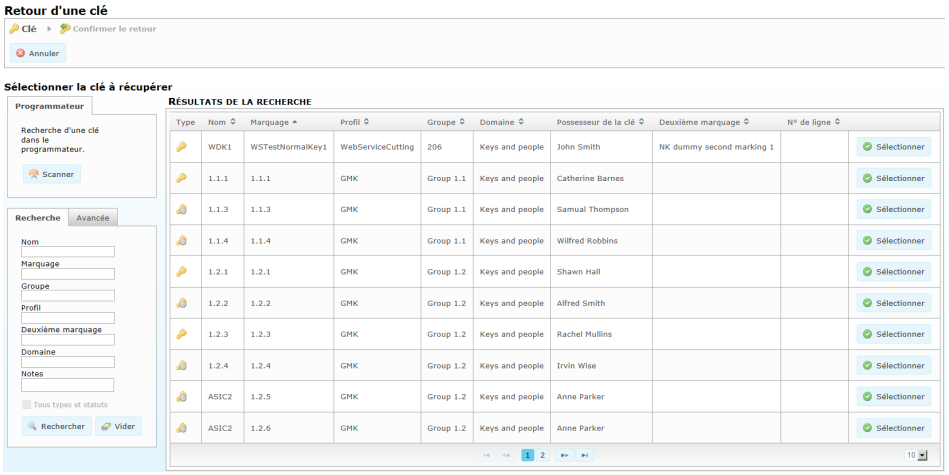
Pour le code de la société d'exploitation ASSA ABLOY, reportez-vous à *Chapitre 9.10 "Code de la société d'exploitation ASSA ABLOY", page 218*.

c) Imprimez le code QR.

4.2.10 Réception de clés utilisateur (Retour)

1) Sélectionnez **Tâches » Retour d'une clé**.

La liste de toutes les clés remises s'affiche.



2) Trouvez et sélectionnez la clé à retourner de l'une des manières suivantes :

- Dans la liste, cliquez sur **Sélectionner** pour choisir la clé à retourner.

  Pour rechercher la clé, saisissez les critères de recherche et cliquez sur **Rechercher**. Voir également *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.
- Si la clé à retourner se trouve dans la fente droite du Boîtier de programmation local, cliquez sur dans le coin supérieur droit de la page pour scanner la clé.

  Dans la plupart des cas, il est recommandé d'utiliser la fonction Scanner pour le retour de clés, car la nouvelle configuration peut alors être programmée immédiatement sur la clé. Ceci est particulièrement important pour les systèmes non distants.

3) Pour retourner une clé :

- Si la clé retournée est scannée dans le boîtier de programmation local, cliquez sur **Réinitialiser la clé et la retourner** ou **Retourner la clé sans la réinitialiser**.

  L'option de réinitialisation est utile pour les clés destinées à recevoir des réglages différents à chaque remise et est l'option recommandée dans la plupart des cas.
- Si la clé retournée n'est pas scannée, cliquez sur **Appliquer**.

4) Facultatif : Créez un reçu. Les reçus sont créés au format PDF et peuvent être imprimés et enregistrés.

REMARQUE !

Cette option n'est disponible que si **Reçus de remise et de retour séparés** est sélectionné dans **Réglages du système**. Ce réglage s'obtient en sélectionnant **Administration » Réglages du système » ADMINISTRATION » Reçus de clé**.

Pour plus d'informations sur la manière de modifier les réglages du système, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

Pour créer ou modifier des modèles de reçu, voir *Chapitre 6.9 "Gestion des modèles de reçu", page 132*.

a) Cliquez sur **Création d'un reçu...**.

La fenêtre **Sélection d'un reçu** s'ouvre.

b) Choisissez la langue appropriée dans la liste déroulante.

c) Choisissez le modèle approprié dans la liste déroulante.

Dans la liste déroulante, tous les modèles de reçus de retour de clés dans la langue sélectionnée sont affichés.

d) Cliquez sur **Imprimer le reçu** ou **Télécharger**.

Si vous sélectionnez **Télécharger**, le reçu est téléchargé dans le dossier **Téléchargements**.

4.2.11 Impression d'un reçu vide

Lorsqu'une clé est remise ou retournée, le reçu est généré au format PDF avec les informations de remise ou de retour. Il est également possible de générer des reçus dont les champs sont laissés vides pour être édités manuellement.

1) **Tâches » Reçu**.
2) Sélectionnez soit **Imprimer un reçu de remise vierge...** soit **Imprimer un reçu de retour vierge...**.
3) Dans la fenêtre pop-up :
   a) Sélectionnez la langue appropriée dans la liste déroulante.
   b) Sélectionnez le modèle approprié.

   Lorsque **Personnaliser** est sélectionné, tous les modèles du même type (modèle de remise ou de retour de clé) dans la langue sélectionnée sont affichés dans la liste déroulante.
4) Cliquez sur **Créer un reçu** ou **Télécharger**.

4.2.12 Gestion d'une clé perdue ou cassée

Cette section décrit comment déclarer perdues ou défectueuses des clés utilisateur. Pour signaler une clé de programmation perdue ou défectueuse, voir *Chapitre 6.11.9 "Déclaration et blocage d'une clé de programmation perdue", page 140* ou *Chapitre 6.11.10 "Déclaration d'une clé de programmation défectueuse ou opérationnelle", page 142*.

4.2.12.1 Signalement d'une clé utilisateur défectueuse

1) Il existe deux façons de commencer à signaler la clé cassée :

- Sélectionnez **Tâches » Déclarer une clé défectueuse**. Passez à *Étape 2*.
- Sur la vue des informations détaillées de la clé défectueuse (pour rechercher la clé, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*), cliquez sur le bouton **Déclarer défectueux**. Passez à *Étape 4*.

2) Saisissez les critères de recherche pour localiser le possesseur de la clé et cliquez sur **Rechercher**.
3) Sélectionnez la clé défectueuse.
4) Cliquez sur **Appliquer**.

   La fenêtre d'informations détaillées de la clé déclarée défectueuse contient l'option permettant de supprimer le statut défectueux.

Si la clé cassée est remplacée par une clé clone, voir *Chapitre 4.2.13 "Remplacement d'une clé utilisateur par un clone d'usine", page 50* pour de plus amples instructions.

4.2.12.2 Signalement et blocage d'une clé utilisateur perdue

Condition préalable :

- Si des cylindres doivent être bloqués et que la tâche de programmation de cylindre est attribuée à une clé utilisateur, assurez-vous que l'option "Bloquer la clé perdue avec les clés utilisateur" est activée dans les réglages du système. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100* pour obtenir des instructions sur la modification de ce paramètre. Ceci n'est applicable qu'à un système à distance.

1) Il existe deux façons de commencer à signaler la clé perdue :

   - Sélectionnez **Tâches » Déclarer une clé perdue**. Passez à *Étape 2*.
   - Sur la vue des informations détaillées de la clé perdue (pour rechercher la clé, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*), cliquez sur le bouton **Déclarée perdue**. Passez à *Étape 4*.

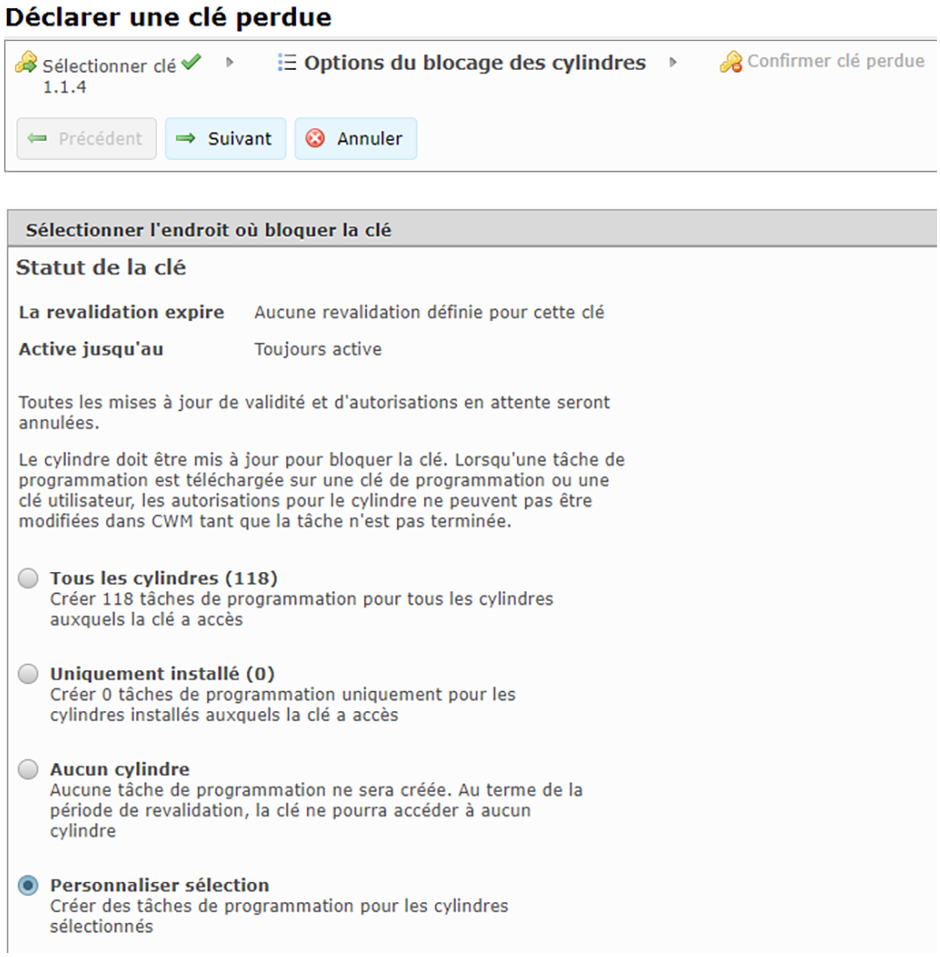
2) Saisissez les critères de recherche pour localiser le possesseur de la clé et cliquez sur **Rechercher**.
3) Sélectionnez la clé perdue et cliquez sur **Sélectionner**.
4) Sélectionnez les cylindres pour lesquels la clé sera bloquée :

   - S'il est nécessaire de programmer les cylindres pour bloquer immédiatement la clé perdue :

     Conseil
     Pour configurer le système afin qu'il bloque la clé perdue dans les cylindres nouvellement ajoutés, activez **Bloquer les clés perdues dans les nouveaux cylindres pendant l'importation d'extension** dans les réglages du système. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

     – Sélectionnez **Tous les cylindres** ou **Uniquement installé** et passez à *Étape 7*.
     – Sélectionnez **Personnaliser sélection** et passez à *Étape 5* pour sélectionner les cylindres.

- Si la clé doit être signalée comme perdue dans CWM sans en bloquer l'accès (par exemple, en attendant l'expiration de la période de revalidation en cours), sélectionnez **Aucun cylindre**, cliquez sur **Suivant** et passez à *Étape 11*.



5) Cliquez sur **Suivant**.
6) Sélectionnez les cylindres pour lesquels la clé perdue sera bloquée.
7) Cliquez sur **Suivant**.
8) Facultatif : Sélectionnez la clé de blocage dans la liste en cliquant sur **Sélectionner**.

> **REMARQUE !**
> Si ce processus est ignoré, des tâches de programmation des cylindres sont créées pour les clés de programmation.

Dans l'onglet **Rechercher**, sélectionnez **Tous types et statuts** pour afficher les clés de programmation.

Dans l'onglet **Avancée**, sous **Type**, sélectionnez les types de clés pour modifier ce qui est affiché dans la liste.

REMARQUE !
Réglages de clé de blocage :

- La clé de blocage doit être de génération 2 avec la version de microprogramme 12.2 ou une version ultérieure.
- La mémoire de la clé de blocage doit être suffisante.

9) Dans la page de confirmation, sélectionnez le niveau de priorité sous **Priorité**.

Les tâches urgentes doivent disposer d'un niveau de priorité élevé.

10)

AVERTISSEMENT !
Par défaut, même si aucune tâche de programmation du cylindre n'est créée pour bloquer la clé perdue, cette clé est ajoutée à CWM dans la **Liste des clés interdites** pour les cylindres concernés. Cette information n'est toutefois pas visible dans CWM. Si ces cylindres sont ultérieurement reprogrammés ou remplacés, les informations sur les clés interdites stockées dans CWM sont appliquées, bloquant de fait la clé perdue. Par conséquent, même si la clé perdue est déclarée retrouvée ultérieurement, elle restera toujours bloquée par les cylindres reprogrammés ou remplacés.

Pour ré-autoriser la clé retrouvée dans ces cylindres, voir *Chapitre 4.9.2 "Configuration des autorisations dans les cylindres", page 81*.

Pour modifier ce réglage par défaut, vous devez désactiver le réglage système **Autoriser de ne pas bloquer les clés perdues dans les cylindres**. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

Après avoir vérifié toutes les informations, cliquez sur **Déclarée perdue**.

11) Facultatif : Cliquez sur **Imprimer la liste des cylindres** pour générer un résumé au format PDF.

12)
- Si une clé spécifique n'a **PAS** été sélectionnée pour programmer les cylindres, continuez à partir de l'*Étape 4* de la *Chapitre 4.4.13 "Programmation des cylindres", page 62*.
- Si une clé spécifique a été sélectionnée pour programmer les cylindres, suivez les instructions ci-dessous.

13) Accédez à la vue des informations détaillées de la clé de blocage sélectionnée.

Conseil
En cliquant sur **Marquage de la clé** sous **Informations sur la clé de blocage**, vous accédez directement à la visualisation des informations.

14) Allez dans l'onglet **Tâches de programmation** et confirmez que le travail de cylindre est affecté à la clé.

15)
- **Programmation dans le boîtier de programmation local**

Insérez la clé de blocage dans la fente droite du boîtier de programmation local et retirez la clé de programmation de la fente gauche de ce boîtier.

- **Programmation dans un boîtier de programmation mural**

  Insérez la clé de blocage dans un boîtier de programmation mural.

La tâche de programmation du cylindre est automatiquement inscrite sur la clé de blocage.

16) Reprogrammez chaque cylindre à l'aide de la clé de blocage.

17) Après avoir programmé les cylindres, signalez les tâches de cylindre terminées en insérant la clé de blocage dans l'un des dispositifs suivants :

- La fente droite du boîtier de programmation local (retrait de la clé de programmation de la fente gauche)
- Un boîtier de programmation mural

4.2.12.3 Signalement d'une clé utilisateur retrouvée

1) Dans CWM, localisez la clé perdue et affichez ses informations détaillées.

   Voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35* ou *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

> **REMARQUE !**
> Les clés perdues sont filtrées à l'aide du filtre **Perdu** de l'onglet **Avancée**.

2) Cliquez sur **Déclarée trouvée**.

   Le statut de la clé devient **En stock**.

3) Autorisez à nouveau la clé en programmant les cylindres concernés. Suivez les instructions de la *Chapitre 4.9.2 "Configuration des autorisations dans les cylindres", page 81*.

   Voir ci-dessous pour savoir quels cylindres sont concernés.

Cylindres concernés

Cylindres qui **doivent être programmés** pour ré-autoriser la clé :

- Cylindres déjà programmés pour bloquer la clé perdue.
- Les cylindres qui n'ont **pas** été programmés pour bloquer la clé perdue doivent être programmés dans le cas suivant :
  - Le cylindre a été **reprogrammé** ou **remplacé**.

    ET

  - Le réglage système **Blocage silencieux des clés perdues dans le cylindre lors de la mise à jour de l'autorisation** est **activé**.

REMARQUE !
Cette procédure s'applique à la fois aux cylindres pour lesquels aucune tâche de programmation n'a été créée lorsque la clé a été déclarée perdue, et aux cylindres pour lesquels des tâches de programmation ont été créées mais n'ont pas encore été exécutées.

Tous les autres cylindres :

La clé dispose déjà d'un accès, il n'est donc pas nécessaire de programmer les cylindres (les tâches de programmation qui ont été créées pour les cylindres mais n'ont pas encore été exécutées sont automatiquement annulées).

4.2.13 Remplacement d'une clé utilisateur par un clone d'usine

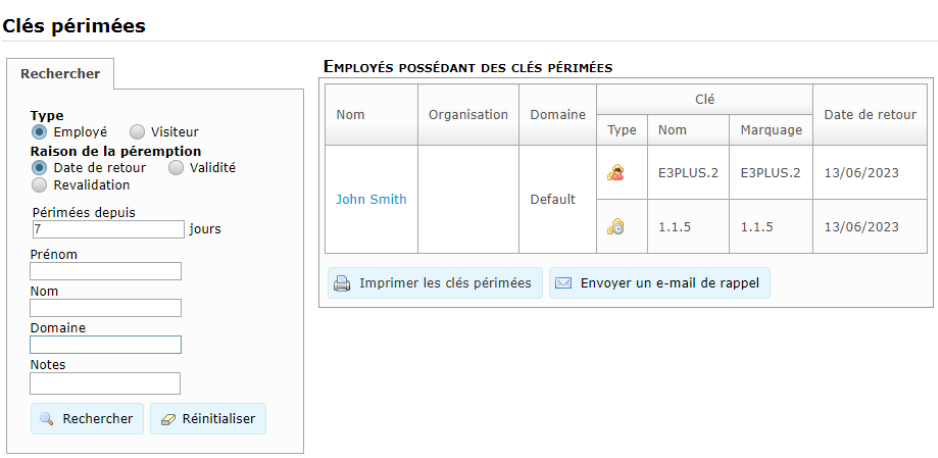
Si un clone de remplacement est livré de l'usine à la suite d'une clé défectueuse, les étapes suivantes doivent être prises pour assurer la fonctionnalité de la clé.

1) Lorsque la clé de remplacement arrive de l'usine, ouvrez le **Administration » Importation d'extension » Télécharger ou récupérer le ou les fichiers d'importation d'extension** pour télécharger dans CWM le fichier CWS fourni (si l'intégration DCS est désactivée) ou pour récupérer le fichier à partir de DCS.
2) Créez et programmez une tâche d'autorisation pour la clé de remplacement. Voir *Chapitre 4.9.1 "Configuration des autorisations dans les clés", page 78*.
3) Créez et programmez une tâche de validation pour la clé de remplacement. *Chapitre 4.10.1 "Configuration de la validité de la clé, de la revalidation et de la validation du code PIN", page 86*.
4) Annulez tous les tâches de planning de l'ancienne clé, recréez-les et programmez-les pour la clé de remplacement. Voir *Chapitre 4.10.3 "Configuration du planning de clé", page 89*.
5) La clé de remplacement est prête à être utilisée.

4.2.14 Affichage des clés utilisateur périmées

1) Sélectionnez **Tâches » Clés périmées**.
2) Dans l'onglet **Rechercher**, sélectionnez **Employé** ou **Visiteur** pour choisir le type d'utilisateur de clé.

   La liste des clés remises aux employés ou aux visiteurs, avec une date de retour dans le nombre de jours spécifié, s'affiche.



Le nombre de jours par défaut peut être modifié dans les Réglages système. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

3) Sélectionnez une **Raison de la péremption**, entrez d'autres critères de recherche, puis cliquez sur **Rechercher**.

   Raison de la péremption :

   - Si **Date de retour** est sélectionné, les clés ayant une date de retour comprise dans le nombre de jours spécifié sont affichées.
   - Si **Validité** est sélectionné, les clés ayant une période de validité se terminant comprise dans le nombre de jours spécifié sont affichées.
   - Si l'option **Revalidation** est sélectionnée, la liste des clés dont la période de revalidation se termine entre les dates spécifiées est affichée.

4) Pour imprimer la liste des clés périmées ou des clés nécessitant une revalidation, cliquez sur **Imprimer les clés périmées**.

5) Pour envoyer un e-mail de rappel aux employés ou aux visiteurs ayant des clés périmées, cliquez sur **Envoyer un e-mail de rappel**.

   Pour que cette option soit disponible, **Messagerie utilisateur** doit être sélectionnée dans **Réglages du système**. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

4.2.15 Mise à jour et revalidation d'une clé utilisateur

Via les boîtiers de programmation locaux
Si une clé est insérée dans le logement de droite du boîtier de programmation local, elle est directement mise à jour pendant l'utilisation de CWM.

Lorsque les actions suivantes ont été effectuées localement, la clé est revalidée en même temps dans le boîtier de programmation local :

- définir le **Planning**
- lire le **Journal des événements**
- changer les **Cylindres dans la liste d'accès**

Si les conditions suivantes sont remplies, une clé est mise à jour et/ou revalidée dans le logement de droite du boîtier de programmation local **sans** clé de programmation :

- Clé de 2e génération avec la version 12.3 du microprogramme ou une version ultérieure
- CLIQ Connect PC est activé

> **REMARQUE !**
> La clé de programmation doit être retirée du logement de gauche du boîtier de programmation local avant mise à jour et revalidation.

Via les boîtiers de programmation à distance
Les utilisateurs de clés peuvent mettre à jour et/ou revalider leurs clés en les insérant dans un boîtier de programmation mural ou un boîtier de programmation CLIQ Mobile.

La clé peut également être mise à jour et/ou revalidée lorsqu'elle est connectée à CLIQ Connect via un boîtier de programmation CLIQ Connect Mobile.

Pour plus d'informations sur la revalidation des clés, voir *Chapitre 8.1.5 "Revalidation de clé", page 169* et *Chapitre 8.1.6 "Revalidation flexible", page 172*.

4.2.16 Copie d'une configuration de clé utilisateur

La configuration d'une clé peut être copiée sur une autre clé scannée dans le boîtier de programmation local. Les réglages suivants sont copiés, le cas échéant :

- Validité
- Planning
- Réglages de revalidation
- Liste d'accès de clé
- Profils d'accès

Pour les clés incluses dans les listes d'accès de cylindre :

- Des tâches de programmation de cylindre sont créées pour mettre à jour les listes d'accès de cylindre.

1) Localisez la clé dont la configuration doit être copiée et allez sur la vue de ses informations détaillées.

   Voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

2) Insérez la clé cible dans le boîtier de programmation local.
3) Cliquez sur **Copier configuration de clé**.

   La clé est scannée.

4) Cliquez sur **Sélectionner**.
5) Sélectionnez une **Priorité** pour les tâches de programmation de cylindre.

   Les tâches urgentes doivent disposer d'un niveau de priorité élevé.

6) Cliquez sur **Appliquer**.

   La configuration existante sur la clé cible est remplacée et des tâches de programmation de cylindre sont créées si nécessaire.

   Un événement spécifiant la date et l'heure du changement et un marquage depuis la clé source et la clé de programmation sont créés.

4.2.17 Impression du rapport sur les clés utilisateur

1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Cliquez sur **Imprimer le rapport de la clé**.
3) Choisissez si les cylindres mécaniques doivent être inclus ou non dans la liste et cliquez sur **OK**.
4) Une prévisualisation est présentée dans la fenêtre pop-up.

   - Pour enregistrer, cliquez sur l'icône d'enregistrement et indiquez le dossier dans lequel enregistrer.
   - Pour imprimer, cliquez sur **...** et sélectionnez **Imprimer**.

4.2.18 Exportation des informations d'une clé utilisateur

1) Sélectionnez **Informations système » Clés**.

   Une liste de toutes les clés s'affiche.

2) Recherchez les clés.

   Voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

3) Dans les résultats de recherche de clé, sélectionnez les clés dont vous souhaitez exporter les données.

4) Cliquez sur **Exporter vers le fichier CSV**.

5) Dans la fenêtre pop-up de téléchargement de fichiers, cliquez sur **Enregistrer**.

   Un fichier CSV est téléchargé dans le dossier **Téléchargements**.

> **REMARQUE !**
> Pour pouvoir ouvrir correctement le fichier dans Excel, le délimiteur du fichier doit être défini selon les réglages régionaux. Pour modifier le délimiteur, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

4.3 Gestion des groupes de clés

4.3.1 Recherche de groupes de clés

1) Sélectionnez **Informations système » Groupes de clés**.

   La liste de tous les groupes de clés apparaît.

Groupes de clés

Les symboles suivants sont utilisés :

- Groupe de clé normale
- Groupe de clé dynamique

2) Saisissez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

   En tapant **Notes** dans le champ de recherche, toutes les notes correspondantes apparaîtront sous forme d'une liste à sélectionner.

3) Cliquez sur **Rechercher**.

4) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur la ligne du groupe de clés correspondant.

4.3.2 Modification des informations de groupe de clé

1) Trouvez le groupe de clés et accédez à ses informations détaillées.

   Voir *Chapitre 4.3.1 "Recherche de groupes de clés", page 53*.

2) Cliquez sur **Modifier**.

3) Pour modifier le nom du groupe de clés, saisissez le nom.

4) Pour ajouter une note, cliquez sur **Ajouter note**. Voir également *Chapitre 4.3.3 "Ajout ou suppression de notes de groupes de clés", page 54*.

5) Cliquez sur **Enregistrer**.

4.3.3 Ajout ou suppression de notes de groupes de clés

1) Localisez le groupe de clés.

   Pour rechercher le groupe de clés, *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

2) - Pour ajouter ou supprimer des notes pour un groupe de clés, allez à l'*Étape 3*.
   - Pour ajouter ou supprimer des notes pour plusieurs groupes de clés, allez à l'*Étape 4*.

3) **Ajouter ou supprimer des notes pour un groupe de clés :**

   1. Sélectionnez le groupe de clés et accédez à ses informations détaillées.
   2. Cliquez sur **Modifier**.
   3. Ajouter ou supprimer une note pour un groupe de clés.

      Pour ajouter une note :

      a) Cliquez sur **Ajouter note...**.
      b) Saisissez un nom pour la note.
      c) Cliquez sur **OK**.

      Pour supprimer une note :
      Cliquez sur la note à supprimer.

   4. Cliquez sur **Enregistrer**.

4) **Ajouter ou supprimer des notes pour plusieurs groupes de clés :**

   1. Sélectionnez les groupes de clés dans les résultats de recherche en cochant les cases correspondantes.

2. **Pour ajouter une note :**

   a) Cliquez sur **Ajouter note...**.

   b) Entrez un nom pour la note.

   c) Cliquez sur **OK**.

   Pour supprimer une note :

   a) Cliquez sur **Supprimer note...**.

   b) Entrez un nom pour la note.

   c) Cliquez sur **OK**.

Voir également *Chapitre 8.2.6 "Notes", page 183*.

4.3.4 Affichage des membres d'un groupe de clé

1) Trouvez le groupe de clés et accédez à ses informations détaillées.

   Voir *Chapitre 4.3.1 "Recherche de groupes de clés", page 53*.

2) Sélectionnez l'onglet **Membres**.

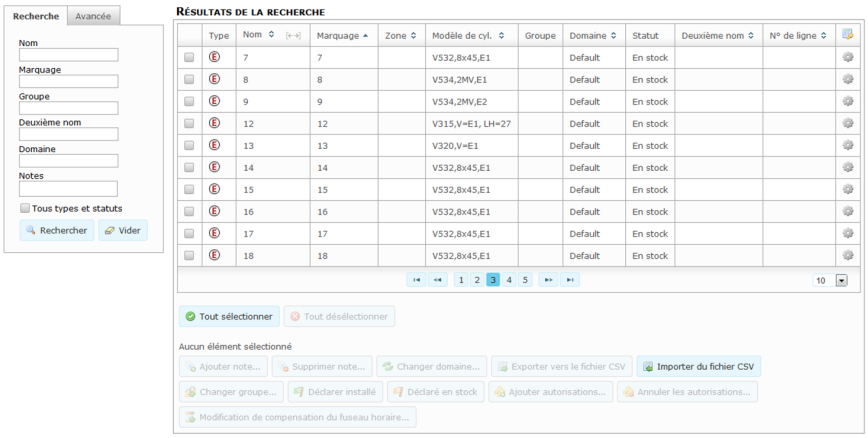
   La liste de toutes les clés de ce groupe de clés s'affiche.

4.4 Gestion des cylindres

4.4.1 Recherche de cylindres

1) Sélectionnez **Informations système » Cylindres**.

   Une liste de tous les cylindres, sauf les cylindres mécaniques et défectueux, est affichée.



   Les symboles suivants sont utilisés :

   E — Cylindre électronique

   M — Cylindre mécanique

   EM — Double cylindre (notre exemple : Entrée A électronique et entrée B mécanique)

2) Sélectionnez l'onglet **Rechercher** ou **Avancée**.

Par défaut, les cylindres mécaniques et défectueux ne s'affichent pas. Pour inclure également tous ces cylindres dans les résultats de recherche, sélectionnez **Tous types et statuts**.

L'onglet **Avancée** inclut également les champs de recherche Type de cylindre, Statut inventaire, Statut opérationnel, Second marquage et, via une liste déroulante, des champs personnalisés (si définis dans **Réglages du système**. Ce réglage s'obtient en sélectionnant **Administration » Réglages du système » ADMINISTRATION » Champs client de cylindre**).

3) Saisissez les critères de recherche.

Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

En tapant **Notes** dans le champ de recherche, toutes les notes correspondantes apparaîtront sous forme d'une liste à sélectionner.

4) Cliquez sur **Rechercher**.

5) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur la ligne du cylindre correspondant.

Pour plus d'informations sur les attributs de cylindre, voir *Chapitre 9.3.5 "Attributs de cylindre", page 204*.

4.4.2 Modification des informations de cylindre

1) Trouvez le cylindre et accédez à ses informations détaillées.

Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

Si **Deuxième nom** ou **Champs client** doivent être modifiés, passez à l'*Étape 6*.

2) Cliquez sur **Modifier**.

3) Modifiez les champs.

Pour plus d'informations sur les attributs de cylindre, voir *Chapitre 9.3.5 "Attributs de cylindre", page 204*.

4)
- Pour ajouter une note, cliquez sur **Ajouter note**. Voir également *Chapitre 4.4.3 "Ajout ou suppression de notes de cylindre", page 57*
- Pour ajouter un lien externe, cliquez sur **Ajouter lien externe**. Voir également *Chapitre 4.4.4 "Gestion des liens externes d'un cylindre", page 57*

5) Cliquez sur **Enregistrer**.

6) **Deuxième nom** et **Champs client** sont modifiés dans l'onglet **Informations complémentaires**.

> **REMARQUE !**
> Champs client définis dans **Réglages du système**. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

a) Sélectionnez l'onglet **Informations complémentaires**.

b) Cliquez sur **Modifier**.

c) Mettez le champ à jour.

d) Cliquez sur **Enregistrer**.

4.4.3 Ajout ou suppression de notes de cylindre

Pour des informations sur les notes, voir *Chapitre 8.2.6 "Notes", page 183*.

1) Sélectionnez **Informations système » Cylindres**.

   La liste de tous les cylindres s'affiche.

   - Pour ajouter ou supprimer des notes pour un cylindre, allez à l'*Étape 2*.
   - Pour ajouter ou supprimer des notes pour plusieurs cylindres, allez à l'*Étape 3*.

2) **Pour ajouter ou supprimer des notes pour un cylindre :**

   1. Sélectionnez le cylindre et accédez à ses informations détaillées.
   2. Cliquez sur **Modifier**.
   3. Ajouter ou supprimer une note pour un cylindre.

      Pour ajouter une note :

      a) Cliquez sur **Ajouter note...**.
      b) Saisissez un nom pour la note.
      c) Cliquez sur **OK**.

      Pour supprimer une note :
      Cliquez sur la note à supprimer.
   4. Cliquez sur **Enregistrer**.

3) **Pour ajouter ou supprimer des notes pour plusieurs cylindres :**

   1. Sélectionnez des cylindres dans les résultats de recherche en cochant les cases correspondantes.
   2. **Ajout d'une note :**

      a) Cliquez sur **Ajouter note...**.
      b) Entrez un nom pour la note.
      c) Cliquez sur **OK**.

      Suppression d'une note :

      a) Cliquez sur **Supprimer note...**.
      b) Entrez un nom pour la note.
      c) Cliquez sur **OK**.

4.4.4 Gestion des liens externes d'un cylindre

Pour des informations sur les liens externes, voir *Chapitre 8.4 "Liens externes", page 186*.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Cliquez sur **Modifier**.
3) **Pour ajouter un lien externe :**

   1. Cliquez sur **Ajouter.**

2. Saisissez un **Nom** pour l'URL.
3. Saisissez l'**URL**. L'**URL** doit commencer par un protocole (http:// ou ftp://, par exemple).

   Si une URL racine a été définie dans les **Réglages système** (élément **Liens externes, URL racine**) il suffit d'ajouter la dernière partie de l'URL. Voir également *Chapitre 6.4 "Modifier les réglages du système", page 100*.
4. Cliquez sur **OK**.

Pour modifier un lien externe :

1. Cliquez sur **Modifier** à côté du lien externe à modifier.
2. Mettez les champs à jour.
3. Cliquez sur **OK**.

Pour supprimer un lien externe :

Cliquez sur **Supprimer** à côté du lien externe à supprimer.

4) Cliquez sur **Enregistrer**.

4.4.5 Affichage des groupes de clés et des exceptions sur une liste d'accès de cylindres

L'onglet **Clés dans la liste d'accès** est utilisé pour afficher les groupes de clés et les exceptions sur la liste d'accès de cylindres.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.
2) Sélectionnez l'onglet **Clés dans la liste d'accès**.

   Une liste de tous les groupes de clés et les exceptions de la liste d'accès des cylindres est affichée. Pour la modifier, voir *Chapitre 4.9.2 "Configuration des autorisations dans les cylindres", page 81*.

4.4.6 Affichage de l'historique des mises à jour d'un cylindre

L'onglet Historique de mise à jour est utilisé pour la traçabilité de la programmation des clés.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.
2) Sélectionnez l'onglet **Historique de mise à jour**.

   La liste de toutes les mises à jour de cylindre apparaît.

   Les symboles suivants sont utilisés :

   - La tâche de programmation existe mais n'a pas été commencée
   - La tâche de programmation a été programmée pour la clé de programmation
   - La tâche de programmation est terminée
   - La tâche de programmation a échoué ou a été annulée
   - La tâche de programmation a été remplacée par une nouvelle tâche

3) Pour afficher les détails complémentaires d'une mise à jour spécifique, cliquez sur le lien dans la colonne **Type**.

4.4.7 Affichage des événements d'un cylindre

L'onglet **Événements** est utilisé pour la traçabilité des opérations administrateur dans CWM, telles que la déclaration d'un cylindre défectueux.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Sélectionnez l'onglet **Événements**.

   La liste de tous les événements de cylindre s'affiche.

4.4.8 Modification du fuseau horaire d'un cylindre

Le fuseau horaire peut être modifié pour les cylindres dans un domaine s'ils sont situés dans des fuseaux horaires différents. Ce réglage est uniquement disponible pour les cylindres de 2e génération.

Pour plus d'informations sur les générations de clé, voir *Chapitre 7.2.5 "Générations de clé", page 162*.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Cliquez sur **Modification du fuseau horaire...**.

3) Réglez **Compensation du fuseau horaire** sur le nombre de minutes souhaité.

4) Régler la priorité des tâches.

5) Cliquez sur **OK**.

   Un travail de programmation de cylindre est créé. Pour programmer le cylindre, voir *Chapitre 4.4.13 "Programmation des cylindres", page 62*.

> **REMARQUE !**
>
> Le bouton **Annulation de la modification du fuseau horaire** est affiché dans les informations détaillées du cylindre lorsque la tâche de programmation est en attente d'exécution.
>
> Cliquez sur le bouton, tout en modifiant, pour annuler la modification du fuseau horaire.

Le fuseau horaire peut être modifié simultanément pour plusieurs cylindres. Sélectionnez les cylindres dans la liste des résultats de recherche et cliquez sur **Compensation du fuseau horaire**.

4.4.9 Modification du statut du cylindre

Le statut d'inventaire des cylindres est soit **en stock**, soit **installé**. Leur statut opérationnel est soit **opérationnel**, soit **défectueux**.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) **Pour passer au statut Installé**

   1. Cliquez sur **Déclarer installé**.

2. Cliquez sur **OK**.

   Il est possible de déclarer simultanément le statut de plusieurs cylindres comme Installé. Sélectionnez les cylindres dans la liste des résultats de recherche et cliquez sur **Déclarer installé**.

Pour passer au statut En stock

1. Cliquez sur **Déclaré en stock**.
2. Cliquez sur **OK**.

   Il est possible de déclarer simultanément le statut de plusieurs cylindres comme étant En stock. Sélectionnez les cylindres dans la liste des résultats de recherche et cliquez sur **Déclaré en stock**.

Déclarer comme défectueux

1. Cliquez sur **Déclarer défectueux**.
2. Sélectionnez **Déclarer défectueux uniquement**.

   Si un processus de remplacement est nécessaire, voir *Chapitre 4.4.10 "Remplacement d'un cylindre défectueux", page 60*.
3. Cliquez sur **Suivant**.
4. Cliquez sur **Appliquer**.

Pour déclarer la remise en service du cylindre

1. Cliquez sur **Déclarer opérationnel**.

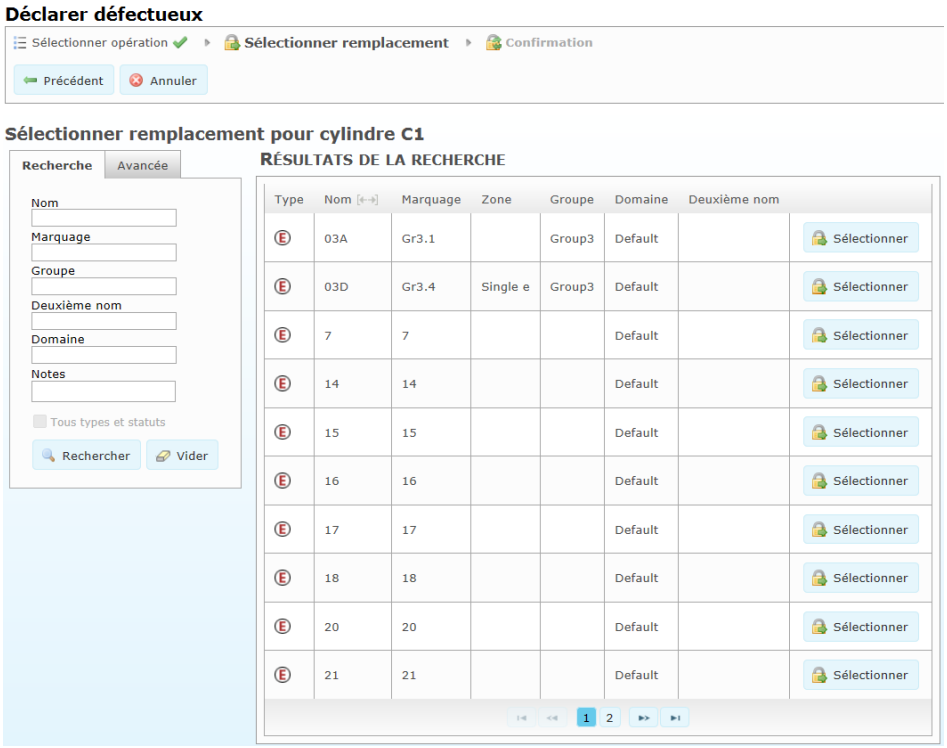
   Cette option est uniquement disponible pour les cylindres précédemment déclarés comme défectueux.
2. Cliquez sur **OK**.
3. Une tâche de programmation est créée.

4.4.10 Remplacement d'un cylindre défectueux

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.
2) Cliquez sur **Déclarer défectueux**.
3) Sélectionnez **Déclarer défectueux et remplacer par un autre cylindre**.
4) Cliquez sur **Suivant**.

Une liste de tous les cylindres de même type que le cylindre déclaré, présents en stock, s'affiche.



5) Pour rechercher les cylindres spécifiques, saisissez les critères de recherche et cliquez sur **Rechercher**.

6) Sélectionnez un cylindre de remplacement en cliquant sur **Sélectionner**.

7) Sélectionnez un niveau **Priorité**.

   Les tâches urgentes doivent disposer d'un niveau de priorité élevé.

8) Cliquez sur **Appliquer**.

   La configuration existante, y compris les mises à jour en attente, du cylindre de remplacement est ignorée et remplacée par la configuration du cylindre défectueux.

   Les traitements de mise à jour à distance sont créés pour les clés associées et les profils d'accès donnant accès au cylindre défectueux sont mis à jour.

4.4.11 Remplacement d'un cylindre avec un clone d'usine

Si un clone de remplacement est livré de l'usine à la suite d'un cylindre défectueux, les étapes suivantes doivent être prises pour assurer la fonctionnalité du cylindre.

1) Lorsque le cylindre cloné arrive de l'usine, allez sur **Administration » Importation d'extension » Télécharger ou récupérer le(s) fichier(s) d'importation d'extension** pour télécharger le fichier CWS fourni sur CWM (si l'intégration DCS est désactivée) ou récupérer le fichier du DCS.

2) Créez une tâche de programmation pour le cylindre de remplacement. Voir *Chapitre 4.4.12 "Demande d'une reprogrammation de cylindre", page 62*.

3) Programmez le cylindre de remplacement. Voir *Chapitre 4.4.13 "Programmation des cylindres", page 62*.

4) Le cylindre de remplacement est prêt à être utilisé.

4.4.12 Demande d'une reprogrammation de cylindre

Lorsqu'un cylindre est reprogrammé, le contenu de sa mémoire est effacé, y compris les journaux des événements. La liste d'accès du cylindre est restaurée lors de sa reprogrammation. Pour réaliser la tâche de reprogrammation de cylindre, il faut disposer d'une clé de programmation maîtresse ou d'une clé normale avec des droits de reprogrammation des cylindres.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Cliquez sur **Reprogrammer**.

   Pour les cylindres à double entrée, cliquez sur **Reprogrammation du côté A**, **Reprogrammation du côté B** ou les deux.

3) Sélectionnez **Priorité**.

   Les tâches urgentes doivent disposer d'une priorité élevée.

4) Cliquez sur **OK**.

Voir également *Chapitre 4.4.13 "Programmation des cylindres", page 62*.

4.4.13 Programmation des cylindres avec une clé de programmation

Conditions préalables :

- Une clé de programmation avec la permission de **Programmation du cylindre**
- Pour des tâches impliquant la modification du groupe auquel appartient le cylindre : une clé de programmation avec **Programmation du groupe de cylindres**
- Pour des tâches de reprogrammation : Une clé de programmation maîtresse ou une clé de programmation normale avec des droits de **Reprogrammation de cylindre**

Si la clé de programmation à utiliser est immédiatement disponible, suivez la procédure décrite *Chapitre 4.4.13.1 "Programmation des cylindres à l'aide de la clé de programmation avec boîtier de programmation local", page 62*.

Si la clé de programmation à utiliser n'est pas immédiatement disponible, suivez la procédure décrite *Chapitre 4.4.13.2 "Programmation des cylindres à l'aide de la clé de programmation Connect ou de la clé de programmation avec boîtier de programmation à distance", page 64*. Cette procédure nécessite un boîtier de programmation à distance ou une clé de programmation CLIQ Connect.

Pour plus d'informations sur la programmation de cylindre, consultez *Chapitre 8.5 "Programmation de cylindre", page 187*.

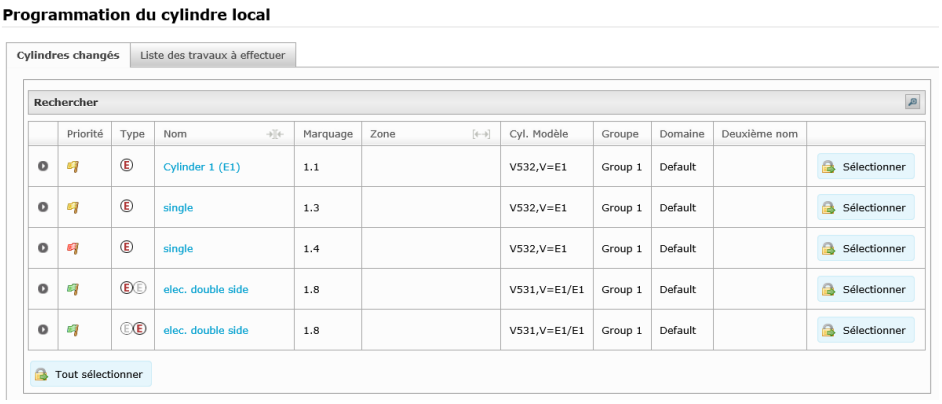
4.4.13.1 Programmation des cylindres à l'aide de la clé de programmation avec boîtier de programmation local

Pour envoyer des tâches de programmation à une clé de programmation immédiatement disponible et programmer des cylindres :

1) Sélectionnez **Tâches » Programmation du cylindre**.

   La liste des cylindres nécessitant une programmation s'affiche. Le niveau de priorité des tâches est indiqué dans la colonne la plus à gauche.

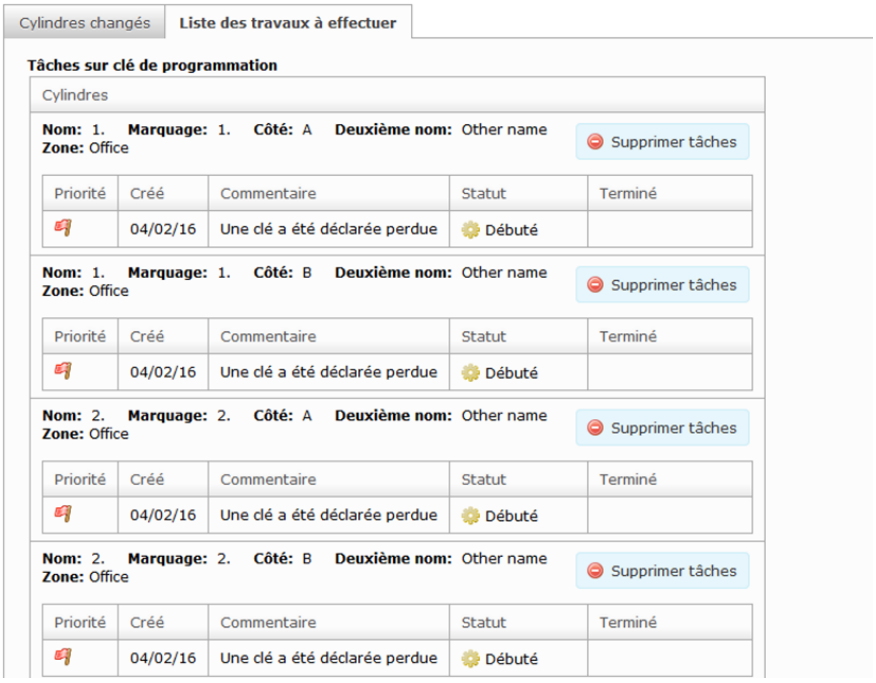
2) Pour sélectionner les tâches à exécuter, cliquez sur **Sélectionner** dans la liste ou sur **Tout sélectionner** (sous la liste).



3) Cliquez sur **Envoyer à la clé de programmation**.

> **REMARQUE !**
> Lorsqu'une tâche de programmation de cylindre est chargée sur une clé de programmation, les réglages d'autorisation de ce cylindre ne sont pas modifiables dans CWM.

- Pour afficher la liste des tâches présentes sur la clé de programmation, sélectionnez l'onglet **Liste des tâches à effectuer**.



- Pour imprimer la liste, cliquez sur **Imprimer la liste des traitements à effectuer**.

4) Insérez la clé de programmation dans chaque cylindre à programmer tour à tour.

ATTENTION !
Laissez la clé de programmation insérée jusqu'à la fin de la tâche de programmation.

En cas d'échec de la tâche, insérez la clé de programmation dans le boîtier de programmation à distance connecté à CWM afin de recharger la tâche de programmation sur la clé de programmation. Voir également *"Reprogrammation"*.

5) Connectez-vous de nouveau à CWM.
6) Sélectionnez **Tâches » Programmation du cylindre**.
7) Sélectionnez l'onglet **Liste des travaux à effectuer**.
8) Cliquez sur **Mettre à jour**.

   Le statut des tâches de programmation est chargé à partir de la clé de programmation.
9) Facultatif : Cliquez sur **Supprimer traitements terminés**.

