TIL TECHNOLOGIES

Une société du groupe vitaprotech

Paramétrage et utilisation du code intrusion CUBE global

Référence du document : GI-15025-FR

Date de publication : 04/03/2025

Paramétrage et utilisation du code intrusion CUBE global

Table des matières

Liste des illustrations

Liste des tableaux

Préface

1. Matériel nécessaire

Réseau de contrôle d'accès et de surveillance intrusion basé sur des *TILLYS* **TILLYS24-CUBE**.

Terminal mural constitué d'un *terminal intrusion TACTILLYS-IP CUBE* **CDA00TY2025-BBIP** équipé d'un *lecteur* **LEC05XF0200-NB6**.

2. Version logicielle

Ce guide décrit comment installer, configurer et mettre en service le code intrusion CUBE global pour la **version logicielle 2025.1.0** de MICROSESAME.

Firmware de la TILLYS CUBE **à partir de 7.2.0**.

Firmware du TACTILLYS-IP **à partir de 7.2.0**.

3. Contexte d'utilisation de ce manuel

Les pastilles de couleur jaune en haut de chaque page indiquent que ce document fournit des instructions d'installation de produits compatibles TIL TECHNOLOGIES.

Le partenaire ou installateur TIL TECHNOLOGIES configure la fonction code intrusion CUBE global sur MICROSESAME.

Le client gère les droits d'accès au TACTILLYS-IP CUBE et les personnes habilitées peuvent changer leur code d'accès aux TACTILLYS-IP.

4. Voir aussi

- *Vidéo de présentation de la détection intrusion CUBE*.
- *Fiche technique du terminal intrusion TACTILLYS-IP CUBE*.
- *Guide utilisateur intrusion et transmission CUBE*
- *Guide de démarrage rapide (GD-10001-FR)*.

5. Réserve de propriété

Les informations présentes dans ce document sont susceptibles d'être modifiées sans avertissement.

Les informations citées dans ce document à titre d'exemples, ne peuvent en aucun cas engager la responsabilité de TIL TECHNOLOGIES. Les sociétés, noms et données utilisés dans les exemples sont fictifs, sauf notification contraire.

Toutes les marques citées sont des marques déposées par leur propriétaire respectif.

Envoyez vos commentaires, corrections et suggestions concernant ce guide à *documentation@til-technologies.fr*

6. Glossaire

Les termes techniques utilisés dans ce guide sont expliqués ci-après.

Authentification	1. **D'une façon générale**, l'authentification consiste à saisir des identifiants (Login / Mot de passe) pour accéder à un équipement comme la *TILLYS*, à une application telle CHECKPOINT pour l'utilisation du terminal MOBILIS 3 par exemple, ou encore à tout ou partie d'un logiciel comme sur MICROSESAME ou KSM. 2. Dans le paramétrage de l'**encodage de MICROSESAME**, l'authentification est une opération qui consiste à vérifier que l'utilisateur est bien légitime à effectuer une ou plusieurs actions sur le badge (accéder à une ou plusieurs informations, écrire des données, créer ou supprimer des applications ou des fichiers ...). 3. Dans le contexte de l'intrusion, l'authentification permet à un identifié de débloquer et de visualiser les fonctions intrusion correspondant à ses droits d'accès. Selon le paramétrage retenu, cette authentification met en œuvre un identifiant et/ou un code intrusion personnalisé.
Client léger	Ordinateur sur lequel l'exploitation de la solution MICROSESAME est effectuée sans aucune installation préalable, au travers de son application WEBSESAME, affichée à l'aide d'un simple navigateur internet.
Code intrusion CUBE global	Code constitué uniquement de chiffres. Ce code est unique par identifié à l'échelle d'une installation. Il permet d'accéder aux fonctions de gestion de l'intrusion sur les claviers TACTILLYS-IP CUBE. Les codes intrusion CUBE globaux sont stockés de façon sécurisée. Leur première attribution est effectuée dans MICROSESAME. Ils peuvent ensuite être modifiés dans MICROSESAME, WEBSESAME ou par l'identifié sur un TACTILLYS-IP CUBE connecté à l'installation.
Fiche identifié	Ensemble complet d'informations relatives à une personne, qui incluent notamment son nom, prénom, service, une durée de validité, ses accès, ses entités, ses identifiants, son activité, son

	niveau opérationnel pour l'accès et son niveau d'habilitation au niveau de la gestion de l'intrusion.
Gestion d'accès	Ensemble de règles définissant la manière dont les personnes peuvent accéder à un lieu protégé, en fonction de leurs autorisations et de l'heure à laquelle elles présentent leur identifiant. Un logiciel dédié à cette fonction permet de créer, modifier et supprimer les règles d'accès pour chaque utilisateur.
GTB	Acronyme de Gestion Technique des Bâtiments. Système de pilotage, de contrôle, de supervision et d'optimisation des divers services comme l'éclairage, le chauffage ou la ventilation, présents dans les bâtiments tertiaires et industriels (immotique).
Intrusion	Changement d'état d'un détecteur qui déclenche une alarme lorsqu'une installation est en surveillance anti-intrusion.
IP	Acronyme anglais d'Internet Protocol. Le protocole Internet permet aux équipements qui l'utilisent de communiquer entre eux par paquets, de type *TCP* ou *UDP*. Le protocole IP est transporté par des réseaux locaux filaires utilisant le protocole de connexion Ethernet. Les cartes ou interfaces réseau équipées de connecteurs de type *RJ45* y ont accès physiquement et y sont identifiées logiquement via leur adresse IP.
Lecteur	Équipement utilisé pour la détection d'un identifiant sur un système de contrôle d'accès. L'identifiant peut prendre différentes formes : badge, code clavier, empreinte biométrique, plaque minéralogique... Selon sa technologie, un lecteur peut être utilisé pour : ● Assurer la simple détection du support de l'identifiant, par exemple un lecteur de type "transparent" qui se limite à détecter la présence d'un badge. ● Assurer en plus la lecture d'un identifiant standard, par exemple un lecteur "simple" qui ne sait lire que le numéro de série d'un badge (identifiant *CSN*). ● Assurer en plus la fonction de déchiffrement d'un identifiant sécurisé encodé dans un badge, par exemple un lecteur sécurisé dans lequel on enregistre la clé des badges.
MICROSESAME	Logiciel de supervision unifiée qui permet de centraliser toutes les informations électroniques du bâtiment : contrôle d'accès,

