



## **Guide utilisateur intrusion et transmission CUBE**

# **Guide utilisateur intrusion et transmission CUBE**

# Table des matières

<b>Préface .....</b>	<b>10</b>
1. Matériel nécessaire .....	10
2. Version logicielle .....	10
3. Contexte d'utilisation de ce manuel .....	10
4. Voir aussi .....	10
5. Réserve de propriété .....	10
6. Glossaire .....	11
<b>1. Contexte de la détection d'intrusion CUBE .....</b>	<b>24</b>
1.1. Vue d'ensemble de la version de base de l'intrusion CUBE .....	24
1.2. Vue d'ensemble de la version multi-TILLYS de l'intrusion CUBE .....	24
1.3. Nouveautés et avantages de l'intrusion CUBE .....	26
1.4. Définition du fonctionnement attendu par le responsable sécurité .....	27
1.5. Prérequis intrusion CUBE à mettre en place par le DSSI du client .....	27
1.6. Gestion de l'intrusion CUBE .....	27
1.7. Informations de référence pour les intégrateurs .....	29
1.7.1. Formats des trames échangées entre TILLYS et terminaux de télésurveillance .....	29
1.7.1.1. Codes intrusion transmis par les détecteurs aux télésurveilleurs .....	29
1.7.1.2. Codes évènements transmis par les groupes aux télésurveilleurs .....	33
1.7.1.3. Télécommandes envoyées à la TILLYS par les télésurveilleurs .....	33
1.7.2. Valeurs du registre numérique d'état des groupes en intrusion CUBE .....	34
1.7.3. Registres du microcode, propres à l'intrusion CUBE .....	36
1.7.4. Fonction du microcode permettant de remonter les informations d'AP d'un TACTILLYS-IP CUBE .....	36
<b>2. Workflows intrusion CUBE .....</b>	<b>37</b>
2.1. Préparation du site informatique .....	37
2.2. Configuration intrusion CUBE par le partenaire avec préparation dans ses locaux .....	37
2.2.1. Workflow - Pré-configuration intrusion CUBE par le partenaire dans ses locaux .....	37

2.2.2. Workflow - Export/import du paramétrage intrusion CUBE .....	37
2.3. Configuration intrusion CUBE par le partenaire sur le site du client .....	38
2.3.1. Workflow - Configuration intrusion CUBE sur le site du client .....	38
2.3.2. Workflow - Configuration d'un badge d'accès au terminal TACTILLYS-IP CUBE .....	38
2.3.3. Workflow - Installation, configuration et paramétrage d'un terminal TACTILLYS-IP CUBE avant sa mise en service .....	39
<b>3. Paramétrage de l'intrusion CUBE par le partenaire .....</b>	<b>40</b>
3.1. Architecture matérielle de configuration de l'intrusion CUBE par le partenaire .	40
3.2. Configuration, paramétrage et maintenance intrusion CUBE sur la TILLYS .....	41
3.2.1. Opérations de configuration intrusion CUBE .....	41
3.2.1.1. Accès à l'interface d'administration de l'intrusion CUBE sur une TILLYS .....	41
3.2.1.2. Configuration d'un groupe de détecteurs intrusion CUBE .....	42
3.2.1.3. Activation de la transmission d'alarmes au télésurveilleur .....	46
3.2.1.4. Configuration multi-TILLYS : génération sur la TILLYS hôte d'un token par TILLYS périphérique .....	46
3.2.1.5. Configuration multi-TILLYS : copie sur une TILLYS périphérique du lien avec la TILLYS hôte .....	48
3.2.1.6. Configuration des détecteurs intrusion CUBE d'une TILLYS .....	49
3.2.1.7. Configuration d'un détecteur intrusion CUBE sur une TILLYS périphérique .....	53
3.2.1.8. Configuration d'une sirène intrusion CUBE .....	53
3.2.1.9. Configuration d'une sirène intrusion CUBE sur une TILLYS périphérique .....	56
3.2.1.10. Comparaison des vues d'ensemble des détecteurs en intrusion CUBE multi-TILLYS .....	56
3.2.1.11. Association d'un terminal TACTILLYS-IP CUBE à un ou plusieurs groupes d'une TILLYS hôte .....	57
3.2.1.12. Configuration des télésurveilleurs .....	59
3.2.1.13. Affichage de la configuration de télésurveillance .....	61
3.2.2. Opérations de paramétrage et de maintenance de l'intrusion CUBE .....	62
3.2.2.1. Création des profils intrusion sur la TILLYS hôte .....	62
3.2.2.2. Choix des groupes de détecteurs gérés par un TACTILLYS-IP CUBE ....	64
3.2.2.3. Choix du mode d'authentification (badge ou badge + code) sur un TACTILLYS-IP CUBE .....	64
3.2.2.4. Choix des applets à charger sur un TACTILLYS-IP CUBE .....	65
3.2.2.5. Choix du niveau de détail des événements du journal de la TILLYS ....	65
3.2.2.6. Choix du niveau de sécurité sur IP entre TILLYS et TACTILLYS-IP CUBE	66
3.2.2.7. Effacement des clés du TACTILLYS-IP (désensibilisation) .....	67
3.2.3. Opérations de gestion de l'intrusion .....	68
3.2.3.1. Éjection manuelle, éjection automatique, éjection permanente ou réinjection automatique .....	68

3.2.3.2. Éjection ou réinjection d'un détecteur .....	68
3.2.4. Opérations de maintenance intrusion CUBE .....	69
3.2.4.1. Activation ou désactivation du port de maintenance d'une TILLYS ....	69
3.2.4.2. Exporter ou importer un fichier de configuration intrusion CUBE .....	70
3.2.4.3. Prolongation de la durée de validité d'un token .....	72
<b>4. Installation, paramétrage et utilisation du terminal TACTILLYS-IP CUBE .....</b>	<b>73</b>
4.1. Opérations d'installation, de configuration et de maintenance d'un terminal TACTILLYS-IP CUBE .....	73
4.1.1. Installation physique et connexion d'un terminal TACTILLYS-IP CUBE .....	73
4.1.2. Accès à l'interface d'administration du terminal TACTILLYS-IP CUBE et affichage des caractéristiques produit .....	73
4.1.3. Changement du mot de passe administrateur du terminal TACTILLYS-IP CUBE .....	74
4.1.4. Réglage de l'heure du terminal TACTILLYS-IP CUBE .....	75
4.1.5. Paramétrage réseau du TACTILLYS-IP CUBE .....	76
4.1.6. Mise à jour du firmware du TACTILLYS-IP CUBE .....	76
4.1.7. Paramétrage de la journalisation des événements du TACTILLYS-IP CUBE ..	77
4.1.8. Désensibilisation du TACTILLYS-IP CUBE .....	77
4.2. Paramétrage du terminal TACTILLYS-IP CUBE .....	78
4.2.1. Authentification et navigation sur un terminal TACTILLYS-IP CUBE .....	78
4.2.2. Consultation des caractéristiques de fonctionnement du TACTILLYS-IP CUBE .....	82
4.2.3. Paramétrage du TACTILLYS-IP CUBE .....	82
4.2.4. Choix des paramètres réseau du TACTILLYS-IP CUBE .....	83
4.2.5. Arrêt de l'alarme d'autoprotection en phase d'installation du TACTILLYS- IP CUBE .....	83
4.2.6. Déconnexion automatique du TACTILLYS-IP CUBE .....	84
4.3. Utilisation du TACTILLYS-IP CUBE .....	84
4.3.1. Armement ou désarmement manuel d'un groupe .....	84
4.3.2. Éjection manuelle de détecteurs en défaut .....	85
4.3.3. Arrêt des sirènes .....	85
4.3.4. Dérogation d'armement sur groupe(s) de détecteurs .....	85
<b>5. Configuration et exploitation de l'intrusion CUBE .....</b>	<b>87</b>
5.1. Import de la configuration intrusion CUBE dans MICROSESAME .....	87
5.2. Procédure de préparation d'un badge de gestion d'intrusion CUBE sur terminal TACTILLYS-IP CUBE .....	88
5.2.1. Préparation d'un badge de contrôle anti-intrusion .....	88
5.2.2. Acquisition d'un identifiant non attribué dans MICROSESAME .....	88
5.2.3. Affectation d'un identifiant disponible à un nouvel identifié .....	89
5.2.4. Attribution de droits d'accès à un nouvel identifié .....	89
5.2.5. Attribution d'un profil intrusion CUBE à un nouvel identifié .....	90

5.3. Gestion des profils intrusion des identifiés sur MICROSESAME ou WEBSesame .....	90
5.4. Affichage du nom des opérateurs à l'origine d'évènements de commande intrusion .....	90
5.4.1. Ouverture de la fiche de configuration de la TILLYS hôte et de l'écran des paramètres de contrôle d'accès .....	91
5.4.2. Choix du texte associé aux identifiés .....	91
5.5. Paramétrage du synoptique sur MICROSESAME .....	91
5.6. Consultation du synoptique sur MICROSESAME .....	92
5.7. Déclaration des opérateurs de détection d'intrusion sur la TILLYS .....	93
5.8. Test de l'installation de détection d'intrusion .....	93
5.8.1. Test des détecteurs .....	93
5.8.2. Test de communication entre la TILLYS et le TACTILLYS-IP CUBE .....	93
<b>6. Gestion de la sécurité par le responsable sécurité .....</b>	<b>94</b>
6.1. Attribution des droits d'accès aux utilisateurs du TACTILLYS-IP CUBE .....	94
6.2. Changement de l'identifiant intrusion utilisé lors de l'identification badge + code sur TACTILLYS-IP CUBE .....	94
6.3. Consultation de l'historique intrusion .....	94
<b>7. Opérations liées à l'intrusion, effectuées par le télésurveilleur .....</b>	<b>95</b>
7.1. Consultation des alarmes en cours .....	95
7.1.1. Syntaxe des messages de polling .....	95
7.1.2. Syntaxe des messages de test cyclique .....	95
7.2. Commande à distance de l'intrusion CUBE .....	95
7.2.1. Armement .....	96
7.2.2. Arrêt sirène .....	96
7.2.3. Désarmement .....	96
7.2.4. Changement de valeur d'un registre de la TILLYS .....	96

## Liste des illustrations

1.1. Architecture matérielle de la version de base de l'intrusion CUBE (10010-001) .....	24
1.2. Architecture matérielle de la version multi-TILLYS de l'intrusion CUBE (10010-002) .....	25
1.3. Configuration multi-TILLYS de l'intrusion CUBE (10010-003) .....	26
3.1. Configuration de l'intrusion CUBE via Ethernet (10010-004) .....	40
3.2. Emplacement des onglets de navigation sur l'écran de configuration de l'intrusion CUBE d'une TILLYS (10010-005) .....	42
3.3. Déclaration d'un détecteur (10010-006) .....	43
3.4. Génération d'un token (10010-007) .....	46
3.5. Copie du token généré (10010-008) .....	47
3.6. Visualisation du groupe de détecteurs d'une TILLYS hôte sur une TILLYS périphérique (10010-009) .....	48
3.7. Saisie du token de la TILLYS hôte sur une TILLYS périphérique (10010-010) .....	49
3.8. Déclaration d'un détecteur (10010-011) .....	50
3.9. Création et configuration d'une fonction sirène (10010-012) .....	54
3.10. Comparaison des vues d'ensemble des détecteurs sur TILLYS hôte et TILLYS périphérique (10010-013) .....	57
3.11. Déclaration du terminal TACTILLYS-IP pour la gestion de l'intrusion CUBE (10010-014) ....	58
3.12. Déclaration du ou des télésurveilleurs pour la gestion de l'intrusion CUBE (10010-015) ..	60
3.13. Affichage de la configuration de télésurveillance (10010-500) .....	62
3.14. Création et configuration des profils intrusion (10010-016) .....	63
3.15. Choix des groupes gérés par le TACTILLYS-IP CUBE (10010-017) .....	64
3.16. Configuration de l'authentification sur un TACTILLYS-IP CUBE (badge ou badge + code) (10010-018) .....	65
3.17. Choix des applets à charger sur un TACTILLYS-IP (10010-019) .....	65
3.18. Niveau de détail des événements journalisés (10010-021) .....	66
3.19. Passage de https à http sur le TACTILLYS-IP (10010-022) .....	67
3.20. Passage de https à http sur la TILLYS (10010-023) .....	67
3.21. Effacement des clés de sécurité du TACTILLYS-IP (10010-024) .....	68
3.22. Éjection ou réinjection de détecteurs sur une TILLYS (10010-025) .....	69
3.23. Activation du port de maintenance sur une TILLYS (10010-026) .....	70
3.24. Choix des options avant l'export d'un fichier de configuration intrusion CUBE (10010-027) .....	71
4.1. Écran d'accueil du TACTILLYS-IP (10010-028) .....	74
4.2. Écran d'accueil du TACTILLYS-IP CUBE (10010-029) .....	74
4.3. Réglage de la date et de l'heure du TACTILLYS-IP CUBE (10010-030) .....	75
4.4. Configuration réseau du TACTILLYS-IP CUBE (10010-031) .....	76
4.5. Mise à jour du firmware du TACTILLYS-IP CUBE (10010-032) .....	77
4.6. Écran de veille du TACTILLYS-IP CUBE (10010-502) .....	78
4.7. Écran d'accueil du TACTILLYS-IP CUBE (10010-503) .....	79
4.8. Écran des détecteurs d'un groupe sur le TACTILLYS-IP CUBE (10010-504) .....	80
4.9. Écran des sirènes d'un groupe sur le TACTILLYS-IP CUBE (10010-505) .....	81
4.10. Caractéristiques de fonctionnement du TACTILLYS-IP CUBE (10010-034) .....	82
4.11. Paramètres de l'IHM du TACTILLYS-IP CUBE : luminosité, thème, langue, niveau sonore (10010-035) .....	82

4.12. Choix des paramètres réseau du TACTILLYS-IP CUBE (10010-036) .....	83
4.13. Arrêt de l'alarme d'autoprotection du TACTILLYS-IP CUBE (10010-037) .....	84
5.1. Préparation de l'import de la configuration intrusion d'une TILLYS dans MICROSESAME (10010-038) .....	87
5.2. L'éditeur de synoptique de MICROSESAME (10010-039) .....	92
5.3. Consultation du synoptique de MICROSESAME (10010-040) .....	93

## Liste des tableaux

1.1. Normes de sécurité informatique applicables .....	27
1.2. Liste des opérations de gestion de l'intrusion avec leur contexte et leur mode opératoire ..	28
1.3. Liste complète des codes intrusion envoyés par les détecteurs .....	30
1.4. Signification des codes intrusion envoyés par les détecteurs .....	30
1.5. Signification des codes événements envoyés par les groupes .....	33
1.6. Liste des télécommandes pouvant être envoyées par les télésurveilleurs à la TILLYS .....	33
1.7. Valeurs possibles du registre numérique d'état des groupes .....	34
3.1. Configuration de l'éjection d'un détecteur .....	69
4.1. Signification des pictogrammes sur l'écran de la liste des groupes sur le terminal TACTILLYS-IP CUBE .....	79
4.2. Signification des pictogrammes des détecteurs sur le terminal TACTILLYS-IP CUBE .....	80
4.3. Signification des pictogrammes des sirènes sur le terminal TACTILLYS-IP CUBE .....	81
4.4. Signification des pictogrammes d'éjection de détecteur sur le terminal TACTILLYS-IP CUBE	81

# 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, **daté du 6 septembre 2024**, décrit comment installer, configurer et mettre en service la fonction intrusion CUBE pour la **version logicielle 2024.2** de MICROSESAME.

Firmware de la TILLYS CUBE à **partir de 7.0.0**.

Firmware du TACTILLYS-IP à **partir de 7.0.0**.

## 3. Contexte d'utilisation de ce manuel

**Le responsable informatique du site ([DSSI](#))** du client a été prévenu à l'avance et a effectué les opérations nécessaires à la sécurisation des échanges de données sur IP.

**Le responsable sécurité** a transmis son cahier des charges au partenaire ou installateur TIL TECHNOLOGIES.

**Le partenaire ou installateur TIL TECHNOLOGIES** configure les TILLYS conformément au cahier des charges dans ses locaux, puis il copie cette configuration sur une clé USB. Sur le site du client, il charge ces configurations sur les TILLYS, puis sur MICROSESAME il connecte et configure les terminaux TACTILLYS-IP CUBE et il teste leur fonctionnement.

**Le client** exploite les fonctions de son ou ses terminaux TACTILLYS-IP CUBE pour armer ou désarmer ses groupes, et les [alarmes](#) intrusion sont transmises au télésurveilleur.

**Le télésurveilleur** gère les alarmes à distance via son terminal.

## 4. Voir aussi

- [Vidéo de présentation de la détection intrusion CUBE](#).
- [Fiche technique du terminal intrusion TACTILLYS-IP CUBE](#).
- [Guide de démarrage rapide de MICROSESAME \(GD-10001-FR\)](#).

## 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.

Aucune partie de ce document ne peut être ni altérée, ni reproduite ou transmise sous quelque forme et quelque moyen que ce soit sans l'autorisation expresse de TIL TECHNOLOGIES.

Envoyez vos commentaires, corrections et suggestions concernant ce guide à [documentation@til-technologies.fr](mailto:documentation@til-technologies.fr)

## 6. Glossaire

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

Alarme	<p>Propriété qui signale un évènement anormal (intrusion, défaut technique, POTL...).</p> <p>Une alarme technique est en surveillance 24 h/24 et elle passe en alarme dès son passage au niveau actif.</p> <p>Une information de détecteurs de type alarme intrusion est en surveillance lorsque leur groupe d'appartenance est armé. Le passage en alarme est donc déterminé non seulement par leur passage à l'état actif mais aussi par l'état d'armement de leur groupe.</p>
Armé	<p>Désigne l'état activé d'un système anti-intrusion, dans lequel l'apparition d'une condition d'alarme intrusion ou hold-up sera immédiatement notifiée au centre de télésurveillance.</p>
Authentification	<ol style="list-style-type: none"><li>1. <b>D'une façon générale</b>, l'authentification consiste à saisir des identifiants (Login / Mot de passe) pour accéder à un équipement comme la <a href="#">TILLYS</a>, 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.</li><li>2. Dans le paramétrage de l'<b>encodage de MICROSESAME</b>, 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 ...).</li><li>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</li></ol>

	retenu, cette authentification met en œuvre un identifiant et/ou un code intrusion personnalisé.
Bus	<p>Dispositif de câblage des équipements qui leur permet d'échanger des d'informations. TIL TECHNOLOGIES utilise trois types de bus :</p> <ul style="list-style-type: none"><li>● Un bus de communication RS485 pour modules. Chaque bus peut gérer un maximum de 8 lecteurs (les modules de porte peuvent gérer un ou deux lecteurs). Bien qu'il s'agisse de "bus", le raccordement peut également être réalisé en mode étoile (longueur totale maximale à respecter).</li><li>● Un bus de communication pour lecteurs. Les lecteurs peuvent être de type RS485 (raccordement direct) ou de types Dataclock ou Wiegand (en utilisant des convertisseurs appropriés).</li><li>● Un bus de communication pour transpondeurs EQUILOCK, dans lequel deux bus RS485 chiffrés peuvent accueillir jusqu'à 32 équipements EQUILOCK chacun, qui servent à gérer des détecteurs intrusion. Le raccordement des détecteurs se fait alors obligatoirement en mode bus, c'est-à-dire chaînés les uns aux autres.</li></ul>
Centre de télésurveillance	Centre de gestion des alarmes qui n'est pas situé dans les locaux de la ou des sociétés surveillées.
Client léger	Ordinateur sur lequel l'exploitation de MICROSESAME est effectuée sans aucune installation préalable, au travers de son application WEBSesame, utilisée à l'aide d'un simple navigateur internet.
Code clavier personnalisé	Code personnel attribué à un identifié qui est utilisé pour effectuer une double authentification pour un contrôle d'accès renforcé. Dans cette configuration, l'identifié doit passer son badge puis saisir son code sur un lecteur de badge muni d'un clavier.
Code identifiant	En gestion de l'intrusion, code qui est transmis avec chaque alarme et qui permet au destinataire télésurveilleur d'identifier la centrale d'alarme à l'origine de cette transmission.
Condition de déclenchement	Le déclenchement d'une alarme du type alarme intrusion est conditionné par la mise en surveillance du groupe d'appartenance. Le type d'alarme conditionne le déclenchement de celle-ci et chaque type d'alarme peut être associé à une mélodie spécifique.
Défaut	Une mise en surveillance ne peut pas être effectuée lorsqu'un détecteur de type alarme intrusion signale un défaut. Il est alors

nécessaire de corriger ce défaut ou d'éjecter ce capteur pour pouvoir procéder à la mise en surveillance. S'il n'est pas possible d'éjecter ce détecteur en défaut, l'alarme se déclenchera dès la mise en surveillance.

Dérogation	<ol style="list-style-type: none"><li>1. <b>En intrusion sur le terminal TACTILLYS-IP CUBE</b> : fonctionnalité permettant de différer l'armement imminent d'un ou plusieurs groupes de détecteurs. Si le droit à la dérogation a été attribué à un opérateur, celui-ci pourra repousser l'armement de l'alarme, en validant une durée prédéfinie qui lui est proposée (dans la limite du nombre de fois qui a été paramétré).</li><li>2. <b>Sur le terminal MOBILIS 3</b> : possibilité de contredire la décision d'accès validée par un terminal, lorsqu'il est utilisé en mode Contrôle d'accès automatique. Si ce paramètre a été activé, un utilisateur du terminal pourra ainsi, par exemple, refuser l'accès à un identifié possédant l'accès à un local technique, sous le motif qu'il ne dispose pas de tous les équipements de sécurité nécessaires.</li></ol>
Désarmé	Désigne l'état désactivé d'un système anti-intrusion, dans lequel l'apparition d'une condition d'alarme intrusion ou hold-up ne sera pas notifiée au centre de télésurveillance.
Destinataire	En gestion de l'intrusion, désigne l'entité choisie - généralement, un centre de télésurveillance - pour la réception des alarmes.
Détecteur	<p><b>Détecteur physique</b> : équipement dont le rôle est de détecter une intrusion dans une zone et qui fait appel à différents types de capteurs : contact magnétique, capteur infrarouge, capteur hyperfréquence... Un détecteur est équipé de deux contacts qui délivrent chacun une information : un contact d'alarme (contact AL qui mentionne une information de détection) et un contact d'autoprotection (contact AP qui fournit une information d'ouverture ou d'arrachement du détecteur). Chez TIL TECHNOLOGIES, un détecteur physique ne peut appartenir qu'à un seul <a href="#">groupe de détecteurs</a>.</p> <p><b>Détecteur virtuel</b> : détecteur logique défini à l'aide de registres internes à la TILLYS. Dans une configuration d'installation où un détecteur physique doit pouvoir appartenir à deux groupes de détecteurs, on lie son fonctionnement à celui d'un détecteur virtuel (par exemple par microcode). Le détecteur physique est alors déclaré dans un des groupes et le détecteur virtuel qui lui est associé est déclaré dans l'autre groupe.</p>
DHCP	Acronyme anglais de "Dynamic Host Configuration Protocol" (protocole de configuration dynamique des hôtes).