4.4.13.2 Programmation des cylindres à l'aide de la clé de programmation Connect ou de la clé de programmation avec boîtier de programmation à distance

Tout au long de la procédure de programmation des tâches de cylindres, l'état de l'interaction avec le boîtier de programmation à distance est indiqué par des LED. Pour plus d'informations sur ces indications, voir *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211* ou *Chapitre 9.5.2 "Indications de boîtier de programmation mural (génération 2)", page 212*.

1) Attribuez les tâches de programmation de cylindre à une clé de programmation :
   a) Localisez la clé de programmation.

      Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*
   b) Sélectionnez l'onglet **Programmation du cylindre**.
   c) Cliquez sur **Attribuer cylindres pour programmation**.
   d) Cliquez sur **Sélectionner** pour chaque tâche de programmation de cylindre à exécuter.

      AVERTISSEMENT !
      Pour les tâches incluant des changements de groupe de cylindres, un maximum de 100 tâches peut être attribué à une clé de programmation. L'attribution d'un plus grand nombre de tâches pourrait entraîner des erreurs de programmation.
   e) Cliquez sur **Appliquer**.

      Après l'attribution à la clé de programmation de la tâche de programmation de cylindre, un e-mail est créé pour le possesseur de la clé de programmation indiquant que des tâches de programmation sont à récupérer.
2) Insérez la clé de programmation dans un boîtier de programmation distant ou connectez la clé de programmation Connect à CLIQ Connect pour charger les tâches de programmation de cylindres.

Une fois la tâche de programmation de cylindre transférée, un e-mail est créé pour le possesseur de la clé de programmation indiquant quels cylindres programmer.

3) Insérez la clé de programmation dans les cylindres à programmer.

> **ATTENTION !**
> Laissez la clé insérée jusqu'à la fin de la tâche de programmation.
>
> En cas d'échec de la tâche, insérez la clé dans le boîtier de programmation à distance connecté à CWM afin de recharger la tâche de programmation sur la clé. Voir également *"Reprogrammation"*.

4) Insérez la clé de programmation dans un boîtier de programmation distant ou connectez la clé de programmation Connect à CLIQ Connect pour mettre à jour le statut des tâches de programmation.

4.4.14 Importation des informations de cylindre

Importation des informations de cylindre permet d'importer en masse des données de cylindre mises à jour. La fonction est uniquement applicable pour la mise à jour de données de cylindre existantes.

Un fichier CSV est utilisé pour l'importation. La manière la plus simple d'écrire un fichier CSV est d'exporter un fichier CSV avec des données de cylindre existantes et ensuite de modifier le fichier exporté dans Excel ou un éditeur de texte. Voir *Chapitre 4.4.15 "Exportation des informations de cylindre", page 66*.

> **REMARQUE !**
> Les informations de cylindre peuvent être importées comme des fichiers CSV, mais aussi comme des **fichiers d'importation d'extension**, mais le contenu ne se recoupe pas. Les fichiers CSV mettent à jour les informations de cylindre que les utilisateurs peuvent modifier dans le GUI alors que les fichiers d'importation d'extension mettent à jour les données d'usine non modifiables. Les fichiers CSV ne peuvent donc pas remplacés les extensions et vice-versa. Pour plus d'informations sur les extensions, voir *Chapitre 6.16 "Importation d'extensions", page 155*.

1) Cliquez sur **Informations système » Cylindres**.
2) Cliquez sur **Importer du fichier CSV**.
3) Cliquez sur **Sélectionner** pour trouver le fichier enregistré localement sur l'ordinateur.
4) Cliquez sur **Ouvrir**.
5) Cliquez sur **Importer** pour importer et valider le fichier.

   Affiche des informations sur le nombre d'entrées valides contenues dans le fichier. Si le fichier ne respecte pas les spécifications, l'importation est impossible.

REMARQUE !
Lors de l'importation des informations de cylindre, seules les colonnes suivantes du fichier CSV sont mises à jour.

- Nom
- Deuxième nom
- Zone
- Statut inventaire
- Champs client (si défini dans **Réglages du système**)

Les données de cylindre existantes sont remplacées.

REMARQUE !
Pour importer des informations de cylindre depuis un fichier CSV, les valeurs de **Marquage** ou les valeurs combinées de **Marquage** et **Deuxième marquage** doivent être uniques.

4.4.15 Exportation des informations de cylindre

1) Recherchez les cylindres.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Dans les résultats de recherche de cylindre, sélectionnez les cylindres dont vous souhaitez exporter les données.

3) Cliquez sur **Exporter vers le fichier CSV**.

   REMARQUE !
   Pour pouvoir ouvrir correctement le fichier dans Excel, le délimiteur du fichier doit être défini selon les réglages régionaux. Pour modifier le délimiteur, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

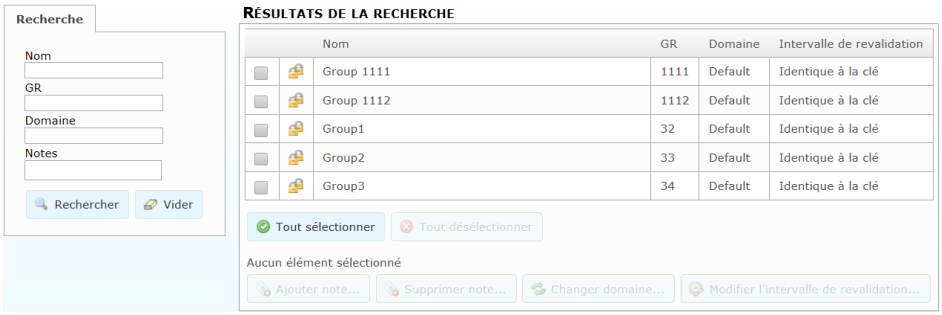
4) Dans la fenêtre contextuelle de téléchargement de fichier, cliquez sur **Ouvrir** ou sur **Enregistrer**.

4.5 Gestion des groupes de cylindres

4.5.1 Recherche de groupes de cylindres

1) Sélectionnez **Informations système » Groupes de cylindres**.

   La liste de tous les groupes de cylindres apparaît.



2) Saisissez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

   En tapant **Notes** dans le champ de recherche, toutes les notes correspondantes apparaîtront sous forme d'une liste à sélectionner.

3) Cliquez sur **Rechercher**.

4) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur le groupe de cylindres correspondant.

4.5.2 Modification des informations de groupe de cylindres

1) Trouvez le groupe de cylindres et accédez à ses informations détaillées.

   Voir *Chapitre 4.5.1 "Recherche de groupes de cylindres", page 67*.

2) Cliquez sur **Modifier**.

3) Pour modifier le nom du groupe de cylindres, mettez le champ **Nom** à jour.

4) Pour ajouter une note, cliquez sur **Ajouter note...**. Voir également *Chapitre 4.5.3 "Ajout ou suppression de notes de groupes de cylindres", page 67*

5) Pour changer de domaine, cliquez sur **Changer domaine...**. Voir également *Chapitre 6.6.8 "Changement du domaine de groupes de cylindres", page 128*.

6) Cliquez sur **Enregistrer**.

4.5.3 Ajout ou suppression de notes de groupes de cylindres

1) Localisez le groupe de cylindres.

   Pour rechercher le groupe de cylindres, *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

2) - Pour ajouter ou supprimer des notes pour un groupe de cylindres, allez à l'*Étape 3*.
   - Pour ajouter ou supprimer des notes pour plusieurs groupes de cylindres, allez à l'*Étape 4*.

3) **Ajouter ou supprimer des notes pour un groupe de cylindres :**

1. Sélectionnez le groupe de cylindres et accédez à ses informations détaillées.
2. Cliquez sur **Modifier**.
3. Ajouter ou supprimer une note pour un groupe de cylindres.

Pour ajouter une note :

a) Cliquez sur **Ajouter note...**.
b) Saisissez un nom pour la note.
c) Cliquez sur **OK**.

Pour supprimer une note :
Cliquez sur la note à supprimer.

4. Cliquez sur **Enregistrer**.

4) **Ajouter ou supprimer des notes pour plusieurs groupes de cylindres :**

1. Sélectionnez les groupes de cylindres dans les résultats de recherche en cochant les cases correspondantes.
2. **Pour ajouter une note :**

a) Cliquez sur **Ajouter note...**.
b) Entrez un nom pour la note.
c) Cliquez sur **OK**.

Pour supprimer une note :

a) Cliquez sur **Supprimer note...**.
b) Entrez un nom pour la note.
c) Cliquez sur **OK**.

Voir également *Chapitre 8.2.6 "Notes", page 183*.

4.5.4 Affichage des membres d'un groupe de cylindres

1) Trouvez le groupe de cylindres et accédez à ses informations détaillées.

Voir *Chapitre 4.5.1 "Recherche de groupes de cylindres", page 67*.

2) Sélectionnez l'onglet **Membres**.

La liste de tous les cylindres de ce groupe apparaît.

4.5.5 Affichage des événements d'un groupe de cylindres

L'onglet Événements est utilisé pour la traçabilité des opérations administrateur dans CWM, telles que le changement de domaine d'un groupe de cylindres.

1) Trouvez le groupe de cylindres et accédez à ses informations détaillées.

Voir *Chapitre 4.5.1 "Recherche de groupes de cylindres", page 67*.

2) Sélectionnez l'onglet **Événements**.

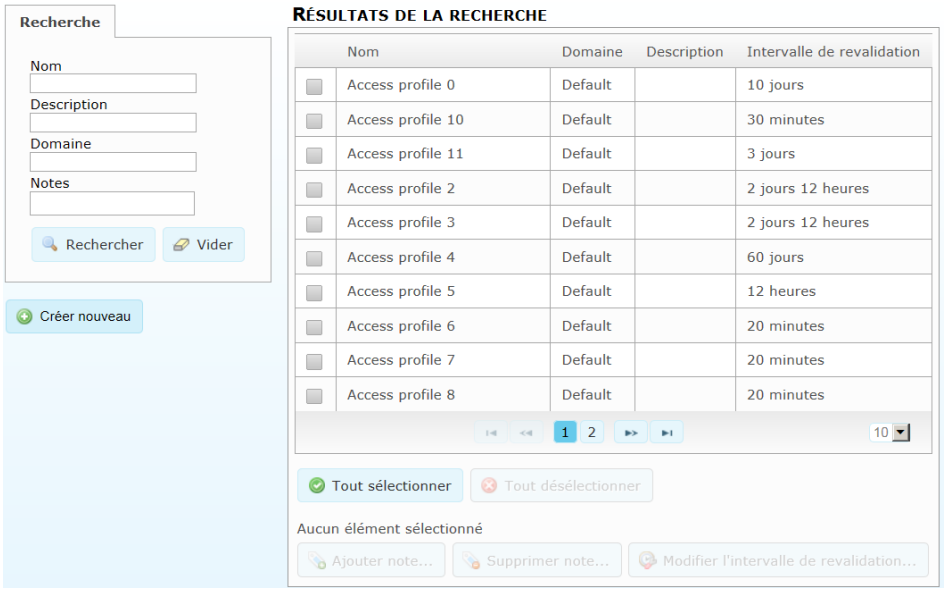
La liste de tous les événements du groupe de cylindres s'affiche.

4.6 Gestion des profils d'accès

4.6.1 Recherche de profils d'accès

1) Sélectionnez **Informations système » Profils d'accès**.

   La liste de tous les profils d'accès apparaît.



2) Saisissez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

3) Cliquez sur **Rechercher**.

4) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur le profil d'accès correspondant.

4.6.2 Création et suppression de profils d'accès

Les profils d'accès s'appliquent uniquement aux clés dynamiques prenant en charge les mises à jour à distance. Ils s'appliquent à une clé ou à une personne.

1) Sélectionnez **Informations système » Profils d'accès**.

2) Pour créer un profil d'accès :

   a) Cliquez sur **Créer nouveau**.

   b) Saisissez le **Nom** et éventuellement une **Description**.

> **REMARQUE !**
> Le champ du nom doit être unique.

   c) Pour changer le domaine par défaut :

   - Cliquez sur **Changer domaine**
   - Cliquez sur **Sélectionner** pour le domaine correspondant.

d) Pour ajouter une note, cliquez sur **Ajouter note**. Voir également *Chapitre 4.6.4 "Ajout ou suppression de notes de profil d'accès", page 70*

e) Pour ajouter un lien externe, cliquez sur **Ajouter lien externe**. Voir également *Chapitre 4.6.5 "Modification de liens externes de profil d'accès", page 71*

f) Cliquez sur **Enregistrer**.

3) Pour supprimer un profil d'accès :

a) Localisez le profil d'accès et affichez les informations détaillées.

Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

b) Cliquez sur **Supprimer**.

c)
- Si aucune clé ou personne n'est associée au profil :

  Cliquez sur **Supprimer le profil**.
- Si des clés ou personnes sont associées au profil :

  a) Confirmez que les profils d'accès ont été supprimés définitivement, puis cochez la case.

  b) Cliquez sur **Supprimer le profil**.

Voir également *Chapitre 8.2.4 "Profils d'accès", page 179*.

4.6.3 Modification des informations de profil d'accès

1) Trouvez le profil d'accès et accédez à ses informations détaillées.

Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

2) Cliquez sur **Modifier**.

3) Mettez les champs à jour.

4) Pour ajouter des notes, cliquez sur **Ajouter note...**. Voir également *Chapitre 4.1.7 "Ajout ou suppression de notes employés ou visiteurs", page 31*.

5) Pour ajouter ou modifier des liens externes, cliquez sur **Ajouter lien externe...**. Voir également *Chapitre 4.1.8 "Gestion des liens externes employé ou visiteur", page 32*.

6) Cliquez sur **Enregistrer**.

4.6.4 Ajout ou suppression de notes de profil d'accès

1) Localisez le profil d'accès.

Pour rechercher le profil d'accès, voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

2)
- Pour ajouter ou supprimer des notes pour un profil d'accès, allez à l'*Étape 3*.
- Pour ajouter ou supprimer des notes pour plusieurs profils d'accès, allez à l'*Étape 4*.

3) **Ajouter ou supprimer des notes pour un profil d'accès :**

1. Sélectionnez le profil d'accès et accédez à ses informations détaillées.
2. Cliquez sur **Modifier**.
3. Ajouter ou supprimer une note pour un profil d'accès.

Pour ajouter une note :

a) Cliquez sur **Ajouter note...**.

b) Saisissez un nom pour la note.

c) Cliquez sur **OK**.

Pour supprimer une note :
Cliquez sur la note à supprimer.

4. Cliquez sur **Enregistrer**.

4) **Ajouter ou supprimer des notes pour plusieurs profils d'accès :**

1. Sélectionnez des profils d'accès dans les résultats de recherche en cochant les cases correspondantes.
2. **Pour ajouter une note :**

a) Cliquez sur **Ajouter note...**.

b) Entrez un nom pour la note.

c) Cliquez sur **OK**.

Pour supprimer une note :

a) Cliquez sur **Supprimer note...**.

b) Entrez un nom pour la note.

c) Cliquez sur **OK**.

Pour plus d'informations sur les notes, voir *Chapitre 8.2.6 "Notes", page 183*.

4.6.5 Modification de liens externes de profil d'accès

1) Trouvez le profil d'accès et accédez à ses informations détaillées.

Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

2) Cliquez sur **Modifier**.

3) Pour ajouter un lien externe :

a) Cliquez sur **Ajouter.**

b) Saisissez un **Nom** pour l'URL.

c) Saisissez l'**URL**. L'**URL** doit commencer par un protocole (http:// ou ftp://, par exemple).

Si une URL racine a été définie dans les **Réglages du système**, il suffit d'ajouter la dernière partie de l'URL. Voir également *Chapitre 6.4 "Modifier les réglages du système", page 100*.

d) Cliquez sur **OK**.

4) Un lien externe peut être supprimé en cliquant sur **Supprimer** pour ce lien.

5) Pour modifier un lien externe :

a) Cliquez sur **Modifier** à côté du lien externe à modifier.

b) Mettez les champs à jour.

c) Cliquez sur **OK**.

6) Cliquez sur **Enregistrer**.

Voir également *Chapitre 8.4 "Liens externes", page 186*.

4.6.6 Affichage des clés associées à un profil d'accès

L'onglet **Clés** affiche toutes les clés associées au profil d'accès sélectionné. Il affiche également les clés des groupes d'accès temporaires expirés associés au profil d'accès sélectionné.

1) Trouvez le profil d'accès et accédez à ses informations détaillées.

   Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

2) Sélectionnez l'onglet **Clés**.

   La liste de toutes les clés dotées du profil d'accès est affichée.

4.6.7 Affichage des événements d'un profil d'accès

L'onglet Événements est utilisé pour la traçabilité des opérations administrateur dans CWM, telles que l'ajout et la suppression de cylindres dans un profil d'accès.

1) Trouvez le profil d'accès et accédez à ses informations détaillées.

   Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

2) Sélectionnez l'onglet **Événements**.

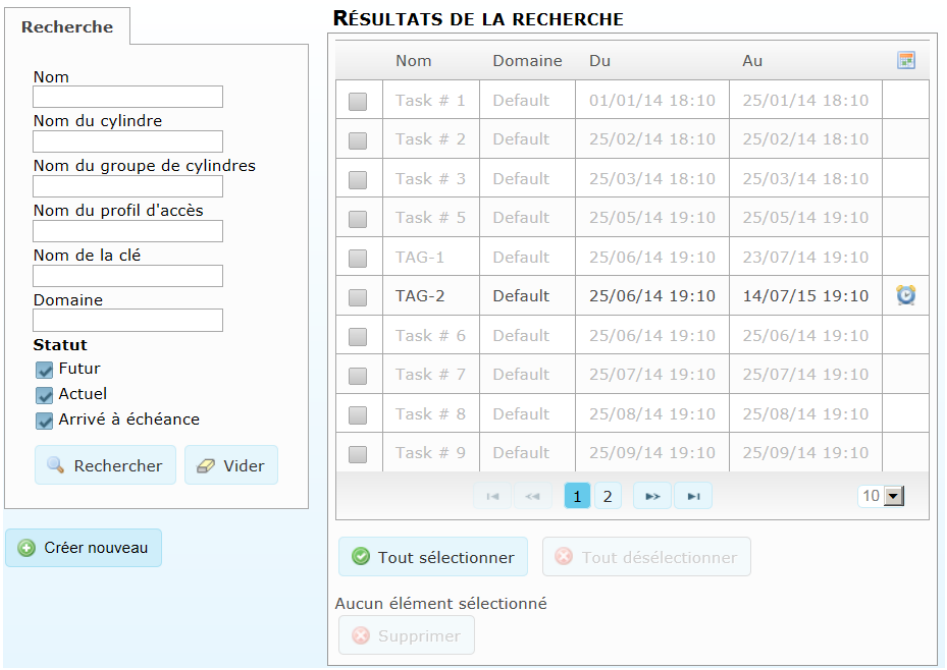
   La liste de tous les événements de profil d'accès s'affiche.

4.7 Gestion des groupes d'accès temporaires

4.7.1 Recherche de groupes d'accès temporaires

1) Sélectionnez **Informations système » Groupes d'accès temporaires**.

   La liste de tous les groupes d'accès temporaires s'affiche.



2) Saisissez les critères de recherche.

Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

3) Pour filtrer la recherche :

   a) Cochez la case **Arrivé à échéance** pour afficher les groupes d'accès temporaires qui ne sont plus valides.

      Dans la liste des résultats, les groupes d'accès temporaires arrivés à échéance sont formatés avec un texte gris.

   b) Cochez la case **Actuel** pour afficher les groupes d'accès temporaires actuellement valides.

      Dans la liste des résultats, les groupes d'accès temporaires actuellement valides sont formatés avec un texte noir et indiqués par une icône :

   c) Cochez la case **Futur** pour afficher les groupes d'accès temporaires qui seront valides dans le futur.

      Dans la liste des résultats, les groupes d'accès temporaires qui seront valides sont formatés avec un texte noir.

4) Cliquez sur **Rechercher**.

5) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur le groupe d'accès temporaire correspondant.

4.7.2 Création et suppression des groupes d'accès temporaires

Les groupes d'accès temporaires s'appliquent uniquement aux clés dynamiques prenant en charge les mises à jour à distance. Ils s'appliquent à une clé.

1) Sélectionnez **Informations système » Groupes d'accès temporaires**.

2) Pour créer un groupe d'accès temporaire :

   a) Cliquez sur **Créer nouveau**.

   b) Saisissez l'**Nom**.

   c) Saisissez les valeurs de période **Du** et **Au** (date).

   > **REMARQUE !**
   > Lorsque le groupe d'accès temporaire n'est plus valide pour une clé, un traitement à distance sera automatiquement créé pour supprimer l'accès au groupe d'accès temporaire de cette clé. Cependant, l'annulation de l'accès de cette clé ne prendra effet que lorsque la clé est mise à jour dans une borne d'actualisation.

   d) Pour changer le domaine par défaut :

   - Cliquez sur **Changer domaine**
   - Cliquez sur **Sélectionner** pour le domaine correspondant.

   e) Cliquez sur **Enregistrer**.

3) Pour supprimer un groupe d'accès temporaire :

   a) Localisez le groupe d'accès temporaire et affichez les informations détaillées.

      Voir *Chapitre 4.7.1 "Recherche de groupes d'accès temporaires", page 72*.

   b) Cliquez sur **Supprimer**.

   c) Cliquez sur **OK**.

Il est également possible de créer un groupe d'accès temporaire à partir de la vue de clé. Sur la fenêtre d'informations détaillées, sélectionnez l'onglet **Groupes d'accès temporaires**, cliquez sur **Créer nouveau** et suivez les instructions données ci-dessus, en commençant par *Étape 2 b*.

Voir également *Chapitre 8.2.5 "Groupes d'accès temporaires", page 181*.

4.7.3 Modification des groupes d'accès temporaires

1) Trouvez le groupe de profils d'accès et accédez à ses informations détaillées.

   Voir *Chapitre 4.7.1 "Recherche de groupes d'accès temporaires", page 72*.

2) Dans la fenêtre des informations détaillées, cliquez sur **Modifier**.

3) Mettez les champs à jour.

4) Cliquez sur **Enregistrer**.

4.7.4 Ajout ou suppression de clés des groupes d'accès temporaires

REMARQUE !
Lorsqu'un groupe d'accès temporaire n'est plus valide pour une clé, un traitement à distance sera automatiquement créé pour supprimer l'accès au groupe d'accès temporaire de cette clé. Cependant, l'annulation de l'accès de cette clé ne prendra effet que lorsque la clé est mise à jour dans une boîtier de programmation à distance. Pour empêcher que le possesseur de la clé n'utilise la clé après l'expiration du groupe d'accès temporaire, effectuez une des opérations suivantes avant d'ajouter des clés :

- Réglez **Active entre les dates sélectionnées** dans les réglages d'activation, voir *Chapitre 8.1.4 "Validité de la clé", page 169*.
- Activez la **Revalidation** de clé, voir *Chapitre 8.1.5 "Revalidation de clé", page 169*.

Il est fortement recommandé d'associer les groupes d'accès temporaires avec la revalidation de clé.

1) Trouvez le groupe de profils d'accès et accédez à ses informations détaillées.

   Voir *Chapitre 4.7.1 "Recherche de groupes d'accès temporaires", page 72*.

2) Sélectionnez l'onglet **Clés**.

3) Cliquez sur **Modifier**.

4) Pour ajouter des clés à un groupe d'accès temporaire :

   a) Cliquez sur **Ajouter clés...**.

b) Cliquez sur **Sélectionner** pour ajouter des clés individuelles. Cliquez sur **Tout sélectionner** pour ajouter toutes les clés.

c) Cliquez sur **Effectué**.

d) Cliquez sur **Enregistrer**.

Une tâche à distance est automatiquement créée.

5) Pour supprimer des clés d'un groupe d'accès temporaire :

a) Cliquez sur **Supprimer** pour supprimer des clés individuelles. Cliquez sur **Tout supprimer** pour supprimer toutes les clés.

b) Cliquez sur **Enregistrer**.

4.7.5 Modification de l'accès explicite pour les groupes d'accès temporaires

1) Trouvez le groupe de profils d'accès et accédez à ses informations détaillées.

Voir *Chapitre 4.7.1 "Recherche de groupes d'accès temporaires", page 72*.

2) Sélectionnez l'onglet **Accès explicite**.

3) Cliquez sur **Modifier**.

4) Pour ajouter ou supprimer des groupes de cylindres :

a) Dans **GROUPES DE CYLINDRES SÉLECTIONNÉS**, cliquez sur **Ajouter groupes de cylindre...**.

Tous les groupes de cylindres disponibles sont affichés.

b) Pour filtrer les groupes de cylindres disponibles, saisissez les critères de recherche et cliquez sur **Rechercher**.

c) Pour ajouter des groupes de cylindre, cliquez sur **Sélectionner** à côté des cylindres à ajouter ou cliquez sur **Tout sélectionner**.

d) Cliquez sur **OK**.

e) Pour supprimer des groupes de cylindres, cliquez sur **Supprimer** à côté des cylindres à supprimer ou cliquez sur **Tout supprimer**.

5) Pour ajouter ou supprimer des cylindres :

a) Dans **CYLINDRES SÉLECTIONNÉS**, cliquez sur **Ajouter cylindres...**.

La liste de résultats de recherche affiche les cylindres disponibles.

> **REMARQUE !**
> Seuls les cylindres dont la liste d'accès de cylindres comporte la clé sélectionnée sont affichés.

b) Pour filtrer les cylindres disponibles, saisissez le critère de recherche et cliquez sur **Rechercher**.

c) Pour ajouter des cylindres, cliquez sur **Sélectionner** à côté des cylindres à ajouter, ou cliquez sur **Tout sélectionner**.

d) Cliquez sur **OK**.

e) Pour supprimer des groupes de cylindres, cliquez sur **Supprimer** à côté des cylindres à supprimer ou cliquez sur **Tout supprimer**.

6) Cliquez sur **Enregistrer**.

4.7.6 Affichage des événements d'un groupe d'accès temporaire

L'onglet Événements est utilisé pour la traçabilité des opérations administrateur dans CWM, telles que l'ajout et la suppression de clés dans un groupe d'accès temporaire.

1) Trouvez le groupe de profils d'accès et accédez à ses informations détaillées.

   Voir *Chapitre 4.7.1 "Recherche de groupes d'accès temporaires", page 72*.

2) Sélectionnez l'onglet **Événements**.

   La liste de tous les événements du groupe d'accès temporaire s'affiche.

4.7.7 Suppression des autorisations de clé redondantes

La suppression des autorisations redondantes est utile en cas d'introduction de profils d'accès dans un système de fermeture dont les clés sont déjà configurées avec des autorisations explicites. Les autorisations explicites sont considérées comme redondantes si la clé est également associée à un profil donnant accès au même cylindre ou groupe de cylindres.

Conseil
Il est recommandé de supprimer les autorisations redondantes pour avoir une meilleure vue d'ensemble des autorisations.

1) Recherchez les clés.

   Voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

2) Dans la liste des résultats de recherche, sélectionnez les clés.

3) Cliquez sur **Supprimer autorisations redondantes...**.

4) Cliquez sur **OK**.

4.8 Affichage des autorisations

4.8.1 Affichage des cylindres accessibles pour les clés ou les groupes de clés

Les autorisations existantes affichent les cylindres auxquels une clé a accès, en prenant en compte à la fois la liste d'accès de la clé et les listes d'accès du cylindre. Ce sont les cylindres que la clé peut effectivement ouvrir.

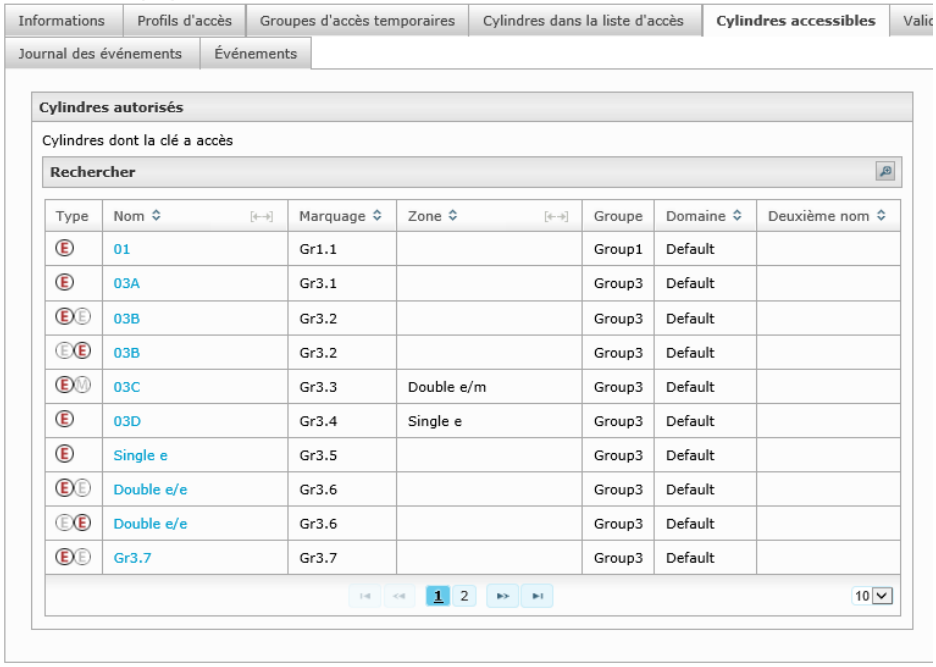
1) Trouvez la clé ou le groupe de clés et accédez à ses informations détaillées.

   Voir *Chapitre 4.3.1 "Recherche de groupes de clés", page 53*.

2) Sélectionnez l'onglet **Cylindres accessibles**.

   La liste de tous les cylindres pour lesquels le groupe de clés est autorisé s'affiche.

1.4.8 - ASIC2 (E3)



Pour les cylindres double entrée, l'entrée A et l'entrée B sont présentées séparément. Le symbole indique l'entrée concernée (l'autre entrée est grisée).

Les informations concernent l'entrée A.

Les informations concernent l'entrée B.

REMARQUE !
Des clés individuelles peuvent être exclues d'accès. Voir *Chapitre 8.1.2 "Autorisation électronique", page 167*.

4.8.2 Affichage des clés avec accès aux cylindres ou aux groupes de cylindres

Les clés avec accès sont les clés pouvant accéder au cylindre en prenant à la fois en compte les listes d'accès des clés et les listes d'accès du cylindre. Ce sont les clés qui peuvent effectivement ouvrir le cylindre.

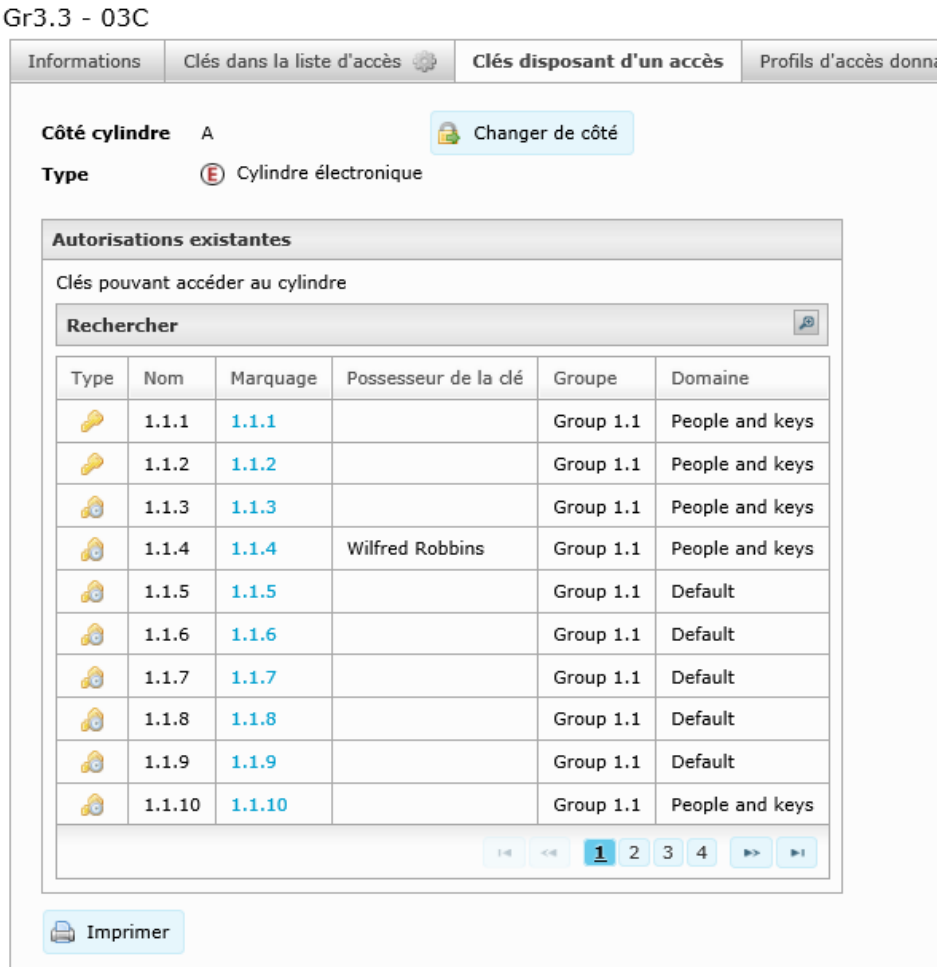
1) Trouvez le cylindre ou le groupe de cylindres et accédez à ses informations détaillées.

   - Pour rechercher un cylindre, voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.
   - Pour rechercher un groupe de cylindres, voir *Chapitre 4.5.1 "Recherche de groupes de cylindres", page 67*.

2) Sélectionnez l'onglet **Clés disposant d'un accès**.

   La liste des clés avec accès actuel au cylindre ou au groupe de cylindres s'affiche.

   Les clés appartenant aux groupes de clés autorisés s'affichent individuellement.



4.8.3 Affichage des profils d'accès donnant accès à un cylindre ou un groupe de cylindres

Les clés associées à un profil d'accès ont automatiquement accès aux cylindres et groupes de cylindres spécifiés par ce profil d'accès. Notez que cela ne signifie pas nécessairement que la clé peut ouvrir le cylindre, étant donné que l'accès effectif dépend également de la liste d'accès dans le cylindre.

1) Trouvez le cylindre ou le groupe de cylindres et accédez à ses informations détaillées.
   - Pour rechercher un cylindre, voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.
   - Pour rechercher un groupe de cylindres, voir *Chapitre 4.5.1 "Recherche de groupes de cylindres", page 67*.
2) Sélectionnez l'onglet **Profils d'accès donnant accès**.

Voir également *Chapitre 4.9.4 "Configurer les autorisations de profil d'accès", page 83*.

4.9 Configuration des autorisations

4.9.1 Configuration des autorisations dans les clés

Les clés dynamiques ont une liste d'accès comportant le cylindre et les groupes de cylindres que la clé est autorisée à ouvrir. Configurer les autorisations dans les clés signifie modifier les autorisations explicites dans cette liste d'accès. La liste d'accès peut également comporter des autorisations implicites provenant de profils d'accès. Pour

configurer les autorisations de profil d'accès, voir *Chapitre 4.9.4 "Configurer les autorisations de profil d'accès", page 83*.

Veuillez noter que la présence d'un cylindre dans la liste d'accès d'une clé ne signifie pas nécessairement que la clé dispose de l'accès effectif, étant donné que l'accès effectif dépend également de la liste d'accès dans le cylindre. Pour afficher les cylindres que la clé peut effectivement ouvrir, voir *Chapitre 4.8.1 "Affichage des cylindres accessibles pour les clés ou les groupes de clés", page 76*.

Pour supprimer tous les accès pour un cylindre, consultez *Chapitre 4.9.3 "Suppression de tous les accès pour un cylindre", page 82*.

Pour plus d'informations sur le principe des autorisations, voir *Chapitre 8.1 "Principes des autorisations", page 167*.

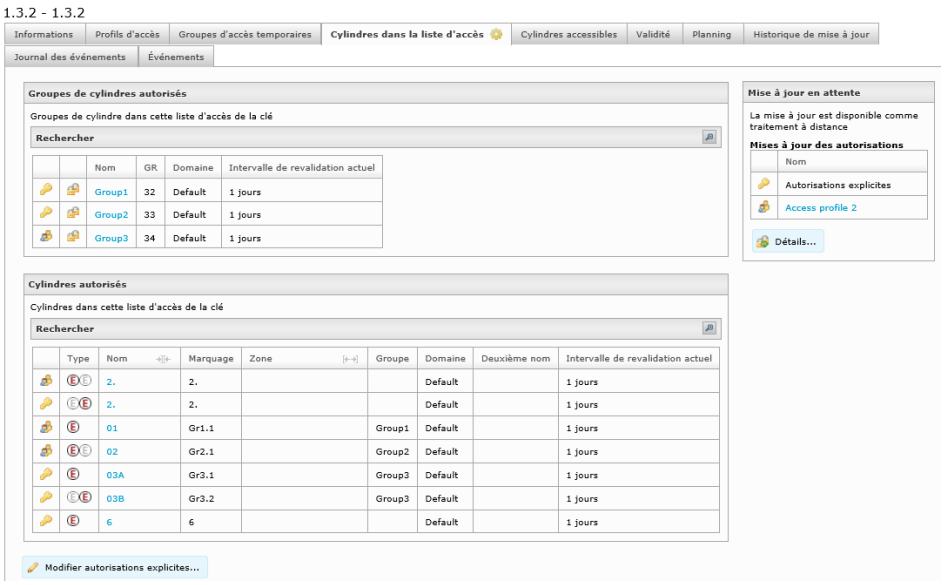
1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Sélectionnez l'onglet **Cylindres dans la liste d'accès**.

   Les cylindres et groupes de cylindres actuellement autorisés s'affichent.



   La liste d'accès contient des autorisations explicites.

   Autorisation explicite

   Autorisation à partir du profil d'accès

   Pour les cylindres double entrée, l'entrée A et l'entrée B sont présentées séparément. Le symbole indique l'entrée concernée (l'autre entrée est grisée).

   Les informations concernent l'entrée A.

   Les informations concernent l'entrée B.

   Les mises à jour à distance en attente sont présentées sous **Mise à jour en attente**.

3) Cliquez sur **Modifier autorisations explicites...**.

   Les autorisations explicites définies pour la clé s'affichent.

Conseil
La suppression de groupes de cylindres ou de cylindres peut se faire directement sur cette vue en cliquant sur **Supprimer** à côté du cylindre ou du groupe de cylindres correspondant.

Lorsque la suppression porte sur des clés avec de longues listes d'accès, il est utile de filtrer d'abord les groupes de cylindres et les cylindres.

4) Pour ajouter ou supprimer des groupes de cylindres :
   a) Dans **Autorisations de groupes de cylindres explicites**, cliquez sur **Changer groupes de cylindre...**.

      Tous les groupes de cylindres disponibles sont affichés.
   b) Pour filtrer les groupes de cylindres disponibles, saisissez les critères de recherche et cliquez sur **Rechercher**.
   c) Cliquez sur **Sélectionner** pour les groupes de cylindres à ajouter ou cliquez sur **Tout sélectionner**.
   d) Cliquez sur **Supprimer** pour les groupes de cylindres à supprimer ou cliquez sur **Tout supprimer**.
   e) Cliquez sur **OK**.
5) Pour ajouter ou supprimer des cylindres individuellement :
   a) Dans **Autorisations de cylindre explicites**, cliquez sur **Changer cylindres...**.

      La liste de résultats de recherche affiche les cylindres disponibles.

      REMARQUE !
      Seuls les cylindres dont la liste d'accès de cylindres comporte la clé sélectionnée sont affichés.
   b) Pour filtrer les cylindres disponibles, saisissez le critère de recherche et cliquez sur **Rechercher**.
   c) Cliquez sur **Sélectionner** à côté des cylindres à ajouter ou cliquez sur **Tout sélectionner**.
   d) Cliquez sur **Supprimer** à côté des cylindres à supprimer ou cliquez sur **Tout supprimer**.
   e) Cliquez sur **OK**.
6) Cliquez sur **Enregistrer**.

   La progression est indiquée dans une fenêtre pop-up avec la durée estimée de l'opération.
7) Si la clé est scannée, cliquez sur **Écrire une liste d'accès localement sur la clé** pour la mettre à jour.

REMARQUE !
Si la revalidation est activée sur la clé, celle-ci est revalidée dans le boîtier de programmation local au cours du processus de programmation.

Sinon, un traitement de mise à jour de clé est créé.

4.9.2 Configuration des autorisations dans les cylindres

Une liste d'accès de cylindre est enregistrée dans chaque cylindre et inclut les clés et groupes de clés autorisés à ouvrir le cylindre. Configurer les autorisations dans les cylindres signifie modifier cette liste d'accès.

Pour les clés utilisateur, le fait qu'une clé soit incluse dans la liste d'accès du cylindre ne signifie pas obligatoirement que la clé dispose d'un accès effectif, étant donné que cet accès dépend également de la liste d'accès de la clé. Pour afficher les clés pouvant effectivement ouvrir le cylindre, voir *Chapitre 4.8.2 "Affichage des clés avec accès aux cylindres ou aux groupes de cylindres", page 77*.

Pour plus d'informations sur le principe des autorisations, voir *Chapitre 8.1 "Principes des autorisations", page 167*.

1) Trouvez le cylindre et accédez à ses informations détaillées.

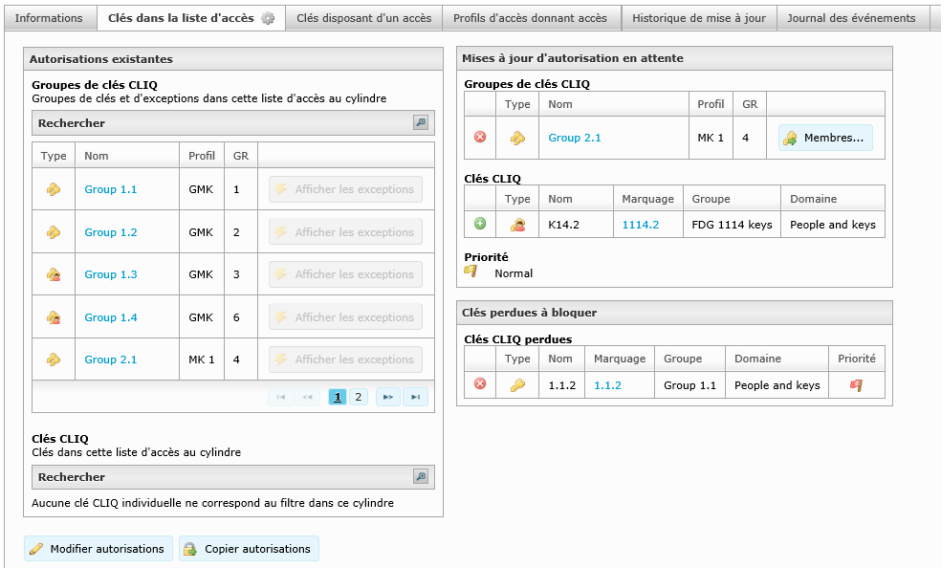
   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Sélectionnez l'onglet **Clés dans la liste d'accès**.

   Les groupes de clés et clés actuellement autorisés s'affichent.

   Tous les traitements de programmation de cylindre avec mises à jour des autorisations sont présentés sous **Mises à jour d'autorisation en attente**.

   Tous les traitements de programmation de cylindre en raison de clés perdues sont présentés sous **Clés perdues à bloquer**.



3) Pour afficher les clés appartenant à un groupe de clés autorisé, mais exclues de l'accès, cliquez sur **Afficher les exceptions**.

4) Cliquez sur **Modifier autorisations**.

5) **Pour ajouter des groupes de clés ou des clés individuelles**

   1. Cliquez sur **Ajouter groupe de clés CLIQ**.

      La liste des résultats de recherche affiche tous les groupes de clés disponibles.

2. Pour filtrer les groupes de clés disponibles, saisissez les critères de recherche et cliquez sur **Rechercher**.
3. Cliquez sur **Sélectionner** pour les groupes de clés à ajouter.

> **REMARQUE !**
> Lorsqu'un groupe de clés est ajouté à une liste d'accès, toute entrée individuelle de clé de ce groupe de clés (désormais redondant) est automatiquement supprimée. Cela signifie que si un groupe de clés est ajouté, puis ultérieurement supprimé, toutes les clés du groupe perdent leur accès, y compris les clés qui disposaient précédemment d'un accès individuel.

4. Cliquez sur **Effectué**.

Pour exclure des clés d'une autorisation de groupe de clé :

1. Cliquez sur **Modifier** pour le groupe de clé.
2. Cliquez sur **Interdire** pour les clés à exclure d'accès.

Pour ré-autoriser des clés d'une autorisation de groupe de clés :

> **REMARQUE !**
> Pour pouvoir ré-autoriser la clé, elle doit avoir été déclarée comme retrouvée.
>
> Cliquez sur **Déclarée trouvée** dans la vue des informations détaillées de la clé.

1. Cliquez sur **Modifier...** pour le groupe de clé.
2. Cliquez sur **Autoriser** pour que les clés autorisent l'accès au cylindre.

Pour supprimer des groupes de clés ou des clés individuelles
Cliquez sur Supprimer pour le groupe de clés à supprimer.

6) Une fois la modification effectuée, cliquez sur **Affichage**.

Un travail de programmation de cylindre est créé.

Pour programmer les cylindres, voir *Chapitre 4.4.13 "Programmation des cylindres", page 62*.

Les autorisations de plusieurs cylindres peuvent être modifiées en même temps. Sélectionnez les cylindres dans la liste des résultats de recherche (voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*) et cliquez sur **Ajouter autorisations** ou **Annuler les autorisations**.

4.9.3 Suppression de tous les accès pour un cylindre

Les cylindres individuels peuvent être supprimés de toutes les clés, tous les profils d'accès et groupes d'accès temporaires.

La possibilité de supprimer tous les accès d'un cylindre nécessite un système de verrouillage avec des clés dynamiques.

1) Trouvez le cylindre et accédez à ses informations détaillées.

Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Sélectionnez **Supprimer les autorisations côté clé**.

> **REMARQUE !**
> Pour supprimer les accès, toutes les clés utilisées pour l'accès au cylindre doivent être mises à jour.

> **REMARQUE !**
> **Supprimer les autorisations côté clé** supprime uniquement le cylindre de la liste d'accès sur les clés prenant en charge les mises à jour à distance.
>
> Pour voir s'il y a des clés ne prenant pas en charge les tâches à distance, avec accès au cylindre, sélectionnez l'onglet **Clés disposant d'un accès**. Pour chacune de ces clés, mettez la clé dans le boîtier de programmation local. Scannez la clé, sélectionnez l'onglet **Cylindres dans la liste d'accès**, cliquez sur **Modifier autorisations explicites** et retirez la clé.
>
> Pour plus d'informations sur les fonctions à distance, consultez *Chapitre 8.3.1 "Présentation de la fonctionnalité à distance", page 183*.

3) Dans la fenêtre pop-up, cliquez sur **OK**.

4.9.4 Configurer les autorisations de profil d'accès

Configurer les autorisations de profil d'accès signifie modifier les autorisations implicites des clés et des personnes associées au profil d'accès.

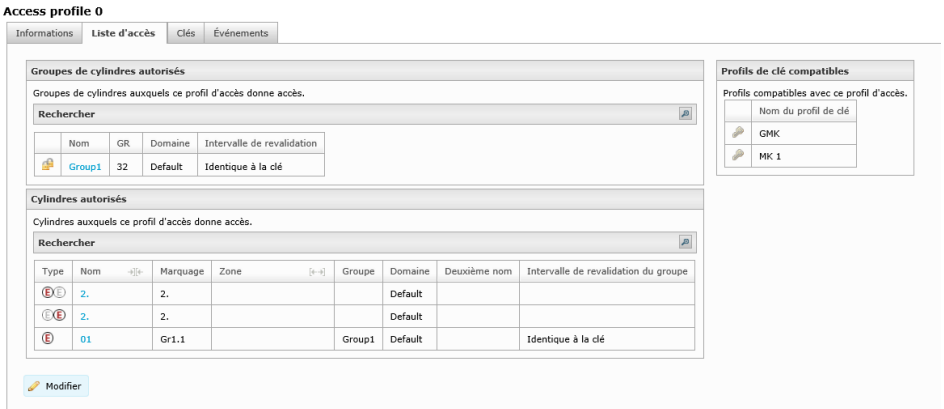
1) Trouvez le profil d'accès et accédez à ses informations détaillées.

   Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

2) Sélectionnez l'onglet **Liste d'accès**.

   Les cylindres et groupes de cylindres actuellement autorisés s'affichent.

3) Cliquez sur **Modifier**.



Pour les cylindres double entrée, l'entrée A et l'entrée B sont présentées séparément. Le symbole indique l'entrée concernée (l'autre entrée est grisée).

Les informations concernent l'entrée A.

Les informations concernent l'entrée B.

4) **Pour ajouter des cylindres ou des groupes de cylindres**

1. Cliquez sur **Ajouter cylindres...** ou **Ajouter groupes de cylindre...**.

   La fenêtre pop-up affiche la liste des cylindres ou groupes de cylindres disponibles.
2. Pour filtrer les résultats, entrez le critère de recherche puis cliquez sur **Rechercher**.
3. Cliquez sur **Sélectionner** pour les éléments à ajouter ou cliquez sur **Tout sélectionner**.
4. Cliquez sur **OK**.

Pour supprimer des cylindres ou des groupes de cylindres

1. Cliquez sur l'icône de recherche et entrez les critères de recherche.
2. Cliquez sur **Rechercher**.

   Le tableau montre les résultats de la recherche.
3. – Pour supprimer certains éléments :

     Cliquez sur **Supprimer**.
   – Pour supprimer tous les éléments des résultats de recherche :

     Cliquez sur **Supprimer toute la liste**.

5) La revalidation flexible peut également être modifiée dans cette vue. Voir *Chapitre 4.10.2 "Configuration de la revalidation flexible", page 88*.

6) Cliquez sur **Enregistrer** pour quitter le mode de modification.

Voir également *Chapitre 8.2.4 "Profils d'accès", page 179*.

4.9.5 Sélection des profils d'accès d'employés ou de visiteurs

Les profils d'accès ne s'appliquent qu'aux clés dynamiques, les autres types de clés ne sont pas concernés.

1) Trouvez l'employé ou le visiteur et accédez à ses informations détaillées.

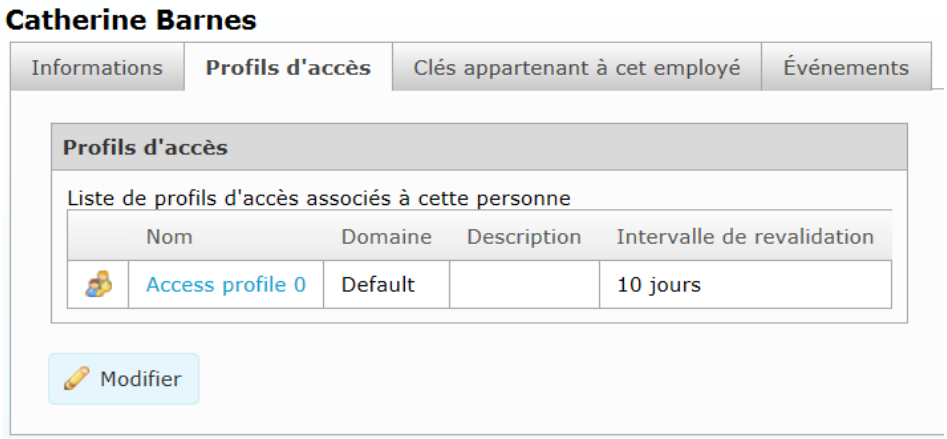
   Voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

2) Sélectionnez l'onglet **Profils d'accès**.

   La liste des résultats de recherche affiche les profils d'accès actuellement associés à l'employé ou au visiteur.

3) Cliquez sur **Modifier**.

   La liste de tous les profils d'accès associés s'affiche.



4) Pour ajouter des profils d'accès :

   a) Cliquez sur **Ajouter profils d'accès**.

      La liste des résultats de recherche affiche tous les profils d'accès disponibles.

   b) Pour filtrer les profils d'accès disponibles, saisissez le **Nom**, la **Description**, le **Domaine** et/ou les **Notes** dans le champ de recherche.

   c) Cliquez sur **Sélectionner** pour sélectionner un profil d'accès ou cliquez sur **Tout sélectionner**.

   d) Cliquez sur **Effectué**.

5) Pour supprimer des profils d'accès, cliquez sur **Supprimer** pour supprimer un profil d'accès ou cliquez sur **Tout supprimer**.

6) Cliquez sur **Enregistrer**.

Les profils d'accès de plusieurs employés ou visiteurs peuvent être simultanément ajoutés ou supprimés. Sélectionnez les employés ou les visiteurs dans la liste des résultats de recherche et cliquez sur **Ajouter profils d'accès** ou **Supprimer profils d'accès**.

Voir également *Chapitre 8.2.4 "Profils d'accès", page 179*.

4.9.6 Sélection des profils d'accès de clé

Les profils d'accès s'appliquent uniquement aux clés dynamiques.

1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Sélectionnez l'onglet **Profils d'accès**.

   La liste des résultats de recherche affiche les profils d'accès actuellement associés à la clé.

3) Cliquez sur **Modifier**.

4) Pour ajouter des profils d'accès :

   a) Cliquez sur **Ajouter profils d'accès**.

      La liste des résultats de recherche affiche tous les profils d'accès disponibles.

b) Pour filtrer les profils d'accès disponibles, saisissez les critères de recherche et cliquez sur **Rechercher**.

c) Cliquez sur **Sélectionner** pour sélectionner un profil d'accès ou cliquez sur **Tout sélectionner**.

d) Cliquez sur **Effectué**.

5) Pour supprimer des profils d'accès, cliquez sur **Supprimer** pour supprimer un profil d'accès ou cliquez sur **Tout supprimer**.

6) Cliquez sur **Enregistrer**.

Les profils d'accès de plusieurs clés peuvent être modifiés en même temps. Sélectionnez les clés dans la liste des résultats de recherche et cliquez sur **Ajouter profils d'accès** ou **Supprimer profils d'accès**.

Voir *Chapitre 8.2.4 "Profils d'accès", page 179*.

4.9.7 Sélection des profils d'accès de groupes d'accès temporaires

1) Trouvez le groupe de profils d'accès et accédez à ses informations détaillées.

   Voir *Chapitre 4.7.1 "Recherche de groupes d'accès temporaires", page 72*.

2) Sélectionnez l'onglet **Profils d'accès**.

3) Cliquez sur **Modifier**.

4) Pour ajouter des profils d'accès à un groupe d'accès temporaire :

   a) Cliquez sur **Ajouter profils d'accès...**.

   b) Cliquez sur **Sélectionner** pour ajouter des profils d'accès individuels.
   Cliquez sur **Tout sélectionner** pour ajouter tous les profils d'accès.

   c) Cliquez sur **Effectué**.

   d) Cliquez sur **Enregistrer**.

5) Pour supprimer des profils d'accès d'un groupe d'accès temporaire :

   a) Cliquez sur **Supprimer** pour supprimer des profils d'accès individuels.
   Cliquez sur **Tout supprimer** pour supprimer tous les profils d'accès.

   b) Cliquez sur **Enregistrer**.

4.10 Configuration de la validité et du planning d'une clé

4.10.1 Configuration de la validité de la clé, de la revalidation et de la validation du code PIN

1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Sélectionnez l'onglet **Validité**.

1.3.2 - 1.3.2

L'onglet Validité s'affiche :

- Réglages de validité : La clé peut être toujours active, toujours inactive ou active sur un intervalle d'activation spécifié par des dates.
- En cas de revalidation :
  - **Intervalle de revalidation** : la durée d'activation de la clé après revalidation, avant la prochaine revalidation.
  - **Prochaine expiration** : Date et heure à laquelle la clé devient inactive si elle n'est pas revalidée.

    Lorsque la revalidation est activée à distance sur une clé qui est **Toujours active**, **La clé doit toujours être revalidée** est affiché, la prochaine expiration sera **Jamais** jusqu'à ce que la clé soit mise à jour.

    Lorsque la revalidation est faite à distance sur une clé qui est **Active entre les dates**, ce sera égal à **Clé active jusqu'au** jusqu'à ce que la clé soit revalidée pour la première fois.
- Si la validation du code PIN est utilisée :
  - **Intervalle de validation de code PIN** : Le temps pendant lequel la clé reste active après une validation du code PIN, avant qu'une nouvelle saisie du code PIN ne soit nécessaire.
- Réglages des dates de changement d'heure

3) Cliquez sur **Modifier validité**.
4) Choisissez si la clé doit être **Inactive**, **Active entre les dates sélectionnées** ou **Toujours active**.
5) Dans le cas où **Active entre les dates sélectionnées** est choisi, saisissez **Clé active à partir du** et **Clé active jusqu'au**.
6) Pour configurer une revalidation :
   a) Sélectionnez **Utiliser la revalidation de la clé**.
   b) Saisissez un nombre de jours, d'heures et de minutes pour l'**Intervalle de revalidation**.

      C'est la période durant laquelle la clé reste active après revalidation dans une boîtier de programmation à distance.
   c) Pour ne permettre qu'une seule revalidation, sélectionnez **Mise à jour unique**.
7) Pour configurer la validation du code PIN :
   a) Sélectionnez **Utiliser la validation du code PIN**.

b) Saisissez un nombre de jours, d'heures et de minutes pour l'**Intervalle de validation de code PIN**.

Le temps pendant lequel la clé reste active après validation par code PIN.

L'intervalle spécifié doit se situer entre 1 minute et 45 jours.

c) Un code PIN aléatoire est généré automatiquement pour **Nouveau code PIN initial**. Il est également possible d'écraser le code PIN généré et d'entrer manuellement un nouveau Code PIN initial.

Sélectionnez **Afficher valeur** pour rendre le code PIN visible.

Si le possesseur de la clé a une adresse e-mail enregistrée, un e-mail avec le code PIN initial lui est envoyé. Ce code PIN doit être changé par l'utilisateur lors de la première utilisation.

8) Pour confirmer les mises à jour :

a) Si la clé est scannée, cliquez sur **Écrire dans la clé**.

La clé est mise à jour avec les nouveaux réglages.

b) Si la clé n'est pas scannée, cliquez sur **Envoyer la mise à jour à distance**.

Un traitement de mise à jour à distance est créé.

La validité, la revalidation et la validation du code PIN peuvent être modifiées pour plusieurs clés à la fois. Sélectionnez les clés dans les résultats de recherche, cliquez sur **Changer réglages de validité...** et suivez les instructions.

Voir également *Chapitre 8.1.4 "Validité de la clé", page 169*, *Chapitre 8.1.5 "Revalidation de clé", page 169* et *Chapitre 8.1.7 "Validation du code PIN", page 173*.

4.10.2 Configuration de la revalidation flexible

ATTENTION !
Comme la revalidation flexible est une fonction avancée complexe, il est recommandé de lire attentivement *Chapitre 8.1.6 "Revalidation flexible", page 172* avant de la configurer.

Conditions préalables :

- Au moins une clé utilisateur dispose d'un microprogramme avec prise en charge de la revalidation flexible (voir *Chapitre 9.7 "Fonctionnalité dépendante du microprogramme", page 214*).
- La fonction est activée dans les **Réglages du système** (voir *Chapitre 6.4 "Modifier les réglages du système", page 100*).

REMARQUE !
En cas d'utilisation de la revalidation flexible, toutes les clés affectées par les réglages de revalidation des profils d'accès ou des groupes de cylindres doivent avoir la revalidation activée.

1) Pour régler l'intervalle de revalidation d'un profil d'accès :

a) Trouvez le profil d'accès et accédez à ses informations détaillées.

Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

b) Cliquez sur **Modifier**.

c) Sélectionnez une option de **Revalidation**.

- Pour spécifier un intervalle de revalidation, sélectionnez **Utilisez un intervalle spécifique**.
- Pour ne pas spécifier d'intervalle de revalidation, sélectionnez **Utilisez les intervalles de revalidation des groupes de cylindres**.

  L'intervalle de revalidation ne concerne que les groupes de cylindres pour lesquels cet intervalle est défini. Sinon, c'est l'intervalle de revalidation configuré sur les clés qui prévaut.

d) Si **Utilisez un intervalle spécifique** a été sélectionné, saisissez l'intervalle en jours, heures et minutes.

e) Cliquez sur **Enregistrer**.

f) L'intervalle de revalidation de plusieurs profils d'accès peut être simultanément modifié. Sélectionnez les profils d'accès dans la liste des résultats de recherche et cliquez sur **Modifier l'intervalle de revalidation**.

2) Pour régler l'intervalle de revalidation d'un groupe de cylindres :

a) Trouvez le groupe de cylindres et accédez à ses informations détaillées.

Voir *Chapitre 4.5.1 "Recherche de groupes de cylindres", page 67*.

b) Cliquez sur **Modifier**.

c) Sélectionnez une option de **Revalidation**.

- Pour spécifier un intervalle de revalidation, sélectionnez **Utilisez un intervalle spécifique**.
- Pour ne pas spécifier d'intervalle de revalidation, sélectionnez **Utiliser les intervalles de revalidation des clés**.

  L'intervalle de revalidation configuré sur les clés est utilisé.

d) Si **Utilisez un intervalle spécifique** a été sélectionné, saisissez l'intervalle en jours, heures et minutes.

e) Cliquez sur **Enregistrer**.

f) L'intervalle de revalidation de plusieurs groupes de cylindres peut être simultanément modifié. Sélectionnez les groupes de cylindres dans la liste des résultats de recherche et cliquez sur **Modifier l'intervalle de revalidation**.

3) Pour vérifier la configuration de l'intervalle de revalidation pour une clé, afficher la colonne **Intervalle de revalidation actuel** pour chaque cylindre dans la liste d'accès de la clé. Voir *Chapitre 4.9.1 "Configuration des autorisations dans les clés", page 78*.

Voir également *Chapitre 8.1.6 "Revalidation flexible", page 172*.

4.10.3 Configuration du planning de clé

Il existe deux types de planning, le Planning de base et le Planning à créneaux horaires multiples (voir *Chapitre 8.1.8 "Plannings de clé", page 174*). Le microprogramme de la clé détermine le type utilisé. Pour plus d'informations sur la prise en charge de type de

planning des différentes versions de microprogramme de clé, voir *Chapitre 9.7 "Fonctionnalité dépendante du microprogramme", page 214*

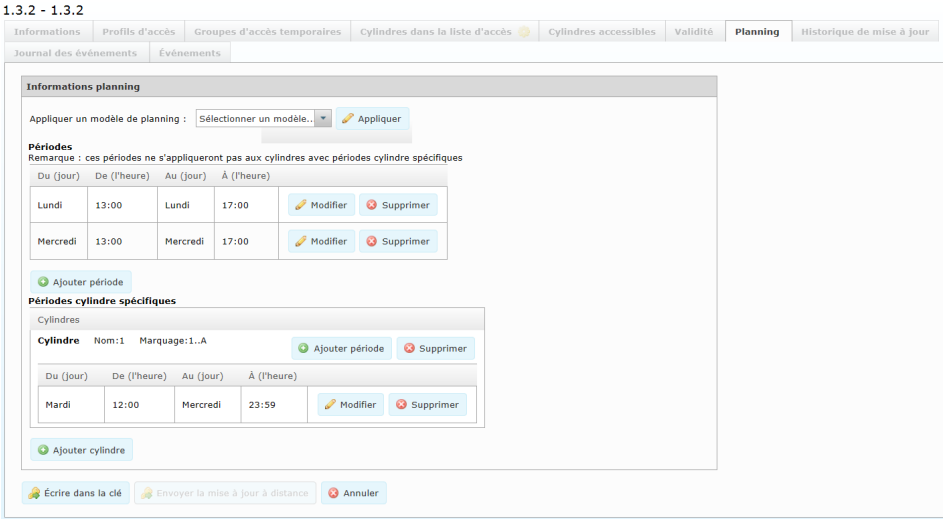
1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Sélectionnez l'onglet **Planning**.

3) Cliquez sur **Modifier planning**.



4) Pour appliquer un modèle de planning, sélectionnez un modèle dans le menu déroulant et cliquez sur **Appliquer**.

   Le modèle est appliqué mais le planning reste modifiable.

5) Déterminez si la clé dispose d'un planning de base ou d'un planning à créneaux horaires multiples.

   Si la clé dispose d'un planning à créneaux horaires multiples, outre **Périodes**, **Périodes cylindre spécifiques** est également affiché.

6) Pour modifier un planning de base :

   a) Cliquez sur **Modifier** dans la ligne du jour à modifier.

   b) Sélectionnez **Toute la journée**, **Jamais** ou **Personnaliser**.

   c) Si l'option Personnaliser est choisie, saisissez les valeurs de période **De (l'heure)** et **À (l'heure)**.

   d) Cliquez sur **Enregistrer**.

7) Pour modifier un planning à créneaux horaires multiples :

   a) Pour ajouter une période :

      - Cliquez sur **Ajouter période**.
      - Saisissez les valeurs de période **Du (date)** et **Au (date)**.
      - Cliquez sur **Enregistrer**.

   b) Pour modifier la période, cliquez sur **Modifier période**.

c) Pour supprimer une période, cliquez sur **Supprimer période**.

d) Pour ajouter une période pour un cylindre spécifique :

- Cliquez sur **Ajouter cylindre**.

  La liste de résultats de recherche affiche tous les cylindres disponibles.
- Pour filtrer les cylindres disponibles, saisissez le critère de recherche et cliquez sur **Rechercher**.
- Cliquez sur **Sélectionner** pour le cylindre à ajouter.
- Ajoutez, modifiez et supprimez les périodes pour le cylindre.

> **REMARQUE !**
>
> **Pour clés de génération 1** :
>
> – Pour les cylindres inclus dans la liste d'accès de clé de façon individuelle (ne faisant pas partie d'un groupe de cylindres), spécifier une ou plusieurs tranches horaires pour un cylindre signifie que le planning général est ignoré pour ce cylindre.
>
> – Pour les cylindres inclus dans la liste d'accès de clé comme faisant partie d'un groupe de cylindres, les tranches horaires spécifiques au cylindre sont ignorées.
>
> **Pour clés de génération 2** :
>
> – La spécification d'une ou plusieurs tranches horaires pour un cylindre signifie que le planning général est ignoré pour ce cylindre.

8) Pour confirmer les mises à jour :

a) Si la clé est scannée, cliquez sur **Écrire dans la clé**.

La clé est mise à jour avec les nouveaux réglages. Si la revalidation est activée sur la clé, la clé sera revalidée en même temps.

b) Si la clé n'est pas scannée, cliquez sur **Envoyer la mise à jour à distance**.

Un traitement de mise à jour de clé est créé.

4.10.4 Configuration du planning d'un groupe de clé

Un planning peut être configuré pour toutes les clés d'un groupe de clé.

1) Trouvez le groupe de clés et accédez à ses informations détaillées.

Voir *Chapitre 4.3.1 "Recherche de groupes de clés", page 53*.

2) Cliquez sur **Configuration de clés groupée**.

3) Sélectionnez **Régler le planning**.

4) Cliquez sur **Suivant**.

5) Saisissez les réglages de planning. Pour référence, voir *Chapitre 4.10.3 "Configuration du planning de clé", page 89*.

6) Cliquez sur **Suivant**.

Les réglages sélectionnés s'affichent.

7) Pour confirmer les mises à jour, cliquez sur **Appliquer**.

Les traitements de mise à jour de clé sont créés.

4.11 Gestion des journaux des événements

Les clés et cylindres standard et dynamiques sont dotés d'une fonction de journal des événements.

Un journal des événements est une liste d'événements qui répertorie les tentatives d'accès. Il indique quel était le possesseur de la clé au moment de la tentative d'accès. Il contient également les enregistrements de programmation de l'appareil. Pour plus d'informations, consultez *Chapitre 8.6 "Journaux des événements", page 189*.

4.11.1 Affichage des journaux des événements pour la clé utilisateur

1) Trouvez la clé et accédez à ses informations détaillées.

   Pour rechercher une clé et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*

   Pour scanner la clé dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*

2) Sélectionnez l'onglet **Journal des événements**.

   Si un journal des événements a été demandé et lu par une boîtier de programmation à distance, la liste des événements du journal des événements s'affiche.

3) Si la fonction **Approbations** est activée (voir *Chapitre 6.4 "Modifier les réglages du système", page 100*) :

   a) Pour demander un nouveau journal des événements, cliquez sur **Demander le journal des événements à distance**.

   b) Saisissez un commentaire pour l'approbateur et cliquez sur **Envoyer la demande**.

4) Si la fonction **Approbations** est désactivée (voir *Chapitre 6.4 "Modifier les réglages du système", page 100*) :

   - Si la clé est dans le boîtier de programmation local, cliquez sur **Lire le journal des événements**. Cela peut prendre un certain temps.
   - Si la clé n'est pas dans le boîtier de programmation local, cliquez sur **Demander le journal des événements à distance**.

     Le journal des événements sera lu à la prochaine insertion de la clé dans une boîtier de programmation à distance, et enregistré dans CWM. Il s'affichera alors dans l'onglet Journal des événements.

   REMARQUE !

   Demander le journal des événements à distance est automatiquement activé à la remise des clés et désactivé au retour des clés.

5) Facultatif : Exportez le tableau au format PDF. Voir *Chapitre 4.11.5 "Exportation des informations de journal des événements", page 94*.

Voir également *Chapitre 8.6 "Journaux des événements", page 189*.

4.11.2 Affichage des journaux des événements pour le cylindre

REMARQUE !
Les journaux des événements de cylindre qui enregistrent les tentatives d'accès par des clés normales n'affichent pas les horaires dans la colonne **Heure dans la clé**.

1) Trouvez le cylindre et accédez à ses informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Sélectionnez l'onglet **Journal des événements**.

   Si des journaux des événements ont été déjà collectés, ils s'affichent dans une liste.

3) Pour demander un nouveau journal des événements, cliquez sur **Demander le journal des événements**.

   Si **Approbations** est activé (voir *Chapitre 6.4 "Modifier les réglages du système", page 100*), saisissez un commentaire pour l'approbateur.

4) Sélectionnez **Priorité**.

   Les tâches urgentes doivent disposer d'une priorité plus élevée.

5) Cliquez sur **OK**.

   Un traitement de programmation de collecte de journal des événements sur le cylindre est créé.

   Pour obtenir le journal des événements sur le cylindre, voir *Chapitre 4.4.13 "Programmation des cylindres", page 62*.

6) Facultatif : Exportez le tableau au format PDF. Voir *Chapitre 4.11.5 "Exportation des informations de journal des événements", page 94*.

Voir également *Chapitre 8.6 "Journaux des événements", page 189*.

4.11.3 Affichage de l'archive de journal des événements

L'archive de journal des événements contient tous les journaux des événements collectés sur les clés et cylindres du système de fermeture. En sélectionnant une clé ou un cylindre, il est possible d'afficher l'ensemble des journaux des événements collectés pour cette clé ou ce cylindre.

Il n'y a aucune restriction quant au nombre de journaux d'événements pouvant être inclus dans l'archive de journal des événements. L'archive peut être configurée pour automatiquement supprimer les journaux des événements de plus d'un nombre de jours défini, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

1) Sélectionnez **Informations système » Archive de journal des événements**.

   Une liste des journaux d'événements montre les interactions entre les clés, les cylindres, les clés de programmation, les boîtiers de programmation à distance et/ou le logiciel.

REMARQUE !
En raison de l'ampleur des données du journal des événements, certaines informations complémentaires telles que les précédents utilisateurs de clé ou les domaines précédents sont affichées avec un certain délai. Pendant que ces informations sont traitées en arrière-plan, le message **Données en cours de traitement** est affiché dans la liste.

2) Spécifiez des critères de recherche et cliquez sur **Rechercher**.

   Par exemple, pour afficher toutes les interactions de clé avec un cylindre spécifique :

   Sélectionnez la **Clé** sous **Récupéré(s) de**, puis sélectionnez le **Cylindre** en précisant son **Nom** ou le **Marquage** du cylindre spécifique sous **Événement par**.

3) Facultatif : Exportez le tableau au format PDF. Voir *Chapitre 4.11.5 "Exportation des informations de journal des événements", page 94*.

4.11.4 Exportation des informations de journal des événements

1) Affichez une liste des journaux des événements :

   - Pour afficher le journal des événements d'une clé spécifique, voir *Chapitre 4.11.2 "Affichage des journaux des événements pour la clé utilisateur", page 92*.
   - Pour afficher le journal des événements d'un cylindre spécifique, voir *Chapitre 4.11.3 "Affichage des journaux des événements pour le cylindre", page 93*.
   - Pour consulter toute l'archive du journal des événements, voir *Chapitre 4.11.4 "Affichage de l'archive de journal des événements", page 93*.

2) Cliquez sur **Impression du journal des événements complet** pour imprimer ou enregistrer le tableau au format PDF.

   Le tableau apparaît dans une fenêtre pop-up.

3) - Pour enregistrer, cliquez sur l'icône d'enregistrement et indiquez le dossier dans lequel enregistrer.
   - Pour imprimer, cliquez sur **...** et sélectionnez **Imprimer**.

4.11.5 Approbation des demandes de journal des événements

Si la fonction **Approbations** est activée, les demandes de journaux des événements doivent être approuvées avant de pouvoir être exécutées. Une clé de programmation avec le rôle d'approbateur doit être utilisée pour se connecter au système et approuver les demandes de journal des événements en attente.

Pour modifier le réglage **Approbations**, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

1) Insérez la clé de programmation de l'approbateur dans la fente gauche du boîtier de programmation local.

2) Connectez-vous au système.

   Seuls les menus **Tâches** et **Réglages** sont accessibles.

3) Sélectionnez **Tâches » Tâches d'approbation**.

   La liste des tâches d'approbation en attente s'affiche.

4) Cliquez sur **Répondre**.

5) Pour approuver : Saisissez éventuellement un commentaire et cliquez sur **Approuver**.

   Pour refuser : Saisissez éventuellement un commentaire et cliquez sur **Refuser**.

Pour afficher les tâches approuvées ou refusées, sélectionnez l'onglet **Historique des approbations**.

5 Réglages de systèmes de fermeture

5.1 Présentation des réglages d'un système de fermeture

Cette présentation détaille le déroulement d'une première installation du système de verrouillage.

Conditions préalables :

- La base de données est préparée et le logiciel de serveur est installé sur le serveur CWM.
- S'il s'agit d'un système à distance, la base de données est préparée et le logiciel de serveur est également installé sur le serveur à distance.
- Les pare-feux et les proxys sont configurés pour permettre le trafic SSL.
  - À partir des PC clients vers le serveur CWM (Port 443 et 8443).
  - À partir des bornes d'actualisation vers le serveur à distance (Port 443).
  - À partir du serveur CWM vers le serveur SMTP (Port 25).

1) Installer un client CWM.

   Voir *Chapitre 2.1 "Présentation de la configuration des clients CWM", page 13*.
2) Installez le certificat de la clé de programmation maîtresse.

   Voir *Chapitre 5.2 "Installer le certificat de clé de programmation maîtresse", page 96*.
3) Connectez-vous à CWM.

   Voir *Chapitre 5.3 "Connexion à un nouveau système de verrouillage", page 97*.
4) Définissez la langue de CWM.

   Voir *Chapitre 3.4 "Réglage de la langue CWM", page 19*.
5) Installer une licence.

   Voir *Chapitre 6.1.1 "Installation des licences", page 99*.
6) Effectuez la configuration initiale.

   Voir *Chapitre 5.4 "Exécution de la configuration initiale", page 98*.

5.2 Installer le certificat de clé de programmation maîtresse

Si l'intégration DCS est activée :

L'adresse e-mail pour le possesseur de la clé de programmation maîtresse est spécifiée dans DCS. Dans l'heure qui suit la préparation de la base de données du système, un e-mail est envoyé à cette adresse.

Le nombre de fois qu'un certificat de clé de programmation maîtresse peut être créé est déterminé par un réglage dans DCS.

L'installation d'un certificat de clé de programmation maîtresse est identique à l'installation d'un certificat de clé de programmation. Pour plus d'informations, consultez *Chapitre 3.2.1 "Enregistrement du certificat de la clé de programmation via CLIQ Connect PC", page 17*.

Si l'intégration DCS n'est pas activée :

Le certificat de clé de programmation maîtresse est déjà fourni. Pour plus d'informations sur la façon d'installer le certificat, voir *Chapitre 3.2.2 "Installation manuelle du certificat de clé de programmation", page 17*.

5.3 Connexion à un nouveau système de verrouillage

Conditions préalables :

- Le boîtier de programmation local est installé. Voir *Chapitre 2.2 "Installation des programmateurs à distance", page 13*.
- Un navigateur Internet pris en charge est disponible. Voir *Chapitre 9.8 "PC client - Configuration requise", page 215*.
- CLIQ Connect PC est installé et en cours d'exécution sur l'ordinateur.

  Voir *Chapitre 2.3 "Installation de CLIQ Connect PC", page 13*.
- CLIQ Connect PC est configuré et connecté à CWM.

  Voir *Chapitre 2.4 "Configuration de CLIQ Connect PC", page 14*.
- La clé de programmation maîtresse avec son code PIN est disponible.
- Un certificat valide pour la clé de programmation maîtresse est installé. Voir *Chapitre 5.2 "Installer le certificat de clé de programmation maîtresse", page 96*.
- L'URL de CWM est disponible.

1) Insérez la clé de programmation dans la fente gauche du boîtier de programmation local.
2) Rendez-vous sur la page de démarrage CWM.
3) Sélectionnez le certificat de la clé de programmation.

   La page de connexion CWM est affichée.
4) Cliquez sur **Identification**.
5) Saisissez le code PIN de la clé de programmation.

   CLIQ Connect PC demande de confirmer l'utilisation de la clé.
6) Cliquez sur **Confirmation**.
7) Sélectionnez le **Fuseau horaire de base** dans la liste déroulante.

   REMARQUE !
   Ce paramètre ne peut pas être modifié dès lors que vous avez cliqué sur **Confirmation**.

8) Sélectionnez les choix pour l'option **Approbation des demandes de journal des événements** parmi ceux qui suivent :

   - **Désactivé**

     Si cette option est cochée, tous les administrateurs peuvent demander des informations sur le journal des événements sans approbation d'un autre administrateur.
   - **Activé**

Si cette option est cochée, tous les administrateurs doivent obtenir l'approbation d'un autre administrateur pour obtenir des informations sur le journal des événements.

Pour plus de détails sur le rôle d'approbateur des journaux d'événements, voir *Chapitre 4.11.6 "Approbation des demandes de journal des événements", page 94*.

9) Cliquez sur **Activer importation d'extension**.

La fenêtre **Confirmation** est ouverte.

10) Vérifiez soigneusement les réglages.

> **AVERTISSEMENT !**
> Les réglages ne peuvent pas être modifiés ultérieurement.

11) Cliquez sur **Confirmation**.

5.4 Exécution de la configuration initiale

1) Débloquez le système de fermeture. Voir *Chapitre 6.3 "Débloquer le Système", page 100*.
2) Modifiez les réglages système. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.
3) Installez les bornes d'actualisation. Voir *Chapitre 6.5.1 "Installation des bornes d'actualisation", page 105*.
4) Créez les domaines. Voir *Chapitre 6.6.4 "Création et suppression de domaines", page 126*.
5) Spécifiez le domaine des cylindres et des groupes de cylindres. Voir *Chapitre 6.6.7 "Changement du domaine de cylindres", page 128* et *Chapitre 6.6.8 "Changement du domaine de groupes de cylindres", page 128*.
6) Installez les profils d'accès. Voir *Chapitre 4.6.2 "Création et suppression de profils d'accès", page 69*.
7) Créez les modèles de reçu pour les reçus de remise et de retour. *Chapitre 6.9 "Gestion des modèles de reçu", page 132*.
8) Créez les modèles de planning. Voir *Chapitre 6.10 "Gestion des modèles de planning", page 134*.
9) Ajoutez et supprimez les rôles administrateur et configurez les autorisations de rôle comme désiré. Voir *Chapitre 6.7 "Gestion des rôles et des autorisations", page 129*.
10) Délivrez les clés de programmation aux administrateurs du système de fermeture. Voir *Chapitre 6.11.7 "Remise de clés de programmation", page 139*.
11) Importez les informations employé dans CWM. Voir *Chapitre 6.8 "Importer les informations employé", page 131*.

6 Configuration des systèmes de fermeture

6.1 Gestion des licences

6.1.1 Installation des licences

Conditions préalables :

- Un nouveau fichier de licence est disponible.
  - Pour l'installer manuellement : La licence est enregistrée sur une clé USB ou sur le disque dur de l'ordinateur.
  - Pour une récupération automatique dans les systèmes avec Intégration DCS : La licence est enregistrée dans DCS.
- La nouvelle licence a un numéro supérieur à celui de la licence installée. Il est impossible d'installer une licence plus ancienne.

1) Sélectionnez **Administration » Licence**.

   Les informations concernant la licence installée et ses caractéristiques s'affichent.
2) Dans le cas de systèmes avec Intégration DCS, pour lesquels la licence est enregistrée dans DCS :

   Cliquez sur **Récupérer une licence**.

   La licence est téléchargée et installée.
3) Dans le cas de systèmes sans Intégration DCS ou pour lesquels la licence n'est pas disponible dans DCS :
   a) Cliquez sur **Sélectionner...**.
   b) Sélectionnez le fichier de la licence.
   c) Cliquez sur **Télécharger**.

      La licence est chargée et installée.

6.1.2 Affichage du statut de la licence

1) Sélectionnez **Administration » Licence**.

   Les informations concernant la licence installée et ses caractéristiques s'affichent.

Pour installer une nouvelle licence, voir *Chapitre 6.1.1 "Installation des licences", page 99*.

6.2 Blocage du système pour maintenance

Un système de fermeture peut être bloqué pour effectuer la maintenance.

1) Sélectionnez **Administration » Maintenance**.
2) Sélectionnez une date et une heure auxquelles bloquer le système spécifique pour maintenance.

   L'heure choisie doit se situer au moins 10 minutes dans le futur.
3) Cliquez sur **Bloquer système**.

6.3 Débloquer le Système

1) Sélectionnez **Administration » Maintenance**.
2) Cliquez sur **Débloquer système**.

6.4 Modifier les réglages du système

Certains des réglages décrits ici s'appliquent uniquement aux systèmes à distance.

1) Sélectionnez **Administration » Réglages du système**.

   Les réglages système s'affichent.
2) Pour modifier les réglages du système, cliquez sur **Modifier**.
3) Mettez à jour les réglages requis :

SYSTÈME

- **Approbations**. Si cette option est sélectionnée, les demandes de journaux des événements de cylindres et de clés doivent être approuvées avant de pouvoir collecter les journaux des événements.

  REMARQUE !
  Restrictions :
  - Connecté avec la clé de programmation maîtresse.
  - Avant de désactiver la fonction d'approbation, vérifiez que toutes les tâches de journal des événements en attente sont annulées ou terminées.
  - Pour activer la fonction d'approbation, veillez d'abord à désactiver **RÉCUPÉRATION AUTOMATIQUE DU JOURNAL DES ÉVÉNEMENTS** sur toutes les clés de programmation. Voir *Chapitre 6.11.13 "Activer ou désactiver la récupération automatique du journal des événements de la clé de programmation", page 144*.

    Après avoir activé la fonction d'approbation, les tâches en attente existantes ne sont pas affectées et ne nécessitent pas d'approbation. Seules les nouvelles tâches de journaux des événements doivent être approuvées.
- **Système CLIQ Remote** indique si la fonctionnalité à distance est ou non activée.

  Est uniquement sélectionnable à la première installation du système de fermeture.
- **Supporte les groupes de cylindres** indique si l'utilisation des groupes de cylindres est ou non activée.

  Est uniquement sélectionnable à la première installation du système de fermeture.
- **Fuseau horaire de base**. Fuseau horaire utilisé pour différentes impressions dans l'application.

Est uniquement sélectionnable à la première installation du système de fermeture.

- **Intégration de services web** permet la communication avec d'autres systèmes, les systèmes RH par exemple.
- **Messagerie utilisateur** autorise CWM à envoyer des e-mails aux employés et aux visiteurs, par exemple.
  - **E-mails après la mise à jour à distance** permet qu'un e-mail comportant les nouvelles informations d'accès soit envoyé aux possesseurs de clés après une mise à jour à distance.

    Cochez la case et cliquez sur **Configurer** pour choisir d'inclure ou non les cylindres mécaniques à cet e-mail.
  - **E-mails après la modification des données des employés** détermine si un e-mail listant les modifications apportées aux informations sur les employés est envoyé à l'administrateur des domaines pour lesquels la clé de l'employé a un accès effectif ou en attente à au moins un cylindre.

    Cocher la case et cliquer sur **Configurer** pour sélectionner le type de modifications générant une notification.
  - **E-mails après la modification des données des visiteurs** permet qu'un e-mail comportant les modifications apportées aux données du visiteur soit envoyé à l'administrateur des domaines pour lesquels la clé du visiteur a un accès effectif ou en attente à au moins un cylindre.

    Cocher la case et cliquer sur **Configurer** pour sélectionner le type de modifications générant une notification.
  - **E-mails après passage hors ligne du boîtier de programmation mural** permet qu'un e-mail soit envoyé à la personne spécifiée lorsqu'un boîtier de programmation mural passe hors ligne.

    Cochez la case et cliquez sur **Configurer** pour entrer le destinataire du courrier et définir le nombre de pulsations consécutives manquantes après lequel la notification est envoyée.
- **Revalidation flexible** permet le réglage de l'intervalle de revalidation par profil d'accès et par groupe de cylindres.
- **Bloquer automatiquement les clés perdues dans le cylindre lors de la mise à jour de l'autorisation**

  Cochez cette case pour permettre au système d'ajouter automatiquement les clés perdues à la liste des clés non autorisées afin de les bloquer dans les cylindres.
- **Bloquer la clé perdue avec les clés utilisateur** permet de programmer une tâche de blocage de cylindre sur n'importe quelle clé utilisateur (clé dynamique) afin de bloquer une clé perdue dans les cylindres.

  Ceci n'est applicable qu'à un système à distance.
- **Bloquer les clés perdues dans les nouveaux cylindres pendant l'importation d'extension** Lors de l'ajout de cylindres à un système, il peut être nécessaire de bloquer les clés précédemment déclarées comme perdues sur les nouveaux cylindres. Si ce réglage est activé, CWM génère

automatiquement des tâches de programmation des cylindres pour bloquer les clés perdues lorsque le fichier d'importation est activé.

- **Administrateurs hiérarchiques** (modifiable uniquement par les Super administrateurs)

  Cochez cette case pour activer la fonctionnalité de hiérarchie des administrateurs, de sorte que l'utilisateur puisse choisir une structure plane ou hiérarchique pour les permissions.

CLIQ REMOTE

- **URL service**. Le serveur utilisé par CWM et les boîtiers de programmation à distance. Il est à noter qu'un avertissement est affiché si l'URL ne correspond pas au nom de l'hôte défini dans le certificat du serveur à distance.
- **Autre URL service**. Option pour spécifier une autre URL au serveur Remote utilisé par CWM et les boîtiers de programmation à distance. L'URL est visible dans l'onglet **Réglages** de l'affichage des boîtiers de programmation à distance uniquement si la version du microprogramme du boîtier de programmation mural ou du boîtier de programmation mobile CLIQ est 4.0 ou supérieure. Il est à noter que **Autre URL service** cible le même serveur à distance que le **URL service**.
- **Certificat CA serveur**. Certificat de l'autorité de certification (AC) délivrant le certificat de serveur sur le serveur CLIQ Remote. Il faut avoir des droits de super administrateur pour importer le certificat.

RÉGLAGES PAR DÉFAUT DE LA CLÉ

- **Activer la revalidation lors de la remise**. Si elle est sélectionnée, l'option de revalidation est disponible dans le flux de remise de la clé.
- **Intervalle de revalidation**. Réglage par défaut de l'intervalle de revalidation de clé.
- **Activer la validation du code PIN lors de la remise**. Si elle est sélectionnée, l'option de validation par code PIN est disponible dans le flux de remise de la clé.
- **Intervalle de validation de code PIN**. Réglage par défaut de l'intervalle de validation de code PIN.
- **Temps jusqu'à remise**. Réglage par défaut du temps restant avant que la clé doive être retournée, à partir de la date de remise. Saisissez `0` si l'heure de fin n'est pas à spécifier.
- **Réglage de validité**. Réglage par défaut de la validité des clés.
- **Durée de validité**. Réglage par défaut de la durée de la validité de la clé lorsque l'option de validité **Active entre les dates sélectionnées** est sélectionnée.

ADMINISTRATION

- **Jours par défaut dans la recherche de clés périmées**. Option de recherche par défaut pour les clés périmées.
- **Langue de messagerie utilisateur**. Langue utilisée pour les e-mails envoyés par CWM, par exemple pour des clés périmées.

- **Reçus de clé** définit si les reçus de remise et de retour doivent être imprimés séparément ou ensemble.
- **Liens externes, URL racine**. URL racine utilisée afin de créer des liens externes pour des clés, des employés, etc.
- **Délimiteur CSV**, un point-virgule ou une virgule est sélectionné pour délimiter les entités lors de l'exportation de fichiers CSV.
- **Journaux des événements et événements**. Les journaux des événements et les événements dont l'ancienneté est supérieure à un nombre de jours définis sont automatiquement supprimés de l'archive des journaux des événements et des événements. Les jours sont comptés à partir de la date à laquelle les journaux des événements et les événements ont été collectés.

  La période de conservation des événements et du journal des événements peut être définie de 1 à 366 jours, par défaut, puis au-delà et jusqu'à 3660 jours en souscrivant une licence supplémentaire.

  À partir de CWM 11.6, la suppression suit la date de création, qui correspond à la date à laquelle l'entrée a été générée sur l'élément physique. Cette méthode remplace la précédente qui consistait à utiliser la date d'analyse, c'est-à-dire la date à laquelle l'entrée a été stockée dans la base de données CWM.
- **Lors de la suppression de personnes**. Si cette option est configurée sur **Marquer comme supprimé**, la suppression d'une personne modifie le statut de cette personne en « supprimé », mais toutes les informations sont conservées dans la base de données. Si cette option est configurée sur **Supprimer de manière permanente** (réglage par défaut des nouveaux systèmes de verrouillage), la suppression d'une personne retire cette personne ainsi que les informations la concernant de la base de données. Le réglage **Supprimer de manière permanente** prend en charge le RGPD et active la fonctionnalité permettant de désactiver une personne. Voir *Chapitre 8.9 "Suppression des données personnelles et conformité RGPD", page 193* pour plus d'informations.

  Lorsque le réglage est modifié de **Marquer comme supprimé** en **Supprimer de manière permanente**, toutes les personnes marquées comme supprimées sont retirées de manière permanente.

  Pour modifier le réglage de **Supprimer de manière permanente** en **Marquer comme supprimé**, toutes les personnes désactivées doivent tout d'abord être activées.
- **Dernière date d'identification récupérée** indique si la date de dernière connexion est collectée pour un certificat de clé de programmation. Si cette option est activée, la **Date de dernière utilisation** est affichée dans l'onglet **Certificats** de la vue détaillée de la clé de programmation. Voir *Chapitre 6.11.14 "Liste des certificats de clé de programmation", page 144*.
- **Champs client de cylindre** définissent les champs personnalisés pour enregistrer d'autres informations de cylindre dans CWM. La valeur des champs personnalisés peut être modifiée dans la vue détaillée de chaque cylindre. Ces champs peuvent également être utilisés pour trouver des cylindres à l'aide de la recherche avancée.
- **Domaine initial de cylindres** définit le domaine attribué pour les cylindres nouveaux ou importés.

- **Domaine initial de personne** définit le domaine attribué pour les employés ou visiteurs nouveaux ou importés.
- **Domaine initial de clé** définit le domaine attribué pour les clés nouvelles ou importées.

AUTHENTIFICATION RÉSEAU POUR UN BOÎTIER DE PROGRAMMATION MURAL DE GÉNÉRATION 2

- **Authentification 802.1x**

  Si l'authentification réseau pour un boîtier de programmation mural du système est activée, il n'est pas possible de sélectionner **Désactivé** au niveau des réglages du système. Cliquez sur **Comment désactiver l'authentification ?** et récupérez la liste des boîtiers de programmation muraux dont l'authentification réseau est activée. Pour désactiver l'authentification réseau au niveau de l'appareil, voir *Chapitre 6.5.7.1 "Modification des réglages du boîtier de programmation mural", page 111*.

- **Nom d'hôte du serveur d'authentification 802.1x**

  Saisissez le nom d'hôte du serveur.

- **Certificat CA du serveur 802.1x**

  Tous les certificats sont répertoriés ici. Si un certificat n'est pas valide, un message d'erreur s'affiche sous le certificat.

  Vous pouvez télécharger jusqu'à 3 certificats au format .pem.

  Pour télécharger un certificat CA :

  a) Cliquez sur **Sélectionner nouveau...**, puis sélectionnez un certificat CA (`. pem`).

  b) Cliquez sur **Télécharger certificat**.

  Le certificat CA est alors affiché.

INTÉGRATION LDAP

- **Activé**. Si sélectionnée, l'option d'intégration LDAP est disponible.
- **Type de serveur LDAP**. Sélectionnez le type de serveur LDAP dans la liste déroulante.
- **Type de connexion**. Sélectionnez dans **START TLS** ou **LDAPS**.
- **Hôte LDAP**. Saisissez l'adresse du serveur LDAP sur le réseau.
- **Port LDAP**. Saisissez le port spécifique nécessaire pour accéder au serveur LDAP.
- **Utilisateur DN** est l'administrateur LDAP ayant accès à Base DN.
- **Mot de passe** est le mot de passe de l'administrateur.
- **Base DN** indique la racine des recherches dans Active Directory.
- **Filtre de recherche** définit les critères de recherche qui permettent de réaliser des recherches plus efficaces.

CONNEXION UNIQUE (SSO)

- **SAML activé**Si elle est sélectionnée, l'option de connexion SSO devient disponible. Pour plus d'informations sur la connexion SSO, voir *Chapitre 8.10 "Authentification unique (SSO)", page 194*.
- **Recharger la configuration SAML à l'enregistrement**Si une configuration SAML est modifiée dans la base de données et si cette option est sélectionnée, un clic sur le bouton **Enregistrer** de cette page recharge la configuration. Après l'enregistrement, le bouton **Télécharger le certificat de vérification** est affiché.
- **Recréer un certificat de vérification**Si une configuration SAML existe déjà sur le système et que cette option est sélectionnée, un clic sur le bouton **Enregistrer** de cette page crée le certificat. Cette opération peut s'avérer nécessaire si le certificat a été modifié ou a expiré. Après l'enregistrement, le bouton **Télécharger le certificat de vérification** est affiché. Téléchargez le certificat et chargez-le dans le service du fournisseur d'identifiants.

CLIQ CONNECT+

- **Afficher les cylindres accessibles**. Si cette option est sélectionnée, les utilisateurs de CLIQ Connect+ peuvent voir quels cylindres sont accessibles à partir de leur clé dans CLIQ Connect+.
- **Inclure les cylindres mécaniques**. Si cette option est sélectionnée, les cylindres mécaniques attribués au détenteur de la clé sont également visibles dans la liste des cylindres accessibles de CLIQ Connect+.
- **Afficher les profils d'accès**. Si cette option est sélectionnée, la liste des profils d'accès attribués à la clé est visible dans CLIQ Connect+

  Pour activer cette fonction, le niveau de permission de l'utilisateur doit être **Vue** ou au-dessus dans le rôle **Clé : Autorisation**. Pour modifier le niveau d'autorisation, reportez-vous à *Chapitre 6.7 "Gestion des rôles et des autorisations", page 129*.

6.5 Gestion des bornes d'actualisation

6.5.1 Installation des bornes d'actualisation

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Modifiez les informations, notes et liens externes de la boîtier de programmation à distance comme désiré.

   Voir *Chapitre 6.5.3 "Modification des informations de boîtier de programmation à distance", page 107*, *Chapitre 6.5.5 "Ajout ou suppression de notes de boîtier de programmation à distance", page 108* et *Chapitre 6.5.6 "Gestion des liens externes de boîtier de programmation à distance", page 109*.

3) Modifiez les réglages de la boîtier de programmation à distance et chargez la configuration dans la boîtier de programmation à distance. Ceci comprend l'installation du certificat.