	détection intrusion, gestion technique, vidéo, interphonie... Le pilotage des différentes fonctions à travers une interface graphique commune rend leur exploitation beaucoup plus simple et les interventions plus efficaces. Les interactions entre les différents systèmes pouvant être complètement automatisées (actions sur évènements), la rapidité des traitements est également garantie.
Paramétrage	Configuration des paramètres déterminant le comportement des diverses fonctionnalités du système (contrôle d'accès, protection anti-intrusion, etc.) en fonction des besoins et des situations pour tous les types d'utilisateur.
Profil d'accès	Ensemble d'informations attribuées à un identifié et définissant des droits d'accès par lecteur et/ou par groupe de lecteur d'un site. Chaque accès est associé à au moins une plage horaire. Les profils d'accès permettent de redéfinir les accès pour une catégorie d'usagers de manière simple et intuitive. Le profil est composé d'une liste d'accès à des lecteurs, groupes de lecteurs ou à des sites. Une plage horaire unique ou différente pour chaque élément de cette liste, complète le profil.
TACTILLYS-IP CUBE	Terminal tactile d'exploitation TIL TECHNOLOGIES qui permet de gérer l'intrusion CUBE. Équipé d'un écran couleur 7 pouces et d'un lecteur de badge, il se raccorde sur le réseau Ethernet du site pour communiquer avec une TILLYS. Les opérateurs authentifiés peuvent afficher les alarmes et défauts en temps réel, mais également arrêter les sirènes, éjecter des points et activer la dérogation ou le report de mise en surveillance automatique.
Terminal intrusion	Il s'agit d'un TACTILLYS-IP CUBE dédié à la fonction intrusion d'une TILLYS . Les terminaux intrusion CUBE sont connectés via *IP*. Un clavier leur est généralement connecté. Ce dispositif permet de gérer une liste spécifique de groupes de détecteurs, ce qui limite l'exploitation à une partie restreinte de l'installation, quel que soit le profil intrusion de l'opérateur qui s'y connecte. Les terminaux intrusion permettent l'armement et le désarmement de leurs groupes de détecteurs, l'acquittement des alarmes, l'éjection ou l'inhibition d'un détecteur, et la gestion des dérogations. Il est également possible d'accéder à l'historique des alarmes intrusion et de faire passer le système en mode de maintenance, pour le tests des détecteurs et des sirènes. L'accès à tout ou partie de ces fonctions est soumis à l'authentification de l'opération intrusion à l'aide d'un badge et/ou d'un code.

TILLYS	Automate *IP* programmable multifonction développé par TIL TECHNOLOGIES qui dispose des fonctionnalités de contrôle d'accès, de détection intrusion et de *GTB*. Grâce à 3 bus RS 485 (A, B et C), chaque TILLYS permet le raccordement de 8, 16 ou 24 lecteurs pour le contrôle d'accès. Elle constitue également une véritable centrale d'alarme. Voir aussi *UTL*.
UTL	Acronyme d'Unité de Traitement Local. Terme générique qui désigne un automate *IP* programmable et multifonction, utilisé dans le domaine du contrôle d'accès, de l'intrusion et de la GTB. C'est grâce à cet automate que vont être gérés par exemple, les accès des identifiés, les informations provenant des lecteurs ou des systèmes anti-intrusion, etc. L'UTL de TIL TECHNOLOGIES est la *TILLYS*, qui se décline en version V2, NG et CUBE.
VoIP	Acronyme anglais de Voice over Internet Protocol. En français, "voix sur IP", cette technologie permet de faire transiter des communications vocales échantillonnées sur des liaisons de données numériques utilisant le protocole IP.
WEBSESAME	Application web du logiciel MICROSESAME. Elle permet l'exploitation d'une grande partie des fonctions de MICROSESAME à l'aide d'un simple navigateur internet (Edge, Chrome, Firefox, Safari...). On la désigne parfois sous le nom de *client léger*.

Chapitre 1. Configuration et utilisation du code intrusion CUBE global

1.1. Configuration de l'authentification par code intrusion CUBE global

Le code intrusion CUBE global est un code constitué uniquement de chiffres. Ce code est unique par identifié à l'échelle d'une installation. Il lui permet d'accéder aux fonctions de gestion de l'intrusion sur les claviers TACTILLYS-IP CUBE.

Les codes intrusion CUBE globaux sont stockés de façon sécurisée. Leur première attribution est effectuée dans MICROSESAME. Ils peuvent ensuite être modifiés dans MICROSESAME, WEBSESAME ou par l'identifié sur un TACTILLYS-IP CUBE connecté à l'installation.

1.1.1. Mise en place de la fonctionnalité code intrusion CUBE global

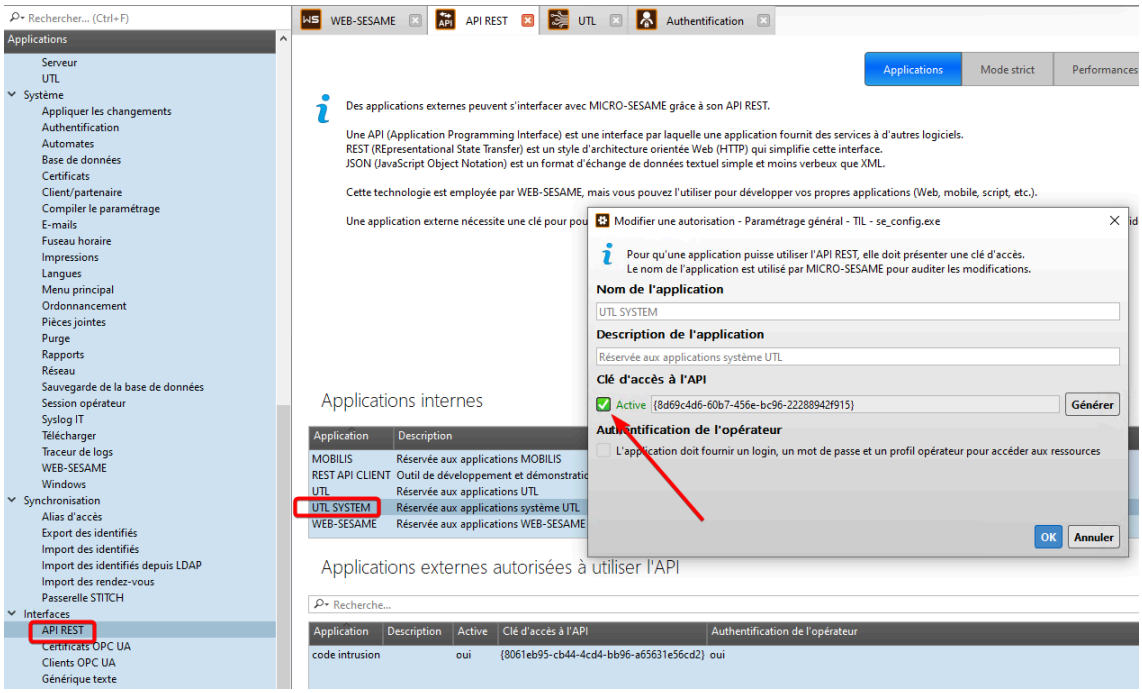
Avant de pouvoir saisir un premier code pour un agent de sécurité, il est nécessaire de mettre en place la fonctionnalité code intrusion CUBE global dans MICROSESAME (voir toutes les sous-sections ci-après).