	<p>Protocole réseau dont la fonction est d'assurer la configuration automatique des paramètres <i>IP</i> d'un équipement réseau (PC, serveur, poste client ...), en lui attribuant une adresse IP, un masque de sous-réseau et une passerelle.</p>
DSSI	<p>Le Directeur de la Sécurité des Systèmes Informatiques d'un site est en charge de la sécurité de son réseau informatique: accès à Internet, firewall, gestion des adresses IP, des protocoles, de la sécurité des ports, de la protection contre les virus, etc.</p>
DTMF	<p>Acronyme anglais de Dual-Tone Multi-Frequency (FV pour fréquence vocale en français).</p> <p>Cette technologie permet de communiquer à distance avec un serveur vocal et d'envoyer à partir d'un centre de télésurveillance des commandes autorisant l'interpellation à distance et/ou activant des micros d'écoute.</p>
Éjection	<p>Action d'exclure de la surveillance, de manière momentanée ou définitive, un ou plusieurs détecteurs intrusion qui sont en condition de défaut, afin de permettre malgré tout la mise en surveillance d'un groupe ou pour éviter le déclenchement d'alarmes. Plusieurs types d'éjection peuvent être paramétrés : éjection manuelle, automatique, avec ou sans réinjection automatique, ou encore éjection permanente.</p>
Éjection automatique	<p>Mode permettant d'éjecter automatiquement un ou plusieurs points en défaut lors de l'armement du groupe les contenant. Ces points sont réinjectés lors du désarmement. Ce mode est particulièrement utile pour les armements automatiques.</p>
Éjection manuelle	<p>Intervention par laquelle un utilisateur permet l'armement d'un groupe de détecteurs malgré une condition de défaut sur un ou plusieurs détecteurs.</p>
Éjection permanente	<p>Mode permettant l'exclusion de points en dérangement sans devoir les éjecter à chaque armement de leur groupe.</p>
État de surveillance	<p>Statut d'un système anti-intrusion. Voir <a href="#">armé</a> et <a href="#">désarmé</a>.</p>
Fiche identifié	<p>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.</p>
Fonction clavier	<p>Fonction interne à la TILLYS liée à la fonction intrusion. Son paramétrage agit sur la gestion des groupes de détecteurs</p>

	concernés et la gestion du buzzer interne aux différents claviers définis.
Fonction intrusion	Fonction interne à la TILLYS qui consiste à surveiller les informations de détecteurs et à déclencher des alarmes sur leur changement d'état. Son paramétrage agit sur la création de détecteurs, groupes de détecteurs, sirènes, claviers, transmetteurs et profils opérateur intrusion (assignation des groupes et claviers gérés et droits sur la fonction intrusion). Elle intègre les notions de mise en ou hors service, temporisations (entrée et sortie), dérogation, éjection, inhibition, acquittement et transmission vers des télésurveilleurs.
Fonction sirène	Fonction interne à la TILLYS liée à la fonction intrusion. Son paramétrage agit sur les différents types de sonneries générées en fonction des événements, les comportements de la sirène principale et de la sirène auxiliaire et leur type de déclenchement, ainsi que l'assignation des groupes de détecteurs concernés.
Fonction transmission	<p>Fonction interne à la TILLYS liée à la fonction intrusion. Son paramétrage agit sur les déclarations de télésurveilleurs (appelés "destinataires" et au nombre maximal de 4), sur les protocoles exploités, sur les codes à transmettre et sur les profils d'appel désirés (appels simultanés ou backups). Sur RTC, les protocoles utilisés sont CESA 200 ou ID Contact. Sur la première version de l'intrusion, un protocole propriétaire TIL TECHNOLOGIES est utilisable sur <a href="#">IP</a>. Sur l'intrusion CUBE, le protocole IP standard utilisé est SIA-DCS (voir DC03).</p> <p>La fonction transmission permet également de définir jusqu'à 32 télécommandes par fonction intrusion, qui permettent à des opérateurs de télésurveillance d'effectuer des actions à distance sur le site, en fonction du niveau qui leur a été attribué (2, 9 ou 32 télécommandes).</p>
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.
Groupe de détecteurs	<p>Ensemble de détecteurs liés au sein d'un même bâtiment, étage, service ou autre par lien logique opérationnel et bénéficiant d'un mode de gestion commun pour :</p> <ul style="list-style-type: none"><li>● la mise en et hors surveillance,</li><li>● l'envoi de codes d'alarme vers un télésurveilleur,</li><li>● la gestion d'une ou de plusieurs sirènes,</li></ul>

- la mise en œuvre de pré-alarmes ou de mécanismes de dérogation.

32 groupes au maximum peuvent être déclarés par fonction intrusion.

Une sirène est normalement associée à un groupe de détecteurs.

GTB	<p>Acronyme de Gestion Technique des Bâtiments.</p> <p>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).</p>
Hostname	<p>Un "nom d'hôte" est un libellé permettant d'identifier un élément d'un réseau et est associé à son adresse IP. Dans le cas d'une configuration DHCP où les adresses <a href="#">IP</a> peuvent être modifiées, un équipement réseau peut être retrouvé grâce à son nom d'hôte.</p>
Identifiant	<p>Élément permettant l'accès d'un identifié. Les identifiants peuvent faire appel à plusieurs technologies (porte clé, carte, plaque minéralogique, empreinte digitale, code numérique...) et divers types de lecteur pour les lire.</p>
Identifié	<p>Personne devant disposer d'un accès au site protégé par le système de contrôle d'accès.</p> <p>Un identifié peut être porteur d'un ou de plusieurs identifiants distincts. Les identifiés peuvent être :</p> <ul style="list-style-type: none"><li>● Des personnes travaillant en permanence sur le site (identifié de type "permanent"),</li><li>● Des intervenants externes au site (identifié ayant une durée de validité spécifique correspondant à la durée de son intervention),</li><li>● Des personnes ayant accès de façon temporaire au site (identifié de type "visiteur").</li></ul>
Information de détecteur	<p>Information de type ToR issue d'un détecteur physique (radar, contact de porte, contact d'autoprotection ...) ou d'un détecteur virtuel (registre interne de la TILLYS).</p>
Inhibition	<p>Désigne l'état désactivé permanent d'une partie d'un système anti-intrusion, malgré l'apparition d'une condition d'alarme intrusion ou braquage. L'alarme n'est alors pas notifiée au centre de télésurveillance, jusqu'à son annulation manuelle.</p>

Intrusion	Changement d'état d'un détecteur qui déclenche une alarme lorsqu'une installation est en surveillance anti-intrusion.
IP	<p>Acronyme anglais d'Internet Protocol.</p> <p>Le protocole Internet permet aux équipements qui l'utilisent de communiquer entre eux par paquets, de type <a href="#">TCP</a> ou <a href="#">UDP</a>.</p> <p>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 <a href="#">RJ45</a> y ont accès physiquement et y sont identifiées logiquement via leur adresse IP.</p>
Lecteur	<p>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 :</p> <ul style="list-style-type: none"><li>● 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.</li><li>● 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 <i>CSN</i>).</li><li>● 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.</li></ul>
Maintenance	Mode de fonctionnement dégradé permettant de rétablir le fonctionnement normal d'un système, pendant une phase de diagnostic puis de résolution de problème.
Masque de sous-réseau	Adresse, d'un format similaire à celui d'une adresse IP, qui est utilisée au sein d'un réseau pour acheminer rapidement des paquets vers une destination particulière au sein de ce réseau, en évitant de passer par toute une série de routeurs.
Microcode	Langage de programmation spécifique exécuté par la TILLYS, qui permet de définir son fonctionnement face aux évènements qui lui sont transmis par l'ensemble des matériels avec lesquels elle est connectée.
MICROSESAME	Logiciel de supervision unifiée qui permet de centraliser toutes les informations électroniques du bâtiment : contrôle d'accès, détection intrusion, gestion technique, vidéo, interphonie...

	<p>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.</p>
Mise en service simplifiée	<p>En intrusion, mise en service proposée par défaut, lorsqu'un utilisateur se connecte à un clavier intrusion. La mise à jour simplifiée affiche trois groupes de détecteurs distincts : le premier recense l'ensemble des groupes définis dans la fonction intrusion, le second et le troisième sont les groupes dits "partiels" qui permettent la mise en service simultanée de groupes présélectionnés.</p>
Mode de connexion	<p><b>Par badge et/ou code</b> - Le passage d'un badge fait remonter les informations d'identification du code identifiant. La saisie d'un code intrusion autorise l'accès aux fonctions intrusion associées à un identifié.</p> <p><b>Hors ligne / en ligne</b> - Sur le terminal MOBILIS 3, définition du mode de fonctionnement. Ce dernier peut fonctionner soit en mode "Hors ligne", il fonctionne alors en mode autonome après avoir importé la base de données des identifiés depuis le serveur MICROSesame, soit en mode "En ligne", il est alors connecté au serveur MICROSesame par le biais d'une connexion Wifi.</p>
Nom d'hôte	<p>Libellé permettant d'identifier un élément de réseau en plus de son adresse <a href="#">IP</a>. En mode <a href="#">DHCP</a>, dans lequel l'adresse IP des matériels change de manière dynamique à chaque démarrage, ce nom permet de retrouver les éléments d'un même réseau malgré leur changement d'adresse IP.</p>
NTP	<p>Acronyme anglais de Network Time Protocol.</p> <p>Protocole permettant de synchroniser sur un réseau informatique l'horloge locale de plusieurs systèmes distincts sur l'heure d'un même serveur de référence.</p>
Paramétrage	<p>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.</p>
Partiel	<p>Sous-groupe d'un groupe de détecteurs qui met en ou hors-service simultanément plusieurs groupes de détecteurs définis (mise en service partielle). Deux profils partiels peuvent être</p>

	configurés par fonction intrusion et peuvent être affectés individuellement à chaque profil intrusion.
Passerelle	<p><b>Passerelle réseau</b> : équipement réseau qui assure le routage de paquets <a href="#">IP</a> entre plusieurs équipements. Il s'agit la plupart du temps de routeurs.</p> <p><b>Passerelle de communication</b> : licence optionnelle pouvant être achetée en vue de faire communiquer le serveur MICROSESAME avec des systèmes tiers (serveur LDAP, système biométrique MORPHO MANAGER ...).</p> <p><b>Passerelle d'import ou d'export</b> : licences optionnelles exploitant l'utilisation de fichiers CSV en vue de récupérer (import) ou de mettre à disposition (export) un ensemble d'informations liées aux identifiés du site.</p>
POE	<p>Acronyme anglais de Power Over Ethernet.</p> <p>Fonctionnalité réseau permettant de fournir une alimentation électrique sur le câble Ethernet.</p>
Polling	<p>Le polling est une fonction qui est utilisée lors de l'utilisation d'une communication <a href="#">IP</a>. Sa périodicité est paramétrable en secondes sur la TILLYS. Elle permet au télésurveilleur de vérifier que la liaison entre la TILLYS et le frontal fonctionne.</p>
Port	<p>Point d'entrée à un service (service web, service DNS, service mail...) sur un équipement (PC, serveur...) connecté à un réseau. Les ports constituent des accès entrants ou sortants et ils permettent aux différents logiciels et/ou systèmes d'exploitation de communiquer entre eux.</p>
Pré-alarme	<p>Dans la fonction intrusion, la pré-alarme définit la temporisation existant entre une demande de mise en service qui a été faite et le démarrage effectif de la surveillance. L'utilisation de la pré-alarme est souvent mise en œuvre pour pouvoir gérer les dérogations. Générant une sonnerie spécifique dès son lancement, la pré-alarme permet d'avertir les occupants potentiels de l'imminence de la mise en surveillance d'une zone, tout en leur laissant la possibilité d'effectuer une dérogation.</p>
Prêt pour mise en surveillance	<p>État d'un groupe de détecteurs indiquant qu'une mise en surveillance est possible sans qu'il soit nécessaire de procéder à l'éjection de détecteurs.</p>
Profil d'accès	<p>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.</p>

	<p>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.</p>
Profil intrusion	<p>Ensemble de groupes de détecteurs sur lesquels peut agir un opérateur intrusion. Ce profil est composé d'un maximum de trois listes de groupes de détecteurs ou d'informations de détecteurs : un groupe de base, permettant la mise en/hors service d'un ensemble de groupes définis, et deux sous-groupes (partiels), permettant la mise en /hors service partielle de l'installation.</p>
Protocole de communication	<p>Ensemble de règles et conventions permettant la communication et l'interopérabilité entre différents systèmes informatiques.</p> <p>Le protocole définit la structure du message envoyé au destinataire. Les protocoles suivants sont utilisables entre la TILLYS et un centre de télésurveillance :</p> <ul style="list-style-type: none"><li>● CESA 200: chaque événement transmis est constitué d'un code numérique de 01 à 96.</li><li>● ID-Contact: chaque événement est constitué de deux codes numériques, un code de type ou de catégorie de 001 à DDD et un deuxième code de type d'événement pour un type donné de 001 à 999. Celui-ci permet également de transmettre le numéro de l'utilisateur mettant en/hors service un groupe.</li></ul>
Réinjection automatique	<p>Mode permettant la réintégration automatique des points qui ont été éjectés au moment de la mise en surveillance parce qu'ils étaient en défaut, dès qu'ils auront retrouvé un état normal et ceci sans attendre la prochaine mise hors surveillance (exemple : fenêtre ouverte ou refermée).</p>
RJ45	<p>Format de connecteur à 8 contacts électriques utilisé en téléphonie et pour les réseaux Ethernet.</p>
RS 485	<p>Norme de communication utilisée dans l'industrie. Sa mise en œuvre par TIL TECHNOLOGIES permet de connecter à la <a href="#">TILLYS</a> des matériels en bus et/ou en étoile jusqu'à 600 mètres de distance.</p>
RTC	<p>Acronyme de Réseau Téléphonique Commuté, qui est le système historique de téléphonie analogique sur paires torsadées, cette technologie est à l'origine conçue pour transporter les communications vocales, avant de transporter des données codées puis décodées (par modem puis modem ADSL). Ce</p>

	<p>système est souvent utilisé en opposition à <a href="#">VoIP</a>, qui désigne quant à lui le transport de communications vocales sur un support prévu à l'origine pour le transport de données numériques.</p>
Sonnerie intrusion	<p>Mélodie personnalisable qui se configure en additionnant les caractères "+" et "-" dans une même chaîne. Toutes les sonneries sont liées aux différents types d'alarmes (intrusion, 24/24H, technique, appel d'urgence, incendie).</p>
Supervision	<p>Surveillance du bon fonctionnement d'un système ou d'une activité, qui permet de faire la distinction entre les fonctionnements normaux et anormaux et d'alerter si nécessaire.</p>
Table de codage	<p>Une table de codage est un tableau où l'on va définir un code événement pour chaque type d'alarme (intrusion, incendie, etc.) qui sera envoyé au télésurveilleur. Ces codes sont donc à définir avec le télésurveilleur choisi.</p>
TACTILLYS	<p>Clavier tactile TIL TECHNOLOGIES dédié à la gestion de l'intrusion, équipé d'un écran couleur 7 pouces. Raccordé sur un bus RS 485 de la TILLYS, il permet à un opérateur intrusion de s'authentifier, afin d'accéder à certaines actions paramétrées dans la fonction intrusion. Il peut être équipé d'un lecteur de badge qui se substitue au code à saisir, ou au contraire qui renforce l'authentification nécessaire d'un opérateur intrusion (passage d'un badge + saisie d'un code).</p>
TACTILLYS-IP CUBE	<p>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.</p>
TCP	<p>Acronyme anglais de Transmission Control Protocol.</p> <p>Protocole de communication bidirectionnel très fiable, utilisé avec <a href="#">IP</a> et fonctionnant en mode connecté. L'émetteur s'assure ainsi que toutes les données transmises ont bien été réceptionnées par le récepteur.</p>
Temporisation d'entrée	<p>Délai prévu pour permettre à un utilisateur détecté d'effectuer la mise hors surveillance avant le déclenchement de l'alarme.</p>
Temporisation d'entrée / de sortie	<p>Délai prévu pour permettre l'entrée ou la sortie de l'utilisateur de la zone surveillée sans déclenchement de la sirène, si le clavier de mise en/hors surveillance est en zone surveillée.</p>

Temporisation de dérogation	Durée paramétrable entre 1 et 5 minutes afin de retarder le début de mise en surveillance d'un ou groupe de détecteur(s).
Temporisation de mise en service	Aussi appelée temporisation de pré-alarme, durée paramétrable en secondes permettant de prévenir l'utilisateur de la mise en surveillance imminente des détecteurs.
Temporisation de sortie	Délai prévu avant déclenchement de l'alarme en cas de détection d'un intrus, afin de permettre à un utilisateur venant de déclencher la mise en surveillance d'une zone d'en sortir malgré sa détection.
Terminal intrusion	<p>Il s'agit d'un TACTILLYS-IP CUBE dédié à la fonction intrusion d'une TILLYS . Les terminaux intrusion CUBE sont connectés via <a href="#">IP</a>. 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.</p> <p>Les terminaux intrusion permettent l'armement et le désarmement de leurs groupes de détecteurs, l'acquiescement 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.</p>
Test cyclique	Opération périodique réalisée par la TILLYS et consistant à effectuer une transmission vers un télésurveilleur pour vérifier le fonctionnement de la ligne de communication. Sa périodicité est paramétrable en minutes sur la TILLYS. La transmission du test cyclique peut être calée ou non sur une heure précise ou être liée à la mise en service d'un ou de plusieurs groupes. Il est possible de paramétrer un test cyclique par destinataire.
TILLYS	Automate <a href="#">IP</a> programmable multifonction développé par TIL TECHNOLOGIES qui dispose des fonctionnalités de contrôle d'accès, de détection intrusion et de <a href="#">GTB</a> . 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 <a href="#">UTL</a> .
ToR	<p>Acronyme de "Tout ou Rien".</p> <p>Cette entrée fonctionne selon deux niveaux logiques qui ne peuvent prendre que la valeur 0 (ouvert) ou 1 (fermé).</p>
UDP	Acronyme anglais de User Datagram Protocol.

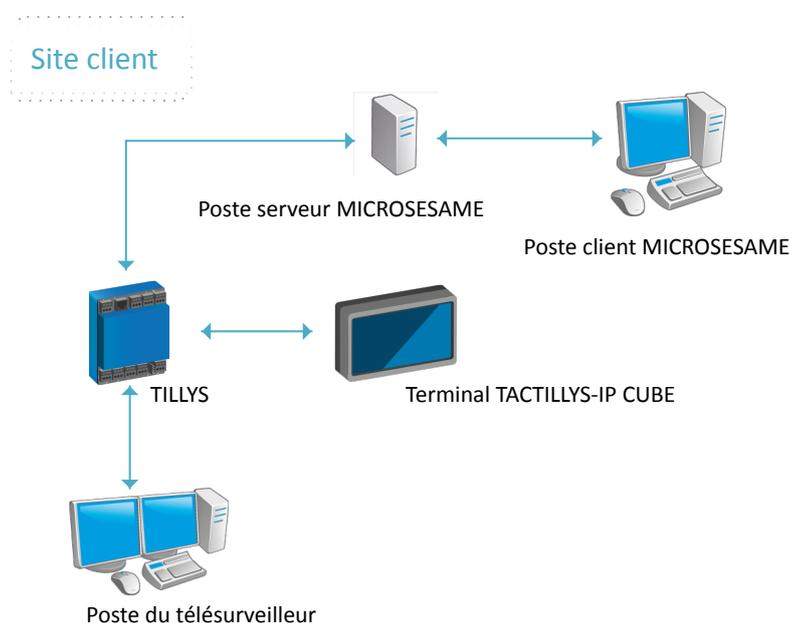
	<p>Protocole de communication très léger mais peu fiable, adapté aux applications où la perte de données occasionnelle est acceptable, comme le streaming en temps réel.</p>
Utilisateur TILLYS	<p>Personne autorisée à s'identifier sur un clavier de commande de la centrale <a href="#">TILLYS</a>, du type TACTILLYS ou TACTILLYS-IP. Chaque utilisateur est associé à un profil d'intrusion, à des droits d'utilisation et à un code d'identification.</p>
UTL	<p>Acronyme d'Unité de Traitement Local.</p> <p>Automate <a href="#">IP</a> programmable et multifonction qui est 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 <a href="#">TILLYS</a>.</p>
VoIP	<p>Acronyme anglais de Voice over Internet Protocol.</p> <p>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.</p>
WEBSesame	<p>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 parle dans ce cas de <a href="#">client léger</a>.</p>

# Chapitre 1. Contexte de la détection d'intrusion CUBE

## 1.1. Vue d'ensemble de la version de base de l'intrusion CUBE

L'architecture matérielle est du type représentée sur le diagramme ci-après.

**Figure 1.1. Architecture matérielle de la version de base de l'intrusion CUBE (10010-001)**



La TILLYS à laquelle le terminal TACTILLYS-IP CUBE est relié gère le groupe de détecteurs. Ses détecteurs et sirènes sont gérables :

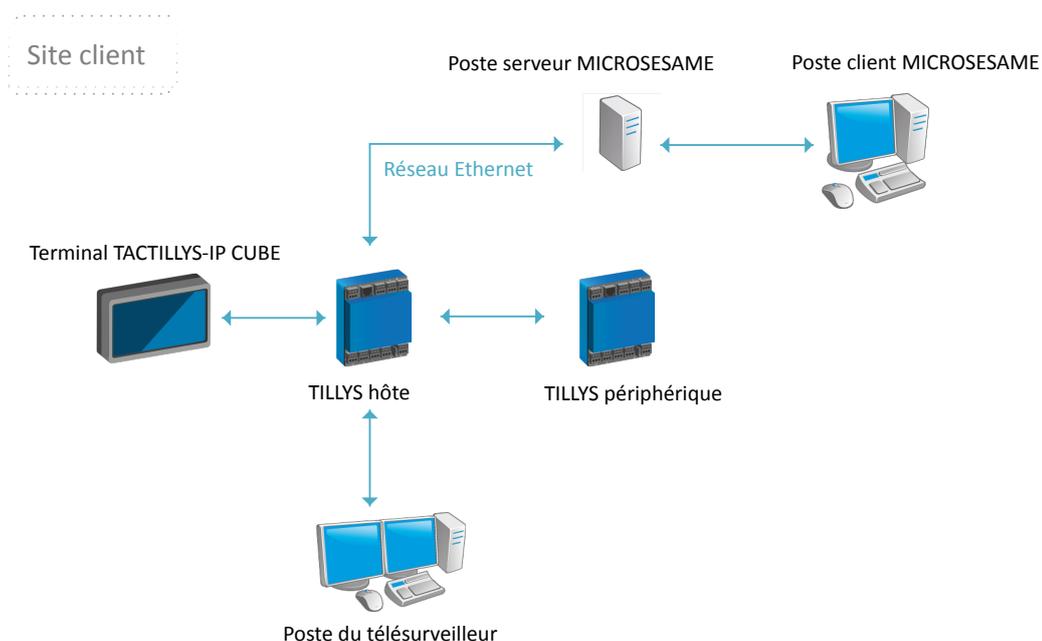
- par le terminal TACTILLYS-IP CUBE,
- par le poste client MICROSESAME,
- par le poste du télésurveilleur.

## 1.2. Vue d'ensemble de la version multi-TILLYS de l'intrusion CUBE

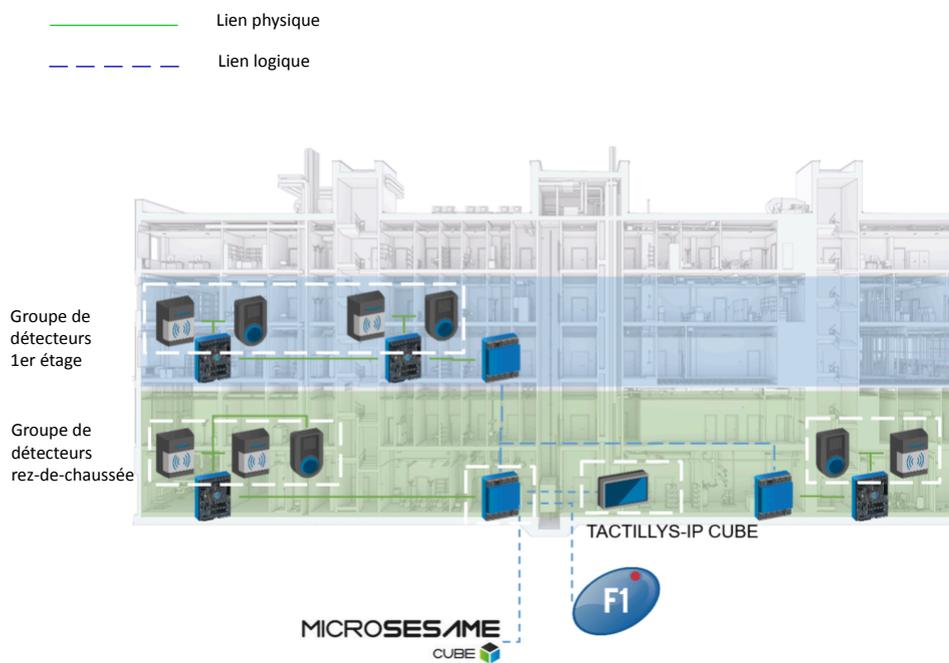
S'il est nécessaire de répartir détecteurs et sirènes sur plusieurs TILLYS, ceci est désormais possible en utilisant une TILLYS hôte et une ou plusieurs TILLYS périphériques reliées en IP sur un réseau Ethernet.