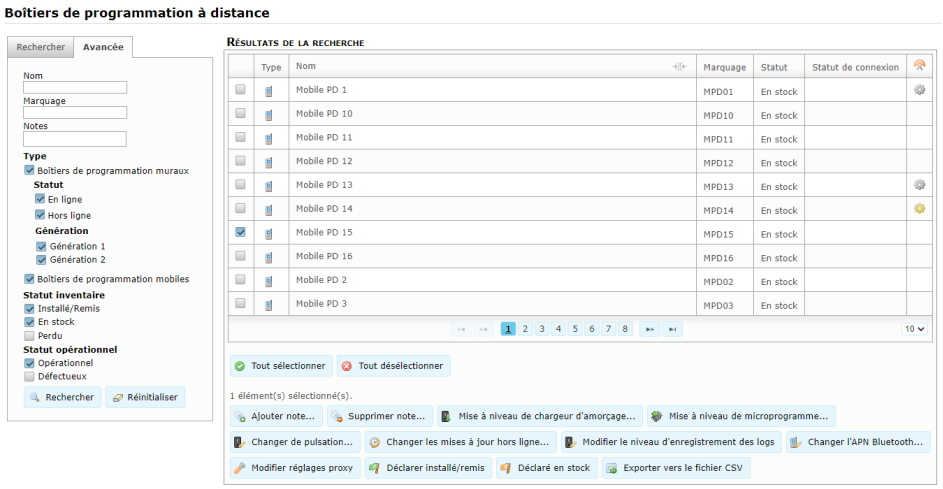
   Pour les boîtiers de programmation muraux, voir *Chapitre 6.5.7 "Configuration de boîtiers de programmation muraux", page 110*.

Pour les boîtiers de programmation mobiles CLIQ, voir *Chapitre 6.5.8.1 "Modification des réglages du boîtier de programmation mobile CLIQ", page 118*.

6.5.2 Recherche de bornes d'actualisation

1) Sélectionnez **Informations système » Boîtiers de programmation à distance**.

   Le résultat de recherche affiche une liste de bornes d'actualisation.



   Les symboles suivants sont utilisés :

   Borne de rechargement de droits

   Boîtier de programmation mobile CLIQ

> **REMARQUE !**
> Les boîtiers de programmation mobiles CLIQ Connect ne sont pas inclus dans la liste.

2) Saisissez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

   Pour filtrer la liste des résultats de recherche par type de boîtier de programmation à distance, cochez la case pour **Boîtiers de programmation muraux** ou **Bornes mobiles** sur l'onglet de recherche **Avancée**.

   Les bornes de rechargement de droits peuvent être filtrées par statut, **En ligne** ou **Hors ligne**.

3) Cliquez sur **Rechercher**.

4) Pour afficher les informations détaillées, cliquez sur la boîtier de programmation à distance correspondante.

Plusieurs bornes d'actualisation peuvent être configurées simultanément. Sélectionnez les bornes d'actualisation dans la liste de résultats de la recherche et cliquez sur un des boutons pour modifier les réglages correspondants.

6.5.3 Modification des informations de boîtier de programmation à distance

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Cliquez sur **Modifier**.
3) Pour modifier le nom de la boîtier de programmation à distance, mettez le champ **Nom** à jour.
4) Pour ajouter des notes, cliquez sur **Ajouter note...**. Voir également *Chapitre 6.5.5 "Ajout ou suppression de notes de boîtier de programmation à distance", page 108*.
5) Pour ajouter ou modifier des liens externes, cliquez sur **Ajouter lien externe...**. Voir également *Chapitre 6.5.6 "Gestion des liens externes de boîtier de programmation à distance", page 109*.
6) Cliquez sur **Enregistrer**.

6.5.4 Modification du statut des informations de la boîtier de programmation à distance

Les bornes d'actualisation ont un statut d'inventaire en stock, remis ou perdu, et un statut opérationnel étant opérationnel ou défectueux.

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) **Pour modifier le statut du boîtier de programmation mural**

   - Déclaration **Installé**
     - Passez à la vue des informations détaillées et cliquez sur **Déclarer installé** puis sur **OK**.
     - Si plusieurs dispositifs doivent être déclarés, sélectionnez Boîtiers de programmation muraux dans les résultats de recherche, cliquez sur **Déclarer installé/remis** puis sur **OK**.
   - Déclaration **En stock**
     - Passez à la vue des informations détaillées et cliquez sur **Déclaré en stock** puis sur **OK**.
     - Si plusieurs dispositifs doivent être déclarés, sélectionnez Boîtiers de programmation muraux dans les résultats de recherche, cliquez sur **Déclaré en stock** puis sur **OK**.
   - Déclaration **Perte**
     - Passez à la vue des informations détaillées et cliquez sur **Déclarée perdue** puis sur **OK**.
   - Déclaration **Retrouvé**
     - Passez à la vue des informations détaillées et cliquez sur **Déclarée trouvée** puis sur **OK**.
   - Déclaration **Défectueux**

- Passez à la vue des informations détaillées et cliquez sur **Déclarer défectueux** puis sur **OK**.

- Déclaration **Opérationnel**

  - Passez à la vue des informations détaillées et cliquez sur **Déclarer opérationnel** puis sur **OK**.

3) **Pour changer le statut du Boîtier de programmation CLIQ Mobile**

- Déclaration **Remis**

  - Passez à la vue des informations détaillées et cliquez sur **Remettre** puis sur **OK**.
  - Si plusieurs dispositifs doivent être déclarés, sélectionnez Boîtiers de programmation muraux dans les résultats de recherche, cliquez sur **Déclarer installé/remis** puis sur **OK**.

- Déclaration **En stock**

  - Passez à la vue des informations détaillées et cliquez sur **Retourner** puis sur **OK**.
  - Si plusieurs dispositifs doivent être déclarés, sélectionnez Boîtiers de programmation muraux dans les résultats de recherche, cliquez sur **Déclaré en stock** puis sur **OK**.

- Déclaration **Perte**

  - Passez à la vue des informations détaillées et cliquez sur **Déclarée perdue** puis sur **OK**.

- Déclaration **Retrouvé**

  - Passez à la vue des informations détaillées et cliquez sur **Déclarée trouvée** puis sur **OK**.

- Déclaration **Défectueux**

  - Passez à la vue des informations détaillées et cliquez sur **Déclarer défectueux** puis sur **OK**.

- Déclaration **Opérationnel**

  - Passez à la vue des informations détaillées et cliquez sur **Déclarer opérationnel** puis sur **OK**.

6.5.5 Ajout ou suppression de notes de boîtier de programmation à distance

1) Sélectionnez **Informations système » Boîtiers de programmation à distance**.

   Une liste de tous les boîtiers de programmation à distance s'affiche.

- Pour ajouter ou supprimer des notes pour un boîtier de programmation à distance, allez à l'*Étape 2*.
- Pour ajouter ou supprimer des notes pour plusieurs boîtiers de programmation à distance, allez à l'*Étape 3*.

2) **Pour ajouter ou supprimer des notes pour un boîtier de programmation à distance :**

1. Sélectionnez le boîtier de programmation à distance et accédez à ses informations détaillées.
2. Cliquez sur **Modifier**.
3. Ajouter ou supprimer une note pour un boîtier de programmation à distance.

   Pour ajouter une note :

   a) Cliquez sur **Ajouter note...**.
   b) Saisissez un nom pour la note.
   c) Cliquez sur **OK**.

   Pour supprimer une note :
   Cliquez sur la note à supprimer.
4. Cliquez sur **Enregistrer**.

3) **Pour ajouter ou supprimer des notes pour plusieurs boîtiers de programmation à distance :**

1. Sélectionnez des boîtiers de programmation à distance dans les résultats de recherche en cochant les cases correspondantes.
2. **Pour ajouter une note :**

   a) Cliquez sur **Ajouter note...**.
   b) Entrez un nom pour la note.
   c) Cliquez sur **OK**.

   Pour supprimer une note :

   a) Cliquez sur **Supprimer note...**.
   b) Entrez un nom pour la note.
   c) Cliquez sur **OK**.

Voir également *Chapitre 8.2.6 "Notes", page 183*.

6.5.6 Gestion des liens externes de boîtier de programmation à distance

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Cliquez sur **Modifier**.
3) **Pour ajouter un lien externe :**

1. Cliquez sur **Ajouter.**
2. Saisissez un **Nom** pour l'URL.
3. Saisissez l'**URL**. L'**URL** doit commencer par un protocole (http:// ou ftp://, par exemple).

Si une URL racine a été définie dans les **Réglages système** (élément **Liens externes, URL racine**) il suffit d'ajouter la dernière partie de l'URL. Voir également *Chapitre 6.4 "Modifier les réglages du système", page 100*.

4. Cliquez sur **OK**.

Pour modifier un lien externe :

1. Cliquez sur **Modifier** à côté du lien externe à modifier.
2. Mettez les champs à jour.
3. Cliquez sur **OK**.

Pour supprimer un lien externe :

Cliquez sur **Supprimer** à côté du lien externe à supprimer.

4) Cliquez sur **Enregistrer**.

Voir également *Chapitre 8.4 "Liens externes", page 186*.

6.5.7 Gestion des réglages et du certificat du boîtier de programmation mural

Conditions préalables :

- Pour un boîtier de programmation mural configuré pour la première fois, **Plug and play** étant désactivé, ou ne pouvant pas se connecter avec les réglages existants :
  - Un câble USB :
    - **Boîtier de programmation mural de génération 1 :** câble Mini USB On-The-Go (OTG) mâle (de type A ou B) vers USB Standard femelle (de type A).

    - **Boîtier de programmation mural de génération 2 :** câble USB-C mâle vers USB Standard femelle (de type A).
  - Une clé USB :
    - **Boîtier de programmation mural de génération 1 :** formatée avec le système de fichier FAT32. La taille recommandée de la clé est de 8 à 16 Go.
    - **Boîtier de programmation mural de génération 2 :** formatée avec le système de fichier FAT32. La taille de la clé USB n'est pas limitée. Utilisez une clé USB-C ou connectez une clé USB-A avec un adaptateur ou un câble standard.
- Pour utiliser la mise à jour hors ligne :
  - Un boîtier de programmation mural de génération 1 avec microprogramme 2.11 ou supérieur ou un boîtier de programmation mural de génération 2.

- Pour installer ou renouveler des certificats **sans** Intégration DCS :
  - Un fichier de certificat .p12. Il est obtenu auprès d'un revendeur CLIQ local.

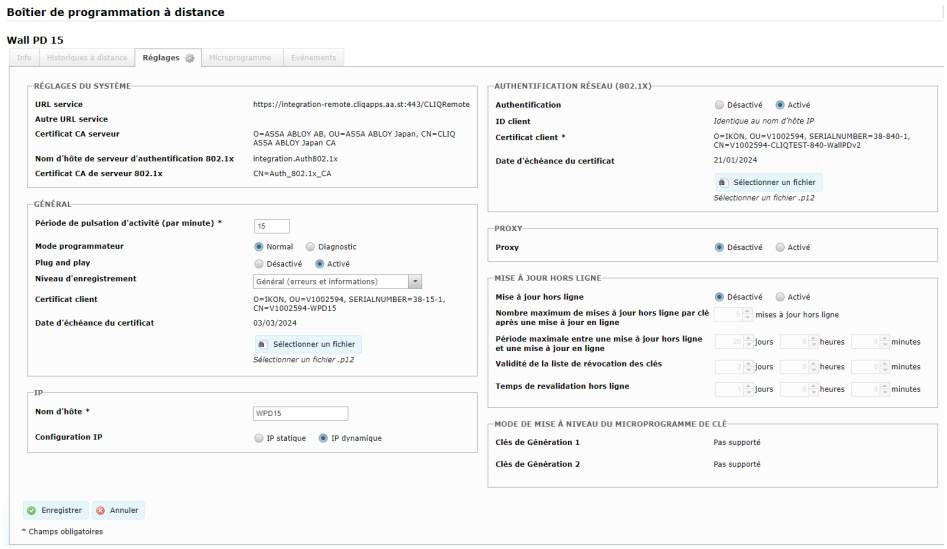
6.5.7.1 Modification des réglages du boîtier de programmation mural

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Sélectionnez l'onglet **Réglages**.

3) Cliquez sur **Modifier**.



4) Mettez à jour les réglages requis :

GÉNÉRAL

- **Période de pulsation d'activité (par minute)**

  Valeur recommandée : 15.

  La fréquence de pulsation est le nombre de minutes entre chaque pulsation envoyée par la borne de rechargement de droits au serveur CLIQ Remote pour signaler à CWM qu'il est en ligne. La borne de rechargement de droits vérifie les mises à jour de borne de rechargement de droits (mises à jour de microprogramme ou de configuration) lorsqu'elle envoie chaque pulsation.

- **Mode programmateur**

  Sélectionnez **Normal**. Ne sélectionnez pas **Diagnostic** à moins d'y avoir été invité par l'assistance technique.

- **Plug and play**

> **REMARQUE !**
> Pour pouvoir fonctionner, **Plug and play** nécessite l'activation de l'intégration DCS et la désactivation de **Réglages proxy**.

Plug and play active le boîtier de programmation à distance pour recevoir automatiquement un certificat d'un serveur, s'il n'en possède pas encore. Le certificat est téléchargé du DCS via l'application d'enregistrement.

Sélectionnez **Activé** (réglage par défaut recommandé) si le boîtier de programmation à distance est utilisé dans un réseau connecté à Internet sans restrictions. Sélectionnez **Désactivé** si un certificat est téléchargé sur le boîtier de programmation à distance en utilisant une clé USB.

- **Niveau d'enregistrement** (Boîtier de programmation de génération 2 uniquement)

  Les boîtiers de programmation muraux envoient des logs d'erreur au serveur Remote et les enregistrements sont conservés en un même endroit pendant 10 jours. Le niveau d'enregistrement est configurable pour les boîtiers de programmation muraux de génération 2 à partir des niveaux suivants :

  - **Critique (erreurs seulement)**
  - **Général (erreurs et informations)**
  - **Détaillé (erreurs, informations et débogage)**
  - **Pas d'enregistrement**

> **Conseil**
> Il est également possible d'appliquer le même niveau d'enregistrement à plusieurs boîtiers de programmation muraux de génération 2 depuis la liste des boîtiers de programmation à distance.

IP

- **Nom d'hôte**

  Le nom d'hôte est le nom de la borne de rechargement de droits sur le réseau. Il est recommandé d'utiliser des noms d'hôtes représentatifs pour identifier facilement le boîtier de programmation à distance lors du dépannage.

- **Configuration IP**

  Sélectionnez **IP statique** ou **IP dynamique**.

  Dans le cas où **IP statique** est sélectionnée, saisissez **Adresse IP**, **Masque de sous réseau**, **Passerelle** et **DNS**.

AUTHENTIFICATION RÉSEAU (802.1X) (Boîtier de programmation mural de génération 2 uniquement)

- **Authentification**

  Sélectionnez **Désactivé** ou **Activé**.

REMARQUE !
Lorsque l'AUTHENTIFICATION RÉSEAU (802.1X) est activée pour la première fois, le boîtier de programmation mural doit être configuré à l'aide d'une clé USB.

Pour des informations plus détaillées, consultez *Chapitre 6.5.7.3 "Configuration d'un boîtier de programmation mural avec AUTHENTIFICATION RÉSEAU (802.1X)", page 116*.

- **ID client** est identique au nom d'hôte IP.
- **Certificat client**

  Un certificat client est affiché ici.

  Pour télécharger le certificat client :

  a) Cliquez sur **Sélectionner un fichier...**.
  b) Dans une fenêtre pop-up, saisissez le mot de passe du fichier certificat, puis cliquez sur **Sélectionner...**.
  c) Dans l'explorateur de fichiers pop-up, sélectionnez un fichier de certificat (`. 12`).
  d) Cliquez sur **Télécharger**.

  Certificat client et **Date d'échéance du certificat** s'affichent.

Pour modifier les réglages relatifs à l'ensemble du système pour 802.1x, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

PROXY

- **Proxy**

  Dans le cas où **Activé** est sélectionnée, saisissez **Hôte**, **Port**, **Nom d'utilisateur** et **Mot de passe**.

  Hôte est l'adresse du serveur proxy sur le réseau.

  Port est le port spécifique nécessaire pour accéder au serveur proxy. Normalement, ces ports sont 8080.

MISE À JOUR HORS LIGNE
Voir également *Chapitre 8.3.3 "Mise à jour hors ligne", page 185*.

REMARQUE !
Pour mettre à jour une clé en mode hors ligne, la clé doit disposer du microprogramme version 6 ou supérieure.

- **Nombre maximal de mises à jour hors ligne après une mise à jour en ligne par clé**

  Spécifie le nombre de mises à jour pouvant être effectuées en mode hors ligne pour chaque clé avant qu'une mise à jour en ligne ne soit nécessaire.

- **Période maximale entre une mise à jour hors ligne et une mise à jour en ligne**

  Spécifie la période après la dernière mise à jour en ligne pendant laquelle les mises à jour hors ligne sont autorisées.

  La valeur définit la période au bout de laquelle la clé doit avoir été revalidée en mode en ligne.

- **Validité de la liste de révocation des clés**

  Spécifie la durée pendant laquelle la liste de révocation des clés est conservée dans le boîtier de programmation mural et pendant laquelle les mises à jour hors ligne sont autorisées. Voir également *Chapitre 8.3.3 "Mise à jour hors ligne", page 185*.

  La valeur définit la période pendant laquelle un boîtier de programmation à distance permet une revalidation hors ligne. Passée cette période, les mises à jour hors ligne ne peuvent plus être réalisées. Par exemple, si une interruption de service de 48 heures est prévue, la période définie doit être au minimum de 48 heures.

- **Temps de revalidation hors ligne**

  Précise la durée pour laquelle la validité de la clé est prolongée. L'intervalle de revalidation réglé sur les clés est ignoré lors des mises à jour hors ligne.

MODE DE MISE À NIVEAU DU MICROPROGRAMME DE CLÉ

REMARQUE !
Les boîtiers de programmation à distance de génération 2 ne prennent pas en charge la mise à niveau du microprogramme pour les clés de génération 1.

Pour activer et désactiver les mises à niveau de clé, voir *Chapitre 6.5.11 "Activation et désactivation des mises à niveau de clé dans les boîtiers de programmation à distance", page 124*.

5) Cliquez sur **Enregistrer**.

6) Transmettez la configuration mise à jour au boîtier de programmation.

- Si la borne de rechargement de droits est en ligne ou qu'il peut se connecter avec ses réglages actuels :

  Les réglages mis à jour seront envoyés à la borne de rechargement de droits à la prochaine pulsation. La borne de rechargement de droits est configurée automatiquement et se connecte au serveur à distance.

  Pour savoir si une borne de rechargement de droits est en ligne, affichez les informations détaillées.

- Si la borne est configurée pour la première fois avec **Plug and play** désactivé, ou ne pouvant pas se connecter avec les réglages actuels :

  a) Insérez une clé USB dans l'ordinateur client.

  b) Cliquez sur **Enregistrer sur fichier** et enregistrez le fichier sur le dossier racine de la clé USB.

REMARQUE !
Assurez-vous qu'aucun fichier, autre que les fichiers de configuration, ne figure dans le dossier racine de la clé USB.

Plusieurs fichiers de configuration peuvent figurer sur la même clé USB.

c) Connectez le lecteur flash USB au boîtier de programmation mural à l'aide du câble USB approprié (voir *Chapitre 6.5.7 "Configuration de boîtiers de programmation muraux", page 110*).

Le boîtier de programmation est configuré automatiquement et se connecte au serveur à distance. Cela doit prendre moins d'une minute.

7) Vérifiez que le voyant CLIQ s'allume, ce qui indique que le boîtier de programmation est en ligne et correctement configuré.

Voir *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211* ou *Chapitre 9.5.2 "Indications de boîtier de programmation mural (génération 2)", page 212*.

6.5.7.2 Installer ou renouveler un certificat de boîtier de programmation mural

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Sélectionnez l'onglet **Réglages**.

3)
- Si l'intégration DCS est activée, cliquez sur **Générer un certificat client**.

  Le certificat est créé.
- Si l'intégration DCS n'est pas activée :

  a) Cliquez sur **Modifier** pour accéder au mode Modifier.

  b) Dans la section **GÉNÉRAL**, cliquez sur **Sélectionner un fichier**.

  c) Cliquez sur **Sélectionner...** et sélectionnez le fichier certificat (.p12)

  d) Entrez le **Mot de passe du fichier certificat**.

  e) Cliquez sur **Télécharger**.

  f) Cliquez sur **Enregistrer** pour sortir du mode Modifier.

4) Transmettez la configuration mise à jour au boîtier de programmation.

- Si la borne de rechargement de droits est en ligne ou qu'il peut se connecter avec ses réglages actuels :

  Les réglages mis à jour seront envoyés à la borne de rechargement de droits à la prochaine pulsation. La borne de rechargement de droits est configurée automatiquement et se connecte au serveur à distance.

  Pour savoir si une borne de rechargement de droits est en ligne, affichez les informations détaillées.
- Si la borne est configurée pour la première fois avec **Plug and play** désactivé, ou ne pouvant pas se connecter avec les réglages actuels :

  a) Insérez une clé USB dans l'ordinateur client.

b) Cliquez sur **Enregistrer sur fichier** et enregistrez le fichier sur le dossier racine de la clé USB.

> **REMARQUE !**
> Assurez-vous qu'aucun fichier, autre que les fichiers de configuration, ne figure dans le dossier racine de la clé USB.
>
> Plusieurs fichiers de configuration peuvent figurer sur la même clé USB.

c) Connectez le lecteur flash USB au boîtier de programmation mural à l'aide du câble USB approprié (voir *Chapitre 6.5.7 "Configuration de boîtiers de programmation muraux", page 110*).

Le boîtier de programmation est configuré automatiquement et se connecte au serveur à distance. Cela doit prendre moins d'une minute.

5) Vérifiez que le voyant CLIQ s'allume, ce qui indique que le boîtier de programmation est en ligne et correctement configuré.

Voir *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211* et *Chapitre 9.5.2 "Indications de boîtier de programmation mural (génération 2)", page 212*.

6.5.7.3 Configuration d'un boîtier de programmation mural avec AUTHENTIFICATION RÉSEAU (802.1X)

Lorsque l'AUTHENTIFICATION RÉSEAU (802.1X) est activée pour la première fois, le boîtier de programmation mural doit être configuré à l'aide d'une clé USB.

> **REMARQUE !**
> Ceci ne s'applique qu'aux boîtiers de programmation muraux de génération 2.

Condition préalable :

- L'**Authentification 802.1x** est activée sur **Réglages du système**. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Sélectionnez l'onglet **Réglages**.
3) Cliquez sur **Modifier** pour accéder au mode Modifier.
4) Téléchargez le certificat client AUTHENTIFICATION RÉSEAU (802.1X) :
   a) Dans la section **AUTHENTIFICATION RÉSEAU (802.1X)**, cliquez sur **Sélectionner un fichier...**.
   b) Dans une fenêtre pop-up, saisissez le mot de passe du fichier certificat, puis cliquez sur **Sélectionner...**.
   c) Dans l'explorateur de fichiers pop-up, sélectionnez un fichier de certificat (. 12).
   d) Cliquez sur **Télécharger**.

   Certificat client et **Date d'échéance du certificat** s'affichent.

e) Cliquez sur **Enregistrer** pour sortir du mode Modifier.

5) Transmettez la configuration mise à jour au boîtier de programmation mural :

a) Insérez une clé USB dans l'ordinateur client.

b) Cliquez sur **Enregistrer sur fichier** et enregistrez le fichier sur le dossier racine de la clé USB.

> **REMARQUE !**
> Assurez-vous qu'aucun fichier, autre que les fichiers de configuration, ne figure dans le dossier racine de la clé USB.
>
> Plusieurs fichiers de configuration peuvent figurer sur la même clé USB.

c) Connectez le lecteur flash USB au boîtier de programmation mural à l'aide du câble (USB-C mâle vers USB standard femelle (type A)).

Le boîtier de programmation est configuré automatiquement et se connecte au serveur à distance.

d) Vérifiez que la LED blanche centrale du boîtier de programmation mural est allumée en continu une fois le processus terminé.

Si les témoins à LED se comportent différemment, voir *Chapitre 9.5.2 "Indications de boîtier de programmation mural (génération 2)", page 212* pour vérifier le statut.

6.5.8 Gestion des réglages et du certificat du boîtier de programmation mobile CLIQ

Conditions préalables :

- Pour les téléphones portables iPhone ou Android :
  - Un boîtier de programmation mobile CLIQ avec microprogramme 2.10 ou version supérieure.
  - Un câble Mini USB est nécessaire pour connecter le boîtier de programmation mobile CLIQ au téléphone sans utiliser Bluetooth. Pour le câble approprié, voir *Chapitre 7.4.2 "Boîtiers de programmation à distance", page 163* .
- Pour un boîtier de programmation mobile CLIQ configuré pour la première fois avec **Plug and play** désactivé ou ne pouvant pas se connecter avec les réglages existants.
  - Un câble USB On-The-Go (OTG) : USB Mini mâle (de type A ou B) vers USB Standard femelle (de type A).

  - Une clé USB formatée avec le système de fichiers FAT32. La taille recommandée de la clé est de 8 à 16 Go.
- Pour utiliser la mise à jour hors ligne :

  - Un boîtier de programmation mobile CLIQ avec microprogramme 2.10 ou version supérieure.

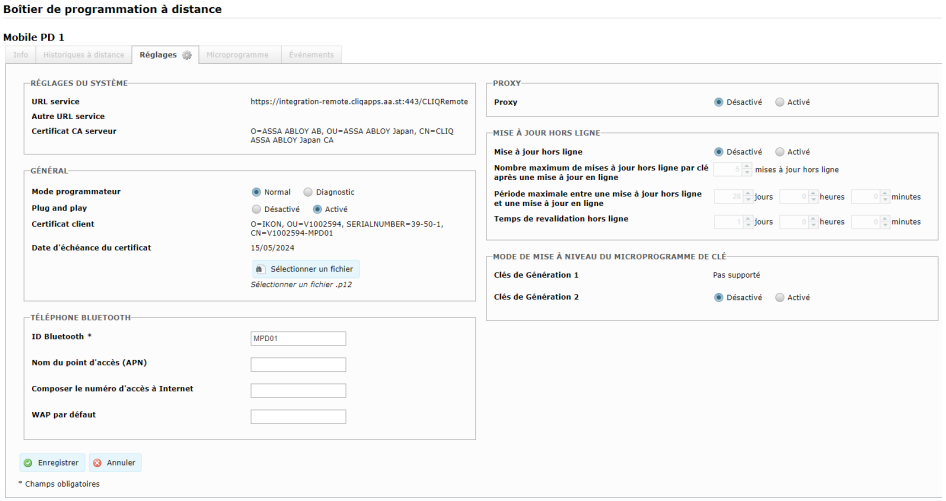
- Pour installer ou renouveler des certificats **sans** Intégration DCS :
  - Un fichier de certificat .p12. Il est obtenu auprès d'un revendeur CLIQ local.
- La documentation fournie avec le boîtier de programmation mobile CLIQ est disponible.

6.5.8.1 Modification des réglages du boîtier de programmation mobile CLIQ

1) Trouvez le boîtier de programmation CLIQ Mobile et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Sélectionnez l'onglet **Réglages**.
3) Cliquez sur **Modifier**.



4) Mettez à jour les réglages requis :

GÉNÉRAL

- **Mode programmateur**

  Sélectionnez **Normal**. Ne sélectionnez pas **Diagnostic** à moins d'y avoir été invité par l'assistance technique.

- **Plug and play**

> **REMARQUE !**
> Pour pouvoir fonctionner, **Plug and play** nécessite l'activation de l'intégration DCS et la désactivation de **Réglages proxy**.

Plug and play active le boîtier de programmation à distance pour recevoir automatiquement un certificat d'un serveur, s'il n'en possède pas encore. Le certificat est téléchargé du DCS via l'application d'enregistrement.

Sélectionnez **Activé** (réglage par défaut recommandé) si le boîtier de programmation à distance est utilisé dans un réseau connecté à Internet

sans restrictions. Sélectionnez **Désactivé** si un certificat est téléchargé sur le boîtier de programmation à distance en utilisant une clé USB.

TÉLÉPHONE BLUETOOTH

Indépendamment des **RÉGLAGES DU TÉLÉPHONE BLUETOOTH**, le boîtier de programmation mobile CLIQ peut être utilisé avec un ordinateur et une connexion par câble USB.

Si vous utilisez un téléphone

- iPhone
- Androïd
- Un autre téléphone portable prenant en charge le profil Bluetooth PAN

Laissez tous les champs dans **RÉGLAGES DU TÉLÉPHONE BLUETOOTH** vides sauf **ID Bluetooth**.

Pour utilisation avec un téléphone portable prenant en charge le profil DUN Bluetooth, saisissez les informations suivantes :

- **ID Bluetooth**

  Un nom pour le boîtier de programmation mobile CLIQ. Ce nom sera visible sur le téléphone portable lors de l'appairage avec le boîtier de programmation CLIQ Mobile.

- **Nom du point d'accès (APN)**

  Nom de la passerelle opérateur réseau entre le réseau mobile et Internet. Exemple : « online.telia.se ». Ce paramètre est donné par l'opérateur de téléphonie mobile.

- **Composer le numéro d'accès à Internet**

  Numéro à appeler pour obtenir l'accès au réseau, exemple : `*99#`. Ce réglage est obtenu auprès de l'opérateur de téléphonie mobile.

- **WAP par défaut**

  L'endroit sur le téléphone portable où sont enregistrés les réglages de connexion Internet. Il s'agit d'un paramètre spécifique au téléphone portable, et la valeur correcte est indiquée dans la documentation du téléphone. Dans la plupart des cas, ce paramètre a la valeur `1`.

PROXY

- **Proxy**

  Dans le cas où **Activé** est sélectionnée, saisissez **Hôte**, **Port**, **Nom d'utilisateur** et **Mot de passe**.

  Hôte est l'adresse du serveur proxy sur le réseau.

  Port est le port spécifique nécessaire pour accéder au serveur proxy. Normalement, ces ports sont 8080.

MISE À JOUR HORS LIGNE

REMARQUE !
Pour mettre à jour une clé en mode hors ligne, la clé doit :

- a récemment été mise à jour dans le même boîtier de programmation mobile CLIQ (elle doit figurer dans les 10 dernières clés mises à jour) ;
- disposer d'un microprogramme version 6 ou supérieure.

- **Nombre maximal de mises à jour hors ligne après une mise à jour en ligne**

  Spécifie le nombre de mises à jour pouvant être effectuées en mode hors ligne avant qu'une mise à jour en ligne ne soit nécessaire. Saisissez `0` pour désactiver la mise à jour hors ligne.

- **Période maximale entre une mise à jour hors ligne et une mise à jour en ligne**

  Spécifie la durée, à partir de la dernière mise à jour en ligne, pendant laquelle les mises à jour hors ligne sont autorisées.

- **Temps de revalidation hors ligne**

  Spécifie la durée pour laquelle la validité de la clé est prolongée. L'intervalle de revalidation réglé sur les clés est ignoré lors des mises à jour hors ligne.

MODE DE MISE À NIVEAU DU MICROPROGRAMME DE CLÉ
Pour activer et désactiver les mises à niveau de clé, voir *Chapitre 6.5.11 "Activation et désactivation des mises à niveau de clé dans les boîtiers de programmation à distance", page 124*.

5) Cliquez sur **Enregistrer**.

6) Transmettez la configuration mise à jour au boîtier de programmation CLIQ Mobile.

- Si le boîtier de programmation mobile CLIQ a déjà été configuré et peut se connecter avec les réglages actuels :

  Les réglages actualisés seront envoyés au boîtier de programmation mobile CLIQ à sa prochaine utilisation. Le boîtier de programmation est configuré automatiquement et se connecte au serveur à distance. Cela doit prendre moins d'une minute.

- Si la borne est configurée pour la première fois avec **Plug and play** désactivé, ou ne pouvant pas se connecter avec les réglages actuels :

  a) Insérez une clé USB dans l'ordinateur client.

  b) Cliquez sur **Enregistrer sur fichier** et enregistrez le fichier sur le dossier racine de la clé USB.

REMARQUE !
Assurez-vous qu'aucun fichier, autre que les fichiers de configuration, ne figure dans le dossier racine de la clé USB.

Plusieurs fichiers de configuration peuvent figurer sur la même clé USB.

c) Connectez le lecteur flash USB au boîtier de programmation CLIQ Mobile à l'aide du câble USB approprié (voir *Chapitre 6.5.8 "Configuration des boîtiers de programmation mobiles", page 117*).

d) Insérez une clé utilisateur dans le boîtier de programmation mobile CLIQ.

La configuration du boîtier de programmation mobile CLIQ est lancée.

e) Lorsque la LED de téléchargement reste allumée en continu, enlevez la clé USB.

7) Pour configurer un téléphone portable afin de l'utiliser avec le boîtier de programmation mobile CLIQ, voir la documentation séparée fournie avec le boîtier de programmation mobile CLIQ.

8) Pour configurer un ordinateur afin de l'utiliser avec le boîtier de programmation mobile CLIQ :

   a) Installez **ASSA ABLOY Network Provider** sur l'ordinateur client.

   b) Utilisez un câble mini-USB pour relier l'ordinateur client au boîtier de programmation CLIQ Mobile. Pour le câble approprié, voir *Chapitre 6.5.8 "Configuration des boîtiers de programmation mobiles", page 117*.

9) Pour vérifier que la configuration est correcte :

   a) Insérez une clé utilisateur dans le boîtier de programmation mobile CLIQ.

   Le boîtier de programmation s'allume et se connecte au serveur à distance. Cela ne doit pas prendre plus d'une minute.

   b) Vérifiez que les LED CLIQ sont allumées en continu.

Cela indique que le boîtier de programmation est en ligne et qu'il est correctement configuré.

Voir également *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211*.

6.5.8.2 Installation ou renouvellement d'un certificat de boîtier de programmation CLIQ Mobile

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Sélectionnez l'onglet **Réglages**.

3) Pour installer ou renouveler un certificat :

   - Si l'intégration DCS est activée, cliquez sur **Créer certificat**.

Le certificat est créé.

- Si l'intégration DCS n'est pas activée et si le fichier de certificat est fourni par le revendeur CLIQ local :

  a) Cliquez sur **Modifier** pour accéder au mode Modifier.

  b) Dans la section **GÉNÉRAL**, cliquez sur **Sélectionner un fichier**.

  c) Cliquez sur **Sélectionner...** et sélectionnez le fichier certificat (.p12)

  d) Entrez le **Mot de passe du fichier certificat**.

  e) Cliquez sur **Télécharger**.

  f) Cliquez sur **Enregistrer** pour sortir du mode Modifier.

4) Transmettez la configuration mise à jour au boîtier de programmation.

- Si le boîtier de programmation mobile CLIQ a déjà été configuré et peut se connecter avec les réglages actuels :

  Cliquez sur **Enregistrer**.

  Les réglages actualisés seront envoyés au boîtier de programmation mobile CLIQ à sa prochaine utilisation. Le boîtier de programmation est configuré automatiquement et se connecte au serveur à distance. Cela doit prendre moins d'une minute.

- Si le boîtier de programmation CLIQ Mobile est configuré pour la première fois avec **Plug and play** désactivé, ou ne peut pas se connecter avec les réglages actuels :

  a) Insérez une clé USB dans l'ordinateur client.

  b) Cliquez sur **Enregistrer sur fichier** et enregistrez le fichier sur le dossier racine de la clé USB.

  > **REMARQUE !**
  > Assurez-vous qu'aucun fichier, autre que les fichiers de configuration, ne figure dans le dossier racine de la clé USB.
  >
  > Plusieurs fichiers de configuration peuvent figurer sur la même clé USB.

  c) Connectez le lecteur flash USB au boîtier de programmation CLIQ Mobile à l'aide du câble USB approprié (voir *Chapitre 6.5.8 "Configuration des boîtiers de programmation mobiles", page 117*).

  d) Insérez une clé utilisateur dans le boîtier de programmation mobile CLIQ.

  La configuration du boîtier de programmation mobile CLIQ est lancée.

  e) Lorsque la LED de téléchargement reste allumée en continu, enlevez la clé USB.

5) Pour configurer un téléphone portable afin de l'utiliser avec le boîtier de programmation mobile CLIQ, voir la documentation séparée fournie avec le boîtier de programmation mobile CLIQ.

6) Pour configurer un ordinateur afin de l'utiliser avec le boîtier de programmation mobile CLIQ :

   a) Installez **ASSA ABLOY Network Provider** sur l'ordinateur client.

   b) Utilisez un câble mini-USB pour relier l'ordinateur client au boîtier de programmation CLIQ Mobile. Pour le câble approprié, voir *Chapitre 7.4.2 "Boîtiers de programmation à distance", page 163*.

7) Pour vérifier que la configuration est correcte :

   a) Insérez une clé utilisateur dans le boîtier de programmation mobile CLIQ.

   Le boîtier de programmation s'allume et se connecte au serveur à distance. Cela ne doit pas prendre plus d'une minute.

   b) Vérifiez que les LED CLIQ sont allumées en continu.

   Cela indique que le boîtier de programmation est en ligne et qu'il est correctement configuré.

Voir également *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211*.

6.5.9 Affichage de l'historique de boîtier de programmation à distance

L'historique présente les événements et faits que les bornes d'actualisation ont signalés à CLIQ Web Manager.

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Sélectionnez l'onglet **Historique**.

6.5.10 Activation et désactivation de la messagerie hors ligne du boîtier de programmation mural

Lorsqu'un boîtier de programmation mural cesse d'envoyer des pulsations pendant un certain temps, Web CLIQ Manager détecte qu'il est hors ligne et envoie un e-mail à une personne déterminée. Cette section explique comment paramétrer cette fonction.

1) Sélectionnez **Administration » Réglages du système**.

   Les réglages système s'affichent.

2) Cliquez sur **Modifier**.

3) Dans la section SYSTÈME, trouvez **E-mails après passage hors ligne du boîtier de programmation mural** sous **Messagerie utilisateur**.

4) • Pour ne pas recevoir l'e-mail, décochez la case, et passez à *Étape 8*.
   • Pour recevoir l'e-mail, cochez la case et passez à l'étape suivante.

   Le bouton **Configurer** situé à côté de la case à cocher devient bleu.

5) Cliquez sur **Configurer**.

   La fenêtre de réglage s'ouvre.

6) Saisissez l'adresse e-mail à laquelle le message est envoyé lorsqu'un boîtier de programmation mural devient hors ligne.

7) Entrez le nombre de pulsations manquantes après lequel l'e-mail est envoyé.

8) Cliquez sur **OK**.

6.5.11 Activation et désactivation des mises à niveau de clé dans les boîtiers de programmation à distance

Pour de plus amples informations sur la mise à niveau de clés, y compris les versions du microprogramme à utiliser, voir *Chapitre 6.15.3 "Mise à niveau de microprogramme sur clés", page 150*.

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Sélectionnez l'onglet **Réglages**.

3) Pour mettre à niveau les clés de génération 1 :

   Pour activer les mises à niveau de clé :
   Dans **Réglages du mode de mise à niveau du microprogramme de clé**, cliquez sur **Commutation en mode mise à jour de clés**.

   Ce bouton est seulement visible une fois l'importation des fichiers de microprogramme nécessaires effectuée, voir *Chapitre 6.15.3 "Mise à niveau de microprogramme sur clés", page 150*.

   Pour désactiver les mises à niveau de clé :
   Dans **Réglages du mode de mise à niveau du microprogramme de clé**, cliquez sur **Passer en mode normal**.

4) Pour mettre à niveau les clés de génération 2 :

   Pour activer les mises à niveau de clé :

   1. Cliquez sur **Modifier**.
   2. Dans **Réglages du mode de mise à niveau du microprogramme de clé**, sélectionnez **Activé**.
   3. Cliquez sur **Enregistrer**.

   REMARQUE !
   Des bornes d'actualisation multiples peuvent être sélectionnées pour la mise à niveau des clés de génération 2.

   Répétez l'*Étape 5 c* de la *Chapitre 6.15.3 "Mise à niveau de microprogramme sur clés", page 150* pour chaque boîtier de programmation à distance à utiliser pour la mise à niveau de clés.

Pour désactiver les mises à niveau de clé :

1. Cliquez sur **Modifier**.
2. Dans **Réglages du mode de mise à niveau du microprogramme de clé**, sélectionnez **Désactivé**.
3. Cliquez sur **Enregistrer**.

6.5.12 Exportation des informations de boîtier de programmation à distance

1) Trouvez le boîtier de programmation à distance et accédez à ses informations détaillées.

   Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

2) Dans les résultats de recherche, sélectionnez les bornes d'actualisation dont les données doivent être exportées.
3) Cliquez sur **Exporter vers le fichier CSV**.
4) Dans la fenêtre pop-up de téléchargement de fichiers, cliquez sur **OK**.

   Un fichier CSV est téléchargé dans le dossier **Téléchargements**.

> **REMARQUE !**
> Pour pouvoir ouvrir correctement le fichier dans Excel, le délimiteur du fichier doit être défini selon les réglages régionaux. Pour modifier le délimiteur, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

6.6 Gestion des domaines

6.6.1 Recherche de domaines

1) Sélectionnez **Administration » Domaines**.

   La liste de tous les domaines apparaît.

2) Saisissez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

3) Cliquez sur **Rechercher**.
4) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur la ligne du domaine correspondant.

6.6.2 Modification des informations sur le domaine

1) Localisez le domaine à modifier.

   Voir *Chapitre 6.6.1 "Recherche de domaines", page 125*.

2) Dans la liste des résultats de la recherche, cliquez sur le nom du domaine.
3) Cliquez sur **Modifier**.
4) Saisissez le nom et la description du domaine.
5) Cliquez sur **Enregistrer**.

6.6.3 Réglages des domaines initiaux pour les objets nouveaux ou importés

Les objets nouveaux ou importés sont attribués au domaine initial correspondant.

Les domaines initiaux existent pour les objets suivants :

- clés
- personnes (employés et visiteurs)
- cylindres (et groupes de cylindre)

> **REMARQUE !**
> Les nouveaux cylindres et les cylindres importés appartenant à un groupe de cylindres seront inclus dans le domaine du groupe de cylindres, et non pas dans le domaine du cylindre initial. Cela signifie que tous les cylindres d'un même groupe appartiennent au même domaine. Pour plus d'informations sur les domaines, voir *Chapitre 8.2.2 "Domaines", page 177*.

Les profils d'accès nouveaux ou importés et les groupes d'accès temporaires sont attribués au domaine initial de cylindres.

Chaque domaine initial a un nom qui peut être modifié. Le nom par défaut est `default`. Les domaines initiaux peuvent partager le même domaine ou avoir des domaines différents.

Pour régler les domaines initiaux pour les clés, personnes ou cylindres :

1) Sélectionnez **Administration » Réglages du système**.
2) Cliquez sur **Modifier**.
3) Sous **ADMINISTRATION**, cliquez sur **Changer domaine...** pour le domaine initial correspondant.

   La liste des domaines autorisés pour l'administrateur s'affiche.
4) Cliquez sur **Sélectionner** sur la ligne du nouveau domaine.
5) Cliquez sur **Enregistrer**.

6.6.4 Création et suppression de domaines

1) Sélectionnez **Administration » Domaines**.
2) Pour créer un domaine :
   a) Cliquez sur **Créer nouveau**.
   b) Saisissez le **Nom** et éventuellement une **Description**.
   c) Cliquez sur **Enregistrer**.
3) Pour supprimer un domaine :

REMARQUE !
Un domaine peut uniquement être supprimé si aucun cylindre, groupe de cylindres, employé, visiteur ou clé n'est connecté à ce domaine. Avant la suppression, videz le domaine en déplaçant les objets sur un domaine différent.

Veuillez vous assurer de déplacer les employés ou visiteurs actifs ou supprimés sur un domaine différent. Pour trouver les employés ou visiteurs supprimés, consultez *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

a) Localisez le domaine et affichez les informations détaillées.

   Voir *Chapitre 6.6.1 "Recherche de domaines", page 125*.

b) Cliquez sur **Supprimer**.

c) Cliquez sur **OK**.

6.6.5 Changement du domaine de clés

1) Sélectionnez **Informations système » Clés**.

   Une liste de toutes les clés s'affiche.

2) Pour rechercher des clés spécifiques, saisissez les critères de recherche et cliquez sur **Rechercher**.

3) Cliquez sur la ligne de clé concernée.

4) Cliquez sur **Modifier**.

5) Cliquez sur **Changer domaine...**.

   La liste des domaines autorisés pour l'administrateur s'affiche.

6) Cliquez sur **Sélectionner** sur la ligne du nouveau domaine.

7) Cliquez sur **Enregistrer**.

Le domaine peut être changé simultanément pour plusieurs clés. Sélectionnez les clés dans la liste des résultats de recherche et cliquez sur **Changer domaine...**.

Voir également *Chapitre 8.2.2 "Domaines", page 177*.

6.6.6 Changement du domaine pour employés ou visiteurs

1) Localisez l'employé ou le visiteur à modifier.

   Pour rechercher un employé ou visiteur et afficher la fenêtre d'informations détaillées, voir *Chapitre 4.1.1 "Recherche d'employés ou de visiteurs", page 24*.

2) Cliquez sur **Modifier**.

3) Cliquez sur **Changer domaine...**.

   La liste des domaines autorisés pour l'administrateur s'affiche.

4) Cliquez sur **Sélectionner** sur la ligne du nouveau domaine.

5) Cliquez sur **Enregistrer**.

Le domaine peut être changé pour plusieurs employés ou visiteurs simultanément. Sélectionnez les employés ou visiteurs dans la liste des résultats de recherche et cliquez sur **Changer domaine...**.

Voir également *Chapitre 8.2.2 "Domaines", page 177*.

6.6.7 Changement du domaine de cylindres

Le domaine des cylindres qui appartiennent à un groupe de cylindres est modifié au niveau du groupe. Voir *Chapitre 6.6.8 "Changement du domaine de groupes de cylindres", page 128*.

1) Sélectionnez **Informations système » Cylindres**.

   La liste de tous les cylindres s'affiche.

2) Pour rechercher des cylindres spécifiques, saisissez les critères de recherche et cliquez sur **Rechercher**.
3) Cliquez sur la ligne de cylindre concerné.
4) Cliquez sur **Modifier**.
5) Cliquez sur **Changer domaine...**.

   La liste des domaines autorisés pour l'administrateur s'affiche.

6) Cliquez sur **Sélectionner** sur la ligne du nouveau domaine.
7) Cliquez sur **Enregistrer**.

Le domaine peut être changé simultanément pour plusieurs cylindres. Sélectionnez les cylindres dans la liste des résultats de recherche et cliquez sur **Changer domaine...**.

REMARQUE !
Il est recommandé de vérifier que le profil d'accès et tous les cylindres et groupes de cylindres appartiennent au même domaine. Il faut en effet s'assurer que les administrateurs d'un domaine donné ne peuvent avoir accès à des cylindres d'autres domaines (par le biais des profils d'accès).

Voir également *Chapitre 8.2.2 "Domaines", page 177*.

6.6.8 Changement du domaine de groupes de cylindres

Pour des cylindres n'appartenant à aucun groupe de cylindres, le domaine est modifié individuellement sur chaque cylindre. Voir *Chapitre 6.6.7 "Changement du domaine de cylindres", page 128*.

1) Sélectionnez **Informations système » Groupes de cylindres**.

   La liste de tous les groupes de cylindres apparaît.

2) Pour rechercher des groupes de cylindres particuliers, saisissez les critères de recherche et cliquez sur **Rechercher**.
3) Cliquez sur la ligne de groupe de cylindre concerné.
4) Cliquez sur **Modifier**.
5) Cliquez sur **Changer domaine...**.

   La liste des domaines autorisés pour l'administrateur s'affiche.

6) Cliquez sur **Sélectionner** sur la ligne du nouveau domaine.
7) Cliquez sur **Enregistrer**.

Le domaine peut être modifié simultanément pour plusieurs groupes de cylindres. Sélectionnez les groupes de cylindres dans la liste des résultats de recherche et cliquez sur **Changer domaine...**.