1.1.1.1. Vérification de l'activation de la clé UTL système

Si cette clé n'est pas activée, il est impossible de modifier la clé à partir du TACTILLYS-IP CUBE.

1. Depuis le menu-principal de MICROSESAME, suivre **Paramétrage > Autres > Paramétrage général > [PAR]**.
2. Faire défiler vers le bas la section de gauche avec l'ascenseur vertical, et dans **Interfaces**, choisir **API REST**.

Figure 1.1. Vérification d'activité de la clé UTL système [10023-051]



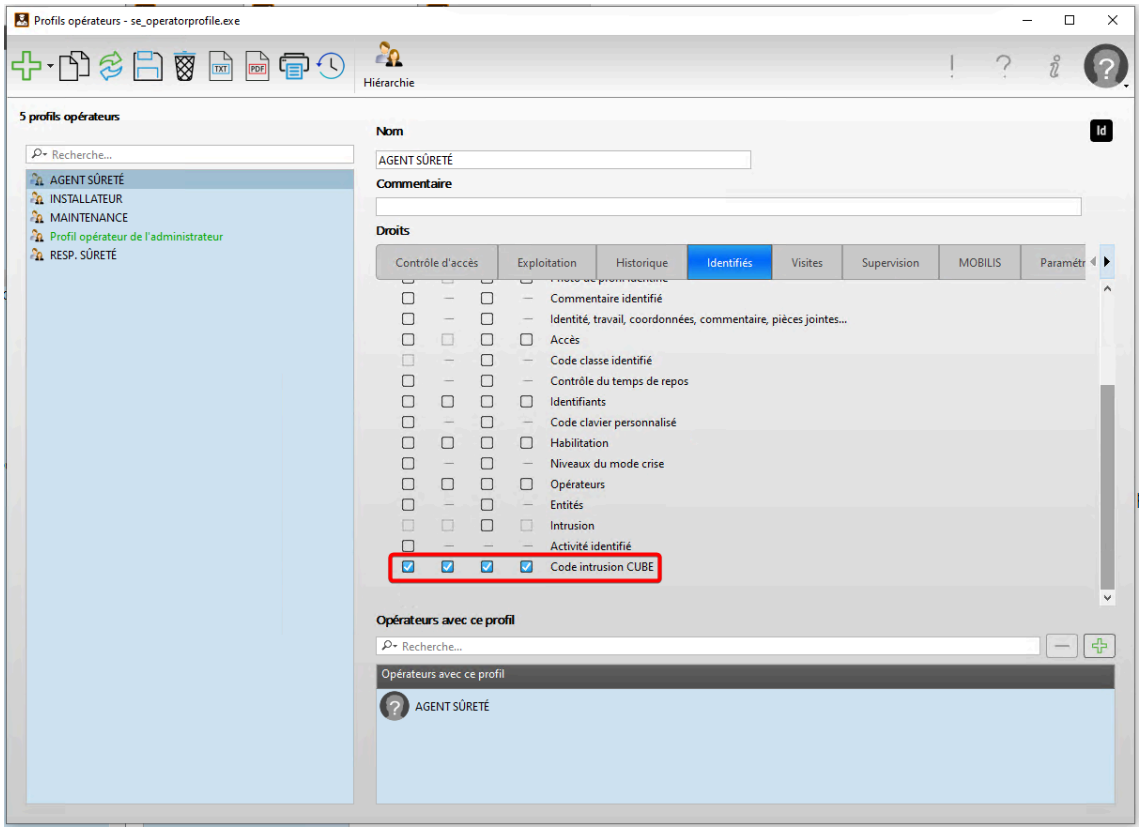
3. Dans la section de droite, faire un double clic sur la ligne UTL.
4. Dans la fenêtre instantanée qui s'affiche, si la case à cocher Clé d'accès à l'API n'est pas cochée, cliquer dessus.
5. Cliquer sur le bouton **OK**.

1.1.1.2. Choix du profil opérateur habilité à générer des codes intrusion CUBE global dans MICROSESAME

Il s'agit de définir le profil autorisé à générer le premier code (et en cas d'oubli, un nouveau code) pour les agents de sécurité gérant l'intrusion à partir des TACTILLYS-IP CUBE d'une installation.

1. Depuis le menu-principal de MICROSESAME, suivre **Paramétrage > Système > Profils opérateur > [PRO]**.
2. Dans la section de gauche, cliquer sur le profil à modifier, puis cliquer sur le bouton **Identifiés**.

Figure 1.2. Attribution des droits de gestion des codes intrusion CUBE global [10023-051]



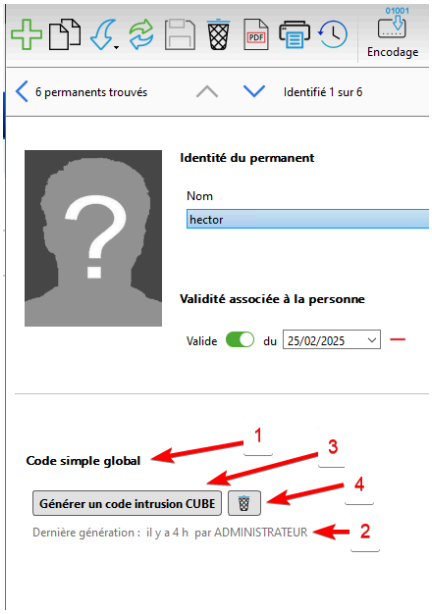
3. Faire descendre l'ascenseur à droite de l'écran pour afficher le bas de la liste des paramètres, puis cocher les cases des droits sur la ligne **Code intrusion CUBE** en fonction des besoins (voir tableau ci-après).