Les détecteurs et les sirènes des TILLYS périphériques sont alors reliés de manière virtuelle au groupe de détecteurs de la TILLYS hôte, qui les gère comme s'ils lui étaient physiquement connectés.

**Figure 1.2. Architecture matérielle de la version multi-TILLYS de l'intrusion CUBE (10010-002)**



Le schéma ci-après représente dans un bâtiment, les liens physiques entre les détecteurs et leurs TILLYS, et les liens logiques sur IP. Ces derniers permettent de déclarer des détecteurs et des sirènes virtuels sur la TILLYS hôte, ainsi que de communiquer avec MICROSESAME et avec les systèmes de télésurveillance comme F1.

**Figure 1.3. Configuration multi-TILLYS de l'intrusion CUBE (10010-003)**

### 1.3. Nouveautés et avantages de l'intrusion CUBE

La solution intrusion CUBE propose quatre nouveautés marquantes par rapport à la version précédente :

- L'utilisation d'[IP](#) au lieu du [bus RS 485](#) entre le terminal [TACTILLYS-IP CUBE](#) et la [TILLYS](#).
- La configuration est effectuée au niveau de la [TILLYS](#), avant la remontée des informations dans [MICROSESAME](#).
- La logique Normalement Fermé est généralisée au niveau des détecteurs.
- La mise en service est possible sans saisir une ligne de microcode.

En termes fonctionnels, l'intrusion CUBE présente quatre avantages qualitatifs déterminants par rapport à l'offre du marché :

- Une cybersécurisation du même niveau que celle du contrôle d'accès, qui est certifié ANSSI.
- Une intégration de la supervision, par l'utilisation d'objets détecteurs, de groupes de détecteurs et de sirènes.
- Une ergonomie d'exploitation améliorée, grâce à la mise en place d'objets de supervision et de widgets natifs, animés dans MICROSESAME.
- Une puissance accrue en termes de fonctionnalités de télésurveillance, grâce à des terminaux IP multi-centrales et à l'utilisation de la transmission SIA.

## 1.4. Définition du fonctionnement attendu par le responsable sécurité

Le responsable sécurité définit le fonctionnement attendu, dans un **cahier des charges** ou un **descriptif fonctionnel**.

Ce document, ainsi que le **plan d'adressage réseau**, permettent au partenaire TIL TECHNOLOGIES de définir les zones du contrôle d'accès et les groupes de détection d'intrusion dans ses locaux, avant d'aller les déployer sur le site de son client.

## 1.5. Prérequis intrusion CUBE à mettre en place par le DSSI du client

Comme le transfert des données d'intrusion est effectué par réseau [IP](#), les normes ci-après sont applicables.

**Tableau 1.1. Normes de sécurité informatique applicables**

Titre de la norme	Référence et lien
SIA Digital Communication Standard - Internet Protocol Event reporting	<a href="#">[SIA-DC-09]</a>
Security Communications – Digital Communications Standard - “SIA Format” Protocol - for Alarm System Communications	<a href="#">[SIA-DC-03]</a>
SIA Digital Communications Standard – Receiver-to-Computer Interface Protocol – for Central Station Equipment Communications	<a href="#">[SIA-DC-07]</a>

## 1.6. Gestion de l'intrusion CUBE

Cette section propose un grand tableau des opérations possibles en fonction de l'état du système anti-intrusion.

**Tableau 1.2. Liste des opérations de gestion de l'intrusion avec leur contexte et leur mode opératoire**

Etat d'alarme	Quoi et comment ?	Pourquoi ?	Où et par qui ?
Avant armement	Paramétrage des groupes  Temporisation d'entrée  Temporisation de sortie  <i>Éjection automatique</i>  Réinjection automatique  <i>Éjection permanente</i>	Déterminer ce qu'il est possible de faire au niveau de la gestion de l'intrusion et qui a le droit d'effectuer ces opérations.	TILLYS hôte (responsable sécurité)
En pré-alarme	<i>Dérogation</i> sur un groupe de détecteurs	Permettre à un ou plusieurs employés de rester travailler après l'heure de fin, dans une zone déterminée, pendant une durée à choisir dans une liste de valeurs.  Éjecter un groupe en défaut.	Terminal TACTILLYS-IP CUBE (utilisateur avec droits intrusion)
En dérogation	Armer l' <i>alarme</i>	Mettre fin à la dérogation et armer l'alarme.	Terminal TACTILLYS-IP CUBE (utilisateur avec droits intrusion)
En pré-alarme	<i>Éjection manuelle</i> d'un détecteur en défaut	Permettre l'armement du groupe.  Éviter de déclencher l'alarme en quittant les locaux avant la fin de la temporisation de sortie	Terminal TACTILLYS-IP CUBE (utilisateur avec droits intrusion)

Etat d'alarme	Quoi et comment ?	Pourquoi ?	Où et par qui ?
Sur le chemin de sortie	Quitter les locaux au plus vite	Éviter de déclencher l'alarme en quittant les locaux avant la fin de la temporisation de sortie	Terminal TACTILLYS-IP CUBE (utilisateur avec droits intrusion)
Alarme armée	Badger sur la porte d'entrée	Atteindre le terminal TACTILLYS-IP CUBE pendant la temporisation d'entrée	Lecteur de contrôle d'accès (utilisateur avec droits intrusion)
Sur le chemin d'entrée	Badger sur le TACTILLYS-IP CUBE pour désarmer l'alarme	Entrer dans les locaux en dehors des heures de travail	Terminal TACTILLYS-IP CUBE (utilisateur avec droits intrusion)
Alarme désarmée	Badger pour entrer dans le bâtiment  Modifier certains paramètres	Accéder aux locaux pendant les heures de travail  Adapter la configuration anti-intrusion aux besoins	Lecteur de contrôle d'accès  TILLYS hôte (responsable sécurité)

## 1.7. Informations de référence pour les intégrateurs

### 1.7.1. Formats des trames échangées entre TILLYS et terminaux de télésurveillance

Cette partie et ses trois sections fournit aux **intégrateurs** une documentation de référence extraite des normes SIA DC-09 et SIA DC-03, ainsi que des exemples de sa mise en œuvre par TIL TECHNOLOGIES.

La TILLYS transmet des trames au format SIA DC-09 qui transportent des charges utiles au format SIA DC-03. Comme ce format peut être sujet à interprétation, les codes SIA DC-03 transmis par la TILLYS aux télésurveilleurs, ainsi que les télécommandes envoyées par les télésurveilleurs à la TILLYS sont détaillés dans les trois sections ci-après.

#### 1.7.1.1. Codes intrusion transmis par les détecteurs aux télésurveilleurs

Pour que les codes intrusion soient transmis pour un détecteur, l'interrupteur **Transmettre des alarmes** doit être actif dans la section **Informations générales** de ce détecteur (voir [Section 3.2.1.6, « Configuration des détecteurs intrusion CUBE d'une TILLYS »](#)).

Le tableau ci-après contient la liste des codes intrusion liés aux détecteurs.

**Tableau 1.3. Liste complète des codes intrusion envoyés par les détecteurs**

Type de signal	Apparition alarme	Disparition alarme	Inhibition	Désinhibition	Éjection	Réinjection
Intrusion	BA	BR	BB	BU	XW	BU
24/24	TA	TR	TB	TU	VW	TU
Intrusion silencieuse	BA	BR	BB	BU	XW	BU
Défaut système	IA	IR	UB	UU	XW	UU
Défaut système silencieux	IA	IR	UB	UU	XW	UU
Urgence	QA	QR	QB	QU	XW	QU
Incendie	FA	FR	FB	FU	XW	FU

Le tableau ci-après donne la signification de ces codes, en anglais puis en français.

**Tableau 1.4. Signification des codes intrusion envoyés par les détecteurs**

Code	Description courte	Description longue	Traduction
BA	Burglary Alarm	Burglary zone has been violated while armed	Intrusion ou intrusion silencieuse sur zone anti-intrusion armée
BR	Burglary Restoral	Alarm/trouble condition has been eliminated	Disparition de l'état d'alarme ou de défaut
BB	Burglary Bypass	Burglary zone has been bypassed	Le signal d'intrusion ou d'intrusion silencieuse sur une zone a été inhibé
BU	Burglary Unbypass	Zone bypass has been removed	Désinhibition ou réinjection d'une zone d'intrusion ou d'intrusion silencieuse
FA	Fire Alarm	Fire condition detected	Apparition d'une alarme de type incendie

Code	Description courte	Description longue	Traduction
FR	Fire Restoral	Alarm/trouble condition has been eliminated	Disparition de l'alarme ou du défaut de type incendie
FB	Fire Bypass	Zone has been bypassed	L'alarme incendie apparue sur une zone a été inhibée
FU	Fire Unbypass	Bypass has been removed	Désinhibition d'une alarme incendie sur une zone ou réinjection de cette zone
IA	Equipment Failure Condition	A specific, reportable condition is detected on a device	Apparition d'une alarme sur signal de type défaut système ou défaut système silencieux
IR	Equipment Fail - Restoral	The equipment condition has been restored to normal	Disparition de l'alarme sur signal de type défaut système ou défaut système silencieux
UB	Untyped Zone Bypass	Zone of unknown type has been bypassed	Inhibition du signal de type défaut système ou défaut système silencieux
UU	Untyped Zone Unbypass	Bypass has been removed	Désinhibition ou réinjection du signal de type défaut système ou défaut système silencieux
QA	Emergency Alarm	Emergency assistance request	Apparition d'alarme sur signal de type urgence
QR	Emergency Restoral	Alarm/trouble condition has been eliminated	Disparition d'alarme sur signal de type urgence

Code	Description courte	Description longue	Traduction
QB	Emergency Bypass	Zone has been bypassed	Inhibition de signal de type urgence sur une zone
QU	Emergency Unbypass	Bypass has been removed	Désinhibition ou réinjection signal de type urgence sur une zone
TA	Tamper Alarm	Alarm equipment enclosure opened	Coffret de protection d'alarme ouvert (apparition d'alarme sur signal de type 24/24)
TR	Tamper Restoral	Alarme equipment enclosure has been closed	Coffret de protection d'alarme refermé (disparition d'alarme sur signal de type 24/24)
TB	Tamper Bypass	Tamper detection has been bypassed	La détection d'autoprotection a été inhibée (inhibition d'alarme sur signal de type 24/24)
TU	Tamper Unbypass	Tamper detection bypass has been removed	La détection d'autoprotection a été désinhibée (désinhibition ou réinjection de signal de type 24/24)
XW	Forced Point	A point was forced out of the system at arm time	Un point a été éjecté de force du système au moment de son armement (éjection du signal, quelqu'en soit le type)

La valeur transmise dans le champ d'adresse (address field) est celle du numéro de signal du détecteur.

### 1.7.1.2. Codes évènements transmis par les groupes aux télésurveilleurs

Pour que les codes évènement soient transmis pour un groupe, l'interrupteur **Transmettre l'armement / le désarmement** doit être actif dans la section **Informations générales** de ce détecteur (voir [Section 3.2.1.2, « Configuration d'un groupe de détecteurs intrusion CUBE »](#)).

Le tableau ci-après liste et décrit la liste des codes évènements liés aux groupes.

**Tableau 1.5. Signification des codes évènements envoyés par les groupes**

Code	Description courte	Description longue traduite	Complément d'informations
CA	Automatic Closing	Armement automatique du système	Zone ou point
OA	Automatic opening	Désarmement automatique du système	Zone ou point
CI	Fail to close	Échec d'armement automatique	Numéro de zone
CE	Closing Extend	Dérogation, pour repousser l'armement	Numéro d'utilisateur

La valeur transmise dans le champ d'adresse (address field) est celle du numéro du groupe.

### 1.7.1.3. Télécommandes envoyées à la TILLYS par les télésurveilleurs

Les télécommandes du tableau ci-après peuvent être utilisées.

**Tableau 1.6. Liste des télécommandes pouvant être envoyées par les télésurveilleurs à la TILLYS**

Code	Description courte	Informations complémentaires	Signification
SA	Set Area	x*y set area x to y, (3 = User Defined, 2 = Perimeter Only, A = Armed, 0 = Disarmed)	Commande d'armement ou de désarmement d'une zone
SB	Set Bypass	x*y set bypass on zone x to y (1 = ON, 0 = OFF)	Commande d'inhibition ou de désinhibition d'un groupe

Code	Description courte	Informations complémentaires	Signification
SS	Set Sounder	x*y set sounder x to y (1 = ON, 0 = OFF)	Commande d'arrêt ou de déclenchement d'une sirène
TP	Trap Account	Compte utilisé pour la programmation à distance	Commande de modification de la valeur d'un registre personnalisé "custom TIL"

Pour chaque télécommande, il est nécessaire de préciser le numéro de groupe pour l'armement, et le délai associé à l'armement et au désarmement (immédiat ou avec pré-alarme), le numéro de signal de détecteur pour la commande d'inhibition, le numéro de sirène pour l'arrêt sirène, le registre et sa valeur pour la télécommande TP, etc.

## 1.7.2. Valeurs du registre numérique d'état des groupes en intrusion CUBE

Ces informations s'adressent aux **intégréateurs**.

Le registre numérique d'état des groupes est défini par l'attribut regStatus de la balise group. Chaque bit de ce registre correspond à une information conformément au tableau ci-après.

**Tableau 1.7. Valeurs possibles du registre numérique d'état des groupes**

Bit index	Masque hexadécimal	Description	Commentaire
0	0x1	1 = au moins un défaut de type "Alarme intrusion" dans le groupe  0 = aucun défaut de type "Alarme intrusion" dans le groupe	Équivaut au registre <a href="#">ToR</a> de synthèse qui peut être défini pour le type "Alarme intrusion"
1	0x2	1 = au moins un défaut de type "Alarme 24/24" dans le groupe  0 = aucun défaut de type "Alarme 24/24" dans le groupe	Équivaut au registre ToR de synthèse qui peut être défini pour le type "Alarme 24/24"
2	0x4	1 = au moins un défaut de type "Alarme intrusion silencieuse" dans le groupe	Équivaut au registre ToR de synthèse qui peut être défini pour le type "Alarme intrusion silencieuse"

Bit index	Masque hexadécimal	Description	Commentaire
		0 = aucun défaut de type "Alarme intrusion silencieuse" dans le groupe	
3	0x8	1 = au moins un défaut de type "Défaut système" dans le groupe 0 = aucun défaut de type "Défaut système" dans le groupe	Équivaut au registre ToR de synthèse qui peut être défini pour le type "Défaut système"
4	0x10	1 = au moins un défaut de type "Appel d'urgence" dans le groupe 0 = aucun défaut de type "Défaut système" dans le groupe	Équivaut au registre ToR de synthèse qui peut être défini pour le type "Appel d'urgence"
5	0x20	1 = au moins un défaut de type "Défaut système" dans le groupe 0 = aucun défaut de type "Défaut système" dans le groupe	Équivaut au registre ToR de synthèse qui peut être défini pour le type "Incendie"
6	0x40	1 = au moins un défaut de type "Défaut système silencieux" dans le groupe 0 = aucun défaut de type "Défaut système silencieux" dans le groupe	Équivaut au registre ToR de synthèse qui peut être défini pour le type "Défaut système silencieux"
16	0x10000	1 = groupe armé 0 = groupe désarmé	
17	0x20000	1 = au moins une alarme en attente d'acquiescement 0 = aucune alarme en attente d'acquiescement	
18	0x40000	1 = pré-alarme en cours 0 = pas de pré-alarme en cours	
19	0x80000	1 = dérogation en cours	

Bit index	Masque hexadécimal	Description	Commentaire
		0 = pas de dérogation en cours	
20	0x100000	1 = temporisation de sortie en cours  0 = pas de temporisation de sortie en cours	
21	0x200000	1 = temporisation d'entrée en cours  0 = pas de temporisation d'entrée en cours	

### 1.7.3. Registres du microcode, propres à l'intrusion CUBE

Les registres ci-après ont été créés, pour une utilisation dans MICROSESAME.

Deux nouveaux registres sont utilisés pour définir les détecteurs physiques : AL\_DETECTEUR\_ID et AP\_DETECTEUR\_ID.

Deux registres virtuels ont également été créés : ENTRE\_AL\_DETECTEUR\_ID et ENTRE\_AP\_DETECTEUR\_ID.

Enfin, de nouveaux types de registres sont utilisés pour gérer l'éjection des détecteurs : EJ\_DETECTEUR\_ID.

### 1.7.4. Fonction du microcode permettant de remonter les informations d'AP d'un TACTILLYS-IP CUBE

La fonction GET\_AP\_TACTILLYS a été créée en V3 pour faire remonter les informations d'autoprotection du TACTILLYS-IP CUBE dans MICROSESAME.

Cette commande permet de faire remonter l'état d'alarme du signal d'AP d'un détecteur en intrusion CUBE, avec 1 pour le signal en alarme et 0 pour l'absence d'alarme.

Cette fonction comporte comme unique argument l'ID du TACTILLYS-IP CUBE, sous la forme d'un nombre entier.

## Chapitre 2. Workflows intrusion CUBE

Ce chapitre fournit des processus opérationnels par profil utilisateur (partenaire, installateur ou agent d'accueil).

D'autres chapitres contiennent des instructions destinées :

- au responsable sécurité (voir [Chapitre 6, Gestion de la sécurité par le responsable sécurité](#)),
- aux personnes habilitées à utiliser le terminal TACTILLYS-IP CUBE (voir [Section 4.3, « Utilisation du TACTILLYS-IP CUBE »](#)),
- aux concepteurs de systèmes tiers de télésurveillance (voir [Section 1.7.1, « Formats des trames échangées entre TILLYS et terminaux de télésurveillance »](#)).

### 2.1. Préparation du site informatique

S'il s'agit d'une première mise en service, se reporter au [Guide de démarrage rapide \(GD-10001-FR\)](#).

### 2.2. Configuration intrusion CUBE par le partenaire avec préparation dans ses locaux

#### 2.2.1. Workflow - Pré-configuration intrusion CUBE par le partenaire dans ses locaux

La partenaire effectue dans ses locaux les opérations suivantes, en amont de sa visite en clientèle :

1. Connexion physique du PC portable au réseau Ethernet
2. [Section 3.2.1.1, « Accès à l'interface d'administration de l'intrusion CUBE sur une TILLYS »](#)
3. [Section 3.2.1.2, « Configuration d'un groupe de détecteurs intrusion CUBE »](#)
4. [Section 3.2.1.6, « Configuration des détecteurs intrusion CUBE d'une TILLYS »](#)
5. [Section 3.2.1.8, « Configuration d'une sirène intrusion CUBE »](#)
6. [Section 3.2.2.1, « Création des profils intrusion sur la TILLYS hôte »](#)
7. [Section 3.2.1.11, « Association d'un terminal TACTILLYS-IP CUBE à un ou plusieurs groupes d'une TILLYS hôte »](#)
8. [Section 3.2.1.12, « Configuration des télésurveilleurs »](#)
9. Continuer avec les étapes du [Section 2.2.2, « Workflow - Export/import du paramétrage intrusion CUBE »](#) : export de la configuration réalisée par le partenaire dans ses locaux, puis import de cette configuration sur le site du client.

#### 2.2.2. Workflow - Export/import du paramétrage intrusion CUBE

Ces deux processus permettent :

- de préparer à l'avance une configuration intrusion CUBE,
- de sauvegarder une configuration intrusion CUBE pour aller la copier sur une autre TILLYS,
- de copier une configuration intrusion CUBE sur le site d'un client,
- de restaurer la configuration d'une TILLYS, pour rétablir une configuration intrusion CUBE sauvegardée ou en cas de remplacement de cette TILLYS.

Pour exporter ou pour sauvegarder une configuration intrusion :

1. [Section 3.2.4.1, « Activation ou désactivation du port de maintenance d'une TILLYS »](#)
2. [Section 3.2.4.2, « Exporter ou importer un fichier de configuration intrusion CUBE »](#)

Pour importer ou pour restaurer une configuration intrusion sauvegardée :

1. [Section 3.2.4.1, « Activation ou désactivation du port de maintenance d'une TILLYS »](#)
2. [Section 3.2.4.2, « Exporter ou importer un fichier de configuration intrusion CUBE »](#)
3. Continuer sur le site du client avec le [Section 2.3.1, « Workflow - Configuration intrusion CUBE sur le site du client »](#)

## 2.3. Configuration intrusion CUBE par le partenaire sur le site du client

### 2.3.1. Workflow - Configuration intrusion CUBE sur le site du client

Le partenaire effectue les opérations suivantes directement en clientèle :

1. Connexion physique du PC portable au réseau Ethernet
2. [Section 3.2.1.1, « Accès à l'interface d'administration de l'intrusion CUBE sur une TILLYS »](#)
3. [Section 3.2.1.2, « Configuration d'un groupe de détecteurs intrusion CUBE »](#)
4. [Section 3.2.1.6, « Configuration des détecteurs intrusion CUBE d'une TILLYS »](#)
5. [Section 3.2.1.8, « Configuration d'une sirène intrusion CUBE »](#)
6. [Section 3.2.2.1, « Création des profils intrusion sur la TILLYS hôte »](#)
7. [Section 3.2.1.11, « Association d'un terminal TACTILLYS-IP CUBE à un ou plusieurs groupes d'une TILLYS hôte »](#)
8. [Section 3.2.1.12, « Configuration des télésurveilleurs »](#)
9. Continuer avec [Section 2.3.2, « Workflow - Configuration d'un badge d'accès au terminal TACTILLYS-IP CUBE »](#)

### 2.3.2. Workflow - Configuration d'un badge d'accès au terminal TACTILLYS-IP CUBE

L'agent d'accueil peut préparer des badges d'accès avec droits intrusion.