REMARQUE !
Il est recommandé de vérifier que le profil d'accès et tous les cylindres et groupes de cylindres appartiennent au même domaine. Il faut en effet s'assurer que les administrateurs d'un domaine donné ne peuvent avoir accès à des cylindres d'autres domaines (par le biais des profils d'accès).

Voir également *Chapitre 8.2.2 "Domaines", page 177*.

6.6.9 Changement de domaine des profils d'accès

1) Localisez le profil d'accès et affichez les informations détaillées.

   Voir *Chapitre 4.6.1 "Recherche de profils d'accès", page 69*.

2) Dans la fenêtre des informations détaillées, cliquez sur **Modifier**.
3) Cliquez sur **Changer domaine**.
4) Cliquez sur **Sélectionner** pour le nouveau domaine.
5) Cliquez sur **Enregistrer**.

REMARQUE !
Il est recommandé de vérifier que le profil d'accès et tous les cylindres et groupes de cylindres appartiennent au même domaine. Il faut en effet s'assurer que les administrateurs d'un domaine donné ne peuvent avoir accès à des cylindres d'autres domaines (par le biais des profils d'accès).

6.7 Gestion des rôles et des autorisations

REMARQUE !
Pour attribuer des rôles à une clé de programmation, voir *Chapitre 6.11.4 "Modification des informations de clé de programmation", page 137*.

1) Sélectionnez **Administration » Rôles**.

   La liste des rôles existants s'affiche.

   Certains rôles sont prédéfinis dans CWM.

2) **Pour créer un rôle :**

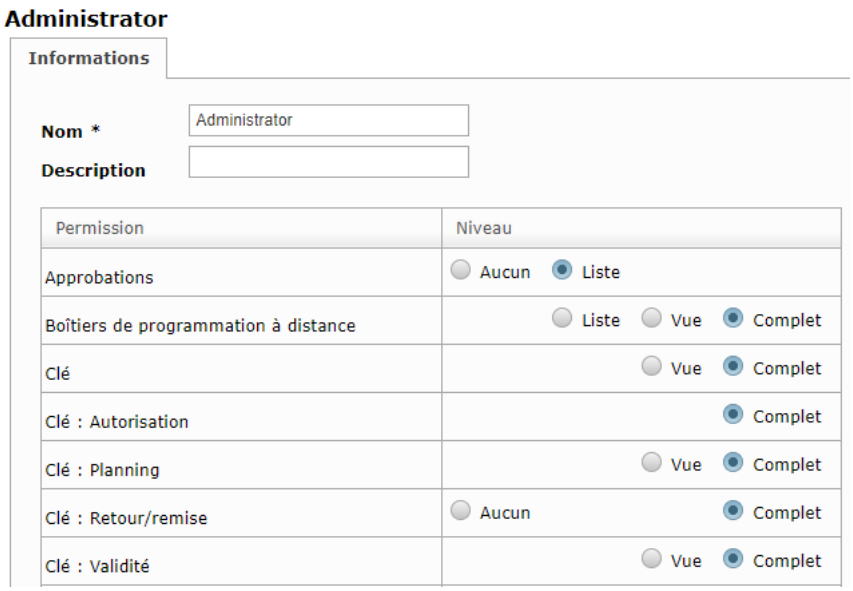
   1. Cliquez sur **Créer nouveau**.
   2. Saisissez un **Nom** et éventuellement une **Description**.
   3. Sélectionnez les autorisations dans la liste.

REMARQUE !

Restrictions :

- L'accès à certaines permissions dépend du niveau des autres permissions. Si une permission spécifique ne peut pas être configurée, vérifiez le niveau des permissions liées.
- Si **Administrateurs hiérarchiques** est activé, l'administrateur ne peut pas accorder de niveau de permission supérieur au sien.

  Par exemple, si un administrateur reçoit le niveau **Liste** de la permission **Cylindre**, l'administrateur ne peut pas accorder aux nouveaux rôles le niveau **Vue** ou **Complet** de la permission **Cylindre**.



Pour modifier un rôle existant :

REMARQUE !

Restrictions :

- Un administrateur ne peut pas modifier son propre rôle ; seul le champ **Description** est modifiable.
- Si **Administrateurs hiérarchiques** est activé, l'administrateur ne peut pas modifier le rôle d'un administrateur ayant des permissions supérieures.
- Si **Administrateurs hiérarchiques** est activé, l'administrateur ne peut pas accorder de niveau de permission supérieur au sien.
- Les rôles **Super administrateur**, **Approbateur** et **CLIQ Connect+** sont en lecture seule et ne peuvent être modifiés.

1. Cliquez sur la ligne correspondant à un rôle.

2. Cliquez sur **Modifier** pour mettre à jour le **Nom**, la **Description** ou les **Autorisations** du rôle.
3. Cliquez sur **Enregistrer**.

Pour supprimer un rôle :

REMARQUE !
Restrictions :

- Les rôles associés à un ou plusieurs administrateurs ne peuvent pas être supprimés.
- Les rôles **Super administrateur**, **Approbateur** et **CLIQ Connect+** sont en lecture seule et ne peuvent pas être supprimés.
- Si **Administrateurs hiérarchiques** est activé, l'administrateur ne peut pas supprimer de rôles ayant un niveau de permission supérieur au sien.

1. Cliquez sur la ligne correspondant à un rôle.
2. Cliquez sur **Supprimer**.
3. Cliquez sur **OK**.

Pour afficher les membres de clé de programmation d'un rôle

1. Cliquez sur la ligne correspondant à un rôle.
2. Sélectionnez l'onglet **Membres**.

Voir également :

- *Chapitre 8.8 "Rôles et autorisations CWM", page 191*
- *Chapitre 9.4 "Autorisations", page 205*

6.8 Importer les informations employé

Les informations employé à importer doivent être enregistrées dans un fichier CSV respectant certaines spécifications. Voir *Chapitre 9.9 "Format du fichier d'importation d'employé", page 215*. Les spécifications exactes sont sujettes à modifications et il est donc recommandé de charger le fichier pour qu'il soit validé.

REMARQUE !
Les employés suivants ne sont pas ajoutés ou mis à jour dans CWM pendant le processus d'importation :

- Employés désactivés.
- Employés intégrés par le LDAP.

1) Sélectionnez **Administration » Importation d'employés**.
2) Cliquez sur **Sélectionner** pour trouver le fichier enregistré localement sur l'ordinateur.
3) Cliquez sur **Ouvrir**.

4) Cliquez sur **Télécharger** pour valider le fichier.

   Affiche des informations sur le nombre d'entrées valides contenues dans le fichier. Si le fichier ne respecte pas les spécifications, l'importation est impossible.

5) Cliquez sur **Importer** pour importer le fichier valide.

6.9 Gestion des modèles de reçu

Le modèle de texte et le logo des reçus de retour ou de remise peut être créé et édité. Les reçus sont créés au format PDF et peuvent être imprimés et enregistrés.

REMARQUE !
Afin de gérer les modèles de reçus, le niveau d'autorisation de l'utilisateur doit être **Complet** dans le rôle **Modèles de reçu**. Pour modifier le niveau d'autorisation, reportez-vous à *Chapitre 6.7 "Gestion des rôles et des autorisations", page 129*.

6.9.1 Création d'un modèle de reçu

Il est possible d'ajouter un nouveau modèle de reçu au système et de le définir ou non comme modèle par défaut.

1) Sélectionnez **Administration » Modèles de reçu**.

   La liste des modèles de reçus est affichée.

2) Cliquez sur **Créer nouveau** sous la liste.

3) Saisissez les champs suivants :

   - **Nom** : Il est utilisé comme nom de modèle.
   - **Type** : Sélectionnez soit **Remettre** soit **Retourner**.
   - **Valeur par défaut pour** : Si le modèle de création est utilisé par défaut, cochez l'une ou l'autre des cases, ou les deux.
   - **Langue** : Sélectionnez la langue appropriée dans la liste déroulante.
   - **Titre** : imprimé sur le reçu en tant qu'en-tête du contenu.

4) Sélectionnez le logotype :

   - Logo du système : Le logo de l'organisation par défaut. Pour modifier le logo du système, voir *Chapitre 6.9.3 "Modification du logo du système", page 134*.
   - Logo personnalisé : Un logo d'entreprise distinct au lieu du logo du système.

     a) Sélectionnez **Utiliser logo personnalisé**.

     b) Cliquez sur **Sélectionner**.

     c) Cliquez sur **Sélectionner...** et sélectionnez le fichier.

        L'image à télécharger doit être inférieure à 2 Mo et au format JPEG, JPG, PNG, BMP ou GIF.

     d) Cliquez sur **Télécharger**.

        Le logo apparaît sur l'écran contextuel.

     e) Cliquez sur **Fermer** pour quitter.

5) Entrez les phrases dans la case **Texte**.

Lors de la création d'un nouveau modèle basé sur le texte standard, il est recommandé de cliquer sur **Utiliser le texte standard** et de modifier le contenu.

La zone de texte comporte des boutons d'édition élémentaires pour formater les textes. Pour appliquer ces styles à un nouveau texte, cliquez sur le bouton et commencez à taper. Pour appliquer ces styles à un contenu existant dans l'éditeur, sélectionnez le texte et cliquez sur le bouton approprié. Les tableaux suivants présentent la liste des boutons disponibles.

B	Gras
I	Italique
U	Souligné
~~S~~	Barré
x^2	Exposant
x_2	Indice
	Liste non ordonnée
	Liste ordonnée
H_1	En-tête de premier niveau
H_2	En-tête de deuxième niveau
T_x	Effacer le formatage

6) Facultatif : Cliquez sur **Aperçu du modèle** pour vérifier le reçu.

7) Cliquez sur **Enregistrer**.

6.9.2 Édition d'un modèle de reçu

1) Sélectionnez **Administration » Modèles de reçu**.

   La liste des modèles de reçus est affichée.

2) Cliquez sur le modèle pour le modifier.

3) Cliquez sur **Modifier**.

4) Modifiez les champs suivants :

   - **Nom** : Il est utilisé comme nom de modèle.
   - **Type** : Sélectionnez soit **Remettre** soit **Retourner**.
   - **Valeur par défaut pour** : Si le modèle de modification est utilisé par défaut, cochez l'une ou l'autre des cases, ou les deux.
   - **Langue** : Sélectionnez la langue appropriée dans la liste déroulante.
   - **Titre** : imprimé sur le reçu en tant qu'en-tête du contenu.

5) Modifier le logotype :

   - Pour modifier le logo du système, voir *Chapitre 6.9.3 "Modification du logo du système", page 134*.
   - Pour modifier le logo personnalisé, cliquez sur **Sélectionner** pour télécharger le nouveau logo.

6) Modifiez les phrases dans la case **Texte**.

   Pour plus d'informations sur le formatage des textes, voir *Chapitre 6.9.1 "Création d'un modèle de reçu", page 132, Étape 5*.

7) Facultatif : Cliquez sur **Aperçu du modèle** pour vérifier le reçu.

8) Cliquez sur **Enregistrer**.

6.9.3 Modification du logo du système

Les modèles de reçus contiennent le logo de la marque par défaut, mais il est possible de personnaliser le logo par défaut.

Conditions préalables :

- Le logo est un fichier image avec un profil de couleurs RVB (le profil CMJN n'est pas pris en charge).
- La taille du logo doit être inférieure à 2 Mo. La taille recommandée est d'environ 120 x 60 pixels.

1) Sélectionnez **Administration » Modèles de reçu**.

2) Cliquez sur **Changer logo système** sous la liste.

3) • Pour passer au logo personnalisé :

   a) Cliquez sur **Sélectionner...**.

   b) Sélectionnez le fichier à télécharger et cliquez sur **Ouvrir**.

   c) Cliquez sur **Télécharger**.

   • Pour passer au logo par défaut, cliquez sur **Restaurer les paramètres par défaut**.

4) Cliquez sur **Fermer**.

6.9.4 Suppression d'un modèle de reçu

1) Sélectionnez **Administration » Modèles de reçu**.

   La liste des modèles de reçus est affichée.

2) Cliquez sur le modèle pour le supprimer.

3) Cliquez sur **Supprimer**.

4) Dans la fenêtre pop-up, cliquez sur **OK**.

6.10 Gestion des modèles de planning

Il existe deux types de modèles de planning, **Modèle de base** et **Modèle à créneaux horaires multiples**.

- Un modèle de base permet de définir une plage horaire par jour de la semaine.
- Un modèle à créneaux horaires multiples permet de définir librement les jours et les périodes. Plusieurs créneaux horaires peuvent être définis pour le même jour de la semaine.

Les deux modèles sont pris en charge par différentes versions de microprogramme de clé. Pour plus d'informations sur la prise en charge des modèles selon la version de microprogramme de clé, voir *Chapitre 9.7 "Fonctionnalité dépendante du microprogramme", page 214*.

1) Sélectionnez **Administration » Modèles de planning**.

2) Pour créer un modèle de planning de base :

a) Cliquez sur **Créer un modèle de base**.

   Par défaut, les tranches horaires sont définies sur Toute la journée.

b) Saisissez le **Nom** et **Description** en option.

c) Pour changer les tranches horaires par défaut, cliquez sur **Modifier** dans la ligne du jour spécifique.

d) Sélectionnez **Toute la journée**, **Jamais** ou **Personnaliser**.

e) Si l'option Personnaliser est choisie, remplissez les valeurs de période **De (l'heure)** et **À (l'heure)**.

f) Cliquez sur **Enregistrer**.

   Si nécessaire, répétez *Étape 2 c* - *Étape 2 f* pour les autres jours.

g) Cliquez sur **Enregistrer**.

3) Pour créer un modèle de planning à créneaux horaires multiples :

   a) Cliquez sur **Créer un modèle à créneaux horaires multiples**.

   b) Saisissez le **Nom** et **Description** en option.

   c) Cliquez sur **Ajouter période**.

   d) Remplissez les valeurs de période **Du (date)** et **Au (date)**.

   e) Remplissez les valeurs de période **De (l'heure)** et **À (l'heure)**.

   f) Cliquez sur **Enregistrer**.

   g) Ajoutez d'autres tranches horaires comme requis.

   h) Cliquez sur **Enregistrer**.

4) Pour modifier un modèle :

   a) Cliquez sur la ligne de modèle concerné.

   b) Cliquez sur **Modifier**.

   c) Mettez à jour les champs et cliquez sur **Enregistrer**.

5) Pour supprimer un modèle :

   a) Cliquez sur la ligne de modèle concerné.

   b) Cliquez sur **Supprimer**.

   c) Cliquez sur **OK**.

Voir également *Chapitre 8.1.8 "Plannings de clé", page 174*.

6.11 Gestion des clés de programmation

6.11.1 Recherche de clés de programmation

1) Sélectionnez **Administration » Clés de programmation**.

2) Saisissez les critères de recherche.

   Lors de la saisie dans les champs de recherche, CWM accepte le début d'un mot recherché ainsi que le symbole astérisque (*). Si la recherche est « Laboratoire 1 », les résultats de recherche pour « Lab », « *1 » ou « Lab*1 » comporteront « Laboratoire 1 ».

3) Cliquez sur **Rechercher**.

4) Pour afficher les informations détaillées d'un résultat de recherche, cliquez sur la ligne de la clé de programmation correspondante.

Pour plus d'informations sur les attributs de clé de programmation, voir *Chapitre 9.3.4 "Attributs de la clé de programmation", page 203*.

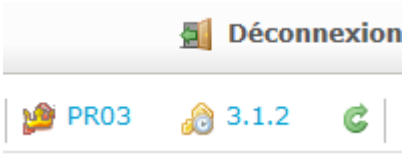
6.11.2 Scanner une clé de programmation

1) Insérez la clé de programmation dans la fente droite du boîtier de programmation local pour la scanner.

> **REMARQUE !**
> La clé de programmation utilisée pour la connexion doit rester dans la fente gauche du boîtier de programmation local.

2) Cliquez sur du coin supérieur droit de la page.

Les clés de programmation du boîtier de programmation local sont affichées sous la barre de navigation.



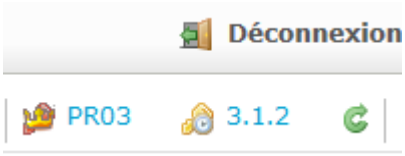
6.11.3 Affichage du statut de la clé de programmation

1) Insérez la clé de programmation à afficher dans la fente droite du boîtier de programmation local.

> **REMARQUE !**
> La clé de programmation utilisée pour la connexion doit rester dans la fente gauche du boîtier de programmation local.

2) Cliquez sur du coin supérieur droit de la page.

Les clés du boîtier de programmation local sont affichées sous la barre de navigation.

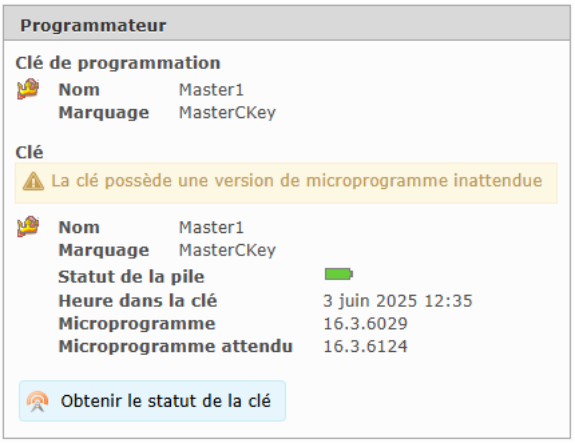


3) Insérez la clé de programmation dans la fente droite du boîtier de programmation local.

La vue des informations détaillées de la clé de programmation s'affiche, avec son **Nom** et son **Marquage** dans la partie droite de la page.

4) Cliquez sur **Obtenir le statut de la clé**.

Les informations de base de la clé de programmation insérée dans la fente de droite s'affichent. Pour plus d'informations sur l'indicateur d'état de la batterie, voir *Chapitre 9.6 "Indications de niveau de batterie", page 213*.



6.11.4 Modification des informations de clé de programmation

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

   Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

   Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Cliquez sur **Modifier**.

   - Pour modifier le nom de la clé de programmation, mettez le champ **Nom** à jour.
   - Pour bloquer la clé de programmation, sélectionnez **Bloquer**.
   - Pour modifier l'autorisation d'enregistrement d'un certificat, sélectionnez **Toujours autorisé**, **Autorisé une fois** ou **Non autorisé**.

     Voir également *Chapitre 8.11 "Intégration DCS", page 194*.
   - Pour attribuer ou modifier les rôles de la clé de programmation, sélectionnez un ou plusieurs rôles.

     REMARQUE !

     Restrictions :

     – Il est impossible de modifier le rôle de la clé de programmation actuellement utilisée pour se connecter.

     – Il est impossible de combiner le rôle Approbateur avec d'autres rôles.

     – Si **Administrateurs hiérarchiques** est activé, l'administrateur ne peut pas attribuer de rôles ayant un niveau de permission supérieur au sien.

3) Cliquez sur **Enregistrer**.

6.11.5 Sélection des domaines de clé de programmation

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Localisez la clé de programmation.

   Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

   Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

3) Sélectionnez l'onglet **Autorisations du domaine**.

4) Cliquez sur **Modifier** pour modifier les domaines.

5) Pour ajouter des domaines :

   a) Cliquez sur **Ajouter domaine...**.

      La liste de résultats de recherche affiche tous les domaines.

   b) Pour filtrer les domaines, saisissez le critère de recherche et cliquez sur **Rechercher**.

   c) Cliquez sur **Sélectionner** à côté des domaines à ajouter, ou cliquez sur **Tout sélectionner**.

   d) Cliquez sur **Effectué**.

6) Pour supprimer un domaine, cliquez sur **Supprimer** à côté du domaine à supprimer ou cliquez sur **Tout supprimer**.

7) Cliquez sur **Enregistrer**.

   Le changement de domaine prendra effet à la prochaine connexion.

6.11.6 Affichage des événements de clé de programmation

L'onglet Événements est utilisé pour la traçabilité de certaines opérations administrateur dans CWM, telles que la date de remise de clé de programmation.

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

   Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

   Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Sélectionnez l'onglet **Événements**.

   La liste de tous les événements de clé de programmation apparaît.

6.11.7 Remise de clés de programmation

Condition préalable :

- L'administrateur a reçu la permission dans sa totalité ; **Clé de programmation : Retour/Remise**.
- L'employé qui reçoit une clé de programmation doit disposer d'une adresse e-mail valide.

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

   Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

   Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Cliquez sur **Remise à un employé**.

   La liste des employés s'affiche.

3) Sélectionnez l'employé dans la liste et cliquez sur **Sélectionner**.

   Un e-mail est envoyé à l'adresse e-mail enregistrée de l'employé avec des instructions sur l'endroit où télécharger CLIQ Connect PC et l'URL du système de verrouillage.

   Pour pouvoir se connecter à CWM, l'employé doit installer un certificat pour la clé. Pour plus d'informations sur la façon d'installer le certificat, voir *Chapitre 3.2 "Enregistrement et installation des certificats de la clé de programmation", page 16*.

> **Conseil**
> Il est fortement recommandé que l'employé modifie le code PIN de la clé de programmation. Pour des instructions, consultez *Chapitre 6.11.11 "Changement du code PIN de clé de programmation", page 142*.

6.11.8 Retour de clés de programmation

Condition préalable :

- L'administrateur a reçu la permission dans sa totalité ; **Clé de programmation : Retour/Remise**.

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

   Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

   Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Cliquez sur **Récupérer la clé de programmation**.

   La clé de programmation ne peut plus être utilisée pour se connecter à CWM.

6.11.9 Déclaration et blocage d'une clé de programmation perdue

1) Localisez la clé de programmation et affichez les informations détaillées.

   Voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*.

2) Cliquez sur **Déclarée perdue**.

3) Les clés de programmation perdues qui contiennent des tâches de programmation de cylindre doivent être bloquées afin d'empêcher toute programmation non autorisée des cylindres.

   - Pour bloquer une clé de programmation contenant des tâches de programmation de cylindre, sélectionnez les cylindres dans lesquels la clé de programmation doit être bloquée :
     - Sélectionnez **Tous les cylindres** ou **Uniquement installé** et passez à *Étape 6*.
     - Sélectionnez **Personnaliser sélection** et passez à *Étape 4* pour sélectionner les cylindres.
   - Pour déclarer la perte d'une clé de programmation sans bloquer de cylindres, sélectionnez **Aucun cylindre**, cliquez sur **Suivant** et passez à l'*Étape 9*.

4) Cliquez sur **Suivant**.

5) Sélectionnez les cylindres pour lesquels la clé de programmation perdue sera bloquée.

6) Cliquez sur **Suivant**.

7) Facultatif : Sélectionnez la clé de programmation de cylindre dans la liste en cliquant sur **Sélectionner**.

   REMARQUE !
   Si ce processus est ignoré, des tâches de programmation des cylindres sont créées pour les clés de programmation.

   Dans l'onglet **Rechercher**, sélectionnez **Tous types et statuts** pour afficher les clés de programmation.

   Dans l'onglet **Avancée**, sous **Type**, sélectionnez Clés utilisateur ou Clés de programmation pour modifier ce qui est affiché dans la liste.

   REMARQUE !
   La mémoire de la clé de programmation de cylindre doit être suffisante.

8) Dans la page de confirmation, sélectionnez le niveau de priorité sous **Priorité**.

   Les tâches urgentes doivent disposer d'un niveau de priorité élevé.

9) Après avoir vérifié toutes les informations, cliquez sur **Déclarée perdue**.

   - Si **aucune tâche** n'est créée pour bloquer la clé de programmation perdue, les tâches de programmation attribuées à cette clé sont annulées et répertoriées sous **Tâches » Programmation du cylindre** .

- Si des tâches sont créées pour bloquer la clé de programmation perdue, la clé utilisée pour le blocage héritera des tâches de blocage de cylindre de la clé de programmation perdue. Les autres tâches de programmation de cylindre attribuées à la clé de programmation perdue sont annulées et répertoriées sous **Tâches » Programmation du cylindre**.

> **AVERTISSEMENT !**
> Par défaut, si aucune tâche de programmation de cylindre n'est créée pour bloquer la clé de programmation perdue, cette clé est ajoutée à CWM dans la liste des **Clés interdites** pour les cylindres concernés. Cette information n'est toutefois pas visible dans CWM. Si ces cylindres sont ultérieurement reprogrammés ou remplacés, les informations sur les clés interdites stockées dans CWM sont appliquées à ces cylindres, bloquant de fait la clé de programmation perdue. Par conséquent, même si la clé de programmation perdue est déclarée trouvée ultérieurement, elle reste bloquée par les cylindres reprogrammés ou remplacés.
>
> Pour ré-autoriser la clé de programmation retrouvée dans la liste d'accès de ces cylindres, voir *Chapitre 4.9.2 "Configuration des autorisations dans les cylindres", page 81*.
>
> Pour modifier ce réglage par défaut, **Autoriser de ne pas bloquer les clés perdues dans les cylindres** doit être désactivé. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

10)
- Si une clé spécifique n'a **PAS** été sélectionnée pour programmer les cylindres, continuez à partir de l'*Étape 4* de la *Chapitre 4.4.13 "Programmation des cylindres", page 62*.
- Si une clé spécifique a été sélectionnée pour programmer les cylindres, suivez les instructions ci-dessous.

11) Accédez à la vue des informations de la clé utilisateur sélectionnée.

> **Conseil**
> En cliquant sur **Marquage de clé** sous **Informations sur la clé de blocage**, vous accédez directement à la visualisation des informations.

12) Allez dans l'onglet **Tâches de programmation** et confirmez que le travail de cylindre est affecté à la clé.

13)
- **Programmation dans le boîtier de programmation local**

  Insérez la clé utilisateur dans la fente droite du boîtier de programmation local et retirez la clé de programmation de la fente gauche de ce boîtier.
- **Programmation dans un boîtier de programmation mural**

  Insérez la clé utilisateur dans un boîtier de programmation mural.

La tâche de programmation du cylindre est automatiquement inscrite sur la clé utilisateur.

14) Reprogrammez chaque cylindre à l'aide de la clé utilisateur.

15) Après avoir programmé les cylindres, déclarez les tâches de cylindre terminées en insérant la clé utilisateur dans l'un des dispositifs suivants :

- La fente droite du boîtier de programmation local (retrait de la clé de programmation de la fente gauche)
- Un boîtier de programmation mural

Après avoir retrouvé la clé de programmation, déclarez-la comme trouvée en cliquant sur **Déclarée trouvée** dans la vue des informations détaillées.

6.11.10 Déclaration d'une clé de programmation défectueuse ou opérationnelle

1) Localisez la clé de programmation et affichez les informations détaillées.

   Voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*.

2) **Déclarer défectueuse**

   1. Cliquez sur **Déclarer défectueux**.
   2. Cliquez sur **OK**.

   Déclarer opérationnelle

   1. Cliquez sur **Déclarer opérationnel**.
   2. Cliquez sur **OK**.

6.11.11 Changement du code PIN de clé de programmation

REMARQUE !
Le code PIN doit avoir 6 caractères. Les caractères suivants sont permis :

- Lettres majuscules (A, B, C, ...)
- Lettres minuscules (a, b, c, ...)
- Chiffres (0, 1, 2, ...)
- Moins (-)
- Trait de soulignement (_)
- Espace ( )
- Spécial (!, $, %, &, ...)
- Parenthèses ([,], {, }, (,), <, >)

Les caractères non anglais ne sont pas autorisés.

1) Pour changer le code PIN d'une clé de programmation normale en utilisant la clé de programmation maîtresse ou une clé de programmation disposant du rôle de super administrateur :

   a) Sélectionnez **Administration » Clés de programmation**.
   b) Insérez la clé de programmation dans le port droit du boîtier de programmation local.
   c) Cliquez sur **Scanner**.
   d) Cliquez sur **Afficher** à côté de la clé de programmation.
   e) Cliquez sur **Régler un nouveau code PIN**.

f) Saisissez l'**Code PIN de la clé de programmation maîtresse**.

g) Saisissez le nouveau code PIN dans **Nouveau code PIN**.

h) Saisissez-le à nouveau dans **Confirmer nouveau code PIN**.

2) Pour changer le code PIN de clé de programmation normale de la même clé utilisée pour se connecter :

a) Sélectionnez **Réglages » Réglages de la clé de programmation**.

b) Cliquez sur **Changer code PIN clé de programmation**.

c) Saisissez l'**Code PIN actuel**.

d) Saisissez l'**Nouveau code PIN**.

e) Saisissez le nouveau code PIN dans **Confirmer nouveau code PIN**.

3) Cliquez sur **OK**.

6.11.12 Déblocage de clés de programmation

Après cinq essais infructueux de connexion avec un code PIN erroné, la clé de programmation est bloquée. Elle sera débloquée en saisissant le code PUK fourni par le revendeur CLIQ. Voir *Chapitre 6.11.12.1 "Déblocage des clés de programmation avec le code PUK", page 143* pour plus d'informations.

REMARQUE !
Après 25 essais de saisie d'un code PUK erroné, la clé de programmation devient inutilisable et doit être remplacée.

Si l'administrateur ne dispose pas du code PUK, le possesseur de la clé de programmation maîtresse peut déverrouiller la clé de programmation. Voir *Chapitre 6.11.12.2 "Déblocage de clés de programmation avec une clé de programmation maîtresse", page 143* pour plus d'informations.

6.11.12.1 Déblocage des clés de programmation avec le code PUK

1) Sélectionnez **Réglages » Réglages de la clé de programmation**.

2) Cliquez sur **Débloquer la clé de programmation**.

3) Saisissez l'**Code PUK**.

Si l'administrateur ne dispose pas du code PUK, contactez un possesseur de clé de programmation maîtresse.

4) Saisissez l'**Nouveau code PIN**.

5) Saisissez l'**Confirmer nouveau code PIN**.

6) Cliquez sur **OK**.

6.11.12.2 Déblocage de clés de programmation avec une clé de programmation maîtresse

La procédure suivante ne peut être exécutée que par un possesseur de clé de programmation maîtresse.

1) Insérez la clé de programmation à débloquer dans la fente droite du boîtier de programmation local.

2) Trouvez la clé de programmation et accédez à ses informations détaillées.

Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

3) Cliquez sur **Régler un nouveau code PIN**.

4) Entrez les éléments **Code PIN de la clé de programmation maîtresse**, **Nouveau code PIN** et **Confirmer nouveau code PIN** pour la clé de programmation bloquée.

5) Cliquez sur **OK** pour enregistrer.

Le nouveau code PIN est programmé dans la clé de programmation placée dans le logement droit du boîtier de programmation local.

6.11.13 Activer ou désactiver la récupération automatique du journal des événements de la clé de programmation

Conditions préalables :

- L'administrateur a la permission d'activer automatiquement les journaux des événements.
- Une clé de 2e génération avec microprogramme 12.6 ou version supérieure.
- Pour l'activation, la fonction **Approbations** doit être désactivée dans **Réglages du système**.

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Trouvez le réglage **RÉCUPÉRATION AUTOMATIQUE DU JOURNAL DES ÉVÉNEMENTS**.

3)
- Pour activer le réglage de la récupération automatique du journal des événements : Cliquez sur **Activer**.
- Pour désactiver le réglage de la récupération automatique du journal des événements : Cliquez sur **Désactiver**.

4) Si la clé de programmation est dans le boîtier de programmation local, cliquez sur **Mise à jour locale de la clé de programmation**.

6.11.14 Liste des certificats de clé de programmation

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Sélectionnez l'onglet **Certificats**.

La **Date de dernière utilisation** de chaque certificat est affichée si le réglage système **Dernière date d'identification récupérée** est activé. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

6.11.15 Révocation des certificats de clé de programmation

La révocation des certificats de clé de programmation est une fonction de sécurité et est normalement utilisée lorsque l'ordinateur d'un administrateur possédant des certificats de clé de programmation a été volé, mais que les clés de programmation sont toujours en lieu sûr. Dans l'exemple de l'ordinateur volé, le certificat de clé de programmation installé est révoqué et de nouveau enregistré.

Pour enregistrer un certificat de clé de programmation, consultez *Chapitre 3.2 "Enregistrement et installation des certificats de la clé de programmation", page 16*.

1) Trouvez la clé de programmation et accédez à ses informations détaillées.

   Pour rechercher la clé de programmation et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*

   Pour scanner la clé de programmation dans le boîtier de programmation local et afficher la fenêtre d'informations détaillées, voir *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*

2) Sélectionnez l'onglet **Certificats**.

3) Cliquez sur **Révoquer certificat** pour chacun des certificats à révoquer.

   Conseil
   Le certificat à enregistrer peut être trouvé dans la colonne **Date de dernière utilisation**. En cas de doute, révoquez tous les certificats et enregistrez-les à nouveau.

   REMARQUE !
   Il n'est pas possible de révoquer le certificat qui a été utilisé pour se connecter au système de fermeture.

4) Cliquez sur **OK**.

6.11.16 Remplacement d'une clé de programmation maîtresse

Si une clé de programmation maîtresse est perdue ou défectueuse, il faut en commander une nouvelle.

Suivez ces instructions pour enregistrer une nouvelle clé de programmation maîtresse et bloquer celle qui est perdue ou défectueuse.

Conditions préalables :

- Les éléments suivants sont disponibles :
  - Une nouvelle clé de programmation maîtresse avec son code PIN.
  - Un certificat pour la nouvelle clé de programmation maîtresse dans le cas où DCS n'est pas intégré.
  - Un fichier d'importation comportant la nouvelle clé de programmation maîtresse.

1) Installez le certificat de la clé de programmation maîtresse.

   Voir *Chapitre 5.2 "Installer le certificat de clé de programmation maîtresse", page 96*.

2) Bloquez CWM pour maintenance

   Voir *Chapitre 6.2 "Blocage du système pour maintenance", page 99*.

3) Importez le fichier comportant la nouvelle clé maîtresse en utilisant l'outil CLIQ de service de gestion Web. Pour plus d'informations, consultez la documentation relative au fonctionnement et à la maintenance de CWM.

> **ATTENTION !**
> Connectez-vous avec la nouvelle clé maîtresse immédiatement après avoir effectué l'importation.
>
> Jusqu'à ce que la nouvelle clé maîtresse soit connectée, l'ancienne peut être utilisée et bloquera la nouvelle si elle est utilisée pour la connexion.

4) Connectez-vous à CWM avec la nouvelle clé de programmation maîtresse.

   CWM détecte qu'il y a plus d'une clé de programmation maîtresse active, bloque automatiquement les autres et les déclare comme perdues.

   L'ancienne clé de programmation maîtresse peut toujours être utilisée pour exécuter toute tâche de programmation de cylindres déjà enregistrés dans la clé, sur les cylindres autorisés. CWM propose alors l'option de création de tâche de programmation de cylindres pour interdire la clé maîtresse bloquée des cylindres.

5) Cliquez sur **Oui, créer des tâches maintenant** ou **Non, vous déciderez plus tard**.

Pour créer des tâches d'interdiction plus tard, connectez-vous avec la nouvelle clé de programmation maîtresse et cliquez sur **Créer des tâches de mise sur liste noire** depuis l'affichage des informations détaillées relatives à la clé de programmation maîtresse bloquée.

6.11.17 Exportation des informations de clé de programmation

1) Recherchez les clés de programmation.

   Voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*.

2) Dans les résultats de recherche, sélectionnez les clés de programmation dont les données doivent être exportées en cochant les cases correspondantes.

3) Cliquez sur **Exporter vers le fichier CSV**.

4) Dans la fenêtre pop-up de téléchargement de fichiers, cliquez sur **Enregistrer**.

   Un fichier CSV est téléchargé dans le dossier **Téléchargements**.

> **REMARQUE !**
> Pour pouvoir ouvrir correctement le fichier dans Excel, le délimiteur du fichier doit être défini selon les réglages régionaux. Pour modifier le délimiteur, voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

6.12 Changement de groupe de cylindres pour cylindres

REMARQUE !
Certains cylindres peuvent présenter une sortie libre sur un boîtier de programmation mural connecté à un appareil externe, par exemple un contrôleur de relais. Dans ce cas, il est impossible de repositionner ces cylindres dans un autre groupe de cylindres.

Pour plus d'informations sur la sortie libre, contacter votre revendeur CLIQ local.

1) Localisez le cylindre et affichez les informations détaillées.

   Voir *Chapitre 4.4.1 "Recherche de cylindres", page 55*.

2) Cliquez sur **Changer groupe**.
3) Cliquez sur **Sélectionner** sur la ligne du groupe de cylindres concerné.
4) Sélectionnez une **Priorité**. Les travaux urgents doivent disposer d'un niveau de priorité élevé.

Le groupe de cylindres peut être modifié simultanément pour plusieurs cylindres. Sélectionnez les cylindres dans la liste des résultats de recherche et cliquez sur **Changer groupe...**.

6.13 Affichage du statut du système

1) Sélectionnez **Administration » Statut du système**.
2) Sélectionnez l'onglet **Statut actuel** pour afficher les statuts en ligne et hors ligne des boîtiers de programmation à distance, du serveur à distance et du serveur d'e-mails.
3) Sélectionnez l'onglet **Historique** pour afficher les anciens changements dans les statuts en ligne et hors ligne des boîtiers de programmation à distance, du serveur à distance et du serveur d'e-mails.

   Pour afficher les événements s'étant produits entre certaines dates :

   a) Saisissez la date de départ dans **Afficher les événements depuis**.
   b) Saisissez une date de fin dans **Afficher les événements jusqu'au**.
   c) Cliquez sur **Rechercher**.

6.14 Afficher les statistiques de base

CWM dispose d'une fonction statistique intégrée qui fournit des statistiques de base sur le système de verrouillage, telles que le nombre de cylindres et de clés.

Condition préalable :

- L'administrateur a reçu l'autorisation de consulter les **Statistiques**.

1) Sélectionnez **Administration » Statistiques**.
2) La page des **Statistiques** est ouverte.
3) Facultatif : cliquez sur **Imprimer les statistiques** ou **Exporter les statistiques** si nécessaire.

6.15 Mise à niveau du microprogramme

La version de microprogramme peut être vérifiée sur la vue des informations détaillées de chaque appareil.

6.15.1 Mise à niveau du microprogramme pour les bornes d'actualisation

> **REMARQUE !**
> Ce chapitre ne concerne pas les boîtiers de programmation mobiles CLIQ Connect.

Le microprogramme doit être fourni au CWM pour mettre à niveau une boîtier de programmation à distance. En cas d'utilisation de l'intégration DCS, les fichiers de microprogramme sont automatiquement extraits de DCS. Sinon, cette opération est effectuée en chargeant en amont un fichier de microprogramme local fourni par le revendeur CLIQ local. Une fois importé dans CWM, le microprogramme du boîtier de programmation à distance peut être mis à jour par l'intermédiaire de CWM ou d'un lecteur flash USB.

Le processus de mise à niveau du microprogramme de boîtier de programmation à distance diffère selon l'intégration DCS :

- Pour utiliser l'intégration DCS, commencez par l'*Étape 2*.
- Pour utiliser un fichier de microprogramme local, commencez par l'*Étape 1*.

1) Pour télécharger et importer un fichier de microprogramme local sans intégration DCS :
   a) Enregistrez le nouveau microprogramme localement sur l'ordinateur.
   b) Sélectionnez **Administration » Microprogramme**.
   c) Cliquez sur **Sélectionner** pour trouver le nouveau microprogramme enregistré sur l'ordinateur.
   d) Cliquez sur **Ouvrir**.
   e) Cliquez sur **Télécharger microprogramme** pour télécharger le microprogramme dans CWM.

      Le microprogramme a été téléchargé.
   f) Cliquez sur **Importer microprogramme** pour importer le microprogramme téléchargé.

      Si l'opération est réussie, un résumé de l'importation du microprogramme s'affiche dans une nouvelle fenêtre.
2) Sélectionnez **Informations système » Boîtiers de programmation à distance**.
3) Cliquez sur la ligne de la boîtier de programmation à distance à mettre à niveau.
4) Sélectionnez l'onglet **Microprogramme** et sélectionnez la version à partir de la section **MICROPROGRAMME** ou **CHARGEUR DE DÉMARRAGE DU MICROPROGRAMME**.

REMARQUE !
La section **CHARGEUR DE DÉMARRAGE DU MICROPROGRAMME** n'est pas affichée pour le boîtier de programmation murale Génération 2.

5) • Pour mettre à niveau le microprogramme des bornes d'actualisation en ligne avec CWM :

a) Sélectionnez la version du microprogramme et cliquez sur **Appliquer**.

b) Activer la mise à niveau.

- Boîtiers de programmation mobiles CLIQ:

  Branchez une clé utilisateur sur secteur sur le boîtier de programmation mobile CLIQ.
- Bornes de rechargement de droits:

  Le microprogramme a été mis à niveau à la prochaine pulsation (prochaine connexion au serveur à distance).

• Pour mettre à niveau le microprogramme d'un boîtier de programmation hors ligne avec une clé USB :

REMARQUE !
La clé USB doit être formatée selon le système de fichiers FAT32 et la taille de mémoire recommandée est de 8 à 16 Go pour les boîtiers de programmation muraux de génération 1 et les boîtiers de programmation mobiles. La taille de la clé n'est pas limitée pour les boîtiers de programmation muraux de génération 2. La clé USB ne doit contenir aucun autre fichier.

a) Sélectionnez la version de microprogramme et cliquez sur **Enregistrer sur fichier** pour enregistrer le fichier à la racine de la clé USB.

b) Connectez le lecteur flash USB au boîtier de programmation à distance à l'aide du câble USB approprié (voir *Chapitre 6.5.8 "Configuration des boîtiers de programmation mobiles", page 117* ou *Chapitre 6.5.7 "Configuration de boîtiers de programmation muraux", page 110*).

La mise à niveau est lancée automatiquement.

c) Activer la mise à niveau.

- Boîtiers de programmation mobiles CLIQ:

  Branchez une clé utilisateur sur secteur sur le boîtier de programmation mobile CLIQ.
- Bornes de rechargement de droits:

  La mise à niveau est lancée automatiquement.

La mise à niveau du microprogramme est terminée lorsque la LED de téléchargement s'arrête de clignoter et s'allume en continu. Pour plus d'informations sur les indications lumineuses de boîtier de programmation à distance, voir *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211* et *Chapitre 9.5.2 "Indications de boîtier de programmation mural (génération 2)", page 212*.

6.15.2 Mise à niveau du microprogramme pour les boîtiers de programmation mobiles CLIQ Connect

1) Connectez le boîtier de programmation mobile CLIQ Connect au PC client sur lequel CLIQ Connect PC est installé, via un câble micro-USB.
2) CLIQ Connect PC vérifie automatiquement la version de microprogramme du boîtier de programmation mobile CLIQ Connect.

   Si une version plus récente est disponible, CLIQ Connect PC suggère de procéder à la mise à niveau du microprogramme.
3) Suivez les instructions qui s'affichent à l'écran.

6.15.3 Mise à niveau de microprogramme sur clés

Le microprogramme doit être fourni au CWM pour mettre à niveau une clé. Pour les systèmes avec intégration DCS, les fichiers de microprogramme sont automatiquement extraits de DCS. Pour les systèmes sans intégration DCS, cette opération est effectuée en téléchargeant en amont un fichier de microprogramme local fourni par le revendeur CLIQ local. Une fois importé, le microprogramme est mis à jour via CWM à l'aide d'un boîtier de programmation distant.

Tableau 1. Type de boîtier de programmation à distance à utiliser pour la mise à niveau de clés

Version de clé	Boîtier de programmation à distance	Version du microprogramme de la boîtier de programmation à distance
Clés utilisateur, génération 1	Boîtier de programmation mural (génération 1)	
Clés utilisateur, génération 2	Boîtier de programmation mural (générations 1 et 2) ou boîtier de programmation mobile CLIQ	
Clés de programmations, génération 2, avec microprogramme 12.0 ou au-dessus	Boîtier de programmation mural (générations 1 et 2) ou boîtier de programmation mobile CLIQ	Microprogramme de boîtier de programmation mural ou boîtier de programmation mobile CLIQ, 6.3 ou supérieure

Version de clé	Boîtier de programmation à distance	Version du microprogramme de la boîtier de programmation à distance
Clés de programmations, génération 2, avec microprogramme inférieur à la version 12.0	Ne peut pas être mis à niveau via CWM	
Clés de programmations, génération 1	Ne peut pas être mis à niveau via CWM	

La génération de clé est visible dans les vues détaillées de clé utilisateur et de clé de programmation, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*, *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*, *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*, ou *Chapitre 6.11.1 "Recherche de clés de programmation", page 135*.

Le processus de mise à jour du microprogramme de clé diffère selon l'intégration DCS :

- Pour les systèmes de fermeture avec intégration DCS, allez à *Étape 4*.
- Pour les systèmes de fermeture sans intégration DCS, continuer à partir de *Étape 1*.

1) Enregistrez le nouveau microprogramme localement sur l'ordinateur.
2) Sélectionnez **Administration » Microprogramme**.
3) Importer le nouveau microprogramme :
   a) Cliquez sur **Sélectionner** pour trouver le nouveau microprogramme enregistré sur l'ordinateur.
   b) Cliquez sur **Ouvrir**.
   c) Cliquez sur **Télécharger microprogramme** pour télécharger le microprogramme dans CWM.

      Si l'opération est exécutée, un résumé du microprogramme téléchargé s'affiche dans une nouvelle fenêtre.
   d) Cliquez sur **Importer microprogramme**.

REMARQUE !
Pour mettre à niveau des clés de génération 1, les éléments suivants doivent être importés :

- Chargeur d'amorçage du microprogramme de boîtier de programmation mural de génération 1
- Microprogramme du boîtier de programmation mural de génération 1, version 2.11 ou supérieure
- Microprogramme de mise à jour de clé du boîtier de programmation mural de génération 1, version 2.11 ou supérieure
- Nouveau microprogramme de clé, un pour chaque type de clé qui sera mis à niveau

REMARQUE !
Pour les systèmes avec l'intégration DCS activée, les fichiers de programmation sont automatiquement récupérés de DCS et listés parmi le microprogramme importé déjà prêt pour l'activation.

4) Pour mettre à niveau des clés utilisateur de génération 1 :

REMARQUE !
Les boîtiers de programmation muraux de génération 2 ne prennent pas en charge la mise à niveau du microprogramme pour les clés utilisateur de génération 1.

a) Sélectionnez **Informations système » Boîtiers de programmation à distance**.

b) Localisez la borne de rechargement de droits à utiliser pour la mise à niveau et affichez les informations détaillées.

Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

S'affichent notamment le chargeur de démarrage du microprogramme et le microprogramme de boîtier de programmation mural existants.

c) Si le chargeur de démarrage du microprogramme de boîtier de programmation mural et le microprogramme doivent être mis à niveau, voir *Chapitre 6.15.1 "Mise à niveau du microprogramme pour les bornes d'actualisation", page 148*.

d) Activer les mises à niveau de clés dans le boîtier de programmation mural, voir *Chapitre 6.5.11 "Activation et désactivation des mises à niveau de clé dans les boîtiers de programmation à distance", page 124*.

Le microprogramme de mise à niveau de clé est envoyé au boîtier de programmation mural. Lorsque le boîtier de programmation mural a chargé le nouveau microprogramme et a redémarré, il est possible de mettre à niveau les clés.

e) Pour chacune des clés utilisateur à mettre à niveau :

- Insérez la clé dans le boîtier de programmation mural de mise à jour de clé.

  Les mises à jour à distance de la clé en attente sont d'abord exécutées, puis la clé est mise à niveau avec le nouveau microprogramme.

  REMARQUE !
  La configuration de la clé, y compris l'ensemble des droits d'accès, est effacée au cours de la mise à niveau du microprogramme. Elle est restaurée en effectuant une mise à jour de la clé après la mise à niveau.

  Le boîtier de programmation mural indique que les mises à jour sont terminées. Pour plus d'informations sur les indications lumineuses de boîtier de programmation à distance, voir *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211*.

- Retirez la clé du boîtier de programmation mural.

Un traitement de mise à jour à distance pour restaurer la configuration de clé est créé dans CWM. Elle sera disponible après quelques minutes.

- Insérez la clé dans une boîtier de programmation à distance pour restaurer la configuration de la clé.