Tableau 1.1. Effet des droits liés aux codes intrusion CUBE globaux

Droit	Effet (les chiffres renvoient à la capture d'écran 10023-062)
Visu	Option permettant de voir (sur la partie Intrusion CUBE de la fiche identifié) si un autre identifié possède un code (1) et qui a effectué sa dernière génération (2).
Créer	Option d'administration permettant de générer le premier code pour un identifié (3).

Droit	Effet (les chiffres renvoient à la capture d'écran 10023-062)
Modif	Option permettant à l'identifié de modifier le code d'un autre identifié (3).
Suppr	Option d'administration permettant de supprimer (4) le code d'un autre identifié (sur la partie **Intrusion CUBE** de la fiche identifié).

Figure 1.3. Section Intrusion CUBE de la fiche identifié (suivre Exploitation > Contrôle d'accès > Identifiés [IDE]) [10023-062]



4. Cliquer sur le bouton Enregistrer.

1.1.1.3. Choix de la longueur du code intrusion CUBE global

Par défaut, sa longueur est de 4 chiffres. Cette procédure est facultative, si un code sur 4 chiffres répond au besoin du site.

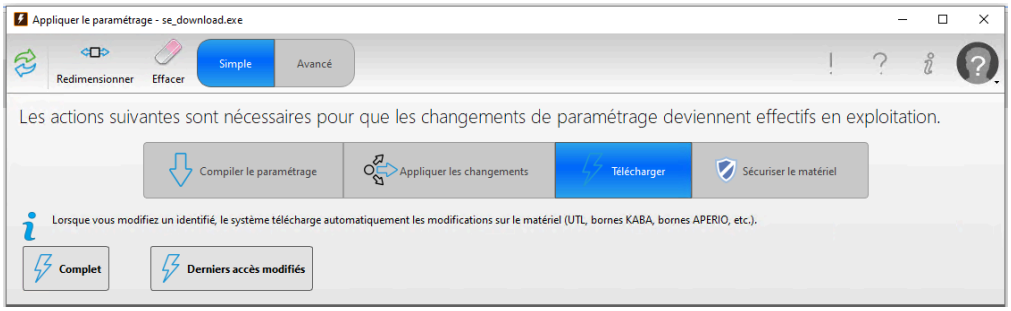
Il est préférable d'effectuer cette modification **avant** la génération des codes intrusion CUBE globaux.

Si la longueur de ce code est modifiée **après la mise en exploitation**, les codes existants seront invalidés et **il sera nécessaire de générer à nouveau tous ces codes**.

1. Depuis le menu-principal de MICROSESAME, suivre **Paramétrage > Intrusion > TILLYS intrusion CUBE > [TIL]**.

2. Dans le champ **Longueur du code intrusion CUBE**, choisir le nombre de chiffres en cliquant sur les flèches.
3. Cliquer sur le bouton Enregistrer.
4. Depuis le menu-principal de MICROSESAME, suivre **Paramétrage > Mise en exploitation > Appliquer le paramétrage > [APP]**.

Figure 1.4. Application du paramétrage (longueur du ciode intrusion CUBE global) [10023-055]



5. Cliquer successivement sur les boutons **Télécharger** et **Complet**.

   Le paramétrage lisible par les TACTILLYS-IP CUBE a été transmis aux TILLYS du réseau.

1.1.1.4. Choix du mode d'authentification par code intrusion CUBE global dans la TILLYS hôte

Cette fonction est disponible à partir de la version 7.2.0 du microprogramme du TACTILLYS-IP CUBE.

1. Dans le menu burger de la TILLYS hôte, suivre **Intrusion CUBE > Configuration intrusion**, puis cliquer sur l'onglet **TACTILLYS-IP**.
2. Dans la deuxième section en partie droite de l'écran, cliquer sur la liste déroulante Mode d'authentification. Choisir *Code intrusion CUBE global*, puis cliquer sur le bouton [Appliquer les paramètres d'authentification].
3. Voir *Section 1.1.1.5, « Import de la configuration intrusion CUBE de la TILLYS dans MICROSESAME »*.
4. Pour définir ou pour modifier le code global, voir *Section 1.1.3, « Attribution d'un code intrusion CUBE global à un identifié dans MICROSESAME »*, puis *Section 1.1.4, « Modification du code intrusion CUBE global d'un identifié par un administrateur »*.

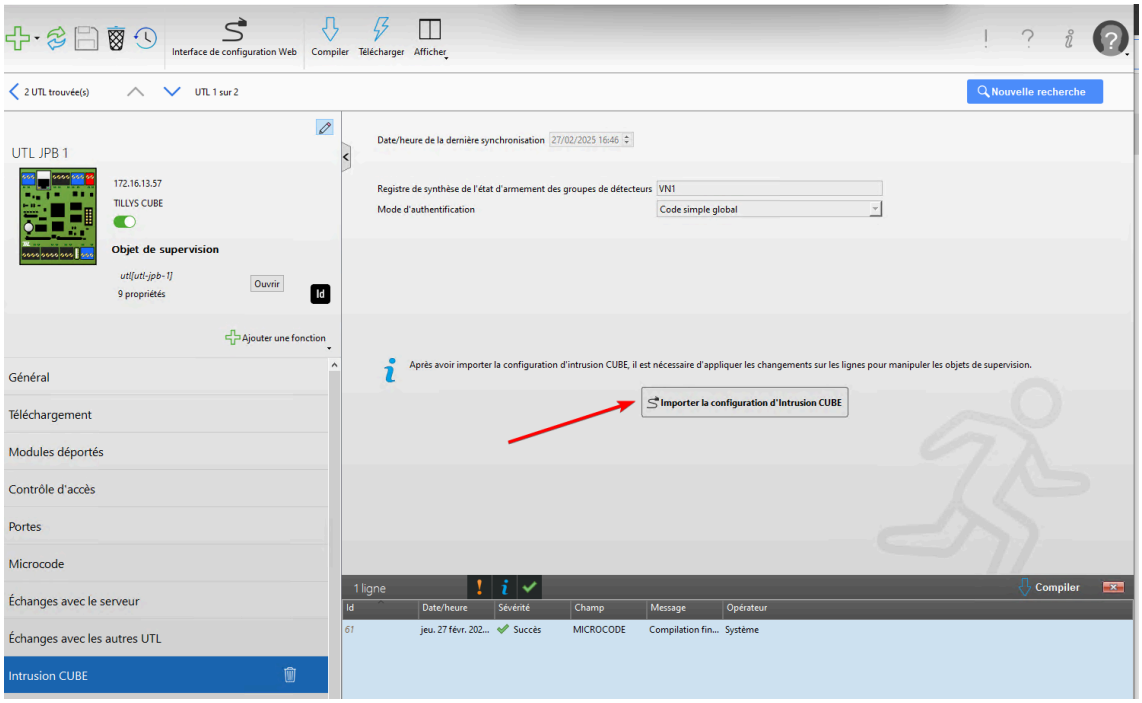
1.1.1.5. Import de la configuration intrusion CUBE de la TILLYS dans MICROSESAME

Cette fonction est disponible à partir de la version 2025.2 de MICROSESAME.

