



CARDIGO - CONFIGURATION ET EXPLOITATION

Table des matières

Préface	6
1. Contexte d'utilisation de ce manuel	6
2. Réserve de propriété	6
3. Glossaire	6
1. Présentation générale	9
2. Configuration de l'écran CARDIGO	10
2.1. Accès au serveur web du CARDIGO	10
2.2. Configurer date et heure du clavier	10
2.3. Mettre à jour le Firmware	10
2.4. Gestion des certificats	10
2.5. Configurer le réseau	13
2.6. Mettre en place l'accès sécurisé au serveur web	14
2.7. Configuration	14
2.7.1. API configuration	14
2.7.2. Reader Configuration	15
2.7.3. General configuration	16
2.8. Aperçu général de la configuration système	16
3. Configuration dans MICROSESAME	18
3.1. Identifiés	18
4. Exploitation	19
4.1. Procédure d'activation des badges	19
4.2. Paramètres	20

Liste des illustrations

4.1. Fenêtre d'accueil 19

4.2. Exemple : Procédure réalisé avec succès19

4.3. Exemple : Échec de la procédure d'activation 19

Liste des tableaux

2.1. Configuration	10
2.2. Compatibilité format de certificats TLS	11
2.3. User submitted certificates	12
2.4. CA certificates	13
2.5. System configuration	13
2.6. Apps configuration	14
2.7. HTTPS	14
2.8. Connexion with MICROSESAME	14
2.9. Credential	15
2.10. Protocol Configuration	15
2.11. General Information	16
2.12. Serial number and versions	16
2.13. Security summary	16
2.14. Network	16
2.15. Hardware information	16

Préface

1. Contexte d'utilisation de ce manuel

Les pastilles de couleur orange ● en haut de chaque page signalent que ce document est un guide utilisateur.

Le partenaire ou installateur HIRSCH configure l'installation chez le client.

2. Réserve de propriété

Les informations contenues dans ce document peuvent être modifiées sans avertissement.

Les informations citées dans ce document à titre d'exemple, ne peuvent en aucun cas engager la responsabilité de la société HIRSCH Secure SAS (nommée HIRSCH dans les documents techniques). Les sociétés, noms et données utilisés dans les exemples sont fictifs, sauf notification contraire.

Toutes les marques citées sont des marques déposées de leurs propriétaires respectifs.

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

Merci d'envoyer vos commentaires, corrections et suggestions concernant ce document à documentation@hirschsecure.fr, en précisant son numéro de référence, sa date et le numéro des pages concernées.

3. Glossaire

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

ANSSI

Acronyme d'Agence Nationale de Sécurité des Systèmes d'Information.

Institution française qui a défini en 2012 pour les sites sensibles des recommandations de sécurité renforcées, lesquelles ont été complétées en 2020 dans la note n° 7.

En jargon de la sécurité, on parle de site ANSSI ou non-ANSSI pour en désigner le niveau de sécurisation par rapport aux cyberattaques. Seuls les lecteurs "[transparent](#)s" sont conformes aux préconisations de l'ANSSI.

API

Acronyme anglais de "Application Programming Interface" (interface de programmation d'application).

Ensemble normalisé d'éléments informatiques intégrés à MICROSESAME qui permettent de mettre à disposition des services et ainsi de faire communiquer MICROSESAME avec d'autres logiciels.