  L'opération de mise à niveau est alors terminée pour cette clé.

f) Désactiver les mises à niveau de clés dans le boîtier de programmation mural, voir *Chapitre 6.5.11 "Activation et désactivation des mises à niveau de clé dans les boîtiers de programmation à distance", page 124*.

Toutes les tâches de mise à niveau de microprogramme de clé en attente sont annulés. Le microprogramme de boîtier de programmation mural normal est envoyé au Boîtier de programmation mural et lorsque le nouveau microprogramme y est chargé et redémarré, il s'exécute de nouveau comme un boîtier de programmation mural ordinaire.

5) Pour mettre à niveau des clés utilisateur ou des clés de programmation de génération 2 :

a) Sélectionnez **Informations système » Boîtiers de programmation à distance**.

b) Afficher les informations détaillées de la boîtier de programmation à distance à utiliser pour la mise à niveau.

Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

- Si le microprogramme de la boîtier de programmation à distance doit être niveau, voir *Chapitre 6.15.1 "Mise à niveau du microprogramme pour les bornes d'actualisation", page 148*.

c) Sur l'onglet **Réglages**, activez les mises à niveau de clés dans le boîtier de programmation à distance. Voir *Chapitre 6.5.11 "Activation et désactivation des mises à niveau de clé dans les boîtiers de programmation à distance", page 124*

d) Sélectionnez **Administration » Microprogramme**.

e) Sélectionnez l'onglet **Microprogramme de la clé utilisateur importé** ou **Microprogramme de la clé de programmation importé** selon qu'il s'agit de la mise à jour de clés utilisateur ou de clés de programmation.

f) Cliquez sur **Appliquer** pour que la mise à niveau de la clé par le microprogramme importé.

Un traitement à distance est automatiquement créé.

REMARQUE !
Le bouton **Appliquer** du microprogramme importé grisé signifie que des mises à niveau à distance sont en attente pour le microprogramme existant. Elles sont indiquées par une icône dans la colonne **Statut**. Suivez la procédure suivante :

- Cliquez sur **Annuler** pour le microprogramme avec les mises à niveau à distance en attente.
- Cliquez sur **OK**.
- Cliquez sur **Appliquer** pour la dernière version du microprogramme.

REMARQUE !
L'ordre de *Étape 5 c* et *Étape 5 f* peuvent être inversé. Il est possible d'appliquer tout d'abord le microprogramme importé, puis d'activer les mises à niveau de clé pour une sélection de bornes d'actualisation.

g) Mettez à niveau chaque clé dans un boîtier de programmation à distance :

REMARQUE !
Pour les clés utilisateur, toute mise à jour à distance en attente pour la clé est d'abord exécutée, puis la clé est mise à niveau avec le nouveau microprogramme.

- Via **Boîtier de programmation mural** ou **PD mobile CLIQ**

  Insérez ou connectez la clé aux dispositifs qui ont été activés pour la mise à niveau de la clé.

  La boîtier de programmation à distance indique que les mises à jour sont terminées. Pour plus d'informations sur les indications lumineuses de boîtier de programmation à distance, voir *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211* ou *Chapitre 9.5.2 "Indications de boîtier de programmation mural (génération 2)", page 212*.

- Sur **Protocole Bluetooth dans l'application CLIQ Connect**

  Conditions préalables :

  – La version du microprogramme de CLIQ Connect doit être 4.1 ou toute version ultérieure.
  – La version du microprogramme de la clé doit être 16.3.3 ou toute version ultérieure.

    La mise à jour du microprogramme des clés dotées d'un microprogramme plus ancien est possible à l'aide d'un boîtier de programmation mural.

  Connectez la clé à CLIQ Connect.

REMARQUE !
Si une mise à niveau du microprogramme est lancée à l'aide de CLIQ Connect et d'une connexion BLE, elle doit être terminée avec la même méthode (c'est-à-dire une connexion BLE à un appareil mobile). Pendant l'état de mise à niveau intermédiaire, la clé semble non fonctionnelle ; elle n'ouvre aucune serrure et ne répond à aucun boîtier de programmation.

6.15.4 Mise à jour des informations du microprogramme de clé dans la base de données CWM

Lorsque le microprogramme de clé est mis à jour, la base de données CWM met automatiquement à jour les informations de microprogramme des clés. Les informations de microprogramme d'une clé peuvent être consultées sur la vue **Informations clé**.

Toutefois, si le microprogramme de clé est mis à jour en dehors du système CWM, par exemple à l'usine, la base de données CWM n'est pas mise à jour avec les dernières informations du microprogramme de clé.

Pour synchroniser les versions de microprogramme de la clé dans la base de données CWM et de la clé physique, procédez comme suit :

- Scannez la clé concernée et vérifiez son statut sur le boîtier de programmation local. Pour plus d'informations, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*.
- Insérez la clé concernée dans un boîtier de programmation à distance.

REMARQUE !
Seules les clés de génération 2 avec le microprogramme 12.3 ou une version supérieure peuvent mettre à jour les informations du microprogramme de la clé via des boîtiers de programmation à distance.

REMARQUE !
Clés de programmation uniquement :

Si une clé de programmation possède une version de microprogramme plus ancienne que celle de la base de données CWM, la base de données CWM du microprogramme n'est pas mise à jour. Cette situation peut entraîner des erreurs lors de l'utilisation de la clé de programmation.

6.16 Importation d'extensions

Le fichier d'importation d'extension doit être fourni au CWM pour importer une extension. À cet effet, téléchargez le fichier d'importation d'extension local.

Avec l'intégration DCS, les fichiers d'importation d'extensions sont automatiquement extraits à partir de DCS. Lancez le processus d'importation d'extensions à partir de l'*Étape 2*.

L'extraction à partir de DCS peut également être forcée en cliquant sur un bouton. Une fois téléchargée, l'importation d'extension doit être activée.

Condition préalable :

- Si les cylindres nouvellement ajoutés doivent bloquer les clés perdues dans le système, activez **Bloquer les clés perdues dans les nouveaux cylindres pendant l'importation d'extensions** dans **Réglages du système**. Lorsque cette option est activée, le système crée automatiquement des tâches de programmation de cylindres afin de bloquer les clés perdues pour ces cylindres lorsque les fichiers d'importation d'extensions de cylindres sont activés. Pour plus d'informations Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

1) Fournissez un fichier d'importation d'extension à CWM.

Pour télécharger un fichier d'importation d'extensions local

1. Sélectionnez **Administration » Importation d'extension » Télécharger ou récupérer le(s) fichier(s) d'importation d'extension**.
2. Cliquez sur **Sélectionner...** pour trouver le fichier d'importation d'extension enregistré localement sur l'ordinateur. Les fichiers d'importation d'extension ont un suffixe « .cws ».
3. Cliquez sur **Ouvrir**.
4. Cliquez sur **Télécharger**. Le fichier d'importation d'extension est téléchargé sur le serveur Web Manager et validé.

Pour extraire manuellement un fichier d'importation d'extensions à partir de DCS

1. Sélectionnez **Administration » Importation d'extension » Télécharger ou récupérer le(s) fichier(s) d'importation d'extension**.
2. Cliquez sur **Récupérer le(s) fichier(s) d'importation d'extension**.

   Une note de statut concernant la procédure de récupération s'affiche.

2) Activez une importation d'extension téléchargée ou récupérée :

> **REMARQUE !**
> Traiter un fichier d'importation d'extension téléchargée ou récupérée peut prendre un certain temps. Lorsqu'une importation d'extension est prête à être activée, une notification est affichée sur la page d'accueil de CWM et un e-mail est transmis à tous les administrateurs dont les rôles incluent des permissions de maintenance.

a) Sélectionnez **Administration » Importation d'extension » Activer importation d'extension**.

   Une note concernant les importations d'extension disponibles est affichée avec les informations sur le nombre de clés, les groupes de clés, les cylindres, les groupes de cylindres et les boîtiers de programmation à distance à activer.

b) Facultatif : Pour obtenir des informations plus détaillées sur les éléments d'extension, cliquez sur **Exporter vers le fichier CSV** pour chaque élément afin de générer un fichier CSV et de confirmer les informations contenues dans ce fichier.

c) Cliquez sur **Activer importation d'extension** pour activer les extensions disponibles.

> **REMARQUE !**
> Seules les importations d'extension téléchargées ou récupérées contenant de nouvelles données peuvent être activées. Les anciennes données ou les données identiques ne peuvent pas être activées.

Une fois activées, un message de confirmation s'affiche sur la page d'accueil de CWM.

Si la fonction **Bloquer les clés perdues dans les nouveaux cylindres pendant l'importation d'extension** est activée, des tâches de programmation de cylindres sont créées. Pour programmer les cylindres, voir *Chapitre 4.4.13 "Programmation des cylindres", page 62*.

7 Matériel CLIQ

7.1 Architecture CLIQ

L'architecture fondamentale du système CLIQ est illustrée en *Figure 1 "Architecture CLIQ", page 158*.

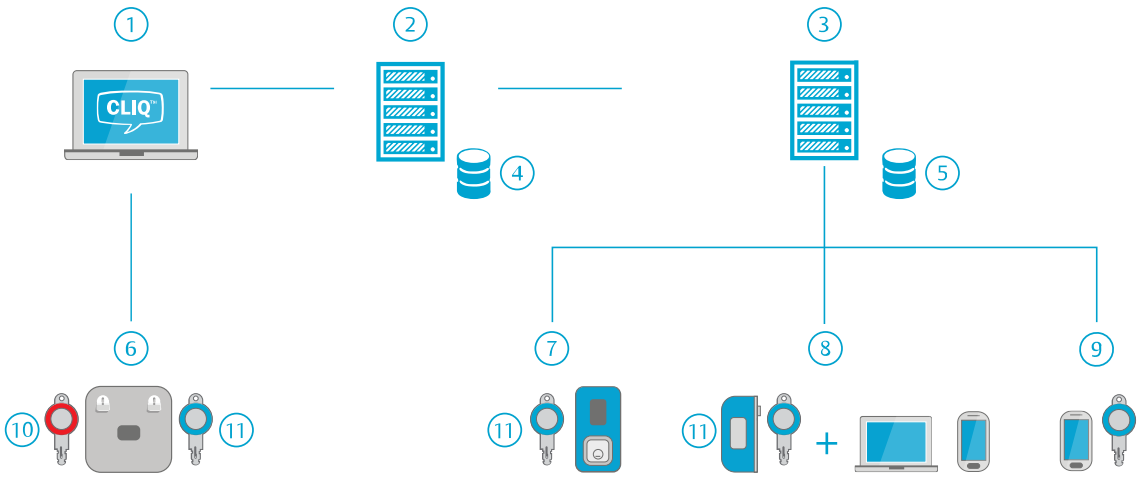


Figure 1. Architecture CLIQ

1. **Poste CWM**. Ordinateur avec navigateur Internet utilisé par un administrateur pour administrer un système de fermeture. Plusieurs clients peuvent être connectés au serveur.

2. **Serveur Web Manager**. Exécute le logiciel CWM et est relié à la base de données CLIQ contenant les informations de l'ensemble des éléments CLIQ, listes d'accès, journaux des événements, etc.

3. **Serveur Remote**. Dans le système à distance, le serveur à distance gère la mise à jour à distance des clés. Les traitements de mise à jour de clé sont envoyés du serveur Web Manager au serveur à distance. Les traitements de mise à jour sont enregistrés dans une base de données jusqu'à leur exécution depuis le boîtier de programmation à distance.

4. **Base de données**. Base de données du serveur Web Manager.

5. **Base de données**. Base de données du Serveur à distance.

6. **Boîtiers de programmation locaux**. Connectés au poste CLIQ Web Manager pour permettre à l'administrateur de s'identifier dans CWM (en utilisant une clé de programmation) et de programmer des clés localement. Pour plus d'informations, consultez *Chapitre 7.4.1 "Boîtiers de programmation locaux", page 163*.

7. **Boîtiers de programmation muraux**. Type de boîtier de programmation à distance. L'insertion d'une clé dans un boîtier de programmation mural entraîne l'exécution des tâches stockées dans la base de données du Serveur Remote pour la mise à jour des clés. Voir *Chapitre 7.4.2 "Boîtiers de programmation à distance", page 163*.

8. **Boîtiers de programmation mobiles CLIQ** et **boîtiers de programmation mobiles CLIQ Connect**. Deux types de boîtiers de programmation à distance. L'insertion d'une clé dans un boîtier de programmation mobile CLIQ ou un boîtier de programmation mobile CLIQ Connect entraîne l'exécution des tâches de mise à jour de clé stockées dans la base de données du Serveur Remote. Voir *Chapitre 7.4.2 "Boîtiers de programmation à distance", page 163*.

9. **Clés CLIQ Connect**. Un type de clé. En connectant la clé à un appareil mobile avec CLIQ Connect, vous pouvez mettre la clé CLIQ Connect à jour sans utiliser de boîtier de programmation. Reportez-vous au manuel CLIQ Connect.

10. **Clés de programmation**. Voir *Chapitre 7.2.4 "Clés de programmation", page 160*.

11. **Clés utilisateur**. Voir *Chapitre 7.2.3 "Clés utilisateur", page 159*.

7.2 Clés

7.2.1 Présentation des clés

Les clés CLIQ sont des clés électromécaniques qui contiennent de l'électronique et une batterie. Chaque clé CLIQ est programmée et peut être contrôlée et gérée avec CWM.

Les clés sont soit des clés système, également appelées **Clés de programmation** et utilisées par les administrateurs du système de verrouillage, soit des **Clés utilisateur**, utilisées par les employés et les visiteurs.

7.2.2 Clés CLIQ Connect

Certaines clés de programmation et clés utilisateur peuvent être mises à jour via la technologie Bluetooth avec un téléphone mobile ou une tablette. Ces clés sont appelées **clés CLIQ Connect**. Les clés qui ne disposent pas de cette capacité peuvent uniquement être mises à jour avec un boîtier de programmation.

7.2.3 Clés utilisateur

Les **Clés Utilisateur** sont utilisées par les employés et les visiteurs afin d'accéder aux installations. Il existe plusieurs types de clés utilisateur.

	**Clé mécanique**	C'est une clé traditionnelle sans des composants électroniques. Elle peut être gérée dans CWM, mais ne peut pas être utilisée avec des cylindres CLIQ.
	**Clé normale**	C'est une clé électromécanique pouvant ouvrir des cylindres mécaniques lorsque le profil et le taillage sont compatibles. Elle peut être autorisée à ouvrir des cylindres CLIQ en fonction de la liste d'accès du cylindre (voir *Chapitre 8.1.2 "Autorisation électronique", page 167*).

Clé standard

Outre ce qui précède, ce type de clé comporte une fonction d'horloge à quartz et peut être programmée pour s'activer entre certaines dates et nécessiter une revalidation (voir *Chapitre 8.1.4 "Validité de la clé", page 169*). Elle peut également être programmée pour avoir accès aux cylindres selon un planning (voir *Chapitre 8.1.8 "Plannings de clé", page 174*). Les clés de ce type peuvent également stocker des journaux des événements (voir *Chapitre 8.6 "Journaux des événements", page 189*).

Clé dynamique

Outre ce qui précède, ce type de clé peut également contenir une liste d'accès des cylindres et des groupes de cylindres que la clé est autorisée à ouvrir (voir *Chapitre 8.1.2 "Autorisation électronique", page 167*). Cette fonction est particulièrement utile dans les systèmes à distance, en permettant le contrôle de l'accès avec des clés faciles à mettre à jour dans des bornes d'actualisation.

Les clés dynamiques et standard peuvent être des **clés CLIQ Connect** (icône de droite) ou non (icône de gauche). Les clés normales ne sont jamais des clés CLIQ Connect. Voir *Chapitre 7.2.2 "Clés CLIQ Connect", page 159* pour plus d'informations.

Voir également *Chapitre 8.1 "Principes des autorisations", page 167*.

7.2.4 Clés de programmation

Les clés système, également appelées **Clés de programmation**, sont des clés utilisées par les administrateurs du système de fermeture. Les clés de programmation n'ouvrent pas les cylindres et servent uniquement à accéder à CWM et à programmer les cylindres.

Il existe deux types de clés de programmation : **Clés de programmation maîtresses** et **clés de programmation normales**.

Clé de programmation maîtresse

La clé de programmation maîtresse est utilisée par le super administrateur pour gérer le système de fermeture. Il n'existe qu'une seule clé de programmation maîtresse par système de fermeture et elle doit être conservée en lieu sûr.

La clé de programmation maîtresse possède les droits exclusifs suivants, qui ne peuvent être attribués à aucune autre clé de programmation :

- Modification du code PIN des autres clés de programmation.
- Exécution de tâches de programmation de cylindres, y compris la mise à jour de l'accès pour des clés de programmation.
- Déclaration d'une clé de programmation retrouvée.

Clé de programmation maîtresse secondaire

Les clés de programmation maîtresses secondaires sont utilisées par les administrateurs. Un système de verrouillage peut comporter plusieurs clés de programmation maîtresses secondaires.

Une clé de programmation maîtresse secondaire a des fonctionnalités restreintes par comparaison avec une clé de programmation maîtresse. Par exemple, elle ne peut pas être utilisée pour activer les importations initiales et certains réglages système ne peuvent pas être configurés.

Clé de programmation normale

Les clés de programmation normales sont remises aux administrateurs. Les clés de programmation normales peuvent être configurées afin de permettre l'accès à certaines fonctions de CWM et de l'interdire à d'autres. Voir *Chapitre 8.8 "Rôles et autorisations CWM", page 191*).

C'est un type particulier de clé de programmation normale qui a le droit d'exécuter la reprogrammation de cylindres. Les autres clés normales n'ont pas ce droit. Les droits de reprogrammation sont programmés sur la clé en usine et ne peuvent pas être modifiés. Pour savoir si une clé de programmation normale possède ou non des droits de reprogrammation, consultez les informations détaillées de la clé. Voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135* ou *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*.

Chaque clé de programmation normale peut être une **clé CLIQ Connect** (icône de droite) ou non (icône de gauche). Voir *Chapitre 7.2.2 "Clés CLIQ Connect", page 159* pour plus d'informations.

REMARQUE !

Le terme **Clé de programmation** est utilisé dans la description de la fonctionnalité relative à la fois aux clés de programmation maîtresses et aux clés de programmation normales.

La capacité de la clé à **programmer des groupes de cylindres** dépend du microprogramme. Seules les clés de programmation avec cette capacité peuvent exécuter les tâches de programmation de cylindres pour lesquelles il est nécessaire de modifier le groupe auquel appartient le cylindre. Pour savoir si une clé de programmation a cette

capacité, consultez les informations détaillées de la clé de programmation. Voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135* ou *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*. Dans les systèmes initialement fournis comme systèmes à groupes de cylindres, toutes les clés de programmation ont cette capacité.

Pour utiliser une clé de programmation dans CWM, un certificat unique doit être installé sur le Client CWM (voir *Chapitre 2.1 "Présentation de la configuration des clients CWM", page 13*). Chaque clé de programmation dispose également de son propre code PIN et de son propre code PUK.

7.2.5 Générations de clé

Il existe deux générations de clé :

- Génération 1
- Génération 2

Une génération de clé est définie par son matériel. Les clés de génération 2 sont les plus récentes et les plus développées.

Toutes les clés de génération 2 sont rétrocompatibles avec les clés de génération 1.

La génération de clé est visible sur la vue de clé détaillée, voir *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35* ou *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34*.

7.3 Cylindres

Il existe deux différents types de cylindre, mécanique et électronique. Les clés de type électronique peuvent contenir des droits d'accès pour des clés et des groupes de clés, ainsi que des informations de journal des événements.

Les cylindres peuvent être à simple entrée ou à double entrée. Pour les cylindres à double entrée, les entrées peuvent être soit du même type, soit de types différents.

Pour la présentation des cylindres, les symboles suivants sont utilisés :

Ⓔ Cylindre électronique

Ⓜ Cylindre mécanique

ⒺⓂ Double cylindre (notre exemple : Entrée A électronique et entrée B mécanique)

Figure 2. Cylindre CLIQ

Un cylindre peut être installé sur plusieurs types de serrures, portes, cadenas, verrous, etc. Un numéro d'identification est inscrit sur chaque corps de cylindre.

Le cylindre électronique enregistre les informations relatives aux :

- Groupes de clés et clés individuelles autorisés

- Clés bloquées
- Journaux des événements standard : Journaux des événements des insertions de clé par les clés du même système de fermeture
- Journaux des événements étrangers : Journaux des événements des insertions de clés par les clés d'autres systèmes de fermeture

Les différentes configurations de cylindre offrent différentes capacités de mémoire. Pour plus d'informations, consultez les informations produit.

7.4 Programmateurs

7.4.1 Boîtiers de programmation locaux

Le boîtier de programmation local est utilisé pour connecter les clés de programmation et les clés utilisateur à CWM.

Figure 3. Boîtier de programmation local

Le boîtier de programmation local est utilisé par les administrateurs du système de verrouillage. Il possède deux fentes pour l'insertion de clés, une à gauche pour les clés de programmation et une à droite pour les clés utilisateur. Pour se connecter à CWM, il est nécessaire de disposer d'un boîtier de programmation local connecté à un Client CWM avec une clé de programmation. Le boîtier de programmation peut être connecté à l'aide du port USB.

Le boîtier de programmation local dispose de deux ports :

- Un port USB
- Un port pour connecter les cylindres (non utilisé avec CWM)

7.4.2 Boîtiers de programmation à distance

Les boîtiers de programmation à distance sont utilisés dans les systèmes à distance pour transférer les données entre la base de données à distance et la clé. Les boîtiers de programmation à distance peuvent être des boîtiers de programmation muraux ou des boîtiers de programmation mobiles. Les boîtiers de programmation muraux et les boîtiers de programmation mobiles CLIQ sont spécifiques au système de fermeture, tandis que les boîtiers de programmation mobiles CLIQ Connect peuvent être utilisés avec tous les systèmes de fermeture.

Notez que chaque appareil prend en charge un type différent de câbles USB :

Appareil	Type de câble USB
Boîtier de programmation mural (génération 1)	Câble Mini USB OTG (On-The-Go)
Boîtier de programmation mural (génération 2)	Câble USB-C
Boîtier de programmation mobile CLIQ	Câble Mini USB
Boîtiers de programmation mobiles CLIQ Connect	Câble micro USB

Lorsqu'une clé est insérée dans un boîtier de programmation à distance, les actions suivantes sont exécutées :

- Les traitements de mise à jour à distance sont exécutés.
- L'heure sur la clé est mise à jour.
- Le journal des événements est lu sur la clé, si ainsi configuré.

Voir également *Chapitre 9.5.1 "Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile", page 211* et *Chapitre 9.5.2 "Indications de boîtier de programmation mural (génération 2)", page 212*.

Si l'option **Actualisation hors ligne** est activée, une clé peut être revalidée via un boîtier de programmation mural ou un boîtier de programmation mobile CLIQ, même si la connexion réseau est temporairement perdue. Voir également *Chapitre 8.1.5 "Revalidation de clé", page 169*. L'actualisation hors ligne n'est pas disponible avec les boîtiers de programmation mobiles CLIQ Connect.

Bornes de rechargement de droits
Deux types de boîtiers de programmation muraux sont disponibles : génération 1 et génération 2. Le boîtier de programmation mural de génération 2 a reçu en plus les fonctionnalités suivantes :

- L'Authentification réseau (802.1x) peut être activée. Pour l'activer ou la désactiver, voir *"AUTHENTIFICATION RÉSEAU (802.1X) (Boîtier de programmation mural de génération 2 uniquement)"* et *Chapitre 6.4 "Modifier les réglages du système", page 100*.
- Aucun chargeur d'amorçage n'est utilisé, c'est-à-dire que le chargeur d'amorçage du microprogramme n'est pas nécessaire.
- Le niveau d'enregistrement pour les logs de l'appareil est configurable ; voir *"GÉNÉRAL"* pour plus de détails.

Le boîtier de programmation mural est généralement fixé au mur et raccordé au serveur Remote par Ethernet.

Figure 4. Boîtier de programmation mural de génération 1

Figure 5. Boîtier de programmation mural de génération 2

Le terme **Pulsation** signifie que le boîtier de programmation mural envoie un signal au serveur à CLIQ Remote pour signifier à CLIQ Web Manager qu'il est en ligne. Le boîtier de programmation mural vérifie également les mises à jour de boîtier de programmation mural (mises à jour de microprogramme ou de configuration) lorsqu'il envoie chaque signal de présence. L'intervalle entre chaque pulsation est configurable.

Lorsqu'un boîtier de programmation mural manque un certain nombre de pulsations, CLIQ Web Manager suppose qu'il est hors ligne et envoie un e-mail à une personne spécifiée. Pour plus d'informations sur la façon d'activer cette fonction, voir *Chapitre 6.5.10 "Activation et désactivation de la messagerie hors ligne du boîtier de programmation mural", page 123*.

Boîtiers de programmation mobiles CLIQ

Le boîtier de programmation mobile CLIQ est un appareil de programmation personnel. Il peut se connecter soit à un ordinateur via un câble mini-USB, soit à un téléphone portable par Bluetooth Low Energy (BLE) pour utiliser la connexion Internet du téléphone portable.

Pour la connexion avec un téléphone portable, le boîtier de programmation mobile CLIQ requiert une alimentation par piles. Lorsque le boîtier de programmation mobile CLIQ est utilisé avec un ordinateur, l'application **ASSA ABLOY Network Provider** doit être installée sur l'ordinateur.

Figure 6. Boîtier de programmation CLIQ Mobile

Boîtiers de programmation mobiles CLIQ Connect

Le boîtier de programmation mobile CLIQ Connect est utilisé pour mettre à jour les clés à l'aide de CLIQ Connect (clés de 2e génération uniquement) ou de CLIQ Connect PC.

Il peut se connecter à un ordinateur via un câble micro-USB ou à un téléphone portable par Bluetooth Low Energy (BLE) pour utiliser la connexion Internet du téléphone portable.

Pour la connexion avec un téléphone portable, le boîtier de programmation mobile CLIQ Connect requiert une alimentation par piles.

Figure 7. Boîtier de programmation CLIQ Connect Mobile

8 Concepts et caractéristiques CLIQ

8.1 Principes des autorisations

Pour qu'une clé puisse ouvrir un cylindre, les conditions suivantes doivent être remplies :

- Le code mécanique est correct. Voir *Chapitre 8.1.1 "Autorisation mécanique", page 167*.
- La clé est active. Pour cela, il est nécessaire que la clé soit active selon les réglages d'activation et, si la revalidation est utilisée, que la clé soit revalidée dans l'intervalle de revalidation spécifié. Voir *Chapitre 8.1.4 "Validité de la clé", page 169*.
- Le cylindre est programmé électroniquement pour autoriser l'accès à la clé. Voir *Chapitre 8.1.2 "Autorisation électronique", page 167*.
- La clé n'est pas bloquée dans le cylindre. Voir *Chapitre 8.1.2 "Autorisation électronique", page 167*.
- Pour les clés dynamiques : La clé a été programmée pour avoir accès au cylindre. Voir *Chapitre 8.1.2 "Autorisation électronique", page 167*.
- Pour Clés dynamiques et clés standard: Le planning de la clé autorise l'accès à l'heure programmée. Voir *Chapitre 8.1.8 "Plannings de clé", page 174*.

8.1.1 Autorisation mécanique

Comme avec un système de clé maîtresse conventionnel, chaque clé du système de fermeture CLIQ dispose d'un panneton mécanique et chaque cylindre est compatible avec un ou plusieurs pannetons de clé. CWM tient le registre des clés disposant de l'accès mécanique à un cylindre, et le prend en compte lorsqu'il détermine la possibilité d'octroyer l'accès électronique.

8.1.2 Autorisation électronique

L'autorisation électronique est basée sur les informations enregistrées dans le cylindre et, pour les clés dynamiques, également dans la clé.

Les informations suivantes peuvent être enregistrées dans les cylindres :

- **Liste d'accès au cylindre** contenant les clés et les groupes de clés ayant accès au cylindre.
- Il est possible de définir des exceptions dans chaque groupe de clé de la liste d'accès afin d'autoriser l'accès à toutes les clés du groupe de clé sauf aux exceptions définies. Ceci est pratique lorsqu'un cylindre doit autoriser l'accès à toutes les clés d'un groupe de clé à l'exception de quelques-unes.

Pour les clés standard et les clés normales, seules les informations du cylindre déterminent si la clé dispose de l'accès au cylindre.

Avec les clés dynamiques, il est possible d'enregistrer les informations suivantes :

- Une **liste d'accès de clé** comportant les cylindres et les groupes de cylindre auxquels la clé a accès.

Pour qu'une clé dynamique puisse ouvrir un cylindre, le cylindre et la clé doivent correspondre. Dans un système à distance normal avec clés dynamiques, les cylindres sont programmés pour autoriser l'accès à toutes les clés et l'accès effectif est contrôlé par la liste d'accès de clé.

Figure 8 "Liste d'accès de clé", page 168 affiche les différentes manières d'inclure les cylindres ou les groupes de cylindres sur la liste d'accès de la clé dynamique :

1. directement
2. via un profil d'accès
3. via un utilisateur associé à un profil d'accès
4. via un groupe d'accès temporaire

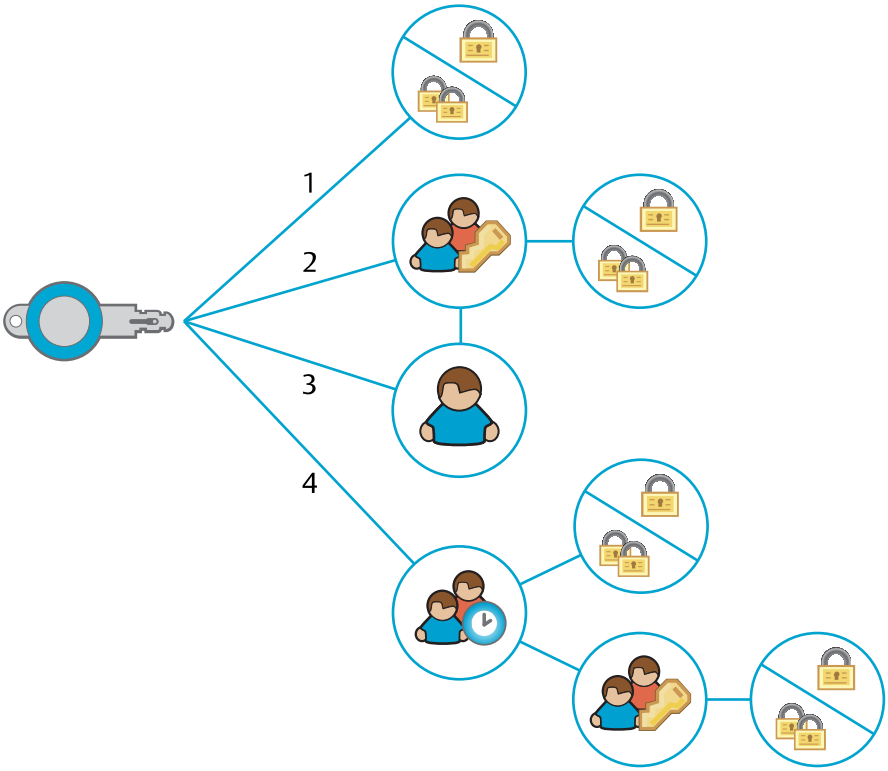


Figure 8. Liste d'accès de clé

La capacité de la liste d'accès de clé est limitée. Les informations détaillées d'une clé dynamique indiquent le nombre maximum d'entrées et le nombre d'entrées utilisées. Les traitements de mise à jour à distance qui excéderaient cette capacité ne seront pas exécutés. Voir également *Chapitre 8.3.2 "Mise à jour à distance", page 184*.

L'une des différences entre les listes d'accès de clé et les listes d'accès de cylindre réside dans la façon dont les entrées de groupe sont gérées. Dans les listes d'accès de clé, les cylindres peuvent simultanément être inclus de manière individuelle ou comme faisant partie d'un groupe de cylindres. Ce n'est pas le cas pour les listes d'accès de cylindre. Lorsqu'un groupe de clé est ajouté à une liste d'accès de cylindre, toute entrée individuelle de clé de ce groupe de clé (désormais redondant) est automatiquement retirée. Cela signifie que si un groupe de clé est ajouté, puis ultérieurement supprimé, toutes les clés du groupe perdent leur accès, y compris les clés qui disposaient précédemment d'un accès individuel.

8.1.3 Accès explicite et implicite

Les listes d'accès peuvent être configurées de deux façons :

- Un **accès explicite** est donné en modifiant les listes d'accès directement sur les clés, les cylindres et les groupes de cylindres.

- Un **accès implicite** est donné aux clés par l'intermédiaire des profils d'accès associés à une personne ou directement à une clé. Voir également *Chapitre 8.2.4 "Profils d'accès", page 179*.

Les clés dynamiques ont une liste d'accès comportant les cylindres et les groupes de cylindres que la clé est autorisée à ouvrir. L'accès de la clé à un cylindre ou un groupe de cylindres peut être implicite ou explicite. L'accès enregistré dans la liste d'accès de la clé est la combinaison des accès implicites et explicites.

Pour plus d'informations, consultez *Chapitre 8.2.4 "Profils d'accès", page 179* et *Chapitre 8.2.5 "Groupes d'accès temporaires", page 181*.

8.1.4 Validité de la clé

La validité de la clé signifie qu'une clé est à tout moment soit **active**, soit **inactive**. Une clé active dispose de l'accès en fonction des réglages d'autorisation et de planning, alors qu'une clé inactive est interdite de tout accès. Notez que la validité de la clé et le planning de la clé sont deux notions différentes. Voir également *Chapitre 8.1.8 "Plannings de clé", page 174*.

Il existe trois façons de contrôler la validité d'une clé :

- **Réglages d'activation**. Une clé peut être définie comme **Inactive**, **Toujours activeActive entre les dates sélectionnées**.

  Active entre les dates spécifiées n'est disponible que pour les Clés dynamiques et clés standard.
- **Revalidation**, une fonction facultative. Avec l'option Revalidation, les clés doivent être mises à jour à des intervalles spécifiés pour rester actives.

  Lorsque la revalidation est sélectionnée, **La clé doit toujours être revalidée.** s'affiche dans **Réglages de validité** sur CWM.

  Voir également *Chapitre 8.1.5 "Revalidation de clé", page 169*.
- **Validation du code PIN**, une fonction facultative pour les clés CLIQ Connect. Pour rester actives avec la validation du code PIN, les clés doivent être validées dans CLIQ Connect à des intervalles spécifiés en utilisant le code PIN.

  Voir également *Chapitre 8.1.7 "Validation du code PIN", page 173*.

Pour qu'une clé soit active, les conditions suivantes doivent être remplies :

- Elle doit être active selon les réglages d'activation.
- Elle doit être revalidée dans l'intervalle de revalidation spécifié (si la revalidation est utilisée).
- Elle doit être validée par code PIN dans l'intervalle de validation de code PIN spécifié (si la Validation du code PIN est utilisée).

Voir également *Chapitre 4.10.1 "Configuration de la validité de la clé, de la revalidation et de la validation du code PIN", page 86*.

8.1.5 Revalidation de clé

La **revalidation de clé** est une caractéristique permettant d'assurer la mise à jour des clés à intervalles précis.

Elle est soumise à licence.

Avec l'option de revalidation de clé, les clés doivent être mises à jour ("revalidées") à des intervalles spécifiés pour rester actives. Une fois revalidée, la clé reste active pendant le nombre de jours, heures et minutes spécifiés comme intervalle de revalidation, à partir du moment auquel elle a été revalidée. Si une clé n'est pas revalidée dans l'intervalle spécifié, elle devient inactive jusqu'à sa prochaine revalidation.

Figure 9 "Revalidation de clé", page 171 affiche le principe de la revalidation de clé. Lorsqu'une clé est revalidée dans un boîtier de programmation à distance, une minuterie démarre (1). L'accès avec la clé est possible tant qu'elle est utilisée dans l'intervalle de revalidation (2). À l'expiration de l'intervalle de revalidation (3), la clé doit être revalidée dans un boîtier de programmation à distance (1). Lorsqu'une clé est revalidée, la minuterie est réinitialisée.

Les clés sont également revalidées dans un boîtier de programmation local lorsque les actions suivantes ont été effectuées localement :

- définir le **Planning**
- lire le **Journal des événements**
- changer les **Cylindres dans la liste d'accès**

Si les conditions suivantes sont remplies, une clé est revalidée dans le logement de droite du boîtier de programmation local **sans** clé de programmation :

- Clé de 2e génération avec la version 12.3 du micrologiciel ou une version ultérieure
- CLIQ Connect PC est activé

REMARQUE !
La clé de programmation doit être retirée du logement de gauche du boîtier de programmation local avant mise à jour et revalidation.

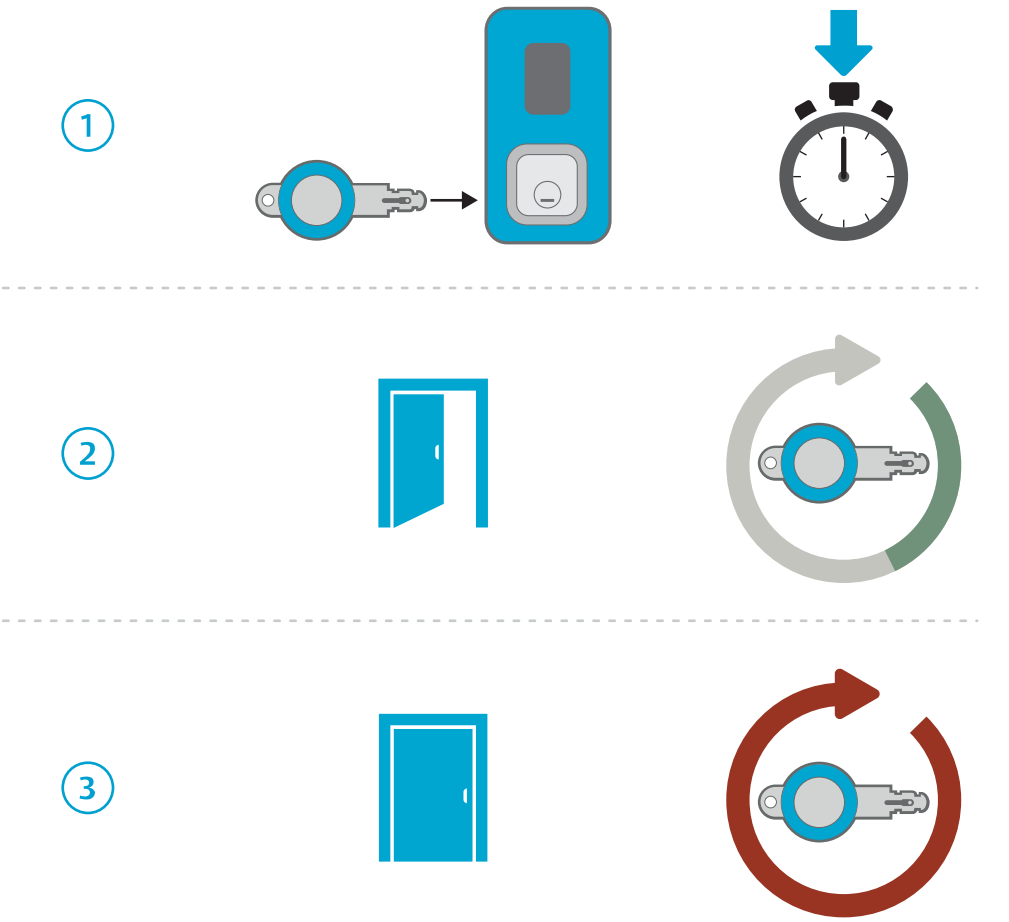


Figure 9. Revalidation de clé

La revalidation offre les avantages suivants :

- Elle veille à ce que les mises à jour de clé en attente soient régulièrement programmées sur les clés.
- Elle assure l'extraction fréquente des journaux des événements de clé.
- Elle limite l'exposition des clés perdues. Une clé perdue perd tous les accès quand le temps spécifié est écoulé. Si elle est déclarée perdue dans CWM, elle ne peut pas être revalidée.

Le réglage de l'intervalle de revalidation est un compromis entre la commodité d'usage pour le possesseur de la clé et la sécurité du système de fermeture. Un intervalle de revalidation court, tel que 24 heures, assure des mises à jour fréquentes et une exposition limitée des clés perdues mais nécessite de la part du possesseur de la clé la mise à jour de sa clé tous les jours. Un intervalle de revalidation plus long est plus pratique pour le possesseur de la clé, mais augmente l'exposition des clés perdues et entraîne des mises à jour des accès et des journaux des événements moins fréquents.

L'une des façons de régler ce problème consiste à utiliser la revalidation de clé en combinaison avec **Validation du code PIN** (pour les clés CLIQ Connect). Voir *Chapitre 8.1.7 "Validation du code PIN", page 173*.

Voir également *Chapitre 4.10.1 "Configuration de la validité de la clé, de la revalidation et de la validation du code PIN", page 86*.

La **revalidation flexible** est une caractéristique avancée permettant de résoudre la question du compromis. Voir *Chapitre 8.1.6 "Revalidation flexible", page 172*.

La fonction **Mise à jour hors ligne** des programmateurs à distance permet de revalider une clé même si la connexion du programmateur à distance avec le serveur est temporairement interrompue. Voir *Chapitre 8.3.3 "Mise à jour hors ligne", page 185*.

8.1.6 Revalidation flexible

La **revalidation flexible** est une fonction avancée en option permettant de définir l'intervalle de revalidation de clé par profil d'accès et par groupe de cylindres. Pour plus d'informations sur la revalidation de clé, voir *Chapitre 8.1.5 "Revalidation de clé", page 169*.

Elle est soumise à licence.

La revalidation flexible est utile dans les situations suivantes :

- Les cylindres ont des sensibilités différentes. Exemple : l'accès à une salle de serveurs peut être plus sensible que l'accès à une salle de réunion.
- Les rôles associés aux profils d'accès ont différentes sensibilités. Exemple : une revalidation plus fréquente peut être requise chez les sous-traitants par rapport aux employés.
- Certains rôles temporaires peuvent requérir des intervalles de revalidation différents. Exemple : une personne en astreinte peut requérir un intervalle de revalidation plus long, mais il lui sera demandé une plus grande prudence avec la clé.

ATTENTION !
En cas d'utilisation de la revalidation flexible, toutes les clés affectées par les réglages de revalidation des profils d'accès ou des groupes de cylindres doivent avoir la revalidation activée.

Avec la revalidation flexible, les intervalles de revalidation peuvent être définis à trois niveaux :

- **Réglage de la clé**. L'intervalle de revalidation défini sur la clé constitue le maximum. Aucun autre réglage dans les profils d'accès ou les groupes de cylindres ne peut donner un intervalle de revalidation plus long que celui-ci.

  Pour configurer l'intervalle de revalidation de clé, voir *Chapitre 4.10.1 "Configuration de la validité de la clé, de la revalidation et de la validation du code PIN", page 86*.
- **Réglages du groupe de cylindres**. Le réglage de l'intervalle de revalidation des groupes de cylindres peut être utilisé lorsque les groupes de cylindres ont des sensibilités différentes.

  L'intervalle de revalidation défini sur un groupe de cylindres limite l'intervalle défini sur la clé pour ce groupe de cylindres. Exemple : si une clé disposant d'un intervalle de revalidation de 14 jours se voit autoriser l'accès à un groupe de cylindres disposant d'un intervalle de revalidation de 7 jours, le réglage de 7 jours s'applique au groupe de cylindres. Mais si le groupe de cylindres dispose d'un intervalle de revalidation de 30 jours, le réglage de 14 jours de la clé s'applique au groupe de cylindres, étant donné que le réglage de la clé constitue toujours le maximum.

  Les cylindres des systèmes à groupe de cylindres héritent de l'intervalle de revalidation défini pour le groupe de cylindres auquel ils appartiennent.

Le réglage de l'intervalle de revalidation d'un groupe de cylindres ne nécessite pas de programmation des cylindres.

Pour configurer l'intervalle de revalidation d'un groupe de cylindres, voir *Chapitre 4.10.2 "Configuration de la revalidation flexible", page 88*.

- **Réglage de profil d'accès**. Le réglage d'intervalle de revalidation des profils d'accès peut être utilisé lorsque les rôles associés à différents profils d'accès ont des sensibilités différentes, ou lorsque le personnel d'astreinte a temporairement besoin d'intervalles de revalidation plus longs.

  L'intervalle de revalidation défini sur le profil d'accès prévaut sur le réglage des groupes de cylindres. Exemple : si un profil d'accès avec intervalle de revalidation de 10 jours autorise l'accès à un groupe de cylindres avec intervalle de revalidation de 7 jours, 10 jours seront appliqués à ce groupe de cylindres pour les clés associées au profil d'accès. Le réglage de la clé constitue encore une fois le maximum.

  Si une clé ou une personne est associée à plusieurs profils d'accès aux intervalles de revalidation différents et que ces profils d'accès autorisent l'accès au même groupe de cylindres, l'intervalle le plus long s'applique. Exemple : si deux profils d'accès, l'un avec un intervalle de revalidation de 10 jours et l'autre de 20 jours, autorisent tous deux l'accès au même groupe de cylindres, 20 jours s'appliquent au groupe de cylindres. Si spécifié, le réglage du groupe de cylindres est ignoré et c'est le réglage de la clé qui définit encore le maximum.

  Pour les groupes de cylindres pour lesquels l'intervalle de revalidation du groupe de cylindres et celui du profil d'accès ne sont pas spécifiés, le réglage de la clé s'applique.

  Pour configurer un intervalle de revalidation de profil d'accès, voir *Chapitre 4.10.2 "Configuration de la revalidation flexible", page 88*.

Conseil
Il est fortement recommandé d'utiliser principalement les réglages de revalidation sur les **groupes de cylindres** ou sur les **profils d'accès**, mais **pas sur les deux à la fois**. L'utilisation conjointe de ces deux notions peut brouiller la vision d'ensemble. Généralement, c'est le réglage des groupes de cylindres qui est utilisé, avec exceptions possibles spécifiées dans les profils d'accès.

8.1.7 Validation du code PIN

La validation par code PIN n'est pas disponible avec le boîtier de programmation mobile CLIQ Connect.

Validation du code PIN permet d'effectuer la validation hors ligne avec un code PIN. Cette validation nécessite l'utilisation de CLIQ Connect et fonctionne uniquement avec les clés utilisateur CLIQ Connect.

Elle est soumise à licence.

Lorsque Validation du code PIN est activé pour une clé, la clé est désactivée après un intervalle de temps spécifié appelé **Intervalle de validation de code PIN**. L'utilisateur de la clé doit alors entrer un code PIN pour l'activer de nouveau. La validation du code PIN est effectuée dans CLIQ Connect, avec l'option **Activer**. Le mécanisme est semblable à celui de la revalidation de clé, mais la validation du code PIN a un but différent :

La revalidation de clé impose au possesseur de la clé de mettre à jour la clé à certains intervalles pour maintenir la clé active. L'administrateur peut ainsi s'assurer que la clé

dispose des dernières mises à jour et la clé peut être désactivée si sa perte est déclarée dans CWM. En outre, lorsque la clé est mise à jour, les journaux des événements sont extraits de la clé si cette fonction est activée. La revalidation de clé nécessite une connexion Internet puisqu'il s'agit d'aller chercher des mises à jour sur le serveur CWM. Aucun code PIN ou mot de passe n'est requis pour valider la clé car il est toujours préférable que les clés disposent des dernières mises à jour. Pour plus d'informations, consultez *Chapitre 8.1.5 "Revalidation de clé", page 169*.

Utiliser la validation du code PIN augmente la sécurité à plusieurs niveaux :

- L'utilisateur doit saisir un code PIN.
- Protection contre le vol ou la perte de clés, même si elles ne sont pas déclarées comme perdues dans CWM.
- Ne nécessite pas de connexion Internet. Une clé peut être validée même si le serveur CWM est en panne ou la connexion Internet perdue.
- Comme il est plutôt facile de valider une clé à l'aide d'un code PIN, l'intervalle de validation par code PIN peut être défini sur une très courte durée, par exemple 30 minutes, ce qui augmente la sécurité.