1. Depuis le menu-principal de MICROSESAME, suivre **Paramétrage > Matériels > Unités de Traitement Local (UTL) [UTL]**.

2. Faire un double clic sur la ligne de la TILLYS configurée en intrusion CUBE.
3. Si l'option Intrusion CUBE n'apparaît pas en bas de la section gauche de l'écran, cliquer sur le bouton **+ Ajouter une fonction** et choisir **Intrusion** dans la liste déroulante.
4. Cliquer sur Intrusion CUBE dans la section gauche de l'écran.
5. Cliquer sur le bouton Importer la configuration d'Intrusion CUBE.
6. En haut de l'écran, cliqer sur le bouton **Télécharger**.

Figure 1.5. Import de la configuration intrusion CUBE de la TILLYS dans MICROSESAME [10023-060]



7. Cocher la case **Tous**, puis cliquer sur le bouton **Exécuter**.

1.1.2. Attribution à un identifié d'un profil opérateur autorisé à gérer le code intrusion CUBE global

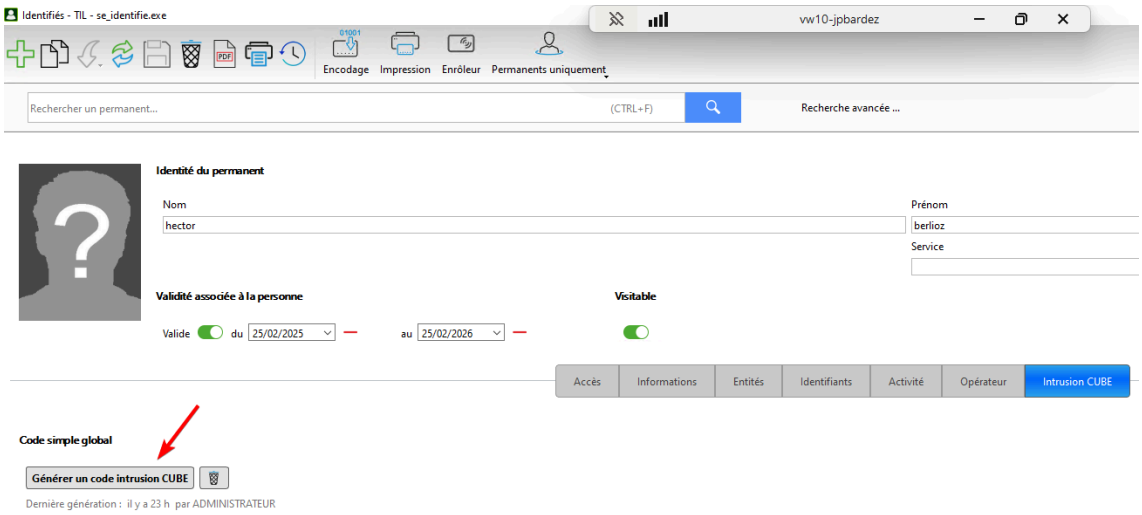
Pour gérer rapidement les droits des identifiés, il est possible de les associer à un profil (voir la section sur les profils opérateur dans le *Guide de référence de MICROSESAME*).

1.1.3. Attribution d'un code intrusion CUBE global à un identifié dans MICROSESAME

Les opérations décrites dans cette section permettent également de supprimer le code intrusion CUBE global d'un identifié, avant de lui attribuer un nouveau code.

1. Depuis le menu-principal de MICROSESAME, suivre **Exploitation > Contrôle d'accès > Identifiés [IDE]**.
2. Cliquer sur l'icône Loupe.
3. Cliquer sur le nom de l'identifié.
4. Dans la partie supérieure de l'écran, cliquer sur le bouton **Intrusion CUBE**.

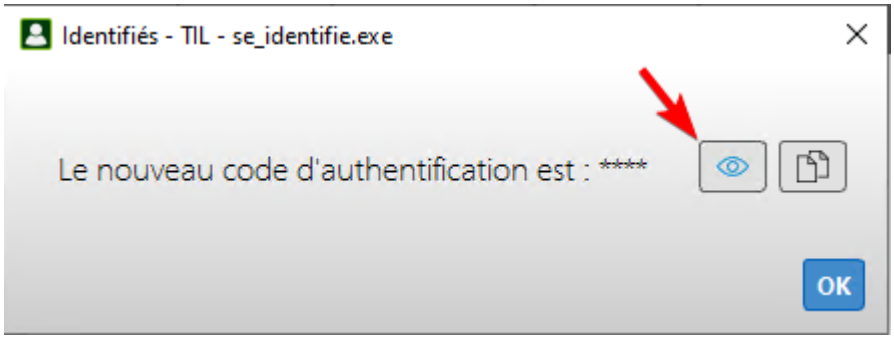
Figure 1.6. Génération d'un code aléatoire de type "code intrusion CUBE global" pour un identifié [10023-050]



5. Pour supprimer un code, cliquer sur l'icône **Corbeille**.

   Pour créer un code, cliquer sur le bouton **Générer un code intrusion CUBE**.

Figure 1.7. Fenêtre instantanée de visualisation d'un nouveau code intrusion CUBE global [10023-054]



6. Pour voir le code, cliquer sur l'icône  **Visualiser**.

Pour copier le code en mémoire, cliquer sur l'icône **Copier**.

7. Pour fermer la fenêtre instantanée, cliquer sur le bouton **OK**.

Ce nouveau code est immédiatement valable sur les TACTILLYS-IP CUBE.

1.1.4. Modification du code intrusion CUBE global d'un identifié par un administrateur

Cette opération peut être effectuée en utilisant :

- MICROSESAME (voir *Section 1.1.4.1, « Modification du code intrusion CUBE global d'un identifié dans MICROSESAME »*),
- WEBSESAME (voir *Section 1.1.4.2, « Création ou re-création du code intrusion CUBE global d'un identifié dans WEBSESAME »*),
- ou le TACTILLYS-IP CUBE (voir *Section 1.1.5.1, « Modification du code intrusion CUBE global par l'identifié sur le TACTILLYS-IP CUBE »*).