Badge	Un badge permet d'identifier une personne sur un système de contrôle d'accès. Il comporte un identifiant (sécurisé ou pas) qui est détecté et traité par une tête de lecture physique. Cette opération peut nécessiter un contact direct (comme avec une carte à puce ou une bande magnétique) ou l'approche à distance (pour un badge NFC ou sans contact). Les badges les plus couramment utilisés sont de technologie MIFARE DESFIRE de type EV1, EV2 ou EV3.
CARDIGO	Clavier alloué à la fonction de validation et d'activation de badges, il est équipé d'un écran couleur 7 pouces et d'un lecteur de badges. Connecté à MICROSESAME via une connexion IP, il permet à un utilisateur d'activer son badge en saisissant un code qui lui a été précédemment transmis (par mail par exemple).
Certificat	Un certificat numérique est une sorte de passeport électronique qui permet à une personne, un ordinateur ou une organisation d'échanger de manière sûre des informations sur Internet en s'appuyant sur une infrastructure à clé publique (PKI). Les échanges entre TILLYS et MICROSESAME se font par défaut de façon sécurisée, à l'aide de certificats auto-signés. Pour les sites nécessitant un niveau de certification de type ANSSI, des certificats signés doivent obligatoirement être mis en œuvre.
Firmware	Microprogramme informatique stocké dans un équipement (TILLYS , modules, clavier TACTILLYS) qui définit son fonctionnement. Un firmware peut être mis à jour pour éviter de remplacer le matériel sur lequel il a été téléchargé.
GTB	Acronyme de Gestion Technique des Bâtiments. Système de pilotage, de contrôle, de supervision et d'optimisation des divers services comme l'éclairage, le chauffage ou la ventilation, présents dans les bâtiments tertiaires et industriels (immotique).
Identifiant	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.
Identifié	Personne physique devant disposer d'un accès au site protégé par le système de contrôle d'accès. Un identifié peut être porteur d'un ou de plusieurs identifiants distincts. Les identifiés peuvent être : • Des utilisateurs réguliers du système de contrôle d'accès, (identifiés de type "permanent")

- Des utilisateurs occasionnels du système de contrôle d'accès dans le cas de visites ou d'interventions externes par exemple, (identifiés de type "visiteur")

IP

Acronyme anglais d'Internet Protocol.

Le protocole Internet permet aux équipements qui l'utilisent de communiquer entre eux par paquets, de type [TCP](#) ou [UDP](#).

Le protocole IP est transporté par des réseaux locaux filaires utilisant le protocole de connexion Ethernet. Les cartes ou interfaces réseau équipées de connecteurs de type [RJ45](#) y ont accès physiquement et y sont identifiées logiquement via leur adresse IP.

MICROSESAME

Logiciel de supervision unifiée qui permet de centraliser toutes les informations électroniques du bâtiment : contrôle d'accès, détection intrusion, gestion technique, vidéo, interphonie... Le pilotage des différentes fonctions à travers une interface graphique commune rend leur exploitation beaucoup plus simple et les interventions plus efficaces. Les interactions entre les différents systèmes pouvant être complètement automatisées (actions sur événements), la rapidité des traitements est également garantie.

TILLYS

Automate [IP](#) programmable multifonction développé par HIRSCH qui dispose des fonctionnalités de contrôle d'accès, de détection intrusion et de [GTB](#). Grâce à 3 bus RS 485 (A, B et C), chaque TILLYS permet le raccordement de 8, 16 ou 24 lecteurs pour le contrôle d'accès. Elle constitue également une véritable centrale d'alarme. Voir aussi [UTL](#).

UTL

Acronyme d'Unité de Traitement Local.

Terme générique qui désigne un automate [IP](#) programmable et multifonction, utilisé dans le domaine du contrôle d'accès, de l'intrusion et de la GTB. C'est grâce à cet automate que vont être gérés par exemple, les accès des identifiés, les informations provenant des lecteurs ou des systèmes anti-intrusion, etc. L'UTL de HIRSCH est la [TILLYS](#), qui se décline en version V2, NG et CUBE.

Chapitre 1. Présentation générale

Le CARDIGO est un écran tactile ayant comme fonctionnement d'activer le badge inactif d'un identifié.



Le CARDIGO communique avec MICROSESAME via le réseau Ethernet (TCP / IP).

La configuration de l'écran s'effectue directement dans le serveur web embarqué dans le CARDIGO tandis que la gestion des identifiés se fait dans MICROSESAME ou WEBSesame.

L'identifié attendu sur site, reçoit un identifiant inactif (badge physique) et un code d'activation de manière séparée.



Par raison de sécurité, il est fortement recommandé d'envoyer le badge et code séparément.

A son arrivée sur site, il pourra ainsi activer son badge de façon autonome.

Chapitre 2. Configuration de l'écran CARDIGO

2.1. Accès au serveur web du CARDIGO

Depuis un navigateur web, se connecter sur le serveur web embarqué du CARDIGO.



En cas de sortie d'usine, renseigner l'adresse IP : 172.16.5.240.

Renseigner plus tard une adresse IP personnalisé.

Une page demande de définir le login et mot de passe lors de la première connexion.