1. [Section 5.2.1, « Préparation d'un badge de contrôle anti-intrusion »](#)
2. [Section 5.2.2, « Acquisition d'un identifiant non attribué dans MICROSESAME »](#)

3. [Section 5.2.3, « Affectation d'un identifiant disponible à un nouvel identifié »](#)
4. [Section 5.2.4, « Attribution de droits d'accès à un nouvel identifié »](#)
5. [Section 5.2.5, « Attribution d'un profil intrusion CUBE à un nouvel identifié »](#)
6. Continuer avec [Section 2.3.3, « Workflow - Installation, configuration et paramétrage d'un terminal TACTILLYS-IP CUBE avant sa mise en service »](#)

### 2.3.3. Workflow - Installation, configuration et paramétrage d'un terminal TACTILLYS-IP CUBE avant sa mise en service

Lors d'une première mise en service, le partenaire ou l'installateur doit effectuer successivement les opérations suivantes :

1. [Section 4.1.1, « Installation physique et connexion d'un terminal TACTILLYS-IP CUBE »](#)
2. [Section 4.1.2, « Accès à l'interface d'administration du terminal TACTILLYS-IP CUBE et affichage des caractéristiques produit »](#)
3. [Section 4.2.2, « Consultation des caractéristiques de fonctionnement du TACTILLYS-IP CUBE »](#)
4. [Section 4.2.3, « Paramétrage du TACTILLYS-IP CUBE »](#)
5. [Section 4.1.3, « Changement du mot de passe administrateur du terminal TACTILLYS-IP CUBE »](#)
6. [Section 4.1.6, « Mise à jour du firmware du TACTILLYS-IP CUBE »](#)
7. [Section 4.1.4, « Réglage de l'heure du terminal TACTILLYS-IP CUBE »](#)
8. [Section 4.1.5, « Paramétrage réseau du TACTILLYS-IP CUBE »](#)
9. [Section 5.1, « Import de la configuration intrusion CUBE dans MICROSESAME »](#)

## Chapitre 3. Paramétrage de l'intrusion CUBE par le partenaire

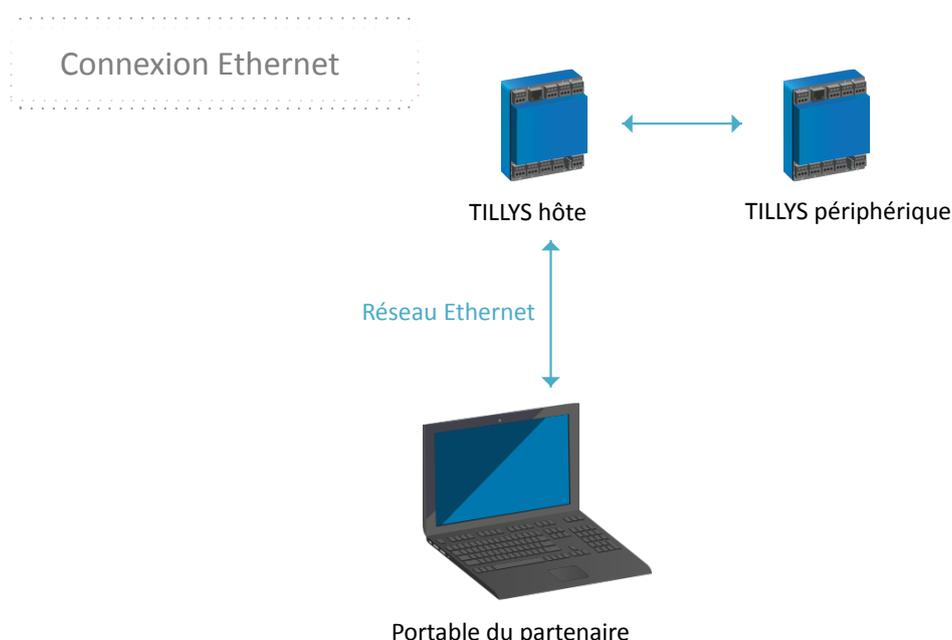
Avec l'intrusion CUBE, la quasi totalité des opérations de paramétrage est maintenant effectuée au niveau de la TILLYS. Ceci permet aux partenaires de préparer à l'avance la configuration des TILLYS pour en effectuer ensuite le chargement rapide sur site, avant d'installer le ou les terminaux TACTILLYS-IP CUBE. Toutes ces opérations peuvent être effectuées et être opérationnelles avant même l'installation de MICROSESAME.

### 3.1. Architecture matérielle de configuration de l'intrusion CUBE par le partenaire

Le partenaire peut effectuer la configuration chez son client final, mais il peut également préparer une configuration intrusion CUBE dans ses propres locaux, avant de se déplacer pour la mettre en place sur le site du client. L'architecture matérielle nécessaire est simplement constituée :

- D'un ordinateur portable connecté à Ethernet,
- D'une ou plusieurs TILLYS (configuration multi-TILLYS), connectées au même réseau Ethernet.

**Figure 3.1. Configuration de l'intrusion CUBE via Ethernet (10010-004)**



## 3.2. Configuration, paramétrage et maintenance intrusion CUBE sur la TILLYS

Les opérations de configuration du dispositif de détection d'intrusion (à télécharger ensuite sur la ou les TILLYS) peuvent être effectuées sur n'importe quelle TILLYS, en amont de la configuration de l'installation chez le client.

Si des détecteurs et des sirènes doivent être connectés à une distance dépassant celle autorisée par la longueur totale du bus [RS 485](#) (600 mètres), l'intrusion CUBE permet de configurer des TILLYS périphériques. La TILLYS hôte gère alors la configuration intrusion pour les détecteurs et sirènes des TILLYS périphériques qui lui sont associés et un token (jeton) sécurise l'échange d'informations.

### 3.2.1. Opérations de configuration intrusion CUBE

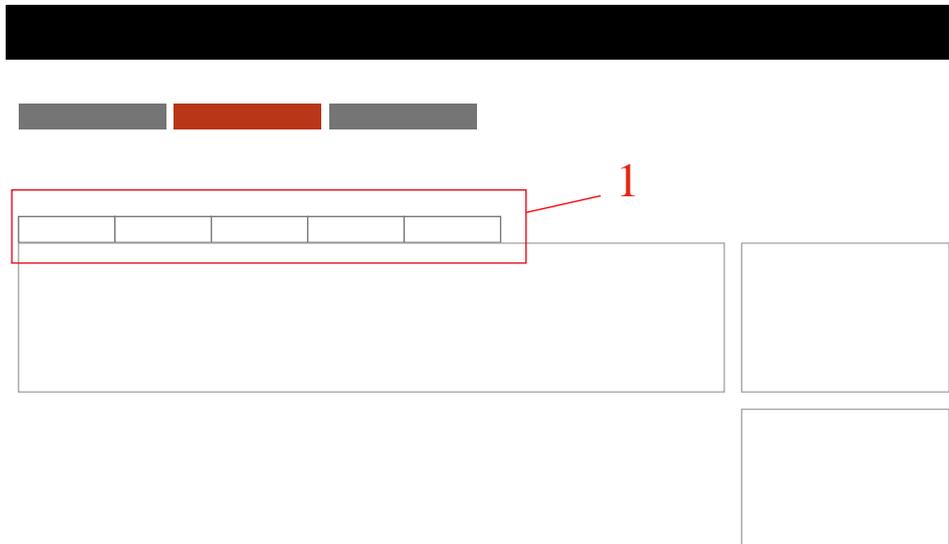
Les sections ci-après présentent toutes les opérations individuelles de configuration, accessibles par l'interface web d'une TILLYS via son adresse IP.

#### 3.2.1.1. Accès à l'interface d'administration de l'intrusion CUBE sur une TILLYS

1. Sur l'ordinateur portable connecté au réseau Ethernet, ouvrir un navigateur et saisir l'adresse IP de la TILLYS à configurer.
2. Saisir le login et le mot de passe d'accès.
3. Dans le menu  burger, suivre **Intrusion CUBE > Configuration intrusion**.

Les onglets de configuration (Groupes, Détecteurs, Sirènes, Profils et TACTILLYS-IP) sont accessibles en haut de la section centrale : voir (1) sur l'illustration ci-après.

**Figure 3.2. Emplacement des onglets de navigation sur l'écran de configuration de l'intrusion CUBE d'une TILLYS (10010-005)**



### 3.2.1.2. Configuration d'un groupe de détecteurs intrusion CUBE

Avec intrusion CUBE, un *groupe de détecteurs* de la TILLYS hôte peut gérer des détecteurs et des sirènes physiquement raccordés sur des TILLYS différentes (configuration multi-TILLYS). Chaque TILLYS peut gérer jusqu'à 32 groupes de détecteurs. Chaque groupe peut gérer des détecteurs physiques et des détecteurs virtuels, raccordés à d'autres TILLYS.

Il est totalement inutile de créer un groupe de détecteurs sur les TILLYS périphériques. L'intrusion CUBE permet de relier leurs détecteurs et sirènes de manière virtuelle au groupe de détecteurs de la TILLYS hôte.

1. Dans le menu  burger de la TILLYS hôte, suivre **Intrusion CUBE > Configuration intrusion**.
2. Cliquer sur l'onglet **Groupes**, puis sur le bouton [ + Ajouter ].

**Figure 3.3. Déclaration d'un détecteur (10010-006)**

3. Renseigner les différents champs selon les tableaux ci-après.

Section Informations générales	Détail des paramètres
<b>Libellé</b>	Saisir un nom représentatif du site pour le groupe de détecteurs.
<b>Transmettre l'armement / le désarmement</b>	Pour transmettre les actions d'armement/désarmement du groupe et l'IP du client au télésurveilleur, cliquer sur l'interrupteur (blanc > bleu).
<b>Registre d'état d'armement</b>	Saisir obligatoirement un registre ToR (M, V ou R, de 1 à 128) qui définira l'armement (valeur à 0) ou le désarmement du groupe (valeur à 1).
<b>Registre de statut (registre d'état)</b>	Saisir éventuellement un registre numérique (MN, VN ou RN, de 1 à 128) dans lequel sera remonté le statut complet du groupe.  Voir aussi les <a href="#">Section 1.7.2, « Valeurs du registre numérique d'état des groupes en intrusion CUBE »</a> .

Section Configuration de l'armement	Détail des paramètres
<b>Numéro de plage horaire pour l'armement automatique</b>	Si un armement automatique sur plage horaire est souhaitée, saisir le numéro d'une plage horaire (de 1 à 250).
<b>Désarmement automatique</b>	Si le désarmement du groupe doit être effectué à la fin d'une plage horaire, dans la cadre d'un armement sur plage horaire, cliquer sur l'interrupteur (blanc > bleu).
<b>Registre d'état prêt pour l'armement</b>	<p>Permet d'indiquer si le groupe de détecteur est prêt pour l'armement :</p> <ul style="list-style-type: none"> <li>● Le registre vaut 1 si aucun des signaux de détecteurs du groupe n'est en état de défaut</li> <li>● Le registre vaut 0 si au moins un signal de détecteur du groupe est en état de défaut.</li> </ul> <p>Saisir éventuellement un registre ToR (M, V ou R, de 1 à 128).</p> <p> Si le signal d'un détecteur défini comme <b>éjectable automatiquement à l'armement</b> est en état de défaut, la valeur du registre d'état <i>prêt pour armement</i> sera 0.</p> <p>Si l'armement est demandé (en automatique, par <i>microcode</i>, ou par télécommande d'un opérateur), le détecteur sera éjecté de la boucle de surveillance et le groupe sera armé.</p>
<b>Temporisation de pré-alarme (en minutes)</b>	<p>Permet de définir un délai avant que l'armement du groupe soit déclenché.</p> <p>Saisir le nombre de minutes souhaité.</p>
<b>Temporisation d'entrée (en secondes)</b>	Saisir le nombre de secondes souhaité, si au moins un détecteur du groupe a été configuré en temporisation d'entrée.

Section Configuration de l'armement	Détail des paramètres
	<p>Ce délai vaut pour tous les détecteurs du groupe configurés en "Temporisation d'entrée" ou "Masqué si tempo d'entrée en cours".</p>
<b>Temporisation de sortie (en secondes)</b>	<p>Saisir le nombre de secondes souhaité, si au moins un détecteur du groupe a été configuré en temporisation de sortie.</p> <p>Ce délai vaut pour tous les détecteurs du groupe configurés en "<a href="#">Temporisation de sortie</a>" ou "Masqué si tempo d'entrée en cours".</p>
<b>Dérogation minimum (en minutes)</b>	<p>Permet de définir la valeur minimale du délai de dérogation proposé pour l'armement.</p> <p>Saisir le nombre de minutes souhaité. Celui-ci sera proposé à l'opérateur sur le terminal intrusion CUBE.</p>
<b>Dérogation maximum (en minutes)</b>	<p>Permet de définir la valeur maximale du délai de dérogation à l'armement. Au-delà de ce délai, l'opérateur doit choisir entre désarmer le groupe ou laisser l'armement s'effectuer.</p> <p>Saisir le nombre de minutes souhaité. Celui-ci sera proposé à l'opérateur sur le terminal intrusion CUBE.</p>
<b>Pas de dérogation (en minutes)</b>	<p>Permet de définir le pas d'incrémentatation du délai de dérogation à l'armement.</p> <p>Saisir le nombre de minutes souhaité. Celui-ci sera proposé à l'opérateur sur le terminal intrusion CUBE.</p>
Section Registres de synthèse	Détail des paramètres
<p>Il est possible de définir l'emplacement de 7 registres de synthèse.</p>	<p>Ils permettent de définir un registre par type d'alarme mentionnant la présence d'un état de défaut sur au moins un signal d'un des détecteurs du groupe :</p> <ul style="list-style-type: none"> <li>● Le registre vaut 0 si aucun des signaux de détecteurs du groupe n'est en état de défaut.</li> </ul>

## Section Registres de synthèse

## Détail des paramètres

- Le registre vaut 1 si au moins un signal de détecteurs du groupe est en état de défaut.

Saisir éventuellement un registre ToR (M, V ou R, de 1 à 128) pour chaque type d'alarme : Intrusion, 24/24, Intrusion silencieuse, Défaut système, Défaut système silencieux, Appel d'urgence ou Incendie.

4. Pour valider, cliquer sur le bouton [ **Enregistrer** ].

### 3.2.1.3. Activation de la transmission d'alarmes au télésurveilleur

Pour activer la transmission d'alarmes au télésurveilleur, activer l'option Transmettre l'armement / le désarmement (voir [Section 3.2.1.2, « Configuration d'un groupe de détecteurs intrusion CUBE »](#)).

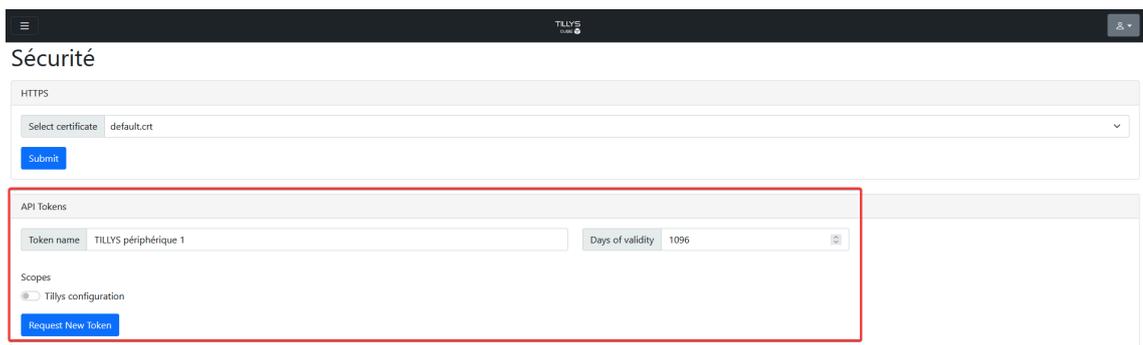
### 3.2.1.4. Configuration multi-TILLYS : génération sur la TILLYS hôte d'un token par TILLYS périphérique

Le raccordement des détecteurs et sirènes des TILLYS périphériques doit se faire en utilisant un token (jeton) par TILLYS périphérique. Ceci permet, en cas de problème de sécurité, de déconnecter chaque TILLYS périphérique indépendamment.

Les tokens ne sont générés qu'une seule fois et ils doivent être conservés dans un fichier client avec ses autres données confidentielles de configuration.

1. Dans le menu  burger de la TILLYS hôte, suivre **Réseau et sécurité > Sécurité**.

**Figure 3.4. Génération d'un token (10010-007)**

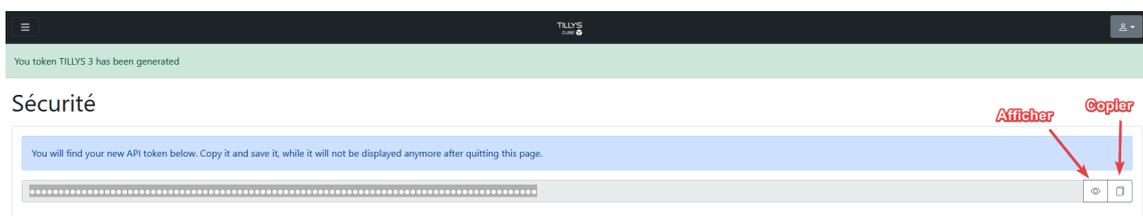


2. Renseigner les différents champs selon les tableaux ci-après.

Section HTTPS	Détail du paramètre
<b>Select certificate</b>	En principe, rien à modifier dans cette section.
Section API Tokens	Détail des paramètres
<b>Token name</b> (nom du jeton)	Saisir un nom identifiant clairement la TILLYS distante.  Pour des raisons de sécurité, les caractères spéciaux ne sont pas pris en compte.
<b>Days of validity</b> (délai d'expiration)	3 ans au maximum (soit 1096 jours).
<b>Scopes</b> (objet)	Cliquer sur l'interrupteur <b>Tillys configuration</b> (blanc > bleu).

3. Pour valider, cliquer sur le bouton [ **Request New Token** ]. Une fenêtre **Sécurité** s'affiche.

**Figure 3.5. Copie du token généré (10010-008)**



4. Complètement à droite sur la ligne prévue pour saisir le mot de passe, un bouton permet de l'afficher et le suivant, de le copier.

Copier la valeur de ce token dans le fichier de configuration de l'installation du client, et y noter également l'adresse IP de la TILLYS périphérique pour laquelle il a été généré.

5. Afin d'éviter une interruption de la surveillance anti-intrusion CUBE sur certaines parties sur lesquelles le token a expiré, fixer dès maintenant avec le client la date de la visite technique de prolongation de la durée de validité du ou des tokens (par exemple, une semaine avant la date d'expiration prévue).

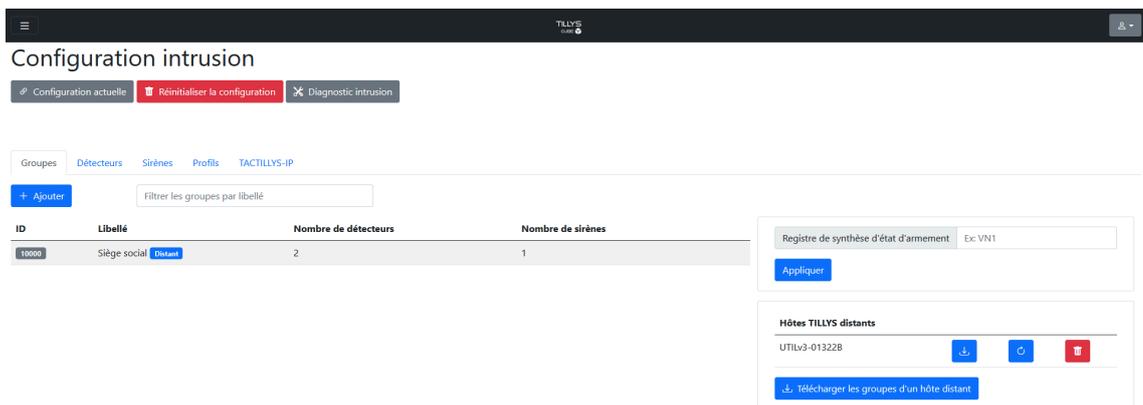
### 3.2.1.5. Configuration multi-TILLYS : copie sur une TILLYS périphérique du lien avec la TILLYS hôte

Cette opération permet de visualiser le ou les groupes de détecteurs de la TILLYS hôte sur une TILLYS périphérique.

S'il existe plusieurs TILLYS périphériques, il est conseillé de définir un token par TILLYS périphérique (voir [Section 3.2.1.4, « Configuration multi-TILLYS : génération sur la TILLYS hôte d'un token par TILLYS périphérique »](#)).

1. Dans le menu  burger de la TILLYS périphérique, suivre **Intrusion CUBE > Configuration intrusion**, puis cliquer sur l'onglet **Groupes**.

#### Figure 3.6. Visualisation du groupe de détecteurs d'une TILLYS hôte sur une TILLYS périphérique (10010-009)



The screenshot shows the 'Configuration intrusion' interface. At the top, there are tabs for 'Configuration actuelle', 'Réinitialiser la configuration', and 'Diagnostic intrusion'. Below this, there are navigation tabs for 'Groupes', 'Détecteurs', 'Sirènes', 'Profils', and 'TACTILLYS-IP'. A search bar is present with the text 'filtrer les groupes par libellé'. A table displays the following data:

ID	Libellé	Nombre de détecteurs	Nombre de sirènes
10000	Siège social <b>Distant</b>	2	1

On the right side, there is a 'Registre de synthèse d'état d'armement' with the value 'Ex: VN1' and an 'Appliquer' button. Below that, the 'Hôtes TILLYS distants' section shows 'UTILV3-013228' with download, refresh, and delete icons, and a 'Télécharger les groupes d'un hôte distant' button.

2. Dans la partie droite de l'écran, cliquer sur le bouton [ **Télécharger les groupes d'un hôte distant** ].

Une boîte de dialogue s'affiche.

**Figure 3.7. Saisie du token de la TILLYS hôte sur une TILLYS périphérique (10010-010)**

3. Renseigner les différents champs selon le tableau ci-après.

Paramètre	Détails
<b>L'hôte distant utilise le HTTPS</b>	<p>En configuration standard, cet interrupteur est activé (blanc &gt; bleu) et le protocole https doit être activé au niveau des deux TILLYS.</p> <p>Si ce n'est pas le cas, le message "Impossible de tirer les groupes de l'hôte : hôte injoignable" s'affiche.</p> <p>Pour plus de détails, voir <a href="#">Section 3.2.2.6, « Choix du niveau de sécurité sur IP entre TILLYS et TACTILLYS-IP CUBE »</a>.</p>
<b>Hôte</b>	Par défaut, ce champ contient la valeur "admin". Saisir l'adresse IP de la TILLYS hôte.
<b>Clé API</b>	Coller la valeur du token précédemment généré (voir <a href="#">Section 3.2.1.4, « Configuration multi-TILLYS : génération sur la TILLYS hôte d'un token par TILLYS périphérique »</a> ).

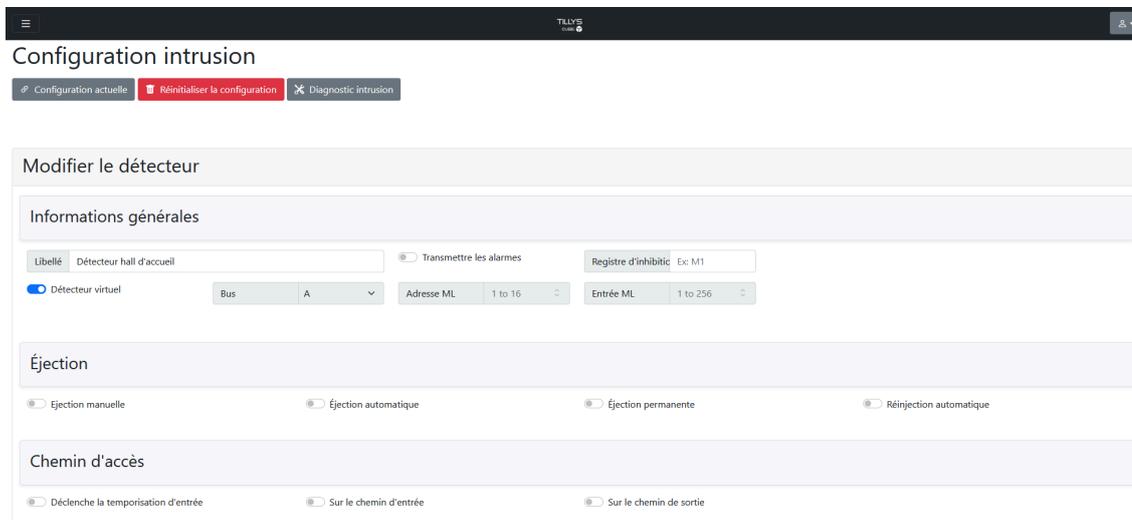
4. Cliquer sur le bouton [ **Télécharger les groupes** ].

### 3.2.1.6. Configuration des détecteurs intrusion CUBE d'une TILLYS

Cette opération s'applique à la TILLYS (hôte ou périphérique) sur laquelle les détecteurs sont physiquement connectés.

1. Dans le menu  burger de la TILLYS, suivre **Intrusion CUBE > Configuration intrusion**, cliquer sur l'onglet **Détecteurs**, puis sur le bouton [ **+ Ajouter** ].