1.1.4.1. Modification du code intrusion CUBE global d'un identifié dans MICROSESAME

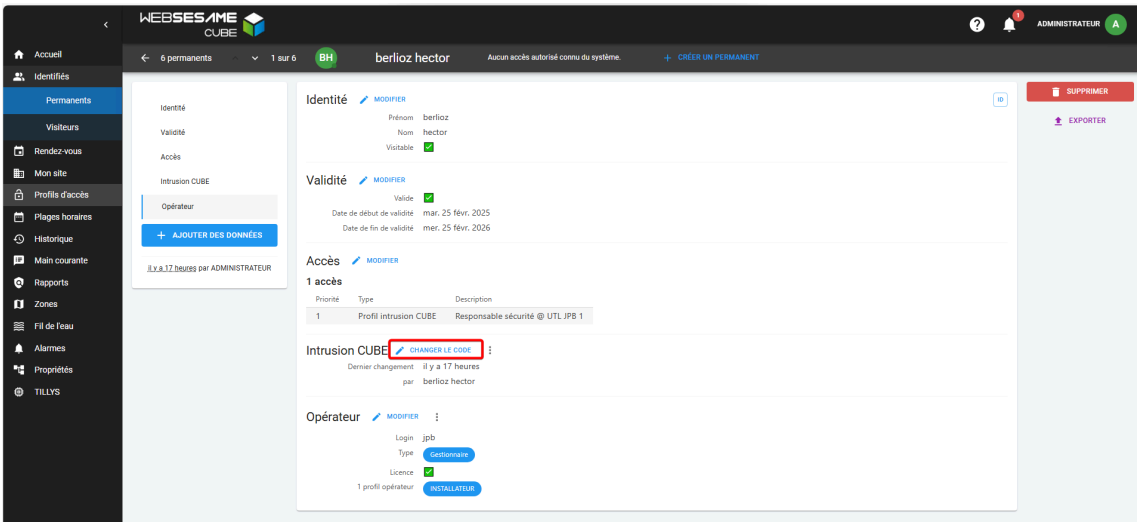
Pour modifier le code intrusion CUBE global d'un identifié dans MICROSESAME, les opérations sont identiques à celles décrite dans la section *Section 1.1.3, « Attribution d'un code intrusion CUBE global à un identifié dans MICROSESAME »*).

1.1.4.2. Création ou re-création du code intrusion CUBE global d'un identifié dans WEBSESAME

Cette procédure fonctionne pour la création du code la première fois ou en cas d'oubli de ce code par l'identifié. Il est nécessaire de disposer du droit de gestion de ces codes.

1. A partir de la page d'accueil de WEBSESAME, suivre Identifiés > Permanents, puis cliquer sur le nom de l'identifié dont le code doit être modifié.

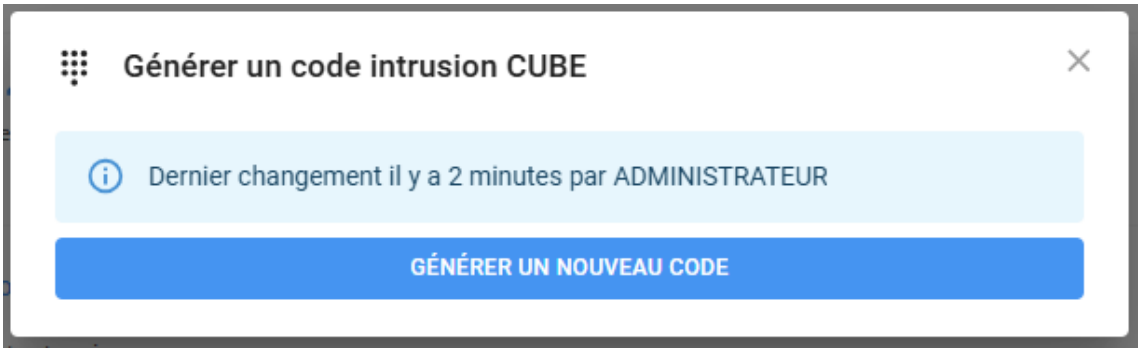
Figure 1.8. Modification du code intrusion CUBE global dans WEBSESAME [10023-056]



2. Cliquer sur le bouton **Changer le code**.

   Une fenêtre de confirmation s'affiche.

Figure 1.9. Fenêtre de confirmation de la génération d'un nouveau code intrusion CUBE global sous WEBSESAME [10023-057]



3. Cliquer sur le bouton **Générer un nouveau code**.

   Le nouveau code s'affiche dans une fenêtre instantanée. Il est valable immédiatement.

Figure 1.10. Fenêtre instantanée d'affichage du nouveau code intrusion CUBE global [10023-065]

4. Pour copier le code en mémoire, cliquer sur l'icône **Copier**.
5. Pour fermer la fenêtre instantanée d'affichage du code, cliquer sur la croix en haut à droite de la fenêtre instantanée.

1.1.5. Modification du code intrusion CUBE global par l'identifié

L'identifié peut modifier son code intrusion CUBE global :

- sur le TACTILLYS-IP CUBE (voir *Section 1.1.5.1, « Modification du code intrusion CUBE global par l'identifié sur le TACTILLYS-IP CUBE »*)
- ou dans WEBSESAME (voir *Section 1.1.5.2, « Modification du code intrusion CUBE global par l'identifié dans WEBSESAME »*).