2.2. Configurer date et heure du clavier

Cette configuration est accessible dans l'onglet **Maintenance > Date and Time**

Tableau 2.1. Configuration

Paramètres	Détails
Date	Renseigner la date
Time	Renseigner l'heure

2.3. Mettre à jour le Firmware

Cette configuration est accessible dans l'onglet **Maintenance > Firmware Upload**

Suivre la procédure ci-dessous pour mettre à jour le Firmware

1. Cliquer sur **Browse** et rechercher le fichier **.IMG**
2. Valider avec **Upload and Flash firmware**
3. Vérifier la complétion avec le log

2.4. Gestion des certificats

Cette configuration est accessible dans l'onglet **Configuration > Certificates**



Des certificats (auto-signés ou signés par un AC) sont nécessaire pour sécuriser :

- La connexion entre le CARDIGO et le serveur MICROSESAME
- L'accès au serveur web embarqué

Tableau 2.2. Compatibilité format de certificats TLS

Action	Fomats compatibles / Extensions	remarques
User submitted certificates : Import PFX	PKCS#12 • .pfx • .p12	N/A
User submitted certificates : Replace CSR	PEM • .crt • .cer • .pem	L'extension de fichier .cer peut aussi être liée à un fichier de type binaire, il convient de vérifier le format du certificat avant de l'importer.  Suivre la procédure suivante pour vérifier que le certificat est en format texte : 1. Effectuer un clic droit sur le certificat 2. Ouvrir avec un éditeur de texte type bloc-notes 3. Vérifier la présence des balises suivantes, respectivement en début et en fin de fichier : • -----BEGIN CERTIFICATE----- • -----END CERTIFICATE-----
CA certificates : Upload	PEM • .cer • .crt • .pem	L'extension de fichier .cer peut aussi être liée à un fichier de type binaire, il convient de vérifier le format du certificat avant de l'importer.

Action	Fomats compatibles / Extensions	remarques
		 Suivre la procédure suivante pour vérifier que le certificat est en format texte : 1. Effectuer un clic droit sur le certificat 2. Ouvrir avec un éditeur de texte type bloc-notes 3. Vérifier la présence des balises suivantes, respectivement en début et en fin de fichier : • -----BEGIN CERTIFICATE----- • -----END CERTIFICATE-----



Les formats **DER** (.cer ou .der) et **PKCS#7** (.p7b ou .p7c) ne sont pas supportés par la TILLYS.

Tableau 2.3. User submitted certificates

Paramètres	Détails
Self-signed certificates	Un certificat auto-signé est un certificat TLS qui est émis par l'entité qui l'utilise Fonction disponible • Generate self-signed
Certificates	Importer un certificat Fonction disponible • Import PFX

Paramètres	Détails
Certificate signature requests (CSR)	Requête envoyée à une autorité de certification (CA - Certificate Authority) pour demander la signature d'un certificat numérique. Fonction disponible • Generate CSR • Parcourir pour trouver un fichier .csr > Valider avec Replace CSR Suivre la procédure suivante pour ajouter un certificat signé 1. Cliquer sur la ligne de la requête CSR puis sur le bouton Browse file 2. Sélectionner le certificat signé puis cliquer sur le bouton Replace CSR  Le nom du fichier du certificat signé doit obligatoirement avoir le même nom que le CSR 3. Une fois le certificat importé, il apparaît dans la partie <i>certificates</i>

Tableau 2.4. CA certificates

Paramètres	Détails
CA certificates	Parcourir pour trouver un fichier .crt / pem / cer > Valider avec Upload

2.5. Configurer le réseau

Cette configuration est accessible dans l'onglet **Configuration > Network**

Tableau 2.5. System configuration

Paramètres	Détails
Hostname	Saisir le nom d'hôte
IP address	Adresse IP du serveur web CARDIGO
Subnet mask	Masque de sous-réseau du CARDIGO
Gateway	Passerelle du CARDIGO

Tableau 2.6. Apps configuration

Paramètres	Détails
Select certificate	Sélectionner un certificat
TCP download ports	Configurer le port de téléchargement TCP

2.6. Mettre en place l'accès sécurisé au serveur web

Cette configuration est accessible dans l'onglet **Configuration > Security**

Tableau 2.7. HTTPS

Paramètres	Détails
Select a certificate	Sélectionner un certificat

2.7. Configuration



Suivre les procédures afin d'obtenir le bon fonctionnement du CARDIGO.