**Figure 3.8. Déclaration d'un détecteur (10010-011)**



2. Renseigner les différents champs selon les tableaux ci-après.

Section Informations générales	Détails des paramètres
<b>Libellé</b>	Saisir un nom pour le détecteur.
<b>Transmettre des alarmes</b>	Cliquer sur l'interrupteur (blanc > bleu), si les alarmes générées par ce détecteur doivent être transmises au télésurveilleur.
<b>Registre d'inhibition</b>	Saisir éventuellement un registre ToR (M, V ou R, de 1 à 128) qui, à l'état 1, permettra l'inhibition du détecteur (pour une opération de maintenance, par exemple).
<b>Détecteur virtuel</b>	<p>Par défaut le détecteur paramétré est un détecteur physique (l'interrupteur <i>Détecteur virtuel</i> est blanc). Renseigner le <i>Bus</i> (A,B ou C), l'adresse du module MI sur lequel le détecteur est raccordé, ainsi que l'entrée ML sur laquelle il est câblé.</p> <p>Configurer un détecteur virtuel consiste à le lier de manière logique à une TILLYS hôte, alors qu'il est physiquement connecté à une TILLYS périphérique. Pour ce faire, agir sur l'interrupteur <i>Virtual Detector</i> (blanc &gt; bleu).</p>

Section Informations générales	Détails des paramètres
	Le numéro de ce détecteur virtuel est alors défini automatiquement (ID présent dans la liste globale des détecteurs).

Section Éjection	Détails du paramètre
	<p>Pour choisir le type d'éjection souhaité pour le détecteur, activer les interrupteurs (blanc &gt; bleu) :</p> <ul style="list-style-type: none"><li>● <i>Peut être éjecté manuellement</i> : éjection manuelle à la mise en service</li><li>● <i>Peut être éjecté automatiquement</i> : éjection automatique à la mise en service</li><li>● <i>Peut être éjecté définitivement</i> : éjection permanente</li><li>● <i>Peut être réarmé automatiquement</i> : réinjection automatique dès la suppression du défaut</li></ul>

Section Chemin d'accès	Détails du paramètre
	<p>Pour autoriser un utilisateur à sortir après l'armement ou à aller jusqu'au terminal intrusion pour le désarmement, et pour choisir le type de temporisation souhaité, activer les interrupteurs (blanc &gt; bleu).</p> <p>Les délais en secondes doivent être configurés dans le paramétrage des groupes de détecteurs.</p> <ul style="list-style-type: none"><li>● <i>Déclenche la temporisation en d'entrée</i> : activation de la temporisation en entrée</li><li>● <i>Sur le chemin d'entrée</i> : masqué si temporisation d'entrée en cours. Le détecteur sera temporairement inhibé, si un autre détecteur du même groupe est en temporisation d'entrée ou de sortie.</li></ul>

Section Chemin d'accès	Détails du paramètre
	<ul style="list-style-type: none"><li>● <i>Sur le chemin de sortie</i> : temporisation en sortie</li></ul>
Section Signaux	Détails du paramètre
	<p>Par défaut les deux signaux, alarme et autoprotection, sont activés (interrupteur bleu). Pour désactiver l'un des signaux, cliquer sur son interrupteur (bleu &gt; blanc).</p> <p>L'alarme intrusion peut être déclenchée lorsque le groupe est armé. Une fonction sirène se déclenche si elle a été associée.</p> <p>L'alarme d'autoprotection est une alarme permanente, dont le déclenchement est indépendant de l'état d'armement du groupe. Une fonction sirène se déclenche si elle a été associée.</p> <ul style="list-style-type: none"><li>● <i>Alarme</i> : cliquer pour l'activer (blanc &gt; bleu).</li></ul> <p><i>Type</i> (type d'alarme) : par défaut Intrusion. Sélectionner le type souhaité dans la liste déroulante.</p> <p><i>Mode</i>(type de contact) : sélectionner une valeur dans la liste déroulante (<i>Normalement fermé</i>).</p> <p><i>Numéro pour le télésurveilleur</i> : valeur à transmettre au télésurveilleur.</p>

Section Signaux	Détails du paramètre
	<ul style="list-style-type: none"><li>● <i>Auto-protection</i> : cliquer pour l'activer (blanc &gt; bleu).</li></ul> <p><i>Type</i> (type d'alarme) : par défaut 24/24. Sélectionner le type souhaité dans la liste déroulante.</p> <p><i>Mode</i> (type de contact) : <i>Normalement fermé</i>.</p> <p><i>Numéro pour le télésurveilleur</i> (référence télétransmission) : valeur à transmettre au télésurveilleur.</p>

Section Assigner au groupe	Détails du paramètre
	<p>Pour affecter le détecteur à un groupe, choisir son nom dans la liste déroulante.</p> <p>S'il s'agit d'un détecteur virtuel, il doit être associé à un groupe de la TILLYS hôte.</p> <p>Cette liste déroulante permet également de désactiver un détecteur.</p>

3. Pour valider le paramétrage effectué, cliquer sur le bouton [ **Enregistrer** ].

### 3.2.1.7. Configuration d'un détecteur intrusion CUBE sur une TILLYS périphérique

En configuration multi-TILLYS, la procédure est identique à celle décrite dans la section [Section 3.2.1.6, « Configuration des détecteurs intrusion CUBE d'une TILLYS »](#) jusqu'au choix du groupe de rattachement : choisir le groupe principal, situé sur la TILLYS hôte. Il est également nécessaire d'activer le commutateur *Détecteur virtuel*.

### 3.2.1.8. Configuration d'une sirène intrusion CUBE

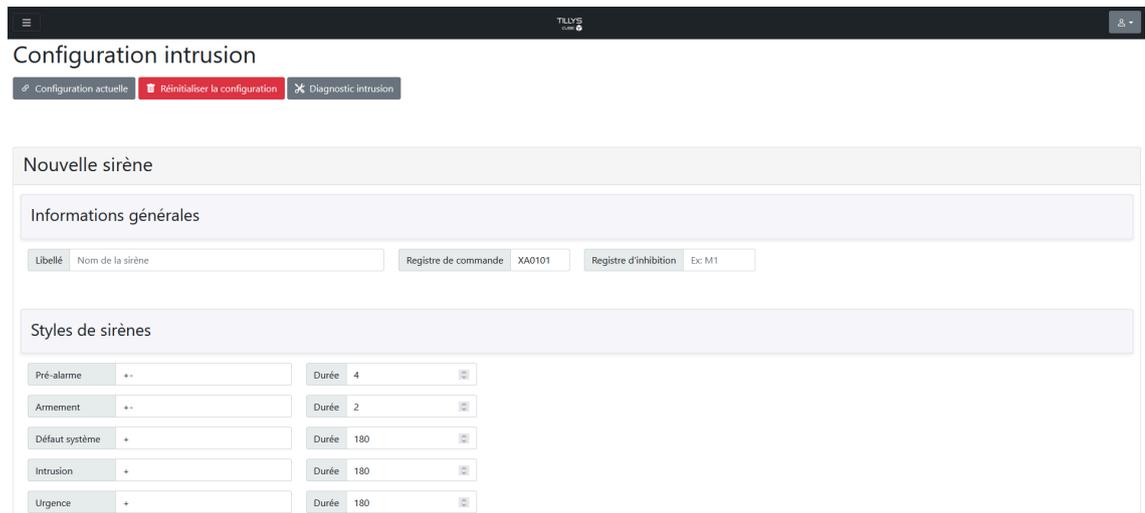
Cette opération s'applique à la TILLYS (hôte ou périphérique) sur laquelle la sirène est physiquement connectée.

Chaque style de sonnerie possède un indice de priorité. Plus cet indice de priorité est élevé, plus la sonnerie sera prioritaire sur les autres.

Exemples : la sonnerie d'alarme intrusion (priorité 4) prend le dessus sur la sonnerie de pré-alarme (priorité 1), et la sonnerie incendie (priorité 6) prend le dessus sur la sonnerie d'alarme intrusion (priorité 4).

1. Dans le menu  burger de la TILLYS, suivre **Intrusion CUBE > Configuration intrusion**, cliquer sur l'onglet **Sirènes**, puis sur le bouton **[ + Ajouter ]**.

**Figure 3.9. Création et configuration d'une fonction sirène (10010-012)**



2. Renseigner les différents champs selon les tableaux ci-après.

Section informations générales	Détail des paramètres
<b>Libellé</b>	Saisir un nom pour la sirène.
<b>Registre de commande</b>	Saisir une valeur de registre ToR valide :  Soit un registre de sortie physique d'un module, par exemple : "XA0102". Dans le cas d'un module MLIO16, il faut que les sorties aient été préalablement définies, pour que le registre soit accepté.  Soit un registre virtuel : un registre de type M,V ou R, de 1 à 128 peut être saisi, en vue d'un déclenchement spécifique défini par microcode.
<b>Registre d'inhibition</b>	Saisir éventuellement une valeur de registre ToR (M, V ou R, de 1 à 128) qui mis à l'état 1 permettra l'inhibition de la sirène (pour une opération de maintenance, par exemple).

Section Styles de sirène	Détail des paramètres
<b>Pré-alarme</b>	<p>Configurer les diverses sirènes en utilisant les signes + et - ainsi que la durée de sonnerie (en secondes).</p> <p>La configuration des sirènes est effectuée au niveau de la durée et non pas à celui du nombre de répétitions.</p> <p>Pour la sirène de pré-alarme, déclenchement avant la période d'armement, afin de permettre à la personne ayant armé le groupe de sortir du bâtiment ou à une personne encore présente de demander une dérogation sur le terminal TACTILLYS-IP CUBE.</p>
<b>Armement</b>	Déclenchement en début de la période d'armement du groupe.
<b>Défaut système</b>	Déclenchement indépendant de l'état d'armement du groupe.
<b>Intrusion</b>	Déclenchement en cas de détection d'un intrus lorsque le groupe est armé.
<b>Urgence</b>	Appel d'urgence. Déclenchement indépendant de l'état d'armement du groupe.
<b>Incendie</b>	Déclenchement indépendant de l'état d'armement du groupe.

Section Assigner aux groupes	Détail des paramètres
	<p>Cette liste permet d'affecter une sirène à un ou à plusieurs groupes.</p> <p>Pour sélectionner plusieurs groupes, maintenir la touche [ <b>CTRL</b> ] enfoncée et cliquer sur les groupes l'un après l'autre, puis relâcher la touche [ <b>CTRL</b> ].</p>

3. Pour valider le paramétrage effectué, cliquer sur le bouton [ **Enregistrer** ].

### 3.2.1.9. Configuration d'une sirène intrusion CUBE sur une TILLYS périphérique

En configuration intrusion CUBE multi-TILLYS, la procédure est identique à celle décrite dans la section [Section 3.2.1.8, « Configuration d'une sirène intrusion CUBE »](#) jusqu'au choix du groupe de rattachement : choisir le groupe principal, situé sur la TILLYS hôte.

### 3.2.1.10. Comparaison des vues d'ensemble des détecteurs en intrusion CUBE multi-TILLYS

L'association de la touche [ **Windows** ] du clavier avec les touches flèche gauche [ ← ] ou droite [ → ] permet de réduire de moitié une fenêtre de navigateur dans la direction de la flèche, et de juxtaposer deux fenêtres sur le même écran, pour en comparer plus facilement les informations.

1. Ouvrir une fenêtre de navigateur et ouvrir la TILLYS hôte, puis cliquer sur les touches [ **Windows** ] + [ ← ].

La fenêtre du navigateur est réduite en largeur et occupe la moitié gauche de l'écran.

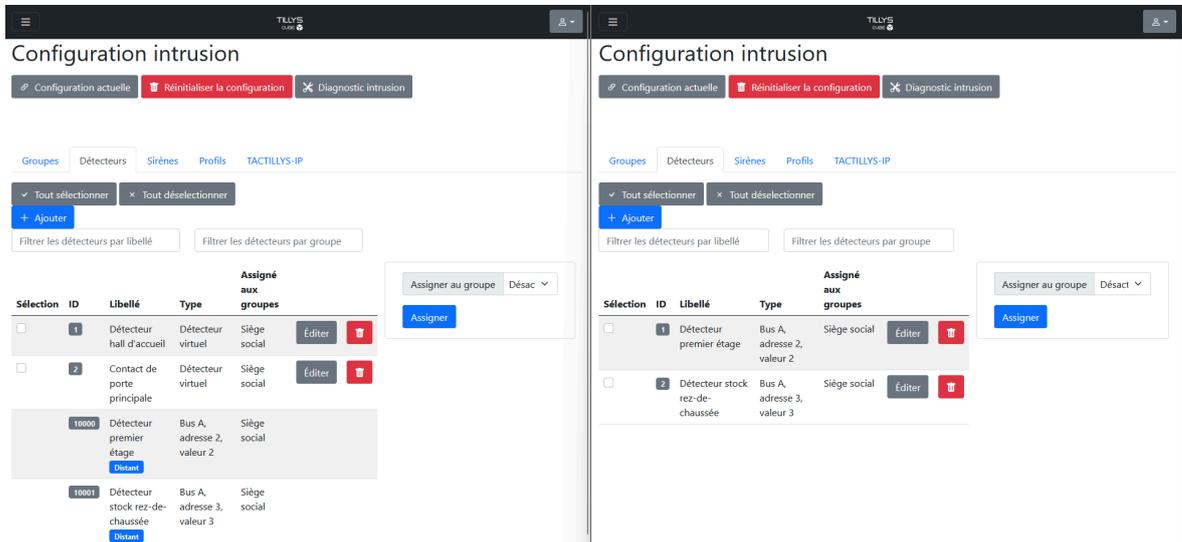
2. Dans le menu  burger de la TILLYS hôte, suivre **Intrusion CUBE > Configuration intrusion**, cliquer sur l'onglet **Détecteurs**.
3. Ouvrir une deuxième fenêtre de navigateur et ouvrir la TILLYS périphérique, puis cliquer sur les touches [ **Windows** ] + [ → ].

La fenêtre du navigateur est réduite en largeur et occupe la moitié droite de l'écran.

4. Dans le menu  burger de la TILLYS périphérique, suivre **Intrusion CUBE > Configuration intrusion**, cliquer sur l'onglet **Détecteurs**.

La comparaison des deux configurations sur un seul écran permet de repérer d'éventuels défauts de configuration.

**Figure 3.10. Comparaison des vues d'ensemble des détecteurs sur TILLYS hôte et TILLYS périphérique (10010-013)**



### 3.2.1.11. Association d'un terminal TACTILLYS-IP CUBE à un ou plusieurs groupes d'une TILLYS hôte

Cette opération permet d'associer un terminal TACTILLYS-IP CUBE à la TILLYS hôte, dont le ou les groupes gèrent des capteurs, des sirènes, ainsi que toutes les opérations liées à l'armement et au désarmement de l'alarme.

1. Dans le menu  de la TILLYS hôte, suivre **Intrusion CUBE > Configuration intrusion**, cliquer sur l'onglet **TACTILLYS-IP**, puis sur le bouton **[ + Ajouter ]**.

**Figure 3.11. Déclaration du terminal TACTILLYS-IP pour la gestion de l'intrusion CUBE (10010-014)**

The screenshot shows the 'Configuration intrusion' interface for a 'Nouveau TACTILLYS-IP'. It features three main sections: 'Informations générales', 'Authentification', and 'Signaux'. Each section contains various input fields and checkboxes for configuring the terminal's settings.

2. Renseigner les différents champs selon les tableaux ci-après.

Section Informations générales	Détail des paramètres
<b>Libellé</b>	Saisir un nom pour le terminal TACTILLYS-IP CUBE.
<b>Adresse IP</b>	Saisir l'adresse IP de ce terminal TACTILLYS-IP CUBE.
<b>Port</b>	Saisir le port de communication exploité pour communiquer avec le terminal (par défaut, 443).
<b>Transmettre les alarmes</b>	Cliquer sur l'interrupteur (blanc > bleu), pour que le terminal émette un signal sonore lorsqu'une alarme est générée dans le système.

Section Authentification	Détail des paramètres
<b>Inactivité maximale (en secondes)</b>	Saisir le nombre de secondes souhaité, correspondant au laps de temps pendant lequel le terminal reste connecté sans aucune action de la part de l'opérateur.

Section Authentification	Détail des paramètres
<b>Nombre maximal de tentatives avant le verrouillage</b>	Saisir le nombre de tentatives de connexion accepté, avant que le terminal se verrouille.
<b>Durée du verrouillage d'authentification</b>	Saisir le temps en minutes pendant lequel le terminal reste verrouillé, après que le nombre maximal de tentatives de connexion ait été atteint.
<b>Délai pour la saisie du code (en secondes)</b>	Saisir le temps maximal en secondes accepté entre le passage d'un badge et la saisie du code associé.
<b>Position aléatoire des touches du clavier numérique</b>	Cliquer sur l'interrupteur (blanc > bleu), pour activer la fonction de positionnement aléatoire des touches numériques.

Section Signaux	Détail des paramètres
<b>Auto-protection</b>	Cliquer sur l'interrupteur (blanc > bleu), pour activer la prise en compte du signal d'auto-protection du terminal.
<b>Type</b>	S'il est activé, le signal d'autoprotection est configuré par défaut sur le type d'alarme 24/24. Sélectionner éventuellement un autre type d'alarme dans la liste déroulante.
<b>Numéro pour le télétransmetteur</b>	

Section Groupes gérés	Détail du paramètre
<b>Assigner au groupe</b>	Cette liste permet d'affecter un terminal TACTILLYS-IP CUBE à la gestion d'un ou de plusieurs groupes.  Pour sélectionner plusieurs groupes, maintenir la touche [ CTRL ] enfoncée et cliquer sur les groupes l'un après l'autre, puis relâcher la touche [ CTRL ].

3. Pour valider, cliquer sur le bouton [ **Enregistrer** ].

### 3.2.1.12. Configuration des télésurveilleurs

1. Dans le menu  burger de la TILLYS hôte, suivre **Intrusion CUBE > Configuration transmetteur**, puis cliquer sur le bouton [ **+ Ajouter** ].

**Figure 3.12. Déclaration du ou des télésurveilleurs pour la gestion de l'intrusion CUBE (10010-015)**

The screenshot shows a web interface for configuring remote transmission. At the top, it says 'Configuration télétransmission' with a 'Réinitialiser la configuration' button. Below, there are two main sections: 'Informations générales' and 'Paramètres du destinataire'. The 'Informations générales' section contains fields for 'Libellé', 'Nom du destinataire', 'Adresse IP', 'Adresse IP du destinataire', and 'Port', 'Port du destinataire'. The 'Paramètres du destinataire' section contains a dropdown for 'Protocole' (set to SIA-DCS), input fields for 'Numéro d'abonné', a dropdown for 'Nombre de tentatives de connexion' (set to 1), and a dropdown for 'Délai entre tentatives (en secondes)' (set to 5).

2. Renseigner les différents champs selon les tableaux ci-après.

Section Informations générales	Détail des paramètres
<b>Section Informations générales</b>	
<b>Libellé</b>	Saisir un nom pour le télésurveilleur.
<b>Adresse IP</b>	Saisir l'adresse IP du télésurveilleur.
<b>Port</b>	Saisir le port de communication du télésurveilleur.
Section Paramètres du destinataire	Détail des paramètres
<b>Protocole</b>	SIA-DCS.
<b>Numéro d'abonné</b>	Saisir la référence client fournie par le télétransmetteur.
<b>Nombre de tentatives de connexion</b>	Saisir le nombre maximal de tentatives de connexion.
<b>Délai entre tentatives (en secondes)</b>	Saisir le temps minimum entre deux tentatives de connexion.

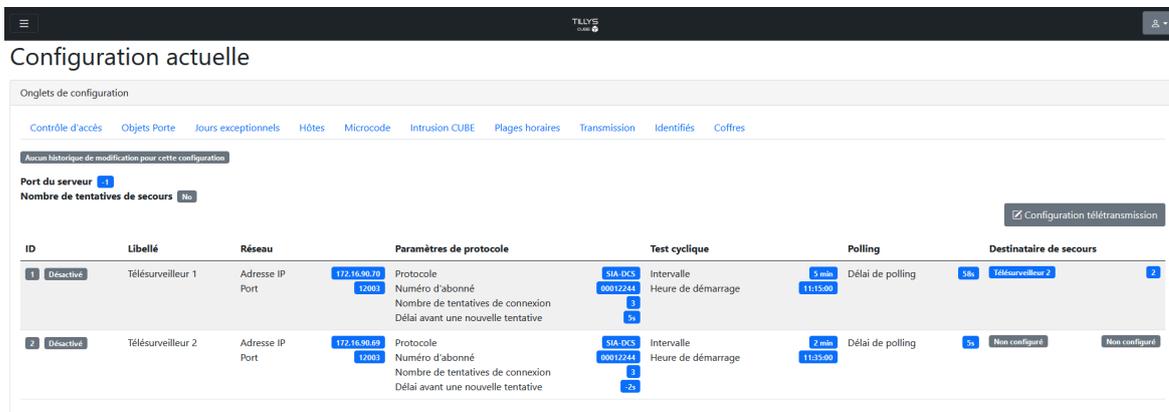
Section Paramètres du test cyclique du destinataire	Détail des paramètres
<b>Heure de démarrage</b>	<p>Les trames du <a href="#">test cyclique</a> sont envoyées par la TILLYS au logiciel de supervision du télésurveilleur (SIG).</p> <p>Il existe un test cyclique par télésurveilleur.</p> <p>Ce paramètre permet de définir l'heure de référence, à partir de laquelle le test cyclique sera effectué.</p>
<b>Intervalle (en minutes)</b>	Ce paramètre permet de définir la périodicité du test cyclique.
Section Paramètres de polling du destinataire	Détail du paramètre
<b>Assigner au groupe</b>	<p>Les trames de <a href="#">polling</a> sont envoyées par la TILLYS hôte au frontal de télésurveillance.</p> <p>Cette liste permet d'associer un terminal TACTILLYS-IP CUBE à un ou à plusieurs groupes.</p> <p>Pour sélectionner plusieurs groupes, maintenir la touche [ <b>CTRL</b> ] enfoncée et cliquer sur les groupes l'un après l'autre, puis relâcher la touche [ <b>CTRL</b> ].</p>
Section Destinataire de secours	Détail du paramètre
Par exemple "Télésurveilleur 2"	Pour pouvoir sélectionner un destinataire de secours dans cette liste déroulante, il doit d'abord avoir été configuré.

- Pour valider, cliquer sur le bouton [ **Enregistrer** ].
- Pour créer un télésurveilleur de secours, reprendre à l'étape 1 pour créer ce nouveau destinataire, puis éditer le destinataire principal et, dans la dernière section de l'écran de saisie, lui affecter le destinataire de secours nouvellement créé.

### 3.2.1.13. Affichage de la configuration de télésurveillance

Dans le menu  burger de la TILLYS hôte, suivre **Intrusion CUBE > Configuration transmetteur**, puis cliquer sur le bouton [ **Configuration actuelle** ].

**Figure 3.13. Affichage de la configuration de télésurveillance (10010-500)**



### 3.2.2. Opérations de paramétrage et de maintenance de l'intrusion CUBE

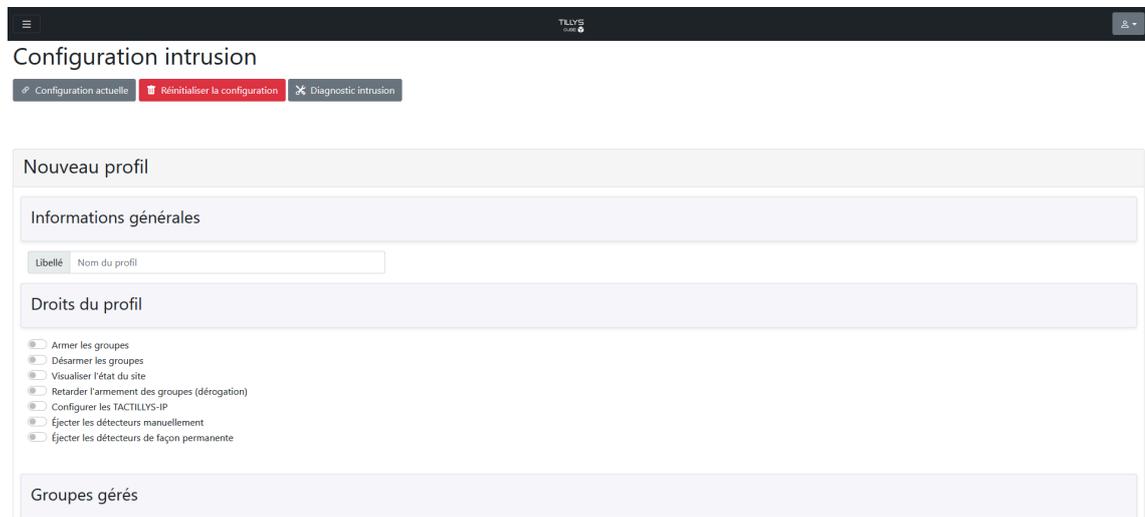
Les sections ci-après présentent les opérations de paramétrage de l'intrusion CUBE, comme le niveau de détail de la fonction de journalisation, le niveau de sécurité des échanges sur IP, et l'utilisation du microcode spécifique à l'intrusion CUBE.