1.1.5.1. Modification du code intrusion CUBE global par l'identifié sur le TACTILLYS-IP CUBE

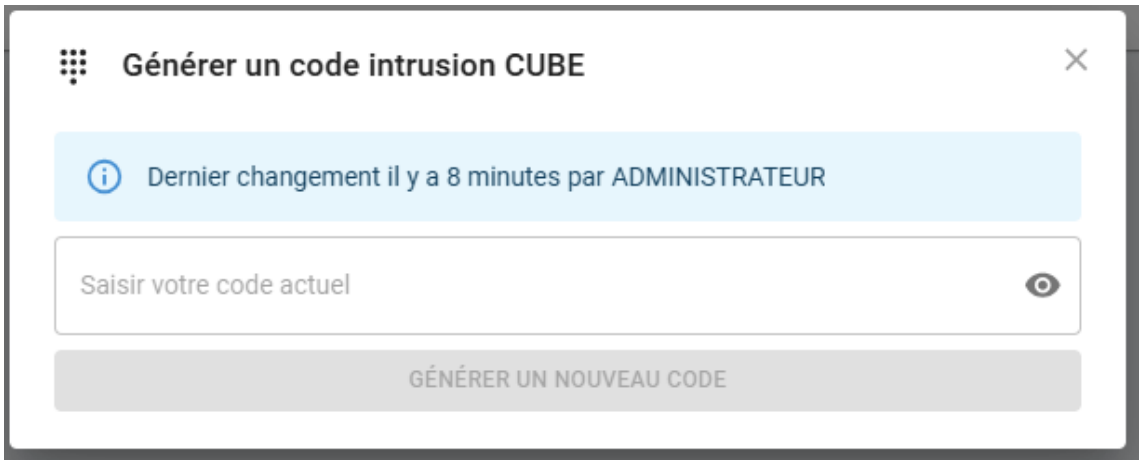
1. Saisir le code intrusion CUBE global actuel sur le lecteur du TACTILLYS-IP CUBE : l'écran d'accueil s'affiche.
2. Toucher l'icône burger en haut à gauche de l'écran, puis l'option **[Réinitialiser code]**.
3. Saisir de nouveau le code intrusion CUBE global actuel.

   Un nouveau code est généré, qui est valable immédiatement.
4. Pour afficher ce code, cliquer sur l'icône **œil**.
5. Pour fermer cette fenêtre, cliquer sur l'icône **Quitter**, en haut à droite de l'écran.

1.1.5.2. Modification du code intrusion CUBE global par l'identifié dans WEBSESAME

1. A partir de la page d'accueil de WEBSESAME, cliquer sur le cercle avec les initiales en haut à droite de l'écran et choisir **Changer de code intrusion CUBE**.

Figure 1.11. Fenêtre de saisie du code intrusion CUBE global actuel par l'identifié [10023-063]



2. Saisir le code actuel, puis cliquer sur le bouton **Générer un nouveau code**.

   Le nouveau code s'affiche dans une fenêtre instantanée. Il est valable immédiatement.

   Il est possible de le copier en cliquant sur l'icône située à droite du code.

Figure 1.12. Fenêtre d'affichage du nouveau code intrusion CUBE global de l'identifié [10023-064]

3. Pour fermer la fenêtre instantanée d'affichage du code, cliquer sur la croix en haut à droite.

1.2. Perte du code intrusion CUBE global par l'identifié

1. Contacter le responsable sécurité autorisé à créer des codes intrusion CUBE globaux.
2. Lui demander de supprimer le code intrusion CUBE global actuel, puis d'en recréer un, selon la procédure décrite à la section *Section 1.1.3, « Attribution d'un code intrusion CUBE global à un identifié dans MICROSESAME »* .

1.3. Utilisation du code intrusion CUBE global sur le TACTILLYS-IP CUBE

1.3.1. Accès au TACTILLYS-IP CUBE par le code intrusion CUBE global

1. Toucher l'écran du TACTILLYS-IP CUBE.
2. Saisir le code intrusion CUBE global.

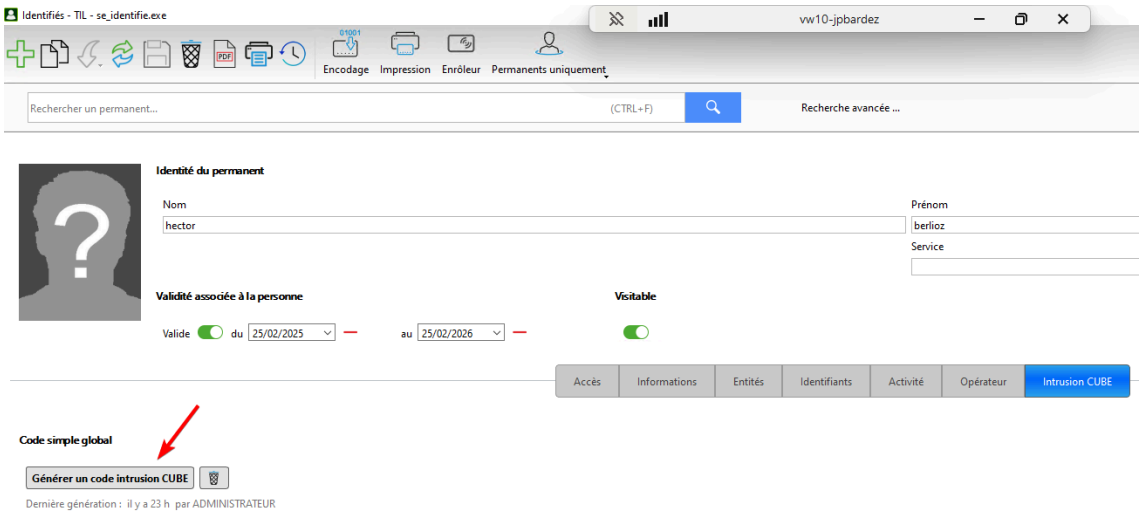
   L'écran d'accueil s'affiche.

1.3.2. Attribution d'un code intrusion CUBE global à un identifié dans MICROSESAME

Les opérations décrites dans cette section permettent également de supprimer le code intrusion CUBE global d'un identifié, avant de lui attribuer un nouveau code.

1. Depuis le menu-principal de MICROSESAME, suivre **Exploitation > Contrôle d'accès > Identifiés [IDE]**.
2. Cliquer sur l'icône Loupe.
3. Cliquer sur le nom de l'identifié.
4. Dans la partie supérieure de l'écran, cliquer sur le bouton **Intrusion CUBE**.

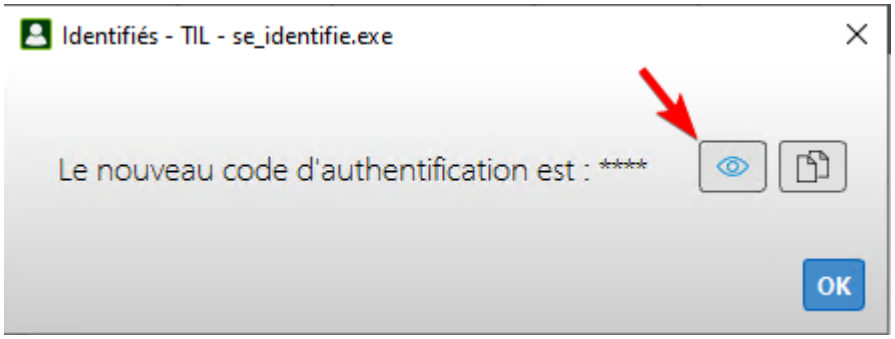
Figure 1.13. Génération d'un code aléatoire de type "code intrusion CUBE global" pour un identifié [10023-050]



5. Pour supprimer un code, cliquer sur l'icône **Corbeille**.

   Pour créer un code, cliquer sur le bouton **Générer un code intrusion CUBE**.