2.7.1. API configuration

Tableau 2.8. Connexion with MICROSESAME

Paramètres	Détails
MICROSESAME IP address	Saisir l'adresse IP du poste serveur MICROSESAME
API Key	Saisir la clé de communication API avec le serveur MICROSESAME.

Paramètres	Détails
	 La clé API est dans les paramètres généraux : API REST et prendre la clé MICROSESAME.

Tableau 2.9. Credential

Paramètres	Détails
Login	Saisir le login opérateur MICROSESAME.
Password	Saisir le mot de passe opérateur.
Operator Profile	Renseigner l'ID du profil opérateur de connexion (Numéro se trouvant dans les identifiés MICROSESAME).



L'opérateur doit posséder les droits opérateur relatifs à la gestion des identifiés + identifiants + code badge

2.7.2. Reader Configuration

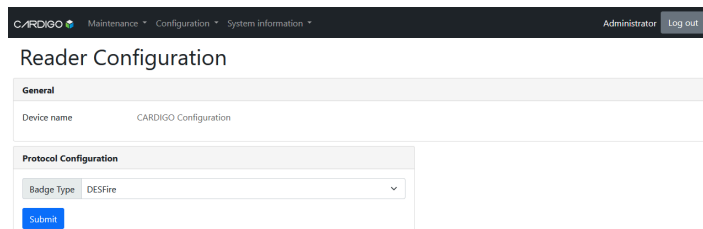


Tableau 2.10. Protocol Configuration

Paramètres	Détails
Badge Type	Définir le type de badge • DESFire : Uniquement pour la lecture de badge DESFire avec module lecteur SSCP • HID SEOS : Lecture de badge HID SEOS ou DESFire avec un module lecteur ELATEC

2.7.3. General configuration

Tableau 2.11. General Information

Paramètres	Détails
Company Name	Renseigner le nom de l'entreprise

2.8. Aperçu général de la configuration système

Cette page est accessible dans l'onglet **System information > Overview**

Product information

Tableau 2.12. Serial number and versions

Paramètres	Détails
Binaries version	Version du Firmware
OS version	Version du système d'exploitation
Serial number	Numéro de série de l'écran CARDIGO

Tableau 2.13. Security summary

Paramètres	Détails
Binaries version	Version du Firmware
HTTPS	Protocole de transfert hypertexte sécurisé
MICROSESAME	Système de communication entre MICROSESAME et l'écran CARDIGO

Tableau 2.14. Network

Paramètres	Détails
IP	Adresse IP du serveur web CARDIGO
Mac address	Adresse MAC du réseau

Tableau 2.15. Hardware information

Paramètres	Détails
Power	Puissance en volt de l'écran CARDIGO

Paramètres	Détails
RAM	RAM de l'écran CARDIGO
Processor cores	Cœurs de processeur de l'écran CARDIGO
CPU Temperature	Température du processeur de l'écran CARDIGO
Hardware revision	Révision du matériel

Chapitre 3. Configuration dans MICROSESAME

3.1. Identifiés

Afin de pouvoir être envoyées à l'identifié, renseigner toutes les informations relatives aux identifiants dans la fiche identifié

Identifiant	Statut	Date début de validité	Date fin de validité	Référence graphique	Modifiable	Numéro de série	Source	Dernier changement
00000000000000000000	Désactivé				Non			8/2 + 4 jours par ADMINISTRATEUR

Code clavier personnalisé

▼ ****

Dans la section Identifiants

- Attribuer la valeur de l'identifiant (code badge).
- Attribuer le code clavier personnalisé qui est attribué à l'identifié.



Pour définir la longueur du code clavier personnalisé, se rendre dans **Paramétrage général** puis **identifiés**.