Elles présentent également les opérations de maintenance comme l'effacement des clés avant l'envoi au SAV d'un terminal TACTILLYS IP défectueux, ainsi que celles permettant de sauvegarder et de rétablir une configuration.

#### 3.2.2.1. Création des profils intrusion sur la TILLYS hôte

1. Dans le menu  burger de la TILLYS hôte, suivre **Intrusion CUBE > Configuration intrusion**, cliquer sur l'onglet **Profils**, puis sur le bouton **[ + Ajouter ]**.

**Figure 3.14. Création et configuration des profils intrusion (10010-016)**



2. Renseigner les différents champs selon les tableaux ci-après.

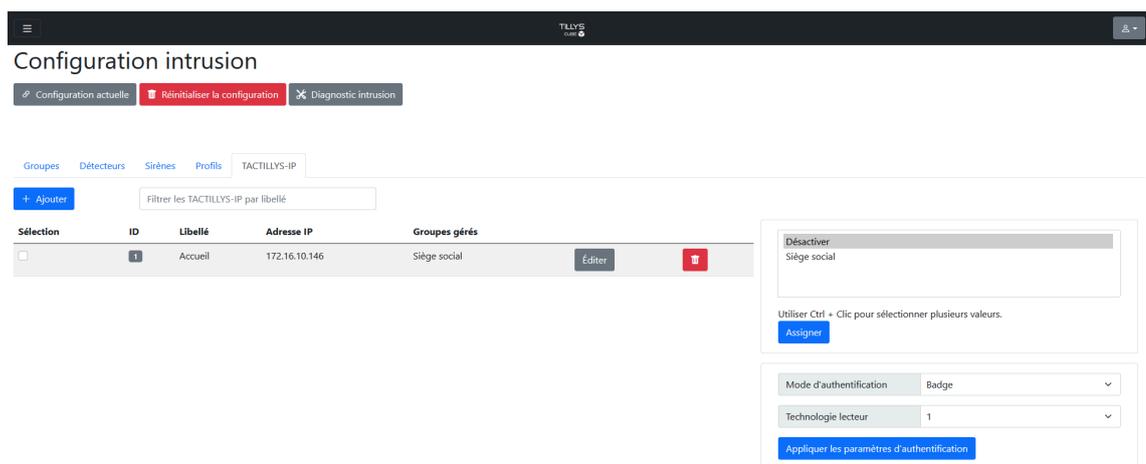
Section Informations générales	Détail du paramètre
<b>Libellé</b>	Saisir un nom pour le profil utilisateur intrusion CUBE.
Section Droits du profil	Détail du paramètre
Sept commutateurs (1 par droit d'accès)	Cliquer sur l'interrupteur (blanc > bleu), pour activer le droit correspondant.
Section Groupes gérés	Détail du paramètre
Liste déroulante	Cette liste permet d'associer un terminal TACTILLYS-IP CUBE à un ou à plusieurs groupes.  Pour sélectionner plusieurs groupes, maintenir la touche [ <b>CTRL</b> ] enfoncée et cliquer sur les groupes l'un après l'autre, puis relâcher la touche [ <b>CTRL</b> ].

3. Pour valider, cliquer sur le bouton [ **Enregistrer** ].
4. Ajouter tous les profils nécessaires en répétant les étapes ci-avant.

### 3.2.2.2. Choix des groupes de détecteurs gérés par un 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 première section en partie gauche de l'écran, cocher la case du groupe.

**Figure 3.15. Choix des groupes gérés par le TACTILLYS-IP CUBE (10010-017)**



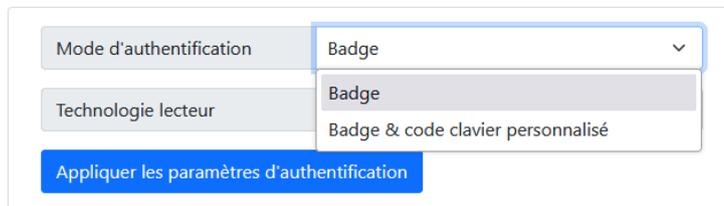
3. Dans la première section à droite de l'écran, choisir le ou les groupes associés au TACTILLYS-IP CUBE, puis cliquer sur le bouton [ **Assigner** ].

### 3.2.2.3. Choix du mode d'authentification (badge ou badge + code) sur un TACTILLYS-IP CUBE

Pour définir ou modifier le code clavier personnalisé d'un utilisateur, voir [Section 6.2, « Changement de l'identifiant intrusion utilisé lors de l'identification badge + code sur 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 *Badge* ou *Badge & code clavier personnalisé*, puis cliquer sur le bouton [ **Appliquer les paramètres d'authentification** ].

**Figure 3.16. Configuration de l'authentification sur un TACTILLYS-IP CUBE (badge ou badge + code) (10010-018)**



Mode d'authentification: Badge

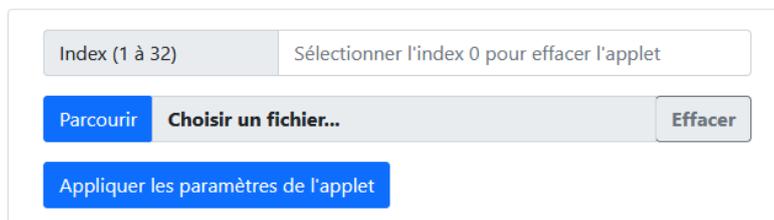
Technologie lecteur: Badge, Badge & code clavier personnalisé

Appliquer les paramètres d'authentification

### 3.2.2.4. Choix des applets à charger sur un 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 troisième section en partie droite de l'écran, saisir une référence d'index, cliquer sur le bouton [ **Parcourir** ], sélectionner le fichier à télécharger, valider et cliquer sur le bouton [ **Appliquer les paramètres de l'applet** ].

**Figure 3.17. Choix des applets à charger sur un TACTILLYS-IP (10010-019)**



Index (1 à 32) Sélectionner l'index 0 pour effacer l'applet

Parcourir Choisir un fichier... Effacer

Appliquer les paramètres de l'applet

### 3.2.2.5. Choix du niveau de détail des événements du journal de la TILLYS

La journalisation des événements permet de trouver l'origine de dysfonctionnements. Elle peut être stockée dans un fichier ou être envoyée au fil de l'eau sur un ordinateur sur lequel Syslog Watcher est installé.

L'affichage au fil de l'eau de la journalisation permet de suivre les logs en temps réel. Il est possible d'activer les deux options (enregistrement dans un fichier et affichage au fil de l'eau)..

Plus le niveau de détail est élevé, plus la puissance de calcul consommée par le processeur est élevée, ainsi que la place occupée en mémoire. Ceci peut ralentir les performances.

1. Dans le menu  burger de la TILLYS hôte, suivre **Système > Logs**.

**Figure 3.18. Niveau de détail des événements journalisés (10010-021)**

The screenshot shows the 'Logs' configuration page in the TILYS interface. It is divided into two main sections: 'Log configuration' and 'Log level'.  
In the 'Log configuration' section, the 'IP Address' is set to '127.0.0.1' and the 'UDP Port' is '514'. There are three radio buttons for log destinations: 'FileLog' (selected), 'SysLog', and 'WebLog'. A 'Submit' button is located below these options.  
The 'Log level' section features a yellow warning banner: 'WARNING : Using debug logs may degrade bus communication performance. Use only when necessary'. Below this is a row of tabs for different system components: 'Access Control', 'Intrusion', 'Safes', 'Supervision / Inter LPU Exchanges', 'Download', 'Bus', 'Web', 'SNMP', 'Certificates', and 'System'. Underneath the tabs, there are five rows of log level settings for 'Badge', 'CGI', 'Security', 'Combus', and 'Comlocal'. Each row has two buttons: a blue 'Normal' button and a yellow 'Maximum' button.

2. Pour envoyer le journal à une adresse IP particulière, saisir cette adresse IP et le port de destination (514 par défaut), cliquer sur le commutateur Syslog (gris > bleu), puis cliquer sur le bouton [ **Submit** ].

Pour enregistrer le journal dans un fichier, cliquer sur le commutateur Syslog (gris > bleu), puis cliquer sur le bouton [ **Submit** ].

Pour visualiser le journal directement dans la console de débogage en bas de cet écran, cliquer sur le commutateur Weblog (gris > bleu), puis cliquer sur le bouton [ **Submit** ].

Il est possible d'activer les 3 commutateurs.

3. Cliquer sur les boutons gris pour choisir sur quels aspects un niveau de détail élevé est nécessaire.

Il est possible de rétablir un niveau de détail plus faible, en cliquant sur les boutons bleus [ **Normal** ].

Pour valider, cliquer sur le bouton [ **Submit** ].

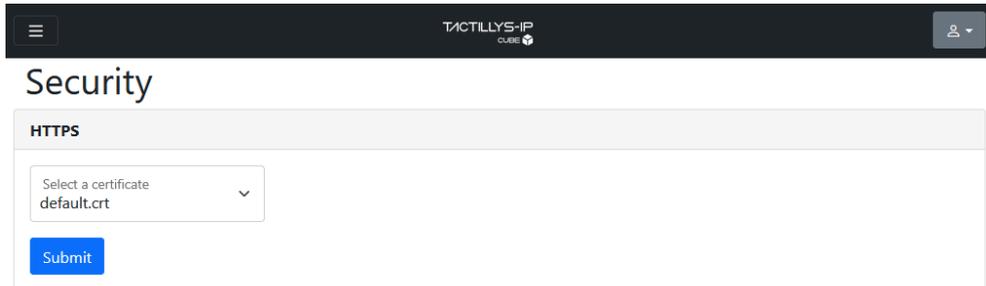
4. Une console de débogage avec des filtres et une zone de recherche permet d'affiner la recherche.

### 3.2.2.6. Choix du niveau de sécurité sur IP entre TILLYS et TACTILLYS-IP CUBE

Cette option permet de choisir le niveau de sécurisation des échanges entre le TACTILLYS-IP et la TILLYS (protocole http ou https). Par défaut, le mode est https, qui est un mode sécurisé. Il n'est pas recommandé d'utiliser le mode http.

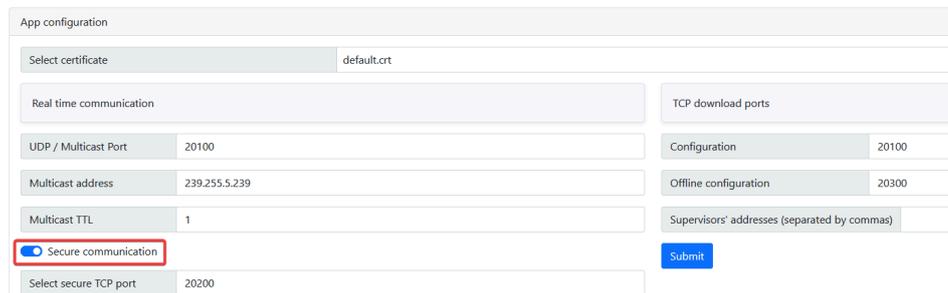
1. À partir de l'interface d'administration du TACTILLYS-IP, cliquer sur l'icône  burger en haut à gauche et suivre **Configuration > Security**.

**Figure 3.19. Passage de https à http sur le TACTILLYS-IP (10010-022)**



2. Dans la liste déroulante **Select a certificate**, choisir **None** et cliquer sur le bouton [**Submit**].
3. Au niveau de la TILLYS, le même paramétrage doit être réalisé dans l'écran **Configuration réseau** : suivre **Réseau et sécurité > Configuration réseau**.

**Figure 3.20. Passage de https à http sur la TILLYS (10010-023)**

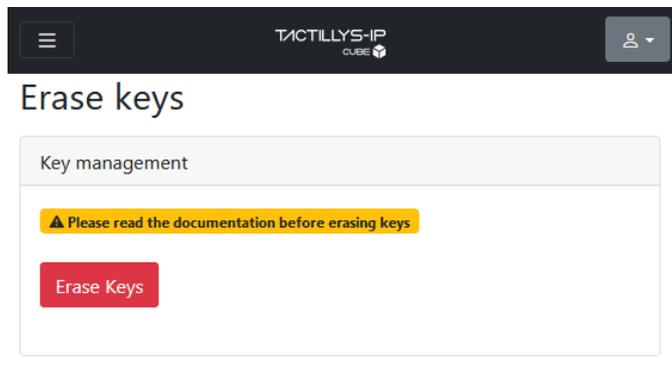


4. Faire défiler l'écran vers le bas, puis désactiver l'option **Communication sécurisée** (passage de bleu à gris) et cliquer sur le bouton [**Enregistrer**].
5. Si nécessaire, la restauration de la communication en mode https sera effectuée dans les mêmes écrans.

### 3.2.2.7. Effacement des clés du TACTILLYS-IP (désensibilisation)

Cette possibilité est à utiliser après avoir retiré un TACTILLYS-IP d'une installation, pour pouvoir l'intégrer dans une autre installation ou avant de l'envoyer en SAV.

1. À partir de l'interface d'administration du TACTILLYS-IP, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Maintenance > Erase Keys**.

**Figure 3.21. Effacement des clés de sécurité du TACTILLYS-IP (10010-024)**

2. Cliquer sur le bouton [ **Erase Keys** ].

### 3.2.3. Opérations de gestion de l'intrusion

Des détecteurs en défaut peuvent empêcher l'armement de l'alarme. Le paramétrage de ces détecteurs peut être éjection manuelle, éjection automatique, éjection permanente ou réinjection automatique.

#### 3.2.3.1. Éjection manuelle, éjection automatique, éjection permanente ou réinjection automatique

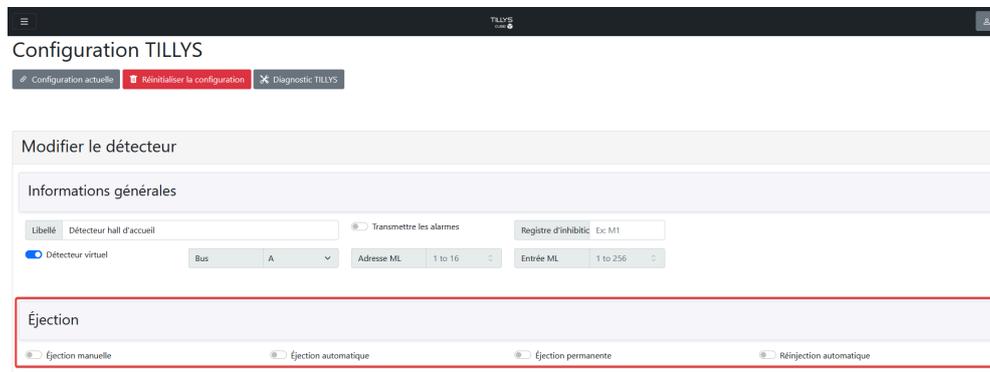
Des détecteurs en défaut peuvent empêcher l'armement de l'alarme. Ces paramètres sont à définir pour chaque détecteur dans son écran de configuration (voir [Section 3.2.3.2, « Éjection ou réinjection d'un détecteur »](#)).

#### 3.2.3.2. Éjection ou réinjection d'un détecteur

Toutes ces opérations sont effectuées sur l'écran de paramétrage de chaque détecteur.

1. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Intrusion Cube > Configuration TILLYS**.
2. Cliquer sur l'onglet Détecteurs.
3. Sur la ligne du détecteur à éjecter ou à réinjecter, cliquer sur le bouton [ **Éditer** ].

**Figure 3.22. Éjection ou réinjection de détecteurs sur une TILLYS (10010-025)**



4. Dans la section Éjection, cliquer sur le commutateur de l'option à activer (blanc > bleu).

**Tableau 3.1. Configuration de l'éjection d'un détecteur**

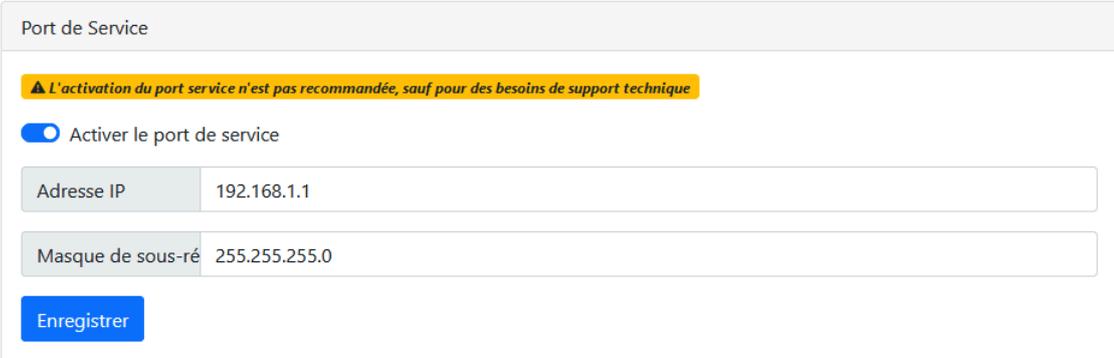
Type d'éjection	Effet
Éjection manuelle	Nécessite une action d'un utilisateur au moment prévu pour l'armement du système.
Éjection automatique	Éjection automatique en cas de défaut, afin de ne pas retarder l'armement du système. Option conseillée.
Éjection permanente	Éjection manuelle d'un détecteur, pendant sa réparation.
Réinjection automatique	Réinjection automatique lorsque l'anomalie de fonctionnement du détecteur a disparu. Option conseillée.

5. En bas de l'écran, cliquer sur le bouton [ Enregistrer ].

### 3.2.4. Opérations de maintenance intrusion CUBE

#### 3.2.4.1. Activation ou désactivation du port de maintenance d'une TILLYS

1. À partir de l'interface d'administration d'une TILLYS, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre Réseau et sécurité > Outils réseau.

**Figure 3.23. Activation du port de maintenance sur une TILLYS (10010-026)**

Port de Service

▲ L'activation du port service n'est pas recommandée, sauf pour des besoins de support technique

Activer le port de service

Adresse IP 192.168.1.1

Masque de sous-ré 255.255.255.0

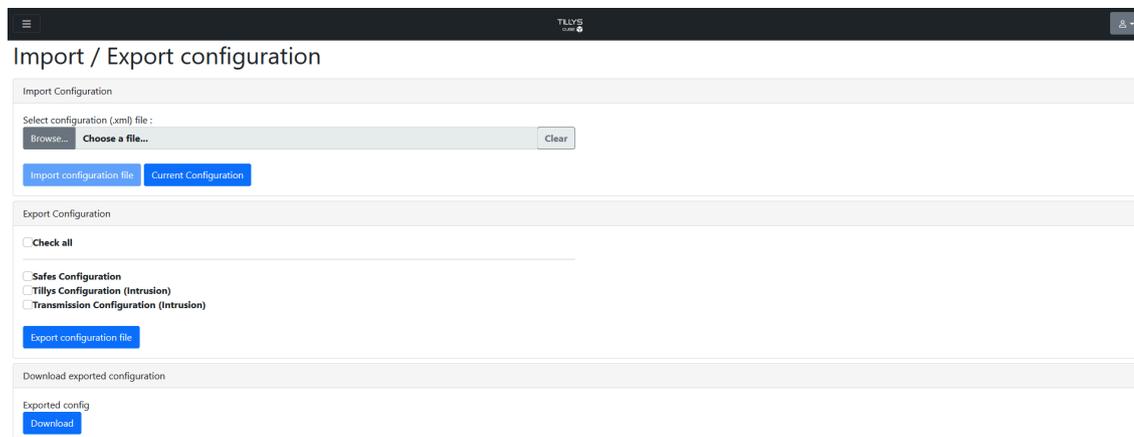
Enregistrer

2. Cliquer sur le bouton [ **Activer le port de service** ], pour l'activer (bleu) ou pour le désactiver (blanc).
3. Cliquer sur [ **Enregistrer** ].

### 3.2.4.2. Exporter ou importer un fichier de configuration intrusion CUBE

1. Pour pouvoir exporter ou importer un fichier de configuration intrusion CUBE sur une TILLYS, son port de maintenance doit être activé (voir [Section 3.2.4.1, « Activation ou désactivation du port de maintenance d'une TILLYS »](#)). Si ce n'est pas le cas, l'option d'Import/export ne sera même pas visible dans le menu.
2. À partir de l'interface d'administration de la TILLYS hôte, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **General > Import/Export Configuration**.

**Figure 3.24. Choix des options avant l'export d'un fichier de configuration intrusion CUBE (10010-027)**



3. Renseigner les différents champs selon le tableau ci-après.

Paramètre	Détails
Section <b>Import Configuration</b>	Pour importer un fichier de configuration, cliquer sur le bouton [ <b>Browse</b> ], sélectionner un fichier, cliquer sur le bouton [ <b>Ouvrir</b> ], puis sur le bouton [ <b>Import configuration file</b> ].
Section <b>Export Configuration</b>	Pour exporter une configuration dans un fichier XML, cocher la ou les cases de votre choix (Toutes, Configuration coffres, Configuration intrusion, Configuration transmission), puis cliquer sur le bouton [ <b>Export configuration file</b> ].
Section <b>Download exported configuration</b>	A la fin de l'export d'une configuration, cliquer sur le bouton [ <b>Download</b> ] pour récupérer le fichier de configuration au format XML, puis stocker ce fichier dans un dossier client.

4. Désactiver le port de maintenance (voir [Section 3.2.4.1, « Activation ou désactivation du port de maintenance d'une TILLYS »](#)), car laisser un port de maintenance ouvert constitue une faille de sécurité.

### 3.2.4.3. Prolongation de la durée de validité d'un token

Avant l'expiration du token qui gère la sécurité des échanges sur IP entre TILLYS au sein d'un groupe multi-TILLYS, une visite de technique de maintenance a été prévue, afin d'éviter toute interruption partielle de service.

Pour prolonger la durée de validité d'un token, créer un nouveau token et l'attribuer à la TILLYS périphérique dont le token arrive à expiration (voir [Section 3.2.1.4, « Configuration multi-TILLYS : génération sur la TILLYS hôte d'un token par TILLYS périphérique »](#)).

# Chapitre 4. Installation, paramétrage et utilisation du terminal TACTILLYS-IP CUBE

## 4.1. Opérations d'installation, de configuration et de maintenance d'un terminal TACTILLYS-IP CUBE

Ces opérations sont effectuées par le **partenaire** TIL TECHNOLOGIES.

### 4.1.1. Installation physique et connexion d'un terminal TACTILLYS-IP CUBE

Pour certains détail de l'installation physique et pour consulter les caractéristiques techniques, voir la [fiche technique du terminal TACTILLYS-IP CUBE](#).

1. Fixer au mur le support du TACTILLYS-IP en position horizontale.
2. Connecter un câble [RJ45](#) en face arrière du TACTILLYS-IP.
3. Enficher un lecteur de badge LEC05XF0200-NB6 sur l'un des 2 connecteurs prévus sur le TACTILLYS-IP.
4. Connecter en face arrière du TACTILLYS-IP un câble d'alimentation pour courant continu.
5. Fixer le TACTILLYS-IP sur son support mural.
6. Connecter le câble RJ45 du TACTILLYS-IP au réseau Ethernet.
7. Connecter le câble d'alimentation du TACTILLYS-IP à un bornier d'alimentation 12-28 V CC. L'écran du TACTILLYS-IP s'allume et le TACTILLYS-IP démarre.



Si l'alarme d'autoprotection se déclenche alors que le TACTILLYS-IP n'est pas encore fixé sur son support mural, voir [Section 4.2.5, « Arrêt de l'alarme d'autoprotection en phase d'installation du TACTILLYS-IP CUBE »](#).