Figure 1.14. Fenêtre instantanée de visualisation d'un nouveau code intrusion CUBE global [10023-054]



6. Pour voir le code, cliquer sur l'icône **Visualiser**.

   Pour copier le code en mémoire, cliquer sur l'icône **Copier**.
7. Pour fermer la fenêtre instantanée, cliquer sur le bouton **OK**.

   Ce nouveau code est immédiatement valable sur les TACTILLYS-IP CUBE.

1.3.3. Modification du code intrusion CUBE global d'un identifié par un administrateur

Cette opération peut être effectuée en utilisant :

- MICROSESAME (voir *Section 1.1.4.1, « Modification du code intrusion CUBE global d'un identifié dans MICROSESAME »*),
- WEBSESAME (voir *Section 1.1.4.2, « Création ou re-création du code intrusion CUBE global d'un identifié dans WEBSESAME »*),
- ou le TACTILLYS-IP CUBE (voir *Section 1.1.5.1, « Modification du code intrusion CUBE global par l'identifié sur le TACTILLYS-IP CUBE »*).

1.3.3.1. Modification du code intrusion CUBE global d'un identifié dans MICROSESAME

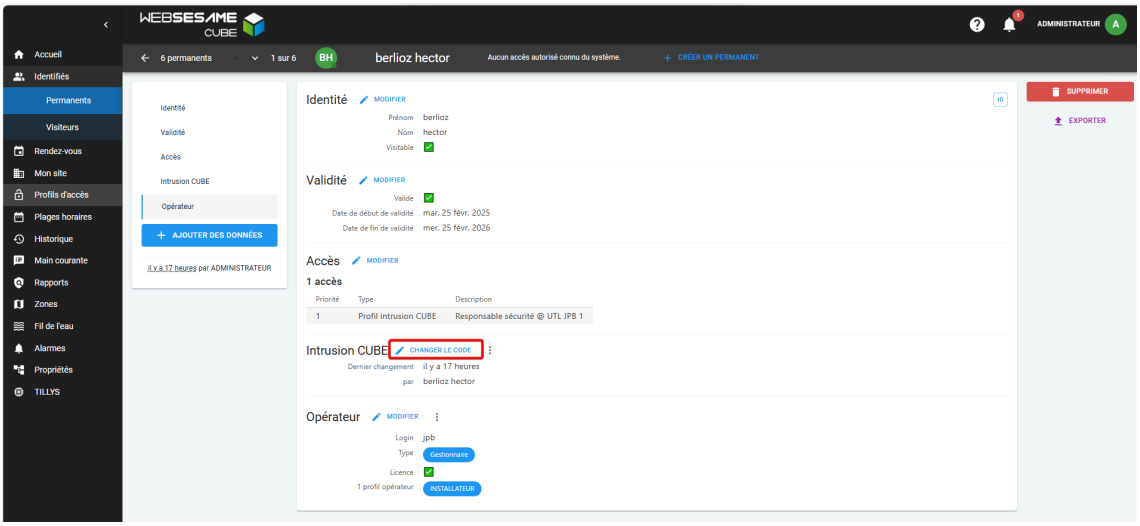
Pour modifier le code intrusion CUBE global d'un identifié dans MICROSESAME, les opérations sont identiques à celles décrite dans la section *Section 1.1.3, « Attribution d'un code intrusion CUBE global à un identifié dans MICROSESAME »*).

1.3.3.2. Création ou re-création du code intrusion CUBE global d'un identifié dans WEBSESAME

Cette procédure fonctionne pour la création du code la première fois ou en cas d'oubli de ce code par l'identifié. Il est nécessaire de disposer du droit de gestion de ces codes.

1. A partir de la page d'accueil de WEBSESAME, suivre Identifiés > Permanents, puis cliquer sur le nom de l'identifié dont le code doit être modifié.

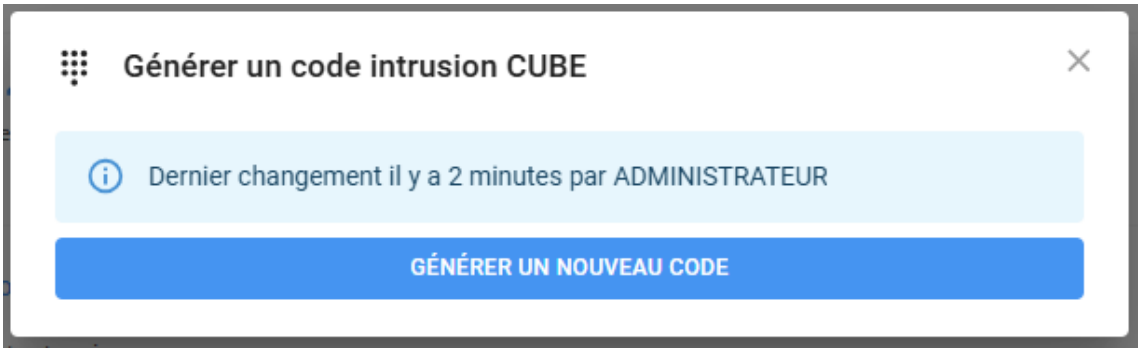
Figure 1.15. Modification du code intrusion CUBE global dans WEBSESAME [10023-056]



2. Cliquer sur le bouton **Changer le code**.

   Une fenêtre de confirmation s'affiche.

Figure 1.16. Fenêtre de confirmation de la génération d'un nouveau code intrusion CUBE global sous WEBSESAME [10023-057]



3. Cliquer sur le bouton **Générer un nouveau code**.

   Le nouveau code s'affiche dans une fenêtre instantanée. Il est valable immédiatement.

Figure 1.17. Fenêtre instantanée d'affichage du nouveau code intrusion CUBE global [10023-065]

4. Pour copier le code en mémoire, cliquer sur l'icône **Copier**.
5. Pour fermer la fenêtre instantanée d'affichage du code, cliquer sur la croix en haut à droite de la fenêtre instantanée.