La meilleure sécurité est obtenue avec une combinaison de revalidation de clé et de validation par code PIN. La revalidation de clé permet de s'assurer que la clé est à jour et avec la validation par code PIN la clé devient rapidement inutilisable pour toute personne ne disposant pas du code PIN.

Dans les paramètres système, il est possible de spécifier si la validation par code PIN doit faire partie du flux de remise et d'indiquer un intervalle de validation de code PIN par défaut. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

Voir également *Chapitre 8.1.4 "Validité de la clé", page 169*, *Chapitre 8.1.5 "Revalidation de clé", page 169* et *Chapitre 4.10.1 "Configuration de la validité de la clé, de la revalidation et de la validation du code PIN", page 86*.

8.1.8 Plannings de clé

Les **Plannings de clé** sont utilisés pour limiter les accès aux clés en fonction d'un programme horaire.

Si l'accès de la clé doit être limité à un certain horaire, tel que les heures bureau, un planning peut être configuré. Selon la version du microprogramme de la clé, deux types de planning horaire sont possibles : le planning horaire de base et le planning horaire à créneaux multiples. Pour plus d'informations sur les versions de microprogramme de clé, voir *Chapitre 9.7 "Fonctionnalité dépendante du microprogramme", page 214*.

- Avec le Planning de Base, il est possible de spécifier une tranche horaire par jour dans la semaine. Le planning s'applique à tous les cylindres.
- Avec le Planning à créneaux horaires multiples, plusieurs tranches horaires distinctes par semaine peuvent être spécifiées et chaque tranche horaire peut s'étaler sur plusieurs jours. Les plannings peuvent également être définis pour chaque cylindre, de façon individuelle.

REMARQUE !

Pour clés de génération 1 :

- Pour les cylindres inclus dans la liste d'accès de clé de façon individuelle (ne faisant pas partie d'un groupe de cylindres), spécifier une ou plusieurs tranches horaires pour un cylindre signifie que le planning général est ignoré pour ce cylindre.
- Pour les cylindres inclus dans la liste d'accès de clé comme faisant partie d'un groupe de cylindres, les tranches horaires spécifiques au cylindre sont ignorées.

Pour clés de génération 2 :

- La spécification d'une ou plusieurs tranches horaires pour un cylindre signifie que le planning général est ignoré pour ce cylindre.

Chaque clé peut être configurée avec un planning unique ou avec un planning basé sur un modèle de planning.

Voir aussi *Chapitre 4.10.3 "Configuration du planning de clé", page 89* et *Chapitre 6.10 "Gestion des modèles de planning", page 134*.

8.1.9 Verrouillage séquentiel

Le **Verrouillage séquentiel** est une fonction exigeant l'insertion de deux clés pour déverrouiller un cylindre.

La fonction Verrouillage séquentiel peut être configurée en usine pour chaque cylindre, de façon individuelle. Elle ne peut pas être configurée depuis CWM.

Pour les cylindres sur lesquels cette fonction est activée, le déverrouillage du cylindre exige l'insertion de deux clés avec autorisation d'accès. Les clés doivent être insérées à la suite, en une minute, pour que le cylindre s'ouvre. Les cylindres dotés de cette fonction peuvent, en option, être configurés pour exiger que les deux clés appartiennent à des groupes de clés différents.

8.1.10 Ouverture retardée

L'**Ouverture retardée** est une fonction qui permet d'accorder l'accès à un cylindre pour une clé nouvellement revalidée après un délai spécifique.

La fonction Ouverture retardée peut être configurée en usine pour chaque cylindre, de façon individuelle. Elle ne peut pas être configurée depuis CWM.

Pour les cylindres sur lesquels cette fonction est activée, le délai configuré (par exemple 15 minutes) est ajouté aux temps d'activation et d'expiration pour toutes les clés accédant au cylindre. Pour les cylindres à haute sensibilité, il est recommandé d'utiliser l'ouverture retardée en association avec un intervalle de revalidation court, par exemple 30 minutes. Ainsi, vous avez la garantie que la clé est inactive la plupart du temps (si elle n'est pas revalidée très fréquemment) et qu'un délai est défini après la revalidation et avant que quiconque ne puisse effectivement ouvrir le cylindre.

Dans les cas où les cylindres présentent des sensibilités différentes, la fonction de revalidation flexible peut être utile. Voir *Chapitre 8.1.6 "Revalidation flexible", page 172*.

8.1.11 Ouverture en ligne

L'**Ouverture en ligne** est une fonction utilisée avec les clés CLIQ Connect pour s'assurer que les clés sont toujours actualisées avant l'ouverture des cylindres. Ceci empêche l'accès pour les clés dont les droits d'accès sont révoqués ainsi que pour les clés marquées comme perdues.

L'ouverture en ligne peut être configurée en usine pour chaque cylindre ou pour chaque clé CLIQ Connect, de façon individuelle. Elle ne peut pas être configurée depuis CWM.

Si la fonction Ouverture en ligne est activée sur une clé CLIQ Connect, l'ouverture en ligne est obligatoire lors de l'accès à n'importe quel cylindre avec cette clé.

Si la fonction Ouverture en ligne est activée sur un cylindre, toutes les clés accédant à ce cylindre doivent réaliser une ouverture en ligne. Cela signifie que l'accès est limité aux clés CLIQ Connect.

Lorsqu'une ouverture en ligne est requise, la clé CLIQ Connect doit être appairée avec CLIQ Connect avant d'être insérée dans le cylindre. Une fois la clé insérée, CLIQ Connect contacte le serveur CWM Remote, récupère les dernières mises à jour de la clé et met la clé à jour. Si, après sa mise à jour, la clé dispose d'un accès au cylindre, ce dernier est immédiatement débloqué.

Les cylindres dotés de la fonction Ouverture en ligne peuvent être configurés pour accepter les **Clés prioritaires** sans exiger d'ouverture en ligne. Les clés peuvent être configurées en usine en tant que Clés prioritaires.

8.2 Fonctions de regroupement

8.2.1 Groupes de clés

Les **groupes de clés** sont utilisés pour définir des droits d'accès et d'autres attributs à un groupe de clés plutôt qu'à chaque clé de façon individuelle.

Les groupes de clés servent principalement lorsque les listes d'accès de cylindre sont utilisées pour contrôler les accès.

Avantages des groupes de clé :

- Les groupes de clé réduisent le nombre d'entrées requises dans les listes d'accès de cylindre.
- L'ajout d'une nouvelle clé à un groupe de clé autorisé dans un cylindre autorise automatiquement l'accès à la nouvelle clé. Aucune programmation des cylindres n'est requise.
- Les groupes de clés peuvent être utilisés pour la configuration groupée de plannings de clés.

Lorsque l'accès à un cylindre est attribué à un groupe de clé, l'accès est automatiquement attribué à toutes les clés du groupe. Il reste cependant possible de définir des exceptions et de bloquer l'accès de certaines clés individuelles.

REMARQUE !
Lorsqu'un groupe de clé est ajouté à une liste d'accès, toute entrée individuelle de clé de ce groupe de clé (désormais redondant) est automatiquement supprimée. Cela signifie que si un groupe de clé est ajouté, puis ultérieurement supprimé, toutes les clés du groupe perdent leur accès, y compris les clés qui disposaient précédemment d'un accès individuel.

Il existe différents types de groupes de clés :

Groupe de clé normale	Il peut comporter des clés standard et les clés normales.
Groupe de clé dynamique	Il peut comporter des clés dynamiques.
Groupe de clé de programmation normale	Il peut comporter des clés de programmation normales.
Groupe de clé de programmation maîtresse	Il peut comporter des clés de programmation maîtresses.

Les clés mécaniques ne peuvent appartenir à aucun groupe de clé.

Pour effectuer une configuration groupée des plannings de clés d'un groupe, voir *Chapitre 4.10.4 "Configuration du planning d'un groupe de clé", page 91*.

8.2.2 Domaines

La fonction **Domaines** est une fonction de groupement administratif qui permet aux administrateurs d'accéder et de contrôler des régions spécifiques d'un système de fermeture.

Elle est soumise à licence.

Les domaines sont utilisés pour diviser les éléments suivants en régions administratives :

- clés
- employés
- visiteurs
- cylindres
- groupes de cylindres
- profils d'accès
- groupes d'accès temporaires

Les groupes de clé et les clés de programmation ne peuvent pas appartenir à un domaine. De ce fait, les administrateurs peuvent visualiser les groupes de clés et les clés de programmation, quels que soient leurs domaines.

Un domaine consiste en un ensemble de groupes d'éléments généralement associés à une région géographique ou organisationnelle. Les clés de programmation associées à un domaine disposent uniquement des droits d'administration pour les cylindres inclus dans ce domaine.

Avantages des domaines :

- Commodité : Travaillant avec des régions du système de fermeture, telles qu'une zone géographique, les administrateurs ne sont pas distraits par les informations des éléments d'autres zones.
- Sécurité : Les administrateurs ne sont pas autorisés à visualiser ou à gérer les éléments d'autres domaines.

À propos des domaines :

- Les cylindres qui appartiennent à un groupe de cylindres sont inclus dans un domaine par le biais de leur groupe de cylindres. En d'autres termes, tous les cylindres d'un même groupe appartiennent au même domaine.
- Les cylindres qui n'appartiennent pas à un groupe, notamment tous les cylindres mécaniques, sont inclus individuellement dans un domaine.
- Les éléments peuvent uniquement appartenir à un domaine (clé, employés, visiteurs, cylindres, groupes de cylindre, profils d'accès et groupes d'accès temporaires).
- Pour les cylindres à double entrée, les deux entrées doivent appartenir au même domaine.
- La clé de programmation d'un administrateur peut être associée à un ou plusieurs domaines, en fonction de son attribution.

> **REMARQUE !**
> Bien que les clés de programmation ne puissent pas appartenir à un domaine, chaque clé de programmation possède une liste de domaines que l'administrateur connecté est autorisé à accéder et contrôler.

Pour associer une clé de programmation à un domaine, voir *Chapitre 6.11.5 "Sélection des domaines de clé de programmation", page 137*.

8.2.3 Groupes de cylindre

Un **groupe de cylindres** est un ensemble de cylindres utilisé pour simplifier l'administration des systèmes de fermeture à grand nombre de cylindres.

Elle est soumise à licence.

Les groupes de cylindres sont utilisés dans les systèmes de fermeture, alors appelés **systèmes à groupes de cylindres**. Ils concernent les cylindres qui prennent en charge les groupes de cylindres. Voir *Chapitre 9.7 "Fonctionnalité dépendante du microprogramme", page 214*.

Les groupes de cylindres sont prédéfinis en usine, mais il est possible de changer les cylindres de groupe par la suite. Néanmoins, cela requiert une programmation de cylindre et il est par conséquent recommandé de soigneusement planifier les groupes à l'avance.

L'accès peut être donné à un groupe de cylindres de la même façon qu'à un cylindre seul. Il est possible de combiner groupes de cylindres et cylindres seuls pour plus de flexibilité.

Avantages des groupes de cylindres :

- Administration simplifiée des systèmes de fermeture comportant un grand nombre de cylindres.
- Étant donné qu'une seule entrée sur la clé peut donner accès à plusieurs cylindres, une clé peut accéder à un très grand nombre de cylindres.
- Lorsqu'un cylindre est ajouté ou retiré d'un groupe de cylindres, les clés ayant accès au groupe de cylindres sont immédiatement affectées. La mise à jour manuelle de la liste d'accès de chaque clé n'est pas nécessaire.

La configuration des groupes de cylindres est un compromis entre différentes considérations :

- Les groupes de cylindres doivent être configurés de sorte que l'accès est normalement accordé à tous les cylindres du groupe.

Il est impossible d'autoriser l'accès à tous les cylindres d'un groupe tout en omettant quelques-uns. Si les conditions l'imposent, les exceptions de cylindre devront être placées dans un groupe séparé.

- Les groupes de cylindres ne doivent pas être trop petits, car il est important de limiter le nombre de groupes. Moins les groupes sont nombreux, plus l'administration en est simplifiée, et plus le nombre d'entrées requises dans les listes d'accès de la clé est faible.
- Les groupes de cylindres doivent néanmoins être suffisamment petits pour être stables, c'est-à-dire qu'il doit être exceptionnel d'avoir à déplacer un cylindre d'un groupe à un autre.

À propos des groupes de cylindres :

- Les cylindres ne peuvent appartenir qu'à un seul groupe de cylindres.
- Les groupes de cylindres ne peuvent appartenir qu'à un seul domaine.
- Pour les cylindres doubles, les deux entrées doivent appartenir au même groupe de cylindres.
- Les cylindres mécaniques ne peuvent appartenir à un groupe de cylindres.

8.2.4 Profils d'accès

Les **profils d'accès** servent à attribuer les accès nécessaires aux personnes disposant de rôles spécifiques, sans avoir à configurer chaque clé individuellement. Les clés peuvent également être directement associées à des profils d'accès.

Elle est soumise à licence.

REMARQUE !
Les rôles définis par les profils d'accès ne doivent pas être confondus avec les rôles définis pour les administrateurs travaillant avec CWM.

Les personnes ayant un rôle spécifique, tel que l'entretien de bureaux, sont associées à un profil d'accès correspondant. Le profil d'accès définit l'ensemble de cylindres et de groupes de cylindres devant être accessibles par les personnes ayant ce rôle précis. Les clés remises aux personnes associées contiennent automatiquement les accès adéquats et définis dans le profil d'accès.

Figure 10 "Profils d'accès", page 180 affiche un exemple avec deux profils d'accès (1, 2), chacun avec un accès à un certain nombre de cylindre ou groupes de cylindres ou les deux (A, B). Les profils d'accès peuvent être associés à une personne (3) ou une clé. Lorsque le profil d'accès est associé une personne, la clé remise à cette personne a automatiquement accès aux profils d'accès associés.

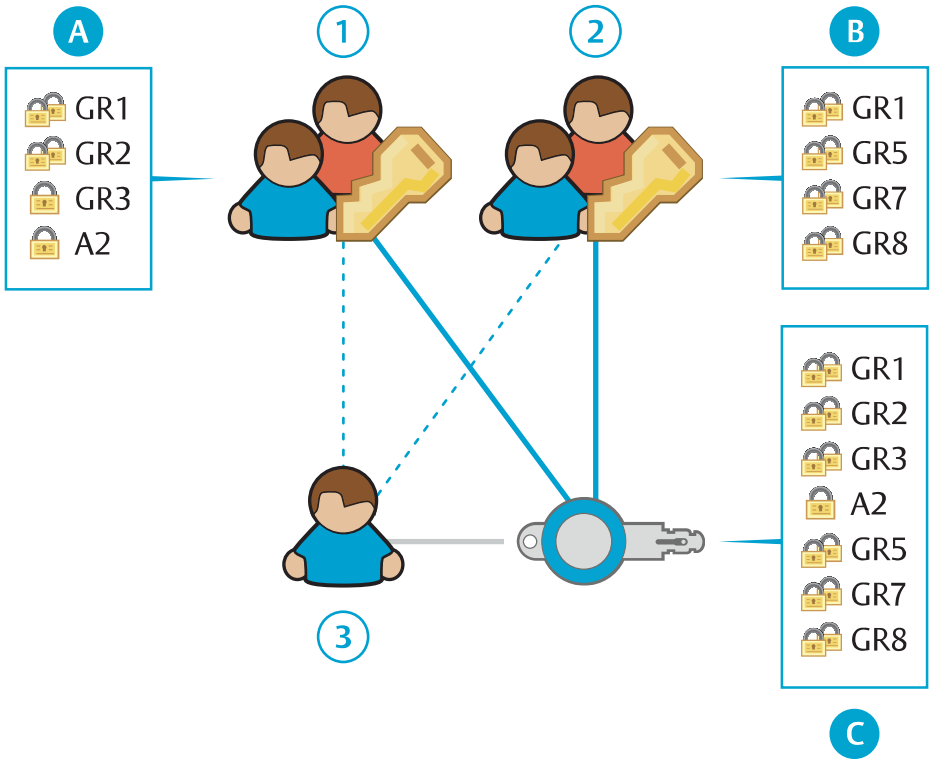


Figure 10. Profils d'accès

Si le profil d'accès est directement associé à une clé, les autres clés appartenant au même possesseur de clés n'héritent pas de ce profil d'accès.

Les profils d'accès sont dynamiques, c'est-à dire qu'un changement dans un profil d'accès met automatiquement à jour le statut des autorisations de clé, car elles sont définies dans CWM (également appelé **État défini**). Un changement dans un profil d'accès crée des traitements de mise à jour à distance pour les clés associées. Aucune programmation de cylindre n'est requise. Pour de plus amples informations sur **État défini** et **État actuel**, voir *Chapitre 9.1.1 "Termes", page 198*.

Les profils d'accès définissent l'**accès implicite** pour les clés, alors que les cylindres et groupes de cylindres autorisés et directement définis pour la clé définissent l'**accès explicite**. L'accès effectif enregistré dans la liste d'accès de la clé est la combinaison des accès implicites et explicites. Cela signifie que la clé peut accéder à la fois aux cylindres définis dans le profil d'accès et aux cylindres définis explicitement pour la clé.

Avantages des profils d'accès :

- Possibilité de gérer simultanément l'accès pour plusieurs personnes ou plusieurs clés.
- Possibilité de définir les profils correspondant à des rôles et d'autoriser l'accès aux personnes ayant un ou plusieurs rôles.
- Lorsqu'un profil d'accès est modifié, les traitements de mise à jour à distance associés sont automatiquement créés.

Remarques sur les profils d'accès :

- Une clé ou une personne peut avoir plusieurs rôles et donc être associée à plusieurs profils d'accès.

- Des cylindres, ainsi que des groupes de cylindres, peuvent être inclus dans un profil d'accès.
- Un profil d'accès appartient à un seul et unique domaine et seuls les cylindres et groupes de cylindres appartenant à ce domaine peuvent être ajoutés.

> **REMARQUE !**
> Il est recommandé de vérifier que le profil d'accès et tous les cylindres et groupes de cylindres appartiennent au même domaine. Il faut en effet s'assurer que les administrateurs d'un domaine donné ne peuvent avoir accès à des cylindres d'autres domaines (par le biais des profils d'accès).

- En cas d'introduction de profils d'accès dans un système de fermeture où les autorisations des listes d'accès de clé sont déjà en utilisation, les listes d'accès de clé peuvent contenir plusieurs entrées du même cylindre ou groupe de cylindres. Pour supprimer les entrées redondantes, voir *Chapitre 4.7.7 "Suppression des autorisations de clé redondantes", page 76*.

> **Conseil**
> Pour garder une meilleure vision d'ensemble lorsqu'on utilise des profils d'accès, il est recommandé de limiter au minimum l'usage des accès explicites.

8.2.5 Groupes d'accès temporaires

Les **groupes d'accès temporaires** sont utilisés pour étendre temporairement l'accès des clés en les associant à une sélection de profils d'accès. L'accès d'un groupe d'accès temporaire est un accès combiné de profils d'accès inclus pendant une période de temps défini avec une date de début et une date de fin.

Il est donné aux clés dans un groupe d'accès temporaire un accès implicite temporaire aux cylindres et groupe de cylindres qui sont attribués aux profils d'accès inclus. En outre, il est donné aux clés un accès implicite temporaire aux cylindres individuels et groupes de cylindres qui sont attribués à un groupe d'accès temporaire.

Figure 11 "Groupes d'accès temporaires", page 182 illustre une clé qui a été ajoutée à un groupe d'accès temporaire (1) avec trois profils d'accès (2, 3, 4) et un jeu de cylindres individuels et groupes de cylindres (4). Chaque profil d'accès a accès à un certain nombre de cylindres ou groupes de cylindres ou les deux (A, B). Pendant une période de temps définie, l'accès à tous les cylindres et les groupes de cylindre (D) est accordé à la clé.

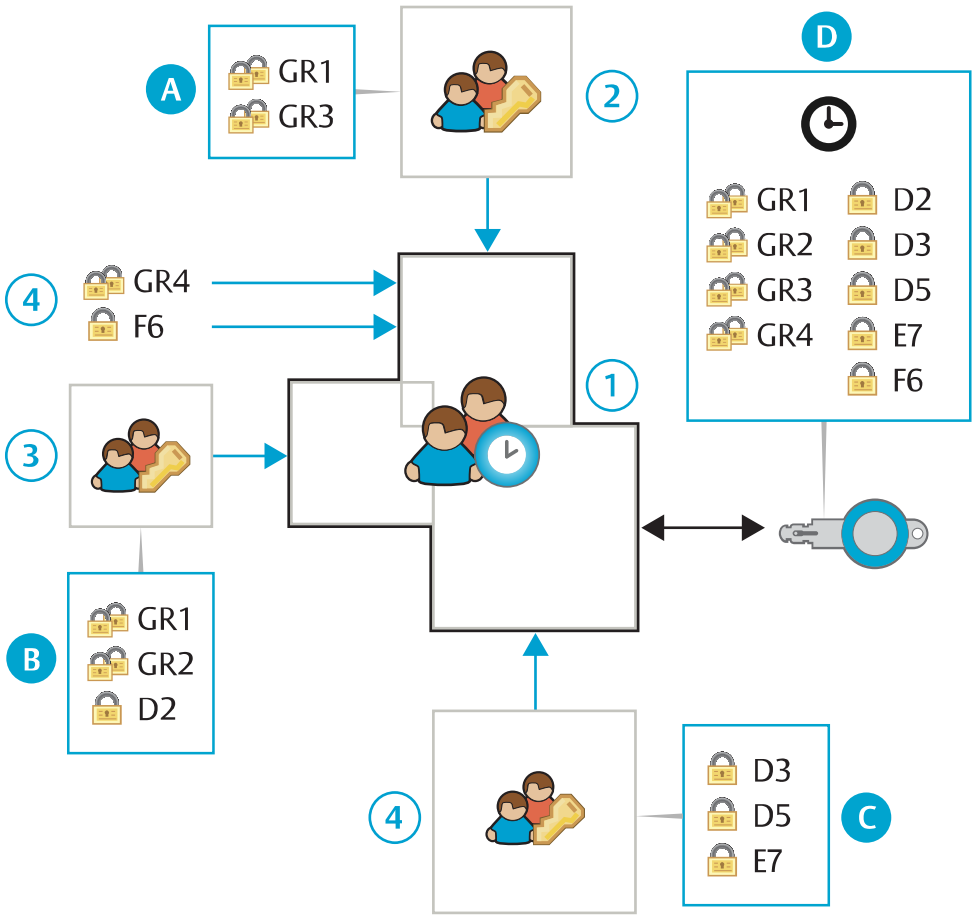


Figure 11. Groupes d'accès temporaires

Un exemple de cette utilisation est lorsque plusieurs techniciens sont d'astreinte et ont besoin d'avoir accès à un certain nombre de profils d'accès pendant la période d'astreinte.

En pratique, la clé est ajoutée à un groupe d'accès temporaire et programmée dans un programmateur local ou une borne d'actualisation. Lorsque le groupe d'accès temporaire n'est plus valide pour une clé, un traitement à distance sera automatiquement créé pour supprimer de la clé, l'accès au groupe d'accès temporaire.

REMARQUE !
L'annulation de l'accès de cette clé ne prendra effet que lorsque la clé est mise à jour dans une borne d'actualisation. Pour empêcher que le possesseur de la clé n'utilise la clé après l'expiration du groupe d'accès temporaire, effectuez une des opérations suivantes avant de remettre la clé :

- Réglez **Active entre les dates sélectionnées** dans les réglages d'activation, voir *Chapitre 8.1.4 "Validité de la clé", page 169*.
- Activez la **Revalidation** de clé, voir *Chapitre 8.1.5 "Revalidation de clé", page 169*.

Il est fortement recommandé d'associer les groupes d'accès temporaires avec la revalidation de clé.

Avantages de groupe d'accès temporaire :

- Possibilité de donner temporairement l'accès à une ou plusieurs clés à un groupe de profils d'accès, cylindres individuels et groupes de cylindres.

Remarques sur le groupe d'accès temporaire :

- Tous les profils d'accès dans un groupe d'accès temporaire doivent faire partie du même domaine.
- Les utilisateurs attribués au domaine par défaut peuvent voir les groupes d'accès temporaires de tous les domaines. Les utilisateurs connectés pour d'autres domaines peuvent uniquement voir les groupes d'accès temporaires dans leurs propres domaines.

8.2.6 Notes

Une **note** est une chaîne de texte pouvant être utilisée pour étiqueter des objets et faciliter ainsi leur localisation et leur administration.

Exemple : les profils d'accès peuvent être groupés par type de rôle auquel ils sont associés et les cylindres groupés selon le bâtiment dans lequel ils sont installés.

Lors de la recherche d'objet, les notes peuvent être utilisées comme critères de recherche.

Les notes sont parfois déjà ajoutées aux fichiers d'extension et disponibles lorsque les fichiers sont importés dans CWM. Il est également possible d'ajouter ou de supprimer manuellement des notes pour les objets suivants :

- Employés (voir *Chapitre 4.1.7 "Ajout ou suppression de notes employés ou visiteurs", page 31*)
- Visiteurs (voir *Chapitre 4.1.7 "Ajout ou suppression de notes employés ou visiteurs", page 31*)
- Clés (voir *Chapitre 4.2.5 "Ajout ou suppression de notes de clé utilisateur", page 37*)
- Groupes de clés (voir *Chapitre 4.3.3 "Ajout ou suppression de notes de groupes de clés", page 54*)
- Cylindres (voir *Chapitre 4.4.3 "Ajout ou suppression de notes de cylindre", page 57*)
- Groupes de cylindres (voir *Chapitre 4.5.3 "Ajout ou suppression de notes de groupes de cylindres", page 67*)
- Profils d'accès (voir *Chapitre 4.6.4 "Ajout ou suppression de notes de profil d'accès", page 70*)
- Bornes d'actualisation (voir *Chapitre 6.5.5 "Ajout ou suppression de notes de boîtier de programmation à distance", page 108*)

Il est possible d'ajouter plusieurs notes à un même objet.

8.3 Fonctionnalité à distance

8.3.1 Présentation de la fonctionnalité à distance

La fonctionnalité à distance permet les mises à jour à distance des configurations de clé. Elle permet également la revalidation et la récupération des journaux des événements à partir d'un site distant.

Elle est soumise à licence.

- **Mise à jour à distance des configurations de clé**

  L'administrateur configure les autorisations et autres réglages de clé sans avoir besoin de la clé. La nouvelle configuration de la clé est enregistrée dans la base de

données du serveur à distance en tant que **traitement de mise à jour à distance**. Lorsque la clé est insérée dans un boîtier de programmation à distance, le traitement de mise à jour est exécuté et la clé est programmée selon la nouvelle configuration.

- **Mise à jour à distance du réglage de l'heure actuelle de la clé**

  Le réglage de l'heure actuelle de la clé est mis à jour à chaque mise à jour de la clé.

- **Extraction à distance de journaux des événements**

  Le journal des événements de la clé est extrait à chaque mise à jour de la clé, sauf si la fonction Approbations des réglages système est activée.

- **Revalidation**.

  La revalidation veille à ce que les clés soient mises à jour à intervalles de temps précis. Pour plus d'informations sur la revalidation, voir *Chapitre 8.1.5 "Revalidation de clé", page 169*.

Voir également *Chapitre 8.3.2 "Mise à jour à distance", page 184*.

Les systèmes sont livrés comme des systèmes à distance ou des systèmes utilisant uniquement des boîtiers de programmations locaux. Un système utilisant uniquement des boîtiers de programmations locaux qui est par la suite, converti en un système à distance peut contenir des clés prenant en charge les mises à jour à distance et des clés ne prenant pas en charge les mises à jour à distance. Dans un système initialement fourni comme un système à distance, toutes les clés prennent en charge les mises à jour à distance à la livraison.

8.3.2 Mise à jour à distance

Les **tâches de mise à jour à distance** sont des mises à jour de clé en attente. Elles ne doivent pas être confondues avec les **tâches de programmation de cylindre** qui sont des mises à jour de cylindre en attente. Pour plus d'informations sur les tâches de programmation de cylindre, voir *Chapitre 8.5 "Programmation de cylindre", page 187*.

À moins que la clé ne soit scannée dans un boîtier de programmation local, toutes les actions nécessitant une mise à jour des informations de la clé entraînent un traitement de mise à jour à distance, notamment la mise à jour des autorisations, de la validité, du planning, etc. Le traitement de mise à jour à distance est exécuté à la prochaine insertion de la clé dans un boîtier de programmation à distance.

Le boîtier de programmation à distance est normalement en ligne, mais il peut aussi être configuré pour autoriser les mises à jour de clé dans certains cas lorsqu'il est hors ligne. Voir *Chapitre 8.3.3 "Mise à jour hors ligne", page 185*.

Dans tout CWM, le symbole utilisé pour les traitements de mise à jour à distance est le suivant :

 Une mise à jour à distance en attente existe pour la clé

Pour afficher les mises à jour d'autorisation à distance en attente, voir *Chapitre 4.9.1 "Configuration des autorisations dans les clés", page 78*.

Dépassement de la capacité de la clé
Les traitements de mise à jour à distance qui dépasseraient la capacité de la liste d'accès d'une clé ne seront pas exécutés. Lorsqu'un tel traitement est créé dans CWM, un e-mail est envoyé à ce sujet à tous les administrateurs qui ont la permission totale sur l'ensemble des **autorisations de clés** et dont l'adresse e-mail a été spécifiée. Le travail est également marqué par le symbole suivant dans CWM :

 Il existe une mise à jour en attente qui dépasse la capacité de la clé

Lorsque des opérations sont réalisées sur une clé unique donnée à partir de la vue relative à cette clé, un traitement de mise à jour à distance est créé instantanément et l'administrateur voit immédiatement si la capacité de la clé est dépassée. En revanche, lorsque les opérations sont faites à partir d'autres fenêtres, les traitements de mise à jour ne sont pas créés instantanément et l'administrateur n'en est pas avisé immédiatement.

Certaines opérations peuvent générer des traitements de mise à jour qui dépassent la capacité de la clé sans que l'administrateur en soit avisé :

- Ajout d'un accès à un profil d'accès
- Ajout de profils d'accès à plusieurs clés
- Ajout de profils d'accès à une personne

Pour résoudre ce problème, il faut réduire le nombre d'entrées de la liste d'accès de la clé. Cela peut être fait en réduisant le nombre d'accès explicites ou le nombre d'accès des profils d'accès concernés, ou encore en supprimant des profils d'accès associés. Le traitement de mise à jour à distance est alors automatiquement adapté.

8.3.3 Mise à jour hors ligne

L'actualisation hors ligne n'est pas disponible avec le boîtier de programmation mobile CLIQ Connect.

La **mise à jour hors ligne** est une fonction permettant de revalider des clés via une borne d'actualisation, même si la connexion réseau est temporairement perdue. Ceci est utile dans les cas où il est essentiel qu'une clé puisse obtenir l'extension de sa validité, même si la connexion réseau est instable. Les mises à jour des accès peuvent être réalisées en mode hors ligne. La mise à jour hors ligne peut être configurée par borne d'actualisation.

Pour limiter les risques et l'exposition des clés perdues, un certain nombre de conditions peuvent être définies pour qu'une mise à jour hors ligne soit autorisée. Les éléments suivants sont configurables :

- Le nombre de mises à jour consécutives pouvant être effectuées en mode hors ligne avant qu'une mise à jour en ligne ne soit nécessaire.
- La durée pendant laquelle les mises à jour hors ligne sont autorisées après la dernière mise à jour en ligne.
- La durée d'extension de la période la validité de la clé lors d'une mise à jour hors ligne. L'intervalle de revalidation réglé sur les clés est ignoré lors des mises à jour hors ligne.

Spécifique aux programmateurs muraux

La clé ne peut pas bénéficier d'une mise à jour hors ligne si elle est incluse dans la **Liste de révocation des clés** stockée dans chaque borne de rechargement de droits. Cette liste contient les clés qui ont été déclarées perdues et qui ne doivent donc pas bénéficier d'une mise à jour hors ligne. La borne de rechargement de droits cherche les nouvelles versions de la liste de révocation des clés à chaque pulsation et n'autorise les mises à jour hors ligne que si la version de la liste stockée dans la borne de rechargement de droits n'est pas trop ancienne. La durée de validité d'une liste de révocation des clés peut être configurée par un paramètre de la borne de rechargement de droits.

Spécifique aux boîtiers de programmation mobiles CLIQ

Seules les clés ayant été mises à jour récemment dans le même boîtier de programmation mobile CLIQ (clés faisant partie des 10 dernières clés actualisées) peuvent être revalidées en mode hors ligne.

Voir également *Chapitre 8.1.5 "Revalidation de clé", page 169*.

Pour configurer la mise à jour hors ligne, voir *Chapitre 6.5.7 "Configuration de boîtiers de programmation muraux", page 110* et *Chapitre 6.5.8.1 "Modification des réglages du boîtier de programmation mobile CLIQ", page 118*.

8.3.4 CLIQ Connect et CLIQ Connect+

CLIQ Connect est une application installée sur un appareil mobile tel qu'un téléphone portable ou une tablette. Elle permet aux possesseurs de clés utilisateur, c'est-à-dire les visiteurs et les employés, de les gérer facilement. CLIQ Connect est disponible pour Android et iOS.

CLIQ Connect offre les fonctions suivantes :

- Validation et modification du code PIN d'une clé Connect.
- Mise à jour des clés Connect via la connexion Bluetooth de la clé
- Mise à jour des autres types de clés utilisateur via un boîtier de programmation mobile CLIQ Connect.

CLIQ Connect+

CLIQ Connect+ peut être utilisé avec CLIQ Connect **version 4.0 ou une version ultérieure**. Grâce à cette fonction, tous les utilisateurs de clés enregistrés peuvent afficher davantage d'informations sur leurs clés, telles que la validité, le planning horaire ou les cylindres accessibles, aussi bien pour les clés connectées que non connectées.

Une fois l'activation effectuée, le possesseur de la clé suit les instructions de l'e-mail envoyé par CWM pour terminer l'installation. L'application est configurée à l'aide d'un code QR inclus dans l'e-mail.

Cette fonction requiert les conditions suivantes :

- Système CWM version 11.2 ou ultérieure.
- La licence **CLIQ Connect+** est reconnue sur le système.

  Pour installer la licence, voir *Chapitre 6.1 "Gestion des licences", page 99*.
- L'utilisateur de la clé est un utilisateur CLIQ Connect+ activé.

  Pour permettre aux utilisateurs de clés d'accéder à CLIQ Connect+, voir *Chapitre 4.1.5 "Activation ou désactivation de CLIQ Connect+ pour les Employés ou les Visiteurs.", page 28*.
- L'utilisateur de clé active le compte CLIQ Connect+ en suivant les instructions de l'e-mail envoyé par CWM.

8.4 Liens externes

Un **lien externe** est une URL, une adresse Internet, pouvant être utilisée pour lier un objet, tel qu'un employé ou un cylindre, à des informations supplémentaires.

Exemple : un employé peut être lié à sa page sur l'Intranet de l'entreprise et un cylindre ou un boîtier de programmation mural peuvent être liés à une carte indiquant leur emplacement.

Des liens externes peuvent être ajoutés aux objets suivants :

- Employés (voir *Chapitre 4.1.8 "Gestion des liens externes employé ou visiteur", page 32*)

- Visiteurs (voir *Chapitre 4.1.8 "Gestion des liens externes employé ou visiteur", page 32*)
- Clés (voir *Chapitre 4.2.6 "Gestion des liens externes d'une clé utilisateur", page 37*)
- Cylindres (voir *Chapitre 4.4.4 "Gestion des liens externes d'un cylindre", page 57*)
- Profils d'accès (voir *Chapitre 4.6.5 "Modification de liens externes de profil d'accès", page 71*)
- Bornes d'actualisation (voir *Chapitre 6.5.6 "Gestion des liens externes de boîtier de programmation à distance", page 109*)

Il est possible d'ajouter plusieurs liens externes à un objet.

8.5 Programmation de cylindre

La programmation de cylindre comprend la mise à jour de la liste d'accès du cylindre ou l'extraction des journaux des événements du cylindre.

Une **tâche de programmation de cylindre** est créée dans CWM dans les cas suivants :

- Les clés autorisées pour un cylindre sont mises à jour.
- Une clé présente dans la liste d'accès des cylindres est déclarée perdue ou défectueuse.
- La reprogrammation d'un cylindre est sélectionnée.
- Une extraction de journal des événements du cylindre est sélectionnée.
- Le groupe de cylindres auquel appartient un cylindre est modifié.

Lorsque les tâches de programmation du cylindre doivent être exécutées, elles sont d'abord chargées sur une clé de programmation dans le Boîtier de programmation local ou le Boîtier de programmation à distance. En insérant la clé de programmation dans le cylindre, la tâche de programmation est exécutée et, le cas échéant, les journaux des événements du cylindre sont chargés sur la clé de programmation. Une fois la tâche de programmation exécutée, la clé de programmation est à nouveau insérée dans le Boîtier de programmation local ou le Boîtier de programmation à distance et le Système de verrouillage peut être mis à jour avec des informations sur les tâches de programmation terminées et les journaux des événements récupérés.

Figure 12 "Programmation du cylindre", page 188 illustre deux manières d'exécuter des tâches de programmation de cylindres :

- Dans le premier cas (1), la tâche de programmation de cylindre est chargée sur la clé de programmation de l'administrateur (A) via un boîtier de programmation local. Cette clé est ensuite transmise puis insérée dans le cylindre nécessitant une programmation. Elle est retournée lorsque la tâche est terminée pour mettre à jour le système de verrouillage.
- Dans le second cas (2), un administrateur se connecte à CWM en utilisant une clé de programmation (A) et prépare les tâches de programmation du cylindre que les autres administrateurs récupéreront avec leurs clés de programmation (B) dans un boîtier de programmation à distance. Les clés de programmation sont alors insérées dans les cylindres puis retournées au boîtier de programmation à distance pour mise à jour du système de verrouillage.

  Il est possible, grâce à l'option de récupération, exécution et confirmation des tâches de programmation via un boîtier de programmation à distance, d'avoir un administrateur préparant les tâches dans CWM et un autre administrateur programmant les cylindres sans être connecté à CWM.

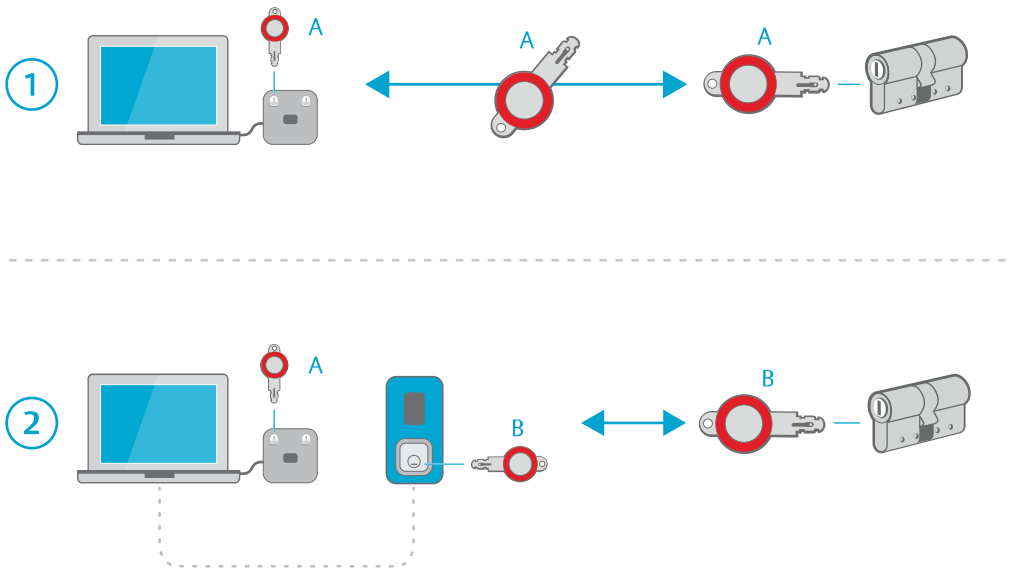


Figure 12. Programmation du cylindre

Dans CWM, le symbole utilisé pour les tâches de programmation de cylindre est le suivant :

- La tâche de programmation de cylindre existe
- La tâche de programmation de cylindre doit être approuvée
- La tâche de programmation de cylindre a été programmée pour la clé de programmation
- La tâche de programmation de cylindre est terminée
- La tâche de programmation de cylindre a échoué ou a été annulée
- La tâche de programmation de cylindre a été remplacée par une nouvelle tâche

Les tâches de programmation de cylindre peuvent être chargées sur les clés de programmation uniquement avec la permission **programmation du cylindre**.

Les tâches impliquant la modification du groupe auquel appartient le cylindre nécessitent également une clé de programmation avec une possibilité de **programmation du groupe de cylindres** Pour savoir si une clé de programmation a cette capacité, consultez les informations détaillées de la clé de programmation. Voir *Chapitre 6.11.1 "Recherche de clés de programmation", page 135* ou *Chapitre 6.11.2 "Scanner une clé de programmation", page 136*. Dans les systèmes initialement fournis comme systèmes à groupes de cylindres, toutes les clés de programmation ont cette capacité.

Voir également *Chapitre 4.4.13 "Programmation des cylindres", page 62* et *Chapitre 8.8 "Rôles et autorisations CWM", page 191*.

Reprogrammation
La reprogrammation peut être utilisée comme première mesure de dépannage si un cylindre ne fonctionne pas comme prévu. Par exemple, si la clé de programmation est

retirée trop rapidement lors de la programmation d'un cylindre, ce dernier ne fonctionne pas correctement et la reprogrammation résout le problème.

Lorsqu'une clé de programmation avec une tâche de programmation qui a échoué est insérée dans un boîtier de programmation à distance, CWM recrée automatiquement la tâche de programmation et l'envoie de nouveau sur la clé. Ceci permet au possesseur de clé d'exécuter de nouveau la tâche de programmation.

CWM notifie également l'administrateur, via e-mail, avec les informations sur la clé utilisée, le cylindre concerné et la raison de l'échec de programmation. Cette fonction est toujours activée et ne peut pas être désactivée.

Lorsqu'un cylindre est reprogrammé, le contenu de sa mémoire est effacé, y compris les journaux des événements. La liste d'accès de cylindre est ensuite restaurée dans le cadre de la reprogrammation. Ce fonctionnement diffère de la programmation normale de cylindre, dans laquelle la liste d'accès de cylindre est uniquement mise à jour et le journal des événements reste inchangé.

Pour réaliser la tâche de reprogrammation de cylindre, il faut disposer d'une clé de programmation maîtresse ou d'une clé normale avec des droits de reprogrammation des cylindres.

Voir également *Chapitre 4.4.12 "Demande d'une reprogrammation de cylindre", page 62*.

8.6 Journaux des événements

Les cylindres, tout comme les clés, disposent d'une fonction journal des événements. Le journal des événements est la liste des événements impliquant des clés demandant l'accès à un cylindre ainsi que des programmations de clé et de cylindre. Il existe deux types de journaux des événements :

- Les **journaux des événements normaux** contiennent les événements dont les dispositifs concernés appartiennent au même système de fermeture.
- Les **journaux des événements étrangers** contiennent les événements dont les appareils impliqués appartiennent à des systèmes de fermeture différents.

Journaux des événements de clé
Seules les clés standard et les clés dynamiques peuvent stocker les journaux des événements.

Le journal des événements de la clé enregistre les cylindres dont la clé essaie d'accéder, le possesseur de clé au moment de l'action (s'il n'est pas supprimé de manière permanente ou désactivé) et les tâches de programmation qui ont été effectués sur la clé. Il enregistre également l'heure et le résultat de ces événements.

Journaux des événements de cylindre
Le journal des événements du cylindre enregistre les clés ayant effectué une tentative d'accès au cylindre, le possesseur de clé au moment de l'action (s'il n'est pas supprimé de manière permanente) et les tâches de programmation qui ont été effectuées sur la clé. Il enregistre également l'heure et le résultat de ces événements. Notez que le journal des événements n'enregistre pas les tentatives d'accès au cylindre par une clé mécanique.

Récupération automatique du journal des événements
Si une clé utilisateur appartient à un système distant, prend en charge les mises à jour à distance, est une clé standard ou dynamique et que les autorisations de journal des événements sont désactivées, la remise de cette clé utilisateur déclenche la création d'une tâche de journal des événements permettant une lecture à distance.

Une clé de programmation peut être programmée pour extraire automatiquement les journaux des événements des cylindres. Cette fonction permet au possesseur de clé d'extraire facilement et rapidement les journaux des événements des cylindres arbitraires dans le domaine. Voir également *Chapitre 6.11.13 "Activer ou désactiver la récupération automatique du journal des événements de la clé de programmation", page 144*.

Suppression automatique de l'archive de journal des événements
L'archive de journaux des événements peut être configurée pour supprimer automatiquement les journaux des événements à partir d'un nombre de jours défini. Ce processus de suppression est basé sur la date de création (date à laquelle l'entrée a été générée sur l'élément physique) plutôt que sur la date d'analyse (date à laquelle l'entrée a été stockée dans la base de données CWM).

Si la licence de l'**Journal des événements étendu et archive des événements** n'est pas reconnue, la période de suppression automatique peut être fixée au maximum à 366 jours.

Si la licence de l'**Journal des événements étendu et archive des événements** est reconnue, la période de suppression automatique peut être fixée au maximum sur 3660 jours.

Approbations
Dans les systèmes de fermeture où la fonction **Approbations** est activée, toutes les demandes de journal des événements de clé et de cylindre doivent être approuvées par un administrateur disposant du rôle d'**Approbateur**. Une fois le journal des événements lu depuis une clé ou un cylindre, il peut être affiché par n'importe quel administrateur disposant de la permission d'affichage des **journaux des événements**. Voir également *Chapitre 8.8 "Rôles et autorisations CWM", page 191*.

La fonction est activée ou désactivée dans **Réglages du système**. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100*.

8.7 Événements

Les opérations effectuées par l'administrateur sur les composants CWM suivants sont stockées sous forme d'événements et accessibles sur l'onglet **Événements** de chaque composant.

- **Employé ou visiteur**

  Pour afficher les événements concernant les employés ou les visiteurs, voir *Chapitre 4.1.10 "Visualisation des événements d'un employé ou d'un visiteur", page 33*.

- **Clé**

  Pour consulter les événements clés, voir *Chapitre 4.2.8 "Affichage des événements d'une clé utilisateur", page 39*.

- **Cylindre**

  Pour afficher les événements de cylindre, voir *Chapitre 4.4.7 "Affichage des événements d'un cylindre", page 59*.

- **Groupe de cylindres**

  Pour afficher les événements de groupe, voir *Chapitre 4.5.5 "Affichage des événements d'un groupe de cylindres", page 68*.

- **Profil d'accès** : tel qu'ajout et retrait de cylindres dans un profil d'accès.

Pour afficher les événements du profil d'accès, voir *Chapitre 4.6.7 "Affichage des événements d'un profil d'accès", page 72*.

- **Groupe d'accès temporaire**

  Pour afficher les événements du profil d'accès, voir *Chapitre 4.7.6 "Affichage des événements d'un groupe d'accès temporaire", page 76*.

- **Boîtier de programmation à distance**.

  Pour afficher les événements du boîtier de programmation à distance, voir *Chapitre 6.5.9 "Affichage de l'historique de boîtier de programmation à distance", page 123*.

- **Clé de programmation**

  Pour afficher les événements de clé de programmation, voir *Chapitre 6.11.6 "Affichage des événements de clé de programmation", page 138*.

Suppression automatique de l'archive des événements
L'archive des événements peut être configurée pour supprimer automatiquement les journaux des événements à partir d'un nombre de jours défini.

Si la licence de l'**Journal des événements étendu et archive des événements** n'est pas reconnue, la période de suppression automatique peut être fixée au maximum à 366 jours.

Si la licence de l'**Journal des événements étendu et archive des événements** est reconnue, la période de suppression automatique peut être fixée au maximum sur 3660 jours.

REMARQUE !
Les événements suivants ne sont pas supprimés automatiquement et restent dans l'historique même après la fin de la période de conservation :

- Activation de clé, cylindre et boîtier de programmation à distance
- Le dernier événement de remise de clé dans les événements Employé ou Visiteur et les événements de Clé.