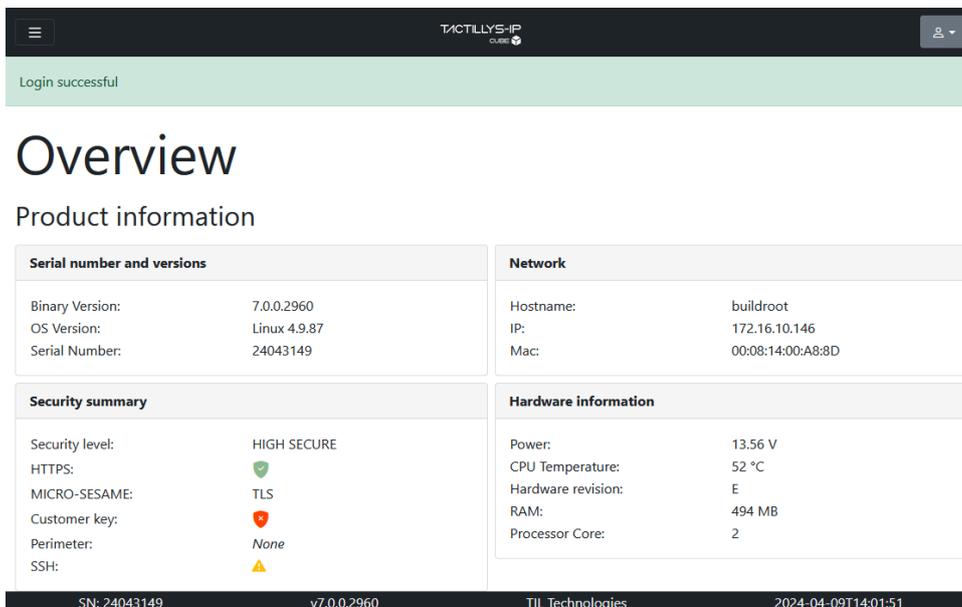
Il est également possible de débrancher et de rebrancher l'alimentation du TACTILLYS-IP, mais ceci fait redémarrer le TACTILLYS-IP (et interrompt l'éventuel processus de paramétrage en cours).

### 4.1.2. Accès à l'interface d'administration du terminal TACTILLYS-IP CUBE et affichage des caractéristiques produit

1. Se procurer le plan d'adressage réseau pour trouver une adresse IP disponible pour le [TACTILLYS-IP CUBE](#).
2. Sur un PC portable connecté au réseau Ethernet, ouvrir un navigateur et saisir l'adresse IP par défaut du TACTILLYS-IP CUBE : 172.16.5.240.
3. Saisir le login et le mot de passe d'accès par défaut (admin/admin). L'écran d'accueil (Overview) s'affiche. Il contient des informations sur la configuration du TACTILLYS-IP.

Il est possible d'afficher cet écran à tout moment, en cliquant sur le logo TACTILLYS-IP en haut de l'écran ou cliquer sur l'icône  burger, puis suivre **System information > Overview**.

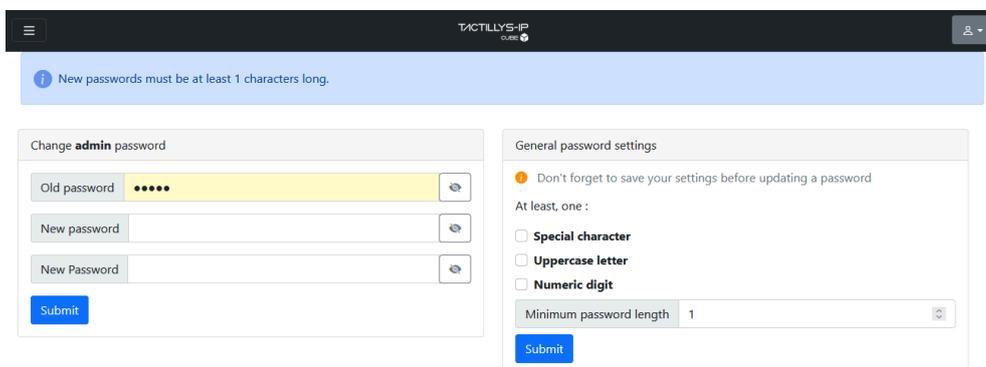
**Figure 4.1. Écran d'accueil du TACTILLYS-IP (10010-028)**



### 4.1.3. Changement du mot de passe administrateur du terminal TACTILLYS-IP CUBE

1. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer en haut à droite de l'écran sur l'icône  User et suivre **User settings**.

**Figure 4.2. Écran d'accueil du TACTILLYS-IP CUBE (10010-029)**



2. Dans les deux champs **New password** (voir figure ci-après), saisir obligatoirement un nouveau mot de passe pour remplacer le mot de passe par défaut (et le noter dans un lieu sécurisé, de manière à garantir sa sécurité).
3. Cliquer sur le bouton [ **Submit** ] dans la section gauche de l'écran.



Avant de choisir le nouveau mot de passe, la section située à droite sur cet écran permet de définir le niveau de sécurité requis pour celui-ci, en cohérence avec le niveau de sécurisation du site (caractères spéciaux, majuscules, chiffres et longueur du mot de passe). Cette section comporte un bouton [ **Submit** ] qui lui est propre.

#### 4.1.4. Réglage de l'heure du terminal TACTILLYS-IP CUBE

L'heure n'est pas gérée par un serveur *NTP* externe. En revanche, elle est téléchargée par la TILLYS dans le terminal TACTILLYS-IP CUBE associé :

- Lors du démarrage ou du redémarrage de la TILLYS,
- Lors de la modification de la date ou de l'heure de la TILLYS,
- Lors de la configuration du TACTILLYS-IP CUBE depuis l'interface web de la TILLYS (ou par import XML).

Il est nécessaire qu'elle corresponde avec celle de la TILLYS pour l'installation des certificats.

S'il devait exister un décalage des horloges du TACTILLYS-IP et de la *TILLYS*, l'heure qui serait prise en compte serait celle à laquelle la TILLYS reçoit les messages ou l'heure à laquelle la TILLYS déclenche l'armement ou le désarmement du site.

Lors du passage à l'heure d'été ou d'hiver, le TACTILLYS-IP CUBE gère automatiquement le changement d'heure.

Il n'est donc presque jamais nécessaire de régler l'heure manuellement.

1. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Maintenance > Date & Time**.

**Figure 4.3. Réglage de la date et de l'heure du TACTILLYS-IP CUBE (10010-030)**



2. Saisir la date, saisir l'heure, puis cliquer sur le bouton [ **Submit** ]. La date et l'heure saisies s'affichent dans la barre d'état, en bas à droite de l'écran.

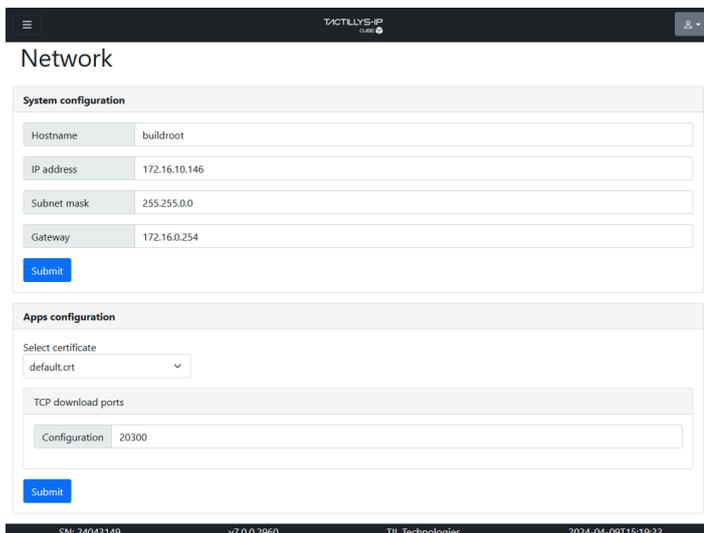
#### 4.1.5. Paramétrage réseau du TACTILLYS-IP CUBE

Pour éviter les conflits d'adresse en cas d'ajout de plusieurs TACTILLYS-IP CUBE, et pour des raisons de sécurité, ne pas laisser l'adresse par défaut du TACTILLYS IP.

Il est également possible de modifier les paramètres réseau à partir du terminal intrusion TACTILLYS-IP CUBE : voir [Section 4.2.4, « Choix des paramètres réseau du TACTILLYS-IP CUBE »](#).

1. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Configuration > Network**.

**Figure 4.4. Configuration réseau du TACTILLYS-IP CUBE (10010-031)**

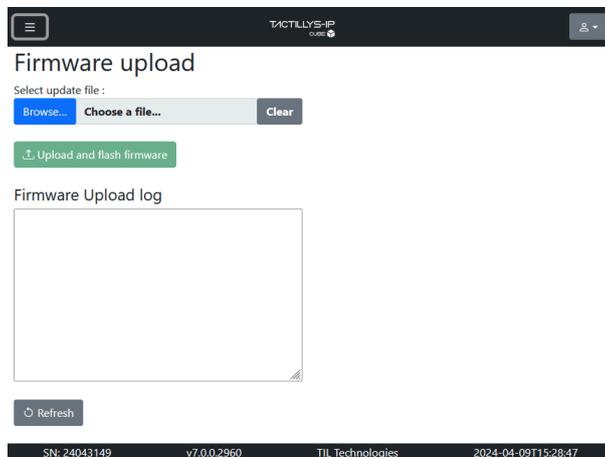


2. Saisir au minimum le [nom d'hôte \(Hostname\)](#), l'adresse [IP \(IP address\)](#), le [masque de sous-réseau \(Subnet mask\)](#) et la [passerelle \(Gateway\)](#), puis cliquer sur le bouton [**Submit**].
3. Cet écran permet, en partie basse, de modifier le [port TCP](#) de téléchargement (20300 par défaut), si ce [port](#) est utilisé pour d'autres applications sur votre réseau (en cas de doute, voir avec le [DSSI](#) du site).

#### 4.1.6. Mise à jour du firmware du TACTILLYS-IP CUBE

Il est toujours bon de charger dans le TACTILLYS-IP CUBE le firmware le plus récent.

1. Dans [l'espace de téléchargement du site du support technique TIL TECHNOLOGIES](#), télécharger le dernier firmware pour le terminal TACTILLYS-IP CUBE et le placer sur le bureau de l'ordinateur.
2. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Maintenance > Firmware Upload**.

**Figure 4.5. Mise à jour du firmware du TACTILLYS-IP CUBE (10010-032)**

3. Cliquer sur le bouton [ **Browse** ] et sélectionner sur le bureau le fichier du firmware à charger sur le TACTILLYS IP, valider, puis cliquer sur le bouton [ **↑ Upload and flash firmware** ]. Cette opération prend plusieurs minutes, puis le TACTILLYS-IP redémarre.

#### 4.1.7. Paramétrage de la journalisation des événements du TACTILLYS-IP CUBE

1. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Maintenance > Log tracer**.
2. Pour envoyer le journal à une adresse IP particulière, saisir cette adresse IP et le port de destination (514 par défaut), cliquer sur le commutateur Syslog (gris > bleu), puis cliquer sur le bouton [ **Submit** ].

Pour enregistrer le journal dans un fichier, cliquer sur le commutateur Syslog (gris > bleu), puis cliquer sur le bouton [ **Submit** ].

Il est possible d'activer les deux commutateur.

3. Choisir le niveau de détail pour les 7 types de trace et cliquer sur le bouton [ **Submit** ].
4. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Intrusion CUBE > Configuration télétransmission**.
5. Au moins un destinataire principal doit être activé. Pour déclarer un destinataire, voir [Section 5.7, « Déclaration des opérateurs de détection d'intrusion sur la TILLYS »](#).

#### 4.1.8. Désensibilisation du TACTILLYS-IP CUBE

Cette opération de maintenance consiste à supprimer d'un TACTILLYS-IP CUBE les clés propres à un site. Elle ne doit être effectuée que lorsqu'un TACTILLYS-IP CUBE est retiré d'une installation

pour l'installer dans une autre, ou avant de l'envoyer au SAV TIL TECHNOLOGIES (sur demande du service client).

1. À partir de l'interface d'administration du TACTILLYS-IP CUBE, cliquer sur l'icône  burger en haut à gauche de l'écran et suivre **Maintenance > Erase keys**.
2. Cliquer sur le bouton [ **Erase keys** ].

## 4.2. Paramétrage du terminal TACTILLYS-IP CUBE

Ces opérations sont effectuées sur le terminal TACTILLYS-IP CUBE par les **utilisateurs disposant des droits intrusion**.

L'utilisateur disposant des droits intrusion passe un badge devant le lecteur du terminal intrusion TACTILLYS-IP CUBE.

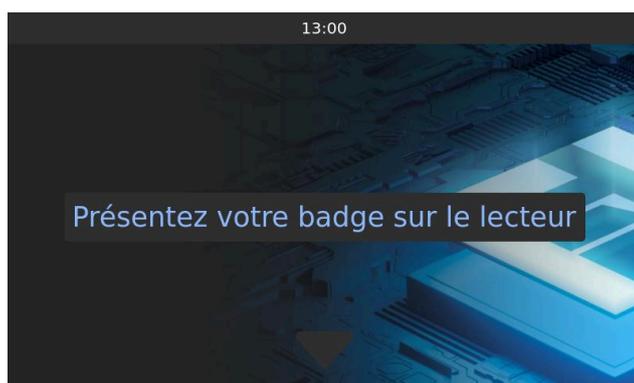
Selon la configuration, il devra peut-être en plus saisir un code (voir [Section 3.2.2.3, « Choix du mode d'authentification \(badge ou badge + code\) sur un TACTILLYS-IP CUBE »](#)).

### 4.2.1. Authentification et navigation sur un terminal TACTILLYS-IP CUBE

Pour pouvoir accéder à l'écran d'accueil du [TACTILLYS-IP CUBE](#), il est nécessaire d'utiliser un badge reconnu par le système de détection d'intrusion : voir [Section 5.2, « Procédure de préparation d'un badge de gestion d'intrusion CUBE sur terminal TACTILLYS-IP CUBE »](#).

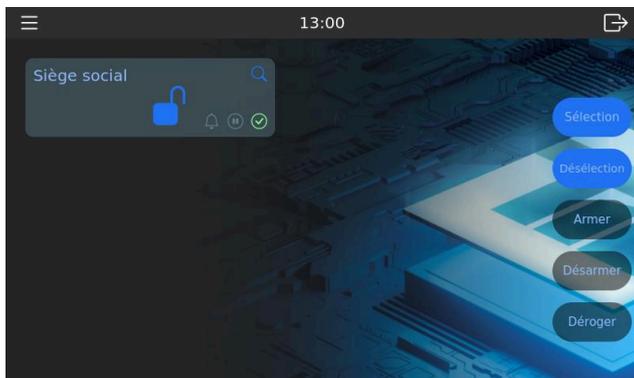
1. En veille, le message "Présentez votre badge sur le lecteur" est affiché sur le terminal TACTILLYS-IP CUBE.

**Figure 4.6. Écran de veille du TACTILLYS-IP CUBE (10010-502)**



2. Passer un badge devant le lecteur (et si nécessaire, saisir le code d'accès et valider) : l'écran d'accueil s'affiche. Cet écran liste les groupes gérés au niveau de ce terminal.

**Figure 4.7. Écran d'accueil du TACTILLYS-IP CUBE (10010-503)**



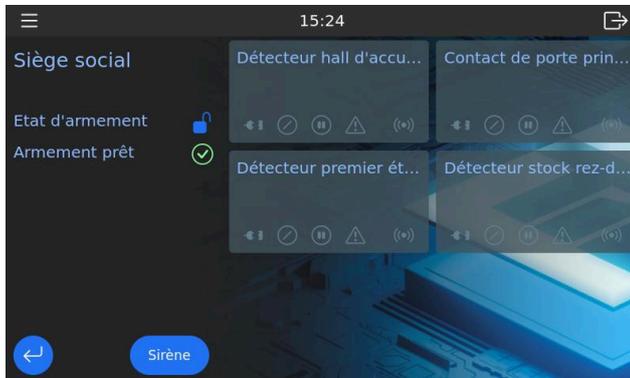
Le tableau ci-après présente la signification des pictogrammes sur cet écran.

**Tableau 4.1. Signification des pictogrammes sur l'écran de la liste des groupes sur le terminal TACTILLYS-IP CUBE**

Pictogramme	Signification
	Heure du prochain armement
	Temporisation d'entrée ou de sortie
	Déroger en cours
	Pré-alarme en cours
	Groupe armé
	Groupe désarmé
	Affichage des détails du groupe (pictogramme vert)
	Armement prêt
	Armement non prêt
	Affichage de la synthèse des alarmes

3. Toucher le pictogramme vert loupe.

**Figure 4.8. Écran des détecteurs d'un groupe sur le TACTILLYS-IP CUBE (10010-504)**



Le tableau ci-après présente la signification des pictogrammes sur l'écran du détail d'un groupe.

**Tableau 4.2. Signification des pictogrammes des détecteurs sur le terminal TACTILLYS-IP CUBE**

Pictogrammes au niveau des détecteurs	Signification
←	État d'éjection (orange = éjecté)
⊘	État d'inhibition (orange = inhibé)
⏸	Temporisation d'entrée ou de sortie (orange = temporisation en cours)
↻	Dérogation en cours
⦿	État d'alerte (orange = alarme, rouge = auto-protection)

4. Toucher le bouton [ **Sirènes** ].

**Figure 4.9. Écran des sirènes d'un groupe sur le TACTILLYS-IP CUBE (10010-505)**



Le tableau ci-après présente la signification des pictogrammes sur l'écran des sirènes.

**Tableau 4.3. Signification des pictogrammes des sirènes sur le terminal TACTILLYS-IP CUBE**

Pictogrammes de l'écran des sirènes	Signification
	État d'alarme (orange = alarme en cours)
	État d'inhibition (orange = inhibé)

5. Pour afficher de nouveau l'écran des détecteurs, toucher le bouton [ **Détecteurs** ].

Pour afficher de nouveau l'écran d'accueil, toucher le bouton [ # ], en bas à gauche de l'écran.

Le tableau ci-après présente la signification des pictogrammes sur l'écran d'éjection, qui s'affiche lorsqu'un détecteur est en défaut.

**Tableau 4.4. Signification des pictogrammes d'éjection de détecteur sur le terminal TACTILLYS-IP CUBE**

Pictogrammes de l'écran d'éjection	Signification
	État d'éjection (orange = éjecté)
	Indication de l'état du défaut en cours (orange = alarme, rouge = auto-protection)

## 4.2.2. Consultation des caractéristiques de fonctionnement du TACTILLYS-IP CUBE

À partir de l'écran d'accueil du TACTILLYS-IP CUBE, toucher l'icône  burger en haut à gauche de l'écran, puis l'option **A propos**.

Les caractéristiques de fonctionnement du TACTILLYS-IP CUBE s'affichent.

**Figure 4.10. Caractéristiques de fonctionnement du TACTILLYS-IP CUBE (10010-034)**



## 4.2.3. Paramétrage du TACTILLYS-IP CUBE

À partir de l'écran d'accueil du TACTILLYS-IP CUBE, toucher l'icône  burger en haut à gauche de l'écran, puis l'option **Paramètres**.

La luminosité de l'écran est réglable, ainsi que le volume sonore.

Il existe 4 thèmes et l'interface est disponible en français, allemand et anglais. Les nouveaux paramètres sont pris en compte sans qu'il soit nécessaire de valider ni de redémarrer.

**Figure 4.11. Paramètres de l'IHM du TACTILLYS-IP CUBE : luminosité, thème, langue, niveau sonore (10010-035)**



#### 4.2.4. Choix des paramètres réseau du TACTILLYS-IP CUBE

1. À partir de l'écran d'accueil du TACTILLYS-IP CUBE, toucher l'icône  burger en haut à gauche de l'écran, puis l'option **Réseau**.

**Figure 4.12. Choix des paramètres réseau du TACTILLYS-IP CUBE (10010-036)**



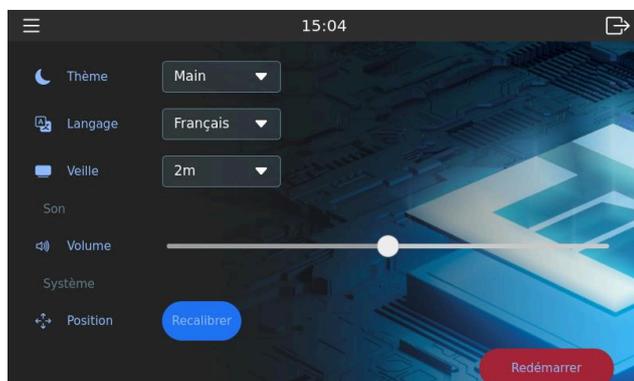
2. Modifier les informations, puis toucher le bouton **[Sauvegarder]**.

#### 4.2.5. Arrêt de l'alarme d'autoprotection en phase d'installation du TACTILLYS-IP CUBE

Pendant la phase de configuration, lors de laquelle le terminal intrusion n'est pas encore fixé sur son support et peut déclencher une alarme d'autoprotection, il est possible de réinitialiser le capteur de position (ce qui arrête également l'alarme).

1. À partir de l'écran d'accueil du TACTILLYS-IP CUBE, toucher l'icône  burger en haut à gauche de l'écran, puis l'option **Paramètres**.
2. Afficher le bas de cet écran en le faisant défiler avec le doigt, puis à droite de l'option **Position**, toucher le bouton **[ Recalibrer ]**.

**Figure 4.13. Arrêt de l'alarme d'autoprotection du TACTILLYS-IP CUBE (10010-037)**



#### 4.2.6. Déconnexion automatique du TACTILLYS-IP CUBE

La temporisation de passage en veille est réglable sur l'écran **Paramètres** du TACTILLYS-IP CUBE.

1. Passer un badge devant le lecteur du TACTILLYS-IP CUBE (et si nécessaire, saisir le code d'accès et valider) : l'écran d'accueil s'affiche.
2. Toucher l'icône  burger en haut à gauche de l'écran, puis l'option **Paramètres**.
3. Sélectionner la valeur souhaitée dans la liste déroulante **Veille**.

### 4.3. Utilisation du TACTILLYS-IP CUBE

Selon la configuration et la complexité des sites, un ou plusieurs terminaux TACTILLYS-IP CUBE sont installés (voir [Section 1.2, « Vue d'ensemble de la version multi-TILLYS de l'intrusion CUBE »](#)).

#### 4.3.1. Armement ou désarmement manuel d'un groupe

L'armement d'un groupe est normalement effectué à l'heure qui a été définie. En cas de défaut sur un détecteur dont l'éjection automatique n'a pas été prévue, l'armement du groupe est impossible.

Si un collaborateur doit retourner brièvement dans les locaux de l'entreprise le week-end, il peut temporairement désarmer l'alarme. Il est possible que celle-ci se réarme automatiquement, de sorte à éviter un oubli qui laisserait le bâtiment hors surveillance pour le reste du week-end.

En cas d'alarme, un agent de sécurité va effectuer une levée de doute au niveau du détecteur. S'il s'agit d'un dysfonctionnement technique, il peut ensuite procéder à l'éjection manuelle du détecteur en défaut, avant de relancer l'armement du groupe (voir [Section 4.3.2, « Éjection manuelle de détecteurs en défaut »](#)).

Les opérations d'armement et de désarmement sont possibles sur MICROSESAME au niveau du synoptique (voir [Section 5.6, « Consultation du synoptique sur MICROSESAME »](#)) ou sur le terminal TACTILLYS-IP CUBE.

1. Passer un badge devant le lecteur du TACTILLYS-IP CUBE (et si nécessaire, saisir le code d'accès et valider) : l'écran d'accueil s'affiche. Cet écran liste les groupes gérés au niveau de ce terminal.
2. Toucher le groupe à armer/désarmer, puis le bouton [ **Armer** ] ou [ **Désarmer** ].

### 4.3.2. Éjection manuelle de détecteurs en défaut

Un détecteur en défaut dont l'éjection automatique n'a pas été prévue peut être éjecté au niveau du synoptique (voir [Section 5.6, « Consultation du synoptique sur MICROSESAME »](#)) ou sur le terminal TACTILLYS-IP CUBE.