Chapitre 4. Exploitation

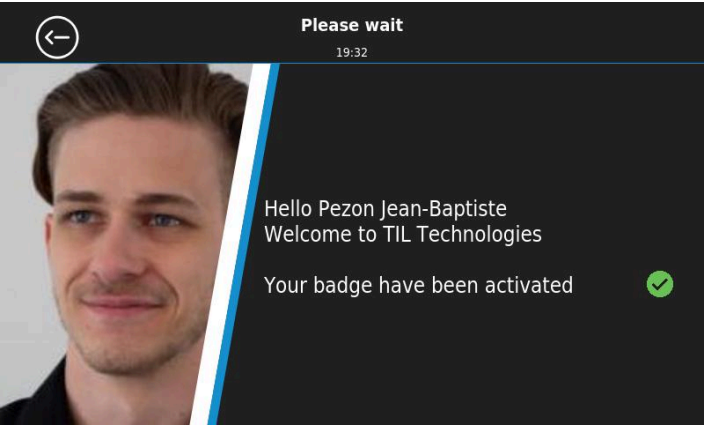
4.1. Procédure d'activation des badges

Figure 4.1. Fenêtre d'accueil

- **Bienvenue, veuillez présenter votre badge.**



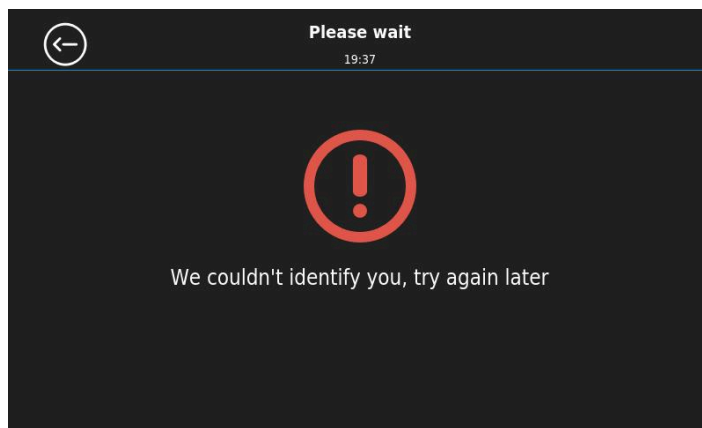
Figure 4.2. Exemple : Procédure réalisé avec succès



1	Présentation du badge sur le clavier.
2	L'identifié renseigne le code reçu par mail.
3	Le code correspond au code clavier personnalisé.
4	Le badge est activé.

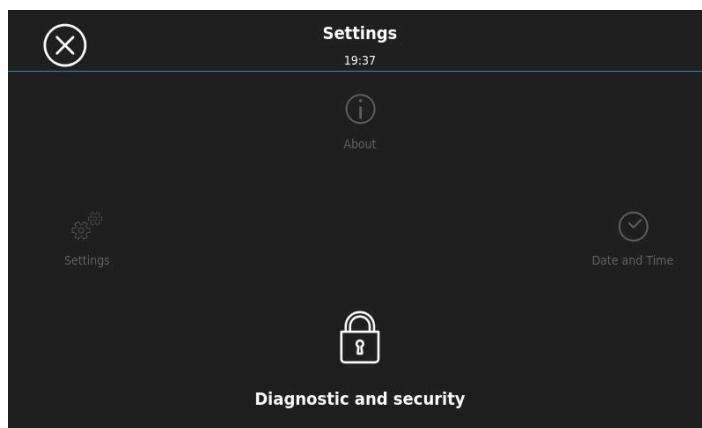
Figure 4.3. Exemple : Échec de la procédure d'activation

- **Nous n'avons pas pu vous identifier, réessayez plus tard.**

**Echec quand le statut est:**

- Oublié
- Perdu
- Volé
- Cassé
- Non rendu
- Inconnu

4.2. Paramètres

**Les paramètres du CARDIGO sont répartie en 4 groupes :**

- Settings (paramètres)
- Diagnostic and security (diagnostic et sécurité)
- Date and Time (Date et Heure)
- About (A propos)

Settings (paramètres)

- Affichage : luminosité, mise en veille de l'écran, personnalisation de l'écran de veille avec logo.
- Audio : volume de l'écran.
- Clavier : touches aléatoires à activer ou non (pendant la saisie du code clavier personnalisé).

Diagnostic and security (diagnostic et sécurité)

- Export des logs.
- Mise à jour du firmware par USB.
- Modification du mot de passe.
- Redémarrer.

Date and Time (Date et Heure)

- Choisir la date dans le calendrier, puis l'heure et les minutes.

About (A propos)

- Adresse IP.
- Adresse MAC.
- Adresse du bus.
- Version logicielle.
- Révision matérielle.
- Numéro de série.
- Température CPU.
- Tension d'alimentation.