8.8 Rôles et autorisations CWM

Les rôles sont définis par la combinaison des permissions données et attribuées aux clés de programmation.

Chaque permission donne aux rôles des niveaux de droit différents pour réaliser une fonction CWM précise.

Rôles
Les fonctions visibles dans CWM dépendent du rôle attribué à la clé de programmation utilisée par l'administrateur connecté. Il est fortement conseillé que les administrateurs n'aient accès qu'aux seules fonctions dont ils ont besoin dans leur travail. Exemple : un administrateur effectuant uniquement des tâches de programmation de cylindre ne devrait avoir accès qu'à cette seule fonction. Un administrateur responsable de la gestion des clés ne devrait avoir accès qu'aux opérations de remise/retour ou déclaration de clé perdue ou défectueuse.

REMARQUE !
Les rôles définis pour les administrateurs travaillant avec CWM ne doivent pas être confondus avec les rôles définis par les profils d'accès.

Les rôles prédéfinis dans CWM sont les suivants :

Tableau 2. Rôles prédéfinis

Rôle	Description
Super administrateur	Toutes les permissions sauf celle d'approbation des demandes de journaux des événements.
Administrateur	Autorisations pour les principales tâches, telles que la configuration d'autorisation, la modification de modèles, etc.
Réceptionniste	Autorisations nécessaires pour les tâches quotidiennes plus simples, telles que la remise ou le retour de clé.
Approbateur	Autorisations pour approuver uniquement les demandes de journal des événements.
Programmateur de cylindre	Autorisations pour exécuter uniquement la programmation de cylindre.
WebService	Utilisé pour l'intégration de services Web.

Les rôles de super administrateur et d'approbateur ne peuvent être ni supprimés ni modifiés. Le rôle WebService peut être modifié mais pas supprimé.

Plusieurs rôles peuvent être attribués à une clé de programmation, mais il est impossible de combiner le rôle Approbateur avec d'autres rôles. Pour plus d'informations sur la façon d'attribuer des rôles, voir *Chapitre 6.11.4 "Modification des informations de clé de programmation", page 137*.

REMARQUE !
Certains droits pour les clés de programmation dépendent du type de clé et ne sont pas configurables par des rôles ou des autorisations. Voir *Chapitre 7.2.4 "Clés de programmation", page 160*.

Par défaut, les rôles décrits ci-dessus se trouvent dans une structure plane. Les administrateurs peuvent créer ou modifier des rôles avec des permissions supérieures à celles qu'ils ont reçues et ils peuvent attribuer et annuler l'attribution de ces rôles sur une clé de programmation.

Lorsque la fonction des administrateurs hiérarchiques est activée, la hiérarchie des rôles est formée et les restrictions suivantes s'appliquent :

- L'administrateur ne peut pas accorder de niveau de permission supérieur au sien.
- L'administrateur ne peut pas attribuer ou supprimer de rôle avec un niveau de permission supérieur au sien.

Le rang des rôles dans la hiérarchie est déterminé par le niveau de permission. Si un rôle reçoit un niveau de permission supérieur à celui qu'a reçu l'administrateur, le rôle est supposé être un rôle supérieur à celui de l'administrateur et ne peut donc pas être modifié ou supprimé par l'administrateur.

La fonction des administrateurs hiérarchiques peut être activée par le Super administrateur depuis la page **Réglages du système**.

Autorisations
Pour chaque rôle, les autorisations sont données par fonction CWM spécifique, telles que la gestion de clés, de cylindres, d'employés, de réglages système, de clés de programmation, etc.

Les permissions à une fonction CWM sont définies à l'un des niveaux suivants :

Tableau 3. Niveaux de permission

Niveau	Description
Aucun	N'autorise aucun accès.
Liste	Autorise la recherche et le listing.
Vue	Autorise également la visualisation des détails.
Complet	Autorise également la modification d'informations.

Pour la liste complète des autorisations et des opérations autorisées à chaque niveau, voir *Chapitre 9.4 "Autorisations", page 205*.

Voir également *Chapitre 6.7 "Gestion des rôles et des autorisations", page 129*.

8.9 Suppression des données personnelles et conformité RGPD

CWM peut être réglé pour traiter les employés et visiteurs supprimés de deux manières différentes : **Supprimer de manière permanente** ou **Marquer comme supprimé**. Le comportement est contrôlé via le réglage système **Lors de la suppression de personnes**.

Supprimer de manière permanente
Pour prendre en charge le RGPD, le réglage Suppression des données personnelles doit être défini sur **Supprimer de manière permanente**. Lorsque le réglage est défini ainsi, la situation suivante s'applique :

- Lorsque vous supprimez une personne, les données correspondantes sont supprimées de la base de données de manière permanente et ne peuvent pas être restaurées. Les références à une personne supprimée dans les journaux des événements sont remplacées de manière permanente par la mention **N/A**.
- Outre l'option **Supprimer**, il existe une fonction permettant de **Désactiver** une personne. La désactivation signifie que toutes les données personnelles sont masquées et ne peuvent être traitées d'aucune manière tant que la personne est désactivée. Les références à une personne désactivée dans les journaux des événements sont remplacées de manière temporaire par la mention **N/A**. Ces références sont restaurées si la personne est réactivée. Seuls les administrateurs dotés de la permission **Désactiver le possesseur de la clé** peuvent désactiver des personnes ainsi qu'afficher et réactiver des personnes désactivées.
- Les informations relatives aux personnes désactivées ne peuvent pas être modifiées, supprimées, exportées ou traitées de toute autre manière.
- Lors de l'importation d'employés depuis un fichier, les employés désactivés dans CWM sont ignorés même si leurs données sont modifiées dans le fichier CSV.

Voir également *Chapitre 4.1.3 "Désactivation ou activation des employés ou des visiteurs", page 26*.

Marquer comme supprimé
Le réglage Suppression des données personnelles défini sur **Marqué comme supprimé** ne respecte pas le RGPD.

Les personnes supprimées ne sont pas retirées de la base de données et les références à une personne supprimée peuvent toujours être présentes, notamment dans les journaux des événements. Les personnes supprimées peuvent être restaurées comme indiqué dans la *Chapitre 4.1.4 "Suppression ou restauration des employés ou des visiteurs", page 27*. Dans CWM, une personne non marquée comme à supprimer est décrite comme **Actif** (à ne pas confondre avec les personnes désactivées ou activées lorsque le réglage système est défini sur **Supprimer de manière permanente**).

8.10 Authentification unique (SSO)

L'authentification unique (SSO) permet aux administrateurs d'accéder au système sans sa clé de programmation.

La fonction SSO doit être configurée individuellement dans chaque système. Lorsque la fonction SSO est prise en charge, le Super Administrateur peut l'activer ou la désactiver selon les besoins. Pour des informations plus détaillées, consultez *"CONNEXION UNIQUE (SSO)"* dans *Chapitre 6.4 "Modifier les réglages du système", page 100*.

Lorsqu'elle est activée, un administrateur qui a reçu une nouvelle clé de programmation doit d'abord enregistrer un certificat à l'aide du CCPC et de la clé de programmation. Une fois le certificat enregistré, l'administrateur peut se connecter au système sans la clé de programmation.

Toutefois, pour certaines opérations, telles que les tâches de programmation nécessitant des données sécurisées stockées sur la clé de programmation, l'administrateur doit malgré tout se connecter à l'aide de la clé de programmation. Dans ce cas, un message invite l'utilisateur à insérer la clé de programmation et à s'authentifier en conséquence.

Les fonctions suivantes nécessitent une connexion avec clé de programmation :

- Programmation du cylindre local : envoi de tâches vers la clé de programmation, mise à jour de son statut et suppression de tâches terminées ou non.
- Copier configuration de clé
- Activer importation d'extension
- Activer ou désactiver la récupération automatique de journaux des événements sur la clé de programmation.
- Déverrouiller la clé de programmation.
- Changer le code PIN de la clé de programmation
- Actualiser le statut de la clé utilisateur insérée dans le boîtier de programmation local via la barre supérieure de la page.

8.11 Intégration DCS

DCS est une application serveur de gestion des certificats et des licences dans le système de fermeture CLIQ.

L'**intégration DCS** permet la génération automatique de certificats pour les clés de programmation et les boîtiers de programmation à distance et évite par conséquent d'avoir à distribuer ces certificats séparément. Elle permet également de récupérer les fichiers de licence, les fichiers de microprogramme et les fichiers d'extension à partir de DCS.

L'intégration DCS doit être activée lors de l'installation du système.

Avec l'intégration de DCS, les certificats de boîtier de programmation à distance sont générés depuis CWM, tandis que les certificats de clé de programmation sont générés via **CLIQ Connect PC**.

L'enregistrement des certificats des clés de programmation peut être **Toujours autorisé** (recommandé), **Autorisé une fois** ou **Non autorisé**. Pour les clés de programmation maîtresse, ces réglages sont faits dans le DCS et pour les clés normales dans CWM (voir *Chapitre 6.11.4 "Modification des informations de clé de programmation", page 137*).

Tableau 4. Réglages de l'enregistrement du certificat

Réglages	Description
Toujours autorisé	Le certificat de clé de programmation peut être enregistré plusieurs fois. C'est utile lorsque le possesseur de la clé doit accéder à CWM à partir de plusieurs ordinateurs.
Autorisé une fois	Le certificat de clé de programmation peut être enregistré une seule fois.
Non autorisé	L'enregistrement n'est pas autorisé.

REMARQUE !
Le renouvellement de certificats est autorisé indépendamment de ce réglage.

Pour générer des certificats de clé de programmation, voir *Chapitre 3.2.1 "Enregistrement du certificat de la clé de programmation via CLIQ Connect PC", page 17*.

Pour générer des certificats de bornes d'actualisation, voir *Chapitre 6.5.7 "Configuration de boîtiers de programmation muraux", page 110* ou *Chapitre 6.5.8 "Configuration des boîtiers de programmation mobiles", page 117*.

Pour récupérer une licence depuis DCS, voir *Chapitre 6.1.1 "Installation des licences", page 99*.

Pour récupérer un fichier d'extension depuis DCS, voir *Chapitre 6.16 "Importation d'extensions", page 155*.

8.12 Intégration LDAP

LDAP signifie Lightweight Directory Access Protocol, protocole logiciel qui permet d'accéder aux services de répertoire. Dans le contexte de CWM, le LDAP est utilisé comme source principale des informations employé par intégration avec CWM. CWM prend en charge OpenLDAP, Microsoft Active Directory et Apache Directory.

Lorsque le LDAP est intégré, les employés ajoutés dans un répertoire actif précis sont automatiquement (une fois par 24 heures) ou manuellement synchronisés avec CWM. Dans CWM, les employés provenant du LDAP coexistent avec les employés dans CWM et leurs prénoms, noms de famille, adresses e-mail et numéros de téléphone portable sont visibles et utilisables dans les recherches.

Si la fonction CLIQ Connect+ est activée et si l'employé est un utilisateur CLIQ Connect+ activé, il n'est pas possible de désactiver ou de supprimer cet employé ou de supprimer son adresse e-mail. Pour davantage d'informations sur la fonction CLIQ Connect+, voir *Chapitre 8.3.4 "CLIQ Connect et CLIQ Connect+", page 186*.

Puisque les informations du LDAP sont en lecture seule, certaines restrictions s'appliquent quant à la gestion de l'employé dans CWM lorsque l'intégration LDAP est activée. *Tableau 34 "Activités disponibles dans CWM lorsque le LDAP est intégré", page 196* indique quels administrateurs peuvent le gérer.

Tableau 5. Activités disponibles dans CWM lorsque le LDAP est intégré

	Employé	
	LDAP intégré	**non intégré à LDAP**
Ajouter	n/a	✓
Modifier	✓* * Seuls les éléments **Domaine** et **NOTES** peuvent être modifiés depuis le GUI.	✓
Supprimer/Désactiver	n/a	✓

L'intégration LDAP est activée ou désactivée depuis la page **Réglages du système**. Voir *Chapitre 6.4 "Modifier les réglages du système", page 100* pour configurer l'intégration LDAP. Les prérequis pour l'intégration LDAP sont que la licence et l'autorisation soient accordées aux administrateurs. Voir *Chapitre 6.1 "Gestion des licences", page 99* pour installer la licence et *Chapitre 6.7 "Gestion des rôles et des autorisations", page 129* pour accorder l'autorisation.

8.13 Obtention d'une licence

Une licence est nécessaire pour utiliser CWM. Les licences sont délivrées par le revendeur CLIQ local, pour chaque système de fermeture.

Une licence valide donne toujours accès aux fonctions de base dans CWM. Les fonctions suivantes sont disponibles en fonction du type de licence :

- À distance
- Domaines
- Profils d'accès
- Groupes d'accès temporaires
- Revalidation
- Revalidation flexible
- Groupes de cylindres
- Services Web
- Validation par code PIN
- Intégration LDAP
- Journal des événements étendu et archive des événements
- CLIQ Connect+

Pour afficher les fonctions accessibles grâce à la licence, voir *Chapitre 6.1.2 "Affichage du statut de la licence", page 99*.

Pour les systèmes avec la fonction **Intégration DCS** activée, CWM vérifie automatiquement les licences disponibles dans DCS au démarrage et toutes les 24 heures. S'il n'y a pas de licence disponible dans DCS ou si l'intégration DCS n'est pas activée, les licences doivent être installées manuellement. Voir *Chapitre 6.1.1 "Installation des licences", page 99*.

Un numéro de licence est attribué aux fichiers de licence lorsqu'ils sont créés. Il est seulement possible d'installer un fichier de licence créé après le fichier déjà installé.

Expiration de la licence et notification par e-mail

Une licence a une **Date d'expiration souple** et une **Date d'expiration fixe**.

Après la date d'expiration souple, des e-mails de notification sont adressés au **Super Administrateur** tous les lundis jusqu'au renouvellement de la licence. Par exemple, si la date d'expiration est un mardi, le premier e-mail est envoyé le lundi suivant. Pour recevoir les e-mails, les administrateurs doivent disposer d'une adresse e-mail enregistrée. Un message d'avertissement est également affiché sur l'interface utilisateur de CWM. Contactez votre revendeur CLIQ pour obtenir une nouvelle licence.

Si la date d'expiration fixe est dépassée, l'utilisation de CWM est bloquée au démarrage. Un message d'avertissement s'affiche sur la page d'accueil et un e-mail est envoyé pour signaler l'expiration de la licence. Contactez votre revendeur CLIQ pour obtenir une nouvelle licence.

Pour plus d'informations sur la façon d'installer les licences, voir *Chapitre 6.1.1 "Installation des licences", page 99*.

Lorsque les licences sont contrôlées par un logiciel externe (et non par DCS), le renouvellement de la licence est généralement effectué à la date d'expiration souple. Dans ce cas, aucun e-mail de notification n'est envoyé.

9 Annexe

9.1 Termes et abréviations

9.1.1 Termes

État effectif	Décrit l'état des autorisations de clé effectivement programmées sur les clés et les cylindres. Voir également **État défini**.
Liste d'accès de cylindre	Liste des clés autorisées, enregistrée dans les cylindres.
Système à groupes de cylindres	Système de fermeture prédéfini pour prendre en charge les groupes de cylindres.
Tâche de programmation de cylindre	Traitement de mise à jour de cylindre pouvant être exécutée sur le cylindre en utilisant une clé de programmation.
Reprogrammation de cylindre	Cette opération efface la mémoire d'un cylindre, puis, à partir de la base de données, restaure la liste d'accès au cylindre, la liste des clés interdites et d'autres configurations, telles que le fuseau horaire.
Intégration DCS	Une fonction de CWM qui permet la génération automatique de certificat pour les clés de programmation et les boîtiers de programmation à distance.
État défini	Décrit l'état des autorisations de clé comme défini dans CWM. Il n'est pas nécessairement identique à l'état effectif, étant donné que certaines autorisations peuvent ne pas avoir été encore programmées sur les clés et les cylindres. Voir également **État effectif**.
Élément	Les clés et cylindres CLIQ constituent les éléments CLIQ.
Accès explicite	Entrée dans la liste d'accès de clé dynamique, ajoutée explicitement pour cette clé. Voir également **Accès implicite**.
Extension	Un complément au système de verrouillage contenant de nouvelles clés, de nouveaux groupes de clés, cylindres, groupes de cylindres et boîtiers de programmation à distance.
Accès implicite	Entrée de la liste d'accès de clé dynamique ajoutée par l'intermédiaire des profils d'accès associés à une personne ou directement à une clé. Voir également **Accès explicite**.
Liste d'accès de clé	Liste des cylindres autorisés, enregistrée dans les clés dynamiques.
Liste des clés interdites	Liste des clés dont l'accès à un cylindre a été bloqué après avoir été déclarées perdues.
Système de verrouillage	Système de cylindres et de clés administrées de manière conjointe. Dans ce guide, le terme est également associé aux boîtiers de programmation et aux informations associées définies dans CWM (tels que les autorisations électroniques, les données employé et

	visiteur, les définitions de rôle administrateur, les réglages système, etc.).
Objet	Entités pouvant être administrées dans CWM, telles que les clés, groupes de clés, cylindres, groupes de cylindres, profils d'accès, bornes d'actualisation, employés et visiteurs.
Système à distance	Système de fermeture avec fonction à distance activée.
Traitement de mise à jour à distance	Traitement contenant des mises à jour de clé pouvant être exécutées sur la clé en l'insérant dans un boîtier de programmation à distance.
USB On-The-Go (OTG)	Norme USB permettant aux périphériques USB d'agir comme un hôte.

9.1.2 Abréviations

CSV	Format de fichiers où les valeurs sont séparées par des virgules
CWM	CLIQ Web Manager
DCS	Digital Content Server
RGPD	Règlement général sur la protection des données (règlement de l'UE concernant le traitement des données personnelles)
Boîtier de programmation	Boîtier de programmation
USB OTG	USB On-The-Go (OTG)

9.2 Symboles CWM

Clés utilisateur


Clé mécanique


Clé normale


Clé standard


Clé standard CLIQ Connect


Clé dynamique


Clé dynamique CLIQ Connect


Groupe de clé normale


Groupe de clé dynamique


Une mise à jour à distance en attente existe pour la clé


Il existe une mise à jour en attente qui dépasse la capacité de la clé

Clés de programmation

 Clé de programmation maîtresse

 Clé de programmation normale

 Clé de programmation normale CLIQ Connect

 Groupe de clé de programmation normale

 Groupe de clé de programmation maîtresse

 La tâche de programmation n'a pas été envoyée vers une clé de programmation

 La tâche de programmation a été envoyée à une clé de programmation mais n'a pas encore été lancée

 Seules certaines tâches de programmation ont été envoyées à une clé de programmation

 La tâche de programmation est terminée

 La tâche de programmation a échoué ou a été annulée

 La tâche de programmation a été remplacée par une nouvelle tâche

Cylindres

 Cylindre électronique

 Cylindre mécanique

 Double cylindre (notre exemple : Entrée A électronique et entrée B mécanique)

 Les informations concernent l'entrée A.

 Les informations concernent l'entrée B.

 La tâche de programmation de cylindre existe

 La tâche de programmation de cylindre doit être approuvée

 La tâche de programmation de cylindre a été programmée pour la clé de programmation

 La tâche de programmation de cylindre est terminée

 La tâche de programmation de cylindre a échoué ou a été annulée

 La tâche de programmation de cylindre a été remplacée par une nouvelle tâche

Autorisations

 Autorisation explicite

 Autorisation à partir du profil d'accès

Boîtiers de programmation à distance

 Borne de rechargement de droits

 Boîtier de programmation mobile CLIQ

9.3 Attributs d'objet

9.3.1 Attributs Employé

Identifiant	Un code ou un identifiant unique utilisé pour distinguer cette personne des autres dans un système.
Titre	Préfixe de courtoisie utilisé devant le nom, tel que M., Mme, Dr.
Prénom	Le prénom de la personne.
Nom	Le nom de famille de la personne.
Domaine	Le domaine auquel la personne appartient.
Organisation	L'entreprise ou l'institution à laquelle la personne est affiliée.
Téléphone	Le numéro de téléphone de la personne.
Département	La division ou l'unité spécifique au sein de l'entreprise dans laquelle la personne travaille.
Fonction	Le titre du poste ou le rôle de la personne au sein de l'organisation.
Adresse e-mail	L'adresse e-mail de la personne.
Région	La zone géographique plus large dans laquelle la personne est située (par exemple, EMEA, APAC).
Langue	La langue principale de la personne.
Zone	Description générale de l'endroit où la personne est basée (peut se chevaucher avec **Ville** ou **État/Région**).
Texte Gmd	
Rue et numéro	La rue où se trouve l'organisation ou la personne.
Code postal	Le code postal de la ville.
Ville	La ville où la personne ou l'organisation est située.
État	État, province ou région d'un pays.
Adresse de l'entreprise	L'adresse complète de l'organisation ou du lieu de travail de la personne.

9.3.2 Attributs Visiteur

Identifiant	Un code ou un identifiant unique utilisé pour distinguer cette personne des autres dans un système.
Titre	Préfixe de courtoisie utilisé devant le nom, tel que M., Mme, Dr.
Prénom	Le prénom de la personne.
Nom	Le nom de famille de la personne.

Domaine	Le domaine auquel la personne appartient.
Organisation	L'entreprise ou l'institution à laquelle la personne est affiliée.
Téléphone	Le numéro de téléphone de la personne.
Département	La division ou l'unité spécifique au sein de l'entreprise dans laquelle la personne travaille.
Fonction	Le titre du poste ou le rôle de la personne au sein de l'organisation.
Adresse e-mail	L'adresse e-mail de la personne.
Région	La zone géographique plus large dans laquelle la personne est située (par exemple, EMEA, APAC).
Langue	La langue principale de la personne.
Zone	Description générale de l'endroit où la personne est basée (peut se chevaucher avec **Ville** ou **État/Région**).
Rue et numéro	La rue où se trouve l'organisation ou la personne.
Code postal	Le code postal de la ville.
Ville	La ville où la personne ou l'organisation est située.
État	État, province ou région d'un pays.
Adresse de l'entreprise	L'adresse complète de l'organisation ou du lieu de travail de la personne.

9.3.3 Attributs de clé

Nom	Nom de la clé.
Possesseur de la clé	Personne à qui la clé est actuellement remise.
Marquage	Marquage de la clé.
Deuxième marquage	Marquage alternatif (pas toujours utilisé).
Profil de clé	Profil et taillage mécanique de la clé.
Groupe	Groupe de clés auquel appartient la clé.
Type	Type de la clé. Pour plus d'informations, voir *Chapitre 7.2.3 "Clés utilisateur", page 159*.
Microprogramme	Version de microprogramme.
Génération	La génération de clé.
Statut	Statut de la clé (**En stock**, **Remise**, **Perdue** ou **Défectueuse**).
Numéro de ligne	Non utilisée.

Dernière mise à jour à distance	Date et heure de la dernière mise à jour via un boîtier de programmation à distance.
Taille de la liste d'accès	Entrées utilisées / Nombre maximum d'entrées dans la liste d'accès de la clé.
Prise en charge fuseau horaire	Indique si la fonction de prise en charge des fuseaux horaires est active.
Notes	Notes définies pour la clé.
Liens externes	URL associées à la clé.

9.3.4 Attributs de la clé de programmation

Nom	Nom de la clé de programmation.
Possesseur de la clé	Employé à qui la clé de programmation est actuellement remise.
Marquage	Marquage de la clé de programmation.
Deuxième marquage	Marquage alternatif (pas toujours utilisé).
Groupe	Groupe de clés auquel appartient la clé de programmation.
Type	Type de clé de programmation. Pour plus d'informations, consultez *Chapitre 7.2.4 "Clés de programmation", page 160*.
Microprogramme	Version de microprogramme.
Génération	Génération de la clé de programmation.
Prise en charge à distance	
Reprogrammation de cylindre	Indique si la clé de programmation dispose des droits de reprogrammation de cylindre.
Programmation du groupe de cylindres	Indique si la clé de programmation peut exécuter les tâches de programmation de cylindre qui modifie le groupe auquel appartient un cylindre.
Mise à jour du microprogramme du cylindre	Indique si la clé de programmation peut ou non mettre à jour le microprogramme du cylindre (en cours de développement).
Statut	Statut de la clé de programmation (**En stock**, **Remise**, **Perdue** ou **Défectueuse**).
Bloquée	Indique si la clé de programmation est bloquée pour tous les accès.
Réglages de validité	Réglage de la validité de la clé de programmation.
Enregistrement du certificat	Indique si l'enregistrement du certificat est autorisé.
Rôles	Indique quels sont les rôles associés à la clé de programmation.

9.3.5 Attributs de cylindre

Nom	Nom du cylindre.
Marquage	Marquage du cylindre.
Statut	Statut du cylindre (**En stock**, **Installé** ou **Perdu**).
Zone	L'emplacement du cylindre.
Fuseau horaire de base	Fuseau horaire à l'emplacement du cylindre.
Modèle de cylindre	Modèle de cylindre.
Longueur	Longueur physique du cylindre. Pour les cylindres double entrée, la longueur est représentée par un chiffre pour chaque entrée. Pour les cylindres borgnes ou avec bouton, la longueur est représentée par un chiffre pour la longueur du cylindre et un autre chiffre pour la longueur du côté borgne/bouton.
Numéro de ligne	Non utilisée.
Bloqué par	Clé de programmation sur laquelle les tâches de programmation de cylindre en attente sont chargés. Lorsqu'un travail de programmation de cylindre est chargé dans une clé de programmation, les réglages de ce cylindre ne sont pas modifiables dans CWM.
Côté cylindre	**A** ou **B** (pour les cylindres double entrée).
Type	**E** (Électronique) ou **M** (Mécanique).
Groupe	Groupe de cylindres auquel appartient le cylindre.
Microprogramme	Version du microprogramme du cylindre.
Compensation du fuseau horaire	Fuseau horaire du cylindre, par rapport au fuseau horaire de base.
Domaine	Domaine auquel le cylindre appartient.
Notes	Notes définies pour le cylindre.
Liens externes	URL associées au cylindre.

9.3.6 Attributs de boîtier de programmation à distance

Nom	Nom du boîtier de programmation à distance.
Marquage	Marquage du boîtier de programmation à distance
Type	**Boîtier de programmation mobile** ou **Boîtier de programmation mural**.
Génération	Génération du boîtier de programmation mural

Adresse MAC	L'adresse physique du boîtier de programmation à distance.
GR	Identifiant de groupe (réservé à usage interne).
UID	Identifiant unique (réservé à usage interne).
Microprogramme	Version de microprogramme.
Chargeur d'amorçage (génération 1 uniquement)	Version du chargeur de démarrage du microprogramme.
Statut	Statut d'inventaire (**En stock**, **Installé**, **Remis** ou **Perdu**). Statut opérationnel (**Défectueux**).
Statut de connexion	**Hors ligne** ou **En ligne**.
Dernière connexion	Borne mobile : date et heure auxquelles la borne mobile était la dernière fois en ligne.
Dernière adresse IP connue	L'adresse IP à partir de laquelle le boîtier de programmation à distance était en ligne la dernière fois.
Notes	Notes définies pour le boîtier de programmation à distance.
Liens externes	URL associées au boîtier de programmation à distance.

9.4 Autorisations

Pour chaque permission, il est possible de sélectionner **Aucun**, **Liste**, **Vue** ou **Complet**. La **Vue** fournit automatiquement la **Liste** et **Complet** fournit automatiquement la **Vue** et la **Liste**.

S'il existe des dépendances entre les autorisations, elles sont énumérées dans la colonne **Dépendances**. Exemple : pour accorder la permission d'autorisations de clé, la permission de vue des clés ainsi que la permission de liste de cylindres sont requises.

Permission	Aucune	Liste Les éléments sont listés.	Vue Les détails des éléments listés sont accessibles.	Complet Les détails des éléments listés sont accessibles et peuvent être manipulés.	Dépendances
Profils d'accès Contrôle l'administration des profils d'accès (création, suppression, modification).		⊗	Peut afficher les détails de profils d'accès.	Peut créer de nouveaux profils d'accès et modifier des profils existants, à l'exception de la liste d'accès qui est contrôlée par le droit d'autorisation de profil d'accès.	
Profil d'accès : Autorisation Contrôle le réglage des autorisations de profil d'accès.		⊗	Peut voir les autorisations de profil d'accès.	Peut ajouter ou supprimer des autorisations aux profils d'accès.	Nécessite une permission d'affichage pour **Profil d'accès**.
Approbations		Option de menu **Travaux d'approbation** disponible. Peut afficher la liste des demandes d'approbation de journal des événements.	⊗	Peut approuver les demandes de journal des événements. Rôle Approbateur uniquement et ne peut pas être modifié.	Uniquement applicable si le réglage d'approbation est activé pendant l'installation initiale.
Journal des événements			L'onglet de journal des événements est visible dans la fenêtre clé et cylindre.	Peut demander les journaux des événements de cylindres et de clés via l'onglet Journal des événements.	
Journal des événements : Automatique		⊗	Permission pour afficher le statut de récupération automatique des journaux des événements pour les clés de programmation.	Permission pour afficher le statut de récupération automatique des journaux des événements pour les clés de programmation.	Nécessite au minimum une permission d'affichage pour **Clé de programmation**.

Permission	Aucune	Liste Les éléments sont listés.	Vue Les détails des éléments listés sont accessibles.	Complet Les détails des éléments listés sont accessibles et peuvent être manipulés.	Dépendances
Clé de programmation	⊗	⊗	Peut afficher les détails de clé de programmation.	Peut modifier les détails de clé de programmation et remettre des clés de programmation.	
Clé de programmation : Retour/Remise		⊗	⊗	Peut retourner et remettre des clés de programmation.	Nécessite une permission de liste pour **Possesseur de la clé : Employé** et une permission d'affichage pour **Clé de programmation**.
Cylindre		Sélectionnable si **Cylindre : Autorisation** est Aucun.	Peut afficher les détails de cylindre.	Peut modifier les détails de cylindre et modifier le statut de cylindre.	
Cylindre : Autorisation			Peut afficher les autorisations de cylindre.	Peut modifier les autorisations de cylindre et demander la reprogrammation de cylindre.	Nécessite une permission d'affichage pour **Cylindre** et une permission de liste pour **Clé**.
Cylindre : Programmation		⊗	⊗	Peut envoyer des tâches de programmation aux clés de programmation.	Nécessite une permission de liste pour **Cylindre**.
Domaine (Aucune permission requise pour afficher les membres de domaine et les autorisations de domaine des clés de programmation)		⊗	⊗	Peut administrer les domaines (ajout, suppression, modification) et modifier les autorisations de domaine des clés de programmation.	

Permission	Aucune	Liste Les éléments sont listés.	Vue Les détails des éléments listés sont accessibles.	Complet Les détails des éléments listés sont accessibles et peuvent être manipulés.	Dépendances
Microprogramme		⊗	⊗	Peut importer le microprogramme.	La mise à niveau du microprogramme nécessite une permission complète pour **Boîtiers de programmation à distance**.
Revalidation flexible (Peut voir les intervalles de revalidation si la revalidation flexible est activée.)		⊗	⊗	Peut modifier les intervalles de revalidation de profil d'accès et de groupe de cylindres.	
Clé	Sélectionnable si **Cylindre : Autorisation** est Aucun.	Peut lister les clés de façon indirecte.	Option de menu **Clés** disponible. Peut afficher les détails de clé.	Peut modifier les détails, le statut inventaire et le statut opérationnel de clé.	
Clé : Autorisation		Sélectionnable si **Clé : Autorisation** est Aucun.	Peut afficher les autorisations de clé.	Peut modifier les autorisations de clé.	Nécessite une permission d'affichage pour **Clé** et une permission de liste pour **Cylindre**.
Clé : Retour/Remise		⊗	⊗	Options de menu **Retour d'une clé** et **Remise d'une clé** disponibles. Peut effectuer les remises et les retours.	Nécessite des permissions de liste pour **Possesseur de la clé : Employé**, **Possesseur de la clé : Visiteur**, **Clé** et **Cylindre** et des permissions complètes pour **Clé : Autorisation**.

Permission	Aucune	Liste Les éléments sont listés.	Vue Les détails des éléments listés sont accessibles.	Complet Les détails des éléments listés sont accessibles et peuvent être manipulés.	Dépendances
Clé : Planning	⊗	⊗		Peut modifier un planning pour une clé, configurer un planning groupé pour un groupe de clés et régler un planning tout en remettant la clé.	Nécessite une permission complète pour **Modèle : Appliquer un planning par modèle** et une permission d'affichage pour **Clé**.
Clé : Historique de mise à jour		⊗	Peut afficher l'historique de mise à jour de la clé sur l'onglet **Historique de mise à jour**.	⊗	Nécessite une permission d'affichage pour **Clé**.
Clé : Validité	⊗	⊗		Peut modifier les réglages de validité groupés pour les clés, modifier les réglages de validité de clé et régler la validité tout en remettant la clé.	Nécessite une permission d'affichage pour **Clé**.
Possesseur de la clé : Désactiver		⊗	⊗	Peut désactiver des personnes ainsi que rechercher et activer des personnes désactivées.	Nécessite une permission complète pour **Possesseur de la clé : Employé** et **Possesseur de la clé : Visiteur**.
Possesseur de la clé : Employé	⊗	⊗	⊗	Peut modifier les détails employé.	
Possesseur de la clé : Importation d'un employé		⊗	⊗	Peut importer les données d'employé.	Nécessite une permission complète pour **Possesseur de la clé : Employé**.
Possesseur de la clé : Visiteur	⊗	⊗	⊗	Peut modifier les détails visiteur.	

Permission	Aucune	Liste Les éléments sont listés.	Vue Les détails des éléments listés sont accessibles.	Complet Les détails des éléments listés sont accessibles et peuvent être manipulés.	Dépendances
Intégration LDAP		⊗	Peut afficher les réglages de **Intégration LDAP** dans la page des réglages du système.	Peut modifier les réglages de **Intégration LDAP** dans la page des réglages du système.	Nécessite une permission d'affichage pour **Réglages du système**.
Maintenance		⊗	⊗	Peut bloquer et débloquer le système.	
Boîtiers de programmation à distance		Peut lister les bornes d'actualisation de façon indirecte.	Option de menu **Boîtiers de programmation à distance** disponible. Peut afficher le détail du boîtier de programmation à distance.	Peut modifier les réglages du boîtier de programmation à distance, mettre à niveau le microprogramme du boîtier de programmation à distance et commuter un boîtier de programmation mural en mode mise à jour de clé afin de l'utiliser pour la mise à niveau du microprogramme de clé.	
Rôles	⊗		Option de menu **Rôles** disponible. Peut afficher la liste des rôles et voir les détails d'un rôle.	Peut administrer les rôles (création, modification, suppression) et attribuer les rôles aux clés de programmation.	
Statistiques		⊗	Peut afficher les statistiques du système.	⊗	
Réglages du système	⊗	⊗			
Statut du système		⊗	Option de menu **Statut du système** disponible. Peut afficher le statut du système.	⊗	Nécessite une permission de liste pour **Boîtiers de programmation à distance**.

Permission	Aucune	Liste Les éléments sont listés.	Vue Les détails des éléments listés sont accessibles.	Complet Les détails des éléments listés sont accessibles et peuvent être manipulés.	Dépendances
Modèle : Appliquer un planning par modèle	⊗	⊗	⊗	Peut appliquer un modèle de planning pour une clé et appliquer un modèle de planning tout en remettant la clé.	Nécessite une permission d'affichage pour **Clé**.
Modèle : Reçu			Option de menu **Modèles de reçu** disponible. Peut imprimer les reçus et prévisualiser les modèles de reçu.	Peut créer, modifier et supprimer les modèles de reçus	
Modèle : Planning	⊗		Peut afficher les modèles de planning.	Peut modifier les modèles de planning.	
Groupe d'accès temporaire		⊗	Peut afficher les groupes d'accès temporaires.	Peut modifier les groupes d'accès temporaires.	

9.5 Indications du boîtier de programmation à distance

9.5.1 Indications de boîtier de programmation mural (génération 1) et de boîtier de programmation mobile

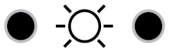
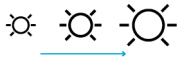
Indications lumineuses du voyant LED		Avertisseur sonore	Signification
Blanc continu			**Sous tension et en ligne**
Clignotement blanc rapide			**Boîtier de programmation mural : acquisition de l'adresse IP** **Borne mobile : initialisation de la connexion Bluetooth ou USB**
Clignotement blanc lent			**Connexion au serveur à distance au cours de la séquence de démarrage**
	Continu	1 bip long	**Mise à jour hors ligne terminée avec succès**
Rouge continu			**Niveau de batterie de borne mobile faible**

Indications lumineuses du voyant LED	Avertisseur sonore	Signification
 Rouge clignotant  Un clignotement		**Batterie de borne mobile déchargée**
 Continu		**Niveau de batterie de clé faible**
 Clignotant		**Connexion pendant la mise à jour à distance**
 Continu		**Connecté pendant la mise à jour à distance**
 Continu		**Mise à niveau de microprogramme terminée**
	1 bip	**Opération terminée avec succès** **Réglages du boîtier de programmation à distance mis à jour**
 Clignotant		**Téléchargement et traitement**
 Continu	1 bip	**E-mail envoyé**
 Continu	3 bips	**Opération terminée avec erreur**

Pour les opérations impliquant une clé, les bips sont répétés toutes les trois secondes jusqu'au retrait de la clé.

9.5.2 Indications de boîtier de programmation mural (génération 2)

Indications lumineuses du voyant LED	Avertisseur sonore	Signification
 Gauche : Clignotement bleu Centre : Éteint Droite : Éteint		**Vérification des réglages 802.1x**
 Gauche : Bleu fixe Centre : Clignotement bleu Droite : Éteint		**Acquisition de l'adresse IP**

Indications lumineuses du voyant LED		Avertisseur sonore	Signification
	Gauche : Bleu fixe Centre : Bleu fixe Droite : Clignotement bleu		**Établissement de la connexion serveur**
	Gauche : Éteint Centre : Blanc fixe Droite : Éteint		**Connecté et prêt à l'emploi**
	Gauche : Éteint Centre : Clignotement blanc Droite : Éteint		**Connexion perdue**
	Début de clignotement des LED en blanc depuis la gauche		**Mise à jour de clé en cours**
	Début de clignotement des LED en bleu depuis la gauche		**Mise à jour du microprogramme ou d'un paramètre en cours**
	Coche verte	2 bips qui augmentent	**Opération terminée avec succès**
	Croix rouge	2 bips qui baissent	**Opération terminée avec erreur pour les opérations**
	Batterie rouge		**Niveau de batterie de clé faible**

9.6 Indications de niveau de batterie

Le niveau de batterie de la clé actuellement scannée dans la fente de droite est indiqué par les symboles suivants.

Indication de niveau de batterie	Signification
	**Niveau de batterie excellent**
	**Niveau de batterie bon**

Indication de niveau de batterie	Signification
	**Niveau de batterie bas**
	**Niveau de batterie critique**

9.7 Fonctionnalité dépendante du microprogramme

Tableau 51 "Exigences pour le microprogramme", page 214 répertorie les fonctions CWM et indique la version de microprogramme la plus basse requise pour les boîtiers de programmation, les clés et les cylindres.

Tableau 6. Exigences pour le microprogramme

Fonctionnalité	**Microprogramme le plus ancien pris en charge**	
Récupération automatique du journal des événements	Clé et clé de programmation	12.7.0
Mise à niveau du microprogramme de la clé de programmation	Boîtier de programmation mural et boîtier de programmation mobile CLIQ	6.3
	Clé de programmation	12.0.0
Compatibilité des boîtiers de programmation mobiles CLIQ Connect	Clé	12.3
Support du groupe de cylindres	Clé	6.3.1
	Cylindre	5.3.1
Revalidation flexible	Clé	6.3.1
Mise à jour des informations du microprogramme de clé via le boîtier de mise à jour à distance	Clé	12.3
Mise à jour hors ligne	Clé	6.3.1
Validation du code PIN	Clé	16.0.0
Boîtier de programmation distant prêt à l'emploi	Boîtier de programmation mural et boîtier de programmation mobile CLIQ	6.2.1
Support Proxy boîtier de programmation distant	Boîtier de programmation mural et boîtier de programmation mobile CLIQ	6.2.1
Mise à jour de la clé de programmation à distance	Clé de programmation	12.0.0

Fonctionnalité	Microprogramme le plus ancien pris en charge	
Prise en charge à distance	Clé	3.0
	Clé de programmation	12.0.0
Revalidation	Clé	3.0
Type de planning - De base	Clé	Uniquement 1.x, 3.x, 5.x
Type de planning - Créneaux horaires multiples	Clé	2.x, 4.x, 6.x, 10 ou supérieure
Fuseau horaire	Clé, clé de programmation et cylindre	10.0.0
Mise à niveau du microprogramme de la clé utilisateur (génération 2)	Clé	10.1

Pour afficher la version de microprogramme d'une clé, affichez les informations détaillées. Voir *Chapitre 4.2.1 "Rechercher des clés utilisateur", page 34* ou *Chapitre 4.2.2 "Scanner une clé utilisateur", page 35*.

Pour afficher la version de microprogramme d'un boîtier de programmation mural, affichez les informations détaillées. Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

Pour afficher la version de microprogramme d'un boîtier de programmation mobile CLIQ, affichez les informations détaillées. Voir *Chapitre 6.5.2 "Recherche de bornes d'actualisation", page 106*.

9.8 PC client - Configuration requise

Produit	Condition requise
Système d'exploitation	• Windows 10 (64 bits) • Windows 11
Navigateur Internet	• Firefox version ESR 138 ou ultérieure • Firefox version 138 ou ultérieure • Google Chrome version 136 ou ultérieure • Microsoft Edge version 136 ou ultérieure * La prise en charge d'Internet Explorer est interrompue en raison de la fin de vie de ce navigateur.
Lecteur PDF	Tout lecteur PDF (Testé avec Adobe Reader)

9.9 Format du fichier d'importation d'employé

Pour pouvoir importer les données des employés, il est nécessaire de disposer d'un fichier avec les données et un format corrects.

Format de fichier
Le fichier est au format CSV (valeurs séparées par des virgules) et codage de caractères **Unicode UTF-8**.

Conseil
Pour s'assurer que le fichier CSV a le bon codage, le **bloc-notes Windows** peut être utilisé. Ouvrez le fichier CSV dans le bloc-notes, sélectionnez **Fichier » Enregistrer sous...**, puis le codage **UTF-8** et cliquez sur **Enregistrer**.

Taille du fichier
La taille maximale du fichier admissible pour l'importation sur CWM est de 7,0 Mo.

Contenu du fichier
Le délimiteur doit être soit la virgule (,), soit le point-virgule (;). Le réglage **délimiteur CSV** n'affecte pas l'importation.

La première ligne est un en-tête représentant tous les noms de champs séparés par des virgules (description des champs). L'en-tête est validé et dépend de la langue. Le texte dans l'en-tête doit correspondre à la langue définie.

Conseil
Cet en-tête peut être rempli en exportant les données Employés dans un fichier CSV puis en supprimant toutes les informations sauf la première ligne. Pendant cette exportation, un champ supplémentaire est ajouté aux autres : **Notes**. Ce champ peut être laissé tel quel, mais il sera ignoré pendant l'importation.

Voir *Chapitre 4.1.12 "Exportation des informations sur les Employés ou les Visiteurs", page 34*.

Chacune des lignes suivantes représente un employé. Les valeurs des champs sont séparées par les délimiteurs et l'ordre des champs doit correspondre à l'en-tête. Un champ doit comporter le caractère délimiteur (virgule ou point-virgule). L'ensemble des données d'un champ doit être placé entre guillemets ("), comme, par exemple, `"11 Wall St, New York, NY"`.

REMARQUE !
Le délimiteur doit toujours être présent, même si le champ est vide.

Les champs et les conditions à remplir sont décrits dans *Tableau 53 "Structure du fichier CSV", page 216*.

Tableau 7. Structure du fichier CSV

N° du champ	Nom	Obligatoire	Nombre de caractères
1	Identifiant		1-50
2	Titre		0-100
3	Prénom	✓	1-49
4	Nom de famille	✓	1-49
5	Domaine		0-100
6	Adresse e-mail		0-100
7	Téléphone		0-100
8	Organisation		0-100
9	Département		0-100

N° du champ	Nom	Obligatoire	Nombre de caractères
10	Rue et numéro		0-100
11	Code postal		0-100
12	Langue		0-100
13	Région		0-100
14	Fonction		0-100
15	Ville		0-100
16	État		0-100
17	Pays		0-100
18	Adresse de l'entreprise		0-100
19	Zone		0-100
20	Téléphone portable		0-100
21	Texte Gmd		0-100

L'**identifiant** doit être unique. Si, dans le fichier, des employés ont le même **identifiant** qu'un employé déjà enregistré dans le système, les informations contenues dans le système sont remplacées par celles du fichier. En revanche, si un employé est ajouté à CWM puis importé sans que son **identifiant** soit spécifié dans le fichier, les entrées correspondant à cet employé seront dupliquées.

REMARQUE !
Les employés mentionnés dans le fichier CSV avec le même identifiant qu'un employé désactivé dans CWM sont ignorés et ne sont donc pas importés.

L'**adresse e-mail** doit être spécifiée dans un format adéquat.

REMARQUE !
Il existe certaines limitations à la modification ou à la suppression de l'adresse e-mail d'un employé ou d'un visiteur dont le statut utilisateur CLIQ Connect+ est activé. Pour plus d'informations, consultez *Chapitre 4.1.6.1 "Informations importantes sur la modification ou la suppression d'adresses e-mail", page 30*.

Un fichier peut contenir au maximum 10 000 employés.

Exemple de fichier

```
Identifiant,Titre,Prénom Nom_de_famille,Domaine,Adresse
e-mail,Téléphone,Organisation,Département,Rue,Code
postal,Langue,Région,Fonction,État,Pays,Adresse de
la société,Lieu de travail,Numéro de téléphone mobile,GMD text

P0,Professor,George,Whitmore,Stockholm,George.Whitmore@assaablo
y.com,3719253729973267730,ASSA ABLOY,Shared Technologies,,,Swed
ish,,System Developer,Stockholm,,Sweden,"Formansvagen 11, 117 4
3 Stockholm",,070-6972135783866065282,GmdText
```

9.10 Code de la société d'exploitation ASSA ABLOY

Code	Société d'exploitation
0	Aucune société spécifiée
1	ASSA ABLOY Opening Solutions Suède (ASSA)
2	ABLOY
3	IKON
4	VACHETTE
6	MEDECO
7	SARGENT
8	ARROW
9	LAPERCHE
10	ASSA ABLOY Opening Solutions Norvège (TRIOVING)
11	ASSA ABLOY Opening Solutions Danemark (RUKO)
12	MUL-T-LOCK
13	ASSA États-Unis
14	ASSA Royaume-Uni
15	ASSA BALT
16	MEDECO CANADA
17	FAB
18	AA Japon
19	TESA
20	AA Nouvelle-Zélande
21	AA Australie
22	AA Singapour
23	AA Hong Kong
24	AA Chine
25	AA Inde
26	KESO
27	Corbin Russwin
28	ABLOY Royaume-Uni
29	ABLOY États-Unis

9.11 Informations sur l'assistance logicielle

9.11.1 Contacter l'assistance logicielle

En cas de problèmes avec CLIQ Web Manager ou un des dispositifs matériels, tels que les clés, les cylindres ou les boîtiers de programmation, n'hésitez pas à contacter votre revendeur CLIQ local. Quel que soit le service pour lequel vous nous contactez, veuillez vous munir du numéro de clé de programmation maîtresse et du numéro de la version de CWM utilisée. Si vous nous adressez un e-mail, indiquez toujours le numéro du système de clé maîtresse dans l'en-tête de l'e-mail.

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.

IKON
ASSA ABLOY

ASSA ABLOY Sicherheitstechnik GmbH

Attilastrasse 61-67
12105 Berlin
GERMANY
Tel. + 49 30 8106-0
Fax: + 49 30 8106-26 00
berlin@assaabloy.com

www.assaabloy.de

Sous réserve de modifications techniques. Program version: V 2025.1. Document number: PB00023 00017 0FR. Language: fr-FR. Published: 2025-05-22.