1. Passer un badge devant le lecteur du TACTILLYS-IP CUBE (et si nécessaire, saisir le code d'accès et valider) : l'écran d'accueil s'affiche. Cet écran liste les groupes gérés au niveau de ce terminal.
2. Toucher l'icône  burger en haut à gauche de l'écran, puis l'option **Ejection**.
3. Toucher le détecteur en défaut (pictogramme  orange ou rouge), puis le bouton [ **Ejecter** ].

### 4.3.3. Arrêt des sirènes

Une sirène peut être arrêtée sur le synoptique (voir [Section 5.6, « Consultation du synoptique sur MICROSESAME »](#)) ou sur le terminal TACTILLYS-IP CUBE.

1. Passer un badge devant le lecteur du TACTILLYS-IP CUBE (et si nécessaire, saisir le code d'accès et valider) : l'écran d'accueil s'affiche. Cet écran liste les groupes gérés au niveau de ce terminal.
2. Toucher le pictogramme vert  loupe du groupe comportant la sirène à arrêter .
3. Toucher le sirène qui sonne (pictogramme  orange ou rouge), puis le bouton [ **Stop sirène** ].

### 4.3.4. Dérogation d'armement sur groupe(s) de détecteurs

L'armement d'un groupe peut être programmé pour avoir lieu automatiquement à une certaine heure. Cependant, les utilisateurs peuvent parfois avoir besoin de rester sur site après l'heure de mise en surveillance, et donc ils peuvent avoir besoin de repousser celle-ci du temps qui leur est nécessaire.

Cependant, pour des raisons de sécurité, ce temps peut être limité, par le responsable sûreté par exemple.

Lorsque la pré-alarme retentit, les personnes encore présentes dans les locaux doivent sortir avant l'expiration du délai de sortie ou, s'ils y sont autorisés, s'identifier sur le terminal TACTILLYS-IP CUBE et demander une dérogation.

1. Passer un badge devant le lecteur du TACTILLYS-IP CUBE (et si nécessaire, saisir le code d'accès et valider) : l'écran d'accueil s'affiche. Cet écran liste les groupes gérés au niveau de ce terminal.
2. Toucher le groupe sur lequel demander une dérogation, puis le bouton [ **Déroger** ] .
3. Choisir la durée de la dérogation et valider.

# Chapitre 5. Configuration et exploitation de l'intrusion CUBE

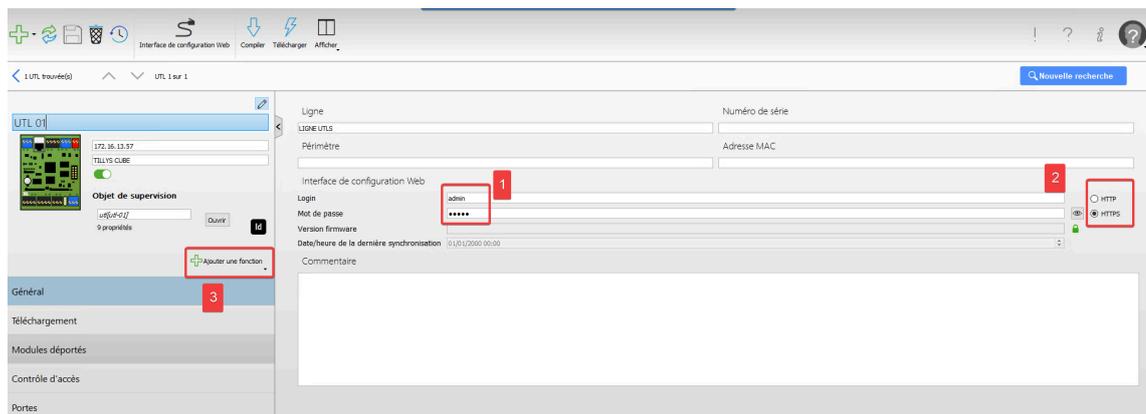
Ces opérations sont effectuées par le **responsable sécurité**.

## 5.1. Import de la configuration intrusion CUBE dans MICROSESAME

Dans le cas d'une configuration multi-TILLYS, toutes les **TILLYS (UTL)** doivent être connues de **MICROSESAME**. Un téléchargement complet est donc nécessaire.

1. Dans l'écran d'accueil de MICROSESAME, suivre **Paramétrage > Matériel > Unité de Traitement Local [UTL]**.
2. Double-cliquer sur le nom de la TILLYS dont le paramétrage doit être importé.

**Figure 5.1. Préparation de l'import de la configuration intrusion d'une TILLYS dans MICROSESAME (10010-038)**



3. Saisir le nom et le mot de passe (1), vérifier le niveau de sécurité (2) et cliquer sur le bouton **[+ Ajouter une fonction]** (3).
4. Dans la liste déroulante, cliquer sur **Intrusion CUBE**.
5. Dans la partie droite de l'écran, cliquer sur le bouton **[Importer la configuration d'intrusion CUBE]**.

## 5.2. Procédure de préparation d'un badge de gestion d'intrusion CUBE sur terminal TACTILLYS-IP CUBE

Un partenaire TIL Technologies, un agent d'accueil ou un agent de sûreté procède à la préparation d'un badge d'accès au terminal anti-intrusion TACTILLYS-IP CUBE dans MICROSESAME, en suivant les étapes décrites dans les sections ci-après.

### 5.2.1. Préparation d'un badge de contrôle anti-intrusion

L'acquisition d'un identifiant dans MICROSESAME lors de l'étape [Section 5.2.2, « Acquisition d'un identifiant non attribué dans MICROSESAME »](#) est effectuée en passant un badge devant un lecteur de contrôle d'accès.



Le lecteur intégré dans le terminal TACTILLYS-IP CUBE n'est pas un lecteur de contrôle d'accès mais un lecteur de contrôle anti-intrusion.

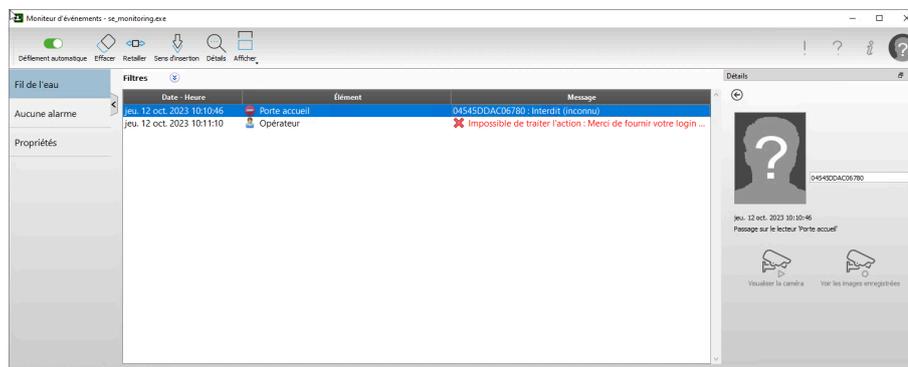
### 5.2.2. Acquisition d'un identifiant non attribué dans MICROSESAME

1. Depuis le menu-principal de MICROSESAME, suivre **Exploitation > Supervision > Moniteur d'évènements [MON]**.
2. Passer un badge non attribué devant le lecteur de contrôle d'accès. Un signal sonore indique que le lecteur fonctionne mais l'accès est interdit car le badge est inconnu (il n'a pas encore été attribué).

Son [identifiant](#) a été acquis par MICROSESAME (il est visible dans le moniteur d'événements) et il est disponible pour un nouvel identifié.

Si le lecteur n'émet pas de signal sonore/visuel, voir l'erreur 00003 dans la section Résolution de problèmes.

3. Cliquer sur l'icône **[Détails]**, en haut à gauche de l'écran. Le détail du badge apparaît dans la fenêtre de droite.



4. A droite de l'emplacement de la photo, placer l'identifiant en surbrillance avec la souris et taper **CTRL + C**. L'identifiant est copié en mémoire : continuer [Section 5.2.3, « Affectation d'un identifiant disponible à un nouvel identifié »](#).

### 5.2.3. Affectation d'un identifiant disponible à un nouvel identifié

1. Depuis le menu-principal de MICROSESAME, suivre **Exploitation > Contrôle d'accès > Identifiés [IDE]**.
2. En haut à gauche de l'écran, cliquer sur **Ajouter**  , renseigner le nom et le prénom du nouvel identifié, puis cliquer sur **Créer**.
3. Cliquer sur **Identifiants**, faire un clic-droit dans la section inférieure de l'écran et cliquer sur **Créer un identifiant**.
4. Taper **CRTL + V**. L'*identifiant* copié (voir [Section 5.2.2, « Acquisition d'un identifiant non attribué dans MICROSESAME »](#)) est collé dans la colonne Code.
5. Saisir une date de début et de fin de validité, puis cliquer sur Entrée.
6. Cliquer sur **Enregistrer**  : le téléversement de ces informations dans la TILLYS est effectué.
7. Depuis le menu principal, suivre **Exploitation > Supervision > Moniteur d'évènements [MON]** (affichage du **Moniteur d'évènement**) et passer le badge devant le lecteur.

Le badge est maintenant associé au nom de la personne que vous avez saisi mais son accès est toujours interdit (pas d'accès au lecteur) et ceci est tout à fait normal car il n'est pas encore associé à des droits d'accès.

Il ne possède pas non plus de profil intrusion CUBE lui permettant d'accéder à un terminal TACTILLYS-IP CUBE.

### 5.2.4. Attribution de droits d'accès à un nouvel identifié

1. Depuis le menu-principal de MICROSESAME, suivre **Exploitation > Contrôle d'accès > identifiés [IDE]**.
2. Rechercher l'*identifié* précédemment créé.
3. Dans sa fiche identifié, cliquer sur **Accès**.
4. Dans la partie inférieure droite cliquer sur .
5. Dans la liste qui s'ouvre, cliquer sur **Tous les sites actuels et futurs**.
6. Dans la fenêtre de paramétrage d'accès qui s'affiche, cliquer sur **OK** (validation des accès 24/24).
7. Cliquer sur **Enregistrer** .
8. Afficher le **Moniteur d'évènement**(depuis le menu principal, suivre **Exploitation > Supervision > Moniteur d'évènements [MON]**), passer le badge devant chaque lecteur attribué précédemment et vérifier qu'en plus que l'identifié soit reconnu, son accès est maintenant autorisé.

### 5.2.5. Attribution d'un profil intrusion CUBE à un nouvel identifié

Les identifiés chargés de gérer un terminal TACTILLYS-IP CUBE doivent disposer au minimum du profil intrusion correspondant à ce terminal.

Ils doivent également disposer de droits d'accès au bâtiment sur les lecteurs de contrôle d'accès.

1. Depuis le menu-principal de MICROSESAME, suivre **Exploitation > Contrôle d'accès > identifiés [IDE]**.
2. Rechercher l'*identifié* précédemment créé.
3. Dans sa fiche identifié, cliquer sur **Accès**.
4. Dans la partie inférieure droite cliquer sur .
5. Cliquer sur le menu burger en milieu de la partie droite de l'écran, puis cocher la case Afficher les profils intrusion CUBE.
6. Dans la section droite, cliquer sur le profil intrusion, cliquer sur la flèche < pour faire passer ce profil dans la section gauche de l'écran.
7. Attribuer de la même manière les droits d'accès au bâtiment dont cet identifié a besoin.
8. Cliquer sur **Enregistrer** .
9. Depuis le menu-principal, suivre **Paramétrage > Matériel > Unités de Traitement Local [UTL]**.
10. Double-cliquer sur la ligne de la TILLYS (*UTL*) connectée au TACTILLYS.
11. Cliquer sur le bouton , puis sur le bouton .
12. Cocher la case Accès et cliquer sur le bouton **[ Exécuter ]**.

### 5.3. Gestion des profils intrusion des identifiés sur MICROSESAME ou WEBSesame

Les profils intrusion peuvent être ajoutés aux profils d'accès des identifiés.

Ils sont également gérables en important des fichiers CSV au bon format, préparés par les services RH, conformément aux processus mis en place par la société utilisatrice du système anti-intrusion.

Voir [Section 3.2.2.1, « Création des profils intrusion sur la TILLYS hôte »](#).

### 5.4. Affichage du nom des opérateurs à l'origine d'évènements de commande intrusion

Il est possible d'afficher le nom et le prénom des opérateurs à l'origine des évènements de commande, en paramétrant le texte associé aux identifiés dans l'option Contrôle d'accès de la TILLYS hôte. Voir les sections ci-après.

### 5.4.1. Ouverture de la fiche de configuration de la TILLYS hôte et de l'écran des paramètres de contrôle d'accès

1. À partir de l'écran d'accueil de MICROSESAME, suivre **Paramétrage > Paramétrage > Matériels > Unités de Traitement Local [ UTL ]**.
2. Double-cliquer sur la ligne de la TILLYS hôte. La fiche de configuration s'affiche.
3. Dans la section gauche de l'écran, cliquer sur l'option **Contrôle d'accès**.
4. Continuer à la section [Section 5.4.2, « Choix du texte associé aux identifiés »](#).

### 5.4.2. Choix du texte associé aux identifiés

Le champ **Texte associé aux identifiés** permet d'afficher un texte de maximum 20 caractères sur un clavier afficheur, en fonction de l'identifié qui s'authentifie.

Il est possible de récupérer et utiliser certaines informations complétées dans la gestion des identifiés :

- Le nom : [lastName]
- Le prénom : [firstName]
- Les libellés de 1 à 16 : [LIB\_01] pour le libellé 1, [LIB\_02] pour le libellé 2 .... [LIB\_16] pour le libellé 16.



Pour afficher sur le clavier le nom suivi du prénom il suffit d'écrire dans le champ teste : [lastName] [firstName]

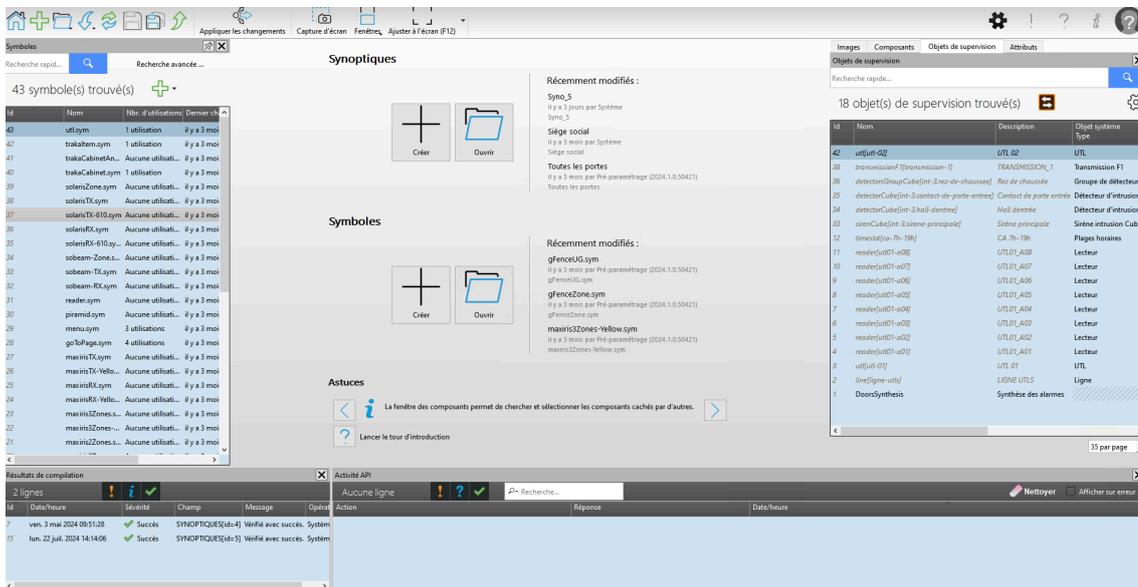
Cliquer sur l'assistant pour consulter des exemples et les options disponibles.

## 5.5. Paramétrage du synoptique sur MICROSESAME

De la même manière que les objets porte simplifient le contrôle d'accès grâce à leur représentation graphique, les objets de supervision simplifient la gestion de l'intrusion.

1. À partir de l'écran d'accueil de MICROSESAME, suivre **Paramétrage > Supervision > Éditeur de synoptique [EDI]**.

**Figure 5.2. L'éditeur de synoptique de MICROSESAME (10010-039)**



2. Faire glisser les objets intrusion (détecteurs, sirènes, TILLYS) de la fenêtre de droite vers l'espace central, à l'emplacement souhaité sur la représentation graphique ou photographique du site.
3. Pour chacun de ces objets, il est possible de cliquer sur les trois points superposés (en haut à droite de chaque objet) pour afficher des options. Pour recevoir les événements d'un objet intrusion, cocher sa case **Historique**.

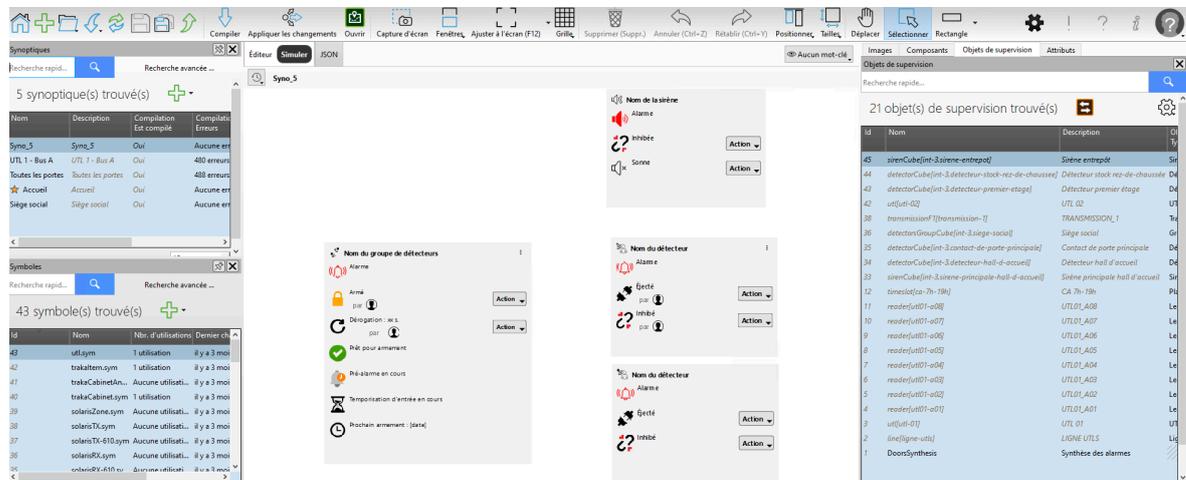
Pour plus d'informations, voir la partie sur l'éditeur de synoptiques dans le [Guide de référence de MICROSESAME](#).

4. Enregistrer la configuration.

## 5.6. Consultation du synoptique sur MICROSESAME

Voir la partie sur la visualisation des synoptiques dans le [Guide de référence de MICROSESAME](#).

Figure 5.3. Consultation du synoptique de MICROSESAME (10010-040)



## 5.7. Déclaration des opérateurs de détection d'intrusion sur la TILLYS

Une fois les profil intrusion définis et cette configuration chargée sur MICROSESAME, il est possible d'attribuer un profil intrusion aux personnes qui doivent gérer l'armement et le désarmement de l'alarme sur terminal TACTILLYS-IP CUBE.

Voir [Section 5.3, « Gestion des profils intrusion des identifiés sur MICROSESAME ou WEBSESAME »](#).

## 5.8. Test de l'installation de détection d'intrusion

### 5.8.1. Test des détecteurs

1. Cliquer sur l'icône  burger en haut à gauche de l'écran de la TILLYS hôte et suivre **Intrusion CUBE > Detector diagnostic**.
2. Circuler dans toutes les pièces du bâtiment comportant un détecteur (l'alarme ne sera pas déclenchée).
3. Vérifier dans le fil de l'eau que tous les détecteurs ont réagi.
4. Désactiver le mode Detector diagnostic.

### 5.8.2. Test de communication entre la TILLYS et le TACTILLYS-IP CUBE

Si la connexion entre le TILLYS et le terminal TACTILLYS-IP CUBE fonctionne, le passage d'un badge disposant des droits intrusion sur le lecteur du terminal TACTILLYS-IP CUBE active son écran d'accueil (ou son écran de saisie du code).

## Chapitre 6. Gestion de la sécurité par le responsable sécurité

### 6.1. Attribution des droits d'accès aux utilisateurs du TACTILLYS-IP CUBE

Cette section propose juste une formulation alternative : voir [Section 5.2.5, « Attribution d'un profil intrusion CUBE à un nouvel identifié »](#) ci-avant.

### 6.2. Changement de l'identifiant intrusion utilisé lors de l'identification badge + code sur TACTILLYS-IP CUBE

La modification du code identifié est effectuée dans MICROSESAME. Cette opération est suivie d'un téléchargement manuel dans la TILLYS.

1. Depuis le menu-principal de MICROSESAME, suivre **Exploitation > Contrôle d'accès > identifiés [IDE]**.
2. Cliquer sur l'onglet Accès, sélectionner le profil d'accès et cliquer sur le bouton **[ Identifiants ]**.
3. Faire défiler l'écran vers le bas et visualiser le code existant ou saisir un nouveau code, puis cliquer sur  Sauvegarder.
4. Pour choisir le mode d'authentification, voir [Section 3.2.2.3, « Choix du mode d'authentification \(badge ou badge + code\) sur un TACTILLYS-IP CUBE »](#).

### 6.3. Consultation de l'historique intrusion

Les opérateurs MICROSESAME ou WEBSesame se connectent sur l'interface web de la TILLYS hôte.

# Chapitre 7. Opérations liées à l'intrusion, effectuées par le télésurveilleur

## 7.1. Consultation des alarmes en cours

Le télésurveilleur peut consulter le détail des alarmes en cours sur son terminal.

Les informations qu'il reçoit lui permettent également de surveiller le bon fonctionnement de la liaison (voir [Section 7.1.1, « Syntaxe des messages de polling »](#) et [Section 7.1.2, « Syntaxe des messages de test cyclique »](#)).

### 7.1.1. Syntaxe des messages de polling

Le [polling](#) est un message de test envoyé par la TILLYS toutes les quelques secondes pour vérifier le bon fonctionnement de la transmission sur IP entre la TILLYS et le frontal de télésurveillance. Il est ensuite transmis au télésurveilleur.

#### Exemple de message de polling

```
E99B0013 "NULL" 0004L0#7005 [ ]
```

Ce message de test contient un message de type "NULL" ne contenant aucune donnée.

Pour activer et configurer le polling, voir [Section 3.2.1.12, « Configuration des télésurveilleurs »](#).

### 7.1.2. Syntaxe des messages de test cyclique

Le [test cyclique](#) est un message de test envoyé par la TILLYS pour vérifier le bon fonctionnement de la transmission sur IP entre la TILLYS et chaque télésurveilleur. Il est activé par exemple, toutes les 3 heures (180 minutes).

#### Exemple de message de test cyclique

```
4558001F "SIA-DCS" 0001L0#7005 [ #7005 | NRP ]
```

Dans ce message, N signifie nouveau et RP est le code événement désignant le test cyclique.

Pour activer et configurer le test cyclique, voir [Section 3.2.1.12, « Configuration des télésurveilleurs »](#).

## 7.2. Commande à distance de l'intrusion CUBE

En plus de l'appel téléphonique du site, de la police ou des pompiers, le télésurveilleur peut effectuer les actions présentées ci-après.

### 7.2.1. Armement

Ceci est possible mais ne se produit pratiquement jamais car il est difficile de vérifier à distance que les locaux sont vides.

### 7.2.2. Arrêt sirène

Le télésurveilleur peut arrêter les sirènes après avoir acquitté les alarmes.

### 7.2.3. Désarmement

Le télésurveilleur peut désarmer un groupe à distance si nécessaire.

### 7.2.4. Changement de valeur d'un registre de la TILLYS

Cette fonctionnalité est disponible à condition que le frontal du télésurveilleur et le logiciel de supervision du télésurveilleur soient compatibles avec ce changement de registre.